Universidad de San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería Mecánica Eléctrica

IMPLEMENTACIÓN DE UN ENLACE DE RED PRIVADA VIRTUAL UTILIZANDO EL PROTOCOLO DE SEGURIDAD IPSec

Belter Molina Guevara
Asesorado por el Ing. Carlos Eduardo Guzman Salazar

Guatemala, junio de 2014

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

IMPLEMENTACIÓN DE UN ENLACE DE RED PRIVADA VIRTUAL UTILIZANDO EL PROTOCOLO DE SEGURIDAD IPSec

TRABAJO DE GRADUACIÓN

PRESENTADO A LA JUNTA DIRECTIVA DE LA
FACULTAD DE INGENIERÍA
POR

BELTER MOLINA GUEVARA
ASESORADO POR EL ING. CARLOS EDUARDO GUZMAN SALAZAR

AL CONFERÍRSELE EL TÍTULO DE

INGENIERO EN ELECTRÓNICA

GUATEMALA, JUNIO DE 2014

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

NÓMINA DE JUNTA DIRECTIVA

DECANO	Ing. Murphy Olympo Paiz Recinos
VOCAL I	Ing. Alfredo Enrique Beber Aceituno
VOCAL II	Ing. Pedro Antonio Aguilar Polanco
VOCAL III	Inga. Elvia Miriam Ruballos Samayoa
VOCAL IV	Br. Walter Rafael Véliz Muñoz
VOCAL V	Br. Sergio Alejandro Donis Soto
SECRETARIO	Ing. Hugo Humberto Rivera Pérez

TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO

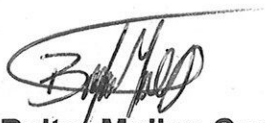
DECANO	Ing. Murphy Olympo Paiz Recinos
EXAMINADOR	Ing. Carlos Eduardo Guzman Salazar
EXAMINADOR	Ing. Francisco Javier Gonzales Lopez
EXAMINADOR	Ing. Byron Odilio Arrivillaga Mendez
SECRETARIO	Ing. Hugo Humberto Rivera Pérez

HONORABLE TRIBUNAL EXAMINADOR

En cumplimiento con los preceptos que establece la ley de la Universidad de San Carlos de Guatemala, presento a su consideración mi trabajo de graduación titulado:

IMPLEMENTACIÓN DE UN ENLACE DE RED PRIVADA VIRTUAL UTILIZANDO EL PROTOCOLO DE SEGURIDAD IPSec

Tema que me fuera asignado por la Dirección de la Escuela de Ingeniería Mecánica Eléctrica, con fecha 7 de junio del 2011.



Belter Molina Guevara

Guatemala 20 de Mayo de 2014

Ingeniero
Guillermo Antonio Puente Romero
Director de la Escuela de Ingeniería Mecánica Eléctrica
Escuela de Ingeniería Mecánica Eléctrica
Facultad de Ingeniería, USAC

Estimado Ingeniero Guillermo Puente

Me permito dar aprobación al trabajo de graduación titulado "IMPLEMENTACION DE UN ENLACE DE RED PRIVADA VIRTUAL UTILIZANDO EL PROTOCOLO DE SEGURIDAD IPSec", del señor Belter Molina Guevara con carnet 2002-12525, por considerar que cumple con los requisitos establecidos.

Por tanto, el autor de este trabajo de graduación y, yo, como su asesor, nos hacemos responsables por el contenido y conclusiones del mismo.

Sin otro particular, me es grato saludarle.

Atentamente

Ing. Carlos Eduardo Guzman Salazar

Asesor

CARLOS GUZMAN SALAZAR
Ingeniero Electricista
Col. No. 2762

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA

FACULTAD DE INGENIERIA

Ref. EIME 21. 2014
Guatemala, 21 de MAYO 2014.

Señor Director
Ing. Guillermo Antonio Puente Romero
Escuela de Ingenierìa Mecànica Elèctrica
Facultad de Ingenierìa, USAC.

Señor Director:

Me permito dar aprobación al trabajo de Graduación titulado: IMPLEMENTACIÓN DE UN ENLACE DE RED PRIVADA VIRTUAL UTILIZANDO EL PROTOCOLO DE SEGURIDAD IPSec, del estudiante Belter Molina Guevara, que cumple con los requisitos establecidos para tal fin.

Sin otro particular, aprovecho la oportunidad para saludarle.

Atentamente,
ID Y ENSEÑAD A TODOS

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
DIRECCION ESCUELA DE INGENIERIA MECANICA ELECTRICA
FACULTAD DE INGENIERIA

Ing. Carlos Eduardo Guzmán Salazar
Coordinador Área Electrónica

SIO

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA

FACULTAD DE INGENIERIA

REF. EIME 21. 2014.

El Director de la Escuela de Ingeniería Mecánica Eléctrica, después de conocer el dictamen del Asesor, con el Visto Bueno del Coordinador de Área, al trabajo de Graduación del estudiante; BELTER MOLINA GUEVARA titulado: IMPLEMENTACIÓN DE UN ENLACE DE RED PRIVADA VIRTUAL UTILIZANDO EL PROTOCOLO DE SEGURIDAD IPSec, procede a la autorización del mismo.

Ing. Guillermo Antonio Puente Romero

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
DIRECCION ESCUELA DE INGENIERIA MECANICA ELECTRICA
FACULTAD DE INGENIERIA

GUATEMALA, 26 DE MAYO 2,014.

Universidad de San Carlos
De Guatemala

Facultad de Ingeniería
Decanato

Ref. DTG.D.260-2014

El Decano de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer la aprobación por parte del Director de la Escuela de Ingeniería Mecánica Eléctrica, al trabajo de graduación titulado: **IMPLEMENTACIÓN DE UN ENLACE DE RED PRIVADA VIRTUAL UTILIZANDO EL PROTOCOLO DE SEGURIDAD IPSec,** presentado por el estudiante universitario: **Belter Molina Guevara** y después de haber culminado las revisiones previas bajo la responsabilidad de las instancias correspondientes, se autoriza la impresión del mismo.

IMPRÍMASE.

Ing. Murphy Olympo Paiz Recinos
Decano

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
DECANO
FACULTAD DE INGENIERIA

Guatemala, junio de 2014

/cc

ACTO QUE DEDICO A:

Dios	Por ser una importante influencia en mi carrera, entre otras cosas.
Mis padres	Antonia Guevara Parada y Herlindo Molina, por su amor incondicional, en especial a mi madre.
Mis hermanos	Robert, Esvin y Freddy Molina, por todo el apoyo brindado.
Mis hermanas	Aracely, Iris, Mary, Odilia y Marina Molina por todo el apoyo brindado.
Mis amigos	Quienes fueron agregándose a mi vida a lo largo de mi formación académica, gracias por su apoyo.
Mi familia	Por ser una importante influencia en mi carrera, entre otras cosas.
Universidad de San Carlos de Guatemala	En especial a la Facultad de Ingeniería por acogerme en su seno y ser mí alma máter, la cual me brindó mis conocimientos científicos, técnicos y éticos, hoy me siento orgulloso de pertenecer a tan prestigiosa casa de estudios.

ÍNDICE GENERAL

ÍNDICE DE ILUSTRACIONES

FIGURAS

TABLAS

GLOSARIO

Acceso remoto Es el acceder desde una computadora a un recurso ubicado físicamente en otra computadora geográficamente en otro lugar, a través de una red local o externa.

Ancho de banda Cantidad de información o de datos que se puede enviar a través de una conexión de red en un período de tiempo dado.

Autenticación Es el proceso de intento de verificar la identidad digital del remitente de una comunicación como una petición para conectarse.

ADSL Asymmetric Digital Subscriber Line es una tecnología de acceso a internet de banda ancha, lo que implica una velocidad superior a una conexión por módem en la transferencia de datos, ya que el módem utiliza la banda de voz y por tanto impide el servicio de voz mientras se use y viceversa.

ATM	Tecnología de *switching* basada en unidades de datos de un tamaño fijo de 53 bytes llamadas celdas. ATM opera en modo orientado a la conexión, esto significa que cuando dos nodos desean transferir deben primero establecer un canal o conexión por medio de un protocolo de llamada o señalización.
Browser	Software que permite el acceso a internet, interpretando la información de archivos y sitios web para que éstos puedan ser leídos.
Byte	Unidad fundamental de datos en los ordenadores personales, un byte son ocho bits contiguos.
Cifrado	Procedimiento que utiliza un algoritmo de cifrado con cierta clave (clave de cifrado) transforma un mensaje, sin atender la estructura lingüística o significado, de tal forma que sea incomprensible o, al menos, difícil de comprender a toda persona que no tenga la clave secreta (clave de descifrado) del algoritmo.
Datagrama	Fragmento de un paquete que es enviado con la suficiente información como para que la red pueda simplemente encaminar el fragmento hacia el Equipo Terminal de Datos (ETD) receptor, de manera independiente a los fragmentos restantes.

Firewall	Software o hardware que comprueba la información procedente de internet o de una red y, a continuación, bloquea o permite el paso de esta al equipo, en función de la configuración del *firewall*.
Frame Relay	Tecnología de conmutación rápida de tramas, basada en estándares internacionales, que puede utilizarse como un protocolo de transporte y como un protocolo de acceso en redes públicas o privadas proporcionando servicios de comunicaciones.
Gateway	Es un dispositivo que permite interconectar redes con protocolos y arquitecturas diferentes a todos los niveles de comunicación. El propósito es traducir la información del protocolo utilizado en una red inicial al protocolo usado en la red de destino.
Hacker	Esto concierne principalmente a entradas remotas no autorizadas por medio de redes de comunicación como internet por personas no ajenas al sistema.
Host	Se refiere a las computadoras conectadas a una red, que proveen y utilizan servicios de ella.
ISP	Internet Service Provider es una empresa que brinda conexión a internet a los clientes.

IPSec	Por las siglas en inglés Internet Protocol Security es un conjunto de protocolos cuya función es asegurar las comunicaciones sobre el Protocolo de Internet (IP) autenticando y/o cifrando cada paquete IP en un flujo de datos.
Modelo OSI	Modelo que define los métodos y protocolos para lograr una comunicación entre los equipos de una red. Este método define el funcionamiento de la redes en 7 capas.
Protocolo	Designa el conjunto de reglas que rigen el intercambio de información a través de una red de ordenadores.
Protocolo datagrama	Protocolo que permite el envío de datagramas a través de la red sin que se haya establecido previamente una conexión, ya que el propio datagrama incorpora suficiente información de direccionamiento en la cabecera.
Protocolo de control	Conjunto de protocolos estándar de la industria que está diseñado para redes de gran tamaño compuestas por segmentos de red conectados mediante enrutadores. TCP/IP es el principal conjunto de protocolos usado en internet.

Protocolo punto	Protocolo que opera en la capa 2 del modelo OSI proporciona conexiones entre dos equipos, estas pueden ser de *router* a *router*, de *host* a red.
Red privada	Es aquella red exclusiva de una sola compañía u organización ya que la información no se comparte con otras compañías.
Red pública	Es una red por la cual circula información de muchas compañías y organizaciones en consecuencia es una red poco segura pero resulta más económico. La internet es una red pública.
Router	Dispositivo que proporciona conectividad a nivel de red o nivel tres en el modelo OSI. La función principal consiste en enviar o encaminar paquetes de datos de una red a otra.
Red privada virtual (VPN)	Tecnología de red que permite una extensión segura de la red local (LAN) sobre una red pública o no controlada como internet. Permite que la computadora en la red envíe y reciba datos sobre redes compartidas o públicas.
Spoofing	Procedimiento que cambia la fuente de origen de un conjunto de datos en una red, por ejemplo, adoptando otra identidad de remitente con el fin de engañar a un servidor *firewall*.

Tunneling	Método que se utiliza para encapsular paquetes dentro de otros paquetes los cuales son enviados a través de la red. Algunos de los protocolos utilizados son PPTP y L2TP.

RESUMEN

En el presente trabajo de graduación se tratará una serie de temas y conceptos con el objetivo de ayudar a todo administrador de redes a comprender los protocolos y algoritmos de encriptamiento que se ven involucrados al momento de implementar un enlace VPN IPSec.

El capítulo 1 es una introducción a las redes privadas virtuales o Virtual Private Network (VPN) en las siglas en inglés, los beneficios que se obtienen al implementar una VPN y lo que se debe de considerar al implementar una VPN. En el capítulo dos se hablará de los protocolos de operación en una red privada virtual, de los modos de operación y el concepto de túnel, algo muy importante en la seguridad de cualquier enlace. El capítulo tres está dedicado a los protocolos que operan en la capa de enlace de datos del modelo OSI, como por ejemplo protocolo PPP, PPTP y el modo en el que establecen una conexión. El capítulo cuatro está dedicado a los protocolos de capa 3, uno de los más importantes es el protocolo IPSec sobre el cual está basado este trabajo ya que es uno de los protocolos más seguros cuando se quiere establecer un enlace VPN. En el capítulo 5 se trata el tema del corta fuego o *firewall* ya que también es un tema importante, si se desea tener más control del tráfico saliente y entrante además del control de los usuarios dentro de la red. Por último, en el capítulo 6, se realiza una implementación de un enlace VPN IPSec utilizando equipos de la familia cisco, también explica paso a paso los comandos implementados.

OBJETIVOS

General

Implementar un enlace de red privada virtual utilizando el protocolo de seguridad IPSec.

Específicos

1. Estudiar los fundamentos de las redes privadas virtuales.

2. Comprender los protocolos de operación en una red privada virtual.

3. Identificar los protocolos que operan en la capa de enlace de datos.

4. Determinar los protocolos que operan en la capa de red.

5. Entender el rol del *firewall* en un enlace VPN.

6. Realizar un enlace VPN IPSec.

INTRODUCCIÓN

Hoy en día existen muchas formas para que las compañías puedan comunicarse entre sí y compartir información confidencial sin importar la distancia a la que se encuentren. Una de las formas más seguras y fáciles de realizar esto es implementando los llamados enlaces VPN IPSec. Para comprender el funcionamiento de este tipo enlaces es necesario hacer un recorrido desde lo más básico, que sería conocer la diferencia entre una red local y una red privada virtual hasta lo más avanzado que son los protocolos y algoritmos de encriptamiento en un enlace VPN.

Cabe mencionar que no solo los protocolos y algoritmos se ven involucrados en un enlace VPN, ya que parte importante de la seguridad de un enlace son los equipos que se utilizan, desde luego hay equipos que son mucho más robustos que otros pero esto no significa que sean los mejores, al contrario se puede incurrir en un gasto innecesario para la empresa, es por eso que los administradores de red deben conocer la estructura de red de la empresa, y los planes de crecimiento de la misma, con esto en mente se puede invertir en equipos de acuerdo a la necesidad de la red. Algunas de las características que se toman en cuenta en un equipo son los protocolos que soporta, la memoria que utiliza, la versión de software, etc.

En este trabajo se analizarán los protocolos para configurar un enlace VPN IPSec y las características de los algoritmos de encriptamiento que se pueden implementar en un enlace de este tipo. Por último, se realizará una aplicación para interconectar dos equipos de forma segura, creando un enlace VPN IPSec.

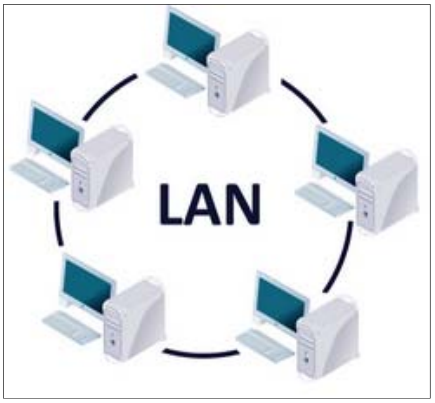
1. REDES PRIVADAS VIRTUALES

1.1. ¿Qué es una red?

Una red informática está formada por un conjunto de ordenadores intercomunicados entre sí que utilizan distintas tecnologías de hardware/software. Las tecnologías que utilizan (tipos de cables, de tarjetas, dispositivo etc.) y los programas (protocolos) varían según la dimensión y función de la propia red. Puede formarse con solo dos computadores aunque también por un número casi infinito; también se da el caso donde múltiples redes están interconectadas entre sí, de hecho así es como está construido lo que se conoce como internet.

Una red, no está formada únicamente solo por computadoras, existen equipos conectados al conjunto que cumplen ciertas funciones en el sistema, por ejemplo: servidores, *hubs*, *switches*, *routers*, concentradores, *firewalls*, *gateways*, etc. Los cuales se adaptan según las necesidades, tamaño y topología de la red, es decir una red de PCs de gran tamaño requerirá equipos que soporten las tareas y exigencias. Un modelo bastante sencillo se muestra en la siguiente figura:

Figura 1. **Estructura básica de una red**



Fuente: http://www.excellgroup.com/portfolio/data/lan.aspx. Consulta: 22 de diciembre de 2013.

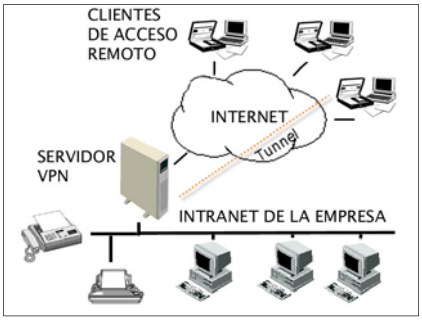
1.2. ¿Qué es una red privada virtual?

Debido a la evolución de la tecnología y que si no se utilizara una infraestructura pública la creación de accesos remotos y creación de redes de área amplia privadas resultarían ser costosos, por ello se buscaron maneras de poder establecer una red privada dentro de una red pública. Como resultado surgieron las Redes Privadas Virtuales (VPN) las cuales han ofrecido muchas ventajas a las corporaciones, siendo la más importante la reducción de costos en la instalación y el mantenimiento de estos enlaces.

Se puede definir a una VPN de la siguiente manera: “Una Red Privada Virtual (VPN, Virtual Private Network) es una tecnología de red que permite una extensión segura de la red local (LAN) sobre una red pública o no controlada como internet”. [1]

[1] http://es.wikipedia.org/wiki/Red_privada_virtual.

Figura 2. **Estructura básica de una red privada virtual**



Fuente: http://html.rincondelvago.com/red-privada-virtual.html.
Consulta: 27 de diciembre de 2013.

En la mayoría de los casos se utiliza la infraestructura de internet para crear VPNs y debido a que es un medio inseguro, es necesario que la seguridad en una VPN sea de suma importancia, dado que la información que circula en un medio público puede ser interceptada por cualquier persona sino se toma las debidas precauciones. Es por eso que una VPN debe de llevar implícitamente mecanismos de seguridad, autenticación y de encriptación de la información, para que esta viaje de forma segura.

1.3. Beneficios que se obtiene al momento de implementar una VPN

- Reducir de costos: para quienes ya utilizan alguna tecnología tradicional de red privada, la implementación de una VPN reduce el costo significativamente, solo por el cambio de tecnología. Por ejemplo cuando se quiera implementar una red que involucre empresas alejadas geográficamente ya no habrá necesidad en términos de seguridad de los enlaces mediante líneas dedicadas (punto a punto) de muy alto costo que caracterizaron a muchas empresas privadas.

- Mecanismos de seguridad: para los casos en que se tenga una comunicación insegura entre dispositivos, con la implementación de una red virtual entre ellos, se puede hacer que los datos viajen seguros. Las VPN requieren estándares altos de seguridad, para la transmisión de la información. Los protocolos como 3DS (Triple Data Encryption Standard) que tienen la tarea de encriptar la información a transmitir y el protocolo IPSec (IP Security) para manejo de los túneles mediante software, brindan un alto nivel de seguridad al sistema.

- Escalable: permite que se agreguen más dispositivos de red o usuarios según sea la necesidad. Si no se considera la escalabilidad de un sistema de VPN puede ser un error costoso si las necesidades de la empresa cambian y la estructura de la red actual no permita nuevas configuraciones. Si se desea agregar más usuarios a la VPN, no es necesario realizar gastos adicionales ya que los equipos se pueden configurar para cierto número de enlaces.

1.4. Clasificación de una VPN

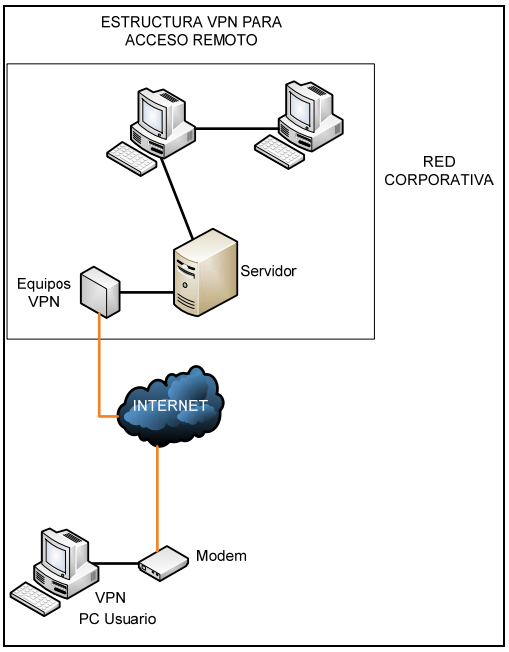
Las empresas pueden usar una red VPN para conectar de manera segura oficinas y usuarios remotos por medio de un acceso a internet suministrado por el proveedor de servicios local, en lugar de enlaces de red de área amplia (WAN) dedicados o enlaces de acceso telefónico de larga distancia. Existen diferentes razones por la cual es necesaria la creación de una VPN, como por ejemplo el crecimiento de la organización, cuando un empleado se desplaza hacia un punto remoto y necesita tener información en tiempo real, o los mismos clientes de la compañía necesitan acceder a la base de datos de la empresa etc.

Las VPNs se pueden crear dependiendo del tipo de requerimiento es por eso que se pueden clasificar en:

1.4.1. VPN de acceso remoto

Este es el modelo más usado y consiste en usuarios o proveedores que se conectan con la empresa desde sitios remotos utilizando internet como el medio para establecer la conexión. Una vez autenticados tienen un nivel de acceso y seguridad como si estuviera directamente en la red local.

