SEGURIDAD DE LA INFORMACIÓN UTILIZANDO IPSEC (INTERNET PROTOCOL SECURITY) PARA IPV6 (INTERNET PROTOCOL VERSION6)

WILMER FABIÁN HERNÁNDEZ BELTRÁN
MANUEL IGNACIO FORERO ARIZA

UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD DE INGENIERÍAS FÍSICO MECÁNICAS
ESCUELA DE INGENIERIAS ELÉCTRICA, ELECTRÓNICA Y TELECOMUNICACIONES
ESPECIALIZACIÓN EN TELECOMUNICACIONES
2012

SEGURIDAD DE LA INFORMACIÓN UTILIZANDO IPSEC (INTERNET PROTOCOL SECURITY) PARA IPV6 (INTERNET PROTOCOL VERSION6)

WILMER FABIÁN HERNÁNDEZ BELTRÁN
MANUEL IGNACIO FORERO ARIZA

MONOGRAFÍA PRESENTADA COMO REQUISITO PARCIAL PARA OPTAR AL TÍTULO DE:
ESPECIALISTA EN TELECOMUNICACIONES

DIRECTOR:
ING. RAUL BAREÑO

UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD DE INGENIERÍAS FÍSICO MECÁNICAS
ESCUELA DE INGENIERIAS ELÉCTRICA, ELECTRÓNICA Y TELECOMUNICACIONES
ESPECIALIZACIÓN EN TELECOMUNICACIONES
2012

AGRADECIMIENTOS

Especialmente a Dios que es el motor de nuestra vida.

A nuestros padres por su ayuda.

A nuestro director Raúl Bareño, por su manera de guiarnos en el proceso.

A los docentes que nos orientaron, incentivaron y nos motivaron a seguir trabajando.

TABLA DE CONTENIDO

Pág.

LISTA DE FIGURAS

Pág.

LISTA DE TABLAS

Pág.

RESUMEN

TITULO: SEGURIDAD DE LA INFORMACION UTILIZANDO IPSEC (INTERNET PROTOCOL SECURITY) PARA IPV6 (INTERNET PROTOCOL VERSION 6) *

AUTORES: HERNANDEZ BELTRAN, Wilmer Fabián
FORERO ARIZA, Manuel Ignacio **

PALABRAS CLAVES: EITF, IPV6, IPSEC, IKE, AH, ESP.

CONTENIDO:

Esta monografía hace un análisis sobre la seguridad en Internet proporcionada por IPsec en ambientes IPv6, basándose en estándares internacionales (RFC) y una guía actualizada de Cisco Systems Inc. Del 2011. En los cuales se habla de los servicios de Autentificación, Integridad, Confidencialidad, Control de Acceso, y el conjunto de protocolos por los cuales este funciona (AH, ESP, IKE, ISAKMP).

Esta monografía es recomendada para los implementadores de esta tecnología, docentes en el área de telecomunicaciones, docentes en las materias de redes, y para el público en general que quiera adquirir conocimientos sobre el tema y se familiarice con IPsec en ambientes IPv6.

Todo aquel que requiera un enfoque sobre la seguridad del nuevo protocolo IPv6, podrá recurrir a esta monografía ampliando mas su conocimiento sobre el tema y logrando comprender a fondo el funcionamiento y manejo que se le da a la seguridad de la información en este nuevo protocolo.

Describe el funcionamiento de IPSec en ambientes IPv6, sus modos de uso, metodologías a usar en IPSec para IPv6, ventajas y desventajas y recomendaciones antes de implementarse.

Tambien se podrá encontrar en los primeros capítulos, historia y funcionamiento de los tipos de criptografía que se uso en un principio y como fue evolucionando a medida que iba pasando el tiempo.

***Trabajo de Grado**
***Universidad Industrial de Santander, Especialización en telecomunicaciones, Escuela de Ingenierías eléctrica, electrónica y telecomunicaciones. Director: Raúl Bareño**

SUMMARY

TITTLE: SEGURIDAD DE LA INFORMACION UTILIZANDO IPSEC (INTERNET PROTOCOL SECURITY) PARA IPV6 (INTERNET PROTOCOL VERSION 6)*

AUTHORS: HERNANDEZ BELTRAN, Wilmer Fabian
FORERO ARIZA, Manuel Ignacio **

KEYWORDS: EITF, IPV6, IPSEC, IKE, AH, ESP.

DESCRIPTION:

This monograph makes an analysis of Internet security provided by IPsec in IPv6 environments, based on international standards (RFC) and an updated guide of Cisco Systems Inc. From 2011. In which we talk about services Authentication, Integrity, Confidentiality, Access Control, and the set of protocols by which this works (AH, ESP, IKE, ISAKMP).

This monograph is recommended for implementers of this technology, teachers in the area of telecommunications, teachers in the areas of networks, and the general public who want to acquire knowledge on the subject and become familiar with IPsec in IPv6 environments.

All one who wants a study about the segurity of the new protocol IPv6, can use this document in wich can get more information about the theme and can know mor deep de function and management that will have the segurity of the information in this protocol.

Describes the operation of IPSec in IPv6 environments, modes of use, methods to use IPSec for IPv6, advantages and disadvantages and recommendations before implementation.

Equal in the first chapters can find history and function of tipes of criptologyuse at the beginning and how it was growing in the past of the time.

***Trabajo de Grado**
***Universidad Industrial de Santander, Especialización en telecomunicaciones, Escuela de Ingenierías eléctrica, electrónica y telecomunicaciones. Director: Raúl Bareño**

INTRODUCCION

En la actualidad, internet es el medio de comunicación más utilizado, con fines académicos, económicos, informativos o simple entretenimiento. Razón por la cual maneja gran cantidad de información tanto privada como pública, que a su vez está expuesta a ser vista por un número indeterminado de personas. Sin embargo, los datos e información que reposa en este medio deben ser asegurados y protegidos para evitar abusos, manipulaciones o un mal uso, por parte de personas inescrupulosas o no autorizados.

La curiosidad, la necesidad de información o el simple morbo, pueden despertar en las personas un deseo por traspasar las barreras de seguridad y acceder a los datos de otros, para transformar, utilizar o simplemente evidenciar los intereses de los propietarios de los mismos. En buena medida, estas acciones se logran a través de amenazas o vulnerabilidades que el remitente permitir, por lo cual se debe tener algunos métodos para protegerla y evitar al máximo el robo o captura de esta información.

IPv6 fue creado debido al agotamiento de las direcciones IPv4, pero en este nuevo protocolo se corrigieron errores que venían de su antecesor. En IPv4 se usaba IPsec pero debía ser implementado, en IPv6 IPsec ya viene inmerso en él y es el protocolo que usa IPv6 para dar seguridad. El conjunto de protocolos y algoritmos que conforman a IPsec, permiten habilitar un sistema, que selecciona los protocolos de seguridad necesarios, determina los algoritmos dependiendo del servicio y pone llaves criptológicas necesarias.

A medida que la tecnología va avanzando su seguridad también debe ser cada vez más robusta e impenetrable; sin embargo, persisten problemas de seguridad en las redes de comunicaciones, que pueden ser: confiabilidad, integridad, autenticación y repudio, para resolver estos problemas se implementa el protocolo IPsec. Control de acceso, autenticación de origen, integridad, reenvío de paquetes, confidencialidad de flujo y confidencialidad, son el conjunto de servicios de seguridad que se pueden obtener usando IPsec, pues estos servicios los brinda la capa IP, y otras superiores como: UDP, BGP, TCP ICMP, entre otros).

IPsec también incorpora diferentes servicios de seguridad, tales como: Integridad sin conexión, control de acceso para prevenir el uso no permitido de recursos, detecta la modificación de un datagrama IP individual, protege de anti replay, autentica el origen de los datos, para secuencias parciales reconoce su integridad, encriptación de flujo de tráfico limitado y encriptación en general.

IPsec tiene muy buenas mejoras como el acceso seguro y transparente, mayor seguridad en el comercio electrónico, las redes montadas en redes públicas son más confiables y seguras, para empleados trabajando a distancia dispone confidencialidad como estando dentro de su red LAN de la oficina.

1. SEGURIDAD Y PROTOCOLOS DE SEGURIDAD

1.1. Seguridad de la información

Al referirse a seguridad de la información esto lleva a pensar en ¿cómo se podría ocultar la información? ¿Qué mecanismos se pueden usar para mantener segura la información? ¿Cómo se puede lograr que la información solo la conozca o comparta una o algunas personas especificas? Entre muchas otras preguntas que pueden surgir para que la información este lo mejor resguardada posible, sin importar en que medio se tenga o transmita. Debido a estas preguntas se ha evolucionado en estos temas y hoy en día, es muy importante cuidar la información transmitida y compartida.

Esta evolución ha conllevado al desarrollo de nuevas tecnologías, aplicaciones, dispositivos y hasta formas de crear la información más segura y consistente y todo esto debido a la información.

Para los fines académicos de la presente tesis, se considera la información como el conjunto de datos que pueden ser almacenados y procesados en computadores; con limitaciones de acceso para leer, copiar o modificar, dependiendo del usuario que la necesite; y así evitar que personas mal intencionadas puedan usarla, compartirla, modificarla o robarla.

Esto permite concluir que la información puede estar concentrada en un punto y puede ser de gran utilidad y valor, también se observa que así como es de gran valor esta podrá ser usada para cosas indebidas o no esperadas.

Si se tiene un lugar donde se almacena bastante información como un centro de cómputo o “data center” y este sufre un accidente donde toda esta información y no se tiene un centro alterno con copia de esta, ¿cómo afectaría la perdida de la información? ¿Qué tiempo tomaría volver a recuperar la información?

Se debe tener presente que este “data center” principal, almacena toda o una buena parte de la información relevante de una compañía o persona, lo que la convierte en una especie de “mina de oro” y a su vez la hace llamativa para ser atacada o vulnerada. Razón por la cual, se hace indispensable concentrar buena parte de los recursos y esfuerzos en generar mecanismos de protección altamente calificados que mimeticen o anulen los intentos de filtración de la misma generando a su alrededor un espectro similar a una potencial caja de seguridad o incluso un bunker.

Por medio de las redes y sistema de información se pueden transmitir gran cantidad de datos, documentos y ofrecer servicios que requieren un nivel de seguridad, que es puesto a prueba constantemente debido a que las redes cada

vez son más concurrentes y comparten la misma infraestructura, por lo que la información tienda a pasar por un mismo lado.

Al querer obtener el máximo provecho de estas redes, las compañías, administradores y ciudadanos deben tener muy presente la seguridad de las mismas. Cuando se logra bloquear e impedir una acción malintencionada o accidente en una red, este acto se interpreta como seguridad de la red, es decir que a mayores ataques bloquee una red, mayor es su nivel de seguridad y por lo tanto aumenta la confianza de los usuarios. Puesto que si alguna de estas acciones son permitidas se pondría en peligro la confidencialidad, autenticidad, integridad y disponibilidad de la información que se requiere transmitir o almacenar.

Al agrupar los continuos incidentes de seguridad se pueden contemplar los siguientes:

- Al transmitir información por medios electrónicos estos pueden ser bloqueados, modificados y copiados.
- Al interceptar estos datos, pueden usarse indebidamente y causar daños por invasión en la privacidad.
- Es muy común que accedan a equipos o redes de computadores para modificar, copiar o dañar datos.
- Diariamente se hacen gran cantidad de ataques informáticos por medio de Internet y en un futuro sufrirán también las redes telefónicas.
- Diferentes tipos de software o programas que se ingresen a una máquina pueden dañar, cambiar o eliminar datos del mismo.
- Recientes ataques o inclusive ataques diarios han llegado a ser muy dañinos y generan un gran costo para el atacado.
- El presentar páginas muy parecidas a las originales o autenticaciones muy parecidas, para hacerse pasar por una entidad o persona también causa daños irremediables, ya que después de poder entrar el atacante puede hacer hasta lo impensable, inclusive la información puede llegar a manos equivocadas.
- Una buena cantidad de incidentes son provocados por acciones imprevistas y sin intención, errores humanos y fallas.

Existen cinco elementos básicos para implementar seguridad, estos son definidos en el estándar ISO 7498-2 [ISO, 1989] que constituyen la seguridad de un sistema y están relacionados a continuación:

1) Confidencialidad: consiste en dar los permisos requeridos a cierta cantidad de personas, sistemas o entidades, con el fin de acceder a los datos de manera segura.
2) Autenticación: por medio de mecanismos controla la procedencia de la información y esta puede ser a nivel de usuario o de computadora.

3) Integridad: Permite comprobar que los datos vienen originales como cuando salieron del remitente.
4) Control de acceso: Define la disponibilidad de los recursos al ser necesitados.
5) No repudio: Permite informar tanto a emisor como receptor la recepción o transmisión de un mensaje, sin que este informe sea negado por alguna de las partes.

En la búsqueda de obtener lugares protegidos para la seguridad de información, se pueden tener en cuenta 6 elementos:

- Seguridad de procedimientos: Mantener protegido cualquier proceso o mantenimiento.
- Seguridad de emanación de compromisos: Se definen compromisos y responsabilidades al manipular información.
- Seguridad física: Físicamente se debe tener un control de los recursos para evitar pérdidas, robos, ingresos no permitidos u inconvenientes.
- Seguridad de comunicaciones: Protección en el canal de trasmisión, garantizando que la información llegue a su destino.
- Seguridad de personal: Permisos dados a ciertas personas para manipular los recursos.
- Seguridad de sistemas operativos: Permite a diferentes usuarios el acceso a los sistemas operativos.

Para mantener una buena seguridad en los sistemas sin importar tipo, procedencia, sistema operativo o aplicación siempre se debe prevenir cualquier ataque o vulnerabilidad.

1.2. Componentes que intervienen en la seguridad informática

En la seguridad informática existe diferentes componentes que influyen en ella, estos se pueden clasificar en 4 grupos:

- Ataques
- Vulnerabilidades
- Contra-medidas
- Amenazas

1.2.1. Ataques

Es el medio por el cual se revientan las vulnerabilidades, se usan para realizar dos tipos de ataques: activos o pasivos.

1.2.1.1. Ataques activos

En este ataque los datos pueden ser modificados o cambiados totalmente, a lo cual se le clasifican en cuatro sub categorías:

- **Sustitución de identidad:** El atacante toma datos de una entidad, para suplantarla. Esta modalidad incorpora otras categorías para ataques activos. Un ejemplo puede ser la captura de secuencias de autenticación y con esta ingresa a datos explícitos e importantes, tomando los privilegios de la entidad que tiene los permisos, como la obtención de contraseñas de acceso en “X” cuenta.
- **Modificación de mensajes:** Los mensajes pueden ser cambiados, total o parcialmente, retardados o reorganizados, esto genera efecto sin permiso. Un ejemplo es un mensaje que solicite depositar dinero en una cuenta y se cambia el número de cuenta para efectuar el pago en otra.
- **Re-actuación:** Se atrapan diferentes mensajes y estos son reenviados continuamente, causando efectos no esperados. Se puede reflejar cuando se hace una transacción bancaría y que este movimiento se haga varias veces.
- **Degradación fraudulenta del servicio:** El bloqueo total o parcial de la gestión del medio informático y de comunicaciones. Un ejemplo sería, cuando los mensajes que se envían son eliminados, hasta congestionar la red con mensajes fraudulentos

1.2.1.2. Ataques Pasivos

Estos ataques no tienen como fin cambiar información, solo monitorearla, o escucharla, para copiar o utilizarla, con estos ataques se analiza el tráfico y toman datos transmitidos, está es una forma más sutil o de menor impacto para tomar información transmitida, y esta puede basarse en:

- Se conoce de donde salió y hacia dónde va la información, gracias al seguimiento que se hace de las cabeceras de los datos o paquetes obtenidos.
- La cantidad de paquetes enviado por las víctimas es controlado para obtener información del manejo normal o anormal de la red.
- Se detecta las horas pico donde se transfiere la información y así logra obtener los horarios de mayor actividad.

Como estos ataques solo son de visualización o monitoreo son difíciles de encontrar. Pero estos pueden ser detenidos o prevenidos usando mecanismos de cifrado y otros que se explicaran en el transcurrir del documento.

1.2.2. Vulnerabilidades

El software existente es pensado, diseñado y programado por humanos, por lo cual es posible que dentro de esta programación se cometan grandes errores o imperfectos, que personas malintencionadas pueden aprovechar para tomar información no autorizada, a estas fallas se les llaman vulnerabilidades.

1.2.3. Contra-medidas

Es la forma que por medio de políticas o procedimientos aplicados logra mejorar las vulnerabilidades y evitar ciertos ataques. Se debe generar un análisis de riesgo, el cual consiste en investigar la red buscando los riesgos que puedan existir y por dónde el atacante pueda tener una entrada a la información que no se quiere conocer, después de este análisis se pueden tomar las contra-medidas correspondientes.

Al analizar la red se pueden conocer muy bien el sistema a proteger y así también generar un buen sistema de seguridad. En el análisis de riesgo se puede obtener alguno de los ítems que se relacionan a continuación:

- Se encuentran amenazas en la red.
- Se encuentra medios o caminos por donde se pueden tener pérdidas de información.
- Se encuentra todas aquellas fallas que quedaron al elaborar el programa del software.
- Se comprueba exactamente los lugares sensibles de la compañía.
- Generar un buen sistema, que entregue seguridad eficiente en precio y tiempos.
- Encontrar que tantas veces se puede repetir una perdida.
- Se generan contra-medidas eficientes.
- Se identifican herramientas de seguridad.

Una representación gráfica de este análisis puede ser la ilustrada a continuación:

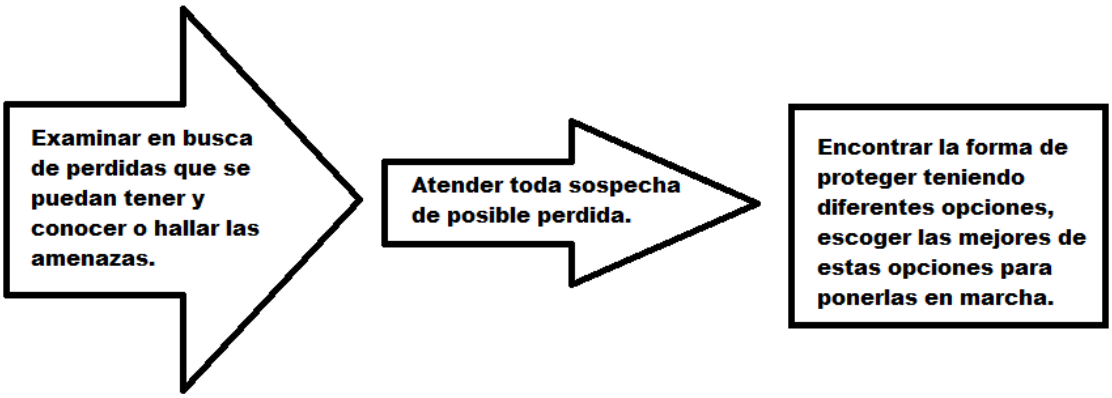

Figura 1: Pasos para la elaboración del análisis de riesgo.

1.2.4. Amenazas

Al transmitir información se pueden obtener los datos enviados, a su vez puede caer en manos de personas diferentes al usuario final, esto permite entender que la amenaza es todo aquel intento para tomar datos del canal de información. Para relacionar una amenaza con un ataque se puede decir que al ejecutar la amenaza ésta se convierte en un ataque, por ejemplo: La puerta de una casa puede estar abierta al pasar un ladrón ésta puede ser la amenaza, si el ladrón entra ese es el ataque. A continuación se explicara un poco los métodos o tipos de amenazas que puedan existir:

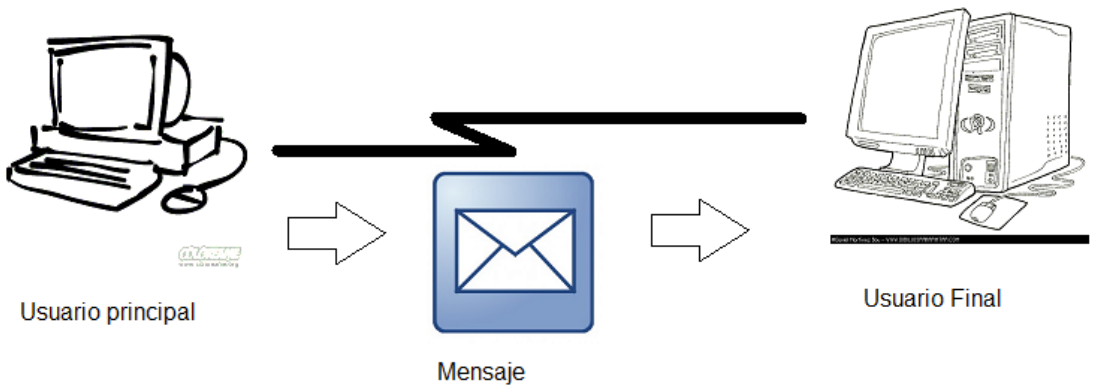

Figura 2: Trasmisión normal de los datos[1].

[1]Imágenes tomadas de los sitios: http://www.coloreamos.com/colorear/imagenes/colorear-dibujo-pc-ordenador.gif
http://www.coloreartusdibujos.com/wp-content/uploads/2012/01/ordenador-sobremesa.png
http://bberryblog.com/wp-content/uploads/2010/10/sobre.jpg visitada el 13 de Junio de 2012

Los tipos de ataques están clasificadas en:

- **Intercepción:** Esta situación se presenta cuando elementos, personas o equipos no autorizados logran obtener información enviada, vulnerando la confidencialidad de la red, por ejemplo: Cuando se escucha una conversación del otro lado del teléfono y se obtienen datos de reuniones o temas que sólo el emisor y receptor deben saber.

