ESPE

UNIVERSIDAD DE LAS FUERZAS ARMADAS

INNOVACIÓN PARA LA EXCELENCIA

VICERRECTORADO DE INVESTIGACIÓN Y VINCULACIÓN CON LA COLECTIVIDAD

MAESTRIA EN REDES DE LA INFORMACIÓN Y CONECTIVIDAD

III PROMOCIÓN

TESIS DE GRADO MAESTRIA DE REDES DE LA INFORMACION Y CONECTIVIDAD

TEMA: “FACTIBILIDAD DE IPSEC PARA IPV6 EN LA RED DE LA UNIVERSIDAD POLITÉCNICA SALESIANA, SEDE QUITO”

AUTOR: ING. LÓPEZ LOGACHO, JORGE ENRIQUE

DIRECTOR: ING. OLEAS, JUAN CARLOS

SANGOLQUÍ, ENERO DEL 2014

UNIVERSIDAD DE LAS FUERZAS ARMADAS
MAESTRIA DE REDES DE LA INFORMACION Y CONECTIVIDAD

CERTIFICADO

ING. JUAN CARLOS OLEAS CASTELO — Director

ING. DARWIN LEONIDAS AGUILAR SALAZAR — Oponente

CERTIFICAN

Que el trabajo titulado **"FACTIBILIDAD DE IPSEC PARA IPV6 EN LA RED DE LA UNIVERSIDAD POLITÉCNICA SALESIANA, SEDE QUITO"**, realizado por **LÓPEZ LOGACHO, JORGE ENRIQUE,** ha sido guiado y revisado periódicamente y cumple normas estatuarias establecidas por la ESPE, en el Reglamento de Estudiantes de la Escuela Politécnica del Ejército.

Debido a que cumple con lo planteado en el plan de tesis y de acuerdo a los requerimientos del programa de maestría, se recomiendan su publicación.

El mencionado trabajo consta de un documento empastado y un disco compacto el cual contiene los archivos en formato portátil de Acrobat (pdf). Autorizan a **LÓPEZ LOGACHO, JORGE ENRIQUE** que lo entregue a Ing. Rodrigo Silva .Msc, en su calidad de Coordinador del Programa de Maestría en Redes y Conectividad, tercera Promoción

Sangolquí, Enero del 2014

Ing. Juan Carlos Oleas Castelo. Msc
DIRECTOR

Ing. Darwin Leonidas Aguilar Salazar .Msc.
CODIRECTOR

UNIVERSIDAD DE LAS FUERZAS ARMADAS

MAESTRIA DE REDES DE LA INFORMACION Y CONECTIVIDAD

DECLARACIÓN DE RESPONSABILIDAD

LÓPEZ LOGACHO, JORGE ENRIQUE

DECLARO QUE:

El proyecto de grado denominado **"FACTIBILIDAD DE IPSEC PARA IPV6 EN LA RED DE LA UNIVERSIDAD POLITÉCNICA SALESIANA, SEDE QUITO",** ha sido desarrollado con base a una investigación exhaustiva, respetando derechos intelectuales de terceros, conforme las citas que constan el pie de las páginas correspondiente, cuyas fuentes se incorporan en la bibliografía.

Consecuentemente este trabajo es mi autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance científico del proyecto de grado en mención.

Sangolquí, Enero del 2014.

LÓPEZ LOGACHO, JORGE ENRIQUE

UNIVERSIDAD DE LAS FUERZAS ARMADAS

MAESTRIA DE REDES DE LA INFORMACION Y CONECTIVIDAD

AUTORIZACIÓN

Yo, **LÓPEZ LOGACHO, JORGE ENRIQUE**

Autorizo a la Escuela Politécnica del Ejército la publicación, en la biblioteca virtual de la Institución del trabajo **"FACTIBILIDAD DE IPSEC PARA IPV6 EN LA RED DE LA UNIVERSIDAD POLITÉCNICA SALESIANA, SEDE QUITO"**, cuyo contenido, ideas y criterios son de mi exclusiva responsabilidad y autoría.

Sangolquí, Enero del 2014.

_____

LÓPEZ LOGACHO, JORGE ENRIQUE

DEDICATORIA

Este trabajo está dedicado a Dios, por su infinito amor, a mi padre, por su constante apoyo, a mi madre, por sus consejos y fe en mí, a mis hermanos, por estar a mi lado incondicionalmente.

AGRADECIMIENTOS

Agradezco a Dios por darme la sabiduría y la perseverancia necesarias, a mis padres Jorge y Graciela por su continuo apoyo y confianza en mis capacidades, a mis hermanos Patricio y Raquel, quienes incondicionalmente han ofrecido su total apoyo para emprender y finalizar esta tarea.

Agradezco a mi Director de Tesis, Ing. Juan Carlos Oleas, supo guiarme con sus conocimientos para cumplir el objetivo final de este proyecto de tesis.

Jorge

INDICE DE CONTENIDOS

INDICE DE TABLAS

INDICE DE FIGURAS

RESUMEN

La información es un bien intangible cuya criticidad e importancia para quien la genera y la recibe es de difícil cuantificación, es responsabilidad de los administradores de red ofrecer entonces un escenario de transporte y gestión de datos que ofrezca la seguridad necesaria; durante el proceso de transferencia, procesamiento y almacenamiento de los datos, la información está sujeta a riesgos de ataques por parte de elementos tanto internos como externos a la red, estos ataques se pueden presentar durante la creación de la información, la transferencia , el procesamiento o el almacenamiento de los datos, es decir el riesgo existe a lo largo de todo el proceso. Existen muchos métodos que están destinados a mejorar la seguridad en la red, la mayoría de ellos trabajan en capa aplicación, sin embargo este trabajo analiza la arquitectura de IPSec e investiga la factibilidad de su implementación sobre IPv6 en un escenario que requiere contar con altos niveles de seguridad. Inicialmente se procederá a la descripción del funcionamiento del protocolo IPSec, su arquitectura, los procesos de autenticación y encriptación. Se hará un levantamiento del estado actual de la red de datos en la Institución, el análisis de la topología física actual, se propondrá el esquema de direccionamiento, los requerimientos de infraestructura y planificación de la implementación de IPSec sobre IPv6. Se procederá al diseño lógico y físico de la propuesta de implementación, posteriormente se realizará la simulación de acuerdo a los parámetros establecidos y finalmente se hará un análisis de los resultados.

Palabras clave: UNIVERSIDAD POLITÉCNICA SALESIANA, SEGURIDADES, ENCRIPTACIÓN, IPSEC, IPV6.

ABSTRACT

The requirements that local and extended networks are exposed present have set the need to set a new protocol – group not only in routing but also in security issues, and this need arises with the aim of solving limitations presented in last protocols that haven't been designed to deal with modern challenges in present telecommunications.

Due to this situation, an IPv6 protocol has become necessary to implement in the local network of the Salesian Polytechnic University – Quito, Campus Girón. In addition, it is necessary to increase security specifically in the third – layer level and the main goal of this research is to analyze the possibility for setting IPSec in the network of the University.

An analysis of IPSec architecture will be done at first in order to correctly choose the kind of application in the network. Then, the network will be analyzed in order to visualize the initial situation and see the technical possibility before implementing IPSec as long as deciding on what is going to be protected. Finally, the simulating method will be applied in order to demonstrate that the protocol settings is possible to implement.

KEY WORDS: SALESIAN POLYTHECNIC UNIVERSITY, SECURITY, ENCRIPTATION, IPSEC, IPV6

INTRODUCCION

Los requerimientos actuales a los que están sujetas las redes tanto de área local como de área extendida, han supuesto la necesidad de adoptar un nuevo grupo de protocolos tanto de direccionamiento como de seguridad entre otros, con el fin de solventar las limitaciones que presentan los protocolos anteriores, los que no han sido diseñados para suplir los retos que las comunicaciones actuales presentan, tal es así que a nivel de direccionamiento se ha visto la necesidad de la implementación de IPv6 en la red de área local de la Universidad Politécnica Salesiana, Sede Quito, Campus Girón, adicionalmente aparece la necesidad de incrementar la seguridad, específicamente a nivel de capa tres, por lo que el objetivo de esta investigación es analizar la factibilidad de la implementación de IPSec en la red de la mencionada institución, inicialmente se hará un análisis de la arquitectura de IPSec, con el fin de elegir el tipo de aplicación del mismo en la red, luego se realizará un análisis de estado inicial de la red para determinar la factibilidad técnica de su implementación y elegir puntualmente que es lo que se va a proteger y finalmente se demostrará en base al método de simulación que la configuración del protocolo puede ser realizada en la infraestructura existente.

.

CAPÍTULO I

IPV6

1.1Tendencias globales del protocolo IP.

En el diseño inicial de IPv4 no se consideró la masificación de Internet y el agotamiento del espacio de direcciones, puesto que la creciente proliferación de host conectados a Internet apunta a que el espacio de direcciones públicas de IPv4 está por agotarse. A esto se añade la necesidad de una configuración más sencilla, ya que la mayor parte de las implementaciones actuales de IPv4 deben configurarse manualmente o mediante un protocolo de configuración de direcciones con estado, como el protocolo de configuración dinámica de host (DHCP).

La comunicación privada a través de Internet requiere servicios de cifrado que protejan los datos enviados ante posibles intrusiones o modificaciones durante el tránsito, razón por la cual se hace imprescindible un requisito de seguridad a nivel de capa 3, aunque el estándar existente es IPSec, en IPv4 es opcional y prevalecen las soluciones propietarias.

Ante la necesidad de facilitar la entrega de datos en tiempo real, existen estándares de QoS para IPv4, el tráfico en tiempo real se basa en el campo Type of Service (TOS o Tipo de servicio) y la identificación de la carga se la realiza mediante un puerto UDP o TCP. Posteriormente apareció un intento de una versión superior, denominada IPv5, donde el encabezado identificaba paquetes que transportaban un protocolo de tiempo real, conocido como ST2, el que garantizaba QoS, sin embargo el protocolo ST nunca fue extensamente usado, razón por la cual esta versión no se oficializó, y la nueva versión del protocolo IP se determinó como IPv6, como lo especifica el RFC 1819.

Esta versión conocida como IPng, resuelve los problemas que empezaron a aparecer con IPv4, dispone de un espacio de direcciones de 128 bits, con una jerarquía muy definida, permitiendo la auto configuración de equipos y mejorando la seguridad e integridad de los datos.

En su arquitectura contiene esquemas de autenticación y privacidad, tanto para proteger a los usuarios en sí, como la misma integridad de la red ante ataques malintencionados o errores.

En 1994 se adopta SIPP, cambiando el tamaño direccional de 64 a 128 bits y se denomina oficialmente como IPng (IP next generation), sus especificaciones se finalizaron en 1995, rebautizándose como IPv6. Las principales fortalezas que aporta el IPv6 frente al IPv4 son:

- **Aumento de las capacidades de direccionamiento.** Al incrementar el tamaño de dirección IP de 32 bits a 128 bits, para dar soporte a más niveles de direccionamiento jerárquico.
- **Soporte mejorado para las extensiones y opciones**. Los cambios en la manera en que se codifican las opciones de la cabecera IP permiten un renvío más eficiente, límites menos rigurosos y mayor flexibilidad para introducir nuevas opciones en el futuro.
- **Capacidad de etiquetado de flujo**. Se agrega una nueva capacidad para permitir el etiquetado de paquetes que pertenecen a flujos de tráfico particulares, para lo cual, el remitente solicita tratamiento especial, como la calidad de servicio no estándar o el servicio en tiempo real.
- **Capacidades de autenticación y privacidad.** En IPv6 se especifican extensiones para utilizar autenticación, integridad de los datos, y confidencialidad de los datos.
- **Autoconfiguración "plug and play".** Sin necesidad de servidores, y facilidades de reconfiguración. Los dispositivos pueden configurar sus propias direcciones IPv6 basándose en la información que reciban del router de la red.
- **Mecanismos de movilidad más eficientes y robustos.** Mobile IP soporta dispositivos móviles que cambian dinámicamente sus puntos de acceso a la red, permitiendo a un host IPv6 dejar su subred de origen mientras mantiene transparentemente todas sus conexiones presentes y sigue siendo alcanzable por el resto de Internet.

1.2 El protocolo IPv6.

IPv6 crea un nuevo formato de dirección IP con el fin de evitar que el número de direcciones IP no se agote, adicionalmente añade mejoras en áreas como el routing y la autoconfiguración de red, razón por la cual este protocolo está diseñado para simplificar las funciones de enrutamiento , mejorar la seguridad y privacidad, un manejo más eficiente de la calidad de servicio, entre

otras funcionalidades, de esta manera IPv6 es totalmente escalable cuyo fin es permitir a los protocolos antiguos y modernos coexistir.

1.2.1 Funcionamiento de IPv6.

IPv6 aparece como una propuesta de solución a las limitaciones que aparecieron en IPv4 como resultado de la masificación de las redes LAN y del acceso irrestricto al entorno Internet, de esta manera para el desarrollo de este protocolo se debió cumplir con requerimientos muy puntuales como un espacio de direcciones mucho más grande, lo que permite una drástica reducción en el uso de las direcciones IP, así mismo facilita la encapsulación de sus propios paquetes o de los de otros protocolos, con el objetivo de añadir clases de servicio para distinguir los tipos de datos transmitidos.

En la actualidad la estructura de la cabecera es más simple, con lo que se consigue mejorar el rendimiento de los routers, la existencia de cabeceras de extensión de autenticación facilita el encriptamiento de seguridad, lo que garantiza la integridad e identidad del paquete. Otros campos de la cabecera son: el identificador de flujo, que tendrá una longitud de 24 bits y favorecerá la adición entre datagramas de una misma conexión; el campo límite, que favorece la rapidez de la transmisión fijando el número máximo de nodos que debe atravesar el datagrama; y los campos versión y prioridad. Tanto la fragmentación como el ensamblado de paquetes los realizan los sistemas finales. En IPv4 unidad máxima de transmisión de un enlace con otro era de 68 octetos, el mínimo permitido por la nueva versión es 576 octetos.

1.2.2 Características de IPv6.

IPv6 ofrece características bastante interesantes como las siguientes:

- **Mayor espacio de direcciones**. La capacidad de direccionamiento es aumentada exponencialmente a 16 bytes, desde la versión anterior de 4 bytes IPv4 El tamaño de las direcciones IP cambia de 32 bits a 128 bits, para soportar: más niveles de jerarquías de direccionamiento y más nodos direccionables.
- **Simplificación del formato del Header**. Algunos campos del header IPv4 se quitan o se hacen opcionales

- **Aumento de la carga útil**. Datos de más de 65.535 bytes.
- **Seguridad en el núcleo del protocolo.** El soporte de IPSec es un requerimiento del protocolo IPv6.
- **Capacidad de etiquetas de flujo**. Puede ser usada por un nodo origen para etiquetar paquetes pertenecientes a un flujo de tráfico particular.
- **Autoconfiguración.** Incluye la creación de una dirección local y global además de la verificación de que esta dirección es única, determinando que información debería ser autoconfigurada al utilizar los procedimientos de autoconfiguración sin estado de dirección y detección de direcciones duplicadas.
- **El mecanismo sin estado de dirección**. Permite al host generar sus propias direcciones usando una combinación de la información localmente disponible y la información indicada por los routers, la cual consta de prefijos que identifican una subred, que está asociada a una conexión. El host establece la interface de conexión que solo identifica una interface en la subred, pero la dirección asignada está compuesta por la combinación de las dos.

En direcciones Aggregable Global Unicast, los 64 bits superiores son definidos por un mensaje desde el router (Router Advertisement) y los 64 bits más bajos son definidos con la dirección MAC (en formato EUI-64).

- **Renumeración y "multihoming**". Facilitan el cambio de proveedor de servicios. Da la posibilidad de que un nodo mantenga la misma dirección IP, a pesar de su movilidad.
- **Detección de direcciones duplicadas**. Debe ser ejecutada para la asignación automática de direcciones, verifica que la dirección única, unicast, asignada en forma automática no exista en forma local ni en forma global.
- **Rutinas de seguridad**. El protocolo IPv6 introduce rutinas específicas para la encriptación y autenticación de los diferentes niveles de paquetes, la aplicación de ellos solamente depende de que estas funciones estén disponibles.

El método de encriptación codifica los paquetes de datos para prevenir la lectura de los mensajes por personas no autorizadas, se verifica que la

dirección de donde fue enviado en mensaje no se pierda y paquete de información no sea interferido en la ruta.

Este protocolo permite encriptar y autenticar no solo los paquetes de datos sino también toda la comunicación entre los diferentes host, además el usuario puede utilizar el algoritmo estándar de seguridad o solicitar el uso de algoritmos adicionales cuando éstos estén disponibles.

- **Método de encriptación**. La implementación del IPv6 incluye 64 bit DES para la encriptación, este algoritmo utiliza una llave secreta simétrica de 64 bits para los niveles de encriptación, esto permite al usuario la opción de encriptar la porción de datos o encriptar el paquete completo incluyendo los encabezados para darle mayor confidencialidad.
- **Método de autenticación**. El protocolo IPv6 incluye el algoritmo MD5, para autenticación de mensajes. Este algoritmo combina el paquete de datos y la llave secreta del emisor del mensaje para generar un número de 128 bits. Si el host destinatario genera el mismo número, esto verifica que el mensaje llego sin ser modificado desde el usuario que lo envió.
- **Reservaciones de ancho de banda**. Un host pude reservar un ancho de banda sólo a una ruta entre un origen y un destino, esta función hace posible proveer de vídeo u otros datos en tiempo real con la garantía de la calidad de servicio.
- **Priorización de paquetes**. A los paquetes se les asignará un nivel de prioridad, asegurando que la transmisión de voz o vídeo no sea interrumpida por paquetes de menor prioridad.
- **Tamaño de paquetes**. IPv6 soporta paquetes de diferentes tamaños hasta un máximo de 4 MB, esto hace la transmisión de vídeo más fácil y asegura que esta versión haga posible la mejor utilización del ancho de banda sobre cualquier medio de transmisión.
- **Descubrimiento de la dirección**. IPv6 permite al host, aprender su propia dirección desde un enrutador con solo encenderlo, eliminando la necesidad de configurar la dirección de cada host. También este protocolo provee procedimientos específicos para localizar una dirección de un sitio local de comunicaciones sin tener un router soportando el DHCP, esto permite al host obtener toda la información relevante de la red desde un enrutador local.

- **Cambios automáticos de dirección**. Dado que las direcciones de la red son distribuidas por los router, cuando se intercambian los proveedores de acceso, solo requiere la actualización del enrutador.
- **Soporte de anfitriones móviles**. IPv6 incorpora algoritmos para enviar paquetes desde una dirección base a otra dirección. Esto permite a los usuarios conectarse a Internet desde cualquier localidad, aun desde teléfonos móviles que sin tener una conexión física reciben sus mensajes.
- **Simplificación de los encabezados**. IPv6 simplifica los encabezados de 12 bits en la versión IPv4 a solamente 8. Esto reduce considerablemente el tiempo de cálculo requerido para procesar el encabezado, de esta manera habrá un incremento en la velocidad de enrutamiento.
- **Optimización del tamaño de paquetes**. Antes de enviar los paquetes de datos, este protocolo determina el tamaño máximo soportado por todos los router a lo largo de la dirección de envío. El host divide el mensaje en paquetes que no requieren fragmentación por el router, reduciendo así la carga computacional.
- **Multicasting.** Reduce la carga en el host, esta función permite al host y al router enviar mensajes de reconocimiento de vecinos, solo los hosts que se han registrado van a recibir este mensaje.
- **Direccionamiento múltiple**. Permite la agregación a la ruta, IPv6 permite múltiple direccionamiento por cada dispositivo de interface, haciendo la agregación de rutas simple y eficiente.
- **Características de auto configuración.** El protocolo IPv6 para router y anfitriones, permite descubrir los hosts vecinos mediante el método de identificación de vecinos (Hoog, 2009, pág. 4) éste contiene todas las características para el descubrimiento como parámetros para la configuración local. Esto provee un incremento en la flexibilidad, como la capacidad de optimizar la convergencia de la red.
- **Compatibilidad con IPv4**. Por la gran capacidad instalada en base a IPv4 en toda la infraestructura de red, las especificaciones para IPv6 incluyen mecanismos diseñados para asegurar la transparencia y gradual transición de IPv4 a IPv6.

- **Traslado de las direcciones del IPv4**. Las direcciones IPv4 son fácilmente trasladadas a la versión IPv6, agregando un prefijo de ceros.
- **Pilas duales del Protocolo**. Todas las implementaciones IPv6 incluyen pilas para la IPv4.
- **IPv6 construido sobre IP v4**. Aquellos host que trabajen bajo IPv6 pueden comunicarse con otros a través del router con IPv4, simplemente con convertir los paquetes de IPv6 dentro de paquetes IPv4.
- **Calidad de servicio (QoS) y clase de servicio (CoS)**. Es el efecto colectivo del rendimiento de la red, lo que determina el grado de satisfacción de los usuarios del servicio y está caracterizada por la combinación de aspectos tales como: soporte, operatividad, seguridad y otros factores específicos de cada servicio, las técnicas y procedimientos de QoS deben ser implementadas en todos los dispositivos de la red.

1.3 Arquitectura de ipv6

IPv6 utiliza un tamaño de cabecera fijo de 40 bytes, que componen un total de ocho campos. Como se puede apreciar en la figura 1, se indica el formato del encabezado que viaja actualmente en cada paquete de IPv4.

Figura 1 Formato del encabezado IPv4
Fuente: (Alba, 2008)

El motivo fundamental por el cual algunos campos son eliminados de debe a la redundancia.

1.3.1 CAMPOS ELIMINADOS.

IPv6 tiene una longitud fija del encabezado de 40 Bytes, el campo **longitud total** se torna innecesaria, existe un nuevo mecanismo de opciones que

permite tener la cabecera de un tamaño constante. La eliminación del campo **desplazamiento** del fragmento obedece a que cambia por completo el mecanismo por el cual IPv6 hace la fragmentación puesto que ya no se permite la fragmentación en ruta, este campo junto a **identificación** e **indicador** son eliminados. La tarea asignada al campo **checksum**, es realizada por otros mecanismos de encapsulado.

1.3.2 CAMPOS MODIFICADOS.

El campo **longitud total** pasa a ser longitud de la carga útil, de hasta 64Kbytes. El campo **protocolo** pasa a llamarse **siguiente cabecera,** al utilizar sucesivas cabeceras encadenadas, esta es la causa por la cual desaparece el campo opciones. El campo **tiempo de vida** pasa a ser nombrado como **límite de saltos**, y permite definir la cantidad máxima de routers por los que el paquete puede atravesar. La **dirección origen** no cambia su nombre, pero pasa de tener una longitud de 32 bits a una de 128 bits. La **dirección destino** mantiene su nombre, pero pasa de tener una longitud de 32 bits a una de 128 bits.

1.3.3 NUEVOS CAMPOS.

Aparece el campo **clase de tráfico**, que es el equivalente a **tipo de servicio** (TOS) en IPv4. La **etiqueta de flujo** identifica paquetes que pertenecen a un mismo flujo permitiendo manejar tráficos con requisitos de QoS en tiempo real. La dirección de la fuente y la etiqueta de flujo determinan unívocamente un flujo. Estos dos campos son los que permiten el uso de QoS y CoS.

IPv6 incrementa la longitud de la cabecera IP de 20 a 40 bytes. La cabecera contiene dos direcciones de 16 bytes para origen y destino, precedidas de 8 bytes de control como se muestra en la figura 2.

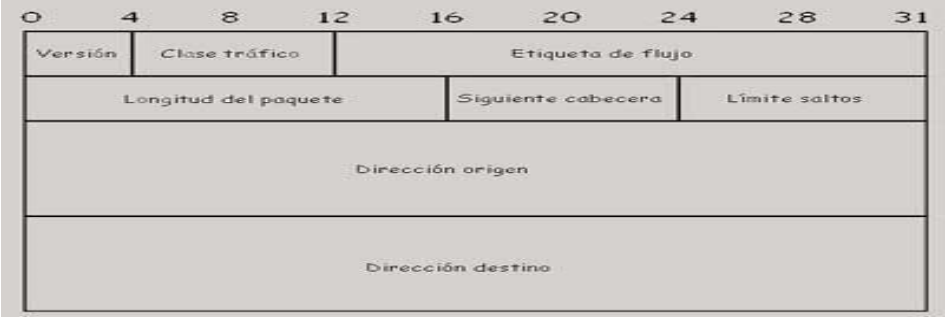

Figura 2 Cabecera IPv6
Fuente: (Bruzual, 2012)

La reducción de la información de control y la eliminación de opciones de la cabecera tienen como fin optimizar el procesamiento del paquete.

- **Versión**, (4 bits). Sirve para que el router se entere de que es un paquete IPv6. Dirección origen y de destino (128 bits cada una).
- **Clase de tráfico** (8 bits). Diferencia entre servicios sensibles a la latencia, como VoIP, de otros que no necesitan prioridad, como tráfico http.
- **Etiqueta de flujo** (20 bits). Permite la diferenciación de flujos de tráfico. Esto tiene importancia a la hora de manejar QoS
- **Siguiente cabecera** (8 bits). Este campo permite a los routers y a los host examinar con más detalle el paquete, a pesar de que el paquete básico IPv6 tiene cabecera de tamaño fijo, el protocolo puede añadir más información para utilizar otras características como encriptación y autenticación. Indica el tipo de cabecera que sigue para determinar la presencia de cabeceras de extensión que proporcionan los mecanismos para añadir información opcional al paquete.
- **Tamaño de payload** La longitud del paquete en bytes (excluyendo la cabecera) codificada como un entero sin signo de 16 bits, describe el tamaño en octetos de la sección de datos del paquete.

Al ser este campo de 16 bits, se podrá usar paquetes de hasta más de 64000 bytes. Sin embargo cuando la longitud es mayor de 64Kb, el campo vale 0 y la cabecera opcional muestra la verdadera longitud.

- **Límite de saltos.** Especifica el número de saltos de router que puede hacer el paquete antes de ser desechado.
- **Source Address**, contiene una dirección de 128 bits.

- **Destination Address**, contiene la dirección de 128 bits.
- **El campo de siguiente cabecera (Next Header Field),** determina que el tamaño de la cabecera IPv6 básica es fijo, adicionalmente permite describir con más detalle las opciones del paquete.

En este campo se codifican las opciones como lo muestra la tabla 1

Tabla 1
Opciones del campo de siguiente cabecera

Siguiente cabecera	Valor del campo
Opciones de Hop-by-Hop	0
Opciones de destino	60
Encaminamiento	43
Fragmento	44
Autenticación	51
Encapsulación	50
Ninguna	59

Fuente: RFC 2460

El campo de siguiente cabecera (NEXT HEADER FIELD)

Hay 8 tipos de cabeceras de extensión, incluyen el campo siguiente cabecera, que identifica el tipo de cabeceras de extensión que viene a continuación o el identificador del protocolo de nivel superior. Todas o parte de estas cabeceras de extensión tienen que ubicarse en el datagrama en el orden especificado, como se muestra en la tabla 1.2. Las cabeceras se van encadenando por medio del uso del campo de siguiente cabecera que aparece tanto en la cabecera fija como en las de extensión. Las cabeceras aparecen en el siguiente orden:

1. Cabecera IPv6 básica.
2. Opciones Hop-by-Hop.
3. Opciones de destino.
4. Encaminamiento.
5. Fragmento.
6. Autenticación.
7. Encapsulación.
8. Opciones de destino.

9. Cabecera nivel superior.

En la tabla 2 se detalla las cabeceras de extensión, identificador, descripción y se hace referencia al RFC que lo respalda.

Tabla 2
Cabeceras de extensión

Cabecera de Extensión	Tipo	Tamaño	Descripción	RFC
Opciones salto a salto (*Hop-By-Hop Options*)	0	Variable	Contiene datos que deben ser examinados por cada nodo a través de la ruta.	RFC 2460
Ruteo (*Routing*)	43	Variable	Métodos para especificar la forma de rutear un datagrama.	RFC 2460, RFC 6275, RFC 5095
Cabecera de fragmentación (*Fragment*)	44	64 bits	Contiene parámetros para la fragmentación .	RFC 2460
Cabecera de autenticación (*Authentication Header (AH)*)	51	Variable	Contiene información para verificar la autenticación de los datos del paquete.	RFC 4302
Encapsulado de seguridad de la carga útil (*(ESP)*)	50	Variable	Lleva la información cifrada.	RFC 4303
Opciones para el destino	60	Variable	Información que necesita ser examinada por los nodos de destino	RFC 2460
No Next Header	59	Vacío	Indica que no hay más cabeceras	RFC 2460

Cada cabecera de extensión debe aparecer una sola vez, salvo la cabecera de opción destino, que puede aparecer hasta dos veces, una antes de la

cabecera ruteo y otra antes de la cabecera de la capa superior. Esto se muestra en la figura 3.

Los routers, solo examinan cabecera IPv6 básica. Existen excepciones como en el caso de que existan cabeceras de opciones Hop-by-Hop o, como en el caso que exista una cabecera de encaminamiento en el que sólo los nodos en ella definidos deberán alterar el paquete.

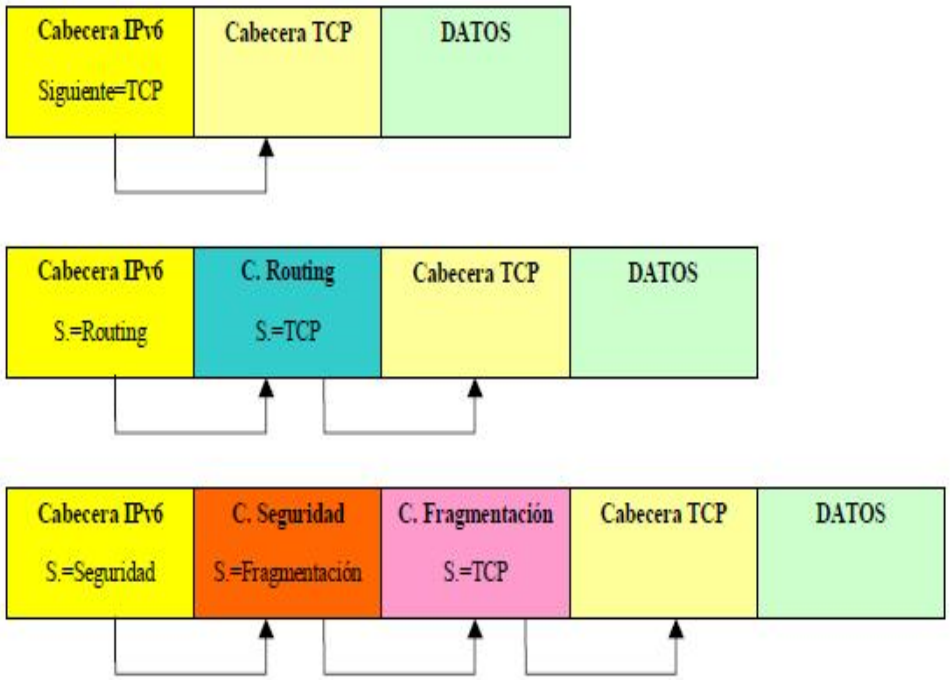

Figura 3
Cabecera IPv6 básica, fragmento y datos
Fuente: (Wikispace, 2012)

1.4 Direccionamiento en ipv6

Existen varios tipos distintos de direcciones IPv6: Unicast, Anycast y Multicast, en la tabla 3 se detalla cada uno de ellos.

Tabla 3
Tipos de direcciones IPv6

Dirección IPv6	Longitud del Prefijo (Bits)	Descripción	Notas
::	128 bits	Sin especificar	Como 0.0.0.0 en Pv4

::1	128 bits	Bucle local	Como las 127.0.0.1 en IPv4
::00:xx:xx:xx:xx	96 bits	Direcciones IPv6 compatibles con IPv4	Los 32 bits más bajos contienen una dirección IPv4.
::ff:xx:xx:xx:xx	96 bits	Direcciones IPv6 mapeadas a IPv4	Los 32 bits más bajos contienen una dirección IPv4. Se usan para representar direcciones IPv4 mediante direcciones IPv6.
fe80:: - feb::	10 bits	Direcciones link-local	Equivalentes a la dirección de loopback de IPv4
fec0:: - fef::	10 bits	Direcciones site-local	Equivalentes al direccionamiento privado de IPv4
ff::	8 bits	Multicast	

Las mismas que deberán ser usadas de acuerdo a los preceptos que se manejan en el diseño de redes y a las especificaciones otorgadas por los organismos de control, en este caso LACNIC, que es la organización responsable de la asignación y administración de las Direcciones IP y recursos relacionados.

1.4.1 Representación de direcciones IPv6

La forma canónica que se utiliza para representar direcciones IPv6 es: x:x:x:x:x:x:x:x, donde cada “x” se considera un valor hexadecimal de 16 Bit. Por ejemplo FEBC:A574:382B:23C1:AA49:4592:4EFE:9982

Toda dirección IPv6 se expresa en base hexadecimal, cuyas direcciones binarias de destinos y proveniencia constan de 128 bits, esto permite un total de 2^{128} direcciones legítimas. Se expresa 8 grupos de 16 bits escritos en notación hexadecimal como por ejemplo

3ffe:ffff:0100:f101:0210:a4ff:fee3:9566

Con mucha frecuencia una dirección posee alguna subcadena de varios ceros consecutivos de forma que se puede abreviar dicha cadena, sólo una

vez, para evitar ambigüedades, mediante “::”. Los ceros a la izquierda de cada grupo se omiten, entonces :0001: puede simplificarse como :1:

Por ejemplo a fe80::1 le corresponde con la forma canónica fe80:0000:0000:0000:0000:0000:0000:0001.

Bloques contiguos de 16bits de ceros pueden simplificarse por única vez con :: , por ejemplo 2002:ffff:0:0:0:0:0:1 puede simplificarse como 2002:ffff::1

Otra forma de escribir direcciones IPv6 es utilizando la ya tradicional notación decimal de IPv4 pero solamente para los 32 bits más bajos de la dirección IPv6. Por ejemplo a 2002::10.0.0.1 correspondería con la representación canónica 2002:0000:0000:0000:0000:0000:0a00:0001, que es equivalente también a escribir 2002::a00:1.

Existen solo dos direcciones reservadas en ipv6:

- Una es la dirección local ::1 (se están simplificando 31 ceros), esta solo se la puede asociar al dispositivo "loopback", es similar en ipv4 a la dirección privada 127.0.0.1
- Otra es :: (todo cero) que corresponde a dirección no especificada y no puede usarse como dirección. No existe la dirección broadcast, por lo tanto en teoría ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff es legítima, pero no se usa.

Otro concepto importante es el prefijo, este determina una reserva del espacio de direccionamiento de la dirección para definir la red y la sub-red, por ejemplo 2002::/16 el prefijo es 16 e indica que los primeros 16 bits corresponden a la caracterización de la red.

1.4.2 Tipos de direcciones IPv6

Las direcciones IPv6 se clasifican de acuerdo a las políticas de ruteo y direccionamiento comunes en networking, de la siguiente manera:

- **Unicast**. Son direcciones asociadas a una sola interfaz, un paquete enviado a una dirección unicast solo se entrega a la interfaz asociada a dicha dirección. Por ejemplo fe80::200:21ff:fea8:4614/10 está asociado a la interfaz Ethernet 0, en un host con dirección MAC 00:00:21:a8:46:14, o la dirección global 3ffe:b80:1daf:1::1.

- **Túneles dinámicos de IPv6 sobre IPv4** (::<dirección ipv4>/96), conocida como direcciones IPv6 compatibles con IPv4, esto permite retrasmitir tráfico IPv6 sobre infraestructura IPv4 (rfc 2893), como por ejemplo ::172.15.20.35/96
- **Direcciones ipv4 en ipv6** (::ffff:<dirección ipv4>/96), permite que los nodos que solo soportan IPv4 puedan ser anexados a la red IPv6, como ejemplo ::ffff:198.160.1.4/96
- **Direcciones unicast locales.** Existen dos tipos de direcciones unicast locales, todo nodo debe por lo menos contener una de ellas: Enlace local (link-local) y sitio (site-local). Las primeras tiene un formato fe80::<id de interfaz>/10 y están asociadas a una interfaz, y no pueden salir de ella ningún paquete que tenga como dirección de destino una de ellas.

Algunos ejemplos:

fe80::200:21ff:fe43:ca26/10, link asociado a una tarjeta de red, aquí el ID de interfaz es un mapeo del número mac (rfc2464).

fe80::c0a8:204/10, link asociado a la interfaz sit1, el ID es un mapeo de la dirección ipv4 de la host 192.168.2.4 escrito en hexadecimal ::c0a8:204 asociada con la tarjeta de red

fe80::1/10 , link asociado a la interfaz l

Las segundas tienen un formato fec0::<id-subred><id-interfaz>/10 y están asociadas a un sitio u organización, son análogas a las redes privadas 192.162.0.0/16, pero con muchos más espacio de direcciones. No pueden salir ni por ruteadores ni por pasarelas los paquetes IPv6 que lleven ese espacio de direcciones. Como ejemplo

fec0::1:200:21ff:fe43:ca26/10, site asociada a una tarjeta de red, cuyo id-subred es :1: a la izquierda del ID 200:21ff:fe43:ca26

- **Direcciones Anycast** (rfc 2526). Tienen el mismo rango que las unicast, cuando una dirección unicast es asociada a más de una interfaz se convierte en una dirección anycast. Existen direcciones anycast asociadas a cada subred requeridas para los ruteadores, su formato es <prefijo de red><subred>::/n, el identificador de interfaz es el cero.

Por ejemplo:

3ffe:b80:1daf:1::/64 acá 3ffe:b80:1daf es el identificador de la red freenet y :1: corresponde a la subred local, 1daf es el túnel asignado.

fe80::/10 Asociada a toda interfaz local

fec0::/10 Asociada a todo el sitio.

- **Direcciones Multicast** (rfc 2375). Es una dirección que caracteriza a un conjunto de nodos, el identificador de grupo asocia a un grupo en particular de interfaces, como ejemplo:

ff01::10, a todos los identificadores de tiempo con identificador de grupo 101 en ámbito del nodo.

ff02::10, a todos en el mismo enlace asociado con la misma interfaz con id-grupo 101.

ff01::10, ídem pero a toda la Internet.

ff15::101 no permanente asociada al sitio. La dirección temporal tiene solo sentido a nivel local.

Existen direcciones multicast reservadas:

ff01::1 Todos los nodos

ff02::1 Todas las interfaces

ff01::2 Todos los routers locales

ff05::2 Todos los routers del sitio

Según el RFC-2373 existen prefijos reservados para NSAP, IPX, direcciones globales unicast aggregatable, direcciones de enlace local, direcciones de enlace de red y direcciones multicast, tal como se especifica en la tabla 4.

Tabla 4
Prefijos reservados de la dirección unicast global

Tipo	Prefijo Binario	Prefijo en hexa	Fracción de espacio de direcciones
Reservado para NSAP	0000 001	02* 03*	1/128
Reservado para IPX	0000 010	06* 07*	1/128
Direcciones globales Unicast	001	2* 3*	1/8
Direcciones enlace-local (**)	1111 1110 10	fe8* .... feb*	1/1024

Direcciones enlace-red (**)	1111 1110 11	fec* .... fef*	1/1024
Direcciones Multicast	1111 1111	ff*	1/256

Fuente: LACNIC

Notas: (*) => resto puede tomar cualquier valor, pero existen por ahora asignaciones limitadas

(**) No pueden traspasar ruteadores ni pasarelas

- **Direcciones unicast globales anexables** (rfc2374) Uno de los problemas que ipv6 resuelve es la mayor organización jerárquica del ruteo en redes públicas anexables (agregable public global net). Se basa en tres niveles:

Topología pública: Asociada a los proveedores y pasarelas de la red troncal asociada a la Internet.

Topología de sitio: Propia de la red interna de la organización

Identificador de interfaz: Asociado con la interfaz de enlace.

1.4.3 Vulnerabilidades asociadas a IPv6.

Este protocolo presenta ciertas deficiencias de seguridad, que en la mayoría de casos son los administradores de red quienes se encargan de mitigarlas, la mayoría de las vulnerabilidades involucran a campos de la cabecera del paquete en donde están especificados los procesos que definen su funcionamiento e interacción con las capas superiores. El protocolo IPv6 y el encabezado en sí no representan ninguna vulnerabilidad de seguridad, el problema es la forma en que estos paquetes son generados y procesados, lo que puede crear brechas de seguridad, entre las principales vulnerabilidades se puede señalar el Internet Control Message Protocol versión 6 o ICMPv6.

