Escuela Superior Politécnica de Chimborazo
FACULTAD DE INFORMÁTICA Y ELECTRÓNICA
ESCUELA DE INGIENERÍA ELECTRÓNICA

"ESTUDIO DE TECNOLOGÍAS VPN PARA LA INTERCONEXIÓN DE SITIOS REMOTOS"

TESIS DE GRADO

Previa obtención del Título de:
INGENIERO EN ELECTRÓNICA Y COMPUTACIÓN

Presentado por:
MAYRA ALEJANDRA MARTÍNEZ ZAMBRANO

Riobamba – Ecuador
2011

A MIS PADRES:

Que con su amor y apoyo incondicional

han cultivado valores que se verán

reflejados a través de muchas generaciones.

NOMBRE	FIRMA	FECHA
ING. IVÁN MÉNES **DECANO DE LA FACULTAD DE INFORMATICA Y ELECTRÓNICA**	……..	……..
ING. PEDRO INFANTE **DIRECTOR DE LA ESCUELA DE REDES Y TELECOMUNICACIONES**	……..	……..
ING. DANIEL HARO **DIRECTOR DE TESIS**	……..	……..
ING. MARCELO DONOSO **MIEMBRO DEL TRIBUNAL**	……..	……..
LCDO. CARLOS RODRIGUEZ **DIRECTOR CENTRO DE DOCUMENTACION**	……..	……..
NOTA DE TESIS	……..	……..

"Yo Mayra Alejandra Martínez Zambrano, soy la responsable de las ideas y doctrinas y resultados expuestos en esta tesis; y, el patrimonio intelectual de la Tesis de Grado pertenece a la ESCUELA SUPERIOS DE CHIMBORAZO".

_____

Mayra Alejandra Martínez Zambrano

ABREVIATURAS

AH	Cabecera de Autenticación
ATM	Modo de transferencia Asíncrona
CHAP	Challenge Handshake Authentication Protocol
CSJ	Corte Superior de Justicia
DES	Estándar de Encriptación de Datos
DH	Deffie Hellman
DHCP	Dynamic Host Configuration Protocol
DNS	Sistema de Nombres de Dominios
ESP	Carga Segura Encapsulada
GRE	Encapsulacion de Ruta Generica
HMAC	Códigos de Autenticación de Mensaje Basado en Resumen
IKE	Intercambio de llaves de Internet
IP	Protocolo de internet
IPSEC	Protocolo de Seguridad de Internet
IPX	Intercambio de paquete de internet
ISAKMP	Internet Security Association and Key Management Protocol
ISP	Proveedor de Servicios de Internet
IV	Vector de Inicialización

L2TP	Protocolo de Túnel de Capa 2
LAN	Red de Área Local
LNS	Punto lógico de terminación de una sesión
MD5	Algoritmo de Resumen de Mensaje
MPPE	Microsoft Point-to-Point Encryption
NAT	Traducción de Direcciones de Red
OSI	Interconexión de Sistemas Abiertas
PAP	Protocolo de Autenticación de Clave
PFS	Perfect Forward Secrecy
PPP	Protocolo Punto Punto
PPTP	Protocolo de Túnel Punto a Punto
PSTN	Redes de Telefonía por Suicheo Público
PVC	Circuito Virtual Permanente
RDSI	Red Digital de Servicios Digitales
RSA	Riverst Shamir Adleman
SA	Asociaciones de Seguridad
SATJE	Sistema Automático de Trámite Judicial
SHA	Algoritmo de Hash Seguro
SPD	Security Policy Database
SPI	índice de parámetros de seguridad
SPI	Índice de Parámetros de Seguridad
SSH	Secure Shell

SSL, TLS	Seguridad para Internet de uso extendido
TCP	Protocolo de Control de Transporte
TDM	Multiplexación por división en el tiempo
UDP	Protocolo de Datagrama de Usuario
VPN	Red Privada Virtual
WAN	Red de Área Extensa

INDICE GENERAL

BIBLIOGRAFÍA

ANEXOS

INDICE DE FIGURAS

INDICE DE TABLAS

INDICE DE ANEXOS

INTRODUCCION

Hace unos años no era tan necesario conectarse a Internet por motivos de trabajo. Conforme ha ido pasado el tiempo las empresas han visto la necesidad de que las redes de área local superen la barrera de lo local permitiendo la conectividad de su personal y oficinas en otros edificios, ciudades, comunidades autónomas e incluso países.

Las redes virtuales privadas utilizan protocolos especiales de seguridad que permiten obtener acceso a servicios de carácter privado, únicamente a personal autorizado, de una empresas, centros de formación, organizaciones, etc.; cuando un usuario se conecta vía Internet, la configuración de la red privada virtual le permite conectarse a la red privada del organismo con el que colabora y acceder a los recursos disponibles de la misma como si estuviera tranquilamente sentado en su oficina.

El objetivo de esta tesis es hacer un estudio comparativo de las tecnologías para la interconexión de sitios remotos y de esta manera se escogerá la mejor opción para el diseño e implementación de una Red VPN en la Corte Superior de Justicia.

El presente documento consta de cinco capítulos: en la primera parte se da una refencia teórica de lo que son les redes privadas Virtuales y sus tecnologías, en la segunda parte se hace referencia al análisis comparativo de los protocolos utilizados y en el capítulo final se da a conocer la implementación de la VPN en la Corte Superior de Justicia de Chimborazo.

CAPITULO I

RESEÑA DEL PROYECTO

1.1. ANTECEDENTES

Las redes privadas virtuales VPN están llamando la atención de muchas organizaciones ya que buscan ampliar las capacidades de sus redes de computadoras y reducir sus costos. Las redes virtuales privadas pueden encontrarse en los lugares de trabajo y en la casa y permiten a los empleados conectarse con seguridad a las redes de la empresa. Los tele-trabajadores y aquellos que viajan con frecuencia, encuentran que las redes VPN son una forma más conveniente de permanecer conectados con la Intranet corporativa. Y consecuentemente también ha existido la necesidad de comunicarse de manera privada, es decir que la información llegue solo a los receptores.

En síntesis una *VPN* es una comunicación punto a punto entre dos subredes de una misma red local, que se realiza a través de internet sin que los nodos locales

de cada extremo se dé realmente cuenta de que la red local global está dividida en dos o más subredes y que no tienen conexiones directas entre ellas.

El poder usar internet como medio de comunicación entre nodos distantes de una misma red local, abarata muchísimo el coste de este tipo de redes que hasta ahora sólo podían montarse mediante costosas líneas dedicadas que unían, esta vez físicamente, punto a punto los nodos de la red.

El uso de estas redes implica temas de configuración de *gateways*, *firewalls* y encriptación de la comunicación, ya que ahora la comunicación pasa por nodos intermedios indeterminados.

La Corte Superior de Justicia y todo su equipo encargado de la sagrada tarea de de ADMINISTRAR JUSTICIA EN NOMBRE DE LA REPUBLICA Y POR AUTORIDAD DE LA LEY.

En mayo del año pasado, en el Registro Oficial No. 337, se publica la **LEY ORGÁNICA DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN**. En ella se estipula la obligación de todas las Instituciones Públicas de mantener informada a la ciudadanía de sus actividades, de forma sencilla, clara y completa.

El Sistema de Trámite Judicial Ecuatoriano SATJE ha venido funcionando hace nueve años en la Corte Provincial de Justicia de Chimborazo en la ciudad de Riobamba brindando a la comunidad un Sistema Judicial más eficiente.

En la actualidad el sistema SATJE se encuentra funcionando en las Judicaturas de los cantones Alausi, Chunchi, Colta y Guamote, pero estos cantones no poseen comunicación directa con la Corte Provincial de Justicia de Chimborazo lo que dificulta cumplir a cabalidad con la Ley de Transparencia de la Información.

1.2. JUSTIFICACIÓN DEL PROYECTO DE TESIS.

Las Redes Privadas Virtuales (VPNs) son una alternativa práctica, segura y eficiente de los enlaces privados que en la actualidad son usados para interconectar redes corporativas y brindar acceso remoto a través de internet.

El estudio de tecnologías VPN ofrece costos bajos porque solo realiza llamadas locales, además de tener la posibilidad de que los datos viajen encriptados y seguros, con una buena calidad y velocidad, también mejorara la productividad y simplifica la topología de red.

Si se decidiera diseñar una red con línea privada: La empresa tendría que contar con su propio cable ya sea de cobre o fibra óptica de un punto a otro, en esta opción el costo es muy elevado porque si por ejemplo se necesita enlazar a la Corte Provincial de Justicia con una Judicatura que se encuentra a 200 Kilómetros de distancia el costo sería por la renta mensual por Kilómetro. Sin importar el uso.

Las Judicaturas de los cantones de Alausí, Chunchi, Colta y Guamote se ven en la necesidad de tener comunicación con la Corte Provincial de Justicia ubicada en la ciudad de Riobamba y de esta manera se puedan publicar los tramites que se realizan a través del Sistema SATJE, todo esto según la Ley de Transparencia de la Información ya que no cuentan con una red WAN que logre este objetivo.

Al existir este problema surge la idea de hacer un estudio de las tecnologías VPN y así poder escoger la mejor opción al implementar una red VPN en esta institución.

Para poder comparar las tecnologías VPN se requerirá de prototipos para las pruebas correspondientes.

1.3. OBJETIVOS

1.3.1. Objetivo general

Estudiar tecnologías VPN para la interconexión de sitios remotos y aplicar el estudio en la Corte Superior de Justicia.

1.3.2. Objetivos específicos:

- Estudiar las tecnologías de interconexión a través de Internet.
- Estudiar las tecnologías VPN y sus diferentes esquemas de seguridad.
- Comparar las tecnologías L2TP, PPTP, IPSEC dentro del ámbito de las redes privadas virtuales.
- Diseñar y construir prototipos de las tecnologías VPN y así comprobar este estudio.
- Definir la infraestructura de la implementación en la Corte Superior de Justicia de Chimborazo.

1.4. HIPOTESIS

El estudio de las tecnologías VPN permitirá escoger la opción más adecuada al implementar una red VPN de manera segura, con bajo costo, calidad y velocidad apropiados y lograr a través de este medio el diseño de una red para la interconexión de las distintas Judicaturas de la Corte Superior de Justicia de Chimborazo.

CAPITULO II

REDES PRIVADAS VIRTUALES VPNs

El mundo ha cambiado bastante en las últimas décadas. Cada vez aumenta la necesidad de comunicarse con sitios remotos y de manera privada. Las empresas y negocios están repartidos en varias sucursales a lo largo de una geografía. Bajo esta situación aparecen las redes privadas para unir varias delegaciones u oficinas de forma rápida y segura con su empresa sin importar su distancia física.

La ventaja que han sustentado los tradicionales enlaces dedicados es la disponibilidad, sin embargo, estos enlaces también son susceptibles de caídas, y su montaje, en cuanto a hardware se refiere, es tan complejo que es prácticamente imposible cambiar a otro proveedor mientras el enlace se restablece. Una red WAN dedicada a un cliente tiene unas ventajas

visibles sobre una red pública como es Internet, cuando se trata de fiabilidad, rendimiento y seguridad.

Hoy en día Internet proporciona WAN de alta velocidad, y la necesidad de redes privadas WAN se ha reducido drásticamente mientras que las VPN que utilizan cifrado y otras técnicas para hacer una red dedicada.

En este capítulo se resume las redes privadas con enlaces dedicados y a continuación se da a conocer lo que son las redes privadas virtuales sus características, tipos de conexión etc.

2.1. ENLACES DEDICADOS

Los enlaces dedicados, como su nombre lo indica, son conexiones permanentes punto-punto, o punto-multipunto, que se valen de una infraestructura de transporte (Capa 1) y/o conmutación (Capa 1 y 2). Los primeros son comúnmente llamados enlaces Clear Channel y los segundos son enlaces Frame- Relay y ATM.

2.1.1. Clear Channel

Clear Channel consiste en un canal de comunicaciones en que un solo transmisor opera a la vez.

Los enlaces Clear Channel ofrecen un rendimiento (throughput) efectivo casi del 100% ya que no usan ningún tipo de encapsulación de nivel 2, es decir, no hay presentes cabeceras de ningún tipo.

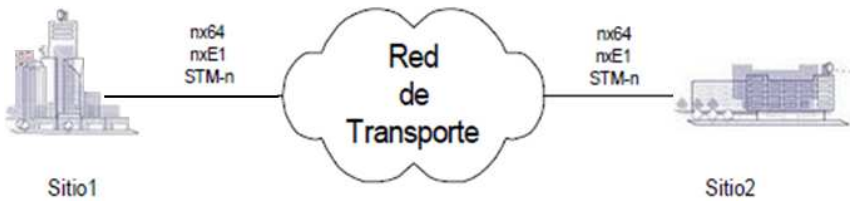


Figura II.1: Enlace típico Clear Channel.

La Figura II.1 muestra un esquema básico de lo que es Clear Channel. Vale la pena aclarar, que los enlaces Clear Channel fueron la primera tecnología WAN que se adoptó usando la infraestructura de voz PCM de los distintos operadores de telefonía locales, nacionales e internacionales. Como era de esperarse, por provenir de una tecnología que no había sido pensada para transmitir datos fue superada rápidamente por otros tipos de tecnologías como Frame Relay y ATM, aunque aun muchas empresas siguen teniendo enlaces Clear Channel.

2.1.2. Frame Relay

Frame Relay o (*Frame-mode Bearer Service*) es una técnica de comunicación mediante retransmisión de tramas, introducida por la ITU-T a partir de la recomendación I.122 de 1988. Consiste en una forma simplificada de tecnología de conmutación de paquetes que transmite una variedad de tamaños de tramas o marcos ("*frames*") para datos, perfecto para la transmisión de grandes cantidades de datos.

La técnica Frame Relay se utiliza para un servicio de transmisión de voz y datos a alta velocidad que permite la interconexión de redes de área local separadas geográficamente a un coste menor. Además proporciona conexiones entre usuarios a través de una red pública, del mismo modo que lo haría una red privada con circuitos punto a punto.

Las redes Frame Relay incorporan los nodos que conmutan las tramas Frame Relay en función del identificador de conexión, a través de la ruta establecida para la conexión en la red. Estas deben garantizar la transferencia bidireccional de los datos entre 2 abonados sin alterar su orden, mediante el intercambio de tramas de información no numeradas. Ello implica que debe proveerse un servicio orientado a conexión. Estas conexiones pueden ser de 2 tipos:

Circuito Virtual Permanente (PVC), donde cada conexión virtual entre dos abonados es establecido por el operador de la red en el momento de la subscripción y solo puede ser modificado por este.

Circuito Virtual Conmutado (SVC), en este caso debe existir un procedimiento de nivel 3 a fin de que los usuarios puedan establecer y liberar las conexiones a voluntad.

2.1.3. ATM (Asynchronous Transfer Mode)

La tecnología ATM, Modo de Transferencia Asíncrona es el corazón de los servicios digitales integrados que ofrecen las nuevas redes digitales de servicios integrados de banda ancha.

Los conmutadores ATM aseguran que el tráfico de grandes volúmenes es flexiblemente conmutado al destino correcto. Los usuarios aprecian ambas cosas, ya que se cansan de esperar los datos y las pantallas de llegada a sus terminales.

Una de las fortalezas de ATM es que paga solamente por la carga de celdas que es efectivamente transportada y conmutada. Hoy día los accesos conmutados a Internet están creando "Cuellos de Botella" en la infraestructura. Para copar este problema los fabricantes no solo han desarrollado sistemas de acceso sino aplicaciones para soluciones de fin a fin con conmutadores ATM, con solventes sistemas de administración de la red.

ATM usa multiplexación por división en el tiempo (Time Division Multiplex TDM) encontrado en la conmutación de circuitos, con la eficiencia de las redes

de conmutación de paquetes con multiplexación estadística. Por eso es que algunos hacen reminiscencias de perspectivas de conmutación de circuitos mientras que otros lo hacen a redes de paquetes orientados a conexión.

2.2. REDES VPN

La Red Privada Virtual (RPV), en inglés *Virtual Private Network* (VPN), es una tecnología de red que permite una extensión de la red local básicamente, una VPN es una red privada que utiliza una red pública para conectar diferentes sedes o usuarios entre sí.

VPN es una red privada que se extiende, mediante un proceso de encapsulación y en su caso de encriptación, de los paquetes de datos a distintos puntos remotos mediante el uso de unas infraestructuras públicas de transporte.

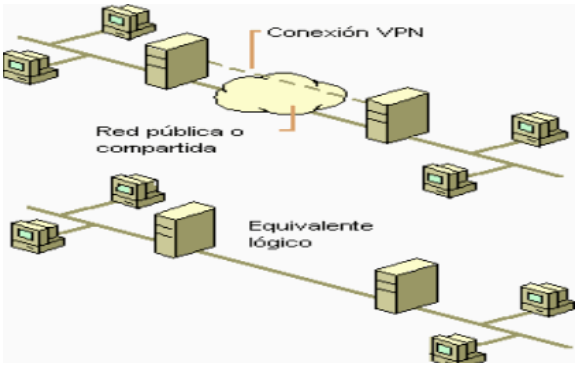


Figura II.2: Conexión VPN y su equivalente lógico.

Como podemos apreciar en la figura II.2 los paquetes de datos de la red privada viajan por medio de un "túnel" definido en la red pública.

2.2.1. TIPOS DE CONEXIÓN

Sistemas basados en Hardware

Los sistemas basados en hardware, son routers que cifran. Son seguros y fáciles de usar, requieren de una configuración correcta, ofrecen un gran rendimiento, porque no malgastan ciclos de procesador haciendo funcionar un Sistema Operativo. Es hardware dedicado, muy rápido y de fácil instalación.

La implementación entre enrutadores provee la capacidad de asegurar un paquete en una parte de la red, esta seguridad se logra a través del tunneling de paquetes.

Las principales ventajas conseguidas con la implementación sobre routers son:

- Capacidad de asegurar el flujo de paquetes entre dos redes, a través de una red pública como internet.

- Capacidad de autentificar y autorizar a usuarios el acceso sobre redes privadas.

