IMPLEMENTACIÓN DE LA SEGURIDAD DEL PROTOCOLO DE INTERNET VERSIÓN 6

IMPLEMENTATION OF SECURITY INTERNET PROTOCOL VERSION 6

AUTOR
JOSUÉ LOBO CONTRERAS
Plan de estudios de Ingeniería de Sistemas
Semillero de Investigación GNU/Linux And Security
*Universidad Francisco de Paula Santander Ocaña
josueloboc@gmail.com
COLOMBIA

AUTOR
DEWAR WILLMER RICO BAUTISTA
Ingeniero de Sistemas
Especialista en Telecomunicaciones
Msc. (c) Ciencias Computacionales
*Universidad Francisco de Paula Santander Ocaña
Docente Tiempo Completo/Director de Investigación y Extensión
Facultad de Ingenierías
dwricob@ufpso.edu.co
COLOMBIA

INSTITUCIÓN
*UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA
UFPSO
Sede Algodonal Via Acolsure – Ocaña – Norte de Santander
info@ufpso.edu.co
COLOMBIA

INFORMACIÓN DE LA INVESTIGACIÓN O DEL PROYECTO: Ingeniería Proyecto de investigación Seguridad en Redes. Universidad Francisco de Paula Santander Ocaña UFPSO. Fecha de inicio, Febrero de 2010. Fecha de Finalización, Octubre de 2011. Ejecutado por, Dewar Willmer Rico Bautista. Financiado, Universidad Francisco de Paula Santander Ocaña UFPSO.

RECEPCIÓN: Noviembre 6 de 2011 **ACEPTACIÓN:** Marzo 20 de 2012

TEMÁTICA: Ingeniería eléctrica, electrónica, telecomunicaciones y telemática: (Gestión y Seguridad en redes)

TIPO DE ARTÍCULO: Artículo de Investigación Científica y Tecnológica.

RESUMEN ANALÍTICO

A través de este artículo se muestra como IPSec puede brindar un nivel de seguridad a la información en las redes de datos que soportan el protocolo de internet de siguiente generación IPv6 y además, establecer una comparación del comportamiento del tráfico IP a través del uso de servicios de seguridad criptográfica para observar cómo influye en el rendimiento de la red.

Se describen las diversas herramientas que se pueden encontrar en Internet y se pueden descargar gratuitamente, se propone uno de los más conocidos el Wireshark (Ethereal), un analizador de protocolos utilizado para realizar análisis y solucionar problemas en redes de comunicaciones para desarrollo de software y protocolos, y como una herramienta didáctica para educación.

Se medirá el flujo de datos con y sin IPSec para IPv6, se buscan resultados que permitan ser analizados y generar conclusiones sobre como los mecanismos de seguridad a través de protocolos son aplicables a solucionar las problemáticas de seguridad en el ambiente de las redes e Internet, no antes tener una idea clara de los requisitos de seguridad, ya que la solución depende de cada escenario.

Finalmente se analizará el flujo de datos de los resultados obtenidos de la prueba con y sin IPSec para IPv6, y así generar el análisis comparativo del tráfico de datos con y sin IPSec habilitado para IPv6.

PALABRAS CLAVES: Gestión, IPSec, IP, IPv6, Seguridad

ANALYTICAL SUMMARY

Through this article shows how IPSec can provide a level of security to information in data networks that support the Internet Protocol Next-Generation IPv6 and also a comparison of the behavior of IP traffic through the use of services cryptographic security to see how it affects the network performance.

It describes the various tools that can be found on the Internet and can be downloaded free of charge, we propose one of the most popular the Wireshark (Ethereal), a protocol analyzer used to perform analysis and solve problems in communication networks and software development protocols, and as a teaching tool for education.

It will measure the flow of data with and without IPSec for IPv6, is looking for results that can be analyzed and general conclusions about how the security mechanisms via protocols are applicable to solve the problems of safety in the network and the Internet, not before having a clear idea of the security requirements, since the solution depends on the stage.

Finally, analyze the data flow test results with and without IPSec for IPv6, and generate a comparative analysis of data traffic without IPSec enabled for IPv6

KEYWORDS: IPSec, IP, IPv6, Management, Security

INTRODUCCIÓN

El Protocolo de internet versión 6 (IPv6) es un protocolo estándar para las redes de datos que están basadas en el modelo de comunicaciones TCP/IP, que nace como una actualización del anterior protocolo IPv4 y de los requerimientos de las Tecnologías de la Información y la Comunicación (TICs).

IPSec es la seguridad del protocolo de internet, que constituye un marco de normas abiertas que proporciona protección a las comunicaciones a través del uso de servicios de seguridad criptográfica, garantizando los tres principios de la seguridad informática en las redes de datos: Confidencialidad, Integridad y Disponibilidad.

1. PROTOCOLO DE INTERNET VERSIÓN 6

IPv6 es la nueva versión del protocolo de Internet. En 1995, la IETF (Internet Engineering Task Force) que desarrolla estándares para los protocolos de Internet, publicó una especificación para el IP de la siguiente generación, conocido como IPng (Internet Protocol next generation). Esta especificación se convirtió en 1996 en un estándar conocido como IPv6, el cual proporciona una serie de mejoras funcionales al IP existente conocido como IPv4, diseñado para ajustarse a las altas velocidades de las redes actuales y a la mezcla de flujo de datos, que incluyen audio y vídeo, pero detrás del desarrollo del nuevo protocolo se halla la necesidad imperante de nuevas direcciones. Los cambios de IPv6 con respecto a IPv4 se explican en el RFC 2460.

