EVALUACIÓN DEL DESEMPEÑO DE LAS REDES IP CON SERVICIOS DE SEGURIDAD PROPICIADOS POR IPSEC

Isabel Cristina Álvarez Fernández

Juan Pablo Hoyos Sánchez

Documento Final de Trabajo de Grado

Director: Ing. Francisco Javier Terán

Universidad del Cauca

Facultad de Ingeniería Electrónica y Telecomunicaciones

Departamento de Telecomunicaciones

Popayán

2010

TABLA DE CONTENIDO

LISTA DE ANEXOS

CAPITULO I

CONCEPTOS FUNDAMENTALES DE FUNCIONAMIENTO DE IPSEC Y MEDICIÓN DE DESEMPEÑO

1. IPSEC: ARQUITECTURA DE SEGURIDAD PARA EL PROTOCOLO DE INTERNET

1.1 INTRODUCCIÓN

IPsec es el conjunto de protocolos usados para proveer servicios de seguridad en la capa de red del modelo de referencia OSI en ambientes IPv4 e IPv6, [1] creando una frontera entre las interfaces protegidas y no protegidas para aplicar tres posibles opciones a los paquetes que desean cruzarla: descartarlos, permitirles el paso sin protección o proporcionarles servicios de seguridad [2].

IPsec se puede utilizar para proteger el tráfico de seguridad entre dos Hosts, entre dos Pasarelas de Seguridad (*Security Gateways - SG*) o entre una pasarela de seguridad y un host; y puede resguardar la carga útil del paquete IP solamente, la carga útil más algunas partes de la cabecera IP, o el paquete IP completo, dependiendo del modo de operación y el protocolo utilizado.

1.2 SERVICIOS DE SEGURIDAD PARA EL PROTOCOLO DE INTERNET

Los servicios de seguridad que pueden ser proporcionados por IPsec, tal y como se definen en el Glosario de Seguridad de Internet [3] son:

- Control de Acceso: Es la protección de los recursos de un sistema contra accesos no autorizados, un proceso por medio del cual el uso de los recursos de dicho sistema es regulado de acuerdo a una política de seguridad y es permitido solo a entidades (usuarios, programas, procesos, u otros sistemas) autorizadas de acuerdo a dicha política.

- Autenticación: Es el proceso de verificar una identidad afirmada por o para una entidad de un determinado sistema. El proceso de autenticación consiste de dos pasos; en el primero (identificación) se presenta un identificador ante el sistema de seguridad, en el segundo (verificación) se presenta o se genera información de autenticación que corrobore el vínculo entre la entidad y el identificador.

- Integridad: Es la propiedad que indica que los datos no han sido modificados, destruidos o perdidos de manera accidental o no autorizada. Trata de la consistencia de los datos y la confiabilidad en los mismos, no de la información que los datos representan o de la confiabilidad de la fuente.

- Confidencialidad: Garantiza que la información no sea revelada a individuos, entidades o procesos no autorizados, mediante el cifrado de dicha información.

- Antirrepetición: Es una forma parcial de integridad de secuencia que detecta los datagramas duplicados dentro de una ventana determinada; es utilizado contra los ataques de reflexión/reenvío de paquetes, en los cuales una transmisión de datos válida es maliciosa o fraudulentamente repetida, ya sea por el emisor original o por un tercero que intercepte los datos. La prestación de este servicio requiere que la gestión de Asociaciones de Seguridad sea de forma automática y no manual.

- Confidencialidad limitada del flujo de tráfico: Es un servicio de confidencialidad que provee seguridad extra y protege contra los análisis de tráfico, es utilizado contra atacantes que pudieran adivinar el tipo de datos que está siendo enviado a partir de la longitud de los paquetes. Con él se añade relleno extra a los paquetes y se envían paquetes falsos con diferentes longitudes a intervalos aleatorios para ocultar la longitud real de los paquetes.

Adicionalmente, otros procesos pueden hacer uso de IPSec para proporcionar el servicio de No Repudio; sin embargo, este servicio en sí no es prestado por la arquitectura IPSec ni por sus protocolos. El No-Repudio es un servicio de seguridad que provee protección frente a la falsa negación de una entidad de haber estado involucrada en una comunicación, aunque no previene que dicha entidad repudie la comunicación.

Por ejemplo, si un algoritmo de clave pública como RSA es combinado con una función hash como MD5 o SHA para calcular y cifrar con la clave privada del emisor un resumen de mensaje (*Message Digest*) se obtiene una firma digital cifrada; y dado que sólo el emisor conoce su clave privada, no puede repudiar el hecho de que fue él quien envió dicho mensaje firmado.

La solicitud del servicio se debe hacer previamente a la ocurrencia del hecho crítico y cuando éste ocurre la evidencia es generada por un proceso que involucra el potencial repudiador y posiblemente también un tercero. La evidencia entonces es transferida al solicitante o guardada por el tercero para su uso posterior en caso de ocurrir un repudio, ante lo cual dicha evidencia es recuperada del sitio de almacenamiento y verificada para resolver la disputa.

1.3 VISIÓN GENERAL DE IPSEC

Uno de los protocolos pertenecientes a la arquitectura IPsec es la Cabecera de Autenticación o *Authentication Header* (AH), que puede proveer los servicios de integridad sin conexión, autenticación del origen de los datos y protección antirrepetición. [4], [5]. El otro es Encapsulamiento de Seguridad de la Carga Útil o *Encapsulating Security Payload*

(ESP) que además de ser capaz de proporcionar los mismos servicios que AH, presta también el de confidencialidad de los datos. [6] [7].

Externamente, los servicios de distribución automática de claves de seguridad y de negociación de asociaciones de seguridad son prestados por un Protocolo de Gestión de Claves y Asociaciones de Seguridad de Internet (ISAKMP) que provee una plataforma tanto para la autenticación de los pares (entidades) mediante mecanismos como los basados en clave pública DSS y RSA, como para el intercambio de claves que se lleva a cabo mediante protocolos como IKE, Oakley y SKEME. [8], [9].

En el presente capítulo se presenta un panorama general de la Arquitectura IPSec, teniendo en cuenta que aunque se exponen los conceptos y su funcionamiento general tanto en IPv4 como en IPv6, este proyecto se enfoca en el comportamiento de IPSec cuando se está trabajando en IPv4; adicionalmente, se tienen en cuenta los principales aspectos de las dos últimas versiones (2da y 3ra) de la arquitectura aun cuando actualmente la mayoría de las implementaciones utilicen la segunda versión detallada en el RFC2401 y asociados.

Los documentos que describen este conjunto de protocolos se dividen en siete grupos que se muestran en la figura 1.1.

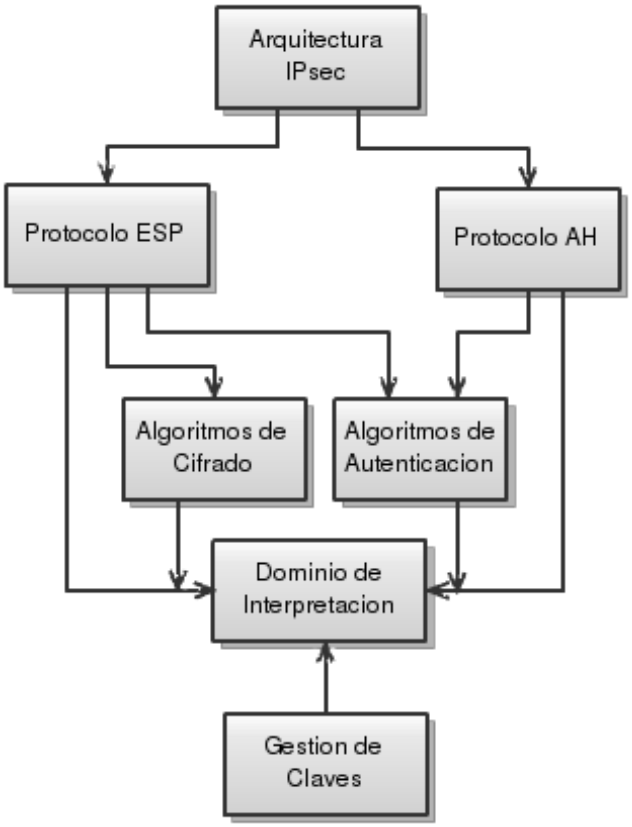


FIGURA 1. 1 ORGANIZACIÓN DE IPSEC [1]

En la Guía De Ruta de IPsec (*IP Security Document Roadmap*) se recomienda que los documentos que describen los algoritmos de autenticación y cifrado incluyan también consideraciones de desempeño, proporcionando algunos datos que se encuentren disponibles, tales como resultados de comparaciones con otros algoritmos, tamaño estándar de los datos de entrada y otros factores que pudieran mejorar o degradar el desempeño del mismo [1].

Sin embargo, aquel tipo de información en casi todos estos RFC es muy limitada o prácticamente inexistente. A manera de resumen, en el Anexo 1 se presenta la información sobre desempeño proporcionada en los documentos descriptivos de aquellos algoritmos relacionados con IPsec.

Aunque la versión 2 de la arquitectura exige el soporte de ambos protocolos, según el RFC 4301 las implementaciones IPsec deben soportar sólo ESP convirtiendo el soporte para AH en un ítem opcional; sin embargo, no se recomienda proveer el servicio de confidencialidad mediante ESP sin prestar también el de integridad. [2], [10]. Asimismo, para la distribución de claves se debe proveer soporte tanto para la configuración manual como para la distribución automática [2].

Se pueden realizar tres tipos de implementación de IPsec: la integración con una implementación nativa IP que requeriría acceso al código fuente IP para *hosts* y *security gateways*, una implementación puesta-en-la-pila (BITS) de protocolos entre el IP nativo y los drivers de red que se emplea generalmente en hosts, y un montaje puesto-en-el-cable (BITW) que utiliza un dispositivo de procesamiento criptográfico externo direccionable a nivel IP y es la implementación típica de una *security gateway* [10].

Adicionalmente, cada protocolo puede ser configurado en dos modos de operación: Transporte y Túnel. En modo transporte se protege únicamente la carga útil del paquete IP mientras que en el modo túnel se protege el paquete IP completo añadiendo una cabecera IP nueva; sin embargo, la cobertura real puede variar dependiendo del protocolo ya que AH puede autenticar también algunas partes de la cabecera cuando trabaja en modo transporte mientras que ESP sólo puede hacerlo en modo túnel.

Al aplicar un protocolo de seguridad en modo transporte, la cabecera AH o ESP es insertada después de la cabecera IP y antes de la cabecera del protocolo de nivel superior o antes de cualquier otra cabecera IPsec que se haya insertado previamente. Su protección abarca la carga útil que sigue a esta cabecera, y en el caso de AH, también los campos de las cabeceras AH e IP que no cambien durante el trayecto.

En modo túnel la cabecera IP interna lleva las direcciones de origen y destino definitivas, mientras un encabezado externo contiene las direcciones de los pares IPsec (por ej., un par de SG); estas direcciones pueden ser una mezcla de IPv4 e IPv6 (IPv4/IPv6 o al contrario). En modo túnel se protege todo el paquete IP interno, incluyendo su cabecera.

Si se requiere fragmentación esta se debe realizar después del procesamiento IPsec, por lo tanto, el modo transporte se aplica sólo a datagramas IP enteros que después pueden ser fragmentados mientras que el modo túnel se aplica a paquetes IP cuya carga útil puede ser un fragmento IP.

Cuando se implementa IPsec en un *host* se deben soportar tanto el modo túnel como el modo transporte, mientras que en una *security gateway* el soporte para modo transporte es opcional dado que se utiliza sólo en los casos en que actúa como un host, por ejemplo, para gestión de red [10] o para prestar seguridad entre dos sistemas intermedios de una ruta [2]. Este requisito de que cualquier SA que involucre a una *security gateway* sea un túnel es para evitar problemas potenciales con la fragmentación y reensamblaje de paquetes IPsec y en circunstancias donde existan múltiples trayectorias para el mismo destino detrás de una *security gateway*.

1.3.1. ASOCIACIONES DE SEGURIDAD (SA)

Una SA es una conexión unidireccional que proporciona servicios de seguridad al tráfico que transporta utilizando AH o ESP, pero no ambos; si se requiere la aplicación de los dos protocolos sobre un flujo de información se deben crear dos o más SAs y combinarlas mediante túneles iterados o adyacencia de transporte.

Según la versión 2 de la arquitectura que aunque fue publicada en 1998 aún se encuentra en la mayoría de las implementaciones, cada Asociación de Seguridad se identifica unívocamente con la terna conformada por la dirección IP del destino, el Índice de Parámetro de Seguridad (SPI) y el identificador del protocolo de seguridad (50 para AH y 51 para ESP). En la versión 3 (año 2005) la identificación se realiza sólo con el SPI, pero una implementación en particular puede utilizar adicionalmente el identificador del protocolo para SA *unicast*.

Si una implementación IPsec soporta *multicast* debe asimismo soportar SAs *multicast*; pero dado que en muchas arquitecturas de este tipo un controlador del grupo (independiente del gestor de claves) asigna unilateralmente el SPI de la SA del grupo pudiendo ser el mismo asignado a una SA *unicast*, se requiere el uso de un algoritmo de demultiplexación capaz de mapear datagramas IPsec entrantes a SAs incluso en caso de presentarse una colisión de SPI [2].

1.3.2. BASES DE DATOS

Para su funcionamiento IPsec requiere de dos bases de datos (tres según la tercera versión de su arquitectura), la Base de Datos de Políticas de Seguridad (Security Policy Database - SPD) que especifica que se debe hacer con cada flujo de tráfico que ingresa o sale y la Base de Datos de Asociaciones de Seguridad (SAD) que contiene parámetros relacionados con cada SA establecida para indicar cómo proteger el tráfico que así lo requiera; la tercera es la Base de Datos de Autorización de Pares (PAD) que provee un vínculo entre un protocolo de gestión de SAs como IKE y la SPD, y que sólo se encontrará en las implementaciones realizadas conforme al RFC 4301.

Dado que las bases de datos deben existir por separado para el tráfico entrante y saliente, el procesamiento de los paquetes que ingresan por una interfaz es diferente a los que salen por la misma. Además, se hace necesario que para cada interfaz que tenga IPsec habilitado haya bases de datos independientes o se incluya una función de selección

explícita para escoger la SPD correcta en base a los datos del paquete, la interfaz de entrada, etc [2].

La SPD se encuentra lógicamente dividida en tres partes SPD-S, SPD-O y SPD-I. La primera de ellas contiene todas las entradas para el tráfico sujeto a la protección de IPsec, SPD-O contiene entradas para todo el tráfico saliente que debe ser descartado o enviado sin seguridad, y SPD-I es aplicada al tráfico de entrada que va a ser pasado sin protección o descartado; sin embargo, si una implementación contiene una sola SPD esta consistirá de las tres partes. En cualquier caso, la SPD es un elemento esencial ya que si un paquete no coincide con ninguna política contenida en ella, el paquete debe descartarse.

La Base de Datos de Autorización de Pares (PAD) es el vínculo entre la SPD y el protocolo de gestión de asociaciones de seguridad. Presta diversas funciones a ambos pares IPsec (iniciador y respondedor) tales como identificar los otros pares o grupos autorizados para comunicarse con dicha entidad IPsec, especificar los protocolos (IKEv1, IKEv2) y métodos utilizados para autenticar los pares (claves pre-compartidas o certificados X.509), proveer los datos de autenticación para cada uno (la clave pre-compartida o la entidad de confianza ante la cual se validará el certificado) y la información para la revisión en listas de certificados revocados si es el caso; además de realizar la localización de pares que se encuentren detrás de una SG y restringir los tipos y valores de Vectores de Inicialización (IV) que puedan ser dados al crear SAs hijas, para evitar que un extremo pueda identificarse como alguien a quien no está autorizado a representar.

En la SAD se encuentran los datos necesarios para aplicar y en el otro extremo retirar la protección IPsec para obtener de nuevo la información de usuario, tales como el SPI, contador del número de secuencia, ventana de antirrepetición, algoritmo de autenticación usado con AH, algoritmos usados con ESP (cifrado, integridad o combinados) y valores relacionados como modos, IVs y llaves; tiempos de vida de las SA (en bytes o tiempo), opciones de desfragmentación y de tratamiento de DSCP.

1.3.3. FUNCIONAMIENTO DE IPSEC

Cuando se desea enviar un paquete el primer paso es consultar la PAD para verificar la identidad del otro extremo de la conexión y su autorización para representar al destinatario, luego se debe consultar la SPD para saber si se debe descartar, enviarlo sin protección o brindarle seguridad; teniendo en cuenta que aunque está establecido que cuando IPsec se implementa y se despliega correctamente no debería ser afectado adversamente el tráfico que no lo emplee para su protección [2], [10], el sólo hecho de tener que realizar esta consulta ya genera un retardo que por mínimo que sea no se hubiera presentado si en aquel punto de la red no hubiera procesamiento IPsec.

En dicha consulta se debe buscar una entrada en la cual los datos del paquete coincidan con los valores de los selectores que son:

- Dirección IP de origen: *unicast*, *anycast*, *broadcast*, rangos de direcciones (usados para que varios *hosts* puedan compartir una única SA) o comodines; para soportar

SAs multicast se debe hacer uso de una SPD de Grupo [2] aunque el RFC2401 no hace esta distinción.

- Dirección IP de destino, bajo las mismas condiciones que la de origen.

- Nombre completo del usuario (usuario@undominio.com), nombre del sistema (nombre completo DNS como host.dominio.com), nombre característico X.500 o una cadena de bytes (el soporte de estos nombres es opcional en sistemas multi-usuario e implementaciones nativas, y no es aplicable a otras implementaciones).

- Protocolos y puertos del nivel superior: número de puerto y de protocolo, valor oculto *OPAQUE* (sólo para IPv6) o cualquiera (comodín).

Si la política especifica que se deben proporcionar uno o más servicios de seguridad, esta entrada definirá también los protocolos de seguridad que se van a emplear, sus modos, opciones de los servicios de seguridad (desfragmentación, mapeo DSCP) y algoritmos a utilizar; vinculando a una o varias SA que en caso de no existir pueden ser creadas o negociadas mediante un protocolo de gestión de SA como IKE, a partir de los valores del paquete. Los parámetros asociados con la SA apropiada están contenidos en la SAD, donde cada una de las entradas es enlazada por entradas en la SPD-S.

Para el tráfico entrante se realiza un proceso inverso, inicialmente el paquete debe ser etiquetado con el ID de la interfaz (física o virtual) por la cual ingreso (si es necesario, para soportar múltiples SPD y sus caches asociados SPD-I), luego el paquete es examinado y si está protegido por IPsec y dirigido al dispositivo local se consulta la SAD para intentar mapearlo a una SA activa, buscando una entrada correspondiente al SPI contenido en el paquete que especificará si se debe aplicar AH o ESP. Para SA *unicast* esta identificación puede realizarse utilizando adicionalmente el ID del protocolo de seguridad mientras que para SA *multicast* la búsqueda se realiza con el SPI y la dirección de destino aunque opcionalmente se puede utilizar también la dirección de origen; además, se debe comparar el paquete con los selectores de entrada identificados en la SAD para verificar que el paquete recibido corresponde a la SA por la cual se recibió.

Si el tráfico no está dirigido al dispositivo local, o si no está protegido aunque éste sea el destino se reenvía a la SPD-I que determinará si el paquete se reenvía a su destino, si debe ser descartado o que acción se debe tomar con él.

En cuanto a los mensajes ICMP el procesamiento es diferente dado que éstos pueden ser básicamente de dos tipos dependiendo de su finalidad (información o de error). Los mensajes ICMP de error (por ejemplo, códigos 3, 11 y 12) se deben tratar según la sección 6.1 del RFC 4301 que indica que aunque lo deseable sería que se descartaran para evitar ataques de Denegación del Servicio (DoS) esto puede llevar a una degradación del servicio debido a fallas en el proceso de mensajes Path-MTU (para determinar el tamaño máximo de paquete que se puede transmitir en la ruta) y redireccionamiento por lo que toda implementación IPsec debe permitir que un administrador local la configure para aceptar o rechazar trafico ICMP no autenticado; mientras que la disposición de los mensajes ICMP que no son de error (por ejemplo, códigos 0, 8, 13 y 14) deben depender de entradas explicitas en la SPD para determinar

si aceptar o rechazar estos mensajes y que acción tomar en caso de aceptarse, asumiendo que este procesamiento de mensajes ICMP tiene lugar en el lado desprotegido de la frontera IPsec. Asimismo, el trafico IKE debe estar explícitamente clasificado para permitirle el paso en la SPD-I.

1.4 PROTOCOLOS DE IPSEC

1.4.1. AH - CABECERA DE AUTENTICACIÓN

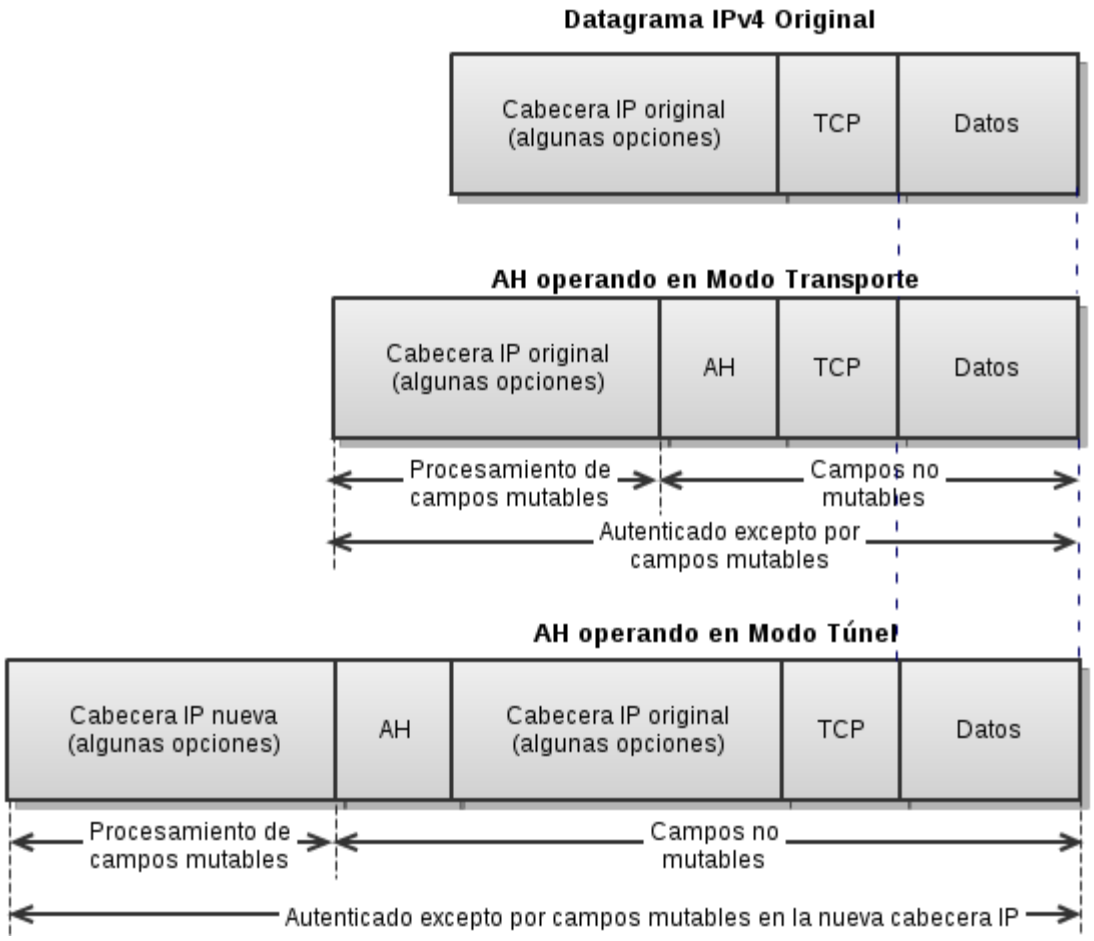


FIGURA 1. 2 ESTRUCTURA DEL DATAGRAMA IP AL APLICAR AH

La Cabecera de Autenticación es un protocolo que se usa para proveer los servicios de integridad sin conexión y autenticación del origen de los datos (conjuntamente llamados "autenticación" o “integridad”) y opcionalmente el de protección antirrepetición, siendo un protocolo apropiado en los casos en que la confidencialidad no sea requerida o permitida. La cobertura de AH está limitada a los campos del paquete IP que no sean mutables en el camino o cuyos valores en recepción sean predecibles, por lo cual la protección proporcionada por AH es por partes.

La estrictez del servicio de autenticación depende de la granularidad de la SA con la cual es empleado AH, teniendo en cuenta que las SA de granularidad fina generalmente son más vulnerables al análisis de tráfico que las SA de granularidad gruesa que llevan tráfico de diversos clientes. Con respecto al servicio de antirrepetición, el emisor automáticamente incrementa el número de secuencia aunque el servicio sólo sea efectivo si el receptor está controlando dicho número de secuencia.

Los campos obligatorios de la cabecera de autenticación son:

- Próxima Cabecera: Campo de 8 bits que identifica el tipo de carga útil después de AH[1].
- Longitud de la carga útil: Campo de 8 bits que especifica la longitud de AH en palabras de 32 bits
- Reservado: campo de 16 bits para uso futuro, debe ser puesto a ceros por el emisor y debe ser ignorado por el receptor.
- SPI: Índice de Parámetros de Seguridad, es un valor arbitrario de 32 bits usado por un receptor para identificar la SA a la que está vinculado un paquete que ingresa (el valor de 0 es reservado para la implementación local y los valores entre 1 y 255 son reservados por IANA). Para SAs *unicast* este valor es generado por el receptor[1].
- Numero de secuencia: De 32 bits, funciona como contador de paquetes por cada SA activa por lo que al prestar el servicio de antirrepetición se debe establecer una nueva SA cada vez que este contador se vaya a desbordar. Si se tienen múltiples emisores sobre una misma SA el servicio de antirrepetición no está disponible debido a que no hay obligación de que los emisores se sincronicen. Para soportar implementaciones IPsec de alta velocidad existe la opción de usar un Numero de Secuencia Extendido (ESN) de 64 bits cuyo uso es negociado por un protocolo de gestión de SAs, mediante el cual sólo se transmiten los 32 bits de menor peso pero tanto emisor como receptor mantienen la secuencia y realizan el cálculo del ICV con los 64 bits[1].
- ICV (*Integrity Check Value*): El Valor de Chequeo de Integridad es un número de 32 bits para verificar que los datos no hayan sido modificados durante la ruta del paquete. Si un campo es mutable y no predecible se pone a cero para el cálculo del ICV, pero si su valor al llegar al destino es predecible se inserta este para calcular el ICV.

1.4.2. ESP - ENCAPSULAMIENTO DE SEGURIDAD DE LA CARGA ÚTIL

Este protocolo puede proveer los servicios de confidencialidad, autenticación del origen de los datos, integridad sin conexión, antirrepetición y confidencialidad limitada del flujo de tráfico.

Los servicios de autenticación del origen de los datos y de integridad sin conexión fueron denominados conjuntamente como "autenticación" [10] y más adelante como "integridad" [7] debido a que los cálculos ejecutados proveen directamente integridad, mientras que la autenticación es el resultado indirecto de vincular la clave usada para integridad a la identidad del otro dispositivo IPsec; típicamente, este vínculo se efectúa mediante el uso de una clave simétrica compartida.

[1] Estos campos también se encuentran en la cabecera de ESP de la misma forma y con la misma función.

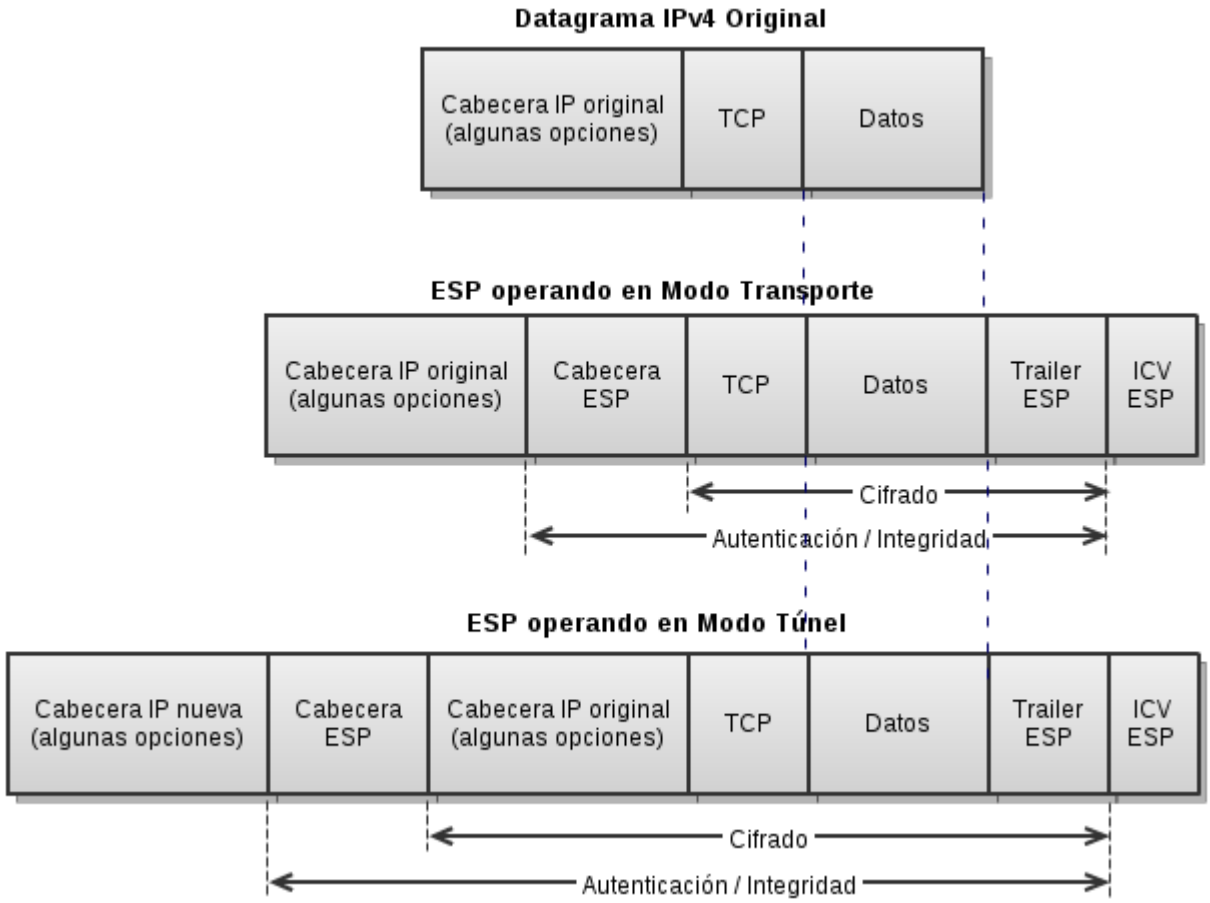


FIGURA 1. 3 ESTRUCTURA DEL DATAGRAMA IP AL APLICAR ESP

La principal diferencia entre la autenticación provista por AH y la que proporciona ESP es el alcance de la cobertura, ya que ESP no protege ninguno de los campos de la cabecera IP a menos que esos campos estén encapsulados por él, haciendo su alcance menor ya que AH sí puede autenticar una cabecera IP externa (sin encapsularla); sin embargo, si sólo se requiere autenticación para los protocolos de nivel superior sería más apropiado utilizar este servicio también con ESP dado que es más eficiente que el uso de ESP encapsulado dentro de AH.

Si una SA indica el uso de ESP se debe proporcionar al menos integridad o confidencialidad, siendo el otro servicio opcional. El uso de sólo-cifrado para proporcionar confidencialidad es permitido por ESP aunque sólo provea protección ante atacantes pasivos ya que el uso de cifrado sin un mecanismo fuerte de protección de integridad puede hacer inseguro el servicio de confidencialidad frente a algunas formas de ataques activos; más aún, un servicio de integridad como AH, aplicado antes del cifrado no necesariamente protege la confidencialidad de sólo-cifrado ante atacantes activos. ESP permite SAs de sólo-cifrado porque pueden ofrecer un desempeño considerablemente mejor y aun proveer un nivel de seguridad adecuada, por ejemplo, cuando la autenticación/integridad de los niveles superiores es ofrecida independientemente.

El soporte de solo-confidencialidad es opcional, mientras que el de confidencialidad con integridad y el de solo-integridad son obligatorios; éste último debido a que en muchos contextos proveer integridad de dicha forma es más atractivo que con AH al hacer el

procesamiento más rápido y más susceptible de canalización en muchas implementaciones. Adicionalmente, el servicio de antirrepetición puede ser seleccionado para una SA solo si se selecciona también el servicio de integridad para dicha SA con el fin de garantizar la protección del número de secuencia.

La confidencialidad del flujo de tráfico (TFC) generalmente es efectiva solo si ESP es empleado en una forma que concierna las direcciones definitivas de origen y destino (en modo túnel serían las de las SG) y si hay suficiente tráfico entre los dos (naturalmente o generado para enmascarar tráfico) para ocultar las características de los flujos de tráfico específicos de los suscriptores individuales. Si se está haciendo uso del modo túnel, la implementación IPsec puede añadir relleno para TFC después de la carga útil y antes del campo de relleno.

Si en el campo de la carga útil, entre la información de sincronización criptográfica se encuentra un IV (vector de inicialización), éste no va cifrado, aunque comúnmente se refiera a él como parte del texto cifrado. Asimismo, otros aspectos pueden variar dependiendo de si se utiliza un sólo algoritmo combinado para proveer integridad y cifrado, o si se utilizan algoritmos por separado para proveerlos.

Hay algoritmos combinados que proveen integridad también a los datos que viajan en texto plano mientras que otros solo protegen la integridad de los campos cifrados. Debido a que los campos de SPI y Número de Secuencia requieren integridad como parte de dicho servicio, si el algoritmo combinado no se los proporciona y no van cifrados, se debe asegurar que reciban el servicio siempre que sea seleccionado, sin importar el estilo del algoritmo combinado utilizado.

Si se usa un algoritmo de integridad por separado, los 32 bits de mayor peso del ESN se incluyen en el tráiler ESP pero no se transmiten; de forma análoga a los bits de relleno del algoritmo de cifrado. Si se usa un algoritmo combinado, es él quien determina si los 32 bits de mayor peso del ESN son transmitidos o se incluyen implícitamente en el cálculo.

El ICV no siempre aparece ya que solo se usa cuando se provee el servicio de integridad. Éste cálculo de integridad se realiza con los valores de SPI, NS, datos de la carga útil y tráiler ESP (implícito y explícito); teniendo en cuenta que el tráiler ESP transmitido (explícito) consta del relleno, longitud del relleno y campos de próxima cabecera mientras que el tráiler implícito (que no se transmite) contiene los 32 bits de mayor peso del ESN si es el caso.

1.5 GESTIÓN DE CLAVES Y ASOCIACIONES DE SEGURIDAD

Los protocolos AH y ESP son independientes de las técnicas de gestión de asociaciones de seguridad, aunque algunas de ellas afectan los servicios de seguridad prestados por IPsec, por ejemplo, el servicio de antirrepetición tanto en AH como en ESP requiere gestión automática de SA; más aún, la granularidad de la distribución de claves empleada por IPsec determina la granularidad de la autenticación provista.

El método más sencillo es gestionar las claves manualmente y para entornos pequeños y estáticos es una buena técnica que permitiría que una SG se comunique con otros sitios internos y externos con una clave configurada manualmente, sin embargo, no es una solución escalable. En entornos más amplios y para soportar los servicios de antirrepetición y creación de SAs bajo demanda se requiere que la administración de SA se haga de forma automática mediante un protocolo de gestión de claves, por defecto IPsec utiliza IKEv2 para

las implementaciones compatibles con el RFC 4301 e ISAKMP con IKEv1 para las anteriores; aclarando que no hay interoperabilidad entre las dos versiones de IKE.

Para los aspectos de descubrimiento de rutas a otros hosts detrás de SGs, su autenticación y la verificación de la autoridad de las SG para representar a dichos hosts se requiere que la implementación provea una interfaz administrativa para configurar esta información manualmente.

1.5.1. INTERNET SECURITY ASSOCIATION AND KEY MANAGEMENT PROTOCOL - ISAKMP

El Protocolo de Gestión de Llaves y Asociaciones de Seguridad de Internet nace como respuesta a la evidente necesidad de un protocolo que negocie, establezca, modifique y elimine asociaciones de seguridad y sus atributos, además de soportar la generación de claves públicas. Asimismo, al ser destinado a soportar la negociación de SAs para protocolos de seguridad en todas las capas de la pila de red, ISAKMP define procedimientos para realizar la autenticación del otro equipo (*peer*) que desea comunicarse, creación y gestión de SAs, técnicas de generación e intercambio de claves y mitigación de amenazas tales como ataques de DoS, reenvío/reflexión de paquetes, hombre-en-el-medio y secuestro de la conexión.

ISAKMP difiere de los protocolos de intercambio de claves debido a que separa claramente los detalles de la gestión de SAs (y de gestión de claves) del intercambio de claves; y con el fin de facilitar una migración progresiva hacia mejores mecanismos y algoritmos establece que las SAs deben soportar diferentes algoritmos de cifrado, mecanismos de autenticación y algoritmos de establecimiento de claves, así como el uso de certificados orientados a host para los protocolos de capas inferiores y orientados a usuario para los de capas superiores [8].

Una SA de ISAKMP es, asimismo, diferente de otros tipos de SAs y se identifica mediante dos campos de cookies en su cabecera. Al inicio del proceso de establecimiento de una SA ISAKMP un extremo asume el rol de iniciador y otro el de respondedor; una vez se ha establecido la SA cualquiera de los dos puede iniciar una negociación en la siguiente fase, haciendo las SAs ISAKMP bidireccionales por naturaleza.