- **Los ataques ICMPv6 y las técnicas de mitigación.** Este protocolo se ha usado durante muchos años como un método de prueba de conectividad y solución de problemas en el entorno de red, sin embargo esto representa una vulnerabilidad en IPv6 puesto que un atacante podría utilizar ICMP para crear exploits, aprovechando que los paquetes al enviarse en una LAN tienen un límite de saltos fijado en 255 como máximo, con el objetivo de prevenir que los paquetes queden indefinidamente en la red causando congestión, en IPv4 esto

se lo controlaba con el TTL, especificado en segundos, por lo tanto los dispositivos de Capa 3 deben descartar o ignorar cualquier paquete especificado con un límite de saltos menor de 255, igualmente si el nodo receptor recibe un paquete que tiene un valor de límite de saltos menor que 255, se da por sentado que este paquete podría haber sido manipulado y los paquetes deben ser rechazados.

Cuándo un enrutador o servidor de seguridad recibe un paquete que tiene un límite de salto igual a 1, se descarta el paquete porque su hop-limit se ha excedido, cuando el router o el firewall descarta el paquete, envía un mensaje ICMPv6 indicando el tiempo excedido, de nuevo a la fuente del paquete. El atacante podría generar una gran cantidad de paquetes que alcanzarán el servidor de seguridad, al igual que su límite de salto se reduce a 0, causando un ataque de consumo de recursos en el firewall, provocando su baja de rendimiento con el consiguiente impacto en el tráfico de la red y en casos más extremos el colapso del equipo conduciendo a una pérdida de conectividad de la LAN hacia la WAN.

Los ataques pueden ser desde un spoofing simple de mensajes ICMPv6 hasta un ataque completo a la infraestructura de la red. Una técnica es simplemente rutear todos los tipos de mensajes ICMPv6 que aún no han sido asignados por la IANA. Los siguientes tipos de mensajes ICMPv6 no deben considerarse (Hoog, 2009, pág. 20).

Los mensajes de error no asignados: Tipo de 5-99 y el tipo 102-126.
Mensajes informativos no asignados: Tipo 155-199 y 202-254.
Mensajes experimentales: Tipo 100, 101, 200, 201.
Los números de extensión Tipo: Tipo 127, 255.

Adicionalmente se debe negar los paquetes de solicitud de eco ICMPv6 que provienen fuera de la red, sin embargo se debe tener mucho cuidado con la forma que se filtra porque algunas de sus funciones siguen siendo necesarias para las operaciones normales.

Un posible medio de ataque podría ser simplemente crear un ataque de denegación de servicio (DoS) al generar muchos paquetes ilegales tales como

paquetes extremadamente grandes o número de saltos erróneos, entonces el dispositivo de red va a responder a cada uno de aquellos con un mensaje de error ICMPv6 dando como resultado el aumento de la carga de trabajo del equipo de tal manera que se podría impulsar la utilización elevada de la CPU del dispositivo causando una degradación del rendimiento.

Se puede mitigar este problema al controlar la velocidad a la que el router genera todos los mensajes de error ICMPv6, los que pueden ser limitados mediante el uso del comando: ipv6 icmp error-interval [milisegundos].

- **Seguridad multicast.** Cuando los diseñadores de IPv6 estaban redactando el protocolo, querían evitar las ineficiencias de los mecanismos de difusión, IPv6 multicast depende de muchas funciones que se tenían IPv4, de hecho IPv6 no tiene ningún método de transmisión de renvío de paquetes multidifusión y en su lugar utiliza multicast para el descubrimiento de vecinos, DHCP, aplicaciones multimedia. Si un atacante podría enviar tráfico a estos grupos de multidifusión, daría al atacante información que podría utilizar para nuevos ataques, por ejemplo tendría información acerca de todos los routers dentro de la red y todos los hosts DHCPv6.

Estos son los nodos de importancia crítica para ayudar a un atacante en la intrusión, ya sea a través de cachés vecinas, actualizaciones obligatorias, o troncales DHCPv6, para lanzar un ataque ciego, es decir sin retorno de tráfico contra todos los servidores DHCPv6, el atacante sólo tiene que enviar su paquete a FF05 ::1:3, causando bajas de rendimiento en toda la infraestructura.

- **Los ataques de denegación de servicio**. Una dirección de origen falso en un paquete destinado a una dirección multicast en la red objetivo del ataque, podría dar lugar a la amplificación del tráfico de retorno, una buena técnica de mitigación contra el ataque DoS consiste en rutear todo el ámbito global y de sito local de los paquetes de multidifusión en la red perimetral. Esto se logra con una lista de acceso IPv6 que rutea todo el tráfico que va hacia o desde el rango de direcciones multicast, es decir toda FF00 :: / 16.
- **Vulnerabilidades en las cabeceras de extensión.** Debido a que las especificaciones del protocolo no han limitado el uso de cabeceras de extensión, potencialmente podrían causar problemas si se usan

maliciosamente. Un atacante podría realizar la manipulación en las cabeceras de extensión para crear ataques al crear un paquete IPv6 que cumpla con la especificación del protocolo y tenga un número ilimitado de cabeceras de extensión unidos entre sí en una lista grande.

Un paquete como este podría causar una denegación de servicio en los sistemas intermediarios o en los sistemas de destino. El paquete manipulado podría también pasar a través de la red sin causar ningún problema, es una manera para que los piratas eviten los firewalls y sistemas de prevención de intrusiones o IPS. Los paquetes que tienen una gran cadena de cabeceras de extensión pueden ser peligrosos puesto que su carga útil no será inspeccionada porque el servidor de seguridad solamente analiza el fragmento inicial.

- **Encabezados Opción desconocida.** Los firewall y dispositivos de capa 3 deben descartar los paquetes que contienen las cabeceras de extensión que no son reconocidos, el problema es que algunos firewalls y otros dispositivos de red simplemente ignoran cualquier cabecera de extensión que no entienden, entonces estos dispositivos pasan estos paquetes sin saber que esto podría ser parte de un paquete malicioso o un paquete manipulado (Hoog, 2009, pág. 52).
- **Doble pila.** En IPv6 la vulnerabilidad puede heredarse de la versión anterior del protocolo, en este caso IPv4, por ejemplo un servidor web puede estar escuchando en el puerto TCP 80 tanto en su dirección IPv4 como en su dirección IPv6, si el filtrado se lo hace en IPv4 y no en IPv6, el servidor web sigue siendo vulnerable.
- **Vulnerabilidades del DNS**. IPv6 se basa más en DNS puesto que las direcciones más grandes son difíciles para recordar, el DNS contiene información sobre todos los sistemas IPv6 de la organización, por lo tanto puede ser utilizado para algunas actividades de reconocimiento, los atacantes pueden saber sobre la información almacenada en los servidores DNS para proceder con la recopilación de datos y generar los ataques posteriores.

1.5 IPSec en IPv6.

IPSec ofrece seguridad a nivel de capa 3, por medio de algoritmos criptográficos que permiten proporcionar servicios de transporte seguros entre dos extremos, adicionalmente se lo usa para proteger una o más trayectorias entre un par de host, o entre un par de security gateway.

En este protocolo los equipos cifran los datos para su transmisión entre hosts, puesto que proporciona protección a los paquetes IP, basado en un esquema de seguridad de extremo a extremo, esto significa que los únicos hosts que tienen que conocer la protección de IPSec son el que envía y el que recibe. IPSec se puede implementar en dos formas:

Modo transporte.- Se usa el encabezado exterior, el encabezado siguiente y los puertos que admita el siguiente encabezado para determinar la directiva IPSec, en la cabecera IPv6 sólo la carga útil del paquete IP está sometida al proceso de cifrado o autenticación, y en algunos casos, a ambos al mismo tiempo.

La ruta se mantiene intacta, puesto que la cabecera IP no está sujeta a modificación, cuando el encabezado de autenticación se utiliza, las direcciones IP no pueden ser traducidas tal como se especifica en la figura 4.

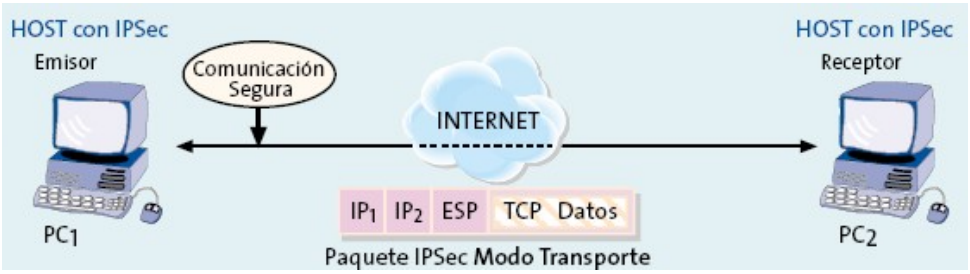

Figura 4 Modo Transporte de IPSec
Fuente: (Unex, 2006)

- **Modo túnel.-** En este escenario, todo el paquete IP se somete a un cifrado o autenticado, sin embargo existen casos en que el paquete IP es cifrado y autenticado al mismo tiempo. Para que el proceso de enrutamiento se realice, todo el nuevo paquete IP se debe encapsular nuevamente, así el protocolo de ruteo se aplica a los paquetes que pasan por el túnel a través de la IP, la estructura de este modo se puede apreciar en la figura 5

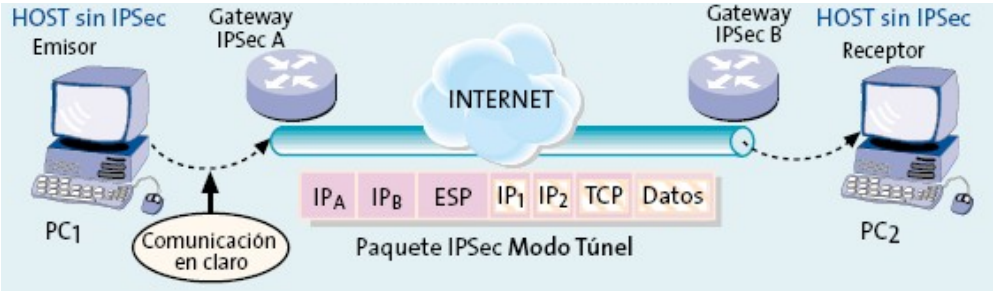

Figura 5 Modo Túnel de IPSec
Fuente: (Unex, 2006)

1.5.1 Arquitectura y funcionamiento de IPSec.

IPSec proporciona un entorno seguro de comunicación a nivel de capa 3, por medio de un proceso de autenticación y el cifrado aplicado al paquete IP, es necesario que ambos extremos compartan dos protocolos de seguridad conocidos como AH y ESP y un protocolo de intercambio de claves llamado Internet Key Exchange o IKE. Cuando se usa el protocolo AH se aplican algoritmos de autenticación de los datos, en el caso de usar protocolo ESP se aplican algoritmos de encriptación que combinan autenticación, integridad de datos, control de acceso al establecer políticas de establecimiento de conexiones IPSec y el manejo de la confidencialidad de datos.

El DOI (Domain of Interpretation) define todos los parámetros que se negocian para establecer canales seguros, incluyendo identificadores únicos para los algoritmos de autenticación y de encriptación durante el proceso de comunicación, además de los procesos para crear las conexiones tipo AH o ESP, adicionalmente especifica los parámetros operacionales para el protocolo IKE tales como tiempo de vigencia de las claves. La Política de Seguridad (SP, Security Policy), define qué tráfico proteger y cuándo hacerlo. La arquitectura se IPSec, se muestra en la figura 6

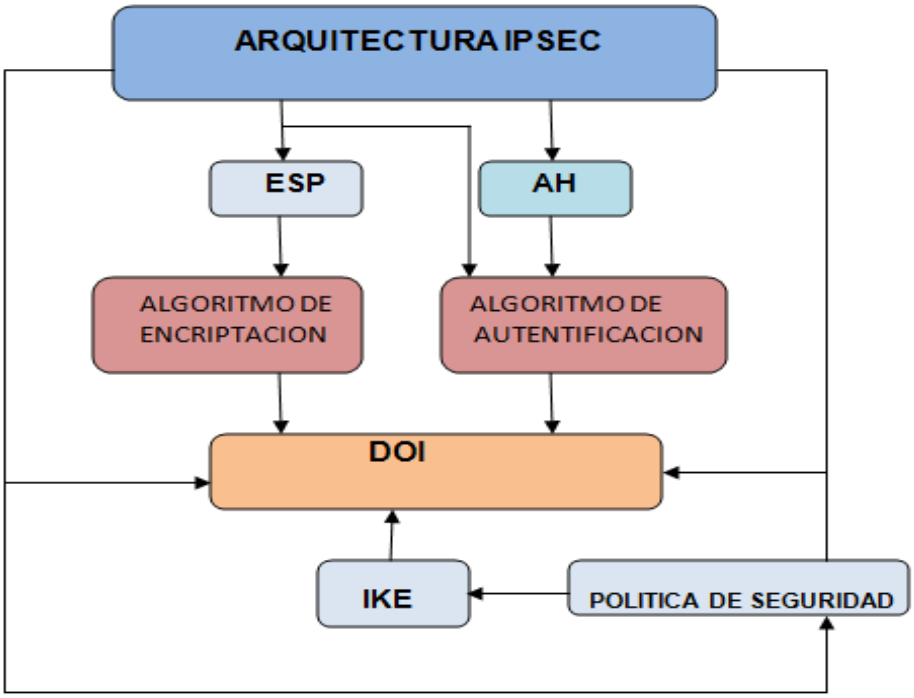

Figura 6 Arquitectura de IPSec
Fuente: (Villagra, 2000)

1.5.2 Security Association (SA).

La asociación de seguridad, administra los servicios de seguridad y parámetros negociados en cada trayectoria segura, la SA administra el escenario de interoperabilidad usada en AH y ESP, así como la relación uno a uno entre transmisor y receptor que define el conjunto de parámetros de seguridad utilizados. Se debe puntualizar que es necesario establecer una SA antes de realizar una cifrado IKE. Un SA contiene los siguientes campos:

- **Sequence Number Counter:** El contador del emisor se inicializa en cero cuando se establece una SA, el emisor incrementa el SA insertando el nuevo valor dentro de este campo, de esta manera el primer paquete enviado con una SA tiene el valor de este campo puesto en 1. Es un valor de 32 bits para generar el número de secuencias transmitidas en las cabeceras AH y ESP.
- **Sequence Counter Overflow:** Indica el desbordamiento del Contador del Número de Secuencia, debe lanzar un alarma y prevenir la transmisión de los paquetes adicionales en la SA. El emisor controla que se complete un ciclo de transmisión antes de insertar un nuevo valor en el campo Sequence

Number, cuando se envía el paquete SA (Francisconi, 2005, pág. 20) antes que se cumpla el ciclo, se produce un desbordamiento del número de secuencia.

- **Anti-Replay Window:** Ventana para limitar la aceptación de datagramas válidos.
- **AH Information:** Algoritmos de autentificación, claves, tiempos de vida, usando AH.
- **ESP Information:** Algoritmo de cifrado y autentificación, claves, valores de inicio, TTL.
- **IPSec Protocol Mode:** Modo de transporte o Túnel.
- **SA Lifetime:** Intervalo de tiempo o bytes después del cual hay que sustituirla por una nueva SA o terminar una SA. Cuando se usa un contador de bytes, la implementación debería contar el número de bytes a los cuales se aplica el algoritmo, en el caso de ESP, es el algoritmo de encriptación y en el caso de AH, es el algoritmo de autenticación, como se puede observar los campos son los mismos en ambos escenarios pero los valores son diferentes de acuerdo al escenario en que se esté trabajando.
- **Path MTU**: Máximo tamaño de paquetes transmitidos sin fragmentación.

Combinación de SA.- Existen cuatro escenarios donde es posible implementar una SA, estas configuraciones deben ser soportadas por hosts IPSec o en los gateway de seguridad.

- **CASO I.** Proporciona seguridad extremo a extremo entre 2 host a través de la red. Tanto el modo transporte cuando se especifica AH en el transform-set y modo túnel, al especificar ESP en el transform-set, pueden ser seleccionados en los host, en este caso no existe ninguna condición para el soporte de enrutamiento en las cabeceras.

El procedimiento indica que para establecer la SA en el modo transporte especifica que se debe aplicar primero ESP, y luego aplicar AH al paquete, tal como se muestra en la figura 7.

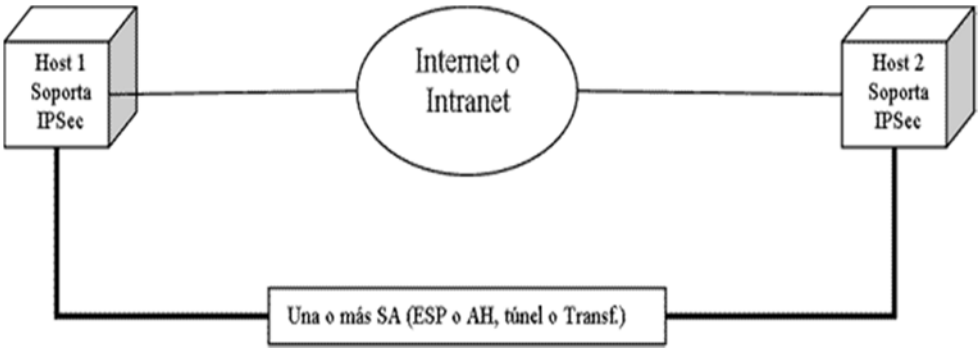

Figura 7 Combinación básica de SA (caso 1)

Fuente: (Multimanía, 2010)

- **CASO II.** Se aplica en escenarios en donde se usa una VPN, como lo muestra la figura 8, este caso trabaja exclusivamente en modo túnel. (Stallings, 2004, pág. 200)

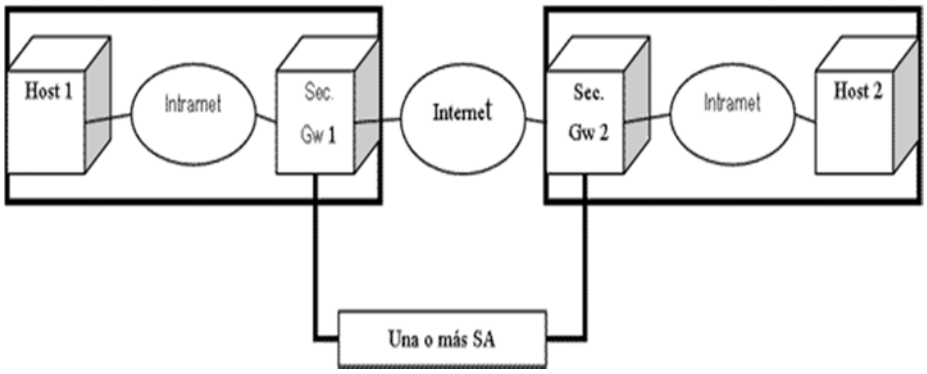

Figura 8 Combinación básica de SA (Caso 2)

Fuente: (Multimanía, 2010)

- **CASO III.** Esta opción combina el caso 1 y el caso 2, con la característica adicional que agrega seguridad extremo a extremo entre el host emisor y el receptor, como se puede apreciar en la figura 9.

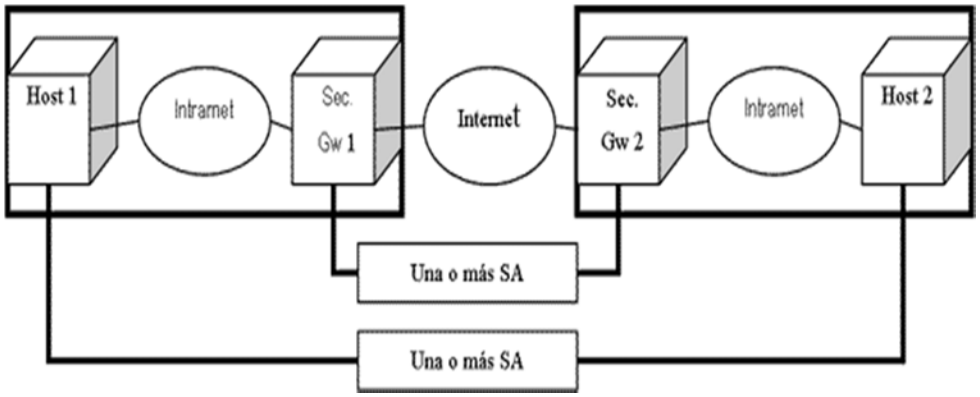

Figura 9 Combinación básica de SA (caso 3)

Fuente: (Multimanía, 2010)

El security gateway debe dejar pasar tráfico IPSec, incluyendo tráfico ISAKMP, a los host que están detrás de este.

- **CASO IV.-** Cuando un host externo que puede ser de tipo móvil, usa internet para alcanzar el firewall de una LAN con el fin de acceder a otro host o a un servidor, en este caso el host externo localiza el Security Gateway dentro de la LAN, el mismo que lo autentica y verifica su autorización por medio del protocolo IKE.

Es necesario que se configure el modo túnel entre el host remoto y el firewall. Las opciones para la SA entre los dos host pueden ser modo transporte o modo túnel, o en su defecto ambos al mismo tiempo, sin embargo se debe aplicar ESP antes que AH.

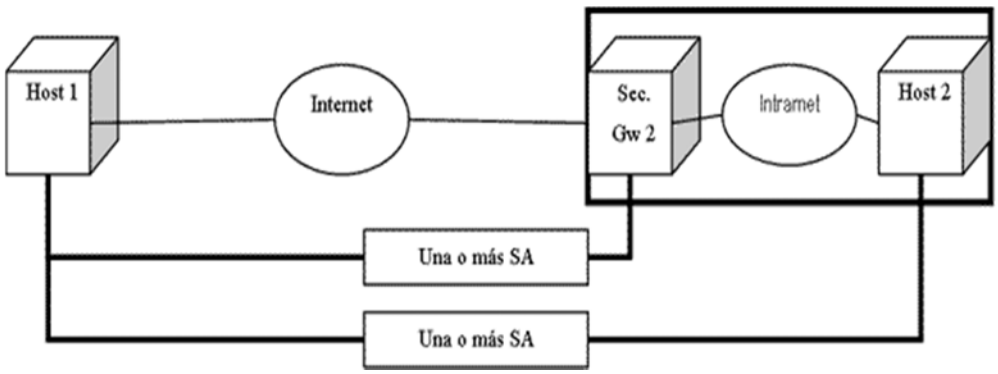

Figura 10 Combinación básica de SA (caso 4)
Fuente: (Multimanía, 2010)

1.5.3 Base de datos SA.

En IPSec existen dos bases de datos que manejan el procesamiento del tráfico, las mismas que son: La base de datos de política de seguridad y la base de datos de asociación de seguridad. La primera especifica las políticas que determinan el tratamiento de todo el tráfico IP de entrada o salida de un host y puerta de enlace segura y la segunda contiene los parámetros asociados a cada SA.

Base de datos de políticas de seguridad (SPD).

Un elemento esencial del proceso de la SA es una SPD que especifica qué servicios deben ser ofrecidos a los datagramas IP y de qué forma. Para cada implementación IPSec es necesario que exista una interfaz de administración, que permita al administrador del sistema manejar la SPD, la misma que debe especificar qué acción ha de realizar en cada caso. En el escenario planteado en este trabajo, el administrador manualmente especifica en el router los selectores como la política ISAKMP, el tipo de autenticación, el algoritmo de hash, el método de intercambio de claves, el algoritmo de cifrado y el tiempo de vida de la SA.

La SPD debe diferenciar entre el tráfico al que debe ofrecer protección IPSec del que no, esto requiere que IPSec debe estar implementada en ambos extremos. Para cualquier datagrama de entrada o de salida, hay tres opciones de procesamiento posibles:

- **Descartar.-** es el tráfico al que no se permite salir del host, atravesar una puerta de enlace, o que se entregue a una aplicación.
- **Evitar IPSec (no IPSec).-** se refiere al tráfico que se le permite pasar sin la protección de IPSec.
- **Aplicar IPSec.-** SPD debe especificar los servicios de seguridad, los protocolos que se emplearán, los algoritmos que se utilizarán, esto aplicado al tráfico protegido. Específicamente, cada paquete de entrada o de salida está sujeto al procesamiento IPSec, y la SPD deberá especificar qué acción será tomada en cada caso.

La SPD contiene una lista ordenada de políticas de entrada, que es introducida por uno o más selectores que definen el conjunto de tráfico IP comprendido por esta política de entrada, que definen las políticas de las SA. Cada entrada incluye un indicador para el tráfico coincidente con esta política, si será desviado, desechado, o procesado por IPSec. Se detalla a continuación las políticas implementadas en el escenario propuesto

```
Catalyst3750(config)# crypto isakmp policy 1 //configuración de la política IKE con prioridad 1
```

Catalyst3750 (config-isakmp-policy)# authentication pre-share //establece el modo de autenticación una clave precompartida

Catalyst3750 (config-isakmp-policy)# hash md5 //establece md5 como algoritmo de hash para garantizar la integridad

Catalyst3750 (config-isakmp-policy)# group 1 //especifica el identificador de grupo de Diffie-Hellman en la política IKE

Catalyst3750 (config-isakmp-policy)# encryption 3des //especifica 3DES como algoritmo de cifrado

Catalyst3750(config-isakmp-policy)# lifetime 86400 // tiempo de vida en segundos para la SA

Catalyst3750 (config-isakmp-policy)# exit

Catalyst3750(config)# crypto isakmp key 0 hh87fkqwfw address ipv6 2800:0068:16:1001:D01:1220:1023:006/128 //define la clave precompartida, en texto plano, “0”, y la IP del que será el otro extremo del túnel en formato IPv6

Catalyst3750 (config)# crypto keyring ANILLO //define el nombre del keyring que se usará durante la autenticación

Catalyst3750 (config-keyring)# pre-shared-key address ipv6 2800:0068:16:1001:D01:1220:1023:006/128 key hh87fkqwfw //define la clave precompartida a usar durante la autenticación IKE

Catalyst3750 (config-keyring)# exit

Catalyst3750 (config)# crypto ipsec transform-set TRANSFORMADA esp-3des //define un transform-set, es decir, una combinación de protocolos y algoritmos que sea aceptable por routers IPSec

Catalyst3750 (cfg-crypto-trans)# crypto ipsec profile PERFIL //define los parámetros que se van a usar para el cifrado IPSec entre los dos routers

Catalyst3750 (ipsec-profile)# set transform-set TRANSFORMADA //especifica transform-set el

Catalyst3750 (ipsec-profile)# exit

Catalyst3750(config)# interface tunnel 1 //configuración de la interfaz virtual tunnel 1

Catalyst3750 (config-if)# ipv6 address 2800:0068:16:3002:C02:1200:0023:12/64

Catalyst3750 (config-if)# ipv6 enable

Catalyst3750 (config-if)# tunnel source 2800:0068:16:1001:D01:1220:1023:007 //orígen del túnel

Catalyst3750 (config-if)# tunnel destination 2800:0068:16:1001:D01:1220:1023:6 //destino del túnel

Catalyst3750 (config-if)# tunnel mode ipsec ipv6 //establece el modo de encapsulamiento para la interfaz tunnel 0

Catalyst3750 (config-if)# tunnel protection ipsec profile PERFIL //asocia la interfaz tunnel 0 con el perfil

Si el procesamiento IPSec es aplicado, la entrada incluirá una especificación de SA (o grupo de SA), como son el listado de protocolos IPSec, los modos, y algoritmos que se emplearán e incluirán cualquier requisito relacionado. La SPD se utiliza para controlar todo el flujo de tráfico en IPSec incluyendo seguridad, manejo de claves (por ejemplo ISAKMP), tráfico entrante y saliente de entidades detrás de una puerta de enlace. Esto significa que el tráfico ISAKMP se debe referenciar explícitamente en la SPD, caso contrario será descartado.

Base de datos de asociación de seguridad (SAD). Cada SA tiene una entrada en la SAD y cada entrada define los parámetros asociados a esa SA. Para el procesamiento de entrada, cada entrada en la SAD es indexada por una dirección IP de destino el tipo de protocolo IPSec y SPI. Para el procesamiento de entrada los siguientes campos del paquete se usan para buscar la SA en la SAD y son requeridos para toda implementación:

- **Dirección IP de Destino**: La dirección de destino IPv6.
- **Protocolo IPSec:** AH o ESP. Usado como un índice para buscar la SA en esta base de datos. Especifica el protocolo IPSec aplicado al tráfico en esta SA.
- **SPI.** Es un valor de 32 bits que se usa para diferenciar SA’s diferentes que tienen el mismo destino (la misma dirección IP de destino) y que usan el mismo protocolo IPSec.

Para cada uno de los selectores definidos, la entrada de la SA en la SAD debe contener el valor o los valores que fueron negociados para esa SA cuando fue creada. Para el emisor, estos valores se utilizan para decidir si una SA dada es apropiada para usarse con un paquete de salida. Esto es parte de la comprobación para saber si una SA existente puede ser utilizada. Para el receptor, este valor es utilizado para comprobar que los valores de los selectores en un paquete de entrada concuerdan con aquellos para la SA. Para el receptor esta es parte de la verificación de que la SA fue la correcta para el paquete.

Los siguientes campos de la SAD son usados en el procesamiento IPSec:

- **Contador de número de secuencia.** Un valor de 32 bit usado para generar el campo Número de Secuencia de la cabecera AH o ESP. Requerido por toda implementación, es usado exclusivamente por el tráfico saliente. El valor obtenido de la simulación es: conn id: 17, flow_id: SW:17, crypto map: Tunnel0-head-0
- **Desbordamiento del contador de secuencia.** Indica si el desbordamiento del Contador del Número de Secuencia debería generar un acontecimiento auditable y prevenir la transmisión de los paquetes adicionales en la SA. Esto es requerido por toda implementación, se usa solamente para el tráfico saliente. En este caso no se obtuvo ningún valor puesto que no hubo tal evento.
- **Ventana anti-replay.** Un contador de 32 bits y un asignador de bits (bit-map) usado para determinar si un paquete AH o ESP es un paquete duplicado. Este debe ser requerido por toda implementación, pero es usado solamente para el tráfico entrante. En la simulación, el resultado da un valor N que significa que no se configuró la detección de paquetes duplicados: replay detection support: N
- **Algoritmo de claves de autenticación AH.** Es requerido esencialmente por la implementación AH. En el caso de esta simulación, no se muestran valores puesto que se está usando el modo túnel.
- **Algoritmo de claves de encriptación ESP.** Este es requerido esencialmente por la implementación ESP. De la simulación se obtuvo lo siguiente: transform: esp-3des
- **Algoritmo de autenticación ESP:** Si el servicio no se selecciona este campo será nulo, debe ser requerido por la implementación ESP, en este caso se obtuvo lo siguiente:

Protection suite of priority 1

encryption algorithm: Three key triple DES
hash algorithm: Message Digest 5
authentication method: Pre-Shared Key
Diffie-Hellman group: #1 (768 bit)

- **Tiempo de vida de la SA:** Un intervalo de tiempo después del cual una SA debe ser remplazada por una nueva SA. En la simulación se determinó el siguiente valor:

lifetime: 86400 seconds, no volume limit

Cuando el tiempo de vida de la SA está por terminar, se genera un indicador que determinará cuando se debe realizar el reemplazo de la SA, el primer tiempo de vida de la SA que expire es el que tiene prioridad en la creación de la siguiente SA, la misma que se crea por medio de IKE que en este caso se encargada de generar el certificado compuesto por la clave pública, necesario para la creación de la nueva SA.

1.5.4 Gestión de claves del SA.

AH y ESP son independientes de la forma de gestión aplicada a las SA, en general la autenticación del origen de los datos en AH y ESP está limitada por el alcance en el uso del algoritmo de autenticación que se comparten entre las múltiples fuentes posibles.

- **Gestión Manual.-** La forma más simple de gestión de claves es permitiendo que el administrador de red configure cada nodo con la clave de las SA. Se usa en ambientes estáticos pequeños, pero la escalabilidad es mala.
- **Gestión Automatizada.-** Facilita el uso de las características anti-replay de AH y ESP, adicionalmente permite una adecuada creación de SA bajo demanda, en el caso del uso de claves orientadas a usuarios o a sesiones.

El protocolo de gestión de claves automáticas por defecto que usa IPSec es IKE bajo el Domino de Interpretación (DOI) de IPSec, a través de ISAKMP donde existe un repositorio de claves generadas automáticamente denominado keyring. Para garantizar que las implementaciones IPSec en cada extremo de la SA usan los mismos bits para las mismas claves, de esta manera la clave o claves encriptadas deben ser extraídas del keyring.

En el caso de la Universidad Politécnica Salesiana se recomienda la gestión de claves manual puesto que en número de enlaces a proteger no es demasiado grande en una primera instancia, si el proyecto se implementara a nivel nacional se torna necesario la administración automatizada por medio del ISAKMP.

1.5.5 Cabecera de autenticación (AH)

Esta cabecera garantiza la integridad y autenticación del origen de los datagramas IP, sin embargo no proporciona ninguna garantía de confidencialidad. Está entre la cabecera IPv6 y el payload, adicionalmente proporciona protección contra reenvíos siempre y cuando ninguno de los campos de la cabecera IP cambien durante el transporte.

AH se puede aplicar solo, en combinación con la carga de seguridad encapsulada llamada ESP, o a través de la modalidad anidada usando el modo túnel. Los servicios de seguridad pueden suministrarse, entre hosts, entre un par de puertas de enlace o entre una puerta de enlace y un host. ESP puede ser usado para proporcionar servicios de seguridad y confidencialidad como la autenticación del origen de datos, protección anti-replay, confidencialidad.

En el caso de la simulación se usó los siguientes servicios:

(config-isakmp-policy)# authentication pre-share.- establece el modo de autenticación con clave precompartida, solamente el modo pre-share es soportado por IPv6, los modos RSAencr y RSAsig son soportados por IPv4.

(config-isakmp-policy)# hash md5 .- establece md5 o message digest 5 como algoritmo de hash para garantizar la integridad, las opciones adicionales son SHA o secure hash algorithm, se escogió MD5 puesto que genera una salida de 128 bits a diferencia de SHA que lo hace con 160 bits (Stallings, 2004), convirtiendo a MD5 en más eficiente.

(config-isakmp-policy)# group 1.- especifica el método de intercambio de claves con el identificador de grupo de Diffie-Hellman en la política IKE, las opciones son: 1 para un identificador de grupo de 768 bits, 2 para un identificador de 1024 bits y 5 para un identificador de 1536 bits (ciscoipv6ttechtips, 2011), los grupos 2 y 5 ofrecen una seguridad más efectiva

pero su rendimiento es pobre, se escogido el grupo 1 por el rendimiento que ofrece dentro del túnel IPSec (Watch Guard System Manager Help, 2010).

(config-isakmp-policy)# encryption 3des.- especifica 3DES como algoritmo de cifrado, se escogió este tipo de encriptación porque es ampliamente usado en entornos de seguridad, sin embargo está siendo desplazado por AES puesto que este último es más seguro y eficiente, las opciones a configurar son: DES, 3DES, AES, AES 192, AES 256, se recomienda en la implementación usar AES256 por su nivel de seguridad.

El protocolo AH protege la integridad del datagrama IP, calculando una HMAC basada en la clave secreta, el contenido del paquete y las partes fijas de la cabecera IP, específicamente las direcciones IP. Tras esto, añade la cabecera AH al paquete, como se muestra en la figura 11. La función de AH se basa en un algoritmo HMAC, es una porción de información utilizada para autenticar un mensaje, los valores MAC se calculan mediante la aplicación de una función hash con clave secreta K, que sólo conocen el remitente y destinatario, la función hash toma dos argumentos: una clave K de tamaño fijo y un mensaje M de longitud arbitraria. El resultado es un código MAC que administra las funciones de autenticación del mensaje, que en este caso es un código de longitud fija.

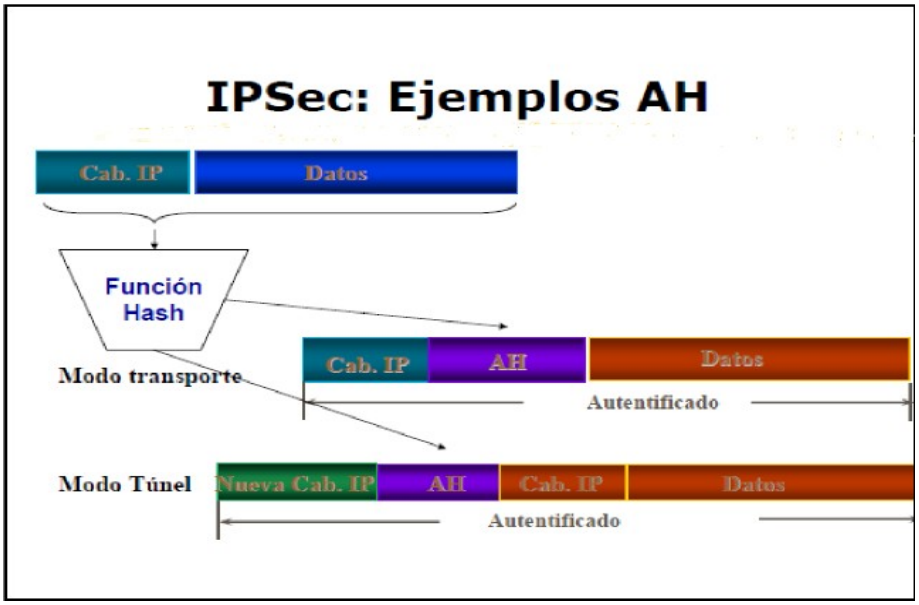

Figura 11 Funcionamiento de la Cabecera de Autenticación
Fuente: (Uribe & Mariela, 2012)

1.5.6 Estructura de la cabecera de autenticación.

AH asegura la integridad de los datos por un proceso que realiza la suma de comprobación que genera un código de autenticación de mensajes, como por ejemplo MD5. Los campos de esta cabecera se detallan en la figura 12.

0 - 7 bit	8 - 15 bit	16 - 23 bit	24 - 31 bit
Next header	Payload length	RESERVED	
Security parameters index (SPI)			
Sequence number			
Hash Message Authentication Code (variable)			

Figura 12 Estructura de la Cabecera de Autenticación
Fuente: (Anónimo, 2012)

Los campos contenidos por esta cabecera son los siguientes:

- **Cabecera Siguiente.** Es un campo de 8 bits que identifica el tipo de carga siguiente después de la cabecera de autenticación. Identifica cuál es el protocolo que será autenticado y cuál es el payload. Por ejemplo indicará si la siguiente cabecera es ESP o una cabecera de ruteo.
- **Campo Tamaño de los Datos.** Este campo de 8 bits especifica la longitud de la cabecera de autenticación, en palabras de 32 bit (dispuesto en unidades de 4 bytes), de esta manera la longitud de la carga se calcula restando 32 bits de los 64 bits del paquete IPv6.
- **Campo Reservado.** Este permite reservar para futuras aplicaciones. Debe estar a 0, ya que este campo es de 16 bits.
- **Campo Índice de Parámetros de Seguridad SPI.** Indica los parámetros de seguridad que, en combinación con la dirección IP, identifican la asociación de seguridad implementada, es un valor arbitrario de 32 bits que, conjuntamente con la dirección de destino IP y el protocolo de seguridad (AH), identifican a la Asociación de Seguridad para este datagrama.
- **Campo Número de Secuencia.** Es utilizado para evitar ataques de repetición para asegurar la protección contra la copia, modificación o reproducción. Identifica en número del datagrama en la comunicación,

estableciendo un orden y evitando problemas de entrega de datagramas fuera de orden.

- **Campo Datos de Autenticación.** Este campo asegura que la longitud de la cabecera AH sea de 64 bits de longitud. En este campo se encuentra el algoritmo que aplica la función hash que es aplicado a los datos de entrada junto con la clave precompartida, la que en el caso de la simulación fue MD-5.

1.5.7 Localización de la cabecera de autenticación

La localización de AH está en relación directa al modo de trabajo en que esté trabajando IPSec.

AH en modo de transporte. La cabecera IP del datagrama se encuentra en la parte más externa de la cabecera IP, seguida de la cabecera AH y, a continuación, la carga útil del datagrama. AH autentica el datagrama entero, a excepción de los campos que varían durante el transporte. En la figura 13, se muestra la ubicación de la cabecera AH.

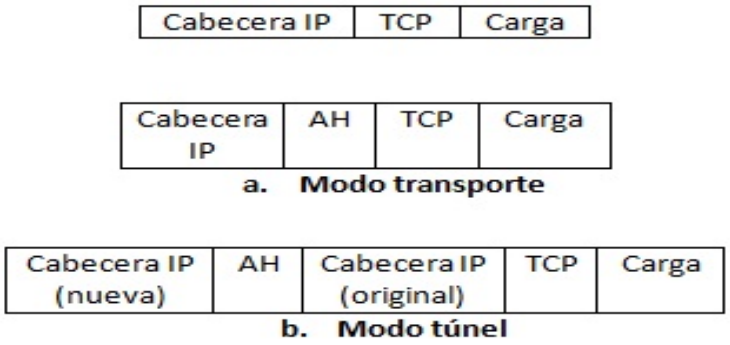

Figura 13 Ubicación de la cabecera AH en Modo Transporte y Modo Túnel
Fuente: (Ingeniería de la Seguridad, 2012)

AH se inserta después de la cabecera IP y antes del protocolo de capa superior, se ve como carga extremo a extremo (end-to-end), y debe aparecer después de las cabeceras de extensión: salto-por-salto (hop-by-hop), de encaminamiento (routing), y de fragmentación. Las opciones de las cabeceras de extensión podrían aparecer antes o después de la cabecera AH.