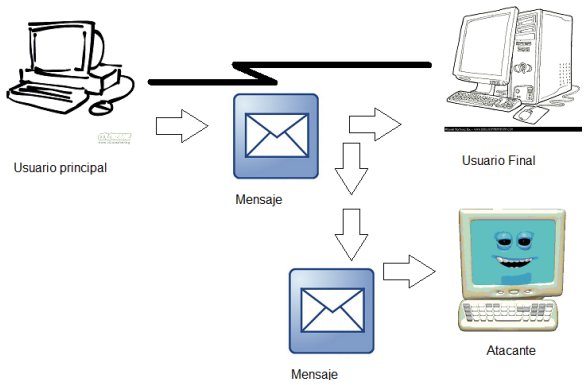

Figura 3: Transmisión interceptada por un atacante[2].

- **Interrupción:** Cuando la información transmitida es destruida o dañada por el atacante, aquí se amenaza la disponibilidad. Un ejemplo es cuando se roban el cobre (tipo de medio de transmisión) o medio de transmisión o simplemente le quitan un pedazo para evitar la comunicación.

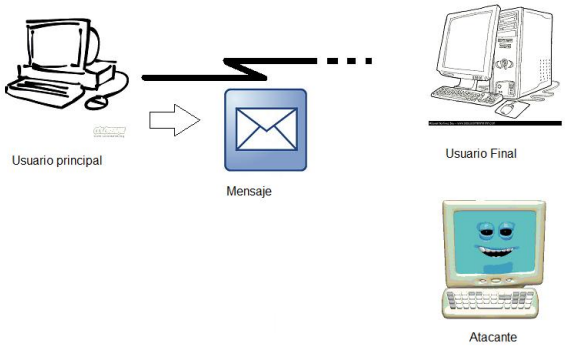

Figura 4: Transmisión interrumpida, la información no tiene por donde llegar a su destino.[3]

[2] Imágenes tomadas de los sitios: http://www.coloreamos.com/colorear/imagenes/colorear-dibujo-pc-ordenador.gif
http://www.coloreartusdibujos.com/wp-content/uploads/2012/01/ordenador-sobremesa.png
http://bberryblog.com/wp-content/uploads/2010/10/sobre.jpg
http://nataliavidente.files.wordpress.com/2011/11/ordenador-3d.gif visitada el 13 de Junio de 2012

[3] Imágenes tomadas de los sitios: http://www.coloreamos.com/colorear/imagenes/colorear-dibujo-pc-ordenador.gif

- **Fabricación:** El atacante crea los datos y los envía al usuario final, estos datos no son los originales y llevan información totalmente errónea, aquí se amenaza la autenticación.

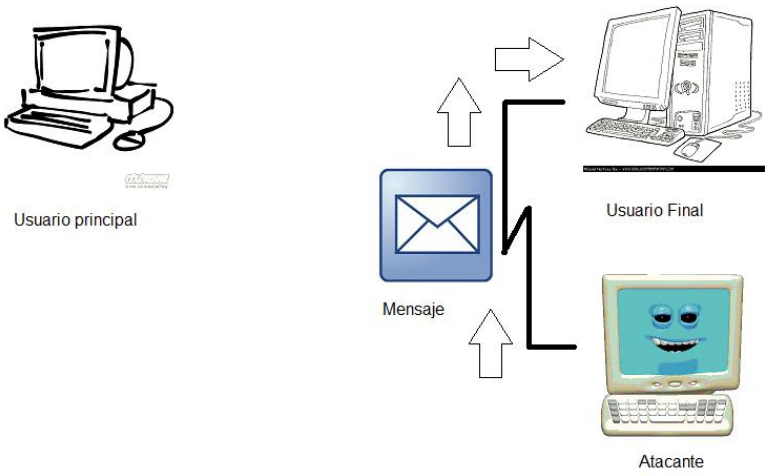

Figura 5: Transmisión fabricada por el atacante.

- **Modificación:** El atacante toma el mensaje original y este es modificado a su manera y reenviado al usuario final con las modificaciones que quiso el atacante. Aquí se amenaza la integridad. Un Ejemplo es la manipulación de montos cuando el mensaje es de dinero o cambios de cuentas cuando se debe hacer una consignación.

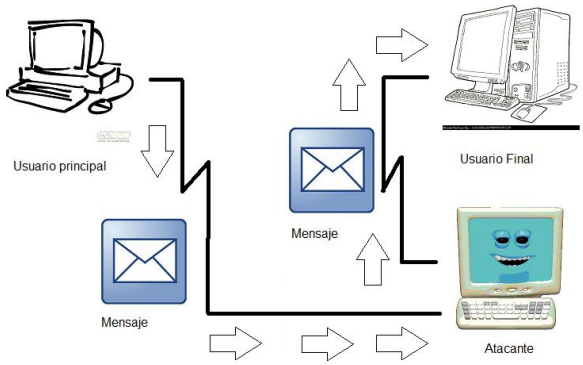

Figura 6: Transmisión modificada por el atacante[4].

---

http://www.coloreartusdibujos.com/wp-content/uploads/2012/01/ordenador-sobremesa.png
http://bberryblog.com/wp-content/uploads/2010/10/sobre.jpg
http://nataliavidente.files.wordpress.com/2011/11/ordenador-3d.gif visitada el 13 de Junio de 2012

[4] Imágenes tomadas de los sitios: http://www.coloreamos.com/colorear/imagenes/colorear-dibujo-pc-ordenador.gif
http://www.coloreartusdibujos.com/wp-content/uploads/2012/01/ordenador-sobremesa.png
http://bberryblog.com/wp-content/uploads/2010/10/sobre.jpg

1.3. Modelo OSI y Seguridad por Capas

1.3.1. Modelo OSI

OSI (Open System Interconections o interconexión de sistemas abiertos), esta interconexión se divide en siete capas las cuales permiten describir como se manejan los datos desde la conexión física hasta el momento donde llegan al aplicativo que maneja el usuario final. Este sistema se usa mucho para la explicación de los entornos de red, debido a que en la actualidad, es del que más se tiene conocimiento.

Figura 7: Modelo OSI [1][5]

La figura anterior muestra las diferentes capas que componen el sistema OSI, están enumeradas y van desde la capa física hasta la capa de aplicación. En la capa física los datos se transmiten por bits y al llegar aquí, desde que empiezan en el aplicativo o terminen en el deben ser convertidos a bits para poder ser transmitidos, este proceso lo permita cada una de las capas vista en la figura 7.

Cada capa tiene un propósito específico y es proveer los servicios a la capa que la sigue ascendentemente, Las capas son separadas estratégicamente para generar comunicación con su homóloga del otro extremo; pero realmente se están comunicando o intercambiando información con sus capas vecinas.

---

http://nataliavidente.files.wordpress.com/2011/11/ordenador-3d.gif visitada el 13 de Junio de 2012

[5] [1] SEGURIDAD EN IP CON EL PROTOCOLO IPSEC PARA IPV6, Universidad de San Carlos de Guatemala, Erick Lujan, 2005

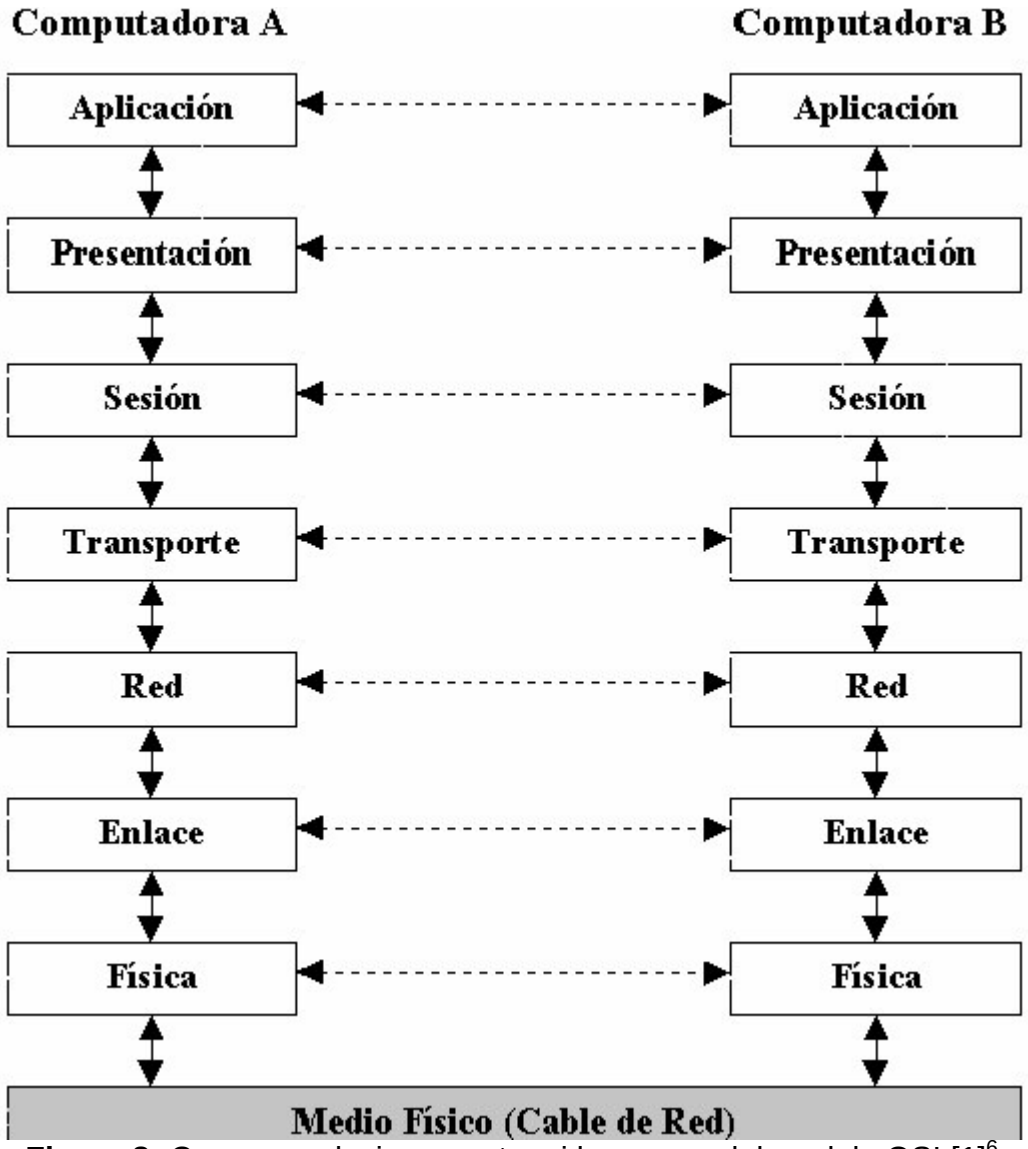

Figura 8: Como se relacionan entre si las capas del modelo OSI [1][6]

En la figura 8. Se puede observar que el único medio para el paso de la información entre las capas es por el medio físico o cable de red y de ahí van o subiendo o bajando por cada una de sus vecinas. En otras palabras, la capa de sesión de la máquina B quiere enviar información, la cual debe pasar por las capas de Transporte, red, enlace y física de la máquina B, entonces es transmitida por el medio físico o Cable y al llegar a la máquina A, debe subir por las capas física, enlace, red y transporte para poder llegar a su contraparte, la capa de sesión de la máquina A.

[6] [1] SEGURIDAD EN IP CON EL PROTOCOLO IPSEC PARA IPV6, Universidad de San Carlos de Guatemala, Erick Lujan, 2005

Entre cada capa debe existir comunicación o interacción, al cual se le llama interfaz y permite puntualizar los servicios que la capa de abajo ofrece a la vecina de arriba, además define cómo se va poder tener acceso a estos servicios entregados. Las capas al comunicarse tienen unas reglas llamadas protocolos

En la capa de comunicación del modelo se definen los servicios en los que se basan el desarrollo de protocolos. Por medio de la **Tabla 1**, se explica la relación que existe entre los servicios y cada una de las capas.

.

Servicio de Seguridad	Capa Física	Capa de Enlace	Capa de Red	Capa de Transporte	Capa de Sesión	Capa de Presentación	Capa de Aplicación
Autenticación de entidad extremo (*Peer Entity*)			SI	SI			SI
Autenticación del origen de los datos			SI	SI			SI
Servicios de Control de acceso			SI	SI			SI
Confidencialidad de la conexión	SI	SI	SI	SI			SI
Confidencialidad orientada a no conexión		SI	SI	SI			SI
Confidencialidad de un campo selectivo						SI	SI
Confidencialidad del flujo de tráfico	SI		SI				SI
Integridad orientada a no conexión			SI	SI			SI
Integridad de un campo selectivo							SI
Origen, no repudio							SI
Recepción, no repudio							SI

Tabla 1: Servicios que presta cada una de las capas del modelo OSI [1][7].

Al detallar la **Tabla 1**, se puede detectar que en servicios de seguridad, la capa de sesión no abarca ninguno, siguiendo con la capa de presentación que solo incorpora uno, la capa física y de enlace manejan dos cada una, la de transporte seis, la capa de red siete y la capa de aplicación los incluye todos.

A continuación se explicara con detalle cada una de las capas del modelo, que tienen relación directa con IPsec: la capa de red y Transporte.

[7] [1] SEGURIDAD EN IP CON EL PROTOCOLO IPSEC PARA IPV6, Universidad de San Carlos de Guatemala, Erick Lujan, 2005

1.3.1.1. Capa de Red

Esta capa se responsabiliza del tráfico de los datos, es decir es la que se encarga de buscar el camino y más óptimo para el envío de la información.

En esta capa se hace el cambio de la dirección MAC del equipo y se le pone la dirección lógica o IP.

Las funciones principales de esta capa son: Direccionamiento, enrutamiento y definición de las mejores rutas.

En esta capa se definen los siguientes puntos:

- Esta capa se encarga del establecimiento, y el estar o no conectado.
- Para el caso de subredes esta capa enruta, conmuta y controla cuando los paquetes se congestionen.
- Se encarga de enrutar y transmitir los paquetes de información en las redes.
- Esta capa selecciona el camino de los mensajes definiendo si el mensaje debe ser enviado a la capa 4 (capa de transporte) o a la capa 2 (capa de Red).
- Se encarga de determinar dentro de los nodos de la red el estado de cada uno de los mensajes.

Para interpretar mejor esta capa es necesario revisar la siguiente clasificación:

Capa de red superior. Esta subcapa no depende de la tecnología que tenga la red, pero si depende moderadamente sobre los grupos de protocolos que se manejan. En la parte de seguridad maneja los siguientes servicios: confidencialidad, control de acceso, autenticación del origen de datos e integridad orientada a no conexión y a secuencia parcial.

Capa de red Inferior. Esta subcapa, por el contrario si depende de la tecnología utilizada en la red y en poca medida de los grupos de protocolos que se manejen. En la parte de seguridad maneja los siguientes servicios: confidencialidad, control de acceso, autenticación del origen de datos e integridad orientada a no conexión y a secuencia parcial, diferenciándose de la capa anterior en la autenticación del origen de los datos en que esta capa es orientada tanto a conexión como a no conexión.

1.3.1.2. Capa de transporte

Como su nombre lo indica es el encargado del transporte y entrega confiable de la información, esta capa se encuentra en toda la mitad y funciona a manera de

puente entre sus niveles superiores los cuales son totalmente orientados a procesamientos y sus niveles inferiores que estos están orientados a las comunicaciones.

En esta capa se definen los siguientes puntos:

- Para los dispositivos de la red permite definir la ubicación de su localidad física.
- La capa 5 (sesión) requiere de unas características de transmisión y calidad de servicio, lo cual esta capa garantiza que este requerimiento se cumpla al llegar los datos de la capa de red.
- Dependiendo del usuario se crea o se le da una única dirección a cada uno.
- Soporta varias Conexiones.
- Para el envío de mensajes esta capa dice que protocolo garantizara su envío.
- Los nodos de la red, son los encargados de establecer la forma de deshabilitar o habilitar sus conexiones.
- Entre dos sistemas permite que la transferencia de datos sea transparente y confiable.

Posee una gran dependencia al grupo de protocolos que se utilicen, en la parte de seguridad maneja los siguientes servicios: confidencialidad, control de acceso, autenticación del origen de los datos, autenticación de la entidad extremo, integridad orienta a no conexión y a conexión, con recuperación de datos. La granularidad de protección radica en los Hosts por conexión.

1.4. Criptología

1.4.1. Significado

Es un estudio sobre los criptosistemas, y consiste en dos técnicas que la complementan: Criptografía y criptoanálisis.

Criptografía: Por medio de esta técnica se convierte un texto inteligible en otro, a este nuevo texto se le llama criptograma, la diferencia entre ambos textos es que uno es fácil de leer y lo puede visualizar cualquier persona mientras que el otro tiene un tipo de clave y no es fácil de entender, solo personas que conozcan su clave pueden leerlo.

Criptoanálisis: Es un análisis a los criptogramas, la persona que lo analiza es capaz de entenderlo y conocer su contenido sin tener permiso para ello.

1.4.2. Criptografía

Cambiar un texto por otro que lleve el mismo significado, pero que no sea entendible para todo el mundo, se llama encriptar. Este procedimiento restringe el acceso a la información real o del documento original.

Figura 9: Ejemplo de un texto original y su criptograma.

Existen dos algoritmos para encriptación: secreto y público, en este último, por su esencia permite el libre acceso, por lo tanto se debe agregar una clave, que debe ser conocida por un selecto grupo de personas y debe ser imprescindible para encriptar y desencriptar. En la actualidad se utilizan algoritmos públicos y claves secretas, debido a las siguientes causas:

- Existe un mismo nivel de seguridad.
- La forma de fabricación de los algoritmos públicos es en cadena, bien sea chips de hardware, como aplicaciones Software. Sale más económico de esta manera.
- Los algoritmos públicos por lo mismo que son públicos son más eficaces y tienen menos posibilidad de fallos, en cambio los algoritmos secretos al no tener tanto trabajo sobre ellos cualquier criptoanalista puede encontrar fallas sin encontrar el secreto del algoritmo.
- Comparando entre una clave y un algoritmo, es más fácil enviar la clave que todo lo que lleva un algoritmo..

La clave es vital en un sistema de comunicación con criptografía, puesto que a pesar de utilizar un algoritmo público, sin la clave es imposible encriptar o desencriptar el documento.

1.4.3. Criptoanálisis

El criptoanálisis contiene diferentes técnicas, y no depende de saber cual algoritmo se use, por medio de aproximación matemática se puede llegar al texto

original o desencriptado. Dependiendo de la información que se tenga se denota la dificultad del análisis, así el criptoanalista puede tener acceso a:

- Un criptograma
- Un criptograma y su texto original.
- Un texto original escogido y su criptograma o viceversa.
- Un texto original y su criptograma ambos obtenidos.

Al no tener suficiente información se hace más difícil descifrar un criptograma, siempre se necesita, por lo tanto se busca la clave que es el “huevo de oro” para descifrar dicho texto.

Las definiciones para un criptograma científico son:

- Distancia univoca: Para descifrar la clave se necesita una mínima cantidad del mensaje, un sistema ideal tienen una distancia univoca infinita.
- Sistema incondicionalmente seguro: La distancia univoca es mayor que el criptograma elaborado.
- Romper un sistema: Conseguir la clave de un sistema criptográfico por un método fácil.
- Sistema probablemente seguro: No se ha encontrado manera de romperlo.
- Sistema condicionalmente seguro: Los duros en el tema de análisis de criptogramas no tienen los medios para romper el criptograma.

En la actualidad, todo sistema es rompible, utilizando todas las claves posibles van a ser vulnerados, debido a esto en la criptología se busca cumplir con las siguientes reglas:

- El valor de la información debe ser menor al precio de rompimiento.
- El tiempo de vida de la información debe ser más corto que el tiempo que se tomen en descifrarlo.

1.4.3.1. Ejemplos de criptoanálisis:

Sistemas de prueba y error. Es el menos científico pero más utilizado, se basa en probar todas las claves posibles, bien sea haciéndolos por una secuencia estipulada o al azar, tomando diferentes claves sin ningún orden específico. En el azar la probabilidad de acierto es de un 50% de los casos intentados.

DES es uno de los sistemas, tiene una clave de 56 bits, la cantidad de claves posibles se calcula 2^56=7,2*10^16. Si se elabora una prueba en un micro segundo, esto tardaría en descifrarlo 1.142 años. Si se elabora 10^6 pruebas en un micro segundo tardaría 10,01 horas para descifrar la clave.
.

Métodos Estadísticos. Es el método tradicional. Por medio de la estadística, se usa la fuente para lograr el objetivo, este método es usado actualmente para algoritmos que ya van cumpliendo su ciclo. Para textos en español existe un estadístico de letras muy común:

8% para la letra l y s
8,7 % para la letra o
12 % para la letra a
16,8% para la letra e

Si se cambian letras por símbolos, se debe observar que cantidad de veces se repite el símbolo y así es fácil hallar la correspondencia entre los símbolos y las letras. Al utilizar agrupaciones de letras se genera el siguiente efecto:

- Con agrupaciones de letras es más fácil su detección debido al agrupar la letras esta se ajustan más a las estadísticas.
- Al agrupar en diagramas ya cambia la dificultad puesto que el alfabeto tiene un total de 26 letras y al agrupar en diagramas de a 2 esto quedaría: 26^2=676 símbolos.

Para dificultar el análisis, se pueden comprimir los ficheros antes de encriptarlos y así se cambia el estadístico.

1.4.4. Clasificación por tipo de clave

Existe una clasificación dependiendo el tipo de clave utilizado: Criptología simétrica y Criptología de clave pública o asimétrica.

1.4.4.1. Criptografía Simétrica

Este sistema es el más antiguo, se tiene referencia desde la época de Julio Cesar (100 – 44 a.c). La clave de encriptación y desencriptación es la misma y por esto se caracteriza. Se conoce como simétrica, debido a tiene una misma clave, y toda su seguridad depende de la seguridad de ella. El encargado de la encriptación después de generar la clave, envía la clave por un medio seguro a aquellas personas que tendrán permiso para ver la información encriptada. El gran problema de estos sistemas es la distribución de las claves, para resolver este inconveniente se usan los sistemas asimétricos, los cuales se montan solo para la transmisión de claves simétricas. Estos sistemas permiten la confidencialidad, excluye la firma digital y autenticación.

