Universidad de San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería en Ciencias y Sistemas

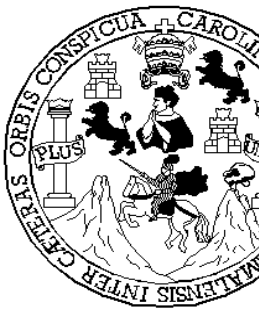
LA IMPORTANCIA DEL USO DE IPSEC EN INTERNET

FLORINDA JAMILETTE BRIZUELA MONTERROSO

Asesorado por Ing. Edgardo Vicente Antonio Cabrera Martínez

Guatemala, octubre de 2004

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA



FACULTAD DE INGENIERÍA

LA IMPORTANCIA DEL USO DE IPSEC EN INTERNET

TRABAJO DE GRADUACIÓN

PRESENTADO A JUNTA DIRECTIVA DE LA
FACULTAD DE INGENIERÍA
POR

FLORINDA JAMILETTE BRIZUELA MONTERROSO

Asesorado por: Ing. Edgardo Vicente Antonio Cabrera Martínez

AL CONFERÍRSELE EL TÍTULO DE

INGENIERO EN CIENCIAS Y SISTEMAS

GUATEMALA, OCTUBRE DE 2004

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

NÓMINA DE JUNTA DIRECTIVA

DECANO	Ing. Sydney Alexander Samuels Milson
VOCAL I	Ing. Murphy Olympo Paiz Recinos
VOCAL II	Lic. Amahán Sánchez Alvarez
VOCAL III	Ing. Julio David Galicia Celada
VOCAL IV	Br. Kenneth Issur Estrada Ruiz
VOCAL V	Br. Elisa Yazminda Vides Leiva
SECRETARIO	Ing. Pedro Antonio Aguilar Polanco

TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO

DECANO	Ing. Sydney Alexander Samuels Milson
EXAMINADOR	Inga. Virginia Victoria Tala Ayerdi
EXAMINADOR	Ing. Franklin Antonio Barrientos Luna
EXAMINADOR	Ing. Jorge Armin Mazariegos Rabanales
SECRETARIA	Ing. Pedro Antonio Aguilar Polanco

HONORABLE TRIBUNAL EXAMINADOR

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

LA IMPORTANCIA DEL USO DE IPSEC EN INTERNET

Tema que me fuera asignado por la Dirección de la Escuela de Ingeniería en Ciencias y Sistemas, con fecha febrero de 2003.

Florinda Jamilette Brizuela Monterroso

ÍNDICE GENERAL

ÍNDICE DE ILUSTRACIONES

FIGURAS

GLOSARIO

Acceso remoto Las compañías buscan mejorar la seguridad de acceso, reducir sus llamadas a larga distancia, para esto se comunican con sus oficinas que están fuera del edificio principal de la compañía utilizando la misma red (intranet) o haciendo uso de internet con la ayuda de dispositivos que permiten tener una comunicación local.

ADSL (*Asymmetric digital subscriber line*, línea asimétrica digital de suscriptor), fue el primer competidor de la industria telefónica por el premio de la distribución local, con la idea que a cada casa donde entra un par trenzado de cobre (para servicio telefónico analógico). También pudieran usarse para vídeo.

Algoritmo Es una secuencia de pasos descrita para realizar una tarea específica utilizando un lenguaje en pseudo-código.

Algoritmo *hash* Es un algoritmo de dispersión.

Análisis de tráfico Es el análisis de la circulación de la información a través de la red con el fin de deducir la información que le es útil al adversario.

Ancho de banda — *Bandwidth*, término técnico que determina el volumen de información que puede circular por un medio físico de comunicación de datos, es decir, la capacidad de una conexión. A mayor ancho de banda, mejor velocidad de acceso, más personas pueden utilizar el mismo medio simultáneamente. Se mide en hertz o bps (bits por segundo).

Arquitectura de red — Es un conjunto de capas y protocolos, ni los detalles de la implementación ni la especificación de las interfaces forman parte de la arquitectura.

Backbone — (Columna vertebral). Conexión de alta velocidad que une computadoras encargadas de hacer circular grandes volúmenes de información. Constituye la estructura fundamental de las redes de comunicación.

BITW — *Bump in the wire*, es una variación en la estructura de las VPN, es la separación de los *router* y los *gateway* de seguridad, en este caso, los *gateway* de seguridad serán utilizados simplemente para el paso del tráfico entre una interfase y otra, y el proceso de IPSec se hará en el camino.

Broadcast	Es un tipo de transmisión de difusión. Ya que hay paquetes que son enviados en la red y para entregar el paquete en el lugar de destino la red pregunta a todos los dispositivos de la red quien es el receptor del paquete, en este caso todos se dan por enterados del paso de información con una sola llamada.
Bundle	Es el nombre que se da al grupo de *security associations* (SAs).
Capa de red	Se encarga de controlar las subredes, y de resolver los problemas de los protocolos, conociendo también el destino de los paquetes que se envían a través de la red.
Certificado	Acreditación emitida por una entidad o un particular debidamente autorizada garantizando que un determinado dato (una firma electrónica o una clave pública) pertenece realmente a quien se supone.
Cifrar	Es encriptar la información.
Compatible	Cuando el software o hardware puede trabajar o entenderse con otro producto, facilitando la migración de datos entre plataformas.
Confidencialidad de datos	Servicio de seguridad que protege los datos para no ser observados.

Configuración Establecer los valores a parámetros y variables, de modo que se permita el adecuado funcionamiento del software o hardware de acuerdo a las características del medio en el que se trabaja.

Control de acceso Este es un mecanismo que controla la red y los recursos de las computadoras de una manera tal que solamente los utilizadores legítimos puedan acceder a ellos dentro de sus límites establecidos.

Cookies Son valores *random* que utiliza Isakmp para identificar las distintas negociaciones que lleva a cabo.

Criptografía Escritura secreta. Útil para diseñar, construir y usar "criptosistemas".

Datagrama Modo de transporte de paquetes donde los paquetes se "enrutan" independientemente y pueden seguir diferentes rutas, por lo cual no hay garantía en la secuencia de entrega.

Default Cuando no se establecen nuevos valores para las configuraciones se asume que seguirán rigiendo los valores que trae de fábrica.

DES *Data encryption standard* , es un algoritmo utilizado para la encripción de datos por ESP, utiliza 56 bits, sin embargo la versión mejorada 3DES (triple DES) utiliza 168 bits.

Dirección IP Cada *host* y "enrutador" de la red tiene una dirección IP, que codifica su número de red y su número de *host*. La combinación es única: no hay dos máquinas que tengan la misma dirección de IP. Todas las direcciones de IP son de 32 bits de longitud y se usan en los campos de dirección de origen y dirección destino de los paquetes IP.

Dispositivo Es cualquier componente de red, *switch*, *host*, computadora, impresora, etc.

Dispositivo *broadband* Este es un dispositivo que utiliza la tecnología *broadband* (difusión).

DNS (*Domain name system*, sistema de nombres de dominio) Se encarga de convertir(resolver) las direcciones electrónicas de internet en la dirección IP correspondiente. Para esto un programa de aplicación llama a un procedimiento de biblioteca llamado "resolvedor" pasándole como parámetro el nombre. El "resolvedor" envía un paquete UDP a un servidor DNS local, que busca el nombre y devuelve la dirección IP al "resolvedor" que entonces lo devuelve al solicitante.

Encapsulación	La “encapsulación” está íntimamente relacionada con la ocultación de la información, definiendo qué partes de un objeto son visibles y qué partes están ocultas.
Encriptar	Método de convertir los caracteres de un texto de modo que no sea posible entenderlo si no se lee con la clave correspondiente.
Enlace *on-demand*	Consiste en un enlace que se establece automáticamente cuando la estación de trabajo del usuario remoto intenta acceder los recursos del sitio central. Así mismo si no hay tráfico sobre el enlace, este se desconecta automáticamente.
Etiquetar	Colocar una marca que permita hacer distinción.
Extranet	Utilización de la tecnología de internet para conectar la red local (LAN) de una organización con otras redes.
Firewall	Es un filtro de seguridad (un conjunto de programas de protección y dispositivos) entre la red interna de una compañía e Internet, y evita que accedan a él intrusos, pero da paso a usuarios de la corporación sin restricciones de acceso.

Firma digital Se logra con un sistema que permita que una parte puede enviar un mensaje "firmado" a otra parte de modo que: el receptor verifique la identidad del transmisor, el transmisor no pueda repudiar después el contenido del mensaje y el receptor no pueda confeccionar él mismo el mensaje.

Flujo de datos *Data flow*. Es el tráfico agrupado, identificado por una combinación de direcciones y máscaras fuentes, direcciones y máscaras destino, puertos fuentes y destinos. Un *data flow* puede representar una sola conexión entre dos servidores TCP, o bien puede representar todo el tráfico entre dos subredes. La protección de IPSec es aplicada a el flujo de datos.

Frame relay Tecnología de transporte de datos por paquetes muy utilizada en las conexiones de líneas dedicadas.

Gateway Dispositivo de comunicación entre dos o más redes locales (LAN) y remotas, usualmente capaz de convertir distintos protocolos, actuando de traductor para permitir la comunicación. Como términos genérico es utilizado para denominar a todo dispositivo capaz de convertir o transformar datos que circulan entre dos medios o tecnologías.

Hacker	Persona que suele dedicarse a violar claves de acceso por pura diversión, o para demostrar fallas en los sistemas de protección de una red de computadoras.
Hardware	Componente físico de la computadora.
IESG	*Internet Engineering Steering Group*, Grupo de dirección de ingeniería de Internet. Grupo voluntario que se encarga de considerar los estándares propuestos por el *Internet Engineering task force* (IETF) que posteriormente serán establecidos por el *Internet architecture board* (IAB).
IETF	(*Engineering task force*, fuerza de trabajo de ingeniería de internet), esta formada por el *Internet architecture board* (IAB), se encarga de los problemas de ingeniería a corto plazo, se dividió en grupos de trabajo, con un problema específico que resolver. Los temas del grupo de trabajo incluyen nuevas aplicaciones, información de usuarios, integración de OSI, "ruteo" y direccionamiento, seguridad, administración de redes, y *standard*.
IKE	*Internet key exchange* Es un protocolo híbrido, es el administración de llaves de IPSec que consiste una serie de pasos que establecen llaves que permiten encriptar o desencriptar información.

Inbound Se refiere al tráfico de información que ingresa a un proceso.

Integridad de datos La característica de asegurarse de que los datos están siendo transmitidos desde el origen a la máquina destino sin alteración desapercibida de los datos.

Interface (Interfaz), La interfaz define cuáles operaciones y servicios primitivos ofrece la capa inferior a la superior (definición para redes). Cara visible de los programas. Interactúa con los usuarios. Abarca las pantallas y su diseño, lenguaje usado, botones, mensajes de error y otros (definición para software).

INTERNET La red de computadoras más extensa del planeta que conecta y comunica a millones de personas. Nació a fines de los años sesenta como ARPANet y se convirtió en un revolucionario medio de comunicación. Su estructura técnica se basa en millones de computadoras que ofrecen todo tipo de información. Estas computadoras, permanecen disponibles las 24 horas, se llaman servidores y están interconectadas entre sí en todo el mundo a través de diferentes mecanismos de líneas dedicadas. Sin importar el tipo de computadora, para intercomunicarse utilizan el protocolo TCP/IP.

Intranet Utilización de la tecnología de internet dentro de la red local (LAN) y/o red de área amplia (WAN) de una organización. Una intranet permite optimizar el acceso a los recursos de una organización. Al extender sus límites más allá de la organización, para permitir la intercomunicación con los sistemas de otras compañías, se le llama extranet.

IPSec *Internet protocol security*, protocolo que trabaja en la capa de red, brinda seguridad al tráfico de datos entre las redes de comunicación de computadoras, cuenta con la autenticación de los datos para que no puedan ser modificados por terceras personas y encripta el contenido de los paquetes para ocultarlos.

ISAKMP *Internet security association and key management protocol*, maneja los cambios de llaves criptográficas, emplea un proceso de dos fases para establecer los parámetros IPSec entre dos nodos IPSec, se encarga de establecer el protocolo más conveniente entre dos *switch*, está diseñado para proteger contra sabotajes en el servicio.

ISAKMPD *Isakmp daemon*, establece SA para encriptar y/o autenticar tráfico en la red.

ISDN *Integrated services data network*, (red digital de servicios integrados), Tecnología rápida de conexión para líneas dedicadas y transmisión de datos. Se utiliza para tener acceso a internet o a una videoconferencia.

ISP *Internet service provider*, (proveedor de servicios de internet). Empresas que ofrecen acceso a los recursos de internet para usuarios a remoto y para servidores de empresas.

L2F *Layer two forwarding*, Es un protocolo de túnel creado por CISCO SYSTEM, es similar a PPTP de Microsoft. L2F habilita la organización para configurar VPN que usan el Internet *backbone* para mover paquetes. Microsoft y Cisco unieron las perspectivas de ambos para un solo y *standard* protocolo llamado L2TP.

L2TP *Layer two tunnel protocol*, es un protocolo *standard* del IETF para la capa 2 con el fin de permitir a los usuarios remotos tener acceso a redes corporativas de forma segura. No proporciona encripción sino que necesita de un servicio que lo brinde.

LAC *L2TP Access Concentrator*. Es uno de los dos componentes de L2TP, siendo este un dispositivo que físicamente termina una llamada.

LDAP *Lightweight directory access protocol*, es un *standard* abierto para los servicios globales o locales en una red y/o en Internet. Actualmente se utiliza principalmente para asociar nombres a números de teléfono y a direcciones e-mail.

Línea dedicada *Leased line*, forma de conexión a internet (con acceso las 24 horas), a través de un cable hasta un proveedor de internet. Esta conexión puede ser utilizada por varias personas en forma simultanea.

LLAVE *Key*, son palabras o frases públicas y privadas que permiten la encripción y desencripción de la información.

LNS *L2TP Network Server*, que es el dispositivo que autentica y termina el enlace PPP (*Point-to-Point Protocol*).

MD5 *Message digest 5*, es un algoritmo de dispersión que asegura que no sería posible computacional-mente producir otro mensaje con la misma dispersión MD5.

MLPPP *Multilink point to point protocol*, protocolo de "multienlaces" punto a punto. La conexión a internet puede ser a 64 kbps (PPP), y a 128 kbps (MPPP) usando simultáneamente más de un canal, según el RFC 1990. En este tipo de acceso el sistema es capaz de combinar múltiples enlaces físicos dentro de un único enlace lógico.

Multicast Es un tipo de transmisión, puede ser punto a multipunto o multipunto a multipunto.

NAT *Network address traslation*. Se refiere al mecanismo de traducción para todos los puertos, en general de salida. Es una opción que tienen algunos *routers* para hacer traducción de direcciones entre una red y la otra. Hace que a los paquetes de información que viajan de una red a la otra se les cambie el "remitente" para que parezca que proceden originalmente del *router*, y a sus respuestas se les cambia el "destinatario" para que sea el remitente original a la vuelta. Sirve principalmente para actuar como *firewall* y aumentar la seguridad o para permitir que varios equipos con direcciones de IP privadas accedan a internet a través de una única IP pública (la del *router*).

Nodo Es una máquina, un *host* o cualquier otro dispositivo de la red de computadoras.

Outbound	Se refiere al tráfico de información que egresa de un proceso.
PAP	Protocolo de autenticación de contraseñas, está diseñado para autenticar sistemas informáticos, no usuarios; y puede requerir autenticación bidireccional.
Password	Es una clave o contraseña, esta palabra se utiliza para validar el acceso de un usuario a un servicio.
PPP	(*Point to point protocol*, protocolo punto a punto) se define en RFC 1661 y otros, realiza detección de errores, reconoce múltiples protocolos, permite la negociación de direcciones de IP en el momento de la conexión, permite la verificación de autenticidad .
PPTP	*Point-to-point tunnel protocol*, a través del uso de una conexión que utilice este protocolo se puede ingresar a internet y convertirla en una comunicación local.
Proceso demonio	Es un proceso que permanece alerta en un servidor, que trabaja de manera transparente para el usuario, de modo que no se nota su presencia en el sistema.

Protocolo	Es un acuerdo (a través de un conjunto de reglas y convenciones) entre las partes que se comunican sobre cómo va a proceder la comunicación. Pueden ser normados (definidos por un organismo capacitado como la CCITT o la ISO) o de facto (creados por una compañía y adoptados por el resto del mercado).
Puerto	Conexión lógica y/o física de una computadora, que permite comunicarse con otros dispositivos externos.
Punto	Hace referencia a un router u otro dispositivo que participa en IPSEC.
Random	Son números generados de manera aleatoria.
Receptor	Computadora o programa que se conecta a la red a la cual se le envía información desde otro dispositivo.
Recursos	Son todos los componentes de la red con los cuales se puede contar (tanto *software* como *hardware*).
Re-keying	Políticas de redistribución de claves de grupo.

RFC (Request for comments, Petición de comentarios) Serie de documentos iniciada en 1967 que describe el conjunto de protocolos de internet y experimentos similares. No todos los rfcs describen *standard* de internet pero todos los *standard* de Internet están escritos en forma de rfcs. En contraste con los protocolos revisados y estandarizados formalmente que son promovidos por organizaciones como CCITT y ANSI.

Router Es un "ruteador", un dispositivo de conexión y distribución de datos en una red. Es el encargado de guiar los paquetes de información que viajan por internet hacia su destino. Opera mediante el uso de tablas y protocolos de enrutamiento.

SA *Security association*, Es un conjunto de parámetros que definen los servicios y mecanismos, tales como llaves, necesarias para proteger la comunicación entre dos puntos que usan IPSEC, son unidireccionales por lo cual necesitan ser creadas para ambos sentidos del flujo de datos.

SHA (*Secure hash algorithm*, algoritmo seguro de dispersión), procesa datos de entrada en bloques de 512 bits pero a diferencia de MD5, genera un compendio de mensaje de 160 bits. SHA comienza por rellenar el mensaje, y luego agrega una cadena de 64 bits para obtener un múltiplo de 512 bits; por último inicializa su buffer de salida de 160 bits.

SIPP (*Simple internet protocol plus*, protocolo simple de internet mejorado) a este protocolo se le dio la designación de IPV6.

SLP *Service location protocol*. El objetivo de SLP consiste en hacer que todos los recursos en red se puedan configurar de forma dinámica gracias al uso de un servicio basado en IP y a agentes de directorio.

Software Componentes intangibles de las computadoras como lo son los programas.

TCP/IP *Transmission control protocol / internet protocol*, (protocolo de control de transmisión / protocolo de internet), conjunto de casi 100 programas de comunicación de datos usados para organizar computadoras en red. Esta compuesta por dos partes: IP que desarma los envíos en paquetes y los "rutea", mientras que el TCP se encarga de la seguridad de conexión, comprueba que los datos lleguen todos y completos.

Timeout	Es una interrupción temporal.
Token	Es un elemento, un símbolo que sirve de señal para activar algún evento.
Túnel	Es una ruta de comunicación segura entre dos puntos, tales como *routers*.
Unicast	Es el tipo de transmisión punto a punto.
VPN	*Virtual private network*. Con la nueva tecnología de redes virtuales sobre Internet las empresas podrán expandirse lógicamente a cualquier lugar, donde se pueda acceder a Internet. Sobre esta infraestructura (Internet) se crea una red privada "virtual" y la oficina principal puede intercambiar información con sus puntos remotos como si estuviesen conectados directamente utilizando líneas dedicadas.

RESUMEN

El rápido progreso de las soluciones para dar seguridad a la información a través de las redes han sido casi exitosas, pero una red casi segura no significa segura.

El protocolo IPSec es la solución propuesta para brindar seguridad a las redes, pues trabaja en la capa de red del modelo OSI a través de la construcción de túneles escriptados entre los puntos de red que se comunican. Los servicios que brinda IPSec son:

- Confiabilidad, a través de la encripción.
- Autenticidad, comprobación del remitente.
- Integridad, a través de la detección de falsificación de datos.
- Protección, defensa contra remitentes no autorizados.
- “Anti-Replay”, para detección y rechazo de paquetes reenviados.