Sistemas basados en Firewall

Estos se implementan con software de cortafuegos (firewall). Tienen las ventajas de los mecanismos de seguridad que utilizan los cortafuegos, incluyendo el acceso restringido a la red interna. También realizan la traducción de direcciones (NAT). Estos satisfacen los requerimientos de autentificación fuerte.

Muchos de los cortafuegos comerciales, aumentan la protección, quitando al núcleo del Sistema Operativo algunos servicios peligrosos que llevan estos por default, 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 de encriptación.

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 ofrece el método más flexible en cuanto al manejo de tráfico. Con este tipo, el tráfico puede ser enviado a través de un túnel, en función de las direcciones o protocolos, en cambio en los VPN por hardware, todo el tráfico era enrutado por el túnel. Podemos hacer un enrutamiento inteligente de una manera mucho más fácil.

2.2.2. TECNOLOGÍAS DE ENTUNELAMIENTO VPNS

Existen varios tipos de arquitectura para las VPN, entre ellas se tratarán las siguientes:

VPN de acceso remoto

Esta implementación se trata de comunicaciones donde los usuarios se conectan con la empresa desde sitios remotos (oficinas comerciales, casas, hoteles, etc.) utilizando Internet como medio de acceso. Una vez autenticados tienen un nivel de acceso muy similar al que tienen en la red local de la empresa.

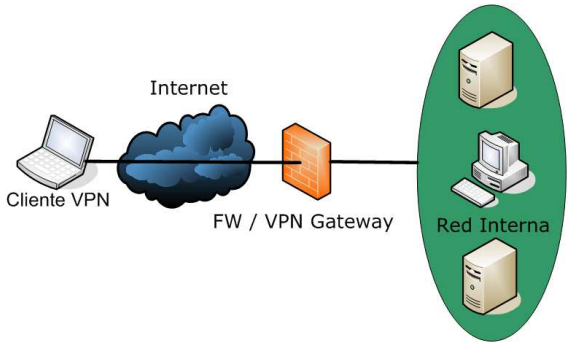


Figura II.3: Infraestructura de una VPN con clientes de acceso remoto.

VPN LAN-a-LAN

Este esquema se utiliza para conectar, por ejemplo, oficinas o sucursales remotas de una empresa con su sede central. Un equipo en la central, que posee un vinculo a Internet permanente, acepta las conexiones vía Internet

provenientes de los otros sitios. A su vez, las sucursales se conectan a Internet utilizando los servicios de su proveedor local de Internet, típicamente mediante conexiones de banda ancha.

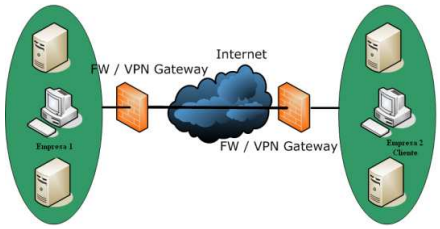


Figura II.4: Infraestructura de una VPN LAN a LAN.

Esta configuración puede ser de dos tipos:

- Tipo Intranet, si la empresa tiene una o más sucursales remotas que quiere unir en una única red privada, puede hacerlo creando una VPN para conectar ambas redes locales.
- Tipo Extranet, cuando la empresa tiene una relación cercana con otra compañía (por ejemplo, una empresa asociada, un proveedor o cliente), entonces pueden desarrollar una VPN que conecte sus redes y permita a estas empresas trabajar en un ambiente compartido.

TUNNELING

Esta técnica consiste en abrir conexiones entre dos máquinas por medio de un protocolo seguro, como puede ser SSH (*Secure Shell*), a través de las cuales se realizan las transferencias inseguras, que pasarán de este modo a ser seguras,

siendo la conexión segura (en este caso de *ssh*) el túnel por el cual se envían los datos para que nadie más aparte de los interlocutores que se sitúan a cada extremo del túnel, pueda ver dichos datos. Este tipo de técnica requiere de forma imprescindible tener una cuenta de acceso seguro en la máquina con la que se quiere comunicar los datos.

Tunneling es una forma de evitar los ataques, sin dejar por ello de utilizar todos aquellos protocolos que carezcan de medios de cifrado, pues las comunicaciones se cifran con un sistema que permita entenderse sólo a las dos máquinas que participan en el intercambio de datos, al no poder descifrar los datos, cualquiera que intercepte desde una tercera máquina los paquetes, no podrá hacer nada con ellos.

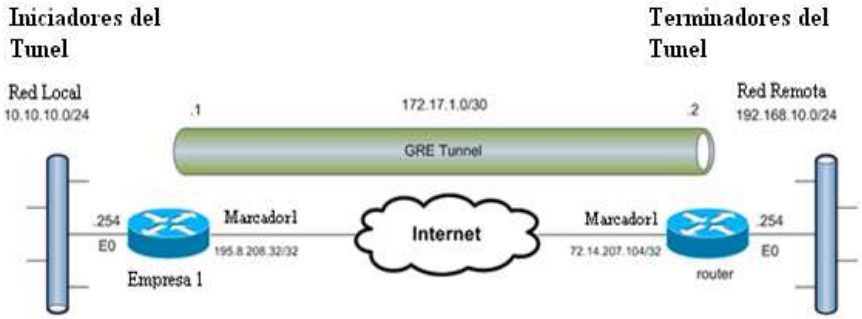


Figura II.5: Componentes básicos de un túnel

Como se puede apreciar en la Figura III – 5 los componentes básicos de un túnel son:

- Un iniciador del túnel

- Uno o varios dispositivos de enrutamiento
- Un conmutador de túneles (opcional)
- Uno o varios terminadores de túneles

El inicio y la terminación del túnel pueden ser hechos por una amplia variedad de equipos o software. Un túnel puede ser empezado, por ejemplo, por un usuario remoto con un computador portátil equipado con un modem análogo y un software de conexión telefónica para hacer una VPN, también puede haber un enrutador de una extranet en una oficina remota o en una LAN pequeña. Un túnel puede ser terminado por otro enrutador habilitado para tal fin, por un switch con esta característica o por un software que haga tal fin.

2.2.3. Requerimientos básicos para una VPN

Por lo general cuando se desea implantar una VPN hay que garantizar la seguridad, integridad y confidencialidad de una VPN por lo que es necesario que proporcione:

- Identificación y autentificación de usuario
- Administración de direcciones
- Cifrado de datos
- Administración de claves
- Soporte a protocolos múltiples

Identificación y autenticación de usuario

La VPN debe ser capaz de verificar la identidad de los usuarios y restringir el acceso a la VPN a aquellos usuarios que no estén autorizados. Así mismo, debe proporcionar registros estadísticos que muestren quien accedió, a que información y cuando.

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

La autenticación es llevada a cabo generalmente al inicio de una sesión, y luego aleatoriamente durante el curso de la misma, para asegurar que no haya algún tercer participante que se haya entrometido en la conversación. La autenticación también puede ser usada para asegurar la integridad de los datos.

Ejemplos de sistemas de autenticación son Challenge Handshake Authentication Protocol (CHAP) y RSA.

Existen dos tipos de técnicas de encriptación que se usan en las VPN: encriptación de clave secreta, o privada, y encriptación de clave pública:

- En la encriptación de clave secreta, se utiliza una contraseña secreta conocida por todos los participantes que necesitan acceso a la información encriptada, dicha contraseña se utiliza tanto para encriptar como para desencriptar la información. Este tipo de encriptación posee el problema que, como la contraseña es compartida por todos los participantes y debe mantenerse secreta, al ser revelada, debe ser cambiada y distribuida a los participantes, con lo cual se puede crear de esta manera algún problema de seguridad.
- La encriptación de clave pública implica la utilización de dos claves, una pública y una secreta. La primera es enviada a los demás participantes. Al encriptar, se usa la clave privada propia y la clave pública del otro participante de la conversación. Al recibir la información, ésta es desencriptada usando su propia clave privada y la pública del generador de la información. La gran desventaja de este tipo de encriptación es que resulta ser más lenta que la de clave secreta.

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

El protocolo más usado para la encriptación dentro de las VPNs es IPSec.

Administración de direcciones

La VPN debe establecer una dirección del cliente en la red privada y debe cerciorarse que las direcciones privadas se conserven así.

Las interfaces virtuales del cliente VPN y del servidor VPN se deben asignar direcciones IP por el servidor de VPN. Por defecto, el servidor de VPN obtiene a las direcciones IP para sí mismo y a clientes de VPN usando Dynamic Host Configuration Protocol (DHCP). También se puede configurar una unión estática de las direcciones IP definidas por una identificación de la red IP y una máscara de subred.

Cifrado de datos

El cifrado de datos es el proceso por el que una información legible se transforma mediante un algoritmo (llamado *cifra*) en información ilegible, llamada *criptograma* o *secreto*. Esta información ilegible se puede enviar a un destinatario con muchos menos riesgos de ser leída por terceras partes. El destinatario puede volver a hacer legible la información, descifrarla, introduciendo la clave del cifrado. A menudo se denomina "encriptación" a este proceso, pero es incorrecto, ya que esta palabra no existe en castellano; se ha importado del inglés "encrypt", que se debe traducir como "cifrar", y por tanto el proceso se debe denominar "cifrado".

Los datos que se van a transmitir a través de la red pública deben ser previamente cifrados para que no puedan ser leídos por clientes no autorizados de la red.

Todas las VPNs tienen algún tipo de tecnología de cifrado, que esencialmente empaqueta los datos en un paquete seguro. El cifrado de datos es considerado tan esencial como la autenticación, ya que protege los datos transportados de poder ser vistos y entendidos en el viaje de un extremo a otro de la conexión.

Los datos son procesados con un algoritmo de hashing para derivar un valor incluido en el mensaje como checksum. Cualquier desviación en el checksum indica que los datos fueron corruptos en la transmisión o interceptados y modificados en el camino.

Administración de claves

La VPN debe generar y renovar las claves de codificación para el cliente y el servidor.

Soporte a protocolos múltiples

La VPN debe ser capaz de manejar los protocolos comunes que se utilizan en la red pública. Estos incluyen el protocolo de internet (IP), el intercambio de paquete de internet (IPX) entre otros.

CAPÍTULO III

TECNOLOGIAS VPNs

Los túneles VPN pueden ofrecer tres servicios de seguridad importantes: autenticación a probar la identidad de los extremos del túnel, encriptación para prevenir el espionaje y la copia de la información confidencial transferida a través del túnel, y las comprobaciones de integridad para asegurar que los datos no se modifican en tránsito.

Figura III.1: VPN en el Modelo OSI

Los túneles pueden existir en varias capas de protocolo como se lo detalla a continuación según la figura III.1:

- Los túneles de nivel 2 llevan de punto a punto el enlace de datos (PPP) las conexiones entre los extremos del túnel de VPN de acceso remoto. En un modo obligatorio, un acceso de red del servidor del ISP intercepta las conexiones de un usuario corporativo de PPP y túneles de estos a la red corporativa. En un modo voluntario, los túneles VPN que prestan toda la seguridad a través de la red pública, de acceso telefónico a los clientes a la red corporativa.
- Los túneles de nivel 3 basadas en IP proporcionan conexiones virtuales. En este enfoque, normal paquetes IP se enrutan entre los extremos del túnel que están separados por cualquier topología de red que intervienen. Paquetes tunelizados se envuelven en IETF definido por las cabeceras que proporcionan la integridad del mensaje y la confidencialidad.

3.1. PPTP: POINT TO POINT TUNNELING PROTOCOL

PPTP es un protocolo desarrollado por Microsoft, U.S. Robotics, Ascend Communications, 3Com/Primary Access, ECI Telematics conocidas colectivamente como PPTP Forum, para implementar redes privadas virtuales o VPN.

PPTP no prevé la confidencialidad o el cifrado, sino que se basa en el protocolo de túnel para proporcionar privacidad. Sin embargo, actualmente sigue siendo muy popular.

Una característica importante en el uso del PPTP es que soporta VPN`s sobre public-switched telephone networks (PSTNs) que son los comúnmente llamados accesos telefónicos a redes.

PPTP amplía el Protocolo punto a punto (PPP) para líneas tradicionales a redes. Además es el más adecuado para las aplicaciones de acceso remoto de VPN, pero también admite interconexión de LAN y opera en la capa 2 del modelo OSI.

PPTP utiliza un túnel para que los paquetes de un protocolo se transporten a través de una red que utilice otro protocolo tal como se muestra en la Figura IV.2. Por ejemplo, los paquetes NWLink pueden encapsularse en paquetes IP. De este modo, los paquetes IPX pueden ser transportados por Internet utilizando TCP/IP. PPTP cuenta con la ventaja añadida de mejorar la seguridad, ya que trabaja al mismo nivel de encriptación que RAS.

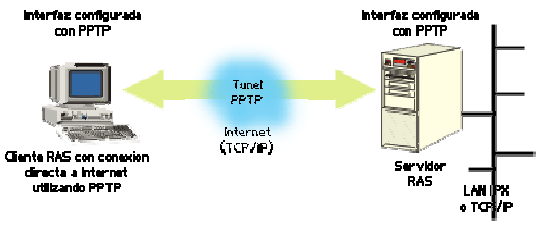


Figura III.2: VPN-PPTP Acceso remoto.

Se examinara dos escenarios distintos en los que se utiliza PPTP. El túnel PPTP entre el cliente y el servidor que permite establecer un canal de comunicación seguro. PPTP que el cliente y el servidor se conecten a través de Internet sin que el cliente tenga que llamar a RAS estableciendo una conexión conmutada. Durante la comunicación, RAS cifra el tráfico entre el cliente y el servidor para generar una corriente de comunicación segura.

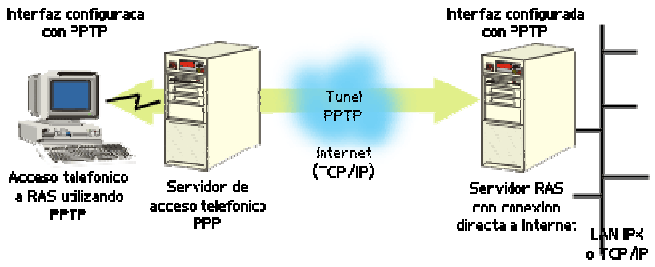


Figura III.3: VPN-PPTP Acceso remoto con RSA.

La figura III.3 muestra un enlace en el que el servidor RAS está conectado a una LAN mediante NWLink el túnel a través de Internet permite que el cliente se conecte a la red NWLink aunque utilice el protocolo TCP/IP.

3.1.1. Usando PPTP

Paquetes de datos dentro de los paquetes de PPTP PPP, a continuación, encapsula los paquetes PPP dentro de los paquetes IP (datagramas) para su transmisión a través de una Internet basada en el túnel VPN. PPTP admite el cifrado de datos y la compresión de estos paquetes. PPTP utiliza también una

forma de General Routing Encapsulation (GRE) para obtener datos desde y hacia su destino final.

PPTP VPN basadas en Internet de acceso remoto son, de lejos la forma más común de PPTP VPN. En este entorno, los túneles VPN se crean a través del siguiente proceso de dos pasos:

a. El cliente PPTP se conecta a su ISP a través de PPP de acceso telefónico a redes (módem tradicional o RDSI).

b. A través del dispositivo de corredor, PPTP crea una conexión de control TCP entre el cliente VPN y el servidor VPN para establecer un túnel. PPTP utiliza el puerto TCP 1723 para estas conexiones.

PPTP VPN también admite la conectividad a través de una LAN. Las conexiones ISP no están obligadas en este caso, por lo que los túneles pueden ser creados directamente como en el paso 2.

Una vez establecido el túnel VPN, PPTP admite dos tipos de flujo de la información:

- Mensajes de control de la gestión y finalmente derribar la conexión VPN. Los mensajes de control pasan directamente entre el cliente VPN y el servidor.
- Paquetes de datos que pasan a través del túnel, hacia o desde el cliente de VPN

3.1.2. Control de conexión PPTP

Una vez que la conexión TCP se establece en el paso 2, PPTP utiliza una serie de mensajes de control para mantener las conexiones VPN. Estos mensajes se enumeran a continuación.

Tabla III.I: Mensajes de control PPTP

Número	Nombre	Descripción
1	StartControlConnectionRequest	Inicia el programa de instalación de la sesión de VPN, pueden ser enviadas por el cliente o servidor.
2	StartControlConnectionReply	Enviado en respuesta a la solicitud de conexión inicio (1), contiene el código de resultado que indica el éxito o el fracaso de la operación de instalación, y también el número de versión del protocolo.
3	StopControlConnectionRequest	Solicitud para cerrar la conexión de control.
4	StopControlConnectionReply	Enviado en respuesta a la solicitud de conexión parada (3), contiene el código de resultado que indica el éxito o el fracaso de la operación de cierre.
5	EchoRequest	Enviados periódicamente por el cliente o servidor a "ping" a la conexión (mantener viva).
6	EchoReply	Enviado en respuesta a la solicitud de eco (5) para mantener la conexión activa.
7	OutgoingCallRequest	Solicitud de crear un túnel VPN enviado por el cliente.
8	OutgoingCallReply	Respuesta a la solicitud de llamada (7), contiene un identificador único de ese túnel.
9	IncomingCallRequest	Solicitud de un cliente de VPN para recibir una llamada entrante desde el servidor.
10	IncomingCallReply	Respuesta a la solicitud de llamada entrante (9), que indica si la llamada entrante debe ser contestada.
11	IncomingCallConnected	Respuesta a la respuesta de llamada entrante (10), establece los parámetros de llamada adicional con el servidor VPN.
12	CallClearRequest	Solicitud de desconexión o una llamada entrante o saliente, enviados desde el servidor a un cliente.
13	CallDisconnectNotify	Respuesta a la solicitud de desconexión (12), enviado de nuevo al servidor.
14	WANErrorNotify	Notificación periódicamente envía al servidor de la Convención, la elaboración, el hardware y las saturaciones del búfer, tiempo de espera y los errores de alineación de bytes.
15	SetLinkInfo	Notificación de cambios en las opciones subyacentes de PPP.