2. SEGURIDAD DEL PROTOCOLO DE INTERNET (IPSEC)

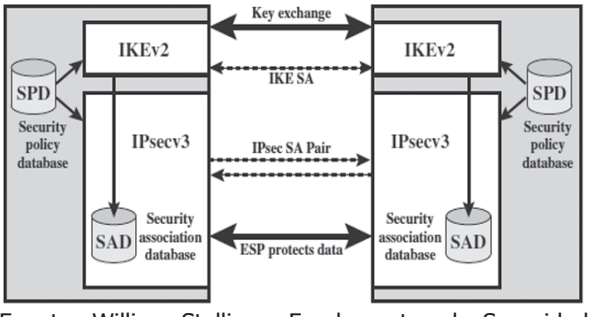
IPSec es un conjunto de mecanismos de seguridad para proteger las comunicaciones que utilizan el protocolo de Internet, a través del uso de los servicios de seguridad criptográfica. Además, admite la autenticación a nivel de red de pares, de origen de datos, integridad de datos, confidencialidad de los datos (encriptación) y protección contra la reproducción.

La implementación de IPSec se basa en las especificaciones elaboradas por la Internet Engineering Task Force (IETF).

2.1 ASOCIACIONES DE SEGURIDAD (SA) RFC 4301

Un concepto significativo que aparece en los mecanismos de autenticación y confidencialidad en IP es el de asociación de seguridad (SA, Security Association). Una asociación es una relación unidireccional entre emisor y un receptor que ofrece servicios de seguridad al tráfico que se transporte. Si se necesita una relación que haga posible un intercambio bidireccional seguro, entonces, se requieren dos asociaciones de seguridad. Los servicios de seguridad se suministran a una SA para que use AH o ESP, pero no ambos.

FIGURA 1. Arquitectura IPSec.



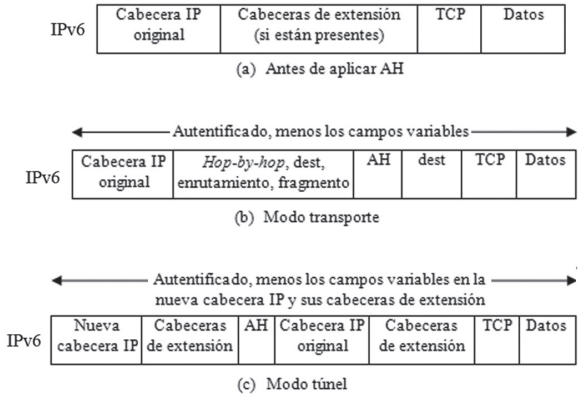
Fuente: William Stallings. Fundamentos de Seguridad en Redes, Aplicaciones y Estándares. Segunda Edición.

2.2 MODOS DE FUNCIONAMIENTO

Tanto AH como ESP permiten dos modos de uso: modo transporte y modo túnel.

Modo transporte: El modo trasporte proporciona protección principalmente a los protocolos de capas superiores. Es decir, esta protección se extiende a la carga útil de un paquete IP. Algunos ejemplos incluyen un segmento TCP o UDP, que operan directamente encima de IP en la pila de protocolos de un host. Normalmente, el modo transporte se usa para la comunicación extremo a extremo entre dos hosts.

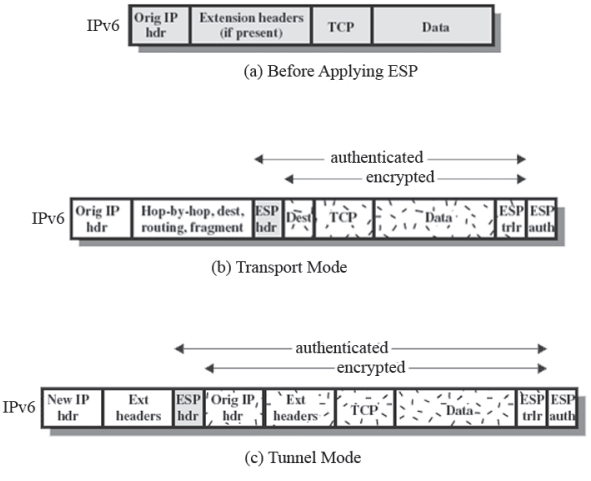
FIGURA 2. Ámbito de autentificación de AH.



Fuente: William Stallings. Fundamentos de Seguridad en Redes, Aplicaciones y Estándares. Segunda Edición.

Modo túnel: El modo túnel proporciona protección al paquete IP completo. Para conseguirlo, después de que han añadido los campos AH o ESP al paquete IP, el paquete completo más los campos de seguridad se tratan como carga útil de un paquete IP «exterior» nuevo con una nueva cabecera IP exterior. El paquete original entero, o interior, viaja a través de un «túnel» desde un punto de la red IP a otro; ningún router a lo largo del camino puede examinar la cabecera IP interior. Como el paquete original esta encapsulado, el nuevo paquete, que es mayor, puede tener direcciones de origen y destino totalmente diferentes, lo cual añade seguridad. El modo túnel se usa cuando uno o los dos extremos de una SA es una pasarela de seguridad, como podría ser un cortafuegos o un router que implementa IPSec.

