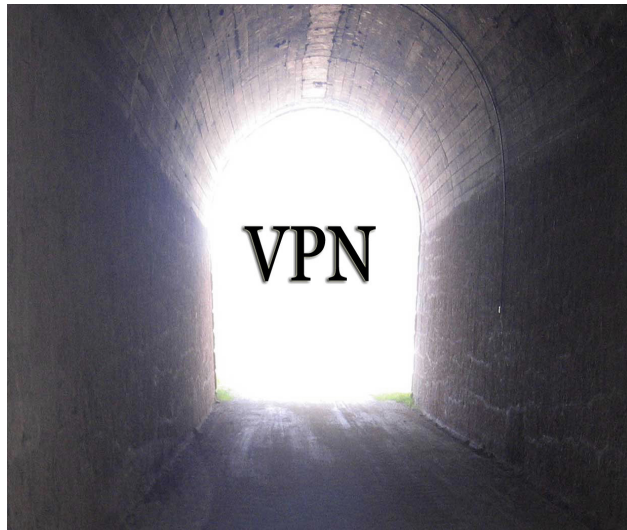




Universidad Nacional del Nordeste
Facultad de Ciencias Exactas, Naturales y Agrimensura

Trabajo de Adscripción
“Nuevas Tendencias en Redes Virtuales Privadas”



Alumno: Gerardo G. Brollo - L.U.: 34.610
Profesor: Mgter. David L. la Red Martínez
Asignatura: Teleproceso y Sistemas Distribuidos
Licenciatura en Sistemas de Información
Corrientes - Argentina

2010

Índice general

1. Redes Virtuales Privadas	1
1.1. Introducción	1
1.2. Tecnologías Anteriores a las VPNs	3
1.2.1. Enlaces Dedicados	3
1.2.2. Enlaces Conmutados	10
1.2.3. PPP - Protocolo Punto a Punto	13
2. Tunelamiento VPN	19
2.1. Etapas Necesarias para una Conexión VPN	19
2.1.1. Conexión	19
2.1.2. Control de Conexión	20
2.1.3. Autenticación	21
2.1.4. Cifrado	22
2.1.5. Control de Acceso	28
2.2. Tunelamiento	32
2.2.1. Funcionamiento del Túnel	33
2.2.2. Tipos de Túneles	34
3. Protocolos VPN	39
3.1. PPTP - Protocolo de Túnel Punto a Punto	39
3.1.1. Relación Entre PPP Y PPTP	40
3.1.2. Componentes de una VPN PPTP	41
3.1.3. Estructura del Protocolo	43
3.1.4. Conexión de Control	43
3.1.5. Operación del Túnel	43
3.1.6. Cabecera Mejorada GRE	44
3.1.7. Cifrado en PPTP	44
3.1.8. Filtrado de Paquetes PPTP	45
3.1.9. Control de Acceso a los Recursos de la Red	45

3.2.	L2TP - Protocolo de Túnel de Capa 2	45
3.2.1.	Componenetes Básicos de un Túnel L2TP	46
3.2.2.	Topología de L2TP	46
3.2.3.	Estructura del Protocolo L2TP	47
3.2.4.	Formato de una Cabecera L2TP	48
3.2.5.	Autenticación en L2TP	50
3.2.6.	Procesos de una Comunicación L2TP	50
3.2.7.	Comparativa Entre PPTP y L2TP	51
3.2.8.	Problemas de L2TP	52
3.3.	IPSec (Internet Protocol Security)	52
3.3.1.	Componentes de IPSec	53
3.3.2.	Bases de Datos de Seguridad	55
3.3.3.	Authentication Header (AH)	58
3.3.4.	Encapsulating Security Payload - ESP	60
3.3.5.	Internet Key Exchange - IKE	63
3.3.6.	Arquitecturas VPN con IPsec	65
3.3.7.	Limitaciones de IPSec	68
3.4.	VPN-SSL	68
3.4.1.	SSL/TLS Secure Sockets Layer/Transport Layer Security	69
3.4.2.	Arquitectura de SSL	70
3.4.3.	Funcionamiento Básico de SSL	72
3.4.4.	Aplicaciones e Implementaciones de SSL	74
3.4.5.	Conceptos y Técnicas de VPN-SSL	74
3.4.6.	Inconvenientes de las VPN-SSL	76
3.4.7.	Ventajas de SSL-VPN sobre IPSec	76
3.4.8.	Software VPN-SSL	77
	Bibliografía	83
	Índice alfabético	85

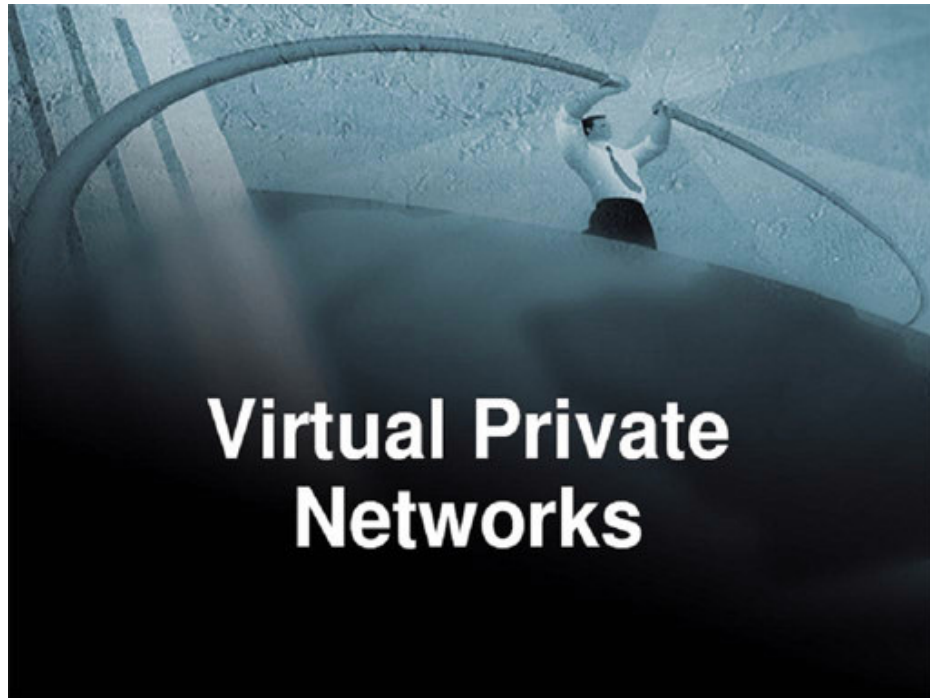
Índice de figuras

1.1. Tecnologías Anteriores a las VPNs.	3
1.2. Esquema Básico de una Red Frame Relay.	5
1.3. Escenario Frame Relay.	6
1.4. Interfaz Frame Relay.	6
1.5. Escenario Típico de una Red Frame Relay.	8
1.6. Dispositivos que Intervienen en una Red ATM.	9
1.7. Caminos Virtuales.	9
1.8. Enlaces Conmutados.	10
1.9. Escenario Típico de una Conexión Analógica de Datos Sobre la RTPC.	11
1.10. Enlaces Analógicos de Último Kilómetro de Ambos Lados.	11
1.11. Adaptador de Terminal RDSI.	12
1.12. Acceso Remoto a Redes.	14
1.13. Red Virtual Privada sobre RAS.	14
1.14. Formato de Trama PPP.	18
2.1. Etapas Necesarias Para Establecer un Túnel VPN.	20
2.2. Esquema Criptográfico.	23
2.3. Servidores Radius de Autenticación.	26
2.4. Esquema de Cifrado con Llave Pública.	27
2.5. Control de Acceso Cliente-Servidor.	28
2.6. Objetos en Active Directory.	31
2.7. Esquema General de Active Directory de Microsoft.	32
2.8. Túneles Voluntarios.	35
2.9. Túneles Obligatorios.	36
2.10. Modelos de Entunelamiento.	37
3.1. Estructura de un Túnel PPTP.	41
3.2. Formato del Paquete IP.	44

3.3. Escenario Típico L2TP.	47
3.4. Relación Entre Tramas PPP y Mensajes L2TP.	48
3.5. Formato de Cabecera L2TP.	48
3.6. Formato de Trama IPSec en Modo Transporte y Túnel.	54
3.7. Ejemplo de una Entrada de Base de Datos de Políticas de Seguridad.	57
3.8. Cabecera de Autenticación AH.	59
3.9. Nuevo Paquete IP Procesado con ESP.	61
3.10. Funcionamiento del Protocolo IPSec.	62
3.11. Protocolo IPSec en Modo Transporte.	63
3.12. Protocolo IPSec en Modo Túnel.	63
3.13. Negociación de Llaves en IKE.	66
3.14. IPsec Sobre Distintas Redes.	67
3.15. Estructura de Protocolos del Protocolo SSL.	71
3.16. Intercambio de Mensajes en SSL.	73
3.17. Advertencia de Instalación de Plugins en Internet Explorer.	75
3.18. Interfaz GUI de OpenVPN Para Sistemas Operativos Windows.	79

Capítulo 1

Redes Virtuales Privadas



1.1. Introducción

La expresión *Redes Virtuales Privadas* se ha hecho muy popular en estos días, pero probablemente muchas personas tengan apenas una idea de su

significado.

A menudo se la asocia con la conectividad de las empresas, cuando trabajadores remotos acceden a la red corporativa, pero actualmente el concepto está ganando popularidad entre los usuarios domiciliarios y las pequeñas organizaciones [1].

Con una *red privada virtual*, dos o más ordenadores o redes remotas pueden conectarse entre sí, de forma segura, para formar una red local virtual que utiliza una infraestructura pública como Internet, como medio para transmitir datos internos.

Se denomina red privada virtual porque no se trata de una red física, pero tiene todas las características de una red de área local (LAN, Local Area Network).

Estas clases de redes virtuales son construidas sobre la infraestructura de una red pública (recurso público, sin control sobre el acceso de los datos), normalmente Internet. Es decir, en vez de utilizarse enlaces dedicados para conectar redes remotas, se utiliza la infraestructura de Internet; una vez que las redes están conectadas es transparente para los usuarios.

La principal motivación para la implantación de las VPNs es la financiera: los enlaces dedicados son demasiado caros, principalmente cuando las distancias son largas. Por otro lado existe Internet, que por ser una red de alcance mundial, tiene puntos de presencia diseminados por el mundo.

Internet es una red pública, donde los datos en tránsito pueden ser *leídos por cualquier equipo*. La *seguridad* en la comunicación entre las redes privadas es imprescindible, se hace necesaria una forma de cambiar los datos codificados, de forma que si fuesen capturados durante la transmisión no puedan ser descifrados. Los datos se transiten codificados por Internet en *túneles virtuales* creados por dispositivos VPNs que utilizan criptografía; esos dispositivos que son capaces de *entender* los datos codificados forman una *red virtual* sobre la red pública. Es esa red virtual la que es conocida como *VPN*.

Los dispositivos responsables para la formación y administración de la red virtual, para proporcionar una comunicación segura, deben ser capaces de garantizar la *seguridad*, *integridad* y *autenticación* de los datos que están siendo transmitidos o recibidos.

1.2. Tecnologías Anteriores a las VPNs

Desde el principio de los tiempos, la humanidad ha tenido la necesidad de comunicarse. Paralelamente también ha existido la necesidad de hacerlo de manera privada, es decir que el mensaje sólo le llegue a determinados receptores.

En las redes de comunicaciones pasa exactamente lo mismo. En especial el sector corporativo siempre ha requerido la implementación de enlaces privados para transportar de forma segura toda su información confidencial. Este capítulo trata sobre la manera en que se realizan los enlaces privados, y las diferentes tecnologías que los soportan.

En la figura 1.1 de la pág. 3 se presenta un esquema resumido de las tecnologías anteriores a las VPNs.

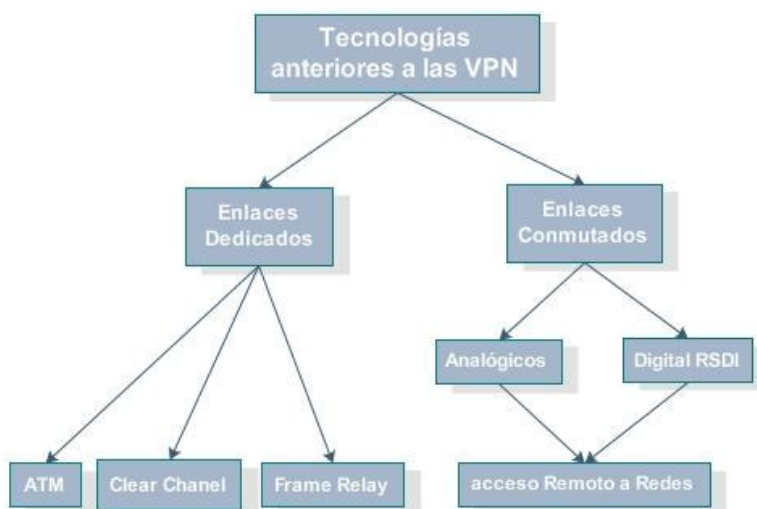


Figura 1.1: Tecnologías Anteriores a las VPNs.

1.2.1. Enlaces Dedicados

Los enlaces dedicados, como su nombre lo indica, son conexiones permanentes punto-punto, o punto-multipunto, que se valen de una infraestructura de transporte de Capa 1 o de conmutación (Capa 1 y 2). Los primeros son

comúnmente llamados enlaces Clear Channel y los segundos son enlaces Frame Relay o ATM.

Clear Channel

Son enlaces donde sólo interviene la red de transporte del proveedor de servicios. Para el mercado corporativo comúnmente van desde los 64 kbit/s hasta los 2048 kbit/s. Los enlaces *Clear Channel* ofrecen un rendimiento efectivo casi del 100 % ya que no usan ningún tipo de encapsulación de nivel 2, es decir, no hay presentes cabeceras de ningún tipo.

Por lo general, la compañía (o cliente en general) debe tener un puerto disponible DTE que cumpla con las especificaciones técnicas del equipo de comunicaciones entregado por el proveedor. Típicamente la mayoría de los equipos que se usan para recibir los enlaces Clear Channel por parte del cliente son enrutadores o switches de nivel 3. Son éstos los que se encargan de manejar los niveles 2 y 3.

En general, las topologías de los enlaces Clear Channel son robustas pero a su vez estáticas. Esto significa que para aumentar o disminuir la velocidad del enlace es necesario cambiar equipos o manipularlos localmente. Lo que se transfiere al cliente en indisponibilidades del servicio no deseadas.

Vale la pena aclarar, que los enlaces Clear Channel fueron la primera tecnología WAN que se adoptó usando la infraestructura de voz de los distintos operadores de telefonía locales, nacionales e internacionales. Como era de esperarse, por provenir de una tecnología que no había sido pensada para transmitir datos fue superada rápidamente por otros tipos de tecnologías como Frame Relay y ATM, aunque aún muchas empresas siguen teniendo enlaces Clear Channel. La figura 1.2 de la pág. 5 muestra un esquema básico, donde se observa la transparencia para una organización del enlace Clear Channel contratado.

Frame Relay

Frame Relay es un protocolo WAN de alto rendimiento que trabaja en la capa física y de enlace de datos del modelo de referencia OSI. Frame Relay fue diseñado originalmente para trabajar con redes RDSI. Frame Relay es una tecnología de *conmutación de paquetes*, que permite compartir dinámicamente el medio y por ende el ancho de banda disponible. La longitud de los paquetes es variable para hacer más eficiente y flexible las transferencias de datos. Estos paquetes son conmutados por varios segmentos de la red hasta que llegan hasta

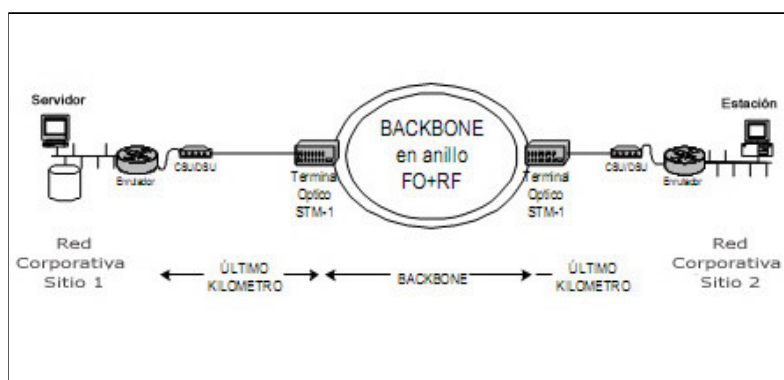


Figura 1.2: Esquema Básico de una Red Frame Relay.

el destino final. Todo el acceso al medio en una red de conmutación de paquetes es controlado usando técnicas de *multiplexación estadística*, por medio de las cuales se minimizan la cantidad de demoras y/o colisiones para acceder al medio.

Ethernet y *Token Ring*, los protocolos de redes LAN más usados, también usan conmutación de paquetes y técnicas de difusión.

Frame Relay es una evolución de las redes X.25, no hace retransmisión de paquetes perdidos ni windowing, características que sí ofrecía su antecesor ya que en los años 70 (época en la que aparece X.25) los medios físicos no eran tan confiables como los de hoy día, y por tanto se necesitaba mayor robustez. Todas las ventajas que ofrecen los medios de hoy día, han posibilitado a *Frame Relay* ofrecer un alto desempeño y una gran eficiencia de transmisión [9].

Una conexión *Frame Relay* usa dispositivos que pueden dividirse en dos categorías: Equipos Terminales de Datos (DTEs) y Equipos Terminales de Circuitos de Datos (DCEs). La figura 1.5 de la pág. 8 ilustra la ubicación de los DTEs y los DCEs en un red *Frame Relay*.

Los DTEs son generalmente considerados equipos terminales de una red específica y típicamente son enrutadores, computadores personales, terminales o bridges. Estos equipos se localizan en las premisas del cliente y en la mayoría de los casos son propiedad de los mismos.

Los DCEs son dispositivos normalmente propiedad del carrier. El propósito de los equipos DCEs es proveer o generar señales de reloj y conmutar los paquetes de la red. Por lo general, son llamados packet switches o conmutadores de paquetes.

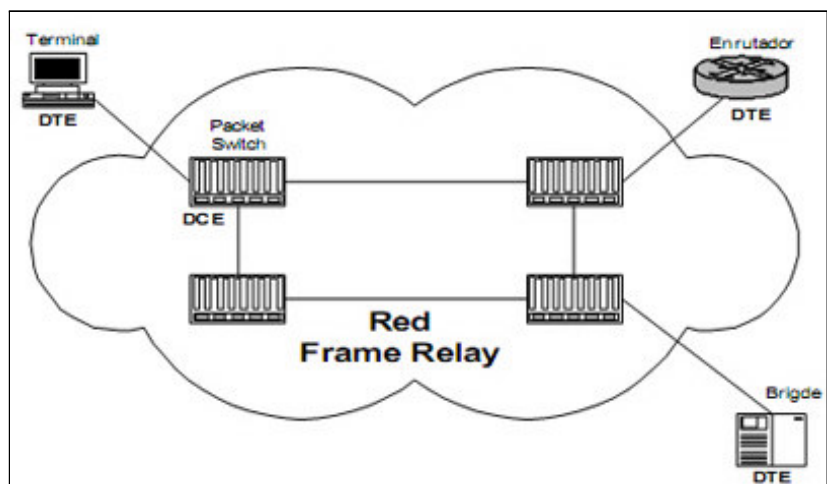


Figura 1.3: Escenario Frame Relay.



Figura 1.4: Interfaz Frame Relay.

En la conexión entre los dispositivos DCE y DTE intervienen dos componentes, uno de nivel físico y otro de nivel de enlace de datos. En el nivel físico se definen todas las características físicas, eléctricas y mecánicas entre los dos, y el nivel de enlace de datos define todas las especificaciones Frame Relay o Frame Relay LMI según sea el caso.

Circuitos virtuales Frame Relay

Frame Relay es una tecnología WAN que usa enlaces orientados a conexión, esto significa que una comunicación se define entre un par de dispositivos y que cada una de las conexiones existentes en la red tiene un identificador asociado particular. Este servicio es implementado usando circuitos virtuales, los cuales son conexiones lógicas creadas entre dos dispositivos DTE a través de la red conmutada de paquetes Frame Relay. Un circuito lógico puede crearse a través de múltiples dispositivos intermediarios DCE dentro de la red Frame Relay.

Los circuitos virtuales Frame Relay se pueden dividir en dos categorías:

Circuitos Virtuales Conmutados (SVCs): son conexiones temporales y que se usan en situaciones donde la transferencia de datos entre un par de dispositivos DTE es esporádica a través de la red Frame Relay.

Circuitos Virtuales Permanentes (PVCs): son conexiones establecidas permanentemente y que se usan en donde la transferencia de datos es continua entre dos dispositivos DTE. Este tipo de conexiones no requieren hacer una llamada de configuración ni de terminación como en los SVCs.

ATM (Asynchronous Transfer Mode)

El Modo de Transferencia Asíncrono (ATM) es un estándar desarrollado por la Unión Internacional de Telecomunicaciones (ITU-T) para transmitir múltiples tipos de servicios, tales como voz, video y datos usando técnicas de conmutación de celdas pequeñas de tamaño fijo. Las redes ATM son, al igual que las redes Frame Relay, orientadas a conexión [9].

ATM es una tecnología de multiplexación y de conmutación de celdas que combina los beneficios de una red de conmutación de circuitos (capacidad garantizada, retardos constantes) y de una red de conmutación de paquetes (flexibilidad y eficiencia para tráfico intermitente). Permite transmisiones desde unos pocos megabits por segundo hasta cientos de gigabits por segundo.