IPSec actúa entre los dos puntos de red configurados para brindar seguridad dentro del túnel creado aún cuando este utilice enlaces de INTERNET, creando un ambiente seguro para el paso de la información. Su máximo rendimiento se aprecia al trabajar con VPN´s.

OBJETIVOS

General

Comprender la importancia del intercambio seguro de paquetes en Internet

Demostrar el uso generalizado del protocolo estándar IPSec para la implementación de Redes privadas virtuales.

Demostrar que Internet es un medio seguro para realizar transacciones electrónicas a través de túneles de encripción basados en IPSec.

Específicos

1. Comprender el funcionamiento de IPSec y sus aplicaciones, a través de la identificación de los componentes de hardware y software asociados.

2. Conocer qué ventajas y desventajas presenta IPSec.

3. Saber elegir entre IPSec y SSL cuando se desee implementar una infraestructura de redes segura a través de Internet u otro tipo de enlace.

INTRODUCCIÓN

El rápido progreso de la tecnología, invita a la investigación, experimentación y aplicación de las nuevas tendencias con el propósito de mejorar constantemente la forma de hacer las tareas; y es está la motivación al realizar este trabajo de tesis, con el fin, de conocer sobre la aplicación del protocolo IPSec al trabajar con redes de computadoras.

Siendo el propósito de desarrollar ampliamente una serie de temas sobre IPSec el que los ingenieros y alumnos de la carrera de "ingeniería en ciencias y sistemas" conozcan y apliquen esta nueva tendencia, que poco a poco se está convirtiendo en un *standard* para manejar la seguridad en las redes de computadoras; con la confianza de que la información que transita por las redes está fuera del alcance de terceras personas, aún cuando los enlaces entre redes se hagan utilizando Internet.

Se han desarrollado protocolos para manejar la seguridad en redes y proteger la información confidencial, sin embargo, estas soluciones han sido casi seguras lo que no significa seguras; además con el uso de internet para enlazar redes este problema se hace más grande, pues internet aunque facilita la obtención de información, debe dejarse claro que fue diseñada con el objetivo de fomentar la investigación, nunca para la realización de transacciones electrónicas seguras, envío de archivos confidenciales, etc.

IPSec es un protocolo propuesto para IP que trabaja en la capa de red, lo que lo hace versátil para su aplicación en las redes de computadoras, ya que a través de la construcción de túneles seguros por parte de IPSec, la información viaja sin alteraciones aún cuando se hace uso de internet.

Este material inicia dando a conocer el protocolo IPSec y sus elementos, su funcionamiento, conociendo sobre los últimos avances en el desarrollo de IPSec y describiendo otros protocolos que se han usado para dar seguridad en redes y realizar transacciones electrónicas, y finalmente, un ejemplo con el propósito de implementar IPSec en Internet para montar una aplicación que permita hacer transacciones electrónicas seguras.

La investigación de este tema ha sido cada vez más fascinante, porque se debe contar con el conocimiento sólido sobre los elementos y funcionamiento de una red de computadoras, y a esto agregar el afán constante de trabajar con redes seguras y con rendimiento óptimo.

El material para elaborar este documento, se obtiene de fuentes fidedignas, pero la mayoría se encuentra publicadas vía internet, ya que los avances son rápidos y constantemente las organizaciones actualizan su información.

Para la realización de las pruebas se hace necesario contar con una red de computadoras, tener acceso a internet para conectarse a un punto remoto de modo que pueda configurarse el protocolo IPSec y colocar la aplicación.

1. CONOCIENDO IPSEC

1.1 Cómo surgió IPSec (1-36)

El modelo que se uso en las primeras redes de computadoras fue conocido como ARPANET creada por el departamento de defensa de los Estados Unidos como una red de investigación, más adelante se necesitó añadir redes de satélite y radios con lo cual se hizo necesario el cambio en la arquitectura de la red; este modelo de referencia se conoció entonces como TCP/IP (*Transmission Control Protocol / Internet Protocol*), que era de uso exclusivo.

En este modelo TCP/IP se encuentra en la capa de "interred" la cual tiene como misión permitir que los nodos ingresen paquetes en cualquier red y los haga viajar de forma independiente a su destino. Esta capa de "interred" define un formato de paquete y protocolo oficial llamado IP (*Internet Protocol*).

El modelo y sus protocolos con el tiempo fueron adoptados por varias empresas que utilizaban redes para la comunicación de sus equipos de computación por lo que se convirtió en un estándar de facto pues la creación de aplicaciones para redes de computadoras que utilizaban estos protocolos aumentó a pasos agigantados.

El uso de este modelo pero principalmente de su protocolo IP en el mercado vino a convertirse con el tiempo en un verdadero problema ya que no se contempló la implementación de ningún tipo de mecanismo de protección contra la alteración de información, ni contra terceras partes que intenten algún tipo de sabotaje contra dicha información que circula a través de las redes de comunicación que utilizan este protocolo.

Este problema surgió debido a que las empresas necesitaron volver las intranet públicas (extranet), pues el entorno en el que estas operan (tanto empresas lucrativas como no lucrativas) las ha obligado a compartir su información con otras instituciones para brindar un mejor servicio y obtener mejores resultados en sus actividades.

Cuando se conoció entonces el problema de la falta de seguridad en la comunicación entre las redes de computadoras, se crearon productos que hasta hoy en día permiten colocar ciertos mecanismos de seguridad para protección de la información que circula por las redes de comunicación. Esto hasta ahora ha sido de preocupación tanto para los administradores de redes de computadoras como para las empresas que proporcionan este protocolo, por lo que han iniciado desde hace algunos años la implementación de lo que se denominó IPSec, que es seguridad para las redes de computadoras que utilizan el protocolo de internet (IP).

1.2 ¿Qué es IPSec?

El término IPSec son las siglas que se utilizan para referirse al protocolo de seguridad de Internet (*Internet Protocol Security*). IPSec es una estructura que brinda seguridad al tráfico de información en las redes de comunicación de computadoras ya que cuenta con la autenticación de los datos para que no puedan ser modificados por terceras personas y encripta el contenido de los paquetes para ocultarlos.

IPSec es una serie de normas que se han establecido para la protección del protocolo de comunicación de internet (IP) ya que especifica las vías para transmitir información privada de manera segura sobre una red de trabajo pública.

Por tanto IPSec se centra en la seguridad que se pueda proporcionar por la capa IP de la red, no se refiere a seguridad a nivel de la aplicación, pudiéndose dividir los requisitos de la seguridad en dos áreas distintas e independientes sin embargo se pueden utilizar juntas o por separado:

- Autenticación e integridad
- Ocultamiento de la información

IPSec fue diseñado por la *Internet Engineering Task Force* (IETF) para IP, IPSec tiene ganada la aceptación entre vendedores de herramientas de encripción y ha llegado a ser un requerimiento para muchas instituciones que desean implementar soluciones para sus redes privadas virtuales (VPN).

IPSec se configura dentro de un marco abierto estándar de desarrollo por la IETF. IPSec brinda seguridad para transmitir información delicada sobre redes no protegidas tales como la internet. IPSec actúa en la capa de red, protegiendo y autenticando los paquetes IP entre los puntos IPsec.

Trabaja con aplicaciones como *Virtual Private Networks* (VPN), esto incluye extranets, intranet y usuarios de acceso remoto. IPSec ofrece una solución robusta de seguridad basado en *standard* o patrones.

1.3 Configuración de la seguridad del IP

IPSec es un conjunto de extensiones de la familia del protocolo IP. Provee servicios de seguridad los cuales permiten la autenticación, integridad, control de acceso y confidencialidad. Es un servicio similar al SSL pero en la capa de red, IPSec es completamente transparente a las aplicaciones, y es mucho más poderoso, pudiendo crear túneles encriptados para las VPN o encriptar solo entre computadoras. IPSec es mucho más complejo que SSL.

Para la configuración del sistema de IPSec y los *gateways* se hace uso de los RFC que tienen buenas recomendaciones de como deben ser implementados y así minimizar confusiones.

Como ya se ha mencionado IPSec es el protocolo propuesto de la capa 3, diseñado para proporcionar seguridad *end-to-end* de la capa de red. El propósito de la configuración de la seguridad del IP (IPSec) es proporcionar el mecanismo y los servicios estándar.

Esto se hace especificando dos cabeceras estándares que se utilizarán con ambas versiones de los datagramas del IP:

- Cabecera de la autenticación del IP (AH).
- Cabecera de "encapsulamiento" de la carga útil del IP (ESP).

Estos dos mecanismos de la capa IP no proporcionan la seguridad contra ataques al tráfico de datos ni ningún otro método utilizado para protegerse en contra de éstos. Nótese que debe también observarse que no se proporciona ningún protocolo específico para la administración de las llaves, aunque la administración de las llaves se conoce que es una parte muy importante del IPSec.

Las aclaraciones anteriores se realizan para que se pueda tener idea de los cambios que se han realizado debido a los defectos que se encontraron anteriormente en los protocolos y algoritmos utilizados.

1.4 Medio en el que trabaja IPSec

Los servicios que brinda IPSec incluyen confiabilidad a través de la encripción, autenticidad a través de la comprobación del remitente, integridad con la detección de falsificación de los datos y protección en cuanto a defensa contra remitentes que no están autorizados para utilizar la información.

IPSec tiene metodologías que permiten administrar las llaves (o claves) públicas y privadas. El protocolo de administración de llaves de IPSec consiste en una serie de pasos que establecen llaves que permiten encriptar o desencriptar información, ya que estas definen el lenguaje común que usarán las dos partes que están conectadas para comunicarse, este protocolo recibe el nombre de IKE (*Internet Key Exchange*).

IPSec trabaja de dos maneras, la primera es en modo de transporte, el segundo método es el modo túnel. Cada uno de estos puntos es tratado ampliamente más adelante.

1.5 Descripción de los elementos de IPSec

1.5.1 Por qué utilizar IPSec (Metas)

IPSec provee los siguientes servicios de seguridad:

- Autenticación del origen de los datos, identificando quién los envía.
- Integridad de los datos, asegura que los datos no han sido cambiados en la ruta.
- Confidencialidad (encripción), asegura que los datos no han sido leídos en la ruta.
- "*Antireplay*", detección de paquetes enviados más de una vez para ayudar a proteger contra ataques.

1.5.2 IPSec consiste en tres componentes

- AH: Cabecera de la autenticación.
- ESP: IP que encapsula la carga útil de la seguridad.
- ISAKMP: Asociación entre el protocolo de seguridad de internet y la llave de administración.

1.5.2.1 AH: Cabecera de autenticación

Authentication header (AH) Viene después del encabezado IP básico, cuenta con criptografía y mecanismos de encripción, hay varios RFC's que enseñan sobre el uso de algoritmos usados en AH, sin embargo, todos deben seguir las especificaciones del RFC2402.

AH tiene a su cargo:

- Integridad de los datos vía la suma de comprobación.
- Origen de datos a través de *password* compartido.
- En juego de nuevo la protección usando como vía el número de secuencia dentro AH de la cabecera.

Figura 1. Datagrama IP

Figura 2. AH-transporte

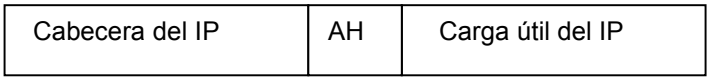
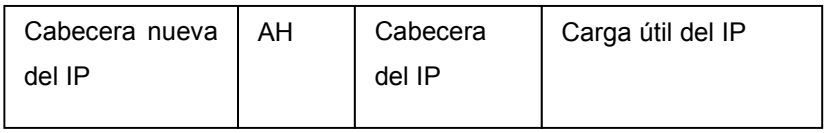


Figura 3. AH-túnel



Autenticación es la característica de saber que los datos recibidos son iguales que los datos que fueron enviados y que el remitente que se anuncia es verdaderamente el remitente real.

La cabecera de la autenticación del IP fue diseñada para proporcionar una sólida integridad y autenticación para los datagramas del IP. Pues la idea de la autenticación es brindar seguridad tanto al transmisor como al receptor del mensaje o paquete.

Esto en cuanto a la confianza que se tenga que la persona que envió el paquete es realmente la persona con la que el receptor compartió su clave secreta. Esto se ha logrado utilizando una función criptográfica para la autenticación sobre los datagramas de IP y usando un *password* como clave secreta de la autenticación .

Antes se tenía la falta de confianza en el uso de las redes públicas, sin embargo, para asegurar su amplio uso en Internet se incluyó el encriptamiento.

1.5.2.2 ESP: Encapsulamiento de la carga útil de IPSec

Encapsulating security payload (ESP) encabezado, permite reescribir la carga de manera encriptada. Varios tipos aplicados a ESP deben seguir el RFC2406. Un encabezado ESP también puede dar autenticación a la carga, pero debe definirse dentro del encabezado.

Figura 4. ESP transporte

Cabecera del IP	Cabecera del ESP	Carga útil del IP	ESP acoplado	ESP autenticación

Figura 5. ESP túnel

Nuevo IP H	ESP H	P H	Carga útil IP	ESP acoplado	ESP autenticación

Figura 6. AH y ESP pueden ser utilizados simultáneamente

Nuevo IP H	Pista AH	ESP AH	Carga útil	ESP acoplado	ESP autenticación

El “encapsulamiento” de la carga útil de la seguridad fue diseñado para proporcionar integridad y dar confidencialidad a los datagramas del IP. Esto se realiza encriptando los datos para protegerlos.

Puede proporcionar también la autenticación pero esto depende de la implementación de los algoritmos y de sus modos del uso. Debe observarse que ESP no brinda "no-renegación" y protección del análisis del tráfico, actualmente la implementación de los algoritmos y modos son estándar de DES.

Algoritmos utilizados en AH y ESP:

- AH utiliza los siguientes algoritmos para autenticar: MD5, SHA-1, RIPEMD-160.
- ESP utiliza los siguientes algoritmos para encriptar: DES, triple DES, DESX, Arcfour, Blowfish, IDEA, CAST128, CAST5-128, RC5.

1.5.2.3 ISAKMP: Asociación del protocolo de seguridad de internet y la administración de la llave.

Diseñado para :

- Proteger contra la negación de los ataques del servicio.
- Proteger contra ataques de hombres en el medio.
- Remitir el secreto (más allá de claves no del valor).

Se ha logrado:

Fase 1: Utilizar la clave pública (*Certs*) para generar una clave principal
Fase 2: Utilizar el MK para negociar asociaciones de la seguridad y otras claves .

ISAKMP: usa valores *random* llamados *cookies* para identificar negociaciones distintas. Con lo anterior puede asumirse que tenemos las llaves que necesitamos para las transacciones seguras.

1.5.3 Componentes tecnológicos

- DES *Data encryption standard* utilizado para empaquetar datos.
  56 *bits* DES-CBC.
  168 *bits* Triple DES (3DES).
- MD5 (variante HMAC) : MD5 *message digest 5* tiene un algoritmo *hash*.
- HMAC tiene una variante *hash* de llave para autenticar datos.
- SHA (variante HMAC): SHA *Secure hash algorithm* es un algoritmo *hash*.
- HMAC tiene una variante *hash* de llave usada para autenticar datos.
- AH *Authentication Header* protocolo de seguridad que brinda autenticación y un servicio opcional de *anti-replay* (no permite repeticiones de envío de paquetes). AH esta inmerso en los datos para ser protegido (es un completo datagrama IP).
- ESP *Encapsulating security Payload*, protocolo de seguridad el cual brinda servicio de privacidad a los datos, opcionalmente también los autentica y da servicios de *anti-replay*. ESP encapsula los datos para ser protegidos.

1.5.4 Utiliza dos modos para comunicarse

AH y ESP soportan 2 modos:

a. Modo transporte

Es la manera por *default*, donde se transmiten directamente de IPSec la información protegida de un *host* a otro *host*. Se le conoce también como organizador principal de *host to host* y brinda protección a las capas altas del protocolo.

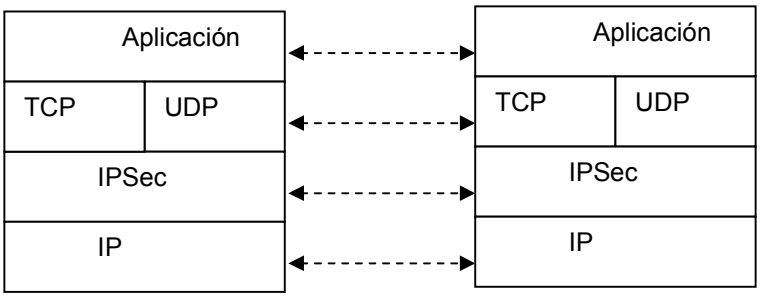
Por ejemplo, un *host* que genera un paquete en el modo transporte, agrega la seguridad en el encabezado antes de los encabezados de la capa de transporte (ejemplo: TCP, UDP), eso significa que el encabezado IP es preparado antes para el paquete. En otras palabras AH agrega al paquete del encabezado de TCP, algunos campos del encabezado IP del punto a punto y luego el encabezado de ESP utiliza la encripción para los datos.

b. Modo túnel

Brinda protección al paquete IP completo. Este modo es usado cuando el encabezado del IP de una red punto a punto esta lista con un paquete "atachado" y uno de los puntos de la conexión segura es solo un *gateway*.

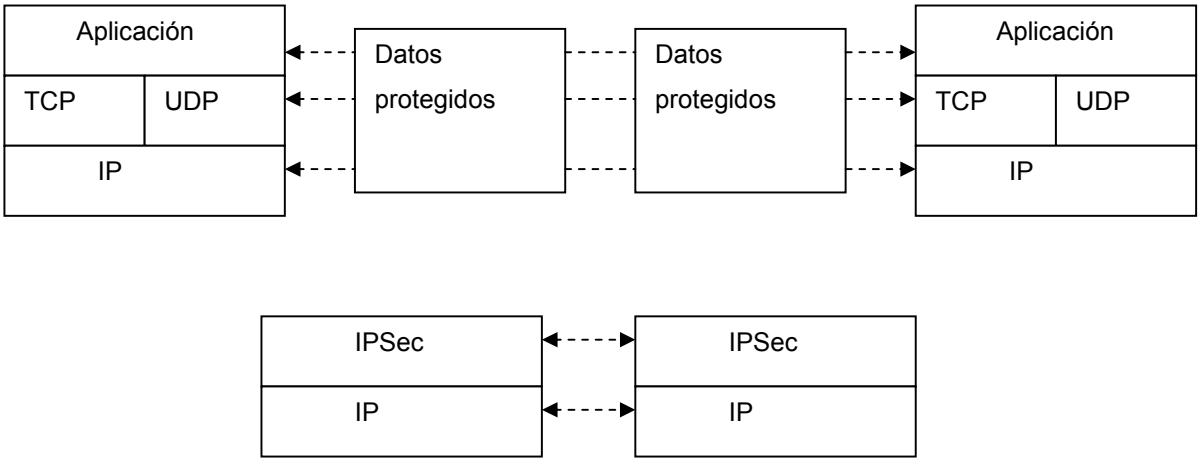
En este modo, el AH y ESP *headers* son usados para cubrir el paquete completo incluyendo el encabezado del punto a punto y el encabezado del nuevo IP es preparado para los paquetes que solo cubren los saltos a los otros puntos de la conexión segura.

Figura 7. Ejemplo de como IP genera tráfico a través de los *host* sin el apoyo de IPSec



Ahora se muestran como los datos son tomados de los cables de la red por dispositivos de seguridad o *gateways* ya que los *gateways* encapsulan por completo el paquete que ha sido encriptado por IPSec, con esto se está incluyendo el encabezado de IP original, luego se agrega la nueva información encriptada y se envía a la forma de aplicación que solicitó la información.

Figura 8. Ejemplo de cómo IP genera tráfico a través de los *host* con el apoyo de IPSec



El modo túnel es utilizado por los dispositivos de VPN que residen en los puntos de entrada y salida de las redes de computadoras pues los túneles son usados para la creación de VPNs seguras ya que se habilita la distribución de redes de comunicación seguras sobre redes públicas.

De cualquier modo, es muy importante recordar que los túneles no soportan multipuntos.