FIGURA 3. Ámbito de cifrado y autenticación de ESP.



Fuente: William Stallings. Fundamentos de Seguridad en Redes, Aplicaciones y Estándares. Segunda Edición.

2.3 SERVICIOS

IPSec proporciona servicios de protección a la capa IP permitiendo que un sistema elija los protocolos de seguridad necesarios, determine los algoritmos que va a usar para los servicios y ubique las claves criptográficas necesarias para proveer los servicios solicitados.

FIGURA 4. Servicios de IPSec.

Servicio	*AH*	*ESP* (Encriptación)	*ESP* (Encriptación y Autenticación)
Control de acceso	✓	✓	✓
Integridad sin conexión	✓		✓
Autentificación del origen de datos	✓		✓
Rechazo de paquetes reenviados	✓	✓	✓
Confidencialidad		✓	✓
Confidencialidad limitada del flujo de tráfico		✓	✓

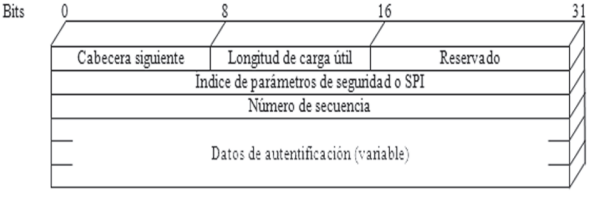
Fuente: William Stallings. Fundamentos de Seguridad en Redes, Aplicaciones y Estándares. Segunda Edición.

3. PROTOCOLO DE CABECERA DE AUTENTICACIÓN (AH) RFC 4302

La cabecera de autentificación proporciona soporte para la integridad de los datos y la autentificación de paquetes IP. La característica de integridad garantiza que no es posible que se produzca modificación no detectada en el contenido de un paquete durante la transmisión. La característica de autentificación permite que un sistema final o dispositivo de red autentifique al usuario o aplicación y filtre el tráfico adecuadamente; también evita los ataques de suplantación de dirección que se observan hoy en día en internet.

La cabecera de autenticación se compone de seis campos, como se ilustra en la Fig. 5.

FIGURA 5. Cabecera de autentificación IPSec.



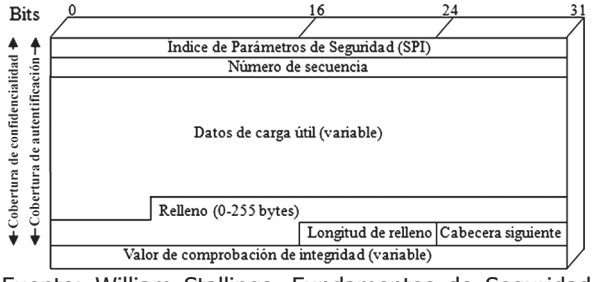
Fuente: William Stallings. Fundamentos de Seguridad en Redes, Aplicaciones y Estándares. Segunda Edición.

4. PROTOCOLO DE CARGA DE SEGURIDAD ENCAPSULADORA (ESP) RFC 4303

La carga de seguridad encapsuladora puede ser utilizada para garantizar la confidencialidad, autenticación del origen de datos, integridad sin conexión, un servicio anti-replay, y la limitación de la confidencialidad del flujo de tráfico IP. El conjunto de servicios prestados depende de las opciones seleccionado en el momento de la configuración de la Asociación de Seguridad (SA) y la ubicación de la implementación de una topología de red.

La Carga de seguridad encapsuladora se compone de siete campos, como se ilustra en la Fig. 6.

FIGURA 6. Formato ESP de IPSec.



Fuente: William Stallings. Fundamentos de Seguridad en Redes, Aplicaciones y Estándares. Segunda Edición.

5. PROTOCOLO DE INTERCAMBIO DE CLAVES DE INTERNET (IKE) RFC 4306

La parte de gestión de claves de IPsec implica la determinación y distribución de claves secretas. La especificación actual de la arquitectura de IPsec asigna soporte para dos tipos de gestión de claves:

Manual: Un administrador de sistema configura manualmente cada sistema con sus propias claves y con las llaves de otros sistemas que se comunican. Esto es práctico para entornos pequeños relativamente estáticos.

Automática: Un sistema automático permite la creación bajo demanda de claves para las SA y facilita el uso de claves en un sistema distribuido grande con una configuración cambiante.
El protocolo de gestión automatizada de claves por defecto para IPSec se conoce como ISAKMP/Oakley y se compone de los siguientes elementos:

Protocolo de determinación de Claves OAKLEY: Es un protocolo de intercambio de claves basado en el algoritmo Diffie-Hellman, pero que proporciona seguridad adicional. Oakley es genérico, ya que no dicta formatos específicos.

Asociación de seguridad y Protocolo de gestión de claves ISAKMP: Proporciona un marco de trabajo para la gestión de claves de Internet y el soporte de protocolos específicos, incluyendo formatos para la negociación de los atributos de seguridad.

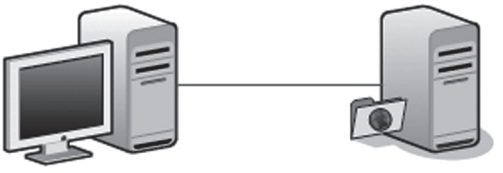
6. ESCENARIOS

Las pruebas realizadas en la presente investigación, se basan en tres escenarios experimentales de red sin conexión a Internet, donde se implementó la seguridad del protocolo de Internet, bajo sistemas operativos GNU/Linux y Microsoft.

