UNIVERSIDAD TÉCNICA DE COTOPAXI

UNIDAD ACADÉMICA DE CIENCIAS DE LA INGENIERÍA Y APLICADAS

CARRERA DE INGENIERÍA EN INFORMÁTICA Y SISTEMAS COMPUTACIONALES

TESIS DE GRADO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN INFORMÁTICA Y SISTEMAS COMPUTACIONALES

TITULO

"ANÁLISIS E IMPLEMENTACIÓN DE SESSION BORDER CONTROLLERS SBC Y ENCRIPTACIÓN DE PAQUETES APLICADA EN LA SEGURIDAD DEL SISTEMA VOIP EN LA UNIVERSIDAD TECNICA DE COTOPAXI EN EL LABORATORIO DE REDES PERIODO 2015 - 2016."

AUTORES:

Chicaiza Chango Víctor Gabriel

Escobar Quinaluisa Enrique Javier

DIRECTOR DE TESIS

Ing. Mario Banda

LATACUNGA - ECUADOR

2016

FORMULARIO DE LA APROBACIÓN DEL TRIBUNAL DE GRADO

En calidad de Miembros del Tribunal de Grado aprueban el presente Informe de Investigación de acuerdo a las disposiciones reglamentarias emitidas por la Universidad Técnica de Cotopaxi y por la Unidad Académica de Ciencias de la Ingeniería y Aplicadas; por cuanto, los postulantes:

- Chicaiza Chango Víctor Gabriel
- Escobar Quinaluisa Enrique Javier

Con la tesis, cuyo título es:

"ANÁLISIS E IMPLEMENTACIÓN DE SESSION BORDER CONTROLLERS SBC Y ENCRIPTACIÓN DE PAQUETES APLICADA EN LA SEGURIDAD DEL SISTEMA VOIP EN LA UNIVERSIDAD TECNICA DE COTOPAXI EN EL LABORATORIO DE REDES PERIODO 2015 - 2016."

Han considerado las recomendaciones emitidas oportunamente y reúnen los méritos suficientes para ser sometidos al **Acto de Defensa de Tesis** en la fecha y hora señalada.

Por lo antes expuesto, se autoriza realizar los empastados correspondientes, según la normativa institucional.

Latacunga, 21 de Marzo del 2016

Para constancia firman:

Ing. Segundo Corrales
PRESIDENTE

Dr. Edwin Vaca
MIEMBRO

Ing. Víctor Medina
OPOSITOR

Ing. Mario Banda
TUTOR (DIRECTOR)

AUTORIA

Todos los criterios emitidos en el presente trabajo de investigación:

"ANÁLISIS E IMPLEMENTACIÓN DE SESSION BORDER CONTROLLERS SBC Y ENCRIPTACIÓN DE PAQUETES APLICADA EN LA SEGURIDAD DEL SISTEMA VOIP EN LA UNIVERSIDAD TÉCNICA DE COTOPAXI EN EL LABORATORIO DE REDES PERIODO 2015 - 2016."

Son de exclusiva responsabilidad de los autores.

……..	……..
Javier Escobar	Gabriel Chicaiza
C.C:172179759-3	C.C:050307431-2

AVAL DE DIRECTOR DE TESIS

En calidad de Director de trabajo de investigación sobre el tema: **"**ANÁLISIS E IMPLEMENTACIÓN DE SESSION BORDER CONTROLLERS SBC Y ENCRIPTACIÓN DE PAQUETES APLICADA EN LA SEGURIDAD DEL SISTEMA VOIP EN LA UNIVERSIDAD TECNICA DE COTOPAXI EN EL LABORATORIO DE REDES PERIODO 2015 - 2016.**"**

De los señores estudiantes: Víctor Gabriel Chicaiza Chango, Enrique Javier Escobar Quinaluisa postulantes de la Carrera de Ingeniería en Informática y Sistemas Computacionales,

CERTIFICO QUE:

Una vez revisado el documento entregado a mi persona, considero que dicho informe investigativo cumple con los requerimientos metodológicos y aportes científicos - técnicos necesarios para ser sometidos a **Evaluación del Tribunal de Validación de Tesis** que el Honorable Consejo Académico de la Unidad de Ciencias de la Ingeniería y Aplicadas de la Universidad Técnica de Cotopaxi designe para su correspondiente estudio y calificación.

Latacunga, 21 Marzo del 2016

EL DIRECTOR

.....

Ing. Mario Banda

C.C 0501916852

DIRECTOR DE TESIS

Universidad Técnica de Cotopaxi

ASESOR METODOLÓGICO

AVAL DE ASESOR METODOLÓGICO

En calidad de **Asesor Metodológico** del Trabajo de Investigación sobre el tema:

"ANÁLISIS E IMPLEMENTACIÓN DE SESSION BORDER CONTROLLERS SBC Y ENCRIPTACIÓN DE PAQUETES APLICADA EN LA SEGURIDAD DEL SISTEMA VOIP EN LA UNIVERSIDAD TECNICA DE COTOPAXI EN EL LABORATORIO DE REDES PERIODO 2015 - 2016."

De los señores estudiantes; Víctor Gabriel Chicaiza Chango, Enrique Javier Escobar Quinaluisa, postulantes de la Carrera de Ingeniería en Informática y Sistemas Computacionales,

CERTIFICO QUE:

Una vez revisado el documento entregado a mi persona, considero que dicho informe investigativo cumple con los requerimientos metodológicos y aportes científicos - técnicos necesarios para ser sometidos a la **Evaluación del Tribunal de Validación de Tesis** que el Honorable Consejo Académico de la Unidad de Ciencias de la Ingeniería y Aplicadas de la Universidad Técnica de Cotopaxi designe para su correspondiente estudio y calificación.

Latacunga, 21 de Marzo del 2016

.....

Dra. Anita Chancusi

ASESOR METODOLÓGICO

CERTIFICADO DE IMPLEMENTACIÓN

CERTIFICADO

Mediante el presente pongo a consideración, que los Egresados, Víctor Gabriel Chicaiza Chango portadora de C.C. # 050307431-2, Enrique Javier Escobar Quinaluisa portadora de C.C. #172179759-3, realizaron su Proyecto de Tesis en la **Carrera de Ingeniería en Informática y Sistemas Computacionales**, con el tema: **"ANÁLISIS E IMPLEMENTACIÓN DE SESSION BORDER CONTROLLERS SBC Y ENCRIPTACIÓN DE PAQUETES APLICADA EN LA SEGURIDAD DEL SISTEMA VOIP EN LA UNIVERSIDAD TECNICA DE COTOPAXI EN EL LABORATORIO DE REDES PERIODO 2015 - 2016."**

Trabajo que se implementó y se dejó en completo funcionamiento.

Es todo cuanto puedo certificar, pudiendo hacer uso del mismo dentro de las leyes de la Republica y Normas Internacionales.

Latacunga, 21 Marzo de 2016

Atentamente,

.....

Ing. Jorge Bladimir Rubio Peñaherrera
C.C 0502222292
Coordinador de la Carrera de Ingeniería en Informática y Sistemas Computacionales

AGRADECIMIENTO

Primero doy gracias infinitamente a Dios, por guiarme y darme fuerzas para culminar mis estudios universitarios. Agradezco a mi madre y a toda mi familia que gracias a sus consejos brindados durante mi preparación profesional me han guiado y han sido un pilar fundamental en mi vida. A todos los maestros de la UNIVERSIDAD TECNICA DE COTOPAXI especialmente al Ing. Mario Banda por aceptar la realización del trabajo de Tesis bajo su dirección. Su apoyo y confianza en la realización del trabajo investigativo ya que atreves de su guía los proporciono las bases suficientes durante la investigación.

A la Universidad Técnica de Cotopaxi de la Unidad Académica Ciencias de la Ingeniería y Aplicadas de la Carrera Ingeniería informática y sistemas computacionales quien nos permitió realizar el trabajo de tesis a través de su confianza y apoyo incondicional.

Javier

DEDICATORIA

Dedico esta tesis primero a Dios, por darme la oportunidad de vivir y estar siempre contigo, por guiarme e iluminar mi mente y por haberme puesto en mi camino personas importantes durante mi preparación profesional.

Mi madre Carlota Quinaluisa, por darme la vida, por creer en mí y porque me apoyo moralmente y económicamente para poder ser un profesional.

Mis tíos, primos por estar dispuestos ayudarme durante mi preparación universitaria.

Todos mis amigos y compañeros de la Universidad Técnica de Cotopaxi quien hemos compartido momentos buenos y difíciles durante mi preparación profesional.

Javier

AGRADECIMIENTO

EL presente proyecto de tesis agradezco a mi Dios por nuca haberme abandonado y bendecirme con su amor por permitirme llegar hasta donde he llegado. Por permitir hacer realidad un sueño tan anhelado. A la UNIVERSIDAD TÉCNICA DE COTOPAXI por brindarme la oportunidad de estudiar y ser un profesional. A mi director de tesis, Ing. Mario Banda por apoyo y dirección, quien con sus conocimientos, su experiencia y paciencia ha logrado en mí que pueda terminar mis estudios con éxito. También me gustaría agradecer a mis profesores que durante toda la carrera profesional, A mi amor Ing. Estefanía Vargas gracias por creer en mí, muchas gracias por hacerme sentir importante y por enseñarme que yo podía hacer la diferencia, y por todo lo que he logrado es por ti.

Gabriel

DEDICATORIA

Dedico este proyecto de tesis primeramente Dios y a mis padres. A Dios por la razón de que siempre ha estado junto a mí, cuidándome y dando fortaleza divina para continuar cada día, a mis padres quienes a lo largo de mi vida han vela por mi bienestar y educación siendo mi apoyo primordial en todo momento. Depositando toda su confianza en cada reto que se prestaba sin dudar ni un solo momento en mi capacidad y perseverancia de cómo llevar una vida responsable y justa. Gracias por el apoyo incondicional y no perder la esperanza en mí. Los amo con toda mi vida.

Gabriel

INDICE GENARAL

INDICE DE GRAFICOS

INDICE DE FIGURAS

INDICE DE TABLAS

RESUMEN

La Propuesta “ANÁLISIS E IMPLEMENTACIÓN DE SESSION BORDER CONTROLLERS SBC Y ENCRIPTACIÓN DE PAQUETES APLICADA EN LA SEGURIDAD DEL SISTEMA VOIP EN LA UNIVERSIDAD TECNICA DE COTOPAXI EN EL LABORATORIO DE REDES “

La presente propuesta de investigación enfoca al aspecto de la inseguridad existente dentro del contexto de la comunicación en el laboratorio de redes de la Universidad técnica de Cotopaxi, en esta realidad se ha evidenciado que la información que fluye dentro de esta red ha sido vulnerada mediante ataques informáticos y accesos ilegales. Dentro del estudio y el análisis técnico se han considerado temáticas como, técnicas de comunicación IP, protocolos para la comunicación, las técnicas de ataques a la red, sesión border controll y Encriptamiento de datos, los cuales fundamentan y orientan el proceso investigativo. Para el estudio y posterior desarrollo de la investigación se han empleado varios métodos que definen los procedimientos, así se tiene presente al método inductivo, método hipotético-deductivo y al método analítico. De esta manera se busca implementar una herramienta adecuada que permita proveer de la seguridad del sistema VoIP basado en la tecnología sesión border controll y Encriptamiento de paquetes el trabajo realizado para la protección de la información de los usuarios que utilizan este medio de comunicación. Esto beneficia a los estudiantes y docentes de la carrera Ingeniería informática y sistemas computacionales de la universidad técnica de Cotopaxi de forma directa ya que podrán mejorar y compartir su información con total seguridad.

ASBTRACT

Proposal "ANALYSIS AND IMPLEMENTATION OF SESSION BORDER CONTROLLERS AND SBC PACKET ENCRYPTION APPLIED AT VOIP SECURITY SYSTEM IN THE TECHNICAL UNIVERSITY OF COTOPAXI LABORATORY NETWORK"

The present proposal research focused on the aspect of insecurity within the context of communication networks in the laboratory at the Cotopaxi Technical University, in this reality has shown that the information flows within this network has been violated by computer attacks and illegal access. Issues such as: IP communication techniques, protocols for communication, network attacks techniques, border control session and data were considered within the study and technical analysis, which based and guided the research process. For the study and further development of the research they have been used several methods to define procedures, so the inductive method, hypothetical-deductive method and the analytical method were presented. In this way it seeks to implement an adequate tool to provide security system based on VoIP session border control and encryption technology package, the done work for the protection of user information using this media. This benefits students and teachers of the major computer systems and computer engineering at the Cotopaxi Technical University directly as they can enhance and share their information safely.

Universidad Técnica de Cotopaxi

CENTRO CULTURAL DE IDIOMAS

AVAL DE TRADUCCIÓN

En calidad de Docente de la Carrera de Ciencias de la Educación, Mención Inglés de la Universidad Técnica de Cotopaxi.

Certifico, que he realizado la revisión del Abstract, de la tesis elaborada por los alumnos: Gabriel Chicaiza y Javier Escobar; con el tema: ""ANÁLISIS E IMPLEMENTACIÓN DE SESSION BORDER CONTROLLERS SBC Y ENCRIPTACIÓN DE PAQUETES APLICADA EN LA SEGURIDAD DEL SISTEMA VOIP EN LA UNIVERSIDAD TECNICA DE COTOPAXI EN EL LABORATORIO DE REDES PERIODO 2015 - 2016."El mismo que cumple con requerimientos técnicos gramaticales del idioma Inglés.

Es todo cuanto puedo certificar en honor a la verdad; pudiendo hacer uso de la presente para los fines legales pertinentes.

Latacunga, 21 de Marzo del 2016

Lic. MSc. Nelly Patricia Mena Vargas
C.I. 0501574297

INTRODUCCIÓN

Es muy evidente el problema sobre la seguridad del sistemas VoIP, los problemas más comunes de la red VoIP son los fraudes, como engañarle al usuario que está manipulando el sistema VoIP para que divulgue los datos personales más valiosos por consecuencia de una acceso desautorizados a una red legal VoIP este ataque es llamado vishing. Otros problemas que pueden afectar el sistema VoIP es la calidad del servicio de las comunicaciones como puede ser la interrupción del sistema VoIP o incluso pueden desconectar este servicio. El problema de la encriptación de paquetes más común es que la mayor parte de su tráfico de información no está encriptados ni cifradas y son vulnerables para que los atacantes puedan robarse la información para fines delictivos.

Con esta investigación se ayudara a mitigar esas amenazas apropiadamente, los riesgos verdaderos deben ser identificados y trazar un mapa de una estructura de seguridad, incluyendo recomendaciones que se han venido usando en las redes de datos normales, así como la implementación del equipo: Session Border Controller. Así como el uso de autenticación de señales encriptación de datos para asegurar que la persona autorizada este llamando.

Para los estudiantes de la Carrera Ingeniería en informática y Sistemas Computacionales a los alumnos de los niveles superiores de la UTC la implementación Session Border Controller y Encriptamiento de paquetes es una solución que permitirá a los encargados del servicio controlar y monitorear las anomalías que se pueden dar en el sistema VoIP las 24 hora del día esto permitirá la toma de decisiones eficientes, identificación de las áreas en las que más se detectan las ataques informáticos.

Todo esto con motivo de mejorar la seguridad en las conversaciones. Este marco puede ser usado para establecer requisitos de seguridad para que entonces los productos usados obtengan un apropiado nivel de seguridad para la solución de estos problemas.

El capítulo I detalla la información sobre las comunicaciones mediante VoIP, protocolos utilizados en el sistema VoIP, seguridad en la red, Técnicas de ataque en la red, Session Border Controller y Encriptamiento de paquetes y demás información que requiera para sustentar la investigación. La información sobre las metodologías que ayuden a llegar la consecución de la implementación motivo de la investigación.

En el capítulo II se realiza un trabajo de campo basada en las metodologías de investigación tradicionales como la entrevistas al personal estudiantil que intervendrá en el desarrollo del proyecto, se comprobara la hipótesis plateada en el anteproyecto, todo esto basado en las normas que rigen la realización de proyectos en la Universidad.

El capítulo III se plantea la propuesta para solucionar el problema plateado en cuanto tiene que ver con la Universidad Técnica de Cotopaxi en los laboratorio de red de la localidad de Latacunga en la cual tiene que ver con la realización la implementación de Session Border Controller y Encriptamiento de paquetes que ayude a la seguridad y mejorar la calidad de las llamadas.

Finalmente en la investigación se obtendrán las conclusiones y recomendaciones las mismas que fueron tomadas en base a la investigación realizada.

CAPÍTULO I

1. SISTEMA DE CONTROL DE SEGURIDA EN LA VOIP.

1.1. Antecedentes

El primer operador de telefonía tradicional que comercializo la VoIP fue telecom Finland en 1996. Los hizo utilizando el software de Volcaltec para establecer comunicación de PC a PC. En 1997. Deutsche Telecom saco un servicio, al que llamo t-NetCall, que permitía realizar llamadas telefónicas de teléfono a teléfono, utilizando Internet. En 1998, fabricantes de equipos, como Cisco o Lucent, decidieron desarrollar dispositivos (routers) especialmente para manejar la voz. También se construyeron los primeros Gateway que permitían hacer llamadas de Pc a teléfono y viceversa. Ese año aparecieron algunas compañías en Estados Unidos que permitían a sus usuarios realizar, con sus propios aparatos telefónicos, llamadas telefonía gratuita de larga distancias a cambio de escuchar unos breves anuncios publicitarios al comienzo y finalización de la llamada. Microsoft saco en agosto de 1996 su conocido software Netmeeting, el cual permitía establecer comunicaciones de voz de tipo de PC a PC. Muchos usuarios obtuvieron sus primeras experiencias de VoIP con este programa.

En el año 2001 este software evoluciono hacia Messenger. En Enero de 2001, Vonage empezó a ofrecer servicios VoIP para empresas. Desde entonces los servicio

de VoIP han sido creciendo en el entorno empresarial. Muchas empresas utilizan VoIP en sus centros de atención al cliente. En Agosto de 2003 sacaron al mercado la primera versión del programa Skype. Este programa permite establecer llamadas telefónicas gratuitas entre ordenadores y a coste local entre ordenador y teléfono fijo tradicional. Recientemente han sacado también una versión para video conferencias. El hecho que en el 2005 la empresa eBay compro Skype por 2.100 millones de euros. Skype es el software de VoIP más extendido del mundo en la actualidad.

1.2. Sistema de Seguridad

Los riesgos que con llevan a usar sistema VoIP no son muy diferentes de los que se pueden encontrar en las redes habituales de IP. Lo primero que se debería tener en mente a la hora de usar voz sobre IP es la encriptación, aunque lógicamente no es sencillo capturar y decodificar los paquetes de datos de voz, encriptar es la única forma de prevenir un ataque.

Lo próximo, como debería esperarse, podría ser el proceso de asegurar todos los elementos que componen la red VoIP: servidores de llamadas, routers, switches, Session Border Controller. Se necesita configurar cada uno de esos dispositivos para asegurar que estén en línea con los que se demanda en términos de seguridad.

1.2.1. Seguridad VoIP

Para (MAYR, Randolf, 2015) en su página web VoIP y Seguridad menciona qué:

> La seguridad es fundamental en cualquier entorno pero se vuelve imprescindible cuando lo que está en juego es pasar el servicio de

> telefonía de la red de comunicaciones con mayores niveles de disponibilidad y mayor despliegue del mundo.

Según (RAMÍREZ ARGÜRO, José, 2010) en su página web Seguridad en la VoIP, menciona qué:

> Es la protección perimetral (IPS, firewalls, análisis avanzado de protocolos), la cual debe actualizarse para incorporar un nivel de seguridad proactivo adecuado frente a estas amenazas en los servicios de VoIP

De acuerdo a lo detallado se puede decir que: La seguridad VoIP la seguridad VoIP aparece por la preocupación por la seguridad de las comunicaciones que afecta al mundo de las redes de datos. Se puede apreciar algunos ataques que tendrán como objetivo el robo de información confidencial y algunos otros degradar la calidad del servicio.

1.2.2. Como Brindar seguridad en VoIP

Para (ORTEGA ACEVES, Juan Israel, 2007) en su página web Seguridad en la VoIP (VoIP sobre IP), menciona qué:

> Separar la voz y datos en diferentes redes lógicas formando VLAN (Virtual Local Área Network) y segmentar la red. De esta manera se segmenta la red y se dedican algunas partes de direcciones IP con reglas propias para voz y otras para datos.