El protocolo ISAKMP puede ser implementado sobre cualquier protocolo de transporte o sobre el mismo IP, pero dado que todas las implementaciones deben ser capaces de enviar y recibir usando el puerto 500 sobre UDP que ha sido asignado por IANA, éste es el comportamiento por defecto en la mayoría de ellas en la actualidad.

A. FASES DE NEGOCIACIÓN DE ISAKMP

ISAKMP permite asegurar el canal de comunicación entre las entidades negociantes al acordar un conjunto de atributos de seguridad que provean protección para los intercambios subsecuentes, indicando también el método de autenticación y de intercambio de llaves que serán utilizados como parte de ISAKMP; para posteriormente establecer una o más SA en nombre de otro protocolo como AH o ESP.

Este enfoque de dos fases puede parecer de alto costo, pero ofrece grandes ventajas ya que el costo de la primera fase se ve amortizado cuando se requiere establecer varias negociaciones de segunda fase y al realizar actividades de gestión de SAs como el restablecimiento al presentarse errores y eliminación de las mismas sin tener que empezar desde cero. Además, los servicios negociados durante la primera fase proveen propiedades de seguridad para la segunda fase, por ejemplo, el cifrado proporcionado por la SA ISAKMP puede proveer protección de la identidad permitiendo negociaciones de segunda fase más simples; mientras que si el canal establecido en la primera fase no provee este servicio tendría que negociarse en la segunda fase.

B. MECANISMOS DE AUTENTICACIÓN

Los mecanismos de autenticación caen en dos categorías de fortaleza: débiles y fuertes. El envío de claves u otra información de autenticación en texto plano es débil debido al riesgo de ser leídos con un analizador de protocolos, adicionalmente, enviar mensajes hash unidireccionales y claves pobremente escogidas también caen en esta categoría debido al riesgo de los ataques de adivinación por fuerza bruta en los mensajes capturados.

Se requiere un mecanismo de autenticación fuerte para los intercambios ISAKMP, ya que sin autenticación se es incapaz de confiar en la identificación de una entidad, lo que hace el control de acceso cuestionable.

ISAKMP utiliza principalmente firmas digitales basadas en criptografía de clave pública para autenticación, aunque también puede haber otros mecanismos de autenticación fuertes que pueden ser especificados adicionalmente como opcionales. Además, aunque dentro de los componentes de autenticación de ISAKMP debe ser usado un algoritmo de firmas digitales, ISAKMP no impone ningún algoritmo de firmas ni autoridad certificadora (CA) especifica. En cambio, permite que una entidad inicie comunicaciones especificando que CAs soporta, y después de la selección de SA el protocolo provee los mensajes requeridos para soportar el intercambio de la información de autenticación en sí.

La Criptografía de Clave Pública es la forma más flexible, escalable y eficiente para que los usuarios obtengan las claves compartidas y las llaves de sesión necesarias para soportar la gran cantidad de formas en que los usuarios de Internet interoperan. Las propiedades de los protocolos de intercambio de claves incluyen los métodos de establecimiento de claves, autenticación, simetría y secreto perfecto a futuro (*perfect forward secrecy*).

Las firmas digitales, tales como el Estándar de Firma Digital o Digital Signature Standard (DSS) y las firmas Rivest-Shamir-Adleman (RSA) son mecanismos de autenticación fuertes basados en clave pública; este tipo de autenticación requiere que cada entidad posea una clave pública y una clave privada. Los certificados son una parte esencial en los mecanismos de autenticación por firmas digitales ya que son los que enlazan la identidad de una entidad específica a sus claves públicas y posiblemente a otra información relacionada con la seguridad tal como privilegios y permisos. La autenticación basada en firmas digitales requiere un tercero de confianza o Autoridad Certificadora para generar, firmar y distribuir apropiadamente los certificados.

Las Autoridades Certificadoras requieren una infraestructura para la generación, verificación, revocación, gestión y distribución. Para dirigirla la IETF ha establecido la Autoridad de Registro de Políticas de Internet (IPRA) como se muestra en la figura 1.4,

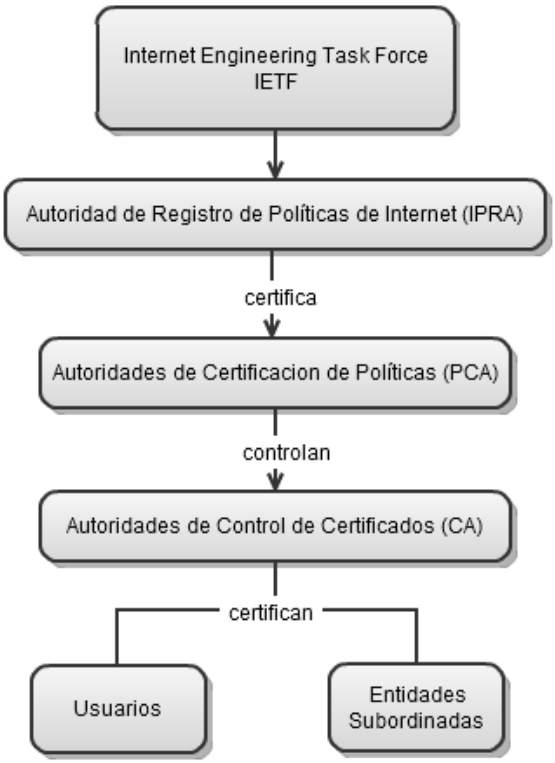


FIGURA 1. 4 JERARQUÍA DE ENTIDADES DE CERTIFICACIÓN

Alternativamente, si no existe una infraestructura, los certificados de la Web de Confianza PGP (PGP- Web-of-Trust) pueden ser usados para proveer autenticación de usuario y privacidad en una comunidad de usuarios que se conocen y confían en los demás.

El nombre de una entidad es su identidad y está ligado a sus claves públicas en los certificados. Los nombres asociados con las claves son direcciones IP y nombres de dominio que tienen significado para entidades que acceden al DNS para obtener esta información, cuando se establecen Webs de Confianza los nombres que se vinculan a las claves públicas usualmente son e-mails y tienen significado sólo para aquellos que entienden e-mail; sin embargo otras Webs de Confianza pueden utilizar otro esquema de nombrado completamente diferente.

C. INTERCAMBIO DE CLAVES

Para realizar el establecimiento de claves los dos métodos comunes en criptografía de clave pública son la generación de claves y el transporte de claves. Un ejemplo de transporte de claves es el uso del algoritmo RSA para cifrar una llave de sesión generada aleatoriamente con la clave pública del receptor que luego se le envía para que la descifre con su clave privada;

éste método impone menos sobre-encabezado computacional debido a que la clave se genera a partir de información de un solo extremo de la comunicación.
En cuando a la generación de claves, un ejemplo común es el algoritmo Diffie-Hellman en el cual dos usuarios inician intercambiando información pública, cada usuario combina matemáticamente la información pública del otro con su propia información privada para calcular una clave secreta compartida que puede ser usada como clave de sesión o para cifrar una clave de sesión generada aleatoriamente. La ventaja de este método es que la clave generada está basada en información de ambos usuarios y la independencia de una clave de intercambio a otra provee secreto perfecto a futuro.

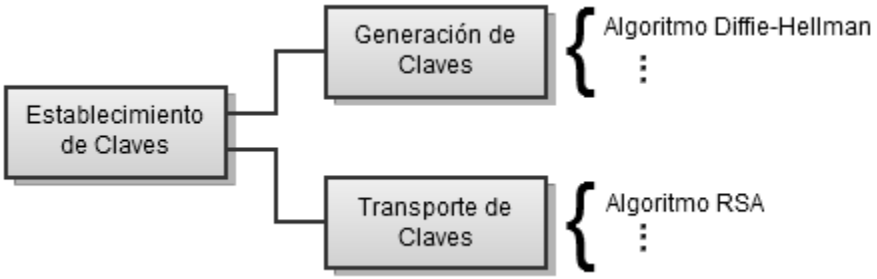


FIGURA 1. 5 ESTABLECIMIENTO DE CLAVES EN CRIPTOGRAFÍA DE CLAVE PÚBLICA

D. PAYLOADS ISAKMP

Para los mensajes de negociación, después de un encabezado de formato fijo pueden ir diferentes tipos de payloads o unidades de información. Cada uno de ellos va precedido por un payload genérico que permite enlazarlos y define los límites de cada payload.

- El payload de Asociación de Seguridad es usado para negociar atributos de seguridad y para indicar el Dominio de Interpretación (DOI) y la situación bajo la cual está tomando lugar la negociación.

- El payload de propuesta (proposal) contiene información usada durante la negociación de la SA. La propuesta consiste de los mecanismos de seguridad o transformadas a ser utilizadas para asegurar el canal de comunicación

- El payload de transformada (transform) contiene información usada durante la negociación de la SA y consiste de un mecanismo de seguridad especifico (por ejemplo, un algoritmo) o transformada para asegurar el canal.

- El payload de intercambio de llave (key exchange) soporta varias técnicas de intercambio tales como Oakley, Diffie-Hellman y RSA, entre otros.

- El payload de identificación contiene datos específicos del DOI usados para intercambiar información de identificación que es utilizada para determinar las identidades de las entidades comunicantes y puede ser utilizada para determinar la autenticidad de la información.

- El payload de solicitud de certificado y el payload de certificado proveen un medio para solicitar la información de certificación, y para transportar los certificados y otra información relacionada a través de ISAKMP respectivamente, y pueden aparecer en cualquier mensaje ISAKMP.

- El payload de hash contiene datos generados por la función hash (seleccionada durante el intercambio del establecimiento de SA) sobre alguna parte del mensaje o estado ISAKMP. Esta información puede ser usada para verificar la integridad de los datos en un mensaje ISAKMP o para autenticación de las entidades negociantes

- El payload de firma contiene datos generados por la función de firma digital, esta información es utilizada para verificar la integridad de los datos en el mensaje ISAKMP y puede ser usada para el servicio de no-repudio.

- El payload "Nonce" ("*mientras-tanto"*) contiene datos aleatorios para garantizar que el intercambio sigue activo y protegerlo ante ataques de reenvío de mensajes.

- El payload de notificación es usado para transmitir datos de información, tales como condiciones de error, a la otra entidad ISAKMP. Por otra parte, el payload de eliminación contiene un identificador especial para indicar que la SA ha sido eliminada de su SAD y que por lo tanto no es válida en adelante.

También existe un payload de fabricante "Vendor" que permite reconocer una instancia remota de sus implementaciones y experimentar con nuevas funcionalidades manteniendo compatibilidad hacia atrás.

E. TIPOS DE INTERCAMBIO ISAKMP

El tipo de intercambio dicta la estructura y el orden de los payloads (campos de carga útil) ISAKMP. Un mensaje de establecimiento de SA consiste de un sólo payload de SA seguido de por lo menos uno, (y posiblemente muchos) payload de propuesta; y al menos un payload de transformada (aunque pueden ser muchos) asociados con cada uno de los payload de propuesta.

Adicionalmente, para modificar una SA ya establecida, ISAKMP utiliza la política de "Creación de una nueva SA seguida de la eliminación de la SA anterior".

- Intercambio Base: Está diseñado para permitir que la información relativa a la autenticación y al intercambio de llaves se transmita a la vez. Esto implica un número pequeño de mensajes a expensas de no proveer protección de la identidad.

- Intercambio de Protección de la Identidad o Modo Principal (IKE): Separa la información de intercambio de llaves de la información relativa a la identidad y su autenticación. Esto provee protección de ambas identidades ya que son intercambiadas bajo la protección de una clave pre-compartida, a expensas de dos mensajes adicionales, es el tipo de intercambio que provee mayor seguridad y la estructura de su mensaje inicial de establecimiento sería como se muestra en la figura 1.6 a continuación:

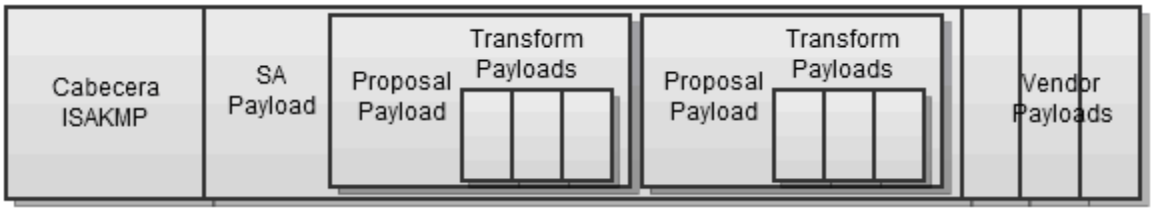


FIGURA 1. 6 PAQUETE EN MODO PRINCIPAL (IKE) O DE PROTECCIÓN DE LA IDENTIDAD (ISAKMP)

- Intercambio de Sólo Autenticación: En él solo la información relativa a autenticación es transmitida y presenta el beneficio de permitir la autenticación sin el costo computacional de calcular claves. Al utilizar este intercambio durante la negociación ninguna de la información que se transmita será cifrada, sin embargo, puede ser cifrada en otros lugares.

- Intercambio Agresivo: Permite que los payload relativos a la SA, intercambio de llaves y autenticación sean transmitidos a la vez, esto reduce el número de mensajes a expensas de no proveer protección de la identidad y de ofrecer sólo un payload de propuesta y uno de transformada. Debido a la naturaleza del presente trabajo de grado este fue el tipo de intercambio seleccionado, ya que no se deseaba negociación de algoritmos y/o protocolos sino una única opción para cada prueba como se indica en la figura 1.7:

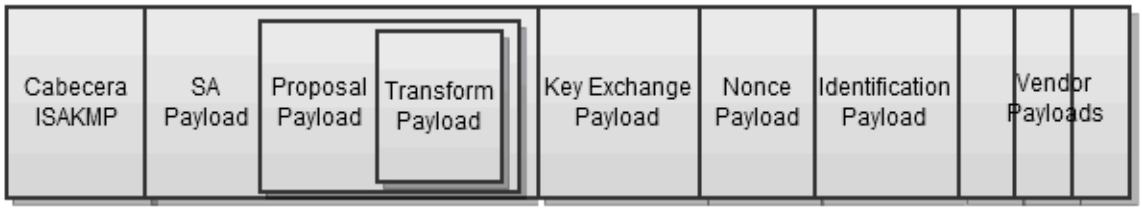


FIGURA 1. 7 PAQUETE EN MODO AGRESIVO

- Intercambio de Información: Está diseñado para una transmisión unidireccional de información que puede ser usada para gestión de SAs.

1.5.2. INTERNET KEY EXCHANGE - IKE

A. IKE-v1

Mientras que ISAKMP provee una plataforma para autenticación e intercambio de claves sin especificar ningún protocolo de intercambio, IKEv1 define un protocolo de intercambio de claves que nace de la combinación de Oakley y SKEME en conjunto con ISAKMP para la obtención de material de autenticación y claves.

Oakley describe una serie de intercambios de llaves llamados "modos" y los servicios provistos por cada uno tales como secreto perfecto a futuro, protección de la identidad y autenticación.

SKEME describe una técnica de intercambio de claves versátil que provee anonimato, repudiabilidad y regeneración rápida de claves.

Mientras Oaklye define "modos", ISAKMP define "fases"; la relación entre ellas es muy directa e IKE presenta diferentes intercambios como modos que operan en una de las dos fases.

En la fase 1 es donde los dos terminales ISAKMP establecen un canal autenticado y seguro con el cual comunicarse, esto es llamado SA ISAKMP. El "modo principal" (main mode) y el "modo agresivo" (aggressive mode) logran esto en un intercambio de primera fase, teniendo en cuenta que el modo principal provee protección de la identidad mientras que el modo agresivo requiere un menor número de mensajes. En esta parte es necesario definir el algoritmo de cifrado y de hash, el método de autenticación y la información del grupo Diffie-Hellman.

En la fase 2 es donde se negocia una SA en representación de otros protocolos como los de IPsec, que necesiten negociación de claves y/o parámetros. El "modo rápido" logra esto en un intercambio de segunda fase.

El Modo de Nuevo Grupo no es por sí mismo de fase 1 o fase 2. Se utiliza posteriormente a la fase 1 y sirve para establecer un nuevo grupo que puede ser usado en negociaciones futuras.

El Modo Principal es una instancia del Intercambio de Protección de la Identidad de ISAKMP; los dos primeros mensajes negocian la política, los dos siguientes intercambian los valores públicos de Diffie-Hellman y datos auxiliares y los dos últimos autentican el intercambio Diffie-Hellman.

De forma similar, el modo agresivo es una instancia del Intercambio Agresivo de ISAKMP; los dos primeros mensajes negocian la política, intercambian los valores públicos de Diffie-Hellman y datos auxiliares y las identidades; adicionalmente el segundo mensaje autentica el respondedor. El tercer mensaje autentica el iniciador y provee prueba de su participación en el intercambio.

B. IKE-v2

La segunda versión de la especificación de IKE no es interoperable con la versión 1, pero tienen suficiente de la cabecera en común como para que las dos versiones pueden correr sobre el mismo puerto UDP sin ambigüedades.

IKEv2 fue realizada con el fin de definir enteramente el protocolo, incorporando los contenidos de lo que eran previamente documentos separados como ISAKMP [8], IKE [9], el Dominio de Interpretación de Internet [11], Traducción Transversal de Direcciones de Red (NAT-Transversal), Autenticación Heredada, Adquisición de Direcciones Remotas y Autenticación Extensible; y de simplificar IKE reemplazando todos los intercambios iniciales con un solo tipo de intercambio.

Asimismo, se buscaba reducir la latencia de IKE en el caso común haciendo que el intercambio inicial fuera de tan sólo dos viajes en redondo (4 mensajes) y permitiendo la posibilidad de transportar la configuración de una SA_Hija en ese intercambio, y otras mejoras que pueden ser consultadas en la especificación de IKEv2 [12].

El flujo de mensajes IKE consiste de una solicitud (*request*) seguida de una respuesta (*response*), donde es responsabilidad del solicitante asegurar la fiabilidad de la transmisión.

La primera solicitud/respuesta de una sesión IKE (*IKE_SA_INIT*) negocia parámetros de seguridad para la *IKE_SA*, envía "*nonces"* y los valores para Diffie-Hellman; mientras que la segunda solicitud/respuesta (*IKE_AUTH*) transmite las identidades, prueba el conocimiento de los secretos correspondientes a las dos identidades y establece una SA para la primera (y a menudo la única) SA_Hija de AH o ESP.

Los tipos de intercambios subsecuentes son CREATE_CHILD_SA para crear asociaciones de seguridad derivadas e INFORMATIONAL para eliminar asociaciones de seguridad, reportar errores y realizar tareas de mantenimiento [12].

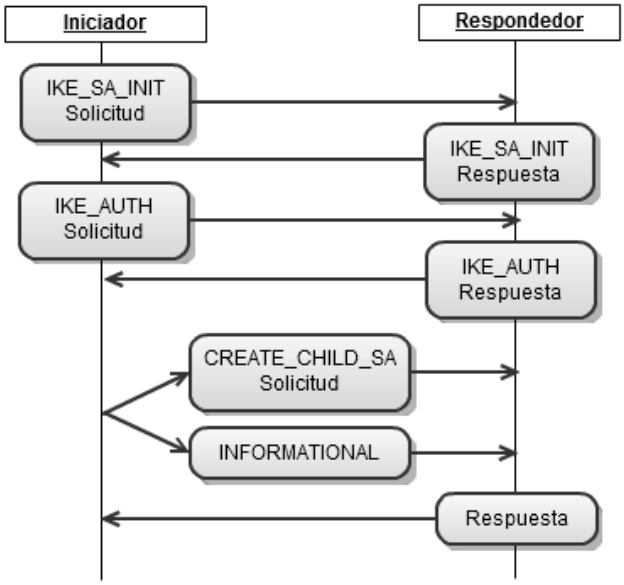


FIGURA 1. 8 INTERCAMBIO DE MENSAJES EN IKEV2

2. ALGORITMOS DE AUTENTICACIÓN Y CIFRADO

2.1 CRIPTOLOGÍA

Su nombre deriva de las palabras griegas *krypto* (oculto) y logos (estudio). Esta ciencia aplicada se encarga del estudio de los sistemas que ofrecen seguridad en medios de comunicación en los que un emisor oculta o cifra un mensaje antes de transmitirlo para que sólo un receptor autorizado pueda descifrarlo. Sus áreas principales de estudio son la criptografía, que es el arte de esconder el significado de las palabras de un mensaje cifrándolas, y el criptoanálisis, que es la ciencia de obtener la información original en ausencia de las claves rompiendo la seguridad proporcionada; aunque también se incluye la esteganografía como parte de la criptología.

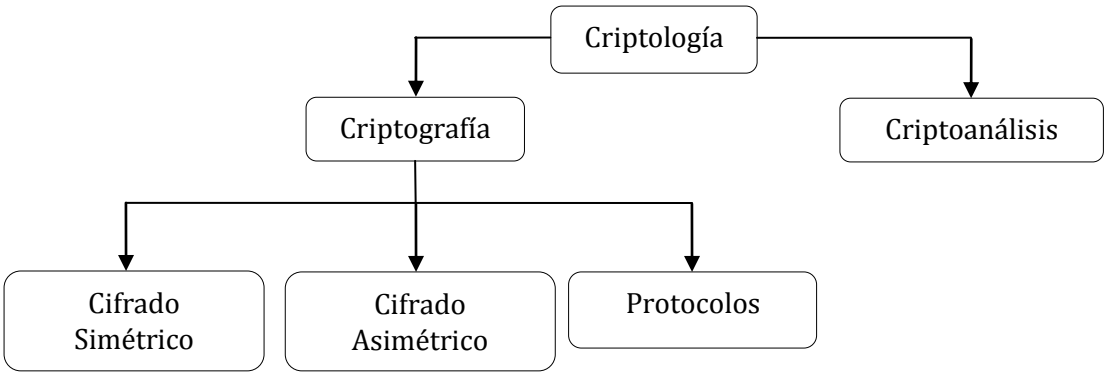


FIGURA 1. 9 CRIPTOLOGÍA

El cifrado es el proceso por el cual un mensaje en texto plano o legible se convierte en un mensaje ilegible o texto cifrado.

2.2 CIFRADO SIMÉTRICO

En los sistemas que utilizan cifrado simétrico se cuenta con una sola llave tanto para cifrar como para descifrar, esta debe ser conocida en el transmisor y en el receptor, por lo que generalmente se le llama *llave privada*. El esquema del proceso de cifrado simétrico se muestra en la figura 1.10. [13], [14].

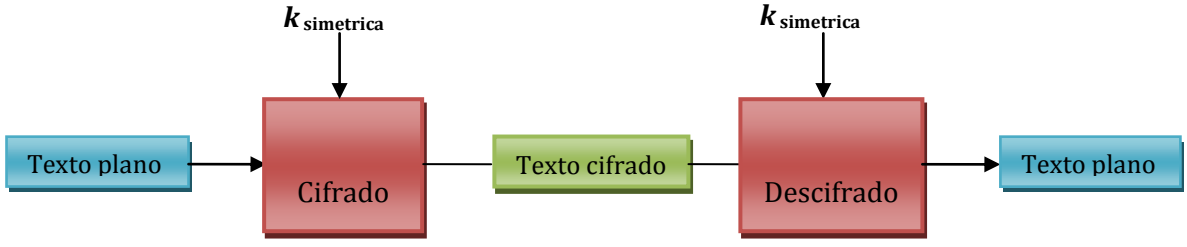


FIGURA 1. 10 CIFRADO SIMÉTRICO

Entre sus principales ventajas se encuentran:

- Requiere considerablemente menos recursos computacionales.
- Presenta una longitud de clave menor que en los procesos asimétricos, con la excepción de los basados en curvas elípticas.
- Usa una clave única que sirve para cifrar y para descifrar.
- Consume menos ancho de banda.
- El cálculo de la clave no requiere que cada parte sepa quién inicio el intercambio.

Por otro lado presenta importantes desventajas como las siguientes:

- La simetría en el protocolo de administración de claves puede proporcionar vulnerabilidades.
- Al ser la clave generada en uno de los extremos, se debe de confiar en él, de lo contrario el método no sirve.
- Debido a que la clave debe estar tanto en el transmisor como en el receptor, se genera incertidumbre en como transmitir la clave si se tiene un canal inseguro.

En la criptografía simétrica se pueden encontrar dos técnicas fácilmente distinguibles dada su funcionalidad [15], [13], como se aprecia en la figura 1.11:

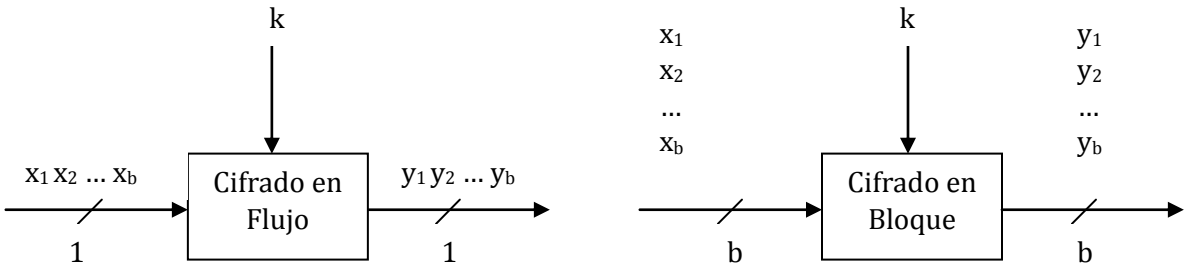


FIGURA 1. 11 TÉCNICAS DE CIFRADO SIMÉTRICO

2.3 CIFRADO ASIMÉTRICO

También conocido como cifrado de clave pública ya que se cuenta con un par de llaves, una pública y una privada. Aunque se puede cifrar con cualquiera de las dos llaves, por seguridad se recomienda utilizar la pública para cifrar y para el proceso de descifrado utilizar la llave privada; así, la llave pública es la que se reparte a los receptores con los que se desea establecer un canal seguro y aunque las llaves estén relacionadas matemáticamente no es factible derivar una a partir de la otra.

Para este tipo de cifrado se considera segura una llave si su longitud es mayor o igual a 1024 bits mientras que en los algoritmos de cifrado simétrico las llaves mayores a 128 bits se consideran seguras [16]; adicionalmente, los algoritmos asimétricos por su complejidad son sustancialmente más lentos que los algoritmos simétricos.

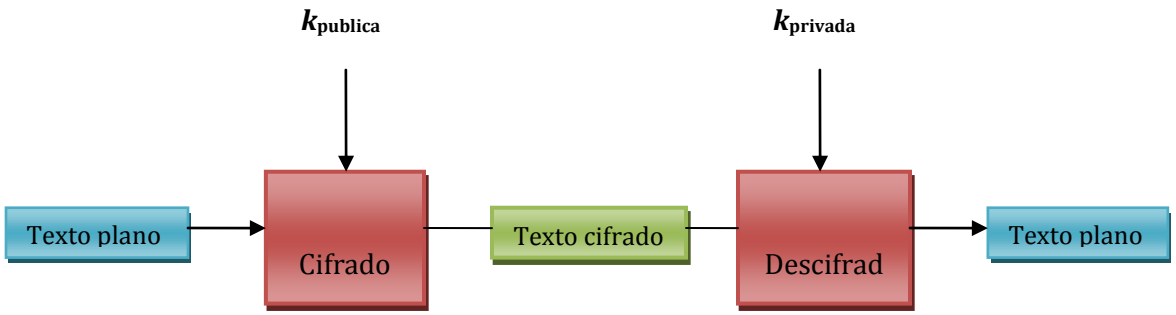


FIGURA 1. 12 CIFRADO/DESCIFRADO ASIMÉTRICO

Así, entre las principales aplicaciones que se puede encontrar, están:

- Establecimiento de clave: Protocolos para el establecimiento de claves sobre canales inseguros, por ejemplo Intercambio de claves Diffie-Hellman o RSA.
- No repudio: A través de las firmas digitales se puede ofrecer no repudio e integridad del mensaje.
- Autenticación: Mediante firmas digitales y protocolos.
- Confidencialidad: se puede cifrar la información usando algoritmos como RSA o ElGamal.

De las anteriores aplicaciones, es importante profundizar en la prestación del servicio de confidencialidad dado que es uno de los de mayor uso para poder establecer un canal seguro sobre un canal inseguro, y es en este entorno donde el cifrado asimétrico cobra importancia, ya que para establecer el canal seguro solo es necesario transmitir la clave para cifrar y no para descifrar, contrario a lo que sucede en los algoritmos simétricos en donde la clave transmitida se utiliza para ambos propósitos; es por esto que en la práctica el uso del cifrado asimétrico se restringe al inicio de sesión [16].

2.4 FUNCIONES HASH O RESUMEN

Las funciones resumen son muy importantes y útiles en el campo de la criptografía, dado que permiten obtener de un mensaje una cadena cuya longitud es fija y más corta, y que permite verificar la integridad del mensaje. El resumen obtenido es una representación única del mensaje y es muy difícil de falsificar. Todas las funciones hash o resumen deben tratar de satisfacer tres pilares de la seguridad:

- Resistencia pre-imagen: No debe ser factible poder obtener el mensaje de entrada, a partir de la salida.
- Segunda resistencia pre-imagen: El resumen de dos mensajes diferentes no debe ser el mismo.
- Resistencia a colisiones y a ataques de cumpleaños.

La probabilidad de poder obtener de dos mensajes diferentes un resumen de igual valor es tan baja que se dice que computacionalmente es imposible, lo cual, junto a su reducido tamaño, es lo que hace tan difundido su uso [15], [16].

Las funciones hash se dividen en dos tipos:

- Funciones hash dedicadas: son todos los algoritmos específicamente diseñados para trabajar como funciones hash.
- Funciones hash basadas en Algoritmos de Bloques: son funciones hash obtenidas a partir del uso de algoritmos de bloques.

La idea básica de las funciones hash es subdividir el mensaje entrante en pequeños bloques de igual tamaño que son pasados secuencialmente a través de la función hash, la cual en su parte interna tiene una función de compresión. El proceso es iterativo originando que el resumen sea la última iteración de la función, como se muestra a continuación en la figura 1.13.

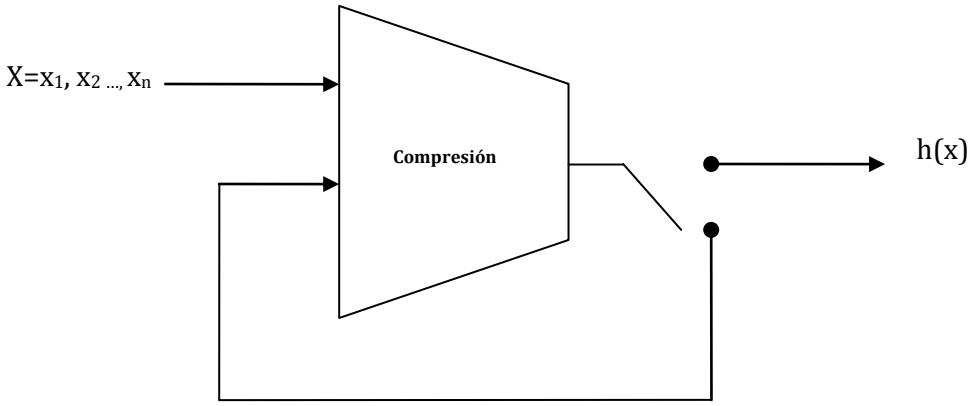


FIGURA 1. 13 FUNCIÓN RESUMEN

2.5 CÓDIGOS DE AUTENTICACIÓN DE MENSAJE POR HASH - HMAC

Los HMAC (Hashed Message Authentication Codes) son el resultado de combinar el uso de las funciones resumen y cifrado simétrico, es decir se utiliza una clave secreta como entrada a la función hash, por lo que el resumen ya no solo depende de la entrada sino que depende además de la clave, incrementando el nivel de seguridad [15].

3. DESEMPEÑO DE UNA RED

Uno de los factores esenciales al realizar una evaluación de desempeño en redes es establecer claramente la diferencia entre Calidad de Servicio (*Quality of Service - QoS*) y Calidad de Funcionamiento de la Red (*Network Performance - NP*), donde la primera de ellas está orientada al usuario y sus parámetros perceptibles ofrecen un marco útil para el diseño de redes pero no son necesariamente utilizables al especificar los requisitos de calidad de funcionamiento de determinadas conexiones de la red; análogamente, los parámetros de NP determinan finalmente la QoS observada por el usuario, pero no describen necesariamente esa calidad de manera significativa para los usuarios sino para el administrador de la misma [17].

Dado que se desean obtener datos más útiles para un proveedor de servicios o un administrador de red, que para un usuario final; esta evaluación se centra en la calidad de funcionamiento de la red que comúnmente se conoce como “desempeño” y no en la calidad de servicio.

Así, la Recomendación I-350 de la ITU-T *“Aspectos Generales de Calidad de Servicio y de Calidad de Funcionamiento en las Redes Digitales Incluidas las Redes Digitales de Servicios Integrados”* define 9 parámetros primarios mediante la matriz 3x3 para medir la calidad de funcionamiento donde las filas son las 3 funciones de comunicación básicas (acceso, transferencia de información de usuario y desvinculación), y las columnas son los 3 criterios que describen la calidad de funcionamiento (velocidad, precisión y seguridad).

En la sección de aportes del anteproyecto del presente trabajo de grado se especificó que la evaluación se realizaría durante la fase de transferencia de la información, dado que durante la fase de acceso y la fase de desvinculación el número de mensajes es muy pequeño y no afectan apreciablemente los valores de las métricas de desempeño de la red; además, estos procesos se realizan cuando expiran las SA, que según el documento del Dominio de Interpretación de IPsec para ISAKMP [11] se da por defecto cada 28.800 segundos (8 horas) y en los enrutadores Cisco utilizados como pasarelas de seguridad cada 86.400 segundos (24 horas).

Por la misma razón, no se evaluaron estas métricas para diferentes configuraciones de los protocolos de gestión de claves y asociaciones de seguridad y sus diversas técnicas de autenticación e intercambio de claves.

Adicionalmente, la Recomendación ITU-T Y.1543 que expone conceptos de medición en redes IP para evaluación de calidad de funcionamiento entre dominios, manifiesta que dado que las rutas de trafico saliente y entrante pueden diferir, los objetivos y medidas para todos los atributos de calidad de funcionamiento en QoS entre dominios (IDQ) son en-un-sentido y reflejan la naturaleza sin-conexión del servicio [18] .

Por otro lado, el grupo de trabajo de Métricas de Desempeño IP *(IP Performance Metrics – IPPM*) del Área de Transporte de la IETF denomina a su vez como “métricas” lo que anteriormente se ha mencionado como “parámetros”, y cuyas características principales se mencionan en el RFC2330 que define un marco general para las métricas particulares a ser

desarrolladas por el IPPM para permitir que los usuarios y los proveedores de servicios tengan un punto común de entendimiento del rendimiento y confiabilidad tanto de las rutas extremo-a-extremo a través de Internet como de las “nubes IP“ que comprenden porciones de esas rutas [19].

3.1 CONCEPTOS FUNDAMENTALES

En el entorno de Internet existen varias cantidades relacionadas al rendimiento y confiabilidad de una red, cuyos valores es deseable conocer; cuando tales cantidades están cuidadosamente especificadas, se conocen como *Métricas.* Aunque es permitido que en la práctica existan dificultades en la medida de ciertas cantidades, sus significados ambiguos no son permitidos, para tal fin cada métrica se define en términos de unidades estándar de medida, recurriendo al uso del sistema internacional de métricas.

3.1.1. TIPOS DE MÉTRICAS

- Métrica individual ó *Singleton***:** Se refiere a métricas, en cierto sentido, atómicas. Por ejemplo: una sola instancia de "capacidad de *throughput*" de un host a otro podría ser definida como una métrica individual, aunque la instancia implica medir los tiempos de un cierto número de paquetes IP.

- Métrica de muestra: Son métricas derivadas de una métrica individual, tomando conjuntamente un número de distintas instancias. Por ejemplo: se podría definir una métrica de muestra de retardo en un sentido desde un host a otro como el equivalente a una hora de mediciones, realizadas en intervalos Poisson con un espaciamiento medio de un segundo.

- Métrica estadística: Se refiere a métricas que son derivadas de una métrica de muestra por un cómputo estadístico de los valores dados por la métrica individual en la muestra. Por ejemplo: el valor medio de todos los valores de retardo en un sentido sobre la muestra dada, podría ser definida como una métrica estadística.

Por otra parte, en la Recomendación X.140 se exponen un conjunto de posibles parámetros de calidad para redes de datos, que para la función de transferencia de información son:

- El retardo de transferencia de paquetes de datos o de la información de usuario, y la velocidad de transferencia de información de usuario o caudal para caracterizar el parámetro de la Velocidad.
- La probabilidad de error, la probabilidad de entrega de información sobrante y la probabilidad de entrega indebida de la información de usuario para caracterizar la Precisión.
- La probabilidad de pérdida de la información de usuario para caracterizar la Seguridad de Funcionamiento [20].

Según la Recomendación ITU-T Y.1543 los atributos básicos utilizados para caracterizar la calidad de funcionamiento de red (IDQ) de una ruta son:

- Retardo medio en-un-sentido (*Mean One-Way Delay*)

- Variación del retardo de paquete en-un-sentido (*One-Way Packet Delay Variation*)
- Tasa de pérdida de paquetes (*Packet Loss Ratio*)
- Indisponibilidad de la ruta (*Path Unavailability*)

La lista de atributos anterior omite algunas métricas comunes a propósito, por ejemplo, el *throughput* de aplicación depende de muchos factores incluyendo perdida de paquetes, retardo de tránsito y otros que no están bajo el control del proveedor de servicio (SP) por lo que el *throughput* de aplicación no es un atributo de calidad de funcionamiento por sí mismo.

La tasa de tráfico ofrecida es parte de las descripciones del servicio y los contratos inter-SP, pero no es considerado un atributo de calidad de funcionamiento. Así, otras métricas como "retardo equivalente a perdidas" y "reordenamiento de paquetes" son útiles, sin embargo, el valor que aportan sobre las métricas seleccionadas arriba no justifica la complejidad adicional que requieren para especificarse, implementarse y desplegarse; aunque puede que el tiempo pruebe lo contrario y se agreguen otras métricas de red básicas en el futuro.