Figura 3. **Acceso remoto de un usuario final a una VPN**



Fuente: elaboración propia, con programa de Visio.

Esta clase de enlace VPN se establece cuando un colaborador de la compañía se encuentra realizando un trabajo de forma remota o algún cliente de la empresa necesita obtener datos en forma remota para futuras transacciones. Luego de la previa configuración de una VPN en el equipo remoto que va hacer conectado a la red se debe adquirir un servicio de internet al ISP local. Y utilizando la infraestructura de internet se crea un túnel de comunicación entre el equipo remoto y el servidor de la organización, lo que brindaría seguridad a la información transmitida. La seguridad sería equivalente a la brindada en una red privada.

Una de las grandes ventajas es que se reducen de manera considerable los costos de conexión debido a que no es necesario establecer comunicación mediante una llamada de larga distancia a un servidor de acceso de red, ya que esto implicaría un gasto mucho más elevado, que es lo que se hacía unos años atrás.

1.4.2. VPN de cliente a servidor

Si surgiera el escenario en el que un usuario que forma parte de una red de área local, que está dentro de un edificio, quiera comunicarse confidencialmente con un departamento específico de la red y que además tenga la confianza de que la información no será interceptada por nadie más. Será necesario crear un túnel con encriptación para que sea garantizada la seguridad y confidencialidad de los datos.

Dentro de los problemas que pueden surgir si no se toman las medidas de seguridad son:

- Todo usuario conectado a la red tendrá acceso a cualquier tipo de servicio.

- La información quedaría disponible para que cualquier persona, fuera o dentro de la red pueda verla, utilizando técnicas como sniffing.

- Se podría falsificar la identificación de usuarios válidos, con información obtenida directamente del medio de transmisión.

Una de las soluciones para este tipo de problemas es la implementación de un servidor VPN dentro de la red, este tendrá la tarea de asegurar los datos y que todo usuario que se encuentre físicamente dentro de la misma red, y que necesite comunicarse con otros usuario de la red, soliciten autorización al servidor VPN para establecer la conexión, es decir el servidor será la puerta de enlace entre los usuarios creando túneles entre ambos equipos, con esto se logrará una comunicación privada entre ambas partes sin que terceros puedan interceptar la información.

Las ventajas que se puede tener al implementar un sistema VPN dentro de una LAN son:

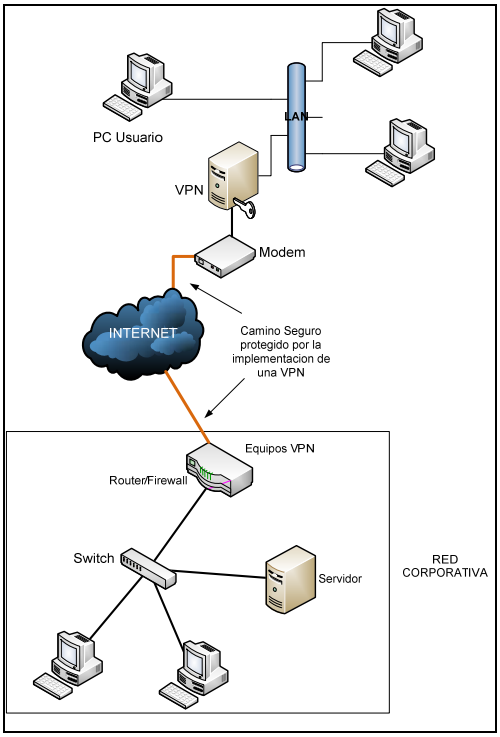
- Transparente a las aplicaciones, es decir: una vez se configura las rutas en los equipos, todo el tráfico será encriptado y se validará sin necesidad de alguna reconfiguración.

- Alta seguridad: al encriptar los datos y las direcciones destino se evita que personas no autorizadas tengan acceso a la información.

- Distintos niveles de seguridad: dependiendo de la necesidad se puede trabajar con claves ya establecidas en los extremos y si se desea más seguridad se pueden implementar certificados digitales.

En la siguiente figura se observa en forma general los niveles de seguridad que se pueden implementar un enlace VPN dentro de una compañía:

Figura 4. **Acceso privado de un cliente o usuario dentro de una red corporativa**



Fuente: elaboración propia, con programa de Visio.

1.4.3. VPN de servidor a servidor

Este sería el escenario en donde dos oficinas de una misma organización y que ambas están remotamente separadas, necesitan comunicarse mediante una red pública, pero si estas oficinas o sucursales no cuentan con las medidas de seguridad para reguardar los datos que viajan por la red, están expuestos a que terceros intercepten la información y la usen para perjudicar a la organización.

Si se realizará una conexión mediante la red pública y sin tomar en cuenta la seguridad se presentarían los siguientes riesgos.

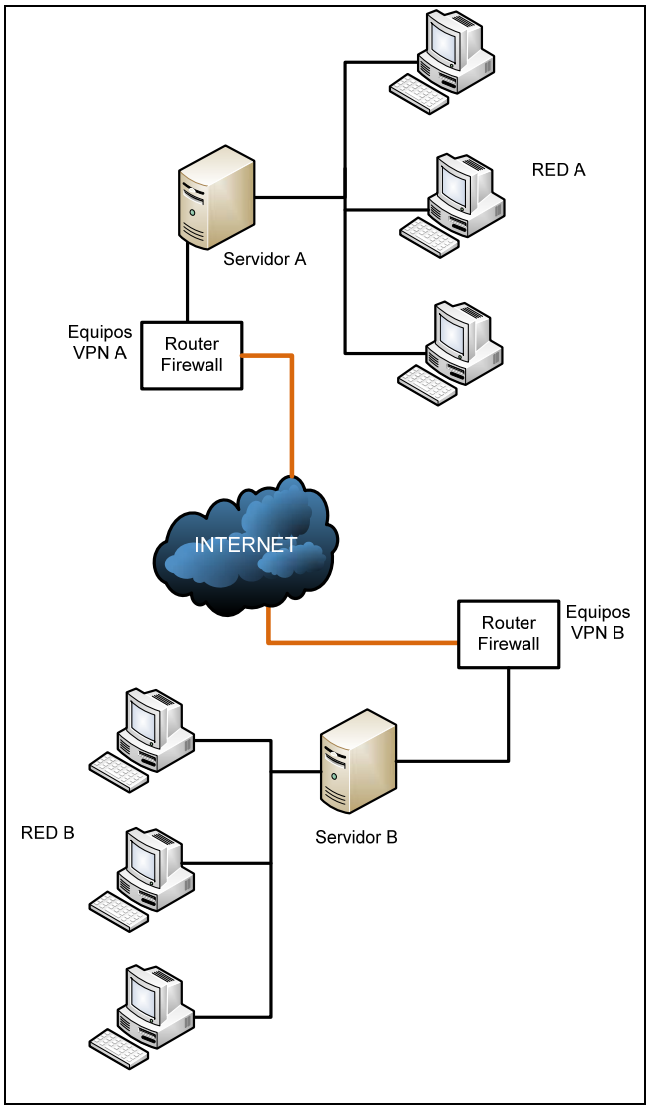
- Cualquier persona dentro de la red pública podrá acceder a la información enviada por la compañía y a si tener libre acceso a cualquier servicio.

- Lograr obtener información de los accesos de usuarios válidos y poder acceder a los datos de autenticación.

Para solucionar el problema de seguridad en ambas oficinas se pueden agregar equipos que protejan el tráfico entrante y saliente, esto se puede hacer para que el servidor VPN pueda administrar los *router* y *firewalls* que son los que hacen posible la creación y disposición de túneles de tal manera que la información sea encriptada antes de la transmisión.

El diagrama muestra una posible solución VPN para dos servidores que administran redes corporativas es el siguiente:

Figura 5. **VPN entre dos redes red A y red B**



Fuente: elaboración propia, con programa de Visio.

Se puede observar que en la salida de los equipos VPN que en este caso podría ser un *router* con un *firewall* incorporado, contienen protocolos de encriptación que otorgan seguridad a la información transmitida por la internet. El *firewall* es el encargado de cerrar el paso de cualquier acceso no autorizado, en este punto no hay ningún peligro porque la información ya pasó por el *firewall*.

Las ventajas que se encuentran al momento de que se implementa un enlace VPN entre dos redes corporativas son las siguientes:

- Alta seguridad: la encriptación es a nivel general es decir se encriptan los datos como las direcciones destino, evitando que cualquier intruso capture o lea la información que está siendo transmitida.

- Diferentes niveles de seguridad: dependiendo de la situación se puede trabajar con claves ya configuradas en los equipos o con certificados de llaves para que haya autenticación en los extremos.

1.5. Tipos de VPN

Existen diferentes formas en las que se pueden implementar las VPN. Cada proveedor de servicios puede ofrecer diferentes soluciones VPN. Sin embargo, las empresas deciden la que mejor se adapte a la necesidad. Los diferentes tipos de VPN son:

- VPN de *firewall*
- VPN de *router* y de concentrador
- VPN por aplicación
- VPN por proveedor de servicios

1.5.1. VPN de *firewall*

También llamado cortafuegos es un dispositivo de hardware o un software que permite filtrar todo tráfico de entrada o salida que hay en una red. Sí el tráfico que entra o sale cumple con una serie de reglas que se pueden especificar, entonces el tráfico podrá acceder o salir de la red u ordenador sin ninguna restricción de lo contrario el trafico será bloqueado. Por lo tanto si un *firewall* cumple con todos los requisitos de configuración se puede evitar que personas no deseadas ingresen a la red además de bloquear el tráfico.

Hoy en día los equipos *firewall* vienen con opciones para configurar VPNs. Empresas como Alcatel, Huawei, Cisco, tienen una gran variedad de dispositivos *firewall* con integración VPN. En este tipo de VPN la administración es más centralizada ya que tanto el *firewall* como la VPN se configuran en un solo dispositivo. Pero también la configuración se vuelve más compleja además de que si el equipo no tiene buen desempeño ejecutando los enlaces VPN y el *firewall* el equipo tendrá bajo rendimiento.

1.5.2. VPN de *router* y de concentrador

La llegada de las aplicaciones web y un enorme aumento del número de comunicaciones está llevando a la necesidad de contar con infraestructuras de seguridad de gran capacidad es por eso que muchas empresas como Cisco, Nortel, Alcatel han sacado al mercado dispositivos llamados concentradores VPN. Estos ofrecen la creación de enlaces VPN integrados dentro de un *router*, poseen las tecnología VPN más importantes y los métodos de cifrado y autenticación para proteger la información.

Estos equipos están diseñados para la creación de enlaces VPN por lo que serían una solución más rápida. Si en la implementación se tiene la necesidad de incrementar el rendimiento únicamente se deben agregar tarjetas al equipo. Estos equipos también cuentan con certificaciones de seguridad.

1.5.3. VPN de *router* por sistema operativo

Los sistemas operativos como Microsoft Windows, NetWare de Novell o Linux en las diferentes distribuciones (Red Hat, Debian,..) ofrecen servicios de VPN ya integrados dentro del mismo sistema operativo. Una de las principales ventajas es que resulta ser bastante económico, dado que en un paquete completo vienen servicios de acceso remoto, servidor web y además mejora los métodos de autenticación y la seguridad del sistema operativo. Estas VPN se utilizan más para acceso remoto.

1.5.4. VPN por aplicación

Este es un software que permite la creación de VPNs en un sistema operativo, como por ejemplo Cisco VPN, la ventaja de estas aplicaciones es que agrega más seguridad al enlace y la desventaja es que no soportan una gran cantidad de usuarios y son más lentas que una VPN basada en hardware. Son vulnerables a las fallas que tenga el sistema operativo.

1.5.5. VPN por proveedor de servicios

Este tipo de VPN son servicios ofrecidos regularmente por el proveedor de servicios de internet. Estos pueden estar basados en tecnología ATM, Frame Relay y actualmente sobre redes completamente IP. En este caso el proveedor

de servicios es el dueño de toda la infraestructura como tal, es decir, de los equipos, de las líneas de transmisión etc.

Dependiendo del ancho de banda contratado por el cliente, así será el rendimiento del enlace VPN, pero de este dependerá el monto que la organización tendrá que pagar mensualmente por la conexión.

1.6. Consideraciones al implementar una Red Privada Virtual (VPN)

Típicamente, al implementar una solución de red remota, una compañía desea facilitar un acceso controlado a los recursos y a la información de la compañía. La solución deberá permitir la libertad para que los clientes *roaming* o remotos autorizados se conecten fácilmente a los recursos corporativos de la red de área local (LAN), y la solución también deberá permitir que las oficinas remotas se conecten entre sí para compartir recursos e información (conexiones de LAN a LAN). Finalmente, la solución debe garantizar la privacidad y la integridad de los datos al viajar a través de internet. Las mismas cuestiones aplican en el caso de datos sensibles que viajan a través de una red corporativa. Por lo tanto, como mínimo, una solución de VPN debe proporcionar todo lo siguiente:

- Autenticación de usuario: se debe autenticar a todo usuario de la red y limitar el acceso de la VPN solo a usuarios autorizados. Además, deberá llevar una estadística y registros de quien o quienes accedieron a cierta información y cuando lo hicieron.

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

- Encriptación de datos: la intención es que los datos que viajan en una red pública no puedan ser leídos por clientes o personas no autorizados.

- Administración de llaves: la solución deberá generar y renovar las llaves de encriptación para el cliente y para el servidor.

- Soporte de protocolo múltiple: la solución deberá manejar protocolos comunes utilizados en las redes públicas; estos incluyen protocolo de internet. Una solución de VPN de internet basada en un Protocolo de Túnel de Punto a Punto (PPTP).

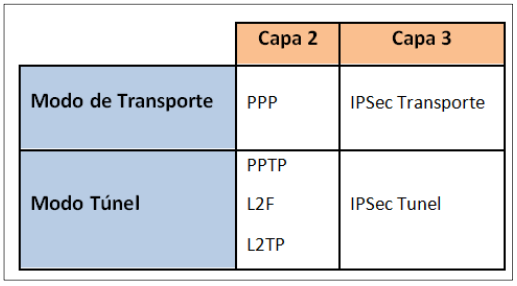
`

2. PROTOCOLOS DE OPERACIÓN EN UNA VPN

Para que una red privada virtual funcione de la manera correcta, se han implementado una serie de protocolos y normas de conectividad orientadas tanto a los equipos terminales como al software del enlace. De esta manera se verá, en los capítulos siguientes, los protocolos fundamentales que involucran un enlace VPN, iniciando desde el protocolo más básico hasta llegar a una configuración más avanzada.

Al momento de determinar el nivel de seguridad de los medios de comunicación VPN se deberá consultar la siguiente clasificación:

Figura 6. **Modos en los que trabajan los protocolo VPN**



	Capa 2	Capa 3
Modo de Transporte	PPP	IPSec Transporte
Modo Túnel	PPTP L2F L2TP	IPSec Tunel

Fuente: elaboración propia, con programa de Visio.

2.1. Modo trasporte en una VPN

Con este método se puede crear una conexión entre dos puntos mediante una red pública, luego se puede crear un túnel para que la información sea más segura, confiable y que se establezcan parámetros de autenticación.

2.2. Modo túnel en una VPN

Lo importante de este método es que mediante la encapsulación y encriptación de las tramas se pueden crear túneles y luego se simularía un enlace punto a punto seguro, sobre la red pública que se está utilizando.

2.3. Concepto de túnel

Cuando se habla de túnel se refiere al método de transformar de forma segura las tramas que serán enviadas en el medio de transmisión de tal manera que no puedan ser interceptadas durante el recorrido. El túnel es una conexión virtual punto a punto sobre el trayecto de la red, esto permite que los usuarios puedan enviar y recibir información sin ningún riesgo. Estas tramas viajarán con encabezados que permitirán que el destino final pueda reconocer que la información va dirigida a él y luego pueda procesarla.

2.3.1. Funcionamiento del *tunneling*

Existen paquetes que no pueden ser transportados en una red basada completamente en IP como por ejemplo paquetes IPX o AppleTalk dado la estructura de la trama. Sin embargo, si este paquete es encapsulado dentro de un paquete IP, entonces podrá ser transportado como cualquier otro paquete

IP. Lo que hace este proceso es simplemente agregarles un encabezado adicional.

Luego, de agregar el encabezado y de encapsularlo, el paquete se envía a través de una ruta lógica denominada túnel que sería el canal directo entre dos extremos. El túnel es la ruta de información lógica a través de la cual viajan los paquetes encapsulados. Tanto para el origen y destino, el túnel es totalmente transparente, ellos únicamente ven una conexión punto a punto. A estos puntos que están en cada extremo del túnel se les denomina interfaces de túnel. Los interlocutores o los *host* desconocen los *routers*, *switches*, servidores *proxy* u otras puertas de enlace de seguridad que pueda haber entre los extremos del túnel.

Cuando el paquete llega al destino, este es desencapsulado para que pueda ser utilizado. En resumen, el *tunneling* es un proceso que consta de los siguientes pasos:

- Encapsulación
- Transmisión
- Desencapsulación

El uso de un túnel abarca todo el proceso de encapsulación, enrutamiento y desencapsulación. El túnel envuelve, o encapsula, el paquete original dentro de un paquete nuevo. Este paquete nuevo puede contener nueva información de direccionamiento y enrutamiento, lo que le permite viajar por la red. Si el túnel se combina con la confidencialidad de datos, los datos del paquete original (así como el origen y el destino originales) no se muestran a quienes observen el tráfico en la red. Cuando los paquetes encapsulados llegan al destino, se

quita la encapsulación y se utiliza el encabezado original del paquete para enrutar este al destino final.

2.3.2. Protocolo pasajero, encapsulador y portador

El proceso *tunneling* involucra tres protocolos diferentes:

- Protocolo pasajero: representa el protocolo que debe encapsularse. Como ejemplos de protocolos pasajeros tenemos PPP y SLIP.

- Protocolo de encapsulamiento: es el que será empleado para la creación, mantenimiento y destrucción del túnel. Ejemplos de protocolo de encapsulamiento son L2F, L2TP, PPTP.

- Protocolo portador: es el encargado de realizar el transporte del protocolo de encapsulamiento. El principal ejemplo de protocolo portador es IP puesto que este tiene amplias capacidades de direccionamiento y es en el que está basado internet.

Figura 7. **Estructura de paquete *tunneling***

Fuente: elaboración propia, con programa de Visio.

2.4. *Tunneling* y VPN

Cuando el uso de túneles se combina con el cifrado de los datos, puede utilizarse para proporcionar servicio de VPN. Las VPN utilizan el *tunneling* para poder ofrecer mecanismos seguros de transporte de datos. Dentro del contexto de las VPN, el *tunneling* involucra tres tareas principales:

- Encapsulación
- Protección de direcciones privadas
- Integridad de los datos y confidencialidad de estos

Para que el proceso de *tunneling* pueda ser llevado a cabo, existen diversos protocolos llamados protocolos de túnel los cuales se encargan de encapsular y desencapsular los datos que viajan dentro de una red privada virtual. Los protocolos de túnel usados por las VPN como PPTP y L2TP son usados para encapsular tramas de la capa de enlace de datos (PPP). Protocolos de túnel como IP sobre IP e IPSec en modo túnel son utilizados para encapsular paquetes de la capa de red.

Es posible colocar un paquete que utiliza una dirección IP privada dentro de un paquete que usa una dirección IP global única para poder extender una red privada sobre una red pública como internet. Puesto que los contenidos del paquete entunelado solo pueden ser interpretados por las interfaces de túnel, las direcciones IP privadas pueden ser ocultadas completamente de las redes IP públicas.

Los mecanismos de integridad y confidencialidad garantizan que ningún usuario no autorizado pueda alterar los paquetes entunelados durante la transmisión sin que el ataque pueda ser detectado y que los contenidos del

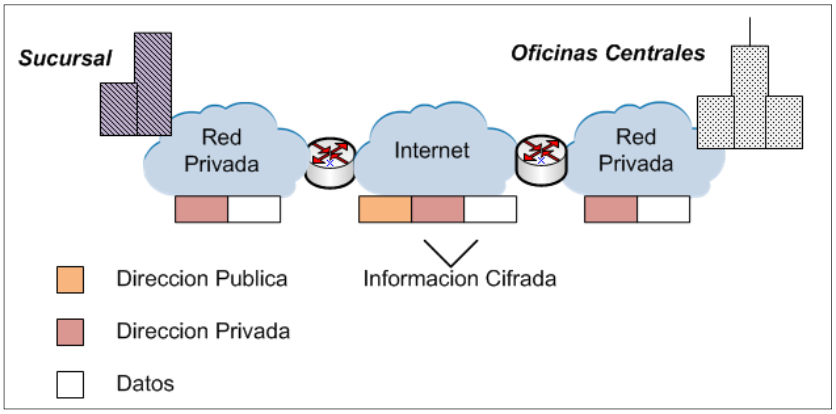
paquete permanecen protegidos de acceso no autorizado. Además, el *tunneling* opcionalmente puede proteger la integridad de la cabecera del paquete IP externo, mediante técnicas de autenticación. Por ejemplo, si se utiliza IPSec los protocolos AH y ESP pueden proporcionar autenticación de los paquetes transmitidos.

Tres protocolos de túnel son los más usados para la creación de una VPN:

- Protocolo de túnel punto a punto (PPTP)
- Protocolo de túnel de capa 2 (L2TP)
- Protocolo de seguridad IP

Los protocolos PPTP y L2TP se enfocan principalmente a las VPN de acceso remoto, mientras que IPSec se enfoca mayormente en las soluciones VPN de sitio a sitio.

Figura 8. **Estructura del proceso *tunneling* en una VPN**



Fuente: GONZALES MORALES, Alexandro. *Redes Privadas Virtuales*. p. 68.

