REDES PRIVADAS VIRTUALES (RPVs)

SOLUCIÓN INTEGRAL DE SEGURIDAD

ENRIQUE CARLOS VANEGAS MATTOS

CORPORACIÓN UNIVERSITARIA TECNOLÓGICA DE BOLÍVAR

FACULTAD DE INGENIERÍA DE SISTEMAS

REDES Y COMUNICACIONES

CARTAGENA, DT Y C

2003

REDES PRIVADAS VIRTUALES (RPVs)

SOLUCIÓN INTEGRAL DE SEGURIDAD

ENRIQUE CARLOS VANEGAS MATTOS

CORPORACIÓN UNIVERSITARIA TECNOLÓGICA DE BOLÍVAR

FACULTAD DE INGENIERÍA DE SISTEMAS

REDES Y COMUNICACIONES

CARTAGENA, DT Y C

2003

REDES PRIVADAS VIRTUALES (RPVs)

SOLUCIÓN INTEGRAL DE SEGURIDAD

ENRIQUE CARLOS VANEGAS MATTOS

Monografía para optar el titulo de

Ingeniero de Sistemas

Director

Margarita Upegui

Magíster en Ciencias Computacionales

CORPORACIÓN UNIVERSITARIA TECNOLÓGICA DE BOLÍVAR

FACULTAD DE INGENIERÍA DE SISTEMAS

REDES Y COMUNICACIONES

CARTAGENA, DT Y C

2003

Nota de aceptación

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

A mis padres

Enrique y Mayra por su apoyo

incondicional, a mis hermanos,

a mis amigos y profesores.

AGRADECIMIENTOS

El autor expresa sus agradecimientos a:

Margarita Upegui, Ingeniera de Sistemas y Directora de la investigación, por sus valiosas orientaciones.

Eduardo Gómez, Ingeniero Eléctrico y Maestro en Ciencias Computacionales, por su constante motivación en este trabajo

CONTENIDO

Pág.

LISTA DE FIGURAS

Pág.

LISTA DE TABLAS

Pág.

GLOSARIO

Autenticación: Proceso de identificar positivamente a la entidad que solicita el acceso. La autenticación por lo general se realiza por medio de una función criptográfica.

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.

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.

Túnel de LAN a LAN: Utilizado en terminología RPV que permite varias sesiones dentro de un túnel.

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.

Cortafuego: 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.

Zona desmilitarizada (DMZ): Una DMZ es la *zona* física detrás de un *servidor de seguridad* de Internet y delante de un servidor de seguridad de segundo nivel que protege los sistemas y datos del servidor. En un escenario típico de una aplicación de Internet, la DMZ es la red de área local virtual (VLAN) física en la que se implementan los servidores Web.

Norma de cifrado de datos (DES): La norma de cifrado de datos desarrollada por IBM en 1977, es una cifra de bloques de 64 bits cifradas en bloques que utiliza una clave de 56 bits.

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 simple de transferencia de correspondencia (SMTP): Protocolo utilizado en Internet para transferir correo electrónico entre clientes y servidores.

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.

Algoritmo internacional de cifrado de datos (IDEA): Función criptográfica que utiliza una clave de 128 bits para cifrar; se usa en el popular paquete PGP.

1. INTRODUCCIÓN

En los últimos años las redes se han convertido en un factor crítico para cualquier organización. Cuando las redes transmiten información vital, dichas redes cumplen con atributos tales como seguridad, fiabilidad, alcance geográfico y efectividad en costos.

Se ha demostrado actualmente que las redes reducen, en tiempo y dinero, los gastos de las empresas, eso significa una gran ventaja para las organizaciones sobre todo las que cuentan con oficinas remotas a varios kilómetros de distancia; pero también es cierto que estas redes remotas han despertado la curiosidad de algunas personas que se dedican a atacar los servidores y las redes para obtener información confidencial. Por tal motivo la seguridad de las redes es de suma importancia, es por eso que se habla tanto de los “firewalls” y las RPVs.

Una Red Privada Virtual (RPV) conecta los componentes de una red sobre otra red. Las redes Privadas Virtuales logran este objetivo mediante la conexión de los usuarios de distintas redes a través de un “tunneling” que se construye sobre Internet o sobre cualquier red pública.

Las RPVs permiten a los usuarios trabajar en sus casas o empresas conectados de una forma segura con el servidor corporativo usando la infraestructura provista

por una red pública (como Internet). Desde el punto de vista del usuario, la RPV es un conexión entre el usuario y el servidor corporativo.

La naturaleza de la interconexión que está entre los dos es transparente para el usuario ya que los datos le aparecen como si fueran enviados a través de su red LAN, como si estuviera en la empresa. Esta tecnología también habilita a las empresas a tener conectadas oficinas centrales con sus sucursales sobre cualquier red pública, mientras se mantienen conexiones seguras. La RPV se conecta a través de la red Internet, formando una red WAN (Wide Area Network) entre los sitios conectados.

2. FUNDAMENTACIÓN

2.1 Definiciones

Virtual: Indica la conectividad dinámica en la red. Esta característica es debido a las necesidades de las organizaciones actuales, donde no existe un estándar en su conectividad, las cuales van creciendo incrementalmente. Este término también se puede asociar a la flexibilidad de los dispositivos que se presentan en la comunicación, adaptándose a los medios y características de transmisión que existan.

Los parámetros de seguridad en los sistemas de "tunneling" individuales se pueden establecer entre sitios no homogéneos y diferentes para alcanzar niveles aceptables de seguridad.

Privada: Indica la seguridad y garantía que debe tener la información que se envía por la red, y la disponibilidad de ésta para los usuarios autorizados. Esta característica es un reto sobre todo cuando se habla de transmisión de datos en Internet. La privacidad es típicamente considerada como el hecho de ocultar información. La RPV podrá ser tan segura como la red interna. La privacidad se presenta cuando un sistema de "tunneling" aparece como un enlace privado.

Cifrado: Indica el proceso de tomar un texto legible y convertirlo en un formato ilegible por medio de una función criptográfica.

Después de haber definido los conceptos de virtualidad, privacidad y cifrado podemos decir que una red privada virtual no es más que un proceso de encapsulamiento donde se transfieren datos de un punto a otro de manera segura.

Una red privada virtual es un esquema económico y flexible de comunicación que proporciona las características y los beneficios propios de una red privada, sin la necesidad de invertir en la infraestructura que esta requiere.

Sin embargo, a pesar de que las redes privadas brindan seguridad y control, solo se encuentran al alcance de aquellas empresas que cuentan con los recursos humanos y el presupuesto suficiente para diseñarlas, implementarlas y mantenerlas, por lo que utilizar este tipo de redes puede desviar sus prioridades estratégicas de negocios hacia otras actividades secundarias. En contraste, con una red privada virtual (Virtual Private Network; VPN) usted no necesita realizar ninguna inversión en infraestructura adicional, puesto que es fácil de diseñar, implementar y actualizar.

Implementar 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. Tampoco es necesario que el cliente adquiera conmutadores para sus localidades, puesto que la inteligencia de la red proporciona la funcionalidad requerida.

Aunque originalmente una red privada virtual estaba diseñada para satisfacer las necesidades de un grupo cerrado de usuarios, y optimizada para administrar su tráfico, ahora se utiliza para comunicarse a cualquier destino, siempre y cuando uno de los extremos de la comunicación este conectado a ella. Esto quiere decir que sirve, por ejemplo, tanto para las llamadas “on-net” (entre puntos conectados a la red por línea física) como para llamadas “off-net” (realizadas a números de la red pública). Las primeras pertenecen a un plan de marcación privado, mientras que las segundas corresponden a números de la red pública. Una red privada virtual se entender de tres formas:

- **Por Intranet:** Es una red privada virtual que se crea entre una oficina central de una empresa y una oficina remota, o entre oficinas centrales y oficinas independientes. El ingreso a la Intranet se realiza desde fuera de la red, por lo que el acceso viene del exterior.

- **Por Acceso Remoto:** Es una red privada virtual que se crea entre oficinas centrales y los usuarios móviles remotos. Una persona con un software de cifrado cargado en su PC, establecerá un “tunneling” de cifrado al dispositivo de la red privada virtual en las oficinas centrales.

- **Por Extranet:** Es la red que se crea entre la empresa y sus clientes o proveedores. La Extranet permitirá el acceso con el protocolo http normal utilizado por los navegadores web actuales, o permitirá que se realice la conexión utilizando otro servicio y protocolos acordados por las partes involucradas, es aquí donde el comercio electrónico tiene su mayor impacto.

2.2 Componentes de una red privada virtual

Las redes privadas virtuales se componen de hardware y software y además requiere de otros tipos de componentes. Estos componentes garantizan que la red privada virtual sea segura.

La disponibilidad se aplica tanto al tiempo de actualización como al de acceso. El control se aplica a la administración de la red, servicios que puede ser de gran ayuda para una empresa debido a la capacitación, experiencia, supervisión y funciones de alerta que ofrecen algunos proveedores de servicios administrados.

La compatibilidad es una componente que esta sujeta a lo compatible que debe ser la arquitectura del protocolo de la red de una empresa con el IP nativo de Internet, y que por ende debe ser capaz de interpretar los protocolos de red de la empresa al nivel tres del modelo ISO.

Una componente principal para una red privada virtual es la seguridad ya que abarca todo el proceso de cifrado de datos hasta las firmas digitales y que también permita la implementación de software de algoritmos de cifrado en el dispositivo de la red privada virtual.

La confiabilidad trata de la no frustración al momento en que la red no tenga problemas o se caiga y si eso ocurre aplicar los servicios administrativos para la supervisión de la red.

2.3 Estructura de las RPV

Una RED PRIVADA VIRTUAL (RPV) es un sistema para simular una red privada sobre una red pública, por ejemplo, Internet. Como se muestra en la figura 1, la idea es que la red pública sea “vista” desde dentro de la red privada como un cable lógico que une las dos o más redes que pertenecen a la red privada.

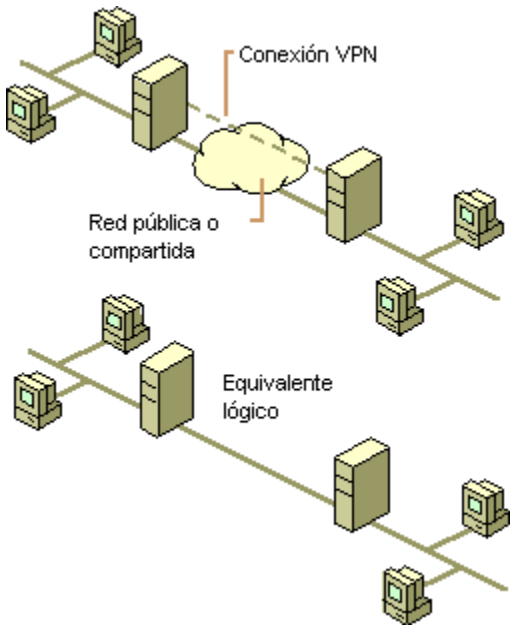

Figura 1. Estructura de una RPV.

Las RPVs también permiten la conexión de usuarios móviles a la red privada, tal como si estuvieran en una LAN dentro de una oficina de la empresa donde se implementa la RPV. Esto resulta muy conveniente para personal que no tiene lugar fijo de trabajo dentro de la empresa, como podrían ser vendedores, ejecutivos que viajan, personal que realiza trabajo desde el hogar, etc.

La forma de comunicación entre las partes de la red privada a través de la red pública se hace estableciendo sistemas de “tunneling” virtuales entre dos puntos para los cuales se definen esquemas de encriptación y autentificación que aseguran la confidencialidad e integridad de los datos transmitidos utilizando la red pública. Como se usan redes públicas, en general Internet, es necesario prestar la

debida atención a las cuestiones de seguridad, que se aborda a través de estos esquemas de encriptación y autentificación y que se describirán luego.

La tecnología de “Tunneling” es un modo de transferir datos en la que se encapsula un tipo de paquetes de datos dentro del paquete de datos de algún protocolo, no necesariamente diferente al del paquete original. Al llegar al destino, el paquete original es desempaquetado volviendo así a su estado original. En el traslado a través de Internet, los paquetes viajan encriptados.

Las técnicas de autenticación son esenciales en las RPVs, ya que aseguran a los participantes de la misma que están intercambiando información con el usuario o dispositivo correcto. La autenticación en RPV es conceptualmente parecido al "logging" en un sistema como nombre de usuario y contraseña, pero con necesidades mayores de aseguramiento de validación de identidades. La mayoría de los sistemas de autenticación usados en RPVs están basados en un sistema de claves compartidas.

La autenticación se lleva a cabo generalmente al inicio de una sesión, y luego aleatoriamente durante el curso de la misma, para asegurar que no haya algún tercer participante que se haya intrometido en la conversación. La autenticación también puede ser usada para asegurar la integridad de los datos. Los datos son procesados con un algoritmo de “hashing” para derivar un valor incluido en el mensaje como “checksum”. Cualquier desviación en el “checksum” indica que los

datos sufrieron alteración en la transmisión o fueron interceptados y/o modificados en el camino. Ejemplos de sistemas de autenticación son “Challenge Handshake Authentication Protocol” “(CHAP)” y “RSA”.