Por otra parte, la ITU-T Y. 1540 que habla del Servicio de comunicación de datos IP y los parámetros de desempeño en cuanto a disponibilidad y transferencia de paquetes IP indica que los parámetros pueden aplicar al servicio extremo-a-extremo (datagramas IP generados por usuarios entre 2 hosts, especificados por sus direcciones IP completas), punto-a-punto (no aplican a desempeño punto-multipunto) y a las porciones de red que proveen o contribuyen a la provisión de tal servicio [21].

3.1.2. MÉTRICAS PRINCIPALES

A) RETARDO EN UN SENTIDO (MEAN ONE-WAY DELAY)

La recomendación Y.1543 resalta la importancia de esta métrica, no solo por lo que representa en sí misma, sino también porque el retardo esta indirectamente relacionado con el *throughput* e impacta las velocidades de otras aplicaciones, es decir, las aplicaciones no funcionan bien si el retardo extremo a extremo entre los host es mayor que un nivel umbral o si existen variaciones erráticas en el retardo al utilizar aplicaciones de tiempo real. Además, retardos altos hacen más difícil mantener grandes anchos de banda para los protocolos de la capa de transporte, mientras que el valor mínimo de esta métrica proporciona una indicación del retardo que se experimentará si el enlace está ligeramente cargado y sus valores cercanos proporcionan un indicador de la congestión presente en el camino; finalmente brinda información indirecta de la presencia de conectividad convirtiéndose en un parámetro fundamental en la evaluación del rendimiento de las redes IP.

Los atributos de retardo se caracterizan por el retardo medio en-un-sentido, aunque opcionalmente se pueden proveer el retardo mínimo y un conjunto especifico de percentiles superiores de las variaciones del retardo; aclarando que este retardo medio correspondería al "retardo en-un-sentido tipo-p-finito" (type-p-one-way-delay) [22].

Por otro lado, aunque parecería lógica la suposición de que el valor del retardo de ida y vuelta (*Round Trip Time*) fuera más importante que el retardo en un solo sentido, las siguientes razones dan el sustento necesario para lo contrario:

- El camino desde la fuente hasta el host podría ser diferente al camino desde el destino

hasta la fuente, dado que diferentes secuencias de enrutadores son utilizadas para el envió y la recepción. Así, el retardo de ida y vuelta estaría midiendo el retardo de dos caminos diferentes.

- Incluso si los dos caminos son los mismos, podrían tener características de rendimiento radicalmente diferentes debido a encolamientos asimétricos.
- El desempeño de una aplicación en muchos casos depende, en esencia, del desempeño en una dirección.
- En redes habilitadas con calidad de servicio, el aprovisionamiento en una dirección podría ser completamente diferente al existente en la otra dirección, un ejemplo claro, es el enlace de subida comparado con el enlace de bajada ofrecido por un proveedor de servicios de internet (ISP).

B) VARIACIÓN DEL RETARDO EN UN SENTIDO (ONE-WAY PACKET DELAY VARIATION)

Algunas de las razones por las cuales es importante saber la variación de retardo presente en un enlace o en la misma red son las siguientes:

- Determinar el tamaño de *buffers* para aplicaciones *broadcast* o multimedia bajo demanda, dado que es necesario saber la máxima variación del retardo, para determinar el tamaño de los buffers.
- Determinar las dinámicas de las colas dentro de la red donde cambios en la variación del retardo pueden generar cambios en el tamaño de la cola de los procesos.
- Además esta métrica es particularmente robusta respecto a variaciones en los relojes, permitiendo el uso de la métrica incluso si los relojes no están sincronizados.

C) TASA DE PÉRDIDA DE PAQUETES IP (IP PACKET LOSS RATIO)

La IPLR está dada por el número de paquetes perdidos sobre el total de paquetes transmitidos, pero es importante considerar que el tiempo máximo de espera debe ser lo suficientemente largo para diferenciar un paquete con un retardo alto de uno perdido (descartado o corrupto). Hay una ligera diferencia entre la definición que da la Recomendación Y.1540 de la IPLR con la Pérdida de Paquetes en-un-sentido-Tipo-p (*type-p-one-way-packet-loss*) definido en el RFC 2680, en el cual los paquetes erróneos son designados como "perdidos".

En la práctica no hay diferencia significativa en los resultados de las medidas porque los paquetes con errores usualmente se descartan antes de llegar a su destino, sin embargo, si el último enlace antes del punto de medida es propenso a los errores entonces la diferencia entre las definiciones de ambos estándares pueden ser significativas [23].

La ITU define también, algunos parámetros opcionales relacionados como la IPER (Tasa de Paquetes IP Erróneos) como el número de paquetes erróneos del total de paquetes transmitidos, la Tasa de Paquetes IP Espurios como el número de paquetes espurios por intervalo de tiempo, la IPRR (Tasa De Paquetes IP Reordenados) como el número de paquetes reordenados del total de paquetes examinados, la IPDR (Tasa De Paquetes IP Duplicados) como el número de paquetes duplicados sobre el total de paquetes transmitidos exitosamente menos los paquetes duplicados y la RIPR (Tasa De Paquetes IP Replicados) como el número de paquetes replicados sobre el total de paquetes transmitidos exitosamente menos los paquetes duplicados.

D) INDISPONIBILIDAD DE LA RUTA (PATH UNAVAILABILITY)

La Recomendación Y-1543 especifica que un periodo se considera de indisponibilidad si hay una perdida excesiva de paquetes (IPLR > 75%) sobre un intervalo de tiempo fijo de 5 minutos.

Adicionalmente, en el RFC 2678 se definen los parámetros para conectividad instantánea unidireccional y bidireccional que pueden ser usadas para evaluar la conectividad a través del tiempo, similar a la función de disponibilidad del servicio de Y.1540 [24].

3.2 METODOLOGÍAS DE MEDICIÓN

La palabra metodología (del griego metà "más allá", odòs "camino" y logos "estudio"), hace referencia al conjunto de procedimientos basados en principios lógicos, utilizados para alcanzar una gama de objetivos que rigen en una investigación científica o en una exposición doctrinal (25 pág. 97).

La Recomendación Y.1543 de la ITU-T especifica algunos requerimientos que deben cumplir las medidas de calidad de funcionamiento, independientemente de la metodología utilizada para realizarlas; entre ellos se destacan:

- Todas las medidas deben ser unidireccionales (*one-way*) pero se pueden proveer estadísticas en ambos sentidos para estimar la calidad de funcionamiento bidireccional (*round-trip performance*).
- Las medidas se toman de cada segmento del modelo de red (sección 8 de la Recomendación) y pueden ser combinadas para formar métricas multi-segmento, sitio-a-sitio, borde-a-borde o Terminal.IP-a-Terminal.IP

Además, se habla de los dos tipos de metodologías de medición: activa y pasiva.

3.2.1. MEDICIÓN ACTIVA

En ella se inyectan paquetes de sondeo (*probes*) en ciertos dispositivos de la red y son enviados a dispositivos extractores que devuelven la información medida al dispositivo inyector. El desempeño de las sondas es utilizado como un predictor del desempeño de los datos de los usuarios dado que se recolectan retardos basados en *time-stamp* y mediciones de pérdidas.

Adicionalmente se debe tener en cuenta de que en el evento en que se supere el nivel de tráfico que se puede cursar, pueden ser retrasados o descartados paquetes, inclusive los paquetes de prueba UDP-Echo y no hay forma de saber cuáles de ellos fueron impactados por un evento provocado por las políticas de manejo de tráfico.

3.2.2. MEDICIÓN PASIVA

Al utilizar este tipo de medición no se inyecta tráfico adicional en la red sino que se monitorean los parámetros en dispositivos que pueden ser elementos de red residentes o entidades de medición independientes.

Los procedimientos de medición pasivos implican la presencia de dos dispositivos de medición que extraen una copia de los datos para crear un sumario de datos de los flujos. En contraste con la medición activa, aquí las rutas pueden cambiar durante el periodo de medición.

Para el presente proyecto se utilizaron las dos metodologías combinadas ya que, como se menciona en la sección de Mediciones Aplicadas de esta Recomendación, la medición pasiva puede tomar ventaja de las sondas de medición activa permitiendo que los dos métodos sean usados de forma cooperativa.

Es así como los parámetros de retardo, variación del retardo, porcentaje de pérdida de paquetes e indisponibilidad se midieron utilizando un protocolo de medición activa (One Way Active Measurement Protocol - OWAMP) [28]; mientras que para monitorear los valores de uso de CPU en los enrutadores y del *throughput* a través de ellos se empleó un protocolo para gestión de redes (Simple Network Management Protocol - SNMP) utilizando conceptos de la metodología de medición pasiva.

Como se sabe, el error está presente en cualquier método de medida, ante lo cual el objetivo principal debe ser identificarlo (comprender y documentar las fuentes de incertidumbre/error), cuantificarlo y reducirlo al mínimo nivel, para brindar el mejor nivel de precisión posible en el valor medido.

Por otro lado, en el RFC 2330 se presentan los principales factores sobre medición de desempeño que ha planteado el grupo de Métricas de Desempeño IP, y que se exponen en detalle en el Anexo 2, correspondiente al desempeño de redes IP.

3.2.3. MÉTODOS DE RECOLECCIÓN DE MUESTRAS

Existen dos tipos de recolección de muestras:

- Periódica: se toman muestras periódicamente, aunque esto podría generar dos grandes inconvenientes:
  - Si la métrica exhibe un comportamiento periódico es probable que se esté analizando solo una parte del comportamiento; además de los problemas que acarrea en cuanto a seguridad por ser predecible y por lo tanto anticipable.
  - El acto de medida puede perturbar lo que se está midiendo (por ejemplo, inyectando tráfico) y perturbaciones periódicas pueden llevar a la red a un estado de sincronización.

- Aleatoria: está basada en el “muestreo aditivamente aleatorio”. Las muestras son separadas e independientes y los intervalos generados aleatoriamente tienen una

distribución estadística común G(t) cuya calidad depende de la distribución. Aunque al utilizar la aleatoriedad se evita el estado de sincronización, tiene dos pequeños inconvenientes:

- El análisis en frecuencia es complicado, debido a que las muestras no ocurren en intervalos fijos tal como es asumido por la técnica de la transformada de Fourier.
- A menos que G(t) sea una distribución exponencial, las muestras siguen siendo de alguna manera predecibles, como se discutió para las muestras periódicas.

De acuerdo a las desventajas anteriormente descritas que presenta la recolección periódica, se profundizó en el método de recolección de muestras aleatorio, y específicamente en la distribución G(t).

3.2.4. CONSIDERACIONES DE TIEMPO

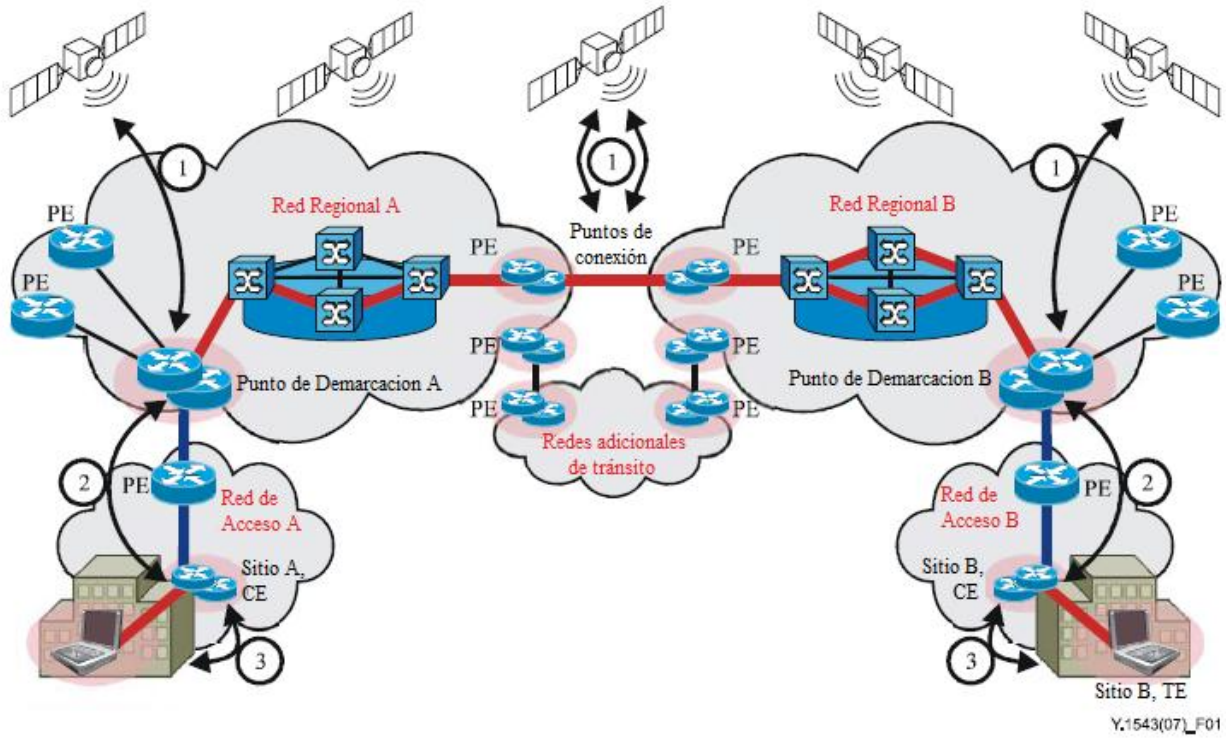


FIGURA 1. 14 PUNTOS DE MEDICIÓN [18]

Después de observar los modelos de medida que plantea la ITU-T, el que mejor se adapta a lo planteado en el anteproyecto es entre TEs (identificados con el número 3 en la figura 1.14) o Equipos Terminales: TE-TE o site-site (algo así como *end-to-end*), y cuyas implicaciones se explican con mayor detalle en el Anexo 2 o en la Recomendación Y.1543.

Entre las escalas de tiempo para las mediciones se destacan la unidad de tiempo de medición conocida como tiempo de "*rollup*" de 5 minutos, y la unidad de tiempo para reporte al cliente que es de 1 mes. Adicionalmente, la Recomendación Y. 1541 sugiere que el intervalo de

evaluación para retardo (IPTD), variación del retardo (IPDV) y tasa de pérdida de paquetes (IPLR) sea de 1 minuto; el RFC 3432 se refiere a este tiempo como "Tcons" [26].

Es vital para la confiabilidad de las medidas realizadas, que todas se realicen sobre las mismas escalas de tiempo, y las condiciones que deben cumplir estas escalas de tiempo.

Dado que comúnmente se utilizan los host para tomar las medidas, estos introducen retardos, cuellos de botella y demás, que se agravan cuando la marca de tiempo (timestamp) de los eventos ocurre a nivel de aplicación, son propios de los host y no tienen nada que ver con el comportamiento de la red. De esta manera para proveer un camino que hable de estos efectos, se introduce la noción de "*wire time*", aclarando que estas nociones son solo definidas en términos de un host H observando un enlace L en una ubicación dada:

- Para un paquete P, el “tiempo de llegada en el cable” (*wire arrival time*) de P en H sobre L es el primer tiempo T en el cual cualquier bit de P ha aparecido en la posición de observación de H sobre L.
- Para un paquete P, el “tiempo de salida por el cable” (*wire exit time*) de P en H sobre L es el primer tiempo T en el cual todos los bits de P han aparecido en la posición de observación de H sobre L.

Aunque usualmente se habla de *wire time* como el tiempo de retardo de propagación de los paquetes, es decir, el tiempo en que le toma en propagarse a través de un enlace L y no el tiempo hasta los host finales, es muy importante especificar como se debe realizar la medida para evitar ambigüedades y toma errónea de medidas.

3.2.5. CONSIDERACIONES DE LOS PAQUETES DE INFORMACIÓN

Aunque sería deseable caracterizar los distintos tipos de tráfico y clases de QoS, esto implicaría una cantidad de mediciones demasiado grande, por lo cual la Recomendación ITU-T Y.1541 sugiere para todas las mediciones un tamaño de campo de información fijo de 160 o 1500 octetos; y especialmente, para la estimación de la calidad de funcionamiento de los parámetros IP cuando se utilizan pruebas de capas inferiores tales como mediciones de errores en los bits se recomienda un campo de información de 1500 octetos

Además, es importante que no se permita la desfragmentación de los paquetes de prueba ya que si un fragmento se pierde o tiene errores todo el paquete se considera perdido o erróneo.

3.3 HERRAMIENTAS PARA MEDICIÓN

Para la selección de la herramienta que permitiera realizar una mediada confiable, se decidió tomar como criterios los conceptos anteriormente descritos. Un corto listado de las herramientas disponibles que se tuvieron en cuenta al realizar la selección es el siguiente:

Herramienta	*Enlace*
1. Ping y sus variaciones, como fping, Hping…	http://linux.die.net/man/8/ping http://linux.die.net/man/8/fping
2. Packit.	http://linux.die.net/man/8/packit
3. Bandwidthd.	http://bandwidthd.sourceforge.net/
4. Traceroute y Visualroute.	http://linux.die.net/man/8/traceroute http://www.visualroute.com/
5. Netcat.	http://netcat.sourceforge.net/
6. iperf.	http://iperf.sourceforge.net/
7. Netperf.	http://www.netperf.org/netperf/
8. **Owamp.**	http://www.internet2.edu/performance/owamp/
9. Ngrep.	http://ngrep.sourceforge.net/
10. Wireshark.	http://www.wireshark.org
11. Ethereal.	http://www.ethereal.com/
12. Smokeping.	http://oss.oetiker.ch/smokeping/
13. MRTG.	http://www.mrtg.jp/en/es_es/
14. Nagios.	http://www.nagios.org/
15. Rrdtool y Cacti.	http://www.cacti.net/
16. NTOP.	http://www.ntop.org/news.php
17. NetCPS.	http://www.netchain.com/netcps/

Al revisar estas herramientas se encontró que casi todas ellas han sido desarrolladas desde la perspectiva del creador y no bajo unos lineamientos claros como un estándar, por lo cual las medidas obtenidas mediante estas herramientas presentan grandes variaciones entre ellas e incertidumbre en los valores obtenidos.

Por otro lado está Owamp que es una herramienta que llena este vacío dado que está basada en los lineamientos del grupo de Métricas de Desempeño IP (IP Performance Metrics – IPPM) de la IETF y además es el resultado de la implementación del RFC 4656, convirtiéndose en la mejor herramienta disponible que además es libre y multiplataforma; aunque para su funcionamiento sobre Windows esté desarrollada en Java que es un lenguaje más lento. Además se ha demostrado que el error en las medidas tomadas bajo Linux es mucho menor que Windows [27], por lo cual se decidió trabajar Owamp desde maquinas Linux, específicamente utilizando la distribución Ubuntu.

3.3.1. PROTOCOLO ACTIVO DE MEDICIÓN EN UN SENTIDO

(*ONE WAY ACTIVE MEASUREMENT PROTOCOL – OWAMP)*

Es un protocolo de medida definido por el grupo IETF IP Performance Metrics (IPPM). Las medidas se realizan unidireccionalmente con el objetivo de poder identificar en qué sentido de la transmisión se encuentra presente la congestión en caso de que exista, dado que los flujos de tráfico son en la mayoría de los casos asimétricos y dependen de muchos factores tales como los procesos de encolamiento.

OWAMP realmente consta de dos protocolos interrelacionados:

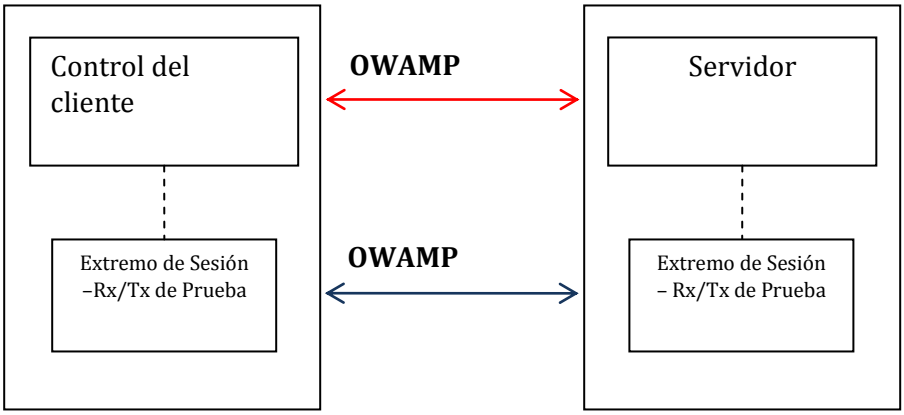


FIGURA 1. 15 PROTOCOLOS DE OWAMP

- OWAMP Control: Es el encargado del establecimiento, control y finalización de la sesión entre los dos extremos, que se establece sobre TCP por el puerto 861 y se mantiene abierta toda la prueba; además, extrae los resultados. También se encarga de negociar:

  - Direcciones
  - Puertos
  - Tiempo de inicio
  - Duración de la sesión
  - Tamaño y cantidad de los paquetes de prueba
  - Intervalo Medio de muestreo.
  - Y otros atributos vistos anteriormente.

- OWAMP Prueba: Luego de que se haya establecido la sesión TCP, OWAMP Prueba se encarga del intercambio de los paquetes de prueba (sondas) sobre el enlace a analizar. Para hacerlo se soporta sobre UDP, mientras que el puerto y el tamaño de paquete han sido negociados previamente.

Ambos protocolos soportan tres modos de operación: *No Autenticado, Autenticado y Cifrado*. El funcionamiento por defecto es No Autenticado, y para habilitar los modos restantes se debe compartir previamente una llave secreta.

La precisión alcanzada en la medida depende de la fuente externa de señal de reloj que se esté usando como referencia; así, si la precisión requerida es del orden de los microsegundos, se requerirá un servidor de tiempo o un receptor GPS en cada punto de medición, pero si por el contrario la precisión requerida puede ser del orden de los milisegundos, se puede utilizar el Protocolo de Tiempo de Red (NTP).

El protocolo OWAMP está diseñado para la medición de:

- Retardo.
- Variación de retardo sobre diferentes percentiles.
- Tasa de Pérdida de Paquetes.
- Error estimado en la medición.

Así, se pueden resumir las grandes ventajas que presenta este protocolo en:

- Precisión y estimación de error: Además de brindar alta precisiones, el protocolo entrega el error estimado como muestra la figura 1.16 en color marrón.
- Negociación de Parámetros: Permite una adaptabilidad única al entorno. Entre los parámetros negociados son de vital importancia:
  - Tamaño y cantidad de los paquetes: Para poder cumplir con requerimientos extra para la medición, como se puede observar en la figura 1.16 resaltado con rojo.
  - Intervalo Medio de Muestreo: Además de ofrecer la posibilidad de utilizar intervalos fijos permite utilizar muestreo Poisson para evitar la medición de comportamientos periódicos, dado que el intervalo entre paquetes de medida debe ser aleatorio. En la figura 1.16 se indica el intervalo medio en color verde, con distribución exponencial.
- Percentiles: El cálculo de la variación del retardo se puede realizar sobre diferentes percentiles del retardo (azul), dependiendo de los requerimientos de cada tipo de tráfico.
- QoS: Permite marcar los paquetes de prueba con un determinado código DSCP.
- Seguridad: Soporta Autenticación y cifrado dificultando la detección del trafico además de generar una problema adicional debido a la negociación de los puertos y el tamaño paquetes.

Se concluyó que Owamp fue desarrollado teniendo en cuenta los requerimientos y conceptos de métricas expuestos anteriormente tanto por la ITU como por la IETF, es una de las herramientas mejor diseñadas y confiables que cumple con la rigurosidad que se debe tener cuando se realizan mediciones sobre redes IP; por lo cual fue utilizada para las medidas tomadas en el proyecto realizadas. [28].

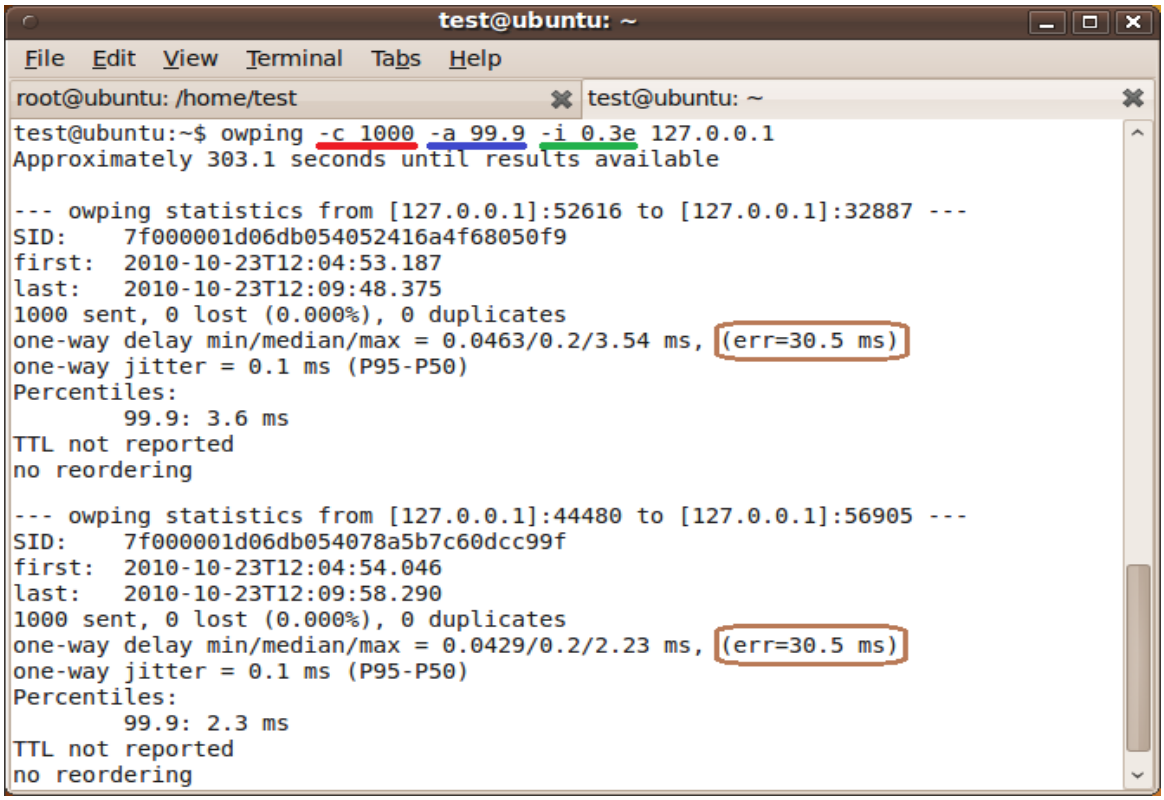


FIGURA 1. 16 CONFIGURACIÓN Y RESULTADOS DE LAS PRUEBAS CON OWAMP

CAPITULO II

EVALUACIÓN DEL DESEMPEÑO DE LOS PROTOCOLOS DE SEGURIDAD PROPORCIONADOS POR IPSEC

1. INTRODUCCIÓN

Para la evaluación del desempeño de las Redes IP con servicios de seguridad proporcionados por IPsec se implementaron los servicios de Integridad con Autenticación, y Confidencialidad en unos escenarios que se denominaron básicos, ya que el principal objetivo a cumplir en esta etapa era conocer el desempeño de las redes IP al utilizar independientemente los protocolos proporcionados por IPsec (AH y ESP) con sus respectivos algoritmos.

Dado que en el capítulo anterior se especificaron los conceptos básicos del funcionamiento de IPsec y de medición de desempeño a nivel IP, a continuación se detallan las pruebas realizadas en los escenarios que se elaboraron con diferentes configuraciones de seguridad proporcionadas mediante IPsec pero con una sola Asociación de Seguridad (SA) unicast.

1.1 SERVICIOS DE SEGURIDAD CONSIDERADOS EN LA EVALUACIÓN

En el presente trabajo se consideraron los servicios de Autenticación + Integridad (como uno solo), y Confidencialidad. Los demás servicios detallados en el capítulo 1 no se incluyeron debido a que no afectan notablemente el desempeño de las redes IP en condiciones de funcionamiento normal.

Por ejemplo, el servicio de control de acceso se presta mediante la definición de una Lista de Control de Acceso (ACL) en la Pasarela de Seguridad y no incluye generación de tráfico adicional al cursado normalmente.

Igualmente el servicio de antirrepetición sólo afectaría el desempeño de la red en el evento de un ataque de DoS, mejorándolo; ya que sin este servicio habría un mayor número de paquetes viajando mientras que al utilizarlo muchos de estos se descartarían al encontrar que son duplicados. Adicionalmente, se eliminan también los paquetes que la red duplique en condiciones normales, pero que en las pruebas realizadas representan una cantidad irrelevante que no afecta el desempeño de la red de forma apreciable.

1.2 MÉTRICAS DE DESEMPEÑO DE LA RED A EVALUAR

Teniendo en cuenta que para obtener datos confiables de *retardo y variación del retardo* con el percentil 99.9 la Tasa de Pérdida de Paquetes IP (IPLR) debía ser menor al 0.1%, se realizaron todas las pruebas con una IPLR = 0

Asimismo, tomando la definición de la ITU presentada en el capítulo 1 de un periodo de indisponibilidad, como aquel en el cual la IPLR > 75%; no se presentan datos de indisponibilidad en este trabajo sino que se centra en los ítems de *retardo y variación* del mismo, y adicionalmente la velocidad y el porcentaje de uso de CPU en los enrutadores que actuaron como Pasarelas de Seguridad.

1.2.1. RETARDO Y VARIACIÓN DE RETARDO

La herramienta Software de medición usada fue Owamp, la implementación realizada por Internet2 del protocolo que lleva el mismo nombre [28], dado que cumplía con los requerimientos establecidos por la ITU-T y con los lineamientos dados por la IETF a través del grupo de Métricas de Desempeño IP - IPPM.

El tiempo de medición para las pruebas básicas fue de media hora, en cada una de las cuales se realizaron dos [2] sesiones de prueba de Owamp de 5 minutos cada una (tiempo de *rollup*) con tiempos aleatorios de espera antes y después de cada una de ellas; como se explicó anteriormente, esto se hizo con el fin de evitar la medición de comportamientos periódicos en la red en caso de que ésta los presente.

En cada sesión se utilizaron 1000 paquetes de prueba de un tamaño correspondiente a 160 bytes en la carga útil y con intervalos de tiempo aleatorios entre ellas con una media de 0.3 segundos.

Aunque los percentiles usuales de *variación de retardo* difieren dependiendo del tipo de tráfico, se realizó el cálculo sobre el percentil 99.9th de retardo en todas las pruebas utilizando el valor correspondiente a los tipos de tráfico más exigentes tales como voz y video en tiempo real. La configuración final utilizada para las pruebas (a excepción del direccionamiento), y un ejemplo de los resultados que entrega Owamp son los que se expusieron previamente en la figura 1.16.

Es importante mencionar, que aunque el cálculo de variación del retardo entregado por Owamp cumple con las especificaciones del RFC [29] en donde se toma como el retardo equivalente al percentil 99.9 menos 0, se consideró que no reflejaba realmente el comportamiento de los paquetes y para éstos cálculos se tomó en su lugar como base el retardo entregado por el paquete de menor retardo durante la prueba.

1.2.2. PORCENTAJE DE USO DE CPU

Adicionalmente a los dos parámetros anteriores se monitoreó el porcentaje de uso de capacidad de procesamiento de los enrutadores a través del protocolo SNMP, mediante la variable *cpmCPUTotal5sec* que hace parte de la *CISCO-PROCESS-MIB*, y que entrega el porcentaje promedio global de CPU ocupada en los últimos 5 segundos.

Para esta medición no se pudo establecer claramente que proceso del enrutador era el encargado de realizar los cálculos asociados al procesamiento de IPsec, sin embargo, al ser un análisis esencialmente comparativo ésta variable que proporciona el uso de CPU de todos los procesos permite apreciar las variaciones al utilizar diferentes configuraciones de IPsec en estas pasarelas de seguridad.

1.2.3. VELOCIDAD

Igualmente, para calcular la velocidad en la red se utilizó el protocolo SNMP asociado a las variables *ifInOctets* que indica la cantidad de bytes que han ingresado por determinada interfaz del enrutador, e *ifOutOctets* que indica la cantidad de bytes que han salido por dicha interfaz, pertenecientes a la *IF-MIB* que proporciona información útil sobre las interfaces del enrutador.

Aunque estas variables entregan un acumulado de la información transmitida desde que inicia el contador, se invocaron cada 5 segundos, calculando la diferencia de información transmitida entre dos mediciones sucesivas y dividiéndola por el tiempo transcurrido entre ellas para obtener la velocidad en bytes por segundo que luego fue convertida a bits por segundo para elaborar las gráficas que se muestran en este capítulo.

2. ESCENARIO BÁSICO

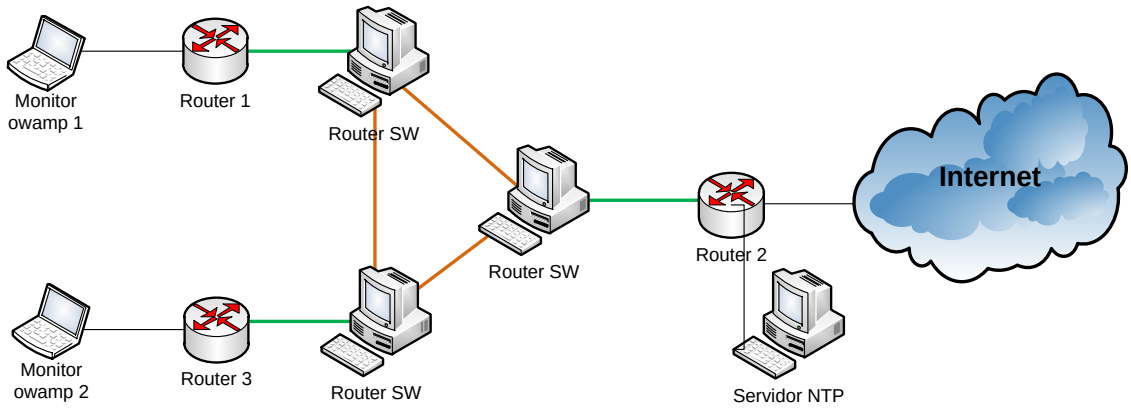


FIGURA 2. 1ESCENARIO BÁSICO

En este aspecto se plantea una diferencia fundamental ya que el escenario básico físicamente es el mismo, sin embargo, de forma lógica se manejan tres escenarios cuyas diferencias radican en la configuración de las Asociaciones de Seguridad de IPsec.

El escenario básico para las pruebas realizadas se muestra en la figura 2.1.Se tiene un *core* formado por tres enrutadores BGP software trabajando con Quagga/Linux, y conectado a cada uno de ellos una pequeña red formada por un enrutador Cisco 2801 con

capacidades criptográficas y un *host* o PC.

En este escenario, los enrutadores Cisco actúan como enrutadores de frontera de la red del proveedor, que al configurarse como pasarelas de seguridad proporcionan servicios de seguridad a través del *core* de la red, aunque en algunas de las configuraciones se asegura el tráfico de host-a-host.

Para realizar el análisis especificado en el anteproyecto, donde se pretende realizar una comparación de los tráficos de voz, video, y datos; se implementó el servicio de VoIP a través de una centralita con Asterisk, el de video mediante un servidor de Streaming con VLC y el de datos con un servidor FTP.

Adicionalmente, se configuró uno de los *hosts* como servidor de tiempo utilizando el Protocolo de Tiempo en Internet (*Network Time Protocol* - NTP) ya que Owamp necesita estar sincronizado con el tiempo UTC para proporcionar valores de retardo y errores estimados que sean confiables, además, todos los equipos de la red que requirieran sincronización utilizaban éste como servidor para eliminar las variaciones que se pudieran generar entre ellos al conectarse a dos servidores diferentes en Internet o al mismo servidor pero (posiblemente) a través de distintas rutas.

Los escenarios planteados para las pruebas se basan en los casos que se especifican en el 1er estándar de la arquitectura [10] y que obligatoriamente deben ser soportados por cualquier implementación con sus respectivas combinaciones de Asociaciones de Seguridad (SA). En su forma básica son los que proporcionan seguridad entre los extremos (Host-Host), entre dos sistemas intermedios de la ruta (SG-SG), y la combinación de estos dos (Host-SG).

Es de anotar, que dada la esencia unidireccional de una SA se hace necesaria la creación de dos SAs para tener una conexión bidireccional; sin embargo, cuando la gestión de SAs no se realiza de forma manual sino mediante un protocolo como IKE tanto las SAs IPsec como las SAs ISAKMP se generan automáticamente en pares para proporcionar seguridad en ambos sentidos de la comunicación.

3. ESCENARIO 1: SG-SG

En este caso las Asociaciones de Seguridad se establecen entre los enrutadores 1 y 3 que actúan como pasarelas de seguridad, por lo que los procesos de integridad y cifrado/descifrado se dan en estos puntos de la red.

La información viaja protegida por IPsec sólo entre las dos pasarelas de seguridad, mientras que entre cada host y su respectiva pasarela de salida (enrutador) el tráfico viaja en texto plano.

Para su despliegue se utilizaron las capacidades criptográficas de los Enrutadores de Servicios Integrados (ISR) Cisco 2801 que posee el Laboratorio de Redes y Servicios Telemáticos del Dpto. de Telecomunicaciones de la FIET de la Universidad del Cauca, y

que permiten la configuración del control de acceso, el establecimiento de las SAs de IPsec y la gestión mediante ISAKMP pero solo en modo túnel, ya que los enrutadores no negocian SAs en modo transporte.