Su naturaleza asíncrona, hace de ATM una tecnología más eficiente que las síncronas tales como TDM. En TDM a los usuarios se les asigna un timeslot,

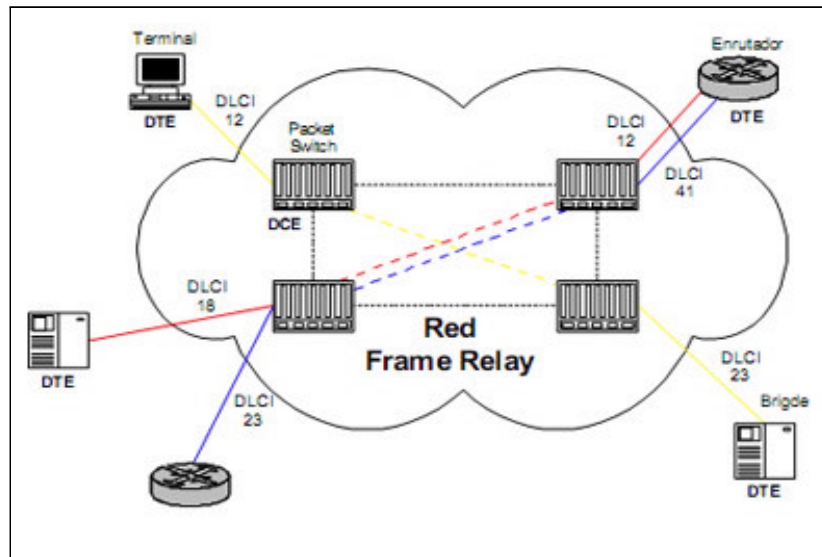


Figura 1.5: Escenario Típico de una Red Frame Relay.

y ningún otro cliente puede transmitir en ese timeslot así el propietario no este transmitiendo. Esto hace que la red no sea muy eficiente. En ATM los timeslots siempre están disponibles y se asignan por demanda basándose en la información que está contenida en las cabeceras de cada celda.

Conexiones Virtuales ATM Las redes ATM son básicamente redes orientadas a conexión, esto significa que se tienen que configurar canales virtuales (VC) a través de la red para la adecuada transferencia de datos. Haciendo la analogía con Frame Relay, un canal virtual equivale a un circuito virtual.

En ATM existen dos tipos de conexiones: los *caminos virtuales* (Virtual Paths - VPs), los cuales son identificados por medio de VPIs (Virtual Path Identifiers), y los *canales virtuales*, los cuales son identificados con una combinación de VPIs y de VCI (Virtual Channel Identifier).

Un camino virtual es una suma de canales virtuales, cada uno de los cuales es conmutado transparentemente sobre la red ATM. La figura 1.7 de la pág. 9 muestra esta relación entre VCs y VPs.

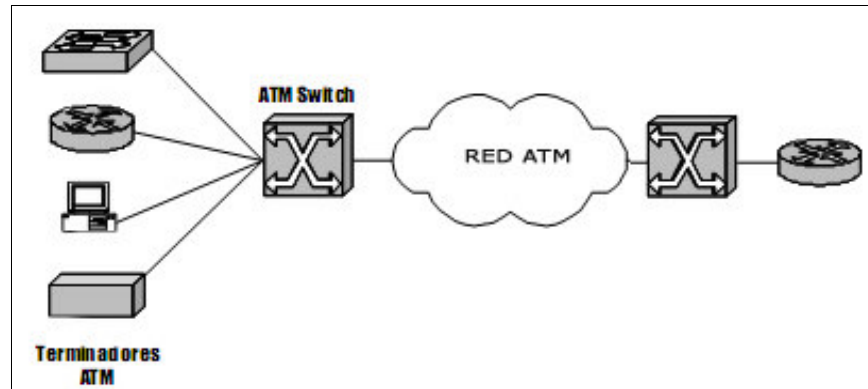


Figura 1.6: Dispositivos que Intervienen en una Red ATM.

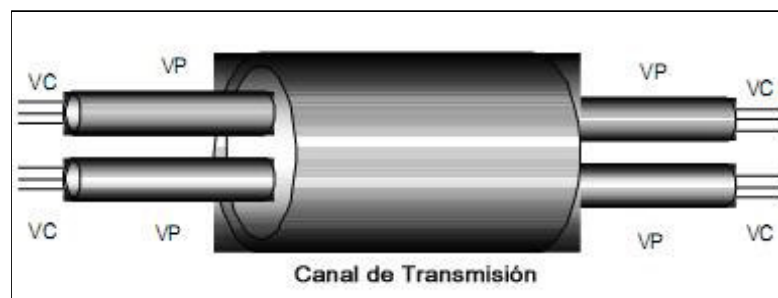


Figura 1.7: Caminos Virtuales.

1.2.2. Enlaces Conmutados

Los enlaces conmutados se dividen en dos tipos: los analógicos y los digitales. Los primeros llegan hasta velocidades de 53 kbit/s para el downlink y hasta de 48 kbit/s para el uplink, los segundos transmiten y reciben a 64 kbit/s o 128 kbit/s. Estos últimos son conocidos como enlaces RDSI (o ISDN, en inglés) que son las siglas de *Red Digital de Servicios Integrados*. Mediante estos enlaces se pueden establecer un *Acceso Remoto a una Red*, el antecesor más próximo a las VPN.

En la figura 1.8 de la pág. 10 se muestra un esquema de los distintos tipos de *enlaces conmutados*.



Figura 1.8: Enlaces Conmutados.

Enlaces Conmutados Analógicos

Fue quizá la primera tecnología de transmisión de datos que usó el hombre para construir redes privadas entre dos sitios remotos. Esto lo hizo aprovechando la *Red de Telefonía Pública Conmutada - RTPC (PSTN, en inglés)*, dicha red ha tenido muchos desarrollos en los últimos 20 años. El servicio tradicional que la RTPC ha prestado ha sido comunicación de voz, y sólo recientemente se empezó a usar para soportar un creciente mercado de transferencia de datos.

En un enlace conmutado de datos, intervienen varios equipos desde el usuario inicial hasta el punto o equipo destino. La figura 1.9 de la página 11 muestra los componentes de un enlace típico de datos sobre la red telefónica pública, se puede notar la necesidad de realizar una conversión A/D y

otra D/A. La inercia que resulta de todo este proceso electrónico es la que en últimas limita a 56 kbit/s una comunicación analógica, que incluso puede llegar a 33.6 kbit/s cuando aparece una tercera y cuarta conversión entre la Central Telefónica 2 y el terminador de la llamada.

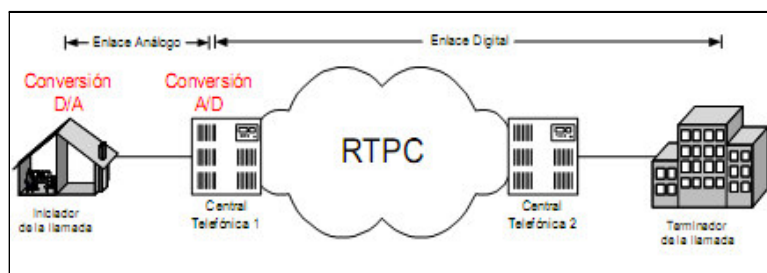


Figura 1.9: Escenario Típico de una Conexión Analógica de Datos Sobre la RTPC.

Se puede notar que la conexión entre el iniciador de la llamada y la central telefónica es analógica, y se lleva a cabo usando el mismo par de cobre de la línea telefónica, para esto se usa un modem analógico, mientras que en el lado del sitio remoto la conexión es digital, y para esto se usan enlaces RDSI.

Cuando este enlace es también analógico, entonces se puede notar que en el proceso total de la conexión intervienen cuatro conversiones, dos A/D y dos D/A, esto hace que la velocidad de transmisión y de recepción máximas sean apenas de 33.6 kbit/s. La figura 11 ilustra este escenario.

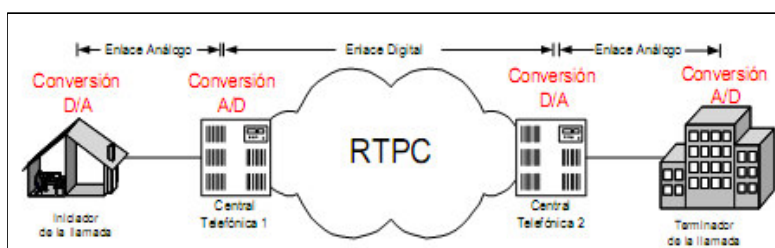


Figura 1.10: Enlaces Analógicos de Último Kilómetro de Ambos Lados.

Enlaces Conmutados Digitales - RDSI

La *Red Digital de Servicios Integrados* (RDSI), es un sistema de telefonía digital que se desarrollo hace más de una década. Este sistema permite transmitir voz y datos simultáneamente a nivel global usando 100% conectividad digital.

En *RDSI*, la voz y los datos son transportados sobre canales B (del inglés Bearer) que poseen una velocidad de transmisión de datos de 64 kbit/s, aunque algunos switches ISDN limitan esta capacidad a solo 56 kbit/s. Los canales D (o canales de datos) se usan para señalización y tiene velocidades de 16 kbit/s o 64 kbit/s dependiendo del tipo de servicio.

Los dos tipos básicos de servicio RDSI son: BRI (del inglés Basic Rate Interface) y PRI (del inglés Primary Rate Interface). Un enlace BRI consiste de dos canales B de 64 kbit/s y un canal D de 16 kbit/s para un total de 144 kbit/s. Este servicio está orientado a brindar capacidad de conexión para usuarios residenciales.

Para acceder a un servicio BRI, es necesario tener una línea RDSI. Si sólo se desean comunicaciones de voz es necesario tener teléfonos digitales RDSI, y para transmitir datos es necesario contar con un adaptador de Terminal - TA (del inglés Terminal Adapter) o un enrutador RDSI.

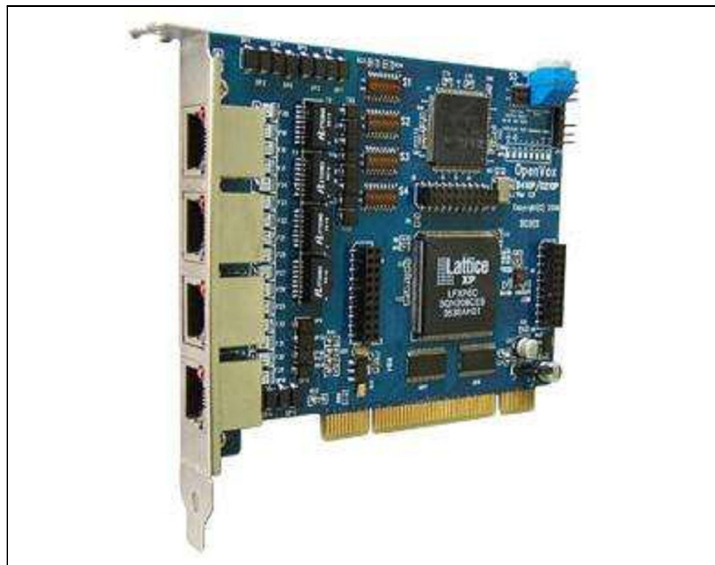


Figura 1.11: Adaptador de Terminal RDSI.

A diferencia de las conexiones *conmutadas analógicas* en una conexión RD-SI el camino es 100% digital desde la central hasta el sitio del abonado, por lo cual no existe ningún tipo de conversiones A/D o viceversa, lo que facilita la obtención de velocidades de 64 kbit/s o 128 kbit/s, lo cual se logra convirtiendo los dos canales B de 64 kbit/s o en un canal lógico de 128 kbit/s. Esta característica es usada solo en transmisión de datos y depende de la facilidad que tenga el equipo terminal de realizar esto. Típicamente esta característica tiene el nombre de Multilink.

Acceso Remoto a Redes

Generalmente cuando hablando de *Servicio de Acceso Remoto* lo relacionamos con un *enlace conmutado* ya sea analógico o digital en escenarios como los descritos en el apartado anterior.

En este tipo de arquitecturas existe un RAS (*Remote Access Server*) que actúa como una puerta de enlace entre el cliente remoto y la red (ver figura 1.12 de la página 14). Después de que un usuario haya establecido la conexión por medio de una llamada, la línea telefónica es transparente para el usuario, y este puede tener acceso a todos los recursos de la red como si estuviera ante un equipo directamente conectado a ella. Se podría decir que el RAS hace que un módem actúe como una tarjeta de red al proyectar un equipo remoto sobre una LAN.

Este tipo de implementación fue el antecesor más próximo de las VPN, sus deficiencias radican en los costos de las llamadas que se deben efectuar, principalmente las de larga distancias y la falta de confidencialidad en la transmisión de la información ya que no soportan encriptación de datos. Un punto a favor para este tipo de conexiones es que no necesita acceso a Internet (o correr sobre TCP-IP en todo caso) como las VPN.

Hoy en día los clientes lo utilizan para conectarse con un Proveedor de Servicios Internet (ISP, Internet Service Provider), también es muy común utilizarlo para realizar la conexión a Internet, la que luego se utilizará para establecer una VPN. En la figura 1.13 de la página 14 se puede apreciar un escenario típico de una VPN sobre una *Conexión de Acceso Remoto*.

1.2.3. PPP - Protocolo Punto a Punto

El Protocolo Punto a Punto (PPP) es un protocolo WAN de nivel de enlace estandarizado en el documento RFC 1661, 1662, 1663. Por tanto, se trata de un protocolo asociado a la pila TCP/IP de uso en Internet. Proporciona un

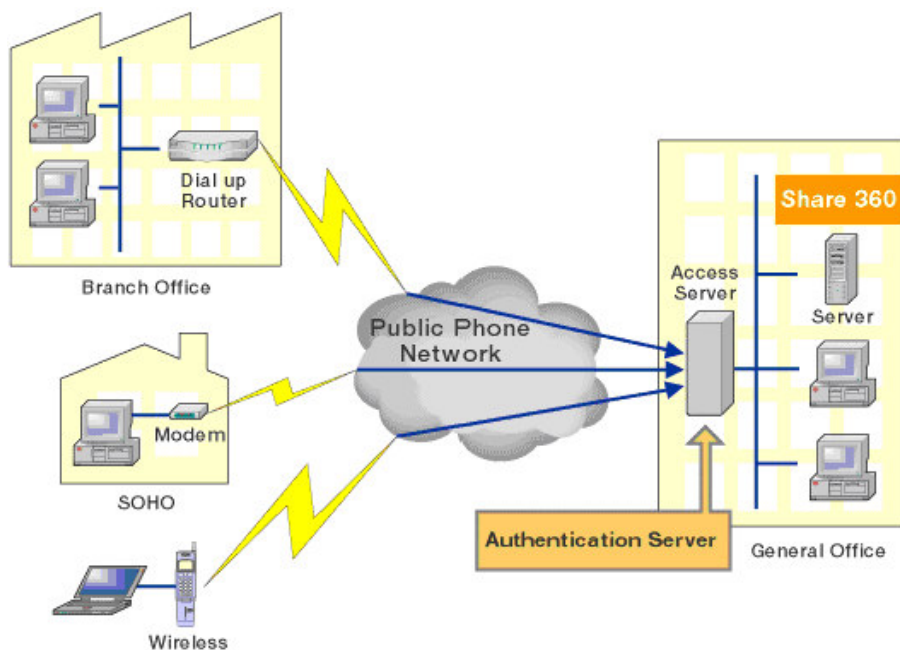


Figura 1.12: Acceso Remoto a Redes.

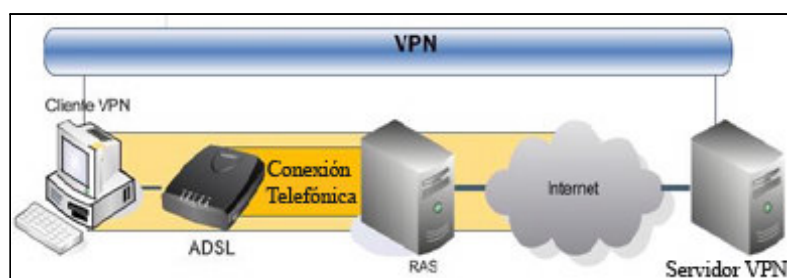


Figura 1.13: Red Virtual Privada sobre RAS.

método estándar para transportar datagramas multiprotocolo sobre enlaces simples punto a punto entre dos *pares*. Estos enlaces proveen operación bidireccional full dúplex y se asume que los paquetes serán entregados en orden.

Generalmente, se utiliza para establecer la conexión a Internet de un particular con su proveedor de acceso a través de un módem telefónico. Ocasionalmente también es utilizado sobre conexiones de banda ancha (como PPPoE o PPPoA). Otro uso que se ha venido dando es utilizarlo para conectar a trabajadores desplazados (p. ej. ordenador portátil) con sus oficinas a través de un *centro de acceso remoto* de su empresa.

Este protocolo cuenta con tres componentes:

1. Un *mecanismo de enmarcado* (armado de tramas) que delinea sin ambigüedad el final de la trama y el inicio de la siguiente. Permite la detección de errores.
2. Un protocolo de *control de enlace* (LCP, Link Control Protocol) para establecer, configurar y probar la conexión de datos.
3. Una familia de protocolos de *control de red* (NCPs, NetworkControl Protocols) para establecer y configurar los distintos protocolos de nivel de red.

Fases de PPP

Existen cuatro fases distintivas de negociación en una sesión de marcación del PPP. Cada una de estas cuatro fases debe completarse de manera exitosa antes de que la conexión del PPP esté lista para transferir los datos del usuario:

Fase Previa: se establece una conexión física por ejemplo, un modem realiza una llamada telefónica al modem del ISP.

Fase1: *Establecer el enlace del PPP.*

PPP utiliza el *protocolo de control de enlace LCP* para establecer, mantener y terminar la conexión física. Durante la fase LCP inicial, se seleccionan las opciones básicas de comunicación. Nótese que durante la fase de establecimiento de enlace (Fase 1), se seleccionan los protocolos de Autenticación, pero no se implementan efectivamente hasta la fase de Autenticación de conexión (Fase 2). De manera similar, durante el LCP, se toma una decisión en cuanto a que si dos iguales negociarán el uso de compresión y/o encriptación. Durante la Fase 4 ocurre la elección real de algoritmos de compresión / encriptación y otros detalles. Entonces se puede decir que los parámetros que son determinados mediante el protocolo LCP en esta fase son:

- Tamaño máximo de la trama - 1500 bytes por omisión.
- Negociar multivínculo para conexiones de un solo vínculo. Esta opción permite la separación de canales de alta y baja prioridad en una conexión de un solo vínculo. Si el servidor de acceso remoto acepta esta característica, puede apreciar un aumento en la calidad del audio. Sin embargo, puesto que esta característica es incompatible con muchos servidores de acceso remoto, no debe habilitarla a menos que se le indique lo contrario.
- Selección (solamente) del método de autenticación.
- Selección (solamente) del protocolo NCP de capa 3. Por ejemplo, el NCP de TCP/IP es el Protocolo de control de protocolo Internet (IPCP, Internet Protocol Control Protocol).

Fase 2: *Autenticar al usuario.*

La mayoría de las implementaciones del PPP proporcionan métodos limitados de Autenticación, típicamente el Protocolo de autenticación de contraseña (PAP), el Protocolo de autenticación de saludo Challenge (CHAP) y Microsoft Challenge Handshake Authentication Protocol (MSCHAP). Vale aclarar que esta fase *no es obligatoria*.

Una variante es el uso de EAP - Protocolo de Autenticación Extensible, que constituye una extensión de PPP. Proporciona un mecanismo estándar para aceptar métodos de autenticación adicionales, permite añadir módulos de verificación en ambos extremos. Al utilizar EAP, se pueden agregar varios esquemas de autenticación, entre los que se incluyen:

- *Tarjetas de Identificación.*
- *Autenticación por Clave Pública* mediante tarjetas inteligentes, certificados y otros.

Fase 3: *Control de rellamado del PPP.*

La implementación de Microsoft del PPP incluye una Fase opcional de *control de rellamado*. Esta fase utiliza el Protocolo de Control de Rellamado (CBCP) inmediatamente después de la fase de autenticación. Si se configura para rellamado, después de la autenticación, se desconectan tanto el cliente remoto como el NAS. Entonces, el NAS vuelve a llamar al cliente remoto en el número telefónico especificado. Esto proporciona un nivel adicional de seguridad a las redes de marcación. El NAS permitirá conexiones a partir

de los *clientes remotos* que físicamente residan sólo en números telefónicos específicos, lo que implica que este nivel de seguridad sólo se puede usar en un escenario donde la conexión a Internet sea sólo a través de Dial-Up o ADSL.

Fase 4: *Invocar los protocolo(s) a nivel de red.*

Una vez que se hayan terminado las *fases previas*, PPP invoca los distintos Protocolos de Control de Red (NCPs) que se seleccionaron durante la fase de establecimiento de enlace (Fase1) para configurar los protocolos que utiliza el cliente remoto. Por ejemplo, durante esta fase el Protocolo de control de IP (IPCP) puede asignar una dirección dinámica a un usuario de marcación.

Para configurar un protocolo de red se usa el protocolo NCP correspondiente. Por ejemplo, si la red es IP, se usa el protocolo IPCP para asignar la dirección IP del cliente y sus servidores DNS.

En la implementación del PPP de Microsoft, el protocolo de control de compresión se utiliza para negociar tanto la compresión de datos (utilizando MPPC) como la encriptación de datos (utilizando MPPE) por la simple razón de que ambos se implementan en la misma rutina.

Fase 5: *Transferencia de datos.*

Una vez que se han terminado las cuatro fases de negociación, PPP empieza a transferir datos hacia y desde los dos iguales. Cada paquete de datos transmitidos se envuelve en un encabezado del PPP el cual quita el sistema receptor. Si se seleccionó la compresión de datos en la fase 1 y se negoció en la fase 4, los datos se comprimirán antes de la transmisión. Si se seleccionaron y se negociaron de manera similar la encriptación de datos, los datos (comprimidos opcionalmente) se encriptarán antes de la transmisión.

Fase 6 : *Finalización del enlace.*

PPP puede terminar el enlace en cualquier momento. Esto puede ocurrir por la pérdida de la señal portadora, una falla de autenticación, una falla de la calidad del enlace, la expiración de un timer, o un cierre administrativo del enlace. LCP es usado para cerrar el enlace a través de un intercambio de paquetes de *terminación*. Cuando el enlace ha sido cerrado, PPP informa a los protocolos de capa de red así ellos pueden tomar la acción apropiada.

