

Trabajo Fin de Grado
Grado en Ingeniería de las Tecnologías de
Telecomunicación

Mejora de la accesibilidad y seguridad del sistema de
telefonía del Departamento de Ingeniería Telemática

Autor: Laura Muñoz Parejo

Tutor: Juan Manuel Vozmediano Torres

Dep. de Ingeniería Telemática
Escuela Técnica Superior de Ingeniería
Universidad de Sevilla

Sevilla, 2017



Trabajo Fin de Grado
Grado en Ingeniería de las Tecnologías de Telecomunicación

Mejora de la accesibilidad y seguridad del sistema de telefonía del Departamento de Ingeniería Telemática

Autor:
Laura Muñoz Parejo

Tutor:
Juan Manuel Vozmediano Torres
Profesor titular

Dep. de Ingeniería Telemática
Escuela Técnica Superior de Ingeniería
Universidad de Sevilla
Sevilla, 2017

Trabajo Fin de Grado: Mejora de la accesibilidad y seguridad del sistema de telefonía del Departamento de Ingeniería Telemática

Autor: Laura Muñoz Parejo
Tutor: Juan Manuel Vozmediano Torres

El tribunal nombrado para juzgar el Proyecto arriba indicado, compuesto por los siguientes miembros:

Presidente:

Vocales:

Secretario:

Acuerdan otorgarle la calificación de:

Sevilla, 2017

El Secretario del Tribunal

A mi abuelo

Agradecimientos

En primer lugar, quería dar las gracias a Vanesa Barrantes, mi profesora particular de Matemáticas, Física y Química durante el instituto. Gracias a ella hoy estoy donde quiero estar. Jamás se me había pasado por la cabeza estudiar Teleco, hasta que ella me aconsejó y me hizo cambiar mi idea inicial de estudiar el Grado de Química. Cuatro años después, solo puedo agradecerle que me ayudase a tomar una de las mejores decisiones de mi vida. Cada día que pasa estoy más orgullosa de haber tomado este camino, estoy más enamorada de mi carrera, de mi especialidad, de las cosas que hago, de las que aprendo y de las que imagino que puedo llegar a hacer.

También quiero agradecer el apoyo recibido por los profesores de CIENCIAS de mi instituto, especialmente a Sagrario Flores y Ramón Encinas, que nunca dejaron de animarme y preocuparse por mí aún años después de irme. Sagrario siempre ha sido para mí un ejemplo de mujer a seguir, no solo por su profesionalidad sino también por su carácter, fortaleza y forma de ser.

Por supuesto no puedo olvidarme de Juan Manuel Vozmediano, mi tutor. Primero, quiero agradecerle que aceptase tutelarme en este proyecto, porque desde que asistí a la primera clase de su asignatura en 2º de carrera supe que tenía que ser él quien me tutelara el proyecto. Asimismo, quiero darle las gracias por la paciencia que ha tenido conmigo, por sus consejos, por preocuparse por mí, por hacerme leer y ver series en versión original para aprender inglés, y por todo lo que me ha enseñado sin importarle las horas que le ha llevado.

Tampoco me puedo olvidar de mis padres y mi hermana. Es a ellos a quienes, principalmente, debo este proyecto por su apoyo incondicional, por impedir que tire la toalla, por enseñarme a ser cada día más fuerte y sobre todo, por hacer posible que haya estudiado fuera de casa con el esfuerzo económico que ello supone. GRACIAS. Igualmente, quiero agradecer al resto de la familia que nunca dejen de creer en mí, incluso cuando ni yo misma creo. Y, especialmente, quiero darle las gracias a mi tía, Esther Muñoz, por sus magníficos consejos que siempre me ayudan a tomar buenas decisiones.

A mis amigas, el *#CuartetoChicasTeleco* por el apoyo emocional que siempre me han brindado y por hacer de estos 4 años la mejor experiencia de mi vida. Solo puedo decirles gracias, gracias por esas cosas que no se pueden contar, por todo lo que hemos vivido y evidentemente, por todo lo que nos queda por vivir.

A mis amigas de toda la vida, Ana Belén e Isa.

Finalmente, agradecer el apoyo y compenetración de mi grupo de trabajos de clase, el *#TrioTelematica*. A *#ElCica* por integrarme rápidamente en su equipo de trabajo durante mis prácticas, por permitirme vivir esa gran experiencia y por enseñarme a pensar de forma diferente. También a todos los profesores de la ETSI que me han dado clase, concretamente, a los de Telemática por todo lo que he aprendido con ellos.

GRACIAS

*Laura Muñoz Parejo
Sevilla, 2017*

Este proyecto se desarrolla en el Departamento de Ingeniería Telemática de la Escuela Superior de Ingenieros de Sevilla. Se centra en la mejora de la accesibilidad al sistema de telefonía IP del Departamento, así como en la adición de seguridad en los elementos que componen dicho sistema. Por ello, tras un análisis previo de las vulnerabilidades que puede sufrir la tecnología VoIP y sus componentes, se han llevado a cabo las siguientes modificaciones en el sistema de telefonía: reconfiguración del servidor de forma que permita a las extensiones SIP ser accesibles desde el exterior; configuración NAT en el router frontera del Departamento, permitiendo la traducción de direcciones de los puertos de señalización SIP y audio RTP establecidos en el servidor; e instalación y configuración de herramientas basadas en **iptables**, que impiden el acceso a usuarios no autorizados.

Durante el desarrollo del proyecto se han realizado tareas de monitorización en la red IP del Departamento con las herramientas **wireshark** y **sngrep**. El uso de éstas ha permitido la detección de fallos en el establecimiento de las llamadas y la detección de tráfico no deseado en la red, lo que ha permitido tomar medidas al respecto. También se ha analizado la robustez de la configuración del servidor de telefonía gracias a la herramienta **SIPVicious**.

Finalmente, con la mejora de la accesibilidad, se permite que los miembros del Departamento puedan acceder al sistema de telefonía de forma segura con su mismo número de extensión desde cualquier sitio con sólo disponer de un acceso a Internet.

Abstract

This project is developed in the Engineering Telematic Department of the Engineers School of Seville. It focuses on improving the accessibility to the IP telephony system of the Department, as well as on adding security to the elements that integrate the system. Therefore, after a previous analysis of the vulnerabilities that can suffer VoIP technology and its components, the following modifications have been made in the telephone system: reconfiguration of the server in a way that permits the SIP extensions to be accessible from the outside; NAT configuration on the Department's router border, allowing address translation of the SIP signaling ports and RTP audio set on the server; and installation and configuration of tools based on **iptables**, which prevent access to unauthorized users.

During the development of the project, monitoring tasks have been carried out in the IP network of the Department with tools like **wireshark** and **sngrep**. These have allowed the detection of failures in the establishment of calls and the discovery of unwished traffic in the network, which have made possible to act on this matter. Telephony server configuration robustness has been also analyzed thanks to the **SIPVicious** tool.