6.1 ESCENARIO 1

Implementación de la seguridad del protocolo de Internet IPSec entre sistemas operativos Microsoft.

FIGURA 7. Esquema de red escenario 1



Windows Seven Ultimate *Windows Server 2008 Enterprise*

La práctica se realizó con los sistemas operativos Windows Server 2008 Enterprise como servidor y Windows 7 Ultímate como cliente. En donde, el servidor ofrece el servicio de red FTP, mediante un servidor de nombres de dominio (DNS), el cual es accedido desde el cliente mediante un software de código abierto para descargas llamado Filezilla ó desde cualquier navegador mediante el servidor web de Windows *Internet Information Services* (IIS7).

Computador 1
Sistema Operativo: Windows Server 2008 Enterprise
Dirección IPv6: 2011:b89:1:1::1
Longitud de Prefijo de red: /125
Puerta de Enlace Predeterminada: Ninguno
Servidor DNS Preferido: Ninguno
Servidor DNS Alternativo: Ninguno
De donde se va a generar el flujo de datos mediante el protocolo FTP (File Transfer Protocol)

Computador 2
Sistema Operativo: Windows 7 Ultímate
Dirección IPv6: 2011:b89:1:1::2
Longitud de Prefijo de red: /125
Puerta de Enlace Predeterminada: Ninguno
Servidor DNS Preferido: 2011:b89:1:1::1
Servidor DNS Alternativo: Ninguno
Cliente, que para este caso sería Filezilla

Software
_Analizador de protocolos Wireshark
_Filezilla 3.5.0
_Microsoft Windows 7 Ultímate
_Microsoft Windows Server 2008 Enterprise
_Xligth FTP Sever
_Zenmap

6.2 ESCENARIO 2

Implementación de la seguridad del protocolo de Internet IPsec entre sistemas operativos GNU/Linux y Microsoft.

FIGURA 8. Esquema de red laboratorio 2

La práctica se realizó con los sistemas operativos Ubuntu Server 11.04 como servidor y Windows 7 Ultímate como cliente. En donde, el servidor Linux ofrece el servicio de red MAIL con *postfix y dovecot*, mediante el servidor de nombres de dominio *bind9*, el cual es accedido desde los clientes mediante el software de mensajería outlook.

Computador 1
Sistema Operativo: Ubuntu Server 11.04
Dirección IPv6: 2011:b89:1:1::1
Longitud de Prefijo de red: /125
Puerta de Enlace Predeterminada: Ninguno
Servidor DNS Preferido: Ninguno
Servidor DNS Alternativo: Ninguno

Computador 2
Sistema Operativo: Windows 7 Utimate
Dirección IPv6: 2011:b89:1:1::2
Longitud de Prefijo de red: /125
Puerta de Enlace Predeterminada: Ninguno
Servidor DNS Preferido: 2011:b89:1:1::1
Servidor DNS Alternativo: Ninguno

Computador 3
Sistema Operativo: Windows 7 Utimate
Dirección IPv6: 2011:b89:1:1::3
Longitud de Prefijo de red: /125
Puerta de Enlace Predeterminada: Ninguno
Servidor DNS Preferido: 2011:b89:1:1::1
Servidor DNS Alternativo: Ninguno

Software
_Analizador de protocolos Wireshark
_Microsoft Outlook 2010
_Microsoft Windows 7 Ultimate
_Nmap
_Racoon
_Servidor BIND9
_Servidor Dovecot
_Servidor Postfix
_Ubuntu Server 11.04
_Webmin 1.550

6.3 ESCENARIO 3

Implementación de la seguridad del protocolo de Internet IPSec entre sistemas operativos GNU/Linux.

FIGURA 9. Esquema de red laboratorio 3

La práctica se realizó con los sistemas operativos Ubuntu Server 11.04 como servidor y Ubuntu 11.04 Desktop como cliente. En donde, el servidor Linux ofrece el servicio de red MAIL con *postfix y dovecot*, mediante el servidor de nombres de dominio *bind9*, el cual es accedido desde los clientes mediante el software de mensajería de código abierto Thunderbird.

