PROPUESTA PARA LA IMPLEMENTACION DE SEGURIDAD A NIVEL DE RED EN LA RED DE DATOS DE LA UNIVERSIDAD DEL CAUCA

Claudia Patricia Arenas Guerrero

Julián Andrés Parra Chacón

Universidad del Cauca

Facultad de Ingeniería Electrónica y Telecomunicaciones

Departamento de Telecomunicaciones

Popayán

2006

PROPUESTA PARA LA IMPLEMENTACION DE SEGURIDAD A NIVEL DE RED EN LA RED DE DATOS DE LA UNIVERSIDAD DEL CAUCA

Claudia Patricia Arenas Guerrero

Julián Andrés Parra Chacón

Documento Final de Trabajo de Grado

Director: Ing. Francisco Javier Terán

Universidad del Cauca

Facultad de Ingeniería Electrónica y Telecomunicaciones

Departamento de Telecomunicaciones

Popayán

2006

A Dios por ayudarme a sobrepasar todos los obstáculos,
A mi papi por su apoyo constante y sus consejos,
A mi mami por su amor, sus palabras y su paciencia,
A mi hermanita por su compañía incondicional,
A toda mi familia por estar siempre ahí
Y a todas las personas que de una u otra forma
Contribuyeron con la culminación de esta etapa.
Este triunfo es para ustedes.

Claudia

Por tanto valor, entrega y amor a mi amada madre
Por su comprensión y apoyo a mi familia
Por tantos momentos tan agradables y por dejarme
disfrutar de su compañía, a mis amigos, gracias

Julián

TABLA DE CONTENIDO

Pag

LISTA DE FIGURAS

pag

LISTA DE TABLAS

pag

LISTA DE ANEXOS

ABSTRACT

La falta de medidas de seguridad en las redes es un problema que está en crecimiento; cada vez es mayor el número de atacantes y cada vez están más organizados, por lo que van adquiriendo día a día habilidades más especializadas que les permiten obtener mayores beneficios. Las redes basadas en el protocolo IP presentan cuatro grandes problemas, los cuales pueden ser aprovechados de diferentes maneras. Estos problemas son: la pérdida de autenticación, la pérdida de confidencialidad, la pérdida de integridad y la pérdida de disponibilidad de los datos. La Red de Datos de la Universidad del Cauca no es ajena a estos problemas; el propósito de este trabajo fue brindar una solución de seguridad que se acomode a las necesidades de la red universitaria sin desmejorar su desempeño. Para ello se realizó un análisis y comprobación de las principales vulnerabilidades que pueden aplicarse sobre dicha red; luego se analizaron los mecanismos de seguridad de mayor importancia en la actualidad, entre ellos el estándar IPSec, el cual es una familia de protocolos diseñada para ofrecer seguridad al protocolo IPv6 y que hoy en día puede aplicarse a IPv4. Por último se diseñaron dos propuestas de seguridad con los resultados obtenidos anteriormente y se escogió la propuesta mas acertada para la Red de Datos, teniendo en cuenta aspectos técnicos más que económicos que aseguren los resultados esperados. Además se plantearon Políticas de Seguridad a nivel Físico, Lógico y Humano, como una buena base para el comienzo de una cultura de seguridad de la información en la Universidad del Cauca.

ABSTRACT

The loss of network security measures is a constantly growing problem; the number of attackers is bigger and each time they are more organized, because of this reason they are acquiring specialized abilities that allow them to obtain greater benefits. IP Protocol based Networks have four big problems, that attackers can take advantage of in different ways. These problems are: the loss of authentication, loss of confidentiality, loss of integrity and the loss of data availability. The University of Cauca´s Data Network is not free of these problems; the purpose of this work was to offer a security solution adjusted to the needs of the university´s network without worsen its performance. For this, an analysis and verification of the main vulnerabilities that can be applied on this network was made; next, the currently most important mechanisms of security were analyzed, among them the IPSec standard, which is a family of protocols designed to offer security to the IPv6 protocol and that at the present it can be applied to IPv4. Finally, with the previously obtained results two security proposals were designed; and the most appropriate one was chosen for the Data Network, considering technical aspects, before economic issues, that can assure the expected results. In addition, Security Policies were propossed, at a physical, logical and a Human level, as a good base for the beginning of an information security culture in the University.

CAPITULO I. ASPECTOS GENERALES

1.1 INTRODUCCION

En la actualidad, las organizaciones son cada vez más dependientes de sus redes de datos y un problema que las afecte, por mínimo que sea, puede llegar a comprometer la continuidad de las operaciones. La seguridad es un concepto cuya definición exacta es difícil de proporcionar; sin embargo, a grandes rasgos se puede indicar que es el conjunto de elementos (metodologías, documentos, programas, mecanismos y dispositivos físicos) encaminados a lograr que los recursos computacionales y de red disponibles en un ambiente dado, sean utilizados única y exclusivamente por quienes tienen la autorización para hacerlo o para realizar determinadas tareas. Adicionalmente, es importante entender que la Seguridad en Redes debe vigilar que los recursos estén siempre disponibles en todo momento.

La falta de medidas de seguridad en las redes es un problema que está en crecimiento; cada vez es mayor el número de atacantes y cada vez están más organizados, por lo que van adquiriendo día a día habilidades más especializadas que les permiten obtener mayores beneficios. Tampoco deben subestimarse las fallas de seguridad provenientes del interior mismo de la organización. La propia complejidad de la red es una dificultad para la detección y corrección de los múltiples y variados problemas de seguridad que van apareciendo. En medio de esta variedad, han ido aumentando las acciones poco respetuosas de la privacidad y de la propiedad de recursos y sistemas. *Hackers, Crakers, entre otros*, han hecho aparición en el vocabulario ordinario de los usuarios y de los administradores de las redes, y todo esto, porque se han identificado cuatro problemas principales, a partir de los cuales comienza a verse la necesidad actual de implementar seguridad en las redes y son: Pérdida de *Confidencialidad*, de *Integridad*, de *Autenticación* y de *Disponibilidad* de los datos; estos problemas abarcan todas las redes de datos entre ellas las redes IP, a las cuales se hará referencia debido a que es el tipo de red que maneja la Universidad del Cauca.

La *Pérdida de Confidencialidad de los datos s*e debe a que la información que pasa de un terminal a otro se transmite por medios compartidos de manera que otros terminales además del destinatario pueden tener acceso a los datos.
La *Pérdida de la Integridad de los datos* se presenta cuando un ente tiene acceso a información no autorizada transmitida por una red y puede manipularla para suprimir la información enviada o cambiarla para remplazarla por información que no corresponde a la original.

La *Pérdida de la Autenticación de las terminales IP* es una de las debilidades de mayor importancia; se produce cuando la máquina que dice ser el origen o el destino de determinada información ha sido suplantada por otra.

La *Negación de Servicio o Pérdida de Disponibilidad* se da según el conocimiento que tenga un ente sobre cual es el origen o el destino, solo examinando la estructura de determinada información; esto permite que dicho ente interrumpa la prestación de determinado servicio, la cual es una de las debilidades más aprovechadas en las redes IP del planeta.

Todos estos problemas pueden ser aprovechados de manera interna o externa a la red, por lo que se hace necesario el diseño de modelos que provean *seguridad* a nivel de enlace de datos y a nivel de red; esto se puede lograr con mecanismos de seguridad como los Firewalls, las VLANs (Virtual Local Area Networks – Redes Virtuales de Área Local), las VPNs (Virtual Private Networks – Redes Privadas Virtuales), entre otros, y protocolos de seguridad como el Protocolo IPSec (IP Security), el cual provee seguridad (autenticación, cifrado, confidencialidad) a nivel de red de acuerdo al Modelo de Referencia OSI[1] de la Organización de Estándares Internacional (ISO[2]).

Además de las técnicas y herramientas criptográficas, es importante recalcar que un componente muy importante para la protección de los sistemas consiste en la atención y vigilancia continua y sistemática por parte de los responsables de la red. A la hora de plantearse en qué elementos del sistema se deben ubicar los servicios de seguridad podrían distinguirse dos tendencias principales:

- *Protección de los sistemas de transferencia o transporte:* En este caso, el administrador de un servicio asume la responsabilidad de garantizar la transferencia segura de la información al usuario final lo más transparente posible. Ejemplos de este tipo de planteamientos serían el establecimiento de un nivel de transporte seguro, con protocolos de seguridad a nivel de red y transporte, la instalación de un Firewall, que defienda el acceso a una parte protegida de una red y la utilización de otros mecanismos que contribuyan a implementar seguridad, como VLANs, VPNs, etc.

- *Aplicaciones seguras extremo a extremo:* Si se piensa, por ejemplo, en el correo electrónico, consistiría en construir un mensaje en el cual el contenido ha sido asegurado mediante un procedimiento de encapsulado previo al envío. De esta forma, el mensaje puede atravesar sistemas heterogéneos y poco fiables sin por ello perder la validez de los servicios de seguridad provistos. Aunque el acto de asegurar el mensaje cae bajo la responsabilidad del usuario final, es razonable pensar que dicho usuario deberá usar una herramienta amigable proporcionada por el responsable de seguridad de su organización. Todo esto puede usarse para abordar el problema de Seguridad en Redes utilizando la seguridad en otras aplicaciones tales como videoconferencia, acceso a bases de datos, etc.

[1] OSI - *Open Systems Interconection.* Modelo de Interconexión de Sistemas Abiertos.
[2] ISO – *International Organization for Standarization*. www.iso.org

Este trabajo está dirigido principalmente a la protección del sistema en los niveles inferiores, tomando más específicamente el nivel de red, ya que éste implementa el protocolo IP, uno de los más utilizados a nivel mundial y sobre el cuál la IETF[3] ha trabajado mucho en todos los aspectos, hasta llegar a su versión 6.

El protocolo IP, *Internet Protocol*, es uno de los más usados para la interconexión de redes en todos los entornos, y naturalmente lo es también en Internet. Su flexibilidad y sus poderosas capacidades lo han impuesto como el vehículo de interconectividad más utilizado y se piensa que lo seguirá siendo por mucho tiempo. La fuerza de IP radica en el sencillo mecanismo que utiliza para el envío de grandes volúmenes de información en pequeños datagramas a través de los diversos esquemas de enrutamiento. De esta forma, y dado que la información que se transmite por la redes es el recurso más valioso de estas, es de vital importancia dedicarse a encontrar todas las debilidades y toda la serie de problemas que son intrínsecos de las redes de datos, incluidas las redes IP, debido a la estructura de dicho protocolo; estos problemas son la pérdida de confidencialidad, pérdida de integridad, pérdida de autenticación y pérdida de disponibilidad de los datos; cada una de estas debilidades puede ser aprovechada por personas mal intencionadas para impedir el normal funcionamiento de una red IP.

El objetivo principal que se persiguió con este trabajo fué analizar el estado de la Red de Datos de la Universidad del Cauca y de los distintos protocolos de seguridad que implementa IP en su versión 6, pero que no contiene IP en su versión 4, además de los mecanismos de seguridad a nivel de red más utilizados. Actualmente, la Red de Datos de la Universidad del Cauca se encuentra en un proceso constante de crecimiento debido a la gran cantidad de información que debe manejar y al aumento del número de usuarios que hacen uso de ella; el impresionante crecimiento de Internet, la conectividad, los adelantos tecnológicos, el advenimiento de nuevos servicios y la necesidad de conocimiento son motivos para interesarse en el tema de la seguridad, que en los últimos años ha cobrado mucha fuerza.

En la Universidad del Cauca, la información manejada entre las diversas dependencias necesita mantener altos niveles de confidencialidad, integridad, autenticación, y disponibilidad, porque cuenta con un Sistema de Información Administrativo para pago de nómina, Servicios Financieros, de tesorería, admisiones y pago de derechos financieros; un Sistema de Información de la Vicerrectoría de Investigaciones para el manejo de proyectos de investigación; un Sistema de Información en la biblioteca para consulta y gestión de la misma; además, en este momento se encuentra en desarrollo el proyecto para implantar el Sistema de Información Académica Sócrates, que prestará servicio de registro, control y gestión de estudiantes y notas de la comunidad universitaria. Esta información es de vital importancia para el buen funcionamiento de la Institución por lo que no debe ser accedida ni manipulada por personas no autorizadas dentro de la Institución y fuera de ella.

El problema radica en que la Red de Datos actualmente no cuenta con una Arquitectura de Seguridad de Red para proteger la información institucional por lo que surge la necesidad de implantar técnicas, procesos y mecanismos que garanticen seguridad a la Red de Datos de la Universidad del Cauca. En este momento la Red funciona sobre el Protocolo IPv4 el cual no implementa

[3] IETF – *Internet Engineering Task Force*. Grupo de trabajo que se encarga de crear protocolos estándares para redes de comunicación. www.ietf.org

esquemas que eviten los problemas de falta de autenticación, confidencialidad, integridad y disponibilidad de los datos, debido a que el datagrama IPv4 presenta diversas vulnerabilidades y cualquiera puede aprovecharse de esa inseguridad; la información viaja en texto plano y no provee métodos de cifrado.

Como respuesta a las deficiencias de IPv4, surge el Protocolo IPv6; su aparición a nivel mundial ha cambiado la forma de pensar acerca del Protocolo IP por los grandes cambios en su arquitectura y los adelantos tecnológicos que trajo consigo, entre ellos la implementación de encapsulamiento, autenticación y privacidad. A pesar de los grandes beneficios que provee IPv6 en el campo de seguridad en redes, la migración a esta arquitectura no es un proceso que pueda llevarse a cabo a corto plazo dentro de la Universidad debido a limitaciones económicas, de infraestructura, y del entorno donde el estándar sigue siendo IPv4; es por esta razón que el propósito del proyecto fué implementar las ventajas que provee la arquitectura IPv6 en cuanto a seguridad para fortalecer las limitaciones de la red IPv4 actual. Además es necesario analizar e implementar algunos mecanismos complementarios que podrían fortalecer la Seguridad a nivel de Red como son los Firewalls, las VLANs y las VPNs. De esta forma se fortalecerá la Seguridad de la Red de Datos de la Universidad del Cauca *a nivel de red* con una arquitectura confiable y robusta, que sitúe a la Institución un paso adelante dentro de la sociedad de la Información y que de igual forma sirva como modelo de referencia para proyectos similares que se lleven a cabo a nivel nacional.

1.2 DESCRIPCION DE LOS CAPITULOS

En el capítulo 1, se realiza un análisis de la Red de Datos de la Universidad del Cauca, su estado actual, las tecnologías de red empleadas, la distribución física de los equipos de red y hosts, el funcionamiento lógico, los Sistemas de Información, los servicios soportados y sobretodo los mecanismos que se utilizan para proveer seguridad a la red.

En el capítulo 2, se estudian los ataques a los que esta expuesta una Red de Datos y las principales vulnerabilidades de las mismas, en particular las redes IP, para identificar y analizar cuales de éstos se están presentando en la Red de Datos de la Universidad del Cauca y formar una idea clara de los aspectos a mejorar; además, se mencionan las posibles soluciones para estas amenazas, como también los procedimientos para brindar mayor protección a la red.

En el capítulo 3, se realiza un estudio detallado de los principales protocolos estándares de seguridad de Red que provee IPv6, implementados sobre redes IPv4, sus principales características, su funcionamiento, ventajas, desventajas y su utilización en las redes actuales.

En el capítulo 4, se detallan los principales mecanismos de seguridad a nivel de red y los más utilizados, como son los Firewalls, las VPNs, las VLANs y los IDSs (Intrusion Detection System – Sistemas de Detección de Intrusos), se describen sus características, aplicaciones y ventajas a la hora de implementarlos.

En el capítulo 5 se presenta una especificación de las principales herramientas que permiten la implementación de los protocolos más importantes de IPv6 sobre redes IPv4, sus características, ventajas y desventajas de funcionamiento; se detallan los procedimientos que se siguieron a la hora de realizar las pruebas de laboratorio utilizando el protocolo IPSec en sus dos modos de funcionamiento, la creación de túneles para Redes Privadas Virtuales, y la implementación de los mecanismos de autenticación más utilizados: Claves Precompartidas, Firmas Digitales RSA y Certificados Digitales; se analizan los resultados de éstas, como base para el diseño de las diferentes propuestas de Seguridad de Red.

Ya que ningún protocolo o mecanismo de Seguridad es totalmente robusto si no está apoyado por un comportamiento ejemplar por parte de los usuarios de una red, es importante plantear Políticas de Seguridad que eduquen a los usuarios de la institución a comportarse de forma que complementen la arquitectura de seguridad.

En el capítulo 6, primero se hace una introducción a las creación de Políticas de Seguridad, qué se debe tener en cuenta a la hora de plantearlas, y se presenta una propuesta sencilla para usuarios y administradores de la red. Seguidamente, se presentan dos propuestas de Seguridad a nivel de Red para la Red de Datos de la Universidad del Cauca, que surgen a raíz de la configuración, implementación y análisis de los resultados obtenidos en los distintos escenarios de prueba de los protocolos y mecanismos de seguridad analizados, sobre las plataformas respectivas. Entre las propuestas planteadas se selecciona la más adecuada para ser implementada en la Institución, su respectivo análisis y justificación, y las ventajas y desventajas de implantar dicha arquitectura.

Al final del documento se presentan las diferentes conclusiones que surgen al finalizar el proyecto, algunas recomendaciones y se proponen trabajos futuros que pueden llevarse a cabo a partir de la propuesta desarrollada y posibles áreas de estudio. Además se adjunta un listado de acrónimos que sirven al lector a familiarizarse con las siglas que se manejan a lo largo del documento.

1.3 SEGURIDAD EN REDES IP

IPSec es un estándar que proporciona servicios de seguridad a la capa IP y a todos los protocolos superiores basados en IP (TCP y UDP, entre otros). Es una muy buena solución para abordar las carencias en cuanto a seguridad del protocolo IP. Dichas carencias son muy graves y, tal como se ha constatado en los últimos años, afectan a la infraestructura misma de las redes IP. Todas las soluciones anteriores se basaban en soluciones propietarias que dificultaban la comunicación entre los distintos entornos empresariales, al ser necesario que éstos dispusieran de una misma plataforma. La falta de interoperabilidad ha sido el principal freno para el establecimiento de comunicaciones seguras, dado que no se ve factible la migración a una determinada plataforma en función de una colaboración empresarial puntual.

Entre las ventajas de IPSec se destacan, que está apoyado en estándares del IETF y que proporciona un nivel de seguridad común y homogéneo para todas las aplicaciones, además de ser independiente de la tecnología física empleada. IPSec puede integrarse en la versión actual de IP (IP versión 4) y, lo que es todavía más importante, se incluye por defecto en IPv6. Puesto que la seguridad es un

requisito indispensable para el desarrollo de las redes IP, IPSec está recibiendo un apoyo considerable: todos los equipos de comunicaciones lo incorporan, así como las últimas versiones de los sistemas operativos más comunes. Al mismo tiempo, ya existen muchas experiencias que demuestran la interoperabilidad entre fabricantes, lo cual constituye una garantía para los usuarios. Otra característica destacable de IPSec es su carácter de estándar abierto. Se complementa perfectamente con la tecnología PKI (Public Key Infrastructure - Infraestructura de Llaves Públicas) y, aunque establece ciertos algoritmos comunes, por razones de interoperabilidad, permite integrar algoritmos criptográficos más robustos que pueden ser diseñados en un futuro.

Entre los beneficios que aporta IPSec, cabe señalar que posibilita nuevas aplicaciones como el acceso seguro y transparente de un nodo IP remoto, facilita el comercio electrónico de negocio a negocio al proporcionar una infraestructura segura sobre la que realizar transacciones usando cualquier aplicación y permite construir una red corporativa segura sobre una red pública.

El protocolo IPSec es ya uno de los componentes básicos de la seguridad en las redes IP. En este momento se puede considerar que es una tecnología suficientemente madura para ser implantada en todos aquellos escenarios en los que la seguridad es un requisito prioritario. Dentro de este trabajo se han descrito, desde un punto de vista técnico, las características del protocolo IPSec definidas en el estándar de la IETF, así como los servicios de seguridad que proporciona. Finalmente, se han presentado varios ejemplos de aplicaciones prácticas en las que IPSec se constituye como la solución más apropiada para garantizar la seguridad de las comunicaciones en cualquier red IP.

1.4 ESTUDIO DE LA INFRAESTRUCTURA ACTUAL DE LA RED DE DATOS DE LA UNIVERSIDAD DEL CAUCA Y LOS MECANISMOS DE SEGURIDAD UTILIZADOS

Actualmente, la Red de Datos de la Universidad del Cauca se encuentra en un proceso constante de cambio debido a la gran cantidad de información que debe manejar, al aumento del número de usuarios que hacen uso de ella, el impresionante crecimiento de Internet, la conectividad, los adelantos tecnológicos y el advenimiento de nuevos servicios. El estudio realizado se dividió en tres partes, la infraestructura física, la infraestructura lógica y la infraestructura de servicios de la red universitaria.

1.4.1 Infraestructura Física de la Red de Datos de la Universidad del Cauca

La Red de Datos de la Universidad del Cauca tiene una estructura física la cual se basa en un campus universitario dividido por sectores:

- Sector de Ingenierías
- Sector de Medicina
- Sector de Educación
- Sector de El Carmen
- Sector de Santo Domingo
- Sector de Vicerrectoría de Investigaciones

- Sector de Las Guacas
- Sector de Santander de Quilichao

En cada sector se encuentran uno o más edificios, los cuales se conectan entre sí por un backbone de fibra óptica multimodo, el cual posee físicamente una topología de doble estrella, que tienen como centro los edificios del Instituto de Postgrados (IPET) y El Carmen, como se muestra en la Figura 1.1. Además existen otros sectores tales como Alfonso López y el Consultorio jurídico en los cuales la densidad de equipos es muy baja.

La conexión con el sector de Santander de Quilichao se realiza a través de la Red Metropolitana de Emtel, conectándose a la Red Nacional de Fibra Óptica para llegar hasta el nodo ubicado en la ciudad de Cali. Desde este nodo se realiza una conexión por medio de un radio-enlace hacia la sede ubicada en Santander de Quilichao.

Actualmente, el acceso WAN o acceso a Internet se realiza a través de los proveedores de servicio de Internet *Telecom* y *Orbitel.* La conexión con Telecom se realiza a través de un Modem HDSL a 2 Mbps; la conexión con Orbitel se realiza por Fibra Óptica a través de la Red Metropolitana de Emtel a 4 Mbps.

El acceso remoto o acceso telefónico se realiza por medio de un enlace primario (PRI – Primary Rate Interface) de la Red Digital de Servicios Integrados (Integrated Service Digital Network – ISDN) para 30 canales (los cuales permiten una velocidad máxima de 56 Kbps si el usuario se conecta a través de una línea telefónica analógica; 64 Kbps cuando el usuario tiene el servicio ISDN; y 128 Kbps cuando tiene el servicio ISDN y utiliza los 2 canales B; este enlace es provisto por la empresa Emtel.

La infraestructura física dentro de cada sector del campus universitario y específicamente dentro de cada edificio posee un cableado estructurado certificado utilizando par trenzado no-apantallado (Unshielded Twisted Pair - UTP) Categoría 5 o superior, teniendo por lo menos un centro de cableado (o rack) en cada edificio y sus respectivos puntos de red que se extienden hasta los puestos de trabajo dentro de ese edificio. En grandes edificios donde las limitaciones de distancia del Cableado Estructurado no permiten que un solo centro de cableado recoja todos los puntos de red, se tienen centros de cableado secundarios que recogen esos puntos de red distantes, y que a su vez se conectan al centro de cableado principal (generalmente conocido como centro de cableado 1, CC1) a través de un número de cables UTP, determinado por el tamaño en puntos de red de los centros de cableado secundarios.

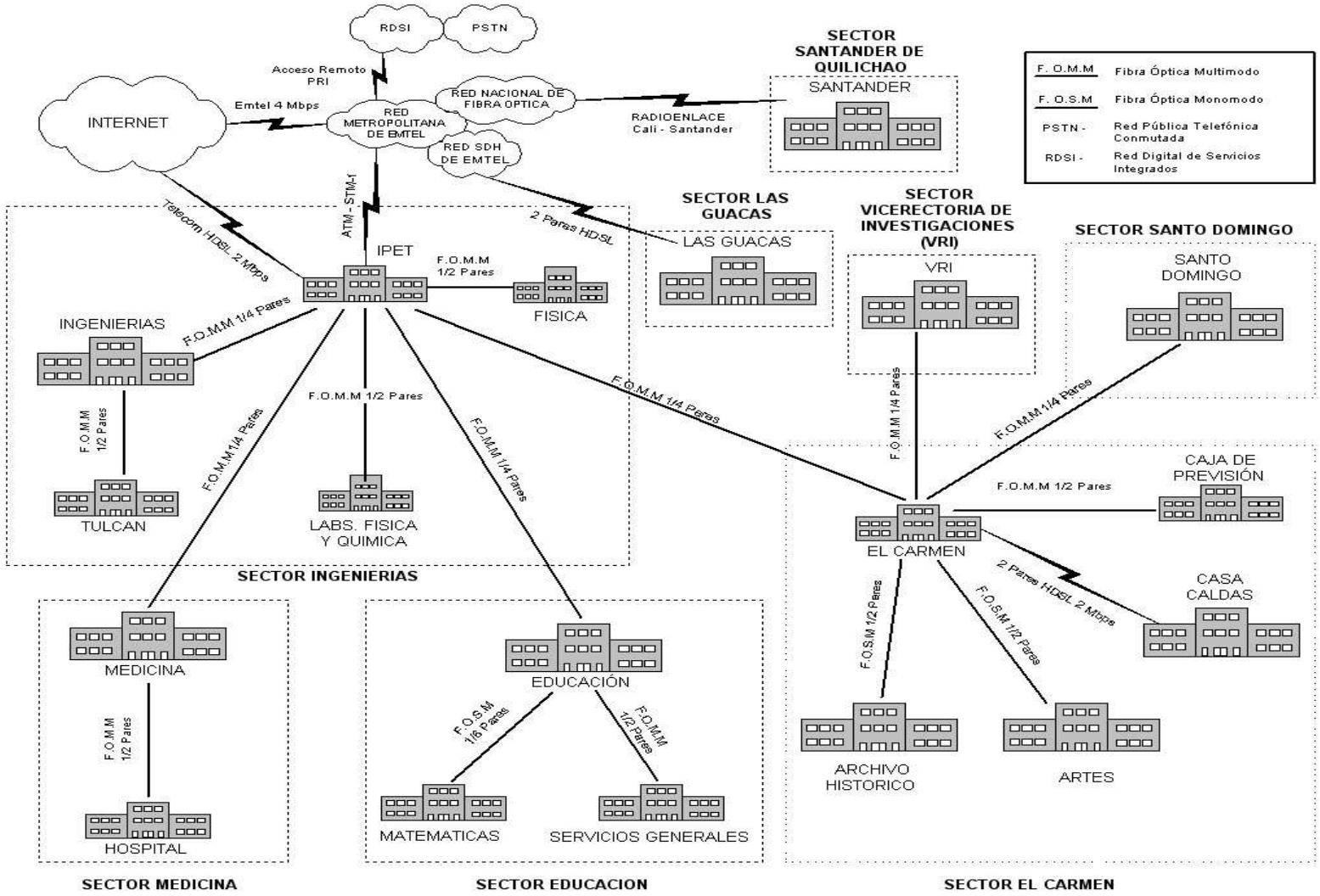


Figura 1.1 Infraestructura física de la Red de Datos de la Universidad del Cauca

La infraestructura física dentro de cada sector del campus universitario y específicamente dentro de cada edificio posee un cableado estructurado certificado utilizando par trenzado no-apantallado (Unshielded Twisted Pair - UTP) Categoría 5 o superior, teniendo por lo menos un centro de cableado (o rack) en cada edificio y sus respectivos puntos de red que se extienden hasta los puestos de trabajo dentro de ese edificio. En grandes edificios donde las limitaciones de distancia del Cableado Estructurado no permiten que un solo centro de cableado recoja todos los puntos de red, se tienen centros de cableado secundarios que recogen esos puntos de red distantes, y que a su vez se conectan al centro de cableado principal (generalmente conocido como centro de cableado 1, CC1) a través de un número de cables UTP, determinado por el tamaño en puntos de red de los centros de cableado secundarios.

1.4.2 Infraestructura Lógica de la Red de Datos de la Universidad del Cauca

La Red de Datos de la Universidad del Cauca es una red de área local (LAN) que utiliza la tecnología que se describe en el estándar 802.3 de la IEEE, en el cual se habla de una red LAN que tiene un método de acceso al medio denominado Acceso Múltiple por Detección de Portadora con Detección de Colisión (Carrier Sense Multiple Access/Collision Detection - CSMA/CD). De manera esquemática el procedimiento seguido por las estaciones que siguen esta técnica es el siguiente: antes de transmitir, una estación monitoriza el medio para escuchar si alguna otra estación está transmitiendo. Si se detecta una transmisión, la estación espera un tiempo aleatorio antes de volver a intentar la transmisión, escuchando de nuevo el medio en primer lugar; si no detecta ninguna transmisión sobre el medio físico, la estación comienza su transmisión. Durante la transmisión de una trama, la estación monitoriza el medio continuamente y si no detecta la transmisión de ninguna otra estación, continúa su transmisión hasta completar la trama. Una vez que se completa la transmisión de la trama, la estación espera un intervalo de 9,6 ms (intervalo entre tramas) antes de volver a efectuar ninguna transmisión. Este intervalo se aprovecha para una comprobación.

IEEE 802.3 permite un funcionamiento a 10 Mbps sobre diferentes medios físicos (coaxial, par trenzado, fibra óptica); sin embargo el estándar ha evolucionado permitiendo alcanzar velocidades de 100, 1000 y 10000 Mbps, oficialmente conocidos como IEEE 802.3u, IEEE 802.3z, e IEEE 802.3a y comúnmente llamados Fast-Ethernet, Gigabit-Ethernet y 10 Gigabit-Ethernet respectivamente. Con el desarrollo posterior de los switchs nivel 2 (conmutadores) la tecnología IEEE 802.3 basada en CSMA/CD (conocida también como Ethernet compartida) ha superado una de sus limitaciones, al permitir la incorporación de mayores cantidades de hosts a la red sin disminuir su nivel de desempeño, objetivo que se alcanza segmentando la red al tener un segmento diferente en cada uno de los puertos del switch, lo que da origen a la tecnología conocida como Ethernet conmutada.

Para su funcionamiento, la Red de Datos cuenta con un backbone en fibra óptica, el cual a pesar de poseer físicamente una topología de doble estrella, lógicamente tiene una topología de una sola estrella centrada en el IPET como se muestra en la Figura 1.2. Aunque físicamente Santo Domingo se conecta al Carmen, lógicamente tiene una conexión directa al IPET ya que se ha "puenteado" la fibra óptica en El Carmen evitando la conmutación de datos en ese punto.

El backbone funciona implementando Fast-Ethernet en forma conmutada a nivel 2, entregando una velocidad de 100 Mbps en cada uno de los enlaces. En cada edificio existe por lo menos un switch Ethernet conectado a dicho backbone a través de su puerto de alta velocidad. Este switch a su vez permite la conexión de la red de acceso constituida por los diferentes hubs Ethernet (los que implementan Ethernet compartido) repartidos entre los centros de cableado principal y secundarios y conectados utilizando el cableado estructurado existente basado en UTP Categoría 5.

El núcleo de la red se encuentra en el edificio del IPET donde se encuentran los equipos que dan acceso a Internet, acceso remoto a la red universitaria y servicios básicos de redes Internet. El acceso a Internet a través de Telecom utiliza la tecnología HDSL (High-rate Digital Suscriber Line) y se conecta mediante dos pares de cobre dedicados a una velocidad de 2 Mbps; el acceso a Internet a través de Emtel se realiza utilizando Fibra Óptica mediante su Red Metropolitana que funciona con la tecnología ATM como se muestra en la figura 1.3. Para el acceso telefónico se tiene un servidor de acceso remoto (Remote Access Server - RAS) Lucent Max 6000, mostrado en la Figura 1.3, que atiende un enlace PRI ISDN con 30 canales contratado con Emtel, y que permite que los usuarios se conecten a una velocidad máxima de 56 Kbps si lo hacen a través de una línea telefónica analógica, o hasta 64 Kbps cuando tienen el servicio ISDN, o hasta 128 Kbps cuando tienen ISDN y utilizan los dos canales B.

La Red de datos de la Universidad del Cauca, dentro de sus mecanismos de seguridad a nivel de red, cuenta con un Firewall implementado con la utilidad IPtables, debido a que viene con todos los Sistemas Operativos GNU/Linux con Kernel 2.4 en adelante. Pero también porque esta misma utilidad permite la implementación del servicio de NAT (Network Address Translation); éste Firewall, en su primera etapa de implementación, solo funciona con el enlace de Telecom. También se cuenta con el PacketShaper, dispositivo para la gestión de ancho de banda y con funciones limitadas de Firewall.

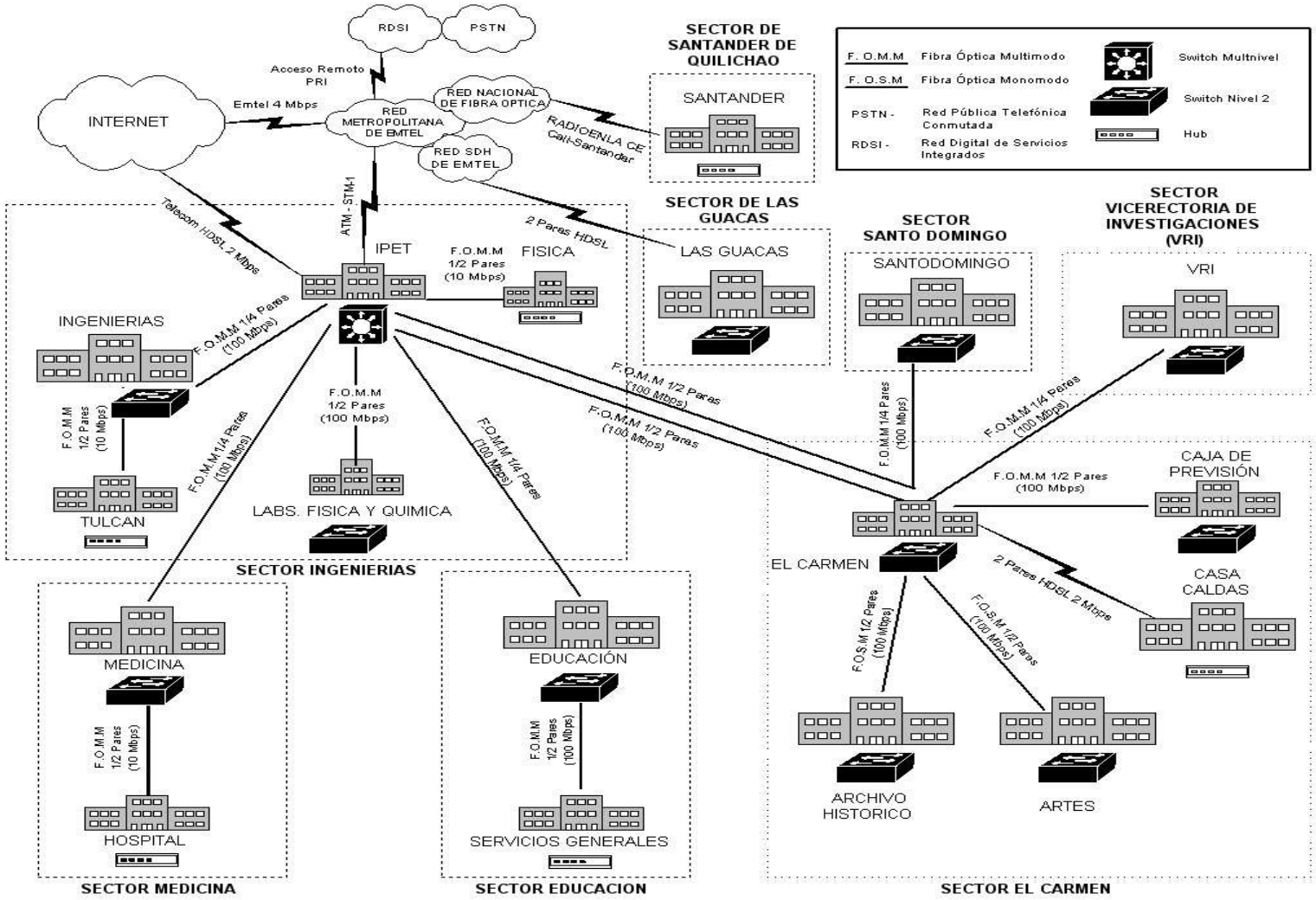


Figura 1.2 Infraestructura lógica de la Red de Datos de la Universidad del Cauca

Por el enlace de Orbitel se tiene un Firewall hardware de Cisco de referencia PIX 515E el cual presta servicios de NAT para la conexión directa hacia Internet de las direcciones autorizadas para ello y protección contra los ataques de red más populares; no se ha implementado filtrado de puertos TCP o UDP, o por aplicaciones; sin embargo dicho Firewall tiene propiedades de Firewall con estado y de algunas características de Proxy Firewall. El Firewall PIX 515E cuenta con seis interfaces de red de las cuales se encuentran en uso cuatro de ellas: la interfaz eth0 se encuentra conectada directamente al enrutador del enlace de Orbitel para el acceso a Internet, la interfaz eth1 da conexión a la VLAN de servidores conectándose a uno de los puertos que pertenecen a dicha VLAN, la interfaz eth2 se conecta directamente al switch para dar conexión a los equipos de la LAN que constituyen la gran mayoría de equipos de la red y la interfaz eth3 se conecta directamente a la interfaz LAN del servidor de acceso remoto para brindar conectividad remota de los usuarios de la Universidad a la Intranet universitaria. El Firewall PIX permite establecer un nivel de seguridad para cada red representada por un número de 0 a 100, donde 0 es la red menos segura que existe y 100 la red más segura. No importa el número que se asigne a cada interfaz, lo que importa es qué interfaz tiene mayor o menor nivel de seguridad para que el Firewall sepa si una comunicación va de una red más segura a una menos segura o viceversa y con este conocimiento aplicar sus algoritmos de seguridad. La configuración de niveles de seguridad para cada interfaz del Firewall es la siguiente:

- ✓ Interfaz eth0 (outside): Seguridad0.
- ✓ Interfaz eth1 (inside): Seguridad100.
- ✓ Interfaz eth2 (lan): Seguridad4.
- ✓ Interfaz eth0 (RAS): Seguridad6.

Como puede observarse la red menos segura es la red que conecta por la interfaz eth0 (Internet) y la más segura es la que conecta por la interfaz eth1 (VLAN de servidores).

Gracias a las capacidades de enrutamiento estático, se han configurado rutas estáticas en el Firewall para la conexión de todas las redes que forman la red de la Universidad del Cauca y las cuales están conectadas a sus interfaces. Este enrutamiento estático se realiza para obligar a que la comunicación entre ciertas redes pase a través del Firewall y así lograr que dichas comunicaciones entre redes estén protegidas gracias a las características de filtro de puertos, de Firewall con estado y de Proxy Firewall que ofrece el Cisco PIX 515E. Todas las conexiones externas desembocan en el switch Cisco Catalyst 4500 de nivel tres ya que este es el núcleo de la red, el cual brinda conectividad entre los sectores de la red y entre dichos sectores y redes externas. En la figura 1.3 se presenta la arquitectura real de interconexión entre Internet y la Intranet de la Universidad del Cauca a la fecha.

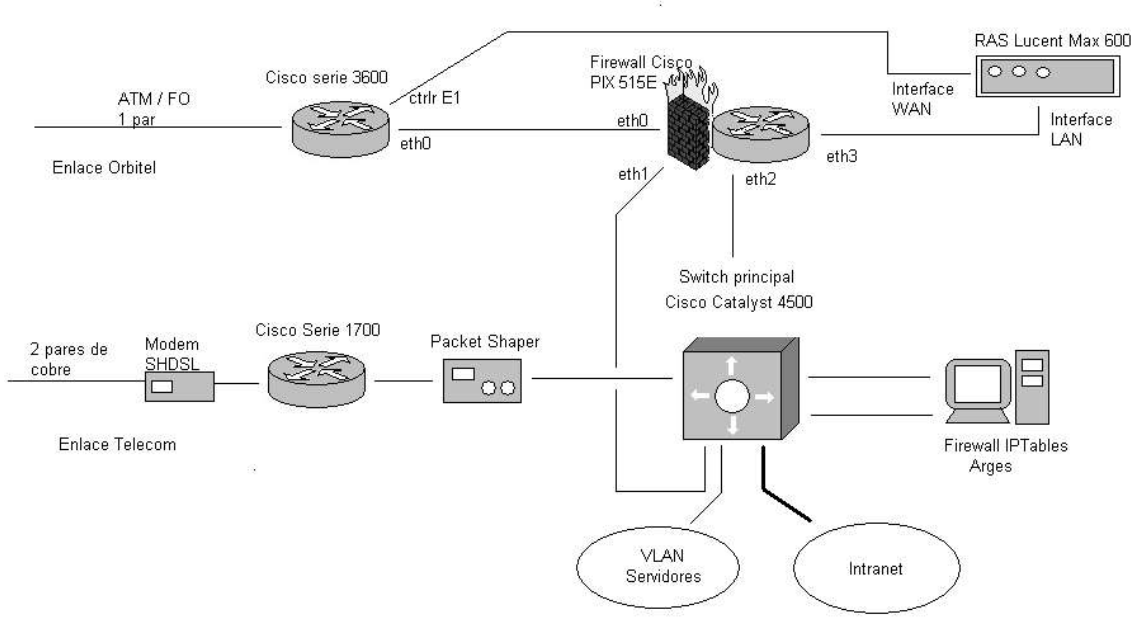


Figura 1.3 Interconexión entre Internet y la Intranet Universitaria

La Intranet universitaria se encuentra dividida en subredes IP lógicas gracias a las capacidades de enrutamiento que brinda el switch de núcleo multinivel que interconecta cada subred. La siguiente es una descripción de cada una de las subredes y se ilustra de manera lógica en la figura 1.4:

- 172.16.0.0/16: Esta subred privada aloja la mayoría de equipos de la red. A ella pertenecen todos los equipos que no tienen conexión directa a redes externas. Los equipos pertenecientes tienen acceso a recursos HTTP y FTP por medio de servidores Proxy y algunos cuentan con servicio de NAT (Traducción de Direcciones de Red) para acceso a otro tipo de recursos que no puede ser accedidos por el servicio de Proxy.

- 172.17.0.0/16: Subred privada asignada a la sede de Santander de Quilichao, enrutada por el enlace de Telecom. Cuenta con acceso a los mismos servicios que la subred anterior. Debido a que las direcciones que se usan en esta sede remota no son enrutables por ser direcciones de una red privada, en la red de Orbitel se han implementado circuitos virtuales ATM para poder enrutar estas direcciones por el mismo enlace que se enrutan las direcciones publicas de Internet.

- 172.19.0.0/16: Subred asignada a la sede del sector de las Guacas. Se enlaza por medio del enlace de Orbitel

- 172.20.0.0/16: Subred asignada a la sede de Santander de Quilichao, enrutada por el enlace de Orbitel.

- 200.21.83.64/26 y 200.21.83.128/26: Son subredes que suministra el proveedor Telecom como parte de sus servicios. Los equipos pertenecientes a estas redes poseen direcciones públicas que los hacen visibles desde redes externas directamente y usan el enlace de Telecom para la conexión externa. Cuentan con la protección del Firewall del equipo Arges que corre el servicio IPtables.

- 10.200.2.0/24: Es una subred interna pero tiene acceso a recursos externos ya que en el borde de la red estas direcciones son traducidas por el Firewall PIX a direcciones de la subred 208.195.214.0/24 que es la subred que suministra el proveedor Orbitel. Este rango de direcciones tienen el mismo comportamiento de direcciones públicas por eso se asignan a equipos que prestan servicios que necesitan ser vistos desde sitios externos a la red universitaria.

- 10.200.1.0/24: Es la subred asignada a los servidores de la Red de Datos, a ella pertenecen la mayoría de servidores de la Red de Datos como los servidores Web, de correo electrónico, DNS, entre otros. Además, esta subred se encuentra separada físicamente por una VLAN constituida por un rango de puertos físicos en el switch principal. Este rango de puertos físicos en el switch se conecta cada uno de los servidores que pertenecen a la VLAN y al Firewall para dar acceso a la VLAN a las demás redes de la Universidad.

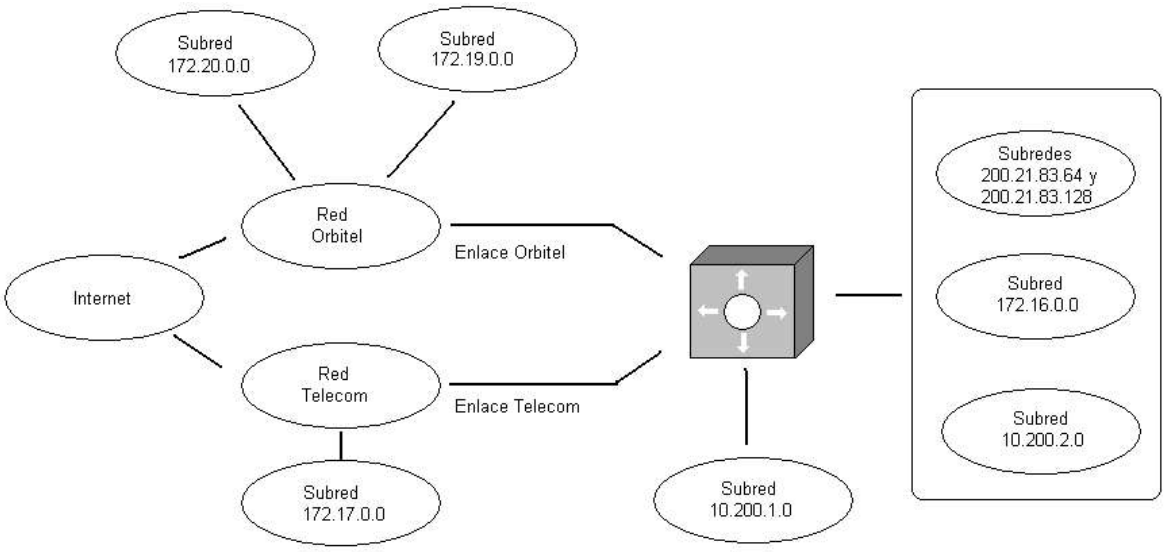


Figura 1.4 Distribución Lógica de las subredes de la Red de Datos.

La red universitaria cuenta con un enlace inalámbrico que provee el servicio a la red EHAS (Enlace Hispano-Americano de Salud), el cual presta servicio de correo electrónico de manera inalámbrica a hospitales aledaños a las poblaciones de Silvia y Guambía. La conexión de la red del proyecto EHAS se observa en la figura 1.5. Los administradores del proyecto EHAS cuentan con el servidor de correo electrónico que tiene por nombre de dominio co.ehas.org; el punto de acceso inalámbrico a la universidad se realiza por medio de un enrutador Wi-Fi el cual se conecta a una antena en el edificio de la Facultad de Ingeniería Electrónica y Telecomunicaciones. En

el otro extremo se encuentra un punto de acceso con un repetidor el cual da conexión a las poblaciones de Silvia y Guambía vía Wi-Fi. Desde estos puntos se distribuye vía VHF a los puestos de salud cercanos. La comunicación se realiza gracias al protocolo UUCP. El Protocolo Unix to Unix Copy (UUCP) permite la ejecución de comandos, transferencia de archivos y correos electrónicos entre máquinas Unix que no cuentan con ciertas condiciones necesarias para conectarse a Internet. El control de acceso a los puntos de acceso de la red EHAS se realiza por listas de direcciones MAC y por protocolo WEP (Privacidad Equivalente a Redes Alambradas). En la actualidad, ambos sistemas son vulnerables a técnicas de suplantación de direcciones MAC y técnicas de descifrado de algoritmos criptográficos débiles como los usados por WEP, respectivamente.

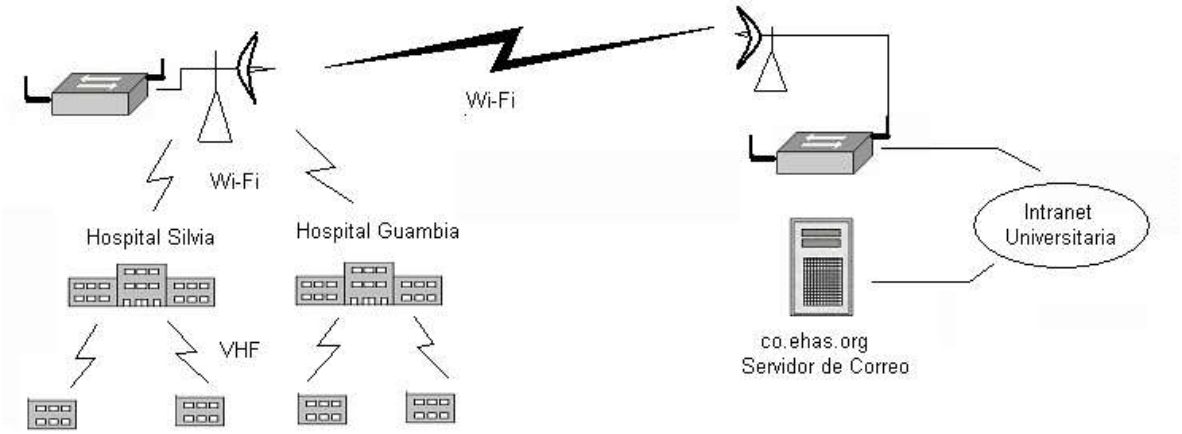


Figura 1.5 Red del Proyecto EHAS

La red universitaria pertenece a la Red Universitaria de Popayán (RUP); ésta es una Red Regional, conformada por varias universidades de Popayán que tiene como objeto promover y coordinar el desarrollo de aplicaciones avanzadas de redes de Telecomunicaciones y cómputo en la región, enfocadas al desarrollo científico y educativo de la sociedad.

La RUP se conecta a la Red Académica de Tecnología Avanzada (RENATA), que es la red de redes regionales académicas en Colombia por medio del operador nacional Telecom. RENATA a su vez se conecta a la red de Cooperación Latinoamericana de Redes Avanzadas (CLARA) para tener acceso de alta velocidad a más de 700 instituciones de educación superior y centros de investigación de América y Europa. CLARA se conecta a la red norteamericana Internet 2 y conecta a la Red Avanzada Europea GEANT gracias al proyecto América Latina Interconectada Con Europa (ALICE).

1.4.3 Infraestructura de Servicios de la Red de Datos de la Universidad del Cauca

Los servicios informáticos prestados en la Red de Datos universitaria están distribuidos por todo el campus, sin embargo se pueden identificar dos nodos que son los de mayor relevancia, los cuales son los servidores de la Red de Datos y los servidores de la división de sistemas. Estos dos nodos soportan los servicios tanto públicos, como privados de mayor importancia para los usuarios de la red.

Los servidores de la Red de Datos (Figura 1.6) se encuentran alojados en el edificio del IPET; desde este sitio se prestan los servicios básicos de Internet como servicio Web, FTP, DNS, Correo Electrónico y servicios complementarios como servicio de directorio, acceso remoto, Proxy HTTP y FTP, Bases de Datos, Restauración de copias de respaldo, alojamiento de archivos y sitios web, entre otros. En la actualidad estos servidores se encuentran protegidos perimetralmente por el Firewall PIX; ninguno cuenta con un Firewall local para proteger cada servidor ya que algunos servicios solo deben ser accedidos por puertos o desde direcciones específicas. La mayoría de servidores corren sobre la distribución Linux Debian 3.1; solo dos de los servidores que cumplen función de DNS para la Intranet corren sobre Microsoft Windows 2000 Server.

La autenticación de usuarios en muchos de los servicios públicos que presta la Red de Datos, se hace por medio del servicio de directorio que implementa el protocolo LDAP (Protocolo Ligero de Acceso a Directorio). Este servicio es prestado por el servidor *juno.unicauca.edu.co*, el cual se encuentra dentro de la red 172.16.0.0/16 para que sea accedido solo desde la Intranet, es más, en la actualidad, el servicio de directorio solo es accedido por otros servicios como correo electrónico, Web, acceso remoto, para autenticar los usuarios de dichos servicios. Pese a esta restricción de acceso, no hay implementado ningún sistema que impida a otros equipos de la Intranet, ver el servidor de directorio.

Todos los servidores de la Red de Datos prestan el servicio de Shell Seguro (SSH) que en su versión dos brinda mecanismos de autenticación y cifrado de datos por medios criptográficos muy seguros. Dependiendo del servidor este servicio es prestado a diferentes grupos dentro de los que se destacan administradores, estudiantes, profesores, funcionarios, grupos de investigación, dependencias, entre otros. La autenticación de los usuarios se realiza de forma local en cada servidor a excepción de los servidores de correo que realizan la autenticación en el servicio de directorio.

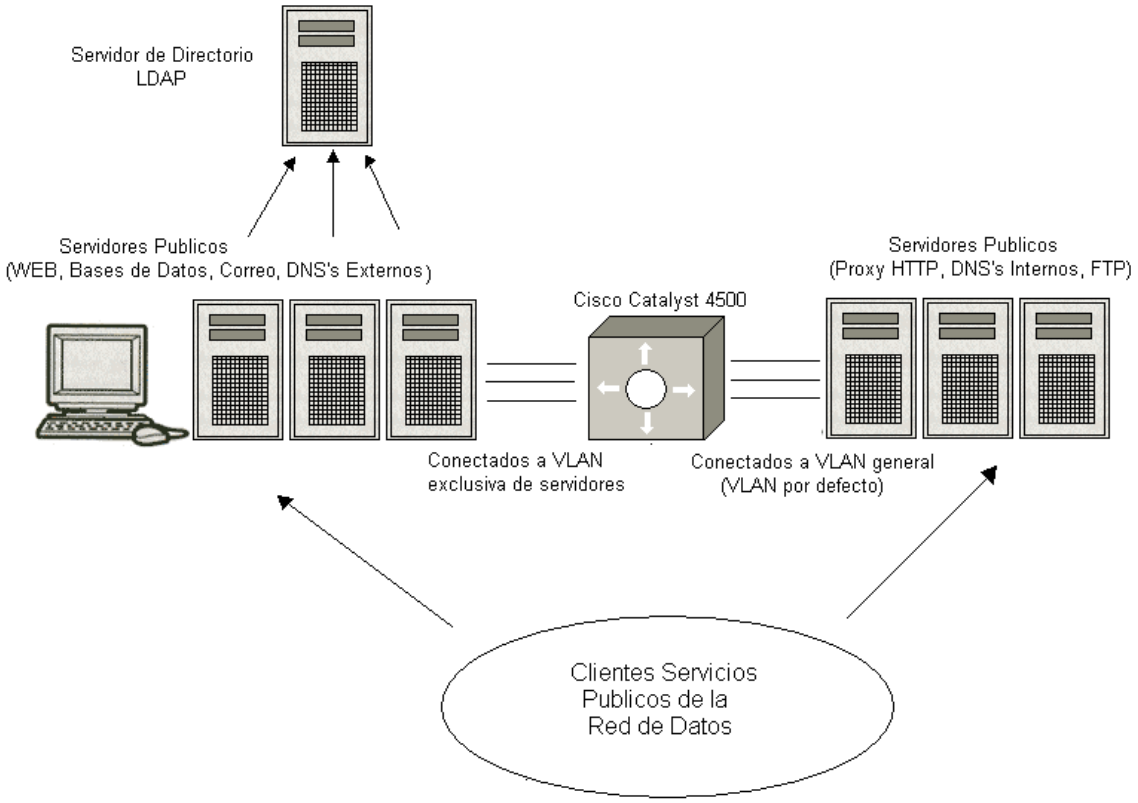


Figura 1.6 Sistemas de Información de la Red de Datos.

El servicio Web corre en el servidor *acuario.unicauca.edu.co*; este implementa el protocolo *http* por medio del servidor apache. Dicho servidor también aloja bases datos institucionales *mysql*. El acceso al servicio Web es de dominio público dentro y fuera de la universidad. A través de él, los usuarios de la Universidad pueden hacer consulta del correo electrónico por medio de login y contraseña. A partir del ingreso de esta información de autenticación, se establece con el servidor una conexión *http* sobre SSL (Secure Socket Layer - Nivel de Socket Seguro) para que la información que se intercambia entre el servidor y el cliente Web sea cifrada y autenticada por medio de certificados digitales. Sin embargo la autenticidad del servidor no puede establecerse completamente ya que el certificado digital que usa, no está firmado por una autoridad de certificación reconocida. Debido a esto aparece un mensaje en el navegador que advierte sobre la falta de confianza en el sitio que se esta visitando gracias al su certificado. Esto hace que sea fácilmente suplantado el servidor Web institucional desde otro equipo con un certificado falso para recolectar información sobre contraseñas o desplegar información falsa sobre la institución universitaria.

El servidor Web también presta servicio de FTP para los usuarios que alojan sitios Web dentro del dominio *unicauca.edu.co*. Estos usuarios son un número pequeño de dependencias y grupos de investigación que tienen sus páginas en el servidor institucional. Algunos de estos usuarios están autorizados a ejecutar comandos gracias al servicio de Shell Seguro (SSH) lo que lo hace vulnerable a la ejecución de comandos, shell scripts o exploits maliciosos para obtener privilegios no autorizados. El servicio de FTP lo ofrece el servidor *odin.unicauca.edu.co*, el cual permite acceso anónimo desde la Intranet y desde Internet. El acceso a consola está

restringido a un número pequeño de usuarios que necesitan subir archivos al servidor FTP para labores específicas, como por ejemplo las actualizaciones de antivirus.

Para la resolución de nombres por medio del servicio DNS hay dos grupos de servidores que realizan esta labor. Los primeros son servidores externos: *dns1.unicauca.edu.co* y *dns2.unicauca.edu.co,* los cuales resuelven peticiones de nombres y direcciones a solicitudes de equipos externos a la red de la Universidad; para que un equipo perteneciente a la Red de Datos con nombre completo de dominio pueda ser visto desde Internet, tienen que estar registrado en estos servidores. El servidor dns1 cumple funciones de maestro y dns2 de esclavo. Los cambios se realizan en el primero y este los replica al segundo, ambos administran las mismas zonas, dentro de las que se pueden encontrar las siguientes: *unicauca.edu.co*, *ucauca.edu.co*, *iereg.org*, *co.ehas.org*, entre otras. El segundo grupo son los servidores DNS internos: *hades.unicauca.edu.co* y *perseo.unicauca.edu.co* los cuales resuelven peticiones de nombres y direcciones a solicitudes desde la Intranet, tienen la misma configuración de zonas y de maestro-esclavo que los del primer grupo. Estos dos últimos servidores funcionan sobre el sistema operativo Microsoft Windows 2000 Server.

El servicio de correo electrónico lo prestan dos servidores, *afrodita.unicauca.edu.co* y *atenea.unicauca.edu.co*, además del servicio de shell remoto a sus respectivos usuarios. Los usuarios del primero se encuentran clasificados por estudiantes de pregrado y estudiantes de posgrado de la Universidad del Cauca y los usuarios del segundo están clasificados en docentes, funcionarios, grupos de investigación, dependencias, entre otros grupos que pertenecen a la misma institución. Las direcciones de correo de los usuarios de la Universidad son de la forma *usuario@unicauca.edu.co,* independiente de a que servidor pertenezca el usuario; gracias a la integración con el servicio de directorio, cuando un correo llega a uno de los servidores, este consulta la dirección completa y al servidor donde debe enviarla.

El servicio de acceso remoto vía telefónica se presta gracias al enlace primario RDSI para 30 canales que provee la empresa Emtel. El usuario se conecta al servidor de acceso remoto (RAS) de la Universidad que solicita autenticar al usuario por medio del protocolo RADIUS en un equipo que corre este servicio. El protocolo RADIUS realiza labores de autenticación y registro de contabilidad de usuarios que se conecta a una red de manera remota. A su vez, el servidor RADIUS autentica al usuario gracias al servicio de directorio. Después de este proceso, el usuario remoto está conectado a la Intranet por medio de la red pública conmutada.

El servicio de Proxy HTTP y FTP de la Red de Datos los prestan dos servidores, *hiperion.unicauca.edu.co* y *temis.unicauca.edu.co*, los cuales realizan traducción de direcciones a nivel de red y almacenamiento de caché de los sitios visitados por los usuarios para mejorar el rendimiento de la navegación en Internet. Los clientes de estos servidores Proxy son los equipos pertenecientes a las redes 172.17.0.0/16 y 172.17.0.0/16.

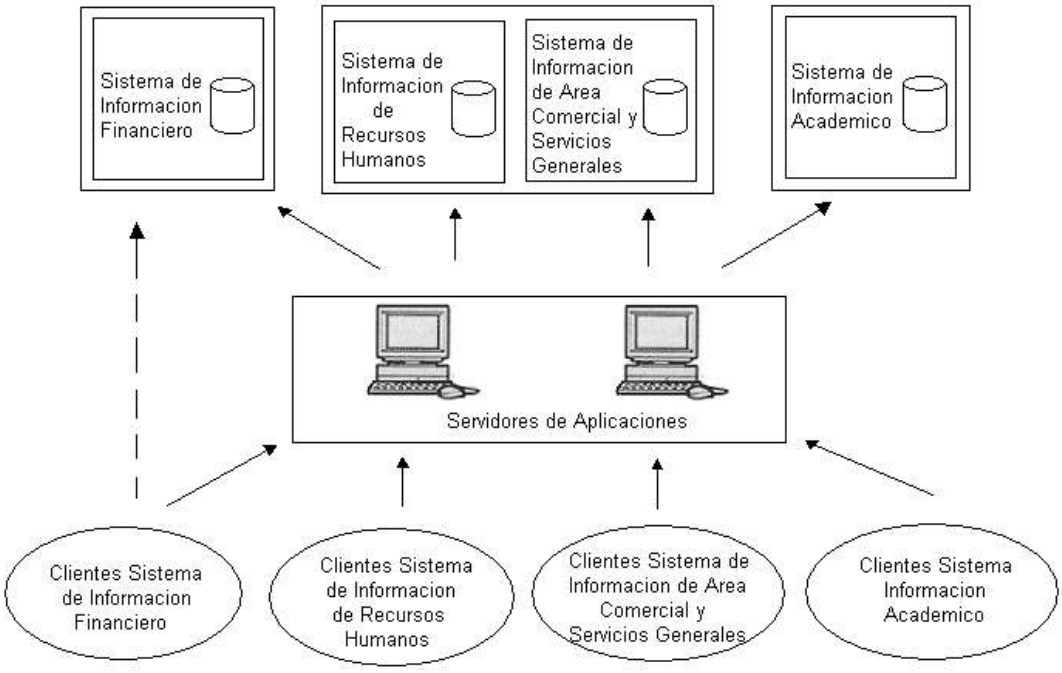


Figura 1.7 Sistemas de Información de la División de Sistemas.

Los servidores de la División de Sistemas se encuentran ubicados en el edificio de la facultad de educación y se conectan al nodo del IPET por fibra óptica. Estos servidores controlan los sistemas de información administrativos más importantes de la Universidad del Cauca como son el sistema de información financiero, el sistema de información de recursos humanos, el sistema de información de área comercial y servicios generales y el sistema de información académico. El sistema de servidores se conforma de un grupo de servidores de aplicaciones y un grupo de servidores de base de datos. Los servidores de aplicaciones operan con el sistema operativo Windows 2000 Server al igual que la mayoría de servidores de bases de datos a excepción del servidor de sistema de información académico el cual opera sobre Red Hat Advanced Server 2.1.

La Figura 1.7 muestra la organización de los sistemas de información que administra la división de sistemas. La máquina de los sistemas de información de recursos humanos y de área comercial es una sola, pero tiene creadas dos instancias para alojar ambos servidores. Los demás sistemas de información alojan sus servicios en una máquina independiente cada uno. Las bases de datos están soportadas por Oracle, las cuales gozan de gran reputación en cuanto a seguridad se refiere.

Los clientes se conectan a los servidores de aplicaciones para luego conectarse directamente al sistema de información correspondiente como por ejemplo en el sistema de información financiera que se muestra en la Figura 1.7. Los clientes de cada sistema de información no se encuentran agrupados geográficamente en el campus universitario lo que hace complejo la creación de VLANs para crear segmentos de red que permitan que solo los clientes autorizados tengan acceso a los servidores de aplicaciones y a los servidores de bases de datos de los sistemas de información. Por ejemplo, el sistema de información académico debe ser accedido por cada facultad, la división de admisiones, entre otras dependencias. La creación de LAN virtuales también es necesaria en este

escenario ya que hay sistemas que manejan información muy importante para la administración de la Universidad como por ejemplo la información de la división financiera; dicha información debe ser accedida solo por usuarios autorizados, pero en este momento, los sistemas de información se encuentran en la red 172.16.0.0/16 lo que los hace vulnerables a ataques desde equipos desde la misma subred y desde equipos de subredes diferentes debido a que, por la falta de separación de VLANs, cualquier servidor de la división de sistemas puede ser visto desde cualquier lugar de la red universitaria.

Resumen

Todo lo visto anteriormente acerca del estado actual de la Red de Datos, su infraestructura Física, Lógica y de Servicios, es una base para estudiar las principales vulnerabilidades a las que puede estar expuesta una red de comunicaciones; en el capitulo 2 se realizó un análisis detallado de éstas para crear el ámbito sobre el cuál se trabajó a lo largo del proyecto.

CAPITULO II. AMENAZAS Y VULNERABILIDADES DE SEGURIDAD EN LA RED DE DATOS DE LA UNIVERSIDAD DEL CAUCA

Las amenazas y vulnerabilidades de las redes están dadas por el riesgo que pueden sufrir los datos que éstas almacenan y transportan; entre los principales riesgos se encuentran el acceso no autorizado, la modificación no autorizada y la imposibilidad de acceder los. Establecer el valor de los datos es algo totalmente relativo, pues la información constituye un recurso que, en muchos casos, no se valora adecuadamente debido a su intangibilidad, cosa que no ocurre con los equipos, la documentación o las aplicaciones.

Existen varias arquitecturas de red para almacenar y transportar los datos de una organización; el primero es el *Modelo de Referencia OSI*, creado por la ISO (International Organization for Standarization). Este modelo no es una arquitectura en realidad porque no especifica los detalles de cada nivel; los niveles de este modelo de referencia son: Nivel físico, nivel de enlace de datos, nivel de red, nivel de transporte, nivel de sesión, nivel de presentación y nivel de aplicación.

La segunda arquitectura es la *arquitectura TCP/IP*; esta arquitectura diseñada por el Departamento de Defensa (DoD) de los Estados Unidos fue creada en la década de los 80's y hoy sirve de base para la interconexión de muchas redes tanto privadas como publicas como Internet. Esta arquitectura plantea solo cuatro niveles los cuales son: Nivel de enlace de datos, nivel de red, nivel de transporte y nivel de aplicación. Aunque el objetivo del estudio es analizar las posibles vulnerabilidades a nivel de red, en la arquitectura TCP/IP se hace necesario estudiar y analizar las posibles vulnerabilidades que se presentan en el nivel inferior (Enlace de datos) ya que este se encarga de dar soporte a los protocolos de nivel de red. Además en la arquitectura TCP/IP los protocolos de nivel de red van muy ligados a los protocolos de nivel de transporte, por lo que también se hace imprescindible tener en cuenta el nivel de transporte a la hora de realizar el estudio de seguridad.

Para agrupar el estudio de las vulnerabilidades, se clasificaron teniendo en cuenta como afectan la comunicación de datos y se encontraron cuatro posibles problemas:

- **Pérdida de Autenticación:** Ocurre cuando los datos recibidos por un miembro de la comunicación no provienen del origen del que dicen provenir.
- **Pérdida de Confidencialidad:** Ocurre cuando un intruso ajeno a una comunicación y no autorizado tiene acceso a los datos intercambiados.

- **Pérdida de Integridad:** Ocurre cuando los datos son modificados en el momento en que se transmiten, sin que los miembros de la comunicación se percaten de ello.
- **Pérdida de Disponibilidad:** Ocurre cuando los datos no pueden ser accedidos porque no se encuentran disponibles; al hablar de redes, cuando una red no está disponible.

Dentro de cada una de estas categorías se encuentran muchas técnicas que se aprovechan de estos problemas que presentan las redes LAN (Local Área Network – Redes de Área Local) y en particular las redes IP, tanto cableadas como inalámbricas, como es el caso de la red universitaria.

2.1 PÉRDIDA DE AUTENTICACIÓN

2.1.1 Suplantación IP (IP Spoofing)

Debido al diseño del protocolo IP, es muy fácil cambiar las direcciones de origen o destino de una trama. Para los ataques de IP Spoofing lo que se hace es alterar la dirección de origen de un datagrama IP para que el destino de determinada comunicación sea engañado por el atacante. La suplantación IP se usa para tipos de engaño, que son: el acceso a recursos que se basan en autenticación por dirección IP, el secuestro de sesiones TCP o simplemente para ocultar la verdadera identidad de un atacante ya sea para el escaneo de un equipo o una red, así como para lanzar un ataque de denegación de servicio engañando a su víctima. El primer caso ocurre cuando desde su equipo, un atacante simula la identidad de otra máquina de la red para conseguir acceso a recursos de un tercer sistema que ha establecido algún tipo de confianza basada en la dirección IP del terminal suplantado. Y como los anillos de confianza basados en estas características tan fácilmente falsificables son aún abundantes (por ejemplo, los comandos '*r*', los accesos NFS, o la protección de servicios de red mediante TCP Wrapper), el Spoofing es en la actualidad un ataque, aunque complejo, factible contra cualquier tipo de organización.

En la suplantación IP entran en juego tres máquinas: un atacante, un atacado, y un sistema suplantado; entre los dos últimos debe existir una relación de confianza. Los administradores establecen relaciones de confianza entre los terminales, que buscan evitar mecanismos de autenticación como la solicitud de login y password para facilitar el acceso o para automatizar procesos que no podrían realizarse si fueran necesarios dichos mecanismos de autenticación. El objetivo del atacante es suplantar la identidad basada en la dirección IP de una de las máquinas para poder acceder sin necesidad de autenticarse en la otra. Para lograr su objetivo necesita por un lado establecer una comunicación con una dirección falsa, y por otro evitar que el equipo suplantado interfiera en el ataque. Lo primero se puede lograr con múltiples herramientas que existen para realizar ataque IP Spoofing o desarrollar un programa propio con librerías de programación para redes como Libnet[1]. Lo segundo lo puede realizar con ataques de denegación de servicio DoS (Denial

[1] Librería LIBNET, disponible en http://www.packetfactory.net/libnet/

of Service – Denegación de Servicio), los cuales serán descritos más adelante, o simplemente esperando a que la máquina a suplantar esté sin actividad.

Establecimiento de una conexión TCP

Una vez el atacante puede suplantar la IP de una de las máquinas que es considerada de confianza, debe proceder a establecer la conexión; para ello tiene que hacer uso del protocolo TCP[2], el cual es un protocolo de nivel de transporte que presta sus servicios a los protocolos de nivel de aplicación. Como muestra la figura 2.1, el establecimiento de una conexión TCP es casi de naturaleza ceremonial, involucrando lo que comúnmente se conoce como el protocolo de intercambio; esto debería ocurrir antes de que se intercambie cualquier dato entre los hosts. El cliente que en este caso es el host A, inicia una conexión con el servidor o host de destino, host B. Los pasos del protocolo de intercambio son los siguientes:

1. El host A envía un segmento TCP SYN para señalizar una petición de conexión TCP al host B con un número de secuencia escogido aleatoriamente que identifica al segmento TCP.
2. Si el host B funciona, ofrece el servicio deseado y puede aceptar la conexión, envía al host A una petición de conexión señalizada con un nuevo SYN identificado por un nuevo número de secuencia que también se escoge aleatoriamente y acusa recibo de la petición de conexión al host A con un ACK identificado con el número de secuencia que recibió en el SYN mas uno. Todo esto se lleva a cabo en un solo paquete.
3. Para terminar, si el cliente recibe el SYN y el ACK, con sus respectivos números de secuencia y todavía quiere continuar con la conexión, envía el último ACK solitario al host B. Este acusa recibo de que el cliente ha recibido la petición de conexión del host B.

Después de ejecutado así el protocolo de intercambio, se establece la conexión. Ahora se pueden intercambiar los datos entre los dos equipos. Si se examina con más detalle se puede observar que se han establecido dos conexiones. La primera se establece entre el cliente y el servidor y la segunda entre el servidor y el cliente; esto es así porque TCP es de doble dirección, lo que significa que los intercambios de datos pueden viajar en ambas direcciones independientemente.

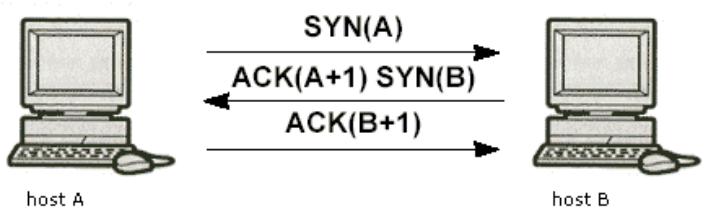


Figura 2.1 Establecimiento de una conexión TCP

[2] TCP - Transmission Control Protocol

Si puede poner fuera de servicio a la máquina suplantada y si puede generar datagramas IP con dirección falsa, el atacante puede continuar con su ataque y para ello debe establecer una conexión TCP con la víctima.

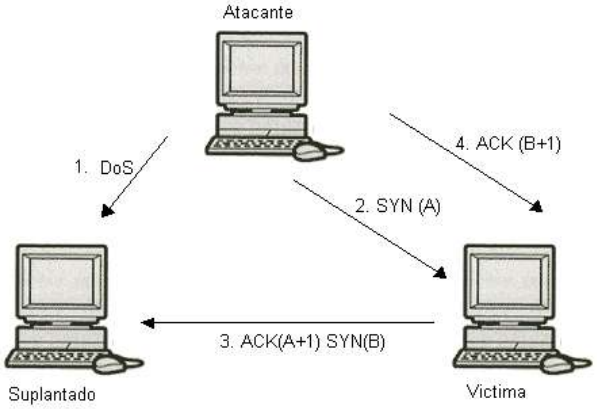


Figura 2.2 Generación de un ataque de suplantación IP

Para ello realiza los siguientes pasos:

1. Enviar un ataque de denegación de servicio DoS sobre la máquina que quiere suplantar para que ésta esté incapacitada de enviar respuestas a la máquina víctima cuando se produzca el ataque de IP Spoofing.
2. El atacante solicita establecer una conexión con la víctima enviando un segmento TCP de sincronización SYN con un determinado número de secuencia escogido aleatoriamente, utilizando en el datagrama IP la dirección IP de la máquina suplantada.
3. La víctima envía una respuesta TCP con un ACK identificado con el número de secuencia recibido en el SYN del paso anterior mas uno y también establece una conexión TCP con la máquina suplantada enviándole un segmento TCP de SYN con su propio número de secuencia a la dirección de la máquina suplantada. Debido a que esta máquina se encuentra incapacitada para responder el atacante debe enviar esta respuesta.
4. El atacante envía la respuesta que espera la víctima la cual es un segmento TCP ACK para aceptar la conexión que quiere establecer dicha víctima; para que el establecimiento de la conexión sea exitoso, este último segmento debe ser enviado con el número de secuencia correcto que es el número de secuencia enviado por la víctima en el paso anterior mas uno; si se envía con un número erróneo la víctima terminará la conexión devolviendo un segmento TCP RST (Reset). Dependiendo de cómo se obtenga el conocimiento de los números de secuencia con que la víctima responde, el IP Spoofing se clasifica en *ciego* (blind) y *no ciego* (no blind).

2.1.1.1 Suplantación IP No Ciega (Non Blind IP Spoofing)

Este ataque toma lugar cuando el atacante y la víctima se encuentran en la misma subred. Debido a esto, el atacante puede conocer los números de secuencia con los que la víctima establece la conexión simplemente utilizando un sniffer para olfatear el tráfico de la red de la máquina suplantada, para saber con que números responder a los segmentos TCP recibidos, eliminando la potencial dificultad de calcularlos exactamente y después de completar el protocolo de intercambio poder enviar datos a la víctima por medio de los segmentos TCP y así entrar a la máquina sin necesidad de autenticarse gracias a la relación de confianza.

Este método es relativamente sencillo de ejecutar, pero impone la restricción de que las máquinas involucradas pertenezcan a la misma subred. Sin embargo, también puede llevarse a cabo cuando se pertenece a diferentes subredes dentro de una Intranet o desde una red externa a una Intranet.

2.1.1.2 Suplantación IP Ciega (Blind IP Spoofing)

Este ataque es más sofisticado ya que los números de secuencia con los que la víctima responderá no podrán ser conocidos por el atacante ya que al estar en una red externa, la utilización de un sniffer es ineficaz; por lo tanto el atacante tendrá que predecir dichos números para que su engaño funcione. Años atrás los sistemas operativos más populares usaban técnicas básicas para generar los números de secuencia; debido a esto un atacante solo tenia que enviar varios paquetes SYN a una máquina objetivo para tomar muestras de los números de secuencia con que dicha máquina genera sus segmentos TCP SYN; con dichas muestras el atacante podría obtener una fórmula para calcular estos números y así predecir con que números responderá la víctima cuando realice el ataque. Sin embargo, los sistemas operativos de la actualidad utilizan la generación de números aleatorios haciendo más difícil el trabajo de predecirlos exactamente. Para evitar este tipo de suplantación deben estudiarse mecanismos de seguridad perimetral para proteger la red de dichas vulnerabilidades que pueden ser aprovechadas desde cualquier lugar externo a la red universitaria.

2.1.1.3 Vulnerabilidades que hacen Posible la Suplantación IP

Como se estudió, para que un ataque de IP Spoofing sea exitoso deben existir tres factores que son:

- Tener un recurso o servicio ofrecido por un host el cual permita acceso por autenticación de dirección IP también conocido como autenticación por host tales como servicios de llamadas a procedimiento remoto RPC (Remote Procedure Call) por ejemplo NFS (Network File System), o NIS (Network Information System), o la suite de servicios R como rlogin o rsh, o cualquier otro tipo de servicio que permita la autenticación por dirección IP.
- Que exista una relación entre un cliente que quiera acceder a un servicio o recurso como los mencionados en el punto anterior y que al acceder no le sea solicitado un password o cualquier forma de autenticación diferente a la dirección IP.
- Que la implementación de la pila TCP/IP del sistema que ofrece el servicio o el recurso sea susceptible a la predicción de los números de secuencia TCP.

Para buscar un servicio vulnerable, simplemente puede usarse un analizador de protocolos o un sniffer para analizar el tráfico que hay en la red, como por ejemplo el analizador de protocolos *Ethereal*[3], para observar el acceso a servicios como rlogin o NFS entre máquinas que tengan relaciones de confianza. En la siguiente práctica se analiza como encontrar posibles conexiones NFS que no requieren autenticación. NFS es uno de los servicios del conjunto de servicios de RPC (Llamada a Procedimiento Remoto) creados por SUN Microsystems[4]. Las llamadas a procedimiento remoto son interfaces de programación para una relación cliente servidor entre dos sistemas. Pueden utilizar TCP o UDP. Fueron diseñadas para facilitar la programación de los servicios de red. Fundamentalmente, el procedimiento es que el cliente invoque un proceso o procedimiento a través de la red; desde el principio la idea era utilizar puertos efímeros para estos procedimientos; sin embargo, ciertos puertos tienen más posibilidades de hospedar ciertos servicios, un hecho que no se les ha escapado a los posibles atacantes. Un programa llamado *portmap* escucha en el puerto 111 (TCP y UDP) y proporciona el número del servicio. Obtener el número del servicio RPC directamente de *portmap* no es difícil para los atacantes. Por ejemplo un programa de usuario llamado *rcpinfo* obtiene todos los servicios y crea una tabla de los puertos y donde están ubicados. Uno de estos servicios es NFS el cual permite montar en la máquina local un sistema de archivos que se encuentra en una máquina remota; después de esto en la máquina local se puede acceder al sistema de archivos como si estuviera montado localmente.

Figura 2.3 Funcionamiento de NFS

En la figura 2.3 aparece el esquema implementado para la práctica; ambos equipos corren bajo el sistema operativo Linux Debian 3.1; el host A operará como cliente y el host B como servidor, cada uno con su correspondiente aplicación NFS para cliente y servidor, para que desde el host A se tenga acceso al sistema de archivos */home* del host B sin necesidad de autenticación y con todos los privilegios del superusuario (que en Linux recibe el nombre de root), se agregó la siguiente línea al archivo */etc/exports* del servidor (host B):

/home 172.16.255.134(rw,no_root_squash,sync)

Se observa que el sistema de archivos a compartir es */home*, también que se va a tener acceso a este sistema de archivos por NFS solo desde la dirección 172.16.255.134 que es la dirección IP del host A, con permisos de lectura y escritura y que no solicite password para el usuario *root*; en otras palabras se esta haciendo autenticación para el usuario *root* solo por dirección IP y sería vulnerable a ser engañado por una suplantación IP. Desde el host A se ejecuta el siguiente comando:

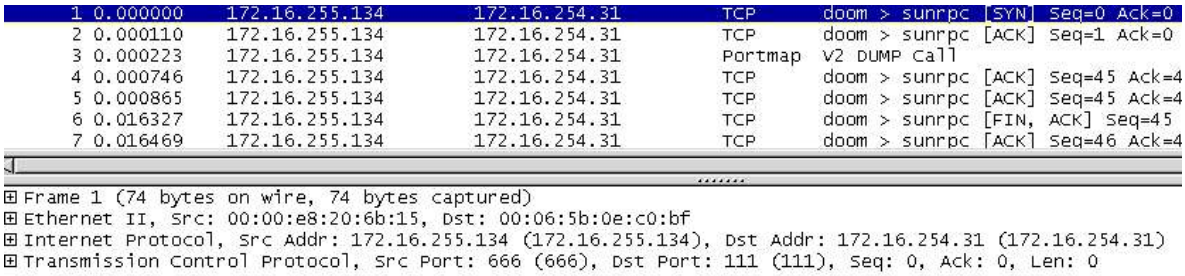
[3] Analizador de Protocolos Ethereal, disponible en todas las plataformas y además provee soporte para analizar tramas IPv6. Disponible en www.ethereal.com/download.html

[4] Estos servicios se encuentran en la lista de las diez vulnerabilidades más explotadas en http://www.sans.org/topten.htm

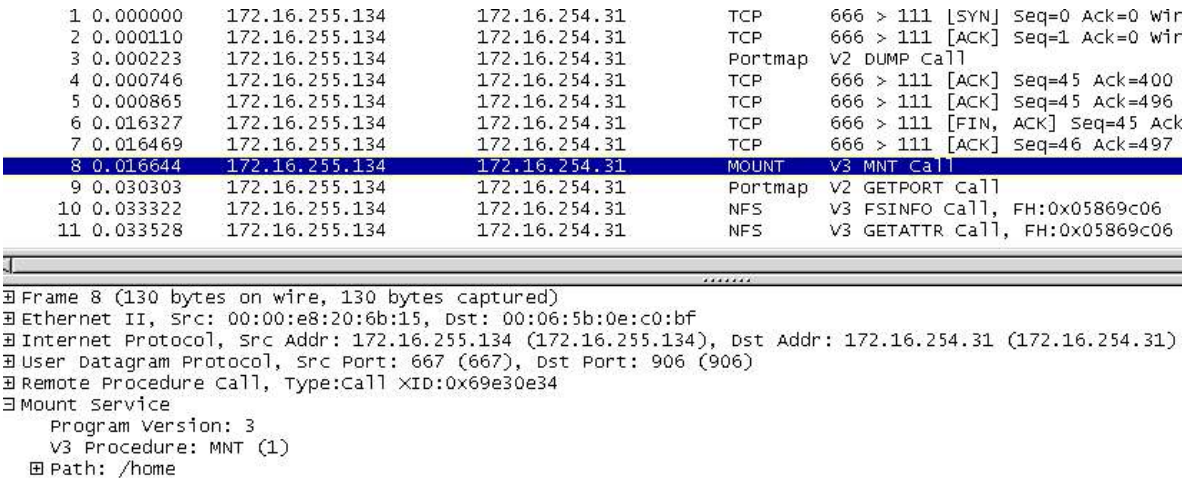
#mount -t nfs 172.16.254.31:/home /home/prueba

Si un atacante pudiera enviar el equivalente a este comando al host B suplantando la dirección del host A, tendría privilegios de lectura y escritura sobre el sistema de archivos en el host remoto, podría leer, borrar, editar e introducir nuevos archivos, en el host atacado.

