UNIVERSIDAD DE QUINTANA ROO
DIVISIÓN DE CIENCIAS E INGENIERÍA

Implementación de una red privada virtual para la empresa Max Computación

TESIS
Para obtener el grado de
Ingeniero en Redes

PRESENTA
Ángel Flores de la Rosa

DIRECTOR DE TESIS
MTI. Vladimir Veniamin Cabañas Victoria

ASESORES
MSI. Laura Yésica Dávalos Castilla
MTI. Melissa Blanqueto Estrada
Dr. Freddy I. Chan Puc
Dr. Homero Toral Cruz

Chetumal Quintana Roo, México, diciembre de 2013

UNIVERSIDAD DE QUINTANA ROO
DIVISIÓN DE CIENCIAS E INGENIERÍA

Trabajo de Tesis elaborado bajo supervisión del Comité de asesoría

y aprobada como requisito parcial para obtener el grado de:

INGENIERO EN REDES

Comité de Trabajo de Tesis

Director: _____

MTI. Vladimir Veniamin Cabañas Victoria

Asesora: _____

MSI. Laura Yésica Dávalos Castilla

Asesora: _____

MTI. Melissa Blanqueto Estrada

Chetumal, Quintana Roo, México, Diciembre de 2013.

AGRADECIMIENTOS

Este espacio quiero dedicarlo a las personas más importantes en mi vida como mi padre, quien siempre me ha apoyado en todos los aspectos, regalándome lo más valioso que tengo hasta el momento: su amistad. De la misma forma debo agradecer a mi madre, quien hasta el sol de hoy sigue preocupándose por el bienestar de toda la familia, tratando en todo momento de mantenernos unidos. Asimismo, considero esencial mencionar en este espacio a mi hermano Rodrigo, siempre al pendiente de lo que pudiera necesitar en lo académico, laboral y más que nada en lo personal.

A los profesores Ezequiel Hernández, Rubén González, Javier Vázquez, Melissa Blanqueto, Laura Dávalos, Jaime Ortegón y Vladimir Cabañas, quiero agradecerles su empeño y dedicación en cada clase impartida, ya que durante mi estadía en esta Universidad no solo aprendí sobre asignaturas divisionales, generales y profesionales, sino también sobre importantes lecciones de vida, que estoy seguro servirán en todo momento de mi existencia.

Así mismo quiero agradecer a aquellos compañeros, quienes a lo largo de mi formación universitaria tuve la oportunidad de conocer, trabajar con ellos y hacerme su amigo, entre ellos se encuentran: Freddie Balam, Jesús Medina, Kareem Young, Jeff Bardales, Angélica González, César Rosado, Yobana Gamboa, Karla Meléndez, Carlos Noverola, Erick Domínguez, Hugo Bastián y Nelsy Cámara.

Igualmente considero de vital importancia agradecer a los señores Ricardo Marín y Sergio Ruiz por brindarme la oportunidad de laborar con ellos en el Instituto del Patrimonio Estatal, donde empecé mi camino profesional y conocí a personas muy agradables como Miguel Heredia y Diego Uch.

Por último y no menos importante, agradezco a todo el personal de la Universidad de Quintana Roo porque con su valioso trabajo contribuyen a formar día con día profesionales de calidad y personas con altos valores morales.

DEDICATORIA

El presente trabajo va dedicado con profundo cariño, respeto y admiración a mis padres Luis Ignacio Flores Morales e Imelda De la Rosa Uc.

RESUMEN

Las formas de comunicación en una organización son una necesidad primordial a nivel mundial y han sufrido cambios a medida que crece la tecnología. Por este motivo surgen las redes organizacionales donde los equipos de cómputo realizan diferentes operaciones e intercambio de datos, esto último ha requerido contar con normas de seguridad para no sufrir modificaciones o pérdidas de información.

Cuando se realizan enlaces punto a punto sobre un medio público las empresas necesitan resguardar de una mejor forma su información para transportarla. Debido a esto y luego de costosos modelos de transporte físico nacen las redes privadas virtuales (VPN), que básicamente realizan túneles seguros a través de una plataforma pública como Internet. Estos túneles virtuales son creados por conjuntos de protocolos especializados que garantizan que la información transmitida no ha sido leída, alterada o dañada y que las partes que intervienen en la conexión sean quienes dicen ser.

El presente trabajo analiza las diferentes formas que hacen posible crear túneles a través de estos medios considerados como poco seguros para quien necesite que sus datos no sean dañados, leídos o eliminados. El estudio abarca tanto los modelos como la estructura que adopta la información al momento de considerarse lista para viajar por el medio inseguro. Se da especial énfasis en este documento al protocolo de seguridad sobre IP llamado IPSec, el cual es un estándar de seguridad que han adoptado la mayoría de los fabricantes de software y hardware para VPN y que reúne la mayoría de las características que hacen de las redes privadas virtuales modelos de comunicación seguros sobre un medio masivo como es Internet.

Finalmente se aborda un caso de estudio, en el cual se ha implementado una VPN a nivel empresarial.

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

CAPÍTULO I

INTRODUCCIÓN A LAS VPN

"Desde el principio no pensábamos en otra cosa que no fuera tener éxito."

Bill Gates

1.1 Introducción

Hasta no hace mucho tiempo las sucursales de una empresa podían tener una red local que operara aislada de las demás. Cada una de estas redes locales tenía su esquema de nombres, su sistema de correo electrónico, e inclusive usaban protocolos que diferían de los usados en otras sucursales. Es decir, en cada lugar existía una configuración totalmente local, que no necesariamente era compatible con las demás configuraciones de otras áreas dentro de la misma empresa.

A medida que la computadora fue incorporada a las empresas, surgió la necesidad de comunicar las diferentes redes locales para compartir recursos internos. Para cumplir este objetivo, debía establecerse un medio físico para la comunicación. Este medio fueron las líneas telefónicas, con la ventaja de que la disponibilidad es muy alta y se garantiza la privacidad. El gran inconveniente del uso de las líneas telefónicas es su alto costo, ya que las empresas de telefonía suelen cobrar un abono mensual más una tarifa por el uso, en el que se tienen en cuenta la duración de las llamadas y la distancia. Si la empresa tiene sucursales dentro del mismo país pero en distintas áreas telefónicas y además tiene sucursales en otros países, los costos telefónicos pueden llegar a ser muy altos. Adicionalmente, si los usuarios móviles deben conectarse a la red corporativa y no se encuentran dentro del área de la empresa, deben realizar llamadas de larga distancia, con lo que los costos se incrementan aún más.

Con la llegada y popularización de Internet, las compañías tienen la posibilidad de crear enlaces virtuales que demandan una inversión relativamente pequeña de hardware, debido a que utilizan la infraestructura ya establecida como publica para la conexión entre los puntos y usuarios de la red. A estos tipos de enlaces se les conoce como Redes Privadas Virtuales (VPN), y muchas empresas comienzan a utilizarlo, ya sea para interconectar subredes o trabajadores distantes.

Se ha demostrado en la actualidad que las VPN reducen en tiempo y dinero los gastos de las empresas, eso ha significado una gran ventaja para las organizaciones, sobre todo las que cuentan con oficinas remotas a varios

kilómetros de distancia, pero también es cierto que estas formas de comunicación remotas han despertado la curiosidad de algunas personas que se dedican a atacar las redes empresariales y los servidores ahí contendidos para obtener información confidencial.

En la actualidad existen dispositivos especiales y software que otorgan niveles de seguridad esenciales para realizar enlaces remotos entre oficinas de la misma empresa, sin necesidad de recurrir a costosas líneas dedicadas.

En este trabajo de titulación se analizarán configuraciones VPN, aspectos técnicos a nivel protocolar del montaje en enlaces VPN, así como los aspectos más importantes a nivel seguridad que se incluyen en los protocolos utilizados para implementar Redes Privadas Virtuales.

1.2 Objetivo General

Realizar un análisis de las diferentes opciones de comunicación más confiables a través de una red pública e implementar una solución de transmisión segura punto a punto en una empresa.

1.3 Objetivos Específicos

- Analizar el funcionamiento estructural de las VPN.
- Identificar métodos de seguridad de transporte y control de acceso en medios de difusión pública como Internet.
- Implementar una VPN sitio a sitio basada en el protocolo IPSec.

1.4 Justificación

Las Redes Privadas Virtuales se han convertido en una de las tecnologías más implementadas hoy en día. Las principales razones de este éxito son el uso de algoritmos de seguridad muy confiables y la reducción de costos en las comunicaciones entre oficinas remotas, trabajadores a distancia, clientes y en muchas ocasiones hasta proveedores.

CAPÍTULO II

REDES PRIVADAS VIRTUALES (VPN)

"El trabajo bien hecho no es solo una responsabilidad con la sociedad, es también una necesidad emocional."

Carlos Slim

2.1 Concepto de VPN

Por sus siglas en inglés, VPN hace referencia a Red Privada Virtual (Virtual Private Network) que básicamente es una tecnología que permite una extensión de la red local sobre una red pública o no controlada como es Internet. Para hacer esto posible de manera segura es necesario integrar los medios para garantizar la autenticación, integridad y confidencialidad de toda la información que sea transmitida.

A continuación se realiza un análisis desde lo más básico del concepto VPN.

2.1.1 Red

Hoy en día las redes y en general el uso de computadoras en las organizaciones, empresas o industrias se ha incorporado de una manera creciente y constituyen una parte importante de la producción. Una red de computadoras o red de datos es un conjunto de equipos (computadoras y dispositivos principalmente) conectados por medio de cables, señales, ondas o cualquier otro medio de transporte de datos, con el fin de compartir información, recursos y servicios principalmente. Para simplificar la comunicación entre los equipos, se definió el Modelo OSI (Open System Interconnection) o modelo de interconexión de sistemas abiertos, el cual especifica 7 distintas capas de abstracción. Con ello, cada capa desarrolla una función específica con un alcance definido.

Es importante mencionar que una red no solo la componen equipos de cómputo, también existen dispositivos conectados al conjunto que cumplen roles diversos en el sistema, por ejemplo: servidores, conmutadores (switches), enrutadores (routers), gateways, cortafuegos (firewalls), etc. Los cuales se incorporan de acuerdo a las necesidades, tamaño y topología de la red. A continuación se puede apreciar en la imagen un modelo de red bastante sencillo:

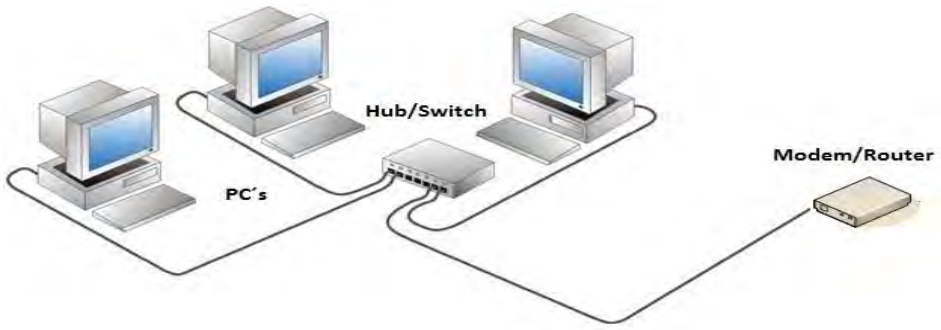

Figura 1 Estructura Básica de una red local (Elaboración propia)

2.1.2 Red Privada

Una red privada se establece luego de presentarse la necesidad de resguardar la información, es decir, existen empresas u organizaciones que deben transmitir sus datos de forma confidencial. Las redes corporativas que manejan tanto antecedentes de fondos como bases de datos tienen carácter de privadas ya que funcionan con una arquitectura cerrada y para terceros es difícil acceder.

Esto se logra con equipos diseñados para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones seguras. Se trata de un dispositivo o conjunto de dispositivos configurados para permitir, limitar, cifrar y descifrar el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios.

2.1.3 Red Privada Virtual

Una Red Privada Virtual (VPN) es una estructura de red la cual tiene capacidad de establecer un canal de comunicación privado sobre una infraestructura de red pública. Entonces, a través de una VPN es posible establecer comunicaciones vía infraestructura pública entre dos estaciones de trabajo remotas, todo sin correr el riesgo que terceras personas ajenas a la organización puedan acceder a dicha información ni al sistema de interconexión (Ver Figura 1).

Esta tecnología permite crear un túnel de encriptación a través de Internet u otra red pública de tal forma que permita a los usuarios que se encuentran en los

extremos del túnel disfrutar de la seguridad, privacidad y funciones que antes estaban disponibles en redes privadas.

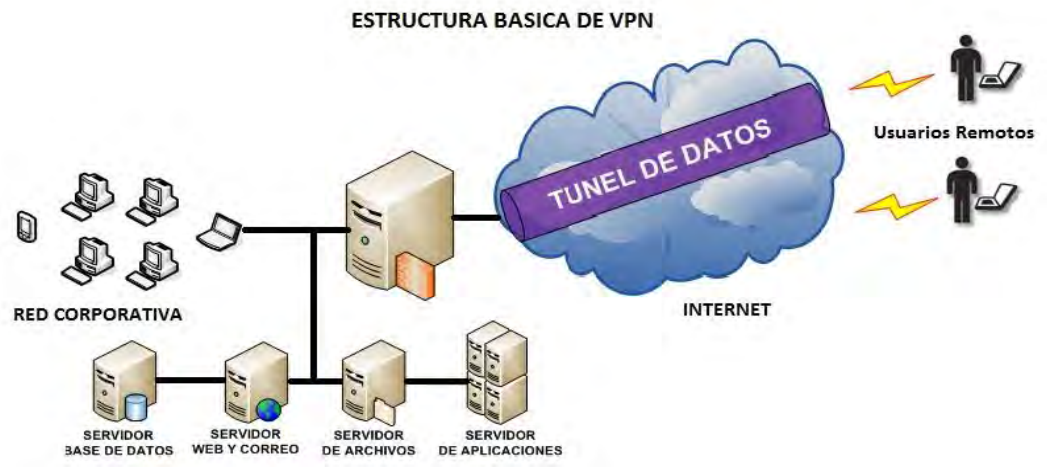

Figura 2 Estructura de una red privada virtual (Elaboración propia)

2.2 Tipos de VPN

En lugar de utilizar una conexión dedicada contratada a una compañía telefónica, una VPN usa conexiones virtuales, encapsuladas por Internet desde la red origen hasta el lugar remoto. Actualmente existen tres tipos de VPN:

2.2.1 Sistemas Basados en Hardware

Las VPN basadas en hardware utilizan básicamente equipos dedicados como por ejemplo los routers, son seguros y fáciles de usar, ofreciendo gran rendimiento ya que todos los procesos están dedicados al funcionamiento de la red a diferencia de un sistema operativo el cual utiliza muchos recursos del procesador para brindar otros servicios. En síntesis, los equipos dedicados son de fácil implementación y buen rendimiento, solo que las desventajas que tienen son su alto costo y que poseen sistemas operativos propios y a veces también protocolos que son propietarios del fabricante del equipo.

2.2.2 Sistemas Basados en Firewall o Cortafuegos

Estos sistemas aprovechan las ventajas que un Firewall puede proveer como los mecanismos de seguridad, incluyendo el acceso restringido a la red interna.

También realizan NAT o traducción de direcciones con lo que satisfacen completamente los requerimientos de seguridad. Muchos de los cortafuegos comerciales, aumentan la protección, quitando al núcleo del Sistema Operativo algunos servicios peligrosos que llevan estos de serie, y les provee de medidas de seguridad adicionales, que son mucho más útiles para los servicios de VPN. El rendimiento en este tipo decrece, ya que no se tiene hardware especializado para cifrado.

2.2.3 Sistemas Basados en Software

Estos sistemas son ideales para las situaciones donde los dos puntos de conexión de la VPN no están controlados por la misma organización, o cuando los diferentes cortafuegos o routers no son implementados por la misma organización. Este tipo de VPN's ofrecen el método más flexible en cuanto al manejo de tráfico, ya que la información puede ser enviada a través de un túnel, en función de las direcciones o protocolos.

2.3 Usos Comunes de las VPN

Existen objetivos específicos para la implementación de una VPN, esto es requerido principalmente cuando se produce el crecimiento de la organización o el desarrollo en distintas plazas, también cuando algún elemento humano es representante de la empresa en algún lugar remoto y necesite adquirir información de la red corporativa, además los mismos clientes de la organización necesitaran acceder a bases de datos de la empresa para realizar algún tipo de transacción o trámite, por estos motivo se pueden clasificar los siguientes usos de las VPN:

2.3.1 Acceso Remoto a Usuarios Sobre Internet

Este tipo de conexión se establece cuando uno o más usuarios de la red corporativa se encuentran realizando un trabajo geográficamente lejos o algún cliente de la empresa necesita obtener datos en forma remota de los sistemas corporativos para futuras transacciones. Luego de la previa configuración VPN del

equipo remoto que va a ser conectado a la red corporativa, se debe adquirir un servicio de Internet al ISP (Proveedor de Servicios de Internet) local. Utilizando la infraestructura de Internet se realiza un túnel de comunicación entre el equipo remoto y el servidor VPN de la organización de manera confiable donde se puede asegurar que los datos serán tan confidenciales como si se tratase de un enlace dedicado. De esta manera en lugar de hacer una llamada de larga distancia (o a un 01-800) a un servidor de acceso de red (NAS) corporativo o externo, únicamente se hace una llamada local al ISP para tener acceso a Internet.

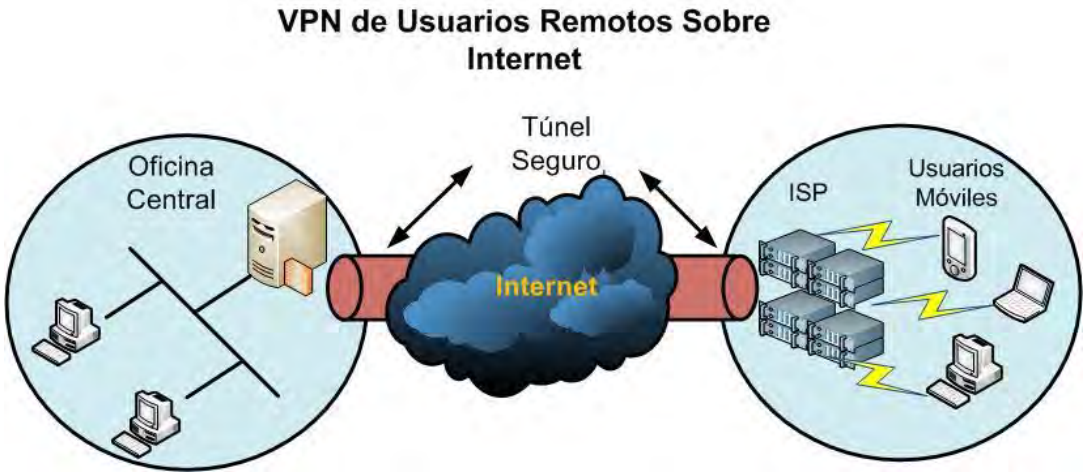

Figura 3 Acceso remoto a usuarios sobre internet (Elaboración propia)

2.3.2 Conexión de Redes sobre Internet

También conocida como “Sitio-Sitio”, es el caso en que dos o más oficinas de una misma organización con infraestructuras de red bastantes robustas como para soportar varios equipos de cómputo creando redes corporativas requieren comunicarse remotamente mediante alguna red pública. En este esquema el servidor VPN de la oficina central, que posee un vínculo permanente a Internet, acepta las conexiones vía Internet provenientes de los sitios y establece el túnel VPN. Los servidores de las sucursales se conectan a Internet utilizando los servicios de su ISP, típicamente mediante conexiones de banda ancha. Esto permite eliminar los costosos enlaces dedicados, sobre todo en las comunicaciones internacionales.

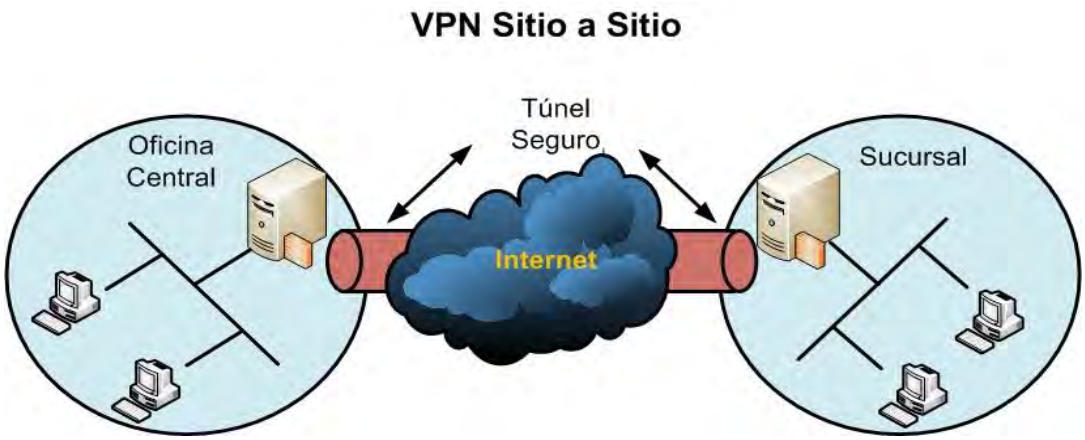

Figura 4 Conexión de redes sobre internet (Elaboración propia)

2.3.3 Conexión de Usuarios Sobre una Intranet

En algunas redes corporativas, los datos departamentales son tan sensibles que el departamento entero es desconectado físicamente del resto de la red local. Si bien esto garantiza la confidencialidad del de la información que maneja el departamento, crea problemas de accesibilidad a la información para otros usuarios que están fuera de esa área de trabajo. Este tipo de configuración permite que el departamento completo esté físicamente conectado a la intranet corporativa, pero separada por un servidor VPN. Es importante mencionar que este servidor VPN no debe actuar como enrutador entre la Intranet y la red departamental.

Al utilizar VPN para conectar ambos extremos de la Intranet, el administrador de la red puede garantizar que únicamente los usuarios que tienen los permisos adecuados (basados en políticas de la empresa u organización) puedan establecer comunicación con el departamento protegido. Adicionalmente, todas las comunicaciones que pasen por la VPN pueden cifrarse para efectos de confidencialidad de información.

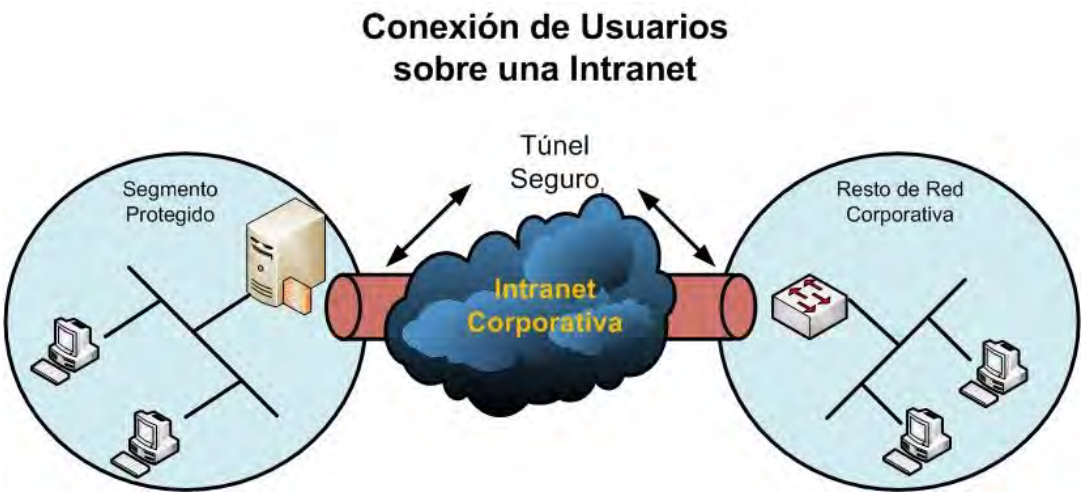

Figura 5 Conexión de usuarios sobre una intranet (Elaboración propia)

Algunas de las ventajas que ofrece trabajar con VPN dentro de la Intranet corporativa son:

- **Implementación transparente a las aplicaciones**: Una vez configurado mediante un simple cambio de rutas, todo el tráfico es automáticamente cifrado y validado sin necesidad de alguna modificación en la forma de operar de la red local.
- **Alta seguridad**: Al cifrar los datos y las direcciones destino se evita que terceras personas tengan a acceso a la información confidencial de la empresa.
- **Distintos niveles de seguridad**: Según sea necesario, es posible operar con contraseñas configuradas durante la implementación o incluso certificados para firmas digitales con autenticación en los extremos.

2.4 Requerimientos Básicos para Establecer una VPN

Típicamente, al implementar una solución de red remota, una empresa desea facilitar el acceso controlado a los recursos y a la información dentro de la red local, por lo que la solución debe permitir la libertad para que usuarios remotos autorizados se conecten fácilmente a los recursos corporativos de la Red de Área Local (LAN). También deberá permitir que las oficinas remotas se conecten entre

sí para compartir recursos e información (Conexiones sitio a sitio). Finalmente la solución debe garantizar la privacidad y la integridad de los datos al viajar a través del medio.

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**: La solución debe verificar la identidad del usuario que realiza la conexión y restringir el acceso de la VPN a usuarios no autorizados. Además, la solución deberá proporcionar registros de auditoría y contables para mostrar quién accedió a que información y cuando.
- **Administración de dirección**: La solución debe asignar una dirección al cliente en la red privada, asegurándose que las direcciones privadas se mantengan así.
- **Encriptación de datos**: Los datos que viajan en una red pública no podrán ser leídos por clientes no autorizados en la red.
- **Administración de llaves**: La solución debe generar y renovar llaves de cifrado tanto para el cliente como para el servidor.
- **Soporte de protocolo múltiple**: La solución debe poder manejar protocolos comunes utilizados en las redes públicas, incluyendo al protocolo de internet (IP), (IPX), etc.

Una solución VPN basada en protocolo de túnel punto a punto (PPTP) o protocolo de túnel de Nivel 2 (L2TP) cumple con todos estos requerimientos básicos y aprovecha la amplia disponibilidad de internet a nivel mundial. Otras soluciones, incluyendo el protocolo de seguridad IP (IPSec), cumplen con algunos de estos requerimientos y siguen siendo útiles para situaciones específicas.