AH en modo túnel. Se crea una nueva cabecera IP y la utiliza como parte más externa del datagrama. La cabecera AH continúa en la nueva cabecera IP. El datagrama original (tanto la cabecera IP como la carga útil original) aparece

en último lugar. AH autentica el datagrama entero, por lo tanto, el sistema que responde puede detectar si el datagrama ha cambiado por el camino. Las direcciones de origen y destino de la parte más externa de la cabecera IP no tienen necesariamente que ser iguales que las direcciones de la cabecera IP original puesto que en este modo la cabecera IP interna lleva la última dirección de origen y de destino, mientras que la cabecera IP externa puede contener otras direcciones IP, por ejemplo direcciones de security gateway o de routers, en el caso de que las direcciones sean las mismas, implica que la cabecera no ha pasado por ningún dispositivo de seguridad intermedio, es decir es un enlace punto punto.

La cabecera AH protege a toda la cabecera interna. La posición de la AH respecto a la cabecera IP externa es la misma que en el modo transporte.

1.5.8 Algoritmo HMAC MD5.

Es una función matemática de un solo sentido, aplicado a un bloque de datos, produce una representación única de 128 bits del bloque y el resultado obtenido es una representación comprimida y codificada de un bloque más grande de datos. Cuando se usa de esta manera, MD5 garantiza sólo la integridad en los datos. El mensaje codificado es sometido a un proceso de cálculo partiendo de un bloque de datos antes de que se envíe y otra vez después de que los datos han sido recibidos, si los resultados en ambos lados son iguales, el bloque de datos no fue alterado en la transmisión.

La autenticidad está garantizada mediante el uso de llaves secretas cuando se calcula el mensaje codificado. El método HMAC usa el algoritmo básico MD5 para calcular los mensajes codificados, pero opera en bloques de datos de 64 bytes que sirven como entrada de un bloque entero de datos que también usa una llave secreta, la que es conocida sólo por los sistemas que se están comunicando cuando se realiza el cálculo de la codificación.

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. Este se envía al receptor, que 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, se concluye 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.

1.5.9 Cabecera de seguridad encapsulada (ESP).

Proporciona confidencialidad, define la forma de cifrar los datos que se desean enviar y la manera de incluir los datos cifrados en el datagrama IP. Ofrece los servicios de integridad y autenticación del origen de los datos incorporando un mecanismo similar al de AH. La estructura de ESP consiste en una cabecera y una cola que rodean los datos a transportar.

ESP cifra los datos por medio de clave simétrica, usa algoritmos de cifrado por bloques, de modo que la longitud de los datos a cifrar tiene que ser un múltiplo del tamaño de bloque, la mayoría de casos es de 8 o 16 bytes. Esta cabecera se usa para proporcionar confidencialidad, autentificación del origen de los datos, integridad sin conexión, confidencialidad limitada del flujo de tráfico.

1.5.10 Funcionamiento de ESP.

ESP proporciona un conjunto de servicios de seguridad, los que pueden ser aplicados solos, o en conjunto con la AH, o a su vez en forma anidada cuando se usa el modo túnel. Esta cabecera se inserta antes que la cabecera IP y después que la cabecera de protocolo de capa superior cuando se trabaja en modo transporte o después de una cabecera IP encapsulada si es que se está en modo túnel. El conjunto de servicios proporcionados depende de las opciones seleccionadas al momento del establecimiento de la SA, los mismos que ya han sido especificados en el apartado 1.5.5. La confidencialidad puede ser seleccionada independientemente del resto de los servicios, se recomienda el uso de la confidencialidad con integridad y autentificación en ESP o AH. La autenticación del origen de los datos y la integridad sin conexión son servicios que están unidos y son ofrecidos como una opción. La confidencialidad del flujo de tráfico requiere de la selección del modo túnel. La confidencialidad y la autentificación son opcionales, sin embargo al menos una de ellas debe ser seleccionada. En la figura 14 se detallan los procesos a realizarse.

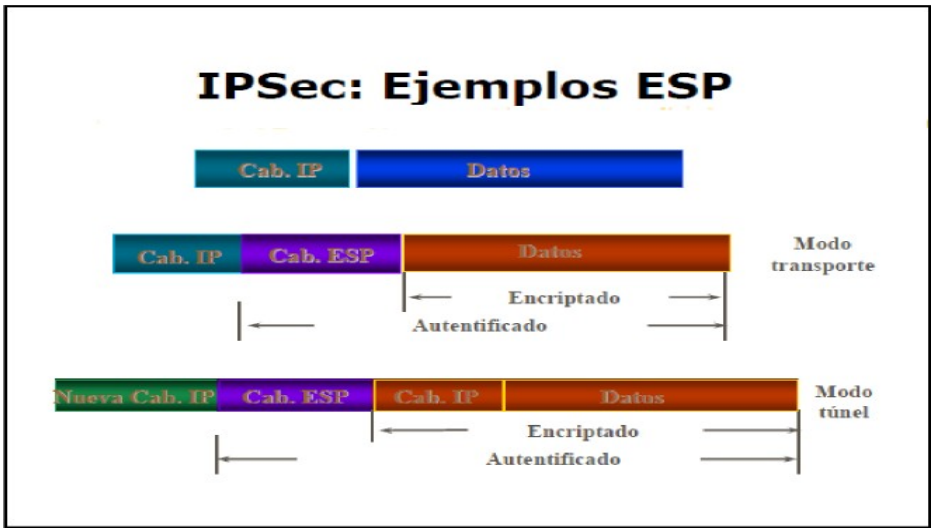

Figura 14 Funcionamiento de ESP
Fuente: (Uribe & Mariela, 2012)

El emisor toma el mensaje original, lo cifra, utilizando una clave determinada, y lo incluye en un paquete IP, a continuación de la cabecera ESP, en el destino, el receptor aplica de nuevo el algoritmo de cifrado con la misma clave, recuperando los datos originales. La distribución de claves de forma segura es esencial para el funcionamiento de ESP, tanto el emisor y el receptor deben estar de acuerdo en el algoritmo de cifrado y en los parámetros comunes.

1.5.11 Estructura de ESP.

El formato o estructura de ESP está basado en varios campos que contendrán diferentes bits y cada uno de estos campos tienen una función importante en la cabecera de IPv6, como se muestra en la figura 15.

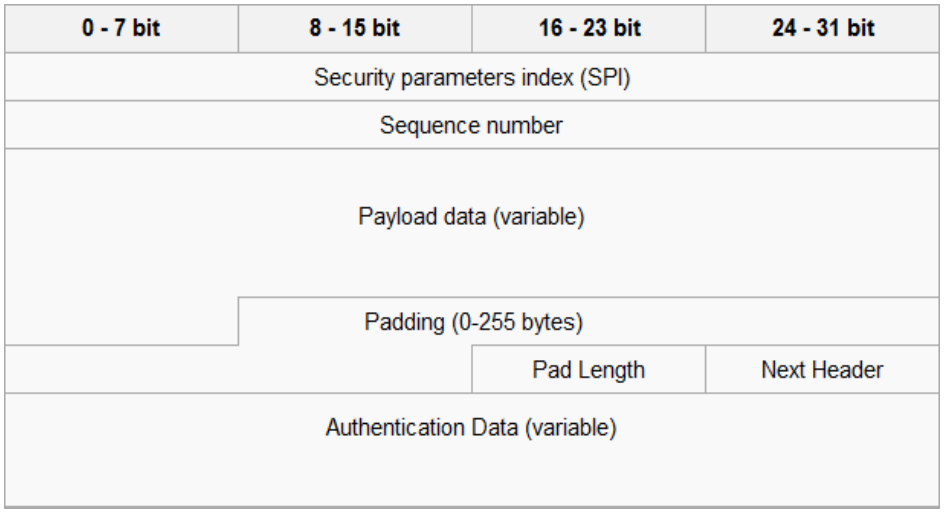

Figura 15 Estructura de ESP
Fuente: (Anónimo, 2012)

- **Campo Índice de Parámetros de Seguridad (SPI).** Identifica los parámetros de seguridad en combinación con la dirección IP. La necesidad del SPI se hace evidente cuando tiene más de una comunicación con la misma dirección IP de destino y protocolo de seguridad AH o ESP.
- **Campo Número de Secuencia.** Es un número siempre creciente, utilizado para evitar ataques de repetición. Este campo es obligatorio y debe estar siempre presente incluso si el receptor elige no habilitar el servicio de anti- replay para una SA en particular, como se especificó antes este servicio previene la duplicación de la cabecera ESP en este caso, que se aplica al tráfico entrante a la interface, cuando la asignación de claves es manual, anti replay se deshabilita. El procesamiento del campo Número de Secuencia está a criterio del receptor, es decir, el emisor debe transmitir siempre este campo, pero el receptor no necesita actuar sobre él.
- **Campo Datos de Carga Útil.** Es un campo de longitud variable que contiene los datos del paquete IP original descritos por el campo siguiente cabecera, es obligatorio y debe tener una longitud de un número entero de bytes.
- **Campo Relleno.** El relleno se basa en 0 a 255 octetos. Se lo usa para la encriptación, y permite ampliar los datos de carga útil con un tamaño que se ajusta a la encriptación, adicionalmente sirve para alinear el siguiente campo.

- **Campo Longitud de Relleno.** Este tipo de campo indica el número de bytes de relleno El rango de valores válidos es de 0 a 255 bytes, donde un valor de cero indica que no hay bytes de relleno presentes. Este campo es obligatorio.
- **Campo Siguiente Cabecera.** Identifica el protocolo de los datos transferidos.
- **Campo Datos de Autenticación.** Contiene los datos utilizados para autenticar el paquete. En este campo se determina la longitud variable y contiene el Valor de Comprobación de Integridad (ICV) calculado sobre el paquete ESP, menos los datos de autenticación.

1.5.12 Localización de ESP.

La localización de la cabecera de seguridad encapsulada se puede hacer de dos formas: Modo de Transporte y Modo Túnel.

- **Modo de Transporte ESP.** En este modo el contenido transportado dentro del datagrama AH o ESP son datos de la capa de transporte. Por tanto, la cabecera IPSec se inserta inmediatamente a continuación de la cabecera IP y antes de los datos de los niveles superiores que se desean proteger. El modo transporte tiene la ventaja de que asegura la comunicación extremo a extremo, pero requiere que ambos extremos entiendan el protocolo IPSec
- **Modo Túnel.** El datagrama AH o ESP es un datagrama IP completo, incluida la cabecera IP original. El modo túnel se usa normalmente cuando el destino final de los datos no coincide con el dispositivo que realiza las funciones IPSec. Se emplea principalmente por los gateway IPSec, con objeto de identificar la red que protegen bajo una misma dirección IP y centralizar de este modo el procesado del tráfico IPSec en un equipo. Adicionalmente es útil, cuando se utiliza junto con ESP, para ocultar la identidad de los nodos que se están comunicando.

1.5.13 Protocolo de intercambio de claves en internet (IKE).

IKE emplea el puerto 500 UDP para su comunicación. Este tipo de protocolo funciona en dos fases. La primera fase establece un ISAKMP SA (Asociación de seguridad del protocolo de gestión de claves de asociaciones de seguridad en Internet).

En la segunda fase, el ISAKMP SA se emplea para negociar y establecer las SA's de IPSec.

La primera fase suele soportar dos modos distintos, el modo principal y el modo agresivo. Ambos modos por igual autentican al host en el proceso de la comunicación de los datos y establecen un ISAKMP SA, aunque el modo agresivo solamente usa la mitad del mensaje para enviar los datos protegidos al otro host, sin embargo este modo presenta una vulnerabilidad puesto que no soporta la protección de identidades y, por lo tanto cuando se trabaja bajo esta modalidad, los datos son susceptibles a un ataque.

En la segunda fase, se intercambia propuestas de asociaciones de seguridad y se negocian asociaciones de seguridad y autenticación basándose en ISAKMP SA, en la comunicación sólo negocian una ISAKMP SA, que se emplea para negociar varias SA's unidireccionales.

1.5.14 Arquitectura de IKE.

El protocolo IKE define en su arquitectura dos fases que determinan la estructura para el establecimiento de un canal auténtico y seguro entre dos usuarios. Utiliza la misma infraestructura de mensajes del protocolo ISAKMP para el intercambio de mensajes, como se puede apreciar en la figura 16.

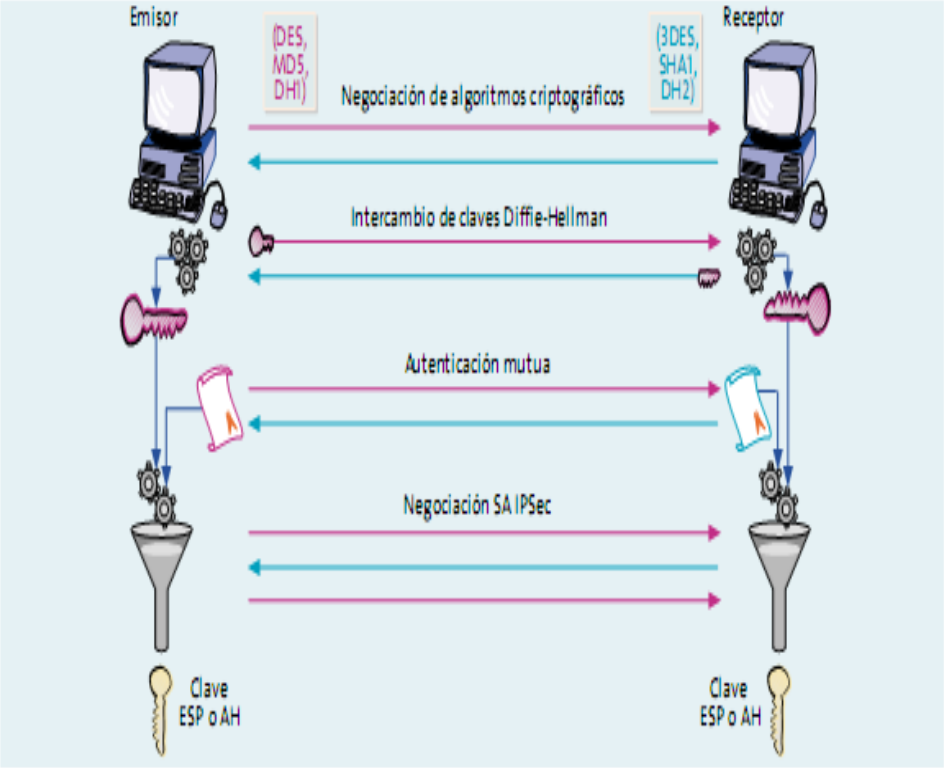

Figura 16 Funcionamiento del Protocolo IKE
Fuente: (Gonzáles & Jose)

Para cada una de las fases se debe tener en cuenta la notación con su significado, tal como se muestra en la tabla 5.

Tabla 5
Notación con sus significados para la Arquitectura del Protocolo IKE

HDR:	Cabecera ISAKMP.
HDR*:	Cabecera cifrada
HASH:	Función Hash.
KE:	Valor público Diffie-Hellman.
SA:	Asociación de seguridad.
Ni y Nr:	Valor temporal (Nonce payload).
[Cert] y SIG:	Certificado y firma digital.
ID:	Identificador.
PubK:	Clave pública.
[ ]:	Opcional.

- **Fase1.** Se negocian las SA, usa el protocolo Diffie-Hellman para el intercambio de una clave común y establece el algoritmo de cifrado 3DES-CBC, el algoritmo de Hash MD5 y del sistema de autenticación. El emisor y el

receptor quedan autenticados mediante cualquiera de las siguientes operaciones:

Autenticación con claves pre-compartidas (Pre-shared Keys).

Autenticación mediante firmas digitales (Digital Signatures).

Autenticación mediante clave pública 1.

Autenticación mediante clave pública 2.

En el caso de la simulación se usó la autenticación con claves pre-compartidas puesto que solamente el modo pre-share es soportado por IPv6, los modos RSAencr o encriptación por RSA y RSAsig o firma digital con RSA sólo son soportados por IPv4

- **Fase 2.** Una vez establecidos los distintos parámetros iníciales de las SA, se inicia un modo rápido (Quick Mode) dónde se vuelven a negociar las SA con el objetivo de evitar ataques de reutilización (Replay) de los datagramas de la fase 1.

Intercambio de claves. Hay dos métodos básicos usados para establecer un intercambio de claves autentificado: El Modo Principal y el Modo Agresivo, cada uno genera material clave autenticado a partir de un intercambio de Diffie-Hellman. El modo principal **debe** ser implementado para establecer un intercambio de claves, el modo agresivo **debería** ser implementado y el modo rápido **se debe** implementar como mecanismo para generar nuevo material clave y negociar servicios de seguridad.

- **Modo Principal.** Asegura la confidencialidad y autenticación en los hosts donde se va a realizar la comunicación, como se observa en la figura 1.17 los dos primeros mensajes se utilizan para la negociación de la política de seguridad para el intercambio. Los siguientes dos mensajes se utilizan como material de claves mediante intercambio Diffie-Hellman. Los últimos dos mensajes se destinan para la autenticación de los pares con las firmas y certificados opcionales cifrados con la clave previamente negociada.

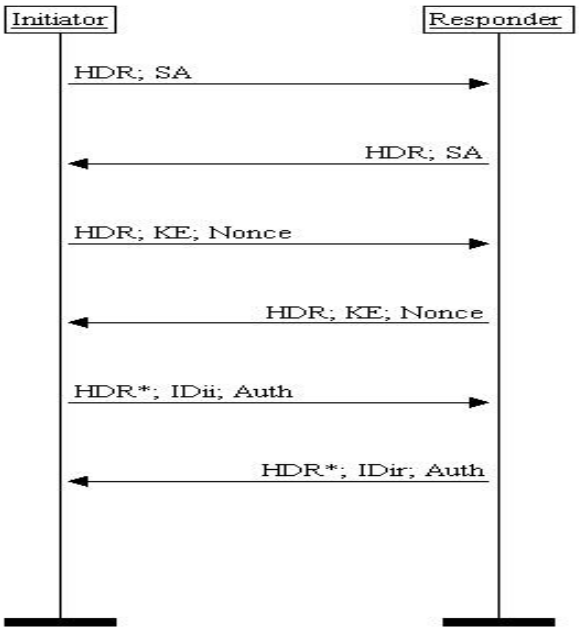

Figura 17 Modo Principal del Protocolo IKE
Fuente: (Savolainen, 2000)

- **Modo Agresivo.** Tiene la misma funcionalidad del modo principal, pero utiliza la mitad de los mensajes para alcanzar su objetivo y no soporta la protección de identidades por lo que es menos seguro.

Este modo transmite la información del usuario de forma clara, permitiendo conocer la identidad del host antes que la autenticación se lleve a cabo. Como se muestra en la figura 18, el primer mensaje negocia la política, intercambia los valores y los datos necesarios para su identificación. El segundo mensaje autentica al emisor y detecta la política y el intercambio de datos que se está realizando entre el emisor y el receptor. El último mensaje se utiliza para la autenticación del emisor y proporciona una prueba de la participación en el intercambio.

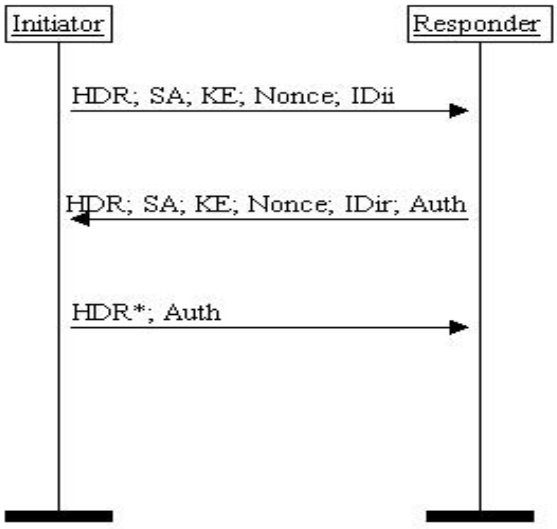

Figura 18 Modo Agresivo del Protocolo IKE
Fuente: (Savolainen, 2000)

La negociación de SA está limitada en el Modo Agresivo, debido a los requerimientos en la construcción de mensajes, el grupo en el cual el intercambio de Diffie-Hellman se ejecuta no puede ser negociado. Además, métodos de autenticación diferentes pueden limitar aún más la negociación de los atributos.

- **Modo Rápido.** Se utiliza para el intercambio en la segunda fase de IKE, está orientado a la negociación de SA y la generación de material de claves nuevas. Todas las cargas útiles, excepto el encabezado ISAKMP están cifradas, el intercambio de claves Diffie-Hellman aumenta la confidencialidad, en este modo, una carga hash debe seguir inmediatamente a la cabecera ISAKMP y una carga SA debe seguir inmediatamente al hash, como se puede apreciar en la figura 19.

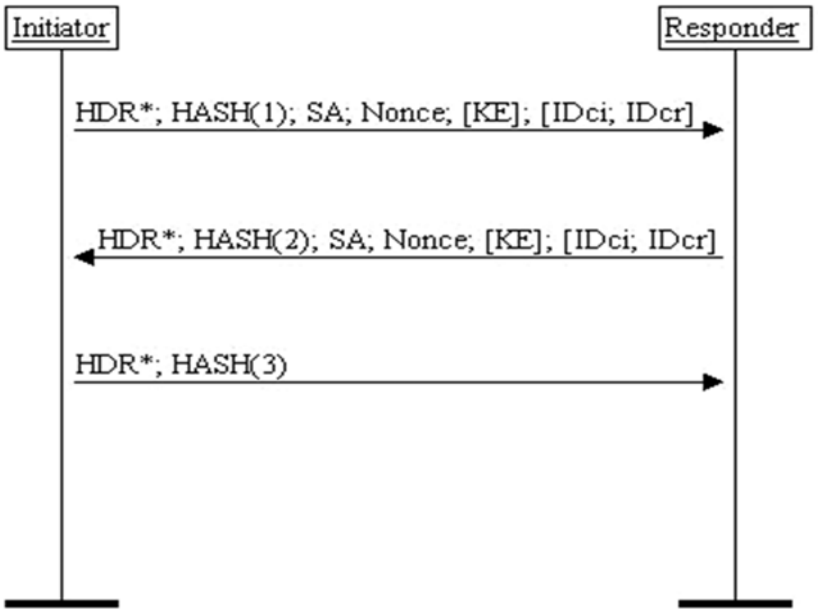

Figura 19 Modo Rápido del Protocolo IKE
Fuente: (Savolainen, 2000)

Tomando como criterio el establecimiento del método de autenticación en ambos extremos y el método de intercambio de claves con el identificador de grupo de Diffie-Hellman en la política IKE, donde las opciones de configuración son: 1 para un identificador de grupo de 768 bits, 2 para un identificador de 1024 bits y 5 para un identificador de 1536 bits (ciscoipv6ttechtips, 2011), los grupos 2 y 5 ofrecen una seguridad más efectiva pero su rendimiento es pobre, se ha escogido el grupo 1 por el rendimiento que ofrece dentro del túnel IPSec (Watch Guard System Manager Help, 2010),por lo tanto el intercambio de claves se realiza en el modo principal.

El método agresivo no se escogió por tener menor seguridad, de la misma manera el método rápido no se tomó en cuenta puesto que no se realiza una generación de claves automáticas en la simulación.

1.5.15 Protocolo de gestión de claves y asociación de seguridades en internet (ISAKMP).

Este protocolo es el escogido para el intercambio de claves y parámetros de seguridad en IPSec, normalmente utiliza IKE para el intercambio de claves, adicionalmente ISAKMP define los procedimientos y formatos de paquetes para establecer, negociar, modificar y eliminar las SA. Proporciona un marco

coherente para la transferencia de claves y datos de autenticación, el mismo que es independiente de la técnica de generación de claves, el algoritmo de cifrado y el mecanismo de autenticación.

1.5.16 Funcionamiento del protocolo ISAKMP.

Este protocolo define los procedimientos para autenticar comunicaciones entre los host, la creación y administración de SA, y las técnicas de generación de claves; negocia, establece, modifica y cancela las SA.

Negociado el Protocolo ISAKMP. Las SA deben soportar los algoritmos de encriptación, autenticación y mecanismos de establecimiento de claves para IPSec. ISAKMP no está sujeto a ningún algoritmo criptográfico específico, técnica de generación de claves o mecanismo de seguridad, por lo que soporta ambientes de comunicaciones dinámicos.

Fases de la Negociación. ISAKMP ofrece dos fases para la negociación.

- **Fase 1.** Dos entidades concuerdan en cómo proteger futuras negociaciones del tráfico entre ellas mismas, estableciendo una SA ISAKMP, que es luego usada para proteger las negociaciones requeridas por las SA de los Protocolos. Dos entidades pueden negociar múltiples SA ISAKMP.
- **Fase 2.** La negociación es usada para establecer las SA para otros protocolos de seguridad, que pueden ser usadas para proteger los intercambios de datos o mensajes.

1.5.17 Arquitectura del protocolo ISAKMP.

Tiene una cabecera de tamaño fijo seguido por un número de cargas variables, donde cada campo realiza una función específica para la seguridad del mensaje, tal como lo muestra la figura 20.

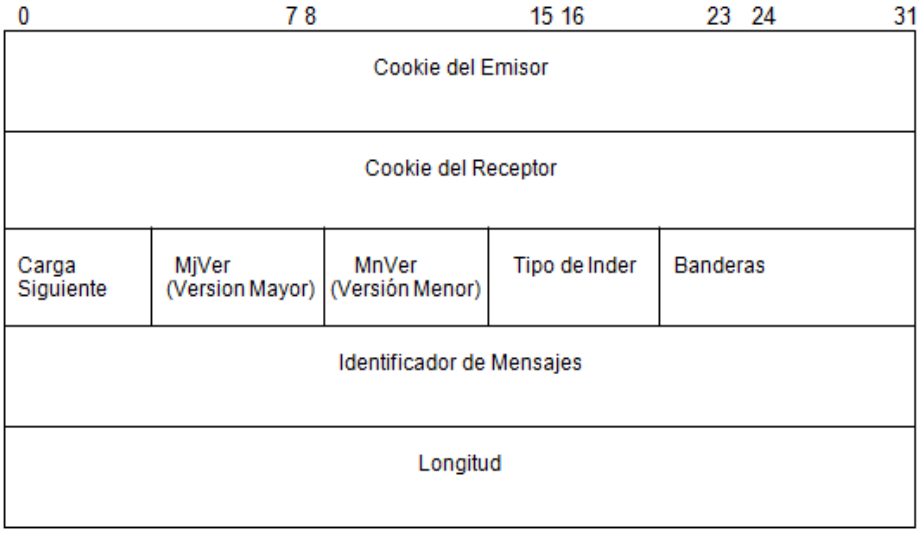

Figura 20 Formato de la Cabecera ISAKMP

Los campos de la Cabecera ISAKMP son:

- **Cookie del Emisor.** Inicia el establecimiento, modifica, o cancela la SA.
- **Cookie del Receptor.** Responde al requerimiento del establecimiento de una SA, o cancelación de la SA.
- **Carga siguiente.** En el primer mensaje, este campo indica el tipo de carga que contienen los siguientes mensajes.
- **Versión Mayor.** Indica la versión mayor del protocolo ISAKMP en uso.
- **Versión Menor.** Indica la versión menor del protocolo ISAKMP en uso. Las implementaciones basadas en Internet de ISAKMP debe fijar la versión menor en cero. Las implementaciones nunca deben aceptar paquetes con un número de versión superior a estos, dado que los números de la versión mayor son idénticos.
- **Tipo de intercambio.** Indica el tipo de intercambio usado. Este indica a los host los mensajes y la carga en los intercambios de ISAKMP.
- **Banderas (Flags).** Indica las opciones específicas que se fijan para los intercambios ISAKMP.
- **Identificador (ID) de Mensaje.** Solamente se usa para identificar el protocolo durante las negociaciones de la Fase 2. Este valor es generado aleatoriamente por el iniciador de la Fase.

En el caso de establecimientos simultáneos de SA, el valor de este campo será diferente porque son generados independientemente. Durante las negociaciones de la Fase 1, el valor debe ser cero.

- **Longitud.** Indica la longitud total del mensaje compuesto de cabecera más la carga, la encriptación puede expandir el tamaño de un mensaje ISAKMP.

1.5.18 Cabecera de carga genérica.

Proporciona una capacidad de encadenamiento de cargas y claramente define los límites de una carga. Su estructura se muestra en la figura 21.

Figura 21 Formato de la cabecera de carga genérica

Los campos de la cabecera de la carga genérica son definidos de la siguiente forma:

- **Carga Siguiente.** Identifica el tipo de carga de la siguiente carga en el mensaje. Si la carga actual es la última en el mensaje, este campo contendrá el valor cero. Este campo proporciona la capacidad de encadenamiento.
- **Reservado.** No es utilizado, debe contener ceros.
- **Longitud de la carga.** Indica la longitud de la carga actual en octetos, incluyendo la cabecera de carga genérica.

1.5.19 Cargas del protocolo ISAKMP

Entre estas cargas se determinan las siguientes:

- **Carga SA.** Usada para negociar los atributos de seguridad, para indicar el DOI y la situación, que es el conjunto de información que será utilizado para determinar los servicios de seguridad requeridos.

- **Carga de la Propuesta.** Contiene información usada durante la negociación de la SA. La propuesta consiste en mecanismos de seguridad, o trasformaciones, que serán usados para asegurar el canal de comunicaciones.
- **Carga de Transformación.** Consiste en un mecanismo de seguridad específico, con el objetivo de asegurar el canal de comunicación. También contiene los atributos SA asociados con la transformación específica.
- **Carga de Intercambio de Clave.** Soporta una variedad de técnicas de intercambio de claves.
- **Carga de Identificación.** Contiene datos específicos del DOI usados para intercambiar información de identificación. Está información es usada para determinar las identidades de los usuarios de la comunicación y puede ser usada para determinar la autenticación de la información.
- **Carga Hash.** Contiene los datos generados por la función hash que fue seleccionada durante el intercambio del establecimiento de la SA, sobre una parte del mensaje del estado de ISAKMP. Puede ser usada para verificar la integridad de los datos en un mensaje ISAKMP, o para la autenticación de las entidades de la negociación.
- **Carga Nonce.** Contiene información aleatoria para garantizar la vida de la conexión durante un intercambio y para proteger contra ataques de reenvío. Si el nonce es usado para un intercambio de clave particular, su uso será dictaminado por el intercambio de claves, puede ser trasmitido como parte de los datos del intercambio de claves, o como una carga separada.

1.5.20 Intercambio de claves de ISAKMP

Es una especificación de un número de mensajes en ISAKMP y los tipos de carga que están contenidos en cada uno de estos mensajes como los servicios de seguridad. Hay tipos de intercambio definidos por ISAKMP. La notación usada se muestra en la figura 22.

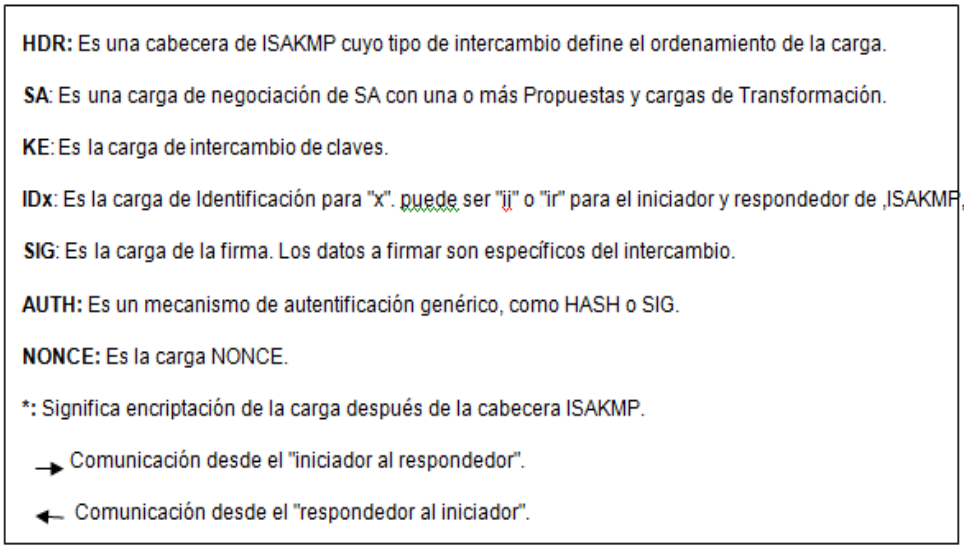

Figura 22 Notación con sus significados para el Intercambio de Claves de ISAKMP

Los intercambios definen los contenidos y el ordenamiento de los mensajes ISAKMP entre usuarios, los diferentes tipos de Intercambios son:

- **Intercambio Base.** Está diseñado para permitir que el Intercambio de Claves y la Autenticación puedan relacionarse con la información que trasmiten simultáneamente. Esta combinación relacionada dentro de un mensaje reduce el número de viajes de ida y vuelta a expensas de no proporcionar protección de identidad. El intercambio de mensajes se muestra en la figura 23

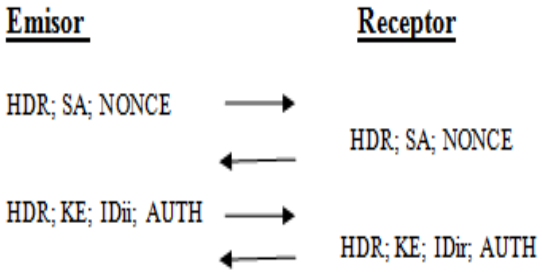

Figura 23 Intercambio base
Fuente: (Vásquez, 2011)

En el primer mensaje, el emisor genera una propuesta que considera adecuada para proteger el tráfico en una situación dada. Las cargas SA, la de la Propuesta, y la de Transformación, son incluidas en la carga SA. En el

segundo mensaje, el receptor indica el conjunto de protección que ha aceptado con las cargas, SA, la de la Propuesta, y la de Transformación. En el tercer y cuarto mensaje, el emisor y el receptor, respectivamente intercambian material clave usado para llegar a un secreto común compartido y a la identificación de la información. Esta información es trasmitida bajo la protección de una función de autenticación acordada.

Intercambio de Protección de Identidad. Está diseñado para separar la información de intercambio de claves de la identificación y de la información relacionada con la autenticación.

En la figura 24 se muestran los mensajes con las posibles cargas enviadas en cada mensaje.

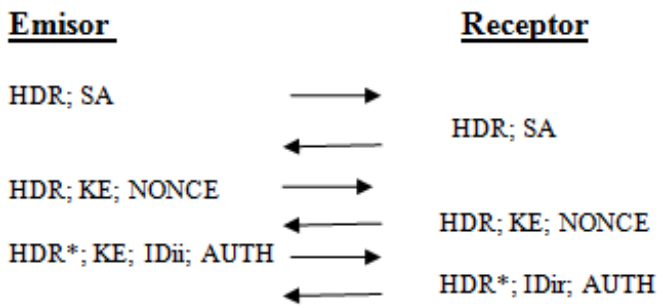

Figura 24 Intercambio de protección de identidad
Fuente: (Vásquez, 2011)

En el primer mensaje, el emisor genera una propuesta que considera adecuada para proteger el tráfico. En el segundo mensaje, el receptor indica el conjunto de protección que ha aceptado con las cargas, SA, la de la Propuesta, y la de Transformación. En el tercer y cuarto mensaje, el emisor y el receptor, respectivamente intercambian material clave usado para llegar a un secreto común compartido y la información aleatoria que es usada para garantizar la vida de la conexión y proteger contra ataques de renvío.

En el quinto y sexto mensaje, el emisor y el receptor, respectivamente, intercambian información de identificación y los resultados de la función de

autenticación acordada. Esta información es trasmitida bajo la protección de un secreto común compartido.

- **Intercambio de Autenticación.** Está diseñado para permitir solamente la autenticación relacionada con la información a trasmitir. Durante la negociación ninguna información trasmitida será encriptada. Sin embargo, la información puede ser encriptada en otros lugares. El intercambio de mensajes se muestra en la figura 25.

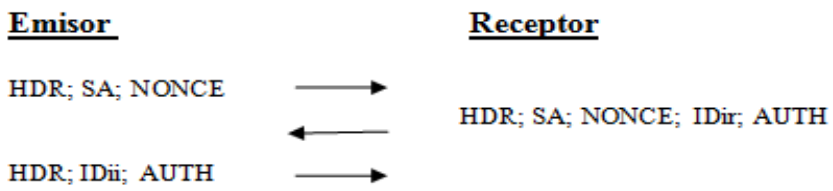

Figura 25 Intercambio de autenticación
Fuente: (Vásquez, 2011)

En el primer mensaje, el emisor genera una propuesta que considera adecuada para proteger el tráfico en una situación dada. Las cargas, SA, la de la Propuesta, y la de Transformación, son incluidas en la carga SA. En el segundo mensaje, el receptor indica el conjunto de protección que ha aceptado con las cargas, SA, la de la Propuesta, y la de Transformación. En el tercer mensaje, el emisor trasmite la información de identificación. Esta información es trasmitida bajo la protección de una función de autenticación acordada.

- **Intercambio Agresivo.** Permite que la SA, el intercambio de claves y las cargas relacionadas con la autenticación sean transmitidas en forma simultánea. Al combinar la SA, el intercambio de claves, y la información relacionada con la autenticación en un mensaje, reduce el número de viajes de ida y vuelta a expensas de no proporcionar la protección de identidad. El intercambio de mensajes en este modo se muestra en la figura 26.

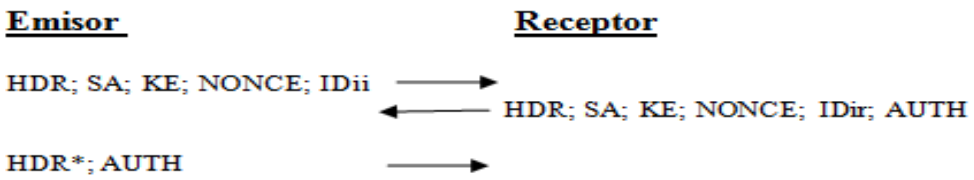

Figura 26 Intercambio agresivo
Fuente: (Vásquez, 2011)

En el primer mensaje, el emisor genera una propuesta que considera adecuada para proteger el tráfico para la situación dada. Las cargas, SA, la de la Propuesta, y la de Transformación, son incluidas en la carga SA (para simplificar la notación). Solamente puede existir una Propuesta y una Transformación ofrecida (es decir no hay elección) acordada para el funcionamiento del intercambio agresivo. En el segundo mensaje, el receptor indica el conjunto de protección que ha aceptado con las cargas, SA, la de la Propuesta, y la de Transformación. En el tercer mensaje, el emisor trasmite los resultados de la función de autentificación acordada. Esta información es trasmitida bajo la protección de un secreto común compartido:

- **Intercambio Informativo.** Permite una transmisión unidireccional de información que puede ser usada para la administración de SA. El intercambio de mensajes en el modo informativo se muestra en la figura 27.

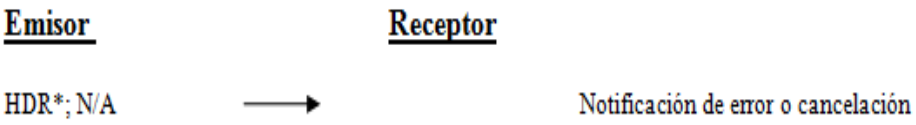

Figura 27 Intercambio de información
Fuente: (Vásquez, 2011)

En el primer mensaje, el emisor o el receptor transmite una notificación ISAKMP o una carga de cancelación.

CAPÍTULO II

SITUACIÓN ACTUAL DE LA UNIVERSIDAD POLITÉCNICA SALESIANA, CAMPUS GIRÓN

2.1 Estructura actual de la institución.

La Universidad Politécnica Salesiana creada mediante Ley N° 63 expedida por el Congreso Nacional y publicada en el registro oficial N° 499 del 5 de agosto de 1994, es una institución autónoma, de educación superior particular, católica, cofinanciada por el Estado. Es una persona jurídica de derecho privado, con finalidad social y sin fines de lucro. Su domicilio principal y matriz se halla en la ciudad de Cuenca, con sedes en las ciudades de Quito y Guayaquil.