Finally, with the improvement of accessibility, members of the Department can access to telephone system securely with the same extension number from anywhere only with an Internet access.

| | |
|---|--------------|
| Agradecimientos | ix |
| Resumen | xi |
| Abstract | xiii |
| Índice | xv |
| Índice de Figuras | xviii |
| Índice de Tablas | xxi |
| 1 Introducción | 1 |
| 1.1 <i>Introducción</i> | 1 |
| 1.2 <i>Motivaciones y objetivos</i> | 3 |
| 2 Planteamiento Del Problema | 5 |
| 2.1 <i>Antecedentes</i> | 5 |
| 2.2 <i>Procedimiento de arranque de los Teléfonos IP</i> | 7 |
| 2.3 <i>Procedimiento de apertura de puerta</i> | 8 |
| 2.4 <i>Plan de numeración</i> | 9 |
| 2.5 <i>Red IP del Departamento</i> | 11 |
| 2.6 <i>Escenario</i> | 13 |
| 2.7 <i>Problemas</i> | 14 |
| 2.7.1 <i>Escaneo de puertos</i> | 14 |
| 2.7.2 <i>Teléfonos que no dejan de sonar</i> | 15 |
| 2.7.3 <i>Tráfico no deseado en la red</i> | 15 |
| 2.7.4 <i>Llamadas maliciosas</i> | 15 |
| 3 Análisis De Vulnerabilidades | 17 |
| 3.1 <i>Seguridad en los componentes del sistema de telefonía</i> | 17 |
| 3.1.1 <i>Terminales</i> | 18 |
| 3.1.2 <i>Red</i> | 18 |
| 3.1.3 <i>Servidor de VoIP</i> | 19 |
| 3.1.3.1 <i>Seguridad en la configuración del servidor de VoIP</i> | 20 |
| 3.1.3.2 <i>Seguridad en el perímetro del servidor de VoIP</i> | 21 |
| 3.1.3.3 <i>Seguridad integrada en el servidor de VoIP</i> | 21 |
| 3.2 <i>Ataques SIP</i> | 21 |
| 3.2.1 <i>Secuestro de registro</i> | 22 |
| 3.2.2 <i>Secuestro de sesión</i> | 22 |
| 3.2.3 <i>Abandono de sesión</i> | 22 |
| 3.3 <i>Detección de ataques al sistema de telefonía</i> | 22 |
| 3.4 <i>Recomendaciones</i> | 23 |

| | | |
|-------------------------|--|-----------|
| 4 | Solución Adoptada | 25 |
| 4.1 | <i>Accesibilidad del servidor de VoIP</i> | 25 |
| 4.2 | <i>Adición de seguridad integrada en el servidor de VoIP</i> | 26 |
| 4.2.1 | Fail2ban | 26 |
| 4.3 | <i>Adición de seguridad en el perímetro del servidor de VoIP</i> | 27 |
| 4.3.1 | Cortafuegos de aplicación | 27 |
| 4.3.2 | Cortafuegos de red | 28 |
| 4.4 | <i>Adición de seguridad en la configuración del servidor de VoIP</i> | 29 |
| 4.4.1 | Configuraciones seguras | 29 |
| 4.4.2 | Cambio de contraseña de los teléfonos IP | 30 |
| 4.4.3 | Modificación del plan de extensiones | 30 |
| 5 | Implementación | 33 |
| 5.1 | <i>Traducción de direcciones (NAT)</i> | 33 |
| 5.1.1 | Configuración NAT en Asterisk | 34 |
| 5.1.1.1 | Configuración de extensiones | 34 |
| 5.1.1.2 | Configuración del servidor | 35 |
| 5.1.2 | Problema de audio | 36 |
| 5.2 | <i>Fail2ban</i> | 38 |
| 5.3 | <i>Cortafuegos</i> | 38 |
| 5.3.1 | Cortafuegos de aplicación | 38 |
| 5.3.2 | Cortafuegos de red | 42 |
| 5.4 | <i>Establecimiento de las configuraciones seguras</i> | 44 |
| 5.5 | <i>Cambio de contraseña de los teléfonos IP</i> | 45 |
| 5.6 | <i>Creación de extensiones para el nuevo plan</i> | 46 |
| 6 | Problemas Frecuentes | 47 |
| 6.1 | <i>Se ha hecho NAT en el servidor Asterisk y no hay audio</i> | 47 |
| 6.2 | <i>La aplicación de telefonía no se registra</i> | 48 |
| 6.3 | <i>Ha introducido mal la contraseña de la cuenta SIP y no puedo registrarse</i> | 48 |
| 6.4 | <i>No puede registrar su extensión desde una de sus subredes locales</i> | 49 |
| 6.5 | <i>Cuando inicia una llamada, al principio recibe audio del otro extremo pero después no</i> | 49 |
| 6.6 | <i>Tiene un softphone que no deja de sonar en una subred con direccionamiento público</i> | 50 |
| 6.7 | <i>Guía de pasos a seguir ante un problema en el sistema de telefonía IP</i> | 50 |
| 6.7.1 | Guía de resolución de problemas de tráfico SIP | 50 |
| 6.7.2 | Guía de resolución de problemas de tráfico RTP | 51 |
| 7 | Conclusiones | 53 |
| 7.1 | <i>Conclusiones</i> | 53 |
| 7.2 | <i>Líneas de continuación</i> | 54 |
| 7.2.1 | IPSET | 54 |
| 7.2.2 | Autenticación basada en dos factores | 56 |
| 7.2.3 | Cifrado del audio RTP | 57 |
| ANEXOS | | 61 |
| Índice de Anexos | | 63 |
| ANEXO A. | Guía De Instalación De Fail2ban | 65 |

| | | |
|--------------------|------------------------------------|-----------|
| ANEXO B. | Configuración De Softphones | 71 |
| ANEXO C. | SIPVicious | 89 |
| Referencias | | 94 |

ÍNDICE DE FIGURAS

| | |
|--|----|
| Figura 1: Esquema básico del sistema de telefonía del Departamento | 5 |
| Figura 2: Torres de protocolos del servidor Asterisk | 6 |
| Figura 3: Tarjeta de comunicaciones Sangoma | 7 |
| Figura 4: Red IP del Departamento de Ingeniería Telemática | 12 |
| Figura 5: Esquema básico de la arquitectura de red del Departamento | 13 |
| Figura 6: Esquema básico del nuevo sistema de telefonía del Departamento | 14 |
| Figura 7: Componentes clave a proteger en un sistema de telefonía IP | 17 |
| Figura 8: Cortafuegos de la red del Departamento | 27 |
| Figura 9: Camino que sigue un paquete IP en el cortafuegos de red | 28 |
| Figura 10: Esquema básico de la arquitectura de red del Departamento | 33 |
| Figura 11: Configuración NAT extensiones | 35 |
| Figura 12: Configuración NAT del servidor | 36 |
| Figura 13: Mensaje SDP | 37 |
| Figura 14: Ausencia de Audio en Linphone | 37 |
| Figura 15: Algoritmo del cortafuegos de aplicación | 39 |
| Figura 16: Nuevo camino que sigue un paquete IP en el cortafuegos de red | 43 |
| Figura 17: Elastix. Configuraciones seguras | 44 |
| Figura 18: Elastix. Type peer | 45 |
| Figura 19: Asterisk. Ajuste de puertos de audio | 48 |
| Figura 20: Problema STUN. Doble información de direccionamiento | 49 |
| Figura 21: Torre del plano de control de un sistema de telefonía de autenticación basada en dos factores | 57 |
| Figura 22: Torre del plano de usuario de un sistema de telefonía con cifrado de audio | 58 |
| Figura 23: Prueba de funcionamiento Fail2ban y softphone Linphone | 69 |
| Figura 24: Dirección IP maliciosa bloqueada en la cadena fail2ban-Asterisk creada por fail2ban | 69 |
| Figura 25: Fichero Fail2ban de registro | 70 |
| Figura 26: Logo de Linphone | 71 |
| Figura 27: Logo de CSipSimple | 71 |
| Figura 28: Linphone escritorio. Asistente de configuración | 72 |
| Figura 29: Linphone escritorio. Usar cuenta SIP | 72 |

