UNIVERSIDAD POLITÉCNICA SALESIANA
SEDE QUITO

CARRERA:
INGENIERÍA DE SISTEMAS

Trabajo de titulación previo a la obtención del título de:
INGENIEROS DE SISTEMAS

TEMA:
ANÁLISIS Y DISEÑO DE LAS SEGURIDADES SOBRE SISTEMAS DE VOIP MEDIANTE LA IMPLEMENTACIÓN DE SESSION BORDER CONTROLLER SBC Y ENCRIPTAMIENTO DE PAQUETES

AUTORES:
FERNANDO FRANCISCO PAILLACHO UNTUÑA
JOSÉ LUIS YÁNEZ RIVERA

TUTOR:
DANIEL GIOVANNY DÍAZ ORTIZ

Quito, septiembre del 2016

CESIÓN DE DERECHOS DE AUTOR

Nosotros Fernando Francisco Paillacho Untuña y José Luis Yánez Rivera, con documento de identificación N° 1721514618 y 1718780792 respectivamente, manifestamos nuestra voluntad y cedemos a la Universidad Politécnica Salesiana la titularidad sobre los derechos patrimoniales en virtud de que somos autores del trabajo de titulación intitulado: "Análisis y diseño de las seguridades sobre sistemas de VoIP mediante la implementación de Session Border Controller SBC y encriptamiento de paquetes", mismo que ha sido desarrollado para optar por el título de: Ingeniero en Sistemas, en la Universidad Politécnica Salesiana, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente.

En aplicación a lo determinado en la Ley de Propiedad Intelectual, en nuestra condición de autores nos reservamos los derechos morales de la obra antes citada. En concordancia, suscribo este documento en el momento que hacemos entrega del trabajo final en formato impreso y digital a la Biblioteca de la Universidad Politécnica Salesiana.

.....

Fernando Paillacho

Cédula: 172151461-8

.....

José Yánez

Cédula: 1718780792

DECLARATORIA DE COAUTORÍA DEL DOCENTE TUTOR/A

Yo Daniel Giovanny Díaz Ortiz declaro que bajo mi dirección y asesoría fue desarrollado el Proyecto de Titulación, (Análisis y diseño de las seguridades sobre sistemas de VoIP mediante la implementación de Session Border Controller SBC y encriptamiento de paquetes) realizado por (Paillacho Untuña Fernando Francisco y Yánez Rivera José Luis), obteniendo un producto que cumple con todos los requisitos estipulados por la Universidad Politécnica Salesiana, para ser considerados como trabajo final de titulación.

Quito, septiembre de 2016

.....

Daniel Giovanny Díaz Ortiz

CI: 1716975501

AGRADECIMIENTOS

En primer lugar a Dios; en segundo lugar a cada uno de los que son parte de mi familia a mi PADRE, mi MADRE, a mis hermanos; por siempre haberme dado su fuerza y apoyo incondicional que me han ayudado y llevado hasta donde estoy ahora.

FERNANDO FRANCISCO PAILLACHO UNTUÑA.

A Dios, a mi PADRE, A mi MADRE y mi HERMANA por haberme forjado como la persona que soy en la actualidad; muchos de mis logros se los debo a ustedes entre los que se incluye este. Me formaron con reglas y con algunas libertades, pero al final me motivaron constantemente para alcanzar mis anhelos.

JOSÉ LUIS YÁNEZ RIVERA.

Índice

Índice de Figuras

Índice de Tablas

Índice de Anexos

RESUMEN

La telefonía IP es vulnerable a muchos ataques, ya que están expuestas a diferentes riesgos de seguridad como son accesos desautorizados y fraudes, ataques de denegación de servicio, ataques a los dispositivos, vulnerabilidades de la red subyacente, enumeración y descubrimiento, ataques a nivel de aplicación.

Por todos estos y otros problemas de seguridad se desarrollan diferentes métodos de seguridad como hardware y software para proteger la información de la red de las empresas es crítico, por tal razón las empresas realizan grandes inversiones de recursos y esfuerzos en garantizar, la calidad de servicio, sino también la integridad y confidencialidad de la información.

Dado que las redes de VoIP tienen desventajas este proyecto tiene como finalidad el análisis y diseño de la seguridad del tráfico VoIP mediante la implementación de un Session Border Controller (SBC) y el encriptamiento de paquetes de voz.

Para lo cual se utilizó el SBC BLOX que es un software libre que nos permite la ocultación de topología controlar las llamadas que se realizan en la red y también nos sirve de una frontera o un punto de conexión entre una red LAN y el Internet.

Por otro lado el encriptamiento de paquetes de voz puede solucionar problemas de seguridad, para lo cual se utilizara el protocolo SRTP el cual provee confidencialidad e integridad, utilizando un algoritmo de autenticación que protege la integridad del paquete original con una llave maestra utilizando el algoritmo AES-CM de encriptación que no permite el cambio de claves maestras.

ABSTRACT

IP telephony is vulnerable to many attacks as they are exposed to various security risks such as unauthorized access and fraud, denial of service attacks on the devices, vulnerabilities of the underlying network, enumeration and discovery level attacks application.

For these and other security issues different security methods such as hardware and software are developed to protect information network business is critical, for this reason companies make large investments of resources and efforts to ensure quality of service , but also the integrity and confidentiality of information.

Since VoIP networks have disadvantages this project is to design and analysis of VoIP traffic safety by implementing a Session Border Controller (SBC) and encryption of voice packets.

Which was used for the SBC BLOX is a free software that allows us to control topology hiding the calls made on the network and also serves as a border or a connection point between a LAN and the Internet.

On the other hand, the encryption of voice packets can solve security problems, for which the SRTP protocol which provides integrity and confidentiality, using an authentication algorithm that protects the integrity of the original package with a master key using was used the AES-CM encryption that does not allow the change of master keys.

Introducción

La tecnología de VoIP en la actualidad todavía posee vulnerabilidades en varios aspectos, debido que para su funcionamiento depende de algunos factores, como son las capas y los protocolos sobre los que trabaja, así también como la red por la que se transmite su información y los diferentes dispositivos que intervienen en su funcionamiento.

Las llamadas que se realizan en un sistema de VoIP, por lo general se exponen a muchos riesgos de seguridad por el medio en que son transmitidas, sea este Internet o por una intranet de una empresa.

En el presente estudio se realizará un análisis y diseño de las seguridades de los sistemas de VoIP que sufren amenazas como la escucha no autorizada de las llamadas de sus usuarios con la implantación de un Session Border Controller (SBC) y la encriptación de los paquetes de VoIP que se transmiten para poder realizar las llamadas.

Dentro de un entorno de pruebas controlado en el que funcionará un servidor de VoIP levantado sobre Asterisk sin ningún tipo de seguridad, se realizarán una serie de diversos ataques de seguridad como son la intercepción de llamadas, denegación de servicios al servidor VoIP, entre otros diferentes ataques. Con este previo se demostrará la vulnerabilidad que existe dentro de un sistema VoIP y la necesidad que existe de implementar diversos tipos de seguridades junto al mismo.

Posterior a la verificación de las vulnerabilidades se realizarán diferente casos de estudio dentro del mismo escenario implementando por separado cada seguridad al sistema VoIP y constatar que dichas seguridades garanticen la confiabilidad de la información y su rendimiento.

CAPITULO I

1.1 Antecedentes

Voz sobre el protocolo de Internet o Voz sobre IP (VoIP) es un conjuntos de recursos hardware y software que hace posible que la voz viaje a través de la red de datos ya sea esta una intranet o el Internet utilizando el protocolo IP para la comunicación entre los diferentes equipos.

Aunque no existen antecedentes de riesgos en VoIP, ya que, los problemas de seguridad que afectan a esta tecnología son los mismos que siempre han afectado a las redes de datos, se crearon formas de poder mitigar los riesgos sobre dicha red y una de estas es la implementación de una Session Border Controller (SBC), ya sea, de hardware o software para fortalecer la seguridad de la red.

Un Session Border Controller (SBC) es un dispositivo dedicado de hardware o una aplicación de software que rige la forma en que se inicia, conduce y termina una red de voz sobre el protocolo de Internet (VoIP). Dentro del SBC las llamadas se las conoce como sesiones. (Rouse, 2015)

Existen diversos estudios realizados sobre SBC de entre los cuales cabe destacar los siguientes: Implementation and performance of VoIP interception based on SIP Session Border Controller" (Menghui & Hua, 2013)", Method for Implementing Session Border Controller Pool, and Session Border Controller" (Ye & Yu, 2014)"

Otra de las seguridades que se puede implementar sobre una red VoIP es la encriptación sobre los paquetes de voz.

En redes se usa la encriptación para ocultar el contenido de una comunicación de forma que solo los usuarios autorizados puedan ver el contenido real de la comunicación. La

encriptación es una de las maneras de prevenirse de un ataque, desafortunadamente se consume ancho de banda.

Existen múltiples métodos de encriptación: VPN (Virtual Private Network), SRTP (Secure RTP), entre otras. La clave, de cualquier forma, es elegir un algoritmo de encriptación rápido, eficiente, y emplear un procesador dedicado de encriptación.

Entre los trabajos sobre encriptación para VoIP se destacan: Securing Real-Time Sessions in an IMS-Based Architecture (Cennamo, y otros, 2009) e Impacts of Security Protocols on Real-Time Multimedia Communications (Kihun, Souhwan, Lo, & Christoph, 2005)

1.2 Problemática

En la actualidad la tendencia de converger todos los servicios posibles dentro de la red de datos, es el escenario más frecuente que se encuentran las empresas desde PYMES hasta grandes corporaciones, esta convergencia se da debido a la gran reducción de costos al permitir la incorporación de diferentes servicios usando un mismo medio ya existente. Debido a esto es que las redes de VoIP permiten la transmisión de voz/video mediante la red que antiguamente solo permitía datos.

Pero todos estos beneficios traen consigo también problemas, y estos problemas son respecto a la seguridad. La mayoría de los riesgos de seguridad son inherentes de las capas sobre las que se apoya la tecnología VoIP. (Krasheninnikova, 2013, pág. 79)

Las amenazas de las redes de telefonía IP se pueden clasificar en accesos desautorizados y fraudes, ataques de denegación de servicio, ataques a los dispositivos, vulnerabilidades de la red subyacente, enumeración y descubrimiento, ataques a nivel de aplicación. (Krasheninnikova, 2013, pág. 79)

Frente a todos estos y muchos más problemas es que se desarrollan diferentes métodos de seguridad para redes VoIP, ya sean soluciones por software o hardware, lo importante es proteger la información que fluye dentro de la red.

Dada la gran desventaja que sufren las redes de VoIP en lo referente a seguridad el presente proyecto tiene como finalidad la de analizar y diseñar la seguridad del tráfico VoIP mediante la implementación de un Session Border Controller de Software y encriptamiento de los paquetes de voz.

1.3 Justificación

Para la resolución a la problemática ya planteada el presente estudio se centrará en el estudio, configuración e implementación de una Session Border Controller (SBC), además del encriptamiento de paquetes, en un ambiente controlado para el análisis y diseño de las seguridades que puede brindar la misma.

El SBC permite ocultación de topología que limitada la cantidad de información que una topología pueda proporcionar a las partes externas o terceros debido al riesgo de exponer equipos a ataques de denegación de servicio.

La Gestión de Tráfico de Medios es una función del SBC que permite controlar el tráfico de medios, donde los operadores de red pueden requerir esta funcionalidad con el fin de controlar el tráfico que se lleva en su red. La gestión del tráfico ayuda a la creación de diferentes tipos de modelos de facturación (por ejemplo, telefonía de video puede ser un precio diferente de llamadas sólo de voz).

La fijación de desajustes de capacidad permite la comunicación entre los agentes de usuario con capacidades diferentes o extensiones. Por ejemplo, un SBC puede permitir a un agente de usuario SIP simple pueda conectarse a una red 3GPP (3rd Generation Partnership Project – Proyecto de Asociación de Tercera Generación), o habilitar una

conexión entre los agentes de usuario que soporten diferentes versiones de IP, diferentes códecs, o que se encuentran en diferentes dominios de direcciones.

El Session Border Controller también permite el mantenimiento de SIP relacionados con vinculaciones NAT, mediante la generación de tráfico de red periódico. La función NAT transversal del SBC es requerida en escenarios donde el NAT está fuera de la SBC (es decir, no en los casos en que SBC se encuentra como un NAT). Así como el Control De Acceso que permite controlar qué tipo de tráfico de señalización y medios ingresa a su red en el borde de la misma.

El control de acceso se puede basar por ejemplo en identificadores de capa de enlace, direcciones IP o identidades SIP. Además de las funciones ya mencionadas anteriormente los SBC también poseen las funciones de Reparación Protocolo y Media Encryption la misma que a través de otras herramientas se podrá realizar la encriptación de paquetes.

Por otro lado a través del encriptamiento de paquetes de voz se puede solucionar los principales problemas de seguridad que son: la privacidad que se refiere a que la información sólo pueda ser leída por personas autorizadas, la integridad que se refiere a que la información no pueda ser alterada en el transcurso de ser enviada, la autenticación que se refiere a que se pueda confirmar que el mensaje recibido haya sido mandado por quien dice lo mando o que el mensaje recibido es el que se esperaba y el no rechazo que se refiere a que no se pueda negar la autoría de un mensaje enviado.

Para poder realizar la encriptación de paquetes de voz se puede utilizar el protocolo SRTP (Protocolo de transporte seguro en tiempo real) el cual es una extensión del protocolo RTP (Protocolo de transporte en tiempo real), por lo que para este proyecto se utilizará SRTP, el cual fue diseñado con una meta de proveer confidencialidad, integridad y protección del paquete por lo tanto SRTP encripta la

carga útil (voz y video) confidencial, para lo cual SRTP utiliza un algoritmo de autentificación que protege la integridad del paquete original con una MKI (Master Key Identifier / Llave Maestra de Identificación).

SRTP puede crear todas las llaves de autenticación y encriptación que se requiera desde una simple llave maestra. Para la realización de esto utiliza una llave de derivación basado en el algoritmo AES-CM (Encriptación avanzada estándar – Modo Contador en inglés Advanced Encryption Standard-Counter Mode, realiza la encriptación de paquetes de carga útil como la voz y video son del mismo tamaño como del paquete original y permite el procesamiento de paquetes fuera de servicio, lo cual implica también el procesamiento de paquetes en paralelo). Esto es importante pues SRTP no permite el cambio de claves maestras. SRTP no define el intercambio de llave en el algoritmo.

Por lo tanto SRTP es un protocolo de Internet eficiente, conciso que funciona bien y ha logrado una buena interoperabilidad en lo que se refiera a VoIP.

1.4 Objetivos

1.4.1 Objetivo general

Analizar y Diseñar las seguridades sobre los sistemas de VoIP mediante la implementación de Session Border Controller (SBC) y encriptación de paquetes.

1.4.2 Objetivos específicos

Identificar los diferentes sistemas de seguridad que se ofrecen para redes VoIP para la mitigación de brechas de seguridad existentes dentro de las mismas.

Analizar los diferentes SBC que se encuentran actualmente en el mercado ya sea de hardware o software.

Identificar las bondades y vulnerabilidades que permite la encriptación de paquetes dentro de sistemas VoIP.

Implementar un SBC de Software dentro de una red VoIP para su análisis en un ambiente de pruebas.

Utilizar herramientas de análisis de red para comprobar la seguridad que ofrecen los SBC y la encriptación de paquetes dentro de redes VoIP.

Proponer el escenario y la configuración más adecuada para implementar SBC sobre VoIP.

1.5 Marco Metodológico

Dentro del marco metodológico que se usará durante todo el proyecto se propone trabajar con tres tipos de metodologías las cuales son: Metodología de la Investigación, Experimental y Documental, ya que al ser un proyecto de investigación el uso de estas metodologías proveerán más beneficios al mismo.

Para el desarrollo del presente proyecto y debido a que el desarrollo del mismo se lo realizará dentro de ambientes controlados se procederá a utilizar más específicamente la investigación de laboratorio

1.4.1 Metodología de la investigación

La Metodología de la Investigación se considera y se define como la disciplina que elabora, sistematiza y evalúa el conjunto del aparato técnico procedimental del que dispone la Ciencia, para la búsqueda de datos y la construcción del conocimiento científico. (Rodriguez U., 2012)

Una de las clasificaciones de la metodología de la investigación es por el lugar, de la cuales se da el tipo de investigación de laboratorio e investigación de campo.

Investigación de laboratorio: Dado que el máximo objetivo es el control, se realiza en un ambiente controlado (de tipo laboratorio) pues carece de las características propias del ambiente natural. Se crea el ambiente óptimo, es de tipo experimental y emplea metodología cuantitativa. (Leal, 2016)

1.4.2 Metodología experimental

El método hipotético-deductivo, como se conoce habitualmente, implica diversas fases:

En primer lugar el investigador deberá elaborar hipótesis precisas acerca de aquel o aquellos aspectos de la realidad que constituyen su objeto de estudio.

A partir de estas hipótesis, el investigador tendrá que realizar ciertas deducciones.

El investigador deberá comprobar de forma empírica la validez de sus hipótesis y deducciones mediante la realización de estudios específicos a los que se denomina experimentos.

A grandes rasgos, los experimentos pueden ser definidos como situaciones artificiales y totalmente controlados de observación que permiten la contrastación empírica de hipótesis sobre la relación de causalidad.

La capacidad de un experimento para contrastar hipótesis causales viene definida por la posibilidad de manipular de forma reversible ciertas variables (variables independientes), también por el control de otras variables (variables extrañas) y por la observación y medida de los cambios que la manipulación de las variables independientes producen en las variables que se desea explicar (variables dependientes). Cuando la naturaleza de alguna de las variables independientes no permite una manipulación, el diseño de investigación que se aplicara será el de manipulación de las variables independientes por selección. (Psicologia Online, 2015)

1.4.3 Metodología cuantitativa

La metodología cuantitativa utiliza la recolección y el análisis de datos para contestar preguntas de investigación y probar hipótesis establecidas previamente, y confía en la medición numérica, el conteo y frecuentemente el uso de estadística para establecer con exactitud patrones de comportamiento en una población. (López, 2016) Las

características que destacan en la metodología cuantitativa, en términos generales es que esta elige una idea, que transforma en una o varias preguntas de investigación relevantes; luego de estas deriva hipótesis y variables; desarrolla un plan para probarlas; mide las variables en un determinado contexto; analiza las mediciones obtenidas (con frecuencia utilizando métodos estadísticos), y establece una serie de conclusiones respecto de la (s) hipótesis. (López, 2016)

CAPITULO II

Estado del Arte

2.1 Situación actual

Dentro de lo que se refiere a Session Border Controller existen algunos estudios realizados tal como:

"Implementation and performance of VoIP interception based on SIP Session Border Controller", desarrollado por Menghui Yang[1] y Hua Liu[2], en dicho estudio se plantea que: VoIP ha surgido como una solución barata y fácil de implementar. La amplia adopción de VoIP genera un mayor riesgo de violaciones de seguridad generalizadas, y plantea nuevos problemas de seguridad relacionados con la privacidad de las comunicaciones, los servicios unificados y la transparencia de acceso al servicio a través de diferentes redes y carriers.

La intercepción legal es uno de estos temas. Mientras que los servicios de VoIP tienen muchas características deseables de comunicación, también se han convertido en una herramienta para actividades ilegales, por ejemplo los delincuentes pueden comunicarse a través de los servicios de VoIP y evitar ser interceptado por las fuerzas del orden. La intercepción legal desempeña un papel crucial para ayudar a las fuerzas del orden para combatir las actividades delictivas en la red.

[1] Recibió el título grado en Aplicaciones Informáticas en la Universidad de Tecnología Automotriz de Hubei, Shiyan, Hubei, China, en 1994. Recibió sus títulos MS y PhD. en Ciencias de la Computación y la Tecnología de la Universidad de Correos y Telecomunicaciones de Beijing, Beijing, China, en 2001 y 2005, respectivamente. De 2005 a 2007, fue con el Departamento de Ciencia y Tecnología de Computadores de la Universidad de Tsinghua, como becario postdoctoral de investigación. Él era un profesor asociado en el Centro de Información de la Red Informática de la Academia de Ciencias de China, Beijing, China, del 2007-2009.

[2] Recibió el título de grado en Ingeniería de Jardinería en la Universidad de Hainan, Hainan, China, en 1995. Recibió el título de MS en Edición y Publicación de la Universidad Normal de Beijing, Beijing, China, en 2001. Ella es ahora una candidata a un PhD. en la Escuela de la Información de Gestión de Recursos de la Universidad Renmin de China, Beijing. Sus intereses incluyen la gestión de recursos de información, el descubrimiento de conocimiento y de gestión.

En este estudio se propone una arquitectura de intercepción utilizado un Session Border Controller (SBC), y un prototipo de la VoIP Protocolo de Iniciación de Sesión (SIP), para interceptación legal.

La principal contribución de este trabajo es la implementación y la medición de las intercepciones legales de llamadas VoIP basadas en un SIP Session Border Controller. En primer lugar, se presenta la arquitectura para la intercepción legal de llamadas de VoIP basadas en un SIP Session Border Controller y la definición de las interfaces entre SBC y la función de entrega, la función de entrega y la función de recolección. En segundo lugar, se implementará un prototipo de la arquitectura propuesta más adelante. Basado en el prototipo, un banco de pruebas está configurado y algunas pruebas se llevan a cabo con el fin de analizar el rendimiento y la capacidad de las funciones de entidades e interfaces.

La problemática planteada se la soluciono en un escenario que está descrito a continuación:

Propuesta de la Arquitectura

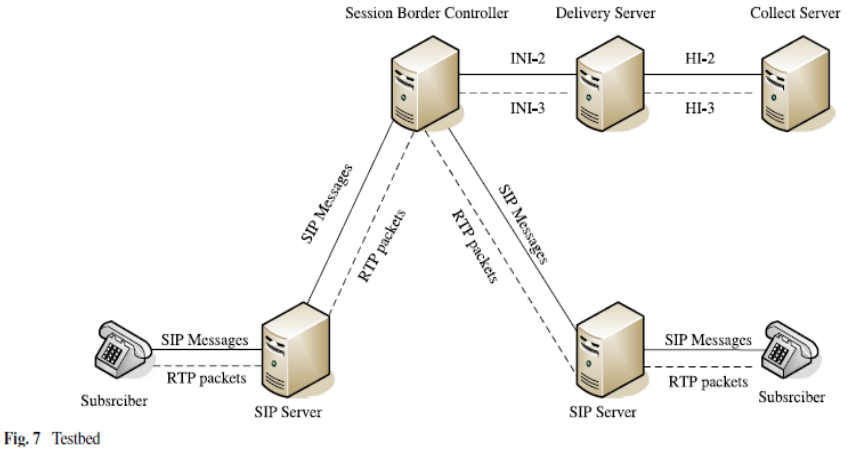

Fig. 7 Testbed

Figura 1. Arquitectura usada en el desarrollo de la investigación
Fuente: (Menghui & Hua, 2013)

La plataforma de pruebas se muestra en la Fig. 1. En el entorno de prueba, se está utilizando el OpenSBC como SBC, este es un software Agente de Usuario Back-to-back (B2BUA, es un elemento de la red lógica en aplicaciones SIP) de código abierto, que utiliza OpenSIPStack como su pila de protocolos subyacente, con las funciones

básicas de la B2BUA. Con el fin de llevar a cabo la intercepción, se implementó interfaces INI en OpenSBC al añadir algunas funciones. La persona que llama y el destinatario están utilizando SIP. El SBC como servidor de entrega y LEA (Law Enforcement Agency) se despliega en tres servidores Blade IBM HS21 con 120 GB de disco duro, 2.048 MB de memoria y Redhat Linux OS, respectivamente.

