EVOLUCIÓN DE LA SEGURIDAD EN LOS PROTOCOLOS DE TUNELAJE PARA REDES PRIVADAS VIRTUALES

LUZ ADRIANA GÓMEZ SERNA

JORGE ALBERTO CONTRERAS MEZA

UNIVERSIDAD TECNOLÓGICA DE BOLIVAR

FACULTAD DE INGENIERIAS

DIRECCIÓN DE PROGRAMAS DE INGENIERIA ELECTRICA Y ELECTRÓNICA

CARTAGENA DE INDIAS, D.T Y C

2005

EVOLUCIÓN DE LA SEGURIDAD EN LOS PROTOCOLOS DE TUNELAJE PARA REDES PRIVADAS VIRTUALES

LUZ ADRIANA GÓMEZ SERNA

JORGE ALBERTO CONTRERAS MEZA

Monografía presentada como registro de aprobación del Minor en Telecomunicaciones

Director

MARGARITA UPEGUI FERRER

Ingeniera Electrónica

Magíster en Ciencias Computacionales

UNIVERSIDAD TECNOLÓGICA DE BOLIVAR

FACULTAD DE INGENIERIAS

DIRECCIÓN DE PROGRAMAS DE INGENIERIA ELECTRICA Y ELECTRÓNICA

CARTAGENA DE INDIAS, D.T Y C

2005

CONTENIDO

Página

LISTA DE FIGURAS

LISTA DE TABLAS

GLOSARIO

ADSL (Asymmetric Digital Subscriber Line)

Es una de las tecnologías que permiten utilizar la línea telefónica de cobre, que en las instalaciones tradicionales conecta la central telefónica con la vivienda de los usuarios, para transmitir datos a alta velocidad, a la vez que mantiene la transmisión de voz. Para ello utiliza frecuencias más altas que las empleadas en el servicio telefónico y sin interferir en ellas, permitiendo así el uso simultáneo del servicio telefónico y para acceder a servicios de datos a través de ADSL.

ANSI (American National Standards Institute)

Se trata del organismo estandarizador norteamericano, pero sus decisiones y normas de estandarización tienen un importante peso específico sobre la industria informática mundial. Incluye el IM (Institute of Electrical and Electronics Engineers) y la VA (Electronic Industries Association). ANSI es la primera organización para fomentar el desarrollo de estándares tecnológicos en los Estados Unidos. ANSI trabaja con grupos industriales y es el miembro Estadounidense de la ISO (International Organization for Standardization) y de la IEC (International Electrotechnical Commission).

APPLETALK

AppleTalk es un conjunto de protocolos de comunicaciones (tales como IPX/SPX y NCP), usado para definir la conectividad en una red AppleShare. En el modelo OSI, AppleTalk se puede comparar con los protocolos de comunicaciones NetWare, debido a que ambos protocolos especifican comunicaciones, que van desde interfaces de aplicaciones hasta acceso a medios.

APPLESHARE

AppleShare es la solución de conectividad de Apple Computers. Requiere un ordenador Macintosh como servidor de red, e incluye software de servidor y de estación de trabajo. Utiliza el Protocolo de Archivo de AppleTalk (AFP). La

solución de conectividad Macintosh de Novell une el software de servidor NetWare for Macintosh con el software para estación de trabajo AppleShare.

ATM

El Modo de Transferencia Asíncrono es una tecnología de conmutación que usa pequeñas celdas de tamaño fijo. En 1988, el CCITT designó a ATM como el mecanismo de transporte planeado para el uso de futuros servicios de banda ancha. ATM es asíncrono porque las celdas son transmitidas a través de una red sin tener que ocupar fragmentos específicos de tiempo en alineación de paquete, como las tramas T1. Estas celdas son pequeñas (53 bytes), comparadas con los paquetes LAN de longitud variable. Todos los tipos de información son segmentados en campos de pequeños bloques de 48 bytes, los cinco restantes corresponden a un header usado por la red para mover las celdas. ATM es una tecnología orientada a conexión, en contraste con los protocolos de base LAN, que son sin conexión. Orientado a conexión significa que una conexión necesita ser establecida entre dos puntos con un protocolo de señalización antes de cualquier transferencia de datos. Una vez que la conexión está establecida, las celdas ATM se auto-enrutan porque cada celda contiene campos que identifican la conexión de la celda a la cual pertenecen.

BLOWFISH

Algoritmo asimétrico de encriptación diseñado por Bruce Schneier en 1993 como una alternativa a los algoritmos de encriptación existentes, tales como DES. Blowfish es un bloque cifrado de 64 bits (por ejemplo, una llave criptográfica y algoritmo son aplicados a un bloque de datos en vez de solo bits) una llave cuya longitud puede variar entre 32 y 448 bits. Este algoritmo es de libre distribución, y la tecnología no está patentada y de libre licencia.

B2B (usiness-to-Business)

Modalidad de comercio electrónico en el que las operaciones comerciales se realizan entre empresas y no con usuarios finales. Algunos, muy pocos, utilizan el acrónimo español EAE.

DECNET

Conjunto de protocolos de red desarrollado por Digital Equipment Corporation, y usado en su familia de ordenadores VAX, para el intercambio de mensajes y otros datos. Es un conjunto de productos hardware y software que implementan la arquitectura de red digital (DNA). Define redes de comunicación sobre LAN Ethernet, redes de área metropolitana con interfaz de datos distribuida de fibra (FDDI MAN) y WAN que utilicen características de transmisión de datos privados o públicos. Aunque en la actualidad DECnet es un protocolo propietario, DEC está uniendo sus protocolos con protocolos OSI para el próximo DECnet Phase V. Cuando este proceso esté terminado, los protocolos DECnet podrían ínter-operar con cualquier nodo de red compatible con OSI.

DES (Data Encryption Standar)

Un popular método de llave asimétrica de encriptación desarrollada en 1975 y estandarizada por la ANSI en 1981 como ANSI X.3.92 DES usa una llave de 56 bits y un método de bloque cifrado el cual descompone el texto en bloques de 64 bits y luego los encripta.

DNS (Domain Name System)

Consiste en una base de datos que relaciona la dirección IP de cada máquina conectada a Internet con su nombre. La dirección IP consiste en cuatro números separados por puntos. No puede haber dos ordenadores con la misma dirección, pues podrían aparecer conflictos y estos no se podrían comunicar. Los nombres están formados por palabras separadas por puntos. La parte final del nombre es el dominio al cual está conectador el ordenador

FIREWALL

Un firewall es un dispositivo que funciona como cortafuegos entre redes, permitiendo o denegando las transmisiones de una red a la otra. Un uso típico es situarlo entre una red local y la red Internet, como dispositivo de seguridad para evitar que los intrusos puedan acceder a información confidencial. Es simplemente un filtro que controla todas las comunicaciones que pasan de una red a la otra y en función de lo que sean permite o deniega su paso. Para permitir o denegar una

comunicación el firewall examina el tipo de servicio al que corresponde, como pueden ser el web, el correo o el IRC. Dependiendo del servicio el firewall decide si lo permite o no. Además, el firewall examina si la comunicación es entrante o saliente y dependiendo de su dirección puede permitirla o no. Un firewall puede ser un dispositivo software o hardware.

FRAME RELAY

Frame Relay es un protocolo lógico de acceso a una red de transmisión de datos, siguiendo normas y recomendaciones internacionales (ITU-T (la antigua CCITT), FR Vendor Forum, ANSI, etc.). De esta manera, al acceder a una red de datos, se puede 'llegar' hasta donde alcance esa red de datos. Por extensión, se denomina acceso FR a la línea digital que une al proveedor con el carrier, es decir, la línea desde el domicilio del proveedor hasta el nodo más cercano del carrier. En las líneas digitales antiguas, la tasa de error era elevada. Por eso se diseñaron protocolos que detectaran el error y pidieran el reenvío de los datos perdidos, o que frenaran al emisor si el receptor no estaba disponible. El protocolo típico del que se habla en este entorno es X.25, que permite corrección de errores, control de flujo, etc. A cambio, incrementa la sobrecarga de los datos. Eso reduce el ancho de banda real de una línea.

GATEWAY

Un gateway es una puerta de enlace entre dos redes distintas. Esto significa que se usa como puente, también tiene este significado, entre una red local, LAN, y una extensa, WAN. El significado más empleado actualmente es para designar al dispositivo hardware software o, más usualmente, una combinación de ambos, que controla el tráfico entre Internet y el ordenador o la red local de ordenadores de una empresa. El dispositivo gateway normalmente está asociado a elementos como routers y switches, que son los que realmente hacen la conexión física con la red. El elemento gateway de una red normalmente actúa también como servidor proxy y firewall

HTTP (HyperText Transfer Protocol)

Es el método utilizado para transferir ficheros hipertexto por Internet. En el World Wide Web, las páginas escritas en HTML utilizan el hipertexto para enlazar con

otros documentos. Al pulsar en un hipertexto, se salta a otra página Web, fichero de sonido, o imagen. La transferencia hipertexto es simplemente la transferencia de ficheros hipertexto de un ordenador a otro. El protocolo de transferencia hipertexto es el conjunto de reglas utilizadas por los ordenadores para transferir ficheros hipertexto, páginas Web, por Internet.

IPX (Protocolo de intercambio de Paquetes entre Redes)

Protocolo de comunicaciones NetWare que se utiliza para encaminar mensajes de un nodo a otro. Los paquetes IPX incluyen direcciones de redes y pueden enviarse de una red a otra. Ocasionalmente, un paquete IPX puede perderse cuando cruza redes, de esta manera el IPX no garantiza la entrega de un mensaje completo. La aplicación tiene que proveer ese control o debe utilizarse el protocolo SPX de NetWare. IPX provee servicios en estratos 3 y 4 del modelo OSI (capas de red y transporte).

ISP (Inernet Service Provider)

Compañía que provee acceso a Internet. El proveedor de servicios entrega un paquete de software, nombre de usuario, password y u número de acceso telefónico.

LDAP (Lightweight Directory Access Protocol)

"Protocolo de Acceso Ligero a Directorio" es una serie de protocolos para acceder a directorios de información, este protocolo de acceso a un directorio desciende de DAP, este último accedía a un directorio pero siempre sobre la pila OSI (X.500) de modo que resultaba mas lenta y perdía eficiencia. LDAP surge en 1993 en la Universidad de Michigan LDAP define una serie de operaciones para la consulta del protocolo y, el método de hacer y obtener los datos de estas consultas o actualizaciones por red. LDAP por su parte soporta autenticación con la librería SASL y el protocolo SSL (Secure Socket Layer) en su versión LDAPv3 de modo que se garantiza la seguridad del tráfico de red.

MD5

Un algoritmo creado en 1991 por el profesor Ronald Rivest que es usado para crear firmas digitales. Es proyectado para maquinas de 32 bits y es más seguro que el algoritmo MD4. MD5 toma un mensaje y lo convierte en una cadena ordenada de dígitos, también llamado un mensaje digerido.

NetBEUI (NetBios Extended User Interfac)

Es una versión mejorada del protocolo NetBIOS usado por sistemas operativos de redes tales como LAN Manager, LAN Server, Windows 95 y Windows NT. Fue diseñado originalmente por IBM para sus LAN manager servers y luego extendida por Microsoft y Novell.

NetBIOS (Network Basic Input Output system)

NetBIOS, una capa de software desarrollado para enlazar un sistema operativo de red con hardware específico, fue originalmente diseñado como el controlador de red para las redes LAN de IBM. Hoy en día, NetBIOS ha sido extendido para permitir a los programas que han sido escritos usando dicho interfaz poder trabajar con la arquitectura Token Ring de IBM. Ha sido adoptado como un estándar mundial y hoy en día es común escuchar que una red local es compatible NetBIOS.

NETWARE

Un sistema operativo de redes de área local desarrollado por la corporación Novell. Es un producto software que corre sobre diferentes tipos de LAN's, desde Ethernet hasta redes IBm token ring. Esto provee a los usuarios y programadores una interfaz consistente que es independiente de el hardware actual usado para transmitir mensajes.

OSPF (Open Shortest Path First)

Es un protocolo de encaminamiento, o enrutamiento, que abre primero el camino más corto a la hora de enviar paquetes. Desarrollado para redes IP, esta basado

en el primer camino más corto o algoritmo de estado de enlace. La ventaja de este algoritmo es que se actualizan rápidamente las tablas de enrutamiento, previniendo problemas tales como ciclos (loops). Su desventaja es su gran requerimiento de memoria y capacidad de procesamiento.

PROXY

El proxy es un servidor que actúa como un caché. Los usuarios que se conecten al proxy, le pedirán las páginas Web o los ficheros que deseen y él se encargará de enviarlos al navegador. El servidor proxy guarda las páginas, así que una página que ya haya sido visitada por cualquier persona, el nuevo usuario que la solicite la cojera de este servidor, no de la Red. Con esto se mejora la velocidad y se evitan posibles colapsos en servidores remotos.

RIP (Routing information Protocol)

Un protocolo de enrutamiento utilizado para intercambiar información entre los routers definido por el RFC 1058 que especifica como los routers intercambian tablas de enrutamiento. Con RIP, los routers intercambian periódicamente tablas enteras. Como esto es ineficiente, RIP ha sido remplazado gradualmente por OSPF.

SNA (Systems Network Architecture)

Conjunto de protocolos de red desarrollado por IBM. Diseñado originalmente en 1974 para las computadoras mainframe de IBM, con el transcurso de los años SNA ha evolucionado y ahora también soporta redes de estación de trabajo par a par.

SPOOFING

Técnica usada para ahorrar ancho de banda en redes WAN, mediante la cual, los dispositivos tales como bridges y routers, responden a pedidos de actualización de enrutamiento destinados a dispositivos remotos enviados por dispositivos LAN. Esto engaña (spoof) al dispositivo LAN y lo hace pensar que la LAN remota sigue

conectada, aunque no lo está. El spoofing ahorra ancho de banda de WAN debido a que nunca se envía ningún paquete a la WAN.

SSH Secure Shell

Desarrollado por SSH Communications security Ltd., es un programa que permite ingresar a otro equipo en la red, esto para ejecutar comandos en un equipo remoto y mover archivos de una máquina a la otra. Este provee una fuerte autentificación y comunicación segura sobre canales inseguros.

TCP (Transmission Control Protocol)

El protocolo de control de transmisión (TCP) pertenece al nivel de transporte, siendo el encargado de dividir el mensaje original en datagramas de menor tamaño, y por lo tanto, mucho más manejables. Los datagramas serán dirigidos a través del protocolo IP de forma individual. El protocolo TCP se encarga además de añadir cierta información necesaria a cada uno de los datagramas. Esta información se añade al inicio de los datos que componen el datagrama en forma de cabecera.

TRIPLE DES

También referenciado como 3DES, un modo del algoritmo de encriptación DES que encripta los datos tres veces. Las tres llaves de 64 bits son usados, en vez de una, por una llave general de 192 bits de longitud(la primera encriptación es encriptada con la segunda llave, y el resultante texto cifrado es nuevamente encriptado con una tercera llave).

TURNKEY

Se refiere a un sistema o paquete de software que ha sido construido, instalado o suministrado por el fabricante complete y listo para operar. En la industria informática es usado para promover un sistema que puede ser rapidamente istalado y operar tan pronto “sale de la caja”.

UDP (User Datagram Protocol)

El protocolo de datagramas de usuario (UDP) puede ser la alternativa al TCP en algunos casos en los que no sea necesario el gran nivel de complejidad proporcionado por el TCP. Puesto que UDP no admite numeración de los datagramas, éste protocolo se utiliza principalmente cuando el orden en que se reciben los mismos no es un factor fundamental, o también cuando se quiere enviar información de poco tamaño que cabe en un único datagrama.

ACRONIMOS

3DES: 3 Data Encryption Standard

AES: Advanced Encryption Standard

AH: Authentication Header

ATM: Asynchronous Transfer Mode

B2B: Business to Business

CA: Certificate Authority (autoridad de Certificación)

CHAP: Challenge Handshake Protocol

CPD: Centro de Proceso de Datos

CRL: Lista de Certificados Revocados

DES: Data Encryption Standard

DNS: Domain Name Service

EAP: Extensible Authentication Protocol

ESP: Encapsulating Security Payload

FR: Frame Relay

GRE: Generic Routing Encapsulation

HGW: Home Gateway

HMAC: Hashed MAC

HTTP: Hyper Text Transfer Protocol

IANA: Internet Assigned Number Authority. En 1999 sustituida por ICANN

ICMP: Internet Control Message Protocol

IDEA: International Data Encryption Algorithm

IETF: Internet Engineering Task Force

IKE: Internet Key Exchange:

IPSec: IP Security

IPX: Internet Packet Exchange

ISAKMP: Internet Security Association and Key Management Protocol

ISP: Internet Service Provider

L2F: Layer 2 Forwarding

L2TP: Layer 2 Tunnelling Protocol

LAC: L2TP Access Concentrator

LAN: Local Area Network

LDAP: Lightweight Directory Access Protocol

LNS: L2TP Network Server

MAC: Message Authentication Code

MD4: Message Digest 4

MD5: Message Digest 5

MSCHAP: Micro Soft Challenge Handshake Protocol

MS-CHAPv2: Micro Soft Challenge Handshake Protocol version 2

NAS: Network Access Server

NetBEUI: Network BIOS Enhanced User Interface

NIC: Network Interface Connector

Oakley: Oakley Key Determination protocol

OSPF: Open Shortest Match First

PAC: PPTP Access Concentrator

PAP: Password Authentication Protocol

PKCS: Public Key Common Standard

PKI: Public Key Infrastructure (Infraestructura de Clave Pública)

PNS: PPTP Network Server

PPP: Point-to-Point Protocol

PPTP: Point-to-Point Tunnelling Protocol

RAS: Remote Access Service

RDSI: Red Digital de Servicios Integrados

RFC: Request For Comments

RIPv2: Routing Information Protocol

RPV: Red Privada Virtual

RSA: Riverst Shamir Adleman

SA: Security Association (Asociación de Seguridad)

SCEP: Simple Certificate Enrollment Protocol

SHA-1: Secure Hash Algorithm

SNA: System Network Architecture

SSH: Secure Shell Protocol

TCP/IP: Transfer Control Protocol/Internet Protocol

ToS: Type of Service

TTL: Time to Live

UDP: User Datagram Protocol

VPDN: Virtual Private Dynamic Network

VPN: Virtual Private Network

WAN: Wide Area Network

XDSL: Digital Subscriber Line

CAPITULO 1

INTRODUCCION

1.1 DESCRIPCIÓN DEL PROBLEMA

El éxito de Internet está modificando la forma de actuar de las empresas a la hora de implementar la interconexión de redes privadas de datos. Actualmente, estas redes privadas y la infraestructura de Internet están operando en paralelo. Sin embargo, todas las ventajas y beneficios ofrecidos a los proveedores de servicio y a los usuarios finales, está provocando que estos *"universos paralelos"* converjan en el concepto de red privada virtual (VPN). Esta convergencia es debida principalmente a cuatro motivos:

1. La movilidad geográfica de puestos de trabajo está llevando a las redes privadas a una situación ingestionable. Los usuarios precisan conexiones que les permitan el acceso desde cualquier lugar del mundo. Estas necesidades, surgidas como consecuencia de la demanda de telecomunicaciones a tiempo completo, están aumentando drásticamente el número de *"oficinas remotas"* que una compañía debe interconectar. Como resultado, muchas redes privadas están convirtiéndose en redes ingestionables e intratables.

2. La necesidad de interactuar de forma on-line con los clientes y los proveedores está añadiendo un nuevo nivel de complejidad, en el cual muchas redes privadas deben tratarse de una manera independiente para su correcta integración y aislamiento respecto al resto. Las redes individuales emplean normalmente diferentes protocolos, diferentes aplicaciones, diferentes portadoras y diferentes sistemas de gestión de red.

Esta escasez de denominadores comunes supone que la interacción de dos redes privadas se convierta en un reto aún mucho mayor.

3. El deseo de consolidar y simplificar la interfaz de usuario se ha convertido en un imperativo de negocio, dado que los usuarios son incapaces de defenderse en muchas de las nuevas aplicaciones.

4. El alto coste necesario para implementar y mantener redes privadas está llevando a éstas a una situación insostenible. Las líneas de larga distancia, así como los servicios conmutados, representan una serie de necesidades diarias. El personal de soporte necesario para gestionar las tecnologías complejas conlleva un crecimiento continuo tanto en el número de personas como en su experiencia. Igualmente, la dependencia de aplicaciones de red requiere un aprovisionamiento separado de backup además de una expansión de la infraestructura de la red privada ya existente.

Estos motivos que generaron la necesidad de implementar VPNs también impulsaron la creación de protocolos de conexión punto a punto como el GRE, y posteriormente el PPP. Aunque cumplían su función, la seguridad que estos protocolos ofrecían dejaba mucho que desear, y es este a menudo, el primer objetivo perseguido por las organizaciones dado que Internet es considerada una red "demasiado pública" para realizar comunicaciones privadas. Sin embargo y aplicando las correspondientes medidas de protección y seguridad, Internet puede convertirse en una red altamente privada y segura. Para poder alcanzar este punto, toda red privada virtual debe cumplir principalmente tres objetivos de seguridad:

- *Proporcionar la seguridad adecuada:* Un sistema mínimo de seguridad debe, al menos, validar a los usuarios mediante passwords con el fin de proteger los recursos de accesos no autorizados. Además, la inclusión de métodos de encriptación permitirá la protección del tráfico a lo largo de su tránsito.
- *Proporcionar facilidad de administración:* La elección de seguridad para la VPN debe ser sencilla de administrar, así como las funciones de administración deben ser seguras frente a posibles accesos ilegales.
- *Transparencia hacia los usuarios:* El sistema de seguridad en el acceso a la red privada virtual debe ser totalmente transparente a los usuarios.