1.5.5 IPSec trabaja en tres maneras:

host-to-host
host-to-network
network-to-network

1.5.6 Encripción

Encripción es el proceso en el cual un mensaje (texto plano) es formado en un segundo mensaje (texto cifrado), usando una función compleja (algoritmos de encripción) y una llave especial de encripción.

Este es un mecanismo que comunmente proporciona confidencialidad ya que lo que hace es encriptar (cifrar) los datos que se envían a través de algoritmos especiales que brindan este tipo de herramienta. Encripción es un proceso a través del cual utilizamos *software* para proteger información sensible mientras se encuentra en tránsito a través de la red de computadoras.

Los algoritmos de encripción y la autenticación utilizados por IPSec son el corazón de los sistemas, ellos son directamente responsables del poder de la seguridad que puede brindar el sistema, sin embargo son la gran desventaja en el área pues como la Internet es una red global, IP debería brindar seguridad de manera uniforme. Muchos países, sin embargo, tienen restringido el uso o exportación de los algoritmos de encripción, lo que significa que IPSec debe ser hábil para balancear entre las restricciones legales y el uso de poderosas encripciones y autenticaciones.

La desencripción es el proceso inverso, en que un texto cifrado es transformado en el texto original usando una segunda función compleja y una llave de desencripción. Las llaves de ambos procesos (encripción y desencripción) podrían ser iguales o diferentes. (Ver llave pública, llave privada, capítulo 2).

1.5.6.1 ¿Cómo funciona la encripción?

La encripción se basa en una clave que se utiliza para cifrar la información, esta consiste en dos partes diferentes: la parte pública y la parte privada. La parte pública de la clave se distribuye a aquellas entidades con las que usted se desea comunicar. La parte privada es sólo para cuando usted decide descifrar lo que le ingresa por la red.

1.6 ¿Quiénes trabajan con IPSec?

Existe una amplia lista de empresas que están, no solo utilizando sino que han desarrollado sus propias versiones de IPSec y continúan realizándoles mejoras dentro de lo que es el mercado de la informática.

Debe comprenderse que todas van tras los mismos objetivos de brindar seguridad al tráfico de información que utiliza redes públicas, pero hasta el momento cada empresa ha dado distintas características a sus versiones lo que provoca ventajas y desventajas de las versiones de IPSec que se ofrecen hoy.

Hasta el momento las versiones de IPSec son utilizadas juntamente con sistemas operativos, pues adquieren los parches y los instalan en sus equipos lo que les permite estar trabajando con seguridad desde la v.4 del IP.

Sin embargo se espera encontrar un estándar que vendría a beneficiar a todos y no solo a un sector de empresas ya que se tendría *software* y *hardware* estándar para trabajar con este protocolo de seguridad.

Los siguientes *gateways* y *routers* han sido reportados como compatibles:

Cisco	IOS
Cisco	PIX
Intel	LanRover
Cendio	Fuego
KAME	for FreeBSD
FreeS/WAN	for Linux
Symantec	Raptor
Ericsson	eBox
F-Secure	VPN+
Teamware	TWISS
3com	Pathbuilder
Nortel	Contivity
CheckPoint	FW-1
Watchguard	Firebox III
Lucent	Access Point

A continuación se muestra una lista de clientes compatibles:

Ashley Laurent VPCom	VPN software
PGP	VPN software
Cisco	IRE client
Microsoft	Windows 2000, XP

1.7 Implementación de seguridad en IPv6

La versión 4 del IP no provee varias características necesarias para que se continúe utilizando, no solo a nivel técnico sino también se han presentado otros problemas para este protocolo como lo son el uso de Internet por parte de mucha gente alrededor del mundo. También se tiene la unión de las industrias de computación, comunicación y de entretenimiento.

Los problemas anteriormente fueron descritos a finales de los años 80 lo que hizo reflexionar que IP tenía que evolucionar y volverse más flexible. Ya en 1,990 IETF inició con los trabajos para la nueva versión de IP.

1.7.1 Características planteadas

- Nunca se quedará sin direcciones.
- Más flexible.
- Más eficiente.
- Resolución de otros problemas.

1.7.2 Metas principales

- Manejo de miles de millones de *hosts*, con asignación de espacio con direcciones suficientes.
- Tablas de enrutamiento más pequeñas.
- Simplificar el protocolo.
- Proporcionar seguridad (autenticidad y confiabilidad).
- Atención a los servicios que necesitan manejar datos en tiempo real.
- Colaborar con la "multitransmisión" permitiendo la especificación de alcance.
- Que los *host* sean móviles.
- Que el protocolo evolucione.
- Que el protocolo nuevo y el antiguo coexistan por mucho tiempo.

Luego de mucho análisis en las propuestas que se tuvieron, se seleccionó una versión modificada de dos de las propuestas hechas (las de Deering y Francis) en 1,993; esta se conoce como de SIPP (*Simple Internet Protocol Plus*), y se le dio el nombre de IPv6.

IPv6 no es compatible con IPv4, pero sí lo es con los demás protocolos de Internet. A nivel técnico se puede decir que IPv6 tiene direcciones más grandes ya que son de 16 *bytes* de longitud y lo más importante es que se ha simplificado la cabecera que contiene 7 campos mientras que la versión anterior tenía 13.

Otro tipo de mejora es el apoyo a las opciones pues esta característica mejora el tiempo de procesamiento de los paquetes. Otra mejora es la prestación de mejor atención al tipo de servicio.

Otra área técnica muy importante, sobre todo para el desarrollo de esta tesis es que se ha incluido seguridad en este nuevo protocolo y para esto las verificaciones de autenticidad y la confiabilidad son claves.

La seguridad en el protocolo es realmente el problema principal sobre el cual se deliberó pues es de suma importancia ya que por las condiciones que se han mencionado en el tema anterior las personas que se comunican a través de las redes de computadoras necesitan en algunas oportunidades, transmitir información delicada que solo concierne a las partes implicadas y no se podía anteriormente garantizar la privacidad de la información, ni la confiabilidad de que no se había alterado la información durante su trayectoria por la red.

¿Dónde debe colocarse la seguridad?, lo mejor probablemente sea en la capa de red porque se tiene entonces un servicio estándar que cualquier aplicación utiliza. Se argumenta que la seguridad solo se ha trabajado a través de aplicaciones que encriptan los datos en el origen y la aplicación destino deshace la encripción.

Un dato curioso que debe tomarse en cuenta es dónde va a funcionar la red con IPSec porque en algunos países tienen leyes estrictas sobre la encripción, por lo tanto el envío de datos cifrados no es de uso común en esos países pues sus políticas están en contra del ocultamiento de información. Esto es un problema para los proveedores ya que todavía continúa en discusión.

Otro punto importante en el tema de seguridad son los algoritmos de encripción que se deben utilizar, ya que los propuestos no parecen ser muy potentes, sin embargo se ha optado por colocar un algoritmo poco conocido. Por lo tanto IPv6 usará un algoritmo de suma de comprobación de primer nivel para efectos de verificación de la autenticidad y un algoritmo débil para la encripción dándose la opción de que el usuario reemplace este algoritmo por el propio.

1.8 Fundamentos para la construcción de IPSec

1.8.1 Funcionamiento de una red con seguridad IPv6 en AH

IPSec es un marco de estándares abierto que brinda a los datos confidencialidad, integridad y autenticación entre los puntos participantes, usa IKE para manejar las negociaciones de los protocolos y algoritmos basados en políticas locales para generar encripción y autenticación de llaves.

IPSec es documentado en una serie de *Internet Drafts*, todos disponibles en http://www.ietf.org/html.charters/ipsec-charter.html todas las implementaciones están según las últimas conversaciones de *Security Architecture for the Intenet Protocol*, *Internet draft* (RFC2401), RFC2402 (*Ip Authentication Header*), como RFC 2410 (El algoritmo de encripción NULL usado con IPSec).

Internet Key Exchange (IKE), es un protocolo híbrido con implementaciones *Oakley* y SKEME *key exchanges* del lado del marco de trabajo del ISAKMP. Este es el que brinda autenticación a los puntos IPSec, negocia las SA de IPSec y establece las llaves IPSec.

Para obtener una comunicación segura entre el transmisor y el receptor, ellos deben ponerse de acuerdo en las claves secretas *password* que utilizarán y que solo ellos conocen. Cada uno de ellos posee un número de clave único de 32 bits; los números que se utilicen son globales por lo que por cada conexión necesitan un número único clave ya que este tiene asociado otros parámetros.

Pasos que se realizan de parte del transmisor del paquete para que cuente con verificación de autenticidad:

- Se construye un paquete que es en sí el conjunto de todas las cabeceras IP y la carga útil.
- Se reemplazan los campos que cambian en el camino por ceros.
- Se rellena el paquete con ceros hasta un múltiplo de 16 *bytes*.
- El *password* también es llenado de ceros hasta un múltiplo de 16 *bytes*.
- Se realiza un cálculo de suma de comprobación cifrada de acuerdo con la base en la concatenación del *password* rellenado, el paquete rellenado y otra vez la clave o *password* rellenado.

La cabecera de verificación de autenticidad se divide en tres partes:

- Número de cabecera.
- Número clave.
- Suma de comprobación cifrada o encriptada.

Cómo el receptor puede confiar que el paquete viene del transmisor con quién se puso de acuerdo para comunicarse:

- Hace uso del número clave para encontrar la clave secreta.
- La clave rellenada se agrega al final y al inicio de cada carga útil rellenada.

- Los campos variables se llenan de ceros y se calcula la suma de comprobación.
- De acuerdo a los puntos anteriores el receptor puede estar seguro que el paquete proviene del transmisor con el que se ha puesto de acuerdo y algo también muy importante, es que tendrá plena confianza en que el paquete no ha sido alterado durante su trayectoria por la red de computadoras.

Es importante que se conozca que la carga útil de un paquete con verificación de autenticidad se envía encriptado ya que no siempre es importante mantener en secreto el mensaje, solo la relación de autenticidad.

1.8.2 Funcionamiento de una red con seguridad IPv6 en ESP

Para el envío de paquetes secretos, se hace a través de esta cabecera de carga útil encriptada. La información que esta cabecera contiene es la siguiente:

- Treinta y dos *bits* que son para la clave o *password.*
- Carga cifrada.
- El algoritmo de cifrado que se utiliza esta a criterio del transmisor y del receptor.

2. IMPLEMENTACIÓN DE IPSEC PARA MONTAR LA INFRAESTRUCTURA SOBRE INTERNET

2.1 Mecanismos de encripción que existen

2.1.1 Mecanismo de encripción a través de *software*

Las compañías se mantienen al ritmo de la tecnología para ofrecer la mejor seguridad a sus clientes. Algunos utilizan *software* para encriptar la información que circula a través de la red, uno de los paquetes de *software* usado actualmente es el cifrado SSL (*Secure Sockets Layer*).

2.1.2 Mecanismo de encripción a través de *hardware*

Una de las maneras para aumentar la velocidad en el proceso de seguridad en las redes es el uso de *hardware* para calcular algoritmos, por ejemplo, el algoritmo DES fue diseñado con un *hardware* rápido de implementación de memoria, sin embargo, muchos de los nuevos algoritmos de encripción han sido diseñados para correr rápido en los modernos microprocesadores, en cambio los IC:s han sido hechos para *hardware* con implementaciones menos atractivas que los viejos algoritmos utilizados.

Para soportar *hardware,* IPSec ha necesitado de adaptadores o módulos:

- *Integrated Services Adapter* (ISA).
- *Integrated services modules* (ISM).

2.1.2.1 *Gateways* de encripción

Algunos proyectos respaldan el uso de *gateways* de encripción oportunistas para proteger la Internet. Estas máquinas usadas como *gateway* están configuradas para el uso de IPSec (los cuales generalmente actúan como *routers*) y tratan de proteger el tráfico de la red, cada vez que la otra terminal lo apoya. La otra terminal debe ser un nodo que esté diseñado para trabajar con IPSec o un *gateway* oportunista. Este podría ser usado para proteger una gran cantidad de tráfico de salida.

2.2 Elementos para el establecimiento de políticas

2.2.1 *Security Association* (SA)

Un SA es un conjunto de parámetros que definen los servicios y mecanismos, tales como llaves, necesarias para proteger la comunicación entre dos puntos que usan IPSec.

Es una descripción de dos o más entidades que usan servicio de seguridad en el contexto de un protocolo de seguridad (AH o ESP) para comunicarse de manera segura a favor de un flujo de datos en particular.

Los enlaces seguros de IPSec son definidos en términos de *security associations* (SAs). Cada SA es definida para una sola dirección de flujo de datos y generalmente de un solo punto a otro, cubriendo tráficos fácilmente distinguibles por algún único selector. Todo el tráfico que fluye sobre un solo SA es tratado de la misma manera. Se puede contar con tráfico que puede estar sujeto a varias SA, eso significa que puede tener varias transformaciones. Los grupos SA son llamados SA *Bundle*.

Los paquetes que llegan se les asigna a una SA particular, esto en base a un árbol de definición de campos (dirección IP destino, *security parameter index* SPI, protocolo de seguridad, etc. que se definen más adelante).

Las acciones que se pueden definir en las políticas de IPSec son las siguientes:

Permit Permitir seleccionar un paquete cuando cumpla con la política establecida (haga "*match*").

Deny Descartar cualquier selección de paquete (cualquier "*match*").

Las SA de IPSec están establecidas ya sea por IKE o por configuración manual del usuario. Las SA son unidireccionales por lo que se necesita que las SA (para cada protocolo) estén establecidas para ambas direcciones al mismo tiempo.

Si se utiliza IKE entonces se establecen automáticamente las SA para el flujo de datos, esto significa que las SA son establecidas cuando se necesitan y expiran luego de un periodo de tiempo (o volumen de tráfico). Si las SA son establecidas manualmente, estas se fijan tan pronto como la configuración necesaria es completada y no haya expirado.

Un SA incluye normalmente los siguientes parámetros (requeridos):

- Algoritmo de la autenticación y modo del algoritmo que es utilizado con el IP AH.
- *Key(s)* usado con el algoritmo de la autenticación en uso con AH.
- El algoritmo del cifrado, modo del algoritmo, con el IP ESP.
- *Key(s)* usado con algoritmo del cifrado en uso con ESP.
- Talla de un campo criptográfico del vector de la sincronización o de la iniciación para el algoritmo del cifrado (recomendados).
- Algoritmo y modo de la autenticación usado con ESP.
- *Key(s)* de la autenticación usado con el algoritmo de la autenticación que es parte ESP.
- Curso de vida de la clave o del tiempo en que el cambio debe ocurrir.
- La dirección de la fuente del SA, puede ser un direccionamiento del comodín, si más de un sistema que envía comparte el mismo SA con el destinatario.
- Sensibilidad llana (por ejemplo: confidencial o sin clasificar) de los datos protegidos (requeridos para todo el sistema que demandan proporcionar seguridad de varios niveles, recomendado para el resto de los sistemas).

Un SA es normalmente en una dirección, mientras que la autenticación en la comunicación de sesiones entre dos *hosts* será regularmente con dos SPI en uso (uno para cada dirección).

Cada SA puede definir un encabezado ESP y un encabezado AH. Una sesión de IPSec debe tener uno u otro pero no ambos y tampoco puede ser definido sin ningún encabezado, en otro caso debería no contar con ningún encabezado para especificar un SPI. Los RFC no dicen qué pasa si el AH o ESP están en desacuerdo sobre los valores del SPI.

2.2.1.1 *Perfect forward secrecy* (PFS)

Está asociado a un valor secreto compartido. Con PFS, si una llave es comprometida, las llaves anteriores y las siguientes no son comprometidas porque las llaves siguientes no son derivadas de las llaves antecesoras.

2.2.2 *Security parameter Index* (SPI)

SPI es un valor *random* de 32-*bit* que identifica las SA para el datagrama determinado. El SPI se considera como un *cookie* que es recibido por SA cuando los parámetros de conexión son negociados.

El valor del índice para los parámetros de seguridad es igual a 0 (cero) para indicar que no existe ninguna asociación de seguridad. El conjunto de valores de índices de los parámetros de seguridad en el rango de 1 a 255 se reserva al *Internet Assigned Numbers Authority* (IANA) para el uso futuro. Un valor reservado de SPI no será asignado normalmente por IANA a menos que el uso de éste valor asignado determinado de SPI se especifique abiertamente en un RFC.

Este SPI es un número, el cual junto con una dirección IP destino y un protocolo de seguridad, identifican una SA en particular.

Los IETF también definen mecanismos automáticos para inicializar sesiones, cambio de llaves, etc. Los RFC que hablan sobre el cambio de llave de ISAKMP son: RFC2407, RFC2408 Y RFC2409.

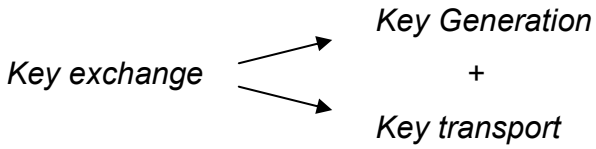
Cuando se usa IKE para establecer la SA, el SPI para cada SA es un número *pseudo-random*. Sin IKE, el SPI es especificado manualmente para cada SA.

2.2.3 Transformador

Para la lista de operaciones hechas en el flujo de datos para brindar datos autenticados, confidenciales y comprimidos. Por ejemplo, una trasformador es el protocolo ESP con el algoritmo de autenticación HMAC-MD5. Otro trasformador es el protocolo AH con 56 bits.

2.2.4 *Key management*

Key management este término hace referencia a crear, distribuir, almacenar y borrar llaves. Lo más importante que hace es intercambiar llaves. Los algoritmos de encripción se usan con llaves de encripción



Con las llaves de autenticación, técnicamente hay dos categorías con problemas:

1. Débil autenticación: Envío de llaves claramente dentro del texto.
2. Fuerte autenticación: Uso de encripción y firma digital.

Llave pública de criptografía: Es un método más fuerte de autenticación.

Internet Key Exchange es una combinación de:

- *Internet security association* y *key management protocol* (ISAKMP), el cual define un marco común para el soporte del establecimiento de las SA.
- *Oakley*, un protocolo de determinación de llave que usa el algoritmo de negociación de llave Diffie-Hellman. *Oakley* soporta el *Perfect Forward Secrecy* (PFS), el cual asegura que si una sola llave es comprometida, este permite el acceso solo a datos protegidos por esa sola llave.

Protocolos de *Key exchange*:

- SKIP
- PHOTURIS
- SKEME
- OAKLEY

2.2.5 ¿Cómo se controla un paquete a través de la red utilizando SA?

Existen dos entidades administradoras que controlan lo que le sucede a un paquete. Una es la *Security Association Database* (SAD) y la otra es la *Security policy database* (SPD).

Para comprender cómo trabajan estas dos entidades, se cita el siguiente caso, cuando existe similitud en el número que dan los selectores que describen algún tráfico de datos, ellos (los selectores) reparten una entrada que necesite proceso, sin embargo, la SPD esta en el siguiente paso.

El SPD está siendo usado para la salida de paquetes, para decidir qué entradas usan SAD, ya que las entradas SAD son retornadas para describir que proceso y que parámetros se aplicarán al paquete. Las entradas especificadas por el SPD son entradas existentes en SAD.

Los campos que han sido creados por SA pueden tomarse ya sea de las entradas SPD o de los paquetes que iniciaron la creación. La salida de paquetes va de la entrada de SPD a las especificaciones de SA. Mientras tanto los paquetes que son tomados de SA (por estar correctos) son usados por SPI.

Los SPD pueden especificar qué tráfico puede pasar por IPSec y cual debería ser desechado. Las entradas para SPD deben ser explícitamente ordenadas como varios paquetes y deben ser procesadas para ser reproducidas.

La SPD es similar a un paquete filtrado donde las acciones deciden sobre la activación de los procesos de SA.

Los selectores pueden incluir SRC y direcciones de destino, números de puertos, aplicaciones y usuarios finales disponibles (solo en *host* basados en SA), nombres de *host*, niveles de seguridad, protocolos, etc.