2.5 Ventajas de las VPN

El uso de las VPN como solución para conectar usuarios remotos, oficinas distantes o departamentos confidenciales en la empresa, presenta varias ventajas notables:

- **Reducción de Costos**: Para una implementación de red que abarque empresas distantes geográficamente ya no será indispensable (en términos de seguridad) realizar conexiones mediante enlaces dedicados de muy altos costos que caracterizaron a muchas empresas privadas, siendo remplazadas en su gran mayoría por ADSL (Línea de Suscripción Digital Asimétrica), que combina ancho de banda a bajo costo, disponible por lo general en la mayoría de las zonas urbanas. También los usuarios remotos obtienen grandes beneficios ya que no necesitan hacer llamadas de larga distancia a la empresa, con la incorporación de ADSL basta con conectarse a internet para enlazarse a través de VPN a los recursos de red en la empresa.
- **Seguridad**: Las Redes Privadas Virtuales utilizan estándares de seguridad para la transmisión de datos, dando como resultado conexiones seguras equivalentes a enlaces dedicados. Protocolos como 3DES (Triple Encriptación de Datos Estándar), el cual cumple la función de cifrar la información a transferir y el protocolo de seguridad IPSec para manejo de los túneles mediante software, brindan un alto nivel de seguridad al sistema.
- **Escalabilidad**: Para agregar usuarios a la red no es preciso realizar inversiones adicionales ya que la provisión de servicios se hace con dispositivos y equipos fáciles de configurar y manejar. Se utiliza la infraestructura ya establecida de Internet por lo que agregar usuarios no significa una gran inversión monetaria y de tiempo.
- **Compatibilidad con tecnologías de banda ancha**: Una VPN puede aprovechar la infraestructura existente de banda ancha (por ejemplo ADSL) lo que implica un alto grado de flexibilidad y reducción de costos al

momento de configurar. Incluso es posible utilizar Voz sobre IP de acuerdo al ancho de banda de la conexión, reduciendo los costos por concepto de telefonía.

- **Mayor productividad**: Debido a un mejor nivel de acceso durante mayor tiempo es posible probar que la productividad de los usuarios de la red aumentará.

CAPÍTULO III

PROTOCOLOS VPN

“Se un prototipo de calidad, mucha gente no está acostumbrada a un ambiente donde se espera la excelencia.”

Steve Jobs

3.1 Concepto de Protocolo

Se entiende por protocolo de comunicación de redes la serie de lineamientos cuya función específica es controlar el intercambio ordenado de datos en una red informática, suministrando diversas características y funciones específicas como la corrección de errores. En forma simple, un protocolo puede definirse como la serie de reglas que permiten y controlan la comunicación entre dos equipos de cómputo en una red.

3.1.1 Protocolos de Capas

En un principio los protocolos fueron sencillos, pero a medida que las organizaciones crecieron y las redes de datos se volvieron más sofisticadas, la logística para dar soporte se volvió más compleja. Debido a lo anterior, fue necesario desarrollar protocolos de capas, cuyo diseño está basado en la filosofía de programación estructurada. El principio de esta disciplina consiste en dividir todo el trabajo de un sistema de información en funciones, módulos o capas más pequeñas para simplificar el diseño y facilitar el control del sistema.

El objetivo de los protocolos de capas es definir todas las funciones de comunicación y separarlas en tareas más específicas (capas). Cada capa realiza una tarea distinta y autosuficiente, pero depende de las capas inferiores. La mayoría de los protocolos de transferencia de datos utilizan algún arreglo de capas, cada capa se comunica con su similar en el equipo remoto por medio del mismo protocolo.

3.2 Modelo OSI

El modelo de interconexión de sistemas abiertos (por sus siglas en ingles OSI) es la definición cuidadosa de las capas funcionales para la conformación de todos los protocolos modernos. Su objetivo es establecer estándares mundiales de diseño para todos los protocolos de comunicaciones, con la idea de que todos los equipos que se fabriquen sean compatibles.

El principio del modelo OSI es el de los protocolos de capas. Mientras las capas interactúan de manera “aparejada” y la interacción entre ellas no se afecte, no es importante la forma como se lleve a cabo la función de esa capa individual. El modelo OSI subdivide la función de comunicación de datos en 7 capas, cada una de ellas se puede considerar como un programa o proceso de computadora que se comunica con el proceso correspondiente en otra computadora remota. Las leyes que rigen esta conversación para determinada capa constituyen el protocolo de esa capa, un protocolo contiene los siguientes elementos principales:

- **Sintaxis:** Define el formato de los datos y los niveles eléctricos de las señales.
- **Semántica:** Define la información de control para la coordinación y manejo de errores.
- **Base de tiempo:** Establece la sincronización del emisor y receptor para la detección adecuada de los bits. También define el acoplamiento de velocidades y la secuencia de paquete de datos.

El modelo OSI no es un protocolo o conjunto de protocolos, es más bien la definición cuidadosa de las capas funcionales para la conformación de todos los protocolos modernos. El objetivo es establecer estándares mundiales de diseño para todos los protocolos de datos de telecomunicaciones con la idea de que todos los equipos de red que se fabriquen sean compatibles entre sí.

Realmente, en el modelo OSI, los datos no se transmiten horizontalmente de equipo a equipo en cada capa, si no que se transfieren verticalmente hacia abajo en la computadora transmisora y verticalmente hacia arriba en la computadora destino. Solo en la capa 1 hay comunicación real entre las maquinas. Para entender mejor la filosofía de funcionamiento del modelo OSI es necesario observar cuidadosamente la siguiente figura donde se ilustran cada una de las capas:

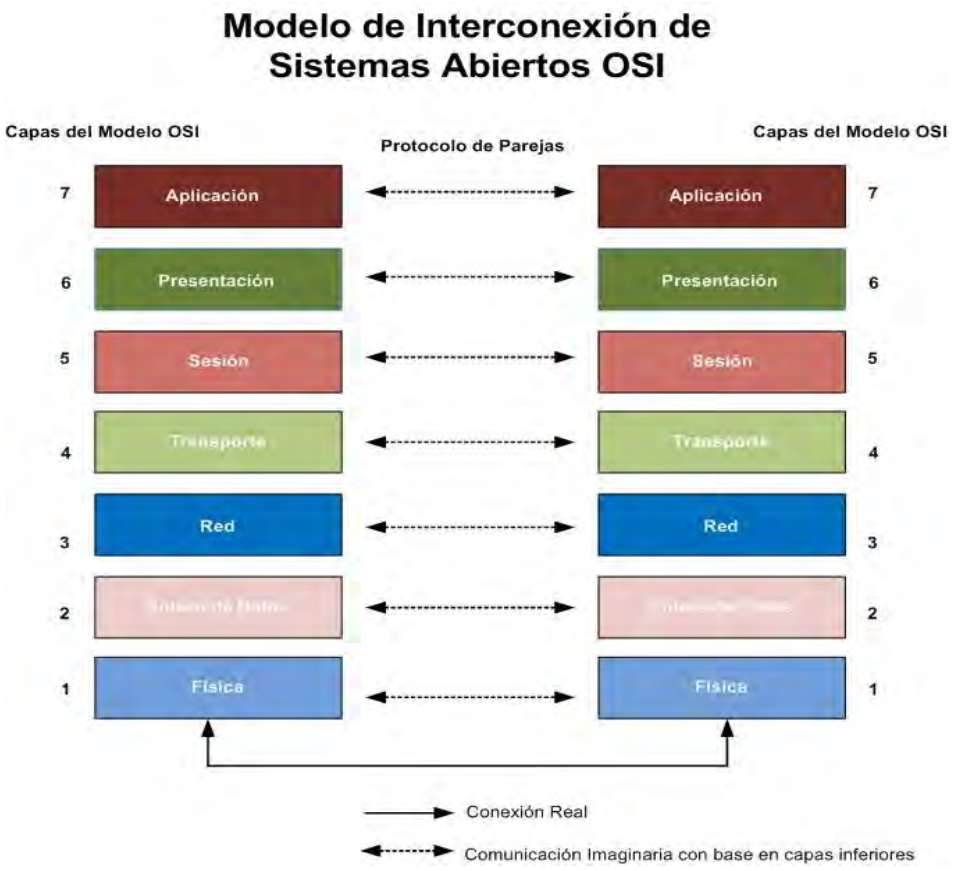

Figura 6 Modelo de Interconexión de Sistemas Abiertos OSI

Las funciones de las capas individuales del modelo OSI se encuentran definidas completamente en los estándares ISO 7498, en resumen son las siguientes:

- **Capa física (1):** Se encarga del establecimiento y la liberación del enlace físico durante la transmisión de los datos. Especifica los requerimientos eléctricos, mecánicos y de procedimiento para tal fin. La unidad de transmisión de la capa física es llamada Bit.
- **Capa de enlace de datos (2):** Se encarga de asegurar la confiabilidad de la transmisión entre nodos adyacentes de los datos considerando un canal ruidoso. Entre las principales funciones que realiza esta capa se encuentran la organización de los datos en conjuntos de ellos llamados paquetes, regular el tráfico mediante buffer, agregar banderas para indicar el principio y el fin de los mensajes, proveer métodos de accesos al canal, foliar los

mensajes que se transmiten y asegurar la sincronía entre las computadoras que se comunican.

- **Capa de red (3):** Es responsable del establecimiento de conexiones a través de una red real, determinando la combinación adecuada de enlaces individuales que se necesitan (función de enrutamiento) y controlando el flujo de mensajes entre equipos. Entre sus funciones específicas podemos mencionar: el establecimiento de rutas desde una fuente hasta un destino para transmitir los paquetes, ensambla los mensajes que recibe de la capa de transporte en paquetes y los desensambla en el otro extremo, realiza control de flujo y error, reconoce prioridad entre los mensajes y los envía con la prioridad asignada y ofrece servicios de interconexión para enlazar redes por medio de enrutadores.
- **Capa de transporte (4):** Controla la integridad del mensaje durante la transmisión entre los extremos del enlace, esto significa que al recibir información de la capa de red, la capa 4 verifica que la información este en el orden adecuado y revisa si existe información duplicada o extraviada. Si la información recibida está en desorden (es posible en redes grandes), la capa de transporte corrige el problema y transfiere la información a la capa de sesión en donde se le dará un proceso adicional.
- **Capa de sesión (5):** Se encarga de iniciar, mantener y terminar la conexión llamada sesión (dialogo entre dispositivos). Las funciones que realiza son las siguientes: controla el dialogo entre dispositivos (quién transmite, cuando, por cuanto tiempo, etc.), sincronización (restablece la comunicación si ocurren problemas con el enlace sin perder los datos), transmite la información del usuario (capa de presentación) en forma ordenada, etc.
- **Capa de presentación (6):** Se encarga de negociar una técnica mutuamente acordada para la codificación de los datos (sintaxis), así como de cualquier conversión que se necesite entre los formatos de código o arreglo de datos para que la capa de aplicación reciba el tipo que reconoce.

Las principales funciones son: compresión de datos, cifrado de datos, transformación de sintaxis entre los datos, etc.

- **Capa de aplicación:** Se encarga de suministrar servicios de transferencia de datos al usuario, es decir, al programa de aplicación. Proporciona los procedimientos precisos que permiten a los usuarios ejecutar los comandos relativos a sus propias aplicaciones. Esta capa es la más alta del modelo OSI y generalmente funciona con el administrador de la red. La transferencia de archivos y el acceso remoto a los mismos son probablemente sus aplicaciones más comunes.

3.3 Protocolos VPN

Los protocolos utilizados para crear VPN's determinan la manera en que los equipos se comunican a través del enlace y también de que manera será resguardada la información transmitida en el mismo. Los protocolos VPN tienen gran impacto sobre la seguridad global del sistema debido a que el protocolo es utilizado para intercambiar claves de encriptación entre los dos extremos del enlace. Si esta operación no se hace de manera segura, un usuario mal intencionado podría ser capaz de reconocer las claves y entonces descifrar el tráfico, anulando así uno de los grandes beneficios de utilizar VPN.

En la siguiente figura es posible observar los protocolos fundamentales de un enlace VPN, empezando desde el protocolo de enlace más sencillo hasta llegar a los de enlaces virtuales más seguros.

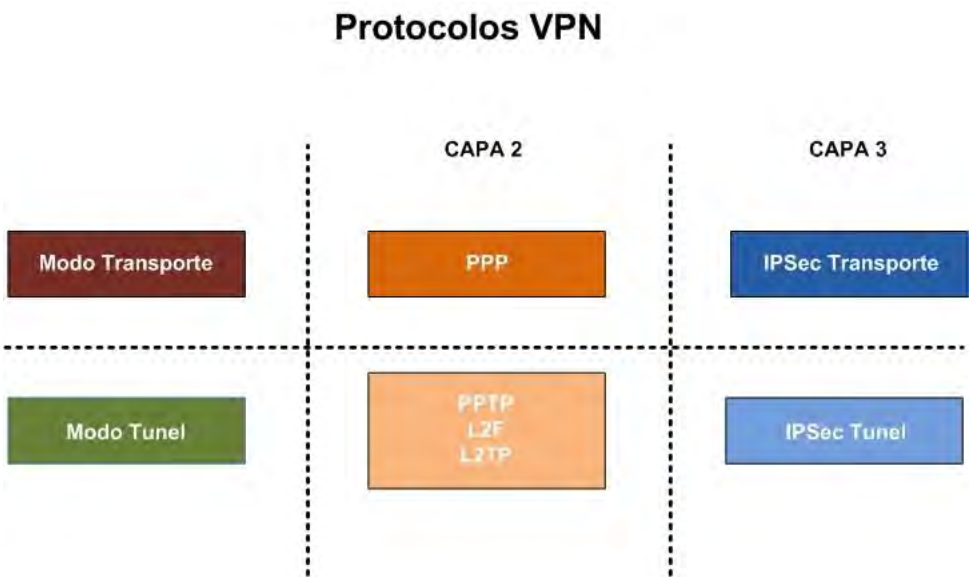

Figura 7 Ubicación de cada protocolo VPN en el modelo de referencia OSI. (Elaboración propia)

3.4 Modo Transporte de las Conexiones VPN

Los estándares VPN definen dos modos distintos de funcionamiento, el modo transporte y el modo túnel, cada uno de estos modos se definen por un protocolo específico y tienen sus propios usos particulares, por lo que se debe tener mucho cuidado al elegir el correcto para implementar en una solución.

El modo transporte se utiliza entre equipos finales (computadoras convencionales) o entre un equipo final y un gateway, si este último está siendo tratado como un host. En este modo solo se cifran los datos, dejando intacto el encabezado IP. En el siguiente ejemplo (Figura 8) el modo transporte se usa para instalar una sesión Telnet cifrada desde la computadora resaltada en amarillo (Angel PC) hasta el Gateway ubicado en la otra sección del enlace, haciendo posible al usuario “Angel” configurar remotamente el dispositivo Cisco PIX.

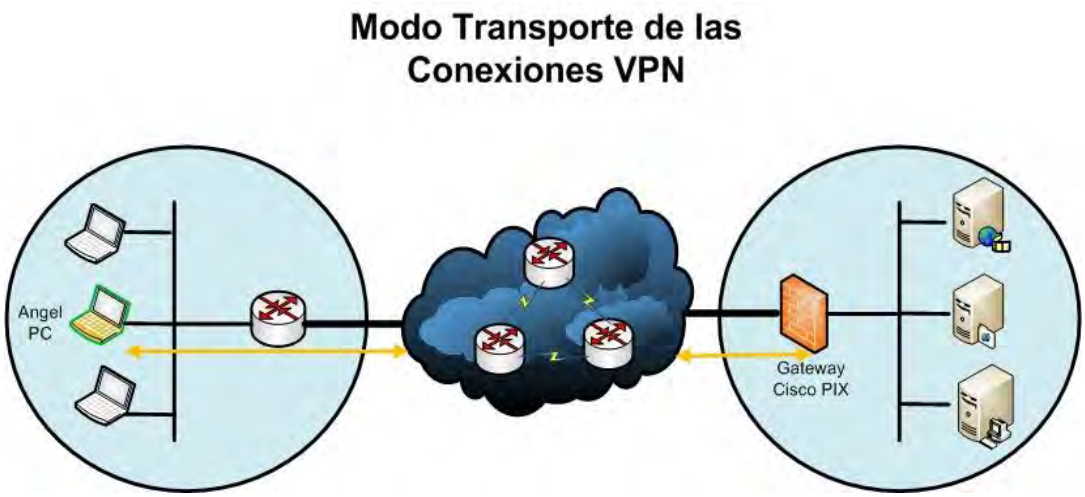

Figura 8 Modo transporte de las conexiones VPN (Elaboración propia)

3.5 Modo túnel de las conexiones VPN

En el modo túnel, los protocolos que intervienen se encargan de asegurar el enlace recién creado mediante algoritmos de cifrado propios de cada protocolo, con el fin de que la información que transmitida sea confiable y segura, logrando de esta forma una asociación segura entre los dispositivos involucrados.

Este modo es utilizado con más frecuencia cuando el extremo de una asociación de seguridad es un router VPN o cuando los dos extremos son routers VPN, donde el dispositivo gateway de seguridad actúa como proxy para los servidores que se encuentran detrás. El modo Túnel cifra tanto la carga útil como el encabezado completo UDP/TCP e IP. El modo túnel se utiliza con mucha frecuencia para cifrar tráfico entre cortafuegos VPN (utilizados como Gateway) o entre un router VPN y un Gateway, como se muestra en la Figura 9.

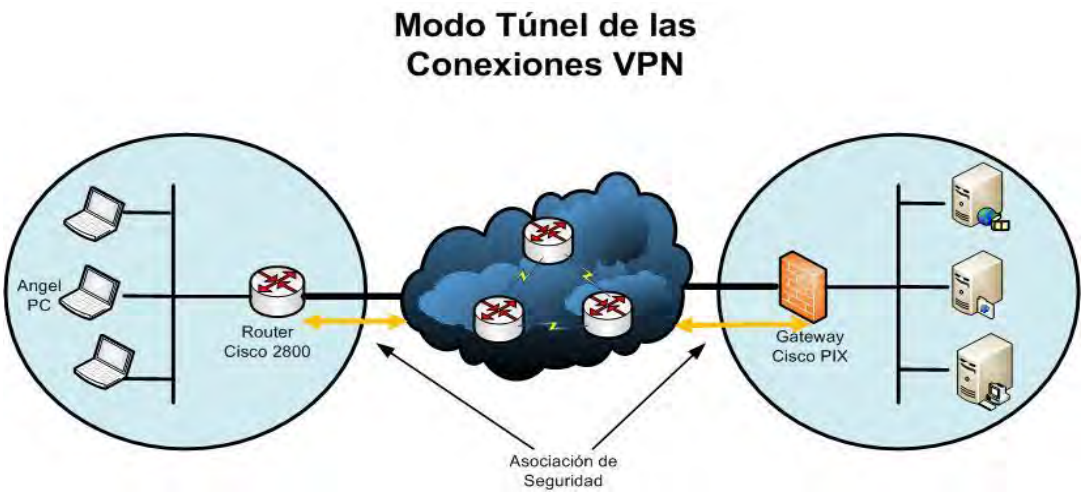

Figura 9 Modo túnel de las conexiones VPN (Elaboración propia)

3.6 Concepto de túnel

Como se ha mencionado en párrafos anteriores, existen mecanismos que aseguran la confidencialidad de las comunicaciones basadas en VPN. Los protocolos utilizados en este tipo de enlaces aseguran que los datos no pueden ser leídos ni modificados en su trayecto. Aunque las distintas tecnologías de redes privadas virtuales poseen algunas características diferentes, comparten muchos elementos en común, como la utilización de túneles seguros para transportar la información entre el emisor y el receptor.

Un túnel es un método que transforma la información para que no sea leída por terceros que estén presentes en el medio de transmisión. Este túnel es creado en forma virtual sobre el trayecto de red que es considerado público o expuesto, es decir los datos viajan ilegibles para los usuarios de la red pública y realizan la trayectoria sin que sean perturbados, brindando altos niveles de seguridad a la información.

El túnel se crea entre dos extremos, entre dos servidores VPN o entre un cliente y un servidor VPN, los cuales se ponen de acuerdo en los protocolos de túnel a utilizar antes de empezar a transmitir la información. Cuando se envían los datos por el túnel, la trama o paquete es descompuesta en fragmentos ilegibles, ofreciendo funciones de seguridad e integridad al contenido. Una vez que los

paquetes llegan al extremo opuesto, se extraen los datos útiles y se procesan como si se hubiesen recibido directamente de un equipo a otro en un medio como la red local.

Existen diferentes alternativas para crear túneles, siendo base aquel mecanismo que permite agregar una cabecera adicional al paquete original para que este pueda circular a través de la red pública hasta su destino, donde se eliminará el encabezado adicional.

Figura 10 Estructura de túnel VPN con tramas de encabezado adicional (Elaboración propia)

3.6.1 Tipos de túneles VPN

Se pueden crear túneles con diferentes características, según sean las condiciones en que se solicitan los servicios:

- **Túnel voluntario:** Se crea cuando un cliente inicia el proceso de conexión con el servidor VPN. Uno de los requisitos de un túnel voluntario es una conexión entre el servidor VPN y el cliente. En este caso la computadora cliente es un punto terminal del túnel y actúa directamente como un cliente del mismo.
- **Túnel obligatorio:** Con túneles obligatorios se pueden crear conexiones entre dos servidores VPN o dos dispositivos de acceso VPN como los routers. En este caso un servidor capaz de soportar una VPN (o más) configura y crea un túnel obligatorio. Con esto, la computadora del usuario

deja de ser un punto terminal del túnel ya que otro dispositivo (el servidor de acceso remoto) es el punto terminal del túnel y actúa como cliente del mismo.

3.6.2 Protocolos de Túnel

Existen tres protocolos relevantes para crear túneles VPN. Estos Protocolos serán objeto de estudio en los siguientes capítulos de este trabajo:

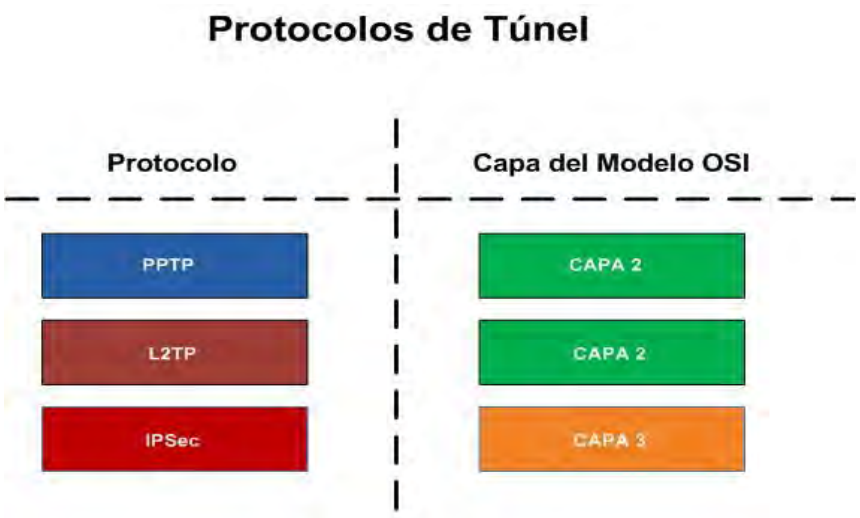

Figura 11 Principales protocolos de Túnel VPN (Elaboración propia)

3.7 Seguridad en las capas del modelo OSI

El protocolo de seguridad a usar en un entorno determinado depende de los servicios de seguridad que se requieren en aplicaciones que necesitan protección. Todos los protocolos de la capa de aplicación tienen la ventaja de que el servicio de seguridad puede ser definido específicamente en términos de las actividades de la aplicación. Por ejemplo, en lo que respecta a los servidores web, sería posible aplicar medidas de seguridad variables a las páginas web individuales. Sin embargo, la mayoría de los protocolos de seguridad de la capa de aplicación, como HTTP, se están convirtiendo en obsoletos por el uso de los protocolos de la capa de transporte o de la capa de red.

En lo relativo a la seguridad de la capa de transporte, todos los mensajes de aplicación deberán ser tratados por igual. Sin embargo, es posible especificar distintos servicios de seguridad para aplicaciones diferentes, siempre y cuando las implementaciones de los fabricantes lo permitan. SSL (Secure Sockets Layer) se ha generalizado y está ampliamente implementado en entornos web. SSH es un protocolo valido para la protección de los protocolos de la capa de transporte y se utiliza mucho para el inicio de sesión remoto seguro (Telnet) y para las transferencias remotas de archivos (FTP).

La seguridad de la capa de red, a través del uso de IPsec, puede definir los servicios de seguridad de la capa IP. Dependiendo de la implementación de cada fabricante, es posible definir los servicios de seguridad en base a las direcciones IP, o es posible proporcionar distintos servicios de seguridad con base a una combinación de dirección IP, protocolo de transporte y aplicación. IPsec tiene la ventaja de ocultar la información de la capa de transporte, además puede protocolos de la misma capa de transporte que no sean TCP como los es UDP. Sin embargo, dado que oculta la información de la capa de transporte, si se requiere información de la cabecera de esta capa para soportar otros requisitos de red (como la calidad de servicio, que podría tener que buscar números de puerto TCP/UDP), podría tener problemas.

Para el caso de las VPN, generalmente es necesario combinar los protocolos de seguridad ya que la mayoría de los entornos utilizan una combinación de protocolos de capa 2 y 3 combinados con IPsec.

CAPÍTULO IV

PROTOCOLOS VPN DE CAPA 2

"¿Cómo sobrevivir logrando que te necesiten? Sobrevives porque haces que ellos necesiten lo que tienes."

Bill Gates

4.1 Protocolo punto a punto (PPP)

Toda comunicación entre dos puntos necesita de normas particulares de conexión, las cuales son esenciales para enviar la información a través del enlace implementado, sin ellas es imposible direccionar o enrutar los paquetes de información a su destino. Para ello es necesario recurrir a protocolos específicos de acuerdo a las necesidades de comunicación, además es importante destacar que se deben considerar las respectivas normas de seguridad y autenticidad para obtener el resultado esperado.

Para estas necesidades se ha diseñado un conjunto de normas estándar de punto a punto PPP (desarrollado por IETF, Internet Engineering Task Force), con el cual es posible encapsular los paquetes de datos que van a ser enviados en tramas PPP y luego se transmiten a través del enlace entre los componentes remotos y la red.

PPP es parte de TCP/IP y básicamente encapsula el protocolo del paquete de información original en uno transportable por Internet (paquete PPP). Además permite incorporar términos de autenticidad para que la seguridad de la red e integridad de la información no sean afectadas. Los estándares de PPP también admiten características avanzadas que no estaban disponibles en estándares más antiguos. PPP acepta varios métodos de autenticación, así como compresión y cifrado de datos. En la mayor parte de las implementaciones de PPP se puede automatizar todo el proceso de inicio de sesión.