Trama PPP

Una trama PPP está basada en HDLC. Tiene un mínimo de 6 bytes y un máximo indeterminado. La trama HDLC con PPP es:

El formato de marco de PPP se escogió de modo que fuera muy parecido al

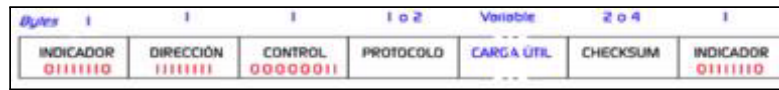


Figura 1.14: Formato de Trama PPP.

formato de marco de HDLC, ya que no había razón para reinventar la rueda. La diferencia principal entre PPP y HDLC es que el primero está orientado a caracteres. PPP, al igual que SLIP, usa el relleno de caracteres en las líneas por discado con módem, por lo que todos los marcos tienen un número entero de bytes.

Capítulo 2

Tunelamiento VPN

2.1. Etapas Necesarias para una Conexión VPN

Toda solución VPN que se requiera implementar, cualquiera sea el protocolo o tecnología a usar, debe cumplir con las siguientes etapas (ver figura 2.1 de la página 20)¹:

2.1.1. Conexión

Establecer la conexión en una de *Red Virtual Privada* es muy similar a establecer una *conexión punto a punto* mediante conexiones de acceso telefónico o de enrutamiento de marcado a petición, es más, en casos como PPTP se usa el mismo protocolo de base (PPP). Hay dos tipos de conexiones VPN:

Conexión VPN de acceso remoto: un cliente de acceso remoto (el equipo de un usuario) realiza una conexión VPN de acceso remoto que conecta a una red privada. El servidor VPN proporciona acceso a los recursos del servidor VPN o a toda la red a la que está conectado el *servidor VPN*. Los paquetes enviados desde el cliente remoto a través de la *conexión VPN* se originan en el equipo cliente de acceso remoto.

Conexión VPN de enrutador a enrutador: un enrutador realiza una *conexión VPN de enrutador a enrutador* que conecta dos partes de una red privada. El servidor VPN proporciona una conexión enrutada a la red a la que está conectado el servidor VPN. En una conexión VPN de enrutador a

¹Existen protocolos como L2TP que no proporcionan encriptación de datos, será necesario combinarlo con otro protocolo como IPsec, para que éste le brinde el servicio de encriptación en una capa inferior (capa 3).

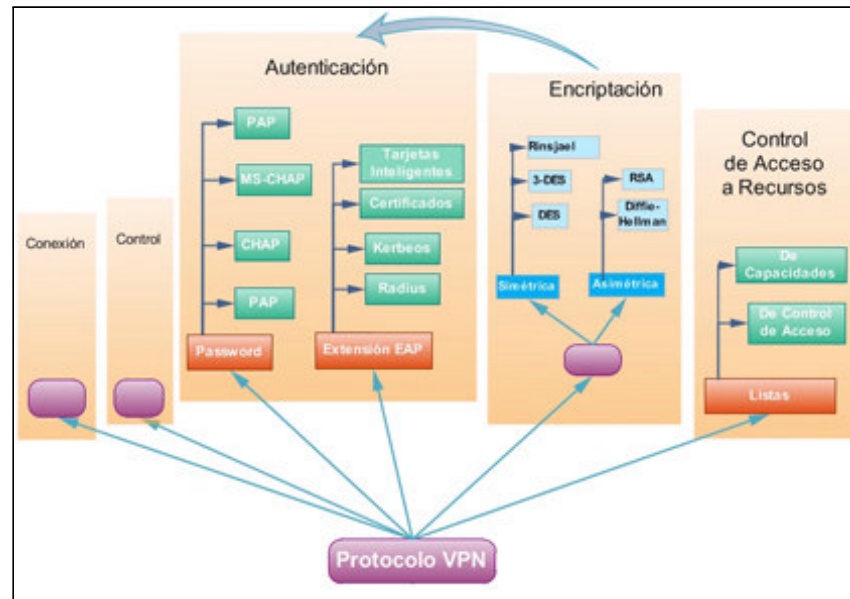


Figura 2.1: Etapas Necesarias Para Establecer un Túnel VPN.

enrutador, los paquetes enviados desde uno de los enrutadores a través de la conexión VPN normalmente no se originan en los enrutadores.

Durante esta etapa se seleccionan las opciones básicas de la comunicación, donde se presenta una negociación de parámetros necesarios para establecer el *túnel*. Ejemplos de estos parámetros son el método de Autenticación (ej.: CHAP, PAP, IKE, etc.), algoritmo de Cifrado, el uso de Compresión, opciones de Rellano, tamaño de la Trama, etc.

2.1.2. Control de Conexión

El control de la conexión es una etapa que está presente desde el establecimiento de la conexión hasta que finaliza la misma. Su objetivo es mantener la conexión estable, esto se puede implementar dentro del mismo túnel VPN o por medio de una conexión paralela. Por ejemplo en el protocolo PPTP, existe una *conexión de Transmisión* UDP (puerto 43), y otra *conexión de Control* TCP (puerto 1723) para el control del túnel.

2.1.3. Autenticación

La *autenticación* es el acto de verificar la identidad de alguien o algo en un contexto definido. En un mundo de seis mil millones de personas no es suficiente simplemente declarar que *se es quien se dice ser*, se debe probarlo.

La *autenticación* involucra usualmente la interacción entre dos entidades, *el objeto de la autenticación* (un usuario o un cliente) que afirma su identidad y un *autenticador* realizando la verificación de la identidad. El usuario entrega información de autenticación la cual incluye la identidad proclamada y la información que soporta dicha identidad al autenticador.

La información de autenticación puede ir desde un simple *password* a un juego completo de parámetros y mensajes. De igual manera, puede ser una simple función como en el caso de la comparación de claves, o la aplicación de complejos algoritmos criptográficos, como en el caso de firmas digitales.

Si la información de autenticación y la función de autenticación están totalmente bajo el control de las dos entidades, el esquema de autenticación es llamado Esquema de *Autenticación Compartido* (two-party). Sin embargo, en muchos casos es más seguro y escalable ayudarse de una tercera parte (o de más) para la autenticación. Esos esquemas son llamados de confianza en terceras partes (*trusted third-party*).

Otro factor a tener en cuenta es la *integridad* y *confidencialidad* de la información de autenticación. Es importante que la información usada para la autenticación sea segura y no sea obtenida de *participantes no autorizados*.

Esas medidas de seguridad no solo deben ser tomadas en el establecimiento del túnel, sino durante el transcurso del intercambio de datos. En el caso de las VPNs esto es muy importante ya que la información de autenticación es transmitida a través de Internet.

Sistemas de Autenticación

La autenticación es parte vital dentro de la estructura de seguridad de una VPN. Sin ella no se podría controlar el acceso a los recursos de la red corporativa y mantener a los usuarios no autorizados fuera de la línea.

Los sistemas de autenticación pueden estar basados en uno de los siguientes tres atributos: *algo que el usuario tiene* (por ejemplo la llave de una puerta); *algo que el usuario sabe* (por ejemplo una clave); ó *algo que el usuario es* (por ejemplo sistemas de reconocimiento de voz ó barrido de retinas). Es generalmente aceptado el uso de un método sencillo de autenticación tal como el

password, pero no es adecuado para proteger sistemas. Los expertos recomiendan los llamados *sistemas de autenticación complejos*, los cuales usan al menos dos de los atributos de autenticación anteriores.

2.1.4. Cifrado

Las Redes Virtuales Privadas gozan de *confidencialidad* gracias al uso del *cifrado de datos*, que oculta la información a cualquier interceptor que no este autorizado. En una tarea de *cifrado*, el emisor y el receptor, deben conocer el conjunto de reglas que rigen el mecanismo como tal. Las llaves son usadas para transformar los datos original en otros resultantes llamados *texto cifrados*.

Criptografía Simétrica

La *Criptografía Simétrica* es un método que usa una *misma clave* para cifrar y para descifrar mensajes. Las dos partes que se comunican han de ponerse de acuerdo de antemano sobre la clave a usar. Una vez ambas tienen acceso a esta clave, el remitente cifra un mensaje usándola, lo envía al destinatario, y éste lo descifra con la misma clave. Un buen sistema de cifrado pone toda la seguridad en la clave y ninguna en el algoritmo. En otras palabras, no debería ser de ninguna ayuda para un atacante conocer el algoritmo que se está usando. Sólo si el atacante obtuviera la clave, le serviría conocer el algoritmo.

Dado que toda la seguridad está en la clave, es importante que sea muy difícil adivinar el tipo de clave. Esto quiere decir que el abanico de claves posibles, o sea, el espacio de posibilidades de claves, debe ser amplio. Hoy por hoy, los ordenadores pueden adivinar claves con extrema rapidez, y ésta es la razón por la cual el tamaño de la clave es importante en los criptosistemas modernos.

Como ambas partes conocen el cifrado, cualquiera de ellas puede reversar el proceso para abstraer el texto original. El cifrado se basa en dos componentes: *un algoritmo* y *una llave*. Un *algoritmo criptográfico* es una función matemática que combina texto plano o cualquier otra información inteligible con una cadena de dígitos llamada *key (llave)* para producir un texto cifrado o no inteligible. Tanto la llave como el algoritmo son cruciales en un proceso de cifrado (ver figura 2.2 de la página 23).

El cifrado basado en un sistema de llaves ofrece una gran ventaja, los *algoritmos criptográficos* son difíciles de idear por lo cual sería traumático usar un nuevo algoritmo cada vez que una parte se quiera comunicar de manera

privada con una nueva. Usando una llave, un usuario podría utilizar el mismo algoritmo para comunicarse con diferentes usuarios remotos; y todo lo que se debería hacer sería utilizar una diferente llave con cada uno de ellos.

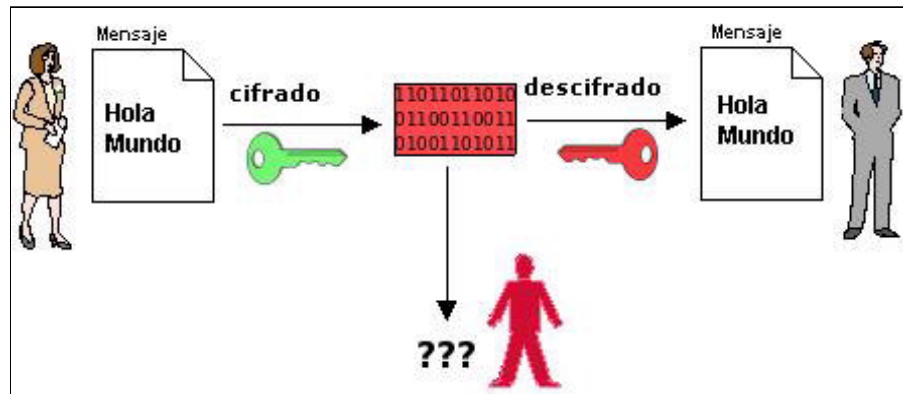


Figura 2.2: Esquema Criptográfico.

El principal problema con los sistemas de cifrado simétrico es el intercambio de claves, sería mucho más fácil para un atacante intentar interceptar una clave que probar las posibles combinaciones del espacio de claves.

Otro problema es el número de claves que se necesitan, si tenemos un número n de personas que necesitan comunicarse entre ellos, entonces se necesitan $n(n-1)/2$ claves para cada pareja de personas que tengan que comunicarse de modo privado. Esto puede funcionar con un grupo reducido de personas, pero sería imposible llevarlo a cabo con grupos más grandes.

Algunos de los *sistemas de autenticación simétricos* más usados son:

- **Passwords Tradicionales:** son la forma más simple de autenticar pero es un método inadecuado para garantizar la seguridad en el acceso a una red, dado que los passwords pueden ser adivinados e interceptados durante transmisiones en la red. Por ejemplo, servicios tales como FTP y Telnet transmiten los nombres y las claves en texto plano, haciéndolos fácilmente interceptables.
- **Passwords Únicos:** Una forma de prevenir el uso no autorizado de Passwords interceptados es evitar que sean reutilizados. Los sistemas de Passwords Únicos restringen el uso de un password a una sola sesión de comunicación, es decir que se requiere un password nuevo para cada

nueva sesión. Estos sistemas, de los cuales S / KEY es el mejor ejemplo, facilitan al usuario la escogencia de un nuevo password para la siguiente sesión generando automáticamente una lista de posibles passwords para el usuario.

- **PAP**(*Protocolo de Autenticación de Passwords*): es un protocolo de dos vías, el host que se está conectando envía un nombre de usuario y un password al sistema destino con el cual trata de establecer su comunicación, y el sistema destino (el autenticador) responde si es el caso, que el computador remoto está autenticado y aprueba su comunicación. PAP es un protocolo de autenticación que puede ser usado al comienzo del establecimiento de un enlace PPP, no es seguro porque la información de autenticación es transmitida en texto plano, esto lo hace vulnerable a que atacantes obtengan información de nombres de usuario y claves de manera fácil.
- **CHAP**(*Challenge Handshake Authentication Protocol*): es muy similar a PAP pero es más seguro para autenticar enlaces PPP. CHAP es un protocolo de tres vías y al igual que PAP, incorpora tres pasos para la autenticación de un enlace, que son:
 1. El autenticador envía un mensaje al nodo remoto.
 2. El nodo calcula un valor usando una función hash y lo envía de regreso al autenticador.
 3. El autenticador avala la conexión si la respuesta concuerda con el valor esperado.

El proceso puede repetirse en cualquier momento del enlace PPP para asegurarse que la conexión no ha sido tomada por otro nodo. A diferencia de PAP, en CHAP el servidor controla la reautenticación. PAP y CHAP tienen algunas desventajas, en ninguno de los dos se pueden asignar diferentes privilegios para acceder a la red a diferentes usuarios remotos que usan el mismo computador. El siguiente protocolo (RADIUS) entrega más flexibilidad para asignar privilegios de acceso.

- **RADIUS**(*Remote Authentication Dial-In User Service*): Es un protocolo AAA (*Autenticación, Autorización y Administración*) para aplicaciones como acceso a redes o movilidad IP. Usa una arquitectura cliente servidor e incluye dos componentes, un *servidor de autenticación* y un *protocolo cliente*. El servidor es instalado en un computador central,

el protocolo cliente es implementado en el *servidor de acceso a la red* (NAS). El proceso de autenticación con RADIUS tiene los siguientes pasos:

- 1. Un usuario remoto marca a un RAS. Cuando la conexión al modem se completa, el RAS pregunta por un nombre de usuario y password.
- 2. Una vez recibidos, el RAS crea un paquete de datos llamado requerimiento de autenticación. Este paquete incluye información tales como el nombre del usuario, el password, el modem de conexión, entre otros. Para evitar que un hacker escuche la información, el RAS actúa como un cliente del RADIUS, cifrando el mensaje con una clave compartida predeterminada entre el RAS y el servidor RADIUS.
- 3. El requerimiento de autenticación es enviado por la red desde el cliente hasta el servidor RADIUS.
- 4. Cuando un requerimiento de autenticación es recibido, el servidor RADIUS valida el requerimiento y verifica la información del nombre de usuario y password.
- 5. Si el nombre de usuario y el password son correctos, el servidor envía un reconocimiento de autenticación que puede incluir información del usuario en la red y los servicios que el requiere.
- 6. Si en este punto del proceso la autenticación no se tiene éxito, el RADIUS envía un mensaje de desconexión al RAS y al usuario se le niega el acceso a la red. La figura 2.3 de la página 26 muestra el escenario correspondiente a los pasos anteriores.

Criptografía Asimétrica

La *Criptografía Asimétrica* o *Criptografía de LLaves Públicas* se basa en el manejo de una pareja de llaves. Cada llave puede encriptar información que sólo la otra puede desencriptar. La llave privada, únicamente es conocida por su propietario; la llave pública, se publica abiertamente, pero sigue asociada al propietario. Los pares de llaves tienen una característica única: los datos encriptados con una llave sólo pueden desencriptarse con la otra llave del par.

Las llaves se pueden usar de dos maneras diferentes: para garantizar *confidencialidad* al mensaje y para probar la *autenticidad* del emisor de un mensaje. En el primer caso, el emisor usa la llave pública del receptor para encriptar

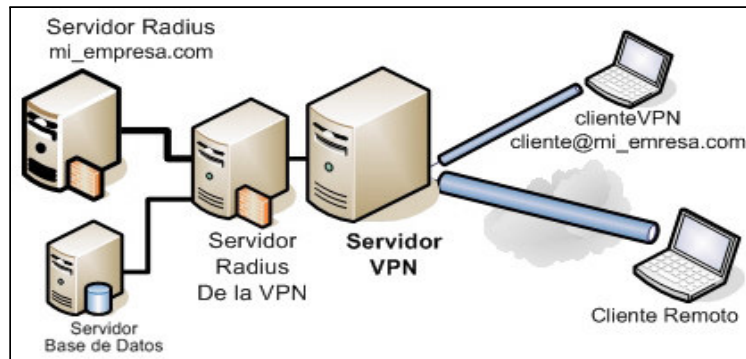


Figura 2.3: Servidores Radius de Autenticación.

un mensaje, de manera que el mensaje continúe siendo confidencial hasta que sea decodificado por el receptor con la llave privada. En el segundo caso, el emisor encripta un mensaje usando la llave privada, una llave a la cual sólo tiene acceso él.

La llave pública del receptor asegura la *confidencialidad*; la llave privada del emisor verifica la *identidad* del mismo. Por ejemplo, para crear un mensaje confidencial, una persona necesita conocer primero la llave pública de su receptor, después deberá usar la misma para encriptar el mensaje y enviarlo. Como el mensaje se encriptó con la llave pública del receptor, sólo éste con su llave privada puede desencriptar el mensaje. Aunque una persona puede encriptar un mensaje con una llave pública o con una llave secreta, usar la llave pública presenta ciertas ventajas. Por ejemplo, la llave pública de la pareja de llaves se puede distribuir en un servidor sin temor de que esto comprometa el uso de la llave privada.

Por ello, no se necesita enviar una copia de la llave pública a todos los receptores; ya que ellos la pueden obtener desde un servidor de llaves mantenido por la compañía, o a través de un proveedor de servicio. La figura 2.4 de la página 27 muestra el esquema con el cual un emisor encripta su mensaje por medio de la llave pública del destinatario y como este último con su llave privada desencripta el mensaje cifrado que le ha llegado.

Otra ventaja de la criptografía con llave pública es que permite que el receptor autentifique al originador del mensaje. La idea básica es esta: ya que el emisor es la única persona que puede encriptar algo con su llave privada, todo aquel que use la llave pública del mismo para desencriptar el mensaje, puede estar seguro de que el mensaje proviene de él. Así, el uso de su llave

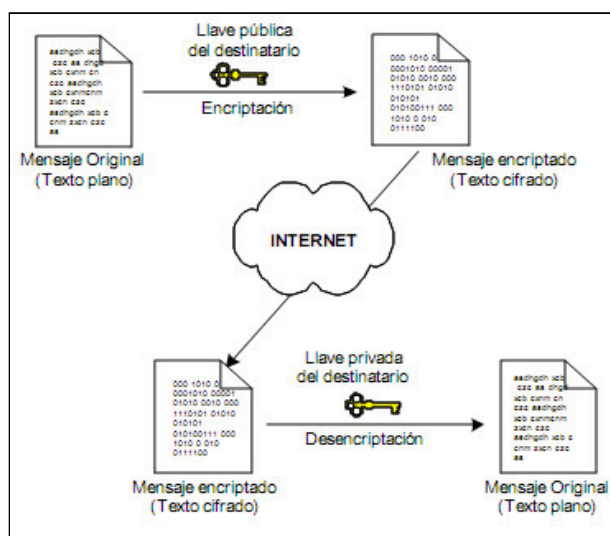


Figura 2.4: Esquema de Cifrado con Llave Pública.

privada en un documento electrónico es similar a la firma en un documento de papel. Pero hay que recordar que aunque el receptor puede estar seguro de que el mensaje proviene del emisor, no hay forma de garantizar que alguien más lo haya leído con anterioridad.

Usar *Algoritmos Criptográficos de Llaves Públicas* para encriptar mensajes es computacionalmente lento, así que se ha descubierto una manera para generar con rapidez una representación corta y única del mensaje, llamada "resumen" (message digest), que se puede encriptar y después usar como *firma digital*.

Algunos algoritmos criptográficos populares y veloces para generar resúmenes se conocen como *Funciones Hash* o *funciones de dispersión de un solo sentido*. Una función de dispersión (hash) de un solo sentido no usa una llave; simplemente es una fórmula para convertir un mensaje de cualquier longitud en una sola cadena de dígitos, llamada *resumen*.

Por ejemplo, suponiendo que el emisor, A, calcula un resumen para un mensaje, y encripta dicho resumen con su llave privada, luego envía esa firma digital junto con un mensaje de texto simple a B.

Después de que B usa la llave pública de A para descriptar la firma digital, B tiene una copia del resumen del mensaje que A calculó. Dado que B pudo descriptar la firma digital con la llave pública de A, sabe que A lo creó,

autenticando así al originador. B usa entonces la misma función de dispersión (que se acordó de antemano) para calcular su propio resumen del mensaje de texto simple de A. Si su valor calculado y el que A envió son iguales, entonces B puede estar seguro de que la firma digital es auténtica, lo que significa que A no sólo envió el mensaje, sino que el mensaje no fue alterado.

Existe una amplia variedad de algoritmos criptográficos para llaves públicas, pero quizá dos de los más importantes han sido Diffie-Hellman y RSA.

2.1.5. Control de Acceso

El control de acceso es un conjunto de políticas y mecanismos que permiten a las partes acceso autorizado a determinados recursos. De esta manera protege al recurso de accesos maliciosos o accidentales de usuarios que no están autorizados a accederlos.

La figura 2.5 de la página 28 muestra un control de acceso en un modelo *cliente-servidor*. Se considera usuario a cualquier entidad (usuario o aplicación trabajando en nombre de ese usuario) que desee acceder al recurso. Se determina por recurso a cualquier objeto que puede ser manipulado de alguna manera, tales como lectura, escritura o modificación, causadas por la realización de alguna acción, tales como la ejecución de un programa o el envío de un mensaje.