Tipos de túneles: los túneles se clasifican de acuerdo a como se establece la conexión entre dos *hosts*. Con base en esto, existen dos tipos de túneles estos son:

- Túnel voluntario
- Túnel obligatorio

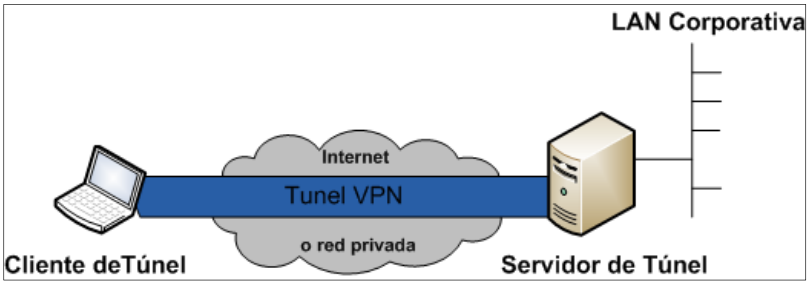
2.4.1. Túnel voluntario

Un equipo, usuario o cliente puede emitir una petición VPN para configurar y crear un túnel voluntario. En este caso, el equipo del usuario es un extremo del túnel que funciona como cliente de túnel. El túnel voluntario se produce cuando una estación de trabajo o un *router* utilizan software de cliente de túnel para crear una conexión VPN con el servidor de túnel de destino. Para ello, debe instalar el protocolo de túnel correspondiente en el equipo cliente. Un túnel voluntario puede ser creado de dos maneras a través de una conexión *dial-up* o a través de una LAN. La figura 9 muestra un túnel voluntario.

A través de una conexión *dial-up*: en este caso, el usuario primero hace una llamada al ISP para conectarse a internet y entonces posteriormente podrá ser creado el túnel. Esta suele ser la situación más común. La conexión a internet es un paso preliminar para crear el túnel, pero no forma parte del proceso de creación del túnel.

A través de una LAN: en este caso, el cliente ya posee una conexión a la red, por lo que el túnel puede ser creado con cualquier servidor túnel deseado. Este es el caso de un usuario de una LAN que crea un túnel para acceder a otra LAN.

Figura 9. **Túnel voluntario**



Fuente: elaboración propia, con programa de Visio.

2.4.2. Túnel obligatorio

Es la creación de un túnel seguro por parte de otro equipo o dispositivo de red en nombre del equipo cliente. Los túneles obligatorios se configuran y crean automáticamente para los usuarios sin que estos intervengan ni tengan conocimiento de los mismos. Con un túnel obligatorio, el equipo del usuario no es un extremo del túnel. Lo es otro dispositivo entre el equipo del usuario y el servidor de túnel que actúa como cliente de túnel.

Algunos proveedores que venden servicios de acceso telefónico facilitan la creación de un túnel en nombre de un cliente de acceso telefónico. El dispositivo que proporciona el túnel para el equipo cliente se conoce como procesador cliente (FEP) o PAC en PPTP, concentrador de acceso (LAC) de L2TP en L2TP o puerta de enlace (Gateway) de seguridad IP en IPSec. Para realizar la función, el dispositivo que proporciona el túnel debe tener instalado el protocolo de túnel adecuado y debe ser capaz de establecer el túnel cuando el equipo cliente intenta establecer una conexión.

Esta configuración se conoce como túnel obligatorio debido a que el cliente está obligado a utilizarlo, pues es creado por el dispositivo que proporciona el túnel. Una vez que 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 se conecta en el NAS, se crea un túnel y todo el tráfico se enruta automáticamente a través de este. Se puede configurar el dispositivo que proporciona el túnel para hacer uno único a todos los clientes hacia un servidor específico del mismo. De manera alterna, el dispositivo que proporciona el túnel podría hacer túneles individuales de los clientes basados en el nombre o destino del usuario.

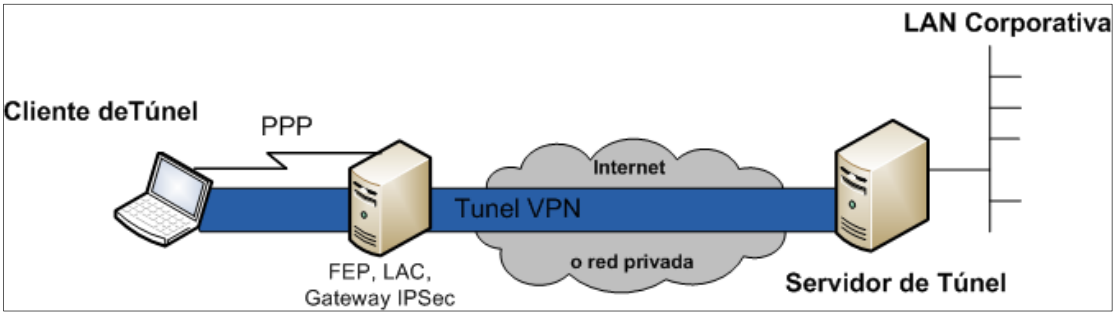
A diferencia de los túneles por separado, creados para cada cliente voluntario, un túnel entre el dispositivo que proporciona el túnel y el servidor del túnel puede estar compartido entre varios clientes. Cuando un segundo cliente se conecta al dispositivo que proporciona el túnel para alcanzar un destino para el cual ya existe un túnel, no hay necesidad de crear una nueva instancia del túnel entre el dispositivo que proporciona el túnel y el servidor del túnel. El tráfico de datos para el nuevo cliente se transporta sobre el túnel existente. Ya que puede haber varios clientes en un único túnel, el túnel no se termina hasta que se desconecta el último usuario túnel.

Una compañía puede contratar a un ISP para que implemente un conjunto de dispositivos que proporcionen túneles por todos los territorios donde existan LAN de la compañía. Estos dispositivos pueden establecer túneles a través de internet hasta un servidor VPN conectado a la red privada de la organización, consolidando así las llamadas de zonas geográficamente dispersas en una sola conexión a internet en la red de la organización.

Una compañía puede contratar a un ISP para que implemente un conjunto de dispositivos que proporcionen túneles por todos los territorios de la compañía donde existan LAN. Estos dispositivos pueden establecer túneles a través de internet hasta un servidor VPN conectado a la red privada de la organización, consolidando así las llamadas de zonas geográficamente dispersas en una sola conexión a internet en la red de la organización.

Existen dos formas de crear túneles obligatorios. En la primera forma, el túnel se crea antes de autenticar al cliente de acceso. Una vez creado el túnel, el cliente de acceso se autentica en el servidor de túnel. En la segunda forma, el túnel se crea después de que el dispositivo que proporciona el túnel autentica al cliente de acceso. La figura 10 muestra cómo se compone un túnel obligatorio.

Figura 10. **Túnel obligatorio**

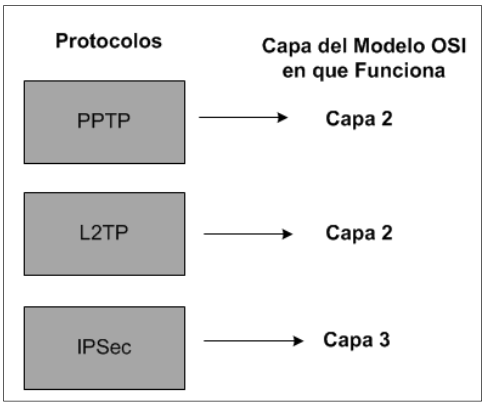


Fuente: elaboración propia, con programa de Visio.

2.5. Protocolo túnel

Los tres protocolos más importantes para crear un enlace de túnel en una red en los que se necesite fiabilidad, seguridad e integridad en la información, son los siguientes:

Figura 11. **Principales protocolos de túnel y capa en que actúa**



Fuente: elaboración propia, con programa de Visio.

3. PROTOCOLOS QUE OPERAN EN LA CAPA DE ENLACE DE DATOS

3.1. Protocolo PPP (Point-to-Point Protocol)

Es un protocolo de nivel de enlace que permite una conexión entre dos *host*. PPP cuenta con métodos de autenticación de conexión, cifrado de la información y compresión de los datos. Los estándares de PPP también admiten características avanzadas que no están disponibles en estándares más antiguos como SLIP (Serial Line Internet Protocol). En la mayor parte de las implementaciones PPP se puede automatizar todo el proceso de inicio de sesión. PPP también ha sido utilizado por los ISP para acceder a la internet ya que encapsula el paquete del mensaje original en uno transportable por el internet (paquete PPP).

3.2. Secuencia de conexión PPP

El protocolo PPP permite establecer una comunicación a nivel de la capa de enlace TCP/IP entre dos computadoras. Un enlace VPN se puede dar cuando el equipo del cliente necesita comunicarse con el servidor VPN de la empresa. Inicialmente se debe solicitar al proveedor de servicios de internet local, que establezca una comunicación mediante PPP, y luego crear un túnel VPN. A continuación las fases para una conexión PPP:

- 1era fase, establecimiento de conexión: durante esta fase se crean las reglas para el manejo y direccionamiento de tramas entre el equipo remoto y el servidor (origen y destino). El cual crea una comunicación continua es decir una transferencia de tramas, aquí se configura el Protocolo de Control de Enlace (LCP) que es quien crea la conexión física, la mantiene y la finaliza.

  Usando LCP se negocia el tipo de autenticación que se va a utilizar, el tamaño de los datagramas, números mágicos para usar durante la autenticación. Luego de establecer la conexión física inicial entre el cliente y el servidor se envía una serie de paquetes LCP para solicitar una la configuración de nivel de enlace de datos (capa 2).

- 2da fase, autenticación: una vez establecido el enlace es elegido el método de autenticación. El usuario remoto tiene que presentar una identificación al servidor de acceso remoto, acción que en caso de ser aceptada permite la conexión y comunicación con la red privada. En esta fase el usuario envía una identificación de usuario al servidor de acceso remoto, y este debe verificar la autenticidad del nombre y las contraseñas de acceso privada. Un buen sistema de autenticación proporciona la seguridad y acceso de clientes autorizados a la información en la red. El protocolo Point-to-Point ofrece métodos de autenticación como PAP, CHAP, MS-CHAP, pero se recomienda que los sistemas tengan métodos de autenticación más complejos es decir que cuenten con el propio servidor RADIUS o TACACS.

- 3ra fase, llamada a protocolos de nivel de red: una vez que el PPP finalizó las fases anteriores, cada protocolo de capa de red (como por ejemplo IP, IPX o AppleTalk) debe ser configurado separadamente por el protocolo de control de red (NCP) apropiado. Cada NCP debe ser abierto y cerrado de a uno por vez.

- 4ta fase, terminación 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.

Después del intercambio de paquetes de terminación, la implementación debe avisar a la capa física que desconecte la línea para forzar la terminación del enlace, particularmente en el caso de una falla de autenticación. El que envía una solicitud de terminación debe desconectarse después de recibir un reconocimiento de terminación, o después de que expire el *timer* correspondiente. El receptor de una solicitud de terminación debe esperar al par para desconectarse, y no lo debe hacer hasta que al menos haya pasado cierto tiempo de reiniciado después de enviar el reconocimiento de terminación. PPP procederá entonces con la fase de enlace muerto. Cualquier paquete recibido durante esta fase que no sea LCP debe ser descartado. La clausura del enlace por LCP es suficiente. No es necesario que cada NCP envíe paquetes de terminación. A la inversa, el hecho de que un NCP sea cerrado no es razón suficiente para causar la terminación del enlace PPP, aún si ese NCP era el único actualmente en el estado abierto.

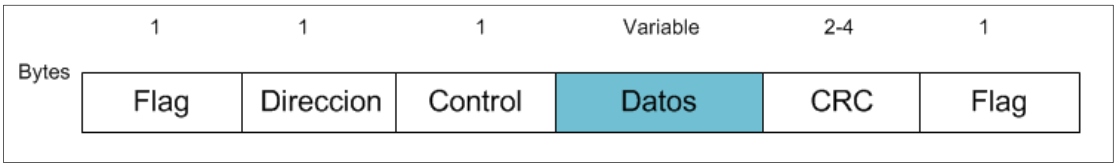
3.3. Transferencia de información

Después de que se establecen las fases antes de la transferencia de datos, los paquetes PPP se envían a través del enlace entre el servidor y el cliente, cuando las tramas llegan al destino son descifradas y procesadas por el receptor.

3.4. Encapsulamiento de paquete como PPP

Permite que diferentes protocolos de la capa de red operen sobre el mismo enlace. Ha sido diseñada cuidadosamente para mantener compatibilidad con el hardware mayormente usado. Los datos o la información que se desea enviar de un terminal a otro es un conjunto de números binarios, estos representan byte de datos, conformando cada bit físicamente como un 1 o un 0 lógico. A medida que estos paquetes van llegando al destino, uno a la vez y en el orden correcto, se va armando el paquete original.

Figura 12. **Paquete procesado como PPP**



Fuente: elaboración propia.

Siendo:

- Flag (bandera): indica el inicio y final de la trama, cuyo valor binario es preestablecido como 01111110 (7Eh).

- Dirección: 1 Byte, este campo no se utiliza y siempre vale 11111111 (FF h), representa la dirección de enlace de datos establecido para el protocolo TCP/IP.

- Control: este campo representa información de control del enlace. Para PPP se fija el valor 00000011 (03h) como indicador de enlace fiable.

- Datos: este campo contiene una IP privada y los datos a transmitir.

- CRC: este campo representa el resultado que se obtiene al aplicar un código redundante cíclico a la trama y se utiliza como un código de detección de errores en la misma. Normalmente es de 2 bytes, pero puede negociarse para medir 4 bytes.

3.5. Operación modo túnel

A continuación se presentan los principales protocolos que trabajan en la capa de enlace de datos del modelo OSI y operan en modo túnel VPN.

3.5.1. PPTP (Point-to-Point Tunneling Protocol)

PPTP es un protocolo de comunicaciones desarrollado por Microsoft, U.S. Robotics, Ascend Communications, 3 Com Corporation, ECI Telematics conocidas colectivamente como PPTP Forum, para implementar redes privadas virtuales entre usuarios de acceso remoto y servidores de red. Ya que es un protocolo de túnel, PPTP encapsula datagramas de cualquier protocolo de red en datagramas IP, que luego son tratados como cualquier otro paquete IP. Una de las ventajas de este tipo de encapsulamiento es que cualquier protocolo puede ser enrutado a través de una red IP, como lo es internet.

El protocolo PPTP permite el intercambio de datos de un cliente a un servidor formando una VPN, la ventaja de utilizar PPTP es el soporte de multiprotocolos de red como IP, IPX etc. Utilizando la infraestructura de internet como medio para realizar la conexión, pero proporcionando todos los parámetros de seguridad.

La idea principal del protocolo PPTP es dividir las funciones de acceso remoto de tal manera que las personas de las empresas puedan utilizar la infraestructura de internet para proveer una conectividad segura entre clientes remotos y redes privadas, es por ello que PPTP proporciona un mecanismo para tunelamineto de tráfico PPP sobre redes IP.

PPTP soporta múltiples protocolos de red, puede ser utilizado para crear VPNs sobre redes públicas o privadas además de aprovechar los mecanismos de autenticación, compresión y cifrado de las tramas.

3.5.2. Equipos involucrados en una conexión PPTP

En la práctica generalmente hay tres ordenadores involucrados:

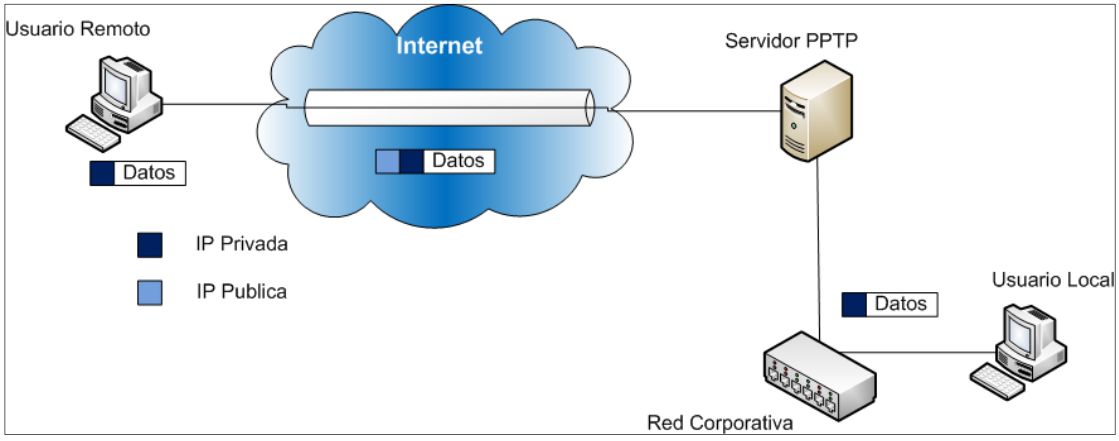
- Un cliente PPTP
- Un servidor de acceso a la red
- Un servidor PPTP (de la red privada)

Cuando un cliente autorizado y que está lejos de la oficina desea conectarse remotamente al servidor de la compañía o de la empresa, lo que inicialmente debe de hacer es conectarse al proveedor de servicios de internet mediante una conexión telefónica, con esto se estaría estableciendo un enlace Point to Point, luego se crea un túnel entre ambos extremos utilizando el

protocolo PPTP (Point to Point Tunneling Protocol) desde el cliente al servidor a través de internet.

En ese instante se crea una sesión de acceso remoto entre el servidor de datos de la compañía y el usuario remoto, logrando acceder a los recursos compartidos como archivos, impresoras, etc. con la seguridad que brinda la creación de un túnel en ambos extremos. La IP de la red privada y el *host* receptor están protegidos por el túnel que se ha creado, en el túnel viajan los datos y a estos se les agrega una cabecera IP privada y un cabecera IP pública, para el paquete pueda viajar a través de la internet y no se pierda en el camino, ya que cuando llega al receptor este desencapsula el paquete y verifica la IP privada constatando que efectivamente la información se dirige a la red local.

Figura 13. **Túnel entre un usuario remoto y una red corporativa a través de una red pública**



Fuente: elaboración propia, con programa de Visio.

3.5.3. Servidor PPTP

Se puede observar que el servidor PPTP es el punto final en cada red privada virtual y luego se interconecta a la red local y la función es la de filtrar la información de entrada y de salida, además controlar los usuarios que ingresan o intentan ingresar a la red. La función del servidor es procesar toda la información en paquetes PPTP antes de salir al medio público, con esto se asegura que la información no sea leída por intrusos, ya que las claves de cifrado son únicas y el único que podrá ver datos será el cliente autenticado y es quien podrá tener acceso a la información compartida en la red.

El servidor PPTP puede ser configurado para determinar que equipos externos pueden conectarse a la red local o qué punto dentro de la red podrá conectarse a internet.

Tipo de hardware requerido en los servidores:

Si se llegase a establecer que una máquina PC realice la función de servidor PPTP, se deberá instalar un sistema operativo que tenga excelente soporte a redes entre estos pueden estar Windows y cualquier distribución de Linux y el programa específico para configuración de puertos de acceso. La máquina deberá tener dos tarjetas de red (Nic, Modem, RDSI etc.), una conectada a la red local y la otra a internet.

Partes esenciales en un servidor PPTP:

- PNS Server: este se configura para correr sobre computadoras en tal caso plataformas de servidor de red como los ya mencionados.

- PAC (PPTP Access Concentrator): dispositivo que asocia una o más líneas capaces de soportar PPTP un ejemplo de este dispositivo sería el equipo Cisco CVPN3002-8E-K9, con este equipo se puede administrar sobre un mismo túnel varias sesiones multiplexadas. Una de las ventajas es que este concentrador reduce la necesidad de implementar equipos caros para permitir conexiones entre equipos.

3.5.4. Cliente PPTP

Si los equipos del proveedor servicios de internet soportan PPTP, no es necesario configurar software o hardware en el punto cliente, solo se necesita una conexión estándar PPP. Aunque esto no es recomendado ya que se genera un tramo inseguro desde el ISP local hasta el cliente remoto.

Si el proveedor de servicios de internet no soporta PPTP, el cliente puede instalar o utilizar un software PPTP y crear una conexión segura, primero utilizando el ISP local se debe establecer una conexión PPP para acceso a internet para luego lograr la conexión PPTP a través de un puerto PPTP del servidor de la empresa.

Tipo de hardware requerido en los clientes:

Además de que el cliente tiene que tener un sistema operativo que sea compatible con el servicio y el hardware a utilizar. Para que se establezca la conexión PPTP se requiere de un módem o tarjeta de red, además de un equipo de conexión a una red telefónica.

Por otro lado, si el cliente accede al servidor PPTP a través de una red de área local (LAN), se necesita de una tarjeta de red (NIC) que lo conecte físicamente.

3.5.5. Comunicación de túnel PPTP

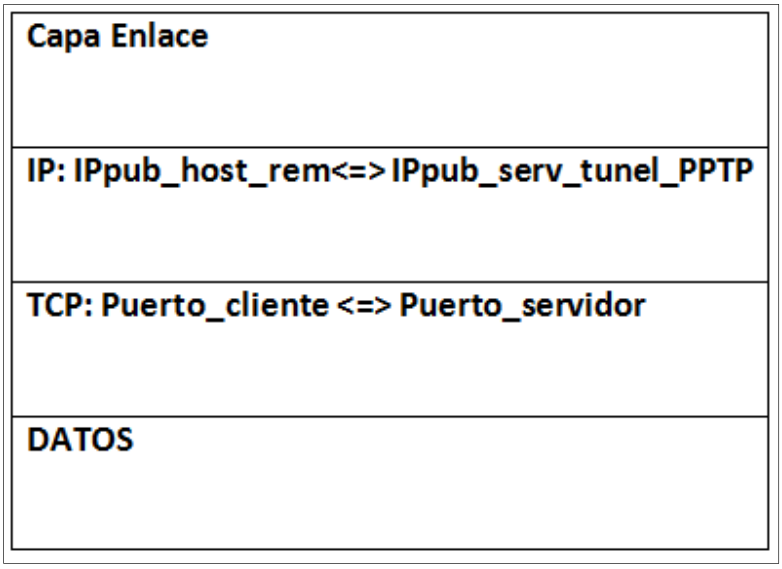
Si se desea acceder de forma remota a una red privada utilizando el modo PPTP se debe tomar en cuenta lo siguiente:

- La conexión entre la red privada, el equipo remoto y el servidor de túneles a través del protocolo TCP.