Con los mensajes de control, PPTP utiliza un llamado cookie mágica. La cookie PPTP magia está cableado al número hexadecimal 0x1A2B3C4D. El propósito de esta cookie es garantizar que el receptor interpreta los datos entrantes en los límites correctos de bytes.

3.1.3. PPTP de Seguridad

PPTP admite la autenticación, cifrado y el filtrado de paquetes. Además utiliza la autenticación basado en PPP protocolos como EAP, CHAP y PAP. PPTP admite el filtrado de paquetes en los servidores VPN. Routers intermedios y otros cortafuegos también puede ser configurado para filtrar el tráfico PPTP de manera selectiva.

3.1.4. Especificación PPTP

Una especificación para PPTP fue publicada como. IETF PPTP pero no ha sido propuesto y ratificado como un estándar por la IETF.

PPTP funciona enviando un período de sesiones PPP regular al par con la Encapsulación de enrutamiento genérico (GRE) de protocolo. Un segundo período de sesiones en el puerto TCP 1723 se utiliza para iniciar y gestionar el período de sesiones GRE. PPTP es difícil avanzar más allá de un firewall de

red, ya que requiere de dos sesiones de red. Como tal, los cortafuegos no pueden dejar pasar este tráfico a la perfección, resultando en una incapacidad para conectarse.

Las conexiones PPTP se autentican con Microsoft MSCHAP-v2 o EAP-TLS. El tráfico VPN es opcionalmente protegidos por Microsoft Point-to-Point Encryption (MPPE).

PPTP permite cifrar y encapsular en un encabezado IP multi-protocolo de tráfico que luego se envían a través de una red IP o una red IP pública, como la Internet. Se puede utilizar PPTP para el acceso remoto y de sitio a las conexiones VPN de sitio. Cuando se utiliza la Internet como la red VPN público, el servidor PPTP está habilitado con una interfaz en Internet y una segunda interfaz en la intranet.

3.1.5. Encapsulación

PPTP encapsula tramas PPP en datagramas IP para la transmisión de la red. PPTP utiliza una conexión TCP para la gestión del túnel y una versión modificada de la Encapsulación de enrutamiento genérico (GRE) para encapsular las tramas PPP para los datos del túnel. Carga de los marcos de encapsulado PPP puede ser codificado, comprimido, o ambos.

3.1.6. Cifrado

La trama PPP se cifra con Microsoft Point-to-Point Encryption (MPPE), utilizando las claves de cifrado generada a partir de la MS-CHAPv2 o proceso de autenticación EAP-TLS. Los clientes VPN deben utilizar el MS-CHAPv2 o protocolo de autenticación EAP-TLS para que las cargas útiles de las tramas PPP a cifrar. PPTP se está aprovechando de la encriptación PPP subyacente y encapsulando una trama PPP previamente codificados.

MSCHAP-v2 puede verse comprometida si los usuarios eligen contraseñas débiles. El certificado basado en EAP-TLS ofrece una opción de seguridad superior para PPTP.

3.2. L2TP (Layer 2 Tunneling Protocol)

L2TP fue creado como el sucesor de PPTP y L2F. Las dos compañías abanderadas de cada uno de estos protocolos, Microsoft por PPTP y Cisco por L2F, acordaron trabajar en conjunto para la creación de un único protocolo de capa 2 y así lograr su estandarización por parte de la IETF. Como PPTP, L2F fue diseñado como un protocolo de túnel usando para ello encapsulamiento de cabeceras. Una de las grandes diferencias entre PPTP y L2F, es que el túnel de este último no depende de IP y GRE, permitiéndole trabajar con otros medios físicos por ejemplo Frame Relay.

Paralelamente al diseño de PPTP, L2F utilizó PPP para autenticación de usuarios accediendo vía telefónica conmutada, pero también incluyó soporte para TACACS+ y Radius. Otra gran diferencia de L2F con respecto a PPTP es que permite que un único túnel soporte más de una conexión. Hay dos niveles de autenticación del usuario: primero, por el ISP antes de crear el túnel; segundo, cuando la conexión está configurada y la autenticación la realiza el gateway corporativo. Todas las anteriores características de L2F han sido transportadas a L2TP.

Encapsulado de tramas PPP sobre cualquier medio, no necesariamente redes IP. En el caso IP se usa UDP, puerto 1701. Tras un largo proceso como borrador, L2TP pasa a ser una propuesta de estándar en Agosto de 1.999.

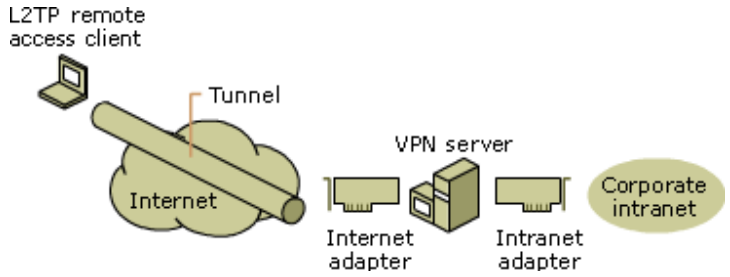


Figura III.4: VPN-L2TP Acceso remoto con RSA.

El L2TP sobre las redes IP utiliza UDP y una serie de mensajes del L2TP para el mantenimiento del túnel. El L2TP también utiliza UDP para enviar tramas del PPP encapsuladas del L2TP como los datos enviados por el túnel. Se pueden cifrar y/o comprimir las cargas útiles de las tramas PPP encapsuladas. La Figura IV.5 muestra la forma en que se ensambla un paquete L2TP antes de su

transmisión. El dibujo muestra un cliente de marcación que crea un túnel a través de una red. El diseño final de trama muestra la encapsulación para un cliente de marcación (controlador de dispositivos PPP). La encapsulación supone el L2TP sobre IP.

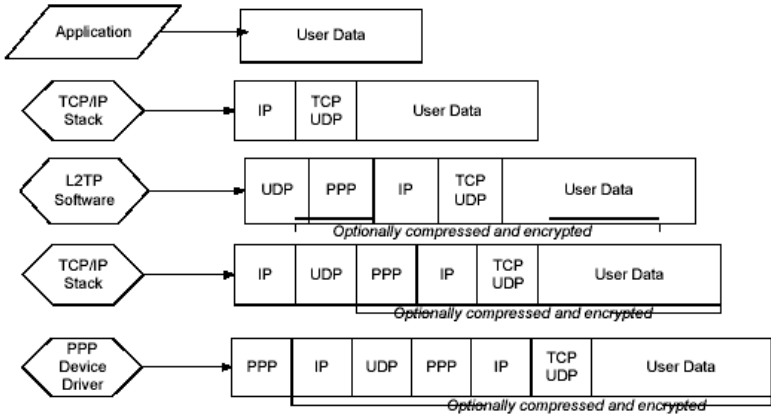


Figura III.5: Ensamblaje del paquete L2TP

3.2.1. Componentes básicos de un Túnel L2TP.

3.2.1.1. Concentrador de acceso L2TP (LAC)

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

3.2.1.2. Servidor de red L2TP (LNS)

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

3.2.1.3. Túnel

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

3.2.2 Topología de L2TP

La figura IV.6 describe un escenario típico L2TP. El objetivo es tunelizar tramas PPTP entre un sistema remoto o un cliente LAC y un LNS localizado en la LAN corporativa.

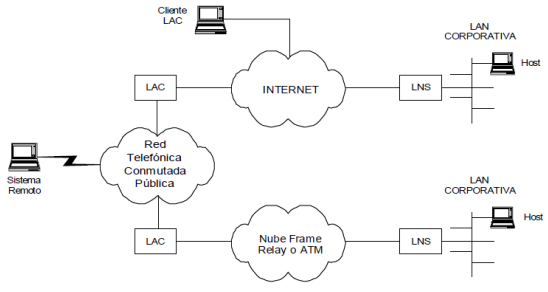


Figura III.6: Distintos escenarios de túneles L2TP.

El sistema remoto inicia una conexión PPP a través de la red de telefonía pública conmutada a un LAC. El LAC luego tuneliza la conexión PPP a través de Internet o una nube Frame Relay o ATM a un LNS por donde accede a la LAN remota corporativa. La dirección del sistema remoto es dada desde la LAN corporativa por medio de una negociación PPP NCP. La autenticación, autorización y acounting puede ser provista por el dominio de la red corporativa remota como si el usuario estuviera conectado a un servidor de acceso de la red directamente.

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

3.2.3. Estructura del Protocolo L2TP

L2TP utiliza dos tipos de mensajes, Los mensajes de control y los mensajes de datos. Los mensajes de control son usados en el establecimiento, mantenimiento y finalización de túneles y llamadas.

Los mensajes de datos son usados para encapsular tramas PPP que está siendo transportadas sobre el túnel. Los mensajes de control utilizan un canal de control confiable con el cual L2TP garantiza la entrega. Los mensajes de datos no son retransmitidos cuando ocurren pérdidas de paquetes.

Las tramas PPP son transportadas sobre un canal de datos no confiable y son encapsuladas primero por una cabecera L2TP y luego por una cabecera de transporte de paquetes que pueden ser UDP, Frame Relay o ATM. Los mensajes de control son enviados sobre un canal de control L2TP confiable, el cual transmite paquetes en banda sobre el mismo transporte de paquetes. Para esto se requiere que números de secuencia estén presentes en todos los mensajes de control. Los mensajes de datos pueden usar esos números de secuencia para reordenar paquetes y detectar pérdidas de los mismos.

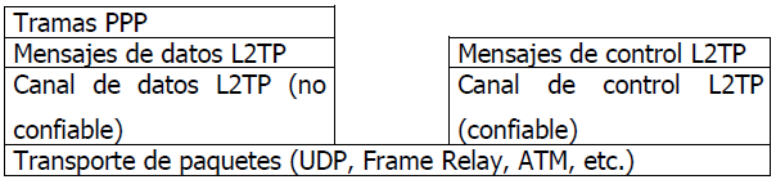


Figura III.7: Estructura del protocolo L2TP

3.2.3.1. Formato de una Cabecera L2TP

Los paquetes L2TP para el canal de control y el canal de datos comparten un formato de cabecera común.

T	L	x	x	S	c	O	P	x	x	x	x	Ver	Length (Opc)
Tunnel ID													Session ID
Ns (Opc)													Nr (Opc)
Offset Size(Opc)													Offset padding (Opc)

Figura III.8: Formato de una cabecera L2TP

El bit T (type), indica el tipo de mensaje, es 0 para un mensaje de datos y 1 para un mensaje de control.

Si el bit L (length) es 1, el campo Longitud está presente. Este bit debe estar puesto en 1 para los mensajes de control.

Los bits x son reservados para futuras extensiones. Todos los bits reservados deben ser puestos en 0 para los mensajes salientes y deben ser ignorados por el receptor.

Si el bit S (sequence) de Secuencia (S) esta puesto en 0, el Ns y Nr están presentes. El bit S debe estar puesto en 1 para los mensajes de control.

Si el bit O (Offset) es 1, el campo de tamaño Offset está presente. El bit O debe ser puesto en 0 para los mensajes de control.

Si el bit P (Priority) es 1, los mensajes de datos deben recibir un trato preferencial en las colas locales y en la transmisión.

Los requerimientos echo LCP usados como keepalive para el enlace deben generalmente ser enviados con este bit puesto en 1 dado que un intervalo de tiempo grande originado por una conexión local puede originar una demora en los mensajes keepalive ocasionando una pérdida innecesaria del enlace. Esta característica es solamente usada por los mensajes de datos. El bit P debe ser puesto en 0 para todos los mensajes de control.

El campo Ver debe ser 2 e indicar la versión de la cabecera L2TP de los mensajes de datos. Los paquetes recibidos con un campo Ver desconocido deben ser descartados.

El campo Length indica la longitud total del mensaje en octetos. El campo Tunnel ID sirve como identificador para el control de conexión. Los túneles L2TP son nombrados por identificadores que tienen significado local únicamente. Es decir, el mismo túnel.

El campo Session ID indica el identificador para una sesión dentro del túnel. Al igual que los identificadores de túnel, las sesiones L2TP son nombradas por identificadores que tienen únicamente significado local.

El campo Ns indica el número de secuencia para los mensaje de datos y de control.

El campo Nr indica el número de secuencia esperado en el siguiente mensaje de control a ser recibido. En los mensajes de datos el campo Nr es reservado, y si es presente debe ser ignorado.

Si el campo Offset Size está presente, especifica el número de octetos después de la cabecera L2TP, a partir de los cuales la carga útil de datos es esperada a que inicie o a que se encuentre.

3.2.3.2. Tipos de mensajes de control

El protocolo L2TP define los siguientes tipos de mensajes de control para la creación, mantenimiento y finalización del túnel.

Manejo de la conexión de control

0 (reserved)

1 (SCCRQ) Start-Control-Connection-Request

2 (SCCRP) Start-Control-Connection-Reply

3 (SCCCN) Start-Control-Connection-Connected

4 (StopCCN) Stop-Control-Connection-Notification

5 (reserved)

6 (HELLO) Hello

Manejo de la llamada

7 (OCRQ) Outgoing-Call-Request

8 (OCRP) Outgoing-Call-Reply

9 (OCCN) Outgoing-Call-Connected

10 (ICRQ) Incoming-Call-Request

11 (ICRP) Incoming-Call-Reply

12 (ICCN) Incoming-Call-Connected

13 (reserved)

14 (CDN) Call-Disconnect-Notify

Reporte de errores

15 (WEN) WAN-Error-Notify

Control de la sesión PPP

16 (SLI) Set-Link-Info

3.2.4. Operación de protocolo

Para tunelizar una sesión PPP con L2TP se necesita llevar a cabo dos pasos, el primero, el establecimiento de una conexión de control para el túnel y el segundo, el establecimiento de una sesión respondiendo al requerimiento de una llamada entrante o saliente.

El túnel y su correspondiente conexión de control deben ser establecidos antes que una llamada entrante o saliente sea iniciada. Una sesión L2TP debe ser establecida antes que L2TP pueda empezar a tunelizar tramas PPP. Múltiples sesiones pueden existir a través de un túnel único y múltiples túneles pueden existir entre el mismo LAC y LNS.

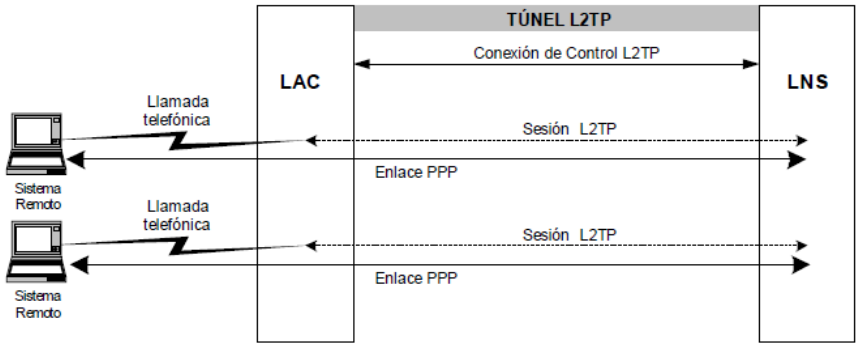


Figura III.9: Túnel de tramas PPP usando L2TP

La figura III.9 ilustra la relación que puede existir entre un LAC y un LNS, claramente se notan los puntos terminales de un enlace PPP de una sesión L2TP, de una conexión de control L2TP y del túnel en sí.

3.3. IPSEC (INTERNET PROTOCOL SECURITY)

IPSEC consiste en un conjunto de propósitos del IETF que delinean un protocolo IP seguro para IPv4 y IPv6, es en realidad una colección de múltiples protocolos relacionados. Puede ser usado como una solución completa de protocolo VPN o simplemente como un esquema de encriptación para L2TP o PPTP. IPsec existe en el nivel de red en OSI, para extender IP para el propósito de soportar servicios más seguros basados en Internet.

Otros protocolos de seguridad para Internet de uso extendido, como SSL, TLS y SSH operan de la capa de transporte (capas OSI 4 a 7) hacia arriba. Esto hace que IPsec sea más flexible, ya que puede ser utilizado para proteger protocolos de la capa 4, incluyendo TCP y UDP, los protocolos de capa de transporte más usados. IPsec tiene una ventaja sobre SSL y otros métodos que operan en capas superiores. Para que una aplicación pueda usar IPsec no hay que hacer ningún cambio, mientras que para usar SSL y otros protocolos de niveles superiores, las aplicaciones tienen que modificar su código.

IPsec es un conjunto de protocolos cuya función es asegurar las comunicaciones sobre el Protocolo de Internet (IP) autenticando y/o cifrando cada paquete IP en un flujo de datos. IPsec también incluye protocolos para el establecimiento de claves de cifrado.

3.3.1. Asociaciones de Seguridad. (SA)

El concepto de asociación de seguridad (SA) es fundamental en IPSec. Tanto AH como ESP, hacen uso de asociaciones de seguridad y una función importante de IKE es el mantenimiento y establecimiento de las asociaciones de seguridad. Cualquier implementación de AH o ESP debe soportar el concepto de asociación de seguridad.

Una SA es una conexión simplex que permite servicios de seguridad al tráfico que transporta. Una SA permite servicios de seguridad mediante el uso de AH o de ESP pero no de ambos. Si ambos no se aplican en un flujo de tráfico, entonces existirán dos o más SAs para permitir la protección al flujo de tráfico.

Para asegurar la comunicación bidireccional típica entre dos Hosts o dos puertas de enlace, se requieren dos asociaciones de seguridad (un a en cada sentido).

Una SA es identificada únicamente por un triplete consistente en un índice de parámetros de seguridad (SPI), una dirección IP de destino y un identificador de protocolo de seguridad (AH o ESP).