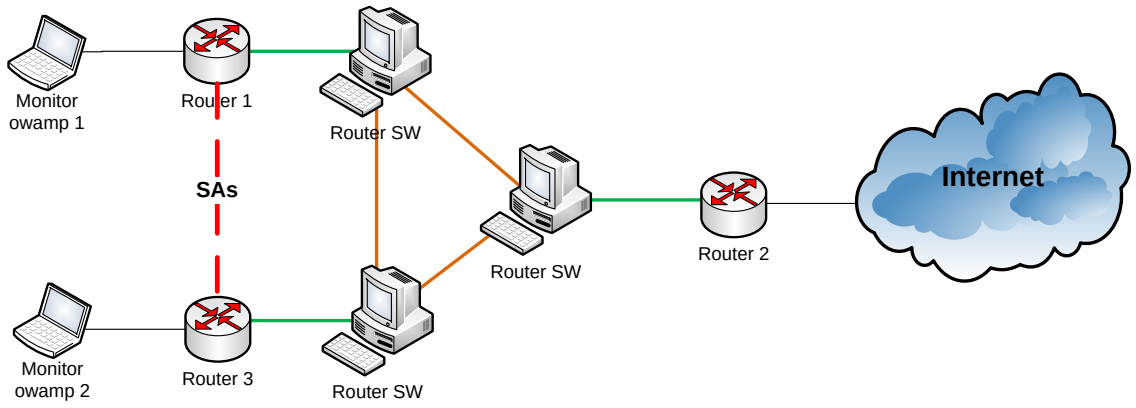


FIGURA 2. 2ESCENARIO CON LAS SA ENTRE SG Y SG

Como escenario esencial del proyecto, fue en éste donde se realizaron la pruebas concernientes a conocer el funcionamiento y operación de los protocolos de seguridad de IPsec con sus respectivos algoritmos, ya que como se especificó en el anteproyecto, se buscaba conocer el impacto en redes IP trabajando con dispositivos diseñados para este fin, a diferencia de los estudios que se habían realizado previamente donde se utilizaban implementaciones en hosts. Como se verá más adelante, los resultados obtenidos de las pruebas en los hosts no muestran una consistencia como la que se observa en las diferentes pruebas realizadas en las SG.

	SG - SG Cisco	Servicio: Protocolo	Modo	Algoritmo(s)	Owamp	Datos	Video	Voz
		Autenticación: AH						
1			Túnel	MD5	✓	✓	✓	✓
2			Túnel	SHA	✓	✓	✓	✓
		Confidencialidad: ESP						
3			Túnel	3DES	✓	✓	✓	✓
4			Túnel	AES	✓	✓	✓	✓
5			Túnel	DES	✓	✓	✓	✓
		Autenticación + Confidencialidad: ESP						
6			Túnel	3DES-MD5	✓	✓	✓	✓
7			Túnel	AES-MD5	✓	✓	✓	✓
8			Túnel	DES-MD5	✓	✓	✓	✓
9			Túnel	3DES-SHA	✓	✓	✓	✓
10			Túnel	AES-SHA	✓	✓	✓	✓
11			Túnel	DES-SHA	✓	✓	✓	✓

TABLA 2. 1PRUEBAS REALIZADAS EN EL ESCENARIO SG-SG

3.1 IMPACTO DE IPSEC EN LOS DIFERENTES TIPOS DE TRÁFICO

Lo primero que de sebe tener en cuenta es que la utilización de IPsec para proporcionar servicios de seguridad con sus dos protocolos y diversos algoritmos tiene un impacto negativo en el desempeño de las redes IP, como lo muestran las figuras 2.3 a 2.8 que reflejan el comportamiento de la red con IPsec con sus respectivas transformadas o combinaciones de algoritmos, al ser aplicadas a diferentes tipos de tráfico; es decir, que la calidad de funcionamiento de la red disminuye ya sea leve o significativamente dependiendo del tipo de tráfico que se esté transmitiendo.

Las gráficas de la sección 3.1 se obtuvieron a partir de las gráficas individuales realizadas para cada prueba, con los datos obtenidos de uso de CPU y de velocidad promedio a través de los enrutadores durante cada una de ellas.

3.1.1. DATOS

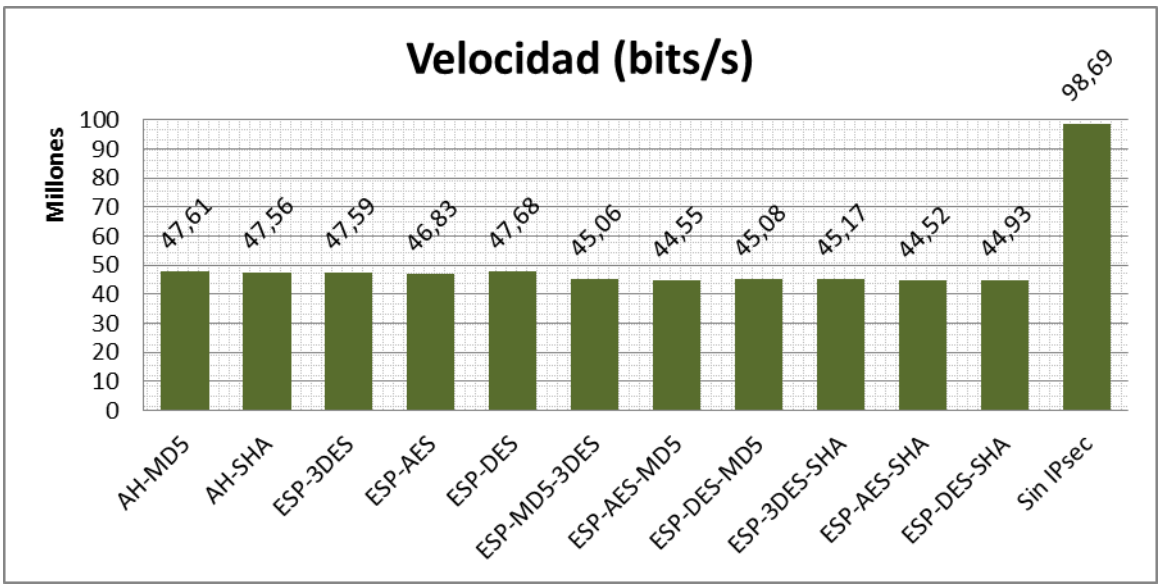


FIGURA 2. 3 VELOCIDADES EN FTP AL IMPLEMENTAR IPSEC

Se tiene una red con una velocidad teórica de 100Mbps, que sin IPsec se aprovecha casi toda; luego, al implementar IPsec con cualquiera de sus configuraciones se observa una caída en la velocidad promedio superior al 50%. La figura 2.3 muestra la velocidad promedio en una transmisión de FTP, que entre los tipos de tráfico evaluados es el que más recursos exige de la red.

También se puede notar el impacto que tiene IPsec observando el uso promedio de CPU que requiere cada enrutador para procesar la información.

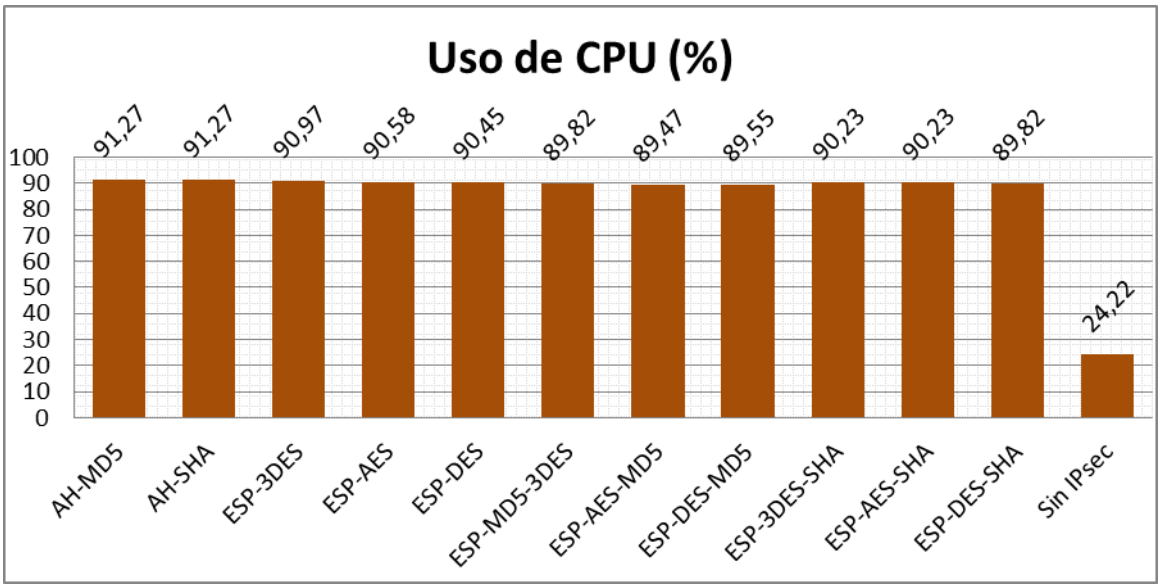


FIGURA 2. 4 USO DE CPU EN LA TRANSMISIÓN DE INFORMACIÓN POR FTP

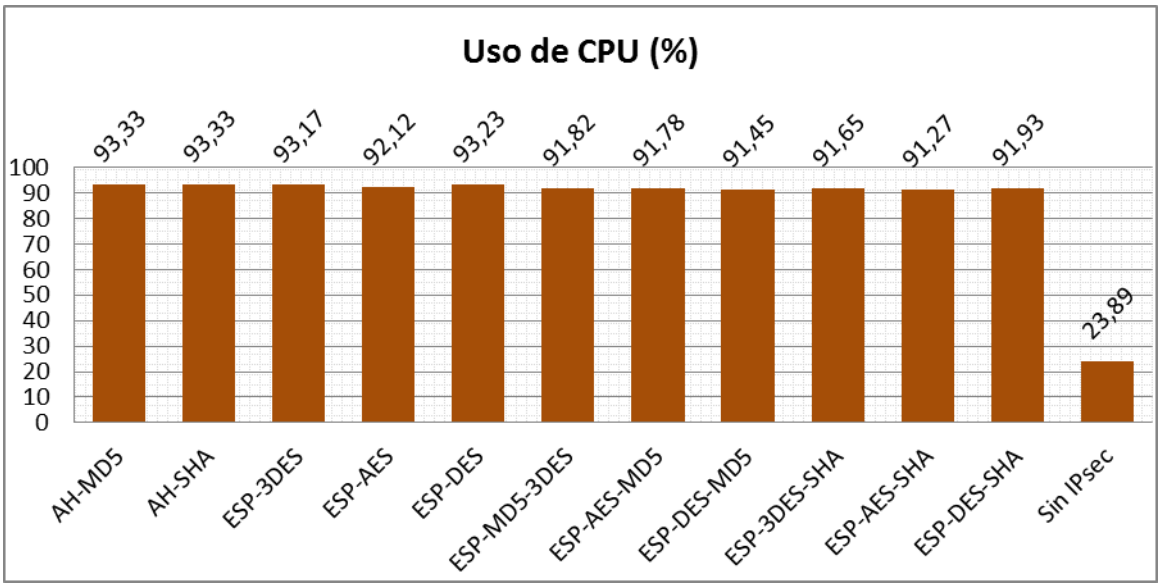


FIGURA 2. 5 USO DE CPU EN LA RECEPCIÓN DE INFORMACIÓN POR FTP

Los procesos en el enrutador conectado al servidor FTP que recibe la información y la protege requieren una cantidad de recursos ligeramente mayor que los que se realizan en el enrutador del cliente, pero de igual forma la diferencia al usar o no usar IPsec para la transmisión de datos a través de FTP es clara y relevante en el detrimento del desempeño que se presenta cuando se utilizan los servicios de seguridad.

Dado que, como se observa en las Figuras 2.4 y 2.5, los datos obtenidos en la pasarela de seguridad que cifra/autentica son consistentes con los obtenidos en la pasarela que descifra/verifica, en adelante en este documento sólo se presentarán los datos de la

pasarela de seguridad que se encuentra en la parte de recepción dado que corresponden al comportamiento de la red que percibe realmente el cliente; los demás datos se pueden consultar en los Anexos.

3.1.2. VIDEO

De igual forma, en la figura 2.6 se observa el impacto que tiene la implementación de IPsec en el consumo de capacidad de procesamiento que se hace en los enrutadores al proteger tráfico de Video en tiempo real; la gráfica muestra los datos obtenidos en recepción, donde el uso de CPU es ligeramente mayor para los tráficos de datos y video.

Mientras tanto, en la figura 2.7 se muestra que el impacto de implementar IPsec para proteger tráfico de video no es tan alto como el que se observó en las pruebas de FTP, dado que el video maneja velocidades constantes y mucho más bajas que el ancho de banda de la red.

Las medidas fueron realizadas utilizando solicitudes SNMP hacia los enrutadores de salida (el que protege la información) y de llegada (el que retira la protección); y se observa que al igual que en FTP los datos son consistentes ya que aunque los procesos que proveen seguridad (cifrado y autenticación/integridad) requieren un uso de CPU ligeramente menor que los que retiran la protección (descifrado y verificación de autenticación/integridad), la relación entre el consumo de estos recursos cuando se implementa IPsec en cualquiera de las configuraciones utilizadas y cuando no se implementa es, en todos los casos, muy alta.

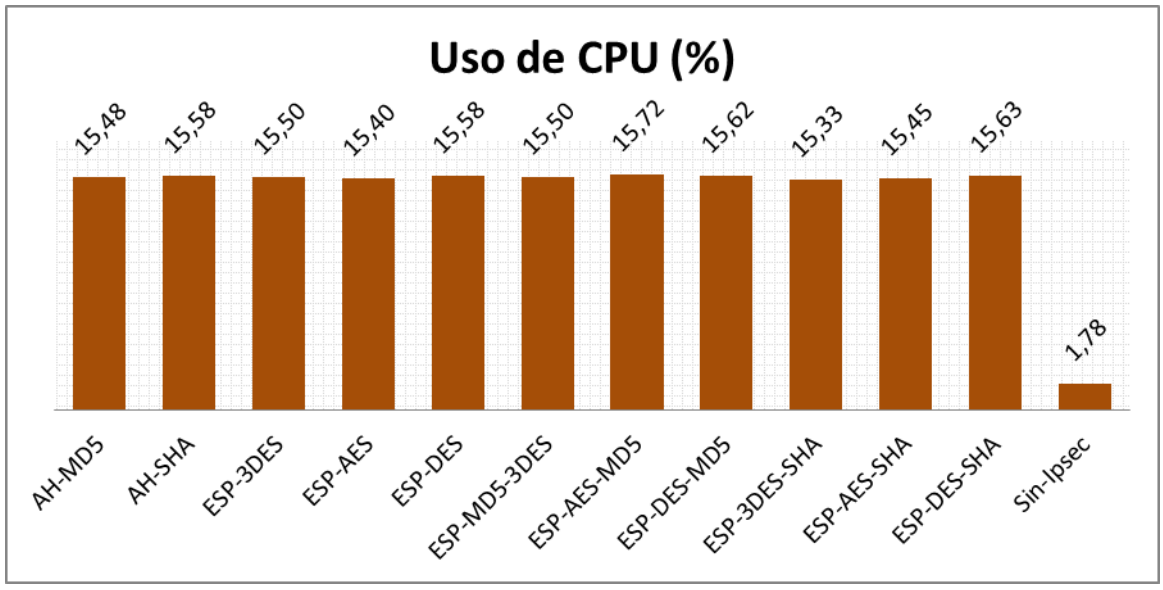


FIGURA 2. 6 USO DE CPU EN LA SG AL QUITAR PROTECCIÓN DE STREAMING DE VIDEO

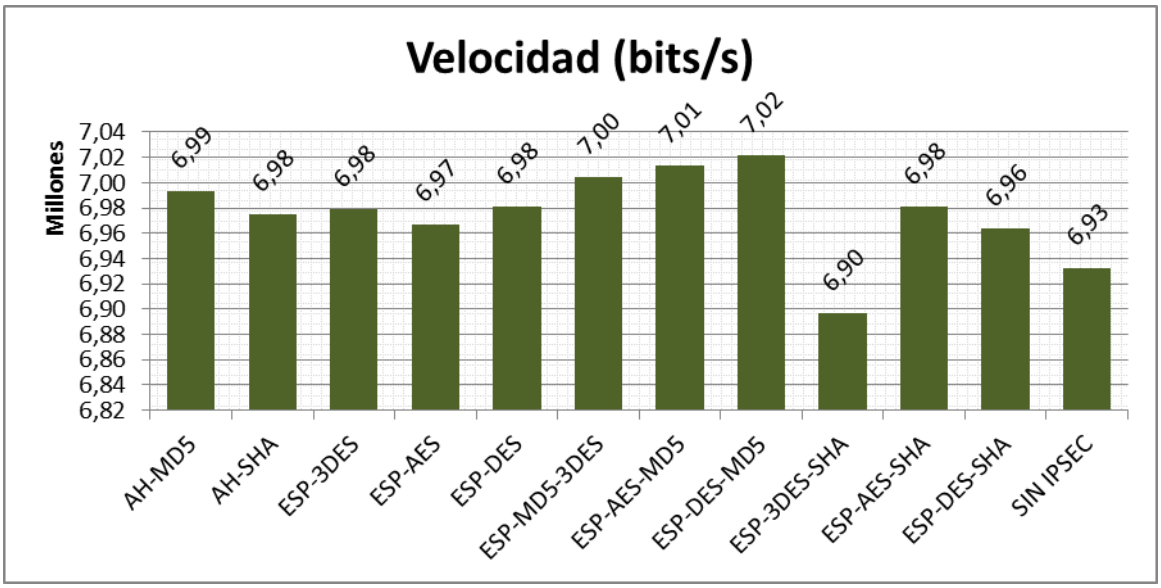


FIGURA 2. 7 VELOCIDAD EN LA SG EN RECEPCIÓN PARA STREAMING DE VIDEO

3.1.3. VOZ

Asimismo, al realizar una llamada por VoIP los datos de uso de CPU en las dos pasarelas de seguridad reflejan una diferencia entre sus valores de hasta 0.11% lo que permite mostrar aquí los datos sólo de recepción teniendo en cuenta que la variación al observar los de transmisión es mínima. Su relación con este parámetro al no implementar IPsec se muestra a continuación en la figura 2.8.

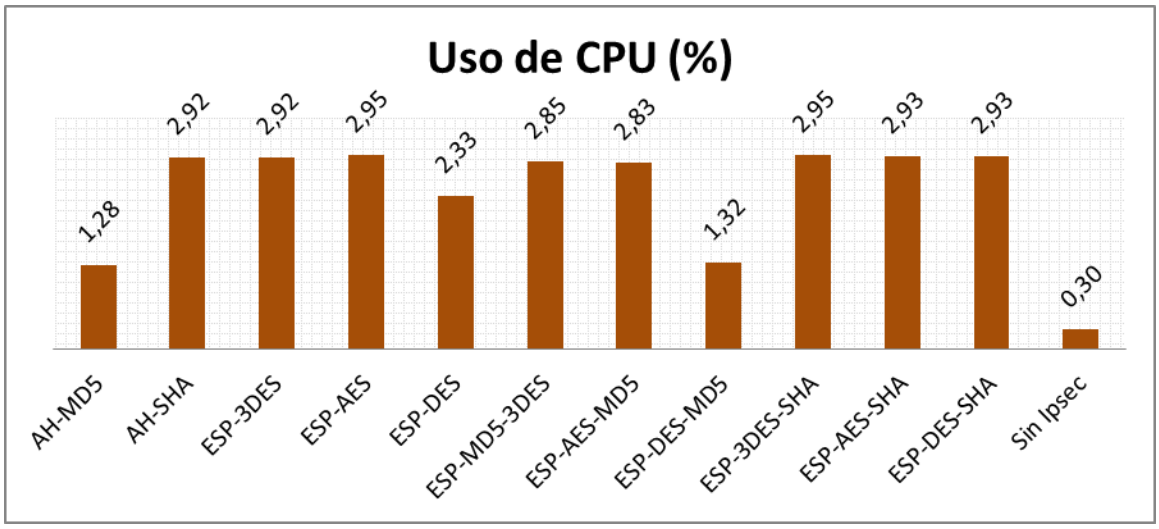


FIGURA 2. 8 USO DE CPU HECHO POR UNA LLAMADA VOIP

Una llamada VoIP al manejar velocidades tan bajas (inferiores a 100kb/s) no tiene un impacto significativo en el consumo de CPU de los enrutadores, de igual manera, en las pruebas realizadas en este escenario el oído humano no percibe si la calidad de la llamada se ha degradado.

De forma similar a la transmisión de video, se emite a una tasa constante y mucho más baja que la capacidad de la red por lo que la velocidad no se ve limitada de igual forma que en la trasmisión de FTP.

3.2 ANÁLISIS CON AH Y SUS ALGORTIMOS

3.2.1. RETARDO Y VARIACIÓN DEL RETARDO

En cuanto al *retardo*, los datos presentados al utilizar autenticación + integridad con MD5 no son tan volátiles como al utilizar SHA; es decir, a pesar de que el retardo en MD5 presenta puntos de inflexión más pronunciados que SHA (máximos más altos y mínimos más bajos), estos son más esporádicos, mientras que en SHA los puntos de inflexión son más frecuentes pero con menor variación con respecto al promedio.

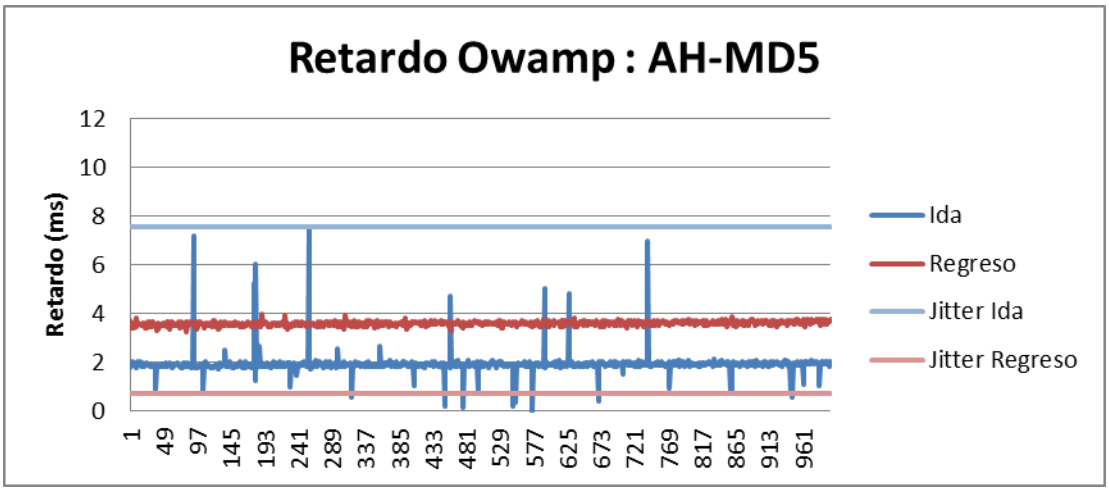


FIGURA 2. 9 RETARDO Y SUS VARIACIONES PARA LAS PRUEBAS DE OWAMP CON AH

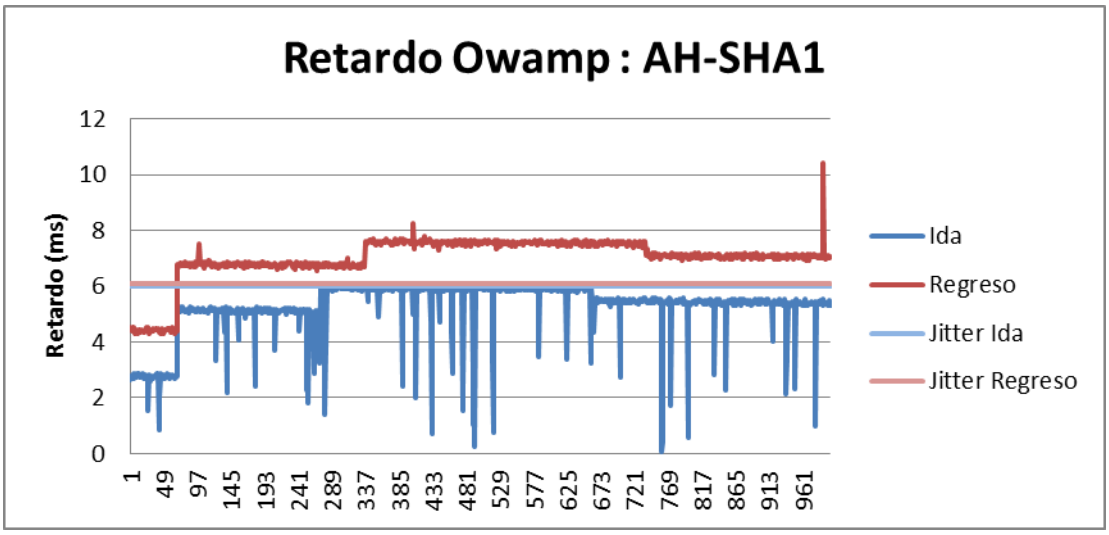


FIGURA 2. 10 RETARDO Y SUS VARIACIONES PARA LAS PRUEBAS DE OWAMP CON AH

Es así como para aplicaciones de tiempo real, MD5 requeriría valores de *buffer* más altos ya que la variación del retardo en general es mayor, pero la mayor parte del tiempo esa capacidad de buffer se mantendrá sin copar, mientras que en SHA los valores de buffer podrían ser menores pero el valor promedio de retardo puede variar durante la transmisión.

A continuación se presenta un resumen de los rangos de valores de retardo y sus variaciones obtenidos al utilizar AH con MD5 y con SHA1. En él se observa que la red presenta un comportamiento asimétrico ya que al regreso, el retardo tiende a ser más alto que a la ida.

Asimismo, el retardo promedio tanto a la ida como al regreso, que se genera al utilizar MD5 es menor que el que se genera cuando se utiliza SHA1.

	MD5	**SHA1**
Retardo en la Ida (ms)	1.93 - 2.08	2.19 - 5.24
Variación de retardo en la Ida	7.58 – 11.8	6.02 - 9.69
Retardo al Regreso	0.41 - 3.61	3.79 - 7.01
Variación de retardo al regreso	0.72 – 3.87	5.69 - 6.11

TABLA 2. 2 RETARDO Y SUS VARIACIONES CON AH

En la tabla 2.2, así como en las siguientes donde se presentan resúmenes de los datos obtenidos, se resalta en color verde los valores que muestran un menor impacto en la calidad de funcionamiento de la red.

3.2.2. DATOS

Al transmitir a través del servicio de FTP la velocidad se ve afectada de forma similar por MD5 y por SHA. Los datos entregados por el cliente FTP muestran como resultado una diferencia en el tiempo de transmisión de aproximadamente un segundo. Asimismo, los valores de uso de CPU son en promedio iguales para FTP; para la prueba de Owamp los valores de uso de CPU oscilan entre 0.175% y 0.2% presentando una diferencia entre MD5 y SHA menor al 0.025%. Para realizar la transferencia se utilizó un único archivo en todas las pruebas de 2133652877 bytes (aproximadamente 2GB).

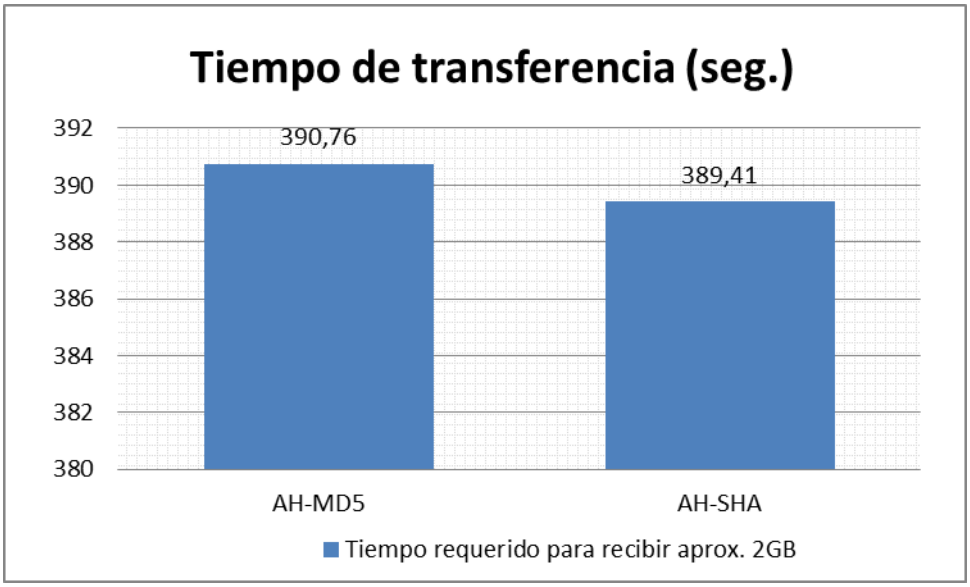


FIGURA 2. 11 TIEMPO DE TRANSFERENCIA PARA UN ARCHIVO DE APROX. 2GB

3.2.3. VIDEO

En la prueba de video se observa que utilizar SHA incrementa el uso de la CPU en 1.63% con respecto a MD5. De igual forma, la diferencia de velocidad entre ellas es menor a 35Kbits por segundo, que no se consideran relevantes frente a la velocidad de transmisión promedio del video (sin IPsec y con diversas formas de IPsec) que es de aproximadamente 6,85Mbits/seg.

3.2.4. VOZ

En la prueba de voz se tienen valores de uso de CPU con SHA de alrededor de 2.65-2.92% en promedio mientras que MD5 utiliza menos recursos de la misma, con porcentajes de uso de 1.28-1.3%. La diferencia en la velocidad entre ellos es mínima, así como la diferencia con la velocidad sin IPsec (86.8kbits/seg.) que es de aproximadamente 133bits/segundo.

		MD5	SHA1
Datos	**Tiempo de Tx.**	390.76 s	389.41 s
	Uso de CPU	93.33%	93.33%
Video	**Velocidad**	6.99Mbps	6.98Mbps
	Uso de CPU	15.48%	15.58%
Voz	**Velocidad**	86.69kbps	86.73kbps
	Uso de CPU	1.28%	2.91%

TABLA 2. 3 VELOCIDAD Y PORCENTAJE DE USO DE CPU CON AH

3.3. ANÁLISIS CON ESP Y SUS ALGORITMOS

En esta sección se presenta un análisis del protocolo ESP al prestar el servicio de sólo-confidencialidad, para los ítems de retardo y variación del retardo, y de desempeño con diferentes tipos de tráfico.

3.3.1. RETARDO Y VARIACIÓN DEL RETARDO

Los valores de retardo obtenidos mediante Owamp se presentan en cada sección resumidos como se muestra a continuación, en ella se indican los valores de Retardo y Variación de Retardo tanto en el trayecto de Ida como en el de Regreso.

	3DES	AES	DES
Retardo ida(ms)	6.35 – 6.95	4.42 – 5.39	4.82 – 4.83
Variación de retardo	7.08 - 7.22	6.98- 8.26	6.74 – 7.93
Retardo regreso	8.22 – 8.77	6.15 – 7.14	6.54 – 6.56
Variacion de retardo	4.59 – 5.69	1.76 - 5	2.14 – 3.85
Ganador			✓

TABLA 2. 4 RETARDO Y SUS VARIACIONES AL PROPORCIONAR SÓLO-CONFIDENCIALIDAD CON ESP

La información suministrada por las pruebas de Owamp permite observar que 3DES es el que presenta el mayor retardo en ambas pruebas, sus valores de variación de retardo indican un comportamiento parecido a AES, dado que en la ida el que presentó una mayor variación fue AES pero en el regreso el mayor valor fue presentado por 3DES. Lo cual se puede corroborar en las figuras 2.12, 2.13 y 2.14 al observar los puntos de inflexión.

3DES presenta un menor número de puntos de inflexión que AES y los valores obtenidos de retardo y variación de retardo en ambas pruebas son muy similares, lo cual da indicios de un comportamiento estable del algoritmo, mientras que DES es el que presenta menor retardo y a su vez menores puntos de inflexión, resaltando que el algoritmo tiene valores casi iguales en ambas pruebas lo que corrobora la estabilidad presente en 3DES dado que es la evolución de DES.

AES aunque presenta en general un mayor retardo que DES, tiene valores promedio muy cercanos a los de éste, lo cual es muy interesante dado que AES a pesar del mayor número de procesos y del tamaño de la clave que ofrece un mayor nivel de seguridad presenta un comportamiento muy similar a DES, pero los valores de retardo y variación de retardo no son tan estables como los presentados por los otros algoritmos.

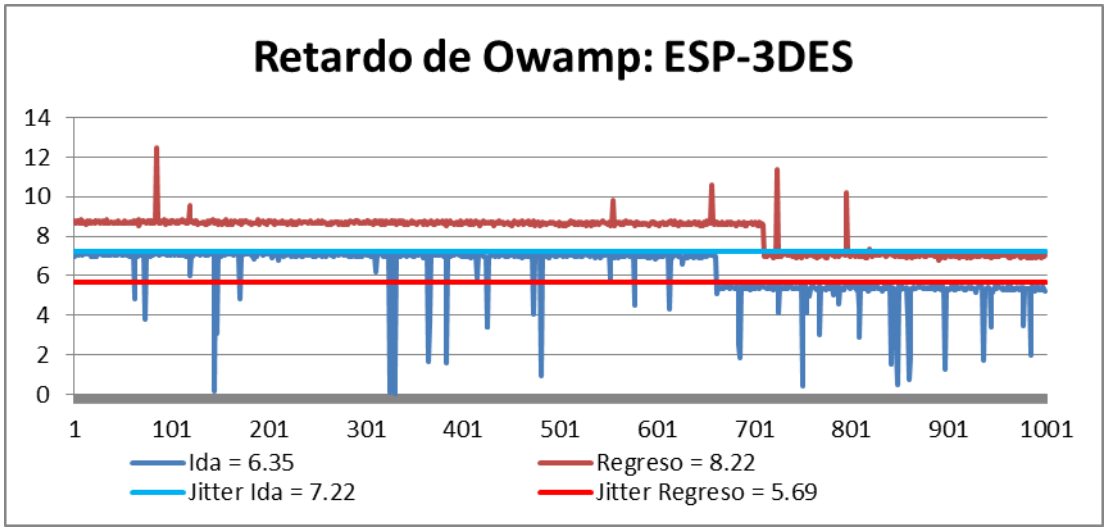


FIGURA 2. 12 RETARDO DE OWAMP ESP-3DES

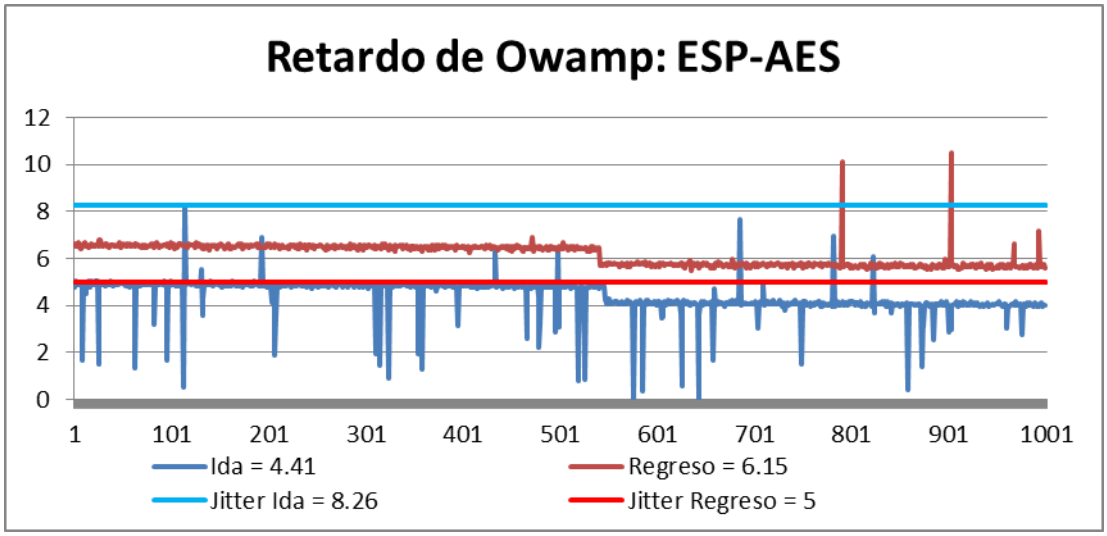


FIGURA 2. 13 RETARDO DE OWAMP ESP-AES

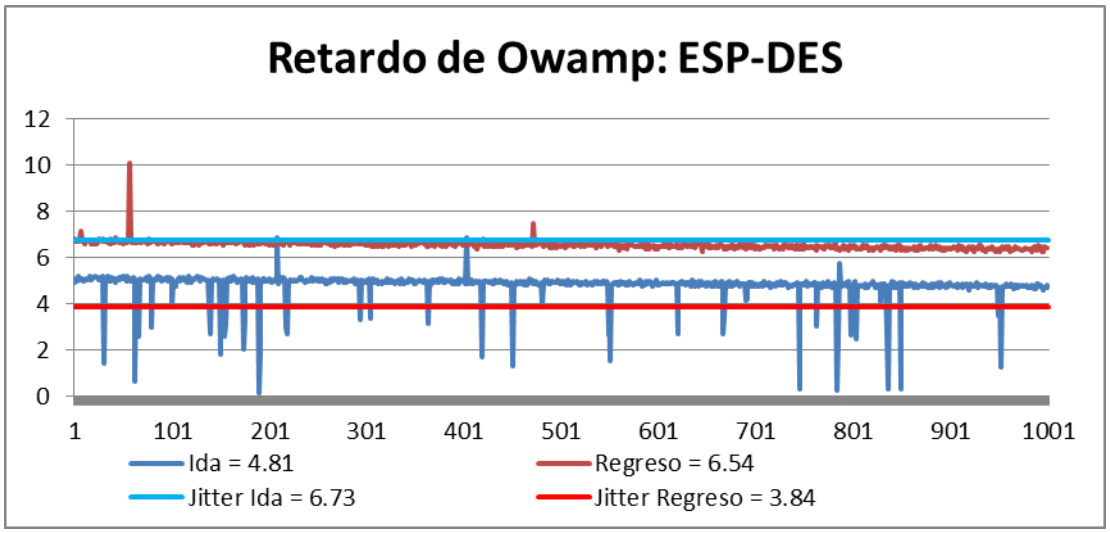


FIGURA 2. 14 RETARDO DE OWAMP ESP-DES

Como se sabe, al tener más variación del retardo las aplicaciones en tiempo real van a requerir mayor tamaño y uso más continuo del *buffer*, así con 3DES se va a requerir una capacidad en él similar a la de AES, pero su uso va a ser más continuo por parte de AES dado que presenta mayores oscilaciones, mientras que con DES la capacidad del *buffer* en términos generales va a ser menor.