Estos son únicamente los aspectos de seguridad mínimos con los que debe contar una VPN. Por eso con el pasar del tiempo los protocolos que únicamente cumplían con estas características comenzaron a ser reemplazados por otros protocolos que ofrecían conexiones mas seguras. Entre estos protocolos se destacó uno en particular , el PPTP, que es una versión mejorada de PPP creada por Microsoft y que incorporó en sus sistemas operativos, con lo que ganó gran popularidad a pesar de las grandes fallas de seguridad que tiene.

Posteriormente mientras PPTP se hacía un nombre en el mercado, Cisco trabajaba en un nuevo protocolo que finalmente se conoció como L2F, mucho mejor que PPTP debido a que incorporaba nuevos métodos de autenticación y algoritmos de encriptación más avanzados.

No pasó mucho tiempo antes de que la seguridad que ofrecía este nuevo protocolo fuera insuficiente ante la presencia de nuevos métodos de hackeo. Como respuesta a este nuevo problema, Microsoft y Cisco decidieron unir las

mejores características de sus protocolos de tunelaje y crear un nuevo protocolo capaz de garantizar no solo la confidencialidad de la información sino también la integridad de la misma.

Todos estos protocolos mencionados son basados en soluciones propietarias que dificultan la comunicación entre los distintos entornos empresariales, al ser necesario que éstos dispongan de una misma plataforma. En la actualidad La falta de interoperabilidad ha sido el principal freno para el establecimiento de comunicaciones seguras, dado que no se ve factible la migración a una determinada plataforma en función de una colaboración empresarial puntual.

Como respuesta a este problema, surge IPSec. Este protocolo esta apoyado en estándares del IETF y proporciona un nivel de seguridad común y homogéneo para todas las aplicaciones, además de ser independiente de la tecnología física empleada. IPSec se integra en la versión actual de IP (IP versión 4) y, lo que es todavía más importante, se incluye por defecto en IPv6.

Puesto que la seguridad es un requisito indispensable para el desarrollo de las redes IP, IPSec está recibiendo un apoyo considerable, todos los equipos de comunicaciones lo incorporan, así como las últimas versiones de los sistemas operativos más comunes. Al mismo tiempo, ya existen muchas experiencias que demuestran la interoperabilidad entre fabricantes, lo cual constituye una garantía para los usuarios. Otra característica destacable de IPSec es su carácter de estándar abierto. Complementado perfectamente con la tecnología PKI y, aunque establece ciertos algoritmos comunes, por razones de interoperabilidad, permite integrar algoritmos criptográficos más robustos que pueden ser diseñados en un futuro.

1.2 OBJETIVOS

1.2.1 Objetivo General:

- Estudiar los diferentes protocolos de acceso remoto y tunelaje, y los servicios de seguridad ofrecidos por estos, para comprender porque el estándar IPSec es la solución mas completa cuando se requiere comunicar dos redes privadas a través de una red publica como la Internet.

1.2.2 Objetivos Específicos:

- Diferenciar los diferentes tipos de redes privadas virtuales.

- Investigar la arquitectura de los protocolos de tunelaje para redes privadas virtuales y los niveles de seguridad que ofrece cada uno de ellos..

- Analizar elementos de seguridad en redes como lo son confidencialidad, autenticación e integridad de los datos, control de acceso y no repudio.

- Estudiar el estándar IPSec y mencionar los diferentes escenarios en los que este es una solución viable a los diferentes problemas de seguridad.

1.3 JUSTIFICACIÓN

Las Redes privadas virtuales cada vez son más populares en todo el mundo debido a la disponibilidad e interoperatividad que éstas ofrecen a los usuarios que las comparten. Sin embargo, popularidad no es sinónimo de seguridad, por lo que muchas veces, la falta de conocimiento sobre las características de los protocolos encargados del transporte de la información entre las redes, pueden llevarnos a seleccionar protocolos ineficientes que comprometan la integridad de los datos que viajan a través de la red pública.

Hace algunos años todavía no era tan importante conectar usuarios a Internet por motivos de trabajo, pero a medida que ha pasado el tiempo las compañías han querido que las redes LAN trasciendan más allá del ámbito de la oficina e incluyeran a los trabajadores y centros de información de otros edificios, ciudades, estados o incluso otros países, y tenían que invertir en hardware y servicios de telecomunicaciones costosos para crear redes amplias de servicio, WAN. Sin embargo ya con Internet, las compañías tienen la posibilidad de crear una red privada virtual que demanda una inversión relativamente pequeña de hardware y utiliza Internet global para la conexión entre los puntos de la red.

Durante un tiempo, las grandes corporaciones habían solucionado el problema mediante sistemas de comunicación como líneas punto a punto y sofisticadas instalaciones de interconexión. Aunque efectivas, estas soluciones quedaban fuera del alcance de organizaciones de menor tamaño y con recursos económicos y técnicos más escasos.

Las redes tipo LAN (Local Area Network) permiten conectar entre si varios ordenadores en una misma oficina. Con la aparición de las nuevas tecnologías hoy en día es posible conectar esta red LAN (uno o más ordenadores) a Internet. Esta conexión puede ser de varias maneras:

- Unidireccional: conexión a Internet desde la red LAN para consulta de información.
- Bidireccional: el acceso es en ambas direcciones, desde la LAN hacia Internet o bien desde Internet hacia la LAN.

Las LAN tradicionales son redes esencialmente restringidas, por lo cual se puede intercambiar información entre las computadoras sin pensar en la seguridad de la información; pero Internet no es seguro, por lo tanto las VPN usan protocolos especiales que permiten encriptar información y permitr únicamente a la persona autorizada desencriptar esa información con un identificador que comprueba que la transmisión se ha hecho desde una fuente confiable.

Para poder comprender cual o cuales protocolos de tunelaje ofrecen los mejores niveles de seguridad, es necesario estudiar sus características, conocer su arquitectura, analizar como enfrentan los problemas de confidencialidad, autenticación e integridad de datos, el control de acceso y el no repudio.

CAPITULO 2

VPN

2.1 GENERALIDADES SOBRE REDES PRIVADAS VIRTUALES

2.1.1 Definición Red Privada Virtual

Una Red Privada Virtual (**VPN**) es una forma de compartir y transmitir información entre un círculo cerrado de usuarios que están situados en diferentes localizaciones geográficas. La tecnología de VPN proporciona un medio para usar el canal público de Internet como un canal apropiado para comunicar los datos privados. Con la tecnología de encriptación y encapsulamiento, una VPN básica, crea un pasillo privado a través de Internet.

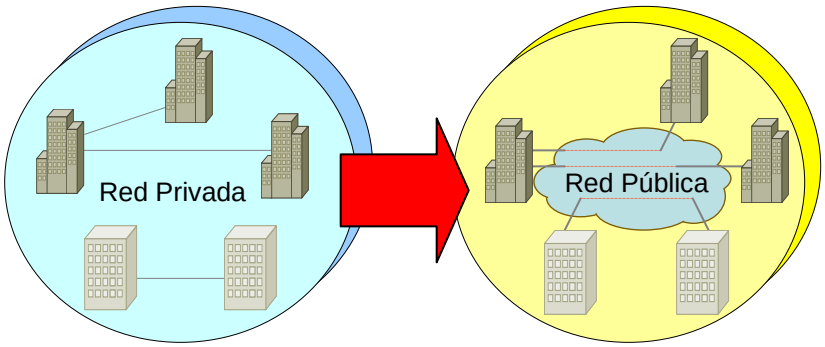


Figura 2.1 Comparación entre un red privada común y una red privada interconectada a través de una red pública.

Una Red Privada Virtual es una red privada que se extiende, mediante un proceso de encapsulación, y en su caso, de encriptación, de los paquetes de datos a distintos puntos remotos mediante el uso de infraestructuras públicas de transporte. Los paquetes de datos de la red privada viajan por medio de un túnel definido en la red pública. En el caso de acceso remoto, la VPN permite al usuario acceder a su red corporativa, asignándole a su ordenador remoto las direcciones y

privilegios de la misma, aunque la conexión la haya realizado por medio de un acceso a Internet público.

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 y 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 para los túneles individuales se pueden negociar 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. La disponibilidad de esta 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 red utilizando VPN podrá ser tan segura como la red interna. La privacidad se presenta cuando un túnel aparece como un enlace privado.

VPN consiste en dos máquinas (una en cada "extremo" de la conexión) y una ruta o "túnel" que se crea dinámicamente en una red pública o privada. Para asegurar la privacidad de esta conexión los datos transmitidos entre ambos ordenadores son encriptados por el Point-to-Point Protocol (PPP[1]), un protocolo de acceso remoto, y posteriormente enrutados o encaminados sobre una conexión previa (también remota, LAN o WAN) por un dispositivo PPTP[2].

Una Red Privada Virtual es una forma de compartir y transmitir información entre un círculo cerrado de usuarios que están situados en diferentes localizaciones

---

[1] Para ampliar información acerca de este protocolo referirse al RFC 1661

[2] Point to Point Tunneling Protocol

geográficas. Es una red de datos de gran seguridad utilizando Internet como medio de transmisión. Aunque Internet es una red pública y abierta, la transmisión de los datos se realiza a través de la creación de túneles virtuales, asegurando la confidencialidad e integridad de los datos transmitidos.

Así, las VPNs constituyen una estupenda combinación entre la seguridad y garantía que ofrecen las costosas redes privadas y el gran alcance, lo asequible y escalable del acceso a través de Internet. Esta combinación hace de las Redes Privadas Virtuales o VPNs una infraestructura confiable y de bajo costo que satisface las necesidades de comunicación de cualquier organización.

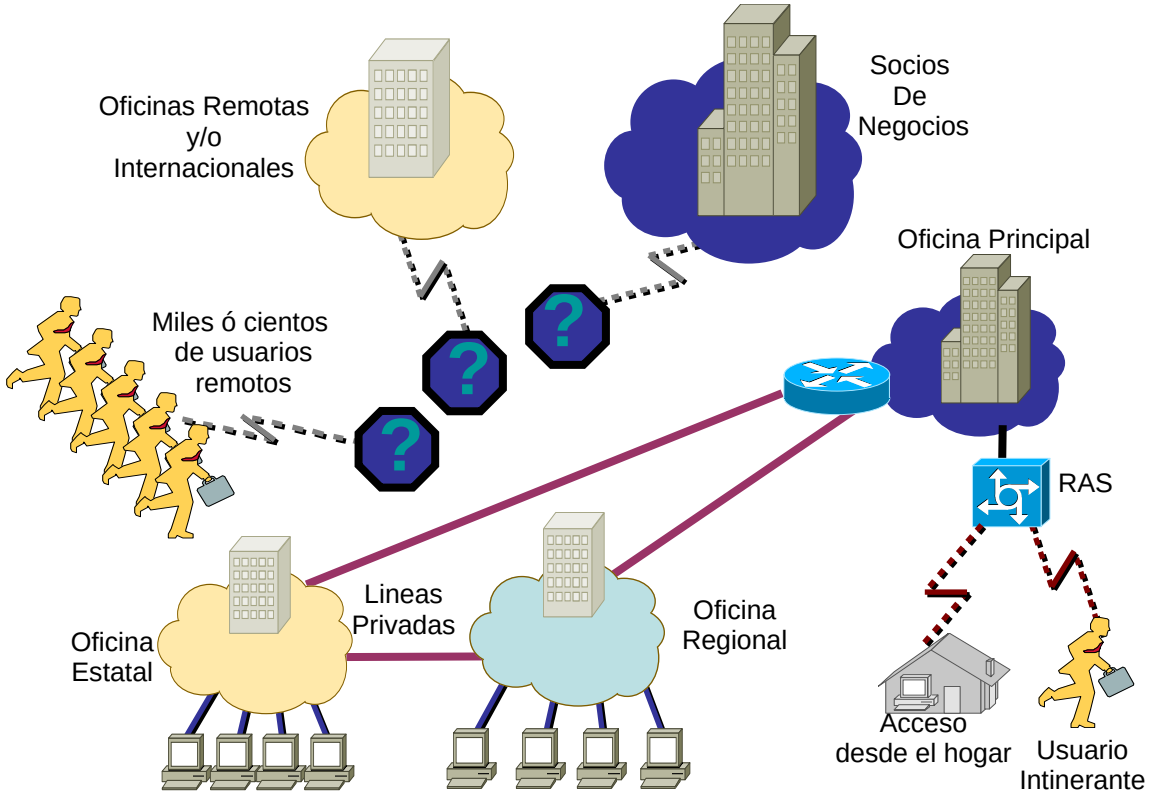


Figura 2.2 Podemos ver una red WAN conectada a través de Líneas Privadas y usuarios RAS a la que nuevos socios y oficinas quieren conectarse sin la necesidad de invertir en líneas privadas. Para ellos la solución mas fiable es la vinculación a la WAN conformando VPNs.

Las VPNs permiten:

- La administración y ampliación de la red corporativa al mejor costo-beneficio.
- La facilidad y seguridad para los usuarios remotos de conectarse a las redes corporativas.

Los requisitos indispensables para esta interconectividad son:

- Políticas de Seguridad.
- Requerimiento de aplicaciones en tiempo real.
- Compartir datos, aplicaciones y recursos.
- Servidor de Acceso y Autenticación.
- Aplicación de Autenticación.

2.2 Características de las Redes Privadas Virtuales

Características que deben garantizar todas las VPN:

- **2.2.1 Confidencialidad**:

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

- **2.2.2 Integridad**:

  Asegura que los datos de origen corresponden a los de destino.

- **2.2.3 Autentificación**:

  Asegura que quien solicita la información exista.

- **2.2.4 Control de acceso**:

  Restringe el acceso a usuarios no autorizados que quieran infiltrarse en la red.

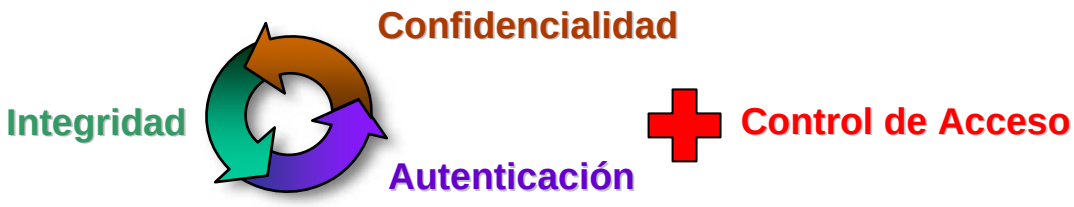


Figura 2.3 Características de seguridad que debe poseer una VPN.

Estas características son ofrecidas gracias a tecnologías y protocolos de seguridad y encriptación que proporcionan seguridad en la transmisión de los datos independientemente de las redes involucradas y de sus medidas de seguridad:

- La privacidad de los datos debe ser garantizada mediante la encriptación de los mismos. La encriptación usa complejas transformaciones matemáticas en la cual los datos se combinan con una llave lógica y luego son desencriptados por la persona que lo recibe usando la misma clave. Administrar estas claves es el aspecto más crucial para la encriptación, cualquier solución de VPDN deberá poseer un mecanismo de negociación de llaves dinámicas.

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

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

2.3 Tipos de Redes Privadas Virtuales

En general existen dos tipos de redes privadas virtuales:

- **2.3.1 Enlaces Cliente-Red**:

  En estos enlaces se encapsula, típicamente, PPP (Point-to-Point Protocol). Las tramas del cliente se encapsulan en PPP, y el PPP resultante se encapsula para crear el VPN. Se emplean, entre otras muchas cosas, para:

  - Acceso seguro de un cliente a la red.
  - Clientes móviles (para independizarlos de la topología física).
  - Puntos de acceso remoto. Por ejemplo, un "pool" de módems en otra ciudad, o clientes nuestros entrando por otro ISP.
  - Enrutado de tramas no utilizables en Internet. Por ejemplo, tramas NetBEUI[3], IPX[4], SNA[5] o DECNET[6].

- **2.3.2 Enlaces Red-Red**:

  En estos casos se está encapsulando el tráfico de una red local, por lo que nos ahorramos el paso PPP anterior. Las tramas de la LAN se encapsulan directamente para crear el VPN. Se utiliza para:

  - Fundir dos redes locales a través de Internet, para que parezcan una sola.

---

[3] NetBEUI
[4] IPX
[5] SNA
[6] DecNet

- Establecer canales con privacidad, autenticidad y control de integridad, entre dos redes independientes.
- Rutado de tramas no utilizables en Internet. Por ejemplo, tramas NetBEUI, IPX, SNA o DECNET.

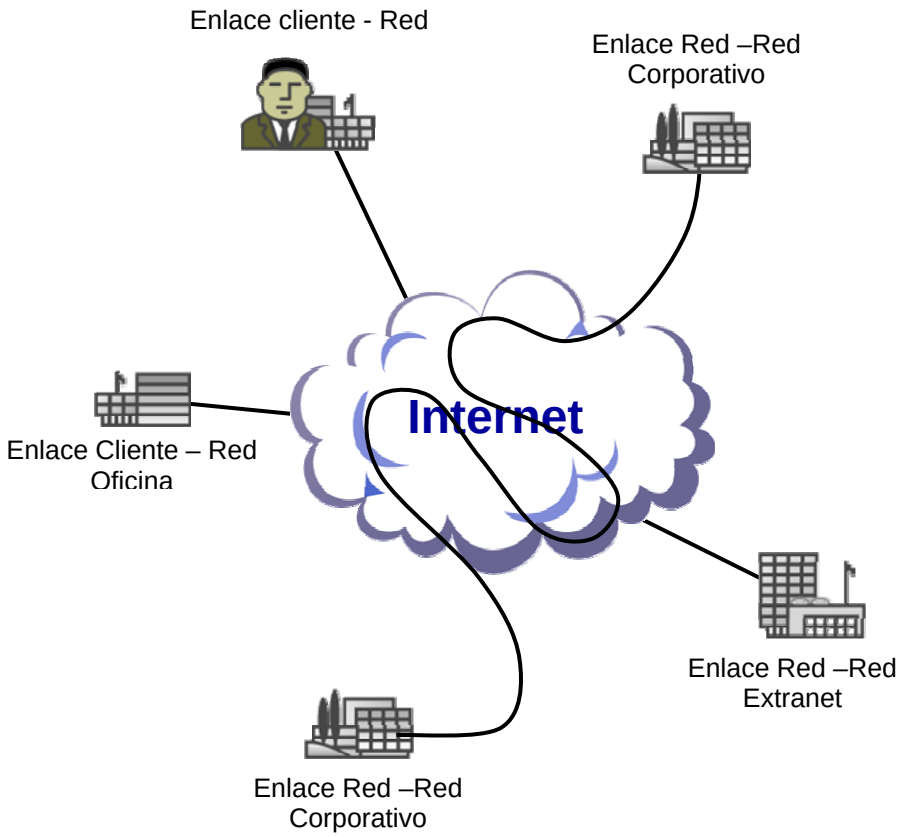


Figura 2.4 En la gráfica se muestran ejemplos de tipos de enlace cliente – red, como lo es un enlace de una oficina de una única oficina el de un usuario por acceso remoto. Además vemos dos ejemplos de enlaces red – red, uno es un enlace de la red de una corporación con otra y otro es la conexión de una extranet que puede ser accesada por las diferentes redes que conformen una VPN con esta.

2.4 Ventajas de las Redes Privadas Virtuales

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

- Reducen los costos frente a otras soluciones de conectividad como arriendo de líneas dedicadas u otros. Las VPN tienen un funcionamiento similar al de las redes tipo WAN pero su coste es muchísimo inferior ya que utiliza la red de Internet para comunicarse entre si, permitiendo de esta manera tener comunicaciones rápidas y seguras entre sus oficinas o desde cualquier lugar exterior de ellas.

  La conexión WAN es posiblemente la solución más estable y segura para una red de cualquier tamaño. Las conexiones son totalmente privadas y usan tecnología estándar. La solidez de una VPN no es estable. Las redes privadas virtuales son una nueva tecnología, ejecutándose sobre una tecnología poco fiable (Internet). Realizando transacciones a través de Internet, comunicaciones entre varias plataformas, procesos de encriptación y similares se consigue un sistema menos fiable que en el caso de una

conexión WAN. Sin embargo, el mundo se mueve más hacia una sociedad interconectada y como van apareciendo nuevos estándares reales (protocolos, hardware, etc.), VPNs tendrán una base estable sobre la que operar.

- No requiere de grandes inversiones en infraestructura. Los enlaces punto a punto implican que la organización debe realizar una cuantiosa inversión inicial en equipamiento para conectar cada una de las sucursales u oficina que posea. Sin embargo, con las VPN tanto la inversión inicial como las tareas de instalación, operación y mantenimiento son mucho más pequeñas.

  Las diferencias reales entre las VPN y las WAN aparecen cuando se considera la escalabilidad de ambas. Una gran WAN requiere una gran inversión en equipamiento especialmente cuando se añaden múltiples redes a lo largo de la zona de actuación de la organización. Con VPN, inicialmente solo se necesita una red central que sólo necesitaría una actualización del ancho de banda aunque se aceptaran conexiones desde múltiples redes.

- Proporciona seguridad e integridad en la transmisión de datos.

2.5 Inconvenientes de las Redes Privadas Virtuales

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

- También se produce una mayor complejidad en el tráfico de datos que puede producir efectos no deseados al cambiar la numeración asignada al cliente VPN y que puede requerir cambios en las configuraciones de aplicaciones o programas (proxy, servidor de correo, permisos basados en nombre o número IP).
- La fiabilidad es menor que en una línea dedicada.
- Se pueden producir ataques por denegación de servicio.
- Es delicada y laboriosa la gestión de claves de acceso y autenticación.