Las siguientes condiciones se deben cumplir para el algoritmo de encriptación para mantener la confidencialidad delante de un criptoanalista:

- Al tener el criptograma no se puede saber el texto ni adivinar la clave.
- Teniendo el texto y el criptograma, el valor para descifrar la clave debe ser más costoso que el valor de la información.

Cuando conoce el texto y el criptograma, se usa el sistema de prueba y error, para encontrar la clave. La forma de encriptación en los algoritmos simétricos es encriptando bloques de texto, que varían en tamaño según el algoritmo utilizado, existen cuatro formas de funcionamiento:

Electronic Codebook (ECB)
Cipher Block Chainning (CBC)
Cipher FeedBack (CFB)
Output FeedBack (OFB)

Los tipos de algoritmos simétricos más utilizados son:

DES (Data encryption Standard)
IDEA (International Data Encryption Algorithm)
RC5

Los anteriores algoritmos son enunciados pero no se detallan debido a que no forma parte integral del tema principal.

1.4.4.2. Criptografía de clave pública o asimétrica

Diffie y Hellman publicaron en 1.976 un artículo titulado “New directions in cryptography”, el cual hablaba de un nuevo tipo de criptografía que permitiera usar dos claves diferentes tanto para la encripción como la desencriptación, una sería conocida y la otra privada. De esta manera todos tenían acceso a la clave pública pero cada uno tenía una clave privada, este articulo revolucionó la criptología, pudiendo utilizar confidencialidad, autenticación y firma digital, también se soluciona el problema con la distribución de claves simétricas.

Dependiendo del servicio requerido se hace la respectiva encriptación:

Confidencialidad: La persona que encripta utiliza la clave pública de la persona a quien será enviado y quien recibe utiliza su clave privada para desencriptar, de esta manera sólo dos personas pueden tener la información del documento.

Autenticación: El emisor encripta total o parcialmente con su clave privada, así cualquier persona puede ubicar de donde viene el mensaje utilizando la clave pública. Este mensaje es auténtico debido a que el único que sabe como leerlo por medio de la clave privada es el emisor.

Firma digital: Funciona de igual manera que el anterior pero aquí siempre se encripta el resumen del mensaje, donde el criptograma obtenido es la firma del emisor, con esto es imposible que el emisor niegue la procedencia del documento. El receptor, no puede modificarlo pro si puede verificar que la firma sea la del emisor. Esta firma lleva implícita la autenticación.

Uniendo estos tres temas, se pueden elaborar sistemas muy completos. Estos algoritmos se basan en funciones matemáticas fáciles de resolver pero complicadas al momento de devolverse, un ejemplo es la potencia con el logaritmo. Al devolvernos en estas funciones se debe tener una clave, de lo contrario sería casi imposible lograr volver al valor original, es por esto que funciones como estas son muy útiles.

Las siguientes condiciones se deben cumplir para el algoritmo de encriptación

- Si se conoce el criptograma la clave no debe ser descifrada.
- Si se conoce el texto y criptograma es más económico el valor de la información que descifrar la clave.
- Si se conoce la clave pública y el texto, un criptograma con clave pública no se podrá generar.

Algunos de los algoritmos más utilizados son:

RSA (Rivest Shamir Adleman)
DSS (Digital Signature Estándar) solo para firmas digitales.
Diffie-Hellman, para distribución de claves. [2]

Los algoritmos anteriores son algunos de los que mayor seguridad genera en el tema de encriptación.

1.5. Protocolos de seguridad

Internet Engineering Task Force (IETF): Esta organización es la encargada que el manejo del Internet cada día sea mejor, se encarga de producir documentos de alta calidad, y técnicamente relevantes, esto influye en cómo la gente anega, diseña y usa el Internet.

AH (Authentication Header) y ESP (Encapsulation security Payload) son los protocolos que se denominan IPsec, estos se ubican en la capa 3 o capa de red del modelo OSI y esta capa es una de las más importantes en la parte de investigación.

La ITEF ha reconocido como estándares algunos protocolos de Criptología los cuales se muestras a continuación:

Capa	Nombre	Protocolos
7	Aplicación	X.400, MSP, X.400, MSP, PEM, S/MIME, PGP, X.500, DNSSEC, Administración de certificados y llaves.
6	Presentación	
5	Sesión	SSL
4	Transporte	TLSP
3	Red	NLSP,ESP,AH
2	Enlace de datos	SILS
1	Física	Enlace síncrono

Tabla 2: Capas y protocolos de criptografía. [1][8]

Algunos de los protocolos más importantes y los que se deben enfocar para este trabajo se describen a continuación:

1.5.1. Secure Socket Layer (SSL)

Netscape es el desarrollador de este protocolo, este permite confidencialidad y autenticación en Internet. Este protocolo no depende de la aplicación funciona como una capa adicional entre la aplicación y el Internet, esto permite que se utilice FTP, Telnet y otras aplicaciones diferentes de Http

Los siguientes pasos permiten la comunicación segura usando SSL:

Pedido de SSL:

SSL maneja un puerto para prestar su servicio, pero al recibir solicitudes este las acepta por un puerto diferente, estas solicitudes son creadas antes de establecer el SSL y se lleva a cabo solicitando una URL de un servidor con soporte de SSL. Entre el servidor y el cliente se hace una negociación de la conexión, después de hacer la solicitud y esta negociación es llamada SSL Handshake.

SSL Handshake:

Esta negociación cumple diferentes propósitos tales como determinar los algoritmos de Criptología a utilizar, autenticación con el servidor y el cliente y generación de la llave secreta, la cual se utiliza en el tiempo que dure la transmisión de mensajes dentro de la comunicación SSL.

[8] [2] **CRIPTOLOGIA**, Escuela universitaria Politécnica de Mataró, Manuel Pons Martorell.

Pasos dentro de la negociación entre cliente y servidor:

- Cliente Hello: El cliente envía un saludo al servidor informándole el algoritmo de Criptología a utilizar y pide la verificación de la identidad del servidor. Cuando el servidor no tiene un certificado que comprueba su identidad, el cliente al enviar los algoritmos de Criptología envía un número aleatorio, este último permite establecer la comunicación usando un conjunto de algoritmos diferentes. El protocolo de intercambio de llave dentro de los protocolos de Criptología define la forma de intercambiar la información entre cliente y servidor, los algoritmos de llave secreta que definen los métodos posibles a utilizar y un algoritmo de una sola vía (hash). En este paso no se intercambia información secreta simplemente se da una lista de posibles opciones.

- Server Hello: La respuesta del servidor lleva consigo su identificador digital, donde va la llave pública, un conjunto de algoritmos criptográficos y de compresión y al igual que el cliente envía un número aleatorio. El algoritmo que se usa es el más fuerte que soporten ambas partes. El servidor también puede pedir una autenticación o identificación del cliente.

- Aprobación del cliente: Según el identificador digital enviado el cliente comprueba su validez. Esto proceso lo hace por medio de una desencriptación al certificado enviado utilizando la llave publica del emisor y validando que este venga de una certificadora de confianza. Sobre el certificado se observa, la fecha, url de servidor, entre otros. Después de que se conoce que el servidor no es una falsedad, el cliente crea una llave aleatoria y la encripta con la llave publica del servidor y el algoritmo criptográfico a utilizar. Esta llave creada se usara en caso de que el Handshake tenga éxito, durante toda la sesión.

- Verificación: Aquí ya conocieron sus llaves tanto servidor como cliente y estas fueron desencriptadas, pero hace falta una verificación más para comprobar la seguridad del canal o que no haya sido alterada la información. Se debe confirmar la valides de las transacciones enviando copia de lo hecho anteriormente, pero esto se envía encriptado con la llave secreta, si al desencriptar se obtiene la información real se completa el Handshake pero si no se debe empezar el proceso de nuevo.

Ya las partes están autenticadas y listas para transmitir información, se utiliza entonces la llave secreta y algoritmos acordados en la negociación. Por cada sesión se usa una llave secreta.

Transmisión de datos:

Ya teniendo el canal SSL seguro, se puede empezar a transmitir datos, y al enviar un mensaje en alguna de las dos partes se genera un digest, el cual se encripta con el mensaje y se envía, el digest sirve para verificar el mensaje.

Finalización de sesión SSL:

El cliente se retira de la sesión, y la aplicación se encarga de informar que no existe seguridad en la comunicación y que el cliente quiere terminar la sesión.

1.5.2. Transport Layer Security (TLS)

SSL es el predecesor de este protocolo, este encripta en la capa de aplicación los segmentos de conexión a la red, utilizando criptografía asimétrica para el intercambio de llaves, criptografía simétrica para la privacidad y códigos de autenticación de mensajes para la integridad de los mensajes. Varias versiones de este protocolo están extendidas en aplicaciones como: Buscadores web, correo electrónico, fax por internet, mensajería instantánea y voz sobre IP.

La última actualización elaborada por la IETF es la RFC 5246 y está basada en las especificaciones anteriores de SSL. El protocolo TLS permite que aplicaciones cliente-servidor para comunicarse a través de una red de una forma diseñada para prevenir el espionaje y la manipulación.

Mientras muchos protocolos pueden ser usados con o sin TLS (o SSL) es necesario indicar al servidor si el cliente está haciendo una conexión TLS o no. Existen dos formas de lograr esto, una opción es usando diferente número de puerto para conexiones de TLS (ejemplo el puerto 443 para HTTPS), la otra opción es usada para regular el número de puerto y tiene la petición del cliente que el servidor debe cambiar la conexión a TLS utilizando un mecanismo de protocolo específico. (Como ejemplo ATARTTLS para correo y protocolos de noticias), este protocolo es similar al SSL, pero este último ha tenido más desarrollo pero el TLS, fue una propuesta del grupo de trabajo de la IETF.

1.5.3. Authentication Header AH (RFC 4302), Encapsulation Security Payload ESP (RFC4303)

Los protocolos AH y ESP se detallaran en el capítulo 2, secciones 2.3.1 y 2.3.2.

2. IPV6 (INTERNET PROTOCOL VERSION 6) e IPSEC (INTERNET PROTOCOL SECURITY)

2.1. Definición de IPv6

Como su nombre lo dice, es la versión 6 del protocolo de Internet, la cual remplazará su versión anterior IPv4 (Protocolo de Internet versión 4), IPv6 permitirá a Internet soportar muchos más dispositivos, incrementando en gran cantidad el número de posibles dirección IPv6.

Internet opera transfiriendo datos entre hosts en paquetes que son ruteados a través de la red como lo especifican los protocolos de enrutamiento. Estos paquetes requieren un esquema de direccionamiento, como IPv4 o IPv6, para especificar su origen y destino. Para ejemplificar, es necesario tener en cuenta, la dirección de cada una de las casas en una ciudad, que permiten llegar a ellas exactamente, igual sucede con las direcciones IP, se debe conocer a cuál dirección IP debe ir los diferentes paquetes enviados. Cada equipo, bien sea un computador o un dispositivo final que tenga acceso a la red debe tener una dirección IP para poderse comunicar.

El crecimiento de Internet ha creado una necesidad de generar más direcciones, lo cual es posible con IPv6, que permite 128 bits contra una dirección Ipv4 que permite 32 bits, por lo tanto tienen 2^128 posibles direcciones. Ipv6 fue desarrollado por la IETF para hacer frente al agotamiento de las direcciones Ipv4. Esta expansión se permite acomodar más equipos y usuarios en Internet, también provee mayor flexibilidad en la asignación de direcciones y eficiencia para el tráfico de ruteo. También, elimina la necesidad primaria para la traducción de direcciones de red (NAT), que ha ganado amplio despliegue como un esfuerzo para aliviar el agotamiento de IPv4.

IPv6 (a partir del 2012), al igual que el más frecuente utilizado IPv4, es un protocolo de capa de conexión en red de conmutación de paquetes y proporciona de extremo a extremo la transmisión de datagramas IP a través de redes múltiples. Esta descrito en el documento de Internet Estándar RFC 2460, publicado en diciembre del 2008. En adición de ofrecer más direcciones, IPv6 también implementa mejoras no presentes en IPv4. El simplifica aspectos en la asignación de direcciones, remuneración de la red y anuncios del router cuando se cambia el proveedor de servicios. El tamaño de la subred de IPv6, ha sido estandarizado, arreglando el tamaño de la porción del identificador del host de una dirección a 64 bits, para facilitar un mecanismo automático para formar el identificador de host en la capa de enlace de los medios de comunicación que abordan la información. Seguridad de la red es también integrada dentro de la arquitectura de IPv6, incluyendo en él la opción de IPsec.

2.1.1. Aspectos de seguridad de IPv6

El protocolo Ipv4 fue creado para intercambiar información y no tiene características reales de seguridad, pero esto no lo limita para ser usado en entidades que necesitan un nivel alto de seguridad.

El fin que debe cumplir la seguridad para telecomunicaciones se puede resumir o describir en tres diferentes temas:

Integridad: Al transmitir información entre un emisor y un receptor debe existir una forma de hallar confiablemente que esta información no fue alterada en el camino, esto es lo que hace la integridad, garantizar que los datos no son alterados en el camino.

Confidencialidad: Que los datos transmitidos solo se utilicen o tengan permiso para utilizarlos el o los destinatarios.

Autenticación: Verificar que los datos enviados vengan del destino que los envió y no de otro destino y que los datos enviados vengan tal y como fueron enviados.

La encripción y utilización de llaves son claves para la integridad y autenticación, también permite la validación del origen de los datos. En cualquier tipo de seguridad surge el gran inconveniente ¿cómo crearla?, y más cuando se envía información por diferentes lugares desconocidos donde pueden encontrarse con sniffers y no ser detectados. Se tienen mecanismos de encriptación y firmas digitales pero no es suficiente para la seguridad, ya que se generan grandes vacíos y posibilidades de que la información sea robada, modificada o perdida

Algunos ataques como intercepción de datos, donde personas no autorizadas acceden y hacen modificaciones en ellas, no son los únicos que se deben tener en cuenta para el tráfico IP, existen otros factores que debe ver y tomar acciones la seguridad en el protocolo IP:

- Ataques DOS (Denial of Service): Esta forma de ataque es cuando la red se llena de información no importante o que no es de la entidad y esto puede bloquear la red, el servidor de correo o el acceso a sus archivos en red.

- Ataques de Spoofing: Cuando el mensaje lleva una identidad diferente a la original, o suplanta la entidad.

Por medio de las llaves se podría mejorar esto temas de ataque pero existen dificultades para su manejo y para poder autenticarse y verificar se requiere de estas llaves en la arquitectura de la seguridad IP. por lo tanto se debe definir una manera segura para la administración y utilización de estas llaves.

2.2. Definición de IPsec

Internet protocol Security (IPsec o Protocolo de seguridad en Internet), es un conjunto de herramientas para la seguridad de la comunicación del protocolo de Internet (IP), usando la Autenticación y encriptación para cada paquete IP de las sesiones de comunicación. IPsec también incluye protocolos para estabilizar la autenticación mutua entre agentes en el principio de la sesión y negociación de las llaves criptográficas que se usaran durante la sesión.

IPsec es un esquema de seguridad de extremo a extremo que opera en la capa de Internet del conjunto de protocolos de Internet. El puede ser usado en protección del flujo de datos entre dos hosts, entre un par de puertas de enlaces de seguridad o entre una puerta de seguridad y un host. IPsec protege cualquier tráfico de aplicaciones a través de la red IP.

IPsec originalmente fue desarrollado por el laboratorio de investigación naval como parte de DARPA - proyecto de investigación patrocinado. Según lo visto anteriormente ESP y AH son protocolos directos de IPsec. ESP fue derivado directamente del protocolo SP3D, y este se deriva del ISO Network-Layer protocolo de seguridad (NLSP). La especificación del protocolo SP3D fue publicada por NIST, pero desarrollada por el proyecto Secure Data Network System de la agencia nacional de seguridad (NSA), AH es derivado en parte por los anteriores estándares del IETF trabajan para la autenticación del Simple Network Management Protocol.

IPsec es oficialmente especificado por IETF en una serie de documento que aborda comentarios de los diversos componentes y extensiones, esto específica el nombre puesto al protocolo IPsec.

¿Cómo trabaja IPsec?

Este protocolo da seguridad entre dos equipos conectados, por un túnel se conocen los paquetes que se pueden o no enviar, qué parámetros intervienen para dar seguridad a los paquetes enviados. Así, cuando un equipo que tiene instalado IPsec reconoce cuando se envía un paquete y la importancia de este paquete, entonces lo maneja y configura para enviar a través del túnel. Estos túneles cuentan con SA que son dadas entre ambos puntos. El IPsec administra el trafico que se necesita sea seguro, donde se configura la lista de acceso y se aplica la lista a la interfaz, utilizando mapas criptográficos.

2.2.1. Funcionalidad y combinación

La Asociación de seguridad (SA), ofrece un grupo de servicios de seguridad, los cuales depende del protocolo de seguridad que se vaya a utilizar, del modo, el punto terminal y los servicios adicionales seleccionados dentro del protocolo.

El anti-replay es uno de los servicios ofrecidos por AH, que permite la integridad de secuencia parcial. Si no se requiere confidencialidad, AH es el protocolo apropiado para este servicio. Para algunos contextos AH proporciona Autenticación para partes de la cabecera IP.

El tráfico y su confidencialidad, la presta opcionalmente ESP (su fuerza se determina según el algoritmo de encriptación que se usa), la autenticación también es una opción. Al usar autenticación en una SA con ESP se puede definir si se usa un anti-replay como en la autenticación, en ese caso tiene y ofrece un alcance en autenticación mucho mayor que el de AH. Para ESP se tienen autenticación y confidencialidad ambas opcionales, pero siempre debe tenerse en cuenta por lo menos una de las dos.

Combinación

Tanto AH como ESP sirven para dar protección a los datagramas transferidos, pero para una SA individual se debe usar uno de ellos y no los dos.

Por políticas de seguridad se puede requerir una combinación de servicios, en cierto flujo particular de datos, pero esto no es posible con una SA. Esto se puede corregir o hacer instaurando diferentes SA para usar la política de seguridad requerida. SA bundle se le llama a la secuencia de AS, por medio de la cual se procesa el tráfico para cumplir con las políticas de seguridad.

Existen dos formas de SA Bundle:

- Entunelamiento repetitivo.
- Transporte adyacente.

Entunelado repetitivo: Usando Entunelamiento Ip se usa diferentes capas de protocolos de seguridad, por lo tanto se logra gran cantidad de niveles de almacenamiento. En el transcurso de la ruta los túneles se originan o termina en nodos diferentes. El Entunelado se divide en tres diferentes tipos:

Misma terminación de las SA: Los túneles correspondientes pueden hacerse con AH o ESP.

La SA es la misma para una terminación: los túneles pueden ser o AH o ESP. En las terminaciones ninguna es igual.

Transporte Adyacente: Sin necesidad de usar Entunelado, a un mismo datagrama se le aplican más de un protocolo de seguridad. Al combinar de esta manera AH y ESP solo da un nivel de combinación.

2.2.2. Bases de datos y Servicios

Para procesar el tráfico en IPsec se tienen dos bases de datos:

SPD (Base de datos de políticas de seguridad)
SAD (Base de datos de asociación de seguridad)

Todo el tráfico IP que entre o salga de un host o puerta de enlace segura, las políticas para decidir su tratamiento los hacen la SPD y la SAD para la SA tiene sus parámetros asociados.

SPD (Base de datos de políticas de seguridad)

Los datagramas IPs son una base de datos que almacena servicios a ofrecer y su modalidad. No se especifican ni la interfaz ni forma. Debe existir una interfaz de administración para así por medio de un administrado pueda dar manejo a la SPD, esto para la implementación de IPsec.

La SPD define la acción que se debe llevar a cabo cuando se tienen paquetes de entrada y salida que IPsec vaya a tratar.

Selectores

Existen diferentes parámetros selectores que soporta el manejo de las SA, esto facilitan el control de la granularidad de las SA:

- Dirección IP origen
- Dirección IP destino
- Nivel de sensibilidad de datos
- Nombres, puede ser el nombre de usuario o el nombre del sistema
- Puertos a ser usados para origen y destino
- Protocolo capa de transporte.

SAD (Base de datos de asociación de seguridad)

La SA debe pasar por la SAD para definir los parámetros que se asocian a la SA. Para el procesamiento de IPsec se usan los siguientes campos de las SAD:

- Desbordamiento del contador de secuencia.
- Ventana anti replay
- Contador de números de secuencia
- Algoritmos de encriptación ESP, IV mode, claves, IV
- Algoritmo de autenticación AH, claves
- Tiempo de vida

- Modo del protocolo IPsec

Existen diferentes parámetros en una negociación de una SA, en ambos protocolos AH y ESP:

Ventana anti replay: Este parámetro es activado cuando IPsec encuentra paquetes reenviados por host no confiables, se usa para los paquetes de entrada.

Numero de secuencia: Es un campo que va aumentado desde 0, cada que se utiliza la SA, este permite detectar ataques de replay.

Sobre flujo del número de secuencia: Al detectar un sobre flujo del campo anterior se establece este campo, donde quien determina que hacer si el campo está activado es la política de seguridad.

Modo: Existen tres: Túnel, transporte o indistinto, si es el caso del último puede ser cualquiera de los dos anteriores.

Tiempo de vida: Por medio de Bytes asegurados se define el tiempo que va a durar la SA, no es recomendable enviar paquetes que sumen 4G usando la misma SA. Software y hardware son los limites encargados de negociar una nueva sesión cuando esta se va a terminar (software) o terminar la sesión (hardware).

Parámetros PMTU (protocolo máximum transfer unit): IPsec agrega un encabezado y eso afecta la longitud del PMTU, esto no implica que se fragmenten o re ensamblen paquetes. IPsec debe poder interactuar para determina la PMTU. La SA tiene constantes dos valores: campo de edad y PMTU.

Destino túnel: se usa solo para el modo túnel, para el encabezado exterior muestra la dirección IP de destino.

SERVICIOS

Para la capa IP se ofrecen diferentes servicios de seguridad estos son ofrecidos por IPsec, a su vez estos servicios disponen de un sistema el cual selecciona protocolos de seguridad necesarios, determina los algoritmos que se utilizaran en los servicios y para cumplir con los servicios solicitados colocar las llaves criptográficas necesarias. Para proveer seguridad se manejan dos protocolos, una para autenticación y otro combinado el primero va ligado al protocolo AH y el segundo al protocolo ESP.