Todas las RPVs tienen algún tipo de tecnología de encriptación, que esencialmente empaqueta los datos en un paquete seguro. La encriptación es considerada tan esencial como la autenticación, ya que protege los datos transportados para evitar que sean vistos y entendidos en el viaje de un extremo a otro de la conexión. Existen dos tipos de técnicas de encriptación que se usan en las RPVs: encriptación de clave secreta, o privada; y encriptación de clave pública.

En la encriptación de clave secreta, se utiliza una contraseña secreta conocida por todos los participantes que necesitan acceso a la información encriptada. Dicha contraseña se utiliza tanto para encriptar como para desencriptar la información. Este tipo de encriptación posee el problema que, como la contraseña es compartida por todos los participantes y debe mantenerse secreta, al ser revelada, debe ser cambiada y distribuida a los participantes, con lo cual se puede crear de esta manera algún problema de seguridad.

La encriptación de clave pública o criptografía asimétrica implica la utilización de dos claves, una pública y una secreta. La primera es enviada a los demás participantes. Al encriptar, se usa la clave privada propia y la clave pública del otro participante de la conversación. Al recibir la información, ésta es desencriptada

usando su propia clave privada y la pública del generador de la información. La gran desventaja de este tipo de encriptación es que resulta ser más lenta que la de clave secreta.

En las RPVs, la encriptación debe ser realizada en tiempo real. Por eso, los flujos encriptados a través de una red encriptan utilizando encriptación de clave secreta con claves que son solamente buenas para sesiones de flujo.

El protocolo más usado para la encriptación dentro de las RPVs es IPSec, que consiste en un conjunto de normas que delinean un protocolo IP seguro para IPv4 y IPv6. IPSec provee encriptación a nivel de IP.

El método “tunneling” permite encapsular paquetes dentro de paquetes para acomodar protocolos incompatibles. Dentro de los protocolos que se usan para la metodología de “tunneling” se encuentran; Point-to-Point Tunneling Protocol (PPTP), Layer-2 Fowarding Protocol (L2FP) y el modo “tunneling” de IPSec.

2.4 Protocolos utilizados en las RPVs

2.4.1 PPTP

Point-to-Point Tunneling Protocol fue desarrollado por los ingenieros de Ascend Communications, U.S. Robotics, 3Com Corporation, Microsoft, y ECI Telematics

para proveer entre usuarios de acceso remoto y servidores de red una red privada virtual.

De manera similar al protocolo de “tunneling”, el PPTP encapsula datagramas de cualquier protocolo de red en datagramas IP, que luego son tratados como cualquier otro paquete IP. La gran ventaja de este protocolo es que cualquier protocolo puede ser enrutado a través de una red IP, como Internet.

El PPTP fue diseñado para permitir a los usuarios conectarse a un servidor RAS desde cualquier punto en Internet para tener la misma autenticación, encriptación y los mismos accesos de LAN como si marcaran directamente al servidor. En vez de marcar a un MODEM conectado al servidor RAS, los usuarios se conectan a su proveedor y luego “llaman” al servidor RAS a través de Internet utilizando PPTP. Existen dos escenarios comunes para este tipo de RPV:

- el usuario remoto se conecta a un ISP que provee el servicio de PPTP hacia el servidor RAS.
- el usuario remoto se conecta a un ISP que no provee el servicio de PPTP hacia el servidor RAS y, por lo tanto, debe iniciar la conexión PPTP desde su propia máquina cliente.

Para el primero de los escenarios, el usuario remoto establece una conexión PPP con el ISP, que luego establece la conexión PPTP con el servidor RAS. Para el

segundo escenario, el usuario remoto se conecta al ISP mediante PPP y luego “llama” al servidor RAS mediante PPTP.

Luego de establecida la conexión PPTP, para cualquiera de los dos casos, el usuario remoto tendrá acceso a la red corporativa como si estuviera conectado directamente a la misma.

El PPTP se basa en el protocolo “Generic Routing Encapsulation” (GRE), que puede ser usado para realizar “tunneling” para protocolos a través de Internet. La versión PPTP, denominada GREv2, añade extensiones para velocidad de conexión.

El paquete PPTP está compuesto por un encabezado de envío, un encabezado IP, un encabezado GREv2 y el paquete de carga. El encabezado de envío es el protocolo de marcado para cualquiera de los medios a través de los cuales el paquete viaja, ya sea Ethernet, frame relay, PPP. El encabezado IP contiene información relativa al paquete IP, como ser, direcciones de origen y destino, longitud del datagrama enviado, etc. El encabezado GREv2 contiene información sobre el tipo de paquete encapsulado y datos específicos de PPTP concernientes a la conexión entre el cliente y servidor. Por último, el paquete de carga es el paquete encapsulado, que, en el caso de PPP, el datagrama es el original de la sesión PPP que viaja del cliente al servidor y que puede ser un paquete IP, IPX, NetBEUI, entre otros. La figura 2 ilustra las capas del “tunneling” PPTP.

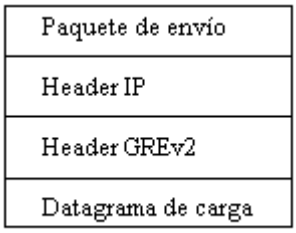

Figura 2. Capas de tunneling PPTP.

Para la encriptación, PPTP utiliza el sistema RC4 de RSA, con una clave de sesión de 40 bits.

2.4.2 IPSec

IPSec trata de remediar algunas falencias de IP, tales como protección de los datos transferidos y garantía de que el emisor del paquete sea el que dice el paquete IP. Si bien estos servicios son distintos, IPSec da soporte a ambos de una manera uniforme.

IPSec provee confidencialidad, integridad, autenticidad y protección a repeticiones mediante dos protocolos, que son “Authentication Protocol” (AH) y “Encapsulated Security Payload” (ESP).

Por confidencialidad se entiende que los datos transferidos sean sólo entendidos por los participantes de la sesión.

Por integridad se entiende que los datos no sean modificados en el trayecto de la comunicación.

Por autenticidad se entiende que los datos deben ser validados.

Por protección a repeticiones se entiende que una sesión no pueda ser grabada y repetida salvo que se tenga autorización para hacerlo.

AH provee autenticación, integridad y protección a repeticiones pero no así confidencialidad. La diferencia más importante con ESP es que AH protege partes del encabezado IP, como las direcciones de origen y destino. ESP provee autenticación, integridad, protección a repeticiones y confidencialidad de los datos, protegiendo el paquete entero que sigue al encabezado.

AH sigue al encabezado IP y contiene diseminaciones criptográficas tanto en los datos como en la información de identificación. Las diseminaciones pueden también cubrir las partes invariantes del encabezado IP. El encabezado de ESP permite rescribir la carga en una forma encriptada. Como no considera los campos del encabezado IP, no garantiza nada sobre el mismo, sólo la carga.

La división de la funcionalidad de IPSec se aplica dependiendo de dónde se realiza la encapsulación de los datos, si es la fuente original o un gateway.

El modo de transporte es utilizado por el host que genera los paquetes. En este modo, los encabezados de seguridad son antepuestos a los de la capa de

transporte, antes de que el encabezado IP sea incorporado al paquete. En otras palabras, AH cubre el encabezado TCP y algunos campos IP, mientras que ESP cubre la encriptación del encabezado TCP y los datos, pero no incluye ningún campo del encabezado IP.

El “tunneling” es usado cuando el encabezado IP entre extremos está ya incluido en el paquete, y uno de los extremos de la conexión segura es un gateway. En este modo, tanto AH como ESP cubren el paquete entero, incluyendo el encabezado IP entre los extremos, agregando al paquete un encabezado IP que cubre solamente el salto al otro extremo de la conexión segura, que, por supuesto, puede estar a varios saltos del gateway.

Los enlaces seguros de IPSec son definidos en función de Security Associations (SA). Cada SA está definido para un flujo unidireccional de datos y generalmente de un punto único a otro, cubriendo tráfico distinguible por un selector único. Todo el tráfico que fluye a través de un SA es tratado de la misma manera. Partes del tráfico puede estar sujeto a varios SA, cada uno de los cuales aplica cierta transformación. Grupos de SA son denominados SA “Bundles”. Paquetes entrantes pueden ser asignados a un SA específico por los tres campos definitorios: la dirección IP de destino, el índice del parámetro de seguridad y el protocolo de seguridad. El SPI puede ser considerado una “cookie” que es repartido por el receptor del SA cuando los parámetros de la conexión son negociados. El protocolo de seguridad debe ser AH o ESP. Como la dirección IP

de destino es parte de la tripleta antes mencionada, se garantiza que este valor sea único. La figura 3 muestra un paquete AH en modo “tunneling” es:

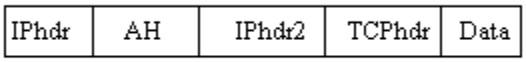

Figura 3. Paquete AH en modo tunneling Un ejemplo en la figura 4 de paquete

AH en modo transporte es:

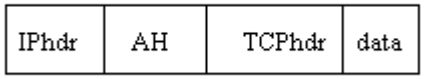

Figura 4. Combinación de encabezado AH y ESP en modo transporte.

Como ESP no puede autentificar el encabezado IP más exterior, es muy útil combinar un encabezado AH y ESP para obtener lo siguiente de la figura 5:

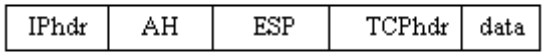

Figura 5. Combinación de encabezado AH y ESP.

Este tipo de paquete se denomina “Transport Adjacency”, como lo muestra la figura 6:

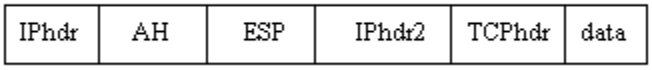

Figura 6. Encabezado AH y ESP en versión de tunneling.

El “Transport Adjacency” autenticaría el paquete completo salvo algunos pocos campos del encabezado IP y también encriptaría la carga. Cuando un encabezado AH y ESP se aplica directamente como en la forma indicada, el orden de los encabezados debe ser el mostrado. Es posible, en el modo de “tunneling” , hacer una encapsulación arbitrariamente recursiva para que el orden no sea el especificado.

2.4.3 L2TP

Layer-2 Tunneling Protocol (L2TP) crea el “tunneling” de paquetes PPP a través de una red de manera tal que sea lo más transparente posible a los usuarios de ambos extremos del “tunneling” y para las aplicaciones que éstos corran. El esquema típico del L2TP, cuyo objetivo es la creación de marcos PPP en “tunneling” entre el sistema remoto o cliente LAC y un LNS ubicado en una LAN local, es el que se muestra en la figura 7:

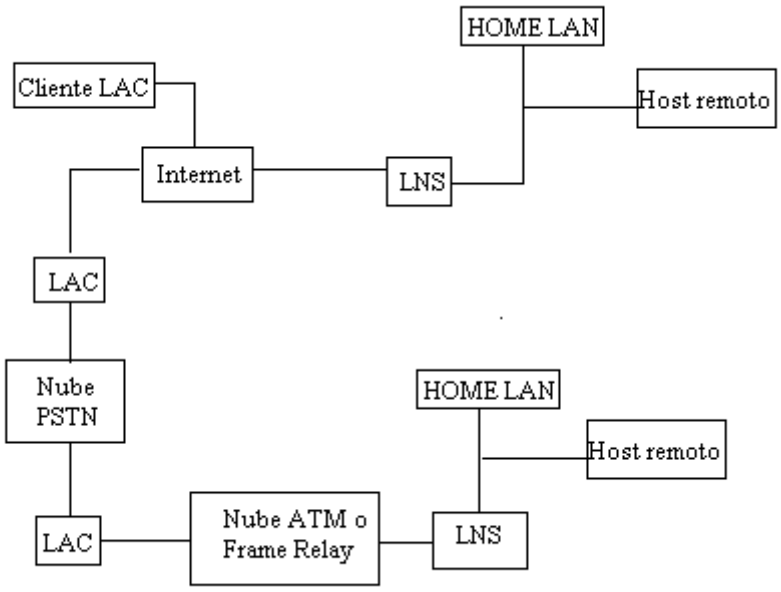

Figura 7. Creación de marcos PPP en tunneling.

Un L2TP Access Concentrator (LAC) es un nodo que actúa como un extremo de un “tunneling” L2TP y es el par de un LNS. Un LAC se sitúa entre un LNS y un sistema remoto y manda paquetes entre ambos. Los paquetes entre el LAC y el LNS son enviados a través del “tunneling” L2TP y los paquetes entre el LAC y el sistema remoto es local o es una conexión PPP.

Un L2TP Network Server (LNS) actúa como el otro extremo de la conexión L2TP y es el otro par del LAC. El LNS es la terminación lógica de una sesión PPP que está siendo puesta desde el sistema remoto por el LAC. Un cliente LAC, es una máquina que corre nativamente L2TP, puede participar también en el “tunneling”, sin usar un LAC separado. En este caso, estará conectado directamente a

Internet. El direccionamiento, la autenticación, la autorización y el servicio de cuentas son proveídos por el Home LAN's Management Domain. L2TP utiliza dos tipos de mensajes: de control y de datos. Los mensajes de control son usados para el establecimiento, el mantenimiento y el borrado de los sistemas de "tunneling" y las llamadas. Utilizan un canal de control confiable dentro de L2TP para garantizar el envío. Los mensajes de datos encapsulan los marcos PPP y son enviados a través del "tunneling". La figura 8 muestra la relación entre los marcos PPP y los mensajes de control a través de los canales de control y datos de L2TP.