Se recomienda usar el servicio de VPN en aquellos casos en que, teniendo una conexión a un proveedor de acceso a Internet ajeno a la organización, se quiera disponer de un servicio sólo autorizado a los ordenadores de la organización o una salida a Internet que sea más conveniente usando las líneas de salida de la organización.

2.6 VPN y Firewalls

A pesar de que los firewalls deberían ser considerados parte de la solución corporativa de seguridad, no son suficientes por sí mismos para crear una VPN. Esto es debido a que un firewall no puede monitorizar o prevenir los cambios de datos que ocurren en un paquete a través de Internet (integridad de datos).

Además, incluso si se instala encriptación basada en host en todos los ordenadores (usando IPSec, por ejemplo), también son necesarios firewalls en la organización. Los firewalls en Internet refuerzan la política de seguridad de la red de la empresa y son parte de un perímetro de defensa. IPSec en cada escritorio provee de privacidad y autenticación pero no asegura que la política de seguridad esté reforzada.

Los firewalls son considerados, a menudo, para ser puntos de terminación VPN (figura 2.5) porque pueden administrar la política de seguridad de la red completa a través de un solo punto. Sin embargo, los firewalls son dispositivos complejos de instalar y gestionar debido a la posibilidad de conflicto entre reglas si no se tiene cuidado al establecer o modificar las reglas base. Adicionalmente, tener firewalls desempeñando servicios VPN incrementa el riesgo en caso de que el firewall falle o se vea comprometido.

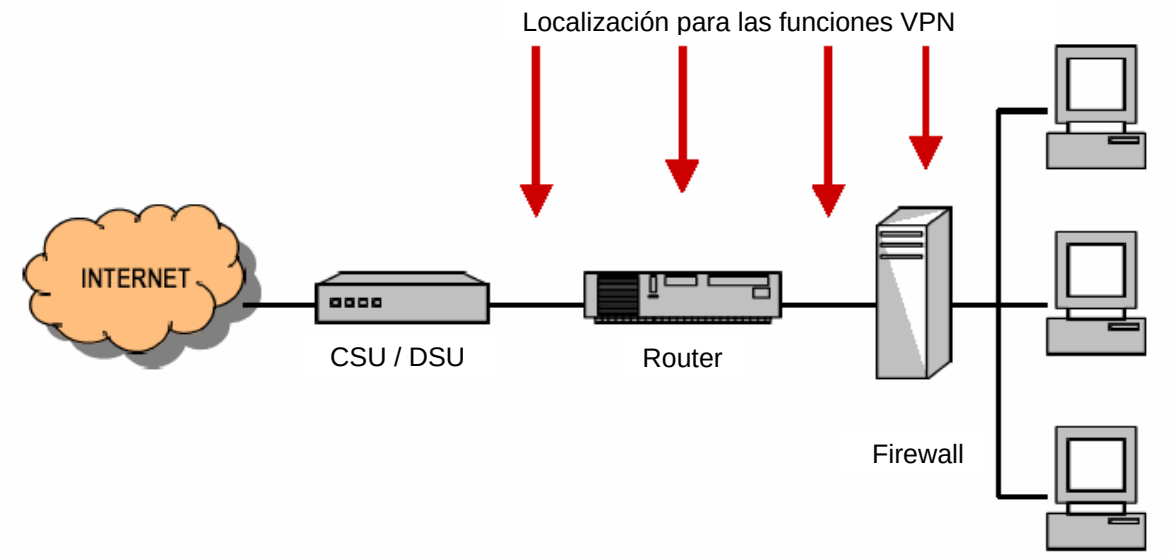


Figura 2.5 Utilización de un Firewall como punto de terminación VPN.

2.6.1 Características

Sin tener en cuenta que protocolo es usado para la VPN, es necesario considerar cómo el firewall se integra con el resto de sistemas de administración de seguridad y red. Si ya se está usando un sistema particular para la autenticación de usuarios remotos, entonces se puede simplificar la transición mediante la instalación de un firewall que sea compatible con el sistema actual.

Si se planea usar un sistema de autenticación basado en certificados digitales, entonces de debe pensar en cómo se distribuirán y verificarán los certificados.

Es muy probable que los firewalls sean instalados en más de un sitio. Si el firewall soporta administración sincronizada de sitios, será más capaz de mantener una política de seguridad más consistente. Esta administración puede involucrar intercambio de ficheros, o algunas otras formas de gestión remota. Si las

capacidades de administración están incluidas en el producto, se asegura que el acceso remoto al firewall es seguro.

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

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

2.7 VPN Hardware

Uno de los mercados de mayor crecimiento para proveer soluciones VPN consiste en ofrecer soluciones VPN integradas en el hardware, las cuales en una única caja (figura 2.6) incluye toda la funcionalidad requerida para VPN, eliminando la necesidad de añadir software y hardware a un firewall existente o un router y, en la mayoría de los casos, cualquier hardware para la conexión WAN.

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

No todos los productos ofrecen las mismas características. Algunos productos están dirigidos a proveer una solución “turnkey” para la seguridad, incluyendo un firewall. Otras soluciones VPN hardware abarcan desde cajas centradas en la encriptación hasta sistemas que sostienen todos los aspectos de una conexión a Internet, incluyendo conexiones WAN, routing, VPNs, DNS, y servicios e-mail, entre otros.

Integrar varias funciones en un producto simple puede ser particularmente atractivo para los negocios que no tienen los recursos necesarios para instalar y mantener diferentes servicios de red y que tampoco quieren fuentes externas para sus operaciones VPN. Incluso, puede resultar algo muy positivo, debido a que esta caja pasa a ser ahora el único punto de fallo. Esta acepta que todas las funciones de seguridad controlando las comunicaciones con Internet pueden fallar cuando un único servicio se cae; pero al menos, un enlace de comunicación roto no significa que los atacantes pueden entrar en la Intranet a través de ese enlace. Sin embargo, es completamente diferente poner un servidor de e-mail o un servidor Web en la misma caja, ya que si esta falla, entonces los empleados pueden perder algunos servicios internos también.

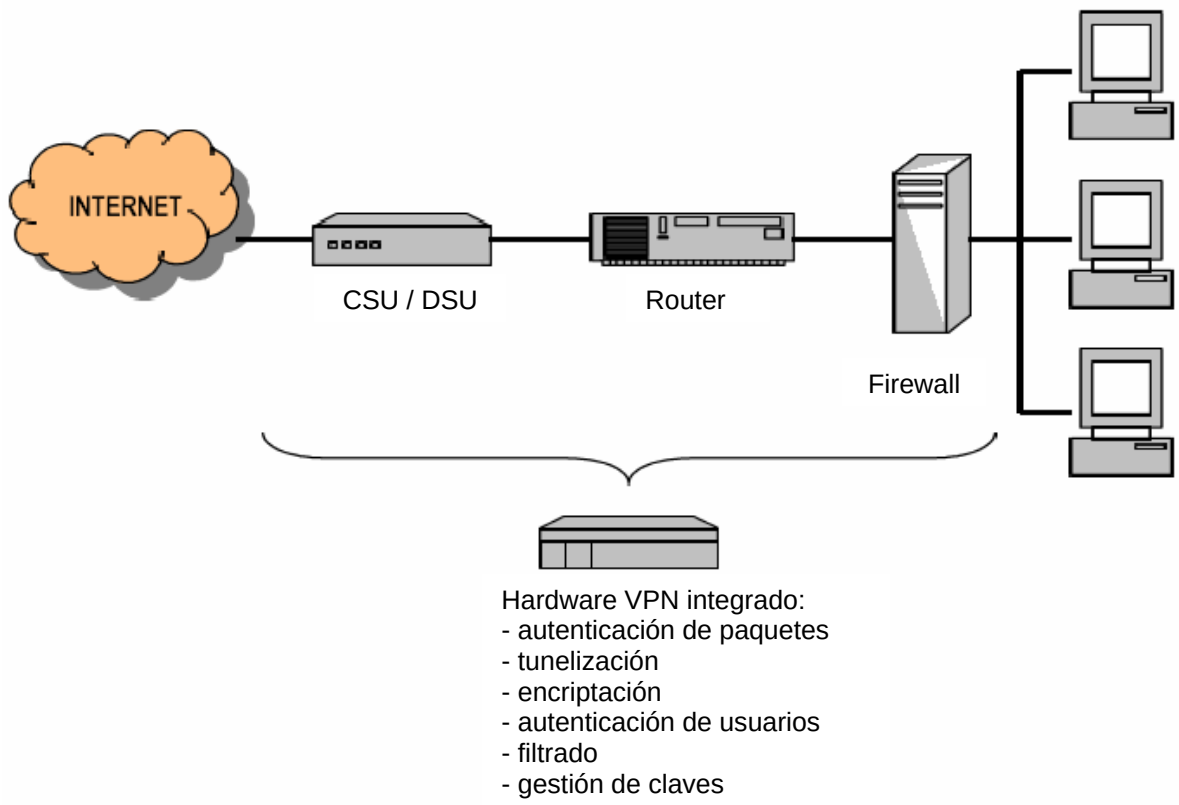


Figura 2.6 Funciones que realiza un equipo VPN Hardware

Como ya hemos indicado en la figura anterior, las funciones importantes de cualquier VPN son: encriptación, autenticación, túneles, y gestión de claves. Dependiendo de que protocolo se planee usar para la construcción de la VPN, se hace un énfasis diferente en cada una de estas funciones. PPTP, por ejemplo, se centra en tunelización e incluye encriptación débil, y L2TP[6] soporta autenticación fuerte de usuarios; por otro lado, IPSec soporta encriptación y gestión de claves, pero todavía necesita trabajar más para ser usado con autenticación fuerte de usuario.

---

[6] Layer 2 Tunneling Protocol

2.7.1 Características

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

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

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

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

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

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

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

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

Las soluciones hardware destacan por su facilidad de configuración e instalación. Sin embargo, pueden resultar algo inflexibles.

Resultan adecuadas para interconectar oficinas remotas, y además existen soluciones híbridas que permiten a clientes software conectarse con servidores hardware.

2.8 VPN Software

Consideramos dos clases de software. Una está compuesta de los productos que proveen servicios VPN para una LAN. La segunda clase de productos son aquellos que pueden ser usados para comunicación host a host sin la necesidad de un gateway seguro.

Los productos que proveen servicios VPN para una LAN cubren una completa gama de características de tunneling y VPN, algunos ofreciendo soporte para protocolos como PPTP, IPSec, ..., y otros usando características propias de tunneling y gestión de claves.

La evolución de VPN, sus requisitos de infraestructura (certificados digitales por ejemplo) y el actual mercado de las redes han hecho las soluciones LAN centralizadas más prioritarias que las soluciones host-to-host.

2.8.1 Características

Las soluciones software VPN para una LAN presentan requerimientos similares a otras soluciones:

Soporte de protocolos: Primero, debemos considerar que protocolos transmitirán a través de VPN – sólo IP o IPX y NETBEUI, ... – Muchos gateways soportan sólo IPSec, lo cual está bien para redes IP, pero que no ayudan si se trata de NetWare sobre IPX, por ejemplo.

Integración son sistemas existentes: También es necesario considerar con integrar el producto con el resto de sistemas de gestión de red y seguridad. Por ejemplo, muchos sistemas dependen de sistemas particulares para la autenticación de usuarios; si ya se está utilizando un sistema particular para la autenticación de usuarios remotos, entonces seleccionando un gateway que es compatible con el sistema actual de autenticación, se simplificará la configuración y gestión de los gateways.

Expedición de certificados digitales: Si se planea usar un sistema de autenticación basado en certificados digitales, entonces se debe pensar en como los certificados serán distribuidos y verificados.

Mantenimiento multisitio: Debemos considerar que, probablemente, los productos serán instalados en más de un sitio. Por este motivo es necesario mantener una política de seguridad lo más consistente posible sobre todo si el producto soporta administración sincronizada de múltiples sitios.

Soporte de algoritmos criptográficos: No todos los productos soportan los mismos algoritmos criptográficos. Los algoritmos IPSec, los algoritmos para encriptación DES CBC y otros algoritmos de autenticación, deberían ser suficientes para aquellos usos considerados de riesgo medio; si el tráfico soportado es de riesgo alto, el producto escogido debería soportar variabilidad automática de claves, incrementando la dificultad de descifrar una clave cuando esta es interceptada (esto es, la clave espira antes de que pueda ser interceptada).

Registro de incidentes: Cada gateway seguro debería tener una forma de registrar los eventos de seguridad (incidentes) e informar de ellos. Incluso sería interesante que el sistema pudiese generar algún tipo de alarma cuando alguna actividad persistente tiene lugar.

Anteriormente indicamos que los productos hardware para VPN ofrecen un mejor rendimiento que cualquier otro producto. Sin embargo, hay distintas razones por las que uno se podría decantar por soluciones software en lugar de por productos hardware.

Primero, el precio. Algunos de los productos software son relativamente baratos o incluso de distribución libre (como es el caso de Microsoft RRAS). Si ya se

dispone del ordenador apropiado en el cual instalar el software, entonces el costo de desarrollar una VPN se reduce incluso más.

Segundo, uno puede estar familiarizado con el sistema operativo o NOS en el cual se ejecuta el software, lo cual conlleva que la administración de la VPN sea más atrayente.

Por último, los servicios y rendimiento de los productos software puede ser todo lo que se necesite. Si se está construyendo una pequeña VPN o bien sosteniendo pequeñas cantidades de tráfico, esto puede no requerir el rendimiento y precio encontrado en muchos de los productos hardware.

Muchos de los productos software para la creación de VPN usan protocolos propietarios y métodos no estándar de intercambio de claves, limitando su interoperabilidad. Pero, algunos de estos mismos productos han llegado a ser compatibles con IPSec, mejorando su interoperabilidad.

El movimiento desde los gateways seguros hasta las redes donde cada computador maneja sus propias sesiones VPN y claves sucederá probablemente de una forma más frecuente en unos pocos años. Al mismo tiempo, un número limitado de productos soportan VPNs host-to-host usando modo de transporte IPSec.

Las soluciones software resultan más flexibles y dinámicas en comparación con las soluciones hardware, e incluso más económicas de ahí que sean una oferta en ebullición.

2.9 EL PROCESO DE TUNEL

Figura 2.7 Proceso de Tunelaje entre dos redes privadas a través de una red publica

El principio de funcionamiento para el proceso de túnel es el siguiente: para enviar un paquete IP al Host2, el Host1 construye el paquete que contiene la dirección IP del Host2, lo inserta en un marco ethernet dirigido al enrutador multiprotocolo que enlaza la intranet 1, y lo pone en el ethernet. Cuando el enrutador multiprotocolo recibe el marco, retira el paquete IP, lo inserta en el campo de carga útil del paquete de capa de red de la WAN, y dirige este último a la dirección de la WAN del enrutador multiprotocolo que enlaza con la intranet2. Al llegar ahí, el enrutador retira el paquete IP y lo envía al Host2 en un marco ethernet.

La WAN puede visualizarse como un gran túnel que se extiende de un enrutador multiprotocolo a otro. El paquete IP simplemente viaja de un extremo del túnel al otro. Sólo el enrutador multiprotocolo tiene que entender los paquetes IP y WAN.

Las redes privadas virtuales crean un túnel o conducto dedicado de un sitio a otro. La tecnología de túneles -Tunneling- es un modo de transferir datos entre 2 redes

similares sobre una red intermedia. También se llama "encapsulación", a la tecnología de túneles que encierra un tipo de paquete de datos dentro del paquete de otro protocolo, que en este caso sería TCP/IP. La tecnología de túneles VPN, añade otra dimensión al proceso de túneles antes nombrado -encapsulación-, ya que los paquetes están encriptados de forma que los datos son ilegibles para los extraños. Los paquetes encapsulados viajan a través de Internet hasta que alcanzan su destino, entonces, los paquetes se separan y vuelven a su formato original. La tecnología de autenticación se emplea para asegurar que el cliente tiene autorización para contactar con el servidor.

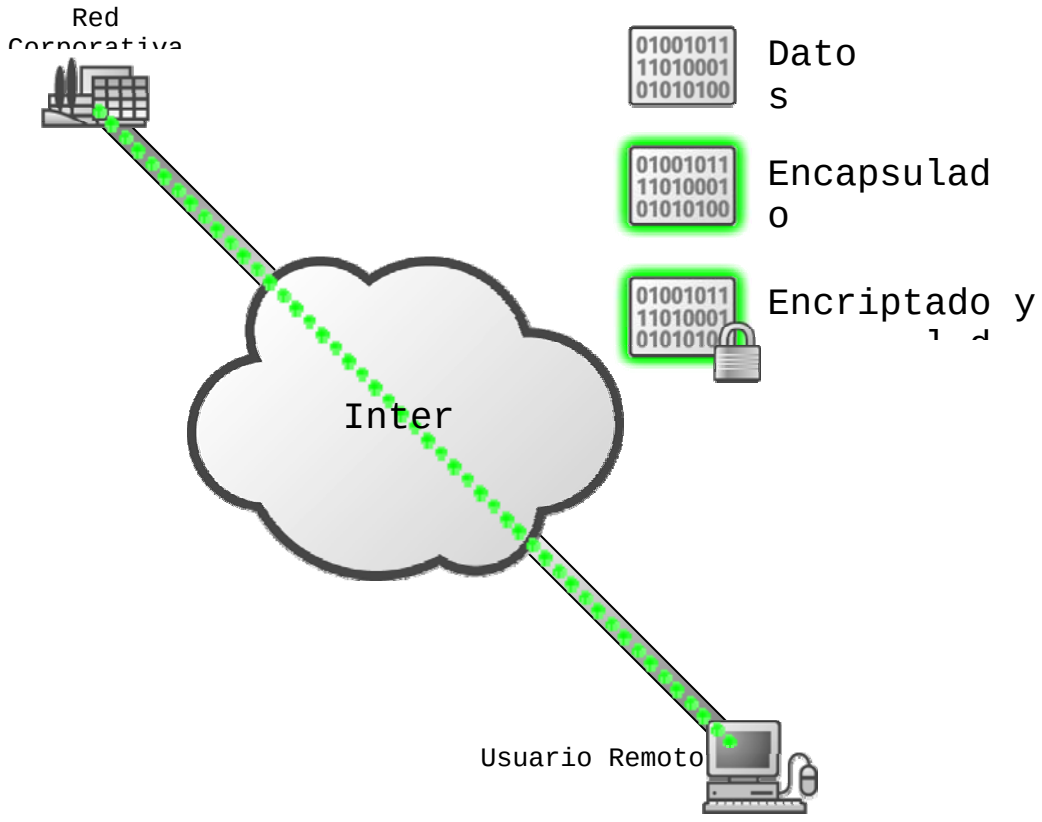


Figura 2.8 Proceso de encapsulación y encriptación de los datos que viajan a través de un túnel en Internet.

El uso de la encriptación en la conexión VPN puede ser necesario en aquellos casos que la información que se vaya a pasar por el túnel sea sensible y requiera privacidad. La conexión encriptada VPN requiere de bastantes recursos tanto en el servidor del túnel como en el ordenador cliente de VPN a parte de requerir la instalación de software especial en el cliente.

Existen muchas aplicaciones y programas que ya hacen dicha encriptación y el encriptar el túnel VPN no nos aporta seguridad adicional. Aplicaciones tales como el correo seguro leído por medio de un interfaz web seguro o una conexión ssh a una máquina multiusuario son suficientemente seguros para no requerir la encriptación adicional, a parte que al encriptar entre el servidor de la aplicación y el cliente de la misma la conexión es absolutamente segura en todo su recorrido, mientras que en una conexión VPN segura la encriptación sólo tiene lugar entre el servidor de túnel y el cliente VPN y la conexión entre el servidor de túneles y el servidor de la aplicación se realiza sin encriptación.

2.9.1 ANTES DEL TUNELADO: PPP, PAP Y CHAP

Debido a que algunos de los protocolos que se van a introducir más adelante en este trabajo, dependen fuertemente de las características originales de PPP, merece la pena hacer una pequeña introducción a este protocolo y a las tecnologías que lo rodean. PPP fue diseñado para enviar datos a través de conexiones de marcado y enlaces punto a punto.

Actualmente se utiliza fundamentalmente para conectarse a Internet a través de la red telefónica básica mediante un módem. PPP encapsula paquetes IP, IPX y NetBEUI en tramas PPP y transmite estas tramas a través de un enlace punto a punto.

Las implementaciones de PPP proporcionan métodos de autenticación. Estos suelen ser PAP, CHAP y MS-CHAP[7].

PAP fue diseñado de manera sencilla y es un protocolo de dos pasos. El host que está conectando y se puede decir que actúa como cliente, envía un nombre de usuario y una contraseña al sistema servidor. Este último, responde si aprueba o no la conexión, convirtiéndose en el propio autenticador de la misma. PAP resulta ser un protocolo bastante inseguro, puesto que envía la información en texto plano.

CHAP es un protocolo similar a PAP, pero resulta más seguro al incorporar un tercer paso para la autenticación. Es un protocolo de desafío y respuesta, lo que

---

[7] Versión mejorada de CHAP desarrollada por Microsoft.

significa que el servidor envía un mensaje de desafío al cliente y este calcula la respuesta mediante MD5.