En base a lo difundido se puede explicar que: De esta manera, no se puede escuchar lo que sucede en la segmento de voz, también se establecen reglas que imposibilitan

que algún intruso a la red de voz pueda poner un sniffer, como lo es la autenticación de MAC o pórticos de seguridad, la cual si no se obtiene con un login y password no se puede entrar a la red, colocando al intruso incomunicado, con lo que se acaban los inconvenientes en esta parte.

1.2.3. Técnicas de ataque en la Red

Con el paso del año se ha ido desarrollando nuevos ataques cada vez más sofisticados para explotar vulnerabilidades tanto en el diseño de la red TCP/IP como en la configuración y operación de los sistemas informáticos que conforman las redes conectadas a internet. Estos nuevos métodos de ataques se han ido automatizando, por lo que en muchos casos solo se necesita un conocimiento técnico muy básico para realizarlos. Cualquier usuario con una conexión a internet tiene acceso en día a numerosas aplicaciones para realizar estos ataques y las instrucciones necesarias para ejecutarlos.

1.2.3.1. Denegación de Servicio (DoS)

Según (ORTEGA, Gabriel,ALZORRIZ, Ignacio,RUIZ,Elio y CASTRO,Manuel , 2014) en su libro titulado: Procesos y herramientas para la seguridad de redes menciona qué:

> Las principales amenazas a las que están expuestas las redes que utilizan VoIP: Denegación de Servicio (DoS) - Al igual que sucede en las redes de datos, existen ataques de denegación de servicio en las redes VoIP. Pág. 41

De acuerdo a lo dicho se puede decir que: Son intentos de negación de servicios malintencionados degradan seriamente el rendimiento de la red

llegando al punto de implementar la utilización de la comunicación VoIP. Se basa en él envió de paquetes especialmente construidos para explotar algunas vulnerabilidades como saturación de los flujos de datos y de la red o sobre carga de procesos en los dispositivos.

1.2.3.2. Spam sobre Telefonía en Internet (SPIT)

Según (TEGNOLOGÍA, KANVERNA, 2015) en su página web Amenazas para la seguridad VoIP, menciona qué:

> Spam sobre Telefonía en Internet (SPIT) - El spam ha dejado de ser exclusivo de los buzones de correo electrónico y comienza a propagarse de forma similar hacia los usuarios de VoIP mediante botnets.

Luego de haber definido se puede decir que: El spam ataca exclusivamente al buzón de correo electrónico, esto comienza a propagarse de forma similar hacia todos los usuarios de la red al igual que el correo basura estos puede hacer que se haga más lento el rendimiento del sistema.

1.2.3.3. Robo del Servicio de Voz

Según (ORTEGA, Gabriel,ALZORRIZ, Ignacio,RUIZ,Elio y CASTRO,Manuel , 2014) en su libro titulado: Procesos y herramientas para la seguridad de redes menciona qué:

> El robo del servicio de VoIP puede ocurrir cuando un usuario no autorizado accede a una red de VoIP, por lo general, mediante un nombre de usuario y contraseña válidas, o bien obteniendo un acceso físico a un dispositivo VoIP y realizando llamadas salientes. Pág. 41

Considerando lo definido se puede decir que: Los robos de servicios son más comunes en el sistema VoIP los hacker se benefician de esto aprovechando para llamar ilegalmente a todas partes del mundo y se aprovechan de los patrocinios que obtiene la VoIP.

1.2.3.4. Secuestro de Registro

Según (TEGNOLOGÍA, KANVERNA, 2015) en su página web Amenazas para la seguridad VoIP, menciona qué:

> Secuestro de Registro - Un secuestro de registro SIP sucede cuando un hacker desactiva un registro SIP válido de un usuario y lo sustituye por una dirección IP pirata. Esto permite al hacker interceptar y redirigir las llamadas entrantes, reproducirlas o finalizarlas en función de sus intereses.

De acuerdo a lo dicho se puede decir que: El Secuestro de registros esto hace que un hacker pueda desactivar el registro SIP de un usuario registrado y lo sustituya por una dirección IP pirata. La cual aprueba obstruir y reorganizar las llamadas solicitadas y podrá controlar las funciones del sistema VoIP a su conveniencia como puede ser la desactivación de servicios.

1.2.3.5. Oyentes no autorizados

Según (NADREU,fernando,PELLAGERO, Izaskun y LESTA, Amaia, 2006; ORTEGA, Gabriel,ALZORRIZ, Ignacio,RUIZ,Elio y CASTRO,Manuel , 2014) en su libro titulado: Fundamentos y aplicaciones de seguridad menciona qué:

> Oyentes no autorizados - Al igual que los paquetes de datos, los paquetes de voz son objeto de ataques a través de un intermediario cuando un hacker falsifica la dirección MAC de dos partes, obligando a los paquetes de VoIP a circular a través del sistema del hacker. Pág. 80

Luego de haber de definido se puede decir que: El Secuestro de registros esto hace que un hacker pueda desactivar el registro SIP de un usuario registrado y lo sustituya por una dirección IP pirata. La cual puede obstruir y reorganizar las llamadas solicitadas y podrá controlar las funciones del sistema VoIP a su conveniencia.

1.2.3.6. Directory Harvesting o Recogida de Direccione

Según (TEGNOLOGÍA, KANVERNA, 2015) en su página web Amenazas para la seguridad VoIP, menciona qué:

> Directory Harvesting o Recogida de Direcciones (DHA) – Esta amenaza se produce cuando los atacantes tratan de encontrar direcciones válidas de VoIP mediante el uso de la fuerza en una red y el pirata informático puede identificar las direcciones válidas de VoIP.

Luego de haber definido se puede decir que: Esta amenaza se produce cuando un hacker trata de encontrar direcciones validas de VoIP mediante el uso de la fuerza de la red.

1.2.3.7. Vishing (Phishing sobre VoIP)

Según (ORTEGA, Gabriel,ALZORRIZ, Ignacio,RUIZ,Elio y CASTRO,Manuel , 2014) en su libro titulado: Procesos y herramientas para la seguridad de redes menciona qué:

> Vishing (Phishing sobre VoIP) El Vishing imita las formas tradicionales de phishing (modalidad de estafa cuyo objetivo es intentar obtener de un usuario información personal y sensible como nombres de usuario, cuentas bancarias como son las contraseñas o números de tarjeta de crédito, entre otros). Pág. 31

En base a lo definido se puede decir que: Es intentar obtener información única y sensitiva como nombres de clientes, cuentas bancarias etc. Esto se realiza atreves de correo basura o suplantación de imagen de una empresa o entidades públicas. El usuario puede caer en esta trampa y aportar los datos correctos que le piden y los delincuentes tienen la libertad de vender esta información a personas maliciosas.

1.3. Comunicaciones mediante Voz IP

Al definir el Sistema VoIP se pueden encontrar varias opciones; unos consideran que es un método por el cual toma la señal de audio analógico otros alegan que es un conjunto de recursos que pueden ser trasmitidos a través del internet.

1.3.1. Sistema VoIP

Para (CARMONA SUARES, Edgar Javier y RODRIGUEZ SALINAS, Elisabeth, 2009) en su libro titulado: Tecnología de la información ambientes web para la calidad educativa menciona qué:

> VOIP o voz vía Internet Protocolo, es un sistema que basa su funcionamiento en la posibilidad que la señal de voz viaje a través de internet, empleando un protocolo IP Pág. 30.

Según (MORO Vallina, 2013) en su libro titulado: Infraestructuras de redes de datos u sistemas de telefonía menciona qué:

> Voz sobre IP es una forma de transmitir llamadas de voz a través de una red TCP/IP, con ello se proporcionan servicios de telefonía sobre red única, en la que constituye la voz y los datos. Pág. 120

Luego de haber definido se puede decir que: La transferencia de datos se realizara en grandes cantidades y a velocidades enormes. Las conversaciones se guardaran en "pedacitos" (paquetes) que se pueden llevar fácilmente, y puesto que el costo de la mayoría de las conexiones de internet se basa en consideraciones del ancho de banda, VOIP lleva muchos paquetes para reducir costos. Si una llamada va a un número de teléfono en otra red o en otro país, el VOIP hace que la conferencia recorra la mayor distancia hasta un centro de Internet lo más cerca posible la localización física de las personas que usted este llamando, y entonces la telefonía convencional (cable o radio) se utilizara para hacer el trayecto final de la llamada.

1.3.2. Digitalización y Transmisión

Para (CABALLAR, José Antonio, 2013) en su libro titulado: VoIP telefonía de internet menciona qué:

> La telefónica IP es convertir la señal analógica que produce la voz en digital, de forma que pueda ser tratada por internet, A este proceso se le conoce como digitalización de la voz. Pág. 5.

Según (SERRANO SANTOYO, Arturo, CABRERA FLORES, Mayer, MARTINEZ, Evelio y GARIBAY RUIZ, Julio, 2010) en su libro titulado: Digitalización y convergencia Global menciona qué:

> La digitalización, desde el punto de vista técnico, es el proceso de convertir señales analógicas en señales digitales, con el propósito de facilitar su procedimiento (codificación, compresión etc.) Y hacer la señal resultante (la digital) más inmune al ruido y a otras interferencias. Pág. 64

Se pudo determinar que: Esto consiste en tomar una muestra de la voz, cuantificarla y convertir este valor en números binarios representando por (0) y (1). El internet es una red que fue pensada para trasmitir datos que no necesitaban llegar al destino de una forma ordenada y en tiempo real. En caso de la voz es distinto, las muestras de voz se codifican y decodifican de forma continua y en tiempo real. La trasmisión digital sobre la analogía es que la primera permite mejor calidad en la comunicación.

1.3.3. Elementos necesarios

Según (CABALLAR, Jose Antonio, 2013) en su libro titulado: VoIP telefonía de internet menciona qué:

> Ordenador.- es necesario contar con el software que realiza la digilitización y codificación, para mejorar la comodidad en la comunicación existente.
>
> Telefonía IP.- Estos equipos tienen una apariencia similar a la de un teléfono tradicional, pero incorporó elementos necesarios para convertir la voz en información IP y viceversa. Pág. 6

Luego de haber dicho se puede decir que: que estos elementos son muy importantes para el sistema VoIP donde se logrará la comunicación entre dos teléfonos IP mediante el internet.

1.3.4. Protocolos utilizados en el sistema VoIP

Son los lenguajes que utilizarán los distintos dispositivos VoIP para su conexión. Esta parte es importante ya que dependería la eficacia y complejidad de la comunicación. Existen varios protocolos comúnmente usados para VoIP, estos protocolos definen la manera en que se conectan entre si y así otras redes usando VoIP.

1.3.4.1. Protocolos de Señalización

Para (HUIDOBRO MOYA, José Manuel y ROLDAN MARTINEZ, David, 2006) en su libro titulado: Tecnología VoIP y telefonía IP menciona qué:

> Es establecer un canal de comunicaciones a través del cual fluya la información del usuario y liberar el canal cuando finalice la comunicación. Pág. 143

Se puede determinar que: Los protocolos de señalización entre terminales son comunes a cualquier tipo de comunicaciones multimedia (Voz, Audio y Video) a través de las redes de paquetes. Aplicadas a la voz sobre paquetes, tienen como objetivo mantener la interfaz con el usuario típica de las redes telefónicas, es decir, generar los tonos y señales necesarios para que los usuarios no perciban que la tecnología de soporte de las llamadas telefónicas ha cambiado.

1.3.4.2. Protocolo H.323

Según (CABALLAR, Jose Antonio, 2013) en su libro titulado: VoIP telefonía de internet menciona qué:

> Es, en realidad, un conjunto de protocolos que definen los componentes y los medios de interacción de los mismo que deben cumplirse para soportar comunicaciones multimedia sobre redes de paquetes sin conexión ni garantía de calidad de servicio, como es el caso de las redes IP. Pág. 104

Luego de haber dicho se puede decir que: Luego de haber detallado se puede decir que: es un conjunto de estándares los cuales definen un conjunto de protocolos para proveer comunicación visual y de audio sobre una red de computadores en el sistema VoIP.

1.3.4.3. Protocolo SIP (SESSION INITATION PROTOCOL)

Para (HUIDOBRO MOYA, José Manuel y ROLDAN MARTINEZ, David, 2006) en su libro titulado: Tecnología VoIP y telefonía IP menciona qué:

> Se trata de un protocolo de control de la carga de aplicación que define como establecer, modificar o finalizar una sesión entre dos o más extremos, independientemente del tipo de sesión de que se trate. Pág. 144

De acuerdo a lo dicho: Es un protocolo de señalización utilizado para crear, modificar y terminar sesiones con uno o más participantes de una red IP. Una sesión puede ser una simple llamada telefónica de doble vía o puede ser una sesión de conferencia multimedia con muchas personas participando.

1.3.4.4. Protocol TRIP (TELEPHONY ROUTING OVER IP)

Según (HUIDOBRO MOYA, José Manuel y ROLDAN MARTINEZ, David, 2006) en su libro titulado: Tecnología VoIP y telefonía IP menciona qué:

> Se define como un sistema de políticas interadministrativas para la notificación de la alcanzabilidad de los destinos de las comunicaciones entre servidores de localización así como la información que debe acompañar a dichas notificaciones. Este protocolo es diseñado para el intercambio de información entre proveedores de servicios.
> Pág. 145

De acuerdo a lo considerado se puede decir que: Es una política interadministrativa para la publicidad de la accesibilidad de los destinos de telefonía entre servidores de localización y por atributos de publicidad de las rutas hacia esos destinos. TRIP puede servir como el protocolo de enrutamiento de telefonía para cualquier protocolo de señalización. También se utiliza para distribuir información de enrutamiento de telefonía entre dominios administrativos de telefonía.

1.3.4.5. Protocolos de Trasporte

Para (HUIDOBRO MOYA, José Manuel y ROLDAN MARTINEZ, David, 2006) en su libro titulado: Tecnología VoIP y telefonía IP menciona qué:

> Son las normas que definen como debe realizase la comunicación entre los extremos por un canal de comunicaciones previamente establecidos.
> Pág. 146

Considerando lo definido se puede decir que: El trasporte de información entre el origen y el o los destinos. Este transporte no solo influye el trasladar los paquetes de información de un lado a otro sino que, además, habrá que fragmentar y reensamblar los paquetes y proveer los mecanismos necesario para reducir el impacto de las pérdidas de señal suele considerarse como una señal de ruido no deseada, el retardo.

Los protocolos de transporte son los responsables de asegurar un envío confiable de los datos entre las computadoras.

1.3.4.6. Protocolo RTP (Real Time Protocol)

Según (CABALLAR, Jose Antonio, 2013) en su libro titulado: VoIP telefonía de internet menciona qué:

> Es el estándar que define las comunicaciones de audio y video en tiempo real sobre redes IP, asumiendo, por lo tanto, la existencia de pérdidas y retardos y la posibilidad de variaciones dinámicas de las características de la red en el trascurso de la comunicación. Pág. 147

Luego de haber definido: Es un estándar para la transmisión confiable de voz y video a través de Internet, suministra funciones de trasporte extremo a extremo y ofrece servicios tales como identificación del tipo de carga numérica de secuencia.

1.3.4.7. Protocolo RTSP (Real Time Streaming Protocol)

Según (HUIDOBRO MOYA, José Manuel y ROLDAN MARTINEZ, David, 2006) en su libro titulado: Tecnología VoIP y telefonía IP menciona qué:

> Es un protocolo de niveles de aplicación que define como debe llevarse a cabo el streaming, Pág. 148

Se puede determinar lo definido que: Es la capacidad de distribución de contenido multimedia de manera que es posible visualizarlos mientras están siendo trasmitidos (es decir, sin necesidad de descargarlos completamente), es decir, el que establece y controla uno o muchos flujos sincronizados de datos, ya sean de audio o de video.

1.3.4.8. Protocolo RTCP (Real Time Protocol)

Según (CABALLAR, Jose Antonio, 2013) en su libro titulado: VoIP telefonía de internet menciona qué:

> Se describe el intercambio de mensajes de controles relacionados, fundamentales, con la calidad de servicios (retardo, tasa de pérdidas etc.). Pág. 149

De acuerdo a lo considerado: Su utilización es recomendable porque promociona información de estado de las comunicación con el fin de detectar, por ejemplo situaciones en las que la calidad de la transmisión no es suficiente aunque no provee de los mecanismos necesarios para mejorar las prestaciones de la red (reservar de ancho de banda, control de la congestión, etc.).

1.3.4.9. Protocolos de Seguridad

Según (HUIDOBRO MOYA, José Manuel y ROLDAN MARTINEZ, David, 2006) en su libro titulado: Tecnología VoIP y telefonía IP menciona qué:

> Los teléfonos y servidores son blancos de ataques. Aunque sean de menor tamaño o parezcan elementos simples, están construidos en base a ordenadores con software. Pág. 156

Según (HUIDOBRO MOYA, José Manuel y ROLDAN MARTINEZ, David, 2006) en su libro titulado: Tecnología VoIP y telefonía IP menciona qué:

> La encriptación es la única manera de prevención frente a un ataque y evitar que si nuestra conversación es capturada, sea inteligible y no tenga

> ningún valor para el atacante aunque, desafortunadamente, consume ancho de banda. Pág. 156

Luego de haber definido: La mejor seguridad es encriptando los paquetes de datos para que no haya ninguna manipulación de personas ajenas para que la información viaje a su destino sin preocupación que sean interceptadas por personas extrañas a la información que viaja en la red cuando estén utilizando el sistema VoIP.

1.3.4.10. Protocolos de Gestión

Según (HUIDOBRO MOYA, José Manuel y ROLDAN MARTINEZ, David, 2006) en su libro titulado: Tecnología VoIP y telefonía IP menciona qué:

> A medida que aumenta la complejidad y el número de las soluciones de VoIP implantadas, se hace más patente la necesidad de herramientas de gestión que, por un lado, permitan medir las prestaciones que ofrece la red en tiempo real y, por otro, proporcione información útil en situación de fallo. Pág. 171

Luego de haber dicho: que se debe buscar soluciones para el mejoramiento del sistema VoIP que permita o proporcione información útil en situación e fallos o de otra índole, esto es lo que pretende evitar el protocolo de gestión..

1.4. Session Border Controller (Sbc)

Es un concepto de seguridad que desde hace unos años se ha venido escuchando con más fuerza, sobre todo lo duro y a veces casi invisible, el poder trabajar con firewall perimetrales a la vez brindar seguridad completa a una plataforma de VoIP.

Por tanto la posibilidad, de tener un elemento o entidad única de seguridad especializada en VoIP y que de cara a internet, para garantizar en gran medida, protección de ataques externos, es muy importante la consideración.

Concepto

Según (JON Hardwick, 2005) en su libro titulado: Session border controller-Enabling the VoIP Revolution menciona qué:

> Session Border Controller (SBC) se han convertido en un elemento importante de Voz moderna sobre IP (VoIP) redes, como los proveedores de servicios buscan proteger la integridad de sus redes y modelos de negocio al tiempo que ofrece diversos servicios a sus clientes. Pág. 3

Luego de haber definido se puede decir que: SBC busca la protección de la integridad de sus redes y modelos de negocio al tiempo que ofrece diversos servicios a sus clientes. Puede realizar una serie de funciones de control de llamadas a aliviar la carga de los agentes de llamadas dentro de la red y también controlar en ancho de banda preciso de la red y puede rechazar nuevas llamadas para no perder la calidad de aquellas que están en curso.

1.4.1. Función de un SBC

Para (GIL Marcel, 2015) en su página web: El ABC del SBC: definición, Características y ventajas Menciona qué:

> Su función es garantizar que las sesiones que se establecen son lícitas, detectando y bloqueando posibles ataques e intrusiones. Otra función de seguridad importante (de forma similar a lo que hace un firewall para los

servicios de datos) es la ocultación de los servicios de voz de la red interna hacia el exterior.

Tomando en cuenta lo dicho se puede deducir que: Su ejecución es descubrir y bloquear posibles ataques de intrusos en el sistema VoIP. Otro complemento que tiene el SBC es la ocultación de los servicios de voz de la red interna hacia el exterior. También el SBC no se limita a monitorizar y examinar las sesiones entre la red interna y la externa, sino que las reconstruye para obtener un control total.