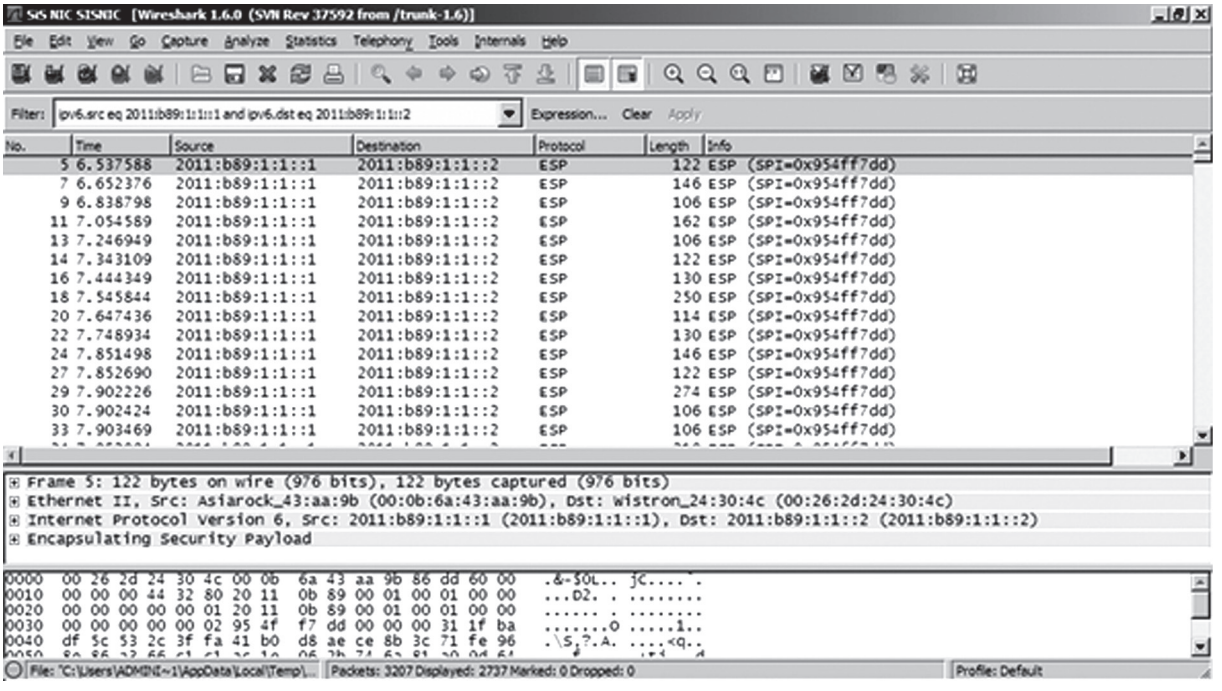
Computador 1
Sistema Operativo: Ubuntu 11.04
Dirección IPv6: 2011:b89:1:1::2
Prefijo de red: /125
Puerta de Enlace: Ninguno
Servidores DNS: 2011:b89:1:1::1
Dominios de búsqueda: ipv6security.edu

Computador 2
Sistema operativo: Ubuntu Server 11.04
Dirección IPv6: 2011:b89:1:1::1
Prefijo de red: /125
Puerta de enlace: Ninguno
Servidores DNS: Ninguno
Dominios de búsqueda: Ninguno
Computador 3
Sistema Operativo: Ubuntu 11.04
Dirección IPv6: 2011:b89:1:1::3
Prefijo de red: /125
Puerta de Enlace: Ninguno
Servidores DNS: 2011:b89:1:1::1
Dominios de búsqueda: ipv6security.edu

Software
_Analizador de protocolos Wireshark
_Evolution 2.32.2
_Mozilla Thunderbird 3.1.10
_Nmap
_Racoon
_Rpcap
_Servidor BIND9
_Servidor Dovecot
_Servidor Postfix
_Ubuntu 11.04
_Ubuntu Server 11.04
_Webmin 1.550

7. RESULTADOS POR ESCENARIO

FIGURA 10. Captura de red de descarga de archivos sobre IPv6 con IPSec.



El análisis de resultados se realiza con base a los reportes generados mediante el analizador de protocolos de red de código abierto Wireshark.

7.1 ESCENARIO 1

Descarga de archivos

FIGURA 11. Estadísticas generales de red de la descarga de archivos sobre IPv6 con y sin IPSec.

Parámetros de red	IPv6 sin IPSec	IPv6 con IPSec
Paquetes	2737	2737
Intervalo de tiempo entre el primer paquete y el último	47,803 Segundos	47,828 Segundos
Promedio de paquetes por segundo	57,256	57,225
Promedio del tamaño del paquete	1419,439 Bytes	1455,349 Bytes
Bytes	3885004	3983290
Promedio de bytes por segundo	81271,416	83283,021
Promedio de Megabits por segundo	0,650	0,666

Tomando como referencia los valores del ancho de banda, obtenidos en las capturas de red con y sin IPSec, se tiene:

0,650 Mbit/seg 0,666 Mbit/seg = |0,016 Mbit/seg|

0,650 Mbit/seg ⟶ 100%
0,016 Mbit/seg ⟶ x

$$x = \frac{0{,}016 \times 100}{0{,}650}$$

$x = 2.4625$

Como se puede observar el aumento del ancho de banda al aplicar los métodos de autenticación y cifrado del protocolo de seguridad de Internet es del 2.4615%, tomando como referencia el ancho de banda estimado en la prueba con IPv6 sin IPSec. De acuerdo a los resultados mostrados en la Figura 11, se observa que aunque el flujo de paquetes IP es el mismo en ambas pruebas, se evidencia un aumento tanto en los tiempos de transmisión de la información, como en el tamaño de bytes transmitidos, lo cual se ve reflejado en el desempeño de la red.

Carga de archivos

FIGURA 12. Estadísticas generales de red de la carga de archivos sobre IPv6 con y sin IPSec.