En el uso de CPU se puede observar un comportamiento muy interesante; a pesar que 3DES realiza tres veces los procesos DES, el porcentaje de uso de CPU es de 0.19% para ambos, mientras que para AES es de tan solo 0.18 %, un poco menor que los dos anteriores.

Respecto a la velocidad, la información obtenida no es concluyente debido al escaso margen de diferencia; sin embargo, se puede observar que tal como se esperaba, DES es el que presenta una mayor velocidad, seguido por AES y por último se encuentra 3DES.

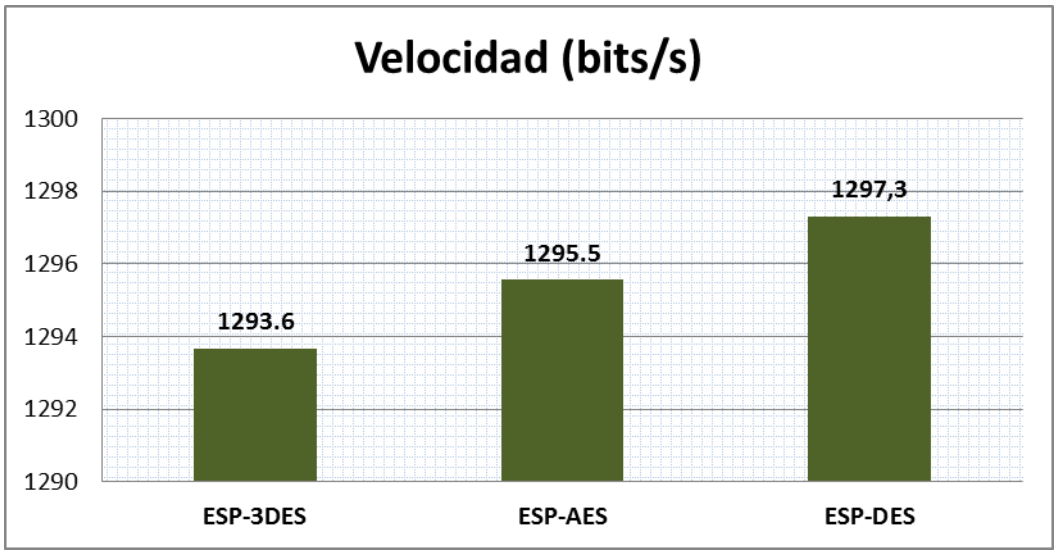


FIGURA 2. 15 VELOCIDAD EN LA SG

3.3.2. DATOS

En la transmisión de datos se puede observar que la CPU presenta valores de uso altos en todas las pruebas, lo cual indica la sobrecarga presentada cuando se realizan procesos asociados a la protección de la información; siendo el valor mínimo de 92.11% por parte de AES, seguido por 3DES con un 93.16% y un poco más arriba DES con un 93.23%.

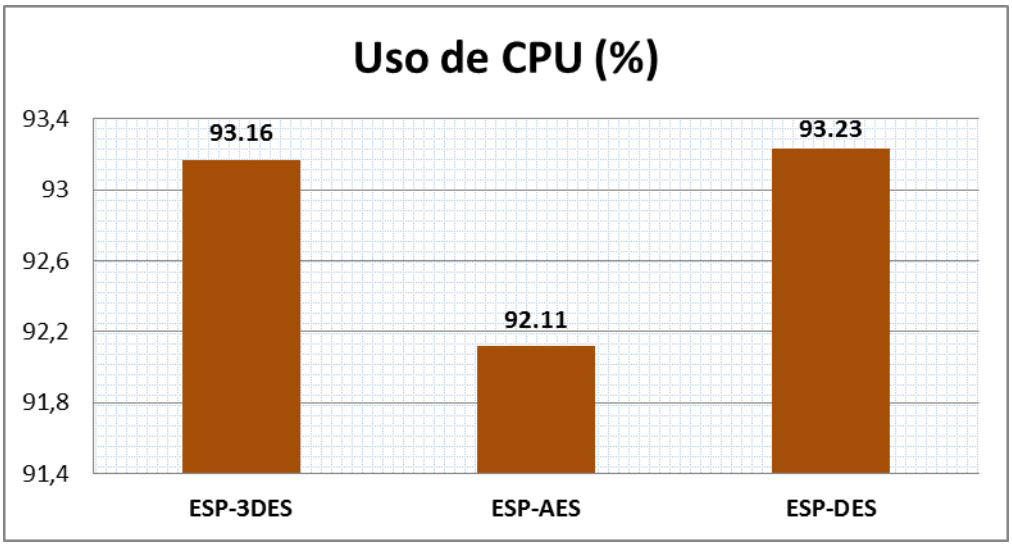


FIGURA 2. 16 USO DE CPU EN LA SG

Las medidas de velocidad obtenidas en esta prueba indican que AES es el que presenta mayor reducción de la velocidad, lo cual se traduce en mayores tiempos de descarga, es decir que se vuelve más lenta la red estando casi 0.9Mb/s por debajo de DES que proporciona una velocidad de 47.67Mb/s, y sorprendentemente 3DES presenta una velocidad de 47.58Mbit/s muy cercana a la de DES.

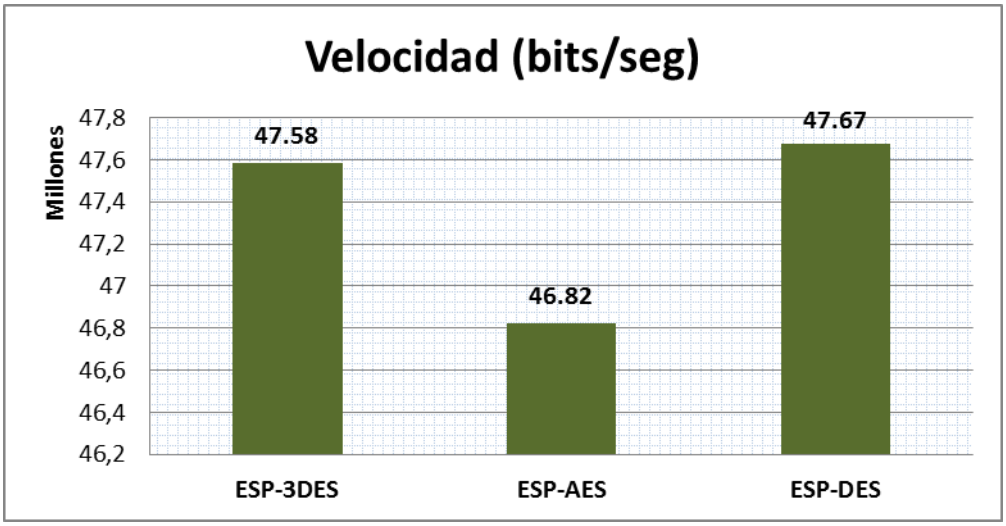


FIGURA 2. 17 VELOCIDAD EN LA SG

3.3.3. VIDEO

Es muy importante resaltar que el comportamiento y las relaciones entre los algoritmos son muy similares a las que se presentaron en las pruebas de FTP, lo que obviamente cambia son los valores de las velocidades como se aprecia en la figura 2.18.

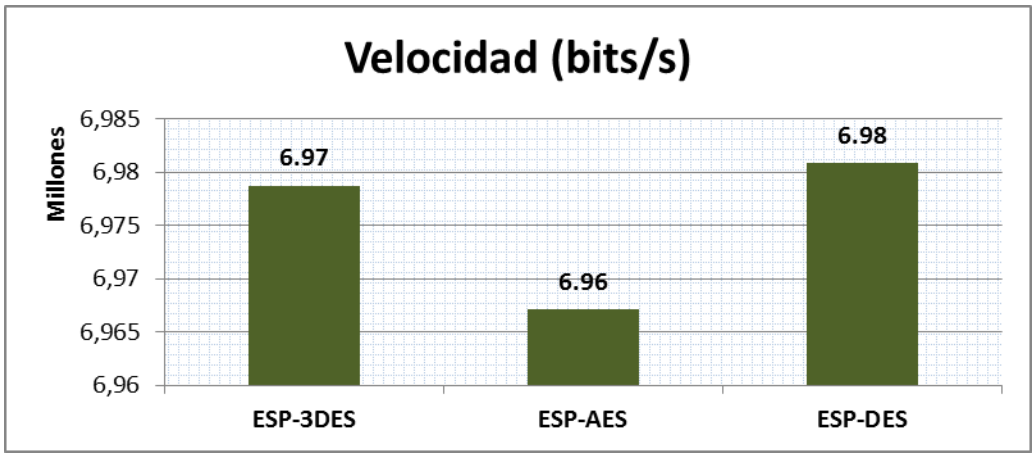


FIGURA 2. 18 VELOCIDAD EN LA SG

Mientras que el uso de CPU muestra algo no visto anteriormente; el algoritmo que más utiliza la CPU es DES con un valor de 15.58% seguido de cerca por 3DES, mientras que el algoritmo que menos utiliza la CPU es AES.

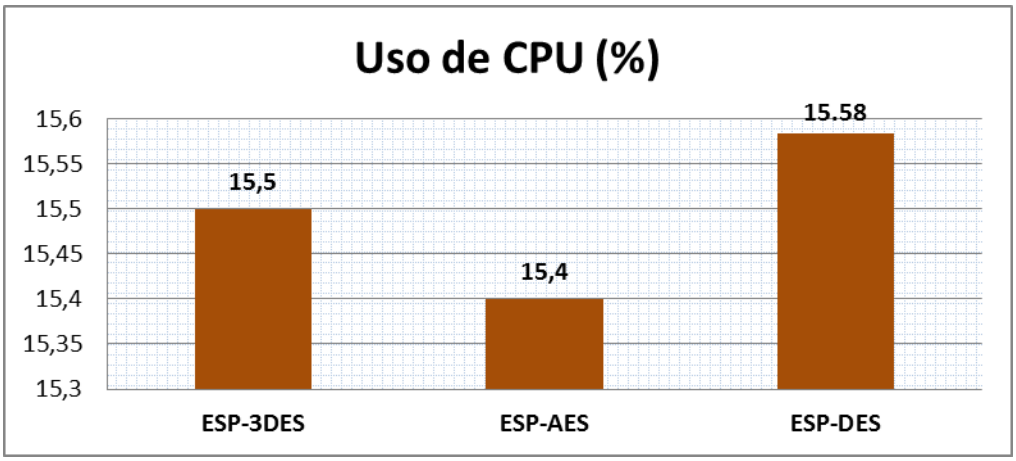


FIGURA 2. 19 USO DE CPU EN LA SG

3.3.4. VOZ

Por otro lado las pruebas de voz muestran a AES como el algoritmo que ocasiona un menor uso del canal, seguido por 3DES con un margen de diferencia de 50bits/s y por DES con 7bits/s más de diferencia.

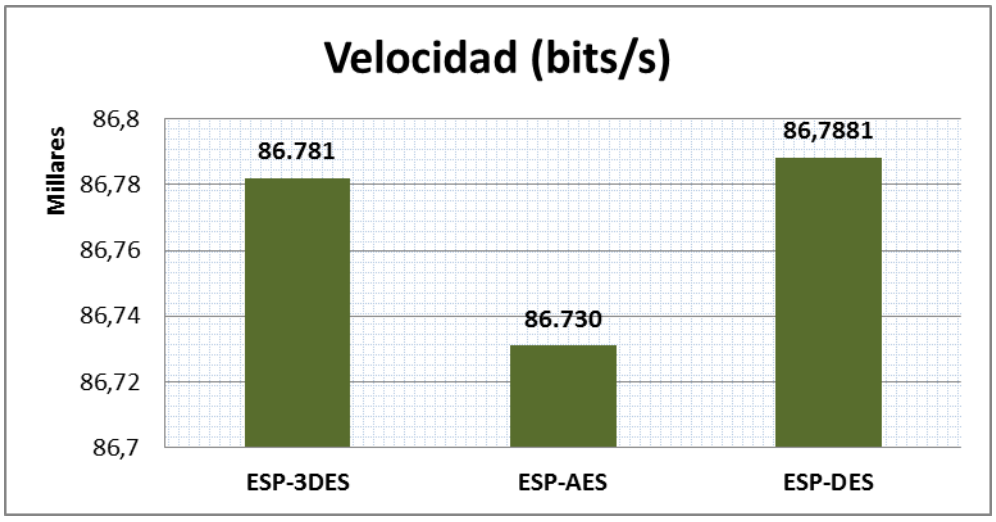


FIGURA 2. 20 VELOCIDAD EN LA SG

Opuestamente al comportamiento anterior es lo mostrado en el uso de CPU, donde el algoritmo que más satura a la CPU es AES, seguido muy de cerca de 3DES, mientras que DES muestra un uso menor de los recursos de procesamiento.

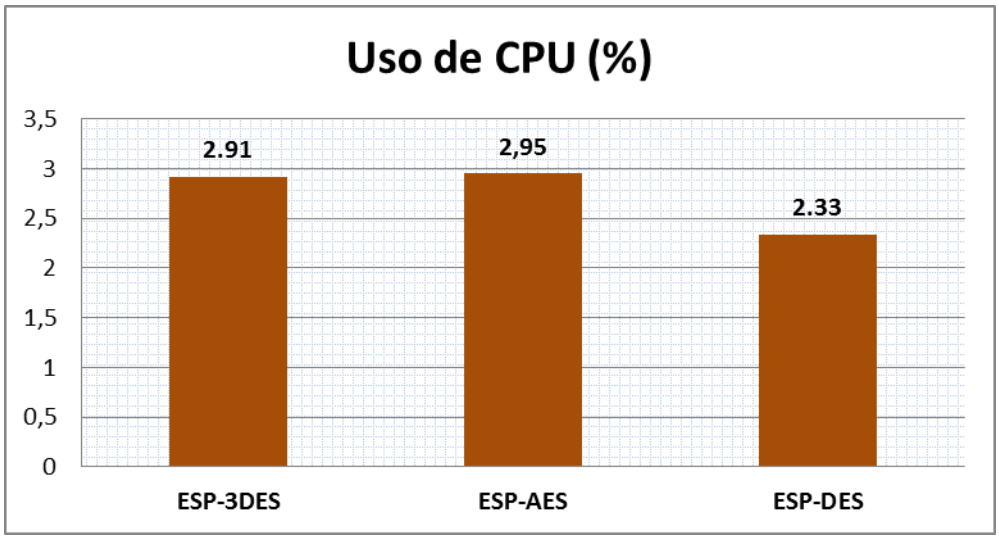


FIGURA 2. 21 USO DE CPU EN LA SG

		3DES	AES	DES
Datos	**Tiempo de Tx.**	389.27 s	395.11 s	388.84
	Uso de CPU	93.16%	92.11%	93.23%
Video	**Velocidad**	6.98Mbps	6.97Mbps	6.98Mbps
	Uso de CPU	15.5%	15.4%	15.58%
Voz	**Velocidad**	86.78kbps	86.73kbps	86.78kbps
	Uso de CPU	2.91%	2.95%	2.33%

TABLA 2. 5 VELOCIDAD Y PORCENTAJE DE USO DE CPU CON ESP

4. ESCENARIO 2: HOST-SG

En este escenario se establecen dos SAs (para comunicación bidireccional) entre el equipo de medición 1 y el enrutador 1, lo cual hace que el tráfico a través de este camino sea protegido por IPsec, pero al pasar el enrutador 1 quede sin protección.

En el equipo de medición se utilizó el programa *VPNClient* de Cisco ya que aunque existen otros clientes disponibles, se decidió trabajar con el cliente Linux proporcionado por Cisco, con el fin de evitar las incompatibilidades y maximizar la eficiencia en los procesos IPsec.

Para las pruebas realizadas en este escenario sólo se tuvieron en cuenta los algoritmos de cifrado AES y 3DES ya que según pruebas preliminares se encontró que el *VPNClient* no negocia Asociaciones de Seguridad con el algoritmo DES y sólo se utilizó el modo túnel debido a que los enrutadores no permitían la configuración en modo transporte. Adicionalmente el *VPNClient* sólo proporciona los servicios de autenticación y confidencialidad conjuntamente utilizando el protocolo ESP, lo que no representa un problema dado que los servicios de autenticación y confidencialidad por separado se evaluaron en el escenario anterior.

Por otro lado, se realizaron pruebas con Owamp, datos y video. En el escenario anterior se observó que el impacto de IPsec en el tráfico de voz no era significativo, y que en su lugar, se podía obtener mejor información del tráfico en tiempo real mediante la emisión de video.

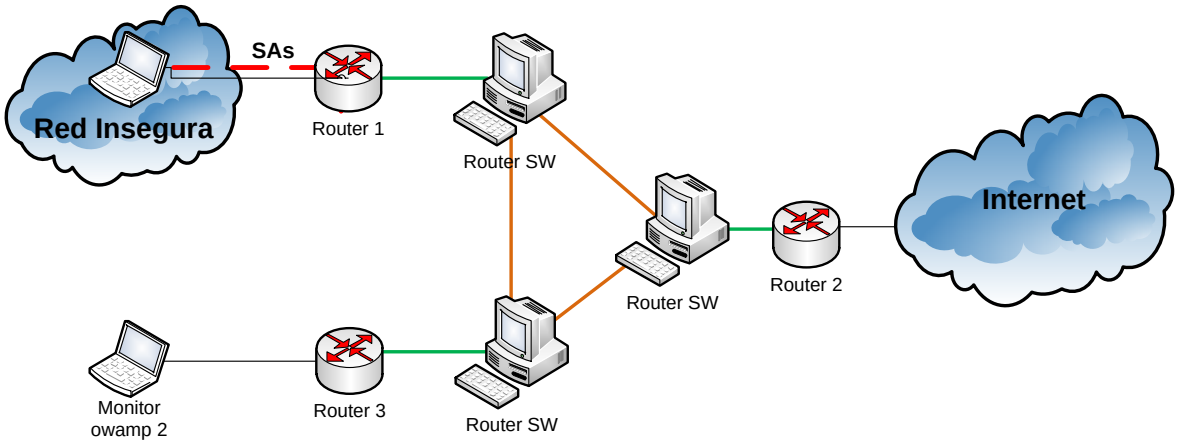


FIGURA 2. 22 ESCENARIO SA ENTRE HOST Y SG

	Host – SG Cisco	Servicio: Protocolo	Modo	Algoritmos	Owamp	Datos	Video
		Autenticación + Confidencialidad: ESP					
1			Tunel	3DES-MD5	✓	✓	✓
2			Tunel	AES-MD5	✓	✓	✓
3			Tunel	3DES-SHA1	✓	✓	✓
4			Tunel	AES-SHA1	✓	✓	✓

TABLA 2. 6 PRUEBAS REALIZADAS EN EL ESCENARIO HOST – SG

4.1 RETARDO Y VARIACIÓN DEL RETARDO

En la prueba de Owamp no se observa una diferencia apreciable en el consumo de CPU, y aunque se nota que hay más tráfico al aplicar IPsec la diferencia de velocidad que muestran la figura 2.23 es de aproximadamente 0.6Kb/s.

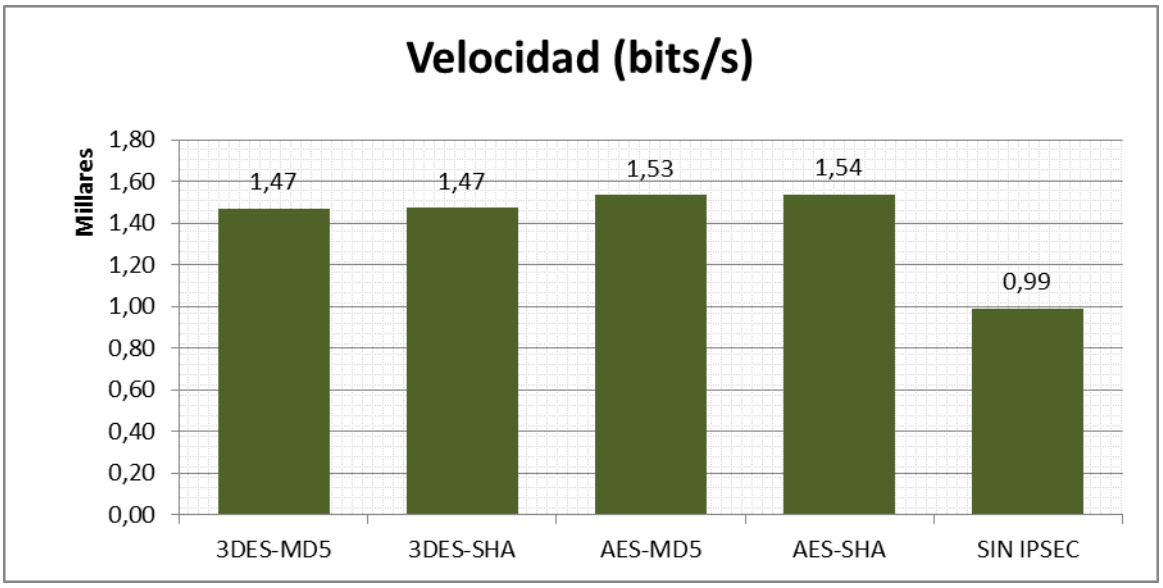


FIGURA 2. 23 VELOCIDAD PROMEDIO EN LAS PRUEBAS DE OWAMP

	3DES-MD5	AES-MD5	3DES-SHA1	AES-SHA1	Sin IPsec
Retardo en la Ida (ms)	2.9 – 4.2	2.39 – 2.95	8.33 – 14.01	3.58 – 5.61	1.43
Variación de retardo en la Ida	6.1 – 6.87	9.81 – 12.05	10.3 – 25.69	13.08 – 16.82	7.88
Retardo al Regreso	4.16 – 5.6	3.36 – 4.25	6.89 – 12.43	1.92 – 4.15	1.16
Variación de retardo al regreso	5.64 – 9.26	4.99 – 5.76	1.85 – 20.01	3.29 – 5.5	4.03

TABLA 2. 7 RETARDO Y SUS VARIACIONES EN EL ESCENARIO HOST-SG

Las combinaciones que utilizan el algoritmo SHA1 para proveer autenticación incrementan la variación del retardo en la Ida con respecto a las que utilizan MD5, asimismo, los datos de la primera fila de la Tabla 2.7 muestran que las combinaciones que utilizan SHA1 presentan un retardo promedio mayor que las que utilizan MD5.

Con respecto a los algoritmos de cifrado es notable que los valores de retardo que se presentan al utilizar 3DES son mayores que al utilizar AES respectivamente; es decir, el retardo que experimentará una transmisión por los procesos IPsec al utilizar 3DES-MD5 serán mayores que con AES-MD5, y las que utilicen 3DES-SHA1 mayores que aquellas con AES-SHA1. Sin embargo, los valores de variaciones de retardo entre los dos algoritmos muestran resultados similares.

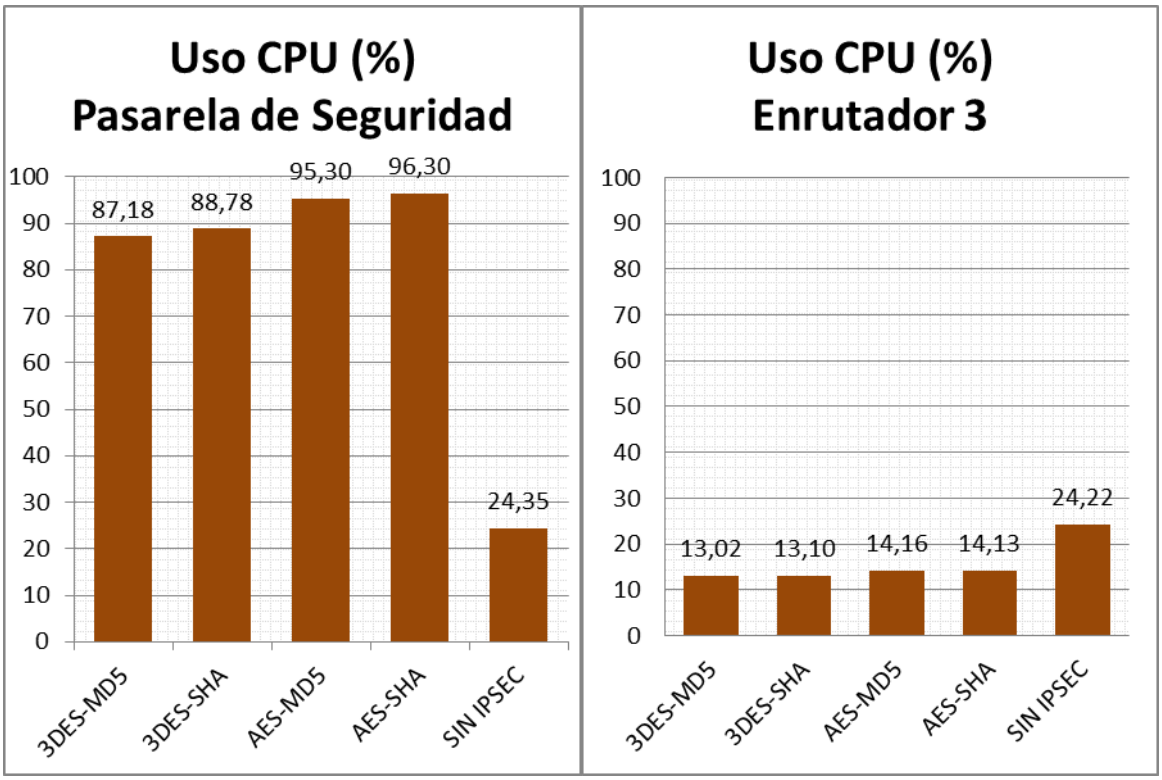
4.2 DATOS

La figura 2.24 permite apreciar el contraste entre el uso que hacen de la capacidad de procesamiento el enrutador que actúa como pasarela de seguridad y el que solo realiza tareas de enrutamiento, asimismo, se observa que las combinaciones que utilizan el algoritmo de cifrado AES requieren mayor consumo de CPU que las que utilizan 3DES.

En la gráfica de Uso de CPU del enrutador 3 (Figura 2.24b) se ve claramente, contrario a lo pensado, que cuando se ha implementado IPsec en el Enrutador 1, el Enrutador 3 usa aproximadamente el 10% menos de CPU; debido posiblemente a que el enrutador 1 debe realizar procesos de cifrado/descifrado con el host lo cual generaría un aumento en el retardo en ese segmento de la red, es decir, el enrutador 1 está enviando los paquetes con un mayor tiempo entre ellos (su tasa de envió de paquetes por segundo disminuye) por lo cual el enrutador 3 tiene más tiempo para procesarlos y no requiere tanta velocidad de procesamiento de la CPU.

Aunque la velocidad de transmisión durante las pruebas con tráfico de datos se reduce notablemente al implementar IPsec, se observa que la velocidad que se puede proveer a un cliente en este escenario es mayor que en el anterior donde la mayor velocidad alcanzada era de 47.68Mbps, mientras que aquí se alcanzaron velocidades promedio de hasta 58.98Mbps.

Por otro lado, entre las cuatro combinaciones realizadas sobresalen las dos que utilizan el algoritmo AES para el cifrado ya que proveen entre 5.68Mbps (con SHA1) y 8.92Mbps (con MD5) más que las combinaciones que utilizan 3DES; mientras que entre MD5 y SHA1 no se establece un impacto claro sobre la velocidad de transmisión de datos.



(a) (b)

FIGURA 2. 24 USO DE CPU EN LOS ENRUTADORES DURANTE LA PRUEBA DE FTP

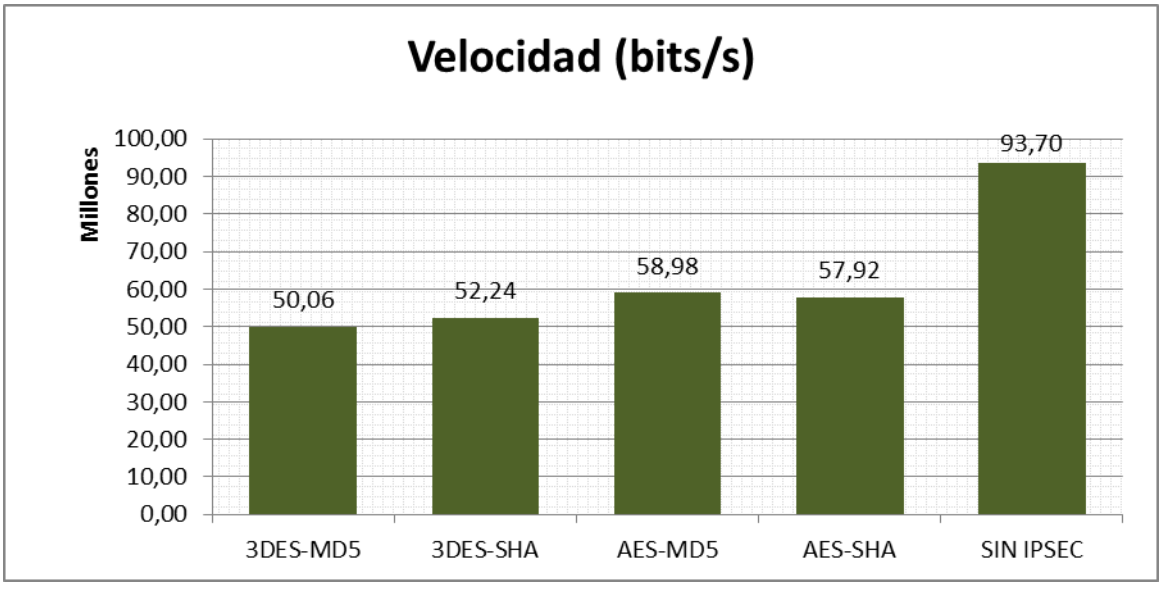


FIGURA 2. 25 VELOCIDAD A LA SALIDA DE LA PASARELA DE SEGURIDAD EN LA PRUEBA DE FTP

4.3 VIDEO

En las pruebas de video también se percibe una reducción de la velocidad de transmisión pero en este caso es pequeña, por lo que la calidad del video no se ve afectada cuando se implementa IPsec. Sin embargo, en los videos capturados se observa que la imagen se congela algunos instantes (con IPsec y sin IPsec), contrario a las pruebas realizadas en el escenario anterior donde la calidad percibida del video era igual a del video original.

El uso de CPU en la pasarela de seguridad se incrementa pero en un porcentaje pequeño, dado que se manejan tasas de transmisión relativamente bajas.

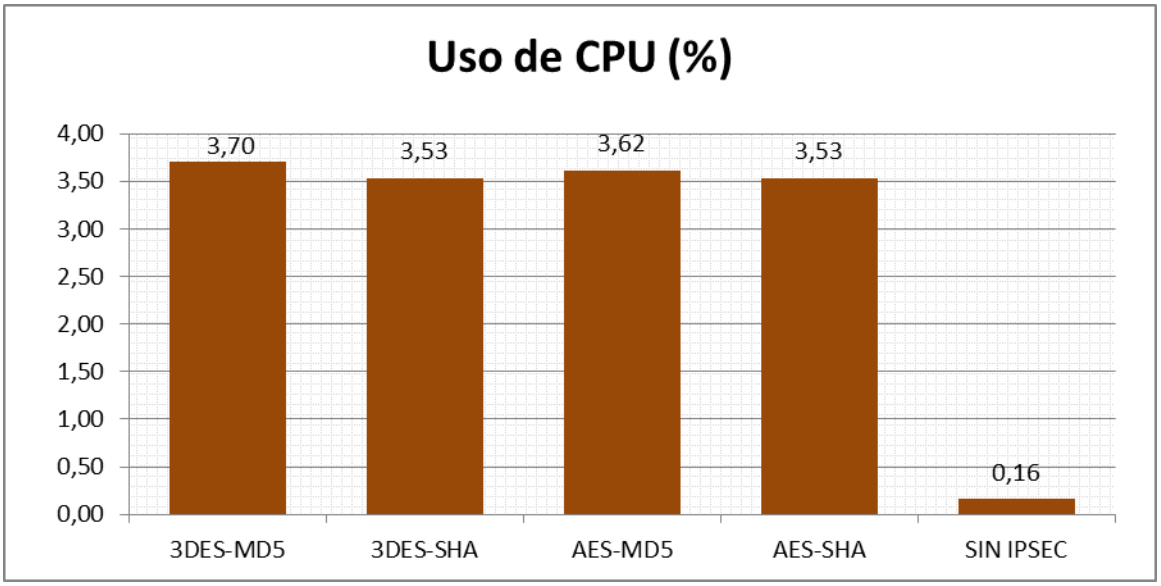


FIGURA 2. 26 USO DE CPU EN LA PASARELA DE SEGURIDAD DURANTE LA PRUEBA DE VIDEO

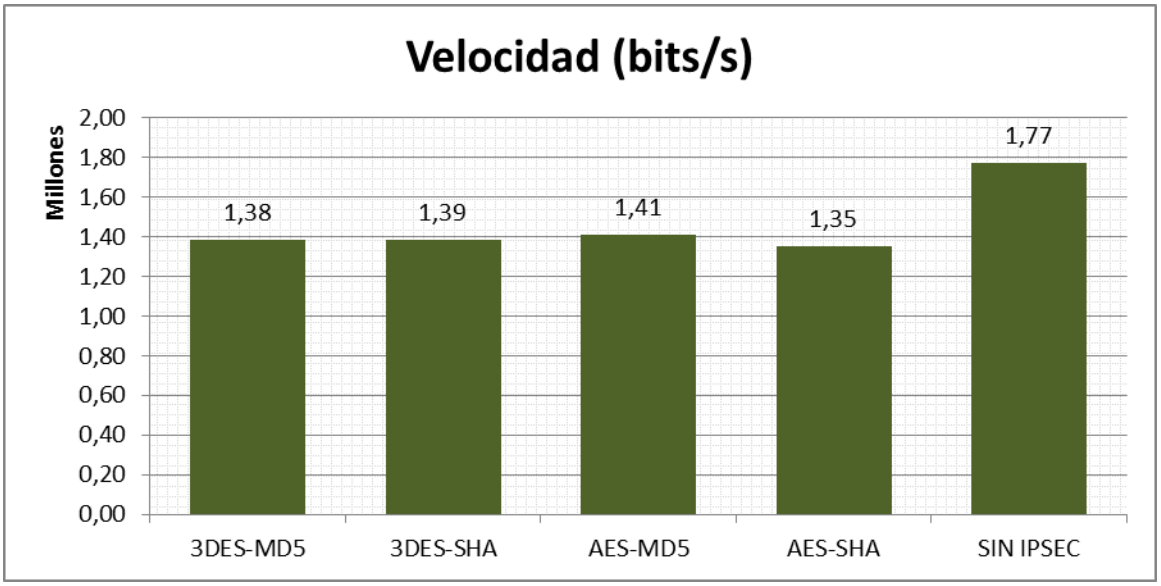


FIGURA 2. 27 VELOCIDAD EN LA PASARELA DE SEGURIDAD DURANTE LA PRUEBA DE VIDEO

A modo de resumen se presenta la siguiente información del funcionamiento de los tráficos de Datos y Video en el escenario Host-SG.

		3DES-MD5	AES-MD5	3DES-SHA1	AES-SHA1	SIN IPSEC
Datos	**Velocidad**	50.06Mbps	58.98Mbps	52.24Mbps	57.92Mbps	93.70Mbps
	Uso de CPU	87.18%	95.30%	88.78%	96.30%	24.35%
Video	**Velocidad**	1.38Mbps	1.41Mbps	1.39Mbps	1.35Mbps	1.77Mbps
	Uso de CPU	3.7%	3.62%	3.53%	3.53%	0.16%

TABLA 2. 8 VELOCIDADES Y USO DE CPU EN LA PASARELA DE SEGURIDAD DEL ESCENARIO HOST-SG

5. ESCENARIO 3 HOST-HOST

Se presenta como el escenario básico en muchos casos, donde los procesos de autenticación, integridad y cifrado se dan en los hosts de origen y destino de la información ocasionando que todo el tráfico entre los extremos viaje protegido por IPsec.

Para este escenario se utilizó la herramienta de software libre OpenSwan que ofrece ventajas sobre las otras como su soporte multiplataforma y la posibilidad de utilizar el Modo Agresivo de ISAKMP que fue utilizado en este trabajo con el fin de forzar el protocolo y algoritmo específico requerido para cada prueba sin darle a los hosts la posibilidad de negociar entre ellos opciones consideradas más seguras.

Como muchas otras implementaciones de IPsec, OpenSwan no ofrece la posibilidad de utilizar AH para proporcionar los servicios de autenticación e integridad sino que los provee utilizando el protocolo ESP ya que, como se mencionaba en el capítulo 1, este protocolo provee además el servicio de confidencialidad. La desventaja de ESP frente a AH en cuanto a la cobertura de la protección de la cabecera IP se subsana haciendo uso del modo túnel en lugar del modo transporte porque de esta forma todo el paquete IP con su cabecera queda encapsulado y con una nueva cabecera IP.

De igual forma, no se permite la configuración de sólo-autenticación (autenticación + integridad) pero si el de sólo-confidencialidad; se permite también la prestación de ambos servicios con el protocolo ESP utilizando algoritmos combinados.