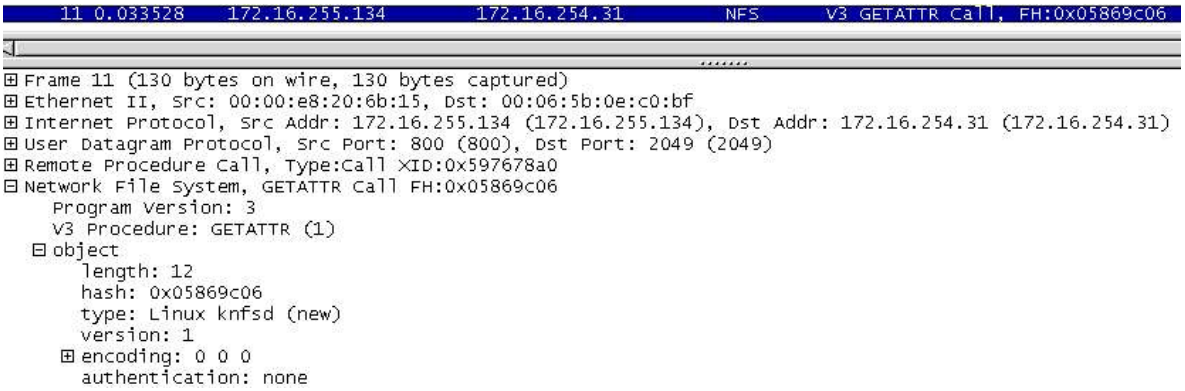
Para identificar que máquinas ofrecen y que máquinas solicitan servicios RPC, basta con olfatear el tráfico que se dirija hacia o desde el puerto TCP 111, por el cual un servidor RPC escucha por medio del *portmap* para ofrecer sus servicios. En *Ethereal* debe ponerse como filtro la siguiente cadena de caracteres para que escuche cualquier conexión desde o hacia el puerto: *port 111;* cuando el host A intenta conectarse al host B vía NFS se realizó la siguiente captura de tráfico:



Si se observa la parte inferior de la captura, se encuentra información detallada de la primer trama capturada, en la cual se analiza que se intenta establecer una conexión TCP desde la dirección 172.16.255.134 y el puerto 666 hacia la dirección 172.16.254.31 y puerto 111 (*sunrcp*); esta captura no ofrece mucha información adicional ya que la siguiente parte de la conexión NFS se realiza en puertos diferentes al 111 y por UDP, sin embargo, teniendo las direcciones IP involucradas en la conexión se configuro Ethereal para que capturara el tráfico que viaja con la dirección de origen del host A y de destino del host B, estableciendo como filtro la siguiente expresión: *src host 172.16.255.134 && dst host 172.16.254.31* y se obtuvo lo siguiente:



En los detalles de la trama seleccionada se puede observar que se puede obtener el sistema de archivos al que se esta accediendo que en este caso es /home; además se puede ver que para acceder al sistema de archivos no hay necesidad de autenticación como se detalla en la última trama capturada mostrada en la siguiente captura:



Con la información recopilada un atacante podría establecer como una máquina objetivo el host B para realizar un ataque de suplantación IP. Este método aunque provee mucha información sobre un posible objetivo, tiene un alcance limitado ya que seria necesario que las tres máquinas, atacante, suplantada y víctima estuvieran en la misma subred para tener acceso a las tramas que intercambian. Otro método con mayor alcance pero que provee menos información es utilizar la herramienta *nmap*[5], la cual puede realizar escaneo de la red en busca de máquinas que presten servicios RPC. Nmap realiza la exploración por medio del envío de paquetes TCP SYN con la opción –S, por esta razón se puede hacer exploración entre subredes. Por ejemplo si se examina si el equipo con dirección 172.16.254.31 tiene el puerto 111 en escucha, se usa *nmap* de la siguiente manera:

```
akira:~# nmap -p 111 172.16.254.31
Starting nmap 3.81 ( http://www.insecure.org/nmap/ ) at 2005-08-25 16:29 COT
Interesting ports on icarus.unicauca.edu.co (172.16.254.31):
PORT    STATE SERVICE
111/tcp open  rpcbind
MAC Address: 00:06:5B:0E:C0:BF (Dell Computer)
Nmap finished: 1 IP address (1 host up) scanned in 0.359 seconds
```

Como se puede observar solo se conoce si el equipo presta servicios RPC, pero no se puede saber cual de los RPC, tampoco con que equipo u equipos puede tener una relación de confianza ni mucho menos si las relaciones de confianza se prestan sin necesidad de autenticación con password.

Otras utilidades que son posible blanco para un ataque de suplantación IP, son las utilidades 'r' y una de las más conocidas es *rlogin*; esta herramienta permite el acceso de un usuario a un servidor el cual le provee un shell o consola de comandos. Por defecto la autenticación para el acceso del usuario se realiza por medio de nombre de usuario y contraseña, sin embargo, el administrador del servidor que corre rlogin puede alterar este mecanismo de autenticación permitiendo que determinado usuario inicie una sesión en el

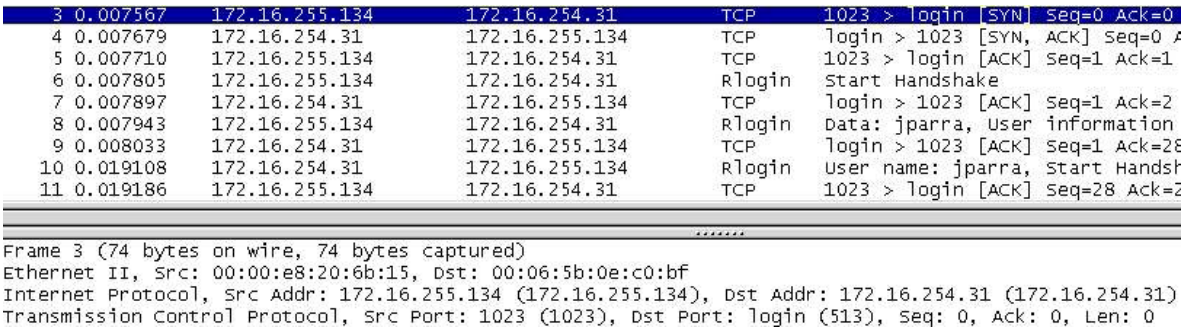
[5] Herramienta de gestión de la red, disponible en www.insecure.org/nmap

servidor; si lo hace desde un equipo con una dirección IP determinada, al hacer esto el administrador crea una relación de confianza con la máquina remota a la cual le solicita autenticación por dirección IP, volviendo el servicio de rlogin vulnerable a un ataque de suplantación IP.

Se llevo a cabo una práctica en la cual se tiene la misma configuración de la figura 2.3, pero en este caso el host B actúa como un servidor de rlogin y el host A es su cliente; el administrador del host A creó una relación de confianza para que el usuario con login jparra pudiera acceder al servidor sin digitar login y password, si lo hace desde el equipo con dirección IP 172.16.255.134. Esto se logra modificando el archivo /etc/hosts.equiv el cual contiene lo siguiente:

172.16.255.134 jparra

De esta manera el usuario *jparra* pudo acceder al host B desde el host A sin necesidad de una contraseña. Durante esta conexión se capturó el siguiente tráfico:



Como se puede observar en la trama número 3, la cual se encuentra seleccionada, se inicia el establecimiento de conexión desde la dirección IP 172.16.255.134 por el puerto TCP 1023 hacia la dirección IP 172.16.254.31 en el puerto TCP 513 (login), el cual es el puerto designado para la escucha de solicitudes de conexión con el protocolo rlogin; también se detalla el usuario con el que se intenta la conexión dando información muy valiosa para generar un posible ataque; en este caso, la obtención de información se da gracias a que el equipo desde donde se capturó el tráfico esta en la misma subred de la víctima. Para no tener esta restricción, puede usarse igualmente el programa *nmap*, pero ahora que explore si la dirección 172.16.254.31 escucha por el puerto TCP 513 con lo que se obtuvo:

```
akira:~# nmap -p 513 172.16.254.31
Starting nmap 3.81 ( http://www.insecure.org/nmap/ ) at 2005-08-25 16:33 COT
Interesting ports on icarus.unicauca.edu.co (172.16.254.31):
PORT    STATE SERVICE
513/tcp open  login
MAC Address: 00:06:5B:0E:C0:BF (Dell Computer)
Nmap finished: 1 IP address (1 host up) scanned in 0.349 seconds
```

Como se puede observar, en este caso solo se observa si los hosts analizados ofrecen servicios de acceso remoto, en este caso, el servicio *rlogin*, pero no puede saberse si el equipo analizado permite el acceso a determinado usuario con autenticación por dirección IP y si es así, tampoco se sabe a que usuario se permite.

2.1.1.4 Secuestro de Sesiones TCP por medio de Suplantación IP

Los dos tipos de suplantación IP estudiados basan su ataque en el establecimiento de la conexión TCP para vulnerar mecanismos de autenticación basados en dirección IP; este ataque puede llevarse a cabo en cualquier momento. El secuestro de sesiones TCP se realiza cuando ya se ha establecido la conexión TCP o sea cuando existe intercambio de datos entre las máquinas conectadas; este ataque es usado cuando se quiere acceder a recursos o privilegios de un usuario que se ha autenticado previamente y el cual sigue conectado al momento del ataque, pero esta no es la única restricción para el atacante, puesto que debe encontrarse en la misma subred de uno de los dos extremos de la conexión ya que es necesario que obtenga acceso a los parámetros que mantienen la sesión TCP los cuales son:

- Las direcciones IP de los equipos involucrados, las cuales no cambian durante el intercambio de datos.
- Los puertos TCP, que en la mayoría de protocolos se comunican por puertos establecidos y no cambian.
- Los números de secuencia, los cuales cambian desde el número de secuencia inicial en función del número agregado de bytes enviados desde un equipo al otro.
- Los números de acuse de recibo, los cuales cambian en función de los números de secuencia entregados y los bytes agregados de los que se acusa el recibo de un equipo a otro.

El ataque de secuestro de sesión TCP ocurre después de un intercambio normal de datos cuando el atacante introduce tráfico TCP suplantando la dirección IP de la víctima basado en los parámetros de la sesión, que son los números de puertos, de secuencia y de acuse de recibo. La grafica 3.4 ilustra los pasos que se siguen para secuestrar una sesión TCP, los pasos de establecimiento de conexión se han ejecutado previamente y a partir del paso 1 se produce el intercambio de datos:

En el paso 1 el host A envía un segmento TCP con número de secuencia A y la bandera PSH activada para indicar que los datos transmitidos se transfieran el protocolo de nivel superior; el número de bytes de datos es 30; además se envía acuse de recibo ACK de número B que se ha establecido previamente cuando se estableció la conexión. En el paso número 2 el host B envía 20 bytes de datos con número de secuencia B y acusa recibo de los bytes que van desde el número de secuencia A mas el número de bytes de datos que transmitió A hacia B. Este procedimiento ocurre en los pasos 3 y 4, hasta que el atacante interviene en el paso 5 creando un estado de desincronización. El estado de desincronización ocurre cuando el próximo byte a ser enviado por el host A es diferente del número de secuencia del próximo byte a ser recibido por el host B; una forma de lograrlo es suplantando la dirección de host A y generando un segmento TCP tal y como lo haría el verdadero host A, con los números de secuencia y de acuse de recibo correctos; para ello tiene que usar un sniffer o un analizador de protocolos y poder ver estos valores, para que cuando el host A transmita el

segmento que cree que es correcto, como en el paso 7, el host B rechace este segmento ya que el host B esta pidiendo que le envíe el segmento que empieza por el número de secuencia A+90.

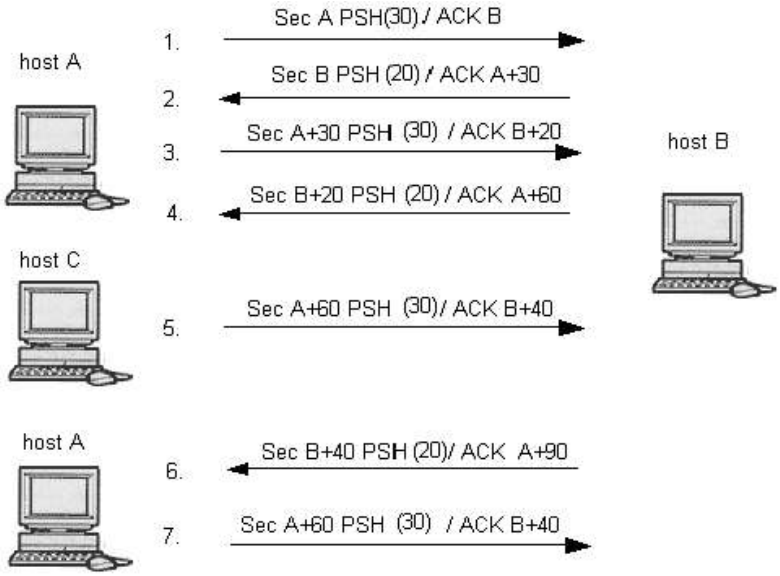


Figura 2.4 Secuestro de una sesión TCP

El propósito de crear el estado de desincronización es que los hosts no puedan seguir intercambiando datos ya que cada host no conoce el número correcto en el que se encuentran los números de secuencia del otro; como el único que los conoce es el atacante, se puede decir que la sesión TCP le pertenece al atacante y por eso se denomina *secuestro de sesión*. Debido a que el atacante puede escuchar cualquier tráfico intercambiado entre los equipos y puede suplantar los paquetes IP de cualquiera de los dos extremos, el resultado es que todo el flujo TCP pasa a través del atacante, donde él puede agregar o quitar información del flujo TCP; esto es especialmente útil en secuestro de sesiones de acceso remoto como *telnet*, donde se podría introducir cualquier tipo de comando como por ejemplo *#echo + + > ~/.rhosts*, lo que permitiría el acceso para el usuario que ha sido víctima del ataque sin necesidad de introducir contraseña.

Cuando el atacante genera el estado de desincronización, genera un estado estable mientras no se transmitan datos; si se transmiten datos, pueden darse dos casos:

- Si el número de secuencia del próximo byte a ser enviado por el host B es menor que el próximo byte a ser recibido por el host A, mas el número de bytes de datos enviados, pero el próximo byte a ser enviado por el host B es mayor que el próximo byte a ser recibido por el host A, el paquete es aceptado y puede ser almacenado para ser usado después (dependiendo del sistema operativo).

- Si el número de secuencia del próximo byte a ser enviado por el host B es mayor que el próximo byte a ser recibido por el host A más el número de bytes de datos enviados, ó el número de secuencia del próximo byte a ser enviado por el host B es menor que el próximo byte a ser recibido por el host A, el paquete es rechazado y se pierden los datos que contenía.

Existe una falla dentro del ataque y es conocida como la tormenta de ACK; se presenta debido a que cuando un equipo recibe un segmento TCP no sincronizado, el equipo lo reconoce y envía un segmento TCP enviando el número de secuencia esperado y usando su número de secuencia; este paquete que también esta desincronizado, puesto que la secuencia ha sido alterada por el atacante, también generará un segmento ACK incorrecto formando un ciclo infinito para cada segmento de datos enviados. El atacante puede resolver el problema de la tormenta ACK si utiliza suplantación ARP (ARP spoofing); este ataque será explicado en otra sección. Esta técnica es la usada por el programa *hunt*, el cual es un software usado específicamente para el secuestro de sesiones TCP.

2.1.1.5 Posibles Vulnerabilidades de Suplantación IP en la Red de Datos de la Universidad del Cauca

Lo primero que se realizó fue examinar la red de la Universidad en busca de máquinas que ofrecen servicios de llamada a procedimiento remoto (RPC) en el puerto 111 o servicios prestados por las utilidades 'r' en el puerto 513; para esto se utilizó el programa *nmap* de la siguiente manera:

#nmap –s –p 111 172.16..**

Dado que la red universitaria no esta dividida en subredes y que la dirección de la red es la de una red privada clase B, 172.16.0.0, con el comando anterior se busca en todos los host cuya dirección empiece por 172.16.*.* que son todos los hosts que pertenecen a la Intranet de la Universidad y que tengan el puerto 111 en escucha. También puede ejecutarse el comando anterior remplazando el último argumento con 200.21.83.64, 200.21.83.128 o 208.195.214.* los cuales son los prefijos de las redes que los proveedores de servicios Telecom y Orbitel han asignado a la red de la Universidad en la actualidad; incluso puede explorar cualquier equipo o red externa a la red de la Universidad la cual pueda ser vista desde Internet. Del mismo modo un atacante puede explorar desde cualquier parte del mundo las redes públicas que tiene asignada la institución, debido a que cualquier equipo en la red tiene una dirección de Intranet y solo basta analizar la dirección de red interna para tener un barrido total. Con este análisis se obtuvo:

```
Starting nmap 3.81 ( http://www.insecure.org/nmap/ ) at 2005-08-25 19:35 COT
Interesting ports on 172.16.2.45:
PORT    STATE    SERVICE
111/tcp filtered rpcbind
MAC Address: 00:13:C4:4D:79:FF (Unknown)
Interesting ports on mina.unicauca.edu.co (172.16.42.6):
PORT    STATE SERVICE
111/tcp open  rpcbind
MAC Address: 00:13:C4:4D:79:FF (Unknown)
```

El análisis se realizó en las horas de la noche; a esta hora no hay estaciones de trabajo de funcionarios o profesores en operación pero sin embargo, fueron encontrados 255 equipos de los cuales 30 tienen el puerto RCP en estado abierto, 96 lo tenían cerrado y 129

en estado filtrado por algún tipo de Firewall. Se analizó los de mayor importancia los cuales son los servidores y las estaciones de trabajo de la Red de Datos, los cuales están distribuidos en las direcciones 172.16.255.*; se encontró que en las estaciones de trabajo el puerto esta abierto y en la mayoría de servidores también se encuentra abierto tales como: servidores de correo (172.16.255.130, 172.16.255.129), servidor de directorio (172.16.255.135), servidores Proxy (172.16.255.211, 172.16.255.212).

También se realizó esta operación en busca de puertos 513 (rlogin) abiertos obteniendo que ninguno se encontraba en escucha ya que la mayoría estaban cerrados y unos pocos se encontraban filtrados.

Sin embargo, para que los sistemas detectados sean vulnerables a una suplantación IP (ciega o no ciega) deben establecer una relación con una o más máquinas; no hay una manera rápida para detectar esto, ya que se tendría que examinar el tráfico en muchos puntos de la Universidad, así que para detectar estas vulnerabilidades se encuestó a los administradores de los puntos más importantes de la red, los cuales son los servidores de la Red de Datos y los servidores de la división se sistemas.

En los servidores y estaciones de trabajo de la Red de Datos, se examinaron uno a uno cada servidor, encontrándose que en el servidor ***Hiperion***, el cual cumple la función de servidor *Proxy HTTP*, y la estación de trabajo ***Akira*** se ofrecía el servicio de NFS sobre una partición del disco duro; esto se realiza para implementar el sistema de copias de respaldo (backups) en disco. Para generar la copia de respaldo, cada servidor monta localmente la partición que compartía *Hiperion* y *Akira*, copiaba los archivos de los que va a realizar el respaldo y desmonta la partición. Todo esto se realizaba por medio de una relación de confianza la cual permitía el acceso sin contraseña desde cada servidor por autenticación de dirección IP, solo a los servidores que necesitan hacer la copia y que son permitidos por el administrador de *Akira* e *Hiperion*; este acceso se permitía con privilegios de superusuario (*root*). Este proceso tenia estas características ya que era un procedimiento automático y temporizado por parte de los servidores en el cual no se podía tener un proceso interactivo, como la digitación de una contraseña y se necesita los privilegios de *root*, ya que los sistemas de archivos de los que se realiza el backup solo pueden ser accedidos por este usuario. En este momento se esta planeando cambiar el sistema de copias de respaldo para que sea realizado sobre cintas magnéticas por medio de la herramienta *flexbackup*; esta herramienta permite el acceso a los sistemas de archivos remotos por medio de *rlogin* o por medio de *ssh*. Ambos métodos permiten el login remoto sin la necesidad de contraseña pero el segundo método no es vulnerable a la suplantación IP ya que la autenticación no la realiza basada en la dirección IP de la máquina que intenta tener la relación de confianza, sino en las propiedades de las llaves criptográficas con que trabaja el protocolo *ssh*.

El análisis anterior demuestra que solo la estación de trabajo *akira* es vulnerable a un ataque de suplantación IP no ciega, ya que ofrece un servicio de llamada a procedimiento remoto y tiene relaciones de confianza con otros servidores; además los servidores y la estación de trabajo se encuentran en una red física diferente, ya que no se encuentran conectados al mismo switch; los primeros se encuentran en el Instituto de Postgrados y la segunda en la Facultad de Ciencias de la Educación. Debido a que la suplantación IP no ciega se basa en la escucha de los números de secuencia TCP, un atacante que pueda obtener estos números colocando un sniffer en el trayecto mencionado puede lanzar un ataque de esta naturaleza y lograría tener acceso a información muy importante. El servidor *Hiperion* por el contrario, no seria vulnerable a la suplantación IP no ciega ya que se encuentra conectado al mismo switch

de los servidores con los que tiene la relación de confianza así que la utilización de un sniffer no seria efectiva desde cualquier punto de la red de la Universidad, incluso si el atacante pudiera tener acceso a la sala de servidores y conectara su sniffer al mismo switch de los servidores. La única posibilidad que tendría para escuchar el tráfico entre los servidores, seria conectar un concentrador (HUB) a uno de los puertos del switch y desde ahí conectar uno de los servidores involucrados y su sniffer. Esto representaría un gran trabajo para una persona ajena a la administración de los servidores, aunque no existe una política de acceso a las salas de computadores y de servidores, además de una política de conexión a los puntos de acceso a la infraestructura de red.

Para realizar el análisis de vulnerabilidades a suplantación IP ciega, se determinó si los equipos en la Universidad cumplen las necesidades de la suplantación IP no ciega, que son el ofrecimiento de servicios remotos y relaciones de confianza; además para este caso es necesario la susceptibilidad del sistema a la predicción de los números de secuencia TCP. Para ello se estudió la implementación que hace el sistema operativo del protocolo TCP/IP en las máquinas más importantes dentro de la Universidad, por medio de el programa *nmap*. La opcion –O de *nmap* permite la identificación del sistema operativo que corre la máquina o máquinas escaneadas por medio de la obtención de respuestas a ciertos segmentos TCP enviados hacia la máquina analizada; estas respuestas forman un patrón el cual se compara con los patrones que *nmap* guarda de los sistemas operativos conocidos, de los que obtiene la respuesta. Una de las técnicas que tiene *nmap* para construir los patrones es la de encontrar patrones en la generación de los números de secuencia iniciales en los segmentos TCP cuando responden a las solicitudes de conexión. Estos pueden ser clasificados en varios grupos como:

- El tradicional 64K, donde los números de secuencia se incrementan en 64000 por cada nueva conexión y se implementó en los primeros sistemas UNIX.
- Incrementos aleatorios (nuevas versiones de *Solaris*, *IRIX, FreeBSD, Digital UNIX*, *Cray*, entre otras).
- Aleatoriedad verdadera (*Linux 2.0.*, OpenVMS, AIX* mas nuevos, etc).
- Sistemas Windows (y unas cuantos mas) usan un modelo "dependiente del tiempo" donde el ISN se incrementa por una pequeña cantidad estática cada periodo de tiempo. Esta técnica es tan vulnerable como el viejo comportamiento de 64K.
- Constante, las máquinas siempre usan exactamente el mismo ISN. Lo usan algunos hubs gestionables *3com* (usan 0x803) e impresoras *Apple LaserWriter* (usan 0xC7001).

Para realizar el estudio de los sistemas operativos se usó el siguiente comando:

#nmap –O 172.16.255.134 -vv

Con el cual se le dice a *nmap* que muestre el sistema operativo de la máquina con dirección IP 172.16.255.134, el cual corre sobre *Linux Debian 3.0r1*, y con la opción –v se le dice que muestre información adicional, como que tan difícil es la predicción de los números de secuencia iniciales de dicha máquina. Se obtiene un resultado como el siguiente:

```
Device type: general purpose
Running: Linux 2.1.X|2.2.X
```

```
OS details: Linux 2.1.19 - 2.2.25
TCP Sequence Prediction:
Class=random positive increments
IPID Sequence Generation: Incremental
Average 'difficulty' over 5 scans - 2344654.6
On this build, I got 'Good luck!' on every scan.
```

Observando la cuarta y la quinta línea se pude ver que *nmap* ha clasificado la predicción de secuencia TCP como incrementos positivos aleatorios; en la séptima línea muestra un número, entre 0 y 9999999, que refleja la dificultad promedio de predecir los números de secuencia iniciales; por último termina con un comentario para el analista sobre que tan vulnerable es este sistema a la predicción. El mismo análisis se realizó sobre los sistemas operativos usados en la red de la Universidad del Cauca según los registros de la Red de Datos, obteniendo los resultados de la tabla 2.1.

Tabla 2.1 Generación de números de Secuencia

Sistema Operativo	Clase de Generación de Secuencia TCP	Dificultad Promedio	Porcentaje en la Red
Slackware-current	Incrementos Positivos Aleatorios	2595171.4	<1%
Debian 3.0r1	Incrementos Positivos Aleatorios	2344654.6	3.6%
Red Hat 9/7	Incrementos Positivos Aleatorios	3591128.2	5.2%
Knoppix 3.3	Incrementos Positivos Aleatorios	3909828.4	<1%
OpenBSD 3.3	Aleatoriedad Verdadera	9999999	<1%
FreeBSD 5.1	Aleatoriedad Verdadera	9999999	<1%
Irix 6.2	Incrementos Constantes	0	0%
Windows 98	Chiste Trivial	0.8	42%
Windows 2000/XP	Incrementos Positivos Aleatorios	46457	48,00%
Cisco IOS	Aleatoriedad Verdadera	9999999	<1%

Un caso especial ocurrió al escanear los enrutadores que conectan la Intranet con las redes externas; cada enrutador (Cisco 3600, Proveedor Orbitel y Cisco 1700 Proveedor Telecom) no produjo patrones que pudieran ser identificados por *nmap* para identificar sus sistemas operativos aunque si identificar la dificultad promedio para predecir la secuencia TCP, la cual es muy alta; en ambos casos se produjo la siguiente salida:

```
Interesting ports on olimpo.unicauca.edu.co (208.195.214.254):
(The 1662 ports scanned but not shown below are in state: closed)

PORT STATE SERVICE
23/tcp open  telnet
No exact OS matches for host (If you know what OS is running on it, see
http://www.insecure.org/cgi-bin/nmap-submit.cgi).
TCP Sequence Prediction: Class=truly random
Difficulty=9999999 (Good luck!)
```

Como puede observarse los sistemas más inseguros son los que existen en mayor porcentaje en la red de la Universidad; sin embargo, no son los más importantes ya que estos se concentran en dos núcleos: los servidores de la Red de Datos y los servidores de la división de sistemas; en ambos grupos, la mayoría de servidores corren sobre sistemas operativos basados en Linux, los cuales

ofrecen gran seguridad, solo dos servidores de la Red de Datos corren sobre Windows 2000 Server que cumplen la función de servidores DNS internos. Aunque la mayoría de los sistemas operativos ofrecen un gran porcentaje de seguridad en cuanto a predicción de números de secuencia no son completamente seguros, a excepción de *FreeBSD* y *OpenBSD* según *nmap*. Para contrarrestar las vulnerabilidades contra la suplantación IP ciega deben implementarse mecanismos que permitan evitar estos ataques desde dentro de la red y en el perímetro de la red para evitar ataques externos, ya que este tipo de suplantación IP no restringe la ubicación del atacante. Uno de estos mecanismos es la implementación de Firewalls. Muchos Firewalls disponibles en el mercado vienen con características especiales para evitar ataque de suplantación IP ciega, por ejemplo, si el Firewall detecta que los números de secuencia generados por un equipo que se encuentra dentro de las zonas protegidas por él son números predecibles, este guarda dichos números y los remplaza por números aleatorios que el mismo genera cerrando cualquier posibilidad de que algún equipo en la red protegida sea blanco de un ataque. Además, se debe utilizar la característica de filtrado de paquetes intrínseca en cualquier tipo de Firewall restringiendo la entrada de paquetes que se dirijan hacia puertos vulnerables como los analizados anteriormente y que sean habilitados solo por solicitudes justificadas según la políticas decretadas por los administradores de la red. Al momento de realizar este estudio la Red de Datos ha adquirido un Firewall hardware Cisco PIX (Private Internet Exchange), el cual es uno de los más populares en el mundo y se ha implementado para proteger las direcciones IP que son enrutadas por el enlace de Orbitel. Este Firewall cumple la característica de aleatorización de números de secuencia pero dentro de las reglas de filtrado no se han creado reglas para el filtrar paquetes

Las vulnerabilidades a un ataque de secuestro de sesión TCP son muy grandes ya que este ataque se basa la capacidad del atacante a escuchar el tráfico TCP; esto es posible en muchos puntos de la Universidad ya que no existen políticas que impidan el uso de tarjetas de red en modo promiscuo ni tampoco mecanismos para detectar este modo de operación de las tarjetas de red. Los equipos de interconexión en los bordes de la red son en la mayoría hubs lo que permite la escucha de tráfico; usuario que tenga abierta una sesión (por ejemplo de *telnet*) puede ser víctima de un secuestro de sesión por un usuario conectado al mismo segmento de red o lo que es lo mismo, conectado al mismo hub. Una posible solución, es la eliminación de hubs como dispositivos de conexión de borde y remplazarlos por switchs, además la implementación de mecanismos que permitan solo a usuarios autenticados usar los recursos de la infraestructura de red como puntos de acceso, para que usuarios no autorizados no introduzcan o escuchen tráfico de la red. La causa principal por la que se puede llevar a cabo este ataque es por las debilidades del protocolo IP para autenticar el origen de los datos. Cualquier tipo de ataque de suplantación IP podría prevenirse si el protocolo IP fuera confiable en cuanto a que quien envía los datos es quien dice ser en realidad; para ello lo mejor es implementar protocolos de seguridad como IPSec, el cual también tiene la propiedad de cifrar la carga útil de IP impidiendo la obtención de los números de secuencia TCP, recurso vital para llevar a cabo el ataque.

La implementación de un IDS (Sistema Detector de Intrusos) es opción para detectar ataques de suplantación IP, ya que los desarrolladores de este tipo de sistemas han encontrado múltiples patrones para detectar estos ataques lo que le da cierta inteligencia al sistema para informar sobre un posible ataque. La colocación de un IDS debe hacerse en sitios estratégicos, ya que si el IDS no tiene acceso al tráfico donde se lleva a cabo el ataque, no podrá detectarlo.

2.1.1.6 Herramientas para llevar a cabo IP Spoofing

En la red Internet se encuentran múltiples herramientas para llevar a cabo variados ataques en base a la suplantación IP. *Hping*[6] es una herramienta para la transmisión de paquetes ICMP, UDP y TCP en los cuales se pueden editar parámetros como tamaño de paquetes, tipo de servicio (TOS), bits de fragmentación y por supuesto direcciones IP. Es usado para analizar reglas de firewalls, escaneo de puertos, evaluación de rendimiento de la red usando paquetes de gran tamaño, entre otras utilidades.

Para realizar una prueba simple de suplantación IP se instaló la herramienta *hping* en su versión 2 sobre la distribución Debian 3.1 con el comando *apt-get install hping2.* Una vez instalado, con el siguiente comando se puede enviar una solicitud de eco ICMP con la opción *–icmp,* con la opcion *–spoof* se le dice a *hping* que envíe los datagramas IP suplantando la dirección IP que se quiera, por ejemplo 172.16.99.99. Por último se coloca dirección IP de destino de la prueba, por ejemplo 172.16.41.108:

#hping2 –-icmp –-spoof 172.16.99.99 172.16.41.108

La respuesta a las solicitudes de eco se enrutará hacia el destino suplantado que en este caso es *172.16.99.99*. Esta sencilla prueba demuestra lo fácil que es hacerse pasar por un equipo a nivel IP.

2.1.2 Suplantación ARP

La red universitaria es una red que cumple con el estándar Ethernet a nivel de enlace de datos; por tal motivo es necesario estudiar que tipo de vulnerabilidades existen en dicho nivel para tener y plantear soluciones para ser tenidas en cuenta en la elaboración de las arquitecturas a proponer.

Cada uno de los equipos dentro de una red posee por lo menos una dirección IP la cual hace parte de una organización jerárquica de direcciones. Dicha organización hace que cada dirección en la red pueda acceder a otra por medio de la selección de una o más rutas, sin embargo, en el nivel inferior al nivel IP se maneja un direccionamiento que no es jerárquico como es el de las direcciones físicas también conocidas como direcciones hardware. Cada interfaz o tarjeta de red en el mundo posee una dirección que es única, pero como los protocolos de alto nivel ubican las máquinas con direcciones IP, debe existir un medio para relacionar las direcciones físicas con las IP. Esta es la razón de existir del protocolo ARP (Protocolo de Resolución de Direcciones), al cual se le da una dirección IP y retorna la dirección física de la interfaz de red que tiene dicha IP; como se explicará más adelante este mapeo de direcciones puede alterarse permitiendo suplantaciones en las comunicaciones.

[6] Herramienta Hping, disponible en http://www.hping.org/

La mayoría de sistemas operativos usan una tabla ARP (caché ARP) para mantener las últimas direcciones usadas por el equipo, la cual es actualizada cada ciertos intervalos de tiempo dependiendo del sistema operativo. Cuando la dirección requerida no se encuentra en la tabla, se envía un mensaje broadcast en la red con formato ARP request (solicitud ARP) que básicamente pregunta a todas las máquinas en el segmento si su IP corresponde a la especificada en la petición. La máquina que concuerda debe responder con un ARP reply (respuesta ARP) al computador que hizo la solicitud. Dicha respuesta incluirá la dirección física del hardware; esta dirección es almacenada en la caché del host solicitante. De allí en adelante todos los paquetes enviados a la IP se asocian con la dirección física que aparece en el caché.

Debido a las falencias descritas en secciones anteriores del protocolo ARP, si se altera un paquete usado en la comunicación entre dos máquinas se podría suplantar la dirección MAC de una de ellas ya que el protocolo recibe paquetes incluso si la máquina no los necesita, con lo que se refresca la tabla con los nuevos datos recibidos, y estos datos pueden ser erróneos o alterados a propósito para realizar ataques ya sea que causen pérdida de confidencialidad, pérdida de integridad de los datos o ataques de denegación de servicio.

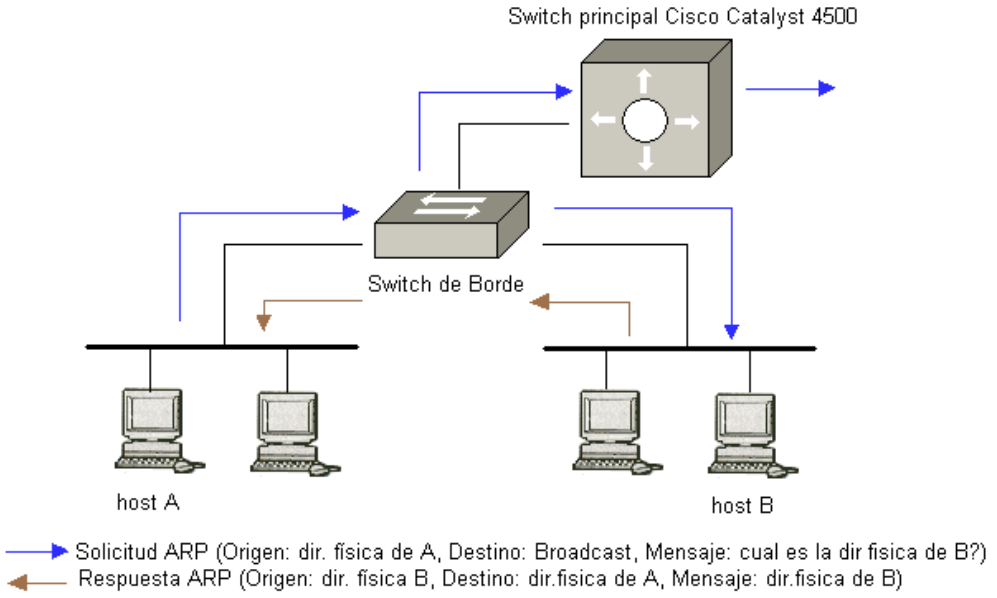


Figura 2.5 Funcionamiento del protocolo ARP.

En la figura 2.5 se observa como funciona el Protocolo ARP ilustrando a pequeña escala dos segmentos de red de los muchos que se tienen en la Universidad; cada segmento lo componen los equipos conectados a un bus el cual puede ser implementado físicamente por un HUB; la información que transita por el bus es difundida a todos los equipos del segmento de red. Cuando el equipo A quiere comunicarse con el equipo B, tiene que saber la dirección física de la interfaz de red de B y si no la tiene almacenada la solicita por medio de un mensaje de broadcast ARP; este mensaje se difunde por todo el dominio de broadcast Ethernet que en el caso de la red universitaria es toda la red, debido a la falta de subdivisión en redes. Esto significa que cualquier mensaje de broadcast ARP generado en alguna parte de la red llegará a cualquier segmento de red.; esto es un factor preocupante en la red debido a la disminución del

rendimiento por la gran cantidad de tráfico ARP. Dado que en el mensaje que envía A se especifica sus direcciones físicas e IP, B puede responder con un mensaje ARP de respuesta dirigido a la dirección física de A. Los switchs por donde pasan los paquetes Ethernet son enrutados a nivel Ethernet ya que cada switch conoce las direcciones físicas de los equipos que tiene conectados y por medio de que puerto puede encontrarlo; gracias a esto, el mensaje de respuesta de B llega al primer switch que encuentra, pero éste sólo leerá el encabezado 802.3 o el Ethernet, como ocurre en un switch de nivel 2. Así la dirección MAC de destino se comparará con la tabla local de ARP encontrando la dirección buscada y el puerto por el que deberá ser reenviado, haciendo llegar la respuesta al equipo A. Esta dirección física será mantenida en memoria por un cierto periodo de tiempo mapeada a la dirección IP del equipo B.

Un ataque de suplantación ARP ocurre cuando un equipo le hace creer a otro que una dirección IP corresponde a una dirección física que no es la verdadera, esto se puede usar para que los paquetes que se envían a determinada IP sean dirigidos hacia el equipo del atacante para obtener determinada información. Este ataque se realiza con el envío de respuestas ARP sincrónicas (si se ha hecho una solicitud ARP previamente) o asincrónicas (si no se ha hecho una solicitud ARP previamente). La mayoría de sistemas operativos actualizan sus tablas ARP cuando llega una respuesta ARP aun si no se ha hecho la solicitud correspondiente a dicha respuesta; además, el hecho de que en el protocolo ethernet no haya mecanismos para autenticar el origen de los paquetes ARP, puede ser aprovechado por un atacante para manipular tablas ARP de otros equipos muy fácilmente, como se muestra en la figura 2.6.

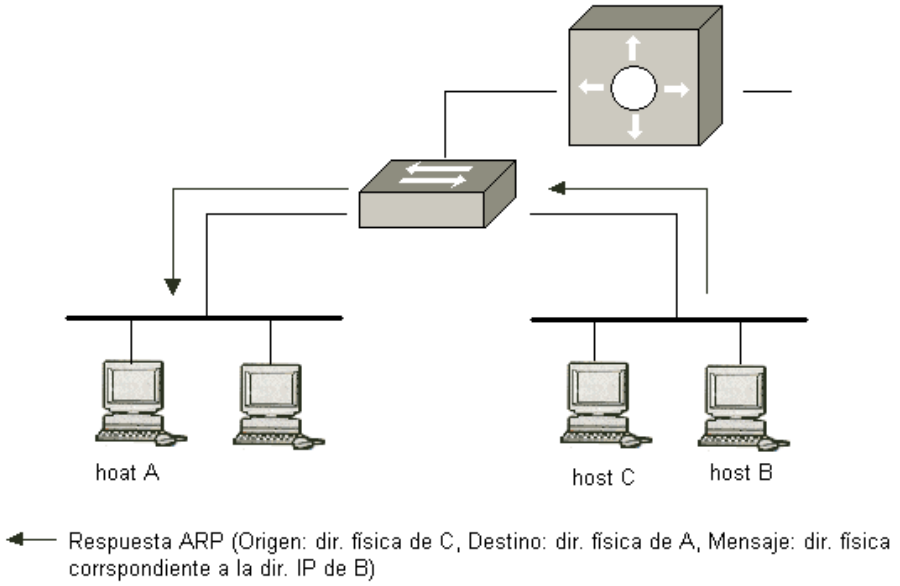


Figura 2.6 Funcionamiento de la suplantación ARP

El atacante solo envía una respuesta ARP que contenga como dirección física de origen, la de C (atacante), la dirección IP de origen, la de B (máquina suplantada), la dirección física de destino, la de A (víctima) y la dirección IP de destino también de A. Esto hará creer a la máquina A que el paquete proviene de B y este proceso hará que cualquier comunicación que el equipo A intente establecer con B sea dirigida hacia B, ya que aunque va dirigida a la dirección IP correcta de B, pero en el nivel inferior (Ethernet) va dirigido hacia la dirección física de C. Para un atacante es relativamente fácil conocer la dirección IP de su víctima: para obtener la dirección física solo

tiene que tratar de establecer una conexión o una solicitud de eco (ping) a la víctima y luego entrar el comando *arp -a* en una consola, este comando devuelve las direcciones físicas de las máquinas almacenadas en la caché relacionadas con su respectiva dirección IP

Para comprobar esta vulnerabilidad se utilizó el programa *arpoison*[7] el cual envía solicitudes o respuestas ARP totalmente personalizados por el usuario; necesita las funciones que provee la librería *libnet*[8]; una vez instalados ambos paquetes se procede a utilizar el comando *arpoison* el cual tiene las siguientes opciones:

-i: interfaz de red por la que se enviaran las respuestas ARP.

-d: dirección IP de destino (víctima).

-s: dirección IP de origen (suplantada).

-t: dirección física de destino (víctima).

-r: dirección física de origen (atacante).

-a: envía solicitudes ARP, sin esta opción se envían respuestas ARP.

-w: tiempo entre el envió de un paquete y el siguiente en segundos

-n: número de paquetes a enviar.

Se tiene la siguiente configuración:

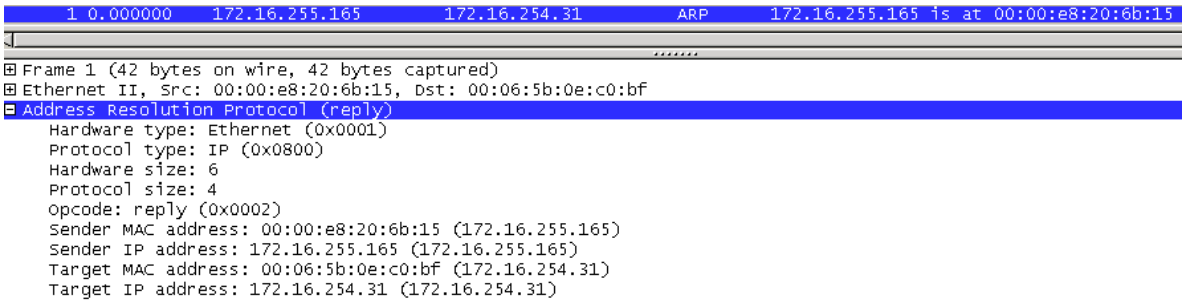
```
host A (víctima), sistema operativo Linux Debian 3.1
dirección IP: 172.16.254.31
dirección física: 00:06:5B:0E:C0:BF

host B (suplantado), sistema operativo Windows XP
dirección IP: 172.16.255.165
dirección física: 00:06:5B:76:05:A8

host C (atacante), sistema operativo Linux Debian 3.1
dirección IP: 172.16.255.134
dirección física: 00:00:E8:20:6B:15
```

Se configuró arpoison para suplantar la dirección física de B ante el equipo A generando respuestas ARP no solicitadas desde C con el siguiente comando:

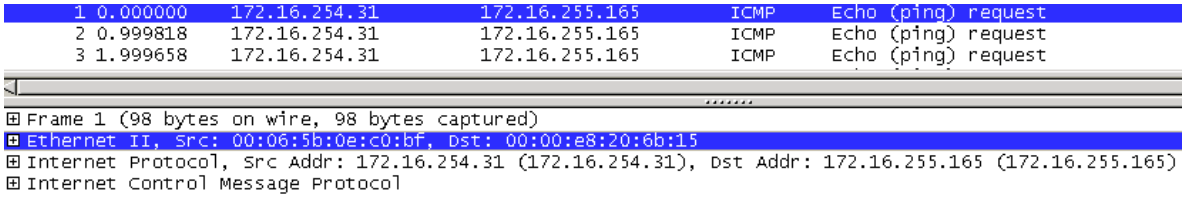
#arpoison -i eth0 -d 172.16.254.31 -s 172.16.255.165 -t 00:06:5B:0E:C0:BF -r 00:00:E8:20:6B:15 -w 1

Este comando produce el siguiente paquete analizado con Ethereal al cual se le ha configurado el siguiente filtro: *arp && host 172.16.254.31,* el cual captura todo el tráfico ARP que se dirija hacia o desde la dirección 172.16.254.31:

[7] Programa Arpoison, disponible en http://arpoison.sourceforge.net
[8] Librerías Libnet, disponible en http://www.packetfactory.net/libnet/



Cuando el host A recibe dicho paquete modifica su tabla ARP; esto puede comprobarse verificando la tabla ARP del host A *arp -a* o también realizando un ping desde el host A hacia el host B y capturando el tráfico ICMP, como se muestra la siguiente captura de tráfico:



Se puede observar que los mensajes ICMP se dirigen hacia la dirección IP correcta pero hacia una dirección física suplantada, la del equipo C, debido a que los switchs involucrados en esta comunicación conocen donde está ubicada la dirección física de destino del paquete que es enviado hacia el host C. El ataque es efectivo aún si el host C se encuentra en un segmento de red diferente de A y B, ya que los switchs saben por qué puertos físicos pueden alcanzar la dirección física de C de acuerdo a sus tablas ARP.

Este sencillo ataque, además de considerarse de suplantación puede considerarse como un ataque de denegación de servicio ya que puede dejar incomunicados dos equipos o también un equipo con el resto de la red si el objetivo del ataque es difundido por un mensaje de broadcast. En la captura anterior se puede observar como las solicitudes de eco (ping) no son respondidas ya que cualquier tipo de comunicación entre los host A y B ha sido interrumpida.

Las evoluciones de este ataque pueden llevar a ocasionar pérdida de confidencialidad y de integridad en las comunicaciones de datos, como por ejemplo el ataque del hombre en el medio (Man in the Middle). Estos problemas serán analizados en secciones posteriores.

2.1.2.1 Posibles Vulnerabilidades de Suplantación ARP en la Red de Datos de la Universidad del Cauca

Debido a que este ataque se lleva a nivel de enlace de datos, no es necesario considerar posibles ataques externos ya que este ataque no puede traspasar redes, por lo tanto no se considerarán mecanismos de defensa en el perímetro de la red, solo mecanismos de protección interna.

Para saber que puntos de la red universitaria podrían sufrir este ataque, se estudiaron los sistemas operativos más utilizados en los puntos de mayor importancia para la red de la Universidad. Para tal efecto se utilizó *arpoison* tal y como se uso para la demostración de la vulnerabilidad y examinando en el lugar de la víctima los sistemas operativos a vulnerar.

El procedimiento fue el mismo: enviar una respuesta ARP falsa hacia el host A y verificar si después de recibirla, el host A cambiaba su tabla ARP con los datos falsos. Si no lo hace se considera que el equipo no es vulnerable a suplantación ARP.

Tabla 2.2 Sistemas Operativos vulnerables a suplantación ARP

Sistema Operativo	Vulnerable a Suplantación ARP
Windows 98	Si
Windows NT	SI
Windows 2000	Si
Windows XP	SI
Linux Red Hat 7/9	Si
Linux Debian 3.1/3.0	Si
Linux Fedora Core 2/3	Si
Sun Solaris	No

Solo existe un servidor que corre sobre Sun Solaris en la Red de Datos de la Universidad y es el servidor *ceres*; en este equipo se encuentra el programa MRTG que toma información sobre el tráfico de los enlaces de Telecom, Orbitel, el ancho de banda consumido por los usuarios que acceden vía telefónica a través del RAS, e información sobre el tráfico en los proxies *Hiperion* y *Temis*. Mediante Ceres también se presta alojamiento de sitios con la plataforma de Java (JSP, Servlets) y bases de datos en *mysql*.

En la actualidad se esta llevando un proceso de subdivisión de redes en la red universitaria, implementándose en el nuevo switch de núcleo nivel 3 Cisco Catalyst 4500, que remplaza al switch Nortel Accelar 1200; esto reduce el alcance de un posible ataque de suplantación ARP. Las nuevas subredes están definidas por los siguientes prefijos:

- 10.200.1.0/24: Subred de la red privada Clase A 10.0.0.0. Está separada en una VLAN destinada para los servidores de la Red de Datos y esta separada físicamente de las demás redes ya que esta VLAN está conformada por un rango de puertos del switch principal a los que están conectados todos los servidores que se encuentran en la sala de servidores del edificio del IPET. Para que un ataque de suplantación ARP sea efectivo contra esta red, el atacante tendría que tener acceso físico a uno los puertos del switch principal que conforman la VLAN de los servidores para así poder estar dentro de la misma red de la víctima.

- 10.200.2.0/24: Subred de la red privada Clase A 10.0.0.0. Es una subred destinada para las direcciones que necesitan acceso directo a Internet (direcciones públicas); está separada lógicamente de las demás redes ya que estas direcciones se encuentran distribuidas por todo el campus universitario y no se encuentran agrupadas físicamente como en el caso anterior. Para un atacante es muy fácil poder llevar a cabo un ataque: primero tiene que pasarse a la misma red de la víctima y para ello solo

necesita saber una dirección que se encuentre en uso, la máscara de subred y la puerta de enlace de la red de la víctima para configurar su equipo y llevar a cabo el ataque.

- 172.16.0.0/16: Red privada clase B, es una subred destinada a todas las direcciones privadas de la Intranet universitaria; este rango de direcciones es el que ha sufrido menos cambios en el proceso ya que la mayoría de equipos en la red pertenecía a esta red. También se encuentra distribuida físicamente lo que hace que no se pueda evitar que un equipo de esta red pase a otra para realizar un ataque.

- 200.21.83.64/26 y 200.21.83.128/26: subredes asignadas por el proveedor Telecom, se encuentran distribuidas por toda la red.

Por lo anterior, sería muy difícil llevar a cabo un ataque de suplantación ARP sobre los servidores de la Red de Datos ya que se necesita acceso físico a estos. Sin embargo, los servidores de la división de sistemas comparten la red desde el punto de vista físico con los demás equipos de la Universidad lo que los pone en un serio riesgo a ser atacados. Estos servidores manejan información de gran importancia para los procesos académicos y administrativos de la Universidad del Cauca, por lo tanto se constituyen en un recurso de gran relevancia a ser tenido en cuenta a la hora de plantear soluciones a los problemas de seguridad en la red.

La causa de la suplantación ARP es la incapacidad del protocolo Ethernet de autenticar el origen de los datos. Este es un problema que no encuentra una solución definitiva aun; solo se puede tratar de disminuir su alcance o implementar mecanismos que permitan detectar cuando quiere ser utilizado.

Para prevenir totalmente esta vulnerabilidad se podrían implementar tablas ARP estáticas usando comandos CLI, "ipconfig /all" en Windows o "ifconfig" en sistemas Unix (Linux), obteniendo de esta forma las direcciones físicas de todos los dispositivos conectados a la red. Si se usa el comando "arp -s" se pueden adicionar entradas estáticas para todos los dispositivos conocidos. Usando estas entradas estáticas se evita que los atacantes alteren las tablas a su gusto pudiendo aprovechar todas las debilidades ya explicadas. Incluso se puede crear un script que llene estas entradas estáticas en los computadores cada vez que estos sean reiniciados. Sin embargo, esto solo es recomendado para redes pequeñas por el número de entradas que habría que ingresar en cada equipo. La red de la Universidad del Cauca puede considerarse de tamaño mediano por lo tanto no se recomienda esta solución ya que cuando un nuevo equipo se conecte a la red o cambie su configuración de red, se tiene que actualizar las tablas ARP en los demás equipos de la red y esto lo convierte en una labor casi imposible de realizar.

También se puede prevenir con la configuración de "Port Security" de los switchs; una de estas características permite forzar al switch a que permita sólo una dirección MAC para cada puerto físico en el switch, lo cual impide que alguien cambie la dirección física de su máquina o trate de enviar paquetes ARP con una dirección diferente a la que esta configurada en el switch. Sin embargo, en la red universitaria no se puede implementar este modelo ya que la mayoría de equipos no se conectan a la red por medio de switchs directamente sino que usan concentradores (hubs). La mejor solución usando Port Security es que no se permita solo una dirección física conectada a los puertos físicos sino un rango; este rango debe corresponder a las máquinas que están bajo el puerto

determinado. Esta solución es muy acertada y conveniente debido a la estructura de la red universitaria, sin embargo deja abierta la posibilidad a que existan víctimas de suplantación ARP si estas se encuentran bajo el mismo puerto del switch en el que se encuentra el atacante.

Para disminuir el alcance de las vulnerabilidades de suplantación ARP se debe subdividir la red en subredes separadas físicamente hasta donde sea posible, como se ha mencionado antes; al ser este ataque de nivel de enlace de datos no puede traspasar subredes si estas están separadas físicamente. De todos modos queda la posibilidad de que ocurran ataques dentro de cada subred, por eso la importancia de la subdivisión, para disminuir el impacto.

Para detectar y monitorear un posible ataque de suplantación ARP la herramienta más popular es *arpwatch;* este programa monitorea el tráfico en la red en busca de paquetes ARP con los cuales llena una tabla en la cual se relaciona la dirección IP de un equipo con su dirección física; si encuentra un par que no se encuentra en su tabla simplemente lo agrega a la tabla, si encuentra un par que esta en su tabla pero alguno de los dos parámetros (dir. IP o dir. Física) no corresponde con la pareja que tenía almacenada, deja un mensaje en un archivo local o lo envía por correo electrónico según como este configurado. Debido a que en la red no hay un mecanismo de asignación dinámica de direcciones IP (como DHCP) esta solución es muy buena para detectar suplantaciones ARP. Este tipo de solución debe ubicarse en cada subred para que sea efectiva ya que debe poder capturar el tráfico ARP que se difunde por broadcast, o sea que debe estar dentro del dominio de broadcast Ethernet de cada subred.

2.2 PÉRDIDA DE CONFIDENCIALIDAD

Cuando se transmiten datos por una red, la mayoría de usuarios consideran que los datos intercambiados son recibidos solo por el o los destinatarios autorizados para tal fin. Sin embargo en las redes y en especial las redes IP que están soportadas sobre el protocolo Ethernet existen mecanismos que hacen que esta premisa no se cumpla. Algunas veces esto se realiza con propósitos benéficos como por ejemplo en detectores de intrusos, analizadores de protocolos, analizadores de ancho de banda, etc. Pero también pueden usarse para acceder a información con propósitos maliciosos.

Una red del tipo Ethernet, es una red de transmisión de paquetes basada en bus común. Al bus común se conectan todos los equipos informáticos de la red. El bus puede ser un simple cable coaxial (10Base10, 10Base100), o puede estar formado por elementos pasivos como concentradores (hubs), que facilitan el cableado estructurado de la red por pares trenzados.

Bajo esta arquitectura de red, cuando un equipo desea transmitir un paquete, comprueba que el bus esta libre y lo envía. Si dos equipos envían simultáneamente un paquete a la red, se produce una colisión. La colisión es detectada por ambos y esperaran un tiempo aleatorio antes de intentar enviar de nuevo la información al bus.

Todos los equipos compatibles Ethernet poseen una dirección MAC también llamada dirección física o dirección hardware única en el mundo, de 48 bits de longitud. Cada fabricante de equipos Ethernet tiene asignado un segmento de direcciones, y es responsabilidad de este asignar una dirección distinta a cada equipo. Las direcciones MAC están almacenadas en una pequeña memoria que poseen las tarjetas de red. Las direcciones MAC se representan en hexadecimal con el siguiente formato: XX:XX:XX:XX:XX:XX

La información es enviada al bus agrupada en forma de tramas o paquetes. Estos paquetes contienen la dirección MAC de destino, la de origen, el tipo de datos, los datos a transmitir y un checksum de comprobación. En condiciones normales, una tarjeta Ethernet solo es capaz de escuchar los paquetes destinados a su dirección MAC o los destinados a todo el mundo (BROADCAST). La dirección MAC de BROADCAST es FF:FF:FF:FF:FF:FF

2.2.1 Olfatear (Sniffing)

Desde hace unos años, es habitual que en todos los sistemas operativos *Unix* se incluya una herramienta de captura y visualización de tráfico. GNU/Linux incluye "*tcpdump*" en todas sus distribuciones. El programa *tcpdump* solo puede ser ejecutado por root, y se trata básicamente, de una herramienta de diagnostico para redes TCP/IP. Puede usarse para analizar nuestro propio tráfico, o el de toda nuestra Ethernet. Para poder escuchar todo el tráfico que circula por un segmento de red, es necesario colocar la tarjeta Ethernet en modo "promiscuo", que significa que recogerá todos los paquetes de la red, aunque el destinatario no sea su propia dirección MAC. Tcpdump fue programado en base a la librería *libnet* la cual es la más popular para programación en redes en cuanto a captura de tráfico se refiere; en base a ella también se han creado programas como *Ethereal*, *Snort* el estándar de facto en detectores de intrusos[9], u *Olfiet*[10] que puede interceptar cualquier tipo de tráfico TCP o UDP y hacer seguimiento de conversaciones de MSN Messenger y de acceso a páginas Web.

El sniffing es la base para muchos otros ataques de muchos tipos, como ataques de suplantación, de denegación de servicio y de acceso no autorizado a información. Sin embargo, por sí solo su alcance es muy pobre ya que se limita al segmento de red que comparte el atacante y sus víctimas. En el caso de la red universitaria, al ser una red ethernet cuyos dispositivos de interconexión de borde son switchs y concentradores (hubs), un intruso solo podría capturar el tráfico que se dirija hacia o desde los dispositivos que están conectados al mismo puerto de un switch, como se mostró en la figura 2.6. Para superar estos límites los atacantes han ideado nuevas técnicas para hacer que los datos lleguen hasta sus tarjetas de red y poder capturarlos.

2.2.2 Hombre en el Medio (Man in the Middle)

[9] SNORT: Disponible en www.snort.org
[10] Sniffer creado en la FIET por Julian Andrés Parra y Andrés Felipe Arboleda. Disponible en www.unicauca.edu.co/~aarboleda

El Hombre en el medio más que una técnica es un concepto el cual puede ser implementado de muchas maneras. Como su nombre lo indica lo que intenta es situar al atacante en medio de una comunicación sin que los dos extremos de la misma se den cuenta de lo ocurrido, ya sea lógicamente o físicamente. Esto hace que además de haber una pérdida de confidencialidad de los datos, también pueda ocurrir una pérdida de integridad de los mismos ya que toda la información intercambiada pasa a través del atacante dándole la habilidad para adicionar, eliminar o cambiar la información a su antojo.

Para llevar a cabo un hombre en el medio físicamente, el atacante debe tener acceso a los puntos de red o gabinetes donde se encuentran los concentradores y switchs para hacer que la información de un extremo se direccione hacia el atacante por medio de conexiones físicas y luego este pueda reenviar dicha información al verdadero destinatario. Este procedimiento puede ser controlado fácilmente en una institución con políticas fuertes en cuanto acceso a los puntos y dispositivos de interconexión a la red; sin embargo las redes pueden no estar concentradas en un mismo lugar y tener sedes remotas, que son interconectadas por organismos externos al control y las políticas de la institución. En el caso de la red universitaria, se tienen dos sedes remotas, una en el municipio de Santander de Quilichao y otra en el sector las Guacas en Popayán; ambas sedes manejan información administrativa y académica muy importante. Para la interconexión se utilizan los servicios de redes externas a la Universidad como son las de los operadores locales Telecom y Orbitel. Este proceso hace que estos operadores se consideren posibles agresores a la seguridad de la Red de Datos, y aunque esto es muy poco probable, en seguridades mejor no estar totalmente confiado.

Para lograr poner un hombre en el medio de manera lógica se manejan técnicas un poco más complejas y dichas técnicas son múltiples; en este estudio se analizaran solo dos para tener claro el concepto del ataque y poder plantear una solución acertada.

2.2.2.1 Hombre en el Medio por Suplantación ARP

Esta técnica se basa en la vulnerabilidad de los extremos de una comunicación al ser engañados por una suplantación ARP; se desarrolló para poder olfatear información que se transmite por fuera del segmento de red del atacante. La figura 2.7 ilustra el procedimiento.

1. Entre el host A y el host B existe un intercambio de información el cual se basa en la dirección IP de los dos extremos. Para que A mande un paquete a B debe saber su dirección IP, luego debe averiguar su dirección MAC lo cual realiza consultando su tabla ARP y si no la encuentra envía un mensaje de broadcast solicitándola. Cuando el paquete Ethernet sale de A los equipos de interconexión hacen que el paquete llegue hasta el segmento de red donde se encuentra B. Lo mismo ocurre en sentido contrario.

2. Cuando el atacante interviene en la comunicación envía una respuesta ARP falsa a ambos equipos diciéndoles que la dirección IP del otro extremo la puede alcanzar por medio de la dirección física del atacante (host C). Debido a esto el host A envía la información a la dirección IP de B pero al formar la trama Ethernet lo envía a C; los equipos de interconexión direccionan el paquete hacia el segmento de red de C, luego el atacante captura el paquete lo reenvía cambiando solo la

dirección física de destino por la dirección MAC de B. Si realiza este procedimiento en sentido de B hacia A, el atacante estará lógicamente en medio de la comunicación y tendrá acceso a la información intercambiada; si los usuarios en los extremos no tienen conocimiento de redes, es muy posible que no se percaten de la ocurrencia del ataque, ya que de todas maneras, se siente un incremento considerable en el tiempo de intercambio de la información.

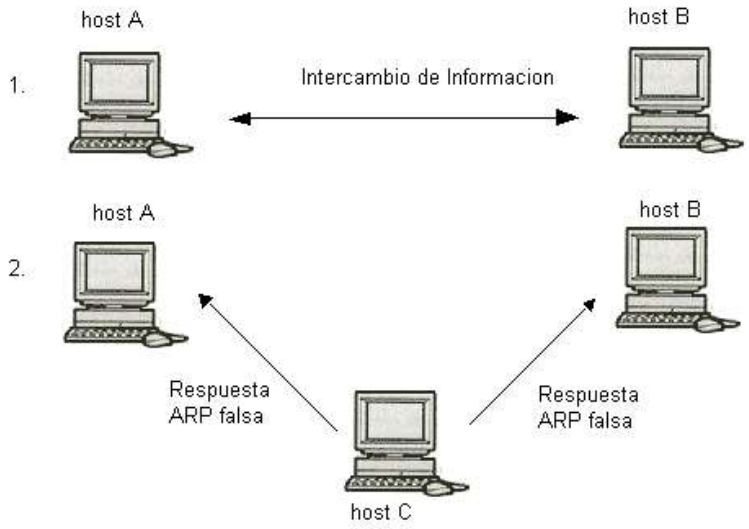


Figura 2.7 Ataque de hombre en el medio

Este ataque se realiza cuando la información que se quiere acceder son datos que se transmiten por fuera del segmento de red del atacante. Incluso podría traspasar una subred si uno de los dos extremos se encuentra en la misma subred del atacante. En este caso se tiene que enviar la respuesta ARP falsa al extremo que comparte la subred y a la gateway que une la subred del atacante y la subred del otro extremo. En el caso de que los dos extremos de la comunicación no se encuentren en la misma subred, es imposible olfatear la comunicación con este método.

2.2.2.2 Hombre en el Medio por Redirección ICMP

Este ataque se basa en los mensajes de redireccionamiento que envían las gateways y los routers cuando detectan que un equipo esta utilizando una ruta que no es la óptima para alcanzar otra red; el router envía un mensaje ICMP que cambia la gateway para esa ruta. Esto se puede aprovechar si un atacante envía un mensaje ICMP de este tipo suplantando la IP de la gateway que usa la víctima, diciéndole que use como gateway la dirección IP del atacante para tener una mejor ruta hacia la red destino (por ejemplo Internet); si la víctima acepta el paquete, todas las conexiones pasaran a través del atacante en sentido host – gateway, pero el atacante no podrá alterar la gateway ya que estos dispositivos no aceptan redireccionamiento así que el ataque será efectivo solo en un sentido de la comunicación.

2.2.3 Clonación de MAC (MAC Cloning)

Las direcciones MAC se pensaron para ser un identificador único globalmente para cada interfaz de red, sin embargo esta premisa no ha sido tenida en cuenta por algunos fabricantes de switchs los cuales permiten que en sus tablas ARP se asigne una misma dirección MAC a más de un puerto. Esto puede ser aprovechado por un intruso para envenenar la caché ARP del switch diciéndole que la dirección física de la víctima también se encuentra en el puerto del switch donde se encuentra el atacante. Esto hará que cada paquete que se dirija hacia la víctima también sea enviado al segmento del atacante y los dejará listos para la captura. Los usuarios de Linux pueden cambiar la dirección física para realizar el mismo ataque utilizando el comando *ifconfig*.

2.2.4 Inundación ARP (ARP Flooding)

Este ataque esta dirigido hacia los switchs de la red; cuando se sobrecargan debido al desborde de su tabla ARP, algunos switchs dejan de llenar la tabla ignorando los paquetes ARP que transitan a través de el y otros entran en modo hub, haciendo que los datos que entran por un puerto se difundan hacia los demás sin que se verifique en que puerto se encuentra la dirección de destino. El desborde de la tabla ARP del switch puede ser aprovechada por un atacante para saltar las barreras que impone el uso de switchs en las conexiones de borde al olfateo de la red de manera sencilla.

2.2.5 Posibles Vulnerabilidades de Pérdida de Confidencialidad

Como se mencionó anteriormente el olfateo de la red es una práctica que puede ser autorizada o no autorizada. La diferencia entre cada caso debe estar bien definida en las políticas de seguridad a nivel de red conocidas por todos los usuarios de la red universitaria. Teniendo en cuenta que la Universidad del Cauca es una institución educativa, estas políticas deben estar orientadas a no restringir las actividades académicas e investigativas que se desarrollen y también las actividades de monitoreo y control de los administradores de sistemas informáticos de las dependencias de la Universidad del Cauca.

La base del olfateo de la red es el uso de tarjetas de red en modo promiscuo; este procedimiento es casi imposible de evitar pero si se puede detectar; para controlar el uso de este recurso desde equipos autorizados y no autorizados se puede usar la herramienta *Neped*. La técnica empleada por *neped* para la detección de tarjetas en modo promiscuo es sumamente sencilla. Se trata de realizar una simple petición ARP para cada una de las IPs de la red, con la salvedad de que los paquetes no van destinados a broadcast (FF:FF:FF:FF:FF:FF), sino a una dirección arbitraria (cualquiera que no exista). Solo las máquinas con la tarjeta Ethernet en modo promiscuo son capaces de ver estos paquetes, y por lo tanto, solo ellas contestarán a las peticiones. Una vez instalado, neped se ejecuta de la siguiente manera:

```
# neped eth0
  ------------------------------------------------------------
  > My HW Addr: 00:06:5B:0E:C0:BF
  > My IP Addr: 172.16.254.31
  > My NETMASK: 255.255.0.0
  > My BROADCAST: 172.16.255.255
  ------------------------------------------------------------
  > Scanning ....
```

```
*> Host 172.16.255.134, 00:00:E8:20:6B:15* Promiscuous mode detected
> End.
```

Esta herramienta es imprescindible en las redes ya que con ella se puede detectar cualquier tipo de ataque que amenace la confidencialidad de los datos de una o más comunicaciones ya que todos estos ataques se basan en el uso de la tarjeta de red en modo promiscuo.

Se estudiaron dos casos de hombre en el medio llevado a cabo físicamente. El primero cuando se modificaban la conexiones físicas; en este caso los administradores de infraestructura no dan acceso a las llaves de los gabinetes de red a personal ajeno a la Red de Datos, ni siquiera a las personas que administran las salas donde se encuentran los gabinetes (esto demuestra claras políticas en ese sentido). Sin embargo, no existen políticas claras en cuanto al uso de los puntos de conexión a la red, ya que no hay reglas para saber que usuarios pueden hacer modificaciones en los puntos de conexión en la red. Las políticas que se planteen en este sentido también deben tener en cuenta las prácticas que se realizan en algunos laboratorios de Telecomunicaciones de la FIET donde se requieren cambiar la infraestructura de la red en el perímetro de la misma. El segundo caso, cuando el hombre en el medio físico es un organismo externo donde no son aplicables las políticas de seguridad de nuestra institución y por lo tanto no se puede aplicar ningún tipo de control ni monitoreo. Para contrarrestar este potencial problema con las sedes remotas de las redes se han creado las VPN (Redes Privadas Virtuales); este concepto de red busca comunicar dos redes que se conectan por medio de una tercera red que es insegura. En el caso de la Universidad de Cauca existen sedes de la red que se encuentra en Santander de Quilichao y el sector de Las Guacas en Popayán, las cuales están interconectadas a través de los operadores locales Telecom y Orbitel. Como se verá más adelante, existen varias técnicas para la implementación de redes privadas virtuales; la opción que ofrece mayor seguridad es la implementación de VPN por medio de IPSec ya que aprovecha todas las características de este protocolo como autenticación, cifrado, protección de la integridad entre otras, que lo hacen diferente de otros medios para implementar VPNs.

Para comprobar la vulnerabilidad de la red a un ataque de hombre en el medio, el primer paso ya se describió en una sección anterior comprobando que la totalidad de los equipos de la red universitaria son vulnerables a una suplantación ARP; ahora se debe comprobar si se puede llevar a cabo el resto del ataque. Teniendo en cuenta las subredes que existen en la Red de Datos se pueden comprobar si se es susceptible a un ataque cuando ambos extremos se encuentran en la misma subred del atacante para lo cual se necesita que ambos extremos sean vulnerables a suplantación ARP ó que solo uno de los extremos se encuentre en la subred del agresor para lo cual se necesita que el extremo que comparte la subred y la gateway (Switch nivel 3 Cisco Catalyst 4500) que conecta las redes sean vulnerables a la suplantación. Si se comprueba la vulnerabilidad para el segundo caso, automáticamente se comprobará la vulnerabilidad para el primer caso. Lo primero fue comprobar si la gateway que interconecta las subredes es vulnerable a la suplantación ARP. Para tal fin se realizaron los siguientes pasos:

1. Se hizo ping a la dirección IP de la gateway; esta dirección es fácil saberla, solo hay que ver la gateway de la ruta por defecto configurada en el equipo que se realiza la prueba. La gateway responde correctamente a la solicitud de ping.

2. Luego se envió una respuesta ARP falsa con destino de la gateway diciéndole que la dirección IP desde donde se realiza la prueba está asociada a una dirección física que no existe. Esto haría que cualquier paquete enviado desde la gateway hacia el equipo de la prueba se perdiera.
3. Se realiza una prueba de ping. No se obtiene respuesta.
4. Se envía una respuesta ARP nuevamente pero esta vez con la dirección física correcta del equipo de prueba.
5. Se realiza por ultima vez ping. Se obtiene respuesta. Los pasos anteriores se muestran a continuación:

```
akira:~# ping 10.200.2.254
PING 10.200.2.254 (10.200.2.254) 56(84) bytes of data.
64 bytes from 10.200.2.254: icmp_seq=1 ttl=255 time=0.712 ms
64 bytes from 10.200.2.254: icmp_seq=2 ttl=255 time=0.692 ms
--- 10.200.2.254 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3001ms
rtt min/avg/max/mdev = 0.692/0.734/0.833/0.057 ms

akira:~# arpoison -i eth0 -d 10.200.2.254 -s 10.200.2.134 -t 00:13:C4:4D:79:FF -r
AA:AA:AA:AA:AA:AA -w 2
ARP reply 1 sent via eth0
ARP reply 2 sent via eth0
akira:~# ping 10.200.2.254
PING 10.200.2.254 (10.200.2.254) 56(84) bytes of data.
--- 10.200.2.254 ping statistics ---
118 packets transmitted, 0 received, 100% packet loss, time 116982ms

akira:~# arpoison -i eth0 -d 10.200.2.254 -s 10.200.2.134 -t 00:13:C4:4D:79:FF -r
00:00:E8:20:6B:15 -w 2
ARP reply 1 sent via eth0
ARP reply 2 sent via eth0

akira:~# ping 10.200.2.254
PING 10.200.2.254 (10.200.2.254) 56(84) bytes of data.
64 bytes from 10.200.2.254: icmp_seq=1 ttl=255 time=0.697 ms
64 bytes from 10.200.2.254: icmp_seq=2 ttl=255 time=0.672 ms
--- 10.200.2.254 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 999ms
rtt min/avg/max/mdev = 0.672/0.684/0.697/0.029 ms
```

Se concluye entonces que la gateway es susceptible a la alteración de sus tablas ARP y por tanto hace a la red de la Universidad susceptible a que se reciba un ataque de hombre en el medio si uno de los dos extremos esta dentro de la subred del atacante.

Para realizar el ataque se utilizó la herramienta *ettercap*[11]; ésta herramienta es la más conocida en cuanto a técnicas de hombre en el medio se refiere, y entre ellas están: suplantación ARP, redirección ICMP, suplantación DHCP, robo de puerto. El esquema de la figura 2.8 muestra el esquema de la red universitaria a pequeña escala donde se llevó a cabo el ataque.

[11] Herramienta Ethercap, disponible en: http://ettercap.sourceforge.net

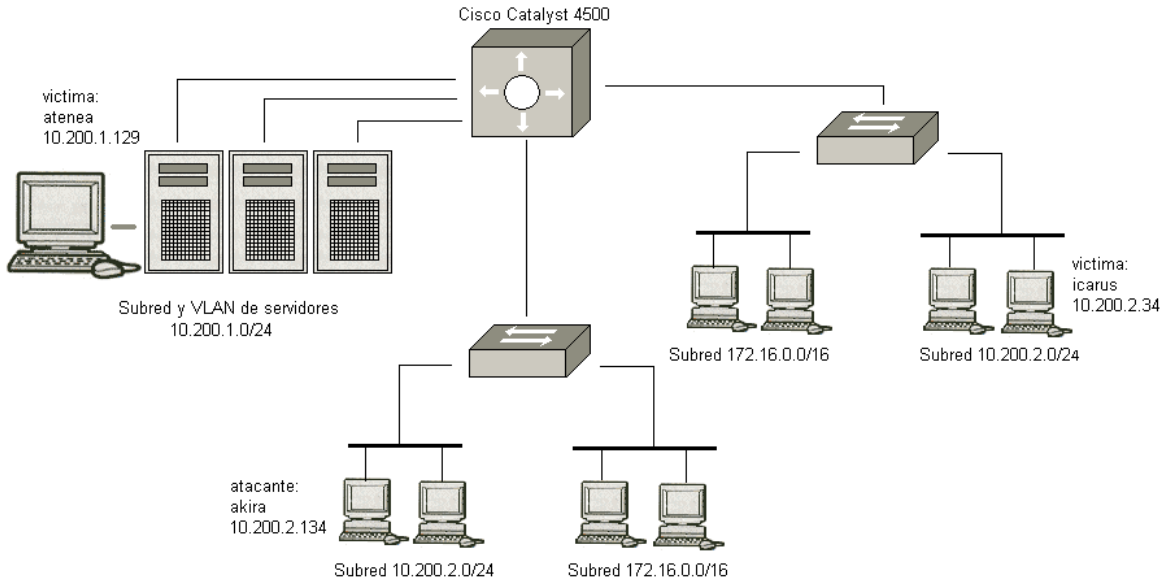


Figura 2.8 Escenario de prueba para comprobar vulnerabilidades de hombre en el medio entre redes de la Universidad del Cauca

En la figura 2.8 se muestra el switch principal de nivel 3 que interconecta las subredes; a la izquierda de este se encuentra la única subred que se encuentra separada físicamente de las demás, la cual está formada por los servidores de la Red de Datos; también forman una VLAN segmentada en los puertos del switch donde los servidores están conectados directamente. En la parte inferior se encuentran cuatro segmentos de red separados por switchs de borde y estos conectados al switch principal. En cada segmento de red se puede observar que hay equipos que pertenecen a las subredes lógicas 172.16.0.0/16 y 10.200.2.0/24 ilustrando la heterogeneidad que existe en la Red de Datos en ese sentido. Como en un ataque de hombre en el medio existen dos víctimas, en este caso son el servidor Atenea el cual se encuentra en la subred de servidores y la estación de trabajo *Icarus*, que está en la subred lógica 10.200.2.0/24. El atacante se sitúa en la estación *Akira*, la cual comparte la red de *Icarus*. Sin embargo, un equipo de la red 172.16.0.0/16 puede pasarse lógicamente a la subred 10.200.2.0/24 si conoce una dirección IP de ese rango y la puerta de enlace (debido a que comparten la red físicamente) para realizar el ataque sobre un equipo de dicha subred.

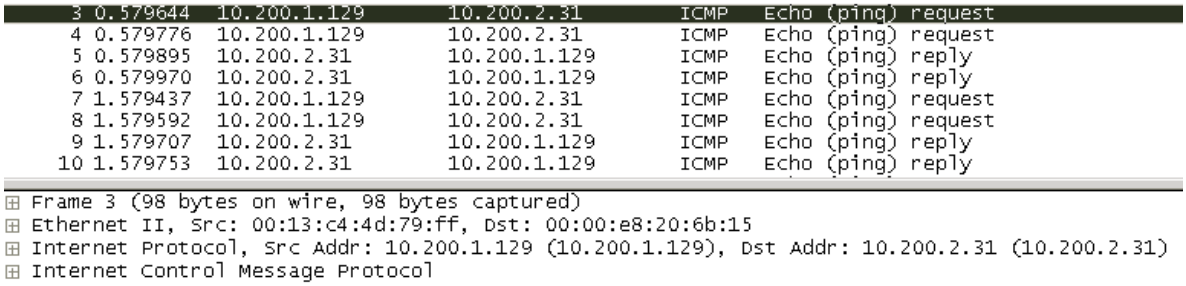
Desde *Akira* se ejecutó el siguiente comando:

```
akira:~# ettercap -T -M arp /10.200.2.254/ /10.200.2.31/

ettercap NG-0.7.1 copyright 2001-2004 ALoR & NaGA

Listening on eth0... (Ethernet)
  eth0 ->       00:00:E8:20:6B:15      10.200.2.134     255.255.255.0

SSL dissection needs a valid 'redir_command_on' script in the etter.conf
File

Privileges dropped to UID 65534 GID 65534...
```

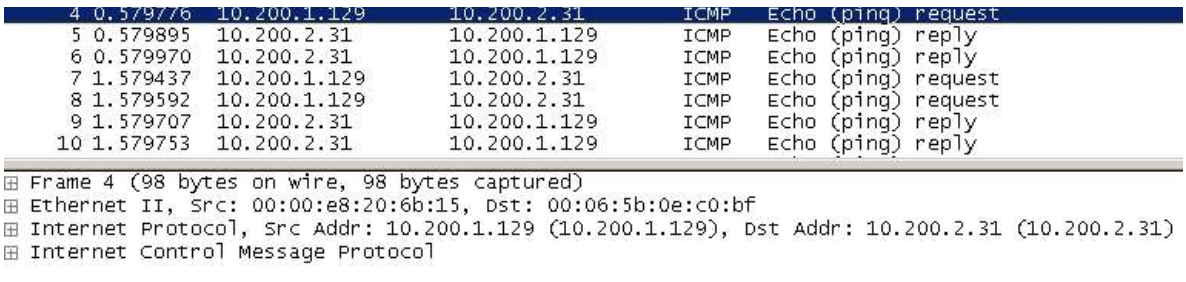
```
  27 plugins
  39 protocol dissectors
  53 ports monitored
7587 mac vendor fingerprint
1654 tcp OS fingerprint
2183 known services

Scanning for merged targets (2 hosts)...

* |==================================================>| 100.00 %

2 hosts added to the hosts list...

ARP poisoning victims:

 GROUP 1 : 10.200.2.254 00:13:C4:4D:79:FF
 GROUP 2 : 10.200.2.31 00:06:5B:0E:C0:BF
Starting Unified sniffing...
```

Con el anterior comando se le dice a *ettercap* que olfatee por medio de suplantación ARP enviando mensajes ARP falsos a Icarus (IP: 10.200.2.31, MAC: 00:06:5B:0E:C0:BF) y a la gateway (IP:10.200.2.254, MAC: 00:13:C4:4D:79:FF) que lo comunica con Atenea.