| | |
|--|----|
| Figura 30: Linphone escritorio. Configuración de una cuenta | 73 |
| Figura 31: Linphone escritorio. Configuración de cuenta finalizada | 73 |
| Figura 32: Linphone escritorio. Preferencias | 74 |
| Figura 33: Linphone escritorio. Configuración | 74 |
| Figura 34: Linphone escritorio. Ajustes de una cuenta SIP | 75 |
| Figura 35: Linphone escritorio. Autenticación necesaria | 75 |
| Figura 36: Linphone escritorio. Configuración de red | 76 |
| Figura 37: Linphone escritorio. Códecs | 76 |
| Figura 38: Linphone Smartphone. Asistente de configuración | 77 |
| Figura 39: Linphone Smartphone. Configuración de una cuenta | 78 |
| Figura 40: Linphone Smartphone. Cuenta registrada | 79 |
| Figura 41: Linphone Smartphone. Menú principal | 79 |
| Figura 42: Linphone Smartphone. Ajustes | 80 |
| Figura 43: Linphone Smartphone. Ajuste de cuenta | 80 |
| Figura 44: Linphone Smartphone. Ajustes de red | 81 |
| Figura 45: CSipSimple. Añadir cuenta | 82 |
| Figura 46: CSipSimple. Asistentes de configuración | 82 |
| Figura 47: CSipSimple. Configuración de una cuenta SIP | 83 |
| Figura 48: CSipSimple. Cuenta registrada | 84 |
| Figura 49: CSipSimple. Marcador telefónico | 84 |
| Figura 50: CSipSimple. Ajustes | 85 |
| Figura 51: CSipSimple. Configuración Sencilla | 85 |
| Figura 52: CSipSimple. Configuración de red | 86 |
| Figura 53: CSipSimple. Llamada | 87 |
| Figura 54: Logo de SIPVicious | 89 |
| Figura 55: SIPVicious-svmap | 91 |
| Figura 56: SIPVicious-svwar sin opciones | 91 |
| Figura 57: SIPVicious-svwar | 92 |
| Figura 58: SIPVicious-svcrack | 92 |
| Figura 59: SIPVicious una vez implementada la solución adoptada de este proyecto | 92 |

ÍNDICE DE TABLAS

| | |
|---|----|
| Tabla 1: Asignación de prefijos en el plan de numeración | 10 |
| Tabla 2: Distribución de extensiones SIP del Departamento | 10 |
| Tabla 3: Subredes del Departamento de Ingeniería Telemática | 11 |
| Tabla 4: Parámetro type | 29 |
| Tabla 5: Nuevo plan de extensiones SIP del Departamento | 31 |
| Tabla 6: Programas SIPVicious | 90 |

1 INTRODUCCIÓN

*Lo importante es no dejar de hacerse preguntas.
- Albert Einstein -*

1.1 Introducción

La **VoIP** (*voice over IP*) es el conjunto de normas, protocolos y recursos (en otras palabras: la tecnología) que permite transmitir el tráfico de voz sobre el protocolo IP en lugar de explotar la red telefónica pública conmutada (RTC o PSTN, siglas de *Public Switched Telephone Network*). Mientras que la red conmutada envía la señal de voz en forma digital empleando conmutación de circuitos, la telefonía IP la envía de forma digital en paquetes de datos; de este modo, al estar basada en el protocolo IP, esta tecnología permite integrar en una misma red las comunicaciones de voz y datos.

El primer antecedente de VoIP fue el protocolo de voz en red (NVP, siglas de *Network Voice Protocol*), creado por el ingeniero israelí Danny Cohen en 1973 para ARPANET como parte de un simulador de vuelo de su creación. En las siguientes décadas la tecnología siguió desarrollándose de forma experimental, sin despertar excesivo interés por parte de la industria por los inconvenientes que presentaba: desconexiones, latencia y transmisión irregular de los datos.

No fue hasta 1995 que una compañía comercial (curiosamente también israelí), VocalTec, sacó por primera vez al mercado una solución basada en la tecnología VoIP, ofreciendo a las empresas un ahorro en sus costes de telefonía. La plataforma no estaba exenta de los inconvenientes mencionados y tenía el inconveniente adicional de que sólo funcionaba entre clientes de la misma plataforma. Aun así, esto supuso el pistoletazo de salida para que otras grandes empresas, entre otras los gigantes Intel y Microsoft, encabezaran un esfuerzo por estandarizar, mejorar y popularizar esta tecnología. Algunas compañías de telecomunicaciones de EE.UU. solicitaron en 1996 al Congreso la prohibición de la telefonía por Internet, lo que muestra hasta qué punto VoIP pasó de ser una tecnología experimental a una importante competencia.

Rápidamente, con el auge de Internet, comenzaron a perfeccionarse los protocolos aplicados y la estandarización de los sistemas de control de la calidad de la voz. Esto mejoró la calidad de la voz enviada y la rapidez de las transmisiones, permitiendo así su generalización.

Hoy en día existen muchos dispositivos que resuelven el problema de la digitalización y codificación de la voz, además de la conversión de medios y conmutación que permiten integrar las llamadas en las redes de telefonía convencional. Para ello, Digium presenta una solución a través de su aplicación Asterisk, cuya

aparición en 1999, junto a la publicación de la especificación del protocolo SIP [RFC2543], marca el comienzo de una nueva década en la que la tecnología se expande y finalmente triunfa en el mercado.

El protocolo SIP (*Session Initiation Protocol*) fue desarrollado por el IETF con la intención de ser el estándar de señalización de sesiones interactivas de usuarios donde intervienen elementos multimedia como video, voz y mensajería instantánea. Su sintaxis es similar a la de los protocolos HTTP y SMTP ya que el protocolo fue diseñado para que la telefonía IP se volviera un servicio más de Internet. Asimismo, existen otros protocolos de señalización para voz sobre IP como H.323 o IAX2. El protocolo IAX2 (segunda versión del protocolo IAX) es de código abierto y es el empleado para el manejo de conexiones VoIP entre servidores Asterisk.

Asterisk es un *software* de código abierto que permite crear aplicaciones y soluciones de comunicaciones multiprotocolo en tiempo real como sistemas de telefonía comercial (conocidos como PBX), distribuidores de llamadas y pasarelas VoIP. En otras palabras, Asterisk permite controlar y gestionar comunicaciones de cualquier tipo, ya sean analógicas, digitales (por medio de líneas troncales) o VoIP (mediante todos los protocolos VoIP que implementa).

Además, este software incluye muchas características que anteriormente sólo estaban disponibles en sistemas propietarios, como buzón de voz, conferencias y distribución automática de llamadas. Igualmente, permite la adición de nuevas funcionalidades con la instalación de módulos concretos, lo que posibilita crear un sistema de telefonía personalizado. La existencia de estos módulos se debe a la naturaleza abierta del código, que facilita al usuario la creación de los mismos.

La complejidad de Asterisk reside en su configuración, ya que requiere el esfuerzo de aprender su lenguaje de programación. Para evitar tener que manejar a la perfección este lenguaje, existen paquetes *software* que facilitan su configuración gracias a una interfaz web. Algunos ejemplos de este tipo de *software* son: Elastix, FreePBX o Trixbox.

