MIDDLEWARE DE SEGURIDAD PARA EL ACCESO A SERVICIOS IMS EN UN ENTORNO 802.11

EDGAR DE LA CRUZ ESPARZA

HERNÁN GEOVANNI TAIMAL

UNIVERSIDAD DEL CAUCA
FACULTAD DE INGENIERÍA ELECTRÓNICA Y TELECOMUNICACIONES
DEPARTAMENTO DE TELEMÁTICA
POPAYÁN, MAYO DE 2009

MIDDLEWARE DE SEGURIDAD PARA EL ACCESO A SERVICIOS IMS EN UN ENTORNO 802.11

EDGAR DE LA CRUZ ESPARZA

HERNÁN GEOVANNI TAIMAL

Trabajo de grado presentado como requisito para optar al título de
Ingeniero en Electrónica y Telecomunicaciones

Director
OSCAR MAURICIO CAICEDO RENDON
Magíster en ingeniería telemática

UNIVERSIDAD DEL CAUCA
FACULTAD DE INGENIERÍA ELECTRÓNICA Y TELECOMUNICACIONES
DEPARTAMENTO DE TELEMÁTICA
POPAYÁN, MAYO DE 2009

TABLA DE CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

Capitulo 1

Introducción

Durante muchos años, los servicios de telecomunicaciones se ofrecieron sobre infraestructuras dedicadas, como la telefonía fija o celular y la televisión, entre otros. A cada servicio generalmente correspondía un único proveedor y un dispositivo de acceso. En contraposición a esto, la banda ancha, el incremento de los terminales inteligentes y las Redes de Próxima Generación (NGN, Next Generation Networking) están provocando un cambio radical en el sector de las telecomunicaciones. En este nuevo panorama, mucho más complejo y competitivo, IMS (IP Multimedia Subsystem) juega un papel clave como modelo de arquitectura para la convergencia de redes y servicios, además su adopción permite a los operadores ofrecer paquetes de servicios cada vez más atractivos para los usuarios, como los denominados triple play, que combinan en una tarifa plana las llamadas nacionales de voz sobre la red fija, Internet de banda ancha y televisión.

La visión ideal de los proveedores de servicios y operadores de red, es proporcionar a los usuarios un terminal con un número único; una única agenda y un buzón de mensajería, para que aprovechen la conectividad de alta velocidad y utilicen los mismos servicios cuando se desplacen. Este cambio está dirigido por: la integración de los servicios de voz y datos sobre una infraestructura de conmutación de paquetes para establecer sesiones IP con calidad de servicio y la integración de las infraestructuras fijas y móviles bajo un conjunto común de mecanismos de señalización y de facturación. Estas ofertas empaquetadas responden, por un lado, a las nuevas demandas de los clientes, que buscan el ahorro que conlleva el consumo conjunto de varios servicios, una mayor previsión del gasto y la comodidad de gestión que aporta disponer de una factura única y un punto único de soporte. Pero también son atractivas para los operadores, ya que les permiten establecer una relación más estrecha y rica con sus clientes, y aprovechar de una forma más eficiente su costosa infraestructura de red.

Las expectativas sobre las mejoras y facilidades proporcionadas por la convergencia señalada y por ende por la red IMS son grandes, sin embargo el hecho de colocar el tráfico sobre la red IP evidencia problemas de seguridad, en IMS estos se agudizan debido a que todo el tráfico, tanto el de señalización como el de las aplicaciones se trasporta en el núcleo IP, el cual es más vulnerable por características intrínsecas a su funcionamiento como el uso de medios compartidos, la conexión de múltiples usuarios y el ofrecimiento de múltiples servicios, por esta razón es necesario el uso de tecnologías que permitan incrementar los niveles de seguridad [1]. Para los operadores de las redes de telecomunicaciones, la seguridad es una de las mayores preocupaciones a la hora de ofrecer servicios sobre su infraestructura de red, por consiguiente es importante tener el control de cada servicio ofrecido, controlar el acceso a sus recursos hardware de red y generar los cobros correspondientes al uso de servicios. Desde el punto de vista de los usuarios la seguridad es importante ya que no estarán dispuestos a ser suplantados, a pagar por servicios no consumidos, ni mucho menos a que su información privada sea divulgada, manipulada o aprovechada por terceras partes [2] [3]. De este modo, la seguridad en la comunicación puede ser un factor determinante para que un cliente prefiera una empresa prestadora de servicios de telecomunicaciones sobre otra [4].

En el TS 33.203 [3] el 3GPP define la arquitectura de seguridad para IMS, la cual proporciona esquemas para la gestión de integridad, confidencialidad y autenticación. Esta arquitectura consta de cinco partes o asociaciones diferentes que garantizan seguridad en distintos puntos, los primeros dos permiten asegurar la comunicación entre el equipo de usuario (UE) y el primer punto de red IMS conocido como P-CSCF; los demás puntos hacen referencia a la protección entre las entidades internas de la red IMS o entre redes de distinto operador.

En el anteproyecto se definió como objetivo general proporcionar seguridad en la comunicación entre el UE y el P-CSCF de una red IMS sobre 802.11 por este motivo el trabajo se enfoca sobre los dos primeros puntos

de la arquitectura de seguridad planteada para IMS. De acuerdo a los objetivos específicos del presente trabajo se tomó como referencia la red de acceso WLAN con la tecnología WiFi ya que esta red presenta gran cantidad de problemas de seguridad que si son resueltos garantizan su aplicación sobre otras menos vulnerables a ataques. Como estrategia para cumplir con los objetivos específicos del proyecto se procedió a establecer una base inicial de conocimiento alrededor de la seguridad en la comunicación del UE y el primer punto de comunicación de una red IMS, a partir del conocimiento se procedió a diseñar e implementar un middleware de seguridad IMS para iniciar y establecer una comunicación segura entre el UE y el P-CSCF, que permita: autenticación mutua entre el UE y la red local (HN, Home Network) IMS, establecer asociaciones de seguridad entre el UE y el P-CSCF y proveer la autorización al UE para el uso de servicios. Finalmente se comprobó el nivel de seguridad prestado por el middleware a través de un servicio de prueba.

En el establecimiento de la base conceptual se encontró principalmente que:

- La integración de estos dos tipos de redes (WLAN y las definidas por el 3GPP) aparte de ser un bueno punto de referencia en cuanto a seguridad, trae beneficios, a los subscriptores, a los proveedores de servicio de las redes definidas por el 3GPP y a los proveedores de servicio de internet inalámbrico. Esto aprovechando las mejores características de ambos tipos de red, como por ejemplo, el gran crecimiento y acogida de las tecnologías de red WLAN como WiFi por factores como: el bajo costo de despliegue y la mayor capacidad de trasferencia de datos (con velocidades de por ejemplo: 54Mbps) en comparación a las redes definidas por el 3GPP, sin embargo tienen un corto alcance y carecen de soporte de roaming y movilidad; por el otro lado los sistemas de comunicaciones de las redes móviles del 3GPP proveen gran cobertura, completa gestión del subscriptor y casi roaming universal. No obstante, están sujetos a ofrecer velocidades de trasferencia de hasta 2Mbps.

- Dentro del entorno de interworking entre redes WLAN y las definidas por el 3GPP (en las cuales se incluye IMS) la seguridad que debe garantizarse es la prestada para IMS, para ello el 3GPP especifica la arquitectura de seguridad 3GPP-WLAN la cual establece que, la autenticación al dominio WLAN haga uso del protocolo AKA basado en un mecanismo desafío-respuesta y criptografía simétrica. También específica que un usuario WLAN para acceder a los servicios de IMS debe realizar el procedimiento de autenticación AKA de manera independiente para cada uno de los dominios involucrados: WLAN, 3G e IMS. Convirtiéndose en un procedimiento ineficiente [6] [7] [8] [9].

Para el diseño e implementación del Middleware se partió de las características de seguridad y eficiencia identificadas en el interworking 3GPP-WLAN, las cuales fueron utilizadas para realizar la caracterización y obtener los requisitos (funcionales y no funcionales) de la solución, con ellos se planteó la arquitectura de referencia para la solución denominada MidSEG, la cual principalmente cumple con: proteger la señalización de IMS en el interworking con la WLAN, controlar el acceso a los dominios, unificar la autenticación del UE a los dominios involucrados, proteger la red contra usuarios no autorizados y mejorar la eficiencia del sistema de autenticación. Una vez definida la arquitectura de MidSEG se procedió a realizar una implementación de referencia, la cual se sometió a pruebas de seguridad y rendimiento. Finalmente, también se evaluó a MidSEG con un servicio de prueba.

En este documento se detalla, cada una de las partes que conllevan a la solución del problema de investigación y al cumplimiento de los objetivos, para ello se organizó de la siguiente forma:

- Cap2. Seguridad para el acceso a servicios IMS en un entorno 802.11, este capítulo contiene: la descripción general de la arquitectura IMS, sus ventajas, entidades y protocolos principales; aspectos de seguridad relevantes, conceptos, mecanismos, ataques y arquitectura de seguridad; escenarios de interworking 3GPP-WLAN; como parte final del capítulo se resume el estado actual de la seguridad en el interworking 3GPP-WLAN, arquitectura de seguridad, propuestas de distintos autores y se resumen las características identificadas en el interworking 3GPP-WLAN.

- Cap3. Middleware de Seguridad para el Acceso a IMS desde WLAN, este capítulo contiene: la caracterización de la solución a partir del análisis de seguridad del interworking WLAN-3GPP realizado en el capítulo 2; requisitos funcionales y no funcionales; seguidamente se establece la arquitectura de referencia, su descripción por subsistemas, actores, casos de uso, componentes, paquetes de análisis, paquetes de diseño, definición de interfaces internas y externas, diagramas de secuencia; diagrama de implantación para MidSEG; con el fin de evaluar la solución planteada se realiza una implementación de referencia; sobre la cual se realizaron tanto pruebas de seguridad como de rendimiento con sus respectivo análisis de resultados.

- Cap4. Servicio de Prueba, el capitulo cuatro está dirigido a probar la implementación de referencia con un servicio de prueba IMS, con el fin de evaluar la seguridad en la señalización del servicio;

- Cap5. Aportes, Conclusiones y Trabajos futuros, se listan los aportes y las conclusiones del trabajo, además se proponen nuevos proyectos a desarrollar sobre el tema.

- Anexo A. Implementación de Referencia de MidSEG, se detalla la implementación de referencia de MidSEG, como complemento a lo presentado en el Cap3.

- Anexo B. Herramientas de la Implementación de Referencia de MidSEG, se describe las herramientas utilizadas, su uso en MidSEG e instalación.

- Anexo C. Manuales de Instalación y Uso de MidSEG, se describe el proceso de instalación y configuración de los subsistemas que conforman el MidSEG y la forma de uso de cada uno de ellos.

- Anexo D. Articulo Middleware de Seguridad para el Interworking WLAN-IMS, artículo sobre el proyecto realizado, el cual se encuentra en revisión en la revista Facultad de Ingeniería de la Universidad de Antioquia, ISSN 0120-6230. Nota: se siguió el formato pedido por la Universidad de Antioquia, pero se cambio el tamaño de la letra y espaciado para quedar acorde al formato de la monografía.

Capitulo 2

Seguridad para el acceso a servicios IMS en un entorno 802.11

Este capítulo presenta la base conceptual sobre la cual se soporta el proyecto. Se hace una descripción general a IMS enfocada sobre la arquitectura de seguridad planteada por el 3GPP, se presentan los escenarios de interworking IMS-WLAN y finalmente se hace un análisis de la arquitectura de seguridad para el interworking WLAN-IMS planteada por el 3GPP tomando como referencia algunos autores.

2.1 IP MULTIMEDIA SUBSYSTEM - IMS

2.1.1 Introducción

IMS es una arquitectura genérica y modular, de interfaces abiertas para la prestación de servicios multimedia y de voz sobre tecnología IP, la cual es definida por el proyecto de asociación de tercera generación (3GPP, 3rd Generation Partnership Project*).* Permite la interoperabilidad y *roaming*[1] entre diferentes redes hacia un núcleo IP logrando así una convergencia de servicios independiente de la red de acceso [1] [11].

En su primera presentación el 3GPP introdujo a IMS en las redes UMTS, Release 5, en el cual se encuentran definidos: servicios de control de flujo de llamada, gestión de sesión, habilitadores de calidad de servicio (QoS, Quality of Service), procedimientos de tarificación, localización, identificación de usuarios y algunos requerimientos de seguridad. Este trabajo ha seguido complementándose en los Raleases 6, 7 y 8 donde principalmente se establecen escenarios de *interworking*[2] con redes WLAN e Internet para mantener los niveles de QoS y seguridad necesarios en la prestación de servicios multimedia sobre una única plataforma y para distintas redes de acceso [11].

2.1.2 Arquitectura

IMS no se orienta a definir las aplicaciones o servicios finales que pueden ofrecerse a los usuarios, sino a la estipulación de la infraestructura y las capacidades de red que los operadores y los proveedores de servicios utilizarán para construir sus propias aplicaciones y servicios comerciales [12]. Por consiguiente IMS adopta una arquitectura horizontal en la que los servicios y las capacidades pueden ser reutilizados por múltiples aplicaciones y se estructura en 4 capas (ver Figura 1) [13]:

- Acceso: representa a las tecnologías de acceso (UMTS, WiFi, xDSL, CDMA2000, Wimax, etc.).
- Transporte: representa a la capa física del núcleo de red IP, está compuesta de enrutadores interconectados, capaces de ofrecer QoS tanto para las redes de acceso como para las de tránsito.
- Control: es la encargada de la lógica de la señalización, permitiendo establecer, modificar y terminar sesiones por medio de los servidores de Control del Estado de la Llamada (CSCF, Call State Control

[1] Capacidad de movilidad del equipo de usuario (UE, User Equipment), sobre redes de telecomunicaciones pertenecientes a otros operadores, los cuales han establecido convenios con el operador local.

[2] Interconexión de diferentes tecnologías y arquitecturas de red, tanto a nivel físico como lógico.

Function). En esta capa también se encuentra el servidor de Funciones de Recursos Multimedia (MRF, Multimedia Resource Function") que ejecutan servicios de valor agregado para el usuario.

- Aplicación: en ella se encuentran los servidores de aplicaciones (AS, Aplication Server), en los cuales el operador puede ofrecer servicios propios o de terceros que le permitan diferenciarse de sus competidores.

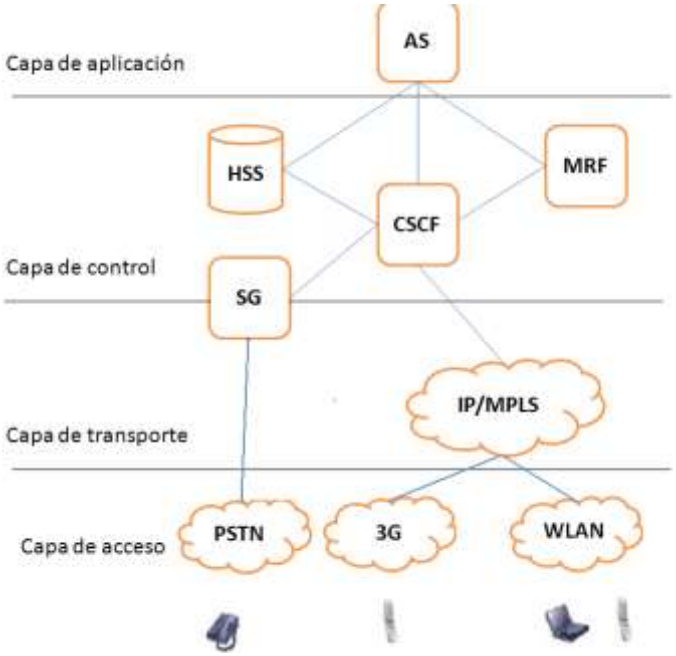

Figura 1. Arquitectura general de IMS.

2.1.2.1 Entidades

Las principales entidades que intervienen en el inicio y control de una sesión IMS son [13] [15] [16]:

Proxy-CSCF (P-CSCF): es el primer punto de contacto con la red IMS. Su función principal es determinar el Interrogating-CSCF (I-CSCF) de la red local del usuario, además interviene en la aplicación de las políticas de calidad y protección de señalización, su comportamiento es el de un proxy al recibir, procesar o reenviar peticiones de servicios, en roaming es el nodo de la red visitada que dirige la señalización hasta la red local.

I-CSCF: es el punto de frontera del dominio IMS para comunicarse con otros dominios, con la ayuda del servidor local de usuario (HSS, Home Suscriber Server) determina el Serving-CSCF (S-CSCF) apropiado para un usuario local en el proceso de registro. Además, puede generar los registros de tarificación de los diferentes servicios prestados por la red.

S-CSCF: desempeña el control y mantenimiento de la sesión de los servicios definidos por el operador de la red para un determinado usuario, responde a las solicitudes SIP realizadas, su funcionalidad se puede resumir en tres aspectos principales: interacción con la plataforma de servicios, registro del usuario y autorización del usuario al uso de servicios.

HSS: es la base de datos principal de IMS donde se almacenan y gestionan los perfiles de usuario, las claves de seguridad, se generan los vectores de autenticación y la llave compartida con el usuario para el procedimiento de autenticación.

Servidores de Aplicación (AS, Application Servers): proporcionan la plataforma de servicios para IMS, soportan los protocolos SIP y Diameter para la comunicación con el S-CSCF y el HSS respectivamente.

Función de recursos multimedia (MRF, Multimedia Resource Function): esta entidad proporciona el procesamiento de los flujos multimedia necesarios para una aplicación y funcionalmente se divide en dos partes: control MRF (MRFC, Controller MRF) y procesamiento MRF (MRFP, Processor MRF). El MRFC muestra una interfaz SIP a los otros componentes de la red, y proporciona las funciones de señalización y control, mientras que el MRFP proporciona las capacidades de procesamiento multimedia.

2.1.2.2 Protocolos

SIP: el protocolo de inicio de sesión (SIP, Session Initiation Protocol) permite establecer, controlar y terminar sesiones multimedia independientes del protocolo de transporte y del tipo de sesión que este siendo establecida, por esta razón SIP ha sido elegido por el 3GPP para el control de sesión y el control de servicio en IMS [17] [18].

El protocolo SIP utiliza un modelo cliente/servidor por lo cual se tienen dos tipos de mensajes, solicitudes del cliente al servidor y respuestas en el sentido contrario. Los dos tipos de mensajes están conformados por una línea con el método o código de respuesta SIP, uno o más encabezados, una línea vacía indicando el fin de los encabezados, y un cuerpo del mensaje que es opcional (Figura 2) [18]. En el RFC 3261 se definen 6 métodos SIP: REGISTER para registrar información de contacto, INVITE para establecer una sesión, ACK para dar respuesta a las solicitudes, CANCEL para abandonar sesiones en establecimiento, BYE para terminar sesiones establecidas y OPTIONS para interrogar las capacidades del servidor [18].

Figura 2. Mensaje genérico SIP

El IETF ha agregado al protocolo básico extensiones y cabeceras privadas para adaptar su uso a las necesidades del entorno móvil, y a las particularidades de UMTS. Por ello, se habla del perfil 3GPP del protocolo SIP, una variante personalizada para la red 3G IMS [17]. La descripción de las extensiones de las cabeceras privadas de SIP para el 3GPP son definidas en el RFC 3455 y la explicación de estas para el uso en una red IMS se pueden consultar en el estándar TS 24.229 del 3GPP [19].

SDP: el protocolo de descripción de sesión (SDP, *Session Description Protocol*) como su nombre lo indica permite la descripción de sesiones multimedia, siendo útil para invitaciones, anuncios, y cualquier otra forma de inicio de sesión. Los mensajes SDP se pueden transportar mediante el protocolo SIP por lo cual es utilizado en la arquitectura de red IMS [20].

Diameter: teniendo en cuenta los requerimientos de las organizaciones de estandarización y necesidades identificadas directamente de la industria de las telecomunicaciones, se desarrolló el protocolo Diameter como un conjunto de mejoras a RADIUS. Diameter proporciona un marco de autenticación, autorización y contabilidad (AAA, Authentication, Authorisation, y Accounting), para aplicaciones de acceso a redes, movilidad en redes IP y roaming. Se define en términos de un protocolo base y un conjunto de aplicaciones. El protocolo base proporciona unidad de datos, capacidades de negociación, manejo de errores y

extensibilidad; por su parte, una aplicación Diameter define funciones específicas y unidades de datos, adicionadas al protocolo base [21] [22].

Los tipos de nodos Diameter son: servidores, clientes y agentes. Un servidor maneja las solicitudes de AAA provenientes del cliente. Los clientes son usualmente dispositivos finales de red que desempeñan el control de acceso y originan las solicitudes de AAA. Los agentes proporcionan la retransmisión, delegación, redirección o traslación de servicios [21] [22].

Diameter es un protocolo punto a punto, lo que significa que cualquier nodo Diameter puede iniciar una solicitud. Además el protocolo base utiliza transporte confiable (TCP o SCTP) y asume que los mensajes son protegidos usando IPsec o TLS [21] [22].

RTP y RTCP: permiten el trasporte de contenido multimedia, la identificación de tipo, control y monitoreo de los datos en tiempo real. Una vez la sesión es establecida los participantes de la sesión intercambian directamente su tráfico a través del protocolo de transporte en tiempo real (RTP, Real-Time Transport Protocol). En las opciones de monitoreo se incluye la posibilidad de establecer la calidad de servicio requerida por el tipo de dato. Información detallada acerca de RTP y RTCP se encuentra en los RFC 1889 [23] y 3550 [24], respectivamente.

2.1.2.3 Puntos de referencia

Los puntos de referencia donde es necesario asegurar la señalización para el proceso de registro de un usuario a los servicios IMS son:

Gm: conecta al equipo de usuario (UE) con el núcleo de la red IMS. Define el transporte de toda la señalización SIP para los procedimientos de registro y gestión de sesión entre el UE y el P-CSCF **[25]**.

Cx: se encarga de la comunicación HSS/I-CSCF o HSS/S-CSCF. Para acceder o modificar la información del HSS tanto el I-CSCF como el S-CSCF hacen uso del protocolo Diameter. Los procedimientos manejados en este punto de referencia pueden dividirse en tres categorías: gestión de localización, manejo de datos de usuario y autenticación [22] [25].

2.1.3 Ventajas

Los cuatro servicios que predominan en el mercado actual de las telecomunicaciones son la voz, el video, el acceso de banda ancha a Internet y sesiones multimedia. La estructura IMS ofrece un medio para consolidar estos cuatro dominios independientes, bajo un mismo modelo de control de sesiones utilizando el protocolo SIP. Como resultado, se tendrán suscriptores con capacidad de movilidad que pueden acceder a la red en cualquier momento, desde cualquier lugar y desde cualquier dispositivo disponible [26].

Para los proveedores de servicios, IMS habilita la creación de servicios de forma fácil y rápida con la definición de interfaces abiertas, logrando así la entrada a nuevos segmentos de mercado con propuestas innovadoras a sus usuarios. Para el suscriptor, IMS abre la posibilidad de contar con un servicio más personalizado y la capacidad de cambiar o adoptar otros de manera dinámica [25].

En términos generales, IMS aporta las siguientes ventajas sobre las infraestructuras utilizadas actualmente:

- Uso de estándares abiertos
- Gestión de sesión (establecer, recibir, modificar y terminar una sesión).
- Calidad de servicio (en servicios multimedia, extremo a extremo y reserva de recursos).
- Privacidad y seguridad (garantiza al operador la remuneración por los servicios prestados, la prestación de sus servicios solo a usuarios autenticados y autorizados, confiabilidad e Integridad de los datos

transportados, IMS define una arquitectura de seguridad para la autenticación de los usuarios y entidades de la red).
- Reducción en los costos operativos de la red (menores costos de transmisión y operaciones simplificadas).
- Mayor habilidad para suplir los requisitos del usuario (distintas formas de acceso, posibilidad de agrupar servicios y facturación común).
- Rápido desarrollo de servicios (desarrollo más dinámico que en infraestructuras actuales, facilidad para crear servicios multimedia, independencia en el tipo de acceso, fortalecimiento de la fidelidad del cliente e incremento en los ingresos por la oferta de nuevos servicios).

2.2 ASPECTOS DE SEGURIDAD EN IMS

2.2.1 Conceptos y Mecanismos de seguridad

2.2.1.1 Criptografía

Es la herramienta básica para prestar seguridad en comunicaciones sobre canales inseguros, consiste en la aplicación de un algoritmo matemático en combinación con una clave sobre la información a transmitir, de forma que sólo quienes poseen la clave de apertura del cifrado podrán acceder a la información inicial [2].

Su objetivo es que las partes involucradas en una comunicación puedan intercambiar información sin que un tercero no autorizado a pesar de que capte los datos sea capaz de entender la información [3] [27].

2.2.1.2 Cifrado simétrico y asimétrico

Un sistema de criptografía puede ser simétrico o asimétrico.

Cifrado simétrico: son sistemas de clave secreta donde el emisor y el receptor utilizan una única clave para cifrar y descifrar. Es decir se utiliza la misma clave para ambos procesos, la complejidad de los algoritmos utilizados para este cifrado es menor que la del cifrado asimétrico por lo que su procesamiento también es menor, sin embargo el uso de una única llave lo hace más vulnerable a los ataques y el mantenimiento de la clave en forma secreta también es un problema [27] [28] [29].

Cifrado asimétrico: en estos sistemas cada usuario posee dos claves una pública y otra privada, una de ellas se utiliza para cifrar y la otra para descifrar. Dependiendo de la aplicación que se quiera dar, la clave pública será de cifrado o viceversa, con la característica que un mensaje cifrado con una de ellas solo se puede descifrar con la otra. La seguridad de estos sistemas depende de lo extremadamente difícil que resulta el cálculo de una de las claves a partir de la otra [27] [28] [29].

Ambos cifrados dependen de un correcto intercambio de claves y del mantenimiento seguro de ellas, por ello generalmente se soportan sobre mecanismos más complejos (p. Ej. protocolo de intercambio de claves en Internet (IKE, Internet Key Exchange)) que permiten el intercambio de forma segura [3] [27].

2.2.1.3 Firma digital

Es una aplicación de la criptografía, consiste en cifrar un mensaje con la clave privada del emisor, lo cual permite la identificación del usuario siempre que se cuente con la respectiva llave pública, ver Figura 3. Los algoritmos utilizados eliminan la posibilidad de falsificar la firma a partir de un documento firmado [28].

Figura 3. Firma Digital.

2.2.1.4 Función HASH

Las funciones Hash o de resumen sirven para comprimir un texto en un bloque de longitud fija. Aplicar una firma digital sobre un mensaje completo consume recursos y generalmente es un proceso lento, por lo que en la práctica se aplican funciones Hash sobre el mensaje para sacar el resumen sobre el cual se aplica la firma digital. Así, el receptor puede comprobar la integridad y autenticidad del mensaje por medio del resumen y la firma digital respectivamente. El resumen tiene la característica de ser único, es decir no existen dos mensajes diferentes con el mismo resultado de la función HASH. Los algoritmos más utilizados para funciones HASH son MD5, SHA-1 y variaciones de SHA-1 conocidas como SHA-2 [28].

2.2.1.5 EAP

El protocolo de autenticación extensible (EAP, Extensible Authentication Protocol) es especificado por el IETF como parte del estándar 802.1x[3] [30] y es frecuentemente usado en redes inalámbricas y conexiones punto a punto. EAP por sí solo no provee autenticación pero define algunas funciones comunes y un mecanismo de negociación del esquema de autenticación como: AKA, MD5, TLS, HTTP sobre SIP, etc. [31].

2.2.1.6 AKA

El protocolo de autenticación y acuerdo de llaves (AKA, Authentication and Key Agreement) proporciona autenticación mutua entre el UE y el servidor AAA de la HN. El acuerdo de llaves se refiere al mecanismo para generar la llave de cifrado y de integridad, utilizando una llave compartida entre el UE y el HSS. El mecanismo AKA puede ser dividido en dos partes: la distribución de los vectores de autenticación (AV, Authentication Vector) del HSS al servidor AAA como se muestra en la Figura 4 y la autenticación y establecimiento de llaves entre el UE y la HN (ver Figura 5) **[32]**.

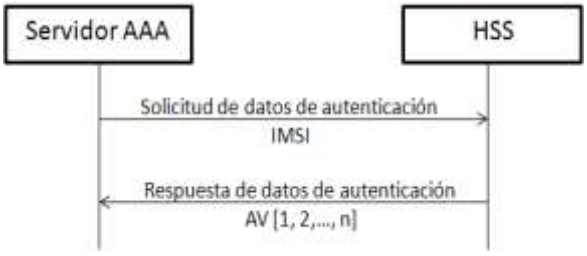

Figura 4. Distribución de vectores de autenticación.

[3] Mecanismo de control de acceso basado en puertos.

Figura 5. Autenticación y establecimiento de llaves

El protocolo AKA no corre directamente sobre IP, por lo que requiere un protocolo para transportar los mensajes entre el UE y el servidor AAA de la HN, IMS hace uso de SIP como medio para encapsular y transportar los mensajes AKA.

2.2.1.7 Seguridad para el protocolo IP (IP Security, IPsec)

Es un framework de estándares abiertos que proporciona confidencialidad, integridad y autenticación de datos entre los puntos de una comunicación a nivel IP. IPsec utiliza al protocolo IKE para el acuerdo de las llaves de autenticación y cifrado. Una vez se cuenta con las llaves se pueden establecer asociaciones de seguridad (SA[4], Security Asocciation).

Para la prestación de servicios de seguridad IPsec utiliza los protocolos: Encabezado de Autenticación (AH, Authentication Header) y Encapsulamiento Seguro de la carga útil (ESP, Encapsulating Security Payload).

IPsec define dos modos de funcionamiento: en modo transporte, solo la carga útil de los paquetes IP es cifrada y/o autenticada. En modo túnel: el paquete IP completo es cifrado y/o autenticado, encapsulándolo dentro de otro paquete IP para su enrutamiento.

Una descripción más completa sobre el funcionamiento de este protocolo se encuentra en [33].

2.2.1.8 IKE

Protocolo que permite el establecimiento y mantenimiento de SA en IPsec. Trabaja en base a solicitudes y respuestas por lo cual sus comunicaciones consisten de una pareja de mensajes llamados intercambios.

Para el establecimiento de un IKE_SA los intercambios iniciadores son el IKE_SA_INIT y el IKE_AUTH, una vez se haya iniciado la negociación de SA con los métodos anteriores se puede realizar los intercambios CREATE_CHILD_SA e INFORMATIONAL en cualquier orden y las veces que sea necesario. En el IKE_SA_INIT se negocian los parámetros de seguridad para el IKE_SA; en el IKE_AUTH se intercambian identidades, se prueba el conocimiento del secreto de las dos identidades y se establece una SA para el primer AH o ESP CHILD_SA. Los otros dos intercambios son usados para informes de error, eliminar SA, comprobar estados, etc.

Una descripción más completa sobre el funcionamiento de este protocolo se encuentra en [34].

2.2.1.9 Seguridad de la Capa de Transporte (TLS, Transport Layer Security)

[4] conexión simple que facilita servicios de seguridad para el tráfico que transporta. Para asegurar un comunicación bidireccional se deben establecer dos SA una para cada sentido.

Protocolo que brinda servicios de autenticación, privacidad e integridad de la información para dos aplicaciones de comunicación. Su seguridad se basa en el uso de llaves públicas, certificados y cifrado simétrico. Para una comunicación bidireccional se debe hacer uso de una infraestructura de llaves públicas (PKI, Public Key Infraestructure), la cual da soporte a los certificados que se manejan por medio de una entidad certificadora y procesos adicionales para el establecimiento de comunicaciones seguras [35].

2.2.2 Arquitectura de seguridad

Para abordar la seguridad en una red de comunicaciones como IMS es necesario considerar los siguientes aspectos [27] [28] [36]:

- Autenticación: consiste en la comprobación fiable de cada extremo de la comunicación, es decir garantizar que el emisor y el receptor de una comunicación son realmente quien dicen ser.
- Autorización: corresponde al paso siguiente a un resultado afirmativo de un procedimiento de autenticación, en el que se conceden los permisos para acceder a las aplicaciones o a información almacenada.
- Confidencialidad: este procedimiento debe realizarse tras una previa autenticación de los extremos de la comunicación, con el fin de proteger toda la información de la comunicación y evitar que sea descifrada por terceros.
- Integridad: evita que la información pueda ser modificada sin que el receptor se dé cuenta.
- No repudio: consiste en evitar que las partes involucradas en la transmisión de datos, nieguen sus acciones una vez las han realizado, en el caso del destinatario, negar la recepción del mensaje; y el envío, en la situación del remitente.

El 3GPP en el TS 33.203 define para IMS la siguiente arquitectura de seguridad, la cual consta de cinco partes o asociaciones diferentes (Figura 6) [3].

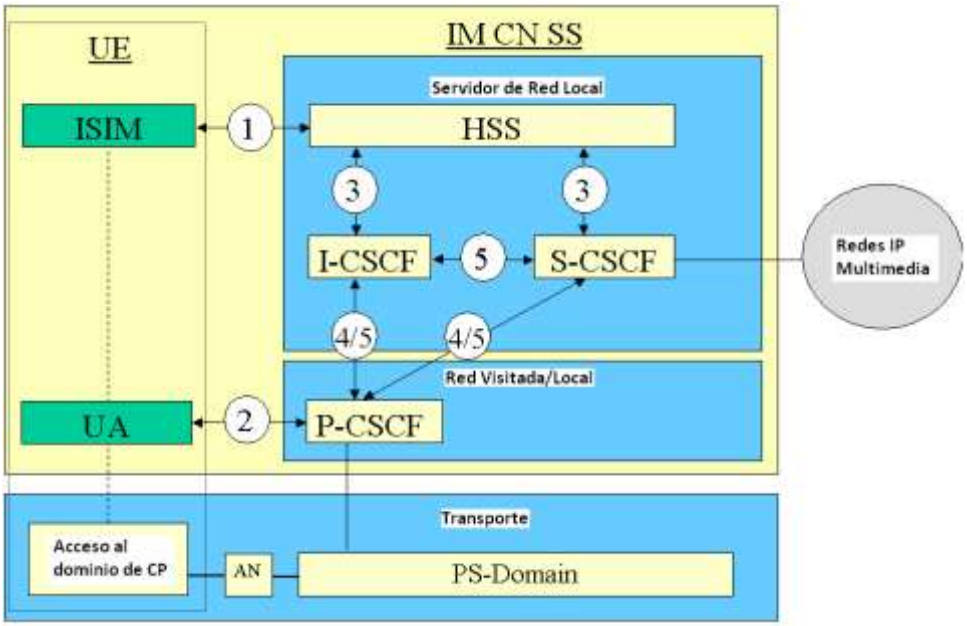

Figura 6. Arquitectura de seguridad IMS

Las diferentes relaciones de seguridad definidas por el 3GPP para IMS proporcionan esquemas para la gestión de la integridad, confidencialidad y autenticación. A continuación se describe cada asociación de seguridad para IMS según la numeración de la Figura 6 [3]:

1. Provee autenticación mutua entre el UE y el S-CSCF, el HSS delega la función de autenticación del subscriptor al S-CSCF, no obstante el HSS es responsable de generar las llaves y desafíos[5]. En el UE se encuentra la colección de datos de seguridad y funciones asociadas con la identidad privada de usuario (IMPI, IP Multimedia Private Identity) y al menos una identidad pública de usuario externa (IMPU, IP Multimedia Public Identity).
2. Provee un enlace seguro y una asociación de seguridad para proteger el punto de referencia Gm, el cual comunica el UE con el núcleo de red del subsistema IP Multimedia (IM CN, IP multimedia Core Network) [37].
3. Provee seguridad dentro del dominio de la red interna para la interfaz Cx.
4. Provee seguridad entre nodos SIP de diferentes redes. Esta asociación de seguridad es únicamente necesaria cuando el P-CSCF reside en la red visitante (VN, Visited Network).
5. Provee seguridad entre los nodos SIP de la red interna. Esta asociación de seguridad también se necesita cuando el P-CSCF reside en la VN.

En el diseño del middleware de seguridad, presentado en el capítulo 3, se toma como referencia las funcionalidades especificadas en los puntos 1 y 2, para proporcionar autenticación mutua, confidencialidad e integridad de la información entre el UE y la red IMS. Además Se hace uso de herramientas OpenSource[6] que implementan la interfaz-Cx, con el fin de lograr un middleware de seguridad más completo.

Este trabajo de grado se enfoca en la seguridad de acceso entre el UE y la red IMS de un operador por lo cual los puntos 4 y 5 no son contemplados ya que involucran aspectos de seguridad en los nodos de la red interna y entre dominios de operadores.

En la arquitectura de seguridad IMS, la protección de integridad y confidencialidad de la señalización SIP se realiza salto a salto como se puede ver en la Figura 7 [3] con un dominio de red seguro (NDS, Network Domain Security). El primer salto es entre el UE y el P-CSCF, los otros dos son inter-dominio e intra-dominio. Se trata de garantizar en IMS la integridad y confidencialidad usuario a red y salto a salto, pero no usuario a usuario. Para asegurar las comunicaciones bajo el mismo dominio administrativo se utiliza la interfaz Zb y entre diferentes dominios la Za, a través de pasarelas de seguridad (SEG, Security Gateway) [38].

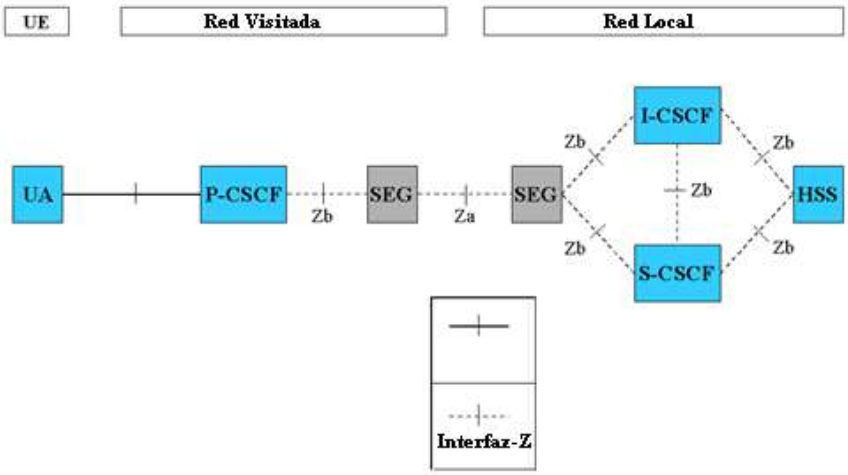

Figura 7. Vista general de la arquitectura IMS y la relación con un NDS

[5] Secuencia de mensajes generados a partir de la solicitud de registro en cuyo contenido se encuentran retos de seguridad o códigos que permiten la identificación de un extremo de la comunicación. Este procedimiento se basa en el uso de las claves públicas y privadas.