Después de hacer esto, *ettercap* reenvía los paquetes que vayan a su dirección MAC con la MAC del verdadero destinatario ya sea en sentido *Atenea-Icarus* o *Icarus-Atenea*. Para comprobar esto se realizó un ping desde *Atenea* hacia *Icarus* para ver lo que ocurre en ambos sentidos. El ping se responde normalmente y se capturó en *Ethereal* el siguiente tráfico:



En la trama 3 de la captura se observa como se recibe una solicitud de echo desde Atenea para Icarus a nivel IP, pero a nivel Ethernet va dirigido hacia la dirección de *Akira* (00:00:E8:20:6B:15).



Luego en la trama cuatro se observa como *akira* envía el mismo paquete cambiando la dirección de origen por la de él y la de destino por la verdadera dirección física de *Icarus*. Lo mismo ocurre en sentido contrario, por eso se ven dos solicitudes (*request*) y dos respuestas (*reply*), porque una es de la víctima origen hacia el atacante y otra del atacante hacia el destino. Cualquier otro tipo de comunicación IP entre los extremos atacados pasará por medio del atacante.

Debido a que las técnicas de hombre en el medio son varias, lo mejor es buscar una solución genérica al concepto y no a cada técnica específica. Por ello la solución que se adapta mejor a este requerimiento, es la implementación del protocolo IPSec en los puntos que la información que se transporta es de gran valor. La ventaja de IPSec frente a otros protocolos es que ofrece cifrado de datos a nivel IP y con él pueden implementarse topologías host-host, red-host, red-red según se necesite.

Las vulnerabilidades como inundación MAC (MAC flooding) y clonación de MAC (MAC cloning) recaen solo sobre los switchs que interconectan la red y en especial los switchs de borde, ya que si se atacan con estas técnicas solamente los switchs intermedios o el switch de núcleo los switchs de borde estarán con sus tablas ARP intactas y no enviaran el tráfico como lo desea el atacante sino que lo enviarán al destinatario verdadero. Los switchs más utilizados en la infraestructura de borde de la red universitaria son el 3COM 3300XL, el Cisco 2950 y el Nortel 350. Sobre estos switchs se llevaron a cabo pruebas de inundación ARP y de suplantación ARP con las facilidades que brinda el programa *arpoison*; las pruebas demostraron que estos tres modelos de switchs son inmunes a estos ataques por lo que hace innecesario plantear una solución en este sentido al problema de perdida de confidencialidad.

2.3 PÉRDIDA DE INTEGRIDAD

La pérdida de integridad en la transmisión de datos se presenta cuando los datos transmitidos por un extremo de la comunicación no llegan de forma correcta al destinatario. En este sentido puede haber eliminación, cambio o adición de información no autorizada. Esto puede ocurrir cuando la información pasa por una red externa o cuando la información se hace transitar por un nodo en una red interna.

Los ataques que realizan estas acciones son técnicas que crean una conexión activa de hombre en el medio. Como se observó en secciones anteriores el concepto de hombre en el medio hace que la información que se intercambia entre dos extremos de la comunicación transite por el sistema del atacante, dándole la capacidad de observar dicha información; este tipo de ataque es un ataque pasivo, pero el atacante también tiene la posibilidad de eliminar, cambiar o adicionar la información que por él transita. Esto lo constituye en un ataque activo, como lo muestra la figura 2.9:

La filosofía del ataque es muy simple; el sistema del atacante recibe paquetes interceptados a una conexión, filtra los paquetes que podrían interesarle ya sea por dirección IP, por número de puerto, por una cadena de caracteres en los campos de datos, entre otros parámetros. Después de ellos puede eliminar el paquete, enviar uno completamente nuevo, o cambiar parte de la información

contenida en el paquete; generalmente la información que se cambia es información referente a los campos de datos de las aplicaciones de alto nivel, sin embargo se puede cambiar cualquier información como direcciones IP, puertos TCP o UDP, nombres de usuario, o contraseñas que se envían en el paquete. Este no es una operación sencilla, ya que en la mayoría de protocolos existen métodos de corrección de errores basados en ARQ (Solicitud de reconocimiento), los cuales envían parámetros adicionales en el paquete para analizar la integridad de la información que se envió. Cualquier cambio en la información del paquete implica recalcular estos parámetros para adicionarlos al paquete falso y así evitar que el receptor lo rechace y pida una retransmisión del mismo.

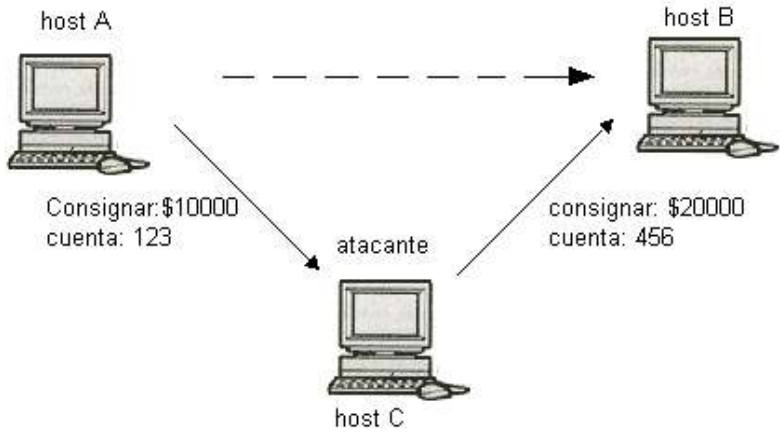


Figura 2.9 Principio de la Pérdida de Integridad de los datos

Para realizar una prueba de pérdida de integridad en las redes se usó Ettercap. Como se describió anteriormente esta herramienta puede realizar un ataque de hombre en el medio de forma pasiva, y también trae la opción de ejecutar un hombre en el medio activo. Para ello se siguieron los siguientes pasos:

1. Se creó un archivo llamado *filtro.ets* con el siguiente contenido:

```
if (ip.proto == TCP && search(DATA.data, "hola") ) {
   replace("hola", "chao");
   msg("Se cambio la palabra hola por la palabra chao.\n");
}
```

Este archivo contiene un filtro que le dirá a Ettercap que en todos los paquetes que capture de la conexión que haya interceptado, que sean paquetes TCP y contengan en el campo de datos la palabra hola, cambie la palabra "hola" por la palabra "chao", recalcule el checksum correspondiente, reconstruya el paquete y lo reenvíe enviando un mensaje a pantalla para confirmar la acción que acaba de realizar.

2. Se compiló este filtro para generar un archivo compilado llamado *filtro.et* que Ettercap pueda entender, por medio del siguiente comando:

```
#etterfilter filtro.ets -o filtro.et

etterfilter NG-0.7.1 copyright 2001-2004 ALoR & NaGA
 12 protocol tables loaded:
        DECODED DATA udp tcp gre icmp ip arp wifi fddi tr eth
 11 constants loaded:
        VRRP OSPF GRE UDP TCP ICMP6 ICMP PPTP PPPoE IP ARP
 Parsing source file 'filtro.ets'  done.
 Unfolding the meta-tree  done.
 Converting labels to real offsets  done.
 Writing output to 'filtro.et'  done.
 -> Script encoded into 6 instructions.
```

3. Luego se ejecutó *Ettercap* con el filtro compilado, para que ejecute la operación que se le ordena sobre el intercambio de información entre el equipo con dirección 10.200.2.31 y la gateway 10.200.2.254 con el comando:

#ettercap-F filtro.et-T -M arp /10.200.2.254//10.200.2.31/

4. Para comprobar el funcionamiento de la herramienta se realizó una conexión desde la dirección 10.200.2.31 hacia el servidor Afrodita por FTP; en este servidor existe un archivo llamado hola en la cuenta del usuario con que se realizó la prueba. A continuación se muestra el resultado de ejecutar el comando ls sobre la conexión FTP establecida.

```
-rw-------   1 jparra   Pregrado     3072 Mar  8  2004 hlpapp32.dll
-rw-r--r--   1 jparra   Pregrado        0 Sep  1  2004 hola
-rw-r--r--   1 jparra   Admin           0 Sep  1  2004 hola2
-rw-r--r--   1 jparra   Admin        1519 Jun 14 16:55 info.txt
```

Ahora se muestra el resultado del comando */s* después de ser víctima del hombre en el medio ejecutado por *Ettercap*:

```
-rw-------   1 jparra   Pregrado     3072 Mar  8  2004 hlpapp32.dll
-rw-r--r--   1 jparra   Pregrado        0 Sep  1  2004 chao
-rw-r--r--   1 jparra   Admin           0 Sep  1  2004 chao2
-rw-r--r--   1 jparra   Admin        1519 Jun 14 16:55 info.txt
```

Como se puede observar, la palabra "hola" ha sido cambiada satisfactoriamente por la palabra "chao".

2.3.1 Posibles Vulnerabilidades de Pérdida de Integridad en la Red de Datos de la Universidad del Cauca

Como en el caso de la pérdida de confidencialidad por la técnica de hombre en el medio, la Red de Datos universitaria es muy vulnerable a ataques que vayan en contra de la integridad de los datos. En este caso también se plantea como la mejor solución la implementación del protocolo IPSec, ya que este ofrece protección a la integridad de la información transportada por él por medio de firmas digitales. Cuando un paquete que ha sido alterado llega a un nodo IPSec, el paquete será descartado.

2.4 PÉRDIDA DE DISPONIBILIDAD

Hablar de pérdida de disponibilidad de los datos es hablar de denegación de servicio. Las redes fueron pensadas para que los datos que por ellas se transportan estuvieran siempre disponibles a quien los necesitara, sin embargo, los atacantes han ideado métodos para lograr reducir dicha disponibilidad. La disponibilidad es un parámetro de la calidad de servicio en cualquier red de telecomunicaciones, por ello la seguridad de la red debe también orientarse a mantener la disponibilidad de los recursos de la red en niveles altos.

Los ataques de denegación de servicio utilizan muchas de las técnicas que se estudiaron con anterioridad y también combinaciones de las mismas. A principios de esta década los ataques de denegación de servicio estaban en furor; alrededor del mundo fueron más de 2000 los sistemas comprometidos con este tipo de ataques, los atacantes penetraron importantes sitios de Internet como CNN y eBay. En general los ataques de denegación de servicio se extienden haciendo poco daño aparte de hacer perder ancho de banda y tiempo y, a veces, estropeando un sistema. En la gran mayoría de estos ataques la dirección de origen es falsa.

2.4.1 Denegación de Servicio por Fuerza Bruta

Los patrones de fuerza bruta han alcanzado un punto tal que son conocidos por casi todas las instituciones que están conectadas a Internet. Lo curioso es que todavía se encuentran sitios y sistemas vulnerables a ellos. Una de las características de muchos de los ataques de denegación de servicio es que los atacantes pueden utilizar un sistema de la red para causar daños a otros.

2.4.1.1 Smurf

El ataque de smurf no tiene otro efecto que el de consumir ancho de banda. Lo más importante que hay que considerar en relación con la efectividad de smurf es que para que la conexión a Internet de un sitio funcione sin complicaciones, se depende de las normativas de seguridad de otros sitios. Es un ataque muy antiguo pero todavía se ve aplicarse y haciendo uso de herramientas de ataque actuales. La razón de que todavía se lleve a cabo el smurf es que todavía funciona.

Como se observa en la figura 2.10, el host B no ha enviado ninguna solicitud ICMP al host de la red 172.16.0.0/16. En lugar de eso un equipo externo (host A) ha introducido una petición a la red. La dirección suplantada será potencialmente impactada por un gran

número de respuestas ICMP. Si tiene una conexión lenta a la red, esto puede causar serios daños; y si hay un gran número de equipos que respondan al smurf se puede hacer daño incluso a las redes rápidas.

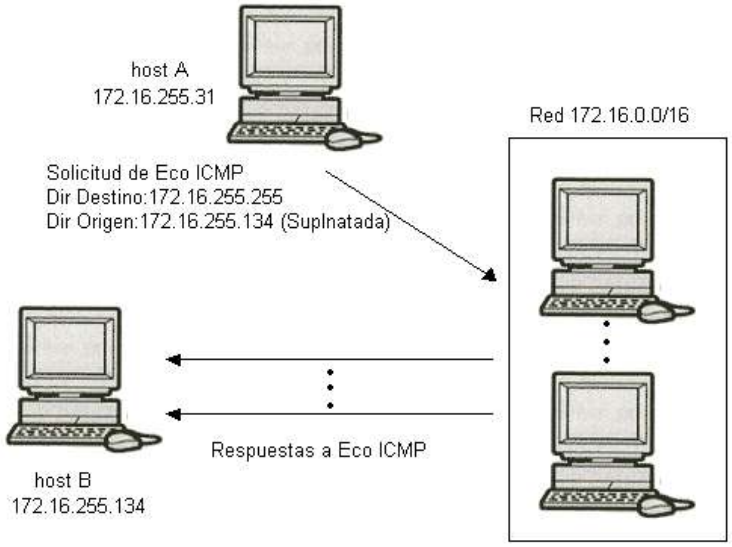


Figura 2.10 Funcionamiento de un ataque Smurf

En la figura 2.10 se puede observar que todos los equipos pertenecen a la misma red (172.16.0.0/16), sin embargo también puede llevarse a cabo aun si el host A se encuentra en otra subred, siempre y cuando las gateways o enrutadores que comunican las subredes permitan el paso de paquetes con direcciones de destino de difusión.

Un aparte del artículo publicado por Cisco titulado "Minimización de los efectos de los ataques de denegación de servicio con Smurfing"[12] ilustra un escenario:

Escenario: Una red conmutada con 100 equipos y un atacante con un enlace T1. El atacante envía, por ejemplo, un flujo de 768kbps de paquetes de solicitud de eco ICMP, con la dirección de origen suplantada de la víctima a la dirección de difusión de la red mencionada. Los paquetes llegan a la red con 100 equipos. Cada uno de ellos toma el paquete y responde creando 100 respuestas a las solicitudes de eco. Multiplicando el ancho de banda se puede observar que se están usando 76.8Mbps salientes desde la red que hace rebotar los paquetes, el cual se le está enviando a la víctima.

Los enrutadores Cisco son los más vendidos en el mundo y la Red de Datos de la Universidad del Cauca accede a Internet por medio de dos enrutadores Cisco; estos productos son clave en la eliminación de los ataques smurf ya que muchos de los ataques de DoS (Denegación de Servicio) utilizan las direcciones de difusión (broadcast) de una red para llevar a cabo sus propósitos. El RFC 919 establece varios estándares de difusión incluyendo la norma de no dejar salir a la dirección 255.255.255.255 desde un enrutador o una gateway.

[12] Artículo disponible en: http://www.cisco.com/en/US/products/hw/routers/ps133/products_tech_note09186a0080143d1b.shtml

La capa de red local siempre puede hacer corresponder una dirección IP en una dirección de capa de enlace de datos. Pero la elección de las direcciones de difusión fue un poco arbitraria; se necesitaba seleccionar un número que no fuera muy lógico asignar a un equipo. El número cuyos bits son todos 1 cumple esa propiedad, claro que no siempre se cumple que la dirección de difusión sea 255.255.255.255 y que esto depende de la dirección de la red y la mascara de subred sobre la que se haga el análisis. La dirección de difusión es muy usada por ejemplo en aplicaciones que no conocen la dirección de un recurso o servicio, para lo cual envían un mensaje a todos los equipos en la subred preguntando por dicho recurso o servicio.

Una de las subredes implementada en la Red de Datos es la subred 172.16.0.0/16 cuya dirección de difusión es la dirección 172.16.255.255. En horas laborales, a una solicitud de eco ICMP hacia está dirección de difusión responderían mas de 1000 equipos, los cuales pertenecen a dicha red.

2.4.1.1.1 Amplificación del Smurf

Es probable que un paquete llegue desde una red externa como Internet a una Intranet como la de la Universidad del Cauca con dirección de destino 255.255.255.255; el paquete descrito, sería un simple paquete de difusión que se extendió hasta los enrutadores que conectan la red interna con el exterior. Dependiendo del funcionamiento del enrutador, este podría difundir el paquete a las interfaces internas amplificando la difusión; por este motivo un paquete procedente de una dirección suplantada termina siendo amplificado en cientos o miles de paquetes. Los sitios que no bloquean ICMP entrantes son conocidos como amplificadores Smurf[13].

2.4.1.2 Eco de Generación de Caracteres (Echo-Chargen)

Es otro ejemplo de ataque de fuerza bruta clásico que utiliza sitios pobremente defendidos y pobremente configurados como amplificadores. Busca generalmente sistemas basados en Unix para que actúen como amplificadores, así que no es tan potente como Smurf, que utiliza cualquier sistema. El servicio de Eco se encuentra en el puerto 7 de UDP; si recibe un paquete devuelve la carga útil. Chargen (generador de caracteres) se encuentra en el puerto 19 de UDP; si se envía un Chargen de cualquier carácter responde con una cadena pseudoaleatoria de caracteres. La combinación de estas dos características es la base de ataque.

Como en el esquema de la figura 2.10, si el atacante suplanta la dirección del host B y envía cierto número de paquetes UDP cada uno hacia un equipo diferente de la red con dirección de origen: la dirección de la víctima, puerto UDP de origen: el puerto de Eco y puerto de destino de cada equipo: el puerto Chargen, todos lo equipos a los que llega el paquete por puerto Chargen responderían a la víctima hacia su puerto de Eco, lo que haría que la víctima respondiera a todos sus emisores por su puerto de Eco hacia el puerto de Chargen creando un ciclo infinito que generaría una disminución del ancho de banda útil de la víctima y dependiendo del número de equipos a los que se envíen los paquetes UDP suplantados se podría lograr una denegación de servicio total.

[13] Se puede encontrar una lista de ellos, incluyendo los 10 más importantes en www.powertech.no/smurf o en www.netscan.org

Este ataque tiene como desventaja con respecto al ataque de smurf, que el atacante no puede enviar un mensaje de difusión a los equipos que masificarán el ataque sino que tiene que enviar mensaje por mensaje a cada dirección IP que usará como "rebote".

2.4.1.3 Inundación SYN (SYN Flooding)

El propósito de este ataque es llenar la cola de conexión de uno o varios puertos TCP de la víctima. Esto lo hace enviando una serie de segmentos TCP de sincronización (SYN) para simular que abrirá una conexión TCP en un puerto específico de la víctima. La conexión estará en un estado medio-abierto ya que no se ha completado el proceso de establecimiento de una conexión TCP. Cada segmento debe tener un puerto de origen diferente para que la víctima almacene información por cada intento de conexión desde un puerto diferente. Cuando se exceda el número límite de conexiones entrantes del servicio que escucha por el puerto atacado puede aceptar, este no aceptará más conexiones, denegando el servicio permanentemente.

Las inundaciones SYN más sencillas utilizan la misma dirección IP de origen para generar las solicitudes de conexión, lo que los hace fácilmente identificables. Sin embargo, ataques más complejos utilizan direcciones de origen suplantadas aleatorias lo que los hace mucho más difíciles de detectar.

Para un sistema de detección de intrusos es muy fácil equivocarse, generando una alarma cuando en realidad no se presenta ningún comportamiento anómalo de inundación SYN. Por ejemplo, los sistemas de correo electrónico deben hacer varios intentos de entrega de un correo, sino lo pudo realizar la primera vez generando varias conexiones sobre el puerto 25 (SMTP) desde una misma dirección IP. Otra falsa alarma se presenta cuando el Microsoft Internet Explorer abre una página web, ya que crea una conexión por cada archivo de formatos gif, jpeg, html, etc. Hasta un limite de 32. Por estos motivos hay que analizar cuidadosamente antes de emitir una alarma de inundación SYN sobre los puertos 25(SMTP), 80(HTTP) y 443(HTTPS) de TCP. La inundación SYN puede ser parte de un ataque mayor, por ejemplo una suplantación IP como cuando se observa un patrón de inundación SYN dirigido contra un puerto de conexión asociado con relaciones de confianza, como 513(rlogin), 22(ssh) o 139(NetBIOS).

La herramienta *hping2* puede implementar un ataque de esta clase por medio del siguiente comando:

#hping2 --faster --rand-source --baseport 30000 --destport 23 --syn 172.16.16.255.254

El comando anterior envía segmentos TCP SYN hacia el puerto 23 de la dirección 172.16.255.254 desde una dirección de origen aleatoria y diferente por cada paquete, con puerto TCP de origen 30000 y los envía cada segmento TCP cada milisegundo. Lo cual desbordaría la cola de conexiones TCP de una máquina.

Aunque este ataque puede llevarse a cabo sobre el puerto de cualquier servicio en escucha, los sistemas operativos actuales se protegen, contra este problema. Una de las maneras de protegerse es no aceptar un número de solicitudes de conexione mayor a un valor preestablecido (por ejemplo, máximo 1041 conexiones) para un puerto TCP. Si llega una nueva solicitud de conexión, se desechará la primera solicitud de conexión que está en la cola y se aceptará la que acaba de llegar. Sin embargo, los dispositivos poco

inteligentes como switchs o routers, por lo general rechazan las nuevas solicitudes de conexión TCP, cuando se ha llenado su cola de conexión. En el ejemplo se ha atacado el switch de núcleo con dirección 172.16.255.254, que posee la Red de Datos, el cual ofrece el servicio de *telnet* para administración remota. Este servicio escucha en el puerto 23 de TCP. Antes del ataque, al tratar de conectarse por *telnet* al switch se obtiene lo siguiente:

```
icarus:~# telnet 172.16.255.254
Trying 172.16.255.254...
Connected to 172.16.255.254.
Escape character is '^]'.


User Access Verification
Password:
```

Lo cual indica que la conexión fue exitosa. Después del ataque se obtiene lo siguiente:

akira:~#telnet 172.16.255.254
Trying 172.16.255.254...

No se logra la conexión, debido a que la cola de conexiones entrantes está llena y no aceptará hasta que deje de recibir solicitudes de conexión y liberé la memoria de las conexiones no establecidas. Un ataque de DoS al servicio de *telnet* exitoso.

2.4.2 Ataques Elegantes

Los ataques de fuerza bruta tienden a aprovecharse de suplantación de direcciones para proporcionar gran cobertura al atacante. Los ataques mas elegantes pueden operar con muchas menos huellas. Sacan provecho de los errores en la capacidad de tratar con condiciones ilegales de la pila IP o incluso de la mala programación, como se verá a continuación.

2.4.2.1 Ataque de Lágrima (Teardrop)

Aprovecha el hecho de que las pilas del protocolo de red no son muy hábiles con las matemáticas y en especial con los números negativos. Un ejemplo de este ataque es el de crear o manipular datagramas IP fragmentados. Por ejemplo si un equipo recibe un paquete con 36 bytes de datos y un desplazamiento de 0 con respecto al datagrama no fragmentado y luego recibe un datagrama de 4 bytes con un desplazamiento de 24 con respecto al datagrama no fragmentado el sistema operativo tendría que regresar de 36 a 24. El escenario anterior no puede presentarse en condiciones normales ya que el desplazamiento del segundo paquete tendría que ser un número mayor o igual a 36. Si el sistema operativo no esta preparado para manejar un número negativo en esa situación lo más seguro es que lo interprete como un número positivo grande y posiblemente altere los datos de memoria que pertenece a otro proceso. Si esto ocurre más de una vez se sobrescribirían campos de memoria que pueden hacer fallar el sistema operativo. Los fabricantes de sistemas operativos han tenido en cuenta estas vulnerabilidades y las han eliminado de sus nuevas versiones, por ello este ataque solo funciona en sistemas operativos viejos.

Otra característica de la fragmentación es que elude sistemas de detección de intrusos que no soportan fragmentación y reconstrucción de paquetes. Si el IDS analiza fragmento por fragmento por separado y no reconstruye el datagrama no fragmentado no podrá analizar toda la información, sino pedazos de ella.

2.4.2.2 Ping de la Muerte (Ping of Death)

Es otro ataque que depende de sistemas operativos vulnerables los cuales son los más antiguos que existen. Todo lo que hay que hacer es exceder el máximo tamaño permisible de un paquete ICMP que es de 65535 bytes y el sistema fallará si no sabe como administrarlo.

Los datagramas IP pueden tener un tamaño de hasta 65535 (2^{16}-1) bytes, lo que incluye el tamaño del encabezamiento (generalmente de 20 bytes si no se especifican opciones IP). Los paquetes mayores que los que puede manejar el nivel inferior (MTU – Unidad Máxima de Transferencia) se fragmentan en paquetes más pequeños que son reconstruidos por el receptor. En las redes Ethernet, como es el caso de la red de la Universidad de Cauca la MTU es de 1500 bytes.

Una solicitud de eco ICMP es una capa de 3 paquetes IP con su pseudoencabezado que consiste en 8 bytes de información de encabezamiento ICMP, seguidos por el número de bytes de datos de la solicitud. Por tanto, el tamaño máximo permitido del área de datos es el tamaño máximo del paquete menos el encabezamiento IP y menos el pseudoencabezamiento (65535 – 20 – 8 = 65507 bytes).

Si se envía una solicitud de eco ilegal con más de 65507 bytes de datos debido a la forma en que se realiza la fragmentación, hay problemas; la fragmentación confía en un valor de desplazamiento de cada fragmento para determinar su posición en la reconstrucción. Por tanto, en el último fragmento es posible combinar un desplazamiento valido con un tamaño de fragmento de forma que la suma (desplazamiento + tamaño) sea mayor que 65535. Como los equipos normales no procesan el paquete hasta que tienen todos los fragmentos y tratan de reconstruirlos, hay posibilidades de que se produzca una sobrecarga de variables internas causando errores en el sistema operativo.

2.4.2.3 Terminación de conexión TCP

Existen dos métodos para terminar una conexión TCP: el método elegante y el método brusco. En el método elegante uno de los dos extremos, el cliente o el servidor, indica al otro a través de un segmento FIN que quiere finalizar la sesión. El extremo receptor le devuelve un ACK lo que acaba con la mitad de la conexión. Entonces el otro extremo debe iniciar un FIN y el extremo receptor deberá acusar recibo de tal segmento.

El segundo método de finalización es una terminación brusca de la conexión. Se lleva a cabo cuando un extremo le envía un segmento TCP RST al otro. Esto finalizará la conexión y no deberá haber intercambio de información entre los extremos. Este método es el más usado por los atacantes para generar ataques de denegación de servicio sobre una dirección o sobre un servicio específico.

El atacante solamente se sitúa con un sniffer a escuchar el tráfico en la red y dependiendo del parámetro que elija (dirección o puerto) para ubicar su víctima debe capturar un paquete que se dirija o salga de ella para luego enviar un paquete igual pero con la bandera de reset puesta en 1 para que la conexión sea interrumpida. El atacante también puede denegar servicio a todo el segmento de red hasta donde tiene alcance para escuchar tráfico, si por cada paquete que capture genera uno igual con la bandera de reset en 1.

2.4.2.4 Envenenamiento ARP

Consiste en envenenar la caché ARP de los equipos; es la misma técnica usada como parte de la suplantación ARP. Como se explicó en la sección 31.2, con esta técnica se puede denegar el servicio de un servidor a un equipo especifico o a una red completa envenenando la caché ARP con respuestas falsas que supuestamente provengan del equipo al que se quiere denegar el servicio o que supuestamente provengan de la gateway que comunica al servidor con otras redes.

2.4.3 Posibles Vulnerabilidades de Pérdida de Disponibilidad en la Red de Datos de la Universidad del Cauca

La Red de Datos de la Universidad del Cauca utiliza, para interconexión tanto interna como externa de sus redes, equipos Cisco que cumplen con los estándares de difusión dictados por la IETF lo que ayuda a minimizar el impacto de un ataque como el de smurf. Sin embargo las subredes que se han creado son muy pocas y cada una alberga a un muchos equipos lo que hace que un ataque smurf sea aún potencialmente peligroso. Para reducir este riesgo se debe hacer una mejor subdivisión de las subredes que existen actualmente y así asegurar que los equipos que respondan a las peticiones maliciosas creadas en estos ataques sean muy pocos.

Para los demás ataques se utilizan soluciones genéricas como la implementación y correcta configuración de Firewalls e IDS, configuraciones de la red como VPNs y VLANs e incluso en algunos la mejor solución es implementar las características de autenticación e integridad que ofrece el protocolo IPSec.

En el Anexo A se realiza una introducción a la seguridad de las redes WLAN actuales y las principales vulnerabilidades del protocolo de seguridad WEP (Wired Equivalent Privacy), ya que dentro de la Universidad del Cauca se están desarrollando varios proyectos con redes Inalámbricas (entre ellos el proyecto EHAS - Enlace Hispano Americano de Salud, que implementa una conexión WiFi con el municipio de Silvia), y es importante tener una idea de este tipo de enlaces en los que también juega un papel importante la seguridad, y sobre los cuales es posible implementar los mismos protocolos y mecanismos de seguridad que se estudiarán más adelante.

Resumen

La Tabla 2.3 muestra un resumen de las vulnerabilidades mas destacadas, aplicables en la Red de Datos de la Universidad del Cauca, sus causas y su solución o soluciones más efectivas.

Tabla 2.3 Resumen de las principales vulnerabilidades, sus causas y soluciones

Vulnerabilidad	Causa	Solución
Suplantación IP	Falta de autenticación de las direcciones de origen en la cabecera IP	• IPSec utilizando AH
Suplantación ARP	Aceptación de respuestas ARP, sin previa solicitud ARP y falta de autenticación de las direcciones de origen en la cabecera Ethernet.	• Port Security • 802.1X • Tablas ARP estáticas • VLANs
Olfateo (Sniffing)	Falta de cifrado de datos en el datagrama IP.	• IPSec utilizando ESP • Cifrado de datos por parte de aplicaciones de nivel superior.
Hombre en el medio pasivo	Falta de cifrado de datos en el datagrama IP.	• IPSec utilizando ESP • Cifrado de datos por parte de aplicaciones de nivel superior.
Hombre en el medio activo	Falta de integridad de los datos en el datagrama IP.	• IPSec utilizando ESP con AH.
Smurf	Falta de autenticación de las direcciones de origen en la cabecera IP.	• IPSec utilizando AH • División en subredes
Inundación SYN	Falta de autenticación de las direcciones de origen en la cabecera IP.	• IPSec utilizando AH
Terminación de conexión TCP	Falta de integridad de los datos en el datagrama IP.	• IPSec utilizando ESP con AH
Envenenamiento ARP (Broadcast)	Aceptación de respuestas ARP, sin previa solicitud ARP y falta de autenticación de las direcciones de origen en la cabecera Ethernet.	• Port Security • 802.1X • Tablas ARP estáticas • VLANs • División en subredes IP

En el capítulo 3 se hace un estudio del protocolo IPSec y sus protocolos relacionados, su arquitectura, y se definen conceptos importantes como las Asociaciones y Políticas de seguridad, que se utilizarán en el capítulo 5 a la hora de hacer la implementación práctica.

CAPITULO III: ESTANDARES DE SEGURIDAD A NIVEL DE RED EN IPv4 E IPv6

3.1 PROTOCOLO IPSec: IP SECURITY

El impresionante crecimiento de Internet y su correspondiente conectividad, además del advenimiento de nuevos servicios, ha propiciado que intrusos técnicamente avanzados consideren como un reto constante el emprender ataques de índole diversa que amenacen la integridad y la privacidad de redes de comunicación de datos en general. Por otro lado, el avance de la tecnología de comunicaciones y sus beneficios ha modificado el rechazo inicial de usuarios gubernamentales o de negocios a relegar en Internet elementos estratégicos de información. En particular el temor a intrusos anónimos provenientes de Internet está obligando a las organizaciones a considerar soluciones radicales tales como la separación entre redes de datos privadas (Intranets) y la red pública Internet. La segmentación obtenida se está constituyendo en un fuerte impedimento para lograr el concepto de una red Internet global, lo que establecería una conectividad fuertemente acoplada.

En 1994, el *Internet Architecture Board* (IAB) emitió el reporte "*Security in the Internet Architecture*" (Seguridad en la Arquitectura de Internet - *RFC 1636*), el cual establecía que Internet requería una mayor y mejor seguridad, además, identificaba las áreas claves que requerían mecanismos de seguridad. Entre las principales necesidades quedaron identificadas: el aseguramiento de la infraestructura de red, tanto del monitoreo como del control del tráfico no autorizado, y la protección del trafico *usuario_final usuario_final* utilizando mecanismos de autenticación y de encriptación.

El protocolo IP, *Internet Protocol*, es uno de los más usados para la interconexión de redes tanto en ambientes académicos como corporativos, y naturalmente lo es también en la Internet pública. Su flexibilidad y sus poderosas capacidades lo han impuesto como un vehículo de interconectividad por un largo tiempo. La fuerza de IP radica en su facilidad y su flexibilidad para el envío de grandes volúmenes de información en pequeños datagramas a través de los diversos esquemas de enrutamiento. Sin embargo, IP presenta ciertas debilidades: la forma en que el protocolo enruta los paquetes hace que las grandes redes IP sean vulnerables a ciertos riesgos bien conocidos de seguridad, que limitan y complican su uso en comunicaciones altamente sensibles. El grupo internacional *IP Security Protocol Working Group* organizado bajo el *Internet Engineering Task Force* (IEFT) desarrolló el ***IP Security Protocol Suite, IPSec,*** como un conjunto de extensiones para IP que ofrecen servicios de seguridad en el nivel de red de acuerdo con el modelo de Interconexión de Sistemas abiertos, OSI (Open System Interconection, basado en la propuesta desarrollada por la Organización de Estándares Internacional - ISO). La tecnología de IPSec se basa en la criptografía moderna, lo que garantiza, por un lado, la privacidad y, por otro, una autenticación fuerte de datos.

Las características de IPSec lo hacen único debido a que implementa seguridades en la capa *de red* más que en la *de aplicaciones*. En el pasado, otros grupos han desarrollado métodos a nivel de aplicación para protección de comunicaciones,

efectivos para resolver problemas de seguridad particulares. Dado que el protocolo IPSec asegura a la red por sí misma, se garantiza que las aplicaciones que se estén usando en la red sean, en efecto, seguras.

Existen ya numerosos productos que implementan IPSec; para ofrecer seguridad en el nivel de IP es necesario que IPSec sea parte del código de red en todas las plataformas participantes (sistemas Windows, Linux y otras), pues de otra manera una aplicación dada podría fracasar al intentar usar las funciones de seguridad del protocolo. IPSec ofrece tres facilidades principales:

- Una función de autenticación, referida como *Authentication Header* (AH).
- Una función combinada de autenticación/encriptación llamada *Encapsulating Security Payload* (ESP).
- Una función de intercambio de llaves, *Internet Key Exchange Protocol* (IKE).

3.1.1 Arquitectura de IPSec

En agosto de 1995, el IETF publicó cinco documentos relacionados con la propuesta para estandarizar la capacidad de seguridad a nivel de toda Internet:

- *RFC 1825*: Descripción de la arquitectura de seguridad.
- *RFC 1826*: Descripción del paquete de extensión para autenticación en IP.
- *RFC 1828*: Especificación del mecanismo de autenticación.
- *RFC 1827*: Descripción de paquete de extensión para encriptación en IP.
- *RFC 1829*: Especificación del mecanismo de encriptación.

Estas características son obligatorias en IPv6 y opcionales en IPv4; en ambos casos, la parte de seguridad se implementa mediante encabezados de extensión que siguen al encabezado principal de IP. Los documentos que contienen la especificación completa de IPSec se agruparon en siete categorías (Figura 3.1):

- *Architecture*: Establece los conceptos generales, requisitos de seguridad, definiciones y mecanismos característicos de la tecnología de IPSec.
- *Encapsulating Security Payload* (ESP): Describe el formato del paquete y las definiciones generales relacionadas para el uso de ESP para la encriptación de paquetes, y opcionalmente la autenticación.
- *Authentication Header* (AH): Describe el formato del paquete y las definiciones generales relacionadas para el uso de AH para la autenticación de paquetes, así como su algoritmo MAC (Message Authentication Code).

- *Encryption Algorithm*: Documentos que describen cómo los diversos algoritmos de encriptación son utilizados por ESP, tales como DES, Triple-DES, RC5, IDEA, CAST, BLOWFISH y RC4.
- *Authentication Algorithm*: Documentos que describen cómo los diversos algoritmos son usados por AH y por la opción de autenticación de ESP.
- *Key Management*: Documentos que describen los esquemas para administración de las llaves.
- *Domain of Interpretation* (DOI): Contiene parámetros necesarios para diversos documentos relacionados entre sí. Estos incluyen identificadores para algoritmos de autenticación y de encriptación aprobados, así como también parámetros operacionales tales como *tiempos de vigencia de llaves* (*key lifetime*). El documento *DOI* de normas para IPSec especifica todos los parámetros asociados con los protocolos AH y ESP, y los asigna como identificadores únicos. Este documento sirve como base de datos de valores para ser referenciados durante la negociación de la Asociación de Seguridad IPSec, como se verá más adelante. El diagrama de la arquitectura de IPSec se muestra en la Figura 3.1.

La arquitectura de Seguridad del Protocolo de Internet conocida como ***IP Security*** (RFC2401), es el esfuerzo más avanzado para estandarizar la seguridad en Internet. IP es el vehículo común para los protocolos de las capas más altas y en consecuencia es susceptible de enfrentar ataques severos, ya sea a la seguridad de los datos manejados por las aplicaciones y transportados por los protocolos de las capas más altas, como TCP (*Transmision Control Protocol*), o al comportamiento de la red en sí misma interviniendo los protocolos de control como ICMP (*Internet Control Message Protocol*) o BGP (*Border Gateway Protocol*). Tanto en la versión actual de IP (IPv4) como en IP de nueva generación (IPv6) es posible utilizar IPSec debido a la modificación retroactiva de los mecanismos de seguridad de IPv6 en IPV4.

IPSec puede usarse para proteger la capa de IP *entre un par de sistemas finales o servidores*, *entre un par de sistemas intermedios, también conocidos como gateways, o entre un servidor y una gateway de seguridad* (una gateway de seguridad es un sistema intermedio que implementa protocolos IPSec). Una *gateway* permite el reenvío de paquetes en la capa de IP, y por tanto puede ser un *router*, un *Firewall* o un servidor. Los protocolos de IPSec tienen las siguientes funciones de seguridad en la capa IP:

- *Autenticación del origen de los datos:* Define mecanismos para garantizar la procedencia de la información, ya sea a nivel de usuario o de equipo.
- *Integridad de datos*: Implica que los datos no han sido modificados o corrompidos de manera alguna desde su transmisión hasta su recepción.
- *Detección de respuesta y protección antirrepetición:* Es la forma como se garantiza la transmisión y la recepción de la información; busca proteger al emisor de que el receptor niegue haber recibido el mensaje y proteger al receptor de que el transmisor niegue haber enviado el mensaje.

- *Confidencialidad de datos*: Implica que la información sea accesible únicamente por las entidades, sistemas o personas autorizadas.
- *Control de acceso:* Establece la forma en que el recurso esté disponible cuando es requerido.

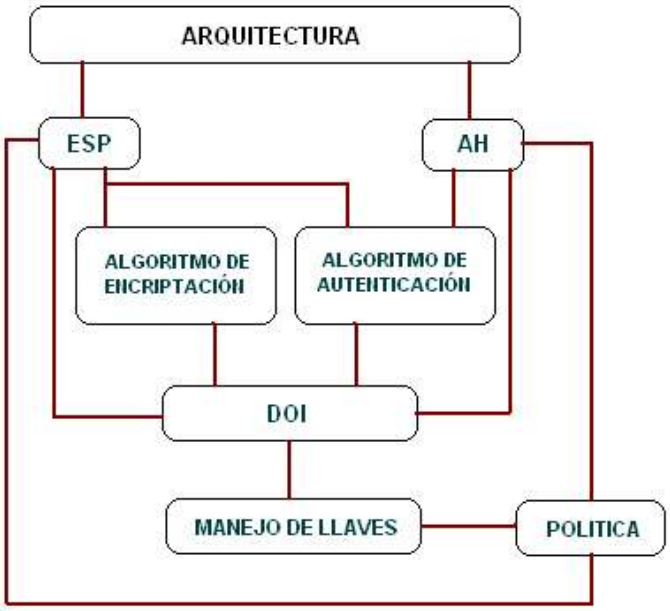


Figura 3.1 Arquitectura de IPSec

Suplementariamente a los mecanismos de seguridad individual implementados por estos servicios, IPSec cuenta con facilidades de administración para la negociación de servicios y de parámetros entre las partes comunicantes, así como también, para el intercambio de llaves criptográficas requeridas por los mecanismos de seguridad básicos, los cuales se diseñaron para no depender de los algoritmos criptográficos actuales y, en consecuencia, propiciar su posible evolución. No obstante, hay algoritmos por omisión definidos para cada servicio, lo cual facilita su interoperabilidad.
La versión más reciente de IPSec consta de los siguientes componentes (ver Figura 3.2):

- Dos *Protocolos de Seguridad*: IP Authentication Header (AH) e IP Encapsulating Security Payload (ESP) que aportan los mecanismos básicos de seguridad dentro de IP, junto con los algoritmos para autenticación y encriptación.
- *Security Associations* (SA), que especifican los servicios de seguridad y los parámetros negociados en cada trayectoria segura IP.
- *Security Databases*, dentro de las cuales se tienen la Base de Datos de Asociaciones de Seguridad (SAD) y la Base de Datos de Políticas de Seguridad (SPD).

Figura 3.2 Componentes de la Arquitectura de IPSec

3.1.2 Protocolos de Seguridad

IPSec está formado por un conjunto de protocolos que proporcionan servicios de seguridad para proteger el tráfico IP. Estos servicios pueden ser implementados gracias a dos protocolos, el *Authentication Header (AH)* y el *Encapsulating Security Payload (ESP)*, además de algunos protocolos y mecanismos para la gestión de llaves cifradas tales como el *Internet Key Exchange Protocol (IKE)*. De esta forma, una implementación satisfactoria de IPSec depende fundamentalmente de una adecuada escogencia del protocolo de seguridad y de la forma como se intercambian las llaves cifradas.

El protocolo AH garantiza integridad, autenticación del origen de los datos, y un servicio opcional antirrepetición. De esta forma, proporciona un mecanismo al receptor de los paquetes para verificar que los datos no hayan sido alterados durante la transmisión. Sin embargo, AH no garantiza confidencialidad, es decir que los datos pueden ser vistos por terceros durante su transporte.

El protocolo ESP si garantiza confidencialidad (encriptación) y flujo de tráfico limitado; adicionalmente ofrece integridad, autenticación del origen de los datos y protección antirrepetición, de manera similar a AH, pero solo uno de estos servicios puede ser proporcionado por ESP al mismo tiempo.

Ambos, AH y ESP son vehículos para control de acceso, basados en distribución de llaves criptográficas y en la administración del flujo de tráfico relativo a esos protocolos de seguridad. El protocolo IKE es muy utilizado para el intercambio automático de llaves cifradas y para negociar todos los parámetros necesarios para establecer una conexión AH o ESP. Este protocolo autentica a los participantes en una primera fase, en una segunda fase se negocian las asociaciones de seguridad y se escogen las claves secretas simétricas a través de un intercambio de claves Diffie Hellmann. El protocolo IKE se ocupa incluso de renovar periódicamente las claves para asegurar su confidencialidad.

Los principales servicios proporcionados por cada protocolo se muestran a continuación:

Tabla 3.1 Servicios de AH y ESP

	AH	ESP (Solo encriptación)	ESP (Encriptación más autenticación)
Control en el acceso	X	X	X
Integridad sin conexión	X		X
Autenticación del origen de los datos	X		X
Rechazo de paquetes Retocados	X	X	X
Confidencialidad		X	X
Confidencialidad limitada por el tráfico		X	X

El protocolo IPSec ha sido diseñado de forma modular, de modo que se pueda seleccionar el conjunto de algoritmos criptográficos deseados para complementar los protocolos anteriores, sin afectar a otras partes de la implementación. Han sido definidos, sin embargo, ciertos algoritmos estándar que deberán soportar todas las implementaciones para asegurar la interoperabilidad en el mundo global de Internet (Figura 3.3). Dichos algoritmos de referencia son DES (Data Encryption Standard – Estándar de Cifrado Datos) y 3DES (Estándar de Cifrado Datos Triple) para cifrado, así como MD5 (Message Digest 5 – Resumen de Mensaje 5) y SHA-1 (Secure Hash Algorithm – Algoritmo Hash Seguro) como Funciones de Hash (algoritmo de cifrado que convierte un mensaje de cualquier longitud en una sola cadena de dígitos). Además es perfectamente posible usar otros algoritmos que se consideren más seguros o más adecuados para un entorno específico: por ejemplo, como algoritmo de cifrado de clave simétrica IDEA (Internacional Data Encryption Algorithm – Algoritmo Internacional de Cifrado de Datos), Blowfish o el más reciente AES (Advanced Encryption Standard – Estándar de Cifrado Avanzado), que se espera sea el más utilizado en un futuro próximo.

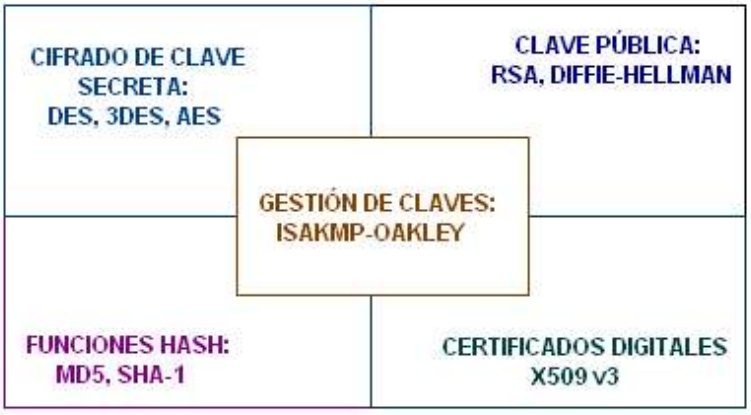


Figura 3.3 Tecnologías Utilizadas en IPSec

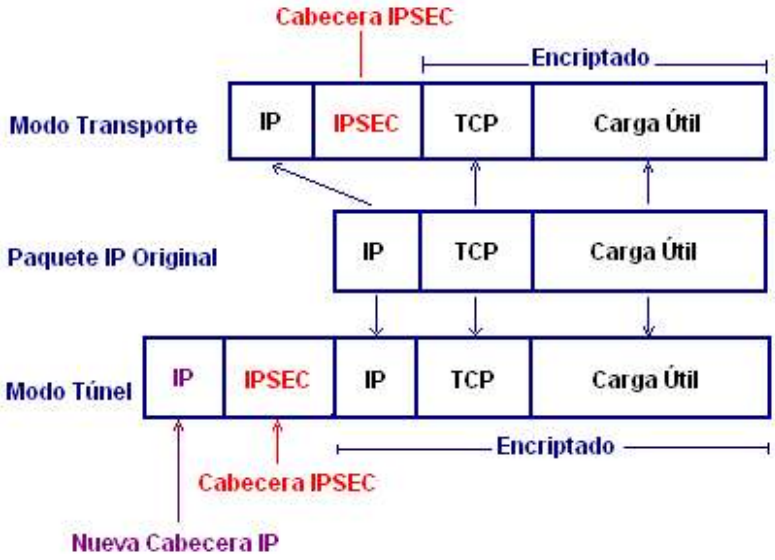


Figura 3.4 IPSec: Modos Túnel y Transporte

Los protocolos AH y ESP pueden ser aplicados cada uno por separado, o combinados, para proveer un robusto set de servicios de seguridad, tanto para IPv4 como para IPv6. Además, dentro de su funcionamiento, IPSec puede proteger el datagrama IP completo o sólo los protocolos de capas superiores, gracias a que estos protocolos soportan dos modos de uso: *Modo Túnel* y *Modo Transporte*. En Modo Túnel, el datagrama IP se encapsula completamente dentro de un nuevo datagrama IP insertando la cabecera IPSec y una nueva Cabecera IP. En Modo Transporte, IPSec sólo maneja la carga útil del datagrama IP, insertando la cabecera IPSec entre la cabecera IP y la cabecera del protocolo del nivel de Transporte (ver Figura 3.4).

Por otro lado, para que los participantes de una comunicación puedan encapsular y desencapsular los paquetes IPSec, se necesitan mecanismos para almacenar las claves secretas, algoritmos y direcciones IP involucradas en la comunicación. Todos estos parámetros se almacenan en *Asociaciones de Seguridad* (Security Associations - SA) y estas a su vez se almacenan en *Bases de Datos de Asociaciones de Seguridad* (Security Asocciation Databases - SAD), como se verá a continuación.

3.1.2.1 Asociaciones de Seguridad (AS)

Una Asociación de Seguridad es una conexión unidireccional (simplex) que ofrece servicios de seguridad al tráfico que pasa a través de ella. Estos servicios de seguridad que ofrece una AS son proveídos por AH o ESP pero no por ambos y son acordados previamente; si se quiere implementar protección con AH y con ESP, deben crearse dos o más AS. De la misma forma, para una comunicación bidireccional entre dos hosts, o entre dos gateways de seguridad, se requieren dos Asociaciones de Seguridad (una en cada dirección).

Cada Asociación de Seguridad está definida por los siguientes 3 parámetros:

- Dirección IP del destino de la Asociación de Seguridad.
- Identificador del Protocolo de Seguridad: es el número que identifica el tipo de protocolo de Seguridad que se utiliza, 51 para AH y 50 para ESP.
- Índice de parámetro de seguridad (SPI - Security Parameter Index): indica cuales son los parámetros de Seguridad específicos a la AS que se está utilizando. Es la forma para que, en una comunicación segura, el origen pueda identificar cual AS debe utilizar para asegurar un paquete y de igual forma, para que el destino identifique cual AS utilizar para verificar la seguridad del paquete recibido. El SPI es un número de 32 bits que se incluye en los encabezados AH y ESP, y el destino utiliza el conjunto *Destino, SPI, Protocolo* para identificar de forma única la AS.

Como se mencionó anteriormente, pueden definirse dos tipos de Asociaciones de Seguridad: en Modo Transporte y en Modo Túnel (Figura 3.4). Una *Asociación de Seguridad en Modo Transporte* es una AS entre dos hosts; en IPv4, un encabezado del protocolo de seguridad en modo transporte aparece inmediatamente después del encabezado IP original y antes de algún protocolo de capa superior (como TCP o UDP). En IPv6 el encabezado del protocolo de seguridad aparece después del encabezado IP base y sus extensiones, pero puede aparecer antes o después de las opciones de destino y antes de los protocolos de capas superiores. En el caso de ESP, una Asociación de Seguridad en modo transporte provee servicios de seguridad solo para los protocolos de capas superiores, no para el encabezado IP o algunos encabezados de extensión que preceden el encabezado ESP. En el caso de AH, la protección se extiende a porciones seleccionadas de los encabezados de extensión, opciones seleccionadas de encabezado IPv4, el encabezado de extensión de IPv6 Hop by Hop o los encabezados de extensión de destino.

Una *Asociación de Seguridad en Modo Túnel*, es esencialmente una AS aplicada a un túnel IP; si el destino de una AS es una gateway de seguridad, la AS debe ser modo túnel. Así, una AS entre dos gateways de seguridad es siempre una AS en modo túnel, como lo es una AS entre un host y una gateway de seguridad. Para una AS en modo túnel, hay un encabezado IP externo que especifica el destino del proceso IPSec, más un encabezado IP interno que especifica el destino final del paquete. El encabezado del protocolo de seguridad aparece después del encabezado IP externo y antes del encabezado IP interno; si se utiliza AH en modo túnel, permite que partes del encabezado IP externo sean protegidas, al igual que todo el paquete IP original; si se emplea ESP, la protección se aplica solo al paquete entunelado, no al encabezado externo.

En general:
a) Un host debe soportar tanto modo transporte como modo túnel.
b) Se requiere que una gateway de seguridad soporte solo modo túnel; si esta maneja modo transporte, este solo debe usarse solo en los casos en los cuales la gateway está trabajando como un host, por ejemplo, en gestión de redes.

A continuación (Tabla 3.2) se presenta un cuadro comparativo de las funciones de encapsulamiento que llevan a cabo los dos protocolos que implementa IPSec, según el modo de operación:

Tabla 3.2 Comparación entre AH y ESP

	Modo Transporte	Modo Túnel
AH	Autentica la carga útil y selecciona porciones del encabezado IP y de los encabezados de extensión de IPv6.	Autentica el paquete IP original completo (encabezado más carga útil), más porciones seleccionadas del encabezado IP exterior y los encabezados de extensión IPv6.
ESP	Encripta la carga útil y cualquiera de los encabezados de extensión IPv6 que sigan al encabezado ESP.	Encripta todo el paquete IP original.
ESP con autenticación	Encripta la carga útil y cualquiera de los encabezados de extensión IPv6 que sigan al encabezado ESP. Autentica la carga útil, pero no el encabezado IP.	Encripta todo el paquete IP original. Autentica todo el paquete IP original.

Como ya se explicó, los datagramas IP transmitidos sobre una AS individual permiten la protección con exactamente un protocolo de seguridad, AH o ESP, pero no con ambos. Algunas veces las políticas de seguridad pueden solicitar una combinación de servicios, para un flujo de tráfico particular, que no se puede conseguir con una única AS. En estos casos será necesario emplear múltiples AS para implementar la política de seguridad requerida. Se aplica el termino *"SA bundle"* (haz o manojo de Asociaciones de Seguridad) a una secuencia de Asociaciones de Seguridad a través de la cual se debe procesar el tráfico para satisfacer la política de seguridad. Las asociaciones de seguridad pueden estar combinadas en "SA bundles" de dos formas:

- *Transporte adyacente:* se aplica más de un protocolo de seguridad sobre el mismo datagrama IP, sin utilizar entunelado. Esta combinación de AH y ESP permite sólo un nivel de combinación.

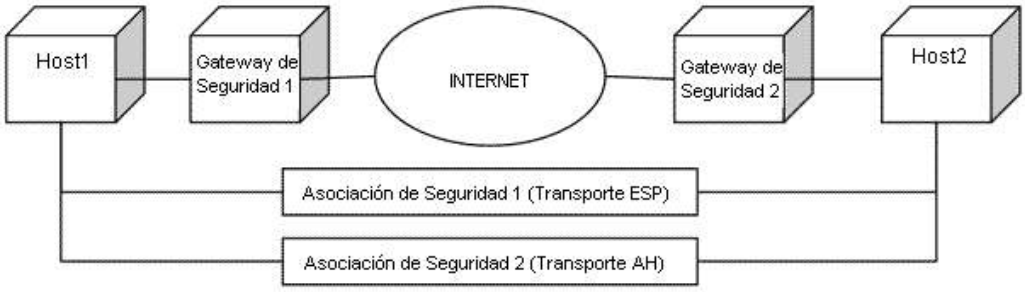


Figura 3.5 Transporte Adyacente

- *Entunelado iterado:* se refiere a la aplicación o al uso de múltiples capas de protocolos de seguridad a través de entunelado IP. Esta combinación permite múltiples niveles de anidamiento. Cada túnel se puede originar o terminar en nodos diferentes a lo largo de la ruta. Hay tres tipos básicos de entunelado iterado:

1. Ambas terminaciones de la AS son las mismas. Cualquiera de los túneles (interno o externo) puede hacerse con AH o ESP.

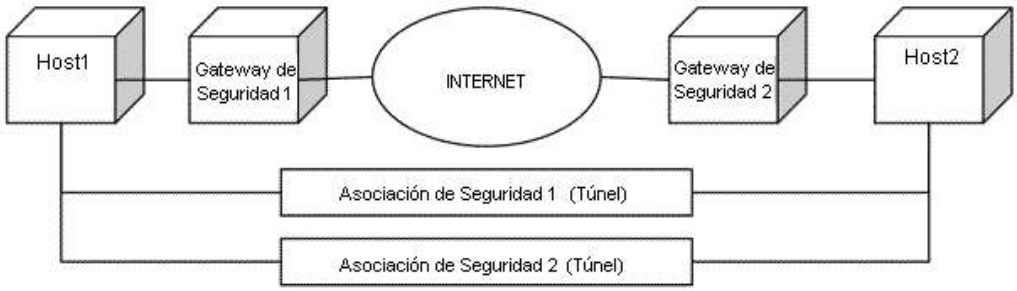


Figura 3.6 Entunelado Iterado con la misma terminación

2. Una terminación de la AS es la misma. Cualquiera de los túneles (interno o externo) puede hacerse con AH o ESP.

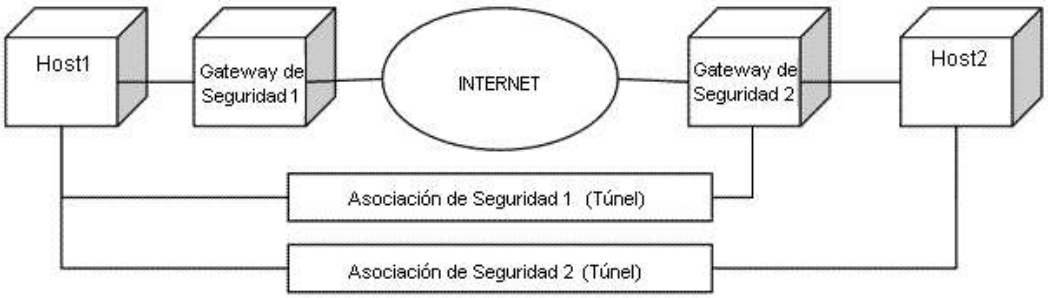


Figura 3.7 Entunelado Iterado donde una terminación no es la misma

3. Ninguna de las terminaciones es la misma.

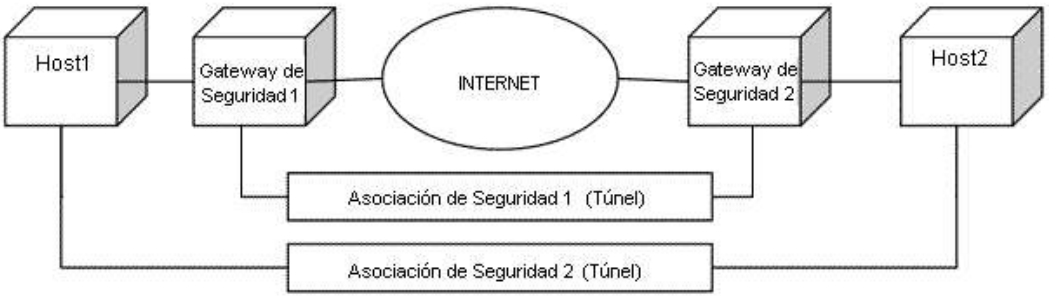


Figura 3.8 Entunelado Iterado con diferentes terminaciones

3.1.2.2 Bases de Datos de Seguridad

IPSec trabaja con dos bases de datos de seguridad:

- *Security Association DataBase*, Base de datos de Asociaciones de Seguridad (SAD).
- *Security Policy Database*, Base de datos de Políticas de Seguridad (SPD).

➢ *Base de Datos de Asociaciones de Seguridad (SAD)*

Esta Base de Datos es la que almacena todos los parámetros pertenecientes a una Asociación de Seguridad; cada AS tiene una entrada en la SAD donde se especifican todos los parámetros necesarios para que IPSec pueda realizar un procesamiento óptimo de los paquetes IP que son administrados por esa AS. Los siguientes campos son usados para el procesamiento de IPSec:

- Dirección IP de origen y destino de la AS.
- Contador del número de Secuencia: valor de 32 bits usado para generar el campo de número de secuencia en los encabezados AH y ESP.
- Contador de secuencia de desborde: una bandera que indica si hay un desbordamiento del número de secuencia para prevenir la transmisión adicional de paquetes en la AS.
- El Índice de Parámetro de Seguridad (SPI).
- Ventana antirrepetición: un contador de 32 bits y un mapa de bits para determinar si un paquete AH o ESP entrante está repetido.
- El protocolo a ser usado por la AS (AH o ESP).
- El modo en el que el protocolo es operado (transporte o túnel).
- Algoritmo de Autenticación de AH y las llaves asociadas.
- Algoritmo de Encriptación de ESP y las llaves asociadas.
- Algoritmo de Autenticación de ESP y las llaves asociadas (si no se utiliza autenticación con ESP, este campo será nulo).
- Tiempo de vide de las llaves de autenticación y de cifrado.
- Tiempo de Vida de la Asociación de Seguridad: intervalo de tiempo después del cual la AS debe ser reemplazada por una nueva AS y un nuevo SPI, o terminada.

Las Asociaciones de Seguridad sólo especifican cómo se supone que IPSec protegerá el tráfico. Para definir qué tráfico proteger, y cuándo hacerlo, se necesita información adicional. Esta información se almacena en las *Políticas de Seguridad* (SP-Security Policy), que a su vez se almacenan en las *Bases de Datos de Políticas de Seguridad* (SPD-Security Policy Database).

Una *Política de Seguridad* suele especificar los siguientes parámetros:

- Direcciones de origen y destino de los paquetes por proteger. En Modo Transporte estas serán las mismas direcciones que en la AS. En modo túnel pueden ser distintas.
- Protocolos y puertos a proteger. Algunas implementaciones no permiten la definición de protocolos específicos a proteger. En este caso, se protege todo el tráfico entre las direcciones IP indicadas.

- La Asociación de Seguridad a emplear para proteger los paquetes.

  - *Base de datos de Políticas de Seguridad (SPD)*

Una base de datos de Políticas de Seguridad es una lista ordenada de políticas de seguridad que deben ser aplicadas a los paquetes IP. Estas políticas son en general reglas que especifican como deben ser procesados los paquetes tanto entrantes como salientes. Además en éstas se especifica qué servicios van a ser aplicados a los datagramas IP y en qué momento. Esta base de datos es consultada durante el procesamiento de todo el tráfico entrante y saliente, incluyendo tráfico NO IPSec; es por esto que la SPD requiere distintas entradas para el tráfico entrante y saliente, además que deben haber SPDs separadas para cada interfaz IPSec habilitada. Además, una SPD debe discriminar entre el tráfico al cual debe aplicar protección IPSec y el tráfico al cual debe permitir el paso sin protección. Para cualquier paquete IP entrante o saliente se manejan 3 acciones posibles; la primera, *Descartar el paquete*, implica no permitir que el tráfico no IPSec salga del host y llegue a la gateway de seguridad, de igual forma como lo haría un Firewall. La segunda acción, *No aplicar IPSec*, se refiere al tráfico al cual debe permitírsele el paso sin protección IPSec. La tercera acción, *Aplicar IPSec*, se refiere al tráfico al cual debe aplicársele protección, y para cada uno, la SPD debe especificar los servicios de seguridad a ser aplicados, protocolos a ser empleados, algoritmos a ser usados, etc.

Cuando un paquete llega a una interfaz de red, IPSec busca primero en la SAD la apropiada Asociación de Seguridad; cuando la identifica, el sistema inicia los procesos SAD y SPD. Después de éste procesamiento, el sistema reenvía el paquete al siguiente salto o si es el caso, le aplica procedimientos adicionales, como las reglas de algún Firewall. El procesamiento SPD se realiza primero en paquetes salientes: si la entrada SPD especifica que un procesamiento IPSec es necesario, se consulta la SAD para determinar si se ha establecido una AS; en caso de que no haya una AS predefinida, se hace una negociación de una nueva AS para el paquete.

Debido a que los procesos de consulta de las Bases de Datos de Políticas de Seguridad se realizan tanto para los paquetes entrantes como salientes, este procedimiento altera de manera significativa y negativa el desempeño de los dispositivos IPSec; en la práctica, este procesamiento es el cuello de botella más representativo en una implementación IPSec.

3.1.3 Fortalezas y Debilidades de IPSec

Entre las ventajas más sobresalientes de IPSec se destacan que está apoyado en estándares del IETF y que proporciona un nivel de seguridad común y homogéneo para todas las aplicaciones, además de ser independiente de la tecnología física empleada. IPSec se integra en la versión actual de IP, y lo que es todavía más importante, se incluye por defecto en IPv6; puesto que la seguridad es un requisito indispensable para el desarrollo de las redes IP, IPSec está recibiendo un apoyo considerable: todos los equipos de comunicaciones lo incorporan, así como las últimas versiones de los sistemas operativos más comunes. Al mismo tiempo, ya existen muchas experiencias que demuestran la interoperabilidad entre fabricantes, lo cual constituye una garantía para los usuarios.

Otra característica destacable de IPSec es su carácter de estándar abierto. Se complementa perfectamente con la tecnología PKI (Infraestructura de Llave Pública) y, aunque establece ciertos algoritmos comunes, por razones de interoperabilidad, permite integrar algoritmos criptográficos más robustos que pueden ser diseñados en un futuro. Entre los beneficios que aporta IPSec, cabe señalar que:

- Posibilita nuevas aplicaciones como el acceso seguro y transparente de un nodo IP remoto.
- Facilita el comercio electrónico de negocio a negocio, al proporcionar una infraestructura segura sobre la que realizar transacciones usando cualquier aplicación.
- Permite construir una red corporativa segura sobre redes públicas, eliminando la gestión y el coste de líneas dedicadas.
- Ofrece al teletrabajador el mismo nivel de confidencialidad que dispondría en la red local de su empresa, no siendo necesaria la limitación de acceso a la información sensible por problemas de privacidad en tránsito.

Es importante señalar que la palabra *seguro* no se refiere únicamente a la confidencialidad de la comunicación, sino también a la integridad de los datos, que para muchas compañías y entornos de negocio puede ser un requisito mucho más crítico que la confidencialidad. Esta integridad es proporcionada por IPSec como servicio añadido al cifrado de datos o como servicio independiente.

Cuando se implementa IPSec en un *router*, éste provee una fuerte seguridad que puede ser aplicada a todo el tráfico que cruza el perímetro servido por el *router*. Por otro lado, IPSec está debajo de la capa *de transporte* (TCP, UDP), por lo que resulta "transparente" para las aplicaciones; no hay necesidad de cambiarlas, ni desde el punto de vista del usuario ni del servidor cuando IPSec se incorpora al *router* o al *Firewall*. También se tiene que IPSec puede ser "transparente" a los usuarios finales: como una política general, puede asumirse que no es necesario involucrar a los usuarios en los mecanismos de seguridad. Finalmente, IPSec tiene la capacidad de ofrecer seguridad individual si ésta fuese indispensable; tal característica es útil para empleados que accedan a la red desde el exterior vía telefónica. Además, es posible asegurar una subred virtual dentro de una organización para aplicaciones sensibles.

En resumen, entre los beneficios de IPSec se tiene: herencia de niveles de seguridad, de *routers* a subredes, transparencia respecto a las aplicaciones, transparencia respecto a usuarios finales, y ofrecimiento de seguridad a nivel individual. Además, IPSec ofrece servicios de seguridad en la capa de IP habilitando un sistema para seleccionar protocolos de seguridad necesarios, determinar algoritmos a utilizar en los servicios y colocar en cualquier lugar las llaves criptográficas requeridas para cumplir con los servicios solicitados. De esta forma, IPSec se convierte en una buena solución a la hora de combatir problemas de inseguridad. Sin embargo, las herramientas que implementan el estándar IPSec en redes IPv4 se encuentran aún en estado de desarrollo, por lo que aun presenta ciertas debilidades; la principal vulnerabilidad descubierta recientemente se presenta en paquetes IPSec a los cuales solo se aplica cifrado y no se verifica la integridad de los datos por medio de autenticación; un atacante podría modificar cuidadosamente una porción seleccionada de la carga útil del paquete, de manera que cuando éste llega a la gateway de seguridad receptora o al host de destino y es procesado por el software IP, se puede obtener un mensaje de error ICMP (Internet Control Message Protocol); debido a su diseño, este protocolo envía los primeros 64 bytes del paquete modificado sin cifrar, en un mensaje de error para indicar al origen la

causa del problema; de esa forma el atacante puede interceptar la comunicación y podría tener acceso a parte de la información que iba cifrada. La mejor forma de evitar este ataque es configurar adecuadamente las políticas de seguridad adicionando a la comunicación autenticación y cifrado para garantizar la integridad y confidencialidad de los datos, por lo que no se convierte en un problema sin solución.

3.2 AUTHENTICATION HEADER (AH) EN IPv4 E IPv6

El Encabezado de Autenticación de IPSec (*Authentication Header* - AH), es un mecanismo que provee las funciones de una integridad fuerte de los datos y de autenticación de los mismos; la *integridad* garantiza que el datagrama no sea alterado en forma inesperada o maliciosa, y la *autenticación* verifica el origen del datagrama (nodo, usuario, red, etc). AH por sí solo no acepta toda forma de encriptación, por lo cual no puede proteger la confidencialidad de los datos enviados sobre Internet. AH está orientado a mejorar la seguridad de Internet global en situaciones donde importar, exportar o usar encriptación puede ser ilegal o estar restringido por disposiciones de gobiernos locales. AH está libre de tales complicaciones, razón por la cual ofrece el servicio de autenticación de paquetes IP, con lo que se reduce la frecuencia de ataques basados en *IP spoofing*. AH asume la forma de un encabezado colocado entre el encabezado de IPv4 o IPv6 y la siguiente trama del protocolo de la capa más alta, tales como TCP, UDP, ICMP, etc. La implementación de AH en IPv4 es opcional; en cambio, la implementación de AH en IPv6 es obligatoria y el datagrama es más complejo.

Para *Modo Transporte (Figura 3.9)*, la cabecera básica del paquete IP original se conserva como la cabecera del nuevo paquete IP y la cabecera de autenticación se inserta entre la cabecera IP y la carga útil original; el ICV o Integrity Check Value (Valor de Chequeo de Integridad) se calcula sobre la totalidad del nuevo paquete IP, así:

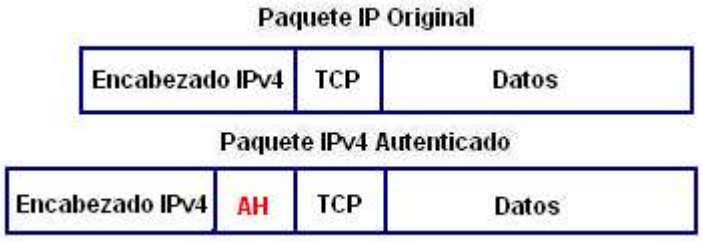


Figura 3.9 Trama IPv4 con AH en Modo Transporte

En IPv6, AH aparece después de los encabezados procesados en cada salto (*hop by hop)*, y antes de los encabezados procesados sólo en el destino final (end to end). El siguiente diagrama (Figura 3.10) muestra la posición de AH en el datagrama IPv6 para Modo Transporte:

Figura 3.10 Trama IPv6 con AH en Modo Transporte

La mayor ventaja para el Modo Transporte es que solo adiciona unos pocos bytes extra al paquete original; sin embargo, debido a que se tiene la misma cabecera original en el nuevo paquete autenticado, solo puede ser utilizado por hosts finales. Esta es una gran limitación cuando los dispositivos que están administrados por esta Asociación de Seguridad actúan como gateways de otros hosts que están detrás de ellos.

Por el contrario, en el *Modo Túnel* se crea una nueva cabecera para el nuevo paquete IP y la cabecera de autenticación se inserta entre la cabecera nueva y la original, tanto en IPv4 como en IPv6 (Figura 3.11, 3.12), así:

Figura 3.11 Trama IPv4 con AH en Modo Túnel

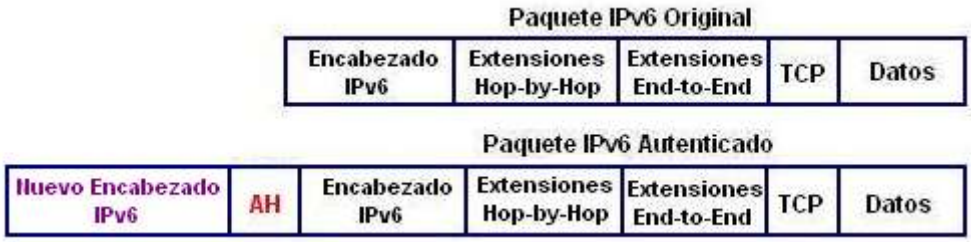


Figura 3.12 Trama IPv6 con AH en Modo Túnel

De esta forma el paquete IP original permanece intacto y se encapsula dentro del nuevo paquete; así se autentica el paquete original completo. La cabecera original permanece totalmente inalterada y contiene las direcciones IP tanto del origen como del destino de los datos originales; la nueva cabecera contiene la dirección IP del origen y del destino de los dispositivos IPSec entre los que viaja el nuevo paquete. De esta forma, el modo Túnel puede usarse tanto entre hosts o entre gateways de seguridad, o entre un host y una

gateway. Su mayor desventaja es que adiciona más bytes extra por lo que el desempeño del enlace y de los dispositivos disminuye por el doble procesamiento de cabecera que se necesita.

La IANA, Autoridad Internet para asignación de Números (*Internet Assigned Numbers Authority*) ha asignado el número de protocolo 51 a AH. Por tanto, el encabezado IP inmediatamente precedente al encabezado de AH debe contener el valor 51 en el campo *Next Header* para IPv6 o en el campo *Next Protocol* en IPv4. AH ofrece mecanismos de integridad y autenticación realizando un cálculo de compendio de mensajes (*message digest calculation*) sobre el datagrama IP completo. Un *compendio de mensaje* es una transformación matemática especial, de un solo sentido, que crea una huella digital única del datagrama, representándolo así mediante un solo número mucho más pequeño. El resultado del algoritmo de compendio de mensaje se coloca en el campo *Datos de Autenticación* del encabezado AH. El formato completo se muestra en la figura 3.13.

La cabecera AH mide 24 bytes, de la siguiente forma: el primer byte es el campo *Siguiente cabecera*; este campo especifica el protocolo de la siguiente cabecera; en Modo Túnel se encapsula un datagrama IP completo, por lo que el valor de este campo es 4; al encapsular un datagrama TCP en Modo Transporte, el valor correspondiente es 6. El siguiente byte especifica la *longitud del contenido del paquete*; este campo está seguido de dos bytes reservados. Los siguientes 4 bytes especifican el *Índice de Parámetros de Seguridad* (Security Parameters Index - SPI); el SPI, junto a la dirección IP de destino y el tipo de protocolo IPSec, especifica la Asociación de Seguridad (AS) a emplear para desencapsular el paquete. El *Número de Secuencia* de 32 bits protege el datagrama frente a ataques por repetición: comienza en 0 cuando se establece la AS y se incrementa por cada paquete saliente que utiliza esta AS. Finalmente, los últimos 96 bits, el *campo de Autenticación*, almacenan el Valor de Chequeo de Integridad (Integrity Check Value - ICV) del paquete; éste se calcula con el algoritmo seleccionado en la AS y es utilizado por el receptor para verificar la integridad del paquete entrante; los algoritmos por defecto requeridos por AH para trabajar son HMAC (*Hashed Message Authentication Code)* con MD5 (Message Digest version 5) y SHA-1 (Secure Hash Algorithm 1). El ICV es un valor Hash (o Valor Resumen, algoritmo de cifrado que convierte un mensaje de cualquier longitud en una sola cadena de dígitos) computado sobre todos los campos que incluye la autenticación; la llave secreta es negociada durante el establecimiento de la AS. La autenticación de un datagrama recibido se verifica cuando el receptor calcula el valor Hash y lo compara con el ICV del paquete entrante; si el paquete no se autentica exitosamente, es descartado.

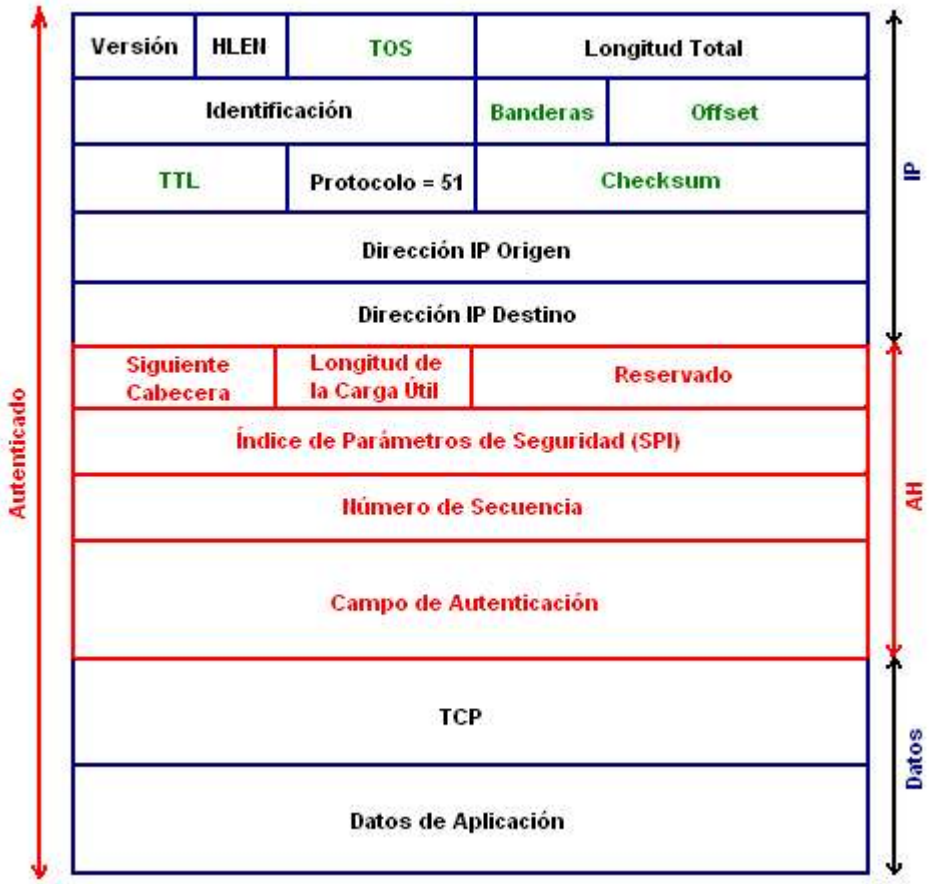


Figura 3.13 Formato del Encabezado de Autenticación AH

Como el protocolo AH protege la cabecera IP incluyendo sus partes inmutables como las direcciones IP, no permite NAT. La *Traducción de direcciones de red* (Network addresses translation-NAT, también conocido como Enmascaramiento de direcciones) reemplaza una dirección IP de la cabecera (normalmente la IP de origen), por una dirección IP diferente. Tras el intercambio, el cálculo del ICV ya no es válido. La extensión a IPSec NAT-transversal implementa métodos que evitan esta restricción. El protocolo AH se ha diseñado pretendiendo que funcione con diversos algoritmos de autenticación, tanto con aquellos ya existentes como con los que han de desarrollarse en un futuro. El documento IPSec DOI asigna un número único para cada algoritmo de autenticación, el cual sirve como identificador durante el proceso de negociación entre sistemas que se están comunicando. Se han definido dos algoritmos para autenticación y son considerados obligatorios de acuerdo con el estándar de IPSec: HMAC-MD5 (*Hashed Message Authentication Code - Message Digest version 5*) y HMAC- SHA1 (*Hashed Message Authentication Code - Secure Hash version 1*).

3.2.1 HMAC-MD5

El algoritmo MD5 (Message Digest version 5) es una función matemática de un solo sentido; aplicado a un bloque de datos, éste produce su representación única de 128 bits; el resultado obtenido es una representación comprimida o codificada de un bloque más grande de datos. Cuando se usa de esta manera, MD5 garantiza sólo la integridad en los datos. Un mensaje codificado ha de ser sometido a un proceso de cálculo partiendo de un bloque de datos (como pueden ser datagramas IP) antes de que se envíe y otra vez después de que los datos hayan sido recibidos. Si los dos compendios calculados son iguales, entonces el bloque de datos no tuvo alteración alguna durante la transmisión (suponiendo que hubiese habido una transmisión maligna). El algoritmo MD5 se detalla en el *RFC 1321*. La autenticidad puede ser garantizada mediante el uso de llaves secretas cuando se calcula el mensaje codificado.
HMAC (Hashed Message Authentication Code) es un método especial. Fue diseñado por Hugo Krawczyk, Ran Canetti y Mihir Bellare. Es un método mejorado de manejo de llaves con funciones Hash, y brinda protección adicional a otros algoritmos, de tal forma que SHA (Secure Hash Algorithm) se convierte en HMAC-SHA, MD5 se convierte en HMAC-MD5. La construcción de HMAC es criptográficamente más fuerte que otras funciones hash. Por ejemplo, MD5 es susceptible a un ataque del tipo colisión, donde es posible encontrar dos entradas diferentes que produzcan el mismo compendio; HMAC-MD5 no es susceptible a este ataque. HMAC usa el algoritmo básico MD5 para calcular los mensajes codificados, pero opera en bloques de datos de 64 bytes que sirve, a su vez, como entrada de un bloque entero de datos. Este también usa una llave secreta (conocida sólo por los sistemas que se están comunicando) cuando se realiza el cálculo de la codificación. HMAC se describe en detalle en el *RFC 2104*.

En un sistema de intercambio de datagramas utilizando HMAC-MD5, el emisor previamente intercambiará la llave secreta, para calcular primero una serie de compendios MD5 de 16 bits por cada bloque de 64 bytes del datagrama. La serie de valores formados por los compendios de 16 bytes se concatenan en un solo valor, el cual es colocado en el campo *Datos de Autenticación* del encabezado AH. El datagrama se envía al receptor, quien debe también conocer el valor de la llave secreta para calcular el mensaje codificado correcto y compararlo con el mensaje codificado recibido por autenticación. Si los valores coinciden, ha de concluirse que el datagrama no fue alterado durante su tránsito por la red, y además, éste fue enviado sólo por otro sistema compartiendo el conocimiento de la llave secreta. Hay que hacer notar que la utilidad de esta técnica se basa en la presunción de que sólo el verdadero emisor (y no un impostor) tiene conocimiento de la llave privada compartida.

3.2.2 HMAC-SHA1

SHA (Secure Hash Algorithm) es un algoritmo desarrollado por el NIST (National Standards and Technology Algorithm) que produce una firma de salida de 160 bits, a partir de bloques de 512 bits del mensaje original. El algoritmo SHA-1 fue desarrollado por la NSA (Agencia Nacional de Seguridad de los Estados Unidos) para ser incluido en el estándar DSS (Digital Signature Standard). Al contrario que los algoritmos de cifrado propuestos por esta organización, SHA-1 se considera seguro y libre de puertas traseras, ya que el hecho de que el algoritmo sea realmente seguro favorece a los propios intereses de la NSA. Este algoritmo es similar a MD5, con la diferencia de que usa la ordenación *big hendian,* lo cual significa que el primer byte es el *más* significativo; se inicializa de igual manera, es decir, añadiendo al final del mensaje un uno seguido de tantos ceros como sea necesario hasta completar 448 bits en el último bloque, para luego yuxtaponer la longitud en bits del propio mensaje (en este caso, el primer byte de la secuencia será el más significativo).

