IPSec DE IPv6 EN LA UNIVERSIDAD DE PAMPLONA

IPSec of IPv6 at the University of Pamplona

RESUMEN
Este artículo describe IPSec fundamentado en: AH que proporciona el servicio de autenticación, ESP que brinda confidencialidad, e IKE que permite gestión de claves e intercambio de parámetros de seguridad. Se enmarca IPSec dentro del protocolo IPv6 siendo la seguridad obligada para el nuevo protocolo, mientras que para IPv4 era sólo opcional. Al término del artículo se documentan las pruebas realizadas aplicando el protocolo IPv6 con su extensión de seguridad IPSec a una red punto a punto en la Universidad de Pamplona.

PALABRAS CLAVES: Asociación de Seguridad, Autenticación, Confidencialidad, IPSec, IPv6.

ABSTRACT
This article describes IPSec based on: AH (IP Authentication Header) that the service of authentication provides, ESP (Protocol Encapsulating Security Payload) that offers confidentiality, and IKE (Internet Key Exchange) who allows to management of keys and interchange of security parameters. IPSec within the IPv6 protocol is framed being the security forced for the new protocol, whereas for IPv4 was only optional. At the end of the article the made tests are documented applying to the IPv6 protocol with their extension of IPSec security to a network point to point.

KEYWORDS: *Association of Security, Authentication, Confidentiality, IPSec, IPv6.*

Dewar Willmer Rico Bautista
Ingeniero de Sistemas. MCC (c)
Docente Tiempo Completo Ocasional
Universidad de Pamplona
dewarrico@unipamplona.edu.co,
ing_dewar@yahoo.com

Yurley Constanza Medina Cárdenas
Ingeniera de Sistemas. MCC (C)
Directora Registro y Control Académico
Coordinadora Centro de Mejores Prácticas
Universidad de Pamplona
yurleymed@unipamplona.edu.co

Luz Marina Santos Jaimes
Ingeniera de Sistemas. M. Sc
Directora Grupo de Investigación Ciencias Computacionales
Categoría C inscrito en Colciencias
Universidad de Pamplona
lsantos@unipamplona.edu.co

1. INTRODUCCIÓN

El protocolo Internet IP, es uno de los más usados para la interconexión de redes tanto en ambientes académicos como corporativos, y naturalmente lo es también en la Internet pública. La fuerza de IP radica en su facilidad y su flexibilidad para el envío de grandes volúmenes de información en pequeños paquetes a través de los diversos esquemas de enrutamiento. Sin embargo, IP presenta ciertas debilidades, la forma como se enrutan los paquetes hace que las grandes redes IP sean vulnerables a ciertos riesgos de seguridad. Debido a los problemas de implementación aparecidos con la versión del protocolo estándar de Internet IPv4, se vio la necesidad de desarrollar mecanismos específicos para el mejor funcionamiento de la red, dando cabida a nuevas versiones del protocolo IP tales como IPv6 extensión IPSec (Internet Protocol Security).

La tecnología de IPSec se basa en criptografía moderna, lo que garantiza, por un lado, la privacidad y, por otro, una autentificación fuerte de datos. Las características de IPSec lo hacen único debido a que implementa seguridad en la capa de red más que en la de aplicación. La realización de pruebas con IPv6 extensión IPSec, constituye un aspecto fundamental en los procesos de transición y utilización de aplicaciones futuras y actuales modificadas para hacer uso de las ventajas operativas ofrecidas por IPv6.

Fecha de Recepción: 5 de Junio de 2008.
Fecha de Aceptación: 4 de Agosto de 2008

1.1 Protocolo IPv6

La nueva versión del protocolo IP recibe el nombre de IPv6; inicialmente se denominó IPng (Protocolo Internet de Próxima Generación), diseñada por la IETF (Internet Engineering Task Force) la cual indicó a través de un RFC (Request For Comments)[1] las necesidades que debía cubrir y las especificaciones que debía cumplir. Este nuevo modelo se convertirá en sucesor de la versión 4 puesto que resuelve deficiencias y aporta funciones como: nuevo direccionamiento[2] [3], encriptación de datos, autoconfiguración, calidad de servicio, enrutamiento jerárquico, seguridad basada en el protocolo IPSec; funciones que hacen que una red tenga mayor velocidad

[1] [1] S. Deering, R. Hinden. Internet Protocol, Version 6 (IPv6) Specification.Internet-Draft, RFC 1752, Enero 1995.