Una entrada SAD debe incluir:

- Dirección IP destino.
- IPsec protocolo (AH o ESP).
- SPI (*cookies*).
- Conteo de secuencia.
- Secuencia con bandera O/F.
- Información de ventana *anti replay*.
- Información y tipo del AH.
- Información y tipo de ESP.
- Información del tipo de vida.
- Bandera del modo utilizado túnel/ trasporte.
- Ruta de acceso a la información MTU.

Un SPD debe contener:

- Puntero para activar SAs.
- Campo selector.

2.3 Como configurar ISAKMP

ISAKMP alguna veces se refiere a *Intenet Key Exchange* (IKE), éste es el mecanismo de cambio de llave para las VPN. Un encuentro concerniente a la seguridad usando métodos mencionados en los RFC 2407, 2408 y 2409.

ISAKMP maneja los cambios de llaves criptográficas que deben normalmente tener un manejador con IPSec, este emplea un proceso de dos fases para establecer los parámetros IPSec entre dos nodos IPSec.

Fase 1: Los dos puntos ISAKMP establecen una seguridad, con un canal autenticado sobre el cual hay una comunicación entre dos procesos demonio.

El establecimiento de *security association* (SA) entre ambos *host*, la elección del modo de trabajo (modo principal (*Main mode*) y modo agresivo (*Aggressive Mode*)) son los métodos usados para establecer el canal.

El modo principal envía información de varias autenticaciones en una secuencia, brindando protección, mientras el modo agresivo no cuenta con protección porque todo lo relacionado con la autenticación es enviado al mismo tiempo, este último modo debe ser usado en casos tales como redes de banda ancha.

Fase 2: Las SA hacen las negociaciones a favor de IPSec. En esta fase se establece el túnel SA entre los *hosts* IPSec.

El modo rápido (*Quick mode*) es usado en la fase 2 ya que no necesita hacer una repetición completa de autenticación, mientras la fase 1 ya tiene establecidas las SA.

En resumen, la fase 1 es usado para obtener seguridad en el canal en el cual se hace la configuración de la fase 2. Aquí puede hacerse una múltiple configuración de la fase 2 dentro del mismo canal de la fase 1. La fase 2 es usada para configurar el túnel actual.

En la fase 1 el nodo IPsec establece una conexión donde se intercambia la autenticación (ya sea un certificado X.509 o una clave compartida preestablecida), esto permite que cada terminal asegure que la otra terminal está autenticada. La fase 2 en un intercambio de llaves determina como la información entre los dos nodos será encriptada.

La manera de usar ISAKMP es la siguiente: Los protocolos ESP y AH son habilitados por *default* en el *kernel*, debe verificarse que los protocolos que se necesitan estén disponibles para los procedimientos fuera de línea, luego es necesario editar las políticas, esto incluye verificar que el estado del archivo de políticas para cualquiera que envía datos usando el ESP sea correcto y además cuenta con la autenticación de la "frase determinada" para saber si tiene permitida la comunicación con ISAKMP. Se puede modificar el archivo para dejar que ISAKMP conozca solo lo que se desee, por Ej. datos con certificados digitales o usando una transformación a través de una encripción para cualquiera que acceda a IPSec. Ver apéndice 1.

2.4 Llave pública

La llave pública es la que se proporciona a los otros clientes de la red con los que se desea comunicar y los que la tengan podrán conocer el contenido del mensaje ya que podrán volver el mensaje recibido a la sintaxis correcta de modo que puedan interpretar la información.

2.4.1 Criptografía de llave pública o asimétrica

Se utiliza una llave pública para encriptar el mensaje y una privada para desencriptarlo. El término llave pública viene del hecho que se puede hacer pública la llave de encripción sin comprometer la privacidad del mensaje o la llave de desencripción. Se utiliza para crear firmas digitales sobre datos, como en el correo electrónico, para certificar el origen de los datos y su integridad.

Por ejemplo: Cuando se envía información personal a alguien en la red, el que envía utiliza la clave pública o llave pública para codificar su información personal. Eso significa que si en algún punto de la transmisión su información es interceptada, ésta se mezcla y se hace muy difícil de descifrar. Una vez que la persona a la que se le envía recibe su información personal cifrada, se utiliza la parte privada de la clave para descifrarla.

Algoritmos de llave pública:

- Diffie-Hellman
- RSA
- ElGamal
- DSA
- DSS

2.5 Llave privada

La llave privada es la clave con la cual se descifra la información encriptada que se recibe por la red de computadoras a la cual se está conectado, de esta manera se podrá conocer el contenido de dicha información confidencial que ha ingresado a la red.

2.5.1 Criptografía de la llave privada o simétrica

Utiliza la misma llave para encriptar y desencriptar el mensaje. Se utiliza para proteger información almacenada en discos duros o para encriptar información transferida entre dos computadores que están enlazados.

Algoritmos de llave privada:

ROT13	crypt
DES	DESX
Triple-DES	RC2
RC4	RC5
IDEA	Skipjack

Por ejemplo: Si alguien en la red le envía información encriptada por medio de su llave pública, cuando se reciba la información el proceso que debe realizarse inicialmente es el de desencriptar o descifrar el mensaje de modo que sea entendible, esto se logra utilizando la llave privada con la que se cuenta. Este proceso lo realiza automáticamente el *software* que se tiene en la computadora (el cual contiene la llave privada) cuando se recibe información.

Una aplicación que se puede mencionar sobre este tema es que hoy día con la necesidad de identificarse se utilizan mecanismos de identificación basados en técnicas de identificación computarizada, *password*, algún elemento (*token*), por ubicación, firmas digitales con llave privada, etc.

2.6 L2TP

El protocolo para un túnel de la capa 2 (L2TP) es una extensión al PPP que permite a los usuarios remotos tener acceso a redes corporativas de una manera segura, usando redes públicas tales como el Internet. L2TP es un protocolo estándar del *Internet Engineering Task Force* que emerge (IETF).
El protocolo para un túnel de la capa 2 es una evolución del protocolo anterior L2F propuesto por Cisco y la salida para señalar el protocolo para un túnel (PPTP) propuesto por Microsoft.

L2TP representa la generación siguiente de los protocolos para crear túneles, además L2TP permite que los usuarios remotos tengan acceso a la red corporativa poniendo llamadas locales y usando la infraestructura de la red pública para alcanzar la red corporativa. Esto reduce cargas de acceso de red eliminando llamadas costosas por ser internacionales. L2TP es una herramienta dominante en la construcción de las redes privadas virtuales (VPN).

L2TP hace un túnel para el tráfico del PPP para redes públicas o privadas, incluyendo el Internet. Proporciona la autenticación de la conexión del PPP usando el PAP, la GRIETA, etc., como en una sesión típica del PPP. Esto se hace para evitar que individuos no autorizados intercepten las comunicaciones que pueden ocurrir al concluir conexiones Internet normales.

Al ejecutar sesiones de *Multilink* PPP (ML-PPP), todas las conexiones que se hacen hacia arriba como un manojo de *Multilink* deben terminar en el mismo servidor. L2TP elimina la necesidad de que las conexiones individuales deban terminar en el mismo servidor del acceso, haciendo un túnel de las sesiones individuales del PPP a un campo común. Esto permite, por ejemplo, a una corporación poner en ejecución los servidores de acceso de una manera más flexible, y a los usuarios remotos no tienen que preocuparse del servidor al que se están conectando.

Una aplicación de este protocolo es la puesta en práctica de *Telenetworks* de L2TP, esta se basa en el bosquejo de la Internet del funcionamiento del PPP del IETF (*draft-ietf-pppext-l2tp-11.txt*). *Telenetworks* utiliza el concentrador del acceso de L2TP (LACA) y los protocolos del servidor de la red de L2TP (LNS).

El protocolo de *Telenetworks* L2TP se pone en ejecución como código fuente en " C " y se puede integrar fácilmente con el protocolo de *Telenetworks Multi-Link* PPP (ML-PPP) y del protocolo ISDN. Proporciona un conjunto de funciones con las cuales el sistema externo puede poner varias funciones de transferencia en ejecución para el control de datos, tales como crear un túnel, suprimir un túnel, comenzar una sesión, envío y recepción de los datos hacia el túnel y del túnel.

2.7 ¿Cómo trabaja IPSec?

IPSec brinda seguridad en un túnel entre dos puntos, como por ejemplo dos *routers*. Se define qué paquetes son importantes y deben ser enviados a través de este túnel seguro, definiéndose también los parámetros que son utilizados para proteger estos paquetes para la especificación de las características de este túnel. De esta manera cuando el punto que trabaja con IPSec se entera que el paquete que va a enviar es importante lo configura y lo envía a través del túnel hacia el punto remoto.

Los túneles cuentan con las *security associations* SA que son establecidos entre los dos puntos IPSec. Las SA definen que protocolos y que algoritmos son aplicados a los paquetes importantes y también especifican la llave que es usada entre los dos puntos. Las SA son establecidas por los protocolos de seguridad (AH o ESP).

Con IPSec se define que tráfico será protegido entre los puntos IPSec para esto se configura la lista de acceso y se aplica la lista a la *interface* haciendo uso de mapas criptográficos.

Por lo tanto el tráfico puede basarse en las direcciones fuentes y destino, y opcionalmente utilizar el protocolo de la capa 4 y el puerto. El acceso a la lista utilizada por IPsec es solo para determinar qué tráfico debe ser protegido por IPSec y no qué tráfico debe ser bloqueado o no permitido a través de la *interface*.

Un mapa criptográfico puede tener múltiples entradas, cada una con una lista de acceso diferente. Las entradas de los mapas criptográficos son buscados en el orden que el *router* intenta seleccionar el paquete para la lista de acceso de esa entrada.

Cuando el paquete es seleccionado por una entrada "permitida" de una lista de acceso en particular y el mapa criptográfico correspondiente es etiquetado, las conexiones son establecidas si fuera necesario.

El mapa de entrada criptográfico es etiquetado como IPSec-ISAKMP, IPSec es activado. Si no existe los SA que IPsec usa para proteger el tráfico en el punto, IPSec usa IKE para negociar con el punto remoto y configurar los SA de IPsec necesarios en favor del flujo de datos.

La negociación utiliza información especificada en las entradas del mapa criptográfico como también la información del flujo de datos de la entrada específica de la lista de acceso. Si la entrada del mapa criptográfico es etiquetado como IPSec-manual, IPSec es activado.

Si no existen SA que IPSec pueda usar para proteger el tráfico en el punto, el tráfico es eliminado. En este caso, las SA con instaladas a través de la configuración, sin la intervención de IKE. Si las SA no existen, IPSec no tiene todas las piezas necesarias para ser configurado. Una vez establecido, el conjunto de las SA (*outbound*, para el punto) son entonces aplicados a los paquetes que activan IPSec.

Si IKE es usado para establecer las SA, estas SA tienen un tiempo de vida que periódicamente expira y requiere de una renegociación. Esto es un agregado al nivel de seguridad.

Múltiples túneles IPSec pueden existir entre dos puntos para asegurar los diferentes archivos de datos, cada túnel es una configuración separada de SA. Por Ej. algunos archivos de datos deben ser autenticados únicamente mientras que otros archivos de datos deben ser encriptados y autenticados.

La lista de acceso asociada con IPSec a las entradas del mapa de criptografía también representa qué tráfico del *router* necesita ser protegido por IPSec.

El tráfico *Inbound* entra en un proceso contra el mapa de criptografía, si un paquete no protegido es seleccionado por una entrada "permitida" en una lista de acceso asociada a IPSec, ese paquete es desechado porque no fue enviado como un paquete protegido IPSec.

Las entradas en un mapa de criptografía también incluye la configuración de los transformadores. Un transformador configurado es una combinación aceptable del protocolo de seguridad, de algoritmos y otras configuraciones para aplicar al tráfico protegido de IPSec. Durante la negociación de SA de IPSec, los puntos se ponen de acuerdo para utilizar un transformador particular cuando protegen un flujo de datos particular.

2.9 Monitoreo y mantenimiento de IPSec

Para el monitoreo de mantenimiento de IPSec es importante tomar en cuenta lo siguiente:

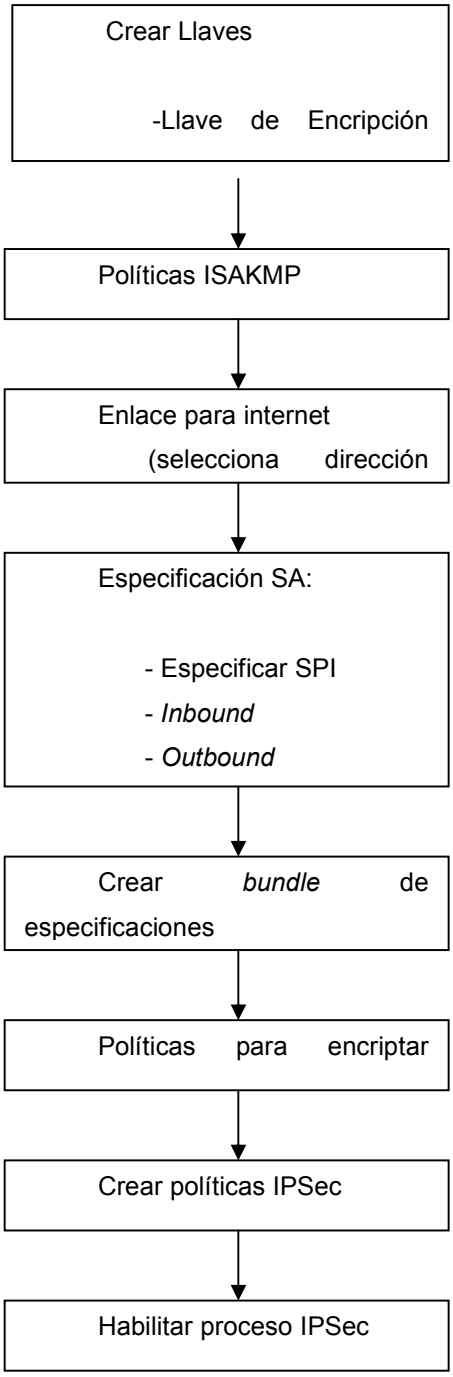
Si la configuración cambia, solo tendrá efecto para las próximas negociaciones de SA.

Si lo que se desea es una nueva configuración y ponerla de inmediato a trabajar, lo que se necesita es limpiar o eliminar las SA establecidas para que las SA puedan ser nuevamente reestablecidas con los cambios de la configuración. Para el establecimiento manual de las SA, solo se eliminan y se reinicializa la SA, de lo contrario nunca tomarán efecto.

SI el *router* esta activo procesando el tráfico IPSec, es aconsejable limpiar solo la parte de la base de datos SA que debería ser afectada por los cambios de la configuración (esto significa limpiar solo las SA establecidas por un mapa de criptografía).

Hacer una eliminación completa de la base de datos de las SA será reservada para cambios a gran escala o cuando un *router* está procesando muy pequeños tráficos IPSec.

Figura 9. Diagrama de flujo para configurar IPSec.



3. IPSEC VRS. OTROS PROTOCOLOS DE SEGURIDAD PARA LA RED

La intención en este capítulo es que se cuente con un marco de referencia que permita contemplar una perspectiva más amplia de lo que se está haciendo para trabajar con una red que asegure la integridad y la confidencialidad de los datos.

Se ha tratado de demostrar que es posible realizar transacciones electrónicas seguras con IPSec a través de internet, sin embargo, en el mercado existen otras opciones, como por ejemplo: SSL el cual se describe a continuación, tomando este protocolo como base por ser de los más conocidos en el medio para realizar este tipo de tareas. También se menciona el protocolo SET como complemento para llevar a cabo transacciones electrónicas que tiene a su cargo SSL.

3.1 *Secure Sockets layer* (SSL)

Este es un protocolo ampliamente extendido en internet por lo que goza de gran popularidad, soportado por los principales navegadores del mercado, *Netscape Navigator* 3.0 en adelante y por *Internet Explorer* 3.0 en adelante.

No se necesita realizar ninguna acción especial para invocar el protocolo SSL, asegurándose solamente de que este habilitado en el navegador, luego basta con seguir un enlace o abrir una página cuya dirección empieza por https://. El navegador se encarga del resto.

3.1.1 Cómo funciona SSL

SSL se ubica en la pila OSI entre los niveles de transporte (TCP/IP) y de aplicación. SSL proporciona sus servicios de seguridad cifrando los datos intercambiados entre el servidor y el cliente con un algoritmo de cifrado simétrico, que puede elegirse entre DES, triple-DES, RC2, RC4 o IDEA, y cifrando la clave de sesión de los algoritmos anteriores mediante un algoritmo de cifrado de clave pública, típicamente el RSA. La clave de sesión es la que se utiliza para encriptar los datos. Se genera una clave de sesión distinta para cada transacción, lo cual permite que aunque sea capturada por un atacante en una transacción dada, no sirva para descifrar futuras transacciones. MD5 o SHA se pueden usar como algoritmos de resumen digital (*hash*).

Este protocolo sigue las siguientes fases:

1. La fase inicial: Donde se ponen de acuerdo sobre el conjunto de algoritmos para mantener la confidencialidad y para la autenticación. El navegador le informa al servidor de los algoritmos que posee disponibles.

2. La fase de autenticación: En la que el servidor envía al navegador su certificado x.509v3 que contiene su clave pública y solicita a su vez al cliente su certificado X.509v3.

3. La fase de creación de clave de sesión: En la que el cliente envía al servidor una clave maestra a partir de la cual se generará la clave de sesión para encriptar los datos intercambiados posteriormente haciendo uso del algoritmo de cifrado simétrico acordado en la fase 1. El navegador envía cifrada esta clave maestra usando la clave pública del servidor que extrajo de su certificado en la fase 2. Posteriormente, ambos generarán idénticas claves de sesión a partir de la clave maestra generada por el navegador.

4. La fase fin: En la que se verifica mutuamente la autenticidad de las partes implicadas y que el canal seguro ha sido correctamente establecido. Una vez finalizada esta fase ya se puede comenzar la sesión segura.

3.1.2 Uso de SSL

SSL constituye una de las soluciones más utilizadas que ofrecen los servicios de comercio electrónico. Su mayor mérito radica en ofrecer una respuesta al principal problema que afronta el comercio en línea: el temor de enviar números de tarjeta de crédito a través de un formulario web y que este sea interceptado por un *hacker*.

La forma más fácil para construir un sistema de comercio en Internet consiste en utilizar un servidor *web* con un catálogo (compuesto por páginas web) con información sobre los productos o servicios ofrecidos y un formulario para procesar los pedidos.

Cuando el cliente termina sus compras, pasa por una "caja virtual" que iniciará el proceso de pago. El usuario debe llenar un formulario con sus datos personales (para comprobar la veracidad de la información de pago) y los datos correspondientes a su tarjeta de crédito (número, fecha de caducidad, titular). Esta arquitectura no exige que el servidor disponga de capacidades especiales para el comercio. Basta con que se utilice como mínimo un canal seguro para transmitir la información de pago.

Sin embargo, este enfoque, aunque práctico y fácil de implantar, no ofrece una solución comercialmente integrada ni totalmente segura. A medida que el comercio crece, esta arquitectura podría llegar a resultar difícil de expandir o de incorporar nuevas tecnologías y componentes a medida que vayan apareciendo.

3.1.3 Desventajas de SSL

- SSL ofrece un canal seguro para el envío de números de tarjeta de crédito, pero carece de capacidad para completar el resto del proceso comercial: verificar la validez del número de tarjeta recibido, autorizar la transacción con el banco del cliente y procesar el resto de la operación con el banco adquiriente y emisor.

- SSL sólo garantiza la confidencialidad e integridad de los datos en tránsito, ni antes ni después. Por lo tanto, SSL solamente asegura que mientras viajan desde el navegador hasta el servidor no serán modificados ni espiados. Lo que el servidor haga con ellos, está ya más allá de la competencia de este protocolo. Los datos podrían ser manipulados irresponsablemente o caer en manos de un atacante que asaltara el servidor con éxito.

- Además, con SSL al producirse ataques sobre servidores de comercio creados sin las medidas de seguridad adecuadas, se puede averiguar números de tarjeta reales.