4.1.1 Secuencia de la conexión PPP

El caso que representa la primera etapa del enlace VPN es cuando un equipo cliente remoto necesita comunicarse con el servidor VPN de su empresa de carácter privado. Para este fin en primer lugar se debe realizar una petición al ISP local para que realice la comunicación mediante PPP, lo cual servirá para implementar un túnel VPN. A continuación se indican las fases de la conexión PPP:

- **Establecimiento del enlace PPP:** Se establecen las reglas para el manejo y direccionamiento de tramas entre el equipo remoto y el servidor (origen y destino). Esto permite que se establezca una comunicación continua (transferencia de tramas). En esta fase se configuran las opciones para la implementación del protocolo de control de enlace (LCP), el cual establece, mantiene y finaliza la conexión física; en otras palabras se seleccionan las opciones de comunicación básicas. Prácticamente luego de la conexión física telefónica inicial entre el cliente remoto y el servidor ISP, se envían una serie de paquetes LCP para realizar la petición de configuración a nivel de capa de enlace de datos (capa 2 del modelo OSI).
- **Autenticación del usuario:** El usuario remoto debe presentar una identificación al servidor de acceso remoto, acción que si es aceptada permite la conexión y comunicación con la red privada. En esta fase el usuario envía una identificación al servidor de acceso remoto y este debe verificar la autenticidad del nombre y las contraseñas de acceso. U buen esquema o sistema de autenticación proporciona la seguridad de la información y el acceso exclusivo a clientes autorizados. PPP ofrece métodos de autenticación como PAP, CHAP, MS-CHAP, etc. Estos algoritmos de autenticación son expuestos más adelante en este capítulo.
- **Llamada a protocolos de control de red:** En esta fase del PPP se invoca a los protocolos de control de red (NCP) que fueron seleccionados por el cliente remoto durante la fase de establecimiento del enlace para configurar los protocolos utilizados para la comunicación. En esta fase el ISP, mediante NCP, otorga dinámicamente una dirección IP pública al equipo cliente para su uso durante la sesión.
- **Finalización del enlace:** LCP puede terminar el enlace en cualquier momento. Esto normalmente se hará por petición del usuario, pero puede darse el caso en que el determinante para finalizar la sesión sea un evento físico.

En resumen, para establecer comunicación sobre un enlace punto a punto, cada extremo del enlace PPP debe enviar paquetes LCP que configuren el

enlace de datos durante la fase de establecimiento del mismo. Una vez establecido el enlace, PPP proporcionará una fase de autenticación opcional antes de seguir en la fase del protocolo de capa de red. La fase NCP establece y configura los distintos protocolos de capa de red, como es IP.

Por defecto, la autenticación previa a la fase NCP no es obligatoria. Si se desea la autenticación del enlace, una implementación especificará la opción de configuración del protocolo de autenticación durante la fase de establecimiento del enlace. Estos protocolos de autenticación están destinados a ser usados principalmente por equipos finales (hosts) y routers que se conectan a un servidor de red PPP a través de circuitos conmutados o líneas de acceso telefónico, pero que también pueden ser aplicados a enlaces dedicados. El servidor puede usar la identificación del host o router de conexión en la selección de las opciones para las negociaciones de la capa de red.

Las negociaciones PPP se componen de la negociación LCP y de la negociación NCP. LCP es el encargado de establecer la conexión con ciertas opciones negociadas, manteniendo la conexión y proporcionando procedimientos que cierran la conexión. Para llevar a cabo estas funciones el LCP utiliza las 4 faces descritas anteriormente.

4.1.2 Formato de trama PPP

La PDU de PPP utiliza la trama HDLC (Control de Enlace de Datos de Alto Nivel), tal y como se estipula en la ISO 3309-1979. El formato de trama PPP se describe en la siguiente figura:

Figura 12 Formato de trama PPP (Elaboración propia)

- **Indicador:** Un byte que indica el principio o el fin de una trama. Este campo se compone de la secuencia binaria 01111110 (7Eh).
- **Dirección:** Un byte que contiene la secuencia binaria 11111111 (FFh), que es la dirección de difusión estándar. PPP no asigna direcciones de estación individuales.
- **Control:** Un byte que contiene la secuencia binaria 00000011 (03h), que requiere la transmisión de datos de usuario en una trama sin secuencia. Representa información de control de enlace el valor binario es fijado como indicador de enlace fiable.
- **Protocolo:** Dos bytes que identifican el protocolo que esta encapsulado en el campo de información de la trama.
- **Datos:** 0 o más bytes que contienen el datagrama del protocolo que se especifica en el campo de protocolo. El final del campo de información se encuentra localizando la secuencia de indicadores de cierre y permitiendo 2 bytes para el campo FCS. La longitud máxima predeterminada del campo de información es de 1.500 bytes. En virtud de un acuerdo previo, las implementaciones PPP pueden usar otros valores para la longitud máxima del campo de información.
- **Secuencia de comprobación de tramas (FCS):** Generalmente está formado por dos bytes. En virtud de un acuerdo previo, las implementaciones PPP pueden utilizar una FCS de cuatro bytes para mejorar la detección de errores.

El LCP puede negociar modificaciones en la estructura de las tramas PPP estándar. Sin embargo, las tramas modificadas siempre serán claramente diferenciables de las tramas estándar.

4.1.3 PAP de PPP

El protocolo de Autenticación por Contraseña (PAP) proporciona una manera muy sencilla de que un host establezca su identidad ante el autenticador, utilizando un intercambio de señales bidireccional. Esto solo se hace en el establecimiento

inicial del enlace. Una vez completada la fase de establecimiento del enlace, se usa el paquete de petición de autenticación para iniciar la autenticación PAP. Este paquete contiene el nombre y la contraseña del usuario que se intenta autenticar como se muestra en la siguiente figura:

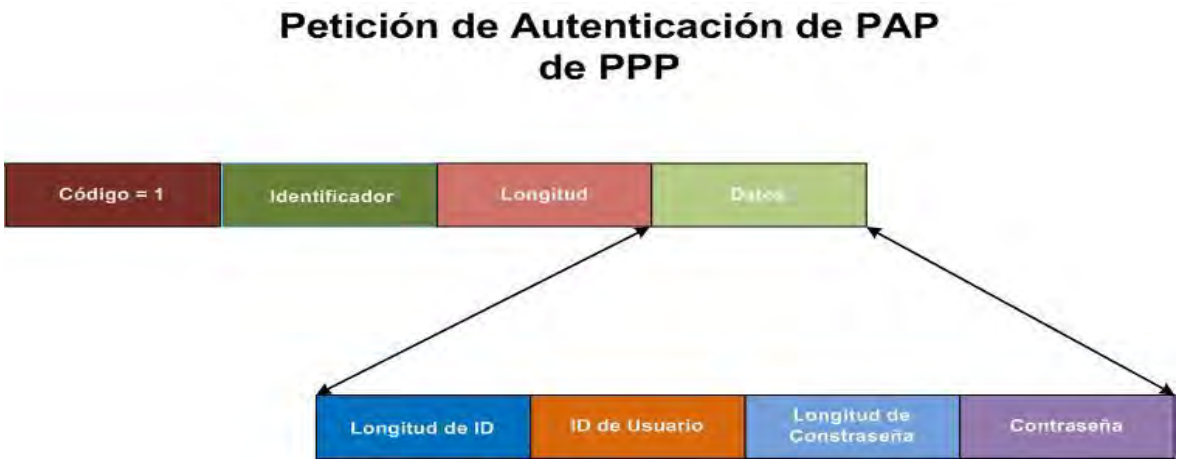

Figura 13 Petición de autenticación PAP de PPP (Elaboración propia)

Este paquete de petición es enviado en repetidas ocasiones hasta que se recibe un paquete de respuesta valido o cuando expira un contador de reintentos opcional. Si el autenticador recibe un par ID de usuario/contraseña reconocible y aceptable, deberá responder con un acuse de recibo (Ack) de autenticación. Si el par ID de usuario/contraseña no es reconocible o aceptable, el autenticador deberá responder con un acuse de recibo negativo (Nak) de autenticación.

PAP no es un método de autenticación sólido. PAP solo autentica al usuario y las contraseñas son enviadas sobre el circuito sin protección alguna. No existe protección frente a los ataques de reproducción o frente a los ataques reiterados de prueba y error. El usuario controla y temporización de los intentos.

La Figura 14 muestra la secuencia de las negociaciones PPP entre un router de una sucursal (el usuario) que trata de autenticarse ante el autenticador que es el servidor de acceso a la red.

Figura 14 Autenticación PAP de PPP (Elaboración propia)

4.1.4 CHAP de PPP

El protocolo de Autenticación de Intercambio de Señales por Desafío (CHAP) de PPP se usa para verificar periódicamente la identidad de un host o usuario, utilizando un intercambio de señales de tres vías. El Protocolo CHAP se ejecuta en el establecimiento del enlace inicial y puede ser repetido en cualquier momento posterior al establecimiento del enlace.

CHAP impone la seguridad de red requiriendo que los equipos compartan un secreto en texto plano. Este secreto nunca se envía por el enlace, se efectúa la siguiente secuencia de pasos:

- Una vez completada la fase de establecimiento del enlace, el autenticador envía un mensaje de desafío al host. El desafío se compone de un identificador (ID), un número aleatorio y el nombre de host del dispositivo local o el nombre de usuario del dispositivo remoto.
- El equipo receptor calcula un valor utilizando una función hash unidireccional; el secreto es la entrada de la función hash unidireccional. Hash es una función matemática que hace corresponder una representación de longitud fija a un mensaje “m” de longitud variable. Esta representación se llama valor resumen del mensaje.

- El equipo envía la respuesta al desafío, que consta de una versión cifrada del ID, una contraseña secreta (el valor hash calculado), un numero aleatorio y el nombre de host del dispositivo remoto o el nombre de usuario de dispositivo remoto.
- Cuando el autenticador recibe la respuesta al desafío, verifica el secreto buscando el nombre que hay en la respuesta y efectuando la misma operación de cifrado. El autenticador compara la respuesta con sus propios cálculos del valor hash esperado.
- Si los valores coinciden, el autenticador enviará un mensaje de éxito y el LCP establecerá el enlace.

La siguiente figura muestra un escenario en el que un router de una sucursal está tratando de autenticarse ante el servidor de autenticación o autenticador.

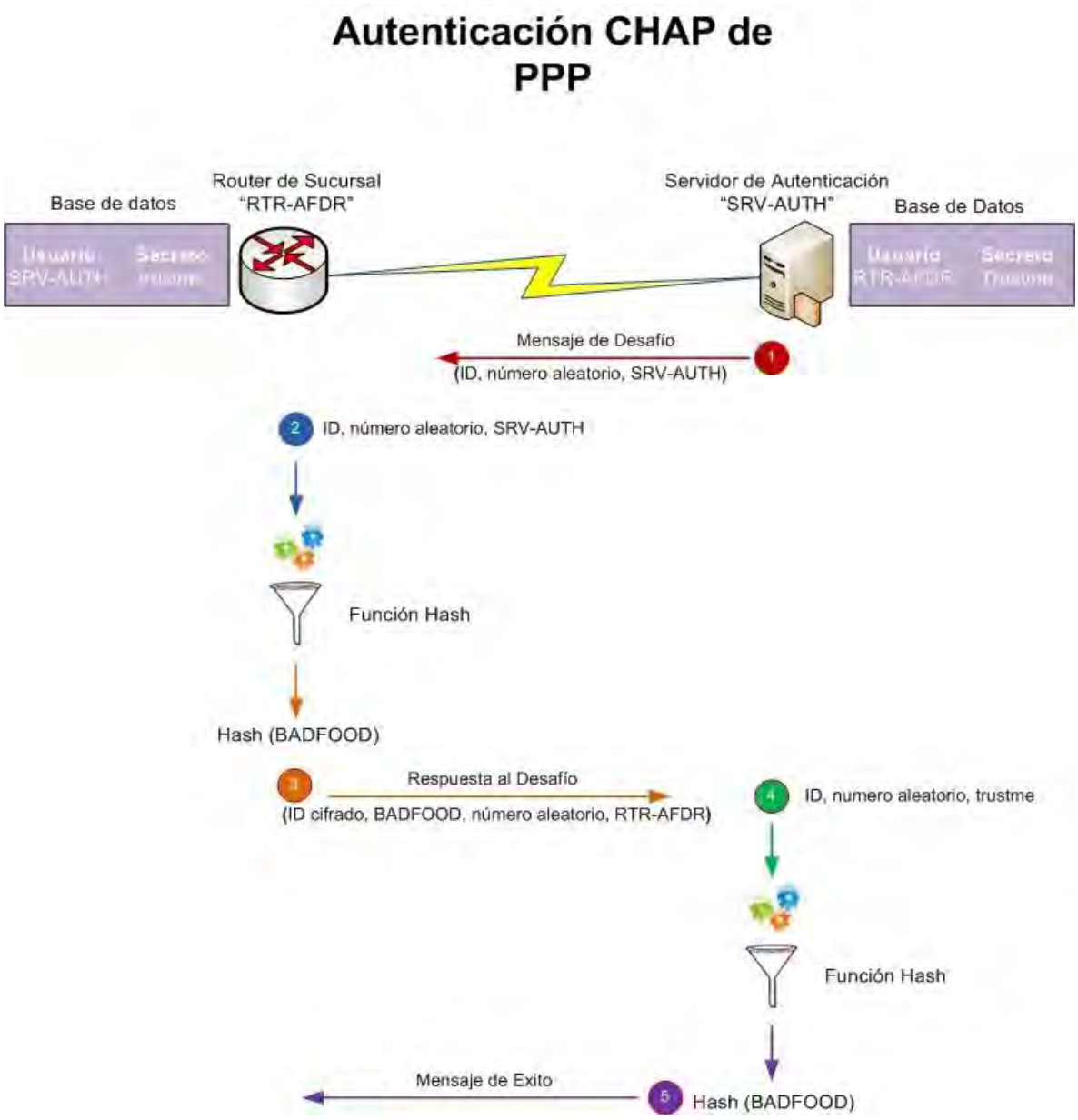

Figura 15 Autenticación CHAP de PPP (Elaboración propia)

Las contraseñas secretas deberán ser identificadas en los dispositivos remoto y local. Estos secretos deberán ser consensuados, generados e intercambiados de una forma segura. Dado que el secreto no se transmite nunca, se impide que otros dispositivos traten de apropiarse de él y de obtener acceso ilegitimo al sistema. Sin la respuesta correcta el dispositivo remoto no podrá conectarse con el dispositivo local.

CHAP proporciona protección frente al ataque de reproducción a través del uso de un identificador que cambia incrementalmente y de un valor de desafío variable. El uso de los desafíos reiterados trata de limitar el tiempo de exposición ante un ataque. El autenticador es el que controla la frecuencia y la temporización de los desafíos.

Normalmente CHAP usa MD5 (Algoritmo de Resumen del Mensaje 5) como función hash unidireccional; es necesario almacenar los secretos compartidos en forma de texto plano. Microsoft posee una variante de CHAP (MS-CHAP), en la que la contraseña se almacena cifrada tanto en el host como en el autenticador. Por lo tanto, MS-CHAP puede aprovecharse de las bases de datos de contraseñas cifradas irreversiblemente disponibles, mientras que el CHAP basado en estándares no puede.

4.1.5 EAP de PPP

El protocolo de autenticación extensible (EAP) de PPP es un protocolo general que sirve para la autenticación PPP y que soporta múltiples mecanismos de autenticación. El protocolo EAP no selecciona un mecanismo de autenticación específico en la fase de control del enlace; más bien, aplaza la selección hasta la fase de autenticación, de forma que el autenticador pueda solicitar más información antes de determinar el mecanismo de autenticación específico.

- Una vez completada la fase de establecimiento del enlace, el servidor de autenticación envía una o más peticiones para autenticar al equipo remoto. La petición posee un campo de tipo que indica lo que se está pidiendo. Entre los ejemplos de tipo de petición se incluyen la identidad, el desafío MD5, la tarjeta de tokens genérica, etc. El tipo de desafío MD5 se relaciona directamente con el protocolo de autenticación CHAP.
- El host envía un paquete de respuesta contestando a cada petición, el paquete de respuesta contiene un campo de tipo que se relaciona con el campo de tipo de la petición.

- El servidor de autenticación finaliza la parte de autenticación con un paquete de éxito o de fallo.

La Figura 16 muestra el funcionamiento del protocolo EAP de PPP. En dicho ejemplo el router de una sucursal está tratando de autenticarse ante el servidor de autenticación.

Figura 16 Autenticación EAP de PPP (Elaboración propia)

Generalmente, el servidor de autenticación envía una petición inicial de identidad seguida de una o más peticiones de información de autenticación. Sin embargo, la petición inicial de identidad no es obligatoria y puede ser omitida en casos donde se supone la identidad, como es el caso de enlaces dedicados.

EAP incorpora más flexibilidad a la autenticación PPP y ofrece la posibilidad de usar tecnologías como los certificados digitales.

4.1.6 Protocolos que utilizan mecanismos de autenticación

Muchos protocolos requieren la comprobación de la autenticación antes de proporcionar derechos de autorización y acceso al usuario o dispositivo, los más importantes son TACACS+, RADIUS, Kerberos, DCE y FORTALEZZA. TACACS+ y RADIUS se suelen utilizar en entornos de acceso telefónico para proporcionar

una base de datos de autenticación escalable y pueden incorporar una serie de métodos de autenticación. Kerberos es un protocolo que se utiliza en ciertos entornos para verificar que los usuarios los servicios de red que estos utilizan sean en realidad quienes o lo que dicen ser antes de conceder privilegios de acceso.

- **TACACS+:** Es la última generación de TACACS, que es un protocolo sencillo de control de acceso basado en UDP. TACACS+ es un protocolo cliente/servidor; el cliente TACACS+ suele ser un NAS (Servidor de Acceso a la Red) y el servidor TACACS+ suele ser un proceso de demonio que se ejecuta en un equipo UNIX. Un componente de diseño fundamental de este protocolo es la separación de la autenticación, autorización y contabilidad. TACACS+ utiliza TCP como transporte, el demonio del servidor suele escuchar en el puerto 49 que es el puerto LOGIN asignado al protocolo TACACS.
- **RADIUS:** El protocolo de Servicio de Usuario de Acceso Telefónico Mediante Autenticación Remota, fue desarrollado como un protocolo de autenticación y contabilidad de servidor de acceso. RADIUS utiliza UDP como transporte y por regla general está considerado como un servicio sin conexión. Los temas relacionados con la disponibilidad, la retransmisión y los tiempos de espera del servidor son gestionados por los dispositivos RADIUS y no por el protocolo de transmisión. RADIUS es un protocolo cliente/servidor, el cliente suele ser un NAS y el servidor suele ser un proceso de demonio que se ejecuta en un equipo UNIX. El cliente es el responsable de pasar información de usuario a los servidores RADIUS designados y de actuar frente a la respuesta devuelta. Los servidores RADIUS son los responsables de recibir las peticiones de conexión del usuario, de autenticarlo y devolver toda la información sobre configuración necesaria para brindar el servicio usuario.
- **Kerberos:** Es un protocolo de autenticación de red de clave secreta que utiliza el Algoritmo Estándar de Cifrado de Datos (DES) para el cifrado y la autenticación. Kerberos fue diseñado para autenticar peticiones de usuario de recursos de red. Este protocolo se basa en el concepto de un tercero de

confianza que ejecuta la verificación segura de usuarios y servicios. En el protocolo Kerberos, este tercero de confianza se denomina Centro de Distribución de Claves (KDC), a veces también llamado servidor de autenticación. El uso principal de Kerberos consiste en verificar que los usuarios y los servicios de red que estos usan son verdaderamente quienes dicen ser, para ello, el servidor Kerberos de confianza emite tikets a los usuarios, los cuales tienen un tiempo de existencia limitado y se almacenan en la cache de credenciales del usuario.

- **DCE:** Es un conjunto de tecnologías de computación distribuida que proporciona servicios de seguridad para proteger y acceder al control de los datos, servicios de nombres que facilitan la localización de los recursos distribuidos y un modelo muy escalable de organización de usuarios, servicios y datos diseminados. DCE posee un diseño modular, soportando la autenticación y autorización. La parte de autenticación implementada es Kerberos, mientras que la parte de autorización funciona de un modo similar a Kerberos, pero está implementada por servidores de privilegios y registros.

4.2 Protocolo de túnel punto a punto (PPTP)

PPTP desarrollado principalmente por Microsoft es un protocolo de túnel de capa 2 del modelo de referencia OSI, que permite el tráfico seguro de datos desde un cliente remoto hasta un servidor corporativo privado, estableciéndose gracias a este la VPN. PPTP es una extensión de PPP ya que aprovecha las fases de autenticación, compresión y cifrado, para después crear el túnel virtual.

El *protocolo de túnel punto a punto* soporta múltiples protocolos de red como IP e IPX que comúnmente transitan sobre las redes públicas como Internet y puede ser utilizados para crear Redes Privadas Virtuales sobre otras redes públicas o privadas como líneas telefónicas (PSTN), redes LAN y WAN, Internet u otras redes públicas basadas en TCP/IP y además aprovecha las ventajas de los mecanismos de autenticación, compresión y cifrado de las tramas de información.

4.2.1 Escenario Típico de una Conexión PPTP

Generalmente hay tres dispositivos involucrados en una implementación

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

Cuando el cliente autorizado decide conectarse de forma remota al servidor de su empresa, desde donde está deberá primero conectarse a un ISP usando una conexión de acceso telefónico a redes (RDSI) mediante el protocolo PPP (primer paso, modo transporte).

El cliente en ese momento establece una conexión de acceso remoto, usando su adaptador de VPN a dicho servidor NAS creándose un túnel privado el cual culmina en el servidor de la organización privada y que conecta los extremos como si estuviesen en la misma red local, con la seguridad de un enlace punto a punto, pudiendo así tener acceso a recursos compartidos tales como carpetas, archivos e incluso impresoras.

A grandes rasgos, el túnel se basa en añadir una cabecera IP adicional al paquete original, donde se direcciona dicha trama con la IP publica del servidor VPN, y la IP privada de la red o host receptor quedaran resguardados, creándose un túnel secreto en la red pública. En la Figura 17 es posible observar el túnel creado entre un usuario remoto y la red corporativa de su empresa.

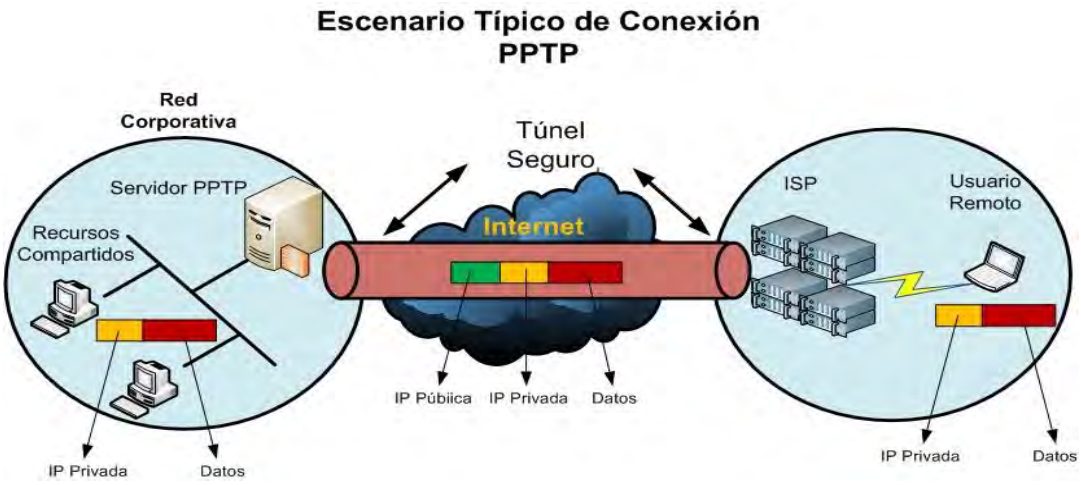

Figura 17 Escenario típico de una conexión PPTP (Elaboración propia)

Este escenario podrá variar según el tipo de conexión que tengan tanto el cliente como el servidor. Organizaciones con acceso permanente a Internet podrán configurar su propio NAS o RAS (Servicio de acceso remoto) para el soporte del protocolo PPTP, permitiendo que colaboradores de cualquier lugar del mundo puedan conectarse a ellos usando su acceso a internet disponible.

4.2.2 Servidor PPTP

El servidor PPTP cumple las funciones de ser el punto terminal en cada red privada virtual, es decir, es el mecanismo de filtro de entrada o salida de información o acceso de usuarios que estén autorizados. Esto lo logra procesando la información confidencial en paquetes PPTP (cuyas claves de cifrado son únicas por cada sesión que se inicie bajo la supervisión del Servidor PPTP) que va a salir al medio público, hasta el usuario final que corresponde al cliente autenticado. Además permite seleccionar la información que trate de ingresar a la red privada, es decir si la información PPTP no corresponde con las claves de cifrado de la sesión que inició con un cliente remoto, simplemente no permite el ingreso del usuario a la red VPN, o si está en uso corta la comunicación. El servidor PPTP también se puede configurar para determinar que maquina externa se puede conectar a la red local o qué punto dentro de la red podrá conectarse a Internet.

Las partes indispensables en un servidor PPTP (además del hardware necesario) son:

- **PNS (PPTP Network Server):** El servidor de red PPTP gestiona la operación sobre computadoras de propósito general o plataformas de servidor de red. Dado que PPTP se fundamenta exclusivamente en TCP/IP y que es independiente del hardware de interfaz, el PNS puede usar cualquier combinación de hardware para interfaz IP, incluyendo los dispositivos LAN y WAN.
- **PAC (PPTP Access Concentrator):** El concentrador de acceso PPTP es el dispositivo que asocia una o más líneas capaces de soportar PPTP, es decir, puede administrar múltiples sesiones multiplexadas sobre el mismo túnel. También este dispositivo presente en el servidor permite proveer servicios a muchos PNS.

El PAC es el responsable de proporcionar la interfaz física a las redes PSTN y RDSI así como proporcionar la terminación lógica de las sesiones LCP de PPP. La participación en los protocolos de autenticación PPP puede ser parte de PAC o del PNS. El PNS es el encargado de la agregación de canales, la terminación lógica de los NCP de PPP, así como del enrutamiento y puenteado multiprotocolo entre las interfaces NAS.

Una de las ventajas más palpables del PPTP es que reduce o elimina la necesidad de uso de otro tipo de equipo de telecomunicaciones para permitir las conexiones de equipos portátiles remotos.

4.2.3 Cliente PPTP

Si es ISP soporta PPTP, no se requiere añadir software o hardware adicional en el punto cliente, solo es necesaria una conexión estándar PPP. Esto no es recomendado ya que se genera un tramo inseguro desde el ISP local hasta el cliente remoto.