3.3 ENCAPSULATING SECURITY PAYLOAD (ESP) EN IPv4 E IPv6

El encabezado *Encapsulating Security Payload* (ESP) realiza funciones de integridad y confidencialidad de los datos por medio de cifrado. Como ya se ha mencionado, la integridad asegura que el datagrama no haya sido alterado en forma inesperada o maliciosa, y la confidencialidad asegura la privacidad de los datos usando técnicas criptográficas. Sin embargo, en una implementación de ESP puede elegirse si se quiere o no utilizar autenticación, ya que es opcional. La confidencialidad se logra por medio de técnicas de cifrado; los algoritmos de cifrado empleados se definen en la AS sobre la cual se envían los paquetes. El algoritmo de cifrado Null, en el cual no se aplica cifrado también es válido. En este caso, ESP solo prestaría el servicio de autenticación del tráfico.

El protocolo ESP, como AH, se diseñó para trabajar en dos modos: *Túnel* y *Transporte*. En Modo Transporte, la cabecera ESP se inserta entre la cabecera básica IP y la carga útil original (Figura 3.14); al igual que en AH, este modo solo puede ser utilizado entre hosts debido a que la cabecera original permanece idéntica. El nuevo paquete IP se muestra a continuación, identificando la parte del paquete que puede ser cifrada y la parte del paquete que puede ser autenticada:

Figura 3.14 Trama IPv6 con ESP en Modo Transporte

Se deben notar los dos tipos de encabezados opcionales mostrados en el formato. Los encabezados *Hop-by-Hop* son procesados por sistemas intermedios (como *routers*) en cada salto, en tanto que los encabezados *End to End* son sólo procesados por el sistema final. La encriptación de ESP no debe interferir con ninguna parte de los encabezados IP necesarios para la entrega correcta del paquete. En IPv4 el encabezado ESP se ubica después del encabezado IP y del encabezado AH, cuando se utilizan de forma combinada (Figura 3.15):

Figura 3.15 Trama IPv4 con AH y ESP en modo Transporte

En Modo Túnel, un datagrama completo es encapsulado y encriptado dentro de un nuevo paquete IP. Se aumenta una nueva cabecera al paquete y el encabezado ESP; cuando se hace esto, las direcciones verdaderas IP, origen y destino, pueden ser ocultas como un simple dato transitando en Internet. Un uso típico de este modo es cuando se esconde un servidor o una topología durante una conexión *firewall-to-firewall* sobre una Red Privada Virtual (Virtual Private Network - VPN); si el túnel se establece entre hosts, las direcciones de origen y destino de la nueva cabecera pueden ser las mismas que en la original. Si el túnel se establece entre gateways de seguridad, las direcciones de la nueva cabecera IP serán las direcciones de las gateways. De esta forma se logra tanto confidencialidad como autenticación del tráfico entre las dos gateways (Figura 3.16, 3.17).

Figura 3.16 Trama IPv6 con ESP en modo Túnel

Figura 3.17 Trama IPv4 con ESP en Modo Túnel

IANA ha designado el número de protocolo 50 para ESP. Esto significa que el encabezado IP inmediatamente precedente al encabezado ESP debe contener el valor de 50 en el campo *Next_Header* (en IPv6) o en el campo *Next_Protocol* (en IPv4). El formato del encabezado ESP se muestra a en la Figura 3.18.

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

IPSec emplea cifradores de bloque para el proceso de cifrado. Por ello, puede ser necesario rellenar la carga del paquete si la longitud de la carga no es un múltiplo de la longitud del paquete; en ese caso se añade la longitud del relleno (pad length). Tras la longitud del relleno se coloca el campo de 2 bytes, *Siguiente cabecera* que especifica la siguiente cabecera. Por último, se añaden los 96 bit de HMAC para asegurar la integridad del paquete; esta HMAC sólo tiene en cuenta la carga del paquete: la cabecera IP no se incluye dentro de su proceso de cálculo. El uso de NAT, por lo tanto, no rompe el protocolo ESP; sin embargo, en la mayoría de los casos, NAT aún no es compatible en combinación con IPsec. NAT-Transversal ofrece una solución para este problema encapsulando los paquetes ESP dentro de paquetes UDP.

El protocolo ESP tiene un diseño flexible que le permite trabajar con diferentes algoritmos de encriptación (también nombradas *transformadas*). IPSec requiere de un algoritmo común por omisión. La *transformada DES-CBC*, puede ser usada en todas las implementaciones de ESP. Sin embargo, dos o más sistemas estableciendo una sesión IPSec pueden negociar el uso de una transformada alternativa. El documento *IPSec DOI* presenta una lista opcional de transformadas ESP. Aquí, entre los algoritmos opcionales están: Triple-DES, RC5, IDEA, BLOWFISH y RC4.

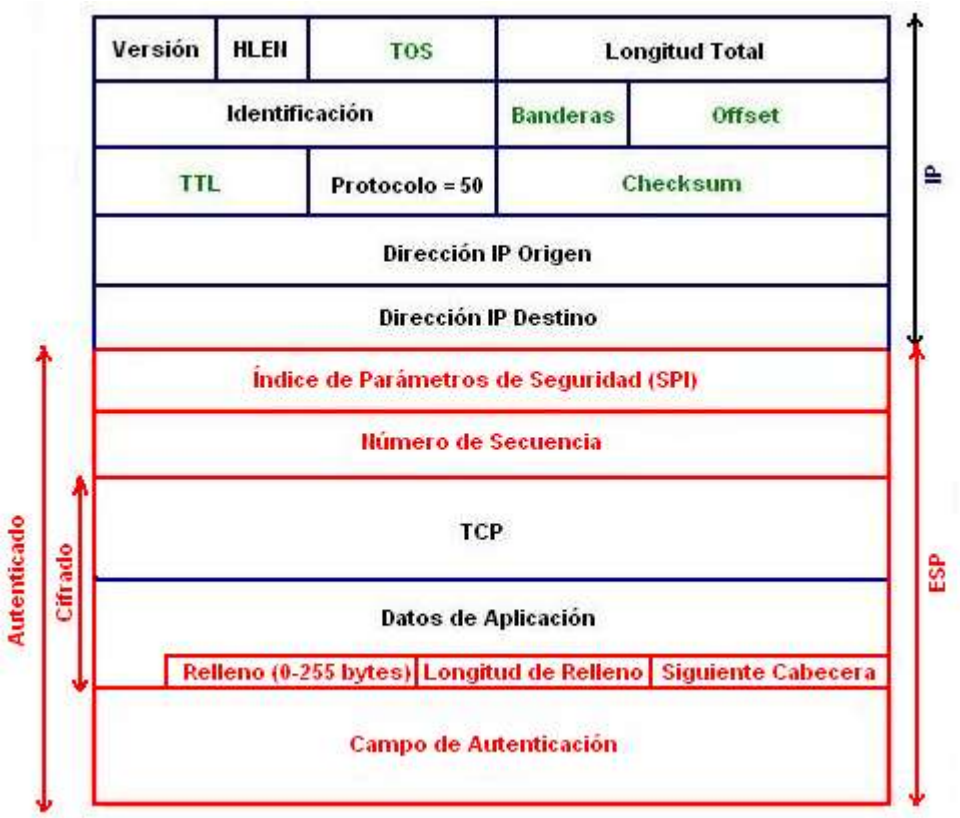


Figura 3.18 Formato del encabezado ESP

3.3.1 Transformada DES-CBC

DES (*Data Encryption Standard*) es un algoritmo de encriptación muy común. Publicado primero en 1977 por el Gobierno de los Estados Unidos de América, se usó para aplicaciones comerciales "no clasificadas". Hoy día todas las patentes han expirado, y existen implementaciones gratuitas disponibles en el mundo. El estándar de IPSec para ESP requiere que todas las implementaciones realicen DES en modo CBC (*Cipher Block Chaining*) como transformada por omisión. Sin embargo, su uso ciertamente no es obligatorio. Todo usuario u organización es libre de elegir otras transformadas de encriptación, o bien no usar encriptación alguna. Tal flexibilidad es particularmente importante dada la reglamentación, desde el punto de vista jurídico, existente en cada país acerca del uso y la exportación de criptografía doméstica.

DES-CBC, tal como se especifica para ESP, trabaja ejecutando una operación matemática sobre bloques de datos de 8 bytes que comprimen ya sea un datagrama completo (modo túnel) o la trama del protocolo de la siguiente capa superior (modo transporte). DES-CBC reemplaza bloques de 8 bytes de datos no encriptados (texto plano) con bloques de 8 bytes de datos encriptados (texto cifrado). Esta propiedad de transformación facilita las funciones de encriptar/desencriptar una ráfaga (*stream*) de datos. Un valor aleatorio, o *vector de inicialización* (IV) de 8 bytes se usa para cifrar el primer bloque del texto plano y asegurar así la aleatoriedad entre mensajes que pueden comenzar con la misma información de texto plano. La característica principal de encriptación de DES-CBC es

una llave idéntica secreta compartida entre las partes comunicantes: es, un *algoritmo criptográfico simétrico*. La llave usada por el emisor para encriptar los datos es la única llave que puede ser usada por el receptor para desencriptar los datos. Por tanto, el uso efectivo de DES-CBC para privacidad de datos depende de la misma llave secreta compartida entre las partes que se están comunicando, y, naturalmente, ha de ser protegida para no ser descubierta por los intrusos. La longitud de la llave especificada para DES-CBC usada dentro de ESP es de 56 bits.

3.4 INTERNET KEY EXCHANGE PROTOCOL – IKE

Una Asociación de Seguridad puede ser configurada manualmente por el administrador del sistema o puede ser negociada dinámicamente por medio de un protocolo de manejo de llaves como IKE. Este resuelve el problema más importante del establecimiento de comunicaciones seguras: la autenticación de los participantes y el intercambio de claves simétricas. Tras ello, crea las Asociaciones de Seguridad y rellena la SAD. Este tipo de negociación es muy importante debido a que en una comunicación de datos no es posible saber en qué momento debe establecerse una AS; además, por motivos de seguridad, las AS no pueden tener un tiempo de vida muy largo porque se expondrían a que algún atacante rompiera los códigos de seguridad. Con IKE, las AS se renegocian periódicamente actualizando así toda la información de seguridad.

Este protocolo funciona en dos fases: La primera fase establece una ISAKMP SA (*Internet Security Association Key Management Security Association - Asociación de seguridad del protocolo de gestión de claves de asociaciones de seguridad en Internet*) entre dos nodos, para acordar en la forma de proteger las comunicaciones que se establecerán entre ellos; una ISAKMP SA es bidireccional y no trabaja sobre el tráfico IPSec. En la segunda fase, el ISAKMP SA se emplea para negociar y establecer las AS de IPSec. Dado que el canal se ha asegurado en la primera fase, las negociaciones dentro de la segunda fase se desarrollan de una manera más sencilla; además, una misma ISAKMP SA se puede usar para negociar varias Asociaciones de Seguridad de IPSec, reduciendo así el número de negociaciones; este caso se presenta en comunicaciones LAN to LAN, donde una gateway de seguridad actúa como un nodo ISAKMP en nombre de los hosts que protege.

La autenticación de los participantes en la primera fase se basa en claves compartidas con anterioridad (Pre Shared Keys - PSK), claves RSA y certificados X.509. Además, la primera fase soporta dos modos distintos: *Modo Principal y Modo Agresivo*. Ambos modos autentican al participante en la comunicación y establecen un ISAKMP SA, pero el modo agresivo sólo usa la mitad de mensajes para alcanzar su objetivo. Esto, sin embargo, tiene sus desventajas, ya que el modo agresivo no soporta la protección de identidades y, por lo tanto, es susceptible a un ataque *man-in-the-middle* (por escucha y repetición de mensajes en un nodo intermedio) si se emplea junto a claves compartidas con anterioridad (PSK). Pero sin embargo este es el único objetivo del modo agresivo, ya que los mecanismos internos del modo principal no permiten el uso de distintas claves compartidas con anterioridad con participantes desconocidos. El modo agresivo no permite la protección de identidades y transmite la identidad del cliente en claro; por lo tanto, los participantes de la comunicación se conocen antes de que la autenticación se lleve a cabo, y se pueden emplear distintas claves pre-compartidas con distintos comunicantes.

En la segunda fase, el protocolo IKE intercambia propuestas de asociaciones de seguridad y negocia asociaciones de seguridad basándose en la ISAKMP SA. La ISAKMP SA proporciona autenticación para protegerse de ataques *man-in-the-middle*. Esta segunda fase emplea el modo rápido. Normalmente, dos participantes de la comunicación sólo negocian una ISAKMP SA, que se emplea para negociar varias (por lo menos dos) AS de IPSec unidireccionales.

La parte de administración de llaves de IPSec involucra la determinación y la administración de llaves secretas; un requisito usual es el uso de cuatro llaves para comunicación entre dos aplicaciones: se transmiten y se reciben pares de llaves tanto para AH como para ESP. Existen dos mecanismos para la administración de llaves:

- *Manual*: El administrador del sistema lo configura manualmente con sus propias llaves y con las llaves de otros sistemas con los que ha de comunicarse. Este método es práctico para un medio ambiente relativamente estático y pequeño.
- *Automático*: Se habilita la creación de llaves para un sistema en base a la demanda de AS y se facilita el uso de llaves en un gran sistema distribuido con una configuración creciente. El protocolo que administra automáticamente las llaves en IPSec se denomina *ISAKMP/Oakley.*

Las llaves se generan una vez se cuenta con los parámetros necesarios en los nodos ISAKMP; el algoritmo Diffie-Hellman es muy importante en la generación de llaves en IKE: éste permite que dos partes generen una llave secreta a partir de parámetros públicos, de tal forma que si alguien quisiera obtener la llave secreta interviniendo la comunicación, sería incapaz de hacerlo. La llave secreta que se genera en la fase 1 es llamada *ISAKMP Master Key* y la que se genera en la fase 2 es llamada *User Master Key*. Sin embargo, el protocolo Diffie-Hellman es vulnerable a ataques en los que alguien intercepta los mensajes que se intercambian y se hace pasar por uno de los nodos. Es por esto que en el intercambio IKE, las dos partes de la comunicación deben ser autenticadas.

Como solución a éste inconveniente se utiliza comúnmente el protocolo OAKLEY, el cual se basa en el esquema Diffie-Hellman, pero permite el intercambio de llaves de una manera segura entre las dos partes autenticadas previamente.

3.4.1 El protocolo ISAKMP

El protocolo *Internet Security Association and Key Management* (ISAKMP) se basa en el concepto central de una Asociación de Seguridad (AS); ésta última es un acuerdo de seguridad unidireccional entre los sistemas que se están comunicando que especifican qué tan segura es una conexión que será establecida. La AS contiene todos los parámetros necesarios para definir completamente el acuerdo de seguridad, tales como: autenticación, algoritmos de encriptación, longitudes de llaves y tiempo de vigencia de las llaves. Todos los parámetros de la AS son organizados dentro de una estructura llamada *Security Parameter Index* (SPI). Una AS es negociada para cada protocolo de seguridad utilizado entre los sistemas interconectados; de esta forma, dos sistemas pueden tener múltiples AS establecidas.

El establecimiento de la AS entre los sistemas se efectúa en dos fases: primero, una ISAKMP AS es negociada entre los sistemas (tales como dos servidores ISAKMP). El protocolo ISAKMP se utiliza para proteger el tráfico entre los sistemas durante la segunda fase de negociación de los protocolos de la AS. Este se diseñó para ofrecer seguridad en todas las capas del protocolo, no sólo en la capa de IP y de sus protocolos asociados AH y ESP. Sin embargo, también es posible para otros protocolos (SSL, TLS, OSPF, etc.) usar ISAKMP para establecer sus propias AS. Cada protocolo de seguridad o servicio usado por los sistemas que se comuniquen tendrá su propia AS y su correspondiente SPI. IANA ha asignado el puerto UDP 500 para uso del protocolo ISAKMP.

3.4.2 El protocolo OAKLEY

El establecer la primera fase de ISAKMP AS involucra el intercambio de llaves autenticadas en la comunicación de ambos sistemas para proteger el tráfico subsecuente y la negociación de los protocolos de seguridad. El protocolo *Oakley Key Determination* es un mecanismo usado para realizar este intercambio seguro. Oakley usa el algoritmo de intercambio de llaves de Diffie-Hellman (D-H), que es una técnica criptográfica de intercambio de llave pública 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. La norma de ISAKMP requiere que las llaves públicas usadas para establecer ISAKMP AS sean autenticadas mediante firmas digitales. ISAKMP no establece algoritmo alguno de firma en particular ni una *autoridad certificadora* (CA), más sin embargo, a instancias de las partes, permite a los sistemas indicar cuáles CA's se aceptarán. A través de la implementación de Oakley, ISAKMP tiene un mecanismo para la identificación de tipos de certificados, de CA's aceptadas y de intercambio de certificados entre sistemas. Una vez que las llaves públicas D-H son intercambiadas y autenticadas y de que una llave secreta haya sido generada, los sistemas que están comunicados pueden establecer una IPSec AS que caracteriza el uso de los protocolos de seguridad AH y ESP.

En el Anexo B se presenta una introducción a los conceptos fundamentales de la Criptografía y la Autenticación, para tener una idea de su funcionamiento, que está íntimamente ligado a la implementación de los Protocolos de IPSec estudiados en este capítulo.

En el Anexo C se describen las características más importantes de protocolos de seguridad a nivel de red como el PPTP (Point to Point Tunneling Protocol) y el L2TP (Layer 2 Tunneling Protocol), además de que se presentan otros protocolos de seguridad de niveles superiores, que también deben ser tenidos a la hora de pensar en una solución de seguridad a todo nivel.

Resumen

En este capítulo se realizó un estudio del Protocolo IPSec y sus protocolos de seguridad: AH y ESP, además del protocolo de Intercambio de Claves, IKE. Estos protocolos, aplicados a una red son una muy buena solución para varias de las vulnerabilidades estudiadas en el capítulo 2; sin embargo, no se pueden dejar de lado otra serie de mecanismos de seguridad, que se estudiarán en el capítulo siguiente.

CAPITULO IV. PRINCIPALES MECANISMOS DE SEGURIDAD EN REDES IP

4.1 FIREWALLS

Los Firewalls de red son dispositivos o sistemas que controlan el flujo de tráfico entre redes empleando diferentes mecanismos de seguridad. En la mayoría de aplicaciones modernas se habla de Firewalls en el contexto de conectividad de Internet. Sin embargo los Firewalls son aplicables en entornos de red que no incluyen o requieren conectividad a Internet. Por ejemplo muchas redes corporativas emplean Firewalls para restringir la conectividad de servicios y funciones sensibles hacia y desde redes internas. Gracias al empleo de Firewalls para controlar la conectividad a estas áreas, una organización puede prevenir el acceso no autorizado a determinados sistemas o recursos en las zonas más importantes. La inclusión de un Firewall adecuado puede proveer un nivel de seguridad que de otra manera no seria alcanzable.

Existen muchas plataformas de Firewall actualmente disponibles por muchos fabricantes. Una manera de comparar las características de estas plataformas es examinando los aspectos del Modelo para la Interconexión de Sistemas Abiertos (OSI). El modelo OSI consta de siete niveles: nivel físico, de enlace de datos, de red, de transporte, de sesión, de presentación y de aplicación. Los Firewalls modernos operan en los niveles dos, tres, cuatro y siete; los Firewalls más básicos operan en los niveles más bajos mientras que los más avanzados operan en la mayoría de niveles de la torre OSI; entre más niveles puedan analizar el Firewall, más efectivo se considera. Incrementar los niveles que un Firewall puede analizar, le permite prestar servicios tales como la autenticación de usuarios. Un Firewall que funciona en niveles dos y tres solamente no negocia con usuarios específicos mientras que un Firewall Proxy de aplicación puede reforzar la autenticación de los usuarios así como los eventos de login para usuarios específicos.

Independiente de la arquitectura del Firewall, estos pueden traer servicios adicionales como la Traducción de Direcciones de Red (NAT), Protocolo de Configuración Dinámica de Equipos (DHCP), funcionalidades de cifrado como las redes privadas virtuales (VPN) y filtrado de contenido de aplicación.

4.1.1 Firewalls de Filtrado de Paquetes

La funcionalidad básica de cualquier Firewall es la de filtrar paquetes; por eso los Firewalls más sencillos son llamados filtros de paquetes. Estos Firewalls son dispositivos de enrutamiento que incluyen funcionalidad de control de acceso para direcciones de equipos y sesiones de comunicación. El control de acceso se realiza utilizando un conjunto de directivas que colectivamente forman

una regla. En la forma más básica un filtro de paquetes opera en los niveles de red y transporte para proveer acceso basado en partes del paquete de red como:

- Dirección de origen
- Dirección de destino
- Tipo de tráfico
- Puerto TCP de origen
- Puerto TCP de destino

Los Firewalls de filtrado de paquetes, así como los enrutadores, pueden filtrar tráfico de red basados en ciertas características del tráfico, como por ejemplo: si el paquete es un ICMP, los atacantes pueden usar este protocolo para inundar redes de tráfico creando ataques de denegación de servicio distribuida. Así como éste, los Firewalls de filtrado de paquetes tienen la capacidad para bloquear otros tipos de ataques que se aprovechan de las debilidades de la pila TCP/IP. Los Firewalls de filtrado de paquetes tienen dos fortalezas, velocidad y flexibilidad. Aunque estos dispositivos usualmente no examinan datos que se encuentran por encima del nivel tres, operan muy cerca.

4.1.1.1 Debilidades Básicas Asociadas con Filtro de Paquetes

- Debido a que no examinan datos de niveles superiores, no pueden prevenir ataques que emplean vulnerabilidades específicas de aplicaciones.
- Debido a la limitada información que se le da al Firewall, la funcionalidad de registro de logs es limitada. Los logs normalmente contienen la misma información utilizada para tomar las decisiones de control de acceso.
- La mayoría de filtros de paquetes no soportan esquemas de autenticación avanzados.
- Generalmente son vulnerables a ataques y exploits que se aprovechan de problemas en la especificación del protocolo TCP/IP tales como la suplantación de direcciones de red. La mayoría de Firewalls de filtrado de paquetes no pueden detectar paquetes en los cuales la información de direccionamiento ha sido alterada.
- Debido a las pocas variables que se manejan en las decisiones de control de acceso, es probable que se creen brechas de seguridad por configuraciones inapropiadas. Es fácil que accidentalmente se permita tráfico que debería estar restringido de acuerdo a las políticas de seguridad.

En conclusión los Firewall de filtrado de paquetes se adaptan bien a entornos de alta velocidad, donde tener logs y autenticación de usuarios no son aspectos importantes.

4.1.1.2 Reglas de Filtrado

Una regla es una serie de condiciones que son establecidas para examinar cada paquete con cada regla; si un paquete coincide con todas las condiciones de la regla, el paquete es rechazado o aceptado según la regla; si no coincide con la regla evaluada, pasa a evaluar la siguiente, si no coincide con ninguna de las reglas establecidas se ejecuta la regla por defecto que generalmente es rechazar el paquete. Cuando se coincide con todas las condiciones de una regla se toma una de las siguientes acciones:

- Aceptar: el paquete pasa a través del Firewall.
- Denegar: el paquete es rechazado, no pasa a través del Firewall, una vez es rechazado envía un mensaje de error al origen del paquete.
- Descartar: el paquete es rechazado, pero no se envía mensaje de error al origen del paquete, en este caso el Firewall no revela su presencia a las redes externas.

Para ilustrar mejor la configuración y el resultado de las reglas de filtrado, la tabla 4.1 muestra algunas de ellas. La primera regla es usada para permitir paquetes que retornan desde sistemas externos a la Intranet 172.16.0.0, para completar conexiones como conexiones TCP. La segunda rechaza paquetes que tengan como dirección de origen la dirección del Firewall, debido a que atacantes pueden suplantar la dirección del Firewall con la intención de realizar ataques para que la victima acepte los paquetes que creen venir del Firewall. La tercera previene accesos externos al Firewall.

La regla número cuatro permite que las máquinas internas inicien conexiones en servidores externos en cualquier puerto, esto puede restringirse a que solo puedan iniciar conexiones solo en los puertos privilegiados que es donde se encuentran la mayoría de los servicios más usados. La quinta y sexta regla permiten el paso de datos SMTP y HTTP. La última regla es tal vez la más importante ya que bloquea cualquier otro paquete desde el exterior hacia la Intranet, aunque esta regla especifica que cualquier paquete no importa su origen ni destino será denegado, las regla anteriores cumplen con una serie de condiciones que hacen que no se restrinja todo tipo de tráfico. Si esta regla fuera omitida accidentalmente o colocada antes de otras que fueran más especificas, todo el tráfico desde el exterior ingresaría a la red interna. Por este motivo siempre deben colocarse las reglas más específicas antes de las reglas más generales para evitar posibles errores lógicos que hagan que nunca sean evaluadas reglas de gran importancia.

Tabla 4.1 Ejemplo de reglas de filtrado

Dirección de Origen	Puerto de Origen	Dirección de Destino	Puerto de Destino	Acción	Descripción
Cualquiera	Cualquiera	172.16.0.0	> 1023	Aceptar	Regla para permitir el retorno de conexiones TCP hacia la Intranet
172.16.255.190	Cualquiera	Cualquiera	Cualquiera	Denegar	Previene que desde el Firewall se pueda conectar a cualquier parte. Esta regla no permite acceso remoto al Firewall dejándolo restringido a acceso local
Cualquiera	Cualquiera	172.16.255.190	Cualquiera	Denegar	Previene acceso externo al Firewall
172.16.0.0	Cualquiera	Cualquiera	Cualquiera	Aceptar	Usuarios internos pueden acceder servidores externos.

Cualquiera	Cualquiera	172.16.255.130	SMTP(25)	Aceptar	Permite a usuarios externos enviar e-mail a través del servidor de correo (172.16.255.130)
Cualquiera	Cualquiera	172.16.255.137	HTTP(80)	Aceptar	Permite acceso externo al servidor Web.
Cualquiera	Cualquiera	Cualquiera	Cualquiera	Denegar	Regla por defecto, todo paquete que no coincidió con las reglas anteriores es rechazado.

Con la información de las reglas del Firewall pueden deducirse fácilmente las políticas de seguridad perimetral de la red:

- Se permite cualquier tipo de acceso desde la Intranet hacia el exterior.
- No se permite acceso desde el exterior hacia la Intranet a excepción de los servicios de SMTP y HTTP.
- Los servidores de correo y Web están ubicados detrás del Firewall.

4.1.2 Firewalls con Inspección de Estado

Estos Firewalls son filtros de paquetes que analizan el funcionamiento del nivel cuatro (transporte) del modelo OSI. Los Firewalls con estado evolucionaron de la necesidad de acomodar ciertas características del protocolo TCP/IP que hacían que la implementación del Firewall fuera compleja. Cuando una aplicación TCP (protocolo orientado a conexión) crea una sesión con un equipo remoto, también se crea un puerto en el origen para la recepción de tráfico proveniente del destino. De acuerdo a las especificaciones de TCP cuando se establece una conexión de este tipo, el puerto origen usado por el cliente debe ser un número mayor a 1023 y menor a 16384 y que el puerto de destino del equipo remoto sea menor que 1024 como por ejemplo el puerto 25 de SMTP (Protocolo de transporte de correo simple).

Los Firewall filtros de paquetes deben permitir el tráfico de entrada en todos los puertos no privilegiados para transporte de datos orientados a conexión como ocurre cuando retornan paquetes desde servidores externos. La apertura de tantos puertos crea un gran riesgo de intrusión por usuarios no autorizados.

En la tabla 4.1 se muestran ejemplos de reglas; la primera permite el tráfico desde el exterior a cualquier dirección interna y hacia cualquier puerto mayor a 1023. Los Firewalls de inspección de estado resuelven este problema creando un directorio de conexiones TCP de salida, de manera que cada conexión tiene su correspondiente puerto cliente no privilegiado. Esta tabla de estado se usa para validar cualquier tráfico de entrada. La solución de inspección de estado es más segura porque el Firewall analiza los puertos cliente individualmente dejando libre los puertos no privilegiados para acceso externo.

Tabla 4.2 Ejemplo de una tabla de estados

Dirección de Origen	Puerto de Origen	Dirección de Destino	Puerto de Destino	Estado de la Conexión
172.16.255.100	1030	210.9.88.29	80	Establecida
172.16.255.102	1031	216.32.42.123	80	Establecida
172.16.255.101	1033	173.66.32.122	25	Establecida
172.16.255.106	1035	177.231.32.12	79	Establecida
223.43.21.231	1990	172.16.255.6	80	Establecida
219.22.123.32	2112	172.16.255.6	80	Establecida
210.99.212.18	3321	172.16.255.6	80	Establecida
24.102.32.23	1025	172.16.255.6	80	Establecida
223.212.212	1046	172.16.255.6	80	Establecida

En esencia los Firewalls con inspección de estado incorporan las características del nivel cuatro a los filtros de paquetes estándar, aunque comparten las fortalezas y debilidades de sus predecesores ya que analizan un mayor número de niveles. En la tabla 4.2 se muestra un ejemplo de una tabla de estado. Los Firewall de inspección de estado están restringidos al uso solo en redes con infraestructura TCP/IP, se pueden acomodar a otros protocolos de red como los filtros de paquetes

4.1.3 Proxy Firewalls

Son Firewalls avanzados que combinan el control de acceso de los niveles bajos con la funcionalidad de los niveles altos, generalmente el nivel siete de aplicación. Los Proxy Firewalls no requieren ruta de nivel tres (nivel de red) entre las interfaces de entrada y de salida del Firewall; el enrutamiento lo realiza el software del Proxy Firewall a nivel de aplicación. En el caso de que esta aplicación deje de funcionar el Firewall será incapaz de enrutar paquetes y por lo tanto dejará inaccesible la red que interconecta ya que todos los paquetes que atraviesan el Firewall deben estar bajo el control de la aplicación.

El Firewall se conecta directamente con las reglas de control de acceso para determinar si un paquete dado puede o no transitar el Firewall. Adicional a las reglas los Proxy Firewall pueden requerir autenticación de usuarios individuales de la red. Esta autenticación puede ser de varias maneras como las siguientes:

- Autenticación por login y contraseña.
- Autenticación por token hardware o software.
- Autenticación por dirección de origen.
- Autenticación biométrica.

Los Proxy Firewall tienen numerosas ventajas sobre los filtros de paquetes y sobre los de inspección de estado. Los Proxy Firewall tienen mayores capacidades para guardar logs o registros de eventos debido a que el Firewall examina no solo direcciones o puertos de los paquetes que transitan en la red, por ejemplo, los logs de un Proxy Firewall pueden contener comandos específicos que pueden ser considerados peligrosos en la red.

Otra ventaja es que permiten a los administradores de seguridad reforzar cualquier tipo de autenticación de usuarios que esté o vaya a ser implementada. También son capaces de autenticar usuarios directamente lo que no pueden hacer sus predecesores que solo pueden autenticar usuarios basándose en sus direcciones de nivel de red donde el usuario reside y dado que las direcciones de red pueden ser fácilmente suplantadas, las capacidades de autenticación inherentes en los Proxy Firewalls son superiores a los de filtros de paquetes e inspección de estado. Finalmente, dado que dichos Firewalls no son simplemente dispositivos de nivel de red son menos vulnerables a ataques de suplantación de nivel de red y nivel de enlace de datos.

La avanzada funcionalidad de los Proxy Firewalls también fomenta muchas desventajas cuando son comparados con los Firewalls anteriores. La primera, debido al análisis completo de los paquetes el Firewall se ve obligado a leer e interpretar cada paquete en su totalidad lo que lo hace más lento. Por esta razón estos Firewalls no son usados en enlaces de gran ancho de banda ni para proteger máquinas que corran aplicativos de tiempo real. Para disminuir la carga de este tipo de Firewall se usa un servidor Proxy dedicado para asegurar los servicios menos sensibles a los retardos de tiempo

Otra desventaja es que estos Firewalls tienden a ser limitados en términos de soporte para nuevos protocolos y aplicaciones, ya que por cada tipo de tráfico que necesita transitar por el Firewall se necesita un agente Proxy específico. La mayoría de desarrolladores de Proxy Firewalls proveen agentes genéricos para soportar protocolos o aplicaciones de red indefinidos. Sin embargo, estos agentes son muy restrictivos opacando las fortalezas de estos Firewalls.

4.1.4 Servidores Proxy Dedicados

Esta configuración difiere de los Firewalls anteriores en que se retiene el control del tráfico pero no tienen funcionalidad de Firewall, por esta razón son ubicados detrás de plataformas de Firewall tradicionales. Generalmente el Firewall principal puede aceptar tráfico de entrada, determina hacia que aplicación se dirige dicho tráfico y lo reenvía hacia el servidor Proxy apropiado, por ejemplo el servidor Proxy de correo. El servidor Proxy realizaría las operaciones de filtrado y registro de logs para después enviarlo a las máquinas internas. Un servidor Proxy también puede aceptar tráfico de salida desde equipos internos, filtrar y registrar el tráfico para pasarlo al Firewall y que este sea enviado al destinatario externo. Un ejemplo puede ser un servidor Proxy HTTP detrás del Firewall en el cual los usuarios tendrían que conectarse para tener acceso a servidores Web externos. En la mayoría de los casos, los servidores Proxy son usados para disminuir el procesamiento del Firewall y para realizar tareas de filtrado y registro de logs que serían muy difíciles de realizar por el Firewall solamente.

Con este esquema las organizaciones pueden restringir tráfico de salida, examinar los correos salientes para saber si transportan virus, restringir el acceso a páginas Web maliciosas, examinar archivos que se descargan vía FTP o HTTP, entre otras aplicaciones. Los expertos en seguridad concuerdan en que la mayoría de problemas de seguridad en las organizaciones provienen del interior de la red; los servidores Proxy contribuyen a disminuir los ataques internos o los comportamientos maliciosos. La figura 4.1 muestra una configuración de Firewall con servidor Proxy dedicado.

Adicionalmente a la autenticación y el registro de logs, los servidores Proxy dedicados son útiles para el análisis de correo electrónico y Web incluyendo los siguientes aspectos:

- Filtrado de aplicaciones o applets de Java.
- Filtrado de controles ActiveX.
- Filtrado de JavaScript.
- Bloqueo de tipos específicos de extensiones multimedia multipropósito de Internet (MIME).
- Análisis y remoción de virus.
- Bloqueo de comandos específicos, por ejemplo el comando *delete* de HTTP.
- Bloquea contenido descrito por al administrador a usuarios elegidos por el administrador.

La figura 4.1 muestra un diagrama de una red empleando servidores Proxy dedicados para Web y para correo electrónico situados detrás de otro sistema de Firewall. En este caso el Proxy de correo actuaría como una gateway para el correo saliente. El Firewall principal enviaría el correo entrante al Proxy para el análisis de su contenido y luego dejarlo disponible al destinatario. El Proxy HTTP manejaría conexiones salientes hacia servidores Web externos y dependiendo del agente se podría filtrar contenido activamente. Muchas organizaciones habilitan el almacenamiento en caché de las páginas más visitadas para reducir el tráfico en el Firewall, como es el caso de los servidores Proxy de la Universidad del Cauca.

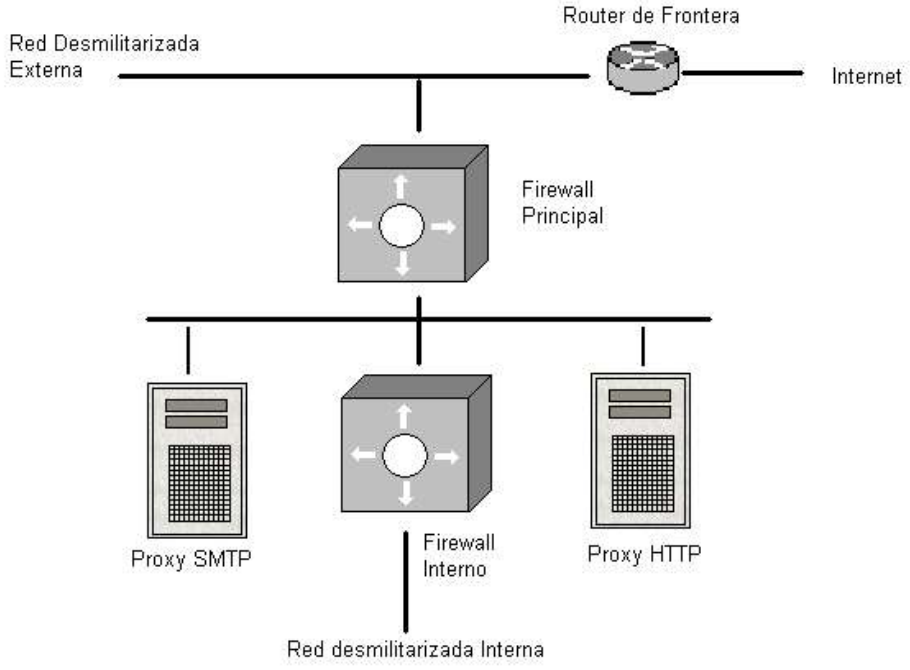


Figura 4.1 Configuración de Firewall con servidor Proxy dedicado

4.1.5 Tecnologías Híbridas de Firewalls

Los recientes avances en la infraestructura de redes y en la seguridad de la información han causado una fusión de conceptos entre las tecnologías de Firewall estudiadas anteriormente. Como resultado de estos avances, los productos de los fabricantes en la actualidad incorporan funcionalidad de muchas clasificaciones de Firewalls existentes. Por ejemplo, muchas aplicaciones de Proxy Firewall han implementado funcionalidades básicas de filtrado de paquetes para proveer mejor soporte para aplicaciones basadas en UDP.

De la misma manera, muchos fabricantes de Firewalls filtros de paquetes y de inspección de estado han implementado funcionalidades básicas de Proxy Firewall para combatir algunas de las debilidades asociadas a sus productos. Esta hibridización no es siempre la mejor manera de que producto es el más conveniente para aplicación para una infraestructura de red dada.

4.1.6 Traducción de Direcciones de Red (NAT)

La traducción de direcciones de red es un proceso muy utilizado en las redes y además es un complemento muy importante para incrementar la seguridad casi siempre acompañando a los sistemas de Firewall. La tecnología de NAT surgió en respuesta a dos de las más grandes traducciones de la ingeniería y la traducción en redes. La primera, NAT es una herramienta efectiva para ocultar el esquema de direccionamiento presente en la traducción de un ambiente protegido por un Firewall. En la práctica NAT permite a una traducción mostrar el esquema de direccionamiento que se quiera mientras se oculta el verdadero esquema, manteniendo la habilidad para conectarse a recursos externos a través del Firewall. La segunda es debido a la escasez de direcciones IP públicas, lo que ha llevado a las organizaciones a usar NAT para el mapeo de direcciones no enrutables a pequeños grupos de direcciones públicas que son de traducción en pequeñas cantidades.

4.1.6.1 Traducción de Direcciones de Red Estáticas

En redes con direcciones estáticas, cada equipo tiene su correspondiente dirección pública enrutable asociada. Pero esto no es fácil de lograr en redes grandes debido a la escasez de direcciones públicas. Con traducción de direcciones de red estáticas es posible ubicar recursos detrás del Firewall, conservando la habilidad para proveer acceso selectivo a usuarios externos. En otras palabras un sistema externo puede acceder un servidor Web interno cuyas direcciones han sido mapeadas con traducción de direcciones estáticas. El Firewall realiza el mapeo en dirección de salida y de entrada. La tabla 4.3 muestra un ejemplo de una tabla de NAT estáticas.

Tabla 4.3 Ejemplo de una tabla de NAT estáticas

Direcciones de Red Internas	Direcciones Públicas Enrutables
172.16.41.101	208.195.214.10
172.16.41.105	208.195.214.11
172.16.41.116	208.195.214.12
172.16.41.113	208.195.214.13

4.1.6.2 Ocultamiento de la Traducción de Direcciones de Red

Cuando se ocultan la traducción de direcciones estáticas, todos los equipos detrás de un Firewall comparten una misma dirección pública como se muestra en la tabla 4.4. De ese modo, todos los equipos que tengan acceso externo de ese tipo detrás del Firewall parecerán uno solo. Este tipo de NAT es muy común pero tiene una visible debilidad en que no es posible crear recursos disponibles a usuarios externos una vez son ubicados detrás del Firewall que los emplea ya que desde afuera hacia dentro no es posible enrutarlos cuando la comunicación se inicia en ese sentido; cuando la comunicación se inicia desde dentro hacia fuera se guardan registros de la conexión haciendo posible enrutar los paquetes de regreso. Otra debilidad de esta técnica es que un Firewall usando traducción de direcciones de red de muchas a una, como también es conocida, debe usar generalmente su propia interfaz externa de red para dar acceso a los equipos que se encuentran detrás de él. Este requerimiento tiende a disminuir la flexibilidad del mecanismo.

Tabla 4.4 Ejemplo de una tabla de ocultamiento de NAT

Direcciones de Red Internas	Direcciones Públicas Enrutables
172.16.41.101	208.195.214.10
172.16.41.105	208.195.214.10
172.16.41.116	208.195.214.10
172.16.41.113	208.195.214.10

4.1.7 Traducción de Direcciones por Puerto (PAT)

Existen dos diferencias principales entre PAT y el ocultamiento de NAT. La primera, es que en PAT no se requiere el uso de la dirección de la interfaz de red externa para todo el tráfico de red. La segunda, con PAT es posible ubicar recursos detrás de un Firewall y hacerlos selectivamente accesibles a usuarios externos. Este acceso puede realizarse gracias al reenvío de conexiones de entrada hacia equipos específicos en ciertos puertos. Por ejemplo, un Firewall usando PAT podría pasar todas las conexiones de entrada hacia el puerto 80 de un servidor Web interno que emplee un esquema diferente (no oficial o RFC 1918) de direccionamiento.

La traducción de direcciones de red por puerto funciona usando la dirección y el puerto del cliente para identificar conexiones de entrada. Por ejemplo, si un sistema que emplea PAT detrás de un Firewall estuviera conectado por telnet con un sistema en Internet, el sistema externo vería una conexión desde la interfaz externa del Firewall junto con el puerto cliente de origen. Cuando el sistema externo responda a la conexión, usará la información de direccionamiento que recibió. Cuando el Firewall PAT recibe la respuesta verá

el puerto cliente de origen dado por el sistema remoto y basado en ese puerto origen determinaría qué sistema interno hizo el requerimiento de conexión. En el ejemplo de la tabla 4.5 un sistema remoto respondería a un intento de conexión usando la dirección de la interfaz externa del Firewall seguida del puerto de salida PAT usado como puerto cliente de origen. El puerto de salida PAT es definido dinámicamente por el Firewall; es secuencial en algunas implementaciones y aleatorio en otras.

Como conclusión, en términos de fortalezas y debilidades cada tipo de traducción de direcciones de red tiene aplicabilidad en ciertas situaciones teniendo como variable la flexibilidad del diseño ofrecido por cada uno. El NAT estático ofrece la mayor flexibilidad pero no es una práctica muy popular debido a la escasez de direcciones IPv4. El ocultamiento de traducción de direcciones fue un paso transitorio en el desarrollo de la traducción de direcciones de red y es poco usada porque la traducción de direcciones por puerto ofrece características adicionales al ocultamiento de NAT, manteniendo el diseño básico y las consideraciones de ingeniería. Por todo esto, PAT se considera la solución más conveniente y segura.

Tabla 4.5 Ejemplo de una tabla PAT

Dirección Interna del Sistema	Puerto Cliente del Sistema Interno	Puerto de Salida PAT
172.16.41.101	1025	3334
172.16.41.105	1035	3335
172.16.41.116	1456	3336
172.16.41.113	1037	3337

4.1.8 Sistemas Firewall en la Red de Datos de la Universidad del Cauca

La Red de Datos cuenta en este momento con dos sistemas de Firewall, cada uno protege un enlace de conexión a Internet. El primer Firewall es un sistema Cisco PIX de la serie 515E el cual es un Firewall hardware destinado a la protección de equipos con direcciones públicas que pertenezcan a la red del proveedor del enlace de Orbitel. El segundo es un sistema basado en el modulo IPtables del sistema operativo Linux el cual es un Firewall software que brinda protección a los equipos pertenecientes a la red del proveedor Telecom. Se estudiará las ventajas y cualidades de cada uno para saber en que estado se encuentra la seguridad perimetral de la red universitaria dada por estos dos sistemas para tener en cuenta los aspectos en que se podría mejorar.

4.1.8.1 Sistema de Firewall Cisco PIX 515E

Actualmente la Universidad del Cauca cuenta con un Firewall Cisco PIX 515E para la protección del tráfico del enlace de Orbitel.

Los Firewall PIX de Cisco son los más populares en el mundo, la referencia 515E es apropiada para redes empresariales de pequeña y mediana escala. Soporta hasta seis interfaces Fast Ethernet 10/100. Es un Firewall de inspección de estado al cual se le han agregado funcionalidades adicionales para hacerlo más robusto, entre las que se encuentran: análisis de algunos protocolos y aplicaciones de altos niveles, servicios de VPN, prevención de intrusiones en línea. Los Firewalls PIX utilizan un algoritmo de

seguridad adaptativo creado por Cisco que provee inspección de estado gracias al seguimiento de las comunicaciones autorizadas de red y a la prevención de accesos no autorizados. Integra más de 24 motores de inspección que realizan el análisis entre los niveles cuatro al siete en el tráfico de red para muchas de las aplicaciones y protocolos más populares hoy en día. Cada una de las características del Firewall PIX se describe en la tabla 4.6.

La topología de conexión del Firewall Cisco PIX en la red se muestra en la figura 4.2. En ella se muestra el enlace hacia Internet que llega por un par de fibra óptica que transporta ATM hacia el enrutador el cual se conecta al Firewall y este al switch de núcleo para dar conectividad a la red LAN de la Universidad.

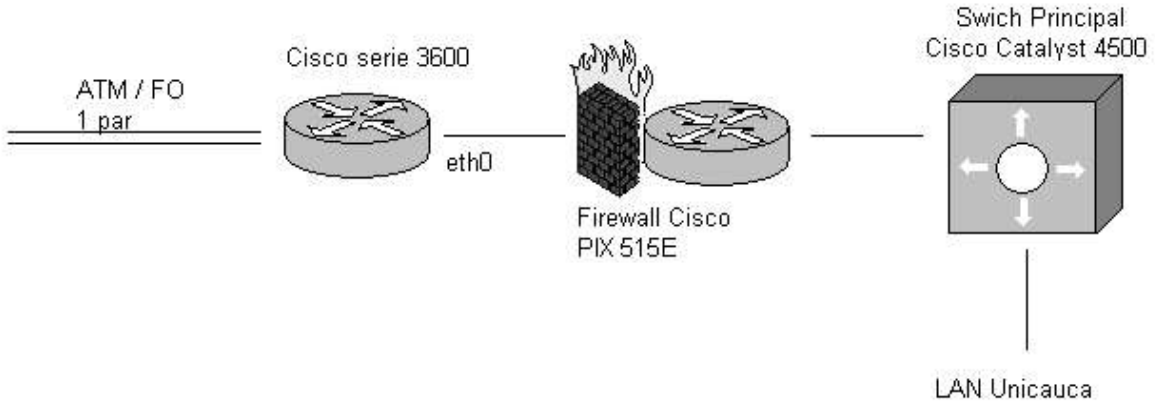


Figura 4.2 Topología de conexión del Firewall Cisco PIX 515E

Tabla 4.6 Características del Firewall PIX de CISCO

Característica	Descripción
Inspección de estado	✓ Provee seguridad perimetral para accesos no autorizado usando un algoritmo adaptativo. ✓ Brinda control de acceso para más de 100 aplicaciones, servicios y protocolos predefinidos con la habilidad para crear aplicaciones y servicios personalizados. ✓ Se pueden crear grupos de objetos reusables lo cuales puede ser referenciados por las políticas de seguridad.
Inspección de protocolos y aplicaciones avanzadas	Integra mas de 24 motores de inspección para protocolos de alto nivel como: HTTP, FTP, SMTP, DNS, SMB, NFS, H.323 versiones 1-4, SIP, SCCP, RTSP y muchos mas.
Servidor VPN	✓ Provee servicios de concentrador VPN para más de 2000 clientes remotos basados en software o hardware. ✓ Extiende el alcance de las VPN's hacia entornos que usan NAT o PAT basado en el estándar de la IETF para NAT transversal.
Cliente VPN	✓ Incluye licencia ilimitada para el Cisco VPN Client. ✓ Tiene novedosas características incluyendo políticas de seguridad dinámicas

VPN sitio – sitio	✓ Soporta los estándares de VPN de IPSec junto con el protocolo IKE. ✓ Aumenta el intercambio de información sobre Internet gracias al aseguramiento de la privacidad, integridad y autenticación con usuarios y redes remotas. ✓ Soporta algoritmos de cifrado como: DES de 56 bits, 3DES de 168 bits, AES de 256 bits.
Prevención de Intrusos	✓ Brinda protección contra mas de 55 tipos de ataque populares que van desde paquetes mal formados hasta ataques de denegación de servicio. ✓ Se integra con Cisco Network Intrusion Detection System para identificar y bloquear dinámicamente nodos de red maliciosos.
Soporte AAA	✓ Se integra con métodos populares de autenticación, autorización y manejo de cuenta vía TACAS+ y RADIUS.
Certificados X.509 y soporte CRL	✓ Soporta SCEP con la soluciones del estándar X.509 de Baltimore, Entrust, Microsoft y Verisign.
Soporte para NAT y PAT	✓ Provee servicios de Traducción de Direcciones de Direcciones de Red así como Traducción de Direcciones por Puerto basados en políticas de manera estática y dinámica.

El Firewall esta configurado para realizar NAT a las direcciones que necesitan ser vistas como públicas del enlace de Orbitel las cuales pertenecen al rango 10.200.1.0/24 y 10.200.2.0/24 traduciéndolas en el rango 208.195.214.0/24. Actualmente no existe ninguna clase de filtro para ninguna dirección: se permite el paso del protocolo IP y de cualquiera de los protocolos que este puede transportar para las direcciones asignadas. Una solución optima sería utilizar PAT para dar acceso a los rango de direcciones mencionado, establecer grupos de políticas de seguridad para asignárselos a cada dirección dependiendo de sus necesidades, identificar e implementar protección sobre los servicios de alto nivel más vulnerables, y crear VPNs para conectar las sedes remotas de la Universidad que se acceden por medio del enlace que protege el Firewall.

4.1.8.2 Sistema de Firewall IPTABLES

IPtables es un sistema de Firewall vinculado al kernel de Linux que se ha extendido enormemente a partir del kernel 2.4 de este sistema operativo. Al igual que el anterior sistema IPchains, el Firewall de IPtables no es un servicio que se inicia o detiene o que se pueda caer por un error de programación (ha tenido alguna vulnerabilidad que permite DoS, pero nunca tendrá tanto peligro como las aplicaciones que escuchan en determinado puerto TCP): IPtables esta integrado con el kernel, es parte del sistema operativo; lo que se hace es aplicar reglas. Para ellos se ejecuta el comando IPtables, con el que se añade, se eliminan, o se crean reglas. Por ello un Firewall de IPtables no es sino un simple script para un interprete de comandos en el que se van ejecutando las reglas de Firewall.

Cuando un paquete llega al kernel de un equipo que soporta IPtables el kernel tiene que decidir que hacer con el dependiendo si el paquete el para el equipo o se dirige hacia otro. La figura 4.3 ilustra el camino que seguirá un paquete durante su paso por el kernel.

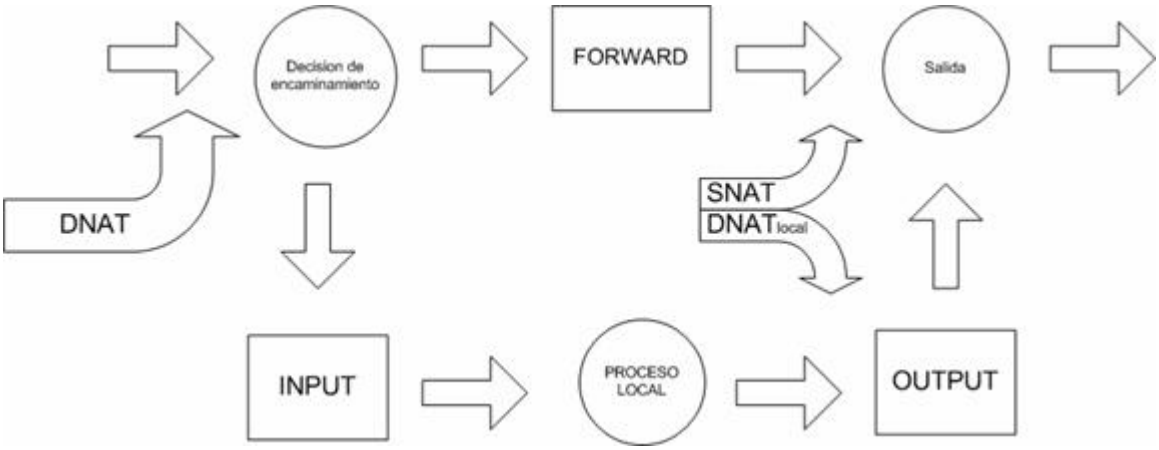


Figura 4.3 Camino de un paquete durante su paso por el kernel de Linux

Como se observa en el gráfico, básicamente se mira si el paquete esta destinado a la propia máquina o si va a otra. Para los paquetes (o datagramas, según el protocolo) que van a la propia máquina se aplican las reglas INPUT y OUTPUT, y para filtrar paquetes que van a otras redes o máquinas se aplican simplemente reglas FORWARD. INPUT, OUTPUT y FORWARD son los tres tipos de reglas de filtrado. Antes de aplicar esas reglas es posible aplicar reglas de NAT: estas se usan para hacer redirecciones de puertos o cambios en las IPs de origen y destino. E incluso antes de las reglas de NAT se pueden introducir reglas de tipo MANGLE, destinadas a modificar los paquetes; son reglas poco conocidas y es probable que no las usen. Por lo tanto se tienen tres conjuntos de reglas en IPTables:

- MANGLE
- NAT: reglas PREROUTING, POSTROUTING
- FILTER: reglas INPUT, OUTPUT, FORWARD.

El Firewall IPtables que opera en la Intranet de la Universidad del Cauca se encuentra corriendo sobre el equipo *arges* el cual se soporta sobra la distribución Linux Debian 3.1. A su vez sirve como puerta de enlace para todas las direcciones del la redes de Telecom. 200.21.83.64/26 y 200.21.83.192/26 protegiendo el enlace suministrado por el mismo proveedor.

Arges se encuentra conectado hacia la red de área local por medio de un switch secundario y hacia el enrutador que da acceso a Internet con el operador Telecom. por medio del switch de núcleo entre el router y Arges hay creada una red punto a punto para que ningún equipo pueda utilizar directamente el router para salir a Internet sino que se hace necesario pasar por el Firewall para así poder hacer un chequeo de los paquetes que entran y salen de la red por el enlace de Telecom. La descripción anterior se observa en la figura 4.4.

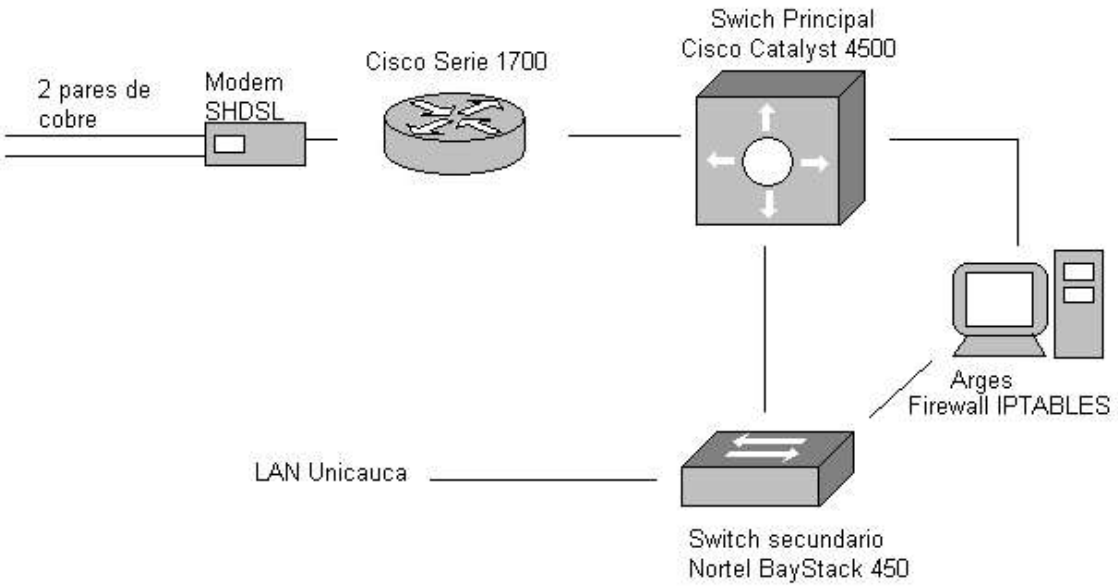


Figura 4.4 Topología de conexión de Arges (Firewall IPtables)

Aunque la configuración de un Firewall con IPtables se realiza con comandos, lo más aconsejable es realizar un script, ya que ello permite: ejecutar todas las reglas de forma continua, evita tener que escribir las reglas cada vez que se reinicie el Firewall, realizar cambios de forma más intuitiva, e incluir otras facilidades y funcionalidades para hacer más practico iniciar y detener el Firewall.

El script elaborado en la red de datos está dividido según las funciones que ofrece: start, stop, restart, test y panic. Lo más importante del script esta contenido en la función start, ya que es la que define las reglas del Firewall. Dicho script es largo y un poco complejo. La función start del script esta dividida en secciones, cada una con un propósito particular, se describirá cada una y se dará un ejemplo para un mejor entendimiento. Estas secciones son:

- Establecimiento de parámetros en el kernel. En esta sección se ubican los comandos para habilitar o deshabilitar opciones en el kernel que aumentan las medidas de seguridad del sistema operativo. Por ejemplo:

  echo 1 > /proc/sys/net/ipv4/icmp_echo_ignore_broadcasts

  Con lo cual se habilita la protección echo broadcast para evitar ataques smurfing.

- Configuración inicial de IPtables. Esta sección contiene los comandos necesarios para inicializar los parámetros de las tablas y las cadenas, y el establecimiento de las políticas por defecto para las cadenas de la tabla filter. Por ejemplo:

  $IPTABLES-P INPUT DROP
  $IPTABLES-P OUTPUT DROP
  $IPTABLES-P FORWARD DROP

Estableciendo las políticas por defecto para las cadenas de la tabla *filter*, como se observa todas las cadenas tienen como política por defecto: denegar. Esto significa que si ningún paquete cumple las condiciones dadas por el administrador, el paquete será denegado sin enviar información de ello a la fuente

- Definición de Redes, Servicios y Condiciones que se deben Bloquear. En esta sección se especifican las reglas para denegar el acceso de paquetes mal formados, direcciones IP inválidas, y puertos de troyanos. Como por ejemplo:

```
$IPTABLES -A bad_tcp -p TCP --tcp-flags SYN,ACK SYN,ACK -m state --state NEW -j REJECT
```

Con el anterior comando se rechazan paquetes TCP mal formados que se utilizan para ataques o para análisis de sistemas operativos.

Para bloquear puertos por los que se propaga el celebre gusano Blaster que ataca sistemas Microsoft Windows.

```
$IPTABLES -A deny_port -p TCP -m multiport --dport 135,4444 -j DROP
```

- Definición de los Estados de Conexión. Desde una perspectiva restrictiva, las condiciones de evaluación de las reglas pueden descomponerse en tres partes: el estado de la conexión; los protocolos y puertos de origen y destino; y las interfaces y direcciones de origen y destino. En esta sección se especifican las reglas con los estados de conexión validos para los paquetes con destino a un servidor y para los paquetes con destino a un cliente.

```
$IPTABLES -A allowed_new -m state --state NEW,ESTABLISHED -j ACCEPT
$IPTABLES -A allowed_new -j DROP
```

Reglas para aceptar paquetes TCP bien formados en el lado del servidor según el estado de la conexión

- Definición de Servicios Básicos. Esta sección contiene las reglas para definir las condiciones relacionadas con los servicios o puertos a los que se puede acceder. Por ejemplo:

```
$IPTABLES -A http_in -p TCP --dport 80 --sport $NOPRIV_PORTS -j allowed_new
$IPTABLES -A http_out -p TCP --sport 80 --dport $NOPRIV_PORTS -j ACCEPT
```

Se caracteriza el servicio Web HTPP dejando pasar paquetes que se dirijan desde servidores hacia clientes del servicio, la variable $NOPRIV_PORTS hace referencia a los puertos TCP no privilegiados.

- Reglas para los Paquetes que entran y salen del Firewall. Sección en la que se definen las condiciones relacionadas con las interfaces y las IP de las reglas para permitir la entrada o salida de paquetes al equipo.

```
$IPTABLES -A INPUT -i $SRT2_IFACE -d $SRT2_IP -s 200.21.83.134 -j ssh_in
$IPTABLES -A OUTPUT -o $SRT2_IFACE -s $SRT2_IP -d 200.21.83.134 -j ssh_out
```

Para permitir el acceso por ssh desde una de las estaciones de trabajo de la red de datos (200.21.83.134) hacia la interfaz referenciada por la variable $SRT2_IFACE con dirección IP dad por la variable $SRT2_IP

- Reglas para los Paquetes Reenviados entre la Intranet e Internet. Sección en la que se definen las condiciones relacionadas con las interfaces y las IP, de las reglas para permitir el redireccionamiento de paquetes que pasan por el equipo.

4.2 VPN (REDES PRIVADAS VIRTUALES)

Hasta no hace mucho tiempo, las diferentes sucursales de una empresa podían tener, cada una, una red local a la sucursal que operara aislada de las demás. Cada una de estas redes locales tenía su propio esquema de nombres, su propio sistema de correo electrónico, e inclusive usar protocolos que difieran de los usados en otras sucursales. Es decir, en cada lugar existía una configuración totalmente local, que no necesariamente debía ser compatible con alguna o todas las demás configuraciones de las otras áreas dentro de la misma empresa.

A medida que los computadores fueron incorporados a las empresas, que surgieron los sistemas de información y se incrementó la importancia de las diferentes redes corporativas, surgió la necesidad de comunicar las diferentes redes locales para compartir recursos internos. Para cumplir este objetivo, debía establecerse un medio físico para la comunicación. Este medio fueron las líneas telefónicas, con la ventaja de que la disponibilidad es muy alta y que se garantiza la privacidad. Además de la comunicación entre diferentes sucursales, surgió la necesidad de proveer acceso a los usuarios móviles de la empresa. Mediante Servicios de Acceso Remoto (Remote Access Services - RAS), este tipo de usuario puede conectarse a la red de la empresa y usar los recursos disponibles dentro de la misma. El gran inconveniente del uso de las líneas telefónicas es su alto costo, ya que se suele cobrar un cargo básico más una tarifa por el uso, en el que se tienen en cuenta la duración de las llamadas y la distancia. Si la empresa tiene sucursales dentro del mismo país pero en distintas áreas telefónicas, y, además, tiene sucursales en otros países, los costos telefónicos pueden llegar a ser exagerados. Adicionalmente, si los usuarios móviles deben conectarse a la red corporativa y no se encuentran dentro del área de la empresa, deben realizar llamadas de larga distancia, con lo que los costos se incrementan. Las VPN son una alternativa a la conexión WAN mediante líneas telefónicas y al servicio RAS, bajando los costos de éstos y brindando los mismos servicios, mediante autenticación, cifrado y el uso de túneles para las conexiones.

Una Red Privada Virtual es un sistema para simular una red privada sobre una red pública, por ejemplo, Internet. Como se muestra en la figura 4.5, la idea es que la red pública sea "vista" desde dentro de la red privada como un cable lógico que une dos o más redes que pertenecen a la red privada. Las VPN también permiten la conexión de usuarios móviles a la red privada, tal como si estuvieran

en una LAN dentro de una oficina de la empresa donde se implementa la VPN. Esto resulta muy conveniente para personal que no tiene lugar fijo de trabajo dentro de la empresa, como podrían ser vendedores, ejecutivos que viajan, personal que realiza trabajo desde el hogar, etc. La forma de comunicación entre las partes de la red privada a través de la red pública se hace estableciendo túneles virtuales entre dos puntos para los cuales se negocian esquemas de encriptación y autentificación que aseguran la confidencialidad e integridad de los datos transmitidos utilizando la red pública. Como se usan redes públicas, en general Internet, es necesario prestar debida atención a las cuestiones de seguridad, que se aborda a través de estos esquemas de encriptación y autentificación y que se describirán luego.

La tecnología de túneles, Tunneling, es una técnica que usa una infraestructura entre redes para transferir datos de una red a otra. Los datos o la carga pueden ser transferidas como tramas de otro protocolo. El protocolo de tunneling encapsula las tramas con una cabecera adicional, en vez de enviarla como la produjo en nodo original. La cabecera adicional proporciona información de routing para hacer capaz a la carga de atravesar la red intermedia. Las tramas encapsuladas son enrutadas a través de un túnel que tiene como puntos finales los dos puntos entre la red intermedia. El túnel es una camino lógico a través del cual se encapsulan paquetes viajando entre la red intermedia. Cuando una trama encapsulada llega a su destino en la red intermedia, se desencapsula y se envía a su destino final dentro de la red.

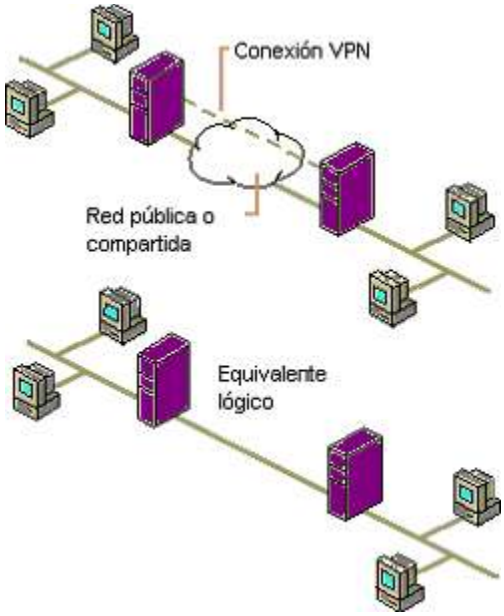


Figura 4.5 Red Privada Virtual y su equivalente lógico

Tunneling incluye todo el proceso de encapsulado, desencapsulado y transmisión de las tramas. Entre las tecnologías de Tunneling más conocidas se encuentran:

- IPSec – Internet Protocol Security Tunnel Mode
- PPTP - Point-to-Point Tunneling Protocol
- L2F – Layer 2 Forwarding
- L2TP – Layer 2 Tunneling Protoco
- DLSW-Data Link Switching (SNA over IP)

- IPX for Novell Netware over IP
- GRE – Generic Routing Encapsulation (rfc 1701/2)
- ATMP – Ascend Tunnel Management Protocol
- MIP – Mobile IP

Las técnicas de autenticación son esenciales en las VPNs, ya que aseguran a los participantes de la misma que están intercambiando información con el usuario o dispositivo correcto. La autenticación en VPNs es conceptualmente parecido al inicio de sesión en un sistema que utiliza nombre de usuario y contraseña, pero con necesidades mayores de aseguramiento de validación de identidades. La mayoría de los sistemas de autenticación usados en VPN están basados en un sistema de claves compartidas. La autenticación es llevada a cabo generalmente al inicio de una sesión, y luego aleatoriamente durante el curso de la misma, para asegurar que no haya algún tercer participante que se haya inmiscuido en la conversación. La autenticación también puede ser usada para asegurar la integridad de los datos. Los datos son procesados con un algoritmo de hashing para derivar un valor incluido en el mensaje como checksum. Cualquier desviación en el checksum indica que los datos sufrieron daños en la transmisión o fueron interceptados y modificados en el camino. Algunos ejemplos de sistemas de autenticación son Challenge Handshake Authentication Protocol (CHAP) y RSA.

Todas las VPNs tienen algún tipo de tecnología de encriptación, que esencialmente empaqueta los datos en un paquete seguro. La encriptación es considerada tan esencial como la autenticación, ya que protege los datos transportados de la poder ser vistos y entendidos en el viaje de un extremo a otro de la conexión. Existen dos tipos de técnicas de encriptación que se usan en las VPN: *encriptación de clave secreta o privada,* y *encriptación de clave pública.*

En la encriptación de clave secreta, se utiliza una contraseña secreta conocida por todos los participantes que necesitan acceso a la información encriptada. Dicha contraseña se utiliza tanto para encriptar como para desencriptar la información. Este tipo de encriptación posee el problema que, como la contraseña es compartida por todos los participantes y debe mantenerse secreta, al ser revelada, debe ser cambiada y distribuida a los participantes, con lo cual se puede crear de esta manera algún problema de seguridad.

La encriptación de clave pública implica la utilización de dos claves, una pública y una privada. La primera es enviada a los demás participantes. Al encriptar, se usa la clave privada propia y la clave pública del otro participante de la conversación. Al recibir la información, ésta es desencriptada usando su propia clave privada y la pública del generador de la información. La gran desventaja de este tipo de encriptación es que resulta ser más lenta que la de clave secreta.

En las VPNs, la encriptación debe ser realizada en tiempo real. Por eso, los flujos encriptados a través de una red son encriptados utilizando encriptación de clave secreta con claves que son solamente buenas para sesiones de flujo. El protocolo más usado para la encriptación dentro de las VPNs es IPSec, que consiste en un conjunto de propuestas del IETF que delinean un protocolo IP seguro para IPv4 e IPv6. IPSec provee encriptación a nivel de IP, como se explicó en el Capítulo 3.

El método de túneles, como se mencionó anteriormente, es una forma de crear una red privada. Permite encapsular paquetes dentro de paquetes para acomodar protocolos incompatibles. Dentro de los protocolos que se usan para la metodología de túneles se

encuentran Point-to-Point Tunneling Protocol (PPTP), Layer-2 Forwarding Protocol (L2FP) y el modo túnel de IPSec. Mediante la Seguridad del protocolo de Internet (IPSec), se puede ofrecer privacidad, integridad, autenticidad y protección contra reproducción para el tráfico de red en las siguientes situaciones:

- Seguridad extremo a extremo de cliente a servidor, servidor a servidor y cliente a cliente mediante el modo de transporte IPSec.
- Acceso remoto seguro desde el cliente a la puerta de enlace a través de Internet mediante el Protocolo de Túnel de capa 2 (L2TP) protegido por IPSec.

IPSec proporciona conexiones seguras entre puertas de enlace a través de redes de área extensa (WAN) externas o conexiones de Internet que utilizan túneles L2TP/IPSec o el modo de túnel IPSec puro. IPSec define los formatos de paquetes IP y la infraestructura relacionada para proporcionar una eficaz autenticación de principio a fin, integridad, protección contra reproducción y, opcionalmente, confidencialidad para el tráfico de red. También se incluye un servicio de petición de negociación y administración de seguridad mediante el Internet Key Exchange (IKE, Intercambio de claves de Internet-RFC 2409), definido por el IETF. Una vez que los equipos del mismo nivel se han autenticado mutuamente, generan claves de cifrado en volumen con el fin de cifrar los paquetes de datos de las aplicaciones. Ambos equipos conocen estas claves, de manera que los datos se encuentran muy bien protegidos contra modificaciones o interpretaciones por parte de atacantes que pudieran actuar en la red.

Es importante hacer una pequeña diferencia entre una Red Privada y una Red Privada Virtual. La primera utiliza líneas alquiladas para formar toda la Red Privada. La segunda lo que hace es crear un túnel entre los dos puntos a conectar utilizando infraestructura publica.

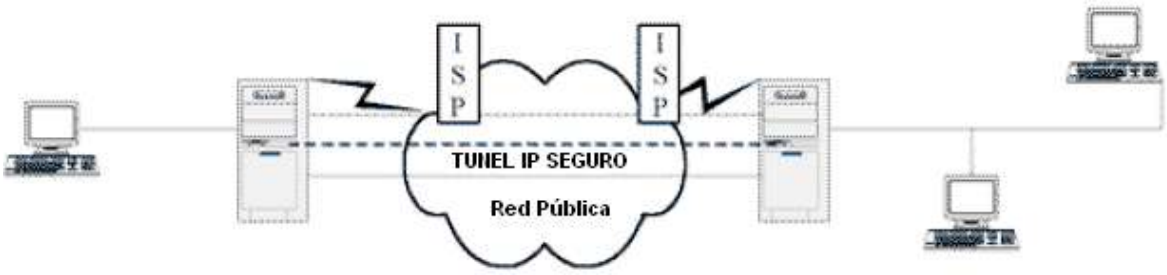


Figura 4.6 Ejemplo de configuración de una VPN

4.2.1 Tipos de VPN's

4.2.1.1 Sistemas Basados en Hardware

Los sistemas basados en hardware, son routers que encriptan. Son seguros y fáciles de usar, simplemente necesitan conectarse y configurar algunas opciones según el tipo de red. Ofrecen un gran rendimiento, porque no malgastan ciclos de procesador haciendo funcionar un Sistema Operativo. Es hardware dedicado, muy rápido, y de fácil instalación.

4.2.1.2 Sistemas Basados en Cortafuegos

Estos se implementan con software de cortafuegos (Firewalls). Tiene todas las ventajas de los mecanismos de seguridad que utilizan los cortafuegos, incluyendo el acceso restringido a la red interna; también realizan la Traducción de Direcciones (NAT). Estos satisfacen los requerimientos de autentificación fuerte. Muchos de los cortafuegos comerciales, aumentan la protección, dando soporte al núcleo del Sistema Operativo en algunas deficiencias que traen consigo, y los provee de medidas de seguridad adicionales, que son mucho más útiles para los servicios de VPN. El rendimiento en este tipo decrece, ya que no se tiene hardware especializado de encriptación.

4.2.1.3 Sistemas Basados en Software

Estos sistemas son ideales para las situaciones donde los dos puntos de conexión de la VPN no están controlados por la misma organización, o cuando los diferentes cortafuegos o routers no son implementados por la misma organización. Este tipo de VPN's ofrecen el método más flexible en cuanto al manejo de tráfico. Con este tipo, el tráfico puede ser enviado a través de un túnel, en función de las direcciones o protocolos; en las VPN por hardware, todo el tráfico es enrutado por el túnel. Con los sistemas basados en software es posible hacer un enrutamiento inteligente de una manera mucho más fácil.

4.2.2 Requerimientos básicos de una Red Privada Virtual

Una Red Privada Virtual provee los siguientes mecanismos básicos, aunque en ocasiones y según las necesidades es posible obviar algunos:

- Autenticación de usuarios: para poder restringir el acceso a la VPN solo a los usuarios autorizados.
- Administración de direcciones: debe asignar una dirección del cliente sobre la red privada, y asegurar que las direcciones privadas se mantienen privadas.
- Encriptación de datos: los datos que viajan por la red pública, deben ser transformados para que sean ilegibles para los usuarios no autorizados.
- Administración de claves: debe mantener un sistema de claves de encriptación para los clientes y los servidores.
- Soporte multiprotocolo: debe ser capaz de manejar protocolos comunes, usando las redes públicas, por ejemplo IP, IPX, etc.

4.2.3 Como funciona una VPN

La tecnología de VPN se centra en el medio que hay entre las redes privadas y las redes públicas. El dispositivo intermediario, ya sea orientado a software, orientado a hardware o la combinación de ambos, actúa como una red privada. Cuando un host local manda un

paquete a una red remota, los datos primero pasan de la red privada por el gateway protegido, viajando a través de la red pública, y entonces los datos pasan por el gateway que esta protegiendo el host destino de la red remota. Una VPN protege los datos cifrándolos automáticamente antes de enviarlos de una red privada a otra, encapsulando los datos dentro de un paquete IP. Cuando estos llegan al destino, los datos son descifrados. El proceso es el siguiente:

- Un equipo cliente llama a un ISP local y conecta a Internet.
- Un software especial cliente reconoce un destino especificado y negocia una sesión de VPN cifrada.
- Los paquetes encriptados son envueltos en paquetes IP para crear el túnel y mandarlos a través de Internet.
- El servidor de VPN negocia la sesión de VPN y descifra los paquetes.
- El tráfico no encriptado fluye a otros servidores y recursos con normalidad.

El fuerte de los componentes en VPN es el cifrado. El objetivo es restringir el acceso a los usuarios y hosts apropiados, y asegurar que los datos transmitidos por Internet sean encriptados para que solo estos usuarios y los hosts sean capaces de ver los datos. La técnica usada es envolver las datos de carga encriptados, con cabeceras que pueden ser interpretadas por los enrutadores. Una vez conectado, una VPN abre un Túnel seguro, en el cual el contenido será encapsulado y encriptado y los usuarios son autentificados.

Pero por supuesto, todos estos mecanismos empleados, aumenta la seguridad en el intercambio de datos pero no añade una reducción en el rendimiento de la comunicación por las sobrecargas. Muchas VPN, ya sean basadas en hardware o en software, deberían ser capaces de procesar la encriptación en conexiones hasta al menos una velocidad de 10BaseT. En velocidades superiores, el consumo de CPU necesaria en las VPN basadas en software es tan elevado que el rendimiento decrece. El los sistemas orientados a hardware, que usan máquinas dedicadas estas velocidades aumentan. En conexiones como módems, el procesamiento en las VPN es mucho más rápido que los retardos introducidos por el ancho de banda disponible. Las pérdidas de paquetes y la latencia en conexiones a Internet de baja calidad afectan al rendimiento más que la carga añadida por la encriptación. En el Capítulo 5 se llevará a cabo la implementación a nivel de Laboratorio de este mecanismo, muy utilizado en la actualidad.

4.3 VLANs (REDES VIRTUALES DE AREA LOCAL)

Hace algún tiempo existía el modelo de red basado en enrutadores, en el que se poseían segmentos independientes y delimitados por cada usuario. Estos enrutadores aparte de ser multiprotocolo podían detener las tormentas de broadcast, pero la desventaja era su sistema compartido. Posteriormente surgió un nuevo modelo en donde se involucraba la parte de switch. Aquí ya no existía contención ni colisión, pero ahora el problema consistía en la expansión del dominio de broadcast por la red.

Los grupos de trabajo en una red, hasta ahora, han sido creados por la asociación física de los usuarios en un mismo segmento de la red, o en un mismo concentrador o hub. Como consecuencia directa, estos grupos de trabajo comparten el ancho de banda disponible y los dominios de "broadcast", con la dificultad de gestión cuando se producen cambios en los miembros del grupo. Más aún, la limitación geográfica que supone que los miembros de un determinado grupo deben de estar situados adyacentemente, por su conexión al mismo concentrador o segmento de la red.

Los esquemas VLAN (Virtual Local Area Network), proporcionan los medios adecuados para solucionar esta problemática, por medio de la agrupación realizada de una forma lógica en lugar de física. Sin embargo, las redes virtuales siguen compartiendo las características de los grupos de trabajo físicos, en el sentido de que todos los usuarios tienen conectividad entre ellos y comparten sus dominios de "broadcast".

La principal diferencia con el hecho de estar en una agrupación física, como se ha mencionado, es que los usuarios de las redes virtuales pueden ser distribuidos a través de una red LAN, incluso situándose en diferentes concentradores de la misma. Los usuarios pueden, así, "moverse" a través de la red, manteniendo su pertenencia al grupo de trabajo lógico (ver Figura 4.7). Por otro lado, al distribuir a los usuarios de un mismo grupo lógico a través de diferentes segmentos, se logra, como consecuencia directa, el incremento del ancho de banda en dicho grupo de usuarios. Además, al poder distribuir a los usuarios en diferentes segmentos de la red, es posible situar puentes y enrutadores entre ellos, separando segmentos con diferentes topologías y protocolos. Así por ejemplo, se pueden mantener diferentes usuarios del mismo grupo, unos con FDDI y otros con Ethernet, en función tanto de las instalaciones existentes como del ancho de banda que cada uno precise, por su función específica dentro del grupo. Todo ello, por supuesto, manteniendo la seguridad deseada en cada configuración por el administrador de la red: Se puede permitir o no que el tráfico de una VLAN entre y salga desde/hacia otras redes. Pero aún se puede llegar más lejos. Las redes virtuales permiten que la ubicuidad geográfica no se limite a diferentes concentradores o plantas de un mismo edificio, sino a diferentes oficinas intercomunicadas mediante redes WAN o MAN, a lo largo de países y continentes, sin limitación ninguna más que la impuesta por el administrador de dichas redes. Las VLAN deben ser rápidas, basadas en switchs para que sean interoperables totalmente (porque los routers no dan la velocidad requerida), su información deberá viajar a través del backbone y deberán ser movibles, es decir, que el usuario no tenga que reconfigurar la máquina cada vez que cambie su ubicación.

4.3.1 Tecnología

Existen tres aproximaciones diferentes que pueden ser empleadas como soluciones válidas para proporcionar redes virtuales: conmutación de puertos, conmutación de segmentos con funciones de bridging, y conmutación de segmentos con funciones de bridging/routing. Todas las soluciones están basadas en arquitecturas de red que emplean concentradores/conmutadores. Aunque las tres son soluciones válidas, sólo la última, con funciones de bridge/router, ofrece todas las ventajas a las VLAN.

4.3.1.1 Conmutadores de puertos

Los conmutadores de puertos son concentradores con varios segmentos, cada uno de los cuales proporciona el máximo ancho de banda disponible, según el tipo de red, compartido entre todos los puertos existentes en dicho segmento. Se diferencian de los conmutadores tradicionales en que sus puertos pueden ser dinámicamente asociados a cualquiera de los segmentos, mediante comandos software. Cada segmento se asocia a un "backplane", el cual a su vez, equivale a un grupo de trabajo. De este modo, las estaciones conectadas a estos puertos pueden ser asignadas y reasignadas a diferentes grupos de trabajo o redes virtuales.