3.2 *Secure electronic transaction* (SET)

SET fue desarrollado en 1995 por Visa y MasterCard, con la colaboración de otras compañías líderes en el mercado de las tecnologías de la información, como Microsoft, IBM, Netscape, RSA, VeriSign y otras.

En cuanto el protocolo SET 1.0 fue finalizado, comenzó a emerger una infraestructura basada en el mismo para soportar su uso a gran escala. Existen fabricantes de *software* que han empezado a crear productos para realizar compras de manera segura a través SET.

Servicios que ofrece SET

- Autenticación: Todas las partes implicadas en la transacción económica (el cliente, el comerciante y los bancos, emisor y adquiriente) pueden autenticarse mutuamente mediante certificados digitales.

- Confidencialidad: La información de pago se cifra para que no pueda ser espiada. Es decir, solamente el número de tarjeta de crédito es cifrado por SET, de manera que ni siquiera el comerciante llegará a verlo, para prevenir fraudes. Si se quiere encriptar el resto de datos de la compra, como por ejemplo qué artículos se han comprado, debe recurrirse a un protocolo de otro nivel

- Integridad: Garantiza que la información intercambiada no podrá ser alterada mientras viaja a través de la red. Para lograrlo se utilizan algoritmos de firma digital.

- Gestión del pago: SET gestiona tareas asociadas a la actividad comercial de gran importancia como el registro del titular y del comerciante, autorizaciones y liquidaciones de pagos, anulaciones, etc.

SET toma en cuenta para realizar sus transacciones:

- El titular de la tarjeta.
- Banco emisor (emite la tarjeta del cliente).
- El banco adquiriente (el que procesa las transacciones con tarjeta y las autorizaciones de pago).
- El comerciante (que vende productos, servicios o información).
- La pasarela de pagos (mecanismo mediante el cual se procesan y autorizan las transacciones del comerciante).
- El procesador (proporciona servicios adicionales operando la infraestructura de telecomunicaciones sobre las que se realizan las transacciones).
- Autoridad de certificación (certifica las claves públicas del titular de la tarjeta, del comerciante y de los bancos).

3.2.1 El funcionamiento de SET

1. Decisión de compra del cliente. El protocolo SET se inicia cuando el comprador pulsa el botón de pagar.
2. Arranque del monedero. El servidor del comerciante envía una descripción del pedido que despierta a la aplicación monedero del cliente.
3. El cliente comprueba el pedido y transmite una orden de pago de vuelta al comerciante. La aplicación monedero crea dos mensajes que envía al comerciante. El primero, la información del pedido, contiene los datos del pedido, mientras que el segundo contiene las instrucciones de pago del cliente (número de tarjeta de crédito, banco emisor, etc.) para el banco adquiriente. En este momento, el *software* monedero del cliente genera un firma dual, que permite juntar en un solo mensaje la información del pedido y las instrucciones de pago, de manera que el comerciante puede acceder a la información del pedido, pero no a las instrucciones de pago, mientras que el banco puede acceder a las instrucciones de pago, pero no a la información del pedido. Este mecanismo reduce el riesgo de fraude y abuso, ya que ni el comerciante llega a conocer el número de tarjeta de crédito empleado por el comprador, ni el banco se entera de los hábitos de compra de su cliente.
4. El comerciante envía la petición de pago a su banco. El software SET en el servidor del comerciante crea una petición de autorización que envía a la pasarela de pagos, incluyendo información relevante acerca de la misma, todo ello convenientemente cifrado y firmado.
5. El banco adquiriente valida al cliente y al comerciante y obtiene una autorización del banco emisor del cliente.
6. El emisor autoriza el pago.

7. El adquiriente envía al comerciante un testigo de transferencia de fondos. En cuanto el banco del comerciante recibe una respuesta de autorización del banco emisor, genera y firma digitalmente un mensaje de respuesta de autorización que envía a la pasarela de pagos, convenientemente cifrada, la cual se la hace llegar al comerciante.
8. El comerciante envía un recibo al monedero del cliente. Cuando el comerciante recibe la respuesta de autorización de su banco, verifica las firmas digitales y la información para asegurarse de que todo está en orden.
9. El software del comerciante genera una petición de transferencia a su banco, confirmando la realización con éxito de la venta. Como consecuencia, se produce el abono en la cuenta del comerciante.
10. Luego el dinero se descuenta de la cuenta del cliente (cargo).

El protocolo definido por SET especifica el formato de los mensajes, las codificaciones y las operaciones criptográficas que deben usarse. No requiere un método particular de transporte, de manera que los mensajes SET pueden transportarse sobre HTTP en aplicaciones web, sobre correo electrónico o cualquier otro método. Como los mensajes no necesitan transmitirse en tiempo presente, son posibles implantaciones de SET eficientes basadas en correo electrónico u otros sistemas asíncronos.

3.2.2 Desventajas de SET

SET esta orientado exclusivamente a dar seguridad a la parte de pago del cliente en una transacción electrónica, pero no brinda ningún tipo de seguridad para el resto de información que se maneja de la transacción.

SET solo soporta transacciones con tarjeta de crédito/débito, y no con otro tipo de tarjetas o formas de pago.

3.3 *Internet protocol security* (IPSec)

En los últimos tiempos la información ha jugado un papel importante en la sociedad. Lo crucial de estos cambios fueron las tendencias tecnológicas y sociales que han impactado casi todos los aspectos. Siendo testigos del desarrollo del mejor significado que tienen los procesos de información que han cambiado las habilidades para obtener, transmitir y evaluar los datos.

Para el mundo de los negocios, estas tendencias han sido significativamente radicales, con el objeto de ser competitivas en la actualidad de acuerdo a la información que existe en el mercado. Una compañía debe brindar el acceso inmediato a la información de sus productos, estrategias e indicadores financieros. Para muchos, una corporación de *web site* es el medio ideal para tales tareas.

Las soluciones a estas necesidades se fundamentan en la comunicación en línea: intranets y extranets. Las intranets son redes internas (en términos de trabajo, basado en sus características de comunicación), que son de uso exclusivo para usuarios que se encuentran dentro de una empresa corporativa.

Las extranets, en comparación son intranets que permiten las conexiones a sucursales que físicamente se encuentran fuera de la compañía.

La mayoría de las compañías están poniendo en uso los métodos más efectivos para aprovechar estas soluciones, combinándolas dentro de un nuevo modelo de comunicación: La red corporativa.

Abarcando las diferentes tecnologías de información, la red corporativa es una entidad que unifica todos los aspectos de la infraestructura de comunicación de la compañía, desde *backbone* principales de redes híbridas, los servicios y aplicaciones para la colocación de una base sobre la cual la información esté distribuida y almacenada tanto para uso interno como externo.

En el centro de la red corporativa está la capacidad de controlar exactamente ¿qué información es accesible para quién? y ¿cuándo?. Los mecanismos de seguridad juegan un papel importante y como el *Internet Protocol* sigue siendo un método dominante de comunicación (para datos y eventualmente para voz y video), es que el estándar IPSec, continua al servicio habilitando las tecnologías para las redes corporativas.

3.3.1 Introducción a las VPN

Los estándar de IPSec permiten enviar información confidencial segura a través de las redes públicas, por consiguiente, esto da paso a la creación de redes privadas virtuales (VPN). Que son grupos de computadoras unidas sobre el mismo *backbone* principal de la red.

La relación de las VPN con las redes corporativas se describe como una parte importante de la red, que a la vez es independiente. Las redes corporativas requieren de enlaces entre los usuarios o grupos de usuarios que construyen las redes: internets y extranets, las oficinas remotas, los políticas de comunicación o socios.

Aunque la definición anterior no es alentadora, inmediatamente al ver el mercado, este revela que las VPN son vendidas en tantas formas diferentes que es difícil elegir la más precisa.

En efecto, las compañías ven a las VPNs como la solución a las necesidades de sus redes corporativas; necesidades que pueden encontrarse en ellas mismas confrontándolas con VPN y cómo ésta trabaja.

Sin embargo, se mantiene el enfoque sobre la tecnología de la seguridad, que sirve como un habilitador para las VPNs que son la infraestructura de la red corporativa.

Uno de los principales motivos detrás de la creación de redes corporativas es la reducción del costo. Las líneas dedicadas, especialmente en redes de comunicación internacionales, tienen un costo excesivo por lo tanto inapropiado para servir como *backbone* principal de red para la red corporativa, especialmente considerando la naturaleza mundial de los negocios.

Para el usuario han surgido dos modelos principales de comunicación en el mercado informal: las redes externas *Frame Relay* y las redes basadas en VPN.

Opción 1, ***Frame Relay***: La tentación de un servicio proveído por el *Frame Relay* es muy fuerte ya que es más barato que las líneas dedicadas y además agregando a la novedad del *Frame Relay*, la noción de ser un circuito cerrado y seguro. Proveedores como Sprint, British Telecom, Deutsche Telecom y AT&T, ofrecen un número de opciones diferentes de *Frame Relay* que proporcionan un enlace internacional de información a una gran lista de características y aplicaciones de apoyo.

El valor aparente del *Frame Relay* parece difícil de superar, sin embargo, se revela que las intranet externas sobre el *Frame Relay* no pueden hacerlo todo al final de cuentas.

La primera desventaja se argumenta al decir que una red con *Frame Relaly* es segura. Aún en un circuito totalmente privado existen problemas de seguridad, pues un circuito de *Frame Relay* es suministrado por una tercera parte; el *backbone* sobre el cual se encuentra la red puede ser cerrado y el usuario no tiene garantía que los proveedores en la red tengan suficientemente protegidos todos los aspectos de la red. El acceso a través del discado a un conductor de la red de *Frame Relay* es un problema de seguridad, la unión del punto de discado hasta los conductores del *backbone* es vulnerable.

En efecto los proveedores y conductores reconocen que la red del *Frame Relay* requiere de medidas de protección para los datos. La solución está basada en un túnel de acuerdo con un borrador de IETF llamado *Layer Two Tunneling Protocol* (L2PT).

Aún con la implementación de L2PT, de cualquier modo, el fluido de datos a través de una intranet corporativa de *Frame Relay* no es seguro. Simplemente colocar L2TP no hace la red segura. Este es un protocolo de túnel cuyo propósito es permitir a los usuarios remotos conectarse a sus redes privadas.

La lista principal de procedimientos de protección de datos no ha sido incluida en L2PT, sin embargo incluye los siguientes elementos básicos:

1. L2TP no encripta los datos, pero se desea que PPP de Microsoft incluya la forma confidencial dentro del borrador de L2TP como un suministrador de encripción. Sin embargo, cuando el autor de borrador de internet dijo que "*PPP encryption*", ellos se referían a los paquetes PPP que contienen paquetes TCP/IP, IPX *o NetBeui* encriptados, pero no a la "encapsulación" de datos. De esta manera L2TP con PPP no ofrecen encripción por lo que un servicio adicional deberá ser requerido.

2. La autenticación proveída por L2TP es solamente para la fase inicial, a lo largo de la línea de *SecureID* o *Radius*. Esto significa que después que el túnel ha sido establecido, no puede ser pirateado por un usuario no autenticado. La sesión en sí no está autenticada.

3. La autenticación en L2TP es en una sola dirección. El servidor identifica al usuario, pero el usuario no identifica al servidor. Además L2TP no provee la *key management*. Si se desean dos maneras de autenticación, los lados deben tener un acuerdo para compartir sus claves secretas, de esta manera, prevenir los efectos de la escalabilidad.

4. L2TP no soporta una autenticación fuerte, tal como la llave pública de encripción o certificados de autenticación. Es vulnerable a los ataques a mitad de la red.

5. L2TP no provee protección en los reenvíos. *Hackers*, pueden accesar una red corporativa de *Frame Relay*, por el reenvío en una sesión autenticada.

Los puntos terminales del túnel pueden autenticarse durante su establecimiento. Esta autenticación tiene los mismos atributos de seguridad como un CHAP y tiene protección razonable en contra de reenvíos durante el proceso del establecimiento del túnel. Este mecanismo no es diseñado para proveer algún tipo de autenticación más allá del establecimiento del túnel es simplemente para usuarios maliciosos quienes pueden entrometerse e introducir paquetes piratas al túnel ya autenticado.

La equidad informativa es aquella en el que el borrador reconoce las vulnerabilidades del *Frame Relay* que están descubiertas. Finalmente el borrador de L2TP, considera que es la mejor solución de seguridad para transmitir información. Para túneles de L2TP sobre IP, IPSec provee una fuerte protección. Este no requiere modificaciones para usar el protocolo L2TP e influye en el IETF para esta área.

Esto último es más relevante pues IPSec es un activador de tecnología. Se sugiere que si una compañía quiere proteger el tráfico de IP sobre el *Frame Relay*, se implemente IPSec y además el L2TP. Esto dice que *Frame Relay*, tiene un costo efectivo en relación con otros protocolos y un *backbone* confiable para una gran red.

Opción 2, La INTERNET: Durante los últimos años, Internet a tomado una posición importante, en el mundo. Internet sirve como un medio efectivo para un intercambio global de información. El acceso básico a Internet está disponible casi en todos lados. Considerando el bajo costo de acceso a Internet es fácil darse cuenta porque los negociadores eligen esta alternativa a la de las líneas dedicadas.

Los riesgos en la seguridad de Internet ha recibido mucha atención en los últimos años pero con la "estandarización" de IPSec y el avance tecnológico de otros tipos de seguridad, es ahora posible el uso de Internet para una LAN enlazada a otra LAN sin arriesgar la confidencialidad de la información. Además, con los servicios agrupados de llamadas locales ISP y de soluciones de software para el cliente, los usuarios de la red pueden acceder su red corporativa vía su intranet segura, sin requerir la compañía del mantenimiento de los *modems* o pagos fuertes de cuentas.

El mercado dominó rápidamente los costos y los redujo para las internet VPNs y durante los últimos dos años el tema ha sido cubierto mundialmente en los negocios y en el medio profesional. Internet VPNs ha llamado tanto la atención que ha atraído a los grandes vendedores y capitales, esto dió como resultado el dirigir la dirección de la inversión de fondos que se volvió rápidamente en un producto desarrollado.

El mercado de VPN ha comenzado a avanzar. La evaluación de los reclamos del mercado ha motivado a mejoramientos en las VPN. El resultado ha sido IPSec como un estándar de seguridad interoperable. La industria también se dio cuenta que la seguridad en el acceso remoto sobre internet es un concepto prometedor pero este debe ser incorporado a la seguridad general de la red como una estrategia efectiva. La experiencia a enseñado a través de los programas pilotos de VPN que internet aún no es capaz de coordinar una red corporativa. Aún con los miles de cables que han sido tendidos y los cables de banda ancha que han sido agregados, Internet aún no provee la cantidad de servicio, confiabilidad y rapidez de otros *backbones* de IP.

Esto se traduce en una prevención sobre el uso de internet para unos servicios tales como: el acceso remoto y envío de mensajes. Pero para las tareas fuertes que requieren de recursos fiables es mejor usar otros IP públicos para la red, como el *Frame Relay*. Tal diferencia, hace pensar que no solo es una práctica necesaria, sino una buena política que mejora el rendimiento.

En conclusión, de acuerdo a las dos opciones descritas los defectos de la seguridad en *Frame Relay*, su rendimiento y los problemas de confiabilidad en los puntos y el atraso en la lógica son papeles que han surgido en las redes corporativas y han preocupado a los usuarios. Sin embargo, ahora IPSec ofrece un rango completo de funciones de seguridad.

Además esto es totalmente transparente para el usuario; la protección de los datos que viajan sin requerir la intervención de usuarios, incluso en la especificación de que datos son enviados encriptados y cuales no.

También, IPSec opera en la tercera capa del paquete de IP. Las redes son independientes y de esta manera, apropiadas para cualquier *backbone* público: INTERNET, *Frame Relay*, ATM, X.25, ISDN, y aún líneas dedicadas. Las IPSec también son independientes. Estas soportan todos los servicios de IP: email, http, ftp, udp, snmp, etc.

Considerando el alcance de las redes corporativas y las aplicaciones que son requeridas para transmitir, IPSec no solo hace posible las redes corporativas, sino también el uso de tales redes compatibles con los rápidos avances tecnológicos y necesidades que tienen y que tendrán.

En efecto, al acercarse a las VPNs, lo mejor es recordar que las VPNs son tecnología, y no una forma específica de *backbone*. Estas no son Internet o *Frame Relay*, y estas protegen las nuevas maneras de pensar que permiten aprovechar el poder de la información para el mejoramiento de las prácticas de negocio.

3.3.2 Ventajas de IPSec

- Incrementa la productividad y eficiencia del empleado a través de la creación de intranets corporativas que son seguras, con un costo adecuado y accesible en todo el mundo.
- Reduce el desarrollo y los costos de operación a través de extranets con las industrias comerciales.

- Reduce el costo del acceso remoto a través del uso de internet con la ayuda de los *modems* y de los números 1-800.
- Aumento de la protección de los datos y la implementación efectiva de la seguridad para las corporaciones que garantizan las transferencias seguras de la información confidencial de la compañía y que controla las operaciones en la red.

3.3.2.1 Costo

Históricamente, las organizaciones han tenido dificultad para balancear entre la protección de la comunicación de sus datos y el alto costo del establecimiento y mantenimiento de esa protección.
Los costos se han clasificado en las siguientes categorías:

- Actualización de *software.*
- Aprendizaje.
- Administración de llaves de criptografía.

Actualización de *software*, porque IPSec brinda seguridad en la red, las aplicaciones están seguras y no necesitan modificaciones en la aplicación. Esta es una gran ventaja ya que elimina la necesidad de estar constantemente actualizando las aplicaciones.

Aprendizaje, ya que IPSec es transparente para el usuario, no requiere que el misma sea capacitado por lo que el costo es eliminado.

Administración de llaves de criptográficas, para brindar seguridad, las llaves criptográficas deben ser cambiadas con regularidad por lo que el administrador de la red debe estar atento para dar el mantenimiento necesario o bien puede hacerse de manera automática con una generación inicial de la llave secreta y la determinación automática de las nuevas llaves. Los costos de hacerse manual se pueden eliminar y tener un máximo de protección que puede ser establecida y mantenida por la misma empresa.

3.3.3 Desventajas

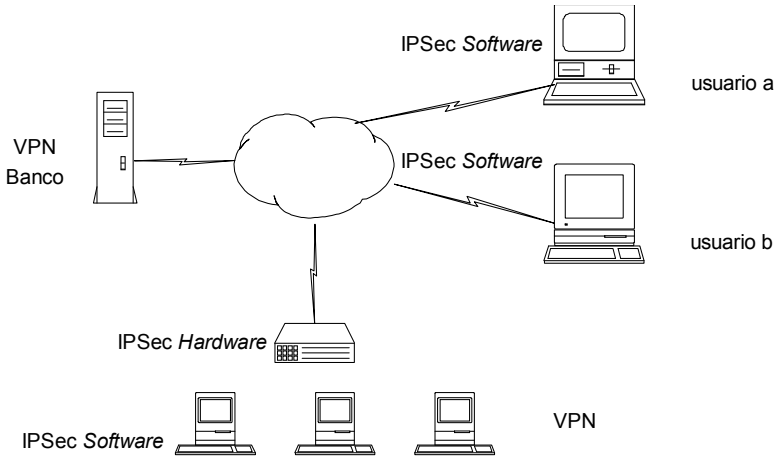
IPSec posee desventajas, sin embargo, se puede tomar un criterio de la conveniencia del uso de IPSec según sean las necesidades que se deban cubrir en una red.

1. Cuando no se cuenta con una VPN se debe instalar *software* en los clientes y esto puede causar conflicto con otras aplicaciones.

2. Se tiene que la colocación de IPSec en una red a través de *hardware* es más barato que con *software* que necesita de UNIX, NT. y que cada central tiene un costo elevado, así como cada cliente.

3. Sobre el tema de la distribución del proceso de IPSec, el producto actual se centra en los *gateway* de seguridad, implementaciones de *firewall*, esto significa que el tiempo consumido por el proceso de seguridad pasará de algún punto central a toda la red. Esto creará embotellamientos en las redes aun en las más rápidas.