[6] software distribuido y desarrollado libremente.

A continuación se describen brevemente los principales ataques de seguridad aplicables a la seguridad de IMS.

2.2.3 Ataques

Resulta difícil garantizar seguridad cuando se trata de la integración de distintas redes como es el caso de IMS, donde se pretende converger múltiples redes de acceso tanto fijas como móviles. Por ejemplo, un atacante podría acceder por un medio inalámbrico, lanzar nodos falsos, interceptar y re-direccionar información confidencial de usuarios legítimos hacia otro lugar, comprometiendo el nivel de seguridad de toda la red. De este modo, para el estudio de la seguridad en IMS es importante considerar los posibles ataques, clasificados en: temporalmente dependientes o independientes. Un ataque dependiente del tiempo requiere un intervalo de tiempo para efectuar el daño sobre la víctima, como es el caso de los ataques por inundación (Flooding), mientras que los independientes del tiempo obtienen sus resultados de manera instantánea sobre el objetivo, como por ejemplo, la inyección de sentencias SQL [25] [39] [40].

2.2.3.1 Ataques dependientes del tiempo

Se caracterizan por dirigir una gran cantidad de paquetes de datos sobre un objetivo con el fin de exceder su capacidad de procesamiento. Para realizar ataques de este tipo se pueden utilizar distintos protocolos entre los que se incluyen, el Protocolo de Mensajes de Control de Internet (ICMP, Internet Control Message Protocol) [41], el Protocolo de Datagramas de Usuario (UDP,User Datagram Protocol) [42], el Protocolo de Control de Transporte (TCP, Transport Control Protocol) [43], y el protocolo SIP.

- **Por inundación de mensajes SIP REGISTER:** consiste en colapsar al P-CSCF por medio del envío de una gran cantidad de mensajes SIP REGISTER con Identificadores Uniformes de Recursos (URI, Uniform Resource Identifier) falsos o suplantados, este ataque se puede realizar de forma distribuida desde varias fuentes. Una vez se logra el colapso del P-CSCF los usuarios legítimos no pueden acceder a sus servicios.

- **Por inundación de mensajes SIP INVITE:** su objetivo y procedimiento es similar al anterior, con la diferencia que se vale del robo de información de las sesiones.

- **Por inundación de mensajes TCP SYN:** el objetivo de este ataque puede ser cualquier servidor o nodo de red que soporte TCP. Consiste en la creación de una gran cantidad de conexiones a medio establecer. El atacante inicialmente envía un mensaje SYN para abrir una conexión, el servidor responde con el mensaje SYN-ACK y queda a la espera de un mensaje de confirmación ACK el cual nunca es recibido porque las direcciones utilizadas son falsas o de destinos inalcanzables. Estas conexiones a medio establecer llenan el buffer del servidor hasta lograr su sobrecarga y consiguiente puesta en fuera de funcionamiento. El ataque se puede realizar también con los mensajes SYN-ACK en este caso se dirigen mensajes SYN a una gran cantidad de destinos en forma aleatoria, forzando a que el SYN-ACK se dirija a la víctima elegida.

- **Por inundación de mensajes ICMP:** este ataque se vale del mensaje ICMP echo solicitud de respuesta. Se dirige este mensaje con la dirección destino de broadcast y como origen la dirección de la víctima. Los múltiples destinos encontrados responden con el mensaje ICMP echo de respuesta sobrecargando la red y colapsando el sistema.

Para evitar los ataques dependientes del tiempo se utilizan sistemas para la detección y prevención de intrusos (IDP, Intrusion Detection and Prevention), los cuales a partir de la detección de anomalías en la red permiten aplicar políticas de seguridad para el control de acceso [44]. El correcto establecimiento de políticas de seguridad también ayuda a evitar este tipo de ataques.

2.2.3.2 Ataques independientes del tiempo

Son una amenaza seria para IMS ya que logran sus resultados de forma inmediata.

- **Falso mensaje SIP BYE:** este ataque es utilizado para terminar una sesión establecida, el atacante envía un falso mensaje SIP BYE a la red IMS como si fuera uno de los participantes de la sesión, finalmente este mensaje hace que el otro extremo termine con la comunicación para ser reemplazado por el atacante ya que la victima seguirá enviando el flujo multimedia. De este modo, el atacante necesita conocer los parámetros de la sesión.

- **Falso mensaje SIP CANCEL:** se vale del mensaje SIP CANCEL utilizado para terminar sesiones que aún no se han establecido. El atacante antes del último mensaje de establecimiento de una sesión envía un falso mensaje SIP CANCEL a la red IMS como si fuera el usuario que originó el INVITE, entonces la red cancela el proceso para el establecimiento de la sesión. Para realizar este ataque, el atacante también debe contar con información de la sesión en proceso de establecimiento.

- **Falso mensaje SIP Re-INVITE:** el mensaje SIP Re-INVITE se utiliza normalmente para cambiar parámetros de una sesión, sin embargo el atacante se vale de este tipo de solicitud para modificar la sesión a su conveniencia como por ejemplo enviar el flujo multimedia de la sesión a un destino malicioso.

- **Inyección de sentencias SQL:** consiste en la modificación de mensajes, lo cual puede presentarse porque SIP está basado en texto y su manipulación resulta fácil. Dentro de un mensaje SIP correcto el atacante puede insertar solicitudes de modificación de la base de datos, por ejemplo borrar el perfil completo de un usuario. La utilización de interfaces Web para la provisión de valor agregado en los servicios hace a IMS más vulnerable a este tipo de ataque.

Los anteriores ataques pueden ser evitados con la autenticación mutua del UE y la red, y protegiendo la señalización tanto en su confidencialidad como integridad.

2.3 INTERWORKING WLAN-IMS

Los sistemas de comunicaciones móviles del 3GPP proveen gran cobertura, completa gestión del subscriptor y casi roaming universal. No obstante, están sujetos a ofrecer velocidades de transferencia de hasta 2Mbps, este ancho de banda resulta pequeño si se compara con otro tipo de tecnologías inalámbricas o cableadas.

Por otro lado, tecnologías de red WLAN como WiFi ha tenido gran crecimiento y acogida por factores como: el bajo costo de despliegue y la mayor capacidad de transferencia de datos (con velocidades de por ejemplo: 54Mbps) si se las compara con las redes definidas por el 3GPP, sin embargo tienen un corto alcance y carecen de soporte de roaming y movilidad.

Así, con la integración de estos dos tipos de redes (WLAN y definidas por el 3GPP) se pueden aprovechar las ventajas de cada una y traer el mayor beneficio a los subscriptores (p. Ej: acceder tanto a los servicios de la WLAN como del 3GPP), a los proveedores de servicio de las redes definidas por el 3GPP (p. Ej: ampliar su cobertura a redes WLAN, brindar servicios que requieren mayor ancho de banda a través de la WLAN), y también, a los proveedores de servicio de internet inalámbrico (WISP, Wireless Internet Service Provider) (p. Ej: ofrecer el acceso a los servicios del 3GPP).

A continuación se describen los escenarios, la arquitectura y los requisitos de seguridad para el interworking WLAN-IMS.

2.3.1 Escenarios Interworking

El 3GPP en el TR 22.934 [45] plantea el enfoque para lograr interworking con las WLAN, mediante seis escenarios incrementales que aumentan progresivamente el nivel de inter-funcionamiento entre los dos sistemas de tal forma que su aplicación garantice flexibilidad y escalabilidad [46].

A continuación se da una breve descripción de cada uno de los escenarios, sin embargo, es necesario precisar que este trabajo de grado de acuerdo a sus objetivos se centra en el escenario tres ya que en el mismo se contemplan los aspectos relacionados con la seguridad y el acceso a los servicios de IMS. No se toman las consideraciones de un escenario superior porque en ellos se tratan aspectos que están fuera del alcance del proyecto como por ejemplo acceso a los servicios de conmutación de circuitos (CS, Circuit Switched).

2.3.1.1 Escenario 1 - Una sola Factura

Este es el más simple esquema del interworking 3GPP-WLAN. El cliente recibe una sola cuenta de cobro del operador móvil por el uso de los servicios de la red 3GPP y la WLAN. De este modo, no se necesita ningún interworking real y el nivel de seguridad de los dos sistemas puede ser independiente.

2.3.1.2 Escenario 2 - Sistema de control de acceso y cobro de la red 3GPP

Este es el escenario donde la AAA es provista por la red 3GPP, cuando un usuario solicita acceso a la WLAN. Reutilizar el sistema de control de acceso del 3GPP da mayores facilidades para el manejo de cuentas, ya que el operador 3G puede permitir a los subscriptores de su base de datos acceder a una WLAN con un mínimo esfuerzo de despliegue. El escenario permite que los usuarios de la WLAN sean autenticados por la red 3GPP, pero éstos no tienen acceso a los servicios de la última.

2.3.1.3 Escenario 3 – Acceso a los servicios de PS del 3GPP

El objetivo de este escenario es permitir al operador de una red 3GPP extender el sistema de servicios basados en conmutación de paquetes (*PS*, *Packet* Switched) a la WLAN, tales como servicio de mensajería multimedia, servicios basados en localización, mensajería instantánea, presencia, etc. Para lograr esto algunos nuevos componentes o mecanismos se deben agregar al núcleo de la red 3G como se verá más adelante. En este escenario la continuidad del servicio entre la red 3G y la WLAN no es requerido.

2.3.1.4 Escenario 4 – Continuidad en el servicio

El objetivo de este escenario es que haya continuidad en los servicios soportados en el escenario 3, cuando se realiza un cambio de acceso entre WLAN y sistemas 3GPP. El cambio puede ser notificado al usuario, pero no será necesario que éste restablezca el servicio. También podría cambiar la QoS y es posible que algunos servicios no puedan mantenerse.

2.3.1.5 Escenario 5 – Continuidad total del servicio

La meta es proveer continuidad del servicio sin interrupciones, entre las tecnologías de acceso, para los servicios soportados en el escenario 3. De este modo, en el escenario 5 se requiere minimizar la pérdida de datos y el retardo del handoff[7].

2.3.1.6 Escenario 6 – Acceso a los servicios de CS del 3GPP

[7] Proceso de comunicaciones móviles para la transferencia del servicio de un punto de conexión a otro.

Permite acceso a los servicios provistos por las entidades de conmutación de circuitos del núcleo de red 3G sobre la WLAN. Este escenario no implica ningún tipo de características de conmutación de circuitos para ser incluida en la WLAN.

La Tabla 1 muestra las capacidades de servicio y operación de cada escenario de interworking WLAN-3GPP. A medida que el escenario aumenta es necesario cumplir con más requerimientos y mecanismos.

Tabla 1. Capacidades de servicio y operación de cada escenario de interworking WLAN-3GPP

Característica	Escenario 1	Escenario 2	Escenario 3	Escenario 4	Escenario 5	Escenario 6
Una sola factura	X	X	X	X	X	X
Clientes comunes	X	X	X	X	X	X
Control de acceso basado en el sistema 3GPP		X	X	X	X	X
Facturación basado en el sistema 3GPP		X	X	X	X	X
Acceso a los servicios de PS del 3GPP			X	X	X	X
Continuidad en el servicio				X	X	X
Continuidad total del servicio					X	X
Acceso a los servicios de CS del 3GPP						X

2.3.2 Arquitectura de Interworking

En [47], el 3GPP describe el estado actual del interworking 3G-WLAN y establece un modelo de referencia para los escenarios 1, 2 y 3, los otros se encuentran aún en investigación. Los elementos considerados para el interworking 3GPP-WLAN son descritos a continuación:

- HN: incluye al servidor de AAA del 3GPP y una pasarela de paquetes de datos (PDG, Packet Data Gateway). El servidor AAA será el encargado de autenticar a los subscriptores que pertenezcan a la HN independiente de la red de acceso, es también el encargado de recuperar la información de autenticación del HSS para ejecutar el procedimiento AKA hacia el equipo de usuario [46]. El PDG ejecuta algunas funciones de enrutamiento para conectar a los usuarios de la WLAN hacia un punto de la red 3G, traduce y mapea direcciones, puede sacar trafico no autorizado con funciones de filtrado de paquetes y generar información de cobro relacionada con el tráfico de datos del usuario [6].

- Red visitante (SN, Serving Network): en el caso de roaming los elementos de la red visitante que intervienen son 3GPP AAA proxy, punto de acceso (AP, Access Point) y WAG (WLAN Access Gateway). El servidor AAA de la SN actúa como proxy reenviando la información de autenticación hacia el servidor AAA de la HN. Cuando un UE accede a los servicios 3G a través de la WLAN, el tráfico es dirigido al WAG para generar la información de cobro de los usuarios que acceden a través del WLAN AN (WLAN Access Network) en el caso de roaming y dirige los paquetes hacia el PDG [46] [6].

- Red de acceso WLAN: contiene al equipo de usuario (UE, User Equipment) y los puntos de acceso inalámbrico (AP, Access Point). El UE permite acceder a la red WLAN, usualmente puede ser un computador o PDA con tarjeta inalámbrica y tarjeta UICC/USIM. El AP es un dispositivo que permite al equipo de usuario conectarse con la red LAN y actúa como cliente, el cual reenvía la información de seguridad al servidor AAA de la HN a través de los proxies AAA [7].

En la Figura 8 se muestra la arquitectura de interworking para los escenarios 2 y 3 en el caso de roaming.

En el escenario 2, el tráfico de autenticación es dirigido a la HN por medio de la SN. El UE se encuentra asociado a un AP, encargado de reenviar el tráfico hacia el proxy AAA para que este último lo dirija al

servidor AAA de la HN del subscriptor. Si el proceso de autenticación es exitoso, el tráfico de los datos del usuario es autorizado y habilitado para alcanzar la Internet.

En el escenario 3, el UE es autenticado como en el escenario 2, sin embargo, si el usuario quiere acceder a los servicios de PS del 3G, el tráfico de sus datos será dirigido hacia el PDG vía el WAG de la SN. En otras palabras el PDG actúa como firewall, contacta otras redes y provee una entrada segura de una red IP pública al núcleo de la red 3G.

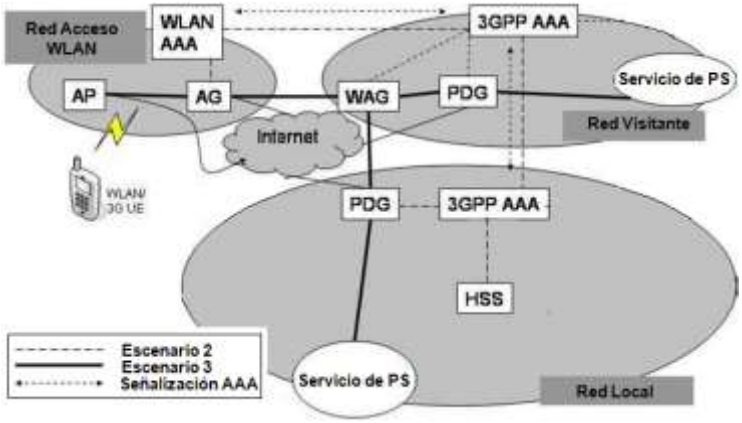

Figura 8. Arquitectura de interworking escenarios 2 y 3

2.3.3 Seguridad 3GPP-WLAN

El 3GPP ha especificado una arquitectura de seguridad para las redes NGN, la cual se encuentra en periodo de maduración [3] [48], apuntando a proteger a los usuarios móviles, la transferencia de datos y la red, con el fin de no comprometer el nivel de seguridad en el interworking WLAN-3GPP. Distintos autores [6] [7] [8] [9] han encontrado que esta arquitectura presenta ineficiencias por lo que han presentando propuestas alternativas en las que explican sus aportes y mejoras a la misma.

En la siguiente sección se explica la arquitectura definida por el 3GPP y a continuación una breve explicación de las propuestas alternas.

2.3.3.1 Arquitectura de Seguridad 3GPP-WLAN definida por el 3GPP

Las redes de tercera generación hacen uso del protocolo AKA, el cual utiliza un mecanismo desafío-respuesta y criptografía simétrica, para la autenticación mutua entre el UE y la red. En las redes WLAN, AKA es transportado por el protocolo EAP permitiendo el uso de la infraestructura de autenticación de las redes definidas por el 3GPP [50].

La arquitectura de seguridad específica que un usuario WLAN para acceder a los servicios de IMS debe realizar el procedimiento de autenticación AKA de manera independiente para cada uno de los dominios: WLAN, 3G e IMS. Tal como se describe a continuación.

Autenticación al dominio WLAN

El usuario y la WLAN son autenticados uno al otro usando el protocolo EAP-AKA [50]. En este caso intervienen el UE, el AP que actúa como cliente AAA, y el servidor AAA encargado de recuperar la información de autenticación del HSS. A continuación se describen los pasos del procedimiento (ver Figura 9) [48]:

- El AP pide la identidad del usuario con una Solicitud EAP.

- El UE responde, enviando una Respuesta EAP al servidor AAA con la identidad de usuario.
- El servidor AAA comprueba sí posee vectores de autenticación para el usuario (almacenados a partir de una previa autenticación).
- Si el servidor AAA no tiene vectores de autenticación, envía la IMSI del usuario para obtener n vectores de autenticación. Los cuales son derivados de la llave compartida, entre el UE y la red 3G, e incluyen: un desafío aleatorio (RAND), la autenticación de la red (AUNT), la respuesta esperada (XRES), la llave de encriptación (CK) y la llave de integridad (IK).
- El servidor AAA selecciona un vector de autenticación y almacena los n-1 vectores para uso futuro.
- El servidor AAA almacena y genera la llave maestra (MK, Master Key) usando la CK, IK y la identidad del usuario, para una rápida re-autenticación. Además de la MK se deriva la llave maestra de sesión (MSK, Master Session Key) empleada en la seguridad de 802.11i para la generación de las llaves de sesión WLAN.
- El servidor AAA envía un desafío AKA en una Solicitud EAP al usuario, el cual contiene el RAND, AUNT y un código de autenticación del mensaje (MAC, Message Authentication Code), el cual verifica la integridad del mensaje EAP.
- El UE recibe el mensaje EAP, verifica la integridad del mensaje con el MAC y ejecuta el algoritmo UMTS-AKA para verificar el AUNT.
- Si es correcto el AUNT, el UE calcula IK, CK, MK y MSK. Análogo al servidor AAA el UE almacena la MK para generar una rápida re-autenticación.
- El UE calcula la respuesta al desafío AKA (SRES) y envía una respuesta EAP con el MAC del mensaje.
- El servidor AAA server verifica la integridad del mensaje, si es correcta comprueba que XRES y SRES sean iguales.
- Si todas las comprobaciones son exitosas, el servidor AAA envía un mensaje EAP exitoso junto con la MSK para el AP.

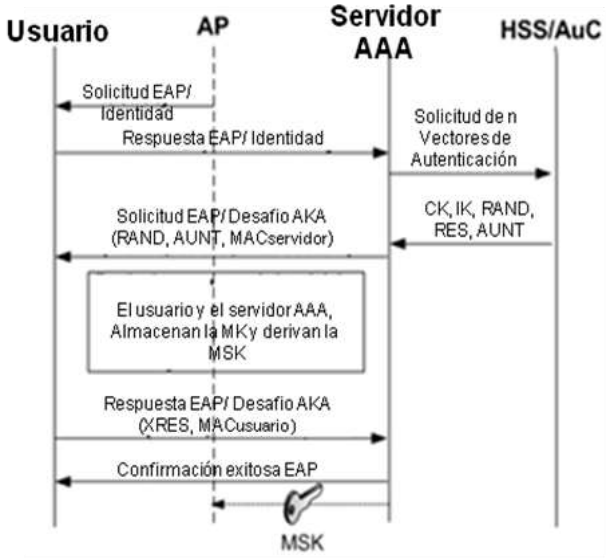

Figura 9. Autenticación al dominio WLAN

Finalizada la autenticación EAP-AKA, el usuario y la WLAN se han autenticado mutuamente. Adicionalmente, el usuario obtiene una dirección IP local que le permite ejecutar el protocolo de intercambio de llaves (IKE, Internet Key Exchange) para la autenticación al dominio 3G.

La autenticación al dominio WLAN tiene el inconveniente de repetirse cada vez que el UE hace hand-off a un nuevo AP, acorde al estándar 802.11.

Autenticación al dominio 3G

Ejecuta el protocolo IKE [49], el cual permite autenticación mutua entre el UE y el PDG, y establecer una asociación bidireccional de seguridad IKE (IKE_SA, Internet Key Exchange Security Association), que provee seguridad para la ejecución del protocolo EAP-AKA. A continuación se describe el proceso (ver Figura 10) [48]:

- Se establecen las IKE_SA entre el PDG y el UE.
- El UE y el servidor AAA ejecutan el protocolo EAP-AKA y el PDG reenvía los mensajes al servidor AAA por medio del protocolo DIAMETER.
- El PDG encapsula el desafío EAP-AKA en IKEv2, agrega su certificado (CERT) y el campo $AUTH_r$.
- El usuario autentica a la red 3G y al PDG verificando los campos AUNT y $AUTH_r$ respectivamente.

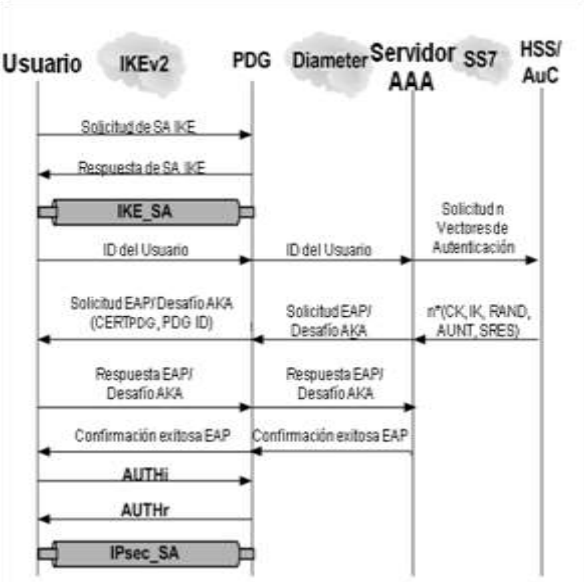

Figura 10. Autenticación al dominio 3G

Como resultado de la autenticación al dominio 3G, el usuario obtiene una dirección IP global o remota, la cuál es usada para acceder a los servicios 3G de PS. Además, se establece un túnel entre el UE y el PDG que provee confidencialidad e integridad a los datos intercambiados entre ellos. Como desventaja se tiene que el UE cada vez que renueva su dirección IP, por hand-off u otra razón, debe repetir esta autenticación y establecer nuevas SA, ya que estas dependen de la dirección IP, además el uso de certificados para la autenticación del PDG implica el despliegue de una PKI y mayor procesamiento para el dispositivo móvil.

Autenticación al dominio IMS

Después del proceso de autenticación al dominio 3G, el usuario debe registrarse en el dominio IMS para acceder a los servicios de PS IMS. Para lograr esto es necesaria una autenticación entre el UE y el S-CSCF, con el fin de obtener un enlace seguro en el punto de referencia Gm [30]. El procedimiento de autenticación a ejecutarse es IMS-AKA, el cuál a diferencia de los anteriores que utilizaban el protocolo EAP para encapsular los mensajes AKA esté lo hace con SIP. A continuación se describe el procedimiento (ver Figura 11) [3]:

- El UE envía un mensaje SIP REGISTER al P-CSCF, en el que se debe incluir el mecanismo de seguridad soportado por el UE.
- El P-CSCF procesa el mensaje SIP REGISTER y utilizando el dominio determina la dirección IP del I-CSCF y redirige la solicitud.

- El I-CSCF elige el S-CSCF a partir de la información que obtiene del HSS, después le reenvía la solicitud de registro.
- Inicialmente el S-CSCF procesa el mensaje REGISTER y obtiene información para la autenticación mutua desde el HSS.
- El S-CSCF responde con un mensaje 401 (No Autorizado) en el que se incluyen llaves de seguridad (IK, CK), información de autenticación (AUNT), y un reto de seguridad (RAND). Este mensaje es reenviado al UE a través del I-CSCF y el P-CSCF.
- El P-CSCF retira la información de seguridad para establecer el canal de seguridad con el UE y pasa la respuesta al UE.
- El UE autentica la red IMS, establece un canal seguro unidireccional con el P-CSCF y envía al S-CSCF la respuesta al reto de seguridad en un nuevo mensaje SIP REGISTER.
- El S-CSCF comprueba la respuesta del UE (XRES = SRES), de ser correcta realiza las siguientes operaciones con el HSS: actualiza el estado, registra la identidad pública y obtiene el perfil del usuario. Luego responde al UE con un mensaje 200 OK para indicarle que ha sido registrado.
- El UE es notificado del estado de registro y el P-CSCF asocia la identidad pública de usuario al UE.

Si el proceso de registro es exitoso, el UE obtiene autorización para el establecimiento de sesiones.

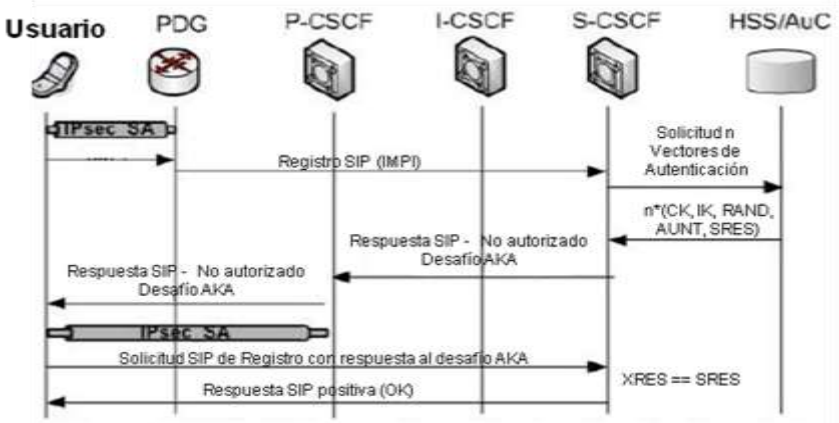

Figura 11. Autenticación al dominio IMS

Considerando las autenticaciones a los dominios WLAN y 3G, se vuelve redundante e ineficiente otra al dominio IMS, teniendo en cuenta que IMS forma parte del dominio 3G. Sin embargo, si es necesario proteger la señalización entre el UE y el P-CSCF, realizar la asignación de un S-CSCF que permita la interacción con la plataforma de servicios de IMS y la actualización del perfil de usuario para la prestación de servicios.

Finalmente con las autenticaciones a los dominios WLAN, 3G e IMS y las SA establecidas se cumple con los puntos uno y dos de la arquitectura de seguridad de IMS (ver sección 2.2.2).

2.3.3.2 Otras Propuestas para la Arquitectura de seguridad 3GPP-WLAN

El modelo de autenticación presentado por el 3GPP para soportar seguridad en un ambiente 3GPP-WLAN, tiene desventajas dado que para acceder a IMS se deben seguir tres procedimientos de autenticación, que involucran la ejecución del protocolo AKA en cada uno, introduciendo sobrecarga a la red debido al intercambio de múltiples mensajes que causan: i) retardo en la autenticación del usuario, ii) aumento en el consumo de recursos de radio y iii) mayor procesamiento de los dispositivos, lo cual puede inducir al aumento del consumo de energía (recursos limitados principalmente en dispositivos móviles). Así, la realización de los tres procedimientos de autenticación AKA tiene un impacto adverso sobre aspectos de QoS ofrecido a usuarios finales, deteriorando el rendimiento del sistema en general [6] [7] [8] [9].

Propuesta de autenticación SIP-Digest-AKA

En la solución propuesta en [9] el autor plantea migrar la funcionalidad de autenticación de capa 2 (802.1x/ EAP-AKA) al nivel de servicio (SIP-Digest-AKA), implementando la confidencialidad y el control de acceso en la capa IP a través de IPsec. De esta forma, con un solo proceso de autenticación se disminuye el retardo, además, migrar la funcionalidad a una capa más alta proporciona mayor flexibilidad para la configuración en la parte de acceso. También tiene la ventaja de ser independiente de la tecnología de acceso (capas 1 y 2) pudiendo ser aplicada tanto a redes 802.11 como a Bluetooth.

La arquitectura de solución (Figura 12), tiene como principal aporte respecto al sistema planteado por el 3GPP, un nuevo dispositivo (WLAN P-CSCF) en la red de acceso con capacidades SIP, implementación de IPsec y control de acceso haciendo uso de filtrado de paquetes, solo usuarios autenticados correctamente son dotados de conectividad IP, para usuarios no autenticados la única comunicación permitida es la que tenga como objetivo realizar autenticación.

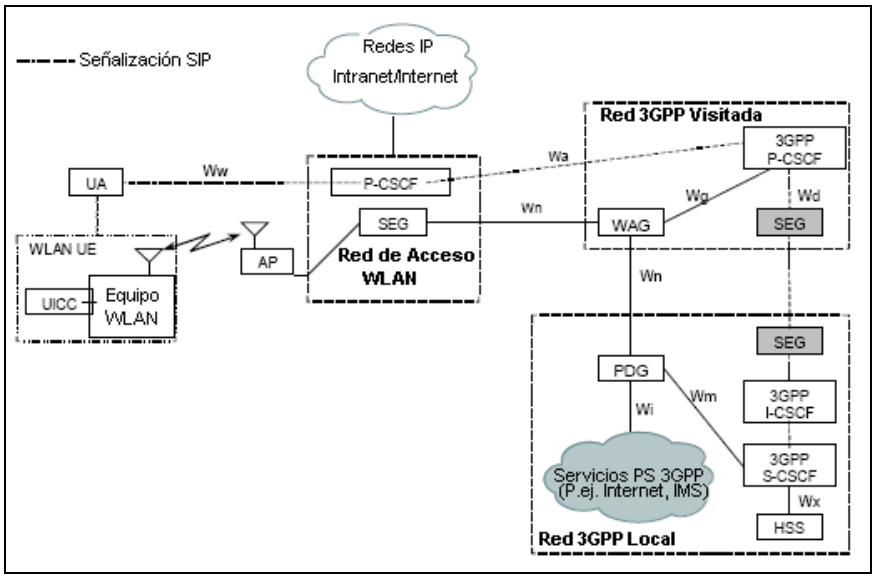

Figura 12. Arquitectura de autenticación propuesta.

Puesto que la autenticación del UE en esta propuesta es basada en SIP-Digest-AKA, la red de acceso proporciona la conectividad SIP/IP a través de las interfaces Ww y Wa, junto con la funcionalidad P-CSCF establecida. La confidencialidad e integridad de la señalización SIP sobre la interfaz Ww es proporcionada utilizando IPsec mientras que la protección en la interfaz Wa se deja a cargo del estándar de protección entre proxies (IPsec o TLS). Después de un correcto procedimiento de autenticación y el establecimiento dinámico de SA entre el UE y el WLAN P-CSCF, se realiza la negociación de SA entre el UE y el WLAN SEG para la protección de los datos del usuario en la interfaz de radio.

La solución presentada en este aparte es genérica para redes WLAN pero no garantiza la seguridad para la señalización entre el WLAN P-CSCF y la red IMS, además no tiene en cuenta en el proceso de registro a las entidades WAG y PDG, por lo que es necesario un intercambio adicional de mensajes para notificarles el resultado del proceso, además no especifica el acceso al dominio 3G al no considerar al PDG [6].

Propuesta de Autenticación EAP-AKA (tres pasos)

La propuesta presentada en [7] [8] consiste en una sola autenticación AKA conformada por 3 pasos. En el primero, el usuario y la WLAN se autentican mutuamente ejecutando EAP-AKA. Además en este paso el

usuario y el servidor de autenticación generan y almacenan la MK. En el segundo, el usuario es autenticado al dominio 3G PLMN ejecutando IKEv2 que omite la encapsulación de EAP-AKA, así, la autenticación de la negociación de los puntos finales (el usuario y el PDG) está basada sobre la MK. El tercer paso elimina la necesidad de ejecutar IMS-AKA para registrarse al dominio IMS, resultando en menos procesamiento del intercambio de mensajes y autenticaciones, el hecho que IMS no autentique al usuario no implica ningún riesgo de seguridad, ya que IMS es localizado dentro y operado por el 3G PLMN, el cual ha sido ya autenticado en pasos previos. Así, la propuesta de autenticación en un solo paso combina la primera y segunda autenticación y elimina los requerimientos para una doble ejecución EAP-AKA, reduciendo en general la sobrecarga de las tres autenticaciones, otra diferencia es que no establece un túnel IPsec entre el usuario y el P-CSCF lo cual no impone ninguna amenaza de seguridad, ya que el despliegue del túnel seguro entre el usuario y el PDG protege los mensajes del protocolo SIP.

La seguridad de esta propuesta se soporta en la privacidad de la llave MK. Si la llave es revelada, un adversario puede autenticarse como un usuario valido al dominio 3G o escuchar el tráfico de datos del usuario legítimo. Los caminos en los cuales el adversario podría recuperar la MK son los siguientes: deduciendo la MK de las llaves de sesión WLAN, vulnerando la seguridad de las entidades que almacenan la MK y ejecutando un ataque de suplantación del servidor AAA. Adicionalmente, los tres pasos propuestos dependen de la autenticación a la WLAN, por lo que cada vez que haya hand-off se deberá realizar el proceso de autenticación completo y considerando la poca cobertura de los AP en WiFi esta solución puede ser ineficiente.

Propuesta de Autenticación EAP-AKA (un paso)

La solución presentada en [6] escoge la capa 2 para autenticación, principalmente por la escalabilidad del protocolo EAP, en el sentido de que si una posible debilidad es encontrada en uno de los métodos de autenticación o en un algoritmo específico de integridad, la solución podría ser fácil y rápidamente adoptada. Además, esto permite al UE escoger entre algunos métodos de autenticación, acorde al nivel de seguridad que el usuario y/o la red quiere alcanzar. La solución provee una autenticación unificada, adicionando un nuevo encabezado en el mensaje EAP por medio del cual el usuario puede escoger los servicios de la red que desea acceder.

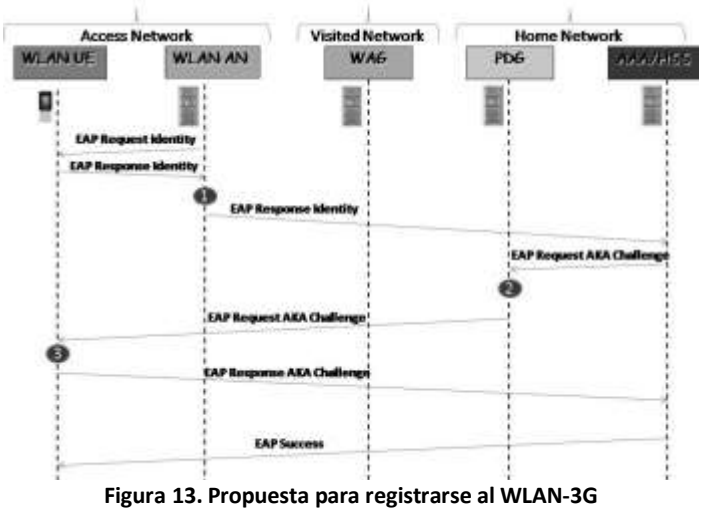

Figura 13. Propuesta para registrarse al WLAN-3G

En la Figura 13, se presenta el esquema de la propuesta de registro al WLAN-3G, su principal desventaja es que no se tienen en cuenta las entidades que pertenecen al domino IMS, por lo consiguiente no se establece un túnel seguro entre el UE y el P-CSCF, otro aspecto es que al igual que la propuesta anterior el proceso de autenticación debe repetirse cada vez que haya hand-off.

2.3.3.3 Resumen

En la Tabla 2 se muestra una comparación de las diferentes características propuestas para la arquitectura de seguridad del interworking WLAN-3GPP.

Tabla 2. Comparación de las arquitecturas de seguridad propuestas para interworking WLAN-3GPP

Característica	3GPP	Autenticación SIP	Autenticación EAP (tres pasos)	Autenticación EAP (un paso)
Uso del protocolo AKA	si	si	si	si
Autenticación a los 3 dominios	si	si	no	si
Autenticación unificada	no	si	no	si
Túnel de seguridad entre el UE y PDG	si	no	si	si
Túnel de seguridad entre el UE y P-CSCF	si	no	no	no
Protección de la interfaz de radio	si	si	si	si
Menor procesamiento del dispositivo móvil	no	si	si	si
Menor trafico de autenticación	no	si	si	si
Menor tiempo para la autenticación	no	si	si	si
Independiente de la tecnología WLAN	no	si	no	no
Ausencia de un sistema PKI	no	si	si	si
Protección contra ataques DoS o DDoS	no	no	no	no
Involucra las entidades de Interworking (PDG y WAG)	si	no	si	si
Involucra las entidades de IMS en la autenticación	si	no	no	no
Evita la adición de nueva entidades en el acceso	si	no	si	si

En el capítulo 3 se realiza el análisis de cada uno los aspectos de la Tabla 2 y posteriormente se describe la solución propuesta en este trabajo de grado, teniendo en cuenta los aspectos determinantes del modelo para la arquitectura de seguridad WLAN-3G del 3GPP y los aportes realizados por otros investigadores.

Capitulo 3

Middleware de Seguridad para el Acceso a IMS desde WLAN

3.1 CARACTERIZACIÓN DEL MIDDLEWARE

En el capítulo 2 se sustentó que establecer el interworking WLAN-IMS es de gran importancia teniendo en cuenta que las tecnologías WLAN permiten mayores tasas de transferencia y menores costos comparado con redes celulares, generando mayores beneficios al operador y servicios para el usuario. También se observó que un punto importante al momento de establecer este interworking es mantener el nivel de seguridad de la red IMS, principalmente en lo relacionado a la privacidad en las comunicaciones con la codificación de la señalización (señalización IMS) y de toda la información que viaja por el aire (para el caso de la WLAN); y por otro lado controlar el acceso a los dominios de red, es decir autorizar o denegar el acceso según las políticas y perfiles de usuario.