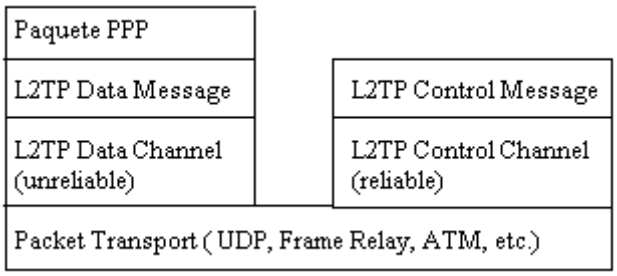

Figura 8. Relación entre marcos PPP y mensajes de control.

Los marcos PPP son enviados a través de un canal de datos no confiable, encapsulados primero por un encabezado L2TP y luego por un transporte de paquetes como UDP, Frame Relay o ATM. Los mensajes de control son enviados a través de un canal de control L2TP confiable que transmite los paquetes sobre el mismo transporte de paquete. Se requiere que existan números de secuencia en los paquetes de control, que son usados para proveer el envío confiable en el canal de control. Los mensajes de datos pueden usar los números de secuencia

para reordenar paquetes y detectar paquetes perdidos. Al correr sobre UDP/IP, L2TP utiliza el puerto 1701. El paquete entero de L2TP, incluyendo la parte de datos y el encabezado, viaja en un datagrama UDP. El que inicia un "tunneling" L2TP toma un puerto UDP de origen que esté disponible, pudiendo ser o no el 1701 y envía a la dirección de destino sobre el puerto 1701. Este extremo toma un puerto libre, que puede ser o no el 1701, y envía la respuesta a la dirección de origen, sobre el mismo puerto iniciador. Luego de establecida la conexión, los puertos quedan estáticos por el resto de la vida del "tunneling".

Sobre la seguridad del paquete L2TP, se requiere que el protocolo de transporte de L2TP tenga la posibilidad de brindar servicios de encriptación, autenticación e integridad para el paquete L2TP en su totalidad. Como tal, L2TP sólo se preocupa por la confidencialidad, autenticidad e integridad de los paquetes L2TP entre los puntos extremos del "tunneling", no entre los extremos físicos de la conexión.

2.5 Arquitectura de una Red Privada Virtual

Existen innumerables opciones para la instalación de las RPVs, Steven Brown[1], clasifica desde las RPVs independientes basadas en caja negra y las RPVs basadas en enrutador hasta las RPVs basadas en software y en firewalls. Además de estas arquitecturas existe una amplia variedad de servicios y características

[1] BROWN, Steven. Implementación redes

que pueden implementarse en estos dispositivos. Es importante tener en cuenta, que se deben separar los servicios RPV de otros servicios de aplicaciones, como por ejemplo, cuando se está utilizando un firewall basado en sistema operativo y decide instalar un producto RPV sobre el sistema operativo.

Después, adicionalmente encima de esto se agrega software de antivirus de algún proveedor y así sucesivamente. A continuación se nombran los tipos de arquitectura:

- RPV proporcionada por un proveedor de servicios red. Es una de las maneras más eficientes de conectar una organización a Internet y disfrutar de los beneficios de una RPV. El proveedor de servicios de red tal vez establecerá un dispositivo en las oficinas de una compañía y creará “tunneling” de RPV. También en algunos casos se puede instalar un conmutador PPTP frontal, la cual creará un “tunneling” de RPV para su respectivo tráfico, también se podría agregar un firewall justo en frente de un dispositivo de red o entre ellos.

- RPV basadas en Firewalls. Estas RPV basadas son la forma más común de implementación de RPV hoy en día, y muchos proveedores ofrecen este tipo de configuración. Si decide que una solución de firewall/RPV es el camino correcto a seguir, sería conveniente observar algunas encuestas

---

privadas virtuales. México.1999. p 93

recientes sobre los productos de cortafuegos, de esta manera podría hacer comparaciones con distintos firewalls. Esta RPV basada en firewall no es más que añadir tecnología RPV únicamente a un firewall de inspección de estados.

- RPV basadas en caja negra. La caja negra se trata de un dispositivo cargado con software de cifrado para crear un “tunneling” de RPV. Algunas cajas negras vienen con software que se ejecuta en un equipo cliente para ayudar a administrar el dispositivo, y otras pueden configurarse a través de un explorador web. Una característica muy importante sobre este tipo de RPV es que en algunos de ellos se le permite utilizar una base de datos existente. Usted configura el equipo para usar autenticación y luego lo dirige al servidor de administrador que instaló. Después configura el servidor de administración para utilizar la base de datos de usuarios existente.

- RPV basadas en enrutador. Estas RPVs son adecuadas para una organización que ha hecho una gran inversión en enrutadores y cuyo personal de sistemas tiene experiencia en ellos. Existen dos tipos de RPVs basadas en enrutadores. En el primer tipo se añade el software al enrutador para permitir que el proceso de cifrado ocurra y en el otro tipo se inserta una tarjeta externa de otro proveedor en el mismo chasis que el enrutador. Los proveedores de estas RPVs pueden proporcionarle una lista de

estadísticas de desempeño que podría mostrarle que la carga de cifrado de su producto es mínima.

- RPVs basadas en acceso remoto. El acceso remoto significa que alguien de fuera está tratando de crear un flujo de paquetes cifrados hacia su organización. Un servidor de acceso instalado en su red, ya sea un enrutador, un firewall, una caja negra o un servidor de autenticación independiente concede el acceso. Este dispositivo de acceso remoto reduce la cantidad de los costosos equipos de líneas rentadas y acceso por marcación remota.

- RPVs basadas en software. Las RPVs basadas en software son básicamente un programa para establecer "tunneling" o cifrado a otro anfitrión. Por lo general se utiliza desde un cliente a un servidor. El tráfico inicia desde un anfitrión específico en su organización y establece una conexión. Después que sale del anfitrión se cifra o se encapsula, dependiendo de la RPV instalada, y se enruta a su destino.

2.6 Seguridad para redes privadas virtuales

La seguridad de una red privada virtual requiere protocolos especiales tales como PPTP, IP Móvil o L2TP, debido a que los sistemas de "tunneling" permiten al servidor realizar todas las comprobaciones de seguridad y la encriptación de

datos. Los estándares emergentes como IPSEC e IP versión 6 brindan seguridad, encapsulación encriptada y “tunneling” para los datos del usuario, puesto que éste se ha vuelto extremadamente más sensitivo sobre la privacidad de sus datos sobre redes públicas.

La empresa que pretenda implementar este tipo de solución para sus requerimientos de comunicación, debe considerar diferentes puntos antes de decidir si una red privada virtual responde como la mejor opción para satisfacer sus necesidades:

- Necesidades de comunicación por departamento, empleado, oficina y localidad.
- Necesidad de ahorro en los costos de llamadas de larga distancia.
- Crecimiento a corto plazo del negocio, y requerimientos de respuestas rápidas.
- Potencial de abuso en llamadas por los empleados o visitantes.
- Necesidad de instrumentos Para restringir el servicio de larga distancia y protegerse contra el abuso del mismo.
- Empleados que viajan.

- Distribución de costos o facturación por departamentos, proyectos o clientes.
- Necesidad de una facturación clara y oportuna y herramientas para el análisis de la facturación.
- Necesidad de instrumentar un plan de marcación privado de acuerdo a sus propias necesidades de regionalización y distribución de los números telefónicos que conformen un directorio propio.

La seguridad de redes debería ser considerada como una parte general de una organización. La seguridad de la información abarca la seguridad de las redes, la seguridad de las computadoras, la seguridad de acceso y seguridad física, entre otras.

2.7 Identificación de ataques

Toda política de seguridad tiene auditorias y registros como pasos principales de sus procesos. Ninguna organización sabe cuando es atacada; si lo supiera, lo podría impedir. Lo que normalmente sucede es que reciben varios avisos que alguien se ha introducido; si esto sucede, es necesario rastrear la intrusión y ver si los archivos de registros pueden identificar de donde vino el intruso, cuál es su IP y quién es su proveedor de servicios, si es posible. Otra forma de identificar un

ataque es a través de monitoreo que no es más que una vista de los paquetes que pasan el limite de la red interna y una infraestructura pública de la empresa.

Aunque no siempre se considera como procedimiento de seguridad, el cifrado de disco duro podría abrir un nuevo conjunto de requisitos para su organización por dos motivos potenciales. Uno es la recuperación de claves, la forma como se manejan las claves tanto públicas como privadas y la forma de utilizar las tecnologías de cifrado en el disco duro o en directorios seleccionados de esa unidad para protegerse de si mismo.

Es importante tener en cuenta algunos requisitos para la seguridad en una red privada virtual. Estos incluyen cifrado, dispositivos RPV, autenticación, cifrado punto a punto, el proceso sin rechazo, administración centralizada de la seguridad y los procedimientos de respaldo/restauración. El cifrado no es más que el proceso de convertir algún texto legible en un texto ilegible. La idea es permitir que solo la persona a la que se le envía lo convierta en un texto legible. Los dispositivos de las RPVs se implementan en firewalls o cortafuegos que se extienden de los límites de la organización hacia el Internet. Además las RPVs se pueden implementar en plataformas de sistemas operativos como UNIX y Windows NT, cajas negras y enrutadores. Las plataformas de los sistemas operativos tienen agujeros que significa debilidad de un sistema operacional.

En cualquier organización es importante tener servidores y aplicaciones protegidos con contraseña. Los usuarios pueden tener varias contraseñas distintas para los diferentes servidores y se recomienda no escribirlas ni decírselas a nadie. Los sistemas de “tunneling” cifrados de RPV aseguran los datos conforme pasan a través de una red pública. Por lo general se utilizan términos con la tecnología RPV: cifrado y “tunneling”. La principal diferencia es que el cifrado solo codifica los datos, mientras que el “tunneling” hace un paquete de datos del paquete original, lo envuelve en su propio paquete y después codifica todo el paquete.

2.8 Criptografía

Pino Caballero Gil[2] define la criptografía como la técnica de convertir un texto explícito, texto en claro (*plaintext*), en otro, llamado criptograma (*ciphertext*), cuyo contenido de información es igual al anterior pero sólo lo pueden entender las personas autorizadas. El criptoanálisis es la técnica de descifrar un criptograma sin tener la autorización. Para encriptar se debe transformar un texto mediante un método cuya función inversa únicamente conocen las personas autorizadas. Así se puede utilizar un algoritmo secreto o un algoritmo público que utiliza una palabra, llamada clave, sólo conocida por las personas autorizadas, esta clave

[2] CABALLERO GIL, Pino.Introducción
a la Criptografía. México D.F. p. 25. 2002

debe ser imprescindible para la encriptación y desencriptación (Figura 9 y Figura 10).

Figura 9. Encriptación Secreta

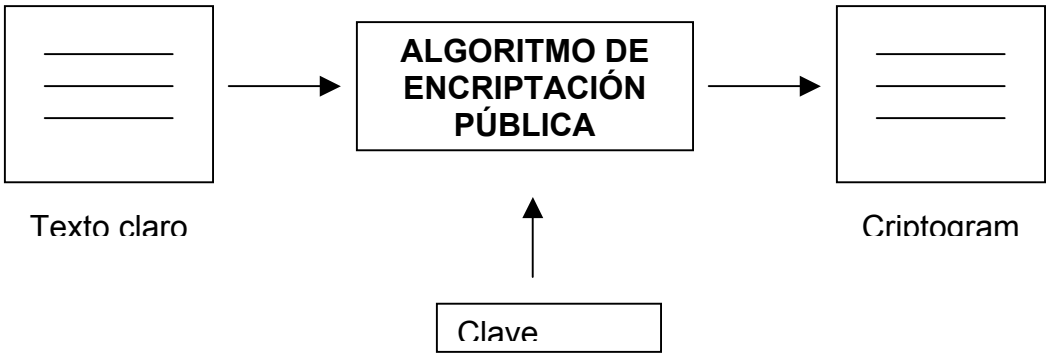

Figura 10. Encriptación Pública

Los sistemas actuales utilizan algoritmo público y claves secretas, debido a los siguientes motivos:

- El nivel de seguridad es el mismo.

- Los algoritmos públicos se pueden fabricar en cadena, tanto chips de *hardware* como aplicaciones *software*. De está manera el desarrollo es más barato.

- Los algoritmos públicos están más probados, ya que toda la comunidad científica puede trabajar sobre ellos buscando fallos o agujeros. Un algoritmo secreto puede tener agujeros detectables sin necesidad de conocer su funcionamiento completo, por lo tanto, un criptoanalista puede encontrar fallos aunque no conozca el secreto del algoritmo.