- Funcionamiento del túnel IP entre el equipo remoto y el servidor de túneles.

Control de la conexión, establece una conexión TCP entre el *host* remoto a través del puerto 1723 del servidor de túneles PPTP. Todas la sesiones que el usuario establezca estarán gestionadas por esta conexión TCP que son transportadas por el túnel PPTP. El formato de los paquetes en el control de la conexión será:

Figura 14. **Formato de la trama de control**



Fuente: elaboración propia.

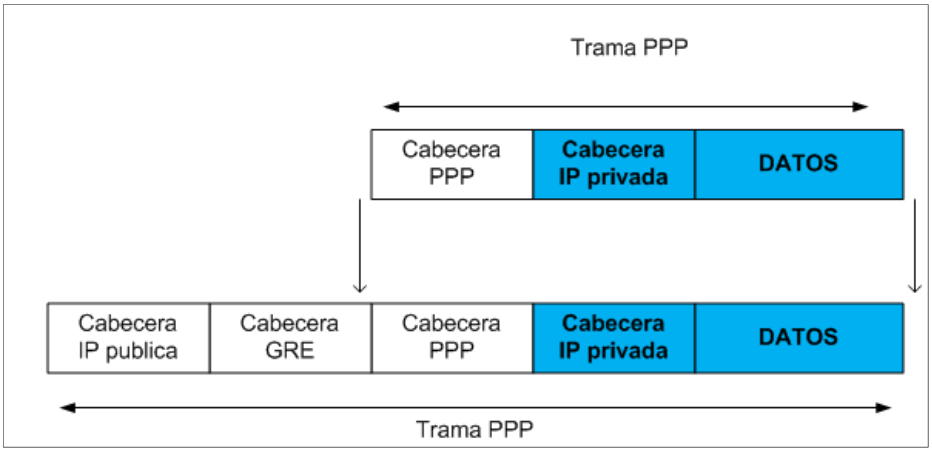
El medio de transmisión o los equipos por los que pasará el túnel serán los equipos que proporcione el ISP y que será la capa de enlace de datos. El protocolo que se emplea en el establecimiento de la conexión punto a punto entre el *host* remoto y el ISP es PPP.

3.5.6. Proceso de encapsulación PPTP

Al momento de que se crea la trama PPP y se utiliza el cifrado de flujos RSA, la trama se comprime con un encabezado PPP, posteriormente se empaqueta en otro encabezado GRE de encapsulamiento de enrutamiento genérico y un encabezado IP en donde se encuentra la dirección origen y destino de la trama.

A continuación se presenta la estructura de la trama PPP ya encapsulada mediante la norma PPTP:

Figura 15. **Encapsulación de una trama PPTP**



Fuente: elaboración propia, con programa de Visio.

- La sección cabecera IP pública es utilizada para que el datagrama viaje a través de la internet. Esta establece la comunicación entre el cliente remoto y el servidor túnel PPTP. Hay que tomar en cuenta que la IP pública es proporcionada por el ISP.

- La sección cabecera GRE encapsula el paquete PPP dentro de un datagrama IP. En otras palabras oculta las IP originales de los *host* emisor y el *host* receptor, en donde solo el servidor PPTP y el cliente PPTP podrán desencapsular la información.

- La sección cabecera PPP establece el nivel de enlace de datos entre el ISP y el usuario remoto, para luego crear el túnel. Además proporciona la autenticación del usuario remoto.

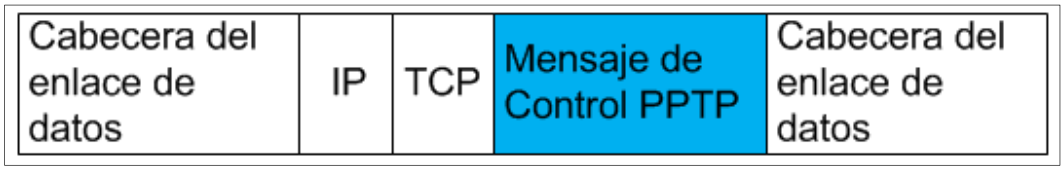
- La sección cabecera IP privada es el direccionamiento IP entre el *host* usuario remoto y el servidor de la red corporativa, para que esta última lo conecte con el *host* usuario local.

En este punto el paquete PPP el desencapsulado y si fuese interceptado, el direccionamiento será ilegible. Una vez que el paquete privado llega al servidor PPTP de la entidad corporativa, este desencapsula la trama, es decir elimina todas las cabeceras para crear el túnel y el paquete puede entrar a la red privada en cuestión.

3.5.7. Control de conexión PPTP

El protocolo PPTP especifica una serie de mensajes que son usados para la sesión de control. Estos mensajes son enviados entre el cliente PPTP y el servidor PPTP. Los mensajes de control establecidos, mantienen y terminan el túnel PPTP. Los paquetes de control consisten en una cabecera IP, una cabecera TCP y un mensaje de control como se ilustra en la siguiente figura:

Figura 16. **Control de conexión PPTP**



Fuente: elaboración propia.

Los mensajes de control son enviados dentro de los paquetes de control en un datagrama TCP. Una conexión TCP es activada entre el cliente PPTP y el server. Este *path* es usado para enviar y recibir mensajes de control. El

datagrama contiene una cabecera PPP, una TCP, un mensaje de control PPTP y las apropiadas reglas.

La siguiente tabla contiene los principales mensajes de control PPTP que son enviados sobre la conexión de control PPTP.

Tabla I. **Mensaje de control PPTP**

Mensaje de Control PPTP	**Propósito del mensaje**
Start-Control-Connection-Request	Enviado por el cliente PPTP para establecer la conexión de control. Cada túnel PPTP requiere que se establezca una conexión de control antes que pueda ser enviado cualquier otro mensaje PPTP.
Start-Control-Connection-Replay	Mensaje que lo envía el servidor PPTP este responde al mensaje Start-Control-Connection-Request.
Outgoing-Call-Request	Mensaje que envía el servidor PPTP para responder al mensaje Start-Control-Connection-Request tráfico de un túnel en partircular.
Outgoing-Call-Reply	Mensaje que envía el servidor PPTP en respuesta al mensaje Outgoing-Call-Request.
Echo-Request	Mensaje que envía el servidor PPTP para mantener la conexión. Si no hay repuesta, el túnel PPTP será finalizado

Continuación de la tabla I.

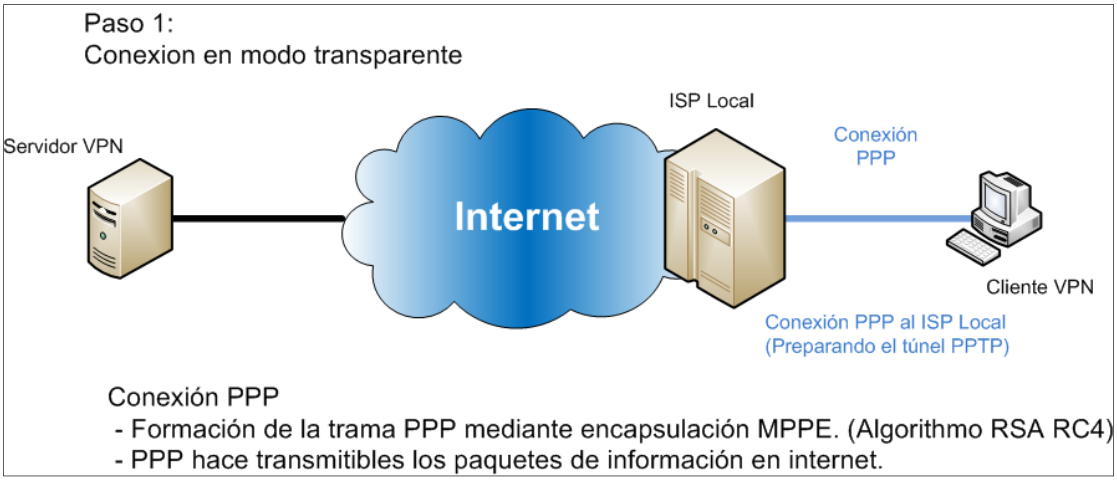
Echo-Reply	La respuesta a un Echo-Request.
WAN-Error-Notify	Mensaje que envía el servidor PPTP a todos los clientes VPN para indicar si hay errores en la interface PPP.
Set-Link-Info	Mensaje que envía el cliente PPTP o el servidor PPTP para establecer las opciones PPP negociadas.
Call-Clear-Request	Mensaje que envía el cliente PPTP que indica que el túnel será terminado.
Call-Disconnect- Notify	Mensaje que envía el servidor PPTP para responder a una solicitud Call-Clear-Request también para indicar que el túnel será finalizado.

Fuente: elaboración propia.

3.5.8. Proceso de una conexión PPTP

El Protocolo de Capa 2 PPTP se puede comprenderse más detalladamente en la siguiente figura:

Figura 17. **Control de conexión PPTP**

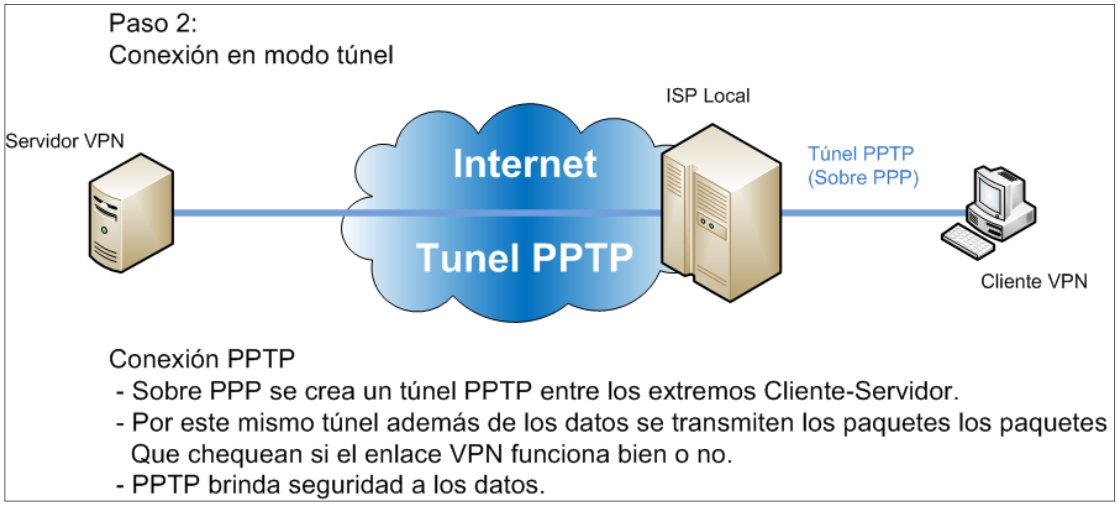


Fuente: elaboración propia, con programa de Visio.

La conexión en modo transparente podría hacerse directamente es decir sin la necesidad de establecer una conexión PPTP, creando un acceso al servidor de la red con los permisos necesarios pero no contaría con la seguridad de un túnel en la red. Este protocolo se establece solo entre la red creada entre el cliente y el ISP, esto sería equivalente a cualquier otro tipo de conexión PPPoE (punto a punto sobre Ethernet) o PPPoA (punto a punto sobre ATM).

Si se quiere tener privacidad y seguridad se debe crear un túnel en internet entre la conexión PPP y el proveedor de servicios (ISP).

Figura 18. **Conexión PPTP en modo transparente**



Fuente: elaboración propia, con programa de Visio.

3.6. L2TP (Layer 2 Tunneling Protocol)

L2TP utiliza PPP para proporcionar acceso telefónico que puede ser dirigido a través de un túnel por internet hasta un punto determinado. L2TP define el propio protocolo de establecimiento de túneles, basado en L2F. El transporte de L2TP está definido para una gran variedad de tipos de paquete de datos, incluyendo X.25, Frame Relay y ATM. Al igual que PPTP este protocolo utiliza la trama PPP creada al conectar Cliente-ISP, donde luego se realiza el túnel de capa 2. Características del protocolo L2TP:

- 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.

- Multiplexación de múltiples sesiones remotas (minimizando el número de túneles en uso). Es decir un servidor puede establecer más de una conexión privada en un túnel.

- 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.

- L2TP, a diferencia de otros protocolos es incapaz de autenticar, cifrar y garantizar la integridad de los paquetes que fluyen a través de un túnel. Por esta razón se utiliza junto con IPSec, ya que este último es el que verdaderamente se encarga de la seguridad de los datos.

4. PROTOCOLOS QUE OPERAN EN LA CAPA DE RED

4.1. IPSec (Internet Protocol Security)

La función de la capa de red del modelo de referencia OSI es especificar el direccionamiento y los procesos que permiten que los datos sean empaquetados y transportados. La encapsulación de la capa de red permite que la información viaje a través de la red en forma de paquetes.

4.1.1. ¿Qué es IPSec?

El Protocolo IPSec es un conjunto de estándares abiertos que permiten comunicaciones privadas y seguras a través de redes que operan bajo el protocolo IP (Internet Protocol) utilizando métodos criptográficos para proteger la información. IPSec proporciona protección a una red local contra los ataques mediante seguridad de extremo a extremo. Solamente los equipos que deben conocer la protección IPSec son el emisor y el receptor. IPSec brinda seguridad entre equipos de redes de área local, clientes y servidores de dominio.

Los protocolos IPSec actúan en la capa de red, la capa 3 del modelo OSI, de manera que el funcionamiento sea bastante transparente al momento de llegar al nivel de aplicación es decir se puede trabajar con HTTP, FTP, Telnet, SMTP, etc. Existen otros protocolos de seguridad que operan desde la capa de transporte hacia la capa de aplicación (capa OSI 4 a 7), como por ejemplo TLS (Transport Layer Security) y SSH (Secure Shell) esto hace que

IPSec sea más flexible y pueda ser utilizado para proteger protocolos de capa 4, como TCP y UDP que son los protocolos más utilizados.

IPSec tiene la ventaja sobre otros métodos, además de operar en capas superiores, no se necesita modificar el código para que una aplicación pueda usar IPSec. La utilidad de IPsec puede ir más allá de las VPNs, ya que dentro de IPSec existe un registro central de intercambio de llaves de internet, con lo cual cada máquina en internet podría comunicarse con otra usando cifrado y autenticación de alto nivel.

4.1.2. Características IPSec

En la actualidad el protocolo de internet IPV4 no tiene ningún tipo de protección; por lo tanto, no garantiza la seguridad de la información es por eso que este puede ser implementando junto con el protocolo IPSec y es de esta manera como puede mantenerse segura durante la transmisión. IPSec puede ofrecer lo siguiente:

- Un nivel de seguridad común y homogéneo para todas las aplicaciones, además de ser independiente de la tecnología física empleada.

- IPSec se integra en la versión actual de IP (IP versión 4) y, lo que es todavía más importante se incluye por defecto en IPv6.

- Permite construir una red corporativa segura sobre redes públicas, eliminando la gestión y el coste de líneas dedicadas.

- Asegura que los datos se transmitan solo entre el emisor y el receptor, sin que hayan terceros que puedan llegar a acceder a esta información.

- Garantiza que los datos no puedan ser cambiados en el camino.

- Permite un mecanismo de firma digital de datos de modo que el receptor pueda verificar que la firma corresponde a la persona que acredita ser la que los envió para certificar que los datos recibidos no son falsos.

- Asegura que una transacción se pueda enviar solo una vez, a menos que se autorice el reenvío.

- Ofrece al teletrabajador el mismo nivel de confidencialidad que dispondría en la red local de la empresa, no siendo necesaria la limitación de acceso a la información sensible por problemas de privacidad en tránsito.

4.1.3. Componentes de IPSec

La versión más reciente de IPSec consiste de los siguientes componentes:

- Authentication Header (AH): proporciona integridad, autenticación y no repudio si se eligen los algoritmos criptográficos apropiados.

- Encapsulating Security Payload (ESP): proporciona confidencialidad y la opción (altamente recomendable) de autenticación y protección de integridad.

- Security Associations (SA): establece los servicios de seguridad y los parámetros específicos de conexión, estos serían la clave, algoritmos, políticas, etc.

Algoritmos que hacen posible la autenticación y encriptación:

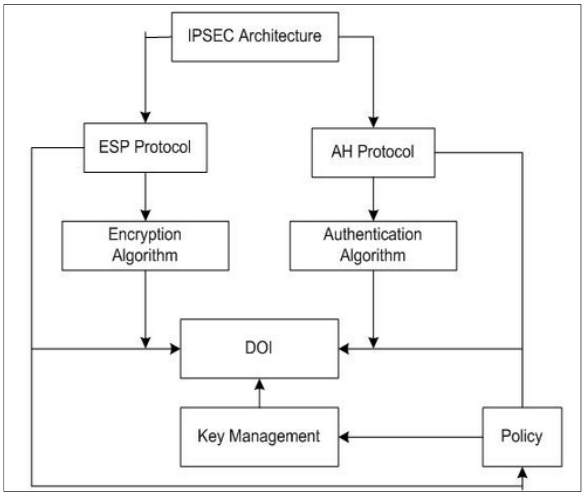
Tabla II. **Algoritmos en el protocolo IPSec**

Algoritmos de autenticación	**Algoritmos de encriptación**	**Opciones de intercambio de claves**
HMAC-MD5 HMAC-SHA1	3DES (168 Bits) DES (56 Bits) Blowfish (40-446 Bits) CAST128 (40-128 Bits)	ISAKMP/Oakley X.509 con firmas DSS Firma RSA Encriptación RSA

Fuente: elaboración propia.

El siguiente diagrama muestra la arquitectura del datagrama IPSec así como los componentes de seguridad, además de los sistemas de manejo de llaves:

Figura 19. **Estructura del protocolo IPSec**



Fuente: http://www.cavium.com/css_ipsec_stk.html. Consulta: 4 de enero de 2014.

- Manejo de llaves: documentos que describen los esquemas para administración de llaves o claves.

- Domain of Interpretation (DOI): son parámetros que incluyen todos los identificadores de los algoritmos de encriptación y el tiempo de vigencia de las llaves de autenticación.

4.1.4. Autentication Header (AH)

Este protocolo forma parte de la seguridad que brinda el protocolo IPSec, garantiza integridad de conexión y autenticación a los datos de origen de los datagramas IP. AH autentica la mayor parte posible del datagrama IP. Los datos transmitidos del paquete IP no cambian en el recorrido y AH siempre los protege. Durante el viaje de los paquetes los campos de la cabecera IP cambian y el receptor no puede predecir el valor. Estos son campos mutables

ya que cambian en el camino y AH no les brinda protección. Para proteger la información de estos campos, se deberá utilizar la modalidad de túnel del protocolo Encapsulated Security Payload (ESP).

El protocolo AH no es aplicable a paquetes de IP fragmentados es decir aqueos paquetes que sobrepasan la Unidad Máxima de Transferencia (MTU). Si el protocolo AH es aplicado a un paquete IP y este no ha sobrepasado el MTU, los equipos intermedios podrán fragmentar el paquete para la entrega. Si el *host* destino recibe el paquete fragmentado, este lo vuelve a ensamblar antes de aplicarle el proceso de AH. Si se solicita proceso de AH para un paquete IP que parece ser un fragmento, se descarta el paquete. Este ataque aprovecha el algoritmo de conjunto del fragmento para crear paquetes falsos y hacerles atravesar el cortafuegos.

4.1.4.1. Trama procesada mediante AH

Como lo indica el nombre, AH es una cabecera de autenticación, se encuentra entre la cabecera IP (tanto IPv4 como IPv6) y los protocolos de transporte que pueden ser mensajes TCP, UDP o ICMP e incluso un datagrama IP completo.

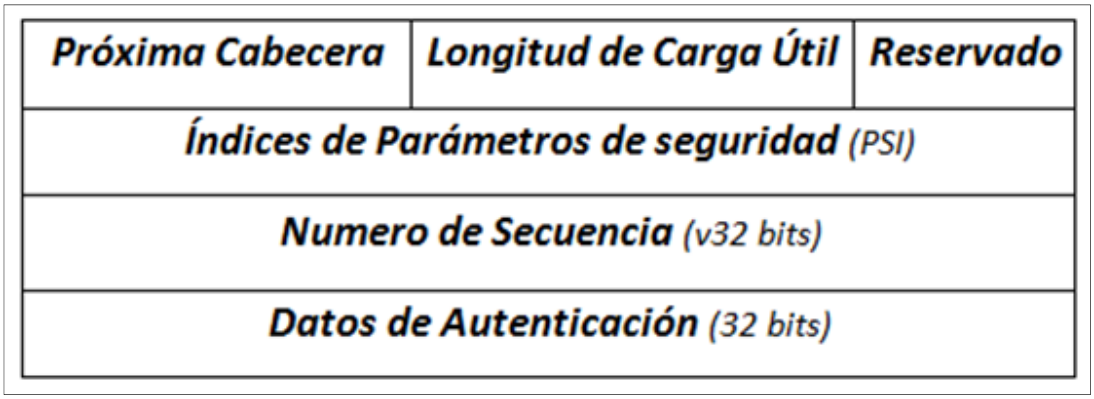
El datagrama final para IPv4 es relativamente simple y además opcional:

Figura 20. **Diagrama con autenticación AH**

Fuente: elaboración propia.

El formato interno de acuerdo al encabezado AH es el siguiente:

Figura 21. **Estructura del datagrama AH**



Fuente: elaboración propia.

En donde:

- Siguiente cabecera: (1 byte) identifica el protocolo de los datos transferidos.

- Longitud de carga útil: tamaño del paquete AH.