El 3GPP plantea una arquitectura de seguridad (ver sección 2.3.3.1) con tres autenticaciones, una para la WLAN, otra al dominio 3G y finalmente a IMS, sin embargo varios autores la critican, identificando como principal problema la ineficiencia en el registro a IMS causada por las tres autenticaciones [6] [7] [8] [9]. De este modo, a partir de las recomendaciones y las propuestas de distintos autores, en la Figura 14 se presenta el modelo del ambiente [51] de la propuesta Middleware de Seguridad para el acceso a IMS desde WLAN, a la cual se le ha denominado MidSEG. Como características esenciales el MidSEG controla el acceso a los servicios WLAN e IMS, protege la interfaz de radio, provee una comunicación segura para la señalización SIP manejada entre el cliente WLAN y el P-CSCF, proporciona una interfaz de comunicación segura con el núcleo IMS y establece el mecanismo de autenticación a los dominios WLAN, 3GPP e IMS. En la siguiente sección se detalla cada una de las características del MidSEG.

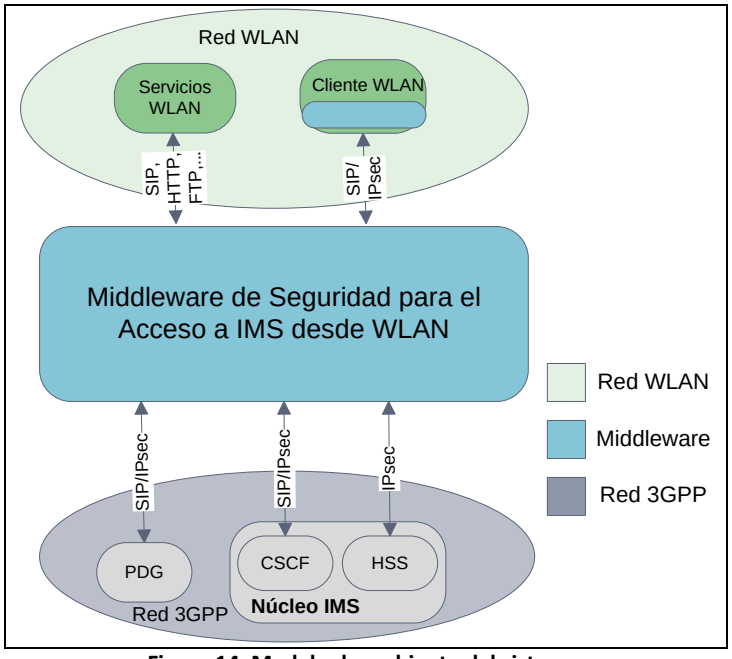

Figura 14. Modelo de ambiente del sistema.

A continuación se presenta el análisis de las características de la Tabla 2 para la completa definición del MidSEG.

3.1.1 Características de seguridad en el interworking WLAN-IMS

- Una de las características identificadas para el interworking WLAN-IMS consiste en el uso del mecanismo AKA el cual: i) Permite la deducción de las claves de integridad y de cifrado. ii) Proporciona autenticación mutua entre el usuario y la red. iii) Utiliza números de secuencia y contadores para evitar repeticiones en los datos de autenticación. iv) Es la recomendación del 3GPP para la autenticación de entidades móviles. A partir de todos estos aspectos se optó por utilizar en MidSEG este mecanismo para la autenticación mutua y el acuerdo de claves entre el UE y la red IMS.

- En cada uno de los tres dominios involucrados en el interworking IMS-WLAN se cuenta con diferentes servicios, entidades, privilegios, etc. Por lo tanto, se requiere una diferenciación en el control de acceso a cada dominio, principalmente la gestión de autorización aplicando los perfiles de usuario configurados y una autenticación previa. De este modo, MidSEG permite reutilizar la autenticación a IMS por cada una de las entidades encargadas del control de acceso en cada dominio, disminuyendo los tres procesos de autenticación descritos en la sección 2.3.3.1 a uno solo, permitiendo la reducción de tráfico de registro, el menor consumo de recursos tanto de red como de procesamiento y un menor tiempo de registro. De esta forma, al hacer uso de la autenticación IMS, es el S-CSCF quien lleva a cabo el procedimiento AKA con el UE para la autenticación mutua y el acuerdo de llaves de sesión entre el usuario y la red. Esta autenticación se reutiliza para controlar el acceso a cada uno de los tres dominios. La unificación de la autenticación a la capa de nivel de servicio trae como ventaja que la seguridad en la comunicación establecida entre el UE y la red IMS es completamente independiente de la red de acceso por lo que se podría aplicar la solución a otras tecnologías.

- Al considerar la seguridad en sistemas inalámbricos se tienen factores adicionales de riesgo ya que cualquiera puede tener acceso al medio de trasmisión y a su vez a la información transportada, además con la ayuda de antenas los ataques pueden ser realizados a grandes distancias, eliminando cualquier rastro físico. Con el objetivo de evitar violaciones de seguridad de este tipo MidSEG cuenta con una entidad en la WLAN que permite iniciar el procedimiento de registro para usuarios no autenticados mediante el uso de mensajes SIP REGISTER. Cuando el registro del UE es exitoso se obtienen las llaves de cifrado e integridad que permiten establecer túneles seguros entre el UE y la entidad de seguridad de la WLAN, garantizando confidencialidad e integridad de la señalización sobre la interfaz inalámbrica.

- Para asegurar la señalización hasta el dominio IMS, MidSEG cuenta con túneles de seguridad configurados entre el subsistema de seguridad de la WLAN (SSW) y el subsistema de seguridad P-CSCF (SSP) ubicada como punto de entrada al núcleo IMS. Con una previa autenticación los túneles seguros proveen privacidad al usuario y protegen a la red contra los abusos (p. Ej: evitar que usuarios ilegítimos obtengan acceso a la red). Además, se establece una comunicación segura entre la entidad de control WLAN y el PDG para permitirle al usuario el acceso a los servicios de la red 3GPP de forma segura. En este punto es importante aclarar que el PDG debe ser configurado para permitir el paso de mensajes SIP REGISTER provenientes de usuarios no autenticados que vayan dirigidos hacia IMS, esto debido a que el PDG es el punto de acceso al 3GPP.

- Los ataques descritos en la sección 2.2.3, se evitan garantizando la autenticidad de cada una de las entidades que participan en la comunicación; con el correcto funcionamiento del MidSEG y de sus servicios de seguridad: autenticación, control de acceso y privacidad de la señalización. Se identifica como una posible vulnerabilidad el ataque por inundación de mensajes SIP REGISTER ya que serán los únicos aceptados para usuarios no autenticados, la cual se salvaguarda estableciendo un límite en la cantidad de mensajes SIP REGISTER de entrada por segundo, de acuerdo a la capacidad de procesamiento de los servidores, evitando así que se sobrecarguen.

- Teniendo en cuenta que en cada uno de los seis escenarios mostrados en la sección 2.3.1 se definen de forma incremental distintos aspectos para lograr un completo interworking WLAN-3GPP, se optó por trabajar con MidSEG en el escenario tres, debido a que trata aspectos como: i) El acceso a los servicios de PS (en los que se encuentra IMS). ii) El acceso a los servicios de AN. iii) La reutilización del mecanismo de autenticación 3GPP. De este modo, se incluyen en el MidSEG propuesto aspectos asociados a: autenticación mutua, autorización a los servicios y el establecimiento de asociaciones de seguridad entre el UE y el P-CSCF.

Como resumen de las características, la Tabla 3 ilustra las características de alto nivel del MidSEG, que sirvieron de base para la identificación de sus requisitos funcionales y no funcionales.

Tabla 3. Caracterización del MidSEG

Característica	Descripción
Realiza la autorización, autenticación y control de acceso	Red IMS
Escenario de interworking	Tres
Proceso de autenticación a los dominios WLAN, 3G e IMS	Unificado
Nivel de autenticación	Servicio
Tecnología de acceso WLAN	Independiente
Protocolo de autenticación	AKA
Protocolo de transporte de AKA	SIP
Entidad encargada de las funcionalidades AA	MidSEG, S-CSCF, PDG,
Protección de integridad y confidencialidad	Túneles de seguridad entre: UE<->MidSEG, MidSEG<->P-CSCF y MidSEG <-> PDG
Control de acceso en la WLAN	MidSEG
Control de acceso en el 3GPP	PDG
Control de acceso en IMS	MidSEG
Protección de la interfaz de radio	IPsec

3.1.2 Requisitos de la solución

A partir de las características mostradas en la Tabla 3, se identificaron los siguientes requisitos para MidSEG.

3.1.2.1 Requisitos funcionales

- Controlar el acceso de paquetes a los dominios WLAN e IMS. De este modo el MidSEG protege las entidades de la red contra abusos y permite el tráfico, únicamente a usuarios registrados. Esta funcionalidad debe estar presente en cada uno de los tres dominios del interworking WLAN-IMS teniendo en cuenta que se ofrecen servicios de distinto tipo.
- Permitir al UE registrarse a la red WLAN, 3GPP o IMS. De esta manera MidSEG permite que el usuario escoja el tipo de acceso y obtenga el uso de los servicios conforme a su elección, por otro lado el

operador tiene la posibilidad de realizar una diferenciación de usuarios y ejecutar el respectivo control de acceso.

- Obtener los desafíos de autenticación que permitan al UE autenticar las redes WLAN, 3GPP e IMS. De este modo, MidSEG evita que terceros suplanten a una o todas las redes.
- Unificar la autenticación del UE a los dominios WLAN, 3GPP e IMS, reutilizando la autenticación realizada por el núcleo IMS. Así, MidSEG evita la suplantación de un usuario legítimo, es decir garantiza que la comunicación de la red es con el usuario y no con alguien diferente.
- Actualizar el estado del usuario. MidSEG modifica el HSS como resultado de un registro satisfactorio con el fin de habilitar los servicios configurados en su perfil (p. Ej: Para una llamada entrante a un usuario, la red debe localizarlo haciendo uso del previo registro realizado), de la misma forma la red debe ser notificada cuando un usuario sale del sistema.
- Validar la integridad de los datos. MidSEG de esta forma garantiza la seguridad en la comunicación establecida entre el UE y el P-CSCF, evitando que alguien ajeno a la comunicación modifique, inserte o elimine información de acuerdo a su conveniencia.
- Cifrar la señalización. De esta forma, MidSEG permite garantizar la confidencialidad en la comunicación entre el UE y el P-CSCF. Cada usuario al momento de registrarse obtiene unas llaves de cifrado diferentes que permiten el establecimiento de asociaciones de seguridad, las cuales garantizan la privacidad en la comunicación y evitan que información confidencial llegue a manos de terceros.
- Proteger la red contra usuarios no autorizados. El MidSEG implementa esta funcionalidad para garantizar al operador la integridad de la infraestructura y la disponibilidad de la red para los usuarios legítimos.

3.1.2.2 Requisitos no funcionales

- Mejorar la eficiencia del sistema de autenticación en el interworking WLAN-IMS en cuanto al retardo, la sobrecarga de la red causada por las múltiples autenticaciones, el consumo de recursos de radio y de procesamiento. Todo esto se logra unificando la autenticación a los dominios WLAN, 3G e IMS.
- Seguridad en la señalización entre el UE y el P-CSCF, esto se logra con el establecimiento de SA entre: UE<->MidSEG y MidSEG<->P-CSCF
- Independiente de la tecnología WLAN utilizada (p. Ej: WiFi, Bluetooth, WiMax, etc.), esto se logra con La unificación de la autenticación a la capa de nivel de servicio y la utilización de IPsec.

3.2 ARQUITECTURA DE REFERENCIA

Para satisfacer los requisitos estipulados en la sección 3.1.2 se plantea como solución al MidSEG, el cual se encuentra dividido en tres subsistemas funcionales: i) Subsistema Cliente de Seguridad WLAN-IMS (SCSWI), ii) SSW y iii) SSP. La arquitectura de referencia utiliza el modelo NGN para describir los subsistemas, dado que el MidSEG permite el interworking de la red IMS (definida bajo el modelo NGN) con la red WLAN, en la Tabla 4 se muestra las funcionalidades del MidSEG en el modelo NGN.

Tabla 4. Funcionalidades del MidSEG en el Modelo NGN

Capa	Funcionalidad
Transporte	Comunicación segura entre los subsistemas y las entidades externas.
Control	Lógica del MidSEG.
Aplicación	Interacción con el usuario.

Los colores usados en la Figura 15 indican lo siguiente:

Azul claro: representa a las entidades externas al MidSEG sobre las cuales se tiene control para realizar cambios en su implementación.
Azul oscuro: representa al MidSEG para el acceso a IMS desde WLAN.

Rojo: representa las entidades externas al MidSEG sobre las cuales no se tiene control y por lo tanto no se pueden realizar cambios en su implementación.

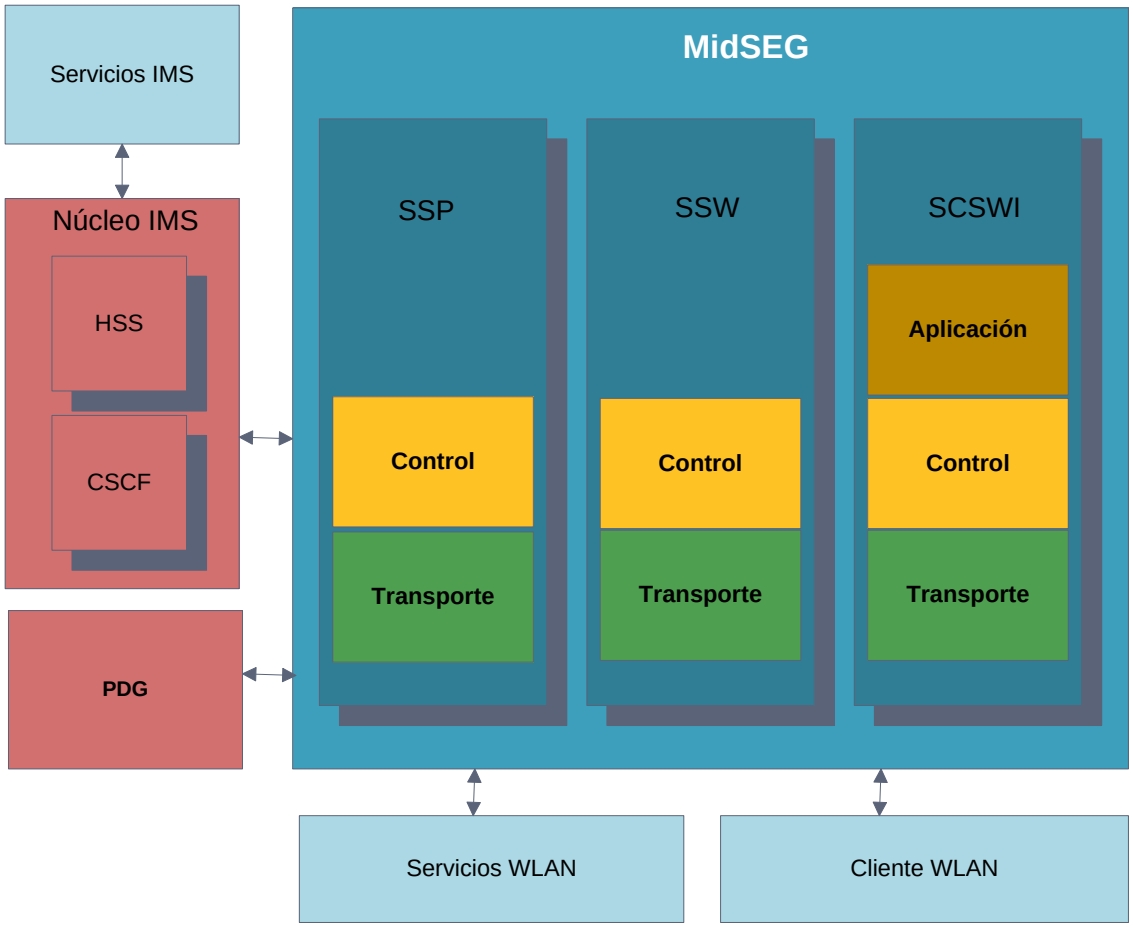

Figura 15 Arquitectura de referencia.

A continuación se describe con más detalle cada uno de los subsistemas que conforman al MidSEG.

3.2.1 Descripción de la Arquitectura de Referencia del Sistema

3.2.1.1 Diagrama de subsistemas

En la Figura 16 se muestra el diagrama de subsistemas, en el cual se indican las interfaces de comunicación con las entidades externas al MidSEG y entre subsistemas. En el diagrama se puede observar que el SCSWI forma parte del Cliente WLAN y que se comunica con el SSW a través de señalización SIP protegida por un túnel IPsec. El SSW a parte de la comunicación con el SCSWI provee una interfaz hacia los servicios WLAN, los cuales usan protocolos de aplicación como SIP, HTTP, FTP, etc. También provee una interfaz de comunicación asegurada por IPsec hacia el SSP con el fin de alcanzar el dominio IMS y proteger su señalización. El SSP hace uso de SIP para comunicarse con el núcleo IMS y de asociaciones de seguridad con el HSS para acceder a la base de datos del HSS.

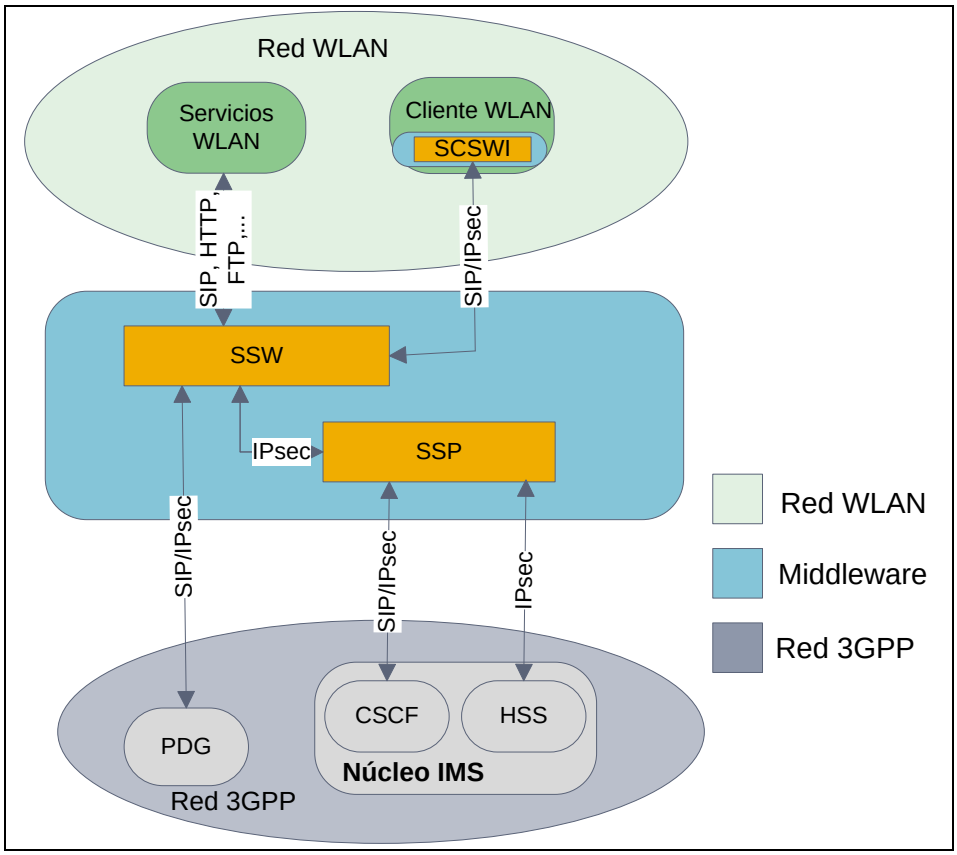

Figura 16 Diagrama de subsistemas

3.2.1.1.1 Subsistema Cliente de Seguridad WLAN-IMS

Inicia el procedimiento de registro elaborando un mensaje SIP REGISTER y lo envía al SSW. A este mensaje, el subsistema le adiciona tres nuevos encabezados, uno de ellos permite transportar los dominios a los cuales el usuario se desea registrar y los otros dos sirven para informar la protección deseada para la interfaz de radio. Los encabezados son: Realm por medio del cual se informa al MidSEG los dominios a los que desea acceder el usuario; AH-Alg que contiene el algoritmo elegido para el protocolo de seguridad AH y ESP-Alg para indicar el algoritmo del protocolo de seguridad ESP.

El establecimiento previo de una llave compartida con la red IMS permite al UE generar la respuesta correcta a los desafíos enviados por la red, calcular las llaves de cifrado e integridad y autenticar a la red, además cuenta con las capacidades para establecer SA dinámicas IPsec a través de AKA con el SSW. Finalmente, el UE provee la interfaz que informa al usuario del estado del proceso de registro.

3.2.1.1.2 Subsistema de Seguridad WLAN

Se encarga de realizar el filtrado de paquetes para controlar el acceso a los dominios WLAN, 3GPP e IMS, provee asociaciones de seguridad para la comunicación con SCSWI, PDG y SSP. Estas SA IPsec permiten proteger: la interfaz de radio para los servicios de la WLAN, la comunicación con el PDG para alcanzar los servicios de la red 3GPP y la señalización de IMS, respectivamente.

Procesa los mensajes SIP necesarios para el registro, del primer mensaje SIP REGISTER obtiene la IP del UE y los algoritmos de seguridad elegidos por el usuario para la protección de la interfaz de radio, del mensaje SIP NO AUTHORIZATION enviado por el SSP, retira las llaves de cifrado y de integridad con las cuales configura

las SA con el SCSWI, y del mensaje SIP OK enviado también por el SSP, obtiene la autorización para el acceso a los dominios elegidos, en esta última parte el subsistema configura el filtrado de tráfico para permitir el paso de paquetes a los dominios autorizados por el SSP y agrega el encabezado Ip-Realm que contiene las direcciones IP con las cuales se deben configurar las SA de IPsec para alcanzar los dominios WLAN, 3GPP o IMS. En este ámbito la información se mantendrá segura dado que se encuentra configurada una SA IPsec para proteger la información de registro.

3.2.1.1.3 Subsistema de Seguridad P-CSCF

Se encarga de controlar el acceso a la red IMS permitiendo únicamente conexiones a los SSW con los que se ha establecido algún tipo de acuerdo para la prestación de servicios. Unifica la autenticación a los dominios WLAN, 3GPP e IMS, actualizando la HSS. Además mantiene un túnel IPsec dinámico a través de IKE con los SSW, con el fin de garantizar confidencialidad e integridad de la señalización manejada entre estos subsistemas.

Esta entidad es el punto de entrada al núcleo IMS de forma que únicamente a través de ella un SSW puede acceder a IMS, para ello se establece una zona desmilitarizada[8] (DMZ, Demilitarized Zone) para las peticiones SIP con el P-CSCF.

Envía la autorización al SSW sobre los dominios registrados por el usuario, agregando un encabezado al mensaje SIP OK denominado Realm-Auth, el cual contiene los dominios en los cuales el usuario ha sido registrado con éxito.

3.2.1.2 Definición de las interfaces de los subsistemas

3.2.1.2.1 Interfaces internas del MidSEG

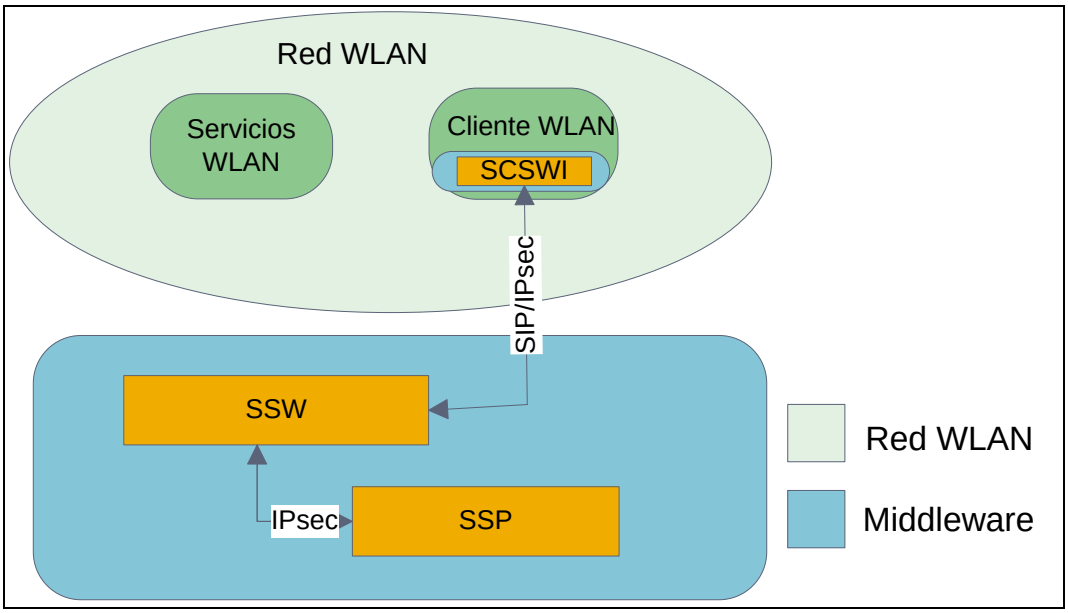

Figura 17. Interfaces internas de los subsistemas

A continuación se describen las interfaces entre los subsistemas de la Figura 17:

[8] Es la parte de la red donde que permite conexiones tanto de la red interna como externa, en este caso es el P-CSCF. El I-CSCF y S-CSCF no pueden ser accedidos directamente por la red externa.

- **SCSWI - SSW**

Estos dos subsistemas se comunican a través de una interfaz IPsec, la cual permite intercambiar información de manera segura. Cada vez que el cliente WLAN se autentica se configura dinámicamente esta interfaz para asegurar la comunicación entre estos dos subsistemas y la señalización IMS.

El SCSWI utiliza el procedimiento AKA para generar las llaves de CK e IK. El SSW obtiene estas llaves del mensaje NO-ATHORIZATION enviado por el SSP, con el fin de establecer las SA de IPsec.

- **SSW - SSP**

Estos dos subsistemas también se encuentran unidos a través de una interfaz de comunicación IPsec, la cual utiliza IKE para el establecimiento dinámico de SA, de esta forma se garantiza la confidencialidad e integridad de los paquetes intercambiados entre estos dos subsistemas. Su seguridad es fundamental ya que el SSP envía a través de ella las llaves de CK e IK con el fin de establecer la interfaz SCSWI – SSW.

Las interfaces SCWI-SSW, SSW-SSP, junto con el filtro configurado en el SSP garantizan la seguridad en la comunicación entre el UE y el P-CSCF ya que los subsistemas intermedios son autenticados y utilizan conexiones IPsec dinámicas, la primera por medio de AKA-SIP y la segunda con IKE, lo que permite mantener la confidencialidad e integridad de la señalización.

3.2.1.2.2 Interfaces externas de los subsistemas

A continuación se describen las interfaces que cada uno de los subsistemas posee con el ambiente externo al MidSEG (ver Figura 18):

Subsistema de Seguridad WLAN

- **Interfaz SIP, HTTP, FTP, …**

Esta interfaz hace referencia a la comunicación que tiene el SSW con los servicios prestados por la WLAN, los cuales únicamente son alcanzables para el usuario por medio del SSW, el cual controla el acceso, permitiendo pasar solo los paquetes de usuarios correctamente autenticados.

- **Interfaz IPsec**

Interfaz de comunicación entre el SSW y el PDG con el objetivo de alcanzar los servicios prestados por la red 3GPP de forma segura, mantiene la confidencialidad e integridad en los datos manejados.

Subsistema de Seguridad P-CSCF

- **SSP-CSCF**

Mediante esta interfaz el SSP puede manejar la señalización SIP que le permite interactuar con el P-CSCF, con el fin de reenviar la señalización SIP a IMS. Esta interfaz es asegurada con el establecimiento de SA IPsec.

- **SSP-HSS**

Mediante esta interfaz el SSP puede interactuar con la base de datos del HSS, con el fin de solicitar las llaves de CK e IK de un usuario y de actualizar el registro a los dominios WLAN, 3GPP e IMS. Esta interfaz es asegurada con el establecimiento de SA IPsec.

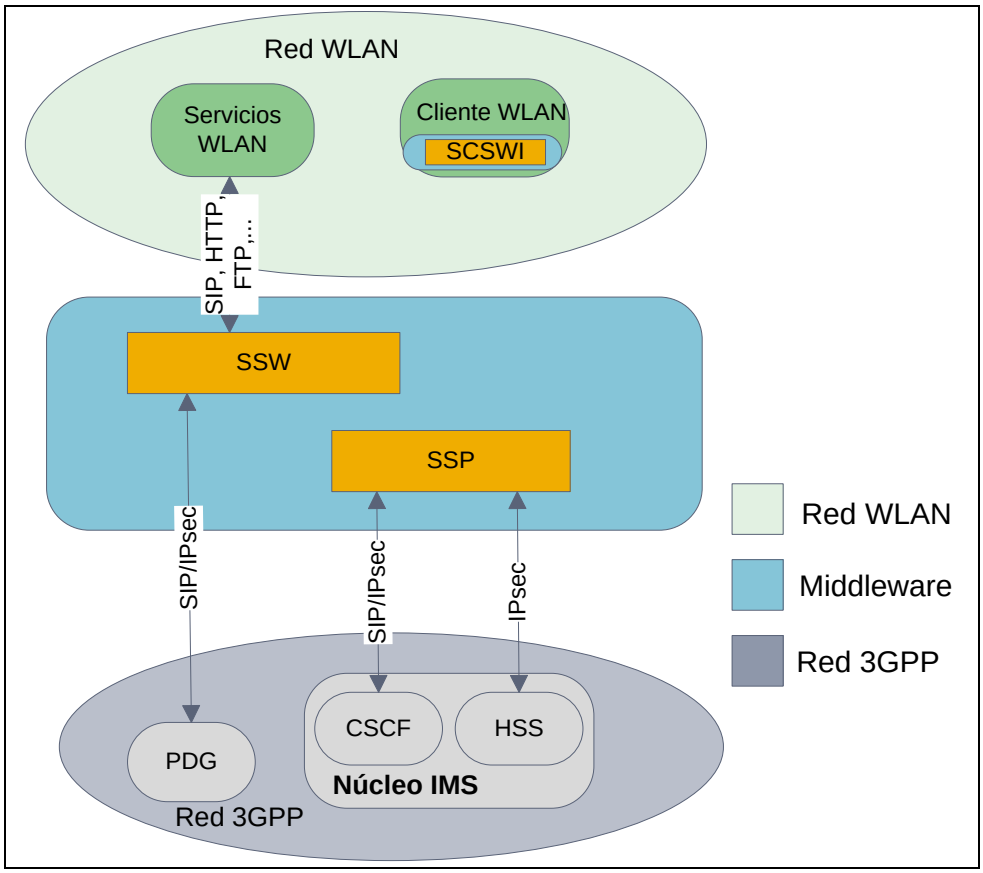

Figura 18. Interfaces externas de los subsistemas

3.2.1.3 Descripción de los subsistemas

3.2.1.3.1 Subsistema Cliente de Seguridad WLAN-IMS

Es la parte del MidSEG que se encuentra en el UE, entre sus funciones están:

- Registrar el UE a los diferentes dominios (WLAN, 3GPP e IMS) que elija el usuario.
- Autenticar a la red.
- Deducir las llaves de CK e IK.
- Establecer SA con el SSW.
- Utilizar SIP como protocolo de transporte del mecanismo AKA.
- Permitir la configuración de seguridad de la interfaz de radio.

Para cumplir con estas funcionalidades el subsistema se subdivide en los componentes mostrados en la Figura 19.

3.2.1.3.1.1 Diagrama de componentes del Subsistema

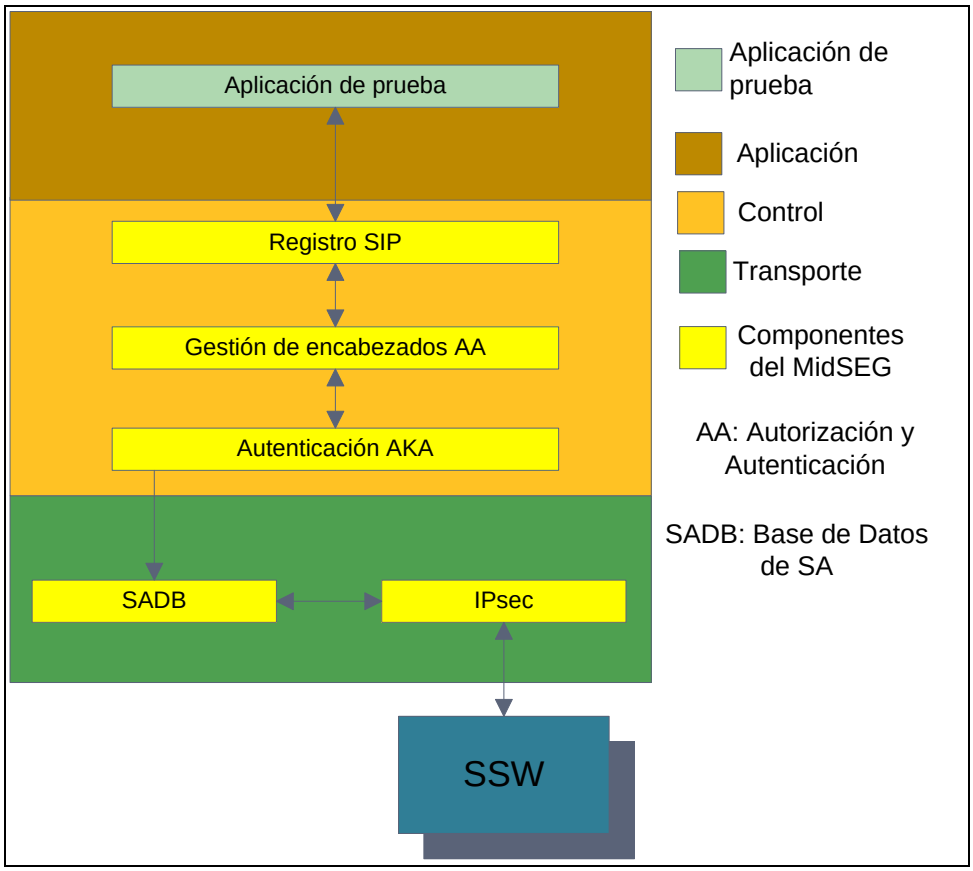

Figura 19. Diagrama de componentes del Subsistema Cliente de Seguridad WLAN-IMS

3.2.1.3.1.2 Componentes del subsistema

Los componentes del subsistema cliente de seguridad WLAN-IMS se encuentran organizados en un modelo NGN.

Capa de Aplicación

- **Aplicación de prueba:** es una aplicación que permite probar el MidSEG, por medio de esta el usuario puede iniciar el procedimiento de registro eligiendo a que dominio quiere acceder, configurando la seguridad que requiere sobre la interfaz de radio. A través de ella MIDSEG informa el estado del proceso de registro.

Capa de Control

- **Registro SIP:** se encarga de retirar y adicionar los encabezados necesarios para el registro, entre los que se encuentran el de autorización, autenticación y de acceso.

- **Gestión de encabezados AA:** construye los encabezados de acceso y autenticación, basándose en la selección de los dominios y en el proceso de autenticación AKA, respectivamente. Además, entrega los parámetros necesarios para ejecutar la autenticación AKA a partir del encabezado SIP de autorización enviado por el S-CSCF y provee las direcciones IP con las cuales el UE se puede comunicar con cada dominio**.**

- **Autenticación AKA:** se encarga de verificar la identidad de la red por medio del mecanismo AKA utilizando un conjunto de algoritmos llamados Milenage los cuales están basados en el estándar de cifrado avanzado (AES, Advanced Encryption Standard), comprueba la integridad del mensaje y la

sincronización con el servidor de autenticación para evitar ataques por replica de paquetes, además genera las llaves de cifrado e integridad, las cuales van a ser usadas en IPsec y una respuesta al desafío utilizando parámetros de seguridad como la llave compartida, un número de secuencia y un número aleatorio encontrado en el desafío.

Capa de Transporte

- **SADB:** aquí se configuran todos los parámetros de IPsec, entre los que se encuentran las direcciones IP de las entidades involucradas en la comunicación, las llaves y las políticas de seguridad que se aplicarán haciendo uso de las SA establecidas.

- **IPsec:** actúa sobre la capa de red permitiendo asegurar las comunicaciones sobre el protocolo IP y capas superiores. De la SADB obtiene las políticas sobre las cuales opera IPsec para proveer confidencialidad e integridad en la comunicación con el SSW.

3.2.1.3.1.3 Interfaces internas

- **Aplicación de prueba – Registro SIP**

Esta interfaz de comunicación permite: iniciar el proceso de registro informando al componente Registro SIP las opciones elegidas y mantener actualizada una interfaz según el estado de registro del cliente.

- **Registro SIP – Gestión de encabezados AA**

Permite al componente Registro SIP solicitar y entregar los encabezados necesarios para el proceso de registro.

- **Gestión de encabezados AA – Autenticación AKA**

Es la interfaz por la cual se transfiere los parámetros de autenticación (RAND, RES, etc.) necesarios para: ejecutar el mecanismo AKA y generar el encabezado de respuesta al desafío.

- **Autenticación AKA – SADB**

Si el registro es exitoso el subsistema utiliza esta interfaz hacia la SADB para configurar los parámetros de IPsec.

- **SADB - IPsec**

Por medio de esta interfaz el componente IPsec obtiene su configuración.

3.2.1.3.1.4 Diagrama de interacción de componentes

En la Figura 20 se muestra el Diagrama de interacción de componentes del Subsistema Cliente de Seguridad WLAN-IMS el cual se describe a continuación:

- La Aplicación de prueba permite al usuario elegir los dominios a los que desea acceder y configurar los parámetros necesarios para realizar la petición de registro pulsando el botón Registrar.
- El SCSWI recibe una solicitud por medio de la Aplicación de prueba y envía los parámetros necesarios para el registro.
- El componente Registro SIP, genera un mensaje SIP REGISTER, al cual se le adicionan los encabezados Realm, AH-Alg y ESP-Alg, obtenidos del componente Gestión de Encabezados AA.
- El componente Registro SIP envía el mensaje al componente IPsec y este al subsistema de seguridad WLAN, en esta parte al tratarse de una primera solicitud de registro el componente IPsec no tiene configurada ninguna política de seguridad ni SA por lo que el mensaje es enviado sin ningún tipo de protección, en caso contrario se aplica la SA asociada a los mensajes de salida hacia el SSW.
- La respuesta por parte del SSW es atendida por el módulo IPsec que aplica las políticas de seguridad actuales para los mensajes de entrada.