1.4.2. Estructura interna de un SBC

Para (HARDWICK, Jon, 2005) su libro titulado: Session border controllers-Enabling the VoIP Revolution menciona qué:

> La función de señalización SBC (SBC-SIG) controla el acceso de los mensajes de señalización de VoIP para el núcleo de la red, y manipula el contenido de estos mensajes. Para ello, al actuar como un agente de usuario Back-to-Back (B2BUA). Pág. 14

De acuerdo a lo considerado se puede decir que: Que controla la señalización de los mensajes y manipula el contenido de estos mensajes con un usuario Back-to-Back.

Según (HARDWICK, Jon, 2005) su libro titulado: Session border controllers-Enabling the VoIP Revolution menciona qué:

> La función SBC Media (SBC-MEDIA) controla el acceso de paquetes de medios a la red, ofrece servicios diferenciados y de calidad de servicio para los diferentes flujos de medios, y evita el robo de servicio. Para ello, al actuar como un proxy RTP. Pág. 15

Considerando lo determinado se puede decir que: La función SBC Media (SBC-MEDIA) controla el acceso de paquetes de medios a la red, ofrece servicios diferenciados y de calidad de servicio para los diferentes flujos de medios, y evita el robo de servicio.

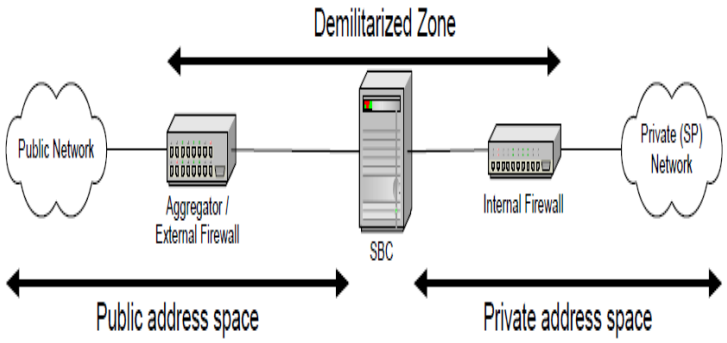
Algunos dispositivos SBC ofrecen ambas funciones en una sola caja (denominados en lo sucesivo SBC-box individual). Otros toman un enfoque distribuido, y separada SBC-SIG y SBC-MEDIA en máquinas separadas (en adelante, SBC de doble caja), a través de protocolos de control de llamada, como H.248 y COPS-PR para vincular los dos.

1.4.3. La Zona Desmilitarizada

Para (HARDWICK, Jon, 2005) su libro titulado: Session border controllers-Enabling the VoIP Revolution menciona qué:

> La zona desmilitarizada (DMZ) es el término conceptual para una pequeña subred (o dispositivo individual) que se encuentra entre una red privada de confianza. Pág. 20

FIGURA Nº 1: La Zona Desmilitarizada



Fuente: HARDWWICK Jon

Luego de haber dicho se puede decir que: Es el término conceptual para una pequeña subred (o dispositivo individual) que se encuentra entre una red privada de confianza. El propósito de la DMZ es evitar que el tráfico hostil o no deseados entren en (o, en algunos casos, dejando) la red privada.

1.4.4. Escenarios de red aplicables para SBC

Según (HARDWICK, Jon, 2005) su libro titulado: Session border controllers-Enabling the VoIP Revolution menciona qué:

> SBC se pueden implementar en cinco escenarios de red principales. En el primero de tres de ellos, el SBC es parte de la DMZ, mientras que en los dos últimos escenarios, es en el núcleo de una red.
>
> En el núcleo de una red como un medio para superar los problemas de topología interna, usan un transcodificador codec centralizado. Pág. 25

Para (HARDWICK, Jon, 2005) su libro titulado: Session border controllers-Enabling the VoIP Revolution menciona qué:

> Permitir la señalización de VoIP y multimedia para atravesar cortafuego básico del cliente, Firewall y NAT transversal. Pág. 37

Luego de haber definido se puede decir que: SBC está desplegado en el borde de las redes de proveedores de servicios, sino que también se puede utilizar en el borde de las redes empresariales. El Session Border Controller desplegado en su borde, y otros tienen un servidor de seguridad más básica para permitir la señalización de VoIP y multimedia para atravesar cortafuegos básicos del cliente, Firewall y NAT transversal, para más detalles sobre esto.

1.4.5. SBC control de recursos de red utilizados por el tráfico de VoIP

Según (HARDWICK, Jon, 2005) su libro titulado: Session border controllers-Enabling the VoIP Revolution menciona qué:

> En esta red, los SBC realizan CAC para prevenir el enlace bajo ancho de banda se conviertan en un exceso de solicitudes con el tráfico de voz. Pág. 38

Considerando lo realizado se puede decir que: que estos recursos están dispuestos a ser utilizados cuando haya un bajón de ancho de banda en el sistema VoIP para mejorar la calidad e la señal.

1.5. Encriptación de paquetes

La encriptación de paquetes algunos autores le definen como el proceso en que uno o varios archivos o datos, son protegidos mediante el uso de un algoritmo que desordena sus componentes, haciendo imposible que sean abiertos o decodificados si es que no se tiene el respectivo permiso para obtener la información.

1.5.1. Concepto

Para (GRETEL, Abdales, 2007) en su página web Encriptación de paquetes, menciona qué:

> Es el proceso mediante el cual cierta información o texto sin formato es cifrado de forma que el resultado sea ilegible a menos que se conozcan los datos necesarios para su interpretación.

Según (GARRE DEL OLMO, Carlos, SANCHEZ CAMPOS, Alberto y MARTÍN DE DIEGO, Isaac, 2012) en su libro titulado: Principios de la seguridad informática para usuarios menciona qué:

> Encriptar es la acción de proteger la información mediante su modificación utilizando una clave. En informática también se usa los términos codificar y descodificar. Pág. 134

De acuerdo a lo definido podemos decir que: Es una medida de seguridad utilizada para que al momento de almacenar o transmitir información sensible ésta no pueda ser obtenida con facilidad por terceros. En lo cual los datos a proteger son traducidos a algo que parece aleatorio que no tiene ningún significado y no puedan ser mal utilizados.

1.5.2. Uso de Encriptación

Para (GRETEL, Abdales, 2007) en su página web Encriptación de paquetes, menciona qué:

> Algunos de los usos más comunes de la encriptación son el almacenamiento y transmisión de información sensible como contraseñas, números de identificación legal, números de tarjetas de crédito, reportes administrativo-contables y conversaciones privadas, entre otros.

Luego de haber realizado se puede decir que: El uso de la encriptación es más dirigida al almacenamiento de paquetes y la transición de información como contraseñas, números de identificación legal, números de tarjetas de crédito, etc. Esto nos permite que la información viaje segura manteniendo su autenticidad.

CAPITULO II

ENTORNO DEL LUGAR DE INVESTIGACIÓN

2.1. Carrera de Ingeniería en Informática y Sistemas Computacionales.

La Carrera de Ingeniería en Informática y Sistemas Computacionales de la Universidad Técnica de Cotopaxi, fue creada en el año de 1997 como respuesta a las demandas del mercado. Su pensum y programas de estudio se han venido actualizando periódicamente para mantenerlo al ritmo de los cambios de la disciplina y de la tecnología que se usa en la profesión. El principio fundamental en el que se basa el pensum vigente es el concepto de aprendizaje en espiral, es decir en forma sucesiva se realiza pasadas a los contenidos de la profesión con un nivel de profundidad y detalle incremental. La UTC propone la Carrera de Ingeniería en Informática y Sistemas Computacionales para preparar profesionales capaces de cumplir las demandas de los usuarios informáticos en las organizaciones, con calidad, técnica, personal, moral y con profundo sentido social, para no solo ocupar puestos de trabajo sino ser capaces de generarlos en mira al desarrollo social del país. Así mismo complementa la gama de carrera y especialidades que ofrece con esta de gran impacto social y económico en el momento actual, además de ser capaz de autoabastecerse en la demanda de cursos en el área informática para otras carreras y soluciones informáticas que las dependencias de la institución requieran,

2.2. Filosofía Institucional

2.2.1. Misión

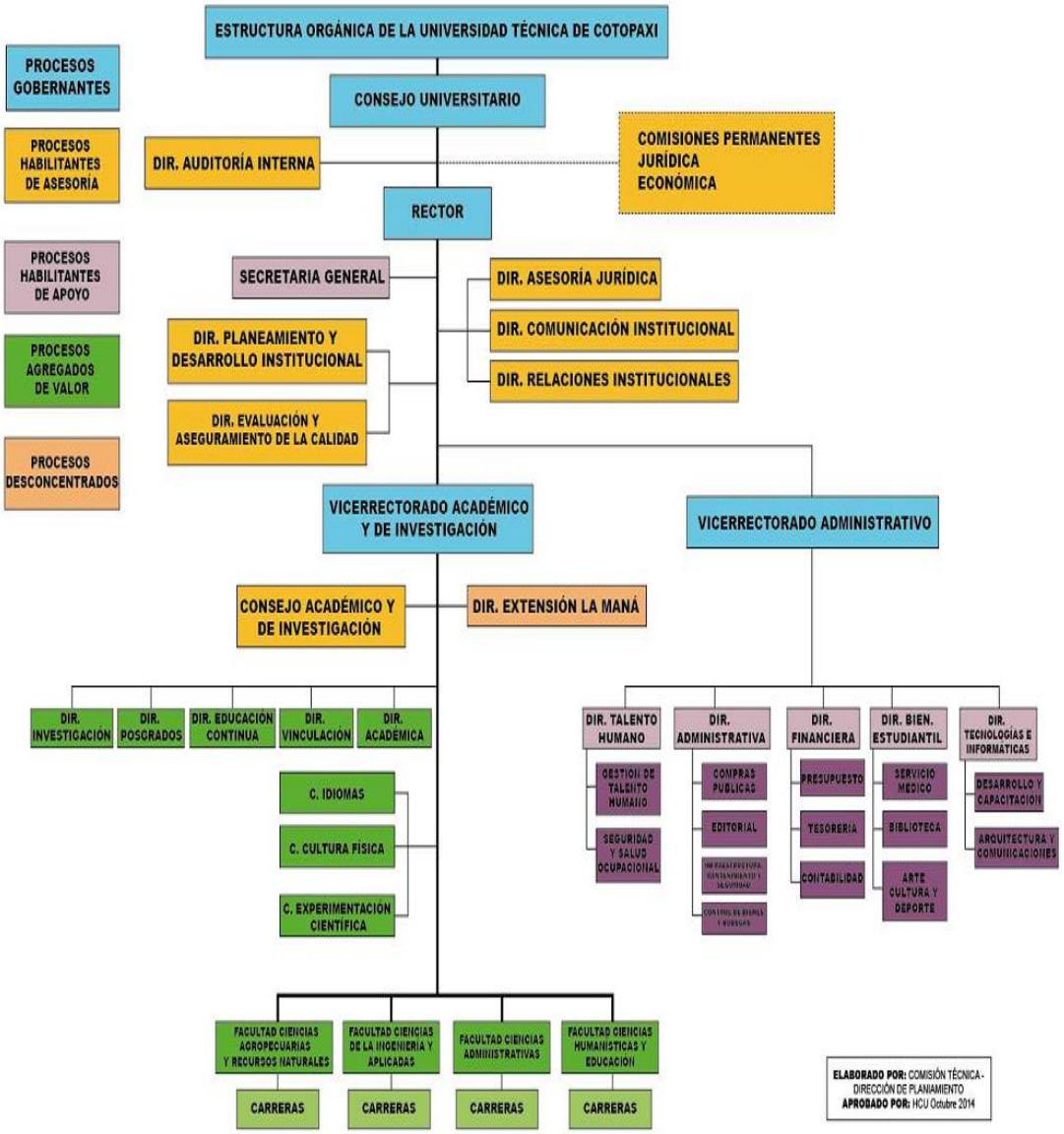
La Carrera de Ingeniería en Informática y Sistemas Computacionales, forma profesionales con sólidos conocimientos en las ciencias de la computación, la ingeniería de software y redes de información, por medio de la síntesis de los saberes humanísticos tecnológicos y científicos, que contribuyan a aplicar la tecnología de la información y comunicación, como parte del desarrollo social y económico de la provincia y del país.

2.2.2. Visión

En el año 2015 la Carrera de Ingeniería en Informática y Sistemas Computacionales lidera los procesos de formación profesional en el desarrollo de tecnologías de última generación, que le permite alcanzar un sólido reconocimiento social.

2.3. Estructura Orgánica de la Universidad Técnica de Cotopaxi

FIGURA Nº 2: Estructura Orgánica de la Universidad Técnica de Cotopaxi



Fuente: Pagina de la universidad www.utc.edu.ec

2.4. Diseño Metodológico

2.4.1. Métodos de Investigación

2.4.1.1. Método Hipotético-Deductivo

Este método ha servido para obtener una gran cantidad de información en forma teórica de la seguridad en el sistema VoIP, Se puede instalar Centos y SBC como hardware, aplicación o máquina virtual y dispone de funcionalidades que harán que su red de telefonía IP sea mucho más segura y se integre mejor con el equipamiento SIP de diferentes fabricantes y proveedores de servicios. Básicamente el Session Border Controller gestiona tanto la media como la señalización de las llamadas VoIP.

2.4.1.2. *Método Inductivo*

El método inductivo es muy importante, ya que provee una aproximación a los hechos reales dentro de nuestro Proyecto de investigación, y ayudo a reunir toda la información sobre Seguridad de los equipos que se protegerán, mediante una de capa de seguridad de los puntos de entrada al sistema de voz IP desde las redes no seguras, evitando el hacking y los fraudes telefónicos. Session Border Controller oculta al exterior la topología de red interna, actuando como un firewall pero con características más adecuadas para el tráfico multimedia.

2.4.1.3. *Método analítico*

El Session Border Controller es usado cada vez más en las redes VoIP para transportar VoIP de forma segura hace que se incremente las seguridades de la comunicaciones para que no puedan ser interceptadas de forma ilícita. Este protege la señalización y los canales de voz respectivamente.

2.5. Tipos de Investigación

2.5.1. Investigación Bibliográfica

La aplicación de este tipo de investigación facilito profundizar los conocimientos adquiridos en el análisis de nuestro tema de investigación. Además nos sirve como base para fundamentar los datos expuestos y para otorgarles confiabilidad y seriedad.

2.5.2. Investigación de Campo

Este tipo de datos permitió la recolección de Información de los estudiantes de la Universidad Técnica de Cotopaxi de los niveles superiores de la Carrera de Ingeniería en Informática y Sistemas Computacionales, para la implementación del presente proyecto, en este caso apoyo con la información del laboratorio de red.

2.5.3. Investigación Experimental

La investigación experimental es aplicada en el laboratorio de redes para la obtención de resultados y el correcto funcionamiento del Session Border Controller para alcanzar los objetivos del experimento, responder a las preguntas de investigación y someter a verificación la hipótesis.

2.6. Instrumentos de la Investigación

Los instrumentos de recolección de datos e información en su recurso metodológico que se materializó mediante un dispositivo o formato (impreso o digital) que se utiliza para poder obtener, registrar o almacenar con los aspectos relevantes del estudio o investigación recabada de las fuentes indagadas.

2.6.1. La encuesta

La encuesta, en nuestro proyecto es un instrumento útil puesto que obtuvimos información básica y necesaria para darnos cuenta de las necesidades y acoplarlo a nuestro proyecto.

2.7. Tratamiento y Análisis Estadístico de los Datos

Para la interpretación de los resultados se utilizará la estadística descriptiva.

2.7.1. Estadística descriptiva

En lo mencionado anteriormente se puede decir que la estadística descriptiva nos arrojó datos reales qué califiquen el proyecto de investigación, con la ayuda de los instrumento de investigación como la encuesta.

2.7.2. Cálculo de la Población y Muestra

A continuación las personas que se tomaran en cuenta o que se encuentran involucrados a esta investigación.

TABLA N° 1: Involucrados

Involucrados	**Cantidad**
Administradores de los Laboratorio de red	4
Estudiantes	105
TOTAL:	109

Fuente: UTC.

Elaborado por: Chicaiza Gabriel, Escobar Javier

Cálculo de la Muestra.

El cálculo de la muestra se lo realiza para obtener un número estimado de individuos involucrados directamente en el desarrollo del proyecto, por lo cual procedemos a calcular:

Para calcular el tamaño de la muestra se utilizó la siguiente fórmula:

Formula:

$$n = \frac{z^2 * pq * N}{NE^2 + Z^2 * pq}$$

n: tamaño de la muestra

Z: Nivel de confianza (1.96)

P: Variable positiva (0.5)

Q: Variable Negativa (0.5)

N: Tamaño de la población

E: Error máximo admisible (0.05)

$$n = \frac{(1.96)^2(0.5)(0.5) * 109}{109(0.05)^2 + (1.96)^2(0.5)(0.5)}$$

n= 28.43/ 1.64

n= 17.3382 n=17

2.8. Análisis e Interpretación de Resultados

Pregunta 1: ¿Piensa usted que es beneficiario el desarrollo de la tecnología de la comunicación?

TABLA N° 2: Desarrollo de la Tecnología

Parámetros	Frecuencia	Porcentaje
Si	99	99%
No	1	1%
TOTAL	100	**100%**

Fuente: Estudiantes de la Carrera: Ingeniería en Informática y Sistemas Computacionales
Elaborado por: Chicaiza Gabriel, Escobar Javier

GRÁFICO Nº 1: Desarrollo De La Tecnología

Fuente: Estudiante de los niveles superiores de la Carrera: Ingeniería en Informática y Sistemas Computacionales
Elaborado por: Chicaiza Gabriel, Escobar Javier

Análisis e Interpretación

La mayoría de los encuestados opino que son indispensable los beneficios que se obtienen al estar comunicado y más aún cuando la tecnología interviene para mejorar la fidelidad de la comunicación y lo más importante es de bajo costo y nos permite una mejor información.

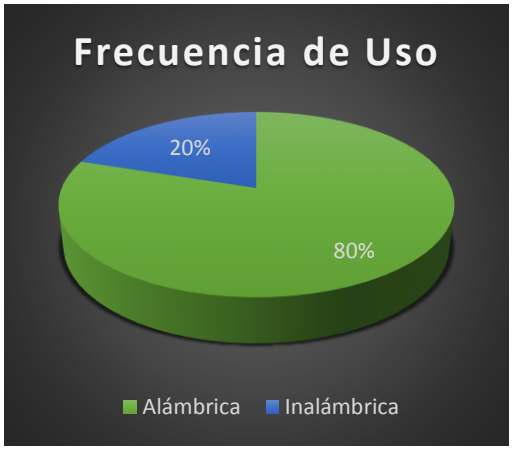
Pregunta 2: ¿Cuál de estos tipos de comunicación has utilizado con frecuencia anterior mente para realizar una llamada de voz?

TABLA N° 3: Tipo de Investigación

Parámetros	Frecuencia	Porcentaje
Red con cable	20	20%
Inalámbrica	80	80%
TOTAL	100	**100%**

Fuente: Estudiante de los niveles superiores de la Carrera: Ingeniería en Informática y Sistemas Computacionales
Elaborado por: Chicaiza Gabriel, Escobar Javier

GRÁFICO Nº 2: Tipo de Investigación



Fuente: Estudiante de los niveles superiores de la Carrera: Ingeniería en Informática y Sistemas Computacionales
Elaborado por: Chicaiza Gabriel, Escobar Javier

Análisis e Interpretación

Todos los encuestados opinan sobre esta tecnología que es una herramienta de productividad fundamental para la creciente fuerza de las llamas telefónicas a través de aplicaciones, video llamadas, video conferencia, aulas virtuales por medio del internet, que vinculan y unen más a las personas.

Pregunta 3: ¿El desarrollo de la tecnología de comunicación te ayudado a solucionar problemas de comunicación?

TABLA N° 4: Problemas de la Comunicación

Parámetros	Frecuencia	Porcentaje
Si	99	99%
No	1	1%
TOTAL	100	**100%**

Fuente: Estudiante de los niveles superiores de la Carrera: Ingeniería en Informática y Sistemas Computacionales
Elaborado por: Chicaiza Gabriel, Escobar Javier

GRÁFICO Nº 3: Problemas de la Comunicación

Fuente: Estudiante de los niveles superiores de la Carrera: Ingeniería en Informática y Sistemas Computacionales
Elaborado por: Chicaiza Gabriel, Escobar Javier

Análisis e Interpretación

Los encuestados opinaron que es muy importante porque esta tecnología reduce costos de llamadas y está disponible en la mayoría de lugares, también puede que al tener varias opciones se pueden tener más oportunidad de realización de la comunicación.

