Universidad Austral de Chile

Facultad de Ciencias de la Ingeniería

Escuela de Electricidad y Electrónica

Protocolos de Seguridad para Redes Privadas Virtuales (VPN)

Tesis para optar al titulo de
INGENIERO ELECTRÓNICO

Profesor patrocinante:
Sr. Pedro Rey Clericus
Ingeniero Electrónico

VICTOR HUMBERTO LIMARI RAMIREZ

VALDIVIA 2004

Profesor Patrocinante

Pedro Rey Clericus: _____

Profesores Informantes

Néstor Fierro Morineaud: _____

Franklin Castro Rojas: _____

AGRADECIMIENTOS

Este espacio lo dedico principalmente a mis padres ya que gracias a su apoyo y esfuerzo han logrado brindarme la posibilidad de optar a cumplir mis metas. También agradezco a todos mis familiares, amigos y compañeros que directa o indirectamente han aportado a que mi trabajo de titulación se concrete.

RESUMEN

Las formas de comunicación computacionales en el mundo entero que se aplican en estos momentos como necesidad primordial, han sufrido evoluciones a medida que crece la tecnología. Y ya a estas altura toda organización tendrá la necesidad de estar comunicada ya sea localmente como con el mundo entero. Por este motivo surgen las redes organizacionales donde entre los nodos terminales se realizan diferentes operaciones e intercambio de datos, los cuales han requerido contar con normas de seguridad para no sufrir modificaciones o perdidas de información. Para las redes locales no existe mayor riesgo debido a que el organizador de la red dará los permisos a cada usuario. Pero cuando se realizan enlaces punto a punto sobre un medio público las empresas necesitaran resguardar de una mejor forma sus bases de datos para transportarlos. Luego de costosos modelos de transporte físico nacen las redes privadas virtuales, que básicamente realizan túneles a través de la plataforma pública.

El presente trabajo analiza las diferentes formas que hacen posible crear túneles a través de estos medios considerados como poco seguro para quien necesite que sus datos no sean dañados, leídos o tergiversados. Estudiándose así, tanto los modelos como la estructura que adopta la información al momento de considerarse listo para viajar por el medio inseguro.

Se da especial énfasis en este documento al protocolo de seguridad sobre IP llamado IPSec, el cual reúne la mayoría de las características que hacen que un modelo sea seguro sobre un medio masivo como lo es la Internet.

Se estudian además las diferentes formas de implementación de esta alternativa, considerándose de gran seguridad la basada en Firewall, la cual contempla la solución IPSec a los problemas antes mencionados.

Y por ultimo se presenta una aplicación a nivel de Cliente VPN, donde el otro extremo basado en Firewall se configura como servidor IPSec VPN de acceso.

SUMMARY

The way of computations communication in the world who are apply in this moments like basic need, it is suffered evolutions to long growth the technology. In this moment every organization will have the need to be communicated, as long locally like with the all world. For this cause born the organizations network where between terminals nodes make different operations and data interchange, who has required count with security norms for not suffer modifications or losing information. To the local networks is not so risk, because the network administrator will give the permission to every user. But when make links point to point over a public environment the company will need to protect to better way their data base to transfer it. After the expensive models of public transport born the virtual private networks, who basically make tunnel throught public platforms.

The present work analyze the different ways who make possible create this tunnels throught this environment considerate like low safe to whom need that them dates don't be damage, reed it or modificate it. Study it, as much the models like the structure who adopt the information to the moment considerate ready to the travel by the insecure way.

Maken an special emphasis in this document to the protocol of security over IP call IPSec, which reunite the most of the characteristic who make a model be safe about a massive way like it is the Internet.

Study besides the different ways of implementation of this alternative, considerate of great safety based on Firewall, which contemplate the solution IPSec to the problems before mentioned.

At last present an applications to level VPN Client, where the other extreme bases in Firewall configured like VPN IPSec Server of access.

OBJETIVOS

Objetivo general

Analizar funcionamiento de los principales protocolos que hacen posible la creación de túneles dentro de una infraestructura publica, llamados accesos VPN.

Objetivos específicos

Análisis del funcionamiento básico y funcional de redes privadas virtuales (VPN).

Investigación acerca de los métodos de seguridad de transporte y control de acceso en medios de difusión publica como Internet.

Investigación sistemática del protocolo de alta seguridad (IPSec) para redes IP.

Realizar una aplicación básica que permita un acceso como Cliente VPN, donde se puedan poner en marcha las medidas que otorgan una seguridad más confiable (Firewall, IPSec, etc.).

INTRODUCCIÓN

Hace unos años con el surgimiento masivo de las estructuras de red locales a niveles empresariales no era aun significativo la conexión de usuarios a Internet para asuntos laborales, pero a medida que ha pasado el tiempo las compañías han requerido que sus redes locales trasciendan más allá del ámbito de la oficina e incluyeran a los trabajadores y centros de información de otros edificios, ciudades, estados o incluso otros países. Para esta causa tenían que invertir en hardware y servicios de telecomunicaciones costosos para crear redes amplias de servicio, además de líneas dedicadas para el acceso WAN. Sin embargo ya con la llegada y popularización de Internet, las compañías tienen la posibilidad de crear enlaces virtuales que demandan una inversión relativamente pequeña de hardware, ya que utilizan la infraestructura ya establecida como publica para la conexión entre los puntos de la red.

Las LAN tradicionales son redes esencialmente restringidas, por lo cual se puede intercambiar información entre las computadoras usualmente sin pensar en la seguridad de la información o preocuparse mucho por ella y verdaderamente cuán importante es esta ya que Internet no es un medio de difusión seguro, nacieron una serie de normas y protocolos especiales que permiten encriptar información y permitir únicamente a la persona autorizada desencriptar esta información con un identificador que comprueba que la transmisión se ha hecho desde una fuente confiable.

Este conjunto se conoce actualmente como configuración VPN de redes, y muchas empresas comienzan a utilizarlo, ya sea para interconectar sub-redes como teletrabajadores. Cuando un empleado se conecta a Internet, la configuración de las VPN les permite "perforar" la red privada de la compañía y navegar en la red como si estuvieran en la oficina.

En la actualidad existen dispositivos especiales que otorgan niveles de seguridad esenciales para realizar enlaces remotos entre empresas, a estos equipos se les conoce como equipos VPN.

En este trabajo de titilación se analizaran configuraciones VPN, aspectos técnicos a nivel protocolar del montaje de enlaces VPN, así como la puesta en marcha de una aplicación de acceso remoto.

ÍNDICE

CAPITULO 1. REDES PRIVADAS VIRTUALES

1.1 Concepto VPN

VPN significa literalmente VIRTUAL PRIVATE NETWORK, en español RED PRIVADA VIRTUAL.

A continuación se realiza el análisis desde lo más básico del concepto VPN:

1.1.1 RED

Las redes y en general el uso de ordenadores en las organizaciones, empresas o industrias hoy en día se han incorporado de una manera creciente, y constituyen parte importante de la producción. Una red corresponde a dos o mas PCs interconectados entre si para lograr una comunicación, intercambio de datos y a la vez poder compartir recursos. Debe estar configurada de tal forma que sea compatible a estadares de conectividad preestablecidos. En la actualidad existen varios tipos de redes, es decir están confeccionadas de maneras diferentes según normativas, topologías o equipos que hacen posible la interconexión.

Una red no la componen solo los PCs, existen equipos conectados al conjunto que cumplen roles diversos en el sistema, por ejemplo: *Servidores*, *Hubs*, *Switches*, *Routers*, *Concentradores*, *Firewalls*, *Gateways*, etc. Los cuales se incorporan de acuerdo a las necesidades, tamaño y topología de la red, es decir una red de PCs de gran envergadura requerirá equipos que soporten las tareas y exigencias. Un modelo bastante sencillo se puede apreciar en la figura siguiente:

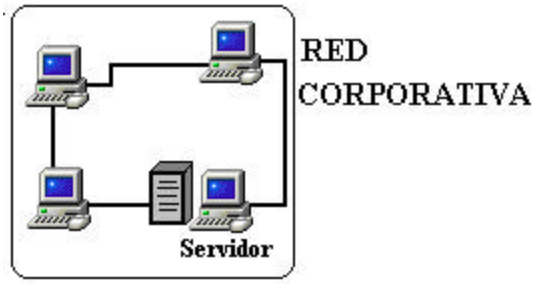


Figura 1-1. *Estructura básica de una RED.*

1.1.2 RED PRIVADA

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

Esto se lograra con equipos especiales que bloquean la entrada a terceros, o simplemente estas redes no están conectadas a un medio de difusión publica.

1.1.3 RED PRIVADA VIRTUAL

Una red privada virtual (VPN) es en esencia una estructura de red la cual tiene la capacidad de establecer un canal de comunicación privado sobre una infraestructura de red pública.

Entonces con VPN es posible establecer una comunicación vía infraestructura publica entre dos estaciones de trabajo remotas sin correr el riesgo que terceras personas ajenas a la organización pueda acceder a dicha información ni al sistema de interconexión.

Esta tecnología permite crear un túnel de encriptación a través de la Internet u otra red publica de tal forma que permita a los usuarios que se encuentran en los extremos del túnel disfrutar de la seguridad, privacidad y funciones que antes estaban disponibles solo en redes privadas.

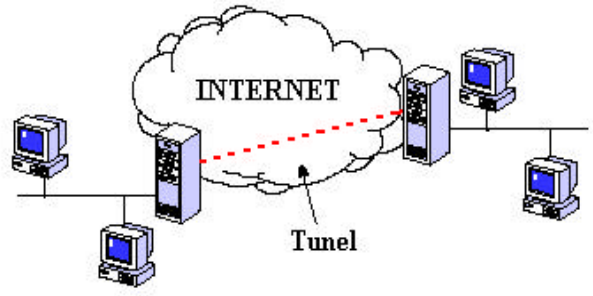


Figura 1-2. *Estructura de una Red Privada Virtual.*

El equivalente lógico a esta red VPN corresponde a un enlace privado punto a punto, lo que implica una inversión bastante costosa si se desea realizar una extensión de la red a una distancia considerable.

Es decir, se debe realizar una arquitectura de cableados y equipos de conectividad que abarque la zona a la cual se desee llegar.

1.2 Razones por las cuales es recomendable implementar una VPN

- Reducción de Costos:

  Para una implementación de red que abarque empresas alejadas geográficamente ya no será indispensable en términos de seguridad realizar enlaces mediante líneas dedicadas (punto a punto) de muy alto costo que caracterizaron a muchas empresas privadas, siendo reemplazadas por ejemplo, por acceso ADSL de un ancho de banda alto y bajo costo, disponible por lo general en la mayoría de las zonas urbanas sin mayores problemas.

  Los usuarios remotos móviles podrán ahorrar altos costos de llamadas telefónicas de larga distancia, bastando con que disque un proveedor de acceso local a la Internet (no IP fija).

- Alta Seguridad:

  Las redes VPN utilizan altos estándares de seguridad para la transmisión de datos, dando un resultado comparable a una red punto a punto. Protocolos como 3DES (Triple data encryption Standard) el cual cumple la función de encriptar la información a transferir y el protocolo IPSec (IP Security) para manejo de los túneles mediante software brindan una alto nivel en seguridad al sistema.

  Además se utilizan varios niveles de autentificación de usuarios para el acceso a la red privada mediante llaves de ingreso, para la asegurar que el usuario es el original y no un tercero que percibe el password de autentificación.

- Escalabilidad:

  Para agregar usuarios a la red no es preciso realizar inversiones adicionales. La provisión de servicios se hace con dispositivos y equipos fáciles de configurar y manejar.

  Se usa la infraestructura de alto nivel establecida ya por los proveedores de Internet y no realizar un enlace físico que puede significar una gran inversión monetaria y de tiempo.

- Compatibilidad con tecnologías de banda ancha:

  Una red VPN puede aprovechar infraestructura existente de banda ancha inalámbrica, TV cable o conexiones de alta velocidad del tipo ADSL o ISDN, lo que implica un alto grado de flexibilidad y reducción de costos al momento de configurar la red. Incluso es posible usar voz sobre IP usando la implementación VPN, y esto implica un significativo ahorro en telefonía de larga distancia.

- Mayor Productividad:

  Debido a un mejor nivel de acceso durante mayor tiempo se podría probar que se obtendría una mayor productividad de los usuarios de la RED.

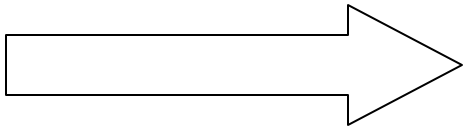
  Además se fomenta el teletrabajo con la consecutiva reducción en las necesidades de espacio físico.

1.3 Usos comunes de las VPN

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

1.3.1 Acceso remoto del Usuario sobre una red publica

Las VPN proporcionan acceso remoto a recursos corporativos sobre la red Internet pública, manteniendo al mismo tiempo privacidad y seguridad de la información.



- **Usuario viajero**
- **Teletrabajador**
- **Cliente Remoto**

RED CORPORATIVA

(Servidor VPN)

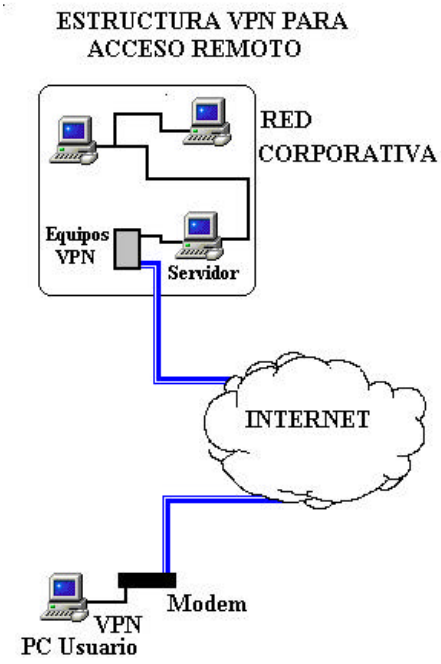


Figura 1-3. *Acceso remoto de un usuario a una VPN.*

Este tipo de conexión se establece cuando un usuario de la red corporativa se encuentra realizando un trabajo geográficamente lejos o algún cliente de la empresa necesita obtener datos en forma remota de las bases para futuras transacciones. Luego de la configuración VPN previa del equipo remoto que va a ser conectado a la red, se debe adquirir un servicio de Internet al ISP local. Utilizando la infraestructura de la Internet de esta manera se realiza un túnel de comunicación del equipo con el servidor VPN de la organización de manera confiable donde se puede asegurar que los datos serán tan confidenciales como si se tratase de una red privada o dedicada.

Además la gran ventaja de esta alternativa es que decrecen significativamente los costos de conexión debido que no es necesario establecer la comunicación mediante llamada de larga distancia a un servidor de acceso de red (NAS), lo cual implica un gasto adicional mucho mas elevado para el logro del objetivo.

1.3.2 VPN Cliente – Servidor

Existe el caso del usuario que forme parte de un ambiente laboral dentro de un edificio donde se implementa una LAN (red de área local), pero este usuario desea comunicarse confidencialmente de manera especifica con solo un departamento de dicha LAN, sin que terceros miembros intercepten la información en cuestión.

Entonces se utilizaran los servicio de encaminamiento de datos de la Internet o los de la misma impuesta por la LAN para realizar un túnel con encriptación y se logre la seguridad y confidencialidad que se requiere.

Algunos de los problemas que surgen si no se toman medidas de seguridad en el tráfico de datos adecuadas son:

- Cualquier usuario conectado a la red tendrá acceso libre a servicios críticos.
- La información que viaja por la red queda sensible a sniffing (visualización por parte de terceros)
- Importación de usuarios validos con datos obtenidos del medio de transmisión.

Y para el caso en que la organización haya implementado un sistema que exija autentificación del usuario que entra al departamento de la red:

- Captura de password por sniffing y posterior importación de usuario.

La alternativa de solución de estos problemas de seguridad es la incorporación del servidor VPN para la RED o departamento dedicado que necesite resguardar datos y requiera la comunicación con usuarios que se encuentre físicamente situados en la RED común para todos.

Es decir con esta implementación se configuran tanto el servidor VPN como los equipos que auténticamente tendrán acceso a la información confidencial, de manera tal que se lograra crear un túnel de comunicación privada entre estas dos partes, sin que terceros puedan captar o capturar los datos de intercambio.

Las ventajas que se obtienen al poner en marcha el sistema VPN dentro de una LAN son:

- Implementación transparente a las aplicaciones:

  Una vez configurado mediante un simple cambio de rutas, todo el trafico es automáticamente encriptado y validado sin necesidad de cambio alguno en la operatoria.
- Alta seguridad

  Al encriptar no solo los datos sino también las direcciones destino, se evita que terceras personas tengan acceso a la información.
- Distintos niveles de seguridad

  Según la necesidad, se puede operar con password preconfigurados o para mayor seguridad con certificados para firmas digitales de RSA 1024/2048 bits para la autentificación de los extremos.

El siguiente esquema permite visualizar en forma global los niveles de seguridad que se puede lograr al implementar un enlace VPN dentro de una organización:

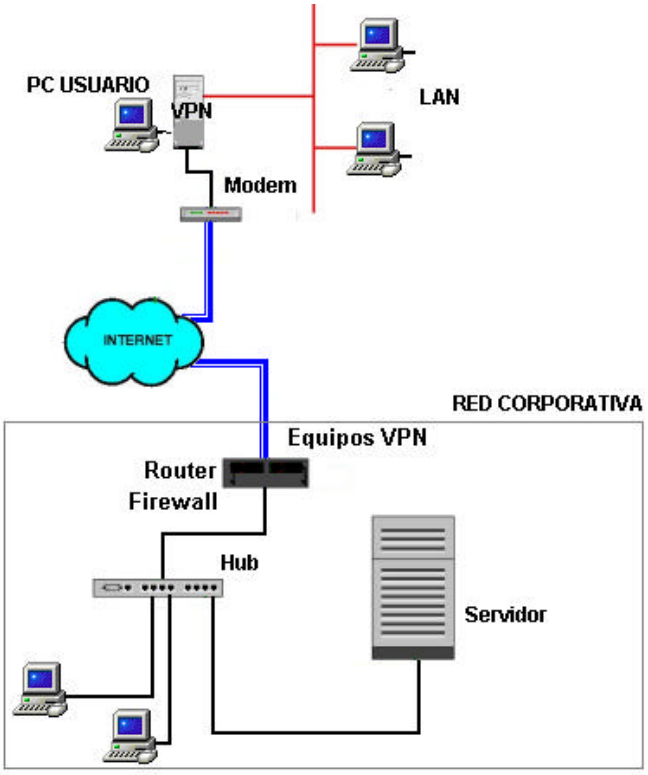


Figura 1-4. *Acceso privado de un cliente dentro de una red corporativa.*

Nota de la figura anterior:

Línea Roja: *Camino Inseguro*

Línea Negra: *Camino Seguro*

Línea Azul: *Camino seguro protegido por modelo VPN*

1.3.3 VPN Servidor – Servidor

Este es el caso en que dos oficinas de una misma organización las cuales poseen un equipamiento de infraestructura lo bastante robusto como para soportar ordenadores creando redes corporativas, las cuales requieran comunicarse remotamente mediante alguna red publica. Si estas sucursales no mantienen las medidas de seguridad para resguardas los paquetes que viajan por la red tendrán el riesgo de que su información privada sea captada o se pueda tener acceso al sistema con fines perjudiciales.

Si se desea optar a una forma de interconexión más segura se deberá invertir en un enlace punto a punto lo cual podría generar altos costos de instalación.

Los problemas que podría generar el modelo en el cual se realiza una interconexión mediante red publica son los que se citan a continuación:

- Cualquier usuario conectado a la red pública podrá tener libre acceso a servicios críticos e información confidencial.
- Información viajando sensible a sniffing (visualización por parte de terceros).
- Importación de usuarios validos con datos obtenidos del medio de transmisión.

Para dar una alternativa solución a este tipo de problemas ambas redes tendrán que incorporar a los terminales de acceso al medio publico barreras de protección mediante un Servidor VPN las cuales administran los equipos tales como Router (enrutador) y Firewall que hacen posible la creación y disposición Off / On de túneles para que la información viaje encriptada y no sea visualizada por terceros.

El esquema que refleja la solución VPN para dos Servidores que administran redes corporativas es el siguiente:

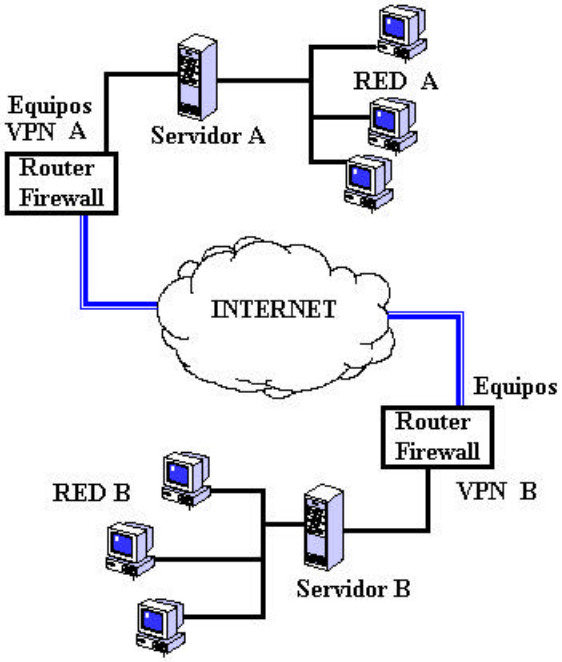


Figura 1-5. *VPN entre dos redes corporativas.*

Se puede establece en la figura anterior que el tramo comprendido a la salida de los equipos terminales que están caracterizados con líneas azules que contienen protocolos de encriptación que contribuyen a la seguridad de la red en el medio en que se esta transmitiendo en esta caso la INTERNET.