En este escenario no se realizaron pruebas con DES, que ya se había examinado en el primer escenario y ofrece un nivel de seguridad inferior a 3DES y AES con un nivel de desempeño muy similar ya que solo mostró un impacto ligeramente menor al evaluar el consumo de CPU en transmisiones de datos mediante FTP. En su lugar se realizaron pruebas adicionales con el algoritmo Camellia para cifrado que provee OpenSwan.

Camellia es un algoritmo de cifrado por bloques, con un tamaño de bloque de 128 bits y claves de 128, 192 y 256 bits que se caracteriza tanto por su idoneidad para implementaciones hardware y software, como por su alto nivel de seguridad. Este algoritmo ha sido escudriñado ampliamente por la comunicad criptográfica durante varios proyectos de evaluación de cripto-algoritmos; particularmente, siendo seleccionado como primitivo criptográfico por el proyecto EU NESSIE (New European Schemes for Signatures, Integrity and Encryption) y también incluido en la lista de técnicas criptográficas para los sistemas de e-Gobierno Japonés realizado por CRYPTREC (Cryptography Research and Evaluation Committees) [30].

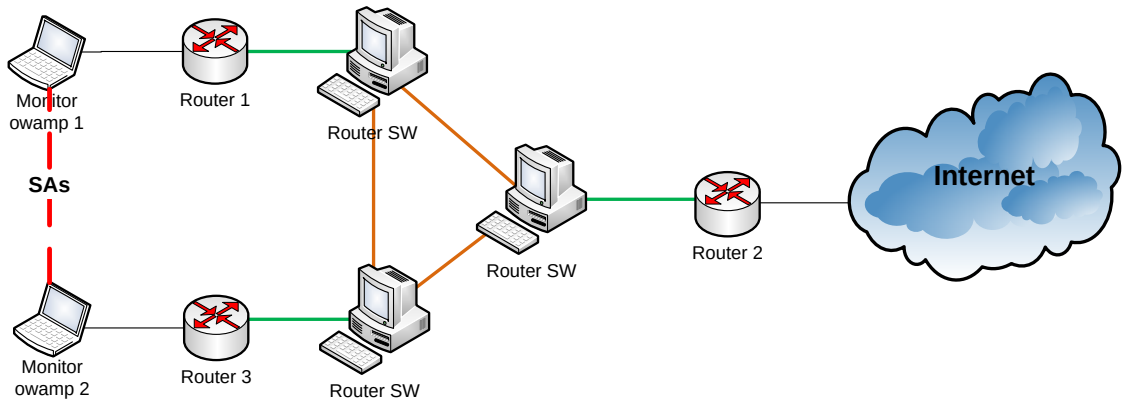


FIGURA 2. 28 ESCENARIO SA ENTRE HOST Y HOST

		Servicio: Protocolo	Modo	Algoritmos	Owamp
	Host – Host OpenSwan	Confidencialidad: ESP:			
1			Tunel	CAMELLIA	✓
2			Tunel	AES	✓
3			Tunel	3DES	✓
4			Transporte	CAMELLIA	✓
5			Transporte	AES	✓
6			Transporte	3DES	✓
		Autenticación + Confidencialidad: ESP			
7			Tunel	AES-MD5	✓
8			Tunel	AES-SHA1	✓
9			Tunel	CAMELLIA-MD5	✓
10			Tunel	CAMELLIA-SHA1	✓
11			Tunel	3DES-MD5	✓
12			Tunel	3DES-SHA1	✓
13			Transporte	AES-MD5	✓
14			Transporte	AES-SHA1	✓
15			Transporte	CAMELLIA-MD5	✓
16			Transporte	CAMELLIA-SHA1	✓
17			Transporte	3DES-MD5	✓
18			Transporte	3DES-SHA1	✓

TABLA 2. 9 PRUEBAS REALIZADAS EN EL ESCENARIO HOST – HOST

5.1. MODOS DE OPERACIÓN

Las pruebas concernientes a comparar el comportamiento de IPsec operando en modo túnel y en modo transporte se realizaron en hosts utilizando el software OpenSwan.

No se pudieron realizar pruebas adicionales referentes a este comportamiento en las pasarelas de seguridad utilizadas (Enrutadores Cisco 2801) ya que aunque se especificara el modo transporte como requerido, no negociaban el funcionamiento en este modo.

Las implementaciones BITW de IPsec que no ofrecen la posibilidad de configuración en modo transporte son bastante frecuentes ya que se establece [2] que el modo transporte debe ser soportado obligatoriamente solo en hosts, mientras que para las pasarelas de seguridad el soporte para modo transporte es opcional y se utiliza sólo en un par de casos específicos mencionados en el capítulo 1.

Como se expuso anteriormente, OpenSwan no permite proveer autenticación mediante AH, ni sólo-autenticación así se realice con ESP; por lo tanto la información es resultado de las pruebas realizadas con ESP para proveer confidencialidad y confidencialidad + autenticación.

5.1.1. ANÁLISIS PARA CONFIDENCIALIDAD

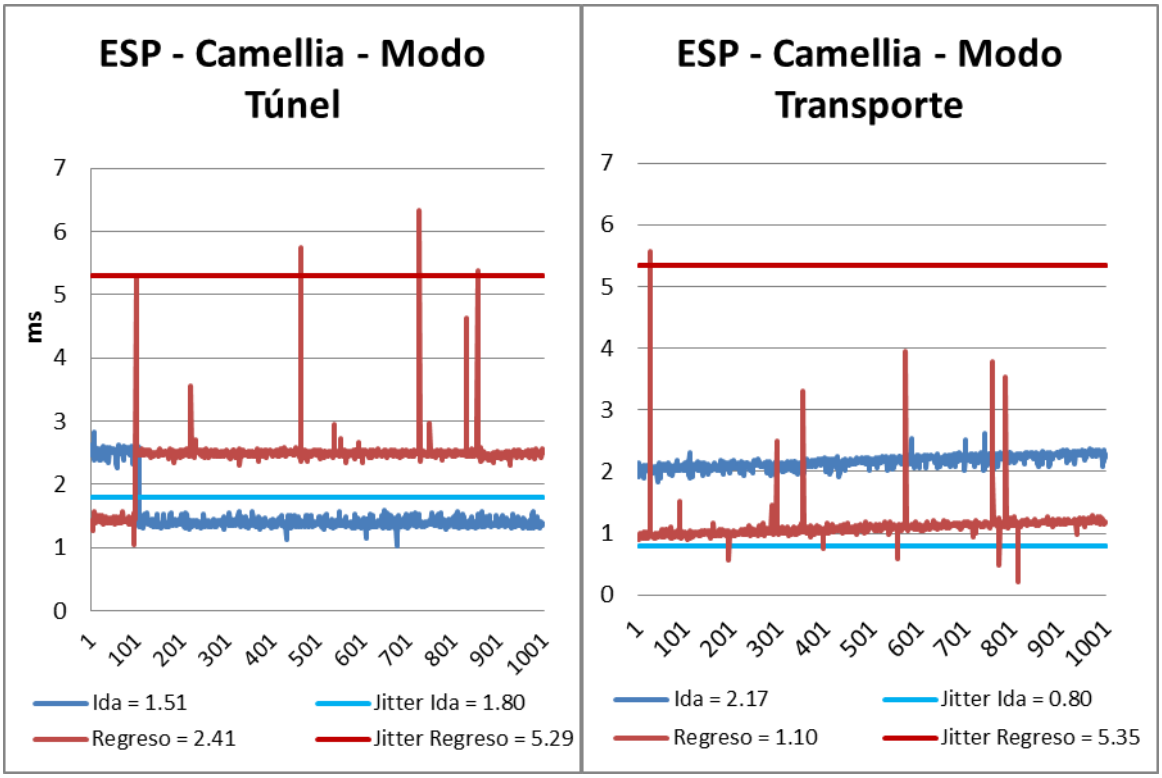
En cuanto al desempeño de la red, proporcionando sólo el servicio de confidencialidad se evaluó el comportamiento del retardo y sus variaciones cifrando con Camellia, AES y 3DES.

Se observó que para Camellia el retardo de ida es mayor en modo transporte mientras que el de regreso es mayor en modo túnel. Para AES se presenta un mayor retardo en modo túnel pero la diferencia es de muy baja magnitud, mientras que para 3DES el retardo es mayor en promedio en modo transporte.

Por otro lado, la variación del retardo se presenta mayor en algunos casos en modo transporte y en otros en modo túnel por lo que no se puede establecer claramente el impacto del modo de operación en la variación del retardo que se presenta al cifrar la información; sin embargo, aunque se presentan puntos de inflexión con similar frecuencia para los dos modos, estos generalmente tienen mayor amplitud en modo transporte.

A continuación se muestran las gráficas de Camellia en modo túnel y transporte (figura 2.29), las demás gráficas utilizadas para la comparación entre los modos de operación de IPsec se pueden encontrar en los anexos. Sin embargo, se muestra la tabla de resumen

2.10 con los rangos de valores obtenidos en retardo y variación de retardo para ambos modos de operación al proporcionar Confidencialidad con Camellia, AES y 3DES.



(a) (b)

FIGURA 2. 29 RETARDO Y SUS VARIACIONES CON CAMELLIA EN AMBOS MODOS DE OPERACIÓN

	Camellia		AES		3DES	
	Túnel	Transporte	Túnel	Transporte	Túnel	Transporte
Retardo en la Ida	1.51 - 2.39	2.17 - 2.64	1.06-1.87	1.04 - 1.33	0.54-0.61	0.11 - 1.46
Variación de retardo	0.64-1.8	0.8 - 0.83	0.68 - 2.07	0.65 - 1.69	0.66 - 1.57	0.5 - 0.58
Retardo al Regreso	1.29-2.41	1.1 - 1.56	0.62-0.78	0.06 - 0.27	0.5 - 1.13	1.05 - 2.6
Variación de retardo	5.29 - 6.15	2.33 - 5.34	2.84 - 5.30	4.5 - 7.38	2.41 - 7.33	4.05 - 5.75

TABLA 2. 10 RETARDO Y SUS VARIACIONES PARA CONFIDENCIALIDAD EN AMBOS MODOS DE OPERACIÓN

5.1.2. ANÁLISIS PARA CONFIDENCIALIDAD + AUTENTICACIÓN

En la combinación de 3DES con MD5 se presenta mayor variación de retardo en modo túnel y los puntos de puntos de inflexión en este modo se presentan con mayor amplitud aunque con menor frecuencia. En modo transporte se presentan picos de retardo

menores, pero se observan variaciones de pequeña amplitud en la mayoría de los paquetes. El retardo en general no muestra resultados concluyentes.

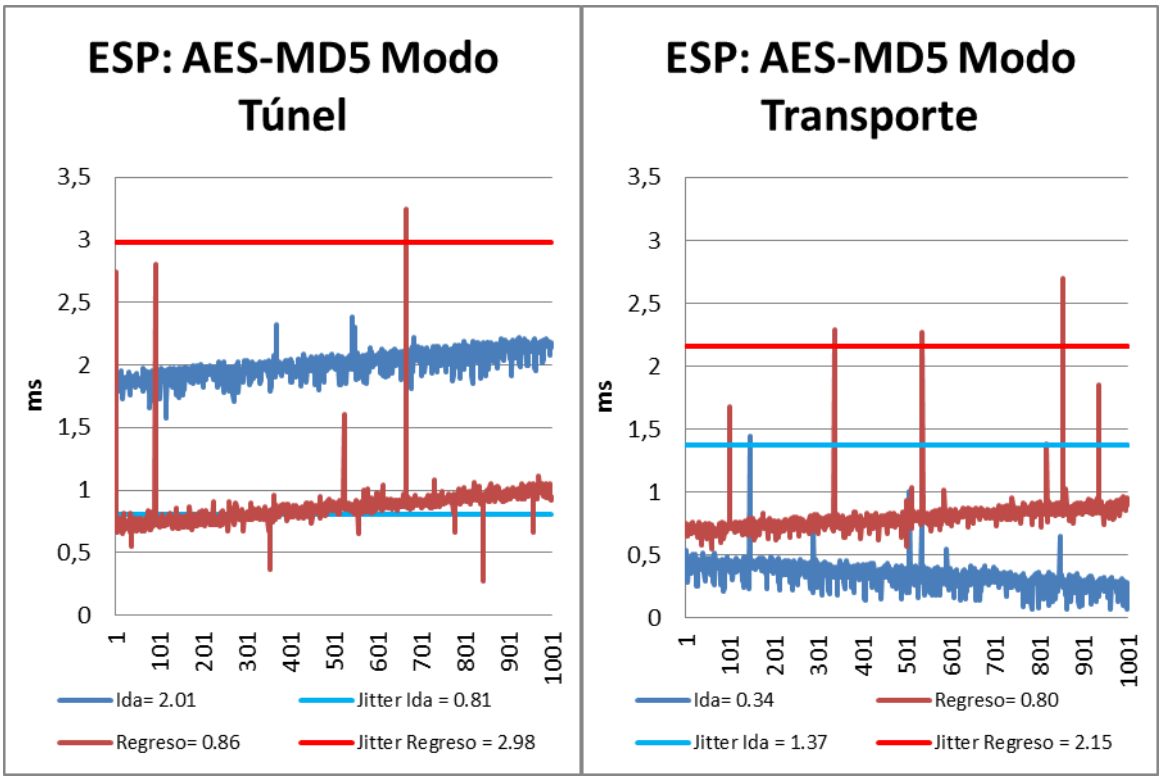
Para 3DES con SHA1 el mayor retardo en general se da en modo transporte, la variación de retardo al regreso es mayor en modo túnel mientras que a la ida es mayor en modo transporte. En modo transporte se presentan cambios bruscos pero sostenidos de retardo parecidos a “escalones” con bajas amplitudes que no se presentan en modo túnel, por otro lado hay una cantidad similar de puntos de inflexión pero con mayores amplitudes en modo transporte.

AES con MD5 presenta mayor retardo promedio en modo túnel y la variación del retardo es similar en los dos modos de operación; sin embargo, en la figura 2.30 se observan más variaciones con baja amplitud en modo transporte y mayor cantidad de puntos de inflexión aunque sus amplitudes son en general similares a los del modo túnel.

Al combinar AES con SHA1 se observa mayor retardo en promedio en el modo túnel, y mayor cantidad de variaciones de baja amplitud en modo transporte, así como puntos de inflexión en mayor cantidad pero menor amplitud al trabajar en modo transporte.

Para Camellia con MD5 se observa un mayor retardo pero más estabilidad en modo túnel, tanto en modo túnel como en transporte se presentan pocos puntos de inflexión aunque de gran amplitud.

Camellia con SHA1 presenta retardo en promedio similar en modo túnel y modo transporte, y como en la combinación anterior, la variación del retardo es similar mostrando pocos puntos de inflexión con gran amplitud.



(a) (b)

FIGURA 2. 30 RETARDO Y SUS VARIACIONES CON AES-MD5 EN AMBOS MODOS DE OPERACIÓN

CAPITULO III

EVALUACIÓN DE LAS COMBINACIONES DE LOS PROTOCOLOS DE IPSEC

1. INTRODUCCIÓN

En este capitulo se detallan las pruebas y análisis realizados para cumplir el segundo objetivo planteado en el anteproyecto del presente trabajo de grado con el cual se busca, después de haber analizado independientemente los protocolos AH y ESP con sus algoritmos relacionados; evaluar y analizar las combinaciones que surgen entre ellos al prestar los servicios de confidencialidad e integridad mediante Asociaciones de Seguridad indepedientes, como se presenta comúnmente en escenarios reales.

2. ESCENARIOS Y COMBINACIONES PLANTEADAS

Como guía para determinar los escenarios se utilizó la sección 4 de la segunda versión de la especificacion de la Arquitectura IPsec [10], donde se exponen las principales combinaciones que deben soportar las implementaciones IPsec. Aunque en la última versión de la arquitectura ya no se requiere soporte para estas SAs anidadas dado que la misma funcionalidad se puede obtener mediante la configuración de la SPD y las tablas de reenvío; estas combinaciones representan un buen ejemplo de los escenarios que se pueden presentar en la realidad.

En la parte de Combinaciones Básicas de SAs (sección 4.5) del RFC 2401 se exponen cuatro ejemplos, donde los dos primeros (Host-Host y SG-SG) utilizan una sola asociación de seguridad y corresponden a los escenarios 3 y 1 de la primera parte de este proyecto, éstos se trabajaron en el capítulo anterior; mientras que el tercero (túnel de Hosts dentro de otro túnel entre SGs) se presenta en la sección 2.2 y el cuarto (Acceso Remoto o Road Warrior) en la sección 2.3 de este capítulo.

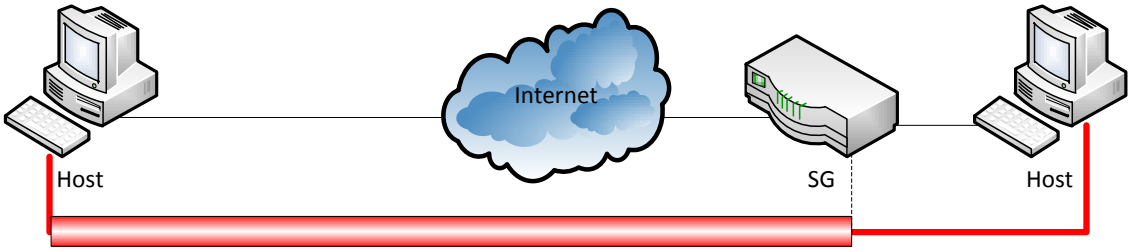


FIGURA 3. 1 ESCENARIO DE ACCESO REMOTO

Al hablar de Asociaciones de Seguridad anidadas, es decir, con dos o más SAs, se presentan dos posibilidades: Adyacencia de Transporte y Túneles Iterados. En el primer caso las SA se configuran en modo transporte y sólo se utiliza un nivel de anidación porque mayores niveles no proporcionan beneficios adicionales, esto debido a que todo el procesamiento IPsec se da en el último destino; mientra tanto, con la segunda opción se pueden dar múltiples niveles de anidado, y aunque se presentan tres casos sólo se requiere soporte para el 2do y el 3ro que se presentan en las Figuras 3.1 y 3.2. El caso adicional de túneles iterados se presenta cuando se realizan dos o más túneles cuyos extremos son los hosts (origen y destino) de la comunicación.

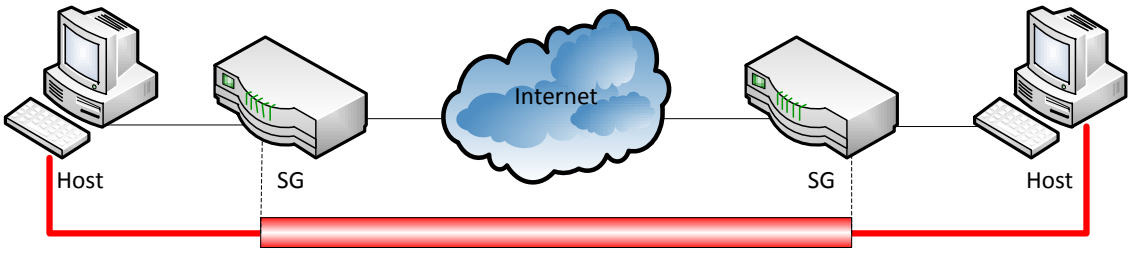


FIGURA 3. 2 SAS EN TÚNELES ITERADOS

2.1 SAS ENTRE PASARELAS DE SEGURIDAD

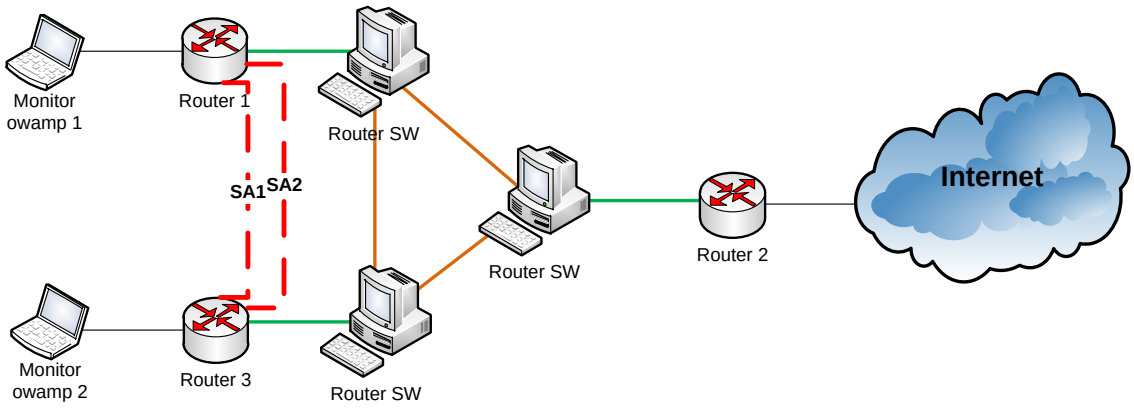


FIGURA 3. 3 ESCENARIO SG-SG CON DOBLE SA

Adicional a los escenarios anteriormente mencionados, se realizó este con el fin de poder comparar el desempeño de IPsec al proporcionar los mismos servicios de seguridad mediante la configuración mostrada en el escenario SG-SG que se presentó en la sección 3 del capítulo anterior, con la que se utiliza aquí. En el caso anterior se ofrecían los servicios de confidencialidad y autenticación con una sola SA utilizando ESP, mientras que en este se provee confidencialidad con ESP y autenticación con AH utilizando 2 SAs anidadas.

Sobre este escenario se desarrollaron tanto pruebas de Owamp como pruebas de Datos y Video. En esta sección se presentan los resultados obtenidos en las pruebas de retardo y variación de retardo.

Se encontró que en este escenario la combinación que presento los menores valores de retardo fue la prestación del servicio de autenticación con AH utilizando al algoritmo SHA1 y de confidencialidad con ESP utilizando el algoritmo 3DES. Además, esta combinación también fue la que tuvo una menor variación de retardo, lo que permite resaltar su eficiencia en este escenario.

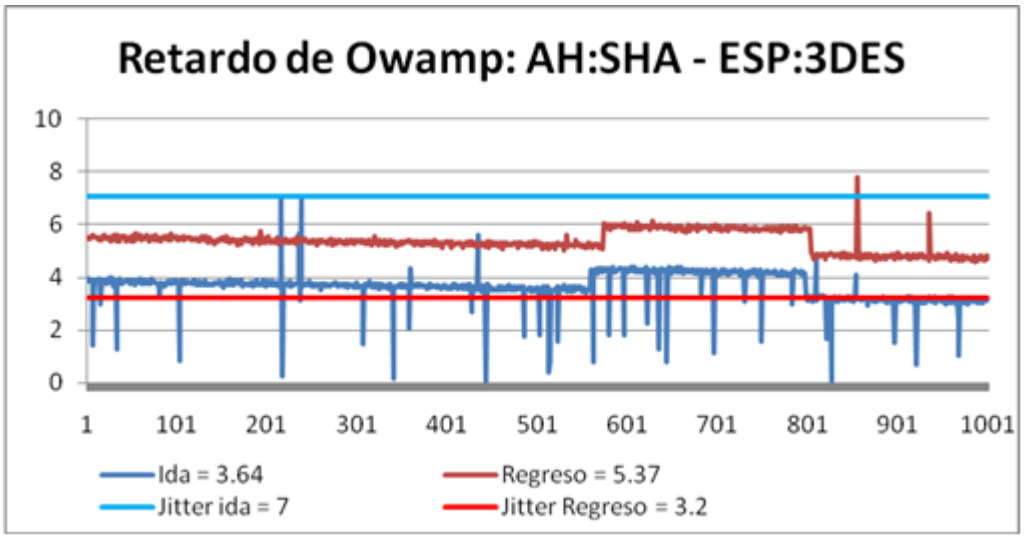


FIGURA 3. 4 RETARDO DE OWAMP PARA AH CON SHA1 Y ESP CON 3DES

Por otro lado la combinación que tuvo un mayor valor de retardo fue la prestación del servicio de autenticación con AH utilizando al algoritmo MD5 y de confidencialidad con ESP utilizando el algoritmo AES; además esta combinación fue la que presentó un mayor valor en la variación de retardo.

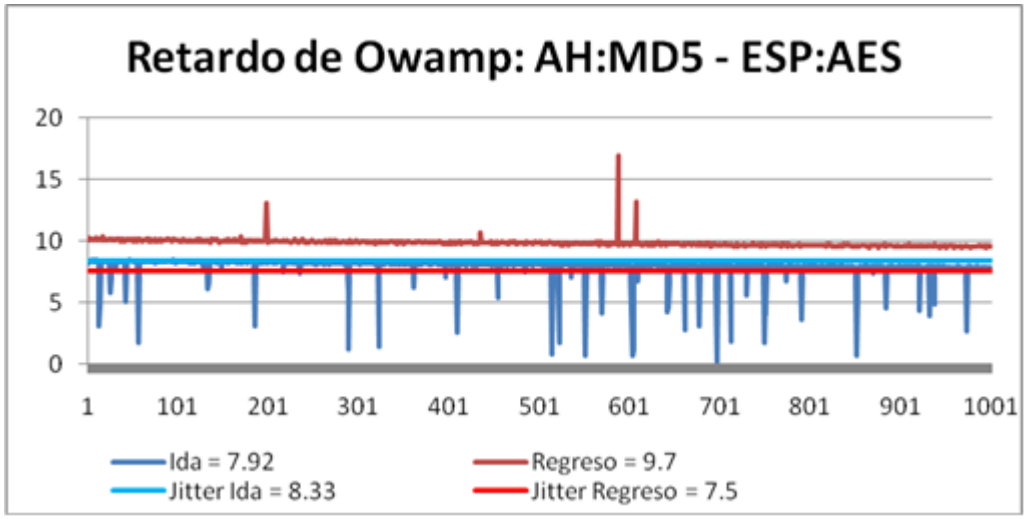


FIGURA 3. 5 RETARDO DE OWAMP PARA AH CON MD5 Y ESP CON AES

Por lo anterior se puede decir que cuando se implementa SHA1 como algoritmo de autenticación para AH, tiene un comportamiento mucho más liviano que MD5 dado que introduce un menor retardo asociado a IPsec en la red, aunque su volatilidad sea superior. Además es de resaltar la eficiencia del algoritmo de confidencialidad 3DES, dado que supera a su antecesor DES en cuanto a desempeño, a pesar de realizar 3 veces los procedimientos del anterior.

Por otro lado se realizó una tabla (3.1) comparativa entre las combinaciones para determinar que algoritmo de autenticación es más eficiente en cada caso, como se muestra a continuación:

	3DES – MD5	3DES – SHA1
Retardo	7.3 – 9.13	3.64 – 5.37
Variación de retardo	1.12 – 10.57	3.2 - 7.04
Ganador		✓

TABLA 3. 1 COMPARACIÓN ENTRE MD5 Y SHA1, UTILIZANDO 3DES PARA CIFRADO

Por lo tanto, cuando se utilice 3DES como algoritmo de confidencialidad para ESP, y además se desea utilizar un algoritmo para brindar autenticación con AH, la mejor opción (de las evaluadas) en cuanto a desempeño sería SHA1.

	AES – MD5	AES – SHA1
Retardo	7.92 – 9.7	5.93 – 7.77
Variación de retardo	7.5 - 8.33	4.5 – 7.88
Ganador		✓

TABLA 3. 2 COMPARACIÓN ENTRE MD5 Y SHA1, UTILIZANDO AES PARA CIFRADO

Asimismo, el mejor algoritmo de autenticación con AH es SHA1, cuando éste es utilizado con AES como algoritmo de confidencialidad para ESP.

	DES – MD5	DES - SHA1
Retardo	7.86 – 9.62	4.89 – 6.66
Variación de retardo	5.08 - 10.48	2.66 - 6.44
Ganador		✓

TABLA 3. 3 COMPARACIÓN ENTRE MD5 Y SHA1, UTILIZANDO DES PARA CIFRADO

De nuevo SHA1 se muestra como la mejor opción entre ambos algoritmos de autenticación, en este caso al utilizar DES como algoritmo de confidencialidad para ESP.

A) COMPARACIÓN ENTRE SERVICIOS UTILIZANDO SÓLO ESP Y AH+ESP

En la actualidad muchas implementaciones no ofrecen siquiera la opción de utilizar AH para el servicio de integridad, al punto de que la última versión de IPsec ya no requiere que se implemente este protocolo sino que permite que todos los servicios de seguridad se puedan prestar solamente con ESP; por lo anterior, como análisis complementario, se evaluó como varía el desempeño de una red cuando se prestan estos servicios utilizando sólo ESP o cuando se utiliza el protocolo AH para proveer el de integridad.

Con los resultados de las pruebas se crearon tablas para poder realizar las comparación, donde al utilizar las mismas combinaciones de algoritmos (utilizando 3DES, DES y AES, con MD5 y SHA1) se varían los protocolos que los utilizan y que permiten establecer el o los protocolo(s) que generen menor impacto en el desempeño de la red.

Las tablas 3.4 y 3.5 contienen la información correspondiente a las combinaciones que hacen uso de 3DES.

	ESP: 3DES AH: MD5	**ESP: 3DES Y MD5**
Retardo ida(ms)	7.31 - 8.73	12.7 – 20.81
Variación de retardo	9.87 – 10.57	15.5 - 22.5
Retardo regreso	9.13 – 10.64	10.9 - 18.84
Variación de retardo	1.12 – 7.66	14.2 – 17
Ganador	✓	

TABLA 3. 4 COMPARACIÓN ENTRE AH+ESP Y ESP CON MD5, UTILIZANDO 3DES PARA CONFIDENCIALIDAD

	ESP: 3DES AH: SHA1	**ESP: 3DES Y SHA1**
Retardo ida(ms)	3.64 – 5.27	2.19 – 8.14
Variación de retardo	6.76 – 7.04	11.07 – 23.97
Retardo regreso	5.37 – 7	3.74 - 8
Variación de retardo	3.2 – 4.94	3.14 – 7.64
Ganador	✓	

TABLA 3. 5 COMPARACIÓN ENTRE AH+ESP Y ESP CON SHA1, UTILIZANDO 3DES PARA CONFIDENCIALIDAD

Cuando se utiliza MD5 para proveer autenticación de los datos y 3DES para la confidencialidad, se observa claramente que los valores de retardo y variación de retardo son menores si la autenticación se provee con AH y la confidencialidad con ESP, ya que

con la misma combinación haciendo uso solamente del protocolo ESP los valores de retardo y su variación son notablemente mayores.

Además, los resultados respecto a 3DES muestran algo muy interesante; el comportamiento de la combinación ya sea con MD5 o SHA1 es mucho mejor si la autenticación es brindada por AH, lo cual indica que aunque este protocolo no sea ampliamente usado es muy compatible con los procesos desarrollados por ESP al utilizar el algoritmo 3DES.

A continuación, se pasa a analizar los resultados de las combinaciones con AES.

	ESP: AES AH: MD5	**ESP: AES Y MD5**
Retardo ida(ms)	7.92 – 13	6.41 - 6.87
Variación de retardo	8.34 – 12.37	13.58 – 18.66
Retardo regreso	9.78 – 14.86	4.62 - 4.99
Variación de retardo	1 – 7.5	2.27 - 4
Ganador		✓

TABLA 3. 6 COMPARACIÓN ENTRE AH+ESP Y ESP CON MD5, UTILIZANDO AES PARA CONFIDENCIALIDAD

	ESP: AES AH: SHA1	**ESP: AES Y SHA1**
Retardo ida(ms)	5.93 – 10.4	3.61 – 4.39
Variación de retardo	7.89 – 10.77	12 – 15.33
Retardo regreso	7.7 – 12.3	1.82 – 2.53
Variación de retardo	1.89 – 4.57	0.9 – 2.33
Ganador		✓

TABLA 3. 7 COMPARACIÓN ENTRE AH+ESP Y ESP CON SHA1, UTILIZANDO AES PARA CONFIDENCIALIDAD

Por otro lado, las combinaciones con AES muestran un comportamiento en términos generales opuesto al presentado con 3DES tanto en retardo como en la variación de retardo; es decir, cuando los servicios de autenticación y confidencialidad son proporcionados solo por ESP se tiene un mejor comportamiento. Así, aunque la variación de retardo en la ida muestra una relación inversa (menor al utilizar AH) tanto con MD5 como con SHA1, en términos generales se puede concluir que si se va a utilizar el algoritmo AES para proveer confidencialidad y asimismo se requiere autenticación, es más eficiente proveer ambos con ESP.

Además, al comparar las últimas columnas de las tablas 3.6 y 3.7 se observa que si se va a proveer autenticación usando sólo ESP, además de confidencialidad (con AES), se genera menor retardo y variación del mismo al preferir SHA1 en lugar de MD5.

Por último se realizó el mismo análisis para las combinaciones obtenidas con DES.

	ESP: DES AH: MD5	**ESP: DES Y MD5**
Retardo ida(ms)	7.86 – 8.55	4.14 – 9.9
Variación de retardo	8.32 – 10.48	20 – 79.32
Retardo regreso	9.62 – 10.35	2.5 - 7.89
Variación de retardo	2.64 – 5.08	1.7 – 8.45
Ganador	✓	

TABLA 3. 8 COMPARACIÓN ENTRE AH+ESP Y ESP CON MD5, UTILIZANDO DES PARA CONFIDENCIALIDAD

	ESP: DES AH: SHA1	**ESP: DES Y SHA1**
Retardo ida(ms)	4.89 – 10.5	4.6 – 6
Variación de retardo	6.44 – 13.27	12.31 – 13.49
Retardo regreso	6.66 – 12.3	2.74 – 4.22
Variación de retardo	2.67 – 12.8	0.75 – 2.09
Ganador		✓

TABLA 3. 9 COMPARACIÓN ENTRE AH+ESP Y ESP CON SHA1, UTILIZANDO DES PARA CONFIDENCIALIDAD

Los resultados muestran que al utilizar DES al tiempo con MD5, la relación de mejor comportamiento se mantiene excepto en el retardo de regreso, así, en términos generales se puede decir que el comportamiento es mejor si se utiliza AH para el proceso de autenticación.

Por otro lado, respecto al uso de SHA1 la relación también se mantiene excepto en este caso en el valor de retardo de ida, así, cuando se utiliza solo ESP el comportamiento es mucho mejor que cuando se utiliza AH en la parte de la autenticación, tanto en retardo como en la variación de retardo.

2.2 ASOCIACIONES DE SEGURIDAD ITERADAS

Este escenario se presenta en los casos en que los usuarios desean cifrar la información entre ellos para obtener confidencialidad, mientras que el administrador de la red ya

provee uno o más de servicios como autenticación, integridad, control de acceso y antirrepetición, entre dos pasarelas de seguridad a las cuales se conectan los usuarios.

En este escenario la seguridad proporcionada por IPsec consta de un par de SAs 1 entre los equipos de medición, es decir extremo a extremo, y otro par de SAs 2 entre los enrutadores 1 y 3; lo anterior exhibe el comportamiento de un túnel dentro de otro túnel donde en primer lugar se cifra la información y se envía por el túnel que va entre los hosts y en segundo lugar se autentica la información ya cifrada y se envía en el túnel entre las dos pasarelas de seguridad.

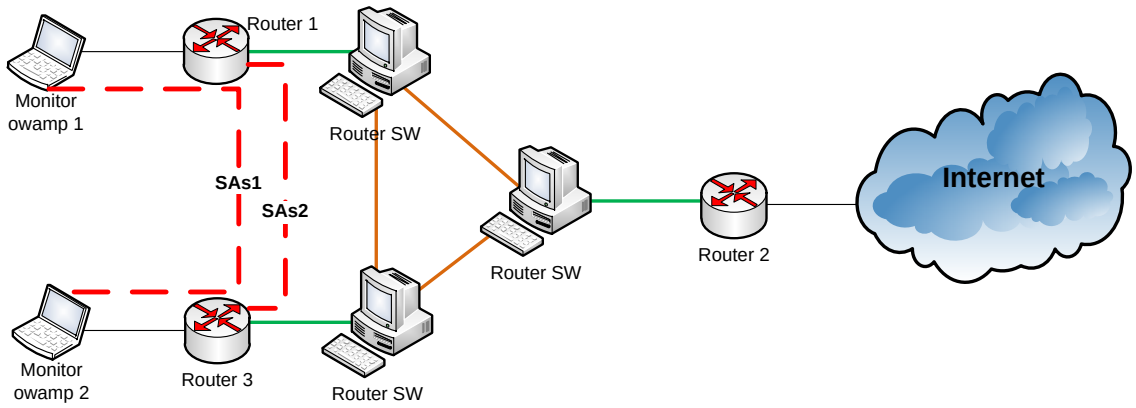


FIGURA 3. 6 ESCENARIO CON SAS ENTRE HOSTS Y ENTRE SGS

Además de las mencionadas anteriormente, en las que se realiza cifrado en la SA interna y autenticación en la externa; se realizaron pruebas para obtener más información del comportamiento de las SA iteradas, las cuales se detallan a continuación con sus respectivos resultados:

		SAs entre Hosts (Internas)	SAs entre SGs (Externas)	Owamp	Datos	Video
1	Host-Host OpenSwan Modo Túnel	3DES	AES	✓	✓	✓
2		AES	3DES-MD5	✓	✓	✓
3		AES	3DES-SHA1	✓	✓	✓
4		AES-SHA1	3DES	✓	✓	✓
5	SG - SG Cisco 2801 Modo Túnel	AES-SHA1	3DES-MD5	✓	✓	✓
6		AES	3DES	✓	✓	✓
7		AES	MD5	✓	✓	✓
8		AES	SHA1	✓	✓	✓
9		AES-MD5	3DES	✓	✓	✓

TABLA 3. 10 PRUEBAS REALIZADAS EN EL ESCENARIO DE TÚNELES ITERADOS

Las pruebas 7 y 8 se realizaron porque el orden más común y que se recomienda en los RFC es precisamente este, en el que primero se provee confidencialidad cifrando la información y luego autenticación mediante la SA externa.