Si el ISP no soporta PPTP, el cliente puede utilizar el software PPTP y crear una conexión segura, primero utilizando el ISP local para establecer una conexión PPP con el fin de tener acceso a internet, para después lograr la conexión PPTP a través del puerto destinado para este servicio en el servidor de la empresa.

4.2.4 Secuencia de la Conexión PPTP

Debido a que PPTP está orientado a conexión, el PNS y el PAC mantienen información sobre la conexión para cada usuario que esté conectado a un PAC y se crea una sesión cuando se intenta una conexión PPP de extremo a extremo entre un servidor de acceso telefónico y el PNS. Los datagramas que estén relacionados son enviados por el túnel entre el PAC y el PNS.

El túnel está definido por un par PNS-PAC y en él se pueden ejecutar diversas sesiones. Una conexión de control que funciona sobre TCP administra el establecimiento, la liberación y el mantenimiento de las sesiones así como del propio túnel.

Existen dos componentes paralelos de PPTP, tal y como se describe a continuación:

- Una conexión de control entre cada par PAC-PNS que funciona sobre TCP.
- Un túnel IP que funciona entre el mismo par PAC-PNS, que se usa para transportar paquetes PPP con encapsulación GRE para las sesiones de usuario que haya entre el par.

4.2.5 Conexión de control PPTP

Antes de que se pueda producir un túnel PPP es necesario establecer una conexión de control entre el par PNS-PAC. La conexión de control es una sesión TCP sobre la cual se intercambia la información de control de llamada y de administración PPTP. Esta sesión se establece iniciando una conexión TCP en el puerto 1723. La sesión de control está asociada de forma lógica, pero separada, de las sesiones que se están canalizando a través del túnel PPTP.

La conexión de control es iniciada por el PNS o por el PAC una vez que estos establecen la conexión TCP subyacente. La conexión de control es la encargada del establecimiento, la administración y liberación de la sesión que se transporta a lo largo del túnel.

Una vez que se establece la conexión de control, el PAC o el PNS pueden iniciar sesiones, requiriendo llamadas salientes o respondiendo a llamadas entrantes. La propia conexión de control es mantenida por mensajes de eco de actividad.

4.2.6 Encapsulación PPTP

Una vez que es creada la trama PPP se empaqueta con un encabezado GRE (Encapsulación de Enrutamiento Genérico) y un encabezado IP en el cual se encuentran las direcciones origen y destino de trama (que corresponden al cliente y servidor VPN).

Los paquetes PPP encapsulados son en esencia paquetes de datos que carecen de elementos de entramado específicos de los medios. La siguiente figura presenta la estructura de la trama PPP ya encapsulada mediante PPTP.

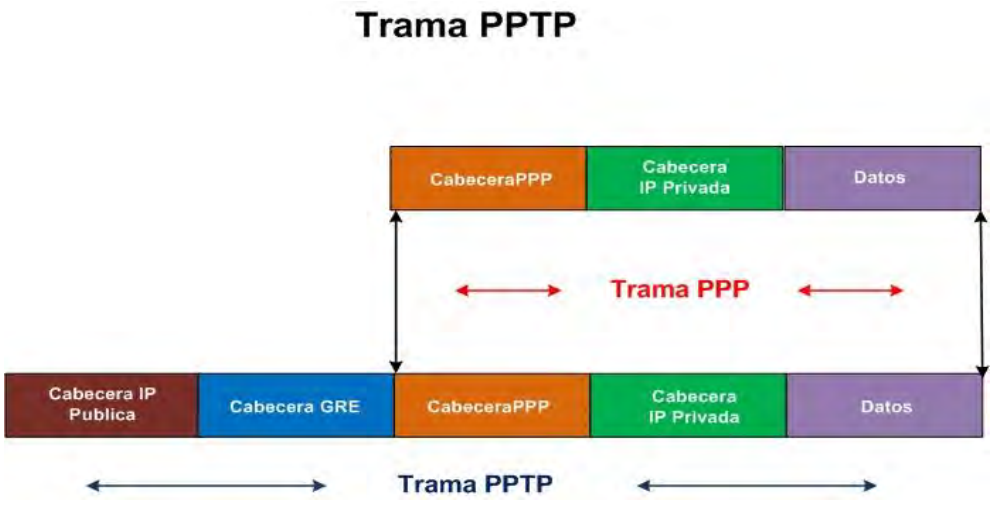

Figura 18 Trama PPTP (Elaboración propia)

- La cabecera IP pública proporciona la información necesaria para que el datagrama atraviese Internet. Esta cabecera establece la comunicación entre el cliente remoto y el servidor de túnel PPTP.
- El encabezado GRE se usa para encapsular el paquete PPP dentro de un datagrama IP, es decir, se ocultan los destinos IP originales del emisor y receptor, que solo el servidor PPTP y el cliente respectivo podrán percibir.
- La cabecera PPP permite establecer el nivel de enlace de datos entre el ISP y el usuario remoto, para así crear el túnel.
- La cabecera IP privada es el direccionamiento IP entre el host del usuario remoto y el servidor de la red corporativa.

Finalmente el paquete PPP es encapsulado y de ser interceptado, su direccionamiento será ilegible. Una vez que el paquete privado llega al servidor PPTP de la entidad corporativa, esta tiene la misión de abrir el paquete encapsulado, es decir, elimina todas las cabeceras establecidas para crear el túnel y el paquete puede entrar a la red privada normalmente.

Para mantener el túnel, PPTP utiliza un control de conexión que se encarga de la administración de los mensajes utilizados para dicho propósito de mantenimiento. Esto incluye la transmisión periódica de mensajes para detectar fallas en la conexión entre el cliente y el servidor 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 19 Paquete de control de conexión PPTP (Elaboración propia)

4.3 Protocolo de reenvío de capa 2 (L2F)

El protocolo L2F se creó en las primeras etapas de desarrollo de las VPN y fue diseñado para establecer túneles de tráfico desde usuarios remotos hasta sus oficinas centrales en su empresa. La principal característica de L2F es que el establecimiento del túnel no depende del protocolo IP ya que puede trabajar con otros medios como Frame Relay.

L2F utiliza el protocolo PPP para la autenticación del usuario remoto, pero también implementa otros sistemas de autenticación como los mencionados anteriormente TACACS+ y RADIUS. L2F permite que los túneles contengan más de una conexión.

Existen dos niveles de autenticación de usuario, primero por parte del ISP anterior al establecimiento del túnel y por otra parte cuando se ha establecido la conexión con la puerta de enlace o Gateway de la empresa. Como L2F es un protocolo de capa de enlace (capa 2 del modelo OSI), ofrece a los usuarios flexibilidad para manejar protocolos distintos a IP como lo son IPX y NetBEUI.

La figura 3-9 muestra un escenario y una serie de pasos a través de los cuales es posible realizar una conexión exitosa mediante L2F:

- El usuario remoto inicia una conexión PPP con su ISP sobre la PSTN o Red Telefónica Pública Conmutada (Public Switched Telephone Network).
- El NAS acepta la conexión y se establece el enlace PPP.
- El ISP autentica al usuario final utilizando CHAP o PAP.
- El NAS inicia el túnel L2F con el Gateway corporativo deseado.
- El Gateway corporativo autentica al usuario remoto y acepta o rechaza el túnel.
- El Gateway corporativo confirma la aceptación de la llamada y del túnel L2F. Si el Gateway corporativo acepta la conexión crea una interfaz virtual para PPP, con el fin de que las tramas de capa 2 puedan pasar ahora por este túnel en ambos sentidos. Las tramas de usuario remoto son recibidas en el NAS, desprovistas de todo entramado de enlace o bytes de

transparencia, encapsuladas en L2F y reenviadas por el túnel adecuado. El Gateway corporativo acepta estas tramas, elimina la encapsulación L2F y las procesa como tramas entrantes normales en relación a la interfaz y protocolo apropiados. El sentido contrario del tráfico se comporta de manera similar: el Gateway corporativo encapsula el paquete L2F y el NAS la elimina antes de enviarla al usuario remoto.

- El Gateway corporativo intercambia las negociaciones PPP con el usuario remoto. Dado que el usuario remoto se ha convertido sencillamente en otro cliente de acceso telefónico del servidor de acceso del Gateway corporativo, la conectividad del cliente podrá ser manipulada ahora utilizando mecanismos tradicionales con respecto a la autorización, la negociación de direcciones, el acceso de protocolos, la contabilidad y el filtrado.
- Los datos de extremo a extremo son canalizados entre el usuario remoto y el Gateway corporativo.

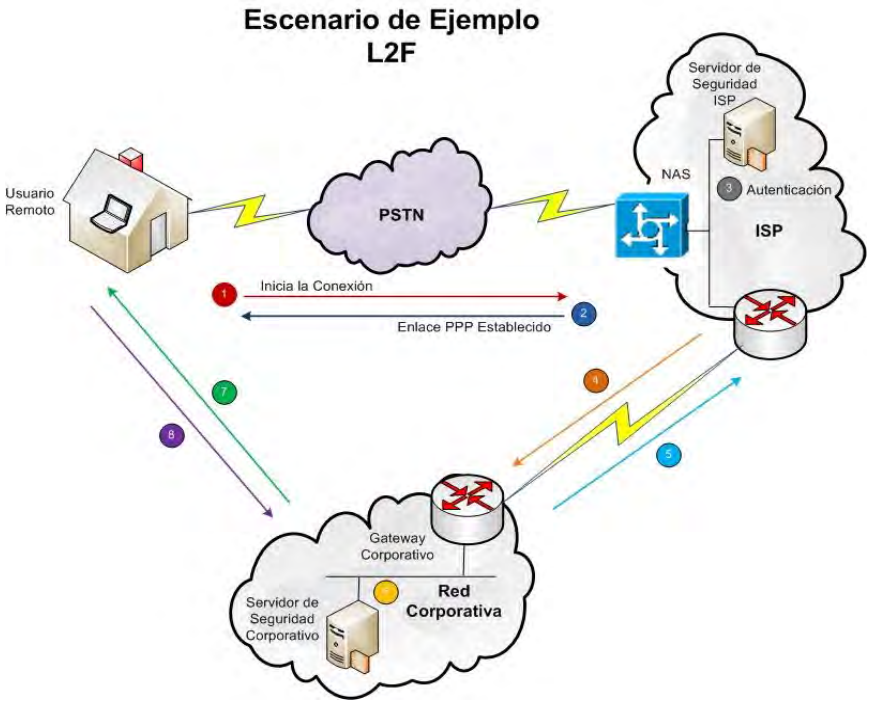

Figura 20 Escenario de ejemplo L2F (Elaboración propia)

4.4 Protocolo de túnel de capa 2 (L2TP)

L2TP fue diseñado por un equipo especial del IETF como heredero aparente de los protocolos PPTP y L2F. Fue creado para corregir las deficiencias de estos protocolos y establecer un estándar aprobado por el IETF. L2TP utiliza a PPP para iniciar el enlace y después define su propio protocolo de establecimiento de túnel basado en L2F. El transporte de L2TP está definido para una gran variedad de tipos de paquete, incluyendo X.25 y Frame Relay.

Como se mencionó anteriormente, L2TP es un protocolo que reúne las mejores características de PPTP y L2F, siendo las siguientes las más notables:

- L2TP cumple las características de PPTP, pero su gama de ruteo es más amplia ya que acepta paquetes de datos que no solamente son IP. Por lo tanto L2TP encapsula las tramas del protocolo punto a punto (PPP) que van a enviarse a través de redes IP, X.25, Frame Relay, modo de transferencia asíncrona ATM, y muchos tipos de redes más.
- Las tramas PPP encapsuladas se pueden cifrar o comprimir. Cuando los túneles L2TP aparecen como paquetes IP, se puede reforzar el cifrado de los datos haciendo uso del método que utiliza el protocolo de cifrado IPSec (IP Security). L2TP en combinación con IPSec proporciona túneles bien definidos e interoperables (Seguridad de alto nivel). Es una buena solución para conexiones seguras de acceso remoto y de enlace remoto de servidor a servidor.
- Admite una amplia gama de protocolos de autentificación que se utilizan para el enlace ISP-Cliente Remoto (Chap, MS-Chap, etc.). Sin embargo soporta otros sistemas de autenticación tales como TACACS+ y RADIUS. Cabe destacar que existen dos niveles de autenticación de usuario, el primero lo realiza el ISP antes de realizar el túnel y una vez creado, la segunda autenticación la realiza el Gateway o servidor corporativo.

4.4.1 Panorámica de L2TP

De una forma similar a PPTP, L2TP define dos entidades:

- **Concentrador de Acceso L2TP (LAC):** Este dispositivo se conecta a la red conmutada o PSTN. El LAC solo tiene que implementar el medio sobre el cual funciona L2TP para pasar el tráfico a uno o más LNS, además de canalizar (poner en túnel) todos los protocolos que sean transportados dentro de PPP. El LAC es el iniciador de todas las llamadas salientes y el receptor de las llamadas entrantes.
- **Servidor de Red L2TP (LNS):** Este servidor funciona en toda plataforma que soporte PPP. El LNS se encarga del lado del servidor del protocolo L2TP. Dado que L2TP se apoya exclusivamente en el medio sobre el cual llegan los túneles, el LNS puede tener una sola interfaz LAN o WAN, pero ser capaz de terminar las llamadas que lleguen en cualquier intervalo completo del LAC de las interfaces PPP. El LNS es el indicador de las llamadas salientes y el receptor de las entrantes.

Existen dos componentes paralelos de L2TP que funcionan sobre un túnel en concreto: los mensajes de control entre cada par LAC-LNS y los paquetes de sobre carga entre el mismo para LAC-LNS.

4.4.2 Panorámica de los Mensajes de Control L2TP

Antes de que se produzca el túnel PPP entre un LAC y un LNS, es necesario intercambiar mensajes de control entre ellos. Estos se intercambian sobre el mismo túnel que se usa para reenviar los datos de sobrecarga después de que haya pasado la información sobre control de llamada y administración L2TP. Los mensajes de control son los responsables del establecimiento, administración y liberación de las sesiones que se transportan a través del túnel, así como del estado del mismo.

Un túnel puede ser establecido por un LAC (para llamadas entrantes) o un LNS (para llamadas salientes). Siguiendo el establecimiento del túnel, el LNS y el LAC

lo configuran intercambiando mensajes de control. Cuando el mensaje de control se completa, el LAC puede iniciar sesiones indicando peticiones entrantes, o el LNS puede pedir llamadas salientes. Si ambos extremos del túnel tienen la capacidad de actuar como un LAC y un LNS a la vez, nada impide el establecimiento de llamadas entrantes o salientes desde ambos lados del mismo túnel.

4.4.3 Panorámica de los paquetes de sobrecarga L2TP

Una vez que se establece un túnel y cuando los mensajes de control han completado la configuración del túnel, éste puede ser usado para transportar paquetes PPP de sesión de usuario. El campo Call ID de la cabecera L2TP indica la sesión a la que pertenece un determinado paquete PPP.

De este modo los paquetes PPP son multiplexados sobre un túnel entre un determinado para LNS-LAC. El valor del campo Call ID se establece durante el intercambio de los mensajes de control de configuración de llamada.

Es normal que haya múltiples túneles en un determinado para LNS-LAC. Con múltiples túneles, es posible usar cada túnel para una sola sesión de usuario. L2TP proporciona un identificador de túnel, de forma que es posible identificar los túneles individuales, aunque procedan de un LAC o un LNS de origen único.

L2TP utiliza el puerto 1701 de UDP. El paquete L2TP completo, incluyendo la sobrecarga y la cabecera L2TP, es enviado en un datagrama UDP. El indicador de un túnel L2TP elige un puerto UDP de origen disponible y lo envía al destino deseado del puerto 1701. El destinatario elige un puerto libre en su propio sistema (puede ser el 1701 o cualquier otro) y envía su respuesta al puerto UDP del iniciador, estableciendo su propio puerto de origen UDP al puerto libre encontrado.

4.4.4 Escenario de ejemplo L2TP

La Figura 21 muestra un escenario L2TP de ejemplo en una empresa genérica. Los puntos más importantes que describen el ejemplo se enumeran a continuación:

- El usuario remoto inicia una conexión PPP con el ISP
- El LAC acepta la conexión y se establece el enlace PPP. L2TP también permite que el LAC compruebe la indicación de una llamada LNS antes de aceptarla.
- El ISP puede ahora realizar una autenticación parcial del sistema o usuario final. Alternativamente, el ISP puede haber determinado ya el LNS de destino a partir de la cadena de información de número de marcado (DNIS). Si el LNS desea aceptar la creación del túnel sin autenticación alguna del indicador de llamada, el LAC puede canalizar la conexión PPP sin haber llegado a comunicarse con el usuario remoto.
- Si no hay conexión de túnel con el LNS deseado, se iniciará una conexión. L2TP está diseñado para ser aislado de los detalles de los medios sobre los que se establece el túnel; L2TP solo requiere que los medio de túnel proporcionen conectividad orientada a los paquetes PPP. Ejemplos de tales medios son UDP y Frame Relay.
- Cuando el túnel existe, se asigna una ranura libre del túnel (un ID de llamada) y se envía una indicación de conexión para notificar al LNS esta nueva sesión. El LNS acepta la conexión o la rechaza.
- Si el LNS acepta la conexión, crea una interfaz virtual para PPP de una forma análoga a la que usaría en una conexión de marcado directo. Con esta interfaz virtual, las tramas de la capa de enlace podrán pasar por el túnel en ambas direcciones. Las tramas del usuario remoto son recibidas, encapsuladas en L2TP y reenviadas en el túnel apropiado. El LNS acepta estas tramas, elimina la encapsulación L2TP y las procesa como tramas entrantes normales para la interfaz y el protocolo apropiados. La interfaz virtual se comporta de manera muy parecida a una interfaz de hardware,

con la excepción de que, en este caso, está físicamente ubicado en el ISP. La otra dirección se comporta de manera análoga, con el LNS encapsulando el paquete L2TP y el LAC eliminando la encapsulación L2TP antes de enviar la interfaz física al usuario remoto.

- En este punto, la conectividad es una sesión PPP, cuyos puntos finales son, en un extremo, la aplicación VPN del usuario remoto y en el otro punto, la terminación de esta conectividad en el soporte PPP del LNS. Dado que el usuario remoto se ha convertido sencillamente en otro cliente de acceso telefónico del LNS, la conectividad del cliente podrá ser manipulada por medio de mecanismos tradicionales en relación a la autorización, el acceso de protocolo y el filtrado de paquetes.

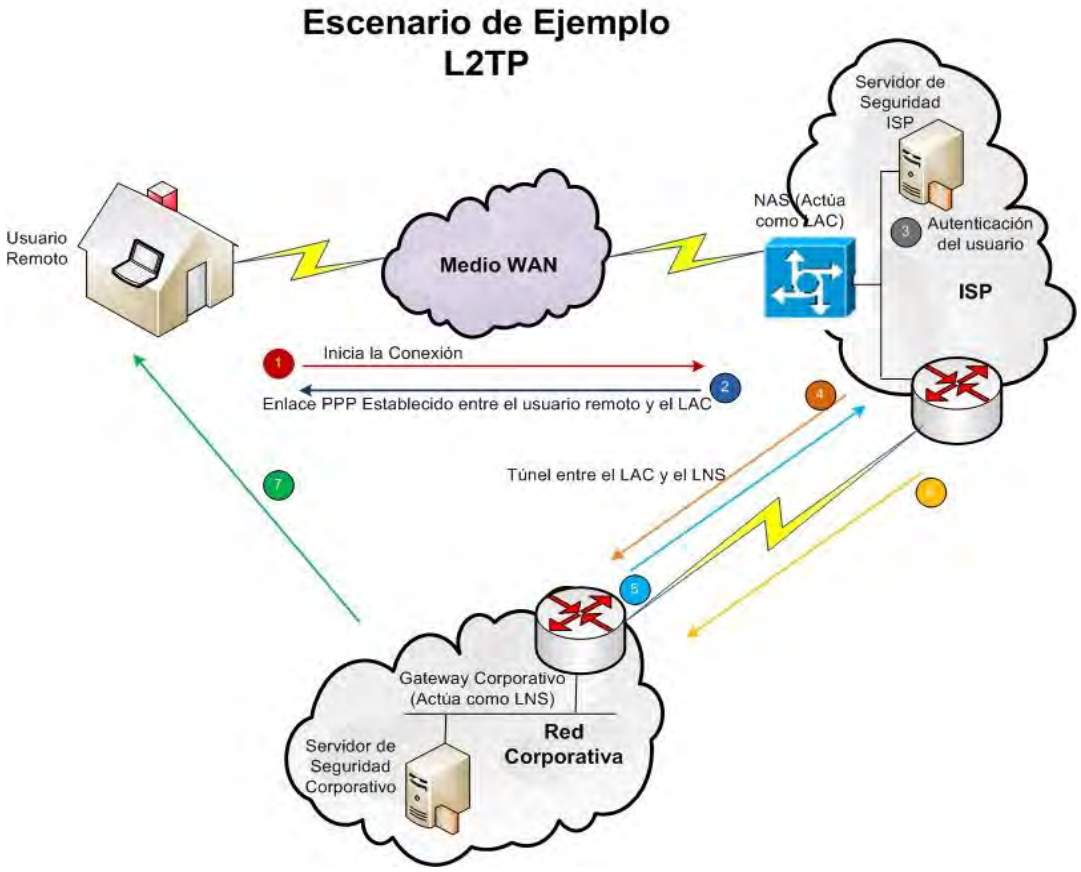

Figura 21 Escenario de ejemplo L2TP (Elaboración propia)

CAPÍTULO V

PROTOCOLOS VPN DE CAPA *3*

"Si quieres tener éxito en la vida, duplica tu porcentaje de fracasos."

Tom Watson

5.1 Protocolo de seguridad para redes IP (IPSec)

IPSec es un conjunto de estándares abiertos que proporcionan seguridad tanto al protocolo IP como a protocolos de capas superiores. Fue desarrollado en un principio para el nuevo estándar IPv6 y después fue adaptado a IPv4. La arquitectura IPSec se describe en el RFC-2401 de la IETF.

Este conjunto de estándares asigna al sistema donde se implementa servicios criptográficos de seguridad como autenticación, integridad, control de acceso y confidencialidad. Es implementado en la capa 3 (capa de red) del modelo OSI, de tal forma que su funcionamiento es bastante transparente al momento de llegar al nivel de aplicación, es decir se puede trabajar con HTTP, FTP, Telnet, SMTP, etc. IPSec es poderoso en comparación a las otras alternativas de túneles de seguridad.

Debido a que IPSec proporciona servicios de seguridad en la capa 3, permite al sistema donde se implementa seleccionar los protocolos de seguridad, determinar los algoritmos a utilizar e instalar cualquier criptografía de clave requerida. El conjunto de protocolos y/o mecanismos de seguridad IPSec empleados en cualquier conexión, y la forma en que se emplean, serán determinados por la seguridad y los requerimientos del sistema, aplicaciones, sitios u organizaciones.

Cuando estos mecanismos se implementan correctamente y se ejecutan, no afectan negativamente a los equipos de red, computadoras y otros componentes de Internet que no empleen estos mecanismos de seguridad para la protección de su tráfico. Estos mecanismos están diseñados para ser independientes del algoritmo. Esta modularidad permite seleccionar diferentes conjuntos de algoritmos sin afectar a las otras partes de la implementación. Por ejemplo, grupos diferentes de usuarios pueden seleccionar grupos diferentes de algoritmos si se necesita.

IPSec se puede utilizar para proteger una o más “trayectorias” entre un par de computadoras, o entre un par de Security Gateway o entre un Security Gateway y una computadora. Para efectos de esta unidad, el término Security Gateway se

utiliza para referirse a un sistema intermedio que implementa los protocolos IPSec, como podrían ser un router o un firewall fronterizos.

En el mundo de las VPN, IPSec crea túneles de trafico cifrados para conexiones punto a punto o simple cifrado entre computadoras. Sin embargo, su utilidad puede ir más allá de las VPN, ya que dentro de IPSec existe un registro central de intercambio de llaves de Internet IKE (Internet Key Exchange), con lo cual cada computadora en Internet podría comunicarse con otra usando cifrado y autentificación de alto nivel.

La Figura 22 describe brevemente y a grandes rasgos la función de IPSec, así como los componentes básicos que debe integrar.

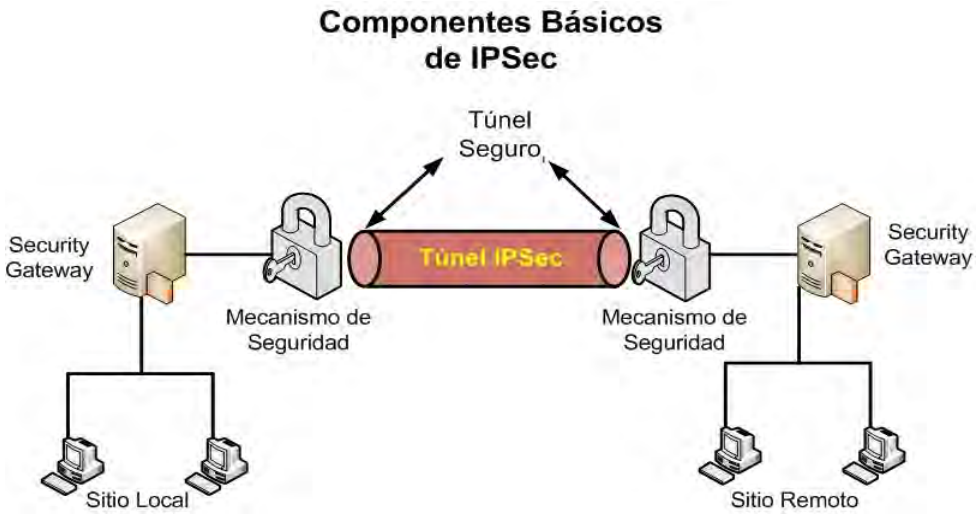

Figura 22 Componentes básicos de IPSec (Elaboración propia)

5.1.1 Servicios de Seguridad IPSec

La versión 4 del Protocolo de Internet (IPv4), no otorga por sí mismo ningún mecanismo de protección a las transferencias de datos, tampoco puede garantizar que el remitente sea quien dice ser. Por lo tanto, un buen mecanismo para remediar esta problemática es el uso de IPSec, ya que ofrece variedad de servicios de seguridad indispensables en toda transmisión de información confidencial. Así mismo, IPSec está diseñado para proporcionar seguridad de alta

calidad basada en criptografía tanto para IPv4 como IPv6. El conjunto de servicios de seguridad incluye:

- **Confidencialidad:** Asegura que los datos transmitidos puedan ser comprendidos únicamente por el emisor y el receptor. Esto evita que terceras personas puedan acceder a la información que se transmite por el medio.
- **Integridad:** Garantiza la exactitud de la información frente a perdidas, alteraciones o destrucción por usuarios mal intencionados o terceras personas.
- **Autenticidad:** Se logra mediante un mecanismo de firma digital, de modo que el receptor puede verificar que la firma corresponde a la persona o usuario que dice ser, con el fin de asegurar que los datos recibidos no son falsos.
- **Protección Anti-Replay (Réplica):** Asegura que un flujo de datos se enviado una sola vez, a menos que el reenvío sea autorizado.