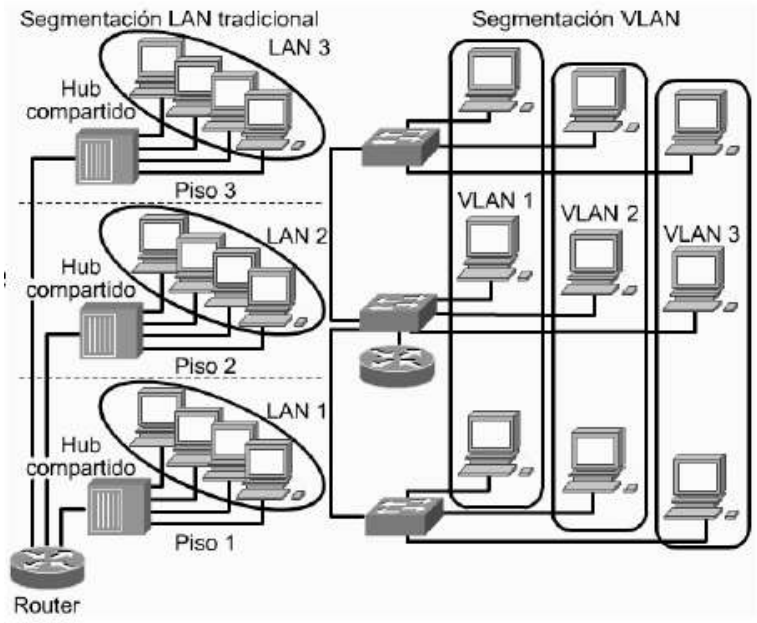


Figura 4.7 Comparación entre una LAN tradicional y una VLAN

Se pueden definir a los conmutadores de puertos como *software patch panels*, y su ventaja fundamental es la facilidad para la reconfiguración de los grupos de trabajo; sin embargo, tienen graves limitaciones. Dado que están diseñados como dispositivos compartiendo un backplane físico, las reconfiguraciones de grupo de trabajo están limitadas al entorno de un único concentrador, y por tanto, todos los miembros del grupo deben de estar físicamente próximos. Las redes virtuales con conmutadores de puertos, padecen de conectividad con el resto de la red. Al segmentar sus propios backplanes, no proporcionan conectividad integrada entre sus propios backplanes, y por tanto están "separados" de la comunicación con el resto de la red. Para ello requieren un bridge/router externo. Ello implica mayores costes, además de la necesidad de reconfigurar el bridge/router cuando se producen cambios en la red. Por último, los conmutadores de puertos no alivian el problema de saturación del ancho de banda de la red. Todos los nodos deben de conectarse al mismo segmento o backplane, y por tanto compartirán el ancho de banda disponible en el mismo, independientemente de su número.

4.3.1.2 Conmutadores de segmentos con bridging

A diferencia de los conmutadores de puertos, suministran el ancho de banda de múltiples segmentos de red, manteniendo la conectividad entre dichos segmentos. Para ello, se emplean los algoritmos tradicionales de los puentes (bridges), o subconjuntos de los mismos, para proporcionar conectividad entre varios segmentos a la "velocidad del cable" o velocidad máxima que permite la topología y protocolos de dicha red.

Mediante estos dispositivos, las VLAN no son grupos de trabajo conectados a un solo segmento o backplane, sino grupos lógicos de nodos que pueden ser conectados a cualquier número de segmentos de red físicos. Estas VLAN son dominios de broadcast lógicos: conjuntos de segmentos de red que reciben todos los paquetes enviados por cualquier nodo en la VLAN como si todos los nodos estuvieran conectados físicamente al mismo segmento.

Al igual que los conmutadores de puertos, mediante comandos software se puede reconfigurar y modificar la estructura de la VLAN, con la ventaja añadida del ancho de banda repartido entre varios segmentos físicos. De esta forma, según va creciendo un grupo de trabajo, y para evitar su saturación, los usuarios del mismo pueden situarse en diferentes segmentos físicos, aún manteniendo el concepto de grupo de trabajo independiente del resto de la red, con lo que se logra ampliar el ancho de banda en función del número de segmentos usados. Aún así, comparten el mismo problema con los conmutadores de puertos en cuanto a su comunicación fuera del grupo. Al estar aislados, para su comunicación con el resto de la red precisan de routers (encaminadores), con las consecuencias de las que ya se ha hablado en el caso anterior respecto de costos y la reconfiguración de la red (Figura 4.8).

4.3.1.3 Conmutadores de segmentos con bridging/routing

Son la solución evidente tras la atenta lectura de las dos soluciones anteriores. Dispositivos que comparten todas las ventajas de los conmutadores de segmentos con funciones de bridging, pero además, con funciones añadidas de routing (encaminamiento), lo que les proporciona fácil reconfiguración de la red, así como la posibilidad de crear grupos de trabajo que se expanden a través de diferentes segmentos de red. Además, sus funciones de routing facilitan la conectividad entre las redes virtuales y el resto de los segmentos o redes, tanto locales como remotas.

Mediante las redes virtuales, es posible crear un nuevo grupo de trabajo, con tan solo una reconfiguración del software del conmutador. Ello evita el recableado de la red o el cambio en direcciones de subredes, permitiéndonos así asignar el ancho de banda requerido por el nuevo grupo de trabajo sin afectar a las aplicaciones de red existentes.

En las VLAN con funciones de routing, la comunicación con el resto de la red se puede realizar de dos modos diferentes: permitiendo que algunos segmentos sean miembros de varios grupos de trabajo, o mediante las funciones de routing multiprotocolo integradas, que facilitan el tráfico incluso entre varias VLAN's.

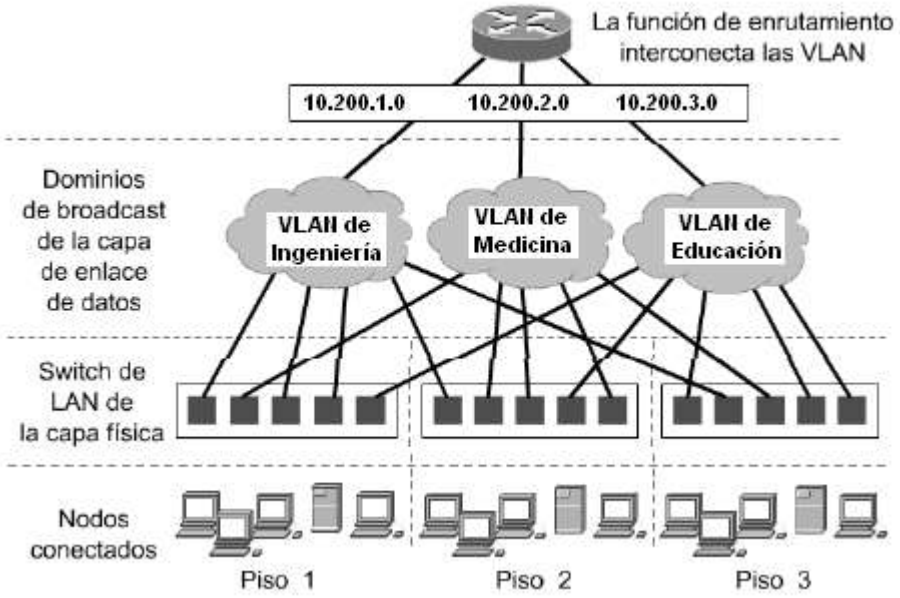


Figura 4.8 Ejemplo de VLAN de Puerto Central

4.3.2 Ventajas de las VLANs

Los dispositivos con funciones VLAN ofrecen unas prestaciones de valor agregado, suplementarias a las funciones específicas de las redes virtuales, aunque algunas de ellas son casi tan fundamentales como los principios mismos de las VLAN. Al igual que en el caso de los grupos de trabajo físicos, las VLAN permiten a un grupo de trabajo lógico compartir un dominio de broadcast. Ello significa que los sistemas dentro de una determinada VLAN reciben mensajes de broadcast desde el resto, independientemente de que residan o no en la misma red física. Por ello, las aplicaciones que requieren tráfico broadcast siguen funcionando en este tipo de redes virtuales. Al mismo tiempo, estos broadcast no son recibidos por otras estaciones situadas en otras VLAN.

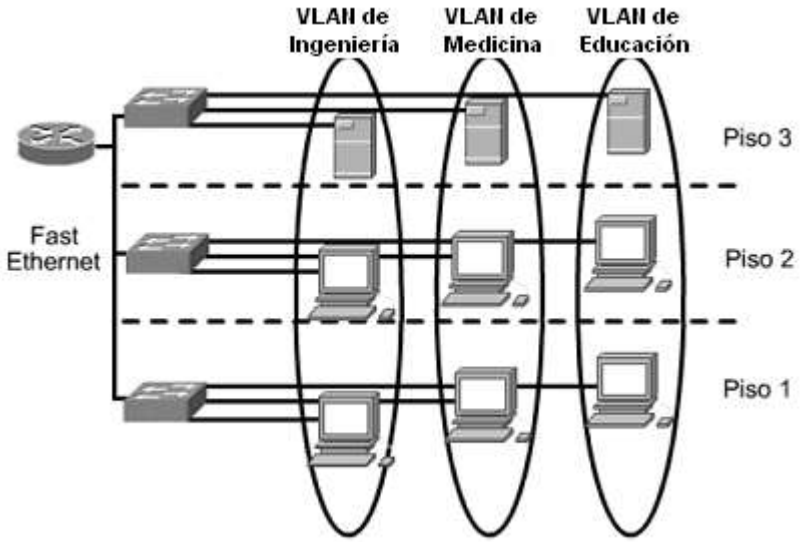


Figura 4.9 Ejemplo de Distribución de una VLAN

Las VLAN no se limitan solo a un conmutador, sino que pueden extenderse a través de varios, estén o no físicamente en la misma localización geográfica (Figura 4.9). Además las redes virtuales pueden solaparse, permitiendo que varias de ellas compartan determinados recursos, como backbones (troncales) de altas prestaciones o conexiones a servidores. Uno de los mayores problemas a los que se enfrentan los administradores de las redes actuales, es la administración de las redes y subredes. Las VLAN tienen la habilidad de usar el mismo número de red en varios segmentos, lo que supone un práctico mecanismo para incrementar rápidamente el ancho de banda de nuevos segmentos de la red sin preocuparse de colisiones de direcciones. Las soluciones tradicionales de internetworking, empleando concentradores y routers, requieren que cada segmento sea una única subred; por el contrario, en un dispositivo con facilidades VLAN, una subred puede expandirse a través de múltiples segmentos físicos, y un solo segmento físico puede soportar varias subredes. Asimismo, hay que tener en cuenta que los modelos más avanzados de conmutadores con funciones VLAN, soportan filtros muy sofisticados, definidos por el usuario o administrador de la red, que permiten determinar con gran precisión las características del tráfico y de la seguridad que deseamos en cada dominio, segmento, red o conjunto de redes. Todo ello se realiza en función de algoritmos de bridging, y routing multiprotocolo.

En el Anexo D se presenta la descripción de una prueba realizada con VLANs en el Laboratorio de Telecomunicaciones de la Universidad del Cauca, que permite entender mejor su funcionamiento en un entorno práctico.

4.4 IDS (SISTEMAS DE DETECCION DE INTRUSOS)

La seguridad en un sistema puede ser clasificada de dos modos: *activa y preventiva*. La *seguridad activa* de un sistema consiste en protegerlo todo lo posible ante potenciales intentos de abuso del mismo. Un Firewall es un buen ejemplo de seguridad activa, trata de filtrar el acceso a ciertos servicios en determinadas conexiones para evitar el intento de forzamiento desde alguno de

ellos. Por otro lado, la *seguridad preventiva* es aquella que se implanta en uno sistema para que informe si en el está teniendo lugar una incidencia de seguridad. No pretende proteger el sistema, pretende alertar de que algo extraño esta sucediendo en el. Un buen ejemplo de seguridad preventiva es un IDS (Intrusion Detection System- Sistema de Detección de Intrusos).

Un sistema de detección de intrusos es aquel que permite recabar información de distintas fuentes del sistema en el que se implanta para alertar de una posible intrusión en las redes o máquinas. La alerta puede ser del hecho de que existe un intento de intrusión, como del modo en el que este se está realizando y en algunos casos por parte de quién esta siendo efectuado. Se puede considerar un sistema de detección de intrusos como un *control de auditoria* que permitirá tomar decisiones a la hora de realizar una auditoria de seguridad de un sistema. Un sistema de detección de intrusos surge como una medida preventiva, nunca como una medida para asegurar los sistemas; ayudan al administrador de dicho sistema a permanecer al tanto de cualquier intención aviesa contra el sistema que administra.

4.4.1 Arquitectura de un Sistema de Detección de Intrusos

Prácticamente todos los sistemas de detección de intrusos tienen ciertas partes bien definidas, como se mencionan a continuación:

- Fuentes de recogida de datos de aplicaciones. Punto de recogida de datos para análisis actual o posterior que bien puede ser una red, el sistema o elementos que residen en el propio sistema.
- Reglas. Estas reglas en muchos casos son las que caracterizan las violaciones que pueden ser cometidas y contra las que se contrastan los datos obtenidos en el punto anterior.
- Filtro. Esta parte se encarga de contrastar las reglas contra los datos obtenidos.
- Detectores de anomalías. En los casos de análisis por anomalías son aquellos que detectan eventos extraños en el sistema o los recursos monitorizados.
- Generador de informes o alarmas. Una vez que se han procesado los datos contra las reglas por el filtro y si existe alguna situación que haga creer que se ha vulnerado o intentado vulnerar la seguridad del sistema, esta parte del detector de intrusos informa al administrador de este hecho (mediante correo, mensajes a móviles, avisos acústicos, etc.).

En la figura 4.10 se puede ver gráficamente como se puede diseccionar la arquitectura de un sistema de detección de intrusos.

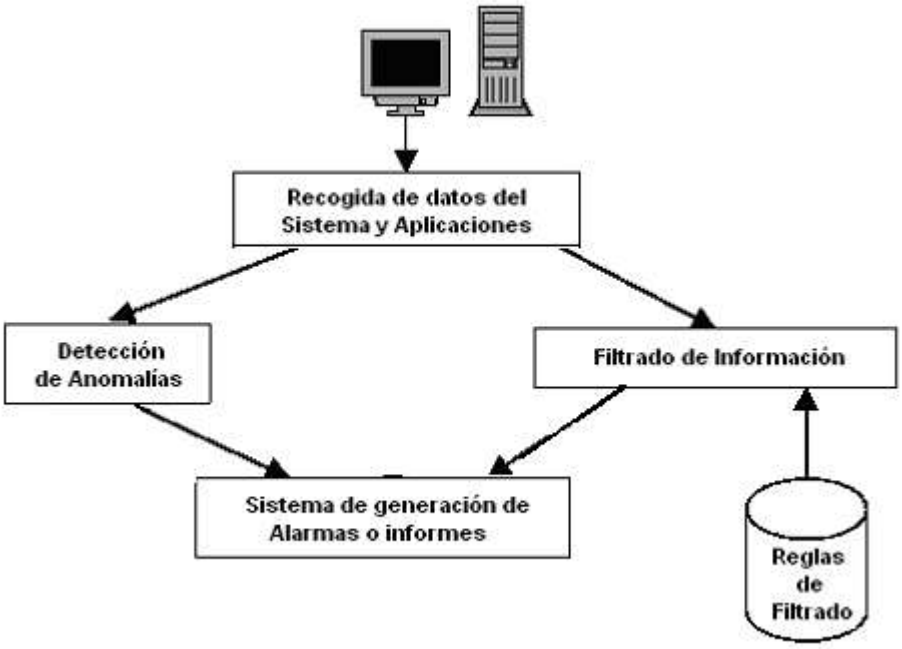


Figura 4.10 Arquitectura de un sistema de detección de intrusos

4.4.2 Tipos de sistemas de detección de intrusos

En este punto es interesante clasificar de algún modo los distintos sistemas de detección de intrusos. Una primera clasificación puede ser entre *sistemas en tiempo real* y aquellos que no lo son. Los sistemas en tiempo real permanecerán constantemente chequeando el sistema buscando alguna señal de un incidente de seguridad e inmediatamente provocarán una alarma. Por otro lado, los sistemas de detección de intrusos que no son de este tipo se usan generalmente cuando existe la creencia de que estamos ante un incidente de seguridad y se usan para recabar información del tipo y alcance de esta incidencia, generalmente sobre registros o información del sistema.

Una clasificación más rigurosa se puede realizar según los medios que utilizan los sistemas de detección de intrusos para monitorizar las incidencias. Se tienen, según esta clasificación cuatro tipos de sistemas:

- *Basados en la red (NIDS-Net IDS):* Sistemas que observan el tráfico de red buscando algún indicio de un ataque conocido. Generalmente una interfaz en modo promiscuo buscando datos sobre una red (suelen pertenecer también al tipo de tiempo real). Un IDS basado en red monitoriza los paquetes que circulan por la red en busca de elementos que denoten un ataque contra alguno de los sistemas ubicados en ella; el IDS puede situarse en cualquiera de los hosts o en un elemento que analice todo el tráfico (como un HUB o un enrutador). Esté donde esté, monitorizaría diversas máquinas y no una sola: esta es la

principal diferencia con los sistemas de detección de intrusos basados en host. Estos IDSs actúan sobre una red capturando y analizando paquetes, es decir, son sniffers del tráfico de red. Luego analizan los paquetes capturados, buscando patrones que supongan algún tipo de ataque. Bien ubicados, pueden analizar grandes redes y su impacto en el tráfico suele ser pequeño. Actúan mediante la utilización de un dispositivo de red configurado en modo promiscuo (analizan todos los paquetes que circulan por un segmento de red aunque estos nos vayan dirigidos a un determinado equipo). Analizan el tráfico de red, normalmente, en tiempo real. No sólo trabajan a nivel TCP/IP, también lo pueden hacer a nivel de aplicación.

Por el tipo de respuesta pueden clasificarse en:

- ✓ Pasivos: Son aquellos IDS que notifican a la autoridad competente o administrador de la red mediante el sistema que sea, alerta, etc., pero no actúa sobre el ataque o atacante.

- ✓ Activos: Generan algún tipo de respuesta sobre el sistema atacante o fuente de ataque como cerrar la conexión o enviar algún tipo de respuesta predefinida en la configuración.

- *Basados en el host (HIDS-Host IDS):* Estos sistemas recaban información del sistema para realizar un análisis de las posibles incidencias pero siempre desde el punto de vista del propio sistema y con sus recursos. Mientras que los sistemas de detección de intrusos basados en red operan bajo todo un dominio de colisión, los basados en máquina realizan su función protegiendo un único sistema; de una forma similar a como actúa un escudo antivirus residente en MS-DOS, el IDS es un proceso que trabaja en background (o que despierta periódicamente) buscando patrones que puedan denotar un intento de intrusión y alertando o tomando las medidas oportunas en caso de que uno de estos intentos sea detectado. Fueron los primeros IDS en desarrollar por la industria de la seguridad informática.

Algunos autores dividen el grupo de los sistemas de detección de intrusos basados en el host, en tres subcategorías:

- ✓ Verificadores de integridad del sistema (SIV): Un verificador de integridad no es más que un mecanismo encargado de monitorizar archivos de una máquina en busca de posibles modificaciones no autorizadas; por norma general, backdoors dejadas por un intruso (por ejemplo, una entrada adicional en el archivo de contraseñas o un /bin/login que permite el acceso ante cierto nombre de usuario no registrado). La importancia de estos mecanismos es tal que en la actualidad algunos sistemas Unix vienen con verificadores de integridad, como Solaris y su ASET (Automated Security Enhancement Tools).

- ✓ Monitores de registros (LFM): Estos sistemas monitorizan los archivos de log generados por los programas (generalmente demonios de red) de una máquina en busca de patrones que puedan indicar un ataque o una intrusión. Los más habituales utilizados en sistemas Unix son los pequeños shellscripts que casi todos los administradores realizan para comprobar

periódicamente sus archivos de log en busca de entradas sospechosas (por ejemplo, conexiones rechazadas en varios puertos provenientes de un determinado host, intentos de entrada remota como root, etc.).

- ✓ Sistemas de decepción: Los sistemas de decepción o tarros de miel (honeypots), como Deception Toolkit (DTK), son mecanismos encargados de simular servicios con problemas de seguridad de forma que un pirata piense que realmente el problema se puede aprovechar para acceder a un sistema, cuando realmente se está aprovechando para registrar todas sus actividades. Se trata de un mecanismo útil en muchas ocasiones (por ejemplo, para conseguir entretener al atacante mientras se rastrea su conexión), pero que puede resultar peligroso, si no se conocen todas las debilidades del sistema.

- *Basados en la aplicación:* Estos recaban datos de una aplicación activa en el sistema (por ejemplo los logs) y buscan evidencias en estos datos. La diferencia con los basados en host es que estos los propios recursos son detectores de intrusos y en el caso de aplicación los datos han de ser filtrados para ser tratados como alarmas.

- *Basados en el objetivo:* Estos monitores se basan en salvaguardar la integridad del objetivo que podría ser cualquier recurso del sistema (por ejemplo el sistema de archivos).

Otra gran clasificación de los IDSs se realiza en función de cómo actúan estos sistemas; actualmente existen dos grandes técnicas de detección de intrusos: las basadas en la Detección de Anomalías (Anomaly Detection) y las basadas en la Detección de Usos Indebidos del Sistema (Misuse Detection):

- *Detección de alguna anomalía:* Se busca sobre el sistema alguna anomalía que pueda hacer creer que hay un incidente de seguridad, pero que puede no ser provocada por esto. La base del funcionamiento de estos sistemas es suponer que una intrusión se puede ver como una anomalía del sistema, para lo que se necesitaría establecer un perfil del comportamiento habitual de los sistemas para ser capaces de detectar las intrusiones por pura estadística: probablemente una intrusión sería una desviación excesiva de la media del perfil de comportamiento.

- *Detección de uso inadecuado:* En estos casos el sistema busca un patrón de un ataque bien definido. El funcionamiento de los IDSs basados en la detección de usos indebidos presupone que se pueden establecer patrones para los diferentes ataques conocidos y algunas de sus variaciones; mientras que la detección de anomalías conoce lo normal (en ocasiones se dice que tienen un Conocimiento Positivo, Positive Knowledge) y detecta lo que no lo es, este esquema se limita a conocer lo anormal para poderlo detectar (Conocimiento Negativo, Negative Knowledge).

4.4.3 Dónde colocar el IDS

Una actitud paranoica podría llevar a instalar un IDS en cada host ó en cada tramo de red. Esto último sería un tanto lógico cuando se trata de grandes redes, pero no es el caso ahora. Lo lógico sería instalar el IDS en un dispositivo por donde pase todo el tráfico de red que se quiere proteger.

Un problema de los IDS es cuando se desea implementarlos en redes conmutadas ya que no hay segmento de red por donde pase todo el tráfico. Otro problema para un IDS son las redes con velocidades de tráfico muy altas en las cuales es difícil procesar todos los paquetes. Si se coloca el IDS antes de los cortafuegos se podrá capturar todo el tráfico de entrada y salida de la red. La posibilidad de falsas alarmas es grande. La colocación detrás del cortafuego monitorizará todo el tráfico que no sea detectado y parado por el Firewall, por lo que será considerado como malicioso en un alto porcentaje de los casos. La posibilidad de falsas alarmas es muy inferior.

Algunos administradores de sistemas colocan dos IDS, uno delante y otro detrás del cortafuegos para obtener información exacta de los tipos de ataques que recibe una red ya que si el cortafuegos está bien configurado puede parar o filtrar muchos ataques.

En ambientes más sencillos, se puede colocar el IDS en la misma máquina que los cortafuegos. En este caso actúan en paralelo, es decir, el Firewall detecta los paquetes y el IDS los analizaría.

4.5 AUTENTICACIÓN

4.5.1 Autenticación Basada en Puerto, Estándar IEEE 802.1x

El estándar IEEE 802.1x define el control de acceso a redes basadas en puertos. Gracias a él se exige autenticación antes de dar acceso a las redes Ethernet. En el control de acceso a redes basadas en puertos se utilizan los elementos físicos que componen una infraestructura de conmutación de la red LAN para autenticar los dispositivos agregados al puerto de conmutación. No se pueden enviar ni recibir tramas en un Puerto de conmutación Ethernet si el proceso de autenticación ha fallado. A pesar de que se diseñó para redes Ethernet fijas, este estándar se ha adaptado para su uso en redes LAN inalámbricas con IEEE 802.11. Windows XP soporta la autentificación IEEE 802.1x para todos los adaptadores de red basados en redes LAN, incluyendo las Ethernet y las inalámbricas, mientras que Windows 2000 debe actualizarse al Service Pack 3 como mínimo y habilitar el soporte 802.1x, como se mostrará más adelante. Para los sistemas operativos basados en Linux, deben instalarse paquetes adicionales que implementen los protocolos del estándar.

El estándar IEEE 802.1x define los términos siguientes:

- El PAE

El Puerto PAE (Port Access Entity), también denominado Puerto LAN, es una entidad lógica que soporta el protocolo IEEE 802.1x asociado con un puerto físico. Un Puerto físico LAN puede hacer las veces de autenticador, el solicitante o ambos.

- El Autenticador

Es un Puerto LAN que exige autenticación antes de permitir el acceso a los Servicios que se suministran a través de él. Para las conexiones inalámbricas, el Autenticador es el Puerto lógico de la LAN en un Punto de Acceso (AP) inalámbrico a través del cual los clientes que trabajan con conexiones inalámbricas acceden a la red fija.

- El Puerto solicitante

El Puerto Solicitante es un puerto de la LAN que solicita acceso a los servicios disponibles a través del Autenticador. En las conexiones inalámbricas, el demandante es el Puerto lógico de la LAN alojado en el adaptador de red LAN inalámbrica que solicita acceso a una red fija. Para ello se asocia y después se autentifica con un Autenticador. Independientemente de que se utilicen para conexiones inalámbricas o en redes Ethernet fijas, los puertos solicitante y de autenticación están conectados a través de un segmento LAN punto a punto lógico y físico.

- El Servidor de Autenticación

Para corroborar los credenciales del Puerto Solicitante, el de autenticación utiliza el servidor de autenticación. Este servidor comprueba los credenciales del solicitante en nombre del Autenticador y después le responde a éste indicándole si el solicitante tiene o no permiso para acceder a los Servicios que proporciona el Autenticador. Hay dos tipos de servidor de autenticación:

- Un componente del punto de acceso: Debe configurarse utilizando los credenciales de los clientes que intentan conectarse. Normalmente no se implementan utilizando puntos de acceso inalámbricos.
- Una entidad distinta: El punto de acceso reenvía los credenciales de la conexión que ha intentado establecerse a un servidor de autenticación distinto. Por lo general un punto de acceso inalámbrico utiliza el protocolo de autenticación remota RADIUS (Remote Authentication Dial-In User Service) para enviar los parámetros de las conexiones que han intentado conectarse al servidor RADIUS (Figura 4.11).

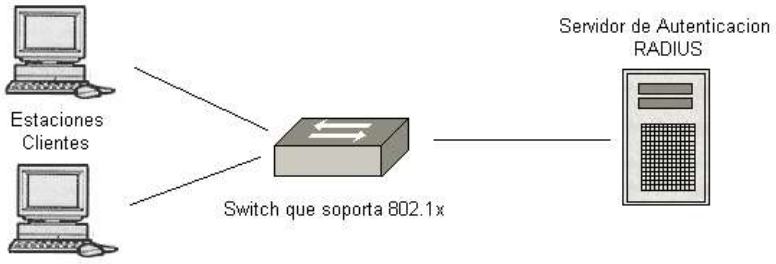


Figura 4.11 Autenticación utilizando un Servidor RADIUS

4.5.1.1 Puertos de acceso sin y con autenticación

El control de acceso basado en el Autenticador define los siguientes tipos de puertos lógicos que acceden a la LAN conectada físicamente a través de un solo puerto LAN fijo:

- *Puerto de acceso sin autenticación*:

El Puerto de acceso sin autenticación hace posible el intercambio de datos entre el autenticador (el switch fijo con soporte 802,1x o el AP inalámbrico) y otros dispositivos dentro de la red fija, independientemente de que se haya autorizado o no al cliente la utilización de la conexión inalámbrica. Un ejemplo ilustrativo es el intercambio de mensajes RADIUS entre un punto de acceso inalámbrico y un servidor RADIUS alojado en una red fija que ofrece autenticación y autorización a las conexiones inalámbricas. Cuando un usuario de una conexión envía una trama, el punto de acceso inalámbrico nunca la reenvía a través del puerto de acceso sin autenticación.

- *Puerto de acceso con autenticación*:

Gracias al Puerto de acceso con autenticación se pueden intercambiar datos entre un usuario de una red inalámbrica y la red física pero sólo si el usuario de la red inalámbrica ha sido autenticado. Antes de la autenticación, el conmutador se abre y no se produce el reenvío entre el usuario de la conexión inalámbrica y el de la red física. Una vez que la identidad del usuario remoto se ha comprobado a través de IEEE 802.1x, se cierra el conmutador y las tramas son reenviadas entre el usuario de la red inalámbrica y los nodos de la red con conexión física. En la figura 4.12 se puede ver la relación que se establece entre los Puertos con y sin autenticación en un punto de acceso inalámbrico.

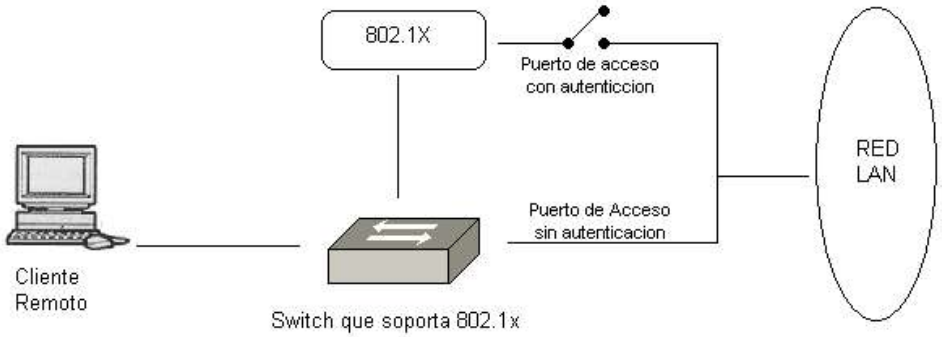


Figura 4.12 Puertos con y sin autenticación

En el conmutador Ethernet de autenticación, el usuario de una red Ethernet puede enviar tramas Ethernet a una red también fija tan pronto como se haya finalizado el proceso de autenticación. El conmutador identifica el tráfico de un usuario de red Ethernet en particular utilizando para ello el Puerto físico al que se conecta a ese usuario. Por lo general sólo se conecta a un usuario de Ethernet

a un Puerto físico a través de un conmutador Ethernet. Debido a las reticencias de muchos clientes remotos ante la idea de consultar y enviar datos utilizando un único canal, se ha tenido que ampliar el protocolo básico IEEE 802.1x. De esta forma un AP inalámbrico o un switch pueden identificar si el tráfico de un determinado cliente remoto es seguro. Esto es posible gracias al establecimiento por ambas partes, tanto del cliente remoto como del punto de acceso de una clave única y especifica para cada cliente. Sólo aquellos clientes remotos que hayan sido autenticados tienen una clave única y específica para cada sesión. Si la autenticación no viene acompañada de una clave válida, el punto de acceso rechaza las tramas que envía el cliente remoto sin autenticación.

4.5.1.2 Protocolo de autenticación extensible (EAP)

Para poder ofrecer un mecanismo de autenticación estándar para 802.1x, la IEEE escogió el protocolo de autenticación extensible (EAP). EAP es un protocolo basado en la tecnología de autenticación del Protocolo Punto a Punto (PPP) que previamente se había adaptado para su uso en segmentos de redes LAN punto a punto. En un principio los mensajes EAP se definieron para ser enviados como la carga de las tramas PPP, de ahí que el estándar IEEE 802.1x defina EAP sobre la red LAN (EAPOL). Este método se utiliza para encapsular los mensajes EAP y así poder enviarlos ya sea a través de segmentos de redes Ethernet o de redes LAN inalámbricas. Los mensajes intercambiados se ilustran en la figura 4.13.

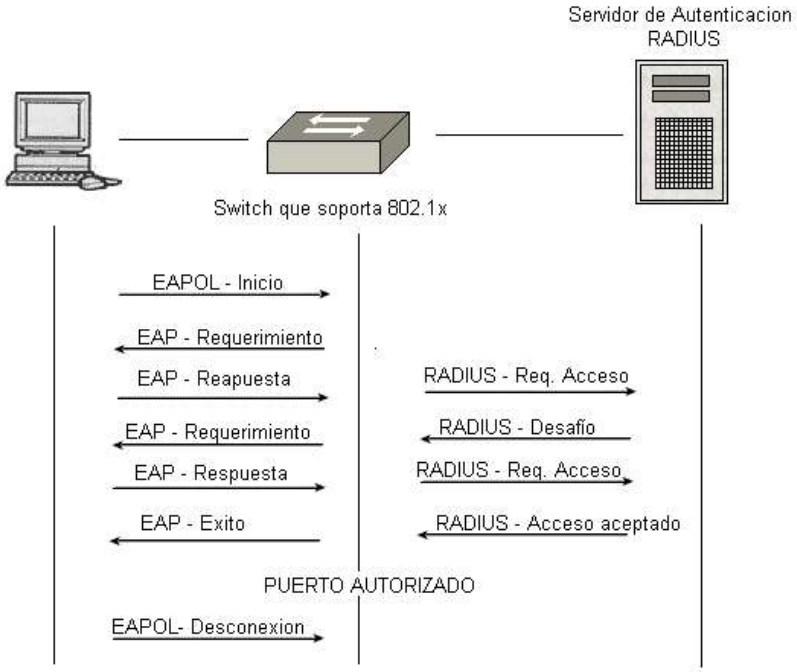


Figura 4.13 Mensajes intercambiados utilizando EAP sobre una red LAN

EAP utiliza el Network Access Server (Autenticador) para abrir un túnel para la autenticación del servidor a través de la red; 802.1x define un número términos especiales:

- Un cliente que pide autenticarse se conoce como *Suplicante*.
- El servidor que autentifica al cliente se conoce como *Servidor de Autenticación*.
- El dispositivo intermediario entre estas dos entidades es el *Network Authentication Server* (NAS) o *Autenticador*. El cual puede ser un punto de acceso o un switch.

EAP define una variedad de métodos autenticación. EAP/MD5 transfiere hash con el nombre del usuario, su contraseña y una cadena arbitraria. El servidor utiliza la clave en texto claro cadena arbitraria para generar su propio hash, el cual se compara con la entrante. Este método es simple, pero es seguro contra ataques tipo diccionario (donde se pretende descifrar la clave basándose en palabras muy utilizadas). Además, en una wireless es imposible crear claves WEP dinámicas utilizando EAP/MD5. Por tanto, este método sólo está indicado para pequeñas redes cableadas. Con la segunda variante, EAP tanto el servidor como el cliente necesitan certificados X.509. Este método es muy seguro, pero implica tener un (Public Key Infrastructure) en funcionamiento. Un tercer método es el Protected Extensible Autentication Protocol; con PEAP, sólo el servidor necesita un certificado para establecer una conexión TLS y enviar el nombre de usuario la contraseña encriptados (MSCHAPv2, Microsoft Challenge Handshake Authentication Protocol). Los administradores sólo necesitan instalar el certificado servidor en cada cliente. Cuando los clientes salen del sistema o cierran la conexión, PEAP detecta el cambio y finaliza la autorización, cerrando las conexiones por ambos lados. En redes sólo cableadas, EAP/MD5 es a menudo la mejor opción. Esto es todo lo que se necesita para asignar dinámicamente VLANs y, a diferencia de PEAP, es un protocolo soportado por una gran variedad de switches. Además de esto, el complicado esfuerzo administrativo es mucho menor que con PEAP o EAP/MD5.

Un switch normalmente proporciona funcionalidad NAS, traduciendo el protocolo EAPOL (EAP sobre LAN) desde el suplicante al servidor RADIUS, que es lo que el servidor de acceso espera. La mayoría de los dispositivos dan esta opción cuando se configura 802.1x. Se debe configurar la dirección y la clave para el servidor Radius. En muchos casos es aconsejable configurar múltiples servidores para proporcionar altos niveles de disponibilidad y ofrecer una solución alternativa en caso de que el servidor principal se caiga.

En el Anexo D se presenta una prueba realizada para ilustrar el funcionamiento en un entorno práctico de la Autenticación por medio de un servidor RADIUS utilizando switches Cisco Catalyst 2950. En el Anexo E se presenta un complemento a este capítulo y una introducción a otros Mecanismos de Seguridad en Redes IP, como Web Security, Router Security, Acceso Remoto y Registros y Auditoría, también importantes ya que constituyen una buena solución para una propuesta de Seguridad completa en una red.

Resumen

En este capítulo se han presentado las principales características de los mecanismos de seguridad que se consideraron de mayor importancia para su implementación en una red. El siguiente capítulo muestra las prácticas realizadas con el Protocolo IPSec en el

Laboratorio de Telecomunicaciones de la Universidad del Cauca y las distintas herramientas que permiten su implementación en redes IPv4 en entornos Linux y Windows.

CAPITULO V. IMPLEMENTACION DE LOS PROTOCOLOS DE SEGURIDAD DE IPv6 EN REDES IPv4 EN ENTORNOS LINUX Y WINDOWS

En este capitulo se plantean algunas prácticas para fortalecer los conceptos estudiados en el capítulo 3, acerca de los protocolos de seguridad de IPv6 y su implementación en redes IPv4; si se desea, pueden consultarse los respectivos RFCs para más información: Arquitectura de Seguridad para IP (RFC 2401), Cabecera de Autenticación IP (RFC 2402), Cifrado de Datos IP (RFC 2406), Asociaciones de Seguridad y Protocolo de Gestión de Claves en Internet - ISAKMP (RFC 2408).

En la actualidad, es fácil encontrar diversas herramientas que permiten implementar la seguridad del Protocolo IPv6 en el mundialmente utilizado Protocolo IPv4, algunas de ellas de uso libre, otras, propiedad de reconocidas empresas del medio. Todas coinciden en la utilización del Protocolo IPSec como base de la implementación de seguridad que ofrecen. En las prácticas que se presentan a continuación, se consideran las herramientas más utilizadas en el momento sobre la plataforma Linux y la forma de implementación de Seguridad sobre Windows.

5.1 PRACTICAS PARA LA IMPLEMENTACION DE SEGURIDAD A NIVEL DE RED UTILIZANDO LAS HERRAMIENTAS DEL PROYECTO USAGI SOBRE LINUX

5.1.1 Proyecto USAGI

USAGI (UniverSAl playGround for IPv6)[1] es un proyecto japonés que trabaja para desarrollar y mejorar la calidad del stack de Protocolos IPv6 e IPSec (tanto en IPv4 como en IPv6) sobre sistemas Linux, de la mano de otros proyectos como WIDE[2], KAME y TAHI[3] project. USAGI está compuesto por voluntarios de varias organizaciones de Japón, pero al mismo tiempo recibe respaldo de organizaciones y personas alrededor del mundo; su desarrollo se ha basado desde el principio en el proyecto FreeS/WAN, pero tienen ciertas diferencias que se observarán más adelante. El objetivo principal de USAGI es contribuir a la comunidad Linux y a la comunidad IP para el desarrollo del Stack IPv6, por medio de algunas modificaciones en el kernel, las librerías y algunas aplicaciones. De esta forma se está consiguiendo un producto libre para ser utilizado por la comunidad Linux e IPv6, además se trabaja en la forma

[1] Proyecto USAGI (UniverSAl playGround for IPv6). http://www.linux-ipv6.org/
[2] Proyecto WIDE (Widely Integrated Distributed Enviroment). www.wide.ad.jp
[3] Proyecto TAHI www.tahi.org

de modificar el kernel para implementar algunas características de IPv6 como IPSec, sobre IPv4. La idea es, en un futuro cercano, que el código USAGI sea incluido con las principales distribuciones del kernel de Linux y de las librerías glibc.

5.1.2 Práctica 1: Instalación de USAGI STABLE RELEASE 5

5.1.2.1 Motivación

En esta práctica se explicará paso a paso la instalación de las fuentes del paquete USAGI en Linux, y el proceso de recompilación del Kernel. La práctica se probó sobre las plataformas Linux Red Hat 9 y Linux Debian Sarge 3.1 en los equipos del Laboratorio de Telecomunicaciones de la Facultad de Ingeniería Electrónica y Telecomunicaciones de la Universidad del Cauca (sin embargo este proceso es independiente de la distribución de Linux). Para llevar a cabo esta práctica, es necesario un equipo que ejecute el sistema operativo Linux (en este caso se utilizó Linux Debian Sarge 3.1).

5.1.2.2 Objetivo

- Realizar la instalación de la herramienta USAGI en una plataforma Linux, habilitar las opciones del protocolo IPSec y recompilar el kernel para tener el soporte necesario para las prácticas siguientes.

5.1.2.3 Desarrollo de la Práctica

Para implementar IPSec en una plataforma Linux (como ya se mencionó, es independiente de la plataforma) se utilizarán las fuentes del kernel USAGI IPSec, las cuales proveen una implementación de los protocolos AH y ESP para IPv4 e IPv6 basadas en un kernel 2.4.21. De esta forma, USAGI IPSec convierte cualquier equipo Linux en una Gateway Segura IPSec, permitiendo implementar topologías Host to Host, Lan to Lan y soportando los modos Trasporte y Túnel para AH y ESP; para estas prácticas se utilizó el Sistema Operativo Linux Debian Sarge y equipos Dell Optiplex GX110. Se debe obtener la versión estable de las fuentes del kernel USAGI STABLE Release 5, *usagi-linux24-stable-20040104.tar.bz2* desde la siguiente dirección: ftp://ftp.linux-ipv6.org/pub/usagi/stable/kit/.

Una vez descargado el paquete USAGI, se debe descomprimir con este comando:
#tar –jxvf ***ruta-fuentes-USAGI****/usagi-linux24-stable-20040104.tar.bz2 –C /usr/src*

- Primero, antes de comenzar a construir los paquetes, se debe preparar el sistema, por lo que se ingresa al directorio de fuentes del kernel: *#cd /usr/src/usagi/* y se ejecuta el siguiente comando:

#make prepare TARGET=$(TARGET); donde $(TARGET) es *linux24*, conveniente para el sistema.

Luego se ingresa al directorio: #cd /usr/src/usagi/kernel/linux24 y se ejecutan los comandos a continuación:

- Para limpiar las fuentes del kernel antes de compilar:

#make mrproper

- Para configurar el kernel para que soporte IPSec, se ejecutan los siguientes comandos:

#make menuconfig ó #make xconfig

Con el cual es posible escoger las características esenciales para el nuevo kernel; este paso es importante debido a que en este punto se deben escoger las características hardware que posee el equipo, y el tipo de sistemas de archivos que se necesiten. A continuación se muestra una descripción de cada característica:

- ✓ ***Code maturity level options:*** Aquí se debe decidir si se desea que las opciones de configuración incluyan opciones que aun no han sido suficientemente probadas, o que están en fase de desarrollo. A menos que se planee desarrollar, o que se necesite absolutamente alguna de estas funciones, lo recomendable es desactivar esta opción; pero para nuestro caso, debido a que los módulos de IPSec están aún en desarrollo, debe dejarse activa (ver tabla 5.1).

- ✓ ***Loadable module support:*** Los módulos son pequeñas partes de código que pueden ser insertadas en el kernel durante el normal funcionamiento de este; esto permite compilar un kernel más eficiente y pequeño, utilizando funciones que no se utilizan siempre en modo de módulos y activarlos solo cuando se necesitan con los comandos *insmod y rmmod*. Es recomendable activar esta opción a menos que se desee construir un kernel monolítico, es decir, un kernel de una sola pieza (ver tabla 5.1).

- ✓ ***Processor type and features:*** Esta opción permite compilar un kernel específico para el tipo de procesador que se está utilizando; solo se debe seleccionar el tipo correcto. Deshabilite la opción *Multiprocessing support.*

  General setup: Aquí se seleccionan opciones generales acerca del funcionamiento base de Linux, como el soporte PCI, si se desea utilizar la función de gestión de energía del PC (APM=Advanced Power Management) y algunas otras cosas. Se debe escoger solo lo necesario.

  Binary emulation of other systems y Memory Technology Device (MTD) support: Para manejar esta parte es necesario poseer conocimientos especiales, de lo contrario, puede dejarse por defecto.

  Parallel port support: Sólo activo si se tiene o tendrá algún dispositivo conectado al puerto paralelo del PC.

  Plug and Play configuration: Sólo activo si se tiene o tendrá algún dispositivo PNP (plug & play).

- ✓ ***Block devices:*** Soporte para el Floppy, dispositivos de tape backup, discos rígidos antiguos, la interfaz de loopback (absolutamente necesaria) y otras pocas opciones. Habilitar las opciones: *Loopback support, RAM Disk Support* e *Initrd Support.*

  Multi-device support: Solo activo si se está utilizando hardware RAID.

- ***Networking options:*** Aquí se pueden configurar las opciones de networking en general (cada opción tiene un texto de ayuda). Esta es una de las partes más importantes para nuestra configuración; las opciones que se deben habilitar se muestran en la tabla 5.1.

  Telephony Support: Sólo activo si se tienen dispositivos de telefonía conectados al PC.

- ***ATA/IDE/MFM/RLL:*** Soporte para dispositivos ATA/IDE (este tipo de dispositivos es el de más frecuente uso, por ejemplos discos rígidos IDE). Preferiblemente debe estar activado.

  SCSI support: Sólo debe estar activo si se tienen dispositivos SCSI. En general es conveniente dejar esta opción *deshabilitada*.

  Fusion MPT device support: Esta opción puede desactivarse si no se tiene conocimiento acerca de cómo funciona.

  IEEE 1394 (FireWire) support (EXPERIMENTAL): Al igual que en la opción anterior, es conveniente desactivarla.

  I2O device support (Intelligent Input/Output (I2O) architecture)*:* Este tipo de arquitectura piensa en el futuro, la idea es que determinados drivers para determinados dispositivos puedan ser independientes del sistema operativo, siempre y cuando exista el módulo para el Sistema Operativo en cuestión.

- ***Network device support:*** Aquí se selecciona el tipo de dispositivo de conexión a la red que se utiliza y las funciones que se desean activar para ese dispositivo. Si se tiene una conexión tipo dial up (con un modem o RDSI) deben seleccionarse todas las opciones PPP; si se tiene una o más tarjetas de red tipo Ethernet, se deben seleccionar los drivers adecuados en la sección Ethernet (10 or 100Mbit, 1000Mbit). Para saber que dispositivos PCI tiene su equipo, utilice el comando *#lspci.*

  Amateur Radio support: Sólo se activa si se tienen dispositivos de radioaficionado.

  IrDA (infrared) support: Sólo se activa si se cuenta con dispositivos infrarrojos.

  ISDN subsystem: Contiene las opciones necesarias para configurar una conexión ISDN y las tarjetas de red RDSI.

  Old CD-ROM drivers (not SCSI, not IDE): Soporte para dispositivos CD-ROM antiguos.

  Multimedia devices: Configuración para tarjetas de video y radio.
- ***Cryptographic support:*** Permite activar soporte para la encriptación del sistema de archivos y de ciertos protocolos de comunicación (ver las opciones a habilitar en la tabla 5.1).

- ***Filesystems:*** Contiene los Tipos de sistemas de archivos soportados; en general se necesita *soporte para CDROM* (ISO 9660 CDROM y Microsoft Joliet CDROM), soporte para *ext3* y si se interactúa con una partición Windows, *soporte para VFAT.* Se debe habilitar la opción *Ext3 Support* y *Journalling File System*.

- ***Library Routines:*** se recomienda habilitar las opciones *zlib Decompression support* y *Compression support*.

- ***Console drivers:*** En general, la configuración de esta opción puede mantenerse por defecto; se habla de soporte para dispositvos VGA (cualquier monitor actual).

  Sound: En esta opción se selecciona, si se tiene, la tarjeta de sonido.

  USB support: Para seleccionar los dispositivos y drivers USB que se necesiten.

  Bluetooth support: Para configuración de dispositivos Wireless.

Kernel hacking: Estas opciones son necesarias si se necesita realizar un debug del kernel; no es necesario aclarar que se necesitan conocimientos muy avanzados.

A continuación se presentan las opciones **necesarias** para llevar a cabo la configuración de IPSec en un equipo:

Tabla 5.1 Nueva configuración del Kernel con la herramienta USAGI

Grupo	OPCION	SELECCION
Code maturity level options	Prompt for development and/or incomplete code/drivers	[*]
Loadable module support	Enable loadable module support.	[*]
	Set version information on all module symbols	[*]
	Kernel module loader	[*]
Cryptographic support (CryptoAPI)	CryptoAPI support	[*]
	[*] Cipher Algorithms --- 128 bit blocksize	[*]
	AES (aka Rijndael) cipher --- 64 bit blocksize	[*]
	3DES cipher --- Deprecated	[*]
	<*> NULL cipher (NO CRYPTO)	[*]
	<*> DES cipher (DEPRECATED)	[*]
	Digest Algorithms	[*]
	<*> MD5 digest	[*]
	<*> SHA1 digest	[*]
Networking options	Packet socket	[*]
	Network Packet Filtering	[*]
	Socket Filtering	[*]
	Unix domain sockets	[*]
	TCP/IP networking	[*]
	The IPsec protocol (EXPERIMENTAL)	[*]
	▪ IPsec: IPsec Debug messages	[*]
	▪ IPsec: IPsec Debugging off by Default	[*]
	IP: tunneling	[*/M]
	IP: IP Security Support	[*]
	IP: Netfilter Configuration ->	
	▪ IP Tables support	[*]
	▪ Packet Filtering	[*]
	▪ REJECT Target Support	[*]
	▪ Packet Mangling	[*]
	The IPv6 protocol (EXPERIMENTAL)	[*/M]
	▪ IPv6: IP Security Support (EXPERIMENTAL)	[*]
	▪ IPv6: IPv6 over Ipv6 Tunneling (EXPERIMENTAL)	<M>

Cuando se ha terminado de configurar todas las opciones necesarias, deben guardarse los cambios, los cuales se almacenarán en el archivo oculto */usr/src/usagi/linux24/.config* (este archivo puede observarse con el comando *#nano .config*); si en otra ocasión fuera necesario recompilar el kernel y no se desea perder las configuraciones que se han hecho anteriormente, debe guardarse este

archivo fuera de */usr/src/usagi/linux24* antes de hacer *make mrproper* nuevamente, o deberán hacerse las configuraciones de nuevo.

- Ahora para compilar los cambios hechos a la configuración del kernel y compilar los módulos que se han instalado:

#make dep Genera las dependencias de código según las opciones que se seleccionaron en *menuconfig*.
#make clean Para asegurar que no hayan dependencias no resueltas.
#make bzImage Compila el kernel que se encuentra en el archivo */usr/src/usagi/linux24/arch/i386/boot/bzImage.*
#make modules Compila los módulos seleccionados en menuconfig.

- Para instalar el kernel y los módulos:

#make install
#make modules_install

Se debe tener en cuenta que la versión del kernel Usagi instalado es la 2.4.21 en este caso.

- Es necesario crear una imagen inicial RAMDisk:

*#mkinitrd –o /boot/initrd.img-**version** versión*

- Se remueve el enlace simbólico al mapa del kernel, System.map:

#rm /boot/System.map

- Se copia y renombra el nuevo kernel y el System.map:

*#cp arch/i386/boot/bzImage /boot/vmlinuz-**version***
*#cp System.map /boot/System.map-**version***

- Se crea un enlace simbólico al System.map**version**:

*#ln –s /boot/System.map-**version** /boot/System.map*

Se edita el archivo */boot/grub/menu.lst* y se añade una nueva entrada correspondiente a este kernel (en otras plataformas Linux sería el archivo */etc/lilo.conf* o */etc/grub.conf*); por ejemplo (recuerde guardar los cambios realizados al archivo):

```
Title                          Usagi, Kernel 2.4.21
Root                                (hd0,4)
Kernel                  /vmlinuz-2.4.21 root=/dev/hda7 ro
Initrd                         /initrd.img-2.4.21
Save default
Boot
```

- Por último, se compilan e instalan las aplicaciones de usuario (*userland applications*), así:

#cd /usr/src/usagi/usagi
#./configure
#make
#make install

- Ahora ya se puede reiniciar el sistema y seleccionar el nuevo kernel: *#reboot.*

P.1.1 En el boot, escoja el nuevo kernel Usagi 2.4.21. ¿Se llevó a cabo correctamente el reinicio del sistema? En caso contrario, repita los pasos anteriores y verifique la configuración realizada para el nuevo kernel.

- Verifique el estado de las interfaces de red con el comando *#ifconfig,* y compruebe que hay conectividad haciendo ping al router que se encuentra en la Sala de Telecomunicaciones:

#ping 10.200.2.50
#ping 172.16.41.108

5.1.2.4 Componentes de USAGI IPSec

USAGI IPSec provee 2 componentes fundamentales para el funcionamiento de IPSec en Linux:

pfkey: es una utilidad para crear, configurar, eliminar y desplegar de forma manual asociaciones y políticas de seguridad IPSec.

pluto: es una herramienta que permite implementar el protocolo IKE.

De esta forma, IPSEC puede ser configurado manualmente utilizando el comando *pfkey* o puede ser configurado dinámicamente a través del demonio de IKE que facilita *pluto.*

- Para instalar ***pfkey***, se debe ingresar al directorio: *#cd /usr/src/usagi/usagi/pfkey/* y ejecutar los comandos:

#./configure -–with-linux-kernel=/usr/src/usagi/kernel/linux24
#make
#make install

- Para instalar ***pluto*** (IKEd), se ingresa al directorio: *#cd /usr/src/usagi/usagi/pluto* y se ejecuta:

#./configure
#make
#make install

Por defecto, los comandos y utilidades de IPSec se encuentran en */usr/local/v6/sbin* y el archivo de configuración y el archivo del material de claves en */usr/local/v6/etc*, como también los archivos *conf.eg* y *secrets.eg.* IPSec puede ser configurado manualmente usando el comando *pfkey* o puede ser configurado dinámicamente a través del demonio de IKE, *pluto*.

- Para que estos comandos puedan ser utilizados desde cualquier ruta en los directorios, copielos al directorio /usr/bin (estando parado sobre la ruta /usr/local/v6/sbin), así:

#cp pfkey /usr/bin
#cp pluto /usr/bin
#cp whack /usr/bin
#cp ipsec /usr/bin
#cp ipsec.conf /usr/bin

P.1.2 Verifique que todos los comandos estén funcionando correctamente, ejecutándolos desde cualquier ruta y observando que aparezcan sus comandos de ayuda.

5.1.2.5 Conclusiones

5.1.3 Práctica 2: Configuración de IPSec en Modo Transporte

5.1.3.1 Motivación

En esta práctica se busca comprender el funcionamiento de las Asociaciones y Políticas de Seguridad en su configuración en Modo Transporte utilizando los protocolos de Seguridad AH y ESP. Esta práctica se divide en dos fases:

- Fase 1: Configuración del Modo Trasporte de forma Manual.
- Fase 2: Configuración del Modo Trasporte de forma Automática.

Para llevar a cabo esta práctica, es necesario el siguiente hardware:

- Dos equipos que ejecuten el sistema operativo Linux (en este caso se utilizó Linux Debian), con soporte USAGI IPSec instalado.
- Una LAN o una WAN para conectar estos dos equipos.

5.1.3.2 Objetivos

- Habilitar AH y/o ESP en Modo Transporte de forma manual.
- Habilitar AH y/o ESP utilizando el intercambio automático de claves.

5.1.3.3 Desarrollo de la Práctica

El escenario utilizado en esta prueba se muestra a continuación (figura 5.1):

10.0.1.1/16

10.0.2.1/16

Figura 5.1 Escenario de Prueba Modo Trasporte Host to Host con direcciones IPv4

En el escenario de prueba se debe tener en cuenta la siguiente información:

Modo: transporte AH/ESP
Algoritmo AH: hmac-md5 (Clave: 0x0123456789abcdef0123456789abcdef)
Algoritmo de Autenticación ESP: HMAC-MD5
(Clave: 0x0123456789abcdef0123456789abcdef)
Algoritmo de cifrado ESP: 3DES-CBC
(Clave: 0xa7a36ebd91863edfba763fa7edcba64d89123ace6359eba7)
SPI: A -> B AH:0x1234 ESP:0x5678, B -> A AH:0x9abc ESP:0xdef0

- *FASE 1: Configuración de IPSec en Modo Trasporte de forma Manual*

La configuración manual se llevará a cabo con direcciones IPv4 e IPv6 para demostrar que para implementar IPSec en cualquiera de las dos versiones del protocolo IP, solo basta con cambiar las direcciones, ya que el concepto de funcionamiento es el mismo.

En el Host A se realiza la siguiente configuración:

#ifconfig eth0 10.0.1.1 netmask 255.255.0.0

a) Tráfico desde el Host A hacia el Host B:

Asociación de Seguridad para AH:
pfkey -A sa -s 10.0.1.1 -d 10.0.2.1 -T ah -S 0x1234 --auth hmac-md5 -- authkey 0x0123456789abcdef0123456789abcdef

Asociación de Seguridad para ESP:
pfkey -A sa -s 10.0.1.1 -d 10.0.2.1 -T esp -S 0x5678 --auth hmac-md5 --authkey 0x0123456789abcdef0123456789abcdef --esp 3des-cbc –espkey 0xa7a36ebd91863edfba763fa7edcba64d89123ace6359eba7

Política de Seguridad para AH:
pfkey -A sp -s 10.0.1.1 -d 10.0.2.1 -T ah -S 0x1234

Política de Seguridad para ESP:
pfkey -A sp -s 10.0.1.1 -d 10.0.2.1 -T esp -S 0x5678

b) Tráfico desde el Host B hacia el Host A:

Asociación de Seguridad para AH:
pfkey -A sa -d 10.0.1.1 -s 10.0.2.1 -T ah -S 0x9abc --auth hmac-md5 --authkey 0x0123456789abcdef0123456789abcdef

Asociación de Seguridad para ESP:
pfkey -A sa -d 10.0.1.1 -s 10.0.2.1 -T esp -S 0xdef0 –auth hmac-md5 --authkey 0x0123456789abcdef0123456789abcdef --esp 3des-cbc --espkey 0xa7a36ebd91863edfba763fa7edcba64d89123ace6359eba7

Política de Seguridad para AH:
pfkey -A sp -d 10.0.1.1 -s 10.0.2.1 -T ah -S 0x9abc

Política de Seguridad para ESP:
pfkey -A sp -d 10.0.1.1 -s 10.0.2.1 -T esp -S 0xdef0

- Ahora, de igual forma debe hacerse en el Host B:

#ifconfig eth0 10.0.2.1 netmask 255.255.0.0

a) Fijar el tráfico desde el Host A hacia el Host B

b) Fijar el tráfico desde el Host B hacia el Host A

- Verifique que las asociaciones y políticas de seguridad se han establecido de forma satisfactoria, utilizando el comando # *ipsec-conf show.*

- Guarde la configuración de las asociaciones y de las políticas de seguridad establecidas utilizando el comando *#ipsec-conf save <nombre-del-archivo>*.

- Es posible recuperar la configuración de las asociaciones y de las políticas de seguridad que se guardaron en el archivo <nombre-del-archivo> utilizando el comando: *#ipsec-conf restore <nombre-del-archivo>.*

Algunos de los comandos que se pueden utilizar con *pfkey* para ver la configuración son:

pfkey -L: para desplegar el estado de las Asociaciones y las Políticas establecidas.

 # pfkey -F any: para borrar todas las asociaciones y políticas de seguridad.
 # pfkey -D ...: para borrar una entrada de Asociación o Política de Seguridad.
 # pfkey --help: para desplegar información de ayuda.

P.2.1 Desde el HostA haga *ping* hasta el HostB. ¿Qué sucede?

- Utilice el analizador de Protocolos de red Ethereal desde otro computador para identificar los tipos de mensajes que recibe el HostB. Utilice el siguiente filtro: *!arp && host 10.0.2.1*

P.2.2 Describa el formato del paquete capturado por Etherealy los campos más importantes de cada encabezado.

P.2.3 Elimine las Asociaciones y las Políticas de Seguridad en el HostA utilizando el comando *#pfkey –F any o #ipsec-conf reset*. Confirme que la configuración haya sido borrada con el comando *#ipsec-conf show*. Haga un ping desde el HostA al HostB; ¿Qué sucede?

- Elimine la configuración de las asociaciones y políticas de seguridad en el HostB. Haga *ping* nuevamente desde el HostA al HostB.

P.2.4 ¿Qué sucede y cual es la diferencia que observa en los paquetes capturados con Ethereal?

P.2.5 Cambie las direcciones de los Hosts por direcciones IPv6. Repita el proceso anterior cambiando las direcciones IPv4 por las nuevas direcciones IPv6 como se muestra en la figura 5.2, para configurar las Asociaciones y Políticas de Seguridad entre los dos Host. Desde el HostA haga *ping6* hasta el HostB. Realice las pruebas respectivas.

3ffe:8070:1024:1::7/64 3ffe:8070:1024:1::15/64

Figura 5.2 Escenario de Prueba Modo Trasporte con direcciones IPv6

- Para asignar las direcciones IPv6 en Linux Debian, se añaden las siguientes líneas al archivo */etc/network/interfaces* así:

```
iface eth0 inet6 static
                        address 3ffe:8070:1024:1::7
                                netmask 64
```

De igual forma que para IPv4, debe tenerse en cuenta la siguiente información para crear las Asociaciones y Políticas de Seguridad:

Modo: transporte AH/ESP
Algoritmo AH: hmac-md5 (Clave: 0x0123456789abcdef0123456789abcdef)
Algoritmo de Autenticación ESP: HMAC-MD5
(Clave: 0x0123456789abcdef0123456789abcdef)
Algoritmo de cifrado ESP: 3DES-CBC
(Clave: 0xa7a36ebd91863edfba763fa7edcba64d89123ace6359eba7)
SPI: A -> B AH:0x1234 ESP:0x5678, B -> A AH:0x9abc ESP:0xdef0

P.2.6 Qué diferencias encuentra con respecto a los paquetes capturados con las direcciones IPv4 y las direcciones IPv6?

- *FASE 2: Configuración de IPSec en Modo Trasporte de forma Automática*

Para implementar el demonio de IKE (IKEd), USAGI se basa en la implementación realizada para pluto en el proyecto FreeS/WAN, pero sin embargo, se encuentran ciertas diferencias:

- La ruta por defecto del archivo ipsec.conf se ha cambiado a: /usr/local/v6/etc/ipsec.conf.

- Pluto de USAGI no utiliza scripts, y soporta DES.

- Tiene soporte para utilizar cifrado ESP sin autenticación ESP.

- Soporte para USAGI IPSec tanto en modo túnel como en modo transporte.

- Soporte para transporte IPv4/IPv6.

Las prácticas en este caso se harán con direcciones IPv4. La configuración es totalmente la misma que al utilizar direcciones IPv6, como se demostró en la Fase 1. Recuerde borrar las asociaciones y políticas definidas anteriormente, con el comando *#pfkey –F any.*

a) Utilizando IKEd en Configuración Manual

Los dos comandos que utiliza IKEd son "*pluto*" and "*whack*". *pluto* es un demonio que corre el protocolo IKE. *whack* es un comando usado para comunicarse con pluto cuando éste está corriendo.

- Asigne a cada Host la dirección IP respectiva, así:

HostA:

#ifconfig eth0 10.0.1.1 netmask 255.255.0.0

HostB:

#ifconfig eth0 10.0.2.1 netmask 255.255.0.0

La secuencia que debe seguirse para configurar IPSec por este método se describe a continuación:

- Se define una llave pre-compartida **en ambos hosts**, utilizando el siguiente formato, y se guarda en el archivo /usr/local/v6/etc/ipsec.secrets, que es la ruta por defecto:

```
10.0.1.1 10.0.2.1 : PSK "Prueba IPv4"
```

- Se corre pluto:

  # pluto

- Se chequea si *pluto* está corriendo o no con el comando *#ps ax* o verificando si se encuentra corriendo en *#ls /var/run*; si se encuentra el archivo *pluto.pid*, significa que *pluto* está corriendo.

- Inicie el Analizador de Protocolos Ethereal en un equipo diferente a los involucrados en la configuración, para que capture los paquetes que se intercambian entre los Host. Utilice el siguiente filtro: *!arp && host 10.0.2.1*

- En ambos Hosts, se configura IKE utilizando el comando *whack*. El parámetro después de –name es el nombre de la configuración. Este parámetro es usado para inicializar, parar y borrar una configuración. El nombre de la configuración para este ejemplo es "pruebaipv4".

  ✓ Si se quiere usar solo Autenticación

 # whack --name pruebaipv4 –ipv4 --host 10.0.1.1 --to -–host 10.0.2.1 –authenticate

Inicie Ethereal en otro equipo, para capturar los paquetes intercambiados; para hacer el establecimiento de la conexión segura se procede en los dos host así:

- Para hacer que el demonio de *pluto* comience a chequear la interface y revise el archivo *ipsec.secrets* para obtener las llaves de autenticación:

 # whack --listen

- Para iniciar el intercambio de llaves utilizando el nombre de la configuración:

 # whack --initiate --name pruebaipv4

- Para ver la información de asociaciones y políticas de seguridad definidas:

#ipsec-conf show

P.2.7 Observe los paquetes capturados por Ethereal y describa los paquetes intercambiados durante la negociación de IKE.

P.2.8 Haga un ping desde uno de los host, hacia el otro, pero antes verifique que Ethereal se haya inicializado en otro equipo para que capture los paquetes. ¿La respuesta al ping es satisfactoria? Describa los paquetes capturados.

- La forma de terminar una conexión, es finalizar la sesión IPSec entre los hosts, borrar la configuración establecida y detener el demonio de *pluto* que está corriendo, así:

whack--terminate--name pruebaipv4; para terminar IPSec entre los hosts.
whack--delete--name pruebaipv4; para borrar la configuración.
whack–shutdown; para detener *pluto*.

- ✓ Si se desea usar solo Cifrado

 # whack --name pruebaipv4 –ipv4 --host 10.0.1.1 --to -–host 10.0.2.1 –encrypt

Inicie Ethereal en otro equipo, para capturar los paquetes intercambiados; para hacer el establecimiento de la conexión segura se procede en los dos host así:

- Para hacer que el demonio de *pluto* comience a chequear la interface y revise el archivo *ipsec.secrets* para obtener las llaves de autenticación:

 # whack --listen

- Para iniciar el intercambio de llaves utilizando el nombre de la configuración:

 # whack --initiate --name pruebaipv4

- Para ver la información de asociaciones y políticas de seguridad definidas:

#ipsec-conf show

P.2.9 Observe los paquetes capturados por Ethereal y describa los paquetes intercambiados durante la negociación de IKE.

P.2.10 Haga un ping desde uno de los host, hacia el otro, pero antes verifique que Ethereal se haya inicializado en otro equipo para que capture los paquetes. ¿La respuesta al ping es satisfactoria? Describa los paquetes capturados.

- La forma de terminar una conexión, es finalizar la sesión IPSec entre los hosts, borrar la configuración establecida y detener el demonio de *pluto* que está corriendo, así:

whack--terminate--name pruebaipv4; para terminar IPSec entre los hosts.
whack--delete--name pruebaipv4; para borrar la configuración.
whack–shutdown; para detener *pluto*.

- ✓ Si se quiere usar tanto autenticación como cifrado:

 # whack --name pruebaipv4 –ipv4 --host 10.0.1.1 --to --host 10.0.2.1 --authenticate --encrypt

Inicie Ethereal en otro equipo, para capturar los paquetes intercambiados; para hacer el establecimiento de la conexión segura se procede en los dos host así:

- Para hacer que el demonio de *pluto* comience a chequear la interface y revise el archivo *ipsec.secrets* para obtener las llaves de autenticación:

 # whack --listen

- Para iniciar el intercambio de llaves utilizando el nombre de la configuración:

 # whack --initiate --name pruebaipv4

- Para ver la información de asociaciones y políticas de seguridad definidas:

#ipsec-conf show

P.2.11 Observe los paquetes capturados por Ethereal y describa los paquetes intercambiados durante la negociación de IKE.

P.2.12 Haga un ping desde uno de los host, hacia el otro, pero antes verifique que Ethereal se haya inicializado en otro equipo para que capture los paquetes. ¿La respuesta al ping es satisfactoria? Describa los paquetes capturados.

- La forma de terminar una conexión, es finalizar la sesión IPSec entre los hosts, borrar la configuración establecida y detener el demonio de *pluto* que está corriendo, así:

whack--terminate--name pruebaipv4; para terminar IPSec entre los hosts.
whack--delete--name pruebaipv4; para borrar la configuración.

whack –shutdown; para detener *pluto*.

Asegúrese de terminar todas las asociaciones y políticas de seguridad definidas anteriormente antes de continuar.

b) Usando IKEd utilizando el archivo de configuración y auto scripts.

Los creadores de USAGI utilizan algunos scripts de FreeS/WAN para llevar a cabo las configuraciones. De esta forma es posible utilizar el comando *ipsec auto* con los archivos "ipsec.conf" e "ipsec.secrets".

Se ha introducido el campo "af" dentro del archivo "ipsec.secrets", que indica la familia de direcciones (Address Family); de esta forma, en este campo es posible escoger *inet* (para IPv4, valor por defecto) o inet6 (para IPv6). Los archivos "ipsec.conf" e "ipsec.secrets" tienen como ruta por defecto el directorio /usr/local/v6/etc.

El escenario de prueba para esta configuración se muestra a continuación (figura 5.3), utilizando direcciones IPv4; si se desea hacerla en IPv6, la configuración es la misma, solo reemplazando las direcciones (ver video *usagi_transporte.camrec*, previa instalación de Camtasia, en el CD adjunto al documento).

En IPv4: 10.0.1.1

10.0.2.1

En IPv6: 3ffe:8070:1024:1::15

3ffe:8070:1024:1::7

Figura 5.3 Escenario de Prueba Modo Trasporte Host to Host utilizando archivos de Configuración

Modo: transporte AH/ESP
Algoritmo AH: HMAC-MD5
Algoritmo de autenticación ESP: HMAC-MD5
Algoritmo de cifrado ESP: 3DES-CBC

El nombre de la asociación de seguridad es "pruebaipv4". Los pasos a seguir para llevar a cabo la configuración son:

- Escribir la llave secreta pre-compartida en el archivo ipsec.secrets, así:

```
10.0.1.1 10.0.2.1 : PSK "Prueba IPv4"
```

- Crear el archivo "ipsec.conf" para la configuración "pruebaipv4". El archivo "ipsec.conf" tiene dos tipos de secciones: la sección *config* de configuraciones y la sección *conn* de conexiones.

La sección *config setup* tiene toda la información que el software necesita para inicializarse. Para este ejemplo, esta sección quedaría de la siguiente forma:

```
config setup
        Interfaces=%defaultroute
        Klipsdebug=none
        Plutodebug=none
        Uniqueids=yes
```

El valor más importante de este ejemplo es el parámetro *interfaces,* el valor especial *%defaultroute* significa que la interfaz de red que *pluto* va a utilizar para establecer sesiones IPSec es la que utiliza la ruta por defecto. Los parámetros *klipsdebug y plutodebug* se utilizan cuando hay problemas más complejos. En los archivos de logs de Linux se encuentra suficiente información para determinar donde están los problemas más comunes.

Las secciones *conn* se utilizan para decirle a pluto que tipo de sesión IPSec se va a establecer o aceptar. Los cambios básicos que definen cada pareja IPSec son:

- ✓ Af=inet/inet6 Indica la familia de direcciones IPv4/IPv6
- ✓ Type=transport/tunnel Especifica los dos modos en los cuales IPSec puede operar.
- ✓ Auth= y Authby= Determinan si la autenticación a implementar es parte de AH o ESP y el tipo de ésta autenticación (secret o rsasig).
- ✓ Left= y Right= Son las direcciones IP asignadas a cada Gateway IPSec.
- ✓ Leftsubnet= y Rightsubnet= Son las subredes que se encuentran detrás de cada Gateway.
- ✓ Leftnexthop= y Rightnexthop= Son las direcciones IP del equipo que recibe la conexión.

Existe una sección conn especial, y es la sección *conn %default*, donde se colocan todos los valores por defecto de todas las secciones conn. En cada sección conn, estos valores se sobrescriben, pero en caso de que se omitan, se tomarán los escritos en esta sección. Por ejemplo:

```
Conn %default
        Keyingtries=0
        Authby=rsasig
        Auto=start
```

A continuación se muestra un ejemplo de una sección conn, para el caso que se está estudiando:

```
conn pruebaipv4
        af=inet
        auto=add
```

```
type=transport
 authby=secret
 left=10.0.1.1
right=10.0.2.1
esp=3des-md5-96
ah=hmac-md5-96
```

En el Host2, el archivo "ipsec.conf" es idéntico, salvo que deben intercambiarse las direcciones de left y right.

- Inicializar el Analizador de Protocolos Ethereal en un host diferente a los utilizados para la práctica; utilice el filtro: *!arp && host 10.0.2.1*.

- Correr el demonio de *pluto* en ambos hosts con el comando: *#pluto*.

- Adicionar la configuración de "pruebaipv4" a *pluto* en ambos hosts, así:

#ipsec auto --add pruebaipv4

- Hacer que *pluto* procese la llave secreta pre-compartida:

#ipsec auto –ready

- Hacer que *pluto* establezca la Asociación de Seguridad IPSec, que está configurada en el archivo ipsec.conf con el nombre de *pruebaipv4*:

#ipsec auto --up pruebaipv4

- Una vez hecho esto, la sesión IPSec está declarada y los hosts deben comenzar a intercambiar información de forma segura, utilizando autenticación y cifrado. Haga ping para verificar que se realice intercambio de información.

P.2.13 ¿Qué diferencias encuentra al observar la captura realizada en configuración automática y la realizada cuando se realizó la configuración manual?

- Guarde la configuración de las asociaciones y de las políticas de seguridad establecidas utilizando el comando *#ipsec-conf save <nombre-del-archivo>.*

P.2.14 Compare la salida de los archivos <nombre-del-archivo> al hacer la configuración manual y al hacer la configuración automática y determine las diferencias que existen al configurar asociaciones y políticas de seguridad de forma manual y de forma

automática. Recuerde que no importa con qué tipo de direcciones IP está trabajando, la configuración en cualquiera de las formas es igual.

Otros comandos útiles son:

- Para borrar la configuración "pruebaipv4":

 # ipsec auto --delete pruebaipv4

- Para cambiar la llave pre-compartida o añadir una nueva:

 # ipsec auto –rereadsecret

5.1.3.4 Conclusiones

5.1.4 Práctica 3: Configuración de IPSec en Modo Túnel

5.1.4.1 Motivación

En esta práctica se busca comprender el funcionamiento de las Asociaciones y Políticas de Seguridad en su configuración en Modo Túnel utilizando los protocolos de Seguridad AH y ESP. Esta práctica se divide en tres fases:

- Fase 1: Conexión entre dos redes con claves manuales.
- Fase 2: Conexión entre dos redes usando IKE.
- Fase 3: Conexión de un Road Warrior (Host Remoto) a una Gateway de Seguridad.

Para llevar a cabo esta práctica, es necesario el siguiente hardware:

- Cuatro equipos que ejecuten el sistema operativo Linux (en este caso se utilizó Linux Debian); dos de ellos con soporte USAGI IPSec.
- Una LAN o una WAN para conectar estos equipos.

5.1.4.2 Objetivos

- Habilitar AH y/o ESP en Modo Túnel de forma manual.
- Habilitar AH y/o ESP utilizando el intercambio automático de claves mediante archivos de configuración.
- Analizar la configuración de la conexión de un Host a una Gateway de Seguridad.

5.1.4.3 Desarrollo de la Práctica

- *FASE 1: Conexión entre dos redes con claves manuales*

En este modo, la Gateway de Seguridad 1 (SG1) y la Gateway de Seguridad 2 (SG2) conectan dos redes sobre una red IPv4 o IPv6 externa usando túneles IPSec. A continuación se muestra la topología implementada (figura 5.4); además se define una Asociación de Seguridad entre SG1 y SG2.

eth0:10.0.1.2 /24 eth0:10.0.1.1/24 eth0:10.0.2.1/24
eth0:10.0.2.2/24
eth1:192.168.10.1/16
eth1:192.168.20.1/16
tnl0:10.0.254.1/30 tnl0:10.0.254.2/30

Figura 5.4 Escenario de Prueba Modo Túnel con direcciones IPv4

La información necesaria para declarar las Asociaciones y Políticas de Seguridad se muestra a continuación:

Modo: túnel AH/ESP
Algoritmo AH: HMAC-MD5 (llave: 0x0123456789abcdef0123456789abcdef)
Algoritmo de Autenticación ESP: HMAC-MD5
(llave: 0x0123456789abcdef0123456789abcdef)
Algoritmo de cifrado: 3DES-CBC
(llave: 0xa7a36ebd91863edfba763fa7edcba64d89123ace6359eba7)
SPI: SG1 -> SG2 AH: 0x1234 ESP: 0x5678, SG2 -> SG1 AH: 0x9abc ESP: 0xdef0

- Primero que todo se deben fijar las interfaces de cada nodo y configurar las gateways SG1 y SG2 como routers. Es importante tener en cuenta que en el Host1 debe configurarse la eth0 de la SG1 como puerta de enlace predeterminada. De igual forma en el Host2 debe configurarse la eth0 de la SG2 como puerta de enlace predeterminada.

En el HOST1:

```
#ifconfig eth0 10.0.1.2 netmask 255.255.255.0
#route –A inet add default gw 10.0.1.1 dev eth0
```

En el HOST2:

```
#ifconfig eth0 10.0.2.2 netmask 255.255.255.0
#route –A inet add default gw 10.0.2.1 dev eth0
```

En SG1:

```
#ifconfig eth0 10.0.1.1 netmask 255.255.255.0
#ifconfig eth1 192.168.10.1 netmask 255.255.0.0
Para habilitar el reenvío de paquetes IP:
# sysctl -w net/ipv4/conf/all/forwarding=1
```

En SG2:

```
#ifconfig eth0 10.0.2.1 netmask 255.255.255.0
#ifconfig eth1 192.168.20.1 netmask 255.255.0.0
# sysctl -w net/ipv4/conf/all/forwarding=1
```

- Luego, se debe fijar el túnel entre SG1 y SG2 y configurar el enrutamiento. Para verificar la configuración del túnel, se utiliza el siguiente comando: *iptunnel show*.

Sobre la gateway SG1:

```
# iptunnel add tnl0 mode ipip local 192.168.10.1 remote 192.168.20.1
# ifconfig tnl0 10.0.254.1 netmask 255.255.255.252
# ifconfig tnl0 up
# route –A inet add -net 10.0.2.0 netmask 255.255.255.0 dev tnl0
```

Sobre la gateway SG2:

```
# ip tunnel add tnl0 mode ipip local 192.168.20.1 remote 192.168.10.1
# ifconfig tnl0 10.0.254.2 netmask 255.255.255.252
# ifconfig tnl0 up
# route –A inet add -net 10.0.1.0 netmask 255.255.255.0 dev tnl0
```

En este momento es posible hacer *ping* desde el HOST1 hasta el HOST2. En caso contrario, debe revisarse la configuración. Realice un *traceroute* para observar el camino que toman los paquetes IP.

- Después de esto, ya se pueden fijar las Asociaciones y políticas de Seguridad, tanto en SG1 y SG2, así:

De SG1 a SG2:

```
# pfkey -A sa -s 192.168.10.1/16 -d 192.168.20.1/16 -T ah -S 0x1234 --auth hmac-md5 --authkey
0x0123456789abcdef0123456789abcdef
# pfkey -A sa -s 192.168.10.1/16 -d 192.168.20.1/16 -T esp -S 0x5678 –esp 3des-cbc –espkey
0xa7a36ebd91863edfba763fa7edcba64d89123ace6359eba7--auth hmac-md5 --authkey 0x0123456789abcdef0123456789abcdef
# pfkey -A sp -s 10.0.1.0/24 -d 10.0.2.0/24 -T ah -S 0x1234 --tunnel --sad 192.168.20.1
# pfkey -A sp -s 10.0.1.0/24 –d 10.0.2.0/24 -T esp -S 0x5678 --tunnel --sad 192.168.20.1
```

De SG2 a SG1:

pfkey -A sa -s 192.168.20.1/16 -d 192.168.10.1/16 -T ah -S 0x9abc --auth hmac-md5 --authkey 0x0123456789abcdef0123456789abcdef
pfkey -A sa -s 192.168.20.1/16 -d 192.168.10.1/16 -T esp -S 0xdef0 --esp 3des-cbc ---espkey 0xa7a36ebd91863edfba763fa7edcba64d89123ace6359eba7--auth hmac-md5 --authkey 0x0123456789abcdef0123456789abcdef
pfkey -A sp -s 10.0.2.0/24 -d 10.0.1.0/24 -T ah -S 0x9abc --tunnel -sad 192.168.10.1
pfkey -A sp -s 10.0.2.0/24 -d 10.0.1.0/24 -T esp -S 0xdef0 --tunnel -sad 192.168.10.1

- Finalmente, se ha configurado el túnel IPSec entre la gateway SG1 y SG2. Guarde la configuración de las asociaciones y de las políticas de seguridad establecidas utilizando el comando #ipsec-conf save <nombre-del-archivo>.

P.3.1 Haga ping desde el HOST1 al HOST2 o viceversa. ¿Qué respuesta espera obtener?

P.3.2 Con el comando #*ipsec-conf show* analice las asociaciones y políticas de seguridad establecidas; explique la configuración.

P.3.3 Inicie el Analizador de Protocolos Ethereal en otro equipo diferente a los utilizados en la configuración y utilice el siguiente filtro: *!arp && host 10.0.2.2.* Haga ping entre el Host1 y el Host2. ¿Qué tipo de paquetes se capturan en la comunicación?

P.3.4 Ahora cambie el filtro por el siguiente: *!arp && host 192.168.20.1*. Haga de nuevo ping entre el Host1 y el Host2. ¿Qué tipo de paquetes se capturan en la comunicación? ¿Por qué?

- *FASE 2: Conexión entre dos redes usando IKE*

Para esta parte de la prueba es necesario realizar la misma configuración anterior en los Host y en las Gateways de Seguridad. Una vez hecho esto, en lugar de utilizar comandos manuales, se utilizan los archivos *ipsec.conf* e *ipsec.secrets*. La configuración de IKE en Modo Túnel es casi la misma que IKE en modo Transporte excepto por las entradas en el archivo ipsec.conf (ver video *usagi1_tunel.camrec y usagi2_tunel.camrec*, previa instalación de Camtasia, en el CD adjunto al documento).

- Escribir una clave secreta pre-compartida en el archivo *ipsec.secrets* así:

```
192.168.10.1 192.168.20.1 : PSK "tunel ipv4"
```

En las dos SG el archivo *ipsec.secrets* es el mismo.

- Escribir la configuración "tunel ipv4" en el archivo *ipsec.conf:*

```
config setup
        Interfaces=%defaultroute
        Klipsdebug=none
        Plutodebug=none
        Uniqueids=yes
```

```
Conn %default
                                                    Keyingtries=0
                                                    Authby=rsasig
                                                       Auto=start
conn tunelipv4
                                                          af=inet
                                                    authby=secret
                                                      type=tunnel
                                                 left=192.168.10.1
                                              leftsubnet=10.0.1.0/24
                                            leftnexthop=192.168.20.1
                                                 right=192.168.20.1
                                            rightsubnet= 10.0.2.0/24
                                           rightnexthop=192.168.10.1
                                                     esp=3des-md5-96
                                                      ah=hmac-md5-96
```

En las SG el archivo *ipsec.conf* es idéntico, salvo que deben intercambiarse las direcciones determinadas en left y right.