La suite de software Asterisk se utiliza como un servidor SIP que se desplegó en unos servidores Blade IBM HS21 con disco duro 120G, 2048 MB de memoria y Redhat Linux OS.

En conclusión sobre el estudio realizado se puede apreciar lo descrito a continuación:

En este estudio se propuso una arquitectura de intercepción usando SBC que proporciona intercepción legal para SIP VoIP, este prototipo fue completamente implementado en la arquitectura de intercepción propuesta.

Se creó un banco de pruebas y dichas pruebas se llevaron a cabo con el fin de analizar el rendimiento y la capacidad de las funciones de entidades e interfaces.

Los resultados del ensayo indicaron que la capacidad de interceptación SBC en los mensajes SIP fue superior a la del stream de RTP.

Con el fin de eliminar el posible cuello de botella de los paquetes interceptados de RTP en SBC, se investigó el mecanismo en el que paquetes de tráfico RTP fueron compartidos entre diferentes funciones de los medios de SBC en OpenSBC.

Los resultados del análisis indican que varias funciones de entidades de los medios de SBC pueden compartir la llegada de paquetes RTP, y podría significativamente disminuir del tiempo de servicio de paquetes RTP en SBC.

Por otra parte el estudio que se publicó para aplicar a ser una patente es: “Method for Implementing Session Border Controller Pool, and Session Border Controller” (Sihai Ye y Qinghua Yu ambos creadores de una gran variedad de patentes para Huawei

Technologies Co., Ltd.), que es la continuación a una patente previa llamada “Method for Enabling Session Border Controller (SBC) pool and SBC” de los mismos autores. Como problemática a resolver en el presente estudio se tiene: para evitar la interrupción de servicios, dispositivos de respaldo generalmente son proporcionados a partir de algunos dispositivos de procesamiento clave en la red.

Además, para cumplir con los requisitos de fiabilidad de la red, un dispositivo de respaldo generalmente necesita ser desplegado en una zona remota. Por consiguiente, la red tiene un requisito para una solución de recuperación de desastres remota para los dispositivos en la misma.

En el arte previo, SBC generalmente provee servicios en modo activo/espera, y dos direcciones IP diferentes se proporcionan para un dispositivo SBC activo y un SBC en espera respectivamente. Una pareja de dispositivos, por ejemplo, un dispositivo terminal o un softswitch en una red cercana, están configurados con direcciones IP de los SBC activos y en espera, y determinan, mediante sondeo separado las dos direcciones IP, si el SBC activo y el en espera están trabajando normalmente.

En un caso normal, la pareja de dispositivos acceden a la dirección de IP del dispositivo SBC activo, e implementa un servicio relacionado utilizando el dispositivo SBC activo; al percibir que el dispositivo SBC activo esta defectuoso, la pareja de dispositivos cambia al dispositivo SBC en espera automáticamente para continuar los servicios correspondientes, a fin de aplicar la recuperación de desastres de dispositivo SBC. Tal solución de recuperación de desastres SBC tiene un requisito especial para la pareja de dispositivos (por ejemplo, un dispositivo de terminal), es decir, el dispositivo de pares necesita ser configurado con dos direcciones IP. En una situación normal, uno de los dos dispositivos se selecciona como un dispositivo activo, y después de que se detecta que el dispositivo activo es anormal, el dispositivo de pares

cambia automáticamente a un dispositivo de copia de seguridad. Además, el dispositivo de copia de seguridad está por lo general en un estado de inactividad, y sólo se utiliza cuando el dispositivo activo es defectuoso, lo que provoca una tasa de utilización de recursos bajo.

Para la resolución de la problemática anterior se tiene que el presente estudio proporciona un método para la implementación de un pool de SBC y un SBC, a fin de evitar recuperación de desastres en un SBC a partir de la colocación de un requerimiento especial por parte de un dispositivo terminal, y el incremento de la tasa de utilización de recursos.

Dicho método para la implementación de un pool SBC, incluye: recepción, por parte de un SBC en el pool SBC, mensajes de servicio de un dispositivo terminal, y determinar si el dispositivo terminal está registrado en el pool SBC, donde el pool SBC incluye al menos 2 SBCs, y los SBCs en el pool SBC se comunican con el dispositivo terminal usando una misma dirección IP; y reenvío de mensajes de servicio a un SBC con el que el dispositivo terminal se ha registrado siempre y cuando el dispositivo terminal haya sido registrado en el pool SBC, de modo que el SBC con el dispositivo terminal está registrado procese los mensajes de servicio. De esta manera, se evita la recuperación de desastres de los dispositivos SBC.

Esquema de Trabajo

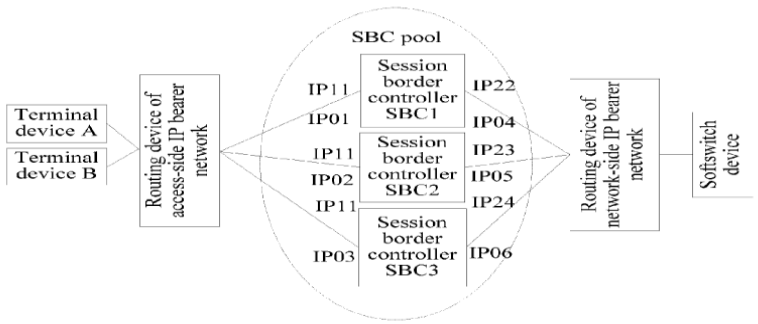

Figura 2. Esquema propuesto para el desarrollo del nuevo método
Fuente: (Sihai Ye, Qinghua Yu)

Continuando con otros estudios previos sobre sistemas VoIP y principalmente sobre el encriptamiento de paquetes multimedia esta: “Securing Real-Time Sessions in an IMS-Based Architecture” desarrollado por: Paolo Cennamo, Antonio Fresa, Maurizio Longo, Fabio Postiglione, Anton Luca Robustelli y Francesco Toro.

En este estudio se describe que: las infraestructuras emergentes de redes móviles totalmente IP basadas en la filosofía de tercera generación de subsistemas multimedia IP se caracterizan por su independencia a la tecnología de radio acceso y a la conectividad ubicua para usuarios móviles.

Actualmente, un gran número de profesionales de networking o afines está enfocándose a temas de seguridad, ya que la mayoría de las amenazas en una red actualmente se ven afectadas por su conexión hacia el dominio público de Internet; y los siguientes que sufrirán por esto serán los usuarios de redes móviles en los próximos años. Mientras que una gran cantidad de actividades de investigación, junto con los esfuerzos de normalización y experimentaciones, se lleva a cabo en los mecanismos de señalización de protección, se han propuesto muy pocos marcos integrados para la protección de datos multimedia en tiempo real en un contexto de IP Multimedia Subsystem (IMS), y menos aún experimental basados en resultados de bancos de pruebas están disponibles. En este trabajo, después de un panorama general de los problemas de seguridad que surgen en un escenario avanzado Subsistema Multimedia IP (IMS), una infraestructura integral para la protección de datos multimedia en tiempo real, basado en la adopción del protocolo seguro en tiempo real, se propone; entonces, el desarrollo de un banco de pruebas para la incorporación de este tipo de funcionalidades, incluyendo mecanismos para la gestión de claves y la transferencia de contexto criptográfico, y permitiendo la configuración de las sesiones de Protocolo de Tiempo Real Seguros (SRTP) se presenta; Finalmente, los resultados

experimentales se proporcionan junto con las evaluaciones cuantitativas y comparaciones de las actuaciones del sistema para sesiones de audio con y sin la aprobación del marco del Protocolo de Tiempo Real Seguro.

El escenario que fue propuesto para el desarrollo de dicho trabajo esta descrito a continuación:

Arquitectura IMS

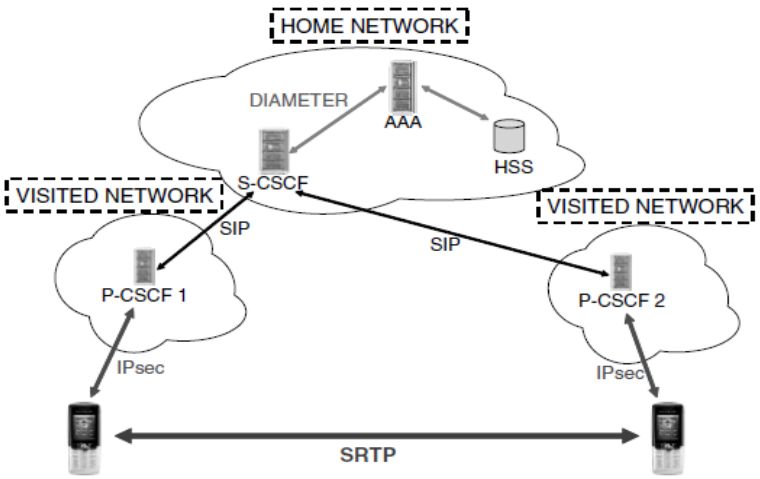

Figura 3. Arquitectura propuesta basada en IMS para las comunicaciones multimedia seguras
Fuente: (Cennamo, y otros, 2009)

El prototipo IMS que se representa en la figura 2, donde se incluyen dos teléfonos móviles que están conectados a la red doméstica IMS (es decir, con el servidor S-CSCF) a través de los nodos P-CSCF (Proxy CSCF, primer punto de contacto del teléfono móvil con la red IMS, desde la perspectiva de señalización.) de red visitada de cada usuario móvil. La Autenticación, Autorización servidor, accounting (AAA) se introduce de acuerdo a la arquitectura IMS definido por el 3GPP. En el escenario de la red representada, cuando un usuario cambia su teléfono móvil en una fase de registro se lleva a cabo mediante el protocolo AKA encapsulado dentro de los mensajes SIP REGISTER. Este protocolo permite una autenticación mutua (que es el usuario y la red autenticarse entre sí): a través de este procedimiento cada usuario independientemente calcula las claves criptográficas y de integridad que serán utilizados en comunicaciones seguras posteriores. Además, durante la fase de registro

se establece una asociación de seguridad IPsec entre cada usuario y su referencia P-CSCF a fin de garantizar una fuerte protección para los mensajes de señalización SIP subsiguientes.

La introducción de la técnica de la criptografía en tiempo real para multimedia fluye con la adopción del protocolo SRTP que está dirigido a garantizar un buen nivel de seguridad en las comunicaciones multimedia.

Uno de los mecanismos que ofrecen un buen nivel de robustez frente a las tipologías *two time pad* de ataques es la introducción de un mecanismo de actualización de clave periódica. En esta propuesta el mecanismo de actualización hacia la señalización SIP IMS no introduce ningún aumento del número de mensajes intercambiados, ya que puede ocurrir que se aprueba un Maestro identificador de clave o un mecanismo (From, Cabecera que contiene la URI del que origina la petición; To, Cabecera que contiene la URI del destino de la petición).

La calidad de la comunicación no llega a ser degradada a pesar de que se aplica una criptografía en tiempo real. En particular, el marco SRTP no influye en la calidad de la voz durante las comunicaciones de VoIP, tanto en términos de retardo y el índice de PESQ-LQ.

La evolución futura se referirá, en primer lugar, al establecimiento práctico de una sesión SRTP también para el contenido de vídeo entre dos usuarios en el prototipo IMS.

Otro desarrollo futuro estará relacionado con la adaptación de la solución arquitectónica presentada en la figura 3 pero enfocado a un escenario multi-conferencia.

2.2 Marco Teórico

2.2.1 Voip

"Voz sobre IP" es la abreviatura de "Voz sobre Protocolo de Internet" ("Voice Over Internet Protocol" en inglés) y es mundialmente conocido como VoIP y se refiere a la transmisión del tráfico de voz sobre redes basadas en Internet en lugar de las redes telefónicas tradicionales PSTN (red telefónica pública conmutada). El protocolo de Internet (IP) fue diseñado originalmente para redes de transición de datos, y debido a su gran éxito fue adaptado a las redes de voz mediante la paquetización de la información y transmisión de la misma como paquetes de datos IP. VoIP está disponible en muchos teléfonos inteligentes, computadoras personales y en los dispositivos de acceso a Internet, tales como tabletas.

La transmisión de VoIP puede facilitar muchos procesos y servicios que normalmente son muy difíciles y costosos de implementar usando la tradicional red de voz PSTN y se puede transmitir más de una llamada sobre la misma línea telefónica. (Valle, 2015, pág. 1).

Con la tecnología que ofrece VoIP las comunicaciones unificadas son posibles, ya que permite la integración de otros servicios disponibles tales como video conferencias, mensajes instantáneos, etc.

Estas y muchas otras ventajas de voz sobre IP están haciendo que las empresas actualmente adopten Centrales Telefónicas VoIP a un paso apresurado. (Valle, 2015, pág. 1)

VoIP y las comunicaciones unificadas permiten:

Reducir los gastos de desplazamiento y formación, mediante el uso de videoconferencias y conferencias en línea.

Actualizar su sistema telefónico de acuerdo a sus necesidades.

Tener un número de teléfono que suena a la vez en varios dispositivos, para ayudar a sus empleados a estar conectados entre sí y con sus clientes.

Reducir sus gastos telefónicos. (Arcos Gaón, 2016, pág. 2)

Utilizar una sola red para voz y datos, simplificando la gestión y reduciendo costes.

Acceder a las funciones de su sistema telefónico en casa o bien en las oficinas de sus clientes, en aeropuertos, hoteles o en cualquier parte donde haya una conexión de banda ancha. (CISCO, 2010)

2.2.1.1 Seguridades sobre el protocolo ip

A medida que crece su popularidad aumentan las preocupaciones por la seguridad de las comunicaciones y la telefonía IP. (Caceres Guayanlema, 2014, pág. 27) VoIP es una tecnología que por su estructura se apoya en muchas otras capas y protocolos ya existentes de las redes de datos. Por eso en cierto modo la telefonía IP hereda ciertos problemas de las capas y protocolos ya existentes, siendo algunas de las amenazas más importantes de VoIP problemas clásicos de seguridad que afectan al mundo de las redes de datos. Por supuesto, existen también multitud de ataques específicos de VoIP como se describirán más adelante. (Krasheninnikova, 2013, pág. 19)

Capas y Protocolos

Figura 4. Esquema de las diferentes capas y protocolos en los que se apoya VoIP
Fuente: (Krasheninnikova, 2013, pág. 19)

La siguiente tabla muestra de forma general las vulnerabilidades que posee cada capa:

Tabla 1.
Tabla de Vulnerabilidades de las Capas en las que se apoya VoIP

Capa	Ataques y vulnerabilidades
Políticas y Procedimientos	Contraseñas débiles. Ej. Contraseña del VoiceMail Mala política de privilegios Accesos permisivos a datos comprometidos.
Seguridad Física	Acceso físico a dispositivos sensibles. Ej. Acceso físico a un gatekeeper. Reinicio de máquinas. Denegaciones de servicio.
Seguridad de Red	DDoS ICMP unreacheable SYN floods Gran variedad de floods
Seguridad en los Servicios	SQL injections Denegación en DHCP DoS
Seguridad en el S.O.	Buffer overflows Gusanos y virus Malas configuraciones.
Seguridad en las Aplicaciones y protocolos de VoIP	Fraudes SPIT (SPAM) Vishing (Phising) Fuzzing Floods (INVITE, REGISTER, etc...) Secuestro de sesiones (Hijacking) Interceptación (Eavesdroping)

	Redirección de llamada s (CALL redirection) Reproducción de llamadas (CALL replay)

Fuente. (Krasheninnikova, 2013, pág. 20)

Cada una de las vulnerabilidades descritas anteriormente afecta de manera directa o indirecta al sistema de VoIP.

DoS.- Significa "Denial of Service" en inglés, y traducido al español se conoce como "ataque de denegación de servicios". Sólo necesitan un ordenador y una conexión a Internet para abrumar el ancho de banda y recursos de un objetivo. (González, 2016)

DDoS.- Significa "Distributed Denial of Service" en inglés, y traducido al español se conoce como "ataque distribuido de denegación de servicios". Este tipo de ataque consiste en un grupo de sistemas que atacan a un solo objetivo para causar una denegación de servicios a usuarios legítimos. (IPNET, 2014)

SQL Injection.- Es un método que se vale de la vulnerabilidad en el código de una aplicación a nivel de validación de operaciones sobre una base de datos.

Buffer overflows.- (desborde de memoria) Se produce cuando un programa informático excede el uso de cantidad de memoria asignado por el sistema operativo, es producido por un error de sistema causado por un defecto de programación, de tal forma que lo sufre escribe más información en memoria.

Phising.- Es un ataque de "ingeniería social" a través de email o mensajería instantánea caracterizado por intentos fraudulentos de adquisición de información sensible mediante suplantación.

Gusanos.- Programas auto-contenidos con capacidad de propagación sin la intervención humana.

Virus.- Programas con capacidad de replicación, cuya actividad se hace patente, es un malware que tiene por objeto alterar el normal funcionamiento de la computadora, sin el permiso o el conocimiento del usuario, infecta a medida que se transmite.

Hijacking.- en español "secuestro" se refiere a toda técnica ilegal que lleve a adueñarse o robar algo (información) por parte de un atacante, se puede aplicar a varios ámbitos de esta manera podemos encontrar el secuestro de conexiones de red, sesiones de terminal, servicios, módems y un largo de servicios informáticos.

Eavesdroping.- Este término es utilizado cuando se realiza una intrusión de escuchar secretamente una conversación sin el consentimiento de las partes; el mismo se ha utilizado tradicionalmente en ámbitos de seguridad en networking.

Pharming.- Es la explotación de una vulnerabilidad en servidores DNS que permite a un "hacker" usurpar un nombre de dominio y redirigir todo el tráfico web legitimo a otra ubicación.

2.2.1.2 Arquitectura de voz sobre ip

El propio Estándar define tres elementos fundamentales en su estructura:

Terminales: son los sustitutos de los actuales teléfonos. Se pueden implementar tanto en software como en hardware.

Gatekeepers: son el centro de toda la organización VoIP, y son el sustituto para las actuales centrales. Normalmente implementan por software, en caso de existir.

Gateways: se trata del enlace con la red telefónica tradicional, actuando de forma transparente para el usuario. (Barcia Esparza, 2015, pág. 14)

Arquitectura VoIP

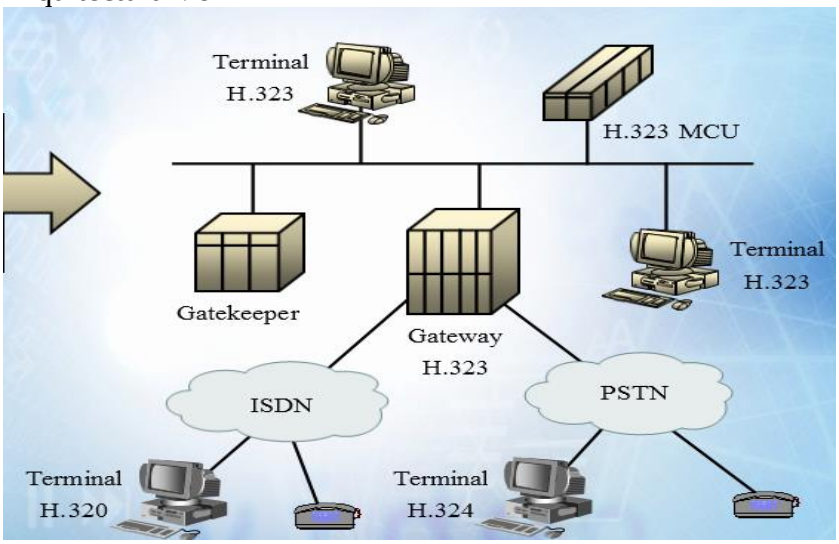

Figura 5. Componentes de la Arquitectura VoIP
Fuente: (Cisco, 2009)

Con estos tres elementos, la estructura de la red VoIP podría ser la conexión de dos delegaciones de una misma empresa. La ventaja es inmediata: todas las comunicaciones entre las delegaciones son completamente gratuitas. Este mismo esquema se podría aplicar para proveedores, con el consiguiente ahorro que esto conlleva. (Barcia Esparza, 2015, pág. 14)

Protocolos de VoIP: son los lenguajes que utilizarán los distintos dispositivos VoIP para su conexión. Esta parte es importante ya que de ella dependerá la eficacia y la complejidad de la comunicación.

Por orden de antigüedad (de más antiguo a más nuevo):

H.323 – Protocolo definido por la ITU-T;

SIP – Protocolo definido por la IETF;

Megaco (También conocido como H.248) y MGCP – Protocolos de control;

UNIStim – Protocolo propiedad de Nortel(Avaya);

Skinny Client Control Protocol – Protocolo propiedad de Cisco;

MiNet – Protocolo propiedad de Mitel;

CorNet-IP – Protocolo propiedad de Siemens;

IAX – Protocolo original para la comunicación entre PBXs Asterisk (Es un estándar para los demás sistemas de comunicaciones de datos, actualmente está en su versión 2, IAX2);

Skype – Protocolo propietario peer-to-peer utilizado en la aplicación Skype;

IAX2 – Protocolo para la comunicación entre PBXs Asterisk en reemplazo de IAX;

Jingle – Protocolo abierto utilizado en tecnología XMPP;

MGCP- Protocolo propietario de Cisco;

weSIP - Protocolo licencia gratuita de VozTelecom. (Rodriguez Espinoza, 2015, págs. 1-2)

2.2.1.3 Protocolo SIP

SIP Protocolo de Inicio de Sesión, es un protocolo desarrollado por IETF que se especifica en la RFC 3261. Este protocolo permite crear, modificar y terminar sesiones en una red IP permitiendo localizar usuarios para cambiar información de voz, videoconferencias, aplicaciones, etc. Es independiente del protocolo de transporte (UDP, TCP).

El protocolo SIP utiliza seis tipos de solicitudes:

INVITE: Establece una sesión.

ACK: Confirma una solicitud INVITE.

BYE: Finaliza una sesión.

CANCEL: Cancela el establecimiento de una sesión.

REGISTER: Comunica la localización del usuario (nombre de equipo, IP).

OPTIONS: Comunica información acera de los métodos y extensiones soportadas por un teléfono SIP.

2.2.2 Sistemas de seguridad para voip

En VoIP las medidas de seguridad deben implantarse a diferentes niveles. Los servidores de telefonía IP tienen que estar protegidos por sistemas operativos especialmente eficaces, además de firewalls y detectores de virus. Realizar un cifrado SIPS y SRTP resulta crucial para garantizar que las comunicaciones sean seguras. Sin embargo, es necesario que el propio teléfono soporte estos protocolos.