Dentro de cada red visto con líneas negras no hay peligro que haya accesos no deseados o captura de información ya que el equipo FIREWALL (cortafuego) es el encargado de cerrar el acceso a terceros no autorizados.

Las ventajas que se pueden citar luego de la implementación de un enlace VPN entre dos redes corporativas mediante una vía pública son:

- Alta seguridad:

  Al encriptar no solo los datos sino también las direcciones destino, evita que un usuario de la red publica ajeno al autorizado para el manejo de la información capture o lea los datos que están siendo enviados.

La información viaja indescriptible entonces no es posible la captura de los datos y la impostación de usuarios.

- Distintos Niveles de Seguridad:
  Según las necesidades, se puede trabajar con claves pre-configuradas o con certificados de llaves para la autentificación de los extremos.

1.4 Tipos de VPN

1.4.1 Sistemas basados en Hardware

Las VPN basadas en Hardware poseen en el extremo del Servidor de la organización un **"router"** o **"enrutador"** dedicado el cual tiene la misión de encriptar los datos, además de abrir y cerrar los túneles VPN cuando funciona como receptor. Estos proporcionan facilidades al usuario que administra la implementación VPN, ya que son seguros, rápidos, de fácil instalación y fáciles de usar. Ofrecen un gran rendimiento ya que no malgastan ciclos en forma tan significativa de procesamiento de operación ya que no requiere un sistema operativo, ya que este es configurado para las operaciones que requiera el servicio VPN.

1.4.2 Sistemas basados en Firewall

Estos sistemas aprovechan las ventajas del **"Firewall"** o **"cortafuego"** como la restricción de acceso a la red o generación de registros de posibles amenazas, y ofrecen además otras opciones como traducción de direcciones o facilidades de autentificación fuerte.

La desventaja de un sistema basado en Firewall afecta en mayor o menor medida al rendimiento del sistema general, lo que puede ser un problema para la organización dependiendo de las necesidades que se requieran. Algunos fabricantes de Firewalls ofrecen en sus productos procesadores dedicados a encriptación para minimizar el efecto del servicio VPN en el sistema.

1.4.3 Sistemas basados en Software

Estos sistemas basados en software son ideales en el caso en que los dos extremos que deseen comunicarse en forma remota y privada no pertenezcan a la misma organización.

Esta solución permite mayor flexibilidad en cuanto a la decisión de que trafico enviar por el túnel seguro VPN, pudiendo decidir por protocolo y dirección donde en un sistema basado en hardware solo se puede decidir por dirección.

Existen desventajas para un sistema basado en software, las cuales consisten en que estos sistemas son difíciles de administrar, ya que necesitan estar familiarizados con el sistema operativo Cliente, la aplicación VPN y los mecanismos de seguridad adecuados.

Nota: Existen fabricantes que ofrecen soluciones basadas en hardware que incorporan software cliente para VPN.

1.5 Requerimientos básicos para establecer una VPN

1.5.1 Con respecto al tipo de conexión

1.5.1.1 OFICINA CENTRAL:

Corresponde a una red corporativa o la red LAN. Esta tendrá que disponer de una IP fija a través de una conexión ADSL para acceso a Internet. Debe disponer además de un dispositivo (Firewall o Router) VPN el cual administre hasta mas de 5 túneles y que permita dar acceso autentificado y seguro a los usuarios y oficinas remotas.

1.5.1.2 USUARIOS REMOTOS:

Estos utilizarán un software especial para la configuración VPN que junto con una conexión a la Internet desde el ISP (proveedor de servicios de Internet) de costo local (con o sin IP fija) permite el contacto con la red privada (oficina central), como si se tratase de un puesto mas de la Red Privada Central de carácter LOCAL.

1.5.1.3 OFICINAS REMOTAS:

Tendrán que disponer de una conexión a la Internet con RDSI o ADSL (no es necesario tener IP fija) que en conjunto con un dispositivo VPN les permite ponerse en contacto con la RED Privada (oficina central) en forma confidencial.

1.5.2 Con respecto a las normas de seguridad

1.5.2.1 AUTENTIFICACION DEL USUARIO:

La configuración VPN deberá verificar la identidad del usuario y restringir el acceso solo a usuarios autorizados.

1.5.2.2 ENCRIPTACION DE DATOS:

Los datos que viajan por la Red Publica fuera de los equipos terminales no podrán ser leídos por clientes no autorizados en la red, por esta razón se utilizan normas de encriptación.

1.5.2.3 ADMINISTRACION DE DIRECCION:

Se deberá asignar a cada cliente de la red interna una dirección de IP privada.

1.5.2.4 ADMINISTRACION DE LLAVES:

La alternativa VPN deberá generar y renovar las llaves de encriptación para el cliente y el servidor.

1.5.2.5 SOPORTE DE PROTOCOLO MULTIPLE:

Se debe habilitar soporte para los protocolos más comunes o usuales utilizados en las redes públicas. Se incluyen protocolos de Internet (IP), central de paquetes de Internet (IPX), etc.

CAPITULO 2. PROTOCOLOS VPN

Para lograr un funcionamiento efectivo de una Red Privada Virtual, se han implementado una serie de protocolos y normas de conectividad orientadas tanto a los equipos terminales como a los sofwares del enlace. De esta forma se presentan en el siguiente capitulo los protocolos fundamentales de un enlace VPN, empezando desde el protocolo de enlace mas básico hasta llegar a un enlace virtual de seguridad mas avanzada.

Para determinar el grado de seguridad de estos medios de comunicación VPN, se deberá consultar la siguiente clasificación:

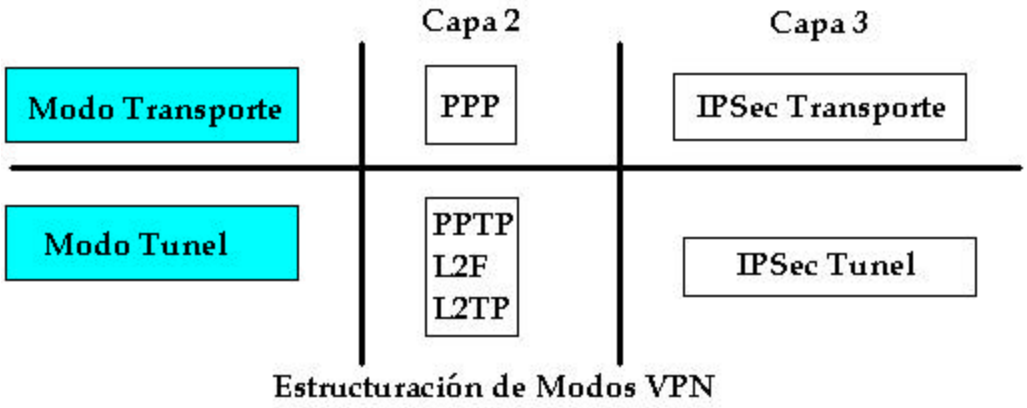


Figura 2-1. *Ubicación de cada protocolo VPN en el modelo de referencia OSI y el modo en que trabaja.*

2.1 Protocolo de Transporte de las conexiones

Este modo de trabajo permite realizar el enlace virtual entre los puntos que deseen comunicarse mediante un sistema público, luego de este paso se puede establecer un túnel para lograr confidencialidad, integridad, autentificación, en resumen la seguridad de la comunicación.

2.2 Protocolo de Túneles de las conexiones VPN

Para cumplir las necesidades de seguridad de los datos transmitidos se han creados métodos que hacen posible el establecimiento de túneles que mediante encapsulación y encriptación de las tramas se emula un enlace punto a punto privado seguro sobre la infraestructura publica que esta siendo usada.

2.2.1 Concepto de Túnel

Un sistema de túnel es un método que transforma las tramas (o paquetes) de información confidencial para que estas no sean leídas por terceros que estén presentes en el medio de transmisión. Este túnel es creado en forma virtual sobre el trayecto de red que es considerado público, es decir las tramas quedan indescifrables para los usuarios de la red pública y realizan la trayectoria sin que estas sean perturbadas creando un camino inviolable.

Existen alternativas de túnel siendo base aquel mecanismo que permite añadir una cabecera adicional al paquete original para que este pueda circular a través de la red pública hasta el servidor de la red corporativa, donde se eliminará el encabezamiento adicional.

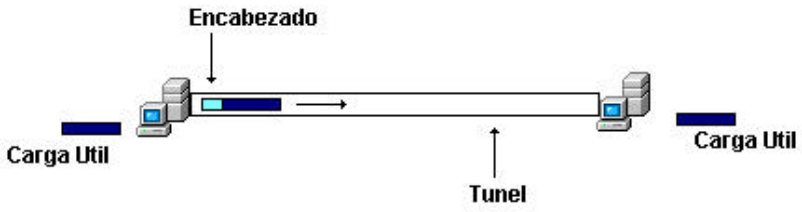


Figura 2-2. *Estructura de túnel de la trama con encabezamiento adicional.*

2.2.2 Tipos de Túneles

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

- ***Túneles voluntarios:*** Un PC de usuario o de cliente puede emitir una solicitud VPN para configurar y crear un túnel voluntario. En este caso, el PC del usuario es un punto terminal del túnel y actúa como un cliente del túnel.
- ***Túneles obligatorios***: Un servidor de acceso de marcación capaz de soportar una VPN configura y crea un túnel obligatorio. Con un túnel obligatorio, el PC del usuario deja de ser un punto terminal del túnel. Otro dispositivo, el servidor de acceso remoto, entre el PC del usuario y el servidor del túnel, es el punto terminal del túnel y actúa como el cliente del túnel.

Nota: Hasta hoy los túneles voluntarios han probado ser el tipo más popular de túnel, debido a que los accesos son espontáneos como Clientes VPN desde cualquier punto terminal.

2.2.3 Protocolos de Túnel

Las tres alternativas protocolares relevantes para lograr un enlace de túnel en una red de comunicación que requiera seguridad y confidencialidad, y que en este documento serán objeto de estudio son las siguientes:

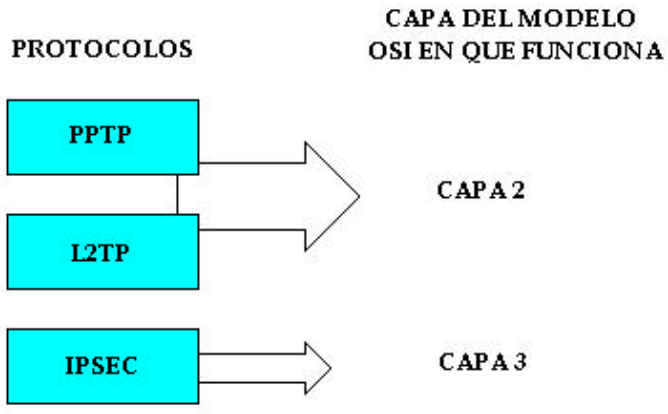


Figura 2-3. *Principales protocolos de túnel y capa en que actúa.*

CAPITULO 3. PROTOCOLOS DE CAPA 2

En este capitulo se realiza un análisis de los protocolos VPN que actúan en la capa 2 de enlace de datos del modelo de referencia OSI.

3.1 Modo transporte en la capa 2

3.1.1 Protocolo PPP (Punto a punto)

Toda comunicación entre dos puntos necesita de normas particulares de conexión las cuales son esenciales para enviar los datos a través del sistema implementado, sin ellas es imposible direccionar o encaminar los paquetes de información a sus destinos. Para lograr un acceso remoto entrante con el servidor terminal de la red es necesario recurrir a los protocolos necesarios para los fines citados, además es importante destacar que se deben considerar las respectivas normas de seguridad y autenticidad para obtener el resultado esperado y no se produzcan problemas.

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

El PPP es parte de TCP/IP y básicamente encapsula el protocolo del paquete de información original en uno transportable por la Internet (paquete PPP). Además se permite incorporar términos de autenticidad para que así la seguridad de la red e integridad de la información no sea afectada.

3.1.2 Secuencia de la conexión PPP

El caso que representa la primera etapa del enlace VPN es cuando un equipo cliente remoto necesita comunicarse con el servidor VPN de su empresa de carácter privado. Para este fin en primer lugar se debe realizar una petición al ISP local para que realice la comunicación

mediante PPP, lo cual servirá para implementar un túnel VPN. A continuación se indican las fases de la conexión PPP:

1. Establecimiento del enlace PPP

   Se establecen las reglas para el manejo y direccionamiento de tramas entre el equipo remoto y el servidor (origen y destino). Esto permite que se establezca una comunicación continua (transferencia de tramas).

   En esta fase se configuran las opciones para la implementación del protocolo de control de enlace (LCP), el cual establece, mantiene y finaliza la conexión física, en otras palabras se seleccionan las opciones de comunicación PPP básicas.

   Prácticamente luego de la conexión física telefónica inicial entre el cliente remoto y el servidor ISP se envía una serie de paquetes LCP para realizar la petición de configuración de nivel de enlace de datos (capa 2).

2. Autentificación del Usuario

   El usuario remoto debe presentar una identificación al servidor de acceso remoto, acción que si es aceptada permite la conexión y comunicación con la red privada.

   En esta fase el usuario envía una identificación de usuario al servidor de acceso remoto, y este debe verificar la autenticidad del nombre y las contraseñas de acceso privada.

   Un buen sistema o esquema de autentificación proporciona la seguridad de la información y el acceso exclusivo de clientes autorizados. PPP ofrece métodos de autentificación como PAP, CHAP, MS-CHAP, siendo más recomendable aun sistemas mas complejos de autenticación teniendo un propio servidor RADIUS o TACACS.

   Nota: Los algoritmos y sistemas de autentificación más importantes son expuestos en el anexo A.

3. Llamada a protocolos de nivel de red.

   En esta fase del PPP se invoca a los protocolos de nivel de red (NCP) que fueron seleccionados por el cliente remoto durante la fase de establecimiento del enlace para configurar los protocolos utilizados para la comunicación. Además en esta fase el ISP

mediante NCP otorga dinámicamente una dirección IP pública al equipo cliente que se acaba de conectar para que la use durante la sesión.

3.1.3 Transferencia de la Información

Luego de establecidas todas las fases previas a la transferencia de datos se envían los paquetes PPP a través del enlace entre el servidor y el cliente, cuando estas tramas llegan a su destino son descifrados por el sistema receptor.

3.1.4 Paquete PPP

La información que se desea enviar desde un PC a otro es un conjunto de números binarios los cuales representan byte de datos, conformado cada bit físicamente como un 1 o un 0 lógico (nivel alto y bajo). A me medida que estos paquetes van llegando a su destino (comunicación serial) se van restaurando el documento original.

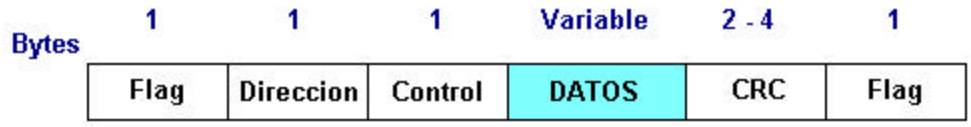


Figura 3-1. *Paquete procesado como PPP.*

Siendo:

- **Flag (Bandera):** Indica el comienzo y finalización de la trama, cuyo valor binario es preestablecido como 01111110 (7E h).

- **Dirección:** Representa la dirección de enlace de datos establecido para TCP/IP. En el caso de PPP siempre ira fijado con el valor 11111111 (FF h).

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

- **Datos:** Será un campo de longitud variable, que contiene IP privada y los datos a transmitir.

- **CRC:** Representa el resultado de aplicar un código redundante cíclico a la trama y sirve como mecanismo de detección de errores en la misma. Normalmente es de 2 bytes, sin embargo puede negociarse para medir 4 bytes.

3.2 Modo túnel en la capa 2

A continuación se presentan los principales protocolos que funcionan como túnel VPN y operan en la capa 2 del modelo OSI.

3.2.1 PPTP (Protocolo de túnel punto a punto)

PPTP desarrollado por Microsoft es un protocolo de túnel del nivel 2 (enlace) del modelo de referencia OSI que permite el trafico seguro de datos desde un cliente remoto hasta un servidor corporativo privado, estableciéndose gracias a este la red privada virtual basada en TCP/IP. Es una extensión del protocolo PPP, es decir aprovecha las fases de autentificación, compresión y cifrado PPP para crear sobre esto el túnel virtual.
PPTP soporta múltiples protocolos de red como IP, IPX o NetBEUI que comúnmente transitan sobre las redes publicas como Internet y puede ser utilizado para crear VPN sobre otras redes publicas o privadas como líneas telefónicas (PSTN acceso telefónico a redes), redes LAN y WAN, Internet u otras redes publicas basadas en TCP/IP y además aprovecha las ventajas de los mecanismos de autenticación, compresión y cifrado de las tramas de información.

3.2.1.1 Escenario típico de una conexión PPTP:

En la práctica general hay normalmente tres ordenadores involucrados en una distribución:

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

Nota: En el caso del acceso de túnel dentro de una LAN el servidor de acceso a la red no será necesario.

Cuando el Cliente autorizado decide conectarse de forma remota al servidor de su empresa, desde donde esté se deberá conectar primero a un proveedor de servicios de Internet local (ISP) usando una conexión de acceso telefónico a redes (RDSI) mediante el protocolo punto a punto PPP (primer paso, *modo transporte*).

Luego usando la conexión a Internet establecida por el protocolo PPP, se crea una conexión túnel controlada del cliente PPTP al servidor PPTP en Internet mediante el protocolo PPTP.

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

Este túnel a rasgos se basa en añadir una cabecera IP adicional al paquete original, donde se direcciona dicha trama con la IP publica del servidor VPN, y la IP privada de la red o host receptor quedaran resguardados, creándose un túnel secreto en la red publica.

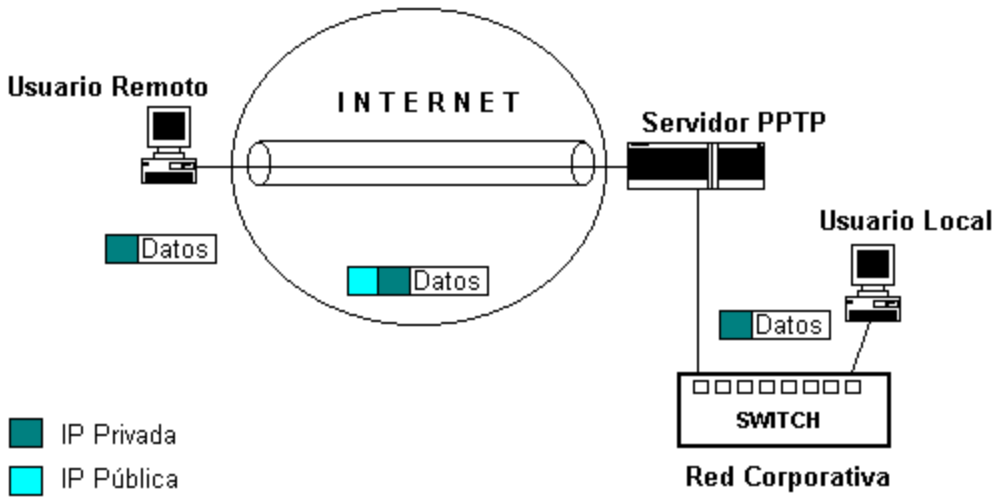


Figura 3-2. *Túnel creado entre un usuario remoto y una red corporativa a través de Internet*.

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

3.2.1.2 Servidor PPTP:

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

Tipo de Hardware requerido en los servidores:
Si se establece una maquina PC como servidor PPTP, se deberá instalar un sistema operativo que tenga excelente soporte a redes, y el programa específico para configuración de puertos de acceso. Además deberá tener dos adaptadores de red (Nic, modem, RDSI, X.25), uno conectado a la red local y el otro a Internet.

Partes esenciales en un Servidor PPTP:

- ***PNS (PPTP Network Server):*** Servidor de la red PPTP. Este se gestiona para operar sobre computadores de propósito general o plataformas de servidor de red.

- ***PAC (PPTP Access Concentrator):*** Es el concentrador de acceso PPTP. Es el dispositivo que asocia una o mas líneas capaces de soportar PPTP, es decir puede administrar muchas sesiones multiplexadas sobre el mismo túnel. También este dispositivo presente en el servidor permite proveer servicios a muchos PNS.

Una de las ventajas más palpables del PPTP es que reduce o elimina la necesidad de uso de sofisticados y caros equipos de telecomunicaciones para permitir las conexiones de equipos portátiles y remotos. PPTP puede usar redes telefónicas normales de forma totalmente segura.

Si es una red basada en Firewall o en Hardware (Router), se deberán configurar adecuadamente dichos equipos para que se establezca un mayor rendimiento de las actividades de red VPN.

3.2.1.3 Cliente PPTP:

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

Si el ISP no soporta PPTP, el cliente puede utilizar el software PPTP y crear una conexión segura, primero utilizando el ISP local estableciendo una conexión PPP para acceso a Internet para después lograr la conexión PPTP a través de un puerto PPTP del Servidor de la empresa.

Tipo de Hardware requerido en los clientes:

Antes que nada se debe asegurar de que exista un sistema operativo compatible con los servicios y trabajo de red. Hecha esta comprobación, para la conexión PPTP se requerirá un modem o una tarjeta de red, además de un equipo de conexión a una red telefónica.

Por otro lado, si el cliente está accediendo al servidor PPTP a través de una red de área local (LAN), se precisa de un adaptador de red (NIC) que lo conecte físicamente a ella.