- El componente Registro SIP recibe un mensaje SIP 401 No Autorizado del SSW.
- Se retira el encabezado de autenticación del mensaje SIP 401.
- Se aplica el mecanismo AKA, con el cual se deducen las llaves de CK e IK, se validan los datos de autenticación, se autentica la red y se genera la respuesta al desafío.
- Con las llaves de CK e IK generadas, el componente Autenticación AKA actualiza las SA y las políticas de seguridad para el tráfico de registro en la SADB, de esta forma, los mensajes subsecuentes serán enviados de forma segura utilizando IPSec con las nuevas llaves.
- Con la respuesta al desafío se adiciona el encabezado de autenticación al mensaje SIP REGISTER y se envía nuevamente al SSW utilizando la SA IPsec configurada.
- Si el procedimiento de registro fue correcto el subsistema recibe un mensaje SIP 200 OK.
- El mensaje SIP 200 OK informa un registro exitoso, lo cual es notificado al usuario a través de la GUI de prueba. De este mensaje se obtienen las direcciones IP para configurar IPsec y utilizarlo tanto para la protección de la señalización IMS como también para el tráfico con la WLAN o la red 3GPP.

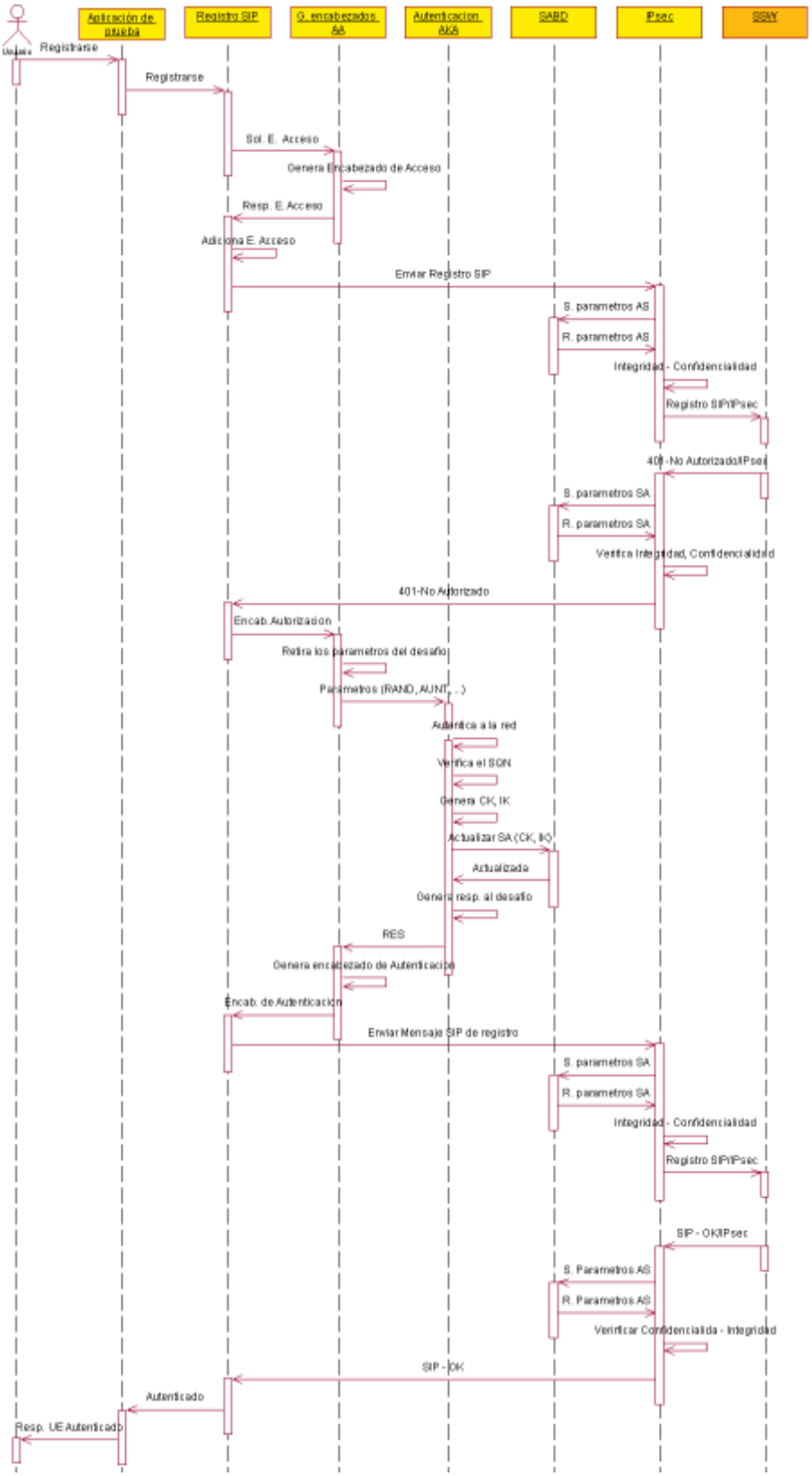

Figura 20. Diagrama de interacción de componentes Subsistema Cliente de Seguridad WLAN-IMS

3.2.1.3.2 Subsistema de Seguridad WLAN

Este subsistema cumple con las funciones:

- Controlar el acceso a los servicios de la WLAN.
- Controlar el acceso a la red IMS.
- Controlar el acceso a la red 3GPP.
- Establecer SA con el SCSWI.
- Establecer SA con el PDG.
- Establecer SA con el SSP.

Para introducir mayor seguridad, lograr mayor eficiencia en el acceso y proteger de usuarios no autorizados, el SSP no es accedido directamente por sus clientes si no a través del SSW. Inicialmente el SSW va ser el encargado de representar a los clientes WLAN ante el SSP para el proceso de registro tal como se ve en la Figura 21. Como resultado de un registro exitoso el SCSWI es representado por el SSW para acceder a los servicios de cada dominio registrado.

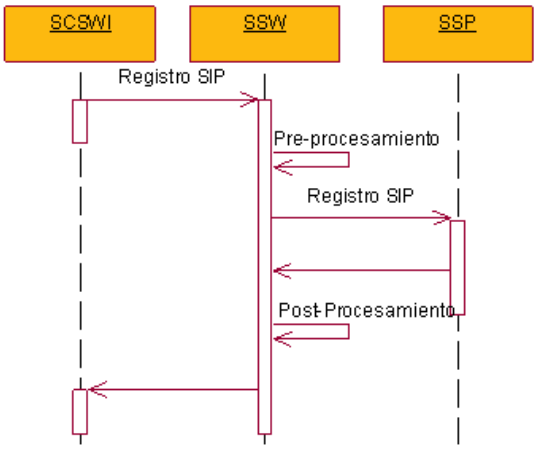

Figura 21. Control de Acceso con los mensajes SIP de registro

3.2.1.3.2.1 Diagrama de Componentes del Subsistema

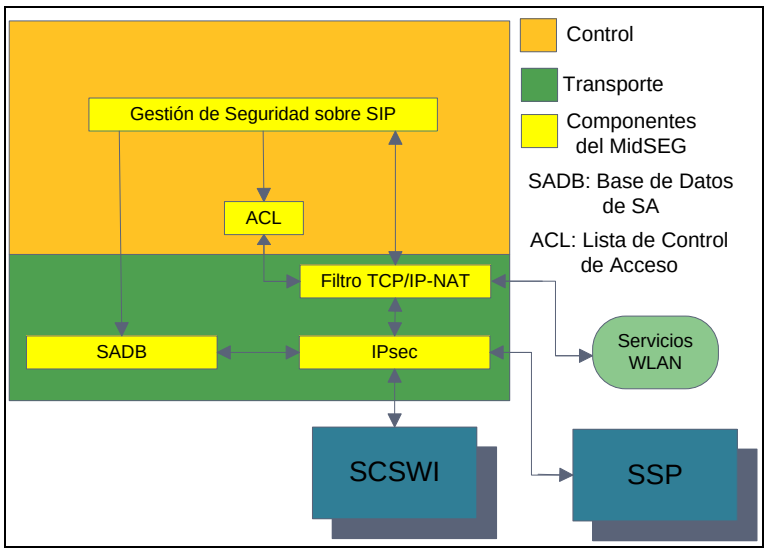

Figura 22. Diagrama de componentes del Subsistema de Seguridad WLAN

3.2.1.3.2.2 Componentes del subsistema

El SSW se divide en los componentes descritos a continuación (ver Figura 22):

Capa de control

- **Gestión de Seguridad sobre SIP:** procesa únicamente los mensajes SIP involucrados en el procedimiento de registro, del mensaje inicial SIP REGISTER obtiene la dirección IP del UE, los algoritmos AH y ESP; del mensaje SIP NO-AUTHORIZATION enviado por el SSP retira las llaves de CK e IK, para luego actualizar la SA IPsec de la señalización de registro; del mensaje SIP OK obtiene la autorización enviada por el SSP para el acceso a los dominios, con esta información configura la ACL y las nuevas SA para cada dominio registrado. Al mensaje SIP OK que será enviado al UE le agrega las direcciones IP con las cuales puede alcanzar los dominios requeridos.

  En el caso de solicitud de un des-registro por parte del usuario, cuando llega la confirmación por parte del SSP con el mensaje SIP OK, configura la ACL para bloquear el tráfico a este usuario, permitiendo solamente mensajes SIP del procedimiento de registro, enviados desde el UE.

  Las SA del último registro exitoso se mantienen hasta obtener las nuevas llaves de CK e IK que permiten establecer nuevas SA, brindando mayor seguridad a las nuevas solicitudes.

- **ACL:** determina los permisos de acceso hacia los dominios WLAN, 3GPP e IMS. Permisos bajo los cuales trabajará el componente denominado Filtro TCP/IP-NAT.

Capa de transporte

- **Filtro TCP/IP–NAT:** su objetivo es filtrar tráfico de acuerdo a la ACL y hacer NAT si es necesario. Para usuarios no registrados, el filtro está configurado para permitir únicamente el tráfico dirigido al puerto por el que escucha la señalización SIP y para usuarios registrados el filtro permite el reenvío de paquetes a los dominios autorizados utilizando el NAT.

- **SADB:** aquí se configuran todos los parámetros de IPsec, entre los que se encuentran las direcciones IP de las entidades involucradas en la comunicación, las llaves y políticas de seguridad que se aplican haciendo uso de las SA establecidas.

- **IPsec:** actúa sobre la capa de red permitiendo asegurar las comunicaciones sobre el protocolo IP estableciendo SA con el SCSWI y el SSP. De la SADB obtiene las políticas sobre las cuales opera IPsec para proveer confidencialidad e integridad en la comunicación.

3.2.1.3.2.3 Interfaces internas

- **Gestión de Seguridad sobre SIP - ACL**

El componente Gestión de Seguridad SIP utiliza esta interfaz para actualizar la ACL luego de un resultado de registro exitoso y también tras la confirmación de un des-registro.

- **Gestión de Seguridad sobre SIP - SADB**

Se utiliza esta interfaz hacia la SADB para configurar los parámetros de IPsec.

- **Gestión de Seguridad sobre SIP - Filtro TCP/IP-NAT**

Interfaz que permite el paso de la señalización SIP entre los componentes Filtro TCP/IP-NAT y Gestión de Seguridad sobre SIP.

- **Filtro TCP/IP-NAT ACL**

Por medio de esta interfaz el componente Filtro TCP/IP-NAT obtiene su configuración.

- **Filtro TCP/IP-NAT - IPsec**

Interfaz de comunicación entre los componentes Filtro TCP/IP-NAT e IPsec, permite al tráfico descifrado dirigirlo al filtro TCP/IP y a los paquetes que necesiten seguridad enviarlos al componente IPsec.

- **SADB - IPsec**

Por medio de esta interfaz el componente IPsec obtiene su configuración.

3.2.1.3.2.4 Diagrama de interacción de componentes

En la Figura 23 se muestra el diagrama de interacción de componentes Subsistema de Seguridad WLAN el cual se describe a continuación:

- El subsistema recibe una solicitud de registro SIP del SCSWI.
- Se aplica el filtro sobre la solicitud de registro SIP.
- Del mensaje SIP REGISTER se obtiene la dirección IP del UE y los algoritmos para los protocolos de seguridad AH y ESP.
- Se re-envía la solicitud de registro hacia el SSP.
- El subsistema de seguridad P-CSCF responde con un mensaje SIP 401 No Autorizado, que indica que el cliente WLAN debe autenticarse.
- Se aplica el filtro y se retiran las llaves de CK e IK necesarias para establecer la SA con el SCSWI.
- Se reenvía el mensaje SIP 401 No Autorizado hacia el cliente WLAN, pero sin las llaves de CK e IK.
- Con las llaves CK e IK se configura las SA en la SADB para asegurar la señalización de registro.
- El SCSWI responde nuevamente con un mensaje SIP de registro el cual contiene la respuesta esperada por la red que permitirá la autenticación del usuario, esta información es recibida de forma segura utilizando la conexión IPsec previamente configurada para la comunicación con el SSP.
- El SSP responde con un mensaje SIP 200 OK, indicando que el cliente WLAN ha sido autenticado correctamente, de este mensaje el subsistema obtiene la autorización de acceso enviada por el SSP del encabezado Realm-Auth.
- Se actualiza la ACL con el fin de permitir el tráfico al usuario para los dominios registrados.
- Configura IPsec para proteger la señalización IMS y la interfaz de radio si el encabezado Realm-Auth así lo indica.
- Se agrega al mensaje SIP 200 OK el encabezado Ip-Realm para indicarle al SCSWI las direcciones IP por las cuales puede acceder a los dominios registrados y luego se reenvía el mensaje hacia el SCSWI.

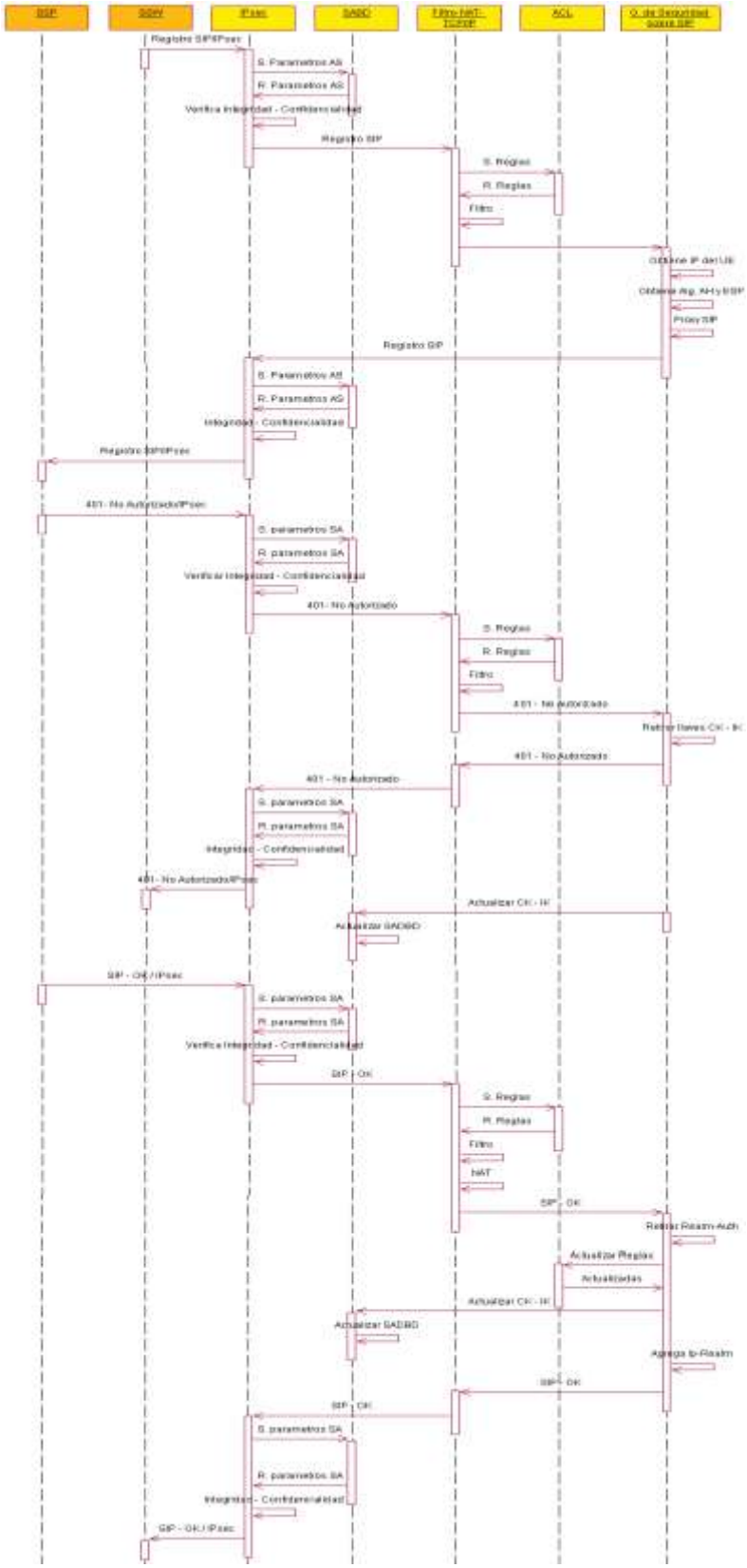

Figura 23 Diagrama de interacción de componentes Subsistema de Seguridad WLAN

3.2.1.3.3 Subsistema de seguridad P-CSCF

Es el punto de entrada al dominio IMS y se encarga de:

- Establecer el control de acceso a los diferentes SSW cuando desean acceder al dominio IMS.
- Procesar los mensajes SIP.
- Mantener temporalmente los dominios a registrar.
- Acceder a la base de datos del HSS para recuperar las llaves de CK e IK que necesita enviarlas al subsistema de seguridad WLAN.
- Actualizar los dominios en los cuales el cliente WLAN fue registrado en la HSS.
- Enviar la autorización de acceso al SSW indicando los dominios registrados.

3.2.1.3.3.1 Diagrama de componentes del subsistema

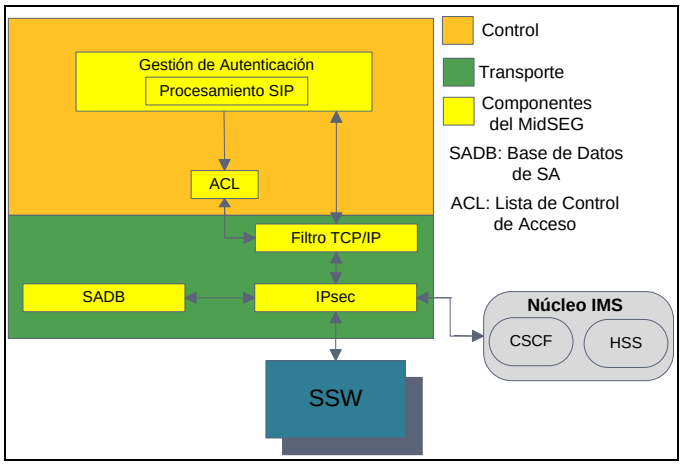

Figura 24. Diagrama de componentes del Subsistema de seguridad P-CSCF

3.2.1.3.3.2 Componentes del subsistema

Capa de control

- **Gestión de Autenticación:** se encarga de gestionar los encabezados SIP adicionales, extrae el encabezado Realm del mensaje SIP de registro para mantener temporalmente los dominios a los cuales el usuario quiere registrarse, adiciona un encabezado con las llaves de CK e IK, las cuales se usan en el túnel IPsec entre el SCSWI y el SSW. Solicita de la HSS las llaves de CK e IK y actualiza los dominios a los que se registró satisfactoriamente el usuario.

- **ACL:** determina los permisos de acceso hacia el dominio IMS, con las cuales trabaja el Filtro TCP/IP.

Capa de Transporte

- **Filtro TCP/IP:** su objetivo es filtrar tráfico de acuerdo a la ACL. La cual se configura para permitir únicamente la comunicación con los SSW con los que se han establecido acuerdos.

- **IPsec:** permite establecer SA con el SSW, con el fin de garantizar confidencialidad e integridad en la comunicación.

- **SADB:** aquí se configuran todos los parámetros de IPsec, entre los que se encuentran las direcciones IP de las entidades involucradas en la comunicación, las llaves y políticas de seguridad que se aplican haciendo uso de las SA establecidas

3.2.1.3.3.3 Interfaces internas

- **Gestión de Autenticación - ACL**

Esta interfaz es utilizada para actualizar la ACL.

- **Gestión de Autenticación - Filtro TCP/IP**

Interfaz que comunica la lógica de control con la parte de transporte.

- **Filtro TCP/IP-NAT - ACL**

Por medio de esta interfaz el componente Filtro TCP/IP-NAT obtiene su configuración.

- **Filtro TCP/IP-NAT - IPsec**

Esta interfaz comunica estos dos componentes, permitiendo que todo el tráfico des-cifrado se dirija al filtro TCP/IP y los paquetes que necesiten seguridad pasen por el componente IPsec.

- **SADB - IPsec**

Por medio de esta interfaz el componente IPsec obtiene su configuración.

3.2.1.3.3.4 Diagrama de interacción de componentes

A continuación se describe el Diagrama de interacción de componentes del Subsistema de seguridad P-CSCF (ver Figura 25):

- El subsistema recibe una solicitud de registro SIP del SSW.
- Aplica las reglas del filtro configuradas en la ACL y sí se trata de un SSW con el cual se han establecido acuerdos se permite el paso de los paquetes.
- El componente Gestión de autenticación extrae el encabezado Realm y guarda temporalmente los dominios a los que el usuario quiere registrarse.
- Se re-envía el registro SIP al núcleo IMS.
- El núcleo IMS responde con un mensaje SIP 401 No autorizado, si el mensaje de registro SIP no tiene el encabezado de autorización correcto.
- Recupera las llaves de CK e IK de la HSS, para adicionarlas al mensaje SIP 401 No Autorizado.
- Se re-envía el mensaje SIP 401 No Autorizado con las llaves hacia el subsistema de seguridad WLAN.
- El SCSWI responde nuevamente con un mensaje SIP de registro el cual contiene la respuesta esperada por la red que permite la autenticación del usuario, esta respuesta es re-enviada al núcleo IMS.
- El núcleo IMS responde con un mensaje SIP 200 OK, si el mensaje de registro SIP contiene la respuesta de autenticación esperada por la red.
- Se actualiza la HSS con el registro de los dominios que el usuario quiere acceder.
- Se borran los dominios solicitados de la base de datos temporal del SSP.
- Se añade el encabezado Realm-Auth con los dominios registrados exitosamente hacia el SSW para que configure su ACL.
- Re-envía el mensaje SIP OK al subsistema de seguridad WLAN.

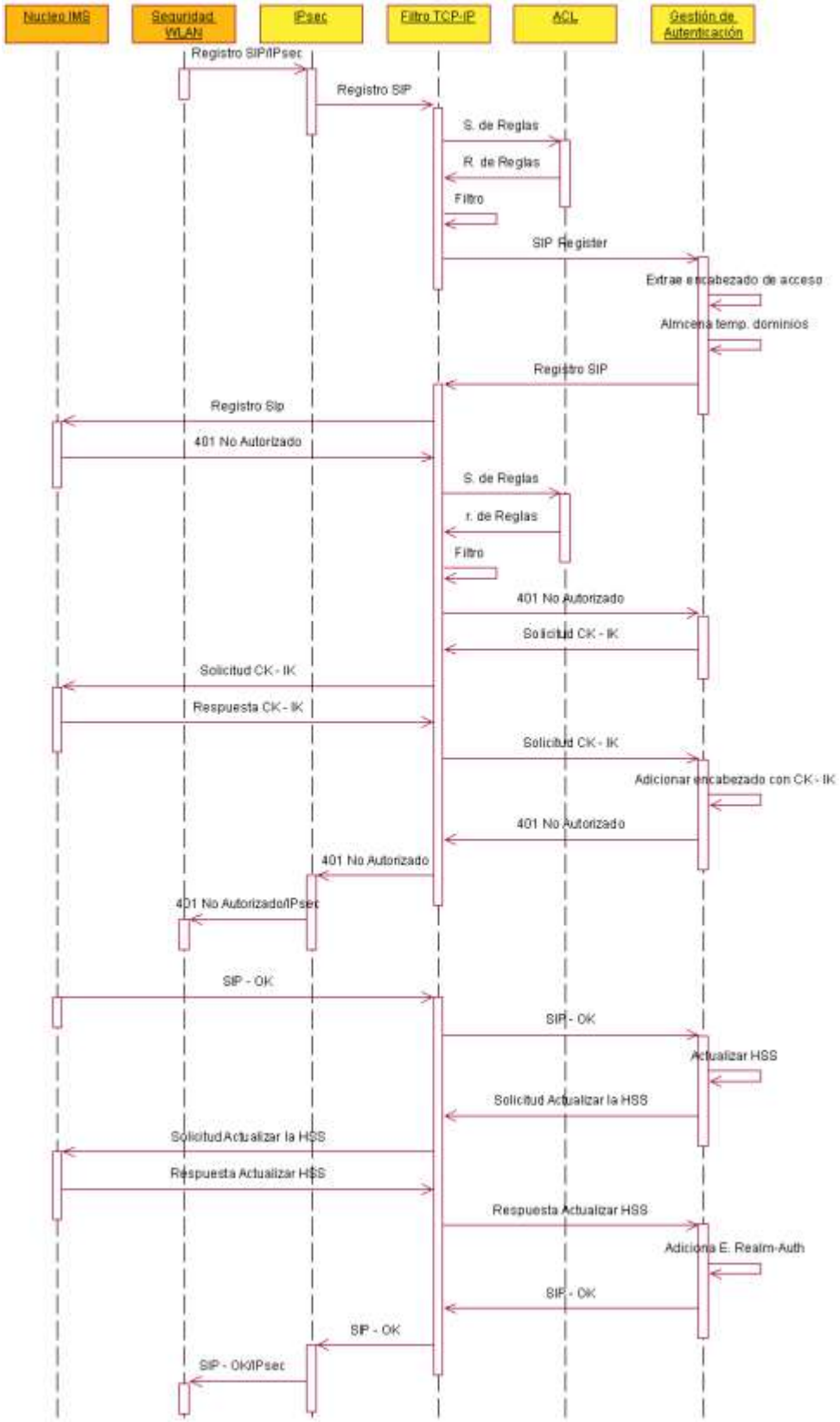

Figura 25. Diagrama de interacción de componentes Subsistema de seguridad P-CSCF

3.3 IMPLEMENTACIÓN DE REFERENCIA

A partir de la arquitectura se realizó la implementación de las funcionalidades principales a lo cual se le denominó implementación de referencia del MidSEG, construida con el fin de evaluar la solución planteada y además servir como orientación a quienes deseen hacer una implementación comercial del MidSEG.

En esta sección se describe la implementación de referencia por subsistemas siguiendo la metodología del Modelo de Construcción de Soluciones [51], para más detalle remítase al Anexo A de esta monografía.

3.3.1 Subsistema de Cliente de Seguridad WLAN-IMS

3.3.1.1 Diagrama de casos de uso del subsistema

Los actores que hacen uso de las funcionalidades del SCSWI son:

- Usuario IMS-WLAN: es la persona que interactúa con la aplicación de prueba instalada sobre UE,él conoce los parámetros de configuración para realizar el registro a IMS, p. Ej: su identidad pública, su identidad privada, dominio al cual pertenece, clave, etc.

- Subsistema de Seguridad WLAN (SSW): subsistema que hace uso de la configuración de seguridad establecida en el equipo de usuario.

Los casos de uso identificados se muestran en la Figura 26.

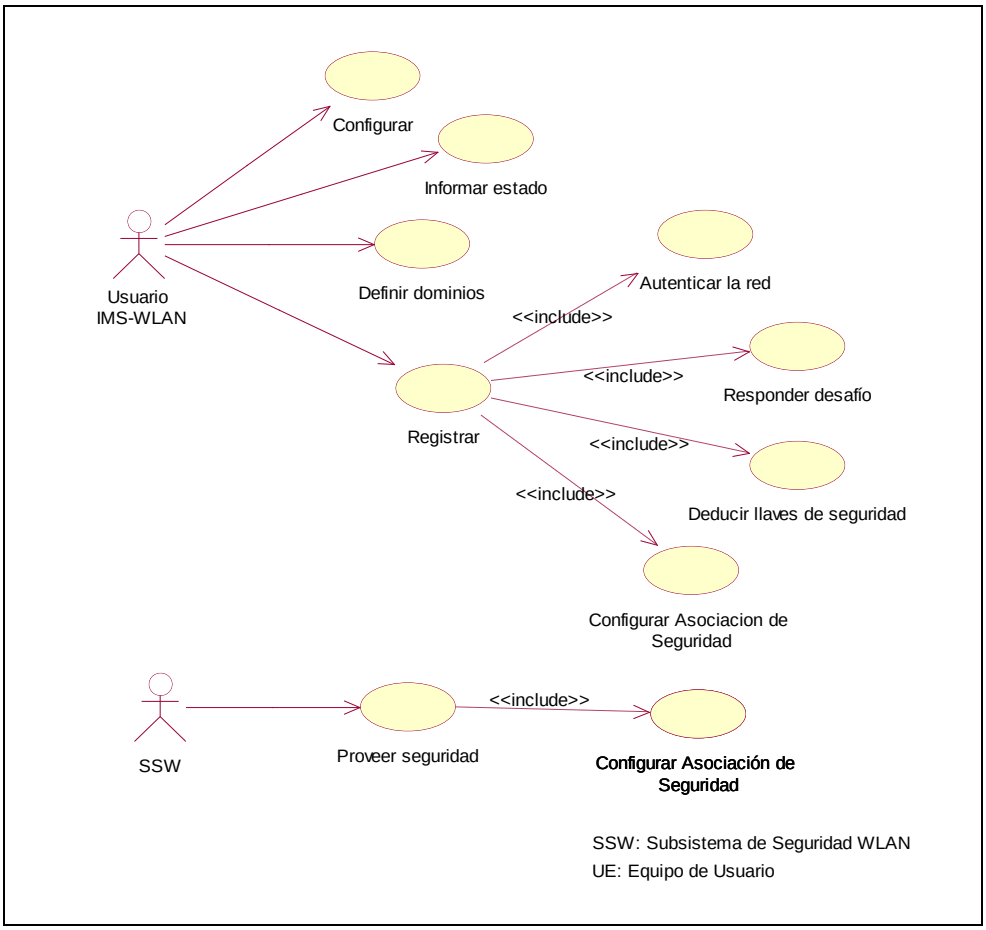

Figura 26. Diagrama de Casos de Uso del SCSWI.

A continuación se describen los casos de uso.

3.3.1.1.1 Casos de Uso Iniciados por el usuario

Caso de uso definir dominios	
Iniciador	Usuario IMS-WLAN
Propósito	Permitir que la aplicación del UE defina los dominios a registrar según la elección del usuario.
Resumen	El usuario elige en la interfaz gráfica de la Aplicación del UE los dominios a registrar WLAN o IMS, estos dominios son configurados en el SCSWI.

Caso de uso configurar	
Iniciador	Usuario IMS-WLAN
Propósito	Permitir que la aplicación del UE configure los parámetros necesarios para el registro IMS-WLAN ingresados por el usuario.
Resumen	El usuario configura datos necesarios para hacer el registro en la Aplicación del UE: identidad pública, identidad privada, clave secreta, dominio de red al cual pertenece, algoritmos de seguridad a utilizar para la protección de la interfaz de radio, etc. Esta información es configurada por la aplicación del UE en el SCSWI.

Caso de uso informar estado	
Iniciador	Usuario IMS-WLAN
Propósito	Permitir que la aplicación del UE informe al usuario el estado del registro.
Resumen	La aplicación del UE extrae del SCSWI el estado del proceso de registro para mostrarlo en la interfaz gráfica. Los estados definidos en el SCSWI son: sin registro, registrado, en proceso y error por tiempo excedido.

Caso de uso registrar	
Iniciador	Usuario IMS-WLAN
Propósito	Realizar el registro del usuario al dominio solicitado (IMS o WLAN) y establecer una comunicación segura con los dominios requeridos.
Resumen	El usuario al momento que elige la opción registrar en la interfaz gráfica de la aplicación del UE inicia el procedimiento de registro que incluye la autenticación de la red, la generación de la respuesta al desafío para su autenticación y la deducción de las llaves de seguridad con las que el SCSWI configura la comunicación segura.

3.3.1.1.2 Casos de Uso Iniciados por el SSW

Caso de uso proveer seguridad	
Iniciador	SSW
Propósito	Proveer confidencialidad e integridad en la comunicación manejada con el SSW.
Resumen	El SSW solicita una respuesta de señalización SIP, cada una de estas solicitudes son respondidas a través de un canal de comunicación seguro, donde se garantiza la confidencialidad e integridad de la información.

3.3.1.2 Diagrama de paquetes de análisis del subsistema

Los paquetes de análisis para el SCSWI son los siguientes:

Aplicación: este paquete contiene a la aplicación de prueba, la cual básicamente consiste en la interface de usuario que permite la configuración del SCSWI y mantiene informado al usuario del proceso ejecutado por MIDSeg. Es importante aclarar que este paquete no forma parte del MidSEG y que es implementado como herramienta de prueba. Este paquete sirve como referencia para las aplicaciones que pretendan hacer uso de MidSEG.

Control: contiene las clases de los componentes del SCSWI presentes en la capa de control de la Arquitectura de Referencia (sección 3.2.1.3.1.1):

- Registro SIP. Maneja la comunicación SIP. Permite el envío de mensajes SIP REGISTER, procesamiento de mensajes SIP NO-AUTHORIZATION y envío de SIP OK.
- Gestión de encabezados AA. Hace referencia al manejo de encabezados sobre la señalización SIP para gestionar la Autorización y Autenticación.
- Autenticación AKA. Utiliza el algoritmo AKA para generar la respuesta de autenticación y obtener las llaves CK e IK, con las que se realiza la configuración de IPsec.

Transporte: hace referencia a la configuración realizada sobre la herramienta de IPsec utilizada sobre el Sistema Operativo (SO), se implementan los componentes:

- IPsec. Para definir las asociaciones de seguridad IPsec.
- SADB. Para definir las políticas de seguridad IPsec que se aplican al tráfico IP, las cuales hacen uso de las asociaciones de seguridad establecidas en el componente IPsec.

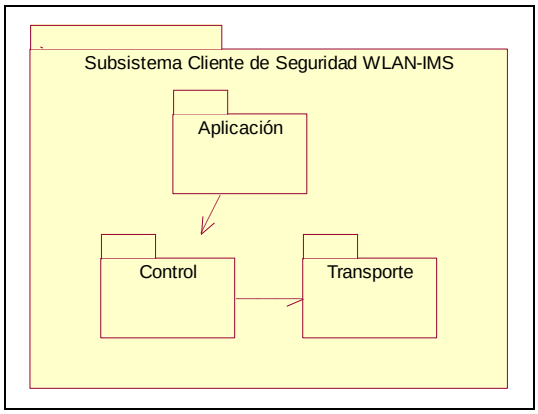

Figura 27. Paquetes de Análisis del Subsistema Cliente de Seguridad WLAN-IMS

3.3.1.3 Diagrama de paquetes de diseño del subsistema

El diagrama de paquetes de diseño del SCSWI se muestra en la Figura 28, indicando las herramientas y librerías que se utilizaron para la implementación de cada paquete:

Aplicación: para la implementación de las interfaces graficas de la aplicación se usó la librería AWT incluida dentro de las librerías de Java [52].

Control: la lógica de control del SCSWI fue realizada a partir de la señalización SIP para su implementación se utilizó el Api Jain-SIP 1.2 [53].

Transporte: la seguridad fue provista en la capa de transporte, su soporte lo dio la herramienta IPsec-tools R0.7.1 [54]. Esta herramienta fue gestionada desde Java.

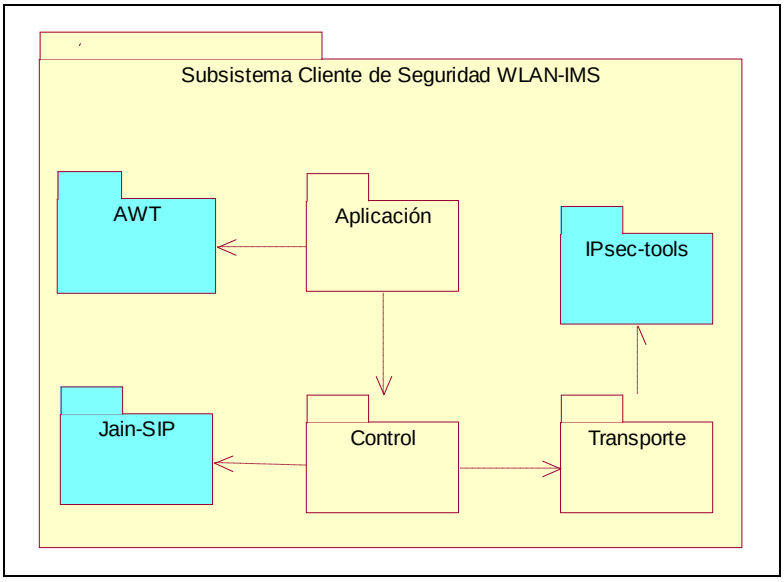

Figura 28. Diagrama de Paquetes de Diseño del SCSWI.

3.3.2 Subsistema de Seguridad WLAN

3.3.2.1 Diagrama de casos de uso del subsistema

Los actores que hacen uso de las funcionalidades del SSW son:

- SCSWI: subsistema que hace uso de la configuración de seguridad establecida con el SSW para acceder a los dominios WLAN e IMS.
- SSP: subsistema que a través de una comunicación segura informa al SSW de los resultados del registro de usuario para la configuración del filtro de acceso y la configuración de IPsec.
- Operador WLAN: entidad encargada de la gestión del SSW.