Elastix es un *software* de código abierto usado para el establecimiento de comunicaciones unificadas basado en Asterisk, que además ofrece sus propios módulos extra como configuración de fax, facturación, videoconferencias, mensajería instantánea, etc. Está provisto de una interfaz web para llevar a cabo la administración y gestión de todos los servicios que presta.

En los últimos años se ha visto un aumento constante en la popularidad de estos *softwares* basados en la tecnología VoIP; tras más de una década y media de su entrada en el mercado, se puede considerar que esta tecnología ha alcanzado por fin su estado de madurez. Desgraciadamente, como siempre pasa con la aparición de una nueva tecnología, durante su desarrollo no se consideró la seguridad como una prioridad. Sus creadores estaban preocupados principalmente por su costo, funcionalidad y fiabilidad. Además de las propias vulnerabilidades que esto provocó, esta tecnología hereda vulnerabilidades de protocolos de los que depende, e incluso, del propio sistema operativo donde se aloja el servidor.

La seguridad es importante en cada contexto, pero especialmente en este ámbito, cuando se está reemplazando la red de comunicaciones más antigua, más grande y más resistente del mundo.

A lo largo de la historia de esta tecnología se han producido una serie de incidentes debidos a la falta de interés de las empresas por la seguridad en las redes de voz. Un ejemplo claro de esta tendencia se produjo en 2009 cuando una compañía australiana fue atacada por un grupo de ciberdelincuentes. Estos realizaron un total de 11.000 llamadas en menos de 46h a través de la red de voz de la compañía, acumulando una factura de \$ 120.000. Esta cifra clasifica el incidente entre los más costosos de los ataques documentados de fraude en la historia de la tecnología VoIP.

Los riesgos y ataques a la tecnología VoIP se extienden más allá del uso fraudulento (llamadas de pago) o de las escuchas de llamadas. Muchos ataques se centran en los puntos finales de la comunicación. En este caso,

en los teléfonos IP o *softphones*, ya que pueden ser puntos de entrada en la red de datos de la organización.

Además, los sistemas operativos donde se alojan los servidores, los protocolos de los que depende, las aplicaciones e interfaces de gestión de los teléfonos IP y las aplicaciones *softphone* son vulnerables al acceso no autorizado, a ataques de código malicioso y a otros muchos ataques, como los ataques de negación de servicio (DoS).

Otra vulnerabilidad importante en esta tecnología son los protocolos que emplea para la descripción de sesiones y de control de media (protocolo SDP), ya que no proporcionan una adecuada autenticación de usuarios, protección de integridad de extremo a extremo o medidas de confidencialidad en la señalización. De esta forma, un atacante puede capturar los paquetes de señalización de la llamada y usar esa información para suplantar a un usuario, permitiéndole por ejemplo acceder a la configuración del servidor donde podría cambiar el plan de numeración para permitir llamadas a números internacionales bloqueados o acceder al correo de voz.

El envío continuo de mensajes no solicitados también afecta a esta tecnología. El flujo de estos mensajes a través de la telefonía IP puede llevar a la descarga de programas en *softphone* que podrían incluir código malicioso oculto o provocar que los teléfonos suenen constantemente. Esto puede degradar el servicio de telefonía IP obligando a cancelar llamadas o hacer que ciertos equipos VoIP no puedan procesarlas por completo.

Hoy en día se puede afirmar que los motivos por los que se realizan ataques a los sistemas de telefonía IP son, sobre todo, económicos: robo de identidad o información, fraude de llamadas, espionaje o para causar interrupción del servicio.

En definitiva, la tecnología VoIP en la actualidad es una de las tecnologías con más auge en las telecomunicaciones y debemos ser conscientes de que es vulnerable y está expuesta a los mismos riesgos que afrontan diariamente las redes IP.

1.2 Motivaciones y objetivos

En la actualidad, la mayoría de las empresas y oficinas cuentan con sistemas de telefonía IP que permiten la incorporación de nuevas necesidades gracias a *software* como Asterisk.

Las principales ventajas que presenta un sistema de telefonía IP son las siguientes:

- Simplificación de la infraestructura de comunicaciones.
- Integración de diferentes sedes de la organización en un sistema unificado de telefonía.
- **Ahorro de costes:**
 - Reducción de costes de gestión.
 - Llamadas internas gratuitas.
- **Funcionales adicionales:**
 - Plan de numeración integrado.
 - Llamada directa de extensión a extensión sin coste.
 - Gestión centralizada del sistema de telefonía.
 - Operadora automática.
 - Sistema de correo vocal (Voicemail).

Se pretende conseguir la deslocalización de clientes SIP, es decir, permitir que el cliente pueda estar disponible con el mismo número de extensión en cualquier parte del mundo sin más que disponer de un acceso a Internet. Además, la incorporación de mecanismos de seguridad que ello conlleva para evitar los posibles ataques al sistema de telefonía y a los propios usuarios de éste.

Algunas de las principales ventajas de esta nueva funcionalidad son las siguientes:

- Acceso al sistema de telefonía desde fuera de la organización.
- Llamadas gratuitas entre miembros de la organización desde el exterior.
- Acceso a servicios telefónicos corporativos para el trabajador desde su domicilio.
- Disponibilidad 24 horas.

El Departamento de Ingeniería Telemática dispone de un sistema de telefonía IP basado en Asterisk conectado al exterior mediante dos líneas troncales, una RDSI y otra analógica. Este sistema de telefonía IP se ha modificado para que los miembros del Departamento puedan acceder a él a través de Internet, es decir, desde el exterior de la red IP del Departamento.

Este proyecto tiene como fin reconfigurar el servidor de VoIP del Departamento de manera que sea accesible desde el resto de Internet. También, dotar de mecanismos de seguridad que disminuyan e impidan, en la medida de lo posible, los posibles ataques a este servicio para conseguir la deslocalización de clientes SIP.

En esta memoria se describen los paquetes *software* instalados, la gestión de las distintas herramientas que conforman el sistema de telefonía, las pruebas de seguridad realizadas y la configuración de todos los equipos implicados para el correcto funcionamiento del sistema.

2 PLANTEAMIENTO DEL PROBLEMA

Divide cada dificultad en tantas partes como sea factible y necesario para resolverlo.
- René Descartes -

Este capítulo se centra en la descripción del sistema actual de telefonía del Departamento de Ingeniería Telemática de la Escuela Superior de Ingenieros, en la reconfiguración del servidor de VoIP y en los problemas surgidos a posteriori, una vez implementado el cambio, cuya solución también son objetivo de este proyecto.

2.1 Antecedentes

El sistema de telefonía del Departamento de Ingeniería Telemática dispone de un servidor de telefonía IP que funciona como pasarela (*gateway*). Esto permite la conversión de señalización y medios, ya que se encuentra conectado al exterior mediante una línea analógica y una RDSI, y en el interior se cuenta con tecnología SIP. En la siguiente figura se muestra un esquema básico del sistema de telefonía del Departamento.