3.2.1.4 Proceso de comunicación del túnel PPTP

El acceso a una red privada remota empleando el modo PPTP dispone de dos componentes que trabajan en paralelo:

1. Control de la conexión a la red privada, empleando el protocolo TCP, entre el equipo (*host*) remoto y el servidor de túneles.
2. Funcionamiento del túnel IP entre el equipo remoto y el servidor de túneles.

Control de la conexión, establece una conexión TCP entre el equipo remoto y el puerto 1723 (reservado para este uso) del servidor de túneles PPTP. Esta conexión tiene como objetivo el establecimiento y la gestión de las sesiones que el usuario establece en la red privada y son transportadas por el túnel. El formato de los paquetes en el control de la conexión será:

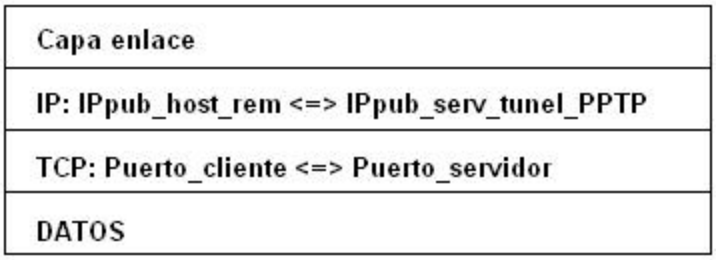


Figura 3-3. *Formato de la trama de control.*

La capa de enlace será la que proporciona el ISP al equipo remoto. Como antes se mencionó se emplea el protocolo PPP en la fase de establecimiento de la conexión punto a punto entre el equipo remoto y el ISP.

La capa de red y transporte gestionan el establecimiento de una conexión TCP desde el cliente (equipo remoto) al puerto 1723 del servidor (servidor PPTP de la red corporativa), empleando el direccionamiento público que proporciona el ISP al equipo remoto (IPpub_host_rem) y que posee el servidor de túneles para el acceso a Internet (IPpub_serv_tunel_PPTP).

3.2.1.5 Encapsulación PPTP

Una vez que es creada la trama PPP mediante el método de cifrador de flujos RSA RC4 del protocolo MPPE (cifrado punto a punto de Microsoft) por el RAS (ya sea de IP, IPX o NetBEUI) esta primero se comprime con un encabezado PPP, luego se empaqueta con un encabezado GRE de encapsulación de enrutamiento genérico (GRE, Generic routing encapsulation) y un encabezado IP en el cual se encuentran las direcciones origen y destino de la trama que corresponden al cliente y servidor VPN.

La siguiente figura presenta la estructura de la trama PPP ya encapsulada mediante la norma PPTP:

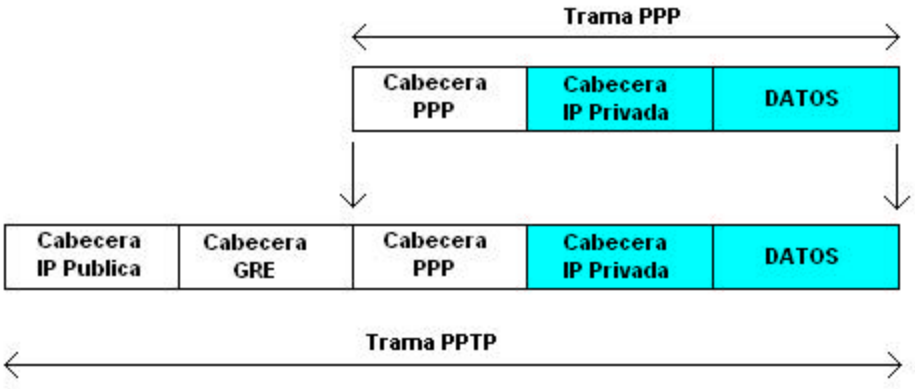


Figura 3-4. *Trama PPTP, con sus cabeceras de encapsulación respectivas.*

- La cabecera IP pública proporciona la información necesaria para que el datagrama atraviese la red de Internet. Esta cabecera establece la comunicación entre el cliente remoto (con IP publica proporcionada por el ISP) y el servidor de túnel PPTP.
- El encabezado GRE se usa para encapsular el paquete PPP dentro de un datagrama IP. Es decir se oculta los destinos IP originales de los host emisor – receptor, que solo el servidor PPTP y el cliente PPTP podrán percibir.
- La cabecera PPP permite establecer el nivel de enlace de datos entre el ISP y el usuario remoto, para así crear el túnel. Además proporciona la autentificación del usuario remoto.
- La cabecera IP privada es el direccionamiento IP entre el host usuario remoto y el servidor de la red corporativa, para que esta ultima lo conecte con el host usuario local.

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

3.2.1.6 Mantenimiento del túnel con el control de conexión PPTP

El control de conexión lleva a cabo el control de la llamada del PPTP y la administración de los mensajes que son utilizados para mantener el túnel. Esto incluye la transmisión periódica de mensajes para detectar fallas en la conexión entre el cliente y el servidor PPTP. Los paquetes de control consisten en una cabecera IP, una cabecera TCP y un mensaje de control como se ilustra en la siguiente figura:

Figura 3-5. *Paquete de control de conexión PPTP.*

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

Tipo de Mensaje de control PPTP	**Propósito**
Start-Control-Connection-Request	Enviado por el cliente PPTP para establecer la conexión de control. Cada túnel PPTP requiere que se establezca una conexión de control antes que pueda ser enviado cualquier otro mensaje PPTP.
Start-Control-Connection- Replay	Enviado por el servidor PPTP para responder al mensaje Start-Control-Connection-Request.
Outgoing-Call-Request	Enviado por el cliente para crear un túnel PPTP. Incluido en el mensaje Outgoing-Call-Request hay un identificador de llamada (*Call-ID*) que es utilizado en la cabecera GRE para identificar el tráfico de un túnel específico.
Outgoing-Call-Reply	Enviado por el servidor PPTP en respuesta al mensaje Outgoing-Call-Request.
Echo-Request	Enviado por el cliente PPTP o el servidor PPTP como un mecanismo para mantener la conexión. Si el Echo-Request no es respondido, el túnel PPTP eventualmente será terminado.
Echo-Reply	La respuesta a un Echo-Request. **Nota:** Los mensajes PPTP Echo-Request y Echo-Reply no están relacionados con los mensajes ICMP Echo Request ni Echo Reply.
WAN-Error-Notify	Enviado por el servidor PPTP por el servidor PPTP a todos los clientes VPN para indicar condiciones de error sobre la interfase PPP del servidor PPTP.
Set-Link-Info	Enviado por el cliente PPTP o el servidor PPTP para establecer las opciones PPP negociadas.
Call-Clear-Request	Enviado por el cliente PPTP indicando que el túnel será terminado.
Call-Disconnect-Notify	Enviado por el servidor PPTP en respuesta a un Call-Clear-Request o por otras razones para indicar que un túnel será terminado.

Stop-Control-Connection-Request	Enviado por el cliente PPTP o el servidor PPTP para informar al otro que la conexión de control será terminada.
Stop-Control-Connection-Reply	Utilizado para responder al mensaje Stop-Control-Connection-Request.

Tabla 1: *Mensajes de control de llamada PPTP.*

3.2.1.7 Proceso detallado del recorrido PPTP

La representación grafica del protocolo de nivel 2 PPTP se puede contemplar en el siguiente esquema, explicado paso a paso:

Figura 3-6. *Conexión PPTP en modo túnel.*

Cabe destacar que esta etapa se puede realizar en forma independiente y crear un acceso al servidor de la red corporativa si este diese los permisos, pero sin contar con la seguridad de un túnel en la red. Este protocolo se establece solo entre la red ATM creada entre el cliente y la ISP, siendo este tramo común a cualquier otro tipo de conexión PPPoE (punto a punto sobre Ethernet) o PPPoA (punto a punto sobre ATM).

Para tener los beneficios de privacidad se crea el túnel en Internet sobre la conexión PPP al ISP hecha entre el cliente y el ISP.

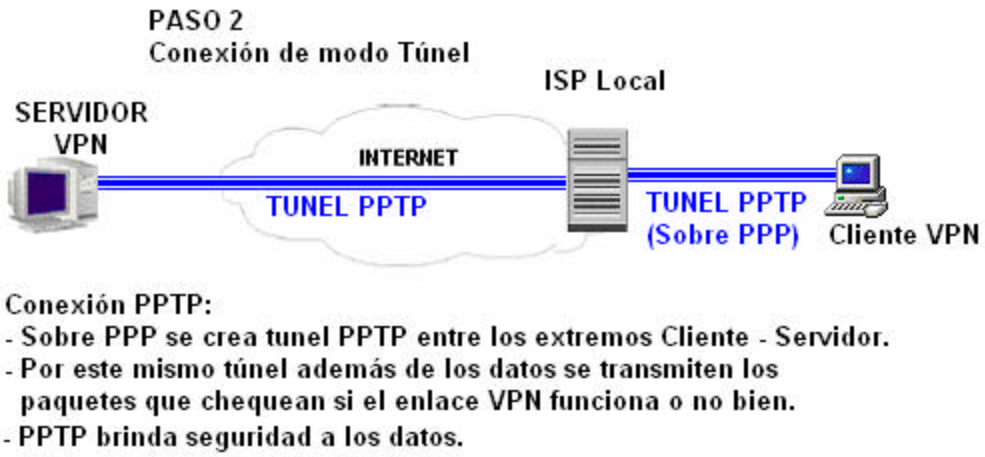


Figura 3-7. *Conexión PPTP en modo transporte.*

3.2.2 L2TP (Protocolo túnel de capa 2)

Al igual que PPTP este protocolo utiliza la trama PPP creada al conectar Cliente – ISP, donde luego se realiza el túnel de capa 2, funcionando de modo bastante similar teóricamente al protocolo antes mencionado. Sin embargo, este sistema ofrece más seguridad a los datos de información que viajan por el medio inseguro.

L2TP es un híbrido entre PPTP (Microsoft) y L2F (Cisco System), y adquiere lo mejor de cada protocolo.

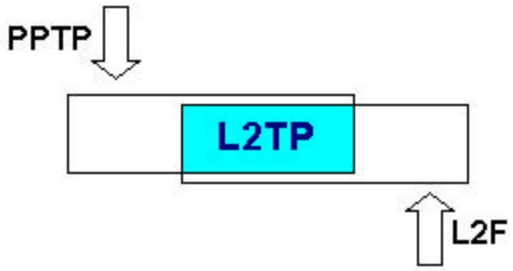


Figura 3-8. *L2TP es la combinación entre PPTP y L2F.*

Siendo las cualidades más trascendentes de L2F, que lo diferencia de PPTP:

1. Acepta y soporta además clientes no IP (Frame Relay, ATM, etc.)
2. Multiplexación de múltiples sesiones remotas (Minimizando número de túneles en uso). Es decir un servidor puede establecer más de una conexión privada un túnel.
3. En el interior de los túneles, cada una de las sesiones multiplexadas mantendrá un numero de secuencia con el objeto de evitar problemas de duplicación de paquetes lo que conllevaría a la congestión del túnel.

Características principales de L2TP:

- Como se dijo anteriormente L2TP es una combinación entre PPTP y L2F. Es decir cumple las características de PPTP, pero su gama de ruteo es más amplia ya que acepta paquetes de datos que no solamente son IP. Por lo tanto L2TP encapsula las tramas del protocolo punto a punto (PPP) que van a enviarse a través de redes IP, X.25, frame relay, o modo de transferencia asíncrona ATM, no se limita solo a medios IP.
- Las tramas PPP encapsuladas se pueden cifrar o comprimir. Cuando los túneles L2TP aparecen como paquetes IP, se puede reforzar la encriptación de los datos haciendo uso del método que utiliza el protocolo de cifrado IPSec (IP Security). L2TP en combinación con IPSec proporciona túneles bien definidos e interoperables (Seguridad de alto nivel). Es una buena solución para conexiones seguras de acceso remoto y de enlace remoto de servidor a servidor.
- Este protocolo admite una amplia gama de protocolos de autentificación que se utilizan para el enlace ISP-Cliente Remoto PPP (Chap, Ms-Chap, etc.). Sin embargo soporta otros sistemas de autentificación tales como TACACS (Terminal Access Control Access Control System) y RADIUS. Cabe destacar que existen dos niveles de autentificación de usuario, el primero lo realiza el ISP antes de realizar el túnel y una vez creado, la segunda autentificación la realiza el gateway o servidor de la empresa privada.

CAPITULO 4. PROTOCOLOS DE CAPA 3

4.1 IPSec (Protocolo de seguridad para redes IP)

4.1.1 Definición de IPSec

Internet Protocol Security, cuya traducción en español es Protocolo de seguridad en Internet. Es un estándar de la IETF (Internet Engineering Task Force) definido y análisis especifico en el RFC 2401.

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

IPSec puede implementarse como un mecanismo de tunelaje estándar (para redes IP), robusto y con posibilidades de expansión, el cual otorga seguridad tanto al protocolo IP de nivel de red como a protocolos de capas superiores.

Se puede usar cualquier protocolo IP sobre IPSec, creando túneles de trafico cifrados para conexiones VPN o simple cifrado entre computadores.

Sin embargo, su utilidad puede ir mas allá de las VPNs, ya que dentro de IPSec existe un registro central de intercambio de llaves de Internet IKE (Internet Key Exchange), con lo cual cada maquina en Internet podría comunicarse con otra usando cifrado y autentificación de alto nivel.

4.1.2 Usos y utilidades de IPSec

El protocolo actual de Internet IPv4 (Protocolo de Internet versión 4), no otorga por si mismo ningún mecanismo de protección a las transferencias de datos, ni siquiera puede garantizar que el remitente sea quien dice ser. Por lo tanto un buen mecanismo para remediar estas deficiencias en redes IP es IPSec, ofreciendo:

- Confidencialidad: Asegura que los datos se transmitan solo entre el emisor y el receptor, sin que hayan terceros que puedan llegar a acceder a esta información.
- Integridad: Garantiza que los datos no puedan ser cambiados en el camino, es decir además usando IPSec se contribuye a la eliminación de errores en el trafico de paquetes.
- Autenticidad: Permite un mecanismo de firma digital de datos de modo que el receptor pueda verificar que la firma corresponde a la persona que acredita ser la que los envió para certificar que los datos recibidos no son falsos.
- Protección a la réplica: Asegura que un transacción se pueda enviar solo una vez, a menos que se autorice su reenvío.

4.1.3 Componentes de IPSec

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

- Dos protocolos de seguridad: IP Authentication Header (**AH**) e IP Encapsulating Security Payload (**ESP**) que aportan los mecanismos básicos de seguridad dentro del trafico de los paquetes IP.
- Security Associations (**SA**): Especifican los servicios de seguridad y los parámetros negociados en cada trayectoria segura IP.
- Algoritmos que hacen posible la autentificación y encriptación:

Algoritmos de Autentificacion	Algoritmos de Encriptacion	Opciones de intercambio de Claves
HMAC - MD5	3DES (168 Bits)	ISAKMP/Oakley
HMAC - SHA1	DES (56 Bits)	X.509 con firmas DSS
	Blowfish (40-446 Bits)	Firma RSA
	CAST128 (40-128 Bits)	Encriptacion RSA

Tabla 2: *Componentes involucrados en el protocolo IPSec.*

La siguiente figura presenta la arquitectura del datagrama IPSec, donde se pueden observar los componentes de seguridad, además de los sistemas de manejo de llaves:

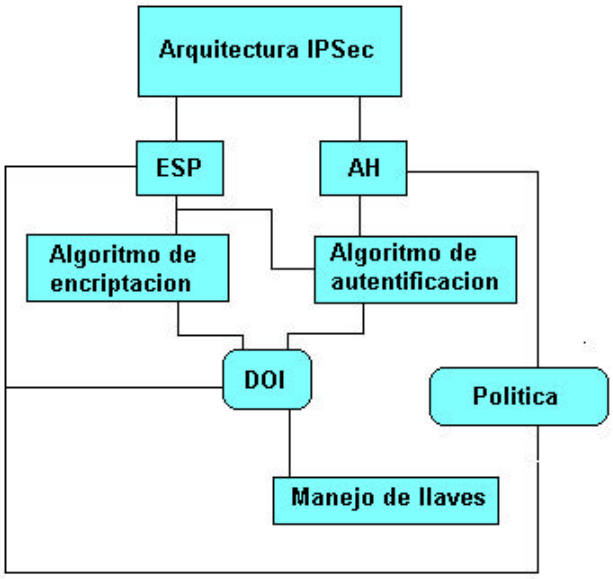


Figura 4-1. *Estructura del protocolo IPSec.*

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

- ***DOI (Domain of interpretation):*** Contiene parámetros necesarios para diversos documentos relacionados entre si. Estos incluyen identificadores para algoritmos de autentificación y de encriptación aprobados, así como también parámetros operacionales tales como tiempos de vigencia de llaves (key lifetime).

4.1.4 AH (Autentificación Header)

El protocolo AH (cabecera de autenticación) el cual esta incluido dentro del estándar IPSec, al aplicarlo o agregarlo al datagrama IP el cual se va a transmitir o recibir proporciona las herramientas necesarias para otorgar a la trama mecanismos que garantizan:

- Integridad: El datagrama no será alterado en forma inesperada o maliciosa.
- Autenticación: Verifica el origen del datagrama (nodo, usuario, red, etc.) y determina si proviene del usuario autorizado.

Sin embargo, no proporciona ninguna garantía de confidencialidad, es decir, los datos emitidos pueden ser vistos por usuarios no autorizados que estén en la red publica por donde viajan, ya que solo no puede aceptar formas de encriptación. AH esta orientado a mejorar la seguridad en la red publica en situaciones en que el uso de encriptación pueda ser ilegal o estar restringido a disposiciones del gobierno local.

4.1.4.1 Formato de la trama procesada mediante AH

La cabecera de autentificación AH se inserta entre la cabecera IP estándar (tanto Ipv4 como IPv6) y los datos transportados que pueden ser un mensaje TCP, UDP o ICMP e incluso un datagrama IP completo.
El datagrama final para Ipv4 es relativamente simple y además es opcional:

Figura 4-2. *Datagrama con autentificación AH.*

Nota: Se analizaran las tramas con mayor profundidad de acuerdo a los modos de funcionamiento IPSec.

El formato interno del encabezado AH es el siguiente:

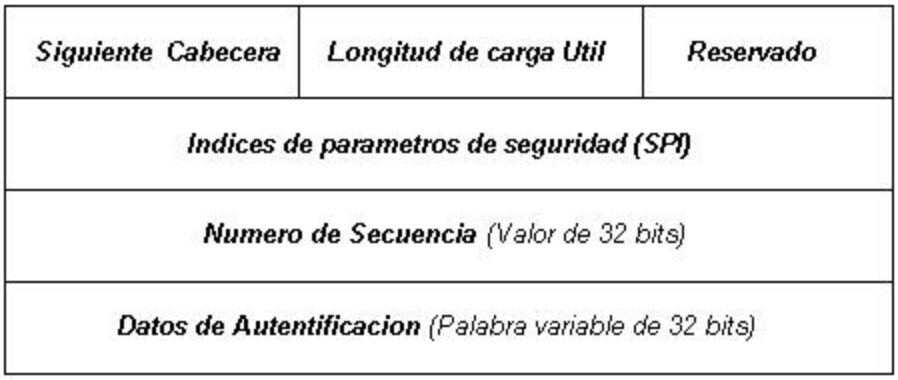


Figura 4-3. *Estructura del datagrama AH.*

Donde:

- ***Siguiente Cabecera:*** (1 byte) Identifica el tipo de dato de la carga útil, es decir el campo que sigue a AH.

- ***SPI:*** O índices de parámetros de seguridad, es un número arbitrario de 32 bits o 4 bytes que define para el receptor el grupo de protocolos de seguridad que se esta usando: algoritmos y claves así como la duración de estas últimas y sus correspondientes iteraciones periódicas para prevenir posibles ataques.

- ***Numero de secuencia:*** (4 bytes) Conocido anteriormente como prevención de repetición (Replay Prevention) es un numero que por medio de un contador va aumentando su valor en 1 cada vez que se aplica a un paquete consecutivo enviado a una misma dirección usando el mismo SPI. No solo mantiene el orden sino que también previene los ataques replay o sea cuando un atacante copia un paquete y lo envía fuera de secuencia para confundir a los extremos. La función antirepetición es opcional, es decir esta función va implícita en el datagrama con AH, pero el extremo receptor decide si hará uso de ella mediante una previa configuración. Aunque por su longitud de 32 bytes pueda llegar a 4.300 millones antes de

volver a comenzar, los contadores tanto del transmisor como del receptor deben resetearse antes de alcanzar el máximo. El reseteo implica establecer una nueva clave.

- ***Datos de autentificación:*** Mas conocido como MAC o ICV, tamaños máximos de 16 (MD5) o 20 (SHA-1) bytes. Estos son el compendio calculado (resultado del algoritmo de autentificación) que servirá al receptor para compararlo con el que obtenga luego de aplicar la misma función hash al datagrama.

AH es un protocolo IP relativamente nuevo, y como tal IANA le ha asignado el número decimal 51. Esto significa que el campo ***Protocolo*** de la cabecera IP tendrá el valor 51, en lugar de los valores 6 o 17 que se asocian a datos TCP o UDP, de esta forma será difícil descifrar que tipo de mensaje es el que se estará transmitiendo.