[2] [2] R. Hinden, S. Deering. IPv6 Addressing Architecture RFC2373.

[3] [3] V. Fuller, T. Li, J. Yu, and K. Varadhan. Classless interdomain routing (CIDR), RFC 1519 September 1993.

desempeño lo cual va acorde a la evolución actual de Internet.

1.2 Formato del Paquete IPv6

El paquete IPv6 en la figura 1 es una evolución de la anterior versión. No se han introducido grandes cambios de contenido o estructura, simplemente se ha mejorado y optimizado. Con respeto al paquete IPv4 se suprimieron siete campos (tamaño de cabecera, tipo de servicio, número de identificación del paquete, banderas, número de byte del paquete fragmentado, checksum, opciones), y se rediseñaron los campos de longitud del paquete, tiempo de vida y tipo de protocolo.

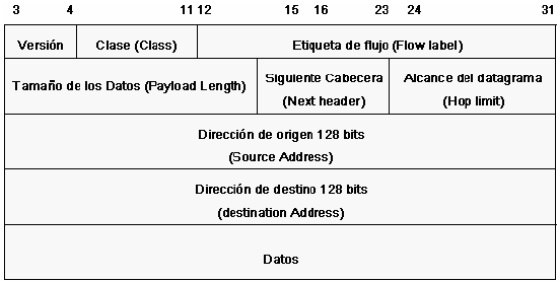

Figura1. Formato del Paquete IPv6

El campo cabecera siguiente indica al router si tras el paquete viene algún tipo de extensión u opción. También permite describir con más detalle las opciones del paquete. En IPv6 se definen una serie de cabeceras de extensión que se colocan justo después de los datos en forma de cadena permitiendo personalizar el paquete. De esta forma se puede tener varias extensiones de cabecera tan solo indicando en el campo cabecera siguiente de cada una de ellas el tipo de la cabecera que vendrá a continuación. En este trabajo solo se hablará de las cabeceras de autenticación (Authentication Header AH) y de encapsulación (Encapsulating Security Payload ESP) que son las utilizadas por IPSec.

2. EL PROTOCOLO IPSec

IPSec es un estándar que proporciona servicios de seguridad a la capa IP y a todos los protocolos superiores (TCP y UDP, entre otros). Entre las ventajas de IPSec se destaca que esta apoyado en estándares de la IETF[4], proporcionando un nivel de seguridad común y homogéneo para todas las aplicaciones, además de ser independiente de la tecnología física empleada. Está basado en un modelo de seguridad extremo a extremo, lo que significa que los únicos hosts o routers que tienen que conocer la protección de IPSec son el que envía y el que recibe. Cada equipo controla la seguridad por sí mismo en su extremo, bajo la hipótesis de que el medio por el que se establece la comunicación no es seguro.

En la figura 2 se muestra el modo en que funciona IPSec, está compuesto por dos protocolos de seguridad de tráfico: AH y ESP, y un protocolo de Gestión de Claves (Internet Key Exchange, IKE).