5.1.2 Componentes de IPSec

IPSec protege los paquetes IP autenticándolos, cifrándolos o llevando a cabo ambas acciones, además de implementarse en la capa 3 del modelo OSI. Debido a esto, una aplicación de Internet puede aprovechar IPSec aunque no esté configurada para el uso del mismo. Cuando se utiliza correctamente, IPSec es una herramienta eficaz para proteger el tráfico entre redes o equipos.

La protección IPSec implica cinco componentes principales:

- **Protocolos de seguridad:** Conjunto de actividades programadas cuya función primordial es brindar protección a los datagramas IP. El Encabezado de Autenticación (AH) firma los paquetes IP y garantiza la integridad. El contenido del datagrama no está cifrado, pero el receptor tiene la seguridad de que el contenido del paquete no se ha modificado. El receptor también tiene la garantía de que los paquetes los ha enviado el remitente. La Carga de Seguridad Encapsulada (ESP) cifra los datos IP,

con lo cual codifica el contenido durante la transmisión de paquetes. ESP también pude garantizar la integridad de los datos mediante una opción de algoritmo de autenticación.

- **Asociaciones de seguridad (SA):** Especifica las propiedades de seguridad que se reconocen entre los equipos participantes en la comunicación (normalmente equipos cliente o Security Gateways). Una única SA protege los datos en una sola dirección. Dado que la mayoría de las comunicaciones son punto a punto o cliente servidor, debe haber dos SA para proteger el tráfico en ambas direcciones. Las asociaciones de seguridad se almacenan en una base de datos llamada SADB (Base de Datos de Asociaciones de Seguridad), la cual asocia un protocolo de seguridad con una dirección IP destino y un número de índice. El número de índice se denomina Índice de Parámetros de Seguridad (SPI). Estos tres elementos identifican de forma exclusiva a un paquete IPSec legítimo. La base de datos garantiza que el receptor reconozca un paquete protegido que llega a su destino. El receptor también utiliza información de la base de datos para descifrar la información, verificar que los paquetes no hayan sido nidificados, volver a ensamblar los paquetes y entregarlos en su destino final.
- **Mecanismo de seguridad:** Los algoritmos de autenticación y cifrado que protegen los datos de los datagramas IP.
- **Administración de claves:** Es la generación y distribución de claves para los algoritmos criptográficos y SPI. Una clave es una cadena alfanumérica secreta necesaria para leer, modificar o comprobar datos protegidos. Las claves se utilizan junto con algoritmos para proteger los datos.
- **Base de datos de directivas de seguridad (SPD):** Especifica el nivel de protección o políticas que determinan el tratamiento de todo tráfico de paquetes IP entrante o saliente de un equipo de cómputo o Security Gateway, según sea el caso. Un paquete puede descartarse, transferirse sin codificar o protegerse con IPSec. Para los paquetes salientes, SPD y SADB determinan el nivel de protección que será aplicado. Para los

paquetes entrantes, SPD determina si el nivel de protección del paquete es aceptable.

IPSec aplica los mecanismos de seguridad a los datagramas IP que se transfieren a la dirección de destino. El receptor utiliza la información de SADB para comprobar que los paquetes que llegan son legítimos y descifrarlos.

5.1.3 Encabezado de Autenticación (AH)

AH forma parte de la arquitectura de seguridad del Protocolo de Internet (IPSec) y está diseñado para proporcionar integridad y autenticación a los datagramas IP. Sin embargo, no proporciona ninguna garantía de confidencialidad, es decir, los datos transmitidos pueden ser vistos por usuarios no autorizados que estén presentes en el medio, ya que por sí mismo, AH no soporta forma alguna de cifrado. AH está orientado a mejorar la seguridad en situaciones en las que el uso de cifrado pueda ser ilegal o estar restringido a disposiciones del gobierno local.

5.1.3.1 Estructura de un Datagrama AH

Como se mencionó anteriormente, AH proporciona autenticación de datos, una integridad sólida y protección contra repetición. Esto se logra situando el encabezado AH entre el encabezado y la carga IP, como se muestra en la siguiente figura

.

Figura 23 Datagrama firmado con AH (Elaboración propia)

Es de suma importancia mencionar que la estructura descrita en la figura 4-2 puede variar de acuerdo a los modos de funcionamiento IPSec descritos más adelante en este capítulo.

El formato interno de AH se describe a continuación.

Figura 24 Estructura interna de AH (Elaboración propia)

- **Siguiente cabecera:** Identifica el tipo de dato de la carga útil, es decir, el campo que sigue después de AH. Su tamaño es de 8 bits.
- **Longitud de carga útil:** Es el campo de 8 bits que especifica la longitud o tamaño de AH.
- **Reservado:** Campo de 16 bits reservado para usos futuros, se debe establecer a 0.
- **Índice de parámetros de seguridad (SPI):** Es un numero arbitrario de 32 bits que define para el receptor el grupo de protocolos, algoritmos y claves de seguridad que se están usando, así como la duración de estas últimas y sus correspondientes iteraciones periódicas para prevenir posibles ataques. Generalmente, el SPI lo usa el receptor para conocer la asociación de seguridad desde la que se ha enviado un paquete.
- **Número de secuencia:** Es un campo de 32 bits que contiene el valor de un contador que aumenta por cada paquete enviado. El emisor debe incrementar este campo en cada paquete que envíe. Este campo no solo mantiene el orden, sino que también previene los ataques de repetición

(replay) que se originan cuando un atacante copia un paquete y lo envía fuera de secuencia para confundir a los extremos. La función anti-replay es opcional ya que va implícita en el datagrama firmado con AH y el extremo receptor decide si hace uso de ella mediante una previa configuración. Aunque por su longitud de 32 bits puede llegar a 4300 millones antes de volver a comenzar, los contadores tanto del emisor como receptor deben ser restablecidos antes de alcanzar el máximo, esto implica establecer una nueva llave.

- **Datos de autenticación:** Este campo contiene el código para la autenticación del mensaje basado en resúmenes (HMAC). Este HMAC protege la integridad de los paquetes ya que solo los miembros de la comunicación que conozcan la clave secreta puedan crear y comprobar HMACs.

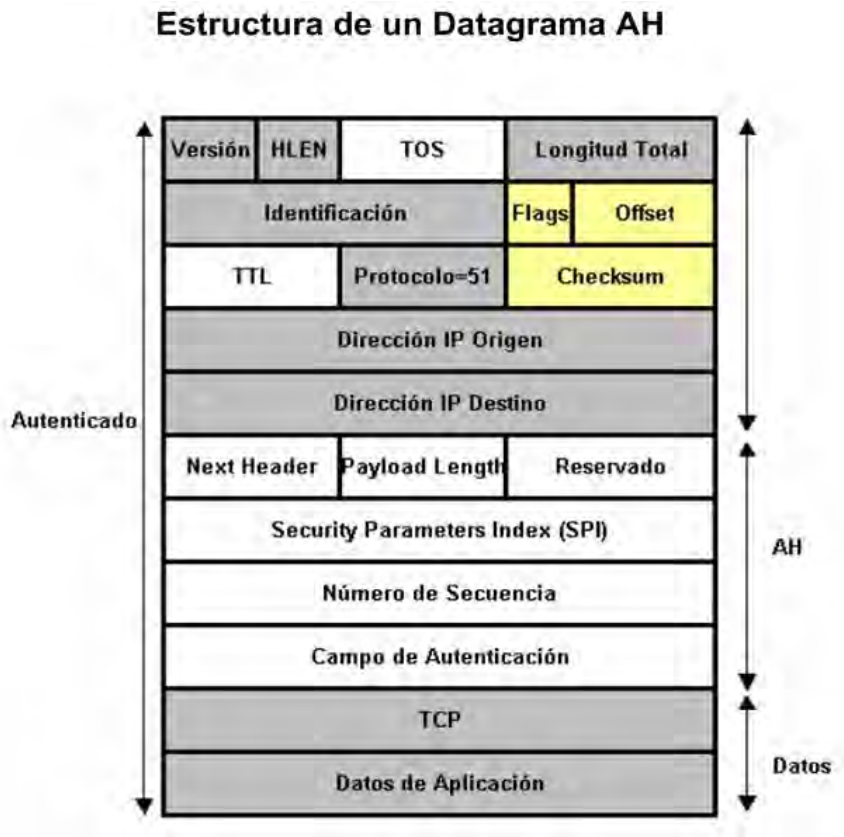

Figura 25 Estructura de un datagrama AH

Es importante destacar, como se observa en la Figura 25, que AH asegura la integridad y autenticidad de los datos transportados y de la cabecera IP, excepto los campos variables: TOS, TTL, Flags, offset y checksum.

Para proteger la integridad del datagrama IP, AH calcula una HMAC basada en la clave secreta, el contenido del paquete y las partes inmutables de la cabecera IP (como son las direcciones IP). Una vez que ambos extremos han establecido una SA, utilizan la clave acordada durante el intercambio inicial para generar los resúmenes que se incluyen en las cabeceras AH. Solo ambos extremos conocedores de la clave podrán calcular los resúmenes y verificar la integridad del paquete. Del mismo modo, un resumen que corresponde con el contenido de un paquete garantiza la autenticidad del emisor, ya que solo este conocerá la clave que la se genera el resumen.

5.1.3.2 HMAC (Hash Message Authentication Code)

El funcionamiento de AH se basa en un algoritmo HMAC, que corresponde a un código para autenticación de mensajes basado en resúmenes.

Este mecanismo consiste en aplicar una función hash a la combinación de un porcentaje de los datos a transmitir y una clave secreta, siendo el resultado un código alfanumérico. Este resultado tiene la propiedad de ser un distintivo del extremo que está transmitiendo, debido a que solo él y el receptor conocen la clave para generar HMACs. De esta forma se asegura que el mensaje enviado proviene del origen esperado y además que el contenido es íntegro.

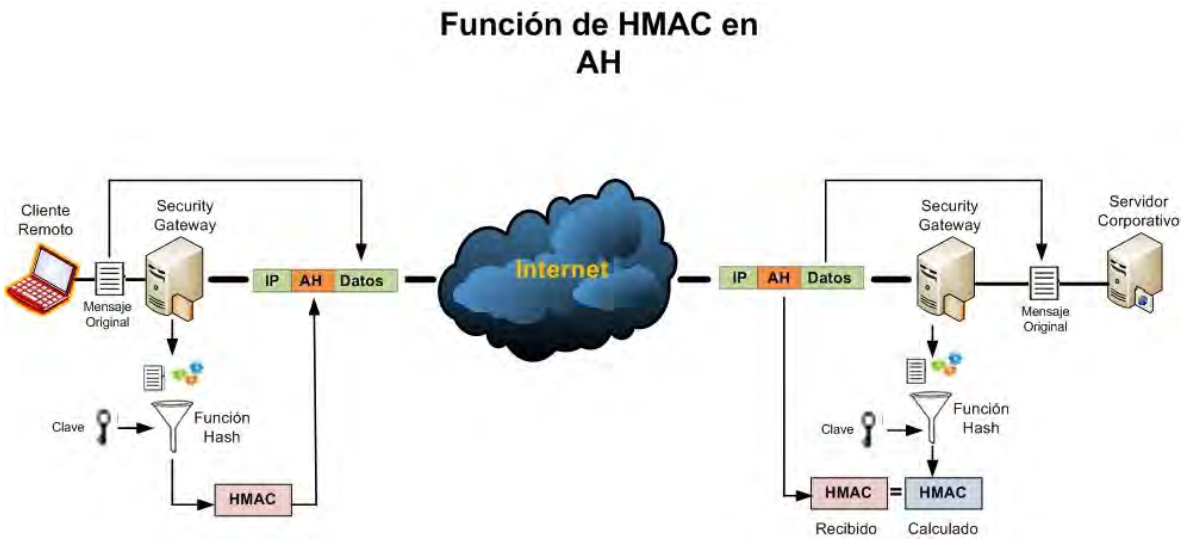

Figura 26 Función HMAC en AH (Elaboración propia)

En la Figura 26 es posible observar detalladamente el proceso de empaquetado y desempaquetado que se lleva a cabo en los equipos que utilizan cabeceras de autenticación (AH). Dicho proceso consiste básicamente en tres pasos principales:

- El emisor calcula un “extracto” del mensaje original, el cual se copia en uno de los campos de la cabecera AH, específicamente en el campo “Datos de Autenticación”.
- El paquete construido se envía a través de la red.
- En el extremo receptor se repite el cálculo del “extracto” y el resultado es comparado con el recibido en el paquete.

Si son iguales el receptor tendrá la seguridad de que el paquete IP no ha sido modificado durante su recorrido por la red y que proviene efectivamente del origen esperado. Es importante reiterar que el “extracto” (HMAC) es imposible de calcular si no se conoce la clave con la que fue calculado y que solo el emisor y el receptor conocen.

5.1.3.3 Funciones Hash

Hash es una suma de comprobación criptográfica o un código de integridad de mensaje que tanto el emisor y el receptor deben calcular para comprobar el

mensaje. Por ejemplo, el equipo remitente utiliza una función hash en conjunto con una clave para calcular la suma de comprobación del mensaje y la incluye en el paquete. El equipo receptor debe calcular la misma función hash (usando la clave compartida por ambos participantes) sobre el mensaje recibido y comparar el resultado que se incluye en el paquete del remitente. Si el mensaje ha cambiado durante el trayecto, los valores de hash serán diferentes y el paquete será descartado.

Para hacer posible la parte de autenticación e integridad se han definido dos algoritmos o funciones hash y es considerado obligatorio el uso de al menos uno de ellos para poder implementar IPSec sobre HMAC.

SHA1 (Secure Hash Algorithm 1) y MD5 (Message Digest 5) producen una representación única comprimida o codificada de 160 y 128 bits respectivamente, correspondiente al datagrama que se desea transmitir. Si estas representaciones son iguales entre el emisor y el receptor, entonces el bloque de datos no sufrió alteración alguna durante la transmisión. Luego se decodifica la representación para llegar al mensaje original.

La autenticación es garantizada mediante el uso de claves secretas cuando es calculado el mensaje codificado (representación codificada). Esta clave solo es conocida por el emisor y el receptor. Dicha clave corresponde a una serie de fragmentos de 16 bits por cada 64 bytes del datagrama a transmitir que debe ser calculado por los extremos. La serie formada por los fragmentos 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.

5.1.3.4 Método de Operación Hash

Los datos enviados electrónicamente pueden deformarse por intervención de terceras personas, o bien por errores en la transmisión. Para evitar esto y asegurar tanto la autenticidad como la integridad de la información se utilizan funciones hash.

Un ejemplo de cómo trabajan este tipo de funciones es utilizando un modo de sustitución, para luego a la información resultante aplicarle una función matemática con el objetivo de obtener la clave del bloque de datos, tal como se muestra a continuación:

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

Figura 27 Método de sustitución Hash (Elaboración propia)

Esta sustitución es básicamente la codificación ASCII, la cual se puede utilizar para fines de ejemplo.

Suponiendo que la información a transmitir es la siguiente frase “LAS EMPRESAS PUEDEN COMUNICARSE EN FORMA REMOTA”, donde cada letra se representa por su equivalente de la tabla y los espacios entre palabras se representan por el número 32, según el código ASCII.

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

- (1°-2°)*3°= Resultado Numérico.

Ejemplo de Sustitución Hash

L	A	S		E	M	P	R	E	S	A	S		P	U
76	65	83	32	69	77	80	82	69	83	76	83	32	80	85
		913			-2849			-138			581			-4080
E	D	E	N		C	O	M	U	N	I	C	A	R	S
69	68	69	78	32	67	79	77	85	78	73	67	65	82	83
		69			3082			170			335			-1411
E		E	N		F	O	R	M	A		R	E	M	O
69	32	69	78	32	70	79	82	77	65	32	82	69	77	79
		2553			3220			-231			2706			-632
T	A													
84	65	32												
		608												

Figura 28 Ejemplo de sustitución Hash (Elaboración propia)

Posteriormente se realiza la suma de todos los resultados: (913 – 2849 – 138 + 581 – 4080 + 69 + 3082 + 170 + 335 – 1411 + 2553 + 3220 – 231 + 2706 – 632 + 608) = 4896. Entonces junto a la frase a transmitir se adjunta el resultado de la operación hash. Si los resultados coinciden se puede asegurar que los datos no han sufrido alteraciones.

5.1.4 Carga de seguridad encapsulada (ESP)

La cabecera ESP está diseñada para brindar una combinación de servicios de seguridad que se pueden aplicar solos, en combinación con AH o de forma anidada. ESP se inserta después de la cabecera IP y antes de la cabecera del protocolo de capa superior (modo transporte), o antes de una cabecera IP encapsulada (modo túnel).

El objetivo primordial es proporcionar confidencialidad, para ello especifica el modo de cifrar los datos que se desean enviar y como este contenido cifrado se incluye en un datagrama IP. Adicionalmente, puede ofrecer los servicios de integridad y autenticación, incorporando un mecanismo similar al de AH.

5.1.4.1 Estructura de un datagrama ESP

Como se muestra en la siguiente figura, ESP solo protege los datos que siguen a su inicio en el datagrama:

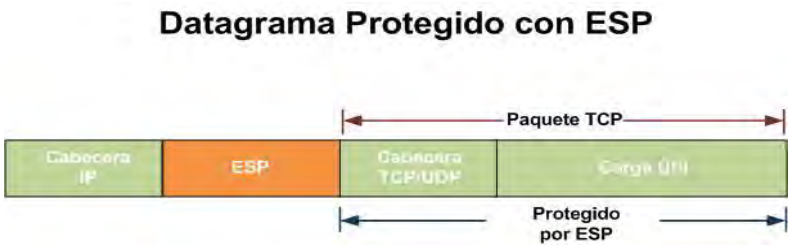

Figura 29 Datagrama protegido con ESP

ESP puede asegurar la integridad del paquete empleando una HMAC y la confidencialidad empleando cifrado. La cabecera ESP se genera y añade al paquete tras cifrarlo y calcular su HMAC.

Dado que ESP proporciona más funciones que AH, el formato de la cabecera es más complejo; este formato consta de una cabecera y una cola que rodean los datos transportados. Dichos datos pueden ser cualquier protocolo IP.

En la Figura 30 se muestra la estructura de una datagrama ESP, en la que se observa como el contenido o carga útil viaja cifrada.

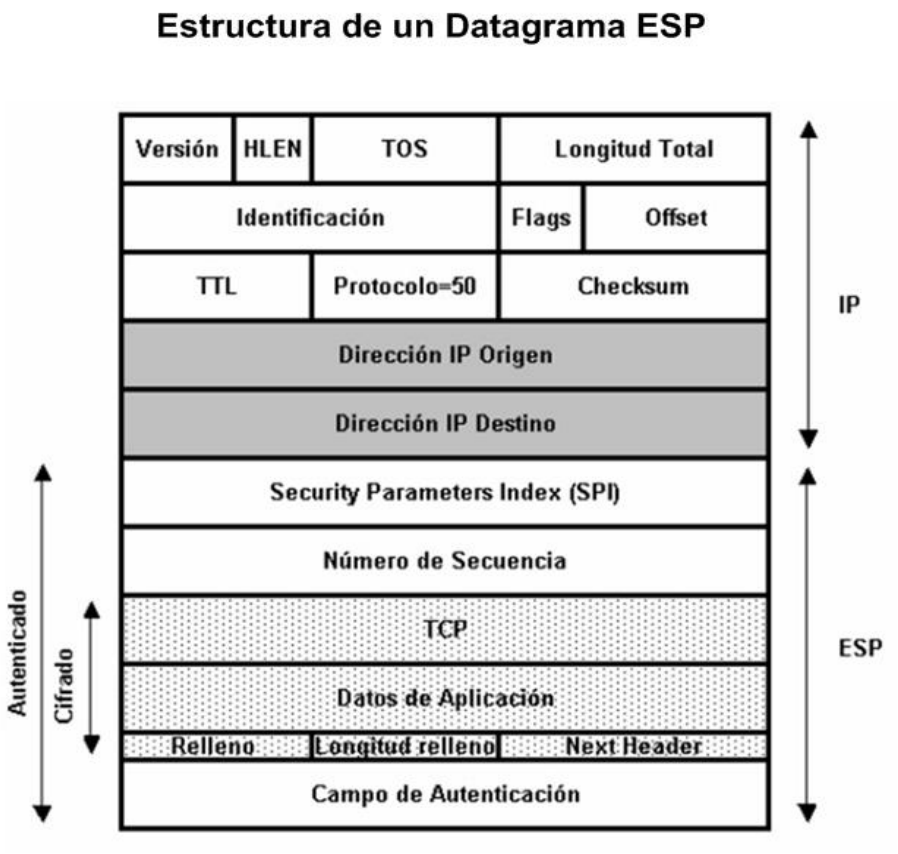

Figura 30 Estructura de datagrama ESP

- **Índice de parámetros de seguridad (SPI):** Al igual que en AH, el campo SPI define para el receptor el grupo de protocolos, algoritmos y claves de seguridad que se están usando, así como la duración de estas últimas y sus correspondientes iteraciones periódicas para prevenir posibles ataques. Generalmente lo usa el receptor para conocer la asociación de seguridad desde la que se ha enviado un paquete y de esta forma poder abrirlo.
- **Número de secuencia:** De la misma forma que en AH, este campo contiene el valor de un contador que aumenta por cada paquete enviado. El emisor debe incrementar este campo en cada paquete que envíe. Este campo no solo mantiene el orden, sino que también previene los ataques de repetición (replay).
- **Datos de aplicación:** Dentro de este campo se encuentran los datos cifrados.

- **Relleno:** IPSec emplea cifradores de bloque para el proceso de cifrado, debido a ello puede ser necesario rellenar la carga del paquete, esto si la longitud de la carga no es múltiplo de la longitud del paquete.
- **Longitud de relleno:** Indica la longitud del campo anterior.
- **Siguiente cabecera:** Este campo identifica el tipo de dato que de la carga útil, es decir, identifica al protocolo de la capa superior (ICMP, TCP, UDP, etc.).
- **Campo de Autenticación**: Este campo contiene el resultado del algoritmo de autenticación que servirá al receptor para compararlo con el que obtenga luego de aplicar la misma función hash al datagrama.

5.1.4.2 Cifrado ESP

La función de cifrado dentro del protocolo ESP es desempeñada por un algoritmo de cifrado de clave simétrica. Típicamente se usan algoritmos de cifrado por bloques, de modo que la longitud de los datos a cifrar tiene que ser un múltiplo del tamaño de bloque (8 o 16 bytes en la mayoría de los casos). Debido a esto existe un campo de relleno (analizado anteriormente), el cual tiene una función adicional: es posible añadir caracteres de relleno al campo de datos para ocultar su longitud real y con esto las características del tráfico. En la Figura 31 se representa como el protocolo ESP permite enviar datos de forma confidencial.

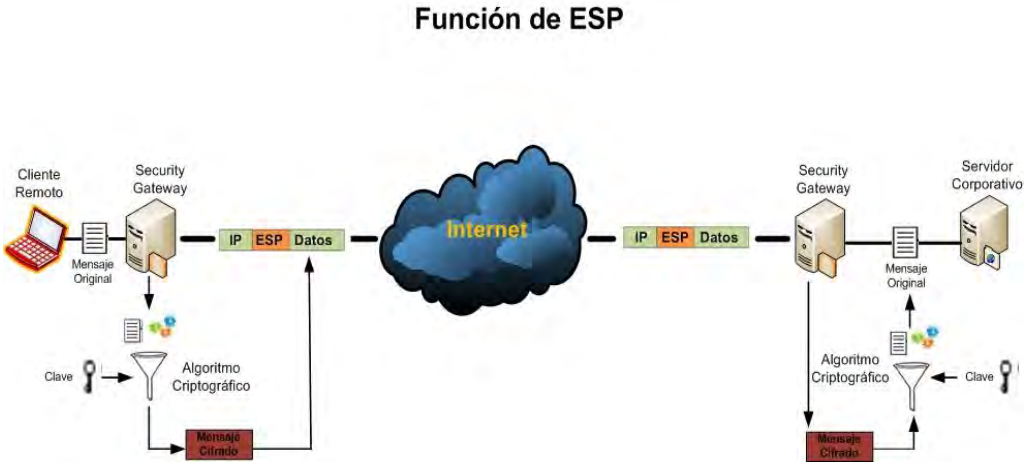

Figura 31 Funcionamiento de ESP (Elaboración propia)

Como es posible observar en la figura anterior, el emisor toma el mensaje original, lo cifra utilizando una clave determinada para incluirlo en un paquete IP, a continuación de la cabecera ESP. Durante el transito hasta su destino, si el paquete es interceptado por un tercero solo obtendrá un conjunto de bits ilegibles. En el destino, el receptor aplica de nuevo el algoritmo de cifrado con la misma clave, recuperando los datos originales.

La distribución de claves de forma segura es, por consiguiente, un requisito esencial para el funcionamiento de ESP tal y como hemos visto anteriormente. También es fundamental que tanto el emisor como el receptor estén de acuerdo con el algoritmo de cifrado y el resto de parámetros comunes que utilizan. Esta labor de puesta en contacto y negociación es realizada por un protocolo de control, denominado IKE y será explicado más adelante.

5.1.4.3 Tipos de Cifrado

- **Cifrado por sustitución**

En el cifrado por sustitución, cada letra o grupo de letras se sustituye por otra letra o grupo de letras para disfrazarlas. El cifrado más antiguo que se conoce es el cifrado de César, atribuido a Julio César. En este método se reemplaza una letra del alfabeto por la 3° que le sigue, entonces, por ejemplo, la palabra “gato” se representa por JDWR. Una sencilla generalización del cifrado de César permite que el alfabeto cifrado se pueda desplazar k letras, en lugar de que siempre sean 3. En este caso, k se convierte en una clave para el método general de alfabetos desplazados circularmente. 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 monoalfabética, en donde la clave está constituida por la cadena de 26 letras, correspondientes al alfabeto completo.

- **Cifrado por transposición o permutación**

A diferencia del cifrado por sustitución, el de transposición rodea las letras pero no las disfraza. En la siguiente figura se describe a detalle el cifrado por transposición común, el de tipo columna. La clave para el cifrado es una palabra o frase que no tiene ninguna letra repetida. En este ejemplo la clave es: “MEGAUPLO” y el texto a transmitir es: “necesita lanzar sus nuevos servicios al mercado antes que sus co”.