- SPI: indica los parámetros de seguridad que, en combinación con la dirección IP, identifican la asociación de seguridad implementada con este paquete.

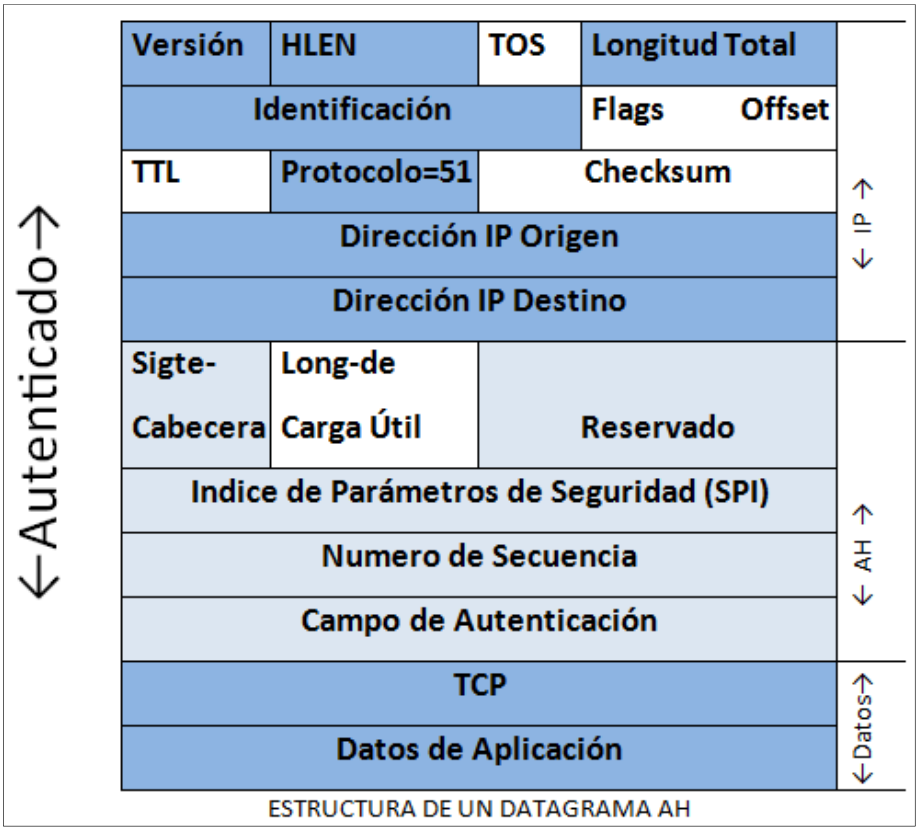
- Número de secuencia: previene los ataques de repetición (*replay*) en forma opcional, también mantiene el orden de llegada de los paquetes. Este campo almacena un número que se incrementa en uno cuando un

paquete es enviado en forma consecutiva a la misma dirección y con el mismo SPI. Utiliza 4 bytes. La función antirepetición es opcional, es decir esta función va implícita en diagrama AH, pero el extremo receptor decide si hará uso de ella mediante una previa configuración. Aunque por la longitud de 32 bytes pueda llegar a 4,300 millones antes de volver a comenzar, los contadores tanto del emisor como del receptor deben resetearse antes de alcanzar el máximo. El reseteo implica establecer una nueva clave.

- Datos de autenticación: estos son el compendio calculado mediante el algoritmo de autenticación (HMA), utilizado por el receptor para comparar lo recibido luego de aplicar la misma operación al datagrama. También se conoce como MAC o ICV, con tamaños máximos de 16 (MD5) o 20 (SHA-1) bytes, AH es un protocolo IP relativamente nuevo y como tal la autoridad que asigna los números a internet (IANA) le ha asignado el número decimal 51. Esto significa que el campo protocolo de la cabecera IP tendrá el valor 51, en lugar de los valores 6 o 17 que se asocian a datos TCP o UDP, con esto será más difícil descifrar el tipo de mensaje que se está transmitiendo.

La trama IP autenticada con la cabecera de autenticación (AH) completa a transmitir presenta la siguiente forma:

Figura 22. **Estructura del protocolo AH**

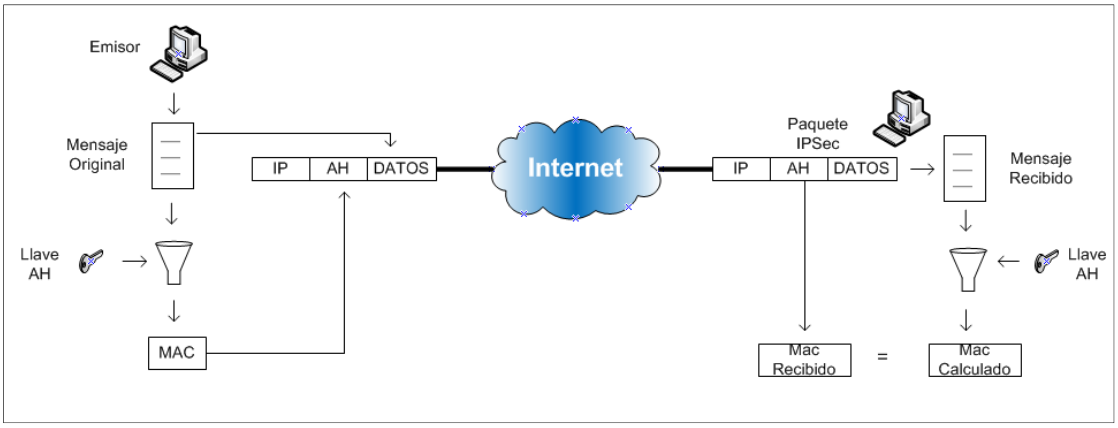


Fuente: PEREZ IGLESIAS, Santiago. Análisis del protocolo IPSec. p. 53.

4.1.4.2. Hashed Message Authentication code (HMAC)

Este algoritmo consiste en aplicar una función *hash* criptográfica con la combinación de una clave criptográfica secreta aplicado a una combinación de un porcentaje de los datos a transmitir y una clave secreta, siendo el resultado un código denominado extracto. Dicha salida tiene la propiedad de que es una huella personal asociada a los datos y la persona que los ha generado, puesto que junto al receptor es la única que conoce la clave. De esta forma se asegura que el mensaje enviado proviene del origen esperado y además con el procedimiento se previene la integridad de dicho mensaje.

Figura 23. **Funcionamiento de AH**



Fuente: elaboración propia, con programa de Visio.

En esta figura se puede observar el modo funcionamiento del protocolo AH:

- El emisor calcula un extracto del mensaje original, el cual se copia en uno de los campos de la cabecera AH, específicamente el campo datos de autenticación.

- Una vez construido el paquete se envía a través de la red.

- En el extremo del receptor de nuevo se realiza el cálculo del extracto y se compara con extremo recibido en el paquete.

Si las claves son iguales el receptor tendrá la certeza que el paquete IP no ha sido modificado en el tránsito y que proviene efectivamente del origen esperado. Cabe mencionar que el extracto o código de autenticación del mensaje (MAC) es imposible de calcular si no se conocen las claves que solo conocen el emisor y el receptor.

4.1.4.3. Funciones HASH

Hay dos funciones o algoritmos que hacen posible la autenticación y es obligatorio el uso de uno de ellos, según el protocolo IPSec.

Message Digest 5 (MD5) y Secure Hash Algorithm 1 (SHA1), que a continuación se detallan:

Tabla III. **Propiedades de la operación HASH**

Operación MD5 o SHA1	**Funcionamiento**
Integridad	SHA-1 MD5 produce una presentación única comprimida o codificada de 150 o 128 bits respectivamente, correspondiente al datagrama que se desee transmitir. Si estas estas representaciones o compendios son iguales entre el emisor y el receptor, entonces el bloque de datos no tuvo alteración alguna durante la transmisión. Luego se codifica la presentación para llegar al mensaje original.
Autenticación	La autenticación es garantizada mediante el uso de claves secretas cuando es calculado el mensaje codificado (representación codificada). Esta clave es únicamente conocida por el emisor y receptor. Dicha clave corresponderá a una serie de compendios de 16 bits por cada 64 bytes del datagrama a transmitir que será calculado entre los extremos. La serie de valores formados por los compendios de 16 bits se concatenan en un solo valor, el cual es colocado en el campo de autenticación del encabezado AH. Luego se comparan las claves y si coinciden los extremos están autenticados.

Fuente: http://www.monografias.com/trabajos76/funciones-hash-criptografia/funciones-hash-criptografia2.shtml. Consulta: 5 de enero de 2014.

4.1.4.4. Funcionamiento del algoritmo HASH

Las funciones *hash* en resumen son algoritmos que consiguen crear a partir de una entrada (ya sea un texto, una contraseña o un archivo, por ejemplo) una salida alfanumérica de longitud normalmente fija que representa un resumen de toda la información que se le ha dado (es decir, a partir de los datos de la entrada crea una cadena que solo puede volverse a crear con esos mismos datos). Las funciones *hash* tiene varios objetivos, entre ellos está asegurar que no se ha modificado un archivo en una transmisión, hacer ilegible una contraseña o firmar digitalmente un documento.

Un ejemplo de cómo trabaja este tipo de funciones se explica usando un modo de sustitución para luego a la información resultante se aplica una función matemática para obtener la clave del bloqueo de datos entrante, tal como se muestra a continuación:

Figura 24. **Método de sustitución HASH**

A	B	C	D	E	F	G	H	I	J	K	L	M
65	66	67	68	69	70	71	72	73	74	75	76	77

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
78	79	80	81	82	83	84	85	86	87	88	89	90

Fuente: REY CLERICUS, Pedro. *Redes Privadas Virtuales*. p. 39.

Esta sustitución es básicamente la codificación ASCII, que se utiliza como ejemplo.

La información a transmitir es la siguiente frase: las empresas pueden comunicarse en forma remota. Donde cada letra se representa por el equivalente de la tabla y los espacios entre palabras se presentan por el número 32 según el código ASCII.

Figura 25. **Ejemplo de sustitución HASH**

L	A	S		E	M	P	R	E	S	A	S		P	U	E
76	65	83	32	69	77	80	82	69	83	76	83	32	80	85	69
D	E	N		C	O	M	U	N	I	C	A	R	S	E	
68	69	78	32	67	79	77	85	78	73	67	65	82	83	69	32
E	N		F	O	R	M	A		R	E	M	O	T	A	
69	78	32	70	79	82	77	65	32	82	69	77	79	84	65	32

Fuente: REY CLERICUS, Pedro. *Redes Privadas Virtuales*. p. 39.

Una vez que se tienen las representaciones numéricas de los caracteres de la frase se procede a efectuar la siguiente función (cada 3 letras) en orden correlativo:

(1º - 2º) * 3º = resultado (integridad + autenticación)

Figura 26. **Resolución ejemplo de sustitución HASH**

L	A	S		E	M	P	R	E	S	A	S		P	U	E
76	65	83	32	69	77	80	82	69	83	76	83	32	80	85	69
		913			-2849			-138			581			-4080	
D	E	N		C	O	M	U	N	I	C	A	R	S	E	
68	69	78	32	67	79	77	85	78	73	67	65	82	83	69	32
	69			3082			170			335			-1411		
E	N		F	O	R	M	A		R	E	M	O	T	A	
69	78	32	70	79	82	77	65	32	82	69	77	79	84	65	32
			3220			-231			2706			-632			608

Fuente: REY CLERICUS, Pedro. *Redes Privadas Virtuales*. p. 40.

Luego se realiza la sumatoria de todos los resultados.

(913 – 2849 – 138 + 581 – 4080 + 69 + 3082 + 170 + 335 – 1411 + 2553 + 3220 – 231 + 2706 – 632 + 608) = 4896

Entonces junto con la palabra o frase a transmitir se adjunta además el resultado de la operación *hash*, al momento que el emisor recibe la información ejecuta la misma función *hash* y si los resultados son los mismos en este caso sería el dato 4 896 se asegura que los datos no han sido alterados y tampoco tienen errores, previamente el emisor y el receptor han acordado la codificación es por ello que se puede asegurar que los datos vienen autenticados.

4.1.5. Encapsulating Security Payload (ESP)

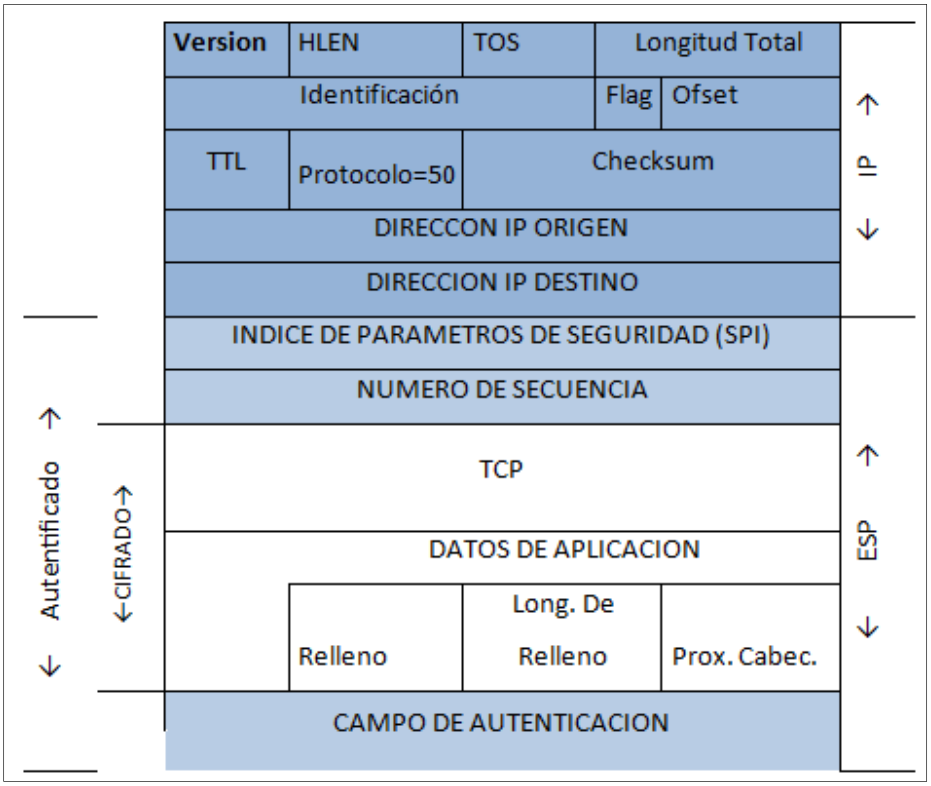
El objetivo principal del protocolo ESP es proporcionar autenticidad de origen, integridad y protección de confidencialidad de un paquete. ESP también soporta configuraciones de sólo cifrado y sólo autenticación, pero utilizar cifrado sin autenticación está altamente desaconsejado porque es inseguro por ello se deben de cifrar los datos que se desean enviar estos se incluyen en el datagrama IP. Adicionalmente, puede ofrecer los servicios de integridad y autenticación dependiendo del modo de funcionamiento.

4.1.5.1. Datagrama IP, procesada mediante ESP

Ya que ESP aporta más funciones de AH, la estructura de cabecera es más compleja; esta consta de una cabecera y una cola que rodean los datos transportados y de esta forma hace los datos más seguros y difíciles de descifrar ante agresiones de terceros. Estos datos a transportar pueden ser cualquier protocolo IP como por ejemplo: TCP, UDP, ICMP o incluso un paquete IP completo.

En la siguiente figura se visualiza un paquete IP el cual fue expuesto al protocolo ESP:

Figura 27. **Estructura de un paquete procesado con ESP**



Fuente: PEREZ IGLESIAS, Santiago. Análisis del protocolo IPSec. p. 54.

En la figura 27 se puede observar que el encabezado ESP tiene los siguientes campos:

- Índice de Parámetro de Seguridad (SPI): permite que el receptor elija la Asociación de Seguridad (SA) con la cual se procesará un paquete recibido. Tiene un tamaño de 4 bytes.

- Número de secuencia: es un número siempre creciente utilizado para evitar ataques de repetición que por medio de un contador va aumentando el valor en 1 cada vez que se aplica a un paquete tamaño 4 bytes.

La cola de ESP tiene los siguientes campos:

- Relleno: es necesario cuando se requiere que el texto sea encriptado por un múltiplo de una cantidad de bytes para mejorar la seguridad.

- Longitud de relleno: indica la longitud de campo anterior.

- Próximo encabezamiento: identifica el protocolo de los datos transmitidos. Es decir (1 para ICMP, 6 para TCP, 17 para UDP, etc.)

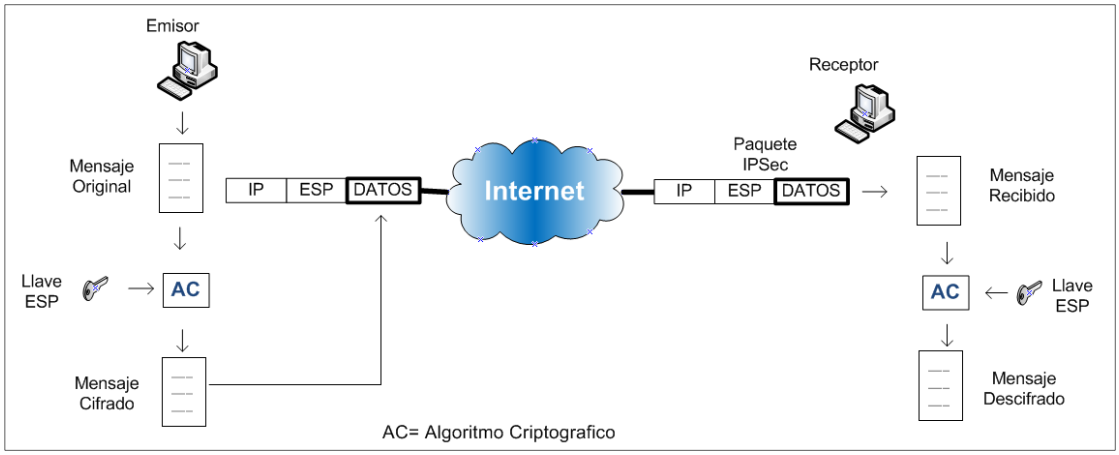
- Campo de identificación: este es el resultado del algoritmo de autenticación que utiliza el receptor para compararlo con el resultado obtenido luego de que se aplique la misma función *hash* al datagrama.

El Internet Assigned Numbers Authority (IANA) ha asignado al campo protocolo de la cabecera IP el valor decimal 50 cuando se utilice ESP. Así como la carga útil, este campo también está cifrado, de esta manera un atacante no sabe qué tipo de contenido es.

4.1.5.2. Cifrado ESP

El cifrado de los de los datos dentro del protocolo ESP debe ser realizada por un algoritmo de cifrado de clave simétrica, como por ejemplo, DES, 3DES, RC5, AES etc. Regularmente se utilizan algoritmos de cifrado de bloque, de manera tal que la longitud de los datos a cifrar tiene que ser el múltiplo del tamaño del bloque. Es por eso que el objetivo del campo relleno que forma parte de la estructura del paquete ESP, es ocultar la longitud real de los datos.

Figura 28. **Funcionamiento del paquete con trama ESP**



Fuente: elaboración propia, con programa de Visio.

En la figura anterior se aprecia como el protocolo ESP permite enviar datos en forma segura. El emisor toma el mensaje este aplica un algoritmo de cifrado simétrico con el que se obtiene una clave determinada y lo encapsula en un paquete IP, seguida de la cabecera ESP. Durante el recorrido hasta el destino, si el paquete fuera capturado por un tercero solo obtendrá un conjunto de bit que no sería información valiosa o no se podría descifrar. Cuando el mensaje llega al receptor este aplica de nuevo el algoritmo de cifrado con la

clave idéntica, recuperando los datos originales. Cabe mencionar que solo el emisor y el receptor deben conocer la clave, de manera que aun atacante se le dificulte descifrar los datos.

4.1.5.3. Tipos de cifrado aplicado a IPSec

Cifrados de sustitución:

El cifrado por sustitución es un método de cifrado por el que unidades de texto plano son sustituidas con texto cifrado siguiendo un sistema regular; las unidades pueden ser una sola letra (el caso más común), pares de letras, tríos de letras, mezclas de lo anterior, entre otros. El receptor descifra el texto realizando la sustitución inversa.

Existen varios cifrados de sustitución:

- La sustitución monoalfabética consiste en reemplazar cada una de las letras del mensaje por otra letra del alfabeto.

- La sustitución polialfabética consiste en utilizar una serie de cifrados monoalfabéticos que son reutilizados periódicamente.

- La sustitución homófona hace posible que cada una de las letras del mensaje del texto plano se corresponda con un posible grupo de caracteres distintos.

- La sustitución poligráfica consiste en reemplazar un grupo de carácteres en un mensaje por otro grupo de carácteres.

El Código Cesar es uno de los más antiguos ya que el uso se remonta a Julio César. El principio de cifrado se basa en la adición de un valor constante a todos los carácteres de un mensaje o, más precisamente, a el código ASCII. En este método que se reemplaza una letra del alfabeto por la 3º que le sigue, entonces a? D, b? E, c? F,…y z? C. Simplemente es cuestión de cambiar todos los valores de los carácteres de un mensaje en un determinado número de posiciones, es decir, sustituir cada letra por otra. Por ejemplo, si cambiamos 3 posiciones del mensaje comment ca marche, obtenemos frpphqw fd pdufkh. Cuando el valor agregado da una letra posterior a la Z, podemos simplemente continuar empezando por la A. La siguiente mejora consiste en tener cada uno de los símbolos del texto en claro, digamos las 26 letras por simplicidad, correlacionadas con alguna otra letra, por ejemplo:

Texto en claro: a b c d e f g h i j k l m n o p q r s t u v w x y z

Texto cifrado: Q W E R T Y U I O P A S D F G H J K L Z X C V B N M

A este sistema general se le conoce como sustitución monoalfabetica, consiste en reemplazar cada una de las letras del mensaje por otra letra del alfabeto.