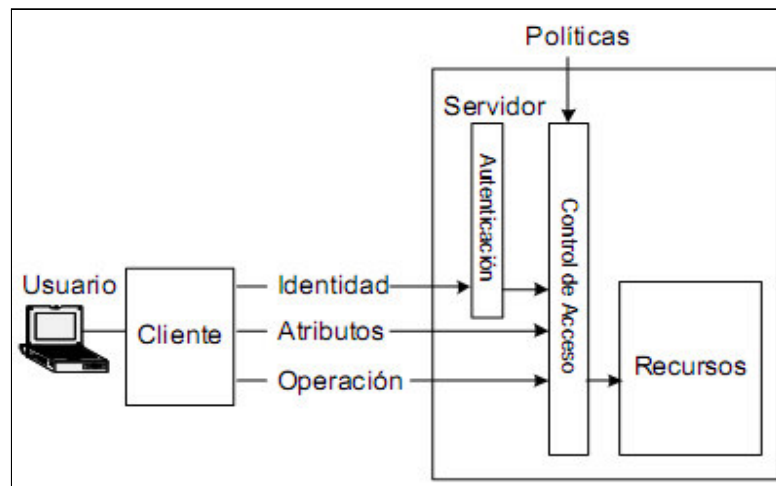


Figura 2.5: Control de Acceso Cliente-Servidor.

Un usuario tiene una identidad y un conjunto de atributos asociados. El

cliente envía la identificación del usuario, los atributos y el requerimiento de una operación al servidor. El servidor puede autenticar la identidad del usuario y remitirlo junto con los atributos y el requerimiento solicitado a los mecanismos de control de acceso. Las políticas son preestablecidas en el mecanismo de control de acceso; la información del usuario es comparada con las reglas de las políticas para determinar los derechos de acceso del usuario a ese recurso.

Mecanismos de Control de Acceso

Los mecanismos de control de acceso son las formas concretas para expresar una regla. Las *listas de control de acceso* y las *listas de capacidades* son dos de los mecanismos más usados para especificar las reglas condicionales.

Listas De Control De Acceso Una ACL (Access Control List) asocia cada recurso con una lista ordenada de qué usuarios pueden tener acceso al recurso y cómo esos usuarios pueden accederlo. Este método es de recurso céntrico; dando el nombre del recurso, del usuario, los atributos del mismo y el tipo de operación, el mecanismo de control de acceso puede buscar la ACL correspondiente a ese recurso y determinar si el usuario puede o no realizar la operación. Los usuarios en algunas ocasiones son puestos en grupos o en clases equivalentes, las cuales tienen los mismos derechos. Esta práctica tiene como objetivo volver más escalables las ACLs dependiendo del número de usuarios en el sistema.

El sistema de archivos UNIX usa una forma de ACL para permitir o denegar las operaciones que pueden ser hechas en los archivos. Hay tres tipos de operaciones básicas: *lectura*, *escritura* y *ejecución*. Cada archivo tiene asociados tres juegos de permisos: uno para el propietario del archivo, uno para el grupo y uno para cualquier otra persona. Cada permiso contiene los tres derechos: lectura (R), escritura (W) y ejecución (X); los derechos que no son garantizados se llenan con un guión (-). Los tres conjuntos con los tres privilegios forman una cadena de nueve dígitos (rwxrwxrwx). A continuación se detalla la salida de un comando UNIX la cual muestra los permisos de varios archivos dentro de ese directorio.

```
-rw----- 1 Juan Contable 383 Mar 13 23:32 Cuentas
-rw-rw-r-- 1 Juan Contable 584 Mar 13 18:17 Empleados
-rwxr-x-- 1 Juan project 164 Mar 13 18:17 useful*
```

En el anterior ejemplo el archivo *Cuentas* tiene permisos de lectura y escritura para el propietario (Juan); el archivo *Empleados* tienen permisos de

lectura y escritura para propietario y para el grupo (Contable), y de lectura para cualquier otra persona; y el archivo *useful* tiene permisos de lectura, escritura y ejecución para el propietario y de lectura y ejecución para el grupo.

Listas de Capacidades Las listas de capacidades (*C-list*) son equivalentes a las ACLs pero son centradas en el usuario a diferencia de las ACLs que son centradas en el recurso. En una *C-list* cada usuario tiene una lista de recursos que puede acceder.

Una *C-list* es usada si los recursos pueden ser agrupados en clases equivalentes, por ejemplo en la clasificación de seguridad militar, donde un documento puede ser marcado como: *no clasificado*, *secreto* o *supersecreto*.

Administración de las Políticas de Control de Acceso

Las políticas de control de acceso usualmente son dinámicas, es decir que nuevas políticas deben ser aplicadas cada vez que nuevos recursos o nuevos usuarios aparecen en la red. El proceso de crear, mantener y distribuir las políticas de control de acceso es llamado *administración de las políticas de control de acceso*.

Una *administradora de políticas* es la entidad que tiene el control sobre todas las políticas de acceso en un sistema. El manejador de las políticas es el servicio responsable de proveer a los administradores de una interfaz fácil de usar que defina, instale, modifique y despliegue políticas. El manejador de políticas también es el encargado de traducir las reglas del lenguaje abstracto que maneja el administrador a expresiones que son usadas en los mecanismos de control de acceso.

Cuando múltiples puntos de control de acceso existen en una red, la administración de las políticas puede ser hecha de una manera *centralizada* o de una manera *distribuida*.

Directorio Activo (Active Directory de Microsoft)

Un ejemplo de *listas de de accesos* con *administración centralizada* es el *Directorio Activo de Microsoft*. En una red *Microsoft Windows*, el servicio de directorio *Active Directory* proporciona la estructura y las funciones para organizar, administrar y controlar el acceso a los recursos de red. .

Active Directory proporciona la capacidad de administrar centralmente la red de Windows. Esta capacidad significa que puede almacenar centralmente

información acerca de la empresa, por ejemplo, *información de usuarios, grupos e impresoras*, y que los administradores pueden administrar la red desde una sola ubicación.

Active Directory admite la delegación del control administrativo sobre los objetos de él mismo. Esta delegación permite que los administradores asignen a un grupo determinado de administradores, permisos administrativos específicos para objetos, como cuentas de usuario o de grupo.

En un dominio hay lo que se llama un servidor principal llamado PDC (Primary Domain Controller) que es quien asigna derechos controla usuarios y recursos. Dado que este servidor puede recibir muchas peticiones de red por parte de los clientes, es posible instalar un servidor de réplica llamado BDC (*Backup Domain Controller*), además en caso de fallo del PDC, éste se sitúa en el dominio como PDC.

Los recursos almacenados en el directorio, como usuarios, impresoras, servidores, grupos, computadores y políticas de seguridad, se conocen colectivamente como *objetos*.

Un objeto es un conjunto nombrado de atributos que representan un recurso de red. Es decir, los atributos son las características de los objetos en el directorio.

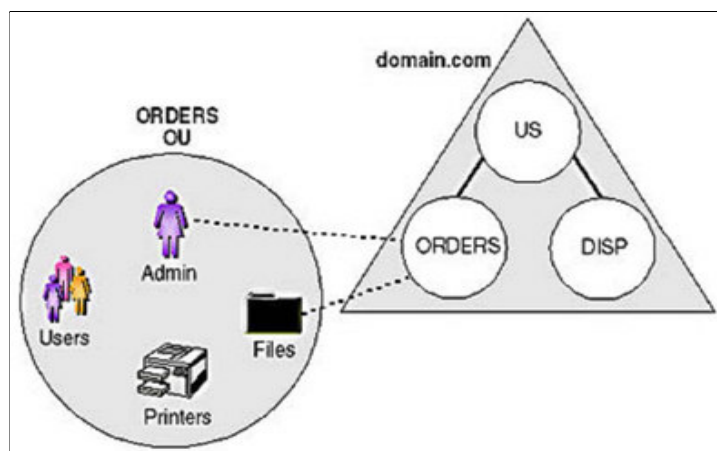


Figura 2.6: Objetos en Active Directory.

Los objetos en *Active Directory* pueden organizarse en clases, que son agrupamientos lógicos de objetos. Ejemplos de clases son las cuentas de usuario, los grupos, las computadoras, las unidades organizacionales, etc. (ver figura

2.6 de la página 31).

Principalmente, un dominio define un límite de seguridad. Un dominio puede contener millones de objetos AD. Por cada objeto dentro de un dominio, AD mantiene ACLs (Listas de Control de Acceso) que controlan que usuarios pueden tener acceso al mismo y que tipo de acceso pueden obtener (ver figura 2.7 de la página 32).

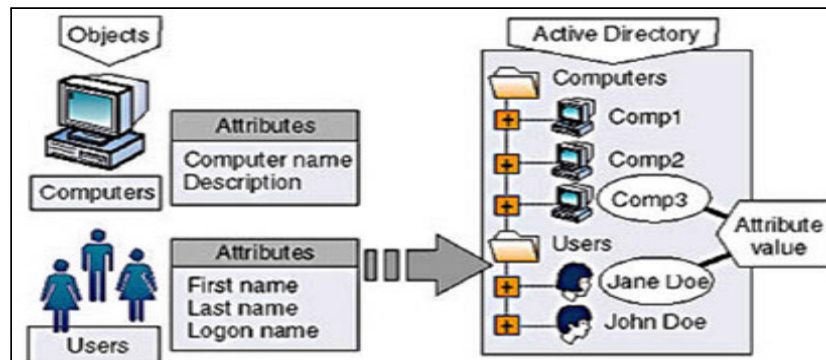


Figura 2.7: Esquema General de Active Directory de Microsoft.

2.2. Tunelamiento

Tunelamiento (*Tunneling*) es una técnica que usa una infraestructura entre redes para transferir datos de una red a otra. Los datos o la carga pueden ser transferidas como tramas de otro protocolo. El *protocolo de tunneling* encapsula las tramas con una cabecera adicional, en vez de enviarla como la produjo en nodo original. La cabecera adicional proporciona información de routing para hacer capaz a la carga de atravesar la red intermedia. Las tramas encapsuladas son enrutadas a través de un túnel que tiene como puntos finales los dos puntos entre la red intermedia. El túnel es una *camino lógico* a través del cual se encapsulan paquetes viajando entre la red intermedia. Cuando un *trama encapsulada* llega a su destino en la red intermedia, se desencapsula y se envía a su destino final dentro de la red. Tunneling incluye todo el proceso de *encapsulado*, *desencapsulado* y *transmisión de las tramas*.

Protocolos de Tuneles

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

basar en el protocolo del túnel de Nivel 2, Nivel 3; o niveles intermedios correspondientes OSI (*Modelo de referencia de interconexión de sistemas abiertos*).

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

Los protocolos de capa 3 corresponden al *nivel de Red*, utilizan paquetes IP o datagramas de *capa de Transporte* (por ejemplo TCP) como carga útil. El modo de túnel de seguridad IP (IPSec) son ejemplos de los protocolos de túnel de capa 3; éstos encapsulan los paquetes IP en un encabezado adicional antes de enviarlos a través de una red IP.

Otros protocolo como MPLS que encapsula la carga útil en una capa adicional entre la *Capa 2* y *Capa 3*. Por último existen también tunelamiento en la *Capa de Aplicación* mediante SSL (Secure Layer Somet) .

2.2.1. Funcionamiento del Túnel

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

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

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

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

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

túnel y envía la carga útil a la red objetivo. La información que se envía entre el servidor del túnel y el cliente del túnel se comporta de manera similar.

2.2.2. Tipos de Túneles

Túneles Voluntarios

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

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

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

Es falso que las VPN requieran una conexión de marcación, pues sólo requieren de una red IP. Algunos clientes (como las PC del hogar) utilizan conexiones de marcación a Internet para establecer transporte IP; esto es un paso preliminar en la preparación para la creación de un túnel, y no es parte del protocolo del túnel mismo. En la figura 2.8 de la página 35 se puede apreciar un escenario típico correspondiente a un *túnel voluntario*.

Túneles Obligatorios

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

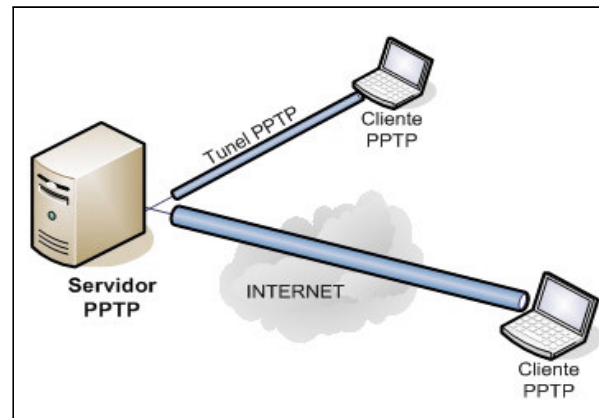


Figura 2.8: Túneles Voluntarios.

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

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

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

En los túneles obligatorios, la computadora cliente realiza una conexión única PPP, y cuando un cliente marca en el NAS se crea un túnel y todo el tráfico se enruta de manera automática a través de éste. Es posible configurar un FEP para hacer un túnel a todos los clientes de marcación hacia un servidor específico del túnel. De manera alterna, el FEP podría hacer túneles individuales de los clientes basados en el nombre o destino del usuario (ver figura 2.9 de la página 36).

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

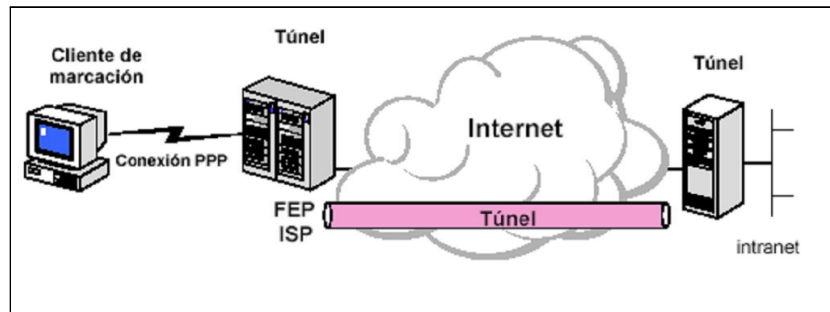


Figura 2.9: Túneles Obligatorios.

del túnel. El tráfico de datos para el nuevo cliente se transporta sobre el túnel existente. Ya que puede haber varios clientes en un túnel único, el túnel no se termina hasta que se desconecta el último usuario del túnel.

Modelos de Entunelamiento

En las VPN los sitios de terminación (*terminadores*) de los túneles son aquellos donde se toman las decisiones de autenticación y las políticas de control de acceso y donde los servicios de seguridad son negociados y otorgados. En la práctica hay tres tipos posibles de servicios de seguridad que dependen de la ubicación de los terminadores. El primer caso es aquel donde el terminador está en el host mismo, donde los datos se originan y terminan.

En el segundo caso el terminador está en el gateway de la LAN corporativa donde todo el tráfico converge en un solo enlace. El tercer caso es aquel donde el terminador está localizado fuera de la red corporativa, es decir en un *Punto de Presencia* (POP) del ISP.

Dado que un túnel VPN se compone de dos terminadores, se pueden obtener seis tipos de modelos de seguridad derivados de la posible combinación de las diferentes localizaciones: *End-to-End*, *End-to-LAN*, *End-to-POP*, *LAN-to-LAN*, *LAN-to-POP* y *POP-to-POP*, en la figura de la página se pueden notar cada uno de estas combinaciones (ver figura 2.10 de la página 37).

En el modelo *End-to-End* el túnel va desde un extremo hasta el otro del sistema. Por lo tanto, los servicios de seguridad son negociados y obtenidos en la fuente y en el destino de la comunicación. Este escenario presenta el más alto nivel de seguridad dado que los datos siempre están seguros en todos los segmentos de la red, bien sea pública o privada. Sin embargo, el total de

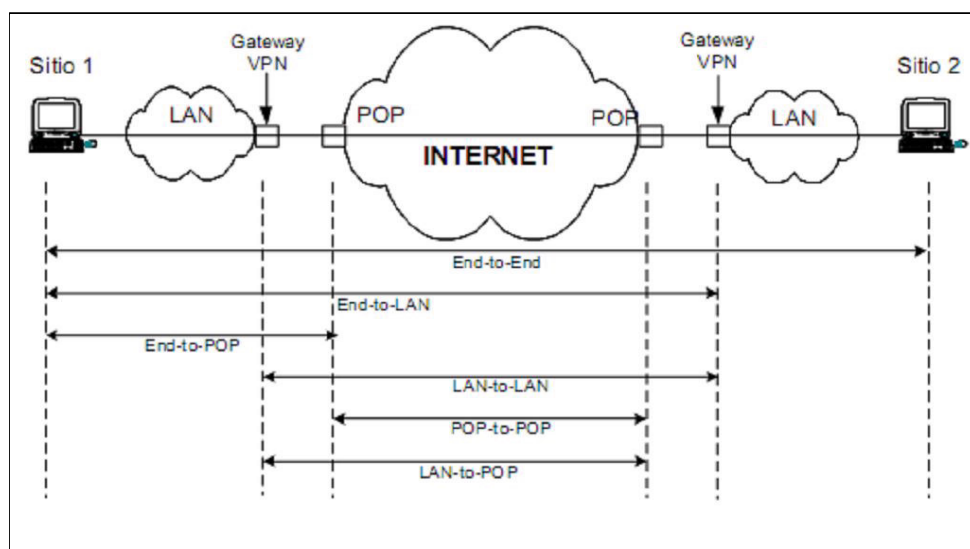


Figura 2.10: Modelos de Entunelamiento.

túneles que pueden haber en una empresa grande, dificulta el manejo de los servicios de seguridad requeridos por dichos host. Este modelo de seguridad es comúnmente visto en implementaciones de capas superiores, como es el caso de SSL (Secure Sockets Layer).

En el modelo *End-to-LAN*, el túnel comienza en un host y termina en el perímetro de una LAN en la cual reside el host destino. Un dispositivo VPN localizado en el perímetro de la red es el responsable de la negociación y obtención de los servicios de seguridad de los host remotos. De esta manera, la seguridad de un gran número de dispositivos en una red corporativa puede ser manejada en un único punto, facilitando así la escalabilidad del mismo.

El modelo de entunelamiento *End-to-POP* es aquel en el cual un host remoto termina el túnel en un POP de la ISP. Un dispositivo VPN o un equipo con funciones de terminador VPN y que se encuentra en la red de la ISP es el responsable por la negociación y concesión de los servicios de seguridad. La entrega de los datos desde el POP hasta el host destino es por lo general asegurada con infraestructura física, la cual separa el tráfico del resto de la red pública. Por lo general en este caso el ISP administra los permisos y controla el acceso según las directivas de los administradores de red de las empresas clientes. La arquitectura de acceso remoto VPN también usa este modelo.

En el modelo *LAN-to-LAN* ambos hosts usan dispositivos VPNs situa-

dos en la frontera de la red corporativa para negociar y conceder servicios de seguridad. De esta manera, las funciones de seguridad no necesitan ser implementadas en los hosts finales donde los datos son generados y recibidos. La implementación de los servicios de seguridad es completamente transparente para los hosts. Esta implementación reduce drásticamente la complejidad en el manejo de las políticas de seguridad. La arquitectura Intranet VPN encaja en este modelo.

En el caso de *LAN-to-POP* el túnel comienza en un dispositivo VPN localizado en la frontera de la red corporativa y termina en un dispositivo VPN el cual se encuentra en un POP de la ISP. En la actualidad prácticamente este entunelamiento no es aplicado.

Finalmente, en el modelo *POP-to-POP* ambos dispositivos VPN son localizados en la propia red de la ISP. Por lo tanto los servicios de seguridad son completamente transparentes para los usuarios finales del túnel. Este modelo permite a los proveedores de servicio implementar valores agregados a los clientes sin que éstos alteren la infraestructura de sus redes. Una tecnología acorde para este modelo es MPLS.

De los seis modelos anteriores el *End-to-LAN* y el *LAN-to-LAN* son los más extensamente usados en las soluciones VPN. Sin embargo, el *POP-to-POP* o *modelo de seguridad basado en red*, ha cobrado vigencia últimamente dado que permite a las ISPs implementar servicios de valores agregados para sus clientes [2].

Capítulo 3

Protocolos VPN

3.1. PPTP - Protocolo de Túnel Punto a Punto

Es quizá el protocolo más sencillo de entunelamiento de paquetes. Es usado, en general, por pequeñas empresas para realizar sus *VPNs LAN-to-LAN*, y en topologías de *acceso remoto*, para trabajadores teleconmutados (teleworkers), tales como vendedores externos o trabajadores que se mantienen en constante movimiento por fuera de sus oficinas.

El protocolo *PPTP* fue propuesto por el Foro PPTP (PPTP Forum), compuesto por 3Com, Ascend (ahora Lucent), Microsoft, ECI Telematics y US-Robotics.

Debido a la integración que hizo Microsoft en sus sistemas operativos, PPTP tuvo gran acogida en el mercado mundial, a tal punto que un protocolo de capa 2 lanzado por Cisco Systems al mismo tiempo, prácticamente no se conoció, L2F (Layer-2- Forwarding).

El protocolo más comúnmente usado para acceso conmutado a Internet es el protocolo punto-a-punto (PPP). PPTP se soporta sobre toda la funcionalidad que PPP le brinda a un acceso conmutado para construir sus túneles a través de Internet. PPTP encapsula paquetes PPP usando una versión modificada del Protocolo de Encapsulamiento Ruteado Genérico (GRE - Generic Routing Encapsulation). Dado lo anterior, PPTP no sólo es capaz de encapsular paquetes IP, sino IPX y NETBEUI, los protocolos de red local más usados.

PPTP utiliza los mecanismos de autenticación que generalmente están asociados a PPP tales como PAP y CHAP, una versión mejorada de CHAP llamada MS-CHAP y desarrollada por Microsoft se encuentra en sus sistemas operativos Windows NT, 2000 y XP. Otra mejora que le ha hecho Microsoft al

protocolo PPTP es la incorporación del método de cifrado MPPE (Microsoft Point-to-Point Encryption).