Ejemplo de Cifrado por Transposición

M	E	G	A	U	P	L	O
5	2	3	1	8	7	4	6
n	e	c	e	s	i	t	a
	l	a	n	z	a	r	
s	u	s		n	u	e	v
o	s		s	e	r	v	i
c	i	o	s		a	l	
m	e	r	c	a	d	o	
a	n	t	e	s		q	u
e		s	u	s		c	o

Figura 32 Ejemplo de cifrado por transposición

El propósito de la clave es numerar las columnas, en donde la columna 1 queda bajo la letra de la clave que se encuentra más próxima al comienzo del alfabeto y así sucesivamente. El texto en claro que se desea transmitir se escribe horizontalmente en renglones. El texto cifrado se lee por columnas, comenzando con la columna cuya letra clave tiene el valor inferior.

Texto en claro: *"necesita lanzar sus nuevos servicios al mercado antes que sus co".*

Texto Cifrado: *"en ssceuelusien cas ortstrevloqcn socmaea vi uoiaurad szne ass".*

En el ejemplo anterior se puede percibir que con este método de cifrado solo se desordena la frase con la palabra clave previamente acordada. La tecnología de clave proporciona servicios de cifrado que aseguran las transmisiones en entornos abiertos.

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

- **Cifrado simétrico**

A los métodos de cifrado de clave privada se les denomina códigos simétricos y consisten en codificar la información con una clave que tanto el emisor como el receptor conocen y mantienen en privado. Una vez cifrado el mensaje, es ilegible y puede ser transmitido por medios poco seguros. Este sistema da por hecho que dicho intercambio de clave ha sido realizado por algún medio seguro, pudiéndose utilizar para ello métodos de claves públicas en conjunción con los métodos de claves privadas.

- **Cifrado asimétrico**

Por otra parte, los métodos de cifrado de clave pública o códigos asimétricos consisten en la creación de dos claves relacionadas para cada usuario. Una se mantendrá en privado y la otra se usará públicamente. Cuando un usuario desea enviar un mensaje confidencial a otro usuario, cifra el mensaje con la clave pública del receptor y luego el receptor decodifica el mensaje con su clave privada. Los mensajes cifrados con una clave pública solo pueden ser descifrados con una clave privada. Es conveniente señalar que si alguna parte de la información o de la firma es modificada, aunque sea ligeramente, entonces el procedimiento de

autenticación indicará que el documento no es auténtico. Si una llave pública autentica un documento firmado, entonces quiere decir que el documento fue firmado con la correspondiente llave privada.

5.1.5 Algoritmos de cifrado

Para cifrar los datos, el protocolo ESP puede utilizar diversos algoritmos de cifrado los cuales tienen funciones que difieren escasamente entre sí, por lo tanto a continuación se analizan los más importantes:

5.1.5.1 DES (Estándar de Encriptación de Datos)

Creado en 1977 con el objetivo de proporcionar al público en general un algoritmo de cifrado normalizado para redes de computadoras. Se basa en un sistema monoalfabético, con un algoritmo de cifrado que consiste en la aplicación sucesiva de varias permutaciones y sustituciones.

Inicialmente el texto en claro a cifrar se somete a una permutación o método de transposición, con bloque de entrada de 64 bits (o múltiplo de 64), para posteriormente ser sometido a la acción de dos funciones principales, una función de permutación con entrada de 8 bits y otra de sustitución con entrada de 5 bits, en un proceso que consta de 16 etapas de cifrado.

En general, DES utiliza una clave simétrica de 64 bits, de los cuales 56 son usados para la encriptación, mientras que los 8 restantes son de paridad y se usan para la detección de errores en el proceso.

Como la clave efectiva es de 56 bits, es posible obtener un total de 2 elevado a 56 claves posibles, que en pocas palabras son alrededor de 72000 billones de claves, por lo que la ruptura del sistema por métodos como la fuerza bruta o diccionario es sumamente improbable, aunque no imposible si se dispone de suerte y una gran potencia de cálculo. Sin embargo, en la actualidad el sistema de cifrado DES se considera poco práctico debido a que produce una longitud de clave corta e invariable y los nuevos equipos pueden llegar a tener la potencia para descifrarlas.

Figura 33 Mensajes con DES (Elaboración propia)

5.1.5.2 3DES (Triple DES)

Para solventar el problema del cifrado DES, se creó 3DES o también llamado Triple DES, basado en tres iteraciones sucesivas del algoritmo DES, con lo que se consigue una longitud de clave de 128 bits y que es compatible con DES simple.

Este hecho se basa en que DES tiene la característica matemática de no ser un grupo, lo que implica que si se cifra el mismo bloque dos veces con llaves distintas se aumenta el tamaño efectivo de la llave.

Para implementarlo, se toma una clave de 128 bits y se divide en dos diferentes de 64 bits, aplicándose el siguiente proceso al texto en claro:

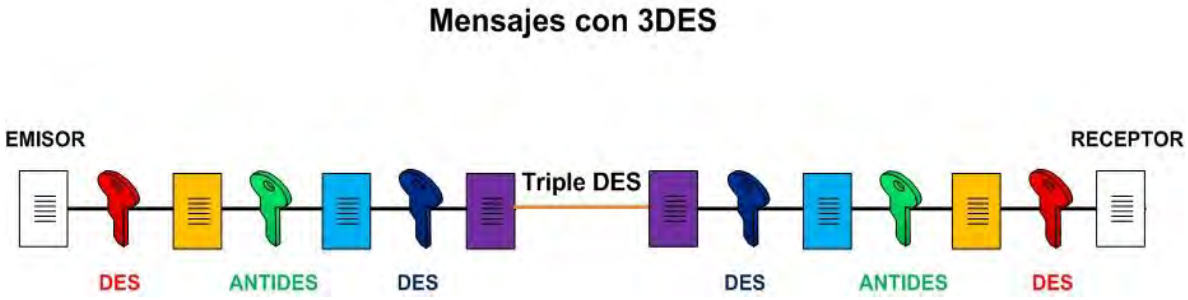

Figura 34 Mensaje con 3DEs (Elaboración propia)

A continuación se describe brevemente el proceso de cifrado de la Figura 34:

- En primer término se aplica al documento en blanco un primer cifrado o encriptación mediante la primera clave, que para este ejemplo llamaremos C1.

- Al resultado (ANTIDES) se aplica un segundo cifrado con la segunda clave, C2.
- Y a este último resultado se le vuelve a aplicar la clave inicial C1, produciéndose de esta forma un tercer cifrado.
- En el extremo RECEPTOR se aplica el proceso inverso para descifrar el mensaje original.

En caso de que la clave de 128 bits esté formada por dos claves iguales de 64 bits, es decir C1=C2, el sistema se comporta como un proceso DES simple.

5.1.6 Modos de funcionamiento IPSec

En primer lugar, para describir los modos de funcionamiento de IPSec se debe entender ampliamente el proceso de encriptación:

- Encapsular en el campo de carga útil de ESP: Para ***modo transporte,*** solo la información original del protocolo de capa superior, es decir los datos de TCP o UDP. Para ***modo túnel*** el datagrama IP original completo.
- Agregar el relleno necesario.
- Cifrar el resultado (carga útil de datos, relleno, longitud del relleno y la siguiente cabecera) usando la llave, el algoritmo criptográfico, el modo indicado en la SA y si existe, datos de sincronización criptográfica.

En la parte del receptor se sigue en general el siguiente procedimiento para “abrir” los paquetes recibidos:

- Descifrar la carga útil de ESP, relleno, longitud del relleno y siguiente cabecera, utilizando la llave, el algoritmo criptográfico, el modo y en su caso los datos de sincronización criptográfica indicados en la SA.
- Procesar el relleno según haya sido especificado por el algoritmo utilizado.
- Reconstruir el datagrama IP original: Para ***modo transporte,*** el encabezado IP original más la información del protocolo de capa superior original en el campo de carga útil de ESP. Para ***modo túnel*** el encabezado

IP encapsulado, más el datagrama IP completo en el campo de carga útil de ESP.

Es importante mencionar que el proceso de encriptación no debe ser sustituto del de autenticación, ya que el segundo es un servicio básico de una comunicación segura, reforzada con la encriptación de datos.

Una vez explicado el proceso de encriptación y su inverso, es posible plantear los modos de operación de IPSec.

El diseño de IPSec contempla dos modos de funcionamiento para sus protocolos:

- **Modo transporte.**
- **Modo túnel.**

La diferencia entre estos dos modos radica en la unidad que se esté protegiendo. En el modo transporte se protege la carga útil (capa trasporte), en el modo túnel se protegen los paquetes (capa de red) y es posible implementar tres combinaciones con los protocolos de IPSec: AH en modo transporte, ESP en modo transporte y ESP en modo túnel.

5.1.6.1 Modo transporte

El modo transporte es el predeterminado para IPSec, por lo que en esta modalidad los protocolos AH y ESP transportan dentro de sus datagramas datos de la capa de transporte (por ejemplo datos TCP o UDP). Por lo tanto, la cabecera IPSec se inserta inmediatamente a continuación de la cabecera IP (otorgada por la capa de red) y antes de los datos de niveles superiores que se desean proteger. El modo transporte tiene la ventaja de asegurar la comunicación extremo a extremo (punto a punto), pero requiere que ambos extremos entiendan y ejecuten el protocolo IPSec.

Si la política de seguridad define que los paquetes deben ser cifrados, se utiliza ESP en modo transporte. En caso que solo se requiera la autenticación, se utiliza AH en modo transporte.

En la Figura 35 se representan dos equipos de cómputo que ejecutan IPSec. Por ejemplo, Alicia en la PC1 envía información a Benito en la PC2, por lo tanto la carga IP está cifrada y firmada para garantizar su integridad. Al recibirse una vez completado el proceso de comprobación de integridad, se descifra la carga de datos del paquete. Benito puede estar seguro de que fue Alicia quién le envió la información, que la misma no ha sufrido cambios y que nadie más ha podido leerla.

Figura 35 Modo de transporte entre equipos IPSec (Elaboración propia)

5.1.6.2 Modo túnel

En el modo túnel el contenido del datagrama AH o ESP es un datagrama IP completo, incluida la cabecera IP original. Así, se toma un datagrama IP al cual se añade inicialmente una cabecera AH o ESP, posteriormente se añade una nueva cabecera IP que es la que se utiliza para poner en ruta los paquetes a través de la red. El modo túnel se usa normalmente cuando el destino final de los datos no coincide con el dispositivo que realiza las funciones IPSec.

El modo túnel es usado mayormente por los Gateways IPSec (Gateways de seguridad), con el objetivo de identificar la red que protegen bajo una misma dirección IP y centralizar de este modo el procesado del trafico IPSec en un equipo. El modo túnel también es útil cuando se utiliza junto con ESP para ocultar la identidad de los nodos que se están comunicando. Otra aplicación del modo túnel, tanto con ESP como con AH, es poder establecer Redes Privadas Virtuales

(VPN) a través de redes públicas, es decir, interconectar de forma segura redes de área local, incluso en el caso de que estas usen direccionamiento privado o no legal en internet. IPSec puede ser implementado bien en un host o en un equipo dedicado, tal como un router o un firewall, que cuando realiza estas funciones se denomina Gateway de seguridad o Gateway IPSec.

En la Figura 36 se muestran dos redes locales que utilizan dos Gateways IPSec para conectarse entre sí y por lo tanto una implementación en modo túnel. También es posible observar que la comunicación entre los equipos de cómputo se realiza a través de una red pública como es internet, por lo que los Gateways IPSec crean un túnel entre sí a través del cual viajan protegidos los datos que intercambian ambos equipos.

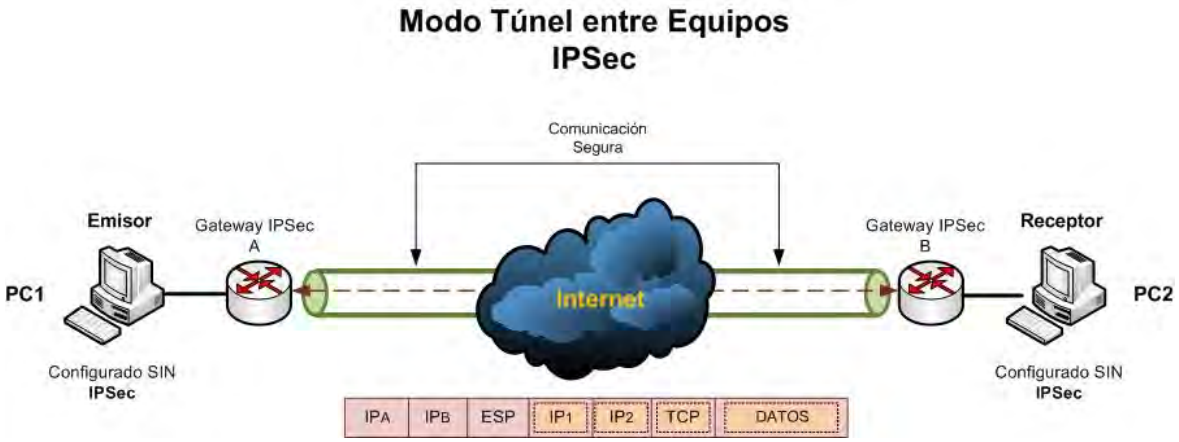

Figura 36 Modo túnel entre equipos IPSec (Elaboración propia)

Como es posible observar en la figura anterior, ambos equipos de cómputo envían y reciben el tráfico en claro, como si estuviesen situados en la misma red local. Este esquema tiene la ventaja de que los nodos situados en redes separadas pueden comunicarse de forma segura y transparente, concentrando al mismo tiempo las funciones de seguridad en un único punto, facilitando de esta forma las labores de administración.

5.2 Asociaciones de seguridad (SA)

Una asociación de seguridad (SA) es el contrato entre dos entidades que deseen comunicarse en forma segura. Las SA determinan los protocolos a utilizar, las transformaciones, las llaves y la duración de la validez de dichas llaves. Esta información SA es almacenada en bases de datos dentro de los dispositivos y tiene la característica de ser de un solo sentido, es decir cada equipo o red con IPSec tendrá tanto una SA para el tráfico que entra como una SA para el tráfico que envía a otras entidades.

Como se mencionó anteriormente, ambos extremos de una asociación de seguridad deben tener conocimiento de las claves, así como del resto de la información que necesitan para enviar y recibir paquetes protegidos por AH o ESP. Así mismo es necesario que ambas entidades estén de acuerdo tanto en los algoritmos criptográficos a emplear como en los parámetros de control. Esta operación puede realizarse mediante una configuración manual o mediante algún protocolo de control que se encargue de la negociación automática de los parámetros necesarios.

En el campo Índice de Parámetros de seguridad SPI de las cabeceras AH y ESP, se especifican las asociaciones de seguridad únicas que se utilizaran entre las dos entidades para lograr la comunicación segura. Este mecanismo está concebido para que en una comunicación segura, la fuente identifique cual SA utilizar para asegurar un paquete por enviar y el destino identifique cual SA utilizar para verificar la seguridad del paquete recibido.

5.2.1 Protocolo IKE (Intercambio de Claves en Internet)

El IETF ha definido al protocolo IKE para realizar tanto esta función de gestión automática de claves como el establecimiento de las asociaciones de seguridad correspondientes. La utilidad de IKE no se limita únicamente a IPSec, sino que es un protocolo estándar de gestión de claves que podría ser útil en otros protocolos como por ejemplo OSPF y RIPv2.

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

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

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

5.2.1.1 Primera fase IKE

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

- El primer método de autenticación se basa en el conocimiento de un secreto compartido que, como su propio nombre indica, es una cadena de caracteres que únicamente conocen los dos extremos que quieren establecer una comunicación IPSec. Mediante el uso de funciones hash cada extremo demuestra al otro que conoce el secreto sin revelar su valor; de esta forma ambos se autentican mutuamente. Para no debilitar la seguridad de este mecanismo de autenticación, debe configurarse un secreto distinto para cada extremo, por lo que el número de secretos crece muy rápidamente cuando aumenta el número de equipos que desean establecer una comunicación IPSec. Debido a lo anterior, en entornos en los que se desea interconectar muchos equipos IPSec la gestión de claves es muy complicada. En este caso no se recomienda el uso de autenticación

mediante secreto compartido, sino autenticación basada en certificados digitales.

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

5.2.1.2 Segunda fase IKE

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

Durante esta fase se negocian las características de la conexión ESP o AH y todos los parámetros necesarios. El equipo que ha iniciado la comunicación ofrecerá todas las posibles opciones que tenga configuradas en su política de seguridad y con la prioridad que se hayan configurado. El sistema receptor aceptará la primera que coincida con los parámetros de seguridad que tenga definidos. Así mismo, ambos extremos se deben informar entre sí del tráfico que van a intercambiarse a través de dicha conexión.

En la figura 4-16 se muestra el modo de operación del protocolo IKE y la forma en la que se obtiene una clave de sesión, que es la que se utiliza para proteger las conexiones ESP o AH según sea el caso.

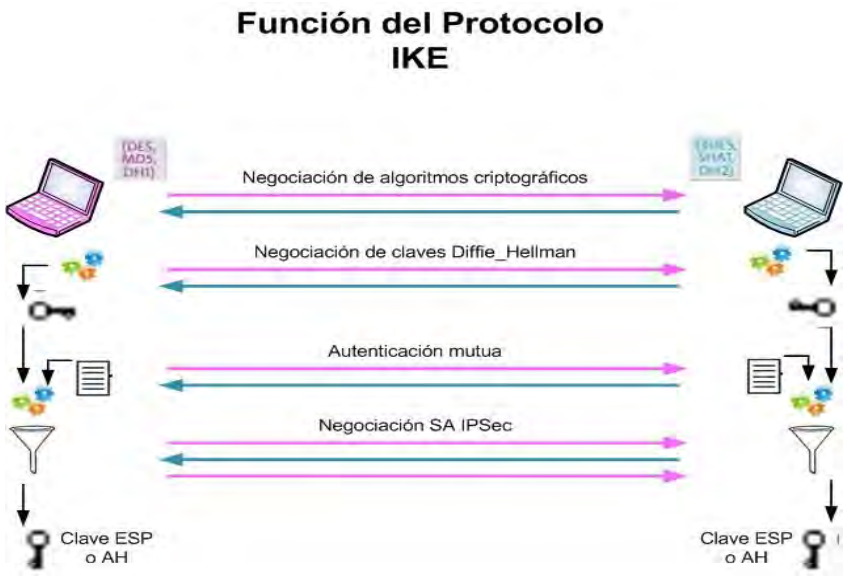

Figura 37 Función del protocolo IKE (Elaboración propia)

5.3 Servicios de seguridad ofrecidos por IPSec

Como se menciona en líneas anteriores, IPSec ofrece diversos servicios de seguridad según sus modos de operación y protocolos involucrados en la implementación. Dichos servicios se describen a continuación.

5.3.1 Integridad y autenticación

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

5.3.2 Confidencialidad

Este servicio se obtiene mediante la función de cifrado incluida en el protocolo ESP. En este caso es recomendable activar la opción de autenticación, ya que si no se garantiza la integridad de los datos el cifrado es inútil. Esto es debido a que aunque los datos no pudiesen ser interceptados por nadie durante el tránsito,

estos podrían ser alterados haciendo llegar al receptor una serie de datos sin sentido que en su momento podrían ser aceptados como tráfico valido.

Además de ofrecer el cifrado del tráfico, el protocolo ESP también tiene herramientas para ocultar el tipo de comunicación que se está realizando; para ello permite introducir caracteres de relleno en el contenido de los datos del paquete de modo que se oculta la verdadera longitud del mismo. Esta es una protección útil contra las técnicas de análisis de tráfico, que permiten a un atacante deducir información útil a partir del estudio de las características del tráfico cifrado. El análisis del tráfico es un riesgo que debe considerarse seriamente ya que recientemente se ha documentado la viabilidad para deducir información a partir del tráfico cifrado de una conexión SSH.

5.3.3 Detección de repeticiones

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

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

5.3.4 Control de acceso

Involucra autenticación y autorización, dado que el uso de ESP y AH requiere el conocimiento de claves y estas son distribuidas de modo seguro mediante una sesión IKE en la que ambos nodos se autentican mutuamente, se garantiza que solo los equipos deseados participan en la comunicación. Es conveniente aclarar

que una autenticación valida no implica un acceso total a los recursos, ya que IPSec proporciona también funciones de autorización. Durante la negociación IKE se especifica el flujo de tráfico IP que circulará a través de la conexión IPSec. Esta especificación es similar a un filtro de paquetes, considerándose el protocolo, las direcciones IP de los puertos origen, el byte “TOS” y otros campos.

Por ejemplo, puede utilizarse IPSec para permitir el acceso desde una sucursal a la red local del centro corporativo, pero impidiendo el paso del tráfico hacia equipos especialmente protegidos.

5.3.5 No repudio

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

5.4 Aplicaciones con IPSec

IPSec permite construir soluciones de comunicación que ofrecen confidencialidad y autenticación en la capa IP, independientemente de cuál sea el medio de transporte (xDSL, ATM, PPP, etc). Además, la inclusión de seguridad en la capa IP tiene la ventaja de que se extiende universalmente, ofreciendo un nivel de seguridad homogéneo de manera independiente del tipo que sean las aplicaciones, siempre que estén basadas en IP.

IPSec tiene muchas implementaciones, a continuación se presentan las más comunes.

5.4.1 Implementación de IPSec en Linux

FreeS/WAN es una implementación libre distribuida bajo licencia GPL (GNU Public Licence) del protocolo IPSec para sistemas operativos GNU/Linux. El proyecto comprende dos grandes áreas, una es el código que se agrega al núcleo de Linux y la otra parte es el código de las herramientas que el usuario utiliza para hacer que se establezcan los túneles entre otras cosas.

Justamente una de las ventajas de utilizar IPSec es que existen muchos otros sistemas operativos que tiene implementado IPSec (además de que es sumamente seguro) y esto permite que con Linux se puedan establecer túneles cifrados con otras redes que tengan sistemas operativos diferentes.

Otro caso común de uso de IPSec a través de FreeS/WAN es el denominado "Road Warrior" o guerrero de carretera. Bajo este nombre contempla el escenario en el que una persona puede conectar un único equipo (Portátil o PDA) a una red corporativa desde fuera de la misma. Este sería el caso de un trabajador que quiere conectar con su empresa desde su casa, un representante en viaje de negocios que necesita conectarse al servidor desde la habitación de su hotel, etc. FreeS/WAN también contempla este caso y es capaz de operar tanto en modo cliente (en el equipo del usuario remoto) como en modo servidor (en el Gateway de entrada hacia la red corporativa) para dar acceso a los Road Warriors.

5.4.2 Implementación de IPSec en Unix

Una puesta en práctica de IPSec de IPSec se incluye en NetBSD y FreeBSD que pertenecen a la misma familia Unix.BSD comprende tres variedades y cada una tiene sus características que lo hace único:

- **OpenBSD:** Enfocado a la seguridad.
- **FreeBSD:** Plataforma i386, priorizando el rendimiento.
- **NetBSD:** Sistema Unix, se ejecuta en mayor número de plataformas de hardware.

OpenBSD, para conseguir su objetivo de máxima seguridad, el proyecto está ubicado en Canadá, donde se exporta con criptografía integrada, esto les ha permitido ser el primer sistema operativo en incluir IPSec. A partir de su versión 2.2, OpenBSD incorpora IPSec de serie.

Existen dos entidades administrativas que controlan lo que le ocurre a un paquete. Una es la SAD o Base de Datos de Asociación de Seguridad, también llamada TDB en el código fuente de IPSec en OpenBSD. Y la otra entidad es la SPD o Base de Datos de Políticas de Seguridad.

Una entrada SAD incluye:

- Dirección IP de destino.
- Protocolo IPSec (AH o ESP).
- SPI (cookie).
- Contador de secuencias.
- Indicador de secuencia.
- Ventana de información anti-replica.
- Tipo de AH e información relacionada.
- Tipo de ESP e información relacionada.
- Información sobre el tiempo de vida.
- Indicadores de modo (túnel o transporte).
- Información sobre el camino MTU.

Una entrada SPD contiene:

- Puntero a SAS activas.
- Campos de selector.

Cada SA puede definir una cabecera ESP y una cabecera AH. Una sesión de IPSec debe tener una de las dos o ambas, pero no se puede definir sin ninguna de las dos.

FreeBSD es un avanzado sistema operativo para arquitecturas x86 compatibles incluyendo procesadores de la familia Intel, Amd y UltraSPARC. FreeBSD es un derivado de BSD, la versión de Unix desarrollada en la Universidad de California, Berkeley. FreeBSD es desarrollado y mantenido por un gran número de personas, mientras que el soporte para otras arquitecturas aún está en fases de desarrollo.

Este sistema operativo ofrece altas prestaciones en comunicaciones remotas, rendimiento, seguridad y compatibilidad que hasta el momento todavía son inexistentes en algunos sistemas operativos. Además proporciona servicios de red robustos, incluso en situaciones de alta carga de trabajo, haciendo un uso eficaz de la memoria con el fin de mantener buenos tiempos de respuesta con cientos o miles de procesos simultáneos.

A partir de la versión 5, FreeBSD contiene una pila IPSec “acelerada por hardware”, conocida como “Fast IPSec”, que fue obtenida de OpenBSD. También emplea hardware criptográfico (cuando es posible) con el fin de optimizar el desempeño de IPSec.

NetBSD es un sistema operativo tipo Unix que por sus características está disponible para múltiples plataformas, desde servidores de gran escala hasta equipos de escritorio y dispositivos de mano. Su limpio diseño y características avanzadas lo hacen excelente tanto en ambientes de producción y entornos de desarrollo. NetBSD es desarrollado y soportado por una gran comunidad internacional. Muchas aplicaciones están fácilmente disponibles a través de colecciones de paquetes desarrolladas para él. Se trata de un sistema operativo maduro, producto de años de desarrollo (los orígenes de BSD se remontan al año 1977) y partiendo del sistema Unix sexta edición. A continuación se describen las principales ventajas de NetBSD:

- Enfocado principalmente a la calidad y portabilidad de código. Actualmente disponible para cerca de 56 arquitecturas.
- Suele ser pionero en implementar nuevas tecnologías (por ejemplo IPv6).
- Alta seguridad y estabilidad. Fue usado en la NASA.

- Sistema de archivos BSD FFS (Fast File System), rápido y confinable.
- Implementa los protocolos más actuales de seguridad en redes, como es el caso de IPSec.
- Soporte nativo de máquinas virtuales XEN en versión 3.0.