2.1.1 Productos y servicios ofrecidos por TI.

Por la característica propia del negocio, el departamento de TI ofrece los siguientes servicios:

- AVAC: Educación Virtual
- VoIP: Telefonía IP para servicio interno
- WIFI: Acceso a internet y servicios de la Universidad
- Portal Institucional: Sitio web con acceso centralizado a servicios como información, correo institucional, ingreso y consulta de notas, evaluación docente, repositorio digital.
- Cámaras IP: Ofrece seguridad interna.
- Sistema de Matriculación: Servicio creado para optimizar el proceso de matriculación académica de los estudiantes
- Internet 2 : Servicio para proyectos de investigación

Funciones del departamento de TI

- **Servicios para la docencia** Las áreas de TI deben asegurar a los estudiantes y docentes de la Universidad el uso de los equipos de TI.

- **Servicios para la administración** Las áreas de TI, una vez recibido los requerimientos de las diferentes áreas académicas o administrativas; analizarán, diseñarán y desarrollarán los programas necesarios para la gestión.
- **Servicios institucionales** Los departamentos de TI deberán promover la automatización de los servicios académicos y administrativos de la UPS, así como el uso de las tecnologías de información y comunicación.

2.1.2 Estructura orgánica funcional del área de TI-Rectorado.

En la figura 28 se detalla la estructura funcional del área de TI-Rectorado

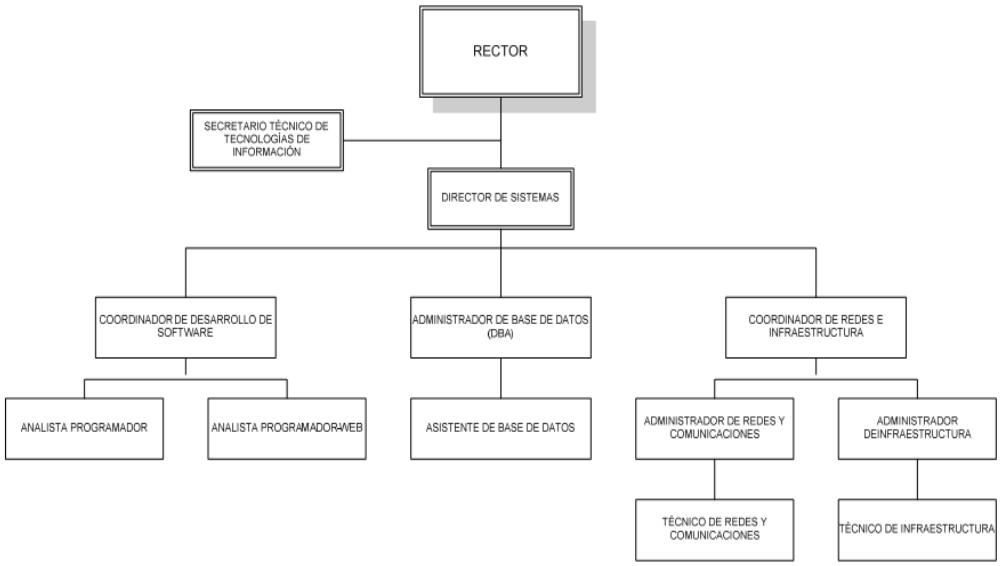

Figura 28 Organigrama Funcional TI-Rectorado
Fuente: Universidad Politécnica Salesiana

Las funciones de los puestos mostrados en el organigrama se muestran a continuación:

Director de Sistemas.- Garantizar la alta disponibilidad en los servicios de TI de la Universidad Politécnica Salesiana.

Coordinador de Desarrollo de Software.- Asegurar la disponibilidad y coordinar el desarrollo, implementación y mantenimiento de las aplicaciones informáticas requeridas dentro de la Universidad Politécnica Salesiana.

Administrador de Base de Datos.- Garantizar la disponibilidad de las Bases de datos de la UPS.

Coordinador de Redes e Infraestructura.- Planificar, definir, realizar, coordinar y supervisar el mantenimiento de la operatividad de la infraestructura

de servidores, telecomunicaciones y de equipos de usuario en toda la Universidad.

Analista Programador.- Desarrollar software web de acuerdo a las necesidades de la Universidad Politécnica Salesiana.

Administrador de Redes y Comunicaciones.- Garantizar el funcionamiento de la Red, Comunicaciones y Seguridad Informática de la Universidad Politécnica Salesiana.

Administrador de Infraestructura.- Garantizar el buen funcionamiento de la Infraestructura de Servidores y Datos dentro de la Universidad Politécnica Salesiana.

Técnico de Redes y Comunicaciones.- Ofrecer soporte al usuario.

El personal directamente responsable de la migración y posterior implementación de IPSec será el Coordinador de Redes e Infraestructura, quien estará a cargo del diseño del plan de migración e implementación, el Administrador de Red, cuyas funciones estarán circunscritas exclusivamente a la gestión de configuración y pruebas, finalmente el grupo de Técnicos de Redes y Comunicaciones estarán designados para dar el soporte y mantener el control de los cambios realizados.

2.1.3 Análisis de la topología física actual.

Dentro del diseño de red de la Universidad, se deberán analizar los siguientes aspectos: Modularidad, jerarquía y resistencia.

Diseño modular.-La modularidad es el principio fundamental del diseño de la red empresarial puesto que define cómo está ensamblada en sus múltiples bloques, que han sido diseñados por separado, esto permite una mejor aplicación de la jerarquía y la redundancia.

Este diseño se compone de los siguientes módulos:

- **Núcleo de la empresa.-** Interconecta el resto de módulos, mantiene la redundancia total y ofrece servicio continuado, en la UPS este módulo está compuesto por el switch Cisco Catalyst 4507R, el equipo cuenta con sistemas redundantes, este dispositivo se encuentra físicamente ubicado en el bloque A del Campus Girón.

Adicionalmente existe un Cisco Catalyst 4507R en el bloque B del mismo Campus operando al mismo tiempo y con todas las configuraciones del switch principal, con el fin de mantener redundancia.

- **Campus de la empresa.-** En este módulo se encuentran todos los elementos de red que operan independientemente, su finalidad es ofrecer conectividad entre el core y los usuarios finales, en el Campus Girón esto se lleva a cabo mediante los switch Cisco Catalyst 3750, los que físicamente se conectan al core por medio de fibra óptica multimodo.
- **Data center de la empresa.-** Aquí se debe identificar tres submódulos: servidores, redes y almacenamiento. El submódulo de servidores está divido en dos áreas a saber: la de servidores internos y la zona desmilitarizada, en el submódulo de los servidores internos, están conectados directamente al switch core, por medio de tecnología Gigabit Ethernet, el segmento de red para SAN está constituido por un servidor HP DL380G7, con capacidad para 21 dispositivos de almacenamiento.

El submódulo de la zona desmilitarizada contiene los servidores de acceso público como el de mail, el servidor web, el de tarifación y antivirus, el DHCP y DNS entre otros, estos equipos van conectados al Cisco ASA 5520. El detalle de los servidores y sus aplicaciones se encuentran en la tabla 6.

La Universidad cuenta con una infraestructura acorde a las necesidades que requiere el modelo de negocio de la institución, se cuenta con soluciones Blade donde reposan las aplicaciones sobre máquinas virtuales como el AVAC que es la plataforma de educación virtual, servidor de archivos, servidor de directorio activo, servidor de aplicaciones, servidor proxi y servidor mail, en otros equipos se han implementado el pool de servidores proxy, la aplicación de gestión de red y el servidor de backup, adicionalmente se dispone de servidores HP Proliant DL-380G4 para el segmento SAN, video conferencia, tarifación y el antivirus. El resto de servidores están sobre plataformas de diferentes tecnologías, que ofrecen servicios de red como DHCP, DNS, SQUID, VoIP, IVR entre otros, cabe destacar que se cuenta con un servidor IBM System X3500 M2 con dos procesadores Intel Xeón 5530, el mismo que está destinado a la aplicación AVAC, que es la aplicación donde reside el aula virtual.

Tabla 6
Detalle de Servidores del Campus Girón

Modelo	Tipo	Sistema Operativo	Aplicación
Intel_Xeon_E5335_2.00GHz/60GB/2GB/NA	SERVIDOR BLADE HS21 8853	Windows Server Enterprise 2008 R2 X64	Proxy Centos
Intel_Xeon0_E5335_2.00GHz/40GB/2GB/NA	SERVIDOR BLADE HS21 8853	GNU/Linux Centos X64	Proxy Centos
Intel_Xeon_E5335_2.00GHz/1,6TB/4GB/NA	SERVIDOR BLADE HS21 8853	GNU/Linux Centos X64	File Server,
Intel_Xeon_E5335_2.00GHz/1,6TB/4GB/NA	SERVIDOR BLADE HS21 8853	Windows Server Enterprise 2003	Active directory 2008
Intel_Xeon_E5335_2.00GHz/1,6TB/4GB/NA	SERVIDOR BLADE HS21 8853	GNU/Linux Centos X64	APM 2008
Intel_Xeon_E5335_2.00GHz/450 GB/24 GB	SERVIDOR BLADE HS22 7870	Vmware: Windows 2008	Proxy Centos para laboratorios CECASIG
Intel_Xeon_E5335_2.00GHz/4TB/ 64 GB	SERVIDOR BLADE HS22 7870	Vmware: 2 Windows 2008, 3 Centos	Mail
Intel_Xeon3.60GHz/2X136,72GB/4GB/NA	DL-380G4	Windows Server Enterprise 2003	Tarifación, antivirus
Intel Xeon_X5650_2,67GHz/2TB/8GB/	DL-380G7	Windows Server Enterprise 2008 R2 X64	Segmento SAN, - storage core LTO de 21 cintas

Continua

Intel_Xeon3.00GHz/500GB/2GB/NA	Clon	Windows Server Enterprise 2003	IVR
Intel_Xeon3.00GHz/2X34,14GB/2GB/NA	Clon	Windows Server Enterprise 2003	DHCP / DNS
Intel_Celeron3.20GHz/149,05GB/2GB/NA	Clon	Windows Server Enterprise 2003	TELEFONIA IP
Intel_Celeron3.20GHz/149,05GB/2GB/NA	Clon	Windows Server Enterprise 2003	TELEFONIA IP
Intel_Celeron3.20GHz/149,05GB/2GB/NA	Clon	Windows Server Enterprise 2003	TELEFONIA IP
Intel_DualCore3.0GHz/160GB/4GB/NA	Clon	GNU/Linux Centos X32	
Intel_PIV 3.0GB/160GB/2GB/NA	Clon	GNU/Linux Centos X32	Biométrico
Intel_Core2Duo2.6GHz/320GB/2GB/NA*	Clon	GNU/Linux Centos X32	SQUID Estudiantes
Intel_Core2Duo2.6GHz/320GB/2GB/NA*	Clon	GNU/Linux Centos X32	SQUID Docentes
Intel_PIII 999Mhz STL2/17GB/512MB/NA	Clon	GNU/Linux Centos X32	Backup
Quad Core Xeon E5410 Processor2x6MB Cache/ 750G/ 4G/	Dell PowerEdge2950	Windows Server Enterprise 2008 R2 X64	Videoconferencia

Continua

Dual core XEON/ 75 G, 75 G/ 2 Gb/	Dell PowerEdge 2850	Windows Server Enterprise 2008 R2 X64	Videoconferencia
Intel Xeon_E5530_2.40GHz/24Gb	System x3500 M2	Vmware: 2 Windows 2008, 2 Centos	AVAC

Fuente: Universidad Politécnica Salesiana

- **Frontera de la empresa.-** Contempla la conectividad a Internet, el acceso WAN y el acceso remoto a los servicios internos de la organización. La Universidad lo realiza por medio de dos proveedores de datos, estos son Telconet a través de un router Cisco 3825 y CNT por medio de un router Cisco 2801, de esta manera los Campus Sur, Kennedy, Cayambe y Latacunga acceden a Internet a través de la infraestructura del Campus Girón. Los enlaces son redundantes entre los Campus Sur, Girón, Kennedy y la sede Cuenca, el acceso a Internet en el Campus Girón tiene un ancho de banda de 25 Mbps, todo el tráfico a Internet se gestiona desde este lugar, tal como se aprecia en la figura 29.

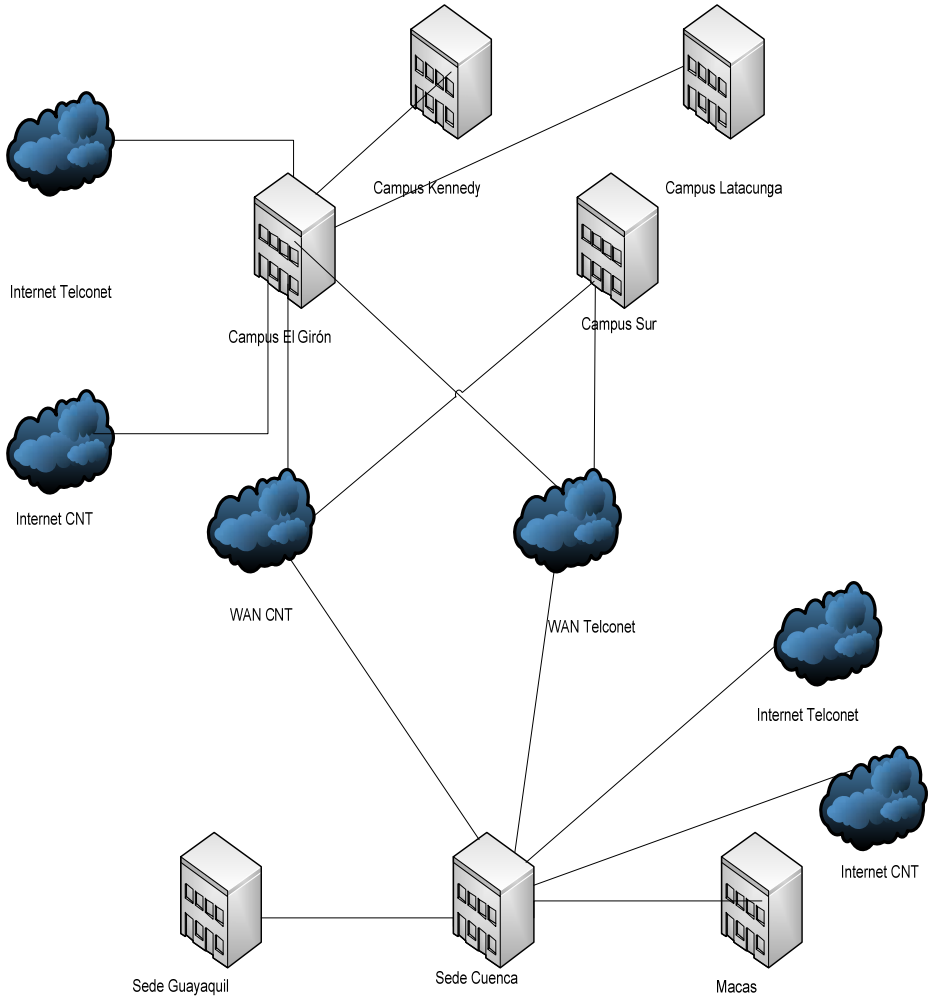

Figura 29 Conectividad a Internet y Acceso WAN

La seguridad de borde se lo controla por un ASA 5520, que entre sus principales funcionalidades, maneja el sistema de prevención de intrusiones y el firewall, el acceso remoto a aplicaciones internas de la organización se lo realiza por medio de un Servidor de Acceso Remoto o RAS, que está conectado a la PSTN de CNT, al igual que el Gateway VoIP. La seguridad se fortalece con un pool de servidores proxy, el control de tráfico y calidad de servicio se lo hace con el Cisco Packet Shaper 1700, tal como se muestra en la figura 30. Adicionalmente las VLAN´s de acceso se gestionan en los switch de capa 3 CISCO 4507R y el acceso a Internet se lo hace por un router CISCO 2801 para el proveedor CNT y un router Cisco 3825 para el proveedor Telconet.

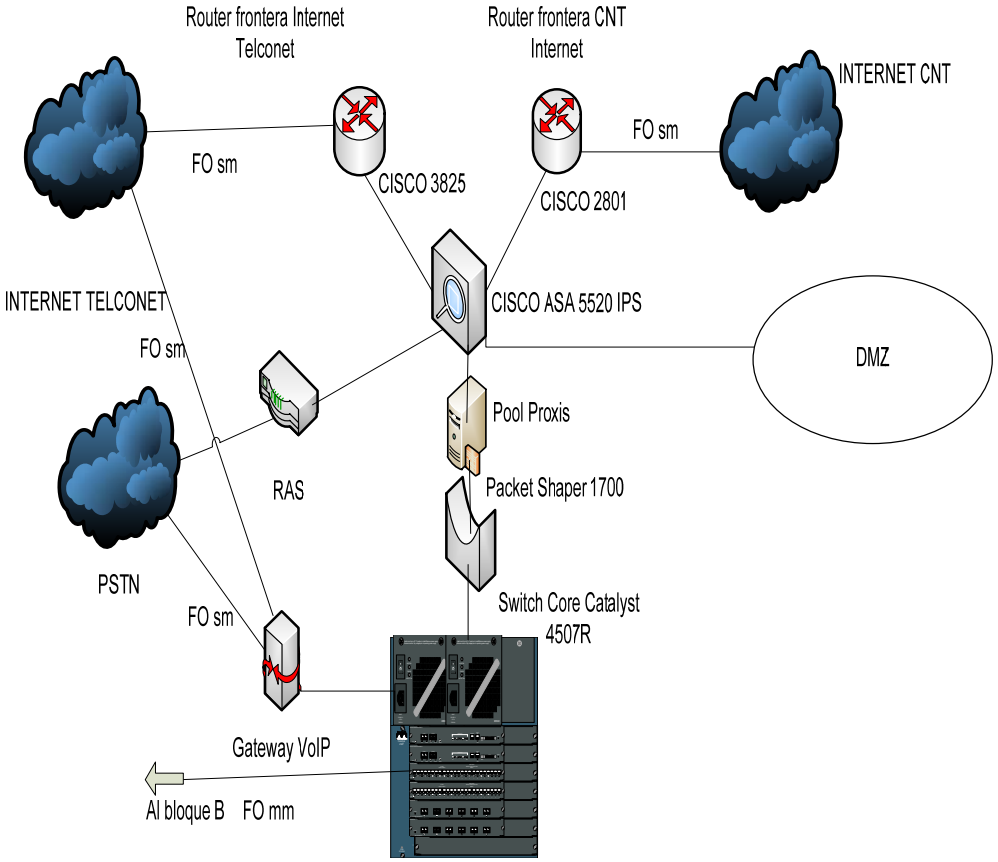

Figura 30 Infraestructura de acceso y seguridad

- **Servicios de red.-** Constituyen un pilar fundamental para la planificación de la posterior implementación de la nueva plataforma IPv6, puesto que al conocerlos puntualmente se puede establecer claramente los métodos y técnicas de migración a seguir, por ejemplo en este caso se deberá analizar si es necesario manejar dual stack para la transición o si es que la migración será a un escenario IPv6 nativo directamente. La respuesta es que la migración se la realizará a un escenario IPv6 nativo puesto que la Institución tiene entre sus objetivos del Plan Estratégico realizar esta actividad a futuro (Domínguez, 2012)

Así en el Campus Girón estos servicios actualmente trabajan exclusivamente sobre la plataforma IPv4, y básicamente manejan servicios de seguridad y administración tales como active directory, proxy, squid y antivirus, aplicaciones como mail, web, AVAC, biométrico, file Server, APM, servicios de infraestructura y de comunicaciones tales como DNS, DHCP, VoIP, videoconferencia, almacenamiento.

- **Servicios de VoIP.-** Estos servicios revisten vital importancia puesto que al momento son uno de los pilares fundamentales de las comunicaciones de la organización. La plataforma VoIP está compuesta de dos escenarios comunes, el primero ubicado en la sede Quito, y el segundo, en la sede Cuenca, ambos tienen exactamente la misma infraestructura, compuesta por un clúster de dos CISCO CallManager 7825 l3 versión 6.0.

Este clúster que presta servicios de IVR y cuentan con una capacidad máxima de 300 end points cada uno, están directamente conectados al switch core y la interconectividad se realiza por medio del Gateway VoIP configurado en un router CISCO 2801, el mismo que provee conectividad directa a la PSTN por medio de 2 E1 y a la nube WAN por medio del acceso que los dos proveedores ofrecen.

Esta topología se muestra en la figura 31.

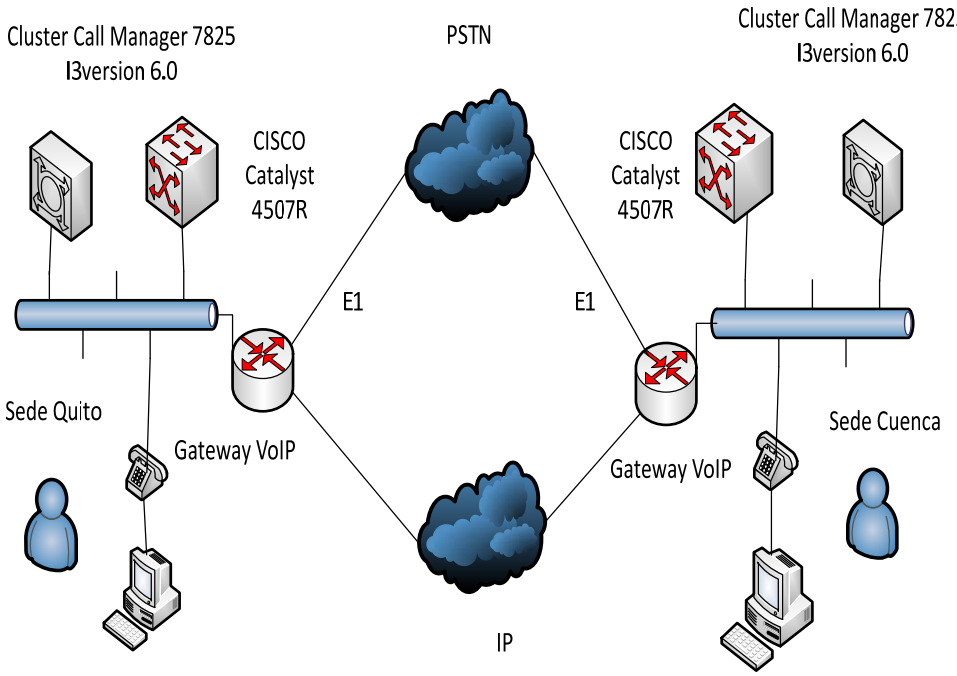

Figura 31 Infraestructura VoIP

Los Campus Sur, Cayambe y Kennedy, acceden al servicio de telefonía IP por medio de la infraestructura ubicada en el Campus Girón, la sede Guayaquil

accede a este servicio por medio de la infraestructura VoIP ubicada en la sede Cuenca.

- **Servicios de video conferencia.-** La plataforma de videoconferencia está provista totalmente por equipos Polycom HDX 8000, con resolución de 1080 pixeles a 30 cuadros por segundo, lo que permite calidad HD, adicionalmente existen funcionalidades para compartición de archivos y contenidos multimedia. Los servidores principales se encuentran en la sede Cuenca, sin embargo, están replicados en el Campus Girón, este servicio usa la misma infraestructura de conectividad con la que cuenta la institución. Los Campus Guayaquil y Macas acceden al servicio por medio de la infraestructura de la sede Cuenca, y los Campus Sur, Cayambe, Kennedy, Latacunga, acceden al servicio por medio de la infraestructura del Campus Girón. El detalle de este servicio se muestra en la figura 32.

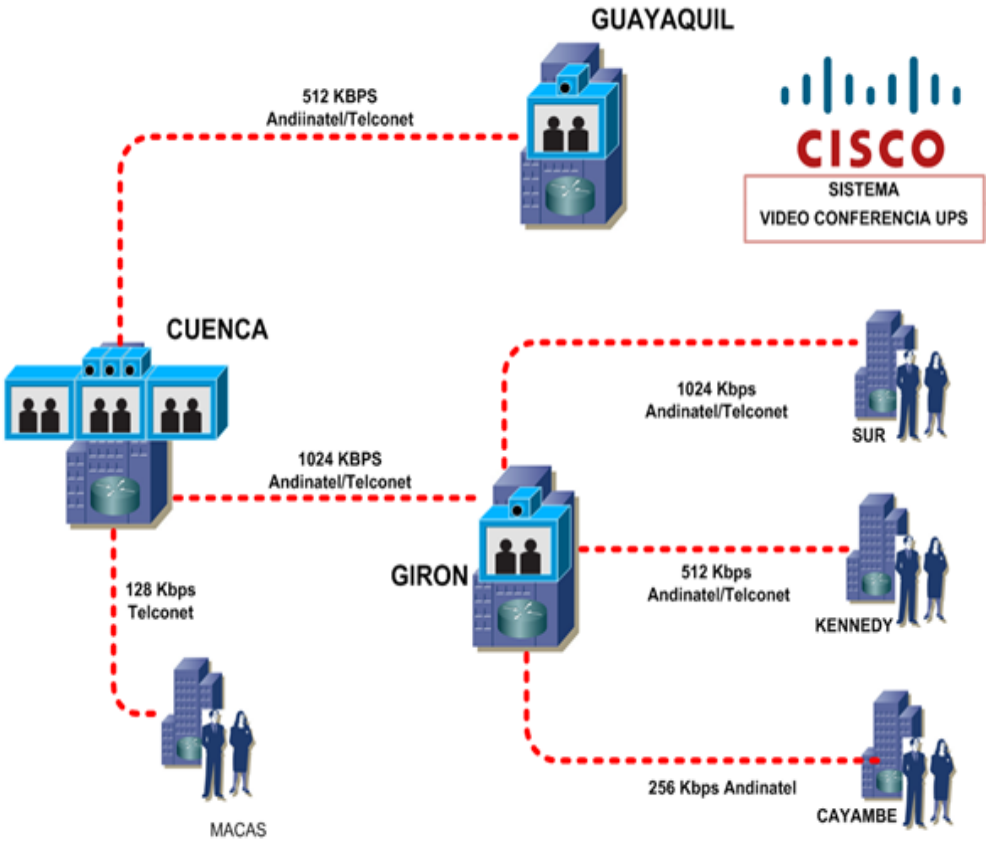

Figura 32 Servicio de Videoconferencia

Fuente: Universidad Politécnica Salesiana
Elaborado por: Juan Carlos Domínguez

El diseño de red modular permite identificar con claridad las funciones de cada sector de la red, de esta manera se mejora la capacidad de administración, gestión de fallos, gestión de cambios y lo más importante, la gestión de seguridades. En la figura 33 se puede apreciar gráficamente como está diseñado modularmente el Campus Girón.

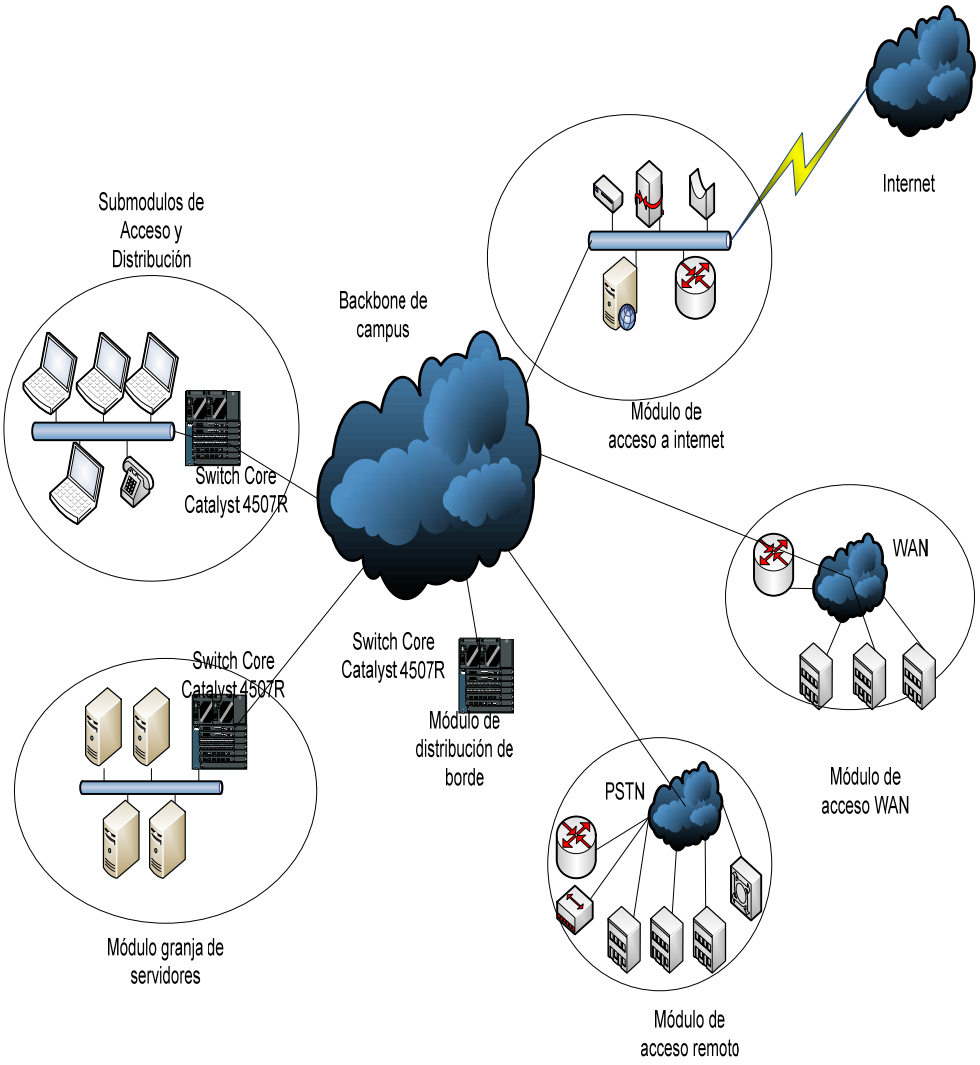

Figura 33 Diseño modular de la UPS

El diseño jerárquico.- Tiene muchos beneficios puesto que permite poner en un orden cada módulo descrito anteriormente, de esta manera se definen

funciones puntuales dentro de cada capa, permitiendo una mayor flexibilidad frente a las actualizaciones, detección de fallas y la escalabilidad, en este caso la red de la UPS es bastante compleja e incluye múltiples protocolos y tecnologías, por lo tanto este modelo ayudará a decidir una manera apropiada de aplicar la propuesta de diseño. Al considerar el modelo jerárquico, se obtiene como resultado una mayor eficiencia en el diseño implementación, mantenimiento, administración y proyección de la red, adicionalmente la infraestructura se torna más confiable, ofreciendo una mejor relación costo/beneficio. Cada capa tiene funciones específicas asignadas.

- **La capa de núcleo**.- Organiza el tráfico de la red tan rápido como sea posible y se encarga de llevar grandes cantidades de tráfico de manera confiable y veloz, por lo que la latencia y la velocidad son factores importantes a tener en cuenta, adicionalmente se maneja ruteo, calidad de servicio y redes privadas virtuales. El tráfico se procesa en la capa de distribución que a su vez envía las solicitudes al core si es necesario. En esta capa el concepto de tolerancia a fallos se torna crítico, puesto que el colapso del núcleo afecta totalmente a la red, adicionalmente dada la importancia de la velocidad, no hace funciones que puedan aumentar la latencia, como access-list, ruteo inter VLAN, filtrado de paquetes, ni tampoco acceso del grupo de trabajo.

En la red actual se dispone de un switch core marca Cisco, de la serie Catalyst 4507R ubicado en el MDF del centro de cómputo, este equipo permite la conectividad del backbone de fibra óptica, que interconecta los switch de piso Cisco Catalyst 3750, los cuales están ubicados en los SDF’s del Campus y se interconectan por fibra óptica a 1 Gbps, como se detalla en la figura 34, este switch de capa 3 contiene 2 módulos de control, 48 puertos, capacidades PoE y 12 módulos GLC. Es en esta capa donde se provee de interconexión entre los dispositivos que conforman la capa de distribución y conectan la red LAN del Campus con redes externas.

- **La capa de distribución.-** Provee el medio de comunicación entre la capa de acceso y el core. Las funciones de esta capa son proveer ruteo, filtrado, acceso a la red WAN, access-list, filtrado de paquetes, cola de espera, se implementa la seguridad y políticas de red.

- **La capa de acceso.-** Controla el acceso de grupos de trabajo a los recursos de red, entre sus funciones están la continuación de control de acceso y políticas de seguridad, creación de dominios de colisión separados y conectividad de grupos de trabajo en la capa de distribución. En esta capa se lleva a cabo la conmutación, ruteo estático exclusivamente, en el Campus Girón esta tarea se la hace mediante los switch Cisco 3750 distribuidos en los SDF tanto del bloque A, como del bloque B, participan 29 switch de piso, se ubican también los switch que conforman la capa de borde.

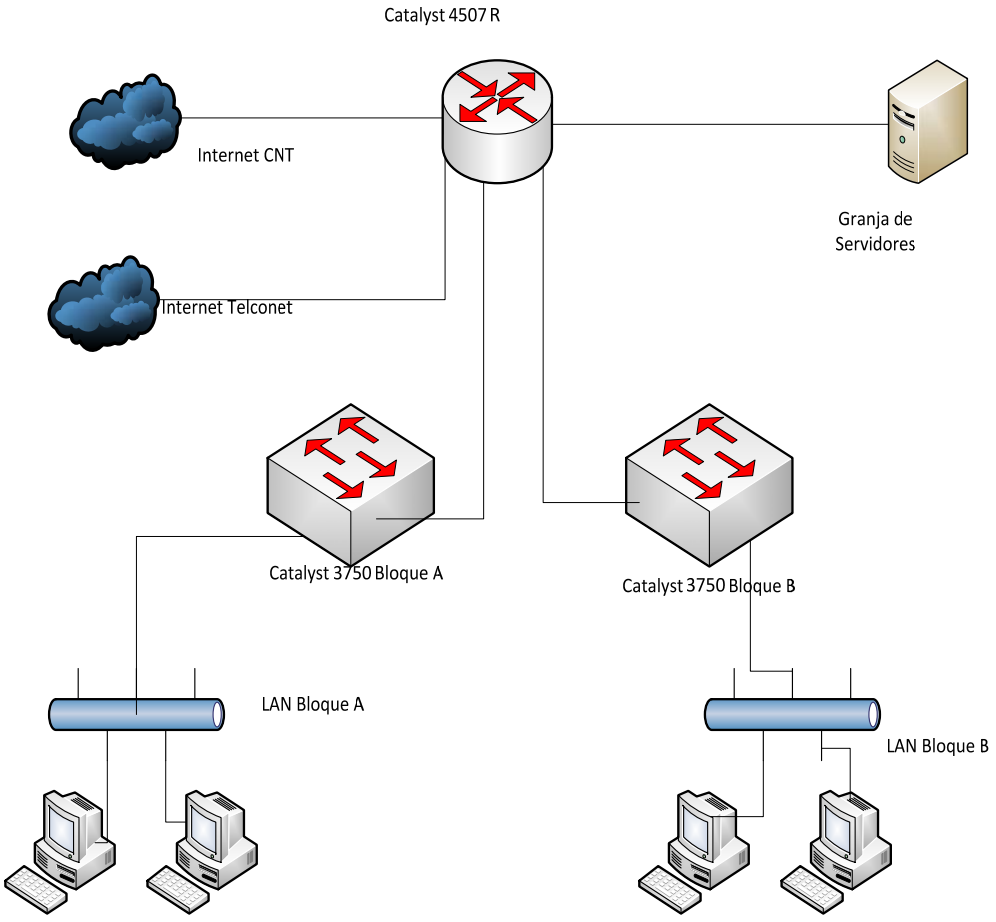

Figura 34 Infraestructura del Campus Girón

Los SDF's con sus respectivos switch proveen servicios a aproximadamente 500 usuarios que ocupan estaciones de trabajo de las cuales 200 estaciones son utilizadas por el personal de la Universidad, tanto docentes como administrativos y las restantes son utilizados por equipos que están ubicados en las diferentes aulas de laboratorios y biblioteca, que son de uso

exclusivo para estudiantes, como se muestra en la figura 35. Los equipos de usuario son tipo desktop, mayoritariamente son clones con procesadores Intel Quad Core o Intel I3, los equipos trabajan con el sistema operativo Windows 7.

Escalabilidad.- Una red escalable puede expandirse rápidamente para admitir nuevos usuarios y aplicaciones sin afectar el rendimiento del servicio, esta capacidad depende del diseño jerárquico en capas en la infraestructura física subyacente y de la arquitectura lógica.

De esta manera la red de la UPS cumple con los requisitos necesarios para soportar un crecimiento continuado, tanto a nivel de aplicaciones como a nivel de infraestructura de comunicaciones incluido aquí el cableado estructurado., la capacidad de crecimiento está de acuerdo a las necesidades que la institución requiera.

Resistencia.- Adicionalmente al diseño modular y al diseño jerárquico es importante considerar la resistencia que presenta la red a fallos puntuales, con el fin de asegurar la continuidad del negocio, en el análisis de situación inicial se ha identificado claramente la existencia de redundancia en cada una de las capas del modelo jerárquico. La UPS Campus Girón cuenta con mecanismos y topologías que aseguran la tolerancia a fallos, existen espejos en la Sede Cuenca, de igual manera a nivel de conectividad los enlaces son redundantes.

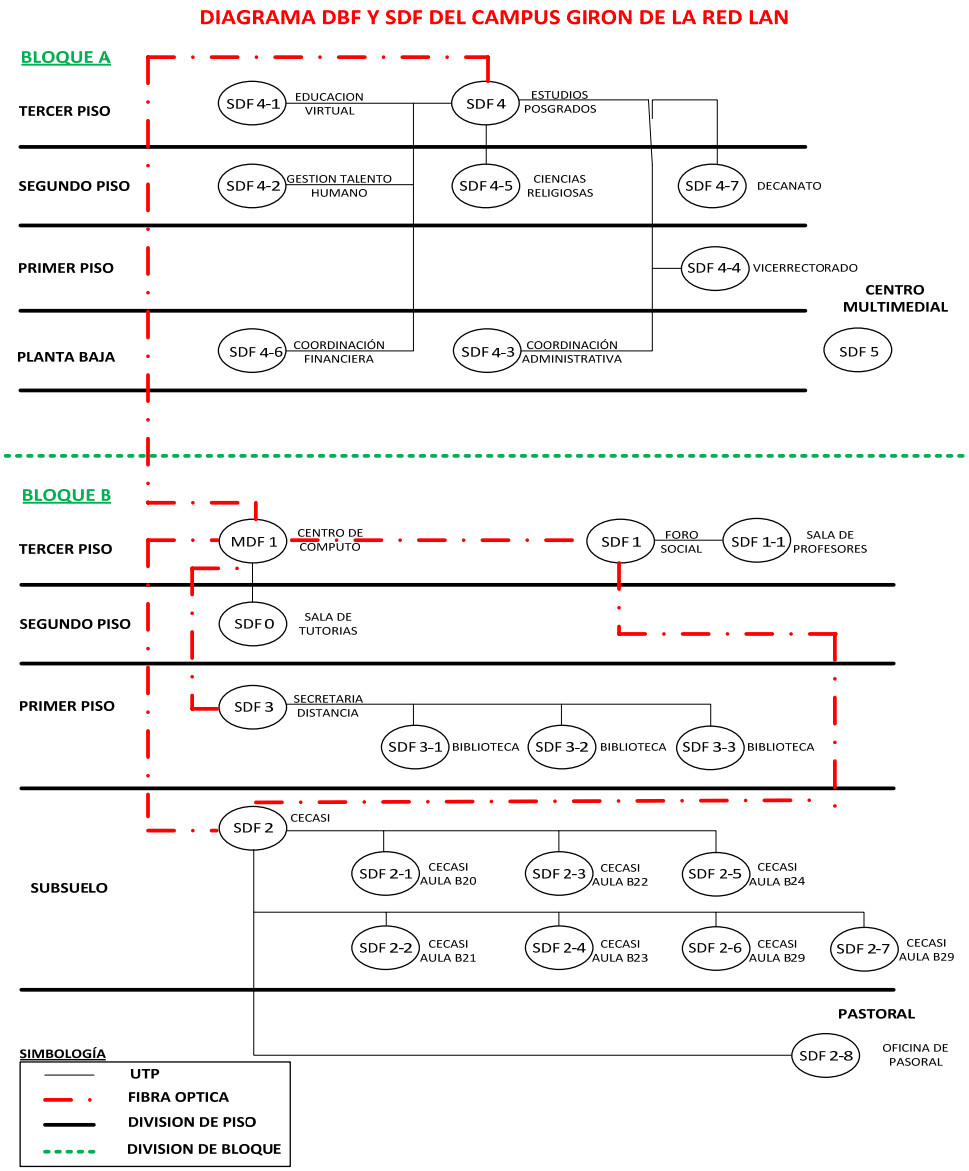

Figura 35 Diagrama SDF
Fuente: (Barrionuevo, 2006)

En la tabla 7, se detalla la distribución de los SDF's, el número de equipos de capa 2 y los puertos disponibles, para el Campus Girón.