La trama IP autentificada con AH completa a transmitir presenta la siguiente forma:

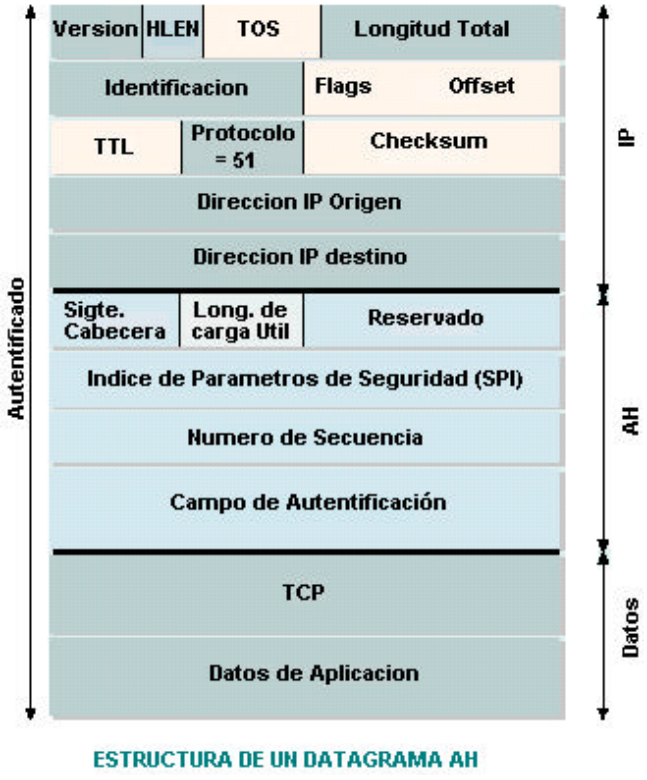


Figura 4-4. *Estructura del protocolo completo.*

El protocolo AH esta compuesto de la siguiente forma:

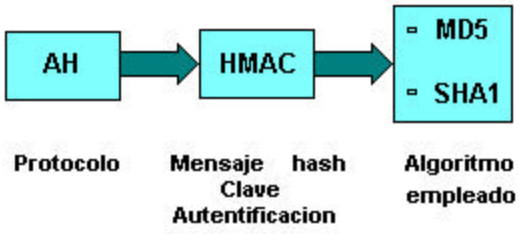


Figura 4-5. *Normas que componen AH.*

4.1.4.2 HMAC (Hashed Message Authentication Code)

El funcionamiento de AH se basa en un algoritmo HMAC, que corresponde a un código de autentificación de mensajes.

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

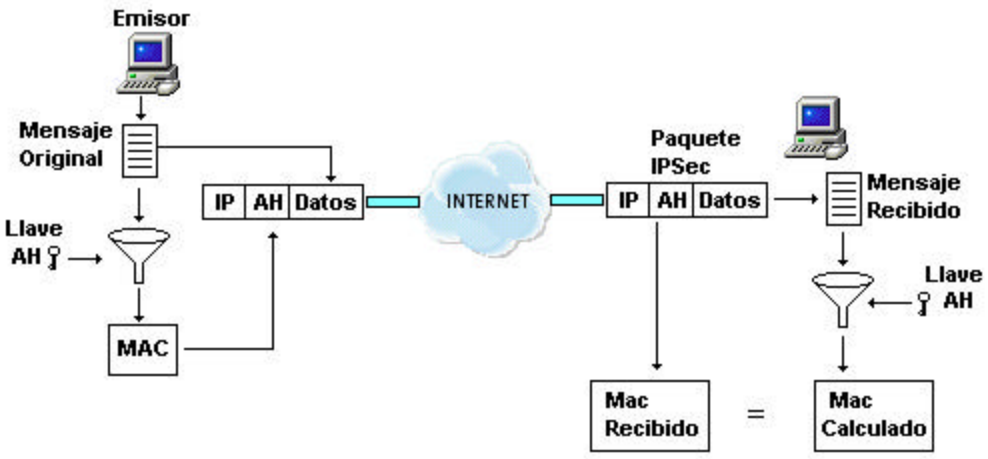


Figura 4-6. *Funcionamiento AH.*

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

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

Si son iguales el receptor tendrá la seguridad de que el paquete IP no ha sido modificado en el transito y que proviene efectivamente del origen esperado. Se debe reiterar de que el extracto (MAC) es imposible de calcular si no se conocen las claves que solo conocen el emisor y el receptor.

4.1.4.3 Funciones HASH:

Se han definido dos algoritmos o funciones Hash (o de dispersión) los cuales hacen posible la autentificación y es considerado obligatorio el uso de uno de ellos, según el estándar IPSec sobre HMAC.

MD5 (Message Digest 5) y SHA1 (Secure Hash Algorithm 1). Cuyos modos de operación se pueden contemplar en la siguiente tabla:

Operación MD5 o SHA1	**Funcionamiento**
Integridad	SHA-1 o MD5 produce una representación única comprimida o codificada de 160 o 128 bits respectivamente, correspondiente al datagrama que se desee transmitir. Si estas representaciones o compendios son iguales entre el emisor y el receptor, entonces el bloque de datos no tuvo alteración alguna durante la transmisión. Luego se decodifica la representación para llegar al mensaje original.
Autentificación	La autentificación es garantizada mediante uso de claves secretas cuando es calculado el mensaje codificado (representación codificada). Esta clave solo es conocida por el emisor y receptor. Dicha clave corresponderá a una serie de compendios de 16 bits por cada 64 bytes del datagrama a transmitir que será calculado entre los extremos. La serie de valores formados por los compendios de 16 bits se concatenan en un solo valor, el cual es colocado en el campo de autentificación del encabezado AH. Luego se comparan las claves y si coinciden los extremos están autentificados.

Tabla 3: *Propiedades de las operaciones HASH.*

4.1.4.4 Funcionamiento HASH:

Los textos y datos en general enviados electrónicamente pueden deformarse, bien por intervención de terceras personas, o bien por errores en las transmisiones. Para se utilizan funciones hash y de esta forma se asegura la autenticidad e integridad de los paquetes.

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

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

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

Figura 4-7. *Método de sustitución HASH.*

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

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

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

Figura 4-8. *Ejemplo de sustitución HASH.*

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

(1° - 2°) * 3° = resultado (integridad + autentificación)

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

Figura 4-9. *Resolución ejemplo de sustitución HASH.*

Luego se realiza la sumatoria de todos los resultados.

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

Entonces junto a la frase a transmitir se adjunta además el resultado de la operación Hash, el emisor al recibir esta información realiza la misma función Hash, y si coinciden los resultados (Ej. 4896) se puede establecer que los datos no han sido ni alterados ni vienen con errores, además el emisor – receptor acuerdan previamente la codificación y gracias a esto se puede asegurar que los mensajes vienen autentificados.

4.1.5 ESP (Encapsulating security payload)

El objetivo principal del protocolo ESP (*Encapsulación de seguridad de datos*) es proporcionar ***privacidad o confidencialidad***, para ello especifica el modo de cifrar los datos que se desean enviar y cómo este contenido cifrado se incluye en un datagrama IP. Adicionalmente, puede ofrecer los servicios de integridad y autenticación dependiendo del modo de funcionamiento.

4.1.5.1 Datagrama IP, procesada mediante ESP

Dado que ESP aporta mas funciones que AH, el formato de la cabecera es más complejo; este formato consta de una cabecera y una cola que enmascaran los datos transportados y de esta forma hacer los datos indescifrables a supuestas agresiones de terceros. Estos datos a transportar pueden ser cualquier protocolo IP (por ejemplo: TCP, UDP o ICMP).

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

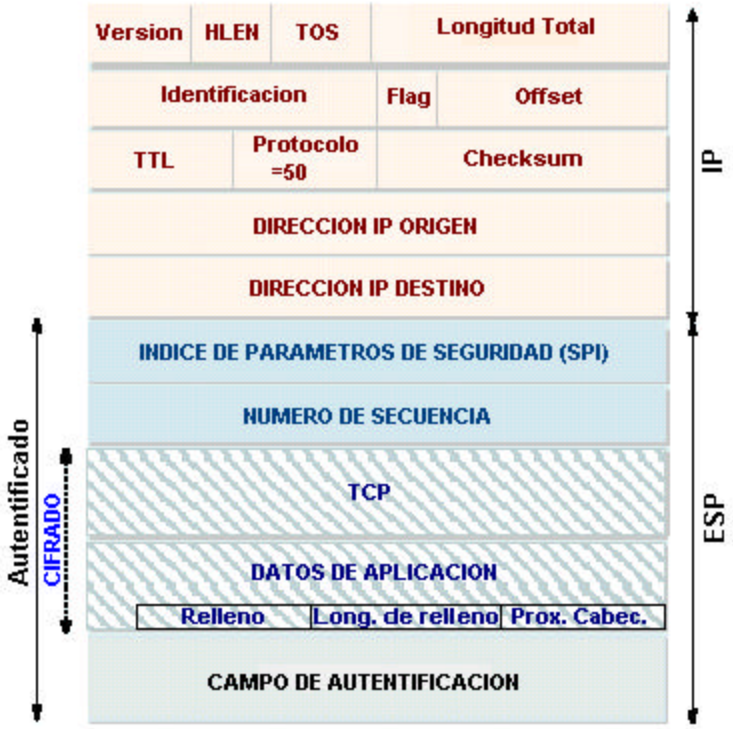


Figura 4-10. *Estructura del paquete procesado con ESP.*

En la figura 4-10 se puede observar que el encabezado ESP tiene los siguientes campos:

- ***SPI (Índice de parámetro de seguridad):*** Define para el receptor el grupo de protocolos de seguridad que se esta usando: algoritmos y claves así como la duración de estas ultimas y sus correspondientes iteraciones periódicas para prevenir posibles ataques. Tiene un tamaño de 4 bytes.

- ***Numero de Secuencia:*** Es un numero que por medio de un contador va aumentando su valor en 1 cada vez que se aplica a un paquete consecutivo enviado a una misma dirección usando el mismo SPI. Tamaño: 4 bytes.

La cola de ESP tiene los siguientes campos:

- ***Relleno:*** Es necesario por un lado si el algoritmo de encriptado requiere que el texto a encriptar sea un múltiplo de cierta cantidad de bytes (dado por ejemplo por el tamaño de los bloques con que trabaja). También es necesario para hacer que el encabezamiento hasta este punto tenga una longitud que sea múltiplo impar de 16 bits. De esta manera los dos próximos campos que siguen, de 8 bits cada uno, harán que el encabezamiento incluyéndolos sea un múltiplo de 16 bits.

- ***Longitud de relleno:*** Indica la longitud del campo anterior.

- ***Próximo encabezamiento:*** Este campo identifica el tipo de dato de la carga útil a encriptar. Bajo IPv4 identifica al protocolo de la capa superior usando la misma numeración de identificación del campo protocolo del IP original (es decir: 1 para ICMP, 6 para TCP, 17 para UDP, etc.)

- ***Campo de identificación:*** Estos son el compendio calculado (resultado del algoritmo de autentificación) que servirá al receptor para compararlo con el que obtenga luego de aplicar la misma función hash al datagrama.

El IANA ha asignado al campo *Protocolo* de la cabecera IP el valor decimal 50 cuando se utilice ESP. Por esta razón dentro del mensaje ESP se indica la naturaleza de los datos (*Próximo encabezamiento)*. Puesto que este campo, al igual que la carga útil, esta cifrado, un atacante que intercepte el datagrama no podrá saber que tipo de contenido es, y el objetivo de ocultar la información quedara cumplido.

4.1.5.2 Cifrado ESP

La función de cifrado dentro del protocolo ESP debe ser desempeñada por un algoritmo de cifrado de clave simétrica. Típicamente se usan algoritmos de cifrado bloque, de modo que la longitud de los datos a cifrar tiene que ser un múltiplo del tamaño de bloque (8 o 16 byte). Entonces el objetivo del campo de relleno dentro del campo *DATOS DE APLICACIÓN* el cual se analizo anteriormente, es ocultar la longitud real de los datos, y por tanto las características del trafico.

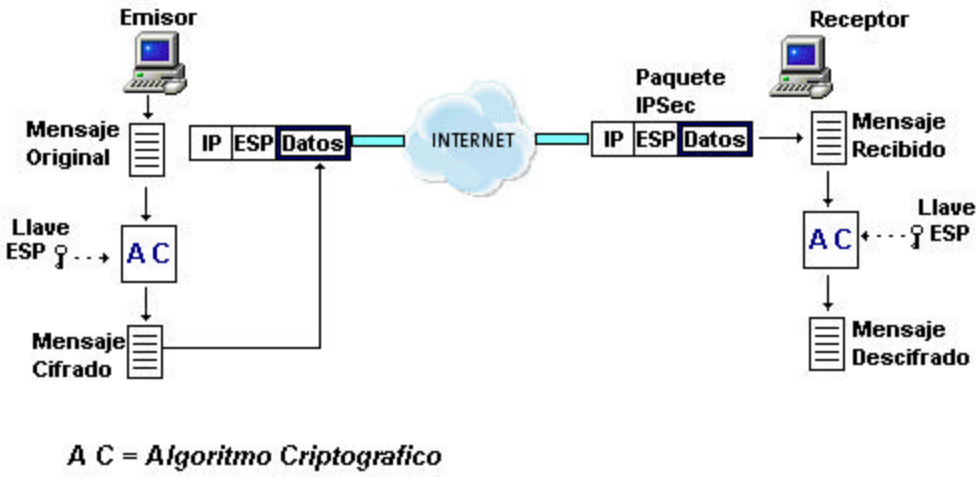


Figura 4-11. *Funcionamiento del paquete con trama ESP.*

En la figura 4-11 se representa como el protocolo ESP permite enviar datos de forma confidencial. El emisor toma el mensaje original, lo cifra, utilizando una clave determinada, y lo incluye en un paquete IP, a continuación de la cabecera ESP. Durante el transito hasta su destino, si el paquete es interceptado por un tercero solo obtendrá un conjunto de bit que no se podrán leer. El receptor aplica de nuevo el algoritmo de cifrado con la clave idéntica, recuperando los datos originales.

Cabe destacar que tanto la clave ESP como AH, la deben conocer únicamente el emisor y el receptor, por lo tanto para un hipotético atacante es casi imposible descifrar los datos sin tener conocimiento de la clave privada.

4.1.5.3 Tipos de Cifrado

- ***Cifradores de sustitución:***

En un cifrador de sustitución, cada letra o grupo de letras se sustituye por otra letra o grupo de letras para disfrazarlas. El cifrado más antiguo que se conoce es el cifrado de César, atribuido a Julio César. En este método se reemplaza una letra del alfabeto por la 3° que le sigue, entonces *a* ? D, *b* ? E, *c* ? F, …, y *z* ? C. Por ejemplo, la palabra *gato* se representa por JDWR. Una sencilla generalización del cifrador de César permite que el alfabeto cifrado se pueda desplazar k letras, en lugar de que siempre sean 3. En este caso, k se convierte en una clave para el método general de alfabetos desplazados circularmente. La siguiente mejora consiste en tener cada uno de los símbolos del texto en claro, digamos las 26 letras por simplicidad, correlacionadas con alguna otra letra, por ejemplo:

Texto en claro: a b c d e f g h i j k l m n o p q r s t u v w x y z
Texto cifrado: Q W E R T Y U I O P A S D F G H J K L Z X C V B N M

A este sistema general se le conoce como sustitución monoalfabética, en donde la clave está constituida por la cadena de 26 letras, correspondiente al alfabeto completo.

- ***Cifradores de transposición o permutación*:**

A comparación con los cifradores de sustitución, estos cifradores reordenan las letras pero no las disfrazan. En la siguiente figura se describe un cifrador de transposición común, el de tipo columna. La clave del cifrador es una palabra o frase que no contiene ninguna letra repetida. En este ejemplo, la clave es MEGABUCK. El propósito de la clave es numerar las columnas, en donde la columna 1 queda bajo la letra de la clave que se encuentra más próxima al comienzo del alfabeto, y así sucesivamente. El texto en claro se escribe horizontalmente, en renglones.

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

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

Tabla 4: *Ejemplo de cifrador de permutación.*

Se elige un bloque de caracteres que formen una matriz de 8 * 8, luego se sitúan horizontalmente en esta (letras en azul) incluyendo los espacios entre palabras.

Texto en claro: “necesita lanzar sus nuevos servicios al mercado antes que sus co”

Texto cifrado: “en ssceuszne asstrevloqcelusien cas ortsa vi oun socmaeiaurad ”

Se puede percibir en el ejemplo anterior que con este método de cifrado solo se ha desordenado la frase con la palabra clave que se ha acordado. La tecnología de clave proporciona servicios de cifrado que aseguran las transmisiones en la red en entornos abiertos.

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

- ***Cifrado simétrico*:** A los métodos de cifrado de clave privada se les denominan códigos simétricos y consisten en codificar la información con una clave que tanto el emisor como el receptor conocen y mantienen en privado. Una vez cifrado el mensaje, es ilegible y puede ser transmitido por medios no seguros. Este sistema da por hecho que

dicho intercambio de clave ha sido realizado por algún medio seguro, pudiéndose utilizar para ello métodos de claves públicas en conjunción con los métodos de claves privadas.

- ***Cifrado Asimétrico***: Por otra parte, los métodos de cifrado de clave pública o códigos asimétricos consisten en la creación de dos claves relacionadas para cada usuario. Una se mantendrá en privado y la otra se sitúa en un área de pública. Cuando un usuario desea enviar un mensaje confidencial a otro usuario, cifra el mensaje con la clave pública del receptor y luego el receptor decodifica el mensaje con su clave privada. Los mensajes cifrados con una clave pública sólo pueden ser descifrados con una clave privada. Es conveniente señalar que si la parte del documento o la parte de la firma es modificado, aunque sea ligeramente, entonces, el procedimiento de autenticación indicará que el documento no es autentico. Si una llave pública autentica un documento firmado, entonces quiere decir que el documento fue firmado con la correspondiente llave privada.

4.1.6 Algoritmos de Cifrado

Para cifrar los datos el protocolo ESP puede usar diversos algoritmos de cifrado los cuales tienen funcionamientos que difieren escasamente entre si, por esta razón se analizaran los más importantes:

4.1.6.1 DES (Estándar de encriptación de datos)

Creado en 1977 con el objeto de proporcionar al publico en general un algoritmo de cifrado normalizado para redes de ordenadores.

Se basa en un sistema monoalfabético, con un algoritmo de cifrado consistente en la aplicación sucesiva de varias permutaciones y sustituciones.

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

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

Como la clave efectiva es de 56 bits, son posible un total de 2 elevado a 56 = 72.057.594.037.927.936 claves posibles, es decir, unos 72.000 billones de claves, por lo que la ruptura del sistema por fuerza bruta o diccionario es sumamente improbable, aunque no imposible si se dispone de suerte y una gran potencia de cálculo.

Sin embargo en la actualidad el sistema de cifrado DES se ha considerado poco practico debido a que produce una longitud de clave corta e invariable, y los nuevos equipos pueden llegar a tener la potencia para descifrarlas.

4.1.6.2 3DES (Estándar de encriptación de datos)

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

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

Para implementarlo, se toma una clave de 128 bits y se divide en 2 diferentes de 64 bits, aplicándose el siguiente proceso al documento en claro:

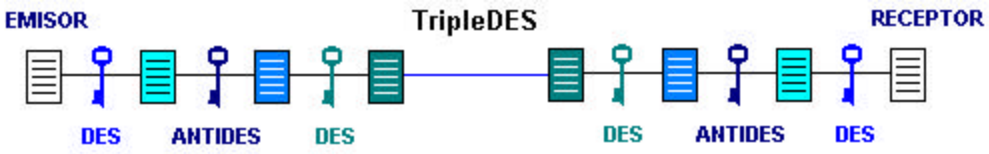


Figura 4-12. *Mensajes con TripleDES.*

Proceso de Cifrado:

1. Se aplica al documento a cifrar un primer cifrado o encriptación mediante la primera clave, C1.

2. Al resultado (ANTIDES) se aplica un segundo cifrado con la segunda clave, C2.
3. Y a este último resultado se vuelve a aplicar la clave inicial C1, produciéndose un tercer cifrado.

En el extremo RECEPTOR se aplica el proceso inverso para descifrar el mensaje original.

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

Nota: Actualmente 3DES usa tres claves diferentes (C1, C2 y C3), lo que hace el sistema mucho más robusto, al conseguirse longitudes de 192 bits (de los cuales solo son efectivos 168 bits, el resto sirve para determinar paridad y así detectar errores).

4.1.7 Modos de funcionamiento IPSec

En primer lugar para describir los modos de funcionamiento IPSec se debe conocer el proceso de encriptación y desencriptación:

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

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

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

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

Luego de mencionar los procesos de encriptación se pueden mencionar los modos de funcionamiento IPSec.

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

- Modo Transporte.
- Modo Túnel.

La diferencia entre estos dos modos radica en la unidad que se este protegiendo, en el modo transporte se protege la carga útil IP (capa Transporte), en el modo túnel se protegen los paquetes (Capa de Red) y se pueden implementar tres combinaciones con los protocolos de IPSec: AH en modo Transporte, ESP en modo Transporte, ESP en modo Túnel.

4.1.7.1 Modo Transporte

En este modo los protocolos AH y ESP interceptaran los paquetes procedentes de la *capa de transporte* a la *capa de red,* y aplicaran la seguridad que haya sido configurada. Es decir en este modo el contenido transportado dentro del datagrama AH o ESP son datos de la capa de

transporte (por ejemplo, datos TCP o UDP). Por tanto, la cabecera IPSec se inserta inmediatamente a continuación de la cabecera IP (otorgada por la capa de red) y antes de los datos de niveles superiores que quieren proteger.

El modo transporte tiene la ventaja de que asegura la comunicación extremo a extremo, pero requiere que ambos extremos entiendan el protocolo IPSec.

- Si la política de seguridad define que los paquetes deben ser encriptados, se utiliza ESP en modo transporte.
- En el caso en que solo sea requerida la autentificación, se utilizara AH en modo transporte.