5.4.3 Implementación de IPSec en Windows

IPSec está soportado actualmente en la mayoría de los sistemas operativos de Microsoft enfocados a servidores, tales como Windows 2000, Windows Server 2003 en todas sus versiones y en el más reciente Windows Server 2008. Así mismo es soportado en sistemas operativos para uso personal, tal es el caso de Windows XP, Windows Vista y Windows 7.

En el caso de los sistemas operativos para servidores, IPSec esta soportado ampliamente y está integrado con el servicio de Directorio Activo. Debido a lo anterior, las políticas IPSec se pueden asignar mediante políticas de grupo, permitiendo que los parámetros se configuren a nivel de dominio, sitio o unidad organizacional.

Actualmente existe una interface gráfica de usuario y varias herramientas basadas en línea de comandos que permiten la configuración de directivas IPSec y el protocolo de intercambio de claves de Internet (IKE).

A partir de Windows XP en su edición profesional, Microsoft integra en sus sistemas operativos un cliente que permite a los equipos de cómputo PC usar conexiones L2TP con IPSec. Esta tecnología es altamente segura para realizar conexiones VPN de acceso remoto a través de redes públicas como Internet.

5.4.4 Implementación de IPSec en Cisco

Cisco Systems es una empresa multinacional líder en redes e internet, principalmente dedicada a la fabricación, venta, mantenimiento y consultoría de equipos de telecomunicaciones. De la misma forma desarrolla el software y protocolos propietarios para instalarlos en la mayoría de sus equipos de fábrica.

Debido a lo anterior, el protocolo IPSec se encuentra soportado en la mayoría de los productos para telecomunicaciones que Cisco ofrece en el mercado, tal es el caso de los más comunes descritos a continuación:

- Familia de enrutadores Cisco 800 series.
- Familia de enrutadores de segunda generación Cisco 1900 series.
- Familia de enrutadores de segunda generación Cisco 2900 series.
- Familia de enrutadores de segunda generación Cisco 2900 series.
- Familia de Firewall Cisco ASA 5500 series.
- Familia de Clientes VPN Cisco AnyConnect, Cisco Easy VPN y Cisco VPN Client.

Es importante mencionar que además de Cisco, existen más empresas en el ramo de telecomunicaciones e Internet cuyos equipos son capaces de soportar IPSec en sus distintas modalidades. Por mencionar algunas de los fabricantes cuyos equipos soportan IPSec:

- Netgear
- TP-LINK
- Intellinet
- Mikrotik
- Ubiquiti
- Juniper

CAPÍTULO VI

CASO DE ESTUDIO: VPN SITIO A SITIO

"Antes que toda otra cosa, la preparación es la clave para el éxito."

Alexander Grahambell

6.1 Introducción

MAX Computación es una empresa que empezó sus operaciones en la ciudad de Mérida, Yucatán hace poco más de 10 años, teniendo como giro principal el soporte técnico especializado a equipos de cómputo de fabricantes reconocidos. Un par de años después, inicia una alianza estratégica con una empresa mayorista de equipos de cómputo, refacciones, accesorios y consumibles. En el año 2010, MAX Computación expande sus operaciones a la Ciudad de Chetumal Quintana Roo, abriendo una sucursal operativa cuya función principal es la comercialización al mayoreo de equipos y refacciones de cómputo.

Derivado de lo anterior, la empresa fue requiriendo un medio de comunicación rentable, ágil y seguro, a través del cual pudiera intercambiar información relevante con la oficina central ubicada en la ciudad de Mérida.

6.2 Justificación

Actualmente la empresa MAX Computación gasta una suma de dinero significativa por concepto de telefonía a larga distancia. Esto debido a que la sucursal ubicada en la ciudad de Chetumal requiere constante comunicación con el cuerpo directivo, personal de ventas y almacén ubicados en la ciudad de Mérida.

De la misma forma, el personal de servicio técnico en la ciudad de Chetumal requiere intercambiar archivos de mediano peso con sus similares en las oficinas centrales. Esto lo hacen normalmente por medio de mensajería instantánea o correo electrónico, presentando como limitante el peso de cada archivo.

Por su parte, el departamento de ventas requiere acceso instantáneo a los servidores de la empresa, con el fin de obtener información actualizada sobre la disponibilidad de productos en el almacén, garantías y demás información crítica para el proceso de venta y post-venta.

En diversas ocasiones, el departamento de Recursos Humanos en las oficinas centrales no puede dar seguimiento oportuno al estado y movimiento de cada

trabajador debido a que el reporte de registro para entradas y salidas del personal puede ser manipulado antes de ser enviado.

Adicionalmente, Max Computación acaba de invertir en un sistema integral, con el que es posible controlar los procesos más significativos de la empresa, como almacén, compras, ventas, facturación y finanzas.

6.3 Propuesta de solución

Derivado de las crecientes necesidades de comunicación entre las oficinas remotas de la empresa y después de analizar diferentes propuestas de líneas dedicadas en arrendamiento, la empresa decide invertir en una solución robusta basada en Redes Privadas Virtuales (VPN) de sitio a sitio utilizando equipos propios.

6.3.1 Situación actual

Actualmente las oficinas centrales y la sucursal remota cuentan con una línea de Internet PYME por cable con la empresa Cablemás de 10Mbps X 1Mbps con direccionamiento público estático en cada una, como se muestra en la siguiente figura:

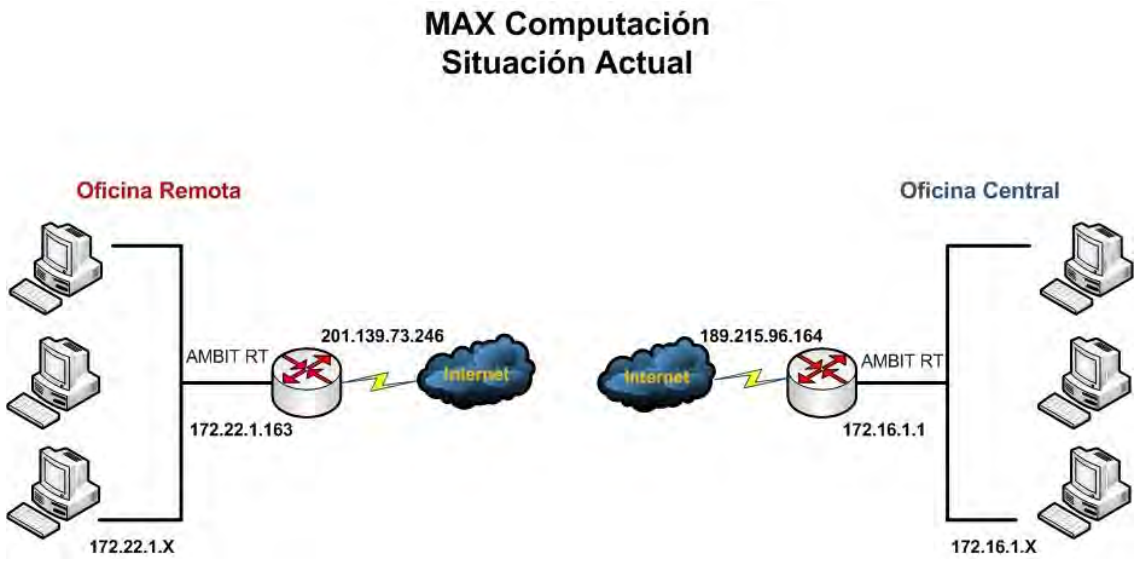

Figura 38 Sistema de comunicación de la empresa. (Elaboración propia)

Cuando uno o más equipos de cualquier oficina desean tener acceso a Internet solo envían una petición al router local (proveído por el ISP) y así logran el acceso a la nube. Algo similar ocurre cuando personal técnico de las oficinas centrales desean tener acceso a un equipo de la oficina remota, en este caso normalmente utilizan una aplicación para escritorio remoto. Pero, ¿Qué pasaría si uno más usuarios de las oficinas centrales desean compartir información con la sucursal remota?

6.3.2 Planteamiento de la solución

MAX Computación decidió invertir en una solución VPN de sitio a sitio, con la finalidad de mantener comunicadas de manera permanente sus oficinas remotas y de esta forma poder intercambiar información en tiempo y forma. También se pretenden enviar dos extensiones telefónicas IP desde las oficinas centrales hasta la sucursal remota, con el fin de reducir los costos por concepto de telefonía a larga distancia. De esta forma, hacer llamadas entre las oficinas no presentará ningún costo ya que todo el tráfico de voz será conducido por la VPN.

Para llevar a cabo la solución VPN de sitio a sitio es necesario considerar algunos factores técnicos que son necesarios para la implementación:

- **Conexiones a Internet**: Cada oficina de la empresa cuenta con una conexión a internet de 10Mbps de bajada y 1Mbps de subida. Si el túnel VPN es implementado sobre estas conexiones se afectaría significativamente el rendimiento tanto del túnel como del acceso a Internet.
- **Equipo**: El router instalado por el ISP no soporta conexiones VPN de ningún tipo, además de tener pocas prestaciones en cuanto a procesamiento y memoria RAM se refiere.

Debido a lo anterior, es necesario contratar una conexión a Internet extra para cada sitio (oficina). Estas conexiones serán las encargadas de soportar el túnel de sitio a sitio entre las oficinas centrales y la sucursal remota. Cada conexión extra deberá ser de 20Mbps de bajada y 2Mbps de subida, ambas con direccionamiento IP público estático.

En cuanto al equipo para implementar la solución, es necesario adquirir un Firewall Cisco PIX de la serie 515 para cada oficina. La serie 515 de cisco se distingue por soportar poco más de 15 túneles VPN de sitio a sitio sin sacrificar recursos a ninguna conexión.

A continuación, se muestra las modificaciones que deben ser aplicadas para poder implementar el túnel de sitio a sitio que facilitará la comunicación entre ambas oficinas de la empresa.

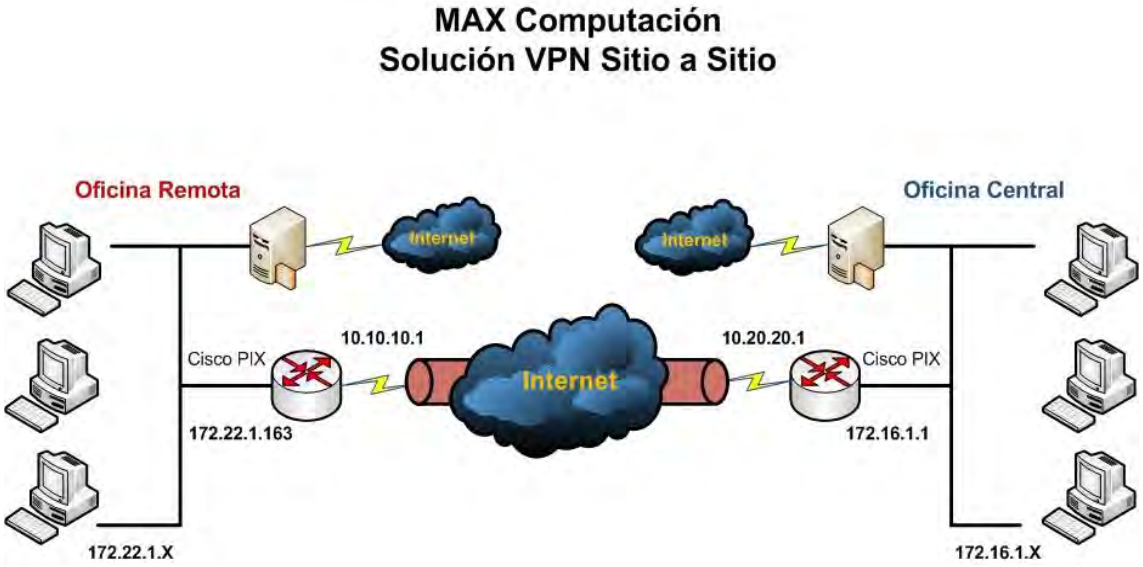

Figura 39 Implementación VPN Site2Site (Elaboración propia)

Para brindar acceso a Internet con las conexiones a Internet ya instaladas anteriormente (10Mbps X1Mbps) es necesario un servidor proxy que desempeñe la función de puerta de enlace para los paquetes que vayan dirigidos a Internet. Mientras que los nuevos equipos Cisco PIX serán las puertas de enlace para acceder al túnel seguro de la VPN.

El servidor proxy es el encargado de hacer cumplir las políticas de navegación en internet previamente definidas por el administrador de la red. En algunos casos también se incluye en la funcionalidad del proxy el administrador de cache web.

En el caso de Max Computación es necesario equipar a los servidores proxy con MS Windows Server 2008 y MS Forefront TMG, cuyas licencias fueron adquiridas en meses anteriores por que ya se tenía en mente instalar servidores proxy en cada oficina remota.

Para hacer más sencillo y efectivo el proceso de administración de dichos servidores, es necesario adquirir una licencia de GFI Web Monitor para MS Forefront TMG. La función de este software es administrar por grupos de contenido la mayor parte de los sitios web en Internet. Debido a esto, el permitir o denegar sitios es más fácil ya que todo está agrupado de acuerdo a propósitos en común, por lo que en la mayoría de las ocasiones solo basta con seleccionar un grupo de sitios y usuarios de la red local para aplicar las políticas vigentes en la empresa.

6.3.3 Análisis de costos

A continuación, en la siguiente tabla se muestra la inversión total en equipos que la empresa MAX Computación tiene que realizar para la implementación de la VPN de sitio a sitio.

CANTIDAD	DESCRIPCIÓN	PRECIO U.	TOTAL
2	Firewall CISCO PIX serie 515.	9199.00	18398.00
		TOTAL:	**18398.00**

Tabla 1 Costo total de los quipos

Los servidores y licencias del sistema operativo MS Windows Server 2008 ya fueron adquiridas desde meses anteriores a la implementación, debido a que la empresa ya tenía en mente realizar la instalación y puesta en marcha de servidores proxy en sus oficinas remotas.

Una vez considerado el costo total en equipos, es necesario considerar los costos por arrendamiento de las nuevas líneas de Internet y las líneas que ya existían anteriormente.

CANTIDAD	DESCRIPCIÓN	PRECIO U.	TOTAL
2	Internet PYME 20Mbps * 2Mbpps. Cargo único mensual	1499.00	2998.00
2	Direccionamiento IP publico estático. Cargo único mensual	700.00	1400.00
2	Internet PYME 10Mbps * 1Mbps. Cargo único mensual	999.00	1998.00
		TOTAL:	**6396.00**

Tabla 2 Costo mensual de servicios de comunicación

La empresa de telefonía Telmex a través de su filial Red Uno, cotizó un enlace privado sitio a sitio con MPLS entre las oficinas remotas de Max computación. Los costos se presentan a continuación:

CANTIDAD	DESCRIPCIÓN	PRECIO U.	TOTAL
1	Enlace privado MPLS 2Mbps* 2Mbps. Cargo único mensual	19600.00	21600.00
	**** Contrato mínimo por 12 meses**	**TOTAL:**	**21600.00**

Tabla 3 Costo mensual por arrendamiento de línea privada

Como se muestra en la tabla anterior, el tiempo mínimo de permanencia que exige la compañía Telmex es de 12 meses para poder correr con los gastos de instalación y equipos sin que tenga que cobrarle una parte a Max Computación.

Para determinar si la solución VPN sitio a sitio es viable en cuanto a costos y funcionalidad, es necesario analizar las tres tablas anteriores.

- El costo total de los equipos Cisco PIX necesarios para la implementación es de **$18398.00** pesos. Mientras que a la vuelta de un año, se pagarían **$76752.00** pesos por concepto de servicios de Internet PYME de 10 y

20Mbps respectivamente. Esto nos da una sumatoria total de gastos durante el primer año de **$95150.00** pesos. A partir del segundo año, el gasto anual descendería a **$76752.00** pesos ya que los equipos fueron comprados durante el primer año.

- Si se arrenda una línea dedicada con la empresa Telmex, no es necesario adquirir equipos si se mantiene la permanencia mínima por un año, pero el gasto anual total por este arrendamiento asciende a los **$259200.00** pesos.

En cuanto a la funcionalidad, el rendimiento de la conexión sitio a sitio sería similar, ya que la implementación propia contaría con canales asíncronos de 20Mb de bajada y 2Mb de subida en cada extremo de la VPN. Mientras que con la línea privada se contaría con 2Mb en canales síncronos en cada extremo de la conexión.

La única variante sobresaliente es que el tiempo de soporte en sitio ante alguna eventualidad o falla en el servicio de la empresa Telmex es de 24hrs máximo, los 365 días del año. Mientras que la empresa Cablemás, para sus usuarios PYME tiene un tiempo de respuesta para casos de soporte en sitio de hasta 48hrs hábiles.

En resumen, implementar la solución de VPN sitio a sitio con equipo propio y sobre líneas de Internet PYME contratadas con la empresa Cablemás, es casi 3 veces más barato que contratar un enlace privado con la empresa Telmex durante el primer año de servicio.

6.4 Implementación

Una vez Instaladas las nuevas líneas de Internet para el túnel, es necesario proceder a la instalación y configuración del servidor proxy que servirá como puerta de enlace a Internet. Posteriormente los equipos deben ser configurados para utilizar el mismo servidor proxy y de esta forma tener acceso a Internet.

Por último es necesario configurar los equipos Cisco PIX. A continuación se describen cada uno de los pasos:

- Ejecutar Cisco ASDM primeramente para el equipo cuya IP es 172.22.1.163 como se muestra a continuación:

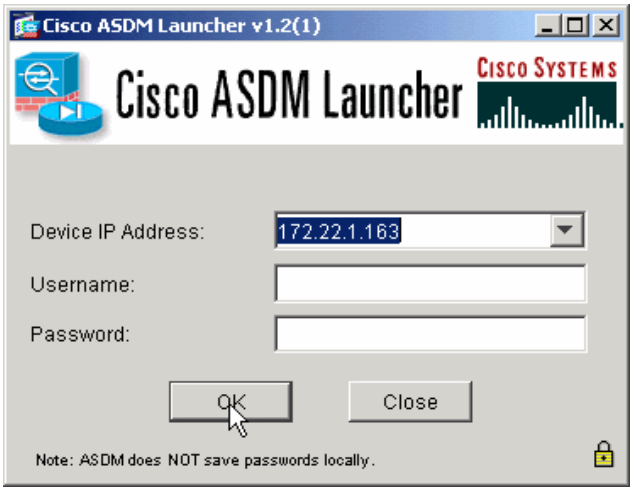

Figura 40 Autenticación CISCI ASDM

- Una vez en el panel principal de ASDM, debe seleccionarse el asistente de VPN (VPN Wizard).

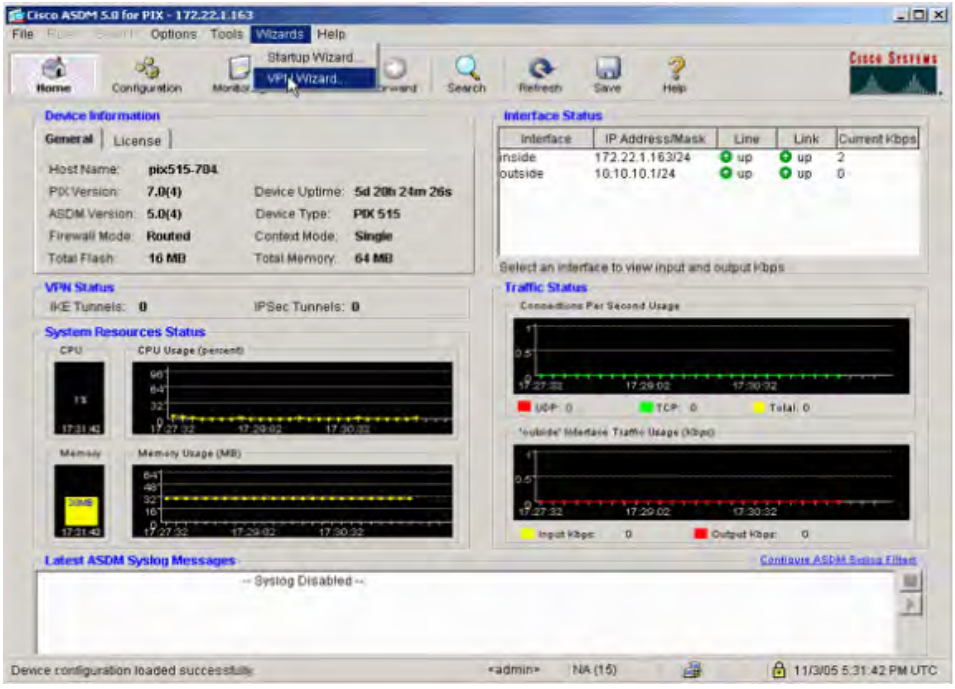

Figura 41 Panel principal de Cisco ASDM

- Una vez iniciado el asistente, es necesario seleccionar la opción sitio a sitio y escoger la interface de acceso al PIX remoto. Para este caso la interface de acceso debe ser la misma que está conectada a Internet (outside), ya que por este medio será generado el tunel VPN que conducirá los datos al sitio remoto.

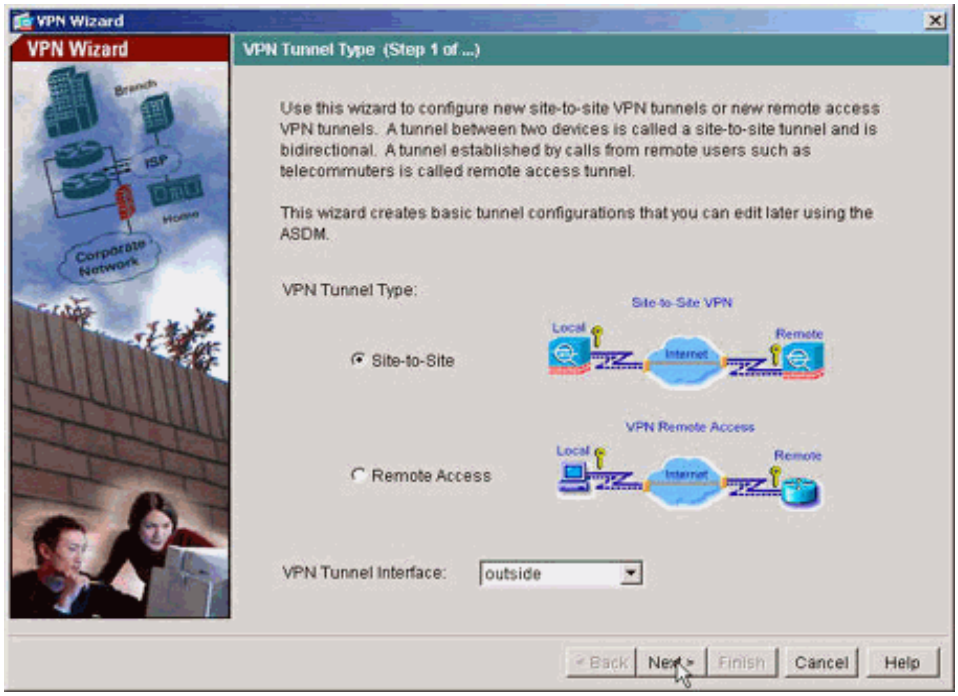

Figura 42 Tipo de túnel VPN

- Despues de haber seleccionado el tipo de tunel y la interface a traves de la cual se establecerá el mismo, es necesario especificar la dirección IP de la interface outside del equipo PIX remoto, para este caso sería 10.20.20.1 (oficinas centrales). Posteriormente, en la misma ventana se debe especificar un nombre para el tunel (Tunnel Group Name), en este caso particular se maneja la misma dirección IP del PIX remoto. Por ultimo es necesario seleccionar el tipo de autenticación que se usará para acceder al tunel seguro. A continuación, se ilustran los parametros utilizados para este caso.

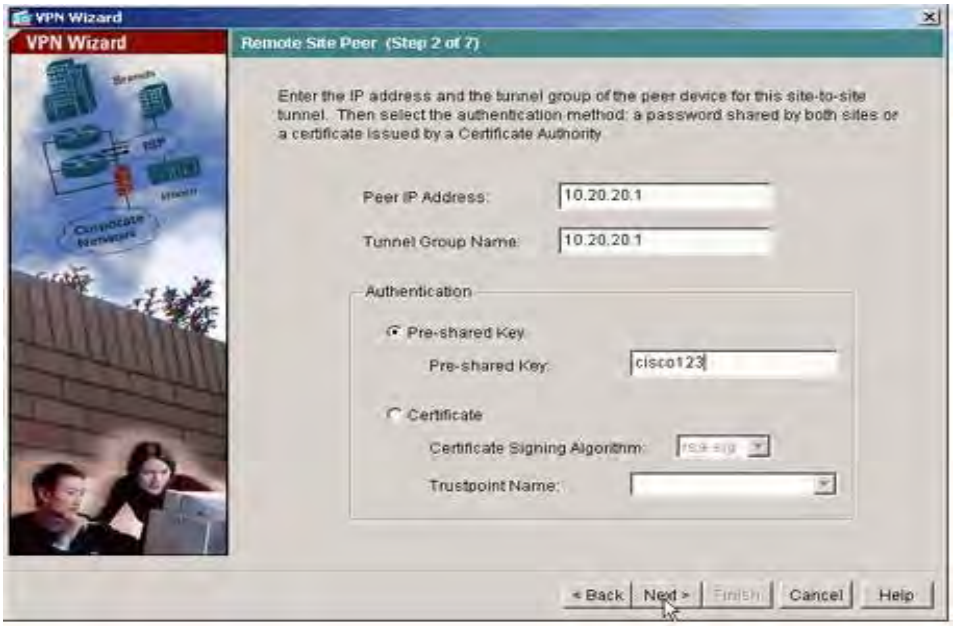

Figura 43 Sitio remoto y autenticación

- Posteriormente es necesario especificar los atributos para IKE, tales como el algoritmo de encriptación, autenticación y el grupo Diffie_Hellman. Comúnmente se conoce a esta fase como “fase1”. Los valores especificados deben ser los mismos para ambos extremos.