Por estas razones existen diversos tipos de sistemas o dispositivos para proporcionar seguridad en redes de VoIP. (Mayr, 2015)

2.2.2.1 SIP proxy

Un SIP Proxy es un servidor que sirve para redirigir paquetes SIP, esto es, recibe un paquete SIP de una IP y lo reenvía a otra IP. Solo paquetes SIP, ni audio, ni vídeo, ni códecs, ni nada. Normalmente el SIP Proxy puede leer y comprender los datos que vienen dentro del paquete SIP para obtener el usuario, la contraseña, etc. y poder autentificar ese usuario y reenviarlo si es un usuario válido o eliminar el paquete si no lo es. Un SIP Proxy es como un router, pero exclusivamente de paquetes SIP. Podemos cambiar el destinatario, contar cuantos INVITE ha enviado, aunque su verdadero poder reside en las miles de cosas más que puede hacer. (Guamán Ullauri, 2015, pág. 115)

2.2.2.2 Firewall

Otro de los sistemas de seguridad que pueden implementarse para VoIP y que puede ser utilizado para este tipo de infraestructura es un firewall, el mismo se encarga principalmente de la seguridad de una red de datos, pero puede ser configurado para trabajar en redes de voz y datos simultáneamente o por separado si se cuenta con la infraestructura adecuada.

Un cortafuegos o firewall es un sistema de defensa basado en el hecho de que todo el tráfico de entrada o salida a la red debe pasar obligatoriamente por un sistema de

seguridad capaz de autorizar, denegar, y tomar nota de todo aquello que ocurre, de acuerdo con una política de control de acceso entre redes.

Controla tanto la comunicación desde el exterior como el tráfico generado desde la propia máquina o red interna. Actúa en base a normas que establece el administrador de seguridad o, en su defecto, el administrador de red o el usuario final. Dichas reglas definen las acciones correspondientes a llevar a cabo cuando se recibe un paquete que cumpla unas determinadas características.

2.2.2.3 Session border controller

Inicialmente los Session Border Controller (SBC) eran máquinas dedicadas situadas en las fronteras entre redes de proveedores hacia clientes o hacia Internet, que evolucionaron hacia una virtualización, en ocasiones integrada con firewall y routers. (Gil, 2015)

SBC proporcionan seguridad, interoperabilidad, enrutamiento y otras funciones en una red de protocolo de inicio de sesión (SIP). Sin embargo, no todos los SBC son creados iguales, y no todos los clientes de SBC tienen las mismas necesidades respecto a seguridad.

Características y Funciones

Aunque la seguridad suele ser la característica principal de un SBC, no es ni mucho menos la única. Entre otras funciones, el SBC también se suele encargar de:

La interoperabilidad asegurar el establecimiento de sesiones, incluso en el caso de elementos de la red interna y externa con señalizaciones distintas (por utilizar diferentes versiones de SIP, por requerir en uno de los lados una seguridad adicional, o por utilizar protocolos de señalización distintos).

La gestión del plan de numeración permitiendo conexiones legítimas y evitando intrusiones y ataques.

La transcodificación, adapta códecs en caso de que el códec usado por la sesión interna y por la sesión externa no coincidan.

El control de admisión limita el número de sesiones establecidas para no sobrepasar el límite soportado por la línea WAN.

La conectividad de usuarios remotos, por ejemplo mediante VPN.

La gestión de la Calidad del Servicio. (Gil, 2015)

2.2.2.3.1 Tipos de session border controller

Existen en el mercado varios tipos de SBC pero de manera macro se los puede clasificar en 2 grupos que son SBC por Hardware y Software.

Dentro de los SBC por Hardware se tiene diferentes equipos de diferentes marcas y cada uno varía dependiendo de las necesidades de cada cliente. Aquí dentro de este grupo también se los puede clasificar por SBC de Clase Carrier y SBC Empresariales.

En lo que refiere a SBC por Software el más común a encontrar es el Virtualized SBC, que no es más que una máquina virtual para trabajar del mismo modo que lo haría un SBC físico.

Dentro de este tipo de Session Border Controller están: Vega Software Enterprise SBC (Virtual Machine) de **Sangoma**, BorderNet Virtualized SBC de **Dialogic**, Virtualized SBC (SWe) de **Sonus, BLOX,** etc.

Para lo cual se optó por trabajar con BLOX pues en primera instancia es Open Source y se adapta a las necesidades requeridas para poder cumplir con los objetivos propuestos para este estudio.

BLOX es un Session Border Controller (SBC) utilizado para controlar la señalización de VoIP y flujos de medios. SBC es responsable de la creación, la realización, y derribado de las llamadas. SBC permite a los propietarios para controlar los tipos de llamadas que se pueden colocar a través de las redes y también superar algunos de los

problemas causados por los cortafuegos y NAT para llamadas VoIP. Un lugar común para un independiente SBC es un punto de conexión, llamada una frontera, entre una red privada de área local (LAN) y la Internet. SBC vigila el tráfico de voz en tiempo real entre las fronteras de la red IP, lo que garantiza su red privada es robusta segura y totalmente manejable.

Características:

SBC está habilitada con el DIP Packet Inspection en el tráfico de VoIP, el apoyo a las firmas de malware clave / vulnerabilidades observadas en implementaciones SIP como extensiones Enumeración DoS y Password Cracking. Apoyo a las PBX de código abierto como Asterisk, FreeSwitch, Trixbox.

Maneja los asuntos SIP-NAT observados en los despliegues de VoIP comunes.

Función de la topología-escondite es prevenir a los clientes u otros proveedores de servicios de aprender detalles sobre la configuración de la red interna, o cómo las llamadas de ser colocado a través de la SBC se encaminan.

La transcodificación - SBC también pueden permitir que las llamadas VoIP que se creará entre dos teléfonos de transcodificación de la corriente de los medios de comunicación, cuando diferentes códec están en uso.

TLS / SRTP - apoyo a la señalización y el cifrado de los medios de comunicación.

Basada en políticas de enrutamiento de llamadas, incluyendo manivela trasera de establecimiento de llamada.

2.2.2.4 Encriptamiento de los paquetes voip

Dentro de lo que es el encriptamiento para los sistemas VoIP se puede mejorar la seguridad y confianza de la red mediante técnicas de encriptación. La encriptación se la puede hacer a dos niveles:

Señalización: mediante protocolo TLS. Ante una eventual intrusión, no se conocen datos de la llamada (códecs, número A/B, IP's, etc…)

Media: mediante protocolo SRTP. Impide la escucha de llamada en caso de captura del flujo, que es relativamente sencillo.

La encriptación puede ser realizada en varios puntos, en el IP TRUNK entre clientes y operadores, en escenarios de acceso donde los clientes se registran contra un softswitch.

SRTP (Secure Real Time Protocol) encripta el audio, por lo que favorece la seguridad pero puede dificultar tareas de troubleshooting. Debe ser usado siempre con TLS para que sea realmente útil. (Quobis, 2012).

Dentro del presente estudio la configuración para poder realizar la encriptación de los paquetes de voz en una llamada VoIP es realizado dentro del mismo servidor, en este caso Asterisk.

Primero dentro de Asterisk se crea un certificado de autorización (CA) el mismo que servirá como base para crear un segundo certificado el mismo que será usado por todas las extensiones en las cuales se desee que la comunicación sea encriptada.

Así también para el encriptamiento no solamente es necesario lo previamente hecho en el servidor de VoIP sino también los clientes que deseen hacer este tipo de llamadas también debe poder soportar el encriptamiento caso contrario no podrán establecer comunicación entre ellos aunque la configuración dentro del servidor sea la correcta.

2.2.2.4.1 Real time protocol

La función principal de RTP es implementar los números de secuencia de paquetes IP para rearmar la información de voz o de video, incluso cuando la red subyacente cambie el orden de los paquetes.

De manera más general, RTP permite: identificar el tipo de información transmitida, agregarle marcadores temporales y números de secuencia a la información transmitida, controlar la llegada de los paquetes a destino. (Mendez Molina, 2015, pág. 25)

Además, los paquetes de difusión múltiple pueden utilizar RTP para enrutar conversaciones a múltiples destinatarios.

El encabezado RTP lleva la siguiente información:

<table>
<tr><th colspan="7">Byte 0</th><th>Byte 1</th><th>Byte 2</th><th>Byte 3</th></tr>
<tr><td>V</td><td>P</td><td>X</td><td>CC</td><td>M</td><td>PT</td><td colspan="3">Numero de Secuencia</td></tr>
<tr><td colspan="10">Marca de Tiempo</td></tr>
<tr><td colspan="10">Origen de Sincronización (SSRC)</td></tr>
<tr><td colspan="10">Origen Contenido (CSRC)</td></tr>
<tr><td colspan="10">Extensión de Cabecera (EH - opcional)</td></tr>
<tr><td colspan="10">Datos</td></tr>
</table>

A continuación se indican los significados de los diferentes campos de encabezados:

Campo de versión V: 2 bits de longitud. Indica la versión del protocolo (V=2);

Campo de relleno P: 1 bit. Si P es igual a 1, el paquete contiene bytes adicionales para rellenar y finalizar el último paquete;

Campo de extensión X: 1 bit. Si X = 1, el encabezado está seguido de un paquete de extensión;

Campo de conteo CRSC CC: 4 bits. Contiene el número de CRSC que le sigue al encabezado;

Campo de marcador M: 1 bit. Un perfil de aplicación define su interpretación;

Campo de tipo de carga útil PT: 7 bits. Este campo identifica el tipo de carga útil (audio, video, imagen, texto, html, etc.);

Campo Número de secuencia: 16 bits. Su valor inicial es aleatorio y aumenta de a 1 por cada paquete enviado. Puede utilizarse para detectar paquetes perdidos;

Campo Marca de tiempo: 32 bits. Refleja el instante de muestreo del primer byte del paquete RTP. Este instante debe obtenerse a partir de un reloj que aumenta de manera monótona y lineal para permitir la sincronización y el cálculo de la variación de retardo en el destino;

Campo SSRC: 32 bits. Identifica de manera única la fuente. La aplicación elige su valor de manera aleatoria. SSRC identifica la fuente de sincronización (simplemente llamada "la fuente"). Este identificador se elige de manera aleatoria con la intención de que sea único entre todas las fuentes de la misma sesión. La lista de CSRC identifica las fuentes (SSRC) que han ayudado a obtener los datos contenidos en el paquete que contiene estos identificadores. La cantidad de identificadores se proporciona en el campo CC;

Campo CSRC: 32 bits. Identifica las fuentes contribuyentes.

2.2.2.4.2 Secure real time protocol

Secure Real-Time Protocol (Secure RTP o SRTP) es una extensión del protocolo RTP con un mecanismo de seguridad mejorada. Proporciona cifrado, autenticación y verificación de la integridad de datos y mensajes transmitidos a través del protocolo de comunicación basado en RTP. Lanzado en 2004, SRTP fue desarrollado por expertos en seguridad de Cisco y Ericsson. SRTP proporciona la funcionalidad del protocolo RTP, mientras que el fortalecimiento de la seguridad de la mensajería unicast y multicast, incluyendo los mensajes multimedia y de comunicación, como la telefonía por Internet y videoconferencia. SRTP hace cumplir un estándar de cifrado avanzado (AES) algoritmo para cifrar y descifrar todos los mensajes entrantes y salientes. El mecanismo de autenticación proporciona un algoritmo de código de

autenticación de mensajes basado en hash (HMAC), que implementa una función hash criptográfica y la clave secreta para validar la autenticidad y la integridad de un mensaje.

SecureRTP también protege contra ataques de repetición mediante el mantenimiento de un índice de mensajes, que se utiliza para verificar los mensajes. (Janssen, 2012)

Características

SRTP proporciona algunas características que aligera la carga en la gestión de claves y aumento de la seguridad, incluyendo:

Una "clave maestra" única puede proporcionar material clave para la confidencialidad y la integridad de la protección, tanto para la transmisión SRTP y la transmisión SRTPC correspondiente. Esto se consigue con una función de derivación de claves, proporcionando "claves de sesión" para la respectiva seguridad primitiva, con seguridad derivada desde la calve maestra.

La derivación de claves se configura periódicamente para actualizar las claves de sesión, limitando la cantidad de texto cifrado que produce una clave fija.

Clave saltada es usada para proteger contra ataques TradeOff.

Integridad total de los paquetes RTP y RTCP.

Paquete SRTP

El formato de un paquete SRTP se presentara en la siguiente figura y explicado a continuación de esta mismo:

Cabecera paquete SRTP

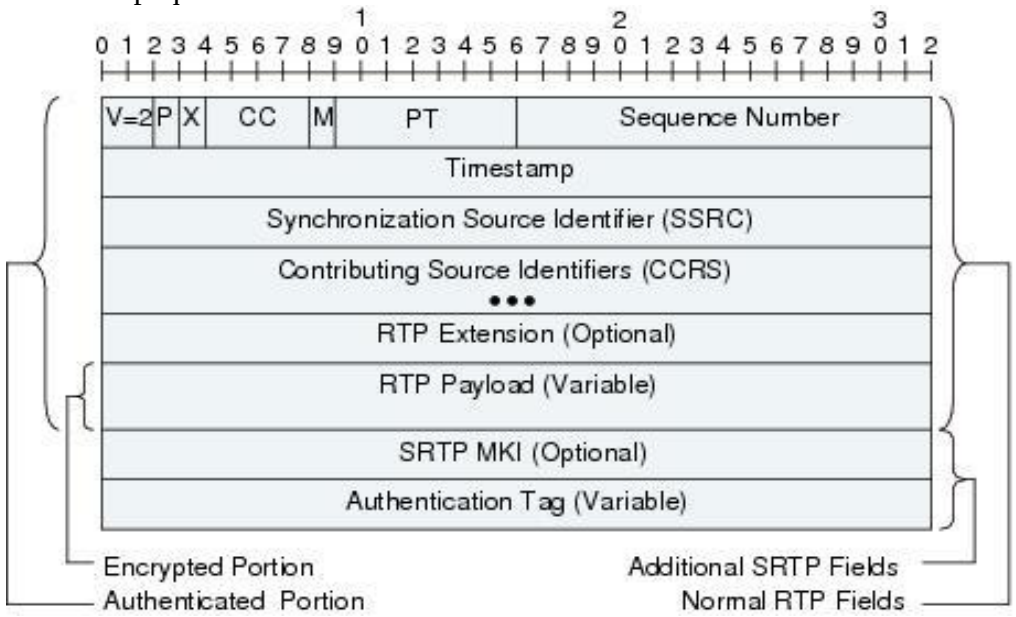

Figura 6. Formato de la cabecera de un paquete SRTP
Fuente: (Cisco, 2009)

Los campos siguientes son los que aparecen dentro de un paquete RTP normal:

Versión (V), campo de 2 bits indica la versión del protocolo la versión actual es 2.

Relleno (P), campo de 1 bit que indica el relleno en el extremo del paquete RTP.

Cabecera de Extensión (X), campo de 1 bit que indica la presencia de una cabecera de extensión opcional.

Marker (M), campo de 1 bit, utilizado para identificar eventos tales como límites de la trama.

Tipo de carga útil (PT), campo de 7 bits que identifica el formato de la carga útil RTP.

Número de Secuencia, campo de 16 bits que se incrementa en uno por cada paquete RTP enviado. Este campo puede ser utilizado por el recibir para identificar paquetes perdidos.

Timestamp, campo de 32 bits que refleja el instante de muestreo del primer octeto del paquete de RTP.

Identificador sincronización de fuente (SSRC) campo de 32 bits que identifica de forma única de transmisión de paquetes RTP.

Contribuir Fuente Identificadores (CSRCs) campo de longitud variable que contiene una lista de fuentes de transmisión de paquetes RTP que han contribuido a una transmisión combinada producida por un mezclador RTP.

Extensión RTP (Opcional), campo de longitud variable que contiene un perfil de identificador específico de 16 bits y un identificador de 16 bits de longitud, seguido de datos de extensión de longitud variable.

RTP, campo longitud de Carga Variable que contiene los datos de las aplicaciones en tiempo real (es decir, voz, vídeo, etc.).

Para lo que SRTP añade dos campos adicionales al paquete:

Master Key Identifier, lo cual traducido al español es Identificador de clave maestra (MKI), campo opcional de longitud configurable, que se utiliza para indicar la clave maestra, de la que se derivaron las claves de sesión individuales para el cifrado y / o autenticación, dentro de un contexto criptográfico dado.

Autenticación Tag, campo recomendado de longitud configurable, que se utiliza para contener los datos de autenticación de mensajes para la cabecera y la carga útil de RTP para el paquete en particular.

Con SRTP, el cifrado se aplica sólo a la carga útil del paquete RTP. La autenticación de mensajes, sin embargo, se aplica tanto a la cabecera RTP, así como la carga útil RTP. Desde autenticación de mensajes se aplica al número de secuencia RTP en la cabecera, SRTP indirectamente proporciona protección contra ataques de repetición.

2.2.3 Herramientas para análisis de seguridad voip

Para poder comprobar que una red es segura lo primero es someterla a diversos ataques usando una gran variedad de herramientas o tácticas de hacking, de esta manera se puede constatar las vulnerabilidades de la red y como mitigar las mismas.

2.2.3.1 Analizador de paquetes

Un analizador de paquetes o un Sniffer es un software que captura de las tramas de una red de computadoras. Los analizadores de paquetes tienen diversos usos, como monitorear redes para detectar y analizar fallos, o para realizar ingeniería inversa en protocolos de red. También es habitual su uso para fines maliciosos, como robar contraseñas, interceptar correos electrónicos, espiar conversaciones de chat, etc.

Los principales usos que se le pueden dar son: captura automática de contraseñas enviadas en claro y nombres de usuario de la red, conversión del tráfico de red en un formato inteligible por los humanos, análisis de fallos para descubrir problemas en la red, medición del tráfico, mediante el cual es posible descubrir cuellos de botella en algún lugar de la red, detección de intrusos, con el fin de descubrir hackers, creación de registros de red, de modo que los hackers no puedan detectar que están siendo investigados, para los desarrolladores, en aplicaciones cliente-servidor. Les permite analizar la información real que se transmite por la red.

Wireshark, es uno de los más populares analizadores que existen. Se trata de una herramienta gráfica utilizada por los profesionales y/o administradores de la red para identificar y analizar el tipo tráfico en un momento determinado. Se trata de un producto gratuito cuyas características más relevantes son: disponible para UNIX, LINUX, Windows y Mac OS, captura los paquetes directamente desde una interfaz de red, permite obtener detalladamente la información del protocolo utilizado en el paquete capturado, cuenta con la capacidad de importar/exportar los paquetes

capturados desde/hacia otros programas, filtra los paquetes que cumplan con un criterio definido previamente, realiza la búsqueda de los paquetes que cumplan con un criterio definido previamente, permite obtener estadísticas, sus funciones gráficas son muy poderosas ya que identifica mediante el uso de colores los paquetes que cumplen con los filtros establecidos. (Gallego León & Ruiz Delgado, 2016)

2.2.3.2 Nmap

Nmap ("Network Mapper") es una utilidad gratis y de código abierto para la detección de redes y auditoría de seguridad. Muchos sistemas y administradores de red también les resultan útil para tareas como el inventario de la red, los horarios de actualización de servicio de gestión y monitoreo de host o servicios ejecutándose en tiempo real. Nmap utiliza paquetes IP puros en formas novedosas para determinar qué servicios están disponibles en la red, ¿qué servicios los anfitriones están ofreciendo?, ¿qué sistemas operativos (y versiones del sistema operativo) se están ejecutando?, ¿qué tipo de filtros de paquetes/cortafuegos están en uso?, y docenas de otras características. Fue diseñado para escanear rápidamente grandes redes, pero funciona bien contra los equipos individuales. Nmap se ejecuta en todos los principales sistemas operativos y paquetes binarios oficiales están disponibles para Linux, Windows y Mac OS.

2.2.3.3 SiVuS

SiVuS es un veterano escáner de vulnerabilidades para redes VoIP que utilizan el protocolo SIP. Este escáner proporciona varias características para verificar la robustez y para asegurar la implementación de una red VoIP segura.

Las características de este escáner son las siguientes:

Generador de mensajes SIP: puede ser utilizado para enviar varios tipos de mensajes a un componente del SIP incluyendo contenido del SDP. Esta característica se puede

utilizar para probar ediciones específicas del SIP o para generar varios ataques, como por ejemplo un ataque de denegación de servicios.

Explorador de componentes del SIP: explora una gama de direcciones IP para identificar los anfitriones que utilizan el protocolo SIP y se puedan utilizar como blancos para el análisis adicional. Es una opción del explorador que permite el descubrimiento preliminar de objetivos antes de una exploración real.

Explorador de la vulnerabilidad del SIP: El explorador proporciona la configuración flexible de varias opciones que se pueden utilizar, para verificar la robustez y la seguridad de una implementación del protocolo SIP. Se realizan chequeos como: análisis de las cabeceras de mensajes del protocolo SIP para identificar vulnerabilidades tales como desbordamientos del buffer o ataques de denegación de servicio, autentificación de mensajes que identifican componentes del SIP, autentificación de las peticiones del registro, inspección para las comunicaciones seguras (SIPS) y verificación de las capacidades de cifrado.

Componente de log: posee un completo sistema de log en HTML que permite omitir mensajes de error para crear logs más fáciles de comprender, también posee base de datos para históricos.

Ayuda del SIP: el interfaz de SiVuS proporciona ayuda rápida en los aspectos más comunes sobre SIP que pueden ser útiles a un usuario mientras que utiliza SiVuS. La ayuda del SIP proporciona información sobre última versión del estándar RFC 3261 (SIP), muestra también ayuda a un usuario para construir mensajes SIP a través del generador.

2.2.3.4 Kali linux

Kali Linux es una distribución Linux basada en Debian dirigida a pruebas de penetración y auditoría de seguridad avanzadas. Kali contiene varios cientos de

herramientas destinadas a diversas tareas de seguridad de la información, tales como pruebas de penetración, informática forense y de ingeniería inversa. Kali Linux es desarrollado, financiado y mantenido por Offensive Security, una empresa líder de capacitación en seguridad de la información.

Kali Linux fue lanzado el 13 de marzo 2013 como una completa reconstrucción de arriba a abajo de BackTrack Linux, adhiriéndose completamente a las normas de desarrollo de Debian.

Incluye más de 600 herramientas de pruebas de penetración: Después de revisar todas las herramientas que se incluyó en BackTrack, se eliminaron un gran número de herramientas que, o bien simplemente no trabajaban o que duplican otras herramientas que proporcionan la misma o similar funcionalidad.

Gratis y siempre lo será: Kali Linux, como BackTrack, es completamente gratis y siempre lo será.

Desarrollado en un entorno seguro: El equipo de Kali Linux está formado por un pequeño grupo de personas que son los únicos de confianza para hacer paquetes e interactuar con los repositorios, todo lo cual se realiza mediante múltiples protocolos seguros.

Algunas de las herramientas usadas para vulnerabilidades en sistemas de VoIP son:

SIPp es una herramienta/generador de tráfico para el protocolo SIP Open Source gratuita. Incluye algunos escenarios básicos de usuarios agentes SipStone (UAC y UAS). También puede leer archivos XML personalizados de escenarios que describen desde simples hasta complejos flujos de llamadas. (Krasheninnikova, 2013, pág. 70)

SIPp también puede enviar el tráfico de medios (RTP) a través de RTP eco y RTP / pcap replay. El medio puede ser de audio o vídeo.

Aunque está optimizado para el tráfico, el estrés y pruebas de rendimiento, SIPp se puede utilizar para ejecutar una sola llamada y de salida, proporcionando un veredicto de aprobado/fallido.

SIPp puede ser utilizado para probar diversos equipos SIP reales como proxis SIP, B2BUAs, servidores de medios SIP, puertas de enlace SIP / x, SIP PBX, etc. También es muy útil para emular miles de agentes de usuario de llamada del sistema SIP.