Parámetros de Red	IPv6 sin IPSec	IPv6 con IPSec
Packets	1529	1529
Between first and last packet	201,337 seconds	197,007 seconds
Average packets/seconds	7,594	7,761
Averaga packet size	75,252 bytes	107,219 bytes
Bytes	115060	163938
Average bytes/seconds	571,479	832,142
Average Mbit/seconds	0,005	0,007

Tomando como referencia los valores del ancho de banda, obtenidos en las capturas de red con y sin IPSec, se tiene:

0,005 Mbit/seg 0,007 Mbit/seg = |0,002 Mbit/seg|

0,005 Mbit/seg ⟶ 100%
0,002 Mbit/seg ⟶ x

$$x = \frac{0{,}002 \times 100}{0{,}005}$$

$x = 40$

Como se puede observar el aumento del ancho de banda al aplicar los métodos de autenticación y cifrado del protocolo de seguridad de Internet es del 40%, tomando como referencia el ancho de banda estimado en la prueba con IPv6 sin IPSec.

Se concluye de este laboratorio:

- Los sistemas operativos Microsoft brindan soporte nativo para el actual protocolo de comunicaciones Internet Protocol versión 6, así como las aplicaciones generadas por comunidades desarrolladoras de software libre brindan soporte para IPv6 mediante requerimientos especiales.
- El rendimiento de la red disminuye al implementar la seguridad del protocolo de Internet sobre el servicio FTP.

7.2 ESCENARIO 2

Envió de mensajes del cliente de correo usuario1 al servidor Ubuntu Server 11.04

FIGURA 13. Comparación de parámetros de red del tráfico IP entre el servidor Ubuntu Server 11.04 y el cliente de correo usuario1 del laboratorio2.

Parámetros de Red	IPv6 sin IPSec	IPv6 con IPSec
Packets	13	13
Between first and last packet	2,573 seconds	2,805 seconds
Average packets/seconds	5,053	4,635
Averaga packet size	96,462 bytes	132,462 bytes
Bytes	1254	1722
Average bytes/seconds	487,438	613,970
Average Mbit/seconds	0,005	0,005

Tomando como referencia los valores del ancho de banda, obtenidos en las capturas de red con y sin IPSec, se tiene:

0,004 Mbit/seg - 0,005 Mbit/seg = |0,001 Mbit/seg|

0,004 Mbit/seg ⟶ 100%
0,001 Mbit/seg ⟶ x

$$x = \frac{0{,}001 \times 100}{0{,}004}$$

$x = 25$

Como se puede observar el aumento del ancho de banda al aplicar los métodos de autenticación y cifrado del protocolo de seguridad de Internet es del 25%, tomando como referencia el ancho de banda estimado en la prueba con IPv6 sin IPSec.

Envió de mensajes del servidor Ubuntu Server 11.04 al cliente de correo usuario2.

FIGURA 14. Comparación de parámetros de red del tráfico IP entre el servidor Ubuntu Server 11.04 y el cliente de correo usuario2 del laboratorio2.

Parámetros de Red	IPv6 sin IPSec	IPv6 con IPSec
Packets	16	18
Between first and last packet	0,073 seconds	0,408 seconds
Average packets/seconds	218,852	44,163
Averaga packet size	290,188 bytes	333,778 bytes
Bytes	4643	5828
Average bytes/seconds	63507,990	14299,104
Average Mbit/seconds	0,508	0,114

Tomando como referencia los valores del ancho de banda, obtenidos en las capturas de red con y sin IPSec, se tiene:

0,508 Mbit/seg - 0,114 Mbit/seg = |0,394 Mbit/seg|

0,508 Mbit/seg ⟶ 100%
0,114 Mbit/seg ⟶ x

$$x = \frac{0{,}114 \times 100}{0{,}508}$$

x = 22.4409

Como se puede observar no hay un aumento del ancho de banda al aplicar los métodos de autenticación y cifrado del protocolo de seguridad de Internet, sino que por el contrario, solo se utiliza un 22.4409% de la red, tomando como referencia el ancho de banda estimado en la prueba con IPv6 sin IPSec.

Se concluye de este laboratorio:

- Las aplicaciones de agentes de correo como evolution, Tuhnderbird y Outlook por comunidades desarrolladoras de software libre brindan soporte para IPv6 mediante requerimientos especiales.
- La aplicación racoon mediante su complemento racoon-tool permite brindar Integridad y cifrado a nuestras comunicaciones.
- La aplicación rpcap permite sniffear los sistemas operativos GNU/Linux a modo texto de manera remota mediante sistemas Microsoft.
- Los servidores Bind9, Dovecot y postfix permiten configurar el servicio de mensajería bajo el protocolo IPv6.
- La aplicación zenmap permite escanear los puertos que están funcionando bajo IPv6.
- La aplicación webmin nos permite administrar sistemas operativos GNU/Linux bajo interfaz gráfica.

7.3 ESCENARIO 3

Envió de mensajes usuario1 al servidor Ubuntu Server 11.04

FIGURA 15. Comparación de parámetros de red del tráfico IP entre el servidor Ubuntu Server 11.04 y el cliente de correo usuario1 del laboratorio3.

Parámetros de Red	IPv6 sin IPSec	IPv6 con IPSec
Packets	26	12
Between first and last packet	7,007 seconds	0,134 seconds
Average packets/seconds	3,711	89,665
Averaga packet size	105,038 bytes	132,000 bytes
Bytes	2731	1584
Average bytes/seconds	389,760	11835,736
Average Mbit/seconds	0,003	0,095

Tomando como referencia los valores del ancho de banda, obtenidos en las capturas de red con y sin IPSec, se tiene:

0,003 Mbit/seg - 0,095 Mbit/seg = |0,092 Mbit/seg|

0,003 Mbit/seg ⟶ 100%
0,095 Mbit/seg ⟶ x

$$x = \frac{0{,}092 \times 100}{0{,}003}$$

x = 3066,6667

Como se puede observar no hay un aumento del ancho de banda al aplicar los métodos de autenticación y cifrado del protocolo de seguridad de Internet, sino que por el contrario, solo se utiliza un 3066,6667% de la red, tomando como referencia el ancho de banda estimado en la prueba con IPv6 sin IPSec.