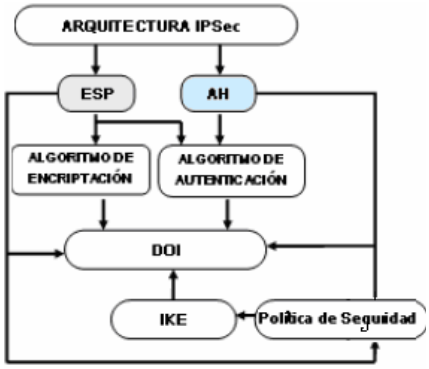

Figura 2. Arquitectura IPSec

Al utilizar el protocolo AH se aplican algoritmos de autenticación de los datos (la información enviada es realmente de quien dice ser), y al emplear el protocolo ESP se aplican algoritmos de encriptación con flexibilidad para soportar combinaciones de autenticación, integridad de datos (seguridad de que cualquier alteración de la información será detectada), control de acceso (se establecen políticas de establecimiento de conexiones IPSec) y confidencialidad de datos (la información enviada no será vista por otras personas).

DOI (Domain of Interpretation) define todos los parámetros que se negocian para establecer canales seguros, incluyendo identificadores únicos para algoritmos de autentificación y de encriptamiento durante el proceso de comunicación, además de las medidas necesarias para establecer una conexión AH o ESP, también especifica parámetros operacionales para el protocolo IKE tales como tiempo de vigencia de las claves (key Exchange), y ubicación de las claves criptográficas requeridas para cumplir con los servicios solicitados.

La Política de Seguridad (SP, Security Policy), almacena información adicional para definir qué tráfico proteger, y cuándo hacerlo. IPsec funciona a partir de dos políticas de seguridad:

- Base de datos políticas de seguridad SPD (Security Policy Database) estas políticas le dicen a IPSec cuando debe o no debe actuar sobre un paquete IPv6.
- Base de datos asociaciones de seguridad SAD (Security Association Database), estas asociaciones le dicen a IPSec cómo debe crear el canal entre las dos máquinas.

[4] [4] Track. S. Kent, R. Atkinson. Security Architecture for the Internet Protocol. RFC 2401. November 1998.

2.1 Asociación de Seguridad

La función de la Asociación de Seguridad (SA Security Association) es proporcionar un método para que dos computadores puedan intercambiar datos de manera segura. Está definida para comunicaciones en un solo sentido (simplex) esto significa que cada par de sistemas que se comunican por lo menos tiene dos SAs, una de origen a destino y otra de destino a origen. Lo mismo ocurre para la asociación de seguridad que se crea para AH o ESP, si estos dos protocolos se aplican a una comunicación juntos, se crearán dos (o más) asociaciones de seguridad.

Para la identificación de una asociación de seguridad se utiliza un Índice de Parámetros de Seguridad (Security Parameter Index, SPI) el cual contiene la dirección IP destino y el identificador de protocolo de seguridad (AH y ESP); con esta información el SPI puede recibir un paquete y saber a que asociación de seguridad hace referencia, y de esta forma poder autenticarlo y/o descifrarlo.

Una asociación de seguridad describe:

- Que algoritmo va a ser usado en la autenticación y las claves para él.
- El algoritmo de cifrado y las claves
- Tiempo de vida de las claves
- Tiempo de vida de la SA
- Dirección IP origen de la SA

2.2 Modos de Operación en IPSEC

Modo Transporte: El contenido transportado dentro del paquete AH o ESP son datos de la capa de transporte. Por lo tanto la cabecera IPSec se inserta a continuación de la cabecera IPv6 y antes de los datos que se desean proteger. El modo transporte solo se cifra los datos, las cabeceras AH y ESP quedan igual.

Modo Túnel: El contenido del paquete AH o ESP es un paquete completo es decir el paquete IPv6 al cual se añade la cabecera AH o ES, posteriormente se añade una cabecera IP que es la que se utiliza para encaminar los paquetes a través de la red.

2.3 Métodos de Seguridad en IPSEC

IPSec ha sido diseñado de forma modular (figura 3) lo cual permite seleccionar el conjunto de algoritmos deseados sin afectar a otras partes de la implementación. Han sido definidos sin embargo ciertos algoritmos estándar que deberán soportar todas las implementaciones para asegurar la interoperabilidad.