El conjunto de servicios de seguridad ofrecido por una SA depende del protocolo de seguridad seleccionado, del modo de la SA, el punto terminal de la SA, y de los servicios opcionales seleccionados dentro del protocolo. Asi se tiene:

AH.- Proporciona autenticación del origen de los datos e integridad sin conexión para datagramas IP. La precisión de estos servicios estará en función de la "granularidad" de la asociación de seguridad con la que se emplea AH. AH ofrece además servicio anti-replay (integridad de secuencia parcial). El Protocolo AH es el apropiado cuando la confidencialidad no se requiere confidencialidad (o cuando no está permitida por prohibición de gobiernos). AH también autenticación para porciones de la cabecera IP (pero no de las partes mutables en la ruta), que pueden ser necesarias en algunos contextos. **ESP** proporciona de forma opcional confidencialidad del tráfico (cuya fuerza depende del algoritmo de encriptación utilizado). Además proporciona, también de forma opcional, autenticación como en el caso anterior. Si se negocia la autenticación para una SA con ESP el receptor también elige si fuerza a cumplir un servicio anti-replay con las mismas características que las ofrecidas por AH. El alcance de la autenticación ofrecida por ESP es más estrecho que el del ofrecido por AH, por ejemplo: las cabeceras que quedan por fuera de la cabecera ESP no están protegidas. Si solo se desea aportar autenticación únicamente a las capas superiores, entonces ESP es la elección apropiada y es más eficiente en tamaño que usar ESP encapsulado con AH. Aunque la confidencialidad y la autenticación son opcionales, no se pueden omitir ambas, al menos una debe ser escogida.

Si se elige el servicio de confidencialidad, entonces una SA con ESP (en modo túnel) entre dos puertas de enlace pueden ofrecer confidencialidad en un flujo

de tráfico parcial. El uso del modo túnel encriptar las cabeceras IP internas, ocultando las identidades de la (última) vía de tráfico y el destino. También usar relleno en la carga de ESP para ocultar el tamaño de los paquetes.

3.3.2. Componentes IPEsec

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

3.3.2.1. Protocolos de Seguridad

IPSec emplea dos protocolos diferentes - AH y ESP - para asegurarla autenticación, integridad y confidencialidad de la comunicación. Puede proteger el datagrama IP completo o sólo los protocolos de capas superiores. Estos modos se denominan, respectivamente, modo túnel y modo transporte. En modo túnel el datagrama IP se encapsula completamente dentro de un nuevo datagrama IP que emplea el protocolo IPSec. En modo transporte IPSec

sólo maneja la carga del datagrama IP, insertándose la cabecera IPSec entre la cabecera IP y la cabecera del protocolo de capas superiores.

3.3.2.1.1. Protocolo AH

La Cabecera de Autenticación o *AH* proporciona en el ámbito de IPSec la autenticación del emisor y la integridad del mensaje mediante el cálculo de un código HMAC. Una vez ambos extremos han establecido una SA, utilizan la clave acordada durante el intercambio inicial como clave simétrica con la que generar los resúmenes que se incluyen en las cabeceras. Sólo ambos extremos conocedores de la clave podrán calcular los resúmenes y verificar la integridad del paquete. Del mismo modo, un resumen que se corresponde con los contenidos de un paquete garantiza la autenticación del emisor, ya que sólo éste conocerá la clave con la que generar el resumen.

En AH, el resumen es calculado sobre la carga útil del paquete y las cabeceras estáticas del mismo, esto es, aquellas que no se modificarán durante el proceso, lo cual incluye las direcciones IP de origen y destino. Esto provoca que AH tenga graves problemas para tratar con NAT, ya que las pasarelas que utilizan este protocolo modifican la dirección IP de origen de los paquetes salientes, y la dirección IP de destino de los paquetes entrantes, acción que precisamente AH se encarga de detectar.

Este proceso restringe la posibilidad de emplear NAT, que puede ser implementada con NAT transversal. Por otro lado, AH puede proteger opcionalmente contra ataques de repetición utilizando la técnica de ventana deslizante y descartando paquetes viejos. AH protege la carga útil IP y todos los campos de la cabecera de un datagrama IP excepto los campos mutantes, es decir, aquellos que pueden ser alterados en el tránsito. En IPv4, los campos de la cabecera IP mutantes (y por lo tanto no autenticados) incluyen TOS, Flags, Offset de fragmentos, TTL y suma de verificación de la cabecera. AH opera directamente por encima de IP, utilizando el protocolo IP número 51. Una cabecera AH mide 32 bits, he aquí un diagrama de cómo se organizan:

<table>
<tr><td>0 - 7 bit</td><td>8 - 15 bit</td><td>16 - 23 bit</td><td>24 - 31 bit</td></tr>
<tr><td>Next header</td><td>Payload length</td><td colspan="2">RESERVED</td></tr>
<tr><td colspan="4">Security parameters index (SPI)</td></tr>
<tr><td colspan="4">Sequence number</td></tr>
<tr><td colspan="4">Hash Message Authentication Code (variable)</td></tr>
</table>

Figura III.15: Cabecera AH

Significado de los campos:

Next header.- Identifica el protocolo de los datos transferidos.

Payload length.- Tamaño del paquete AH.

RESERVED.- Reservado para uso futuro (hasta entonces todo ceros).

Security parameters index (SPI).- Indica los parámetros de seguridad que, en combinación con la dirección IP, identifican la asociación de seguridad implementada con este paquete.

Sequence number.- Un número siempre creciente, utilizado para evitar ataques de repetición.

HMAC.- Contiene el valor de verificación de integridad (ICV) necesario para autenticar el paquete; puede contener relleno.

3.3.1.2.2. Protocolo Encapsulating Security Payload (ESP)

El protocolo ESP proporciona autenticidad de origen, integridad y protección de confidencialidad de un paquete. ESP también soporta configuraciones de sólo cifrado y sólo autenticación, pero utilizar cifrado sin autenticación está altamente desaconsejado porque es inseguro. Al contrario que con AH, la cabecera del paquete IP no está protegida por ESP (aunque en ESP en modo túnel, la protección es proporcionada a todo el paquete IP interno, incluyendo la cabecera interna; la cabecera externa permanece sin proteger). ESP opera directamente sobre IP, utilizando el protocolo IP número 50.

Los primeros 32 bits de la cabecera ESP especifican el *Índice de Parámetros de Seguridad* (SPI). Este SPI especifica qué SA emplear para desencapsular el paquete ESP. Los siguientes 32 bits almacenan el *Número de Secuencia*. Este número de secuencia se emplea para protegerse de ataques por repetición de mensajes. Los siguientes 32 bits especifican el *Vector de Inicialización* (IV - Initialization Vector) que se emplea para el proceso de cifrado. Los algoritmos de cifrado simétrico pueden ser vulnerables a ataques por análisis de frecuencias si no se emplean IVs. El IV asegura que dos cargas idénticas generan dos cargas cifradas diferentes.

IPSec emplea cifradores de bloque para el proceso de cifrado. Por ello, puede ser necesario rellenar la carga del paquete si la longitud de la carga no es un múltiplo de la longitud del paquete. En ese caso se añade la longitud del relleno (pad length). Tras la longitud del relleno se coloca el campo de 2 bytes *Siguiente cabecera* que especifica la siguiente cabecera. Por último, se añaden los 96 bit de HMAC para asegurar la integridad del paquete. Esta HMAC sólo tiene en cuenta la carga del paquete: la cabecera IP no se incluye dentro de su proceso de cálculo.

El uso de NAT, por lo tanto, no rompe el protocolo ESP. Sin enmbargo, en la mayoría de los casos, NAT aún no es compatible en combinación con IPsec. NAT-Transversal ofrece una solución para este problema encapsulando los paquetes ESP dentro de paquetes UDP.

0 - 7 bit	8 - 15 bit	16 - 23 bit	24 - 31 bit
Security parameters index (SPI)			
Sequence number			
Payload data (variable)			
	Padding (0-255 bytes)		
		Pad Length	Next Header
Authentication Data (variable)			

Figura III.16: Diagrama de paquete ESP:

Significado de los campos

Security parameters index (SPI).- Identifica los parámetros de seguridad en combinación con la dirección IP.

Sequence number.- Un número siempre creciente, utilizado para evitar ataques de repetición.

Payload data.- Los datos a transferir.

Padding.- Usado por algunos algoritmos criptográficos para rellenar por completo los bloques.

Pad length.- Tamaño del relleno en bytes.

Next header.- Identifica el protocolo de los datos transferidos.

Authentication data.- Contiene los datos utilizados para autenticar el paquete.

3.3.2.2. Protocolos de Gestión de Claves (IKE).

Para implementar soluciones VPN con encriptación, es necesario cambiar periódicamente las claves de encriptación. Fallos en los cambios de las claves hacen a la red ser susceptible de ataques de fuerza bruta. IPsec resuelve el problema con IKE, que utiliza otros dos protocolos para autenticar a los pares y generar las claves. IKE utiliza DH para generar claves simétricas. También gestiona la negociación de otros parámetros de seguridad, como los datos a proteger, fuerza de las claves, los métodos de hash y protección contra replays. Utiliza el UDP 500.

IKE negocia las SA, que son acuerdos entre dos peers en un intercambio IPsec, y consiste en todos los parámetros requeridos para establecer una comunicación satisfactoria.

Funciones IKE:

- Negociación de las características de las SA
- Generación automática e las claves
- Refresco automático de las claves
- Configuración manual razonable

Las SA requieren:

- Internet Security Association and Key Management Protocol (ISAKMP)→es un protocolo que define los mecanismos para

implementar IKE y negociar las políticas de seguridad. ISAKMP se puede implementar sobre cualquier protocolo de transporte.

- SKEME→es un protocolo de intercambio de claves que define como derivar material de claves de autenticación con un refresco rápido de claves.
- OAKLEY→un protocolo de intercambio de claves que define con adquirir las claves de autenticación. El mecanismo básico es el algoritmo DH.

IKE negocia automáticamente las SA IPsec y establece comunicaciones IPsec seguras sin configuración manual previa. Incluye estas características:

- Elimina la necesidad de especificar manualmente todos los parámetros de seguridad en los dos peers
- Permite especificar un tiempo de vida para las SA IPsec
- Permite el cambio de las claves durante las sesiones IPsec
- Permite soporte a las Certification Authority para hacer escalable la implementación
- Permite autenticación dinámica a los peers

3.3.2.2.1. Modos y Fases IKE.

A. Fases IKE.

IKE fase 1

Es la negociación inicial de las SAs entre dos peers IPsec, puede incluir autenticación. Esta conversación entre dos peers puede ser susceptible de espionaje sin comprometer significativamente el intercambio de claves. Las SAs de fase uno son bidireccionales, los datos pueden ser enviados y recibidos usando las mismas claves generadas. Ocurre en dos modos: modo principal y modo agresivo.

IKE fase 1.5 (opcional)

A fin de autenticar a los participantes clientes de la VPN, se puede utilizar un protocolo llamado Extender Authenticaton (Xauth), que provee autenticación de usuarios en los túneles IPsec dentro del protocolo IKE. Adicionalmente se pueden intercambiar otros parámetros entre los peers, DNS, IP address.

IKE fase 2

Esta fase la negocia el ISAKMP. Como las SA que son utilizadas por IPsec son unidireccionales, se necesitan claves separadas para los diferentes flujos. Los dos peers están entonces de acuerdo en los transform sets, hash methods, y otros parámetros. Quick mode es el método utilizado para las SA de fase 2.

IPsec Transform Sets

En vez de negociar cada protocolo individualmente, los agrupa en transform sets.

Security Associations

Cuando los peers llegan a un acuerdo en los parámetros de seguridad que van a utilizar, cada dispositivo guarda la información en una Security Policy Database (SPD). Esta base de datos incluye los algoritmos de encriptación y autenticación, ip destino, modo de transporte, tiempo de vida de las claves, etc. Esto es lo que se llama SA. Cada SA es unidireccional por lo que se necesitan dos SA para tener comunicación bidireccional. El servicio VPN indexa la SA con un numero llamado Security Parameter Index (SPI). En vez de enviar los parámetros individuales por el túnel, el origen inserta el SPI en el encabezado ESP. Al llegar al destino, el peer saca toda la información y la guarda en su SPD y procesa los datos según su SPD.

Ipsec Tunnel Operation

Los dos últimos pasos:

- Data Transfer

Al completarse la fase 2 de IKE y quick mode establece las IPsec SA, comienza el intercambio de datos entre los hosts.

- IPsec Tunnel Termination

Las IPsec SA se terminan borrándolas o por time out. Puede darse por time out cuando durante un tiempo determinado o un número determinado de bytes han pasado por el túnel. Cuando terminan las SA, las claves se descartan. Si se necesita reestablece la comunicación el proceso comienza de nuevo.

B. Modos de operación IKE

Main mode

Comienza las sesión IKE con un indicador enviando una propuesta de conexión al vecino. Estas propuestas definen los protocolos de autenticación y encriptación que son aceptables, la longitud de las claves y las características de secretismo a utilizar~PFS perfect forward secrecy. Múltiples propuestas se pueden enviar en una oferta. El primer intercambio entre nodos establece las políticas básicas de seguridad. El peer elige la propuesta adecuada y envía la elegida al que inicio la comunicación. El siguiente intercambio pasa las claves públicas DH y otros datos. Todas las negociaciones siguientes son encriptadas dentro de la SA IKE. El tercer

intercambio autentica la sesión ISAKMP. Una vez que la SA IKE se ha establecido, la negociación IPsec (quick mode) comienza.

Aggressive Mode

Separa la IKE SA en tres paquetes, con toda la información requerida para la SA pasada por el initiator. El responder envía la propuesta, claves, y la identificación y autentica la sesión en el siguiente paquete. El initiator contesta autenticando la sesión. La negociación es más rápida que en el main mode y los id de initiator y responder pasan en texto plano.

Quick mode

Es similar al aggressive mode, excepto la negociación que debe ser protegida dentro de la IKE SA. Negocia la SA para la encriptación de datos y administra el intercambio de calves para la IPsec SA. Si el respondent da una respuesta negativa, el initiator solicita el main mode.

CAPITULO IV

ESTUDIO COMPARATIVO DE LAS TECNOLOGIAS VPN

El objetivo primordial del estudio comparativo es seleccionar la alternativa más adecuada para el diseño de una red VPN en la Corte Superior de Justicia, para lo cual se toma en consideración los Factores cuantitativos y cualitativos de las tecnologías VPN.

4.1. IDENTIFICACION DE LAS ALTERNATIVAS A COMPARAR

Los protocolos a comparar son:

- PPTP
- L2TP
- IPSEC

4.2. DETERMINACION DE LOS FACTORES

Los Factores que influyen en la elección de la mejor opción se presentan a continuación:

TABLA IV.I: Variables con sus respectivos factores

VARIABLE	FACTORES
COSTOS	• Costo de implementación • Costo de mantenimiento
USABILIDAD	• Escenarios VPN • Popularidad • Disponibilidad de los recursos y de la información
CONTROL DE ACCESO A LOS RECURSOS	• Algoritmos de autenticación • Vulnerabilidad
INTEGRIDAD	• Algoritmos de cifrado

4.2.1. COSTOS

Costo de Implementación

Es el costo que tendrá la implementación VPN tomando en cuenta el requerimiento de equipos y certificados.

Costo de Mantenimiento

Se considera el costo anual por el mantenimiento de la VPN

4.2.2. USABILIDAD

Escenarios VPN

Son los escenarios que se pueden implementar en cada una de las tecnologías VPN.

Popularidad

Independientemente del modo de funcionamiento la popularidad implica el conocimiento que tiene la colectividad de las tecnologías VPN.

4.2.3. CONTROL DE ACCESO A LOS RECURSOS

Métodos de Autenticación

La autenticación es una característica que trata de asegurar el origen de una información, evitando de esta forma posibles suplantaciones

Algoritmos de autenticación

Aseguran a los participantes de la misma red que están intercambiando información con el usuario o dispositivo correcto.

Vulnerabilidad

Se refiere a que tan susceptible es la red a los ataques.

4.2.4. INTEGRIDAD

Algoritmos de cifrado

La información legible se transforma mediante un algoritmo (llamado *cifra*) en información ilegible, llamada *criptograma* o *secreto*.

4.3. CLASIFICAR LOS FACTORES EN SUBJETIVOS Y OBJETIVOS

Para el mejor manejo de los factores a continuación se procederá a clasificar los factores en Factores objetivos y subjetivos:

4.3.1. Factores Objetivos.- Son aquellos factores que se pueden cuantificar.

- Costo de Implementación
- Costo de Mantenimiento

- Escenarios VPN
- Algoritmos de autenticación
- Algoritmos de cifrado

4.3.2. Factores subjetivos.- Son aquellos factores que no se pueden cuantificar.

- Modo de funcionamiento
- Popularidad
- Vulnerabilidad

4.4. OBTENCION DE LA MEJOR TECNOLOGÍA VPN RESPECTO A LOS FACTORES DE LAS TECNOLOGIAS VPN

Este propósito se cumplirá a través del método de Brown y Gibson

4.4.1. MÉTODO DE BROWN Y GIBSON

Este método, combinan los factores posibles de cuantificar con los no cuantificables a los que asignan valores ponderados de peso relativo. El Método consta de cuatro etapas:

4.4.1.1. Asignar un valor relativo a cada Factor Objetivo FO_i para cada factor.

4.4.1.2. Estimar un valor relativo de cada Factor Subjetivo FS_i para cada factor.

TABLA IV.II: Factores de estudio y su ponderación

FACTOR	PONDERACIÓN
Costo de Implementación	0,15
Costo de Mantenimiento	0,15
Escenarios VPN	0,09
Algoritmos de autenticación	0,07
Algoritmos de cifrado	0,20
Método de autenticación	0,15
Popularidad	0,05
Vulnerabilidad	0,14
TOTAL	1,00

El peso relativo, sobre la base de una suma igual a uno, depende fuertemente del criterio y experiencia del Evaluador.

4.4.1.3. Combinar los factores objetivos y subjetivos.- Al comparar las tecnologías VPN, se procede a asignar una calificación a cada factor en una tecnología VPN de acuerdo a una escala predeterminada en este caso será de 0-20.

La suma de las calificaciones ponderadas permitirá seleccionar la tecnología VPN que acumule el mayor puntaje.