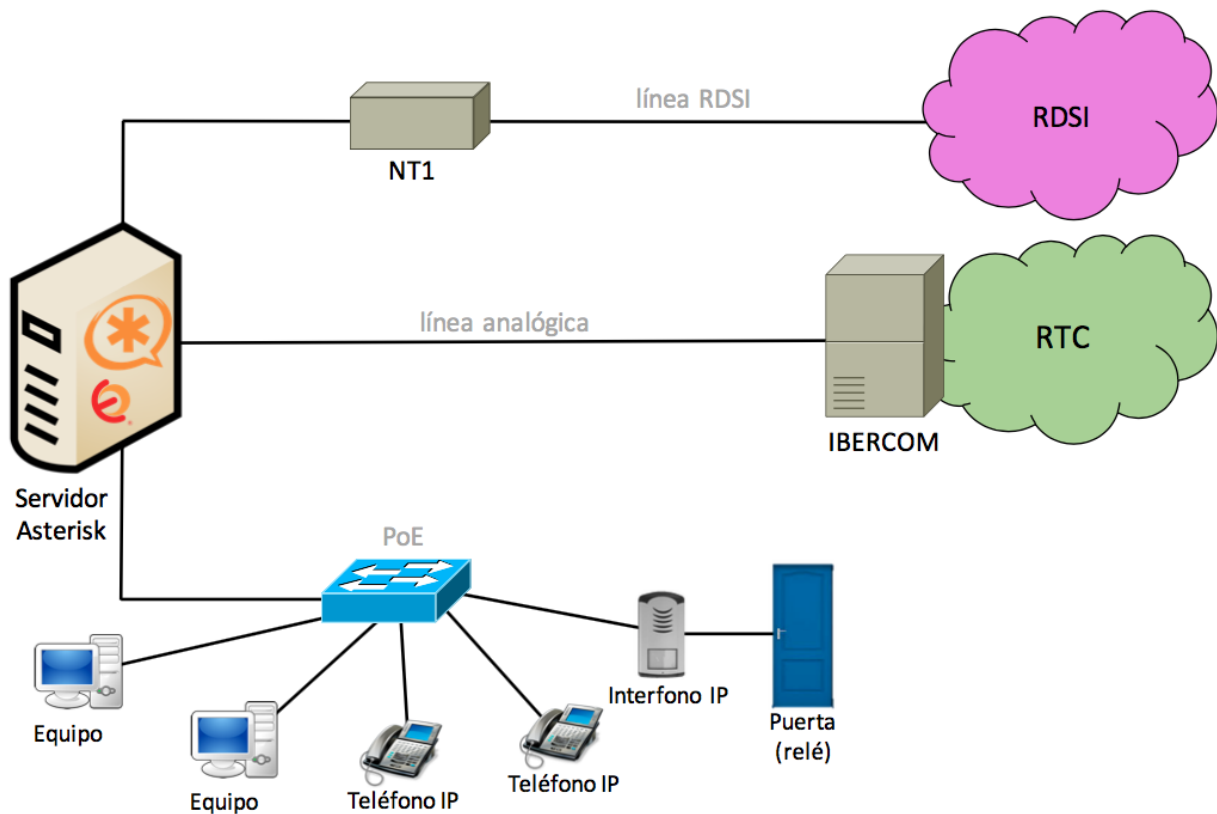


Figura 1: Esquema básico del sistema de telefonía del Departamento

Además, éste dispone de un mecanismo de apertura y cierre de puerta mediante un relé y un interfono IP conectado al servidor de VoIP.

La línea analógica no está conectada directamente al exterior, sino a una central telefónica tipo Centrex¹, contratada por la Universidad de Sevilla y denominada IBERCOM, que conecta con el exterior. El objetivo de IBERCOM es abaratar costes entre las llamadas internas de la Universidad, permitiendo un cierto plan de marcado para distinguir entre llamadas internas y externas. La línea RDSI conecta directamente con el exterior gracias a un NT1.

El servidor de telefonía del Departamento funciona bajo el *software* de Asterisk. Se trata de un *software* libre que trabaja sobre cualquier distribución de Linux. Proporciona funcionalidades de una central telefónica PBX (*Private Branch Exchange*), es decir, permite controlar y gestionar comunicaciones de cualquier tipo, ya sean analógicas, digitales o VoIP.

Gracias al diseño escalable y modular de Asterisk, se puede modificar su comportamiento con la instalación y eliminación de módulos concretos. Esto permite la creación de un sistema de telefonía personalizado. Para evitar tener que manejar a la perfección el lenguaje que usa Asterisk y lo engorroso que es su programación, existen paquetes de *software* que facilitan su uso y configuración gracias a una interfaz web. Además, ofrecen sus propios módulos extra como configuración de fax, videoconferencias, mensajería instantánea, etc. Algunos ejemplos de estos *softwares* son Elastix o FreePBX.

El paquete *software* utilizado en el Departamento es Elastix. Éste funciona sobre una distribución Linux basada en CentOS. Se puede acceder a su interfaz web desde cualquier equipo ubicado en la misma subred que el servidor con Elastix. Para ello, sólo es necesario introducir la dirección IP del servidor en un navegador web y autenticarse debidamente.

El paquete Elastix incluye componentes como: Asterisk para las funcionalidades de Centralita, FreePBX para la configuración de Asterisk de una forma más sencilla vía web, y otros *softwares* de código abierto que proporcionan otro tipo de servicios como, por ejemplo, *Postfix* para el correo electrónico.

Debido al uso del paquete Elastix en el Departamento, de aquí en adelante al servidor de telefonía se le llamará servidor de VoIP, Asterisk, PBX o centralita.

A continuación, se muestran las torres de protocolos del servidor Asterisk:

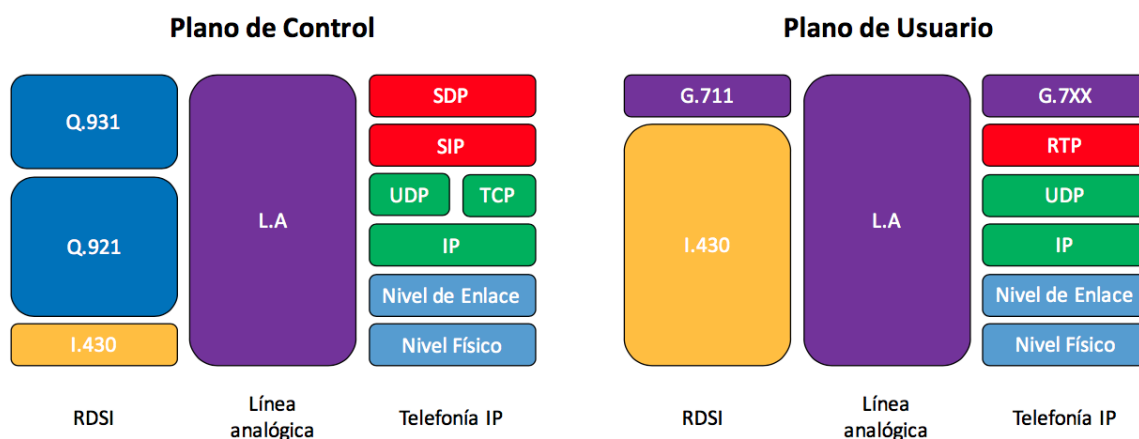


Figura 2: Torres de protocolos del servidor Asterisk

¹ El servicio Centrex (*Central Office Exchange Service*) consiste en proporcionar una centralita virtual, creada por un proveedor de servicios, sobre una central digital pública.

El Departamento de Ingeniería Telemática está compuesto por trece despachos de profesores, una oficina de secretaría, una sala de reuniones, una sala de becarios y una sala de servidores. Dispone de un sistema de cableado estructurado que permite que la red de datos esté distribuida por toda la superficie.