Dichos algoritmos de referencia son: algoritmos de cifrado (3DES, DES), algoritmos de hash (MD5 y SHA-1); además de poder utilizar otros algoritmos como: Encriptación de clave pública Diffie-Hellman, RSA, etc.

Figura 3. Algoritmos utilizados por IPSec

IPSEC opera de dos formas AH y ESP definidos en los siguientes numerales.

2.4 Temas de Desempeño

Implementar seguridad con IPv6, tiene por supuesto un costo en el desempeño, como cualquier desarrollo de criptografía, esto es particularmente significativo cuando la protección es aplicada a todo el tráfico. La mayor parte del tráfico en las organizaciones no requiere protección IPSec. Por ejemplo, no es necesario proteger una conexión del usuario desde el hogar a la red corporativa con una VPN IPsec cuando todos ellos están navegando o descargando archivos.

IPsec puede tener un alto impacto sobre el throughput y poder de procesamiento requerido en dispositivos. Puede ser insignificante en términos de poder de procesamiento para un computador de usuario estándar, puede muy rápidamente llegar a ser un problema cuando IPsec es desarrollado sobre un servidor VPN con varios cientos de usuarios o sobre un móvil de bajo poder o dispositivo portátil [5].

3. PROTOCOLO AH

El protocolo AH[6] es el procedimiento utilizado por IPSec para garantizar la integridad y autenticación de los paquetes, suministrando un medio al receptor para autenticar el origen de los datos comprobando que no se sufrió alteración durante la comunicación. Sin embargo no provee servicios de confidencialidad, los datos transmitidos pueden ser vistos por terceros. Como lo indica su nombre, AH es una Cabecera de Autenticación, la cual se inserta entre la cabecera IPv6 y los datos transportados, de forma que los proteja de posibles ataques. Siendo AH un protocolo nuevo, el IANA7 le

[5] [5] Latif Ladid. Security and Privacity with IPv6. European Task Fork Communication. 2004

[6] [6] S. Kent, and R. Atkinson. IP Authentication Header (AH). RFC 2402, Noviembre de 1198.

asignó el número decimal 51[7]; esto significa que al campo cabecera del paquete IPv6 se le asigna 51.

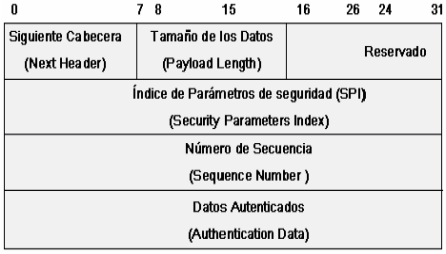

Figura 4. Cabecera de Autenticación AH

3.1 Cabecera de Autenticación

En la figura 4 se muestra la cabecera de autenticación AH, extensión de la cabecera básica IPv6. A continuación se definen cada uno de los campos:

- Cabecera Siguiente (Next Header): identifica cual es el protocolo que se encuentra en el segmento de datos.
- Longitud de carga útil (Payload Length), especifica la longitud de los datos en palabras de 32 bits.
- Reservado: reservado para uso futuro. Se debe fijar a cero.
- Índice de Parámetros de Seguridad (SPI). Es un valor arbitrario de 32 bits que, conjuntamente con la dirección de destino IP y el protocolo de seguridad (AH), identifican la Asociación de Seguridad para este paquete.
- Número de Secuencia (Sequence Number): Identifica el número del paquete en la comunicación, estableciendo un orden y evitando problemas de entrega de paquetes fuera de orden o ataques externos mediante la reutilización (Replay Attacks) de paquetes.
- Datos Autenticados (Authentication Data): Se obtienen realizando el algoritmo de hash entre algunos campos de la cabecera IP, la clave secreta y los datos enviados.