Es más fácil y más seguro transmitir una clave que todo el funcionamiento de un algoritmo.

Para poder entender un poco de la criptografía, es tiempo de plantear que tipo de problemas resuelve ésta. Los principales problemas de seguridad que resuelve la criptografía son: la privacidad, la integridad, la autenticación y el no rechazo. La privacidad se refiere a que la información sólo pueda ser leída por personas autorizadas.

Ejemplos: en la comunicación por teléfono, que alguien intercepte la comunicación y escucha la conversación quiere decir que no existe privacidad. Si mandamos una carta y por alguna razón alguien rompe el sobre para leer la carta, ha violado la privacidad.

En la comunicación por Internet es muy difícil estar seguros que la comunicación es privada, ya que no se tiene control de la línea de comunicación. Por lo tanto al cifrar (esconder) la información cualquier intercepción no autorizada no podrá entender la información. Esto es posible si se usan técnicas criptográficas, en particular la privacidad se logra si se cifra el mensaje con un método simétrico.

La integridad se refiere a que la información no pueda ser alterada en el transcurso de ser enviada.

Ejemplos: cuando compramos un boleto de avión y están cambiados los datos del vuelo, puede afectar los planes del viajero. Una vez hecho un deposito en el banco, si no es capturada la cantidad correcta causará problemas. La integridad es muy importante en las transmisiones militares ya que un cambio de información puede causar graves problemas.

En Internet las compras se pueden hacer desde dos ciudades muy distantes. La información tiene necesariamente que viajar por una línea de transmisión de la cual no se tiene control, si no existe integridad podrían cambiarse. Por ejemplo el número de una tarjeta de crédito, los datos del pedido, en fin, información que causaría problemas a cualquier comercio y cliente.

La autenticidad se refiere a que se pueda confirmar que el mensaje recibido haya sido enviado por quien dice lo envió o que el mensaje recibido es el que se esperaba.

Ejemplo: cuando se quiere cobrar un cheque a nombre de alguien, quien lo cobra debe someterse a un proceso de verificación de identidad para comprobar que en efecto es la persona quien dice ser, esto en general se lleva a cabo con una credencial que anteriormente fue certificada y acredita la identidad de la persona que la porta. La verificación se lleva a cabo comparando la persona con una foto o con la comparación de una firma convencional. Por Internet es muy fácil engañar a una persona con quien se tiene comunicación respecto a la identidad. Resolver este problema es por lo tanto muy importante para efectuar comunicación confiable. Las técnicas necesarias para poder verificar la autenticidad tanto de personas como de mensajes usan quizá la más conocida aplicación de la criptografía asimétrica que es la firma digital, de algún modo ésta reemplaza a la firma autógrafa que se usa comúnmente. Para autenticar mensajes se usa criptografía simétrica.

El no rechazo, se refiere a que no se pueda negar la autoría de un mensaje enviado. Cuando se diseña un sistema de seguridad, una gran cantidad de problemas pueden ser evitados, si se puede comprobar autenticidad, garantizar privacidad, asegurar integridad y evitar el no-rechazo.

2.8.1 Criptografía Simétrica

Los algoritmos de encriptamiento convencional, también llamados cifradores simétricos, cifradores tradicionales o cifradores de una sola clave, se vienen usando desde hace siglos atrás; razón por la cual encontramos algunos clásicos y otros modernos. Dentro de los algoritmos clásicos, muy vulnerables hoy en día, se encuentra el cifrador Julio Cesar, el cifrador monoalfabético, el cifrador Vigenére, entre otros. Dentro de los algoritmos modernos de encriptamiento convencional, se pueden mencionar el DES, IDEA, CAST, RC2, RC5. En este capítulo se describen detalladamente los procesos de ciframiento, procesos de desciframiento y un análisis criptoanalístico de algunos de estos algoritmos.

La clave de ciframiento debe ser la misma clave de desciframiento. En el peor de los casos debe haber una dependencia directa entre estas, de tal manera que sea computacionalmente fácil calcular una a partir de la otra.

El algoritmo de ciframiento es el mismo algoritmo de desciframiento o en el peor de los casos el uno contiene procedimientos inversos del otro.

2.8.2 Criptografía Asimétrica

La criptografía clásica estaba basada en permutaciones y sustituciones y en la criptografía moderna se utilizan en mayor proporción funciones matemáticas. Para

los esquemas convencionales de encriptamiento las claves usadas por los algoritmos de encriptamiento y desencriptamiento son las mismas, aunque esto no es una condición necesaria; ya que es posible desarrollar un algoritmo criptográfico que permita usar una clave para la encriptamiento y otra para la desencriptamiento, los cuales son llamados criptosistemas de clave pública.

La característica más importante de los criptosistemas de clave pública es que computacionalmente no es factible determinar la clave de desencriptamiento cuando se conoce únicamente el algoritmo de encriptamiento y la clave de encriptamiento. En particular, el sistema más popular de clave pública que se verá detalladamente más adelante y conocido como el RSA, tiene la ventaja de que ambas claves pueden ser usadas indistintamente en el algoritmo de encriptamiento con la otra clave en el algoritmo de desencriptamiento.

Los Criptosistemas de clave pública tienen 3 aplicaciones importantes:

- Encriptamiento/Desencriptamiento: El transmisor encripta el mensaje con un recipiente de claves públicas.

- Firma digital: El transmisor envía un mensaje con su clave privada. La firma es generalmente un pequeño bloque de datos del mensaje.

- Intercambio de claves: Los dos lados cooperan para intercambiar una sesión de claves. Muchos enfoques diferentes son posibles, involucrando las claves privadas de una de ambas partes.

2.8.3 Sistema RSA

RSA es un criptosistema de clave pública usado para los servicios de autenticación y privacidad, el cual fue inventado por Ron Rivest, Adi Shamir y Leonard Adleman. RSA trabaja de la siguiente manera: Se toman dos números primos grandes ***p*** y **q**, y se calcula su producto ***n=p.q****,* ***n*** se llama el módulo; se debe encontrar un número ***e*** menor que ***n*** y primo relativo con ***(p-1)(q-1)*** y encontrar su inverso ***d*** módulo ***(p-1)(q-1****),* de tal forma que *de* ***1 mod (p-1)(q-1***); ***e*** y ***d*** son llamados los exponentes público y privado respectivamente. La clave pública es el par ***(e, n)*** y la clave privada el par ***(d, n***). El factor ***pq*** debe ser secreto o sino el algoritmo es destruido.

El sistema RSA se realiza en los siguientes siete pasos, en el cual cada usuario calcula sus claves privadas y públicas:

1. Seleccionar al azar dos números primos grandes (Mayores de 100 dígitos) ***p*** **y** ***q.***

2. Calcular ***n=p.q***

3. Seleccionar un número entero e menor que n y primo relativo con *f* ***f(n)= (p-1)(q-1)***

4. Calcular d, tal que ***d 1 mod*** *f* ***f(n)***

5. Publicar ***P (e, n)*** como clave pública y guardar ***S (d, n)*** como clave privada.

2.8.4 Firmas Digitales

Las dos principales técnicas usadas para los mecanismos de autenticación y firmas digitales son las sumas de chequeo y las funciones “Hash”, tanto en el esquema de criptografía convencional como en el de clave pública.

Inicialmente se discutirán los requerimientos del servicio de autenticación a partir de diversas formas de ataques que se pueden presentar en este servicio. Más adelante se muestran diversas maneras y procedimientos criptográficos usando sumas de chequeo, funciones “Hash” y analizando para cada caso como se garantizan los requerimientos del Servicio de Autenticación. De igual forma, se estudian las firmas digitales, indicando los requerimientos de estas y analizando dos enfoques muy utilizados: Firma digital directa y firma digital a través de un árbitro. Es importante decir que existen unos protocolos de autenticación basados en sumas de chequeo y funciones Hash, los cuales son usados en servicios de autenticación mutua y autenticación de una sola vía.

La autenticación de mensajes protege a dos partes que intercambian mensajes de una tercera parte, sin embargo este esquema no protege las dos partes entre sí ya que existen diversas formas mediante las cuales pueden haber disputas entre las dos partes intercambiables de mensajes.

2.8.4.1 Propiedades y requerimientos de una firma digital

Una firma digital debe tener las siguientes propiedades:

1. Debe ser posible verificar autor, fecha y hora de la firma.

2. Debe ser posible autenticar el contenido a la hora de la firma.

3. Las firmas deben ser verificables por terceras partes para resolver disputas.

Así la función de firma digital incluye la función de autenticación y sus requerimientos son los siguientes:

1. La firma debe contener un bloque de bits que dependa del mensaje que está siendo firmado.

2. La firma debe usar información única del emisor para prevenir que se niegue o altere el mensaje.

3. Debe ser relativamente fácil producir la firma digital.

4. Debe ser relativamente fácil reconocer y verificar la firma digital.

5. Debe ser computacionalmente difícil construir una firma digital para un nuevo mensaje y una firma digital existente o construir una firma digital fraudulenta para un mensaje dado.

6. Debe ser práctico retener una copia de la firma digital.

2.8.5 Descripción general de PGP (Pretty Good Privacy)

Pretty Good Privacy (PGP) o "Privacidad bastante buena", es una aplicación informática de criptografía de alta seguridad que permite intercambiar ficheros y mensajes con privacidad, autenticación y firma digital. PGP está basado en cifrado convencional, cifrado de clave pública y función Hash.

2.8.5.1 Ventajas

El uso de PGP en el correo electrónico aporta **ventajas** significativas que no conviene desestimar:

1. Evita todos los inconvenientes que hemos reseñado previamente.

2. Hace valer el derecho constitucional a la Intimidad de nuestras comunicaciones, frente a los que pretendan -ahora o en el futuro- controlar Internet.

3. Contribuye a que el cifrado de mensajes se convierta en una práctica común en Internet.

2.9 Ventajas de las redes privadas virtuales

- Renta de enlaces a suministradores autorizados, por lo que la empresa se convierte en propietaria de la red, logrando operaria y administrarla con libertad: control total sobre la red.
- Ofrecen seguridad.
- Costos de uso prefijados y posibilidad de disponer de servicios de valor agregado.

2.10 Desventajas de las redes privadas virtuales

- Fuerte inversión en infraestructura (enlaces, equipo, recursos humanos, capacitación) para tender enlaces físicos entre las distintas localidades, para adquirir e instalar los conmutadores necesarios y para habilitar las localidades.
- Largos plazos de instalación de las líneas.
- Gastos de operación, administración y mantenimiento de la red.
- Costo adicional por ampliación de equipos centrales.
- Renta fija mensual por los enlaces dedicados aunque la red salo se ocupe parte del tiempo.

- Mantenimiento complejo.
- Poca flexibilidad.
- Interrupción de la comunicación cuando un enlace se satura o fractura, hasta que los técnicos reparen el desperfecto.

3. IMPLEMENTACION DE UNA RED PRIVADA VIRTUAL

Cuando se va a implementar una RPV en una empresa se debe conocer bien cuales son los requisitos, ya que no todas las configuraciones son iguales. La razón para elegir una configuración cortafuego o firewall/RPV es que ésta contiene todos los pasos necesarios para implementar la seguridad y una RPV. Si la empresa ya tiene un firewall y solo esta agregando un dispositivo RPV independiente, entonces puede ser tan sencillo como conectar y usar. También hay que tener en cuenta las bases para poder implementar una RPV. Es muy importante tener en cuenta los aspectos de direccionamiento, acceso remoto, DNS.

3.1 Direccionamiento

Steven Brown[3] explica que antes de implementar, se debe considerar algunos aspectos de direccionamiento IP. Para utilizar el dispositivo de firewall/RPV, antes se debe conseguir espacio para la dirección IP, esto se hace de dos maneras:

- Puede obtenerlo de InterNIC.
- Puede obtenerlo de un PSI (Proveedor de Servicios de Internet) local.

Cuando se obtiene el espacio para la dirección por parte de su PSI, quizá tenga que implementar servicios como SMTP, DNS y servidores WEB de acuerdo con el espacio que le asignaron para la dirección. Debe tener en cuenta que las tablas DNS reflejen estas nuevas direcciones. Tanto reconfigurar las tablas NAT como actualizar las tablas DNS es un paso importante para una implementación.

3.2 Acceso Remoto

En este caso se debe considerar la ubicación del servidor de autenticación y el tipo de usuario que va a autenticar. Por lo general se cuenta con tres opciones para establecer el servidor de autenticación: la DMZ, la red interna y la propia RPV.

Si instala el servidor en la DMZ, debe asegurarse que firewall/RPV puede comunicarse con el servidor de autenticación. Si por ejemplo, emplea un servidor RADIUS, asegúrese que el firewall/RPV puede comunicarse con ese servidor usando el protocolo RADIUS.

Si decide instalar el dispositivo de autenticación en la red interna, tiene que revisar la compatibilidad al igual que la sincronización. Algunos dispositivos RPV solo permiten una cantidad especifica de tiempo para registrarse. Si se demora la

---

[3] BROWN, Steven. Implementación redes privadas virtuales. México.1999. p 176

conexión termina, significa que cuando la respuesta regrese al servidor, el firewall terminará la conexión. Por consiguiente existen dos esquemas de autenticación que puede considerar:

- Los usuarios que salen a Internet.
- Los usuarios que llegan a la red interna.