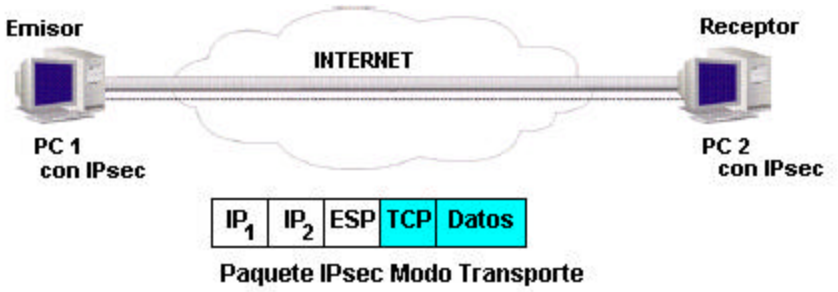


Figura 4-13. *Modo transporte entre 2 PC configurados como IPSec.*

En la figura 4-13 se representan dos equipos que entienden IPSec y que por lo tanto se comunican de forma segura. Esta comunicación se realiza en modo transporte, por lo tanto la información que se protege es únicamente el protocolo TCP o UDP, así como los datos de aplicación.

4.1.7.2 Modo Túnel

En este modo el contenido del datagrama AH o ESP es un datagrama IP completo (información original), incluida la cabecera IP original. Es decir el paquete es totalmente cifrado o encapsulado.

El proceso básicamente es el siguiente: Al paquete IP original se añade inicialmente una cabecera AH, ESP o ambas, posteriormente se añade una nueva cabecera IP que es la que utiliza para encaminar los paquetes a través de la red.

El modo túnel se usa normalmente cuando el destino final de los datos no coincide con el dispositivo que realizan las funciones IPSec.

El modo túnel es empleado principalmente por los Gateways (pasarelas) IPSec de una red local la cual desee comunicarse remotamente con objeto de identificar la red que protegen bajo una misma dirección IP, es decir los equipos de la red proyectaran una dirección origen o destino que coincide con la dirección IP del gateway de la red, ocultándose su propia IP.

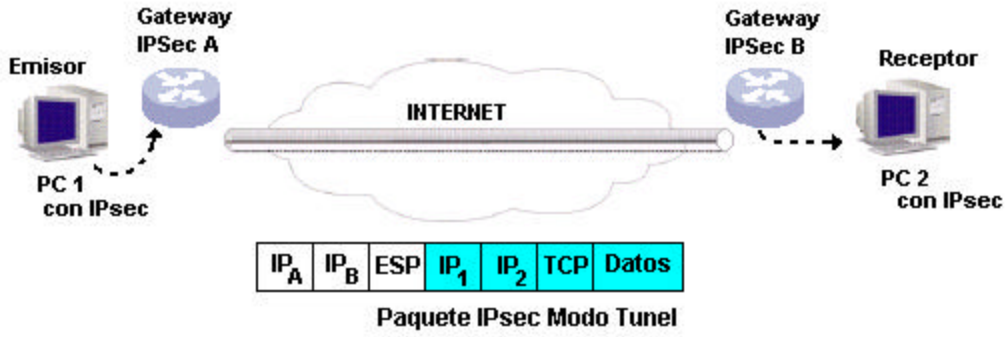


Figura 4-14. *Modo túnel entre 2 PC configurados como IPSec, usando Gateways de ruteo.*

En la figura 4-14 se observan dos redes que utilizan para conectarse gateways IPSec respectivamente, estos emplean una implementación en modo Túnel. La comunicación se realiza a través de la red publica INTERNET, entre un PC situado en la red local y otro situado en una red local remota, de modo que entre los gateways IPSec se establece un túnel a través del cual viajan protegidas las comunicaciones entre ambas redes locales. Sin embargo ambos PCs envían y reciben el trafico en claro (sin encriptar), como si estuviesen en la misma red local, los gateways son los que realizan el trabajo de encriptación y autentificación IPSec.

Cuando ESP es usado en modo túnel, las IP origen y destino se cifran como parte de la información, y las IPs de los gateways pasan a establecen la trayectoria de la comunicación. Además tanto la documentación TCP, UDP como los datos de aplicación son encriptados en este modo de funcionamiento.

4.2 Gestión y manejo de claves dentro de una asociación IPSec

4.2.1 SA (Asociaciones de Seguridad)

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

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

4.2.2 Administración de Claves

El intercambio de llaves tanto de autentificación como de encriptación de dos equipos que deseen establecer una conexión IPSec puede realizarse de dos maneras:

1. Manual:

   En forma manual se configuran los equipos que involucra la conexión IPSec, estableciendo secretos compartidos entre los extremos que se conectan. Es decir, a priori el conjunto emisor – receptor IPSec acordara una SA específica y la usara para autentificar los accesos y enmascarar los datos.
2. Automática:

   Esta forma establece automáticamente la asignación de las claves de la asociación IPSec, y el sistema considerado como norma tanto para Ipv6 como para IP versión 4 es el protocolo IKE.

4.2.3 Protocolo IKE (Intercambio de claves en Internet)

El IETF ha definido el protocolo *IKE* para realizar la gestión automática de claves como el establecimiento de las SAs correspondientes. IKE no es un estándar de IPSec, sino es una alternativa para negociar las claves en forma automática.

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

- ***ISAKMP:*** El protocolo de asociaciones de seguridad en Internet y manejo de llaves, se emplea para establecer, negociar, modificar y eliminar SA. Este define de forma genérica el protocolo de comunicación y la sintaxis de los mensajes que se utilizan en IKE.
- ***Oakley:*** Especifica la lógica de cómo se realiza de forma segura el intercambio de una clave entre dos entidades que no se conocen previamente. Oakley usa el algoritmo de intercambio de claves Diffie_Hellman (negociación punto a punto de claves), que corresponde a una técnica criptográfica de intercambio de llaves públicas que permite a cada sistema generar una llave secreta única en forma independiente basada en el conocimiento de cada una de las otras llaves públicas.

El principal objetivo del protocolo IKE consiste en establecer una conexión cifrada y autentificada entre dos entidades que deseen realizar una conexión segura, a través de la cual se negocian los parámetros necesarios para hacer uso de una asociación de seguridad IPSec. Esta negociación se lleva a cabo en dos fases:

1. La fase común a cualquier aplicación, en la que ambos nodos establecen un canal seguro y autentificado. Dicho canal seguro se consigue mediante el uso de un algoritmo de cifrado simétrico (encriptación de la información) y un algoritmo HMAC (autentificación del paquete). Las claves necesarias se derivan de una clave maestra que obtiene mediante un algoritmo mediante un algoritmo de intercambio de claves Diffie_Hellman. Este procedimiento no garantiza la identidad de los nodos, para ello es necesario un paso previo adicional de autentificación de la entidad.

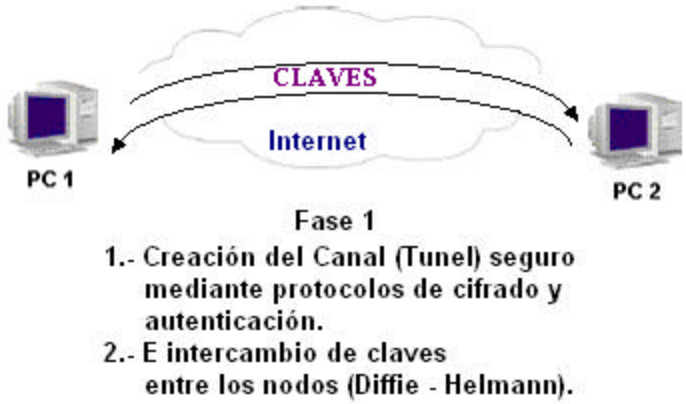


Figura 4-15. *Establecimiento de canal seguro y negociación de claves IKE.*

2. En la segunda fase el canal seguro IKE es usado para negociar los parámetros de seguridad específicos asociados al protocolo IPSec. Durante esta fase se negocian las características de conexión AH o ESP y todos los parámetros necesarios. El proceso comienza cuando el equipo que ha iniciado la comunicación ofrezca todas las posibles opciones que tenga configuradas en su política de seguridad y con las prioridades con que se hayan configurado. El sistema receptor aceptara la primera que coincida con los parámetros de seguridad que tenga definidos. Así mismo ambos nodos se irán informando a cerca del tráfico que van a intercambiar a través de dicha conexión.

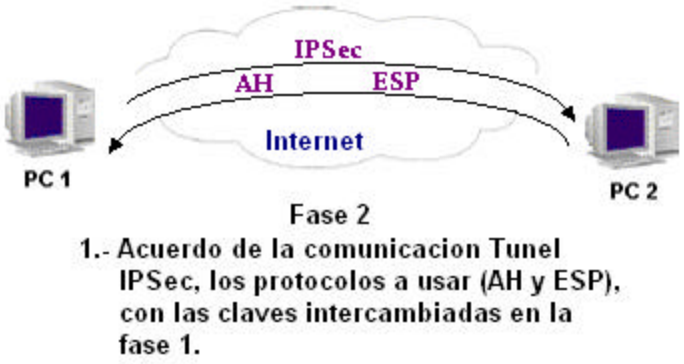


Figura 4-16. *Negociación de las claves IPSec.*

4.2.4 Certificados Digitales

Como antes se mencionó con la encriptación simétrica o cifrado simétrico, tanto el remitente como el destinatario cuentan con una llave secreta compartida. La distribución de la llave secreta debe ocurrir (con la protección adecuada) antes de cualquier comunicación encriptada. Sin embargo, con la encriptación asimétrica, el remitente utiliza una llave privada para encriptar o firmar digitalmente los mensajes, mientras que el receptor utiliza una llave pública para descifrar estos mensajes.

La llave pública puede distribuirse libremente a todos los que necesiten recibir mensajes encriptados o firmados digitalmente. El remitente necesita proteger cuidadosamente sólo la llave privada.

Para garantizar la integridad de la llave pública se publica con un *certificado*. Un certificado (o certificado de llave pública) es una estructura de datos que está firmada digitalmente por una autoridad certificadora (CA); una autoridad en la que los usuarios del certificado pueden confiar. El certificado contiene varios valores, como el nombre y el uso del certificado, la información que identifica al propietario de la llave pública, la llave pública misma, una fecha de expiración y el nombre de la autoridad certificadora. La CA utiliza su llave privada para firmar el certificado.

Si el receptor conoce la llave pública de la autoridad certificadora, el receptor puede verificar que el certificado sea, en efecto, de esa CA y, por lo tanto, que contiene información confiable y una llave pública válida. Los certificados se pueden distribuir de manera electrónica (a través de acceso al Web o correo electrónico), en tarjetas inteligentes o en discos flexibles.

Figura 4-17. *Encriptación de mensajes usando certificados digitales para la desencriptación.*

En resumen, los certificados de llaves públicas proporcionan un método conveniente y confiable para verificar la identidad de un remitente. IPSec puede utilizar de manera opcional este método para la autenticación de extremo a extremo, otorgando mayor seguridad a las futuras transacciones que sean realizadas, si se opta por esta alternativa.

4.3 Combinación entre IPSec y L2TP

Esta combinación es sumamente efectiva en términos de seguridad y compatibilidad de entornos de red, ya que:

- IPSec otorga seguridad de alto nivel en encriptación y autentificación, pero tiene la desventaja de que solo opera entre redes IP.
- Por el contrario L2TP se encarga de realizar túneles basados en el protocolo PPP, que soporta diversos protocolos de redes (ATM, Frame Relay, etc.)

Esta unión permite el trabajo en conjunto de ambos protocolos, siendo L2TP el medio de por el cual las tramas de información viajaran, formándose con esto el túnel o vía de transporte L2TP. La contribución de IPSec, determina el conjunto robusto de protocolos que permiten salvaguardar los paquetes VPN.

Y de esta manera se obtiene un resultado mucho mas amplio del concepta, ya que se otorga mayor seguridad y confiabilidad, en varios entornos de red. Tal como se puede observar en la figura 4-18:

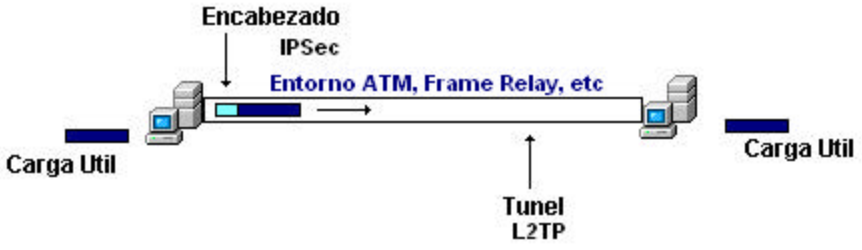


Figura 4-18. *Túnel combinado entre IPSec y L2TP.*

CAPITULO 5. CORTAFUEGOS (FIREWALL)

5.1 Definición de Firewall

Un cortafuegos es un sistema que impone una política de seguridad entre la organización de red privada e Internet. El cortafuegos determina cual de los servicios de red pueden ser accedidos dentro de esta por los que están fuera, es decir quien puede entrar para utilizar los recursos de red pertenecientes a la organización.

Un ejemplo de implementación de una red protegida se puede apreciar en el siguiente esquema:

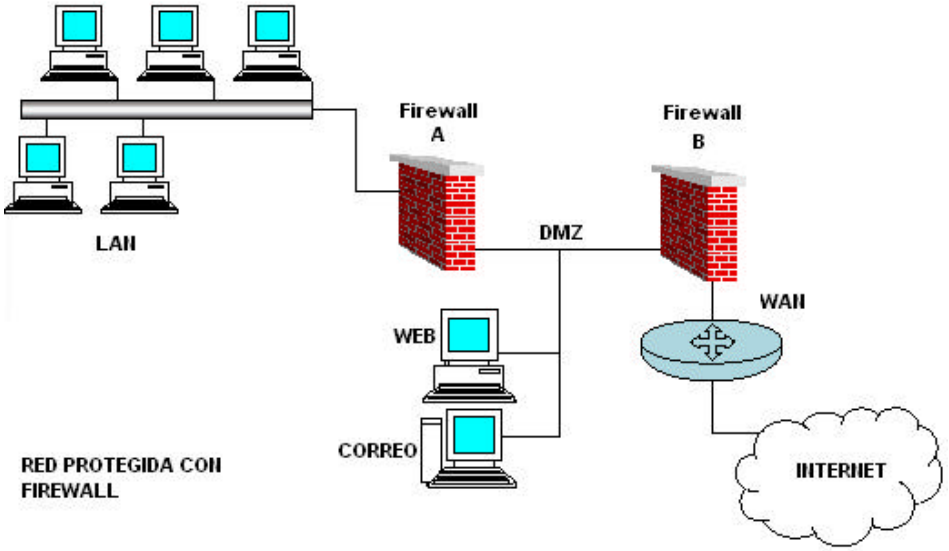


Figura 5-1. *Red protegida por Firewall, tanto para la red interna como para los DMZ.*

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

El equipo cortafuegos (Firewall) separa la red interna (Intranet) de la red publica (Internet), monitorizando y filtrando todas las conexiones de Internet a la red privada y viceversa en un único punto que será considerado como el punto fuerte de defensa.

Para el caso en que la red cuente con servidores dedicados (Web, FTP, CORREO, etc.) como en el caso de la figura, se agrega un cortafuego adicional el cual separa el DMZ (Zona desmilitarizada) de la red interna LAN y de la red externa INTERNET.

El Firewall B permite el tráfico al DMZ y del DMZ hacia fuera. El Firewall permite el tráfico saliente y entrante desde la red LAN a la Internet.

5.2 Filtrado realizado por los Firewall

Los cortafuegos monitorizan y filtran todo el tráfico, tanto entrante como saliente.

En principio existen tres técnicas de filtrado y monitorización del tráfico:

- Filtrado a nivel paquetes.
- Filtrado a nivel de aplicación (Proxy).
- Filtrado a nivel de conexión.

1.- Filtrado a nivel paquetes: El principio básico del filtrado a nivel de paquetes reside en el análisis de la información presente en las cabeceras de los paquetes IP, tomando las decisión de rehusar/permitir el paso de cada una de las tramas que son recibidas. Entre estos campos hay que destacar las direcciones IP fuente y destino, el puerto destino (TCP/UDP) y el tipo de paquete transportado. En este caso, la implementación puede llevarse a cabo por medio del router existente en la conexión a Internet y sus listas de acceso.

Consideraciones: La autenticación está basada en las direcciones IP, este método posee una baja fiabilidad (Ej.: suplantación de IP de autentificación) por lo cual no resulta el más adecuado en aquellos casos en los cuales el Firewall debe soportar autentificaciones de clientes externos, sin embargo este problema queda solucionado si existe un Servidor

VPN en la red corporativa o si el firewall posee servicios VPN, filtrando a los paquetes IP entrantes.

2.- Filtrado a nivel de Aplicación: La base principal de los cortafuegos con filtrado a nivel de aplicación (Proxy) reside en el bloqueo de la totalidad del tráfico a nivel IP entre la red interna e Internet. Los clientes internos establecen una conexión con el cortafuegos y a partir de ese momento dialogan con un servidor (Proxy) presente en éste en lugar de hacerlo directamente con el servidor de Internet. El Proxy actúa como intermediario de la comunicación, comprobando los permisos de los clientes y en su caso, realizando la conexión al servidor remoto en Internet. En principio, este tipo de cortafuegos ofrece el nivel más alto de seguridad. No es necesario preocuparse por los huecos de seguridad en el protocolo IP dado que todo el tráfico a este nivel es bloqueado. Además, al trabajar a nivel de aplicación los proxies permiten la monitorización de los datos al igual que otros muchos servicios, extendiendo las capacidades de registro. En este caso, los clientes no precisan la resolución de nombres y direcciones dado que los servidores externos se encuentran representados por el Firewall. En el otro sentido, el Firewall permite la ocultación interna de la red siendo únicamente visible su interfaz por lo que tampoco es necesaria la resolución de nombres de los clientes internos. Además, permite la posibilidad de ejecutar software o efectuar los mencionados túneles que realicen conexiones con diferentes redes privadas en Internet. Para ello, es necesario el establecimiento de líneas virtuales (enlaces VPN) por las cuales los datos intercambiados viajen encriptados y autenticados (por ejemplo empleando IPSec).

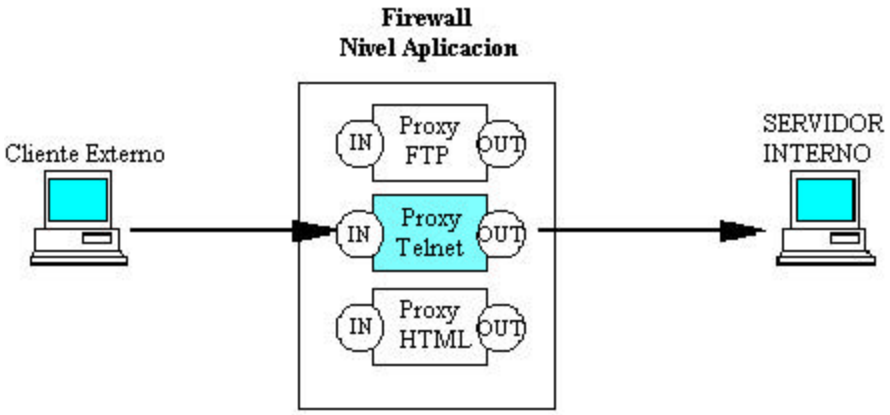


Figura 5-2. *Filtrado a nivel de aplicación (Proxy)*

En la figura anterior se puede visualizar que el Firewall chequea el acceso del Cliente Externo (remoto) a la aplicación Telnet, y si este no tuviese los permisos negociados seria imposible realizar dicha aplicación contra el servidor de la red local privada. En el caso de un cliente que estuviese dentro de la red privada, el trafico emitido/recibido siempre deben pasar por el Firewall Proxy, por lo tanto las aplicaciones están condicionadas a este.

Consideraciones: Aun no es posible disponer de un proxy genérico que sea capaz de soportar todos los servicios, sino que cada servicio dispone de su proxy (http-proxy, ftp proxy, etc.), lo que contribuye a la sobrecarga de aplicaciones al servidor de la red corporativa. Además, los proxies no son mecanismos transparentes dado que las aplicaciones deben configurarse para que establezcan su conexión al cortafuegos en lugar de a los servidores externos.

3.- Filtrado a nivel de conexión: El principio básico de los cortafuegos con filtrado a nivel de conexión no reside en el tratamiento sobre los datagramas IP, sino en el control de la conexión entre un cliente y un servidor. Su principal problema reside en la imposibilidad de realizar una autenticación fuerte dado que ésta es llevada a cabo empleando únicamente el nombre de usuario (protocolo SOCKS). En este tipo de filtrado no existe la posibilidad de realizar una monitorización de los datos intercambiados entre el cliente y el servidor: una vez establecida la conexión, el firewall actúa de una manera transparente. El hecho de que no sea capaz de implementar una mecanismo de autenticación fuerte unido a la no monitorización del protocolo cliente/servidor supone la principal diferencia con los cortafuegos de tipo Proxy. En la práctica, los cortafuegos son combinaciones entre las técnicas de filtrado a nivel IP, a nivel de aplicación y a nivel de conexión. La determinación estas técnicas dependerá del nivel de la flexibilidad, transparencia, y seguridad requerido.