El desafío consiste en un identificador de sesión y una cadena arbitraria. Con ellos, el cliente elabora una respuesta mediante un condensado en MD5 de estos dos elementos más la contraseña. Dicha respuesta incluye también fuera del condensado MD5 el nombre de usuario. Una vez que el servidor recibe la respuesta del cliente, la puede comparar con el resultado esperado y aceptar o no la conexión. Como el desafío y la respuesta se elaboran con sistemas de condensado de un solo sentido, el servidor no podrá deshacer el condensado de la respuesta del cliente. Por lo que deberá elaborar el mismo condensado él mismo. Es fácil darse cuenta de que este esquema depende de que el servidor y el cliente compartan cierta información de antemano, porque en otro caso el condensado no podría coincidir.

Esta información compartida es la contraseña de usuario.

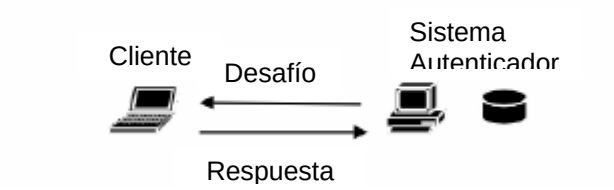


Figura 2.9 Funcionamiento de CHAP. El desafío lleva un identificador de sesión y una cadena arbitraria. La respuesta consiste en un condensado MD5 del identificador de sesión, la cadena arbitraria y la contraseña. Además, la respuesta incluye el nombre de usuario fuera del condensado.

MS-CHAP funciona en esencia como lo hace CHAP. Como en CHAP, el autenticador envía al cliente un desafío que consiste en un identificador de sesión y una cadena arbitraria.

El cliente remoto debe incluir en la respuesta el nombre de usuario y un condensado MD4 que incluye la cadena arbitraria, el identificador de sesión y un condensado MD4 a su vez de la contraseña. Este esquema en el que en el condensado de la respuesta se incluye el condensado de la contraseña, permite que el servidor almacene las contraseñas a su vez condensadas en lugar de hacerlo en texto plano. De este modo, el servidor podrá reproducir el proceso para comparar el resultado con la respuesta del cliente sin necesidad de tener la contraseña original en texto plano, resultando así un poco más seguro ante ataques.

MS-CHAP proporciona también códigos de error y mensajes nuevos que no se encontraban en CHAP. Algunos de estos mensajes permiten cosas como el cambio de contraseña o la posibilidad de detectar contraseñas expiradas.

Una vez que una conexión PPP ha sido negociada, autenticada y establecida, el protocolo comienza a transferir datos entre los dos puntos. Cada paquete que se transmite se encapsula en el origen con una cabecera PPP que es retirada por el sistema que lo recibe.

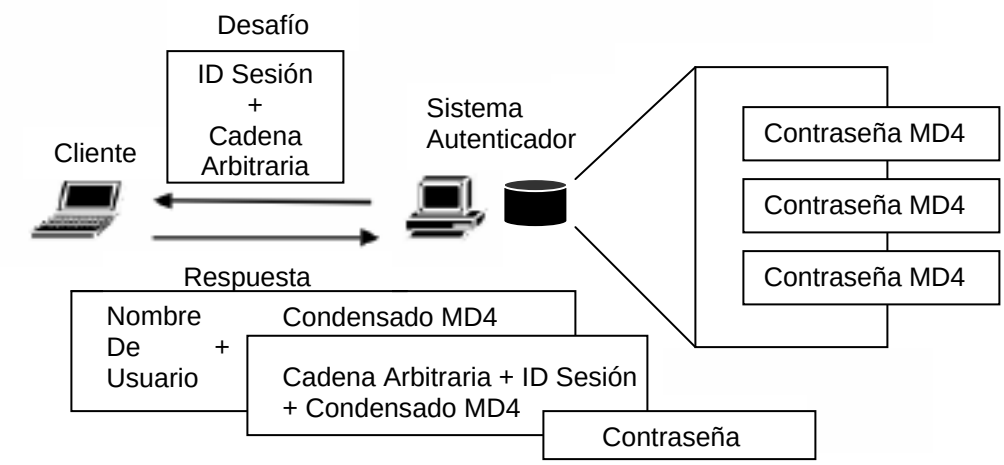


Figura 2.10 La figura trata de ilustrar el funcionamiento de MS-CHAP. La mas interesante mejora respecto a CHAP reside

en el hecho de que la contraseña no ha de ser almacenada en el servidor como texto plano. El servidor conserva una versión condensada de la contraseña, con la que podrá construir él también la respuesta para compararla con la que llega del cliente. En ningún momento es necesario que la contraseña viaje en claro por la red y tan solo el cliente tiene una versión en texto plano de la misma.

De esta manera se obtiene la carga útil de PPP que como ya se ha dicho puede incluir protocolos diversos (IP,IPX. . .)

8	16	24	40bits	Variable	16 - 32 bits
Flag	Address	Control	Protocol	Information	FCS

Tabla 2.1 Estructura del protocolo PPP

- ***Flag*** **-** indicates the beginning or end of a frame, consists of the binary sequence 01111110.
- ***Address*** **-** contains the binary sequence 11111111, the standard broadcast address. (Note: PPP does not assign individual station addresses.)
- ***Control*** **-** contains the binary sequence 00000011, which calls for transmission of user data in an unsequenced frame.
- ***Protocol*** **-** identify the protocol encapsulated in the information field of the frame.
- ***Information*** **-** Zero or more octet(s), contain the datagram for the protocol specified in the protocol field.
- ***FCS*** **-** Frame Check Sequence (FCS) Field, normally 16 bits. By prior agreement, consenting PPP implementations can use a 32-bit FCS for improved error detection.

CAPITULO 3

PPTP

El Protocolo de Túnel Punto-a-Punto (Point to Point Tunneling Protocol) es un protocolo que permite establecer conexiones con túneles PPP, a través de una red IP, creando una VPN. La compañía Microsoft, ha implementado sus propios algoritmos y protocolos con soporte PPTP, el Microsoft PPTP, este es uno de los mas ampliamente extendidos, por la popularidad de los productos Microsoft (Windows 98/ME, NT4, 2000) los cuales llevan incluidos de serie estos protocolos.

Fue desarrollado por el Forum PPTP que esta constituido por la siguientes organizaciones: Ascend Communications, Microsoft Corporation, 3 Com/Primary Access, ECI Telematics, and U.S. Robotics.

3.1 GENERALIDADES

Las siglas PPTP[1] corresponden en ingles con "*Point-to-Point Tunneling Protocol*".

PPTP se diseñó para proporcionar comunicaciones autenticadas y cifradas entre un cliente y una puerta de enlace[2] o entre dos puertas de enlace (sin necesitar una infraestructura de clave pública) utilizando un Id. de usuario y una contraseña. Apareció por primera vez en 1996, dos años antes de la disponibilidad de IPSec y L2TP. El objetivo del diseño era la simplicidad, la compatibilidad multiprotocolo y la capacidad de cruzar una amplia gama de redes IP.

El protocolo de túnel punto a punto utiliza una conexión TCP, por el puerto 1723, para el mantenimiento del túnel y tramas PPP en tramas IP encapsuladas mediante Encapsulación de enrutamiento genérico GRE[2] "*Generic Routing Encapsulation*" para los datos del túnel. Las cargas, partes de datos útiles, de las tramas PPP encapsuladas se pueden cifrar o comprimir. El uso de PPP proporciona la capacidad de negociar los servicios de autenticación, cifrado y asignación de dirección IP.

Actualmente este protocolo, aunque muy popular en el mundo de Microsoft, esta siendo sustituido por el L2TP.

---

[1] Las especificaciones de este protocolo se encuentran en el RFC 2637.
[2] Gateway ó Pasarela.

3.2 Escenario típico de conexión PPTP

Una máquina cliente (Windows 95 o NT 4.0) se conecta a un Proveedor de Servicios de Internet (ISP) utilizando una conexión de acceso telefónico a redes. En otro punto de Internet existe una máquina (NT 4.0 Server) con el servicio de servidor de acceso remoto (RAS) conectado a ella, bien directa y permanentemente, mediante un adaptador de Red o también mediante una conexión de acceso remoto, usando su adaptador de red privada virtual, a dicho servidor, creándose un túnel privado sobre Internet, que conecta ambas máquinas como si estuvieran en la misma red local, pudiendo así tener acceso a recursos compartidos tales como carpetas o impresoras.

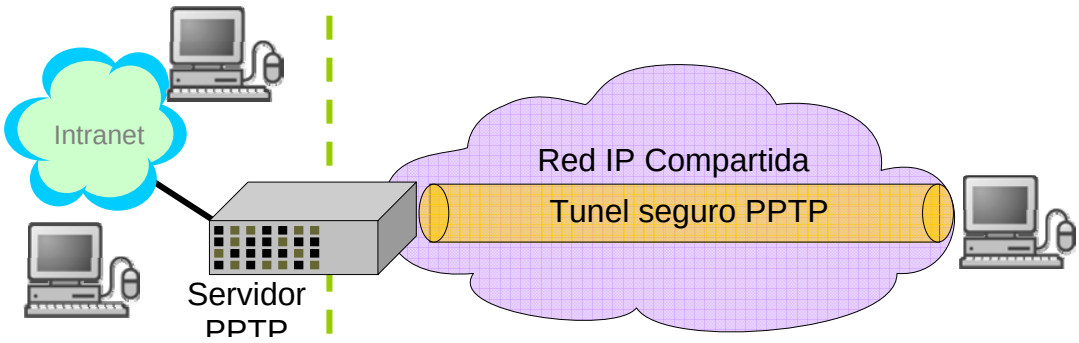


Figura 3.1 Túnel PPTP a través de una red IP compartida como lo es Internet.

Este escenario puede variar según el tipo de conexión que tengan tanto el cliente como el servidor. Organizaciones con acceso permanente a Internet, pueden configurar servidores de acceso remoto para que soporten PPTP. Esto permite que colaboradores en cualquier parte del mundo puedan conectarse a ellos, usando sus accesos a Internet habituales. Así, será posible participar de los recursos de la red corporativa, con seguridad garantizada, y sin los cortes habituales de las llamadas de larga distancia a estos servidores de acceso remoto.

3.3 Servidores PPTP

Un servidor PPTP tiene dos reglas principales: actúa como el fin de punto de los túneles de PPTP y envía paquetes a y por el túnel. Los servidores PPTP envían paquetes a una computadora destino para procesar en paquete PPTP obtenido de dirección o nombre de la red privada en el paquete PPP encapsulado.

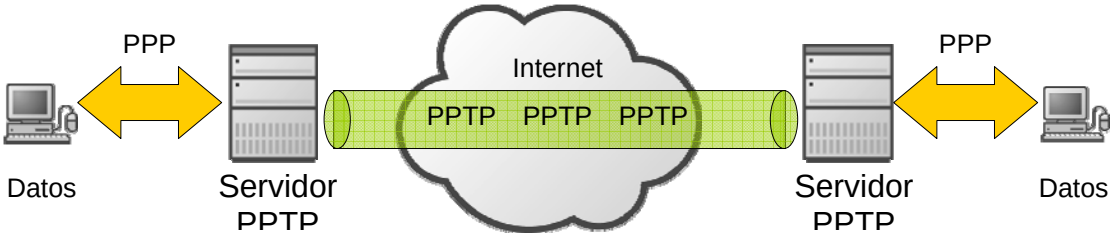


Figura 3.2 Transformaciones que sufren los datos al viajar a través de una VPN que funciona con PPTP.

El servidor PPTP solo puede filtrar paquetes, usando filtros PPTP. Con los filtros PPTP se puede colocar el servidor para restringir quien puede conectarse a la red local o a Internet.

Estableciendo un servidor PPTP a tu sitio corporativo se establecen una pocas restricciones, especialmente si el servidor PPTP esta siendo colocado en el sitio privado del firewall. PPTP ha sido diseñado para que solo un número de puerto TCP/IP pueda usarse para transmitir datos a un firewall, número de puerto 1723. Esta escasez de configuraciones de números de puertos puede hacer al firewall más susceptible a ataques. Solo si se tiene el firewall para filtrar tráfico por el protocolo, necesitarás colocarlos permitiendo a GRE pasar por él.

Tipo de Hardware requerido en los servidores:

La máquina configurada como PPTP server debe tener la configuración mínima requerida para correr Windows NT 4.0 Server. Además, debe tener dos adaptadores de red (NIC, módem, RDSI, X25), uno conectado a la red local LAN, y otro a Internet.

Una de las **ventajas** más palpables del PPTP es que reduce o elimina la necesidad de uso de sofisticados y caros equipos de telecomunicaciones para permitir las conexiones de equipos portátiles y remotos. PPTP puede usar redes telefónicas normales de forma totalmente segura.

3.4 Clientes PPTP

Si el equipamiento ISP soporta PPTP, no requiere añadir software o hardware en el final del cliente; solo es necesaria una conexión estándar PPP. En la otra mano, si el ISP no soporta PPTP, un cliente Windows NT puede utilizar PPTP y crear una conexión segura, primero utilizando ISP y estableciendo una conexión PPP, después a través de un puerto PPTP conectarse con el cliente.

Tipo de Hardware requerido en los clientes:

El cliente puede ser una máquina con Windows NT 4.0, tanto Server como Workstation, o Windows 95. En ambos casos, se requieres de un módem o tarjeta RDSI, además de un equipo de conexión a una red telefónica (plaqueta en pared,

teléfono móvil que soporte este tipo de conexiones, etc.) Por otro lado, si el cliente está accediendo al servidor PPTP a través de una red de área local (LAN), se precisa de un adaptador de red (NIC) que lo conecte físicamente a ella.

3.5 Posibilidades de utilización de PPTP

Debido a su carácter público, sin duda PPTP resulta fácil de adquirir y de utilizar. PPTP uno de los únicos protocolo de red que puede utilizarse para crear redes virtuales privadas.

Este protocolo de red que permite el tráfico seguro de datos desde un cliente remoto a un servidor corporativo privado, estableciéndose así una Red Privada Virtual (VPN) basada en TCP/IP. PPTP soporta múltiples protocolos de red (IP, IPX y NetBEUI) y puede ser utilizado para establecer dichas redes virtuales a través de otras redes públicas o privadas como líneas telefónicas, redes de área local o extensa (LAN's y WAN's) e Internet y otras redes públicas basadas en TCP/IP.

También se puede utilizar para crear redes privadas virtuales entre distintos sistemas operativos.

Además, permite utilizar enlaces de Internet económicos para crear conexiones seguras entre ordenadores.

- *Para Windows:*

El PPTP de Microsoft está destinado a la creación de redes privadas virtuales. De hecho en los sistemas 95, 98 y NT el protocolo PPTP esta incluido gratuitamente.

Para establecer una conexión permanente PPTP hay que utilizar el servicio Routins and Remote Access Service de Windows NT.

La implementación de Microsoft, además, sufre de varios importantísimos errores de diseño que hacen que su protección criptográfica sea inefectiva para alguien más motivado que un simple observador casual. Por tanto no debería ser utilizado.

- *PPTP-linux: un cliente PPTP para Linux:*

PPTP-linux permite la conexión a un servidor PPTP para un Linux o para otro paquete Unix (puertos de pptp-linux a otras variantes de Unix es trivial).

3.6 Partes de un PPTP

El túnel lleva datagramas entre PAC y PNS. Muchas sesiones son multiplexadas sobre un mismo túnel:

3.6.1 PAC (PPTP Acces Concentrator)

Es un concentrador de acceso PPTP. Es un dispositivo que asocia una o más líneas capaces de soportar PPP (Point to Point Protocol) y el manejo

del protocolo PPTP. PAC necesita solamente TCP/IP para pasar sobre el tráfico de una o más PNS.

3.6.2 PNS (PPTP Network Server)

Es el servidor para red de PPTP. Sirve para operar sobre computadoras de propósito general y plataformas de servidores. PNS dirige la parte del servidor del protocolo PPTP mientras PPTP confía completamente TCP/IP y es independiente de la interfaz de Hardware, el PNS puede usar cualquier combinación de hardware de interfaz IP, incluyendo dispositivos LAN y WAN.

PPTP esta implementado para PAC y PNS. Existen actualmente relacionados muchos PAC y PNS, un PAC puede proveer servicio a muchos PNS.

PPTP usa una forma parecida a GRE (Generic Routing Encapsulation) para llevar los paquetes PPP de usuario. Permite a bajo nivel controlar la congestión y flujo que va a llevarse a través de los túneles usados para llevar los datos de usuarios entre PAC y PNS.

Este mecanismo permite la eficiencia del uso del ancho de banda disponible para los túneles y evita retransmisiones innecesarias y desbordamiento en los buffers.

PPTP requiere el establecimiento de un túnel para cada comunicación PNS-PAC. Este túnel es usado para llevar todos los paquetes PPP de sesión de usuario participando un par determinado de PNS y PAC. Una llave está presente en el encabezamiento GRE indicando a cual sesión en particular pertenece el paquete

PPP. De esta manera los paquetes PPP son multiplexados y demultiplexados sobre un túnel simple entre el PNS y PAC dado. El valor a usar en el campo de la llave es establecido por la llamada, estableciendo el procedimiento mediante el cual toma el control de la conexión.

El encabezamiento GRE también contiene la secuencia de información que ha sido usada para desempeñar algún nivel de control de congestión y detección de errores sobre el túnel. Luego la conexión de control es usada para determinar la tasa y los parámetros de almacenamiento temporal que han sido usados para regular el flujo de paquetes PPP para una sesión particular sobre el túnel.

16	32 bits
Length	PPTP message type
Magic cookie	
Control message type	Reserved 0
Protocol Version	Reserved 1
Framing capability	
Bearing capability	
Maximum channels	Firmware revision
Host name (64 Octets)	
Vendor string (64 Octets)	

Tabla 3.1 Estructura del protocolo PPTP.

- ***Length*** **–** Longitud total en octetos del mensaje PPTP incluyendo el encabezado.
- ***PPTP message type*** **–** El tipo de mensaje. Sus posibles valores son: 1 Mensaje de control ; 2 Mensaje de administración.

- ***Magic cookie -*** Magic cookie es siempre enviada como la constante 0x1A2B3C4D. Su propósito básico es permitir al receptor asegurarse de que está apropiadamente sincronizada con la trama de datos TCP.
- ***Control Message Type –*** Los valores pueden ser: 1 Petición de Inicio del control de conexión. 2 Respuesta de Inicio del control de conexión; 3 Petición de parar el control de la conexión; 4 Respuesta de parar el control de la conexión; 5 Echo-Request; 6 Echo-Reply.
- ***Call Management –*** Los valores son: 7 Petición llamada saliente; 8 Respuesta llamada saliente; 9 Petición llamada entrante; 10 Respuesta de llamada entrante; 11 Llamada entrante conectada; 12 Petición de despeja de llamada; 13 Notificación de llamada desconectada; 14 Notificación de error en la WAN.; Control de Sesión PPP - 15 Información para establecer enlace.
- ***Reserved 0 & 1 –*** Debe ser puesto a 0.
- ***Protocol version –*** Número de la versión de PPTP.
- ***Framing Capabilities –*** Indica el tipo de trama que el transmisor de este mensaje puede proveer: 1 – Trama asíncrona soportada; 2 – Trama síncrona soportada.
- ***Bearer Capabilities –*** Indica las capacidades de la portadora que el transmisor del mensaje puede proveer.: 1 – Acceso análogo soportado; 2 – Acceso digital soportado.
- ***Maximum Channels –*** El número total de sesiones PPTP individuales que este PAC puede soportar .
- ***Firmware Revision –*** Contiene la revisión del número de ….del PAC usado, cuando es emitido PAC, o la versión del driver PNS PPTP si es emitida por PNS.
- ***Host Name –*** Contiene el nombre DNS the el PAC o PNS emitido.

- ***Vendor Name –*** Contiene la cadena específica del vendedor describiendo el tipo de PAC que está siento usado, o el tipo de software de PNS que está siendo usado si la petición ha sido emitida por el PNS.

3.7 PPTP relacionado con Firewalls

PPTP complementa el uso de firewalls y cubre la necesidad de otro tipo diferente de seguridad. Los firewalls aseguran la red corporativa privada regulando estrictamente los datos que llegan desde Internet. PPTP asegura la privacidad de los datos intercambiados entre clientes y servidor a través de Internet.

El tráfico PPTP usa el puerto TCP 1723, y el identificador IP 47. Por tanto, un firewall puede configurarse para habilitar el tráfico a través de ellos. Un servidor PPTP situado detrás de él aceptará los paquetes PPTP que éste le envíe, extraerá el paquete PPP del datagrama IP, descifrará el paquete, y lo enviará a la máquina destino de la red privada. Por tanto, se habrán combinado la seguridad del firewall en cuanto a la defensa de red privada de paquetes ajenos a ella, y la del PPTP, en lo que respecta a la seguridad con la que los paquetes de datos relativos a la red privada que han sido enviados a través de la red pública TCP/IP (Internet).

CAPITULO 4

L2TP

El protocolo de túneles L2TP, ha nacido de la combinación de las características del protocolo PPTP y L2F (Layer 2 Forwarding). L2TP es un protocolo de red que facilita la creación de túneles para enviar tramas PPP. Encapsula las tramas PPP para que puedan ser enviadas sobre redes IP, X.25, Frame Relay o ATM. La carga útil de las tramas PPP, puede ser encriptada y/o comprimida. Se puede usar L2TP directamente sobre diferentes tipos de WAN, por ejemplo, Frame Relay, sin una capa de transporte IP. L2TP usa UDP y una serie de mensajes de L2TP para los mantenimiento de túneles sobre redes IP. L2TP permite múltiples túneles entre los dos puntos finales.