3.2 Funcionamiento del protocolo AH

El funcionamiento se observa en la figura 5

- La función hash o algoritmo de hashing es aplicado a la combinación del mensaje de entrada y una clave,
- Esto da como salida la representación del mensaje en forma de una cadena de dígitos que se denomina MAC, esto es como una huella digital de los datos.
- El MAC se copia en el campo datos autenticados del paquete AH, de esta forma queda construido el paquete IPSec el cual se envía a través de la red,
- En el origen se aplica la función hash y se hace el cálculo del MAC, se compara con el recibido en el paquete, si son iguales, el receptor tiene la seguridad de que el paquete no ha sido modificado durante la comunicación y que procede efectivamente del origen esperado.

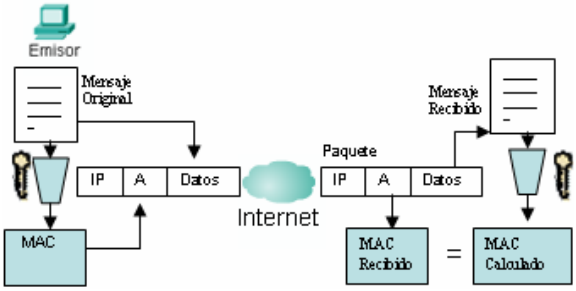

Figura 5. Funcionamiento del protocolo AH

4. PROTOCOLO ESP

El objetivo principal del protocolo ESP[8] es proporcionar confidencialidad; define el modo de cifrar los datos que se desean enviar y cómo este contenido cifrado se incluye en el paquete IPv6, adicionalmente, puede ofrecer los servicios de integridad y autenticación del origen de los datos incorporando un mecanismo similar al de AH.

4.1 Cabecera de Cifrado de Seguridad

La Cabecera de ESP es propia de IPv6, es colocada después de todos los encabezados en el paquete y se le asignó el número decimal 50.

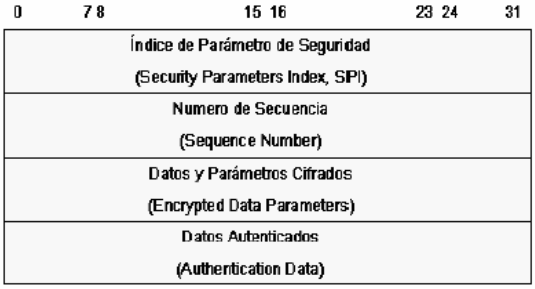

Figura 6. Cabecera de Cifrado de Seguridad (ESP)

La figura 6 muestra los campos incluidos en la cabecera de cifrado de seguridad.

[7] [7] Protocol Numbers: http://www.iana.org/assignments/protocol-numbers

[8] [8] S. Kent, and R. Atkinson. Protocol Encapsulating Security Payload (ESP). RFC 2406 Noviembre de 1998.

- Índice de Parámetros de Seguridad (SPI), específica que asociación de seguridad emplear para desencapsular el paquete ESP.
- Número de Secuencia (Sequence Number). Este número de secuencia se emplea para protegerse de ataques por repetición de mensajes.
- Datos Cifrados, Es un campo de longitud variable que contiene el mensaje encriptado. La información que utiliza el algoritmo de encriptación para su funcionamiento es incluida dentro de este campo. Dentro de este campo se definen también los campos de relleno, longitud del relleno y cabecera siguiente.

4.2 Funcionamiento del Protocolo ESP

La función de cifrado en el protocolo ESP se realiza mediante un algoritmo de cifrado de clave simétrica, este algoritmo maneja cifrado de bloque, de modo que la longitud del mensaje tiene que ser múltiplo del tamaño del bloque (8 o 16 bytes, en la mayoría de los casos). Por esta razón existe un campo de relleno en la cabecera de cifrado de seguridad ESP.

En la figura 7 se representa como el protocolo ESP permite enviar los datos de forma confidencial.

- Para enviar los mensajes el emisor toma el mensaje original, y le aplica el algoritmo de criptografía simétrica 3DES,
- El mensaje cifrado se incluye en el paquete IPSec, a continuación de la cabecera ESP. Durante el tránsito hasta su destino, si el paquete es interceptado por un tercero sólo obtendrá un conjunto de bits incoherentes.
- En el destino, el receptor aplica de nuevo el algoritmo de cifrado recuperando los datos originales.