Figura 10. Aplicación de IPSec en una red de computadoras



4. Otro punto importante es recordar que los túneles basados en IPSec no soportan multipuntos, existen otros protocolos de túneles de la capa 3 pero no son soportados por IPSec.

3.4 ¿Qué protocolo utilizar?

Una empresa expande su red de computadoras para alcanzar metas de negocio, proveer de acceso remoto a sus trabajadores, nuevas sucursales y negociar con los socios en tiempo real y centralizar las aplicaciones y datos, esta no es una opción a largo plazo sino una necesidad. Cuando una compañía expande su red de trabajo el número de puntos de red crece exponencialmente.

El administrador debe balancear el costo de expansión contra la seguridad, integridad y escalabilidad de la solución. Basados en estos factores, las VPN basadas en IP emergen como la mejor opción para habilitar acceso remotos seguros.

Dependiendo únicamente de las metas y necesidades de la empresa, se selecciona el tipo adecuado de VPN que es un paso difícil. Los tipos más populares de VPN están basados en dos protocolos diferentes: IPSec y SSL.

IPSec para VPN está basado en un conjunto de protocolos de seguridad como se ha mencionado en los capítulos anteriores, operando en la capa de red (capa 3 del modelo OSI). Esto involucra el punto de origen y el del cliente remoto que comunica para construir el túnel seguro encriptado sobre el cual los datos pueden transmitirse de modo seguro. Dentro las empresas que manufacturan el mejor equipo en la actualidad se encuentra *Cisco, Nortel, Checkpoint and Sonic* WALL que incluyen el soporte para IPSec en sus redes.

SSL para VPN está basado en el protocolo común para administrar la seguridad de los datos trasmitidos en Internet. SSL se utiliza con o sin cliente, y usa un programa localizado en una capa entre el protocolo de internet HTTP (*Hypertext transfer protocol*) y el protocolo TCP (*Transport Control Protocol*) en la capa de comunicación. SSL es soportado por los *browsers* de Microsoft y Netscape, para productos de los servidores web.

Áreas que deben tomarse en cuenta para escoger el protocolo de conveniencia:

3.4.1 Seguridad

Con la tecnología VPN, los datos viajan a través de redes con infraestructura pública (internet). Como ya se ha mencionado la información puede ser vista, interceptada y reproducida por usuarios no autorizados si no se toman las medidas de seguridad. Además que se pueden conectar más estaciones de trabajos en las VPN para fines maliciosos por *hackers*. En le capítulo 2 se mencionó que IPSec brinda dos tipos de servicios de seguridad: *Authentication Header* (AH), la cual habilita la autenticación del usuario final, y *Encapsulating security payload* (ESP), la cual soporta autenticación del usuario final y encripción de datos. Por aparte los protocolos para el intercambio de llave como el protocolo ISAKMP/Oakley pueden ser seleccionados. IPSec también facilita la autenticación en ambas direcciones usando uno de los algoritmos más fuertes de encripción como lo es el TripleDES (3DES).

En el otro bando está SSL, que utiliza una llave pública y una privada para la encripción del sistema RSA, el cual también incluye el uso de certificados digitales. Como cualquier máquina con enlace al web puede usar el acceso a una VPN basada en SSL, tomando en cuenta que la autenticación en ambos sentidos no está disponible. Alguien con el *username* correcto y el *password* puede acceder el VPN basado en SSL de cualquier pc conectada al internet.

Conclusión: Las VPN basadas en IPSec ofrecen una mejor autenticación del usuario final y encripción de los datos en la capa de red, haciéndola mucho más seguras que la solución VPN basada en SSL.

3.4.2 Costo total de propiedad (*Total cost of ownership*)

Los costos de propiedad para una solución VPN consisten en: costo de equipo, costo de desarrollo y costo del soporte de la puesta en marcha.

3.4.2.1 Costo del equipo

Para el servidor: Ambas soluciones para VPN IPSec y SSL necesitan un dispositivo final localizado en el centro corporativo de datos para finalizar todos los túneles VPN.

En el caso de la solución IPSec ésta será un *router*/concentrador de la compañía Cisco, Nortel o Checkpoint. Con SSL, será un servidor con el *software* instalado por el proveedor del SSL para la VPN.

Para el sitio remoto: Con la solución IPSec se necesita un cliente VPN (ya sea *software* o *hardware*), para establecer y mantener la conexión VPN. Hay bastante *software* para el cliente gratis disponible con la compra de un dispositivo terminal, mientras que el *hardware* para el cliente tiene un costo entre $500.00 y $1000.00 por punto dependiendo de la empresa y características solicitadas. Con más soluciones SSL para VPN, no hay sitios remotos por lo tanto no existen costos asociados.

3.4.2.2 Costo de desarrollo

En el servidor: La configuración del sitio del servidor para IPSec es mucho más sencilla porque el dispositivo tiene un constructor GUIs para facilitar el proceso. También, la conexión segura es una aplicación independiente, lo cual significa que inmediatamente la conexión es establecida, todas las aplicaciones pueden ser accesadas y operadas desde cualquier punto de la red. No así para el servidor de SSL. Pues cada aplicación debe estar configurada individualmente para trabajar con el sitio del *host* SSL. Esto requiere un gran esfuerzo por lo que se traduce en un significativo alto costo. Por lo tanto desarrollar un sitio para el servidor con SSL puede ser más costoso y consumir mayor tiempo que desarrollar un sitio en el servidor con IPSec.

En el sitio remoto: IPSec requiere una pequeña cantidad de configuraciones iniciales en el cliente VPN, que tiene un pequeño costo. Con la solución SSL el cliente VPN no requiere configuración.

3.4.2.3 Costo del soporte

En el sitio del servidor: Desde *head-end devices*, para ambas soluciones IPSec y SSL para VPN tienden a la estabilidad, el sitio en el *host* mantiene los costos mínimos. Los contratos de reemplazo del hardware son precios comparativos y cubren más *upgrade* de *software/firmware*. El único costo que se menciona para SSL es el que se aplica cuando se desarrolla una nueva aplicación fuera de la configuración para trabajar con SSL. Mientras que para IPSec las aplicaciones son independientes.

En el sitio remoto: Los sitios remotos IPSec y usuarios necesitan soporte. Esto incrementa los costos de entrenamiento y soporte de la mesa de ayuda de la empresa. Las VPN's SSL no incluyen a clientes remotos, de tal forma que no hay costos asociados

Conclusión: Redes Virtuales (VPN's) SSL sin cliente. Aunque los costos de un sitio en el servidor son tan grandes como las redes virtuales IPSec, las VPN con SSL están surgiendo en esta categoría, ya que no existen costos de equipo remoto en el sitio de configuración o de soporte.

3.4.3 Interoperabilidad

No siempre se puede tener el control sobre el ambiente de las redes, especialmente si esto involucra varios negocios con distintos socios, proveedores, etc. La interoperabilidad entre los diversos dispositivos de la red y los componentes llega a ser crítico para las soluciones VPN.

IPSec es una solución *standard* para VPN, esto permite una excelente interoperabilidad. Los dispositivos de diferentes vendedores pueden ser configurados para trabajar efectivamente con los otros y crear conexiones seguras en la VPN.

La mayoría de dispositivos finales son difícilmente servidores Linux/Uníx con *software* propietario SSL-habilitado cargado. Tanto como cada vendedor desarrolla su propio *software* propietario, estos dispositivos finales no se pueden comunicar entre sí. De esta forma, las soluciones de red privada virtual SSL de diferentes vendedores tienen muy pobre interoperabilidad. La tecnología SSL VPN aún no posee una interoperabilidad estable y confiable de dispositivo a dispositivo, siempre segura solución VPN en la que los estándares de diferentes vendedores puedan ser desarrollados. Sin embargo, esto puede cambiar en el futuro.

Conclusión: IPSec para VPN, es una solución basada en un *standard* para VPN y permite a los dispositivos y componentes de distintos proveedores trabajar efectivamente unos con otros.

3.4.4 Escalabilidad

Una compañía continuamente agrega nuevas aplicaciones y nuevos usuarios a sus sistemas y red. El dar acceso a los usuarios remotos para las nuevas aplicaciones y datos en una solución VPN, es vital para maximizar los beneficios de las aplicaciones.

Para IPSec las aplicaciones son independientes, tan pronto como una nueva aplicación es agregada al sistema, su acceso a través de la red VPN es habilitada. Sin embargo, agregar nuevos usuarios requiere del desarrollo de *hardware* y *software* adicional en el sitio remoto. Además, algunas configuraciones en los sitios del servidor requieren que se agreguen nuevos usuarios.

SSL requiere ya sea de un *proxy server* o aplicaciones que habiliten el web. Si una aplicación con una misión difícil (como CRM o ERP) es desarrollada, debe ser habilitada por el web o configurada para trabajar con el SSL del *proxy server*. Una cantidad considerable de configuración se necesitará en un punto de la aplicación. Sin embargo, como SSL no necesita un cliente remoto, agregar nuevas localizaciones y usuarios es fácil.

Conclusión: Neutral. IPSec como solución para VPN escala mejor en términos de aplicación. SSL para VPN escala mejor en términos de usuario.

4. ÚLTIMOS AVANCES PARA IPSEC

Los últimos avances en la tecnología de la comunicación están acentuados en la necesidad de la seguridad para Internet. El grupo de trabajo para el protocolo de seguridad de IP (IPSEC), trabaja para el desarrollo de mecanismos de seguridad para los clientes del protocolo IP. Un protocolo de seguridad en la capa de red será desarrollado para brindar seguridad a través de la criptografía, este servicio será flexible para soportar combinaciones de autenticación, integridad, control de acceso y confidencialidad.

El grupo de trabajo de IPSec se restringe a la siguiente información para mejorar la existencia del protocolo de administración de la llave (IKE) y del protocolo de encapsulación:

1. Cambios a IKE para soportar NAT*Firewall* traversal (travesía).
2. Cambio en IKE para soportar SCTP.
3. Nuevas documentaciones para el soporte de AES-CBC, AES-MAC, SHA-2 y del modo rápido EAS para el uso de encripción en *hardware*.
4. Documentación de IKE MIB.
5. Secuencia numérica de extensiones para ESP para el soporte de expansión del espacio de la secuencia numérica.
6. Estandarización de los procedimientos de administración de llave de IKE.

4.1 Últimas metas alcanzadas (2-1)

- Se ha fijado como un borrador de internet el protocolo de seguridad de IP.
- Se ha fijado como un borrador de internet las especificaciones para la administración de la llave de intenert (IKE)
- Se ha propuesto el *Intenet key management protocol* al IESG para considerarlo como un patrón.
- Se ha llevado a cabo las pruebas de interoperabilidad de la *Encapsulation security payload* (ESP) y *Authentication header* (AH).
- Se ha propuesto la revisión del borrador de internet para ESP, AH y la arquitectura para IPSec
- Se ha propuesto la revisión del borrador de internet de la arquitectura de IPSec, ESP, AH a la IESG para que se consideren como patrones.

4.2 Restricciones:

En este momento, IPSec puede ser aplicado a datagramas IP "*unicast*" únicamente ya que el grupo de trabajo de IPSec aún no cuenta con edición de direcciones de las llaves de grupos de distribución, como se ha descrito anteriormente no trabaja con *multicast* o datagramas IP para *broadcast*.

5. APLICACIÓN DE IPSEC EN REDES CORPORATIVAS

5.1 Red de conexión de bancos con proveedores de servicios públicos

Una de las ventajas que ofrecen al consumidor las entidades que prestan servicios públicos, tales como telefonía fija, telefonía celular, energía eléctrica y agua, es el pago de sus servicios en los bancos del sistema nacional. De este modo los consumidores se acercan al banco más cercano para efectuar sus pagos en cualquiera de las ventanillas, donde se les registra el monto de sus pagos, el tipo de servicio que cancelan, fecha en la que se hace la transacción, y cualquier otro dato que sea de utilidad para la empresa que presta el servicio público o mucho mejor aún el usuario se conecta por medio de Internet a su banco y luego el banco de forma segura se conecta con el proveedor de servicio para asegurar la confidencialidad, integridad y autenticidad de la transacción.

El banco almacena la información de los consumidores y luego la envía a la entidad de servicio público. Dependiendo del tipo de servicio que preste el banco puede realizar consultas del historial de pago por consumidor, estado en el que se encuentra clasificada la cuenta del cliente (moroso, al día, etc.). La información en este caso es solicitada a la entidad de servicio público quien es la dueña de tal información.

La vía para la actualización de la información entre los bancos y los proveedores de servicio público se realiza utilizando los enlaces de red que existen entre ellos. Toda la información viaja a través de la red local de los bancos hacia la red pública (INTERNET), para llegar al *host* destino (entidad pública).

En este ejemplo se encuentran conectados a través de enlaces de red tres bancos distintos, con aplicaciones propias, que utilizan plataformas y equipo de computación de acuerdo a su conveniencia con dos entidades que prestan servicio público (servicio de energía eléctrica y agua potable).

El objetivo es la implementación de seguridad al sistema anteriormente descrito, a nivel de red, por lo que se optó por el protocolo de seguridad para IP IPSec ya que se comporta de modo transparente para el usuario final y las aplicaciones con las que trabajan actualmente las distintas organizaciones.

Se ha manejado una diversidad de combinaciones entre equipo de computación y *software*, ya que actualmente cada entidad maneja su información con el equipo y *software* que más se ajusta a sus necesidades. Sin embargo esto no representa ningún obstáculo para comunicar de forma segura a tales entidades y permitirles el intercambio de información haciendo uso de los enlaces de red con los que ya cuentan. Para esto se han configurando túneles seguros que protejan la información desde su origen hasta su destino, sin alteraciones ni fuga de información.

En el diagrama se muestra como interactúan las entidades bancarias con las proveedoras de servicios públicos.

El banco América cuenta con "Solaris 8" como plataforma para sus aplicaciones propias; para la protección de su información la red interna detiene ataques del exterior utilizando un *firewall* con tecnología "Cisco Pix". La información que se envía a través de Internet lo hace utilizando un túnel seguro que se ha creado con IPSec el cual asegura los paquetes que vienen desde el *firewall* del banco hasta el *firewall* de los proveedores de servicios públicos. Aunque un equipo como el *firewall* o cualquier otro equipo de computación envíe paquetes a una velocidad mayor que la que recibe el equipo receptor, se puede configurar para que puedan enviar y recibir paquetes sin problemas, además uno de los servicios que presta IPSec es el *Anti-replay*, el cual evita la recepción de los paquetes más de una vez.

El banco Progreso utiliza como plataforma Linux Advanced Server y "HP-UX", cuenta con un *firewall* tecnología “CheckPoint 1" para proteger su red de ataques externos a través del cual tienen salida al internet. La configuración del túnel seguro se ha hecho para proteger la información que viaja a través del internet, para esto ha sido necesario activar IPSec desde el *firewall* del banco Progreso, hasta el *firewall* de los proveedores de servicios públicos.

Mientras el banco del Sol posee un servidor con "Windows 2000 advanced server", tiene una red interna con la que se comunican las máquinas del banco. En este caso el banco cuenta con un *router* "Motorola", sin embargo, el túnel seguro con IPSec Inicia desde el servidor, el cual tiene instalado Windows 2000 Server que soporta IPSec hasta el *firewall* de cualquiera de las entidades proveedoras de servicios públicos.

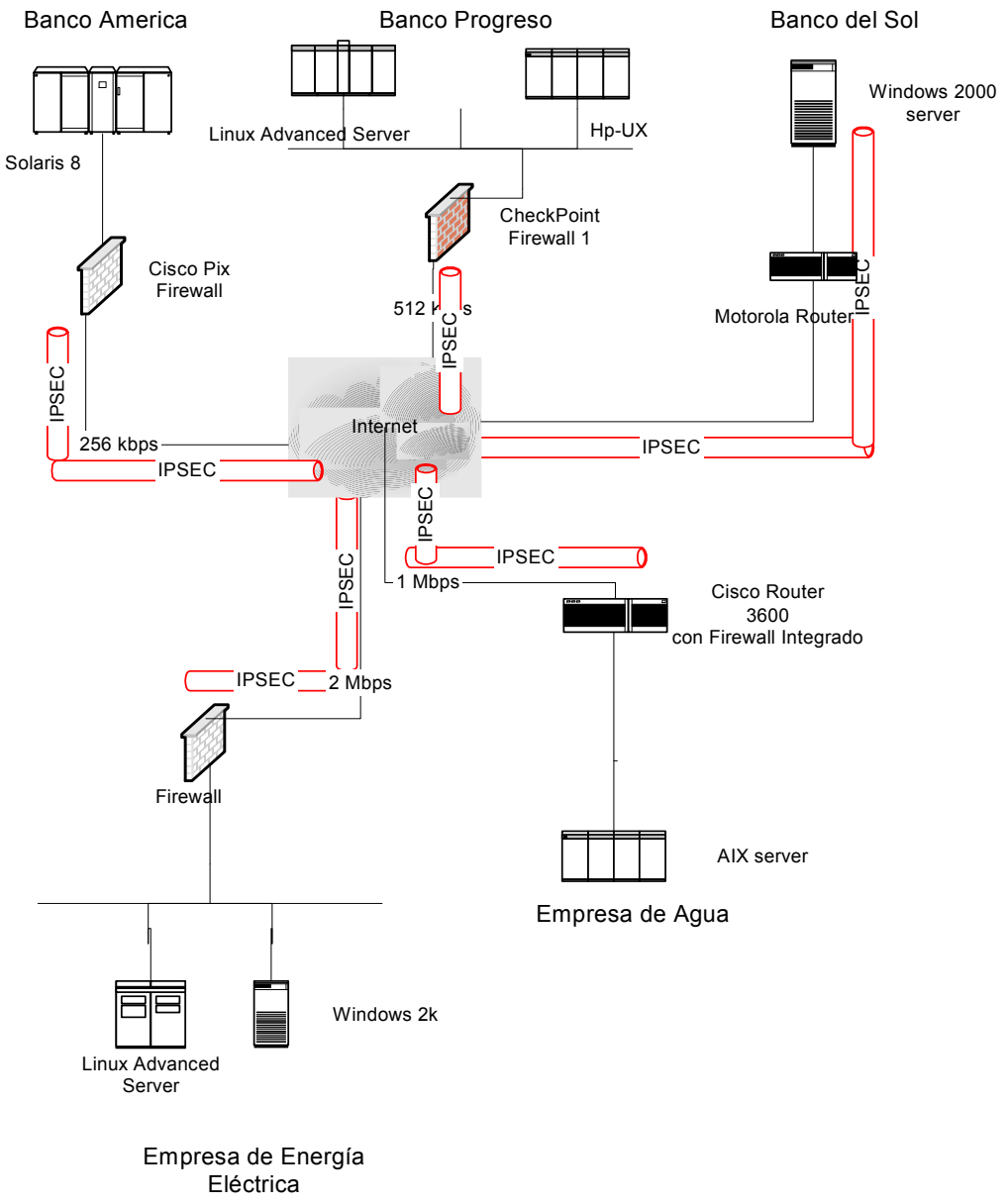
En este punto se muestra la gran ventaja de utilizar IPSec ya que los canales de comunicación son seguros y no importa el número de PC´s que se necesiten comunicar de forma segura, ya que el *firewall* o *router* encriptarán todos los paquetes que se intercambien entre las entidades.

La configuración del túnel desde el servidor del banco del Sol hasta la compañía de energía eléctrica se muestra más adelante.

Por su parte la empresa de servicio de energía eléctrica utiliza equipo de computo con distintas plataformas, estas son "Linux Advanced server" y la otra "Windows 2000". El ingreso y salida de información al exterior de la red interna o intranet se hace a través de un *firewall*.

La empresa de servicio de agua potable utiliza como plataforma "AIX server", también cuenta con la configuración de una intranet, y su salida al internet lo hace a través de un "Cisco router 3600 con firewall integrado", punto hasta el cual llega el túnel IPSec que viene desde cualquiera de los bancos. En el siguiente diagrama de red se muestra la interacción descrita.

Figura 11. Diagrama de red de conexión de bancos con proveedores de servicios públicos



5.1.1 Configuración de IPSEC a través de *hardware*

Este es un caso de acceso completo a VPN con *firewall* y direcciones de internet fijas. (ver apéndice).