Cifradores de transposición o permutación:

Los cifrados por sustitución conservan el orden de los símbolos de texto plano, pero los disfrazan. Los cifrados por transposición, reordenan las letras pero no las disfrazan.

El texto cifrado se lee por columnas comenzando con la columna cuya letra clave tiene el valor inferior.

A continuación se presenta un ejemplo de transposición columnar:

Tabla IV. **Ejemplo de cifrador de permutación**

S	I	S	T	E	M	A
5	3	6	7	2	4	1
R	E	D	E	S	I	N
A	L	A	M	B	R	I
C	A	S	A	B	C	D

Fuente: http://es.kioskea.net/contents/139-cifrado-de-sustitucion. Consulta: 7 de enero de 2014.

La clave del cifrado es sistema. El objetivo de la clave es numerar las columnas, estando la columna número 1 bajo la letra de la clave más próxima al comienzo del alfabeto y así sucesivamente, en este ejemplo, la A, luego la E, etc. El texto plano se escribe horizontalmente, en filas, las cuáles se rellenan para completar la matriz si es necesario. El texto cifrado se lee por columnas, comenzando por la 1, luego la 2,3, etc.

En el ejemplo, el texto plano es redes inalámbricas y el cifrado será:

nidsbbelaircracdasema.

Hay dos tipos de tecnologías de cifrado, de clave privada (cifrado simétrico) y de clave pública (cifrado asimétrico).

- Cifrado simétrico: los algoritmos simétricos, o de clave secreta, se caracterizan por ser altamente eficientes (en relación al tamaño de la clave) y robustos. Se les llama así porque se emplean la misma clave para cifrar y para descifrar. Se basan en el uso de claves secretas que previamente hay que intercambiar mediante canales seguros, con los riesgos que ello supone. Todas las partes deben conocerse y confiar totalmente la una en la otra. Cada una de ellas debe poseer una copia de la clave que haya sido protegida y mantenida fuera del alcance de los demás. Además, dichas claves no se deben utilizar para varios mensajes, ya que si se interceptarán algunos de ellos, se podrían encontrar métodos para descodificarlos.

- Cifrado asimétrico: es el método criptográfico que usa un par de claves para el envío de mensajes. Las dos claves pertenecen a la misma persona que ha enviado el mensaje. Una clave es pública y se puede entregar a cualquier persona, la otra clave es privada y el propietario debe guardarla de modo que nadie tenga acceso a ella. Además, los métodos criptográficos garantizan que esa pareja de claves sólo se puede generar una vez, de modo que se puede asumir que no es posible que dos personas hayan obtenido casualmente la misma pareja de claves.

Si el remitente usa la clave pública del destinatario para cifrar el mensaje, una vez cifrado, sólo la clave privada del destinatario podrá descifrar este mensaje, ya que es el único que la conoce. Por tanto, se logra la confidencialidad del envío del mensaje, nadie salvo el destinatario puede descifrarlo.

4.1.6. Algoritmos de cifrado

El protocolo ESP puede utilizar diferentes tipos de algoritmo de cifrado para resguardar los datos, no hay mucha diferencia en el funcionamiento de estos algoritmos, por lo que se analizarán los más importantes:

4.1.6.1. Algoritmo de encriptación de datos (DES)

Se trata de un sistema de cifrado simétrico por bloques de 64 bits, de los que 8 bits (un byte) se utilizan como control de paridad (para la verificación de la integridad de la clave). Cada uno de los bits de la clave de paridad (1 cada 8 bits) se utiliza para controlar uno de los bytes de la clave por paridad impar, es decir, que cada uno de los bits de paridad se ajusta para que tenga un número impar de 1 dentro del byte al que pertenece. Por lo tanto, la clave tiene una longitud útil de 56 bits, es decir, realmente sólo se utilizan 56 bits en el algoritmo.

El algoritmo se encarga de realizar combinaciones, sustituciones y permutaciones entre el texto a cifrar y la clave, asegurándose al mismo tiempo de que las operaciones puedan realizarse en ambas direcciones (para el descifrado). La combinación entre sustituciones y permutaciones se llama cifrado del producto.

La clave es codificada en 64 bits y se compone de 16 bloques de 4 bits, generalmente anotada de k1 a k16. Dado que solamente 56 bits sirven para el cifrado, como la clave efectiva es de 56 bits, son posible un total de 2 elevado a 56= 72.057.594.037.927.936 claves posibles, es decir, unos 72 000 billones de claves, por lo que la ruptura del sistema por fuerza bruta o diccionario es

sumamente improbable, aunque no imposible si se dispone de suerte y una gran potencia de cálculo.

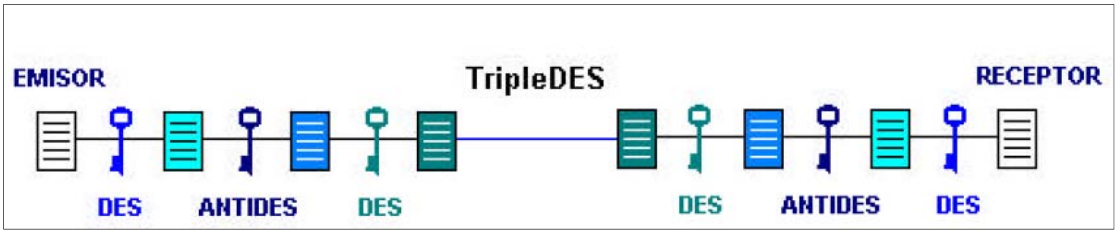
4.1.6.2. Triple algoritmo de encriptación de datos (3DES)

Recordar que DES es un sistema mono alfabético que fue desarrollado en colaboración con IBM. 3DES fue creado con la finalidad de mejorar el cifrado DES, este sería el predecesor y así estar preparados para que si por algún motivo DES fuese corrompido entrará en funcionamiento 3DES.

3DES realiza algo tres veces más que un algoritmo DES regular. Este también utiliza tres llaves en cada bloque de texto plano. En vez de utilizar una llave de 56 bits desde la tabla de llaves, 3DES encripta el texto plano con la primera llave, encripta ese texto encriptado con otra llave de 56 bits y luego encripta nuevamente el texto encriptado con otra llave de 56 bits.

3DES también es capaz de trabajar con llaves más extensas para hacerlo más seguro. Para descifrar este algoritmo se tendrían que descubrir las tres llaves diferentes. No solo eso, el texto será desencriptado solo cuando las tres llaves correctas sean usadas en el orden correcto.

Figura 29. **Mensajes con triple DES**



Fuente: http://social.msdn.microsoft.com/Forums/es-ES/7699b06f-2f84-44be-8552-65d9f0956934/encriptar-mensaje-soap-usando-tripledes-xmlenc?forum=webdeves. Consulta: 9 de enero de 2014.

Para cifrar mediante el algoritmo Triple DES se siguen los siguientes pasos:

- Dividir la clave de 128 bits en dos partes de 64 bits: k1 y k2
- Cifrar el texto en claro con k1. El resultado es conocido como ANTIDES
- Cifrar ANTIDES con k2
- Cifrar el resultado con k1
- Si k1=k2 el resultado coincide con un cifrado mediante DES

Cuando el receptor recibe el mensaje este aplica el proceso inverso para descifrar el mensaje original. En el caso en que la claves de 128 bits este formada por dos claves iguales de 64 bits, es decir k1=k2, el sistema se comporta como un proceso DES simple.

4.1.7. Modos de funcionamiento IPSec

Cabe mencionar que la encriptación no debe sustituir a la autenticación, ya que esta última refuerza la encriptación de la información. Los modos de funcionamiento de IPSec son:

- Modo transporte
- Modo túnel

La diferencia entre estos dos modos es que en modo transparente el encabezado exterior determina la directiva IPsec que protege el paquete IP interior o carga útil IP, en el modo túnel el paquete IP interior determina la directiva IPsec que protege el contenido en otras palabras se protegen los paquetes (capa de red).

4.1.7.1. Modo transporte

En este modo la cabecera AH o ESP es insertada entre el área de datos y la cabecera IP, de tal forma que se mantienen las direcciones IP originales.

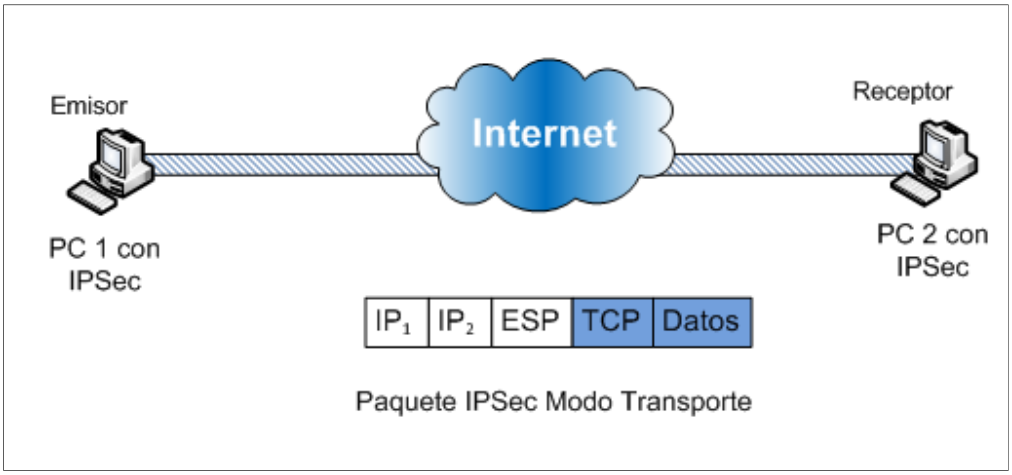
El contenido encapsulado en un datagrama AH o ESP proviene directamente de la capa de transporte. Por tanto, la cabecera IPSec se insertará a continuación de la cabecera IP y justo antes de los datos aportados por la capa de transporte. De esta forma, sólo la carga útil es cifrada y autenticada.

El modo transporte asegura la comunicación extremo a extremo pero los extremos deben saber de la existencia del protocolo IPSec para poder entenderse.

- Si la política de seguridad define que los paquetes deben ser encriptados se utiliza ESP en modo transporte.

- En el caso en que solo sea requerida la autenticación se utiliza AH en modo transporte.

Figura 30. **Modo transporte entre 2 equipos configurados con IPSec**



Fuente: elaboración propia, con programa de Visio.

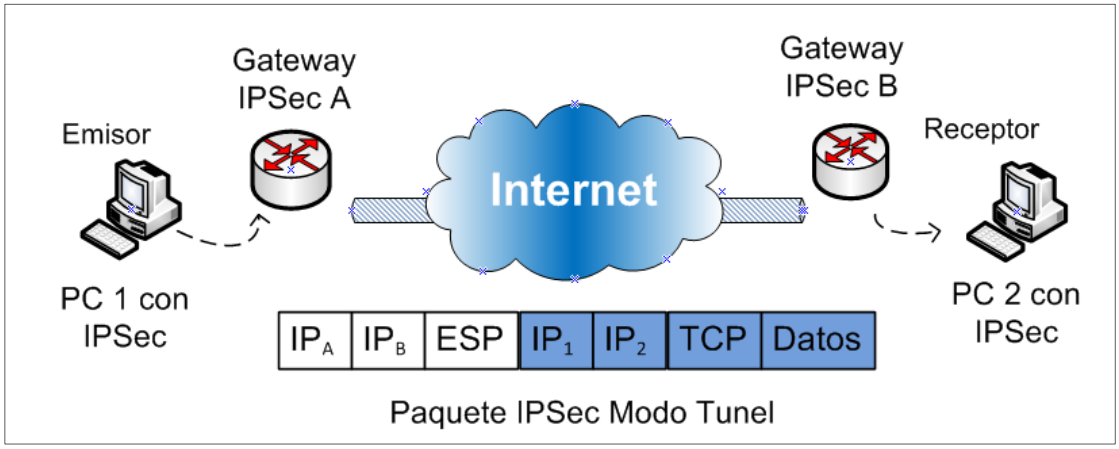
En esta figura se observan dos PCs que tienen configurado IPSec, por lo tanto se comunican en forma segura. Dado que el intercambio de información se realiza en modo transparente, la información está protegida únicamente por el protocolo TCP o UDP.

4.1.7.2. Modo túnel

En el modo túnel, el paquete IP entero (cabecera + datos) es cifrado y autenticado. Este paquete será encapsulado en un nuevo paquete IP, por tanto, la dirección IP cambiará por la del último paquete IP. Al paquete original se le añade una cabecera AH o ESP y a continuación se le añade la cabecera IP que servirá para encaminar el paquete a través de la red.

El modo túnel normalmente es usado para comunicar redes con redes, pero también se puede usar, para comunicar ordenadores con redes y ordenadores con ordenadores. Este modo de funcionamiento facilita que los nodos puedan ocultar la identidad de otros nodos que se estén comunicando.

Figura 31. **Modo túnel entre 2 equipos configurados con IPSec, usando gateway de ruteo**



Fuente: elaboración propia, con programa de Visio.

En la figura anterior se observan dos redes que utilizan para conectarse Gateway IPSec, estos trabajan en modo túnel para comunicarse. La comunicación se hace a través de la red pública (internet) y se hace a través de los Gatways IPSec que crean un túnel a través del cual la comunicación viajará de forma segura hay que tomar en cuenta que los Gateways IPSec son los que reciben la comunicación, la encriptan y la vuelven a enviar, la reciben la desencriptan y la envían a el destino final.

4.2. Control de claves en una asociación IPSec

Para que en toda comunicación se pueda encapsular paquetes IPSec, se necesitan mecanismos para almacenar las claves secretas, algoritmos y dirección IP involucradas en la comunicación. Todos estos parámetros se almacenan en Asociaciones de Seguridad (SA).

4.2.1. Asociación de seguridad (SA)

Una cosa particularmente curiosa de IPSec es que está orientado a conexión, a pesar de que se encuentre en la capa IP. Se debe a que la seguridad se fundamenta en la existencia de una clave que conocen los dos sistemas que se van a comunicar y que tiene una validez determinada. Esto no significa, sin embargo, que los paquetes de tipo UDP pierdan sentido, sino que para cualquier tipo de comunicación segura antes se habrán debido establecer una serie de parámetros. De ahí se tomó el término conexión, que en terminología IPSec se conoce como Asociación de Seguridad (SA o Security Association).

Las asociaciones de seguridad se identifican de forma única por una tupla compuesta por un Índice de Parámetro de Seguridad (SPI), una dirección IP

destino y un identificador del protocolo de seguridad (AH o ESP). Los sistemas participantes en alguna comunicación con IPSec deberán almacenar el SPI, de forma que se pueda identificar fácilmente la asociación de seguridad a la que pertenece cada paquete.

Si bien la especificación de IPSec está fuera del ámbito de especificar cómo se ha de implementar la gestión de las asociaciones de seguridad, sí que sugiere que estas sean gestionadas por dos bases de datos nominales: la base de datos de asociaciones de seguridad (SAD o Security Association Database) y la base de datos de políticas de seguridad (SPD o Security Policy Database).

La base de datos de políticas de seguridad especifica las políticas a la hora de gestionar cualquier tipo de tráfico, vaya a ser este cifrado o no. Normalmente, esta base de datos estará formada por una serie de reglas, asociada cada una de ellas a un selector (direcciones origen y destino, protocolo de la capa de nivel superior, puerto). Para cada paquete que se envíe o reciba por parte del nodo se tomará una de las siguientes decisiones según la base de datos de políticas de seguridad: descartarlo, aplicar alguna regla de cifrado o autenticación, o pasarlo en claro.

4.2.2. Administración de claves

Puede darse de la siguiente manera:

- Manual: es cuando el emisor y receptor que hablan IPSec establecen una asociación de seguridad específica y esta se utilizará para autenticar los accesos y enmascarar los datos cabe mencionar que la configuración de los equipos que involucran la conexión IPSec se hace de forma manual.

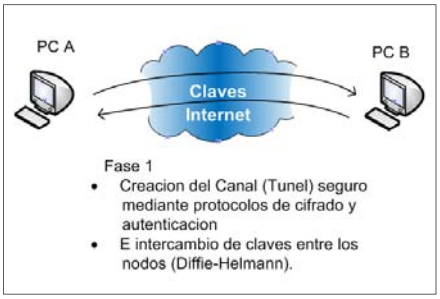
- Automática: esta forma establece automáticamente la asignación de las llaves de la asociación IPSec y el sistema considerando como norma tanto para IPv6 como para IPv4 es el protocolo IKE.

4.2.3. Protocolo IKE (Internet Key Exchange)

El protocolo IKE no sólo se encarga de la gestión y administración de las claves sino también del establecimiento de la conexión entre los participantes correspondientes. El Protocolo IKE se divide en 2 fases:

- IKE Phase 1: la fase 1 de IKE, trabaja sobre el puerto 500 UDP de forma bidireccional. Se encarga de autenticar y proteger las identidades de los equipos que hablan IPSec. Negocia una política IKE SA que concuerde en parámetros entre los 2 equipos para proteger el intercambio de claves. Genera un intercambio Diffie-Hellman autenticado, para obtener claves compartidas. A partir de esta clave, establece un túnel encriptado para la negociación de los parámetros de la fase 2.

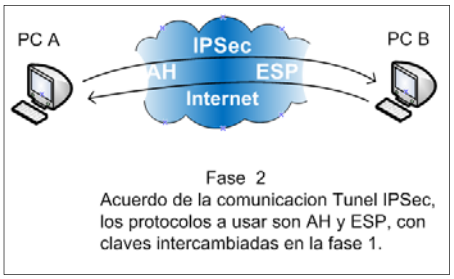
Figura 32. **Establecimiento de canal seguro y negociación de claves IKE**



Fuente: elaboración propia, con programa de Visio.

- IKE Phase 2: la fase 2 de IKE, trabaja con los protocolos 50 ESP, 51 AH y con el puerto 4500 UDP. Se encarga de negociar los parámetros IPsec SA, esto se realiza dentro del túnel IKE SA. Establece las asociaciones IPsec SA. Renegocia periódicamente estas SA para garantizar la seguridad durante todo el tiempo de vida del túnel. Opcionalmente puede realizar intercambios Diffie-Hellman.

Figura 33. **Negociación de las claves IPSec**



Fuente: elaboración propia, con programa de Visio.

Diffie-Hellman es un algoritmo para generar un túnel seguro entre 2 puntos. Cuando el tiempo de vida caduca, las 2 fases se renegocian, pero las claves Diffie-Hellman se mantienen. Para forzar la renovación de estas claves, podemos utilizar PFS (Perfect Forward Secrecy), que asegura que cada nueva clave criptográfica no estará relacionada de ninguna manera con la anterior.

4.2.4. Certificados digitales

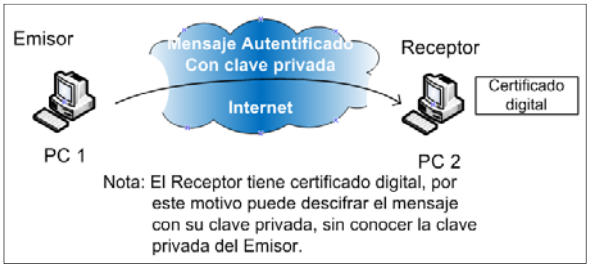
La eficacia de las operaciones de cifrado y firma digital basadas en criptografía de clave pública sólo está garantizada si se tiene la certeza de que la clave privada de los usuarios sólo es conocida por dichos usuarios y que la

pública puede ser dada a conocer a todos los demás usuarios con la seguridad de que no exista confusión entre las claves públicas de los distintos usuarios.

Para garantizar la unicidad de las claves privadas se suele recurrir a soportes físicos tales como tarjetas inteligentes o tarjetas PCMCIA que garantizan la imposibilidad de la duplicación de las claves. Además, las tarjetas criptográfica suelen estar protegidas por un número personal sólo conocido por el propietario que garantiza que, aunque se extravíe la tarjeta, nadie que no conozca dicho número podrá hacer uso de ella.

Por otra parte, para asegurar que una determinada clave pública pertenece a un usuario en concreto se utilizan los certificados digitales. Un certificado digital es un documento electrónico que asocia una clave pública con la identidad del propietario. Adicionalmente, además de la clave pública y la identidad del propietario, un certificado digital puede contener otros atributos para, por ejemplo, concretar el ámbito de utilización de la clave pública, las fechas de inicio y fin de la validez del certificado, etc. El usuario que haga uso del certificado podrá, gracias a los distintos atributos que posee, conocer más detalles sobre las características del mismo.

Figura 34. **Encriptación de mensajes usando certificados digitales para la desencriptación**



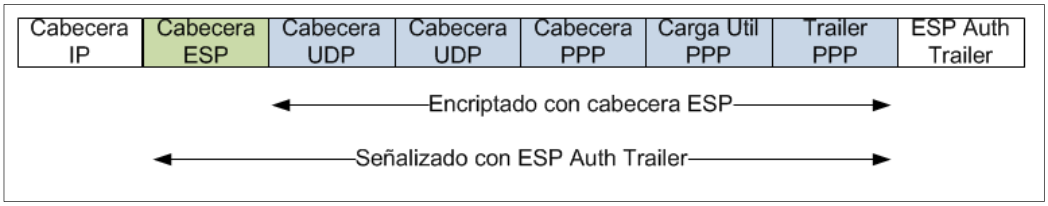
Fuente: elaboración propia, con programa de Visio.

4.3. IPSec y L2TP

L2TP e IPSec se combinan para proporcionar túneles y seguridad para los paquetes IP, IPX y de otros protocolos que viajen por cualquier red IP. IPSec también puede realizar túneles sin L2TP, pero sólo se recomienda para la interoperabilidad, cuando una de las puertas de enlace no admite L2TP o PPTP.