Una de las ventajas que tiene PPTP por ser un protocolo de nivel 2, es que puede transmitir protocolos diferentes a IP en sus túneles, a diferencia de IPsec que se restringe a trabajar solamente con paquetes IP.

3.1.1. Relación Entre PPP Y PPTP

PPP es el protocolo más comúnmente usado para acceso a Internet, prácticamente el único, además es usado en algunos enlaces seriales punto a punto WAN. PPP trabaja en la capa 2 del modelo OSI, e incluye métodos para encapsular varios tipos de datagramas para ser transferidos sobre enlaces seriales, entre ellos IP, IPX y NETBEUI. El protocolo PPTP depende de PPP para crear la conexión conmutada entre el cliente y el servidor de acceso a la red. PPTP confía las siguientes funciones a PPP:

- Establecimiento y finalización de la conexión física.
- Autenticación de los usuarios.
- Creación de datagramas PPP.

Luego que el enlace PPP es creado, el protocolo PPTP define dos diferentes tipos de paquetes: paquetes de control y paquetes de datos, cada uno de los cuales es asignado a diferentes canales lógicos. PPTP separa los canales de control y de datos usando un flujo de control que corre sobre TCP y un flujo de datos que está encapsulado con cabeceras IP usando GRE. La conexión TCP es creada entre el cliente y el servidor PPTP. Esta conexión es usada para intercambiar mensajes de control.

Los paquetes de datos contienen los datos del usuario, es decir, los datagramas del protocolo de capa de red usado. Los paquetes de control (*control del enlace*) son enviados periódicamente para indagar sobre el estado del enlace y las señales de manejo entre el cliente y el servidor PPTP. Los paquetes de control también se usan para enviar información de manejo básica del dispositivo y de configuración. Los mensajes de control establecen, mantienen y finalizan un túnel PPTP.

Después de que el túnel PPTP se ha establecido, los datos del usuario son transmitidos entre el cliente y el servidor PPTP. Estos datos son transmitidos en datagramas IP contenidos dentro de los paquetes PPP.

Los datagramas IP son creados usando una versión modificada del protocolo GRE (Generic Routing Encapsulation); esta modificación consiste en incluir un identificador de los host que puede ser usado para controlar los privilegios de acceso y la capacidad de reconocimiento, la cual es usada para monitorear la velocidad de transferencia a la cual los paquetes están transmitiéndose en el túnel.

La cabecera GRE es usada para encapsular el paquete PPP dentro del datagrama IP. La información útil del paquete (*payload*) es esencialmente el paquete PPP original enviado por el cliente. Dado que PPTP opera con un *protocolo de capa 2*, debe incluir una cabecera que depende del medio en el cual el túnel está transmitiendo, esta puede ser Ethernet, Frame Relay o PPP. La figura 3.1 de la página 41 muestra la estructura en los diferentes sitios de un túnel de un paquete IP usando encapsulación PPTP desde el sistema cliente hasta la LAN corporativa.

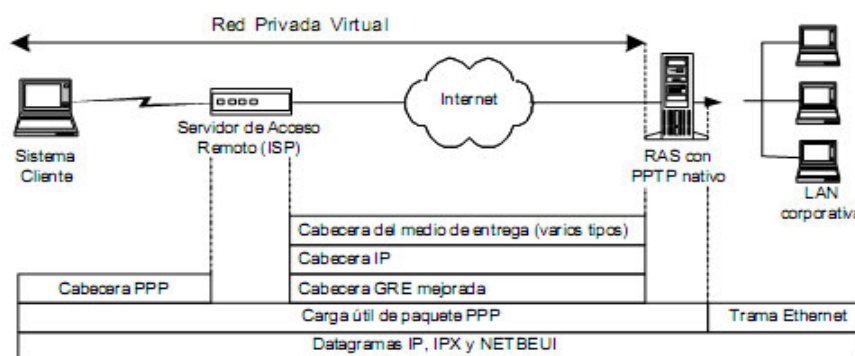


Figura 5.2 Estructura de un túnel PPTP

Figura 3.1: Estructura de un Túnel PPTP.

3.1.2. Componentes de una VPN PPTP

Servidores PPTP

Un servidor PPTP tiene dos funciones básicas, la primera es actuar como el punto final del túnel PPTP y la segunda es reenviar los paquetes a y desde el computador en la red privada. Para reenviar los paquetes al computador destino, el servidor desencapsula el paquete PPTP obteniendo el nombre del computador o la dirección IP privada que se encuentra dentro de este. Una de

las características de los servidores PPTP es la de poder filtrar únicamente el tráfico PPTP dependiendo de si esta condición aparece o no en el perfil del usuario, de esta manera, se puede restringir a un usuario para que se conecte a la red local o se conecte a Internet. Por lo general los servidores PPTP están en las premisas de la red corporativa, en algunos casos el servidor PPTP está ubicado dentro de la red privada y está protegido por el firewall (zona militarizada). Cuando esto ocurre, es necesario abrir el puerto TCP 1723, o si el firewall permite filtrar no por puerto sino por protocolo, se deberá permitir el protocolo GRE (puerto 47).

Software Cliente PPTP

Como se dijo anteriormente, si el NAS del ISP soporta PPTP no se necesita ningún software o hardware adicional en el extremo final del cliente, solamente que éste pueda establecer una conexión PPP. Por otro lado, si el ISP no soporta PPTP, el cliente deberá utilizar un software cliente PPTP en su computador para poder crear el túnel. La mayoría de los sistemas operativos cuentan con un cliente PPTP nativo.

Servidores de Acceso a la Red

Los servidores de acceso a la red también llamados servidores de acceso remoto o concentradores de acceso, son los encargados de soportar las conexiones PPP de una gran cantidad de clientes que se conectan a este por medio de enlaces telefónicos conmutados. Sus funciones van desde el establecimiento de la conexión física (modulación, demodulación, compresión de datos, corrección de errores, etc.) hasta labores de enrutamiento presentes en la capa 3 del modelo OSI. Dentro de un túnel PPTP se pueden encontrar NAS actuando como clientes PPTP o simplemente como un concentrador de acceso PPP. PPTP permite que las funciones realizadas por un servidor de acceso a la red (NAS) sean separadas usando una arquitectura cliente-servidor.

Comúnmente, las siguientes funciones son implementadas por un NAS:

1. Brindar una interfaz física entre la red telefónica pública conmutada y los módems. Esto incluye conversiones A/D y D/A, conversiones síncronas a asíncronas y manipulaciones de flujos de datos.
2. Terminación lógica de enlaces PPP.
3. Autenticación de enlaces PPP.

4. Sumarización de canales (*protocolo multilink PPP*).
5. Terminación lógica de protocolos de control de red (NCP).
6. Enrutamiento multiprotocolo y bridging.

PPTP divide estas funciones entre los dos componentes que se definen en el protocolo, a saber PAC y PNS. El PAC o *concentrador de acceso PPTP* es el responsable de las funciones 1, 2 y algunas veces 3. El PNS o *servidor de red PPTP*, es el responsable de las funciones 3, 4, 5 y 6.

El protocolo PPTP es única y exclusivamente implementado entre el PAC y el PNS. Un PAC puede atender muchos PNSs. Un único PNS puede ser asociado a muchos PACs [5].

3.1.3. Estructura del Protocolo

PPTP define una conexión de control entre cada pareja PAC-PNS la cual opera sobre TCP; y un túnel IP operando sobre la misma pareja PAC-PNS el cual es usado para transportar paquetes PPP con encapsulamiento GRE.

3.1.4. Conexión de Control

Antes que el entunelamiento PPP ocurra entre un PAC y un PNS, una conexión de control debe ser establecida entre ellos. La conexión de control es una sesión TCP que mantiene control sobre la llamada e intercambia mensajes de información. Por cada pareja PAC-PNS debe existir una conexión de control y un túnel. La conexión de control es la responsable por el establecimiento, el manejo y la liberación de las sesiones que existen en el túnel, esto lo realiza a través del puerto 1723.

3.1.5. Operación del Túnel

PPTP necesita el establecimiento de un *túnel* por cada pareja PNS-PAC. Este *túnel* se utiliza para transportar todos los paquetes PPP de las diferentes sesiones involucradas en la pareja PNS-PAC. Una clave que se encuentra presente en la cabecera GRE indica qué paquetes PPP pertenecen a qué sesión. De ésta manera, los paquetes PPP son multiplexados y desmultiplexados sobre un único túnel existente entre una pareja PNS-PAC. El valor del campo *Clave* es definido dentro del proceso de establecimiento de la llamada.

La cabecera GRE también contiene información de reconocimiento y de secuencialización con la cual se realiza control de congestión y detección de errores en el túnel.

Los datos del usuario transportados por el protocolo PPTP son esencialmente paquetes de datos PPP. Los paquetes PPP son transportados entre el PAC y el PNS, encapsulados en paquetes GRE los cuales a su vez son transportados sobre IP. Los paquetes encapsulados PPP son esencialmente paquetes de datos PPP sin ningún elemento de tramado de medio específico. Los paquetes IP transmitidos sobre los túneles entre un PAC y un PNS tienen la estructura general que se muestra en la figura 3.2 de la página 44.

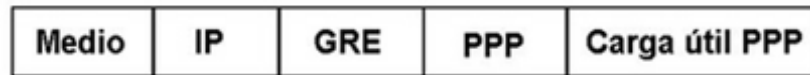


Figura 3.2: Formato del Paquete IP.

3.1.6. Cabecera Mejorada GRE

La cabecera GRE usada por PPTP es una versión ligeramente mejorada de la especificación estándar del protocolo GRE. La principal diferencia es la definición de un nuevo campo de reconocimiento de número (*acknowledgment number*), usado para determinar si un paquete particular GRE o un conjunto de paquetes ha arribado al lado remoto del túnel. Esta capacidad de reconocimiento no es usada en conjunto con ningún tipo de retransmisión, en vez de eso, se usa para determinar la velocidad de transferencia a la cual los paquetes de datos del usuario son transmitidos sobre el túnel.

3.1.7. Cifrado en PPTP

La trama PPP se cifra con el *cifrado punto a punto de Microsoft* (MPPE, Microsoft Point-to-Point Encryption) mediante claves de cifrado generadas en los procesos de autenticación MS-CHAP, MS-CHAP v2 o EAP-TLS. Los clientes de red privada virtual deben utilizar el protocolo de autenticación MS-CHAP, MS-CHAP v2 o EAP-TLS para poder cifrar las cargas de las tramas PPP. PPTP aprovecha el cifrado PPP subyacente y encapsula una trama PPP cifrada anteriormente. Una llave de encriptación es generada usando una mínima parte del password situados en cliente y server. El RSA RC4 standard

es usado para crear estos 40 bits (128 dentro de EEUU y Canada) de llave de sesión basada en el password de un cliente. Esta llave es después usada para encriptar y desencriptar todos los datos intercambiados entre el server PPTP y el cliente. Los datos en los paquetes PPP son encriptados. El paquete PPP que contiene un bloque de datos encriptados es después metido en un datagrama IP para su enrutamiento.

3.1.8. Filtrado de Paquetes PPTP

Esta opción incrementa el rendimiento y fiabilidad de la seguridad de red si esta activada en el servidor PPTP. Cuando esta activa acepta y enjuta solo los paquetes PPTP de los usuarios autorizados. Esto prevé el resto de paquetes entren en la red privada y en el servidor de PPTP.

3.1.9. Control de Acceso a los Recursos de la Red

Después de la *autenticación*, todo el acceso a la LAN privada continúa usando las estructuras de seguridad de la misma LAN. El acceso a recursos en devices NTFS o otros recursos de la red requieren los permisos correctos de cada usuario, tal como si estuvieses conectado físicamente dentro de la LAN. La existencia de un *Controlador de Dominio* por ejemplo, tiene validez en esta configuración.

3.2. L2TP - Protocolo de Túnel de Capa 2

L2TP [11] fue creado como el sucesor de PPTP y L2F. Las dos compañías abanderadas de cada uno de estos protocolos, Microsoft por PPTP y Cisco por L2F, acordaron trabajar en conjunto para la creación de un único *protocolo de capa 2* y así lograr su estandarización por parte de la IETF.

Como PPTP, L2F fue diseñado como un protocolo de entunelamiento usando para ello encapsulamiento de cabeceras. Una de las grandes diferencias entre PPTP y L2F, es que el entunelamiento de éste último no depende de IP y GRE, permitiéndole trabajar con otros medios físicos por ejemplo Frame Relay. Paralelamente al diseño de PPTP, L2F utilizó PPP para *autenticación de usuarios* accedando *vía telefónica conmutada*, pero también incluyó soporte para TACKCS+ y RADIUS.

Otra gran diferencia de L2F con respecto a PPTP es que permite que un único túnel soporte más de una conexión. Hay dos niveles de autenticación

del usuario: primero, por la ISP antes de crear el túnel; segundo, cuando la conexión está configurada y la autenticación la realiza el gateway corporativo.

Todas las anteriores características de L2F han sido transportadas a L2TP. Como PPTP, L2TP utiliza la funcionalidad de PPP para proveer acceso conmutado que puede ser tunelizado a través de Internet a un sitio destino. Sin embargo, como se ha mencionado anteriormente, L2TP define su propio protocolo de entunelamiento basado en L2F permitiendo transporte sobre una amplia variedad de medios de empaquetamiento tales como X.25, Frame Relay y ATM.

Dado que L2TP es un *protocolo de capa 2*, ofrece a los usuarios la misma flexibilidad de PPTP de soportar otros protocolos aparte de IP, tales como IPX y NETBEUI.

Microsoft incluye L2TP a partir del sistema operativo Windows 2000, ya que las mejoras de L2TP con respecto a PPTP saltan a la vista.

3.2.1. Componentes Básicos de un Túnel L2TP

Concentrador de acceso L2TP (LAC): es un nodo que se encuentra en un punto extremo de un túnel L2TP. El LAC se encuentra entre un LNS y un sistema remoto y reenvía los paquetes a y desde cada uno. Los paquetes enviados desde el LAC hasta el LNS van tunelizados. En algunas ocasiones el sistema remoto actúa como un LAC, esto se presenta cuando se cuenta con un software cliente LAC.

Servidor de Red L2TP (LNS): es un nodo que se encuentra en un punto extremo de un túnel L2TP y que interactúa con el LAC, o punto final opuesto. El LNS es el punto lógico de terminación de una sesión PPP que está siendo tunelizada desde un sistema remoto por el LAC.

Túnel: un Túnel existe entre una pareja LAC-LNS. El túnel consiste de una *conexión de control* y de ninguna o más sesiones L2TP. El túnel transporta datagramas PPP encapsulados y mensajes de control entre el LAC y el LNS.

3.2.2. Topología de L2TP

La figura 3.3 de la página 47 describe un escenario típico L2TP. El objetivo es tunelizar tramas PPP entre un sistema remoto o un cliente LAC y un LNS localizado en la LAN corporativa.

El sistema remoto inicia una conexión PPP a través de la *red de telefonía pública conmutada* a un LAC. El LAC luego tuneliza la conexión PPP a través



Figura 3.3: Escenario Típico L2TP.

de Internet o una nube Frame Relay o ATM a un LNS por donde accesa a la *LAN remota corporativa*. La dirección del sistema remoto es dada desde la LAN corporativa por medio de una negociación PPP NCP. La *autenticación*, *autorización* y *accounting* puede ser provista por el dominio de la red corporativa remota como si el usuario estuviera conectado a un servidor de acceso de la red directamente. Este escenario pertenece a una Sesión Obligatoria L2TP.

En una *Sesión Voluntaria*, un cliente LAC (*un host que corre L2TP nativo*) puede también crear un túnel hasta la LAN corporativa sin usar un LAC externo. En este caso, el host tiene un software cliente LAC y previamente ha estado conectado a la red pública, tal como Internet. Una *conexión PPP virtual* es luego creada y el software cliente LAC hace un túnel hasta el cliente LNS. Como en el caso anterior, el *direccionamiento*, la *autenticación*, la *autorización* y el *accounting* pueden ser provistos por el dominio de la LAN corporativa remota.

3.2.3. Estructura del Protocolo L2TP

L2TP utiliza dos tipos de mensajes, los *mensajes de control* y los *mensajes de datos*. Los *mensajes de control* son usados en el *establecimiento*, *mantenimiento* y *finalización de túneles* y *llamadas*. Los *mensajes de datos* son usados para encapsular tramas PPP que está siendo transportadas sobre el túnel. Los *mensajes de control* utilizan un canal de control confiable con el cual L2TP garantiza la entrega. Los mensajes de datos no son retransmitidos cuando ocurren pérdidas de paquetes.

La figura 3.4 de la página 48 muestra la relación de las tramas PPP y los mensajes de control con los *canales de datos y control* L2TP respectivamente. Las tramas PPP son transportadas sobre un canal de datos no confiable y son encapsuladas primero por una cabecera L2TP y luego por una cabecera de transporte de paquetes que pueden ser UDP, Frame Relay o ATM.

Los *mensajes de control* son enviados sobre un canal de control L2TP confiable, el cual transmite paquetes en banda sobre el mismo transporte de paquetes. Para esto se requiere que números de secuencia estén presentes en todos los mensajes de control. Los mensajes de datos pueden usar esos números de secuencia para reordenar paquetes y detectar pérdidas de los mismos.

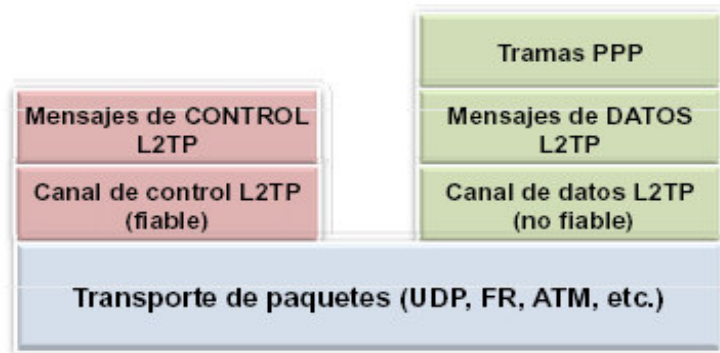


Figura 3.4: Relación Entre Tramas PPP y Mensajes L2TP.

3.2.4. Formato de una Cabecera L2TP

Los paquetes L2TP para el canal de control y el canal de datos comparten un formato de cabecera en común, la figura 3.5 de la página 48 muestra el formato dicha cabecera L2TP:

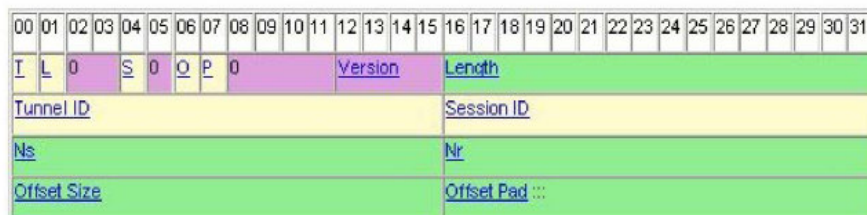


Figura 3.5: Formato de Cabecera L2TP.

- **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 está configurado, los campos Ns y Nr también deben estar configurados. Los mensajes de Control deben tener configurado este bit.
- **O:** Used Offset. 1 bit. Los 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.

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 autenticación 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.

3.2.5. Autenticación en L2TP

La autenticación 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 está establecido, el Concentrador de Acceso (LAC) del ISP asigna un nuevo ID de llamada para identificar la conexión con el túnel e inicia una sesión para devolver la información autenticada. El *servidor de red corporativa* emprende la *segunda fase de autenticación* para decidir si acepta o no la llamada. La llamada comienza indicando al ISP el método de autenticación o la información de autenticación 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 autenticación a la capa de PPP, la cual aporta una amplia gama de opciones, 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*.

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

3.2.6. Procesos de una Comunicación L2TP

1. **Conexión y comunicación PPP:** el *cliente remoto* usa el protocolo PPP para establecer la conexión con un IPS, la cual constituye la *primer fase de autenticación L2TP*.
2. **Conexión de control L2TP (establecimiento del túnel):** es la conexión inicial que hay que establecer entre el LAC y el LNS antes de que se puedan establecer *sesiones*. El establecimiento de la conexión de control incluye la autenticación de la entidad par por el LNS y la negociación de las facilidades soportadas.
3. **Establecimiento de la sesión:** una vez establecido el túnel entre el LAC y el LNS se establece una sesión dentro del túnel por cada conexión PPP existente entre LAC y LNS. Cada sesión se corresponde a un flujo de tramas PPP entre el LAC y el LNS. El LAC solicita al LNS que acepte una sesión para una llamada entrante y el LNS solicita al LAC que acepte una sesión para una llamada saliente. Seguidamente se completa el proceso de autenticación PPP entre el usuario remoto y el LNS. A

continuación se inicia el envío de paquetes NCP para elegir y configurar uno o más protocolos de red:

- Ej.: IPCP para indicar que el protocolo de red es IP.
- Ej.: ECP para encriptar las tramas de la conexión PPP entre el usuario remoto y el LNS.

4 **Envío de datos de usuario:** el usuario puede empezar el envío de datos a través del túnel. Estos datos van cifrados.

5 **Descifrado de los datos por el LNS:** el LNS recibe los datos, los descifra y los entrega a la red corporativa. Si el LNS envía información al usuario también la cifra antes de enviarla a través del túnel.