- Inicializar el Analizador de Protocolos Ethereal en un host diferente a los utilizados para la práctica; utilice el filtro: *!arp && host 10.0.2.1*.

- Correr el demonio de *pluto* en ambas SG con el comando: *#pluto*.

- Adicionar la configuración de "tunelipv4" a *pluto* en ambas SG, así:

#ipsec auto --add tunelipv4

- Hacer que *pluto* procese la llave secreta pre-compartida:

#ipsec auto –ready

- Hacer que *pluto* establezca la Asociación de Seguridad IPSec, que está configurada en el archivo *ipsec.conf* con el nombre de *tunelipv4*:

#ipsec auto --up tunelipv4

- Una vez hecho esto, la sesión IPSec está declarada y los hosts deben comenzar a intercambiar información de forma segura entre las Gateways de Seguridad, utilizando autenticación y cifrado. Haga ping para verificar que se realice intercambio de información.

P.3.5 Observe los paquetes capturados por Ethereal y describa los paquetes intercambiados durante la negociación de IKE.

P.3.6 Observe los paquetes intercambiados una vez se ha realizado la negociación ISAKMP entre las Gateways de Seguridad; describa los encabezados de seguridad.

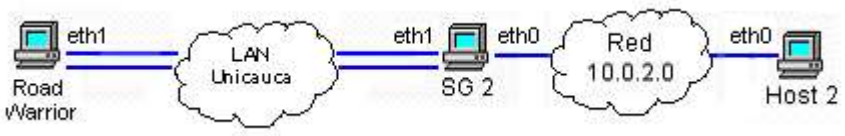
- Guarde la configuración de las asociaciones y de las políticas de seguridad establecidas utilizando el comando #ipsec-conf save <nombre-del-archivo>.

P.3.7 Compare la salida de los archivos <nombre-del-archivo> y determine las diferencias que existen al configurar asociaciones y políticas de seguridad de forma manual y de forma automática en modo túnel.

Recuerde bajar las asociaciones y políticas de seguridad con el comando #*ipsec auto -–delete tunelipv4*.

➢ *Fase 3: Conexión de un Road Warrior (Host Remoto) a una Gateway de Seguridad.*

En esta sección, el Road Warrior (RW) y la Gateway 2 (SG2) se comunican sobre una red IPv4 externa usando Túneles IPSec. El RW tiene solo una interfaz física, como se muestra a continuación (figura 5.5). Una Asociación de Seguridad se aplica entre el RW y la SG2.



eth0:10.0.2.1/24 eth0:10.0.2.2/24
eth1:192.168.10.1/16 eth1:192.168.20.1/16
tnl0:10.0.254.1/30 tnl0:10.0.254.2/30

Figura 5.5 Escenario de Prueba Road Warrior (Host Remoto) to Gateway

La información a tener en cuenta para configurar las Asociaciones y Políticas de Seguridad se muestra a continuación:

Modo: tunnel AH/ESP
Algoritmo AH: HMAC-MD5 (llave: 0x0123456789abcdef0123456789abcdef)
Algoritmo de Autenticación ESP: HMAC-MD5
(llave: 0x0123456789abcdef0123456789abcdef)
Algoritmo de Cifrado ESP: 3DES-CBC
(llave: 0xa7a36ebd91863edfba763fa7edcba64d89123ace6359eba7)
SPI: SG1 -> SG2 AH: 0x1234 ESP: 0x5678, SG2 -> SG1 AH: 0x9abc ESP: 0xdef0

Este proceso se llevará a cabo de forma manual para observar claramente la definición de las políticas de seguridad para el tráfico entre el RW y el Host2, o la red 10.0.2.0. Primero que todo, se deben fijar las interfaces de cada nodo y configurar SG2 como un router.

En el HOST2:

ifconfig eth0 10.0.2.2 netmask 255.255.255.0
Se debe definir la SG2 como puerta de enlace predeterminada para el Host2:
#route –A inet add default gw 10.0.2.1 dev eth0

En el RW:

ifconfig eth1 192.168.10.1 netmask 255.255.0.0

En la SG2:

ifconfig eth0 10.0.2.1 netmask 255.255.255.0
ifconfig eth1 192.168.20.1 netmask 255.255.0.0
Se habilita el reenvío de paquetes IP:
sysctl -w net/ipv4/conf/all/forwarding=1

Luego, se debe fijar el túnel entre el RW y la SG2, y configurar el enrutamiento. Para chequear la configuración de Túnel, se utiliza el siguiente comando *#iptunnel show tnl0* una vez terminada la configuración.

En el RW:

iptunnel add tnl0 mode ipip remote 192.168.20.1 local 192.168.10.1
ifconfig tnl0 up
ifconfig tnl0 10.0.254.1 netmask 255.255.255.252
route –A inet add –net 10.0.2.0 netmask 255.255.255.0 dev tnl0

En la SG2:

iptunnel add tnl0 mode ipip remote 192.168.10.1 local 192.168.20.1
ifconfig tnl0 up
ifconfig tnl0 10.0.254.2 netmask 255.255.255.252

En este momento es posible hacer ping desde el RW hasta el Host2. En caso de que no funcione el ping, debe revisarse la configuración. El siguiente paso es crear las Asociaciones y Políticas de Seguridad tanto en el RW como en la SG2.

Del RW a la SG2:

pfkey -A sa -s 192.168.10.1/16 -d 192.168.20.1/16 -T ah -S 0x1234 --auth hmac-md5 --authkey 0x0123456789abcdef0123456789abcdef
pfkey -A sa -s 192.168.10.1/16 -d 192.168.10.1/16 -T esp -S 0x5678 –esp 3des-cbc –espkey 0xa7a36ebd91863edfba763fa7edcba64d89123ace6359eba7--auth hmac-md5 --authkey 0x0123456789abcdef0123456789abcdef
pfkey -A sp –s 10.0.254.1 -d 10.0.2.0/24 -T ah -S 0x1234--tunnel -sad 192.168.20.1
pfkey -A sp -s 10.0.254.1 -d 10.0.2.0/24 -T esp -S 0x5678--tunnel -sad 192.168.20.1

De la SG2 al RW:

pfkey -A sa -s 192.168.20.1/16 -d 192.168.10.1/16 -T ah -S 0x9abc --auth hmac-md5 --authkey 0x0123456789abcdef0123456789abcdef
pfkey -A sa -s 192.168.20.1/16 -d 192.168.10.1/16 -T esp -S 0xdef0 --esp 3des-cbc --espkey 0xa7a36ebd91863edfba763fa7edcba64d89123ace6359eba7--auth hmac-md5 --authkey 0x0123456789abcdef0123456789abcdef
pfkey -A sp -s 10.0.2.0/24 -d 10.0.254.1 -T ah -S 0x9abc --tunnel --sad 192.168.10.1
pfkey -A sp -s 10.0.2.0/24 -d 10.0.254.1 -T esp -S 0xdef0 --tunnel --sad 192.168.10.1

- Finalmente, se ha configurado el túnel IPSec desde el Road Warrior a la Gateway de Seguridad 2. En este momento es posible hacer ping desde el RW al HOST2, y chequear con Ethereal que se están encriptando los paquetes.

P.3.8 Utilice Ethereal para analizar los paquetes que se intercambian entre el RW y la SG2 y los paquetes que se intercambian entre el Host2 a la SG2. ¿Cuál es la diferencia?

P.3.9 ¿Qué pasa si no se fijan asociaciones y políticas de seguridad en uno de los extremos del túnel?

5.1.4.4 Conclusiones

5.2 PRACTICAS PARA LA IMPLEMENTACION DE SEGURIDAD A NIVEL DE RED UTILIZANDO LAS HERRAMIENTAS DEL PROYECTO FREES/WAN Y OPENSWAN SOBRE LINUX

5.2.1 Proyecto FreeS/WAN

El proyecto FreeS/WAN es realizado por grupos de Investigación apoyados por Novell, SUSE y ASTARO Internet Security, y su principal objetivo es llevar a cabo implementaciones de libre distribución de IPSec en el núcleo del Sistema Operativo Linux; estas implementaciones son soportadas por varios kernels y corren en diferentes plataformas. Entre los objetivos del proyecto están: extender IPSec al desarrollo de *Opportunistic Encryption*, lo que permitiría que dos sistemas pudieran asegurar sus comunicaciones sin una conexión preestablecida; generar una implementación de IPSec sin restricciones, de libre distribución y código abierto; proveer a Linux de una herramienta de alta calidad y rendimiento que implemente IPSec para cualquier CPU y que sea interoperable con cualquier otra implementación de IPSec. Como ya se ha visto, IPSec provee servicio de cifrado y autenticación a nivel IP (Internet Protocol); en otras palabras, IPSec le da a IPv4 algo que no tiene, seguridad de datos (cifrado) y autenticación. En esta parte del documento se va a explicar cómo utilizar esta implementación y se describirán las prácticas más comunes en un ambiente de prueba.

El proyecto FreeS/WAN comprende dos grandes áreas: una es el código que se agrega al núcleo de Linux (actualmente es un parche separado ya que no integra el núcleo) y la otra parte es el código de las herramientas que el usuario utiliza para hacer que se

establezcan los túneles (entre otras cosas). Las fuentes de este proyecto se pueden obtener del sitio oficial de FreeS/WAN[4]. Dado que FreeS/WAN es una implementación de IPSec en Linux es lógico inferir que no es la única implementación de IPSec en Linux, como ya se ha visto, y que además IPSec esta implementado en otros sistemas operativos.

Para realizar las prácticas serán necesarios 2 equipos con Sistema Operativo Linux, que se puedan conectar de algún modo a Internet (en forma directa). Se instalará FreeS/WAN en ambos y, luego se determinará el tipo de autenticación que se va a utilizar. Antes de hacer todo esto, es necesario entender bastante bien, qué significa "determinar que tipo de autenticación se va a utilizar".

5.2.2 Tipos de túneles

La autenticación es el momento inicial cuando desde un nodo de la VPN se quiere establecer un túnel hacia otro nodo. Lo primero que tienen que hacer los nodos es asegurarse que cada uno es quien dice ser. Para realizar esta tarea existen varios métodos. En FreeS/WAN básicamente existen 3 tipos diferentes, que son:

- ***Pre-shared-keys*** (claves pre-compartidas o preacordadas) donde los dos nodos saben de antemano qué clave van a utilizar.
- ***Claves o Firmas Digitales RSA*** (uso de claves asimétricas), en el cual se generan claves asimétricas en cada nodo y las partes públicas de cada clave son esparcidas por toda la red; de esta forma solamente aquellos que tengan la parte privada de la clave serán los verdaderos dueños de las partes públicas esparcidas.
- ***Certificados X509***, donde sólo aquellos certificados que estén firmados por una entidad certificante en la cual se confíe, serán considerados como nodos válidos.

Si bien todos los métodos tienen sus pros y sus contras, para los expertos en el tema es claro que la mejor opción es la autenticación con certificados, por su simpleza de administración y por su gran interoperabilidad con otras plataformas (es común que otras implementaciones de IPSec utilicen esta autenticación).

5.2.3 Instalación

FreeS/WAN tiene dos partes principales: el parche de *ipsec* para el núcleo (**KLIPS**) que implementa AH (Authentication Header), ESP (Encapsulating Security Payload) y el manejo de paquetes dentro del núcleo. La otra parte son las herramientas de usuario (**pluto**), el cual implementa IKE (Internet Key Exchange), y es quien negocia las conexiones con otros equipos. Lo primero que hay que hacer es lograr que el núcleo entienda IPSec. Esto se puede hacer de varias formas; una es aplicando el parche a las fuentes del núcleo, compilarlo (con las opciones requeridas) y ejecutarlo; la otra forma es utilizar algún módulo de FreeS/WAN ya compilado y así hacer que el núcleo entienda IPSec utilizando la capacidad modular de los núcleos de Linux. En el sitio que produce los parches para

[4] Las fuentes de este proyecto se pueden obtener de sitio oficial de FreeS/WAN http://www.freeswan.org

X509, se generan paquetes RPMs, que son como archivos ejecutables si hablamos en términos de Windows. También se generan los paquetes *Super Freeswan* que son paquetes que vienen con muchos parches "no oficiales" para FreeS/WAN, pero en ocasiones muy útiles. Deben descargarse los paquetes RPM acordes a la distribución de Linux que se esté utilizando, en este caso Fedora Core 4. Una vez descargados los paquetes RPM del sitio Web, se instalan de esta forma:

#rpm -Uvh freeswan-module-<version>.rpm
#rpm -Uvh freeswan-userland-<version>.rpm

Y eso es todo, ya se tiene soporte IPSec en Linux. En este caso se han instalado los paquetes *freeswan-module-2.06_2.4.20_8-0.i386.rpm y freeswan-userland-2.06_2.4.20_8-0.i386.rpm*, descargados del sitio http://www.freeswan.org

5.2.4 Entendiendo la configuración de FreeS/WAN

La gente de FreeS/WAN ideó una forma de escribir los archivos de configuración que al principio es un poco difícil de entender, pero que con la práctica se adquiere la suficiente experiencia. Cuando ellos diseñaron esta herramienta, quisieron hacer que los archivos de configuración de todos los nodos de la red VPN fueran iguales (o extremadamente parecidos), por lo que en vez de utilizar nombres de variables como "remoto" o "local" (dado que se deben invertir dependiendo el lugar donde se esté), utilizaron variables como "izquierda" o "derecha". De esta forma, no importa qué nodo se esté configurando, el "nodo izquierdo" siempre es el mismo en todos los puntos (lo mismo sucede con el derecho, por supuesto). Lo cierto es que la complejidad de las cosas no siempre juegan a favor, con lo cual son menos las veces donde los archivos de configuración de los nodos son iguales, que en las que lo son diferentes. Por otro lado, los desarrolladores prefirieron utilizar este tipo de sintaxis para disminuir la confusión que puede generar el uso de palabras como "local" o "remoto" al implementar la VPN. Por último hay muchos ejemplos en la documentación de FreeS/WAN que supone números de IP fijos, sin embargo, FreeS/WAN soporta de forma segura y confiable el uso de direcciones IP dinámicas en sus configuraciones.

5.2.4.1 Autenticación

Lo primero que hace IPSec a la hora de establecer un túnel es determinar si el equipo que intentar establecer el túnel es quien dice ser, y que además es un equipo válido con el cual se quiere establecer un túnel. Luego entre las partes deciden que claves van a utilizar y finalmente (luego de muchas otras cosas en el medio) el túnel se establece y ambas partes empiezan a comunicarse con el protocolo ESP (y AH según el caso). Para autenticar se pueden usar muchos métodos, como ya se han mencionado, pero en esta práctica se utilizarán 2 con los cuales se obtienen respuestas satisfactorias y son adecuados a nuestras necesidades: *pre shared keys* (claves compartidas preacordadas) y *Firmas Digitales RSA*.

[5] Página de desarrollos no oficiales de FreeSWan: http://www.freeswan.ca

- *Pre Shared Keys*

En este tipo de autenticación se utiliza una única clave en todos los nodos de la VPN (clave en texto plano). El nodo que esta recibiendo la conexión de otro nodo de la VPN determina que el nodo que está realizando la conexión es válido si tiene la clave correcta. Las ventajas de utilizar *pre shared keys* son dos: una es la facilidad de configurar este tipo de autenticación, y la segunda es que es un tipo de autenticación que la gran mayoría de implementaciones de IPSec tienen, por lo tanto es probable que se tenga más oportunidad de interoperar con otras implementaciones si se utiliza este tipo de autenticación. La gran desventaja que tiene este tipo de autenticación es la pobre administración de estas claves. Además que si se hacen túneles VPN con otras empresas u otros administradores, obligatoriamente se tienen que utilizar las mismas claves. Es un tipo de autenticación válido, pero debería ser el último recurso a utilizar.

- *Firmas digitales RSA*

Las firmas digitales son firmas asincrónicas (eso quiere decir que la firma digital se divide en dos: una parte privada y otra pública); esta es una forma sencilla de autenticación entre dos Linux con FreeS/WAN y definitivamente muy segura. Lo bueno de esta forma de autenticación es que cada nodo tiene su propia firma; esto hace que si en algún nodo se comprometió la parte privada de la firma, entonces se puede dar de baja ese nodo únicamente y el resto de los nodos de la red pueden seguir encriptando sin temor. El tamaño de las firmas por defecto es bastante generoso (2192 bits) aunque se puede aumentar si se quiere. El funcionamiento de estas firmas es simple: cada nodo arma su par de claves e intercambian la parte pública de la misma (o las publica en un DNS). Entonces cuando uno de los nodos recibe un pedido de conexión del otro, éste verificará si el nodo remoto es quien dice ser revisando el mensaje enviado. Este mensaje viene firmado digitalmente por el nodo que inició la conexión, y el nodo receptor deberá determinar si esta firma es válida utilizando la clave pública del nodo remoto. El proceso en realidad es mucho más complejo, pero garantiza seguridad y robustez. El mantenimiento de estas claves puede llegar a ser algo tedioso (si hay muchos nodos), pero por la facilidad de implementación vale la pena hacer el esfuerzo.

- *Certificados X509*

Los certificados X509, son la mejor opción a utilizar. La idea con los certificados es tener una CA (Certificate Authority - Autoridad Certificante) que actúa de validadora de certificados; si un certificado (que provenga de cualquier lado en Internet) esta firmado por la CA en la que se confía, entonces se asume que este certificado es un certificado válido. Es importante aclarar que el nodo que esta recibiendo la conexión no tiene la clave pública del nodo que inició la comunicación; éste solo revisará si el certificado esta firmado con la CA en la que se confía. Por otro lado, y antes de asumir la validez de un certificado firmado, se revisa lo que se llama la CRL (Certificate Revocation List - Lista de Certificados Revocados), que es un archivo donde están todos los certificados en los que *no* se confía más (y que han sido firmados en algún momento por la CA). En esta lista van a parar todos los certificados que por alguna razón han sido comprometidos. El único inconveniente es que dar el primer paso con una CA y *openssl* puede llegar a ser tedioso (pero no después de leer esta documentación).

5.2.5 Configuración

FreeS/WAN posee un archivo principal de configuración *ipsec.conf*, que puede estar en /etc o en /etc/freeswan (dependiendo de la distribución de Linux); en este archivo se lleva a cabo toda la configuración. Hay otros archivos de configuración como el *ipsec.secrets* donde se pone la información de claves pre-compartidas y firmas RSA. Por último hay un directorio /etc/ipsec.d que se utiliza generalmente al trabajar con el parche de autenticación X509. El ipsec.conf tiene dos tipos de secciones: la sección de *Configuración* (config) y la sección de Conexiones (conn). En este momento la única sección de configuración que se acepta en FreeS/WAN es la sección de configuración "setup".

La sección *config setup* tiene toda la información que el software necesita al inicializarse. Este es un ejemplo de esta sección:

```
config setup
    interfaces=%defaultroute
    klipsdebug=none
    plutodebug=none
    uniqueids=yes
```

El valor más importante en este ejemplo es el del parámetro interfaces; el valor especial *%defaultroute* significa que la interface de red que **pluto** va a utilizar para establecer las conexiones cifradas, es la que utiliza la ruta por defecto (la que sale a Internet generalmente). En el caso de que los túneles se estén armando sobre otra red que no sea Internet, es posible que sea necesario cambiar este valor. Los parámetros de debug, klipsdebug y plutodebug, se utilizan cuando hay problemas más complejos; los mensajes normales, que se graban en los logs, dan suficiente información para determinar dónde están los problemas comunes.

Las secciones *conn* se utilizan para decirle a **pluto** que tipo de conexiones se van a establecer o aceptar. En lo que respecta a secciones *conn* hay una que es especial y es la sección *conn %default*; esta sección va a tener los valores por defecto de todas las secciones *conn*. Luego en cada seccion *conn* se podrán sobreescribir los valores, pero en caso que se omitan, se tomaran los escritos en esta sección. Este es un ejemplo de sección *conn %default:*

```
conn %default
       keyingtries=0
       authby=rsasig
```

El parámetro *keyingtries* determina cuantas veces **pluto** va a intentar para establecer un conexión; el valor cero indica que siga intentando eternamente. El parámetro *authby* determina la forma en que se va a estar haciendo la autenticación: el valor *secret* es cuando se utiliza pre-shared keys (claves pre-compartidas) y se utiliza el valor *rsasig* cuando se va a autenticar con una firma digital RSA (cuando se utilizan certificados X509 también se usa este tipo de valor). En las prácticas se trabajará la configuración que solo permite un túnel por sección conn, que de hecho es lo más usual.

```
conn prueba
       left=172.16.41.123
       leftrsasigkey=0sAQO1wwYJq.........
       right=173.16.41.124
```

```
rightrsasigkey=0sAQNt1jXTSQ.........
auto=add
```

Este ejemplo se lee de la siguiente manera (se va a utilizar el valor *left* para el host A y *right* para el host B): dado que el host A (left) está conectado directamente a Internet, se puede utilizar el valor *%defaultroute* que le indica a **pluto** que tome el número de IP asignado a la interface que tiene la ruta por defecto o, si se quiere, puede colocarse el número de la dirección IP estática. El parámetro *leftrsasigkey* indica la parte pública de la clave RSA del host A. Con respecto al lado derecho (right), se puede ver que el parámetro *right* tiene la dirección IP que tiene el lado derecho de la conexión. Al igual que el lado izquierdo, el derecho también tiene una clave pública RSA. Por último, el parámetro *auto=add* indica que esta conexión deberá agregarse a las conexiones disponibles, pero **pluto** no hará nada con él al momento de inicializar todo el servicio; este campo puede contener el valor *start* que indica que al inicializar el servicio, **pluto** intente establecer la conexión.

5.2.6 Práctica 4: Utilizando FreeS/WAN para configurar autenticación con Pre-shared Keys

5.2.6.1 Motivación

Cada uno de los tipos de autenticación tiene su propia forma de configuración. En esta sección se detalla la configuración de autenticación con llaves pre-compartidas, utilizando los archivos de configuración de FreeS/WAN.

5.2.6.2 Objetivo

- Habilitar ESP para autenticación y cifrado, en Modo Transporte con llaves pre-compartidas y utilizando los archivos de configuración.

5.2.6.3 Desarrollo de la Práctica

La topología utilizada se muestra a continuación (figura 5.6):

172.16.41.123

172.16.41.124

Figura 5.6 Escenario de prueba en Modo Transporte con FreeS/WAN

- Para configurar este tipo de autenticación es necesario poner en un solo lugar la clave única compartida. Este lugar es el archivo /etc/ipsec.secrets. Para utilizar este tipo de autenticación se escribe lo siguiente en el archivo /etc/ipsec.secrets:

<direcciones_ip_que_intervienen>: PSK "clave"

Por ejemplo:

```
172.16.41.123 172.16.41.124 : PSK “prueba con freeswan”
```

Este archivo es el mismo en los dos equipos en los que se va a llevar a cabo la configuración. En el caso de que se tenga una configuración para aceptar IP dinámicas, la única dirección que habría que colocar en este punto es la conocida, del PC que se está configurando.

- El siguiente paso es configurar la conexión, en el archivo */etc/ipsec.conf*, que para esta topología y para el host A, quedaría como se muestra a continuación:

```
config setup
                                interfaces=%defaultroute
                                    klipsdebug=none
                                    plutodebug=none
                                     uniqueids=yes
conn %default
                                     keyingtries=0
                                     authby=rsasig
                                       auto=start
conn prueba
                                        auto=add
                                      authby=secret
                                   left=172.16.41.123
                                  right=172.16.41.124
```

Debe recordar que en cada host deben intercambiarse los valores de *left* y *right*.

- Primero que todo, verifique que cada equipo tenga definida una ruta por defecto a Internet, utilizando el comando #route –n. De lo contrario escriba el siguiente comando: #*route –A inet add default gw 172.16.255.254*

- Para utilizar IPSec, es necesario iniciar el servicio: #*service ipsec start*, que inicia el demonio Pluto y adiciona la configuración de *prueba* a *pluto* en ambos hosts.

- Para hacer que *pluto* procese la llave secreta pre-compartida:

  #*ipsec auto -–ready*

- Ahora, por último, para hacer que *pluto* establezca la Asociación de Seguridad IPSec, que está configurada en el archivo *ipsec.conf* con el nombre de *prueba*:
  #ipsec auto --up prueba

  - Una vez hecho esto, la sesión IPSec está declarada y los hosts deben comenzar a intercambiar información de forma segura, utilizando autenticación y cifrado. Haga ping para verificar que se realiza intercambio de información.

  - Para observar el estado de las conexiones establecidas y declaradas, utilice el comando *#ipsec whack -–status*

P.4.1 Haga un ping desde uno de los host, hacia el otro, pero antes inicie Ethereal para que capture los paquetes. ¿La respuesta al ping es satisfactoria?

P.4.2 Observe los paquetes capturados por Ethereal durante la negociación de IKE. ¿Hay diferencias entre la negociación con *FreeS/WAN* y la negociación con USAGI?

P.4.3 Elimine la conexión *prueba* con *#ipsec auto -–delete prueba*. Adicione la línea *auth=ah* a la conexión prueba en el archivo */etc/ipsec.conf* y suba la conexión nuevamente. ¿La conexión se estableció correctamente? ¿Por qué?

5.2.6.4 Conclusiones

5.2.7 Práctica 5: Utilizando FreeS/WAN para configurar autenticación con Firmas Digitales RSA

5.2.7.1 Motivación

En esta práctica se utiliza la configuración de autenticación con Firmas Digitales RSA para la conexión segura entre dos equipos, utilizando los archivos de configuración de FreeS/WAN (ver video *openswanLlavesRSA.camrec*, previa instalación de Camtasia, en el CD adjunto al documento).

5.2.7.2 Objetivo

- Habilitar ESP para autenticación y cifrado, generando Firmas Digitales para la autenticación en los archivos de configuración.

5.2.7.3 Desarrollo de la Práctica

- Primero que todo, elimine la conexión prueba de la práctica anterior en ambos hosts con el siguiente comando *#ipsec auto --delete prueba.*

Las firmas digitales no son tan difíciles de configurar y son más administrables. Para configurar este tipo de autenticación se necesita el archivo */etc/ipsec.secrets* de la práctica anterior, y a continuación se debe ejecutar el siguiente comando:

 # ipsec rsasigkey –verbose nbits > /etc/ipsec.secrets

Donde *nbits* identifica el número de bits a utilizar para construir la llave, en este caso utilice 1024. Este comando cambiará el contenido del archivo *ipsec.secrets* por un contenido parecido al siguiente:

```
: RSA {
      # RSA 1024 bits fw.ny4487.com.ar Tue Sep 24 01:14:02 2005
      # for signatures only, UNSAFE FOR ENCRYPTION
      #pubkey=0sAQNsU3ATU3ifMuaMgf5eGTTc7X...........
      #IN KEY 0x4200 4 1 AQPY+BA6k+J7em...........
      Modulus: 0xd8f8103a93e27b7a6afbfa6c6b..........
      PublicExponent: 0x03
      PrivateExponent: 0x24295809c35069e9bc7f546........
      Prime1: 0xed2ef593c6...........
      Prime2: 0xea2e8fe4f956...........
      Exponent1: 0x9e1f4e...........
      Exponent2: 0x9c1f0a98a6...........
      Coefficient: 0x497825b73814334...........
      }
      # do not change the indenting of that "}"
```

Si bien las líneas son largas y sus números son aleatorios, hay una línea que es de interés; es la línea que contiene la parte pública de la clave (la que comienza con #pubkey=0sAQNs...); esta línea debe copiarse (sin el #pubkey=) al archivo /etc/ipsec.conf en el parámetro [left|right]rsasigkey= (en el que corresponda, por supuesto), como se verá a continuación; se debe hacer lo mismo en el otro nodo y ambos /etc/ipsec.conf deberán contener la parte pública de la clave de los dos nodos.

Según la versión de Frees/WAN, el contenido de este archivo no se genera bien, y puede haber problemas a la hora de iniciar la conexión. Debe confirmar los siguientes detalles:

- La línea "**: RSA {**", no aparece en el contenido del archivo *ipsec.secrets*, por lo que debe escribirla como se muestra: Escriba **:***espacio***RSA***espacio***{**
  De igual forma para cerrar las llaves al final: *tabulación***}**

  - Teniendo esto, se debe modificar el contenido del archivo *ipsec.conf,* que queda como se muestra a continuación para el host A:

```
config setup
                                interfaces=%defaultroute
                                     klipsdebug=none
                                     plutodebug=none
                                      uniqueids=yes
conn %default
                                      keyingtries=0
                                      authby=rsasig
                                        auto=start
conn prueba
                                         auto=add
                                       authby=rsasig
                                         auth=esp
                                    left=172.16.41.123

leftrsasigkey=0sAQNsU3ATU3ifMuaMgf5eGTTc7XWKSJfrmdYJ+LkCeMXJRqQnftKPZpruAVfeLAsB0
p+fblsxqBZlW60zBe5sjuBZlDdgvVIMTJU6owCVbZs7zt5ogdw371Bhd2aQGxFIOoDWLIzuiJ6tKMqDHw
Umh4UjTLNm+GwDy9J7782mz4jS6Q==
                                   right=173.16.41.124

rightrsasigkey=0sAQN+cl/LY7D6bhtqE0RvmH2qOCrDEVr5sRc4+vQtwh+K8ZPOjEJfnFXca/BF3aHc
1zKNvCfQs/ClQYxoaDtq6fRNQw/3qwiwDGcpyEFphyyO2KW3NKiHDWhbLsv17pwdnfIiIhG8GApupSDGN
POIAlZVlBCHFmuezuNf+3X1jiPN8Q==
```

- Como se observa, es necesario copiar la llave pública de cada host generada en el archivo *ipsec.secrets* (información después del parámetro pubkey=). Y de igual forma que en las veces anteriores, se debe hacer lo correspondiente en el host B, donde se debe intercambiar la dirección IP de left por right respectivamente.

- Primero que todo, verifique que cada equipo tenga definida una ruta por defecto a Internet, utilizando el comando #route –n. De lo contrario escriba el siguiente comando:
  #route –A inet add default gw 172.16.255.254

- Inicie Ethereal y a continuación inicie el servicio de IPSec con el comando:
  #service ipsec start

- Para hacer que *pluto* proceselas firmas digitales: *#ipsec auto -–ready*

- Ahora, por último, para hacer que *pluto* establezca la Asociación de Seguridad IPSec, que está configurada en el archivo *ipsec.conf* con el nombre *prueba*: *#ipsec auto --up prueba*

Una vez hecho esto, la sesión IPSec está declarada y los hosts deben comenzar a intercambiar información de forma segura, utilizando autenticación y cifrado.

- Para observar el estado de las conexiones establecidas y declaradas, utilice el comando *#ipsec whack -–status*

P.5.1 Haga un ping desde uno de los host, hacia el otro. Observa en Ethereal alguna diferencia entre las configuraciones automáticas en los puntos anteriores y con firmas RSA?

P.5.2 Cambie el tamaño de las llaves RSA a 4096 bits con el siguiente comando *#ipsec rsasigkey –verbose 4096 > /etc/ipsec.secrets.* ¿Se nota algún cambio en el archivo */etc/ipsec.secrets*? ¿En que afecta este cambio la comunicación entre los equipos?

5.2.7.4 Conclusiones

5.2.8 Práctica 6: Utilizando Openswan para configurar autenticación con Certificados Digitales

5.2.8.1 Herramienta Openswan

El primero de Marzo de 2004, los creadores de FreeS/WAN anunciaron que el proyecto FreeS/WAN había terminado por muchas razones; de esta forma, el *Proyecto Openswan* tomaría su lugar en los desarrollos. Openswan está basado en las distribuciones de Super FreeS/WAN, y ya incluye la mayoría de los parches que los usuarios querían. En este momento, su funcionamiento está basado en FreeS/WAN 1.x y 2.x. En esta práctica se va a utilizar Openswan 2.4.2-1; esta herramienta funciona igual que FreeS/WAN y utiliza los mismos comandos y los mismos archivos de configuración, ya que es la continuación de este interesante proyecto, y la única diferencia con FreeS/WAN es que no se necesita instalar los parches para soporte x.509, sino que ya soporta este tipo de autenticación, además de que soporta también autenticación del encabezado IP por medio del encabezado de Autenticación AH, entre otras funcionalidades y mejoras que se le han ido añadiendo. En las versiones de FreeS/WAN/Openswan 2.x, básicamente hay que tener dos cosas en cuenta en el archivo *ipsec.conf*: debe añadirse una línea "versión 2", al inicio del archivo indicando la versión y deben removerse las líneas "plutoload" y "plutostart" o asignarles el valor *none*. De igual forma, al utilizar certificados, éstos deben ubicarse en la ruta /etc/ipsec.d/certs/ y no en /etc/ipsec.d/, como en la versión 1.x. (ver video *openswanCertificados.camrec*, previa instalación de Camtasia, en el CD adjunto al documento).

5.2.8.2 Motivación

En esta práctica se utiliza la configuración de autenticación con Certificados Digitales x.509 para la conexión segura entre dos equipos, utilizando los archivos de configuración de Openswan.

5.2.8.3 Objetivo

- Habilitar AH y ESP para autenticación y cifrado, generar los Certificados Digitales para la autenticación y configurar los archivos de configuración respectivamente.

5.2.8.4 Desarrollo de la Práctica

Al igual que en FreeS/WAN, los archivos "ipsec.conf" e "ipsec.secrets" tienen como ruta por defecto el directorio /etc/ipsec.conf y /etc/ipsec.secrets. Esta prueba se llevó a cabo sobre dos equipos corriendo Linux Debian 3.1 y en dos equipos corriendo Linux Fedora Core 4; la única diferencia entre estas dos distribuciones es la forma de instalación, ya que la configuración es la misma en ambos sistemas operativos. En la página de Openswan, www.openswan.org/download, es posible encontrar las fuentes que pueden instalarse sobre cualquier distribución del sistema operativo Linux. El escenario de prueba para esta configuración se muestra a continuación (figura 5.7):

172.16.41.123

172.16.41.124

Figura 5.7 Escenario de Prueba de Openswan utilizando autenticación por medio de Certificados Digitales

Para crear certificados digitales es necesario crear antes una autoridad certificadora que los emita; todo esto puede llevarse a cabo utilizando la herramienta OpenSSL. Para esta prueba los certificados se generaron en una maquina corriendo sobre Linux Debian 3.1 y Debian OpenSSL 0.9.7g, pero pueden generarse en cualquier máquina corriendo cualquier plataforma Linux y con OpenSSL instalado. Los pasos a continuación aplican para cualquier plataforma, pero debe tenerse especial cuidado con los directorios en los cuales se guardan los archivos.

- Como primer paso debe editarse el archivo */etc/ssl/openssl.cnf,* así:

```
[ ca ]
default_ca = CA_prueba          #La sección de la Autoridad Certificadora por
                                defecto
[ CA_prueba ]

dir=/etc/ssl/pruebaCA     #Directorio donde se quiere guardar todo
certs=$dir/certs          #Directorio donde se guardan los certificados
crl_dir=$dir/crl        #Donde se guardan los archivos de revocación
database=$dir/index.txt   #Archivo index de la base de datos.
#unique_subject=no         #Se fija en NO para permitir la creación de varios
Certificados con el mismo subject

new_certs_dir=$dir/newcerts #Lugar por defecto para nuevos certificados
certificate=$dir/cacert.crt #El certificado de la Autoridad Certificadora
serial =$dir/serial     #El número serial actual (número de certificados)
```

```
crl=$dir/crl.pem        #El CRL actual
private_key=$dir/private/cakey.key #La clave privada
RANDFILE=$dir/private/.rand     #Archivo de número privado aleatorio

x509_extensions=usr_cert        #Extensiones para añadir al certificado
default_days=365                #Duración del certificado
```

En este archivo se define el directorio */etc/ssl/pruebaCA* como el directorio para almacenar la información referente a la entidad certificadora y a los certificados emitidos. Dentro de ese directorio se deben crear toda una serie de subdirectorios para guardar la información necesaria e imprescindible como por ejemplo el certificado o clave de la entidad (tanto privada como pública). También debe tenerse en cuenta el tiempo de caducidad por defecto; en este caso se han fijado claves con un periodo de caducidad de 1 año.

Los subdirectorios creados fueron:

#mkdir /etc/ssl/pruebaCA/
#mkdir /etc/ssl/pruebaCA/certs
#mkdir /etc/ssl/pruebaCA/private
#mkdir /etc/ssl/pruebaCA/newcerts
#mkdir /etc/ssl/pruebaCA/crl
#echo "01" > /etc/ssl/pruebaCA/serial
#touch /etc/ssl/pruebaCA/index.txt

Se ingresa al directorio donde va a estar la autoridad: #cd /etc/ssl/pruebaCA

- Con esta estructura lista, se debe crear la entidad de certificación local con el siguiente comando, el cual crea un certificado y una llave privada para el equipo donde se está creando la entidad:
  #openssl req -nodes -new -x509 -keyout private/cakey.key -out cacert.crt -days 365

El programa pregunta por datos sobre la ubicación del destinatario del certificado; hay que tener en cuenta que cuando pregunte por *Common Name* se debe colocar el nombre completo del equipo donde se encuentra ubicada la entidad certificadora, en este caso: *ryst6.unicauca.edu.co (172.16.41.106).* Después de esto se crean una llave privada (cakey.key) y una llave pública (cacert.crt), que se utilizaran para firmar los certificados creados.

- A continuación se debe realizar un requerimiento de un nuevo certificado, para uno de los clientes que utilizará dicho certificado para comunicarse con otro equipo por medio de IPSec. Para realizar el requerimiento se utiliza el siguiente comando, teniendo en cuenta que la práctica se llevo a cabo en el Laboratorio de Telecomunicaciones sobre los equipos *ryst3.unicauca.edu.co* y *ryst4.unicauca.edu.co*:
  #openssl req -nodes -new -keyout ryst3.unicauca.key -out ryst3.unicauca.csr

Esto crea una llave privada contenida en *ryst3.unicauca.key* y una solicitud de certificado en *ryst3.unicauca.csr*; el programa pregunta nuevamente por datos de la ubicación del destino del certificado y cuando pregunta por el *Common Name* se debe colocar en este caso *ryst3.unicauca.edu.co*.

- El paso siguiente es firmar la solicitud de certificado; para esto es necesario que la autoridad tenga la solicitud para generar el certificado firmado con el siguiente comando:
  #openssl ca -out ryst3.unicauca.crt -in ryst3.unicauca.csr

Después de esto, el programa pregunta si se quiere firmar el certificado: *¿Sign the Certificate? [Y/n]*, a lo que debe responder *Yes*. Listo, de igual forma debe hacerse el proceso de requerimiento y firma para el certificado del equipo ryst4.

- Con los dos certificados listos, se procede a instalar Openswan en los dos equipos; en este caso, para **Debian** se hizo uso de una utilidad del Sistema Operativo Debian llamado *apt-get,* que busca paquetes ya compilados para Debian en una serie de supositorios (páginas Web) determinados; Openswan ya existe y por eso es posible instalarlo utilizando esta herramienta. En primer lugar, si se están utilizando direcciones que no son reales, se le debe colocar el siguiente valor a esta variable de entorno para que utilice proxy:

  #export http-proxy=http://proxy.unicauca.edu.co:3128
  #export ftp-proxy=ftp://proxy.unicauca.edu.co:3128

- A continuación se debe actualizar la base de datos de paquetes descargables disponibles con el comando: *#apt-get update*

- Utilizando el siguiente comando es posible buscar si existen los instaladores para este paquete: #apt-cache search <nombre del paquete>, en este caso:
  #apt-cache search openswan

- Por último, para llevar a cabo la instalación, se debe utilizar el comando #apt-get install <nombre del paquete>, y para este caso se requieren los siguientes paquetes:
  #apt-get install kernel-patch-openswan
  #apt-get install openswan

Al instalar el paquete Openswan, se deben contestar una serie de preguntas así:

- En el cuadro *Configuración de Openswan*, presione *Enter* para Aceptar.
- En el cuadro *A qué nivel desea comenzar Openswan*, escoja *"After PCMCIA"* y presione *Enter*.

- A la pregunta: *¿Desea reiniciar Openswan?*, escoja *Si* y *Enter*.
- A la pregunta: *¿Desea habilitar Opportunistic Encryption en Openswan?*, escoja *No* y *Enter*.
- A la pregunta: *¿Desea crear un par de claves pública/privada RSA para este host?* Escoja *No* y *Enter*.

Haciendo esto en cada equipo, ya se tiene instalada la herramienta Openswan, con soporte para x.509 en Debian.

- Para Linux **Fedora Core 4** se descargó el paquete compilado de Openswan para esta distribución desde:
  http://www.openswan.org/download/binaries/fedora/4/i386/openswan2.4.2-1.i386.rpm

  Nota: Si en la máquina se encuentra instalado el paquete FreesWan, para que no se produzcan conflictos, debe desinstalarse FreesWan con el comando:
  #rpm –e freeswan-userland

- Se procede entonces a instalar Openswan con: #rpm –i openswan2.4.2-1.i386.rpm

  Con lo anterior se tiene la herramienta lista en Fedora Core 4.
- Ahora, es necesario copiar los *certificados y las llaves privadas* desde el equipo utilizado como Autoridad de Certificación, a cada uno de los equipos participantes en la configuración, en los directorios respectivos, así:

Para ryst3:

El certificado del equipo respectivamente:
#scp root@172.16.41.106:/etc/ssl/pruebaCA/ryst3.unicauca.crt /etc/ipsec.d/certs
El certificado de la autoridad certificadora:
#scp root@172.16.41.106:/etc/ssl/pruebaCA/cacert.crt /etc/ipsec.d/cacerts
La llave privada de cada equipo respectivamente:
#scp root@172.16.41.106:/etc/ssl/pruebaCA/ryst3.unicauca.key /etc/ipsec.d/private
Repita el mismo procedimiento de copia en el equipo ryst4.

- A continuación, debe llevarse a cabo la siguiente configuración en los archivos *ipsec.conf* e *ipsec.secrets* en cada uno de los equipos participantes, al igual que como se hizo en FreeS/WAN, pero indicándole que se va a utilizar autenticación por medio de certificados digitales.

En el archivo */etc/ipsec.secrets*, se escribe el texto siguiente:

```
: RSA host.example.com.key "password"
```

Donde *password* es la contraseña que se introdujo a la hora de generar el certificado de cada equipo (si se introdujo alguna, sino, se deja en blanco, así: “”).

A continuación se muestra un ejemplo del archivo */etc/ipsec.conf* para el equipo ryst3:

```
version                                 2.0

config setup
                              interfaces=%defaultroute
                                   klipsdebug=none
                                   plutodebug=none
                                    uniqueids=yes

conn %default
                                    keyingtries=0
                                    authby=rsasig
                                      auto=start

conn prueba
                                       auto=add
                                     authby=rsasig
                                        auth=ah
                                   left=172.16.41.123
                                  leftrsasigkey=%cert
                             leftcert=ryst3.unicauca.crt
                                  right=172.16.41.124
                                 rightrsasigkey=%cert
      rightid=/C=CO/ST=Cauca/L=Popayan/O=Unicauca/OU=ReddeDatos/CN=ryst4.unicauca
      .edu.co

#Disable Opportunistic Encryption
include /etc/ipsec.d/examples/no_oe.conf
```

El valor que debe introducirse en el parámetro *rightid* es el contenido en el campo *subject* del certificado y puede averiguarse en cada equipo utilizando el siguiente comando:

#openssl x509 -in /etc/ipsec.d/certs/ryst4.unicauca.crt -noout -subject

En el equipo ryst4 el archivo es igual, salvo que deben invertirse los valores de left y right; ryst4 ahora sería el equipo en left. De igual forma en ese equipo, debe colocarse el nombre respectivo a su certificado, y el *rightid* sería el de ryst3. Se coloca el *rightid* del compañero, para que Openswan pueda verificar la información que contiene el certificado.

Hay algunos cambios con respecto a los archivos de configuración vistos anteriormente, como se puede observar; en los parámetros *leftrsasigkey* y *rightrsasigkey*, se le dice a Openswan que se van a usar los certificados que están ubicados en las rutas por defecto (directorios en los que se ubicaron ya).

De esta forma ya se tiene lista la configuración; primero que todo, verifique que cada equipo tenga definida una ruta por defecto a Internet, utilizando el comando *#route –n.* De lo contrario escriba el siguiente comando: *#route –A inet add default gw 172.16.255.254*

- inicialice Ethereal para capturar los paquetes intercambiados y a continuación, inicie el servicio de IPSec con el comando:
  #service ipsec start para Fedora.
  #/etc/init.d/ipsec start para Debian.

- Para hacer que *pluto* haga la negociación de los certificados digitales, tanto en ryst3 como en ryst4:
  #ipsec auto –-ready

- Ahora, por último, para hacer que *pluto* establezca la Asociación de Seguridad IPSec, que está configurada en el archivo *ipsec.conf* con el nombre de *prueba,* tanto en ryst3 como en ryst4::
  #ipsec auto --up prueba

- Una vez hecho esto, la sesión IPSec está declarada y los hosts deben comenzar a intercambiar información de forma segura, utilizando autenticación y cifrado.

P.6.1 Observe los paquetes ISAKMP intercambiados durante la negociación. Analícelos y describa las principales características observadas.

P.6.2 Haga un ping desde uno de los host, hacia el otro y observe los paquetes intercambiados en Ethereal. ¿Observa alguna diferencia entre las configuraciones automáticas en los puntos anteriores y con certificados digitales?

5.2.8.5 Conclusiones

5.2.9 Uso de las herramientas de FreeS/WAN y Openswan

FreeS/WAN provee un comando **ipsec** que se utiliza para indicarle a **pluto** qué hacer con cada conexión "conn"; incluso para indicarle nuevas configuraciones sin tener que reiniciar el servicio de *ipsec*. A continuación se describen algunas de las formas del comando más utilizadas:

- Agrega una "conn" a las conexiones disponibles al demonio **pluto** que se esta ejecutando, este comando se utiliza cuando se agregó una sección "conn" al /etc/ipsec.conf y no se desea -- o no se puede -- bajar el servicio de IPSec:

ipsec auto --add <**conn**>

- Se le indica a **pluto** que inicie una conexión "conn":

ipsec auto --up <**conn**>

- Se le indica a **pluto** que elimine la conexión "conn" de los túneles disponibles en memoria, esto da de baja la conexión si ésta estuviera establecida:

ipsec auto --delete <**conn**>

- Determina el estado de las conexiones, de todas las conexiones, las establecidas y las declaradas:

ipsec whack --status

- Reinicia todo el servicio de IPSec:

ipsec setup restart

5.3 PRACTICA PARA LA IMPLEMENTACION DE SEGURIDAD A NIVEL DE RED SOBRE WINDOWS

5.3.1 Configuración de IPSec en Windows 2000 Server

Mediante la Seguridad del protocolo de Internet (IPSec), se puede ofrecer privacidad, integridad, autenticidad y protección contra reproducción para el tráfico de red en las siguientes situaciones:

- Seguridad extremo a extremo de cliente a servidor, servidor a servidor y cliente a cliente mediante el modo de transporte IPSec.
- Acceso remoto seguro desde el cliente a la puerta de enlace a través de Internet mediante cifrado en modo Túnel del Protocolo IPSec.

IPSec proporciona conexiones seguras entre puertas de enlace a través de redes de área extensa (WAN) externas o conexiones de Internet que utilizan túneles L2TP/IPSec o el modo de túnel IPSec puro; el modo de túnel IPSec no está diseñado para acceso remoto a redes privadas virtuales (VPN). El sistema operativo Windows 2000 Server simplifica la implantación y la administración de la seguridad de red mediante la Seguridad IP de Windows 2000, con una robusta implementación de la Seguridad del protocolo de

Internet. Diseñado por el Internet Engineering Task Force (IETF) como la arquitectura de seguridad del protocolo Internet (IP), IPSec define los formatos de paquetes IP y la infraestructura relacionada para proporcionar una eficaz autenticación de principio a fin, integridad, protección contra reproducción y, opcionalmente, confidencialidad para el tráfico de red. También se incluye un servicio a petición de negociación y administración de seguridad mediante el Internet Key Exchange (IKE, Intercambio de claves de Internet - RFC 2409), definido por el IETF. IPSec y los servicios relacionados en Windows 2000 se han desarrollado conjuntamente entre Microsoft y Cisco Systems, Inc.

La seguridad IP de Windows 2000 se basa en la arquitectura IETF IPSec al integrarse con los dominios de Windows 2000 y los servicios Active Directory si es el caso. La implementación del IKE proporciona tres métodos de autenticación basados en estándares del IETF para establecer la confianza entre sistemas:

- Autenticación Kerberos v5, proporcionada por la infraestructura de dominio basada en Windows 2000, que se utiliza para distribuir comunicaciones seguras entre equipos en un dominio o en dominios de confianza.
- Firmas de clave pública o privada que utilizan certificados, compatibles con algunos sistemas de certificados como los de Microsoft, Entrust, Verisign y Netscape.
- Contraseñas, llamadas *claves de autenticación compartidas previamente*, que se utilizan estrictamente para establecer relaciones de confianza entre equipos, no para protección de los paquetes de datos de las aplicaciones.

Una vez que los equipos del mismo nivel se han autenticado mutuamente, generan claves de cifrado en volumen con el fin de cifrar los paquetes de datos de las aplicaciones. Ambos equipos conocen estas claves, de manera que los datos se encuentran muy bien protegidos contra modificaciones o interpretaciones por parte de atacantes que pudieran actuar en la red. Cada equipo del mismo nivel utiliza IKE para negociar el tipo y la intensidad de las claves que se utilizarán, así como el tipo de seguridad con el que se protegerá el tráfico de aplicaciones. Las claves se actualizan automáticamente, según la configuración de la directiva IPSec, de forma que proporcionen una protección constante bajo el control del administrador.

5.3.1.1 Escenarios para utilizar IPSec de extremo a extremo

La Seguridad del Protocolo de Internet (IPSec) en Windows 2000 esta diseñada para que la distribuyan los administradores de redes, de forma que los datos de aplicación de los usuarios puedan protegerse de manera transparente. En todos los casos, la utilización de la autenticación Kerberos y confianza de dominios es la elección más sencilla para la distribución. Los certificados o las claves previamente compartidas pueden utilizarse para dominios sin confianza o interoperabilidad con terceros. La Directiva de grupo puede utilizarse para ofrecer la configuración de IPSec, conocida como una *directiva IPSec*, a varios clientes y servidores.

5.3.1.2 Servidores seguros

La seguridad IPSec para todo el tráfico IP de unidifusión es *solicitada pero opcional*, o bien *solicitada y necesaria*, según establezca la configuración del servidor llevada a cabo por el administrador. Mediante este modelo, los clientes solamente necesitan una directiva predeterminada para responder a las peticiones de seguridad de los servidores. Una vez que se han establecido las asociaciones de seguridad IPSec entre el cliente y el servidor, una en cada dirección, permanecerán vigentes durante una hora después de que se haya enviado el último paquete. Transcurrida esa hora, el cliente borrará las asociaciones de seguridad y volverá al estado inicial "sólo responder". Si el cliente envía paquetes sin proteger al mismo servidor otra vez, el servidor volverá a establecer la seguridad IPSec. Éste es el enfoque más sencillo y puede llevarse a cabo con seguridad siempre que los primeros paquetes enviados por la aplicación no contengan datos delicados y que se permita al servidor recibir de los clientes paquetes de texto sin formato y sin proteger. Esta configuración del servidor resulta apropiada únicamente para servidores de red internos, ya que el servidor se configura mediante directiva IPSec para que admita paquetes entrantes de texto sin formato y sin proteger. Si el servidor se coloca en Internet NO se debe utilizar esta configuración, debido a la posibilidad de que los ataques de denegación de servicio puedan aprovecharse de la capacidad del servidor para recibir paquetes entrantes sin proteger.

Si se puede tener acceso al servidor directamente desde Internet o si los primeros paquetes del cliente contienen datos delicados, el cliente debe recibir una directiva IPSec para que solicite seguridad IPSec para el tráfico cuando intente enviar datos al servidor. Esto se mostrará más adelante con la Configuración de acciones de Filtrado IPSec; de esta forma, los clientes y servidores pueden tener reglas específicas para permitir, bloquear o proteger sólo ciertos paquetes de red, específicos del protocolo o del puerto. Este enfoque es más difícil de configurar y resulta más propenso a errores, ya que requiere un profundo conocimiento del tipo de tráfico de red que envía y recibe una aplicación, además de coordinación administrativa para asegurar que todos los clientes y servidores tengan directivas compatibles.

5.3.1.3 Impacto de la directiva Servidor seguro en un equipo

Sólo los clientes IPSec que puedan llevar a cabo la negociación correctamente podrán comunicarse con el equipo servidor seguro. Así mismo, el Servidor Seguro no podrá comunicarse con ningún otro equipo, como los Servidores del Sistema de Nombres de Dominio (DNS), a no ser que se pueda proteger el tráfico mediante IPSec. Dado que en el servidor se ejecutan muchos procesos en segundo plano, es probable que no puedan comunicarse y generen mensajes de registro de suceso. Esto es normal, ya que la directiva Servidor seguro predeterminada es muy severa e intenta proteger casi todos los paquetes IP antes de permitir que pasen a la red. Para un uso real en entornos de producción, deberá crear una directiva personalizada que tenga el comportamiento deseado, de acuerdo con los requisitos de seguridad, la topología de la red y la utilización de aplicaciones de servidor específicas.

- *Permitir que clientes no IPSec puedan comunicarse con un servidor*

Para permitir que también se puedan comunicar los clientes no IPSec, debe asignar la directiva *Servidor* en lugar de la directiva *Servidor Seguro*. Esta directiva siempre solicita seguridad, pero permite la comunicación no segura con los clientes y vuelve al texto sin formato si el cliente no contesta a la petición de negociación de IKE. Si el cliente contesta en algún momento, se entabla una

negociación que debe completarse con éxito. Si la negociación falla, la comunicación se bloquea durante un minuto y se vuelve a intentar otra negociación. Para obtener más información acerca de la configuración que se utiliza para controlar este comportamiento, consulte la sección *Configurar una Acción de Filtrado IPSec,* más adelante

5.3.2 Práctica 7. Configuración de Seguridad entre dos equipos Windows

5.3.2.1 Motivación

La idea de esta práctica es conocer y comprender el funcionamiento de IPSec de Windows 2000. Se puede configurar una directiva de seguridad IP localmente en cada equipo y, posteriormente, implementar esta directiva y comprobar los resultados para obtener comunicaciones de red seguras (ver videos *windows.camrec*, previa instalación de Camtasia, en el CD adjunto al documento). Para llevar a cabo esta práctica, es necesario el siguiente hardware:

- Dos equipos que ejecuten el sistema operativo Windows 2000. Se pueden utilizar dos sistemas Windows 2000 Professional o Server, uno que actúe como cliente y otro que actúe como servidor por lo que respecta a IPSec. Los dos sistemas de pruebas deben ser miembros del mismo dominio de Active Directory si se tiene implementado, o bien estar dentro de un dominio de confianza.
- Una LAN o una WAN para conectar estos dos equipos.

5.3.2.2 Objetivos

- Crear una directiva IPSec propia.
- Comprobar el estado de la seguridad IP entre dos equipos Windows.
- Recolectar información de la conexión segura.
- Utilizar Certificados para realizar la autenticación de una conexión segura.

5.3.2.3 Desarrollo de la Práctica

La topología utilizada será la siguiente (figura 5.8):

172.16.41.107

172.16.41.105

Figura 5.8 Escenario de Prueba de IPSec entre dos equipos Windows

Antes de comenzar es necesario recolectar la siguiente información sobre ambos equipos:

- El nombre del equipo (haga click con el botón secundario del *mouse* en el icono *Mi PC* del escritorio, haga click en *Propiedades* y, a continuación, en la ficha *Identificación de red*).
- La dirección IP; haga click en *Inicio*, en *Ejecutar*, escriba *cmd* y después haga click en *Aceptar*. Escriba *ipconfig* en el símbolo del sistema y presione *Entrar*. Una vez obtenida la dirección IP, escriba *exit* y presione *Entrar*.

➢ *Crear una consola personalizada*

- Inicie una sesión en el primer equipo como un usuario con privilegios administrativos. En nuestro caso, el primer equipo se llama Ryst7 (Nota: En el resto del documento, Ryst7 hace referencia al primer equipo de prueba y Ryst5 al segundo equipo de prueba. Si sus equipos tienen nombres diferentes, asegúrese de seguir los pasos utilizando el nombre correcto).

- Crear una consola MMC personalizada. En el escritorio de Windows, haga click en *Inicio*, *Ejecutar* y en el cuadro de texto Abrir escriba ***mmc***. Haga click en *Aceptar*.

  En el menú Consola, haga click en *Agregar o quitar complemento*. En el cuadro de diálogo Agregar o quitar complemento, haga click en *Agregar*. En el cuadro de diálogo Agregar un complemento independiente, haga click en *Administración de Equipos* y, a continuación, haga click en *Agregar*. Compruebe que *Equipo local* está seleccionado y haga click en *Finalizar*.

- En el cuadro de diálogo Agregar un complemento independiente, haga click en *Directiva de grupo* y, a continuación, haga click en *Agregar*. Compruebe que *Equipo Local* está seleccionado en el cuadro de diálogo del objeto Directiva de Grupo y haga click en *Finalizar*.

- En el cuadro de diálogo Agregar un complemento independiente, haga click en *Certificados* y, a continuación, haga click en *Agregar*. Seleccione *Cuenta de Equipo* y, a continuación, haga click en *Siguiente*. Compruebe que Equipo Local está seleccionado y haga click en *Finalizar*. Para cerrar el cuadro de diálogo Agregar un complemento independiente, haga click en *Cerrar*. Para cerrar el cuadro de diálogo Agregar o quitar complemento, haga click en *Aceptar.*

En este punto, como resultado se obtienen 3 elementos añadidos en la consola, panel derecho: *Administración de Equipos, Directiva de Grupo y Certificados*.

➢ *Habilitar la directiva de auditoria en el equipo:*

En el siguiente procedimiento, se configurará la auditoria para que se anote un suceso cuando IPSec se vea envuelto en la comunicación. Posteriormente, estas anotaciones servirán como confirmación de que IPSec funciona correctamente.

- En la Consola MMC, seleccione *Directiva de Equipo Local* en el panel izquierdo y haga click en + para expandir el árbol. Expanda la opción *Configuración del Equipo*, *Configuración de Windows*, *Configuración de la Seguridad*, *Directivas Locales* y seleccione *Directiva de Auditoria* (ver figura 5.9).

- Desde la lista de Atributos que aparece en el panel derecho, haga doble click en *Auditar Sucesos de Inicio de Sesión*. Aparecerá el cuadro de diálogo Auditar Sucesos de Inicio de Sesión. En el cuadro de diálogo Auditar sucesos de Inicio de Sesión, haga click para activar ambas casillas de verificación *Auditar estos intentos: Correcto y Error* y haga click en *Aceptar*. Repita los pasos anteriores para el atributo *Auditar el Acceso a Objetos*.

➢ *Configurar el Monitor de seguridad IP*

Para supervisar las conexiones de seguridad correctas que creará la directiva IPSec, utilice la herramienta Monitor de seguridad IP. Antes de crear ninguna directiva, inicie y configure la herramienta.

- Para iniciar el Monitor de seguridad IP, haga click en *Inicio*, haga click en *Ejecutar* y escriba ***ipsecmon*** en el cuadro de texto Abrir. Haga click en *Aceptar*. Haga click en *Opciones en el Monitor de Seguridad IP* y cambie el valor predeterminado de Cantidad de segundos de actualización de 15 a 1. Haga click en *Aceptar.*

- Minimice la ventana del Monitor de seguridad IP. Esta herramienta minimizada se utilizará para supervisar las directivas que se configurarán posteriormente.

Repita todo este procedimiento en el segundo equipo, Ryst5, desde la sección de *Creación de una consola personalizada.*

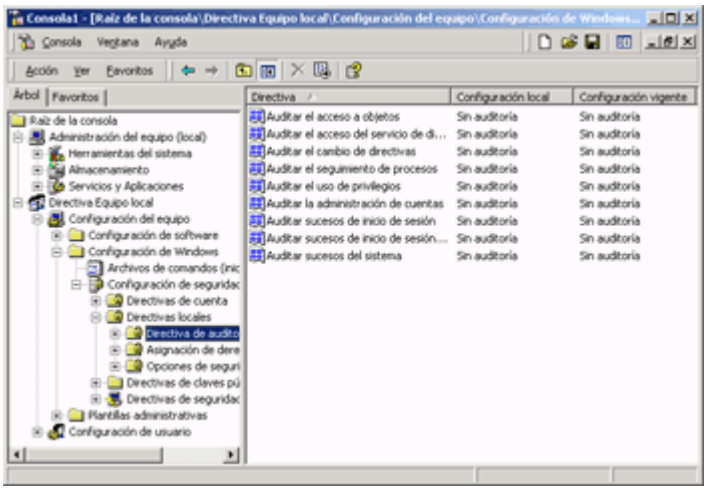


Figura 5.9 Desplazarse a Directiva de auditoria en la Consola de IPSec

➢ *Crear una Directiva IPSec Personalizada*

Si desea proteger el tráfico entre dos equipos que deben comunicarse con otros equipos sin necesidad de una conexión segura, debe crear una *Directiva Personalizada*, ya que las Directivas Integradas (las que vienen por defecto) requieren la autenticación Kerberos que proporciona el controlador de dominio. Existen otras razones para crear una directiva personalizada, como por ejemplo si desea proteger el tráfico basado en direcciones de red. A continuación se creará una directiva IPSec personalizada, para la cual se definirá una regla de seguridad, a continuación se definirá una lista de filtros y finalmente se especificará la acción de filtrado.

- Para crear una directiva IPSec: En el equipo Ryst7, en el panel izquierdo de la Consola MMC, haga click con el botón secundario del mouse en *Directivas de Seguridad IP en la Máquina Local* y, a continuación, haga click en *Crear Directiva de Seguridad IP*. Aparecerá el Asistente para directivas de seguridad IP. Haga click en *Siguiente*.

  Escriba *PruebaIPSec* como el nombre de la directiva (o el nombre que prefiera) y haga click en *Siguiente*. Desactive la casilla de verificación *Activar la Regla de respuesta predeterminada* y haga click en *Siguiente*. Asegúrese de que la casilla de verificación *Modificar propiedades* está activada (la opción predeterminada es que sí lo esté) y haga click en *Finalizar*.

- En el cuadro de diálogo *Propiedades* de la directiva que acaba de crear, asegúrese de que la casilla de verificación *Usar el asistente para agregar* de la esquina inferior derecha se encuentra activada y haga click en *Agregar* para iniciar el *Asistente para Reglas de Seguridad*. Haga click en *Siguiente* para avanzar por el Asistente.

- Seleccione *Esta regla no especifica un túnel* (opción predeterminada) y haga clic en *Siguiente*. Seleccione el botón de radio *Todas las conexiones de red* (opción predeterminada) y haga clic en *Siguiente*.

➢ *Configurar un método de autenticación IKE*

A continuación se especificará la manera de que los equipos confíen unos en otros, bien especificando el modo en que se autentifican a sí mismos o demuestran su identidad a los demás al intentar establecer una asociación de seguridad. IKE para Windows 2000 proporciona tres métodos de autenticación para establecer la confianza entre equipos:

- **Autenticación Kerberos v5** proporcionada por el dominio Windows 2000 que sirve como *Centro de Distribución de Claves Kerberos v5* (KDC). Éste proporciona una cómoda implantación de comunicaciones seguras entre equipos Windows 2000 que son miembros de un dominio o a través de dominios de confianza. IKE sólo utiliza las propiedades de autenticación de Kerberos. La generación de claves para asociaciones de seguridad IPSec se realiza mediante métodos IKE RFC 2409.
- **Firmas de clave pública o privada** que utilizan certificados compatibles con algunos sistemas de certificados, incluidos los de Microsoft, Entrust, Verisign y Netscape.
- **Clave previamente compartida**, que es una contraseña utilizada estrictamente para establecer la confianza entre equipos.

En esta prueba se va a utilizar la autenticación de clave *previamente compartida*. Esta clave es una palabra o frase que deben conocer tanto el emisor como el receptor para confiar el uno en el otro. Ambos extremos de la comunicación IPSec deben conocer este valor. No se utiliza para cifrar los datos de aplicación; se utiliza únicamente durante la negociación para establecer si los dos equipos confiarán el uno en el otro. La negociación IKE utiliza este valor, pero no lo envía a través de la red. Sin embargo, la clave de autenticación se almacena como texto sin formato dentro de la directiva IPSec. Cualquier persona con acceso administrativo al equipo puede ver el valor de la clave de autenticación. El administrador debe establecer controles de acceso personalizados en el directorio de la directiva IPSec para evitar que los usuarios normales puedan leer la directiva IPSec. Por lo tanto, Microsoft no recomienda el uso de una clave previamente compartida para la autenticación IPSec, excepto con fines de prueba o en aquellos casos en los que sea necesario para la interoperabilidad con implementaciones IPSec de terceros. En su lugar, Microsoft recomienda utilizar la autenticación de certificados.

- Para configurar el método de autenticación para la regla: Elija *Usar esta cadena para proteger el intercambio de claves* y escriba la cadena *ABC123*. No debe utilizar una cadena en blanco. Haga clic en *Siguiente*.

➢ *Configurar una lista de filtros IPSec*

La seguridad IP se aplica a los paquetes IP a medida que se envían y se reciben. Los paquetes se comparan con filtros al ser enviados (salientes) para ver si se deben proteger, bloquear o enviar como texto sin formato. Los paquetes también se comparan al ser recibidos (entrantes) para ver si se deberían haber protegido y para bloquearlos o permitirles entrar en el sistema. Hay dos tipos de filtros: los que controlan la *seguridad del modo de transporte IPSec*, y los que controlan la *seguridad del modo de túnel IPSec*.

Los filtros de túnel IPSec se aplican primero a todos los paquetes. A continuación, si no coincide ninguno, se examinan los filtros de modo de transporte IPSec. Debido al diseño de los filtros de transporte IPSec de Windows 2000, algunos tipos de tráfico IP no se pueden proteger, entre los que se encuentran:

- Direcciones de difusión, terminadas generalmente en .255, con máscaras de subred adecuadas.
- Direcciones de multidifusión desde 224.0.0.0 hasta 239.255.255.255.
- Tipo de protocolo 46 de RSVP IP. Este tipo está pensado para señalizar las peticiones de Calidad de servicio (QOS) para datos de aplicación que sí se pueden proteger mediante IPSec.
- Origen UDP o puerto de destino 88 de Kerberos. Kerberos es un protocolo seguro utilizado por la negociación IKE de IPSec para autenticar otros equipos de un dominio.
- Puerto UDP de destino 500 de IKE. Esto es necesario para permitir que IKE negocie los parámetros de la seguridad IPSec.

Estas excepciones se aplican a los filtros de modo de transporte IPSec. Los filtros de modo de transporte se aplican a los paquetes de host que tienen una dirección de origen del equipo que ha remitido el paquete, o una dirección de destino del equipo que va a recibir el paquete. Los túneles IPSec sólo pueden proteger el tráfico IP de unidifusión; los filtros utilizados para túneles IPSec deben basarse únicamente en direcciones, no en campos de protocolo ni de puerto. Si el filtro de túnel fuese específico de un protocolo o puerto, ciertos fragmentos del paquete original no se enviarían a través del túnel y se perdería el paquete IP completo. Si se reciben en una interfaz paquetes de unidifusión Kerberos, IKE o RSVP y se redirigen a otra interfaz mediante el reenvío de paquetes o el Servicio de enrutamiento y acceso remoto, no quedan eximidos de los filtros de modo de túnel IPSec y pueden enviarse a través del túnel. Los filtros de modo de túnel IPSec no pueden filtrar paquetes de multidifusión o de difusión, por lo tanto no se pueden enviar por el túnel IPSec.

Asegúrese siempre de *reflejar* los filtros al configurar filtros IP para tráfico que se debe proteger. Reflejar los filtros configura automáticamente tanto los filtros entrantes como los salientes. Configure los filtros entre los dos equipos; debe configurar un filtro saliente que especifique su dirección IP como la dirección de origen y la dirección de su compañero como la dirección de destino. A continuación la configuración del proceso de reflejo configurará automáticamente un filtro entrante que especifique la dirección de su compañero como dirección de origen y la dirección IP de su equipo como destino. En este sencillo caso, habrá sólo una especificación de filtro reflejado en la lista de filtros. Es necesario definir la misma lista de filtros en ambos equipos.

- Para configurar una Lista de filtros IP:

En el cuadro de diálogo *Lista de Filtros IP*, haga click en *Agregar* (figura 5.10). Aparecerá una lista vacía de filtros IP. Llame al filtro *Filtro de PruebaIPSec*. Asegúrese de que ha seleccionado *Usar el asistente para agregar* en la parte derecha de la pantalla y haga click en *Agregar*. Así se iniciará el *Asistente para Filtros IP*. Haga click en Siguiente para continuar.

- Para aceptar *Mi dirección IP* como la dirección de origen predeterminada, haga click en *Siguiente*. Elija *Una dirección IP específica* en el cuadro de lista desplegable, escriba la Dirección IP del compañero y haga click en *Siguiente*. Haga click en *Siguiente* para aceptar el tipo de protocolo *Cualquiera*.

- Asegúrese de que la casilla de verificación *Modificar Propiedades* está desactivada (opción predeterminada) y haga click en *Finalizar*. Haga click en *Cerrar* para abandonar el cuadro de diálogo Lista de filtros IP y volver al Asistente para regla nueva. En el cuadro de diálogo *Lista de filtros IP*, seleccione el botón de radio que se encuentra junto a *Filtro de PruebaIPSec.*

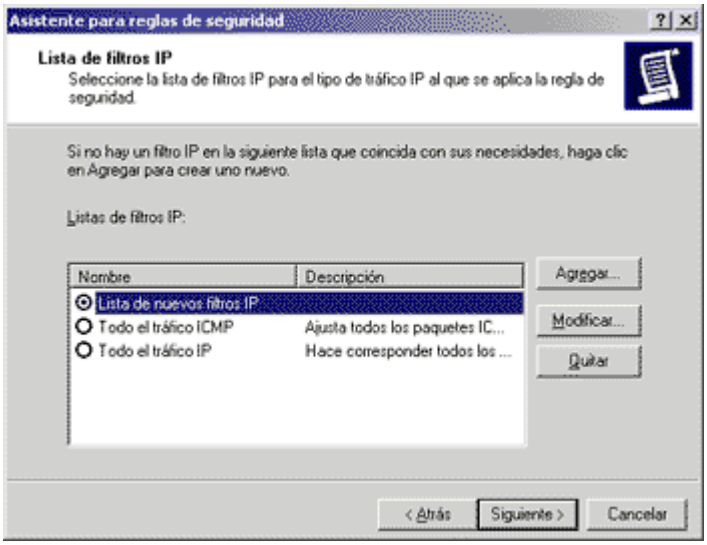


Figura 5.10 Crear un nuevo filtro IP

- Haga click en *Siguiente*. Lea la siguiente sección antes de realizar los pasos necesarios para configurar la acción de filtrado.

➢ *Configurar una acción de filtrado IPSec*

Hasta este momento se acaban de configurar los filtros de entrada y de salida para paquetes TCP/IP coincidentes. Lo siguiente consiste en configurar la acción que se realizará con esos paquetes. Los paquetes que coincidan con los filtros se pueden permitir, bloquear o proteger; si desea proteger el tráfico, ambos equipos deben tener configurada una directiva de negociación *compatible*. Las directivas predeterminadas integradas resultan adecuadas para probar las distintas características. Si desea experimentar con capacidades específicas, deberá crear su propia acción de filtrado.

Existen dos métodos para permitir la comunicación entre equipos que no pueden utilizar IPSec:

- Utilizar la acción de filtrado *Permitir* para permitir que los paquetes se envíen sin cifrar o sin proteger. Utilice esta acción junto con un filtro que haga coincidir el tráfico que desea permitir en su propia regla dentro de la directiva IPSec. Los usos habituales de este método son permitir tráfico de tipo ICMP, DNS o SNMP, o permitir tráfico hacia ciertos destinos, como la puerta de enlace predeterminada, servidores DHCP y DNS u otros sistemas no IPSec.

- Configurar la acción de filtrado para que utilice la configuración *Retroceso a comunicación no segura*. Esta opción aparecerá en el asistente. Si se selecciona esta opción en el asistente se habilitará el parámetro de la acción de filtrado *Permitir la comunicación no segura con equipos no compatibles con IPSec*. Utilizar esta configuración permite la comunicación no segura con un destino, al retroceder a texto sin formato si el destino *no contesta a la petición de negociación IKE*. Si el cliente contesta en algún momento, se entabla una negociación que debe completarse con éxito. Si la negociación IKE falla, los paquetes salientes que coincidan con el filtro se desecharán o bloquearán durante un minuto, después de lo cual otro paquete saliente provocará que se intente otra negociación IKE. Esta configuración sólo afecta a las negociaciones IKE que inicie el equipo. No tiene efecto sobre los equipos que reciben una petición y por lo tanto responden a ella. El estándar IKE no proporciona un método para que ambos sitios negocien la vuelta al modo normal, no seguro o de texto sin formato.

Ahora, para configurar la acción de filtrado:

- En el cuadro de diálogo *Acción de filtrado* que se muestra en la Figura 5.11, active la casilla de verificación *Usar asistente para agregar* y, a continuación, haga click en *Agregar*. Haga click en *Siguiente* para dirigirse al Asistente para acciones de filtrado.

- Llame a esta acción de filtrado *Acción de filtrado de PruebaIPSec* y haga click en *Siguiente*. En el cuadro de diálogo *Opciones generales de acciones de filtrado*, seleccione *Negociar la seguridad* y haga click en *Siguiente*.
- En la siguiente página del asistente, haga click en *No comunicar con equipos que no son compatibles con IPSec* y, a continuación, haga click en *Siguiente*. Seleccione *Media* en la lista de métodos de seguridad y haga click en *Siguiente*. Asegúrese de que la casilla de verificación *Modificar Propiedades* está desactivada (opción predeterminada) y haga click en *Finalizar* para cerrar este asistente.

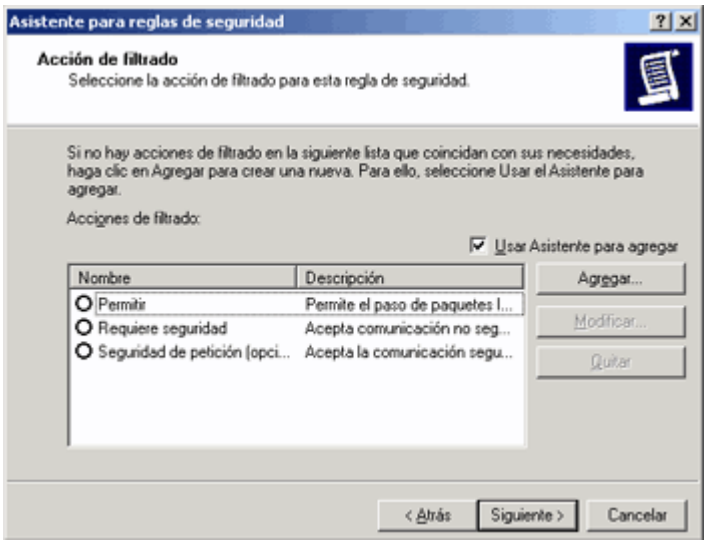


Figura 5.11 Configurando la Acción de Filtrado

- En el cuadro de diálogo *Acción de filtrado*, haga click en el botón de radio que se encuentra junto a *Acción de filtrado de PruebaIPSec* y haga click en *Siguiente*. Asegúrese de que la casilla de verificación *Modificar propiedades* está desactivada (opción predeterminada) y haga click en *Finalizar*.

Se acaba de configurar la acción de filtrado que se utilizará durante las negociaciones con su compañero. Tenga en cuenta que esta acción de filtrado puede volver a utilizarse en otras directivas. Haga click en *Cerrar* en la página Propiedades que aparecerá. Acaba de configurar con éxito una directiva IPSec. Antes de continuar, *repita todos los pasos de este procedimiento* en el equipo Ryst5.

➢ *Comprobar la Directiva IPSec Personalizada*

Ahora que ya se ha creado una directiva IPSec, debe comprobarse antes de aplicarla en una red. En el panel izquierdo de la consola MMC, seleccione *Directivas de Seguridad IP en la Máquina Local.* Observe que además de las tres directivas integradas, en el panel derecho aparece la directiva *pruebaIPSec* que se acaba de configurar.

- Haga click con el botón secundario del mouse en *pruebaIPSec* y haga click en la opción *Asignar* del menú contextual. El estado de la columna *Directiva asignada* deberá cambiar de No a Sí. Antes de continuar, lleve a cabo este paso en ambas máquinas.

- Inicialice el Analizador de Protocolos Ethereal en un equipo diferente a los que está utilizando y coloque como filtro la dirección de uno de los equipos de la configuración, así: *!arp && host 172.16.41.107*

- Abra una ventana de línea de comandos y escriba *ping dirección_ip_compañero*. Deberá recibir cuatro respuestas *Negociando la seguridad IP*. Repita el comando, deberá recibir cuatro respuestas de ping correctas.

P.7.1 Analice los paquetes intercambiados y describa las cabeceras de seguridad.

- Restaure la ventana *Monitor de seguridad IP,* minimizada anteriormente. Deberá ver los detalles de la Asociación de seguridad actualmente en uso entre los dos equipos, así como estadísticas del número de bytes Autenticados y Confidenciales transmitidos, entre otras.

P.7.2 Describa las asociaciones de Seguridad establecidas.

- Desasigne la directiva pruebaIPSec en uno de los equipos y devuélvalo al estado anterior. Esta vez, cuando haga click con el botón secundario del mouse sobre la directiva, haga click en *Desasignar*.

P.7.3 Haga ping desde el Host1 al Host2. ¿Qué respuesta espera obtener?

➢ *Utilizar la autenticación de certificados*

La implementación de IPSec en Windows 2000 proporciona la capacidad de autenticar equipos con IKE mediante certificados. Todas las validaciones de certificados las lleva a cabo la API de cifrado (CAPI). IKE solamente sirve para negociar los certificados a utilizar y proporciona seguridad para el intercambio de credenciales de certificados. La directiva IPSec especifica la entidad emisora (CA) raíz que se utilizará, no el certificado específico. Ambos extremos deben tener una CA raíz común en la configuración de sus directivas IPSec. He aquí los requisitos del certificado que se utilizará en IPSec:

- Certificado almacenado en la cuenta del equipo (almacén del equipo)
- El certificado contiene una clave pública RSA que tiene su correspondiente clave privada RSA que se puede utilizar para firmas RSA.
- Se utiliza durante un determinado período de validez
- Se confía en la entidad emisora raíz
- Se puede construir una cadena válida de entidades emisoras mediante el módulo CAPI

Estos requisitos son muy elementales. IPSec no requiere que el certificado de la máquina sea del tipo IPSec, ya que las entidades emisoras existentes puede que no emitan este tipo de certificados.

➢ *Generación de Certificados para Windows*

Para crear certificados digitales en general es necesario crear antes una autoridad certificadora que los emita; todo esto puede llevarse a cabo utilizando la herramienta OpenSSL, como se hizo anteriormente. Para esta prueba los certificados se generaron en una maquina corriendo sobre Linux Debian 3.1 y Debian OpenSSL 0.9.7g, pero pueden generarse en cualquier máquina corriendo cualquier plataforma Linux y con OpenSSL instalado. Los pasos a continuación aplican para cualquier plataforma, pero debe tenerse especial cuidado con los directorios en los cuales se guardan los archivos.

- Como primer paso debe editarse el archivo */etc/ssl/openssl.cnf,* así:

```
[ ca ]
default_ca = CA_prueba          #La sección de la Autoridad Certificadora por
                                defecto
[ CA_prueba ]

dir=/etc/ssl/pruebaCA     #Directorio donde se quiere guardar todo
certs=$dir/certs          #Directorio donde se guardan los certificados
crl_dir=$dir/crl        #Donde se guardan los archivos de revocación
database=$dir/index.txt   #Archivo index de la base de datos.
#unique_subject=no        #Se fija en NO para permitir la creación de varios
Certificados con el mismo subject

new_certs_dir=$dir/newcerts #Lugar por defecto para nuevos certificados
certificate=$dir/cacert.crt #El certificado de la Autoridad Certificadora
serial =$dir/serial     #El número serial actual (número de certificados)
crl=$dir/crl.pem        #El CRL actual
private_key=$dir/private/cakey.key #La clave privada
RANDFILE=$dir/private/.rand     #Archivo de número privado aleatorio

x509_extensions=usr_cert        #Extensiones para añadir al certificado
default_days=365                #Duración del certificado
```

En este archivo se define el directorio */etc/ssl/pruebaCA* como el directorio para almacenar la información referente a la entidad certificadora y a los certificados emitidos. Dentro de ese directorio se deben crear toda una serie de subdirectorios para guardar la información necesaria e imprescindible como por ejemplo el certificado o clave de la entidad (tanto privada como pública). También debe tenerse en cuenta el tiempo de caducidad por defecto; en este caso se han fijado claves con un periodo de caducidad de 1 año.

Los subdirectorios creados fueron:

#mkdir /etc/ssl/pruebaCA/
#mkdir /etc/ssl/pruebaCA/certs
#mkdir /etc/ssl/pruebaCA/private
#mkdir /etc/ssl/pruebaCA/newcerts
#mkdir /etc/ssl/pruebaCA/crl
#echo "01" > /etc/ssl/pruebaCA/serial
#touch /etc/ssl/pruebaCA/index.txt

- Con esta estructura lista, se debe crear la entidad de certificación local con el siguiente comando, el cual crea un certificado y una llave privada para el equipo donde se está creando la entidad:

  #cd pruebaCA

  #openssl req -nodes -new -x509 -keyout private/cakey.key -out cacert.crt -days 365

El programa pregunta por datos sobre la ubicación del destinatario del certificado; hay que tener en cuenta que cuando pregunte por *Common Name* se debe colocar el nombre completo del equipo donde se encuentra ubicada la entidad certificadora, en este caso: *ryst13.unicauca.edu.co.* Después de esto se crean una llave privada (cakey.key) y una llave pública (cacert.crt), que se utilizaran para firmar los certificados creados.

- A continuación se debe realizar un requerimiento de un nuevo certificado, para uno de los clientes que utilizará dicho certificado para comunicarse con otro equipo por medio de IPSec. Para realizar el requerimiento se utiliza el siguiente comando, teniendo en cuenta que la práctica se llevo a cabo en el Laboratorio de Telecomunicaciones sobre los equipos ryst5.unicauca.edu.co y ryst7.unicauca.edu.co:

  #openssl req -nodes -new -keyout ryst5.unicauca.key -out ryst5.unicauca.csr

Esto crea una llave privada contenida en *ryst5.unicauca.key* y una solicitud de certificado en *ryst5.unicauca.csr*; el programa pregunta nuevamente por datos de la ubicación del destino del certificado y cuando pregunta por el *Common Name* se debe colocar en este caso ryst5.unicauca.edu.co.