A continuación se conocerá los servicios proporcionados:

- Integridad sin conexión.

- Control de acceso
- Autentificación de origen.
- Confidencialidad.
- Rechazo de paquetes retocados
- Confidencialidad limitada por flujo de trafico

	AH	ESP (sólo encriptación)	ESP (encriptación más autentificación)
Control en el acceso	√	√	√
Integridad sin conexión	√		√
Autentificación de origen	√		√
Rechazo de paquetes retocados	√	√	√
Confidencialidad		√	√
Confidencialidad limitada por el flujo del tráfico		√	√

Tabla 3: Servicios prestados por IPsec según el algoritmo. [1][9]

2.2.3. Componentes de IPsec

SPWG (Security Protocol Working Group), este grupo pertenece a la IETF, y fueron los encargados del desarrollo de la especificación completa de IPsec, de done obtuvieron 7 componentes:

Carga útil de seguridad de encapsulación: ESP: A los paquetes que se envían les define un formato y al usar ESP para encriptar los paquetes da las definiciones generales para esto, opcional da la autenticación.

Arquitectura: Mecanismos característicos de la tecnología IPsec, requisitos de seguridad y definiciones son establecidos por estos componentes, estos son conceptos generales.

Cabecera de autenticación AH: Como ESP a los paquetes que se envíen le define un formato y al usar AH para encriptar los paquetes da las definiciones generales para esto.

Algoritmo de autenticación: El uso de AH y la opción de autenticación de ESP son descritos en estos documentos.

[9] [1] SEGURIDAD EN IP CON EL PROTOCOLO IPSEC PARA IPV6, Universidad de San Carlos de Guatemala, Erick Lujan, 2005

Algoritmo de encriptación: Son documentos donde los Algoritmos de encriptación de ESP se describen.

Administración de llaves: Los esquemas para la administración de las llaves se encuentran en estos documentos.

Dominio de interceptación DOI: Para documentos que manejan algún tipo de relación este componente almacena parámetros necesarios para esto. Entre estos parámetros se encuentran identificadores para algoritmos de autenticación y encriptamiento aprobados.

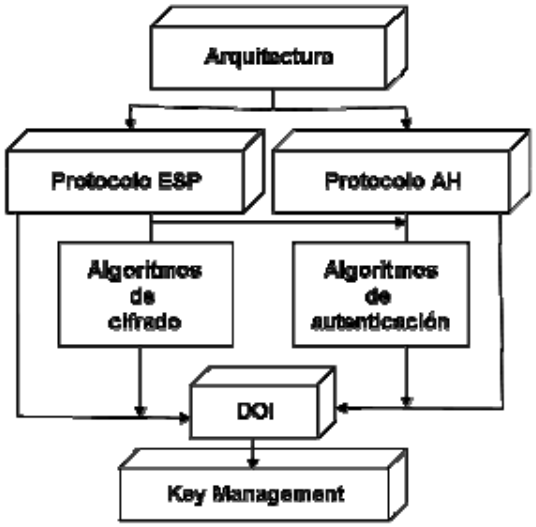

Figura 10: Diagrama de los componentes de IPsec [1][10].

2.2.4. Funcionamiento

Antes de empezar la transmisión de los datos, el nivel de seguridad es negociado por un equipo abalado para IPsec, este debe permanecer durante toda la sesión. En el transcurso de esta negociación, se definen algunos métodos como: Autenticación, método túnel (este puede ser opcional), método de hash y un método de cifrado (este también puede ser opcional). Con la información que se intercambia en la negociación se definen las claves secretas de autenticación que usara cada equipo. Estas claves nunca serán transmitidas, después de crear la clave, se autentican y se puede empezar una transmisión segura.

Se puede definir el nivel de seguridad en alto o bajo, dependiendo lo que diga las directivas IP de los equipos destino u origen.

[10] [1] SEGURIDAD EN IP CON EL PROTOCOLO IPSEC PARA IPV6, Universidad de San Carlos de Guatemala, Erick Lujan, 2005

2.2.4.1. PKI e integración con IPsec

PKI (infraestructura de clave pública), en una comunidad de usuarios se requiere de emitir, revocar, y renovar certificaciones digitales, esto es permitido por elementos y procedimientos administrativos los cuales están agrupados con el nombre de PKI.

PKI debe velar por la seguridad en las transacciones electrónicas valiéndose de los entornos de claves propio y la eficiente gestión de certificados confiables, esto permite cumplir con las garantías de autenticación, confidencialidad y no repudiación.

Al ser implementado da la opción de manejar los siguientes servicios:

- Servicios de Certificación
- Servicios de certificación temporal y timbre digital
- Tener variedad y compatibilidad de solución de encriptación
- En la implementación de los proyectos que se presenten problemas asesora y apoya para dar solución a ellos.

Componentes principales de PKI

Para lograr una organización coherente en los PKI, se deben interrelacionar las principales características de los distintos elementos enunciados a continuación:

- Autoridad de certificación
- Certificación digital y lista de renovación
- Pares de claves matemáticamente relacionadas.

La estructura formal dentro de la cual se desarrollar estos elementos se determina por:

- Políticas de certificación.
- Manuales de procedimientos.

La autoridad de certificación es aquel que todos los demás usuarios fueron reconocidos como certificador de identidades digitales de todos. Este se encarga de emitir los certificados, después de evaluarlos por medio de las políticas de certificación. Debe ser muy confiable, ésto lo logra por medio de una seria y exitosa gestión.

Su principal función es pedir las certificaciones necesarias para verificar la identidad de los solicitantes.

Algunas maneras para encontrar o saber quiénes son estas autoridades certificadoras:

- Por persona: en el certificado no se coloca su nombre como persona física o entidad.
- Por organización: Se certifican personas que pertenezcan a una organización.
- Por residencia: Certifica por medio de una dirección geográfica.

Las políticas de certificación y los manuales de procedimientos son los encargados del funcionamiento general de PKI, esto lo hacen por medio de la definición de asuntos tales como: la certificación a ser emitida por la autoridad de certificación, hasta dónde puede llegar o que puede cubrir la información plasmada en el certificado, pasos para registrarse, hasta dónde puede llegar el compromiso y tipo de compromiso que tenga la AC para los usuarios y en sentido contrario, los límites del certificado, etc.

Combinación de IPsec con PKI

Al tener una gran cantidad de nodos comunicándose mediante IPsec, cada uno de ellos se deben autenticar de una manera fiable y esta autenticación e posible implementando las PKI en IPsec.

Los nodos IPsec son los encargados de los certificados en IPsec y el fin de estos certificados es tener un camino confiable para autenticar el nombre de cada dispositivo.

Un certificado digital estará dispuesto para cada uno de los equipos de IPsec y este tendrá la clave pública y toda la información necesaria para reconocer el dispositivo. La autoridad de certificación debe avalar o permitir por medio de su firma la unión entre la clave pública y la identidad. Los equipos IPsec tendrán conocimiento sobre el CA y deben tener una copia del certificado de la CA

Dentro de los protocolos de IPsec no se especifican los protocolos para la interacción de los dispositivos IPsec con PKI. El formato X.509v3 y el estándar PKCS son usados por los fabricantes como formato común de los certificados y para la solicitud y descarga de los mismos. Pero no hay un estándar para que los dispositivos Ip dialoguen con la PKI.

Por lo tanto dependiendo del fabricante pueden existir una gran variedad de posibilidades, se necesitan de algunas operaciones con la PKI, por parte de los nodos IPsec, tales como: Tener el certificado del CA, Pedir y bajar un certificado y también validar certificaciones recibidas.

En el directorio que maneja la PKI se almacenan una lista de certificados revocados, es en esta lista donde los nodos IPsec verifican los certificados. Los nodos obtienen esto manteniendo una copia de la CRL, la cual está en constante actualización haciendo una consulta LDAP en el directorio de la PKI. Los tiempos de actualización de estos registro pueden tardar horas, luego este proceso puede tardar un tiempo para que los nodos estén enterados de los cambios y certificados revocados.

SCEP es un protocolo que permite la descarga y solicitud de certificados, Este protocolo ha sido diseñado por Cisco Systems Inc. Y VeriSign y está basado en intercambiar mensajes PKCS, por medio del protocolo HTTP, esto permite que los procesos de solicitud y descarga de certificados sean automáticos.

2.2.4.2. Modos de uso en intranet y extranet

Para la capa IP IPsec permite generar soluciones de comunicaciones que brinda confidencialidad y autenticación sin importa el medio que se use para el transporte (FR, PPP, xDSL o ATM). Al adicionar seguridad a la capa IP existe una ventaja que esta solución se amplía universalmente, garantizando un nivel de seguridad homogéneo sin importar el tipo que sean las aplicaciones, lo que importan es que su base sea IP.

Los tres escenarios siguientes son los cuales IPsec les proporciona una buena solución:

1. Intranet
2. Accesos remotos
3. Extranet

Intranet

Red interna o red local, es la interconexión de diferentes dispositivos en una empresa u organización utilizando un medio común IP.

IP es un medio de transporte universal el cual es usado por diferentes compañías para la transmisión de sus datos, existen algunas que aún no usan IP pero el objetivo es migrar todo a IP. De la misma manera esto hace que las compañías estén intercomunicadas entre sí con sus sucursales.

Para cualquier compañía por muy pequeña que sea hasta la más grande es importante su información o datos manejados dentro de ella, luego la seguridad es un papel vital para estas redes, para cubrir esta seguridad confiable e integra se usa el IPsec.

Así la entidad que tenga su red local tenga infraestructura informática a la cual sale muy costoso adicionarle mecanismos de seguridad, su solución puede ser la adición de un Gateway IPsec el cual por medio de su infraestructura IP logra dar una excelente seguridad.

Accesos remotos

La gran mayoría de compañías, que tienen personal por fuera de sus oficinas pero información en sus bases de datos necesitan da permiso de acceso a estos datos a sus empleados, lo cual lo hacen por medio de acceso remoto sin importar en qué lugar del mundo se encuentren.

Este acceso remoto se puede hacer instalando un software en el equipo remoto y por medio de este se puede acceder a la información de la compañía de forma segura y transparente como si se estuviese en la oficina, esto permite:

- Revisar el correo electrónico
- Revisar información compartida en la red
- Revisar el servidor web corporativo
- Tener presente su agenda de negocios.

Una de las técnicas actualmente adoptadas por muchas compañías es tener personal trabajando desde su casa, o que el personal tenga acceso a la red corporativa sin tener que estar dentro de la compañía.

Debido a la alta vulnerabilidad que se puede tener al tener estos accesos remotos y la información que se va a manejar se deben soportar o aplicar solución que sean muy seguras.

IPsec puede dar esta seguridad implementando en el dispositivo del empleado un software que se encarga de la conexión segura con los datos de la compañía. Este software es compatible con todos los sistemas operativos pues vienen ya incluidos en su desarrollo.

Para equipos que no integran en su sistema operativo la solución de IPsec existen aplicaciones comerciales o de libre acceso para que sean instaladas y utilizadas desde estos terminales.

Para dar más soporte a la seguridad de IPsec se puede utilizar mecanismo conocidos como contrafuegos y autenticación fuerte mediante certificados digitales.

Extranet

Red externa, esta red es la cual une a una compañía con sus distribuidores o compañías aliadas a ellos, es una red donde se debe salir de su entorno normal para ubicar otras empresas colaboradoras.

Sin importar que equipos tenga cada una de las compañías interconectadas en la extranet, ellas se podrán comunicar en la parte de seguridad bajo un mismo lenguaje el de IPsec.

Las extranet han aparecido para compañías que manejen los mismos productos a que tengan temas entre sus productos que se relacionen de alguna manera, todo esto debe tener una seguridad muy alta para que la información compartida entre ellas no sea tomada y utilizada.

IPsec así como en las dos opciones anteriores es una solución de seguridad muy completa ya que por sus protocolos permite que las conexiones entre las compañías sean lo más seguras posibles y que la información que se vaya a transmitir sea confiable y llegue a su destino final.

2.3. Seguridad del protocolo IPsec en IPv6

2.3.1. Authentication Header (AH, RFC4302)

Es un miembro del protocolo IPsec. Este protocolo garantiza la integridad de la conectividad y autenticación del origen de los datos para los paquetes Ip. Además, opcionalmente puede proteger contra los ataques de repetición usando la técnica de la ventana deslizante y descartando paquetes viejos.
Para IPv4 el AH protege la carga Ip y todos los campos de la cabecera del datagrama, exceptuando los campos mutables. Los campos de cabecera en IPv4 son: DSCP/TOS, ECN, Banderas, compensación de fragmentos, TTL y una cabecera de control.
Para IPv6 AH protege la gran cantidad de IPv6, Cabecera base, AH el mismo, cabecera de extensión no mutable después de AH, y la carga IP. Protección para la cabecera de IPv6 excluye las celdas mutables: DSCP, ECN, nivel de flujo, y limite hop.

Ah opera directamente in la parte superior de IP, usando el número de protocolo IP 51.

La siguiente tabla muestra como el paquete AH es construido e interpretado.

***Authentication Header* format**

Offsets	**Octet 16**	**0**								**1**								**2**								**3**							
Octet 16	**Bit 10**	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**	**21**	**22**	**23**	**24**	**25**	**26**	**27**	**28**	**29**	**30**	**31**
0	**0**	*Next Header*								*Payload Len*								*Reserved*															
4	**32**	*Security Parameters Index (SPI)*																															
8	**64**	*Sequence Number*																															
C	**96**	*Integrity Check Value (ICV)*																															
...	**...**	…																															

Tabla 4: Construcción del paquete AH [3][11]

Next Header (8bits): Esta cabecera indica que protocolo de capa superior estaba protegiendo. El valor se obtiene de la lista de números de protocolos Ip.

Payload Len (8bits): El tamaño de este AH en unidades de 4 octetos, luego un valor de 0 equivale a 8 octetos, un valor de 1 equivale a 12 octetos. Aunque el tamaño se mide en unidades de 4 octetos, la longitud de esta cabecera debe ser un múltiplo de 8 octetos, si se envía en un paquete de IPv6. Esta restricción no aplica para AH en IPv4.

[11] [3] http://en.wikipedia.org/wiki/IPsec Visitada el 16-6-2012 a las 12:56 p.m.

Reserved (16 bits): Reservado para el futuro (se llena de seros mientras tanto).

Security Parameter Index (32 bits): Valor arbitrario el cual es usado (en conjunto con la dirección IP de destino) para identificar la asociación de seguridad de la parte receptora.

Sequence number (32 bits): Una monótona sucesión estrictamente creciente en número (incrementada en 1 por cada paquete enviado) para prevenir ataques repetitivos. Cuando la detección de repetición está habilitada, números de secuencia no son reutilizados, ya que se debería volver a renegociar una asociación de seguridad antes de un intento de incrementar el número de secuencia más allá de su valor máximo.

Integrity Check Value (múltiplo de 32 bits): El valor de comprobación es de longitud variable, puede contener el relleno para alinear el campo en un límite de 8 octetos para IPv6 o un límite de 4 octetos para IPv4.

Ventaja
Al usar AH en el modo transporte se genera un bajo costo de procesamiento.

Desventaja
No se autentican aquellos campos del Header IP que se cambian en el camino.

2.3.2. Encapsulating Security Payload (ESP, RFC4303)

Así como AH es un miembro del paquete IPsec. Dentro de IPsec provee origen de autenticación, Integridad y confidencialidad en la protección de paquetes. También soporta configuración solo de encriptación y autenticación, pero el uso de encriptación sin autenticación no es aconsejado porque es muy inseguro. A diferencia de la cabecera AH ESP en modo transporte no proporciona integridad y autenticación para paquetes Ip original. Sin embargo, en modo túnel, en todo el paquete IP original se encapsula con un encabezado de un paquete nuevo adicionado. La protección de ESP es ofrecida a toda la parte interior del paquete IP, mientras que la cabecera exterior se mantiene desprotegida ESP opera directamente en el tope de IP, usando el número de protocolo IP 50.

La siguiente tabla muestra como el paquete AH es construido e interpretado:

Encapsulating Security Payload format

Offsets	Octet$_{16}$	0								1								2								3							
Octet$_{16}$	Bit$_{10}$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	*Security Parameters Index (SPI)*																															
4	32	*Sequence Number*																															
8	64	*Payload data*																															
...	...																																
...	...									*Padding (0-255 octets)*																							
...	...																																
...	...																	*Pad Length*								*Next Header*							
...	...	*Integrity Check Value (ICV)*																															
...	...	...																															

Tabla 5: Construcción e interpretación del paquete ESP [3][12]

Security Parametrs Index (32 bits): Se usa un valor arbitrario (en conjunto con dirección Ip de destino) para identificar la asociación de seguridad de la parte que recibe.

Sequence Number (32 bits): Una monótona secuencia de un número creciente (incrementado por 1 para cada paquete enviado) para proteger contra ataques repetitivos. Hay un contador separado mantenido para toda asociación de seguridad.

Payload data (variable): Los contenidos protegidos del paquete IP original, incluyendo todos los datos utilizados para proteger el contenido. El tipo de contenido que fue protegido es indicado por la celda de la siguiente cabecera.

Padding (0-255 octetos): Relleno para encriptación, para extender el Payload data a un tamaño que case la encriptación de tamaño de bloque de cifrado y para alinear la siguiente celda.

Pad Length (8bits): Tamaño del relleno (en octetos).

Next Header (8 bits): Tipo del siguiente encabezado, el valor es tomado de la lista de números de protocolos IP.

Integrity Check Value (múltiplo de 32 bits): Valor de chequeo con tamaño variable. Él puede contener relleno para alinear la celda a 8 octetos límites para IPv6 o 4 octetos límites para IPv4.

[12] [3] http://en.wikipedia.org/wiki/IPsec Visitada el 16-6-2012 a las 12:56 p.m.

Ventajas
Al igual que AH, genera un leve costo de procesamiento

Desventaja
No se genera autenticación ni encriptación en el modo transporte.

2.4. Metodología de IPsec para IPv6

Existen varias formas o maneras de aplicar IPsec en IPv6, algunas de ellas son las siguientes:

- Redes privadas virtuales.
- Road Warrior
- Seguridad extremo-extremo.

Redes privadas virtuales (VPN)

Esta tecnología permite ampliar la red local montándose en una red pública. Para entenderlo a mejor manera se puede decir que teniendo la red de una empresa por medio de una VPN se puede tener acceso a los archivos de la red estando fuera de ella. Su mismo nombre lo dice es una red privada pero no es real es virtual o en la red y solo las personas autorizadas tienen permiso a ellas.

Para esto se necesita tener una muy buena seguridad para poder autenticarse y que la información sea integra. Todo esto se puede llevar a cabo por medio de IPsec para garantizar la mejor seguridad.

Al implementar y configurar bien el IPsec en estas redes se disminuye el valor de la transferencia de los datos entre dos lugares.

Road Warrior

Traducido al español es el guerrero de la calle, esto se refiere a las empresas que tienen trabajadores fuera de las oficinas y necesitan tener acceso a los datos de la red corporativa.

Se puede usar IPsec para la seguridad y transmisión de estos datos manteniendo la privacidad de los mismos.

Seguridad Extremo-extremo

Este método genera un túnel entre cada uno de los host que estén en la red, es decir que existirán n cantidad de túneles dependiendo del diagrama topológico de la red y al hacer esto los costos de implementación se elevarían.

Este no es un método viable para compañías pues al tener tantos host se deberían hacer muchos túneles.

Este método es muy seguro debido a que mantiene un buen control sobre la máquina que requiere seguridad.

2.5. Modos de operación de IPsec

IPsec consta de dos modos de operación, los cuales se describen a continuación:

- Transporte
- Túnel

2.5.1. Transporte

En este modo los datos transferidos son los únicos que se cifran o autentican, al no cifrar ni modificar la cabecera IP el enrutamiento se mantiene sin cambios, pero al utilizar AH las direcciones no se puede traducir, puesto que si se hiciera no se utilizaría el hash. El hash asegura siempre las capas de aplicación y transporte, por ende no se pueden modificar.

Este modo se utiliza para transmisiones de un computador a otro.

2.5.2. Túnel

En este modo tanto la cabecera como los datos son cifrados o autenticados. Para que el enrutamiento logre funcionar al hacer esto se debe encapsular en un nuevo paquete IP.

Este modo se usa para las transmisiones entre redes o también de red a computador o de computador a computador pasando por Internet.

Mejor modo

No se encontró una respuesta a cuál de los dos modos es mejor pero a criterio personal cada modo se usa dependiendo de la seguridad o nivel que se requiera, y se hace más seguro cifrar y autenticar la totalidad de los datos, por lo tanto se puede decir es más seguro el modo túnel.

2.6. IKE (Internet Key Exchange (RFC2409)

Este protocolo permite establecer una SA en el protocolo de IPsec. IKE está basado en los protocolos Oakley e ISAKMP. IKE trabaja con X.509 certificados para la autenticación los cuales son pre-compartidos o distribuidos usando los DNS y Diffie-Helman Key Exchange para establecer una sesión secreta compartida a partir de la cual se deriva las llaves de criptografía.

La mayoría de implementaciones de IPsec consisten en un IKE daemon que funciona en el espacio del usuario y una pila IPsec en el kernel que procesa los paquetes IP actuales.

Fases de IKE

Este se puede dividir en dos fases:

La primera fase permite establecer una comunicación de autenticación segura utilizando el algoritmo de intercambio de llave Diffie-Hellman, el cual genera una llave compartida, esta llave es secreta y se usa para futuras comunicaciones IKE.

Al usar llaves pre compartidas, firmas o llaves públicas en la encriptación se puede dar la autenticación. Esta fase opera en ambos modos túnel y transporte.

La segunda fase los pares utilizan el canal establecido en la fase uno este canal es seguro, por medio de este canal es negociada la SA en favor a otros servicios como IPsec. Esta fase solo opera en un modo rápido.

IKE es la versión más actualizada del protocolo ISAKMP.

IKEv2 (RFC 5996, se puede encontrar mayor información de este RFC en el capítulo 3)

Esta es una nueva versión del IKE estipulada en diciembre del 2005.