Envió de mensajes del servidor Ubuntu Server 11.04 al usuario2

FIGURA 16. Comparación de parámetros de red del tráfico IP entre el servidor Ubuntu Server 11.04 y el cliente de correo usuario2 del laboratorio3.

Parámetros de Red	IPv6 sin IPSec	IPv6 con IPSec
Packets	14	20
Between first and last packet	0,109 seconds	5,400 seconds
Average packets/seconds	128,380	3,703
Averaga packet size	230,643 bytes	229,200 bytes
Bytes	3229	4584
Average bytes/seconds	29610,002	848,821
Average Mbit/seconds	0,237	0,007

Tomando como referencia los valores del ancho de banda, obtenidos en las capturas de red con y sin IPSec, se tiene:

0,237 Mbit/seg - 0,007 Mbit/seg = |0,001 Mbit/seg|

0,237 Mbit/seg ⟶ 100%
0,23 Mbit/seg ⟶ x

$$x = \frac{0{,}23 \times 100}{0{,}237}$$

x = 97,0464

Como se puede observar no hay un aumento del ancho de banda al aplicar los métodos de autenticación y cifrado del protocolo de seguridad de Internet, sino que por el contrario, solo se utiliza un 97,0464% de la red, tomando como referencia el ancho de banda estimado en la prueba con IPv6 sin IPSec.

Se concluye de este laboratorio:

- La aplicación ipsec-tools permite proteger las conexiones extremo a extremo, pero es deficiente ya que presenta un fallo en su estructura.
- Los analizadores de protocolos de red o sniffer Wireshark y Tshark tienen soporte para el análisis de la arquitectura tanto de IPv6 como de IPSec.
- La aplicación nmap permite scanear los puertos que están funcionando bajo IPv6.

Para que IPSec garantice la protección del flujo de datos, las cabeceras IP deben someterse a modificaciones mediante algoritmos matemáticos, para que los paquetes circulen con su carga cifrada por la red. Al emplear estos mecanismos el tamaño del paquete aumenta como se evidencia en el ítem "Promedio del tamaño por paquete", lo que genera que el consumo de ancho de banda sea mayor.

7.4 DESEMPEÑO

El desempeño de la red es un factor significativo en la implementación de mecanismo de seguridad, por esto, la Figura 17, muestra los distintos valores del ancho de banda en cada una de las pruebas realizados con IPv6 y sus extensiones de seguridad IPSec en cada escenario.

FIGURA 17. Rendimiento de la red en la implementación de IPSec.

Escenario	Pruebas	IPv6 sin IPSec	IPv6 con IPSec
Escenario 1	Prueba 1	0,650 Mb/s	0,666 Mb/s
	Prueba 2	0,005 Mb/s	0,007 Mb/s
Escenario 2	Prueba 1	0,004 Mb/s	0,005 Mb/s
	Prueba 2	0,508 Mb/s	0,114 Mb/s
Escenario 3	Prueba 1	0,003 Mb/s	0,095 Mb/s
	Prueba 2	0,237 Mb/s	0,007 Mb/s

Como se puede observar en la mayoría de las pruebas realizadas en los distintos escenarios experimentales, se produce un consumo mayor del ancho de banda al implementar las extensiones de seguridad de IPSec, lo cual genera un desmejoramiento en el rendimiento de la red. Esto sucede, ya que al implementar la seguridad del protocolo de internet sobre IPv6, se emplean métodos y procedimientos matemáticos que generan modificaciones en los datos transmitidos, por lo que el tamaño de los archivos aumenta considerablemente y hace que la red genere un mayor numero de paquetes IP para enviar la información.

FIGURA 18. Soporte de los programas para el protocolo de internet IPv6.

Parámetros de Red	Soporte IPv6	Dependencia de IPv4 sobre IPv4
Apache 3	Si	No
Binn 9	Si	No
Debian 6	Si	No
Dig	Si	No
Dovecot	Si	No
Evolution	Si	No
Google Chrome	Si	No
Internet Explorer	Si	No
Internet Information Services	Si	No
Ipsec tools	Si	No
Microsoft Outlook	Si	No
Microsoft Windows Server 2008 Enterterprise	Si	No
Microsoft Windows 7 Ultimate	Si	No
Mozilla Filezilla	Si	No
Mozilla Firefox	Si	No
Mozilla Thunderbird	Si	No
Mutt	Si	No
Nmap - Zenmap	Si	No
Postfix	Si	No
Racoon	Si	No
Rpcap	Si	Si
Tshark	Si	No
Ubuntu Desktop 11.04	Si	No
Ubuntu Server 11.04	Si	No
Webmin	Si	Si
Wireshark	Si	No
Xlight FTP Server	Si	No

8. CONCLUSIONES

- Los resultados generados a través de laboratorios demostraron que la implementación de la seguridad del protocolo de Internet IPSec en redes de área local con IPv6, se puede realizar en sistemas operativos tanto propietarios como libres, pero en algunos escenarios de red el nivel de seguridad no es aceptable debido a que la funcionalidad de las aplicaciones es deficiente.