- El paso siguiente es firmar la solicitud de certificado; para esto es necesario que la autoridad tenga la solicitud para generar el certificado firmado con el siguiente comando:

  #openssl ca -out ryst5.unicauca.crt -in ryst5.unicauca.csr

Después de este comando, se pregunta si se desea firmar el certificado, a lo que se debe responder afirmativamente: *¿Sign the certificate? [Y/n]: Y*

- Para que los clientes Windows puedan entender los certificados generados en plataformas Linux, estos deben convertirse al formato *.p12, los cuales son *certificados para el intercambio de información personal*; en estos certificados se incluye la llave privada correspondiente a la llave publica generada para ryst5 y firmada por la entidad certificadora. Para esto se utiliza el siguiente comando:

  #openssl pkcs12 -export -in ryst5.unicauca.crt -inkey ryst5.unicauca.key -certfile /usr/ssl/pruebaCA/cacert.crt -out ryst5.unicauca.p12

Después de este comando pregunta por un password de exportación; introduzca un password fácil de recordar, ya que se utilizará más adelante al importarlo en el equipo respectivo; en este caso: *Enter export password: ryst5*

Compruebe que la inscripción del certificado se ha llevado a cabo correctamente; la carpeta *Certificados Personales* en el equipo del cliente Windows debe contener el nombre del certificado de ese equipo respectivamente.

Ahora en el equipo Windows:

- Copie al Escritorio el certificado **.p12** del equipo donde tiene la Autoridad Certificadora al equipo donde se encuentra el cliente Windows, utilizando SSH y SFTP.

- Abra la consola MMC; en el panel izuierdo escoja *Certificados (Equipo Local)* y seleccione la carpeta *Personal*; en el panel derecho, oprima el botón derecho del mouse. Seleccione *Todas las Tareas*, luego *Importar*. En el asistente para Importación de Certificados, dé click en *Siguiente*. Escoja el archivo .p12 respectivo y dé click en *Siguiente*. Escriba la contraseña que introdujo a la hora de la exportación, en este caso *ryst5*; escoja *Colocar todos los Certificados en el Siguiente Almacén* y verifique que está seleccionada la carpeta *Personal*. Dé click en *Siguiente* y por último en *Aceptar*. Haga click en el símbolo + que se encuentra junto a Certificados (Equipo local) para expandirlo. Expanda la carpeta Personal y haga click en la carpeta *Certificados*. En el panel derecho deberá ver un certificado emitido para el Administrador o para el nombre de usuario con el que inició la sesión en el equipo *ryst5* y un certificado de la CA, *ryst13*.

- Haga doble click en el certificado *ryst5* del panel derecho. Deberá contener el mensaje "*Tiene una clave privada correspondiente a este certificado*". Observe el nombre de la CA donde aparece Emitido por: (en nuestro ejemplo es Unicauca). Haga click en *Aceptar*. Si en las propiedades del certificado del equipo aparece *"No tiene una clave privada correspondiente a este certificado",* la suscripción ha sufrido un error y el certificado no servirá para la autenticación IKE de IPSec. Es necesario obtener correctamente una clave privada que corresponda a la clave pública del certificado del equipo.

- Expanda *Entidades emisoras raíz de confianza* y haga click en la carpeta *Certificados*. Copie el certificado ryst13.unicauca.p12 en la carpeta Certificados; desde este momento se puede confiar en el certificado. *Repita todos los pasos de este procedimiento* para recuperar un certificado en la otra máquina de pruebas (ryst7).

  - *Configurar la autenticación del certificado para una regla*

Si va a crear una nueva regla, puede buscar la entidad emisora que se utilizará. Se trata de una lista de certificados de entidades emisoras que se encuentran en la carpeta *Entidades emisoras raíz de confianza*, no una lista de los certificados personales de

su equipo. Esta especificación de CA en una regla IPSec tiene dos finalidades. En primer lugar, proporciona IKE con una CA raíz en la que confía. IKE en su equipo enviará una petición de un certificado válido a esta CA raíz para el otro equipo. En segundo lugar, la especificación de la CA proporciona el nombre de la CA raíz que utilizará el equipo para buscar su propio certificado personal en respuesta a una petición del interlocutor. (Precaución: Debe seleccionar al menos la entidad emisora raíz de la que depende el certificado del equipo, esto es, la CA de nivel superior en la ruta de certificación del certificado de equipo que se encuentra en el almacén personal del equipo).

- Vuelva a la carpeta *Directivas de seguridad IP* en la consola MMC. Haga doble click en la directiva *PruebaIPSec* en el panel derecho. Asegúrese de que la opción *Filtro de Prueba IPSec* está seleccionada y haga click en *Modificar.* Seleccione el botón de radio para *Todo el tráfico IP*. Haga click en *Modificar.* Asegúrese de que la casilla de verificación *Asistente para regla nueva* está activada y haga click en *Aceptar*.

- Haga click en la ficha *Métodos de autenticación*. Seleccione la Clave previamente compartida con los detalles ABC123 y haga click en *Modificar.* Seleccione la opción *Usar un certificado de esta entidad emisora de certificados (CA)* y haga click en *Examinar*. Haga click para seleccionar la CA utilizada anteriormente: en este ejemplo se trata de *ryst13.unicauca.edu.co*. Haga click en Aceptar (ver Figura 5.12).

El editor de Reglas IPSec permite crear una lista ordenada de entidades emisoras de certificados que el equipo enviará a petición del equipo interlocutor durante la negociación IKE. Para que la autenticación tenga éxito, el equipo interlocutor debe tener un certificado personal emitido por una de las entidades emisoras raíz de la lista. Puede continuar agregando y organizando entidades emisoras de certificados cuanto desee.

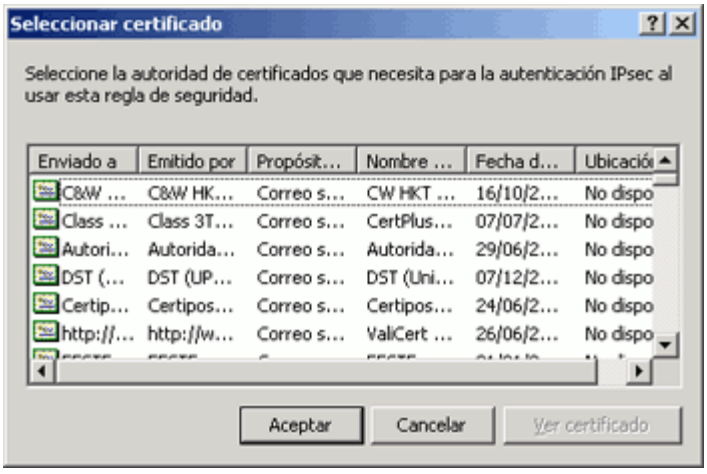


Figura 5.12 Seleccionar un certificado

- Haga click en *Aceptar* dos veces y, a continuación, haga click en *Cerrar*. Repita el procedimiento completo en el otro equipo. Inicialice Ethereal e intente hacer ping desde cada uno de los equipos al otro.

P.7.4 ¿Qué respuesta obtiene?

P.7.5 Analice los mensajes ISAKMP de la negociación e identifique la principal diferencia con respecto a los mensajes intercambiados cuando se utilizó la clave precompartida.

Puede pedir la lista de métodos de autenticación para especificar certificados en primer lugar y, a continuación, Kerberos o clave previamente compartida. Sin embargo, no se puede fragmentar la lista de certificados incluyendo en medio un método sin certificados. Al agregar CA raíz adicional, se puede crear una lista de CA raíz en las que confíe, que es mayor que la lista de entidades que han emitido un certificado para su equipo. Esto resulta necesario para la interoperabilidad en muchos escenarios empresariales. Es importante entender que el equipo puede recibir peticiones de certificado de un interlocutor destinatario que puede incluir o no una CA raíz en la lista de entidades emisoras de certificados especificada en directiva IPSec. Es necesaria la coordinación con el administrador del destino para acordar la CA raíz que utilizará cada extremo. Si la petición del destino incluye una entidad emisora de certificados en esta lista, IKE comprobará si su equipo tiene un certificado personal válido que dependa de esta CA raíz. Si lo hace, elegirá el primer certificado personal de equipo válido que encuentre y lo enviará como la identidad del equipo.

Si su equipo recibe una petición de certificado de una CA raíz que no estaba especificada en esta regla de directiva IPSec, enviará el primer certificado que encuentre y que dependa del nombre de CA raíz especificada en su propia regla de directiva IPSec. Dado que las peticiones de certificados son opcionales en el estándar *RFC 2409*, una vez que su equipo acepte la autenticación por certificado debe enviar un certificado incluso aunque no reciba una petición de certificado IKE, o si la petición de certificado no coincide con los nombres de CA raíz de la directiva de su equipo. En este caso, es probable que la negociación IKE produzca un error, ya que los dos equipos no pudieron ponerse de acuerdo en una CA raíz común. Si la petición del destino no incluye una de las entidades emisoras de certificados, se producirá un error en la negociación IKE.

5.3.2.4 Conclusiones

5.4 EVALUACIÓN DEL RENDIMIENTO EN UNA TRANSMISIÓN DE DATOS UTILIZANDO IPSEC

Se evaluó el rendimiento en la transmisión de flujo datos sobre el protocolo TCP soportándose a su vez sobre IPSec en IPv4. El rendimiento fue medido con *netperf* para Linux (http://www.netperf.org/netperf/DownloadNetperf.html) sobre una topología Gateway-to-Gateway como lo muestra la figura 5.13:

Figura 5.13 Escenario de prueba del desempeño de una comunicación que utiliza IPSec

Para instalar *netperf* se procede como con la mayoría de paquetes de código fuente, descomprimiendo, configurando (#./configure), compilando (#make) e instalando (#make install).

La prueba se realizó entre los extremos de la red, se configuró IPSec de manera manual en ambos extremos con la herramienta *pfkey* usando las diferentes opciones de configuración. En el host B se subió el servidor de *netperf* con el comando *netserver*, diciéndole que escuche conexiones por el puerto 40000 de TCP de la siguiente manera: *#netserver –p 40000.* En el host A se ejecuta *netperf* con la mayoría de opciones por defecto diciéndole que el servidor al que debe conectarse tiene la dirección IP 10.200.2.2 y que lo haga en el puerto 40000 de TCP. El comando retorna los siguientes valores después de un minuto:

```
root@ryst14 netperf-2.4.1]# netperf -H 10.0.2.2 -p 40000
TCP STREAM TEST from 0.0.0.0 (0.0.0.0) port 0 AF_INET to 10.0.2.2 (10.0.2.2)
port 0 AF_INET
Recv   Send    Send
Socket Socket  Message  Elapsed
Size   Size    Size     Time     Throughput
bytes  bytes   bytes    secs.    10^6bits/sec

 87380  16384  16384    10.08       6.22
```

Se puede observar que el valor más importante es el rendimiento medido en 10^6bits/sec (Mbps).

Las opciones de configuración de IPSec probadas fueron las siguientes:

- ✓ Autenticación por HMAC-MD5.
- ✓ Autenticación por HMAC-SHA1.
- ✓ Cifrado por 3DES-CBC.
- ✓ Autenticación por HMAC-MD5 y cifrado por 3DES-CBC.
- ✓ Autenticación por HMAC-SHA1 y cifrado por 3DES-CBC.

Los resultados obtenidos se muestran en la Tabla 5.2:

Tabla 5.2 Resultados de la Prueba de Rendimiento

Configuración	Rendimiento (Mbps)
Sin IPSec	6,22
HMAC-MD5	2,08
HMAC-SHA1	2,75
3DES-CBC	0,53
HMAC-MD5/3DES-CBC	0,3
HMAC-SHA1/3DES-CBC	0,23

Debido a que IPSec introduce campos nuevos en la cabecera IP, el tamaño de los campos de datos superiores al nivel IP será más pequeño. Como puede observarse (Figura 5.14), solamente la autenticación del datagrama IP degrada el rendimiento de la red un poco menos de la mitad. El cifrado ejerce una degradación mayor y la utilización de autenticación y cifrado combinados son aún más perjudiciales para el rendimiento de aplicaciones superiores al nivel IP.

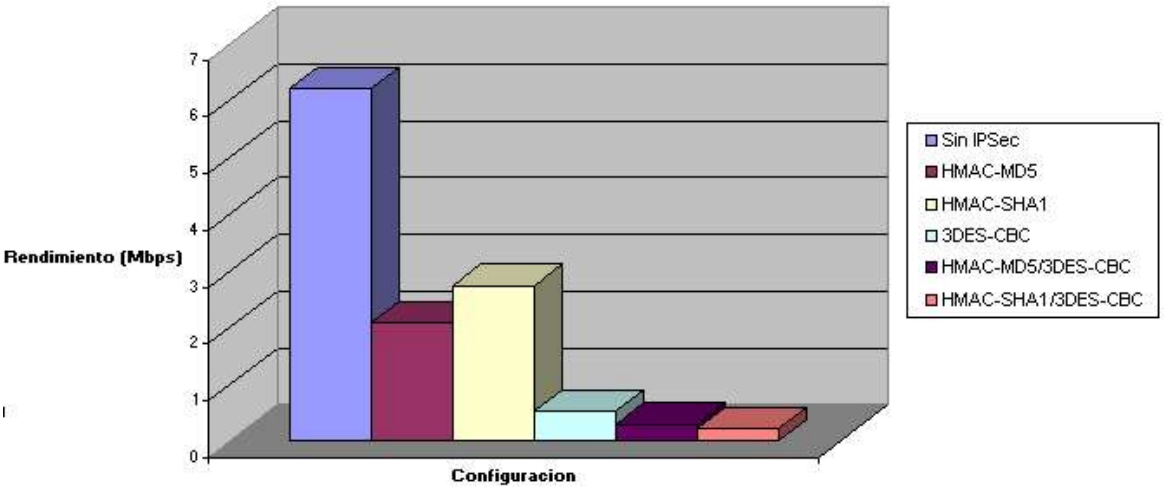


Figura 5.14 Gráfica Rendimiento vs Configuración de IPSec

Siempre que se desee implementar seguridad con IPSec debe tenerse en cuenta estas medidas ya que, como se puede ver, cuando se incrementa la seguridad de una comunicación se puede estar afectando considerablemente su rendimiento.

CAPITULO VI: PROPUESTAS DE SEGURIDAD A NIVEL DE RED

6.1 POLÍTICAS DE SEGURIDAD

En la actualidad, la seguridad ha adquirido gran auge, dadas las cambiantes condiciones y las nuevas plataformas de información disponibles. La posibilidad de interconectarse a través de redes, ha abierto nuevos horizontes que permiten explorar más allá de las fronteras de la organización. Esta situación ha llevado a la aparición de nuevas amenazas en los sistemas de información. Consecuentemente, muchas organizaciones gubernamentales y no gubernamentales internacionales han desarrollado documentos y directrices que orientan en el uso adecuado de estas destrezas tecnológicas y recomendaciones con el objeto de obtener el mayor provecho de estas ventajas, y evitar el uso indebido de las mismas. Esto puede ocasionar serios problemas en los bienes y servicios de las empresas en el mundo.

En este sentido, las *Políticas de Seguridad* surgen como una herramienta organizacional para concientizar a cada uno de los miembros de una organización sobre la importancia y la sensibilidad de la información y servicios críticos que favorecen el desarrollo de la organización y su buen funcionamiento. Para esto es importante preguntarse: ¿Cuál puede ser el valor de los datos? Establecer el valor de los datos es algo totalmente relativo, pues la información constituye un recurso que, en muchos casos, no se valora adecuadamente debido a su intangibilidad, cosa que no ocurre con los equipos, la documentación o las aplicaciones. Además, las medidas de seguridad no influyen en la productividad del sistema por lo que las organizaciones son reticentes a dedicar recursos a esta tarea. Cuando se habla del valor de la información, se hace referencia, por ejemplo, a qué tan peligroso es enviar cierta información a través de Internet, donde viajan no únicamente ésta información sino millones de datos más, gráficas, voz y vídeo.

De hecho, este tema es complejo. El peligro más grande radica no en enviar la información sino una vez que ésta información, unida a la de miles de usuarios más, reposa en la base de datos de una organización; con un único acceso no autorizado a esta base de datos, es posible que alguien obtenga todos los datos e información importante de la misma. En efecto, el tema no está restringido únicamente a Internet. Aunque no se esté conectado a Internet, una red está expuesta a distintos tipos de ataques, que pueden llevarse a cabo dentro de la misma red, incluidos los virus. Por esto, y por cualquier otro tipo de consideración que se tenga en mente, es realmente válido pensar que cualquier organización que trabaje con computadores, y hoy en día más específicamente con redes de computadores, debe tener normativas que exijan hacer buen uso de los recursos y de los contenidos de la información.

Dado que se está tratando con conceptos que pueden tener múltiples interpretaciones, es prudente recordar ciertos significados específicos:

- ✓ *Seguridad:* es "la cualidad o el estado de estar libre de daño" y, *seguro* está definido como "libre de riesgo".
- ✓ *Información:* bien intangible que necesita ser compartido.
- ✓ *Redes:* es "el conjunto sistemático de vías de comunicación e infraestructura para el intercambio de información".

Uniendo todas estas definiciones, es posible establecer qué se entiende por Seguridad en redes:

- ✓ *Seguridad en redes:* es "la capacidad de proporcionar servicios de intercambio de información de forma segura (libre de riesgos) y proteger los recursos que se utilizan para esto".

Por otro lado, un concepto importante es el de Seguridad Global; el concepto de red global incluye todos los recursos informáticos de una organización, aún cuando estos no estén interconectados:

- Computadores personales y computadores portátiles.
- Redes de área local (LAN).
- Redes de área metropolitana (MAN).
- Redes nacionales y supranacionales (WAN).

De manera que, *seguridad global* es "mantener bajo protección todos los componentes de una red global". Y con todo esto se llega a que los usuarios de un sistema son una parte a la que no hay que olvidar ni menospreciar. Siempre hay que tener en cuenta que la seguridad comienza y termina con las personas.

Entre los principales conceptos a la hora de hablar de Requerimientos de Seguridad, se tienen:

- ✓ *Confidencialidad:* la información solo puede ser accedida por el receptor a quien va dirigida.
- ✓ *Integridad:* el receptor debe ser capaz de validar que la información no ha sido alterada durante la transmisión.
- ✓ *Autenticación:* posibilidad de verificar que tanto el origen como el destino de la información son quien dicen ser.
- ✓ *Disponibilidad:* Mantener los recursos y la información siempre disponibles para los usuarios.
- ✓ *No repudio:* que ni el origen ni el destino puedan negar una transmisión.

Dos conceptos importantes a la hora de hacer el análisis para llevar a cabo una propuesta de seguridad, son:

- ✓ *Amenazas:* Personas o procesos que representan un peligro potencial para los bienes o servicios de una organización.

- ✓ *Vulnerabilidades:* son la forma o mecanismo por medio del cual las amenazas pueden afectar los bienes y servicios de una organización.

Obtener de los usuarios la concientización de los conceptos, usos y costumbres referentes a la seguridad, requiere tiempo y esfuerzo. Que los usuarios se concienticen de la necesidad y, más que nada, de las ganancias que se obtienen implementando planes de seguridad, exige trabajar directamente con ellos, de tal manera que se apoderen de los beneficios de tener un buen plan de seguridad; de esta forma, ante cualquier problema, es muy fácil determinar dónde se produjo o de dónde proviene. Para realizar esto, la técnica más utilizada por las grandes empresas y que ha dado muy buenos resultados, es hacer "grupos de trabajo" en los cuales se informen los fines, objetivos y ganancias de establecer medidas de seguridad, de tal manera que los destinatarios finales se sientan informados y tomen para sí los conceptos. Este tipo de acciones favorece, la adhesión a estas medidas.

La implementación de políticas de seguridad, trae consigo varios tipos de problemas que afectan el funcionamiento de la organización. ¿Cómo pueden impactar si se implementan para hacer más seguro el sistema? En realidad, la implementación de un sistema de seguridad conlleva indudablemente a incrementar la complejidad en la operación de la organización, tanto técnica como administrativa. Por ejemplo, la disminución de la funcionalidad o el decremento de la operatividad tal vez sea uno de los mayores problemas.

6.1.1 Concepto de Políticas de Seguridad

Las Políticas de seguridad describen principalmente, la forma adecuada de uso de los recursos de una red, las responsabilidades y derechos tanto de usuarios como administradores, describe lo que se va a proteger y de lo que se está tratando de proteger; las políticas son parte fundamental de cualquier esquema de seguridad eficiente. Las Políticas de Seguridad establece el canal formal de acción del personal, en relación con los recursos, servicios e información importantes de la institución. No se trata de una descripción técnica de mecanismos de seguridad, ni de una expresión legal que involucre sanciones a conductas de los usuarios; es más bien una descripción de lo que se desea proteger y el por qué de ello.

Una política de seguridad puede ser *prohibitiva*, si todo lo que no está expresamente permitido está denegado, o *permisiva*, si todo lo que no está expresamente prohibido está permitido. Evidentemente la primera aproximación es mucho mejor que la segunda de cara a mantener la seguridad de un sistema; en este caso la política contemplará todas las actividades que se pueden realizar en los sistemas, y el resto (las no contempladas), serán consideradas ilegales.

Cualquier política debe contemplar seis elementos claves en la seguridad de un sistema de información:

- Disponibilidad: Es necesario garantizar que los recursos del sistema se encontrarán disponibles cuando se necesitan, especialmente la información crítica.
- Utilidad: Los recursos del sistema y la información manejada en el mismo ha de ser útil para alguna función.
- Integridad: La información del sistema debe mantenerse tal y como se almacenó por un agente autorizado.
- Autenticidad: El sistema ha de ser capaz de verificar la identidad de sus usuarios, y los usuarios la del sistema.

- Confidencialidad: La información sólo ha de estar disponible para agentes autorizados, especialmente su propietario.
- Posesión: Los propietarios de un sistema han de ser capaces de controlarlo en todo momento; perder este control en favor de un usuario malicioso compromete la seguridad del sistema hacia el resto de usuarios.

Para cubrir de forma adecuada los seis elementos anteriores, con el objetivo permanente de garantizar la seguridad corporativa, una política se suele dividir en puntos más concretos a veces llamados *normativas*. El **estándar *ISO 17799*** define las siguientes líneas de acción:

- *Seguridad organizacional:* Aspectos relativos a la gestión de la seguridad dentro de la organización (cooperación con elementos externos, outsourcing[1], estructura del área de seguridad, etc.).
- *Clasificación y control de activos:* Inventario de activos y definición de sus mecanismos de control, así como etiquetado y clasificación de la información corporativa.
- *Seguridad del personal:* Formación en materias de seguridad, cláusulas de confidencialidad, reporte de incidentes, monitorización de personal, etc.
- *Seguridad física y del entorno:* Bajo este punto se engloban aspectos relativos a la seguridad física de los recintos donde se encuentran los diferentes recursos de la institución (incluyendo los humanos) y de los sistemas en sí, así como la definición de controles genéricos de seguridad.
- *Gestión de comunicaciones y operaciones:* Este es uno de los puntos más interesantes desde un punto de vista estrictamente técnico, ya que engloba aspectos de la seguridad relativos a la operación de los sistemas y telecomunicaciones, como los controles de red, la gestión de copias de seguridad o el intercambio de software dentro de la organización.
- *Controles de acceso:* Definición y gestión de puntos de control de acceso a los recursos informáticos de la organización: contraseñas, seguridad perimetral, monitorización de accesos, etc.
- *Desarrollo y mantenimiento de sistemas:* Seguridad en el desarrollo y las aplicaciones, cifrado de datos, control de software, etc.
- *Gestión de continuidad de negocio:* Definición de planes de continuidad, análisis de impacto, simulacros de catástrofes.
- *Requisitos legales:* Evidentemente, una política ha de cumplir con la normativa vigente en el país donde se aplica; si una organización se extiende a lo largo de diferentes países, su política tiene que ser coherente con la normativa del más restrictivo de ellos. En este apartado de la política se establecen las relaciones con cada ley: derechos de propiedad intelectual, tratamiento de datos de carácter personal, exportación de cifrado, junto a todos los aspectos relacionados con registros de eventos en los recursos (logs) y su mantenimiento.

[1] Outsourcing: Contratar los servicios de seguridad de una compañía externa, especializada en la materia, y que permita olvidarse al personal de la empresa de los aspectos técnicos de seguridad.

6.1.2 Elementos de una Política de Seguridad

Como se mencionó en el apartado anterior, una Política de Seguridad debe orientar las decisiones que se toman en relación con la seguridad. Por tanto, requiere de una disposición por parte de cada uno de los miembros de la organización para lograr una visión conjunta de lo que se considera importante. Las Políticas de Seguridad deben considerar entre otros, los siguientes elementos:

- Alcance de las políticas, incluyendo facilidades, sistemas y personal sobre la cual aplica. Es una invitación de la organización a cada uno de sus miembros a reconocer la información como uno de sus principales activos así como, un motor de intercambio y desarrollo. Invitación que debe concluir en una posición.
- Objetivos de la política y descripción clara de los elementos involucrados en su definición.
- Responsabilidades por cada uno de los servicios y recursos a todos los niveles de la organización.
- Requerimientos mínimos para configuración de la seguridad de los sistemas que abarca el alcance de la política.
- Definición de violaciones y de las consecuencias del no cumplimiento de la política.
- Responsabilidades de los usuarios con respecto a la información a la que tienen acceso.

Las Políticas deben ofrecer explicaciones comprensibles acerca de por qué deben tomarse ciertas decisiones, sensibilizar por qué son importantes estos u otros recursos o servicios. De igual forma, las Políticas de Seguridad establecen las expectativas de la institución en relación con la seguridad y lo que ella puede esperar de las acciones que la materializan. Deben mantener un lenguaje común libre de tecnicismos y términos legales que impidan una comprensión clara de las mismas, sin sacrificar su precisión y formalidad dentro de la empresa.

Por otra parte, la Política debe especificar la autoridad que debe hacer que las cosas ocurran, el rango de los correctivos y sus actuaciones que permitan dar indicaciones sobre la clase de sanciones que se puedan imponer. No debe especificar con exactitud qué pasara o cuándo algo sucederá; no es una sentencia obligatoria de la ley.

Finalmente, las Políticas de Seguridad como documentos dinámicos de la organización, deben seguir un proceso de actualización periódica sujeto a los cambios organizacionales relevantes: crecimiento de la red, cambio en la infraestructura computacional, alta rotación de personal administrativo, desarrollo de nuevos servicios, cambio o diversificación de los equipos o sistemas operativos utilizados, entre otros.

6.1.3 Ciclo para la implantación de una Propuesta de Seguridad

En la figura 6.1 se puede observar el ciclo que debe seguir la construcción de una propuesta de Seguridad; en él, están plasmadas todas las etapas que intervienen en el estudio realizado a la organización para declarar e implementar las Políticas de Seguridad. Como se puede ver, es un ciclo repetitivo ya que, como se mencionó anteriormente la implantación de Políticas de Seguridad en una empresa es algo dinámico, que debe mantenerse en un proceso de actualización constante a la par con los desarrollos en la infraestructura, recursos, servicios y demás cambios administrativos de la red.

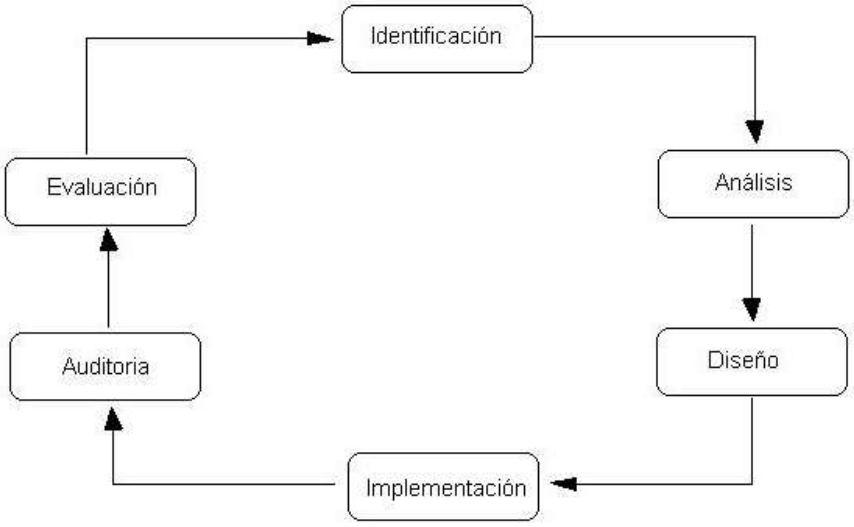


Figura 6.1 Diagrama del ciclo para la implantación de una propuesta de Seguridad

Se comienza realizando una *identificación* de los recursos que necesitan asegurarse y que están relacionados con el funcionamiento de la organización: recursos físicos y lógicos con que cuenta en la red, la información que se puedan robar, qué se puede perder sin consecuencias graves y sobre todo, algo que tal vez es lo más importante a la hora de pensar en la implementación de una propuesta de Seguridad: *¿Qué tanto se está dispuesto a invertir en seguridad?* Se considera tal vez el punto más importante, ya que la inversión en Sistemas de Seguridad puede ser alta, proporcional a las necesidades de protección de la organización y no siempre se está dispuesto a asumirla.

Seguido de esto, se debe realizar un *análisis* de los riesgos, amenazas y vulnerabilidades relacionado con la seguridad. En este sentido deben analizarse todos los recursos, servicios e información importante que necesite ser protegida, cual es el estado actual de la red y que mecanismos implementa para garantizar esta seguridad. Identificar los recursos, sus vulnerabilidades, las principales amenazas y los riesgos que corren al no poseer medidas de protección.

Una vez se tenga esto, es necesario realizar el *diseño* de las propuestas de seguridad y los procesos asociados a estas. Este diseño se realiza de forma lógica, describiendo lo que debe hacerse y cuales deben ser los alcances y la funcionalidad requerida de la tecnología o los mecanismos a implementar.

Una vez llevadas a cabo las tres etapas anteriores, es posible realizar la *implementación* de la tecnología de seguridad y los procesos escogidos en el diseño lógico, al igual que los procesos complementarios definidos y soportados en recursos humanos, e implementar una política de concientización de la seguridad de la red y capacitación especializada para los miembros de la organización.

Como último paso, pero muy importante y con el propósito de asegurar el cumplimiento de todo lo anterior, debe realizarse la *auditoría* y la *evaluación* de la propuesta implementada. La auditoría implica asegurarse de que las políticas y las tecnologías implementadas están cumpliendo con las metas iniciales planteadas y formular un método que permita identificar los problemas en estas políticas y tratarlas de forma rápida. En la evaluación, se mide la eficacia de la propuesta de Seguridad implementada, con base en las auditorías, y se hacen los ajustes requeridos. Con el objeto de confirmar el buen funcionamiento de lo implementado, es una buena opción simular eventos que atenten contra la seguridad del sistema.

Como el proceso de seguridad es un proceso dinámico, es necesario realizar revisiones al programa de seguridad, al plan de acción y a los procedimientos y normas implementados. Estas revisiones, tendrán efecto sobre los puntos tratados anteriormente y de esta manera, el ciclo se vuelve a repetir. Es claro que el establecimiento de Políticas de Seguridad es un proceso dinámico sobre el que hay que estar actuando permanentemente, de manera tal que no quede desactualizado para que, cuando se le descubran debilidades, éstas sean subsanadas y finalmente, que su práctica por los integrantes de la institución no caiga en desuso.

Existen tres preguntas fundamentales que debe responder cualquier política de seguridad y son:

- ¿Qué se quiere proteger?
- ¿Contra quién?
- ¿Cómo?

Se deberían proteger todos los elementos de la red interna, incluyendo hardware, software, datos, etc. de cualquier intento de acceso no autorizado desde el exterior y contra ciertos ataques desde el interior que puedan preverse y prevenirse. Sin embargo, es posible definir niveles de confianza, permitiendo selectivamente el acceso de determinados usuarios externos a determinados servicios o denegando cualquier tipo de acceso a otros. La respuesta a la tercera pregunta es la más difícil de resolver y la que requiere unas soluciones más dinámicas y cambiantes en lo que se refiere a la vigencia de dicha política de seguridad.

Se pueden plantear soluciones u opciones en dos aspectos básicos, llamados *Paradigmas de Seguridad*:

- Todo lo que no se prohíbe expresamente está permitido
- Todo lo que no se permite expresamente está prohibido

A continuación, se hará un análisis de los principales aspectos que se ven afectados a la hora de hablar de seguridad, y se plantearán algunas soluciones específicas para el estado actual de la Red de Datos.

6.2 POLÍTICAS DE SEGURIDAD PARA LA RED DE DATOS DE LA UNIVERSIDAD DEL CAUCA

Teniendo en cuenta lo expresado anteriormente, es posible comenzar a considerar los aspectos para llevar a cabo la propuesta de las principales Políticas de Seguridad que se deben tener en cuenta en la Red de Datos de la Universidad del Cauca. Los aspectos más importantes a incorporar en las Políticas de Seguridad son:

- Procedimientos para reconocer actividades no autorizadas.
- Definir acciones a tomar en caso de incidentes.
- Definir acciones a tomar cuando se sospeche de actividades no autorizadas.
- Conseguir que la política sea refrendada por el estamento más alto posible dentro de la organización.
- Divulgar la política de forma eficiente entre los usuarios y administradores.
- Articular medidas de auditoria de nuestro propio sistema de seguridad.
- Establecer plazos de revisión de la política en función de resultados obtenidos.

Definido el modelo de seguridad a utilizar, es necesario definir las herramientas con las que se contará para su implementación práctica.

6.2.1 Identificación

A continuación se enumeran los recursos más importantes para la buena operación de la Red de Datos de la Universidad del Cauca, y que son los recursos que deben ser protegidos.

- *Servidores:* Incluyen todos los equipos que están configurados como servidores y que son claves para el funcionamiento de la red. Entre ellos se tienen como servidores de dominio publico: Atenea (Servidor de correo electrónico y de Shell Remoto para docentes, funcionarios, grupos de investigación, dependencias, etc.), Afrodita (Servidor de correo electrónico y de Shell Remoto para estudiantes de pregrado y posgrado), Juno (Servidor de Autenticación de Usuarios), Acuario (Servidor Web), Odín (Servidor FTP), DNS1 y DNS2 (Servidores de Nombres de Dominio), Hiperion y Temis (Servidores Proxy HTTP y FTP); también los servidores de la división de sistemas que soportan servicios académicos administrativos y financieros de la Universidad. Otro sector donde se ofrecen servicios, es la Vice-rectoría de Investigaciones; los servidores de esta dependencia prestan servicios de correo electrónico, DNS y alojamiento web para los usuarios y trabajadores de la Vice-rectoría. Debido a que estos servidores no prestan servicios al resto de la Universidad, no se consideran de mucha importancia. En esta parte se tiene en cuenta la parte Hardware de los servidores, ya que su parte Software, Sistema Operativo y datos se tendrán en cuenta más adelante.

- *Dispositivos de interconexión de Red:* se incluyen Firewalls, Routers, Switches, Hubs, Transceivers, y Tarjetas de Interfaz de Red de cada equipo conectado a la red.

- *Equipos terminales:* Los equipos de los usuarios finales, conectados a la red.

- *Sistemas Operativos y aplicaciones:* Abarca los Sistemas Operativos que corren en los servidores nombrados anteriormente (Linux Debian 3.1, Windows 2000 Server y Red Hat Advanced Server 2.1), los sistemas operativos de los equipos terminales de los usuarios, y las aplicaciones (como los protocolos TCP/IP, demonios que ofrecen diferentes servicios, instaladores del hardware, aplicaciones de gestión y demás software utilizado en los diferentes equipos conectados a la red).

- *Información:* Se identifican todos los datos de los usuarios (que deben ser confidenciales) y del sistema. Entre los datos de los usuarios se tiene: la cuenta de correo electrónico, información de notas y demás información de su estado académico y financiero. Además, información confidencial que maneja la Universidad para sus asuntos de gestión. Entre los datos del Sistema, se tiene toda la información que se necesita para el normal funcionamiento de la red, como passwords, información de las diferentes bases de datos, archivos de configuración y tablas de enrutamiento de los dispositivos de interconexión, copias de seguridad, etc.

- *Instalaciones Físicas:* En este recurso se incluye el cableado estructurado (UTP 5 y Fibra Óptica, gabinetes de red, UPS, salas del área de servidores, salas de trabajo de los estudiantes, tomas de conexión del cableado, entre otros.

- *Factor Humano:* Es tal vez el recurso más importante, ya que incluye Administradores, Operadores, Monitores, usuarios de la Red, y demás personal universitario constituído por administrativos, profesores, estudiantes y empleados, que son la base para que la red funcione correctamente, así como para su mantenimiento y seguridad.

6.2.2 Análisis

En esta parte se consideran las Amenazas a las que están expuestos cada uno de los recursos nombrados anteriormente, para identificar más fácilmente las vulnerabilidades de los mismos y su nivel de riesgo.

6.2.2.1 Recurso Servidores:

- Acceso no autorizado: se presenta cuando una persona logra acceder físicamente a este recurso sin estar autorizado para ello, ya que puede causar daños físicos o lógicos en el equipo y así provocar problemas de seguridad del mismo. Se le asigna un nivel de probabilidad Alto, ya que es muy factible que alguien no autorizado ingrese al área de servidores, porque no se cuenta con vigilancia que limite el acceso. Por lo tanto el nivel de Riesgo de que se presente un problema de este tipo es **Alto**.

- Robo: indica que alguien tome sin autorización un servidor o alguno de sus componentes y lo retire del área de servidores. Se le asigna un nivel de probabilidad Bajo, ya que no se considera probable que un usuario, alguno de los responsables de la red

(quienes tendrían mayor facilidad para lograr acceder a esta área) o alguna persona en particular, quiera arriesgarse a burlar la seguridad de las diferentes dependencias de la Universidad intentando sacar uno de estos equipos. Por lo tanto el nivel de Riesgo de que se presente un problema de este tipo es **Bajo**.

- Modificación sin autorización: es el hecho de que una persona modifique la configuración del Hardware de un servidor, como apagarlo, reiniciarlo, o desconectar alguno de sus componentes esenciales. Se le asigna un nivel de probabilidad Bajo, ya que no se considera muy probable que un usuario o un administrador de la red ocasione este tipo de daño a un servidor, para provocar un problema en la red que ellos mismos utilizan o administran. Por lo tanto el nivel de Riesgo de que se presente un problema de este tipo es **Medio**.

- Daños físicos: son amenazas contra la integridad física del servidor, causados por diferentes fenómenos como: terremotos, incendios, inundaciones, etc. U ocasionados por alguna persona voluntaria o involuntariamente. Los daños a un equipo pueden ser parciales o totales. Se le asigna un nivel de probabilidad Bajo, por las mismas causas anteriores, además que fenómenos de este tipo se presentan muy poco. Por lo tanto el nivel de Riesgo de que se presente un problema de este tipo es **Bajo.**

- Fallas: se refieren a mal funcionamiento de un equipo o a un daño que se presente en él o alguno de sus componentes, causado por mala calidad, tiempo de vida, o falta de mantenimiento. Se le asigna un nivel de probabilidad Bajo, ya que la Universidad ha adquirido equipos de buena calidad y continuamente se encuentran en revisión, por lo que los fallos no se presentan frecuentemente. Por lo tanto el nivel de Riesgo de que se presente un problema de este tipo es **Bajo.**

6.2.2.2 Recurso Dispositivos de Interconexión de red:

- Modificación no autorizada de la configuración del Software: se refiere a cambios en la configuración del archivo de configuración software de alguno de estos dispositivos, por ejemplo en las tablas de enrutamiento de un Router. Se le asigna un nivel de probabilidad Medio, ya que aunque todos los equipos cuentan con una protección por medio de passwords para permitir el acceso a sus archivos configuración y solo los manejan los administradores de la red, estos password viajan en texto plano, y el acceso remoto se realiza por medio de telnet, que no ofrece ningún tipo de seguirdad. Por lo tanto el nivel de Riesgo de que se presente un problema de este tipo es **Medio.**

- Modificación no autorizada de la configuración Hardware: por ejemplo desconectar algún puerto de un switch o un hub, o cualquier modificación de la configuración externa o física de alguno de los equipos. Se le asigna un nivel de probabilidad Alto, ya que muchos de estos equipos se encuentran instalados en cabinas sin seguridad, a las que puede tener acceso cualquier persona. Por lo tanto el nivel de Riesgo de que se presente un problema de este tipo es **Alto.**

- Robo: Igual que como se definió para los servidores. Se le asigna un nivel de probabilidad Alta, debido a que ya se han llevado a cabo robos de otros dispositivos como Video Beams a plena luz del día y no ha sido posible definir los implicados en el hecho, a pesar de que se cuenta con cierto nivel de seguridad a la salida de las instalaciones físicas de la Universidad. Por lo tanto el nivel de Riesgo de que se presente un problema de este tipo es **Alto.**

- Daños físicos: Igual que como se definió para los servidores. Se le asigna un nivel de probabilidad Medio por las mismas razones anteriores. Por lo tanto el nivel de Riesgo de que se presente un problema de este tipo es **Medio.**

- Fallas: Igual que como se definió para los servidores. Se le asigna un nivel de probabilidad Bajo ya que los equipos son de muy buena calidad. Por lo tanto el nivel de Riesgo de que se presente un problema de este tipo es **Bajo.**

6.2.2.3 Recurso Estaciones de Trabajo:

- Revelación de Passwords: cuando una persona no autorizada averigua la contraseña asignada a la cuenta de algún usuario para entrar al sistema, o las contraseñas de una estación de trabajo haciendo uso de software para este fin. Se le asigna un nivel de probabilidad Alto, ya que los usuarios prestan poca atención a la seguridad y son poco cuidadosos a la hora de seleccionar sus contraseñas; además es muy fácil para un usuario instalar software en las estaciones de trabajo para capturar este tipo de información. Por lo tanto el nivel de Riesgo de que se presente un problema de este tipo es **Alto.**

- Cambios no autorizados en la configuración de red de los equipos: cuando se realizan cambios no autorizados en las direcciones IP de las estaciones de trabajo, o cualquier cambio en la configuración TCP/IP de las mismas. Se le asigna un nivel de probabilidad Alto ya que es muy fácil que cualquier usuario cambie esta información impidiendo que el equipo pueda acceder a la red. Por lo tanto el nivel de Riesgo de que se presente un problema de este tipo es **Alto.**

- Acceso físico sin autorización: ingreso no autorizado de una persona al área donde se encuentra una estación de trabajo. Se le asigna un nivel de probabilidad Alto ya que es muy fácil que cualquier usuario ingrese a una sala aún cuando no está autorizado a hacerlo debido a la falta de control en las mismas; de igual manera el acceso a computadores personales de los monitores, etc. Por lo tanto el nivel de Riesgo de que se presente un problema de este tipo es **Alto.**

- Robo: indica que una persona tome una estación de trabajo o alguno de sus componentes y lo retire del área asignada sin autorización. Para este caso, se le asigna un nivel de probabilidad Alto, ya que es relativamente fácil que cualquier usuario tome alguno de los componentes de una estación de trabajo y se la lleve sin autorización. Por lo tanto el nivel de Riesgo de que se presente un problema de este tipo es **Alto.**

- Daños físicos: amenazas contra la integridad de las estaciones de trabajo, por fenómenos naturales u ocasionados por una persona voluntaria o involuntariamente. Se le asigna un nivel de probabilidad Alto ya que es muy probable que estos equipos sufran daños debido al alto nivel de utilización por parte de los usuarios. Por lo tanto el nivel de Riesgo de que se presente un problema de este tipo es **Alto.**

- Fallas: se refieren a mal funcionamiento del equipo o a un daño que se presente en él o alguno de sus componentes, causado por mala calidad, tiempo de vida, o falta de mantenimiento. Se le asigna un nivel de probabilidad Alto por la misma razón que en el punto anterior. Por lo tanto el nivel de Riesgo de que se presente un problema de este tipo es **Alto.**

6.2.2.4 Recurso Sistemas Operativos de red y aplicaciones:

- Acceso no autorizado: se presenta cuando una persona no autorizada utiliza las aplicaciones o el sistema operativo un equipo, violando sus mecanismos de seguridad y control de acceso, o suplantándose por un usuario válido del sistema. Se le asigna un nivel de probabilidad Medio ya que ha sido una situación que se ha presentado en la Universidad, y no es difícil que vuelva a presentarse. Por lo tanto el nivel de Riesgo de que se presente un problema de este tipo es **Medio.**

- Modificación no autorizada: es la modificación total o parcial de la configuración del Sistema Operativo o de alguna aplicación que tenga como consecuencia su indisponibilidad total o parcial. Se le asigna un nivel de probabilidad Bajo ya que se considera poco probable que alguien pueda interesarse por cambiar el funcionamiento de determinada aplicación, pero aunque no es fácil, podría llegar a suceder. Por lo tanto el nivel de Riesgo de que se presente un problema de este tipo es **Bajo.**

- Instalación de Software peligroso: introducción de virus, caballos de troya, gusanos y demás aplicaciones que puede llegar a causar daños parciales o totales de los recursos software de la red e impedir el correcto funcionamiento de la misma. Se le asigna un nivel de probabilidad Medio porque es un problema muy común y que puede además presentarse de forma involuntaria, ya que los usuarios no tienen suficiente cuidado con la información que manejan y con el software que le introducen a los equipos. Por lo tanto el nivel de Riesgo de que se presente un problema de este tipo es **Medio.**

- Fallas: ocasionadas por suspensión del fluído eléctrico; se le asigna un nivel de probabilidad Medio porque es un evento común y a pesar de que la parte de servidores tiene un sistema de UPS, estás tienen un duración corta, y si el corte en la energía se produce por largos periodos de tiempo, la red quedaría sin servicio. Por lo tanto el nivel de Riesgo de que se presente un problema de este tipo es **Medio.**

6.2.2.5 Recurso Información:

- Robo o destrucción: eliminación o indisponibilidad total de la información de modo que los usuarios finales no puedan utilizarla, y si pueden hacerlo usuarios no autorizados que dispongan de ella. Se le asigna un nivel de probabilidad Bajo porque una persona conciente no se arriesgaría robando información del sistema sabiendo por ejemplo, que en los servidores con sistema Linux se cuenta con un registro de las actividades de los usuarios que acceden a él. Para alguien externo a la red, la información no es muy importante. Por lo tanto el nivel de Riesgo de que se presente un problema de este tipo es **Bajo.**

- Modificación no autorizada: implica que se modifique la información totalmente o en parte, por lo que la información pierde su valor. Se le asigna un nivel de probabilidad Bajo por las mismas razones anteriores. Por lo tanto el nivel de Riesgo de que se presente un problema de este tipo es **Bajo.**

- Lectura no autorizada: es la observación del contenido de la información por personas no autorizadas. Se le asigna un nivel de probabilidad Alto ya que es una práctica que puede resultar mucho más fácil que robar o modificar la información. Por lo tanto el nivel de Riesgo de que se presente un problema de este tipo es **Alto.**

- Virus: software malicioso que puede afectar considerablemente la información, hasta el punto de llegar a ser irrecuperable. Se le asigna un nivel de probabilidad Alto por las mismas razones expuestas anteriormente. Por lo tanto el nivel de Riesgo de que se presente un problema de este tipo es **Alto.**

6.2.2.6 Recurso Instalaciones Físicas:

- Acceso no autorizado: implica el ingreso al área donde se encuentra un recurso de la red, para acceder a él, sin estar debidamente autorizado. Se le asigna un nivel de probabilidad Alto ya que los recursos se encuentran expuestos en sitios de fácil acceso para cualquier persona. Por lo tanto el nivel de Riesgo de que se presente un problema de este tipo es **Alto.**

- Daños físicos: son amenazas contra la integridad física de las instalaciones de la Universidad, donde se encuentran los recursos de la red, causados por diferentes fenómenos naturales, u ocasionados por alguna persona voluntaria o involuntariamente. Se le asigna un nivel de probabilidad Bajo, ya que es poco probable que se presente algún fenómeno natural destructivo, y por la dificultad para alguien de llevar a cabo esta labor. Por lo tanto el nivel de Riesgo de que se presente un problema de este tipo es **Bajo.**

6.2.2.7 Recurso Personal Humano:

- Indisponibilidad: que el personal encargado de administrar los recursos no pueda llevar a cabo sus tareas por factores como enfermedad, problemas personales, o por insuficiencia de personal. Se le asigna un nivel de probabilidad Bajo, ya que aunque estos factores se presentan, en la Red de Datos cuentan con personal suficiente como para cubrir a una persona que tenga problemas. Por lo tanto el nivel de Riesgo de que se presente un problema de este tipo es **Bajo.**

- Errores voluntarios: que alguno de los responsables de la red lleve a cabo actividades dañinas contra los recursos antes mencionados de forma conciente, para atentar contra el buen funcionamiento de la red. Se le asigna un nivel de probabilidad Bajo, ya que es poco probable que sean las mismas personas encargadas del buen funcionamiento de la red las que le causen daños que ellos mismos tendrán que solucionar, aunque se puede llegar a presentar por beneficios externos. Por lo tanto el nivel de Riesgo de que se presente un problema de este tipo es **Bajo.**

- Errores involuntarios: de igual forma que lo expuesto anteriormente, pero los errores se cometen sin la intención de causar daño. Se le asigna un nivel de probabilidad Medio, porque los seres humanos siempre cometeremos errores en mayor o menor medida y por diversos motivos, y más aún cuando muchos de los operadores de la red son los mismos estudiantes de la Universidad que muchas veces están aprendiendo sobre la misma. Por lo tanto el nivel de Riesgo de que se presente un problema de este tipo es **Medio.**

- Desconocimiento de las políticas de Seguridad y demás procedimientos de operación de la red: cuando los encargados de la red no conocen las consideraciones de seguridad que se deben aplicar para realizar su trabajo. Se le asigna un nivel de probabilidad Alto, porque hasta el momento no se han planteado políticas de seguridad para la red ni se ha hecho una divulgación de las normas a tener en cuenta al utilizar estos recursos. Por lo tanto el nivel de Riesgo de que se presente un problema de este tipo es **Alto.**

- Desconocimiento del funcionamiento técnico: falta de conocimientos técnicos específicos a la labor que realiza el personal de la red. Se le asigna un nivel de probabilidad Medio, porque aunque el personal de la red de Datos está muy calificado para realizar su labor y se mantiene en constante capacitación, siempre habrá labores específicas para las cuales harán falta conocimientos específicos y más aún cuando se habla de seguridad. Por lo tanto el nivel de Riesgo de que se presente un problema de este tipo es **Medio.**

6.2.3 Diseño

En esta fase se deben definir las Políticas de Seguridad que servirán de base para solucionar las distintas amenazas que han sido identificadas y que están generando los diferentes niveles de riesgo en la Red de Datos de la Universidad. Además, se realizará el diseño lógico de tres Propuestas de Seguridad a implementar en la Red de Datos y la que, según las necesidades actuales de ésta, sería la más acertada.

Las Políticas de Seguridad se van a dividir basándose en 3 criterios:

- Políticas de Seguridad a Nivel Físico
- Políticas de Seguridad a Nivel Lógico
- Políticas de Seguridad a Nivel Humano

6.2.3.1 Políticas de Seguridad a Nivel Físico

En este sentido se tendrán en cuenta todos los componentes físicos de la red, las instalaciones y plataformas Hardware, en cuanto a mantenimiento y control de acceso. Se tendrán en cuenta varios aspectos así:

6.2.3.1.1 Instalaciones de la red

En este punto se considera que lo referente al cableado estructurado y la seguridad en este sentido fueron tenidos en cuenta a la hora del diseño.

➢ Medidas relacionadas con el acceso:

Es uno de los puntos más críticos en cuanto a la seguridad física de la red y debe tener en cuenta como mínimo lo siguiente:

- El control de acceso a las salas de servidores debería estar controlado por medio de sistemas electrónicos que se aseguren de que solo accedan al área personas autorizadas. El acceso a cualquier sala de la red debe ser controlada por el administrador, y mientras no haya un miembro autorizado, estas salas deben permanecer con llave.

- Los equipos importantes para el funcionamiento de la red deben estar aislados físicamente por una puerta que debe permanecer siempre cerrada con un vigilante cerca de ella. Los equipos no deben ser visibles al público, para evitar planeación de accesos no autorizados.

- El acceso a las salas públicas debe ser controlado y supervisado por medio de la identificación de los usuarios mediante su carné o recibo de matrícula y del registro de los mismos según los horarios en los que utilicen los recursos.

- El acceso a los equipos de interconexión de la red debe ser muy limitado y solo deben utilizarlos los monitores de la red. Los armarios de comunicaciones deben permanecer con llave y deben administrarlas personas autorizadas por el administrador de la red.

➢ Medidas relacionadas con el aseo y el mantenimiento:

- Deben plantearse procedimientos para llevar a cabo el mantenimiento preventivo de los servidores y demás equipos de desarrollo y equipos de interconexión, para asegurar el buen funcionamiento de la red.

- El aseo en la sala de servidores se debe hacer con mucho cuidado para evitar levantar partículas de polvo que afecten los equipos. Debe realizarse limpieza de los equipos con instrumentos para este fin.

➢ Salas de servidores de la División de Sistemas y la Red de datos:

Son las salas en las que se encuentran los equipos más importantes para el funcionamiento de la red; para la Universidad del Cauca, los servidores están alojados en el edificio del IPET y en el edificio de la facultad de educación.

- Estas salas solo deben ser utilizada para albergar los equipos de red y comunicaciones tales como servidores, equipos de interconexión, etc. ya que estos necesitan un nivel de seguridad preferencial. No deben utilizarse para guardar cosas que no se utilizan.

- Estas salas deben ser lo suficientemente grandes como para permitir una expansión en caso de que fuera necesario. Los equipos deben estar separados para permitir una buena ventilación, y debe tenerse en cuenta un espacio como zona de tránsito para los operadores de los equipos. Debe ser un área que provea un ambiente cómodo para los operadores del sistema.

- Los servidores deben estar ubicados en mesas amplias diseñadas para esta clase de equipos que permitan la cómoda utilización de los mismos.

- Se debe implementar un piso o techo falso que permita la organización de los cables de alimentación y de comunicación de los equipos.
- Estas salas deben tener sistemas de aire acondicionado, sistemas de aislamiento de ruido, y sistemas de regulación de voltaje y alimentación ininterrumpida. Los equipos centrales deben estar en una sala aparte donde el ruido y la temperatura que provocan no sea crítico.

- Las salas deben tener sensores de detección de incendios ubicados estratégicamente, sistemas de extinción que no utilicen agua y en caso de inundación, debe tener desagües efectivos. Deben haber extinguidores en sitios de acceso rápido y las personas que trabajan en la sala deben tener conocimiento de la ubicación de éstos.

- Los cables de comunicaciones deben estar preferiblemente aislados de los cables de alimentación para evitar posibles interferencias.

- Deben ser áreas restringidas totalmente para usuarios no autorizados.

➢ Salas de Servicio Público de Acceso a Internet:

Son las salas que utilizan los usuarios de la red para sus labores académicas.

- Estas salas deben tener reguladores de voltaje para todos los equipos.

- Deben implementar sistemas de detección de incendios y tener extinguidotes ubicados en sitios de fácil acceso.

- Deben ser salas lo suficientemente grandes para una correcta ventilación y para brindar un ambiente cómodo de trabajo, además de contar con zonas de tránsito adecuadas.

- Los cables de alimentación y comunicaciones de los equipos deben estar ubicados correctamente para evitar accidentes.

➢ Salas de Equipos de interconexión de red:

Son los lugares en los que se albergan los equipos de interconexión de red. Deben cumplir con lo siguiente:

- Los equipos deben estar asegurados físicamente a los armarios de comunicaciones utilizando tornillos de amarre, para evitar accidentes y posibles robos.

- El área debe tener sistemas de protección contra sobrevoltaje y alimentación ininterrumpida.
- Los equipos de alimentación y de comunicaciones deben estar separados físicamente.

- Deben tener buen espacio de circulación del aire.

- Deben ser áreas restringidas totalmente para usuarios no autorizados.

- Deben contar con sistemas de protección contra incendios, además de contar con extinguidores y demás soluciones que no utilicen agua.

➢ Medidas relacionadas con la seguridad Humana:

- Todas las pantallas de los equipos deben contar con protectores de radiación y filtros para evitar molestias en los operadores y usuarios cuando hacen uso de estos por largos periodos de tiempo.

- Todas las instalaciones físicas, en especial la sala de servidores, deben contar con sistemas de aire acondicionado; todas las salas deben tener un buen sistema de ventilación para que el aire circule libremente.

Sanción: En caso de cometer acciones indebidas relacionadas con la infraestructura física de la red, se debe responder ante la administración de la misma, caso en el cual, el administrador debe hablar con el decano de la Facultad e imponer castigos desde llamados de atención y anotaciones en la Hoja de Vida, hasta la desvinculación de la Universidad e incluso llevarlo a ámbitos judiciales, según el caso.

6.2.3.2 Políticas de Seguridad a Nivel Lógico

En esta parte se indican aspectos correspondientes a la seguridad del software del sistema y demás aplicaciones y datos utilizados en la red.

➢ Medidas relacionadas con el control de acceso Lógico:

En esta parte se trata todo lo relacionado con los mecanismos que proveen las aplicaciones y sistemas operativos para permitir que solo personal autorizado tenga acceso a los recursos software. Estas políticas se basan en dar a cada usuario los privilegios mínimos para acceder a un recurso y realizar las tareas necesarias.

- En cada sala debe permitirse el acceso sólo a los otros equipos de la misma sala y solo en casos necesarios, a la información que se encuentra en los discos duros de cada equipo, y para fines académicos, a los servidores internos. No debe permitirse acceso a la información de otras subredes o a la configuración de red de los equipos, a no ser que sea necesario para una labor académica y el administrador lo permita, bajo su supervisión. Los equipos de las salas públicas deben tener acceso a Internet y al correo electrónico.

- Los equipos y aplicaciones instaladas para ser usados por el personal administrativo de la Universidad, deben ser configuradas para que la información aquí almacenada solo sea accesible para las dependencias que lo requieran. Para esto se debe hacer

uso de las herramientas que proveen los sistemas operativos y demás aplicaciones, como control de acceso por passwords, autenticación y encriptación.

- Los usuarios tiene la obligación de mantener estos controles y utilizarlos adecuadamente, según las instrucciones del personal encargado, como se plantea en la Política a nivel Humano más adelante.

- Toda la información sensible que se tenga almacenada en los equipos no debe ser compartida y debe ser protegida por controles de acceso que proveen los sistemas operativos y las aplicaciones.

- Los jefes de cada dependencia deben determinar qué datos son sensibles y necesitan ser protegido y qué datos necesitan ser compartidos.

- Si hay datos que deben ser compartidos por un número determinado de usuarios, deben utilizarse mecanismos de encriptación y de control de acceso. Si se requiere compartir un password de acceso, no deben manejarlo más de 10 personas.

- El intercambio de mensajes de carácter oficial entre las diferentes divisiones de la Universidad que se realice a través de correo Electrónico en la red interna, o los archivos que se compartan, deben protegerse de falsificación por medio de Firmas Digitales, para asegurar que el origen es de la persona que dice ser, y no se pueda falsificar la identidad. Si es necesario, deben implementarse mecanismos de encriptación para que el contenido del mensaje sea totalmente confidencial.

- Para identificación de los usuarios se utilizará un Login o nombre de usuario y una contraseña o password como método de autenticación. Se definen dos tipos de passwords: Los *Passwords Personales*, que solo es conocido por el propietario y que son la base de la identificación de los usuarios y de las acciones que realizan, utilizados por ejemplo para el acceso a sus correos electrónicos. Los *Passwords de Acceso*, utilizados para autorizar el acceso a recursos o datos compartidos por varios usuarios. Puede ser conocido por varias personas autorizadas. Estos passwords deben cumplir con ciertas características que se definirán más adelante.

- El sistema exigirá siempre a todos los usuarios con cuentas electrónicas y al personal que administra los recursos que se autentique con su password personal; de igual forma para los usuarios que se conectan de forma remota por la línea telefónica. Bajo ninguna circunstancia se permitirá pasar por alto los mecanismos de identificación y autenticación del sistema.

- Es obligatorio para los usuarios utilizar todas estas funciones correctamente para proteger sus datos de intrusos o personas no autorizadas.

- Siempre que se requiera la introducción de passwords para el acceso a un recurso, el sistema solo dará la posibilidad de introducirlo máximo 5 veces, después de lo cual terminará la sesión y el evento debe quedar registrado en el equipo, para evitar intentos ilegales de adivinar las contraseñas de acceso.

- Cualquier usuario debe cerrar la sesión en un recurso cuando tenga que abandonar el terminal y nunca dejarlo desatendido mientras la sesión esté activa. De igual forma, todas las sesiones remotas deben finalizar tras 10 minutos de inactividad.

➢ Medidas relacionadas con los Passwords:

Existen unos requerimientos mínimos que deben cumplir todos los usuarios de la red a la hora de seleccionar y manejar sus passwords. Es conveniente que sea el sistema el que exija y valide el cumplimiento de las condiciones exigidas; estas condiciones deben ser conocidas por todos los usuarios desde el primer día que utilicen algún recurso de la red:

- Todos los passwords que se utilicen en el sistema deben tener una longitud mínima de 8 caracteres, compuestos por una combinación de letras mayúsculas, minúsculas, números y caracteres alfanuméricos.

- No se debe utilizar como password el nombre de usuario o cualquier información personal como el nombre, fecha de nacimiento, cumpleaños, etc, que pueda ser obtenida fácilmente.

- Tampoco se deben utilizar secuencias de números que sea fácil predecir, ni passwords solo compuestos por letras y números.

- No se deben utilizar palabras que se encuentren en un diccionario de cualquier idioma.

- El password debe ser fácil de recordar para su propietario, pero difícil de predecir por cualquier otra persona; los passwords no deben ser anotados en ninguna parte, ni almacenados en ningún archivo.

- El tiempo de vida del password debe ser de máximo 3 meses. Los usuarios deben cambiar sus passwords periódicamente y cumpliendo con las exigencias planteadas.

- No está permitido compartir los passwords personales. Los passwords de acceso deben ser conocidos solo por las personas autorizadas.

- Cuando se vaya a establecer una sesión o cuando se vayan a transmitir claves o passwords a través de algún tipo de comunicación con una red externa, éstos deben ser transmitidos de forma segura, utilizando encriptación.

- El propietario del password está obligado a velar por su seguridad y evitar que sea utilizado por personas no autorizadas.

- La seguridad del password debe estar relacionado con la importancia de los datos que protege. Los administradores de la red, que tienen privilegios especiales deben escoger passwords muy seguros y tomar todas las precauciones para protegerlos.

- Todas las bases de datos o archivos que almacenen los passwords personales y los de acceso de los usuarios, deben estar protegidos contra lectura o modificación no autorizada; para esto deben estar encriptados. Además deben existir por lo menos 2 copias de seguridad para esta información, igualmente aseguradas.

- Si un usuario olvida su password personal, deberá contactar única y personalmente al grupo de operadores de la red, encargados de crear y eliminar las cuentas electrónicas de los usuarios. Este personal encargado deberá asignar el nuevo password señalado por el usuario y eliminar el anterior. Después de esto, el usuario debe cambiar de nuevo su password, para evitar una violación a su cuenta.

- Si por algún motivo se tiene la sospecha de que un password ha sido comprometido, debe cambiarse inmediatamente e informar al personal de la red encargado de esto, para verificar si las sospechas son ciertas. Todos los usuarios están obligados a informar de cualquier actividad no autorizada y de la violación de cualquier Política de Seguridad.

- Si los operadores de la red detectan que el archivo que almacena los passwords de todos los usuarios ha sido accedido sin autorización, deben avisar a todos los usuarios de la red para que realicen el respectivo cambio de sus passwords para evitar problemas en sus cuentas.

- En cualquier equipo de red se deben eliminar los passwords o cuentas por defecto que vienen desde la fábrica, como root, guest, etc., ya que estas son conocidas por muchas personas.

- Los administradores que manejan cuentas con privilegios especiales no deben conectarse a los servidores a través de ningún computador de la red interna, y menos desde el exterior, ni por acceso telefónico, a no ser que la comunicación esté asegurada por medio de autenticación y encriptación, para evitar que la información de acceso sea interceptada por personas no autorizadas. Preferiblemente los servidores deben ser gestionados desde su propia consola.

- Todo el proceso de creación de cuentas debe estar completamente documentado.

- Debe llevarse a cabo un análisis periódico de las cuentas de los usuarios para detectar aquellas inactivas por mucho tiempo, e informarle al propietario de la situación por escrito antes de eliminarlas. Una cuenta se declara inactiva cuando no se ha utilizado por más de 6 meses; las cuentas deben ser renovadas cada semestre, y las que no sean renovadas, deben ser eliminadas. La renovación debe hacerse directamente con los administradores de la red.

➢ Medidas relacionadas con los Registros de eventos:

La Red de Datos de la Universidad debe llevar un registro de las actividades que realizan los usuarios y los procesos que tienen acceso al sistema. De esta forma se pueden determinar por medio de éstos registros cuando determinado usuario (identificado con su login) ha llevado a cabo alguna acción ilegal sobre algún recurso de la red.

- Los registros de eventos deben mantenerse completamente protegidos contra la modificación o lectura no autorizada.

- Estos registros deben ser revisados cada semana con el fin de revisar posibles violaciones, errores, actividades no autorizadas o sospechosas que indiquen que la seguridad del sistema ha sido comprometida.

- El personal encargado de la revisión y análisis de los datos entregados por un registrador de eventos debe tener un alto grado de conocimiento del sistema y de todas las actividades que se podrían presentar.

- Los usuarios deben saber en qué momentos están siendo monitorizados por un registrador de eventos, para que se sientan menos motivados a realizar actividades no autorizadas.

➢ Medidas relacionadas con la conexión a redes externas:

Todos los usuarios de la red pueden disfrutar de todos los servicios de Internet, por lo que es función de la Red de Datos asegurarse de que se presten todos los servicios satisfactoriamente:

- Los administradores de la red deben definir qué servicios son los más utilizados e importantes para los usuarios de la red interna, con el fin de eliminar el resto, que pueden llegar a ser fuentes de problemas de seguridad.

- Por otro lado, para los usuarios externos, se deben inhabilitar todos los servicios y habilitar solo los que son necesarios para estos usuarios externos. Todos los puertos y servicios que no sean utilizados en los servidores y que son accesibles desde el exterior, deben ser desactivados para evitar que se conviertan en puertas traseras para usuarios malintencionados.

- Los servicios e información que solo deben ser utilizados por los usuarios de la red interna, deben estar ubicados en servidores diferentes de aquellos que proveen servicios e información al exterior, para no exponerlos a ataques desde el exterior.

- Los servicios al exterior deben tener los mecanismos de seguridad más fuertes con el fin de evitar ataques externos. De igual forma, la comunicación con las otras sedes de la Universidad debe estar protegida por medio de autenticación y encriptación para el manejo de información de la Intranet.

- Todos los accesos hacia el exterior y desde el exterior sin excepción deben pasar por el Firewall dispuesto para proveer el servicio de seguridad en el acceso.

➢ Medidas relacionadas con las copias de seguridad:

Es obligación del personal de operaciones de la red realizar copias de seguridad de la información sensible del sistema y de los usuarios, para el buen funcionamiento de la red.

- Es obligación de este personal definir cuales son los datos del sistema a los cuales se les hará copias de seguridad. Por lo menos deben existir copias de seguridad de todas las bases de datos, de los registros de eventos, de la configuración actual del sistema y sus aplicaciones y de los equipos de interconexión.

- Cada usuario tiene la obligación de realizar las copias de seguridad de su información, y no dejar información crítica en ningún equipo de uso público.

- Las copias de seguridad deben realizarse por lo menos cada dos semanas, aunque hay información crítica a la cual debería realizársele copias diariamente.

- Como mínimo deben mantenerse 2 copias de seguridad: una en el lugar de trabajo y otra almacenada en otro lugar en el caso de que sea imposible ingresar al lugar en el que se encuentra la primera.

- Los medios donde se almacenan las copias de seguridad deben revisarse, de manera que no hayan sufrido daños por humedad, o que estén siendo almacenados de forma incorrecta.

➢ Medidas relacionadas con la prevención de problemas de seguridad:

- Los administradores de la red deben utilizar herramientas que verifiquen la integridad y confidencialidad de los datos y la integridad y disponibilidad de los equipos de la red.

- En todos los equipos se deben instalar herramientas antivirus; en los equipos servidores debe hacerse el análisis de los mismos por lo menos 1 vez al mes. En los equipos de acceso público, es obligación de los monitores realizar diariamente un escaneo del equipo; en los equipos asignados a un usuario en particular, es el usuario el encargado de hacerlo diariamente.

- El personal encargado de la red, debe realizar ataques controlados para verificar la seguridad del sistema, para detectar puntos débiles antes de que lo hagan personas malintencionadas. La información sobre las vulnerabilidades en la seguridad de la red debe mantenerse confidencial.

- Tanto los administradores de la red como los monitores de las diferentes salas, deben estar al tanto de los diferentes parches para prevenir problemas de los sistemas operativos y demás programas, que diariamente se distribuyen en las páginas autorizadas, además de estar al día con las diferentes actualizaciones. El personal encargado debe estar atento a los diferentes avisos sobre vulnerabilidades que se publican a diario en sitios Web de confianza.

- Los equipos identificados como críticos para el funcionamiento de la red deben tener redundancia para asegurar la disponibilidad de la información y de los servicios que ofrece.

- Es responsabilidad del personal de la red mantener informados a los usuarios sobre posibles problemas de seguridad y mantener vías de comunicación eficientes para atender inquietudes de los usuarios.

➢ Medidas relacionadas con la documentación:

Todos los procedimientos de operación, instalación y mantenimiento de los recursos software y hardware de la red deben estar debidamente documentados para el personal que realiza estas tareas, así como manuales sobre distintos aspectos del sistema y sobre seguridad. Toda red debe contar por lo menos con los siguientes documentos:

- Planes de contingencia.
- Políticas generales de seguridad.
- Análisis de Riesgo.
- Reglas de comportamiento.
- Normas propias de la Universidad sobre la red y sus servicios.
- Plan de copias de seguridad.
- Procedimientos de instalación, configuración, operación y mantenimiento de equipos Hardware y Software.
- Plan de auditoria.
- Manuales de usuario sobre operación y seguridad de la red.
- Procedimientos y planes de seguridad para implementar las políticas (autenticación y encriptación).
- Manuales de los equipos y las aplicaciones que proveen los fabricantes.
- Plan de respuesta a incidentes de seguridad.
- Plan de entrenamiento y cursos de capacitación para los usuarios.

La creación de estos documentos es función del grupo de seguridad y los operadores de red, quienes deben estar constantemente actualizándolos conforme la evolución de la red y los equipos. Así mismo, se debe garantizar la disponibilidad y la distribución de los documentos de carácter público y mantener confidencialidad en los documentos de carácter privado.

Sanción: En caso de cometer acciones indebidas mientras se utilizan los beneficios de la red o si se comenten faltas en el cumplimiento de alguna de las Políticas anteriores, se debe responder ante la administración de la misma, caso en el cual, si el administrador debe hablar con el decano de la Facultad e imponer castigos desde llamados de atención y anotaciones en la Hoja de Vida, hasta la desvinculación de la Universidad e incluso llevarlo a ámbitos judiciales.

6.2.3.3 Políticas de Seguridad a Nivel Humano

El aspecto humano es el punto más crítico cuando se habla de seguridad de una red de datos y más aún cuando se trata de una institución pública, ya que existe desconocimiento de los derechos y deberes de cada persona que compone la red (administradores, operadores, monitores, usuarios, etc.) y esto causa que se puedan presentar problemas. Además no existe una cultura referente al buen uso de la red, por lo que la primera medida es educar a los usuarios y demás personal acerca de todo lo que se puede hacer o no con las instalaciones y servicios de la red, qué pueden aprovechar de ella, y como lo pueden conseguir.

➢ Características generales del personal de la Red de Datos:

Un empleado de la red de datos es aquel que tiene a su cargo diferentes tareas de administración, operación, gestión y mantenimiento de la red y que para ejecutarlas, debe tener cierto conocimiento de diferentes temas de redes y sistemas telemáticos en diferente grado, según sus responsabilidades y el cargo ejercido.

- El administrador de la red de datos tiene como funciones principales dirigir, planificar y controlar todas las actividades de la red, de las que es responsable ante la vicerrectoría administrativa. Debe proponer objetivos y políticas, preparar el programa de trabajo a seguir, establecer políticas de personal y salariales específicas para los diferentes grupos, mantener actualizada la estructura organizativa, especificar la normalización para el desarrollo y la documentación del trabajo, desarrollar las diferentes normas de interacción con los usuarios, entre otras muchas, para las cuales debe contar con una preparación profesional suficiente que sirva de guía para el demás personal. Debe ser un Ingeniero en Electrónica y Telecomunicaciones con especialización en Redes y Servicios Telemáticos o afines.

- Los operadores de la red se encargan de la operación y el mantenimiento de los servidores y demás equipos importantes para el correcto funcionamiento de la red, la gestión de estos equipos, su configuración, velar por su buen desempeño, y diseñar y analizar los nuevos sistemas a implementar. Además debe ser capaz de presentar e implementar propuestas para el mejoramiento de la red, preparar documentos y manuales de procedimientos y realizar los cambios a un servicio o configuración cuando sea necesario. Debe ser un estudiante de Ingeniería Electrónica y Telecomunicaciones de últimos semestres, con énfasis en Telecomunicaciones, o un estudiante de Ingeniería de sistemas con conocimientos en Redes y Servicios Telemáticos.

➢ Plan de Admisión del personal:

Debido a que muchas de las personas que se hacen cargo de la red son estudiantes de últimos semestres, se lleva a cabo una renovación continua del personal. Es importante tener en cuenta ciertos detalles a la hora de realizar reclutamiento de personal para la red, de forma que la persona elegida tenga la calidad humana y las cualidades profesionales para desarrollar un cargo:

- Nivel de conocimiento.
- Personalidad y Responsabilidad.
- Interés en llevar a cabo la labor.
- Ética.
- Trabajo en Equipo.
- Pertenencia.

Esto debe ser evaluado entre dos o más administradores de la red de forma detallada, haciendo uso de entrevistas personales, técnicas y exámenes de aptitud.

➢ Recomendaciones para los grupos de la Red de Datos:

- Solo el administrador puede tomar decisiones que afecten directamente la prestación de los servicios, asignación de tareas, contratación de personal, compra de equipos, aunque debe dar cierta libertad controlada a los miembros de su equipo, debe estar al tanto de todo lo que ocurre en la red.

- Todos los integrantes de la red están obligados a cumplir las funciones asignadas y a colaborar con el desarrollo de la red, como una dependencia de investigación independiente.

- Todas las responsabilidades en cuanto a funcionamiento de la red y al bienestar de los equipos fundamentales, recaen sobre el administrador. Él será quien dentro de su equipo determine quién está comprometida en algún fallo y prescindir de esa persona.

- Cada persona de la red debe ser capaz de realizar las tareas asignadas al grupo al cual pertenece; en el caso de nuevos miembros, sus compañeros de trabajo deben encargarse de darle la capacitación que necesite y el apoyarlo en todo momento.

- Se deben elaborar manuales de procedimientos frecuentes y repetitivos, para que estén disponibles para cualquier miembro del equipo que lo requiera.

- El ambiente de trabajo debe ser sano, sin que se sienta la relación jefe-empleado, debe haber un ambiente de amistad y trabajo en equipo, ya que este es un grupo cuya motivación es aprender y colaborar con la Universidad.

- Cada grupo de trabajo debe tener un lugar de trabajo fijo, sin interferir con los demás.

- Dentro del grupo de operadores, es recomendable que cada persona se encargue de un grupo de servidores y vele por su correcto funcionamiento; en éste caso sólo él y el administrador tendrían acceso a estos servidores y de esta forma es posible segmentar la seguridad de la red.

- El administrador de la red debe tener acceso a todos los recursos físicos y lógicos.

- El acceso a la sala de servidores solo debe ser permitida al administrador de la red y a los operadores. En cualquier otro caso, se debe tener autorización del administrador y una persona externa debe estar siempre acompañada de una de las personas autorizadas.

- En las salas públicas el monitor debe llevar un control de las personas que necesitan acceder a ellas, pidiendo carné y motivo por el cual necesita la red.

- No se debe hacer uso indebido de los beneficios que se reciben al formar parte del grupo de la Red de Datos. No se debe modificar o borrar información confidencial de los usuarios o para beneficio propio. En caso de acciones indebidas, el miembro del grupo deberá someterse a las acciones disciplinarias correspondientes.

➢ Comportamiento de los usuarios de la Red de Datos:

Todas las reglas que se planteen en este sentido deben ser dadas a conocer a todos los usuarios de la red y estar publicadas en las salas de acceso público. De igual forma deben ser acatadas por todos los usuarios de la red sin excepción; cada usuario es responsable de sus acciones en la red. Si algún estudiante, profesor, administrativo o cualquier otro empleado viola una de las políticas de seguridad, estará sujeto a las acciones disciplinarias correspondientes según el reglamento de la universidad y según los estamentos superiores lo dispongan. Estas acciones disciplinarias pueden ir desde una advertencia verbal o escrita, hasta la suspensión del servicio temporal o definitivo y hasta la expulsión de la Universidad, dependiendo de la violación.

- Las cuentas de los usuarios son personales e intransferibles.

- Leer y aceptar el Reglamento acerca del uso de la red.

- Utilizar contraseñas de más de 8 caracteres, combinando letras, números y caracteres alfanuméricos. No utilizar nombres propios o información personal ni palabras de diccionario en cualquier idioma.

- Cambiar la contraseña periódicamente por lo menos cada 3 meses.

- Aceptar todas las recomendaciones del personal que trabaja en la red de datos acerca de la seguridad y manejo de los archivos.

- Hacer uso racional de los recursos y servicios de la red.

- No visitar ni descargar archivos de páginas cuyo origen sea poco confiable.

- No comer ni beber cerca de los equipos de red.

- En caso de problemas de acceso a cuentas, a servicios, a equipos o de sospechas de problemas de seguridad, acudir únicamente al personal autorizado de la Red de Datos.

- Se deben cuidar los recursos físicos de la red y no modificar sus configuraciones ni la disposición del cableado.

- Leer el manual de Seguridad para los usuarios de la red, que debe ser escrito por el personal de la Red de Datos, para que todas las personas estén al tanto de lo que puede ocurrir si no tienen cuidado a la hora de trabajar en la red.

- En caso de cualquier acción sospechosa o poco común que detecte sobre la infraestructura de la red, avisar inmediatamente a la administración.

Sanción: En caso de cometer acciones indebidas mientras se utilizan los beneficios de la red, se debe responder ante la administración de la misma, caso en el cual, si el administrador lo considera necesario, puede hablar con el decano de la Facultad e imponer castigos desde llamados de atención y anotaciones en la Hoja de Vida, hasta la desvinculación de la Universidad e incluso llevarlo a ámbitos judiciales, según el caso.

Cuando un usuario ingresa a la Universidad, debe firmar un contrato aceptando todo lo anterior y comprometiéndose a hacer un correcto uso de los recursos de la red.

El uso de los recursos y servicios de la red dependen del cuidado que se les dé, principalmente, por lo que la mejor medida es educar a los usuarios para que sepan que esto es un servicio serio para su propio beneficio.

6.2.4 Propuestas de Seguridad a nivel de Red para la Red de Datos de la Universidad del Cauca

Primero que todo, una vez estudiada la arquitectura actual de la Red de Datos, el esquema más acertado para su implementación es el Esquema de **seguridad perimetral** acompañado de un esquema de **seguridad interna**, como piedra angular para el cumplimiento de las políticas definidas. En este esquema, el acceso desde el exterior, necesariamente debe estar centralizado de manera efectiva en un único punto, en el que se concentrarían la gran mayoría de las medidas. De esta forma es posible aprovechar el Firewall Cisco PIX 515E que ya implementa la Red de datos en su enlace con Orbitel y el Firewall por software IPTables con el enlace a Telecom. También se deben agilizar medidas para mejorar la seguridad de los sistemas internos, que aunque no impliquen un modelo de seguridad en profundidad, sí deben proporcionar los resultados esperados, ya que la mayoría de ataques hacia una red provienen de los usuarios internos de la misma. Las estrategias y los paradigmas de seguridad a utilizar se evaluarán en cada una de las arquitecturas a proponer, para escoger la más acertada.

Antes de llevar a cabo las propuestas es importante tener claro el flujo de información que maneja la Red de la Universidad del Cauca, como se muestra en la figura 6.2.

Como se puede observar, hay tres tipos de flujos de información a través de toda la Red de Datos de la Universidad: primero, se tiene el Flujo de Información que se intercambia directamente con Internet gracias a las direcciones reales que contrata la Universidad del Cauca y las cuales están distribuidas por todas los sectores de la misma; en segundo lugar, el Flujo de Información de Acceso a Servicios que proveen los Servidores Públicos de la Red de Datos tales como Web, DNS, Proxy Http, Correo, entre otros, que son accesados desde todos los sectores de la Universidad incluyendo las sedes remotas; este es el Flujo de Información de mayor densidad. Por último el Flujo de Información de Acceso a Servicios que proveen los Servidores Privados de la División de Sistemas, dentro del cual se encuentra información de los sistemas Financieros, de Recursos Humanos, de Recursos Físicos y muy pronto de Información Académica. La información Financiera puede ser consultada por la mayoría de las dependencias administrativas de la Universidad, entre ellas las Decanaturas de cada Facultad, pero solo tienen acceso con privilegios administrativos los funcionarios de la División Financiera que están agrupados en el segundo piso del edificio de Santo Domingo y la Vice-rectoría Administrativa, las cuales manejan información importante que es necesario proteger. La información de Recursos Humanos, también importante, es accedida solamente por los Funcionarios de la División de Recursos Humanos, la Vice-rectoría Administrativa y otras oficinas que se encuentran concentrados en el Edificio de Santo Domingo. La información de Recursos Físicos es accedida solamente por los funcionarios del Área de Servicios Generales.

6.2.4.1 **PROPUESTA 1: Propuesta de Seguridad basada en Subredes e IPSec**

Uno de los propósitos de esta propuesta es dividir la red de la Universidad del Cauca en VLANs basándose en la ubicación física de los diferentes sectores, lo que permite al mismo tiempo llevar a cabo una subdivisión en subredes IP. La subdivisión en subredes disminuye el tamaño de los dominios de Broadcast ARP, lo cual minimiza el impacto de ataques a nivel de enlace de datos como suplantación ARP, envenamiento de caché ARP entre otros, como se estudio en el capitulo 2. Además manejar dominios pequeños disminuye el tráfico Broadcast limitándolo a cada subred, lo que aumenta considerablemente el rendimiento de la red.