Una forma de explicación podría ser:

Se tienen dos equipos ambos equipos tienen sus propios parámetros de seguridad.

Si el segundo equipo está recibiendo gran cantidad de conexiones IKE, el equipo 2 le enviara un mensaje de respuesta desencriptado del IKE_sa_init con un mensaje de notificación de valor cookie en una carga de notificación. Esto garantiza que el equipo 1 es capaz de entender una respuesta del equipo 2.

2.7. Host to host IPsec

IPsec puede ser configurado para conectar un computador de escritorio o puesto de trabajo a otro por una comunicación de host to host. Este tipo de conexión usa la red a la cual cada equipo está conectado para crear un túnel seguro entre ambos. Esta conexión maneja pocos requerimientos, tal como la configuración de IPsec en cada host. El host solo necesita un canal dedicado para atraer la red y un sistema operativo para crear la conexión IPsec.

Para una conexión Host to Host se requiere de la siguiente información:

- La dirección IP de cada uno de los equipos o host.
- Un único nombre para identificarlos la conexión IPsec y distinguirla de otros dispositivos o conexiones.
- Una llave de encriptación o una generada automáticamente.
- Una llave de autenticación pre compartida que es usada para iniciar la conexión y el intercambio de llaves de encriptación durante la sesión.

3. GUIA BASICA DE CONFIGURACION IPSEC EN AMBIENTES IPV6

La configuración de IPsec en ambientes IPv6 que se describe a continuación sirve para cualquier sistema operativo de red, en este caso se hará basado en Cisco Systems Inc., lo único que cambia en otros sistemas operativos serían los comandos, pero la implementación es totalmente transparente y la misma para todos.

En el capitulo anterior se observo que IPsec es un componente obligatorio en Ipv6, debido a que Ipv6 se definió con un protocolo de seguridad que no trae su antecesor Ipv4 desde sus inicios, pero este protocolo de seguridad debe ser configurado para su buen funcionamiento. IPsec para Ipv6 en modo túnel y encapsulación se utiliza para la protección de tráfico unicast y multicast.

Esta guía se nombra a modo de ejemplo para configuración de IPsec en IPv6.

3.1. Requerimientos para la configuración de IPsec para la seguridad de IPv6

Se debe conocer algunos puntos básicos para poder entender la configuración de IPsec, estos se nombran a continuación:

- Se debe tener conocimientos de IPv4
- Se debe tener conocimeinto sobre la configuración básica y el direccionamiento en IPv6.

3.2. Información sobre la configuración de IPsec para la seguridad de IPv6.

A continuación se hace un pequeño resumen de la información relevante o importante para poder implementar de la mejor manera el protocolo IPsec, este resumen consta de los siguientes items:

- OSPF para la autenticación IPv6 con IPsec
- IPsec para IPv6

3.2.1. OSPF para la autenticación IPv6 con IPsec

Los paquetes OSPF para IPv6 deben ser autenticados, esto con el fin de que esto paquetes no sean alterados o reenviados al router, causando que este funcione de una manera diferente a la cual fue configurado. IPsec es usado por OSPF para IPv6, el cuál funciona como una interfaz de programa de aplicación segura (API) donde adiciona autenticación para los paquetes OSPF. Y esta aplicación fue creada para darle soporte a IPv6.

Para habilitar la autenticación en OSPF para IPv6 se requiere de IPsec, para usar autenticación se necesitan de imágenes criptológicas, ya que solo ellas incluyen el API de IPsec necesario para el uso de OSPF.

Las celdas de autenticación de OSPF para IPv6 se dejaron de usar en las cabeceras de OSPF. Se debe garantizar la integridad, autenticación y confidencialidad de los intercambios de enrutamiento al correr OSPF en IPV6, esto se logra basándose o utilizando los encabezados de (AH) y (ESP). Estas extensiones de cabecera pueden ser usadas para garantizar autenticación y confidencialidad a OSPF para IPv6.

En diferentes ocasiones se configura una pólica de seguridad al implementar IPsec, esta política es una combinación del índice de la política de seguridad (SPI) y la llave (genera y valida el valor de message digest [MD5]). Tanto en el área OSPF como en una interfaz puede ser configurado IPsec. Para cada interfaz que se configura con IPsec se define una política diferente para tener una mayor seguridad. Configurando IPsec en un área de OSPF la política se aplica a toda el área, sin incluir la interfaz que estén directamente configuradas con IPsec. Al implementar IPsec en OSPF este es transparente para la persona que lo usa.

3.2.2. IPsec para IPv6

Como se comentó en el capítulo 2 IPsec fue creado por la IETF y este provee seguridad a la información enviada en una red desprotegida tal como Internet. IPsec funciona en la capa de red protegiendo y autenticando los paquetes IP que se manejan entre dispositivos IPsec.

La funcionalidad de IPsec es similar en IPv4 e IPv6, pero el modo túnel de lado a lado, solo funciona en IPv6.

Las cabeceras de AH y ESP se utilizan para implementar IPsec en IPv6, donde AH genera o garantiza la integridad y la autenticación del origen, Esta también protege gran parte de las celdas de la cabecera IP y autentica el origen por medio de una firma basada en un algoritmo y la cabecera ESP prevé confidencialidad, autenticación del origen, integridad en la conectividad del interior del paquete, anti-replay y confidencialidad en el límite de bajo tráfico.

3.2.2.1 IPsec protección de Lado a lado usando una interfaz de túnel virtual (VTI)

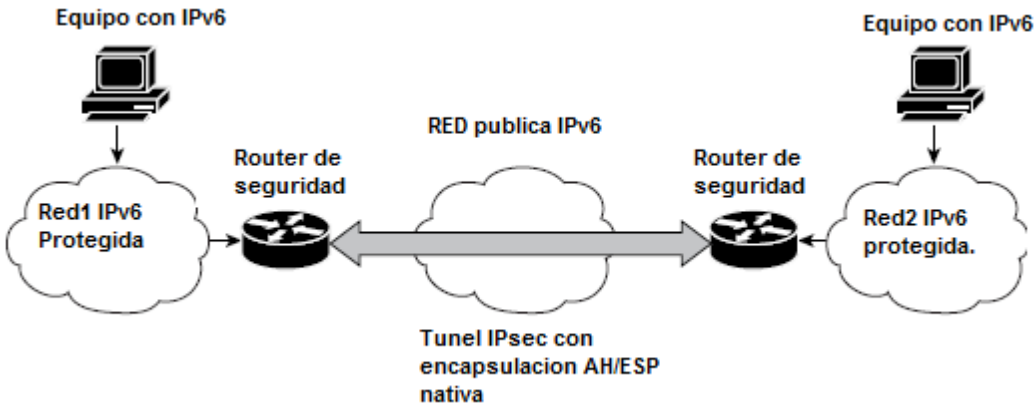

Figura 11: Interfaz de túnel con IPsec[13]

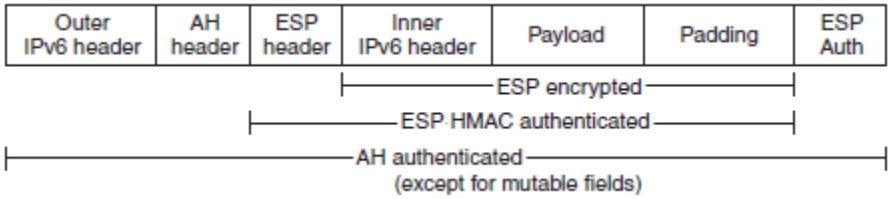

Figura 12: Formato de empaquetamiento para IPv6 usando IPsec.

En la figura se puede observar el diagrama o formato de empaquetamiento que utiliza IPsec para IPv6.

3.3. Como configurar IPsec para la seguridad en IPv6

Para la configuración de IPsec en IPv6 se tocaran los siguientes temas.

- Configuración de una VTI para host-to-host usando la protección de IPsec para IPv6.
- Verificar la configuración del modo túnel de IPsec
- Problemas en la configuración y operación de IPsec para IPv6

[13]Capítulo 3 hasta el 3.3.3, Tomado, traducido y editado de: Implementing IPsec in IPv6 Security, Cisco Systems Inc., 2001-2011, http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-ipsec.pdf

3.3.1. Configuración de una VTI para host-to-host usando IPsec para IPv6.

Para configurar una VTI para host-to-host usando IPsec se requiere de diferentes tareas, citadas a continuación:

- Pasos para crear la política de IKE y pre compartir la llave en IPv6
- Pasos para configurar un conjunto de transformaciones de IPsec (este se refiere al conjunto de algoritmos a utilizar para AH y ESP) y perfil IPsec.
- Pasos para configurar un perfil ISAKMP en IPv6.
- Pasos para configurar un túnel IPsec VTI en IPv6.

3.3.1.1. Crear la política de IKE y pre compartir la llave en IPv6

La negociación IKE debe ser protegida, por lo tanto cada negociación IKE comienza aceptando un par de políticas IKE comunes. Esto garantiza que las negociaciones y envíos posteriores de IKE estén autenticados.

Después de las dos partes aceptan la política, se definen los parámetros para una SA establecida entre cada lado, y esta SA aplica para el tráfico IKE durante la negociación.

En cada par se pueden configurar múltiples políticas prioritarias, cada una con diferente combinación de los valores de los parámetros. Para cada política creada se asigna una única prioridad, esta prioridad puede variar de 1 a 10000 donde uno (1) es la más prioritaria.

A continuación se detallan los pasos que se requieren para la configuración de un router para crear la política IKE y pre compartir la llave en IPv6.

1. enable
2. configure terminal
3. cryptoisakmp policy *priority*
4. authentication{**rsa-sig** | **rsa-encr**| **pre-share**}
5. hash{**sha**| **md5**}
6. group{**1** | **2** | **5**}
7. encryption{**des** | **3des** | **aes**| **aes 192** | **aes 256**}
8. lifetime*seconds*
9. exit
10. cryptoisakmp key *password-type keystring*{**address** *peer-address* [*mask*] | **IPv6**
{*IPv6-address*|*IPv6-prefix*} | **hostname** *hostname*} [**no-xauth**]
11. cryptokeyring*keyring-name* [**vrf***vrf-name*]
12. pre-shared-key {**address** *address*[*mask*] | **hostname** *hostname*| **IPv6** {*IPv6-address* | *IPv6-prefix*}}

Key*key*

La explicación de cada uno de los pasos se detalla a continuación:

Paso 1

Se habilita el router a configurar, después de este comando el router queda habilitado para empezar su programación y se muestra Router#.

Paso 2

Se entra en el modo de configuración global del router, al editar este comando y dar enter el estado del router queda: Router (config)#

Paso 3

Se define la prioridad de la política de IKE se entra al modo de configuración de ISAKMP, en este paso se configura desde 1 en adelante la prioridad de la política de IKE, donde 1 es la prioridad más alta, después de dar enter el router queda dentro del modo de configuración de la política de ISAKMP en el router se ve: Router (config-isakmp-policy)#

Paso 4

En este paso se define el método de autenticación dentro de la política de IKE, rsa-slg y rsa-encr no son soportadas por IPv6, para IPv6 siempre debe ser Pre-share, que es pre compartida, después del enter en el router se ve: Router (config-isakmp-policy)#

Paso 5

Especifica el algoritmo Hash dentro de las políticas de IKE, se tienen dos tipos de algoritmo sha o md5, después de dar enter se mantiene en el modo de configuración de ISAKMP.

Paso 6

Especifica el identificador de grupo Diffie-Helman dentro de las políticas de IKE, este puede ser 1,2 o 5, después de dar enter se mantiene en el modo de configuración de ISAKMP.

Paso 7

Especifica el algoritmo de encriptación dentro de las políticas de IKE, los algoritmos permitidos son: des, 3des, aes, aes 192, aes 256, después de dar enter se mantiene en el modo de configuración de ISAKMP.

Paso 8

Especifica la vida o tiempo que permanecerá una SA. Este valor es opcional. Al dar enter se mantiene en el modo de configuración de ISAKMP.

Paso 9

Se sale del modo de configuración de ISAKMP, pasando al modo de configuración global.

Paso 10

Configura una llave pre compartida de autenticación.

Paso 11

Define diferentes llaves encriptadas las cuales serán usadas durante la autenticación de IKE.

Paso 12

Define una llave pre compartida para ser usada durante la autenticación de IKE.

3.3.1.2. Pasos para configurar un conjunto de transformación de IPsec y un perfil IPsec.

1. enable
2. configure terminal
3. crypto IPsec transform-set *transform-set-name transform1* [*transform2*] [*transform3*]
[*transform4*]
4. cryptoIPsec profile *name*
5. set transform-set *transform-set-name* [*transform-set-name2...transform-set-name6*]

La explicación de cada uno de los pasos se detalla a continuación:

Paso 1

Se habilita el router a configurar, después de este comando el router queda habilitado para empezar su programación y se muestra Router#.

Paso 2

Se entra en el modo de configuración global del router, al editar este comando y dar enter el estado del router queda: Router (config)#

Paso 3

Se define el conjunto de transformación y ubica el router en el modo de configuración de transformación. SE da un nombre l conjutno de transformación y se define el algoritmo de AHy ESP a usar.

Paso 4

Definir los parámetros de IPsec que serán usados para la encriptación de IPsec entre dos routers IPsec.

Paso 5

Específica que conjunto de transformacionespuede ser usada con la entrada del mapa criptográfico.

3.3.1.3 Pasos para configurar un perfil ISAKMP

1. enable
2. configure terminal
3. cryptoisakmp profile *profile-name* [**accounting** *aaalist*]
4. self-identity{**address** | **address IPv6**] | **fqdn**| **user-fqdn***user-fqdn*}
5. match identity {**group** *group-name* | **address** {*address* [*mask*] [*fvrf*] | **IPv6** *IPv6-address*} | **host**
host-name | **host domain** *domain-name* | **user** *user-fqdn* | **user domain** *domain-name*}

La explicación de cada uno de los pasos se detalla a continuación:

Paso 1

Se habilita el router a configurar, después de este comando el router queda habilitado para empezar su programación y se muestra Router#.

Paso 2

Se entra en el modo de configuración global del router, al editar este comando y dar enter el estado del router queda: Router (config)#

Paso 3

Se define un perfil ISAKMP y audita las sesiones de IPsec

Paso 4

Define la identidad que usa la IKE local para identificarse el mismo al equipo remoto.

Paso 5

Coincide con una identidad de un par remoto, en un perfil ISAKMP

3.3.1.4. Pasos para configurar un túnel IPsec VTI en IPv6

1. enable
2. configure terminal
3. IPv6 unicast-routing
4. interface tunnel *tunnel-number*
5. IPv6 address *IPv6-address/prefix*
6. IPv6 enable
7. tunnel source {*ip-address* | *IPv6-address* | *interface-type interface-number*}
8. tunnel destination {*host-name* | *ip-address* | *IPv6-address*}
9. tunnel mode {**aurp**| **cayman**| **dvmrp**| **eon** | **gre**| **gre multipoint** | **gre IPv6** | **ipip**
[**decapsulate-any**] | **IPsec IPv4** | **iptalk**| **IPv6** | **IPsec IPv6** | **mpls**| **nos**| **rbscp**}
10. tunnel protection IPsec profile *name* [**shared**]

La explicación de cada uno de los pasos se detalla a continuación:

Paso 1

Se habilita el router a configurar, después de este comando el router queda habilitado para empezar su programación y se muestra Router#.

Paso 2

Se entra en el modo de configuración global del router, al editar este comando y dar enter el estado del router queda: Router (config)#

Paso 3

Habilita el enrutamiento de IPv6 unicast. Solo se necesita habilitar una vez, sin importar cuantas interfaces de túnel se requieran configurar.

Paso 4

Especifica una interfaz de túnel y número, se entra en el modo de configuración de interfaz.

Paso 5

Asigna una dirección IPv6 a la interfaz de túnel, luego ese tráfico de IPv6 puede ser ruteado por el túnel.

Paso 6

Habilita IPv6 en el túnel.

Paso 7

Establece la fuente de la dirección para la interfaz del túnel.

Paso 8

Se configura la dirección de destino para la interface de tunnel.

Paso 9

Establece el modo de encapsulación para la interfaz de túnel. Para IPsec, solo son soportadas las letras de IPsec IPv6.

Paso 10

Asocia una interfaz de túnel con un perfil IPsec. IPv6 no soporta palabras compartidas.

3.3.2. Verificar la configuración del modo túnel de IPsec

1. show adjacency [**summary** [*interface-type interface-number*]] | [*prefix*] [*interface]*
interface-number] [**connectionid***id*] [**link** {**IPv4 | IPv6 | mpls**}] [**detail**]

2. show crypto engine {**accelerator** | **brief** | **configuration** | **connections** [**active** | **dh** |
dropped-packet | **show**] | **qos**}
3. show crypto IPsec sa[**IPv6**] [*interface-type interface-number*] [**detailed**]
4. show crypto isakmp peer [**config**| **detail**]
5. show crypto isakmp policy
6. show crypto isakmp profile [**tag** *profilename*| **vrf***vrfname*]
7. show crypto map [**interface** *interface*| **tag** *map-name*]
8. show crypto session [detail] | [**local** *ip-address* [**port** *local-port*] | [**remote** *ip-address* [**port**
remote-port]] | **detail**] | **fvfr***vrf-name* | [**ivrf***vrf-name*]
9. show crypto socket
10. show IPv6 access-list [*access-list-name*]
11. show IPv6 cef[**vrf**] [*IPv6-prefix/prefix-length*] | [*interface-type interface-number*] [**longer-prefixes**
| **similar-prefixes** | **detail** | **internal** | **platform** | **epoch** | **source**]]
12. show interface *typenumber***stats**

La explicación de cada uno de los pasos se detalla a continuación:

Paso 1

La información de reenvió de Cisco Systems Inc. Express, de adyacencia de tabla o adyacencia de la tabla nivel 3 de hardware es mostrada.

Paso 2

Despliega un resumen de la información de configuración para los motores de cryptología.

Paso 3

Despliega las características que se usaron con la SA actual en IPv6

Paso 4

Despliega la descripción del par de equipos

Paso 5

Despliega los parámetros de cada política IKE

Paso 6

Lista todos los perfiles ISAKMP que se definieron en el router

Paso 7

Despliega la configuración del mapa criptográfico.

Paso 8

Despliega la información de estado de las sesiones de Criptología.

Paso 9

Lista los puntos de cryptología.

Paso 10

Despliega el contenido de todas las listas de acceso de IPv6.

Paso 11

Despliega las entradas en el reenvió de información base de IPv6 (FIB)

Paso 12

Despliega el número de paquetes que fueron encendidos, enviados mas rápido y distribuidos.

3.3.3. Problemas en la configuración y operación de IPsec para IPv6

1. enable
2. debug crypto IPsec [error]
3. debug crypto engine packet [detail] [error]

La explicación de cada uno de los pasos se detalla a continuación:

Paso 1

Se habilita el router a configurar, después de este comando el router queda habilitado para empezar su programación y se muestra Router#.

Paso 2

Despliega los eventos de IPsec en la red

Paso 3

Despliega el contenido de los paquetes IPv6.

Implementing IPsec in IPv6 Security, Cisco Systems Inc., 2001-2011[14]

Después de estudiar la configuración de un router para IPsec se tocaran temas relacionados a los RFC que involucran IPsec, de los cuales se dará una breve explicación.

3.4. RFCs de IETF orientados en IPSEC para ambientes IPV6

Los estándares de la IETF (RFCs), estándares en los cuales está basada la configuración que se le debe dar a IPsec en ambientes IPv6 son el RFC 4301 y 4309, para IPv6, en los cuales se puede decir que el funcionamiento de IPsec da una solución de seguridad bastante amplia y confiable a muchos de los problemas de seguridad que presenta IPv6 al configurarse. Dichos documentos de la IETF, sobre la configuración de IPsec en ambientes IPv6, resume lo siguiente: En ambientes IPv6 el protocolo IPsec funciona de forma segura, siempre y cuando en su configuración se apliquen los estándares RFCS de la IETF para tráfico de la información en modo túnel o en modo transporte usando los protocolos de autenticación y algoritmos de encriptación. [4]

Los estándares de la IETF (RFC) describen completamente el funcionamiento, configuración y la forma de utilización de los protocolos de autenticación AH, ESP y las llaves a utilizar en modo transporte y túnel (IKEv2).

A continuación se verá en resumen algunos de los RFC ya obsoletos, los cuales han venido siendo actualizados, por los visto en el capitulo 2.

3.4.1. RFC 4301 Security architecture for the Internet Protocol

IPsec utiliza dos protocolos para proporcionar servicios de seguridad del tráfico:

- Cabecera de Autenticación (AH)
- Carga útil de Seguridad encapsulante (ESP).

Ambos protocolos se describen en detalle en sus respectivas RFC.

ESP puede proporcionar sólo la integridad, sin confidencialidad, por lo que es comparable a AH, en la mayoría de los contextos.

La cabecera de autenticación IP (AH) ofrece integridad y origen de datos de autenticación, con opcional (a discreción de El receptor) características anti-replay.

[14]Capítulo 3 hasta el 3.3.3, Tomado, traducido y editado de: Implementing IPsec in IPv6 Security, Cisco Systems Inc., 2001-2011, http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-ipsec.pdf

El encapsulante de Seguridad (ESP) Peso de la carga de protocolo ofrece el mismo conjunto de los servicios, y también ofrece la confidencialidad. El uso de ESP para proporcionar confidencialidad sin integridad es no recomendado.
Cuando se utiliza con el ESP activado confidencialidad, están limitados por las disposiciones de confidencialidad del flujo de tráfico, es decir, disposiciones para ocultar paquetes de longitud, y para facilitar eficiente la generación y descartar los paquetes

Ambos ofrecen AH y ESP de control de acceso, a través de la forzada distribución de claves criptográficas y de la gestión de tráfico. Corrientes dictadas por la Política de Seguridad de Base de Datos

Estos protocolos pueden aplicarse individualmente o en combinación para IPv4 e IPv6 y prestar servicios de seguridad. Sin embargo, la mayoría de requisitos de seguridad pueden ser satisfechos mediante el uso de ESP por sí solo.