3.2.7. Comparativa Entre PPTP y L2TP

- Con PPTP, el cifrado de datos comienza después de que la conexión se procese (y, por supuesto, después de la autenticación PPP). Con L2TP, el cifrado empieza antes de la conexión PPP negociando una asociación de seguridad IPsec.
- Las conexiones PPTP usan MPPE, un método de cifrado basado en el algoritmo de encriptación *Rivest-Shamir-Aldeman* (RSA) RC-4, y usa llaves de 40, 56 o 128 bits. Las conexiones L2TP usan *Data Encryption Standard* (DES), con llaves de 56 bits para DES o tres llaves de 56 bits para 3-DES. Los datos se cifran en bloques (bloques de 64 bits para el caso de DES).
- Las conexiones PPTP requieren sólo autenticación a nivel de usuario a través de un protocolo de autenticación basado en PPP. Las conexiones L2TP / IPsec requieren el mismo nivel de autenticación a nivel de usuario y, además nivel de autenticación de máquina usando *certificados digitales*.
- PPTP requiere que el tránsito entre - redes sea una Internetwork IP. L2TP únicamente requiere que los medios de túnel proporcionen conectividad de punto a punto orientada al paquete. L2TP puede ejecutarse sobre IP (usando UDP), Frame Relay, X.25, ATM.
- PPTP sólo puede soportar un túnel entre dos puntos extremos. L2TP permite el uso de túneles múltiples entre puntos extremos.

- L2TP proporciona autenticación de túnel, mientras que PPTP no lo hace, sin embargo, cuando ya sea que PPTP o L2TP se ejecute sobre IPSec, la autenticación de túnel es proporcionada por IPSec para que no sea necesaria la autenticación de túnel nivel 2.

3.2.8. Problemas de L2TP

A pesar de que L2TP ofrece un acceso económico, con soporte multiprotocolo y acceso a redes de área local remotas, no presenta unas características criptográficas especialmente robustas. Por ejemplo:

- Sólo se realiza la operación de autenticación entre los puntos finales del túnel, pero no para cada uno de los paquetes que viajan por él. Esto puede dar lugar a suplantaciones de identidad en algún punto interior al túnel.
- Sin comprobación de la integridad de cada paquete, sería posible realizar un ataque de denegación del servicio por medio de mensajes falsos de control que den por acabado el túnel L2TP o la conexión PPP subyacente.
- L2TP no cifra en principio el tráfico de datos de usuario, lo cual puede dar problemas cuando sea importante mantener la confidencialidad de los datos.
- A pesar de que la información contenida en los paquetes PPP puede ser cifrada, este protocolo no dispone de mecanismos para generación automática de claves, o refresco automático de claves. Esto puede hacer que alguien que escuche en la red y descubra una única clave tenga acceso a todos los datos transmitidos [11].

3.3. IPSec (Internet Protocol Security)

El estandar reconocido para conexiones VPN

En IPv4 no se desarrollaron mecanismos de seguridad inherentes al protocolo, por tanto, protocolos y procedimientos adicionales a IPv4 fueron necesarios para brindar servicios de seguridad a los datos. IPSec [4] es un conjunto de protocolos diseñados para proveer una seguridad basada en criptografía robusta para IPv4 e IPv6, de hecho IPSec está incluido en IPv6.

Entre los servicios de seguridad definidos en IPsec se encuentran, *control de acceso, integridad de datos, autenticación del origen de los datos, protección antirepetición y confidencialidad en los datos*. Entre las ventajas de IPsec están la *modularidad del protocolo*, ya que no depende de un algoritmo criptográfico específico.

3.3.1. Componentes de IPsec

IPsec está compuesto por tres componentes básicos: los *Protocolos de Seguridad* (AH y ESP), las *Asociaciones de Seguridad* (SAs) y las *Bases de Datos de Seguridad*; cada uno de los cuales, trabaja de la mano con los demás y ninguno le resta importancia al otro.

Protocolos de Seguridad

IPsec es un conjunto de protocolos que provee varios servicios de seguridad. Esos servicios de seguridad trabajan gracias a dos protocolos, el *Authentication Header* (AH) [5] y el *Encapsulating Security Payload* (ESP) [6], y también al uso de protocolos y procedimientos para el manejo de llaves criptográficas tales como IKE (*Internet Key Exchange Protocol*) [8].

El éxito de una IKE es un protocolo que permite a dos entidades IPsec negociar dinámicamente sus servicios de seguridad y sus llaves de cifrado al igual que la autenticación de la sesión misma implementación IPsec depende en gran medida de una adecuada escogencia del protocolo de seguridad y de la forma como se intercambian las llaves criptográficas.

AH es un protocolo que añade una nueva cabecera justo después de la cabecera IP original. AH provee autenticación del origen de los datos e integridad de los mismos, también provee integridad parcial para prevenir *ataques de repetición*. Este protocolo es apropiado cuando se requiere *autenticación* en vez de *confidencialidad*.

ESP provee confidencialidad para el tráfico IP, al igual que autenticación tal cual como lo hace AH, pero sólo uno de estos servicios puede ser proporcionado por ESP al mismo tiempo.

Asociaciones de Seguridad (SAs)

Una SA define las *medidas de seguridad* que deberían ser aplicadas a los paquetes IP basados en quién los envía, hacia dónde van y qué tipo de carga útil ellos transportan. El conjunto de servicios de seguridad ofrecidos por una

SA dependen de los protocolos de seguridad y del modo en el cual ellos operan definidos por la SA misma.

La figura 3.6 de la página 54 muestra los dos modos en los cuales un protocolo de seguridad puede operar: *transporte* y *túnel*; la diferencia radica en la manera como cada uno de ellos altera el paquete IP original.

El modo de transporte es diseñado para proteger los protocolos de capas superiores tales como TCP y UDP.

En modo túnel, el paquete IP original se convierte en la *carga útil* de un nuevo paquete IP. Esto le permite al paquete IP inicial, ocultar su cabecera IP para que sea encriptada, considerando que el paquete IP externo sirve de guía a los datos a través de la red.

Las SAs pueden ser negociadas entre dos entidades IPSec dinámicamente, para lo cual se basan en políticas de seguridad dadas por el administrador del sistema o estáticamente especificadas por el administrador directamente.

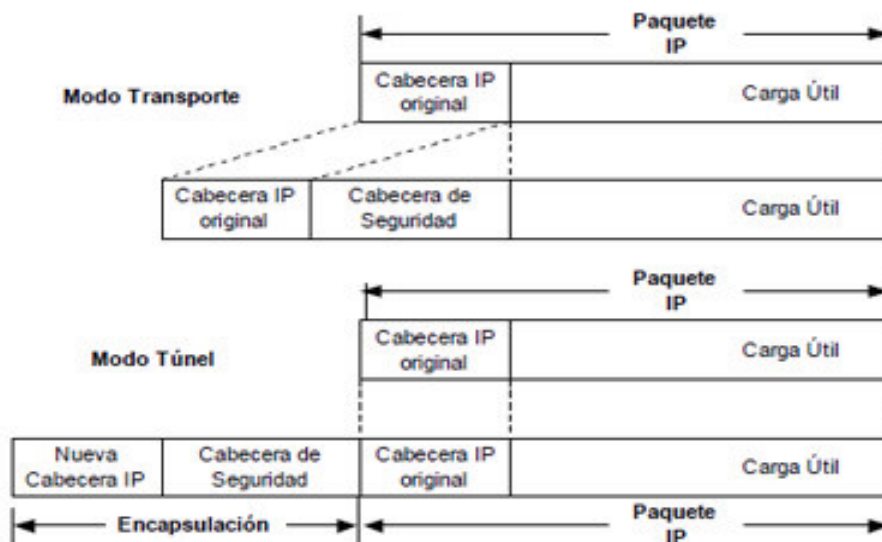


Figura 3.6: Formato de Trama IPSec en Modo Transporte y Túnel.

Una SA es únicamente identificada por tres parámetros: una *dirección IP de destino*, un *identificador del protocolo de seguridad* y un *índice del parámetro de seguridad* (SPI). La dirección IP de destino es aquella por la cual se identifica el punto final de la SA, el SPI es un número de 32 bits usualmente escogido por el punto final de destino de la SA y que sólo tiene significado local dentro

de ese punto destino. El identificador del protocolo de seguridad es un número con el cual se define cada uno de ellos, 51 para AH o 50 para ESP.

Como se nota, la dirección IP del origen no se usa para definir una SA, esto dado que una SA se define entre dos hosts o gateways para datos enviados en una sola dirección, de aquí que, si dos dispositivos necesitan intercambiar información en ambas direcciones usando IPsec, requerirán de dos SAs, una para cada sentido.

En modo de transporte, la cabecera IP original se mantiene intacta y una cabecera de seguridad es colocada entre la cabecera IP misma y su carga útil. La cabecera IP original es modificada para que el receptor del paquete entienda que antes de la carga útil se encuentra una cabecera de seguridad. En modo túnel, el paquete IP original se convierte en la carga útil de un paquete IP encapsulado. La cabecera IP nueva le indica al receptor del paquete que una cabecera de seguridad se encuentra a continuación de ella.

3.3.2. Bases de Datos de Seguridad

IPsec trabaja con dos bases de datos de seguridad, en una se encuentran las *políticas de seguridad* y en la otra las *asociaciones de seguridad*, SPD (*Security Policy Database*) y SAD (*Security Association Database*) respectivamente. El administrador de políticas define un conjunto de servicios de seguridad para ser aplicados al tráfico IP tanto entrante como saliente. Esas políticas son guardadas en las SPDs y son usadas por las SAs cuando éstas se crean. Todas las SAs son registradas en la SAD.

Bases de Datos de Asociaciones de Seguridad (SAD)

La base de datos de asociaciones de seguridad almacena todos los parámetros concernientes a las SA's, cada una de ellas tiene una entrada en la SAD donde se especifican todos los parámetros necesarios para que IPsec realice el procesamiento de paquetes IP que son gobernados por esa SA. Entre los parámetros que se encuentran en una SAD se tienen:

- El índice de parámetro de seguridad.
- El protocolo a ser usado por la SA (ESP o AH).
- El modo en el cual el protocolo es operado (túnel o transporte).
- Un contador numérico secuencial.

- La dirección IP fuente y destino de la SA.
- El algoritmo de autenticación y la llave de autenticación usadas.
- El tiempo de vida de la SA.

Para el procesamiento de los paquetes IP entrantes una SA apropiada es encontrada en la SAD tal que concuerde con los siguientes tres valores: la *dirección IP destino*, el *tipo de protocolo IPSec* y el *SPI*. La dirección IP de destino y el tipo de protocolo IPSec son obtenidos de la cabecera IP y el SPI se obtiene de la cabecera AH o ESP. Si una SA es encontrada para el paquete IP entrante en mención, éste es procesado de acuerdo a los servicios de seguridad especificados. Luego se aplican al paquete todas las reglas descritas en la SPD para la SA que lo gobierna.

Para el procesamiento de paquetes IP salientes, primero se aplica el procesamiento relacionado con la SPD. Si se encuentra una política para el paquete de salida que especifique que un procesamiento IPSec es necesario, la SAD es buscada para determinar si una asociación de seguridad ha sido previamente establecida.

Base de Datos de Políticas de Seguridad (SPD)

Una *base de datos de políticas de seguridad* es una lista ordenada de políticas de seguridad a ser aplicadas a los paquetes IP. Dichas políticas son en general reglas que especifican cómo los paquetes IP deben ser procesados. La SPD es mantenida por el administrador del dispositivo IPSec.

Una entrada SPD tiene dos componentes: un *juego de selectores* y una *acción*. Los *selectores* clasifican un paquete IP sobre una *acción*. Un *selector* es un parámetro y el valor o rango de valores para este parámetro. Los parámetros generalmente se encuentran dentro de una de estas dos categorías:

- Aquellos que se encuentran dentro de un paquete IP, tales como, la dirección IP, número de protocolo y números de puertos de capas superiores.
- Aquellos que se derivan de la credencial de autenticación de una entidad de comunicación, tales como, una dirección de correo o un nombre distinguido DN (Distinguished Names) en *certificados digitales*.

Diferentes operadores lógicos como AND, OR y NOT pueden ser aplicados a las políticas para combinar más de un selector.

Cuando un paquete IP contiene valores que concuerdan con los especificados por algún selector de una entrada, la acción que se especifica en dicha entrada es aplicada al paquete. Hay tres opciones: aplicar el servicio de seguridad IPsec, descartar el paquete IP o permitir que el paquete IP omita el procesamiento IPsec.

La figura 3.7 de la páginas 57 muestra una entrada en una base de datos de políticas de seguridad para un paquete entrante y saliente, claramente se notan las partes que componen un selector como lo son los parámetros y su correspondiente valor, al frente se encuentra la acción que IPsec tomaría si los paquetes IP concuerdan con los valores de los selectores.

Entrantes	Selectores	Acción
	dirección_IP fuente = 10.0.0.92 AND	IPsec (ESP, 3DES, HMAC-SHA-1)
	dirección de e-mail fuente = financiera@telesat.com.co nombre_distinguido fuente = Andrés Gómez	
	dirección_IP destino = 192.89.0.169	Omitir

Salientes	Selectores	Acción
	dirección_IP destino = 10.0.0.92	IPsec (ESP, 3DES, HMAC-SHA-1)
	nombre_distinguido destino = Andrés Gómez	
	dirección_IP fuente = 192.89.0.169	Omitir

Figura 3.7: Ejemplo de una Entrada de Base de Datos de Políticas de Seguridad.

La SPD trata al tráfico saliente y entrante de manera separada, esto es, que se deben aplicar políticas de seguridad distintivas de entrada y de salida por cada interfaz de red. Cuando un *paquete IP* llega a una interfaz de red IPsec primero busca en la SAD la apropiada SA, cuando la encuentra, el sistema inicia los procesos SAD y SPD. Después del procesamiento SPD, el sistema reenvía el paquete al siguiente salto o le aplica procedimientos adicionales tales como las reglas de algún *firewall*.

3.3.3. Authentication Header (AH)

El AH (*Protocolo de Cabecera de Autenticación*) es usado para propósitos de autenticación de la carga útil IP a nivel de *paquete por paquete*, esto es autenticación de la integridad de los datos y de la fuente de los mismos. Como el término autenticación indica, el protocolo AH se asegura que los datos entregados dentro del paquete IP son auténticos, es decir, que han arribado a su destino sin ninguna modificación. AH también provee de un mecanismo de protección opcional *antirepetición de paquetes IP*. Sin embargo, AH no protege la *confidencialidad* de los datos, es decir, no recurre a ningún tipo de cifrado de los mismos.

El protocolo AH define cómo un paquete IP sin protección es convertido en uno nuevo que contiene información adicional y que brinda *autenticación*. El elemento fundamental usado por AH es una cabecera de autenticación como se muestra en la figura 3.8 de la pág. 59. El nuevo paquete IP es formado insertando la cabecera de autenticación, bien sea, después de la nueva cabecera IP o después de la cabecera IP original modificada según sea el modo en el cual trabaje la SA.

Cuando la cabecera de autenticación es insertada, la cabecera IP que la precede deberá indicar que la próxima cabecera que se encuentra es la cabecera de autenticación y no la carga útil del paquete original. La cabecera IP realiza esta acción colocando el campo Protocolo en el valor 51 (valor de protocolo para AH).

La cabecera de autenticación contiene seis campos:

- **Next Header:** identifica el tipo de protocolo de la carga útil del paquete IP original.
- **Payload Len:** especifica la longitud de la cabecera de autenticación (no confundir con cabecera original del paquete IP).
- **Reserved:** se encuentra reservado para uso futuro, actualmente debe ser puesto en 0.
- **Security Parameter Index:** es un número arbitrario de 32 bits. Este valor es usado junto con la dirección IP de destino y el tipo de protocolo IPSec (en este caso, AH) únicamente para identificar la SA para este paquete IP.
- **Sequence Number:** es un campo de 32bits que mantiene un incremento monótonico de la secuencia de paquetes IPSec.

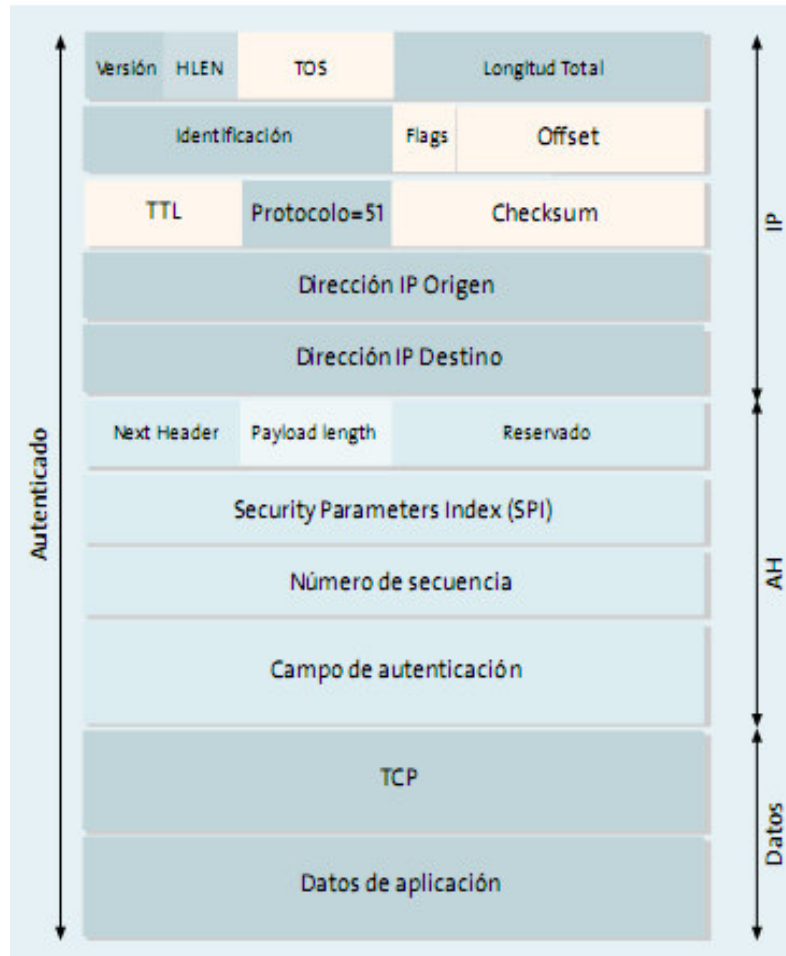


Figura 3.8: Cabecera de Autenticación AH.

- **Authentication Data:** es un campo de longitud variable que contiene el valor de chequeo de integridad ICV (*Integrity Check Value*) para este paquete IP.

Hay que tener en cuenta, que la autenticación no puede ser aplicada sobre la cabecera entera del paquete IP, ya que algunos campos de la cabecera IP original cambian durante el tránsito por Internet. Esos campos son llamados Campos Mutables, y son:

- Type of service (TOS).
- Fragment offset.
- Fragmentation flags.
- Time to live (TTL).
- Header checksum.

Para realizar el proceso de autenticación, el emisor calcula el ICV y lo ubica en el campo Authentication Data. El ICV es un valor *hash* computado sobre todos los campos que la autenticación incluye. La llave secreta es negociada durante el establecimiento de la SA. La *autenticación* de un paquete recibido es verificada cuando el receptor calcula el valor hash y lo compara con el ICV del paquete entrante. Si el paquete IP no es autenticado exitosamente entonces es descartado.

3.3.4. Encapsulating Security Payload - ESP

El protocolo ESP (*Encapsulating Security Payload*) provee *autenticación*, *confidencialidad* de los datos por medio de *cifrado* y una protección opcional antirepetición para los paquetes IP. La *autenticación* y el *cifrado* son también opcionales, pero al menos una de ellas debe ser empleada; de lo contrario, este protocolo carecería de fundamento.

La *confidencialidad* es lograda por medio de técnicas de *cifrado*. Los algoritmos de cifrado empleados para los paquetes IP son definidos por la SA sobre la cual los paquetes son enviados. En este caso, ESP solamente presta el servicio de autenticación para el tráfico. Al igual que con AH varios campos adicionales son insertados en el paquete IP para que presten los servicios mencionados anteriormente.

Muchos de esos campos tienen el mismo significado que en AH, pero la diferencia es que éstos se encuentran a lo largo del paquete IP, algunos en la cabecera ESP, otros en el trailer ESP y otro está en el segmento de autenticación ESP. La figura 3.9 de la pág. 61 muestra la conformación de un paquete IP después que se ha procesado con el protocolo ESP, se observan la ubicación de los campos dentro de cada uno de los segmentos del nuevo paquete.

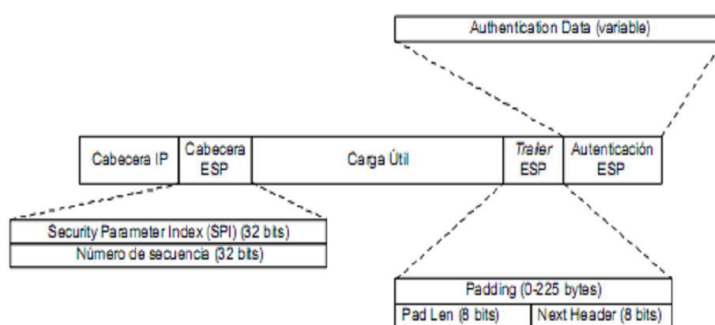


Figura 3.9: Nuevo Paquete IP Procesado con ESP.

La cabecera ESP se encuentra después de la nueva cabecera IP o después de la cabecera IP original modificada, esto dependiendo del modo. El trailer ESP se encuentra al final del paquete IP original y el segmento de autenticación ESP se encuentra después del trailer. Si la autenticación no es aplicada, el segmento de autenticación ESP no es añadido. Si el cifrado es aplicado, cada una de las partes desde el final de la cabecera ESP hasta el final de el trailer ESP son encriptadas (ver figura 3.10 de la página 62).

Al igual que en el protocolo AH, los campos *SPI*, *Sequence Number*, *Next Header* y *Authentication Data*, se encuentran definidos a lo largo del nuevo paquete IP. También se encuentran otros dos campos, el campo *Padding* es usado para rellenar los datos a ser encriptados y completar un límite de 4 bytes, por tanto este campo es de longitud variable. El campo *Pad Len* especifica la longitud del relleno para poder luego ser eliminado después de que los datos son desencriptados.