Los teléfonos IP necesitan alimentación. Para evitar utilizar el cable de alimentación de estos, las tomas RJ45 que emplean para conectarse a la red están dotadas de “*Power over Ethernet*” (**PoE**). Estas tomas son alimentadas gracias a un *switch* Cisco, denominado PoE en las figuras, que se encuentra en una sala externa. Las tomas de cada despacho están numeradas de forma que sea fácil averiguar a qué puerto del *switch* están conectadas.

El servidor Asterisk se encuentra en la sala de servidores conectado a una toma Ethernet sin PoE para unirse a la red interna de datos, y a las tomas correspondientes a la línea analógica y a la línea RDSI, que le permiten conectarse con el exterior.

De esta forma, quedan interconectados todos los teléfonos IP, el interfono IP y el servidor Asterisk dentro de la red del Departamento a través del *switch* PoE; y también, hacia el exterior gracias a las líneas analógica y RDSI por medio de una tarjeta de comunicaciones insertada en el propio servidor.

La tarjeta de comunicaciones instalada en el servidor del Departamento es una Tarjeta **Sangoma B700 FlexBRI Hybrid Voice Card** que dispone de cuatro puertos RDSI (BRI) y dos puertos analógicos. Físicamente, en esta tarjeta solo pueden apreciarse dos puertos RDSI y un puerto analógico. Esto es debido a que cada puerto funciona como si fuesen dos gracias a un cable Y. Así, con tres cables Y se consiguen cuatro puertos RDSI y dos puertos analógicos.



Figura 3: Tarjeta de comunicaciones Sangoma

2.2 Procedimiento de arranque de los Teléfonos IP

El Departamento dispone de **teléfonos IP Grandstream GXP1405** que permiten ser configurados de dos formas diferentes: manualmente, mediante interfaz web propia del teléfono; automáticamente, mediante un fichero de configuración especial, vía TFTP/HTTP/HTTPS.

Por motivos de comodidad y simplicidad, los teléfonos se configuran automáticamente mediante un fichero de configuración vía TFTP, en lugar de mediante la interfaz web de cada teléfono.

La interfaz web de Elastix contiene una herramienta denominada “*Endpoint Configurator*” que era capaz de detectar los teléfonos IP Grandstream del Departamento y generar un fichero de configuración para cada uno de ellos, diferenciándolos según sus MAC. Sin embargo, esta herramienta ya no funciona para la

versión Elastix-2.5.0-1 instalada en el Departamento. Por este motivo se posee un script, denominado `reconf.sh`, que genera los mismos ficheros de configuración de los terminales que generaba anteriormente la herramienta.

El sistema de telefonía del Departamento contiene todos los ficheros de configuración de los teléfonos almacenados en el mismo directorio, `/tftpboot/tel` del servidor Asterisk, manteniendo así un orden. El script mencionado anteriormente, como hacía la herramienta “*Endpoint Configurator*”, crea dos ficheros de configuración. Un fichero llamado “`cfgMAC`” binario y otro “`gxpMAC`”, donde “MAC”, se refiere a la dirección MAC² del teléfono en cuestión. El archivo “`cfgMAC`” es el que el teléfono toma para su configuración; y el archivo “`gxpMAC`” es un fichero en texto plano que contiene lo mismo que el fichero “`cfgMAC`” pero de forma legible.

El procedimiento de arranque de un teléfono de la red del Departamento se describe a continuación. Al iniciarse, el teléfono pide, por defecto, su dirección IP al servidor DHCP. Este servidor está configurado para anunciarle, además de la dirección IP asignada a su MAC, la dirección del servidor TFTP y el directorio donde tiene que buscar los ficheros de configuración. Esto es posible gracias a una opción de los servidores DHCP, en concreto, la opción 66.

Así pues, la configuración de los teléfonos IP GXP1405 está totalmente automatizada. Para que el teléfono IP adquiera su configuración, en primer lugar, ha de haberse ejecutado el script `reconf.sh` que permite crear sus ficheros de configuración y, posteriormente, solicitar el fichero “`cfgMAC`” al servidor TFTP. Finalmente, debe reiniciarse para tomar la configuración descrita.

Otra característica de interés de estos teléfonos es que, cuando reciben una llamada, muestran en su pantalla el número de extensión que llama o el nombre de usuario al que pertenece dicha extensión si lo tiene almacenado en memoria. Para ello, el teléfono dispone de una agenda telefónica con todos los usuarios y su extensión correspondiente. Este modelo en concreto permite la obtención vía TFTP/HTTP/HTTPS del fichero XML que contenga la agenda telefónica (*phonebook*). El fichero de agenda telefónica debe ser llamado “`gs_phonebook.xml`” y en el caso del Departamento se encuentra en el directorio `/tftpboot/tel` junto con la configuración de los teléfonos.

2.3 Procedimiento de apertura de puerta

El **interfono IP CyberData**, al igual que los teléfonos, también permite la configuración tanto vía interfaz web, como vía fichero de configuración. El fichero de configuración es un fichero especial XML, descargado de la página web oficial de CyberData y configurado con una adaptación a las necesidades del Departamento.

Al igual que los teléfonos IP, el interfono obtiene su dirección IP y la información necesaria para encontrar su fichero de configuración a través del servidor DHCP. El interfono está configurado, por defecto, para que al arrancar realice la consulta DHCP. Gracias a la opción 150 de este servidor, el interfono obtiene la dirección IP del servidor TFTP donde se encuentra su fichero de configuración. Esta opción es muy similar a la opción 66, empleada por los teléfonos para la obtención de la información de configuración, con la diferencia de que sólo se indica la dirección IP del servidor TFTP y no el directorio dónde se ubica el fichero de

² Ejemplos de nombres de los ficheros de configuración de un teléfono según su MAC podrían ser: `cfg000b82337bc3` y `gxp000b82337bc3`.

configuración. Por este motivo, el fichero de configuración del interfono se encuentra en el directorio /tftpboot/ ya que es el directorio dónde, por defecto, se busca el fichero de configuración.

La puerta del Departamento de Ingeniería Telemática posee un sistema de apertura que funciona gracias a dos relés. Un relé externo controlado por el interfono IP y otro relé interno. El relé interno es el encargado de abrir y cerrar el circuito que controla al relé externo de la puerta. El interfono activa su relé interno cuando tiene establecida una llamada SIP con alguno de los teléfonos del Departamento y se ha marcado un código de “apertura de puerta”. El número de “apertura de puerta” es enviado al interfono como un código DTMF y, si éste es correcto, el interfono cerrará el circuito externo y abrirá la puerta.

En definitiva, el funcionamiento es el siguiente: un usuario llama desde el interfono a una extensión interna del Departamento; el teléfono interno es descolgado y establece una llamada SIP; desde el teléfono interno se tecldea el código de “apertura de puerta”; el interfono lo recibe y activa su relé interno cerrando el circuito y abriendo la puerta.

Además, el interfono dispone de una funcionalidad que permite abrir la puerta mediante el marcado de un “código de seguridad”³ desde el propio interfono. De esta forma, los profesores del Departamento pueden abrir la puerta desde el exterior tecleando el “código de seguridad” en el interfono sin necesidad de usar la tarjeta de la Universidad.

Igualmente, el interfono dispone de una funcionalidad de auto-respuesta de llamadas entrantes. De forma que, si se llama a la extensión 20 (interfono), la llamada será descolgada automáticamente. Esto es muy útil para abrir la puerta desde cualquier sitio siempre que se conozca el número de “apertura de puerta”.