Cada protocolo soporta dos modos de uso: modo de transporte y de túnel AH y ESP principalmente para proporcionar protección por medio de las calves ISAKMP, las cuales no son de uso obligatorio.[15]

3.4.2. RFC 4309 Using advanced encryption standard (AES) CCM mode with IPsec encapsulating security payload (ESP)

Este documento describe el uso de Advanced Encryption Standard (AES) con CBC-MAC (CCM), con una inicialización explícita vectorial (IV), con una carga útil de seguridad IPsec encapsuladora (ESP) con mecanismo para garantizar la confidencialidad, la autenticación del origen de datos, e integridad sin conexión.

[15] **Security Architecture for the Internet Protocol,** Network Working Group S. Kent Request for Comments: 4301 K. Seo Obsoletes: 2401 BBN Technologies Category: Standards Track. World Wide Web http://www.ietf.org/rfc/rfc4301

La carga útil de ESP, se estructura como se muestra en el gráfico.

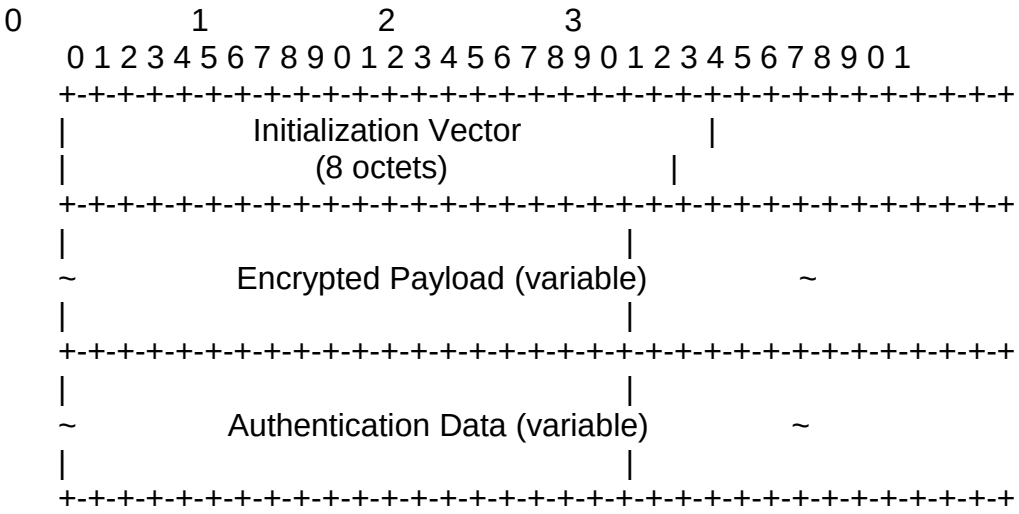

Figura 13: ESP Payload Encrypted with AES CCM

Construcción de AAD

La integridad de los datos y la autenticación del origen de datos para la Seguridad Índice de parámetros (SPI) y (extendido) los campos de número de secuencia es siempre sin cifrar.
Dos formatos están definidos:
Uno para 32-bits números de secuencia y uno para 64-bits números de secuencia extendidos. El formato con números de secuencia de 32-bit se muestra en el gráfico, y el formato con 64-bits números de secuencia extendidos se muestra en el gráfico.

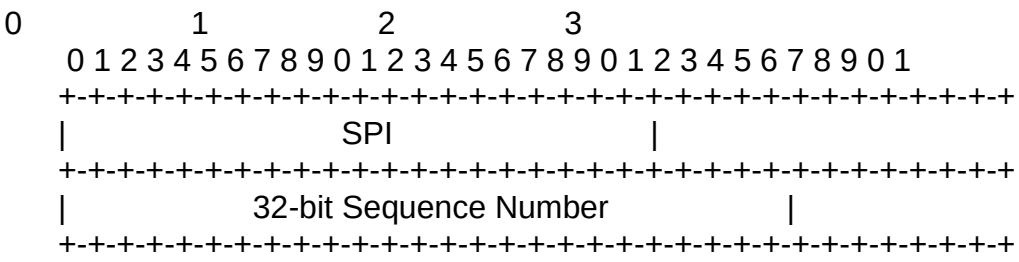

Figura 14: AAD Format with 32-bit Sequence Number

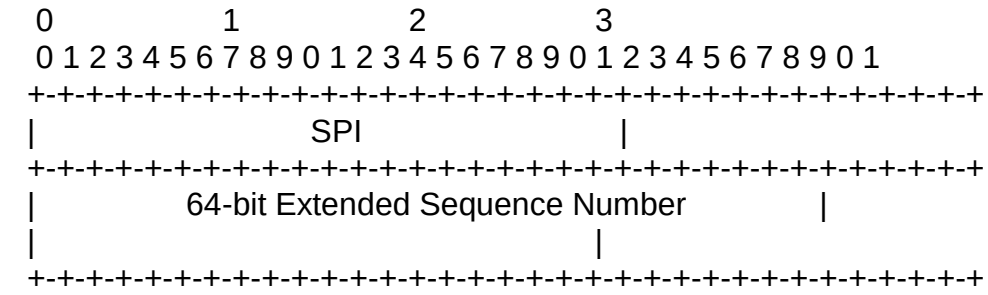

Figura 15: AD Format with 64-bit Extended Sequence Number

Convenios de IKE

Describe el uso delas convenciones utilizadas para generar claves, los valores materiales y su uso con AES-CCMcon (IKE) protocolo. Los identificadores y atributos necesarios para negociar una asociación de seguridad que utiliza AES CCM también se definen.[16]

3.4.3. RFC 5996. Internet Key Exchange Protocol Version 2 (IKEv2)

Este documento describe la versión 2 de la Internet Key Exchange (IKE) protocolo. IKE es un componente de IPsec utilizar para realizar la autenticación y el establecimiento y mantenimiento de asociaciones de seguridad (SA). Este documento sustituye y actualiza el RFC 4306, e incluye todas las de las aclaraciones de la RFC 4718. Este documento describe un protocolo - el Internet Key Exchange (IKE). La versión 1 de IKE se ha definido en el RFC 2407 [traducción], 2408 [ISAKMP], y 2409 [IKEv1]. IKEv2 sustituye todos los RFC. IKEv2 se define en [IKEv2] (RFC 4306) y se aclaró en [clarifi] (RFC 4718).

Este documento sustituye y actualiza el RFC 4306 y RFC 4718. IKEv2 fue un cambio en el protocolo IKE. En contraste, el documento actual no sólo proporciona una aclaración de IKEv2, sino que hace mínimos cambios en el IKE protocolo. IKE lleva a cabo la autenticación mutua entre ambas partes y establece una asociación de seguridad IKE (SA), que incluye compartir información secreta que se puede utilizar para establecer de manera eficiente para SV Carga de seguridad encapsuladora (ESP) [ESP] o la autenticación de cabecera (AH) [AH] y un conjunto de algoritmos criptográficos para ser utilizado por las asociaciones de seguridad para proteger el tráfico que llevan. En este documento, el término "Suite" o "suite criptográfica" se refiere a un conjunto completo de algoritmos utilizados para proteger a una SA. Un iniciador propone una o más suites de los

[16]**Using Advanced Encryption Standard (AES) CCM Mode with IPsec Encapsulating Security Payload (ESP)**, Network Working Group R. Housley Request for Comments: 4309 Vigil Security Category: Standards World Wide Web http://tools.ietf.org/rfc/rfc4309.txt

algoritmos de cotización compatibles que se pueden combinar en suites en forma de mezcla y del fósforo. IKE puede negociar el uso de la PI Compresión (IP Comp) [IP-COMP] en relación con una SA ESP o AH. El SAs para ESP o AH que ponerse en marcha a través de ese IKE que se llama "Niño SA".
Todas las comunicaciones IKE constan de un par de mensajes: una petición y una respuesta. La pareja se llama un "intercambio", y se llama a veces una "solicitud / respuesta de pareja". El primer intercambio de mensajes el establecimiento de una SA IKE se llama IKE_SA_INIT e IKE_AUTH intercambios, los intercambios posteriores IKE se llaman CREATE_CHILD_SA o Intercambios de información. En el caso habitual, hay una sola IKE_SA_INIT de cambio y un solo intercambio de IKE_AUTH (un total de cuatro mensajes) para establecer la SA IKE y el primer hijo SA. En casos excepcionales, puede haber más de uno de cada uno de estos intercambios. En todos los casos, todos los intercambios IKE_SA_INIT DEBE completar antes de cualquier tipo de cambio sí, entonces todos los intercambios IKE_AUTH DEBE Escenarios de uso IKE se utiliza para negociar las SA ESP o AH en un número de diferentes escenarios, cada uno con sus propios requisitos especiales.

Las diferencias significativas entre los RFC 4306 y este documento Este documento contiene aclaraciones y ampliaciones de IKEv2 [IKEv2]. Muchas de las aclaraciones se basan en **CLARIFICAR**.

*Los cambios que se mencionan en este documento se discuten en el trabajo de IPsec Grupo y, después de que el Grupo de Trabajo se disolvió. Este documento contiene explicaciones detalladas de áreas que no estaban claros en IKEv2, por lo que es útil para los implementadores de IKEv2. El protocolo se describe en este documento conserva el mismo e importante número de versión (2) y el número de versión menor (0) como se utilizó en el RFC 4306. Es decir, el número de versión * no * es cambiado de RFC 4306.*

El pequeño número de cambios técnicos figuran en esta lista no se espera que afecta a las implementaciones de RFC 4306 que ya han sido desplegados en el momento de la publicación de este documento.

Este documento hace que las figuras y referencias un poco más consistentes de lo que eran en [IKEv2]. IKEv2 los desarrolladores han señalado que los requisitos deben de nivel en el RFC 4306 son a menudo poco clara en que no se dicen cuando se está bien, no obedecer a los requisitos
En este documento se elimina la discusión de anidación AH y ESP. Esta fue una error en el RFC 4306 causado por el desfase entre el acabado y el RFC 4306 RFC 4301. Básicamente, IKEv2 se basa en la RFC 4301, que no incluyen "grupos de SA" que formaban parte de la RFC 2401. Mientras que una sola paquete puede ir a través de IPsec tiempos de procesamiento múltiples, cada uno de estos pases utiliza una por separado, SA, y los pases son coordinadas por el

transmisión de las tablas. En IKEv2, cada una de estas asociaciones de seguridad tiene que ser creado utilizando un intercambio CREATE_CHILD_SA separado.

Este documento elimina la discusión de la INTERNAL_ADDRESS_EXPIRY configuración de atributo, ya que su aplicación era muy problemática
Este documento también se elimina INTERNAL_IP6_NBNS como un atributo de configuración. En este documento se elimina el subsidio para los mensajes de rechazo en el que las cargas no estaban en el orden "correcto", y ahora las implementaciones DEBEN NO rechazarlas. Esto es debido a la falta de claridad donde las órdenes para las cargas útiles se describen. Las listas de artículos con el RFC 4306 que terminó en el registro de la IANA fueron recortadas para incluir sólo los elementos que se han definido en el RFC realidad 4306. Además, muchas de esas listas están precedidas por el mismo de instrucciones importantes para los desarrolladores que realmente debe mirar el registro de la IANA en el momento de desarrollo, ya que los elementos nuevos que han añadido desde el RFC 4306.

En este documento se añade una aclaración sobre si las notificaciones son y son no se envía encriptada, dependiendo del estado de la negociación en el tiempo.

Este documento trata más sobre la forma de negociar de modo combinado sistemas de cifrado. "La carga útil debería ser incluido" fue cambiado a ser "La carga útil IKE deberá ser incluido". Esto también llevó a cambios en Sección 2.18. En la sección 2.1, no hay nuevo material que cubre cómo el iniciador SPI y / o dirección IP se utiliza para diferenciar si se trata de un "medio abierta" IKE SA o de una nueva solicitud.

Este documento se aclara el uso de la bandera crítico en la Sección 2.5. En la Sección 2.8, "Tenga en cuenta que, cuando cambio de claves, el nuevo Niño SA pueden tener Selectores de diferentes algoritmos de tráfico y que el viejo "era ha cambiado a "Tenga en cuenta que, cuando cambio de claves, el nuevo Niño SA no debe tienen diferentes selectores de tráfico y algoritmos que el viejo ". La nueva Sección 2.8.2 cubre simultánea de reintroducción de claves IKE SA. La nueva Sección 2.9.2 cubre los selectores de tráfico en reintroducción de claves. Este documento se añade la restricción en la sección 2,13 de que todos funciones pseudoaleatorias (PRF) se utilizan con IKEv2 DEBE tomar variable teclas de tamaño. Esto no debe afectar a las implementaciones porque no hubo PRF estandarizados que tienen teclas de tamaño fijo. Kaufman, et al. Normas Track [Página 21] RFC 5996 IKEv2bis septiembre 2010 Sección 2.18 requiere hacer un intercambio de Diffie-Hellman, cuando cambio de claves la IKE_SA. En teoría, la RFC 4306 permite una política donde el Diffie- Hellman era opcional, pero esto no era útil (o caso), cuando el cambio de claves IKE_SA.

Artículo 2.21 se ha ampliado en gran medida para cubrir los diferentes casos donde las respuestas de error son necesarias y las respuestas adecuadas a

ellos. Sección 2.23 aclaró que, en NAT transversal, tanto ahora como en UDP encapsulado paquetes IPsec y no-UDP-encapsulado de paquetes IPsec Es necesario entender cuando se recibe. Se añadió la sección 2.23.1 para describir NAT cuando el modo de transporte es solicitado. Se agregó una sección de 2,25 a explicar cómo actuar cuando hay tiempo colisiones al eliminar y / o cambio de claves SA, y dos nuevo error notificaciones (TEMPORARY_FAILURE y CHILD_SA_NOT_FOUND) fueron definido.

En la Sección 3.6, "Implementaciones DEBE apoyar el método HTTP para hash y URL de búsqueda. El comportamiento de los métodos URL otros no es actualmente se especifica, y los métodos no deberían ser utilizados en la ausencia de un documento que especifica que "se añadió. En la sección 3.15.3, un puntero a un nuevo documento que se relaciona con configuración de direcciones IPv6 se añadió. Apéndice C se amplió y aclaró.2. Detalles del protocolo IKE y Variaciones IKE normalmente escucha y lo envía en el puerto UDP 500, aunque los mensajes IKE También pueden ser recibidos en el puerto UDP 4500 con un poco diferente formato (véase la sección 2.23). Dado que UDP es un datagrama (no confiable) protocolo IKE incluye en su definición de la recuperación de la transmisión errores, incluyendo la pérdida de paquetes, repetición de paquetes, y la falsificación de paquetes. IKE está diseñado para funcionar tanto tiempo como (1) al menos uno de una serie de paquetes retransmitidos llega a su destino antes de que se agote el tiempo; y (2) el canal no está tan lleno de paquetes falsificados y se reproducen para para agotar la capacidad de la red o la CPU de uno u otro extremo. Incluso en ausencia de los requisitos mínimos de eficiencia, es IKE diseñado para fallar limpia (como si la red se ha roto). Aunque IKEv2 mensajes están destinados a ser corta, que contienen estructuras sin superior duro unido en el tamaño (en particular, digitales certificados), y IKEv2 sí mismo no tiene un mecanismo para Kaufman, et al. Normas Track [Página 22] RFC 5996 IKEv2bis septiembre 2010 fragmentación de mensajes de gran tamaño. IP define un mecanismo para la fragmentación de los mensajes UDP de gran tamaño, pero las implementaciones pueden variar en el máximo tamaño de los mensajes compatible. Además, el uso de la fragmentación IP abre una implementación de denegación de servicio (DoS) [DOSUDPPROT].

Por último, algunos de NAT y / o implementaciones de firewall puede bloquear la IP fragmentos. Todas las implementaciones IKEv2 deberá ser capaz de enviar, recibir, y el proceso de Mensajes IKE que son de hasta 1280 bytes de largo, y deben ser capaces de para enviar, recibir y procesar los mensajes que son de hasta 3000 octetos de largo. IKEv2 implementaciones deben ser conscientes de la UDP máxima tamaño de los mensajes compatibles y pueden acortar los mensajes, dejando algunos certificados o propuestas criptográficas privado si eso va a mantener Mensajes de debajo del máximo. El uso del "Hash" y la URL formatos más de incluir los certificados en los intercambios siempre que sea posible se puede evitar la mayoría de los problemas. Las implementaciones y la

configuración hay que tener en cuenta, sin embargo, que si las búsquedas de URL es posible sólo después de la Niño SA se establece, las cuestiones de recursividad podría evitar que esto técnica de trabajo. La carga UDP de todos los paquetes que contienen los mensajes enviados en el puerto de IKE 4500 debe comenzar con el prefijo de cuatro ceros, de lo contrario, el receptor no sabe cómo manejarlos. [17]

[17]**Internet Key Exchange Protocol Version 2 (IKEv2)**, Internet Engineering Task Force (IETF) C. Kaufman, Request for Comments: 5996, Microsoft Obsoletes: 4306, 4718, P. Hoffman Category: Standards Track. VPN Consortium ISSN: 2070-1721, Y. Nir, P. Eronen. World Wide Web http://tools.ietf.org/html/rfc5996, visitada el 10 de agosto de 2012 2:50pm

4. FUNCIONAMIENTO DE IPSEC

Los protocolos de IPsec actúan en la capa de red, la capa 3 del modelo OSI. IPsec es una parte obligatoria de IPv6. IPsec funciona dando seguridad en modo transporte (extremo a extremo) del tráfico de paquetes, en el que los ordenadores de los extremos finales realizan el procesado de seguridad, o en modo túnel (puerta a puerta) en el que la seguridad del tráfico de paquetes es proporcionada a varias máquinas (incluso a toda la red de área local) por un único nodo.

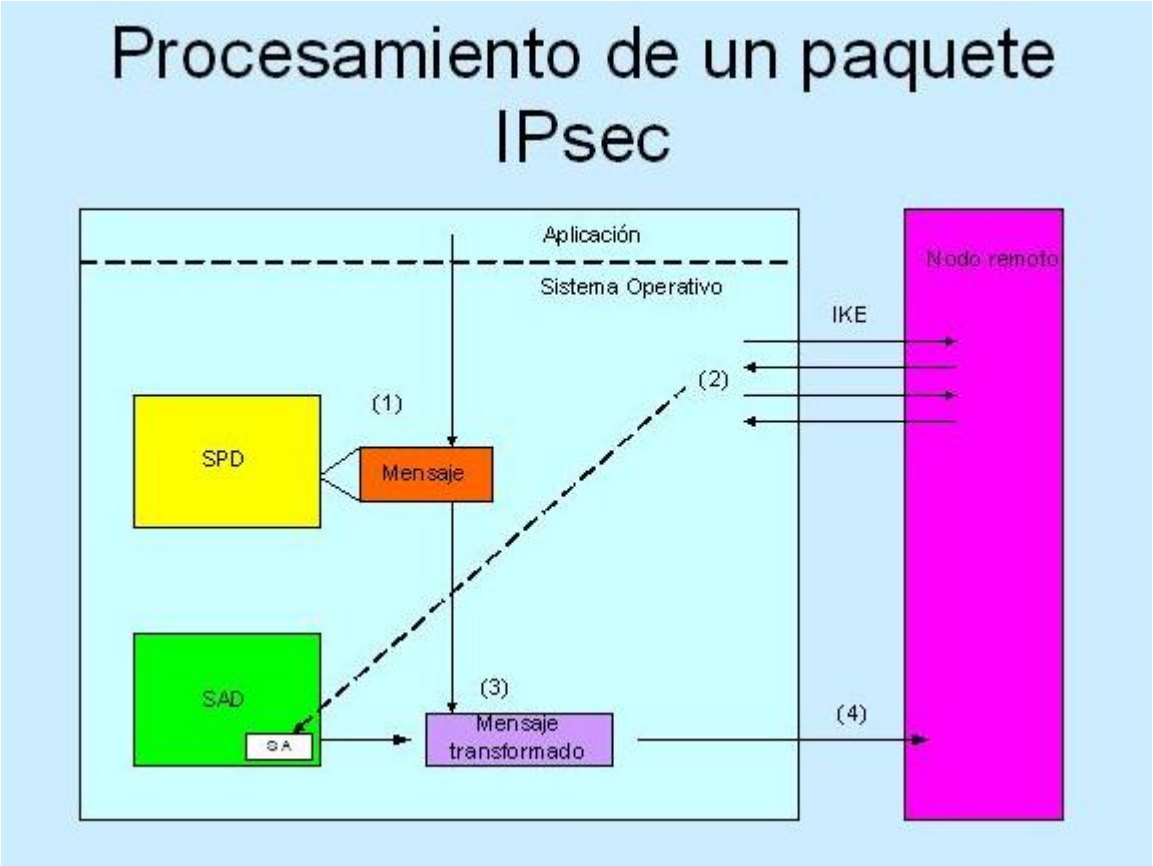

Figura 16: Procesamiento de un paquete IPsec [18]

IPsec proporcionar servicios de seguridad tales como:

1. Cifrar el tráfico: De forma que no pueda ser leído por nadie más que las partes a las que está dirigido.

[18] **IPsec**, Word Wide Web http://congreso.seguridad.unam.mx/2005/seguridad2005/ponencias/IPSec/html/img15.html Consultada el 10 de agosto de 2012 10:54am

2. Validación de integridad Asegurar que el tráfico no ha sido modificado a lo largo de su trayecto.
3. Autenticar a los extremos: Asegurar que el tráfico proviene de un extremo de confianza.
4. Anti-repetición: Proteger contra la repetición de la sesión segura.

Usando:

- Algoritmos de cifrado (DES, 3DES, IDEA, Blowfish).
- Algoritmos de hash (MD5, SHA-1).
- Tecnologías de clave pública (RSA).
- Certificados digitales.

IPsec utiliza una arquitectura de un servidor de políticas:

- Repositorio: Este almacena las definiciones de servicios, plantillas, políticas IPsec. Se implementa con archivos planos, con directorios LDAP o con base de datos.
- Consola de administración: Es la interfaz de usuarios que permite a los administradores definir nuevos servicios.
- Procesamiento central de facilidades: Traduce políticas de negocio de alto nivel en detalladas reglas IPsec y las almacena en el repositorio.
- Consumidor de políticas: Este adquiere políticas en nombre de los diferentes elementos de red y adapta reglas en formatos específicos de los dispositivos y los distribuye.