Los casos de uso identificados para el SSW se muestran en la Figura 29

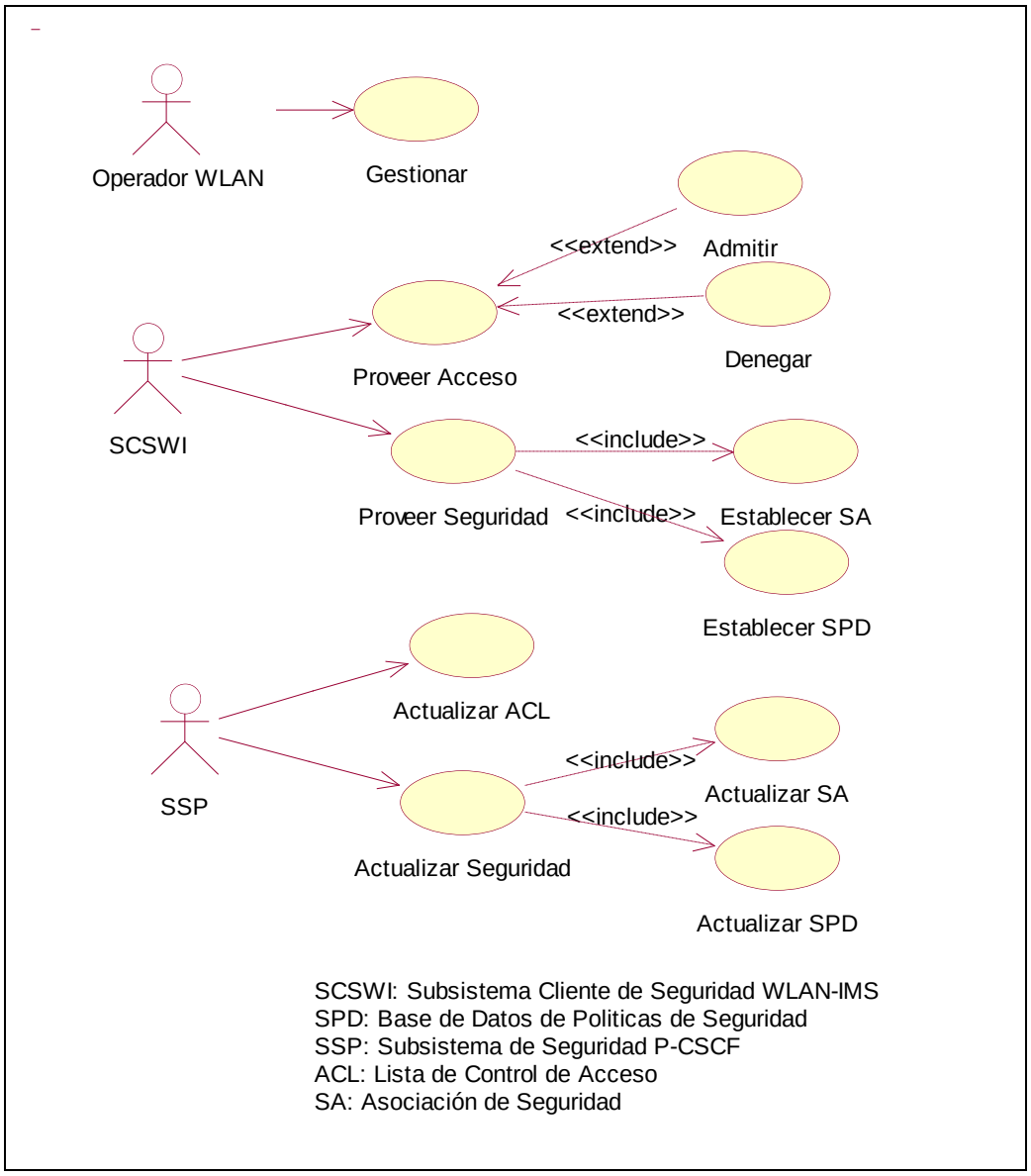

Figura 29. Diagrama de casos de uso del SSW.

A continuación se describen los escenarios de cada caso de uso para el subsistema SSW

3.3.2.1.1 Casos de uso iniciados por el operador WLAN

Caso de uso gestionar	
Iniciador	Operador WLAN
Propósito	Permitir a la entidad responsable de la red WLAN configurar el SSW.
Resumen	El responsable de la red WLAN configura el SSW para comunicarse con un SSP el cual proveerá la información de control de acceso a los dominios WLAN e IMS, esta gestión también hace referencia al proceso de iniciar y parar el servidor.

3.3.2.1.2 Casos de uso iniciados por el SCSWI

Caso de uso proveer acceso	
Iniciador	SCSWI
Propósito	Permitir al SCSWI acceder a los servicios de la WLAN o de IMS.
Resumen	Cuando llega una solicitud de acceso (a uno de los dominios IMS o WLAN) desde el SCSWI, el SSW aplica las reglas contenidas en la ACL.

Caso de uso proveer seguridad	
Iniciador	SCSWI
Propósito	Proveer confidencialidad e integridad en la comunicación manejada con el SCSWI.
Resumen	El SCSWI solicita una respuesta de señalización SIP, cada una de estas solicitudes son respondidas a través de un canal de comunicación seguro, donde se garantiza la confidencialidad e integridad de la información.

3.3.2.1.3 Casos de uso iniciados por el SSP

Caso de uso actualizar seguridad	
Iniciador	SSP
Propósito	Permitir la configuración dinámica de la comunicación IPsec entre el SSW y el SCSWI.
Resumen	Tras el envío de confirmación de un registro exitoso por parte del SSP se realiza la configuración dinámica de unas nuevas SA para la comunicación con el SCSWI. En esta configuración se renuevan las SA para el tráfico de registro manejado por el MidSEG, las SA para la señalización de IMS y las SA para la protección de la interfaz de radio.

Caso de uso actualizar ACL	
Iniciador	SSP
Propósito	Permitir la configuración dinámica del filtro de control de acceso.
Resumen	Tras el envío de confirmación de un registro exitoso por parte del SSP se realiza la configuración dinámica de las reglas del filtro.

3.3.2.2 Diagrama de paquetes de análisis del subsistema

Los paquetes de análisis para el SSW son los siguientes (ver Figura 30):

Control: contiene las clases de los componentes del SSW presentes en la capa de control de la Arquitectura de Referencia (sección 3.2.1.3.2.1):

- Gestión de Seguridad sobre SIP. Se encarga de atender los eventos de la comunicación SIP, realiza la configuración de IPsec y del filtro para el control de acceso a los dominios, almacena temporalmente los parámetros de configuración de seguridad para la protección de la interfaz de radio y también guarda el registro de las SA asociadas a un determinado usuario.
- ACL. Permite la definición de las reglas para el control de acceso sobre el filtro TCP.

Transporte: hace referencia a la configuración sobre las herramientas IPsec, filtro y NAT utilizadas sobre el Sistema Operativo (SO), se implementan los componentes:

- Filtro TCP/IP-NAT. En él se aplican las reglas de control de acceso y de NAT para el tratamiento del trafico IP.
- IPsec. Para definir las asociaciones de seguridad IPsec.
- SADB. Para definir las políticas de seguridad IPsec que se aplican al tráfico IP, las cuales hacen uso de las asociaciones de seguridad establecidas en el componente IPsec.

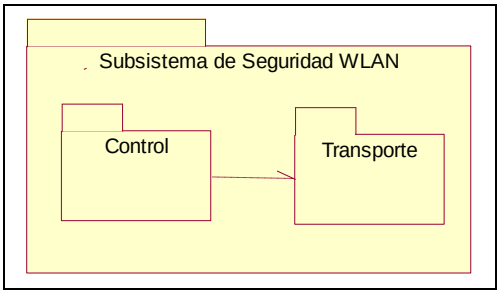

Figura 30. Diagrama de Paquetes de Análisis del SSW

3.3.2.3 Diagrama de paquetes de diseño del subsistema

El diagrama de paquetes de diseño del SSW se muestra en la Figura 31, indicando las herramientas y librerías que se utilizaron para la implementación de cada paquete:

Control: la lógica de control del SSW fue realizada a partir de la señalización SIP para su implementación se utilizó el Api Jain-SIP 1.2 [53], de su lógica de funcionamiento también hizo parte la persistencia temporal de algunos datos de registro para ello se utilizo una base de datos montada en mysql-server 5.0.51a [55], La cual fue accedida gracias a la librería java mysql-connector-java-3.1.12-bin [56].

Transporte: la seguridad y el control de acceso fueron provistos en la capa de transporte. Para ello se utilizo la herramienta IPsec-tools R0.7.1 [54] e IP-tables 1.3.8 [57] respectivamente, ambos gestionados desde Java.

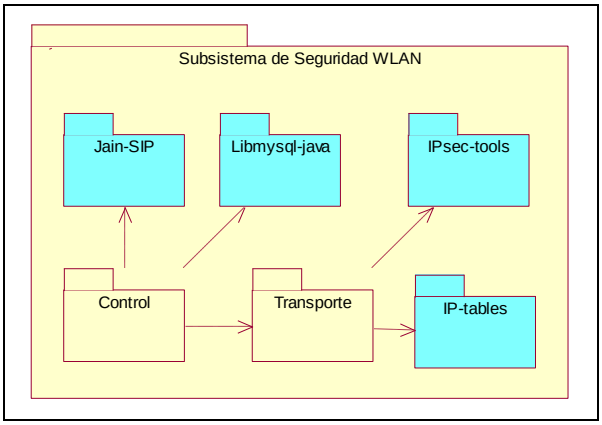

Figura 31. Diagrama de Diseño del SSW

3.3.3 Subsistema de Seguridad P-CSCF

3.3.3.1 Diagrama de casos de uso del subsistema

Los actores que hacen uso de las funcionalidades del SSP son:

- SSW: subsistema que hace uso de la configuración de seguridad establecida con el SSP para la realización del registro de usuarios y para la prestación de servicios IMS.

- Operador IMS: entidad encargada de la gestión del SSP.

Los casos de uso identificados para el SSP se muestran en la Figura 29.

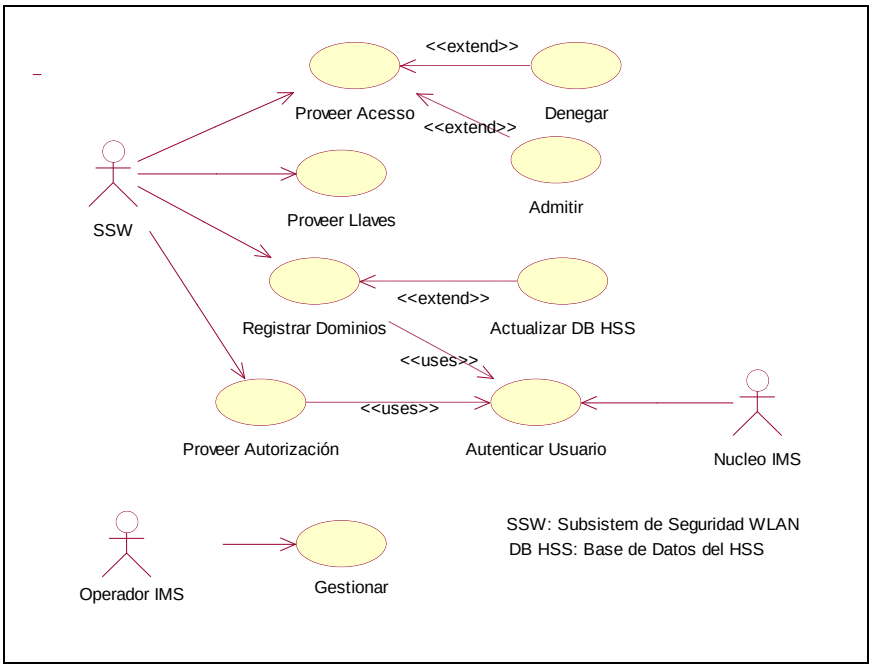

Figura 32. Diagrama de Casos de Uso del SSP.

A continuación se describen los escenarios de cada caso de uso del subsistema SSP

3.3.3.1.1 Casos de uso iniciados por el SSW

Caso de uso proveer acceso	
Iniciador	SSW
Propósito	Permitir que un usuario acceda a los servicios IMS a través de un SSW.
Resumen	El SSW envía una solicitud de acceso a los servicios IMS representando a un usuario, si el SSP está configurado para permitir que ese SSW ofrezca servicios de IMS le permite el acceso.

Caso de uso proveer llaves	
Iniciador	SSW
Propósito	Proveer al SSW las llaves Ck e Ik para la configuración dinámica de IPsec con el SCSWI.

Resumen	El SSP extrae del HSS las llaves de seguridad CK e IK, estas son enviadas sobre SIP al SSW para la configuración dinámica de IPsec con el SCSWI.

Caso de uso registrar dominios	
Iniciador	SSW
Propósito	Realizar el registro de un usuario a los dominios especificados, haciendo uso de la autenticación suministrada por el núcleo IMS.
Resumen	Tras la autenticación realizada por el núcleo IMS el SSP registra los dominios solicitados por el usuario en la HSS.

Caso de uso proveer autorización	
Iniciador	SSW
Propósito	Enviar la autorización de acceso al SSW de un usuario a los dominios especificados, haciendo uso de la autenticación suministrada por el núcleo IMS.
Resumen	Tras la autenticación realizada por el núcleo IMS el SSP envía al SSW la autorización de acceso a los dominios solicitados por el usuario.

3.3.3.1.2 Casos de uso iniciados por el operador IMS

Caso de uso gestionar	
Iniciador	Operador IMS
Propósito	Permitir a la entidad responsable del dominio IMS configurar el SSP.
Resumen	El responsable de la red IMS configura el SSP para comunicarse con el P-CSCF de la red IMS con el fin de permitir el uso de sus servicios desde una determinada WLAN, esta gestión también hace referencia al proceso de iniciar y parar el servidor.

3.3.3.2 Diagrama de paquetes de análisis del subsistema

Los paquetes de análisis para el SSP son los siguientes (ver Figura 33):

Control: contiene las clases de los componentes del SSP presentes en la capa de control de la Arquitectura de Referencia (sección 3.2.1.3.3.1):

Gestión de Autenticación. Se encarga de atender los eventos de la comunicación SIP, una vez el usuario se ha autenticado realiza: el registro a los dominios sobre el HSS, envía la autorización y las llaves para que el SSW configure las asociaciones de seguridad IPsec con el SCSW.

ACL. Permite la definición de las reglas para el control de acceso sobre el filtro TCP/IP.

Transporte: hace referencia a la configuración sobre las herramientas IPsec y filtro utilizadas sobre el Sistema Operativo (SO), se implementan los componentes:

- Filtro TCP/IP-NAT. En él se aplican las reglas de control de acceso para el tratamiento del tráfico IP.

- IPsec. Para definir las asociaciones de seguridad IPsec.
- SADB. Para definir las políticas de seguridad IPsec que se aplican al tráfico IP, las cuales hacen uso de las asociaciones de seguridad establecidas en el componente IPsec.

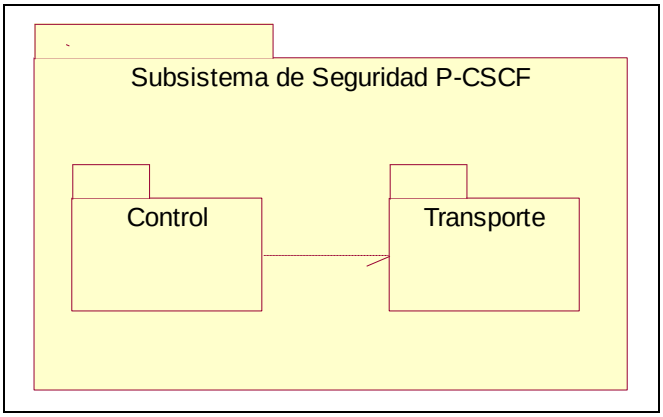

Figura 33. Diagrama de Paquetes de Análisis del SSP

3.3.3.3 Diagrama de paquetes de diseño del subsistema

El diagrama de diseño del SSP se muestra en la Figura 34, indicando las herramientas y librerías que se utilizaron para la implementación de cada paquete:

Control: la lógica de control del SSP fue realizada a partir de la señalización SIP para su implementación se utilizó el Api Jain-SIP 1.2 [53], de su lógica de funcionamiento también hizo parte el acceso a la base de datos montada sobre mysql-server 5.0.51a [55] de la HSS la cual fue accedida gracias a la librería de Java mysql-connector-java-3.1.12-bin [56].

Transporte: la seguridad y el control de acceso fueron provistos en la capa de transporte. Para ello se utilizó la herramienta IPsec-tools R0.7.1 [54] y IP-tables 1.3.8 [57] respectivamente, ambos gestionados desde Java.

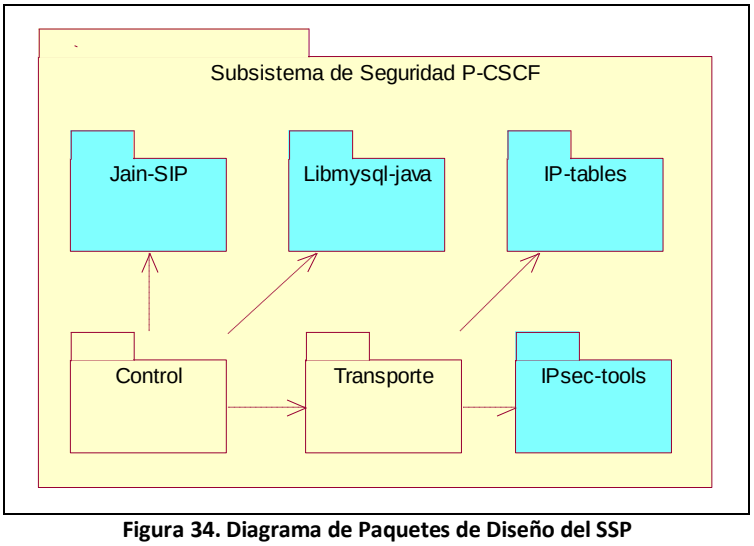

Figura 34. Diagrama de Paquetes de Diseño del SSP

3.4 Modelo de Implantación

En la Figura 35 se representa el modelo de implantación de referencia para el sistema:

- Usuario, el cual conoce la llave compartida y la configuración necesaria para acceder a la red IMS que gestiona su registro a los dominios de red.

- Equipo de Usuario (UE) con las siguientes características: SO Ubuntu 8.04, jdk-1.6, ipsec-tools R0.7.1, jain-sip 1.2, SCSWI y tarjeta inalámbrica para la conexión WLAN.

- Access Point, punto de acceso WLAN que permite la conexión inalámbrica con el UE, esta conexión puede estar asegurada con algún protocolo de seguridad propio de WiFi, se realizaron pruebas con un AP Linksys modelo WAP54G utilizando WEP, WPA y sin seguridad.

- Servidor Middleware de Seguridad WLAN, equipo de red con las siguientes características: SO Ubuntu 8.04, jdk-1.6, ipsec-tools R0.7.1, ip-tables 1.3.8, jain-sip 1.2, mysql-connector-java-3.1.12-bin, mysql-server 5.0.51a, SSW y con tres interfaces de comunicación. Es el único camino físico que tiene el AP para alcanzar los servicios de la WLAN e IMS.

- IPv4: nube que representa las redes IP que se encuentran entre IMS-WLAN. Correspondió a la red interna que tiene la Universidad del Cauca junto con su conexión a Internet.

- Servidor Middleware de Seguridad P-CSCF, equipo de red con las siguientes características SO Kubuntu 8.04, jdk-1.6, ipsec-tools R0.7.1, ip-tables 1.3.8, racoon, jain-sip 1.2, mysql-connector-java-3.1.12-bin, SSP y con dos interfaces de comunicación. Es el único camino por el cual un SMSW puede alcanzar el núcleo IMS.

- Red IMS, compuesta principalmente por el CSCF, el HSS y un servidor de nombres de dominio (DNS). Estos componentes son simulados sobre un único servidor con las siguientes características: SO Kubuntu 8.04, jdk-1.6, ipsec-tools R0.7.1, racoon, mysql-server 5.0.51a, bind9 1:9.4.2, OpenIMSCoreKDE2008-12-08.r608 y con una interfaz de comunicación.

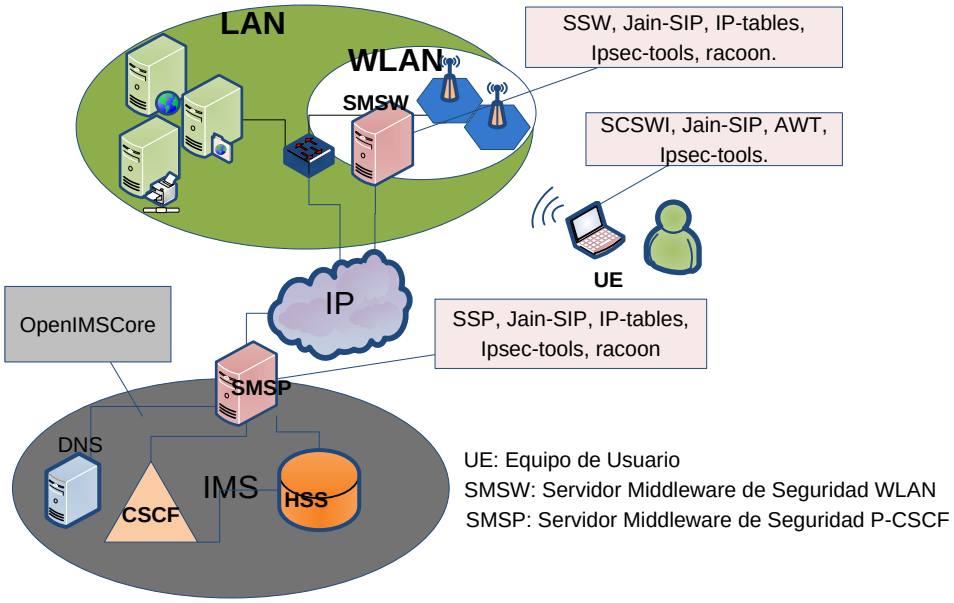

Figura 35. Modelo de Implantación del Sistema

3.5 EVALUACIÓN DE SEGURIDAD

Para realizar este proceso se siguió la metodología OSSTMM (Open-Source Security Testing Methodology Manual) [58], la cual nos permitió confrontar el diseño de los requerimientos de seguridad planteados en la sección 3.1.2 con las posibles vulnerabilidades definidas antes del diseño.
Los criterios seguidos para este proceso se presentan en la Figura 36, los cuales fueron adaptados de los criterios establecidos para un plan de pruebas de la tesis que sigue la metodología OSSTMM "*criterios para establecer políticas de seguridad de la información y plan de contingencia, caso de estudio el centro de datos de la Universidad del Cauca",* desarrollada por Carolina Guevara Campo y Fabián Andrés Mera, y dirigida por el Ingeniero Siler Amador [59].

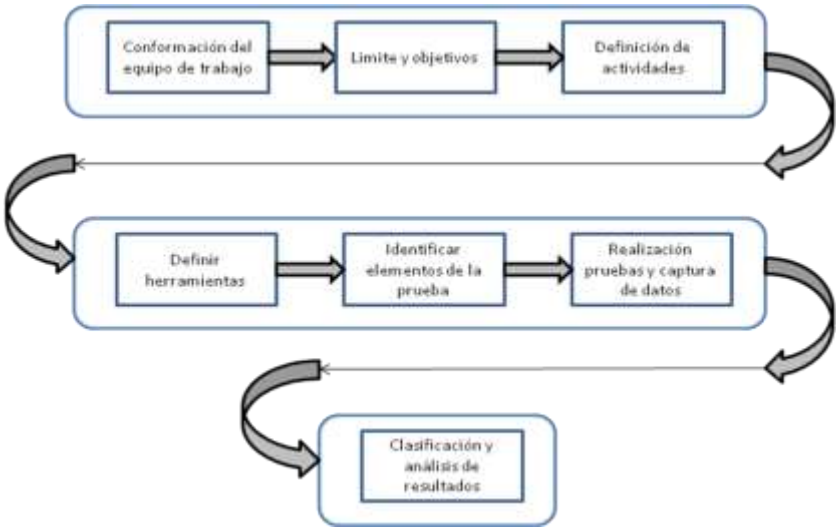

Figura 36. Criterios para la evaluación de MidSEG

La Figura 36 muestra el flujo seguido para la evaluación de MidSEG:

1. Determinación del equipo de trabajo para revisar las pruebas,
2. Definición del límite y alcance de las pruebas, donde se delimita los objetivos y se plantea la topología aproximada de la red objeto de estudio.
3. Definición de las actividades a realizar.
4. Definición de las herramientas necesarias para llevar a cabo las pruebas
5. Identificación de los equipos y elementos a los cuales se realizaran las pruebas
6. Realización de las pruebas y consignación de los datos y análisis de estos.

3.5.1 Equipo de Trabajo

Para la ejecución de las pruebas de seguridad se cuenta con:

- 2 desarrolladores: encargados de definir, realizar y analizar las pruebas.
- 1 asesor: encargado de verificar el cumplimiento de las pruebas.

3.5.2 Definir límite y objetivos

Teniendo en cuenta que el objetivo a evaluar es la implementación de referencia de MidSEG, comprobando los requisitos funcionales definidos en 3.1.2.1 para el acceso a servicios IMS desde una red 802.11, se plantea un laboratorio de prueba con el fin de delimitar las máquinas que se van a evaluar y el ambiente en

el que se encuentran. De esta forma, se creó un ambiente conformado por el núcleo IMS, el MidSEG, la red de acceso WiFi, un cliente y un atacante, como se puede ver en la Figura 37.

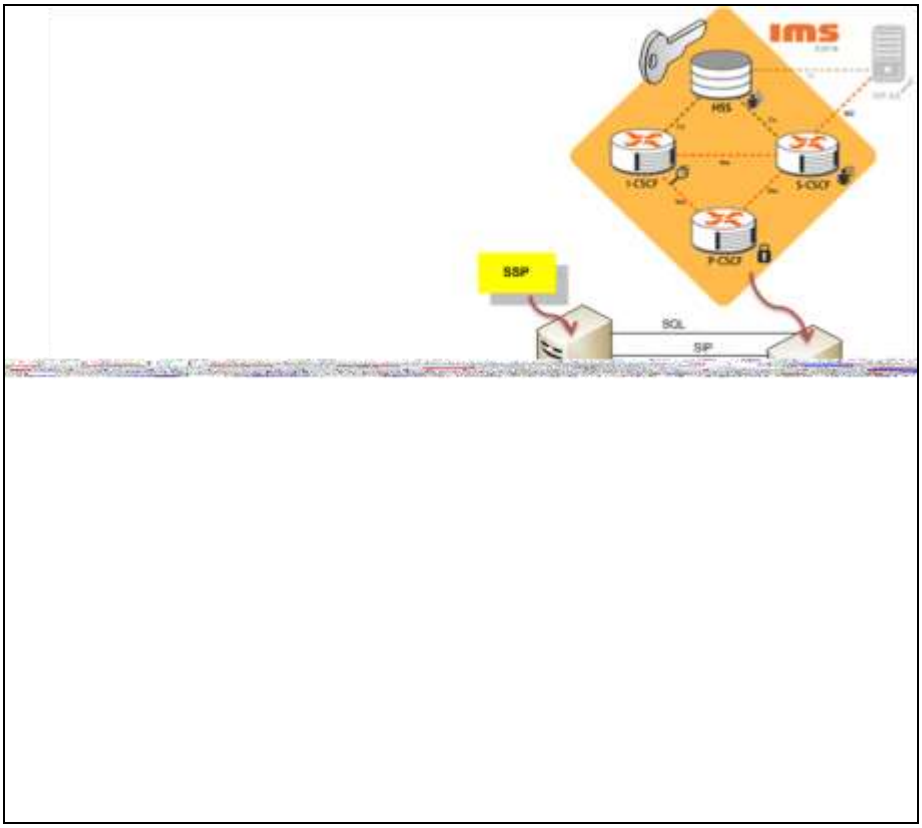

Figura 37. Ambiente de evaluación de MidSEG

- **Dominios:** para el ambiente de prueba se utilizaron los dominios de la Tabla 5, los cuales son considerados como privados.

Tabla 5. Dominios

Dominio	Red	Mascara de Red
WLAN	172.17.0.0	255.255.0.0
Servicios WLAN	10.0.0.0	255.0.0.0
IMS	192.168.2.0	255.255.255.0

- **Servidores:**

  Servidor Middleware de Seguridad WLAN (SMSW): este equipo posee tres interfaces de red (ver Tabla 6) necesarias para alcanzar los diferentes dominios, en este se ejecuta el SSW.

Tabla 6. Interfaces SMSW

Interfaz	Dirección	Descripción
1.	172.17.12.1	Es la puerta de enlace para los usuarios de la WLAN.
2.	10.200.2.203	Permite acceder a los servicios de la WLAN.

3.	192.168.30.203	Permite acceder a IMS

Servidor Middleware de Seguridad P-CSCF (SMSP): es el punto de entrada al núcleo IMS, posee 2 interfaces de red (ver Tabla 7) y en este se ejecuta el SSP.

Tabla 7. Interfaces SMSP

Interfaz	Dirección	Descripción
1.	192.168.2.1	Es la puerta de enlace para el núcleo IMS.
2.	192.168.30.99	Es el punto de entrada y salida del núcleo IMS.

Servidor Núcleo IMS: en este se encuentra el núcleo de IMS (P-CSCF, I-CSCF, S-CSCF y HSS), por limitaciones de recursos todos se encuentran instalados en un mismo equipo el cual posee una interfaz de red (ver Tabla 8).

Tabla 8. Interfaz Servidor Núcleo IMS

Interfaz	Dirección	Descripción
1.	192.168.2.99	Es la dirección IP del servidor.

- **Cliente:**
  UE: el equipo de usuario utilizado es un portátil, ejecutando al SCSWI. Utiliza una tarjeta inalámbrica para acceder a la red 802.11.

Tabla 9. Interfaz cliente WLAN

Interfaz	Dirección	Descripción
1.	172.17.12.12	Dirección IP del cliente.

3.5.3 Actividades a realizar

- Verificar el funcionamiento de los subsistemas SSW, SSP.
- Creación de contraseñas seguras en los servidores.
- Verificar firewall, mecanismos de protección, puertos y servicios que se tienen bloqueados o autorizados.
- Verificar políticas referentes a la señalización SIP entre el UE y el P-CSCF.

3.5.4 Definir Herramientas

Las herramientas utilizadas para las pruebas son:

- Wireshark es un analizador de protocolos de red, permite examinar de forma detallada la información de los paquetes capturados [60].

- John the ripper, su principal propósito es encontrar contraseñas débiles de Linux utilizando los archivos donde se encuentran cifradas (passwd y shadow). Para lograrlo se puede usar diccionarios o un modo incremental [61].

- Nmap es una herramienta diseñada para realizar exploración y auditorías de seguridad en una red. Permite determinar equipos, servicios y sistemas operativos que se ejecutan en una maquina remota [62].

- CommView for WiFi es una herramienta para monitorear redes inalámbricas 802.11 a/b/g/n. Para poder utilizarlo se debe tener una tarjeta compatible con el controlador de este producto, en este caso se utilizo una tarjeta PCI marca D-Link de referencia AirXpert DWL-AG520 [63].

3.5.5 Identificar elementos de la prueba

Las pruebas son realizadas sobre los elementos y comunicaciones entre: SMSW, SMSP y UE.

3.5.6 Realización de las pruebas, captura de datos y análisis

- ***Prueba: Controlar el acceso de paquetes a los dominios WLAN e IMS.***

  Número de pruebas realizadas: 4.

  a. Comprobar, que un usuario no registrado no puede acceder a los servicios de la WLAN o IMS.

     Si un usuario no registrado desea acceder a Internet desde la WLAN a IMS no lo puede hacer, porque el firewall configurado con iptables se lo impide, ya que el reenvió de paquetes por defecto tiene la política de denegar todos los paquetes (ver Figura 38).

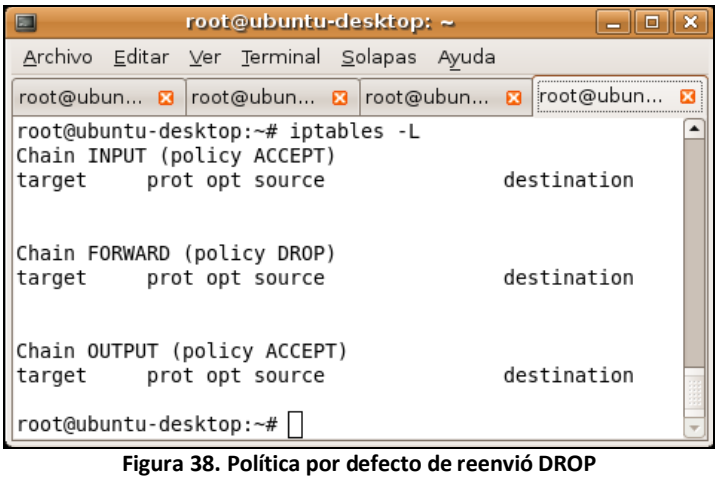

Figura 38. Política por defecto de reenvió DROP

Se verifica haciendo un ping a la dirección IP 10.200.2.254, cuando el cliente de la WLAN no está registrado. En la Figura 39 se puede ver que de 21 solicitudes ICMP no hay ninguna respuesta debido a que todos los paquetes son rechazados por el SSW.

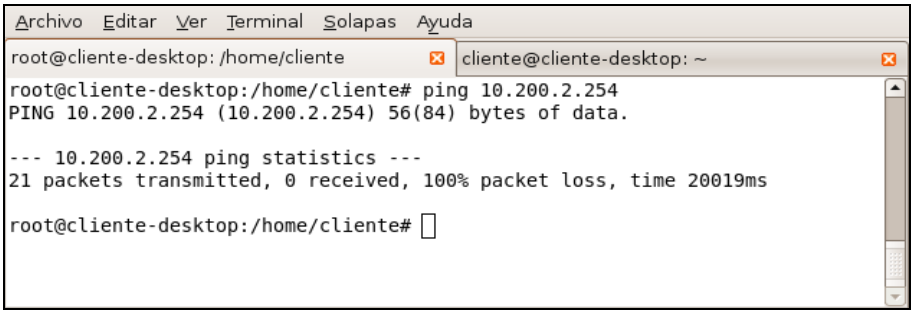

Figura 39. Prueba ICMP cuando el cliente no está registrado.

b. Si el usuario se registra exitosamente a la WLAN el firewall se modifica automáticamente, permitiendo acceder a los servicios de la WLAN pero no a IMS. En la Figura 40 se puede ver como las políticas de reenvió del firewall permiten pasar el trafico del cliente 172.17.12.12 hacia los servicios de la WLAN y no hacia la dirección 192.168.30.99, la cual es el punto de entrada al dominio IMS.

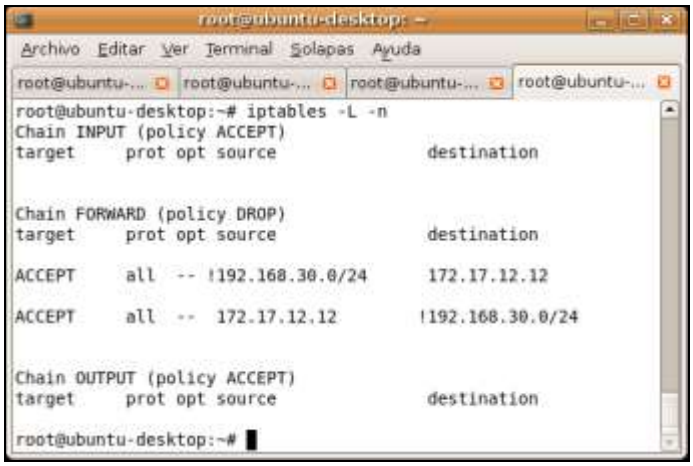

Figura 40. Firewall después de un registro exitoso a la WLAN

Después de haberse registrado el cliente WLAN, puede hacer ping a la dirección IP 10.200.2.254, logrando respuesta como se puede ver en la Figura 41.

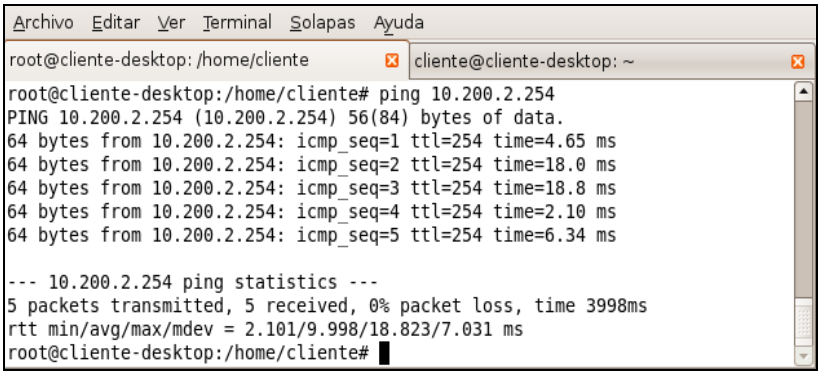

Figura 41. Prueba ICMP cuando el cliente está registrado a la WLAN

Si un atacante utiliza la dirección IP de un usuario registrado, este no podrá acceder a las autorizaciones otorgadas al cliente WLAN, debido a que existe un túnel IPsec entre el cliente WLAN y el SSW por lo que a cada paquete que llegue al SSW se le verifica su integridad y confidencialidad con las respectivas SA. Para que el atacante tenga éxito debería conocer las SA, las cuales cambian con cada registro.

Si se tuviera solo las políticas del firewall y no las SA, un usuario sólo con suplantar la dirección IP de un cliente registrado adquiriría acceso a los dominios registrados.

Un cliente WLAN registrado solo al dominio WLAN, no puede acceder a los servicios de IMS directamente. Esto lo comprobamos haciendo ping a la dirección IP que da acceso al dominio IMS (ver Figura 42) y tratando de registrarnos directamente al núcleo IMS (ver Figura 43).

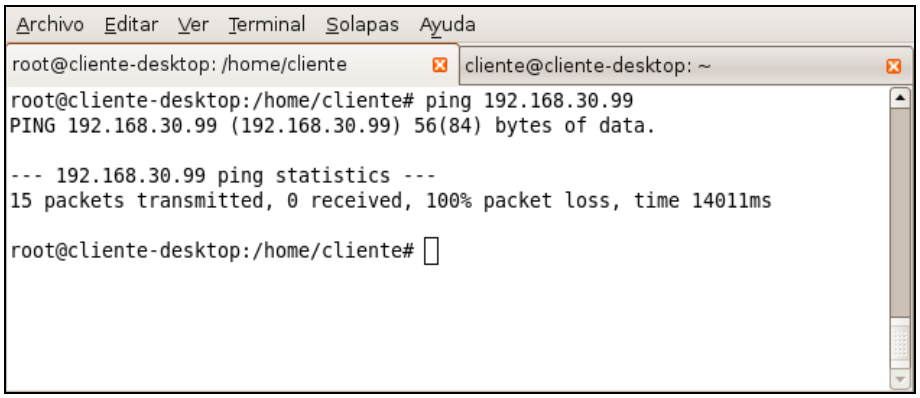

Figura 42. Prueba ICMP al punto de entrada a IMS, cliente registrado a WLAN.