5.3 Equipos firewall VPN

Para los tres alternativas de configuración de filtrado de los Firewall es necesario realizar configuraciones a nivel VPN, con el objeto de que el sistema de seguridad sea mas robusto. De esta forma los Firewall mas eficientes que existen en el mercado presentan condiciones VPN, los cuales son capaces de lograr las siguientes funciones fundamentales:

Autenticación: Prueba que el usuario es quien dice ser. Puede ser que la autenticidad se establezca al inicio de la conexión de red y luego se asuma que los siguientes mensajes de una dirección de red determinada se originan desde la parte autenticada, para esto cada cierto tiempo el Firewall comprueba identidad a través de los mensajes (procesados mediante un agente de cifrado) enviados por el extremo cliente.

Integridad de datos: Asegura que los datos no se modifican en tránsito. Se requiere autenticación de cada mensaje, sin importar el contenido del mismo. Estos se denominan mensajes seguros.

Privacidad de datos: Asegura que los datos no son leídos en tránsito. En este caso no sólo se autentica cada mensaje sino que también se encripta. Esta opción se realiza a través de protocolos VPN, y pueden ser corroboradas sus claves tanto por el servicio VPN como por los Firewalls instalados en la red corporativa.

A continuación se realizara la descripción y funcionamiento del equipo FIREWALL Cisco PIX que se presenta como una buena alternativa de soluciones VPN de seguridad en el mundo informático y empresarial.

5.3.1 Firewall Cisco PIX

El Firewall Cisco PIX es un equipo que ofrece amplias medidas de seguridad, al momento de ser configurado dentro de una red corporativa que brinde servicios tanto dentro de su propia infraestructura privada como en entornos públicos.

Figura 5-3. *Equipo Firewall Cisco PIX.*

El modo de funcionamiento de estos equipos radica en el principio de los equipos Firewall, los cuales filtran todos los flujos de información y datos que pretendan acceder a la Intranet, además de lograr niveles muy superiores de control de acceso.

Los PIX, pueden realizar túneles VPN hacia el exterior de la red que de todas maneras agiliza los procesos de los servidores de la red que estaban destinados a estas tareas, y estos tienen la capacidad de salvaguardar la integridad de la información e identificación tanto de los clientes internos como remotos de todo el entorno.

5.3.1.1 Características VPN

Estos equipos trabajan con el protocolo de capa 3 IPSec, y por lo tanto tienen licencia para operar con robustos protocolos de encriptación de tramas como 3DES, Diffie Hellman, y pueden autentificar mediante MD5 y SHA a uno o más usuarios de acceso remoto en forma local sin necesidad de contar con un servidor RADIUS o TACACS.

Tienen la capacidad de crear 10 túneles IPSec, tanto VPN Lan to Lan, como Clientes VPN de acceso remoto.

Cisco PIX, puede ocupar una base de datos local para autenticar usuarios, o también definir un servidor TACACS o RADIUS externo, para que autentique a los usuarios que en uno u otro escenario deben ingresar User y Password, como por ejemplo para Cliente VPN, PDM, Telnet, SSH, etc.

5.3.1.2 Acceso remoto VPN

Para acceder a un Firewall Cisco PIX de una red privada, el usuario remoto deberá contar con una cuenta de acceso, la cual deberá pasar por todas las pruebas de autentificación antes mencionadas. Estas pruebas tendrán éxito solo cuando se realicen las respectivas configuraciones tanto en el Firewall PIX, como en el equipo remoto del usuario VPN.

Cabe destacar que dicha configuración otorgara las autorizaciones que tenga el cliente remoto sobre la monitorización del PIX, es decir existirán clientes con el privilegio de realizar mantención remota del PIX como otros que ni siquiera tengan acceso a sus opciones, todo dependerá del permiso que se haya pre-configurado.

Una vez que el acceso haya traspasado los niveles implementados por el PIX, el usuario remoto tendrá todos los beneficios de la red interna local que se hayan autorizado. Y los propios clientes internos podrán acceder a otros puntos remotos sin la necesidad de exponerse ante posibles ataques en medios no protegidos de la red.

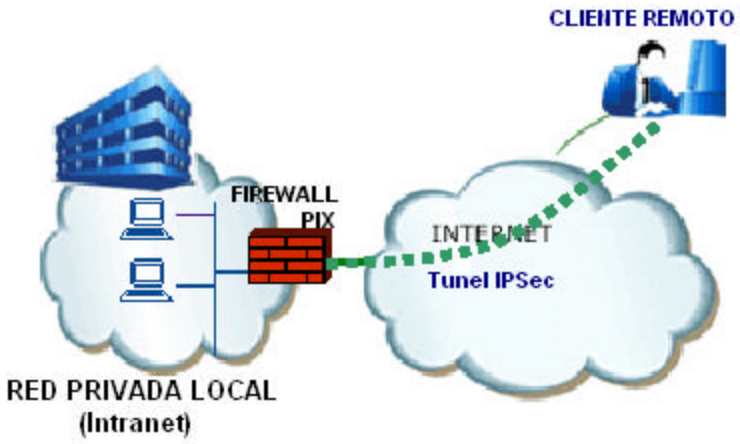


Figura 5-4. *Cliente remoto PIX, comunicándose en forma privada con red privada PIX.*

5.3.1.3 Enlace punto a punto

En el caso en que se desee realizar un enlace punto a punto o multipunto, entre sucursales remotas se deberá hacer uso de un Firewall PIX en cada uno de los extremo de entrada al medio publico. Este se efectúa con el objeto de otorgar mayor seguridad tanto al nodo emisor como el receptor.

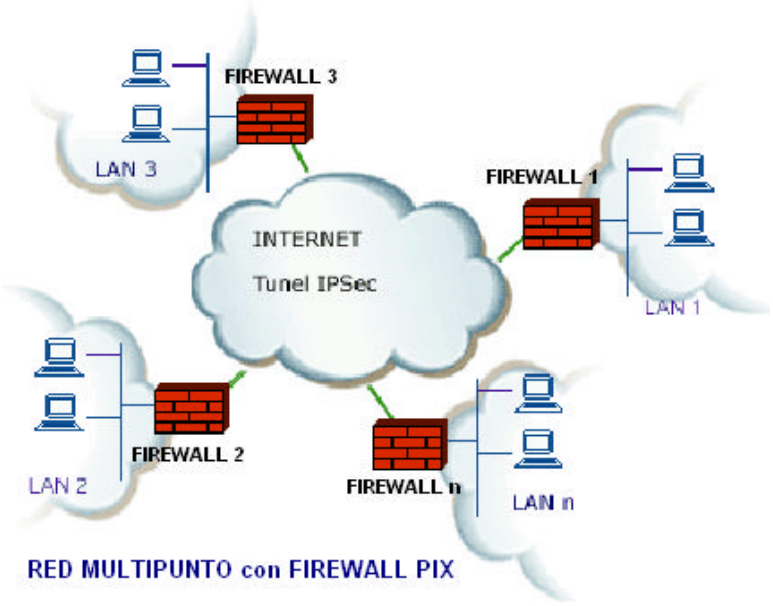


Figura 5-5. *Red multipunto con políticas de seguridad IPSec de Firewall Cisco PIX.*

CAPITULO 6. APLICACIÓN VPN

6.1 Acceso remoto, seguro y privado mediante túnel IPSec realizado por firewall Cisco PIX.

6.1.1 Configuración del acceso remoto VPN en el Firewall PIX

Para realizar la configuración en el Firewall Cisco PIX de un cliente de acceso remoto mediante la interfase de administración por http o PDM (Herramienta de administración por http del PIX), en primer lugar se requiere que este habilitado el *servidor http* (vía comandos) del Firewall y además que la IP del equipo que se destina para hacer la configuración, este autorizado a usar esta herramienta.

Nota: Se configurará un acceso remoto VPN (o Cliente VPN), con versión de PDM 3.0 y en el caso del software usado para el cliente Remoto, un VPN Remote Access 3.6.

El Software VPN de Cisco es gratuito y se puede bajar desde la página de Cisco, Existen versiones para Windows 9X, 2000, XP, etc. Para descargar software VPN cliente, se requiere un registro en la página de Cisco, luego ingresar al sgte. link: http://www.cisco.com/cgi-bin/tablebuild.pl/vpnclient-3des

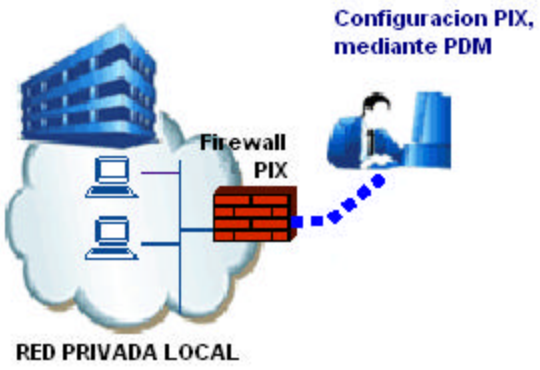


Figura 6-1. *Configuración del Cisco PIX, mediante un equipo PC con herramienta PDM.*

Existe además la posibilidad de usar el protocolo o aplicación SSH (Shell Seguro) en el equipo configurador, para realizar la habilitación en el Firewall Cisco PIX del acceso Cliente

Remoto. Pero solo acepta comandos, tal como la aplicación Telnet. Esta aplicación se contempla en este documento en ANEXO.

Paso 1:

El primer paso de la configuración es la creación el grupo VPN, que será etiquetado como el nombre del túnel especifico. Para este caso se elige:

Group Name: VPN_01

Password: vpn_01

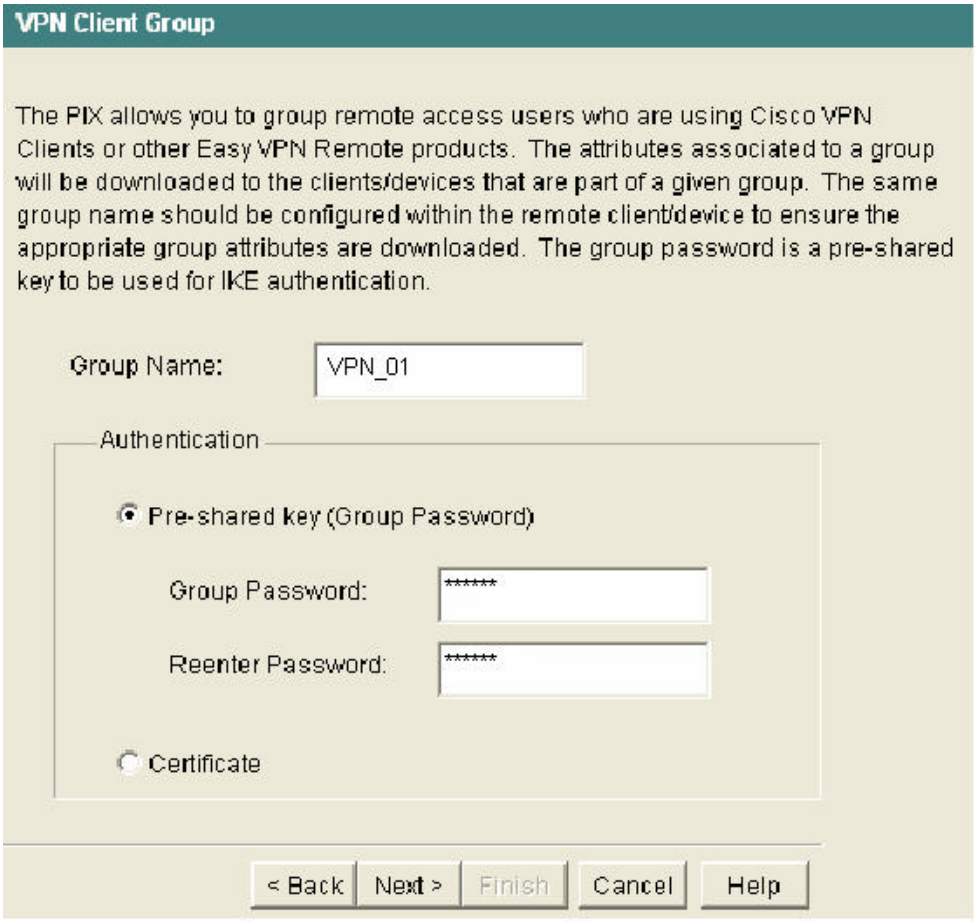


Figura 6-2. *Configuración del grupo VPN y contraseña con su respectiva confirmación.*

Paso 2:

Luego es necesario crear un usuario que será autentificado en forma local por el Firewall PIX, una vez que se conecte mediante el software VPN:

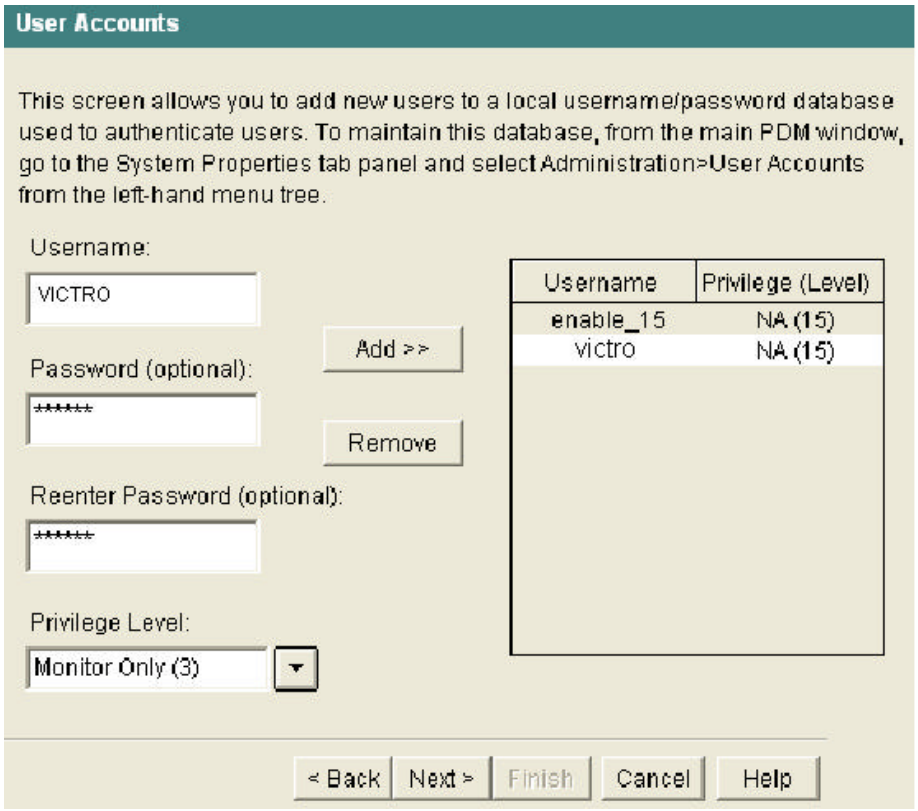


Figura 6-3. *Habilitación del cliente remoto, mas su contraseña de acceso.*

Paso 3:

La configuración de los protocolos IPSec de acceso VPN de un cliente remoto, consta de 2 fases:

- Negociación IKE (Fase 1): Esta fase establece los protocolos que se usaran para el intercambio de claves para el nuevo enlace VPN. Donde se contemplan las claves para la autentificación SHA o MD5, encriptación 3DES y el grupo Diffie Hellman para el intercambio entre el nodo Firewall PIX y el Cliente.
- Túnel IPSec (Fase 2): En esta fase se especifican los protocolos IPSec que se utilizaran en todo el enlace, además de las claves para autentificación y encriptación. Este traspaso de

información esta respaldado por la fase 1. De esta forma la configuración IPSec es indescifrable para terceras personas.

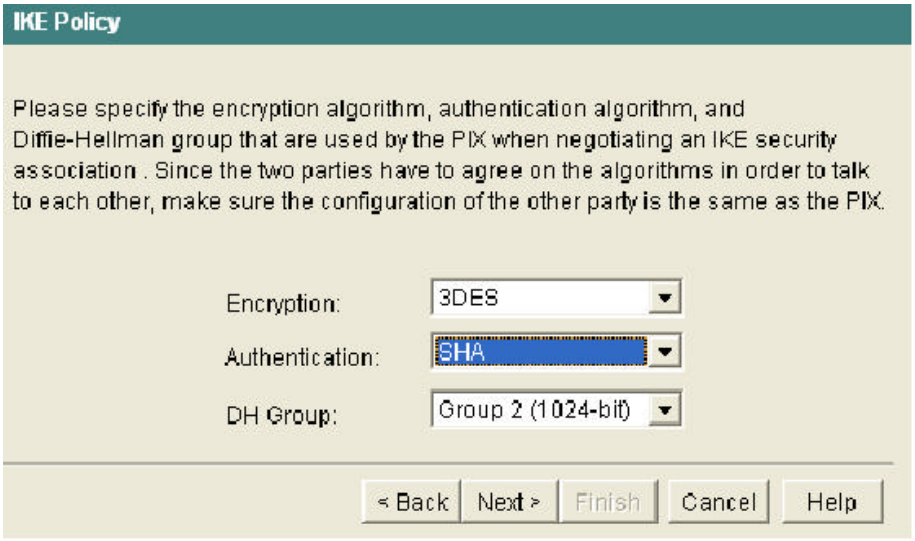


Figura 6-4. *Configuración de fase 1, de negociación IKE.*

Selección IKE:

- Encriptación: 3DES
- Autentificación: SHA
- Diffie_Hellman: Grupo 2 (1024 bits).

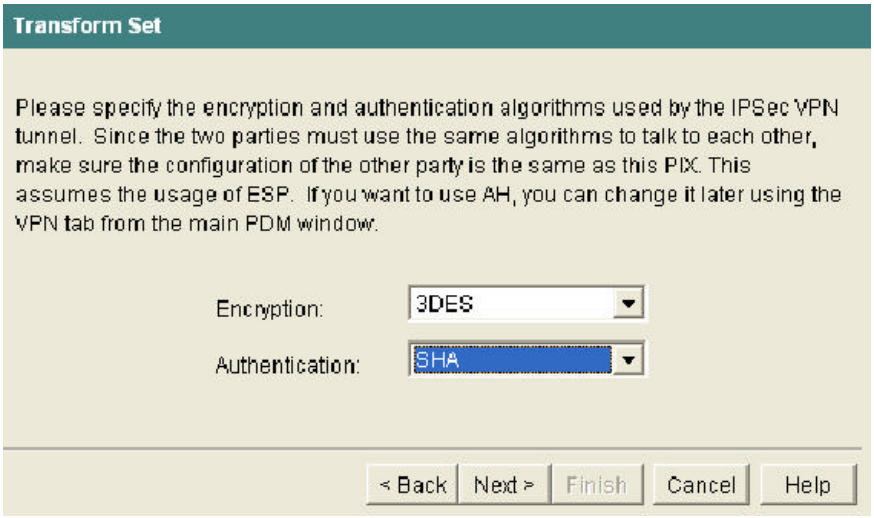


Figura 6-5. *Configuración de fase 2, de parámetros IPSec.*

6.1.2 Configuración del cliente VPN

Para realizar la conexión como Cliente VPN, es necesario:

- Un acceso a Internet, ya sea conmutado (MODEM) o xDSL.
- Tener instalado el software Cliente VPN 4.0, el cual se puede obtener del sitio que ha sido enunciada anteriormente.
- Poseer las claves del cliente.
- Las rutas privadas del servidor de acceso a la red.

Paso 1:

Como en cualquier aplicación de software ejecutable debe hacerse doble clic en la setup de la aplicación:

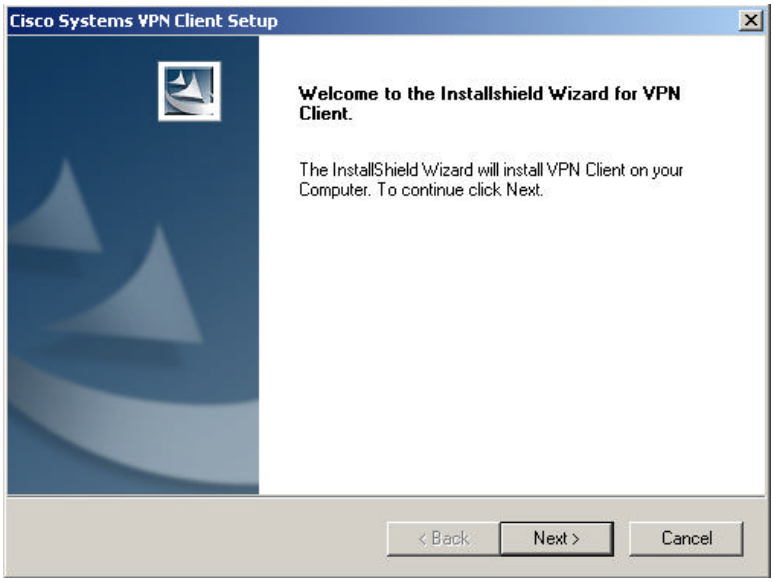


Figura 6-6. *Instalación de la aplicación VPN.*

Luego se realizan los pasos de rutina como aceptar los términos del contrato del software y dar un destino de ubicación en disco de la instalación, se despliega el estatus de instalación del software (Barra de porcentaje de la instalación). Para luego terminar la instalación donde se pide reiniciar el equipo para que los cambios se establezcan en el sistema del PC.

Nota: Dentro de la instalación del software este incorpora al sistema un adaptador virtual de VPN al sistema.