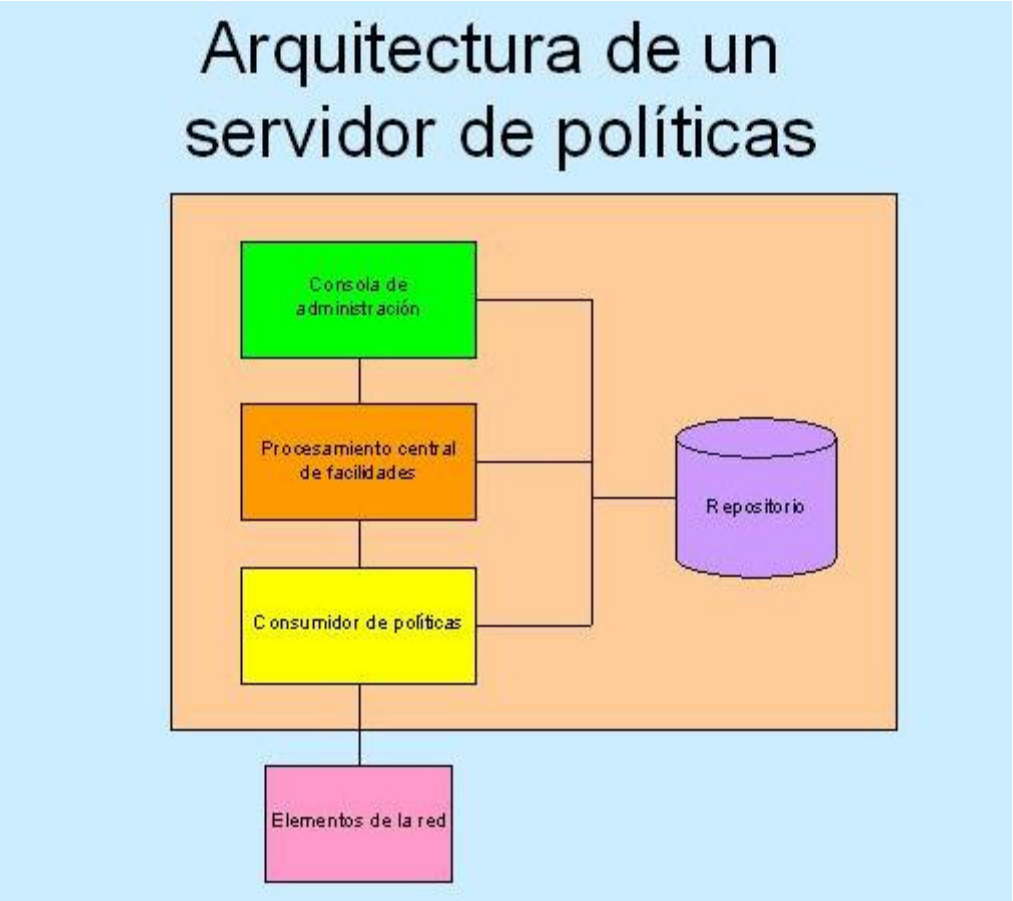

Figura 17: Arquitectura de un servidor de políticas[19]

4.1. Modo transporte

Al operar IPsec en modo transporte, el contenido transportado dentro del datagrama (AH o ESP) son datos de la capa de transporte (por ejemplo, datos TCP o UDP). Por tanto, la cabecera IPsec se inserta inmediatamente a continuación de la cabecera IP y antes de los datos de los niveles superiores que se desean proteger. El modo transporte tiene la ventaja de asegurar la comunicación extremo a extremo, pero requiere que ambos extremos entiendan el protocolo IPsec como se muestran en las siguientes figuras.

[19] **IPsec**, Word Wide Web http://congreso.seguridad.unam.mx/2005/seguridad2005/ponencias/IPSec/html/img15.html Consultada el 10 de agosto de 2012 10:54am

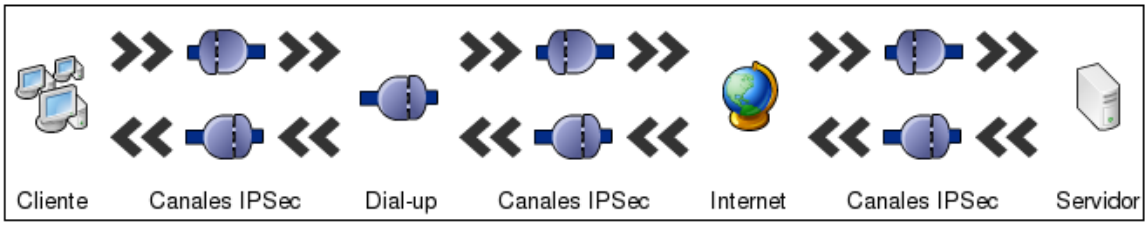

Figura 18: Modo transporte de IPsec[20]

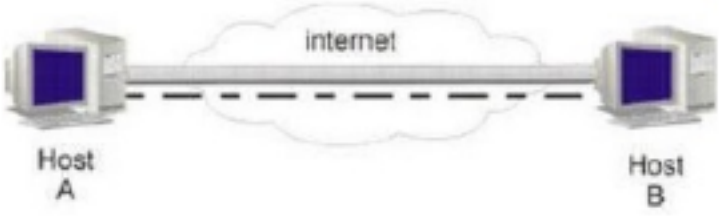

Figura 19: Modo Transporte de Pc a Pc utilizando IPsec[21]

En el modo transporte (los datos que se transfieren) del paquete IP es cifrada y/o autenticada. El enrutamiento permanece intacto, ya que no se modifica ni se cifra la cabecera IP; sin embargo, cuando se utiliza la cabecera de autenticación (AH), las direcciones IP no pueden ser traducidas, ya que eso invalidaría el hash. Las capas de transporte y aplicación están siempre aseguradas por un hash, de forma que no pueden ser modificadas de ninguna manera (por ejemplo traduciendo los números de puerto TCP y UDP). El modo transporte se utiliza para comunicaciones ordenador a ordenador.

4.2. Modo túnel

En el modo túnel, todo el paquete IP (datos más cabeceras del mensaje) es cifrado y/o autenticado. Debe ser entonces encapsulado en un nuevo paquete IP para que funcione el enrutamiento. El modo túnel se utiliza para comunicaciones red a red (túneles seguros entre routers, p.e. para VPNs) o comunicaciones ordenador a red u ordenador a ordenador sobre Internet.
La familia de protocolos IPsec está formada por dos protocolos: el **AH** (Authentication Header - Cabecera de autenticación) y el **ESP** (Encapsulated Security Payload - Carga de seguridad encapsulada).

[20]Protocolo IPsec, World Wide Web http://laurel.datsi.fi.upm.es/proyectos/teldatsi/teldatsi/protocolos_de_comunicaciones/protocolo_ipsec. Consultada el 10 de agosto de 2012 10:54am

[21]Configuración IPsec implementando protocolo ESP en modo Transporte. World Wide Web http://es.scribd.com/doc/13460605/Configuracion-Ipsec-implementando-protocolo-ESP-en-modo-Transporte. Consultada el 12 de agosto de 2012 10:40am

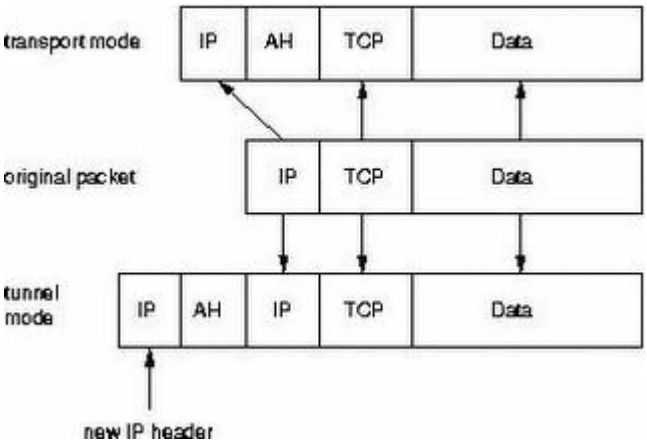

Figura 20: Datagramas en Modo transporte y túnel de IPsec[22]

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

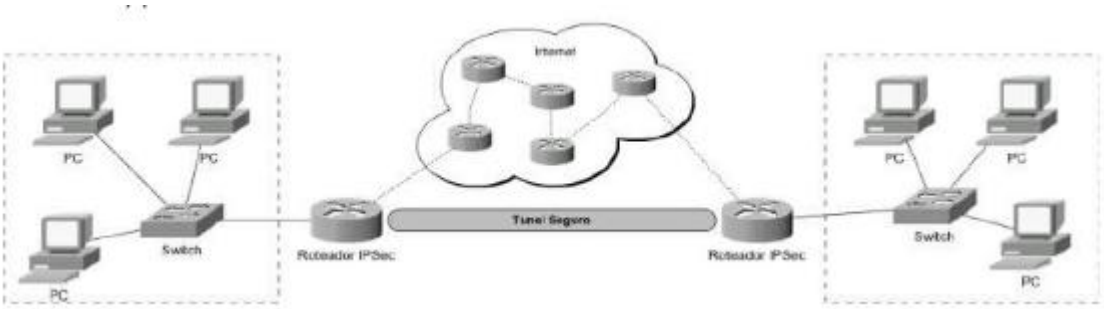

Figura 21: Modo túnel de IPsec en una red[23]

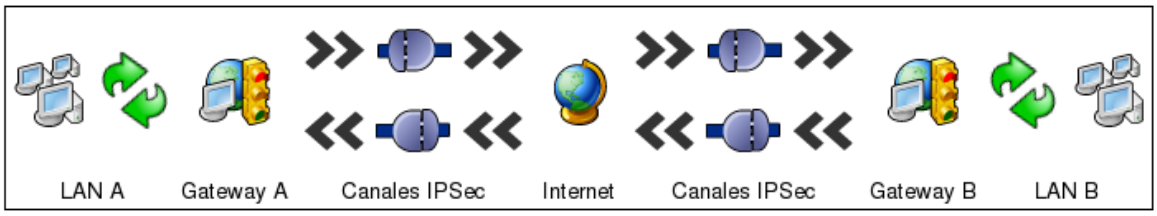

Figura 22: Funcionamiento en modo túnel de IPsec[24]

[22]Módulo de seguridad, World Wide Web http://modseguridad.blogspot.com/2008/05/ipsec.html consultada el 12 de agosto de 2012 5:40pm

[23]Modulo de seguridad, World Wide Web http://modseguridad.blogspot.com/2008/05/ipsec.html consultada el 12 de agosto de 2012 5:40pm

4.3. Funcionamiento de AH

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 23: Datagrama de AH[25]

Significado de los campos:
Next header
Identifica el protocolo de los datos transferidos.
Payload length
Tamaño del paquete AH.
RESERVED
Reservado para uso futuro (hasta entonces todo ceros).
Security parameters index (SPI)
Indica los parámetros de seguridad que, en combinación con la dirección IP, identifican la asociación de seguridad implementada con este paquete.
Sequence number
Un número siempre creciente, utilizado para evitar ataques de repetición.
HMAC
Contiene el valor de verificación de integridad (ICV) necesario para autenticar el paquete; puede contener relleno.

[24]Protocolo IPsec, World Wide Web http://laurel.datsi.fi.upm.es/proyectos/teldatsi/teldatsi/protocolos_de_comunicaciones/protocolo_ipsec. Consultada el 10 de agosto de 2012 10:54am

[25]Modulo de seguridad, World Wide Web http://modseguridad.blogspot.com/2008/05/ipsec.html consultada el 12 de agosto de 2012 5:40pm

HMAC se ilustra en la siguiente imagen:

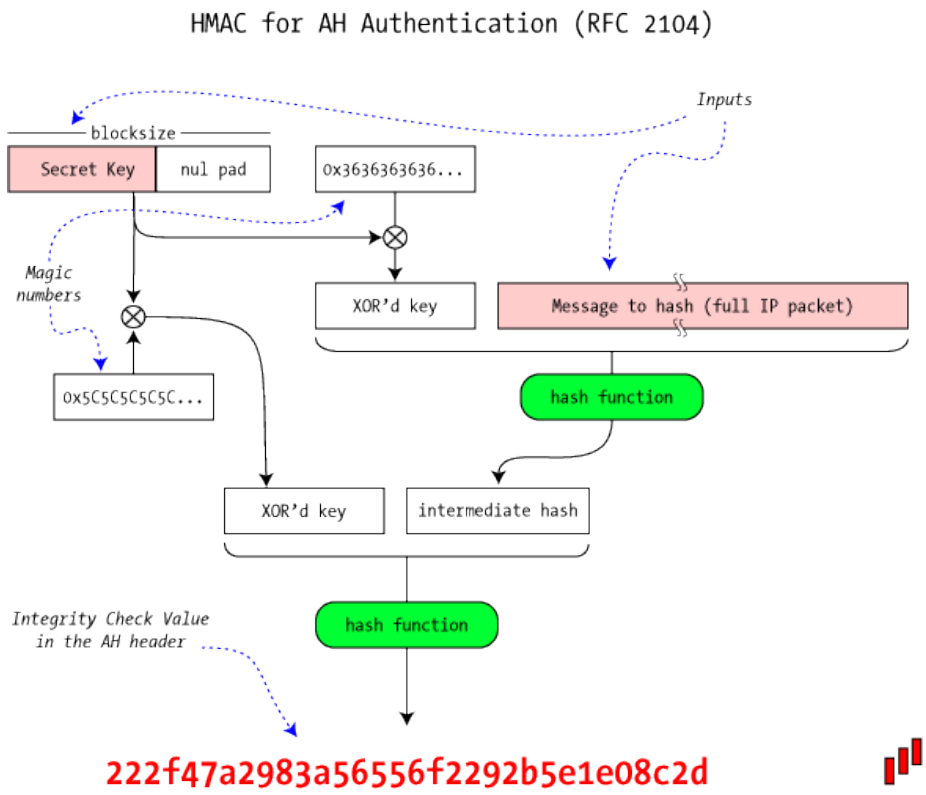

Figura 24: HMAC por el RFC 2104[26]

IPsec no define ni obliga como debe hacerse la autentificación, simplemente ofrece un marco de seguridad en la que los dos hosts que realicen la comunicación se pongan de acuerdo sobre qué sistema van a usar. Pueden usarse firmas digitales o funciones de encriptación, pero es obligatorio que ambos los conozcan y sepan cómo usarlos.

La función del protocolo AH es proteger la integridad del datagrama IP. Para llevar a cabo esta tarea, AH calcula una HMAC basada en la clave secreta y el contenido del paquete y las partes inmutables de la cabecera IP, como se muestra en la siguiente figura y se había explicado en los capítulos 1 y 2.

[26]Protocolo IPsec, World Wide Web http://laurel.datsi.fi.upm.es/proyectos/teldatsi/teldatsi/protocolos_de_comunicaciones/protocolo_ipsec. Consultada el 10 de agosto de 2012 10:54am

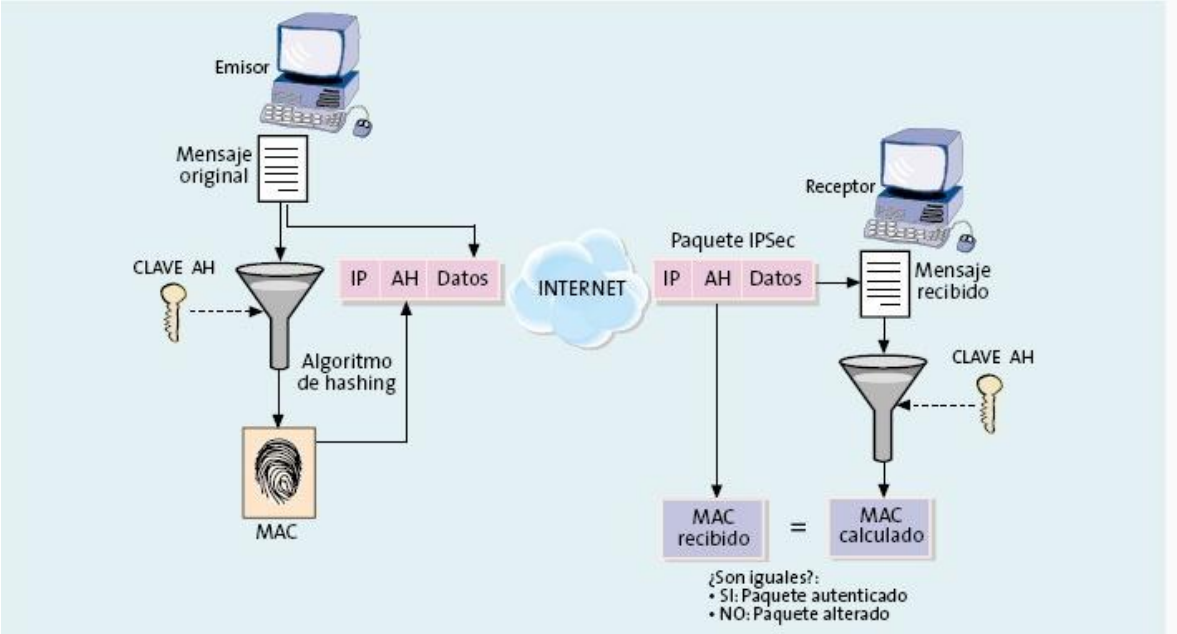

Figura 25: Funcionamiento de AH para IPsec[27]

4.3.1. NAT y AH

AH da una protección muy fuerte a los paquetes porque cubre todas las partes que se consideran inmutables. Pero esta protección tiene un costo: AH es incompatible con NAT (Network Address Translation). Dado que el campo TTL y el checksum de la cabecera siempre son modificados "al vuelo", AH sabe que tiene que excluirlos de su protección, pero no tiene que excluir a las direcciones IP. Estas están incluidas en el control de integridad, y cualquier cambio en las direcciones Ip de origen y destino va a hacer que el control de integridad falle cuando llegue al destinatario. Dado que el valor del control de integridad contiene una llave secreta que sólo la saben el host origen y el host destino, el dispositivo NAT no puede recalcular el ICV.

[27] Red privada Virtual, World Wide Web http://campusvirtual.unex.es/cala/cala/mod/resource/view.php?id=1883. Consultada el 11 de agosto de 2012 11:00am

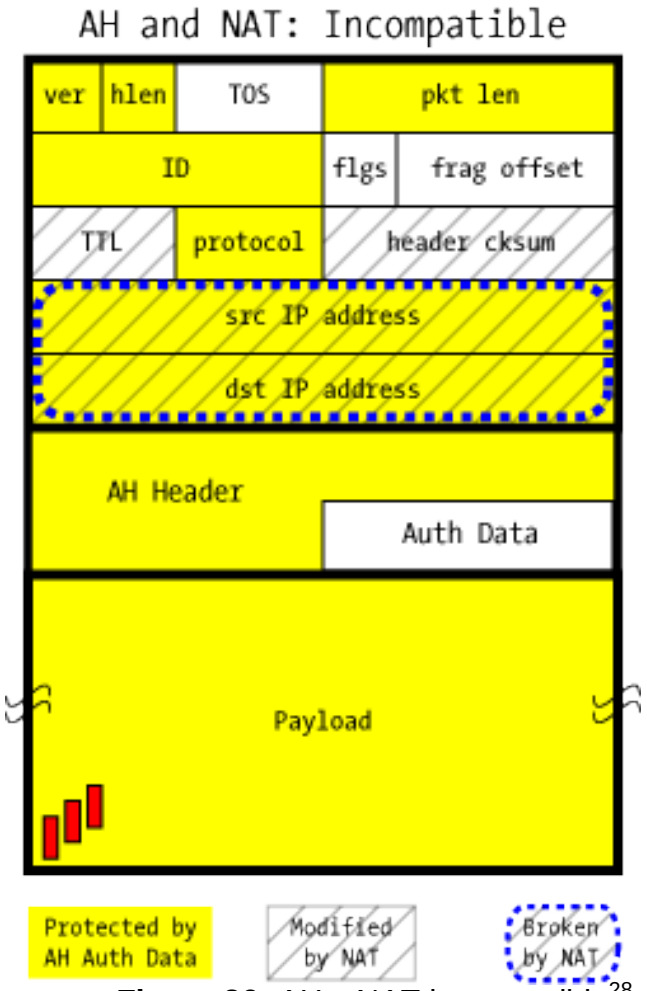

Figura 26: AH y NAT incompatible[28]

4.4. Funcionamiento de ESP

El protocolo ESP proporciona la integridad del paquete empleando una HMAC y la confidencialidad empleando cifrado. La cabecera ESP se genera y añade al paquete tras cifrarlo y calcular su HMAC. A diferencia de AH, que da una pequeña cabecera antes de la carga útil, ESP rodea la carga útil con su protección. Los parámetros de seguridad Index y Sequence Number tienen el mismo propósito que en AH, pero se encuentran como relleno en la cola del paquete del campo "siguiente campo" y el opcional "Authentication data".

[28]Protocolo IPsec, World Wide Web http://laurel.datsi.fi.upm.es/proyectos/teldatsi/teldatsi/protocolos_de_comunicaciones/protocolo_ipsec. Consultada el 10 de agosto de 2012 10:54am

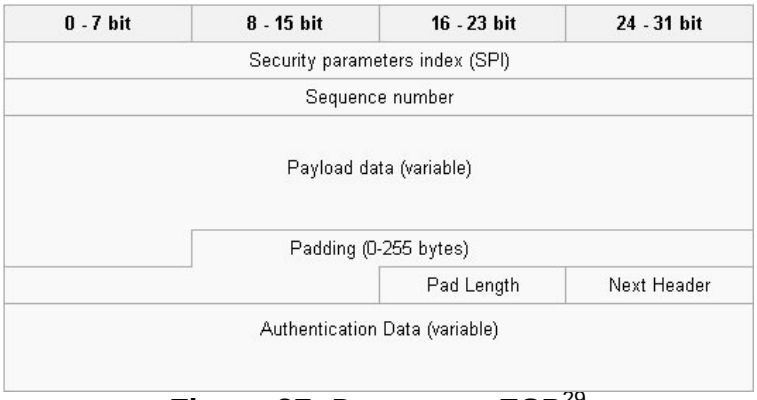

Figura 27: Datagrama ESP[29]

Security parameters index (SPI)
Identifica los parámetros de seguridad en combinación con la dirección IP.
Sequence number
Un número siempre creciente, utilizado para evitar ataques de repetición.
Payload data
Los datos a transferir.
Padding
Usado por algunos algoritmos criptográficos para rellenar por completo los bloques.
Pad length
Tamaño del relleno en bytes.
Next header
Identifica el protocolo de los datos transferidos.
Authentication data
Contiene los datos utilizados para autenticar el paquete.