Ambos utilizan un esquema de autenticación para lograr el acceso, a continuación se presentan algunos esquemas de autenticación:

- Autenticar todo acceso individual a Internet.
- Sin autenticación interna, pero registrando cada sitio que visitan.
- Autenticar y registrar cada sitio que visitan.
- Emplear una herramienta de filtración para la web.
- Autenticar a los usuarios que llegan al sitio.
- Autenticar y registrar a todos aquellos que lleguen al sitio.

3.3 SMPT/DNS

El servicio de dominios y el protocolo de transferencia de correo son aspectos muy importantes cuando se configuran los dispositivos de red.

Se pueden tener servidores internos por separado para manejar el tráfico de DNS y de correo separados en la zona DMZ. Si se deja el servidor en esta zona, sus servidores internos son los únicos responsables de estos servicios. Todo el tráfico de Internet debería ir a la zona DMZ. Solo se debería permitir que el tráfico tipo SMTP o DNS pasara del firewall al DMZ. En el firewall solo se permite que el tráfico pase ya sea a Internet o al servidor de DNS interno.

3.4 Instalación de una RPV

Una red privada virtual (Virtual Private Network) es una red privada que se extiende, mediante un proceso de encriptación de los paquetes a distintos puntos remotos mediante el uso de infraestructuras públicas de transporte. Las empresas deciden el tipo de configuraciones para sus RPVs dependiendo de los requisitos que están conllevan.

Después de que el modelo a instalar es aprobado por la administración, las oficinas centrales y sucursal tienen que contactar a sus PSI locales para obtener un espacio de dirección cuando se haya asignado la dirección IP, el personal

técnico asignará el espacio de dirección pública a los distintos dispositivos de todos los departamentos.

A continuación, la figura 11 se muestra una conexión RPV.

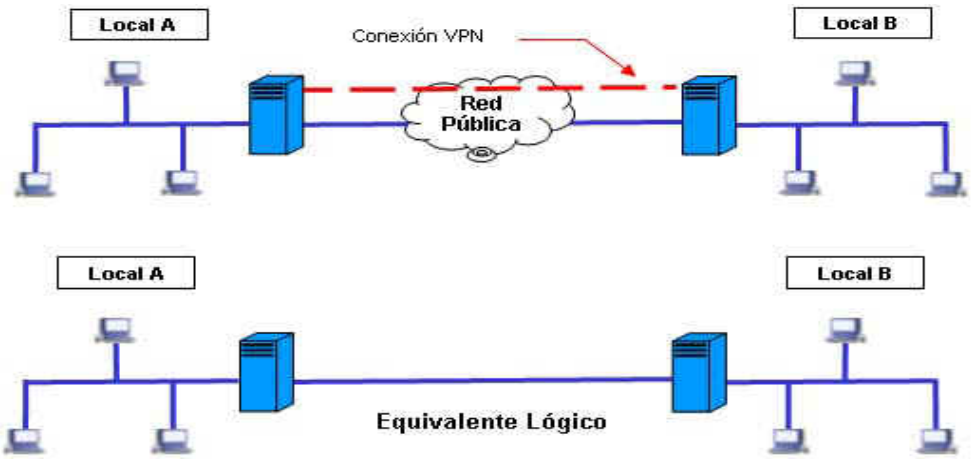

Figura 11. Conexión RPV

Por lo general las PSI se encargan del direccionamiento IP entre el enlace serial del enrutador externo y su conexión. También para las interfaces se utiliza un direccionamiento IP disponible.

Las RPVs tienen una manera de evitar las formas tradicionales de enrutamiento. No es posible enrutarlas a Internet a menos que se cuente con una dirección IP pública. Las RPVs se apegan a esto, pero cuando los datos llegan a la red, si se esta empleando NAT, pueden surgir problemas de enrutamiento. En cuanto a la autenticación se involucran dos pasos. El primer paso es agregar las reglas apropiadas al firewall para permitir el acceso a la red. Después, debe agregar un grupo de usuarios a ese objeto de red para que el dispositivo vea el tráfico de la

red y que aplique las reglas de autenticación de usuarios. El tráfico interno de los usuarios dispone de varias opciones. Puede permitir el acceso irrestricto a Internet desde las redes internas o puede restringirlas sólo a ciertos servicios.

Después de configurar los dispositivos de la RPV y que también se utilice el cifrado apropiado y la configuración de administración de claves, es necesario instalar las reglas de la RPV, que no son más que un significado cuando un dispositivo descarta cualquier tráfico que no está permitido explícitamente por reglas previas. Al aplicarle la regla establecerá una conexión al otro firewall en la sucursal o en cualquier parte donde se encuentre, permitiendo que los usuarios remotos tengan conectividad con la RPV. El primer paso para crear una RPV de LAN a LAN es intercambiar las claves entre cada dispositivo de firewall/RPV. Esto realiza el intercambio de claves entre los sitios y establece u "tunneling" que se empleará con base en la demanda. Cuando un usuario quiera conectarse a una oficina a una sucursal, el tráfico saldrá cifrado del dispositivo RPV de la sucursal. Ahora, lo último que falta por hacer es permitir que los usuarios remotos tengan la capacidad de establecer una RPV con otras sucursales. Para esto se necesita los siguientes pasos:

- Instalar el software RPV de un fabricante en los equipos portátiles remotos.
- Configurar el software.
- Añadir usuarios a la base de datos.

- Instalar una política de reglas que permita hacer esto.

Después de ver los pasos necesarios para la implementación, ahora vemos como se instalan utilizando el software y en que sistema operativo, en este caso hablaremos de RPV instaladas en Windows y Linux.

Utilizar Internet como infraestructura para conectar redes privadas es una solución óptima en términos de costos. Para incorporar seguridad en la comunicación entre las redes privadas a través de una red pública, es necesario lograr intercambiar datos codificados de forma que, si los datos son capturados durante la transmisión, no pueden ser descifrados. Los datos transitan codificados por Internet en "sistemas virtuales de “tunneling", creados por dispositivos RPV que utilizan criptografía. Estos dispositivos capaces de entender los datos codificados forman una "red virtual" sobre la red pública.

Los conceptos básicos y el funcionamiento RPV son presentados en la figura 12.

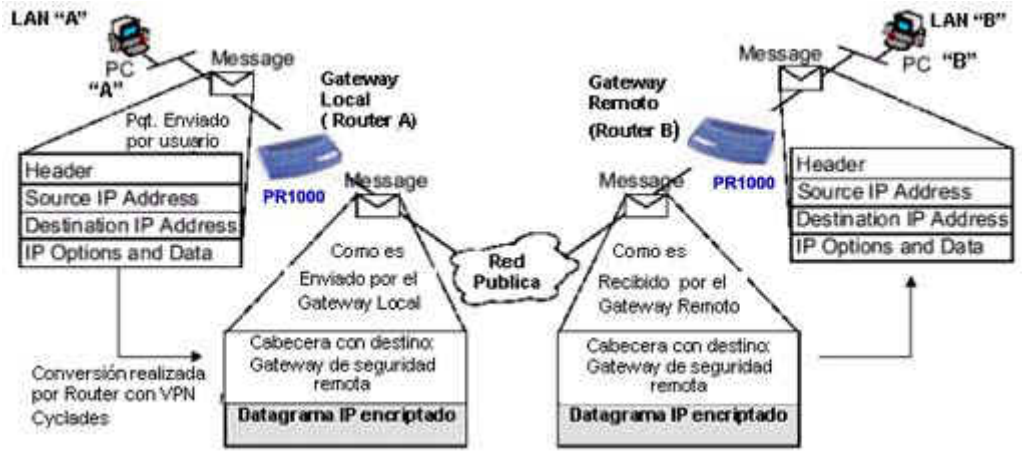

Figura 12. Funcionamiento de una RPV

1. Un datagrama IP (message) es enviado por la PC “A” en la LAN “A”, hacia la PC “B”, en la LAN “B”.

2. El mensaje llega al gateway Local (Router A)

El Router tiene 2 tablas, una con las direcciones de red seguras locales y otra con las direcciones de red remotas seguras.

3. Si la dirección IP de origen esta contenida en la lista de la red de seguridad local y la dirección IP de destino esta contenida en la lista de la red de seguridad remota entonces el mensaje es encriptado como muestra la figura, en base a una contraseña, esta será la misma que utilizara el Gateway remoto para encriptar y desencriptar los mensajes que van y vienen de la LAN A.

4. La cabecera del paquete encriptado tiene como dirección IP de destino la dirección del gateway remoto (Router B). Una vez que el paquete llega al Gateway remoto, este es desencriptado y enviado a su destino (PC B) tal como fue originado por la PC A. El proceso es similar cuando la PC B quiere enviar un mensaje a la PC A. Para el desarrollo de la configuración usaremos el siguiente esquema el cual muestra el direccionamiento IP para la conexión RPV de dos redes remotas a través de Internet

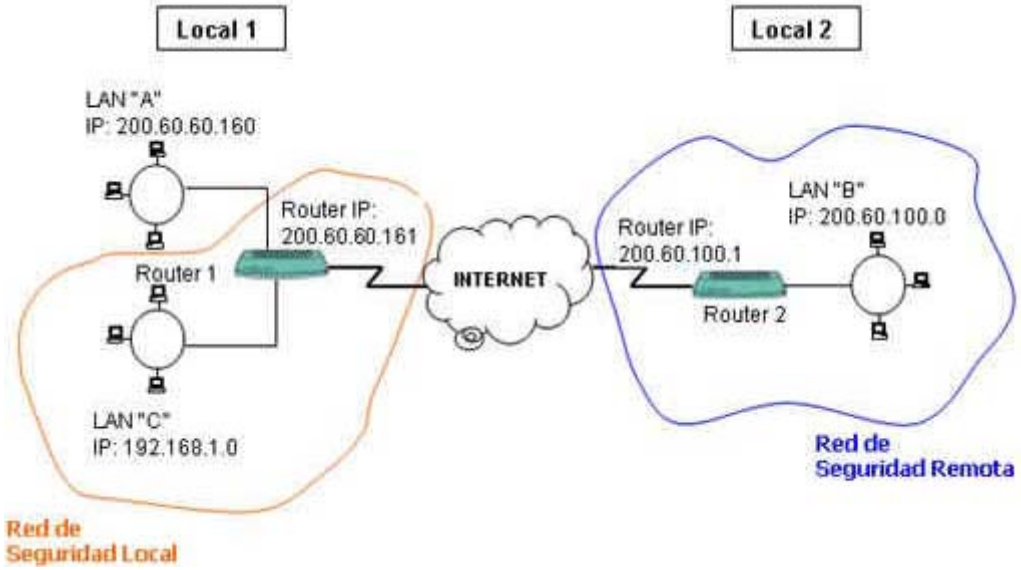

Figura 13. Red de Seguridad Local

Como se muestra en la figura 13, las únicas redes que podrán intercambiar información de forma segura a través de Internet es la red Lan C y la red Lan B.

Cabe resaltar que aunque la red Lan C es una red de direcciones IP privadas (no validadas en Internet) los datagramas desde esta red pueden transitar por Internet ya que como se explicó anteriormente, cuando estos paquetes van de una red de seguridad local a una red de seguridad remota, estos son encriptados y encapsulados y la nueva cabecera tendrá como IP de destino la del Router IP remoto.

También se aprecia que en la red local 1 aparte de la red Lan C hay otra red local, la red Lan A con dirección de red pública (validas en Internet) esta red también podrá comunicarse de con la red remota B (y con cualquier otra en Internet) pero

de forma no segura (su transmisión puede ser interceptada y modificada en el camino) ya que en el presente ejemplo de configuración no será considerada como una red Local segura. Vamos a suponer los siguientes datos para el enlace a Internet en cada uno de los locales son los mostrados en las siguientes tablas.

Local 1

Direcciones LAN	Cliente	Direcciones WAN	Usuario	Remota
Dirección IP	200.60.60.161	Dirección IP	172.22.16.86	172.22.16.85
Máscara	255.255.255.240	Máscara	255.255.255.252	255.255.255.252

Tabla 1. LAN número1

Local 2

Direcciones LAN	Cliente	Direcciones WAN	Usuario	Remota
Dirección IP	200.60.100.1	Dirección IP	172.22.5.174	172.22.5.173
Máscara	255.255.255.240	Máscara	255.255.255.252	255.255.255.252

Tabla 2. LAN número2

En el siguiente ejemplo de configuración de RPV. Consideraremos que los Router se encuentran completamente configurados según los datos mostrados arriba, y que se ha comprobado el enlace a Internet. Según se puede observar en la figura 13 el Router 1 tendrá dos direcciones en la interfase Fast Ethernet, una primaria

con dirección privada y una secundaria con dirección pública. Los pasos que deberemos de seguir son los siguientes:

Habilitación de la Función RPV en el Router

Configuración del Router IP

Configuración de los parámetros de las redes RPV

a. Como añadir red local

b. Como añadir gateway remoto

c. Como añadir la red remota

d. Como habilitar RPV

Para un mejor entendimiento del proceso se describirá paso a paso el proceso de configuración del Router 1, siendo este similar para el caso del Router 2, al final se mostrara el listado de la configuración para este Router.