4.1 INTRODUCCION

L2TP[1] es un protocolo estándar diseñado para transmitir datos y conectar de forma segura redes a través de Internet. Aceptado ya por la mayoría de firmas y vendedores de productos de conectividad, se prevé que en un futuro inmediato constituya una de las funciones más revolucionarias, importantes, y usadas, por todo tipo de redes de datos mundiales en la creación de Redes Privadas Virtuales. L2TP es un protocolo estándar aprobado por el IETF (Internet Engineering Task Force), en oposición al protocolo propietario de Microsoft PPTP (Point-to-Point Tunneling Protocol). Es soportado prácticamente por la totalidad de firmas del mercado de la comunicación de datos, incluyendo Microsoft y Cisco.

L2TP, Protocolo de Túneles Capa 2 (Layer Two Tunneling Protocol [L2TP]) es una extensión del Protocolo Túnel Punto a Punto (Point to Point Tunneling Protocol [PPTP]) usado por los Proveedores de Servicio de Internet (Internet Service Provider [ISP]) para permitir la operación de VPN sobre Internet. L2TP emerge de la fusión de las mejores características de otros protocolos de túneles: PPTP de Mircrosoft Corp. y L2F (Layer 2 Forwading) de Cisco Systems.

Con la ayuda de L2TP e Internet, las llamadas de larga distancia pueden ser sustituidas por llamadas locales al proveedor de Internet. Por lo que se realizan importantes ahorros en el precio de la factura telefónica.

L2TP es un protocolo de comunicación entre dispositivos de datos y es transparente a las aplicaciones de usuario existentes. No hay necesidad de invertir en programas nuevos para aprovechar las ventajas del L2TP.

---

[1] Las especificaciones de este protocolo se encuentran en el RFC 2661.

4.2 DESCRIPCIÓN DEL PROTOCOLO L2TP

Las siglas L2TP corresponden en inglés con "Layer 2 Tunneling Protocol".
L2TP es un protocolo maduro en la senda de los estándares IETF que ha sido ampliamente implementado.

L2TP encapsula las tramas del protocolo punto a punto (PPP) que van a enviarse a través de redes IP, X.25, Frame Relay, o modo de transferencia asíncrona ATM "Asynchronous Transfer Mode".

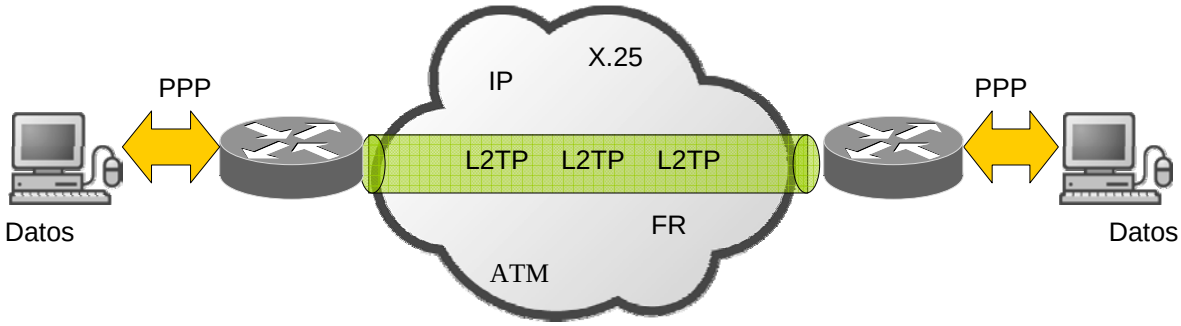


Figura 4.1 Los datos se encapsulan en tramas PPP y posteriormente se convierten a tramas L2TP, con lo que están preparados para enviarse a través de cualquiera de las reds que se ilustran en la fugura.

Cuando está configurado para utilizar IP como su transporte, L2TP se puede utilizar como protocolo de túnel VPN en Internet. L2TP sobre IP utiliza el puerto UDP 1701 e incluye una serie de mensajes de control L2TP para el mantenimiento del túnel.

También utiliza UDP para enviar tramas PPP encapsuladas en L2TP como datos del túnel. Las tramas PPP encapsuladas se pueden cifrar o comprimir. Cuando los túneles L2TP aparecen como paquetes IP, aprovechan la seguridad IPSec

estándar mediante el modo de transporte IPSec para obtener una fuerte protección de integridad, reproducción, autenticidad y privacidad.

L2TP se diseñó específicamente para conexiones cliente a servidores de acceso a redes, así como para conexiones puerta de enlace a puerta de enlace. Mediante la utilización del protocolo PPP, L2TP gana compatibilidad multiprotocolo para protocolos como IPX y Appletalk.

L2TP también proporciona una amplia gama de opciones de autenticación de usuario, incluidos CHAP, MS-CHAP, MS-CHAPv2 y el Protocolo de autenticación extensible EAP *"Extensible Authentication Protocol"* que admite mecanismos de autenticación de tarjetas token y tarjetas inteligentes.

L2TP/IPSec, por lo tanto, proporciona túneles bien definidos e interoperables, con la seguridad de alto nivel e interoperabilidad de IPSec. Es una buena solución para conexiones seguras de acceso remoto y de puerta de enlace a puerta de enlace.

4.3 TERMINOS PRINCIPALES DE L2TP

4.3.1 LAC (L2TP ACCES CONCENTRATOR)

El LAC es un dispositivo físico que se añade a los elementos de interconexión de la red conmutada; como lo es la red telefónica convencional RDSI[2], o se coloca con un sistema de terminación PPP capaz de gestionar el protocolo L2TP. Un LAC sólo necesita implementar el medio sobre el cual opera el L2TP para admitir el tráfico de una o más LNS.

Puede "tunelizar" cualquier protocolo que incluya el PPP. LAC es el iniciador de las llamadas entrantes y el receptor de las llamadas salientes. También se le conoce como el servidor de acceso a la red. Por favor refiérase a la Figura 4.2.

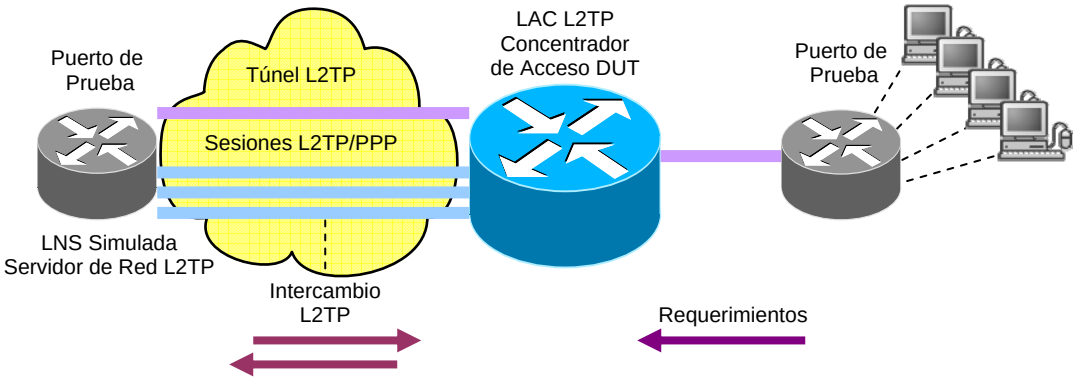


Figura 4.2 Componentes físicos de una VPN trabajando con L2TP.

[2] Red Digital de Servicios Integrados

4.3.2 LNS (L2TP NETWORK SERVER)

Un LNS opera sobre cualquier plataforma con capacidad de terminación PPP. LNS gestiona el lado del servidor del protocolo L2TP. Ya que L2TP se apoya sobre el medio al que llegan los túneles L2TP, LNS sólo puede tener una única interfaz LAN o WAN, aunque es capaz de terminar las llamadas entrantes en cualquiera de la amplia gama de las interfaces PPP LAC (asíncronos, RDSI, PPP sobre ATM, PPP sobre Frame Relay). LNS también se conoce como Home Gateway (HGW). Para una mejor comprensión por favor véase a la Figura 4.2.

4.3.3 SERVIDOR DE ACCESO A LA RED (NETWORK ACCESS SERVER)

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

4.4 AUTENTICACION Y ENCRIPTACIÓN

La autentificación de un usuario ocurre en 3 fases en L2TP.

En la primera fase, el ISP puede usar el número de teléfono de la llamada recibida, el número llamado o el nombre del usuario determinado que el servicio de L2TP requiere y entonces iniciar un túnel de conexión al servidor de red apropiado. Cuando un túnel esta establecido, el Concentrador de Acceso (LAC) del ISP asigna un nuevo ID de llamada para identificar la conexión con el túnel y inicia una sesión para devolver la información autentificada.

El servidor de red corporativa emprende la segunda fase de autentificación para decidir si acepta o no la llamada. La llamada comienza indicando al ISP si incluir CHAP, PAP, EAP[3] o la información de la autentificación de otros, el servidor de red usará esta información para decidir si acepta o rechaza la llamada.

Después que la llamada ha sido aceptada, el servidor de red puede iniciar la tercera fase de autentificación a la capa de PPP. Este paso deberá ser similar al usado por una compañía para autentificar a usuarios de acceso remoto quienes están conectándose por un viejo camino, por ejemplo usando un módem.

A través de estas 3 fases de autentificación L2TP garantiza que el usuario final, ISP y el servidor de red están conectados con quien dicen ser.

Si el túnel de autentificación L2TP es deseado, es necesario distribuir las claves. La distribución manual de claves sería factible en un número de casos limitados, pero en un caso de múltiple entrega, éste se torna en una solución muy poco

---

[3] Extensible Authentication Protocol

viable. Para ello se debe implementar protocolos de funcionamiento de llaves, para automatizar, agilizar y garantizar la adecuada distribución de llaves.

4.5 VENTAJAS DE L2TP

Una de las mayores ventajas de L2TP es proporcionar seguridad en el acceso a los recursos corporativos privados sobre Internet. Los componentes de mayor importancia son aquellos que definen el punto final de un túnel basado en este protocolo, entre los cuales se encuentra el concentrador de acceso L2TP (LAC) como parte del equipamiento del ISP, y el servidor de red L2TP (LNS). En el caso de los ISPs además del hardware implementado en el mismo se tiene en cuenta el software necesario requerido que puede ser reducido para el enlace de los clientes móviles, los cuales necesitaran negociar en la primera fase de autentificación de usuarios. Por otro lado, el LNS deberá ser atendido y mantenido por el personal de la empresa, mientras que estas actividades son responsabilidad del ISP con relación al LAC. Véase figura 4.3.

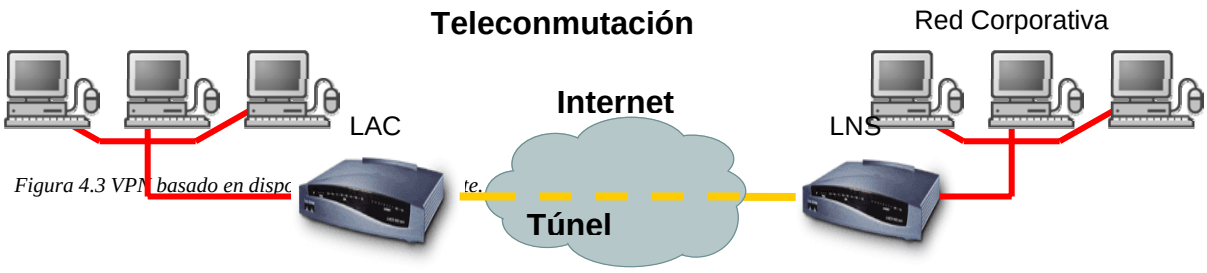
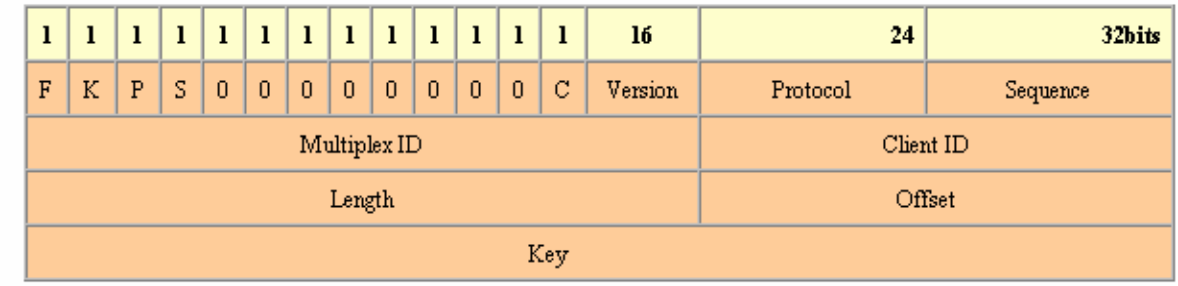


Figura 4.3 VPN basado en dispo te.

4.6 ARQUITECTURA DE L2F



1	1	1	1	1	1	1	1	1	1	1	1	1	16	24	32bits
F	K	P	S	0	0	0	0	0	0	0	0	C	Version	Protocol	Sequence
Multiplex ID														Client ID	
Length														Offset	
Key															

Tabla 4.1 Estructura del protocolo L2F.

- ***Version –*** La máxima versión del software L2F.
- ***Protocol –*** El campo del protocolo especifica el protocolo portado sin el paquete L2F.
- ***Sequence –*** El número de secuencia es presentado si el bit S en la cabecera L2F está puesta a 1.
- ***Multiplex ID –*** Este paquete identifica una conexión particular sin un túnel.
- ***Client ID –*** La identificación del cliente (CLID) asiste puntos finales en demultiplexación de túneles.
- ***Length –*** Es el tamaño en octetos del paquete completo, incluyendo el encabezado, todos los campos y la carga útil.
- ***Offset –*** Este campo especifica el número de bytes despúes de la cabecera L2F en la cual se espera que empiece la carga útil. Este campo es presentado si el bit F en el encabezado es puesto a 1.
- ***Key –*** El campo de llave es presentado si el bit K está puesto en el encabezado L2F. Este es parte de el proceso de autenticación.
- ***Checksum –*** El checksum del paquete. El campo checksum está presente si el bit C en el encabezado L2F está puesto a 1.

4.7 ARQUITECTURA DE L2TP

Este protocolo pertenece al conjunto de protocolos TCP/IP, respondiendo a las características descritas en la Tabla 1.

Conjunto de Protocolos	TCP/IP
Tipo	Aplicattion Layer Tunneling Protocol
Protocolo IP	115
Puerto IP	1701 (UDP)
Protocolos Relacionados	L2F (Layer 2 Forwarding), PPTP (Point To Pont Tunneling Protocol)

Tabla 4.2. Descripción L2TP.

Como se puede observar en la Tabla 2, la cabecera del protocolo L2TP es parte del conjunto de cabeceras de un datagrama IP.

Tabla 4.3. Posición de la cabecera L2TP en el datagrama IP.

Tabla 4.4. Cabecera L2TP, versión 2.

- ***T, Message Type. 1 bit.*** Especifica si es un mensaje de control (0) o datos (1).
- ***L, Used Length. 1 bit.*** Mensajes de Control DEBEN tener configurado este bit.
- ***S, Used Sequence. 1 bit.***. Si esta configurado, los campos Ns y Nr tambien deben estar configurados. Mensajes de Control DEBEN tener configurado este bit.
- ***O, Used Offset. 1 bit.*** Mensajes de Control DEBEN tener configurado este bit.
- ***P, Priority. 1 bit.*** Este debe recibir tratamiento especial en la cola local.
- ***Version. 4 bits.*** Indica la versión del protocolo L2TP. DEBE ser configurado a 2, el valor 1 es reservado para detección L2F .
- Length., 16 bits. Opcional. El tamaño total del mensaje, este campo existe si L esta configurado.
- ***Tunnel ID. 16 bits.*** Indica el identificador de control de la conexión, los túneles son nombrados por identificadores locales.
- ***Session ID. 16 bits.*** Indica el identificador de la sesión dentro de un túnel.
- ***Ns, Sequence Number. 16 bits.*** Optional. Indica el número de secuencia para el mensaje de control o los datos actuales.
- ***Nr, Sequence Number Expected. 16 bits.*** Optional. Indica el número de secuencia esperado en el siguiente mensaje de control a ser recibido.
- ***Offset Size. 16 bits.*** Optional. Especifica el número de bytes donde la cabecera finaliza y comienzan los datos.
- ***Offset Pad.*** Relleno

CAPITULO 5

IPSEC

IPSec es un conjunto de estándares del IETF para incorporar servicios de seguridad en IP y que responde a la necesidad creciente de garantizar un nivel de seguridad imprescindible para las comunicaciones entre empresas y comercio electrónico. En este trabajo se ofrece una breve introducción a los detalles técnicos del estándar IPSec y se discuten los servicios de seguridad que proporciona. Finalmente se presentan varios escenarios prácticos, donde se detallan las ventajas que ofrece utilizar un protocolo de seguridad estándar como IPSec.

5.1 INTRODUCCION

IPSec[1] es un estándar que proporciona servicios de seguridad a la capa IP y a todos los protocolos superiores basados en IP (TCP y UDP, entre otros). Por fin existe un estándar que aborda las carencias en cuanto a seguridad del protocolo IP. Dichas carencias son muy graves y, tal como se ha constatado en los últimos años, afectan a la infraestructura misma de las redes IP.

Todas las soluciones descritas anteriormente se basaban en soluciones propietarias que dificultaban la comunicación entre los distintos entornos empresariales, al ser necesario que éstos dispusiesen de una misma plataforma. La falta de interoperabilidad ha sido el principal freno para el establecimiento de comunicaciones seguras, dado que no se ve factible la migración a una determinada plataforma en función de una colaboración empresarial puntual.

Entre las ventajas de IPSec destacan que está apoyado en estándares del IETF[2] y que proporciona un nivel de seguridad común y homogéneo para todas las aplicaciones, además de ser independiente de la tecnología física empleada. IPSec se integra en la versión actual de IP (IP versión 4) y, lo que es todavía más importante, se incluye por defecto en IPv6.

Puesto que la seguridad es un requisito indispensable para el desarrollo de las redes IP, IPSec está recibiendo un apoyo considerable: todos los equipos de comunicaciones lo incorporan, así como las últimas versiones de los sistemas operativos más comunes. Al mismo tiempo, ya existen muchas experiencias que

---

[1] Las especificaciones de este protocolo se encuentran en el RFC 2401.

[2] IETF página: *http://www.ietf.org/html.charters/ipsec-charter.html*

demuestran la interoperabilidad entre fabricantes[3], lo cual constituye una garantía para los usuarios.

Otra característica destacable de IPSec es su carácter de estándar abierto. Se complementa perfectamente con la tecnología PKI y, aunque establece ciertos algoritmos comunes, por razones de interoperabilidad, permite integrar algoritmos criptográficos más robustos que pueden ser diseñados en un futuro.

Entre los beneficios que aporta IPSec, cabe señalar que:

- Posibilita nuevas aplicaciones como el acceso seguro y transparente de un nodo IP remoto.
- Facilita el comercio electrónico de negocio a negocio, al proporcionar una infraestructura segura sobre la que realizar transacciones usando cualquier aplicación. Las *extranets* son un ejemplo.
- Permite construir una red corporativa segura sobre redes públicas, eliminando la gestión y el coste de líneas dedicadas.
- Ofrece al teletrabajador el mismo nivel de confidencialidad que dispondría en la red local de su empresa, no siendo necesaria la limitación de acceso a la información sensible por problemas de privacidad en tránsito.

Es importante señalar que cuando citamos la palabra "seguro" no nos referimos únicamente a la confidencialidad de la comunicación, también nos estamos refiriendo a la integridad de los datos, que para muchas compañías y entornos de negocio puede ser un requisito mucho más crítico que la confidencialidad. Esta integridad es proporcionada por IPSec como servicio añadido al cifrado de datos o como servicio independiente.

---

[3] ICSA Certified IPSec Products: *http://www.icsa.net/html/communities/ipsec/certification/certified_products/index.shtml*

5.2. DESCRIPCIÓN DEL PROTOCOLO IPSec

IPSec es, en realidad, un conjunto de estándares para integrar en IP funciones de seguridad basadas en criptografía. Proporciona confidencialidad, integridad y autenticidad de datagramas IP, combinando tecnologías de clave pública (RSA), algoritmos de cifrado (DES, 3DES, IDEA, Blowfish), algoritmos de *hash* (MD5, SHA-1) y certificados digitales X509v3.

Figura 5.1 Tecnologías utilizadas en IPSec.

En la **Figura 5.1** se observa como IPSec es el resultado de la complementariedad de varias de estas técnicas.

El protocolo IPSec ha sido diseñado de forma modular, de modo que se pueda seleccionar el conjunto de algoritmos deseados sin afectar a otras partes de la implementación. Han sido definidos, sin embargo, ciertos algoritmos estándar que deberán soportar todas las implementaciones para asegurar la interoperabilidad en el mundo global de Internet. Dichos algoritmos de referencia son DES y 3DES, para cifrado, así como MD5 y SHA-1, como funciones de *hash.* Además es

perfectamente posible usar otros algoritmos que se consideren más seguros o más adecuados para un entorno específico: por ejemplo, como algoritmo de cifrado de clave simétrica IDEA, Blowfish o el más reciente AES[4] que se espera sea el más utilizado en un futuro próximo.

Dentro de IPSec se distinguen los siguientes componentes:

- Dos protocolos de seguridad: *IP Authentication Header* **(AH)** e *IP Encapsulating Security Payload* **(ESP)** que proporcionan mecanismos de seguridad para proteger tráfico IP.
- Un protocolo de gestión de claves *Internet Key Exchange* **(IKE)** que permite a dos nodos negociarlas claves y todos los parámetros necesarios para establecer una conexión AH o ESP.