Tabla 7
Detalle de distribución de los switches Campus Girón

NOMBRE	UBICACIÓN DEL SDF	CANT. SWITCH	PUERTOS
MDF1	Centro Cómputo	4	**68**
SDF0	Sala de Tutorías	1	**8**

SDF1	Foro Social	1	**20**
SDF1-1	Sala de Profesores	1	**16**
SDF2	CECASI	2	**44**
SDF2-1	CECASI Aula 1	1	**24**
SDF2-2	CECASI Aula 2	1	**24**
SDF2-3	CECASI Aula 3	1	**24**
SDF2-4	CECASI Aula 4	1	**24**
SDF2-5	CECASI Aula 5	1	**24**
SDF2-6	CECASI Aula 6	1	**24**
SDF2-7	CECASI Aula 6B	1	**24**
SDF2-8	Pastoral	1	**8**
SDF3	Secretaria	2	**44**
SDF3-1	Biblioteca 1	1	**8**
SDF3-2	Biblioteca 2	1	**20**
SDF3-3	Biblioteca 3	1	**8**
SDF4	Principal Bloque A	2	**44**
SDF4-1	Educación Virtual	1	**8**
SDF4-2	Gestión del Talento	2	**32**
SDF4-3	Administración	1	**16**
SDF4-4	Vicerrectorado	1	**24**
SDF4-5	Ciencias Religiosas	1	**16**
SDF4-6	Financiero	1	**24**
SDF4-7	Decanato	1	**16**
SDF5	**Audiovisuales**	**2**	**72**

Fuente: (Moreno & Cristian, 2012)

2.1.4 Vulnerabilidades que justifican IPSec en la Universidad Politécnica Salesiana, Campus Girón.

La Universidad Politécnica Salesiana ofrece servicios informáticos a estudiantes, docentes, y personal administrativo, los mismos que manejan información que permite el correcto desarrollo de cada una de las actividades realizadas por estos tres grandes grupos de usuarios, en cada uno de ellos existen servicios que generan información cuya importancia depende directamente del contenido de la misma.

Cada uno de estos servicios contiene vulnerabilidades que han sido detectadas, como por ejemplo se muestra lo detectado con el analizador de

vulnerabilidades VEGA 1.0 (VEGA, 2010), esta aplicación es un escáner de vulnerabilidades de código abierto que prueba la seguridad de aplicaciones web, donde se puede determinar la existencia de vulnerabilidades como Inyecciones SQL, Cross-Site Scripting (XSS), Shell Injection, Local File Inclusion, Integer Overflow, entre otras, está programado en Java y basado en una interfaz gráfica por la cual se puede ejecutar en Linux, OS X y Windows.

El día 8 de julio del 2013 este proceso de detección se lo realizó desde un host conectado a la red interna donde se realizó un barrido a la dirección del portal institucional de la Universidad, determinó algunas vulnerabilidades de las cuales se indican a continuación las de más alto riesgo como se muestra en la figura 36

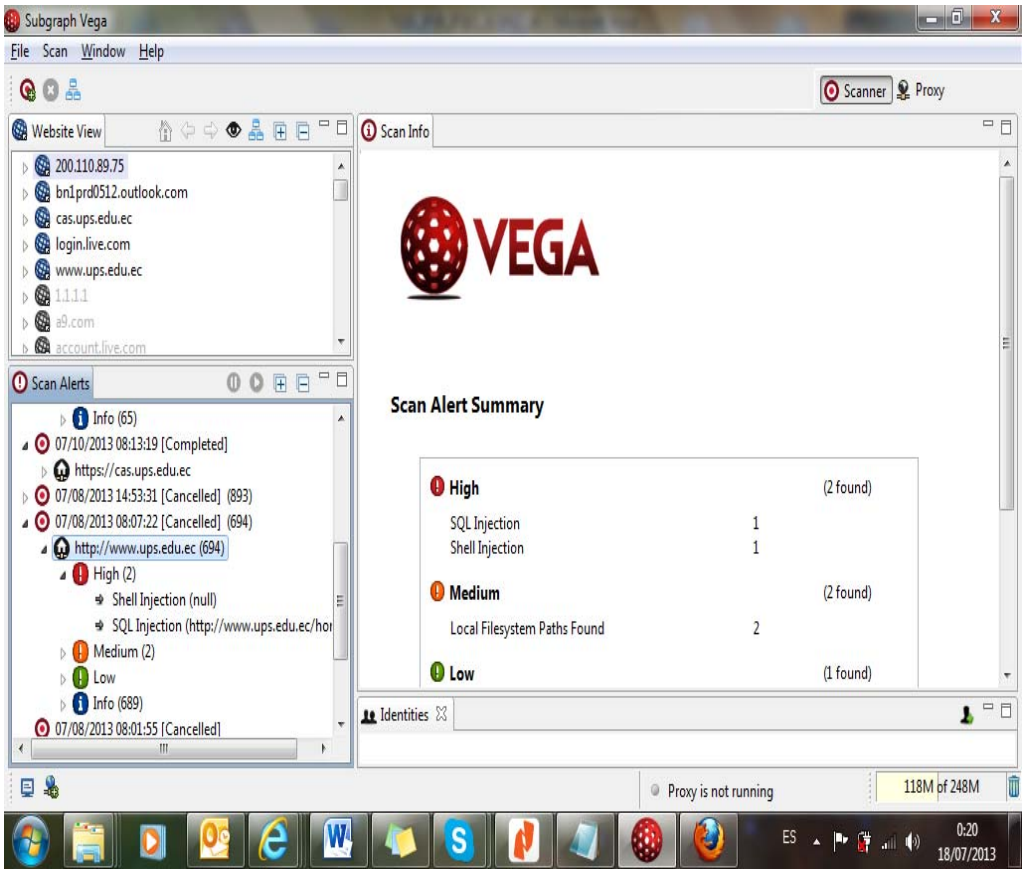

Figura 36 Área de trabajo de la aplicación VEGA
Fuente: Captura del programa VEGA

La primera vulnerabilidad detectada fue de tipo SQL Injection, en la figura 37 se puede observar el resultado del scan realizado al portal institucional.

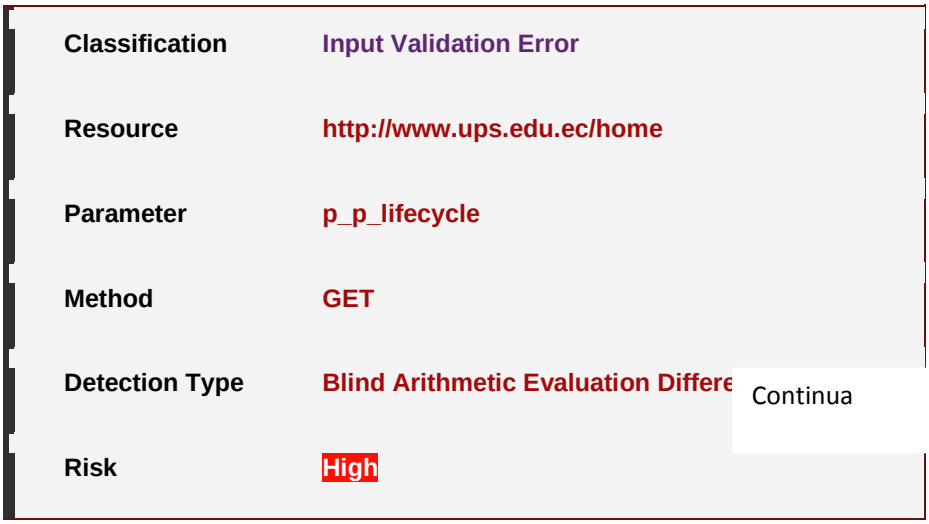

Figura 37 Vulnerabilidad tipo SQL Injection
Fuente: Captura del programa VEGA

La vulnerabilidad fue detectada en la solicitud detallada a continuación:

GET
/home?p_p_id=62_INSTANCE_fEd1&p_p_lifecycle=0'"&p_p_state=maximized&p_p_mode=view&p_p_col_id=_118_INSTANCE_Kms4__column-1&p_p_col_count=2&_62_INSTANCE_fEd1_struts_action=/journal_articles/view&_62_INSTANCE_fEd1_groupId=10156&_62_INSTANCE_fEd1_articleId=3737943&_62_INSTANCE_fEd1_version=1.5

Se detectó una posible vulnerabilidad de inyección SQL, estas vulnerabilidades están presentes cuando se utiliza un dato externo para construir una consulta SQL. Si no se toman precauciones, la entrada desde el exterior suministrado (por lo general un parámetro GET o POST) puede modificar la cadena de consulta de tal manera que lleva a cabo acciones como lectura o escritura autorizada el acceso a los datos almacenados en la base de datos, con el riesgo de una posible modificación de los mismos.

La siguiente vulnerabilidad detectada es de tipo Shell Injection, como se evidencia en la figura 38.

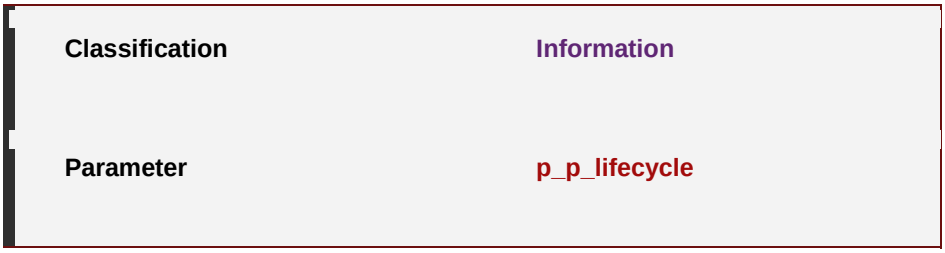

Figura 38 Vulnerabilidad tipo Shell Injection
Fuente: Captura del programa VEGA

Se determinó que la vulnerabilidad aparece en la siguiente solicitud:

REQUEST

GET /home?p_p_id=62_INSTANCE_Oz6a&p_p_lifecycle=0'true'&p_p_state=maximized&p_p_mode=view&p_p_col_id=_118_INSTANCE_Kms4__column-2&p_p_col_count=2&_62_INSTANCE_Oz6a_struts_action=/journal_articles/view&_62_INSTANCE_Oz6a_groupId=10156&_62_INSTANCE_Oz6a_articleId=3762511&_62_INSTANCE_Oz6a_version=1.1

Esta vulnerabilidad conocida como inyección de comandos ocurre cuando datos suministrados externamente son inadecuadamente filtrados y pueden verse como un comando del sistema que puede ser ejecutado a través de un intérprete de comandos o shell.

Las vulnerabilidades de este tipo pueden ser explotadas mediante metacaracteres de shell para ejecutar comandos adicionales que no estaban destinados a ser ejecutados inicialmente en la aplicación. Las funciones tipo system (), son a menudo responsables puesto que son muy sencillas de utilizar. Estas vulnerabilidades pueden permitir el acceso remoto a los atacantes.

El día 10 de Julio del 2013 se realizó un escaneo a la dirección. https://cas.ups.edu.ec, que es la ubicación del Servicio de Autenticación Central donde se gestiona el acceso de los docentes a los servicios internos del portal como pase de notas, aula virtual, rol de pagos, listas de alumnos, horarios, correo interno, entre otros.

El resultado se puede evidenciar en la figura 39

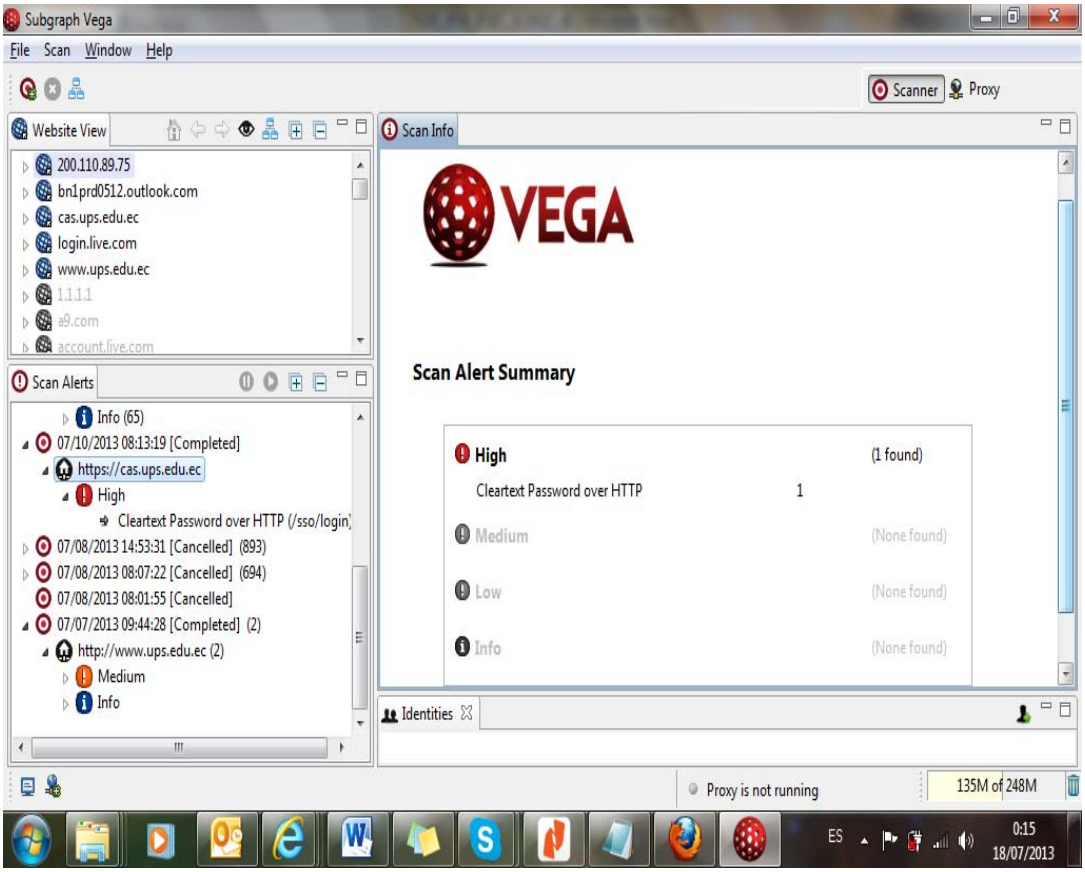

Figura 39 Resultados del escaneo del URL del Servicio de Autenticación Central
Fuente: Captura del programa VEGA

En este escaneo se encontró la vulnerabilidad tipo Clear Text en el campo login, tal como se muestra en la figura 40.

Classification	**Environment**

Figura 40 Vulnerabilidad tipo Clear Text
Fuente: Captura del programa VEGA

La misma que fue encontrada en la siguiente solicitud:

REQUEST

GET /sso/login?service=http://www.ups.edu.ec/c/portal/login&service=http://www.ups.edu.ec/c/portal/login

Se detectó un formulario con un campo de introducción de la contraseña que lo redirige a un destino inseguro (HTTP). Esta vulnerabilidad podría provocar la divulgación no autorizada de las contraseñas de los usuarios a los atacantes de la red.

Finalmente se realizó un nuevo escaneo a la dirección www.ups.edu.ec, con la finalidad de encontrar posibles vulnerabilidades adicionales a las ya detectadas con anterioridad, obteniéndose los resultados que se muestran en la figura 41.

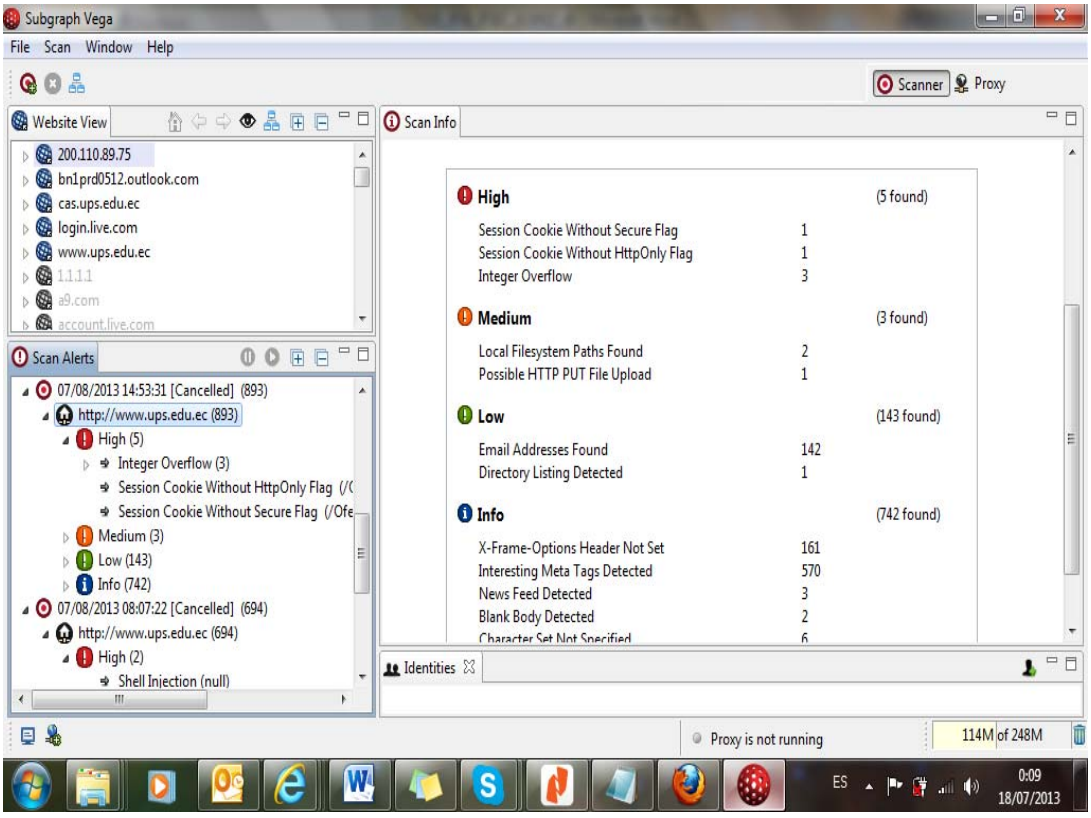

Figura 41 Resultados del escaneo de la dirección www.ups.edu.ec
Fuente: Captura del programa VEGA

Se determinó la existencia de una vulnerabilidad identificada como Integer Overflow, que responde a un desbordamiento de variable tipo entero, la mencionada vulnerabilidad se evidencia en la figura 42.

Classification	**Boundary Condition Error**
Resource	**/home?p_p_id=62_INSTANCE_fEd1&p_p_lifecycle=2147483648&p_p_state=maximized&p_p_mode=view&p_p_col_id=_118_INSTANCE_Kms4__column-1&p_p_col_count=2&_62_INSTANCE_fEd1_struts_action=/journal_articles/view&_62_INSTANCE_fEd1_groupId=10156&_62_INSTANCE_fEd1_article[illegible]&_62_INSTANCE_fEd1_version=1.5**

Continua

Parameter	**p_p_lifecycle**
Method	**GET**
Risk	**High**

Figura 42 Vulnerabilidad tipo Integer Overflow
Fuente: Captura del programa VEGA

La misma que fue detectada en la siguiente petición:

REQUEST

GET /home?p_p_id=62_INSTANCE_fEd1&p_p_lifecycle=2147483648&p_p_state=maximized&p_p_mode=view&p_p_col_id=_118_INSTANCE_Kms4__column-1&p_p_col_count=2&_62_INSTANCE_fEd1_struts_action=/journal_articles/view&_62_INSTANCE_fEd1_groupId=10156&_62_INSTANCE_fEd1_articleId=3737943&_62_INSTANCE_fEd1_version=1.5

La vulnerabilidad de desbordamientos de entero se produce cuando los tipos de datos enteros exceden su valor máximo, el comportamiento resultante puede tener implicaciones de seguridad por ejemplo si se utiliza como el tamaño de un buffer de datos, puede resultar en omitir de comprobaciones del tamaño del buffer, esto podría provocar condiciones de desbordamiento del buffer. Finalmente se detectó la vulnerabilidad tipo Cookie Without Secure Flag, el resultado se muestra en la figura 43.

Classification	**Information**
Resource	**/OfertaPosgrado-portlet/ofertaPosgrado.jsp**

Figura 43 Vulnerabilidad tipo Cookie Without Secure Flag
Fuente: Captura del programa VEGA

La vulnerabilidad fue detectada en la siguiente petición y se muestra en la figura 44

Figura 44 Detalle de la cookie de sesión sin seguridad
Fuente: Captura del programa VEGA

Se detectó que una cookie de sesión conocida pudo haber sido creada sin la bandera que indica que es segura. Las cookies de sesión son las credenciales de autenticación que pueden estar expuestas a los intrusos de la red para obtener acceso no autorizado a las aplicaciones Web.

Adicionalmente se recurrió a analizar el log del CISCO ASA 5520, con la dirección IP 172.17.3.253, este proceso se lo realizó por medio del uso de la aplicación FireGen, que es un software que realiza el análisis de conexiones recibidas y rechazadas, para luego clasificarlas por puerto y protocolo, ofreciendo además gráficas de visualización de los resultados de los análisis, en la tabla 8 se muestra la información de identificación del log que fue analizado.

Tabla 8
Identificación del log obtenido del ASA 5520

Info	Value
Log profile	Log profile 20130608004111

Analyzed log(s)	C:\Users\George\Documents\logs\LOG-ASA3.log (08,00 MB)
Firewall type	Cisco Pix/ASA
Analysis interval	All entries in the specified log

Del análisis del log, se pudo determinar que el día 5 de junio del 2013 entre las 11h00 y 13h00 se produjo una actividad fuera de lo normal en la red, puesto que se detectó 50.799 denegaciones y 292 alarmas, tal como se puede ver en la figura 45.

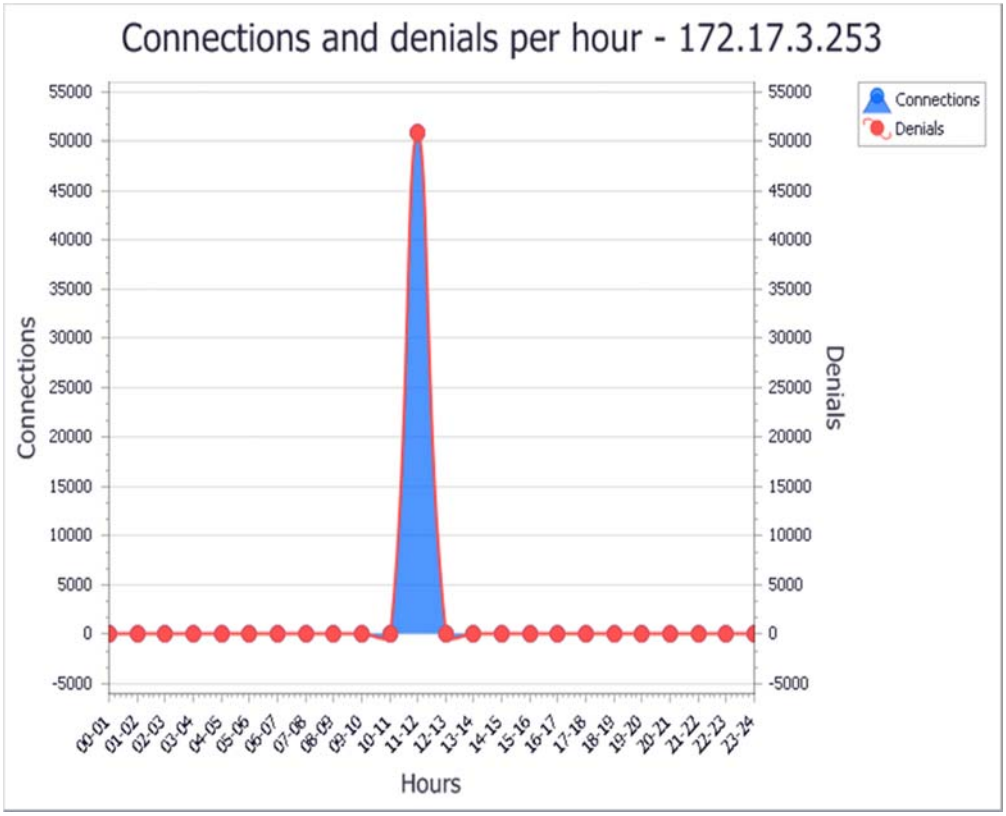

Figura 45 Conexiones denegadas por el ASA
Fuente: Captura del programa Firegen

De acuerdo a la información obtenida del log, se pudo determinar que la dirección 172.17.1.65 que pertenece a la red local de la Universidad, ha generado 996 conexiones, de las cuales 31 intentos de conexión fueron

bloqueados, estas conexiones fueron destinadas al servidor https y al http, donde reside la aplicación del aula virtual y el acceso al portal institucional respectivamente, la dirección 31.13.69.160 pertenece a una red externa, generó 792 conexiones, de las cuales 655 fueron rechazadas, igualmente el destino fueron los protocolos antes mencionados.

El detalle de las conexiones recibidas por el ASA en el lapso de mayor actividad se muestra en la tabla 9.

Tabla 9
Conexiones recibidas por el ASA

Destination	Connections	First denial	%	Comment
172.17.1.65	996	05/06/2013 11:18:49	12,08	31 denials recorded on 05/06/2013 11:19:27
31.13.69.160	792	05/06/2013 11:18:39	09,61	655 denials recorded on 05/06/2013 11:18:47
200.110.89.75	449	05/06/2013 11:19:19	05,45	
200.110.126.35	257	05/06/2013 11:18:38	03,12	
172.17.1.69	247	05/06/2013 11:18:41	03,00	8 denials recorded on 05/06/2013 11:18:48
200.110.126.25	181	05/06/2013 11:18:45	02,20	
23.67.244.177	150	05/06/2013 11:30:55	01,82	
69.171.242.27	106	05/06/2013 11:18:49	01,29	
200.110.126.17	104	05/06/2013 11:26:25	01,26	
31.13.69.161	93	05/06/2013 11:18:45	01,13	

Fuente: Captura del programa Firegen

Los protocolos que han recibido la mayoría de intentos de conexión bloqueados son HTTPS, HTTP y el servidor SQUID, el resto de puertos mostrados en la gráfica, pertenecen al rango de los puertos dinámicos

asignados a aplicaciones propias de la Institución, tal como se muestra en la tabla 10.

Tabla 10
Intentos de conexión por puerto

No	Denied protocol	Connections	First denial	%	Comment
1	TCP/443 - ssl-https	4.420	05/06/2013 11:18:37	53,61	
2	TCP/80 – http	2.422	05/06/2013 11:18:38	29,38	
3	TCP/3128 -squid-http	1.243	05/06/2013 11:18:41	15,08	
4	TCP/50869	06	05/06/2013 11:32:34	00,07	
5	TCP/50787	05	05/06/2013 11:29:38	00,06	
6	TCP/50783	05	05/06/2013 11:29:38	00,06	
7	TCP/50792	05	05/06/2013 11:29:38	00,06	
8	TCP/50793	05	05/06/2013 11:29:38	00,06	
9	TCP/50794	05	05/06/2013 11:29:38	00,06	
10	TCP/50795	05	05/06/2013 11:29:38	00,06	

Fuente: Captura del programa Firegen

El consolidado de conexiones bloqueadas se muestra en la siguiente gráfica, como se puede observar y de acuerdo a lo anteriormente expuesto, la mayoría de denegaciones se producen en las conexiones destinadas al puerto 443, al puerto 80 y al 3128, tal como se puede evidenciar en la figura 46.

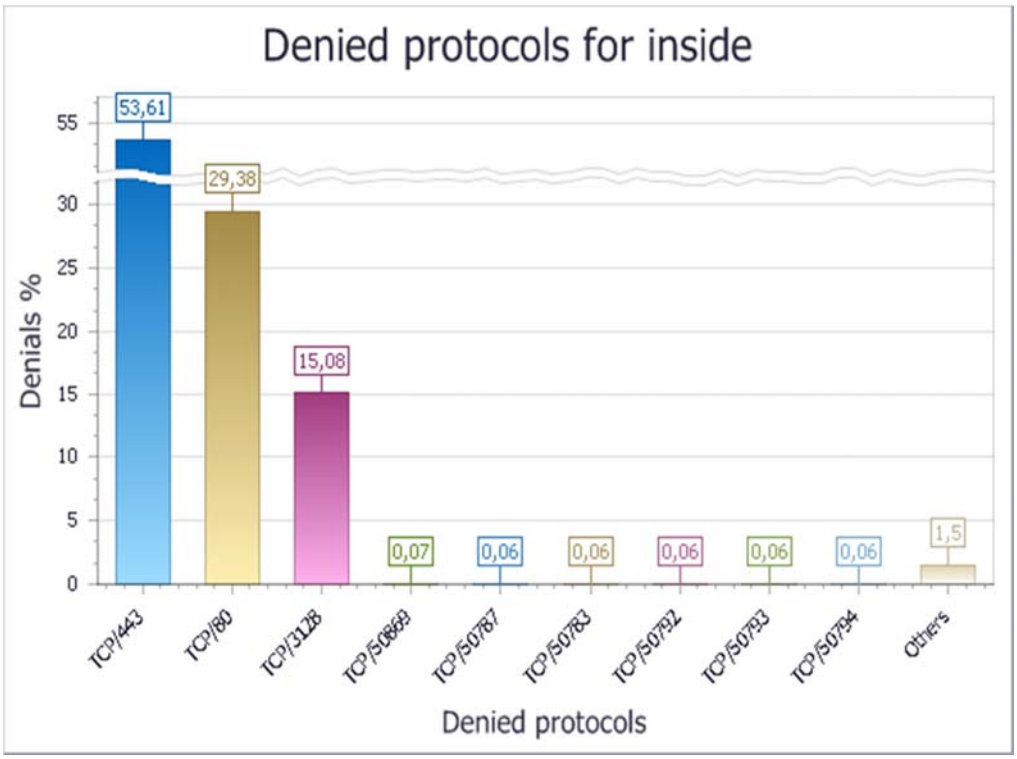

Figura 46 Porcentaje de conexiones bloqueadas por puerto
Fuente: Captura del programa Firegen

La tabla 11 muestra los intentos de conexión bloqueados provenientes de la red interna, como se puede observar la mayoría provienen de los host de los usuarios internos que quieren acceder sin los permisos necesarios a los servicios.

Tabla 11
Conexiones internas bloqueadas

Source	Connections	First denial	%	Comment
172.17.121.3	832	05/06/2013 11:18:45	10,09	832 denials recorded on 05/06/2013 11:18:45

172.17.123.175	420	05/06/2013 11:23:04	05,09	420 denials recorded on 05/06/2013 11:23:04
1.1.1.1	371	05/06/2013 11:18:38	04,50	371 denials recorded on 05/06/2013 11:18:38
172.17.120.248	345	05/06/2013 11:18:45	04,18	312 denials recorded on 05/06/2013 11:18:45
172.17.121.77	317	05/06/2013 11:19:03	03,84	
172.17.122.60	257	05/06/2013 11:26:15	03,12	
172.17.122.198	250	05/06/2013 11:18:45	03,03	
172.17.71.70	246	05/06/2013 11:18:49	02,98	
172.17.121.150	225	05/06/2013 11:19:50	02,73	
172.17.122.49	223	05/06/2013 11:19:33	02,70	

Fuente: Captura del programa Firegen

La tabla 12 muestra el número de intentos de conexión provenientes de redes externas, como se puede observar, la dirección 184.173.219.67 es quien genera un número importante de intentos dirigidos al servidor HTTP, en la figura 2.19 se puede observar los intentos de conexión externos a los respectivos protocolos.

Tabla 12
Intentos de conexión por direcciones IP externas

Destination	Connections	First denial	%	Comment
184.173.219.67	2.921	05/06/2013 11:18:37	12,92	

172.17.12.129	1.935	05/06/2013 11:18:38	08,56	
192.221.116.254	1.511	05/06/2013 11:18:48	06,68	
4.23.59.254	1.501	05/06/2013 11:18:49	06,64	
8.254.20.254	1.100	05/06/2013 11:18:50	04,86	
8.8.4.4	1.045	05/06/2013 11:18:38	04,62	
192.168.253.11	756	05/06/2013 11:28:59	03,34	
200.93.216.2	739	05/06/2013 11:18:39	03,27	393 denials recorded on 05/06/2013 11:18:39
200.93.216.5	724	05/06/2013 11:18:40	03,20	

Fuente: Captura del programa Firegen

La tabla 13 muestra los intentos de conexión por protocolo, provenientes de redes externas, como se observa, el protocolo HTTP y el DNS son los que tienen más intentos de conexión bloqueados, con el 53,77% el 12,42% respectivamente, a continuación en el puerto 514, perteneciente al syslog y el puerto 443 que es del protocolo https, aunque tienen un menor número de intentos de intrusión, se puede evidenciar que están siendo víctimas de un número bastante considerable de intentos de intrusión.

Tabla 13
Intentos de conexión por protocolo

No	Denied protocol	Connections	First denial	%	Comment
1	TCP/80 – http	12.159	05/06/2013 11:18:37	53,77	
2	UDP/53 – dns	2.809	05/06/2013 11:18:38	12,42	
3	UDP/514 – syslog	1.935	05/06/2013 11:18:38	08,56	
4	UDP/24582	756	05/06/2013	03,34	

			11:28:59	
5	TCP/443 - ssl-https	724	05/06/2013 11:19:02	03,20
6	UDP/123 – ntp	472	05/06/2013 11:18:43	02,09
7	TCP/25 – smtp	183	05/06/2013 11:18:49	00,81
8	UDP/16384	112	05/06/2013 11:24:11	00,50
9	TCP/993	89	05/06/2013 11:38:14	00,39
10	UDP/16385	88	05/06/2013 11:24:11	00,39

Fuente: Captura del programa Firegen

En la tabla 14, se detallan las direcciones de los host tanto internos como externos que han tenido más intentos de conexión bloqueados.

Tabla 14

Servicios vulnerables ofrecidos por TI

Destination	Connections	First denial	%	Comment
172.17.1.65	996	05/06/2013 11:18:49	12,08	31 denials recorded on 05/06/2013 11:19:27
31.13.69.160	792	05/06/2013 11:18:39	09,61	655 denials recorded on 05/06/2013 11:18:47
200.110.89.75	449	05/06/2013 11:19:19	05,45	
200.110.126.35	257	05/06/2013 11:18:38	03,12	
172.17.1.69	247	05/06/2013 11:18:41	03,00	8 denials recorded on 05/06/2013 11:18:48
200.110.126.25	181	05/06/2013 11:18:45	02,20	

Fuente: Captura del programa Firegen

De la información recabada del log obtenido del ASA, se pudo determinar que los servicios informáticos que ofrece la Institución siempre están sujetos a intentos de conexión no permitidos, algunos de ellos se podrían interpretar como intentos de ataques que pueden provenir tanto desde entornos externos como internos, los intentos de conexión no permitidos se producen en cualquier momento, estas conexiones bloqueadas no necesariamente significa que sean ataques, los bloqueos pueden obedecer a intentos de conexión de usuarios que no tienen las credenciales adecuadas para acceder a los servicios o a la aplicación de las políticas de seguridad de la red, si bien es cierto la infraestructura de seguridad actual con la que cuenta la Universidad Politécnica Salesiana ofrecen niveles de seguridad apropiados, se evidencia que existen vulnerabilidades como las mostradas en el inicio de este apartado, pues se pudo demostrar en primera instancia que un host interno puede realizar un escaneo de vulnerabilidades determinando la existencia de algunas de ellas de tipo errores de validación como el ejemplo de SQL injection, ejecución de código remoto como el caso de Shell injection, desbordamientos de buffer como en el caso de integer overflow, cookies inseguras como la de tipo cookie without segure flag. Estas vulnerabilidades representan un riesgo para el normal funcionamiento de la red y demuestran que los servicios de red que se manejan no son invulnerables, no obstante es necesario el disponer de mecanismos adicionales que ofrezcan un reforzamiento de la seguridad, no solo destinados a la capa aplicación sino al resto de capas, una de las capas donde estos mecanismos son más efectivos es en la capa red, puesto que en esta capa se pueden usar técnicas de sniffing, suplantación de mensajes, intercepción de mensajes, modificación de datos denegación de mensajes.

De acuerdo al tipo de información generada por los grupos de usuarios identificados y a las vulnerabilidades detectadas se puede determinar que hay una razón más que suficiente para justificar la implementación de IPSec en el Campus Girón, con este protocolo se puede reforzar la seguridad de capa tres selectivamente en un determinado segmento de la red, los que serán seleccionados de acuerdo a las necesidades de la Institución, tal como se

muestra en apartado 2.2.4, el protocolo se puede implementar independientemente de los requerimientos de escalabilidad que la red exige.

2.1.5 Esquema de direccionamiento.

En el Campus Girón de usa una red clase B, específicamente en el segmento 172.17.0.0, esto en razón del número de usuarios existentes, adicionalmente la red se ha dividido en varias VLAN´s, por motivos de seguridad y administración.

El nombre de la subred, el rango de host disponibles, la submáscara y los detalles generales de la red se detallan a continuación en la tabla 15.

Tabla 15
Esquema de direccionamiento IPv4 – campus Girón

Direccionamiento IPv4	
Nombre de Subred	LAN El Girón
Descripción	Red LAN UPS Campus El Girón
Network	172.17.0.0
Mascara	255.255.0.0
Rango IP	172.17.0.0 - 172.17.15.0

VLAN en el Campus Girón.- El objetivo principal del uso de VLAN es tener una subred IP separada de manera lógica, las VLAN permiten que redes IP y subredes múltiples coexistan en la misma red conmutada, reducen el tamaño del broadcast y adicionalmente ayudan en la seguridad y administración de la red.

En el Campus Girón el switch de capa tres, Cisco Catalyst 4507R es el encargado de administrar las 33 VLAN existentes, cada una de acuerdo al departamento o actividad asignados, entre las más relevantes están las VLAN 999 asignada a Telconet, la misma que permite la salida a Internet, igualmente las VLAN 114 y 115, que están asignadas a los Wireless LAN Controller, implementadas con el objetivo de tener un control centralizado del segmento WIFI, en este mismo concepto la VLAN 7 está asignada al segmento

inalámbrico al que tienen acceso los estudiantes, esta VLAN soporta alto tráfico en horas pico y debe estar totalmente controlada en sus contenidos, la VLAN 8 se asignó al segmento inalámbrico donde tienen acceso los docentes, la VLAN 6 contiene el servicio VoIP.

En la tabla 16 se detalla la información de las VLAN activas en la red del Campus.

Tabla 16
VLAN's - Campus Girón

VLAN	Nombre	Estado
1	Default	Active
3	ADMINISTRATIVA	Active
4	VLAN-RELOJ	Active
6	VoIP	Active
7	UPS-NET-ESTUDIANTES	Active
8	UPS-NET-DOCENTES	Active
9	VLAN-SALA-INTERNET	Active
10	VIDEO	Active
11	INTERNET	Active
12	IUS	Active
13	SOL	Active
14	INSPECTORIA-MINISTRATIVA	Active
15	ADB	Active
16	Abya-Yala	Active
17	CAMARA-IP	Active
18	LNS	Active
30	PACKET	Active
99	VLAN0099	Active
112	Administrativosv2	Active
114	VLAN-WLC	Active
115	VLAN-WLC2	Active
116	WLC-ESTUDIANTES	Active
118	IDIOMAS	Active
704	CECASIG	Active
708	CENTRO-MULTIMEDIAL	Active
710	SALA-DE-PROFESORES	Active
711	SALA-INTERNET	Active

810	SERVIDORES-INTERNOS	Active
820	SERVIDORES-PUBLICOS	Active
830	SERVIDORES-PROXY	Active
999	TELCONET	Active

2.2 Propuesta con IPv6.

Una vez que se ha realizado el levantamiento de estado inicial de la red del Campus Girón, se realizará la consiguiente propuesta de implementación del protocolo IPSec sobre la plataforma IPv6, para lo cual en primer lugar se deberá hacer un análisis del esquema de direccionamiento, posteriormente se deberá revisar los requisitos de hardware.

2.2.1 Propuesta de direccionamiento.

En el Ecuador, quien está encargado de administrar las direcciones IPv6 es el consorcio CEDIA, actualmente existen 13 redes IPv6 asignadas por LACNIC, de las cuales se identifica a la red de la Universidad Politécnica Salesiana, con la red 2800:68:0016::/48 (CEDIA, 2012), para los proveedores se tiene la dirección 2800:2a0::/32 asignada a Telconet y la dirección 2800:370::/32, asignada a CNT (CEDIA).