L2TP encapsula los paquetes originales primero en una trama PPP (con compresión cuando es posible) y después, en un mensaje UDP con el puerto 1701. Como el mensaje UDP es una carga de IP, L2TP utiliza el modo de transporte IPSec para proteger el túnel. El protocolo intercambio de claves de internet de IPSec negocia la seguridad para el túnel L2TP mediante autenticación basada en certificados o autenticación por claves compartidas previamente. Si se establecen correctamente asociaciones de seguridad IPSec de modo principal y de modo rápido, L2TP negocia el túnel, incluyendo las opciones de compresión y autenticación de usuario y realiza la autenticación de usuario basada en PPP.

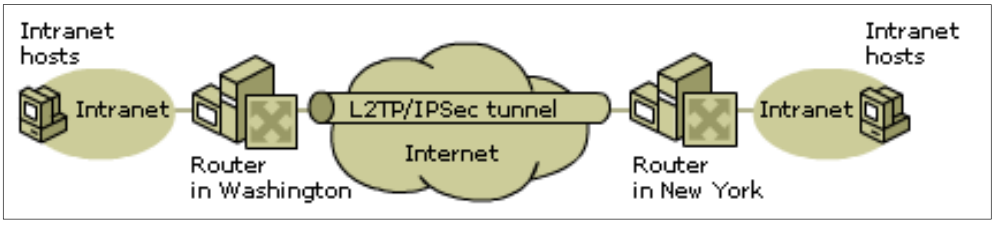
Figura 35. **Encabezado IPSe / L2TP**



Fuente: http://msdn.microsoft.com/es-es/library/cc775944(v=ws.10).aspx.
Consulta: 12 de enero de 2014.

El paquete original, que aquí aparece como carga PPP, incluye las direcciones de origen y destino originales utilizadas en la red privada. El encabezado IP exterior, mostrado como Encabezado IP, contiene las direcciones de origen y destino del servidor y el cliente VPN en la red pública. El encabezado L2TP contiene información de control del túnel L2TP. El encabezado PPP identifica el protocolo del paquete original (por ejemplo, IP o IPX).

Figura 36. **Túnel combinado entre IPSec y L2TP**



Fuente: http://msdn.microsoft.com/es-es/library/cc775944(v=ws.10).aspx.
Consulta: 13 de enero de 2014.

5. FIREWALL

5.1. Definición de *firewall*

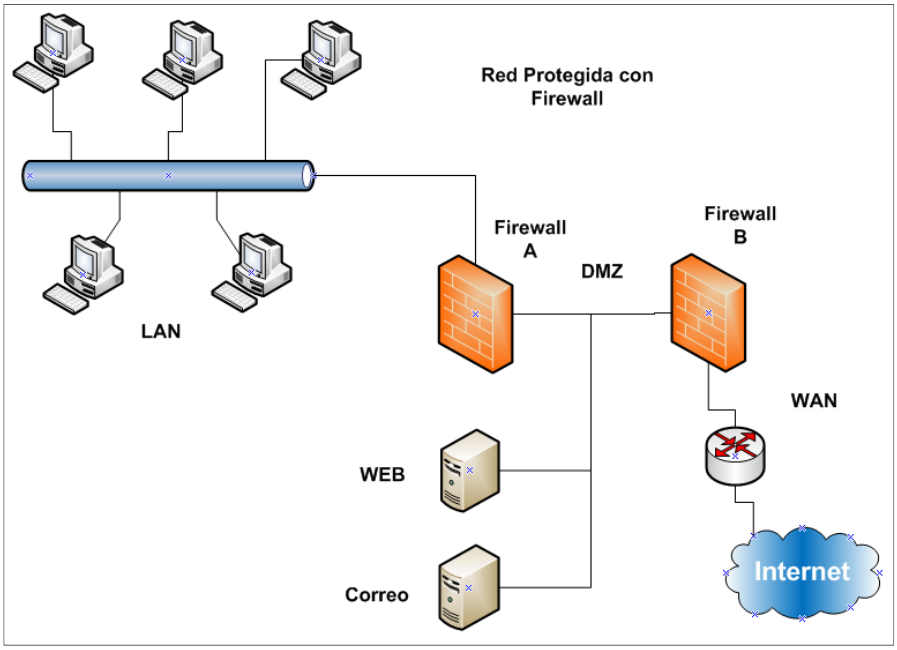
Un cortafuego o *firewall* es un sistema que previene el uso y el acceso no autorizado a un ordenador. Los cortafuegos pueden ser software, hardware, o una combinación de ambos. Se utilizan con frecuencia para evitar que los usuarios no autorizados de internet tengan acceso a las redes privadas conectadas con internet, especialmente intranets.

Todos los mensajes que entran o salen de la intranet pasan a través del cortafuegos, que examina cada mensaje y bloquea los que no cumplen los criterios de seguridad especificados.

Es importante recordar que un cortafuego no elimina problemas de virus del ordenador, sino que cuando se utiliza conjuntamente con actualizaciones regulares del sistema operativo y un buen software antivirus, añadirá cierta seguridad y protección adicionales para el ordenador o red.

Un ejemplo de implementación de una red protegida podría ser el siguiente esquema:

Figura 37. **Red protegida por 2 *firewall* para la red interna y el área DMZ**



Fuente: elaboración propia, con programa de Visio.

Gracias a estos sistemas una red privada se encuentra protegida contra accesos no autorizados procedentes de internet. Al momento de requerir seguridad en una red corporativa son de gran utilidad es por esto que se analizará el comportamiento como contribuyente de la seguridad en una VPN.

El equipo *firewall* separa la red interna (intranet) de la red pública (internet), monitoreando y filtrando todo el tráfico de internet hacia la red privada y viceversa en un único punto que será considerado como el punto fuerte de la defensa.

Si fuera una red que contara con servidores dedicados (Web, FTP, Correo etc.) como se muestra en la figura anterior, se agrega un cortafuego adicional el cual separa el DMZ (zona desmilitarizada) de la red interna LAN y de la red externa internet.

El *firewall* B permite el tráfico al DMZ y del DMZ hacia afuera. El *firewall* permite el tráfico saliente y entrante desde la red LAN a la internet.

5.2. Filtrado por medio de *firewalls*

Los *firewalls* monitorizan y filtran todo el tráfico, tanto entrante como saliente. En principio existen tres técnica de filtrado y monitorización del tráfico:

- Filtros de paquetes
- Filtros a nivel de aplicación
- Filtros de circuitos

5.2.1. Filtros de paquetes (stateless pakect filtering)

Estos *firewall* se basan en un conjunto de reglas que especifican la acción a tomar dependiendo de las características del paquete analizado:

- IP origen
- IP destino
- Puerto de origen (en paquetes TCP o UDP)
- Puerto de destino (en paquetes TCP o UDP)
- Cabeceras de estado (en paquetes TCP)

Este tipo de *firewall* no almacena un registro de que conexiones han sido establecidas con éxito, debido a esto y al hecho de que las cabeceras TCP/IP de un paquete pueden ser falsificadas estos filtros son susceptibles a *Spoofing* de paquetes.

La autenticación se basa en las direcciones IP, ya que este método posee poca fiabilidad, y no resultaría el más adecuado en los casos en los que el *firewall* tiene que soportar autenticación de clientes externos, pero este problema puede solucionarse si existiese un servidor VPN dentro de la red corporativa o si el *firewall* permitiera filtrado a los paquetes IP entrantes.

5.2.2. Filtros a nivel de aplicación

Estos *firewall* son grandes suites que, además de realizar filtrado de paquetes con control de estado de conexión, incluyen o utilizan software de *proxy* para protocolos específicos.

Este software de *proxy* analiza los paquetes a nivel de contenido y puede, por ejemplo:

- Filtrar contenidos en transferencias HTTP o FTP
- Examinar el tráfico de correo electrónico en busca de SPAM o virus
- Se pueden proteger servicios TELNET y SNMTP
- Navegación por páginas no deseadas

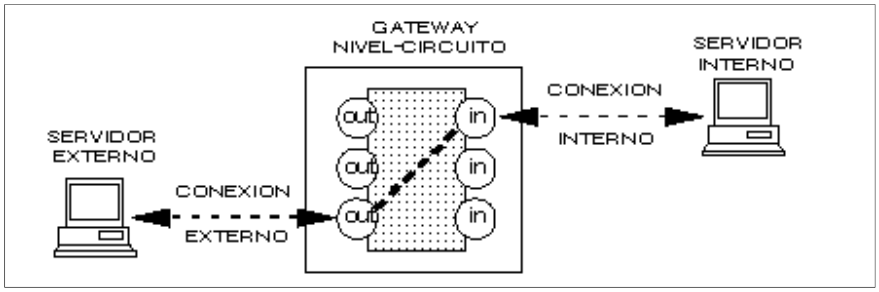
Los filtros de paquetes son demasiado rígidos, difíciles de configurar y las capacidades de registro histórico son muy limitadas. Además el funcionamiento se basa en un sistema todo o nada: el acceso a un servicio en o desde una máquina se permite o no, pero no hay un término medio.

El siguiente paso es usar pasarelas a nivel de aplicación (Gateway o *proxy*): en estos sistemas el usuario no accede directamente al servicio sino un sistema intermedio que realiza las comprobaciones pertinentes, anota la transacción, toma una decisión y si es positiva, actúa de intermediario entre el cliente y el servicio remoto correspondiente, posiblemente controlando la ejecución del protocolo del servicio y tomando notas adicionales.

Para ello se coloca en la máquina puente un tipo especial de servidor (no sólo www, sino también de otros servicios, como por ejemplo: FTP, Gopher, Wais…), denominado *proxy*, que actúa como cliente de los servidores externos a la vez que como servidor de los clientes externos. Así no será necesario que un usuario se conecte a la máquina puente para realizar un FTP al exterior. Simplemente, configurará el cliente de FTP para que emplee el servidor de la máquina puente como *proxy*. A partir de este momento, creerá establecer conexiones con el exterior, cuando en realidad el cliente FTP se estará conectando con el *proxy* y pidiéndole que este establezca una conexión con el exterior para extraer un fichero y luego entregárselo. Es decir, enviará al apoderado a la internet externa ya que él no está autorizado a salir. Lo mismo ocurre con un servicio www. Un cliente interno podría acceder a un servidor corporativo de la intranet y, a la vez, ser incapaz de establecer conexiones con el exterior. Si se instala un servidor *proxy* de www en la máquina puente y se configuran los clientes de la intranet para utilizarlo, estos dirigirán todas las peticiones HTTP (HyperText Transport Protocol) al *proxy* que, a la vez, recuperará por ellos la información del exterior y se la devolverá a ellos.

El usuario tendrá la sensación de conectarse directamente ya que todo el proceso será, para él, transparente.

Figura 38. **Red protegida por 2 *firewall* para la red interna y el área DMZ**



Fuente: http://www.monografias.com/trabajos3/firewalls/firewalls.shtml.
Consulta: 18 de enero de 2014.

En la figura anterior el *firewall* se asegura de identificar el acceso del cliente externo a la aplicación telnet, si este usuario externo no tuviera los permisos necesarios no puede acceder a dicha aplicación hacia el servidor de la red local privada.

5.2.3. Filtros de circuitos (stateful packet filtering)

Además del filtro de paquetes tradicional, este tipo de *firewall* crea y mantiene una tabla donde se registran todas las conexiones establecidas con éxito (es decir, todas aquellas cuyo paso hubiera sido permitido inicialmente por el filtro de paquetes).

Esto significó una mejora en el desempeño al permitir que los paquetes que pertenecen a conexiones ya establecidas y válidas pasen a través del *firewall* sin tener que ser analizados nuevamente y una mayor confiabilidad al

verificar la validez de las conexiones evitando que paquetes con cabeceras falsificadas vulneren la seguridad del entorno que se pretende proteger.

5.3. Equipos VPN con *firewall* integrado

Para los tres tipos de filtrado de los *firewall* mencionados en la sección anterior se necesita realizar configuración a nivel VPN, esto se hace con el objetivo de hacer un sistema de seguridad más confiable. Cualquier equipo *firewall* del mercado puede realizar las siguientes funciones:

- Autenticación: asegura que la persona que intente establecer la conexión de red sea la indicada, luego de esto los equipos aseguran que el envío de mensajes sea con los equipos que deben de ser evitando que haya algún tercero intentando modificar los mensajes. Los *firewall* comprueban la identidad de la comunicación a través de los mensajes y lo hacen periódicamente.

- Integridad de datos: aseguran que la información transmitida no sea modificada a lo largo del camino a esto se le denomina mensajes seguros.

- Privacidad de datos: aseguran que la información no sea leída durante la transmisión ya que los datos viajan encriptados. Esto se realiza utilizando los protocolos VPN para que la información no sea descifrada por terceros.

5.3.1. *Firewall* de seguridad de red Cisco RV220W

Conectividad de alto rendimiento y seguridad para una oficina pequeña: este tipo de *firewall* permite que las oficinas pequeñas disfruten de conectividad de banda ancha, tanto cableada como inalámbrica, de forma segura y confiable a internet, otras oficinas y a los empleados que trabajan remotamente. Este *router* inalámbrico de alto rendimiento ayuda a mejorar la productividad al ofrecer un rápido acceso a archivos de gran tamaño y aplicaciones con elementos multimedia que los empleados utilizan todos los días.

Diseñado para ofrecer una mayor flexibilidad en conexiones remotas altamente seguras, el RV220W admite VPN con seguridad IP (IPsec) y capa de *sockets* seguros (SSL), que a menudo se denomina VPN híbrida. Las VPN con IPsec permiten que otras oficinas se conecten tal como si estuvieran físicamente conectadas a la red de la empresa principal. Las VPN con SSL, que permiten conexiones seguras a través de cualquier navegador, son específicas de la aplicación y ofrecen un medio de extender el acceso controlado de socios comerciales y otras personas, sin poner en riesgo los datos cruciales para ayudar a proteger mejor la red y los datos, Cisco RV220W incluye funciones de seguridad de clase empresarial y el filtrado web opcional basado en la nube. La instalación es simple mediante utilidades y asistentes de configuración basados en el navegador.

Funciones:

- Conexiones Gigabit Ethernet de alto rendimiento, tanto de forma interna como de forma externa, además de un punto de acceso inalámbrico integrado que acelera las transferencias de archivos para mejorar la productividad.

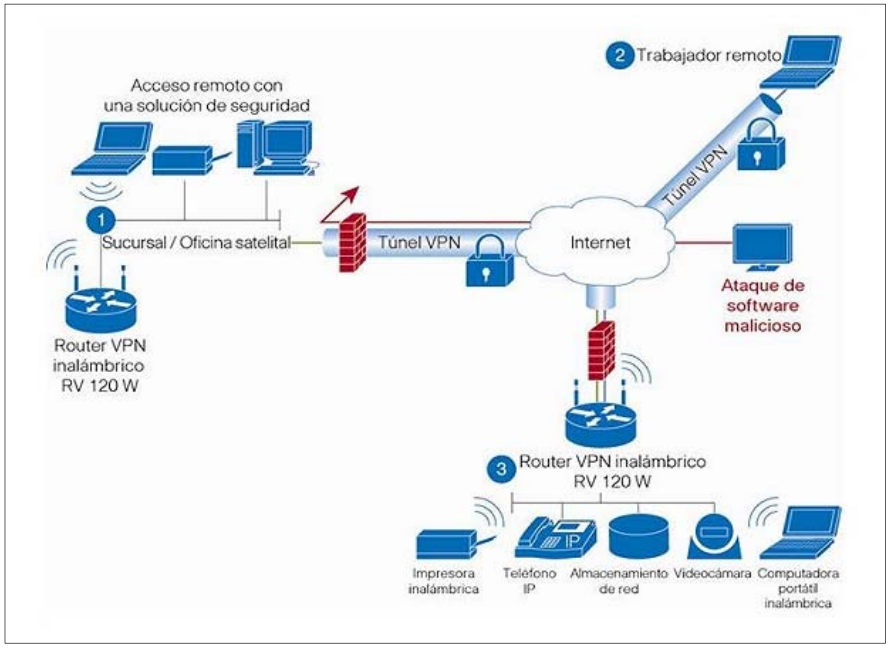
- Switch Gigabit Ethernet 10/100/1000 Mbps de 4 puertos.

- Radio inalámbrica seleccionable de banda doble que ayuda a reducir la interferencia para mejorar el rendimiento inalámbrico.

- Funciones de VPN híbrida (con IPsec y SSL) que permiten un acceso seguro a otras oficinas, empleados que trabajan de forma remota y partners comerciales.

- Administrador de dispositivos intuitivo basado en el navegador con asistentes de instalación que facilita la instalación y el uso.

Figura 39. **Aplicación con *router* VPN RV120 W**



Fuente: *Firewall* de seguridad de red Cisco RV220W. Manual del Router VPN 120 W. Cisco Sytems. p. 3.

5.3.1.1. Características VPN Cisco RV220W

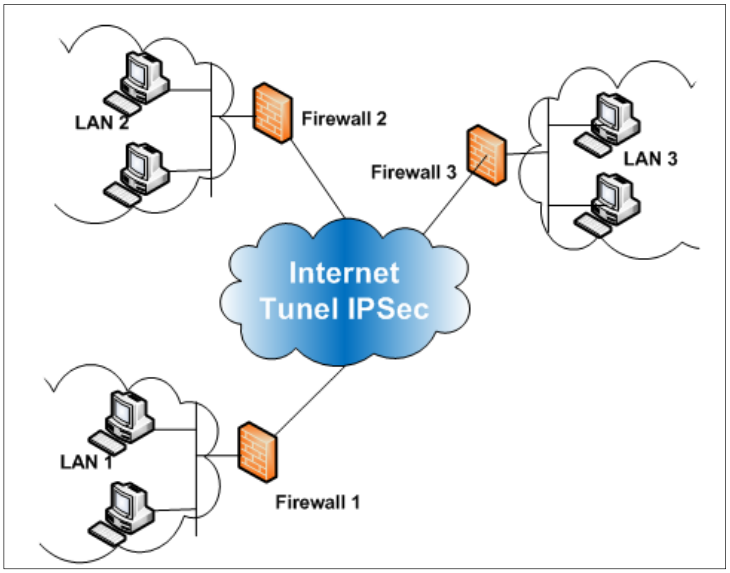
Este tipo de equipos soportan o trabajan con el protocolo de Capa 3 IPSec, esto hace que puedan ofrecer características de seguridad más robustas e implementar protocolos de encriptación de tramas como Diffie Hellman, 3DES, DES etc. También pueden utilizar los algoritmo MD5 y SHA para autenticación además de contar con un servidor RADIUS o TACACS para usuarios remotos.

Tiene la capacidad de crear túneles IPSec, tanto VPN LAN to LAN, como clientes VPN de acceso remoto. Cisco RV220W puede utilizar una base de datos local para autenticar a los usuarios, o para establecer un servidor TACACS externo, para que autentique a los usuarios remotos y que estos deban ingresar usuario y contraseña.

5.3.1.2. Enlace Punto a Punto, Cisco RV220W

Si se deseara llevar a cabo un enlace punto a punto o multipunto, entre sucursales remotas se deberá hacer uso de un *firewall* como por ejemplo el Cisco RV220W estos se deben encontrar en cada uno de los extremos de entrada del medio público. Esto se hace con el objeto de otorgar mayor seguridad tanto al nodo emisor como el receptor.

Figura 40. **Red con políticas de seguridad IPSec / *Firewall***



Fuente: elaboración propia, con programa de Visio.

6. IMPLEMENTACIÓN DE UN ENLACE VPN IPSEC

6.1. Parámetros y configuración del enlace

Toda empresa u organización necesita de una u otra manera intercambiar información con los socios, no importando la distancia y sin comprometer la información. Una red privada virtual site-to-site, proporciona confidencialidad y privacidad para que los datos puedan viajar de manera segura a través de la internet. Algo muy importante es que, implementar este tipo de escenarios, es sumamente rentable para las organizaciones y garantiza la integridad de los datos.

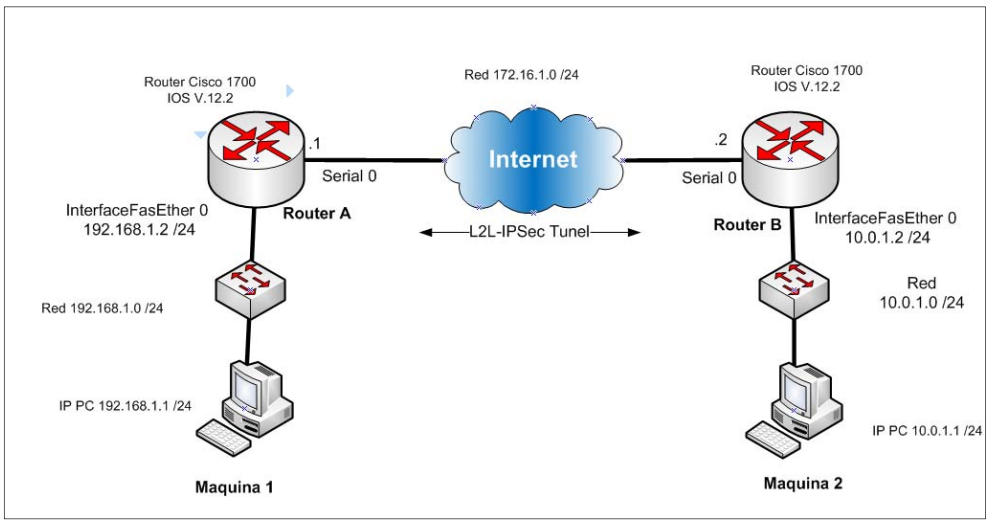
En esta guía se dan las instrucciones paso a paso de cómo implementar una VPN site-to-site utilizando IPSec y *routers* cisco de manera tal que cualquier persona con poca experiencia aproveche esta tecnología sin incurrir en una gran inversión.

Pasos para configurar una VPN IPsec site-to-site utilizando una clave previamente compartida, el escenario se presenta en la figura 40:

- Definir qué parámetros serán utilizados en la fase 1 de IKE (ISAKMP Túnel).
- Definir qué parámetros serán utilizados en la fase 2 de IKE (IPSec Túnel).
- Crear una lista de acceso para identificar el tráfico deseado.
- Crear un *crypto map* y aplicarlo a la interface apropiada.