TABLA IV.III: Asignación de valores a los Factores Objetivos y Relativos

	Tec. a comparar / Factor	PPTP	L2TP	IPSEC
FACTORES OBJETIVOS	Costo de Implementación	400,00	300,00	250,00
	Costo de Mantenimiento	2400,00	2000,00	200,00
	Escenarios VPN	2	2	3
	Algoritmos de autenticación	2	1	2
	Algoritmos de cifrado	1	1	2
FACTORES SUBJETIVOS	Métodos de Autenticación	14	16	17
	Popularidad	20	14	12
	Vulnerabilidad	5	14	18

En la Tabla IV.III se combinan los factores objetivos y subjetivos pero no todos están en la escala predeterminada.

El método dice que todos los factores deben ser calificados en la misma escala en este caso 20 puntos para lo cual se aplica una regla de tres simple a los factores cuantificables excepto los costos ya que no se puede asignar una alta calificación al costo más alto sino por el contrario se debe asignar la mayor calificación al menor costo para lo cual se aplica una regla de tres inversa. Y

para los factores subjetivos se procede a asignar una calificación directa de acuerdo a la encuesta realizada.

Costo de implementación

El costo aproximado en una posible instalación de VPN PPTP es de $500, 600 para $L2TP y $850 para IPSEC, tomando en cuenta que el menor costo será el más conveniente para la empresa.

Para IPSEC:

850,00 – 500,00 = 350

500_____20

350_____X $= \frac{(150)(20)}{500} = 14$

20 – 14 = 6

La calificación del costo de implementación para IPSEC es 6

Para L2TP:

600,00 – 500,00 = 100

500_____20

100_____X $= \frac{(50)(20)}{500} = 4$

20 – 4 = 16

La calificación del costo de implementación para L2TP es 16

Para PPTP:

Por ser el menor costo tiene una calificación de 20

Costo de Mantenimiento

En este caso el costo aproximado de mantenimiento en una posible instalación de VPN PPTP es de $2.468, 2.000 para $L2TP y $200 PARA IPSEC anuales, tomando en cuenta que el menor costo será el más conveniente para la empresa.

Para PPTP:

2400,00 – 200,00 = 2200,00

200_____20

2200_____X $= \frac{(2200)(20)}{200} = 220$

20 – 220 = -200

Cuando el costo es negativo como en este caso -200 se procede a asignar una calificación de cero.

Para L2TP:

2000,00 – 200,00 = 1800

200_____20

1800_____ X $= \frac{(1800)(20)}{200} = 180$

20 – 180 = -160

Al igual que el costo anterior es negativo por lo tanto se procede a asignar una calificación de cero.

Para IPSEC:

Como es el menor valor de todos entonces tiene una calificación de 20

200,00

Escenarios VPN

En el caso de los escenarios se tiene que PPTP, L2TP se puede implementar en sus dos escenarios Acceso remoto de Host a Red, de Red a Red y túnel aunque para esta última tanto PPTP como L2TP tenga que combinarse con IPSEC para

cumplir con este propósito, por lo que las tres tecnologías poseen un puntaje de 20.

Algoritmos de Autenticación

IPSEC a través del algoritmo Hash se tiene md5, SHA. Pero cabe recalcar que IPSec se puede combinar con PPTP o L2TP para ofrecerles mayor seguridad a estos protocolos por lo que también utiliza los algoritmos de autenticación de éstos. Entonces la calificación asignada a IPSec es de 20 puntos.

L2TP a más de usar los protocolos nativos de PPTP como PAP y CHAP también trabaja con TACACS+ y Radius obteniendo una calificación de 13,33 puntos.

PPTP utiliza la autenticación basado en PPP protocolos como MS-CHAP, CHAP, PAP y SPAP. Obteniendo una calificación de 6,66 puntos.

Métodos de Autenticación

Los métodos de autenticación en PPTP es la autenticación de usuarios locales por ende es muy susceptible y al igual que las comparaciones anteriores se la combina con IPSEC para obtener mejores resultados y en este caso en PPTP y

L2TP se tiene como métodos de autenticación: claves pre compartidas y Autoridades certificadoras y en IPSEC se tiene claves pre compartidas, RSA y Autoridades certificadoras[1].

Algoritmos de Cifrado

PPTP.- trabaja con Microsoft Point-to-Point Encryption (MPPE) y GRE, por lo que se tiene una calificación de 8 sobre veinte.

5_____20

2_____ X $=\frac{(1)(20)}{5}=$ 8

L2TP trabaja con los mismos que PPTP ya que si quisiera trabajar con otros algoritmos de cifrado más seguros tendrían q trabajar conjuntamente con IPESEC.

5_____20

2_____ X $=\frac{(2)(20)}{5}=$ 8

[1] En el Anexo1, sección de Control de Acceso encontramos los Métodos de Autenticación de PPTP, L2TP e IPSEC

IPSEC Trabaja con cualquiera de los siguientes algoritmos de encriptación: des, 3des, aes128, aes256, aes192 y GRE.

5_____20

4_____ X $=\frac{(4)(20)}{5}=16$

Popularidad

Los resultados para la popularidad se obtuvieron de la encuesta realizada a conocedores de Redes VPN[2].

Para PPTP

Por tener una acogida mayor a los otros protocolos tiene una calificación de 20 puntos.

Para L2TP

Se procede hacer una regla de tres para saber el resultado.

17_____20

15_____ X $=\frac{(15)(20)}{17}=17{,}64$

Para IPSEC

[2] En el Anexo2, entramos la encuesta realizada y sus resultados obtenidos

Se procede hacer una regla de tres para saber el resultado.

17_____20

13_____ X $= \frac{(13)(20)}{17} = 15{,}29$

Vulnerabilidad

Se determinado que PPTP es un protocolo altamente vulnerable y que incluso existe software de dominio popular para romper la seguridad que este protocolo ofrece. L2TP es un protocolo que por sí solo no ofrece la seguridad necesaria por lo que tiene que aliarse con IPSEC y a pesar de esto se encuentran vulnerabilidades cuando este utiliza claves predeterminadas por lo que se recomienda utilizar autoridades certificadoras y finalmente IPSEC ofrece soluciones a sus vulnerabilidades.[3]

4.4.1.4. Seleccionar la tecnología que tenga la máxima ponderación.

[3] En el Anexo1 sección Control de Acceso encontramos Vulnerabilidades de PPTP, L2TP E IPSEC

TABLAIV.IV: Ponderación de las Tecnologías de Acceso Remoto

TEC. A COMPARAR / FACTOR		PPTP		L2TP		IPSEC	
	Peso 0-1	**Calificación**	**Ponderación**	**Calificación**	**Ponderación**	**Calificación**	**Ponderación**
Escenarios VPN	0,09	20	1,8	20	1,8	20	1,8
Algoritmos de autenticación	0,07	6,67	0,4669	13,3	1,4	20	1,4
Algoritmos de cifrado	0,2	8	1,6	8	0,8	16	4
Costo de Implementación	0,15	20	1,2	16	2,4	6	3
Costo de Mantenimiento	0,15	0	0	0	0	20	3
Método de Autenticación	0,15	12	1,8	14	2,1	17	2,55
Popularidad	0,05	20	1	17,64	0,882	15,29	0,7645
Vulnerabilidad	0,14	8	1,12	12	1,68	17	2,38
TOTAL			**10,79**		**11,06**		**16**

El puntaje final de los protocolos comparados sobre una escala de veinte puntos son los siguientes:

10,79 para PPTP, 11,06 para L2TP y 16 para IPSEC por lo que la tecnología más adecuada para el diseño e implementación de una red VPN es la Tecnología IPSEC por poseer mejores características que PPTP YL2TP.

CAPITULO V

IMPLEMENTACION DE LA RED VPN EN LA CORTE SUPERIOR DE JUSTICIA DE CHIMBORAZO

En este capítulo se hace énfasis en la implementación de la Red Privada Virtual en la Corte Superior de Justicia de Chimborazo que permitirá la comunicación de la misma con la Judicatura de Alausí.

Asimismo se presenta paso a paso la configuración de los equipos de Riobamba y Alausí detallando respectivamente su funcionamiento de igual manera las pruebas de interconexión realizadas una vez implementada la Red Privada Virtual.

5.1. PLAN INCIAL

5.1.1. DATOS GENERALES

Nombre del Proyecto: Implementación una Red Privada Virtual en la Corte Superior de Justicia de Chimborazo.

Sector solicitante: Corte Superior de Justicia

Responsables del Proyecto:

Director Provincial de Chimborazo del Consejo de la Judicatura:

Dr. Luis Miranda Astudillo

Informáticos:

Ing. Catalina García, Ing. Cristina Palmay y Egda. Mayra Martínez

Usuarios: Todo el personal de las judicaturas.

5.1.2. ASPECTOS GENERALES:

Nombre de la Empresa: Corte Superior de Justicia

Ubicación: Riobamba, Calles Pichincha y Primera Constituyente

Misión de la Empresa:

Administrar justicia en el ámbito de sus competencias, de manera independiente, imparcial, responsable, diligente y proba, respetando estrictamente los principios generales del derecho, las normas constitucionales, internacionales y legales del ordenamiento jurídico ecuatoriano, con el fin de garantizar, a través de criterios jurisprudenciales uniformes, motivados y congruentes, el ejercicio de la justicia, la seguridad jurídica y la igualdad ante la Ley.

Organigrama estructural:

A fin de dar cumplimiento a lo que dispone el artículo 7 literal a) de la Ley Orgánica de Transparencia y Acceso a la Información Pública, Registro Oficial No. 24, de 18 de mayo del 2004, la Corte Nacional de Justicia publica su Estructura Orgánica Funcional, actualizada , según la Figura V.I.

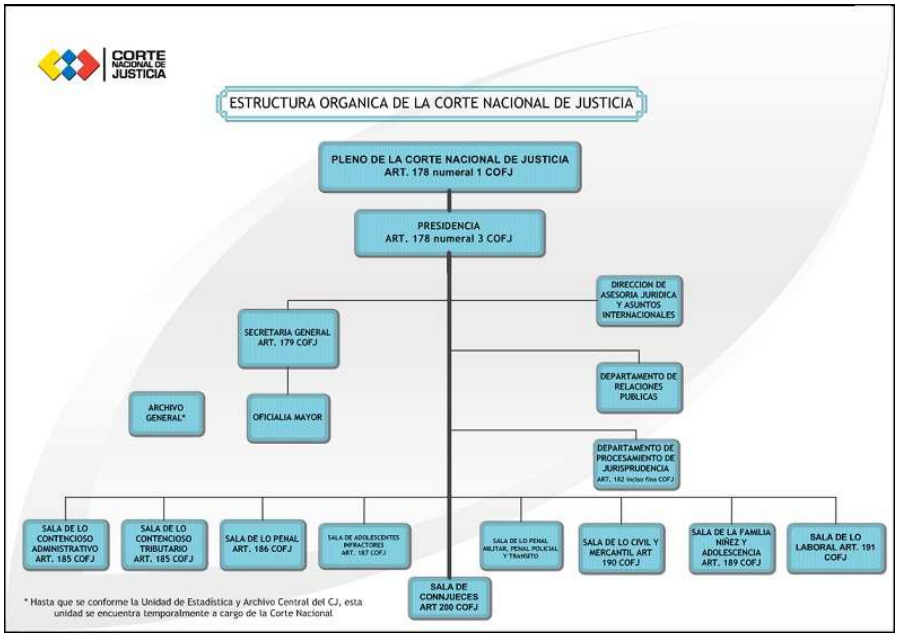


Figura V.1: Estructura orgánica de la Corte Nacional de Justicia.

Sistema de Red:

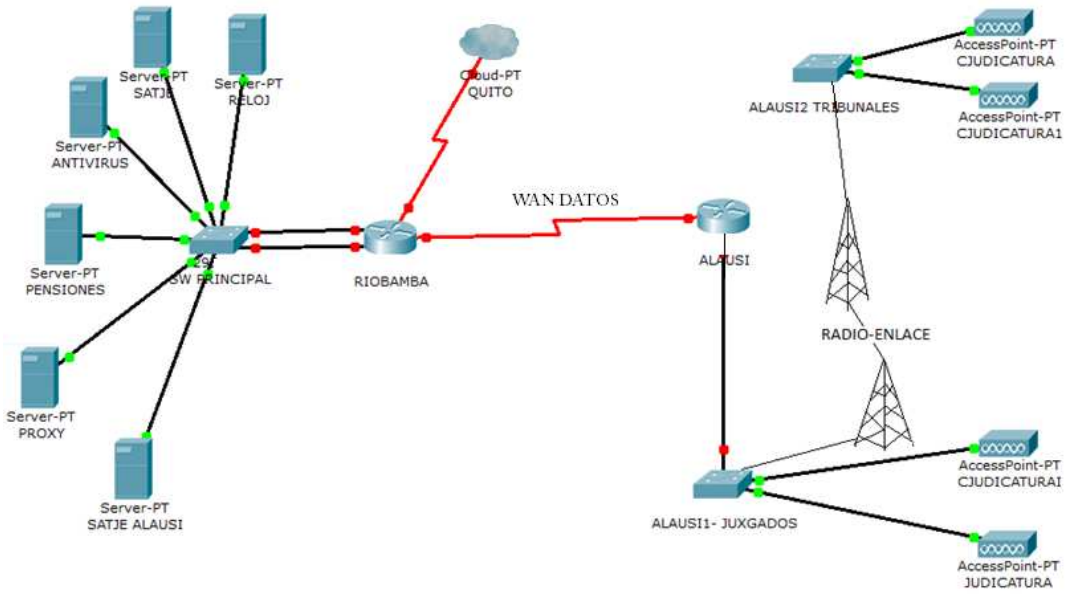


Figura V.2: Red de la CSJ de Chimborazo.

La figura V.1 muestra la comunicación que tiene la Judicatura de Riobamba con la ciudad de Alausí y Quito, a continuación la Tabla V.I explica detalladamente la función de los servidores y enlace de la ciudad de Riobamba y Alausí.

TABLA V.I: Función de servidores Riobamba y Alausí

CIUDAD	SERVIDORES	FUNCIÓN
RIOBAMBA	Reloj	Control de ingreso del personal
	SATJE	Sistema de trámite judicial Ecuatoriano
	Antivirus	Evitar los virus
	Pensiones	Emitir pago de pensiones al banco de Guayaquil
	Proxy	Genera el proxy a la red
	SATJE Alausí	Servidor del Sistema de trámite judicial para Alausí
	WAN	Enlace de Riobamba con los cantones
ALAUSÍ	WAN	Enlace de Alausí con Riobamba

Sistema a mejorar

Con el presente proyecto se pretende mejorar la seguridad en el transporte de la información del Sistema de Trámite Judicial Ecuatoriano hacia los cantones a través de la red WAN con esto se beneficiara a los usuarios que manejan este sistema tanto de Riobamba como de los cantones en los que se implemente.

Fuentes de información

- **Fuentes Internas**

  Centro de cómputo de la CSJ

  Documentos informativos de la Corte Superior de Justicia

- **Fuentes Externas**

  CNT

  Libros, Internet

5.2. INICIO DEL PROYECTO

5.2.1. Definición de los problemas de la red actual y Oportunidades de mejoría

La definición de los problemas y las oportunidades de mejoría de la red actual se los analizaran a través de la estructura PIECES.

5.2.1.1. Estructura PIECES

Creada por James Wetherbe permite realizar una clasificación de la necesidad de mejorar algunos ámbitos los cuales se explican en la Tabla V.II.

TABLA V.II: Estructura PIECES

ESTRUCTURA	PROBLEMAS	OPORTUNIDADES
Prestaciones	El trabajo realizado por los usuarios de la red no satisface su desempeño diario	Mejorar la productividad y tiempo de respuesta de la WAN.
Información	Caídas del sistema, infiltraciones a la red.	Ingreso, salida y almacenamiento de la información
Economía	Costo de conectividad	Mejorar la productividad de la red sin costos adicionales
Control y Seguridad	Baja seguridad de la red.	Mejorar la seguridad de la WAN
Eficacia	Observar la conducta de los empleados	Cumplir con las tareas con el mínimo de recursos
Servicio	Retraso en la atención al cliente por las caídas de la red.	Optimizar el servicio al cliente

5.3. FACTIBILIDAD

5.3.1. Factibilidad Técnica

5.3.1.1. Hardware

Hardware Existente

TABLA V.III: Hardware existente.

Cantidad	Descripción	Estado
1	Switch CORE Catalyst 4503 Series Multi Layer 2/3 6	Muy bueno
1	Router CISCO 1900	Muy bueno
1	Router CISCO 887	Muy Bueno

En la tabla V.III describe un switch 4505 que es el principal donde se conectan los servidores y demás usuarios, un router CISCO 1900 ubicado en la ciudad de Riobamba que permite el enlace WAN con los cantones de Chimborazo y un router cisco 887 ubicado en la ciudad de Alausí permite el enlace WAN de Riobamba con esta ciudad.

Hardware Requerido

La siguiente tabla muestra el hardware que se necesita para la implementación de la Red Privada Virtual.[4]

[4] El anexo3 presenta la documentación de gestión para la utilización de los equipos de CNT.

TABLA V.IV: Hardware requerido

Cantidad	Descripción	Observaciones
1	Router Cisco	Se requiere que el router de la ciudad de Riobamba sea cambiado con otro que a mas de soportar la configuración actual también tenga soporte VPN

5.3.1.2. Software

Software Existente

Se considera el IOS de los router como software ya que sin un IOS adecuado no sería posible la implementación de este proyecto. La tabla V.V explica la situación actual de los equipos.

TABLA V.V: Software existente

Nombre	Descripción	Estado
IOS	No existe la autorización debida para la configuración de los routers de Riobamba y Alausí Y El IOS del Router de Riobamba no tiene la licencia para configurar VPN	No legal

Software Requerido

- Hacer un requerimiento a la Corporación Nacional de Telecomunicaciones para el cambio del router de la ciudad de Riobamba con un router que soporte VPN.
- Solicitar los respectivos permisos para el acceso y configuración de los routers de CNT.

5.3.1.3. Personal Técnico

Personal Técnico Existente

Es el personal encargado en la administración y manipulación directa de la red y se los menciona en la siguiente tabla.

TABLA V.VI: Personal técnico existente

Nombre	**Función**
Ing. Catalina García	Analista 1
Ing. Cristina Palmay	Analista 2

Personal Técnico Requerido

La tabla V.VII muestra el personal necesario para que el presente proyecto pueda ser factible.