Al hacer el análisis de la red se identificaron seis sectores principales teniendo en cuenta su ubicación geográfica y concentración de equipos como se muestra en la figura 6.3. A cada sector se debe asignar una subred (un rango de direcciones) y a su vez cada subred debe pertenecer a una VLAN configurada en el switch de núcleo Cisco Catalyst 4507, con que cuenta ya la Red y que tiene las siguientes características de seguridad:

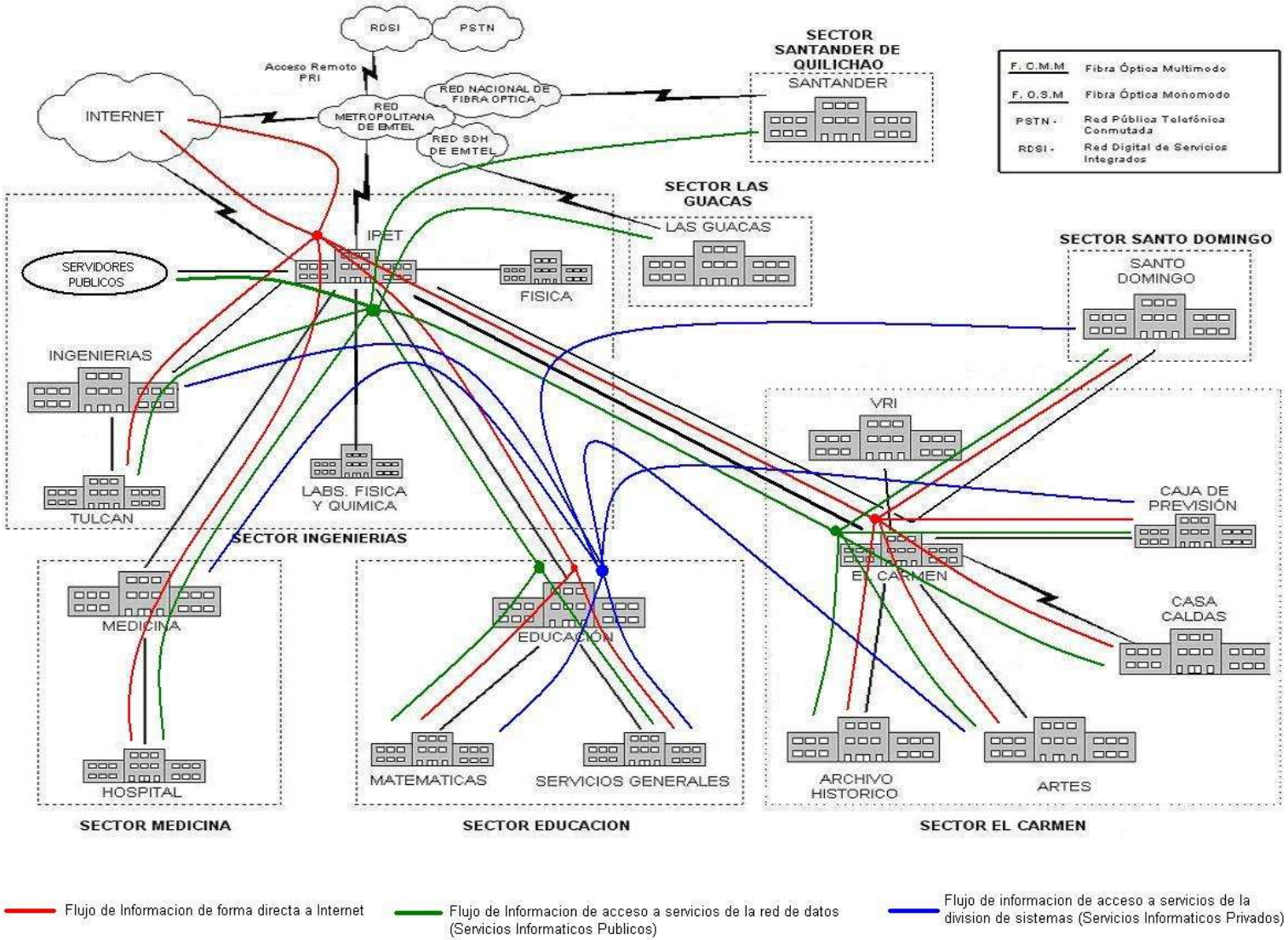


Figura 6.2. Diagrama de Flujo de la Información a través de la red

- Autenticación de puerto por 802.1X
- Listas de control de acceso para prevenir el acceso no autorizado a aplicaciones o servicios.
- Gran numero de VLANs permitidas, hasta 4096.
- VLANs Privadas.
- Analizador de puerto para monitorear puertos simples o agrupados en VLANs por medio de un puerto especial.
- SSH para conexión remota con el switch.
- Port Security para asegurar el acceso de las maquinas a la red.
- Inspección de ARP dinámica.

De esta forma, cada subred utilizará un rango de direcciones diferente y el switch de núcleo nivel 3 será el encargado de realizar el enrutamiento y la conmutación entre ellas como se muestra en la figura 6.4:

- Sector Ingenierías (Subred 10.100.0.0/16, VLAN Ingenierías, VLAN ID 100)
- Sector IPET (Subred 10.200.0.0/16, VLAN ServidoresPublicos, VLAN ID 200)
- Sector Medicina (Subred 10.300.0.0/16, VLAN Medicina, VLAN ID 300)
- Sector Educación (Subred 10.400.0.0/16, VLAN Educación, VLAN ID 400)
- Sector El Carmen (Subred 10.500.0.0/16, VLAN ElCarmen, VLAN ID 500)
- Sector Santo Domingo (Subred 10.600.0.0/16, VLAN StoDomingo, VLAN ID 600)

Para efectos de seguridad los servidores públicos que se encuentran en el IPET (servidores de la red de datos) deben asignarse a una VLAN exclusiva; esto se facilita debido a que éstos servidores se encuentran conectados directamente al switch; el resto de equipos que se encuentran en el sector del IPET harán parte de la VLAN Ingenierías debido a que su número es reducido.

En el switch nivel 3 se deben crear las 6 interfaces VLAN que se describieron anteriormente, según los sectores identificados; después de esto, se debe configurar la asignación de una VLAN a cada subred. Para esto, a cada Interface VLAN se debe asignar una dirección IP que corresponderá a la puerta de enlace que se configurará a los equipos de cada subred, por ejemplo (ver Figura 6.4):

1 A la Interface VLAN Ingenierías se le asigna la dirección IP: 10.100.255.254 con máscara de subred 255.255.0.0.
2 A la Interface VLAN ServidoresPublicos se le asigna la dirección IP: 10.200.255.254 con máscara de subred 255.255.0.0.
3 A la Interface VLAN Medicina se le asigna la dirección IP: 10.300.255.254 con máscara de subred 255.255.0.0.
4 A la Interface VLAN Educación se le asigna la dirección IP: 10.400.255.254 con máscara de subred 255.255.0.0.
5 A la Interface VLAN ElCarmen se le asigna la dirección IP: 10.500.255.254 con máscara de subred 255.255.0.0.
6 A la Interface VLAN StoDomingo se le asigna la dirección IP: 10.600.255.254 con máscara de subred 255.255.0.0.

De esta manera, la tarea de realizar el enrutamiento entre subredes la realizará el switch de núcleo sabiendo que cada subred la tiene conectada directamente por una interface VLAN. Además de esto, deben tenerse en cuenta dos casos especiales. La red maneja un rango de direcciones IP Reales provistas por el proveedor Telecom, que comprenden los rangos

200.21.83.64/26 y 200.21.83.128/26 y se encuentran distribuidas por todo el campus universitario, por lo cual debe crearse una *VLAN DireccionesTelecom* para estos equipos, a la que pertenezcan todos los puertos del switch de núcleo y que dicha VLAN abarque las dos subredes provistas por Telecom. Las puertas de enlace predeterminadas para estos equipos seguirán siendo la 200.21.83.126 para la red 200.21.83.64/26 y la 200.21.83.190 para la red 200.21.83.128/26 que pertenecen al Firewall IPTables. De esta forma cada puerto del switch de núcleo permitirá el paso del tráfico proveniente de la VLAN asignada y de la VLAN DireccionesTelecom:

- DireccionesTelecom (VLAN DireccionesTelecom, VLAN ID 700)

También, se recomienda mantener la seguridad perimetral que se encuentra implementada mediante el Firewall IPTables (en el enlace con el proveedor Telecom) y el Firewall PIX 515E (en el enlace con el proveedor Orbitel), pero se debe realizar un análisis de las reglas definidas en el Firewall IPTables, y adaptarlas de igual manera para el Firewall PIX, que se encuentra en este momento sin reglas de filtrado de puertos definidas. Se debe aplicar una estrategia que garantice que "todo lo que no esté expresamente permitido sea rechazado".

Por otro lado, deben tenerse en cuenta los servidores de la División de Sistemas, en los que se maneja la información Financiera, de Recursos Humanos y Físicos; esta información no es de dominio público, por esta razón es muy importante aislar el tráfico de estos servidores hacia el resto de la red que no debe acceder a ella. En la División de Sistemas también se encontrarán los servidores del Sistema Académico Sócrates, pero el acceso a la gran parte de esta información es de dominio público a través de la Web, ya que todos los estudiantes de la Universidad tendrán la opción de consultar sus notas; el acceso por parte de las secretarías de Facultad, las cuales gestionan esta información, será también vía Web, utilizando ciertos mecanismos de autenticación a nivel de aplicación, por lo que no se tendrá en cuenta dentro de la propuesta.

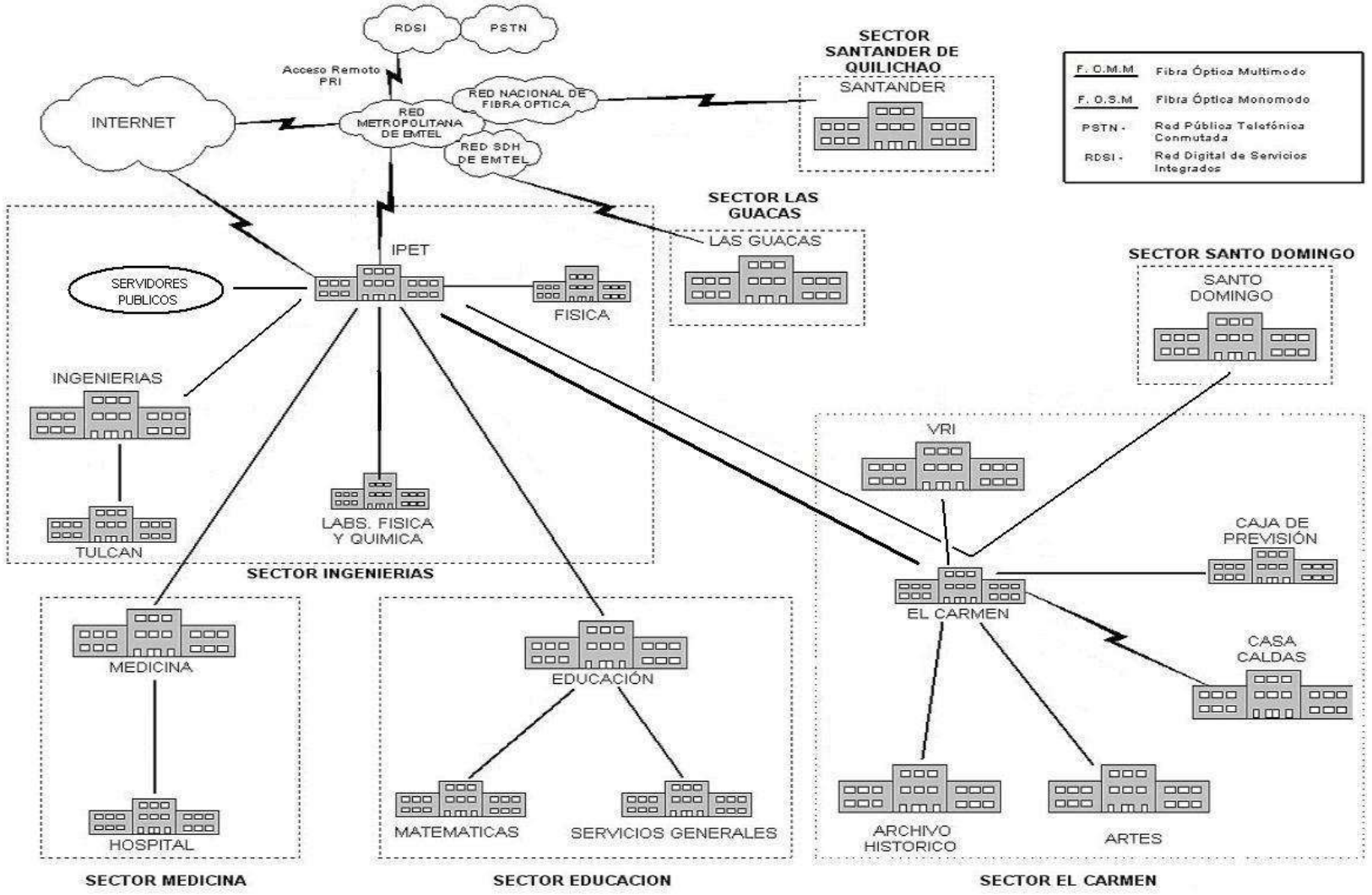


Figura 6.3. Sectores en que se divide la Red de la Universidad del Cauca

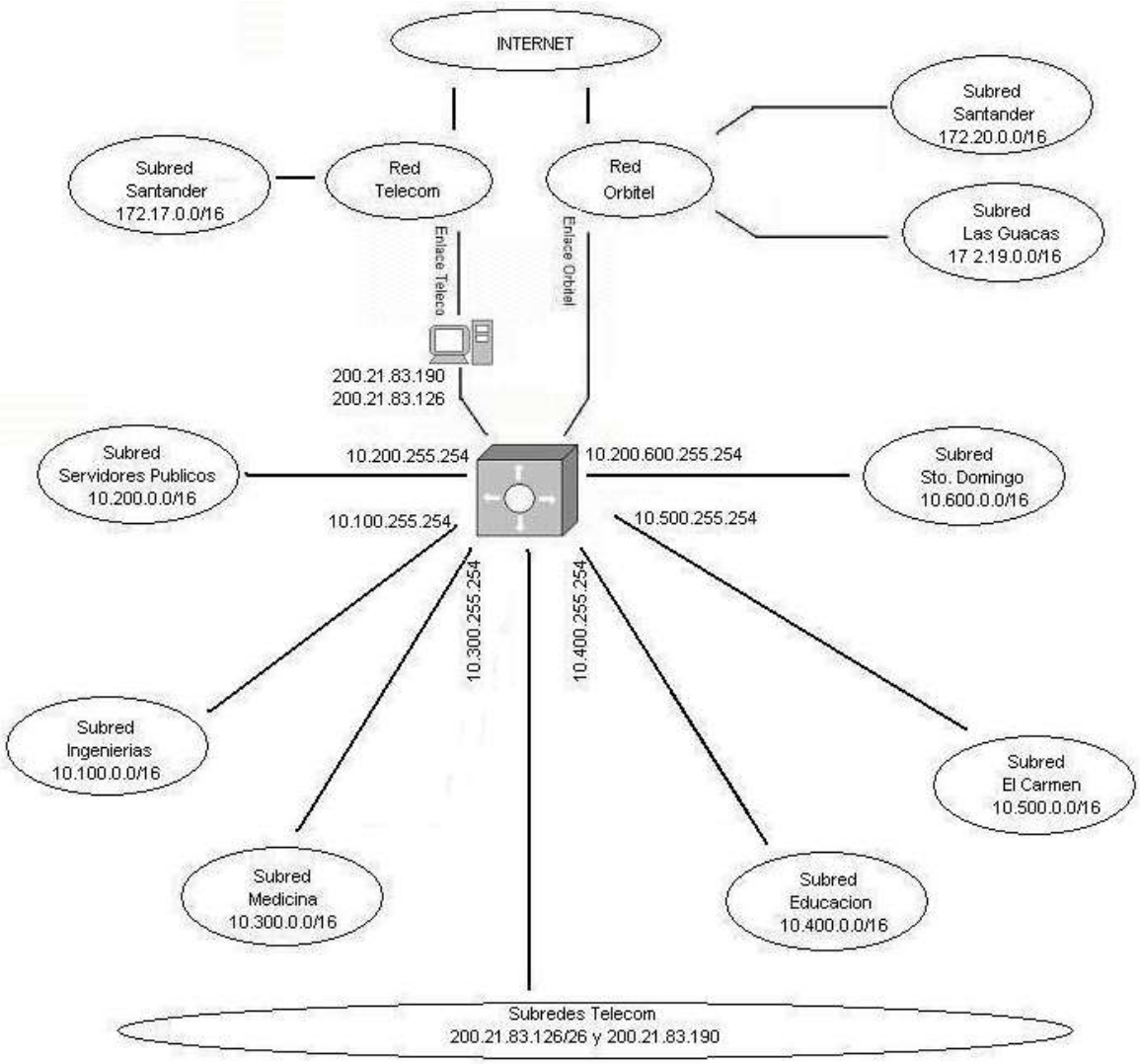


Figura 6.4. Subdivisión en subredes y VLANs

En la Figura 6.2 se puede observar el diagrama de flujo de información que se transmite en este momento sobre la red de la Universidad. Como se puede observar, la información Financiera es accedida desde todas los sectores por los Decanos; ellos cuentan con una aplicación instalada en sus equipos que se conecta directamente con el Servidor de Bases de Datos ubicado en la División de Sistemas, teniendo privilegios solo para consultar la información relacionada con el presupuesto de su Facultad. La información Financiera es también accedida principalmente desde la División Financiera y la Vice-rectoría Administrativa en Santo Domingo, desde la Caja de Previsión, desde las oficinas de recursos Físicos y la Caja de Servicios en el Área de Servicios Generales, que se conectan al servidor de Bases de Datos a través de un Servidor de Aplicaciones también ubicado en la División de Sistemas; sin embargo, existen otras oficinas que también tienen acceso a esta información y están dispersas por todas las sedes de la Universidad. La información de Recursos Humanos es accedida por la oficina de Recursos Humanos, por la oficina de Planeación, la Vicerrectoría

Administrativa y dos personas de la División Financiera, todas ellas ubicadas en el sector de Santo Domingo. La información de Recursos Físicos tiene un manejo centralizado desde el Área de Servicios Generales.

De todo lo anterior, se considera sensible la información intercambiada en las conexiones con los Servidores Privados; estos serán los enlaces a proteger, al igual que el acceso no autorizado a los servidores. A partir de este punto, se plantea implementar seguridad mediante IPSec a las comunicaciones que se realizan entre los clientes y los servidores Privados y entre la red de la Universidad en Popayán y sus sedes remotas.

- ✓ *Conexiones entre los Clientes y los servidores Privados:*

Para estas conexiones, que como se describió anteriormente necesitan protección debido a que a través de ellas se envía información de los procesos administrativos de la universidad, se propone implementar el Protocolo IPSec en su Modo Transporte para garantizar seguridad extremo a extremo y porque se facilita la configuración debido a que los clientes no se encuentran agrupados físicamente. Para esto es necesario implementar soporte IPSec en los Servidores que se quieren proteger y en los clientes que acceden a ellos. Todos los servidores tienen instalado Sistema Operativo Windows 2000 Server y los equipos clientes corren sobre Windows 2000 o XP, por lo que el soporte IPSec está garantizado.

Para configurar IPSec entre un cliente y el servidor al cual debe tener acceso, se debe implementar una *Directiva Personalizada* que utilice un filtro para una *Dirección IP específica (como se implementó en la práctica 6 del Capitulo 5)*, en este caso, la dirección IP del servidor destino de la conexión; de igual forma en el servidor, debe declarar una directiva que asegure la conexión con el cliente. Como se observó en las prácticas, el mejor método de autenticación es el de certificados Digitales, porque provee una mayor seguridad y es más gestionable; sin embargo, está sujeto a la implementación de una *Entidad de Certificación Cerrada* para la Universidad del Cauca, que es un proyecto que se está llevando a cabo al interior de la Red de Datos. Esta Entidad Certificadora recibirá los requerimientos de creación de Certificados, verificará que los datos sean reales y expedirá el respectivo certificado, que deberá ser instalado en el equipo respectivo y por medio del cual se llevará a cabo la autenticación y cifrado. De esta forma, cada servidor deberá tener definidas tantas directivas de seguridad como clientes accedan a él y los clientes definirán la directiva para la conexión con el servidor que necesiten acceder.

- ✓ *Conexiones con la Sede remota de Santander de Quilichao*

El estado actual del enlace con la sede de Santander de Quilichao se muestra en la figura 6.5. La conexión remota con ésta sede se realiza a través del enlace del proveedor Orbitel y del proveedor Telecom; debido a que la información desde y hacia Santander se trasporta sobre una red pública, está expuesta a sufrir ataques de diversa índole, que podrían afectar su confidencialidad, integridad y la autenticidad de la información. Por esta razón, se considera necesario que la Universidad garantice la seguridad de esta conexión

por medio de una VPN sobre IPSec (Modo Túnel) en cada uno de los enlaces. Para esto, es necesario introducir dos Gateways de Seguridad en cada enlace, para garantizar que todo el tráfico entre ellas será intercambiado de forma segura.

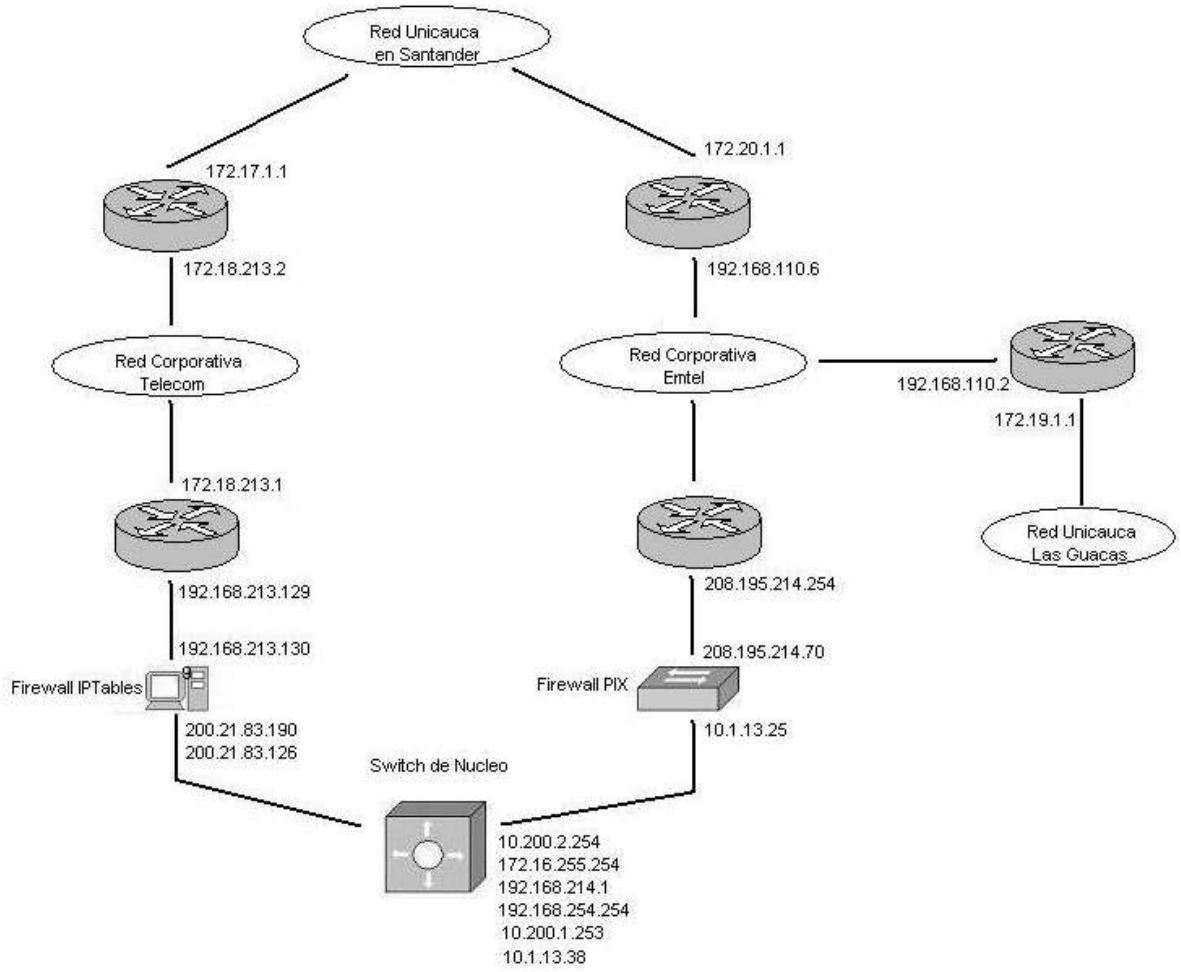


Figura 6.5. Estado actual del enlace con la sede de Santander de Quilichao

Para el enlace proporcionado por el proveedor Telecom, se introduce una *Gateway de Seguridad 1* entre el switch de núcleo y el equipo que corre el Firewall IPTables, como se muestra en la figura 6.5. De esta forma, esta SG1 pasará a ser la nueva puerta de enlace de los equipos que manejan direcciones IP reales de los rangos 200.21.83.64/26 y 200.21.83.128/26 (antes era el equipo que corre el Firewall IPTables, con las direcciones 200.21.83.126 y la 200.21.83.190). En el Firewall IPTables se tienen definidas ciertas reglas de bloqueo de puertos y otras consideraciones de seguridad, las cuales seguirán funcionando sin ningún problema sobre los paquetes protegidos. En el otro extremo del túnel, se debe introducir una Gateway de Seguridad 2 entre el router y la red de Santander de Quilichao (que comprende las subredes 172.17.0.0/16 y 172.20.0.0/16); de esta forma, la SG2 protegerá todo el tráfico desde y hacia estas subredes.

Estas Gateways de Seguridad son equipos normales, como los Dell con procesador Pentium 4 que está adquiriendo la Universidad, sobre las cuales esté montado el Sistema Operativo Linux Debian 3.1, el cual es de libre distribución y se ha comprobado que proporciona la estabilidad necesaria para soportar cualquier servicio y es por esto que sobre él se encuentran la mayoría de los servidores de la red; además estas SG deben tener dos interfaces de red, para permitir la configuración mostrada en la figura 6.6.

El soporte IPSec puede ser proporcionado utilizando la herramienta Usagi, utilizando autenticación y cifrado por medio de Firmas Digitales RSA (ver la Práctica 3 del capitulo 5, para la Configuración de IPSec en Modo Túnel). Debido a que la Gateway de Seguridad 1 protege información proveniente de la subred 200.21.83./24 (que es el rango de las direcciones IP reales que provee Telecom), es necesario plantear una asociación y políticas de seguridad para ésta; entre la información a tener en cuenta en la configuración de IPSec en la SG1 se tiene:

left=208.21.83.126
leftnexthop=192.168.215.2
leftsubnet=200.21.83.0/24
right=172.17.1.1
rightnexthop=192.168.216.1
rightsubnet=172.17.0.0/16

De igual forma en la SG2, debe considerarse la misma información para crear las Asociaciones y Políticas de Seguridad, teniendo en cuenta que los parámetros left y right deben ser intercambiados.

Como se puede observar, las asociaciones solo se plantean para la subred 172.17.0.0/16 de Santander de Quilichao, ya que la información de los equipos pertenecientes a la subred 172.20.0.0/16, se enruta por el enlace de Orbitel, que se describe a continuación.

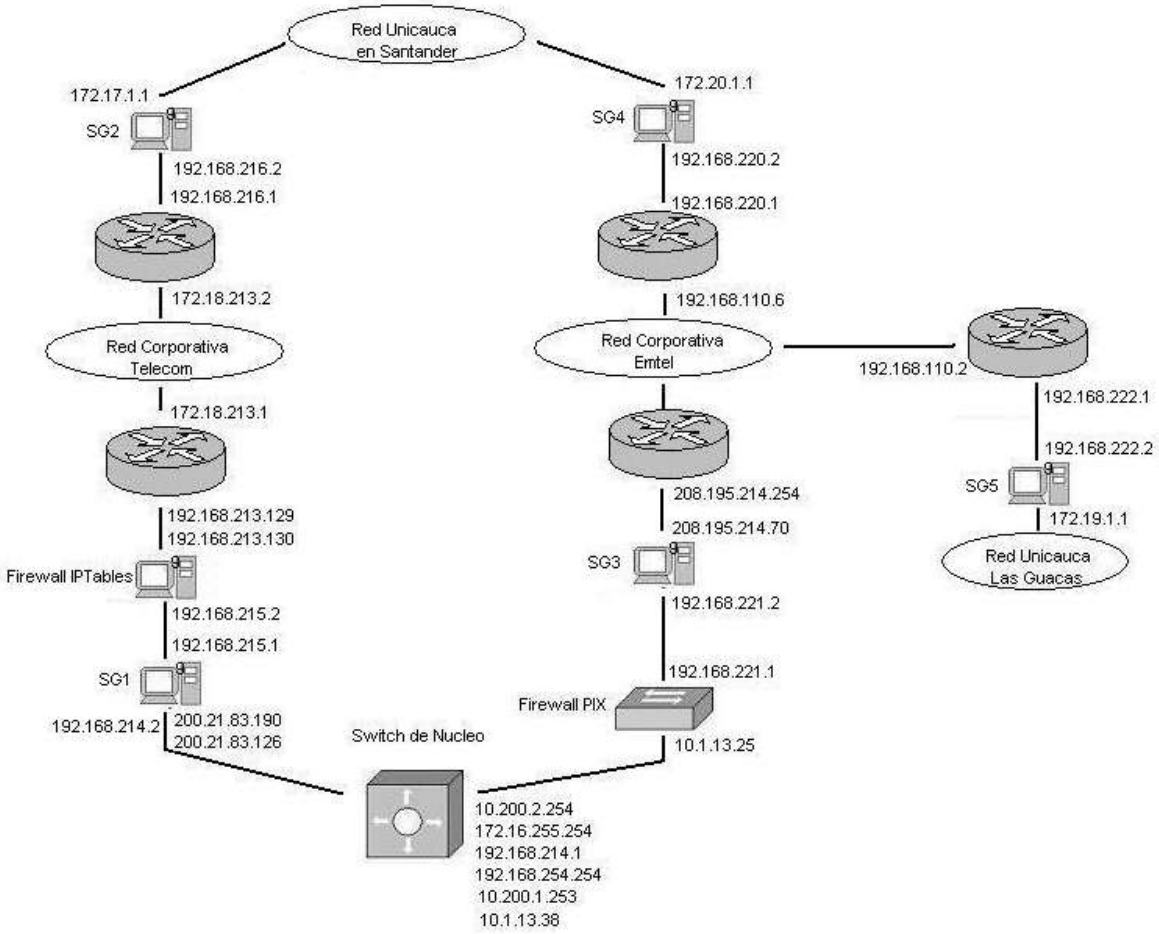


Figura 6.6. VPNs en los enlaces con las sedes remotas.

Hasta aquí ya se tiene planteado el mecanismo para asegurar uno de los enlaces con la Sede de Santander de Quilichao. Ahora es necesario hacer lo mismo en el enlace por medio del proveedor Orbitel. En este caso, existe una diferencia que se debe tener en cuenta; este enlace en este momento implementa un Firewall PIX 515E, el cual no tiene definidad unas reglas de filtrado como el Firewall IPTables, pero que esta llevando a cabo la función de NAT (Traducción de Direcciones de Red) sobre algunas direcciones de la subred actual 10.200.2.0/24 que necesitan los privilegios de una IP real para realizar diferentes funciones, ya determinadas por los administradores de la red. Como se estudió en el Capítulo 3, las implementaciones actuales de IPSec no soportan NAT, ya que, si se protege una trama IP insertándole el encabezado AH y ESP, éstos realizan la autenticación y cifrado del paquete teniendo en cuenta las direcciones Origen y Destino originales; además las Asociaciones y Políticas de Seguridad se realizan entre las direcciones de los extremos del túnel; si se hace NAT sobre el paquete ya protegido, éste cambia la dirección de origen del paquete y al llegar a la SG del otro extremo, ésta no va a ser capaz de llevar a cabo la negociación IPSec, porque las condiciones especificadas en las Asociaciones y Políticas de Seguridad no coinciden. Es por esto que se debe introducir una *Gateway de Seguridad 3* entre el Firewall PIX y el router del proveedor de Orbitel, como se muestra en la figura 6.5. De esta forma, la SG protegerá el tráfico proveniente de la subred 10.0.0.0/8 y de la subred 208.195.214.0/24 que son las direcciones de las subredes de la intranet y las direcciones IP reales que se

asignan al llevar a cabo la función de NAT en el PIX, respectivamente. En el otro extremo, debe introducirse una Gateway de Seguridad 4 entre el router de Orbitel y la red de Santander de Quilichao (por este enlace se transporta la información de la subred 172.20.0.0/16). Para este caso es necesario plantear 2 Asociaciones y Políticas de Seguridad diferentes, como en el caso anterior, para considerar el tráfico proveniente de las dos subredes que se trasporta por este enlace. La información que se debe tener en cuenta en la configuración de IPSec para la conexión con equipos de la subred 10.0.0.0/8 en la SG3 se tiene:

left=208.195.214.70
leftnexthop=208.195.214.254
leftsubnet=10.0.0.0/8
right=172.20.1.1
rightnexthop=192.168.220.1
rightsubnet=172.20.0.0/16

La información a tener en cuenta en la configuración de IPSec para la conexión con equipos de la subred 208.195.214.0/24 en la SG3 se tiene:

left=208.195.214.70
leftnexthop=208.195.214.254
leftsubnet=208.195.214.0/24
right=172.20.1.1
rightnexthop=192.168.220.1
rightsubnet=172.20.0.0/16

De igual forma en la SG4, debe considerarse la misma información para crear las asociaciones y políticas de seguridad, teniendo en cuenta que los parámetros left y right deben ser intercambiados.

Así, se tienen implementadas las dos VPNs necesarias para proteger el tráfico desde y hacia la sede remota de Santander de Quilichao. A pesar de que se intentó llevar a cabo la propuesta de forma que el impacto sobre la configuración actual fuera el menor posible, como se observa, se deben llevar a cabo algunos cambios en las direcciones de las interfaces de los routers, por lo que se debe dar a conocer la propuesta a los proveedores para que realicen los cambios respectivos, ya que los únicos Routers que maneja la Red de Datos de la Universidad son los del enlace a través del proveedor Telecom.

- *Conexiones con la Sede remota del Sector las Guacas*

La conexión con la sede remota del Sector las Guacas se realiza a través del enlace del proveedor Orbitel, que se soporta sobre la red Metropolitana de Emtel; en esta conexión es muy posible que la información sea interceptada ya que se trasporta sobre una red pública, por lo que se propone implementar la seguridad en la comunicación por medio de una VPN sobre IPSec (Modo Túnel). Para esto es necesario introducir dos Gateways de Seguridad, una en cada extremo como se muestra en la figura 6.6, para de esta forma proteger el tráfico que se transporta entre las subredes definidas en la intranet y la red de las Guacas, 172.19.0.0/16.

Como se observa en la figura 6.6, se tiene ya una *Gateway de Seguridad 3* entre el Firewall PIX 515E y el Router de Orbitel (que se introudjo en el diseño de la VPN con Santander de Quilichao); como ya se explicó, la Gateway de Seguridad se introduce después del Firewall debido a que éste realiza NAT (Traducción de Direcciones de red) para algunas direcciones configuradas en él, que necesitan ser convertidas a direcciones IP reales y las implementaciones de IPSec no soportan este servicio, ya que cambia por completo la definición de la conexión segura. En el otro extremo se introduce una *Gateway de Seguridad 5* entre el router de Emtel que da conexión a la sede de las Guacas, y la red 172.19.0.0/16, convirtiéndose en la nueva puerta de enlace por defecto para esta red.

Las Gateways de Seguridad son equipos normales, con dos interfaces de red, con un Sistema Operativo Linux Debian 3.1, de libre distribución y considerado el más estable; soporte IPSec por medio de la herramienta Usagi utilizando autenticación y cifrado por medio de Firmas Digitales RSA (ver la Práctica 3 del capitulo 5, para la Configuración de IPSec en Modo Túnel). Debido a que la Gateway de Seguridad 3 protege información proveniente de las subredes 10.0.0.0/8 y 208.195.214.0/24, es necesario plantear dos asociaciones y políticas de seguridad diferentes, una correspondiente a cada subred protegida; entre la información a tener en cuenta en la configuración de IPSec para la conexión con equipos de la subred 10.0.0.0/8 en la SG3 se tiene:

left=208.195.214.70
leftnexthop=208.195.214.254
leftsubnet=10.0.0.0/8
right=172.19.1.1
rightnexthop=192.162.222.1
rightsubnet=172.19.0.0/16

La información a tener en cuenta en la configuración de IPSec para la conexión con equipos de la subred 208.195.214.0/24 en la SG3 se tiene:

left=208.195.214.70
leftnexthop=208.195.214.254
leftsubnet=208.195.214.0/24
right=172.19.1.1
rightnexthop=192.162.222.1
rightsubnet=172.19.0.0/16

De igual forma en la SG5, debe considerarse la misma información para crear las asociaciones y políticas de seguridad, teniendo en cuenta que los parámetros left y right deben ser intercambiados. De esta forma se ha implementado la VPN necesaria para proteger el tráfico desde y hacia la sede remota de las Guacas. A pesar de que se intentó llevar a cabo la propuesta de forma que el impacto sobre la configuración actual fuera el menor posible, como se observa, se deben llevar a cabo algunos cambios en las direcciones de las interfaces de los routers, por lo que se debe dar a conocer la propuesta a los proveedores para que realicen los cambios respectivos.

- *Consideraciones Adicionales*

Adicionalmente, se recomienda mantener la seguridad perimetral que se encuentra implementada mediante el Firewall IPTables y el Firewall PIX 515E, haciendo un análisis de las reglas de filtrado, como se recomendó en la Propuesta 1.

Para esta propuesta se necesitan los siguientes equipos:

6 equipos Dell optiplex GX280 ya que no se requieren equipos con capacidades de servidor, imprescindible que traiga incorporado dos interfaces de red; sus características son:

- Procesador pentium 4 de 3.8GHz
- Memoria RAM de 512MB
- Disco Duro de 10GB
- Dos interfases de red Gigabit Ethernet.

➢ *Ventajas de la Propuesta 1*

La propuesta anterior tiene las siguientes ventajas:

- Satisface muchas necesidades de seguridad en cuanto a autenticación y cifrado a nivel de red en conexiones de alta sensibilidad para la Universidad.
- Divide la red de la Universidad del Cauca en subredes IP lo cual trae múltiples beneficios en cuanto a seguridad y rendimiento se refiere.
- Se interconectan de forma segura las sedes remotas con las que cuenta la Universidad del Cauca.
- Es fácil de implementar, ya que las configuraciones de las que se requieren se realizan sobre pocos sectores y dicha configuración no es muy compleja.
- Es una propuesta económica, ya que no se necesitan equipos nuevos de muy alto costo. Se trabaja sobre la infraestructura que existe. Solo se necesitan 5 nuevos equipos que funcionen como gateways de seguridad los cuales no tienen que ser de muy altas prestaciones.

➢ *Desventajas de la Propuesta 1*

- No cuenta con mecanismos que permitan monitorear riesgos de seguridad en la red.
- Los aspectos de seguridad se cubren solo sobre los sectores más sensibles de la red, dejando los sectores masivos sin protección o con la protección existente en el momento.
- No restringe el uso de la red a usuarios no autorizados en la red universitaria.

6.2.4.2 **PROPUESTA 2. Propuesta de Seguridad Integrada**

En este caso se parte de la propuesta anterior y se busca introducir unos mecanismos adicionales que son muy utilizados en la actualidad, pero cuya implementación es extensa y aumenta considerablemente los costos y el impacto sobre la infraestructura actual de la Red de Datos. El resultado de implementar esta propuesta se muestra en la figura 6.7; los mecanismos adicionales son:

- ✓ *Implementación de autenticación por medio del Estándar 802.1x:*

Para esto es necesaria la eliminación de todos los Hubs que se encuentran en el borde de la red y reemplazarlos por switches que soporten esta característica, como el switch Cisco Catalyst 2950 cuyas características se enuncian a continuación. Una vez hecho esto, se debe habilitar en cada puerto al que esté conectado un equipo el soporte de autenticación por 802.1x y configurarle como servidor de autenticación el Servidor RADIUS que se tiene implementado en la Universidad del Cauca, que puede realizar la verificación de cualquier usuario registrado en la red consultando el Servicio de Directorio LDAP. De esta forma antes de que un usuario pueda tener acceso a la red, debe realizar el proceso respectivo de introducir su login y password, evitando que usuarios no autorizados (externos) puedan introducir u obtener tráfico de la red libremente.

- ✓ *Implementación de Port Security:*

Una vez estructurada la red LAN, totalmente conmutada, se puede implementar la característica de Port Security, en la cual se le configura a cada puerto del switch qué dirección o direcciones MAC debe permitir y cualquier intento de suplantación de la dirección física será impedido. Esto conlleva a una reconfiguración por parte de los administradores y operadores de la red cada vez que se deba llevar a cabo un cambio en la ubicación de un equipo o la introducción de uno nuevo.

- ✓ *Sistemas de Detección de Intrusos:*

Se propone la introducción de un equipo que implemente un Sistema de Detección de Intrusos como *Snort* en el borde de cada subred, como se muestra en la figura 6.7. Este equipo deberá estar conectado a un puerto del switch configurado como *Mirror Port*, para que el Sistema de Detección de Intrusos tenga acceso a todo el tráfico intercambiado por el Switch. A éstos IDS deben configurárseles Modos de Alerta Full y Modos de Alarma por Socket en el cual se mandaría la información a una aplicación determinada de la cual debe estar pendiente todo el tiempo el administrador, y el Modo de Alarma SMB, que envía mensajes de notificación tipo Windows. Cada IDS debe mantenerse diariamente actualizado con los últimos filtros para la prevención de nuevas amenazas.

- ✓ *Protección del enlace de Telecom con un Firewall PIX 515E*

En este momento el enlace con el proveedor Telecom se encuentra protegido por un equipo corriendo el Firewall por software IPTables; a pesar de que éste a dado buenos resultados, se propone la adquisición de otro Firewall PIX 515E para su implementación en este enlace, ya que es un equipo mucho más robusto y provee mayor número de características no solo en el filtrado de paquetes sino tambien en la inspección de estado completo y soporte para mecanismos de seguridad a nivel de aplicación, como por ejemplo

filtrado de javascript, uso de certificados digitales, controles ActiveX, entre otras, que sirven para complementar la seguridad perimetral. Además la implementación de un nuevo Firewall PIX ofrece un nivel de redundancia alto, ya que cuenta con un puerto serial por donde se puede conectar a otro Firewall PIX, en este caso al instalado para proteger el enlace con Orbitel y en el caso de que alguno llegue a fallar, el otro toma su configuración y de esta forma, no dejaría parte de la red desprotegida.

Estos mecanismos adicionales aumentan la robustez del Sistema de Seguridad de la Red de Datos de la Universidad del Cauca y proporcionan mayor disponibilidad, confidencialidad, autenticación e integridad a los usuarios de la red.

Dentro de las principales características del switch Catalyst 2950 que lo hace apropiado para su uso en toda la red, se encuentran:

- Soporte para implementar VLANs privadas, lo que provee seguridad y aislamiento entre puertos, asegurando que el tráfico de información viaje directamente de su punto de entrada a un punto de salida específico a través de una trayectoria virtual y no pueda ser dirigida a un puerto diferente.
- Soporte para el estándar 802.1x que permite a los usuarios ser autenticados dependiendo del puerto de la LAN por el cual están accesando, lo cual es una ventaja muy grande para los clientes que tienen un gran número de usuarios accediendo a la red.
- Soporte para el Estándar 802.1x con Port Security (Seguridad basada en puertos), mediante el cual es posible autenticar el puerto y gestionar el acceso a la red para todas las direcciones MAC; así, solo algunas direcciones MAC definidas son habilitadas para que se puedan conectar a un determinado puerto del switch.
- Soporte para el Estándar 802.1x con VLAN Assignment, que permite una asignación dinámica de VLANs para un usuario respectivo sin importar donde se realice a cabo la autenticación (el usuario pertenecerá a la mismas VLAN sin importar desde que lugar se conecte a la red).
- Soporte SSHv2, que provee seguridad a nivel de red encriptando el tráfico de los administradores durante las sesiones Telnet.
- MAC Address Notification, permite a los administradores de la red recibir notificaciones cuando nuevos usuarios se han adicionado o han sido removidos de la red.
- Seguridad Multinivel en el acceso por consola, previene que usuarios no autorizados alteren la configuración del Switch.
- Autenticación TACACS+ y RADIUS que habilita control centralizado del switch y restringe que usuarios no autorizados alteren su configuración. (TACACS+- Terminal Access Controller Access Control System- es un protocolo muy nuevo de Autenticación que permite a un Servidor de Acceso Remoto comunicarse con un Servidor de Autenticación como RADIUS para determinar si un usuario tiene o no medio de acceso a la red).
- Soporte a Sistemas de Detección de Intrusos (IDSs) para monitorear, rechazar y realizar reportes de violaciones a la seguridad de la red.
- Monitoreo y control con SNMPv3 (non-crypto) de dispositivos de red, gestión de configuraciones, colección de estadísticas, desempeño, y seguridad.

- Software Asistente de Seguridad de Red de Cisco, que provee facilidades para gestionar características de seguridad para restringir el acceso de usuarios a un servidor, a una porción de la red o el acceso total a la red.
- Soporte para el software CiscoWorks, que provee flexibilidad para la gestión de la red por medio de una interface de gestión común para los switches y routers Cisco.

El switch Cisco Catalyst 2950 tiene un costo aproximado de US$800. Si es posible, se recomienda que todos los switches de la red sean Cisco de este tipo, ya que tienen una ventaja y es que con la herramienta *CiscoWorks* es posible configurarlos y gestionarlos remotamente, lo que ayudaría en este caso en el que el trabajo de configuración es arduo debido a que deben configurarse tanto los switches de borde como los intermedios o de distribución. Como se puede observar, esta implementación es un poco laboriosa debido al seguimiento que debe hacerse para la configuración de los switches respectivos en las conexiones con cada cliente, pero es una buena solución para evitar que usuarios no autorizados tengan acceso a los servidores Privados.

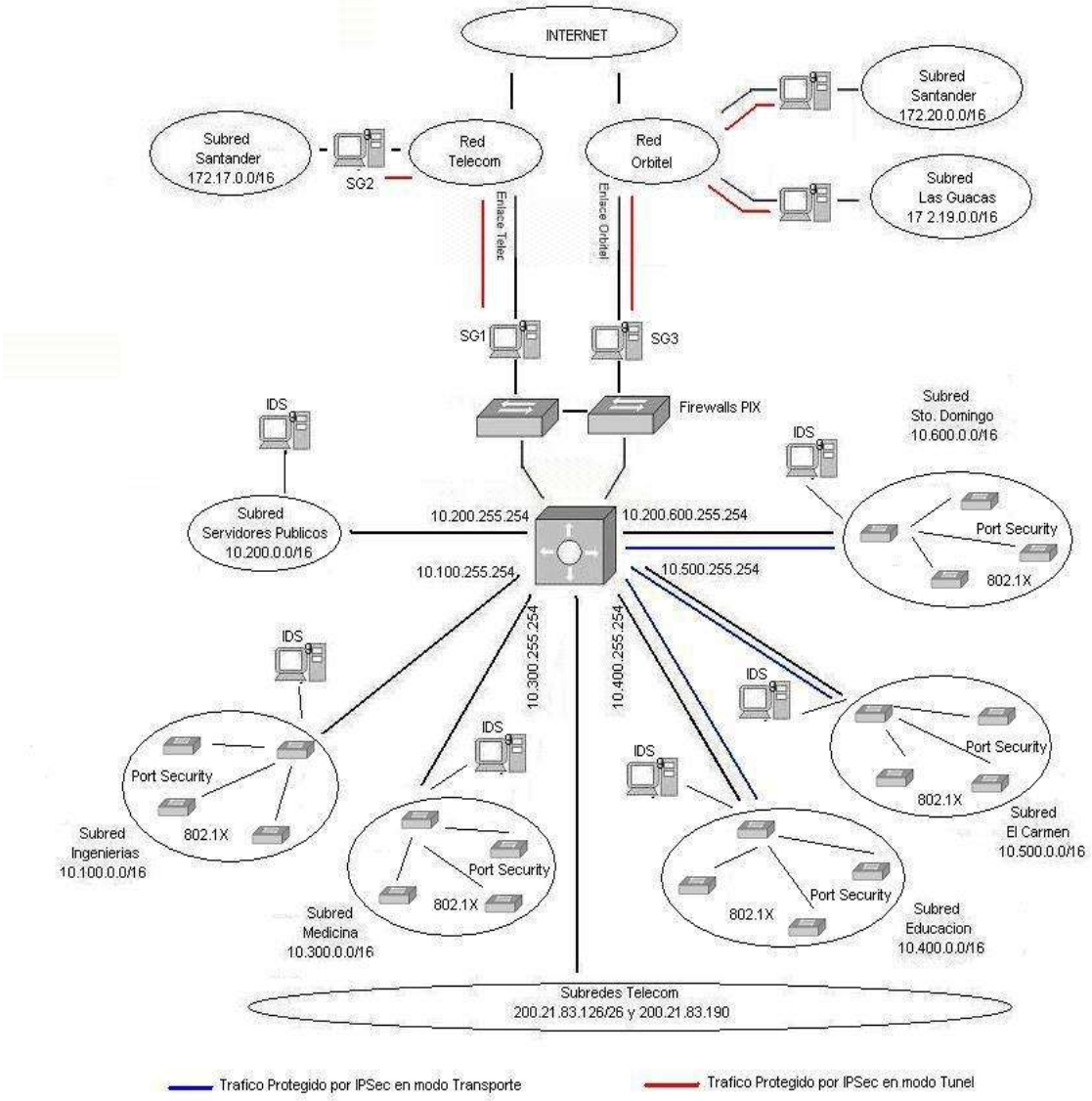


Figura 6.7. Propuesta de seguridad Integrada.

También podría pensarse que para tener una arquitectura de red integrada, una buena opción sería tener instalado protocolo IPSec en todos los terminales de la red lo cual convertiría a la red de datos en una red completamente blindada a nivel de red. No se recomienda esta migración puesto que se considera inviable por las siguientes razones:

- IPSec fue diseñado para proteger tráfico que requiere un alto nivel de seguridad y para proteger los niveles superiores de la pila TCP/IP. En la Universidad del Cauca se ofrecen servicios que tienen protecciones a nivel de aplicación como por ejemplo servicio Web seguro, shell seguro, entre otros, los cuales protegen los datos de los principales servicios a los que acceden los

usuarios de la red ofreciendo un nivel aceptable de seguridad. IPSec no se considera imprescindible para incrementar el nivel de seguridad que existe en la mayoría de servicios que se prestan pero sí en los más sensibles.

- La implementación de IPSec en todos los terminales de la red, se convertiría en un trabajo muy laborioso ya que se requiere la configuración de cada terminal; además se debe escoger el método de autenticación que se va a utilizar, el cual puede ser: llaves pre-compartidas, firmas RSA o certificados digitales. El primero es el más fácil de implantar pero el menos inseguro sobre todo por el tamaño de la red universitaria. El segundo es más seguro pero trae consigo problemas en la gestión y creación de las llaves por el número de terminales. El tercero requiere la implementación previa de una autoridad de certificación para la expedición de certificados digitales.

- La implementación de IPSec a nivel global traería consigo una un gran decremento en el rendimiento de la red debido a la implementación de seguridad en servicios masivos de red que no requieren un gran nivel de seguridad pero si requieren alto rendimiento por la cantidad de usuarios que acceden a ellos.

La adquisición de nuevos equipos para llevar a cabo esta propuesta es grande debido la gran cantidad de concentradores y switchs que no soportan las características de seguridad planteadas y se encuentran en el borde de la red. La Universidad del Cauca cuenta en este momento con un switch de núcleo Cisco Catalyst 4507, 5 switchs de distribución Cisco Catalyst 3750 ubicados en los sectores de Santo Domingo, Educación, Ingenierías y uno para backup; 2 switch Cisco Catalyst 2950 ubicados en el sector de Educación. El resto de Equipos se detalla en las tablas 6.1 y 6.2, lo que da un total de 89 de equipos que sería necesario reemplazar, y para tener una red homogénea se recomienda el reemplazo de todos estos equipos por el switch Cisco Catalyst 2950. Por lo tanto se necesitarían un total de 89 equipos de esta serie, además de los 6 equipos PC que servirán como gateways de seguridad para interconectar las sedes remotas.

Tabla 6.1 Equipos Gestionables

EQUIPOS GESTIONABLES			
CANTIDAD	**EQUIPO**	**REFERENCIA**	**TOTAL X MARCA**
9	NORTEL	BAYSTACK350-24P	21
6	"	BAYSTACK150-24P	
2	"	BAYSTACK28200	
1	"	ACELAR1200	
1	"	BAYSTACK302F	
1	"	BAYSTACK450	
1	"	BAYSTACK15124P	
4	3COM	PSHUB5024P	51
5	"	PSHUB4012P	
4	"	3300MX	
2	"	PSHUBDUAL500	
35	"	PSHUB4024P	

Tabla 6.2 Equipos No Gestionables

EQUIPOS NO GESTIONABLES			
CANTIDAD	**EQUIPO**	**REFERENCIA**	**TOTAL X MARCA**
1	PLANET	DH2400	5
2	"	DH160116 P	
1	"	DH16-02	
1	"	DH2401	
1	SURCCOM	32 PTOS	4
2	"	16 PTOS	
1	"	8 PTOS	
2	TIGERSTACK	3328T24P	2
3	DLINK	DLINK24 PTOS	3
2	ACME	8 PTOS	3
1	"	----------	
1	ENCORE	16 PTOS	1

- *Ventajas de la Propuesta 2.*

La propuesta anterior tiene las siguientes ventajas:

- Satisface muchas necesidades de seguridad en cuanto a autenticación y cifrado a nivel de red en conexiones de alta sensibilidad para la Universidad.
- Divide la red de la Universidad del Cauca en subredes IP lo cual trae múltiples beneficios en cuanto a seguridad y rendimiento se refiere.
- Se interconectan de forma segura las sedes remotas con las que cuenta la Universidad del Cauca.
- Cuenta con mecanismos de monitorización de la red, en búsqueda de comportamientos extraños que puedan poner en riesgo la información.
- Se implementan mecanismos para la prevención de la mayoría de los ataques que se pueden llevar a cabo en la red, no solamente en los sectores más sensibles sino en el resto de la Red de Datos de la Universidad del Cauca.
- Restringe el acceso al medio solo a los usuarios que pertenezcan a la institución universitaria.

- *Desventajas de la Propuesta 2.*

- Tiene un costo elevado, debido a la cantidad de equipos y a la mano de obra necesaria para llevarla a cabo.
- No se implementan mecanismos de autenticación y cifrado de los datos extremo extremo para el protocolo IP en todos los equipos.
- Requiere de mucho tiempo para llevar a cabo su implementación, no porque sea muy compleja, sino porque hay que realizarla en muchos lugares y equipos. Además esta propuesta se compone de varios mecanismos trabajando simultáneamente, por lo que hay que tener mucho cuidado de que un mecanismo no interfiera con otro.

6.2.5 Recomendación y Justificación de la Propuesta más Apropiada para su Implementación en la Red de Datos de la Universidad del Cauca.

Para la escogencia de la propuesta más acertada se deben tener en cuenta los aspectos tanto técnicos como económicos. Sin embargo se han tenido en cuenta en mayor grado los aspectos técnicos, ya que por el trabajo llevado hasta el momento se ha concluido que las inversiones en seguridad que se realizan en una red tienen un gran factor costo/beneficio aunque este no se perciba inmediatamente. Por ello se concluye que la propuesta que se ajusta en mayor medida a las necesidades de la red universitaria es la propuesta 2, *Propuesta de Seguridad Integrada*, ya que contrarresta la mayoría de vulnerabilidades que se presentan en este momento en la Red de Datos de la Universidad del Cauca, protege de manera confiable la información sensible que se transporta sobre la red, y además implementan mecanismos que logran seguridad completa en todos los sectores de la red y en las áreas de mayor importancia. De esta forma y contando con los mecanismos de seguridad a niveles superiores con que ya cuenta la Red de Datos es posible que los usuarios se sientan tranquilos al manejar su información y de igual forma, personas ajenas a la red sean incapaces de acceder a ella sin la debida autorización. De igual manera los administradores de la Red de Datos tendrán herramientas para ejercer un mayor control sobre el comportamiento de los usuarios y los equipos de la red y podrán realizar un monitoreo constante que los ayudará a mejorar constantemente los aspectos en los que se encuentren debilidades.

6.2.6 Presupuesto

6.2.6.1 Presupuesto de la Propuesta de Seguridad basada en Subredes e IPSec

Tabla 6.3 Presupuesto para la Propuesta 1

RECURSOS HUMANOS		
ITEM/PERSONAL	**DIRECTOR DEL PROYECTO**	**REALIZADOR DEL PROYECTO**
Nº de horas por semana	40	40
Nº de Semanas	12	12
Nº Total de Horas	480	480
Puntos/hora	2.5	1.5
Nº de Puntos	1200	720
Costo del Punto	$6661	$6661
Costo por persona	$7`993.200	$4'795.920
Nº de Personas	2	2
Costo	15`986.400	$9'591.840
Total	**$25`578.240**	

RECURSOS HARDWARE			
DESCRIPCIÓN	**CANTIDAD**	**COSTO**	**COSTO TOTAL**
Equipos Dell optiplex GX280	5	$2'480.000	12`400.000
Total	**12`400.000**		

RECURSOS SOFTWARE			
DESCRIPCIÓN	**CANTIDAD**	**COSTO**	**COSTO TOTAL**

Linux Debian Sarge 3.1	5	$0	$0
Openswan	5	$0	$0
Total	$0		
AUI (20%)	**7`595.648**		
COSTO TOTAL DE LA PROPUESTA 1	**$45`573.888**		

6.2.6.1 Presupuesto de la Propuesta de Seguridad Integrada

Tabla 6.4 Presupuesto para la Propuesta 2

RECURSOS HUMANOS			
ITEM/PERSONAL	**DIRECTOR DEL PROYECTO**		**REALIZADOR DEL PROYECTO**
Nº de horas por semana	40		40
Nº de Semanas	24		24
Nº Total de Horas	960		960
Puntos/hora	2.5		1.5
Nº de Puntos	2400		1440
Costo del Punto	$6661		$6661
Costo por persona	$15`986.400		$9`591.840
Nº de Personas	2		4
Costo	31`972.800		$38`367.360
Total	**$70`340.160**		
RECURSOS HARDWARE			
DESCRIPCIÓN	**CANTIDAD**	**COSTO**	**COSTO TOTAL**
Equipos Dell optiplex GX280	11	$2'480.000	$27`280.000
Switch Cisco Catalyst 2950	89	$1`680.000	$149`520.000
Firewall PIX 515E	1	$5'250.000	$5`250.000
Total	**182`050.000**		
RECURSOS SOFTWARE			
DESCRIPCIÓN	**CANTIDAD**	**COSTO**	**COSTO TOTAL**
Linux Debian Sarge 3.1	11	$0	$0
Openswan	5	$0	$0
Snort	6	$0	$0
Total	$0		
AUI (20%)	**54`314.768**		
COSTO TOTAL DE LA PROPUESTA 2	**$306`704.928**		

6.2.7 Auditoría y Evaluación

Antes de hablar de auditoría y evaluación, es importante tener en cuenta ciertas etapas intermedias que deben llevarse a cabo antes de la implementación de la propuesta de Seguridad que ayudarán al cumplimiento de las Políticas de Seguridad planteadas; primero, dentro de la etapa de **Revisión**, debe llevarse a cabo una *evaluación independiente de las Políticas*; una vez la documentación de las políticas ha sido creada y se ha iniciado la coordinación inicial, éstas deben ser remitidas a un grupo de personas para su evaluación antes de su aprobación final. El beneficio de esto es que los evaluadores podrán ver las Políticas desde una perspectiva diferente o más vasta que las personas que las redactaron; de esta forma es posible aumentar la credibilidad de las Políticas gracias a la información recibida de los diferentes especialistas del grupo de revisión. De esta forma los creadores de las Políticas pueden recopilar todos los comentarios y recomendaciones de los evaluadores para realizar cambios en las Políticas y efectuar todos los ajustes y las revisiones necesarias para obtener una versión final de las Políticas, lista para la aprobación por parte de las directivas.

En segundo lugar, y dentro de la etapa de **Aprobación**, está precisamente la *aprobación de las Políticas por parte de las Directivas*; es prácticamente el paso final en la fase de desarrollo de las Políticas. El objetivo de esto es obtener el apoyo de la administración de la Universidad, a través de la firma de las personas con esa autoridad. La aprobación es el punto de partida para iniciar la implementación de las Políticas.

Dentro de la etapa de **Comunicación y Concientización**, es muy importante *Difundir las Políticas*; las políticas deben ser inicialmente difundidas a los miembros de la comunidad universitaria y a quienes sean afectados directamente por ellas (contratistas, proveedores, usuarios de ciertos servicios, etc). Debe planificarse muy bien esta etapa con el fin de determinar los recursos necesarios y el enfoque que debe ser seguido para mejorar la visibilidad de las Políticas. Así mismo, se debe realizar una etapa de *concientización de las Políticas* para facilitar su cumplimiento; deben determinarse los métodos más efectivos para cada grupo de audiencia (reuniones informativas, cursos de entrenamiento, mensajes de correo, etc) y de igual forma la difusión de material de concientización (presentaciones, afiches, circulares, etc).

Dentro de la etapa de **Cumplimiento**, se incluyen todas las actividades relacionadas con la ejecución de las Políticas; implica trabajar con otras personas de la Universidad, vice-rectores, decanos, jefes de departamento, y los jefes de otras dependencias para interpretar cuál es la mejor forma de implementar las Políticas en diferentes situaciones y oficinas; debe asegurarse de que las Políticas son entendidas por aquellos que van a implementarlas, monitorearlas, hacerles el debido seguimiento, reportar regularmente su cumplimiento y medir el impacto inmediato de las Políticas en las actividades Operativas de la Universidad. Así, es posible comenzar a realizar la *implementación de la Propuesta de Seguridad* y los diferentes mecanismos necesarios para poner en práctica lo definido en las Políticas, por parte de los administradores y monitores de la Red de Datos.

Después de esto es posible hablar de llevar a cabo el proceso de **Auditoría**; ésta es una etapa de monitoreo realizada para seguir y reportar la efectividad de los esfuerzos en el cumplimiento de las Políticas y en la implementación de la Propuesta de Seguridad; casi todos los procesos de la red pueden ser monitorizados; la idea de realizar Auditorías periódicas al sistema de Seguridad es mantener un seguimiento de la eficiencia y la adecuación de la implementación realizada a la infraestructura de la Universidad y determinar si se están cumpliendo con los parámetros definidos a la hora de la identificación y análisis que se llevó a cabo antes del diseño de las Políticas de Seguridad. Una buena Auditoría comprende la revisión y la evaluación independiente y objetiva, si es posible por parte de personas externas y teóricamente competentes del entorno de la Universidad, abarcando todo las áreas relacionadas con la seguridad de la red, la tecnología y procedimientos, su idoneidad y el cumplimiento de éstos, de los objetivos fijados, los contratos y las normas legales aplicables, el grado de satisfacción de usuarios y directivos, los controles existentes y el análisis de riesgos

La auditoría consiste en contar con los mecanismos para poder determinar qué es lo que sucede en el sistema, qué es lo que hace cada uno y cuando lo hace. De la misma forma se puede definir un proceso de Control, donde se contraste el resultado final obtenido contra el deseado a fin de incorporar las correcciones necesarias para alcanzarlo, o verificar la efectividad de lo obtenido. Existe dos mecanismos básicos para realizar una auditoría: los *logs de eventos*, donde es posible encontrar el registro de todas las actividades realizadas en un equipo y los *Sistemas de Detección de Intrusos* que, bien administrados, permiten monitorear el comportamiento del tráfico de determinada porción de la red que supervisan. Complementariamente, se obtiene información importante de la observación de administrativos, docentes, estudiantes y demás empleados, y de las revisiones y análisis de los reportes de contravenciones y de las actividades realizadas en respuesta a incidentes. Una auditoría incluye actividades continuas para monitorear el cumplimiento o no de las Políticas a través de métodos formales e informales y el reporte de las deficiencias encontradas a las personas encargadas. Es posible que debido a problemas de coordinación, falta de personal, de equipos y otros requerimientos operacionales, no todas las Políticas puedan ser cumplidas de la manera que se pensó en el comienzo, o de alguna forma la Propuesta de Seguridad deba sufrir algunos cambios con respecto a lo planteado; por esta razón, cuando el caso lo amerite, es probable que se requieran *excepciones* a las Políticas para permitir a ciertas personas u oficinas el no cumplimiento de alguna de las Políticas. Debe establecerse un proceso para garantizar que las solicitudes de excepciones son registradas, seguidas, evaluadas, enviadas para aprobación o desaprobación, documentadas y vigiladas a través de un periodo de tiempo establecido para la excepción. El proceso también debe permitir excepciones permanentes a determinadas Políticas, al igual que la no aplicación temporal por circunstancias de corta duración.

Con esta información recolectada, es posible realizar un proceso de **Evaluación**, en la cual se incluyen las respuestas de la administración a actos u omisiones y a deficiencias detectadas en la auditoría, que tengan como resultado contravenciones de las Políticas, con el fin de prevenir que sigan ocurriendo; esto significa que una vez una deficiencia u contravención sea identificada, se debe determinar una acción correctiva y aplicarla a los procesos (revisión del proceso y mejoramiento), a la tecnología (actualizaciones) y a las personas (acciones disciplinarias) involucradas, con el fin de reducir la probabilidad de que vuelva a ocurrir. Es muy importante incluir información sobre las acciones correctivas adelantadas para garantizar el cumplimiento de la etapa de concientización.

La evaluación permite también garantizar la vigencia y la integridad de las Políticas; esto incluye hacer seguimiento a las tendencias de cambios (cambios en la tecnología, en los procesos, en la arquitectura de red, en las personas, en la organización, en el enfoque del manejo de la información, etc) que pueden afectar una Política. Así, se deben recomendar y coordinar modificaciones resultado de estos cambios, documentándolos en la política y registrando las actividades de cambio. De esta forma es necesario revisar todas las etapas anteriores, por lo que el ciclo se repite.

En el caso de que una política haya cumplido con su finalidad y ya no sea necesaria (por ejemplo cuando se realiza un cambio en la tecnología a la cual aplicaba o se creó una nueva política que la reemplaza), entonces debe ser retirada; el retiro corresponde a la *eliminación del ciclo de vida* de una política del inventario de las Políticas activas para evitar confusión, archivarla para futuras referencias y documentar la información sobre la decisión de retirarla (justificación, quién autorizó, fecha, etc).

De esta forma es importante que se implemente un mecanismo de auditoría y a su vez de evaluación de los resultados de la información obtenida en esta, para que así sea posible detectar aquellos puntos débiles que no se han tenido en cuenta al plantear las Políticas de Seguridad y que deben mejorarse para cumplir con las necesidades de protección de la información y de los recursos. Todas las etapas planteadas en este capítulo para el ciclo de vida de las Políticas de Seguridad son muy importantes y no deben omitirse; no importa como se agrupen, tampoco si son abreviadas por necesidad de inmediatez, pero cada etapa debe ser realizada. Y no solo se requiere que todas las etapas sean realizadas, sino tener en cuenta de que algunas de ellas deben ser ejecutadas de manera cíclica, como se vio en la figura 6.1.

Resumen

En este capítulo se plantearon algunas Políticas de Seguridad que sirvan de base para implementar unas políticas robustas para la utilización de los recursos de la Red de Datos de la Universidad del Cauca. Además, se plantearon 2 propuestas para la implementación de Seguridad a nivel de red y se escogió la propuesta que más le conviene a la Red teniendo en cuenta aspectos técnicos más que económicos. A continuación, se presentan las conclusiones que quedan del desarrollo del proyecto y algunas recomendaciones y trabajos futuros que se pueden llevar a cabo teniendo como base este documento.

CONCLUSIONES

Con el desarrollo del presente trabajo de grado se puede concluir lo siguiente:

- Las deficiencias del protocolo TCP/IP han llevado a los atacantes de redes a idear diversos mecanismos para vulnerar las redes basadas en dicho protocolo y, aunque todas las falencias parecen haber sido descubiertas, no se debe descuidar la aparición de nuevas vulnerabilidades.

- La protección de los datos se realiza con diferentes mecanismos a los niveles más altos de la pila TCP/IP; IPSec brinda protección por autenticación y cifrado de los datos a nivel de red y por ende dando la misma protección a los niveles de transporte y aplicación. Por todo esto IPSec ofrece el mayor nivel de seguridad que se puede implementar sobre una red.

- La aplicación de Seguridad es indispensable en las redes públicas. IPSec tiene enfoque diferente a otros protocolos de seguridad más populares como SSH y SSL, que funcionan en la capa de transporte y están ligados con una aplicación particular. Con IPSec pueden establecerse comunicaciones seguras extremo a extremo, de forma flexible y bajo diversas configuraciones, sin importar la aplicación del nivel de usuario.

- Una VPN no es solamente una red virtual (conmutada), es además privada, no representa una solución completa, y no brinda protección total a una red; una VPN protege únicamente el canal por donde transita la información de un extremo a otro de la VPN. Si uno de los extremos de la VPN o de una conexión segura host-to-host se compromete, se pierde la protección. Más aún, una VPN o conexión segura no impide totalmente las intrusiones a un equipo, es decir, el hecho que se apliquen VPNs o conexiones seguras no sustituye el esfuerzo que debe hacerse por implementar mecanismos de seguridad en sistemas.

- IPSec representa una muy buena solución para ataques tipo Spoofing. IPSec cifra y autentica paquetes IP y como se pudo constatar, se protege totalmente el contenido de la carga útil pero los encabezados quedan visibles, pudiendo representar información útil para los intrusos.

- Los mecanismos de seguridad que actualmente se implementan en la red universitaria están orientados a la protección de la información a nivel perimetral en general, más no a la protección de las amenazas internas, ni de la información intercambiada entre las diferentes sedes.

- La Red de Datos de la Universidad del Cauca cuenta con una excelente infraestructura tanto a nivel de red como a nivel de servicios ya que posee un importante número de equipos de red, servidores, estaciones de trabajo y un gran despliegue de cableado a lo largo del campus universitario. Sin embargo, la protección que se le brinda a los datos y servicios es muy poca debido a la falta de una arquitectura de seguridad a nivel de red integral.

- La migración de IPv4 hacia IPv6 permitirá que la Red de Datos de la Universidad del Cauca esté preparada para la nueva generación de Internet, con la cual se podrán obtener mayores beneficios, prestar nuevos y mejores servicios y superar muchas de las deficiencias del protocolo de Internet actual, sobre todo las deficiencias de seguridad. Ya que los protocolos de seguridad que implementa IPv6 se pueden transportar a IPv4, una posible migración a nivel de seguridad no es muy traumática si primero hay una familiarización en la versión 4.

- Los Protocolos de Seguridad de IPv6 implementados sobre redes IPv4 permiten proteger la información de los diferentes ataques a los que está expuesta a través de la red pública Internet y dentro de la Red Interna, pero de la misma forma disminuye considerablemente el rendimiento de una comunicación debido al aumento de los encabezados y al procesamiento que se realiza sobre los paquetes.

- Para llevar a cabo la implementación de una propuesta de seguridad a nivel de red, es necesario establecer diferentes fases de desarrollo de acuerdo a las capacidades económicas y administrativas de la Universidad del Cauca. Para obtener un buen resultado que satisfaga a toda la comunidad, deben tenerse en cuenta los puntos de vista financiero, administrativo, técnico y por supuesto la opinión de los usuarios de la red.

- Las políticas de seguridad son la base de una arquitectura de seguridad sólida y robusta. Para el planteamiento de dichas políticas deben dejarse a un lado los conceptos técnicos para concentrarse en los procesos administrativos que se quieren proteger.

- Es importante llevar a cabo un proceso de concientización de la comunidad Universitaria acerca de la importancia de los recursos de la Red, y del cumplimiento de las Políticas de Seguridad planteadas.

RECOMENDACIONES

- Reforzar los mecanismos de seguridad perimetral e implementar mecanismos de protección interna basados en los conceptos de prevención y monitoreo de posibles amenazas contra la información, partiendo de la premisa de que la mayor parte de ataques contra una red se originan desde el interior de la misma.

- La seguridad es un aspecto que debe tenerse en cuenta en todos los procesos informáticos y a nivel de red. Por este motivo se recomienda la creación de un área especializada en seguridad que sirva como consultora ante cualquier inquietud sobre seguridad informática y seguridad a nivel de red. Además que dicha área desarrolle proyectos encaminados a descubrir falencias en la Red de Datos y darles solución. Por último el área de seguridad deberá permanecer actualizada sobre mecanismos de protección y problemas de seguridad los cuales surgen frecuentemente.

- No descuidar los posibles riesgos de seguridad que se puedan presentar a nivel de red en la red universitaria por complejos que parezcan, ya que el hecho de que sean complejos no implica que no se pueda realizar.

- El protocolo IPSec está en etapa de exploración y comprensión, es un estándar de la IETF en proceso de re-evaluación sobre la cual se han sometido propuestas de simplificación a nivel de drafts; hay aún mucho trabajo por hacer sobre el análisis de vulnerabilidades de la arquitectura de IPSec y sobre todo del protocolo para manejo dinámico de llaves IKE donde la propuesta se está gestando con el nuevo protocolo *son-of-IKE* o *IKE versión 2*.

- Se recomienda realizar un estudio de las diferentes herramientas que permiten la implementación de Opportunistic Encryption, para facilitar la configuración de las Asociaciones y Políticas de Seguridad en varias comunicaciones, lo cual facilitaría considerablemente la configuración de las VPNs.

- Existen diferentes iniciativas de instrumentación de IPSec en diversas plataformas para ampliar su uso; hay aún mucho trabajo de desarrollo por hacer con respecto a la integración de nuevos protocolos en las redes de nueva generación como Multicast, MultiProtocol Levels Switching (MPLS), PKI, Multicast Key Management Protocol (MKMP), entre otros.

- A la fecha, el direccionamiento usado en la red de datos de la Universidad del Cauca es estático ya que la dirección de un terminal no cambia frecuentemente. Este tipo de direccionamiento es ideal para el funcionamiento de IPSec ya que las direcciones de origen y destino son parámetros estáticos para la configuración de las aplicaciones que implementan IPSec. Por este motivo se recomienda el estudio del funcionamiento de IPSec sobre un entorno de direccionamiento dinámico, donde las direcciones de los terminales cambian frecuentemente, y la extensión de la Seguridad a nivel de Red en general para Redes Móviles.

- Debido a que el protocolo AH protege la cabecera IP incluyendo las partes inmutables de dicha cabecera como las direcciones IP, el protocolo AH no permite NAT. La extensión IPSec NAT Transversal implementa métodos que evitan esta restricción. Por este motivo se recomienda el uso de NAT Transversal en vez del NAT simple utilizado hasta la fecha.

BIBLIOGRAFIA

- ATKINSON, Randall. **"IP Authenticaction Header"**. [Request for Comments 1826]. 1995. [Documento en línea] http://www.ietf.org

- ATKINSON, Randall. **"IP Encapsulating Security Payload (ESP)"**. [Request for Comments 1827]. 1995. [Documento en línea] http://www.ietf.org

- BORGHELLO, Cristian. **"Políticas de Seguridad".** 2001. [Documento en línea] http://www.seguinfo.com.ar/tesis/cap9.pdf http://www.seguinfo.com.ar/tesis/tesis.htm

- BRADEN, Bob. CLARK, David. CROCKER, Steve. HUITEMA, Christian. **"Security in the Internet Architecture",** [Request for Comments 1636]. 1994. [Documento en línea] http://www.ietf.org

- HERMIDA QUINTERO, Victor Alberto. RODRIGUEZ ORTIZ, William James. **"Propuesta de Migración de la Red de Datos de la Universidad del Cauca hacia la tecnología IPv6 sobre Redes Ethernet de Alta Velocidad"**. Universidad del Cauca. 2005.

- KARN, Phil. METZGER, Rerry. SIMPSON, William Allen. **"The ESP DES-CBC Transform".** [Request for Comments 1829]. 1995. [Documento en línea] http://www.ietf.org

- KENT, Stephen. ATKINSON, Randall. **"Security Architecture for Internet Protocol"**. [Request for Comments 2401]. 1995. [Documento en linea] http://www.ietf.org

- METZGER, Rerry. SIMPSON, William Allen. **"IP Authenticaction Using Keyed MD5".** [Request for Comments 1828]. 1995. [Documento en línea] http://www.ietf.org

- NORTHCUTT, Stephen. NOVAK, Judy. **"Detección de Intrusos, Guía Avanzada, 2ª edición".** Prentice Hall. 2001.

- OPPENHEIMER, Priscilla. **"Top-Down Network Design Second Edition"**. Cisco Press. 2004.

- PAZ CABRERA, Diego Alejandro. URBANO RAMOS, Liliana Andrea. **"Diseño e Implementación de un laboratorio Internet Desde la perspectiva de Enrutamiento, Seguridad y QoS".** Universidad del Cauca. 2003.

- SILES PELAEZ, Raúl. **"Análisis de Seguridad de la familia de protocolos TCP/IP y sus Servicios Asociados"**. Edición 1. 2002. [Documento en línea] http://www.rediris.es/cert/doc/segtcpip/Seguridad_en_TCPIP_Ed1.pdf

- Sitio con tutoriales sobre IPSec: http://www.ipsec-howto.org/

- Sitio oficial del proyecto USAGI: http://www.linux-ipv6.org

- Sitio oficial del proyecto Kame: http://www.kame.net

- Sitio oficial del proyecto FreeS/WAN: http://www.freeswan.org/

- Sitio oficial del proyecto Openswan: http://www.openswan.org/

- Soporte IPv6 en Windows 2000. Disponible online en : http://msdn.microsoft.com/downloads/sdks/platform/download.asp

- VILLALON HUERTA, Antonio. **"Seguridad en UNIX y Redes".** 2002. [Documento en línea] http://andercheran.upv.es/~toni/personal/unixsec.pdf

ACRÓNIMOS

A

ACL, Access Control List

AH, Authentication Header

AP, Access Point

AS, Association Security

ARP, Address Resolution Protocol

ATM, Asynchronous Transfer Mode

B

BGP, Border Gateway Protocol

C

CA, Certification Authorities

CBC, Cipher Block Chaining

CHAP, Challenge-Handshake Authentication Protocol

CRC, Cyclic Redundancy Check

CSMA/CD, Carrier Sense Multiple Access/Collision Detection

D

DEA, Data Encryption Algorithm

DES, Data Encryption Standard

DESX, DESeXtension

DHCP, Dynamic Host Configuration Protocol

DNS, Domain Name Server

DOI, Domain of Interpretation

DoS, Denial of Service

DSS, Digital Signature Standard

E

ECB, Electronic Code Block

ECC, Elliptic Curve Cryptosystem

EHAS, Enlace Hispano-Americano de Salud

ESP, IP Encapsulating Security Payload

ESSID, Extended Service Set Identifier

F

FTP, File Transfer Protocol

G

GRE, Generic Routing Encapsulation

H

HDSL, High-rate Digital Suscriber Line

HMAC, Hashed Message Authentication Code

HTTP, Hypertext Transfer Protocol

I

IAB, Internet Architecture Board

IANA, Internet Assigned Number Authority

ICMP, Internet Control Message Protocol

ICV, Integrity Check Value

IDEA, International Data Encryption Algorithm

IDS, Intrusion Detection System

IEEE, Institute of Electrical & Electronics Engineers

IETF, Internet Engineering Task Force

IKE, Internet Key Exchange

IMAP, Internet Message Access Protocol

IP, Internet Protocol

IPSec, IP Security

IPv4, IP Versión 4

IPv6, IP Versión 6

ISAKMP, Internet Security Association Key Management Security Association Protocol

ISDN, Integrated Service Digital Network

ISO, Internacional Standard Organization

IV, Initialization Vector

L

L2TP, Layer 2 Tunneling Protocol

LAN, Local Area Network

LDAP, Lighweight Directory Access Protocol

M

MAC, Message Authentication Code

MD5, Message Digest versión 5

MIB, Management Information Base

MPPE, Microsoft Point to Point Encryption

N

NAT, Network Address Translation

NCP, Network Control Protocol

NCSA, Nacional Center for Supercomputing Applications

NFS, Network File System

NIS, Network Information System

NIST, National Standards and Technology Algorithm

NMS, Network Management System

NSA, National Security Agency

O

OSI, Open System Interconnection

P

PAP, Password Authenticaction Protocol

PDU, Protocol Data Unit

PGP, Pretty Good Privacy

PIX, Private Internet Exchange

PKI, Public Key Infrastructure

POP, Post Office Protocol

PPP, Point to Point Protocol

PPTP, Point-to-Point-Tunneling Protocol

PSK, Pre-Shared Keys

R

RAS, Remote Access Server

RFC, Request for Comment

RMON, Remote Monitoring

RPC, Remote Procedure Call

RSA, Rivest, Shamir, Adleman

S

SA, Security Association

SAD, Security Association Database

SET, Secure Electronic Transaction

SHA, Secure Hash versión 1

S-HTTP, Secure Hypertext Transfer Protocol

SMI, Structure of Management Information

S/MIME, Secure/Multipurpose INTERNET Mail Extensions

SMTP Seguro, Simple Mail Transfer Protocol

SNMP, Simple Network Management Protocol

SPD, Security Policy Database

SPI, Security Parameters Index

SSL, Secure Socket Layer

T

TCP, Transport Control Protocol

TLS, Protocolo Transport Layer Security

U

UDP, User Datagram Protocol

USAGI, UniverSAl playGround for Ipv6

UTP, Unshielded Twisted Pair

UUCP, Unix to Unix Copy Protocol

V

VLAN, Virtual Local Area Network

VPN, Virtual Private Network

W

WECA, Wireless Ethernet Compatibility Alliance

WEP, Wired Equivalent Privacy

WiFi, Wireless Fidelity

WLAN, Wireless LAN