Cuando un cliente intenta mandar una petición SIP al núcleo IMS, sin registro previo al dominio IMS, el SSW no permite transferir ningún tráfico hacia IMS como se puede ver en la Figura 43. Al no obtener respuesta el cliente la retransmite varias veces hasta que se cumple el tiempo de vida del paquete.

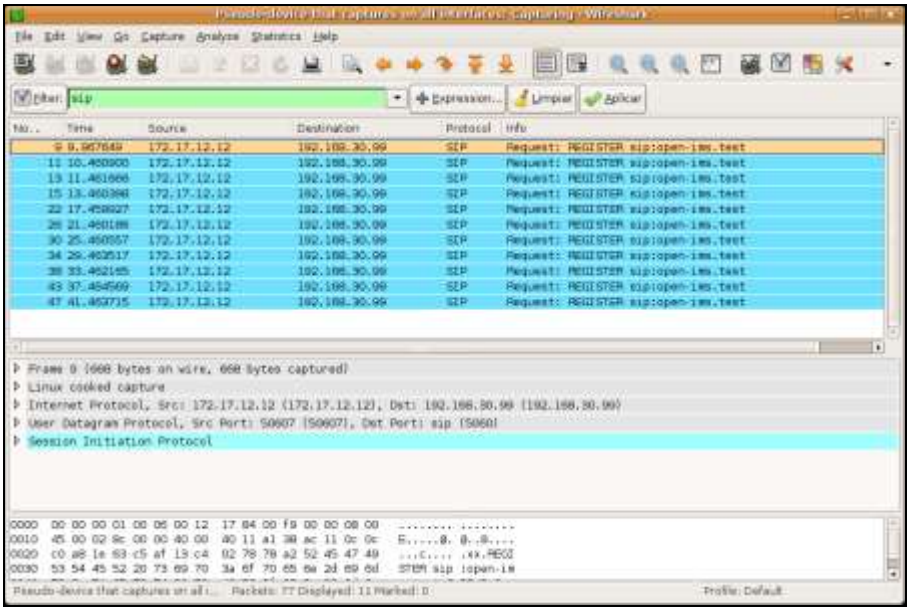

Figura 43. Intento de registrarse a IMS directamente sin haberse registrado

c. Si el usuario se registra a IMS puede acceder directamente a sus servicios, pasando a través del MidSEG.

Cuando el cliente WLAN se registra al dominio IMS se modifica automáticamente el filtro del SSW para poder acceder a IMS como se ve en la Figura 44.

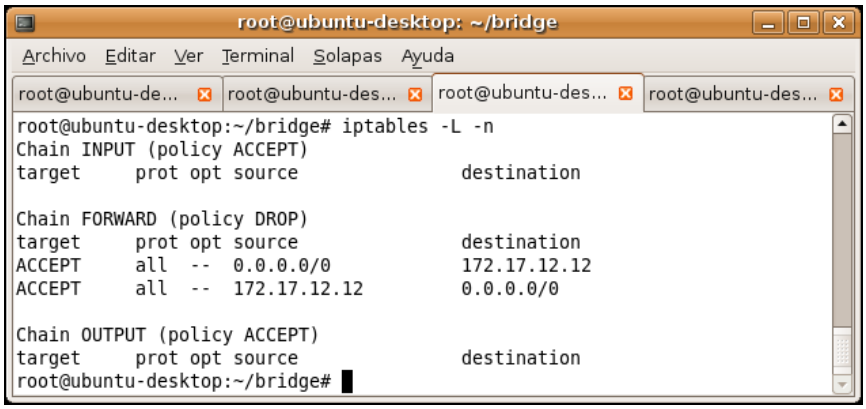

Figura 44. Firewall después de un registro exitoso a IMS

Si el cliente WLAN se registra al dominio IMS este puede acceder directamente al punto de entrada de IMS como se puede ver en la Figura 45.

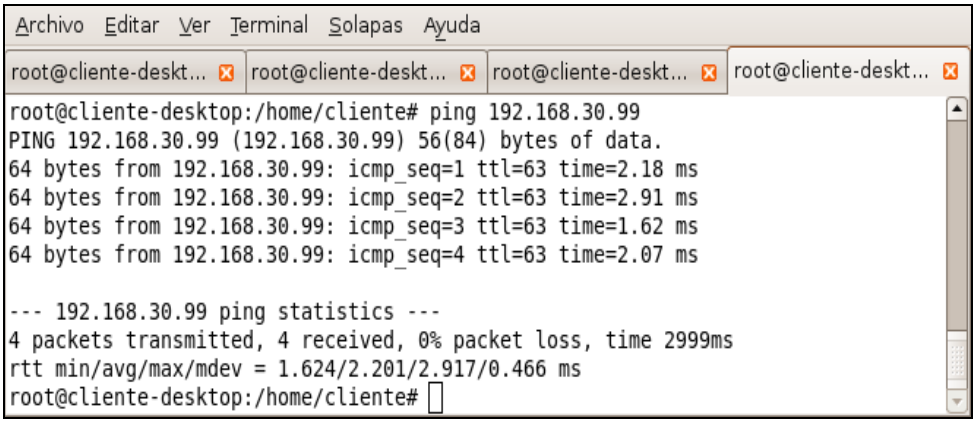

Figura 45. Prueba ICMP al punto de entrada a IMS, cliente registrado a IMS

Cuando el usuario intenta acceder directamente a IMS, haciendo peticiones SIP estas serán aceptadas por el SSW y el SSP direcciona las peticiones al P-CSCF. Esto permite que el MidSEG sea independiente de las peticiones SIP que se le hagan al núcleo IMS después de haberse registrado. En la Figura 46 se puede ver como una petición SIP hacia la 192.168.30.99, que es el punto de entrada de IMS es aceptada, en esta prueba para comprobar los mensajes se deshabilitó momentáneamente el cifrado de los paquetes tanto en el cliente como en el SSW.

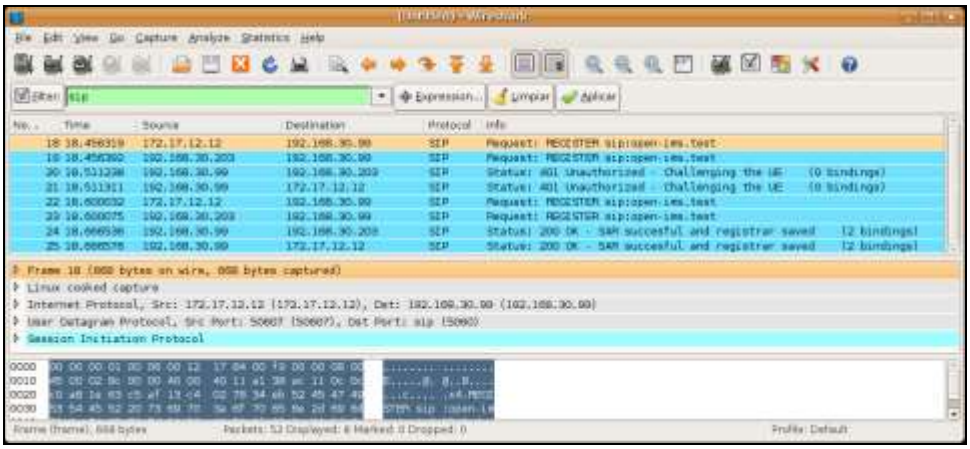

Figura 46. Peticiones SIP al núcleo IMS directamente.

d. Comprobar que el cliente WLAN puede registrarse o des-registrarse al núcleo IMS por medio de MidSEG.

Cuando el usuario se des-registra el filtro se actualiza inmediatamente, eliminando las políticas de reenvió para el usuario de registrado como se puede ver en la Figura 47.

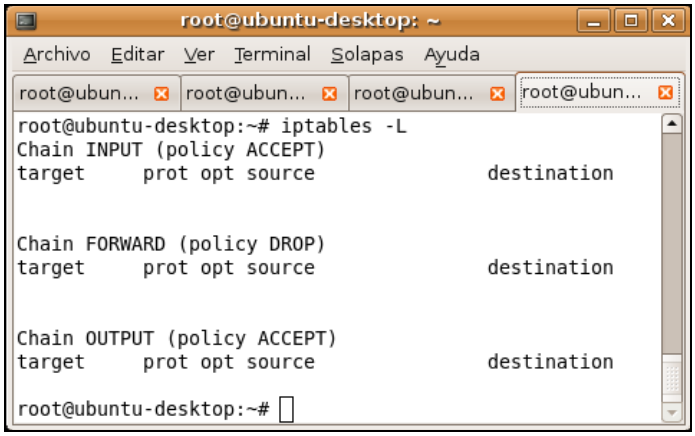

Figura 47. Políticas de reenvío (FORWARD) son eliminadas.

La solicitud de des-registro es un registro SIP manteniendo el mismo encabezado del call-ID de la solicitud de registro y el encabezado expires se encuentra en cero, en la Figura 48 se puede ver como una solicitud de des-registro es dirigida al SSW del MideSEG con dirección IP 172.17.12.1 y no directamente al núcleo IMS. En esta prueba para comprobar los mensajes se deshabilitó momentáneamente el cifrado de los paquetes.

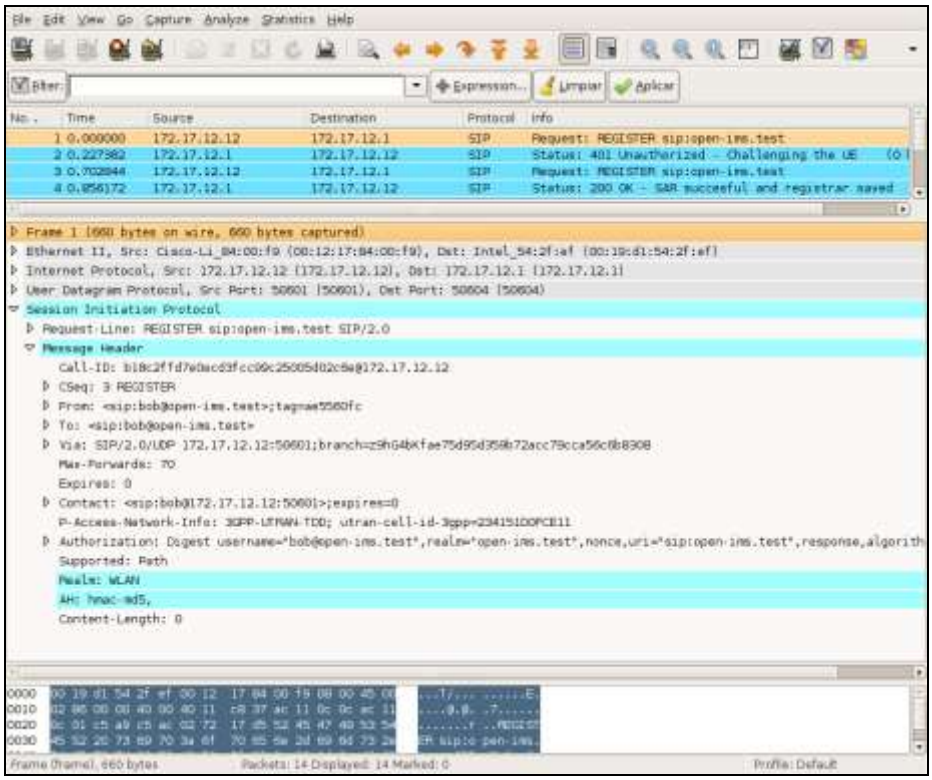

Figura 48. Solicitud de des-registro

- ***Prueba: actualizar el estado del usuario modificando la HSS como resultado de un registro satisfactorio.***

  Numero de pruebas realizadas: 3.

  La manera de representar un usuario no registrado en la tabla Registro es un cero (ver Figura 49). La importancia de esta tabla es que mantiene el registro del usuario a cada dominio, con el fin de que sea reutilizado por los diferentes dominios (p. Ej: el 3GPP la puede usar para saber si un usuario esta registrado o no).

Figura 49. Estado de la tabla Registro antes de Registrarse

Después de que el usuario se registra a los dominios WLAN o IMS, la tabla de Registro se modifica como se muestra en la Figura 50 y Figura 51, respectivamente.

Figura 50. Estado de la tabla Registro cuando se registra a la WLAN

Figura 51. Estado de la tabla Registro cuando se registra a IMS

- ***Prueba: validar la integridad y confidencialidad de los datos para garantizar la seguridad en la comunicación establecida entre el UE y el P-CSCF.***

  Número de pruebas realizadas: 3

  a. En la Figura 52, sin el uso de IPsec, se comprueba que la confidencialidad y privacidad de la señalización IMS puede ser fácilmente vulnerada, ya que esta viaja en texto plano por lo que puede ser vista por alguien que use un analizador de protocolos como Wireshark.

     Cuando la señalización SIP no es cifrada, esta puede ser fácilmente interpretada, por lo que un atacante puede conocer los servicios que se intenta acceder o con quien se quiere establecer una sesión.

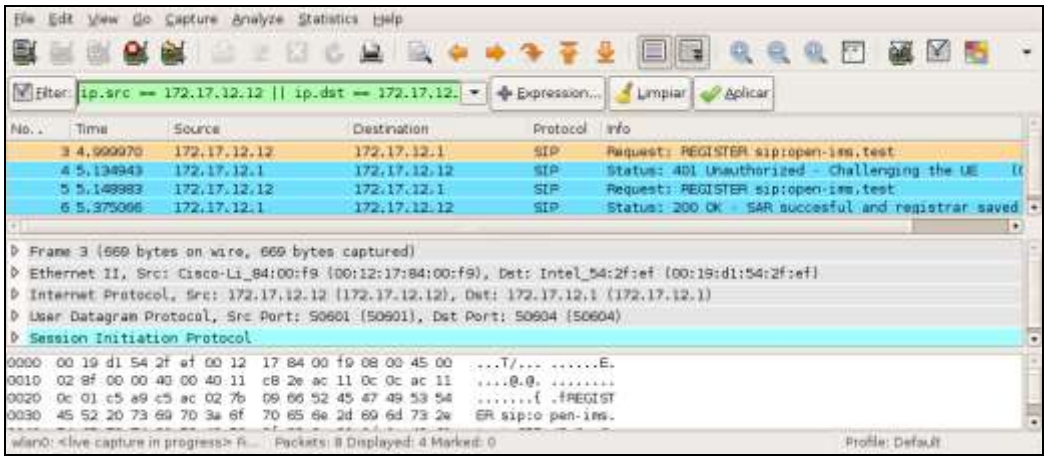

Figura 52. Señalización sin uso del MidSEG

  b. La señalización es protegida por medio de IPsec que utiliza el protocolo ESP para proporcionar confidencialidad e integridad en la señalización SIP.

     La primera vez que un usuario se autentica, los dos primeros mensajes no estan cifrados (Register y No-Autorizado). Como se puede ver en la Figura 53.

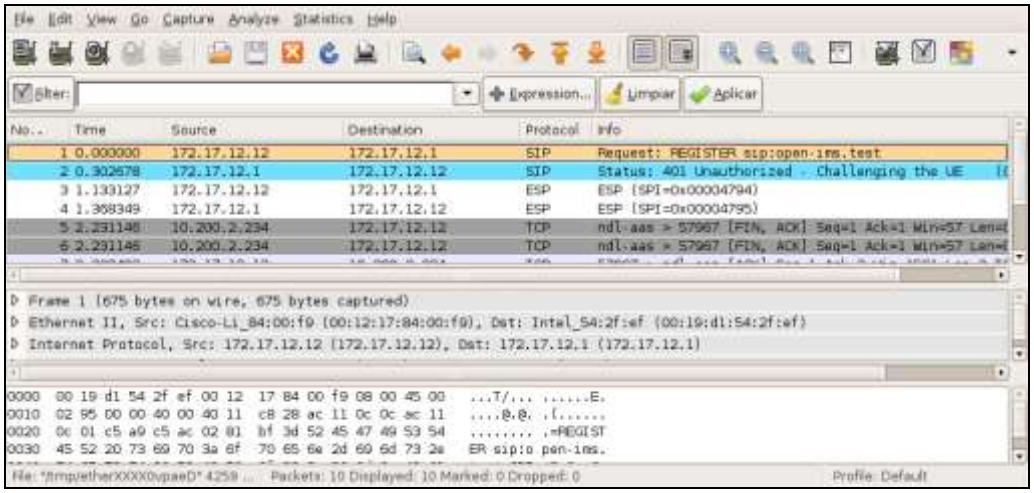

Figura 53. Primer registro de un usuario.

En las subsecuentes autenticaciones todos los mensajes se cifran, ya que hacen uso de las llaves utilizadas en un registro anterior (ver Figura 54).

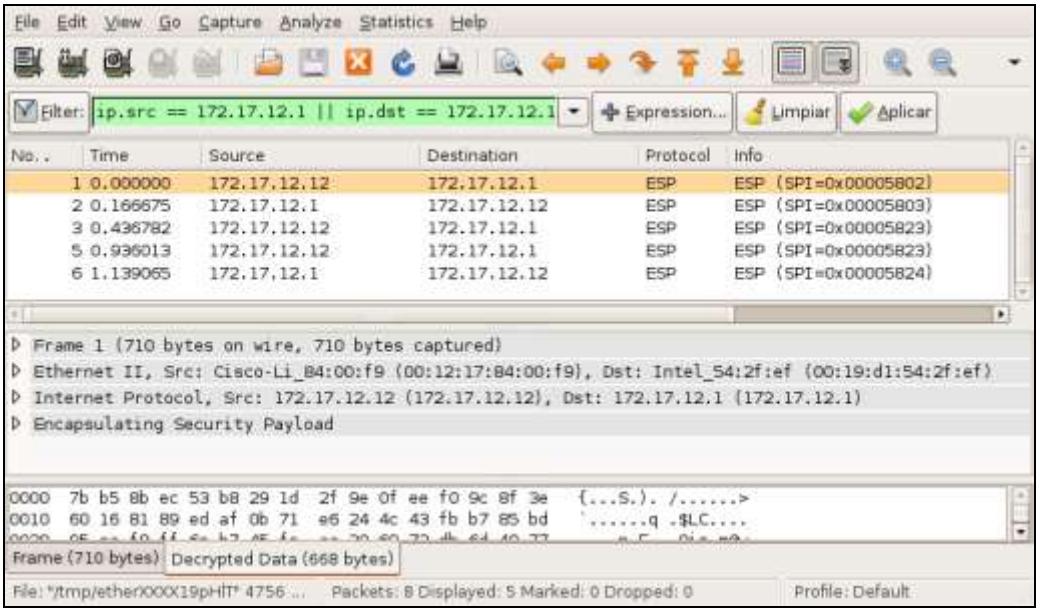

Figura 54. Señalización después del primer registró

c. No se encontró un ataque para descifrar el trafico IPsec, pero Wireshark proporciona una configuración de tal manera que si se conocen los algoritmos utilizados en IPsec, las direcciones entre los que existe la SA, los SPIs y las llaves de cifrado y autenticación se puede descifrar el tráfico (ver Figura 55).

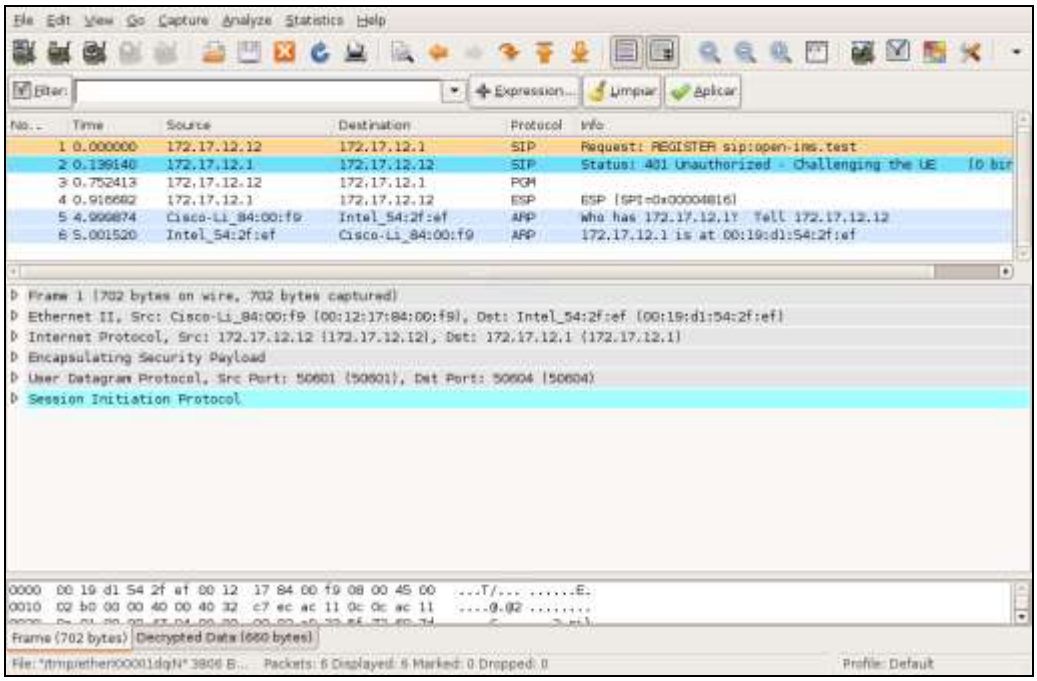

Figura 55. Señalización IPsec descifrada con Wireshark

Esta información puede ser conseguida del archivo /etc/ipsec-tools.conf. Debido a que este tiene permisos de lectura para todos los usuarios (ver Figura 56).

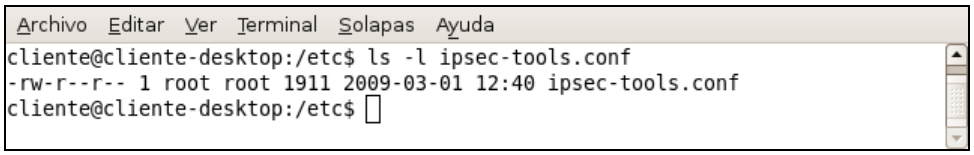

Figura 56. Permisos del archivo ipsec-tools.conf

Un usuario, sin necesidad de ser root, puede ver esta información con un editor de texto como se muestra en la Figura 57.

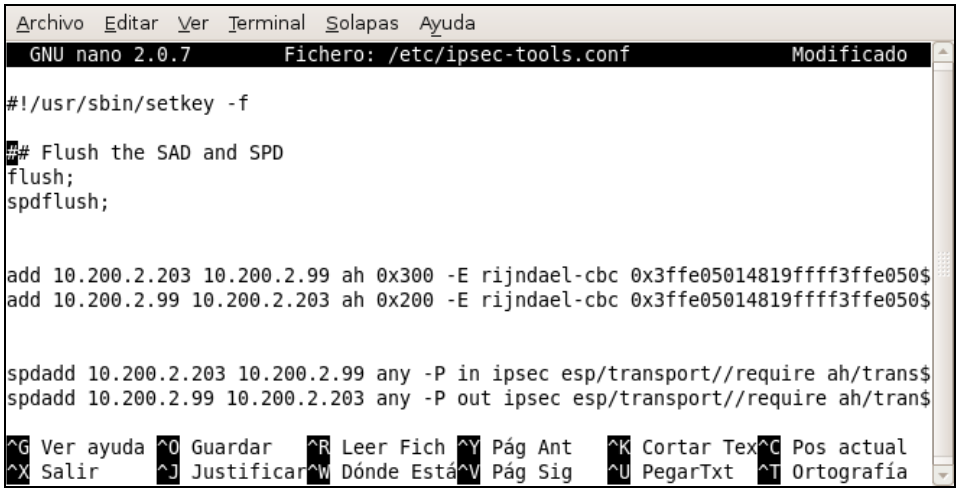

Figura 57. Archivo ipsec-tools.conf

Para que la información no pueda ser vista por usuarios no autorizados, se cambian los permisos del archivo ipsec-tools.conf para que solo puedan ser vistos por el usuario root como se muestra en la Figura 58.

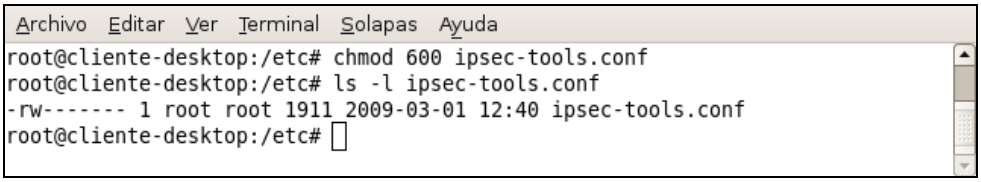

Figura 58. Cambio de permisos ipsec-tools.conf

- ***Prueba: comprobar contraseñas seguras de root.***

Número de pruebas realizadas: 2.

Para realizar esta prueba se utilizó la herramienta John the Ripper en un sistema operativo Windows. Partiendo de los archivos passwd y shadow, los cuales se encuentran en el directorio /etc y contienen las contraseñas cifradas del equipo.

a. Modo Diccionario
Se realizó con una lista de palabras encontradas en el archivo password, obteniendo que las claves evaluadas no se encuentran en el diccionario utilizado (ver Figura 59), lo cual no significa que no pueda estar en otro.

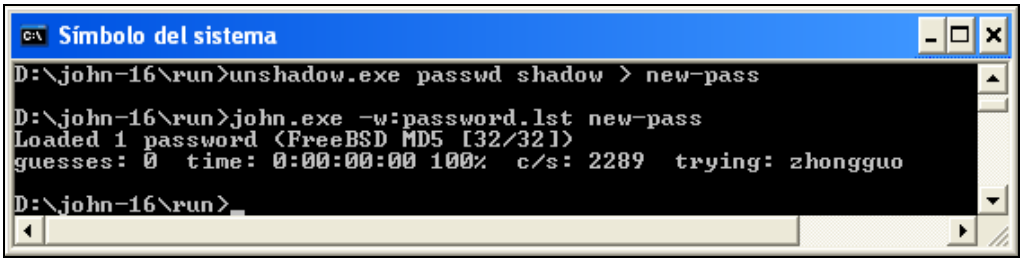

Figura 59. Ataque de fuerza bruta con Jhon the Ripper

b. Modo Incremental
Con este método Jhon the Ripper realiza automáticamente una combinación de letras, números y caracteres para probarlos como posibles contraseñas. Como ejemplo se puede ver la Figura 60, donde la aplicación Jhon the Ripper fue detenida después de 16 horas sin encontrar resultados exitosos.

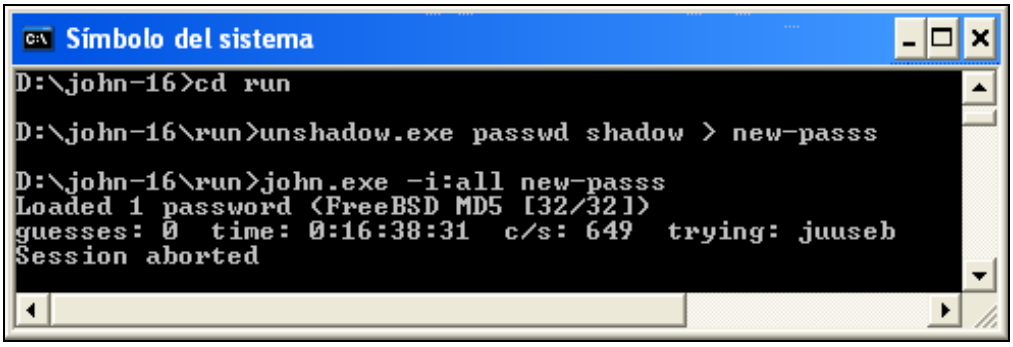

Figura 60. Ataque incremental con Jhon the Ripper

De esta manera se comprueba que las contraseñas utilizadas en los servidores son seguras, en caso de lograr su des-cifrado las contraseñas deberán ser cambiadas por otras más seguras.

- ***Prueba: explorar equipos con Nmap.***

La herramienta Nmap permite una exploración de puertos TCP y UDP, para determinar que puertos y servicios asociados están abiertos en los equipos. Esto se realizó en los equipos de MidSEG (SMSW y SMSP) con el fin de detener servicios que no se estén usando y poder utilizar el filtro para que este tipo de escaneo falle.
La Figura 61 nos muestra que el resultado de intentar escanear el equipo 172.17.12.1 con nmap es exitoso, mostrando que tiene abiertos los puertos 53 (DNS), 3306 (Mysql), 5900 (vnc) y 51622 (ssh). También nos da información acerca del sistema operativo que está usando (Linux 2.617 - 18).

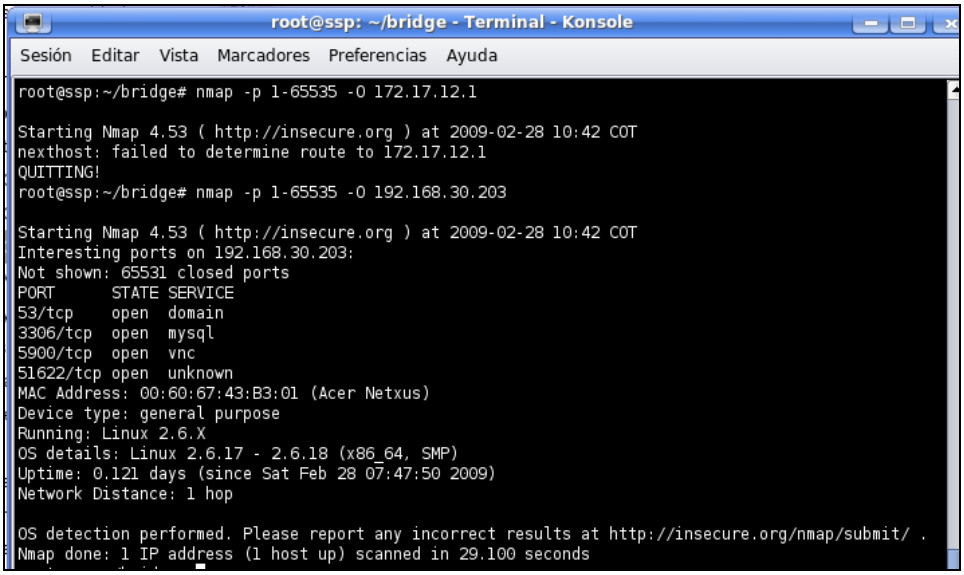

Figura 61. Prueba nmap al SMSW

Teniendo en cuenta que los puertos abiertos son de servicios que no se están utilizando, fueron cerrados, a continuación se repitió la prueba (ver Figura 62) obteniendo que los 65535 puertos estaban cerrados. Los puertos cerrados no tienen ninguna aplicación escuchando en los mismos pero pueden ser accesibles (recibe y responde a los paquetes de prueba de nmap).

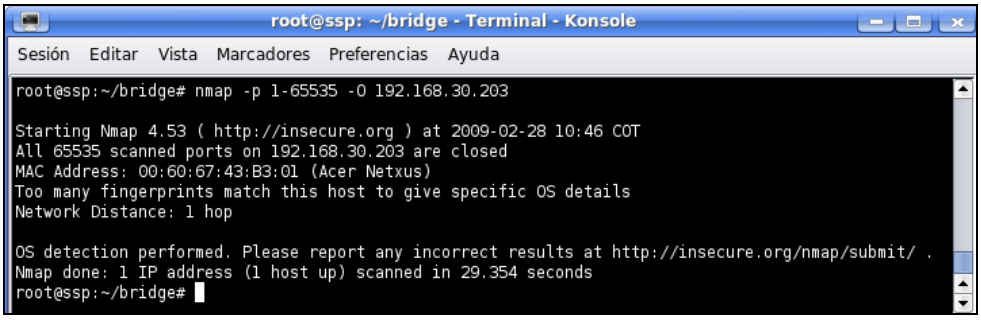

Figura 62. Prueba nmap cerrando los servicios no utilizados

Si un atacante utiliza nmap para intentar hacer el mismo escaneo con el filtro funcionando, obtendrá un bloqueo que no le da información sobre el sistema operativo ni le permite saber si se encuentra abiertos o cerrados los puertos (ver Figura 63).

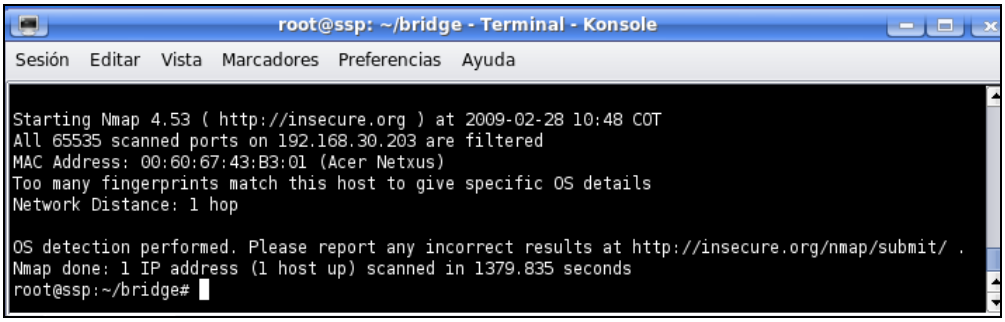

Figura 63. Prueba nmap activando el filtro

- ***Prueba: evaluar la seguridad del MidSEG en la WLAN***
  Número de pruebas realizadas 5.

  Se realizó con el fin de verificar la seguridad prestada por el MidSEG en los paquetes de la interfaz inalámbrica. Para poder capturar los paquetes de la interfaz inalámbrica se utilizó la herramienta CommView for WiFi 6.1 [63], la cual permite analizar el tráfico inalámbrico sin estar conectado directamente a un AP.

  a. Primero el PC atacante sin estar asociado al AP, que se configuró sin seguridad, capturó una serie de paquetes. En este caso, todos los paquetes van sin cifrar por lo que se puede identificar claramente los encabezados SIP como se muestra en la Figura 64.

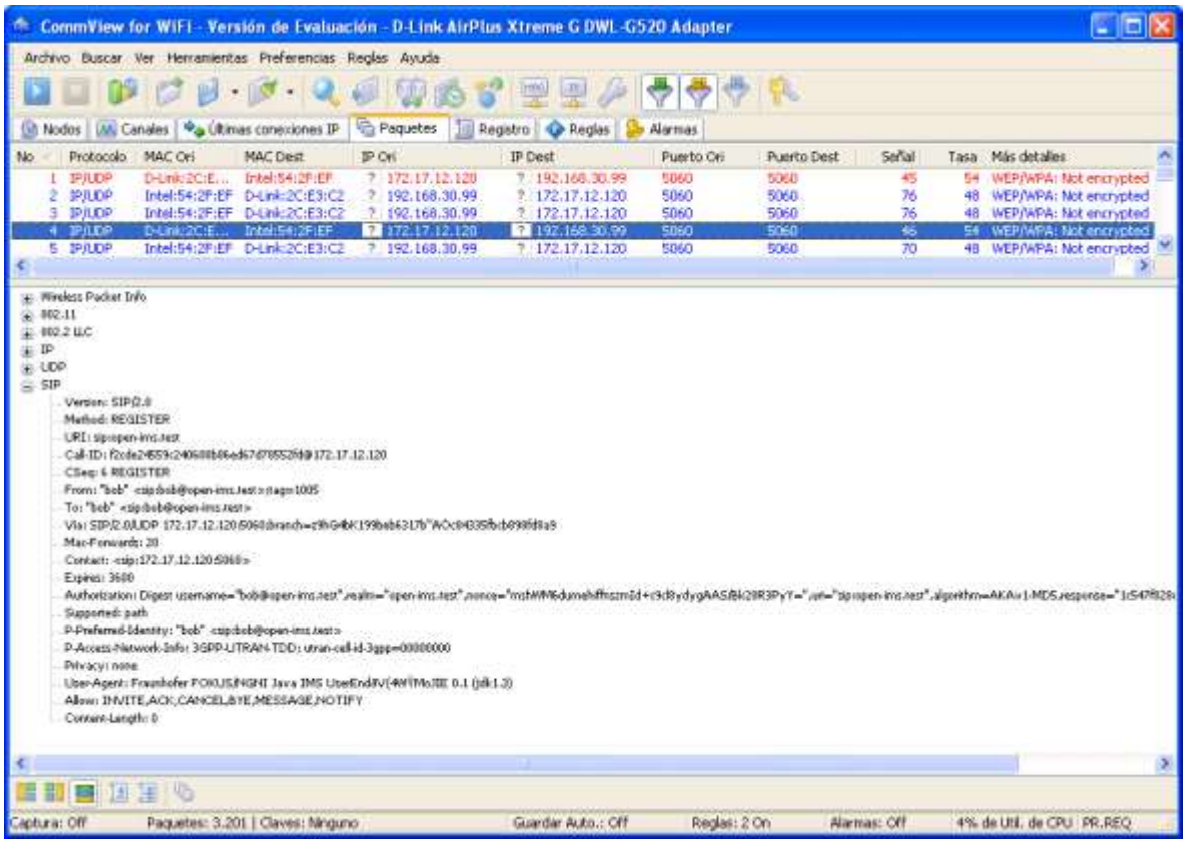

Figura 64. Captura de paquetes sin seguridad

b. Ahora se capturaron paquetes del AP, el cual estaba configurado con seguridad WEP (ver Figura 65), en este caso los paquetes estaban cifrados con la llave compartida entre el AP y los clientes WLAN.