El escenario que se estará trabajando el siguiente:

Figura 41. **IPSec LAN-to-LAN entre dos computadoras**



Fuente: elaboración propia, con programa de Visio.

6.2. Configuración de *router* A

Este es un *router* cisco 1700 con una versión 12.2 del sistema operativo. Se debe tomar en cuenta que la versión 12.0 del IOS (Internetwork Operating System) no soporta el protocolo IPSec. Se ha decidido trabajar con la versión 12.2 ya que cumple con los fines de este trabajo sin embargo, mientras más reciente sea la versión del IOS, tendrá la capacidad de manejar algoritmos de encriptación más robustos pero a si será la demanda de procesamiento y memoria del dispositivo. Por defecto el *router* 1700 maneja 8 MB de memoria.

Como primer paso se debe establecer una política de ISAKMP, en este caso se utilizará este protocolo para establecer las asociaciones y las claves criptográficas, esto apoya a que la comunicación sea segura.

- Router_A>enable
- Router_A# configure terminal
- Router_A(config)#crypto isakmp policy 1

Luego se fijan los parámetros de una clave previamente compartida. Se utilizará 3DES para la integridad de los datos encriptados. Se hará uso de Diffie-Hellman Group 2, lo que hace este algoritmo es establecer o acordar una clave secreta entre dos máquinas, que se están comunicando a través de un canal inseguro, el resultado de este algoritmo es que proporciona una clave secreta que no puede ser descubierta por un atacante, aunque logre capturar los mensajes. Se configura también un tiempo en segundos de vida *lifetime* que obliga al equipo a autenticar y a generar una nueva clave cada cierto tiempo. Como se vio anteriormente si, se utiliza IPSec entre dos equipos, es obligatorio utilizar un algoritmo de autenticación y en este caso se utilizará el algoritmo SAH1.

- Router_A(config-isakmp)#authentication pre-share
- Router_A(config-isakmp)#hash sha
- Router_A(config-isakmp)#encryption 3des
- Router_A(config-isakmp)# group 2
- Router_A(config-isakmp)# lifetime 86400
- Router_A(config-isakmp)# exit

Se define la clave y con quién o qué interface será validada en este caso es con la interface serial 0 del *router*_B, en esta demostración se utilizó la clave cisco, pero en un entorno de la vida real debe de configurarse una clave más fuerte, utilizando caracteres alfanuméricos.

- Router_A(config)#crypto isakmp key cisco address 172.16.1.2
- Router_A(config)#end

Se establece el conjunto de transformación de cómo se establecerá el túnel IPSec siempre utilizando el algoritmo 3DES para la encriptación.

- Router_A(config)#crypto ipsec transform-set Prueba esp-3des esp-sha-hmac

Luego se define una lista de acceso (ACL) que permita el ingreso de cualquier dispositivo de la red 10.0.1.0 /24 a la red 192.168.1.0.

- Router_A(config)#access-list 101 permit ip 192.168.1.0 0.0.0.255 10.0.1.0 0.0.0.255

Ahora se aplica la correspondencia criptográfica a la interfaz de salida para que los paquetes salgan de forma segura, según los parámetros previamente configurados. El nombre de esta correspondencia es *router*_A_to_*router*_B. También se configura el peer con el que se hará el intercambio de información, en este caso la interface del siguiente salto. Se debe de asociar el tráfico de esta interface con el tráfico restringido por la lista de acceso configurada anteriormente. También debe de asociarle los parámetros configurados en la transformación con nombre prueba al *crypto map* creado.

- Router_A(config)#crypto map router_A_to_router_B 10 ipsec-isakmp
- Router_A(config-crypto-map)# set peer 172.16.1.2
- Router_A(config-crypto-map)# set address 101
- Router_A(config-crypto-map)#set transform-set prueba

Por último se asocia todos los parámetros configurados en la interface serial. No olvidar guardar la configuración con el comando *write*.

- Router_A(config)#interface serial 0
- Router_A(config-if)#crypto map router_A_to_router_B
- Router_A(config-if)#exit
- Router_A# write

6.3. Configuración de *router* B

Tomar en cuenta que la política configurada en el *router*_A debe hacer match con la que se configurará en el *router*_B de lo contrario no se podrá dar la comunicación entre ambos equipos.

- Router_B>enable
- Router_B# configure terminal
- Router_B#(config)#crypto isakmp policy 1
- Router_B(config-isakmp)#authentication pre-share
- Router_B(config-isakmp)#hash sha
- Router_B(config-isakmp)#encryption 3des
- Router_B(config-isakmp)# group 2
- Router_B(config-isakmp)# lifetime 86400
- Router_B(config-isakmp)# exit

Ahora se crea la Clave, como se explicó anteriormente, pero el peer en este caso es la ip de la interface serial en el *router*_A.

- Router_B(config)#crypto isakmp key cisco address 172.16.1.1.1
- Router_B(config)#end

Se define el conjunto de trasformación como se hizo en el *router* A.

- Router_B(config)#crypto ipsec transform-set Prueba esp-3des esp-sha-hmac

De nuevo se crea la lista de acceso, pero tomando en cuenta que el origen es la red 10.0.1.0 y el destino es la IP 192.168.1.0, lo contrario la configuración realizada en el *router*_A

- Router_B(config)#access-list 101 permit ip 10.0.1.0 0.0.0.255 192.168.1.0 0.0.0.255

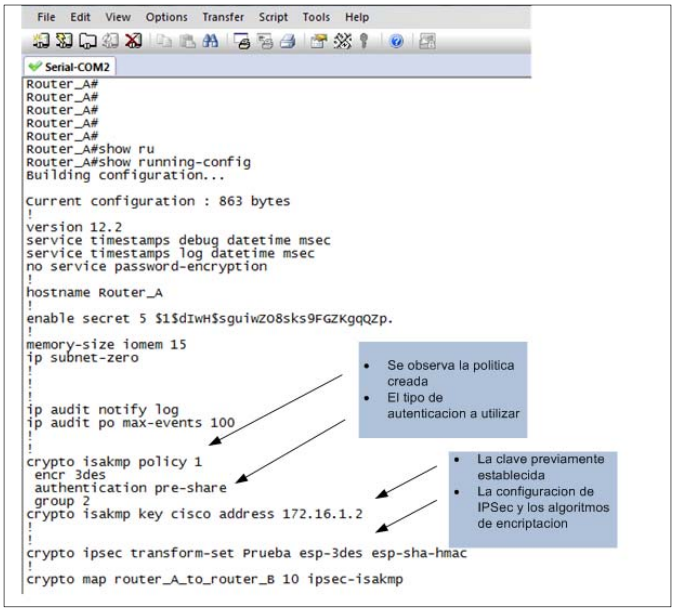
Se crea el *crypto map* y se enlaza a la interface de salida que sería la interface serial 0 del *router*_B.

- Router_B(config)#crypto map router_B_to_Router_A 10 ipsec-isakdmp
- Router_B(config-crypto-map)# set peer 172.16.1.1
- Router_B(config-crypto-map)# set address 101
- Router_B(config-crypto-map)#set transform-set prueba
- Router_B(config-crypto-map)#exit
- Router_B(config)#interface serial 0
- Router_B(config-if)#crypto map router_B_to_router_A
- Router_B(config-if)#exit

6.4. Verificar el funcionamiento del túnel IPSec

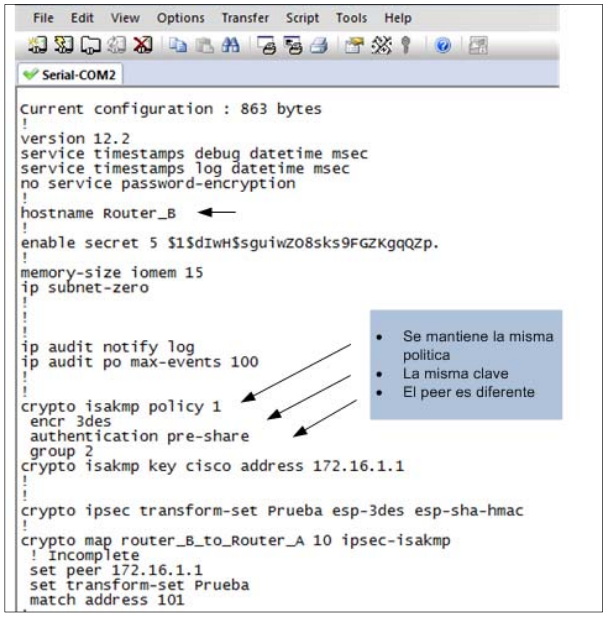
El comando *show crypto session* es de gran utilidad para verificar si ambos equipos lograron establecer sesión. También se podría verificar la conectividad de ambos equipos realizando un PING a uno de ellos y si el PING es exitoso, ambos equipos estarían compartiendo información de forma segura utilizando el protocolo IPSec.

Figura 42. **Configuración activa *router* A**



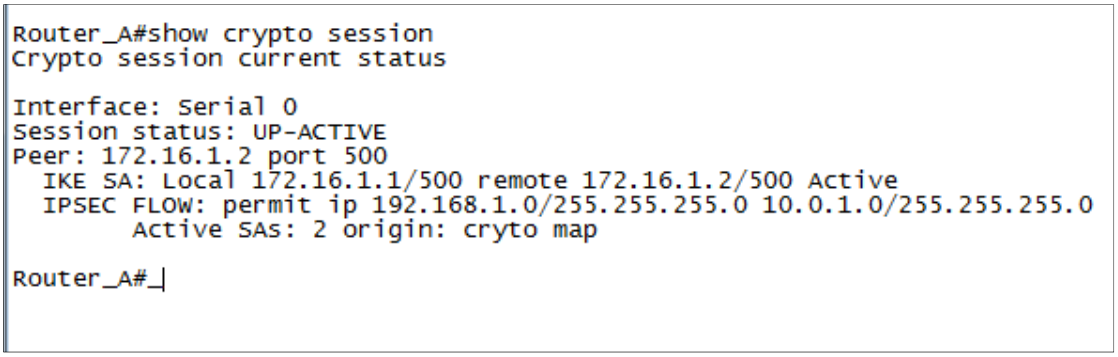
Fuente: elaboración propia, con programa de Vandyke Secure CRT.

Figura 43. **Configuración activa *router* B**



Fuente: elaboración propia, con programa de Vandyke Secure CRT.

Figura 44. **Funcionamiento de la VPN IPSec en 2 equipos**



Fuente: elaboración propia, con programa de Vandyke Secure CRT.

En la figura anterior se puede observar que el estatus de la sesión esta *up active* esto indica que el enlace VPN está activo y listo para compartir o enviar información entre ambos equipos. El comando utilizado reconoce la IP de la interface o equipo con el que se está comunicando, en este caso, la interface serial 0 del *router*_A se está comunicando hacia la IP 172. 16.1.2. Cabe mencionar que también despliega la redes que únicamente tendrán comunicación entre ellas en este caso, son la redes 192.168.1.0 /24 y la red 10.0.1.0 /24. Esta regla fue creada cuando se configuró la lista de acceso. Sin embargo, esto no garantiza que una persona no autorizada capture los paquetes mientras viajan a través de internet, como se mencionó anteriormente es un medio público y es aquí en donde entra en juego el protocolo IPSec ya que como se ha visto a lo largo de este trabajo utiliza diferentes técnicas de encriptación, de autenticación y de negociación.

CONCLUSIONES

1. Los beneficios de una red privada virtual son bastante convenientes para una compañía ya que reducen los costos significativamente, los mecanismos de seguridad son altos y es de alta escalabilidad, esto se debe a que se utiliza una infraestructura pública.

2. Parte importante de un enlace VPN no importando el modo de operación, es el túnel que se crea en ambos extremos de la conexión, es este el que transforma de forma segura las tramas que son enviadas en el medio de transmisión para que no puedan ser interceptadas.

3. Los protocolos de capa de enlace dados son los que establecen la conexión del enlace VPN e indican cuando inicia y cuando finaliza. Estos hacen posible los métodos de autenticación como PAP, CHAP, MS-CHAP.

4. Parte fundamental de la seguridad que brinda IPSec es que trabaja con el algoritmo Internet Key Exchange (IKE), que en conjunto permite que un usuario pueda comunicarse con otro, usando un cifrado y autenticación de alto nivel. Es por eso que se considera a IPSec el protocolo más seguro para implementar enlaces VPN.

5. El *firewall* brinda seguridad extra a la información que entra e ingresa a la red local de la compañía, asimismo controla el acceso de usuarios a la red.

6. Configurar una lista de acceso en un enlace VPN restringe la comunicación solo a un grupo de usuarios y refuerza aún más la seguridad.

RECOMENDACIONES

1. Es importante que, antes de implementar un enlace VPN, se conozca el ancho de banda que se tiene contratado con el proveedor de servicios de internet, de lo contrario la transferencia de información será lenta, independientemente de la capacidad de los equipos que se tenga en las oficinas.

2. IPSec puede utilizar diferentes protocolos para administrar las claves como por ejemplo DES, 3DES e IKE. Pero se debe tomar en cuenta que para este tipo de enlaces el más seguro es IKE.

3. Es importante recordar que un *firewall* no elimina problemas de virus del ordenador, pero si se utiliza en conjunto con actualizaciones regulares del sistema operativo y un buen software de antivirus, añadirá cierta seguridad y protección adicional para el ordenador de la red.

4. Cuando se implemente una configuración VPN IPSec con *routers* cisco, se debe tomar en cuenta la versión del sistema operativo que maneja el *router* ya que de esta dependerá los protocolos y algoritmos de encriptamientos que se manejaran en el equipo.

BIBLIOGRAFÍA

1. *Asociación de Seguridad* [en línea] http://spi1.nisu.org/recop/al02/peraltaspi/node3.html [Consulta: 20 de febrero de 2014].

2. *Blog sobre redes* [en línea] [ref. 23 de julio de 2006] http://blog.internexo.com/2006/07/vpn-redes-virtuales-privadas.html [Consulta: 8 de diciembre de 2013].

3. CONTRERAS VEGA, Gerardo. *Introducción a la seguridad en Internet y Aplicaciones*. México: Thompson 2004. 231 p.

4. *Concepto de VPN* [en línea] http://www.ehowenespanol.com/vpn-sobre_132952/ [Consulta: 20 de octubre de 2013].

5. *Conexión PPP* [en línea] http://juandeg.tripo.com/pp.htm [Consulta: 18 de enero de 2014].

6. *Cifrado DES* [en línea] http://es.kioskea.net/contents/130-introduccion-al-cifrado-mediante-des [Consulta: 10 de febrero de 2014].

7. *Certificados Digitales* [en línea] : https://www.cert.fnmt.es/curso-de-criptografia/certificados-digitales [Consulta: 18 de marzo de 2014].

8. *Encriptación* [en línea] http://carlosvazquez10.blogspot.com/2014/04/ encriptacion-metodos-paso- por.html [Consulta: 4 de febrero de 2014].

9. *Ecured* [en línea] http://www.ecured.cu/index.php/Cifrado [Consulta: 5 de febrero de 2014].

10. GONZALES MORALES, Alexandro. *Redes privadas virtuales*. México: Limusa Noriega. 2006. 100 p.

11. *Intercambio de claves en internet* [en línea] [ref. 2 de enero de 2010] Disponible en web: http://www.redeszone.net/ [Consulta: 3 de marzo de 2014].

12. MANUEL, Jose. *Criptografía y seguridad en computadores*. 3a ed. México: Thompson 2001. 220 p.

13. *Mastermaganize* [en línea] http://www.mastermagazine.info/termino /7160.php[Consulta: 16 octubre de 2013].

14. *Protocolo Punto a Punto* [en línea] http://msdn.microsoft.com/es-es/library/cc738840(v=ws.10).aspx
[Consulta: 13 enero de 2014].

15. PÉREZ IGLESIAS, Santiago. *Análisis del protocolo IPSec*. México: Grijalva River 2001. 140 p.

16. *Point to Point Protocol* [en línea] [ref. 18 de noviembre de 2013] Disponible en web: http://es.wikipedia.org/wiki/Point-to-Point_Protocol [Consulta: 16 de enero de 2014].

17. *Protocolo PPP* [en línea] http://txdedatoscapi.tripod.com/protocolo_ppp.htm [Consulta: 20 de enero de 2014].

18. *Red Privada Virtual* [en línea] http://es.wikipedia.org/wiki/Red_privada_virtual [Consulta: 18 octubre de 2013].

19. PIEPRZYK, Josef. *Cryptography an introduction to computer security*. Australia: Prentice Hall 1989. 544 p.

20. BROWN, Steven. *Implementación de redes privadas virtuales*. México: McGraw-Hill 2001. 595 p.

21. *Todo sobre redes* [en línea] http://redesprivadasvirtuales-vpn.blogspot.com/ [Consulta: de diciembre de 2013].

22. *VPN* [en línea] [ref. 6 de junio 2006] Disponible en web: http://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/14144-static.html [Consulta: 18 de diciembre de 2013].

ANEXOS

Anexo 1: Especificaciones del producto Cisco RV220W Security Firewall

WAN/DMZ	
10/100/1000 Mbps Gigabit Ethernet	1-port
DMZ	Software-based
LAN	
10/100/1000 Mbps Gigabit Ethernet	4-port switch
VLAN support	Yes
Wireless	
High-Speed 802.11n	Yes
802.11b/g compatibility	Yes
Multiple SSID's	4
Routing & Network	
IP and MAC filtering	Yes
Port forwarding and triggering	Yes
IPv6	Yes
RIP v1/RIP v2	Yes/Yes
Inter- VLAN routing	Yes
Quality of Service (QoS)	Yes
Security & VPN	
SPI firewall	Yes
DES/3DES/AES	Yes/Yes/Yes
Site-Site/QuickVPN/SSL connections	25/25/5
Content/URL filtering	Yes
Web threat protection Optional Cisco ProtectLink Web service	Optional Cisco ProtectLink Web service
Management	
Browser based configuration (HTTP/HTTPS)	Yes
SNMP	v1, v2c, and v3

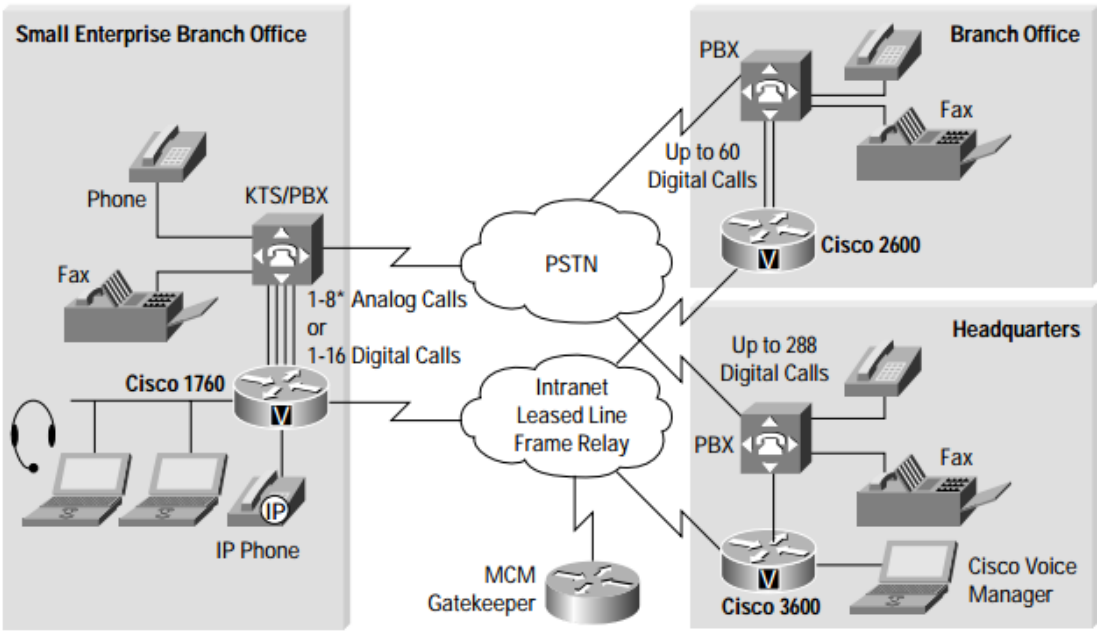
Fuente: Cisco y afiliados. Especificaciones Cisco RV220W Security *Firewall*. p. 2.

Anexo 2: Características *Router* Cisco Series 1700

Benefits	Features
Flexibility and investment protection	• Offers modular data and voice slots (except Cisco 1701, 1711, 1712) • Provides customization through a wide range of WAN and voice interface cards (except Cisco 1701, 1711, 1712) • Presents migration path to multiservice voice and data integration (Cisco 1751 and 1760)
Security	• Offers Cisco IOS® stateful inspection firewall • Provides VPN IP Security (IPSec) encryption (Digital Encryption Standard [DES] and Triple DES [3DES]) • Enables encryption up to T1/E1 speeds (4-Mbps full duplex) using optional VPN module (included in Cisco 1711 and 1712—optional for the other Cisco 1700 Series models)
Business-class DSL	• Supports ADSL and G.shdsl • Offers enhanced quality of service (QoS) over DSL • Offers toll-quality voice over DSL
Multiservice data and voice integration (Cisco 1751 and 1760)	• Provides support for analog and digital voice calls • Supports IP telephony • Interoperates with next-generation voice-enabled business applications such as integrated messaging and Web-based call centers • Works with existing telephone infrastructure: phones, fax machines, key telephone system (KTS) units, and private branch exchanges (PBXs) (including digital PBXs)
Remote Manageability	• Supports CiscoWorks management applications • Enables QoS and traffic prioritization through Cisco IOS Software

Fuente: Cisco y afiliados. *Especificaciones Cisco 1700*. p. 2.

Anexo 3: Integración de multiservicios con *Router* Cisco 1700



Fuente: Cisco y afiliados. *Especificaciones Cisco 1700*. p. 7.