3.4.1 Habilitación de la Función RPV

Por defecto la Función RPV está deshabilitada. Para activarla, con el ROUTER ID solicite el password, e ingréselo en la siguiente secuencia de menú.

Main Menú: 6. ADMIN 2. ENABLE FEATURE

---

1. IPX 2. VPN

Select option ==> 2 < Selecciones la opción 2 >

Router ID : 6645D50700007B

Type password :_____ **< Introduzca el Password >**

3.4.2 Configuración del Router IP

Cada interfase del Router tiene una dirección IP (o más de una opcionalmente), adicionalmente el Router puede ser configurado para tener una dirección IP asociada que lo identifique como equipo dentro de una red, la cual debe ser la dirección de alguna de las interfaces, esta deber ser una dirección enrutada en Internet (Pública).

El ROUTER IP se usa cada vez que una única dirección IP se necesite para identificar el Router. Es importante que cada Router se use como un gateway local o remoto de seguridad tenga este parámetro definido, este no se define automáticamente. Configure esta dirección en el menú:

Main Menú: 1. CONFIG 6. IP

Cyclades-PR1000 (PR1000) IP Menu

1. DNS client 2. TCP 3. DHCP

4. Router IP 5. IP Helper

(L for list) Select option ==> 4 < Seleccione la opcion 4 >

En el ejemplo el Router IP del Router 1 es 200.60.60.161, que corresponde a la dirección de la interfase LAN.

Default Router IP Address for Applications [0.0.0.0] : **200.60.60.161**

3.4.3 Configuración la Función RPV

a. Como añadir la red local

Definir la red de seguridad local, en el menú:

Main Menú: 1. CONFIG 4. SECURITY 7. VPN

Cyclades-PR1000 (PR1000) VPN Menu

1. Remote Gateways 2. Local IP Networks 3. Remote IP Networks

4. Options

(L for list) Select option ==> 2 **< Seleccione 2 >**

Y después en:

1. Add Network 2. Delete Network 3. Edit Network

4. Clear Local Networks

(L for list) Select option ==> 1 **< Seleccione 1 >**

Ingrese la dirección IP y la máscara de la Red local donde se encuentra todas las PCs que harán uso de la función de RPV. En el ejemplo la red: 192.168.1.0 deberá ser añadida

Local Network IP address [0.0.0.0] : **192.168.1.0**

Local Network Netmask [255.0.0.0] : **255.255.255.0**

b. Como añadir el gateway Remoto (router 2)

En el menú:

Main Menú: 1. CONFIG 4. SECURITY 7. VPN

Cyclades-PR1000 (PR1000) VPN Menu

1. Remote Gateways 2. Local IP Networks 3. Remote IP Networks

4. Options

(L for list) Select option ==> 1 **< Seleccione 1 >**

y después en:

1. Add Gateway 2. Delete Gateway 3. Edit Gateway

(L for list) Select option ==> 1 **< Seleccione 1 >**

Ingrese la dirección IP del Gateway remoto (Router IP del router 2) además de la contraseña (secret). Esta contraseña es aplicable a cada par de routers, si el router 2 define la contraseña como : nuevo, entonces la del router 1para el router 2 debe ser: nuevo. En el ejemplo la dirección IP del Gateway remoto es: 200.60.100.1

Remote Security Gateway IP address [0.0.0.0] : 200.60.100.1

Secret [] : **nuevo**

c. Como añadir la red remota

Ahora la red remota de seguridad debe ser definida. En el menú:

Main Menú:1. CONFIG 4.SECURITY 7.VPN

Cyclades-PR1000 (PR1000) VPN Menu

1. Remote Gateways 2. Local IP Networks 3. Remote IP Networks

4. Options

(L for list) Select option ==> 3 **< Seleccione 3 >**

y después en:

1. Add Network 2. Delete Network 3. Edit Network

4. Clear Remote Networks

(L for list) Select option ==> 1 **< Seleccione 1 >**

Ingrese la dirección IP y la máscara de la red remota de seguridad. La dirección IP del Gateway de seguridad remota (paso 3) a la cual está conectada esta red, también debe ser ingresada aquí. En el ejemplo la dirección IP de la red de seguridad remota es: 200.60.100.0 y la dirección IP del Gateway remoto es: 200.60.100.1

Remote Network IP address [0.0.0.0] : **200.60.100.0**

Remote Network Netmask [255.0.0.0] : **255.255.255.240**

Remote Security Gateway IP address [0.0.0.0] : **200.60.100.1**

d. Como habilitar la RPV

Finalmente activar la función de RPV y configurar las opciones del RPV. En el menú:

Main Menú: 1. CONFIG 4. SECURITY 7. VPN

En el menú:

Cyclades-PR1000 (PR1000) VPN Menu

1. Remote Gateways 2. Local IP Networks 3. Remote IP Networks

4. Options

(L for list) Select option ==> 4 **< Seleccione 4 >**

Active el estado de la función RPV, en el Router y de ser necesario, configure las opciones del RPV. Estas opciones deben ser las mismas para todos los gateway de seguridad remota en una RPV.

Cyclades VPN status ((A)ctive or (I)nactive) [I] : **a < activa el tunnel**

vpn >

Tunnel keepalive timeout in seconds [60] : ↵

Tunnel keepalive retries [5] : ↵

Tunnel inactivity timeout in seconds [600] : ↵

Time interval for VPN retries in seconds [10] : ↵

Presionar ESC , ESC, ESC

(D)iscard, save to (F)lash or save to (R)un configuration : **F < Guarde la Configuracion >**

Antes de poder iniciar tráfico de paquetes entre los routers 1 y 2 el Router 2 deberá ser configurado de manera similar al procedimiento descrito. A continuación se muestra el listado de la configuración para el Router 2

Remote Security Gateways:

Gateway IP address Secret

200.60.60.161 nuevo

Local IP Networks:

Destination Subnet Mask

200.60.100.0 255.255.255.240

emote IP Networks:

Destination	Subnet Mask	Security Gateway
192.168.1.0	255.255.255.0	200.60.60.161

Cyclades VPN is active Tunnel keepalive timeout in seconds 60

Tunnel keepalive retries 5

3.5 Configuración de protocolos

3.5.1 Configuración de una RPV bajo Windows

Para configurar una RPV 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 RPV. 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 en la figura 14, y al cual se accede a través de la opción *Propiedades* del icono *Entorno de Red*, se presiona el botón "*Add*."

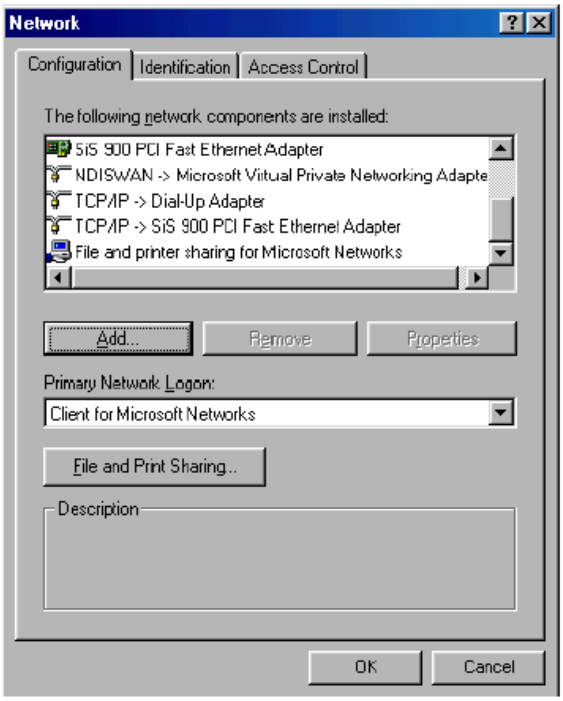

Figura 14. Dialogo de red.

Aparecerá la siguiente pantalla, como se muestra en la figura 15, se deberá seleccionar "*Adapte*r" y luego presionar el botón "*Add*".

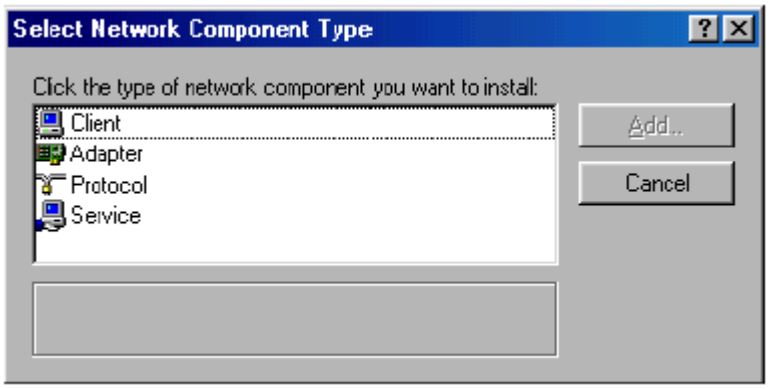

Figura 15. Ventana de componentes de red

Aparece el cuadro "*Select Network Adapters*", donde se deberá elegir el fabricante y el adaptador como se muestra en la figura 16:

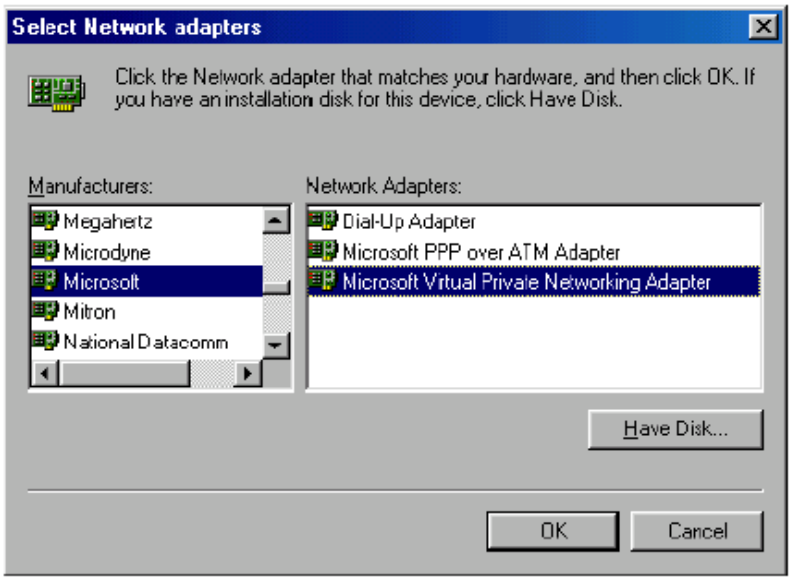

Figura 16. Ventana de "Network adapters"

Posteriormente, para instalar la conexión a la LAN, se deberá acceder al *Acceso Remoto a Redes* que se muestra en la figura 17.

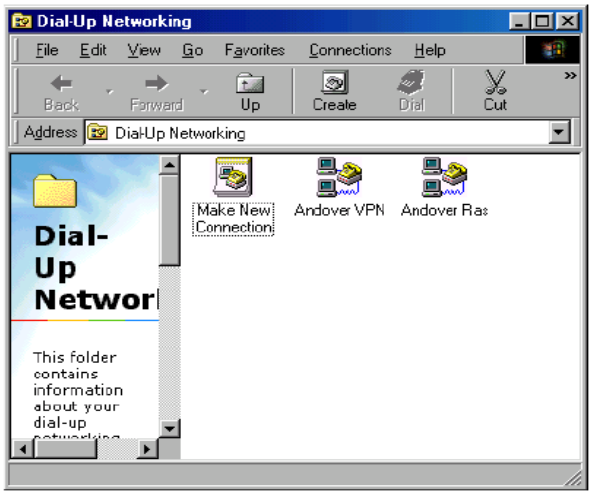

Figura 17. Ventana de “Dial-up network”

Se selecciona "*Make a New Connection*", como se ilustra en la figura 18, apareciendo la siguiente pantalla, donde se podrá elegir el adaptador de RPV:

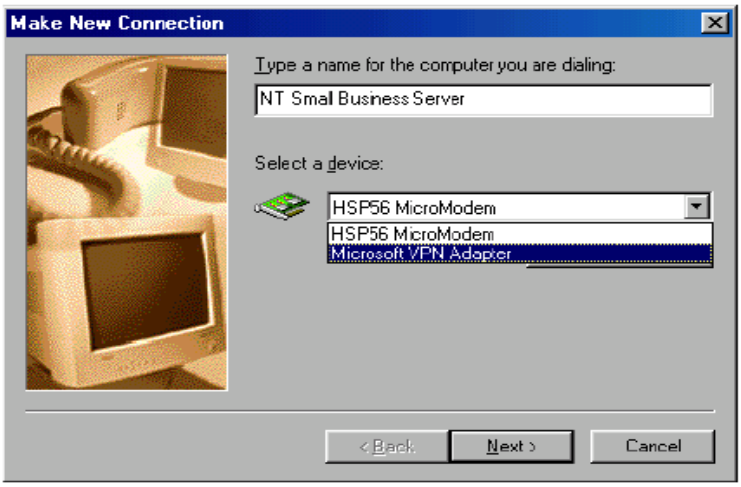

Figura 18. Ventana de “Make a new connection”