Pregunta 4: ¿Qué software o aplicación utiliza para comunicación mediante voz?

TABLA N° 5: Software o Aplicación

Parámetros	Frecuencia	Porcentaje
Skype	30	30%
whatsapp	35	30%
Viber	20	20%
Line	10	15%
Ninguno	5	5%
TOTAL	100	**100%**

Fuente: Estudiante de los niveles superiores de la Carrera: Ingeniería en Informática y Sistemas Computacionales
Elaborado por: Chicaiza Gabriel, Escobar Javier

GRÁFICO Nº 4: Software o Aplicación

Fuente: Estudiante de los niveles superiores de la Carrera: Ingeniería en Informática y Sistemas Computacionales
Elaborado por: Chicaiza Gabriel, Escobar Javier

Análisis e Interpretación

Se concluye que los encuestados usan distintas aplicaciones móviles y de escritorio para comunicarse, las mismas que tienen libre utilización, limitadas por tiempo de uso, o de funcionalidad de la aplicación.

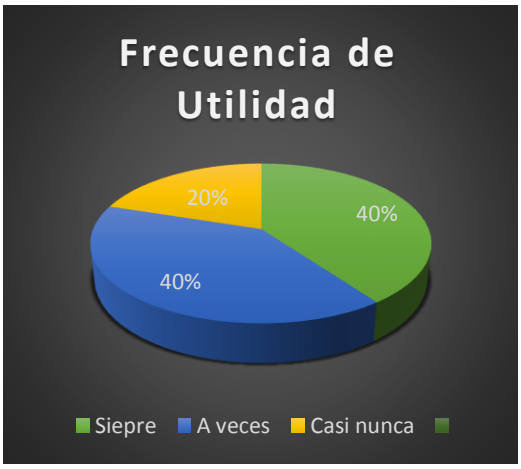
Pregunta 5: ¿Con que frecuente utiliza este tipo de aplicaciones?

TABLA N° 6: Tipo de Aplicaciones

Parámetros	Frecuencia	Porcentaje
Siempre	40	40%
A veces	40	40%
Casi nunca	20	20%
TOTAL	100	**100%**

Fuente: Estudiante de los niveles superiores de la Carrera: Ingeniería en Informática y Sistemas Computacionales
Elaborado por: Chicaiza Gabriel, Escobar Javier

GRÁFICO Nº 5: Tipo de Aplicaciones



Fuente: Estudiante de los niveles superiores de la Carrera: Ingeniería en Informática y Sistemas Computacionales
Elaborado por: Chicaiza Gabriel, Escobar Javier

Análisis e Interpretación

Se concluye que el uso de las aplicaciones depende del ámbito en el que se desempeña el usuario, eso puede influir en el tiempo que de utilización a las aplicaciones.

Pregunta 6: ¿Cuál crees tú que es la calidad de las llamadas por las aplicaciones?

TABLA N° 7: Calidad de Llamadas

Parámetros	Frecuencia	Porcentaje
Excelente	50	50%
Buena	30	30%
Regula	18	18%
Mala	2	2%
TOTAL	100	**100%**

Fuente: Estudiante de los niveles superiores de la Carrera: Ingeniería en Informática y Sistemas Computacionales
Elaborado por: Chicaiza Gabriel, Escobar Javier

GRÁFICO Nº 6: Calidad de Llamadas

Fuente: Estudiante de los niveles superiores de la Carrera: Ingeniería en Informática y Sistemas Computacionales
Elaborado por: Chicaiza Gabriel, Escobar Javier

Análisis e Interpretación

Los usuarios opinan que la calidad de las llamadas depende de diferentes factores como: tipo y calidad del dispositivo para realizar la llamada, calidad o intensidad de la señal en el dispositivo, tipo de conexión y lugar donde se encuentra.

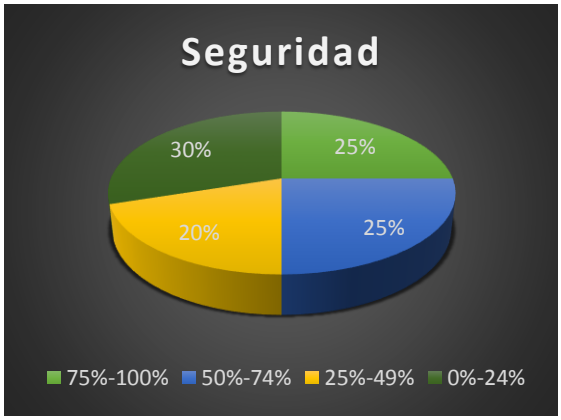
Pregunta 7: ¿En cuánto la seguridad, que tan confiable crees que es al momento de realizar la llamada?

TABLA N° 8: Confiabilidad de las Llamadas

Parámetros	Frecuencia	Porcentaje
75%-100%	25	25%
50%-74%	25	25%
25%-49%	20	20%
0%-24%	30	30%
TOTAL	100	**100%**

Fuente: Estudiante de los niveles superiores de la Carrera: Ingeniería en Informática y Sistemas Computacionales
Elaborado por: Chicaiza Gabriel, Escobar Javier

GRÁFICO Nº 7: Confiabilidad de las Llamadas



Fuente: Estudiante de los niveles superiores de la Carrera: Ingeniería en Informática y Sistemas Computacionales
Elaborado por: Chicaiza Gabriel, Escobar Javier

Análisis e Interpretación

Los encuestados opinan que la seguridad depende de la red a la que estén conectados, también que los filtros por donde pasa la información estén bien implementados y no dejen que intrusos intercepten las comunicaciones.

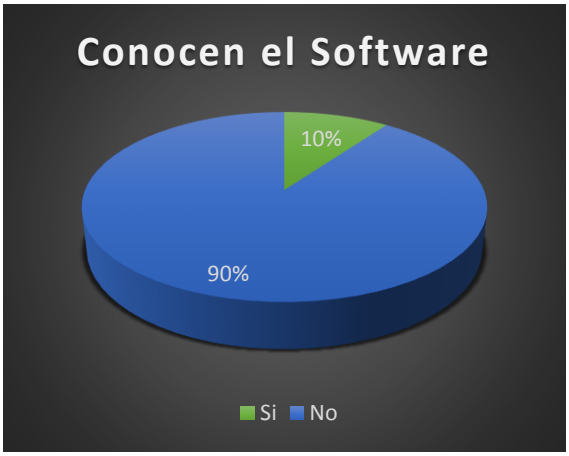
Pregunta 8: ¿Has escuchado sobre la aplicación sección borden controller (permite hacer llamadas)

TABLA N° 9: Session Border Controller

Parámetros	Frecuencia	Porcentaje
Si	10	10%
No	90	90%
TOTAL	100	**100%**

Fuente: Estudiante de los niveles superiores de la Carrera: Ingeniería en Informática y Sistemas Computacionales
Elaborado por: Chicaiza Gabriel, Escobar Javier

GRÁFICO Nº 8: Session Border Controller



Fuente: Estudiante de los niveles superiores de la Carrera: Ingeniería en Informática y Sistemas Computacionales
Elaborado por: Chicaiza Gabriel, Escobar Javier

Análisis e Interpretación

Para los encuestados los términos aplicación sección borden no son muy conocidos, lo cual permitió que respondieran negativamente a la pregunta en cuestión pero también se observa que surgió el interés o la curiosidad de saber más acerca de ese término.

Pregunta 9: ¿Estarías dispuesto a utilizar este software (SBC) o aplicación para hacer llamadas de buena calidad, seguridad, y disponibilidad?

TABLA N° 10: Utilización SBC para las Llamadas

Parámetros	Frecuencia	Porcentaje
Si	90	90%
No	10	10%
TOTAL	100	**100%**

Fuente: Estudiante de los niveles superiores de la Carrera: Ingeniería en Informática y Sistemas Computacionales
Elaborado por: Chicaiza Gabriel, Escobar Javier

GRÁFICO Nº 9: Utilización SBC para las Llamadas

Fuente: Estudiante de los niveles superiores de la Carrera: Ingeniería en Informática y Sistemas Computacionales
Elaborado por: Chicaiza Gabriel, Escobar Javier

Análisis e Interpretación

Los encuestados opinan que sería una bueno opción utilizar las características de SBC para las comunicaciones seguras, donde se mantienen las comunicaciones intactas pero con un re direccionamiento para cada una de las comunicaciones y una mejor fidelidad de la comunicación.

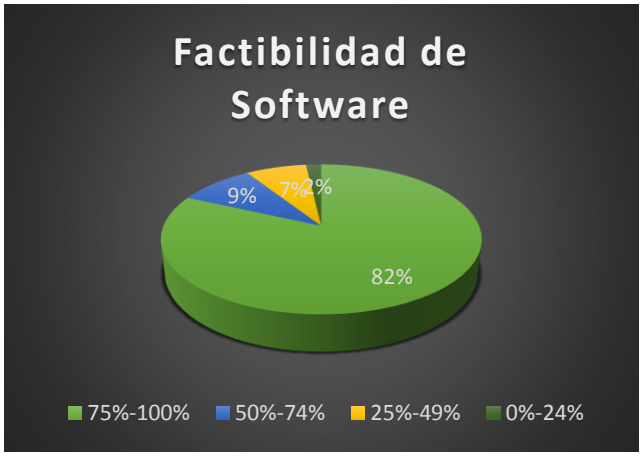
Pregunta 10: ¿Qué tan factible crees tú que se pueda implementar este software en la universidad?

TABLA N° 11: Implementar este Software

Parámetros	Frecuencia	Porcentaje
75%-100%	80	82%
50%-74%	10	9%
25%-49%	8	7%
0%-24%	2	2%
TOTAL	100	**100%**

Fuente: Estudiante de los niveles superiores de la Carrera: Ingeniería en Informática y Sistemas Computacionales
Elaborado por: Chicaiza Gabriel, Escobar Javier

GRÁFICO Nº 10: Implementar este Software



Fuente: Estudiante de los niveles superiores de la Carrera: Ingeniería en Informática y Sistemas Computacionales
Elaborado por: Chicaiza Gabriel, Escobar Javier

Análisis e Interpretación

Los encuestados opinan que sería muy factible su utilización en la universidad para mejorar el porcentaje de seguridad en las comunicaciones internas de la universidad como también evitar cortes y mantener la señal constante.

2.9. Comprobación de la Hipótesis

Después de proporcionar los cuestionarios de opinión, de los Estudiantes de la Universidad Técnica de Cotopaxi de la Carrera Ingeniería en informática y Sistemas Computacionales se procedió a la tabulación manual de los datos de manera independiente, tal como se presenta a continuación:

El desarrollo del ANÁLISIS E IMPLEMENTACIÓN DE SESSION BORDER CONTROLLERS SBC Y ENCRIPTACIÓN DE PAQUETES APLICADA EN LA SEGURIDAD DEL SISTEMA VOIP mejorará la transferencia de información de estudiantes y profesores en laboratorio de redes de la Carrera de Ingeniería en Informática y Sistemas Computacionales de la Universidad Técnica De Cotopaxi.

Para la verificación de la hipótesis se procedió a realizar las encuestas detalladas anteriormente en donde se pudo verificar que la hipótesis es verdadera tomando en cuenta la tabulación de los datos en donde se evidenciar que 82% está de acuerdo a la implementación de Session Border Controller sbc y encriptación de paquetes aplicada en la seguridad del sistema VoIP, el 90% indican que la implementación de un sistemas de gestión de inventarios, la generación de seguridad y confortabilidad en exigencia de transmisión de datos, El 85% dicen que con la implementación de este sistema se mejorará la inseguridad y demora de transferencia de información. Por todo esto es factible la implementación de Session Border Controller sbc y encriptación de paquetes aplicada en la seguridad del sistema VoIP en el laboratorio de la Carrera de Ingeniería en Informática y Sistemas Computacionales.

Para la comprobación se realizó las pruebas correspondientes del Session Border Controller y Encriptamiento de paquetes en la seguridad del sistema VoIP para su correcto funcionamiento. Así pues en la implementación se verificó que esté funcionando correctamente el equipo virtualizado.

El SBC en muchos casos, con el fin de ocultar la topología de la red y proteger la red de paquetes de servicios, el controlador de SBC es un dispositivo que se utiliza en redes de VoIP para ejercer control sobre la señalización y por lo general también los flujos de medios que interviene en la preparación, ejecución de llamadas.

El SBC se aplica en la seguridad, calidad de servicio y mecanismo de control sobre la admisión a las sesiones de VoIP. El Session Border Controller se instaló en un punto de demarcado entre una parte de una red y otra. El SBC es como un servidor de seguridad para VoIP. A menudo se configura como un agente de usuario

Después de realizar el análisis correspondiente a la VoIP y sus características; se puede verificar y revisar como es el funcionamiento de ataques en la red y determinar cómo afecta a la VoIP.

Al determinar las herramientas e implementar el Session Border Controller para una mejora en la seguridad se concluyó que los aspectos de fidelidad de la comunicación aumentaron y dan una mejor experiencia dentro del laboratorio.

CAPITULO III

3. IMPLEMENTACIÓN DE SESSION BORDER CONTROLLERS SBC Y ENCRIPTACIÓN DE PAQUETES APLICADA EN LA SEGURIDAD DEL SISTEMA VOIP

3.1. Presentación

La propuesta se fundamentó en los resultados de la investigación; así como también en las disposiciones legales y constitucionales expuestas en la constitución de la Republica y la Ley Orgánica de Educación Superior.

La implementación de Session Border Controller y encriptamiento de paquetes aplicada en el sistema VoIP, se efectuó en razón de los actuales avances tecnológicos y necesarios de la universidad de contar de un laboratorio de práctica de redes para lograr una educación de calidad con calidez.

Los Docentes y Autoridades universitarias, tienen la facultad y obligación de ir formando su criterio acerca de la necesidad de fortalecer los procesos de enseñanza-aprendizaje a través del uso del laboratorio equipado con los actuales avances tecnológicos,

Para el desarrollo de esta investigación se ordenó y compendio la información obtenida en el medio nacional e internacional, analizando los avances tecnológicos y necesidades actuales, los cuales son sumamente necesarios en la

formación profesional del Ingeniero en Informática y Sistemas Computacionales, por lo tanto consideramos que nuestra propuesta es de gran interés en el proceso académico y formación profesional.

3.2. Objetivos

3.2.1. Objetivo general

Analizar e Implementar una herramienta para la seguridad del sistema VoIP basa en la tecnología de Session Border Controller y encriptamiento de paquetes para la protección de las personas que utilizan este medio de comunicación.

3.2.2. Objetivos específicos

- Diseñar los aspectos y características relevantes del sistema de seguridad VoIP hasta la actualidad mediante la aplicación de técnicas adecuadas de recolección de información también se determinarán los métodos de investigación precisos para el desarrollo, lo cual permitirá el establecimiento de medidas de protección.
- Analizar un estudio de cómo actúan los ataques en el sistema VoIP.
- Determinar las herramientas necesarias para monitorear los ataque en el sistema.
- Proponer los procedimientos necesarios para la implementación de Session Border Controller y encriptamiento de paquetes como medida de seguridad en los Sistemas de VoIP.

3.3. Justificación e Importancia

La importancia de las seguridades sobre el sistema VoIP con Session Border Controller y encriptamiento de paquetes se utiliza en entornos de vigilancia, seguridad y también para el control de la calidad de las comunicaciones. Esto permite controlar el número de llamadas simultáneamente y el ancho de banda preciso y pueden rechazar nuevas llamadas para no perder la calidad de aquellas que estén en curso.

La tecnología en sistema VoIP básica que posee en la actualidad, está evolucionando a las novedosas redes de nueva generación. En esta solución de red, se sustituye la infraestructura de la comunicación de circuitos por una infraestructura de conmutación de paquetes basada en el protocolo IP que permite la trasmisión de voz sobre una red originalmente concebida para el flujo de datos. Este planteamiento ofrece múltiples ventajas entre las cuales destacan.

- Optimización del ancho de banda necesario para la conectividad.

- Reducción de costos: La reducción de costos asociados a la realización de llamadas regionales y en especial al tráfico de llamadas internacionales, han sido el motor fundamental del desarrollo de telefonía redes VoIP. Esta reducción considerable de costos en la telefonía tanto para el prestador de servicios como para el usuario final logrará que el servicio se pueda manifestar a lo largo y ancho de las sociedades.

La aceptación y expansión que tiene hoy en día los sistemas de VoIP cuentan con una gran capacidad de procesamiento, almacenamiento y personalización con la que cuenta este hardware y software. Esto deriva a una gran flexibilidad y agilidad en los procesos de seguridad, ahorrando costes y gran cantidad de tiempo. Así pues, se desean aprovechar todas estas características para su aplicación en el proceso de seguridad.

En la actualidad el sistema VoIP se ha convertido en un gran problema por las inseguridades que tiene el sistema VoIP, que les ponen en riesgos tanto como a los empleados como a los clientes. Es importante que todas las personas que utilizan este medio se sientan seguras, con la garantía que no tendrán ningún problema en la llamada sobre VoIP.

Una forma de garantizar la utilización del sistema VoIP, es mediante la implementación de Session Border Controller y encriptamiento de paquetes que permitirá el monitoreo constante de anomalías que se pudieran dar. En la actualidad existe la tecnología para el control y señalización de las llamadas VoIP que tengan una visión total de lo que está sucediendo en la red. Que permitirá actuar rápido y tomar las decisiones del caso que llegara ocurrir algún evento que requiera la intervención de los encargados del servicio VoIP. Dentro de los eventos que se pudiesen detectarse de cualquier índole.

Los investigadores luego de realizar una minuciosa investigación en fuentes bibliográficas por medio del internet podemos decir que tenemos suficiente información tanto textos y videos actuales.

El análisis sobre la implementación de Session Border Controller y Encriptamiento de paquetes aplicada en la seguridad del sistema VoIP tienen un gran desarrollo ya que la mayoría de empresas e instituciones utilizan el sistema VoIP esto hace posible la utilización y compatibilidad de muchas herramientas.

La prevención es detectar los problemas de denegación de servicio, que afectan a la disponibilidad del servicio VoIP. O los accesos desautorizados que puedan terminar afectando la confidencialidad del servicio (escuchar de forma no autorizada de la suplantación de identidad, robos del servicio de voz, redirección, etc.).

El proyecto es factible por que la Carrera de Ingeniería en Informática y Sistemas Computacionales cuenta con los recursos humanos y tecnológicos que se requiere para el proyecto.

Los equipos están en capacidad para implementación del SBC y también si el personal está capacitado y se cuenta con el suficiente conocimiento.

En cuanto al aspecto educativo el proyecto servirá de apoyo para aquellas personas que en el futuro necesiten implementar sistemas de seguridad o para aquellos que simplemente necesiten consultar un aspecto relevante del sistema VoIP.

3.4. Metodología de la Propuesta

En esta metodología nos dice que la implementación del Session Border Controller y Encriptamiento de paquetes aplicada en el Sistema VoIP, es la suma de todas las

actividades de planeación y control, enfocadas a mantener una red eficiente y con altos niveles de disponibilidad.
La metodología presentada se basa en un modelo con tareas bien definidas y complementarias. Esta modularidad permite su mejor entendimiento y facilita su implementación.

Se enfatiza en todos los aspectos relacionados en la buena operación de una red, como son el control sobre los sucesos en el sistema VoIP, la visualización de los tipos de tráfico, la determinación y atención oportuna de problemas, aspectos de seguridad.

3.4.1. Fase 1 Recopilación de información de las generaciones de redes en la seguridad informática

En este capítulo se explican detalladamente todos los pasos realizados para la implementación del presente trabajo especial de grado. Empezamos por la documentación y levantamiento de información de Session Border Controller y encriptamiento de paquetes, la evaluación del equipo y finalmente una matriz de riesgos que permitirá la seguridad del sistema VoIP que es el objetivo de este trabajo.
Levantamiento de la información esta fase inicial consistió en investigar detalladamente y exhaustivamente la información necesaria para poder llevar a cabo el proyecto, empezando las redes basadas en conmutación de circuito, como redes telefónicas, las redes basadas en conmutación de paquetes, o eres como son las redes generación. Se realizó una investigación exhaustiva sobre el equipo Session Border Controller, los elementos que la conforman, protocolos de señalización utilizados por esta tecnología, ventajas de este tipo de red. Se realizaron búsquedas electrónicas a

través del internet en libros. La información más relevante se encuentra documentada en el marco teórico del presente documento.