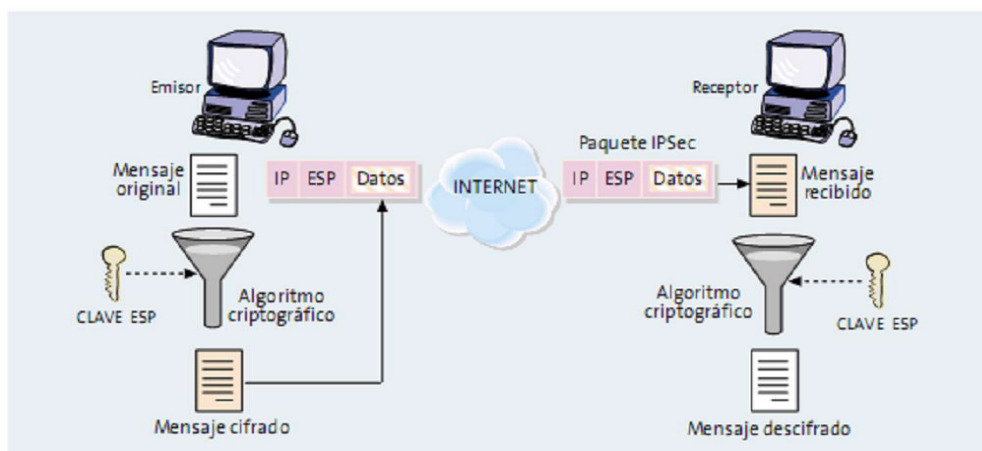


Figura 3.10: Funcionamiento del Protocolo IPSec.

Modo Transporte

En el *modo transporte*, la cabecera ESP es insertada entre la cabecera IP y la carga útil original, y los segmentos trailer y de autenticación ESP son añadidos si son necesarios. Si el paquete está siendo sujeto de un segundo proceso de encapsulamiento ESP, la nueva cabecera ESP es puesta después de la primera y los segmentos trailer y de autenticación son añadidos después de los primeros campos de su mismo ítem. Dado que la cabecera IP original sigue sin alteraciones, el modo de transporte para el protocolo ESP, al igual que en AH, solamente puede ser usado entre hosts. El modo de transporte es el más usado cuando no es necesario ocultar o autenticar las direcciones IP tanto de la fuente como del destino. En la gráfica 3.11 de la pág. 63 se detalla la conformación del nuevo paquete IP usando ESP en modo transporte, además se muestra la parte del paquete que puede ser encriptada y la parte del paquete que puede ser autenticada.

Modo Túnel

En modo *túnel*, el paquete IP original enteramente es encapsulado dentro de un nuevo paquete IP. En la figura 3.12 de la pág. 63 se muestra cómo la nueva cabecera IP y la cabecera ESP son puestas al comienzo del paquete IP original, y los segmentos trailer y de autenticación ESP son añadidos al final del mismo. Si el túnel se encuentra establecido entre hosts, las direcciones IP

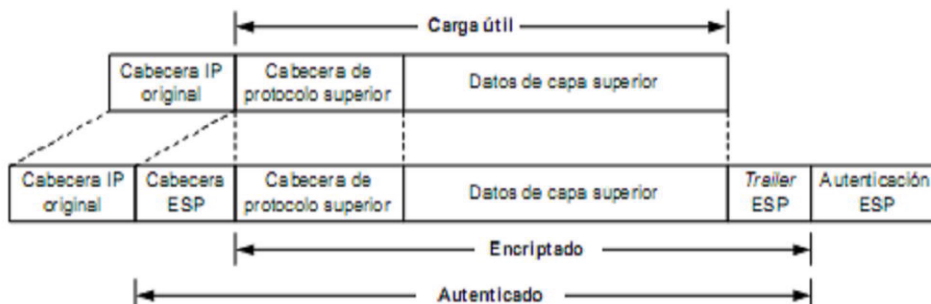


Figura 3.11: Protocolo IPsec en Modo Transporte.

fuente y de destino, en la nueva cabecera IP pueden ser las mismas que en la cabecera original. Si el túnel se encuentra establecido entre dos gateways de seguridad, las direcciones en la nueva cabecera IP serán las direcciones de los gateways. Ejecutando ESP en modo túnel entre gateways de seguridad se puede lograr tanto *confidencialidad* como *autenticación del tráfico* en tránsito entre los dos gateways.

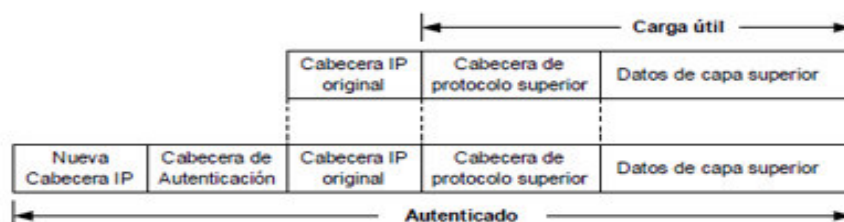


Figura 3.12: Protocolo IPsec en Modo Túnel.

3.3.5. Internet Key Exchange - IKE

Un concepto esencial en IPsec es el de asociación de seguridad (SA) que consiste en 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 unidi-

recional, 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 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.

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 [7].

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:

Fase 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:

1. **Secreto compartido:** como su propio nombre indica, es una cadena de caracteres que únicamente conocen los dos extremos que quieren es-

tablecer una comunicación IPsec. Mediante el uso de 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.

2. **Certificados digitales:** esta implementación soluciona el problema anterior. 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*).

Fase 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. En la figura 3.13 de la pág. 66 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.

3.3.6. Arquitecturas VPN con IPsec

Intranet VPN con IPsec

En la actualidad, incluso las organizaciones 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

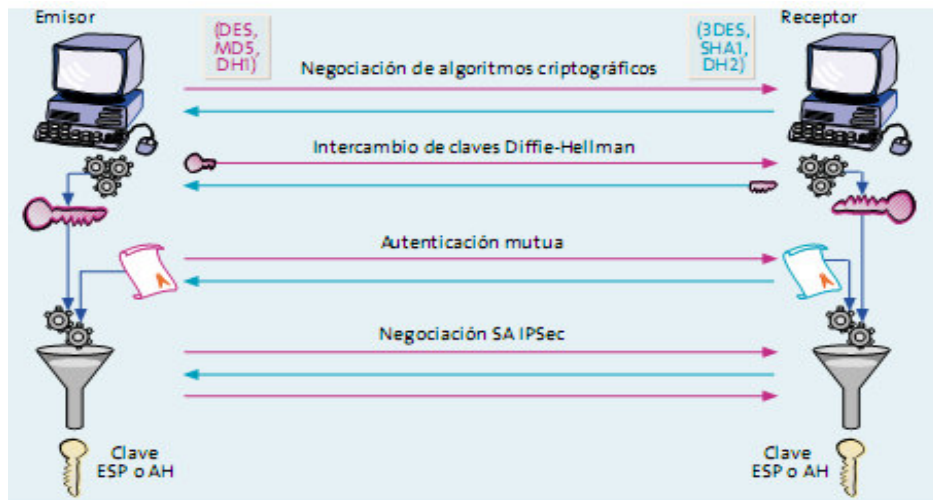


Figura 3.13: Negociación de Llaves en IKE.

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 3.14 de la página 67, es habitual que las oficinas de una organización, debido a su elevado número, presenten una gran diversidad de tecnologías de acceso. Para grandes empresas 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 el mercado están disponibles *gateways IPSec* comerciales que incorporan la posibilidad de configuración redundante y el establecimiento de 50.000 túneles simultáneos o más. Estas prestaciones son suficientes incluso para las organizaciones más grandes.

Acceso Remoto con IPSec

Mediante la instalación de un software en el PC, denominado *cliente IPSec*, es posible conectar remotamente equipo móviles (o PC remota) a la red local de la corporación de forma totalmente segura. El uso del estándar IPSec per-

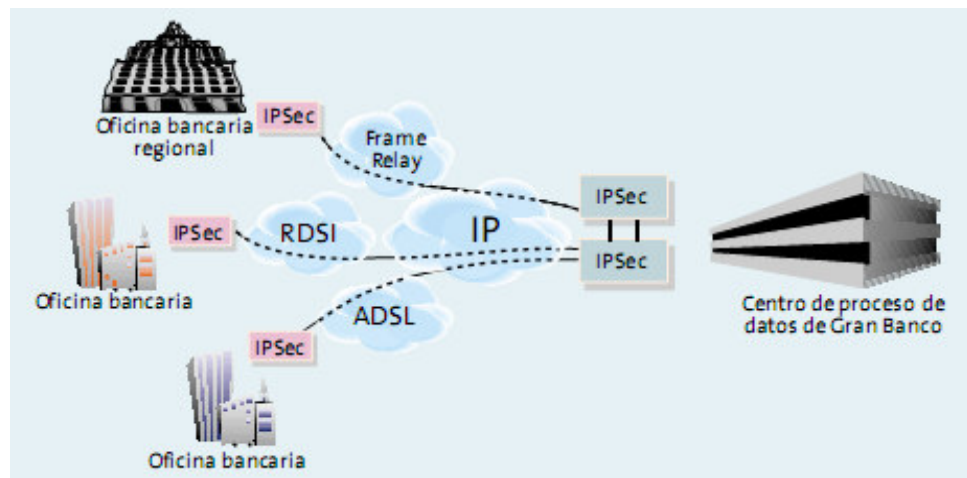


Figura 3.14: IPsec Sobre Distintas Redes.

mite 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. La variedad de sistemas operativos no supone dificultad alguna, ya que todos los sistemas operativos Windows a partir de su versión 2000, Solaris (a partir de versión 8), Linux, etc., incluyen este *cliente IPsec*. Asimismo, 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, 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.

Extranet VPN con IPsec

En un escenario *Extranet VPN* 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, 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.

Una *Extranet VPN* 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 *usuarios remotos* se reduce a un PC portátil (o PC remota) con un *cliente IPSec*.

3.3.7. Limitaciones de IPSec

Si bien podría lograr VPN seguras, la *conectividad remota* y de sitio a sitio ha demostrado ser insuficiente en una gran cantidad de escenarios, debido principalmente a las siguientes limitaciones:

- IPSec VPN es costoso, las instalaciones de clientes consumen tiempo, carecen de la flexibilidad necesaria para proporcionar seguridad de acceso remoto a empleados, clientes y socios.
- Para los usuarios remotos que intentan conectarse a los recursos corporativos, IPSec VPN puede plantear dificultades en que se les permita cruzar algunos cortafuegos corporativo. Esto no es un problema sólo cuando la mayoría de las empresas tienen sus mismos puertos abiertos, entrantes y salientes, que pueden no ser siempre el caso.
- IPSec VPN son programas completos y, por tanto, son grandes, generalmente de 0,1 a 8 megabytes. Esto significa que la descarga es lenta y que no funcionan bien en pequeños dispositivos como PDAs y Blackberry.

3.4. VPN-SSL

Combinar seguridad y sencillez es lo que prometen las Redes Virtuales Privadas basadas en SSL

La tecnología *VPN-SSL* (ó *SSL-VPN*) nació de las necesidades de las empresas que surgen a causa de estos problemas y limitaciones. Esto significó un cambio de paradigma en la propia percepción de la *seguridad, acceso remoto*, el objetivo de una VPN de acceso remoto ya no era sólo la construcción de los túneles de acceso seguro entre dispositivos remotos y redes de confianza,

sino proporcionar a los usuarios autenticados autorizados y con acceso a la información confidencial. La introducción de VPN-SSL trajo una revolución hacia la transparencia en la entrega de soluciones de acceso remoto VPN.

Los objetivos iniciales de la primera generación de *VPN-SSL* son facilitar el acceso a través de *cortafuegos* y una solución de acceso remoto que trabaje desde cualquier lugar independientemente de los dispositivos NAT's y un clientes VPN's.

Tradicionalmente IP (IPSec) entre otras, requiere la instalación de *software cliente* un equipo remoto para poder establecer una conexión, mientras que *SSL-VPN cliente* no necesita instalación y ofrece la funcionalidad de un *VPN clientes* o *Web VPN*. Los usuarios pueden tener acceso a las aplicaciones o archivos compartidos sólo con navegadores web estándares, esta es sin dudas una de las mayores ventajas de esta tecnología (*se dice que si existe conexión HTTPS entonces debe funcionar*).

Para las empresas, SSL-VPN ofrece *versatilidad, facilidad de uso, seguridad y acceso remoto* desde cualquier lugar a socios y clientes, usando los más variados dispositivos como computadoras portátiles, dispositivos móviles, equipos de casa y público. Las implementaciones por software más comunes bajo esta tecnología son SSTP (Secure Socket Tunneling Protocol) de Microsoft y OpenVPN del movimiento Open Source, mientras que por hardware hoy en día existen muchos dispositivos que la soportan.

3.4.1. SSL/TLS Secure Sockets Layer/Transport Layer Security

TLS (*Transport Layer Security - Seguridad de la Capa de Transporte*) es el sucesor del SSL (*Secure Sockets Layer*). Ambos protocolos se utilizan para proporcionar comunicaciones seguras en Internet, usando un modelo de *autenticación y privacidad de la información* entre extremos sobre Internet mediante *criptografía*. Esto es fundamental para mantener la seguridad en el comercio vía Internet.

SSL fue diseñado de manera *modular* (extensible), con soporte para compatibilidad hacia delante y hacia atrás y negociación entre las partes (peer-to-peer). La versión 3.0 del SSL fué desarrollada por Netscape en 1996, que fué la base para desarrollar la versión 1.0 del TLS, protocolo estándar IETF definido en el RFC 2246 por primera vez. El objetivo de Netscape era crear un canal de comunicaciones seguro entre un cliente y un servidor que fuese independiente del sistema operativo usado por ambos, y que éstos se beneficiaran de forma dinámica y flexible de los nuevos adelantos en materia de cifrado, a medida de

que éstos estuvieran disponibles. SSL fue diseñado como un protocolo seguro de propósito general, existen pequeñas diferencias entre SSL 3.0 y TLS 1.0, pero el protocolo permanece sustancialmente igual. El término *SSL* según se usa en este trabajo, se aplica a ambos protocolos (SSL y TLS) a menos que el contexto indique lo contrario.

Normalmente, en SSL sólo el servidor es autenticado (es decir, se garantiza su identidad) mientras que el cliente se mantiene sin autenticar; la autenticación mutua requiere un despliegue de *infraestructura de claves públicas* (PKI) para los clientes. Esta tecnología permite a las aplicaciones *cliente-servidor* comunicarse de una forma diseñada para prevenir escuchas (*eavesdropping*), la falsificación de la identidad del remitente y mantener la integridad del mensaje.

Las primeras implementaciones de SSL sólo podían usar claves simétricas de 40 bits como máximo, ya que el gobierno de los EEUU imponía restricciones sobre la exportación de tecnología criptográfica. Esta clave era de 40 bits ya que las agencias de seguridad nacional americanas podían atacarla mediante fuerza bruta y poder leer así el tráfico cifrado, mientras que los posibles atacantes con menores recursos no podrían leerlo. Finalmente, después de diferentes juicios y la aparición de mejores productos criptográficos diseñados en otros países, se rebajaron las restricciones de exportación de tecnología criptográfica, desapareciendo casi por completo la limitación de claves de 40 bits. Actualmente se usan claves de 128 bits, o incluso más, para las claves de cifrado simétricas. Las implementaciones actuales proporcionan las siguientes opciones:

- **Para criptografía de clave pública:** RSA, Diffie-Hellman, DSA (*Digital Signature Algorithm*) o Fortezza.
- **Para cifrado simétrico:** RC2, RC4, IDEA (International Data Encryption Algorithm), DES (Data Encryption Standard), Triple DES o AES (Advanced Encryption Standard).
- **Con funciones hash:** MD5 o de la familia SHA.

3.4.2. Arquitectura de SSL

SSL trabaja sobre el protocolo TCP y por debajo de protocolos como HTTP, IMAP, LDAP, etc., y puede ser usado por todos ellos de forma transparente para el usuario. Opera entre la *capa de transporte* y la *capa de sesión* del modelo OSI (o entre la capa de transporte y la de aplicación del modelo

TCP-IP) y está formado, a su vez, por dos capas y cuatro componentes bien diferenciados (ver figura 3.15 de la página 71).

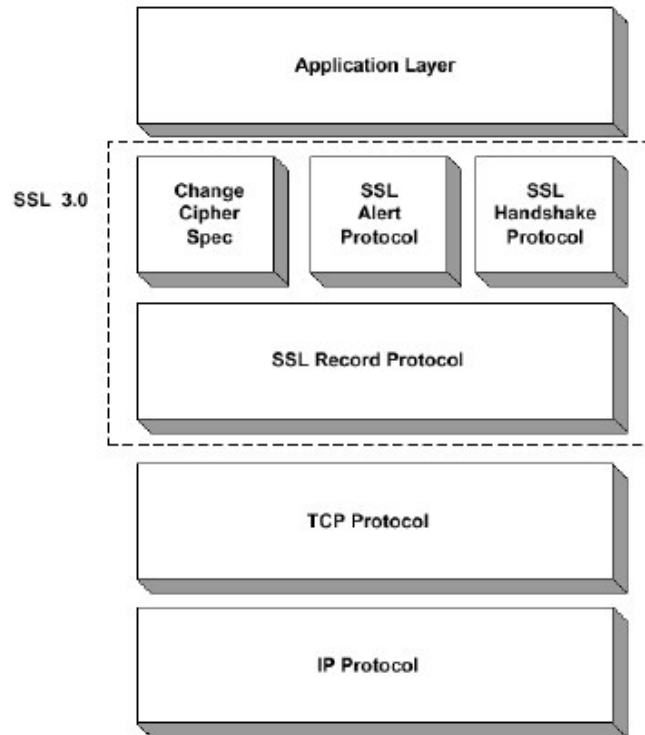


Figura 3.15: Estructura de Protocolos del Protocolo SSL.

El *protocolo de registro* (*Record Protocol*) se encarga de encapsular el trabajo de los elementos de la capa superior, construyendo un canal de comunicaciones entre los dos extremos objeto de la comunicación.

El verdadero corazón de SSL está en el *protocolo de Handshake* que es el encargado de intercambiar la clave que se utilizará para crear un canal seguro mediante un algoritmo eficiente de cifrado simétrico. También es responsabilidad de este protocolo coordinar los estados de ambos extremos de la transmisión.

El *protocolo de Alerta* es el encargado de señalar problemas y errores concernientes a la sesión SSL establecida.

Por último, el *Change Cipher Spec Protocol* está formado por un único mensaje consistente en un único byte de valor 1 y se utiliza para notificar un

cambio en la estrategia de cifrado.

3.4.3. Funcionamiento Básico de SSL

El *protocolo de Handshake* es el encargado de negociar los atributos de la sesión SSL que permitirán construir un *canal seguro de comunicaciones*. En primer lugar el cliente envía un mensaje *Client Hello* al servidor el cual debe de responder con un mensaje similar de *Server Hello*. Estos mensajes son utilizados para dar a conocer ciertas características de ambos: versión del protocolo usada, algoritmos de cifrado conocidos y preferidos, funciones hash y métodos de compresión a utilizar. En este momento, además, el servidor asigna un identificador a la sesión y se hace constar la fecha y hora de la misma. Generalmente el servidor, que es el segundo en contestar, elige los algoritmos más fuertes de entre los soportados por el *cliente*. Si no hay acuerdo en este punto se envía un mensaje de error y se aborta la sesión.

A continuación del mensaje de *Server Hello*, el servidor puede enviar su *Certificado* (típicamente un X.509) de forma que sea autenticado por el cliente y que, además, este reciba su *clave pública*. Si no es así, le envía al cliente su clave pública mediante un mensaje de *Server Key Exchange* (o también si ha enviado su Certificado y este es únicamente para firma y autenticación). Está claro que al menos uno de estos dos mensajes es necesario para establecer el canal seguro. Un último mensaje que puede enviar el servidor en esta fase de negociación es una solicitud de certificado al cliente. Por último, la fase concluye con el envío, por parte del servidor, de un mensaje de *Server Hello Done*.

Si el Servidor ha solicitado su certificado al cliente, este debe de responder con él o con un mensaje de alerta indicando que no lo posee. A continuación se envía un mensaje de *Client Key Exchange* donde el cliente envía al servidor la clave maestra cifrada mediante la clave pública, además un número aleatorio generado por él y que actuará como clave del algoritmo simétrico acordado para el intercambio de datos.

Por último, si el cliente ha enviado un certificado y éste tiene capacidades de firma, enviará adicionalmente un mensaje de *Certificate Verify* firmado digitalmente con objeto de que el servidor pueda verificar que la firma es válida. En este punto el cliente da por concluida la fase mediante un mensaje de *Change Cipher Spec* seguido, inmediatamente, de un mensaje de *Finished* que ya va cifrado mediante los algoritmos y claves recién negociados.

En respuesta, el servidor envía su propio mensaje de *Change Cipher Spec* y, a continuación, su mensaje de *Finished* cifrado con los parámetros negociados.

En este momento finaliza la fase de *Handshake* y cliente y servidor pueden intercambiar datos libremente. Podemos ver un esquema de este intercambio de mensajes en la figura 3.16 de la página 73:

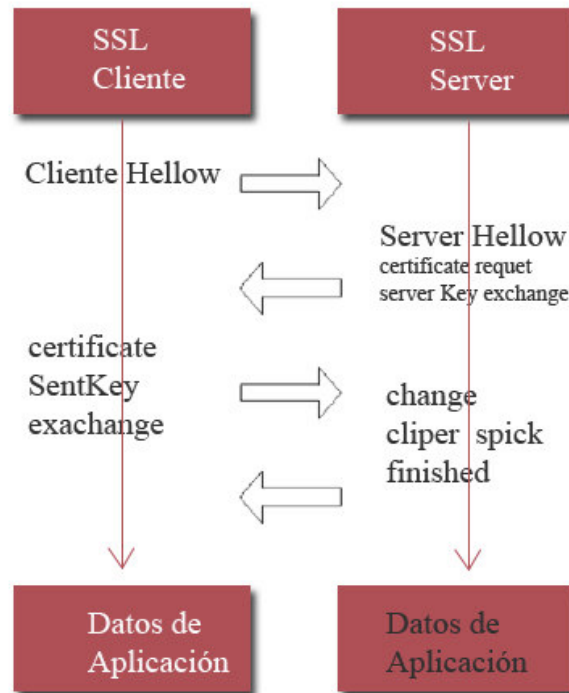


Figura 3.16: Intercambio de Mensajes en SSL.