Luego de presionar el botón "*Next*", se deberá introducir la dirección IP del servidor RPV en la figura 19:

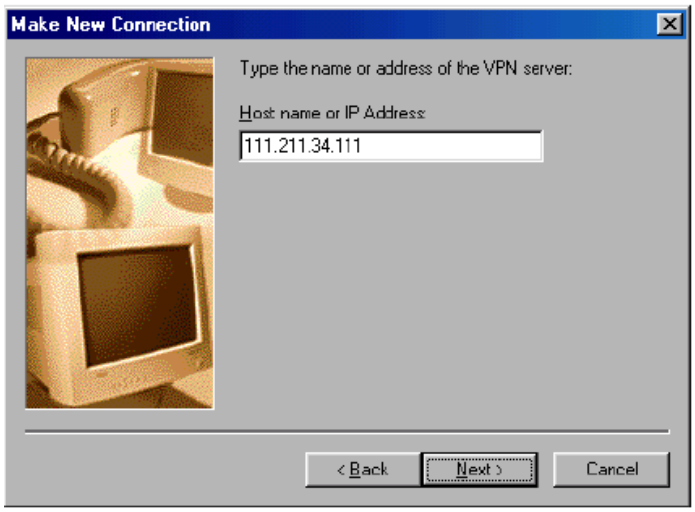

Figura 19. Ventana de “Make a new connection”

De esta manera se finaliza la creación de la nueva conexión, así aparece, como se muestra en la figura 20:

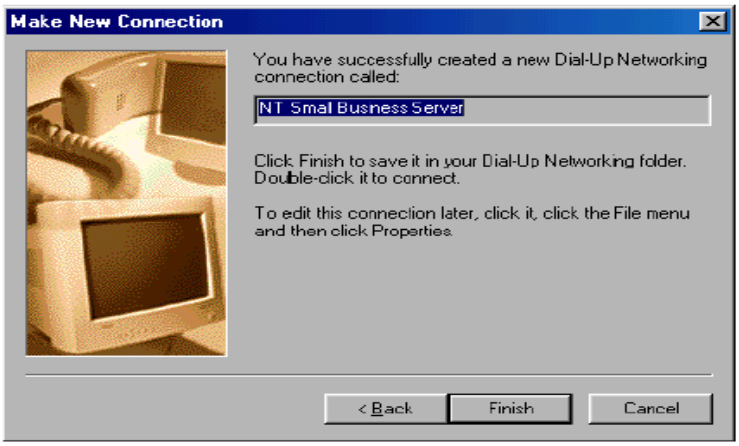

Figura 20. Ventana de “make a new connection”

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

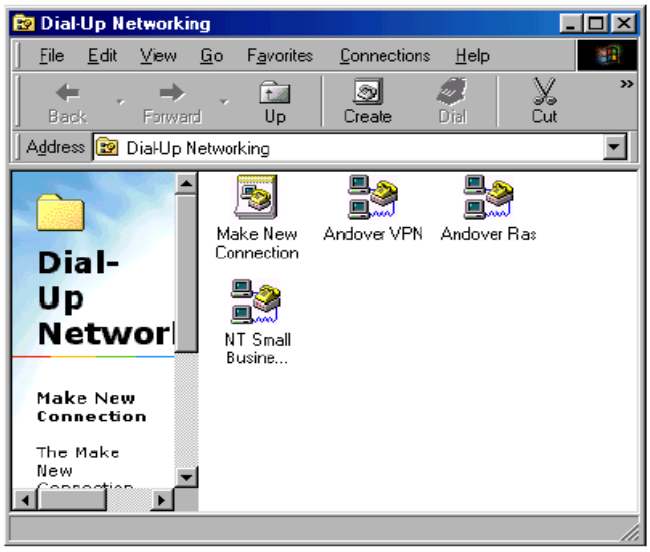

Figura 21. Ventana de “Dial-up network”

Al hacer doble-click en el icono de la conexión RPV, como muestra la figura 22, donde se debe introducir el nombre de usuario, la contraseña y la dirección IP del servidor NT:

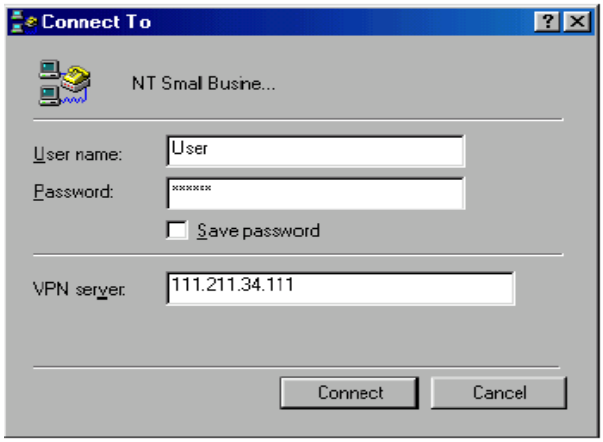

Figura 22. Ventana de conexión RPV

Para configurar el servidor RPV, 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 hace lo siguiente.

Dentro de *Red* en el *Panel de Control*, seleccionando *Protocolos* (figura 23), se deberá presionar el botón *Agregar*:

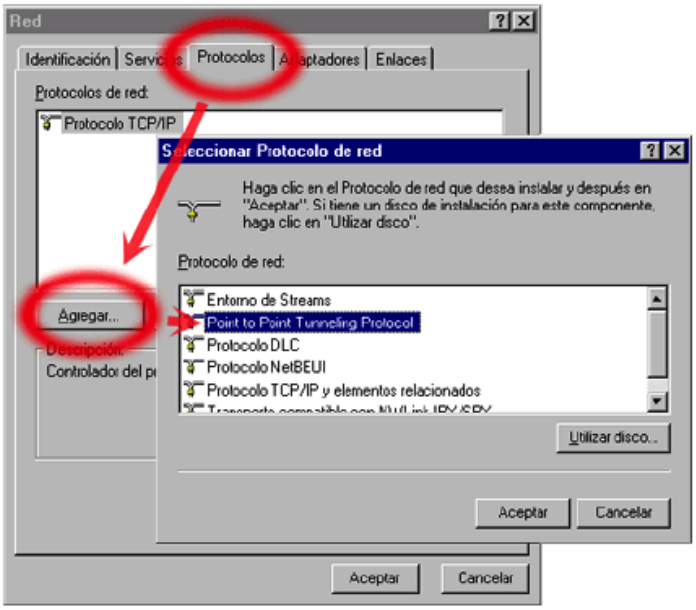

Figura 23. Ventana de Protocolo de red.

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 la figura 24, se establecen 2 RPV:

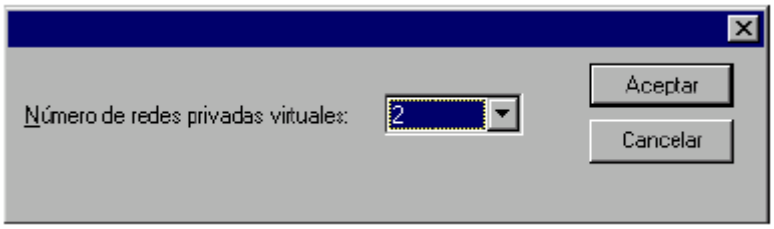

Figura 24. Ventana para escoger el número de RPVs

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 25):

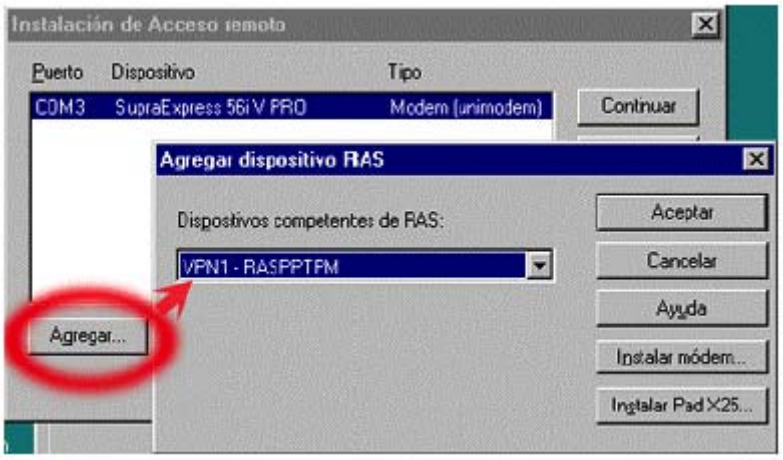

Figura 25. Ventana de Herramientas de configuración RAS

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 servidor.

Para la activación del filtro PPTP, se debe selecciona la pestaña "*Protocolos de Panel de Configuración / Red*". Dentro de esta pantalla, se elige *Protocolo TCP/IP*, luego *Propiedades*. En la pestaña *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 "tunneling" RPV 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 RPV añadidos a la configuración RAS al instalar PPTP. Esta lista sólo muestra los RPV 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 módem.

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

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

3.5.2 Configuración de una RPV bajo LINUX

En este apartado se explica la configuración del demonio de RPV (DRPV) sobre Debian, pero no debiera traer ningún problema configurarlo en otra distribución.

RPVD 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 RPV mediante un medio seguro, ya que es la clave que ambos extremos de la RPV comparten.

Configuración de los extremos de la RPV, 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 montar la RPV, 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

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

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)

4. PROBLEMAS

Las RPV son una masa confusa de tecnologías. Steven Brown [4]explica que se pueden experimentar problemas; lamentablemente, en muchos casos no es culpa de la RPV. A continuación se detallan algunas áreas donde se pueden presentar problemas:

- **Usuarios con marcación remota:** es muy posible que los usuarios de marcación remota no puedan conectarse al dispositivo RPV para establecer un "tunneling" de cifrado. Este problema en particular es uno de los que más frecuentemente ocurre cuando se implementa una RPV. Específicamente estos problemas son causados pro fallas del software instalados en los equipos portátiles.

- **RPV de LAN a LAN:** aquí es necesario realmente comprender la configuración para establecer la RPV de Lan a Lan. No importa si se trata de IPSec, PPTP o L2TP, si no entiende el protocolo empleado, no va hacer que funcione la RPV. Existen muchas formas de configurar una RPV con protocolos distintos. PPTP Y L2TP son protocolos de segundo nivel, e IPSec es un protocolo de nivel tres. Por lo tanto puede combinar ambos. Sin embargo, es posible que al combinarlos haya problemas en cualquier

[4] BROWN, Steven. Implementación redes

protocolo. Antes de resolver los problemas relacionados con estos protocolos, primero debe saber como establecer esta configuración.

- **Servicios de autenticación:** esta es otra cosa que se debe revisar una vez que se hayan configurado las conexiones de marcación remota a la RPV, las conexiones RPV de LAN a LAN y las conexiones de extranet a la RPV. Estos usuarios deben estar autenticados. Si el dispositivo de autenticación no puede comunicarse con el dispositivo de la RPV o no puede responder lo suficientemente rápido, la comunicación se suspenderá en diversos periodos.

- **Proxy:** dependiendo del tipo de dispositivo que coloque junto al punto de acceso a Internet, se pueden confundir los problemas del proxy con los problemas de la RPV. En este caso, debe averiguar qué tanto pueden adentrarse los usuarios en la red.

- **Enrutamiento WAN interno:** el enrutamiento es otra causa principal de los problemas en las RPVs. Sin una configuración adecuada de una política de enrutamiento que envíe los paquetes que llegan a través del dispositivo RPV, no habrá comunicación.

- **Internet:** algunos PSI (Proveedores de Servicio de Internet) bloquean los paquetes cifrados. Si un enrutador, suyo o de cualquiera en la trayectoria

---

privadas virtuales. México.1999. p 266

entre el usuario y la red corporativa, establece un filtro para bloquear estos paquetes, nunca habrá comunicación.

- **Problemas de cifrado:** Entre dos RPVs, puede haber problemas de cifrado. Los mecanismos de claves, los tiempos para realizar el intercambio de claves, los problemas de comunicación y las actualizaciones pueden afectar las comunicaciones entre los dos sitios.

- **Direccionamiento:** antes de establecer una RPV, necesita conocer los aspectos concernientes al direccionamiento, ¿Tiene un espacio de dirección privada o pública? ¿Emplea una NAT? Si no es así, y piensa utilizar IPSec en modo “tunneling”, entonces necesitará direcciones públicas.

- **RPV múltiple:** Si utiliza un dispositivo RPV múltiple, como una estación UNIX, y decide usarlo como una combinación firewall/RPV, y considera tener zonas DMZ múltiples, entonces debe considerar el flujo del tráfico, los aspectos del enrutamiento y los posibles aspectos de la NAT en la misma caja.

Podemos ver que existen muchas áreas donde se requieren de habilidades para resolver problemas de las RPVs. Podría decirse que el paso más importante en la solución de los problemas de RPV es el aislamiento. Si no puede aislar el problema, puede tomarle mucho tiempo encontrarlo. También es importante saber

toda la información posible sobre aspectos como archivos de registros, ventanas múltiples en el dispositivo, entre otros, puesto que quizá tenga que vigilar el dispositivo RPV mientras alguien intenta crear un “tunneling”.