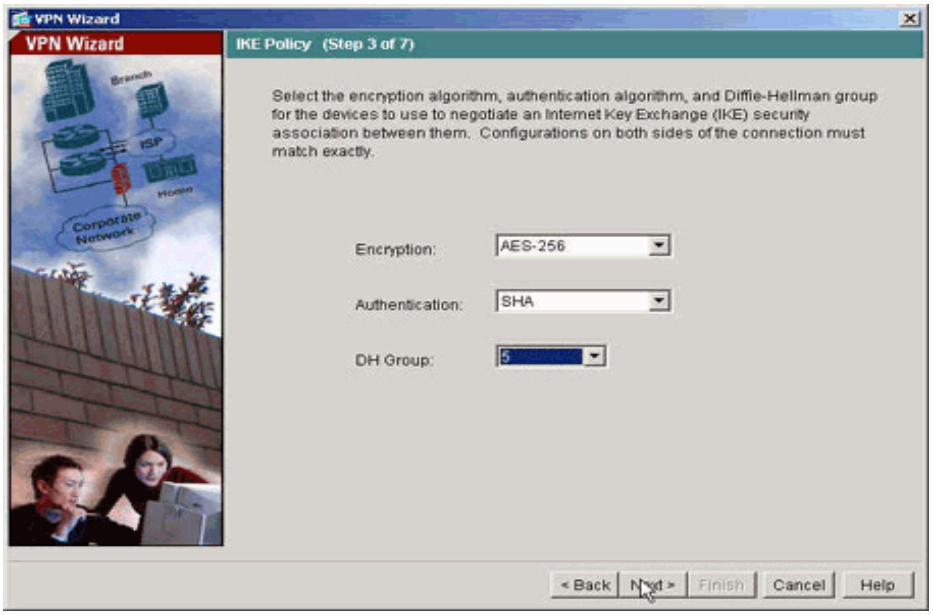

Figura 44 Atributos para IKE (Fase1)

- A continuación es necesario especificar los atributos a usar para IPSec, comúnmente se le conoce a esta fase como “fase 2”. Los valores introducidos en esta fase deben ser los mismos en ambos extremos.

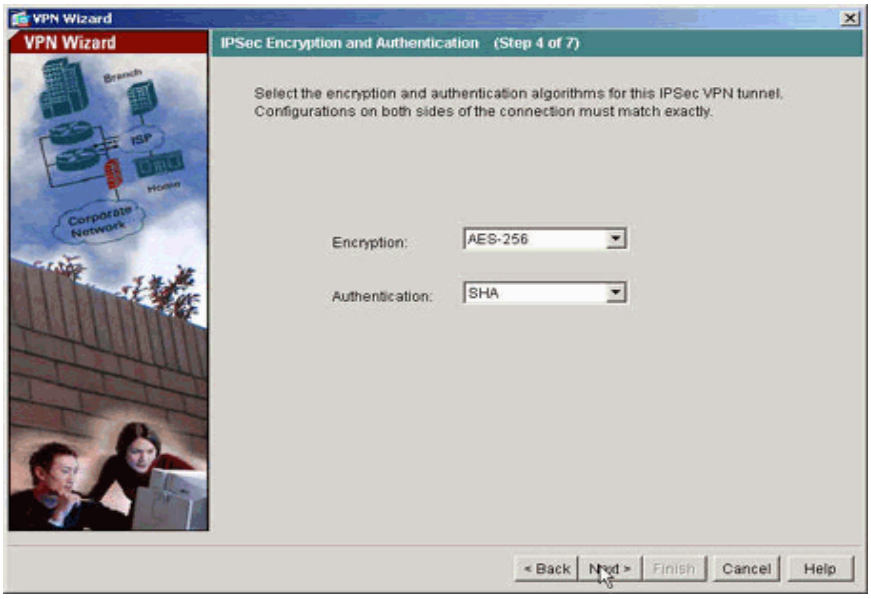

Figura 45 Atributos para IPSec (Fase 2)

- Posteriormente es necesario especificar los anfitriones, cuyo tráfico se debe permitir entre el tunel VPN.

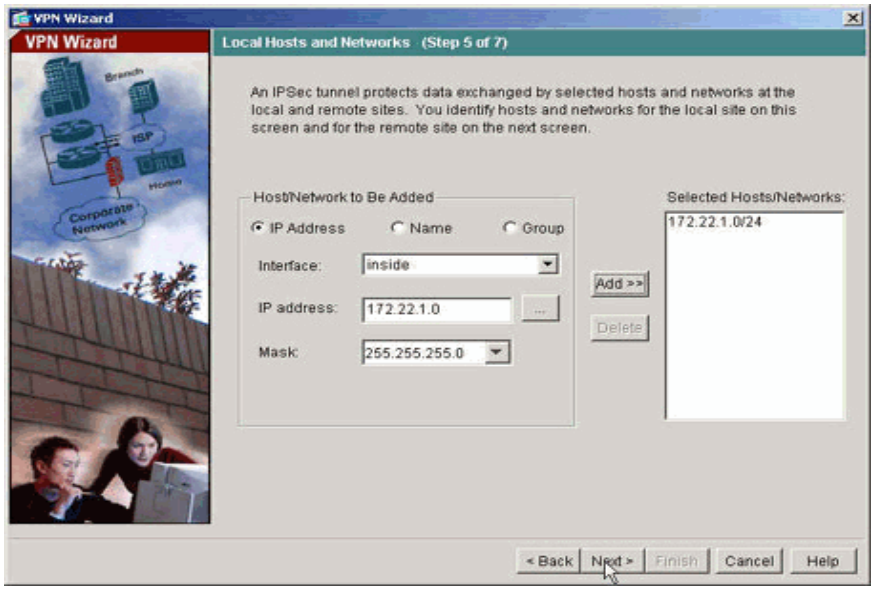

Figura 46 Anfitriones VPN

- Por último el asistente nos muestra un resumen de todos los parámetros seleccionados, es importante revisar cada uno para el correcto funcionamiento del enlace.

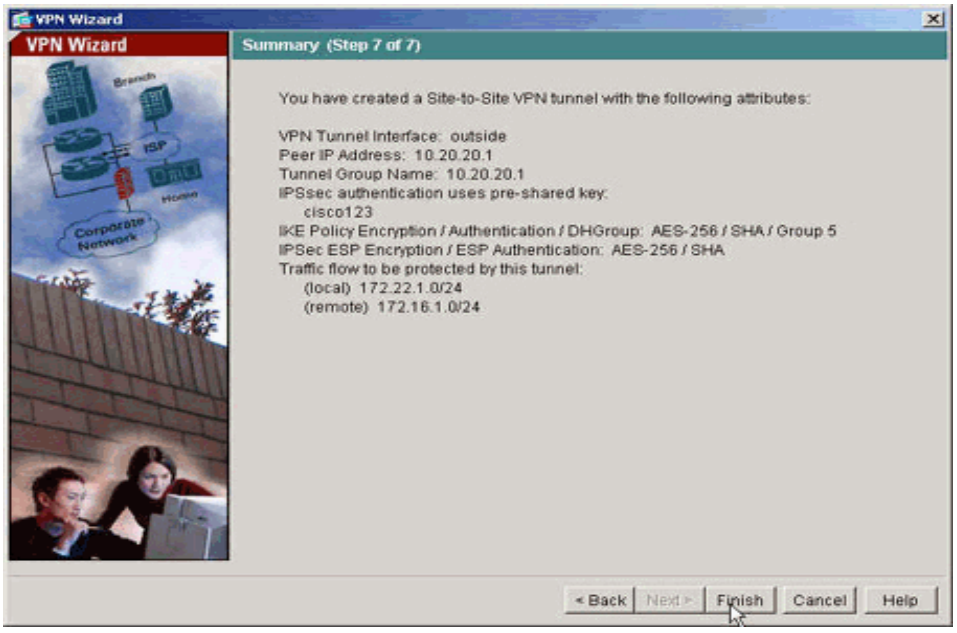

Figura 47 Resumen de la configuración

Para verificar que el tunel está creado correctamente y que está activo solo es necesario regresar al menú principal de ASDM. En la sección de en medio (VPN status) podemos observar que aparece un tunel IKE e IPSec activos. Para monitorear el tunel recién creado basta con seleccionar la opcion “Monitoring” ubicada en el menú principal.

Una vez revisado mediante el ASDM que el túnel fue configurado exitosamente y está funcionando, es necesario realizar las pruebas de comunicación de extremo a extremo entre cada uno de los equipos de cómputo interesados.

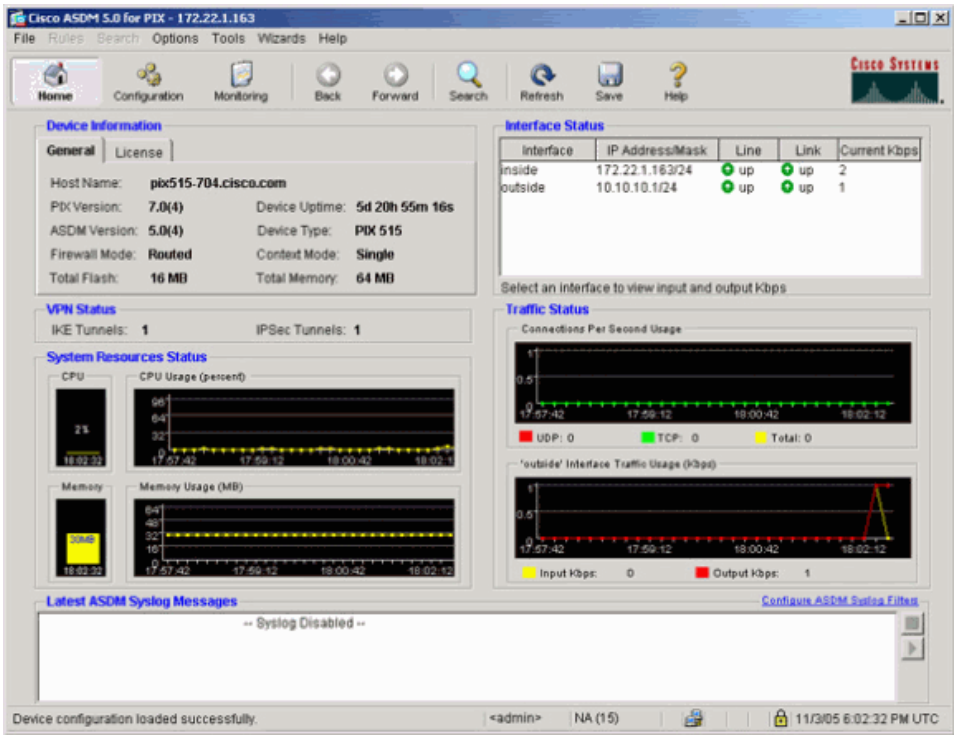

Figura 48 Verificando el funcionamiento del túnel

Ya que la configuración de los equipos Cisco esta concluida, es necesario cambiar las puertas de enlace de cada usuario en las redes locales de cada oficina para que puedan acceder a la VPN y de esta forma comunicarse entre sí. La puerta de enlace predeterminada para la oficina en chetumal es 172.22.1.163, mientras que la puerta de enlace para la central de merida es 172.16.1.1.

El servidor DNS que se debe configurar para los usuarios de Mérida y Chetumal es el mismo que se encuentra en las oficinas centrales (Mérida) ya que mediante la conexión VPN sitio a sitio los usuarios de la oficina remota en Chetumal van a poder acceder a cualquier servicio en las oficinas centrales como si estuviern conectados localmente ahí.

A continuación, en la siguiente imagen se muestra la configuración IP de un equipo perteneciente a la sucursal de chetumal.

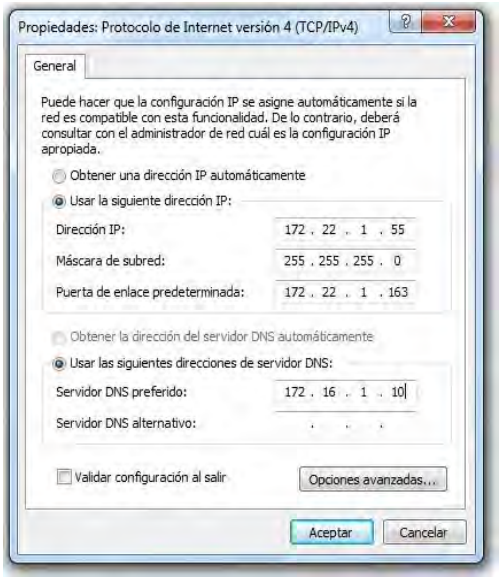

Figura 49 Configuración de IP para usuarios en Chetumal

Como se mencionó anteriormente, el acceso a Internet debe ser controlado por el servidor proxy local de cada oficina. Para esto es necesario configurar en el navegador de internet de cada usuario la dirección IP del servidor proxy correspondiente a su ubicación.En el caso de la oficina remota de Chetumal, la dirección IP del servidor proxy local es 172.22.1.1 tal y como se muestra a continuación.

Figura 50 Configuración del servidor proxy para los navegadores

Durante la primera semana despues de implementada la VPN sitio a sitio solo se intercambiaba información referente al sistema integral que la empresa usa para controlar sus ventas, facturación, inventario, etc. También se utilizó para tareas simples de compartir recursos, como intercambiar archivos de ofimatica y soporte entre ambas sucursales.

Durante las dos semanas siguientes se implementaron dos líneas telefonicas IP en la sucursal de Chetumal, ambas dependientes del conmutador IP ubicado en la central de Mérida. La integración de dichas líneas se realizó sin inconveniente alguno y se usaron durante las jornadas comunes de trabajo.

Posteriormente se integró un reloj checador IP basado en huella digital, cuyo servidor de datos está ubicado en la sucursal de Mérida, esto con la finalidad de obtener reportes concretos y oportunos de las entradas y salidas del personal de la sucursal en Chetumal.

CONCLUSIONES

"No quería fundar esta empresa. Mi objetivo no era ganar un montón de dinero, era construir buenos ordenadores. Sólo fundé la empresa cuando me di cuenta que podría ser un ingeniero para siempre."

Steve Wozniak

Conclusiones

Las VPN son una robusta combinación entre seguridad e interoperabilidad, que cada vez más se ofrecen como una solución a las demandas de comunicación para las organizaciones en crecimiento y expansión. Debido a lo anterior y a los altos niveles de seguridad otorgados dentro de medios públicos, las Redes Privadas Virtuales pueden remplazar enlaces dedicados que requieren grandes inversiones económicas para su implementación y mantenimiento.

Los distintos protocolos VPN estudiados en este trabajo, ofrecen cada uno diferentes normas de operación, seguridad, compatibilidad y entorno. Siendo el más destacado y confiable el protocolo IPSec, que ofrece distintos niveles de seguridad según los modos de operación y escenarios que el personal calificado en la empresa elija para su implementación. Así mismo y gracias a los distintos protocolos y algoritmos de seguridad que emplea para su funcionamiento, IPSec se consolida como una solución altamente confiable y segura para llevar a cabo comunicaciones a través de medios desprotegidos como es Internet.

Es importante destacar que antes de realizar una implementación VPN a nivel empresarial es necesario analizar detalladamente los requerimientos de la empresa en cuanto a seguridad y velocidad, los cuales varían de acuerdo al tamaño de la red corporativa, el tipo de información a transmitir y el nivel de seguridad requerido. En algunas ocasiones las empresas requieren transmitir información de manera ágil, sin retardos y con bajo costo económico. Mientras en la mayoría de los casos, gran parte de las empresas decide sacrificar un poco la velocidad a cambio de maximizar la seguridad del enlace VPN.

Mediante la implementación del caso de estudio “VPN sitio a sitio para la empresa MAX Computación” me fue posible observar detalladamente todos los aspectos que son necesarios considerar desde la planeación hasta la implementación de una solución de este tipo. De igual forma me fue posible analizar varios escenarios en los que se pudo implementar esta VPN y así escoger el que mejor se adapte a las necesidades de la empresa. Debido a lo anterior pude comprender el por qué

las VPN siguen siendo hoy en día una opción de bajo costo, con altas prestaciones de rendimiento y seguridad.

Durante la planeación del caso de estudio me fue posible comprender que no solo basta con plantear una solución de conexión entre dos redes distantes o entre un usuario distante y una red local, también es necesario plantear los diferentes puntos en los que la nueva implementación afectará positiva o negativamente a la red local y todos los procesos que los usuarios comúnmente ejecutan en la misma. En el caso de MAX Computación, se buscó no afectar en la medida de lo posible la forma de operar de los diferentes sistemas de información con los que la empresa cuenta hoy en día. De la misma forma se buscó agilizar y optimizar el intercambio de información entre los usuarios y los sistemas de información, así como también agregar servicios que contribuyan a la optimización de los procesos de la empresa, tal es el caso de la telefonía IP.

Por último, durante la fase de pruebas, me fue posible observar detalladamente el rendimiento de la red con altos, medios y bajos niveles de seguridad, obteniendo como resultado un enlace con muy poco retardo en el caso de bajos niveles de seguridad y un enlace más robusto para niveles de seguridad muy altos. Estos resultados de acuerdo y con base en los modelos de equipos utilizados para el caso de estudio. Mientras más prestaciones en cuanto a memoria, procesador y almacenamiento local tengan los equipos a utilizar en una implementación, mejor será el rendimiento de la misma, tomando en cuenta también los requerimientos de seguridad y si los equipos son basados en software o hardware.

BIBLIOGRAFÍA

“Hay que decir no a mil cosas para estar seguro de que no te estas equivocando o que intentas abarcar demasiado.”

Steve Jobs

Bibliografía

Bollapragada, V., Khalid, M. & Scott Wainner. *IPSec VPN Design.* Indianapolis : Cisco Press, 2005.

Carmouche, J. (2006). *IPSec Virtual Private Network Fundamentals.* Indianapolis*:* Cisco Press.

Eastlake, D. *Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH).* Recuperado 20 de diciembre de 2009. Disponible en http://www.ietf.org/rfc/rfc4305.txt

Francisconi, H. (2005). *IPSec en Ambientes IPv4 e IPv6.* Mendoza : Hugo Adrian Francisconi.

Hoffman, P. *Cryptographic Suites for IPSec.* Recuperado 30 de diciembre de 2009. Disponible en http://tools.ietf.org/html/rfc4308

Kent, S. *IP Encapsulating Security Payload.* Recuperado 20 de diciembre de 2009. Disponible en http://www.ietf.org/rfc/rfc4303.txt

Kent, S. & Atkinson, R. *Security Architecture for the Internet Protocol.* Recuperado 15 de noviembre de 2011. Disponible en http://www.ietf.org/rfc/rfc2401.txt

Kent, S. & Atkinson, R. *IP Authentication Header (AH).* Recuperado 15 de noviembre de 2011. Disponible en http://www.ietf.org/rfc/rfc2402.txt

Kent, S. & Seo, K. *Security Architecture for the Internet Protocol (Update RFC 2401).* Recuperado 15 de diciembre de 2009. Disponible en http://tools.ietf.org/html/rfc4301.

Krawczyk, H., Bellare, M. & Canetti, R. *HMAC (Keyed-Hashing for Message Authentication).* Recuperado 15 de febrero de 2010. Disponible en http://www.ietf.org/rfc/rfc2104.txt

Lewis, M. (2006). *Comparing Designing and Deploying VPNs.* Indianapolis : Cisco Press.

Mason, A. (2002). *Redes Privadas Virtuales de Cisco Secure*. Madrid : Pearson Education.

Mathon, P. (2004). *VPN Implementación en Windows Server 2003.* Barcelona *:* ENI.

Thayer, R. *IP Security (Document Roadmap).* Recuperado 25 de noviembre de 2009. Disponible en http://www.ietf.org/rfc/rfc2411.txt

GLOSARIO

"No hay reto que no podamos alcanzar trabajando unidos con claridad en los objetivos y con conocimiento de los instrumentos para lograrlos."

Carlos Slim

Glosario

Acceso Remoto — La capacidad de un equipo de cómputo en un lugar determinado para conectarse a un dispositivo u otro equipo de cómputo en otra ubicación geográfica.

ADSL (Línea de Suscripción Digital Asimétrica) — Se refiere a una tecnología que esta implementada para mejorar el ancho de banda de los hilos del cableado telefónico convencional gracias a una serie de métodos de compresión.

Ancho de Banda — La gama de frecuencias disponible para señalizar la diferencia entre las frecuencias más altas y las más bajas de una banda, se miden en Hertz.

ASCII (Código Estándar Americano para el Intercambio de Información) — Un código de datos binarios, consistente en siete bits de datos más un bit de paridad o símbolos especiales, establecido por la ANSI (Instituto Nacional Americano de Estándares), para la compatibilidad entre servicios de datos.

ATM (Modo de Transferencia Asíncrona) — Tecnología de red de alta velocidad que maneja datos, voz y video en tiempo real. ATM se define en el estándar Broadband RDSI (BISDN) y proporciona un ancho de banda “bajo demanda” cargando a los clientes por la cantidad de datos que envían. Las velocidades son escalables, empezando con velocidades lentas, pasando por velocidades intermedias de 25, 51, y 100 Mbps, y con velocidades altas de 155, 622 Mbps, y hasta la gama Gigabit. .

Byte — Agrupación fundamental de información binaria formada por 8 bits. Es la unidad mínima que puede direccionarse, pero no la unidad mínima que puede tratarse.

Cifrado — El cifrado es un método que permite aumentar la seguridad de un mensaje o información mediante la codificación del contenido, de manera que sólo pueda leerlo la persona que cuente con la clave de cifrado adecuada para descodificarlo. Por ejemplo, si se realiza una compra a través de Internet, la

información de la transacción (como su dirección, número de teléfono y número de tarjeta de crédito) suele cifrarse a fin de mantenerla a salvo.

Codificación — Transformación de un mensaje en forma codificada, es decir, especificación para la asignación unívoca de los caracteres de un repertorio (alfabeto, juego de caracteres) a los de otro repertorio. También se usa para referirse a la conversión de un valor analógico en una señal digital según un código prefijado.

Datagrama — Entidad de datos independiente que transporta información suficiente en orden de ser puesta en ruta desde un equipo origen a un equipo destino, sin tener que depender de que se haya producido anteriormente tráfico alguno entre ambos.

Dominio — Estructura jerárquica que organiza los equipos de Internet de forma que sea fácil recordar por su nombre.

Enrutador (Router) — Elemento que determina la trayectoria o ruta más eficiente de datos entre dos segmentos de la red. Opera mediante el uso de tablas y protocolos de enrutamiento.

Estándar — Conjunto de reglas y regulaciones acordado por una organización oficial de estándares o por aceptación general en el mercado (estándar de facto).

Ethernet — Tipo de red de área local desarrollada en forma conjunta por Xerox, Intel y Digital Equipment. Se apoya en la topología de bus, tiene anchos de banda elevados y se ha convertido en un estándar para las redes corporativas.

Firewall (Cortafuegos) — Es un dispositivo que funciona como protector entre redes, permitiendo o denegando el tráfico entre las mismas según las políticas con las que haya sido configurado. Un uso típico es situarlo entre una red local e Internet, como dispositivo de seguridad para evitar que los intrusos puedan acceder a información confidencial.

Frame Relay — Protocolo de enlace mediante circuito virtual permanente muy usado para dar conexión directa a Internet.

FTP (Protocolo de Transferencia de Archivos) — Protocolo mediante el cual es posible intercambiar cualquier tipo de archivos. El funcionamiento es sencillo, una persona desde su computadora invoca un programa cliente FTP para conectar con otra computadora, que a su vez tiene en ejecución el programa servidor FTP. Una vez establecida la conexión y debidamente autenticado el usuario con su contraseña, se puede empezar a intercambiar archivos.

Gateway, Puerta de enlace, pasarela — Dispositivo de comunicaciones que interconecta sistemas diseñados conforme a protocolos propietarios, o entre un sistema con un protocolo propietario y un sistema abierto, teniendo lugar una conversión completa de protocolos hasta la capa 7 del modelo de referencia OSI.

HDLC (Control de Enlace de Datos de Alto Nivel) — Protocolo que proporciona recuperación de errores en caso de pérdida de paquetes de datos, fallos de secuencia y otros, por lo que ofrece una comunicación confiable.

Host — En una red informática, es un equipo de cómputo central que facilita a los usuarios finales servicios tales como capacidad de proceso y acceso a bases de datos, y que permite funciones de control de red. Actualmente también se les conoce así a los equipos de cómputo que conforman una red de área local.

IETF (Fuerza de Trabajo en Ingeniería de Internet) — Organismo que tiene como principal función la investigación y desarrollo de nuevas tecnologías, junto con el análisis de nuevas propuestas y la regulación de los estándares publicados bajo la forma RFC.

IP (Protocolo de Internet) — El protocolo utilizado tanto en un equipo emisor como en el receptor para la comunicación de datos, a través de una red de paquetes conmutados. Los datos en una red basada en IP son enviados en bloques como paquetes de información.

IPX (Internet Packet Exchange) — Un protocolo de comunicación en Novell NetWare que crea, mantiene y termina la conexión entre dispositivos de red, tales como estaciones de trabajo y servidores.

ISP (Proveedor de Servicios de Internet) — Empresa u organización que provee la conexión de computadoras a Internet, ya sea por líneas dedicadas o por líneas conmutadas. Es una entidad, habitualmente con ánimo de lucro, que además de dar acceso a Internet a personas y empresas, les ofrece una serie de servicios (hospedaje de páginas web, consultoría de diseño e implantación de webs e Intranets, etc.).

MD5 — Es un algoritmo que se suele utilizar, entre otras cosas, para realizar la comprobación de la integridad de archivos binarios, siendo muy utilizado por ejemplo para comprobar la integridad y legitimidad de archivos en internet. El algoritmo MD5 genera un digesto (número único) a partir del análisis y suma de los caracteres de una cadena binaria, que es llamado cheksum.

NAT (Traducción de Direcciones de Red) — Es un mecanismo utilizado por enrutadores y/o cortafuegos para intercambiar paquetes entre dos redes con direccionamientos incompatibles. Tal es el caso de una red local e Internet.

Proxy — Servidor especial encargado, entre otras cosas, de centralizar el tráfico entre Internet y una red local, de forma que evita que cada una de las computadoras de la re local tenga que disponer necesariamente de una conexión directa a Internet. Al mismo tiempo contiene mecanismos de seguridad (firewall o cortafuegos) los cuales impiden accesos no autorizados desde el exterior hacia la red local.

PSTN (Red de Telefonía Publica conmutada) — Es una red telefónica por conmutación de circuitos tradicional optimizada para comunicaciones de voz en tiempo real.

RAS (Servidor de Acceso Remoto) — Es un equipo especializado múltiples canales de comunicación. Como estos canales son bidireccionales, surgen dos

modelos: múltiples entidades conectadas a un único recurso o una única entidad conectada a múltiples recursos.

TCP (Protocolo de Control de Transmisión) — Protocolo que posibilita la administración de datos que provienen del protocolo IP. TCP es un protocolo orientado a conexión y permite que dos equipos de cómputo que están comunicados controlen el estado de la transmisión.

Telnet — Servicio de red en el cual un usuario se conecta de forma remota a otro equipo, como si lo hiciera desde un equipo local.

UDP (Protocolo de Datagramas de Usuario) — Basado en el intercambio de datagramas, UDP permite el envío de las mismas a través de la red sin que se haya establecido previamente una conexión, ya que el propio datagrama incorpora suficiente información de direccionamiento en su cabecera. UDP no tiene confirmación ni control de flujo, por lo que los paquetes pueden adelantarse unos a otros.