SIPVicious Suite es un conjunto de herramientas que se pueden utilizar para auditar los sistemas de VoIP basado en SIP. En la actualidad consta de cinco herramientas:

Svmap - esto es un escáner de SIP. Enumera los dispositivos SIP que se encuentran en un rango de IP.

Svwar - identifica extensiones activas en una PBX.

Svcrack - un Password Cracker en línea para PBX SIP.

Svreport - gestiona las sesiones y exportaciones de informes en diversos formatos.

Svcrash - intenta detener exploraciones no autorizadas de svwar y svcrack.

2.2.4 Asterisk

Asterisk es un programa de software libre (bajo licencia GPL) que proporciona funcionalidades de una central telefónica (PBX). Como cualquier PBX, se puede conectar un número determinado de teléfonos para hacer llamadas entre sí e incluso conectar a un proveedor de VoIP. (Barcia Esparza, 2015, pág. 18)

Para conectar teléfonos estándares analógicos son necesarias tarjetas electrónicas telefónicas FXS o FXO fabricadas por Digium u otros proveedores, ya que para conectar el servidor a una línea externa no basta con un simple módem.

Asterisk reconoce muchos protocolos VoIP como pueden ser SIP, H.323, IAX y MGCP. Asterisk puede interoperar con terminales IP actuando como un registrador y como Gateway entre ambos, otro de los puntos fuertes del software Asterisk es que

permite la unificación de tecnologías: VoIP, GSM y PSTN. (Barcia Esparza, 2015, pág. 18)

Funciones básicas:

Transferencias (directa o consultiva): Permite transferir una llamada en curso a otra extensión. Existen dos formas:

Transferencia atendida: consultando al nuevo destino si quiere que le pasen la llamada,

Transferencia directa: pasando la llamada sin consultar al destinatario.

En versiones anteriores a la 1.8, al transferir una llamada se perdía el CLID (el número del usuario llamante). Esto no ocurre con la versión 1.8, que mantiene por tanto el CLID tras una transferencia.

Desvíos: Permiten la transferencia automática de una llamada entrante hacia un número determinado (interno o externo) cuando se cumplen determinadas condiciones: por ejemplo si el número está ocupado, si no contesta, etc.

Capturas (de grupo o de extensión): La captura permite coger una llamada que se está recibiendo en una extensión desde otra distinta.

Captura de extensión: por defecto se hace con el código *8 + la extensión.

Captura de grupo: se predefinen unos determinados grupos de extensiones de modo que al marcar un código de Asterisk - por defecto el *8 - se coge cualquier llamada que esté recibiendo el grupo en el que estamos.

Conferencia múltiple: En función del modelo de terminal se podrá establecer una comunicación entre múltiples usuarios de la centralita.

Llamada directa a extensión: Si además del número de cabecera disponemos de diferentes números públicos (DDIs), podremos enrutar directamente la llamada entrante a uno de estos DDIs, a una extensión de la centralita.

Ring groups: grupos de llamadas. Una llamada entrante podrá ser dirigida directamente a un ring group, que es un grupo de extensiones que sonaran de acuerdo a una determinada estrategia previamente establecida. Si la llamada no se descuelga no podrá ser tratada posteriormente y se perderá.

DND (Do not disturbe): Opción de no molestar, que podrá ser configurado en Asterisk mediante un código o directamente en el terminal. (Quarea Voz Datos IP, 2015)

CAPITULO III

Pruebas de Rendimiento y Resultados

3.1 Establecimiento del escenario de pruebas

Para el desarrollo de la parte práctica de este proyecto se planteó dos escenarios durante su desarrollo, el primero de ellos es el que se muestra en la siguiente gráfica.

Escenario de Pruebas

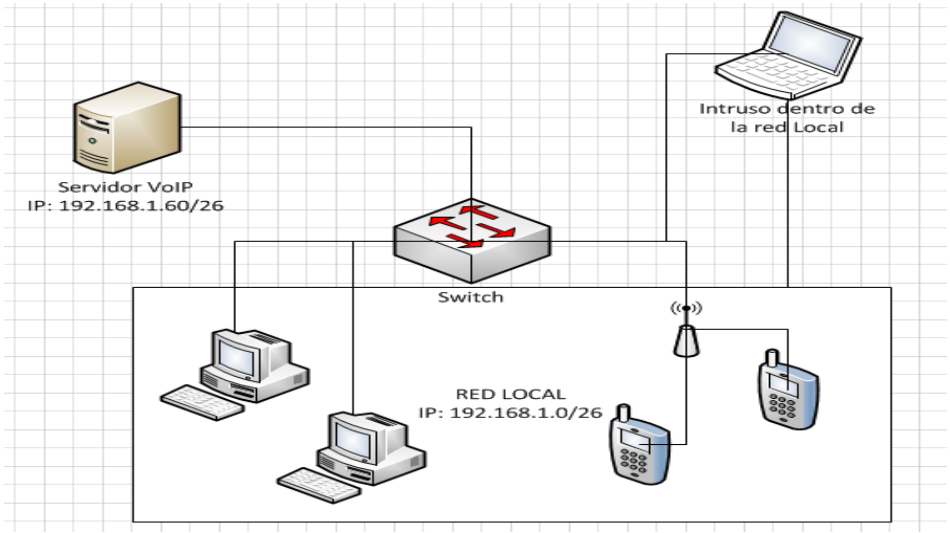

Figura 7. Escenario #1 Segmento LAN utilizado para la primera prueba
Elaborado por: Paillacho – Yánez

Con este escenario se trabajará para las pruebas de vulnerabilidad en el segmento LAN y sin un SBC de por medio. El segundo escenario planteado es el final y que actualmente se encuentra configurado y es el mostrado a continuación.

Arquitectura Final

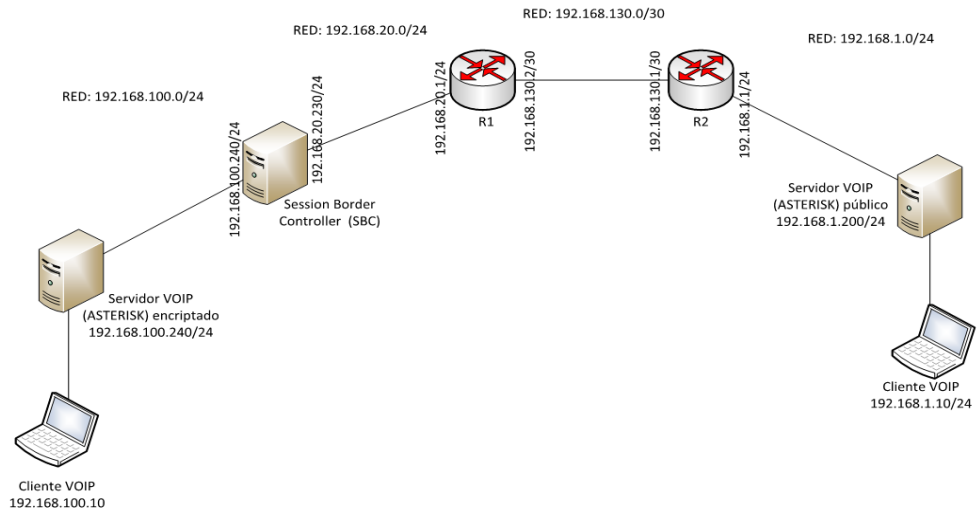

Figura 8. Escenario #2 - LAN-SBC-WAN
Elaborado por: Paillacho – Yánez

En este escenario es donde se realizaron la mayor parte de las pruebas de seguridad ya que es el escenario completo donde se incluye los segmentos LAN – SBC – WAN.

3.2 Verificación de vulnerabilidades de la PBX

Dentro de las pruebas a realizar es el ataque al servidor y clientes de la red VoIP mediante diferentes técnicas de hackeo y herramientas cuando estos se encuentran sin ninguna protección o seguridad a más de la que vienen configuradas por defecto en estos sistemas; y al contrario cuando estos se encuentran con sus seguridades configuradas Captura de Paquetes en una comunicación entre terminales SIP

La primera prueba realizada es mediante el uso del analizador de paquetes “Wireshark” intervenir en la comunicación entre dos usuarios y así obtener los paquetes de voz que se transmiten con la finalidad de lograr obtener el audio de la conversación entre dichos usuarios.

A	ESCENARIO DE PRUEBA #1
A-1	CASO 1 : Red sin ningún tipo de seguridad

Topología Lógica de Red

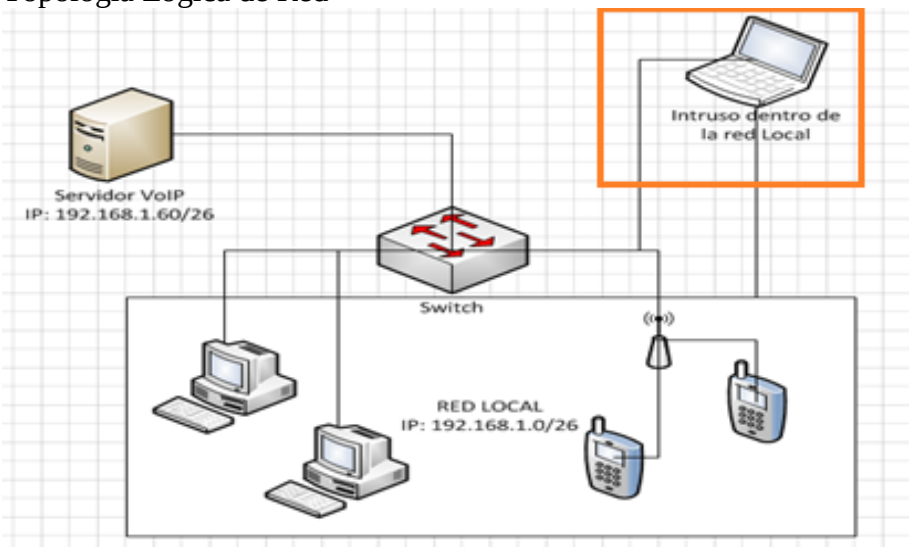

Figura 9. Topología Lógica de Red utilizada en el escenario de pruebas #1
Elaborado por: Paillacho – Yánez

B	METODOLOGÍA

Para el desarrollo de esta prueba se aplicaron las bases de la metodología investigativa y experimental, las mismas que permitieron debido a la naturaleza del proyecto obtener resultados adecuados para el cumplimiento del objetivo del presente estudio.

La primera prueba se la realizará en el escenario propuesto en la figura 9, el cual no posee ningún tipo de seguridad salvo las que vienen configuradas por defecto, en dicho escenario se realizará un ataque mediante un sniffer o analizador de paquetes en este caso en particular Wireshark. Mediante el uso de esta herramienta se realizará la intrusión entre la comunicación de dos clientes de VoIP para obtener los paquetes de voz que se transmiten y posteriormente se realizara el análisis de los mismos para comprobar la información obtenida.

C	RESULTADOS OBTENIDOS

Captura Paquetes RTP

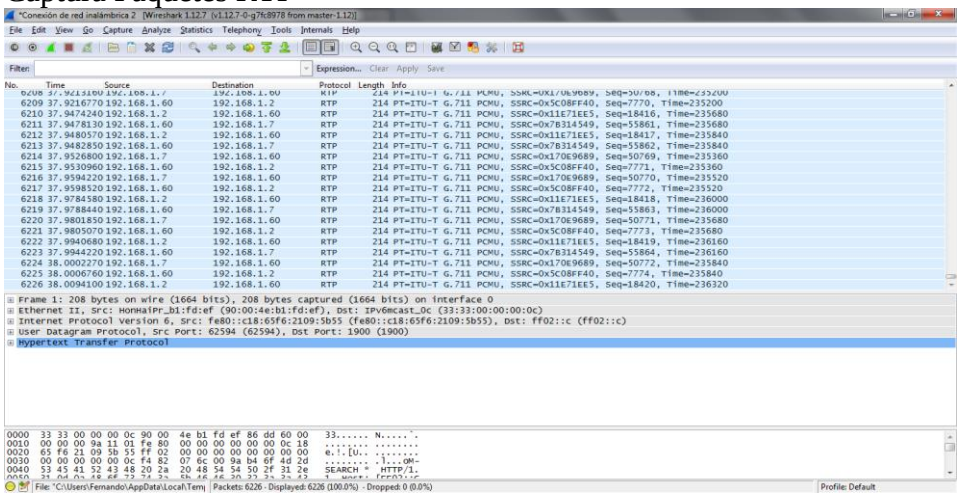

Figura 10. Captura de Paquetes RTP en una comunicación VoIP mediante Wireshark
Elaborado por: Paillacho – Yánez

Streams Paquetes RTP

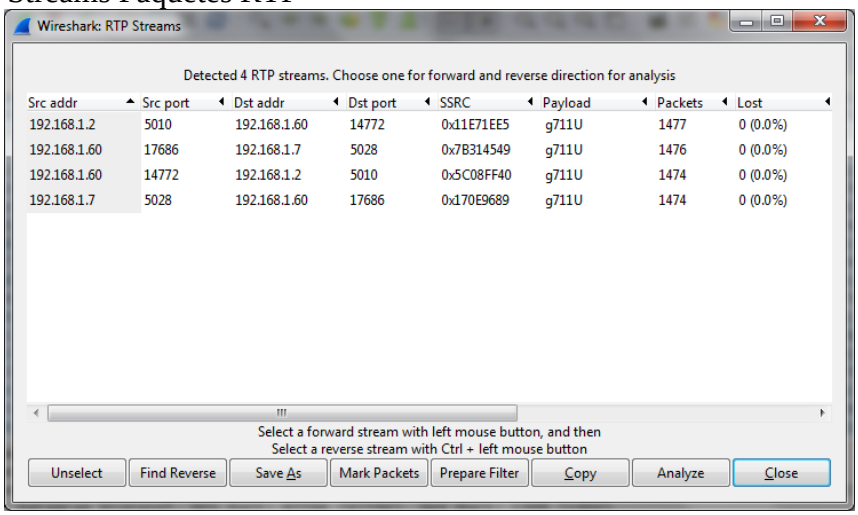

Figura 11. Streams RTP capturados de una comunicación
Elaborado por: Paillacho – Yánez

Análisis de los Streams

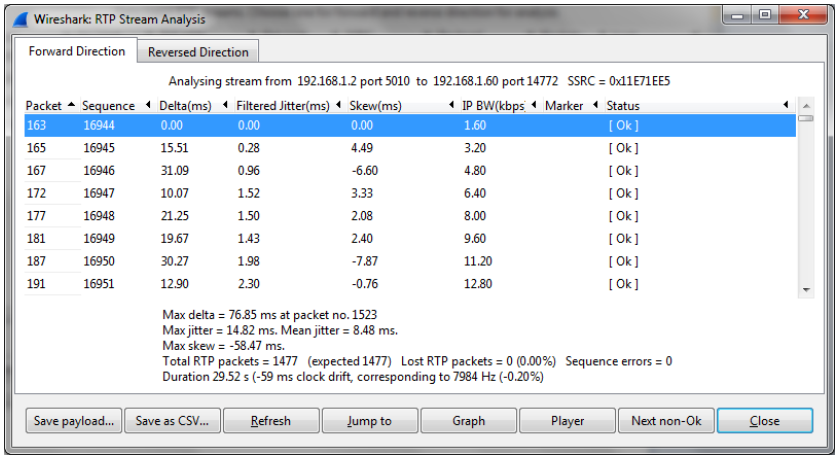

Figura 12. Análisis de uno de los streams capturados
Elaborado por: Paillacho – Yánez

Reproducción del stream

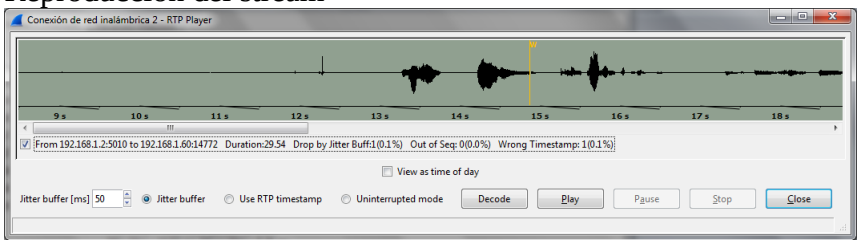

Figura 13. Decodificación y reproducción del audio capturado en los paquetes RTP
Elaborado por: Paillacho – Yánez

Los paquetes que se trasmiten en una comunicación de voz sin cifrar son del tipo RTP, y como se puede observar en la figura 8 los paquetes que se están transmitiendo corresponden a este tipo de paquetes, los mismos pueden ser analizados por el mismo sniffer para obtener el audio.

La obtención de los paquetes RTP nos devuelven algunas cadenas de stream como se muestra en la figura 11 y figura 12, las cuales pueden ser decodificadas para finalmente obtener el audio.

Como se aprecia en la gráfica que se muestra en la figura 12 se puede observar claramente que los datos de voz fueron capturados y los mismos ya están en manos de quienes realizaron el ataque.

Como una aclaración en el escenario propuesto el ataque provenía desde un equipo comprometido dentro de la red interna donde se encontraba nuestro servidor de VoIP.

A	**ESCENARIO DE PRUEBA #2**
A-1	**CASO 2 : Red utilizando encriptación de paquetes de voz dentro de Asterisk**

Topología de Red

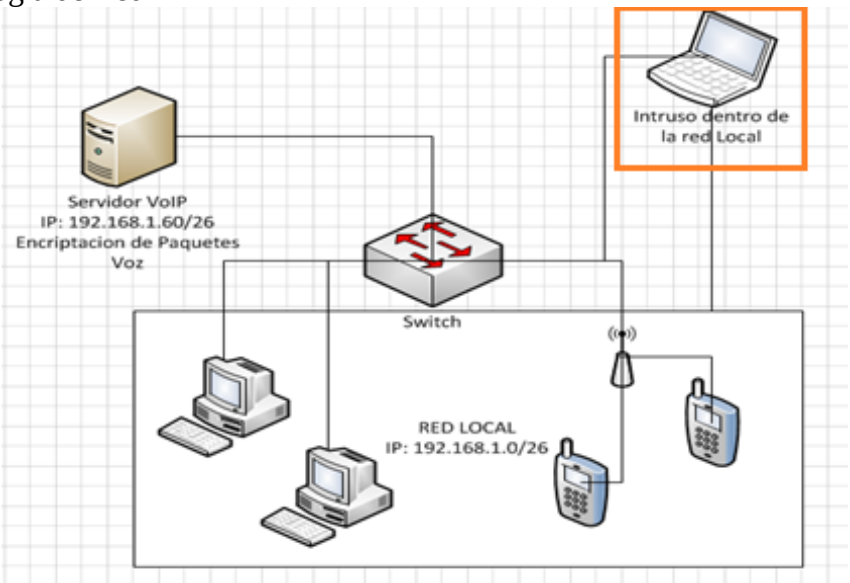

Figura 14. Topología Lógica de Red - Escenario de Pruebas #2
Elaborado por: Paillacho – Yánez

B	**METODOLOGÍA**

De manera similar que en el escenario de pruebas #1 durante este escenario se aplicaron las metodologías investigativa y experimental para obtener los mejores resultados en este escenario de pruebas.

Esta segunda prueba se la realizará en el escenario propuesto en la figura 14 , en el cual la única seguridad que se ha configurado es la encriptación de paquetes dentro del servidor Asterisk, en este escenario se realizará un ataque mediante un sniffer o analizador de paquetes en este caso en particular Wireshark.

Mediante el uso de esta herramienta se realizará la intrusión entre la comunicación de dos clientes de VoIP para obtener los paquetes de voz que se transmiten y posteriormente se realizara el análisis de los mismos para comprobar la información obtenida.	
C	**RESULTADOS OBTENIDOS**

Captura Paquete RTP

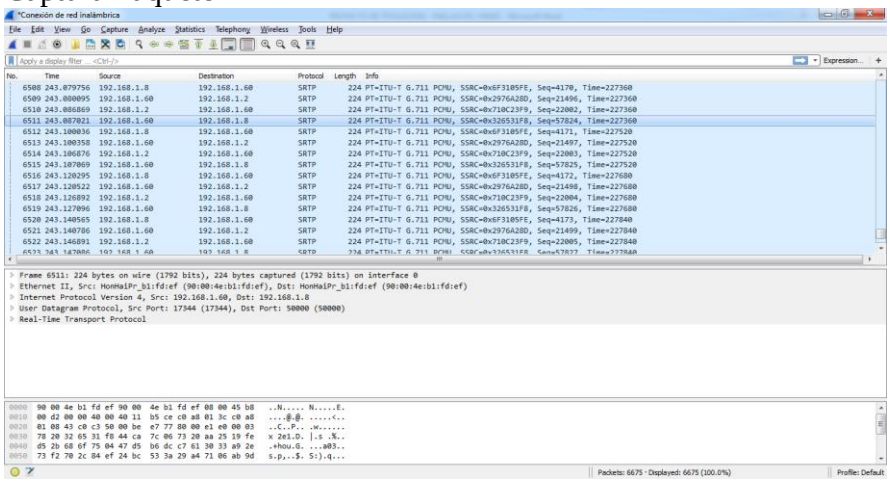

Figura 15. Captura de Paquetes RTP en una comunicación VoIP mediante Wireshark
Elaborado por: Paillacho – Yánez

Stream SRTP capturado

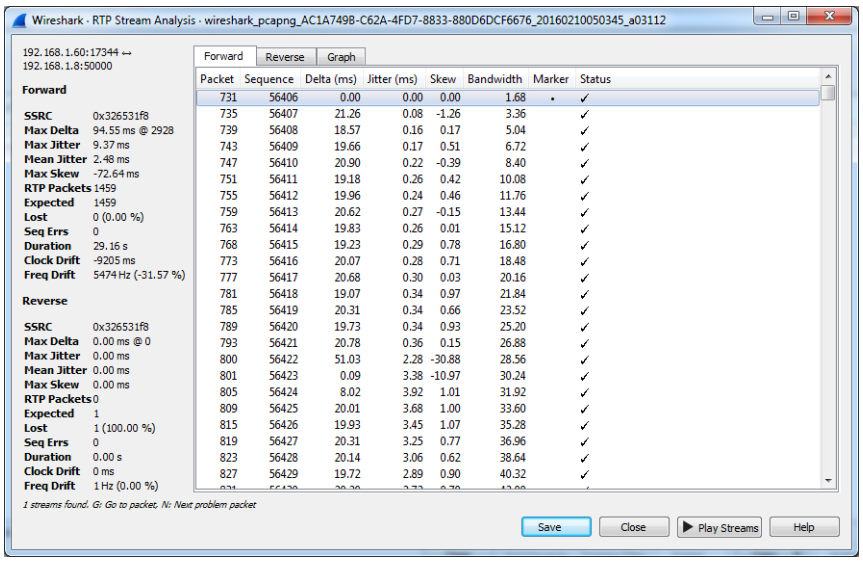

Figura 16. Análisis de uno de los Streams capturados
Elaborado por: Paillacho – Yánez

Análisis de Stream

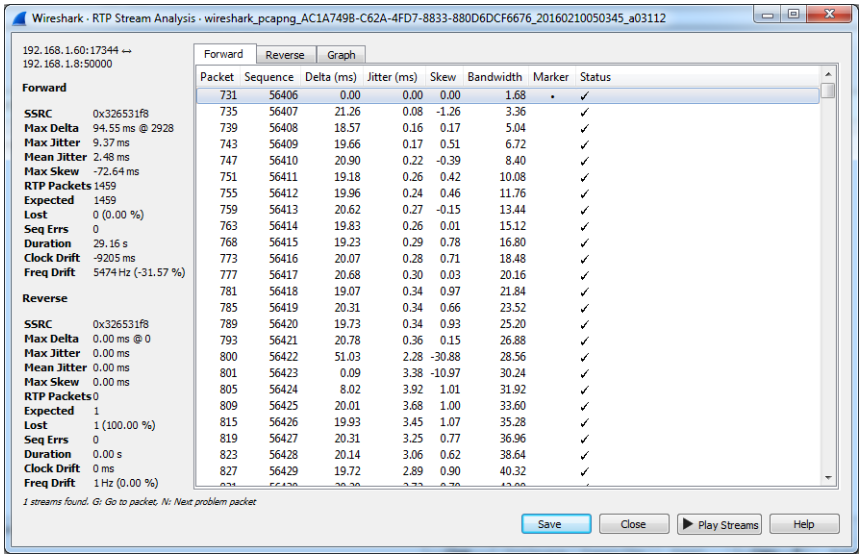

Figura 17.Análisis de uno de los Streams capturados
Elaborado por: Paillacho – Yánez

Reproducción paquete SRTP

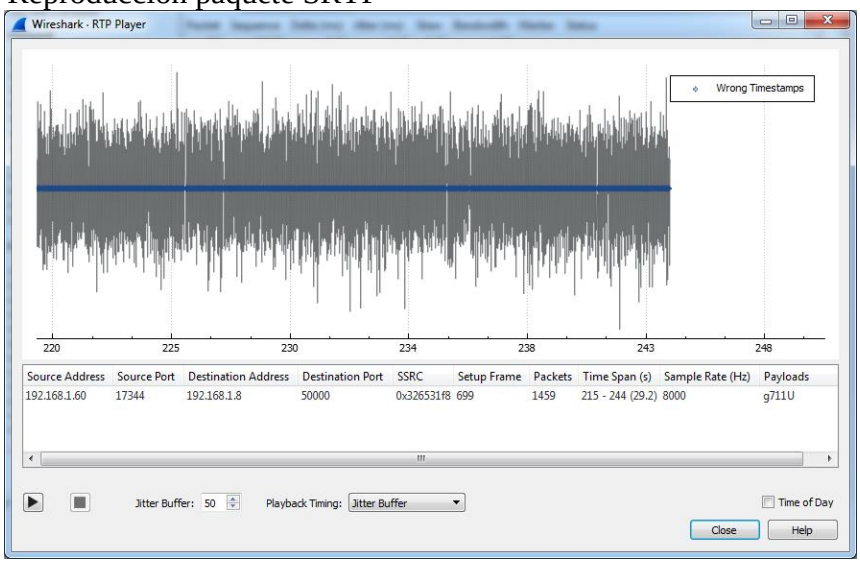

Figura 18. Decodificación y reproducción del audio capturado en los paquetes SRTP
Elaborado por: Paillacho – Yánez

Los paquetes que se trasmiten en una comunicación de voz cifrada son del tipo SRTP, y como se puede observar en la figura 15, se puede ver que dichos paquetes se están transmitiendo, los mismos pueden ser capturados mediante un programa analizador de paquetes (sniffer) para un posterior análisis para intentar descifrar el audio que guardan dichos paquetes.