5. CASO DE ESTUDIO

5.1 Conceptualización

Con independencia del tipo de red WAN que en las empresas decidan utilizar: Frame Relay, Punto a Punto, IP o ATM, ya sean basadas en técnicas de routing o de conmutación, lo cierto es que el concepto de **Redes Privadas Virtuales** (RPV o VPN -Virtual Private Networks-) constituye una pieza fundamental en el diseño y arquitectura de las Redes de Nueva Generación sobre las que se basarán las comunicaciones empresariales de las próximas décadas.

Combinando las ventajas de las redes dedicadas (seguridad QoS) con las correspondientes a las redes compartidas (sencillez y bajo coste), las RPVs proporcionan la arquitectura básica necesaria para transportar de forma segura los nuevos servicios y aplicaciones convergentes (Web Call Centre, Formación a Distancia, Comunicadores Personales,...). Mediante el establecimiento de unas rutas (tunneling) a través de una red compartida (red IP), se transmite de forma transparente la información pertinente entre los dos extremos del “tunneling”, con total independencia del tipo de tráfico que éstas envíen y de la clase de estación que lo origine.

La implementación de redes RPV puede realizarse con Router NETBuilder, pero lo cierto es que una nueva generación de sistemas de la familia 3Com PathBuilder

conocidos como Conmutadores de “Tunneling” (Tunnel Switch) ofrecen una capacidad y rendimiento considerablemente superior a los presentados por los routers convencionales.

Las soluciones WAN que Cititronic ofrece al mercado se caracterizan por su flexibilidad, fiabilidad y los beneficios que para las empresas representa.

Flexibilidad

Tanto si una empresa decide implementar sus comunicaciones WAN con tecnología de routing convencional, como si se decide por la utilización de “tunneling”, las plataformas **3Com PathBuilder, 3Com NetBuilder y 3Com CoreBuilder** permiten diseñar soluciones Multitecnología con soporte multiprotocolo (IP, SNA, X.25, Frame Relay, ATM,…) de extremo a extremo que sean Escalables, de alto Rendimiento y basadas en Estándares.

Multi-tecnología

Los sistemas PathBuilder, NETBuilder y CoreBuilder como principales elementos de una solución WAN, se caracterizan por soportar, de forma modular, configuraciones y conexiones basadas en múltiples tipos de tecnologías: Routing, “tunneling”, Líneas dedicadas, Voz/Fax sobre IP, Multimedia sobre IP, etc.

Escalabilidad

Algunas personas piensan que todo equipo modular es un equipo escalable. Sin embargo, aunque la modularidad es un elemento necesario, el concepto de escalabilidad tiene un significado mucho más exigente que la simple modularidad. La solución y sistemas NETBuilder, PathBuilder y Total Control, presentan características muy inportantes, como rendimiento, que presenta un elevado número de conexión unido a la necesidad de implementaciones de técnicas de seguridad sobre la red WAN y por lo cual hace necesario disponer de equipos que eviten cualquier situación de cuello de botella. En este sentido, es necesario resaltar que los equipos 3Com incorporan módulos multiprocesador que permiten un proceso distribuido de la información a transmitir a la vez que cuenta con elementos hardware específicos para tareas de encriptado.

Cualquier solución presenta un inconveniente difícil de salvar para su utilización: no es interoperable con implementaciones de otros fabricantes o con soluciones definidas por la industria como estándares (de derecho o de facto). Para evitar esta situación, 3Com participa de forma activa en los principales foros de estandarización, garantizando de esta forma que sus equipos y soluciones cumplen las normas y recomendación establecidas por los organismos de estandarización (ITU-T, IETF, ISO, ATM Forum, etc.).

5.2 La solución de Volkswagen para comunicar a sus concesionarios

Wolkswagen de México implementó un sistema para optimizar el proceso de compra y venta de sus automóviles, y *Gedas North America* fue la compañía encargada de instalar la red de comunicación *Dealer Communication Systems* (Sistema de Comunicación de Concesionarios; DCS). Por medio de esta red, 190 concesionarios distribuidos a lo largo de la República Mexicana están conectados para realizar todas sus transacciones, desde el pedido de autos hasta su facturación.

El antiguo sistema de órdenes de automóviles con el que trabajaba la compañía estaba basado en sistemas centrales, por lo que constantemente se enfrentaba a problemas inherentes a su plataforma. Era lento, difícil de operar y de actualizar, y se caía continuamente.

Los vendedores necesitaban un sistema confiable, flexible y fácil de operar y mantener. Con estas especificaciones, *Gedas North America* implementa una red privada virtual, involucrando a un *carrier* nacional y a otro internacional, permitiendo la ampliación de la intranet de Volkswagen para conectar a todos sus concesionarios. Esta implementación extendió su funcionalidad hacia cuatro áreas.

- **Autos:** consulta de existencia, asignación, pedidos, registros de venta, consulta de crédito, precios y retenciones, autocapacitación por computadora y ayuda en línea.

- **Refacciones:** creación y consulta de pedidos, ayuda en línea, capacitación por computadora y cambio de password.

- **Area comercial:** detalles de los movimientos financieros, refacciones en plazo de gracia y pendientes de factura, ayuda en línea y autocapacitación por computadora.

- **Funcionalidad en correo electrónico:** envío y recepción de mensajes y archivos, directorio de destinatarios, ayuda en línea y autocapacitación por computadora.

Así mismo, la empresa que implementa una red privada virtual, goza de disponibilidad permanente en las líneas de su red, sin pago de renta fija. Además, el cobro que realiza el suministrador se calcula de acuerdo con el tipo de enlace donde se genera y donde concluye la llamada, por distancia y tiempo de uso; es decir, se paga únicamente por lo que se usó. Para facturar una llamada, Jennifer Jauckens señala que Alestra toma en cuenta la infraestructura sobre la cual se origina cada llamada, así como la infraestructura sobre la que se entrega, lo que representa ahorros significativos.

6. CONCLUSIONES Y OBSERVACIONES

Hasta no hace mucho tiempo, las diferentes sucursales de una empresa podían tener, cada una, una red local a la sucursal que operara aislada de las demás. Cada una de estas redes locales tenía su propio esquema de nombres, su propio sistema de email, e inclusive tenían sus protocolos que diferían de los usados en otras sucursales. Es decir, en cada lugar existía una configuración totalmente local, que no necesariamente debía ser compatible con alguna o todas las demás configuraciones de las otras áreas dentro de la misma empresa.

A medida que la computadora fue siendo incorporada a las empresas, surgió la necesidad de comunicar las diferentes redes locales para compartir recursos internos de la empresa. Para cumplir este objetivo, debía establecerse un medio físico para la comunicación. Este medio fueron las líneas telefónicas, con la ventaja de que la disponibilidad es muy alta y que se garantiza la privacidad.

Además de la comunicación entre diferentes sucursales, surgió la necesidad de proveer acceso a los usuarios móviles de la empresa. Mediante Remote Access Services (RAS), este tipo de usuario puede conectarse a la red de la empresa y usar los recursos disponibles dentro de la misma.

El gran inconveniente del uso de las líneas telefónicas es su alto costo, ya que se suele cobrar un abono mensual más una tarifa por el uso, en el que se tienen en

cuenta la duración de las llamadas y la distancia hacia donde se las hace. Si la empresa tiene sucursales dentro del mismo país pero en distintas áreas telefónicas, y, además, tiene sucursales en otros países, los costos telefónicos pueden llegar a ser prohibitivos.

Adicionalmente, si los usuarios móviles deben conectarse a la red corporativa y no se encuentran dentro del área de la empresa, deben realizar llamadas de larga distancia, con lo que los costos se incrementan.

Las Redes Privadas Virtuales (RPV) son una alternativa a la conexión WAN mediante líneas telefónicas y al servicio RAS, bajando los costos de éstos y brindando los mismos servicios, mediante el uso de la autenticación, encriptación y el uso de “tunneling” para las conexiones.

El término RPV se refiere a una Red Privada Virtual (Red Privada Virtual), la cual utiliza Internet como mecanismo de transporte, manteniendo la seguridad de los datos en la RPV. La configuración más común de RPV es a través de una red interna principal y nodos remotos usando RPV para lograr el acceso completo a la red central. Los nodos remotos son comúnmente oficinas remotas o empleados trabajando en casa. También pueden vincularse dos redes más pequeñas para conformar una red simple, incluso más grande.

Los parámetros de seguridad para los sistemas de “tunneling” individuales se pueden negociar entre sitios no homogéneos para alcanzar niveles altos de

seguridad. No disminuye el perfomance de las redes. Las RPVs dan confiabilidad a los usuarios y garantizan transacciones de índole privado. Instalando RPV, se consigue reducir las responsabilidades de gestión de un red local.

Para implementar una solución con RPV se requiere un examen cuidadoso de las necesidades de red y seguridad, porque las soluciones elegidas van a tener un fuerte impacto en la red existente y por ende en la organización.

La seguridad de una red privada virtual requiere protocolos especiales de "tunneling" tales como PPTP, IP Móvil o L2TP, debido a que los sistemas de "tunneling" permiten al servidor realizar todas las comprobaciones de seguridad y la encriptación de datos. Los estándares emergentes como IPSec e IP versión 6 brindan seguridad, encapsulación encriptada y "tunneling" Para los datos del usuario, puesto que éste se ha vuelto extremadamente más sensitivo sobre la privacidad de sus datos sobre redes públicas.

La empresa que pretenda implementar este tipo de solución para sus requerimientos de comunicación, debe considerar diferentes puntos antes de decidir si una red privada virtual responde como la mejor opción para satisfacer sus necesidades:

-Necesidades de comunicación por departamento, empleado, oficina y localidad.

-Necesidad de ahorro en los costos de llamadas de larga distancia.

-Crecimiento a corto plazo del negocio, y requerimientos de respuestas rápidas - Potencial de abuso en llamadas por los empleados o visitantes.

-Necesidad de instrumentos para restringir el servicio de larga distancia y protegerse contra el abuso del mismo.

-Empleados que viajan.

-Distribución de costos o facturación por departamentos, proyectos o clientes.

7. BIBLIOGRAFÍA

Libros de Referencia

BROWN, Steven. Implementación de Redes Privadas virtuales. México D.F. Editorial Mc Graw Hill, 1999.

CABALLERO GIL, Pino. Introducción a la Criptografía. México D.F. Editorial RA-MA, 2002.

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

RODRÍGUEZ, E. Jorge Introducción a las Redes de Área Local, Mexioo D.F. Editorial Mcgraw-Hill.Interamericana, 2000.

STALLINGS, William. Comunicaciones y Redes entre Computadores, Madrid España. Editorial Prentice may, 1997.

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

ZACKER, Craig. REDES (MANUAL DE REFERENCIA), Madrid España, Editorial MC Graw Hill, 1999.

RAYA, Cristina y RAYA, José Luis. Redes Locales, Madrid España. Editorial RA-MA, 2001.

Paginas Web:

CYCLADES. Electronic sources: MLA styles of citation. Configuración de routers. USA: Cyclades, 2001 8 p. (En línea) Enero 25, 2003 Disponible en: <http://www.cyclades.com.pe/Soporte/PRx000/Bulletin111.htm>

GOMEZ, A. F. Citation Styles. En: Online: Seguridad en Redes. Redes Privadas Virtuales. Murcia, España: Universidad de Murcia. Febrero 3, 2003.

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

VIPTEL. Electronic sources: MLA styles of citation. Mexico: Viptel, 2002 5 p. (En línea) Enero 25, 2003 Disponible en:

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

LAFACU.COM. Electronic sources: MLA styles of citation. México: lafacu.com, 2003 15 p. (En línea) Marzo 5, 2003 Disponible en. <http://www.lafacu.com/apuntes/informatica/Redes_Virtuales_Privadas/ default.htm>

MICROSOFT Corporation. Citation Styles. Online: Troubleshooting PPTP connectivity issues in Windows NT 4.0. España: Microsoft Corporation. Abril 10, 2003. <http://www.eu.microsoft.com/intlkb/spain/E10/7/19.asp.

SGI España. Citation Styles. En: OnlineArticulos de Interes. Madrid, España. Abril 20, 2003. <http://www.sgi.es/prensa/articulos_interes/sic-ssgs-oct98.pdf>

Nombre de archivo: RPVs - Parte I.doc
Directorio: D:\Monografia\.Doc
Plantilla: C:\WINDOWS\Application Data\Microsoft\Plantillas\Normal.dot
Título: REDES PRIVADAS VIRTUALES (RPVs)
Asunto:
Autor: enrique vanegas mattos
Palabras clave:
Comentarios:
Fecha de creación: 30/05/03 02:08 A.M.
Cambio número: 7
Guardado el: 16/06/03 11:56 P.M.
Guardado por: enrique vanegas mattos
Tiempo de edición: 48 minutos
Impreso el: 16/06/03 11:57 P.M.
Última impresión completa
Número de páginas: 102
Número de palabras: 14,504 (aprox.)
Número de caracteres: 82,676 (aprox.)