Paso 2:

Una vez instalado el software en el sistema se procede a crear la conexión del cliente remoto al servidor privado (Firewall PIX) de la red corporativa:

- Primero se clickea el icono de acceso de la aplicación cliente VPN instalado en el PC del cliente, donde aparece la siguiente ventana:

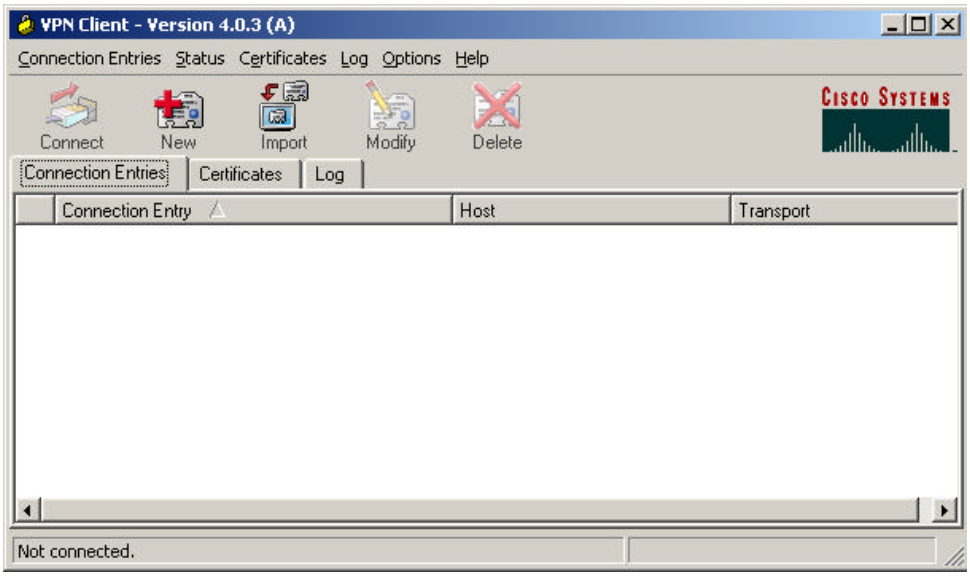


Figura 6-7. *Creación del acceso VPN.*

Es necesario mencionar que no hay conexión acceso existente ya que la grilla esta vacía, además la barra de estatus indica que el equipo no esta conectado.

- Luego se pincha dentro de la aplicación el icono NEW, para realizar una nueva conexión al servidor Firewall. La cual se utilizara cada vez que el cliente remoto se necesite conectar como VPN.

- Al realizar esta acción aparece una ventana donde se confirmara el grupo de trabajo antes creado dentro de la configuración del FIREWALL con las ID específicos además de las contraseñas de acceso.

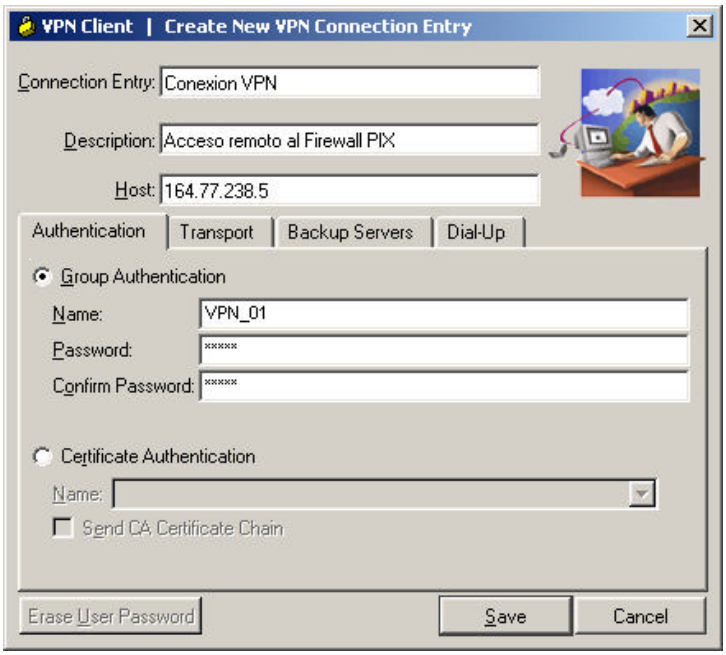


Figura 6-8. *Confirmando el grupo de trabajo para el acceso a la VPN.*

Cabe destacar que para este paso de creación del Cliente VPN, se debe especificar la IP valida del Firewall PIX (Host), ya que es esencial para el ruteo de la sesión. Además para esta aplicación no utilizare certificados digitales, ya que estas aplicaciones son más utilizables para niveles empresariales.

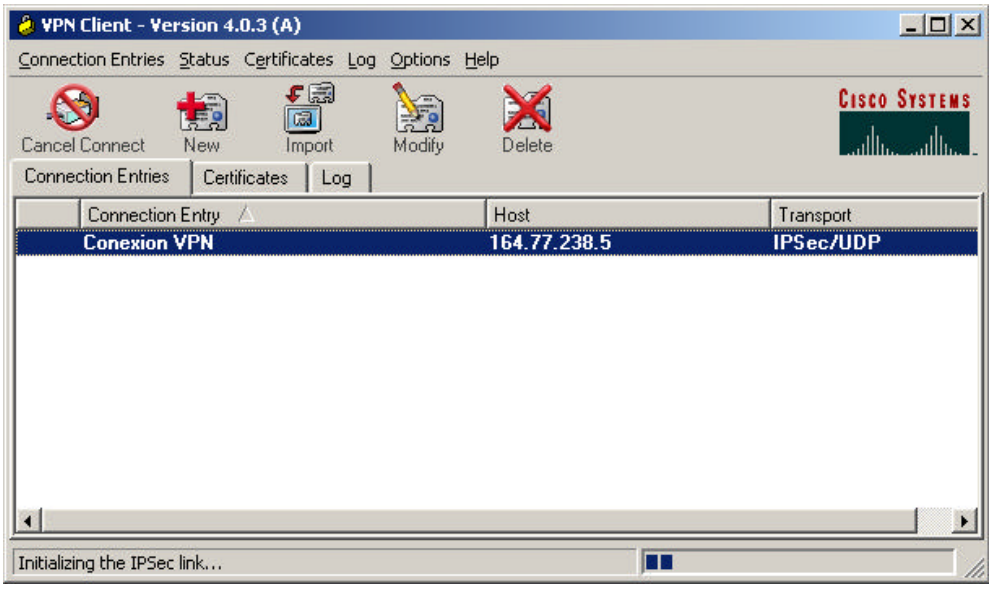


Figura 6-9. *Intentando la conexión al host: 164.77.238.5*

Luego pedirá el nombre ID de autentificación más el password de acceso, el cual fue previamente configurado en el Firewall como:

ID: Victro
Password: Victro

En estos momentos el equipo Cliente VPN, ocultara la IP que le dio el ISP, y tendrá una nueva que apuntara al Host: 164.77.238.5. Logrando la conexión privada si es que se han establecido los permisos pertinentes.

Los equipos que están dentro de la red corporativa ocuparan IP privadas, y solo desde el Host servidor se podrá acceder a ellas. Yo personalmente me conecte a un servidor Web que estaba detrás del Firewall con IP: 10.0.0.5

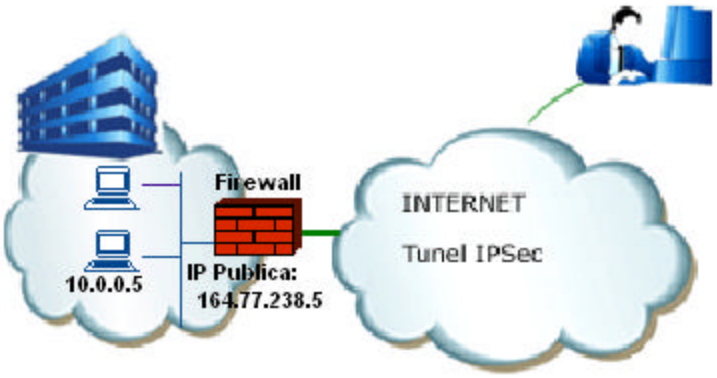


Figura 6-10. *Establecimiento del enlace VPN, entre cliente VPN y el Firewall de la red corporativa.*

Y a partir de este momento se pueden ejecutar aplicaciones propias dentro de una red privada como compartir archivos, impresoras, video conferencia, voz, aplicaciones remotas, etc. Pero con la gran diferencia de que tales aplicaciones nadie mas podrá descifrar sin importar de que estas se transmitan en un medio publico como lo es la Internet, ya que estas están encriptadas.

Inconveniente: He notado en esta aplicación que las aplicaciones entre mi PC remoto, y el servidor Web situado después del Firewall momentos de lentitud, debido al trabajo de cifrado y encriptación que se realiza en el servidor de resguardo. Pero de todas maneras para prácticas de alta delicadeza y confidencialidad es necesario asumir estos sacrificios.

CAPITULO 7. CONCLUSIONES

Uno de los mayores cambios tecnológicos se presentan en el ámbito de las comunicaciones, y principalmente en las redes de datos, que se han ido transformando en medios esenciales para realizar transacciones, interacciones multimediales, operaciones cotidianas, etc. Y de una u otra forma facilitan las operaciones tanto laborales, como de interés personal. De esta forma gracias a este trabajo he podido corroborar la importancia de los sistemas de datos, y como se estudian cada día nuevas tecnologías para ser implementadas y probadas, creándose tanto para generar necesidades como para dar soluciones a los problemas existentes.

He podido comprobar además que una de las mayores inquietudes actuales es velar por la seguridad de los sistemas e información que se transmiten por los medios de difusión de datos, ya que así como hay organizaciones y personas que contribuyen al avance de la seguridad, existen entes con actitudes malintencionadas que siempre intentaran invadir y dañar los archivos, además de infectar los sistemas.

VPN es una robusta combinación entre seguridad e interoperabilidad, que cada vez mas se ofrece como solución a las organizaciones en crecimiento y expansión. Ya que estas otorgan altos niveles de seguridad dentro de un medio de transmisión publico, y permiten reemplazar enlaces dedicados que requieren grandes inversiones para su establecimiento. Por lo tanto dado sus ventajas en función a cada nivel de seguridad que requiera una organización es recomendable establecer este tipo de tecnología.

Los protocolos que componen las funciones VPN estudiados en este trabajo de titulaciones ofrecen cada uno diferentes normas de operación, con niveles diferentes tanto en seguridad como en compatibilidad de sistema y entorno. Siendo el más destacable y además confiable para ser utilizado el protocolo IPSec, el cual se puede implementar en medios IP públicos como lo es la Internet, así se puede realizar una transmisión privada y por ende segura entre dos puntos separados remotamente sin perder la confiabilidad de un enlace punto a punto.

Hay diversos esquemas de implementación de VPN, los cuales varían según tamaño de la red corporativa y seguridad que requiera para sus servidores. Estos pueden estar basados en software o hardware, siendo estos últimos los más efectivos al momento de efectuar procesos de autentificación y encriptación, debido a que no adhieren sobrepeso a los servidores dedicados a los enrutamientos dentro de la propia red local, agilizando el trabajo dentro de esta. Además que manejar parámetros bastante potentes de seguridad que seria poco probable implementar como software.

Por otro lado el hecho de existir un ente regulador, que todo el tiempo este procesando claves y encriptaciones a los mensajes, provoca lentitud en los flujos bidireccionales. Pero con el avance de la tecnología nuevos y robustos procesadores dedicados a los hardwares con bancos de memoria muy potentes agilizaran estos procesos, dando más dinamismo a las conexiones de este tipo.

Por último, es conveniente a nivel empresarial invertir en una buena combinación VPN entre hardware y software para optar por la tranquilidad del sistema, y no sufrir ataques o acceso indeseados que pueden ocasionar efectos lamentables a todo el conjunto de recursos.

Bibliografía

LIBROS

[1]. Antonio Villalón, *Seguridad en Unix y Redes, Octubre 2000.*

[2]. Steven Brown, *Implementación de redes privadas virtuales*, Ed. McGraw-Hill 2000

RFC

[3]. S.Kent and R. Atkinson, *IP Authentication Header (AH),* RFC 2402, November 1998.

[4]. S. Kent and R. Atkinson, *IP Encapsulating Security Payload (ESP),* RFC 2406, November 1998.

[5]. D. Harkins, D. Carrel, Cisco Systems. *The Internet Key Exchange (IKE),* RFC 2409. Nov 1998

SITIOS WEB

[6]. www.pdos.lcs.mit.edu/~cananian/Projects/PPTP

[7]. www.certisur.com.ar/productos /vpn/

[8]. www.cisco.com

[9]. www.ns.racsa.co.cr/servicios/vpn

[10]. www.vpnlabs.org/

[11]. www.gulp.org.mx/articulos/vpn.html

[12]. www.cisco.com/en/US/products/sw/secursw/ps2120/products_configuration_guide_chapter09186a00800eb0b3

Anexo A: Glosario

Acceso Remoto — La capacidad de un ordenador en un emplazamiento para conectarse a un dispositivo en otro emplazamiento.

ADSL (Línea de Suscripción Asimétrica Digital) — Se refiere a una tecnología que esta implementada para mejorar el ancho de banda de los hilos del cableado telefónico convencional que transporta hasta 16 Mbps (megabits por segundo) gracias a una serie de métodos de compresión.

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

ARP (Address Resolution Protocol) — Un proceso con Protocolo de Control de Transmisión / protocolo Internet (TCP/IP) que dibuja las direcciones IP en las direcciones Ethernet; se necesita TCP/IP para su utilización con Ethernet.

ASCII (American Standard Code for Information Interchange) — Pronunciado asky. Un código de datos binarios, consistente en siete bits de datos más un bit de paridad o símbolos especiales, establecido por la ANSI, para la compatibilidad entre servicios de datos.

Asíncrono — Dos señales son asíncronas o no están sincronizadas, cuando sus correspondientes instantes significativos no coinciden. También es un término referido a una transmisión no sincronizada, en la cual el sincronismo entre emisor y receptor se establece de nuevo en el terminal, para cada carácter transmitido, mediante la recepción de un bit de arranque; se finaliza con un bit de parada. Es el modo típico para transmisiones en telegrafía, minicomputadores y ordenadores personales.

ATM (Asynchronous Transfer Mode) — Tecnología de red de alta velocidad que maneja datos, voz y video en tiempo real. ATM se define en el estándar Broadband RDSI (BISDN) y proporciona un ancho de banda ”bajo demanda” cargando a los clientes por la cantidad de datos que envían. Las velocidades son escalables, empezando con velocidades lentas de 2.048 Mbps con velocidades intermedias de 25, 51, y 100 Mbps, y con velocidades altas de 155, 622 Mbps, y hasta la gama Gigabit.

Backbone — Línea de transmisión de información de alta velocidad o una serie de conexiones las cuales conjuntamente forman una vía con gran ancho de banda. Un backbone puede conectar dos puntos o redes distanciados geográficamente a altas velocidades.

Bridge (Puente) — Unidad Funcional que interconecta dos redes de área local que utilizan el mismo protocolo de control de enlace lógico pero distintos protocolos de control de acceso al medio dentro del nivel 2 de OSI.

Browser — Aplicación para visualizar todo tipo de información y navegar por el ciberespacio que cuentan con funcionalidades plenamente multimedia. Como ejemplo de navegadores tenemos Internet Explorer y Netscape. Estos programas pueden también actualizarse a sus últimas versiones de forma gratuita.

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

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

Datagrama — Entidad de datos autocontenida e independiente que transporta información suficiente en orden de ser encaminada desde su ordenador de origen a su ordenador de destino sin tener que depender de que se haya producido anteriormente tráfico algunos entre ambos o la red de transporte.

Digital — Es una forma de representar la realidad mediante unas corrientes de valores finitos formadas por unos y ceros.

DNS (Domain Name System) — El "Sistema de Nombres de Dominio" es un servicio de búsqueda de direcciones IP de sistemas centrales (o hosts) basándose en los nombres de dominio de estos.

Dominio — Estructura jerárquica que organiza las máquinas de Internet de forma que sea fácil recordar su nombre.

Encriptado — Proceso de codificación y ocultación de paquetes de datos para impedir su lectura por terceros y asegurar la confidencialidad de determinadas transacciones.

Enlace (Link) — Apuntador de hipertexto que sirve para saltar a otra página web, a otro servidor, o a otro servicio (correo, FTP) cuando se navega por Internet.

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

Equipo Terminal de Datos — Se refiere por ejemplo al ordenador conectado a un módem que recibe datos de éste.

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

Ethernet — Tipo de red de área local desarrollada en forma conjunta por Xerox, Intel y Digital Equipment. Se apoya en la topología de bus, tiene ancho de banda de10 Mbps de forma que presenta una elevada velocidad de transmisión; y se ha convertido en un estándar de red corporativa.

Extrarred — Interconexión entre dos o más organizaciones a través de sistemas basados en la tecnología Internet. Web privada accesible externamente mediante claves de acceso.

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

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

Hacker — Persona que tiene un conocimiento profundo acerca del funcionamiento de redes de forma que puede advertir los errores y fallas de seguridad del mismo. Al igual que un cracker busca acceder por diversas vías a los sistemas informáticos pero con fines de protagonismo.

Host — En una red informática, es un ordenador central que facilita a los usuarios finales servicios tales como capacidad de proceso y acceso a bases de datos, y que permite funciones de control de red.

Hub — Equipo para diversos tipos de cables y para diversas formas de acceso que sirve de plataforma integradora para distintas clases de cables y de arquitectura.

IP (Internet Protocol) — El protocolo utilizado en gateways para conectar redes a Nivel de Red OSI (Nivel 3) y superiores. IP enruta un mensaje a través de la red.

IPX (Internet Packet Exchange) — Un protocolo de comunicación en Novell NetWare

que crea, mantiene y termina la conexión entre dispositivos de red, tales como estaciones de trabajo y servidores.

ISP (Internet Service Provider) — Organización que provee la conexión de computadoras a Internet, ya sea por líneas dedicadas o por líneas conmutadas. Es una entidad, habitualmente con ánimo de lucro, que además de dar acceso a Internet a personas físicas y/o jurídicas, les ofrece una serie de servicios (hospedaje de páginas web, consultoría de diseño e implantación de webs e Intranets, etc.).

ISDN (Integrated Services Digital Network) — Es el máximo organismo de normalización a nivel internacional con sede en Ginebra. Su **Technical Committe** 97 (TC97) es responsable del modelo de referencia de siete capas definidos para sistemas de comunicaciones directas (Véase OSI). Edita propuestas de normas internacionales "Draft International Standard (DIS)". Juntamente con el IEC son los dos organismos competentes para emitir normas internacionales.

Linux — Versión de libre distribución del sistema operativo UNIX el cual tiene todas las características que se pueden esperar de un moderno y flexible UNIX. Incluye multitarea real, memoria virtual, librerías compartidas, dirección y manejo propio de memoria y TCP/IP. Además, usa las características hardware de la familia de procesadores 386.

Protocolo de Control de Transmisión (TCP) — Forma de comunicación básica de Internet la cual hace posible que cualquier tipo de información (mensajes, gráficos o audio) viaje en forma de paquetes sin que estos se pierdan y siguiendo cualquier ruta posible.

Protocolo de Datagramas de Usuario (UDP) — Protocolo que no pide confirmación de la validez de los paquetes enviados por la computadora emisora. Este protocolo es actualmente usado para la transmisión de sonido y vídeo a través de Internet. El UDP está diseñado para satisfacer necesidades concretas de ancho de banda y como no reenvía los datos perdidos, es ideal para el tráfico de voz digitalizada debido a que un paquete perdido no afecta la calidad del sonido. Entre las aplicaciones que utilizan este protocolo encontramos a Real Audio.

Proxy — Servidor especial encargado, entre otras cosas, de centralizar el tráfico entre Internet y una red privada, de forma que evita que cada una de las máquinas de la red interior tenga que disponer necesariamente de una conexión directa a la red. Al mismo tiempo contiene mecanismos de seguridad (firewall o cortafuegos) los cuales impiden accesos no autorizados desde el exterior hacia la red privada. También se le conoce como servidor cache.

Sniffer (Husmeador) — Programa que busca una cadena numérica o de caracteres en los paquetes que atraviesan un nodo con el objetivo de conseguir alguna información y normalmente se usa con fines ilegales.

SNMP — Acrónimo de Simple Network Management Protocol. Protocolo estándar para la administración de red en Internet. Prácticamente todos los sistemas operativos, routers, switches, módems cable o ADSL módem, firewalls, etc. se ofrecen con este servicio.

Spoofing — Procedimiento que cambia la fuente de origen de un conjunto de datos en una red, por ejemplo, adoptando otra identidad de remitente con el fin de engañar a un servidor firewall.

Telnet — Servicio de Internet en el cual el usuario de conecta de forma remota a otro ordenador, como si se hiciera desde un terminal local.

UDP — Acrónimo de User Datagram Protocol. Protocolo dentro del TCP/IP que convierte mensajes de datos en paquetes para su envío vía IP pero no verifica que hayan sido entregados correctamente.

Anexo B: Modelo de referencia OSI

El modelo de referencia de Interconexión de sistemas abiertos OSI, es un conjunto de especificaciones que describe una arquitectura de red para conectar distintos dispositivos. Este modelo es la base para poder organizar, entender y monitorear los distintos tipos de protocolos y su ámbito de actuación.

El modelo OSI consta de 7 niveles o capas:

1.- Capa Física: A este nivel corresponde la determinación de las especificaciones correspondientes a las características mecánicas y físicas (conectores, cableado, etc.) requeridas para establecer, mantener y desactivar los enlaces físicos en un sistema de red.

2.- Capa de enlace de datos: Los protocolos de este nivel son los responsables de transmitir sin errores y establecer conexiones lógicas entre estaciones. Esto se consigue empaquetando los bits provenientes de la capa física en bloques de datos (tramas) y enviando estas tramas con la necesaria sincronización y orden. Este nivel realiza la detección y corrección de errores que puedan producirse en el nivel físico. Protocolos de esta capa son: Ethernet, Token Ring, Frame Relay, PPP, PPTP, L2TP, etc.