Durante la transmisión de datos los mensajes el *protocolo de registro* se encarga de fragmentar y comprimir cada mensaje, para luego aplicarle una *función hash* a cada uno de los bloques, proceso con el cuál pretende asegurar la integridad de los mismos. Por último realiza el cifrado de los datos y los envía al otro extremo donde el mismo protocolo realizará un proceso inverso de reconstrucción.

Una sesión SSL puede comprender múltiples conexiones. Adicionalmente, se pueden establecer múltiples sesiones SSL simultáneas, cada una de ellas es controlada por una *máquina de control de estados*.

3.4.4. Aplicaciones e Implementaciones de SSL

Una de las ventajas de SSL es que *es independiente del protocolo de aplicación*, ya que es posible ubicarlo por encima del mismo en forma transparente. Este protocolo tiene multitud de aplicaciones en uso actualmente, la mayoría de ellas son *versiones seguras* de programas que emplean protocolos que no lo son. Hay versiones seguras de servidores y clientes de protocolos como el HTTP (HTTPS en este caso), NNTP, LDAP, IMAP, POP3, etc.

Existen multitud de implementaciones del protocolo, tanto comerciales como de libre distribución, una de las más populares es la biblioteca *OpenSSL*, que constituye la base del software *OpenVPN*, disponible bajo licencia GNU. El lenguaje Java también incluye soporte para el protocolo con la *Extensión de Sockets Seguros de Java (JSSE)*.

Cada una de las aplicaciones SSL tiene las siguientes propiedades:

- **Privada:** después de un proceso inicial de *handshake* en el cual se define una clave secreta, se envía la información encriptada por medio de algún método simétrico (DES, RC4).
- **Segura:** aporta identidad de cada extremo, es autenticada usando métodos de cifrado asimétricos o de clave pública (RSA, DSS).
- **Confiable:** el transporte del mensaje incluye un control de la *integridad* del mismo usando una MAC cifrada con SHA y MD5.

3.4.5. Conceptos y Técnicas de VPN-SSL

El *acceso remoto seguro* basado en SSL aglutina diversas tecnologías, basados en cuatro conceptos básicos:

- **Proxy:** todos los dispositivos y software SSL-VPN ofrecen al menos la función de proxy de páginas Web. Cuando el usuario se conecta a un servidor Web, éste descarga la página solicitada y se la envía a su navegador sobre una *conexión SSL*.
- **Conversión de aplicaciones:** las cosas se complican cuando se trata de cualquier otro dato que no sean una página Web. Surge entonces la *conversión de aplicaciones*. Cuando, por ejemplo, los dispositivos SSL-VPN han de tratar los servidores de ficheros, por lo general *hablará*

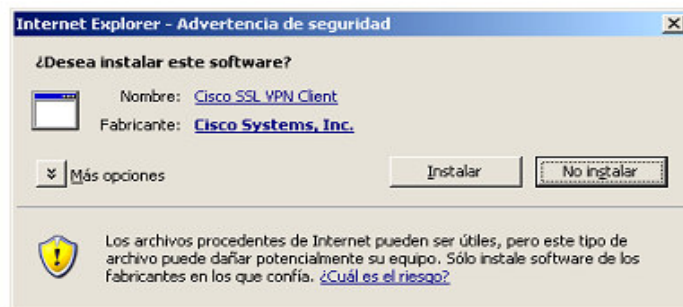


Figura 3.17: Advertencia de Instalación de Plugins en Internet Explorer.

como protocolo nativo CIFS (de Microsoft), o FTP. Por ello, habrá de convertirlos a HTTP y HTML, a fin de que el usuario final vea el servidor de ficheros como si fuera una página Web; es decir, la aplicación se *websifica*.

- **Port forwarding:** pero la conversión de aplicaciones sólo funciona efectivamente con ciertas transacciones. Se impone, entonces, la técnica *port forwarding*, que requiere en el sistema cliente una herramienta del tipo *Java* o *ActiveX* (Pluning de Microsoft). Consiste en dedicar a cada aplicación un puerto determinado en el que se tunelizan los paquetes dentro de *conexiones SSL*. El server SSL-VPN los *abre* y los envía al *servidor de aplicaciones*. Se trata de una técnica muy efectiva pero muestra serias limitaciones, por ejemplo, sólo funciona con aplicaciones muy predecibles en cuanto a sus requerimientos y necesidades de conectividad de red. La figura 3.17 de la página 75 muestra un *mensaje de advertencia* en el navegador Internet Explorer, antes la instalación de un ActiveX correspondiente al *software cliente* de un dispositivo de la empresa *Cisco*.
- **Extensión de red:** conecta el sistema del usuario final a la red corporativa mediante controles de acceso exclusivamente basados en información de nivel de red, como dirección IP de destino y número de puerto. Dependen del sistema operativo que se utiliza y requiere acceso administrativo al sistema local. Las extensiones de red SSL-VPN corren en lo alto del protocolo SSL, sacrificando la mayor seguridad que ofrece *IPSec*.

3.4.6. Inconvenientes de las VPN-SSL

Secure Sockets Layer (SSL) para realizar el *acceso remoto* se basa en un concepto simple, utilizar la encriptación y capacidades de autenticación incorporado en todos los navegadores web para proporcionar *acceso remoto seguro* a aplicaciones corporativas.

Una ironía de las VPN-SSL es que su activo más importante es su aspecto más problemático. La libertad y la movilidad del navegador significa que los usuarios puedan ejecutar aplicaciones y recursos de la red de acceso desde cualquier parte, un kiosco del aeropuerto, un café Internet, incluso la casa de un amigo. Mientras que la libertad puede aumentar la productividad, también expone su red a un número ilimitado de equipos de seguridad cuyo estado es desconocido. Su red puede experimentar un mayor riesgo de virus, troyanos y otros códigos maliciosos, tales como capturadores de teclado [3].

El acceso basado en navegador tiene otras complicaciones también como la de *autenticación de usuario*, por defecto está limitado a un *nombre de usuario y contraseña*, que es notoriamente inseguro. Por último, los costos de los dispositivos VPN-SSL (Hardware) son elevados, aunque exista una variedad de precios entre las opciones que ofrecen los distintos fabricantes, existe una gran diferencia de precios con otros dispositivos que manejan protocolo como L2TP e IPsec. Esta última desventaja o inconveniente se podría decir que es *relativa*, porque una implementación IPsec puede ser redituable en costos de hardware pero costosa en tiempo de configuración y mantenimiento.

3.4.7. Ventajas de SSL-VPN sobre IPsec

Las principales ventajas son las siguientes:

- SSL-VPN son a menudo mucho menos costoso que el despliegue de redes VPN IPsec. Esto se debe a que, con clientes SSL-VPN, no hay costo de licencias de software de propiedad del cliente, sin gastos generales de administración involucrados en la instalación de software cliente, y menos tiempo necesario para el apoyo técnico de clientes debido a la facilidad de uso [10].
- SSL-VPN permite a las organizaciones a crear la identidad del usuario de acceso basado en políticas, que ofrece acceso a la red granular a los empleados, socios y clientes sobre la base de la identidad del usuario y el perfil de trabajo [10].

- SSL utiliza el puerto TCP 443, que normalmente se abre en los cortafuegos, trabajará a través de firewalls sin ninguna configuración especial [3].
- IPSec usa puertos UDP específicos, si no están en uso, estos puertos estarán bloqueados por el servidor de seguridad.
- SSL-VPN también puede proporcionar una ventaja de seguridad. Cuando el acceso está restringido a aplicaciones específicas, las posibilidades de acceso no autorizado se reducen.
- Hoy en día, SSL-VPN ofrece también protección de datos en el navegador, después de que el usuario cierra la sesión, a fin de eliminar la información sensible que pueda haber sido utilizado durante el curso de un acceso seguro. Esto incluye la eliminación de cualquier caché las credenciales de usuario y la eliminación de la cola o temporal en caché de archivos. Algunos SSL-VPN pueden ser configuradas para evitar que un usuario realice copias locales de la información sensible de la empresa en un equipo de trabajo.
- Conexiones pobres, intermitentes e interrumpidas no causan la caída de la VPN.
- Permite mediante un *certificado digital*, usar su navegador para verificar la autenticidad del sitio y comunicarse con él en forma segura.

3.4.8. Software VPN-SSL

Aunque se emplea SSL para crear túneles no existe un estándar que especifique cómo funciona una VPN-SSL, sino que hay distintas implementaciones que funcionan bastante bien. Entre las más interesantes se encuentran *OpenVPN* del movimiento Open Source y el protocolo *SSTP (Secure Socket Tunneling Protocol)* de Microsoft.

OpenVPN

OpenVPN es una solución de conectividad basada en software: SSL (Secure Sockets Layer) bajo la librería OpenSSL y VPN Virtual Private Network (Red Virtual Privada). Soporta diferentes medios de autenticación como certificados, smart cards, y / o usuarios / contraseñas, y permite políticas de control de acceso para usuarios o grupos usando reglas de firewall aplicadas a las interfaces virtuales de la VPN. Esta solución resulta una muy buena opción

en tecnologías Wi-Fi (redes inalámbricas EEI 802.11) y soporta una amplia configuración, entre ellas balanceo de cargas entre otras. Está publicado bajo licencia de código libre (Open Source).

Es una solución multiplataforma que ha simplificado mucho la configuración de VPN's dejando atrás los tiempos de otras soluciones difíciles de configurar como IPSec haciéndola más accesible para gente inexperta en este tipo de tecnología [12].

Esta arquitectura está implementada sobre la capa 2 y capa 3 del modelo OSI, de esta manera los túneles de OpenVPN pueden transportar tramas Ethernet, paquetes IPX, y los paquetes NETBIOS del navegador (Explorer) de la red Windows, que son un problema en la mayoría de las otras soluciones VPN.

Algunas de características de OpenVPN son:

- **Protección de sesión con el cortafuego interno:** en una sesión conectada con la *oficina central* de su compañía mediante un *túnel VPN* puede cambiar el setup de su red en su ordenador portátil, para enviar todo su tráfico de la red a través del túnel. Una vez que OpenVPN haya establecido un túnel, el cortafuego central en la oficina central de la compañía puede proteger el ordenador portátil, aún cuando él no sea una máquina local. Solamente un puerto de la red se debe abrir de forma local para trabajar la sesión. El *cortafuego central* protege al empleado siempre que él o ella esté conectado a través del VPN.

Las conexiones de OpenVPN pueden ser establecidas a través de casi cualquier cortafuego, se dice que "*si tienes acceso a Internet y si puedes tener acceso a la Web, los túneles de OpenVPN deben poder trabajar*".

- **Soporte de Proxy y configuraciones:** OpenVPN tiene soporte de Proxy y se puede configurar para funcionar como un servicio de TCP o de UDP, y como *servidor* o *cliente*. Como servidor, OpenVPN espera simplemente hasta que un cliente solicita una conexión, mientras que como cliente, intenta establecer una conexión según su configuración.
- **Apertura de un solo puerto en el cortafuegos para permitir conexiones entrantes:** desde OpenVPN 2.0, el modo especial del servidor permite conexiones entrantes múltiples en el mismo puerto del TCP o del UDP, mientras que todavía usa diversas configuraciones para cada conexión. Los *interfaces virtuales* permiten reglas muy específicas del

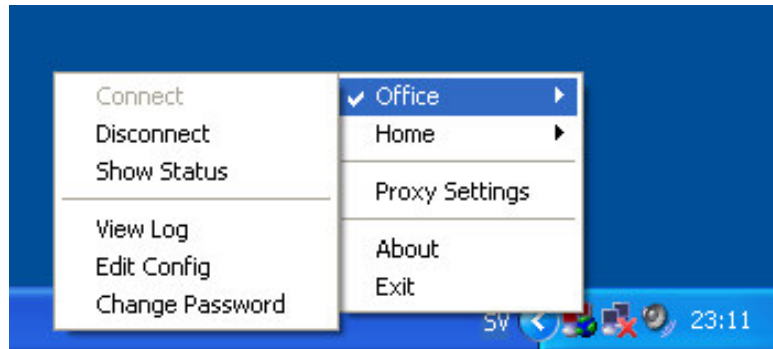


Figura 3.18: Interfaz GUI de OpenVPN Para Sistemas Operativos Windows.

establecimiento de una red y del cortafuegos donde todas las reglas, restricciones, mecanismos de la expedición, y conceptos como NAT se pueden utilizar con los túneles de OpenVPN.

- **Alta flexibilidad con posibilidades extensas de lenguaje interpretado (scripting):** OpenVPN ofrece numerosos puntos durante la conexión para la ejecución de los scripts individuales. Estos scripts se pueden utilizar para una gran variedad de propósitos de la autenticación, recuperación en caso de fallos (failover) entre otros.
- **Soporte transparente y alto rendimiento para IP's Dinámicas:** si se usa OpenVPN, no hay necesidad de utilizar más IPs estáticas de cualquier lado del túnel. Ambos puntos finales del túnel pueden tener acceso barato de ADSL con el IPs dinámicas y los usuarios no notarán un cambio del IP de cualquier lado. Las sesiones del *Terminal Server de Windows* y las sesiones *seguras de Shell* (SSH) parecerán congeladas solamente por algunos segundos, pero no terminarán y continuarán con la acción solicitada después de una corta pausa.
- **Instalación simple en cualquier plataforma:** la instalación y el uso son increíblemente simples. Especialmente, si se ha intentado instalar IPSec con diversas configuraciones, se apreciará la facilidad de instalación de OpenVPN. En plataformas Windows se cuenta con una interfaz gráfica muy amigable que permite el monitoreo de la Red Privada Virtual, la cual puede ser visualizada en la imagen 3.18 de la página 79.
- **Diseño modular:** el diseño modular consta de un alto grado de simplicidad en seguridad y el establecimiento de una red virtual es excepcional.

Ninguna otra solución VPN puede ofrecer la misma gama de posibilidades a este nivel de seguridad. Con respecto a la estabilidad, OpenVPN es un programa muy robusto y ofrece la posibilidad de implementar esquemas de servidores redundantes y con balance de carga [13].

Las principales desventajas de OpenVPN son las que se mencionan seguidamente:

- Todavía existe poca gente que conoce como usar OpenVPN.
- Al día de hoy sólo se puede realizar conexiones entre computadoras. Pero esto empieza a cambiar, dado que ya existen compañías desarrollando dispositivos con clientes OpenVPN integrados.
- No tiene compatibilidad con IPSec que justamente es el estándar actual para soluciones VPN [12].

SSTP (Secure Socket Tunneling Protocol)

El protocolo *Secure Socket Tunneling Protocol* (SSTP) de Microsoft es, por definición, un protocolo de *capa de aplicación* que encapsular tráfico PPP por un canal SSL del protocolo HTTPS. El uso de habilita la compatibilidad con métodos de autenticación seguros, como EAP-TLS. El empleo de HTTPS significa que el tráfico pasa a través del puerto 443 (TCP), un puerto que se suele usar para el *acceso web* y eliminando así los problemas asociados con las conexiones VPN basadas en L2TP o PPTP (conocido *error 800 - problemas de conectividad*), que pueden ser bloqueadas por algunos proxies Web, firewall y routers en las configuraciones de los carrier's.

La *Capa de sockets seguros* (SSL) proporciona seguridad de nivel de transporte con negociación, cifrado y comprobación de integridad de claves mejorados.

SSTP se basa en el protocolo SSL en lugar de PPTP o IPSec, a pesar de que está estrechamente relacionado con SSL, no se puede hacer una comparación directa entre SSL y SSTP, porque SSTP es sólo una diferencia de protocolo de túnel SSL. Existen muchas razones para elegir SSL y no IPSec como base para SSTP, las ventajas mencionadas en el apartado anterior son validas también para este protocolo, otras razones son:

- Debido a que IPSec se ha desarrollado para *conexión seguras de sitio a sitio*, es probable que presente problemas para *usuarios remotos* que

intentan conectarse desde un lugar con un número limitado de direcciones IP.

- IPsec no soporta *dynamic DNS*.

Esta tecnología sólo está soportada por Windows Server 2008 y Windows Vista Service Pack 1; existen también paquetes de software como IAG 2007, un software que funciona como punto de bastión en interfaces de entrada a redes LAN's Corporativas [13].

Funcionamiento Básico de SSTP Cuando se inicia una conexión VPN-SSTP sucede lo siguiente:

1. EL software cliente (*SSTP client*) establece una conexión TCP con el servidor SSTP entre un puerto dinámico del cliente y el puerto 443 del servidor.
2. El cliente SSTP envía un *SSL Client-Hello*, indicando que el cliente quiere crear una *sesión SSL* con el servidor.
3. EL servidor SSTP envía su certificado de máquina al cliente.
4. El Cliente SSTP valida el certificado de equipo, determina el método de cifrado para la *sesión SSL*, genera una clave para la misma y cifra esta con la clave pública del certificado del servidor SSTP, y a continuación lo envía al servidor.
5. El servidor SSTP descifra la clave de sesión SSL mandada por el cliente con su clave privada. Todas las comunicaciones posteriores se realizan ya con la nueva clave negociada.
6. El cliente SSTP envía una petición de HTTP sobre SSL al servidor de SSTP.
7. El cliente SSTP negocia un túnel SSTP con el servidor SSTP.
8. El cliente SSTP negocia una *conexión PPP* con el servidor SSTP. Esta negociación incluye las credenciales de autenticación del usuario, el método de autenticación y la configuración de IPv4 e IPv6.
9. El cliente SSTP comienza a enviar tráfico IPv4 o IPv6 sobre el *enlace PPP*.

Bibliografía

- [1] G. Brollo. *Redes Virtuales Privadas*. Brollo, Argentina, 2009.
- [2] Network Magazine. *Internet-based VPNs: Business or Cattle Class*. Revista Network Magazine, USA, 2004.
- [3] D. Piscitello. *Completing the Secure Application Access Puzzle: SSL VPNs offer the Greatest Promise, but their Capabilities Still need some Enhancement*. Business Communications Review, USA, 2005.
- [4] RFC2401. *Security Architecture for the Internet Protocol*. www.wikipedia.org, USA, 1998.
- [5] RFC2402. *IP Authentication Header*. RFC2402, USA, 1999.
- [6] RFC2406. *IP Encapsulating Security Payload (ESP)*. RFC2406, USA, 1999.
- [7] RFC2408. *Internet Security Association and Key Management Protocol - ISAKM*. RFC2408, USA, 1999.
- [8] RFC2409. *The Internet Key Exchange (IKE)*. RFC2409, USA, 1999.
- [9] Kim Lew Spanier and Stevenson. *Internetworking Technologies Handbook*. Cisco Press, USA, 1997.
- [10] Cyberoam White. *SSL VPN over UTM Ú Secure Remote Access*. Business Communications Review, USA, 2005.
- [11] Wikipedia. *L2TP - Layer 2 Tunneling Protocol*. www.wikipedia.org, USA, 2009.
- [12] Wikipedia. *SSL VPN*. Wikipedia, USA, 2009.
- [13] www.microsoft.com. *SSTP en Windows Server 2008*. Microsoft, USA, 2010.

Índice alfabético

- AAA, 24
- active directory, 30
- AES, 70
- ATM, 7, 8, 46, 47, 51
- Authentication Header (AH), 58

- BRI, 12

- CHAP, 20, 24, 50
- clear channel, 4
- controlador de dominio, 45

- DES, 51, 70
- Diffie-Hellman, 28, 64, 70
- DNS, 17
- DSA, 70

- EAP, 16, 50
- EAP-TLS, 44, 80
- ECP, 51
- ESP, 60
- Ethernet, 41, 78

- Firewall, 57
- Fortezza, 70
- Frame Relay, 4, 5, 7, 8, 41, 45–47, 51

- GRE, 40–44
 - cabecera mejorada, 44
- hash, 24, 27, 60, 65
- HDLC, 17
- HMAC, 64

- HTTP, 70
- HTTPS, 80

- IDEA, 70
- IETF, 45, 64, 69
- IKE, 20, 63–65
- IMAP, 70
- Internet, 2, 13, 34, 46, 47, 69
- IPCP, 17, 51
- IPSec, 34, 51–53, 55, 56, 63–67, 78
- IPv4, 52
- IPv6, 52, 81
- IPX, 46
- ISAKMP, 64
- ITU-T, 7

- L2F, 39, 45, 46
- L2TP, 33, 34, 46, 47, 50–52
- LAN, 2, 5, 13, 34, 37, 41, 45, 46
- LDAP, 70
- listas de capacidades, 30
- listas de control de acceso, 29

- MD5, 70
- MPLS, 38
- MPPC, 17
- MPPE, 17, 40, 44, 51
- MS-CHAP, 44, 50

- NAS, 16, 25, 42
- NAT, 79
- NCP, 17
- NETBEUI, 46

- NTFS, 45
- Oakley, 64
- Open Source, 78
- OpenSSL, 74, 77
- OSI, 4, 33, 70

- PAP, 20, 24
- password únicos, 23
- password tradicionales, 23
- PKI, 65, 67, 70
- POP, 36–38
- PPP, 13, 15–17, 33, 39, 41–47, 50–52, 80
- PPTP, 33, 34, 39–46, 51
- PRI, 12
- protocolo de autenticación extensible, 16
- proxy, 78

- RADIUS, 24, 45
- RAS, 13, 28
- RC2, 70
- RC4, 70
- RDSI, 10–12
- Redes Virtuales Privadas, 1
- RFC, 69
- RSA, 44, 51, 70
- RSDI, 4
- RTPC, 10

- S/KEY, 24
- SAD, 55
- SHA, 70
- SPD, 55
- SSL, 33, 37, 69–73
- SSL/TLS, 69
- SSTP, 80

- TACKCS+, 45
- TCP, 20, 40, 42, 43, 54, 70, 78
- TCP-IP, 13, 71
- triple DES, 70
- tunelamiento, 32

- UDP, 20, 47, 54, 78
- UNIX, 29

- VPN, 2, 10, 13
- VPN-SSL, 68, 69

- WAN, 4, 7
- Wi-Fi, 78

- X.25, 5, 46, 51
- X.509, 72