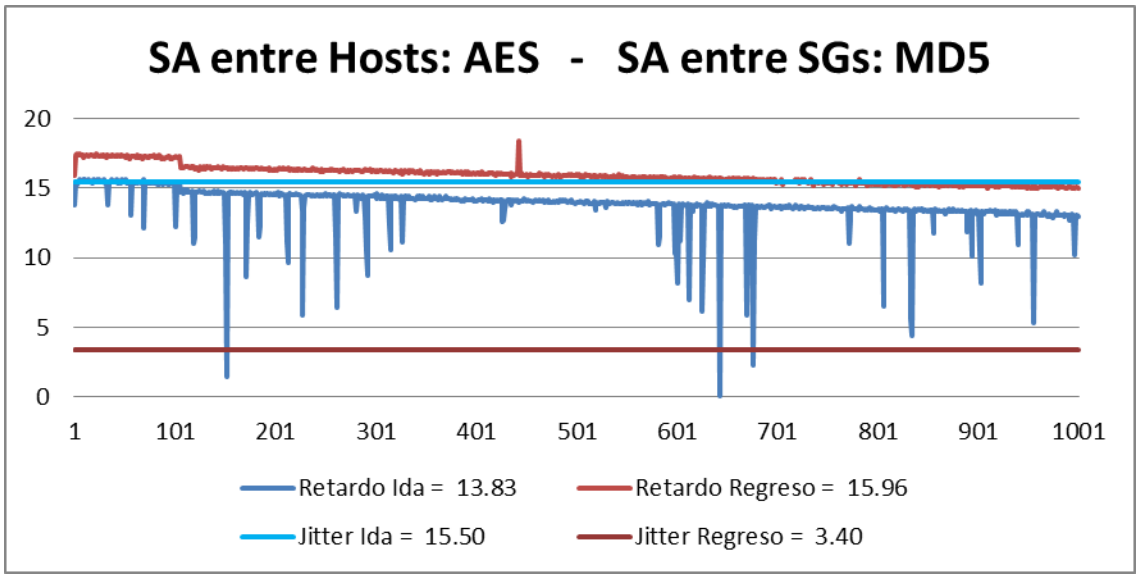


FIGURA 3. 7 RETARDO AL UTILIZAR AES CON MD5 EN SA ITERADAS

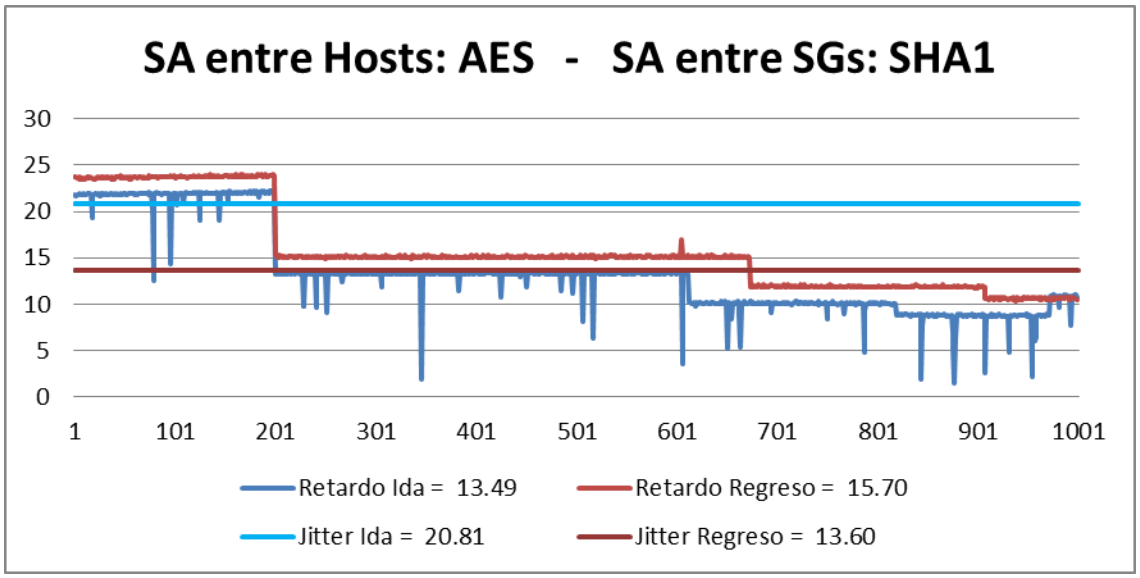


FIGURA 3. 8 RETARDO AL UTILIZAR AES CON SHA1 EN SA ITERADAS

Entre los posibles algoritmos que ofrecen los enrutadores para este caso, que contienen AES y 3DES para cifrado, con MD5 y SHA1 para autenticación; se seleccionó AES para este análisis debido a que previamente se encontró que la degradación en el desempeño de la red que éste ocasiona es menor que la que provocan los otros algoritmos evaluados.

	Hosts: AES SGs: MD5	Hosts: AES SGs: SHA1
Retardo ida(ms)	5.72 – 13.83	6.32 – 13.49
Variación de retardo	15.5 – 16.99	9.59 – 20.81
Retardo regreso	8.11 – 15.96	8.31 – 15.7
Variación de retardo	3.4 – 13.73	5.98 – 13.6

TABLA 3. 11 SAS ITERADAS PARA PROVEER CONFIDENCIALIDAD Y AUTENTICACIÓN

Se observa que el retardo promedio para las combinaciones AES con MD5 y AES con SHA1 es muy similar tanto en la ida como al regreso; asimismo, aunque la variación de retardo presenta un rango de valores mayor en la prueba de ida, el comportamiento en general tiene características análogas.

Por otro lado, se comparan los valores de la tabla 3.11 con las últimas columnas de las tablas 3.6 y 3.7, con los mismos algoritmos respectivamente pero diferente configuración, ya que en la tabla 3.11 se muestran los resultados de proveer confidencialidad por ESP en una SA interna entre los hosts y autenticación con AH mediante una SA externa entre las SG, mientras que la última columna en cada una de las otras tablas (3.6 y 3.7) muestra estos mismos servicios proporcionados mediante una sola SA con ESP; encontrándose que el uso de 2 SA iteradas en esta configuración puede incrementar notablemente el retardo y su variación en la red, y teniendo mayor impacto en la combinación de AES con SHA1.

Las pruebas 1 y 6 fueron desarrolladas con el fin de analizar la incidencia de invertir el orden de las dos asociaciones de seguridad.

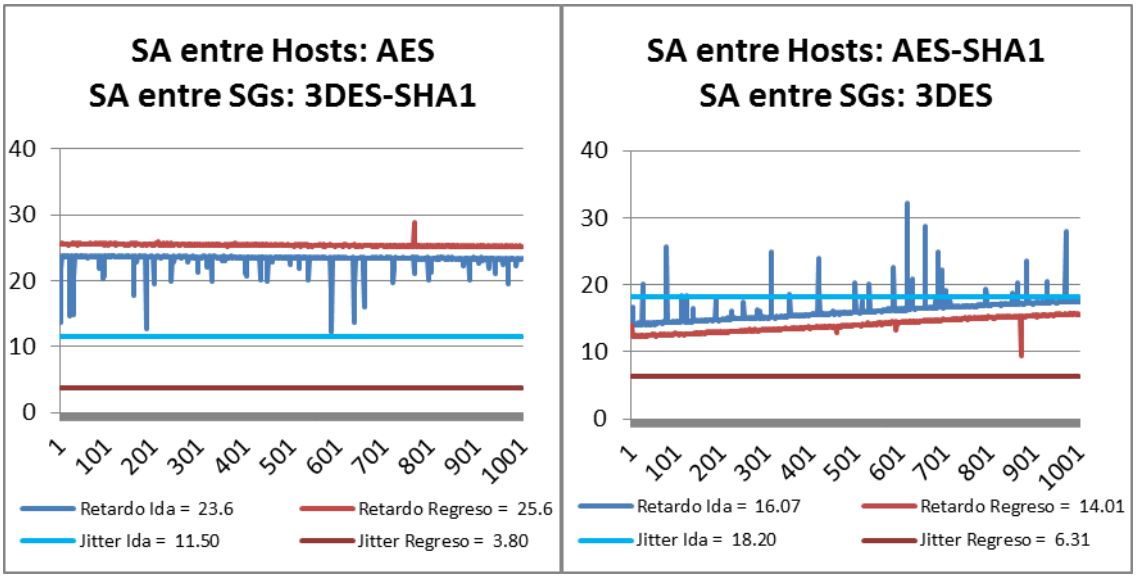
	Hosts: 3DES SGs: AES	Hosts: AES SGs: 3DES
Retardo ida(ms)	5.13 – 5.37	2.48 – 8.63
Variación de retardo	6.66 – 7.51	9.6 – 14.13
Retardo regreso	7.03 – 7.33	1.21 – 10.65
Variación de retardo	2.26 – 5.95	3.31 – 16.77

TABLA 3. 12 IMPACTO DEL INTERCAMBIO DE SAS EN EL RETARDO Y SU VARIACIÓN

Inicialmente, se encontró que si se ve afectado el desempeño de la red debido al intercambio del orden de las SA. Así, en la prueba 1 donde se cifra primero con 3DES y luego con AES el retardo presenta valores más consistentes entre las pruebas (rangos de valores más estrechos), mientras que al cifrar primero con AES y luego con 3DES los valores de retardo pueden ser menores o mucho mayores; algo similar sucede con los valores de variación de retardo.

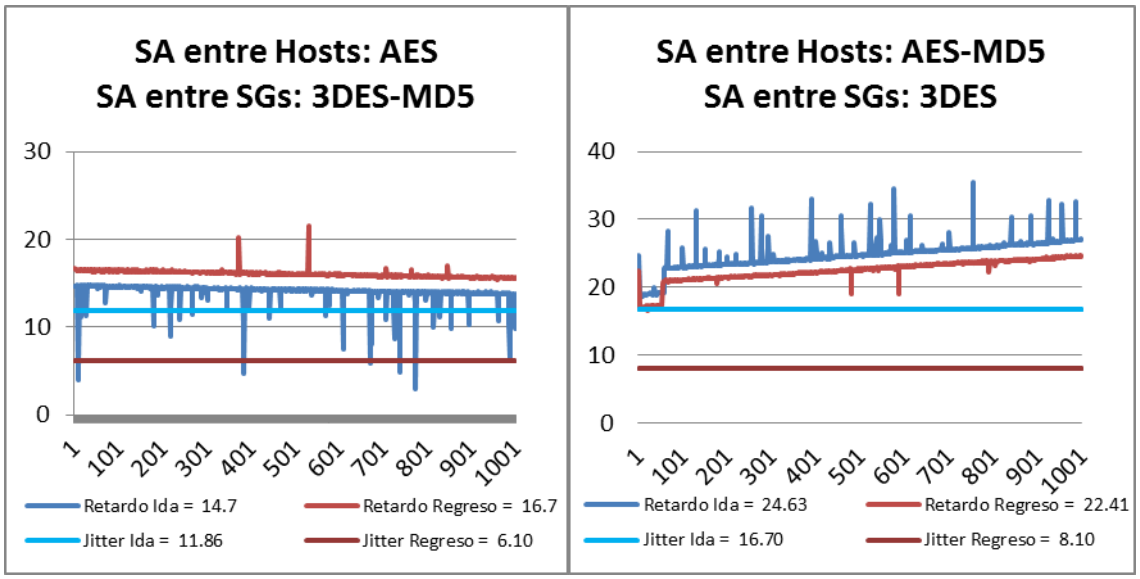
En las pruebas 3 y 4, así como en las 2 y 9 se realizó cifrado en ambas SAs y autenticación en sólo una de ellas. Se conservaron los mismos algoritmos de cifrado y autenticación, y en el mismo orden, pero se varió la SA en la que se realizaba el proceso de autenticacion.

En las pruebas pruebas 3 y 4 se utilizó el algoritmo AES para la SA interna entre los dos hosts y 3DES para la SA externa entre las SG, con SHA1 como único algoritmo de autenticación en la prueba 3 (SA externa) y en la prueba 4 (SA interna); mientras que para las pruebas 2 y 9 el algoritmo de autenticación utilizado fue MD5 tanto en la SA externa (prueba 2) como en la interna (prueba 9).



(A) SA EXTERNA (B) SA INTERNA

FIGURA 3. 9 RETARDO CON AUTENTICACIÓN POR SHA1 EN SAS EXTERNA E INTERNA



(A)SA EXTERNA (B)SA EXTERNA

FIGURA 3. 10 RETARDO CON AUTENTICACIÓN POR MD5 EN SAS EXTERNA E INTERNA

	Hosts: AES SGs: 3DES-SHA1	Hosts: AES-SHA1 SGs: 3DES	Hosts: AES SGs: 3DES-MD5	Hosts: AES-MD5 SGs: 3DES
Retardo ida(ms)	19.24 – 23.39	10.05 – 16.07	10.66 – 14.02	7.23 – 24.63
Variación de retardo	11.5 – 13.81	18.20 – 29.52	11.53 – 11.86	16.7 – 17.33
Retardo regreso	21.27 – 25.40	7.85 – 14.01	12.70 – 16.04	5.52 – 22.41
Variación de retardo	3.8 – 13.99	6.31 – 31.76	5 – 6.1	8.1 – 8.52

TABLA 3. 13 RETARDO AL VARIAR LA SA QUE REALIZA AUTENTICACIÓN CON MD5 Y SHA1

Se observa que al utilizar SHA1 como algoritmo de autenticación los valores de retardo son mayores si se realiza la autenticación en la SA externa (entre las SGs) mientras que los de variación del retardo alcanzan valores mucho más altos cuando estos procesos se dan por parte de la SA interna (entre los hosts).

Por otro lado, si el algoritmo de autenticación predefinido es MD5 los valores de retardo presentan rangos mas estrechos al utilizarlo en la SA externa, además de que son en general menores que los obtenidos al utilizarlo en la SA interna; mientras que si se utiliza en la SA interna se pueden presentar valores mucho mas bajos o mucho más altos. Los

valores de variacion del retardo presentan valores consistentes en ambos casos, pero son mayores al realizar la autenticación en la SA interna.

Finalmente, la prueba 5 proporciona 2 niveles de seguridad completa, teniendo confidencialidad y autenticacion extremo-a-extremo entre los clientes, donde además el proveedor proporciona confidencialidad y autenticación para los datos de sus usuarios entre las SG de frontera.

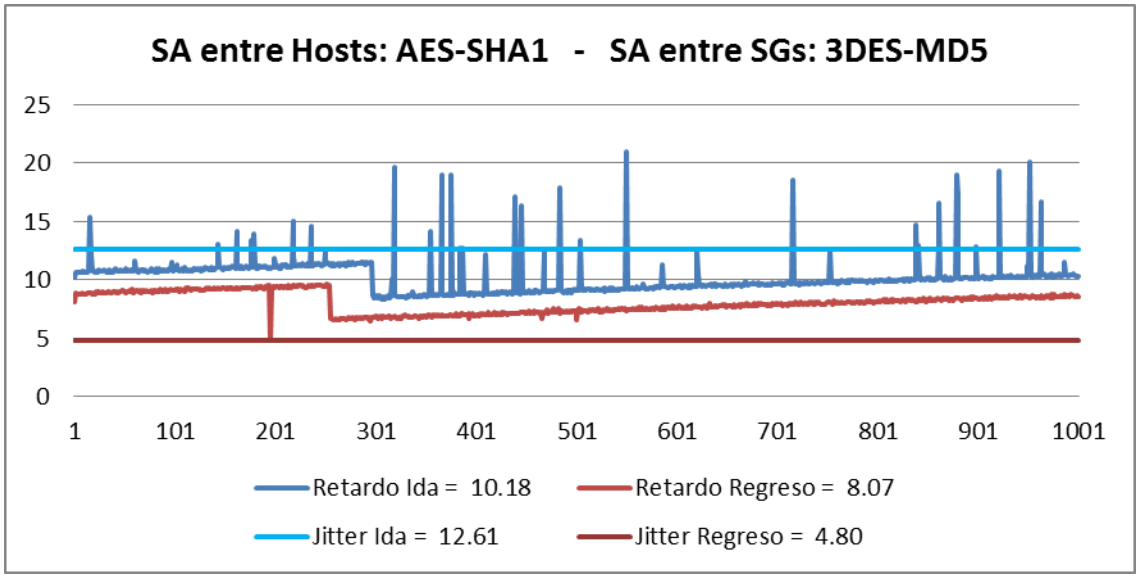


FIGURA 3. 11 RETARDO CON 2 NIVELES DE SEGURIDAD

Al comparar los resultados que se muestran en esta tabla con los de la 3.11, en la que se proporciona un solo nivel de seguridad (AES con MD5 y SHA1), se observa que el impacto de un segundo nivel de seguridad no es mucho mayor que el ocasionado por uno sólo; el retardo en la ida es el que mayor diferencias presenta, pudiendo incrementarse entre 3.86 y 4.46mseg en sus valores mínimos, mientras que los valores máximos se mantienen similares.

	Hosts: AES-SHA1 **SGs: 3DES-MD5**
Retardo ida(ms)	10.18 – 13.4
Variación de retardo	12.61 – 18.48

Retardo regreso	8.07 – 11.45
Variación de retardo	4.8 – 12.18

TABLA 3. 14 RETARDO CON AES+SHA1 ENTRE HOSTS Y ADICIONALMENTE CON 3DES+MD5 ENTRE SGS

2.3 ACCESO REMOTO

En este escenario se establecen un par de SAs entre el Equipo1 y el Enrutador1. Por otro lado se establece otro par de SAs 2 entre el Enrutador1 y el Equipo2 con los mismos parámetros que las SAs establecidas previamente.

Este escenario es conocido como *road warrior* o acceso remoto, en el cual un cliente (Equipo1) se conecta a través de una red insegura a una pasarela de seguridad que puede ser, por ejemplo, la gateway de una red empresarial; y que protege el tráfico hasta llegar al destino (Equipo2) que generalmente es un servidor u otro equipo dentro de la red empresarial.

Así, un par de SAs protegen el tráfico entre el cliente y la frontera de la red privada, mientras que las otras dos protegen el tráfico desde este punto hasta el otro extremo. A diferencia del escenario Host-Host de la primera parte, en los equipos de medición se emplea el *VPNClient* de Cisco que permite realizar la negociación de ambos túneles.

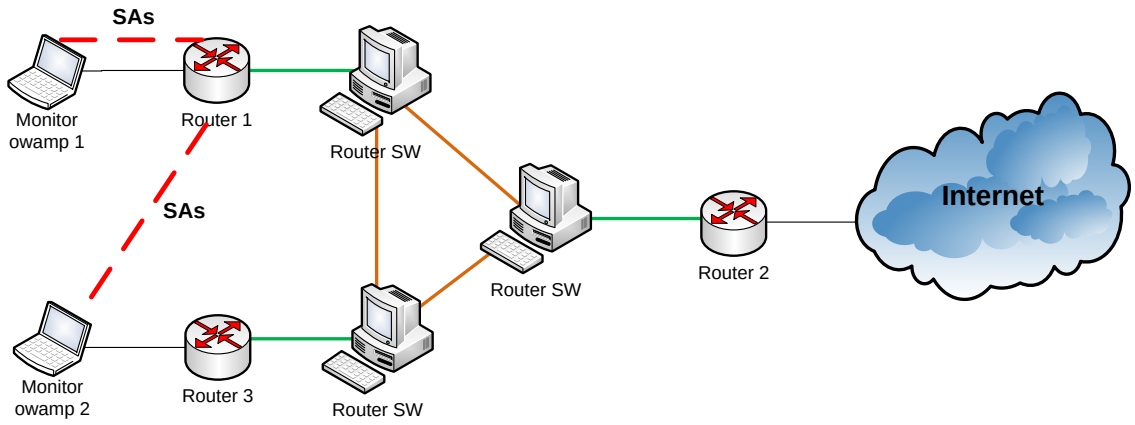


FIGURA 3. 12 ESCENARIO SA ENTRE HOST A SG A HOST

Las pruebas en este escenario se realizaron sobre plataformas GNU/Linux debido a que Owamp funciona mejor sobre dicha plataforma, y como se mencionó en el capítulo 1, sobre Windows los valores de medida obtenidos no son tan exactos.

Este es uno de los escenarios de redes más importantes y comunes en la actualidad, pero debido a limitaciones de las herramientas usadas en GNU/Linux no se pudo crear el túnel dentro de otro túnel en esta plataforma; sin embargo, se configuró el escenario como se muestra en la Figura 3.13 sobre la plataforma Windows.

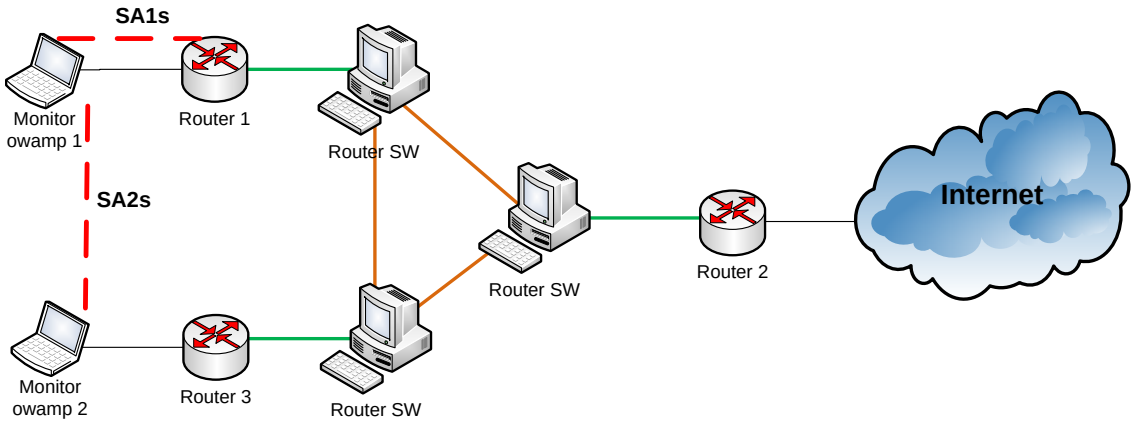


FIGURA 3. 13 ESCENARIO SA ENTRE HOST A SG A HOST EN WINDOWS

En el escenario se continuó con el uso del *VPNClient* de Cisco, y se pasó de OpenSwan a la herramienta de IPsec integrada en el sistema operativo Windows, mientras que la configuración en la SG se mantuvo intacta.

Debido a que se deseaba plantear un escenario más real se trabajaron dos tipos de pruebas, las primeras con Owamp para caracterizar el retardo inherente a la configuración de la red, y las segundas que manejaban un flujo de tráfico de datos por FTP en un sentido y otro de Streaming de video en el sentido contrario.

		Servicio: Protocolo	Algoritmo(s)	Owamp	Datos + Video
	Acceso Remoto Cisco VPN Modo Túnel	Autenticación y Confidencialidad: ESP - Modo Túnel.			
1			MD5-3DES	✓	✓
2			MD5- AES	✓	✓
3			SHA1-3DES	✓	✓
4			SHA1-AES	✓	✓

TABLA 3. 15 PRUEBAS REALIZADAS EN EL ESCENARIO DE TÚNELES ITERADOS

Dado que el uso de DES cada vez es menor, justificado en gran medida por sus vulnerabilidades, para las pruebas en este escenario como en los anteriores se omitió su uso, por lo que el análisis se enfocó en 3DES y AES que son algoritmos más seguros y ampliamente utilizados a nivel mundial.

A continuación se pueden observar los resultados obtenidos por OWAMP en las combinaciones con 3DES.

	ESP: 3DES MD5	ESP: 3DES SHA1
Retardo ida(ms)	0.88 – 0.97	23.5 – 28.3
Variación de retardo	10.2 – 16.7	18.5 – 24.4
Retardo regreso	1.68 – 2.2	21.6 – 26.47
Variación de retardo	3.62 – 7.37	15.2 - 16
Ganador	✓	

TABLA 3. 16 COMPARACIÓN MD5 Y SHA1, UTILIZANDO 3DES PARA CONFIDENCIALIDAD

Claramente se observa que el desempeño al utilizar SHA1 se deteriora mucho en comparación con MD5, y principalmente se ve la degradación en el retardo, donde se pasa de valores que no superan los 2.2 mseg en la combinación 3DES con MD5 a 28.3mseg en 3DES con SHA1; valores tan altos que afectarían notablemente el comportamiento de una aplicación en tiempo real.

Un comportamiento similar se observa en la variación de retardo, y aunque las diferencias no son tan grandes, el desempeño de la combinación 3DES con SHA1 es bajo, con valores de hasta 24.4 mseg que requerirían un tamaño de buffer significativo para las aplicaciones que lo requieran, como por ejemplo, las de tiempo real.

Por otro lado tenemos los resultados de las pruebas de AES.

	ESP: AES MD5	ESP: AES SHA1
Retardo ida(ms)	4.73 – 5.3	4.3 – 8.6
Variación de retardo	11.7 – 14.6	5.73 – 15.95
Retardo regreso	2.7 – 3.4	6.15 – 6.75
Variación de retardo	3.1 – 4.96	4.86 – 9.17
Ganador	✓	

TABLA 3. 17 COMPARACIÓN MD5 Y SHA1, UTILIZANDO AES PARA CONFIDENCIALIDAD

A pesar que los valores sean más cercanos en los resultados de ambas combinaciones, se puede observar claramente que la combinación AES MD5 presenta un mejor comportamiento, tanto en retardo como en la variación de retardo. Además, es de resaltar la estabilidad mostrada en ambas pruebas; es decir los valores de la combinaciones no están tan alejadas entre sí como los registrados en el anterior caso, pero al comparar todas las combinaciones tanto las de 3DES como las de AES, se puede observar que la que menor retardo presentó fue 3DES con MD5 mientras que las menores variaciones de retardo fueron con AES y MD5, además, quien presentó el peor comportamiento fue 3DES con SHA1 dejando ver claramente el gran impacto en el desempeño que ocasiona el uso de SHA1.

En el escenario de Acceso Remoto se transmitieron simultáneamente video y datos; la transferencia de video se estableció desde el equipo 1 hacia el equipo 2, mientras que el flujo de datos FTP viajaba en sentido contrario. Los resultados obtenidos corresponden a las configuraciones en las cuales se utilizó el protocolo ESP para brindar el servicio de confidencialidad y el protocolo AH para la autenticación.

Al analizar los tiempos de transmisión de la información mediante FTP se encuentra que la combinación de ESP con AES y AH con SHA1 es la que más tiempo requiere para la transmisión; aunque esto es sólo una apreciación y no se considera una conclusión debido a que los tiempos de las combinaciones son muy cercanos.

Por otro lado, se observa claramente un incremento de alrededor del doble del tiempo de transferencia para el mismo archivo de datos en las combinaciones frente al no-uso de IPsec, como se aprecia a continuación:

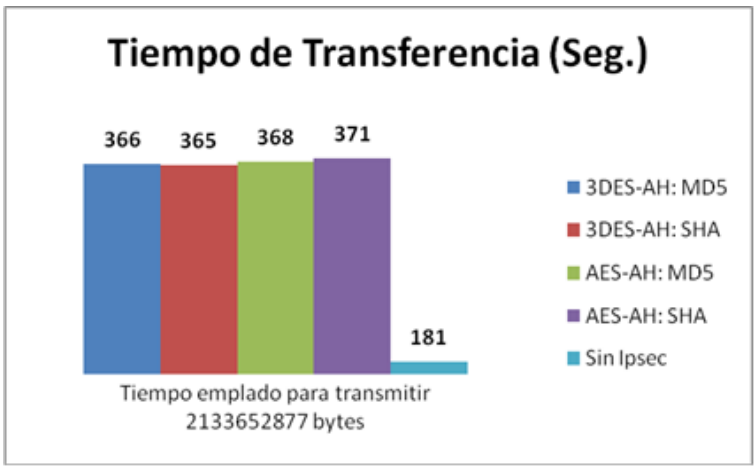


FIGURA 3. 14 TIEMPO DE TRANSFERENCIA DE DATOS CON FTP

En la Tabla 3.18 se encuentra la velocidad de transmisión para las distintas combinaciones evaluadas, de la cual se puede observar claramente que la velocidad disminuye a casi la mitad cuando se hace uso de la arquitectura IPsec para proveer seguridad.

	3DES MD5	3DES SHA1	AES MD5	AES SHA1	Sin IPsec
Velocidad (kB/s)	5689	5703.5	5653.7	5601.6	11476

TABLA 3. 18 VELOCIDAD DE TRANSFERENCIA DE DATOS CON FTP

Por otro lado, en la transferencia de video se obtuvieron datos del número de errores en la transmisión que se presentaban durante cada prueba; éste se incrementa sustancialmente cuando se implementan servicios de seguridad, tanto así que se pasa de tener 10 errores sin IPsec a 256 errores que corresponden a la combinación 3DES con SHA1 y 322 errores al utilizar la combinación AES con MD5, como se muestra a continuación en la figura 3.15.

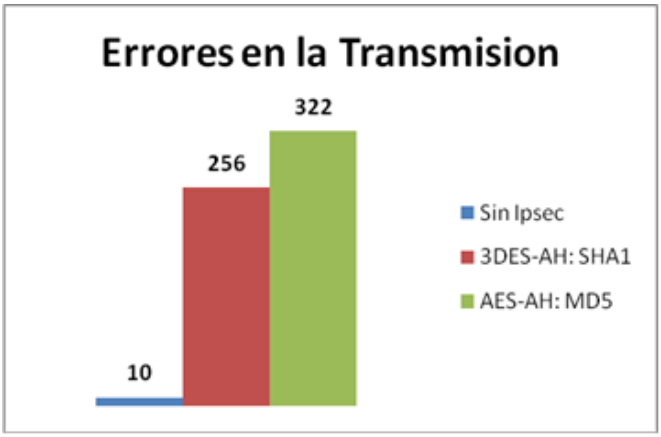


FIGURA 3. 15 ERRORES EN LA TRANSMISION DE VIDEO

4. ANÁLISIS DE LAS COMBINACIONES EN CADA ESCENARIO

Como parte del cumplimiento del tercer objetivo, se analizaron los resultados de las pruebas realizadas con el fin de establecer que configuraciones utilizadas para proveer los servicios de autenticación y confidencialidad tienen mayor y menor impacto en el desempeño de las redes IP.

Las pruebas se realizaron utilizando el protocolo ESP con los algoritmos MD5 y SHA1 para efectuar la autenticación, y 3DES, AES y DES para cifrar y descifrar la información.

4.1 COMBINACIONES 3DES CON MD5

A) PRUEBAS OWAMP: MEJOR COMPORTAMIENTO

De acuerdo a los resultados obtenidos de las pruebas con Owamp, en las cuales se utilizó esta combinación; se encontró que el mejor comportamiento lo presentó en los escenarios de Host-a-Host (sección 5 del anterior capítulo) y de Acceso Remoto (sección 2.3 del presente capítulo).

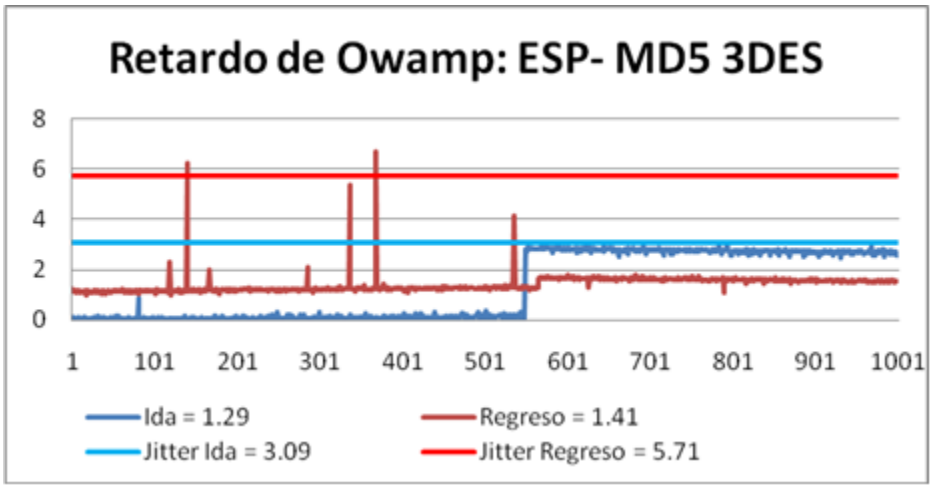


FIGURA 3. 16 RETARDO DE OWAMP PARA ESP CON MD5 Y 3DES EN EL ESCENARIO HOST-HOST

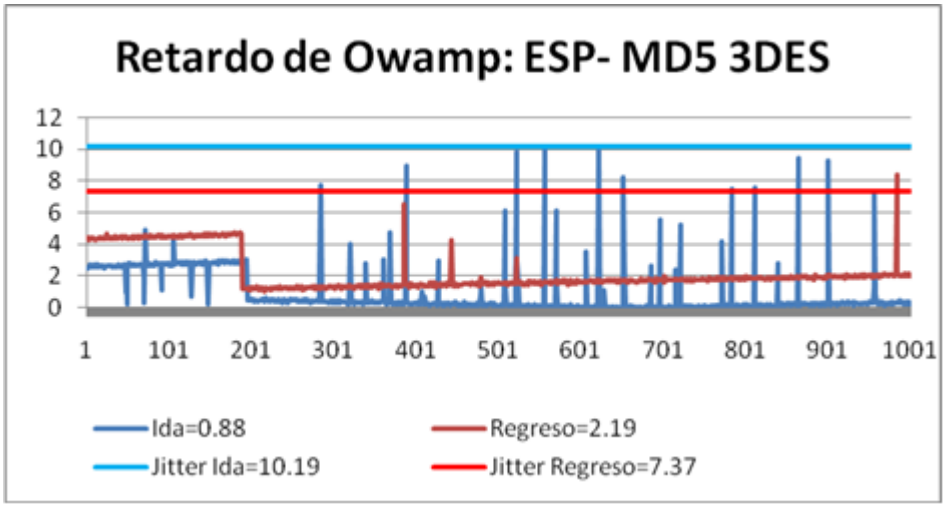


FIGURA 3. 17 RETARDO PARA ESP CON MD5 Y 3DES EN EL ESCENARIO DE ACCESO REMOTO

Por lo anterior se concluye que cuando la mayor parte del proceso se realiza sobre el host los valores de retardo se reducen drásticamente, probablemente debido a que las capacidades de procesamiento del computador superan actualmente los recursos hardware del enrutador físico.

Respecto a la variación de retardo el mejor comportamiento se presenta en el escenario de Host a Host, lo cual viene a corroborar lo anteriormente dicho.

B) PRUEBAS OWAMP: PEOR COMPORTAMIENTO

La combinación presentó un aumento notable en los valores de retardo y variación de retado en el escenario de SG-SG, lo cual ratifica la conclusión de que cuando los procesos de autenticación con MD5 y cifrado con 3DES (utilizando ESP) son realizados por parte de los enrutadores físicos, el desempeño de la red disminuye.

Este comportamiento probablemente es debido a que los procesos de autenticación y cifrado requieren más tiempo en el enrutador que en un computador debido a la diferencia en capacidad de procesamiento, lo cual a su vez aumenta al retardo total presente en el trayecto de red monitoreado.

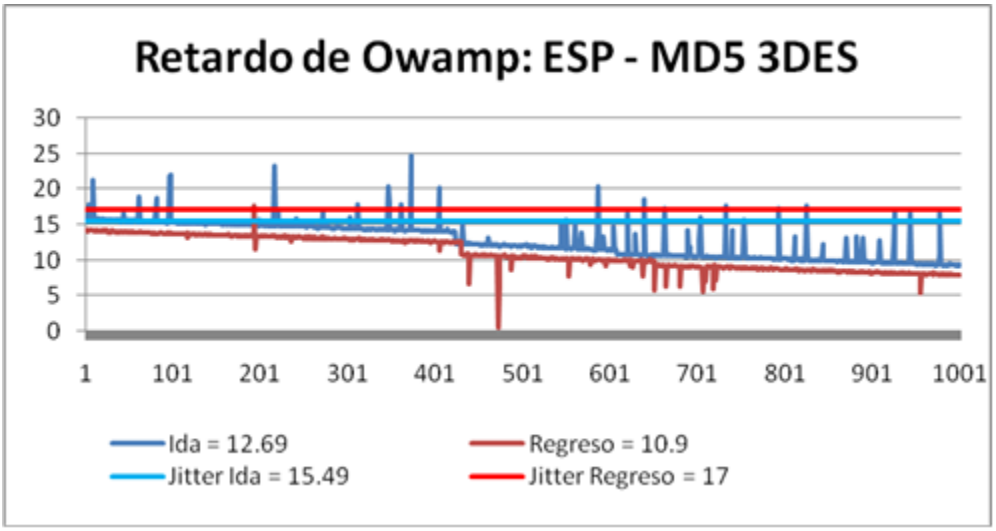


FIGURA 3. 18 RETARDO DE OWAMP DE ESP CON MD5 Y 3DES EN EL ESCENARIO SG-SG

4.2 COMBINACIONES 3DES CON SHA1

4.1 PRUEBAS OWAMP: MEJOR COMPORTAMIENTO

Las diferentes pruebas realizadas muestran que la combinación presentó buen comportamiento en sólo un escenario (Host-Host), a diferencia de MD5 y 3DES que lo tuvo en dos escenarios; esto lleva a pensar que la combinación aquí analizada hace un mayor uso de recursos y tiempo de procesamiento que la anterior, y que se ven reflejados en mayor retardo. Además, se sigue mostrando la eficiencia en los procesos de autenticación y cifrado ejecutados en los computadores.