5.2.1 EL PROTOCOLO AH

El **protocolo AH**[5] es el procedimiento previsto dentro de IPSec para garantizar la integridad y autenticación de los datagramas IP. Esto es, proporciona un medio al receptor de los paquetes IP para autenticar el origen de los datos y para verificar que dichos datos no han sido alterados en tránsito. Sin embargo no proporciona ninguna garantía de confidencialidad, es decir, los datos transmitidos pueden ser vistos por terceros.

Tal como indica su nombre, AH es una cabecera de autenticación que se inserta entre la cabecera IP estándar (tanto IPv4 como IPv6) y los datos transportados,

---

[4] AES Home page: *http://www.nist.gov/aes/*
[5] IP Authentication Header. RFC 2402.

que pueden ser un mensaje TCP, UDP o ICMP, o incluso un datagrama IP completo (ver la **Tabla 5.1**). AH es realmente un protocolo IP nuevo, y como tal el IANA le ha asignado el número decimal 51. Esto significa que el campo *Protocolo* de la cabecera IP contiene el valor 51, en lugar de los valores 6 ó 17 que se asocian a TCP y UDP respectivamente. Es dentro de la cabecera AH donde se indica la naturaleza de los datos de la capa superior. Es importante destacar que AH asegura la integridad y autenticidad de los datos transportados y de la cabecera IP, excepto los campos variables: TOS, TTL, *flags, offset* y *checksum* (ver la **Tabla 5.1**).

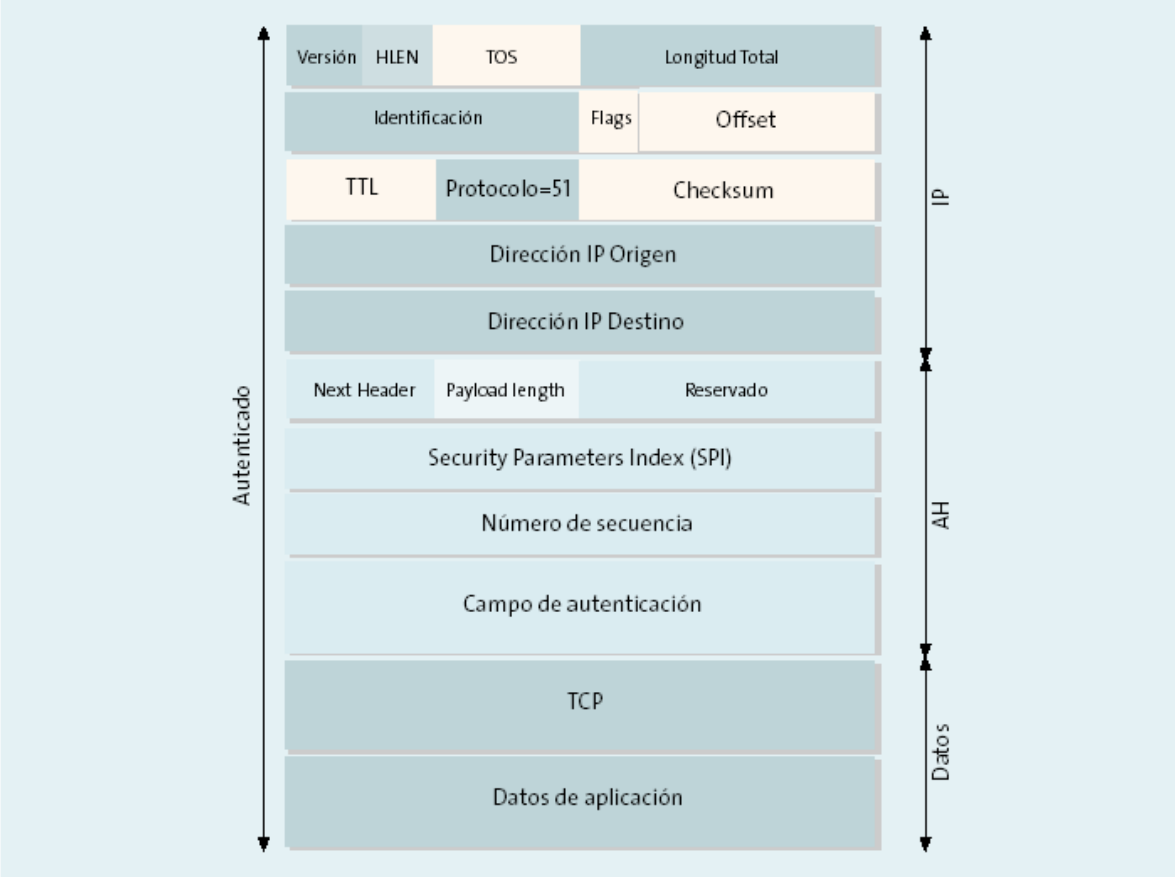


Tabla 5.1 Estructura de un datagrama AH.

El funcionamiento de AH se basa en un algoritmo HMAC[6] , esto es, un código de autenticación de mensajes. Este algoritmo consiste en aplicar una función *hash* a la combinación de unos datos de entrada y una clave, siendo la salida una pequeña cadena de caracteres que denominamos extracto. Dicho extracto tiene la propiedad de que es como una huella personal asociada a los datos y a la persona que lo ha generado, puesto que es la única que conoce la clave.

En la **Figura 5.2** se muestra el modo en que funciona el protocolo AH. El emisor calcula un extracto del mensaje original, el cual se copia en uno de los campos de la cabecera AH. El paquete así construido se envía a través de la red, repitiéndose en el extremo receptor el cálculo del extracto y comparándolo con el recibido en el paquete. Si son iguales, el receptor tiene la seguridad de que el paquete IP no ha sido modificado en tránsito y que procede efectivamente del origen esperado.

Si analizamos con detalle el protocolo AH, podemos concluir que su seguridad reside en que el cálculo del extracto (MAC) es imposible sin conocer la clave, y que dicha clave (en la **Figura 5.2**, clave AH) sólo la conocen el emisor y el receptor.

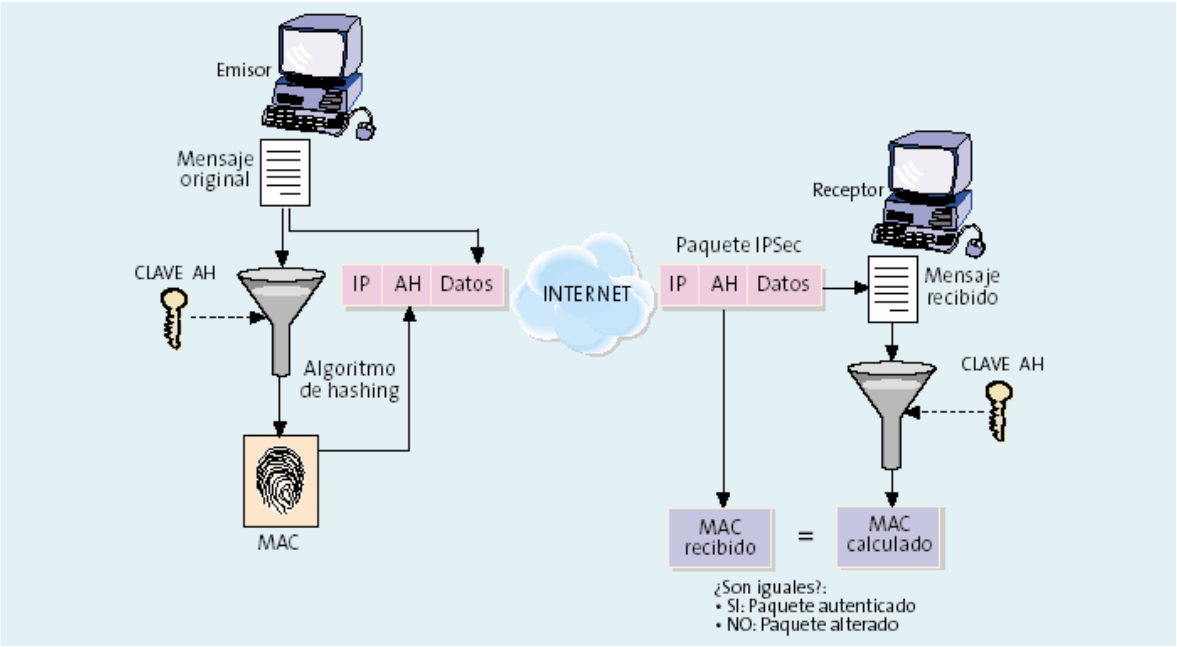


Figura 5.2 Funcionamiento del protocolo AH.

[6] Keyed-Hashing for Message Authentication. RFC 2104.

5.2.2 EL PROTOCOLO ESP

El objetivo principal del **protocolo ESP** (*Encapsulating Security Payload*)[7] es proporcionar confidencialidad, para ello especifica el modo de cifrar los datos que se desean enviar y cómo este contenido cifrado se incluye en un datagrama IP. Adicionalmente, puede ofrecer los servicios de integridad y autenticación del origen de los datos incorporando un mecanismo similar al de AH.

Dado que ESP proporciona más funciones que AH, el formato de la cabecera es más complejo; este formato consta de una cabecera y una cola que rodean los datos transportados. Dichos datos pueden ser cualquier protocolo IP (por ejemplo, TCP, UDP o ICMP, o incluso un paquete IP completo). En la **Tabla 5.2** se muestra la estructura de un datagrama ESP, en la que se observa cómo el contenido o carga útil viaja cifrado.

El IANA ha asignado al protocolo ESP el número decimal 50[8]. Esto implica que el campo *Protocolo* de la cabecera IP contendrá el valor 50, mientras que dentro del mensaje ESP se indica la naturaleza de los datos. Puesto que este campo, al igual que la carga útil, está cifrado, un hipotético atacante que intercepte el paquete no podrá saber si el contenido es TCP o UDP; esto es completamente normal ya que el objetivo que se persigue es, precisamente, ocultar la información.

---

[7] IP Encapsulating Security Payload (ESP). RFC 2406.

[8] Protocol Numbers: *http://www.iana.org/assignments/protocol-numbers*

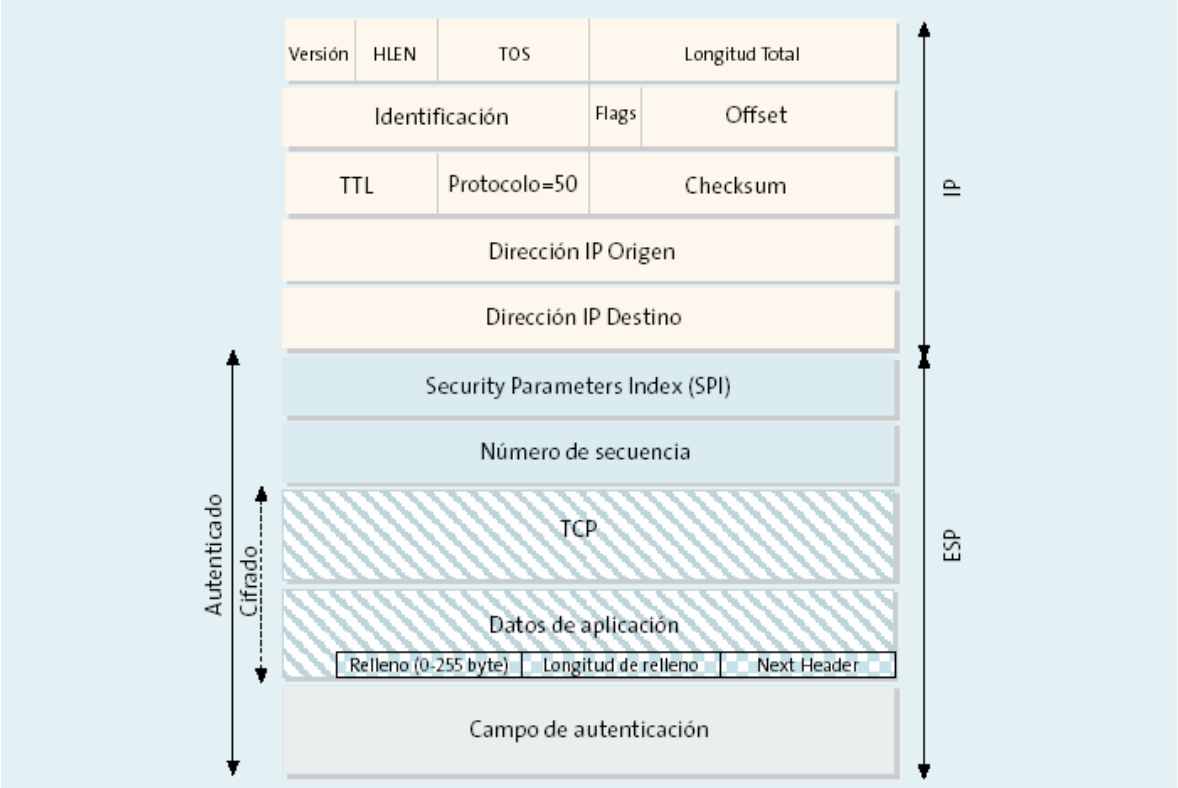


Tabla 5.2 Estructura de un datagrama ESP.

La función de cifrado dentro del protocolo ESP es desempeñada por un algoritmo de cifrado de clave simétrica. Típicamente se usan algoritmos de cifrado bloque, de modo que la longitud de los datos a cifrar tiene que ser un múltiplo del tamaño de bloque (8 o 16 byte, en la mayoría de los casos). Por esta razón existe un campo de relleno, tal como se observa en la **Tabla 5.2**, el cual tiene una función adicional: es posible añadir caracteres de relleno al campo de datos para ocultar así su longitud real y, por tanto, las características del tráfico. Un atacante suficientemente hábil podría deducir cierta información a partir del análisis de ciertos parámetros de las comunicaciones, aunque estén cifradas, tales como el retardo entre paquetes y su longitud. La función de relleno está pensada para dificultar este tipo de ataques.

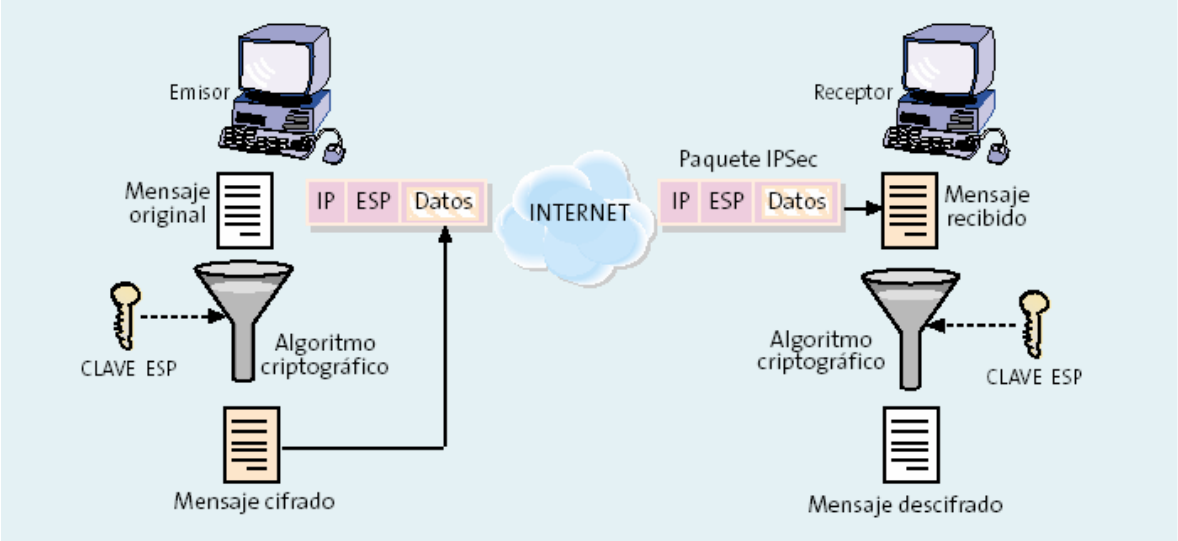


Figura 5.3 Funcionamiento del protocolo ESP.

En la **Figura 5.3** se representa cómo el protocolo ESP permite enviar datos de forma confidencial. El emisor toma el mensaje original, lo cifra, utilizando una clave determinada, y lo incluye en un paquete IP, a continuación de la cabecera ESP. Durante el tránsito hasta su destino, si el paquete es interceptado por un tercero sólo obtendrá un conjunto de bit ininteligibles. En el destino, el receptor aplica de nuevo el algoritmo de cifrado con la misma clave, recuperando los datos originales. Está claro que la seguridad de este protocolo reside en la robustez del algoritmo de cifrado, es decir, que un atacante no puede descifrar los datos sin conocer la clave, así como en que la clave ESP únicamente la conocen el emisor y el receptor.

La distribución de claves de forma segura es, por consiguiente, un requisito esencial para el funcionamiento de ESP y también de AH, como hemos visto anteriormente. Asimismo, es fundamental que el emisor y el receptor estén de acuerdo tanto en el algoritmo de cifrado o de *hash* y como en el resto de parámetros comunes que utilizan. Esta labor de puesta en contacto y negociación

es realizada por un protocolo de control, denominado IKE, que veremos más adelante.

5.3. LOS MODOS TRANSPORTE Y TUNEL

Antes de entrar en los detalles del protocolo IKE es necesario explicar los dos modos de funcionamiento que permite IPSec. Tanto ESP como AH proporcionan dos modos de uso:

5.3.1 *El modo transporte.*

En este modo el contenido transportado dentro del datagrama AH o ESP son datos de la capa de transporte (por ejemplo, datos TCP o UDP). Por tanto, la cabecera IPSec se inserta inmediatamente a continuación de la cabecera IP y antes de los datos de los niveles superiores que se desean proteger. El modo transporte tiene la ventaja de que asegura la comunicación extremo a extremo, pero requiere que ambos extremos entiendan el protocolo IPSec.

5.3.2 El modo túnel.

En éste el contenido del datagrama AH o ESP es un datagrama IP completo, incluida la cabecera IP original. Así, se toma un datagrama IP al cual se añade inicialmente una cabecera AH o ESP, posteriormente se añade una nueva cabecera IP que es la que se utiliza para encaminar los

paquetes a través de la red. El modo túnel se usa normalmente cuando el destino final de los datos no coincide con el dispositivo que realiza las funciones IPSec.

El modo túnel es empleado principalmente por los *gateways* IPSec, con objeto de identificar la red que protegen bajo una misma dirección IP y centralizar de este modo el procesado del tráfico IPSec en un equipo. El modo túnel también es útil, cuando se utiliza junto con ESP, para ocultar la identidad de los nodos que se están comunicando. Otra aplicación del modo túnel, tanto con ESP como con AH, es poder establecer Redes Privadas Virtuales (RPV) a través de redes públicas, es decir, interconectar de forma segura redes de área local, incluso en el caso de que éstas usen direccionamiento privado o no legal en Internet.

a)

b)

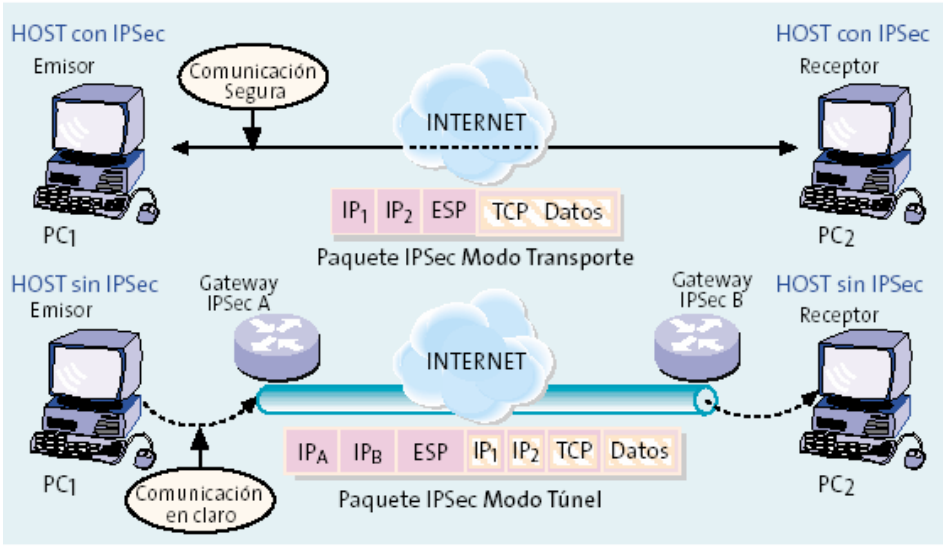


Figura 5.4 Los modos de funcionamiento transporte y túnel de IPSec.

IPSec puede ser implementado bien en un *host* o bien en un equipo dedicado, tal como un *router* o un *firewall,* que cuando realiza estas funciones se denomina *gateway* IPSec. La **Figura 5.4** muestra los dos modos de funcionamiento del protocolo IPSec, donde:

1. En la **Figura 5.4a** se representan dos *hosts* que entienden IPSec y que se comunican de forma segura. Esta comunicación se realiza en modo transporte, por tanto la información que se protege es únicamente el protocolo TCP o UDP, así como los datos de aplicación.

2. En la **Figura 5.4b** se muestran dos redes que utilizan para conectarse dos *gateways* IPSec y, por tanto, emplean una implementación en modo túnel. Se puede ver que la comunicación se realiza a través de una red de datos pública, entre un PC situado en una red local con otro PC situado en una red local remota, de modo que entre los *gateways* IPSec se establece un túnel a través del cual viajan protegidas las comunicaciones entre ambas redes locales. Sin embargo ambos PCs envían y reciben el tráfico en claro, como si estuviesen situados en la misma red local. Este esquema tiene la ventaja de que los nodos situados en redes separadas pueden comunicarse de forma segura y transparente, concentrándose, al mismo tiempo, las funciones de seguridad en un único punto, facilitando así las labores de administración.