Para Latinoamérica y el Caribe, la dirección asignada por LACNIC es 2800::/12, en el caso de usuarios finales u organizaciones se asignan direcciones con prefijo /48 del rango. En éste caso se tiene el rango 2800:68::/32 que es de propiedad de CEDIA, este rango se ha subdividido en bloques más pequeños para las instituciones que son miembros, estos bloques son /48.

Las asignaciones se han realizado tomando en cuenta el RFC3177. Cada una de las instituciones que forman parte de CEDIA tienen un bloque /48 que da la posibilidad de que cada institución tenga 65536 subredes internas con prefijo /64. En el formato de la dirección IPv6 se considera la parte de red y parte de interface. La dirección asignada a la Politécnica Salesiana tiene una red /48, es decir tiene 64bits -48bits = 16 bits disponibles para las subredes, la asignación de direcciones internas debe considerar que las subredes más pequeñas deberán estar con prefijo /64 y se recomienda que sean asignadas a

Departamentos, donde se asume que internamente no se realizará otra subred dentro de ella.

Tomando en cuenta que la subred más pequeña será /64, eso quiere decir que en esta subred puede existir 2^{64} hosts, todas las interfaces serán /64, es decir de los 128 bits totales de cada dirección, los primeros 64 representarán la red, y los siguientes 64 representarán la interface. Para sumarizar, se tiene del bit 48 al 63, es decir con estos bits se puede tener 2^{16} (65536) subredes, lo cual es más que suficiente para la institución. De esta manera en la dirección 2800:0068:16:0001:A01:1200:0023:003; la parte subrayada pertenece a la porción de red y la parte restante pertenece a la porción de interface, los primeros 32 bits definen la red de CEDIA -> 2800:68, los siguientes 16 bits definen la red de la UPS ->:16:, los siguientes 16 bits definen a cada una de las redes de la UPS :1:, los últimos 64 bits son los que definen a un host específico: A01:1200:0023:003. El esquema de direccionamiento propuesto para el Campus Girón se detalla en la tabla 17.

Tabla 17
Esquema de direccionamiento IPv6

VLAN	Nombre	Dirección red	Prefijo
1	Default	2800:68:16:100::	56
3	ADMINISTRATIVA	2800:68:16:300::	56
4	VLAN-RELOJ	2800:68:16:1700::	56
6	IPT	2800:68:16:1800::	56
7	UPS-NET-ESTUDIANTES	2800:68:16:A00::	56
8	UPS-NET-DOCENTES	2800:68:16:A01::	56
9	VLAN-SALA-INTERNET	2800:68:16:A02::	56
10	VIDEO	2800:68:16:1900::	56
11	INTERNET	2800:68:16:2000::	56
12	IUS	2800:68:16:2100::	56
13	SOL	2800:68:16:2200::	56

Continua

14	INSPECTORIA-ADMINISTRATIVA	2800:68:16:2300::	56
15	ADB	2800:68:16:2400::	56
16	Abya-Yala	2800:68:16:2500::	56
17	CAMARA-IP	2800:68:16:2600::	56
18	LNS	2800:68:16:2700::	56
30	PACKET	2800:68:16:2800::	56
99	VLAN0099	2800:68:16:2900::	56
112	Administrativosv2	2800:68:16:3000::	56
114	VLAN-WLC	2800:68:16:3100::	56
115	VLAN-WLC2	2800:68:16:3200::	56
116	WLC-ESTUDIANTES	2800:68:16:3300::	56
118	IDIOMAS	2800:68:16:3400::	56
704	CECASIG	2800:68:16:3500::	56
708	CENTRO-MULTIMEDIAL	2800:68:16:3600::	56
710	SALA-DE-PROFESORES	2800:68:16:3700::	56
711	SALA-INTERNET	2800:68:16:3800::	56
810	SERVIDORES-INTERNOS	2800:68:16:200::	56
820	SERVIDORES-PUBLICOS	2800:68:16:4000::	56
830	SERVIDORES-PROXY	2800:68:16:4100::	56
999	TELCONET	2800:68:16:1000::	56

El esquema de direccionamiento considerará que cada dependencia reciba una dirección con prefijo /56, todas las subredes dentro de cada Facultad reciben una dirección /64, y todas las interfaces reciben una dirección /64. De acuerdo a las recomendaciones especificadas en las RFC 3177 y RFC 3531, se procede a la distribución de la planificación de direcciones IPv6, obteniéndose 32 dependencias con direcciones asignadas con prefijo /56, se

dispondrá adicionalmente de 255 subredes /64 dentro de cada dependencia con el fin de respetar la escalabilidad.

2.2.2 Requerimientos de infraestructura con IPv6.

La infraestructura actual con que cuenta el Campus Girón, permite la implementación del protocolo IPv6, la Institución realiza actualizaciones periódicas de hardware y software de acuerdo al cumplimiento del Plan Operativo Anual, documento guía que la Universidad toma como referencia para el cumplimiento de actividades a desarrollarse, por lo tanto los equipos y aplicaciones pueden trabajar con este protocolo, los estudios existentes sobre el protocolo IPv6 aplicado a la Universidad Politécnica Salesiana, solamente hacen referencia a: “Implementación de un plan piloto para la interconexión de IPv6 sobre IPv4, utilizando el protocolo dual stack en la Universidad Politécnica Salesiana Campus Sur dentro de la subred CIMA”, desarrollado por Moreno Constante Alex Alfonso y el trabajo denominado “Estudio, análisis y diseño para integrar a la UPS al protocolo de red IPv6 e incorporarla a Internet2”, por Muñoz Vallejo René Stalin, ambos trabajos no realizan el levantamiento de la infraestructura y requerimientos en el Campus Girón, razón por la cual se procedió a hacer un levantamiento del equipamiento de servidores y aplicaciones, determinándose que todos ellos cumplen con los requerimientos para trabajar con este protocolo. Los sistemas operativos de los servidores tienen las funcionalidades IPv6. El detalle de la plataforma de hardware y software del sistema operativo que posee la Universidad en el datacenter se muestra en la tabla 18.

Tabla 18
Infraestructura existente

Modelo	Tipo	Sistema Operativo	Aplicación	Soporta IPv6
Intel_Xeon_E5335_2.00GHz/60GB/2GB/NA	SERVIDOR BLADE HS21 8853	Windows Server Enterprise 2008 R2 X64	Proxy Centos	Si
Intel_Xeon_E5335_2.00GHz/40GB/2GB/NA	SERVIDOR BLADE HS21 8853	GNU/Linux Centos X64	Proxy Centos	Si

Intel_Xeon_E5335_2.00GHz/1,6TB/4GB/NA	SERVIDOR BLADE HS21 8853	GNU/Linux Centos X64	File Server,	Si
Intel_Xeon_E5335_2.00GHz/1,6TB/4GB/NA	SERVIDOR BLADE HS21 8853	Windows Server Enterprise 2003	Active directory 2008	Si
Intel_Xeon_E5335_2.00GHz/1,6TB/4GB/NA	SERVIDOR BLADE HS21 8853	GNU/Linux Centos X64	APM 2008	Si
Intel_Xeon_E5335_2.00GHz/450 GB/24 GB	SERVIDOR BLADE HS22 7870	Vmware: Windows 2008(3 Máquinas Virtuales)	Proxy Centos para laboratorios CECASIG	Si
Intel_Xeon_E5335_2.00GHz/4TB/ 64 GB	SERVIDOR BLADE HS22 7870	Vmware: 2 Windows 2008, 3 Centos (2 Máquinas Virtuales)	Mail	Si
Intel_Xeon3.60GHz/2X136,72GB/4GB/NA	DL-380G4	Windows Server Enterprise 2003	Tarifación y antivirus	Si
Intel Xeon_X5650_2,67GHz/2TB/8GB/	DL-380G7	Windows Server Enterprise 2008 R2 X64	Segmento SAN,storage core LTO de 21 cintas	Si
Intel_Xeon3.00GHz/500GB/2GB/NA	Clon	Windows Server Enterprise 2003	IVR	Si
Intel_Xeon3.00GHz/2X34,14GB/2GB/NA	Clon	Windows Server Enterprise 2003	DHCP / DNS	Si
Intel_Celeron3.20GHz/149,05GB/2GB/NA	Clon	Windows Server Enterprise 2003	TELEFONIA IP	Si
Intel_Celeron3.20GHz/149,05GB/2GB/NA	Clon	Windows Server	TELEFONIA IP	Si

Continua

		Enterprise 2003		
Intel_Celeron3.20GHz/149,05GB/2GB/NA	Clon	Windows Server Enterprise 2003	TELEFONIA IP	Si
Intel_DualCore3.0GHz/160GB/4GB/NA	Clon	GNU/Linux Centos X32	WEB	Si
Intel_PIV 3.0GB/160GB/2GB/NA	Clon	GNU/Linux Centos X32	SIEVAC	Si
Intel_PIV 3.0GB/160GB/2GB/NA	Clon	GNU/Linux Centos X32	Biométrico	Si
Intel_Core2Duo2.6GHz/320GB/2GB/NA*	Clon	GNU/Linux Centos X32	SQUID Estudiantes	Si
Intel_Core2Duo2.6GHz/320GB/2GB/NA*	Clon	GNU/Linux Centos X32	SQUID Docentes	Si
Intel_PIII 999Mhz STL2/17GB/512MB/NA	Clon	GNU/Linux Centos X32	Backup	Si
Quad Core Xeon E5410 Processor2x6MB Cache/ 750G/ 4G/	Dell PowerEdge 2950	Windows Server Enterprise 2008 R2 X64	Videoconf	Si
Dual core XEON/ 75 G, 75 G/ 2 Gb/	Dell PowerEdge 2850	Windows Server Enterprise 2008 R2 X64	Videoconf	Si
Intel Xeon_E5530_2.40GHz/24Gb	System x3500 M2	Vmware: 2 Windows 2008, 2 Centos	AVAC	Si

Continua

2.2.3 Planificación de la implementación de IPSec.

La implementación del protocolo requiere un proceso cuidadosamente planificado y coordinado, que incluye desde la gestión de cambios hasta capacitación al personal que está al frente de la administración de la red, esta investigación aporta en primera instancia un levantamiento de la infraestructura existente, la descripción de la arquitectura del protocolo, la propuesta de implementación que dará las pautas al administrador de TI para la puesta en

operación del protocolo y las pruebas hechas en base a la simulación del escenario, de esta manera se han identificado los siguientes lineamientos a tener en cuenta para la correcta planificación de la implementación del protocolo propuesto.

- **Análisis de situación inicial.-** Esta investigación ha determinado con claridad las razones para adoptar el nuevo protocolo de seguridad, en lo que refiere a los requerimientos del negocio, se deberá tener en cuenta la interoperabilidad entre los servicios que presta la institución, la infraestructura existente, la misma que luego de realizar el levantamiento de información demostró la capacidad de operar en entornos IPv6, por lo tanto es posible implementar IPSec, otro factor que se toma en cuenta es la criticidad de la información que se gestiona, como es el caso de la generada por el sistema de matriculación, aula virtual y gestión académica, el grupo de usuarios identificados como docentes, estudiantes y personal administrativo, genera información que debe ser tratada con altos niveles de seguridad, de acuerdo a cada una de sus actividades, es por lo tanto obligación de la Institución ofrecer los mecanismos adecuados para garantizar que la información se tramite de una forma segura, finalmente uno de los impedimentos para la difusión de IPv6 y sus protocolos asociados es la falta de conocimiento por parte de los responsables de TI, en este trabajo de define puntualmente la arquitectura de ambos protocolos y se demuestra la factibilidad de la operación de IPSec en el escenario propuesto, estos factores justifican la implementación de IPSec en el Campus.
- **Análisis de beneficios.-** La gestión de seguridades es una actividad crítica en el proceso de la administración de red, dentro de esta gestión se deben proveer los mecanismos para asegurar la confiabilidad, integridad y autenticidad de los datos, más aun de aquellos que revisten gran importancia para los procesos propios del modelo de negocio de la Institución, en este caso es la educación y la administración académica de los estudiantes, la información generada entonces debe ser protegida tanto a nivel de capa 2, capa 3 y capa 7, la implementación de IPSec al trabajar en capa 3 ofrece seguridad extra en el tráfico de las VLAN, adicionalmente un atacante difícilmente podría acceder en esta capa al flujo de datos puesto que se maneja

encriptación en un túnel virtual, los beneficios obtenidos con la implementación del protocolo de seguridad se reflejarán en elevar el nivel de protección en las respectivas VLAN seleccionadas de acuerdo al tipo de información que pasa por ellas, de esta manera se mantiene la continuidad del negocio puesto que la seguridad y la operatividad quedan garantizados.

- **Análisis de costos.-** Todo cambio en la configuración de una red conlleva los costos asociados, ya que en estos escenarios de migración se debe tener en cuenta las actualizaciones de hardware, software, aplicaciones y los costos operativos, en el caso de la Universidad, el impacto económico es muy bajo puesto que la inversión necesaria en lo referente a las actualizaciones de las aplicaciones para que sean compatibles con IPv6 y a las actualizaciones de los IOS en los router y en el switch core, ya ha sido hecha, de acuerdo a un plan progresivo de migración de IPv4 a IPv6 que se lo está llevando a cabo de acuerdo al Plan Operativo Anual.
- **Análisis de riesgos.-** La red es un ente dinámico y su comportamiento cambia de una u otra manera de acuerdo a los cambios de configuración que se realicen en ella, el potencial riesgo en el caso de la implementación de IPSec radica en el impacto que generará en el rendimiento de los segmentos de red donde estará configurado el mencionado protocolo, sin embargo como se especificará al final de la investigación en base a los resultados de la simulación, el impacto del protocolo en el tráfico no reviste un riesgo significativo para el funcionamiento de las aplicaciones que cursan por esas VLAN.

Un factor de riesgo a tomar en cuenta es aquel que refiere a la capacitación del personal que estará a cargo de la implementación, se deberá planificar puntualmente un cronograma de capacitación dirigido a los administradores de red y a los técnicos de TI, en primera instancia se deberá difundir la arquitectura y funcionalidades de IPv6, las vulnerabilidades del protocolo y finalmente la arquitectura e implementación de IPSec. El equipo técnico debe estar correctamente capacitado tanto para la configuración, monitoreo y solución de fallas, como para futuras actualizaciones. El propósito de esta investigación es ofrecer la información necesaria sobre las vulnerabilidades de IPv6, la arquitectura de IPSec, una guía de configuración y las pruebas de

funcionamiento del protocolo, de esta manera el riesgo técnico queda minimizado al momento de la implementación.

A nivel legal, el riesgo no existe puesto que para la propuesta de direccionamiento se ha tomado en cuenta muy puntualmente los parámetros y bloques de direcciones asignados por LACNIC.

- **Entrenamiento.-** El administrador de red junto con su equipo de técnicos deberán recibir una adecuada capacitación en lo que refiere a la arquitectura del protocolo IPv6 y de IPSec, como se ha demostrado en el levantamiento de estado inicial de la red, la infraestructura de conectividad es puramente de la marca CISCO, por lo tanto se recomienda un programa de capacitación a nivel de CCNP 1 (Flores, 2007) puesto que los contenidos manejan redes escalables, direccionamiento avanzado y ruteo entre otros temas, de esta manera el personal involucrado en el proceso de implementación tendrá el conocimiento necesario para realizar las configuraciones necesarias en los equipos encargados de la conectividad.
- **Equipos de transición.-** El administrador de red deberá crear un equipo de personas dedicadas exclusivamente a la tarea de implementación del protocolo, este equipo estará encabezado y bajo la autoridad del director del departamento de TI. Cada grupo de trabajo tendrá sus respectivas tareas de trabajo claramente definidas, los pasos a seguir se recomienda sean los siguientes:

En primer lugar se debe realizar la planificación del direccionamiento IPv6 tanto en los equipos activos de la red como en los host, para este efecto se ha dispuesto en esta investigación el rango de direcciones IP asignadas a la Institución por el CEDIA.

El segundo paso es la identificación de las VLAN´s a proteger, las mismas que serán aquellas que se han propuesto en este documento y han sido elegidas de acuerdo al tipo de información que transfieren, estas VLAN están configuradas en el switch CISCO Catalyst 4507R.

En tercer lugar se deberá configurar el protocolo de ruteo OSPF entre el switch CISCO Catalyst 4507R y los switch CISCO Catalyst 3750, cabe destacar que estos últimos soportan este protocolo de ruteo (CISCO), de acuerdo a la información obtenida del respectivo datasheet.

Finalmente se procederá a la configuración de los túneles IPSec en cada una de las VLAN seleccionadas, los parámetros de configuración se detallan en el apartado 3.3.7, donde se detalla con claridad los pasos a seguir. Las pruebas y monitoreo se realizarán de acuerdo a lo especificado en los manuales de gestión de red.

Planificación del piloto.- Cuando se introduce una nueva tecnología o un nuevo protocolo a una red en operación, es necesario primero hacer las pruebas preliminares en laboratorio, donde se puede controlar las variables y corregir los errores, para realizar este proceso se deberá realizar tareas como:

- **Identificación del plan de direccionamiento**, el que permitirá identificar el rango de direcciones que se van a usar.
- **El tipo de red** a usarse, en este caso es una red IP,
- **Los servicios de red**, que en este caso serán los mismos que actualmente existen en la red IPv4.
- **La administración de red.-** se manejará de la misma manera y con los mismos parámetros como se lo hace en el entorno IPv4
- **Aplicaciones de red.**-Se manejarán las mismas aplicaciones que al momento la Universidad las tiene, por ejemplo VoIP y videoconferencia.

Planificación del direccionamiento. Como se especificó en el apartado 2.2.1, el direccionamiento se ha planificado de acuerdo al bloque de direcciones asignado por LACNIC y CEDIA para la Universidad, con la red 2800:68:0016:: , para los proveedores se tiene la dirección 2800:2a0::/32 asignada a Telconet y la dirección 2800:370::/32, asignada a CNT. Las subredes más pequeñas estarán con prefijo /56, así el rango asignado en la planificación está desde la dirección 2800:68:16:100::/56 hasta la 2800:68:16:4000::/56, de acuerdo a la tabla 2.5, cada dependencia recibe una dirección con prefijo /56, obteniéndose 32 dependencias.

- **Mecanismos de transición.-** En base a la capacidad de coexistir IPv4 e IPv6, durante el diseño se debe tomar en cuanta cuáles serán los mecanismos a usar para migrar de un protocolo a otro, puede ser tunneling, dual stack o traducción. En el caso de la UPS, el escenario es IPv6 nativo, todos los host,

servidores, equipos activos, servicios y aplicaciones trabajarán exclusivamente con este protocolo.

Seguridad.- Una organización debe destinar una gran cantidad de recursos para garantizar la seguridad de los datos, en este caso la investigación se centra exclusivamente en el protocolo IPSec, tanto el piloto, como la implementación propuesta manejarán este protocolo, en el capítulo anterior ya se realizó la revisión del funcionamiento del protocolo de seguridad, por lo tanto los conceptos están claros para su posterior implementación.

2.2.4 Propuesta de implementación de los túneles IPSec.

IPSec se configurará en modo túnel puesto que todo el paquete se someterá a un proceso de cifrado con 3DES y a un autenticado por medio de clave pre compartida con MD5, adicionalmente este modo permite establecer la seguridad entre los Security Gateway sin necesidad de configurar IPSec en los host, haciéndolo más flexible en el caso de implementar un mayor número de host a cada segmento protegido, igualmente la combinación de las SA será de acuerdo al Caso I por tres razones, primero el escenario es una intranet y el protocolo se configurará entre los Security Gateway internos, segundo se usará exclusivamente la cabecera ESP y finalmente se generarán varias SA's entre el switch core y cada switch de distribución respectivamente. No se escogió el modo transporte por que se protege solo a la carga útil y la cabecera IP no se somete a modificación, esto podría dar lugar a generar una vulnerabilidad en el escenario de implementación, así mismo los modos II, III y IV no se tomaron en cuenta porque no se está pasando por el entorno Internet.

Luego de un análisis de vulnerabilidades a las que están sujetos los servicios que ofrece la red del Campus Girón, se determinó con claridad cuáles serán las VLAN donde se implementará IPSec, de acuerdo a los criterios expuestos anteriormente, de esta manera se ha decidido proteger las siguientes VLAN:

Administrativa.- Esta VLAN es usada para la gestión de la información del sistema administrativo de docentes y estudiantes, por ejemplo de facturación, documentación, matriculación y notas, entre otras aplicaciones.

IUS.- Esta VLAN transfiere información entre la Red Internacional de Universidades Salesianas y la UPS.

SOL.- Aquí se maneja la información del sistema de educación virtual

Inspectoría-Administrativa.- En esta VLAN se maneja información importante de los procesos administrativos correspondientes a la Inspectoría Salesiana.

Abya-Yala.- Este segmento maneja información relevante al departamento de imprenta.

LNS.- La información generada por la librería gestiona tópicos como pedidos, transacciones e inventario entre otros, por lo que debería estar protegida

Administrativos V2.- La información que se genera en este segmento reviste importancia puesto que pertenece a aquella generada por el sistema QUIPUX, de documentación electrónica

VLAN WLC.- Las controladoras de la red inalámbrica deberán estar protegidas puesto que gestionan las configuraciones de los puntos de acceso de toda la red WIFI.

VLAN WLC2.- El criterio se aplica como en el caso anterior.

WLC Estudiantes.- El criterio se aplica como en el caso anterior.

Idiomas.- En este segmento se transfiere información que tiene que ver con las matrículas y procesos académicos pertenecientes al Instituto de Inglés, así como la respectiva información administrativa propia de las actividades del instituto.

Servidores Internos.- A esta VLAN están conectados todos los servidores que ofrecen servicios a nivel interno, así sea cual fuere las función de cada uno de ellos, el segmento debería estar totalmente protegido.

Servidores Públicos.- A esta VLAN están conectados todos los servidores que ofrecen servicios externamente, así sea cual fuere las función de cada uno de ellos, el segmento en debería estar totalmente protegido

Servidores proxy.- Esta VLAN deberá estar obligatoriamente protegida, puesto que el servidor proxy directamente está dentro de la infraestructura de seguridad.

En la tabla 19 se detalla el listado de las VLAN´s del Campus Girón que serán protegidas y las que no, de acuerdo a los criterios anteriormente expuestos.

Tabla 19
Detalle de las VLAN a ser protegidas

VLAN	Nombre	Dirección de red	IPSec
1	Default	2800:68:16:100::	No
3	ADMINISTRATIVA	2800:68:16:300::	Si
4	VLAN-RELOJ	2800:68:16:1700::	No
6	IPT	2800:68:16:1800::	No
7	UPS-NET-ESTUDIANTES	2800:68:16:A00::	No
8	UPS-NET-DOCENTES	2800:68:16:A01::	No
9	VLAN-SALA-INTERNET	2800:68:16:A02::	No
10	VIDEO	2800:68:16:1900::	No
11	INTERNET	2800:68:16:2000::	No
12	IUS	2800:68:16:2100::	Si
13	SOL	2800:68:16:2200::	Si
14	INSPECTORIA-ADMINISTRATIVA	2800:68:16:2300::	Si
15	Audiovisuales Don Bosco	2800:68:16:2400::	No
16	Abya-Yala	2800:68:16:2500::	Si
17	CAMARA-IP	2800:68:16:2600::	No
18	LNS	2800:68:16:2700::	Si

Continua

30	PACKET	2800:68:16:2800::	No
99	VLAN0099	2800:68:16:2900::	No
112	Administrativosv2	2800:68:16:3000::	Si
114	VLAN-WLC	2800:68:16:3100::	Si
115	VLAN-WLC2	2800:68:16:3200::	Si
116	WLC-ESTUDIANTES	2800:68:16:3300::	Si
118	IDIOMAS	2800:68:16:3400::	Si
704	CECASIG	2800:68:16:3500::	No
708	CENTRO-MULTIMEDIAL	2800:68:16:3600::	No
710	SALA-DE-PROFESORES	2800:68:16:3700::	No
711	SALA-INTERNET	2800:68:16:3800::	No
810	SERVIDORES-INTERNOS	2800:68:16:200::	Si
820	SERVIDORES-PUBLICOS	2800:68:16:4000::	Si
830	SERVIDORES-PROXY	2800:68:16:4100::	Si
999	TELCONET	2800:68:16:1000::	Si

Elaborado por: Jorge López

En la figura 47, se muestra la topología lógica del Campus Girón, en rojo se ha indicado las VLAN que se las va a proteger, de acuerdo a la información que maneja cada una de ellas.

Adicionalmente se puede observar que se está protegido todo el segmento donde están situados los dispositivos encargados de la seguridad de la red.

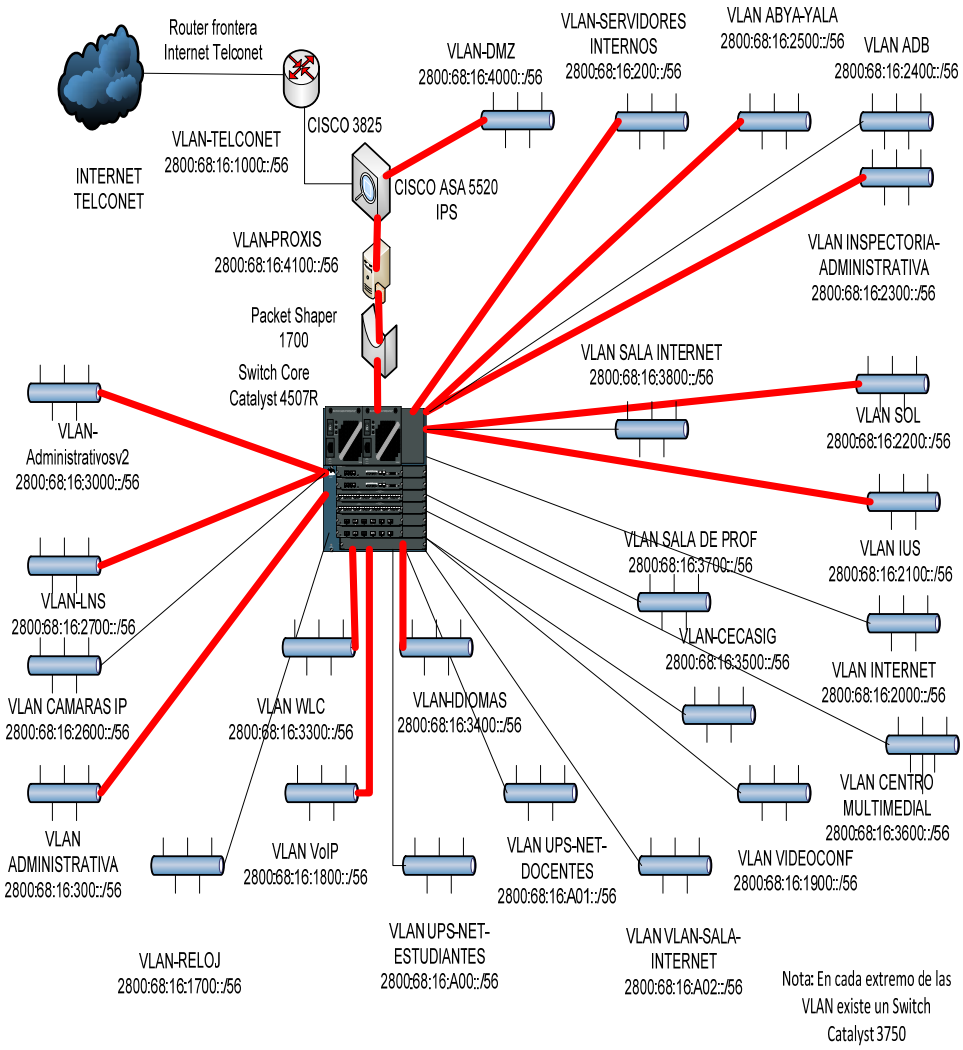

Figura 47 Diagrama de las VLAN a proteger con IPSec
Fuente: Universidad Politécnica Salesiana

Como se puede apreciar en la figura anterior, se ha propuesto la implementación de los túneles IPSec entre el switch core y las respectivas VLAN seleccionadas de acuerdo a los criterios expuestos anteriormente, las mismas que están resaltadas en rojo, cabe destacar que no se han tomado en cuenta todas las VLAN del Campus puesto que al implementar en todas ellas los túneles IPSec, daría como resultado una carga extra en el equipo del core, y como consiguiente impactaría notoriamente en el tráfico ya que el proceso de implementación de IPSec requiere cabeceras extras como la ESP, adicionalmente debe generar procesos como la compartición de claves y la generación de las interfaces tunnel.

CAPITULO III

ANÁLISIS DE FACTIBILIDAD CON IPSEC EN IPV6

3.1 Diseño lógico en IPv6.

El diseño lógico se tomará de acuerdo a la distribución de las VLAN, ya especificado en la tabla 2.5, del apartado 2.2.1, de acuerdo a los estándares dados por LACNIC y por la red CEDIA, así se han identificado las VLAN junto con la dirección y prefijo asignados y se dispondrán de acuerdo a la figura 48.

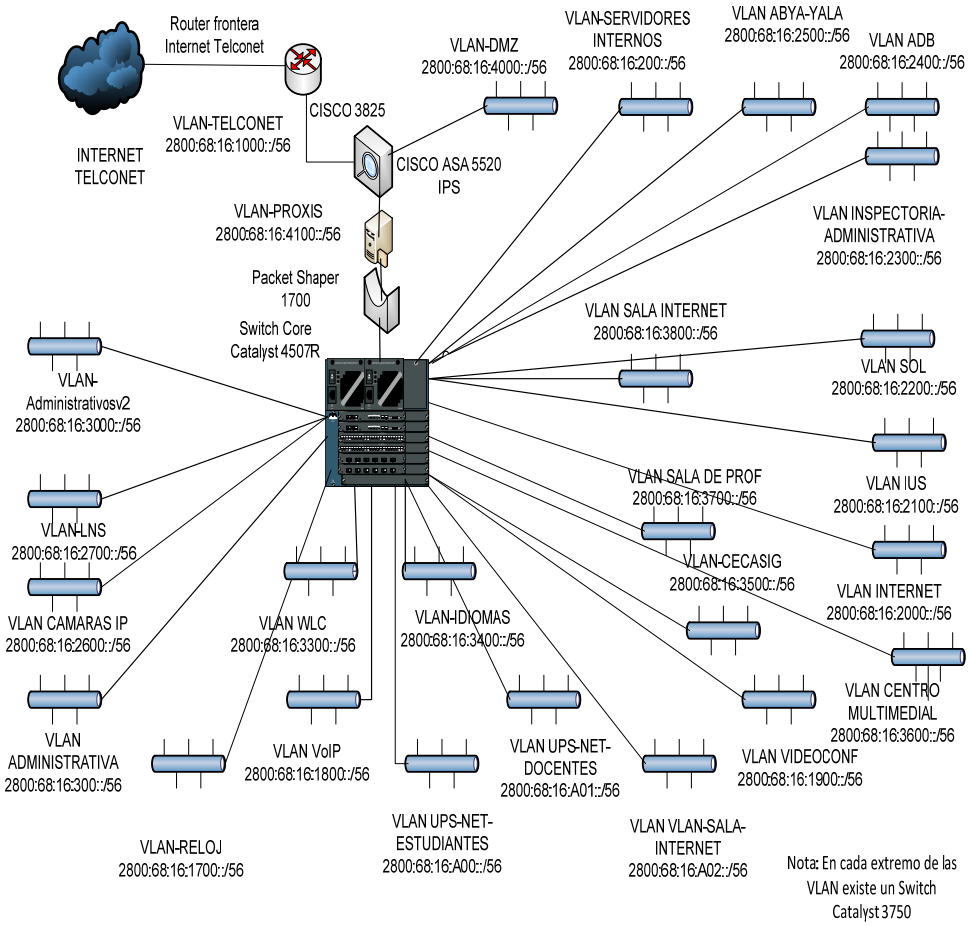

Figura 48 Diseño Lógico

Fuente: Universidad Politécnica Salesiana

La VLAN 820 que lleva el nombre de SERVIDORES-PUBLICOS, que en otras palabras pertenecen a la DMZ, la VLAN 830 llamada SERVIDORES-PROXY y la VLAN 999 denominada TELCONET estarán conectadas al ASA 5520, tal como se muestra en la figura 3.1. El resto de las VLAN estarán configuradas en el Catalyst 4507R.

3.2 Diseño físico en ipv6.

El diseño físico se lo realizará tomando en cuenta la infraestructura existente en la actualidad en el Campus Girón, a nivel de hardware, los equipos soportan el protocolo IPv6.

3.2.1 Topología física.

La topología física tiene cuatro grandes sectores que presentan relevancia, estos son la parte de acceso a Internet, que se realizará por medio de los router 3825 para el caso de Telconet, y 2801 para el caso de CNT.

Igualmente se dispone del servidor de acceso remoto a la PTSN al igual que la salida VoIP por medio del Gateway; se tiene la DMZ, donde se ubicarán los servidores públicos. La seguridad está compuesta por el ASA 5520, el pool de servidores proxy y el Packet Shaper 1700. Los servidores internos y todo lo que es acceso y distribución están directamente conectados al switch core Catalyst 4507R. Tal como se muestra en la figura 49.

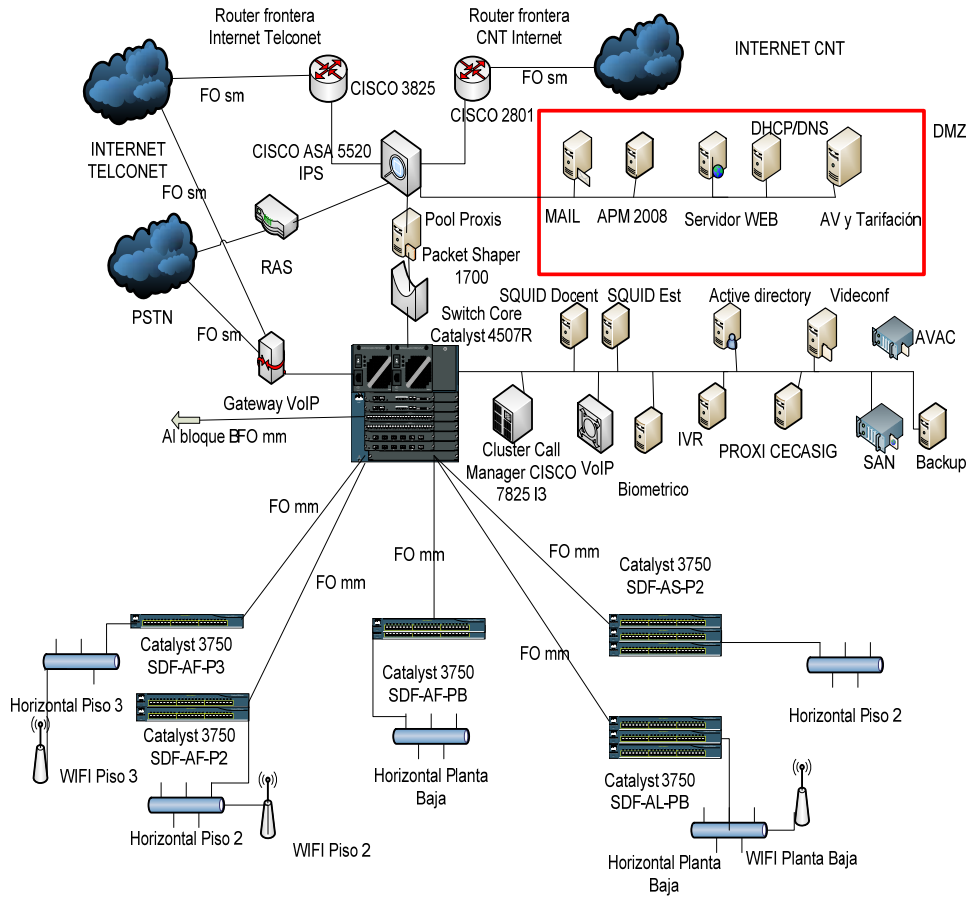

Figura 49 Topología física del bloque A

Fuente: Universidad Politécnica Salesiana

El bloque A mantiene una interconexión con el bloque B por medio de un enlace de fibra óptica multimodo, en este bloque, el núcleo es otro switch Catalyst 4507R donde irán conectados los switch de piso Catalyst 3750, los que a su vez mantendrán la conectividad con los segmentos de cableado horizontal y con los accesos inalámbricos, tal como se aprecia en la figura 50.

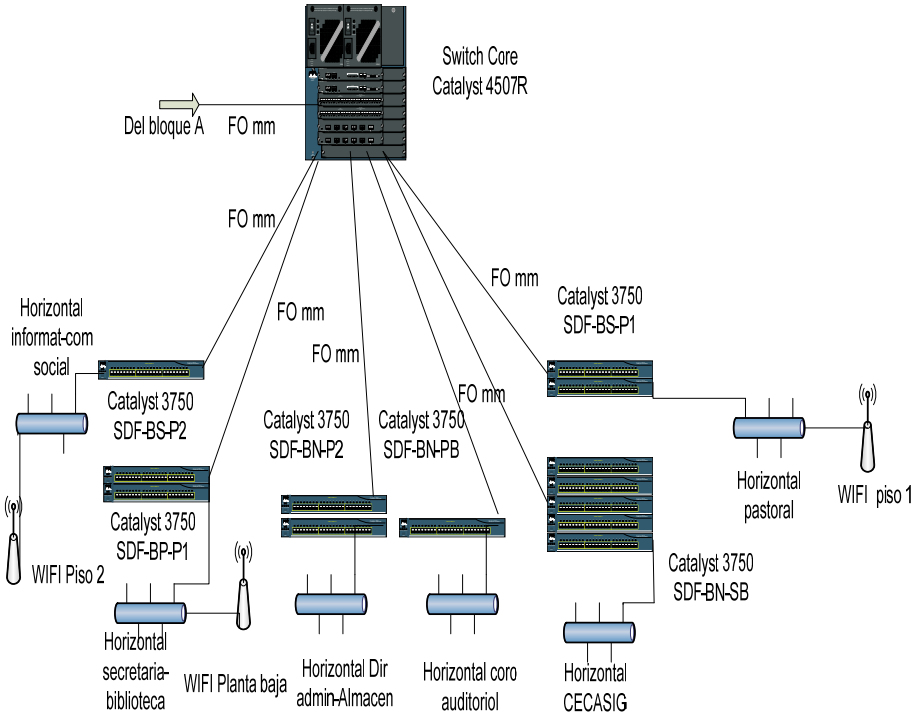

Figura 50 Topología física del bloque B

Fuente: Universidad Politécnica Salesiana

3.3 Simulación de implementación con IPSec.

Este proceso se lo realizará en una plataforma de simulación conocida como GNS3, se escogió esta aplicación puesto que permite obtener los datos muy cercanos a los reales, adicionalmente trabaja con los IOS reales de CISCO, por lo que las configuraciones, y los resultados serán los mismos que se los tendrían en el caso de trabajar con equipos reales. En los siguientes puntos se verán los detalles de la realización de este proceso.

3.3.1 Diseño físico empleado en la simulación.

En la figura 51 se muestra el diseño físico implementado en la simulación, toda la infraestructura es Cisco.

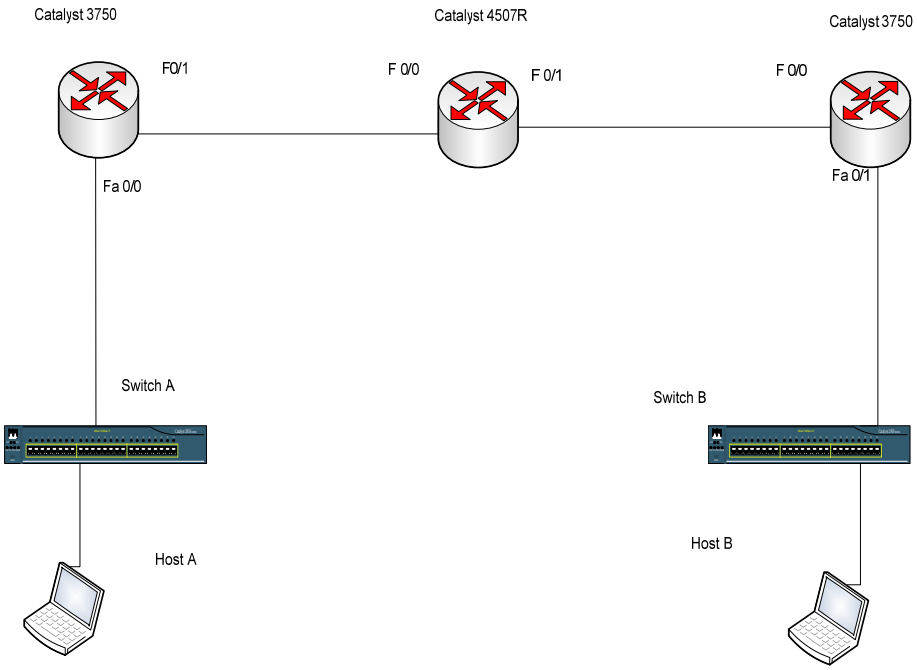

Figura 51 Diseño físico implementado en la simulación

3.3.2 Diseño lógico implementado.

Para el diseño lógico se ha previsto el mismo esquema de direccionamiento asignado a la Universidad, previamente se ha definido la clave pre-compartida, en un formato alfanumérico, el IOS usado en la simulación es el implementado en el emulador del router Cisco 2691, esta versión del IOS permite la implementación de los protocolos de seguridad como IPSec, algoritmos de seguridad DES, 3DES, AES. En la figura 52 se muestra el diseño lógico a implementarse en la simulación.