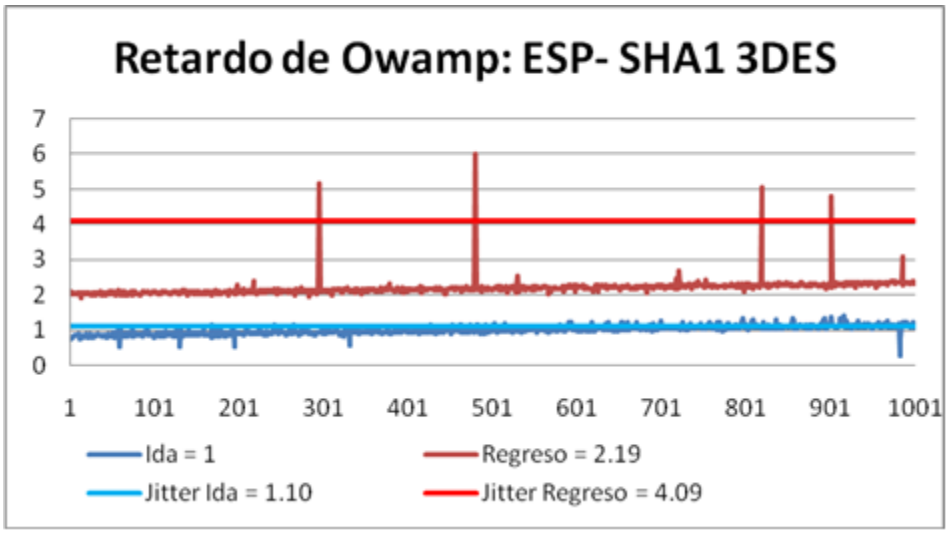


FIGURA 3. 19 RETARDO DE OWAMP PARA ESP CON SHA1 Y 3DES EN EL ESCENARIO HOST-HOST

4.2 PRUEBAS OWAMP: PEOR COMPORTAMIENTO

El peor comportamiento de esta combinación muestra unos valores bastante altos en el escenario de Acceso Remoto, muy superiores a los presentados por la combinación MD5 con 3DES. Por consiguiente se puede concluir que al utilizar SHA1 como algoritmo de autenticación y 3DES como algoritmo de confidencialidad, el retardo se aumenta considerablemente y de forma similar el valor de la variación de retardo, convirtiéndose en los valores más altos obtenidos entre todas las combinaciones analizadas; lo que tendría un impacto considerable en las aplicaciones de tiempo real o *Streaming*.

Además, es importante resaltar que mientras que la combinación MD5 con 3DES en este escenario presento un muy buen comportamiento, la de SHA1 con 3DES fue donde peor se comportó.

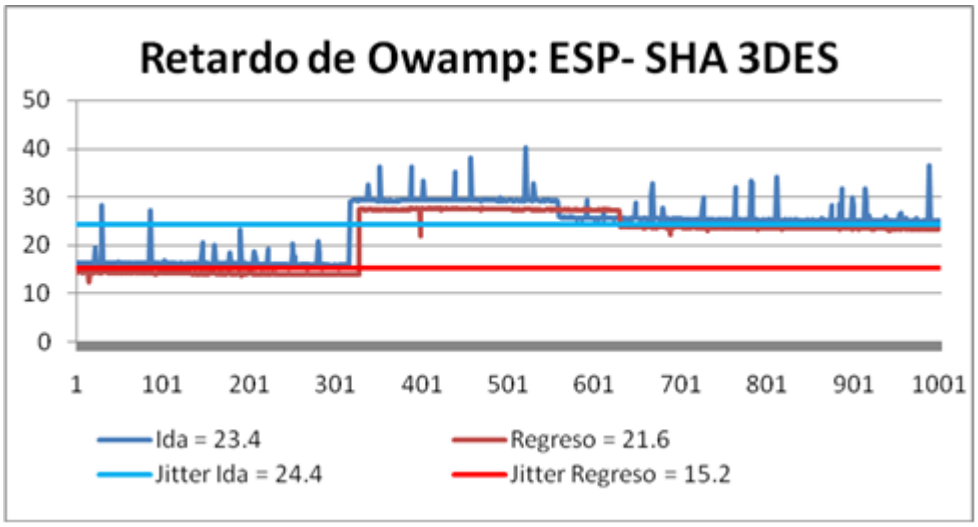


FIGURA 3. 20 RETARDO DE OWAMP PARA ESP CON SHA1 Y 3DES EN EL ESCENARIO DE ACCESO REMOTO

4.3 COMBINACIONES DES CON MD5 Y SHA1

Las pruebas de estas combinaciones que incluyen a DES solo se realizaron en el escenario SG-SG, debido al poco uso que se le está dando actualmente a este algoritmo dados sus problemas de seguridad.

Los datos obtenidos muestran que la combinación que presenta mayor retardo es SHA1 con DES, y aunque las diferencias no sean considerables, probablemente en aplicaciones exigentes que dependan en gran medida de este parámetro podrían ser notables estas pequeñas diferencias. Adicionalmente, se observa que aunque el comportamiento presentado se puede considerar bueno, los valores son mayores que los generados por las combinaciones anteriores.

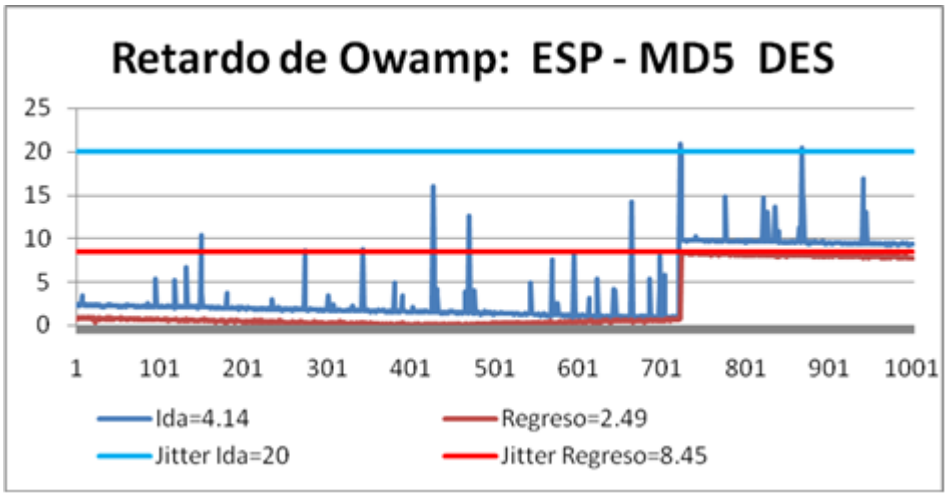


FIGURA 3. 21 RETARDO MEDIDO POR OWAMP PARA ESP CON MD5 Y DES EN EL ESCENARIO SG-SG

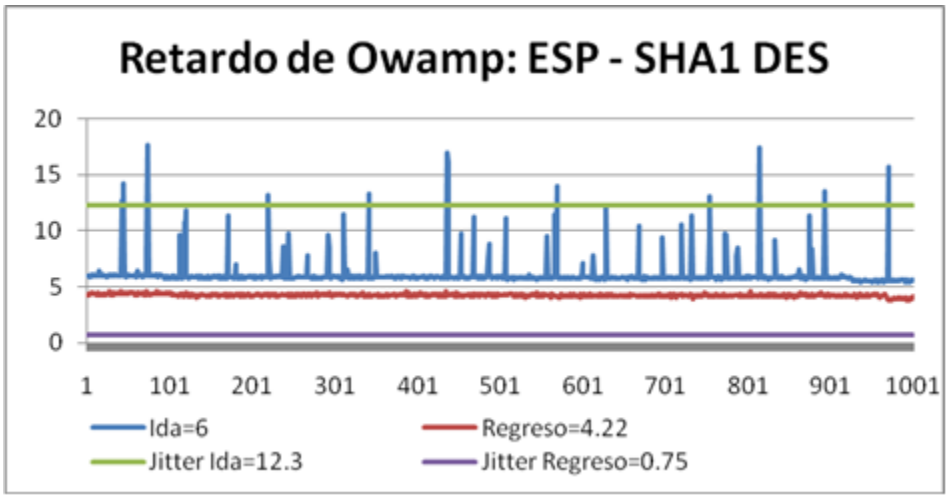


FIGURA 3. 22 RETARDO MEDIDO POR OWAMP PARA ESP CON SHA1 Y DES EN EL ESCENARIO SG-SG

Las diferencias en la variación de retardo de MD5 con DES son importantes respecto a los valores presentados por la combinación de SHA1 y DES, aunque el número de puntos de inflexión sea menor. Es de resaltar que la variación de retardo de la combinación MD5 con DES es el tercer valor más alto que se presentó entre en todas las combinaciones analizadas.

Respecto al uso de CPU, las diferencias son de máximo 0.01% por lo que se puede decir que el uso de CPU es el mismo; tal como se puede apreciar en la figura 3.23.

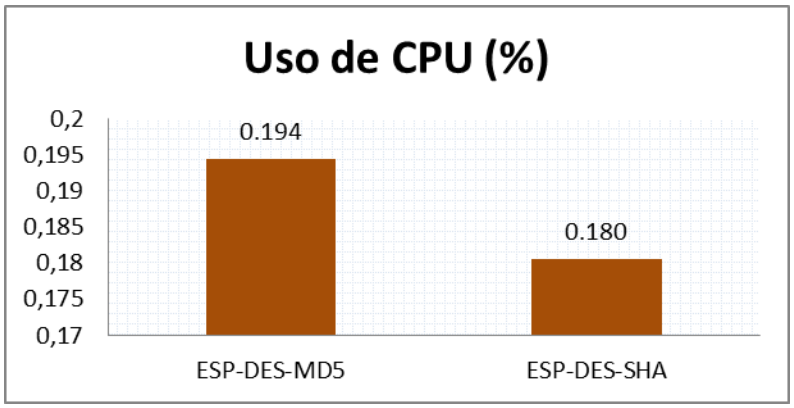


FIGURA 3. 23 USO DE CPU ENTRE MD5 CON DES Y SHA1 CON DES

4.4 COMBINACIONES AES CON MD5

A) PRUEBAS OWAMP: MEJOR COMPORTAMIENTO

Los resultados de retardo obtenidos por Owamp indican que donde mejor se comportó fue en el escenario de Host-Host, en el cual presentó valores muy bajos, con grandes diferencias respecto a los demás escenarios donde fue configurado y medido.

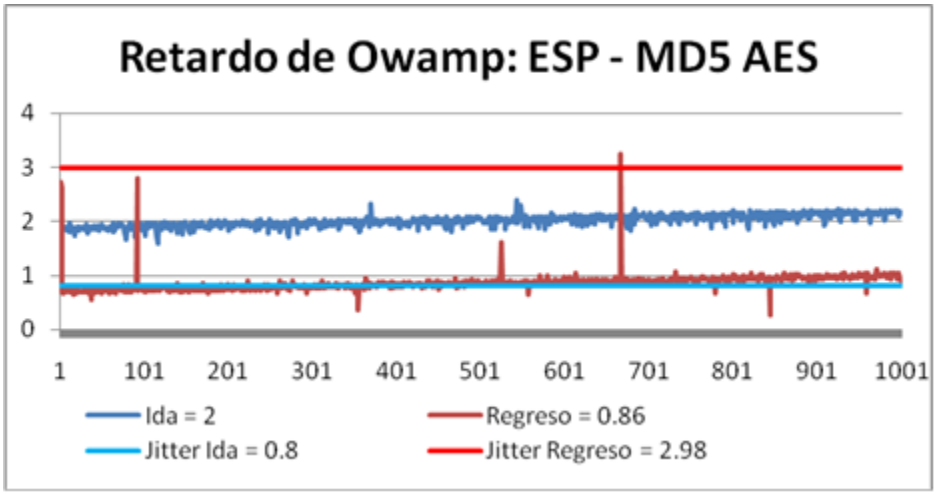


FIGURA 3. 24 RETARDO DE OWAMP CON MD5 Y AES EN EL ESCENARIO HOST-HOST

Por otro lado se encontró que en la variación de retardo también fue en este escenario donde presentó menores valores.

B) PRUEBAS OWAMP: PEOR COMPORTAMIENTO

Como era de esperarse, cuando los procesos de autenticación y cifrado no son realizados en los computadores, los valores de retardo y variación de retardo se incrementan. Así, dónde peor se comportó fue en el escenario de SG-SG.

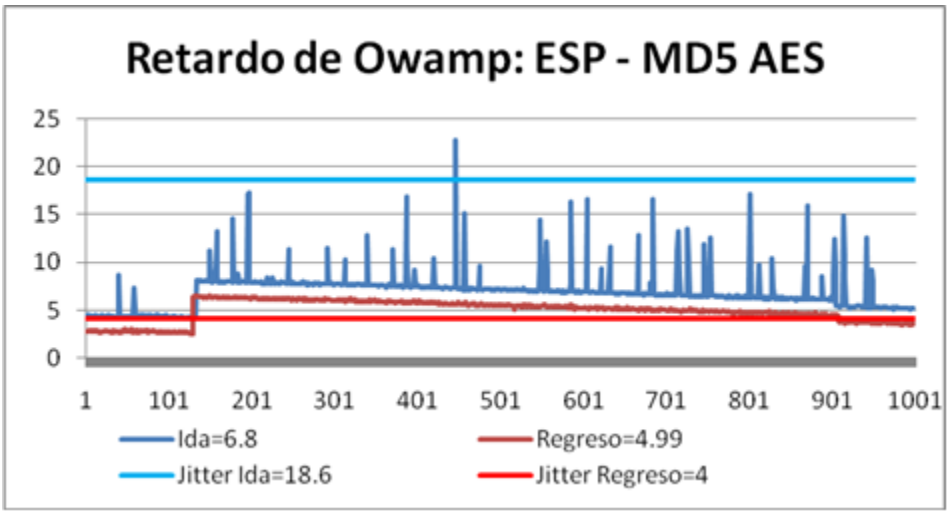


FIGURA 3. 25 RETARDO DE OWAMP CON MD5 Y AES EN EL ESCENARIO SG-SG

Igualmente, en este escenario es donde se presenta el mayor valor de la variación de retardo. También cabe resaltar que el escenario de Acceso Remoto fue el segundo escenario donde se presentó un desempeño bajo, tanto en retardo como en variación de retardo.

4.5 COMBINACIONES AES CON SHA1

A) PRUEBAS OWAMP: MEJOR COMPORTAMIENTO

Entre los diferentes escenarios en que la combinación fue probada se comportó de mejor forma respecto al retardo en el escenario Host a Host.

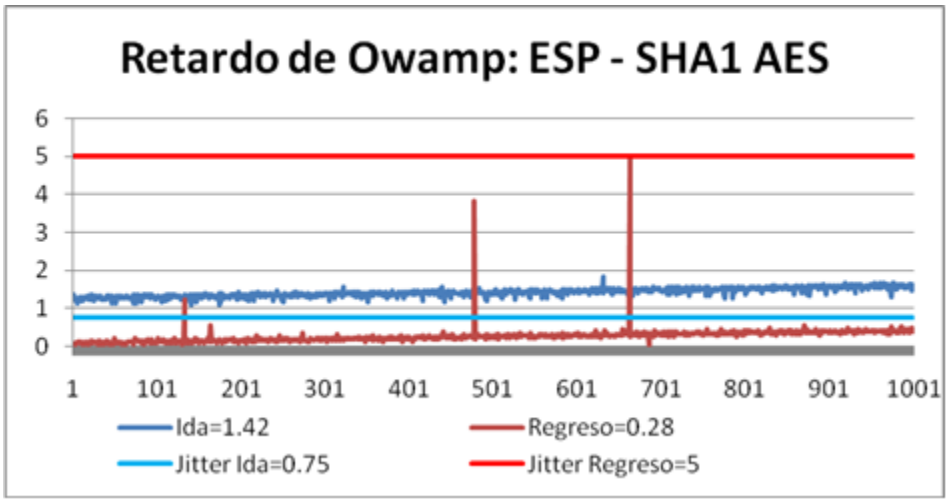


FIGURA 3. 26 RETARDO DE OWAMP CON SHA1 Y AES EN EL ESCENARIO HOST-HOST

La variación de retardo tuvo el mejor comportamiento en este escenario, lo cual comprueba la eficiencia de desarrollar los procesos de autenticación y cifrado en los computadores.

Lo anterior es muy interesante, dado que ratifica la conclusión que cuando los procesos de autenticación y cifrado del protocolo ESP son realizados por parte de los enrutadores físicos, el valor de retardo y variación de retardo aumenta. Este comportamiento muy probablemente es debido a que los procesos de autentificación y cifrado hacen que el enrutador, debido a su limitación en recursos hardware, le tome más tiempo que el que le toma a un computador, lo cual a su vez aumente al retardo total en el trayecto medido de la red.

B) PRUEBAS OWAMP: PEOR COMPORTAMIENTO

Aunque por lo anteriormente dicho se esperaría que el escenario donde peor se comporta fuera el escenario SG-SG, en este caso fue el de Acceso Remoto.

Analizando estos datos se observa que aunque parezca una contradicción a lo concluido, si se revisa con cuidado la información presentada se observa que entre los escenarios donde peor se comportaron las diferentes combinaciones el escenario de Acceso Remoto aparece en más de dos ocasiones; esto es debido a que en este escenario aparece una SG, por la cual está pasando todo el tráfico y que es la encargada de descifrar la información (o verificar una autenticación) que le llega por una SA para luego cifrarla (o realizar nuevos cálculos de integridad y autenticación) y enviarla por la otra SA.

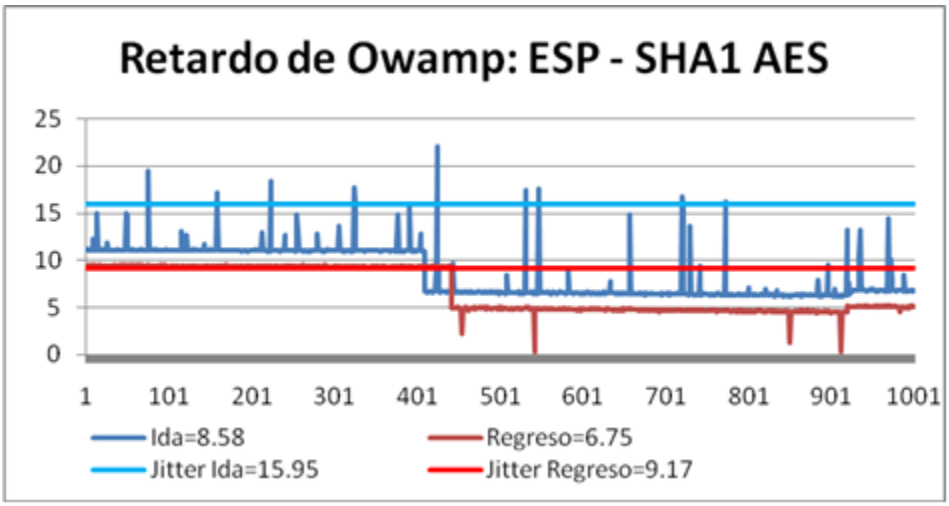


FIGURA 3. 27 RETARDO DE OWAMP CON SHA1 Y AES EN EL ESCENARIO DE ACCESO REMOTO

Además, el escenario Host a SG, fue el segundo escenario donde peor se comporta seguido de cerca por el escenario SG-SG, ratificando lo anteriormente dicho.

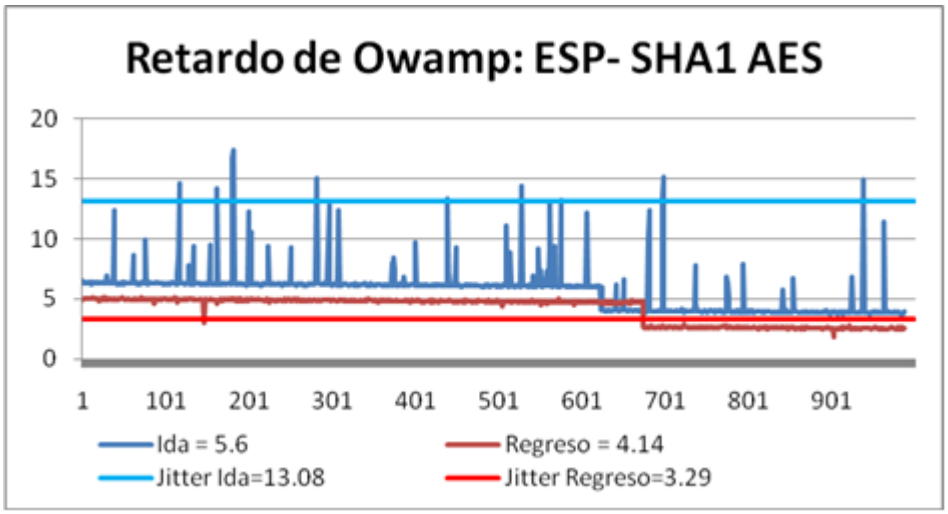


FIGURA 3. 28 RETARDO DE OWAMP CON SHA1 Y AES EN EL ESCENARIO HOST-SG

La variación de retardo como se aprecia en las figuras 3.27 y 3.28 es muy alto, tanto así que la combinación SHA1 con AES presenta el segundo valor más alto entre todas las pruebas de las combinaciones analizadas.

CAPITULO IV

CONCLUSIONES Y RECOMENDACIONES

1. IPSEC Y SUS PROTOCOLOS

Con el adelanto que han tenido en los últimos años las tecnologías de la información y las comunicaciones, las personas y empresas han empezado a darle más valor a su información; lo cual ha llevado a una creciente necesidad de proveer servicios de seguridad para la misma, generando niveles de seguridad que van desde los equipos en los que se almacena y procesa la información, las redes por las que se transmite y el personal que tiene acceso a ella.

Sin embargo, el incrementar los niveles de seguridad repercute de forma negativa en otros aspectos y el implementar IPsec no es la excepción. Así, en base a los resultados de las pruebas al implementar servicios de seguridad propiciados por esta arquitectura en el presente trabajo, se puede concluir que según el tipo de tráfico cursado la degradación en el rendimiento de la red puede llegar hasta un 50% en la velocidad y un uso de la CPU mayor al 90%. Estos valores se consideran trascendentales dado que si se tiene un enlace de 100Mbps se estarían perdiendo 50Mbps de capacidad debido al despliegue de los servicios de seguridad.

1.1 AUTHENTICATION HEADER - AH

El primero objetivo de este trabajo era conocer acerca del comportamiento de IPsec con sus protocolos independientemente, así, para el protocolo de autenticación e integridad AH se concluye que el algoritmo de autenticación que mejor se comportó (generó menor degradación del desempeño) fue en términos generales SHA1; dado que las velocidades entre SHA1 y MD5 difieren por 5bits/seg, pudiéndose considerar que proporcionan una velocidad igual e igual consumo de CPU. Por otro lado, se encontró que el retardo generado por MD5 es menor pero su variación de retardo es mayor que la de SHA1.

Parámetros	MD5	SHA1
Retardo		
Jitter		
Seguridad		

TABLA 4. 1 COMPARACIÓN ENTRE LOS ALGORITMOS MD5 Y SHA1

1.2 ENCAPSULATING SECURITY PAYLOAD

1.2.1. ESP: CONFIDENCIALIDAD

El comportamiento de la red con los diferentes algoritmos utilizados es similar, tanto respecto a la velocidad generada como al uso de CPU, siendo la máxima diferencia de apenas 1%. Respecto al retardo y variación del mismo se puede observar que DES ocasiona un bajo impacto en el desempeño; algo que ya se esperaba debido a que su nivel de seguridad es bajo, lo cual representa un menor número de procesos y de complejidad si se compara con AES o 3DES.

Parámetros	3DES	AES	DES
Retardo			
Jitter			
Seguridad			

TABLA 4. 2 COMPARACIÓN ENTRE LOS ALGORITMOS 3DES, AES Y DES

1.2.2. ESP: AUTENTICACIÓN + CONFIDENCIALIDAD

Por otro lado era importante analizar el comportamiento de la red al implementar los servicios de autenticación y confidencialidad con ESP; al hacerlo se observó que la combinación que menor degradación del desempeño ocasionó fue MD5 con AES en el escenario Host-a-SG.

Parámetros	MD5 3DES	MD5 AES	SHA1 3DES	SHA1 AES
Retardo				
Jitter				
Seguridad				

TABLA 4. 3 ESCENARIO HOST A SG

Mientras tanto, en el escenario de SG a SG hubo dos combinaciones que presentaron un buen comportamiento, MD5 con AES y SHA1 con AES; lo cual corrobora la alta eficiencia del algoritmo de cifrado AES.

Parámetros	MD5 3DES	MD5 AES	MD5 DES	SHA1 3DES	SHA1 AES	SHA1 DES
Retardo						
Jitter						
Seguridad						

TABLA 4. 4 ESCENARIO SG – SG

En el escenario de Acceso Remoto la combinación que menor detrimento en el desempeño ocasionó fue MD5 con 3DES, aunque seguida muy de cerca por la combinación de MD5 con AES.

Parámetros	MD5 3DES	MD5 AES	SHA1 3DES	SHA1 AES
Retardo				
Jitter				
Seguridad				

TABLA 4. 5 ESCENARIO ACCESO REMOTO

De los anteriores resultados se concluye que la combinación que mejor desempeño tuvo tanto en retardo como en la variación de retardo fue la de MD5 con AES.

1.3 AH+ESP: AUTENTICACIÓN CON AH Y CONFIDENCIALIDAD CON ESP

En muy interesante ver que cuando el protocolo que realiza la autenticación no es ESP sino AH, la combinación que mejor se comporta es SHA1 con 3DES, corroborando la conclusión presentada en la sección 1.1 de este capítulo de que cuando se autentica con AH es mejor utilizar SHA1. Por otra parte se observa que cuando se utiliza la combinación de MD5 con DES es mejor utilizar la autenticación con AH, mientras que si se utiliza SHA1 con DES es mejor utilizar todo con ESP.

Además el comportamiento del algoritmo AES se ve afectado al utilizar la autenticación por AH, pasando de ser el mejor a casi el peor, pero se observó que la combinación con la que presenta el mejor comportamiento es SHA1 con AES. Así, al analizar todos los resultados obtenidos se concluye que al utilizar la autenticación por AH la mejor opción entre las evaluadas es SHA1.

Parámetros	MD5 3DES	MD5 AES	MD5 DES	SHA1 3DES	SHA1 AES	SHA1 DES
Retardo						
Jitter						
Seguridad						

TABLA 4. 6 ESCENARIO SG – SG

2. COMPORTAMIENTO DE ESCENARIOS

2.1 MEJOR ESCENARIO: HOST-HOST

De todos los resultados obtenidos en los diferentes escenarios se observó que éste fue en el cual se presentaron menores retardos y variaciones de retardo al implementar servicios de seguridad, como también un menor uso de CPU. El despliegue de los diferentes servicios no afectó de manera notoria el desempeño de la Red IP, como se puede apreciar en la sección 5 del capítulo 2.

2.2 PEOR ESCENARIO: HOST A HOST CON SG – SG.

Aunque en varios de los escenarios se presentaron valores altos de retardo y/o variación de retardo, el escenario que en promedio mantiene valores muy altos para casi todas las pruebas, sino todas, fue el de Asociaciones de Seguridad Iteradas, en el cual se creaba un túnel entre los hosts que luego iba dentro de otro túnel entre las SGs.

2.3 MÁS ESTABLE: SG- SG.

Por otro lado es importante resaltar que además de valorar el escenario que menor impacto sufre con servicios de seguridad, un factor clave es la estabilidad; por lo cual se realizó un análisis de este aspecto evaluando cuando se presentaba una menor variación en sus resultados y se encontró que el escenario más estable fue el de SG-SG.

2.4 OTROS ESCENARIOS

A continuación se presenta un análisis de los escenarios restantes, excluyendo a Host-Host que tuvo el menor impacto en su desempeño y el de SAs Iteradas que tuvo el mayor, con el fin de poder apreciar también el comportamiento de los demás escenarios en cuanto a retardo y variación de retardo, que se resumen en las tablas 4.7 y 4.8.

Retardo	SG – SG AH o ESP	SG – SG AH+ESP	Host-SG	Acceso Remoto
MD5 3DES				
MD5 AES				
MD5 DES				
SHA1 3DES				
SHA1 AES				
SHA1 DES				

TABLA 4. 7 COMPARACIÓN DE RETARDO ENTRE ESCENARIOS

Variación de Retardo	SG – SG AH o ESP	SG – SG AH+ESP	Host-SG	Acceso Remoto
MD5 3DES				
MD5 AES				
MD5 DES				
SHA1 3DES				
SHA1 AES				
SHA1 DES				

TABLA 4. 8 COMPARACIÓN DE VARIACIÓN DE RETARDO ENTRE ESCENARIOS

En las tablas 4.7 y 4.8 se observa que las combinaciones que en general menor retardo generan son MD5 con AES y SHA1 con AES, y la que presenta menor variación de retardo en general es SHA1 con AES. Por esta y las anteriores apreciaciones, se concluye que el mejor desempeño de los algoritmos para confidencialidad fue el mostrado por AES, y de las combinaciones utilizadas para proveer autenticación con confidencialidad quienes presentaron el mejor comportamiento fueron MD5 con AES y SHA1 con AES.

2.5 SA'S ITERADAS

No solamente los proveedores, en la actualidad también los usuarios son conscientes del valor de su información y buscan protegerla mediante SA's extremo a extremo; adicionalmente, dado que pertenecen a una intranet que puede ser una red empresarial o un ISP, es muy probable que esta Red IP también ofrezca algún nivel de seguridad, así, se analizó también el comportamiento en un escenario Host a Host con SAs de SG a SG.

Una de las principales observaciones es tener siempre en cuenta que el orden en el que se establezcan las SAs si afecta el desempeño de las redes IP que implementen servicios de seguridad propiciados por IPsec (pag. 74); es decir, si se establece un primer par de SAs con AES y luego otro par de SAs con 3DES, al invertir este orden no se va a percibir el mismo desempeño, pudiendo mejorar o empeorar.

Retardo	Host - Host	SG – SG	Variación de Retardo	Host - Host	SG – SG
Mejor	3DES	AES	Mejor	3DES	AES
Peor	AES	SHA1 3DES	Peor	AES SHA1	3DES
	AES MD5	3DES		AES	SHA

TABLA 4. 9 COMPARACIONES DEL ESCENARIO ACCESO REMOTO

Las SAs entre los Hosts con AES y entre las SGs con 3DES, e incluso en el orden inverso mostraron el mejor comportamiento, pero al agregar autenticación ya sea entre los Hosts o entre las SGs, el desempeño se degrada notablemente; esto permite concluir que la prestación del servicio de autenticación genera procesos extra que terminan por incrementar notablemente tanto el retardo como la variación del mismo en las redes.

Además, al implementar dos niveles de seguridad (ya sea agregando autenticación o autenticación+confidencialidad) se observa como el desempeño de la red se ve degradado notablemente, tanto así, que en este escenario se presentaron valores más altos de retardo y variación de retardo y por tal motivo fue catalogado como el peor de ellos. Este escenario permitió apreciar de forma más significativa el costo que se paga al mejorar el nivel de seguridad para la información que se transmite a través de una Red IP.

3. RECOMENDACIONES Y APORTES DEL TRABAJO

Con respecto a las implementaciones IPsec utilizadas, fue vital contar con los enrutadores Cisco 2801 del Departamento de Telecomunicaciones, ya que como mostraron los resultados, fueron las que permitieron obtener los valores más estables entre una prueba y la otra proporcionando mayor confiabilidad a los datos obtenidos; por esto, en caso de requerirse mediciones de desempeño de IPsec se sugiere utilizar implementaciones como éstas.

Además, se resalta la implementación de IPsec incluida en el sistema operativo Windows XP ya que permitió desplegar uno de los escenarios más importantes y ampliamente utilizados en la actualidad, de acuerdo a las referencias estudiadas y con mucha mayor facilidad para un usuario estándar. Por esto, se sugiere no descartar de antemano la posibilidad de desarrollar pruebas adicionales con otras implementaciones u otros sistemas operativos ya que la realización de las mismas puede aportar información valiosa para el trabajo; en su lugar, se recomienda proponer y ejecutar algunas de ellas de acuerdo a las limitaciones que vayan presentando las herramientas seleccionadas durante el desarrollo del proyecto.

Las herramientas de medición de desempeño fueron un factor importante en la primera etapa del proyecto, ya que previamente a la fase de pruebas era necesario saber qué tipo de información se requería obtener, como debía ser obtenida según estándares y trabajos previos, y que herramientas podían entregarla de dicha forma; por lo cual se exploraron las herramientas mencionadas en el capítulo 1 y otras adicionales.

Algunas de ellas se utilizaron como ayudas para entender a un nivel más profundo el funcionamiento de las redes con seguridad y corroborar la información entregada por Owamp; sin embargo, Owamp demostró ser una herramienta que provee la flexibilidad y estabilidad para obtener la cantidad y calidad de datos que requiere una medición de desempeño confiable en los entornos planteados.

Asimismo, se encontró que el tráfico de datos por FTP fue el más exigente para la red, por lo cual en las pruebas realizadas con este tipo de tráfico se pudieron obtener valores de velocidades y tiempos de transferencia que reflejan el desempeño de las redes en casos de alto tráfico o *worst-case-scenarios*.

4. TRABAJOS FUTUROS

Como continuación y complemento al trabajo realizado, se exponen los siguientes trabajos que podrían aportar mayor información para el conocimiento de IPsec y su impacto en el desempeño de las redes IP:

- Estudio de Vulnerabilidades vs. Desempeño en IPsec.
- Análisis del desempeño de IPsec en ambientes inalámbricos (802.11, NFC, etc.).
- Evaluación de desempeño de otros protocolos de seguridad como L2TP, etc.

Adicionalmente al protocolo de medición One-way Active Measurement Protocol que proporciona la guía para mediciones en un sentido, y en el cual se basó la implementación de la herramienta Owamp; existe un protocolo llamado Two-way Active Measurement Protocol que es un protocolo abierto para la medición de métricas en ambos sentidos. Está basado en el RFC de OWAMP [28] y se adhiere a su arquitectura y diseño, pero sus implementaciones aún se encuentran en desarrollo, por lo que se recomienda explorarla en trabajos futuros relacionados con el área.

BIBLIOGRAFÍA

[1] IETF, RFC2411, IP Security Document Roadmap, [En línea] http://www.ietf.org/rfc/rfc2411

[2] IETF, RFC4301, Security Architecture for the Internet Protocol, [En línea] http://www.ietf.org/rfc/rfc4301

[3] IETF, RFC2828, Internet Security Glossary, [En línea] http://www.ietf.org/rfc/rfc2828

[4] IETF, RFC2402, IP Authentication Header, [En línea] http://www.ietf.org/rfc/rfc2402

[5] IETF, RFC4302, IP Authentication Header, [En línea] http://www.ietf.org/rfc/rfc4302

[6] IETF, RFC2406, IP Encapsulating Security Payload (ESP), [En línea] http://www.ietf.org/rfc/rfc2406

[7] IETF, RFC4303, IP Encapsulating Security Payload (ESP), [En línea] http://www.ietf.org/rfc/rfc4303

[8] IETF, RFC2408, Internet Security Association and Key Management Protocol (ISAKMP), [En línea] http://www.ietf.org/rfc/rfc2408

[9] IETF, RFC2409, The Internet Key Exchange (IKE), [En línea] http://www.ietf.org/rfc/rfc2409

[10] IETF, RFC2401, Security Architecture for the Internet Protocol, [En línea] http://www.ietf.org/rfc/rfc2401

[11] IETF, RFC2407, The Internet IP Security Domain of Interpretation for ISAKMP, [En línea] http://www.ietf.org/rfc/rfc2407

[12] IETF, RFC4306, Internet Key Exchange (IKEv2) Protocol, [En línea] http://www.ietf.org/rfc/rfc4306

[13] Cisco Press, IPSec VPN Design, 2005.

[14] IPSec - The New Security Standard For The Internet, Intranets, And Virtual Private Networks Prentice Hall, 2nd Ed.2003

[15] Cisco Press, Implementing Cisco IOS Network Security (IINS) (Self-Study), 2009.

[16] Cisco Press, Understanding Cryptography - A Textbook for Students and Practitioners, 2009.

[17] ITU-T, Rec I.350, Aspectos Generales De Calidad De Servicio Y De Calidad De Funcionamiento En Las Redes Digitales Incluidas Las Redes Digitales De Servicios Integrados, [En línea] http://www.itu.int/rec/T-REC-I.350-199303-I/en

[18] ITU-T, Rec Y.1543, Measurements in IP networks for inter-domain performance assessment, [En línea] http://www.itu.int/rec/T-REC-Y.1543/en

[19] IETF, RFC2330, Framework for IP Performance Metrics, [En línea] http://www.ietf.org/rfc/rfc2330

[20] ITU-T, Rec X.140, Parámetros Generales De Calidad De Servicio Para Comunicación A Través De Redes Públicas De Datos, [En línea] http://www.itu.int/rec/T-REC-X.140/en

[21] ITU-T, Rec Y.1540, Internet protocol data communication service – IP packet transfer and availability performance parameters, [En línea] http://www.itu.int/rec/T-REC-Y.1540/en

[22] IETF, RFC2679, A One-way Delay Metric for IPPM, [En línea] http://www.ietf.org/rfc/rfc2679

[23] IETF, RFC2680, A One-way Packet Loss Metric for IPPM, [En línea] http://www.ietf.org/rfc/rfc2680

[24] IETF, RFC2678, IPPM Metrics for Measuring Connectivity, [En línea] http://www.ietf.org/rfc/rfc2678

[25] Metodología de la investigación: desarrollo de la inteligencia, Cengage Learning Editores, 2006, pag. 97.

[26] ITU-T, Rec Y.1541, Objetivos de calidad de funcionamiento de red para servicios basados en el protocolo Internet, [En línea] http://www.itu.int/rec/T-REC-Y.1541/en

[27] Accuracy Evaluation of Ping and J-OWAMP, Luleå, 2006, Swedish National Computer Networking Workshop, pags 57-60.

[28] IETF, RFC4656, A One-way Active Measurement Protocol (OWAMP), [En línea] http://www.ietf.org/rfc/rfc4656

[29] IETF, RFC3393, IP Packet Delay Variation Metric for IP Performance Metrics (IPPM), [En línea] http://www.ietf.org/rfc/rfc3393.txt

[30] IETF, RFC 3713, A Description of the Camellia Encryption Algorithm, [En línea] http://www.ietf.org/rfc/rfc3713.txt