3.- Capa de Red: Los protocolos de este nivel son los responsables de las funciones de direccionamiento y control necesarios para mover los datos a través de la red. También tiene que establecer, mantener y finalizar las conexiones, incluyendo la conmutación de paquetes, el enrutamiento, la congestión de datos y la traducción de direcciones lógicas a direcciones físicas. Los protocolos mas importantes de este nivel son: IP, IPX, NetBeui, así como los protocolos de enrutamiento RIP, BGP, y por supuesto el protocolo de seguridad IP: IPSec.

4.- Capa de transporte: Este nivel asegura que los paquetes se entreguen sin errores, secuencialmente y sin pérdidas ni duplicaciones. Este nivel reempaqueta los mensajes, dividiendo los mensajes largos en varios paquetes. En la recepción se desempaquetan los mensajes, volviéndose a obtener los mensajes como antes de enviarse. Protocolos existentes en este nivel son: TCP, UDP y SPX, así como ARP, RARP y VoIP, entre otros.

5.- Capa de sesión: Este nivel permite que dos dispositivos distintos establezcan, usen y finalicen una conexión llamada sesión. Este nivel realiza además el reconocimiento de nombres y las funciones, como la seguridad, necesaria para permitir a dos aplicaciones comunicarse a través de la red.

6.- Capa de presentación: Este nivel determina el formato utilizado para intercambiar datos entre equipos en red. Se puede llamar el traductor de la red. En la etapa de emisión, este nivel convierte los datos desde un formato enviado por el nivel de aplicación a otro formato intermedio reconocido. En la recepción, este nivel convierte el formato intermedio a un formato útil para el nivel de aplicación del equipo receptor.
El nivel de presentación es responsable de convertir los protocolos, traducir los datos, codificar los datos, expandir los comandos gráficos, etc.

7.- Capa de aplicación: Este nivel sirve de ventana para que los procesos de aplicación tengan acceso a los servicios de red. Este nivel representa los servicios a disposición de las aplicaciones del usuario, como por el ejemplo el software para servicios FTP, para el acceso a base de datos y para correo electrónico.

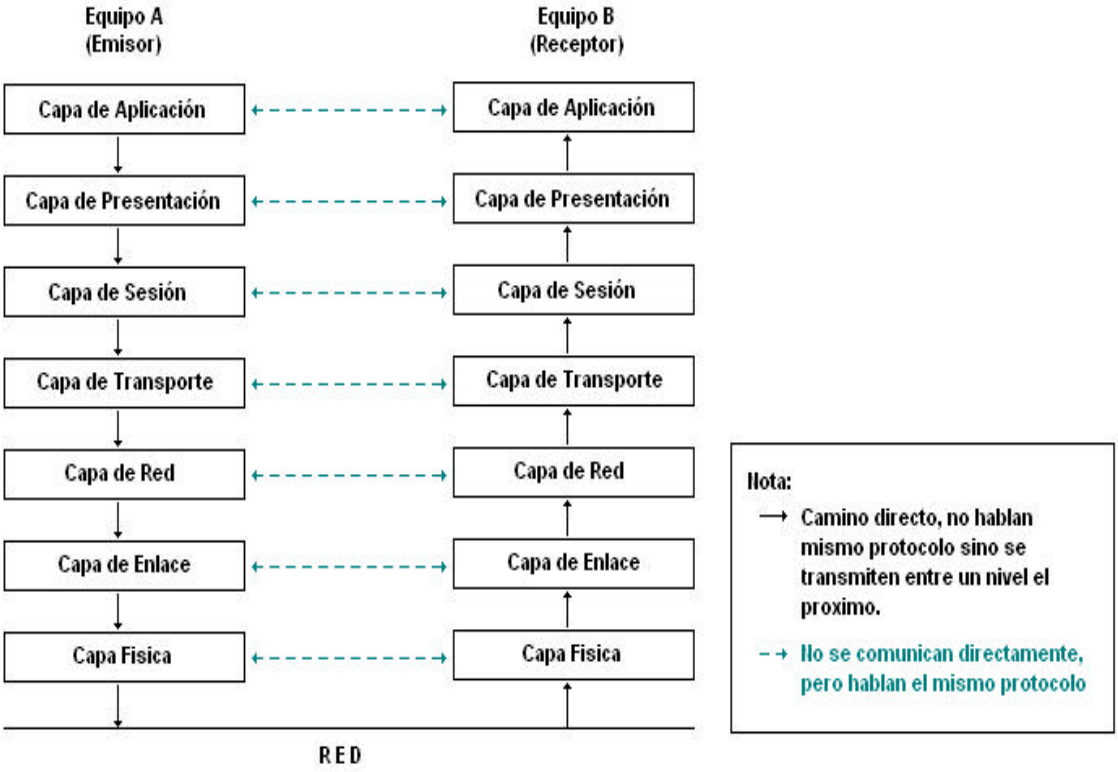


Figura B-1: *Estructura del modelo de referencia OSI.*

Anexo C: Métodos de Autentificación

1.1.- Protocolos de Autentificación:

El modelo PPP proporciona alternativas de autentificación que son limitadas en comparación a sistemas de seguridad más sofisticados que mas adelante serán analizados, algunos de estos son:

- PAP (Protocolo de autentificación de contraseñas):

Este protocolo establece un método bastante sencillo e inseguro de autentificación del usuario. Los datos de autentificación no son codificados entonces se corre el riesgo de que sean captados por terceros y usados por estos para acceder a la red privada en forma tránsfuga.

Como opera este modelo:

El servidor de acceso remoto solicita al equipo usuario remoto el nombre y contraseña de acceso, y el protocolo PAP preestablecido los devuelve en texto claro, es decir sin codificación.

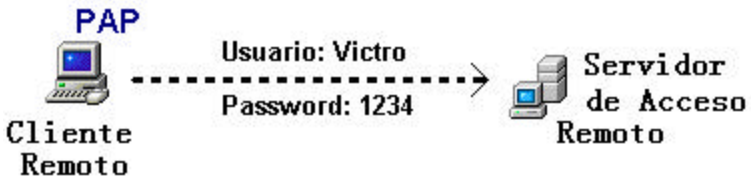


Figura C-1: *Autentificación mediante PAP (texto claro).*

- CHAP (Protocolo de autentificación de intercambio de señales de reconocimiento):

Este es otro mecanismo que a diferencia de PAP envía la autentificación codificada, y de esta manera evita la transmisión de la contraseña real del usuario a través de la conexión.

Otra ventaja con respecto al protocolo de autentificación PAP es que CHAP verifica periódicamente la identidad del usuario remoto. La verificación se produce inmediatamente después de la fase de conexión, y se puede reiterar en cualquier momento, con el enlace ya establecido.

Pasos que seguidos por el protocolo CHAP:

1. El servidor de acceso remoto que desea verificar la autenticidad del usuario remoto entrante le envía un mensaje de prueba.
2. El cliente ante este llamado responde con un valor calculado mediante el algoritmo MD5.
3. El servidor compara la respuesta del cliente con su propio cálculo del valor correcto. Si no se recibe el mensaje correcto de autentificación la conexión no es permitida y se cierra de inmediato.
4. A intervalos aleatorios, el servidor envía un nuevo mensaje al cliente y se repiten los pasos.

El último paso se realiza como medida de prevención debido a que terceros no autorizados pueden aprovechar la desconexión de los clientes autorizados para entrar sin autentificarse.

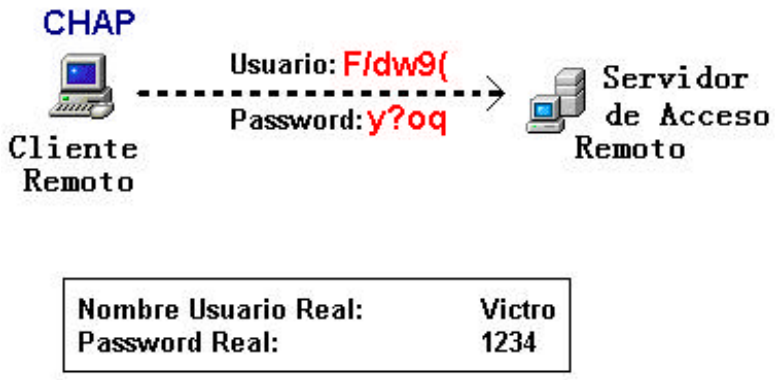


Figura C-2: *Autentificación mediante PAP (texto encriptado). Bastante mas seguro que el anterior.*

- MS-CHAP (Microsoft CHAP):

Es un mecanismo de autentificación codificada muy similar al método CHAP, el cual funciona de la siguiente forma:

1. El Servidor de acceso remoto envía una señal de reconocimiento al cliente remoto, que consiste en un ID de sesión además de una cadena de reconocimiento arbitraria.
2. El cliente debe regresar el nombre del usuario, una cadena de reconocimiento arbitraria del mismo nivel y una codificación de:
   La cadena de reconocimiento recibida.
   Identificador de sesión ID.
   Contraseña del usuario.
3. Luego el servidor compara los valores de autentificación, para luego permitir o no el acceso como usuario autorizado.

Este diseño proporciona un nivel de seguridad adicional ya que permite que el servidor almacene contraseñas con hash en lugar de contraseñas en texto claro.

1.2.- Sistemas de autentificación:

Entendiéndose por sistema no un simple protocolo que actúa como software de autentificación, sino una maquina que cuenta con bases de datos de sus clientes remotos para identificarlos y permitirles la entrada, además realizar el cifrado de autentificación para que un miembro de la red corporativa viaje sin peligro de ser interceptado por terceros. Estos sistemas por lo general se instalan en la Intranet como servidores dedicados donde sus servicios otorgan seguridad de mayor nivel:

1.- RADIUS: Como antes se ha dicho RADIUS es un servidor instalado en la red el cual soporta tanto PAP como CHAP como protocolos de interacción con el usuario. Cuando el cliente remoto crea la comunicación con el ISP, se envía a través de NAS una autentificación del usuario que contempla la ID y la password privada (cifrada o en claro depende del protocolo usado), esta información llega al servidor RADIUS de la red corporativa la cual calcula el valor de dicha autentificación, si corresponde a lo que tiene en sus registro permite la entrada del usuario remoto.

El RADIUS organizado en una estructura jerárquica con varios archivos y directorios agrupados en una base de datos **raddb** (*Radius Database*). Se disponen de los siguientes archivos:

- *Usuarios*: Contiene el perfil del usuario: información de seguridad y configuración, nombre de usuario, método de autentificación, dirección y máscara, etc.
- *Diccionarios.* Define los atributos y valores que se memorizan en el archivo de usuario.
- *Clientes.* Contiene la lista de username y password de la red. Se utiliza para la autentificación de acceso.

2.- TACACS: Este sistema también funciona como un servidor de acceso remoto que actúa en la entrada de la red corporativa, el cual controla el flujo de clientes autorizados. Este sistema además contempla su propio método de envío de identificación de los propios clientes locales de la Intranet.

3.- KERBEROS: Es desarrollado en el MIT como un sistema de autentificación para sistemas abiertos en entornos distribuidos. El proceso se realiza cuando se inicia la sesión (*logon*) del tipo cliente-servidor. Se fundamenta en *tickets* que se obtienen de un servidor y que tienen una duración limitada de tiempo. El ticket contiene toda la información del cliente para asegurar su identidad. También se generan tickets para una sesión en particular que permiten la criptografía entre pares. Utiliza DES para criptografiar y autentificar.

La versión Kerberos-5 es un Standard de Internet (RFC-1510).

Kerberos tiene 3 fases: En la primera el usuario obtiene una credencial para ser usada en el proceso de requerimiento de acceso a otro servicio. En la segunda el usuario requiere la autentificación para el servicio especificado. En la tercera el usuario presenta sus credenciales al servidor. Existen tickets y autenticadores (este contiene información adicional del cliente). Ambos usan criptografía de clave privada pero con diferentes claves (key). El ticket contiene: los nombres del cliente y servidor, la dirección IP del cliente, el timestamp y lifetime de IP y una clave random para la sesión.

Figura C-3: *Autentificación ejecutada por el servidor de la red.*

Anexo D: Protocolo SSH

Tradicionalmente cuando un usuario remoto desea conectarse a una red Unix a través de una Shell, lo realizara mediante el acceso cliente Telnet, que viene por lo general en los sistemas operativos. El cual presenta varias falencias en lo que a seguridad se refiere.

En este sistema tradicional tanto el login como la password (así como el resto de la sesión) se transmiten en texto claro a través de la red local o incluso a través de routers y nodos ajenos. Esto quiere decir que cualquiera que tenga activado un sniffer puede capturar nuestras sesiones con el potencial peligro que ello conlleva. Muchos servidores deshabilitan el puerto telnet, porque debido a la falta de encriptación es la manera más insegura de conectarse.

Shell Segura:

La alternativa mas conveniente es usar el protocolo SSH (Secure Shell) para la implementación y puesta en marcha de un acceso remoto a una red Unix mediante un medio publico, el cual se basa en la arquitectura cliente/servidor, como es habitual para estas aplicaciones de red.

Todo es como en una sesión telnet tradicional, pero con la particularidad de que todas las comunicaciones serán encriptadas. Es decir tanto los parámetros de autentificación (login y password) como las sesiones serán encriptadas por un algoritmo de encriptación que se debe incluir en la configuración del cliente SSH.

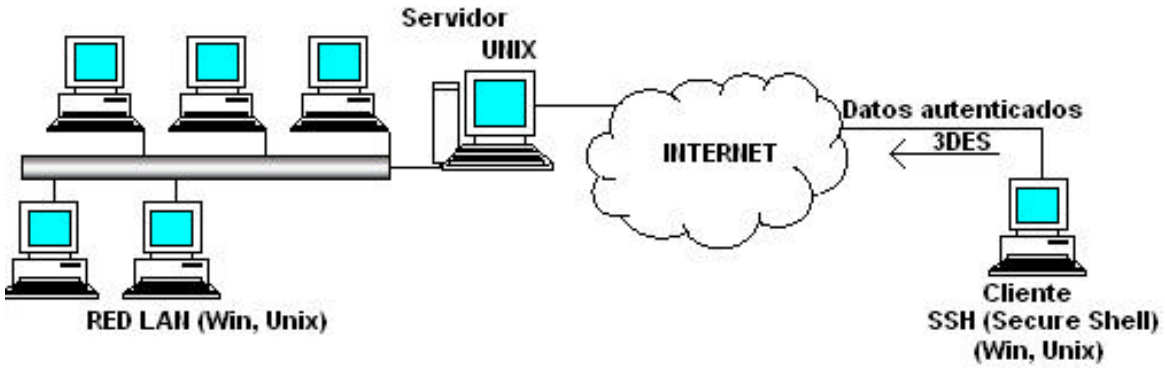


Figura D-1: *Cliente SSH, con acceso al servidor Unix.*

Pasos para entrar al sistema:

1.- Requerimientos:

Para poder acceder al servidor UNIX desde un punto remoto como cliente encriptado, se necesita:

- Un acceso a Internet, mediante un ISP local.
- Una cuenta de acceso al Servidor, esta negociación se realiza previamente, y se establece en las bases de datos del servidor.
- Debido a que SSH es un servicio tal como el servicio Telnet, se debe tener un cliente *Secure Shell (SSH)*, para realizar la aplicación SSH. El cliente mas recomendado es PuTTY (para Windows) y OpenSSH (Para Unix) , el cual se distribuye gratuitamente en la red en:

http://www.chiark.greenend.org.uk/~sgtatham/putty/download.htm

2.- Instalación del cliente PuTTY:

Una vez descargado el cliente SSH, en este caso se analizara el acceso en plataforma Windows PuTTY, se debe instalar el software en el sistema del PC cliente remoto.

Opciones a llenar para la configuración del software:

- **Host Name:** Este es el nombre del servidor en el que se te ofrece el servicio. Para el caso es *victro.accesossh.cl*
- **Port:** Este es el puerto al cual se va a conectar en el sistema del PC. Secure Shell (SSH) usa el puerto 22.
- **Saved Session:** Esta opción corresponde al nombre que se le quiera dar a la conexión de acceso al servidor en este caso fue *Conexión Victro*.

El username y contraseña se entregó anteriormente ante el servidor cuando se negoció el cliente remoto con este. Cabe destacar que toda la sesión que se realizara esta cifrada, tanto los datos de autenticación como la información en cuestión.

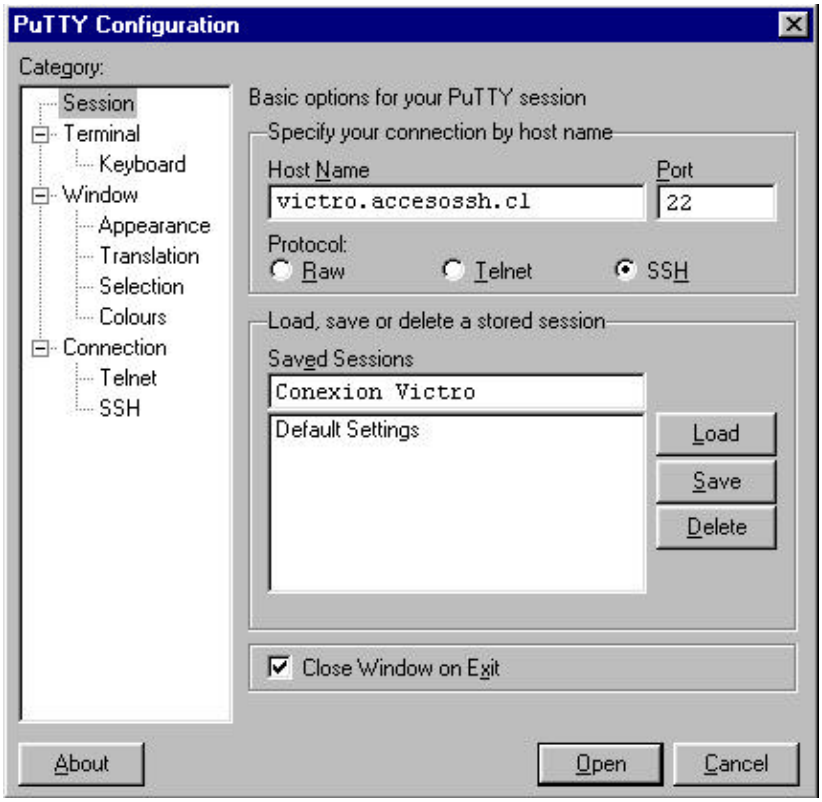


Figura D-2: *Configuración del software Cliente SSH, PuTTY.*

Luego se agrega a la lista de accesos para la conexión remota al servidor Unix, mediante SSH.

Para finalizar se selecciona el algoritmo de encriptación, siendo muy recomendable usar 3DES.

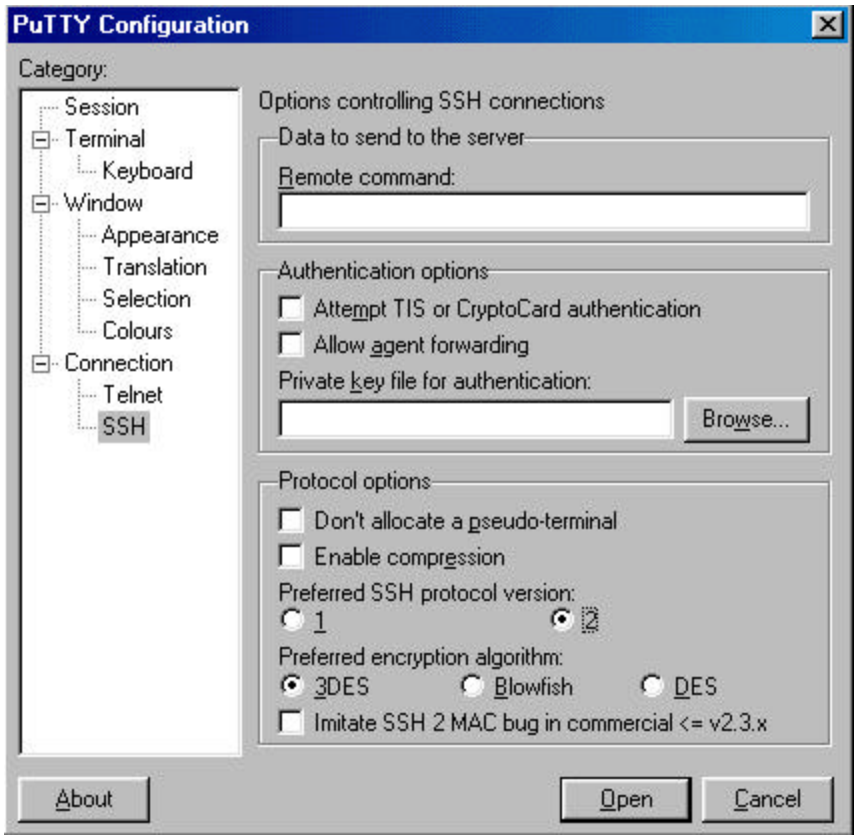


Figura D-3: Selección del protocolo de encriptación dentro de configuración del software cliente PuTTY.

Dentro de la categoría SSH, es muy importante seleccionar la versión 2 del protocolo SSH (opción *Preferred ssh protocol version)* para garantizar que coincida con la versión del servidor.

3.- Conexión al Servidor remoto:

Luego de la instalación y configuración del software cliente PuTTY, aparecerá un icono en el sistema (opcional en el escritorio de Windows). Al presionar dicho icono, aparecerá la aplicación SSH con cliente PuTTY con agentes de encriptación, que es la variación de Telnet (como antes se dijo). Antes de acceder al servidor se debe ingresar los parámetros de autentificación, requeridos por la aplicación. Una vez ingresados se logra una conexión terminal dentro de la red privada remota.

Figura D-4: *Administrador Shell Cliente PuTTY.*