La seguridad que se proporciona está en la robustez del algoritmo de cifrado, es decir, que un atacante no puede descifrar los datos sin conocer la clave, así como la clave ESP únicamente la conocen el emisor y el receptor.

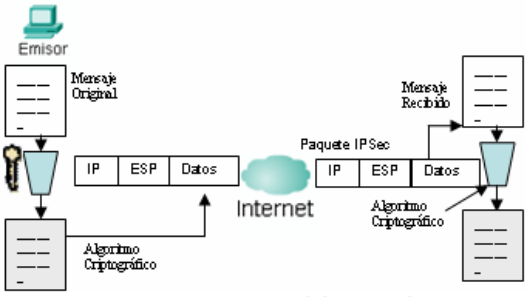

Figura 7. Funcionamiento del Protocolo ESP

5. PROTOCOLO IKE

Es un protocolo de control que se encarga de poner en contacto y negociar los algoritmos, claves y demás elementos para la comunicación segura con IPSec entre dos computadores. El IETF ha definido el protocolo IKE[9] para realizar tanto esta función de gestión automática de claves como el establecimiento de las asociaciones de seguridad correspondientes.

IKE es un protocolo híbrido que ha resultado de la integración de dos protocolos complementarios: *ISAKMP y OAKLEY.*

ISAKMP define de forma genérica el protocolo de comunicación y la sintaxis de los mensajes que se utilizan en IKE, esto facilita los procedimientos y formatos del paquete para establecer, negociar, modificar y eliminar asociaciones de seguridad. OAKLEY especifica la lógica de cómo se realiza de forma segura el intercambio de una clave entre dos partes que no se conocen previamente.

6. PRUEBAS DE IPSec

Para el desarrollo de las diferentes pruebas se configuró una red como muestra la figura 7. Los equipos contaban con sistema operativo Red Hat Linux 9.0.

Figura 8. Esquema de pruebas

La instalación de IPv6 requiere una serie de cambios y modificaciones, estos varían según el sistema operativo elegido (FreeBSD, Windows, LINUX...), los pasos que se explican a continuación son para sistemas operativos LINUX.

- Se configura el equipo con la dirección IPv4 y la máscara
- Se carga el protocolo IPv6, editando el archivo *etc/sysconfig/network*, se agrega la línea *NETWORKING_IPV6=YES*
- Se modifica el archivo de la interfaz ethernet, en su archivo de configuración *etc/sysconfig/network-scripts/ifcfg-eth0* se agrega la línea *IPV6INIT="yes"* y se asigna la dirección IPv6 con, *IPV6ADDR=" 3ffe:8070:1026:1::1/64"*
- Se guardan los cambios y se reinicia la red con */etc/init.d/network restart*
- Se utiliza el comando *ifconfig* para verificar la configuración
- Se verifica la conectividad con ping6 3ffe:8070:1026:1::2

[9] [9]D. Harkins and D. Carrel. The Internet Key Exchange. RFC 2409, Noviembre de 1998.

Hasta el momento existe conectividad IPv6 pero no hay transmisión segura, para esto se instaló y configuró en cada uno de los equipos Frees/wan, lo cual es una implementación de los protocolos IPSec en Linux[10] ofreciendo a IPv6 servicio de cifrado y autenticación.

Básicamente Frees/Wan, está formado por:

- KLIPS (kernel IPsec). Se trata de la implementación de los protocolos AH y ESP, y se encarga, también, de la gestión de paquetes dentro del kernel del sistema.
- Pluto. Es el demonio del protocolo IKE, se encarga de negociar las conexiones con otros sistemas.
- Varios scripts que proporcionan al administrador, una interfaz con los protocolos IPSec.