Capturar paquetes de tipo SRTP devuelven algunas cadenas de stream como se muestra en la figura 16 y figura 17, las cuales de manera similar a cuando se realizó la captura de los paquetes sin cifrar se tiene la opción para ser decodificadas e intentar obtener el audio.

Como se observa en la gráfica que se muestra en la figura 16 se puede observar claramente que el audio capturado de los paquetes cifrados SRTP generaron un audio lleno de ruido, el mismo que no es entendible y de esta forma la conversación se logró mantener segura a pesar del ataque realizado y nuestra información se mantiene segura.

A	**ESCENARIO DE PRUEBA #3**
A-1	**CASO 3 : Red con Session Border Controller implementado**

Topología Final

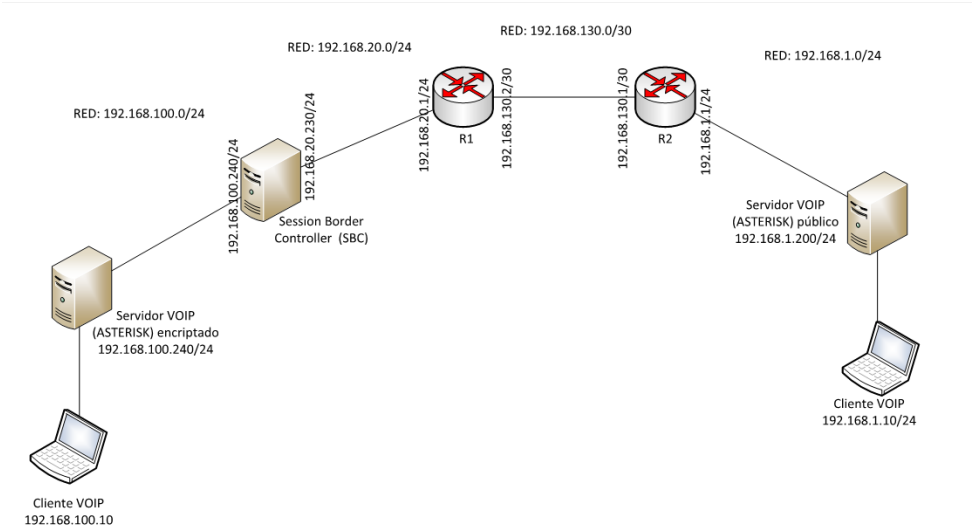

Figura 19. Escenario de Pruebas #3 para una Red de VoIP con un SBC incluido
Elaborado por: Paillacho – Yánez

B METODOLOGÍA

De manera similar que en el escenario de pruebas #1 y 2 durante este escenario se aplicaron las metodologías investigativa y experimental para obtener los mejores resultados en este escenario de pruebas.

En esta tercera prueba se la realizará en el escenario propuesto en la figura 19, en el cual el diseño del escenario cambia completamente debido a la forma en la que trabaja el SBC. De igual forma se requiere realizar una captura de los paquetes de voz, sin embargo, hay que tener en consideración que el ataque desde la sección externa WAN hacia a la red LAN no efectuarse debido a que la forma en que se comunican estos dos segmentos es únicamente a través del SBC y solamente paquetes de voz son los que se pueden transmitir; una comunicación por paquetes de datos es imposible debido a la forma en la que está configurado el escenario.

C RESULTADOS OBTENIDOS

Captura Comunicación

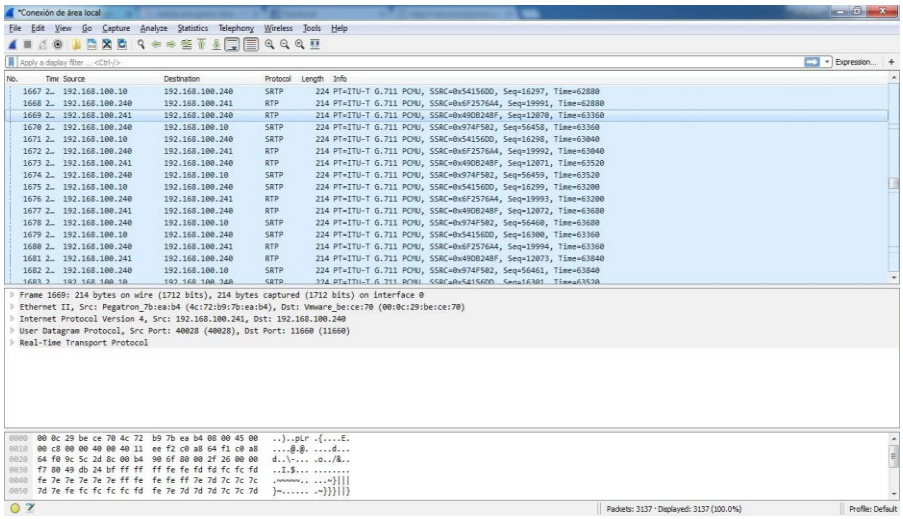

Figura 20. Captura de Paquetes de una Comunicación VoIP entre un cliente interno-SBC-cliente externo

Elaborado por: Paillacho – Yánez

Lista de Streams

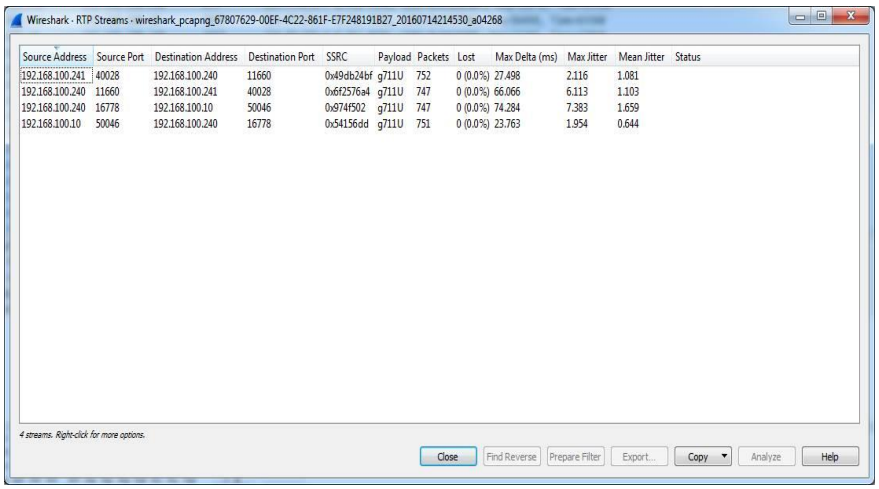

Figura 21: Lista de streams capturados de la comunicación entre cliente interno-SBC-cliente externo

Elaborado por: Paillacho – Yánez

Análisis de los Streams

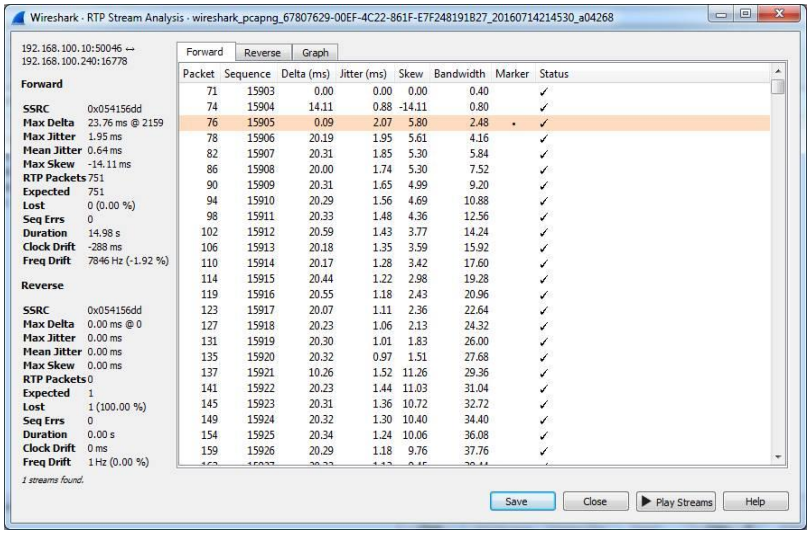

Figura 22: Análisis de los streams capturados entre la comunicación de un cliente interno-SBC-cliente externo
Elaborado por: Paillacho – Yánez

Reproducción de la Captura

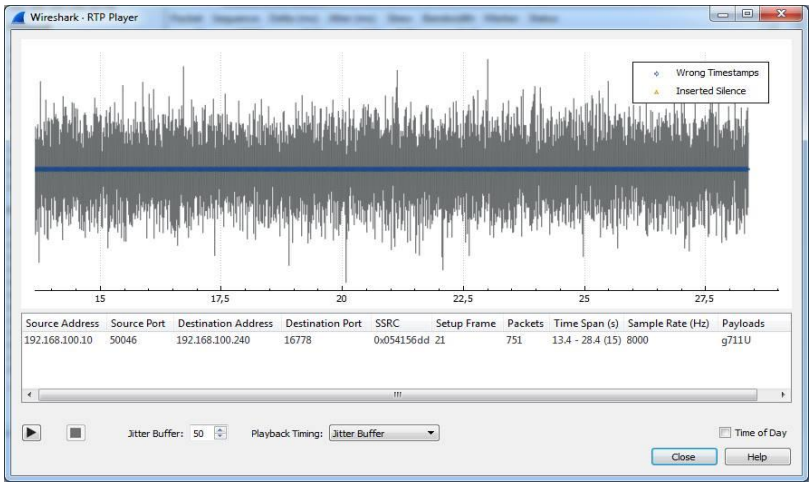

Figura 23. Decodificación del audio obtenido de la comunicación entre un cliente interno-SBC-cliente externo
Elaborado por: Paillacho – Yánez

Como se aprecia en la figura 20 el tipo de paquetes que se transmiten entre un cliente interno que realiza una comunicación hacia un cliente externo es del tipo SRTP que se obtienen con la habilitación en la troncal los media encryption, tanto en la parte LAN como para la parte WAN.

De la obtención de los paquetes SRTP de esta comunicación, se tiene algunas cadenas de streams como se muestra en la figura 21 y figura 22, las cuales pueden ser decodificadas para finalmente obtener decodificar el audio obtenido que sería ruido. Como se aprecia en la gráfica que se muestra en la figura 23 se puede observar una gráfica que indica que los datos de voz fueron capturados y los mismos ya están en manos de quienes realizaron el ataque, pero como se observa en la figura 23 no podrán escuchar la conversación, pues solo tendrán ruido.

El ataque que se realizó se lo hizo desde un equipo desde el lado externo (WAN), lo demostrado en esta prueba significa que BLOX como SBC realizando las configuraciones de la habilitación de los media encryption.se puede realizar una conversación más segura que con solo utilizando la encriptación sin un SBC.

3.2.1 Escaneo de dispositivos sip

Para el escaneo de dispositivos SIP se utilizará la herramienta provista dentro del Sistema Operativo para detección de vulnerabilidades Kali Linux; la herramienta en cuestiones que provee este sistema operativo es “svmap”, este es un script desarrollado en python el hace un escaneo según con los parámetros que se le ejecute para obtener todos los dispositivos SIP existentes.

A	**ESCENARIO DE PRUEBA #1**
A-1	**CASO 1 : Red sin ningún tipo de seguridad (incluye encriptamiento)**

Topología de Red

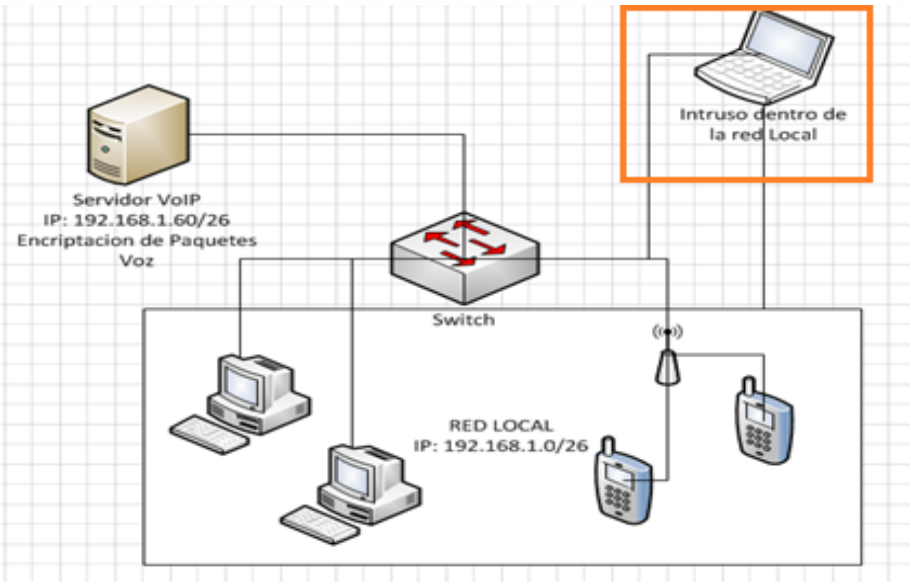

Figura 24. Topología de Red - Escenario de Pruebas #1 - Prueba 2
Elaborado por: Paillacho – Yánez

B	METODOLOGÍA

Para el desarrollo de esta prueba se aplicaron las bases de la metodología investiga y experimental, siendo estas dos metodologías las que permitieron mediante la aplicación de métodos de prueba y error en reiteradas ocasiones, obtener resultados satisfactorios necesarios para la culminación de este estudio. Mediante el uso de la metodología de investigación se logró obtener los conocimientos necesarios para el uso de la herramienta en distintos escenarios para obtención de resultados aplicando los conceptos de la metodología experimental.

C	RESULTADOS OBTENIDOS

SVMAP

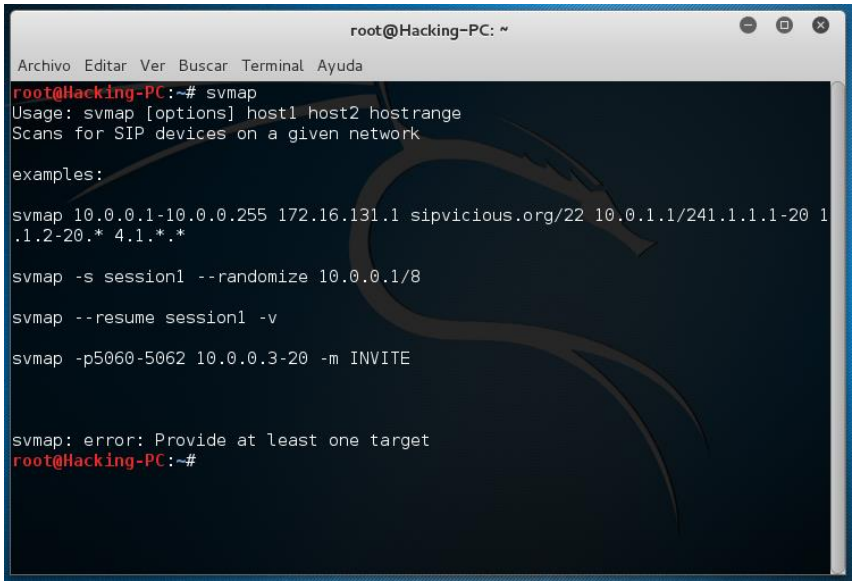

Figura 25. Ejemplos parámetros usados por el comando svmap
Elaborado por: Paillacho – Yánez

Escaneo a la topología

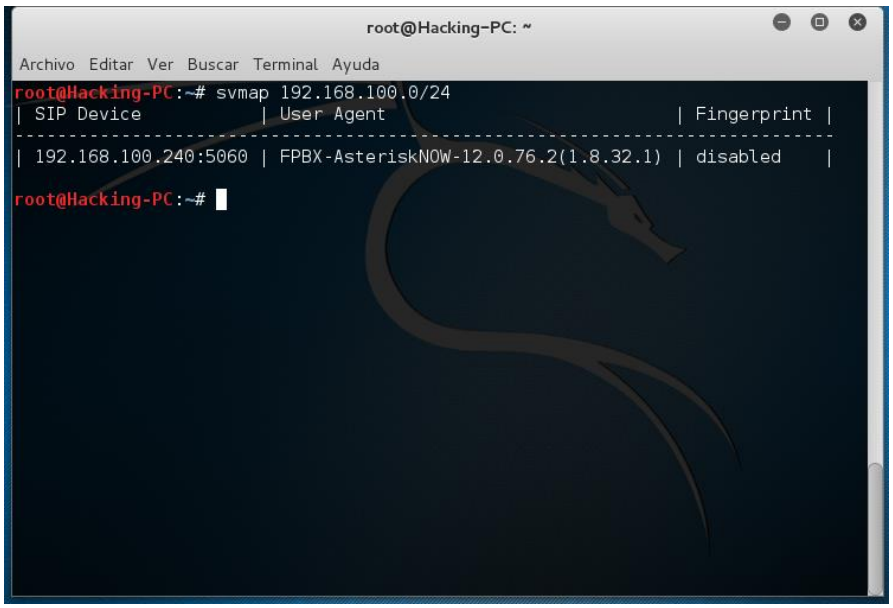

Figura 26. Escaneo de dispositivos SIP realizado por el svmap al escenario propuesto
Elaborado por: Paillacho – Yánez

Ejemplo captura SVMAP

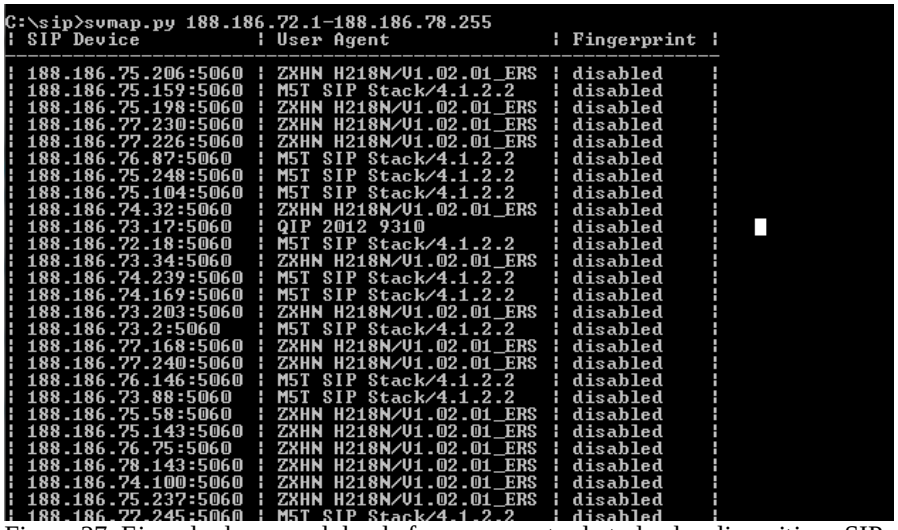

Figura 27. Ejemplo de una red donde fueron encontrado todos los dispositivos SIP utilizando svmap
Fuente: (Suicidemouse, 2014)

Para el escaneo de dispositivos SIP se utilizó un equipo que contaba con el SO Kali Linux y desde el mismo dentro del modo de consola se procedió a ejecutar el comando svmap con sus respectivos parámetros para saber que dispositivos SIP forman parte de la red escaneada.

Como se puede apreciar en la figura 25 los parámetros necesario para realizar un escaneo de dispositivos SIP mediante el svmap es conocer la dirección de la red que se va a atacar en el caso en cuestión mostrado la red a atacar era una red /24; como único dispositivo encontrado en la red a pesar de que varios clientes estaban conectados a la red solo fue comprometida la información del servidor de VoIP que corresponde a su dirección IP.

El comando svmap provisto por Kali Linux es muy poderoso cuando de escanear dispositivos SIP de una red se trata, sin embargo Asterisk por defecto al momento de crear extensiones no permite que las mismas puedan ser escaneadas o al menos al conectarse la mismas a un softphone no pueden ser escaneadas debido a los puertos que utilizan para engancharse al servidor. Además como se

puede apreciar en la figura 27 utilizando de igual manera el comando svmap se obtuvieron los resultados que se muestran en la misma, donde se puede apreciar todos los dispositivos SIP perteneciente al rango de direcciones IP especificadas para el escaneo.