Para iniciar con la configuración es necesario tener una interface separada, sin NAT ("*network address traslation*"), para permitir un acceso completo a VPN y también accesar internet, esta separación de interface es conocida como *L2TP Tunnel*, quien la lleva a cabo. Esto puede ser usado cuando una cabecera oficial y un punto remoto oficial tienen una dirección IP fija. La sentencia para salir del túnel de tráfico en una VPN es:

PPP1=IPSEC OVER L2TP>>PPP0

Los pasos a seguir son los siguientes:

1. Configurar L2TP tunnel.
2. Definir un enlace a la internet, IPSEC/L2TP tunnel y dirección IP.
3. Agregar un *router default* para no encriptar el acceso a internet.
4. Agregar un *router* para VPN para el tráfico de PPP1.
5. Definir políticas del *firewall.*
6. Aplicar NAT para el tráfico de los enlaces en internet.
7. Configurar la interface pública para el tráfico L2TP.
8. Configurar SA para IPSEC.

9. Definir las políticas de internet.
10. Definir políticas para encriptar tráfico en las VPN.
11. Configurar las políticas selectivas para definir que tráfico se envía a través del túnel VPN.
12. Habilitar la llave de negociación ISAKMP.
13. Crear el archivo de configuración.

Para realizar el paso 12 se sigue lo siguiente: Cuando existen dos *switch* con distintos protocolos, ISAKMP se encarga de elegir el más conveniente. Ej. DES, en caso que no halla licencia en uno de los *switch* para manejar otro algoritmo de encripción se indica manualmente. Cuando se necesita configurar un nuevo algoritmo de encripción como 3DES no necesita hacer ningún cambio.

Por seguridad debe conectarse una terminal al puerto 0 (cero) para crear la llave de seguridad a través de varios comandos, las llaves pueden ser *random* en un *switch* y luego ingresarlas en el otro manualmente.

Al iniciar la negociación con ISAKMP/IKE del protocolo IPSec con la llave secreta entre los 2 *switch*, el tráfico ISAKMP es protegido por ISAKMP SA.

1. Crear las políticas ISAKMP.
2. Crear las especificaciones SA. El parámetro KEYMANAGEMENT es configurado con ISAKMP.SPI.
3. Crear un *bundle* de especificaciones.
   Con aplicación para ESP y AH.
4. Crear políticas IPSec.
5. Habilitación del proceso IPSec y el proceso de ISAKMP.

Es sumamente importante crear y configurar el archivo para reinicializar el sistema, sin esto todas las llaves serán destruidas al reiniciar el *switch*.

Configuración del *switch* remoto:

Los mismos pasos.

5.1.2 Configuración de IPSEC a través de *software*

Para el caso práctico la plataforma que se utiliza en los puntos para establecer el túnel es “Windows Advanced Server” con un enlace a Internet que permite la comunicación entre las redes.

Para este ejemplo se cuenta con:

- Una red interna del Banco del Sol que se identifica con el IP 172.16.4.0.
- Una red remota para la Empresa Eléctrica (red interna) que se identifica con el IP 192.168.64.0.
- Un enlace que permite la comunicación entre las dos redes Banco del Sol y Empresa Eléctrica a través de Internet.
- Un adaptador de la puerta de enlace de Windows para la red interna Banco del Sol que se identifica con el IP 172.16.4.3.
- Un adaptador de la red externa de la puerta de enlace de Windows 192.168.32.7.
- Un adaptador de la red externa de la puerta de enlace de terceros con la dirección IP 192.168.32.8.
- Un adaptador de la red interna Empresa Eléctrica con la dirección IP 192.168.64.6.

El objetivo es establecer un túnel que permita el tráfico que va de la red del Banco del Sol a la red de Empresa Eléctrica, como también del tráfico que viaja desde la red de Empresa Eléctrica a la red del Banco del Sol de modo que la información se enrute a través de una sesión segura. Pasos para el establecimiento del túnel IPSec:

1. Se debe crear una directiva o política de seguridad IP en el servidor del Banco del Sol. Por *default* la directiva IPSec se crea con la configuración predeterminada para el modo principal de IKE, desactivando la regla de respuesta predeterminada.

2. Crear una lista de filtros de la red Banco del Sol a la red Empresa Eléctrica. Para agregar una lista de filtros dirigirse a la ficha “Lista de Filtros IP”

   - Agregar un filtro especificando su nombre.
   - En la dirección de origen seleccionar "Subred IP específica", escribir la dirección IP y máscara de la subred del Banco del Sol.
   - En la dirección de destino seleccionar "Subred IP específica", escribir la dirección IP y máscara de la subred Empresa Eléctrica.
   - Desactivar la verificación "reflejado".

   En la ficha "protocolo", el tipo de protocolo se establece a "cualquiera" porque los túneles IPSec no admiten filtros específicos de un puerto o de un protocolo. El nombre del filtro se muestra en el “monitor de IPSec” cuando el túnel se activa.

3. Crear una lista de filtros de la red Empresa Eléctrica a la red Banco del Sol. Para esto se sigue la secuencia descrita en el paso dos, además deben tomarse en cuenta las mismas consideraciones descritas en el paso anterior.

4. Configurar una regla para un túnel de la red Banco del Sol a la red Empresa Eléctrica. Para poder configurar la nueva regla del túnel, se selecciona la lista de filtros que se ha creado en la ficha “Lista de filtros IP”.

   - En la pestaña "Configuración del túnel" se selecciona la opción: "El extremo del túnel se especifica mediante esta dirección IP" colocando la dirección IP del adaptador de la red externa de la puerta de enlace de terceros.
   - En la ficha "Tipo de conexión" se selecciona "Todas las conexiones de red".
   - Crear una nueva acción de filtrado ya que las acciones predeterminadas permiten el tráfico entrante sin cifrar.
   - Activar la opción "Negociar la seguridad" (La opción "Confidencialidad directa perfecta" es válida si el otro extremo del túnel también se configura para usar esta opción).
   - Luego de activar la opción anterior se permite agregar algoritmos para ESP, lo mejor es dejar la opción "Alto" seleccionada.
   - Especificar el nombre de la nueva acción de filtrado y grabar.
   - Seleccione la nueva acción de filtrado

En la ficha "Métodos de autenticación" se configura el método que se desee, puede ser clave compartida que es lo menos seguro pero que se utiliza en este caso por ser un ejemplo, también están los certificados de confianza y otros métodos.

5. Configurar una regla para un túnel de la red Empresa Eléctrica a la red Banco del Sol.En las propiedades de la directiva IPSec, se crea una nueva regla:

   Se repite la configuración del paso 4.
   En la ficha "Tipo de conexión", seleccionar "Todas las conexiones de red" (Cualquier tráfico saliente en el tipo de interfaz que coincida con los filtros intenta ser introducida en el túnel hasta el extremo especificado en la regla. El tráfico entrante que no coincida con los filtros se descarta porque debe ser recibido de forma segura por el túnel IPSec.).
   Seleccionar la nueva acción de filtrado que ha creado.
   En la ficha "Métodos de autenticación", configurar el mismo método usado en la primera regla. En ambas reglas debe usarse el mismo método.

   Se debe tener precaución de que ambas reglas creadas, estén habilitadas en la directiva.

6. Se asigna la nueva directiva IPSec a la puerta de enlace de Windows. Este es un paso sencillo pues para asignarla solo se necesita ir al "complemento de MMC", "Equipo local" en "Directivas de seguridad IP" y elegir la opción de "asignar".

   Después de la asignación de la directiva, se cuenta con dos filtros activos adicionales, estos son creados por "RRAS" automáticamente para el tráfico L2TP. Para ver los filtros activos se escribe en el símbolo del sistema el siguiente comando: netdiag/test:ipsec/debug>arch_JB.txt. (Ver apéndice)

7. Configurar el filtrado de RRAS. Esto permite que el tráfico que tenga una dirección de origen o de destino llegue a la red Banco del Sol o a la red Empresa Eléctrica. Para esto se crea en el Banco del Sol un filtro de salida para la interfaz externa, de modo que se descarte todo el tráfico excepto los paquetes de la red Banco del Sol a la red Empresa Eléctrica y otro filtro en Empresa Eléctrica para descartar el tráfico excepto los paquetes de la red Empresa Eléctrica a la red Banco del Sol. También tendrá que permitir el tráfico hacia y desde el Banco del Sol a la red de terceros (*IP3rExt)* para permitir la negociación de IKE cuando se esté creando el túnel:

   Crear un filtro de salida nuevo del Banco del Sol a Empresa Eléctrica.

Crear otro filtro de salida nuevo del Banco del Sol hacia terceros (Colocar la dirección IP hacia terceros y la máscara de subred en el área de red de destino. En este caso la dirección se necesita para realizar la negociación de IKE, por lo que la máscara de subred que debe colocarse debe ser 255.255.255.255 y activar la casilla de verificación "Omitir todos los paquetes que no cumplen el criterio especificado abajo").
Crear un filtro de entrada de Empresa Eléctrica al Banco del Sol (Crear otro filtro de entrada de terceros a Banco del Sol con las mismas especificaciones del filtro de salida hacia terceros).

Si el servidor RRAS tiene más de una interfaz conectada a Internet o si hay varios túneles IPSec, se debe escribir filtros que no sean de RRAS para cada túnel IPSec (cada subred IP de origen y de destino) para todas las interfaces de Internet.

Para solucionar el problema de enviar tráfico por el túnel saliente en la interfaz equivocada se define una ruta estática de forma que se enlace el tráfico a la red Empresa Eléctrica con la interfaz externa correspondiente:

Crear una ruta estática nueva.
Seleccionar la interfaz fija que desea usar para el tráfico de salida en el túnel (en este caso se puede utilizar una IP externa).
Colocar la dirección IP de la red Empresa Eléctrica y la máscara de red.
Para la "puerta de enlace" se coloca el nombre del adaptador hacia terceros y establecer en el valor predeterminado uno (1) en "Métrica".

Para probar el túnel, se hace “ping” desde un equipo del Banco del Sol a un equipo de la Red Empresa Eléctrica o viceversa. Si se ha creado los filtros correctamente y se les ha asignado la directiva correcta, las dos puertas de enlace establecen un túnel IPSec de forma que pueden enviar el tráfico ICMP desde el comando “ping**”** en formato cifrado. Se puede hacer uso de varias herramientas que provee *Windows Advanced Server*, por ejemplo:

Habilitar la “Auditoria de los sucesos de inicio de sesión y el acceso a objetos”: Esta herramienta registra los sucesos en la bitácora de seguridad, tomando como base la información de los intentos de una negociación IKE y si tuvo éxito o no.

Monitor de seguridad IP, para cargar esta herramienta ejecute el "ipsecmon". Dicha herramienta muestra estadísticas de IPSec y las asociaciones de seguridad activas. Si se utiliza el comando "ping" para intentar establecer el túnel , se puede observar una asociación de seguridad solo si la creación del túnel ha sido correcta, de lo contrario el tráfico ICMP no se ha protegido con IPSec.

Monitor de red, se utiliza para capturar el tráfico que pase a través de la interfaz de IP externa mientras intenta hacer “ping” al equipo. Si puede ver paquetes ICMP en la captura con direcciones IP de origen y de destino, IPSec no está protegiendo el tráfico.

Si no ve este tráfico ICMP pero, en su lugar, ve paquetes ISAKMP y ESP, IPSec está protegiendo el tráfico. Los paquetes de ISAKMP indican que la negociación de IKE real está teniendo lugar mientras que los paquetes de ESP son los datos de carga cifrados por el protocolo IPSec.

CONCLUSIÓN

1. El paso de información en la red pública es una actividad delicada; en la actualidad existen empresas virtuales que han causado un gran impacto en Internet por el volumen de información que procesan, lo que se traduce en una fuerte cantidad de transacciones electrónicas que constituyen el punto de vista de interés ya que la información que viaja a través de la red es tan valiosa que la comunicación debe ser segura.

2. El Protocolo de seguridad para IP "IPSec" trabaja a nivel de la capa de red protegiendo la información de ataques de terceros, proporcionando una gran ventaja para su utilización inmediata ya que las aplicaciones con las que cuentan actualmente los sistemas no necesitan ningún tipo de adaptación para continuar operando a través de la red por ser totalmente transparente para tales aplicaciones.

3. Reducción de costos importantes en la generación de aplicaciones seguras debido a que no se necesita mayor inversión en las áreas de programación de las aplicaciones, capacitación de personal, cambio de equipo de hardware, etc.

4. La mayoría de las redes de computadoras no manejan el protocolo IPSec, sin embargo, la tendencia es que este protocolo se convierta en un estándar de seguridad para asegurar (garantizar) las comunicaciones en general, que se realicen en la capa de red. Muestra del esfuerzo por la comunicación segura es que la versión Ipv4 no cuenta IPSec, sin embargo, la versión Ipv6 ya maneja este protocolo.

   Para utilizar el protocolo de seguridad IPSec debe tomarse en cuenta que deben configurarse ambos puntos del túnel que permitan el paso de información segura, esto implica que los puntos que deseen conectarse deben contar con la configuración del protocolo.

5. Para trabajar con IPSec es necesario que la máquina receptora y la máquina que envía paquetes a través de la red cuenten con la configuración de IPSec, esto incluye la configuración de las cabeceras AH y ESP, el establecimiento de las políticas SA que norman la comunicación entre las máquinas, siempre dentro del marco de trabajo ISAKMP el cual define la negociación de las llaves entre los puntos de red que se comunican.

RECOMENDACIONES

1. Debido a la versatilidad y expansión a nivel local y mundial de Internet, las organizaciones transnacionales, empresas nacionales y usuarios en general han encontrado en este medio, un canal de comunicación entre dos puntos de red permitiéndoles el acceso a información actualizada en cualquier momento además de contar con la facilidad y comodidad de realizar transacciones financieras, compras a proveedores que se encuentran a miles de kilómetros o simplemente un medio más de ventas.

   Sin embargo se tiene claro que su creación fue con fines de investigación por lo que cada usuario de INTERNET debe estar conciente de lo expuesta que está su información en la red pues no se cuenta con mecanismos de seguridad intrínsecos, como tampoco se garantiza que los datos no hallan sufrido manipulación u otro ataque durante su paso a través de este medio. Por tal razón se vuelve necesario el uso de tecnología que permita resguardar todo tipo de información sensible (cuentas bancarias, números de tarjeta de crédito, información de clientes, etc.), minimizando así el riesgo de plagio y manipulación de información.

2. Para las redes privadas virtuales VPN que utilizan enlaces de red vía Internet, es elemental la construcción de túneles encriptados basados en IPSec, para proteger su información. Ésta solución garantiza una comunicación segura en un medio público, libre de ataques. Su implementación puede ser a través de *software* o *hardware* de su conveniencia.

3. Sin embargo, si lo que se necesita es que cientos o miles de usuarios que no se conocen, accedan de forma segura a una aplicación en Internet y no se pueda implementar IPSec por el inconveniente que se tiene que instalar *software* y/o *hardware* de VPN del lado del cliente y el servidor, el mejor camino será instalar un certificado digital autorizado por una entidad internacional en el servidor que contiene la aplicación y que los clientes accedan a la misma por medio de una conexión SSL (https) a través de un *browser* a la dirección "url" determinada.

El uso de túneles encriptados basados en IPSec convierten a Internet en un medio seguro para el paso de paquetes de información pues con ello obtenemos confidencialidad a través de la *encripción* asegurando que los datos no han sido leídos en el camino, *autenticación* de los datos de origen ya que el IPSec receptor puede autenticar el fuente de los paquetes enviados, *integridad* garantizando que el paquete no ha sido alterado durante su trayectoria a través de la red y *"anti-replay"* pues IPSec puede detectar y rechazar paquetes reenviados.

REFERENCIAS

1. Tenenbaum, Andrew S. Redes de computadoras. 3ª. Ed. México: Ed. Prentice mayo, 1997

2. IP security protocol (IPSEC). http: //www.ietf.org/html.charters/ipsec-charter.html. Consultado en junio de 2003

BIBLIOGRAFÍA

1.O'Relffy & Associates, Inc. **The whole Internet: User's guide & catalog**. USA: Ed. Krol, 1994. p.m. 45-60

2.Acevedo García, Oscar Guillermo. La importancia del uso de mecanismos de seguridad en internet. Tesis del ingeniero en informática y sistemas. Guatemala, URL, Ingeniería, 1996

3.Tenenbaum, Andrew S. **Redes de computadoras.** 3ª ed. México. Ed. Prentice mayo, 1997. pp. 46,437,446,448

4.**13.0-Using IPSec(ip security protocol)**. http://www.openbsd.org/faq/faq13.html. Consultado en abril de 2003

5.**Chapter 29 IP Security (IPSec)**. http://www.alliedtelesyn.co.n2/documentation/switchblade/241/pdf/ipsec.pdf. Consultado en abril de 2003

6.**Chapter 34 IP security (IPSec)**. http://www.alliedtelesyn.co.n2/support/rapier/rapier221/switch.pdf. Consultado en abril de 2003

7. **Comercio electrónico**.
http://www.iec.csic.es/criptonomicon/comercio/ssl.html.
Consultado en mayo de 2003

8. **Configuring IPSec network security**.
http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/
113/113t-3/ipsec-htm. Consultado en junio de 2003

9. **Documentos internet draft**.
http://www.ietf.org/html.charters/ipsec-charte.html. Consultado en
junio de 2003

10. **Encuentran fallos de seguridad en el protocolo SSL**.
http://www.delitosinformaticos.com/seguridad/noticias/1046034/
6644475.shtml. Consultado en junio de 2003

11. **Future work in IPSec**.
http://www.usenix.org/events/usenix99/full-paper/deraadt/
deraadt-html/node10.html. Consultado en junio de 2003

12. **How to use Photuris with IPSEC?**.
http://www.citi.umich.edu/u/provos/photuris/howtouse.html.
Consultado en julio de 2003

13. **IEEE.** http://www.ieee.org/portal/index.asp. Consultado en julio de 2003

14. **Introduction to SSL**.
http://www.developer.netscape.can/doxs/manuals/security/sslin/contents.htm. Consultado en agosto de 2003

15. **IP security for Microsoft Windows 2000 Server**.
http://www.microsoft.com/windows2000/techinfo/howitworks/security/ip-security.asp. Consultado en agosto de 2003

16. **Ip Security for Microsoft Windows 2000 server**.
http://www.microsoft.com/windows2000/docs/ip_security.doc. Consultado en septiembre de 2003

17. **Ip security for Microsoft Windows 2000 Server**.
http://www.microsoft.com/windows2000/techinfo/howitworks/security/ip_security.asp. Consultado en septiembre de 2003

18. **IPSec.DK.** http://www.ipsec.dk. Consultado en octubre de 2003

19. **IpSec-IP security protocol**.
http://www.cs.technion.ac.il/labs/Projects/spring98/ipsec/netLab/pres/sld007.htm. Consultado en octubre de 2003

20. **IPSec Technet**.
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/itsolutions/network/maintain/security/ipsecarc.asp. Consultado en octubre de 2003

21. **IPV6.** http://www.ipv6.org. Consultado en octubre de 2003

22. **IRTF.** http://www.irtf.org/irtf. Consultado en noviembre de 2003

23. **NetBSD documentation: NetbSD IPSEC.** http://www.netbsd.org/Documentation/Network/ipsec. Consultado en enero de 2004

24. **Securing Windows 2000 Communications with IP security filters, Part One.** http://www.microsoft.com/windows2000/technologies/communications/ipsec/default.asp. Consultado en febrero de 2004

25. **SSL.** http://www.webopedia.com/term/s/ssl.html. Consultado en abril de 2004

APÉNDICE

Para configurar ISAKMP se presenta el siguiente ejemplo, que hace alguna modificación al archivo de políticas que contenga:

```
KeyNote-Version: 2
Comment: Esta política acepta SAs de ESP de un nodo remoto que
         usa una clave o password
Authorizer: "POLICY"
Licensees: "passphrase:mekmitasdigoat"
Conditions: app_domain == "IPsec policy" &&
          esp_present == "yes" -> "true";
```

La implementación dará como resultado un túnel VPN usando solo ESP sobre un servidor A, con una dirección IP 249.2.2.2 externa.

```
[General]
Retransmits=     5
Exchange-max-time=120
Listen-on=              249.2.2.2
```

De forma similar para ISAKMP en el servidor B 249.3.3.3 que representa el IP externo para este servidor.