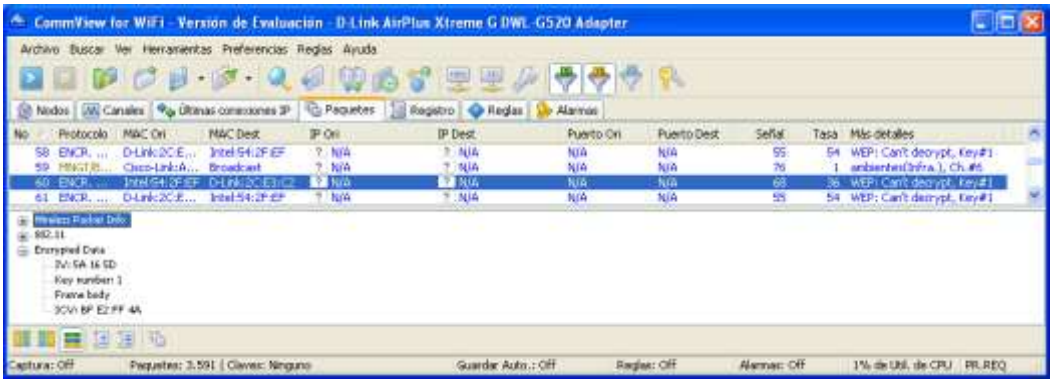

Figura 65. Captura de paquetes con seguridad WEP

c. La seguridad WEP puede ser vulnerada con la unión de herramientas como: airodump-ng, aireplay-ng, aircrack-ptw, que permiten encontrar la contraseña WEP configurada. En nuestro caso partimos de que conocemos la contraseña y se la configuramos al PC que esta capturando los paquetes, obteniendo que se pueden ver claramente todos los paquetes de otros clientes, como cuando no se tenía ninguna seguridad asociada al AP, en la Figura 66 se muestra que los paquetes a pesar de tener seguridad WEP son descifrados.

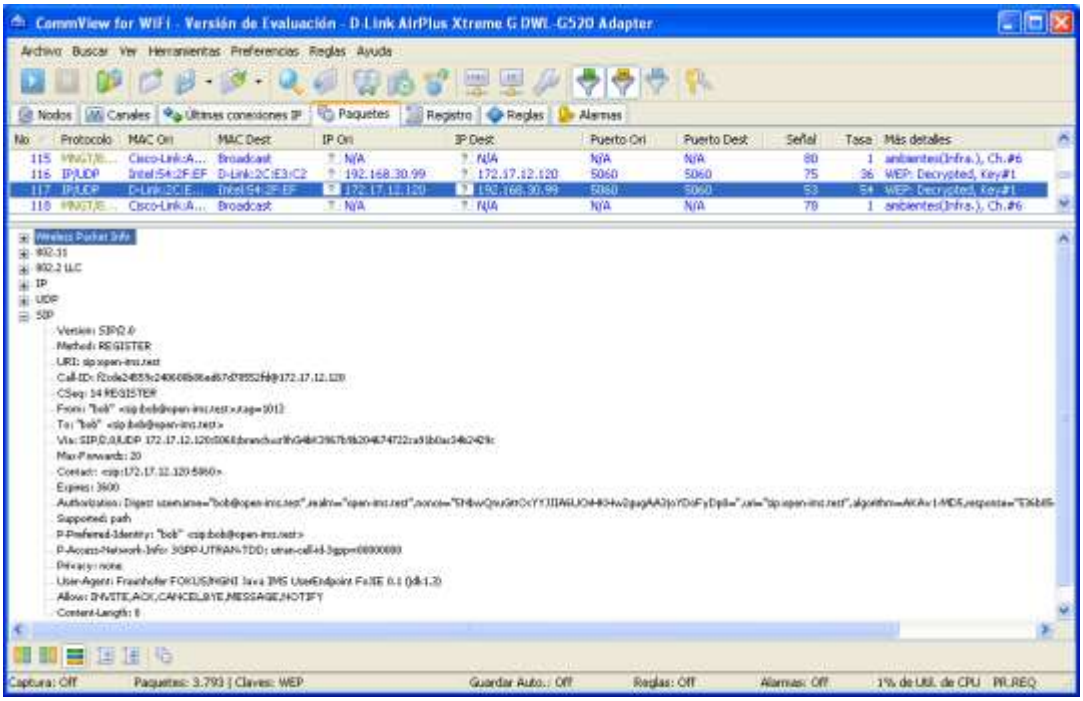

Figura 66. Captura de paquetes con seguridad WEP descifrada

d. Se cambió la seguridad del AP a WPA personal, la cual podría ser vulnerada con ataques de fuerza bruta que logren obtener la contraseña. Se capturaron paquetes sin tener la clave y después configurándola en el PC, obteniendo que no se pueden descifrar los paquetes con seguridad WPA (Figura 67) por el hecho de que las claves utilizadas para cifrar los paquetes son distintas para cada cliente y cambian dinámicamente. Aunque no se puede descifrar los paquetes utilizando seguridad

WPA personal, si se puede tener acceso a los servicios que preste el AP si se logra conseguir la contraseña.

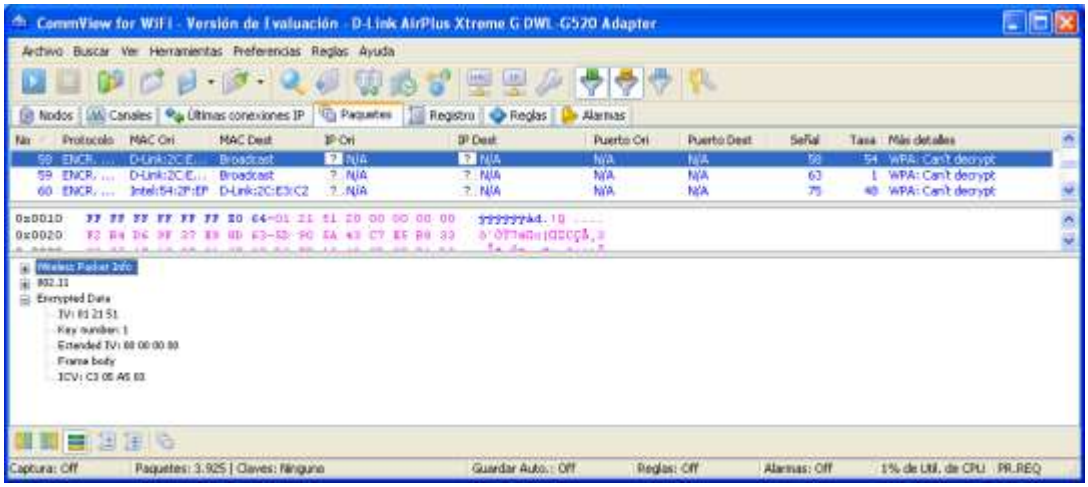

Figura 67. Captura de paquetes con seguridad WPA personal

e. De los cuatro casos anteriores se puede ver que el peor se da cuando una AP no utiliza seguridad, por lo que se prueba el MidSEG con una conexión WLAN sin seguridad obteniéndose que los paquetes no pueden ser descifrados debido a que se utiliza IPsec (ver Figura 68) para garantizar la confidencialidad e integridad de los paquetes. También, es necesario tener en cuenta que las llaves utilizadas en las SA entre el MidSEG y el SCSWI son diferentes para cada usuario y que estas son renovadas con cada autenticación.

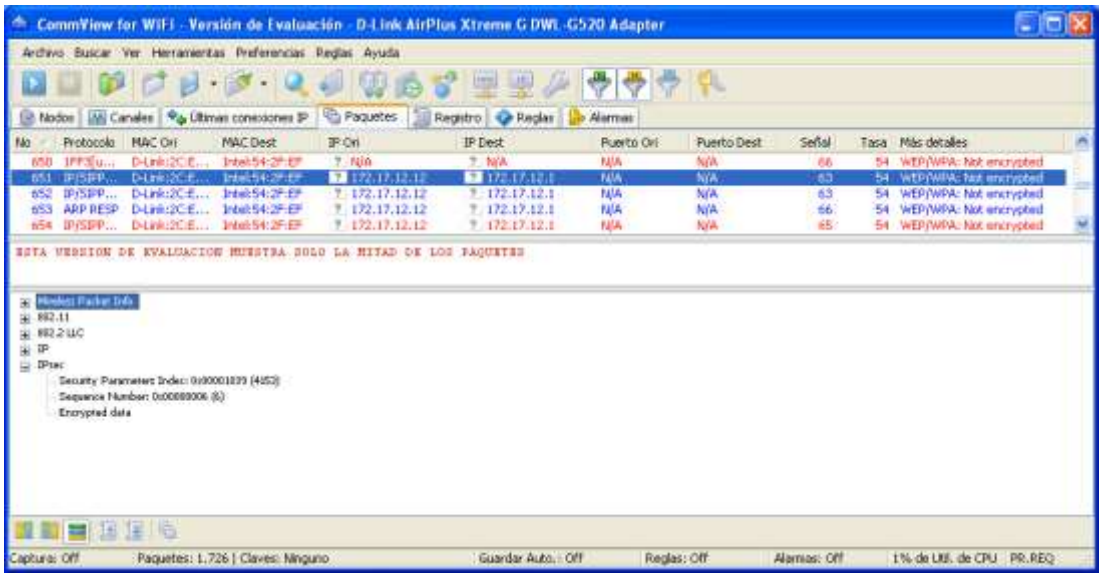

Figura 68. Captura de paquetes con la seguridad del MidSEG y sin seguridad inalámbrica

3.6 EVALUACIÓN DE RENDIMIENTO

Las pruebas de rendimiento son realizadas con el fin de comprobar la incidencia sobre el desempeño de la red cuando se utiliza MidSEG. Las propuestas presentadas en [6] [7] [8]no hacen una implementación de referencia y en [9] sólo se plantea el diagrama de despliegue.

3.6.1 Prueba 1: Comparar los tiempos de registro con y sin seguridad

Desarrollo: Esta prueba se realizó con la diferencia de tiempos entre mensajes SIP REGISTER y SIP OK.

Primero se llevo a cabo la prueba con el SCSWI sin seguridad, esta se repitió 100 veces (ver Tabla 10), obteniendo un promedio de 265,9 milisegundos en registrarse.

Tabla 10. Tiempo de registro sin seguridad (10 resultados de 100)

Registro	Tiempo
1	292
2	295
3	274
4	245
5	285
6	274
7	257
8	249
9	254
10	243
Promedio	265,9

Posteriormente se efectuó la prueba con el SCSWI con seguridad (ver Tabla 11), obteniendo un promedio de 532,9 milisegundos en registrarse.

Tabla 11. Tiempo de registro con seguridad (10 resultados de 100)

Registro	Tiempo
1	518
2	565
3	545
4	525
5	523
6	562
7	516
8	514
9	546
10	527
Promedio	532,9

Como era de esperarse el tiempo de registro de un usuario con seguridad es mayor, debido a que el procesamiento de los paquetes aumenta tanto en el cliente como en los servidores, ya que se tienen que realizar tareas adicionales sobre el paquete como: cifrar, descifrar, verificar la integridad y comprobar la confidencialidad.

En el proceso de registro se hacen 2 solicitudes SIP REGISTER y se obtienen sus respectivas respuestas SIP UNAUTHORIZED y SIP OK, lo que equivale a 2 viajes de ida y vuelta (RTT, Round-Trip Time) por lo que el valor para un RRT es de 266,45 ms, por consiguiente utilizar SA no provoca retransmisiones de mensajes SIP por

encontrarse por debajo del tiempo RTT por defecto de 500 ms, establecido en el RFC 3261 [18]. No obstante, cuando cambien las condiciones del ambiente a algo más hostil es más susceptible que se den retransmisiones SIP utilizando la seguridad de MidSEG por ser mayor el tiempo en registrarse a través de este.

3.6.2 Prueba 2: Comparar la carga extra en la red debida a los encabezados ESP de IPsec

Desarrollo: Se realizó la prueba con la ayuda de la herramienta Wireshark, la cual permite obtener el tamaño del paquete capturado.

En la Tabla 12 se muestra el tamaño en bytes de los paquetes SIP necesarios en un proceso de registro o des-registro.

Tabla 12. Bytes de Paquetes sin cifrar

	Paquetes SIP No Cifrados			
	REGISTER	UNAUTHORIZED	REGISTER	OK
Registro	674	1042	799	1018
Desregistro	668	1042	793	957
Registro	674	1042	799	1017
Desregistro	668	1042	793	953

En la Tabla 13 se muestra el tamaño de los paquetes cifrados con el protocolo ESP de IPsec.

Tabla 13. Bytes de Paquetes Cifrados con ESP

	Paquetes SIP Cifrados			
	REGISTER	UNAUTHORIZED	REGISTER	OK
Registro	710	1078	830	1054
Desregistro	702	1078	830	990
Registro	710	1078	830	1054
Desregistro	702	1078	830	990

La cabecera ESP se genera y se añade al paquete tras cifrarlo y calcular su código de integridad. En la Figura 69 se puede ver la cabecera ESP, la cual consta de un índice de parámetros de seguridad (SPI, Security Parameter Index), un número de secuencia (SN, Sequence Number), un vector de inicialización (IV, Initialization Vector), carga cifrada, un relleno, longitud del relleno, cabecera que especifica la siguiente cabecera y por último un código de integridad del paquete (HMAC, Hash Message Authentication Code). En la Tabla 14 se resume el tamaño de los bytes adicionados al paquete y su utilidad [64].

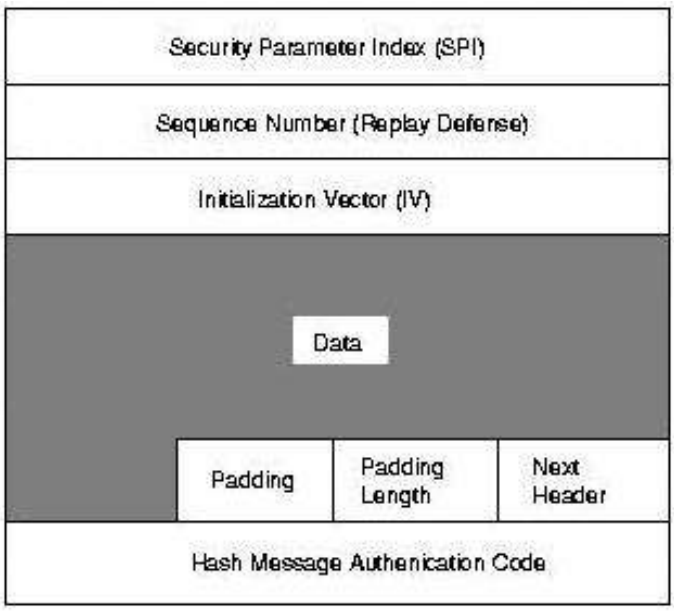

Figura 69. Cabecera ESP

Tabla 14. Bytes de la cabecera ESP

Campos	Bytes	Utilidad
SPI	4	Especifica la SA que se va ha usar.
SN	4	Protege Contra la repetición de paquetes.
VI	4	Asegura que cargas iguales generen cargas diferentes.
Relleno	0-12	0-7 bytes para operaciones de cifrado de bloque DES o 3DES más de 0-3 alinear el texto cifrado termine .
	2	Especifica el tamaño del relleno y la siguiente cabecera.
HMAC	12	Asegura integridad del paquete.

Teóricamente los bytes adicionados por la cabecera ESP estarán entre 26 y 37 bytes. Esto se comprueba haciendo la diferencia entre las tablas 13 y 12 (ver Tabla 15).

Tabla 15. Diferencia en bytes entre la Tabla 13 y Tabla 12

	Paquetes SIP Cifrados			
	REGISTER	UNAUTHORIZED	REGISTER	OK
Registro	36	36	31	36
Desregistro	34	36	37	33
Registro	36	36	31	37
Desregistro	34	36	37	37

3.6.3 Prueba 3: Determinar cuántas peticiones SIP pueden procesar los servidores del MidSEG

Limitaciones: No se pueden utilizar herramientas especializadas en generar tráfico SIP para pruebas de rendimiento como SIPp o SIPSAK, debido a que nuestro SCSWI adiciona nuevos encabezados para el correcto funcionamiento del MidSEG, los cuales no son proporcionados por estas herramientas software especializadas.

Desarrollo: Se modifica el código del SCSWI para que ejecute determinadas peticiones SIP REGISTER por segundo, las cuales se aumentan con el objetivo de encontrar cuál es el límite de MidSEG. Primero se realiza la prueba sin establecer SA, por lo que la señalización SIP va en texto plano. Los resultados se pueden ver en la Tabla 16, encontrando que a partir de las 50 solicitudes SIP REGISTER/seg se comienza a disminuir los registros exitosos al núcleo IMS hasta llegar a cero en 150 solicitudes SIP REGISTER/seg.

Tabla 16. Solicitudes SIP sin cifrar

Solicitudes	Respuestas		
SIP REGISTER/Seg	SIP OK	Time Out	SIP Busy
10	10	0	0
20	20	0	0
50	47	3	0
60	51	9	0
70	46	5	19
80	44	5	37
90	29	3	61
100	12	6	84
120	6	9	101
140	3	12	124
150	0	42	108
500	0	404	98
750	0	726	23
950	Excepción		

Aunque no se obtengan respuestas exitosas (SIP OK), las solicitudes SIP son procesadas a través del MidSEG de ahí que el consumo de recursos de los servidores del MidSEG aumenta cuando se incrementan, alcanzando el MidSEG una excepción (ver Figura 70) con 950 solicitudes por memoria RAM insuficiente.

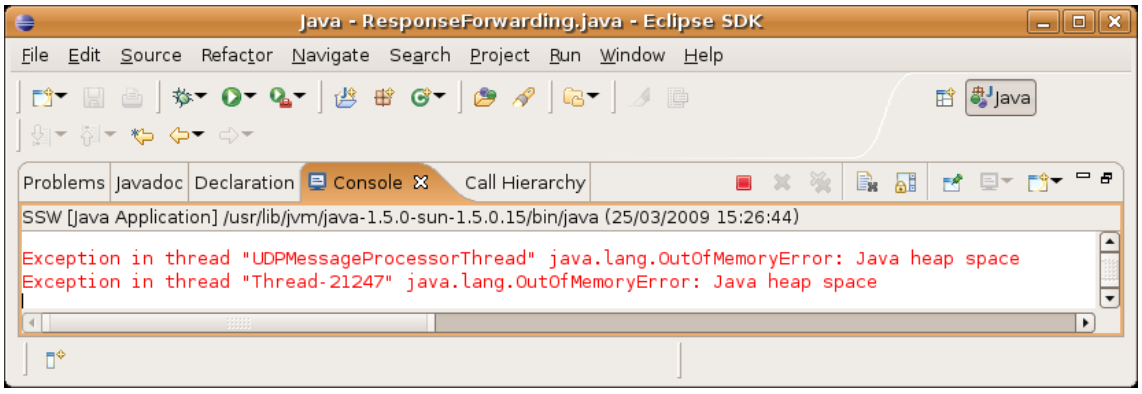

Figura 70. Excepción Lanzada por el MidSEG con 950 solicitudes

Cuando se envían más de 69 solicitudes de registro, el núcleo IMS responde con mensajes SIP 600 BUSY, como se ve en la Figura 71, no obstante que el núcleo responda como ocupado no le compete al MidSEG y es responsabilidad del operador garantizar la disponibilidad de este. Para la prueba realizada se puede deber a que el núcleo IMS se encuentra en una misma máquina y solo se tiene un S-CSCF por lo que este se ve sobrecargado.

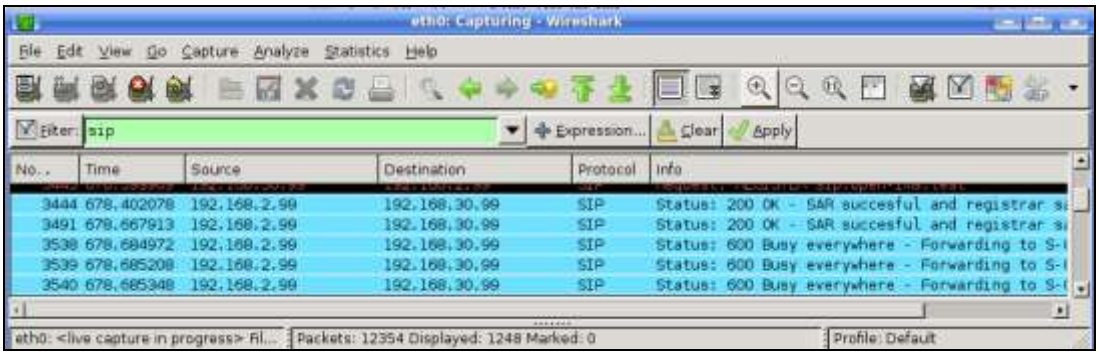

Figura 71. Responde ocupado el S-CSCF del núcleo IMS con más de 69 solicitudes SIP REGISTER

Para efectuar las solicitudes SIP REGISTER utilizando el protocolo ESP, primero se registró el SCSWI para establecer las SA y posteriormente se utilizó el SCSWI modificado. Los resultados se pueden ver en la Tabla 17, comparándolos con los resultados de no usar SA (ver Tabla 16) no se encuentran cambios significativos.

Tabla 17. Solicitudes SIP usando ESP

Solicitudes	Respuestas		
SIP REGISTER/Seg	SIP OK	Time Out	SIP Busy
10	10	0	0
20	20	0	0
50	48	2	0
60	50	10	0
70	46	5	19
80	45	6	35
90	29	3	61
100	15	4	82
120	7	7	98
140	4	11	123
150	0	42	108
300	0	160	142
450	Mensaje SIP 480 – Indisponible interfaz Cx		

La diferencia que se encontró al usar SA es que no se alcanzaba a saturar el MidSEG puesto que primero el núcleo IMS enviaba un mensaje SIP 480 (ver Figura 72.), indicando que la interfaz Cx estaba indisponible, por consiguiente no se podía acceder al HSS y se necesitaba reiniciar el servidor HSS para regresar el servicio del núcleo IMS a la normalidad. Es responsabilidad del operador garantizar la disponibilidad de sus servidores y no le compete al MidSEG. Para la prueba realizada la utilización de IPSec exige mayor procesamiento al equipo donde se instaló el núcleo IMS de ahí que este responda así.

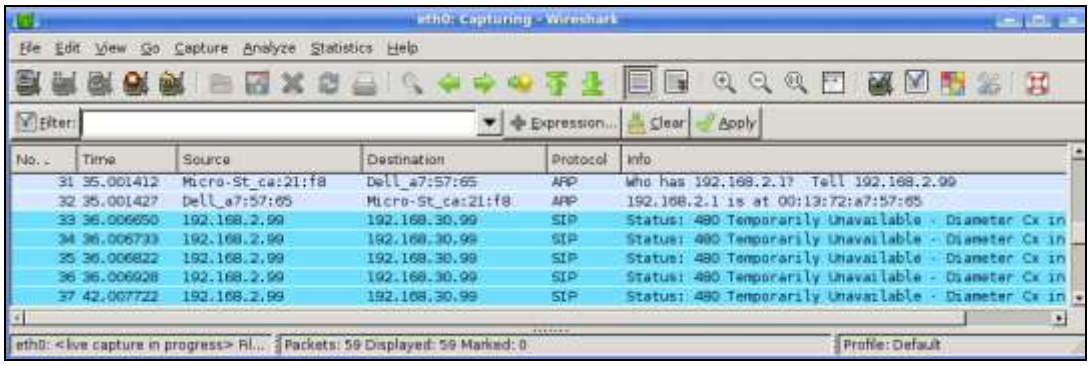

Figura 72. Mensaje SIP 480 enviado por el núcleo IMS

Capitulo 4

Servicio de Prueba

4.1. INTRODUCCIÓN

El servicio utilizado para verificar la confidencialidad e integridad en la señalización SIP al establecer una sesión es independiente de MidSEG. Debido a que se asegura la comunicación entre el UE y el punto de entrada a la red IMS, autenticando y cifrando cada paquete IP por medio de IPsec, el cual trabaja en la capa 3 del modelo OSI y no necesita ningún cambio para su uso por aplicaciones de niveles superiores. De este modo, por facilidad de evaluación se escogió el servicio de telefonía IP, ya que algunos clientes IMS lo traen implementado. Se verifica primero el establecimiento de la sesión de VoIP utilizando MidSEG pero sin SA para poder analizar el tráfico capturado y posteriormente se hace con SA para comprobar la confidencialidad e integridad.

4.2. METODOLOGÍA

Para poder iniciar una sesión, el UE previamente debe registrarse al núcleo IMS por medio de MidSEG. Teniendo en cuenta que en el registro se establecen SA que no permiten ver la señalización SIP, se plantean dos pruebas las cuales permite comprobar el establecimiento de una sesión IMS y verificar la confidencialidad e integridad de la señalización SIP.

En la Figura 73 se muestra el ambiente en el cual se ejecutaron las pruebas, conformado por el núcleo IMS, el MidSEG, la red de acceso WiFi, dos UE con el SCSWI y un PC para capturar el tráfico a analizar.

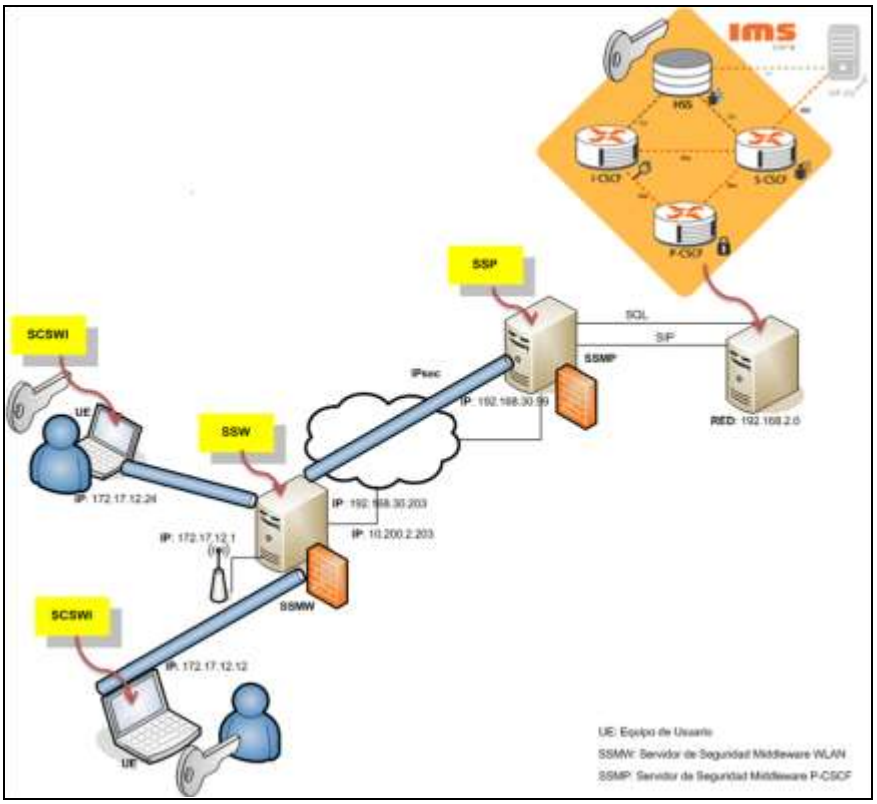

Figura 73. Ambiente de Pruebas del Servicio IMS

Para realizar las pruebas se utilizó:

- El cliente SCSWI que permite el registro a IMS y establece las SA con el MidSEG.
- El cliente IMS Open IMS Cliente Lite [65] que permite probar el servicio de telefonía IP a través del MidSEG.
- La herramienta Wireshark para capturar el tráfico.

4.2.1. Prueba 1: Verificar el establecimiento de una sesión sin SA

Esta prueba se realiza con el fin de verificar el correcto establecimiento de una sesión con el servicio de telefonía IP. Para comprobar esto primero se realiza el registro a IMS por medio de MidSEG pero se configura tanto el SCSWI como el SSW para no establecer SA con el fin de poder entender el tráfico capturado por la herramienta Wireshark.

Sin SA el trafico SIP capturado al establecer una sesión es fácilmente comprensible como se muestra en la Figura 74, donde el usuario que inicia la llamada tiene como URL SIP sip:alice@open-ims.test y dirección IP 172.17.12.24 mientras que el destino de la llamada es sip:bob@open-ims.tes con dirección IP 172.17.12.12.

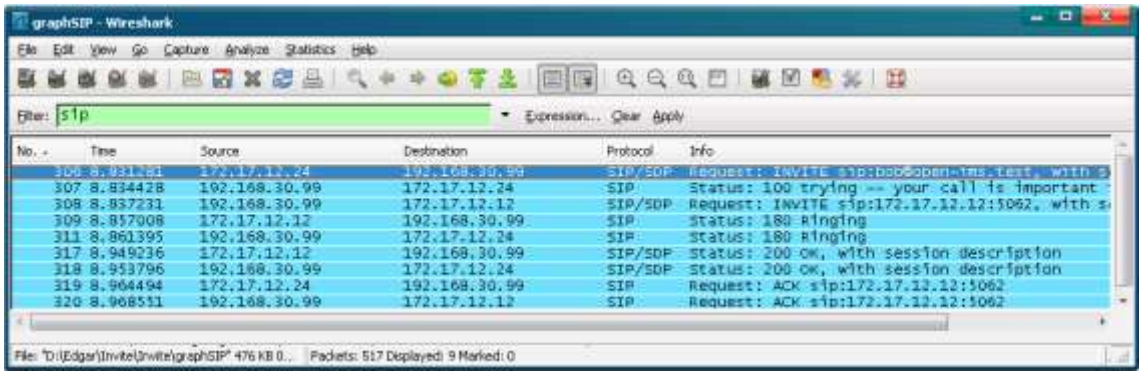

Figura 74. Establecimiento de una sesión

Por medio de la herramienta Wireshark uno puede reconstruir el flujo de paquetes del establecimiento de una sesión como se muestra en Figura 75.

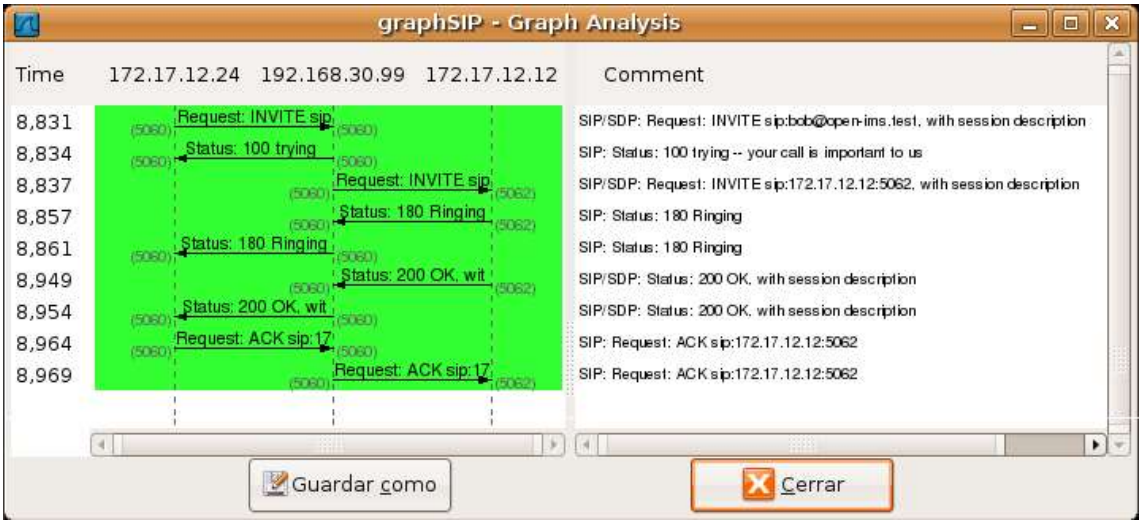

Figura 75. Diagrama de secuencia del establecimiento de una sesión

Con las capturas realizadas se describe el establecimiento de una sesión:

1. La usuaria alice@open-ims.test envía una solicitud SIP INVITE al proxy SIP con dirección IP 192.168.30.99. En la Figura 76 se muestra en detalle la solicitud SIP INVITE, en la cual se puede ver todos los encabezados SIP, como de donde viene con el campo From (alice@open-ims.test), hacia dónde va dirigía la invitación con el campo To (bob@open-ims.test), la descripción de la sesión que Alice desea establecer (audio, por el puerto 8000, flujo RTP, códec soportados G.711, GSM), etc.

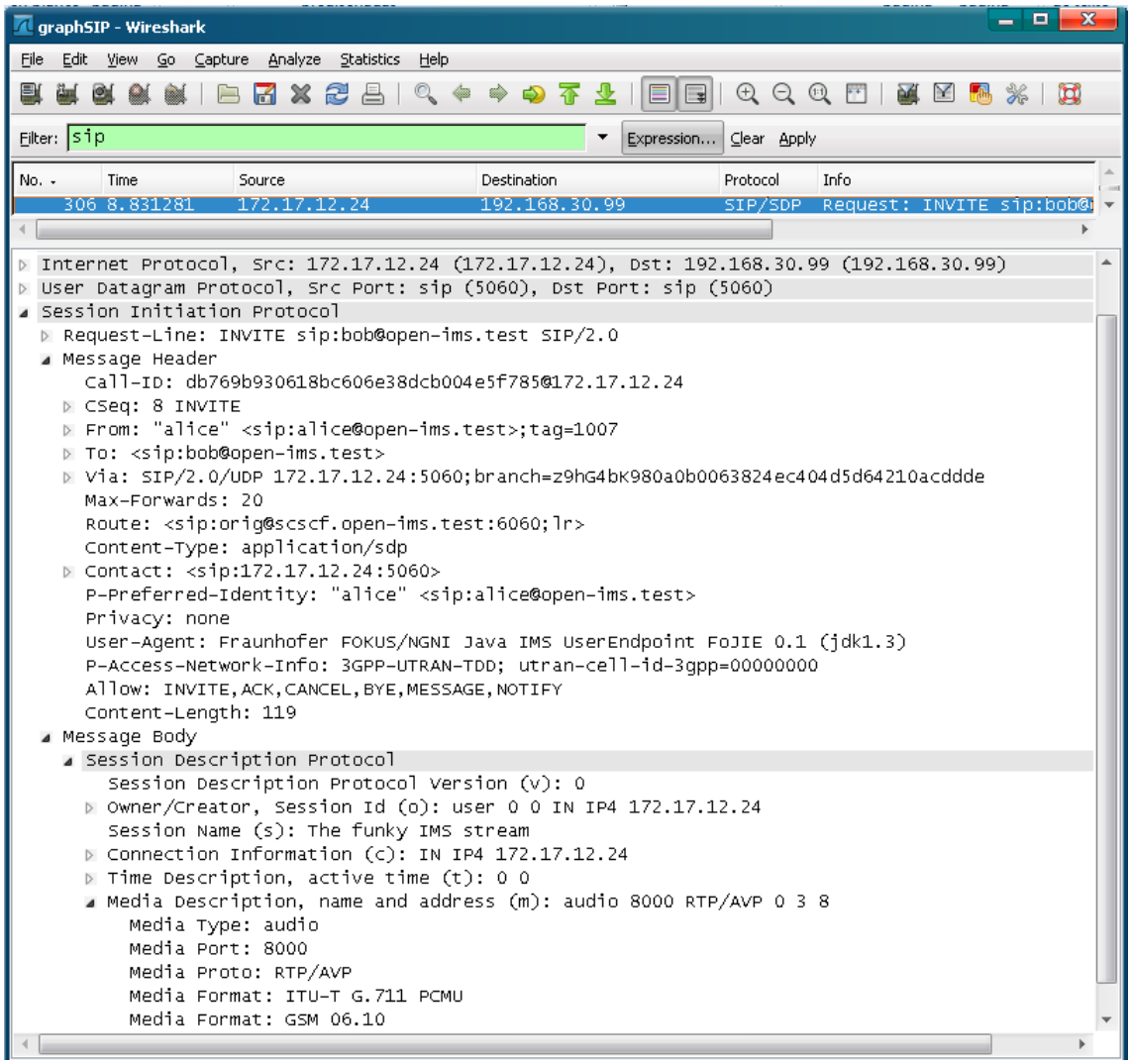

Figura 76. Solicitud Invite

2. A continuación se envía una solicitud SIP TRYING 100 a Alice para parar las retransmisiones de solicitudes INVITE.

3. El proxy SIP que en este caso es el CSCF reenvía la solicitud SIP INVITE a bob@open-ims.test.

4. Bob envía un mensaje RINGING 180 al CSCF, cuando el teléfono comienza a sonar.

5. El CSCF reenvía la solicitud RINGING 180 a Alice.

6. Cuando Bob acepta la llamada envía un mensaje SIP OK al CSCF.

7. El CSCF re-envía la respuesta SIP OK a Alice. En la Figura 77 se ve en detalle la respuesta SIP OK, con la que Bob confirma el establecimiento de la llamada e indica los parámetros para la sesión (audio, por el puerto 8000, flujo RTP, códec soportados G.711, GSM).

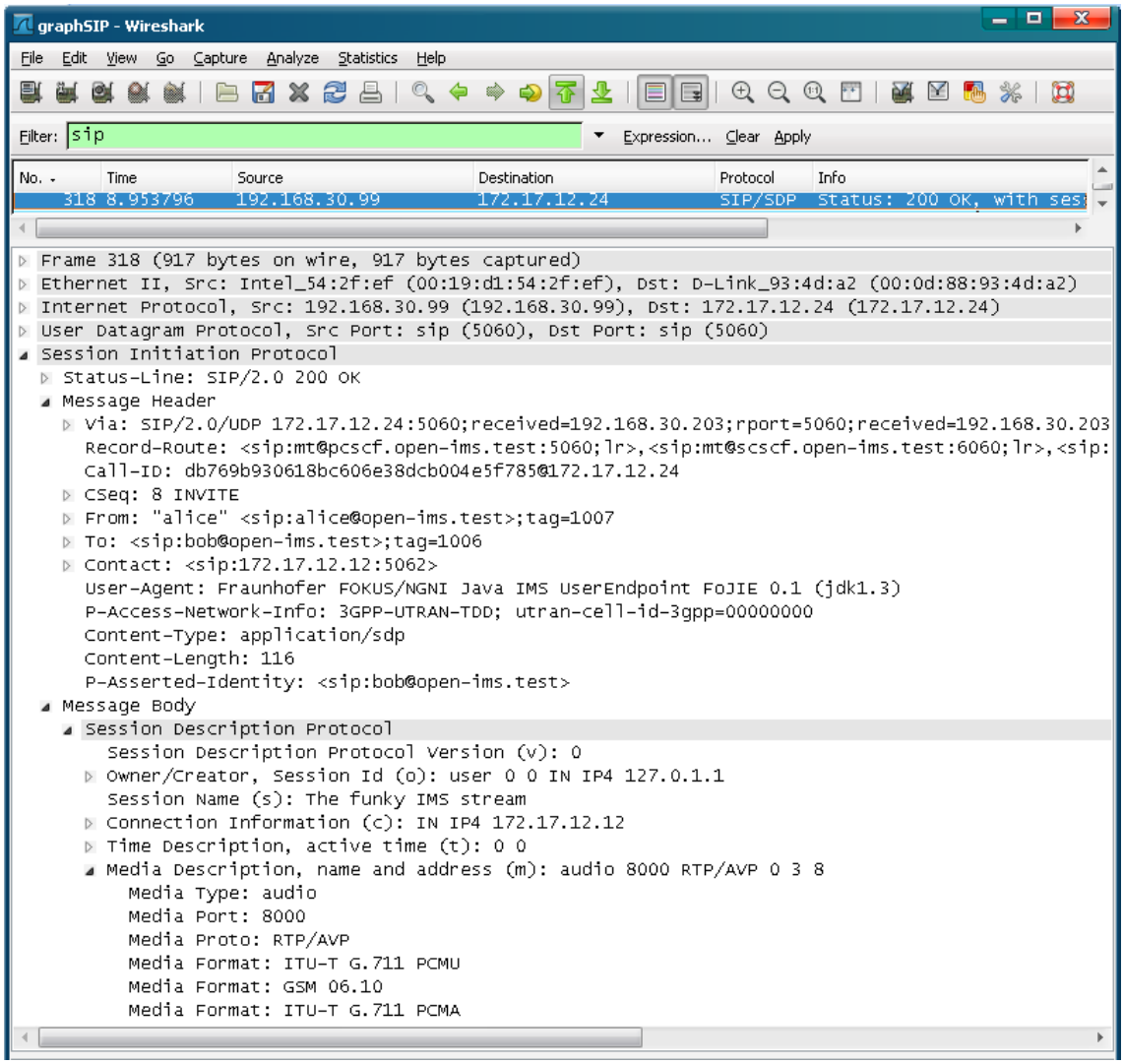

Figura 77. Respuesta SIP OK

8. Alice envía el mensaje SIP ACK al CSCF

9. El CSCF reenvía el mensaje SIP ACK, confirmando que Alice está de acuerdo con la llamada.

Cuando la llamada está establecida el flujo RTP para trasportar la voz se establece directamente entre los UE ya que el CSCF solo participa en la señalización SIP entre los UE, como se ve en la Figura 78.