5.4. IKE: EL PROTOCOLO DE CONTROL

Un concepto esencial en IPSec es el de asociación de seguridad (SA): es un canal de comunicación unidireccional que conecta dos nodos, a través del cual fluyen los datagramas protegidos mediante mecanismos criptográficos acordados previamente. Al identificar únicamente un canal unidireccional, una conexión IPSec se compone de dos SAs, una por cada sentido de la comunicación.

Hasta el momento se ha supuesto que ambos extremos de una asociación de seguridad deben tener conocimiento de las claves, así como del resto de la información que necesitan para enviar y recibir datagramas AH o ESP. Tal como se ha indicado anteriormente, es necesario que ambos nodos estén de acuerdo tanto en los algoritmos criptográficos a emplear como en los parámetros de control. Esta operación puede realizarse mediante una configuración manual, o mediante algún protocolo de control que se encargue de la negociación automática de los parámetros necesarios; a esta operación se le llama negociación de SAs.

El IETF ha definido el **protocolo IKE**[9] para realizar tanto esta función de gestión automática de claves como el establecimiento de las SAs correspondientes. Una característica importante de IKE es que su utilidad no se limita a IPSec, sino que es un protocolo estándar de gestión de claves que podría ser útil en otros protocolos, como, por ejemplo, OSPF o RIPv2.

---

[9] The Internet Key Exchange. RFC 2409.

IKE es un protocolo híbrido que ha resultado de la integración de dos protocolos complementarios:

ISAKMP y Oakley. ISAKMP define de forma genérica el protocolo de comunicación y la sintaxis de los mensajes que se utilizan en IKE, mientras que Oakley especifica la lógica de cómo se realiza de forma segura el intercambio de una clave entre dos partes que no se conocen previamente.

El objetivo principal de IKE consiste en establecer una conexión cifrada y autenticada entre dos entidades, a través de la cual se negocian los parámetros necesarios para establecer una asociación de seguridad IPSec. Dicha negociación se lleva a cabo en dos fases:

1. La fase común a cualquier aplicación, en la que ambos nodos establecen un canal seguro y autenticado.
   Dicho canal seguro se consigue mediante el uso de un algoritmo de cifrado simétrico y un algoritmo HMAC. Las claves necesarias se derivan de una clave maestra que se obtiene mediante un algoritmo de intercambio de claves Diffie-Hellman. Este procedimiento no garantiza la identidad de los nodos, para ello es necesario un paso adicional de autenticación.
   Existen varios métodos de autenticación, los dos más comunes se describen a continuación:

   - El primer método de autenticación se basa en el conocimiento de un secreto compartido que, como su propio nombre indica, es una cadena de caracteres que únicamente conocen los dos extremos que quieren establecer una comunicación IPSec. Mediante el uso de funciones *hash*

cada extremo demuestra al otro que conoce el secreto sin revelar su valor; así los dos se autentican mutuamente. Para no debilitar la seguridad de este mecanismo de autenticación, debe configurarse un secreto distinto para cada par de nodos, por lo que el número de secretos crece muy rápidamente cuando aumenta el número de nodos. Por esta razón en entornos en los que se desea interconectar muchos nodos IPSec la gestión de claves es muy complicada. En este caso no se recomienda el uso de autenticación mediante secreto compartido, sino autenticación basada en certificados digitales.

- En los estándares IPSec está previsto el uso de un método de autenticación que se basa en utilizar certificados digitales X509v3. El uso de certificados permite distribuir de forma segura la clave pública de cada nodo, de modo que éste puede probar su identidad mediante la posesión de la clave privada y ciertas operaciones de criptografía pública. La utilización de certificados requiere de la aparición de un elemento más en la arquitectura IPSec, la **PKI** (Infraestructura de Clave Pública), cuya integración se tratará con detalle más adelante.

2. En la segunda fase el canal seguro IKE es usado para negociar los parámetros de seguridad específicos asociados a un protocolo determinado, en nuestro caso IPSec.

Durante esta fase se negocian las características de la conexión ESP o AH y todos los parámetros necesarios. El equipo que ha iniciado la comunicación ofrecerá todas las posibles opciones que tenga configuradas en su política de seguridad y con la prioridad que se hayan configurado. El

sistema receptor aceptará la primera que coincida con los parámetros de seguridad que tenga definidos. Asimismo, ambos nodos se informan del tráfico que van a intercambiarse a través de dicha conexión.

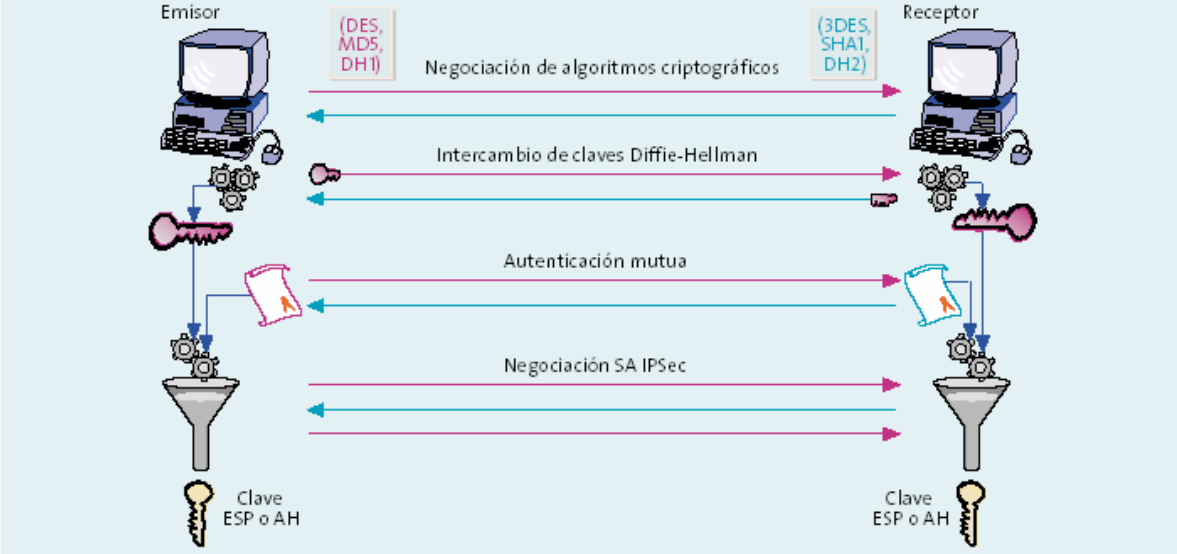


Figura 5.5 Funcionamiento del protocolo IKE.

En la **Figura 5.5** se representa de forma esquemática el funcionamiento del protocolo IKE y el modo en que se obtiene una clave de sesión, que es la que se utiliza para proteger las conexiones ESP o AH.

5.5. INTEGRACIÓN DE IPSEC CON UNA PKI

El uso de una PKI aparece en IPSec como respuesta a la necesidad de un procedimiento para autenticar de forma fiable a un conjunto de nodos que desean comunicarse mediante IPSec, siendo dicho conjunto de nodos muy numeroso. La

existencia de una PKI ofrece otras ventajas, ya que se centraliza el alta y baja de los usuarios, además se posibilita la introducción de tarjetas inteligentes para soportar los certificados, lo cual es muy interesante para la aplicación de IPSec en un entorno de teletrabajadores o usuarios móviles.

Bajo el nombre de PKI (Infraestructura de Clave Pública) se engloban todos los elementos y procedimientos administrativos que permiten emitir, revocar y, eventualmente, renovar los certificados digitales para una comunidad de usuarios. En el caso de IPSec los sujetos de los certificados son los nodos IPSec, mientras que la función de los certificados es proporcionar un medio fiable para autenticar la identidad de los dispositivos IPSec. Cada uno de los dispositivos IPSec dispondrá de un certificado digital que contendrá su clave pública y la información suficiente para identificar de forma unívoca al dispositivo (tal como su nombre DNS, su dirección IP o su número de serie). Esta asociación entre clave pública e identidad está avalada por la firma de la Autoridad de Certificación (en adelante CA) integrada en la PKI, que da validez al certificado. Se supone que todos los dispositivos IPSec reconocerán como válida la misma CA, para lo cual deberán disponer de una copia del certificado de la propia CA.

Los protocolos para la interacción de los dispositivos IPSec con una PKI no están especificados en ninguno de los protocolos de IPSec. Todos los fabricantes utilizan X.509v3[10] como formato común de los certificados, así como los estándares de la serie PKCS para la solicitud y descarga de certificados. Sin embargo, el protocolo de comunicaciones, mediante el cual los dispositivos IPSec dialogan con la PKI, no está totalmente estandarizado. Esto hace que existan varias alternativas según el fabricante de que se trate.

---

[10] Internet X.509 Public Key Infrastructure Certificate and CRL Profile. RFC 2459.

En general los nodos IPSec necesitan realizar ciertas operaciones básicas con una PKI: acceder al certificado de la CA, solicitar y descargar un certificado, así como comprobar la validez de un certificado recibido.

En la actualidad, la mayoría de los nodos IPSec realizan la validación de los certificados mediante consultas de la Lista de Certificados Revocados (CRL), que se almacena en el directorio de la PKI. Para ello, cada uno de los nodos mantendrá una copia de la CRL, que actualizará periódicamente mediante una consulta LDAP al directorio de la PKI. Típicamente, los periodos de actualización de la CRL serán del orden de horas, de modo que existirá cierto retardo desde que la PKI revoca un certificado hasta que todos los dispositivos tengan constancia de dicha revocación.

Para la solicitud y descarga de certificados existe un protocolo denominado SCEP[11], que se ha convertido en un estándar de facto en las operaciones de registro y descarga de certificados para aplicaciones IPSec. SCEP es un protocolo desarrollado originalmente por Cisco y Verisign, que se basa en el intercambio de mensajes PKCS, mediante protocolo HTTP, para automatizar los procesos de solicitud y descarga de certificados.

En la **Figura 5.6** se representan los flujos de comunicación entre una PKI y un nodo IPSec. Inicialmente, cada uno de los nodos genera un par de claves (pública y privada) y envía una petición de certificado a la CA, en la que incluye información de su identidad y su clave pública. Al mismo tiempo, el nodo descarga el certificado raíz de la CA; a continuación, la CA genera un certificado para el dispositivo IPSec y éste lo recibe. A partir de ese momento el nodo IPSec podrá usar su certificado en una negociación IKE para autenticarse frente a otros

---

[11] ANDREW NOURSE: *Internet Draft.* Febrero de 2001 (Draftnourse-scep-04.txt).

dispositivos. Periódicamente los dispositivos IPSec accederán al directorio de la PKI para actualizar la CRL.

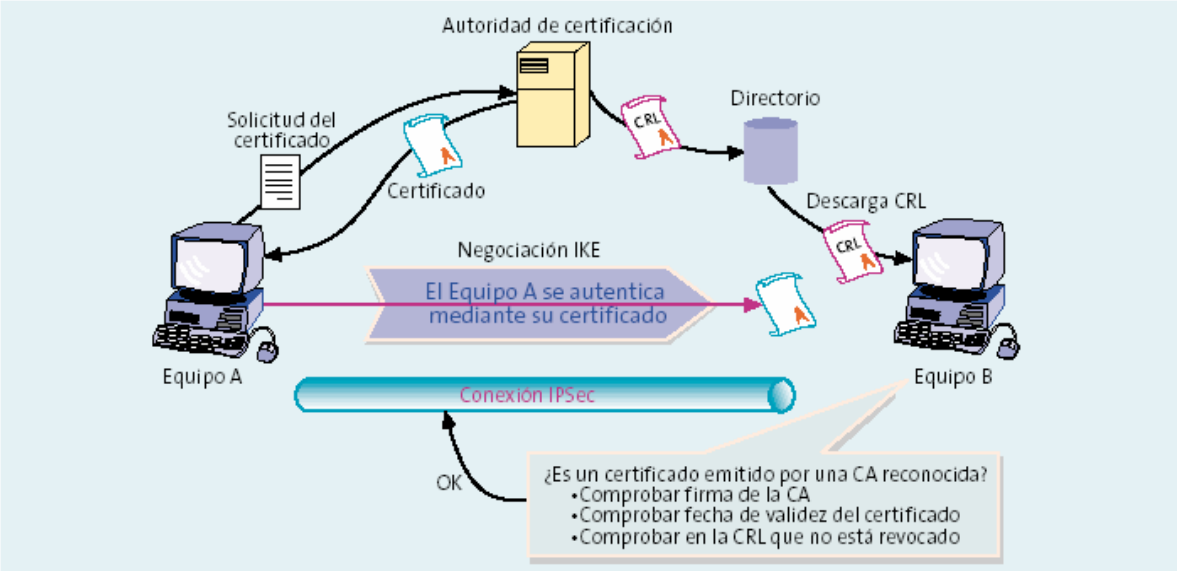


Figura 5.6 Integración de una PKI en IPSec.

5.6 SERVICIOS DE SEGURIDAD OFRECIDOS POR IPSec

En este apartado se analizan las características de los servicios de seguridad que ofrece IPSec. Dichos servicios son:

5.6.1 Integridad y autenticación del origen de los datos.

El protocolo AH es el más adecuado si no se requiere cifrado. La opción de autenticación del protocolo ESP ofrece una funcionalidad similar, aunque esta protección, a diferencia de AH, no incluye la cabecera IP. Como se comentó anteriormente, esta opción es de gran importancia para aquellas

aplicaciones en las cuales es importante garantizar la invariabilidad del contenido de los paquetes IP.

5.6.2 Confidencialidad

El servicio de confidencialidad se obtiene mediante la función de cifrado incluida en el protocolo ESP. En este caso es recomendable activar la opción de autenticación, ya que si no se garantiza la integridad de los datos el cifrado es inútil. Esto es debido a que aunque los datos no pudiesen ser interpretados por nadie en tránsito, éstos podrían ser alterados haciendo llegar al receptor del mensaje tráfico sin sentido que sería aceptado como tráfico válido.

Además de ofrecer el cifrado del tráfico, el protocolo ESP también tiene herramientas para ocultar el tipo de comunicación que se está realizando; para ello permite introducir caracteres de relleno en el contenido de los datos del paquete, de modo que se oculta la verdadera longitud del mismo. Ésta es una protección útil contra las técnicas de análisis de tráfico, que permiten a un atacante deducir información útil a partir del estudio de las características del tráfico cifrado. El análisis de tráfico es un riesgo que debe considerarse seriamente, recientemente se ha documentado[12] la viabilidad para deducir información a partir del tráfico cifrado de una conexión SSH. Es previsible que este tipo de ataques se harán más habituales y sofisticados en el futuro, conforme se generalice el cifrado de las comunicaciones.

---

[12] Análisis de tráfico del protocolo SSH, versión 1: *http://www.openwall.com/advisories/OW-003-sshtraffic-analysis.txt*

5.6.3 Detección de repeticiones

La autenticación protege contra la suplantación de la identidad IP, sin embargo un atacante todavía podría capturar paquetes válidos y reenviarlos al destino. Para evitar este ataque, tanto ESP como AH incorporan un procedimiento para detectar paquetes repetidos. Dicho procedimiento está basado en un número de secuencia incluido en la cabecera ESP o AH, el emisor incrementa dicho número por cada datagrama que envía y el receptor lo comprueba, de forma que los paquetes repetidos serán ignorados.

Esta secuencia no podrá ser modificada por el atacante, debido a que se encuentra protegida por medio de la opción de integridad para cualquiera de los dos protocolos (AH y ESP) y cualquier modificación en este número provocaría un error en la comprobación de la integridad del paquete.

5.6.4 Control de acceso: autenticación y autorización

Dado que el uso de ESP y AH requiere el conocimiento de claves, y dichas claves son distribuidas de modo seguro mediante una sesión IKE en la que ambos nodos se autentican mutuamente, existe la garantía de que sólo los equipos deseados participan en la comunicación. Es conveniente aclarar que una autenticación válida no implica un acceso total a los recursos, ya que IPSec proporciona también funciones de autorización. Durante la negociación IKE se especifica el flujo de tráfico IP que circulará a través de la conexión IPSec. Esta especificación es similar a un filtro de paquetes, considerándose el protocolo, las direcciones IP de los puertos origen y

destino, el byte "TOS" y otros campos. Por ejemplo, puede utilizarse IPSec para permitir el acceso desde una sucursal a la red local del centro corporativo, pero impidiendo el paso de tráfico hacia máquinas especialmente protegidas.

5.6.5 No repudio

El servicio de no repudio es técnicamente posible en IPSec, si se usa IKE con autenticación mediante certificados digitales. En este caso, el procedimiento de autenticación se basa en la firma digital de un mensaje que contiene, entre otros datos, la identidad del participante. Dicha firma, gracias al vínculo entre la clave pública y la identidad que garantiza el certificado digital, es una prueba inequívoca de que se ha establecido una conexión IPSec con un equipo determinado, de modo que éste no podrá negarlo. En la práctica, sin embargo, esta prueba es más compleja, ya que requeriría almacenar los mensajes de negociación IKE y, además, no está definido un procedimiento para referenciar este evento a una fecha concreta.

5.7 APLICACIONES PRACTICAS DE IPSec

La tecnología IPSec permite construir soluciones de comunicaciones que ofrecen confidencialidad y autenticación en la capa IP, independientemente de cual sea el medio de transporte (FR, PPP, xDSL o ATM). Además, la inclusión de seguridad en la capa IP tiene la ventaja de que se extiende universalmente, ofreciendo un

nivel de seguridad homogéneo de manera independiente del tipo que sean las aplicaciones, siempre que estén basadas en IP.

En este apartado veremos como el protocolo IPSec proporciona una solución viable para tres escenarios:

5.7.1 Interconexión segura de redes locales.
5.7.2 Acceso seguro de usuarios remotos.
5.7.3 Extranet o conexión de una corporación con sus *partners* y proveedores.

Para cada uno de los escenarios mencionados se desarrolla una aplicación práctica concreta y se presentan las ventajas de utilizar IPSec.

5.7.1 LA INTERCONEXIÓN SEGURA DE REDES LOCALES (INTRANET)

La mayoría de las corporaciones utiliza IP como medio de transporte universal, y las que todavía no usan IP tienen planes de migrar completamente a esta tecnología en un futuro próximo. Asimismo, la naturaleza distribuida de las empresas hace necesaria una infraestructura de comunicaciones que interconecte todas sus oficinas o puntos de venta. Por *intranet* se entiende una red de comunicaciones basada en una infraestructura de comunicaciones pública o privada que conecta todos los puntos de trabajo de una empresa y que tiene como medio común IP.

En la **Figura 5.7** se muestra un ejemplo de *intranet* en entorno financiero. Dicha *intranet* conecta todas las oficinas bancarias con el centro de proceso de datos (CPD) de un gran banco. La seguridad es vital en este entorno, y los requisitos de confidencialidad e integridad de las comunicaciones se cubren perfectamente mediante el uso de la tecnología IPSec.

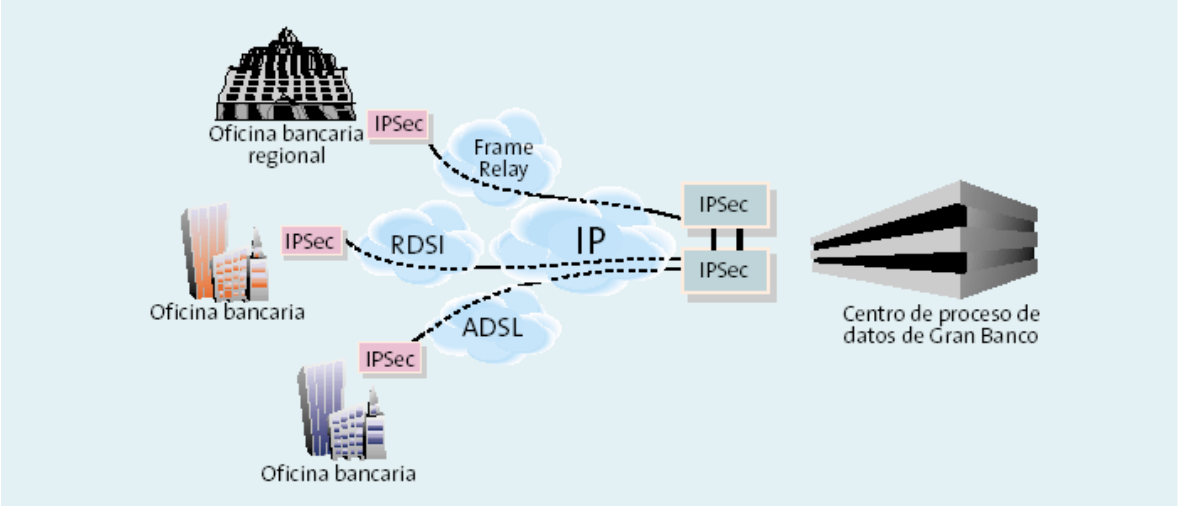


Figura 5.7 Interconexión de redes locales en entorno financiero.

En la actualidad, incluso las oficinas bancarias más pequeñas disponen de una infraestructura informática que consta de una red local con varios PCs que usan una variedad de aplicaciones y protocolos para los que es imposible o muy costoso añadir mecanismos de seguridad. Sin embargo, todo el tráfico de esta red local está basado en IP o puede ser encapsulado en IP, de modo que la instalación de un *gateway* IPSec es la mejor solución para garantizar la seguridad de las comunicaciones de la oficina con el exterior.