[29]Modulo de seguridad, World Wide Web http://modseguridad.blogspot.com/2008/05/ipsec.html consultada el 12 de agosto de 2012 5:40pm

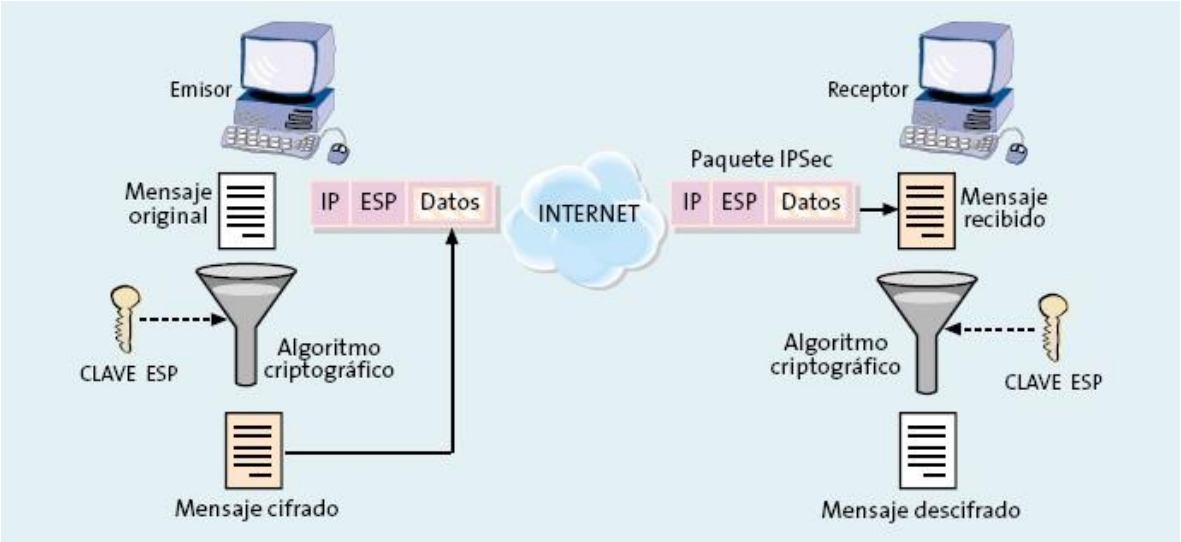

Figura 28: Funcionamiento de ESP para IPsec[30]

4.5. Funcionamiento de IKE

IPsec tiene un mecanismo de acción para establecer el intercambio dinámico de llaves compartidas secretas a través de IKE (Internet Key Exchange).
IKE tiene formas de negociar el intercambio de llaves:

- Main Mode
- Agressive Mode

Main Mode
Una sesión de IKE se inicia con cuando el iniciador envía una propuesta o varias propuestas a la respuesta solicitada. Las propuestas que definen los protocolos de cifrado y autenticación son aceptables, ¿cuánto tiempo debe permanecer activa las teclas, y su confidencialidad directa perfecta debe ser forzada?, por ejemplo. Varias propuestas se pueden enviar en una sola oferta. El primer intercambio entre los nodos, establece la política de seguridad básica, el iniciador propone algoritmos de cifrado y autenticación que está dispuesto a utilizar. La respuesta elige la propuesta adecuada (se puede suponer una propuesta elegida) y lo envía al iniciador. Lo siguiente que pasa es que el intercambio pasa de Diffie-Hellman claves públicas y otros datos. Todas las nuevas negociaciones se cifran en el IKE SA. El tercer intercambio autentica la sesión de ISAKMP. Una vez que el SA IKE

[30]Protocolo IPsec, World Wide Web http://laurel.datsi.fi.upm.es/proyectos/teldatsi/teldatsi/protocolos_de_comunicaciones/protocolo_ipsec. Consultada el 10 de agosto de 2012 10:54am

se ha establecido, la negociación IPsec (modo rápido) comienza.

Agressive Mode
Modo Agresivo aprieta la negociación de IKE SA en tres paquetes, con todos los datos necesarios para la SA aprobada por el iniciador. La respuesta envía la propuesta, la clave, la identificación y la autenticación de la sesión en el siguiente paquete. El iniciador responde mediante la autenticación de la sesión. La negociación es más rápida, el iniciador y el respondedor ID se comunican.

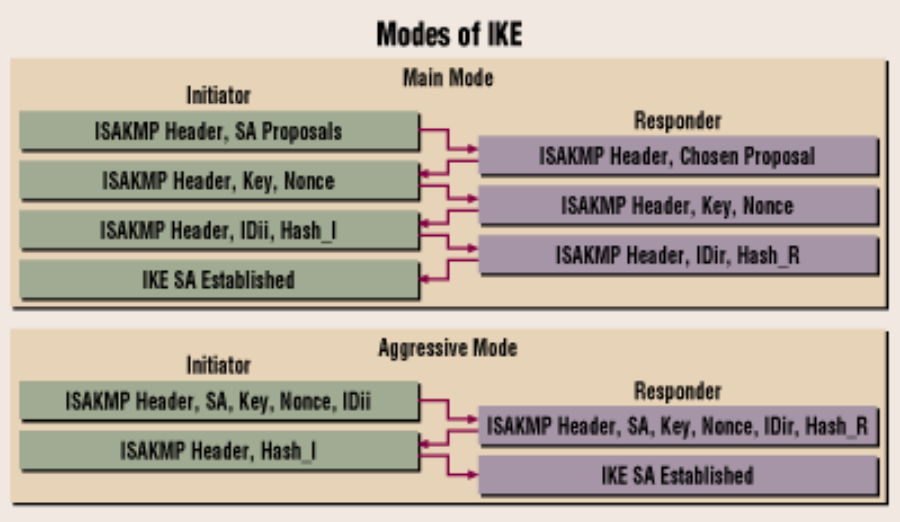

Figura 29: Formas de Negociar IKE[31]

Cuando IKE hace la negociación cada uno de los dos dispositivos involucrados debe suministrar su lista de métodos de autenticación, algoritmos de cifrado y algoritmos de hash. Ambas partes acuerdan un método de autenticación, un algoritmo cifrado y un algoritmo hash, los cuales se usan para generar las llaves criptográficas compartidas. Este método de autenticación permite comunicar entre si las dos partes relacionadas y construir una verdadera confianza.

[31]Main Mode Vs. Aggressive Mode, World Wide Web https://supportforums.cisco.com/docs/DOC-8125 consultada el 12 de gusto 8:00pm

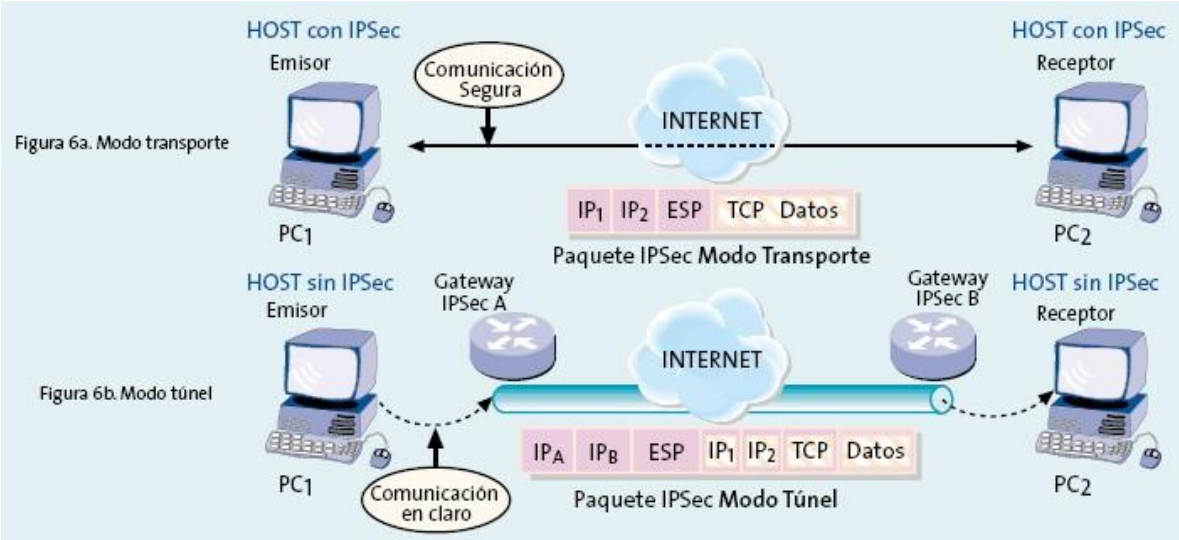

Figura 30: Funcionamiento de IKE para IPsec[32]

En los puntos extremos de la conexión se tienen llaves criptográficas secretas que permitirán iniciar negociaciones seguras para crear las SA que requiere IPsec, esta es la función de IKE.
Políticas de IKE:
Discard: El paquete es eliminado.
Bypass: El paquete se le permite pasar sin protección adicional IPsec.
Protect: El paquete es extendido con protección IPsec.

[32]Protocolo IPsec, World Wide Web http://laurel.datsi.fi.upm.es/proyectos/teldatsi/teldatsi/protocolos_de_comunicaciones/protocolo_ipsec. Consultada el 10 de gusto de 2012 10:54am

5. RECOMENDACIONES PARA IPSEC EN IPV6

En la configuración de IPsec la persona encargada de configuración, debe tener un conocimiento avanzado de los estándares RFC a utilizar, para escoger la mejor solución posible para su escenario de red (ya bien sea en modo túnel o de transporte), teniendo en cuenta el hardware que lo soporte, las nuevas tecnologías que se adaptan a él y las políticas de seguridad a tener en cuenta a la hora de implementar.

IPsec es un estándar de seguridad que viene obligatorio en ambientes IPv6, pero es recomendable que se implementen otras medidas de seguridad para la información como firewall, etc., ya que IPsec no es solo la solución de seguridad para prevenir ataques por parte de hackers, que se presenten en el escenario de red que se va a administrar.

Una empresa que necesita seguridad y gran cantidad de servicios en su red, (voz, datos y video) podría utilizar esta tecnología como una opción de seguridad, obteniendo una VPN segura y con gran cantidad de servicios.

Es importante efectuar la debida verificación de IPsec en ambientes IPv6, cuando se configura este protocolo en cada uno de los router, y realizar las pruebas de intercambio de información entre ambos puntos de la red, para monitorear si efectivamente se estableció el protocolo IPsec en ambientes IPv6.

6. CONCLUSIONES

IPsec en ambientes IPv6 es seguro si se cumplen los estándares RFC 4301 y 4309 (Tercera generación actualizada para IPsec) de la IETF en la configuración, ya que estos estándares dan soporte a los protocolos AH, ESP y a los algoritmos de encriptación dando una guía de soporte para configurar enlaces de red en el manejo de la información ya sea en modo túnel o de transporte.

IPv6 fue creado debido al agotamiento de las direcciones IPv4, pero en este nuevo protocolo se corrigieron algunos errores que venían de su antecesor, como la seguridad, en IPv4 se usaba IPsec pero debía ser implementado, en IPv6 IPsec ya viene nativo y es uno de los diferentes protocolos que utiliza IPv6. El conjunto de protocolos y algoritmos que conforman a IPsec, permiten habilitar un sistema seguro, seleccionando los protocolos y algoritmos de seguridad necesarios, dependiendo del modo de uso de IPsec (modo túnel o transporte).

Este documento proporciona una guía básica y directiva para la configuración e implementación de IPsec en IPv6 empleando algoritmos de encriptación y de autentificación. El lector debe seguir todos los procedimientos de seguridad y directivas descritas en la Arquitectura de Seguridad, Protocolo ESP, Protocolo AH, y los algoritmos de autentificación y encriptación.

IPsec es un protocolo que está sobre la capa del protocolo de Internet (IP), dicha tecnología le permite a dos o más equipos comunicarse de forma segura).IPsec consta de tres sub-protocolos:

- Encapsulated Security Payload (ESP), que protege los datos del paquete IP de interferencias de terceros, cifrando el contenido utilizando algoritmos de criptografía simétrica (como Blowfish, 3DES).
- Authentication Header (AH), que protege la cabecera del paquete IP de interferencias de terceros así como contra la falsificación (“spoofing”), calculando una suma de comprobación criptográfica y aplicando a los campos de cabecera IP una función hash segura. Detrás de todo esto va una cabecera adicional que contiene el hash para permitir la validación de la información que contiene el paquete.
- Un protocolo de gestión de clave criptográfica: el denominado ‘intercambio de claves por Internet (IKE), que se utiliza para negociar las conexiones IPsec.

ESP y AH pueden utilizarse conjunta o separadamente, dependiendo del entorno.

IPsec puede utilizarse para cifrar directamente el tráfico entre dos equipos (modo de transporte) o para construir “túneles virtuales” entre dos subredes, que pueden

usarse para comunicación segura entre dos redes corporativas (modo de túnel). Llamándose así una red privada virtual (Virtual Private Network, o VPN)

Utilizando un túnel VPN con IPsec en IPv6, representa una solución favorable y confiable para las empresas que solicitan este servicio. La complejidad de IPsec es alta, debido a su encriptación y autenticidad que brinda en las VPNs.

En la configuración de IPsec en ambientes IPv6 se puede especificar el tráfico que se va encriptar como por ejemplo voz, video y datos. Los resultados obtenidos por el protocolo IPsec en ambientes IPv6 demuestran que son muy estables en el intercambio de información por su integridad, confidencialidad, autenticidad y calidad de envió de información transmitida a través de Internet, proporcionando así una alta seguridad en el escenario de red.

Se puede concluir que la mejor forma de usar IPsec, de modo túnel debido al alto grado de encriptación que se necesita para que los datos se autentiquen de un extremo a otro de forma segura, ya bien sea una red en IPv4 con un túnel elaborado en IPv6.

BIBLIOGRAFIA

Algorithms for Internet Key Exchange version 1 (IKEv1, Network Working Group, P. Hoffman, and Request for Comments: 4109. VPN Consortium Updates: 2409. Category: Standards Track. World Wide Web http://www.IETF.org/rfc/rfc4109.txt, consultada el 15 de junio de 2012 2:28pm, [20]

ANÁLISIS DEL PROTOCOLO IPsec EN AMBIENTE IPv6, Sandoval Carrillo Sandra Milena
http://www.unipamplona.edu.co/unipamplona/hermesoft/portalIG/home_1/recursos/tesis/contenidos/pdf_tesis/pdf_2/02052007/analisis_del_protocolo_IPsec.pdf, consultada el 18 de junio de 2012 a las 2:35pm, [5]

Cryptographic Suites for IPsec, Network Working Group, P. Hoffman
Request for Comments: 4308, VPN Consortium Category: Standards Track. World Wide Web http://www.IETF.org/rfc/rfc4308.txt, consultada el 15 de junio de 2012 2:36pm [23]

CRIPTOLOGÍA, Escuela universitaria Politécnica de Mataró, Manuel Pons Martorell.
http://www.tierradelazaro.com/public/libros/cripto.pdf Visitada el 15-6-2012 a las 10:30 a.m. [2]

Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers, Network Working Group, K. Nichols Request for Comments: 2474 Cisco Systems Inc. S. Blake Category: Standards Track. Cisco Systems Inc., D. Black. EMC Corporation. World Wide Web http://www.IETF.org/rfc/rfc2474.txt, consultada el 15 de junio de 2012 2:25pm [18]

Dynamic Authorization Extensions to Remote Authentication Dial in User Service (RADIUS), Network Working Group, M. Chiba, Request for Comments: 3576, G. Dommety, Category: Informational, M. Eklund. Cisco Systems, Inc., D. Mitton, Circular Logic, UnLtd, B. Aboba. Microsoft Corporation. World Wide Web http://www.IETF.org/rfc/rfc3576.txt, consultada el 15 de junio de 2012 2:27pm [19]

Hacking IPv6 II – Interceptación de tráfico mediante envenenamiento de caché (MITM) – (1ª parte)
http://www.iniqua.com/2011/03/18/hacking-IPv6-ii-interceptacion-de-trafico-mediante-envenenamiento-de-cache-mitm-1%C2%AA-parte/
Consultada el 20 de junio de 2012 a las 10:00am [9]

Implementing IPsec in IPv6 Security
http://www.cisco.com/en/US/docs/ios/IPv6/configuration/guide/ip6-IPsec.html, visitada el 23 de junio de 2012 **[26]**

Internet Key Exchange (IKEv2) Protocol, Network Working Group, C. Kaufman, Ed. Request for Comments: 4306, Microsoft Obsoletes: 2407, 2408, 2409, Category: Standards Track. World Wide Web http://tools.IETF.org/html/rfc4306, consultada el 15 de junio de 2012 2:32pm [22]

Internet Key Exchange Protocol Version 2 (IKEv2), Internet Engineering Task Force (IETF) C. Kaufman, Request for Comments: 5996, Microsoft Obsoletes: 4306, 4718, P. Hoffman Category: Standards Track. VPN Consortium
ISSN: 2070-1721, Y. Nir, P. Eronen. World Wide Web http://tools.IETF.org/html/rfc5996, visitada el 10 de agosto de 2012 2:50pm [24]

Internet Protocol, Version 6 (IPv6) specifications, Network Working Group. S. Deering Request for Comments: 2460, Cisco Systems Inc., R. Hinden, Category: Standards Track Nokia. World Wide Web http://tools.IETF.org/html/rfc2460, consultada el 15 de junio de 2012 2:24pm [17]

Internet Security Association and Key Management Protocol (ISAKMP)
Network Working Group, D. Maugham, Request for Comments: 2408, National Security Agency, Category: Standards Track, M. Schertler, Security, Inc., M. Schneider, National Security Agency, J. Turner, RABA Technologies, Inc. World Wide Web http://www.IETF.org/rfc/rfc2408.txt, consultada el 15 de junio de 2012 2:15pm [15]

IP Authentication Header, Network Working Group, S. Kent
Request for Comments: 2402, BBN Corp R. Atkinson, Category: Standards Track, World Wide Web http://www.IETF.org/rfc/rfc2402.txt, consultada el 15 de junio de 2012 2:05pm [11]

IP Encapsulating Security Payload (ESP), Network Working Group S. Kent, Request for Comments: 2406, BBN Corp
R. Atkinson, Category: Standards Track, @Home, World Wide Web
http://www.IETF.org/rfc/rfc2406.txt, consultada el 15 de junio de 2012 2:08pm

IPSEC,
http://en.wikipedia.org/wiki/IPsec Visitada el 16-6-2012 a las 12:56 p.m. [3]

IPSEC EN AMBIENTES IPV4 E IPV6
http://francisconi.org/sites/default/files/IPsec_en_Ambientes_IPv4_e_IPv6.pdf
Visitada el 15-6-2012 a las 9:00 a.m. [1]

IPV6 PARA TODOS, Guía de uso y aplicación para diversos entornos. http://www.IPv6tf.org/pdf/IPv6paratodos.pdf, visitada el 20 de junio de 2012 a las 2:10pm **[25]**

IPV6 SUPPORT FOR THE IPSEC VSPA http://www.cisco.com/en/US/docs/ios/IPv6/configuration/guide/ip6-IPsec.html#wp1086601, visitada el 20 de junio de 2012 a las 2:00pm [4]

IPv6 Tunnel through an IPv4 Network http://www.cisco.com/en/US/tech/tk872/technologies_configuration_example09186a00800b49a5.shtml **[27]**

NUEVAS AMENAZAS DE SEGURIDAD EN IPV6, Miguel Ángel Díaz Fernández, Álvaro Vives Martínez, César Olvera Morales http://www.mundointernet.es/IMG/pdf/ponencia162_1.pdf [7]

Security Architecture for the Internet Protocol, Network Working Group, S. Kent, and Request for Comments: 2401, BBN Corp, R. Atkinson Category: Standards Track. World Wide Web http://www.IETF.org/rfc/rfc2401.txt, consultada el 15 de junio de 2012 2:00pm [10]

The Internet IP Security Domain of Interpretation for ISAKMP, Network Working Group, D. Piper Request for Comments: 2407,Network Alchemy, Category: Standards Track, World Wide Web http://www.IETF.org/rfc/rfc2407.txt, consultada el 15 de junio de 2012 2:10pm [14]

The Internet Key Exchange (IKE), Network Working Group, D. Harkins, Request for Comments: 2409, D. Carrel, Category: Standards Track, Systems Inc. World Wide Web http://www.IETF.org/rfc/rfc2409.txt, consultada el 15 de junio de 2012 2:21pm [16]

THE SAFETY ANALYSIS OF IPSEC BASED ON IPV6 PROTOCAL, Hongyan Li, Xueying Zhang, Jiaqi Fan College of Information Engineering of Taiyuan University of Technology Taiyuan [8]

The Use of HMAC-SHA-1-96 within ESP and AH, Network Working Group, C. Madson, Request for Comments: 2404, Cisco Systems Inc. Category: Standards Track, Glenn, World Wide Web http://tools.IETF.org/html/rfc2404, consultada el 15 de junio de 2012 2:07pm [12]

VULNERABILIDADES SOBRE LAS TRAMAS Y PROTOCOLOS, Hidalgo Julio César, Jaramillo Sebastián
http://www.supertel.gob.ec/pdf/Consideraciones%20de%20Seguridad%20para%20Implementacion%20de%20IPv6%20FA.pdf [6]