A	ESCENARIO DE PRUEBA #2
A-1	CASO 2 : Red que incluye un SBC como equipo de seguridad

Topología de Red

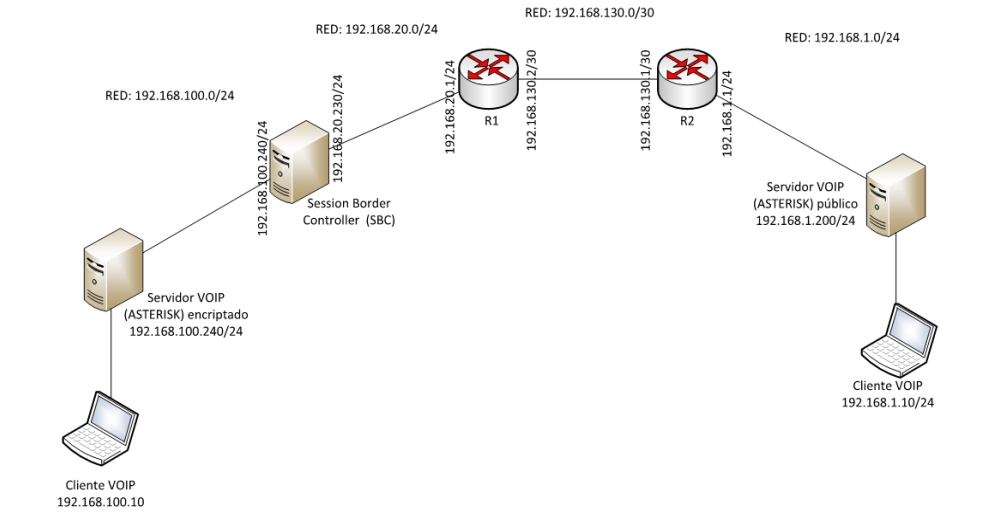

Figura 28. Topología Lógica de Red - Escenario Pruebas #2 – Prueba 2
Elaborado por: Paillacho – Yánez

B	METODOLOGÍA

Para el desarrollo de esta prueba muy similar al caso #1 se aplicaron las bases de la metodología investiga y experimental, siendo estas dos metodologías las que permitieron mediante la aplicación de métodos de prueba y error en reiteradas ocasiones, obtener resultados satisfactorios necesarios para la culminación de este estudio. Mediante el uso de la metodología de investigación se logró obtener los conocimientos necesarios para el uso de la herramienta en distintos escenarios para obtención de resultados aplicando los conceptos de la metodología experimental.

C	RESULTADOS OBTENIDOS

Ataque con SVMAP

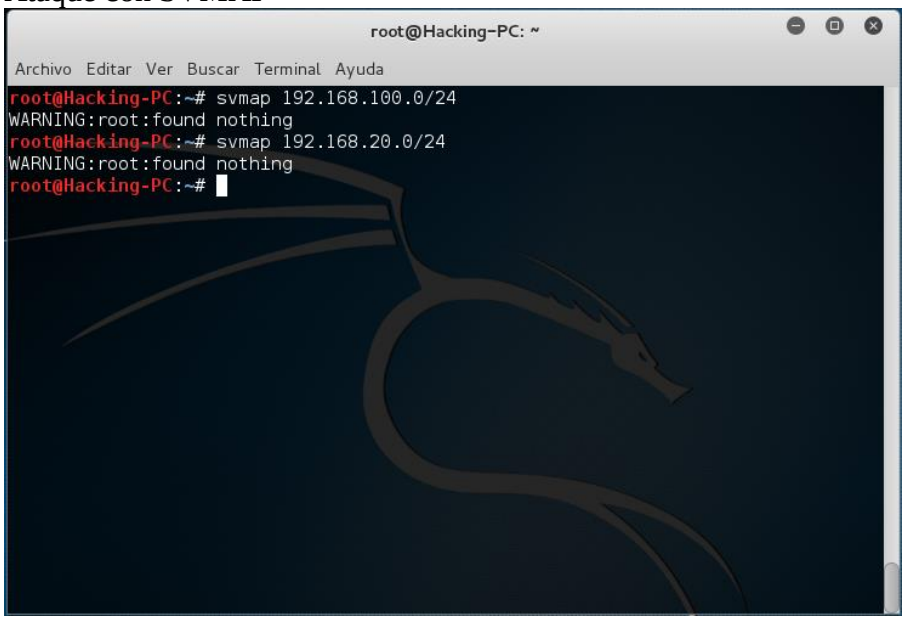

Figura 29. Ataque hacia la red interna utilizando comando svmap
Elaborado por: Paillacho – Yánez

Para esta prueba la única captura es la que se muestra en la figura 29 donde se ve que se realizan dos ataques de escaneo de dispositivos SIP sin ningún resultado satisfactorio para el lado del atacante, el primer escaneo va dirigido hacia el segmento de la red LAN mientras que el segundo está dirigido hacia el segmento WAN del SBC para verificar si este podía ofrecer alguna información pero sin ningún resultado.

Como se indicó antes la comunicación entre los segmentos LAN y WAN se realizan únicamente mediante el SBC y este solo permite el paso de paquetes de voz por lo que ataques como el escaneo de dispositivos SIP desde el lado externo no es posible como se muestra en la figura 29. De este modo queda comprobado que el uso de un SBC en el borde de nuestro segmento de red interna nos protege de ciertos tipos de ataques que normalmente serian exitosos sin la implementación del mismo.

3.2.2 Ataque de denegación de servicio

Un ataque de denegación de servicio o también conocido como DoS por sus siglas en ingles Denial of Service o en su versión más moderna DDoS (Distribuited Denial of Service), es un ataque muy común en estos tiempos cuando lo que se desea es inutilizar algún servicio de importancia para el atacado. La característica más básicas para este tipo de ataques es el uso del flood o flooding el cual consiste en inundar de peticiones al equipo que proporciona un servicio o recurso, llegando al punto de saturar al mismo, lo que provoca que la disponibilidad del servicio no sea accesible hasta que el atacante detenga su ataque o la victima tome las contramedidas correspondientes.

A	ESCENARIO DE PRUEBA #2
A-1	CASO 2 : Red que incluye un SBC como equipo de seguridad

Topología de Red

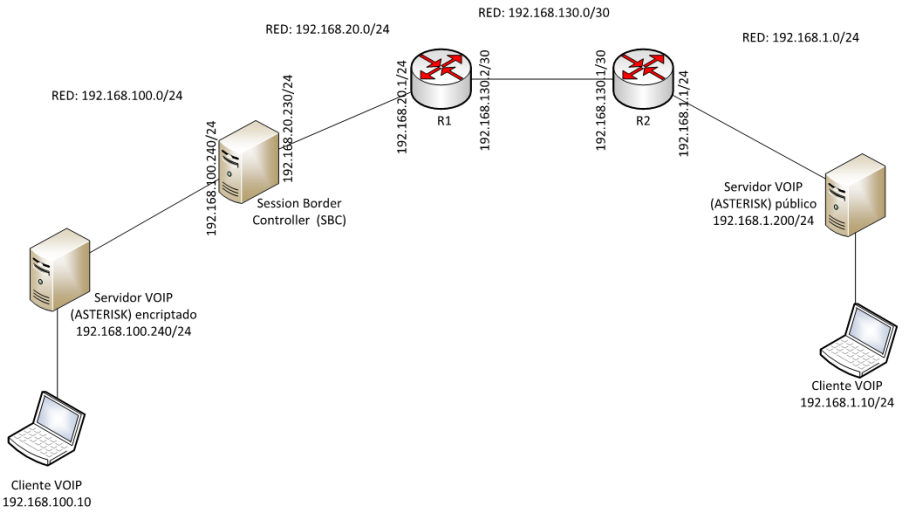

Figura 30.Topología Lógica de Red - Escenario Pruebas #2 – Prueba 3
Elaborado por: Paillacho – Yánez

B	METODOLOGÍA

Para el desarrollo de esta prueba muy similar al caso #1 se aplicaron las bases de la metodología investiga y experimental, siendo estas dos metodologías las que permitieron mediante la aplicación de métodos de prueba y error en reiteradas ocasiones, obtener resultados satisfactorios necesarios para la

culminación de este estudio. Mediante el uso de la metodología de investigación se logró obtener los conocimientos necesarios para el uso de la herramienta en distintos escenarios para obtención de resultados aplicando los conceptos de la metodología experimental.

C RESULTADOS OBTENIDOS

Comando inviteflood

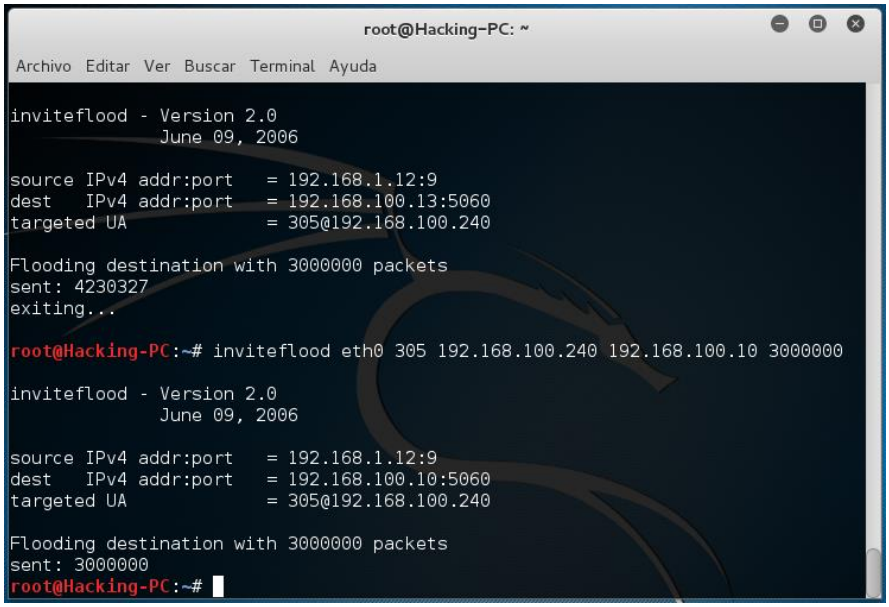

Figura 31: Ataque hacia la red interna desde un equipo ubicado en el lado externo usando el comando inviteflood.
Elaborado por: Paillacho – Yánez

Softphone BLINK

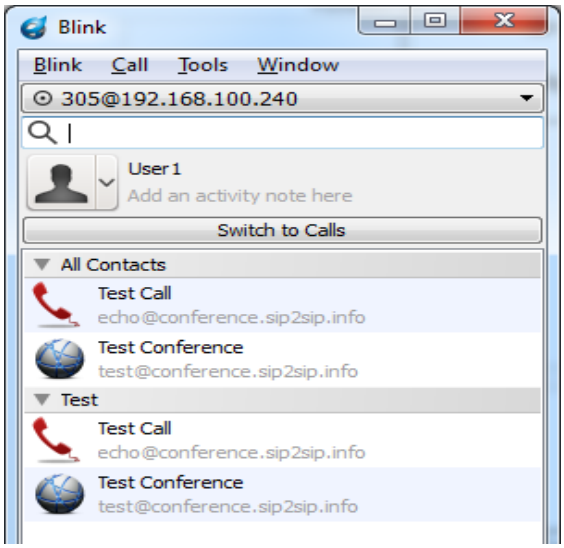

Figura 32. Softphone que muestra la extensión activa durante el ataque de flooding
Elaborado por: Paillacho – Yánez

Estadísticas FreePBX

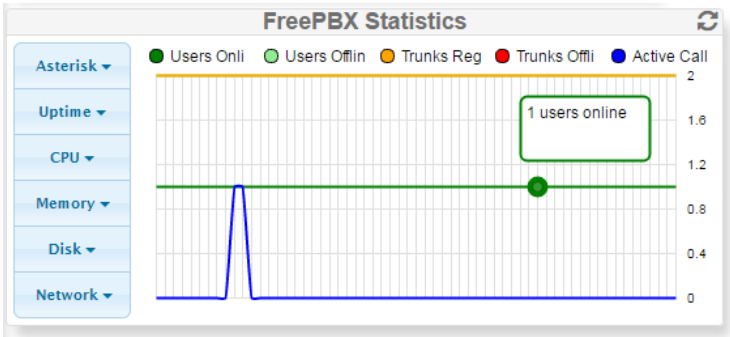

Figura 33:Imagen del FreePBX que muestra que las extensiones en línea se mantuvo fijo durante el ataque
Elaborado por: Paillacho – Yánez

Para esta prueba la única captura es la que se muestra en la figura 31 donde se puede apreciar que se hace uso del comando inviteflood como parámetros indicando que se atacara a la interfaz eth0, a la extensión 305 seguido de la dirección del servidor de VoIP, luego la dirección IP del cliente de la extensión y finalmente el número de paquetes que se enviara en este caso 3000000. Utilizar este comando en primera instancia compromete al atacante tanto como al atacado porque desde la interfaz del atacante salen una gran cantidad de paquetes hacia el destino, y como finalmente estos paquetes no saben cómo llegar debido a la topología del escenario de estudio los mismo se descartan en el camino y de esta manera el objetivo del ataque se mantiene a salvo.

Como dato adicional cuando este tipo de ataque es realizado las conexiones de las extensiones con el servidor de VoIP se pierden debido al gran número de paquetes que recibe el servidor en este caso como se aprecia en las figuras 32 y 33 tanto nuestro softphone como el servidor muestran que las extensiones activas siempre lo estuvieron durante el ataque.

3.3 Comparativa de tráfico voz VoIP con seguridad y sin seguridad

Como último paso de las pruebas de rendimiento se procedió a realizar una comparativa del tráfico VoIP basado en los escenarios sin seguridad y con seguridad,

para poder evidenciar si el rendimiento de la red se vería afectado al momento de implementar la seguridad o si se ausentaba la misma se tenía un rendimiento mejor.

A continuación se presentan dos gráficas que representan el uso de ancho de banda dado en bytes vs el tiempo, las duración de las llamadas fue de aproximadamente 30 segundos en los dos escenarios.

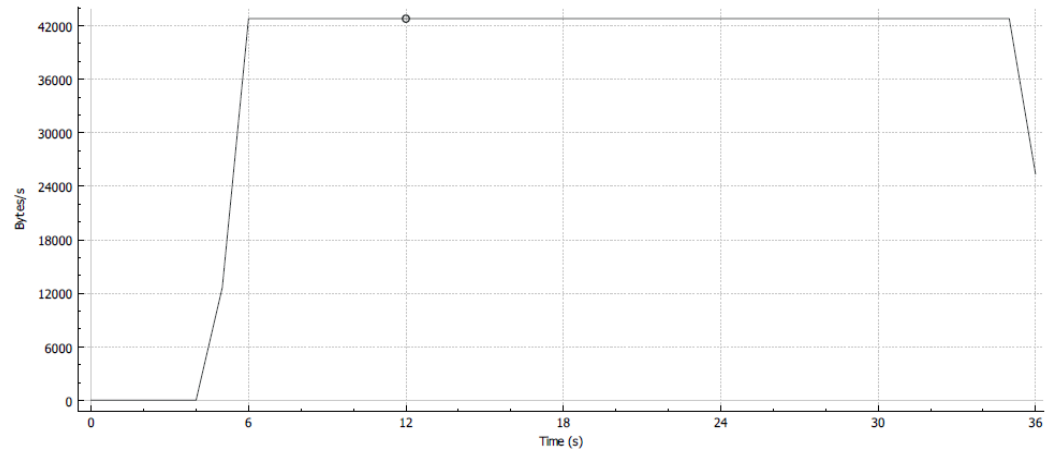

Figura 34: Tráfico VoIP Bytes vs Tiempo - Sin Seguridades
Elaborado por: Paillacho – Yánez

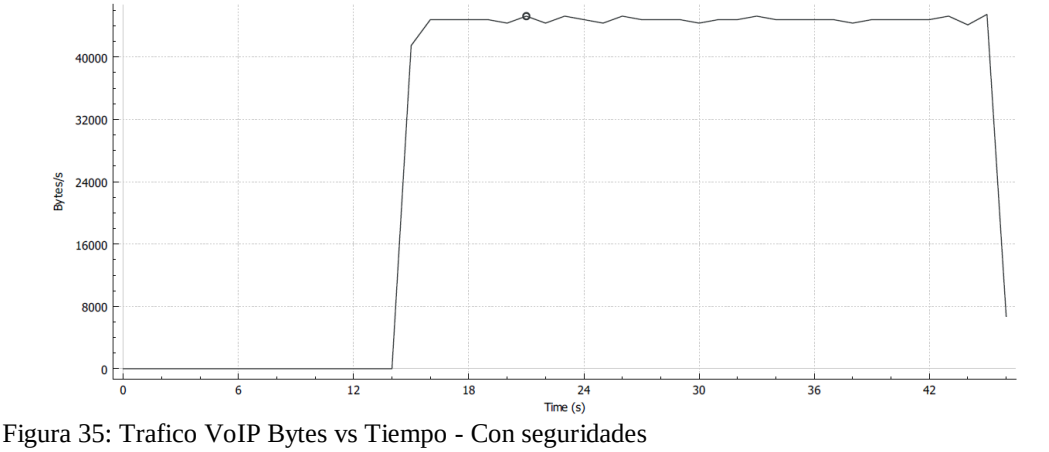

Figura 35: Trafico VoIP Bytes vs Tiempo - Con seguridades
Elaborado por: Paillacho – Yánez

De las dos gráficas se puede apreciar algunas características a destacar, una de ellas es que en ambas comunicaciones ambas están por sobre los 42000 bytes que se utilizan durante la llamada. Otro punto a destacar es que la diferencia del uso de ancho de banda entre las dos comunicaciones con y sin seguridad es de aproximadamente 2000

a 3000 bytes que representado en KB se está hablando de unos 2 a 3 KB extras por seguridad en llamadas solo de voz.

Con esto en mente el rendimiento de la red no se ve tan afectado por la implementación de las seguridades a la misma, y la única forma de que esto pueda afectar al rendimiento de red seria que se realizaran una cantidad considerable de llamadas simultáneamente para que esto represente un riesgo al rendimiento de la red.

Conclusiones

- Aplicaciones OpenSource para la implementación de sistemas VoIP a pesar de no tener algún costo monetario requiere de un esfuerzo mayor en su configuración, las mismas que deben realizarse desde modos de consola y en pocos casos se cuenta con alguna GUI para su fácil configuración.
- Para una red de VoIP existe una gran variedad de opciones a escoger cuando de seguridad se trata, comenzando con soluciones simples como seria realizar configuraciones adicionales al mismo servidor de VoIP, también las soluciones que son usadas en redes de datos también son válidas como sería configurar un firewall lógico o implementar uno físico en la red para mejorar la protección de los datos.
- En el mercado existen gran variedad de SBC, dichas soluciones se encuentran disponibles tanto en hardware como en software; la solución en software se puede encontrar tanto en OpenSource como software propietario con costos muy similares a las soluciones SBC en hardware además de que las mismas cuentan con un servicio de soporte incluido en sus precios.
- La implementación de una solución de un Session Border Controller OpenSource, es recomendable usarla para ámbitos de PYMES debido a que este tipo de solución resulta en bajos costos económicos a primera vista, sin embargo, el costo por conocimientos necesarios para realizar la implementación del mismo pueda resultar mucho mayor a la de uno por hardware o software privado. Para definir correctamente que tipo de SBC se debe implementar en una empresa es necesario realizar los respectivos estudios sobre lo que se requiere proteger y la infraestructura con la que se cuenta para ello.

- Para el análisis de las vulnerabilidades dentro de un sistema de VoIP, dos herramientas son esenciales para dicho estudio, la primera de ellas es Wireshark como analizar de paquetes (sniffer) y el Sistema Operativo Kali Linux diseñado exclusivamente para el análisis de vulnerabilidades; el cual cuenta con las herramientas necesarias para probar las fortalezas y debilidades de nuestros sistemas de seguridad implementados. Contra el ataque de un sniffer como lo es Wireshark la mejor solución es usar la encriptación de paquetes de voz. Cuando hablamos de ataques de DDoS y escaneo de dispositivos SIP ambos se los puede realizar desde Kali Linux, la solución de un SBC es la mejor defensa debido a que este tipo de ataques provienen desde el exterior, y el SBC se encarga de mitigar los efectos que pueden lograr este tipo de ataques dada a la configuración básica que el mismo tiene.
- Durante este estudio se logró establecer que cada tipo de SBC existente en el mercado se puede aplicar a ciertos tipos de escenarios para los cuales fueron desarrollados, del igual manera, la encriptación de paquetes se la puede realizar desde el mismo servidor de VoIP que se esté usando o incluso si se tiene implementaciones de VoIP completamente por hardware dicha encriptación ya viene incluida en los mismo dispositivos terminales (teléfonos IP).

Recomendaciones

- Realizar un análisis previo del escenario sobre el cual se vaya trabajar y verificar si la solución de SBC seleccionada se adapta al mismo, para evitar la realización de trabajos extras en cambios ya sea sobre el escenario o buscando otro.
- Realizar un estudio basándose en un mismo escenario con dos diferentes tipos de SBC ya sean por hardware, software o mixto; para comprobar si la implementación de un SBC se aplica a cualquier tipo de escenario propuesto.

Lista de Referencias

3CX Innovating Communications. (2 de Octubre de 2014). Obtenido de 3CX Innovating Communications: http://www.3cx.es/voip-sip/voz-sobre-ip/

3CX Innovating Comunication. (25 de Agosto de 2015). *3CX Innovating Comunication*. Obtenido de http://www.3cx.es/voip-sip/central-telefonica-pbx/

Arcos Gaón, L. M. (25 de Febrero de 2016). Voz sobre IP. *Voz sobre IP*. Ibarra, Pichincha, Ecuador.

Barcia Esparza, E. A. (Diciembre de 2015). TRABAJO DE INVESTIGACIÓN CIENTÍFICA . *Sistema De Comunicación Voip Para La Empresa Coandes Cía. Ltda. Sucursal Esmeraldas*. Esmeraldas, Esmeraldas, Ecuador.

Caceres Guayanlema, J. S. (2014). Tesis de Grado. *Analisis De Vulnerabilidades En Protocolos Utilizados En Centrales Voip Con Ipv6 Utilizando Troncales Sip*. Riobamba, Ecuador.

Cennamo, P., Fresa, A., Longo, M., Postiglione, F., Robustelli, A. L., & Toro, F. (2009). *E-business and Telecommunications.* Berlin: Springer-Verlag.

Cisco. (2009). *Cisco docs*. Recuperado el 27 de Mayo de 2015, de Cisco TelePresence Secure Communications and Signaling: http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Video/telepresence.html

CISCO. (30 de Mayo de 2010). *CISCO*. Obtenido de CISCO: http://www.cisco.com/web/ES/solutions/es/voice_over_ip/index.html

ControlNET. (26 de Agosto de 2016). *ControlNET*. Obtenido de ControlNET - Centrales IP – Software PBX: http://www.controlnet.cl/centrales-ip-software/

EcuRed: Conocimiento con todos y para todos. (10 de Mayo de 2015). Obtenido de Conocimiento con todos y para todos:

http://www.ecured.cu/index.php/Metodolog%C3%ADa_de_la_investigaci%C3%B3n_documental

Galán Amador, M. (13 de Septiembre de 2011). *Metodología de la Investigación*. Obtenido de http://manuelgalan.blogspot.com/2011/09/la-investgacion-documental_1557.html

Gallego León, J., & Ruiz Delgado, J. M. (25 de 08 de 2016). *http://hpc.aut.uah.es/*. Obtenido de http://hpc.aut.uah.es/: http://hpc.aut.uah.es/~jgallego/LabAR/Prac_3/Prac3.ManualWireshark.pdf

Gil, M. (06 de Abril de 2015). *Teldat*. Obtenido de El ABC del SBC: definición, características y ventajas: http://blog.teldat.com/?p=410&lang=es

González, G. (6 de 11 de 2016). *blogthinkbig.com*. Obtenido de http://blogthinkbig.com/ataque-ddos/

Guamán Ullauri, M. A. (2015). Tesis de Grado. *Implementación De Un Sistema De Comunicaciones Unificadas Ip En Una Empresa Mediana Usando Software Con Licencia Pagada*. Guayaquil, Guayas, Ecuador.