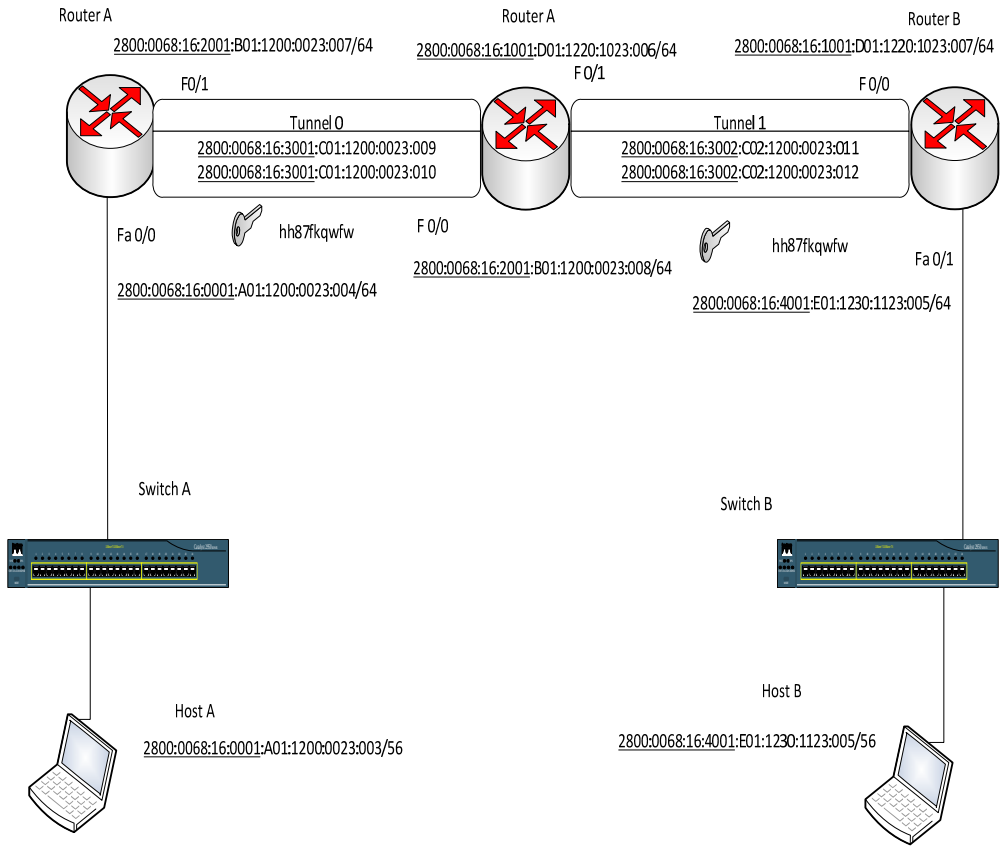

Figura 52 Diseño lógico implementado

3.3.3 Software de simulación GNS3.

GNS3 es un emulador-simulador gráfico de redes, soporta la plataforma CISCO IOS de routers, equipos ATM, Frame Relay, switch Ethernet y PIX firewalls, está basado en la plataforma Dynamips, fue desarrollado en Python a través de PyQt, la interfaz gráfica ofrece entornos reales al usar la tecnología SVG para proveer alta calidad en la presentación del diseño de las topologías de red. Dynamips es un emulador de routers Cisco para plataformas 1700, 2600, 3600, 3700 y 7200, permite ejecutar imágenes de IOS estándar de esos dispositivos.

Entre las características más relevantes se puede mencionar que GNS3 permite el diseño de topologías de red complejas, incluye herramientas como WireShark, con el fin de capturar el tráfico entre cualquiera de los dispositivos simulados. Adicionalmente permite asociar una interfaz de red real para enviar tráfico por ella.

3.3.4 Escenario de simulación.

La simulación está formada por dos routers CISCO 2961, dos switch Ethernet y dos host, se debe disponer cada uno de los dispositivos al espacio de trabajo y configurar tanto sus interfaces como el protocolo de ruteo dinámico.

La topología final será la siguiente: los routers Catalyst_3750 y Catalyst3750 estarán directamente conectados por medio de la interface serial, por las interfaces Ethernet el router Catalyst_3750 está conectado al switch Ethernet y este a su vez al Host A, el router Catalyst3750 está conectado al switch Ethernet y este a su vez al Host B, tal como se muestra en la figura 53.

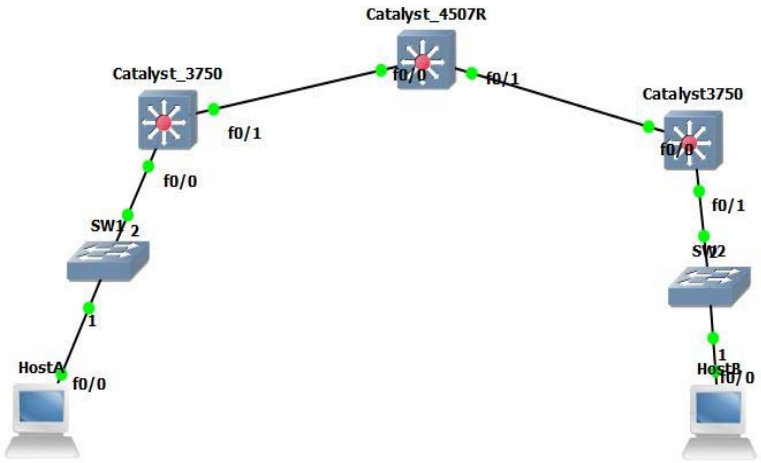

Figura 53 Escenario de simulación implementado
Fuente: Captura del programa GNS3

Para conectar los router mediante las interfaces, se usa el icono con forma de conector ubicado en el panel de controles superior del espacio de trabajo, hacer click en uno de los nodos a conectar, arrastrándolo hasta el otro nodo, posteriormente es necesario activar los nodos con el icono play. Una vez que las interfaces señalen el status activo, se debe abrir las consolas de cada uno de los nodos, que emularán las consolas de los routers, se puede entonces usar el Cisco IOS command-line interface y proceder a configurar el router exactamente como si se lo realizara en un equipo físico.

3.3.5 Configuración de la simulación.

Se requiere definir los parámetros inicialmente para configurar las interfaces y posteriormente para el protocolo IPSec, por lo tanto es necesario establecer una tabla donde se especifiquen datos a usarse en los routers denominados Catalyst_3750 y Catalyst3750. Todo esto se muestra en la tabla 20.

Tabla 20
Requisitos de Configuración

DESCRIPCION	HOST A	HOST B	ROUTER A	Switch Core	ROUTER B
Nombre del dispositivo	Host A	Host B	Catalyst_3750	Catalyst_4750R	Catalyst3750
Versión del IOS	No	No	c2691-advipservicesk9-mz.124-15.T6	c2691-advipservicesk9-mz.124-15.T6	c2691-advipservicesk9-mz.124-15.T6
Contraseña de consola	No asignada	No	Cisco	Cisco	Cisco
Dirección IPv6 Fa0/0	2800:68:16:1:A01:1200:23:3	2800:68:16:4001:E01:1230:1123:6	2800:68:16:1:A01:1200:23:4	2800:68:16:2001:B01:1200:23:8	2800:68:16:1001:D01:1220:1023:7
Dirección IPv6 Fa0/1	2800:0068:0016:1:A01:1200:23:2	No	2800:68:16:2001:B01:1200:23:7	2800:68:16:1001:D01:1220:1023:6	2800:68:16:4001:E01:1230:1123:5
Dirección IPv6 Tunnel0	No	No	2800:68:16:3001:C01:1200:23:9	2800:68:16:3001:C01:1200:23:10	
Dirección IPv6 Tunnel1				2800:68:16:3002:C02:1200:23:11	202:C02:1200:23:12
Protocolo de ruteo	No	No	OSPF	OSPF	OSPF
Protocolo de ruteo del túnel	No	No	Estático	Estático	Estático
Clave	No	No	hh87fkqwfw	hh87fkqwfw	hh87fkqwfw
Protocolo de seguridad	No	No	IPSec, IKE, ISAKMP	IPSec, IKE, ISAKMP	IPSec, IKE, ISAKMP
Algoritmo de cifrado	No	No	3DES	3DES	3DES
Algoritmo hash	No	No	MD5	MD5	MD5

Continua

Intercambio de llaves	No	No	Diffie-Hellman Grupo 1 de 768 bits	Diffie-Hellman Grupo 1 de 768 bits	Diffie-Hellman Grupo 1 de 768 bits
Método de autenticación	No	No	Pre-share	Pre-share	Pre-share
Tiempo de vida IKE	No	No	86400 segundos	86400 segundos	86400 segundos

En esta tabla también se especifican las direcciones tanto para las interfaces Fast Ethernet, serial y para la configuración del túnel virtual, así mismo la contraseña compartida, el algoritmo hash, el método de intercambio de claves y el tiempo de vida de la sesión.

3.3.6 Configuración básica.

Inicialmente se procederá con las configuraciones de las interfaces fast Ethernet y serial respectivamente, esto en ambos routers, siguiendo los lineamientos de la tabla 20, posteriormente se configurará sobre estas interfaces, el protocolo de ruteo dinámico OSPF, el detalle de las configuraciones se expone a continuación.

Catalyst 3750

Catalyst_3750(config)# interface fastethernet 0/0 // Especifica la interface donde se va a implementar la configuración//

Catalyst_3750(config-if)# ipv6 enable // activa el protocolo IPv6//

Catalyst_3750(config-if)# ipv6 address 2800:0068:16:0001:A01:1200:0023:004/64 //asigna una dirección ipv6 a la interface//

Catalyst_3750(config-if)# ipv6 ospf 1 area 0 //Activa el protocolo de ruteo//
Catalyst_3750(config-if)# no shutdown // Habilita la interface//
Catalyst_3750(config-if)# exit
Catalyst_3750(config)# ipv6 router ospf 1
Catalyst_3750(config-rtr)# router-id 10.1.1.3 //Establece una identificación para el proceso de ruteo//
Catalyst_3750(config-rtr)# exit // sale del modo de configuración anterior//

Catalyst_3750(config)# ipv6 unicast-routing //Activa el reenvío de paquetes IPv6 en modo unicast //

Catalyst_3750(config)# interface fastethernet 0/1

Catalyst_3750(config-if)#ipv6 address 2800:0068:16:2001:B01:1200:0023:007/64 //asigna una dirección ipv6 a la interface//

Catalyst_3750(config-if)# ipv6 ospf 1 area 0 //Activa el protocolo de ruteo//

Catalyst_3750(config-if)# no shutdown // Habilita la interface//

Catalyst_3750(config-if)# exit // Sale del modo de configuración anterior//

Catalyst_3750(config)# ipv6 router ospf 1

Catalyst_3750(config-rtr)# router-id 10.1.1.3 //Establece una identificación para el proceso de ruteo//

Catalyst_3750(config)# exit

Catalyst_3750(config)# ipv6 unicast-routing //Activa el reenvío de paquetes IPv6 en modo unicast //

Catalyst_4507R

Catalyst_4507R(config)# interface fastethernet 0/0//especifica la interface donde se va a implementar la configuración//

Catalyst_4507R(config-if)# ipv6 enable // activa el protocolo IPv6//

Catalyst_4507R(config-if)#ipv6 adress 2800:0068:16:2001:B1:1200:0023:008/64 //asigna una dirección ipv6 a la interface//

Catalyst_4507R(config-if)# ipv6 ospf 1 area 0 //Activa el protocolo de ruteo//

Catalyst_4507R(config-if)# no shutdown // Habilita la interface//

Catalyst_4507R(config-if)# exit

Catalyst_4507R(config)# ipv6 router ospf 1

Catalyst_4507R(config-rtr)# router-id 10.1.1.4 //Establece una identificación para el proceso de ruteo//

Catalyst_4507R(config-rtr)# exit // sale del modo de configuración anterior//

Catalyst_4507R(config)# ipv6 unicast-routing //Activa el reenvío de paquetes IPv6 en modo unicast //

Catalyst_4507R(config)# interface fastethernet 0/1

Catalyst_4507R(config-if)#ipv6 address
2800:0068:16:1001:D1:1220:1023:006/64 //asigna una dirección ipv6 a la interface//
Catalyst_4507R(config-if)# ipv6 ospf 1 area 0 //Activa el protocolo de ruteo//
Catalyst_4507R(config-if)# no shutdown // Habilita la interface//
Catalyst_4507R(config-if)# exit // sale del modo de configuración anterior//
Catalyst_4507R(config)# ipv6 router ospf 1
Catalyst_4507R(config-rtr)#router-id 10.1.1.4 //Establece una identificación para el proceso de ruteo//
Catalyst_4507R(config)# exit
Catalyst_4507R(config)# ipv6 unicast-routing //Activa el reenvío de paquetes IPv6 en modo unicast //

Catalyst3750

Catalyst3750(config)# interface fastethernet 0/0 // Especifica la interface donde se va a implementar la configuración//

Catalyst3750(config-if)# ipv6 enable // activa el protocolo IPv6//
Catalyst3750(config-if)#ipv6 address
2800:0068:16:1001:D01:1220:1023:007/64 //asigna una dirección ipv6 a la interface//

Catalyst3750(config-if)# ipv6 ospf 1 area 0 //Activa el protocolo de ruteo//
Catalyst3750(config-if)# no shutdown
Catalyst3750(config-if)# exit
Catalyst3750(config)# ipv6 router ospf 1
Catalyst3750(config-rtr)# router-id 10.1.1.5 //Establece una identificación para el proceso de ruteo//
Catalyst3750(config-rtr)# exit
Catalyst3750(config)# ipv6 unicast-routing //Activa el reenvío de paquetes IPv6 en modo Unicast //
Catalyst3750(config)# interface fastethernet 0/1
Catalyst3750(config-if)#ipv6 address
2800:0068:16:4001:E01:1230:1123:005/64 //asigna una dirección ipv6 a la interface//

Catalyst3750(config-if)# ipv6 ospf 1 area 0 //Activa el protocolo de ruteo//
Catalyst3750(config-if)# no shutdown // Activa la interface//
Catalyst3750(config-if)# exit // Sale del modo de configuración anterior//
Catalyst3750(config)# ipv6 router ospf 1
Catalyst3750(config-rtr)# router-id 10.1.1.5 //Establece una identificación para el proceso de ruteo//
Catalyst3750(config-rtr)# exit
Catalyst3750(config)# ipv6 unicast-routing //Activa el reenvío de paquetes IPv6 en modo unicast //

3.3.7 Configuración de IPSec.

Para implementar IPSec, inicialmente se debe implementar los parámetros IKE, utilizados para validar las políticas entre pares, este protocolo define el método de intercambio de claves sobre IP en la fase de negociación segura, los pares intercambian las políticas IPSec para la autenticación y la encriptación del tráfico de datos. IKE controla la autenticación, el algoritmo de encriptación y el método de intercambio de claves usado por las políticas para encriptar tráfico de datos enviado a través de un túnel VPN, este control se lo realiza en ambos extremos.

Para permitir la negociación, en primer lugar hay que crear una política ISAKMP y configurar la asociación entre los pares que participan en esta política, en este punto se define la autenticación, los algoritmos de encriptación y la función hash utilizada para enviar tráfico de control entre los dos nodos de la VPN. La elección de un algoritmo de encriptación controlará la confidencialidad del canal de control entre los dos nodos, adicionalmente el algoritmo hash controla la integridad de los datos. Para la autenticación de claves pre-compartidas se usará encriptación 3DES y MD5 como algoritmo hash, adicionalmente se usa Diffie-Hellman grupo 1 para crear una clave secreta compartida por los pares para la política IKE. La SA tendrá un tiempo de vida de 86400 segundos, que es tiempo máximo en el que una política de seguridad se utiliza sin necesidad de negociarla de nuevo, esta configuración se debe aplicarla a los dos nodos.

El ipsec transform-set es un parámetro de configuración cifrada que negocian los routers para formar las SA. IKE está formado por una cabecera de autenticación, en esta simulación se usara el modo túnel, razón por la cual se usará la cabecera ESP, se procederá a configurar el túnel IPSec, inicialmente se implementará una política IKE y una clave pre-compartida en el router A. La política será la misma en los dos extremos:

Catalyst_3750

Catalyst_3750 (config)# crypto isakmp policy 1 //configuración de la política IKE con prioridad 1, al crear la nueva política IKE, de debe identificar cada una con un prioridad definida de 1 a 10000, donde 1 es la prioridad más alta, lo que define que esta política será gestionada primero

Catalyst_3750 (config-isakmp-policy)# authentication pre-share //establece el modo de autenticación con clave precompartida, solamente el modo pre-share es soportado por IPv6, los modos RSAencr y RSAsig son soportados por IPv4.

Catalyst_3750 (config-isakmp-policy)# hash md5 //establece md5 o message digest 5 como algoritmo de hash para garantizar la integridad, las opciones adicionales son SHA o secure hash algorithm, se escogió MD5 puesto que genera una salida de 128 bits a diferencia de SHA que lo hace con 160 bits (CISCO, 2012), convirtiendo a MD5 en más eficiente.

Catalyst_3750 (config-isakmp-policy)# group 1 //especifica el método de intercambio de claves con el identificador de grupo de Diffie-Hellman en la política IKE, las opciones son: 1 para un identificador de grupo de 768 bits, 2 para un identificador de 1024 bits y 5 para un identificador de 1536 bits (ciscoipv6ttechtips, 2011), los grupos 2 y 5 ofrecen una seguridad más efectiva pero su rendimiento es pobre, se escogido el grupo 1 por el rendimiento que ofrece dentro del túnel IPSec (Watch Guard System Manager Help, 2010) , las funcionalidades del intercambio de claves se especifican con más claridad en el ítem 1.5.14

Catalyst_3750 (config-isakmp-policy)# encryption 3des //especifica 3DES como algoritmo de cifrado, se escogió este tipo de encriptación porque es

ampliamente usado en entornos de seguridad, sin embargo está siendo desplazado por AES puesto que este último es más seguro y eficiente, las opciones a configurar son: DES, 3DES, AES, AES 192, AES 256, se recomienda en la implementación usar AES256 por su nivel de seguridad.

Catalyst_3750 (config-isakmp-policy)# lifetime 86400 //especifica el tiempo de vida en segundos para la SA, es el tiempo máximo en el que una política de seguridad se utiliza sin necesidad de negociarla de nuevo. Este valor se ha escogido para que la política dure 1 día, el valor en segundos queda a criterio del administrador de red, si es muy corto el establecimiento de la SA impactará en el rendimiento, si es muy largo se corre el riesgo de convertirse en una brecha e seguridad. La configuración se deberá aplicar a los dos nodos donde se aplica el túnel

Catalyst_3750 (config-isakmp-policy)# exit

R1(config)#crypto isakmp key 0 cisco address ipv6 2800:0068:16:2001:B01:1200:0023:008/128 //define la clave precompartida, “hh87fkqwfw”,en texto plano, “0”, y la IP del que será el otro extremo del túnel

Catalyst_3750 (config)# crypto keyring ANILLO //define el nombre del keyring que se usará durante la autenticación, el keyring es el repositorio de claves que negocia IPSec.

Catalyst_3750 (config-keyring)# pre-shared-key address ipv6 2800:0068:16:2001:B01:1200:0023:008/128 key chh87fkqwfw //define la clave precompartida a usar durante la autenticación IKE, la dirección IP deberá ser la de la interfaz de llegada del otro extremo.

Catalyst_3750 (config-keyring)# exit

R1(config)# crypto ipsec transform-set TRANSFORMADA esp-3des //define un transform-set, es decir, una combinación de protocolos y algoritmos que sea aceptada por los routers IPSec, en este caso como el modo de trabajo es tipo túnel, se debe poner ESP, si fuese en modo transporte debería ir AH

Catalyst_3750 (cfg-crypto-trans)# crypto ipsec profile PERFIL //define los parámetros que se van a usar para el cifrado IPSec entre los dos routers

Catalyst_3750 (ipsec-profile)# set transform-set TRANSFORMADA //especifica el nombre del transform-set que se va a usar, es un nombre que identifica el proceso, un transform-set define las políticas de seguridad que serán aplicadas al tráfico que entra o sale de la interfaz, en el ítem 3.3.7 se explica puntualmente la funcionalidad de este comando.

Catalyst_3750 (ipsec-profile)# exit

Catalyst_3750 (config)# interface tunnel 0 //configuración de la interfaz virtual tunnel 0 aplicada a la interfaz del router origen

Catalyst_3750 (config-if)# ipv6 address
2800:0068:16:3001:C01:1200:0023:009/64

Catalyst_3750 (config-if)# ipv6 enable

Catalyst_3750 (config-if)# tunnel source
2800:0068:16:2001:B01:1200:0023:007 //define el origen del túnel, en la interfaz física del router origen.

Catalyst_3750(config-if)# tunnel destination
2800:0068:16:2001:B1:1200:0023:008 //define el destino del túnel, en la interfaz física del router destino.

Catalyst_3750 (config-if)# tunnel mode ipsec ipv6 //establece el modo de encapsulamiento para la interfaz tunnel 0

Catalyst_3750 (config-if)# tunnel protection ipsec profile PERFIL //asocia la interfaz tunnel 0 con el perfil

Catalyst_3750(config-if)# exit

Catalyst_3750 (config)# ipv6 route 2800:0068:16:4001:E01:1230:1123:005/64 tunnel 0 //configura una ruta estática de forma que todo el tráfico que vaya a la red local de la derecha pase por el túnel, se recomienda en este caso generar la ruta estática puesto que el administrador tendrá un control total de este enlace.

Catalyst_4507R

Catalyst_4507R (config)# crypto isakmp policy 1 //configuración de la política IKE con prioridad 1

Catalyst_4507R(config-isakmp-policy)# authentication pre-share //establece el modo de autenticación con clave precompartida

Catalyst_4507R(config-isakmp-policy)# hash md5 //establece md5 como algoritmo de hash para garantizar la integridad

Catalyst_4507R(config-isakmp-policy)# group 1 //especifica el identificador de grupo de Diffie-Hellman en la política IKE

Catalyst_4507R(config-isakmp-policy)# encryption 3des //especifica 3DES como algoritmo de cifrado

Catalyst_4507R(config-isakmp-policy)# lifetime 86400 //especifica el tiempo de vida en segundos para la SA

Catalyst_4507R(config-isakmp-policy)# exit

Catalyst_4507R(config)# crypto isakmp key 0 cisco address ipv6 2800:0068:16:2001:B01:1200:0023:008/128 //define la clave precompartida, “hh87fkqwfw”,en texto plano, “0”, y la IP del que será el otro extremo del túnel 0

Catalyst_4507R(config)# crypto isakmp key 0 cisco address ipv6 2800:0068:16:1001:D01:1220:1023:006/128 //define la clave precompartida, “hh87fkqwfw”,en texto plano, “0”, y la IP del que será el otro extremo del túnel 1

Catalyst_4507R(config)# crypto keyring ANILLO //define el nombre del keyring que se usará durante la autenticación

Catalyst_4507R(config-keyring)#pre-shared-key address ipv6 2800:0068:16:2001:B01:1200:0023:008/128 key chh87fkqwfw //define la clave precompartida a usar durante la autenticación IKE

Catalyst_4507R(config-keyring)# pre-shared-key address ipv6 2800:0068:16:1001:D01:1220:1023:006/128 key chh87fkqwfw //define la clave precompartida a usar durante la autenticación IKE

Catalyst_4507R(config-keyring)# exit

Catalyst_4507R(config)# crypto ipsec transform-set TRANSFORMADA esp-3des //define un transform-set, es decir, una combinación de protocolos y algoritmos que sea aceptada por los routers IPSec

Catalyst_4507R(cfg-crypto-trans)# crypto ipsec profile PERFIL //define los parámetros que se van a usar para el cifrado IPSec entre los dos routers

Catalyst_4507R(ipsec-profile)# set transform-set TRANSFORMADA //especifica el transform-set que se puede usar

Catalyst_4507R(ipsec-profile)# exit

Catalyst_4507R(config)# interface tunnel 0 //configuración de la interfaz virtual tunnel 0

Catalyst_4507R(config-if)#ipv6 address
2800:0068:16:3001:C01:1200:0023:10/64

Catalyst_4507R(config-if)# ipv6 enable

Catalyst_4507R(config-if)# tunnel source
2800:0068:16:2001:B01:1200:0023:008 //define el origen del túnel

Catalyst_4507R(config-if)# tunnel destination
2800:0068:16:2001:B1:1200:23:007 //define el destino del túnel

Catalyst_4507R(config-if)# tunnel mode ipsec ipv6 //establece el modo de encapsulamiento para la interfaz tunnel 0

Catalyst_4507R(config)# interface tunnel 1 //configuración de la interfaz virtual tunnel 1

Catalyst_4507R(config-if)# ipv6 address
2800:0068:16:3002:C02:1200:0023:11/64

Catalyst_4507R(config-if)# ipv6 enable

Catalyst_4507R(config-if)# tunnel source
2800:0068:16:1001:D01:1220:1023:006 //define el origen del túnel

Catalyst_4507R(config-if)# tunnel destination 2800:0068:16:1001:D1:1220:1023:7 //define el destino del túnel

Catalyst_4507R(config-if)# tunnel mode ipsec ipv6 //establece el modo de encapsulamiento para la interfaz tunnel 0

Catalyst_4507R(config-if)# tunnel protection ipsec profile PERFIL //asocia la interfaz tunnel 0 con el perfil

Catalyst_4507R(config-if)# exit

Catalyst_4507R(config)# ipv6 route 2800:0068:16:4001:E01:1230:1123:005/64 tunnel 0 //configura una ruta estática de forma que todo el tráfico que vaya a la red local de la derecha pase por el túnel

Catalyst_4507R(config)# ipv6 route 2800:0068:16:0001:A01:1200:23:004/64 tunnel 1 //configura una ruta estática de forma que todo el tráfico que vaya a la red local de la izquierda pase por el túnel

Catalyst3750

Catalyst3750(config)# crypto isakmp policy 1 //configuración de la política IKE con prioridad 1

Catalyst3750 (config-isakmp-policy)# authentication pre-share //establece el modo de autenticación una clave precompartida

Catalyst3750 (config-isakmp-policy)# hash md5 //establece md5 como algoritmo de hash para garantizar la integridad

Catalyst3750 (config-isakmp-policy)# group 1 //especifica el identificador de grupo de Diffie-Hellman en la política IKE

Catalyst3750 (config-isakmp-policy)# encryption 3des //especificamos 3DES como algoritmo de cifrado

Catalyst3750(config-isakmp-policy)# lifetime 86400 // tiempo de vida en segundos para la SA

Catalyst3750 (config-isakmp-policy)# exit

Catalyst3750(config)# crypto isakmp key 0 hh87fkqwfw address ipv6 2800:0068:16:1001:D01:1220:1023:006/128 //define la clave precompartida, en texto plano, “0”, y la IP del que será el otro extremo del túnel en formato IPv6

Catalyst3750 (config)# crypto keyring ANILLO //define el nombre del keyring que se usará durante la autenticación

Catalyst3750 (config-keyring)# pre-shared-key address ipv6 2800:0068:16:1001:D01:1220:1023:006/128 key hh87fkqwfw //define la clave precompartida a usar durante la autenticación IKE

Catalyst3750 (config-keyring)# exit

Catalyst3750 (config)# crypto ipsec transform-set TRANSFORMADA esp-3des //define un transform-set, es decir, una combinación de protocolos y algoritmos que sea aceptable por routers IPSec

Catalyst3750 (cfg-crypto-trans)# crypto ipsec profile PERFIL //define los parámetros que se van a usar para el cifrado IPSec entre los dos routers

Catalyst3750 (ipsec-profile)# set transform-set TRANSFORMADA //especifica el transform-set

Catalyst3750 (ipsec-profile)# exit

Catalyst3750(config)# interface tunnel 1 //configuración de la interfaz virtual tunnel 1

Catalyst3750 (config-if)# ipv6 address 2800:0068:16:3002:C02:1200:0023:12/64

Catalyst3750 (config-if)# ipv6 enable

Catalyst3750 (config-if)# tunnel source 2800:0068:16:1001:D01:1220:1023:007 //origen del túnel

Catalyst3750 (config-if)# tunnel destination 2800:0068:16:1001:D01:1220:1023:6 //destino del túnel

Catalyst3750 (config-if)# tunnel mode ipsec ipv6 //establece el modo de encapsulamiento para la interfaz tunnel 0

Catalyst3750 (config-if)# tunnel protection ipsec profile PERFIL //asocia la interfaz tunnel 0 con el perfil

Catalyst3750 (config-if)# exit

Catalyst3750 (config)# ipv6 route 2800:0068:16:0001:A01:1200:0023:004/64 tunnel 0 //configura una ruta estática de forma que todo el tráfico que vaya a la red local de la izquierda pase por el túnel

Todos los nodos deben ser configurados de forma igual para que la conexión en el túnel se establezca, adicionalmente el nombre del transform-set debe ser el mismo dentro del comando ipsec profile.

3.3.8 Procedimiento de pruebas a realizarse en el escenario de simulación.

Una vez que se ha realizado la simulación, se torna necesario manejar un procedimiento de pruebas con el objetivo de validar los resultados obtenidos, de esta manera el primer paso a seguir será la verificación de las configuraciones en los routers, por medio de los respectivos comandos show running-config, show crypto ipsec sa y show crypto isakmp policy, cada uno de ellos mostrará las configuraciones generales del dispositivo, las configuraciones de las asociaciones de seguridad y de las políticas de seguridad implementadas respectivamente.

Posteriormente se deberá realizar la respectiva prueba de conectividad por medio de un ping extendido donde se debe poner énfasis en enviar un datagrama de tamaño igual a 1500 bytes con un timeout de 5 segundos, esto con el fin de simular tráfico real, como paso final se recurrirá al analizador de paquetes Wireshark con el fin de visualizar en tiempo real los protocolos y cabeceras de seguridad implementados, adicionalmente esta aplicación mostrará el consolidado de paquetes pasados de acuerdo a cada protocolo. Finalmente se deberá hacer una comparación del comportamiento de los paquetes entre dos escenarios con la misma topología: sin IPSec, ruteado con OSPF y con IPSec, ruteado con OSPF

3.3.9 Comprobación de la configuración IPSec.

Este proceso de lo realiza mediante el comando show crypto ipsec sa, que como resultado indica las direcciones de las interfaces de entrada y salida de los paquetes encriptados, indica el número de paquetes encriptados y desencriptados, el número de errores durante la encriptación, el túnel virtual que está usando esa ruta, el identificador de la cabecera ESP y de la SA, el identificador del crypto-map, el algoritmo de cifrado así como el tiempo de vida de la clave de encriptación, entre los parámetros más importantes tal como se muestra en la figura 54.

```
Catalyst_4507R#show crypto ipsec sa

interface: Tunnel0

   Crypto map tag: Tunnel0-head-0, local addr
2800:68:16:2001:B01:1200:23:8

  protected vrf: (none)

  local  ident (addr/mask/prot/port): (::/0/0/0)

  remote ident (addr/mask/prot/port): (::/0/0/0)

  current_peer 2800:68:16:2001:B01:1200:23:7 port 500

    PERMIT, flags={origin_is_acl,}

   #pkts encaps: 10, #pkts encrypt: 10, #pkts digest: 10

   #pkts decaps: 36023, #pkts decrypt: 36023, #pkts verify: 36023

   #pkts compressed: 0, #pkts decompressed: 0

   #pkts not compressed: 0, #pkts compr. failed: 0

   #pkts not decompressed: 0, #pkts decompress failed: 0

   #send errors 0, #recv errors 0

    local crypto endpt.: 2800:68:16:2001:B01:1200:23:8,

    remote crypto endpt.: 2800:68:16:2001:B01:1200:23:7
```

path mtu 1514, ip mtu 1514, ip mtu idb Tunnel0

current outbound spi: 0xA299BCF3(2727984371)

inbound esp sas:

spi: 0xE8A19F25(3902906149)

transform: esp-3des ,

in use settings ={Tunnel, }

conn id: 17, flow_id: SW:17, crypto map: Tunnel0-head-0

sa timing: remaining key lifetime (k/sec): (4576641/542)

IV size: 8 bytes

replay detection support: N

Status: ACTIVE

inbound ah sas:

inbound pcp sas:

outbound esp sas:

spi: 0xA299BCF3(2727984371)

transform: esp-3des ,

in use settings ={Tunnel, }

conn id: 18, flow_id: SW:18, crypto map: Tunnel0-head-0

sa timing: remaining key lifetime (k/sec): (4584845/534)

IV size: 8 bytes

replay detection support: N

Status: ACTIVE

```
        outbound ah sas:

        outbound pcp sas:

    interface: Tunnel1

        Crypto map tag: Tunnel1-head-0, local addr
2800:68:16:1001:D01:1220:1023:6

        protected vrf: (none)

        local  ident (addr/mask/prot/port): (::/0/0/0)

        remote ident (addr/mask/prot/port): (::/0/0/0)

        current_peer 2800:68:16:1001:D01:1220:1023:7 port 500

          PERMIT, flags={origin_is_acl,}

        #pkts encaps: 10, #pkts encrypt: 10, #pkts digest: 10

        #pkts decaps: 36018, #pkts decrypt: 36018, #pkts verify: 36018

        #pkts compressed: 0, #pkts decompressed: 0

        #pkts not compressed: 0, #pkts compr. failed: 0

        #pkts not decompressed: 0, #pkts decompress failed: 0

        #send errors 0, #recv errors 0

         local crypto endpt.: 2800:68:16:1001:D01:1220:1023:6,

         remote crypto endpt.: 2800:68:16:1001:D01:1220:1023:7

         path mtu 1514, ip mtu 1514, ip mtu idb Tunnel1

         current outbound spi: 0x9C72937(164047159)


         inbound esp sas:

          spi: 0x3FEC33A0(1072444320)
```

transform: esp-3des ,

in use settings ={Tunnel, }

conn id: 19, flow_id: SW:19, crypto map: Tunnel1-head-0

sa timing: remaining key lifetime (k/sec): (4443697/645)

IV size: 8 bytes

replay detection support: N

Status: ACTIVE

inbound ah sas:

inbound pcp sas:

outbound esp sas:

spi: 0x9C72937(164047159)

transform: esp-3des ,

in use settings ={Tunnel, }

conn id: 20, flow_id: SW:20, crypto map: Tunnel1-head-0

sa timing: remaining key lifetime (k/sec): (4451901/645)

IV size: 8 bytes

replay detection support: N

Status: ACTIVE

outbound ah sas:

outbound pcp sas:

El resultado de la aplicación de este comando se puede evidenciar en la figura 54 y 55 respectivamente.

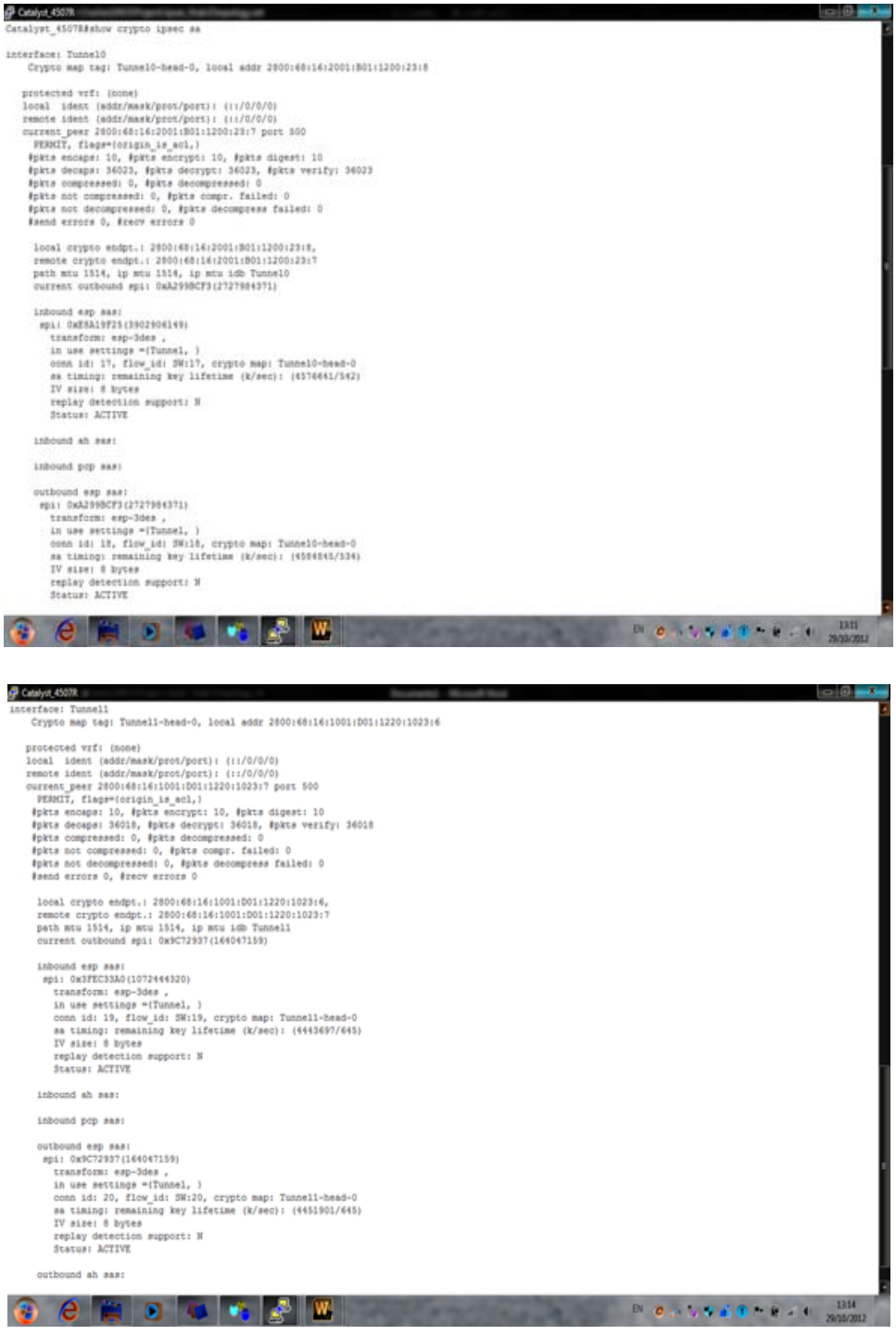

Figura 54 Resultado del comando show crypto ipsec sa
Fuente: Captura del programa GNS3

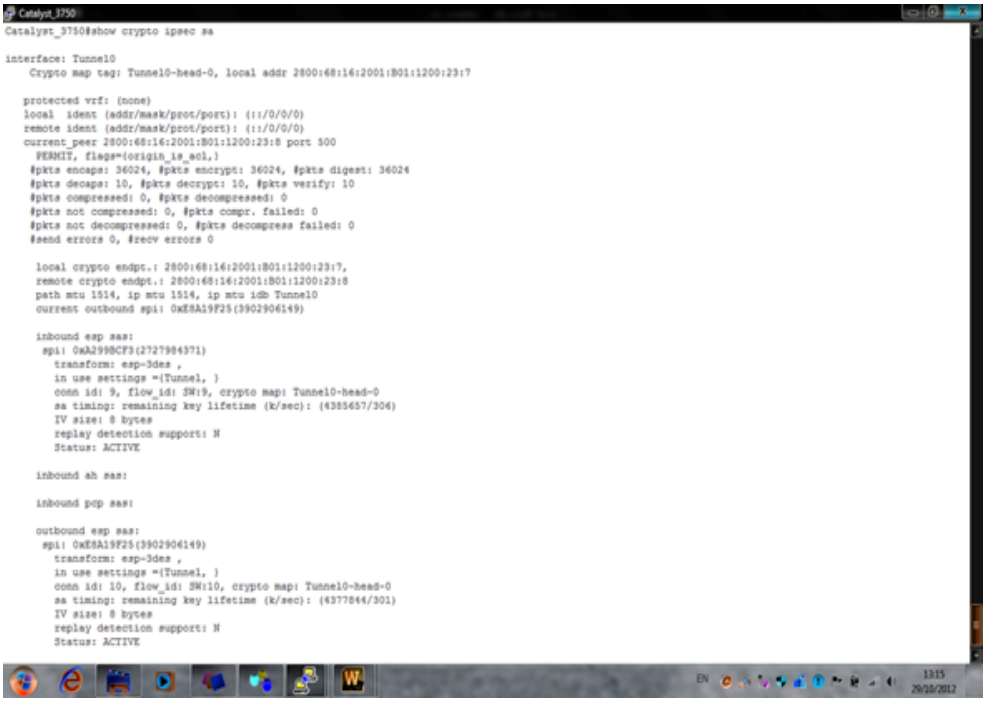

Figura 55 Resultado del comando show crypto ipsec sa
Fuente: Captura del programa GNS3

Como se puede apreciar, en los tres nodos los resultados de número de paquetes son coherentes, puesto que el mismo número de paquetes inyectados en un extremo es el mismo número de paquetes encriptados y desencriptados, sin existir ningún error, adicionalmente muestra los parámetros

con que fue configurado el protocolo IPSec, para un mejor detalle se ha usado el comando show crypto isakmp policy, donde se mostrarán las políticas ISAKMP configuradas en el router, tal como lo detalla la figura 3.9, donde se puede observar el algoritmo de encriptación 3DES, el algoritmo de hash MD5, el método de clave precompartida, el grupo Diffie-Hellman, el tiempo de vida de la clave, el método de autenticación, en este caso RSA, determinado que se han cumplido los parámetros de configuración requeridos.

```
Catalyst_4507R#show crypto isakmp policy

Global IKE policy

Protection suite of priority 1

        encryption algorithm:   Three key triple DES

        hash algorithm:         Message Digest 5

        authentication method:  Pre-Shared Key

        Diffie-Hellman group:   #1 (768 bit)

        lifetime:               86400 seconds, no volume limit

Default protection suite

        encryption algorithm:   DES - Data Encryption Standard (56 bit keys).

        hash algorithm:         Secure Hash Standard

        authentication method:  Rivest-Shamir-Adleman Signature

        Diffie-Hellman group:   #1 (768 bit)

        lifetime:               86400 seconds, no volume limit

Catalyst_4507R#
```

Figura 56 Resultado del comando show crypto isakmp policy
Fuente: Captura del programa GNS3

3.3.10 Verificación de la conectividad

La conectividad se puede verificar haciendo un ping normal o un ping extendido desde el Host A al Host B y viceversa, como se muestra en la figura 57 y la figura 58 respectivamente, se obtuvo la siguiente salida

HostA#ping

Protocol [ip]: ipv6

Target IPv6 address: 2800:68:16:4001:E01:1230:1123:6

Repeat count [5]: 2500

Datagram size [100]: 1500

Timeout in seconds [2]: 5

Extended commands? [no]:

Sweep range of sizes? [no]:

Type escape sequence to abort.