Para finalizar esta primera fase del trabajo, al igual que para el equipo Session Border Controller se realizó una investigación exhaustiva acerca de esta tecnología, como su implementación en la seguridad del sistema VoIP y los elementos que la conforman, los protocolos de señalización utilizados, y los benéficos de la implementación de esta tecnología. Para esto también se realizaron búsquedas electrónicas en libros.
Evaluación de equipo Session Border Controller.

Se inició con la evaluación del equipo en una máquina virtual, se estudió a profundidad el Session Border Controller, sus ventajas, a partir de la documentación y toda la información recopilada, para determinar puntos vulnerables o posibles brechas presentes, a nivel de seguridad de la operación. Que puedan atentar contra este equipo o contra los servicios ofrecidos a los usuarios finales.

El procesó a elaborar una máquina virtual con un servidor Centos para la prueba del equipo, con los aspectos a evaluar necesarios para determinar los riesgos presentes o potenciales en la implementación que se puedan ocasionar la degradación o negación de los servicios. Las pruebas se fundamentaron en dos principales partes; el protocolo SIP (Session initiation protocol), encargado de iniciar, mantener y finalizar las llamadas; y el protocolo H.323 que está definido para la señalización y la gestión de las sesiones, y para la comunicación entre elementos de control de la red. Una página de SBC sirvió mucho para la realización de las pruebas, para la configuración de los parámetros y características necesarias para la iniciar las pruebas y establecer trazas para capturar la señalización correspondiente. Se configuraron las variables de monitoreo a tener en consideración durante la evaluación, en cuanto a comportamiento del servicio, porcentaje de uso de la máquina virtual del software sbc, la RAM y tráfico de red, las pruebas propuestas se ejecutaron en su totalidad.

3.4.2. Fase 2 Levantamiento de las máquinas virtuales

3.4.2.1. Requisitos Servidor Dhcp

- 1 PC
    - Intel Core i7-6700T
    - Procesador (8M Cache, up to 3.60 GHz)
    - 4 RAM
    - Disco Duro 500
    - Sistema Operativo Windows8 64 bit
- Bridget network device

3.4.2.2. Servidor Dhcp

Es un servidor que recibe peticiones de clientes solicitando una configuración de red IP. El servidor a dichas peticiones proporciona los parámetros que permitan a los clientes auto configurarse. Para que un PC solicite la configuración en un servidor, en la configuración de red de los PCs hay que seleccionar la opción "Obtener dirección IP automática.

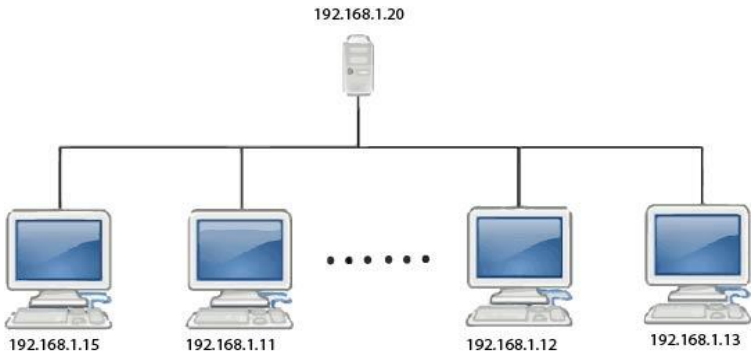
3.4.2.3. Funcionamiento de una petición Dhcp

El servidor solo asigna direcciones dentro de un rango prefijado. Si por error hemos configurado manualmente una IP estática perteneciente al rango gestionado por nuestro servidor Dhcp, podría ocurrir que dicha dirección sea asignada dinámicamente a otro PC, provocándose un conflicto de IP. En ese caso el cliente solicitara y comprobara, otra dirección IP. Que no esté asignada actualmente a ningún otro equipo de nuestra red.

La primera Vez que seleccionemos una Pc que su configuración IP se determine por DHCP, este pasara a convertirse en un cliente DHCP e intentara localizar un servidor Dhcp para obtener una configuración desde el mismo. Si no encuentra ningún

servidor Dhcp, el cliente no podrá disponer de dirección IP y por lo tanto no podrá comunicarse con la red. Si el Cliente encuentra un servidor Dhcp, este le proporcionara, para un periodo predeterminado, una configuración IP que le permitirá comunicarse con la red. Cuando haya transcurrido el 50% del periodo, el cliente solicitara una renovación del mismo.

FIGURA Nº 3: Dhcp



Fuente: Chicaiza Gabriel, Escobar Javier

3.4.2.4. Requisitos Session Border Controller

- 1 PC
  - Intel Core i7-6700T
  - Procesador (8M Cache, up to 3.60 GHz)
  - 4 RAM
  - Disco Duro 500
  - Sistema Operativo Windows8 64 bit
- Bridget network device

3.4.2.5. Session Border Controller

Un SBC es un dispositivo de sesión de cuenta VoIP que controla la admisión de llamadas a una red en la frontera de la red. De forma opcional (dependiendo del

dispositivo), también se puede llevar a cabo una serie de funciones de control de llamadas.

El SBC se ha convertido en un elemento importante de voz a través de redes IP (VoIP), como proveedores de servicios buscan para proteger la integridad de sus redes y modelos de negocio al tiempo que ofrece diversos servicios a sus clientes.

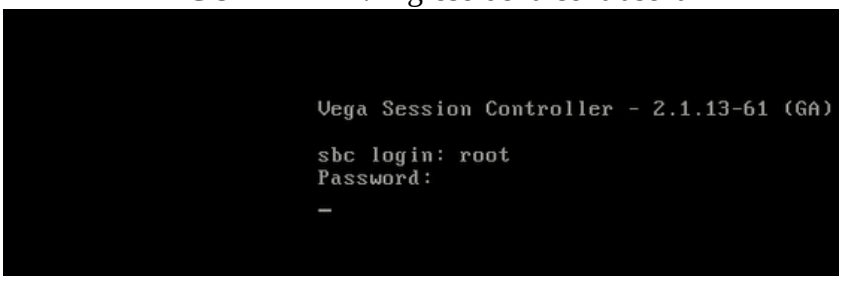
La mayoría de las personas estaría de acuerdo en que un SBC es una especie de servidor de seguridad para el tráfico de voz sobre IP. Sin embargo, tan pronto como empiece a mirar más allá de este consensó inicial, existe un desacuerdo considerable en cuanto a lo que realmente es un SBC, y que función debe ofrecer. El SBC están presionando a cubrir una amplia variedad de nichos con el fin de competir por cuotas de mercado, y en parte debido a la verdadera gama de escenarios en los que los proveedores de servicios están buscando soluciones.

3.4.2.6. Implementación del Session Border Controller

Ejecución del SBC.

Este paso observamos la pantalla donde colocamos nuestro usuario y contraseña.

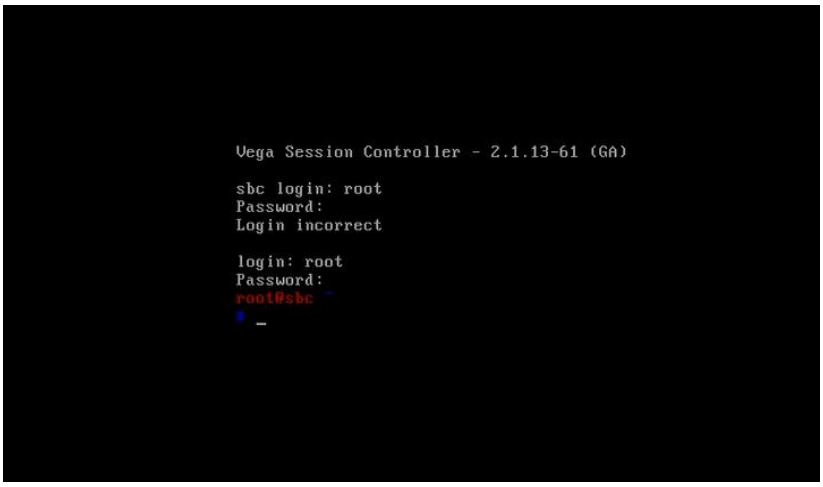
FIGURA Nº 4: Ingreso de la contraseña



Realizado por: Chicaiza Gabriel, Escobar Javier

Luego de poner correctamente el usuario y la contraseña ya que sale que ya estamos en el SBC.

FIGURA Nº 5: Visualización SBC



Realizado por: Chicaiza Gabriel, Escobar Javier

Comandos del sistema

El sistema de SBC está basado en Linux

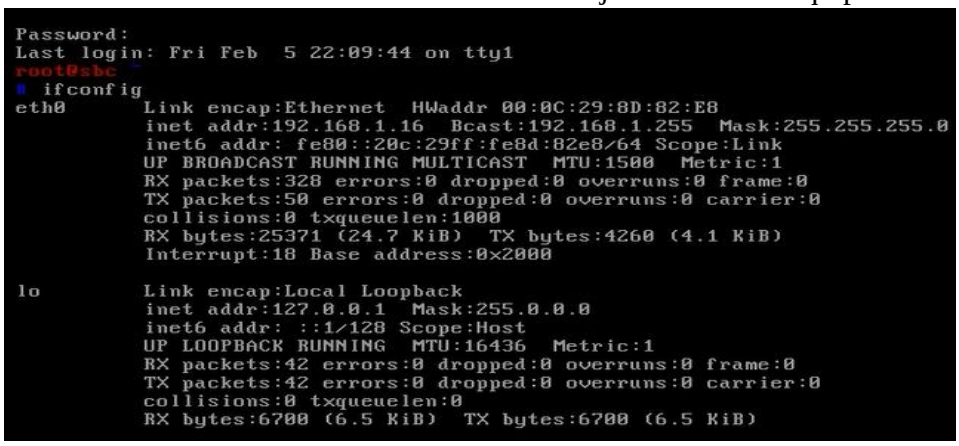
Los comandos más utilizados son:

Tcpdump: Captura la red a un archivo.

Ethtool: Proporciona información detallada de la interfaz de la red.

Ifconfig: Muestra los contadores de errores en las interfaces Ethernet.

FIGURA Nº 6: Visualización de la tarjeta de red del equipo



Realizado por: Chicaiza Gabriel, Escobar Javier

Visión General

La sección de visión general obtiene SBC información del estado del SBC así como el iniciar, detener, reiniciar los servicios del SBC.

TABLA N° 12: *Tablero (Dashboard)*

Sesión	**Descripción**
Estado de Sistemas	Proporciona la información del SBC de su estado como el CPU la Memoria y los estados de servicios.
Tablero de Control	Se utiliza para inicializar, detener, reiniciar los servicios del SBC.

Realizado por: Chicaiza Gabriel, Escobar Javier

Señalización (Signaling)

Esta sección se muestra los detalles de los recursos SBC y la información de la señalización.

TABLA N° 13: Señalización (Signaling)

Session	**Descripción**
Estado del Perfil SIP	Configuraciones y estados detallados de cada perfil SIP creado.
Estado Trunk SIP	Configuraciones y estados detallados de cada Trunk SIP creado
Estado de Session del SIP	Detalla todas las Sesiones SBC actualmente activas.

Realizado por: Chicaiza Gabriel, Escobar Javier

Medios de comunicación

Esta sección se muestra los detalles de los recursos SBC para los medios de información relacionados.

TABLA N° 14: Medios de comunicación

Session	**Descripción**
Estado de la Interfaz de medios de comunicación.	Muestra numerosas listas de todas las interfaces de hardware soportado por el SBC.

Realizado por: Chicaiza Gabriel, Escobar Javier

Seguridad

La sección de seguridad proporciona la información de IP bloqueadas para cada uno de los servicio de seguridad.

Configuración

Sección de configuración se utiliza para la configuración de las características del SBC.

Sistema

Sección del sistema se utiliza para la configuración de las funciones enlazadas con el sistema, incluyendo notificaciones, puntos de auditoria, copia de seguridad y restauración.

Informes

Proporciona registros detallados e información de tráfico basado en tiempo real.

Ayuda

Proporciona ayuda y la actualización de la información.

Conexión inicial modo grafico Webgui

Esto permitirá conectar con nuestro SBC atreves del navegador web.
Colocar la IP en la parte superior del navegador la cual es 192.168.1.16 nos sale en modo gráfico y colocamos nuestro usuario y contraseña para donde ingresar a la plataforma de SBC.

FIGURA Nº 7: Modo gráfico contraseña

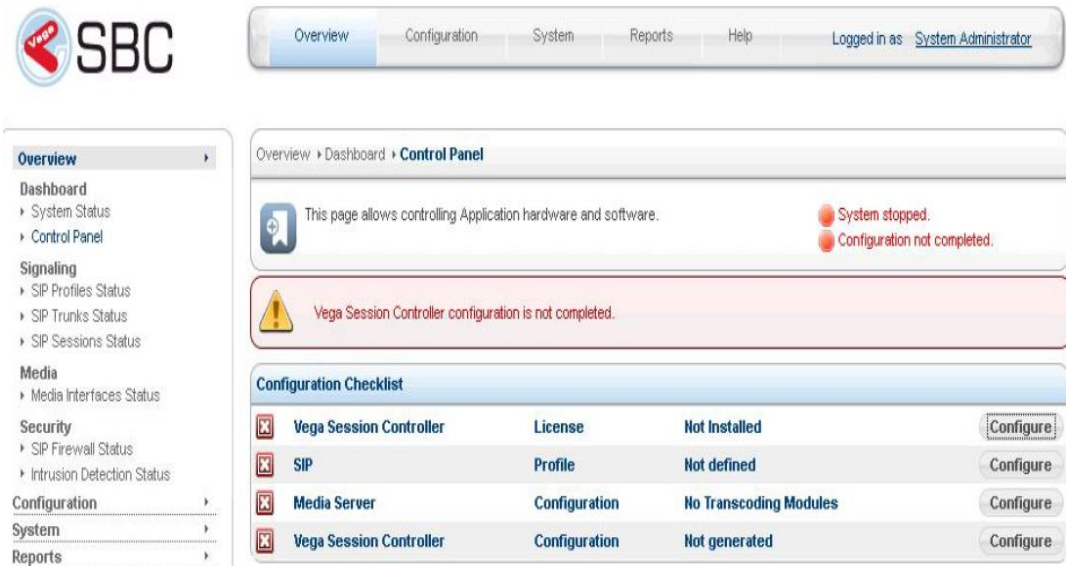
Realizado por: Chicaiza Gabriel, Escobar Javier

Sbc WebGUI estado inicial

En la parte superior de la pantalla WebGUI contiene diálogos de información que se utilizan para proporcionar mensajes importantes para el usuario.

Por debajo del dialogo de información, se encuentra la lista de verificación de configuración que indica cuales son la configuración mínima necesarias para obtener el correcto funcionamiento del SBC.

FIGURA Nº 8: Estado de inicio del SBC



Realizado por: Chicaiza Gabriel, Escobar Javier

Interfaz de señalización.

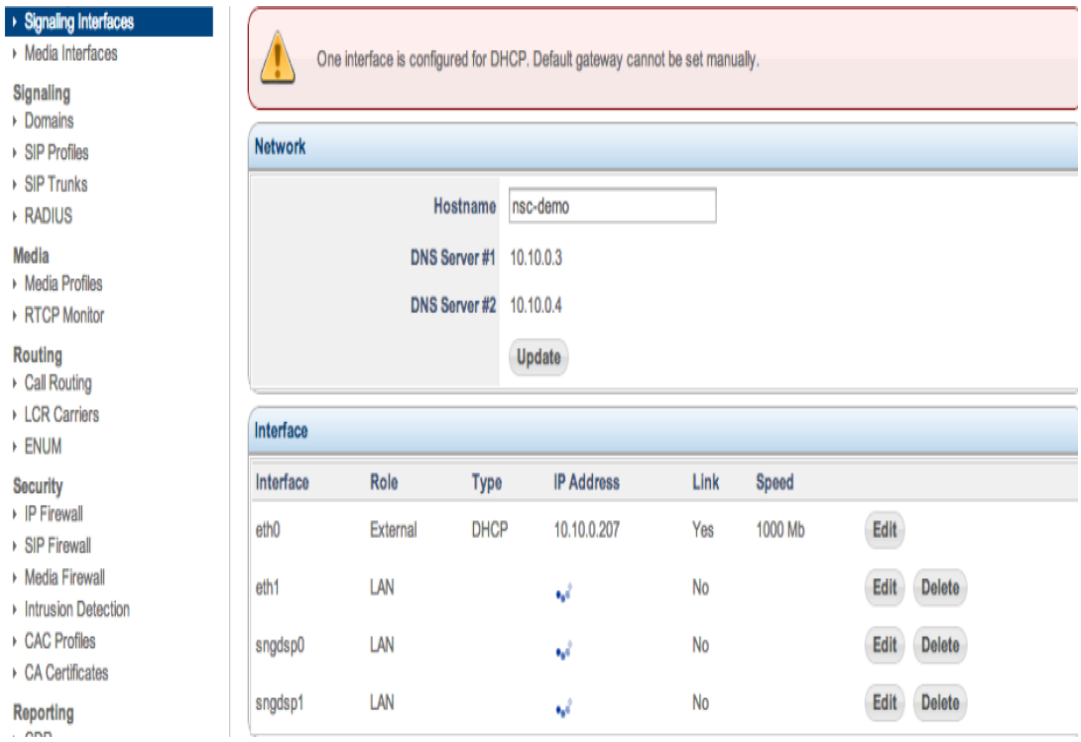
Es una interfaz de señalización que trata cualquier tipo de señalización del SIP que entra y sale del equipo SBC.

Se utiliza para transportar el tráfico de señalización SIP.

Señalización de interfaz primaria (eth0).

Interfaz de Señalización Secundaria (eth1)

FIGURA Nº 9: Configuración Signaling Interfaces



Realizado por: Chicaiza Gabriel, Escobar Javier

Esta interfaz de los medios de comunicación se ocupa de todas las formas de la comunicación que entra y sale del equipo SBC.

El primer paso para configurar las interfaces de comunicación es seleccionar el modo de medios de comunicación en el que operara.

- Hidden (Oculto)

  Las direcciones IP se ocultan en la red por defecto y es recomendable.

  Utiliza una dirección IP única para todos los medios de comunicación.
- Exposed (Expuesto)

  Las direcciones IP estarán expuestas a la red.

Usos múltiples de direcciones IP de los medios de comunicación.

- Disabled.(Desactivado)

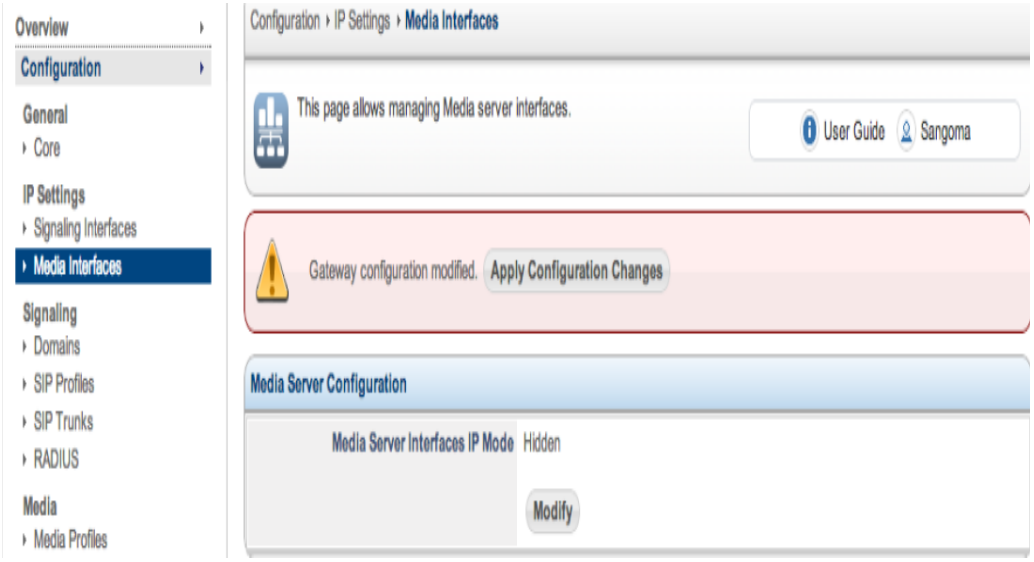
  Modelo de software sin interfaz.

  Se utiliza en entornos de VM.