TABLA V.VII: Personal técnico requerido

Función	**Formación académica**	**Experiencia en:**
Pasante	Egresada de Ingeniería Electrónica	Implementación de redes

5.4. MIEMBROS DEL PROYECTO

Usuarios

Son todos los usuarios directos o indirectos para quienes se optimiza la red.

Analistas

Jefe del Proyecto: Ing. Catalina García.

Diseñadores y Programadores

Ing. Cristina Palmay y Egda. Mayra Martínez

Operadores

Responsables del Centro de Cómputo:

Ing. Cristina Palmay y Ing. Catalina García.

5.5. BENEFICIOS

5.5.1. Beneficios Tangibles

Dentro de los beneficios tangibles que se pretenden con este proyecto son: mejorar la productividad mejorar la productividad del Sistema de Trámite Judicial en el cantón Alausí, proteger la WAN de usuarios no autorizados autenticando usuarios y cifrando la información que por viaja a través de ésta.

Evitar en lo posible las caídas de la red.

5.5.2. Beneficios Intangibles

Entre estos beneficios se pretende que los clientes estén satisfechos la atención brindada, mejorar el servicio a la comunidad y consecuentemente la imagen de la empresa.

Además mejorar el ánimo de los empleados de la empresa al igual que su ambiente de trabajo.

5.6. IMPLEMENTACION DEL PROYECTO

5.6.1. CONFIGURACIÓN DEL ROUTER DE RIOBAMBA

Cabe destacar una vez más que se pretende una comunicación centralizada donde los cantones puedan comunicarse únicamente la Corte Superior de Justicia de Chimborazo ubicada en la ciudad de Riobamba.

Antes de empezar con la configuración hacemos una representación gráfica de las subredes que se desean proteger con la VPN

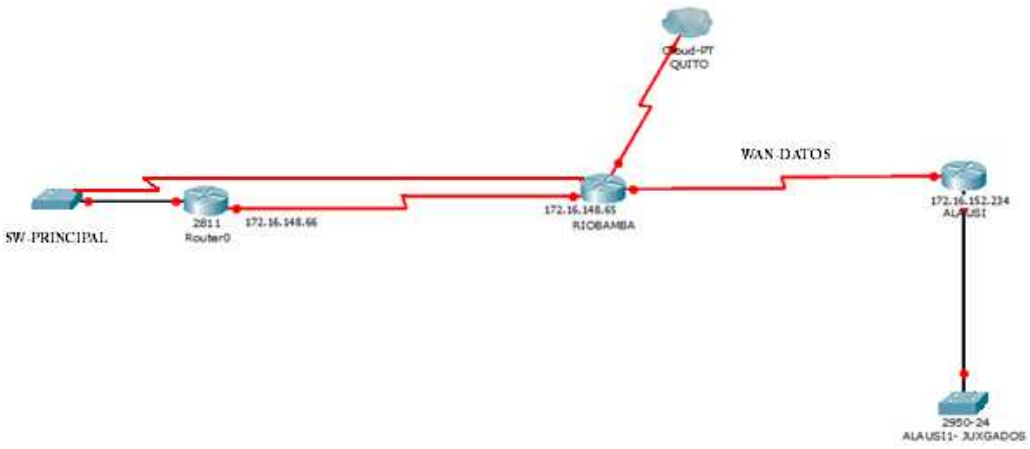


Figura V.3: Enlace WAN de la Corte Superior de Justicia de Chimborazo.

La Figura V.2 muestra las subredes que viajarán a través del túnel VPN. Dichas subredes: son la subred 172.16.148.0/24 que pertenece a los usuarios de sistemas y de gestión y la 172.16.152.0/24 perteneciente a los Juzgados del Cantón Alausí.

Una vez seleccionado el direccionamiento que viajará por la VPN se procede a la configuración del router de Riobamba empleando IPSEC con llaves pre-compartidas.

Paso 1.- Preparar IKE e IPSEC

a) Determinar la política IKE.- Política IKE fase 1

Figura V.4: Despliegue de políticas IKE

Como se puede apreciar en figura V.3 para esta primera fase se despliega el algoritmo de cifrado DES de 56 bits, algoritmo Hash MD5 (HMAC). Como ya menciono en un principio el método de autenticación es pre compartido por lo que se utiliza Pre-Shared. El intercambio de llaves pre compartidas será a través del Grupo 1 de 768 bit de Deffie-Hellman con un tiempo de vida IKE SA de 86400 segundos.

b) Determinar la política IPSEC.- Transformada IKE fase 2

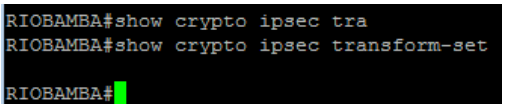


Figura V.5: Transformada IKE fase 2

En la figura VI.3 se despliega la transformada para verificar que no haya otras transformadas configuradas y en el caso de haberlas evitar nombrarlas igual.

c) Verificar la configuración actual

La configuración actual debe ser revisada para verificar que si existen políticas IPSEC configuradas y que puedan interferir con las políticas que se planean configurar. Ver la Figura V.3 y Figura V.4

d) Asegurarse que la red funcione sin cifrado

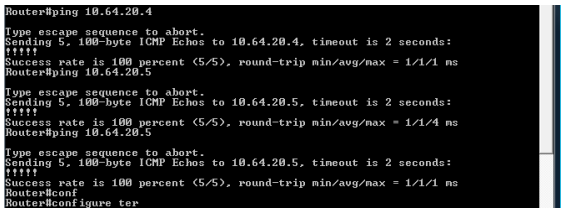


Figura V.6: Conectividad de las subredes.

La Figura VI.5 presenta la conectividad de las subredes del Centro de Cómputo de Riobamba con el cantón Alausí y el enlace WAN.

Paso 2.- Configurar IKE

a) Habilitar o deshabilitar IKE

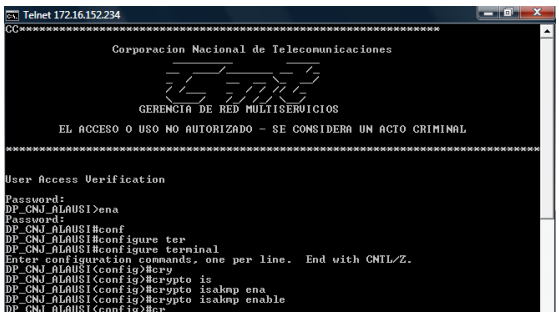


Figura V.7: IKE habilitado

La figura VI.6 habilita IKE de manera global. Cabe mencionar que IKE está habilitado por default y se habilita globalmente en todas las interfaces del router. Una ACL puede bloquear una IKE en una interfaz particular.

b) Crear la política IKE

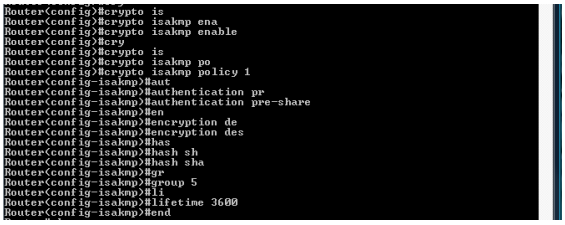


Figura V.8: Política IKE

En la Figura V.7 se define la política IKE la cual es un conjunto de parámetros usados durante la negociación IKE fase 1. Las políticas se ejecutan en orden ascendente.

c) Configuración de la identidad ISAKMP

Los peers IPSEC se autentican mutuamente durante la negociación ISAKMP. Esta identidad puede ser la IP o el nombre del host

d) Configuración de llave pre compartida

Figura V.9: Claves pre-compartidas

En la Figura V.8 se configura la clave "mi_clave" para la autenticación pre-compartida y se lo dirige hacia el extremo del enlace WAN de Alausí

10.64.20.6, cabe mencionar que el direccionamiento IP del extremo de Riobamba es 172.16.148.66

e) Verificar la configuración IKE

Paso 3.- Configurar IPSEC

a) Configuración de la transformada

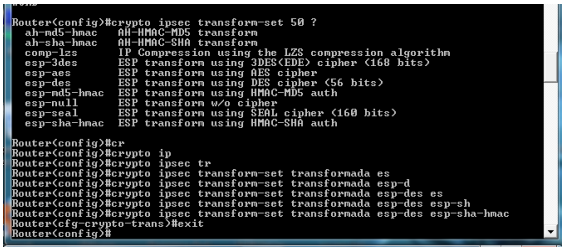


Figura V.10: Transformada.

La Figura V.9 muestra la configuración de la transformada con el nombre "transformada", se escogió la transformada ESP ya que es un mecanismo para el cifrado de la carga y trabaja en modo Tunnel. La transformada es negociada durante el QUICK MODE en la fase 2 de IKE. Se pueden configurar múltiples transformadas y después asignarla por medio de un cryto map. Durante la negociación los peers buscan un conjunto de transformadas que sean idénticas en ambos peers.

b) Configuración global del tiempo de vida de la Asociacion Segura (SA) de IPSEC

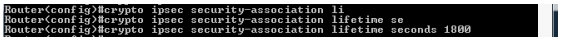


Figura V.11: Tiempo de vida de SA

La figura V.10 determina cuanto tiempo tiene una SA de IPSEC permanecerá válida entes de ser renegociada en este caso se asigna un valor de 1800. El tiempo de vida de la SA es negociado durante la fase 2 de IKE, los tiempos de vida en las SA de IPSEC en los crypto maps sobre escriben los tiempos de vida globales de las SA de IPSEC. Cuando una SA expira una nueva es negociada sin interrumpir el flujo de datos.

c) Crear una crypto ACL

Figura V.12: Lista de Acceso

En la Figura V.11 se crea la crypto ACL que identifica el flujo del tráfico que va a ser protegido. El tráfico que coincide con la ACL es protegido y cifrado y el que no en texto claro. Las ACLs deben ser simétricas cuando se usan con IPSEC. En esta ACL la red de origen es la subred del centro de computo 172.16.148.0/24 y su destino la red 172.16.152.0/24 de Alausí por lo que su simétrica será una ACL de origen 172.16.152.0 /24 y destino 172.16.148.0/24.

d) Crear crypto mapas

Figura V.13: Crypto map

En la figura V.12 se crea un crypto map al cual se lo nombró “mimapa”.

Los crypto mapas agrupan todas las partes de la configuración IPSEC como lo muestra la Figura VI.13.

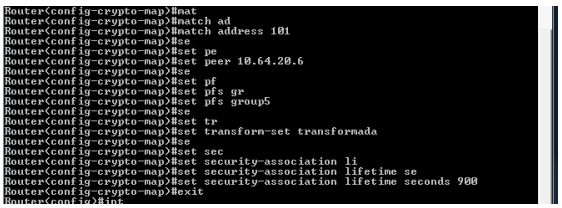


Figura V.14: Agrupamiento de IPSEC en un crypto map

- La ACL empleada

- El peer VPN remoto

- La transformada a utilizarse

- El método de administración de llaves

- El tiempo de vida de las SA.

Los crypto maps pueden aplicarse a una sola interfaz, múltiples interfaces pueden compartir el mismo crypto map si se desea aplicar la misma política a múltiples interfaces.

e) Aplicar el crypto map a la interfaz designada

Figura V.15: Crypto map en la interfaz.

En la Figura V.14 se le asigna el crypto map creado a la interfaz por la que se quiere transportar el trafico deseado en este caso ésta interfaz Vlan 1 es la que tiene asignada la IP 172.16.148.66.

5.6.2. CONFIGURACIÓN DEL ROUTER DE ALAUSÍ

Para la configuración del Router de Alausí se procede a configurar de manera similar, los únicos cambios que se realizan son el Paso 2 y Paso 3 de la configuración del router de Riobamba y se precisan a continuación:

Paso 2.- Configurar IKE

d) Configuración de llave pre compartida

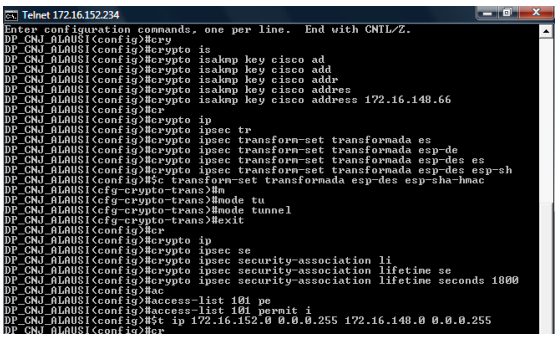


Figura V.16: Claves pre-compartidas Alausí

En la Figura V.15 se configura la clave "cisco" que es la misma en los dos extremos del túnel VPN. Para la autenticación pre-compartida y se lo dirige

hacia el extremo del enlace WAN de Riobamba 172.16.148.66, cabe recordar que el direccionamiento IP del extremo de Alausí es 10.64.20.6.

Paso 3.- Configurar IPSEC

c) Crear una crypto ACL

Figura V.17: Lista de Acceso Alausí

En la Figura V.16 se crea la crypto ACL que identifica el flujo del tráfico que va a ser protegido. Y se lo explica claramente en la Figura VI.10.

e) Aplicar el crypto map a la interfaz designada

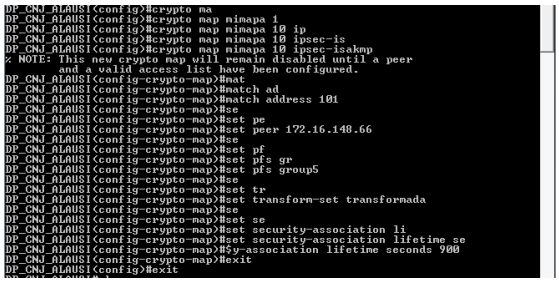


Figura V.18: Creación del mapa

En la Figura V.17 se le asigna el crypto map creado a la interfaz por la que se quiere transportar el trafico deseado en este caso ésta interfaz BVI1 es la que tiene asignada la IP 10.64.20.6.

5.6.3. PRUEBAS Y VERIFICACIÓN DE IPSEC

a) Desplegar las políticas IKE configuradas

b) Desplegar la transformada configurada

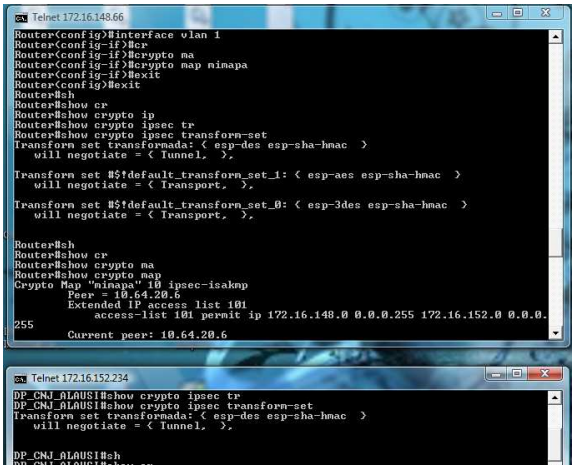


Figura V.19: Transformada

c) Desplegar el estado actual de las SAs

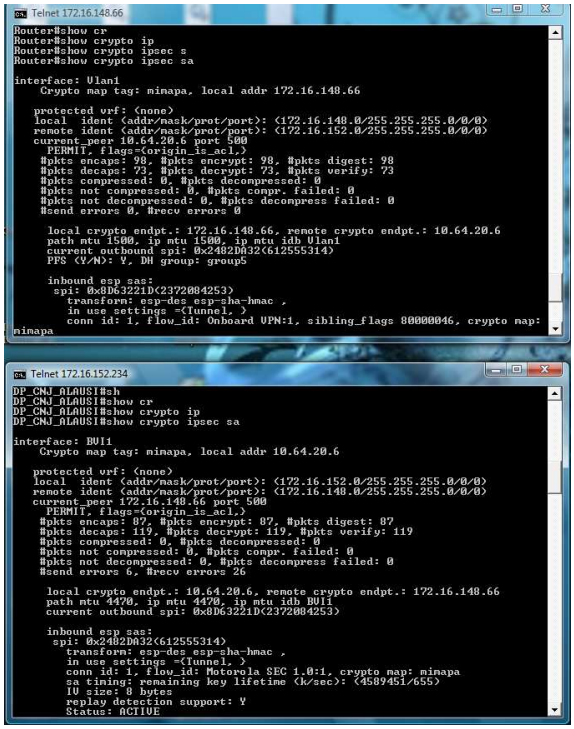
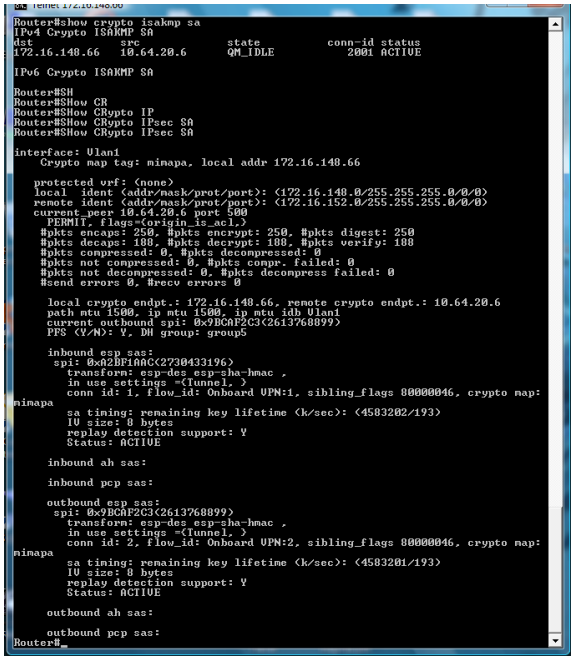


Figura V.20: Despliegue del estado de la SA antes del ping.