Sending 2500, 1500-byte ICMP Echos to 2800:68:16:4001:E01:1230:1123:6, timeout is 5 seconds:

!!!

Success rate is 100 percent (2500/2500), round-trip min/avg/max = 88/306/2176 ms

HostA#

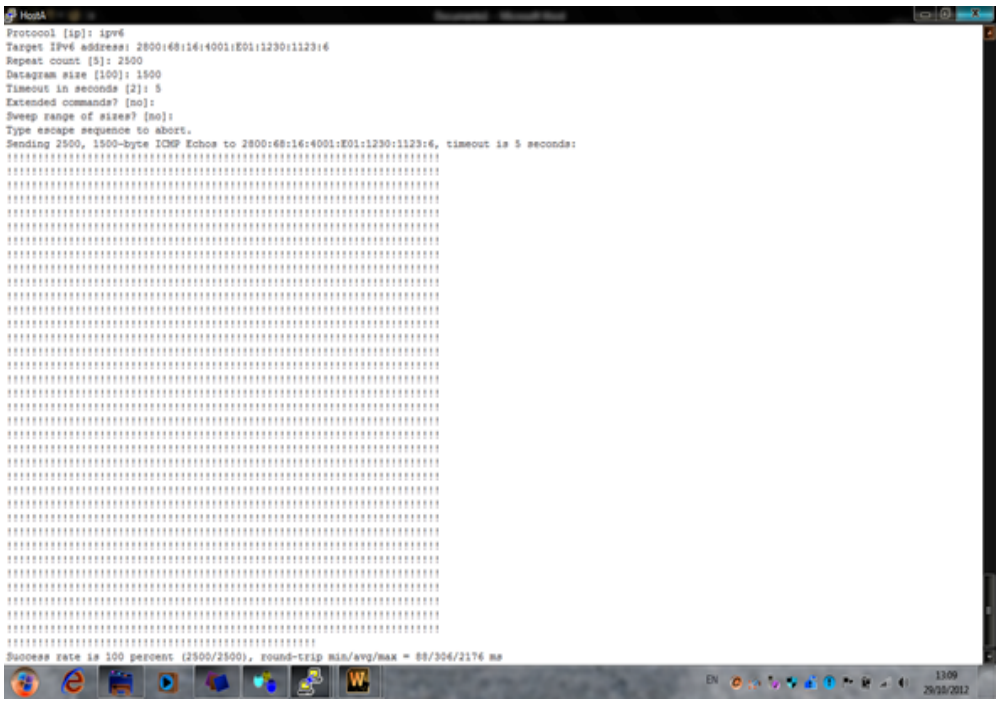

Figura 57 Resultado del ping extendido entre el Host A y el Host B
Fuente: Captura del programa GNS3

HostB#ping

Protocol [ip]: ipv6

Target IPv6 address: 2800:68:16:1:A01:1200:23:3

Repeat count [5]: 2500

Datagram size [100]: 1500

Timeout in seconds [2]: 5

Extended commands? [no]:

Sweep range of sizes? [no]:

Type escape sequence to abort.

Sending 2500, 1500-byte ICMP Echos to 2800:68:16:1:A01:1200:23:3, timeout is 5 seconds:

!!!

Success rate is 100 percent (2500/2500), round-trip min/avg/max = 96/322/2100 ms

HostB#

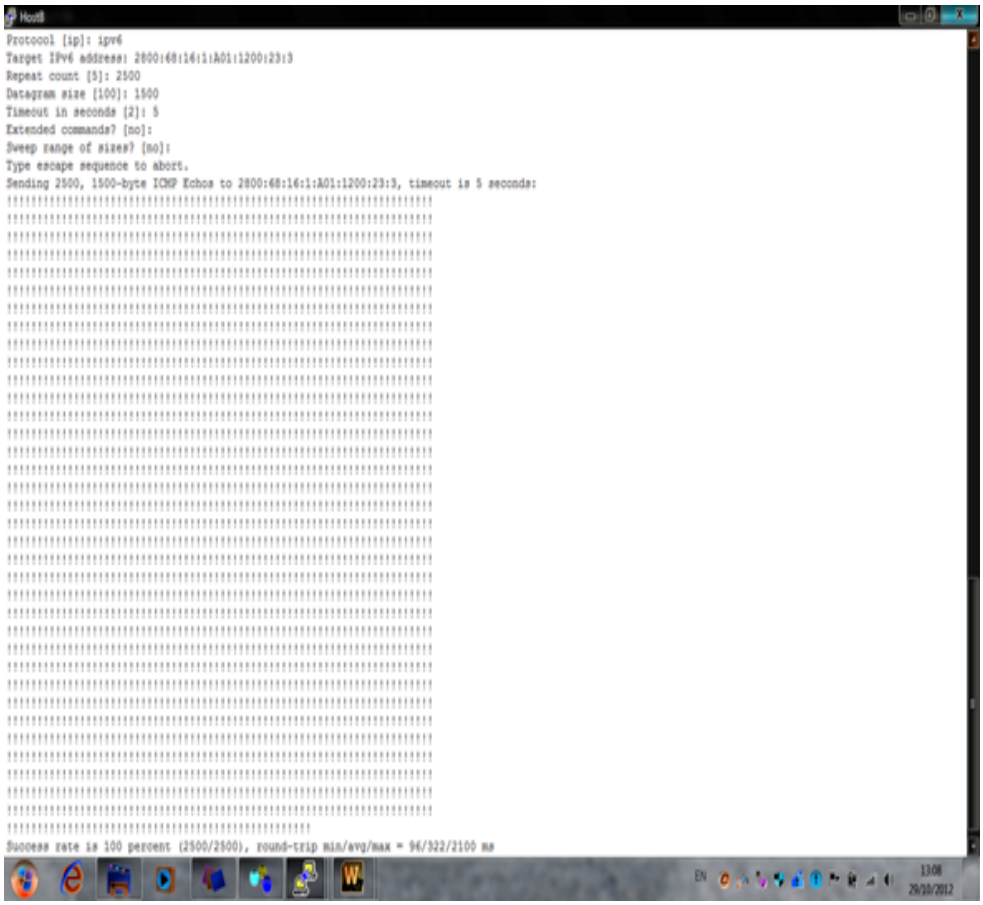

Figura 58 Resultado del ping entre el Host B y el Host A
Fuente: Captura del programa GNS3

Como se puede observar en ambos casos, la conectividad está establecida y el porcentaje de paquetes transportados es del 100%, con una demora promedio de 322 ms, lo que significa que ningún paquete se perdió de extremo a extremo, a pesar que los mencionados paquetes fueron sometidos al proceso de encriptación. Las pruebas se han realizado con un tamaño de paquete igual a 1500 bytes y con un tiempo de vida de 5 segundos, valores que normalmente son los que se encuentran en una red real. Adicionalmente se recurrió a un analizador de paquetes, en este caso Wireshark, con el fin de visualizar los protocolos que están siendo usados en la simulación, la captura se la realizó en el nodo denominado Catalyst_4507R que está cumpliendo las funcionalidades de nodo central, como se puede observar en la figura 59.

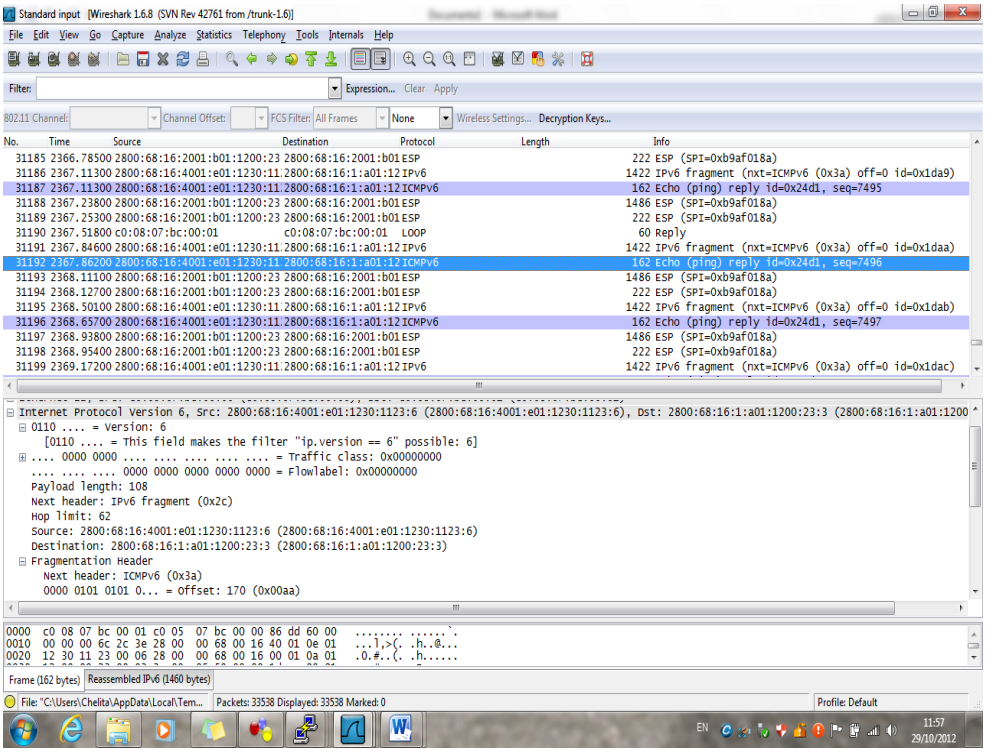

Figura 59 Interface principal del sniffer Wireshark.
Fuente: Captura del sniffer Wireshark.

3.3.11 Análisis de resultados.

De un total de 33538 paquetes que se pasaron en la simulación se puede observar en la figura 3.13 que el 100% de los paquetes que fueron enviados a cada nodo, el mismo porcentaje fue recibido por los respectivos routers, la carga de la seguridad encapsulada es del 48,07% en el ramal derecho y del 51,69% en el ramal izquierdo, lo que aproximadamente corresponde al 50% del tráfico pasado, es decir a 16122 paquetes, de los cuales 8227 son paquetes ICMPv6 y 8059 paquetes son exclusivamente de datos.

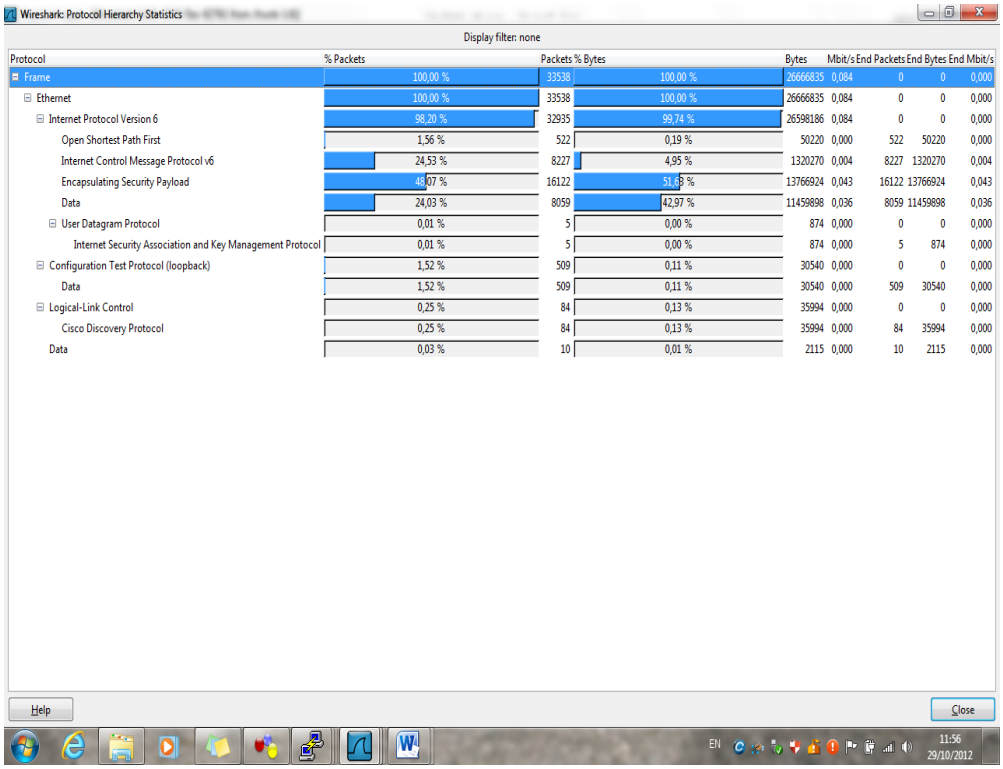

Figura 60 Interface principal del sniffer Wireshark
Fuente: Captura del sniffer Wireshark.

Estos valores reflejan claramente que la implementación de IPSec no reviste una carga apreciable en el escenario de simulación, sin embargo cabe destacar que en el escenario real significaría un aumento de carga a la red, precio más que justificado a pagar a cambio de aumentar la seguridad, esto valida la propuesta anteriormente expuesta que refiere a que los túneles IPSec solo se deberán implementarse en las VLAN´s que pasan tráfico que necesariamente se debe proteger.

De una muestra tomada de 5458 paquetes que se cursaron por el escenario de simulación, se procedió a realizar un análisis del porcentaje de los mismos que han pasado por los siguientes enlaces:

- Entre el switch 3750 y el 4507R, con 5458 paquetes.
- Entre el switch 4507R y el 3750 con 5458 paquetes.
- Entre el host A y el switch 4507R con 2791 paquetes.
- Entre el host B y el switch 4507R con 2791 paquetes.

Para realizar el análisis del comportamiento de los paquetes, se recurrió a comparar el número de paquetes pasados en los mismos enlaces por dos escenarios diferentes, con la topología especificada en el apartado 3.3.4, el primer escenario no contempló IPSec, no así el segundo, de esta manera se tomó en cuenta el porcentaje de paquetes transferidos de acuerdo al protocolo, así se identificó paquetes IPv6, OSPF, ICMPv6, ESP, ISAKMP y LLC.

Como se puede apreciar en la tabla 3.2, existe una diferencia muy pequeña entre el número de paquetes pasados en el enlace desde el switch 3750 al 4507R en ambos escenarios; se evidencia que el número de paquetes IPv6 pasados es mayor en el escenario con IPSec, lo que indica que en el entorno seguro los paquetes tienden a pasar íntegramente, asegurando su entrega.

El motivo de esta diferencia reside en que cuando el paquete entra en el túnel generado por el Security Gateway, se añaden cabeceras adicionales, las que se han mencionado durante este trabajo, en virtud de los mecanismos de encapsulación y manejo del encriptamiento que se manejan dentro de IPSec.

Tabla 21
Porcentaje de paquetes cursados entre el switch 3750 y el switch 4507R

	3750 A-4507 sin IPSec	**3750 A-4507 con IPSec**
IPV6	47,37	47,82
OSPF	45,14	44,86
ICMP	2,23	2,54
LLC	0,75	0,72
ESP		3,64
ISAKMP		0,42

En la figura 61 se muestra gráficamente la correlación de ambos escenarios, donde se puede evidenciar la cercanía del porcentaje de paquetes cursados. Adicionalmente se muestran los porcentajes de paquetes ESP e ISAKMP.

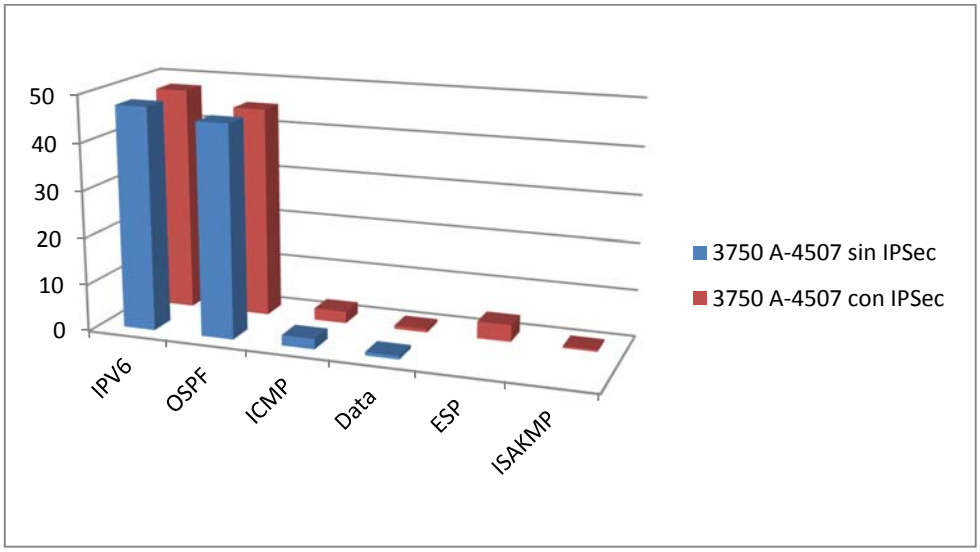

Figura 61 Detalle de los porcentajes de paquetes cursados en el enlace clasificados por protocolo

En la tabla 22 se detalla el porcentaje de paquetes enviados en cada escenario, en el enlace entre el switch 3750 ubicado a la derecha y el switch 4507R, la apreciación es la misma que en el caso anterior.

Tabla 22
Porcentaje de paquetes cursados entre el switch 3750 el switch 4507R

	3750B- 4507 sin IPSec	3750B-4507 con IPSec
IPV6	43,66	44,28
OSPF	41,14	40,84
ICMP	2,52	2,73
Data	0,55	0,53
ESP		10,92
ISAKMP		0,7

En la figura 62 se aprecia gráficamente los porcentajes de los paquetes enviados.

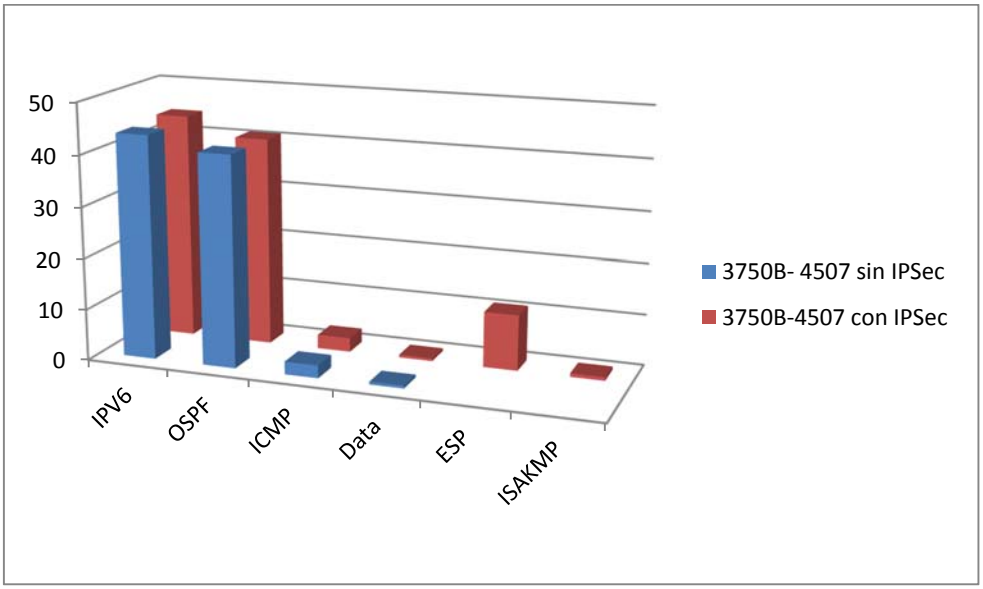

Figura 62 Detalle de los porcentajes de paquetes cursados en el enlace clasificados por protocolo

En la muestra con 2795 paquetes tomada entre los host A y B en ambos escenarios se aprecia el mismo comportamiento de los paquetes, es decir la cantidad de paquetes recibidos es mayor en la simulación con IPSec, se tomó una muestra diferente para validar el comportamiento del protocolo. Los valores se detallan en la tabla 23.

Tabla 23
Porcentaje de paquetes cursados entre el host A y el switch 4507R

	Host A - 4507 sin IPSec	Host A - 4507 con IPSec
IPV6	43,36	43,74
OSPF	40,85	37,85
ICMP	3,01	5,89
Data LLC	1,43	1,47

Al igual que en los casos anteriores, en la figura 3.16 se puede apreciar la cantidad de paquetes cursados en el enlace especificado, como se aseveró anteriormente el comportamiento es el mismo que en los enlaces entre los switches.

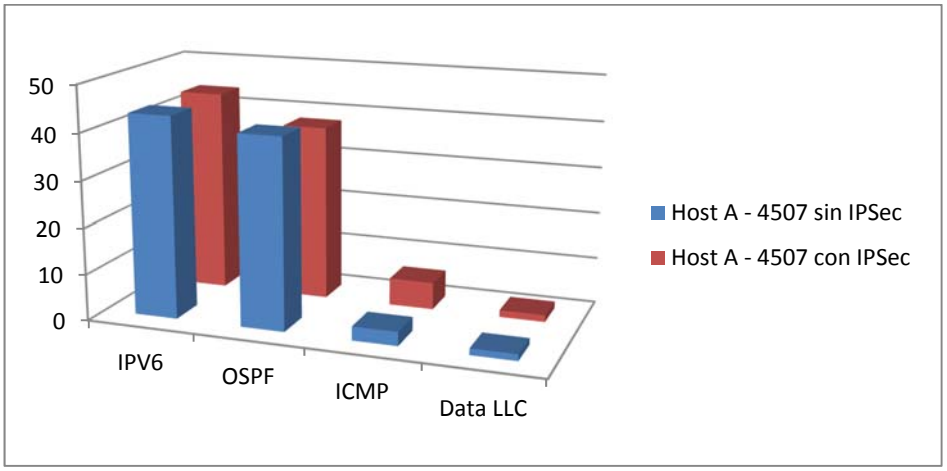

Figura 63 Detalle de los porcentajes de paquetes cursados en el enlace clasificados por protocolo

En la tabla 24 se muestra el porcentaje de paquetes pasados en el enlace entre el host B y el switch 4507R, al igual que en casos anteriores, la tendencia es la misma, se puede observar que aunque que la diferencia entre ambos escenarios es mínima, el porcentaje de paquetes cursados es mayor en el escenario con IPSec.

Tabla 24 Porcentajes de paquetes cursados entre el host B y el switch 4507R

	Host B - 4507 sin IPSec	**Host B - 4507 con IPSec**
IPV6	32,1	32,24
OSPF	27,41	29,6
ICMP	2,64	4,69
Data LLC	0,89	0,91

De los datos obtenidos en el enlace mencionado, se generó la gráfica donde se puede apreciar los porcentajes de cada paquete por tipo.

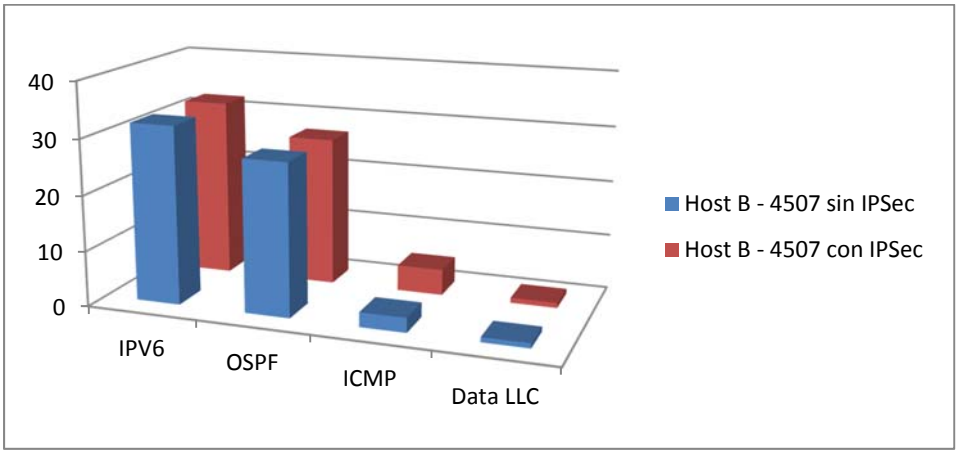

Figura 64 Detalle de los porcentajes de paquetes cursados en el enlace clasificados por protocolo

CAPITULO VI

4.3 CONCLUSIONES

- La investigación demostró la factibilidad de la implementación del protocolo IPSec en un entorno nativo IPv6 dentro de un escenario LAN, como en el caso del Campus Girón de la Universidad Politécnica Salesiana, de acuerdo a la información levantada del estado inicial, se pudo determinar que la infraestructura de red y servidores es totalmente compatible con IPv6 y por lo tanto con IPSec puesto que este protocolo de seguridad es un estándar abierto y obligatorio en la nueva plataforma de direccionamiento, se asegurará la confidencialidad, integridad y autenticidad de la información transferida.
- IPv6 no es la solución absoluta en materia de seguridad, contiene vulnerabilidades tal como se detalló en el capítulo 1 de este trabajo, razón por la cual la seguridad debe ser inherente en el diseño de la red, por lo tanto es imperioso que se implementen mecanismos de seguridad de capa 3 tales como IPSec, el que entre sus ventajas muestra una total transparencia ante las aplicaciones de capas superiores, adicionalmente las múltiples opciones de configuración lo hacen muy flexible para adaptarse a cualquier escenario.
- La elección de los parámetros de configuración del protocolo IPSec deberán ajustarse al escenario de implementación elegido, en el caso de esta

investigación se determinó el uso del escenario de combinación de SA perteneciente al caso II, donde se trabaja exclusivamente en el modo túnel, por lo tanto maneja cabeceras ESP que proporcionan servicios de seguridad y confidencialidad por medio de mecanismos de clave precompartida, adicionalmente se deberá implementar algoritmos de hash para garantizar la integridad de la información y un método de intercambio de claves adecuado en la política IKE de tal manera que no afecte el rendimiento del enlace, la elección más adecuada en esta investigación fue el uso del identificador de grupo 1 de Diffie-Hellman.

- El impacto de una implementación de IPv6 en una red existente basada en IPv4 es mínimo, puesto que los cambios solamente se lo realizan a nivel de capa red, de esta manera se mantiene intacto el diseño jerárquico de la red, esto se pudo evidenciar durante este trabajo puesto que la propuesta de implementación se la realizó sobre los segmentos de red existentes, tomando en cuenta que al poner mecanismos de seguridad y encriptación, los paquetes aumentan de tamaño y pasará más tráfico por el firewall, donde se limita la inspección profunda de los paquetes, reduciendo con esto el rendimiento de la red. Este protocolo demostró durante la simulación tener una afectación perceptible sobre los paquetes IPv6, de acuerdo a lo anteriormente dicho, si bien el escenario de simulación estaba considerando poca carga de tráfico relativamente, indica que en un caso real se tendrá un impacto significativo en el throughput, produciendo los consabidos problemas de latencia.
- La implementación de IPSec en una red LAN no necesariamente se la debe hacer en todo el escenario, sino más bien a segmentos determinados que en el caso de esta investigación fueron elegidos en base al tipo de información que se cursa por ellos, la razón para tomar este tipo de criterio de implementación radica en que el implementar mecanismos de seguridad influirá en el rendimiento de la red en un escenario real, adicionalmente se considera que en la red objeto de esta investigación existen VLAN´s que no requieren protección puesto que la información que se tramita en esos segmentos no revisten criticidad alguna, como ejemplo se tiene la VLAN 7, asignada para el acceso inalámbrico por parte del grupo de usuarios denominado ESTUDIANTES, en este segmento de red no se tramita información que requiera mecanismos adicionales de protección puesto que solo se la usa para

acceso controlado a internet y a la plataforma de educación virtual, no así otros segmentos de red como por ejemplo la VLAN 112 denominada ADMINISTRATIVOSv2, la que cursa información muy delicada como por ejemplo la generada por el sistema de gestión y matriculación académica.

- El uso de IPSec en la red de la Universidad Politécnica Salesiana Campus Girón ofrecerá ventajas tales como transparencia ante los servicios de capa aplicación, determinando que su implementación revestirá un mínimo impacto en la infraestructura de red actual, de esta manera no se deberá hacer ningún cambio en la capa aplicación, el proceso de implementación se realizará exclusivamente en dispositivos de capa red, se propone trabajar en modo túnel puesto que la protección se centrará en los segmentos de red especificados en el capítulo 2, de esta manera la protección se creará entre los Security Gateway evitando establecer configuraciones adicionales en los host, permitiendo una administración de seguridad más eficiente al manejar un mismo esquema de gestión de claves y autenticación en cada segmento, dando como resultado la fiabilidad en el paso de información, como se demostró en el análisis de tráfico cursado en la simulación.

4.4 RECOMENDACIONES

IPv6 es un protocolo relativamente nuevo y no ha tenido la oportunidad de trabajar ampliamente en entornos de red como lo ha hecho IPV4, por lo que sus ventajas y desventajas no se han demostrado totalmente aún, adicionalmente existen limitantes como por ejemplo algunos equipos activos de red que no soportan el protocolo en si o parte de él, puede aseverarse que la poca experiencia y el desconocimiento de las potencialidades del protocolo por parte de los administradores de red hacen que la implementación de IPv6 en una empresa se vuelva más compleja y pueda derivar en agujeros de seguridad que exploten aspectos que IPv6 utiliza para su funcionamiento.

- Se recomienda en forma general, implementar políticas de seguridad, tales como controles de acceso a los segmentos de red inalámbricos y políticas de uso de contraseñas.
- Adicionalmente el administrador de TI deberá realizar regularmente pruebas de intrusión a fin de determinar el estado de la seguridad de la red, en especial en los segmentos donde se ha dispuesto los túneles IPSec, la elección de estos segmentos de red se deberá realizar en base a criterios como tipo de información que se maneja, universo de usuarios existentes en la red y la infraestructura de seguridad de red preexistente. Los administradores de red deben estar al tanto de la forma en que los atacantes realizan el reconocimiento de las vulnerabilidades de la red y como las aprovechan, por lo tanto la gestión de seguridades deberá realizarse de acuerdo a los estándares recomendados por ejemplo ISO 27001.
- Se recomienda programas de entrenamiento y capacitación continua dirigidos al grupo de trabajo encargado del departamento de TI, en este caso específicamente en el área referente a IPv6 y sus implicaciones de seguridad como políticas de control de acceso, control de vulnerabilidades y métodos de mitigación de ataques.

LISTA DE REFERENCIAS

Ingeniería de la Seguridad. (2012). Recuperado el 12 de enero de 2012, de Blog dedicado a la ingenieria de la seguridad: http://ingenieriadelaseguridad2013.blogspot.com/p/ip-sec.html

Alba, E. (2008). Herramientas Web para la enseñanza de protocolos de comunicación. Recuperado el 16 de febrero de 2013, de Cabecera IPv4: http://neo.lcc.uma.es/evirtual/cdd/tutorial/red/cabipv4.html

Anónimo. (2012). Redes Zone. Recuperado el 08 de julio de 2012, de ADLS Zone: http://www.redeszone.net/2011/08/30/ipsec-volumen-ii-ah-cabecera-de-autenticacion/

Barrionuevo, V. (2006). Informe de análisis de la situación actual de la infraetructura de networking del Campus Giron. p3. (J. López, Entrevistador) Quito, Pichincha, Ecuador.

Bruzual, R. (2012). IP version 6. Recuperado el 22 de febrero de 2012, de Especialización en Comunicaciones y Redes de Comunicación de Datos: http://neutron.ing.ucv.ve/revista-e/No5/IP%20versi%C3%B3n%206.htm

CEDIA. (2012). Obtenido de http://ipv6.cedia.org.ec/index.php/asignaciones

CEDIA. (s.f.). La Realidad. Obtenido de http://ipv6.cedia.org.ec/index.php/la-realidad

CISCO. (2012). Seguridad y VPN : Negociación IPSec/Protocolos IKE. Obtenido de Una introducción al cifrado de la seguridad IP (IPSec): http://www.cisco.com/cisco/web/support/LA/7/75/75045_IPSECpart1.html

CISCO. (s.f.). Cisco Catalyst 3750 Series Switches. Obtenido de http://www.cisco.com/en/US/products/hw/switches/ps5023/index.html

ciscoipv6ttechtips. (2011). Cisco Configuration. Recuperado el 15 de agosto de 2013, de http://www.ciscoipv6ittechtips.com/39th-article-the-group-and-hash-ipv6-ike-commands.html

Domínguez, J. C. (12 de julio de 2012). Seguridades de la red de la UPS. (J. López, Entrevistador) Quito, Pichincha, Ecuador.

Flores, I. E. (28 de Agosto de 2007). Cisco Networking Academy. Obtenido de Universidad Don Bosco: http://cnap.udb.edu.sv/ccnpdetail.html

Francisconi, H. A. (agosto de 2005). Recuperado el 21 de febrero de 2013, de http://francisconi.org/sites/default/files/IPsec_en_Ambientes_IPv4_e_IPv6.pdf

Gonzáles, I., & Jose, T. (s.f.). UFM. Recuperado el 20 de febrero de 2012, de http://www.tesis.ufm.edu.gt/pdf/3930.pdf

Hoog, S. (2009). IPv6 Security. Indianapolis: Cisco Press.

Moreno, A., & Cristian, V. (marzo de 2012). Repositorio UPS. Recuperado el marzo de 2012, de http://dspace.ups.edu.ec/handle/123456789/3538

Multimanía. (2010). Recuperado el 06 de octubre de 2013, de http://usuarios.multimania.es/txk/contenido/IPSec_II.php

Savolainen, S. (2000). Internet Key Exchange (IKE). Obtenido de http://www.niksula.cs.hut.fi/~sjsavola/SoN/essay.html

Stallings, W. (2004). Fundamentos de Seguridad en Redes.Aplicaciones y Estándares (Segunda ed.). Madrid: Person Education.

Unex. (13 de marzo de 2006). Cala Virtual. Recuperado el 10 de julio de 2013, de Red Privada Virtual: http://cala.unex.es/cala/cala/mod/resource/view.php?id=1883

Uribe, E., & Mariela, M. (2012). Scrib. Recuperado el 15 de agosto de 2012, de http://es.scribd.com/doc/12836622/IPsec

Vásquez, J. (2011). Cisco.

VEGA. (2010). SUBGRAPH, 1.0. Recuperado el 18 de septiembre de 2013, de Open Source Segurity: http://subgraph.com/vega_download.php

Villagra, V. (2000). Universidad de México. Recuperado el 20 de julio de 2013, de https://www.dit.upm.es/~villagra/

Watch Guard System Manager Help. (2010). About Diffie-Hellman Groups. Recuperado el 15 de agosto de 2013, de

http://www.watchguard.com/help/docs/wsm/11/en-US/index_Left.html#CSHID=en-US%2Fbovpn%2Fmanual%2Fdiffie_hellman_c.html|StartTopic=Content%2Fen-US%2Fbovpn%2Fmanual%2Fdiffie_hellman_c.html|SkinName=WSM (en-US)

Wikispace. (2012). Protocolo IPv6. Recuperado el 23 de febrero de 2012, de http://protocoloip6.wikispaces.com/cuadro+comparativo+entre+la+descripci%C3%B3n+de+la+cabecera+IPv4+y+la+cabecera+IPv6

[1] Francisconi, Hugo Adrián. IPSec en ambientes IP4 e IPv6, primera edición, Agosto del 2005. Villa Nueva, Guaymallen, Mendoza Argentina, ISBN 987-43-9727-6.

[2] McFarlan Shannon, Sambi Muninder, Sharma Nikihil, Hooda Sanjay. IPv6 for enterprise Networks, Copyright © 2011 Cisco Systems, Inc. Published by Cisco Press. ISBN-10: 1-58714-227-9.

[3] Hogg Scott. IPv6 Security, Copyright © 2009 Cisco Systems, Inc. Published by Cisco Press. ISBN-13: 978-1-58705-594-2.

[4] Luján Montes Erick Fernando. Seguridad en IP con el protocolo IPSec para ipv6. Universidad San Carlos de Guatemala. Guatemala, octubre de 2005.

[5] Verdejo Álvarez Gabriel. El protocolo IPv6 y sus extensiones de seguridad IPSec. Febrero del 2000. Universidad Autónoma de Barcelona, Escuela Técnica superior de Ingeniería

[6] Izquierdo Manzanares Antonio. Tesis doctoral: Metodología para la validación y evaluación remota de implementaciones de protocolos de seguridad. Aplicación a la arquitectura IPSec. Octubre de 2.006, Leganés, Universidad Carlos III de Madrid, Departamento de Informática.

[7] Teare Diane. Implementing Cisco IP route, Junio 2010. Indianapolis, Cisco Systems, Inc. Cisco Press.

[8] Cisco Team. Security for VPNs with IPsec Configuration Guide Cisco IOS Release 12.4T, Americas Headquarters, Cisco Systems, Inc. Disponible en: http://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_vpnips/configuration/12-4t/sec-sec-for-vpns-w-ipsec-12-4t-book.pdf.

[9] Cisco Systems, Implementing IPSec in IPv6 Security, Marzo 25, 2011, Systems 2007, Inc. Disponible en: http://www.cisco.com/en/US/docs/ios/ios_xe/ipv6/configuration/guide/ip6-ipsec_xe.pdf

[10] Moreno Constante Alex Alfonso, Valencia Falcón Cristian Alejandro. Implementación de un Plan Piloto para la interconexión de IPv6 sobre IPv4, utilizando el Protocolo Dual Stack en la Universidad Politécnica Salesiana Campus Sur dentro de la subred CIMA (Centro de Investigación en Modelación Ambiental) con la frontera del proveedor Telconet. Marzo 2012, Quito. Universidad Politécnica Salesiana.

[11] Vásquez Clavijo Jenny E. Análisis de las funcionalidades de los protocolos de seguridad IPSec, IKE, ISAKMP sobre IPv6 e implementación en una red prototipo bajo infraestructura CISCO, Agosto 2011, Quito. Universidad Politécnica Salesiana.

[12] Stallings William, Fundamentos de Seguridad en Redes. Aplicaciones y Estándares, Pearson Educacion, Madrid 2004, segunda edición.