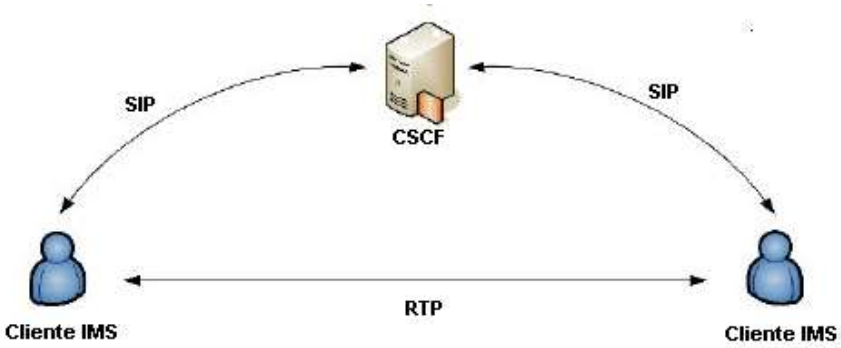

Figura 78. Señalización SIP y flujo RTP

En la Figura 79 se puede ver el flujo de paquetes en el establecimiento de una llamada de VoIP, donde se distingue más claramente que el CSCF solo interviene en la señalización SIP y los UE establecen el flujo RTP directamente entre Alice con dirección IP 172.17.12.24 y Bob con dirección IP 172.17.12.12, después que se negocian los parámetros de la sesión entre los UE por medio de SIP/SDP.

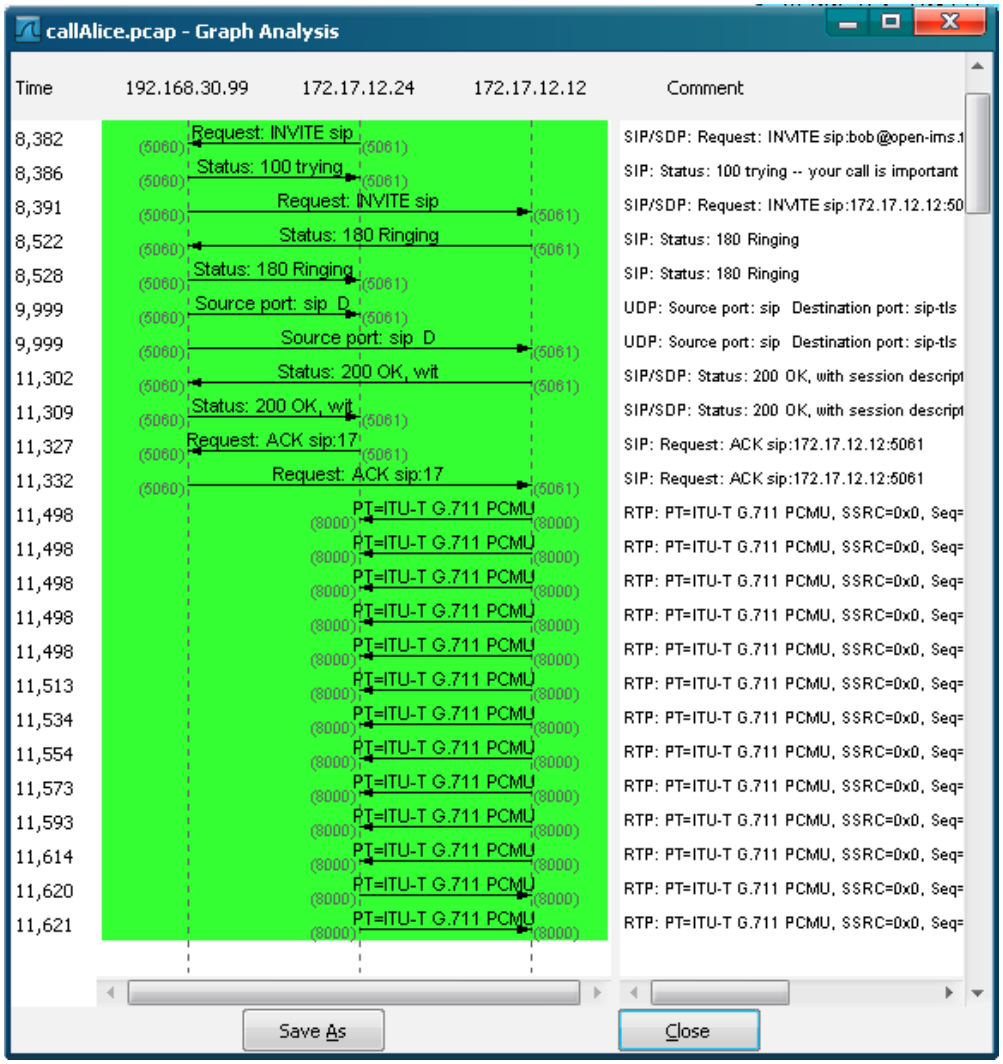

Figura 79. Diagrama de secuencia en el establecimiento de una llamada de VoIP

En la Figura 80 se muestra la finalización de la sesión, la cual se describe a continuación:

10. Alice envía una solicitud SIP BYE hacia el CSCF, el cual posteriormente la reenvía a Bob.

11. Bob responde con un mensaje SIP OK confirmando la finalización de la llamada.

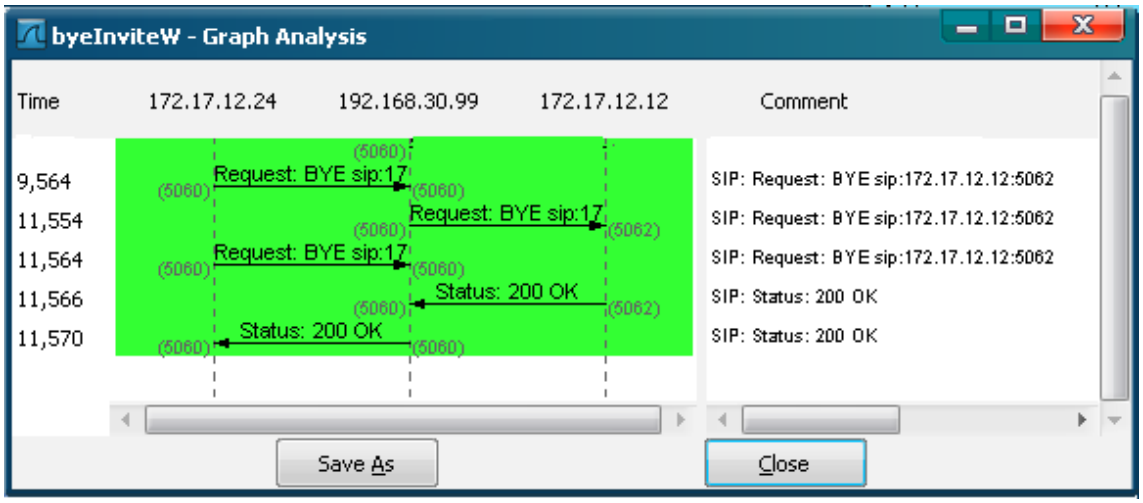

Figura 80. Diagrama de secuencia al finalizar una sesión

Si un atacante captura los paquetes SIP y RTP, puede ver quien realizó la llamada, el tiempo y el estado de la llamada como se ve en la Figura 81. Además si decodifica los paquetes RTP lograría reproducir la llamada (ver Figura 82).

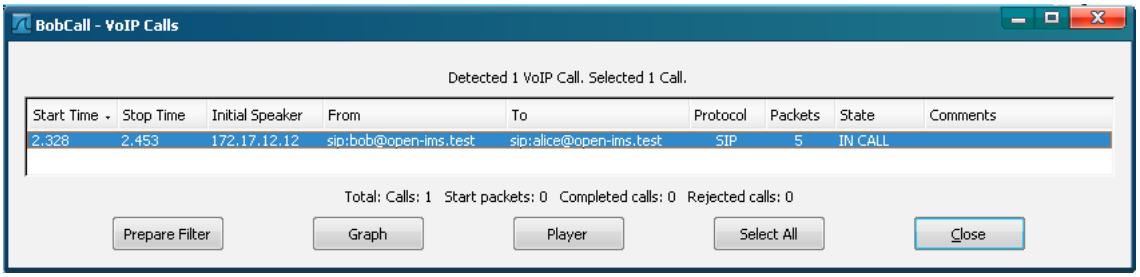

Figura 81. Identificación de llamadas de VoIP

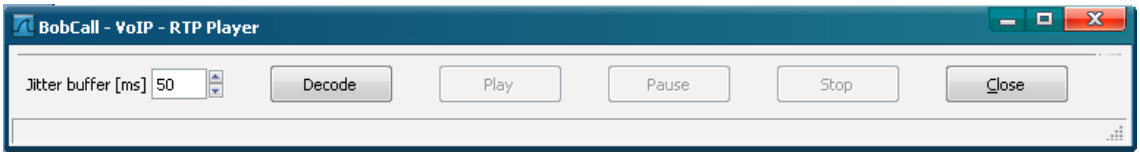

Figura 82. Decodificación y reproducción de la llamada de VoIP

4.2.2. Prueba 2: Verificar la integridad y confidencialidad de una sesión con SA

Esta prueba se realiza con el fin de verificar la integridad y confidencialidad de una sesión con el servicio de telefonía IP. Para comprobar esto primero se realiza el registro a IMS por medio de MidSEG, el cual establece las SA entre el UE y el SMSW.

Cuando se intenta capturar el tráfico del establecimiento de una sesión entre Alice y Bob, con las SA que establece el MidSEG con el SCSWI, la herramienta Wireshark nos muestra que los paquetes están cifrados

con ESP (ver Figura 83), por lo que no se puede asegurar que tipo de datos están cifrados y en este caso no se distinguen los mensajes SIP del flujo RTP.

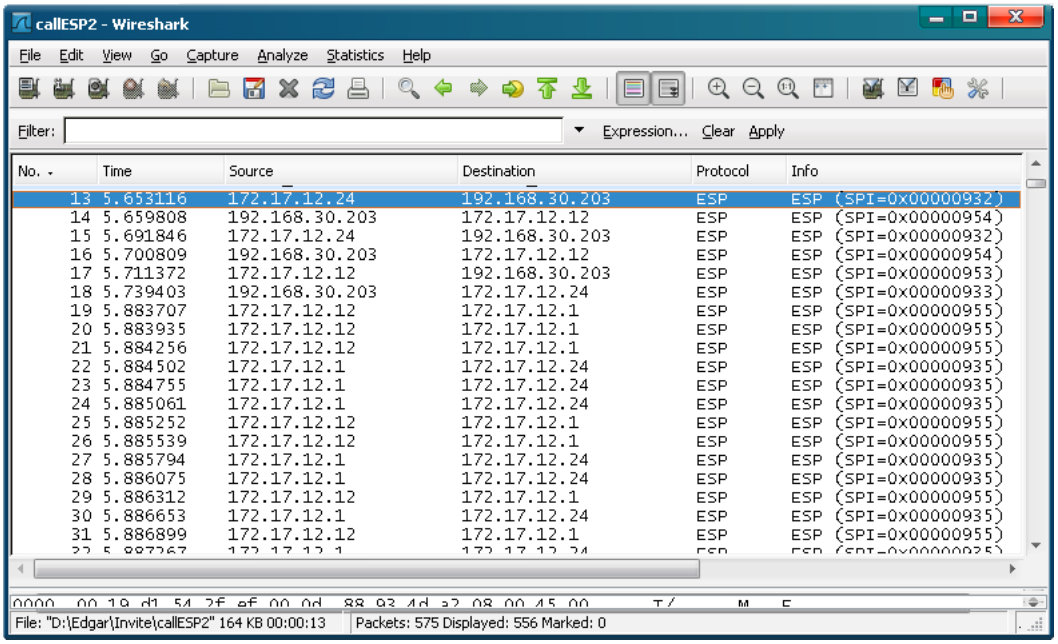

Figura 83. Establecimiento de una sesión de VoIP con SA

De los paquetes capturados no se puede observar quien está realizando la invitación o los parámetros de descripción de sesión que se ven claramente cuando no se usan SA. La Figura 84 nos muestra la secuencia de los paquetes en el establecimiento de una sesión de VoIP entre Alice y Bob. Para garantizar la confidencialidad e integridad del flujo de paquetes RTP entre Alice y Bob se utiliza las SA con la puerta de enlace 172.17.12.1, que tienen como política de seguridad cifrar todos los paquetes y encapsularlos en un túnel entre el UE – 172.17.12.1, por lo que el tráfico RTP entre Bob y Alice ya no se da directamente sino a través de la puerta de enlace que garantiza la confidencialidad e integridad de los paquetes.

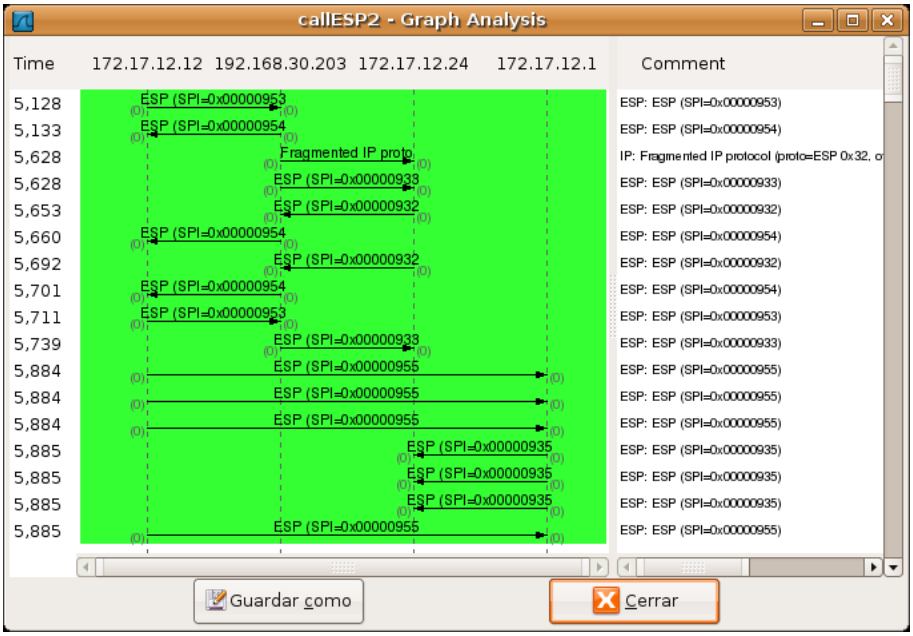

Figura 84. Diagrama de secuencia del establecimiento de una llamada de VoIP con AS

A diferencia de la Figura 79 en la que no se establecen SA, en la Figura 84 aparece la dirección 192.168.30.203 y no la dirección 192.168.30.99, debido a que toda la señalización dirigida hacia el núcleo IMS (192.168.30.99) esta encapsulada en un túnel IPsec entre la dirección IP del SCSWI y la dirección IP 192.168.30.203, esto se puede ver claramente en la Figura 85, la cual muestra el paquete descifrado con dirección IP origen 192.168.30.99 encapsulado por la dirección IP 192.168.30.203.

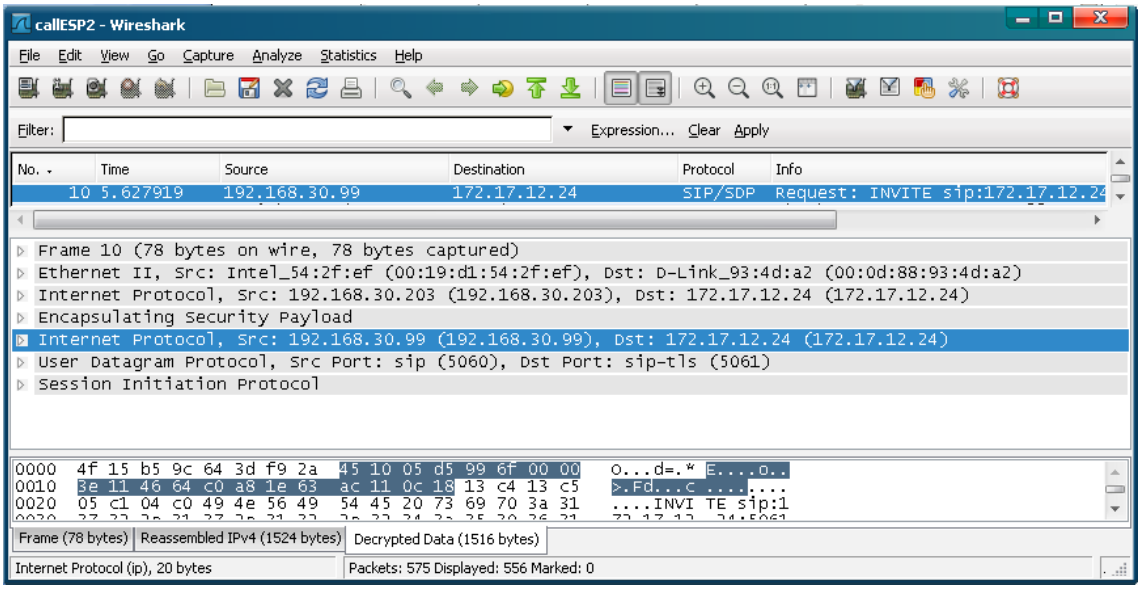

Figura 85. Túnel IPsec

Para proteger la integridad del paquete IP, el protocolo ESP utiliza HMAC, de tal forma que si algún dato del paquete IP es cambiado el receptor obtendrá un HMAC incorrecto por lo que rechaza el paquete.

Si un atacante intenta reconstruir la llamada para reproducirla no lo puede hacer por que los paquetes están cifrados, en la Figura 86 al intentar identificar las llamadas de VoIP de los datos capturados no se obtiene ninguna debido a las SA establecidas entre el SCSWI y el MidSEG.

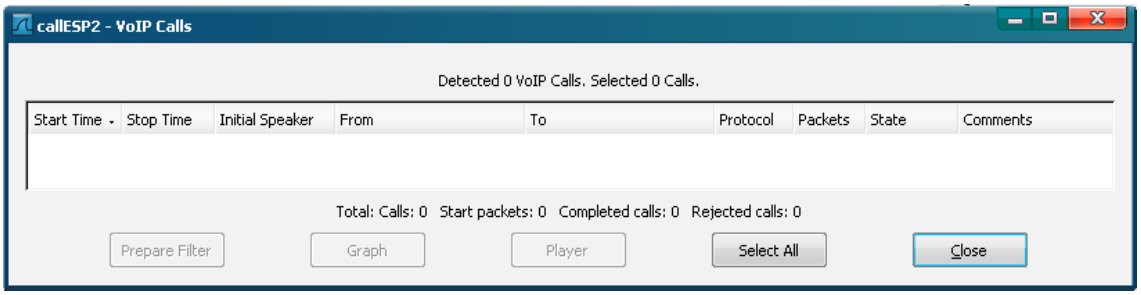

Figura 86. Identificación de llamadas de VoIP con SA

4.3. Conclusiones

- Cuando MidSEG no utiliza SA en una sesión:
  - El trafico SIP capturado es fácilmente comprensible.
  - Se puede reconstruir el flujo de paquetes, por lo que se puede determinar entre quien se establece y que servidor SIP se utiliza.
  - No se garantiza la confidencialidad debido a que cualquiera que capture los paquetes puede ver claramente su contenido.

- Si se decodifica los paquetes RTP entre los UE que se estableció la sesión, se logra reproducir la llamada.

- Cuando una sesión es instalada con SA entre el UE y el MidSEG:
  - No se puede determinar el tipo de paquetes capturados, ya que están cifrados.
  - Garantiza la confidencialidad e integridad de los paquetes, ya que solo pueden ser entendidos entre los que se estableció las SA.
  - No se logra reproducir los paquetes capturados de una llamada debido a que están cifrados.

Capitulo 5

Aportes, Conclusiones y Trabajos futuros

5.1 APORTES

El desarrollo del proyecto trajo consigo una mayor cantidad de aportes que los esperados en el anteproyecto, a continuación se describen cada uno de los aportes logrados y se los clasifica en: arquitectónicos, técnicos y sociales.

5.1.1 Aportes Arquitectónicos

Se definió la arquitectura de referencia de MidSEG para el interworking 3GPP-WLAN (instanciada para IMS), la cual se describe en la sección 3.2 y contribuye en los siguientes aspectos:

- Elección de las opciones y/o recomendaciones de seguridad para incrementar los niveles de seguridad en la comunicación entre el UE y el P-CSCF. Esto se realizó en 3.1 con la caracterización de MidSEG.
- Adaptación a un entorno móvil/inalámbrico 802.11, de 2 puntos de seguridad establecidos para IMS (autenticación mutua entre el UE y el S-CSCF y protección de seguridad al punto de referencia Gm). Con MidSEG la autenticación mutua se sigue realizándo entre el UE y el S-CSCF, pero ahora la señalización es encaminada a través de MidSEG y la seguridad en la comunicación entre el UE y el P-CSCF se garantiza por medio de SA IPsec entre el UE – MidSEG y MidSEG – P-CSCF.
- La arquitectura planteada unifica las autenticaciones a los dominios WLAN, 3GPP e IMS en una sola. Aunque la implementación de referencia no fue probada con otra red 3GPP aparte de IMS el sistema podría funcionar sin mayores cambios debido a que en la caracterización del MidSEG se tuvo en cuenta la entidad PDG, la cual funciona como firewall y enrutador de frontera del dominio 3GPP.
- Autenticación a nivel de servicio, permitiendo que el MidSEG sea independiente de la tecnología de acceso. Esto se logró transportando el protocola AKA en la señalización SIP.
- Control de acceso a los dominios WLAN, 3GPP e IMS. Esto es logrado con: las características de firewall del SSW, la autenticación a nivel IP realizada por IPsec, la gestión de autenticación realizada por el SSP y el resultado de la autenticación del SCSWI.
- Seguridad en la señalización entre el UE y el P-CSCF. Esto se hace con el establecimiento de SA IPsec dinámicas entre: SCSWI-SSW, SSW-SSP y SSP-P-CSCF.
- Protección de la interfaz de radio, para ello se establece una SA IPsec que es utilizada para proteger todo el tráfico.

5.1.2 Aportes Técnicos

En la implementación de referencia del MidSEG se realizaron aplicaciones y configuraciones de herramientas, las cuales son un aporte a la comunidad académica de la facultad para la construcción de aplicaciones de seguridad y de señalización SIP, en un ambiente WLAN-IMS. Estos aportes se describen a continuación:

- Utilización y/o configuración de herramientas de software libre tales como: Núcleo Linux, JDK, Eclipse, JAIN-SIP, ipsec-tools, iptables, OpenIMSCore, raccon, Wireshark, bind9, MySQL y John the Ripper. Las cuales son de código abierto, colaborando en el desarrollo de herramientas de dominio público que ayudan al proceso de enseñanza y aprendizaje de nuevas tecnologías. La utilidad de cada una de las herramientas se puede ver en el anexo B.
- Implementación del protocolo AKA sobre SIP, permite realizar la autenticación a nivel de servicio del SCSWI ante los dominios WLAN e IMS.

- Definición e implementación de la interfaz Java para la configuración de IPsec. Sirve para configurar políticas y SA de IPsec desde una aplicación Java.
- Definición e implementación de la interfaz Java para la configuración del control de acceso en el SSW, con el objetivo de crear un filtro que se modifica desde una aplicación Java.
- Configuración dinámica de IPsec entre el SCSWI y el SSW. Es utilizado para la negociación de las llaves IK y CK a través del de la autenticación AKA y el protocolo SIP.
- Configuración dinámica del filtro a través de la señalización SIP y el resultado de la autenticación AKA. Permite configurar las reglas de control de acceso dependientes del dominio registrado por el SCSWI.

5.1.3 Aporte Social

- A nivel social se aporta en el desarrollo de sistemas de seguridad que permitan aumentar la confianza de los usuarios en los servicios en línea, agilizando el desarrollo de la sociedad de la información.

5.2 CONCLUSIONES

- La seguridad ofrecida en MidSEG a nivel IP se basa en la autenticación mutua entre el UE y el S-CSCF a través del protocolo AKA transportado en la señalización SIP, con la utilización de IPSec.
- La confidencialidad e integridad en la señalización SIP, prestada por MidSEG es alta debido a que utiliza IPsec ESP con autenticación, al cual no se le han encontrado fallas.
- La seguridad de MidSEG es escalable, ya que ante posibles vulnerabilidades encontradas en el algoritmo de cifrado y/o de autenticación utilizado en IPsec, puede ser cambiado por uno mejor.
- Utilizar IPsec garantiza la confidencialidad e integridad en los datos de protocolos pertenecientes a capas superiores IP, haciendo que MidSEG sea una solución independiente a las aplicaciones, esto permite que todo el tráfico en la interfaz inalámbrica sea cifrado (HTTP, FTP, SSH, etc.).
- La unión del filtro TCP/IP con las políticas de seguridad de IPsec garantiza el acceso a los dominios únicamente a los usuarios que están autorizados y autenticados.
- La implementación de referencia del MidSEG es independiente de la tecnología de acceso debido a que la autenticación está en el nivel de servicio.
- Unificar la autenticación a los dominios WLAN, 3GPP e IMS permite reducir: el consumo de recursos de radio, el procesamiento en los dispositivos y el retardo en la autenticación.
- MidSEG aprovecha las SA establecidas entre los clientes y el servidor SMSW para garantizar la confiabilidad e integridad del tráfico (p. Ej: RTP) entre los UE que pertenezcan a la WLAN.
- La definición e implementación de la interfaz java para la configuración dinámica de IPsec permite el aprovechamiento de la seguridad brindada por IPsec de manera transparente para el usuario.

5.3 TRABAJOS FUTUROS

- Evaluar el MidSEG en un ambiente IMS con otras tecnologías de acceso, con el fin de determinar sobre cuales tecnologías el MidSEG es aplicable y realizar adaptación del mismo.
- Explorar la seguridad de la tecnología SIM y su posible aplicación en el SCSWI.
- Proveer al MidSEG de funcionalidades que permitan prestar calidad de servicio.
- Implementación de un middleware de seguridad que garantice la confidencialidad e integridad de la comunicación entre dominios IMS.

Bibliografía

[1] T. Glemser, R. Lorenz. "Seguridad en la Voz sobre IP – Protocolos SIP y RTP", Revista hakin9 No 5, 2005. PP 24-35.

[2] Jorge Ramió Aguirre, "SEGURIDAD INFORMÁTICA", Universidad Politécnica de Madrid, España, Sexta edición, 1 de Marzo 2006.

[3] Siler Amador Donado, Miguel Angel Niño, Andres Flechas. "Seguridad Computacional", Universidad del Cauca 2002.

[4] Carlos Silva Ponce de León, "Seguridad de las Redes y Sistemas de Telecomunicaciones Críticos", Revista de Telecomunicaciones No 116, Octubre/Diciembre de 2008.

[5] 3GPP TS 33.203, "3G security; Access security for IP based services", Release 8, Junio 2008.

[6] D. Celentano, A. Fresa, M. Longer, A.L. Robustelli, "IMPROVED AUTHENTICATION FOR IMS REGISTRATION IN 3G/WLAN INTERWORKING", Personal, Indoor and Mobile Radio Communications, 2007. PIMRC 2007. IEEE 18th International Symposium on Publication Date: 3-7 Sept. 2007. pp 1-5.

[7] C. Ntantogian, C. Xenakis, "REDUCING AUTHENTICATION TRAFFIC IN 3G-WLAN INTEGRATED NETWORKS", Personal, Indoor and Mobile Radio Communications, 2007. PIMRC 2007. IEEE 18th International Symposium on Volume , Issue , 3-7 Sept. 2007. pp. 1–5.

[8] C. Ntantogian, I. Stavrakakis, C. Xenakis, "Reducing the User Authentication Cost in NextGeneration Networks", Wireless on Demand Network Systems and Services, 2008. WONS 2008. Fifth Annual Conference on Publication Date: 23-25 Jan. 2008. pp. 65-72.

[9] L. Veltri, S. Salsano, G. Martiniello, "Wireless LAN-3G Integration: Unified Mechanisms for Secure Authentication based on SIP", Communications, 2006. ICC '06. IEEE International Conference, Volume: 5,.June 2006. pp. 2219-2224.

[10] R. Chen, E. Su, V. Shen, Y. Wang. "Introduction to IP Multimedia Subsystem (IMS)". Articulo de IBM, 12 Sep 2006.

[11] 3G Americas, "IMS Application Enabler and UMTS/HSPA Griwtg Catalyst", http://www.financialtech-mag.com/000_estructura/index.php?ntt=6199&vn=1&sec=25&idb=93, julio 2006.

[12] S. ZNATY, J. Dauphin, R. Geldwerth. "IP Multimedia Subsystem: Principios y Arquitectura". http://www.efort.com/media_pdf/IMS_ESP.pdf

[13] 3GPP TS 23.228, "IP Multimedia Subsystem (IMS)", Release 8, Junio 2008.

[14] A. Villalonga, "Implementación de un servidor proxy SIP en JAVA", Trabajo de fin de carrera, Universidad Politecnica de Cataluya, julio de 2006.

[15] ETSI, "Overview of 3GPP Release 5 Summary of all Release 5 Features",. Junio 2003.

[16] J. Muñoz, X. Velasco, "Cliente móvil SIP para un sistema IVR basado en la arquitectura de servicios IMS", Tesis de Pregrado. Facultad de Ingeniería Electrónica y Telecomunicaciones. Universidad Del Cauca, Popayán, Colombia, 2006.

[17] S. Znaty, J. Dauphin, R. Geldwerth, "SIP : Session Initiation Protocol". http://www.efort.com/media_pdf/SIP_ESP.pdf.

[18] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, E. Schooler, "SIP: Session Initiation Protocol", IETF. RFC 3261, Junio 2002.

[19] 3GPP TS 24.229, "IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP)". Release 8, 2008.

[20] M. Handley, V. Jacobson. "SDP: Session Description Protocol". IETF RFC 2327. Abril 1998

[21] J. Loughney. "Diameter Command Codes for Third Generation Partnership Project (3GPP) Release 5", IETF RFC 3589, September 2003.

[22] S. Tomac, M. Sikirica, L. Skorin-Kapov, and M. Matijasevic, "Implementation of the Diameter-based Cx interface in the IP multimedia subsystem", in Proceedings of the Twenty-nineth International Convention MIPRO 2006, vol. 2, 2006, pp. 109-114.

[23] H. Schulzrinne, S. Casner, R. Frederick, V. Jacobson. "RTP: A Transport Protocol for Real-Time Applications". IETF RFC 1889.

[24] H. Schulzrinne, S. Casner, R. Frederick, V. Jacobson, "RTP: A Transport Protocol for Real-Time Applications". IETF. RFC 3550, julio 2003.

[25] Muhammad Sher, "Secure Service Provisioning (SSP) Framework for IP Multimedia Subsystem (IMS)", Universidad de Berlin,Berlin 2007.
[26] I. Muñiz, "Un Rompecabezas Llamado IMS", cinit – centro de investigación e innovación en telecomunicaciones. Mayo 2007.
[27] Z. Solarte, "Plataforma para Servicios de Facturación y Pago en Ambientes Móviles Ubicuos", Tesis de Maestría. Facultad de Ingeniería Electrónica y Telecomunicaciones. Universidad Del Cauca, Popayán, Colombia, 2009.
[28] J. Cuesta, M. Puñales, "PKI Infrastructura de Clave Pública Seguridad en Redes Telemáticas", 2001, disponible en http://asignaturas.diatel.upm.es/seguridad/trabajos/trabajos/curso%2001%2002/pki.pdf.
[29] M. Lucena "Criptografía y Seguridad en Computadores", Junio de 2001, disponible en http://iie.fing.edu.uy/ense/asign/seguro/Criptografia.pdf.
[30] L. Blunk, J. Vollbrecht, "PPP Extensible Authentication Protocol (EAP)",IETF RFC 2284, Marzo 1998.
[31] Jonas Kullenwall. "Study of security aspects for Session Initiation Protocol". Tesis de maestria, Department of Electrical Engineering Linköping University Abril 2002.
[32] Y. Zhang, M. Fujise,"Security Management in the Next Generation Wireless Networks", International Journal of Network Security, Vol. 3, No.1, pp.1-7, July 2006.
[33] S. Kent, K. Seo, "Security Architecture for the Internet Protocol", IETF RFC 4301, Diciembre 2005.
[34] C. Kaufman, "Internet Key Exchange (IKEv2) Protocol". IETF RFC 4306, Diciembre 2005.
[35] T. Dierks, C. Allen, " The TLS Protocol", IETF RFC 2246, Enero 1999.
[36] IBM España, "Las propuestas de IBM para el desarrollo de la Sociedad de la Información", Enero de 2004
[37] 3GPP TS 23.002, "Technical Specification Group Services and System Aspects; Network architecture, 2007
[38] 3GPP TS 33.210, "Technical Specification Group Services and System Aspects; 3G security; Network Domain Security; IP network layer security", 2007.
[39] S. Muhammad, T. Magedanz, "3G-WLAN Convergence: Vulnerability, Attacks Possibilities and Security Model". The Second International Conference on Volume, Abril de 2007. pp. 198-205.
[40] A. Awais , M. Farooq ,M. Younus, "Attack Analysis & Bio-Inspired Security Framework for IP Multimedia Subsystem", Proceedings of the 10th annual conference on Genetic and evolutionary computation, 2008.
[41] J. Postel, "INTERNET CONTROL MESSAGE PROTOCOL", IETF RFC 792.
[42] J. Postel, "User Datagram Protocol", IETF RFC 768.
[43] Network Working Group," Transmission Control Protocol", IETF RFC 793.
[44] M. Sher, T. Magedanz, "Protecting IP Multimedia Subsystem (IMS) Service Delivery Platform from Time Independent Attacks", Information Assurance and Security, 2007. IAS 2007. Third International Symposium, pp. 171-176, Agosto 2007.
[45] 3GPP TR 22.934, "Feasibility study on 3GPP system to Wireless Local Area Network (WLAN) Interworking", Release 7, Junio 2007.
[46] Chou-Chen Yang; Kuan-Hao Chu; Ya-Wen Yang, "3G and WLAN Interworking Security: Current Status and Key Issues". International Journal of Network Security, Vol.2, No1, Enero 2006. pp. 1-13.
[47] 3GPP TS 23.234. "3GPP system to Wireless Local Area Network (WLAN) interworking". Release 7. Junio 2008.
[48] 3GPP TS 33.234, "3G Security; Wireless Local Area Network (WLAN) Interworking security", Release 8, Marzo 2008.
[49] C. Kaufman, "Internet Key Exchange (IKEv2) Protocol". IETF RFC 4306, Diciembre 2005.
[50] IETF, "Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)". RFC 4187, Enero 2006.
[51] Carlos Serrano. "Modelo Integral para el Profesional en Ingeniería". Popayán: Editorial Universidad del Cauca, 2005.
[52] JDK, disponible en http://java.sun.com, 30 de Marzo de 2009
[53] JainSIP, disponible en https://jain-sip.dev.java.net, 30 de Marzo de 2009.
[54] Ipsectools, disponible en http://ipsec-tools.sourceforge.net/, 30 de Marzo de 2009

[55] MySQL, disponible en http://dev.mysql.com, 30 de Marzo de 2009.
[56] MySQL Connector, disponible en http://dev.mysql.com/doc/refman/5.0/en/connector-j.html, 30 de Marzo de 2009
[57] Iptables, disponible en http://www.netfilter.org/projects/iptables/index.html, 30 de Marzo de 2009
[58] P. Herzog, "OSSTMM - Manual de la Metodología Abierta de Testeo de Seguridad"
[59] Guevara, C.; Mera, F. "Criterios para establecer políticas de seguridad de la información y plan de contingencia, caso de estudio el centro de datos de la universidad del cauca". Tesis de Pregrado. Facultad de Ingeniería Electrónica y Telecomunicaciones, Universidad del Cauca, Popayán, Colombia, Marzo 2008.
[60] Wireshark, disponible en http://www.wireshark.org, 30 de Marzo de 2009.
[61] John The Ripper, disponible en http://www.openwall.com/john/, 30 de Marzo de 2009.
[62] Nmap, disponible en http://nmap.org/, 30 de Marzo de 2009.
[63] CommView for WiFi, disponible en http://www.tamos.com/products/commview/, 30 de Marzo de 2009
[64] S. Kent, R. Atkinson, "IP Encapsulating Security Payload (ESP)", IETF RFC 2406. November 1998.
[65] Open IMS Client, disponible en http://www.open-ims.org/openic, 30 de Marzo de 2009