Modo oculto

El modo oculto es más fácil de gestionar. En este modo todas las interfaces de medios están ocultas del sistema y todo el tráfico IP generado.

FIGURA Nº 10: Configuración Media Interfaces

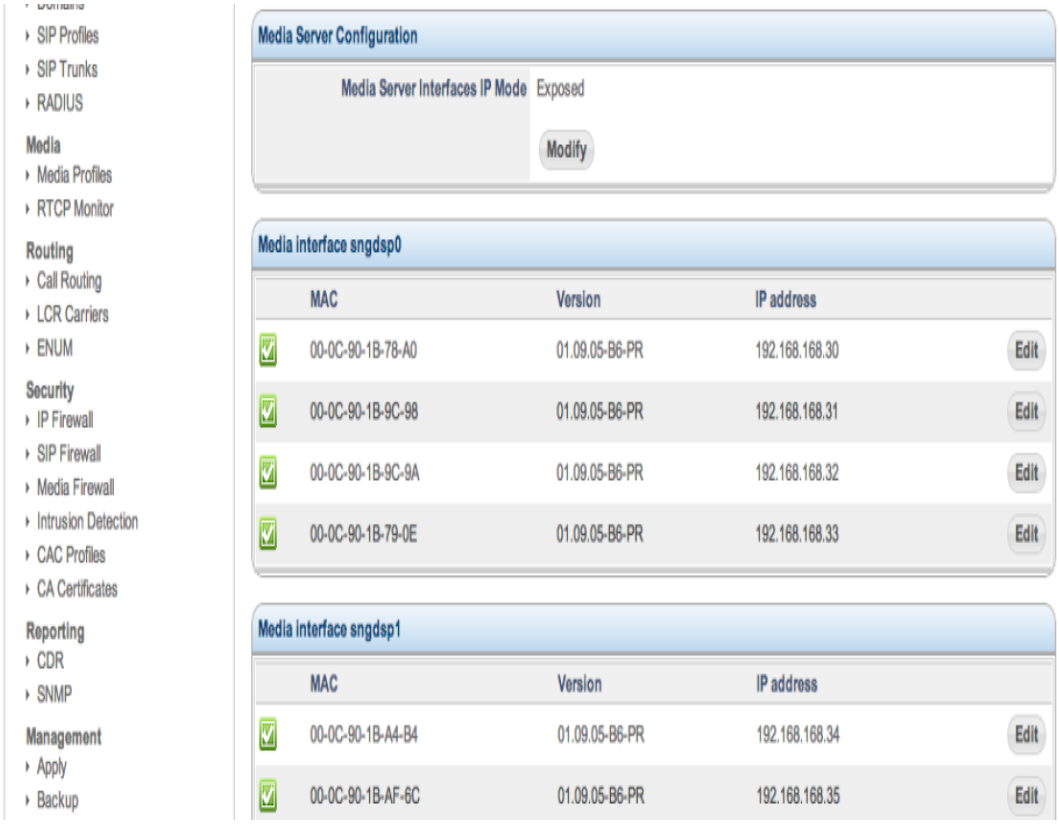


Realizado por: Chicaiza Gabriel, Escobar Javier

Modo Expuesto

Requiere una configuración más cuidadosa ya que las interfaces serán expuestas a su red y podrán ser observadas por todos los usuarios.

FIGURA Nº 11: Configuración Media Interfaces



Realizado por: Chicaiza Gabriel, Escobar Javier

Configuración del dominio SIP

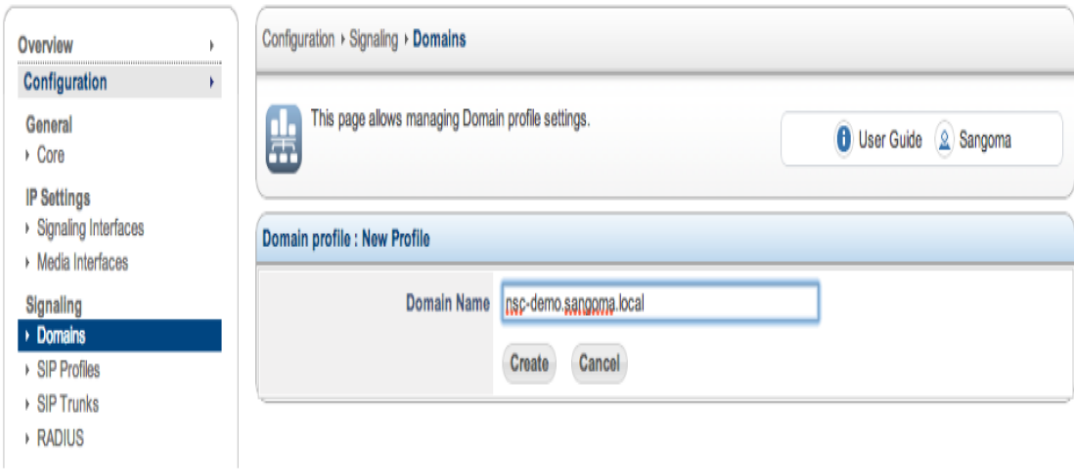
Los dominios también se conocen como “reinos” dentro de las redes SIP.

Un dominio SIP se utiliza para autenticar a los usuarios dentro de la SIP para los procesos de registro.

Los perfiles de dominio se utilizan para definir la forma en que los usuarios se autentican con el SBC.

Esto permite que se oculte la topología para que nadie de la red corporativa pueda saber acerca de los equipos que están conectados al SBC.

FIGURA Nº 12: Configuración Domains



Realizado por: Chicaiza Gabriel, Escobar Javier

Perfil de configuración SIP

Un perfil SIP es una cuenta basada en el SBC, que contiene un conjunto de atributos SIP que están asociados al mismo SBC.

- El perfil del SIP se utiliza como una configuración de los puntos finales externos que pueden conectarse al SBC.

- Enlaza una dirección IP, Puerto, y otras características relacionadas con el SIP a un Perfil SIP.

- También enlaza rutas de llamadas, perfiles de dominio, perfiles de soporte u trunks SIP a Perfil de SIP.

- El perfil SIP describe información local en el SBC.

FIGURA Nº 13: Configuration SIP Profiles

Realizado por: Chicaiza Gabriel, Escobar Javier

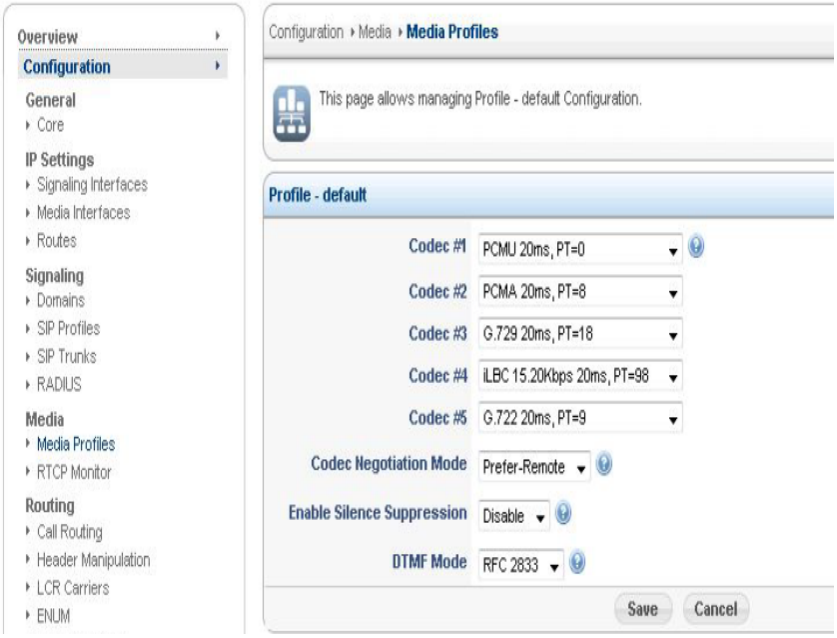
Medios de perfil de configuración

Un perfil de los medios de comunicación es una lista de atributos que definen lo que los códec de audio se utilizan las llamadas.

Los perfiles de soporte están unidos a uno o muchos perfiles del SIP.

- Dependiendo de caso de uso.
    - El usuario puede crear un perfil de los medios de comunicación por un perfil SIP.
    - El usuario puede crear un perfil de los medios de comunicación para muchos perfiles SIP.

FIGURA Nº 14: Configuración Media Profiles



Realizado por: Chicaiza Gabriel, Escobar Javier

Audio Códec

Un códec de audio es un programa implementado como un algoritmo que comprime y descomprime audio digital de los datos.

- Se puede configurar por perfil de los medios de comunicación.

SIP Trunk (Gateway)

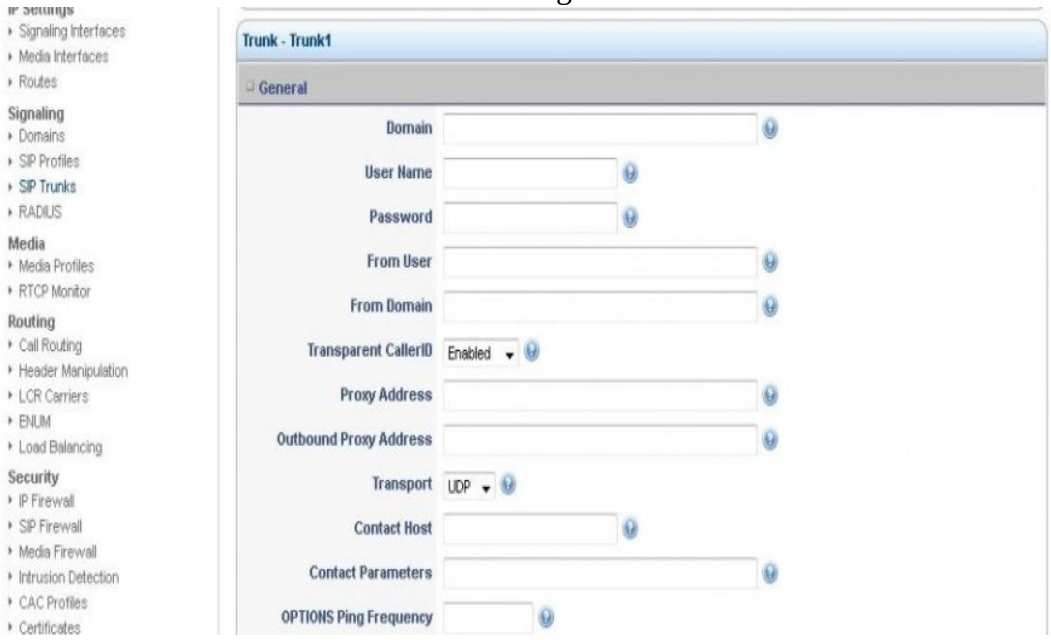
SIP Trunks se utiliza para conectar SBC a un SIP remotamente a un agente proveedor/usuario.

- Es la descripción de como el SBC se comunicara con ese punto final.
- Ejemplo: La dirección IP, el puerto, etc.

SIP Trunk suele contener.

- Información del dominio remoto
- Credenciales de autenticación remota
- La información del registro remoto.

FIGURA Nº 15: Configuración SIP Trunks



Realizado por: Chicaiza Gabriel, Escobar Javier

Enrutamiento de llamadas

SBC proporciona tres interfaces se llaman interfaces de enrutamiento.

- Enrutamiento de llamadas WebGUI.
- Método de configuración por defecto.

XML enrutamiento avanzado de llamadas de archivos.

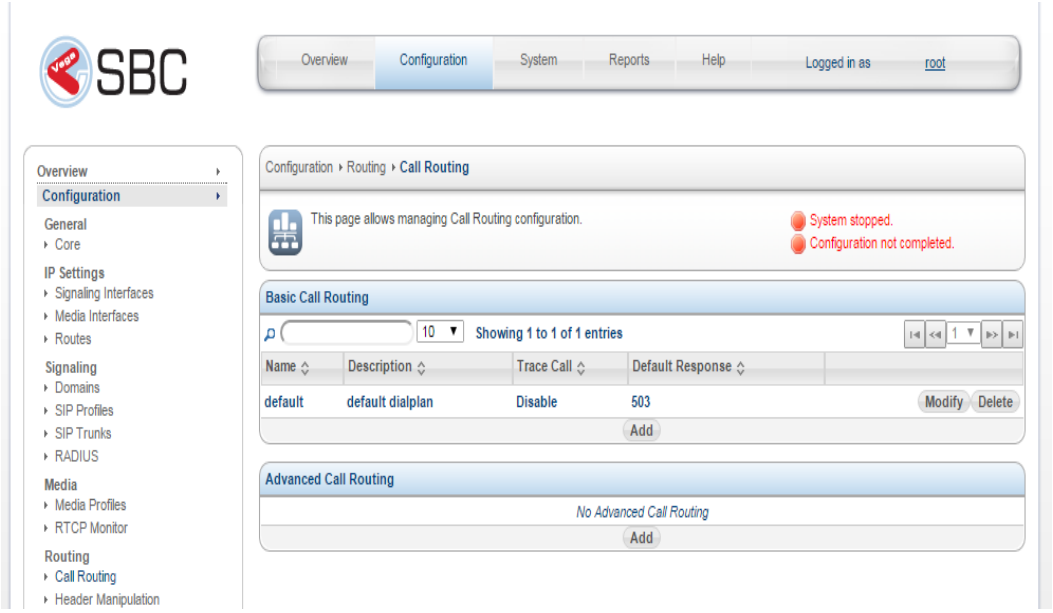
- Uno o más archivos de configuración XML se pueden utilizar para almacenar la información de enrutamiento de llamadas.
- Diseñado para usuarios avanzados.

Base de datos remoto.

- Para cada llamada SBC solicita la información de la base de datos centralizada enrutamiento.

Es el proceso utilizado para las llamadas telefónicas a través de una red de telefonía IP, como es una máquina virtual esta como default.

FIGURA Nº 16: Configuración Call Routing



Realizado por: Chicaiza Gabriel, Escobar Javier

Esta utiliza la interfaz gráfica de usuario de la SBC permitirá a los usuarios crear reglas de enrutamiento.

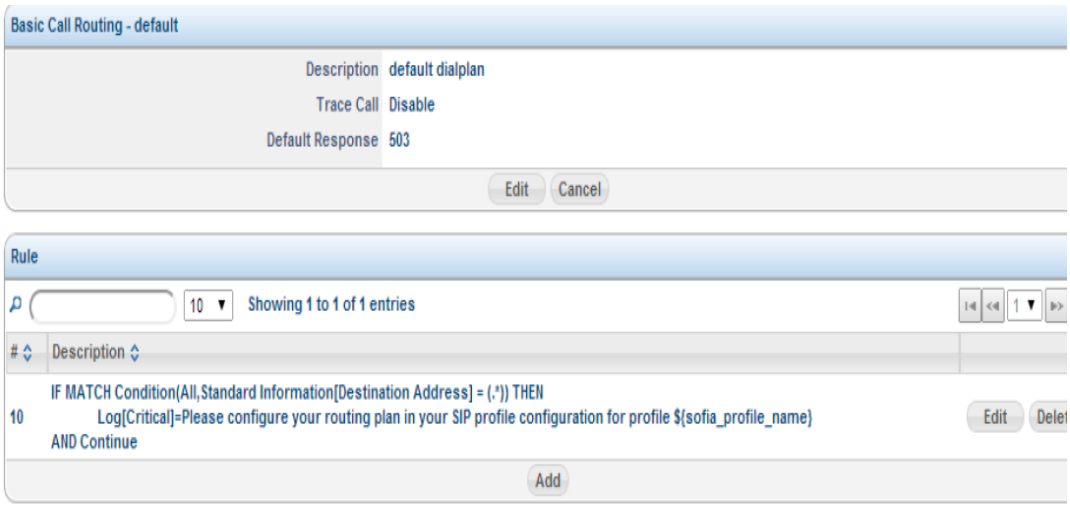
Se modela de manera que cualquiera sería capaz de crear casi cualquier tipo de escenario sin la necesidad de aprender XML.

- Cada plan de marcado se basa en que puede tener varias reglas asociadas con ella.

    - Cada regla se refiere a una condición específica que debe ser cumplida.

- Se puede programar la regla de continuar a la siguiente regla se pasa o no pasa.

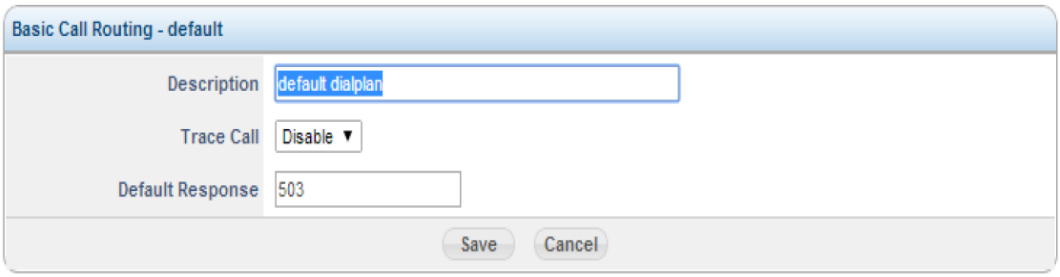
FIGURA Nº 17: Configuración Basic Call Routing



Realizado por: Chicaiza Gabriel, Escobar Javier

- Reglas
  - Esta sección trata de las normas específicas que se van a procesar dentro del plan de marcado.
  - Cada regla se describe en función de las selecciones elegidas dentro de la configuración de la regla.

FIGURA Nº 18: Configuración Basic Call Routing

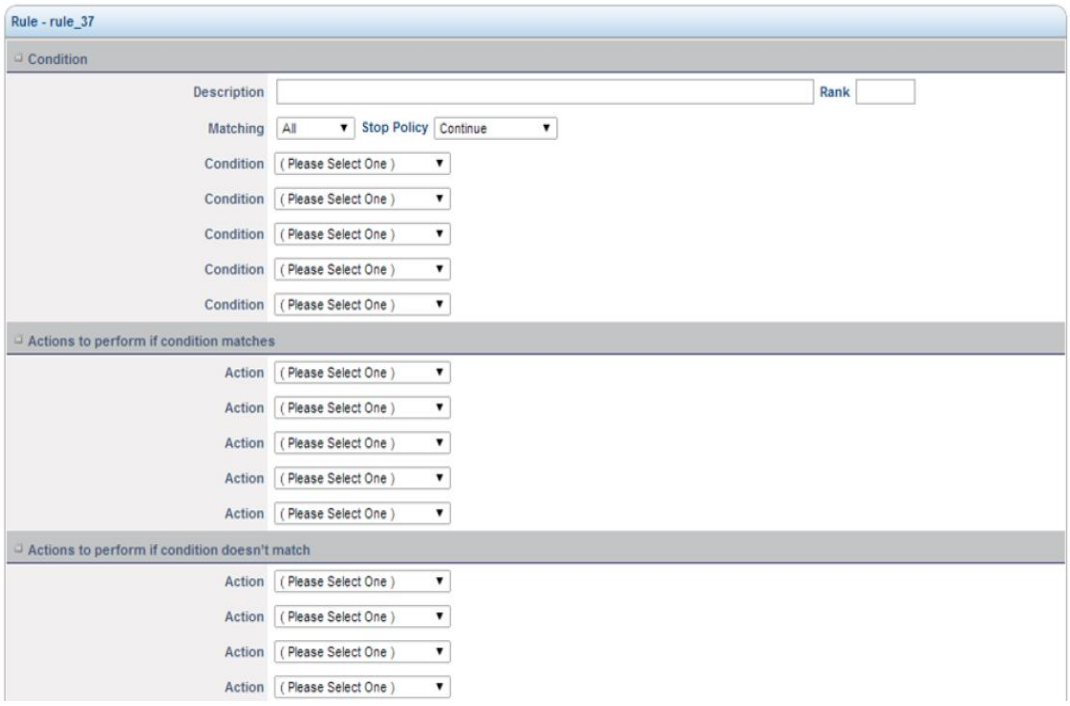


Realizado por: Chicaiza Gabriel, Escobar Javier

- Los parámetros por defecto identifican la descripción del plan de marcado, y lo que la respuesta SIP predeterminado los código será en un caso de fallo.
- Descripción
    - Descripción de lo que va a lograr el plan de marcado
- Rastreo de llamada.
    - Si el plan de marcado /perfil de llamadas de encaminamiento incluirá una señalización en el registro del SBC.
- Respuestas predeterminadas.
    - Código de respuesta SIP por defecto que será enviada en el caso de que el plan de marcado no pueda procesar la llamada a la que se entrega a ella.