Gutiérrez Gil, R. (22 de Mayo de 2015). *Universidad de Valencia.* Obtenido de Universidad de Valencia: http://www.uv.es/montanan/ampliacion/trabajos/Seguridad%20VoIP.pdf

Hautakorpi, J., Camarillo, G., Penfield, R., Hawrylyshen, A., & Bhatia, M. (Abril de 2010). Requirements from Session Initiation Protocol (SIP) Session Border Control (SBC) Deployments. *RFC 5853*.

IPNET. (10 de 11 de 2014). *ELEVA TU LÍMITE*. Obtenido de https://elevatulimite.wordpress.com/2014/11/10/que-es-un-ataque-ddos-y-como-funciona/

Janssen, C. (29 de Noviembre de 2012). *Techopedia*. Obtenido de Techopedia: http://www.techopedia.com/definition/16483/secure-real-time-protocol-secure-rtp-or-srtp

Kihun, H., Souhwan, J., Lo, I. L., & Christoph, R. (2005). *Information Security Applications.* Berlin: Springer-Verlag.

Krasheninnikova, E. (25 de Agosto de 2013). SEGURIDAD EN VOIP. *APLICACIÓN DE SEÑUELOS*. Madrid, España. Obtenido de http://www.dit.upm.es/: http://www.dit.upm.es/~posgrado/doc/TFM/TFMs2012-2013/TFM_Elena_Krasheninnikova_2013.pdf

Leal, L. J. (09 de Agosto de 2016). *ASESORIA DE TESIS Y TRABAJOS DE GRADO*. Obtenido de ASESORIA DE TESIS Y TRABAJOS DE GRADO: http://asesoriatesis1960.blogspot.com/2010/09/asesoria-de-tesis-trabajos-de-grado-e_05.html

López, E. A. (09 de Agosto de 2016). *Eumed.net Enciclopedia Virtual*. Obtenido de Eumed.net Enciclopedia Virtual: http://www.eumed.net/tesis-doctorales/2012/eal/metodologia_cuantitativa.html

Mayr, R. (5 de Mayo de 2015). *Teldat*. Obtenido de VoIP y seguridad: http://blog.teldat.com/?p=448&lang=es

Mendez Molina, M. M. (Mayo de 2015). Monografia. *Telefonia Ip Y Sus Caracteristicas Funcionales Como Desarrollo En La Comunicación*. Ventanas, Ecuador.

Menghui, Y., & Hua, L. (2013). Implementation and performance of VoIP interception based on SIP session border controller. *Telecommunication Systems* , 345-361 .

Psicologia Online. (10 de Mayo de 2015). Obtenido de Psicologia Online: http://www.psicologia-online.com/pir/la-metodologia-experimental.html

Quarea Voz Datos IP. (14 de Septiembre de 2015). *http://www.quarea.com/es/asterisk_funcionalidades_basicas_avanzadas*. Obtenido de http://www.quarea.com/es/asterisk_funcionalidades_basicas_avanzadas

Quobis. (5 de Marzo de 2012). *Slideshare*. Obtenido de Webinar seguridad VoIP: http://es.slideshare.net/Quobis/webinar-seguridad-voip

Rodriguez Espinoza, J. (07 de 06 de 2015). Voz sobre IP. *Voz sobre IP*. Guayaquil, Guayas, Ecuador.

Rodriguez U., M. L. (7 de Marzo de 2012). *Metodologías de la Investigación*. Obtenido de Metodologías de la Investigación: https://metodologiasdelainvestigacion.wordpress.com/2012/03/07/introduccion-general-a-la-metodologia-de-la-investigacion/

Rojano, E. (16 de 12 de 2013). *Qué es un SIP Proxy y cual elegir ¿Kamailio u openSIPS?* Obtenido de https://www.sinologic.net/blog/2013-12/introduccion-sip-proxy-kamailio-opensips.html

Rouse, M. (7 de Mayo de 2015). *Techtarget*. Obtenido de Techtarget: http://searchtelecom.techtarget.com/definition/session-border-controller

Suicidemouse. (25 de Octubre de 2014). *Free Hacks*. Obtenido de Free Hacks: https://freehacks.ru/showthread.php?t=1807

Valle, J. (14 de Noviembre de 2015). Voz sobre IP. *Voz sobre IP*. Guayaquil, Guayas, Ecuador.

Ye, S., & Yu, Q. (2014). Method For Implementing Session Border Controller Pool, And Session Border Controller. *United States Patent Application Publication*.

ANEXOS

Anexo 1. Instalación Asterisk 1.8

AsteriskNow es una distribución especialmente adaptada para hacer funcionar Asterisk en cuestión de minutos ya que viene con todos los requerimientos y dependencias de software pre configuradas como el sistema operativo Linux CentOS 6.5 y Asterisk 1.8, permitiendo una instalación más rápida y sencilla.

Instalación Asterisk

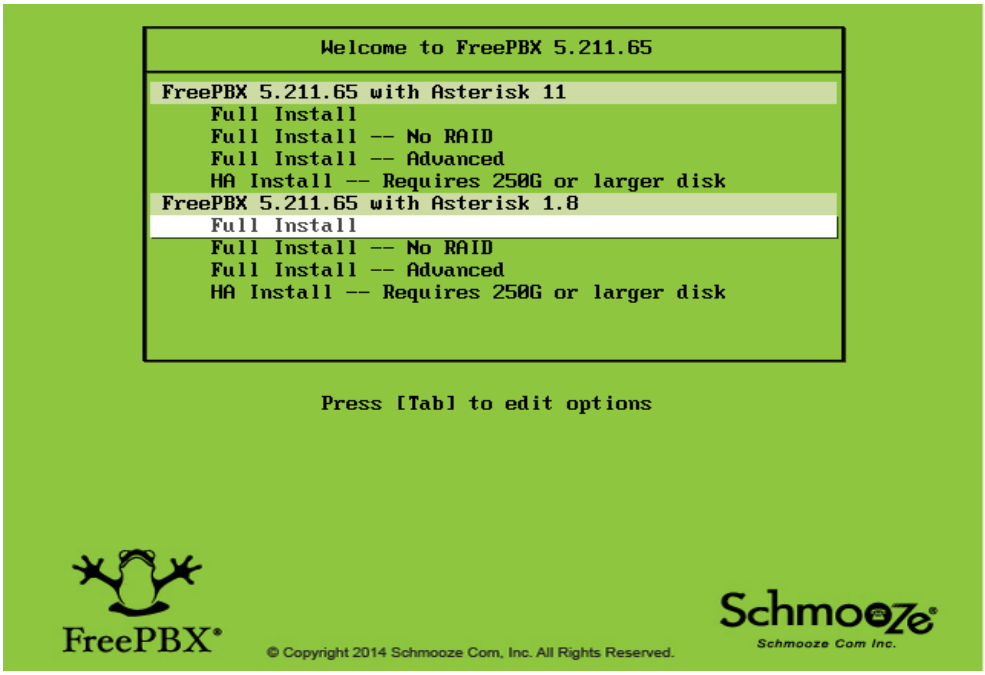

Figura 36. Selección del tipo de Instalación Asterisk
Elaborado por: Paillacho – Yánez

Para este estudio se instaló la versión 1.8 de Asterisk y FreePBX 5.211.65 como entorno grafico para una fácil administración y configuración de características específicas de Asterisk. La opción elegida fue Full Install.

Continuando con la instalación lo siguiente es seleccionar la tarjeta de red con la se trabajará en caso de que el equipo posea más de una, así como también la configuración IP de la misma y en este caso la configuración fue de IP estática.

Selección tarjeta red

Figura 37. Selección de la tarjeta de red en la instalación
Elaborado por: Paillacho – Yánez

Configuración TCP/IP

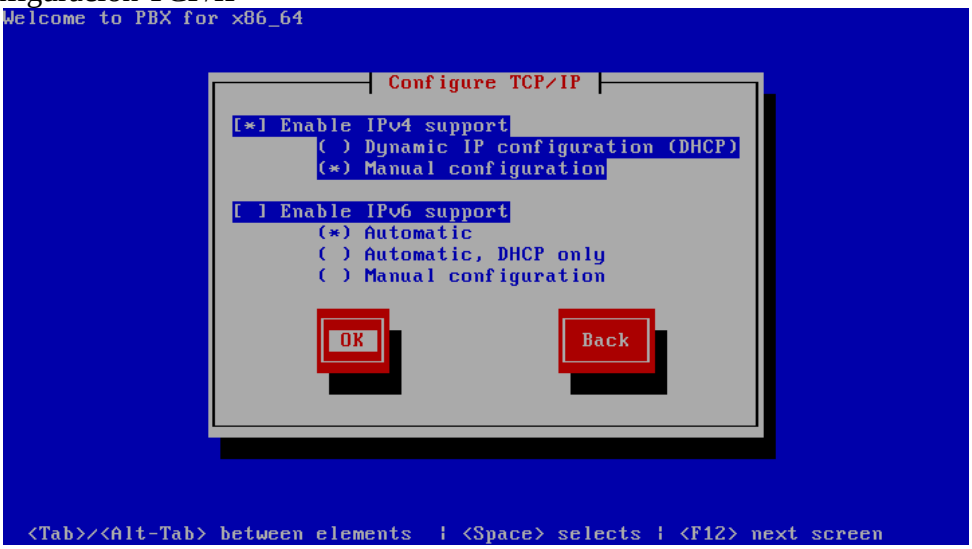

Figura 38. Configuración de los protocolos IP a usarse
Elaborado por: Paillacho – Yánez

Configuración direcciones

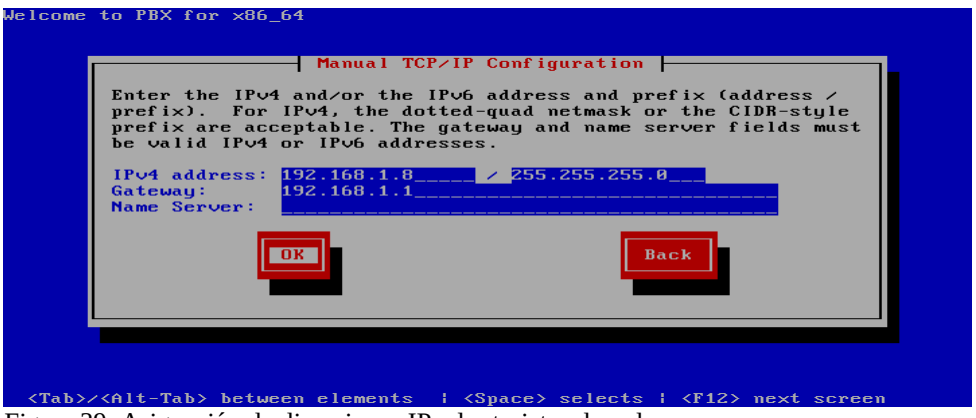

Figura 39. Asignación de direcciones IP a las tarjetas de red
Elaborado por: Paillacho – Yánez

Continuando con la instalación lo siguiente es seleccionar la zona horaria y configurar una contraseña para el usuario administrador.

Zona Horaria

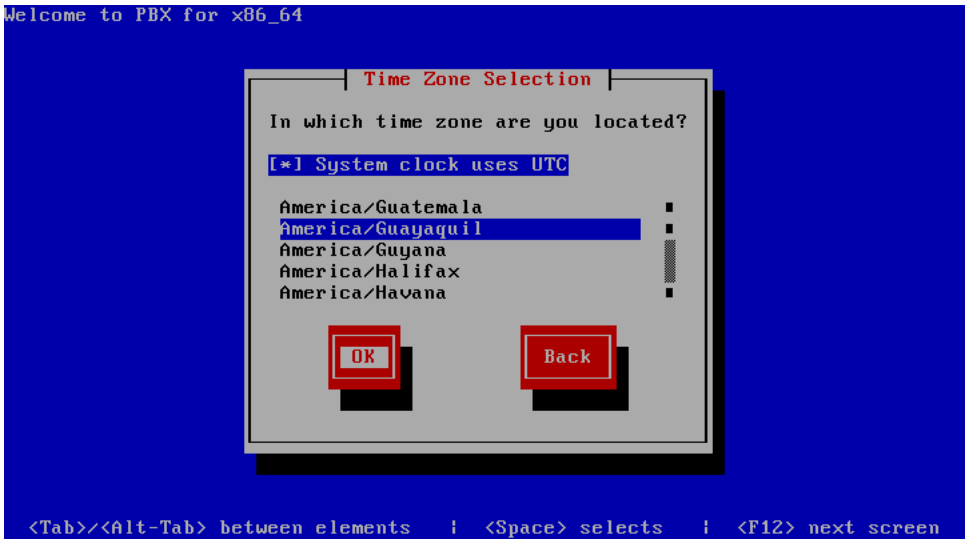

Figura 40. Selección de la zona horaria adecuada
Elaborado por: Paillacho – Yánez

Creación contraseña ROOT

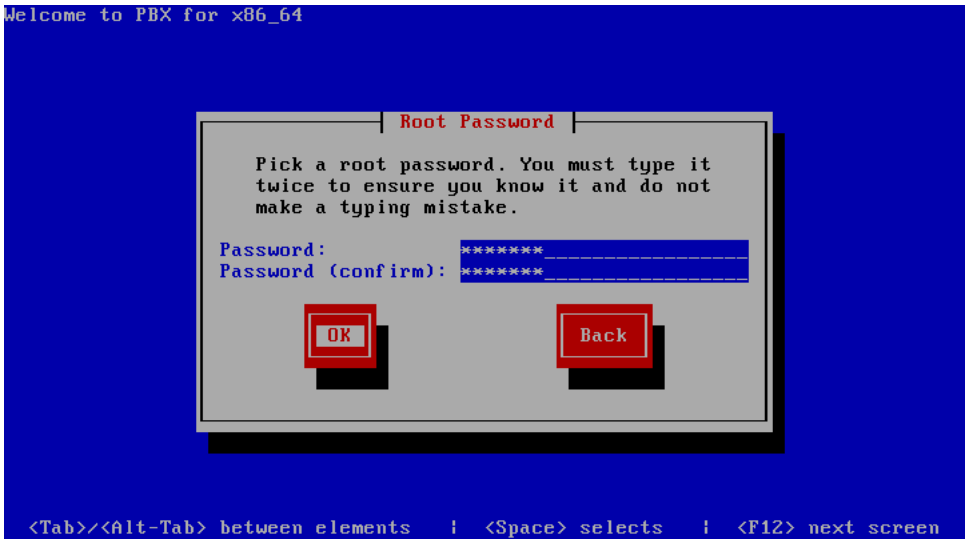

Figura 41. Asignación de una contraseña para el usuario ROOT del sistema
Elaborador por: Paillacho – Yánez

Una vez terminado los pasos previos la instalación comenzará y mostrara una barra de progreso la cual una vez llena finalizará con la instalación y reiniciará automáticamente el equipo.

Con la instalación finalizada al equipo solo se puede ingresar mediante consola ya no que no posee modo grafico propio del sistema operativo así que para las posteriores configuraciones se ingresará desde un equipo remoto mediante un navegador web.

Para realizar la configuración mediante navegador en el mismo ingresamos la dirección IP correspondiente que fue previamente configurada en la instalación. La ventana que se mostrará por primera vez indicará la creación de un usuario y su respectiva contraseña; cabe aclarar que este usuario es independiente del usuario administrador del sistema operativo donde estará funcionando Asterisk.

Creación usuario de la GUI

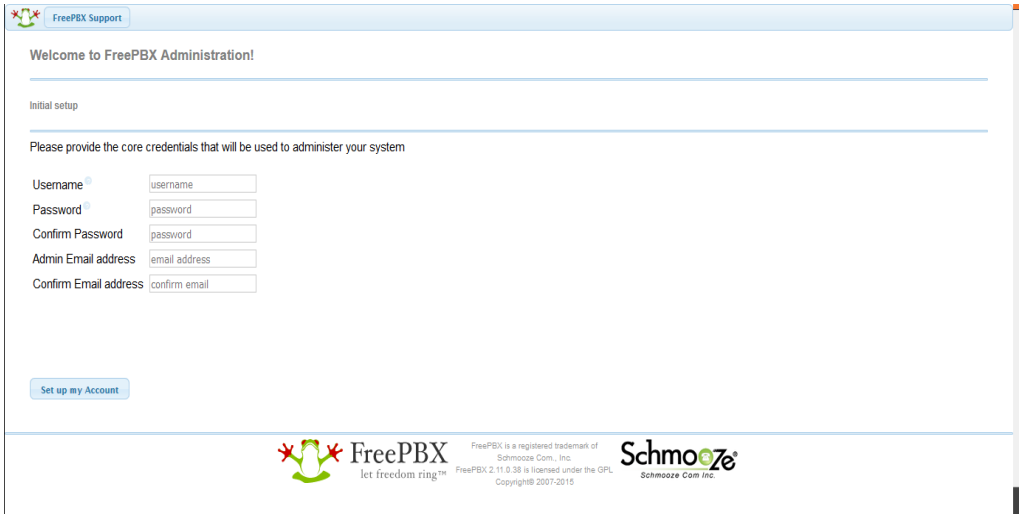

Figura 42. Creación y asignación de contraseña a un usuario de la GUI de Asterisk
Elaborado por: Paillacho – Yánez

Ventana final

Figura 43. Ventana final de la GUI antes de empezar a trabajar con Asterisk
Elaborado por: Paillacho – Yánez

Anexo 2. Instalación de BLOX - SBC

Para la instalación del Session Border Controller se eligió a BLOX porque además de poseer una interfaz gráfica administrativa de fácil uso es Open Source. Para la instalación se debe tener en cuenta que en el equipo donde se vaya a realizar la instalación deberá tener al menos dos tarjetas de red.

Una vez insertado el disco de instalación en el equipo aparecerá la siguiente pantalla.

Instalación BLOX

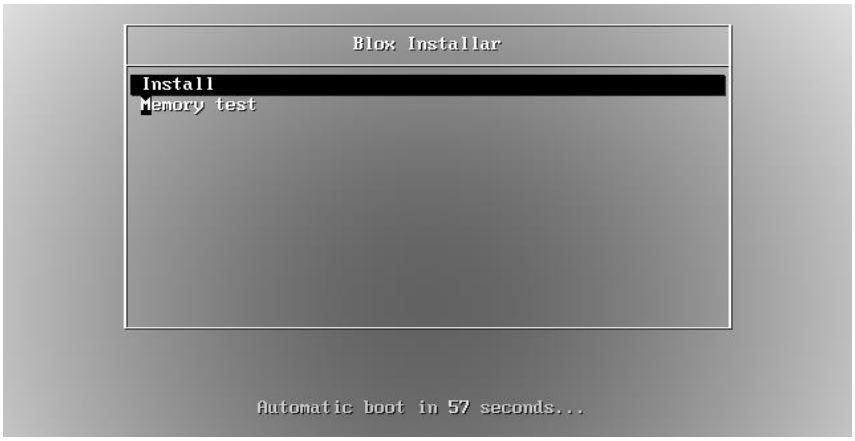

Figura 44. Instalación de BLOX como SBC
Elaborado por: Paillacho – Yánez

Lo siguiente después de escoger la opción "Install", es seleccionar el idioma del sistema y posterior al mismo el idioma del teclado que se está usando.

Selección del Idioma

Figura 45. Selección del idioma a utilizarse en el SO
Elaborado por: Paillacho – Yánez

Idioma Teclado

Figura 46. Selección idioma del teclado que reconocerá el SO
Elaborado por: Paillacho – Yánez

Posterior a lo realizado anteriormente es seleccionar la zona horaria donde se encuentra localizado el equipo en donde se instalará el SBC y así como también proporcionar una contraseña para el usuario administrador.

Zona Horaria

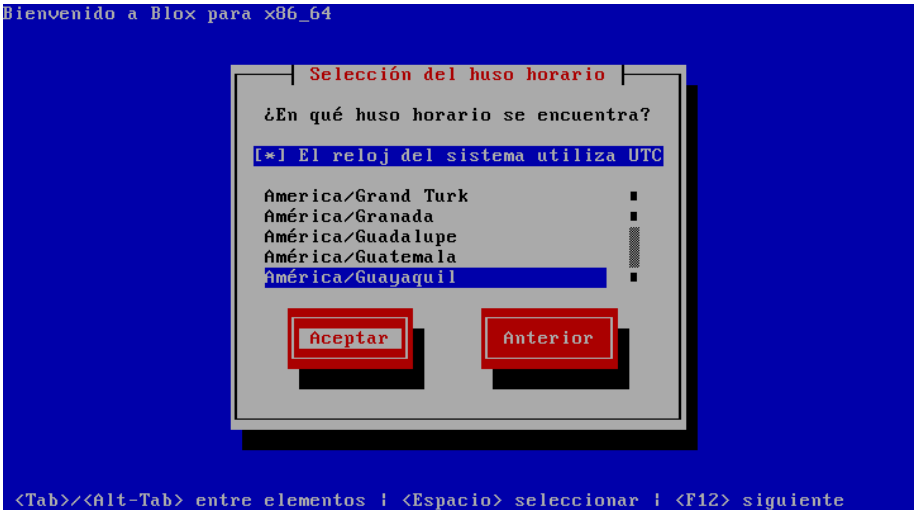

Figura 47. Selección de zona horaria adecuada
Elaborado por: Paillacho – Yánez

Contraseña root

Figura 48. Asignación de contraseña al usuario root
Elaborado por: Paillacho – Yánez

Como paso final es seleccionar la opción de cómo se instalará el sistema si será en todo el disco o en alguna partición en específico y finalmente aparecerá la pantalla con la barra de progreso de la instalación.

Anexo 3. Configuración certificados para encriptación de datos

Cuando de seguridad se trata lo primero antes de crear nuestras extensiones dentro del servidor de VoIP es crear los certificados necesarios para la encriptación de los paquetes de voz, para ello se realizan los siguientes pasos dentro del FreePBX que es la interfaz GUI de Asterisk.

Primero dentro del menú Admin, buscar la opción Certificate Management, tal como se muestra en la siguiente imagen.