Este es el lugar donde se puede configurar las variables que afectarán principalmente el comportamiento de ISAKMP.

El Listen-on especifica el valor IP que Isakmp debería escuchar, solo es necesario el IP de internet del *gateway*.

Ahora para el servidor A se edita el ISAKMP.

[Fase 1]

249.3.3.3= HostB

Para el servidor B:

[Fase 1]

249.2.2.2= HostA

Con lo anterior se describen las direcciones IP que son aceptadas en el orden en que se negociaron en la fase 1 de conexión. Hay que recordar que la fase 1 solamente autentica el punto remoto para asegurarse que hay quien conteste. Luego, en el servidor A:

[Fase 2]

Connections= HostA-HostB

en el servidor B:

[Fase 2]

Connections= HostB-HostA

Esto describe la conexión para la fase 2, esta fase es la que determina que protocolo de ambos puntos usará para la comunicación.

En el parámetro connections se iguala a una etiqueta, si el servidor remoto no tiene una dirección IP, puede especificarse entonces una como *default* a la cual harán referencia aún cuando no aparezca en la lista de Connections = etiqueta.

En el servidor A:

[HostB]

Phase= 1

Transport= tcp

Local-address= 249.2.2.2

Address= 249.3.3.3

Configuration= Default-main-mode

Authentication= mekmitasdigoat

#Flags=

En el servidor B: Configurar el [HostA].

Descripción de las variables anteriores:

Phase = 1, es necesario porque el código ISAKMP usa los mismos procedimientos de la fase 1 y fase 2.

Transport, da distintas posibilidades para los distintos puntos.

Local-address, es la dirección destino que vienen en los paquetes que envían los puntos. Se tienen casos en los que hay varias interfases escuchando para las conexiones de la fase 1, pero en este ejemplo solo hay una interfase escuchando para la fase 1, por lo tanto este es el IP de la interfase que esta escuchando en este punto.

Address, es la dirección IP de donde viene el paquete.

Configuration, aquí como ejemplo se utilizo por *default* un modo especificado en el archivo.

Autenticación, es la "frase compartida" para ser usada para este punto en particular. Esta frase obtiene el paso a las políticas para verificar si el punto tiene permiso para el uso de IPSec dentro del servidor. Si se cambia la frase debe también hacerse el cambio del archivo de políticas porque el archivo está diseñado para actuar con esta frase.

En el servidor A:

[HostA-HostB]

Phase=	2
ISAKMP-peer=	HostB
Configuration=	Default-quick-mode
Local-ID=	Net-A
Remote-ID=	Net-B

En Host B: las mismas especificaciones para el servidor A.

Ambos servidores tienen una configuración individual que ISAKMP debe usar para hablar entre los dos *gateways* para una conexión particular. La variable phase 2 es necesario porque el código ISAKMP usa las mismas funciones para autenticar la fase 1 y 2. Esto es obligatorio para trabajar en las VPN.

ISAKMP-Peer: es el nombre del *host*. Significa que se puede hablar a un punto en particular para establecer una conexión fase 2.

Configurations: Describe los estándar o patrones que el servidor y el punto particular en la conexión deben soportar.

Local-ID : Es la posición que ha pasado para que el otro *gateway* pueda configurar la tabla de rutas apropiada que hace la trasferencia de datos sobre la red VPN.

REMOTE-ID: Permite configurar adecuadamente la tabla de rutas para la trasferencia de datos de la red privada VPN a una red privada remota VPN.

Ahora la sección IPSec-ID, para esto la información que se coloca debe existir en el archivo isakmp.conf tanto para el servidor A como para el B. El ejemplo configura el servidor A como 192.168.1.0/255.255.255.0, el cual fue conectado a la red A y el servidor B 192.168.20.0/255.255.255.0 sobre la red B.

```
[Net-A]
ID-type=        IPV4_ADDR_SUBNET
Network=        192.168.1.0
Netmask=        255.255.255.0

[Net-B]
ID-type=        IPV4_ADDR_SUBNET
Network=        192.168.20.0
Netmask=        255.255.255.0
```

Se cuenta con dos secciones que hacen referencia a los identificadores Local-ID y Remote-ID. Estos describen las rutas que deberían configurarse para permitir el tráfico de una red privada a otra.

ID-type: puede configurarse dependiendo de lo que soporte la implementación.

Ahora en ambos servidores el archivo de ejemplo debería leerse así:

```
[Default-main-mode]
DOI=                    IPSEC
EXCHANGE_TYPE=          ID_PROT
Transforms=             3DES-SHA
```

En esta sección se describe lo que se necesita para los métodos de encripción en la fase 1. Hasta este momento iniciamos con el dominio de nuestro interés IPSec.

La variable EXCHANGE_TYPE está colocada como ID_PROT, la que identifica los protocolos que son reconocidos por la autenticación.

Transforms : es la transformación requerida o asignada para el cambio, en este caso en el siguiente bloque tenemos la configuración del archivo en el que se establece que se está recibiendo un paquete encriptado con 3DES y el checksum esta siendo verificado con SHA.

```
[Default-quick-mode]
DOI=                    IPSEC
EXCHANGE_TYPE=          QUICK_MODE
Suites=                 QM-ESP-3DES-SHA-PFS-SUITE,QM-ESP-
                        DES-MD5-PFS-SUITE
```

Este nuevo bloque menciona los requerimientos para la encripción de los datos que son enviados a través de una VPN.

Suites: Puntos para IPsec que describe los distintos esquemas disponibles de encripción ente los dos servidores.

Esta es la configuración mínima para crear una simple pero sólida VPN.

CONFIGURACIÓN A TRAVÉS DE *HARDWARE*

CASO 1: IPSec con administración manual de llaves.

1. Ingreso de llave secreta: Se necesita 2 llaves, una para encripción DES y una para HMAC MD5. Los valores en los *switch* para las llaves deben ser los mismos.
2. Crear las especificaciones SA: Parámetro que debe ser configurado a manual, especificar SPI, el *inbound*, *outbound*, configurar la variable *keymanagement*.
3. Crear un *bundle* de especificaciones con aplicación para ESP y AH.
4. Crear políticas IPSec.
5. Habilitación del proceso IPSec.

Configuración del *switch* remoto:

1. Ingreso de llave secreta.
2. Crear SA.
3. Crear un *bundle* de especificaciones, con aplicación para ESP y AH.
4. Crear políticas IPSec.
5. Habilitación del proceso IPSec.

CASO 3: IPSEC con túnel encriptado.

-Requiere de *software* con versión 1.8.1 ó más reciente.
-En encripción "MiniAcelerator Card" (EMAC).
-Puede requerir licencia de características IPSEC ISAKMP.

1. Definir una seguridad oficial. Los comandos deben ser ingresados en orden para definir una seguridad oficial. Debe definirse un usuario.
2. Generar una llave *random* en la cabecera oficial del *switch*. El valor de la llave será usado para las negociaciones de encripción ISAKMP.
3. Se configuran las variaciones de los casos anteriores.

CASO 3.1: Acceso completo a VPN con direcciones fijas de internet.

Configurar la cabecera oficial del *switch*.

1. Configure el nombre del *switch*
   Ej.: SET SYSNAME: "HEAD OFFICE ipsec"
2. Agregar la seguridad que será oficial y configurar un *timeout* .
3. Haga el enlace para internet y seleccione la dirección IP.
4. Configurar las especificaciones SA para IPSec.
5. Definir las políticas.
6. Configurar las políticas para encriptar el tráfico VPN.
7. Configurar las políticas de selección para definir que tráfico será enviado a través del canal VPN.
8. Configurar las políticas para tener acceso desencriptado al resto de la internet.

9. Habilitar ISAKMP para negociaciones.
10. Crear o modificar el archivo de configuración para las inicializaciones.

Ej.

```
CREATE CONF=IPSEC.CFG
SET    CONF=IPSEC.CFG
```

Con estas instrucciones crea el archivo y copia las definiciones.

Configuración del *switch* remoto:

Los mismos pasos.

CASO 3.2: Acceso completo a VPN con asignación dinámica de direcciones de internet

1. Configurar el nombre del *switch.*

   Ej.

   SET SYSNAME: "HEAD OFFICE ipsec"
2. Agregar la seguridad que será oficial y configure un *timeout.*
3. Agregar un usuario que será autenticado por el punto IPSec.
4. Haga el enlace para internet y seleccione la dirección IP.
5. Configurar las especificaciones SA para IPSec.
6. Definir las políticas.
7. Configurar las políticas para encriptar el tráfico VPN.
8. Configurar las políticas de selección para definir que tráfico es enviado a través del canal VPN.
9. Configurar las políticas para tener acceso desencriptado al resto de la internet.
10. Habilitar ISAKMP para negociaciones.
11. Crear o modificar el archivo de configuración para las inicializaciones.

Configuración del *switch* remoto: Los mismos pasos.

En la versión 1.9.1, permite autenticación del punto dinámico.

CASO 3.4: Acceso restringido a las VPN con *firewall* y asignación dinámica de direcciones de internet.

Se usa cuando una oficina remota utiliza un enlace "on-demand" para el internet y asigna direcciones IP a través de un proveedor de servicios de internet (ISP "internet service provider").

Porque las direcciones IP no son conocidas ya que IPSec esta configurado para permitir puntos dinámicos, la oficina de cabecera debe contar una dirección IP fija.

En este caso solo hay una interface pública, la salida de tráfico será a través del proceso NAT antes de pasar por IPSec.

El *firewall* NAT está definido para la cabecera de la oficina y para el *switch* de la oficina remota.

Configuración de la cabecera del *switch* de la oficina.

1. Configurar el nombre del *switch*
2. Agregar la seguridad oficial y configurar un *timeout* automático.
3. Definir un usuario quien autenticará el punto IPSec .
4. Definir el enlace entre las direcciones IP y el internet.
5. Definir las políticas para el *firewall.*
6. Aplicar NAT para el tráfico a PPP1.

7. Definir una regla que permitirá el acceso al trafico ISAKMP.
8. Definir para cual servicio privado local los puntos dinámicos pueden tener acceso.
9. Configurar las especificaciones SA para IPSec.
10. Definir las políticas IPSec.
11. Defina políticas para encriptar tráfico para la oficina remota (que es un punto dinámico).
12. Configure una política de encripción para el tráfico seleccionado .
13. Habilitar ISAKMP "Key negotiation".
14. Crear o modificar el archivo de configuración para cuando se reinicialice la máquina.

Configuración del *switch* remoto:

1. Configurar el nombre del *switch*.
2. Agregar una seguridad oficial y configurar un *timeout* automático.
3. Defina la llamada ISDN.
4. Configurar "on-demand" con acceso PPP a internet, y direcciones IP apropiadas.
5. Definir políticas para el *firewall.*
6. Aplique NAT para el tráfico de PPP1. Los puntos dinámicos inicializan la negociación, por eso no necesitan reglas para ISAKMP (puerto 500), el tráfico inicializado dentro del *firewall* esta permitido por *default*.
7. Configurar las especificaciones SA para IPSEC.
8. Definir las políticas IPSec.
9. Definir una política para encriptar tráfico direccionadas a la cabecera oficial.
10. Encriptar el tráfico enviado a la interface pública en el *firewall* opuesto.

11. Definir una política para habilitar el acceso no encriptado al resto de la internet.
12. Habilitar ISAKMP "Key negotiation".
13. Crear o modificar el archivo de configuración para cuando se reinicialice la máquina.

CASO 3.5: Un túnel IPSEC a través de un dispositivo *gateway* NAT con acceso completo a VPN con direcciones fijas a Internet.

El dispositivo *gateway* NAT debe estar configurado con "eNAT" que permite reglas para recibir del exterior tráfico inicializado con L2TP.

El orden para el tráfico de salida de una VPN es:

Traffic >> PPP1=IPSEC OVER L2TP>>PPP0

Configuración del *switch* de cabecera de la oficina:

1. Definir el nombre del *switch.*
2. Agregar la seguridad oficial y configurar el *timeout.*
3. Configurar el L2TP. Como IPSec esta aplicado a PPP1 y por estar PPP1 en un túnel L2TP, IPSec esta aplicado al tráfico antes que el tráfico sea enviado a través de L2TP túnel.
4. Definir el enlace para internet, IPSEC/L2TP tunnel y las direcciones IP.
5. Agregar una ruta por *default* para accesar a la información no encriptada en internet.
6. Agregar una ruta para la VPN al tráfico PPP1.
7. Definir políticas de *firewall.*
8. Aplicar NAT para el enlace del tráfico de internet.

9. Configurar la interface pública para permitir el tráfico L2TP a través del *firewall.*
10. Configurar las SA para IPSEC.
11. Definir una política IPSec.
12. Definir una política para encriptar tráfico VPN.
13. Configurar una política de selección para definir que tráfico es enviado a través del túnel VPN.
14. Habilitar ISAKMP "Key negotiation".
15. Crear o modificar el archivo de configuración para cuando se reinicialice la máquina.

Configuración del *switch* de la oficina remota:

Los mismos pasos.

Configuración del dispositivo *broadband* (ADSL modem)

El Ej. L2TP esta siendo usado por el túnel IPSec a través del dispositivo *broadband*.

1. Configurar el nombre del aparato (dispositivo).
2. Conectar a una LAN.
3. Definir una interface de internet.
4. Definir un *gateway* para el internet (opcional).
5. Definir direcciones de traslación.
6. Definir una regla permitida.

Verificación del túnel IPSEC

Para confirmar que el tráfico está siendo encriptado puede utilizarse algún comando de conteo como:

SH IPSEC POLI= TEST1 COUNT

Cada vez que haga ping se colocarán 5 ping, las salidas serán incrementadas por 5, también la repetición de tráfico deberá incrementar de 5 en 5.

Además es importante que las políticas de IPSec sean configuradas en el orden correcto.

GENERACIÓN DE ARCHIVO

Archivo denominado "arch_JB.txt" cuenta con la siguiente información:

Gathering IPX configuration information.
Opening \device\NwlnkIpx failed
Querying status of the netcard drivers... passed
Testing domain membership... passed
Gathering NetBT configuration information.
Gathering IP security information

Tests complete.

Computer name: MAQ1X
DNS host name: maq1X
DNS domain name: (null)
System info : Windows 2000 Server (build 2195)
Processor : x86 family 6 model 8 stepping 1, genuineIntel
Hotfixes :
Installed? name
Yes Q147222

Netcard queries test . . . . . : passed

Information of netcard drivers:

Description: paralelo directo
Device: \DEVICE\{9F0E1494-7B36-4EB5-8E99-00EAF715CFD6}
GetStats for 'paralelo directo'.

Description: minipuerto WAN (PPTP)
Device: \DEVICE\{B3A762C6-A4AF-4204-865D-C7BE7DD3C9EA}
GetStats for 'minipuerto WAN (PPTP)'.

Description: minipuerto WAN (IP)
Device: \DEVICE\NDISWANIP

Media state:	connected
Device state:	connected
Connect time:	04:35:10
Media speed:	28 Kbps.
Packets sent:	0
Bytes sent (optional):	0
Packets received:	0
Directed pkts recd (optional):	0
Bytes received (optional):	0
Directed bytes recd (optional):	0

Description: minipuerto WAN (L2TP)
Device: \DEVICE\{D137B25C-7299-4711-99A9-2C97728C588D}

GetStats for 'minipuerto WAN (L2TP)'.

Description: D-Link DFE-680TXD DirectPort CardBus
Device: \DEVICE\{C468A9AB-34AA-45F4-BD07-69E898B464CC}

Media state:	connected
Device state:	connected
Connect time:	04:35:10
Media speed:	10 Mbps
Packets sent:	1002
Bytes sent (optional):	0
Packets received:	2396
Directed pkts recd (optional):	282
Bytes received (optional):	0
Directed bytes recd (optional):	0

[PASS] - At least one netcard is in the 'connected' state.

Per interface results:

Adapter : conexión de área local
Adapter ID . . . . . : {C468A9AB-34AA-45F4-BD07-69E898B464CC}

Netcard queries test . . . : passed

Global results:

Domain membership test . . . . . : passed

Machine is a . . . . . : standalone server

Netbios workgroup name . . . . : GRUPO_TRABAJO

Dns domain name is not specified.

Dns forest name is not specified.

Domain guid. . . . . : {00000000-0000-0000-0000-000000000000}

Logon user . . . . . : administrador

Logon domain . . . . . : MAQ1X

NetBT transports test. . . . . : passed

List of NetBt transports currently configured:

NetBT_Tcpip_{C468A9AB-34AA-45F4-BD07-69E898B464CC}

1 NetBt transport currently configured.

IP Security test . . . . . : Passed

Local IPSec Policy Active: 'Tunel IPsec prueba red A'

IP Security Policy Path: SOFTWARE\Policies\Microsoft\Windows\IPSec\

Policy\Local\ipsecPolicy{5E1A2585-5508-4DCF-8EDE-4F515BFE046B}

There are 1 filters

lista_nuevos_filtros_ip_Jamy

Filter Id: {7C422946-7BB5-4720-B784-D35D483CC216}

Policy Id: {A775C954-EB45-4BDD-A5FA-E1121F6D9269}

IPSEC_POLICY PolicyId = {A775C954-EB45-4BDD-A5FA-

E1121F6D9269}

Flags: 0x0

Tunnel Addr: 0.0.0.0

PHASE 2 OFFERS count = 1

Offer #0:

ESP[DES MD5 HMAC]

Rekey: 0 seconds / 0 bytes.

AUTHENTICATION INFO Count = 1

Method = preshared key: XXX

Src addr : 192.168.32.0 Src mask : 255.255.255.0

Dest addr : 192.168.64.0 Dest mask : 255.255.255.0

Tunnel addr : 192.168.64.100 src Port : 0 dest port : 0

Protocol : 0 tunnelfilter: yes

Flags : outbound

The command completed successfully

ANEXOS

RFC consultados: sec (2.2)

RFC 1320 - The MD4 Message-Digest Algorithm.
RFC 1321 - The MD5 Message-Digest Algorithm.
RFC 1828 - IP Authentication using Keyed MD5.
RFC 1829 - The ESP DES-CBC Transform.
RFC 2040 - The RC5, RC5-CBC, RC5-CBC-Pad, and RC5-CTS Algorithms.
RFC 2085 - HMAC-MD5 IP Authentication with Replay Prevention.
RFC 2104 - HMAC: Keyed-Hashing for Message Authentication.
RFC 2144 - The CAST-128 Encryption Algorithm.
RFC 2202 - Test Cases for HMAC-MD5 and HMAC-SHA-1.
RFC 2207 - RSVP Extensions for IPsec Data Flows.
RFC 2268 - A Description of the RC2 Encryption Algorithm.
RFC 2367 - PF_KEY Key Management API, Version 2.
RFC 2401 - Security Architecture for the Internet Protocol (IPsec).
RFC 2402 - IP Authentication Header (AH).
RFC 2403 - The Use of HMAC-MD5-96 within ESP and AH.
RFC 2404 - The Use of HMAC-SHA-1-96 within ESP and AH.
RFC 2405 - The ESP DES-CBC Cipher Algorithm With Explicit IV.
RFC 2406 - IP Encapsulating Security Payload (ESP).
RFC 2407 - The Internet IP Security Domain of Interpretation for ISAKMP.

RFC 2408 - Internet Security Association and Key Management Protocol (ISAKMP).

RFC 2409 - The Internet Key Exchange (IKE).

RFC 2410 - The NULL Encryption Algorithm and Its Use With Ipsec.

RFC 2411 - IP Security Document Roadmap.

RFC 2412 - The OAKLEY Key Determination Protocol.

RFC 2451 - The ESP CBC-Mode Cipher Algorithms.

RFC 2631 - Diffie-Hellman Key Agreement Method.

RFC 2709 - Security Model with Tunnel-mode IPsec for NAT Domains.