Enrutamiento de llamadas creación de reglas.

FIGURA Nº 19: Creación de Reglas



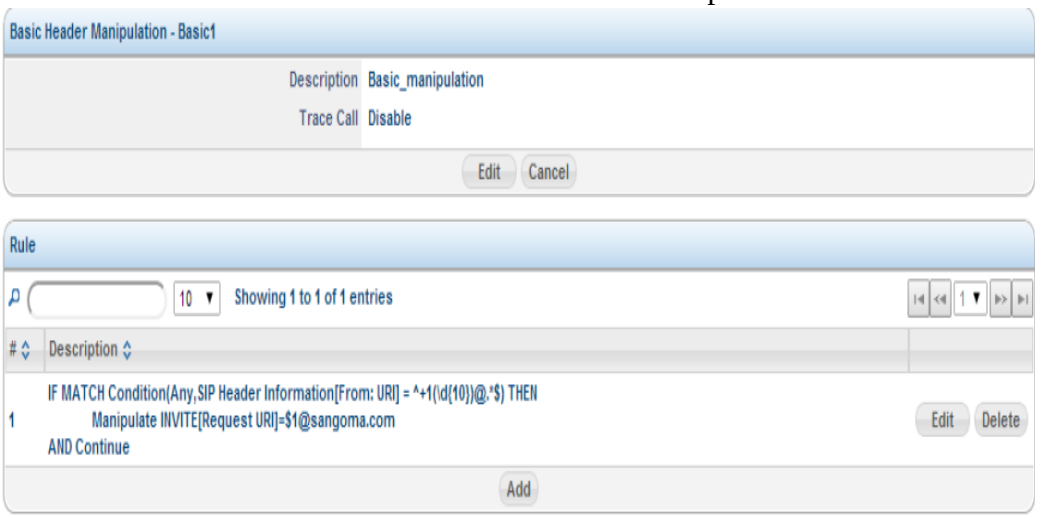
Realizado por: Chicaiza Gabriel, Escobar Javier

- Área de condición.
    - Se puede configurar hasta 5 condiciones que la regla que serán validadas.
    - El rango es la prioridad de la regla dentro del plan de marcado.
    - La política de parada determina si el plan de marcado debe detener el proceso si la regla coincide, o si deberá continuar a la siguiente regla.
- Acciones para llevar a cabo si la condición coincide con la sección.
    - Puede configurar hasta 5 acciones para llevar a cabo si las condiciones enumeradas se corresponden.
    - Puede haber diferentes acciones.
- Las Acciones para si la condición no coincide con la Session.
    - Puede configurar hasta 5 acciones para llevar acabo si la condición no coincide.
    - Puede haber diferentes acciones.

WebGUI: Manipulación del encabezado básico

Permite que a usuario no familiarizado con XML para construir reglas necesarias para la manipulación de la información SIP en llamadas entrantes o salientes.

FIGURA Nº 20: Basic Header Manipulation



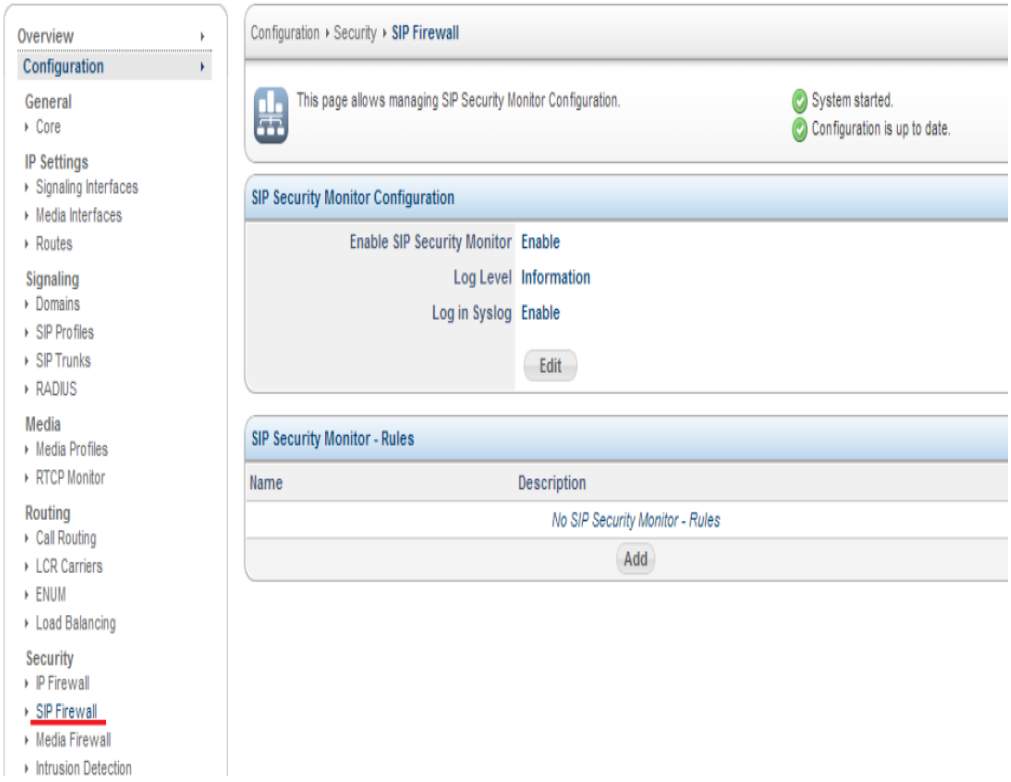
Realizado por: Chicaiza Gabriel, Escobar Javier

SIP Firewall

El servidor de seguridad SIP puede ayudar en la detección de conexiones SIP fracasadas en el SBC.

- El concepto general es el firewall SIP se compone de reglas que uno u otro daría o bloquearía al delincuente que intenta ingresar a la red por los intentos fallidos.
- Estas reglas pueden ser dirigidas hacia todas las IP y el agente de usuario o solo cierto agente de usuario o dirección IP.
- Además de estas reglas se pueden asociar a todos los perfiles de SIP o ciertos perfiles SIP.

FIGURA Nº 21: SIP Firewall



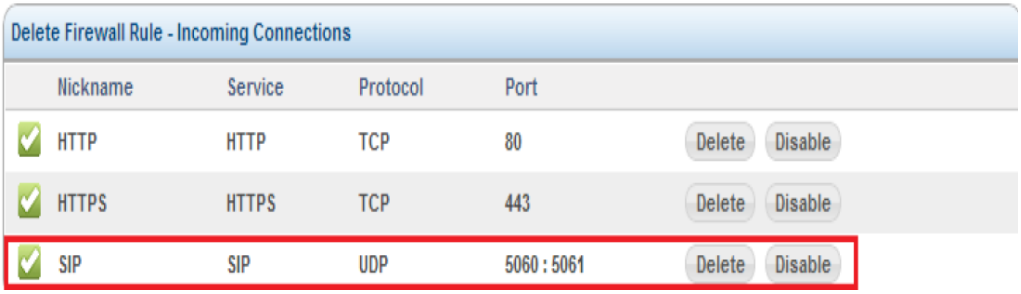
Realizado por: Chicaiza Gabriel, Escobar Javier

IP Firewall

El objetivo del IP firewall es bloquear todos los servicios en el SBC, excepto los que están en la lista de servicios permitidos.

Esto ayudará a proteger la unidad y se nos permitirá únicamente los servicios definidos.

FIGURA Nº 22: IP Firewall



Realizado por: Chicaiza Gabriel, Escobar Javier

Detección de intrusos SBC

El sistema de detección de intrusos en el SBC se ha pre configurado con una serie de ataques conocidos.

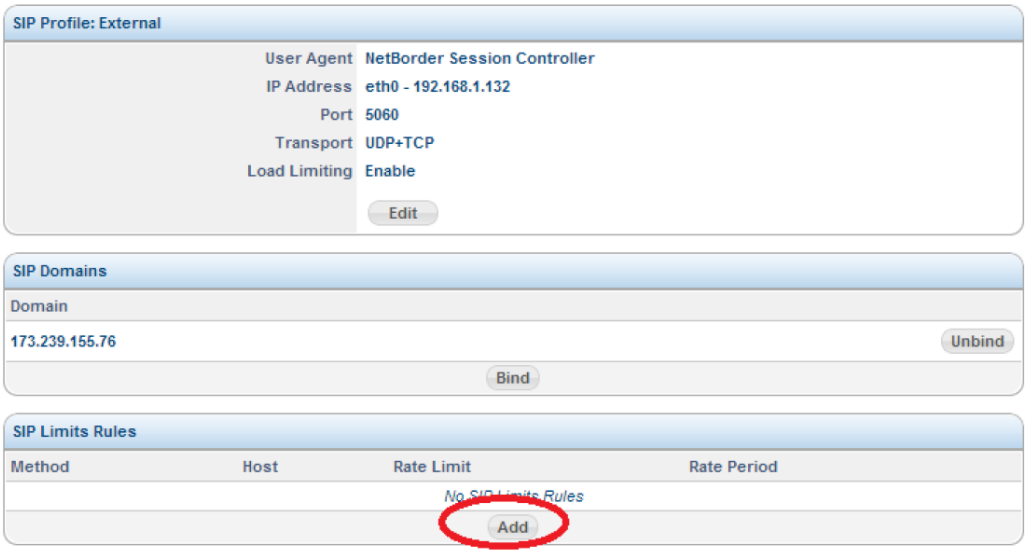
FIGURA Nº 23: Intrusion Detection

Realizado por: Chicaiza Gabriel, Escobar Javier

SIP Rate Limiting

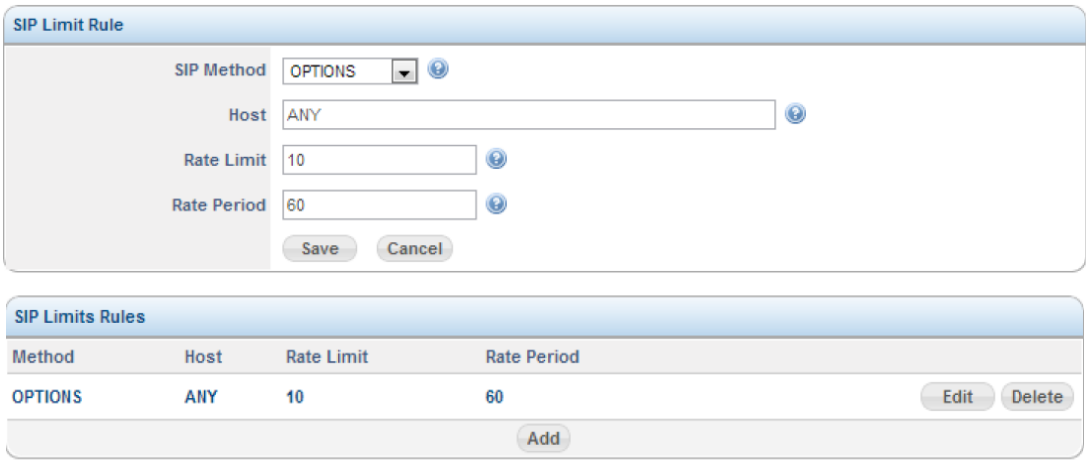
El propósito de la limitación de velocidad es evitar que un host que envíe demasiadas solicitudes SIP.

FIGURA Nº 24: SIP Rate Limiting



Realizado por: Chicaiza Gabriel, Escobar Javier

FIGURA Nº 25: SIP Rate Limiting



Realizado por: Chicaiza Gabriel, Escobar Javier

Operación SBC

SBC y sus servicios se divide en tres secciones.

- Servicios de Aplicaciones
    - La Principal es aplicación SBC
- Servicios de Seguridad
    - Los servicios de seguridad asociados con la aplicación principal SBC
- Servicios de medios.
    - Servicios para los medios que trabajan con la aplicación principal SBC.

TABLA N° 15: Descripción de Servicios SBC

Servicios	**Sección**	**Descripción**
NetSession Border Controller	Aplicación de Servicios	Principal SBC servicio de aplicación SIP para el mejoramiento de la seguridad.
IP Firewall	Seguridad Servicios	Configuración IP firewall. Se utiliza para crear reglas de cortafuego IP, como bloqueo de puertos. IP firewall se utiliza automáticamente por otros servicios de seguridad como parte del conjunto la seguridad SBC.

Detección de Intrusos	Seguridad Servicios	Reglas de detección de intrusos. Cuando las reglas de coincidencia de patrones de ataque conocida, el evento se pasa al servicio de prevención de intrusiones.
Prevención de Intrusos	Seguridad Servicios	Proceso de eventos de detección de intrusiones y aplicara las reglas del cortafuego en la IP entrante direcciones o puertos como el bloqueo.
Cubierta Segura	Seguridad Servicios	La consola de acceso SSH
Seguridad SIP de monitoreo	Seguridad Servicios	Se sujeta a la aplicaion principal SBC y monitoreo de eventos de señalización SIP. Una vez que se detecta un evento que se necesita acción. Tales como la detección de sobrecarga del SIP registro de paquetes y emplea el servicio de seguridad a tomar medidas como el bloqueo.
Medios de comunicación firewall	Seguridad servicios	Se sujeta a la aplicación principal SBC y monitorea eventos de medios. Se abre y se cierra puertos locales basándose en la información.

Realizado por: Chicaiza Gabriel, Escobar Javier

3.4.3. Fase 3 Pruebas

3.4.3.1. *Introducción*

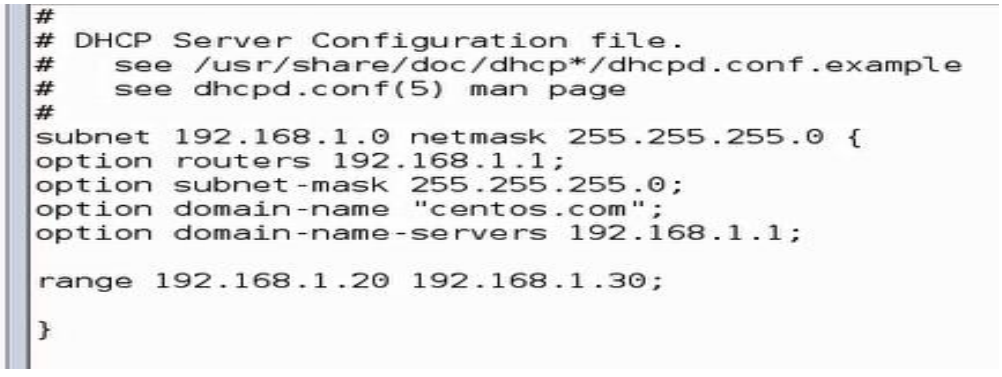
Las pruebas que se llevaron a cabo para comprobar el correcto estado y funcionamiento de los servicios implementados, servirá en gran medida para conocer más afondo su funcionamiento, se realizaron pruebas prácticas y explicativas las cuales aclaran cualquier duda sobre la operatividad de los servicios.

3.4.3.2. *Comprobación operatividad servidor dhcp*

Para comprobar el funcionamiento del servidor dhcp en la red, se realiso la configuración del equipo con dirección IP 192.168.1.20.

Configuracion del dhcp.

FIGURA Nº 26: Prueba Dhcp

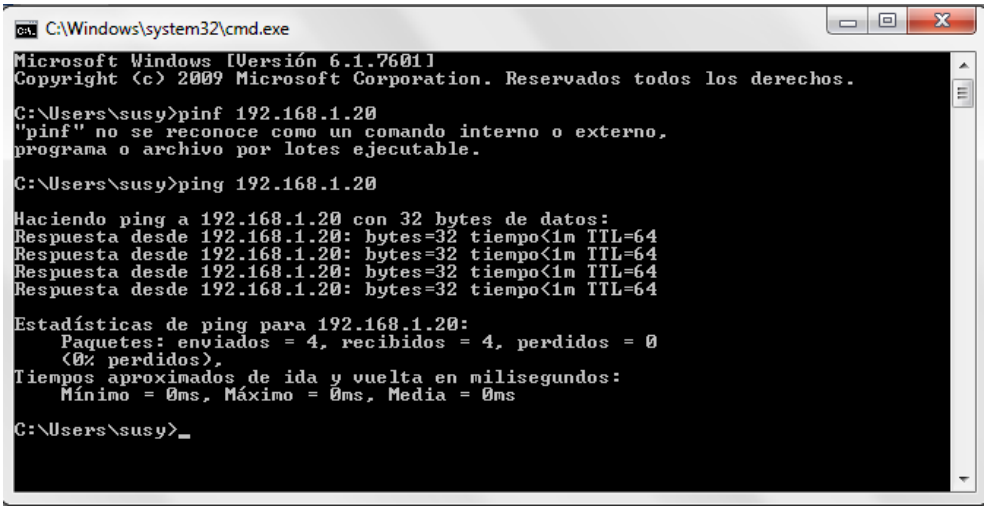


Realizado por: Chicaiza Gabriel, Escobar Javier

Al listar la configuración del equipo cliente se puede observar que opción de Dhcp está activa y que la dirección del servidor DHCP es la 192.168.1.20.

Para probar si hay conexión con nuestro servidor dhcp hacemos un ping desde mi cliente a mi servidor para que vean que si ahí conexión.

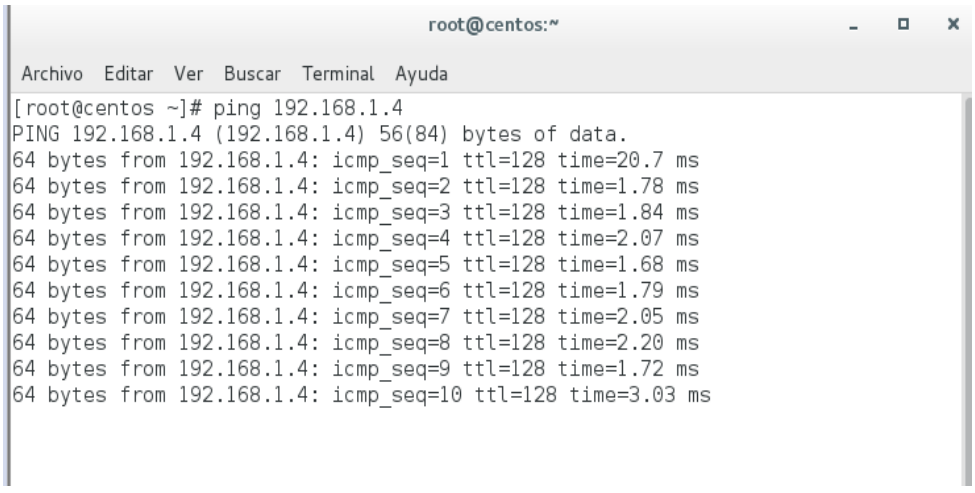
FIGURA Nº 27: Conexión con el Servidor DHCP



Realizado por: Chicaiza Gabriel, Escobar Javier

Ahora comprobamos si hay conexión desde mi servidor dhcp al cliente.

FIGURA Nº 28: Conexión con el Usuario



Realizado por: Chicaiza Gabriel, Escobar Javier

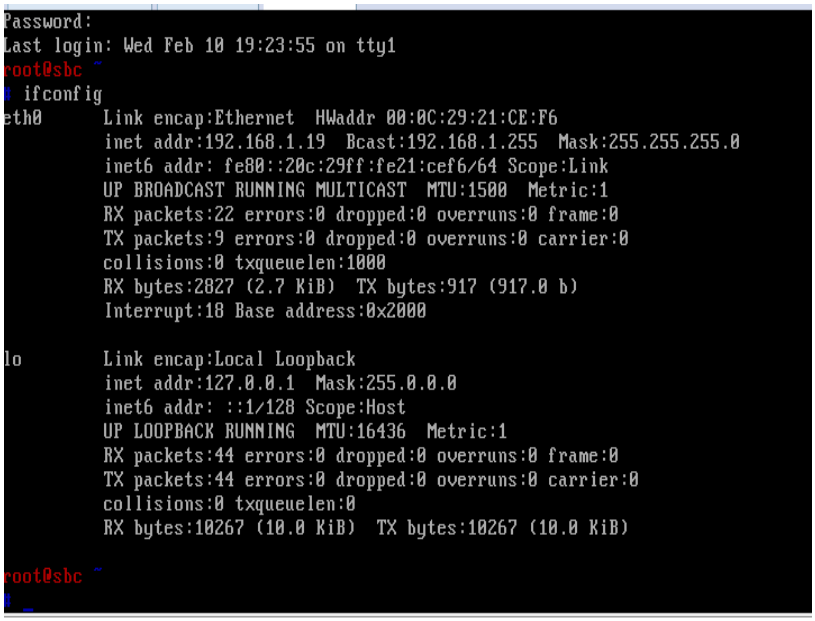
3.4.3.3. *Comprobación operatividad servidor dhcp al SBC*

Para ve si hay conexión con SBC con el servidor dhcp verificar que en el SBC que IP tenemos en el equipo.