Creación CA

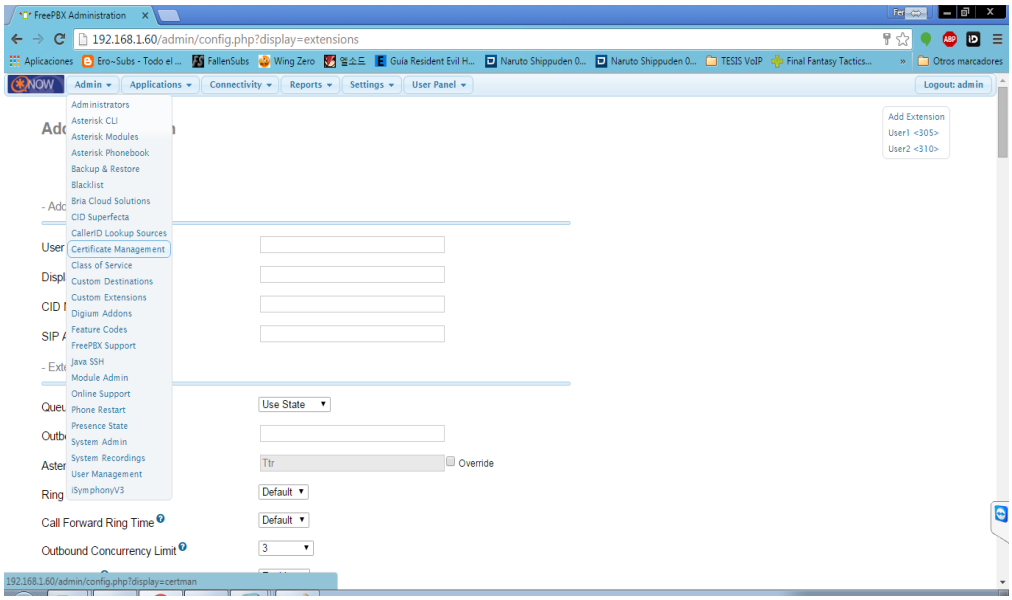

Figura 49. Creación Certificate Authority Settings
Elaborado por: Paillacho – Yánez

Una vez dentro de esta opción lo primero es crear un Certificate Authority Settings (CA) en caso de que no existiera uno, por defecto Asterisk crea un certificado CA por defecto cuando se instala, así una vez seleccionada esta opción dentro del FreePBX aparecerá algo similar a lo que se muestra en la siguiente figura.

Eliminar Certificado autorización por defecto.

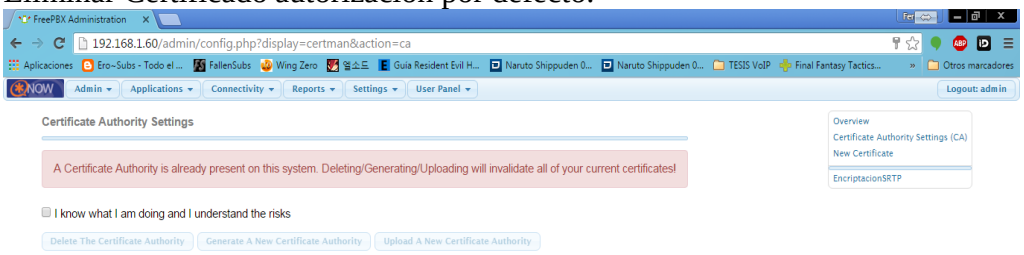

Figura 50. Eliminación certificado por defecto
Elaborado por: Paillacho Yánez

Se recomienda eliminar el certificado por defecto y crear uno nuevo con los parámetros que se crea conveniente, cuando el certificado CA este creado el siguiente paso es crear el certificado que será usado por las extensiones SIP.

Cuando se crea este certificado lo único que se debe hacer es seleccionar el CA, darle un nombre y una descripción adecuada para dicho certificado, tal como se muestra en la imagen siguiente.

Nombrar Certificado Autorización

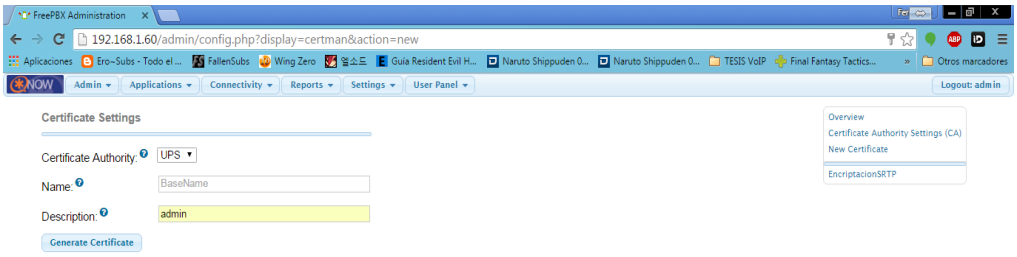

Figura 51. Nombrar certificado por defecto
Elaborado por: Paillacho Yánez

Anexo 4. Creación de extensiones SIP en Asterisk usando los certificados para encriptación

Los pasos para la creación de extensiones SIP son sencillos, al menos si se lo realiza utilizando la ayuda de la GUI que proporciona FreePBX. Lo primero que se debe hacer para crear una extensión SIP es dirigirse al siguiente menú.

Creación extensión.

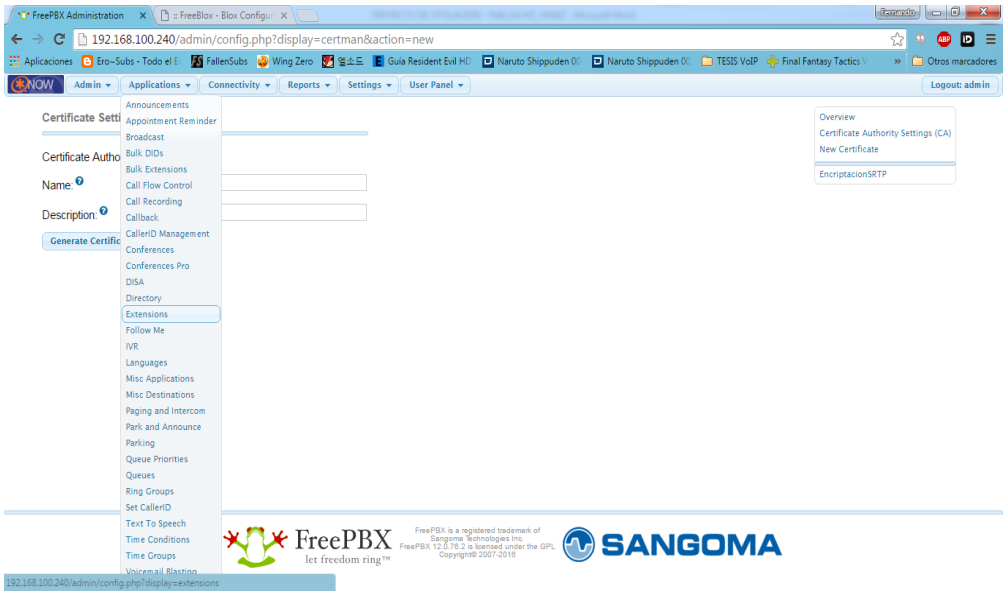

Figura 52. Creación extensión
Elaborado por: Paillacho – Yánez

Una vez dentro del Menú, seleccionar la opción Add Extension, y en la opción de Device seleccionar Generic CHAN SIP Device y click en el botón Submit.

Dentro de esta opción es donde por fin se procederá a crear la extensión con todas sus características.

Crear Extensión SIP

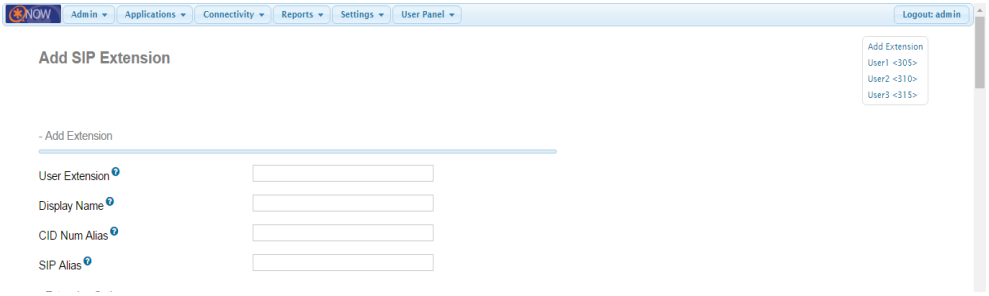

Figura 53. Crear extensión SIP
Elaborado por: Paillacho – Yánez

De las primeras opciones que se muestran cuando se crea una extensión se tiene las que se muestran en la imagen anterior.

User Extension.- Es el nombre de la extensión, normalmente es un valor numérico

Display Name.- El nombre que se desplegara a las otras extensiones cuando esta intente comunicarse.

CID Num Alias y **SIP Alias** son parámetros opcionales por lo que no se los mencionará.

El siguiente grupo de opciones de vital importancia para crear una extensión son los que se muestran a continuación

Seguridad extensión SIP

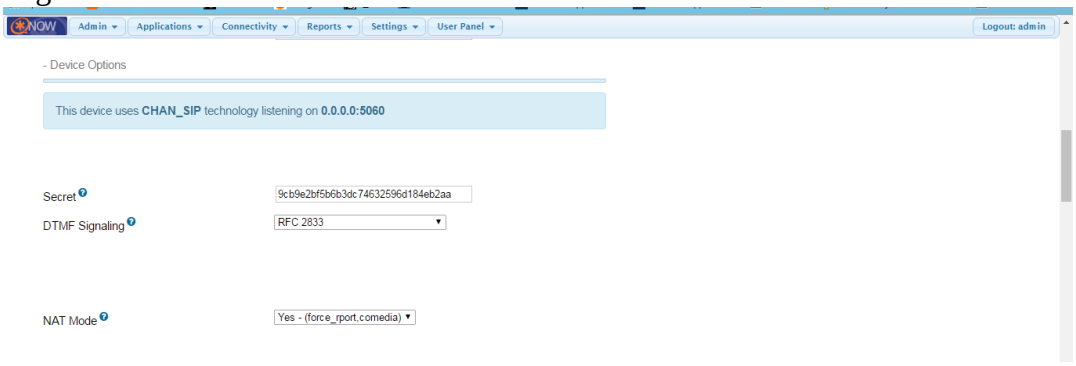

Figura 54. Contraseña en extensión SIP.
Elaborado por: Paillacho – Yánez

El parámetro **Secret** es el más importante ya que es la contraseña que tendrá dicha extensión y es la que se necesitará para poder enlazar un teléfono IP o un softphone con esta extensión, si la rigurosidad que mantiene Asterisk para sus contraseñas no fue

cambiada, el valor para el parámetro Secret debe ser del tipo alfanúmero con al menos una letra y un número para que sea válida.

El siguiente grupo es el más importante ya que será en donde especifiquemos que nuestra extensión usará un certificado para cifrar sus llamadas

Crear certificado de encriptamiento.

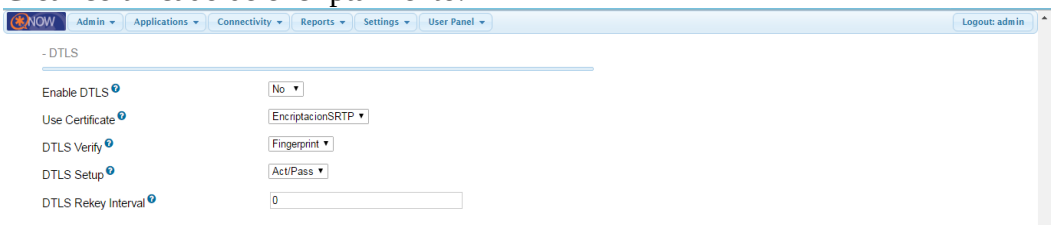

Figura 55. Certificado de encriptamiento.
Elaborado por: Paillacho – Yánez

Este grupo es el DTLS, las opciones son las siguientes:

Enable DTLS.- Escoger Yes para habilitar el uso del certificado en esta extensión

Use Certificate.- Seleccionar el certificado correspondiente para esta extensión si dentro del servidor Asterisk existen varios certificados creados.

DTLS Verify.- Marcar en la opción No

Los restantes parámetros dejar los valores por defecto.

Una vez llenados los parámetros anteriores que son los mínimos requeridos para una extensión que usara encriptación en sus llamadas dar click en botón de Submit y la extensión estará creada.

ANEXO 5: Configuración de la integración de Asterisk con BLOX

Una de las configuraciones más importantes realizadas dentro de este estudio, fue la de integrar BLOX que es el SBC hacia Asterisk para poder realizar la comunicación con las seguridades que ofrece un SBC.

Dichas configuraciones se basarán en el siguiente escenario:

Topología de red.

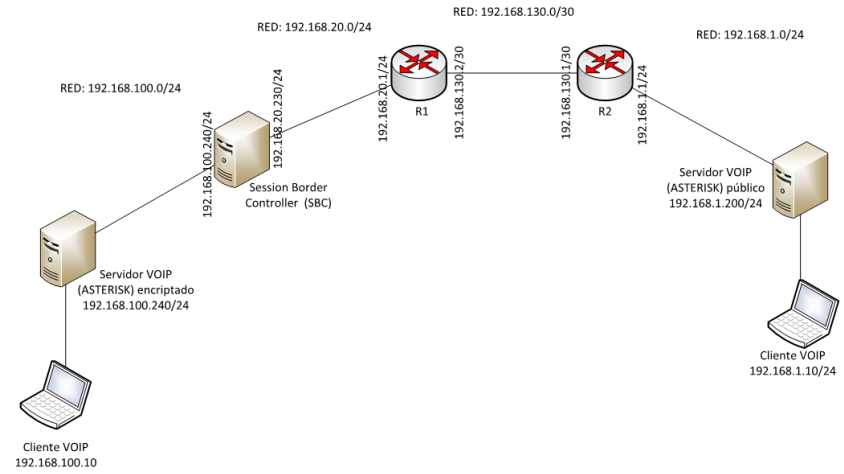

Figura 56. Topología de red.
Elaborado por: Paillacho – Yánez

Para realizar las configuraciones pertinentes dentro de BLOX se usara la ayuda de una GUI, dentro de la cual lo primero es configurar las interfaces de red del equipo que hará de SBC.

Colocar las direcciones IP correspondientes tanto para la interfaz LAN y WAN, según el esquema mostrado anteriormente.

Configuracón IP en BLOX

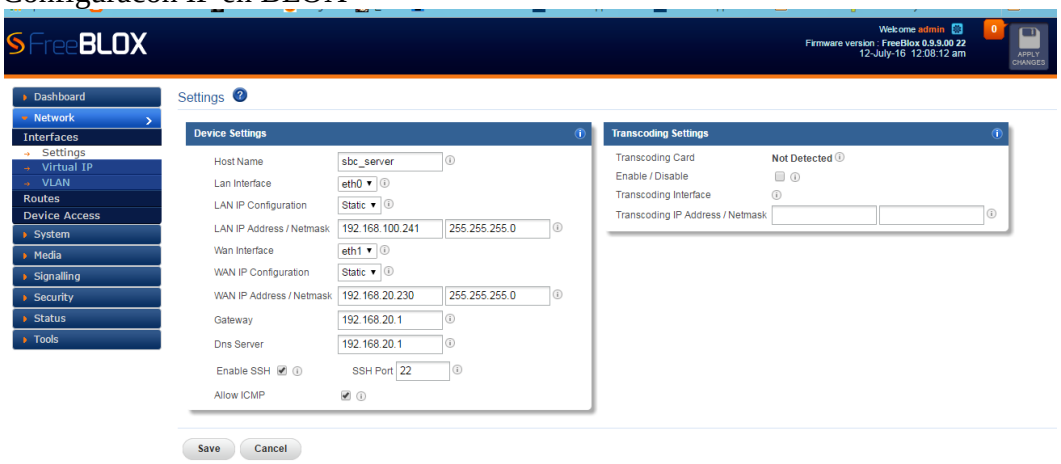

Figura 57. Configurar direcciones IP´s en BLOX.
Elaborado por: Paillacho – Yánez

Lo siguiente es crear los perfiles SIP tanto para la interfaz LAN y WAN

Configurar Perfile SIP

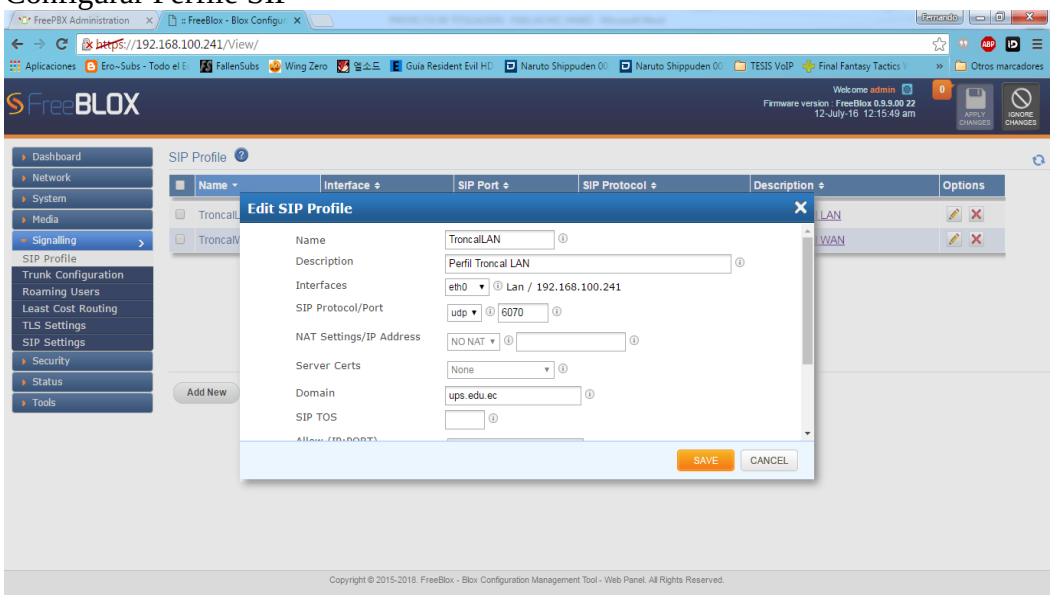

Figura 58. Configuración perfil SIP LAN.
Elaborado por: Paillacho – Yánez

Configurar perfil SIP

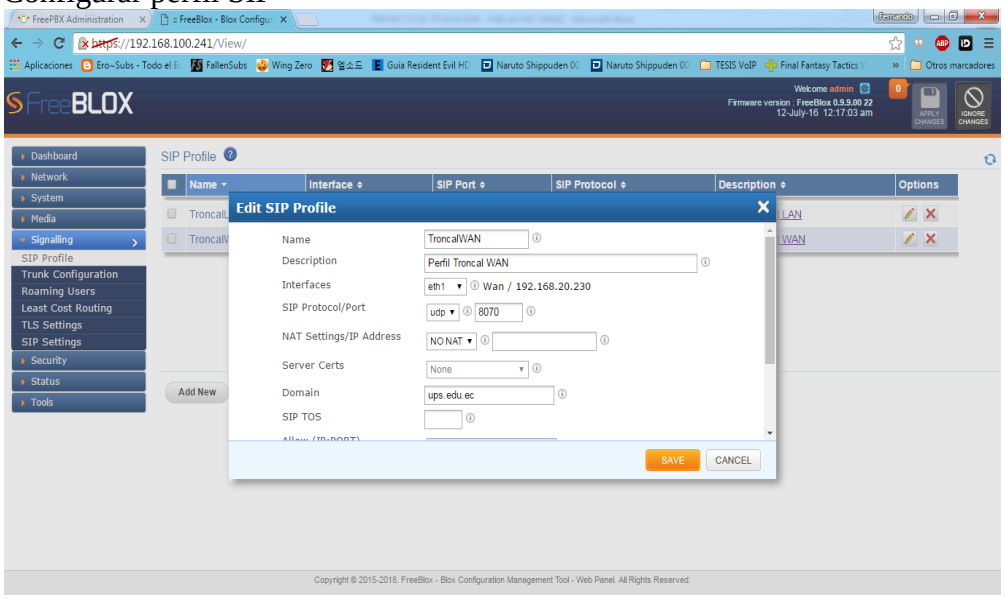

Figura 59. Configuración perfil SIP WAN.
Elaborado por: Paillacho – Yánez

Una vez creados los perfiles SIP el siguiente paso es configurar la troncal (Trunk Configuration) la cual contendrá la información del servidor de VoIP que es el que nos provee el servicio para llamadas externas, así como también los perfiles SIP que se crearon anteriormente, la configuración debe ser similar a lo que se muestra en las siguiente figuras.

Configuración Troncal

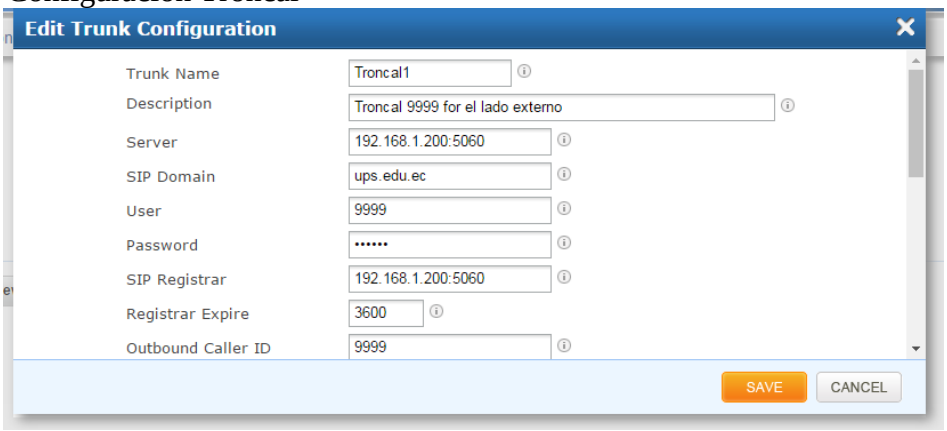

Figura 60. Configuración Troncal
Elaborado por: Paillacho Yánez

Configuración Troncal

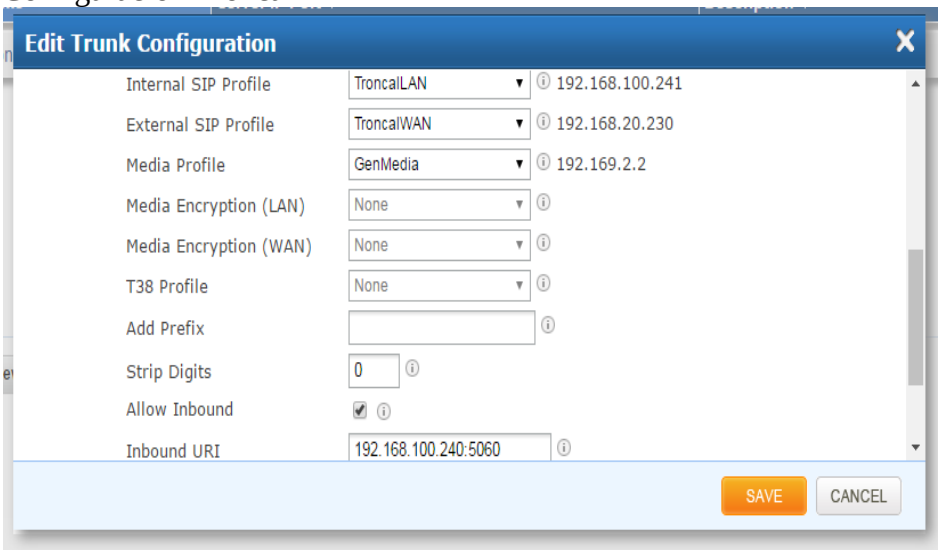

Figura 61. Configuración Troncal.
Elaborado por: Paillacho - Yánez