Para su instalación se descarga del sitio ftp://ftp.xs4all.nl/pub/crypto/freeswan/binaries , se puede instalar sobre cualquiera de los siguientes Kernels: 2.0.3X, 2.2.1X o 2.4.X. Además se descargan las utilidades de Frees/Wan y el paquete para comprobación de las claves *freeswanrpmsign.asc.*

A continuación se importa la clave a la base de datos RPM digitando en la consola la ruta en la que se guardó:
cd /instalar/Freeswan
rpm --import freeswan-rpmsign.asc

Para comprobar la existencia de las firmas se debe digitar el comando:
rpm --checksig freeswan.rpm*

Para instalar RPM se deben ejecutar los siguientes comandos en la consola: *rpm -ivh freeswan*.rpm*
Para el correcto funcionamiento de los protocolos IPSec es necesario configurar el archivo *ipsec.secrets* pues en el se guardan las claves utilizadas para la autenticación de las conexiones IPSec.

Para configurar ipsec.secrets se debe ejecutar el siguiente comando en la consola:
ipsec newhostkey --output /etc/ipsec.secrets
cat /etc/ipsec.secrets

Para verificar que la instalación fue exitosa se digita el comando: *ipsec verify*

Para comprobar que la instalación ha sido correcta se ejecuta ifconfig y se observa que aparece una interfaz virtual llamada ipsec0. Para verificar el tráfico encriptado entre los dos equipos se utilizó el analizador de protocolos *Ethereal* para linux[11]. *Ethereal* contiene un analizador de protocolo de red, también conocido como "*sniffer"*. Provee una interfaz gráfica y muchas opciones de organización y filtrado de información, de este modo permite ver todo el tráfico que pasa a través de una red estableciendo la configuración en modo promiscuo.

[10] [10] http://www.freeswan.org
[11] [11] http://www.ethereal.com/

7. CONCLUSIONES

Realizar conexiones seguras a través del protocolo IPSec en ambiente IPv6 garantiza el uso de fuertes algoritmos de encriptación y técnicas de criptografía para asegurar la confidencialidad y autenticidad de los datos que son transmitidos, aunque con estas características de seguridad adicionadas pueden causar una desmejora en el desempeño de la red.

Investigar las características del protocolo IPv6 permitirá garantizar en un futuro la utilización de direccionamiento IP de 128 bits para el uso de direcciones IP públicas en nuestras redes, permitiendo la expansión de las redes.

De los resultados obtenidos, se puede resaltar que es indispensable realizar pruebas con IPv6 extensión IPSec, para estar preparados para el cambio de aplicaciones y demás servicios de red durante todo el período de transición de IPv4 a IPv6.

La documentación de pruebas realizadas en el presente estudio facilitará posteriores trabajos encaminados a la implementación de redes IPv6 con extensión IPSec, ya que cubren buena parte del camino en cuanto a la instalación y configuración en Linux de los servicios relacionados.

8. REFERENCIAS BIBLIOGRAFICAS

[1] S. Deering, R. Hinden. Internet Protocol, Version 6 (IPv6) Specification.Internet-Draft, RFC 1752, Enero 1995.
[2] R. Hinden, S. Deering. IPv6 Addressing Architecture RFC2373.
[3] V. Fuller, T. Li, J. Yu, and K. Varadhan. Classless interdomain routing (CIDR), RFC 1519 September 1993.
[4] Track. S. Kent, R. Atkinson. Security Architecture for the Internet Protocol. RFC 2401. November 1998.
[5] Latif Ladid. Security and Privacity with IPv6. European Task Fork Communication. 2004
[6] S. Kent, and R. Atkinson. IP Authentication Header (AH). RFC 2402, Noviembre de 1198.
[7] Protocol Numbers:
http://www.iana.org/assignments/protocol-numbers
[8] S. Kent, and R. Atkinson. Protocol Encapsulating Security Payload (ESP). RFC 2406 Noviembre de 1998.
[9]D. Harkins and D. Carrel. The Interet Key Exchange. RFC 2409, Noviembre de 1998.
[10] http://www.freeswan.org
[11] http://www.ethereal.com/