Para la verificación que IP tenemos vamos a utilizar el comando ifconfig.

Ifconfig: Muestra los contadores de errores en las interfaces Ethernet.

FIGURA Nº 29: Prueba SBC



Realizado por: Chicaiza Gabriel, Escobar Javier

Como podemos ver esta imagen el servidor dhcp hecho en Centos nos a dado la ip 192.168.1.19.

3.4.3.4. *Comprobación operatividad del SBC modo Grafico*

En esta parte comprobaremos la conexión SBC en modo grafico utilizando un navegador web, para esto nos figamos la IP que nos dio nuestro servidor dhcp la cual es 192.168.1.19 esta IP colocamos en la parte superior del navegador para ver si podemos ingresar en modo grafico al SBC.

FIGURA Nº 30: Comprobación modo gráfico

Realizado por: Chicaiza Gabriel, Escobar Javier

Nota; Cuando utilizamos el servidor dhcp la IP del SBC puede cambiar por eso primero debemos verificar en el SBC que IP tenemos para poder conectarnos en modo gráfico.

Como podemos observar la conexión fue exitosa y podemos comenzar la prueba del SBC.

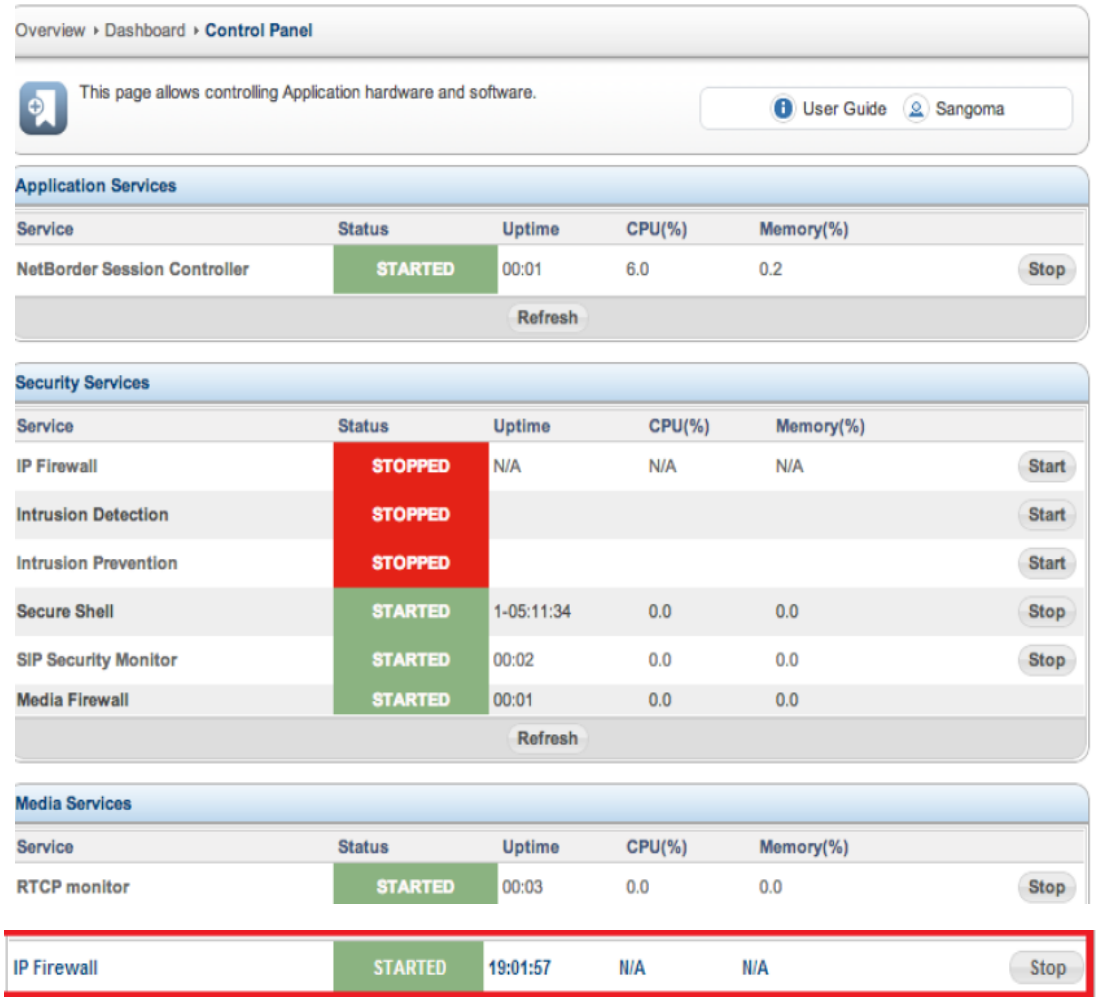
3.4.3.5. *Comprobación operatividad del SBC modo Grafico*

En esta parte vamos a comprobar los servicios del SBC que estén correctamente funcionando.

Panel de Control SBC

Debido a que el servicio de Session Border Controller son los servicios principales de la aplicación, otros servicios se activan automáticamente con él depende de cómo este configurado el servicio. Para comprobar el estado de sus perfiles SIP nos vamos a información general- panel de control- Estado SIP.

FIGURA Nº 31: Servicios Activados



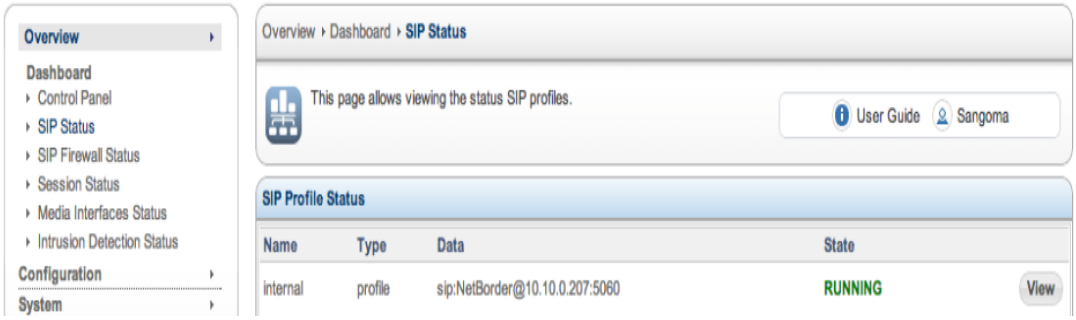
Realizado por: Chicaiza Gabriel, Escobar Javier

En esta ventana observaremos los servicios activados que están funcionando normalmente. Ya que este panel de control es utilizado para iniciar o detener los servicios del SBC.

3.4.3.6. *Comprobación operatividad SIP Status*

Este comprueba si está corriendo correctamente tenemos que observar la palabra running es que el servicio esta iniciado.

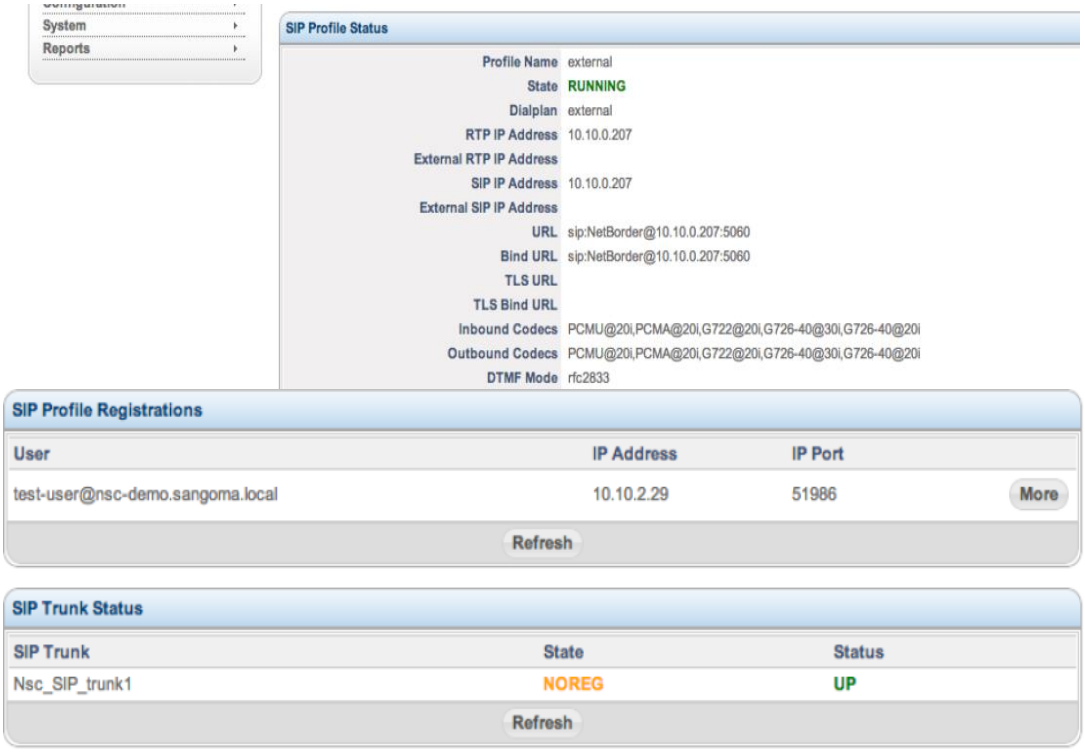
FIGURA Nº 32: SIP Status



Realizado por: Chicaiza Gabriel, Escobar Javier

A continuación hacemos clic en Ver para poder ver más detalles de sus perfiles, incluyendo el estado de las líneas trunk SIP y los registros SIP.

FIGURA Nº 33: SIP Status

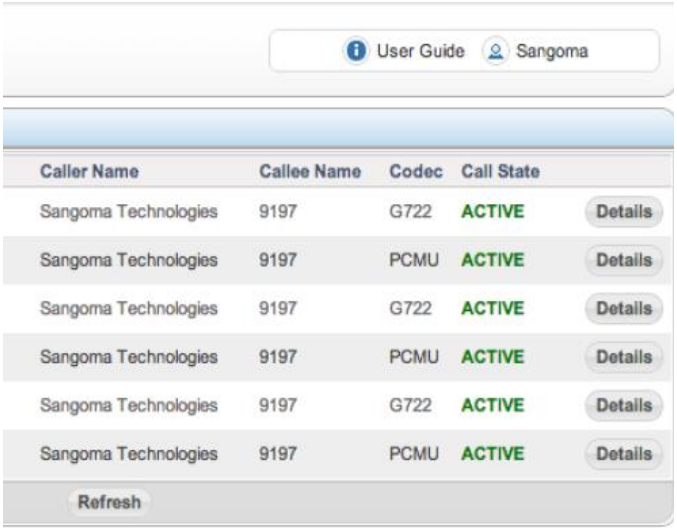


Realizado por: Chicaiza Gabriel, Escobar Javier

3.4.3.7. *Comprobación operatividad Estados de la Sesión SBC*

Para comprobar las sesiones activas (llamadas activas) y sus detalles, permite observar la información general – panel de control- sesión estado.

FIGURA Nº 34: Session Status



Realizado por: Chicaiza Gabriel, Escobar Javier

CONCLUSIONES

- La información obtenida a través de los distintos medios bibliográficos fue muy abundante pero siempre hay que tener en cuenta la confiabilidad de la fuente, la mayoría de la información obtenida fue muy útil ya que no permitió desarrollar de la mejor manera este proyecto, con esta se obtuvo conocimientos nuevos y actualizados para fortalecer experiencias y aportar muchos beneficios en el desarrollo de la vida profesional.

- En la implementación del tema de tesis ha facilitado incrementar la experiencia del uso Session Border Controller y encriptamiento de paquetes se logró cumplir con los objetivos principales de este proyecto, con lo que el laboratorio podrá difundir y optimizar los servicios que brinda el sistema VoIP y palpar la realidad en el tema de seguridad y la importancia que tiene el aplicar las políticas de cada una de las instituciones, a través del trabajo practico en el laboratorio de red.

- Se podrá brindar una mejor seguridad ya que ayudará hacer uso de la opción de consulta en línea, lo que les permite conocer a la red de acceso de un proveedor de servicios y una red troncal para dar servicio a los clientes residentes, empresariales, departamentales e instituciones.

RECOMENDACIONES

- Cuando se vaya a elegir un hardware para ordenadores, es importante realizar un estudio de la infraestructura de hardware a nivel de servidores con que cuenta su organización; con el fin de definir parámetros determinantes en la elección del software de virtualización de ordenadores.

- Para acceder al Session Border Controll el usuario debe pedir autorización al departamento encargado, con el fin de establecer la red de comunicación.

- El personal autorizado para utilizar este software debe contar previamente con una capacitación acerca de Session Border Controller (SBC) y encriptación e paquetes aplicada en la seguridad del laboratorio de red, para manipular correctamente el sistema.

- Se cuenta un manual de usuario en caso que se encuentren algún conflicto de Instalación y configuración del Servidor Dhcp y Session Border Controller para su mejor funcionamiento de servicio.

GLOSARIO

- **Botnets**

  Es un conjunto de robot informatice que se ejecuta de manera automática infectando a todos los servidores que estén conectados a la red.

- **B2BUA (Back-to-Back)**

  Es una aplicación para controlar llamadas entre usuarios SIP, mantiene el estado de las llamadas y las mantiene para conseguir información sobre caída de un proveedor SIP.

- **CAC (Call Admission Controll)**

  Se utiliza para asegurar o mantener un cierto nivel de calidad de audio en redes de comunicación de voz.

- **Firewall**

  Es un Sistema de seguridad de la red, ya sea en hardware o software, que controla el tráfico de la red entrante y saliente basada en un conjunto de reglas.

- **Hacker**

  Persona con grandes conocimientos de información que se dedica a acceder ilegalmente a sistemas informáticos ajenos y manipularlos.

- **IP**

  Se trata de un estándar que se emplea para el envío y recepción de información mediante una red que reúne paquetes commutados.

- **Phishing**

  Es un método utilizado por los delincuentes cibernéticos para estafar y obtener información confidencial de forma fraudulenta como puede ser una contraseña o información detallada sobre sus tarjetas de crédito.

- **Nat Tranversal**

  Es un término aplicado a las técnicas que establecen y mantienen conexiones en redes utilizando protocolos TCP/IP que atraviesan el Gateway.

- **TRIP**

  Protocolo de dominio interadministrativa basada en políticas para la publicidad de la accesibilidad de los destinos de telefonía entre servidores de localización.

- **VOIP**

  Es una tecnología que proporciona la comunicación de voz y sesiones multimedia.

- **VLAN**

  Es un método para crear redes lógicas independientes dentro de una misma red física.

- **Vishing**

  Es una táctica de fraude electrónico en el que los individuos son engañados para que releven la información personal o financiera.

BIBLIOGRAFÍA

Bibliografía citada

- **ORTEGA, Gabriel,ALZORRIZ, Ignacio,RUIZ,Elio y CASTRO,Manuel . 2014.** Procesos y herramietnas para la seguridad de red. Madrid : s.n., 2014.
- **NADREU,fernando,PELLAGERO, Izaskun y LESTA, Amaia. 2006.** Fundamento y Apliaciones de Seguridad. Barcelona, España : MARCOBO S.S, 2006.
- **CARMONA SUARES, Edgar Javier y RODRIGUEZ SALINAS, Elisabeth. 2009.** Tecnología de la infomación y la comunicación ambientes web para las calidad educativa. 2009.
- **MORO Vallina. 2013.** Infestructura de redes de datos y sistemas de telefonía. 2013.
- **CABALLAR, Jose Antonio. 2013.** VoIP telefonía de internet. España : Thomson Editores Spain Paraninfo S.A, 2013.
- **SERRANO SANTOYO, Arturo, CABRERA FLORES, Mayer, MARTINEZ, Evelio y GARIBAY RUIZ, Julio. 2010.** Digitalizacion y Convergencia Global. s.l. : CONVER-GENTE, 2010.
- **HUIDOBRO MOYA, José Manuel y ROLDAN MARTINEZ, David. 2006.** TEcnología VoIP y telefonía IP. Mexico : Alfaomega Grupo editor, Mtxico, 2006.
- **HARDWICK, Jon. 2005.** Session borde controllers. 2005.
- **GARRE DEL OLMO, Carlos, SANCHEZ CAMPOS, Alberto y MARTÍN DE DIEGO, Isaac. 2012.** PRincipios de la seguridad informatica para usuarios. Madird : DYKINSON, S.L. Meléndez Valdés, 61-28015 Madrid, 2012.

Bibliografía Consultada

- **ARIAS, fidias. 2006.** EL proyecto de Invetigación guía para su elaboración. 2006.
- **AVILA BARAY, Hector Luis. 2006.** Introducción a la metodología de la investigación. 2006.
- **BERNAL TORRES, Cesar Ausgusto. 2006.** Metodología de la Investigación para administración, económica, humanidades y ciencias sociales. 2006.
- **CANALLAR, José Antonio. 2007.** VoIP la telefonía de internet . 2007.
- **EMERGENCIA, COORDINACION DE. 2007.** Redes telecomunicaciones. 2007.
- **GARCÉS, Hugo. 2000.** Investigación científica. Quito : Abya-yala, 2000.
- **JON Hardwick. 2005.** Seccion border controller-Enabling the VoIP Revolutation. 2005.
- **LEDESMA, MArtin e SEPÚLVEDA, Patricio. 2013.** Metodología de la investigacion. 2013.
- **LEIVA, Francisco. 2001.** Nociones de la Metodología de la investigación . 2001.
- **MORA LEDESMA, Martin y SEPULVEDA Patricio. 1999.** Metodología de la investigación. 1999.
- **RODRIGUEZ MOGUEL, Erneto,A. 2005.** Metodología de la invetigación. México : s.n., 2005.
- **TAMAYO, Mario. 1999.** La Investigación. 1999.

- **VALLINA, MORO. 2013.** Infestructuras de redes de datos u sistemas de telefonía. s.l. : Paraninfo S.A, 2013.

Bibliografía Electrónica Digital

- **GIL Marcel. 2015.** El ABC del SBC: definición, Características y ventajas. [En línea] 06 de 04 de 2015. [Citado el: 25 de 05 de 2015.] http://blog.teldat.com/?tag=session-border-controller&lang=es.
- **GRETEL, Abdales. 2007.** Encriptación de Paquetes. [En línea] 24 de 09 de 2007. [Citado el: 25 de 05 de 2015.] https://www.google.com.ec/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0CBwQFjAA&url=http%3A%2F%2Fencripdedatos.blogspot.com%2F&ei=pI1jVbq3IM3jsATIv4PgBA&usg=AFQjCNGNMRdD-r0G22haPAyh42w-4t4elA.
- **MAYR, Randolf. 2015.** VoIP y Seguridad. [En línea] 05 de 05 de 2015. [Citado el: 25 de 05 de 2015.] http://blog.teldat.com/?p=448&lang=es.
- **ORTEGA ACEVES, Juan Israel. 2007.** Seguridad en la VoIP (VoIP sobre IP). [En línea] 01 de 2007. [Citado el: 26 de 11 de 2015.] http://www.enterate.unam.mx/Articulos/2007/enero/voip.htm.
- **PORTILLO, Susana. 2012.** Historia de la seguridad infomática. [En línea] 6 de 08 de 2012. [Citado el: 23 de 04 de 2015.]
- **RAMÍREZ ARGÜRO, José. 2010.** Seguridad en la VoIP. [En línea] 08 de 07 de 2010. [Citado el: 26 de 11 de 2015.] http://www.magazcitum.com.mx/?p=630#.Vlep73YvfIU

- **TEGNOLOGÍA, KANVERNA. 2015.** Amenazas para la Seguridad VoIP. [En línea] 04 de 05 de 2015. [Citado el: 25 de 05 de 2015.] http://www.3dgames.com.ar/Noticias/10033.amenazas-para-la-seguridad-voip-watchguard.

ANEXOS