- IPv6 se ha extendido del ámbito experimental a la implementación real, ya que permitirá que las redes de datos sigan evolucionando día tras día, por lo que su estructura fue mejorada respecto a los fallos que presenta su antecesor IPv4.

- IPSec es una solución de seguridad para las redes de comunicaciones que están soportadas sobre IPv6, ya que garantiza los tres principios básicos de la seguridad informática: Confidencialidad, Integridad y Disponibilidad mediante sus algoritmos de autentificación y cifrado.

- Realizar conexiones seguras a través de IPSec sobre IPv6 garantiza la protección de la información que es trasmitida por las redes, aunque las extensiones de seguridad reducen el rendimiento de la red en un 66,67% de los casos, ya que los parámetros de seguridad modifican el paquete IP.

- Además, IPSec es transparente a las aplicaciones, así que tiene un enfoque diferente a otros protocolos de seguridad como SSH y SSL, que funcionan en la capa de transporte y están ligados con una aplicación particular.

- Las configuraciones de IPSec realizadas en la presente investigación, solo pueden ser aplicados a intranets o redes internas, ya que se utilizan en modo transporte, debido a que la comunicación es directa entre el cliente y el servidor.

- La seguridad informática es un campo de estudio crítico de las redes de comunicación, lo que conlleva a pensar que esta disciplina debería contemplarse como una capa transversal de los modelos de comunicaciones TCP/IP y OSI.

9. REFERENCIAS BIBLIOGRAFICAS

[1] MAIORANO, Ariel. CRIPTOGRAFÍA Técnicas de desarrollo para profesionales. Alfaomega. Año 2009.

[2] BEHROUZ, A. Forouzan. Transmisión de datos y redes de comunicaciones, cuarta edición. McGraw-Hill. Año 2007.

[3] CARRACEDO, Gallardo Justo. Seguridad en redes telemáticas. McGraw-Hill. Año 2004

[4] RICO, Dewar y SANTOS, L. M. Seguridad de protocolo de internet: estado del arte. Ingenio UFPSO. Año 2009.

[5] OLIFER Natalia y OLIFER Víctor. Redes de computadores. McGraw-Hill. Año 2009.

[6] ETERSEN, Richard. Linux VI Edición. McGraw-Hill. Año 2009.

[7] STALLINGS, William. Network security essentials applications and standards, fourth edition. Prentice Hall. Año 2011.

10. REFERENCIAS ELECTRÓNICAS

[1] RICO, Dewar y SANTOS, L. M. IPSec DE IPv6 EN LA UNIVERSIDAD DE PAMPLONA [en línea]<http://www.utp.edu.co/php/revistas/ScientiaEtTechnica/docsFTP/111011320-325.pdf> [citado el 10 de abril de 2010]

[2] RICO, Dewar y SANTOS, L. M. IPSec DE IPv6 EN LA UNIVERSIDAD DE PAMPLONA [en línea http://www.utp.edu.co/ciencia/index.php?UnArt=1&&id=1102> [citado el 10 de abril de 2010]

[3] Publib.boulder.ibm.com. Protocolo Cabecera de Autenticación (AH) [en línea] <http://publib.boulder.ibm.com/html/as400/v4r5/ic2931/info/RZAFM241AHDEFANDCO.HTM> [citado el 10 de abril de 2010]

[4] Publib.boulder.ibm.com. Protocolo Encapsulated Security Payload (ESP) [en línea] <http://publib.boulder.ibm.com/html/as400/v4r5/ic2931/info/RZAFM231ESPDEFANDCO.HTM> [citado el 10 de abril de 2010]

[5] SciencieDirect. Security threats to Internet: a Korean multi-industry investigation [en línea] <http://linkinghub.elsevier.com/retrieve/pii/S0378720601000714> [citado el 11 de abril de 2010]

[6] 6SOS, IPv6 Servicio de información y soporte. El protocolo IPv6. [en línea] <http://www.6sos.org/documentos/6SOS_El_Protocolo_IPv6_v4_0.pdf> [citado 12 de abril de 2011]

[7] Internet Enginnering Task Force. RFC 2460, Internet Protocol, version 6 (IPv6) Specification. [en línea] < http://www.ietf.org/rfc/rfc2460.txt > [citado 15 de marzo de 2010]

[8] Internet Enginnering Task Force. RFC 4301, Security Architecture for the Internet Protoocol. [en línea] < http://www.ietf.org/rfc/rfc4301.txt > [citado 28 de marzo de 2010]

[9] Internet Enginnering Task Force. RFC 4302, IP Authentication Header. [en línea] < http://www.ietf.org/rfc/rfc4302.txt > [citado 14 de abril de 2010]

[10] Internet Enginnering Task Force. RFC 4303, IP Encapsulating Payload (ESP). [en línea] < http://www.ietf.org/rfc/rfc4303.txt > [citado 20 de junio de 2010]

[11] Internet Enginnering Task Force. RFC 4306, Internet Key Exchange (IKEv2) Protoocol. [en línea] < http://www.ietf.org/rfc/rfc4306.txt > [citado 26 de agosto de 2010]