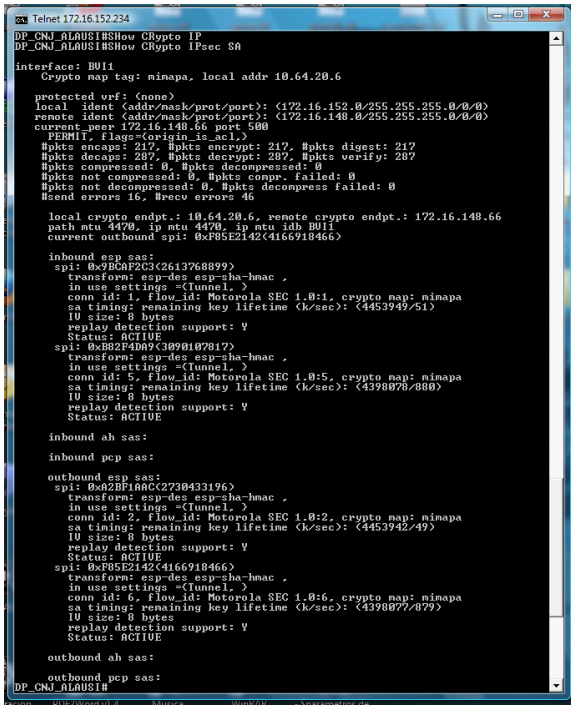
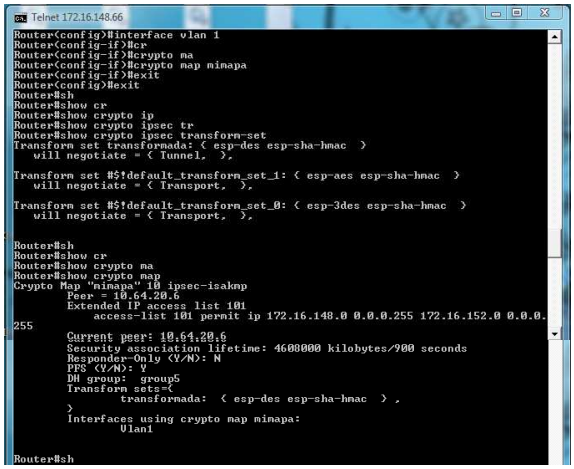


Figura V.21: Despliegue del estado de la SA después del ping.

Como se observa en la Figura 20 y Figura 21 los paquetes encriptados y des encriptados aumentaron después del ping.

d) Desplegar los crypto maps



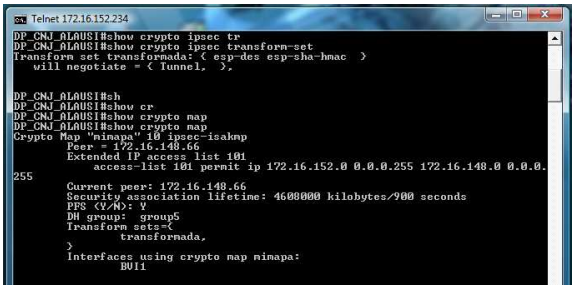


Figura V.22: Despliegue del Mapa

e) Habilitar la salida del DEBUG para los eventos ISAKMP

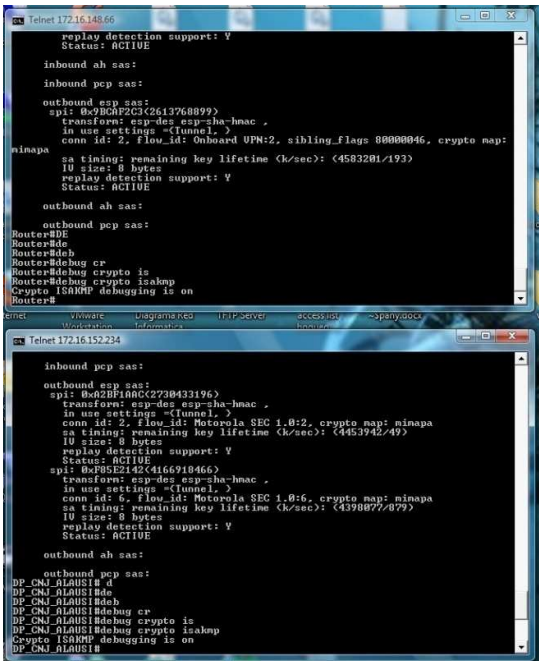


Figura V.23: Salida Debug para ISAKMP

f) Comprobar conectividad

g) Habilitar la salida del DEBUG para los paquetes IP

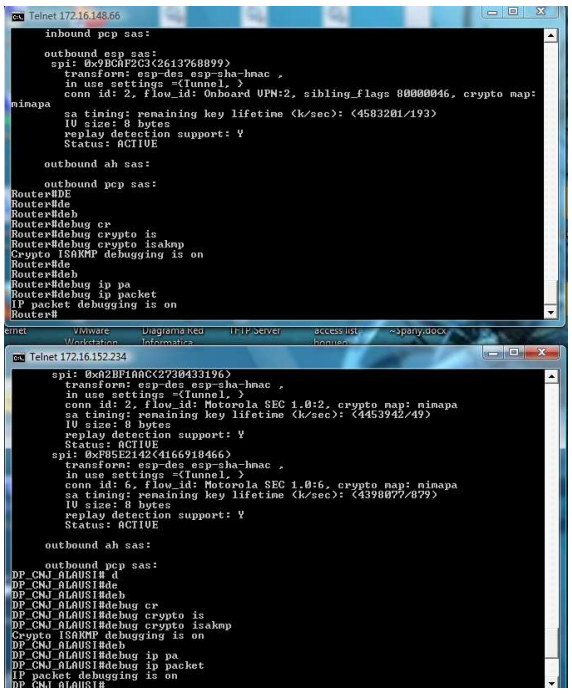


Figura V.24: Salida Debug para IP

CONCLUSIONES

La seguridad de PPTP ha sido completamente rota y las instalaciones con PPTP deberían ser retiradas o actualizadas a otra tecnología de VPN. La utilidad ASLEAP puede obtener claves de sesiones PPTP y descifrar el tráfico de la VPN.

La elección más adecuada para el diseño e implementación de una Red VPN en la Corte Superior de Justicia es IPSEC por poseer mejores características en seguridad, costo e integridad de la información que son necesarias en la empresa.

Tanto los protocolos PPTP y L2TP necesitan combinarse con IPSEC para brindar a los usuarios mayor seguridad en el transporte de la información.

Las VPN reducen coste eliminando la necesidad de largas líneas de coste elevado.

Los requisitos de seguridad sobre las conexiones VPN son cada día mayores, así que para evitar esta debilidad se debe usar autenticación y cifrado para el intercambio de la información.

RECOMENDACIONES

Se recomienda el diseño e implementación de una red VPN utilizando el protocolo IPSEC y así tener confidencialidad, integridad y autenticidad de la información que se transmite a través de los sitios remotos.

Antes de implementar IPSEC se recomienda que la red posea conectividad.

Los routers a utilizar deben tener soporte VPN con sus respectivas licencias habilitadas.

Dado que por lo general VPN es un servicio contratado se recomienda solicitar los respectivos permisos para su implementación así como se lo hizo en la Corte Superior de Justicia solicitándolo a la Corporación Nacional de Telecomunicaciones.

RESUMEN

Se realizó un estudio comparativo entre las tecnologías VPN de interconexión de sitios remotos para el diseño e implementación de la opción más adecuada en la Corte superior de Justicia de Chimborazo con la ciudad de Alausí y de esta manera resolver el problema de seguridad.

La comparación y elección de la mejor opción, se realizó en base a técnicas para la recolección de información son la lectura y observación científica.

Las tecnologías VPN: PPTP, L2TP e IPSEC se las comparó en base a los siguientes factores: Costo de Implementación, Costo de mantenimiento,

Escenarios VPN, Algoritmos de autenticación, Algoritmos de cifrado, Método de autenticación, Popularidad y Vulnerabilidad. Para lo cual se empleó el método de Brown y Gibson, obteniendo los siguientes resultados: 10,79 para PPTP, 11,06 para L2TP y 16,8 para IPSEC por lo que la tecnología más adecuada para el diseño e implementación de una Red Privada Virtual es la Tecnología IPSEC por poseer mejores características que PPTP L2TP se determinó que la mejor tecnología para el diseño e implementación de una red privada virtual es IPSEC por brindar autenticidad, confidencialidad e integridad en la información.

Se implementó una red privada virtual con IPSEC en la Corte Superior de Justicia mejorando el sistema de comunicación en la red, se comprobó la hipótesis planteada. Se recomienda la utilización de algoritmos de cifrado y autenticación para un mejor desempeño de la red.

SUMMARY

A comparative study between the interconnection VPN tecnologies of the remote sites was carried out for the desing and implementation of the most adequate option at the Corte Superior de Justicia de Chimborazo with the Alausí city so as to solve the security problem. The comparison and election of the best option were carried out on the basis of the techniques for the information collection such as reading and scientific observation. The VPN technologies: PPTP, L2TP and IPSEC were compared on the basis of following factors: implementation cost, maintence cost, VPN scenaries, authentication

algorithms, ciphering algorithms, authentication method, popularity and vulnerability. For this the Brown and Gibson method was used with the following results: 10.79 for the PpTP, 11.06 for the L2TP and 16.8 for the IPSEC; the most adecuate technology because it provides authenticity eliability and integrity in the information. A Private Virtual Network with IPSEC was implemented at the Corte Superior de Justicia improving the network communication system; the hypothesis was tested. It is recommended to use the ciphering algorithms and authentication for a better performance of the network.

BIBLIOGRAFIA

1. **ALONSO, J.** 2009. Redes Privadas Virtuales, Madrid RA-MA, pp. 26

2. **PAZ, B. y ROMERO, D. 2006.** Diseño en Implementación de una Red Virtual Privada para la Universidad Técnica Luis Vargas Torres de la ciudad de Esmeraldas (Tesis) Ingeniería en Sistemas. Riobamba Escuela Superior de Politécnica de Chimborazo. Facultad de Informática y Electrónica. Escuela de Ingeniería en Sistemas, pp. 26-27-32

BIBLIOGRAFIA DE INTERNET

3. PROTOCOLO TÚNEL DE CAPA 2

- http://enredajo.blogspot.com/2009/03/que-es-una-vpn-y-tipos-de-vpn.html

  20100920

- http://html.rincondelvago.com/red-vpn.html

  20100814

- http://es.scribd.com/doc/43372246/Guia-para-la-implantacion-de-Windows-2000-Server

  20101215

- http://www.fiuba6662.com.ar/6648/presentaciones/tordillo/Informe-htm-Tordillo/L2TP.htm

  20101215

- http://www.nicatech.com.ni/l.htm

4. PROTOCO TÚNEL PUNTO PUNTO

- www.microsoft.com

  20100512

5. PROTOCOLO SEGURO DE INTERNET

- http://www.rfc-es.org/rfc/rfc2401-es.txt

  20110423

- www.cisco.com

  20100609

6. REDES PRIVADAS VIRTUALES

- http://exa.unne.edu.ar/depar/areas/informatica/SistemasOperativos/tfgerardobrollo.pdf

  20090823

- http://www.univalle.edu.co/~telecomunicaciones/trabajos_de_grado/informes/tg_FernandoArevalo.pdf

20091114

ANEXOS

Anexo 1: DESARROLLO DE LAS VARIBLES PARA LA COMPARATIVA DE LAS TECNOLOGIAS VPN

CONTROL DE ACCESO A LOS RECURSOS

MÉTODO DE AUTENTICACION PPTP

PPTP soporta el método de autenticación del grupo de usuarios locales (Usuario/password)

Resumen del proceso MS-CHAPv2

MS-CHAPv2 proporciona autenticación mutua con la generación de claves de cifrado de datos iniciales más seguros para el Cifrado punto a punto de Microsoft (MPPE) y diferentes claves de cifrado para los datos enviados y los datos recibidos. La autenticación se basa en el método desafío respuesta:

1. El cliente solicita un desafío del servidor.

2. El servidor devuelve un desafío aleatorio de 16 bytes.

3. El cliente genera un número de 16 bytes aleatorio denominado "Peer Authenticator Challenge".

4. El cliente genera una clave de 8 bytes partiendo del desafio recibido previamente del servidor, el generado por el equipo cliente y la cuenta de usuario.

5. La respuesta de 24 bytes, es generada utilizando la funcoón del hash NT de Windows y la clave generada en el paso 4.

6. El servidor utiliza el hash de la contraseña del usuario almacenada en la base de datos para descifrar la respuesta. Si el bloque descifrado coincide con el desafío, el cliente es autenticado.

7. El servidor utiliza la clave de 16 bytes del cliente y el hash de la contraseña para crear una respuesta del autenticador de 20 bytes.

8. El cliente procesa una respuesta del autenticador. Si la respuesta procesada coincide con la respuesta recibida, el servidor es autenticado.

Puesto que PPP no aporta un sistema de cifrado adicional al proceso de negociación de la autenticación, este procedimiento del intercambio de claves puede ser interceptado mediante una ataque MITM para realizar un ataque offline a posteriori. Una contraseña corta y débil podrá ser obtenida con mayor eficacia que una contraseña más larga y compleja. El mejor algoritmo basado exclusivamente en usuario y contraseña es MS-CHAPv2, pero incluso éste es susceptible a un ataque basado en diccionario.

VULNERABILIDADES DE PPTP

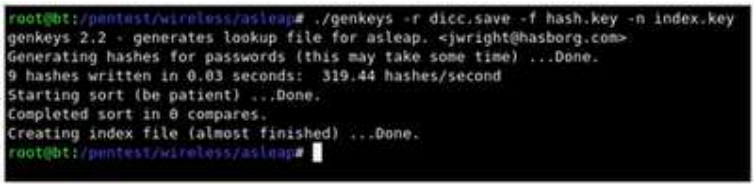
Los sistemas CHAP, PAP, SPAP cuentan, desde hace tiempo, con vulnerabilidades conocidas que permiten su explotación y sólo deben implementarse en entornos "legacy" como solución de compatibilidad y, por supuesto, tomando medidas de protección añadidas.

En el caso de sistemas MS-CHAPv2, Bruce Schneier, Mudge & David Wagner publicaron en 1999 un paper llamado "Cryptanalysis of Microsoft's PPTP Authentication Extensions (MS-CHAPv2) en el que se explican las debilidades de las implementaciones MS-CHAPv1 y MS-CHAPv2. Este trabajo fue

continuado por Jochen Eisinger que publicó en 2010 "Exploiting known security holes in Microsoft's PPTP Authentication Extensions (MS-CHAPv2) en el que se describe el algoritmo que hay que implementar para realizar una ataque con éxito a un proceso de autenticación MS-CHAPv2 mediante una explotación offline. Es decir, una vez grabada la sesión.

Ataque con asleap + ettercap paso a paso

En este sentido la aplicación asleap, creada originalmente para atacar los procesos de autenticación Wifi de Cisco para el protocolo LEAP, fue modificada en 2007 para poder atacar el proceso de autenticación MS-CHAP v2. Para esta demostración se hace uso de esta herramienta, junto con la aplicación Ettercap que será la utilizada para la realización del ataque MITM. En todo este ejemplo se utiliza el LiveCD Backtrack que contiene, desde el año 2008, ambas herramientas. Y se usará Backtrack 4. El ataque es de tipo diccionario, por lo que es necesario crear previamente los ficheros de hashes e índices asociados al diccionario de términos. Este diccionario es, simplemente, un fichero de texto plano que contendrá las palabras a probar. La generación del fichero de índices y hashes se construye con la utilidad genkeys que viene conjuntamente con asleap. La siguiente imagen muestra la generación de los ficheros de hashes e índices.



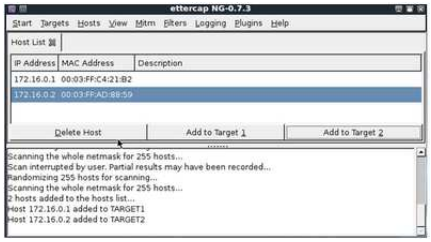
Generación de los ficheros de hash e índice con genkeys

Como se ha comentado previamente, el ataque de MITM se realizará mediante Ettercap. Esta herramienta dispone de un plugin que permite extraer el intercambio de desafío y respuesta de una conexión VPN PPTP. El procedimiento para la realización del ataque de hombre en medio sigue la secuencia habitual:

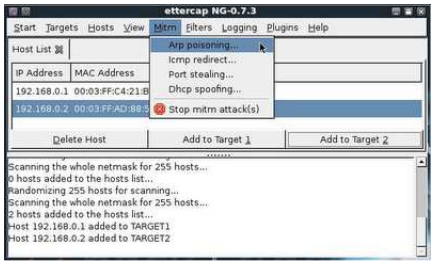
- Habilitar el sniffing.
- Seleccionar los equipos a envenenar.
- Iniciar el envenenamiento.

Las siguientes 4 imágenes muestran estos procesos.

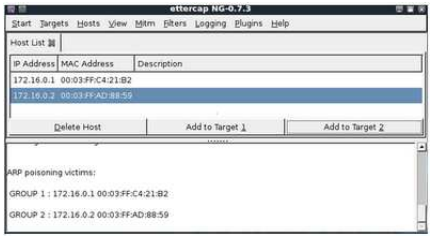
Preparación ataque MITM



Selección de objetivos para el envenenamiento

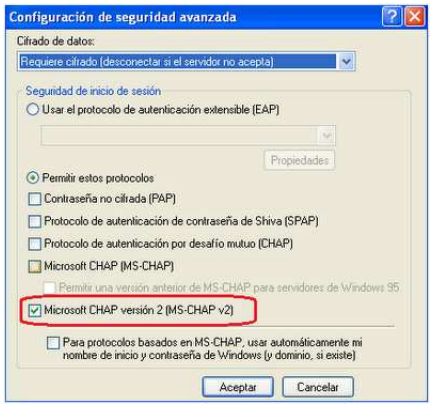


Activación de envenenamiento



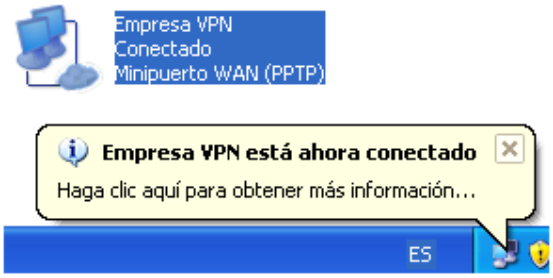
ARP Poisoning en proceso

Antes del inicio de la comunicación, se comprueba que el único mecanismo de autenticación admitido por el cliente es MS-CHAP v2. Sería factible un ataque adicional en la que tanto el cliente como el servidos admitieran MS-CHAP y MS-CHAP v2generando una degradación de la autenticación a MS-CHAP v1, que es más sencillo. En el mismo, aunque la negociación cliente-servidor determinará que la mejor autenticación sería MS-CHAP v2 un atacante en medio podría re-negociar la comunicación entre ambos extremos para degradarlo a MS-CHAP, más vulnerable.