Como puede observarse en la **Figura 5.7**, es habitual que las oficinas bancarias, debido a su elevado número, presenten una gran diversidad de tecnologías de acceso. Para grandes bancos con presencia multinacional y oficinas dispersas en

muchos países esta diversidad será mayor, de forma que incluso podría plantearse la conexión de algunas oficinas directamente a través de Internet. En cualquier caso, IPSec garantiza la protección de las comunicaciones con independencia de la tecnología de acceso empleada.

En cuanto al centro de proceso de datos, los requisitos críticos son la fiabilidad y la capacidad para mantener un elevado número de sesiones simultáneas. En el mercado están disponibles *gateways* IPSec comerciales que incorporan la posibilidad de configuración redundante y el establecimiento de 25.000 túneles simultáneos o más. Estas prestaciones son suficientes incluso para las redes bancarias más grandes.

5.7.2 EL ACCESO SEGURO DE USUARIOS REMOTOS

La gran mayoría de las empresas necesitan proporcionar a sus usuarios algún procedimiento para el acceso remoto a los recursos corporativos. Estos usuarios con necesidades de acceso remoto pueden ser agentes de ventas, teletrabajadores o directivos en viaje de negocios; en todos los casos se requiere la necesidad de poder acceder de forma segura a los sistemas informáticos de la empresa a cualquier hora y en cualquier lugar, incluso en el extranjero. Además, las previsiones de futuro apuntan a que estas necesidades de acceso remoto van a crecer espectacularmente.

La tecnología IPSec permite comunicar el PC del usuario remoto a las máquinas del centro corporativo, de modo que se soporten todas las aplicaciones IP de

forma transparente. Mediante la instalación de un software en el PC, denominado "cliente IPSec", es posible conectar remotamente dicho equipo móvil a la red local de la corporación de forma totalmente segura, con la ventaja de que el usuario remoto, desde cualquier lugar del mundo, del mismo modo que si estuviese físicamente en su oficina, podrá:

- Leer y enviar correo.
- Acceder a discos compartidos en red.
- Acceder al servidor web corporativo.
- Consultar la agenda.

El uso del estándar IPSec permite garantizar la confidencialidad y la autenticación de las comunicaciones extremo a extremo, de modo que esta solución de acceso remoto se integra perfectamente con los sistemas de seguridad de la red corporativa.

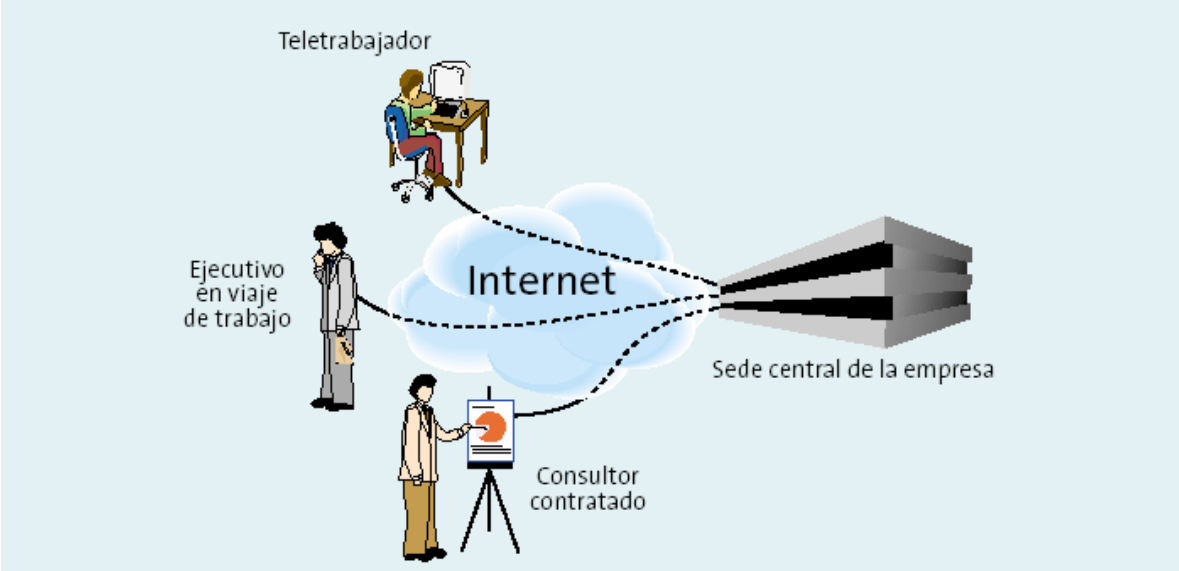


Figura 5.8 Acceso seguro de usuarios remotos a una corporación.

En la **Figura 5.8** se presenta un escenario típico de acceso remoto seguro a una corporación. En nuestro ejemplo esta corporación, o empresa, se dedica a la producción de software informático. Esta empresa, al igual que cualquier compañía del sector de las tecnologías de la información, comparte una serie de características únicas. Podemos destacar la deslocalización de los recursos humanos, ya que cada vez es más habitual que los empleados trabajen fuera de su oficina, bien por estar en viaje de trabajo o bien por estar en su casa como teletrabajadores. También será muy frecuente la colaboración en proyectos de consultores externos contratados, para los cuales es necesario habilitar acceso a los recursos de la empresa.

Dada la creciente competitividad en el sector informático, la protección de la propiedad intelectual, de la información estratégica y de nuevos productos, e incluso de la propia imagen de la empresa, imponen requisitos de control de acceso y de confidencialidad que hacen imprescindible la implantación de un sistema de acceso remoto que sea suficientemente seguro.

El protocolo IPSec permite construir una solución que cumple estos requisitos de seguridad. En este entorno, los usuarios remotos dispondrán de un software instalado en su PC de trabajo que les permitirá establecer una conexión segura con la red local de la compañía. La variedad de sistemas operativos no supone dificultad alguna, ya que todos los sistemas operativos recientes como Windows 2000 o Solaris 8 incluyen un cliente IPSec. Asimismo, para los sistemas operativos más difundidos, y que no integran IPSec, existen aplicaciones de cliente IPSec, tanto comerciales como de libre distribución. Incluso existe un cliente IPSec para Palm Pilot.

Para garantizar la seguridad de esta solución y evitar intrusiones, como las que han afectado a Microsoft y otras corporaciones en el pasado[13], es necesario complementar la tecnología IPSec con el uso, en los equipos remotos, de cortafuegos personales y autenticación fuerte mediante certificados digitales X.509 residentes en tarjeta inteligente.

Desde el punto de vista del administrador de la red informática de la corporación, los requisitos prioritarios serán la facilidad de gestión y la necesidad de autenticar de forma fiable a cada usuario. La integración de IPSec con una infraestructura de clave pública (PKI) proporciona una respuesta adecuada a estos requisitos.

5.7.3 LA EXTRANET

Por *extranet* se entiende una red de comunicaciones que interconecta a una empresa con todos los agentes con los cuales mantiene relaciones comerciales: consumidores, proveedores y *partners.* En este escenario la interoperabilidad que ofrece el estándar IPSec es una ventaja clave frente a otras soluciones; cada empresa comprará equipos de fabricantes distintos, pero todos ellos podrán conectarse de forma segura utilizando IPSec como lenguaje común.

La tendencia actual es la aparición de *extranets* en las que convergen todas las empresas que participan en un mismo sector productivo. Previsiblemente, el comercio electrónico negocio a negocio (B2B) evolucionará en este sentido, para proporcionar puntos de encuentro virtuales en los que se establezcan relaciones

---

[13] Para ampliar esta información visitar la página: http://news.zdnet.co.uk/story/0,,s2082326,00.html

comerciales de empresa a empresa de forma segura. Estos mercados virtuales especializados se articularán de forma natural en torno a la elaboración de un producto o la provisión de un servicio concreto: fabricación del automóvil y el tipo de industria que lleva asociada, distribución y comercialización de alimentos, sector asegurador, etc.

En nuestro caso tomaremos como ejemplo el sector asegurador: una *extranet* que conecte las compañías aseguradoras y los agentes de ventas debe cumplir unos estrictos requisitos de seguridad, que incluso están regulados por normativas legales. Este es un ejemplo claro en el que IPSec aparece como la solución más apropiada, dado que es una tecnología avalada por estándares internacionales, garantiza la interoperabilidad entre los equipos de distintos fabricantes y proporciona el más alto nivel de seguridad gracias a las técnicas criptográficas más modernas.

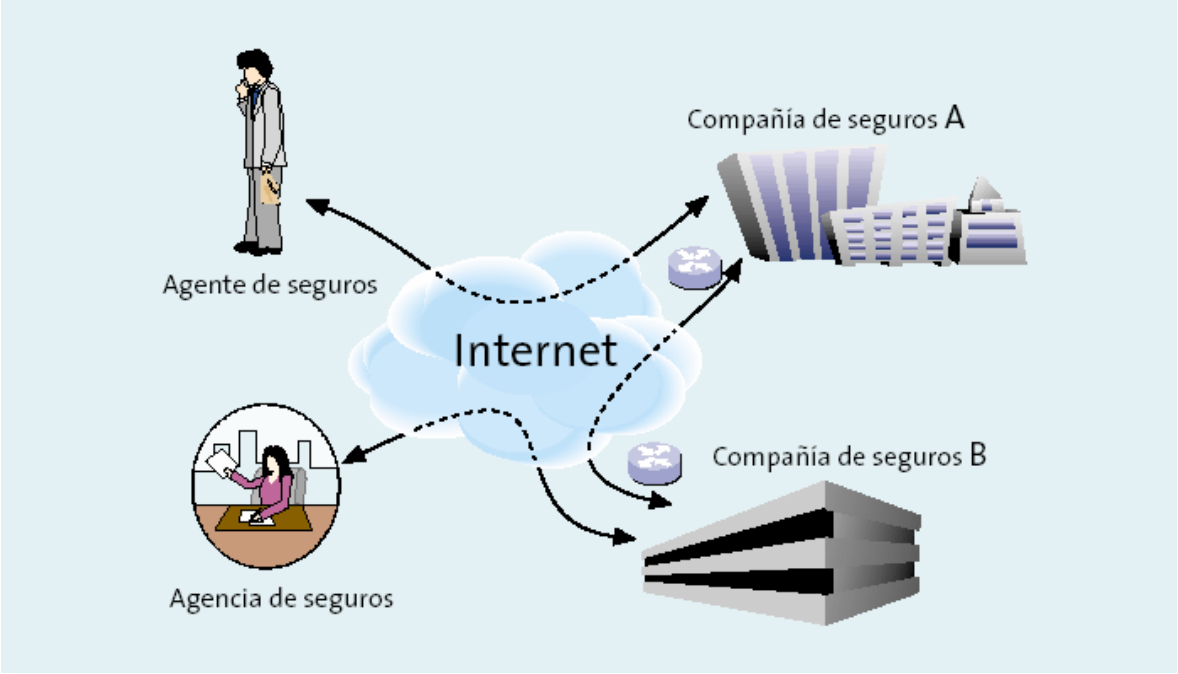


Figura 5.9 Extranet aplicada en el sector de seguros.

En la **Figura 5.9** se muestra un esquema de una *extranet* para el sector de seguros. En dicha figura se puede observar como dos compañías se comunican de forma segura para intercambiar información sobre las pólizas de seguros. Al mismo tiempo los agentes de ventas y las oficinas de seguros pueden acceder a la información comercial necesaria para su negocio. Una *extranet* como esta puede llevarse a cabo perfectamente usando IPSec; para ello se requiere la instalación de un *gateway* IPSec en cada uno de los puntos de presencia de la *extranet,* mientras que el equipamiento de los agentes de ventas se reduce a un PC portátil con un cliente IPSec.

Tecnología	Puntos Fuertes	Puntos Débiles	En desarrollo
IPSec	• Opera independiente de las aplicaciones de niveles superiores. • Subconjunto de IPv6. • Ocultación de direcciones de red sin emplear NAT. • Acoplamiento con las técnicas criptográficas existentes y futuras.	• No proporciona la gestión de usuarios. • Interoperabilidad entre los fabricantes. • No estandarizado.	• Estandarización de todas las facetas de PKI, incluyendo los protocolos de intercambio de certificados y el formato de éstos. • El IETF está en su desarrollo.
PPTP	• Soporta tunneling extremo a extremo y entre servidores. • posibilidad de valor añadido para el acceso remoto. • Proporciona una capacidad multiprotocolo. • Empleo de encriptación RSA RC-4.	• No proporciona encriptación de datos para los servidores de acceso remoto. • Precisa un servidor NT como terminador del tunel. • Sólo usa encriptación RSA RC-4.	• Integración con IPSec.
L2F	• Habilita el tunneling multiprotocolo. • Soportado por la gran mayoría de fabricantes.	• No posee encriptación. • Autenticación débil. • No dispone de control de flujo sobre el tunel.	• Implementaciones que empleen el nombre de usuario y dominio en el establecimiento del túnel.
L2TP	• Combina L2f y PPTP. • Necesidad de una red de paquetes para operar bajo X.25 y Frame Relay.	• No existencia de mecanismos de protección del tráfico de control y datos	• Estandarización y operación en proceso. • Será adoptado por los fabricantes para el acceso remoto una vez completo.

Tabla 5.3 Comparativa global entre las diferentes tecnología VPN.

Características	Descripción	PPTP/ PPP	L2TP/ PPP	L2TP/ IPSec	Transporte IPSec	Túnel IPSec
Autenticación de usuario	Puede autenticar al usuario que está iniciando las comunicaciones.	Si	Si	Si	WIP[14]	WIP
Autenticación del equipo	Permite autenticar los equipo implicados en las telecomunicaciones	Si	Si	Si	Si	Si
Compatible con NAT	Puede pasar por traductores de direcciones de red para ocultar uno o ambose xtremos de las comunicaciones	Si	Si	No	No	No
Compatibilidad multiprotocolo	Define un método estándar para transmitir tráfico IP y no IP.	Si	Si	Si	No	WIP
Asignación dinámica de direcciones IP de túnel	Define una forma estándar de negociar una dirección IP para la parte de túnel de las comunicaciones. Es importante para que los paquetes devueltos se enruten de vuelta a través de la misma sesión en vez de a través de una ruta sin túnel e insegura y para eliminar la configuración manual estática del sistema	Si	Si	Si	No disponible	WIP

	final.					
Cifrado	Puede cifrar el tráfico que transmite.	Si	Si	Si	Si	Si
Utiliza PKI	Puede utilizar PKI para implementar el cifrado y/o la autenticación.	Si	Si	Si	Si	Si
Autenticidad de paquetes	Proporciona un método de autenticidad para asegurarse de que el contenido del paquete no se modifica mientras se transmite.	No	No	Si	Si	Si
Compatibilidad multidifusión	Puede transmitir tráfico multidifusión IP además del tráfico IP de difusión simple.	Si	Si	Si	No	Si

Tabla 5.4 Comparación entre los protocolos de seguridad, indicando las diferentes características que los distinguen.

[14] Las tarjetas inteligentes son dispositivos que permiten alojar información en un microprocesador al cual se puede acceder y leer o escribir información según sea la aplicación donde se utilicen.

CONCLUSIONES

Actualmente las redes privadas virtuales se han convertido en una necesidad para las organizaciones modernas. Muchas de ellas eligen establecer estas redes desconociendo los peligros a los que es expuesta la información que viaja a través de ella. Una VPN no representa una solución completa, y no brinda protección total a una red, solo protege el canal por donde transitan los datos de un extremo a otro, pero no brinda ninguna protección con respecto a las intrusiones que puedan existir en las computadoras (virus, ataques de hackers, etc.), es decir, si uno de los extremos de la VPN o de una conexión segura host-to-host se compromete, se pierde la protección.

La aparición de los protocolos de tunelaje como otra alternativa además de las costosas líneas dedicadas, para la interconexión de redes privadas a través de una red pública, permitió que cada vez mas empresas adoptaran estos servicios. Estos protocolos han ido evolucionando junto con las redes que interconectan. Entre estos avances están el desarrollo de métodos que garantizan la integridad y autenticación del origen de los datos, la confidencialidad y el control de acceso, factores importantes a la hora de evaluar la seguridad ofrecida por una tecnología de interconexión como lo son los protocolos de tunelaje.

Algunas recomendaciones para alcanzar un buen nivel de seguridad en una red serían crear una política de seguridad que contemple todos los recursos de una red y los usuarios que hay en ella, además de complementarla con IPSec en las conexiones que requieran seguridad, un Firewall para complementar el control de acceso, sistemas de detección de intrusos, instalación de los parches de sistemas

operativos según corresponda, que los usuarios utilicen claves de accesos a sus computadoras, etc.

IPSec es un estándar de seguridad extraordinariamente potente y flexible. Su importancia reside en que aborda una carencia tradicional en el protocolo IP: la seguridad. Gracias a IPSec ya es posible el uso de redes IP para aplicaciones críticas, como las transacciones comerciales entre empresas. Al mismo tiempo, es la solución ideal para aquellos escenarios en que se requiera seguridad, independientemente de la aplicación, de modo que es una pieza esencial en la seguridad de las redes IP.

El protocolo IPSec es ya uno de los componentes básicos de la seguridad en las redes IP. En este momento se puede considerar que es una tecnología suficientemente madura para ser implantada en todos aquellos escenarios en los que la seguridad es un requisito prioritario. Se ha descrito, desde un punto de vista técnico, las características del protocolo IPSec, así como los servicios de seguridad que proporciona. También presentamos varios ejemplos de aplicaciones prácticas en las que IPSec se constituye como la solución más apropiada para garantizar la seguridad de las comunicaciones.

IPSec trabaja a nivel de red, las líneas futuras de investigación seria desarrollar una variación de IPSec end-to-end, es decir, que asegure la transmisión de datos o proteja dichos datos de sistema a sistema o de usuario a usuario, es decir, una aplicación parecida a SSH pero que trabaje a nivel de red.

BIBLIOGRAFÍA

VPNC, 2004, *Definiciones y requerimientos en cuanto al tema de VPN (Virtual Private Network).* *http://www.vpnc.org*

IETF,1996, *Grupo de trabajo en ingeniería de Internet.*
http://www.ietf.org

TELEM@TICA,2003, *Revista de las tecnologías de la información y las comunicaciones. Edición No.18 Octubre 31.*
http://www.cujae.edu.cu/revistas/telematica

MICROSOFT CORPORATION,1998, *PPTP Frecuently Asked Questions.*
http://www.microsoft.com/ntserver/productinfo/faqs/PPTPfaq.asp

IP SECURITY PROTOCOL (IPSec), *IETF page.*
http://www.ietf.org/html.charters/ipsec-charter.html

RFC2401, *Request For Comment desarrollado por la IETF sobre el protocolo IPSec.* *http://www.ietf.org/rfc/rfc2410.txt*

PROTOCOL DICTIONARY, 2005, *Web con información sobre las arquitecturas de los protocolo (PPP, PPTP, L2F, L2TP, IPSEC).*
http://www.javvin.com/dictionary.html

SERVICIO DE ACCESO REMOTO,2004, *web con información sobre los servicios RAS.* *http://fmc.axarnet.es/winnt4svr/indice_m.htm*

RFC 1194, IETF 1996, *PPP Challenge Handshake Authentication Protocol.* *http://www.ietf.org/rfc/rfc1994.txt*

RFC 2637, IETF, *Point-To-Point Tunneling Protocol.* *http://www.ietf.org/rfc/rfc2637.txt.*

MICROSOFT CORPORATION. *PPTP Frequently asked Questions.* http://www.microsoft.com/ntserver/ProductInfo/faqs/PPTPfaq.asp

MICROSOFT CORPORATION. *Virtual Private Networking: Frequently Asked Questions.* *http://www.microsoft.com/windowsserver2003/techinfo/overview/vpnfaq.mspx*

RFC 2406, IETF 1998, *IP Encapsulating Security Payload (ESP).* *http://www.ietf.org/rfc/rfc2406.txt.*

RFC 3193, IETF 2001, *Request For Comment desarrollado por la IETF sobre el protocolo L2TP.* *http://www.ietf.org/rfc/rfc2661.txt.*

RFC2401, 1998*, S. Kent. BBN Corp. R. Atkinson. @Home Network. Security Architecture for the Internet Protocol. Network Working Group. Request for Comments: 2401 Category: Standards Track. November 1998.* *http://www.ietf.org/rfc/rfc2401.txt*

RFC2402, 1998*, S. Kent. BBN Corp. R. Atkinson. @Home Network. IP Authentication Header. Network Working Group. Request for Comments: 2402 Category: Standards Track. November 1998.*
http://www.ietf.org/rfc/rfc2402.txt

RFC2409, 1998, D. Harkins, D. Carrel, Cisco Systems. The Internet Key Exchange (IKE). Network Working Group. Request for Comments: 2409 *Category: Standards Track. November 1998.*
http://www.ietf.org/rfc/rfc2409.txt

IETF, 1996, *Grupo de trabajo en Ingeniería de Internet.*
http://www.ietf.org

WILIAM STALLINGS, 2000, *COMUNICACIONES Y REDES DE COMPUTADORES. . España: Editorial Prentice Hall 6ª edición. Capitulo 18 Seguridad en Redes.*

ANEXOS

Anexo A.

ESPECIFICACION TECNICA DE UN EQUIPO VPN EDGE

Anexo B.

ESPECIFICACION TECNICA DE UN EQUIPO VPN GATEWAY / FIREWALL

Anexo C.

ESPECIFICACION TECNICA DE UN EQUIPO VPN FIREWALL