Selección de autenticación MS-CHAP v2

Al mismo tiempo que se produce el proceso de autenticación el atacante está recibiendo los datos del proceso de autenticación.



Conexión PPTP establecida

La información obtenida por Ettercap con los datos correspondientes a la autenticación del usuario administrator, se recogen en la siguiente figura. En ella se ven los datos correspondientes al desafío y la respuesta derivada del hash NT de la contraseña de este usuario. En este caso la password es admin. No es utilizado en esta circunstancia el hash Lan Manager que, como se puede ver, aparece relleno con ceros.

Captura Hashes. Challenge y Response del usuario administrator

Crackeo de la password

Los datos recuperados se pueden utilizar para la realización del ataque de diccionario, con los ficheros creados previamente con Genkeys. Para ello además del fichero de hash y el de índice, se proporcionan los datos de desafío y respuesta tal y como pueden ver en la siguiente figura.

Ataque offline a la autenticación con asleap

Evidentemente la contraseña empleada, admin, es lo suficientemente débil para el ataque sea eficaz en poco tiempo. Otros tipos de contraseñas requerirían un esfuerzo desmesurado para obtenerlas.

SOPORTE PPTP

Una característica importante en el uso del PPTP es que soporta VPN`s sobre public-switched telephone networks (**PSTNs**) que son los comúnmente llamados accesos telefónicos a redes.

PPTP amplía el Protocolo punto a punto (PPP)

PPTP utiliza también una forma de General Routing Encapsulation (GRE) para obtener datos desde y hacia su destino final.

PPTP permite que un único túnel soporte una conexión.

DOCUMENTACION:

Entre la principal documentación que se encontró para el estudio copamrativo se tiene:

Internet:

- **http://support.microsoft.com/kb/550769/es**
- **http://foro.hackhispano.com/showthread.php?t=36238**
- **http://www.pablin.com.ar/computer/info/varios/pptnvpn.htm**

CONTROL DE ACCESO PARA L2TP

METODO DE AUTENTICACION

El estándar de IETF L2TP también ofrece autenticación de túnel, en los modos de obligatorios y voluntarios. Sin embargo, L2TP por sí misma no proporciona

la integridad del mensaje o la confidencialidad. Para ello, debe combinarse con IPSec.

Autoridades Certificadoras

No es necesario mantener un conjunto de contraseñas para las entidades que deben autenticarse por medio de certificados. Para las conexiones L2TP/IPSec, la entidad que se autentica mediante el certificado es un equipo. Las contraseñas se deben seguir manteniendo para la autenticación de usuarios de las conexiones L2TP/IPSec.

Las CA solamente emiten certificados a las entidades de confianza. Por ejemplo, si utiliza los servicios Certificate Server de Windows 2000 e intenta obtener un certificado a través de una inscripción en el Web, deberá contar con un conjunto válido de credenciales de dominio de Windows 2000.

Dado que cada certificado está firmado por su emisor, los certificados nuevos son difíciles de crear y los certificados existentes difíciles de duplicar (sin obtener una copia). Estas medidas impiden que un usuario no autorizado se haga pasar por el titular de un certificado.

La desventaja de utilizar certificados para la autenticación es que es necesario implementar un PKI para poder emitir los certificados a los usuarios.

Cuando se solucionan problemas relacionados con intentos de conexión incorrectos, es preciso en primer lugar determinar si el error está provocado por la autenticación IPSec o la autenticación L2TP basada en PPP para lo cual hay que activar el registro Isakmp.log y el registro PPP y volver a intentar la

conexión. Si no se incluye información nueva en el registro PPP, puede que la autenticación IPSec haya sido incorrecta. Consulte el contenido del archivo Isakmp.log para determinar las causas del problema.

Las claves compartidas previamente

Las claves compartidas previamente es que no requiere una infraestructura PKI, que es necesaria para utilizar certificados para la autenticación L2TP/IPSec. Las claves compartidas previamente son muy fáciles de configurar en un cliente de acceso remoto. Un equipo que ejecute Windows 2000 Server sólo puede configurar una clave compartida previamente para todas las conexiones L2TP/IPSec que necesitan una clave compartida previamente para la autenticación.

La clave compartida previamente puede escribirse o pegarse en la utilidad Microsoft IPSec VPN Configuration. Si se escribe, existe la posibilidad de que el usuario cometa un error de configuración.

Si se cambia la clave compartida previamente de un servidor VPN, un cliente que utilice una clave compartida previamente no podrá conectarse a ese servidor hasta que cambie la clave compartida previamente en el cliente.

VULNERABILIDADES DE L2TP/IPSEC

Una clave compartida previamente es una secuencia de caracteres cuya confidencialidad depende del método de distribución y de su solidez. Si la seguridad de la clave compartida previamente puede vulnerarse, cualquier

intruso podría autenticar la parte IPSec de la conexión, aunque seguiría necesitando un conjunto de credenciales válido para la parte PPP de la conexión. En cambio, es muy difícil poner en peligro la integridad de un certificado.

A diferencia de los certificados, el origen, el historial y la duración de una clave compartida previamente no puede determinarse.

Por estos motivos, el uso de una clave compartida previamente para autenticar conexiones L2TP/IPSec se considera un mecanismo de autenticación insuficiente. Si desea utilizar un método de autenticación sólido y duradero, se recomienda utilizar PKI y certificados.

DOCUMENTACION:

Entre la principal documentación que se encontró para el estudio copamrativo se tiene:

Internet:

http://support.microsoft.com/kb/314831/es

www.ietf.org/rfc2661.txt&rurl

CONTROL DE ACCESO PARA IPSEC

METODOS DE AUTENTICACION

Llaves pre-compartidas

Las Los peers IPSEC se autentican mutuamente durante la negociación ISAKMP usando la llave precompartida que es un cifrado simetrico y la identidad ISAKMP. Esta identidad puede ser el nombre o el nombre del host. A persar de que cisco IOS usa como método de identidad la dirección IP por defecto

RSA

Se determinan detalladamente las políticas de seguridad para el cifrado asimétrico o público como lo es RSA incluyendo la distribución de llaves

Autoridades certificadoras

Al configurar Autoridades Certificadoras se proporciona mayor seguridad a la VPN.

Los tipos de certificados almacenados en el router: El router posee su propio certificado de identidad, el certificado raíz de la CA, Certificados RA (vendedor especifico de la CA).

El número de CRLs almacenadas en el router: Uno si la CA no soporta RA, multiples CRLs si la CA soporta RA.

Mediante el siguiente código. **Crypto ca certifícate query,** ya que evita que los certificados se almacenen localmente en el router manejando asi el uso de la memoria NVRAM.

VULNERABILIDADES DE IPSEC

El protocolo de encapsulación segura (ESP) también soporta configuraciones de sólo cifrado y sólo autenticación, pero al utilizar cifrado sin autenticación está altamente es inseguro. Al contrario que con AH, la cabecera del paquete IP no está protegida.

En la mayoría de los casos, NAT aún no es compatible en combinación con IPsec. NAT-Transversal ofrece una solución para este problema encapsulando los paquetes ESP dentro de paquetes UDP.

DOCUMENTACION:

Entre la principal documentación que se encontró para el estudio copamrativo se tiene:

Internet:

- http://technet.microsoft.com/es-es/library/cc757905%28WS.10%29.aspx
- www.6win.com/6WINGate-software.html
- http://www.ccure.org/article-print-979.html

Anexo 2: ENCUESTA

ESCUELA POLITECNICA SUPERIOR DE CHIMBORAZO
FACULTAD DE INFORMATICA Y ELECTRÓNICA

ESCUELA DE INGENIERÍA ELECTRONICA

La siguiente encuesta trata de medir la popularidad de los protocolos que trabajan en entornos de redes privadas virtuales VPN.
Fecha: 20 de Abril del 2011

1. Ha escuchado usted del Protocolo PPTP para la implementación de VPN?

   SI ☐ NO ☐

2. Ha escuchado usted del Protocolo L2TP para la implementación de VPN?

   SI ☐ NO ☐

3. Ha escuchado usted del Protocolo IPSEC para la implementación de VPN?

   SI ☐ NO ☐

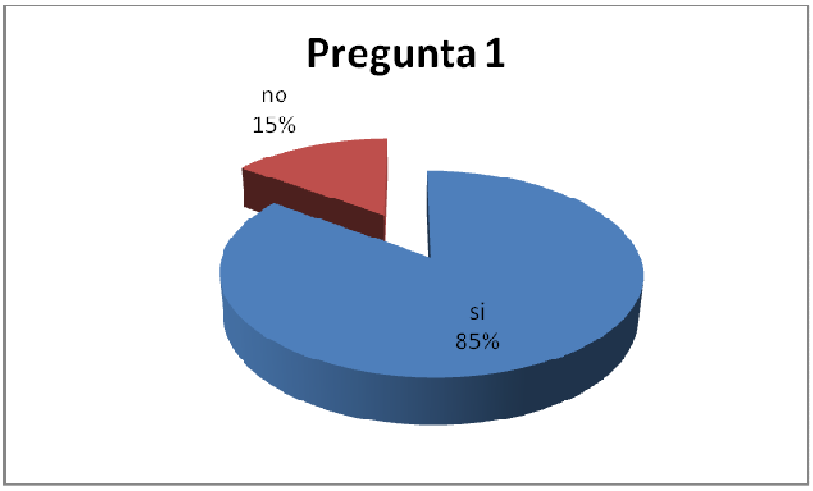
ANÁLISIS DE LOS RESULTADOS:
En la encuesta realizada el 20 de Abril del 2011 realizada a 20 personas con conocimientos en computación, para medir la popularidad de los protocolos

que trabajan en entornos de redes privada virtuales se obtuvieron los siguientes resultados.

En la pregunta 1
Ha escuchado usted del Protocolo PPTP para la implementación de VPN?

SI ☐ NO ☐

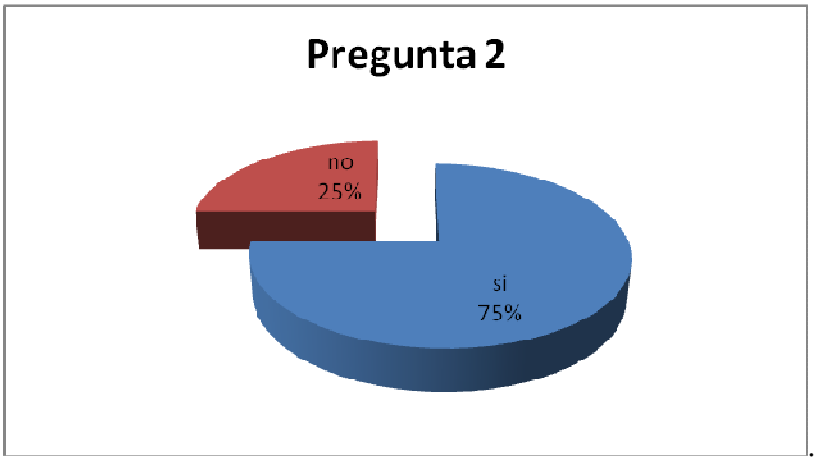
Resultados:
17 personas que pertenecen al 85% dijeron que si han escuchado de PPTP.
3 personas que pertenecen al 15% dijeron que no han escuchado de PPTP.



En la pregunta 2
Ha escuchado usted del Protocolo L2TP para la implementación de VPN?

SI ☐ NO ☐

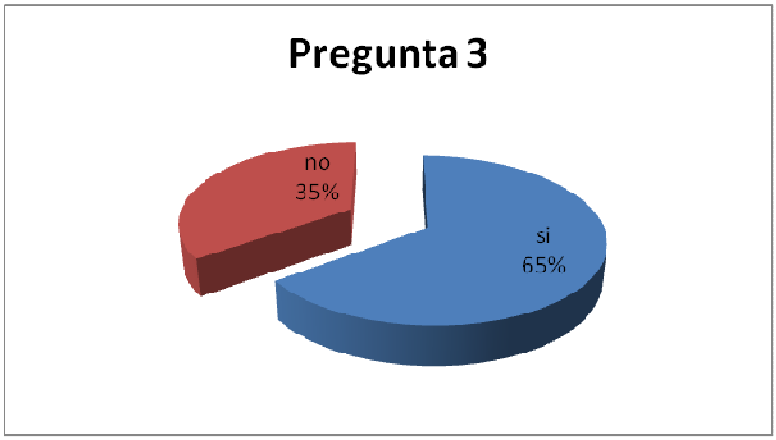
Resultados:
15 personas que pertenecen al 75% dijeron que si han escuchado de L2TP.
5 personas que pertenecen al 25% dijeron que no han escuchado de L2TP



En la pregunta 3
Ha escuchado usted del Protocolo IPSEC para la implementación de VPN?

SI ☐ NO ☐

Resultados:
13 personas que pertenecen al 65% dijeron que si han escuchado de IPSEC.
7 personas que pertenecen al 35% dijeron que no han escuchado de IPSEC



Anexo 3: DOCUMENTACION DE GESTION PARA LA UTILIZACIÓN DE LOS EQUIPOS DE CNT

Anexo 4: CONFIGURACIÓN DE LOS ROUTERS

RIOBAMBA

User Access Verification

Password:
Router>ena
Password:
Router#sh
Router#show runn
Router#show running-config
Building configuration...

Current configuration : 1757 bytes
!
! Last configuration change at 15:35:27 UTC Tue Jul 5 2011
!
version 15.0
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
!
boot-start-marker
boot-end-marker
!
enable secret 5 1FQbF$5voSz9wmp1p7hEvUUIeGL1
!
no aaa new-model
memory-size iomem 10
!
!
ip source-route
!

```
!
!
!
ip cef
no ipv6 cef
!
!
license udi pid CISCO887-K9 sn FTX143601JB
!
!
!
!
!
!
crypto isakmp policy 1
 authentication pre-share
 group 5
 lifetime 3600
crypto isakmp key cisco address 10.64.20.6
!
crypto ipsec security-association lifetime seconds 1800
!
crypto ipsec transform-set transformada esp-des esp-sha-hmac
!
crypto map mimapa 10 ipsec-isakmp
 set peer 10.64.20.6
 set security-association lifetime seconds 900
 set transform-set transformada
 set pfs group5
 match address 101
!
!
!
!
!
interface BRI0
 no ip address
 encapsulation hdlc
 shutdown
 isdn termination multidrop
!
interface ATM0
 no ip address
 shutdown
 no atm ilmi-keepalive
```

```
!
interface FastEthernet0
!
interface FastEthernet1
!
interface FastEthernet2
!
interface FastEthernet3
!
interface Vlan1
 ip address 172.16.148.66 255.255.255.0
 crypto map mimapa
!
interface Vlan2
 no ip address
!
interface Vlan11
 no ip address
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 10.10.10.1
ip route 10.64.20.4 255.255.255.252 172.16.148.65
ip route 172.16.151.0 255.255.255.0 172.16.148.65
ip route 172.16.152.0 255.255.255.0 172.16.148.65
!
access-list 101 permit ip 172.16.148.0 0.0.0.255 172.16.152.0 0.0.0.255
!
!
!
!
!
control-plane
!
!
line con 0
 no modem enable
line aux 0
line vty 0 4
 exec-timeout 5 0
 password cisco
 login
!
```

scheduler max-task-time 5000
end

Router#

ROUTER DE ALAUSÌ

CC**********

Corporacion Nacional de Telecomunicaciones

GERENCIA DE RED MULTISERVICIOS

EL ACCESO O USO NO AUTORIZADO - SE CONSIDERA UN ACTO CRIMINAL

****

User Access Verification

Password:
DP_CNJ_ALAUSI>ena
Password:
DP_CNJ_ALAUSI#sh
DP_CNJ_ALAUSI#show runn
DP_CNJ_ALAUSI#show running-config
Building configuration...

Current configuration : 2325 bytes
!
version 12.4
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname DP_CNJ_ALAUSI
!

```
boot-start-marker
boot-end-marker
!
!
no aaa new-model
!
!
ip cef
!
!
!
!
no ip domain lookup
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
!
multilink bundle-name authenticated
!
!
!
!
crypto isakmp policy 1
 authentication pre-share
 group 5
 lifetime 3600
crypto isakmp key cisco address 172.16.148.66
!
crypto ipsec security-association lifetime seconds 1800
!
crypto ipsec transform-set transformada esp-des esp-sha-hmac
!
crypto map mimapa 10 ipsec-isakmp
 set peer 172.16.148.66
 set security-association lifetime seconds 900
 set transform-set transformada
 set pfs group5
 match address 101
!
archive
 log config
  hidekeys
!
!
!
bridge irb
```

```
!
!
interface ATM0
 no ip address
 no atm ilmi-keepalive
 dsl operating-mode auto
!
interface ATM0.38 point-to-point
 description BRIDGE_IPs
 pvc 0/38
  encapsulation aal5snap
 !
 bridge-group 1
!
interface FastEthernet0
 speed 100
!
interface FastEthernet1
!
interface FastEthernet2
!
interface FastEthernet3
!
interface Vlan1
 description CONEXION_LAN
 ip address 172.16.152.234 255.255.255.0
!
interface BVI1
 description CONEXION_WAN
 ip address 10.64.20.6 255.255.255.252
 crypto map mimapa
!
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 10.64.20.5
!
!
no ip http server
no ip http secure-server
!
access-list 101 permit ip 172.16.152.0 0.0.0.255 172.16.148.0 0.0.0.255
!
!
!
!
control-plane
```

```
!
bridge 1 protocol ieee
bridge 1 route ip
banner motd ^CCC**********************************************************
```