2.4 Plan de numeración

El Departamento se atiene a un **plan de numeración** para el establecimiento tanto de llamadas internas como externas. A continuación, se detallarán la distribución de las extensiones y las reglas de marcado para salir al exterior.

El plan de numeración existente para las llamadas al exterior se organiza en torno a una línea analógica y otra línea RDSI. Como se ha mencionado con anterioridad, la línea analógica no está conectada directamente al exterior, sino a IBERCOM, que conecta con el exterior, mientras que la línea RDSI se encuentra conectada directamente al exterior gracias a un NT1.

La línea analógica con ID: 954 487 384 se usa para atender llamadas entrantes. De manera que, si hay una llamada entrante a este número, saltará una centralita automática a la que habrá que especificarle qué número de extensión es a la que se quiere llamar. Con respecto a la línea RDSI, se tiene contratado un acceso básico (BRI) con ID: 954 467 090. Este acceso básico es utilizado para las llamadas salientes.

No obstante, para salir al exterior, el usuario puede hacerlo por la línea analógica 954 487 384 o por la línea RDSI 954 467 090. Es recomendable que la línea analógica se use lo menos posible, ya que, si se ocupa en llamadas salientes, no podrá establecerse ninguna llamada entrante nueva. La recomendación para salir al exterior es usar preferentemente la línea RDSI y como segunda opción, la analógica. Sin embargo, existe otra posibilidad, en caso de no querer salir por la línea RDSI. Esta opción se denomina “elección automática de línea analógica” y consiste en salir al exterior por la línea analógica. Esta elección de línea es transparente para el

³ El “código de seguridad” debe estar precedido del carácter ‘#’ para que el interfono pueda distinguir entre marcado de “código de seguridad” (precedido de ‘#’) y marcado de extensiones (no llevan ‘#’).

usuario, la realiza la centralita automáticamente.

Todas estas opciones para realizar llamadas al exterior son posibles gracias a la configuración de ciertos prefijos que conforman el plan de marcado.

A continuación, se detallarán los prefijos que usa el Departamento tanto para llamar al exterior como al interior. Los prefijos son los siguientes:

| PREFIJO | DESTINADO A ... |
|-------------------------------------|--|
| 0 | Salida al exterior (analógica y RDSI) |
| 2X 3X 4X | Extensiones SIP |
| 52 | Salida por línea analógica |
| 55 | iptel.org |
| 6XX | Buses RDSI (sin uso actualmente) |
| 9 | Elección automática de línea analógica |

Tabla 1: Asignación de prefijos en el plan de numeración

Para salir al exterior es necesario marcar el prefijo ‘0’. Las llamadas pueden salir al exterior tanto por la línea RDSI como por la línea analógica. No obstante, el servidor de VoIP está configurado para que, preferiblemente, las llamadas salientes lo hagan por la línea RDSI. Un ejemplo sería: “0 955 804 353”.

Los prefijos ‘2X’, ‘3X’ y ‘4X’ están reservados para las extensiones SIP internas. El plan de numeración del Departamento organiza la distribución de estas extensiones de forma que cada profesor tenga una extensión SIP asignada a su teléfono IP. En la siguiente tabla se muestra la distribución de las extensiones:

| EXTENSIÓN | ASIGNADA A ... |
|------------------|--------------------|
| 20 | Puerta |
| 21-33, 35 | Profesores |
| 34, 36-39 | Salas / Secretaria |
| 40 | FAX |

Tabla 2: Distribución de extensiones SIP del Departamento

El prefijo ‘52’ es utilizado para salir al exterior por la línea analógica. Además, IBERCOM necesita recibir el prefijo ‘0’ para salir al exterior. Si no recibe dicho prefijo, considerará que la llamada es interna a la Universidad de Sevilla. Para llamadas internas habría que marcar “52 XXXXX”. Para llamadas externas “520 XXX XXX XXX”.

El prefijo de marcado ‘55’ se emplea para redirigir las llamadas de una extensión SIP interna a una cuenta de un proveedor de servicio VoIP, en este caso iptel.org. El objetivo es que, si el profesor no se encuentra en su despacho pueda contestar a las llamadas con destino a su extensión desde su teléfono móvil. Hoy en día esta funcionalidad no está en uso.

Anteriormente, para la centralita original RDSI (NT2) el prefijo ‘6XX’ estaba destinado al bus RDSI, que contenía tres interfaces S básicos donde se podían conectar teléfonos RDSI adicionales. Hoy, con las características del sistema de telefonía del Departamento no tiene sentido.

Para la opción denominada “elección automática de línea analógica”, el usuario debe simplemente marcar el prefijo ‘9’. Además, al tratarse de la línea analógica, ha de tenerse en cuenta el prefijo ‘0’ de IBERCOM para las llamadas externas. Por tanto, habría que marcar: “9 XXXXX” para las llamadas internas de la Universidad de Sevilla y “90 XXX XXX XXX” para las llamadas externas.

Puede observarse que la longitud del número que sigue al prefijo para las llamadas internas de la Universidad de Sevilla es diferente al usado para las llamadas externas. Esto se debe a que los números internos de la Universidad usan una numeración de sólo cinco dígitos (XXXXX) mientras que las llamadas externas necesitan la numeración normal de 9 dígitos (XXX XXX XXX).

2.5 Red IP del Departamento

La red IP del Departamento de Ingeniería Telemática está organizada en subredes de direccionamiento público y privado.

El Departamento posee un rango de direcciones públicas contiguas desde la dirección 193.147.162.128 hasta la 193.147.162.191 asignadas por la Universidad de Sevilla. Este rango de direcciones, junto con otros rangos de direcciones privadas, componen las 7 subredes del Departamento. A continuación, se muestra una tabla con todas las subredes de éste y su respectivo rango de direcciones:

| NOMBRE SUBRED | DIRECCIÓN DE RED | RANGO DE DIRECCIONES | DIRECCIÓN DE DIFUSIÓN |
|--------------------|--------------------|-----------------------|-----------------------|
| PROFES | 193.147.162.128/27 | 193.147.162.129-158 | 193.147.162.159 |
| PISCIS | 193.147.162.160/28 | 193.147.162.161-174 | 193.147.162.175 |
| EXT | 193.147.162.176/29 | 193.147.162.177-182 | 193.147.162.183 |
| FREE | 193.147.162.184/29 | 193.147.162.185-190 | 193.147.162.191 |
| LAB | 172.16.16.0/24 | 172.16.16.1-254 | 172.16.16.255 |
| AB | 172.16.17.0/24 | 172.16.17.1-254 | 172.16.17.255 |
| GESTIÓN | 192.168.192.0/19 | 192.168.192.1-223.254 | 192.168.223.255 |
| PERIFÉRICOS | 10.16.16.0/24 | 10.16.16.1-254 | 10.16.16.255 |

Tabla 3: Subredes del Departamento de Ingeniería Telemática

Las subredes están distribuidas de la siguiente forma:

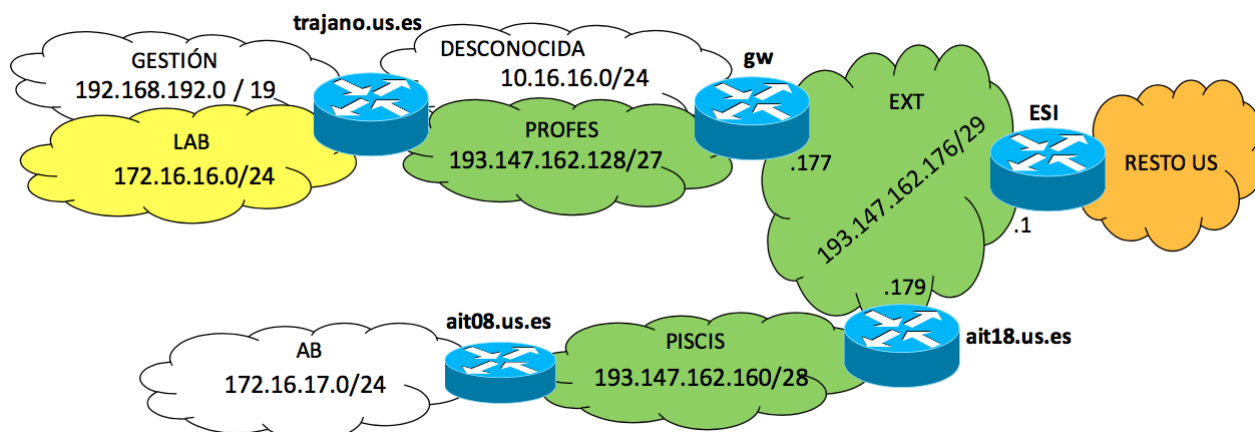


Figura 4: Red IP del Departamento de Ingeniería Telemática

Como se puede apreciar en la figura, el router de la ESI es el que da salida a Internet. A través de una de sus interfaces conecta con la subred EXT del Departamento. Esta subred, principalmente, cuenta con dos routers. Uno de ellos, el **router gw**, es el router ubicado en el propio Departamento, mientras que el otro, el **router ait18.us.es**, se encuentra en el Laboratorio del Departamento, ubicado en el edificio de enfrente.

De aquí en adelante se va a hablar de dos segmentos de red. Uno correspondiente a las subredes que se encuentran en el propio Departamento y otro, con las subredes que se encuentran en el Laboratorio del Departamento.

Las subredes con direccionamiento privado sólo son accesibles desde el segmento de red donde se encuentran. Por ejemplo, la subred GESTIÓN sólo puede ser accesible desde la subred LAB, PROFES y PERIFÉRICOS, y la subred AB, sólo desde la subred PISCIS. Sin embargo, los routers frontera de cada segmento realizan traducción de direcciones (*Source NAT*) permitiendo a estas subredes acceder a Internet.

En el segmento de red del Departamento se encuentra la subred PROFES, que es donde se ubican los equipos de los profesores. Debido a la escasez de direcciones públicas y al aumento del número equipos de profesores en esta subred, se creó la subred PERIFÉRICOS con direccionamiento privado. Esta subred es empleada por los equipos que no necesitan una dirección pública, como impresoras o equipos que no son servidores. En la subred PROFES, además, se encuentra el equipo más importante de Departamento, **trajano.us.es**. Actualmente este equipo, aparte de ser el servidor web del Departamento, actúa como router conectando con las subredes LAB y GESTIÓN.

La subred LAB es donde se ubican los equipos de telefonía (los teléfonos IP, el servidor VoIP, el interfono...) y otros equipos como puntos de acceso e impresoras. Mientras, la subred GESTIÓN es la dedicada a la gestión y administración de los equipos de nivel 2 del Departamento.

Tal como se ha mencionado, el router frontera de este segmento de red es el **router gw**. Este router, además, actúa como Proxy ARP y es el encargado de la traducción de direcciones (NAT).

Un Proxy ARP se ocupa de responder a las peticiones ARP de una interfaz como delegado de las direcciones de otra. Esto es necesario, ya que para el **router ESI** el rango de direcciones públicas asignadas por la Universidad de Sevilla al Departamento no está distribuido en subredes, sino conectadas directamente. De esta forma, sin un proxy ARP sería imposible acceder desde Internet a las subredes con direccionamiento público creadas por el Departamento, debido a que todos los paquetes se quedarían en el segmento de red que une el router ESI con el router gw sin respuesta.

En el otro segmento de la red, el segmento del Laboratorio del Departamento de Ingeniería Telemática, se encuentra la subred PISCIS, cuyo nombre viene de un proyecto que fue asignado anteriormente al Departamento. El equipo **ait08.us.es** de esta subred es el que conecta con la subred interna de este segmento, la subred AB. En esta subred es donde se encuentran los equipos del Laboratorio que los alumnos utilizan para sus prácticas.

Finalmente, la subred FREE es donde se encuentran las direcciones públicas que no se utilizan.

2.6 Escenario

Tal como se ha descrito en el apartado anterior, la red IP del Departamento de Ingeniería Telemática se compone de dos segmentos de red: uno corresponde a las subredes que se encuentran en el propio Departamento y otro, a las subredes que se encuentran en el Laboratorio.

El segmento de red del Departamento consta, entre otras, de dos subredes, una subred con direccionamiento privado, denominada LAB, y otra con direccionamiento público, denominada PROFES.

En la subred PROFES se alojan algunos servidores entre los que se encuentra el servidor **trajano.us.es**, que es el servidor principal del Departamento y, además, el encargado de encaminar el tráfico de una subred a otra. Esta subred a su vez es la que da salida a Internet, su router frontera dispone de un firewall basado en **iptables** que permite el filtrado IP y traducción de direcciones (NAT).

En la subred con direccionamiento privado (subred LAB), se encuentran los equipos y teléfonos IP de los profesores. Asimismo, en esta subred se encuentra el servidor de VoIP del Departamento, Asterisk, sin poder ser accesible desde el resto de Internet.

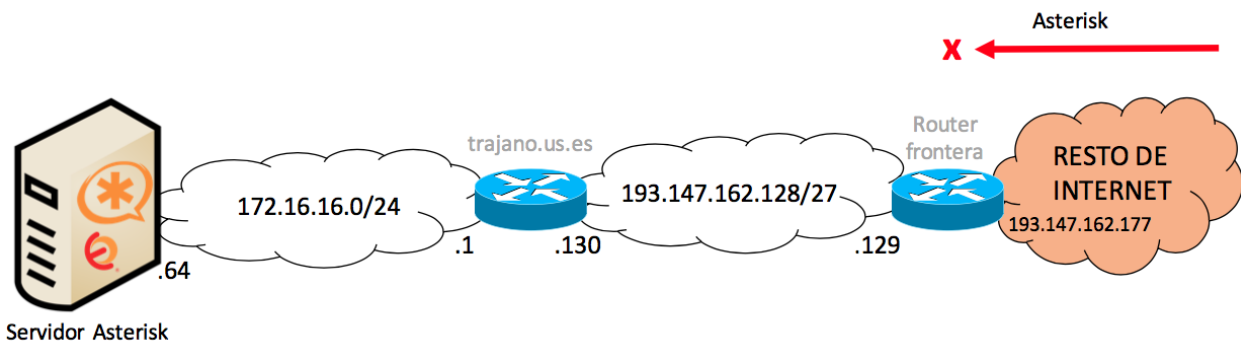


Figura 5: Esquema básico de la arquitectura de red del Departamento

En este proyecto se pretende crear una nueva arquitectura de red para que el servidor de VoIP pueda ser accesible desde Internet, permitiendo así a los clientes SIP, los profesores, acceder al sistema de telefonía del Departamento desde cualquier otro sitio. En estas circunstancias, el nuevo sistema de telefonía queda como se muestra en la siguiente figura:

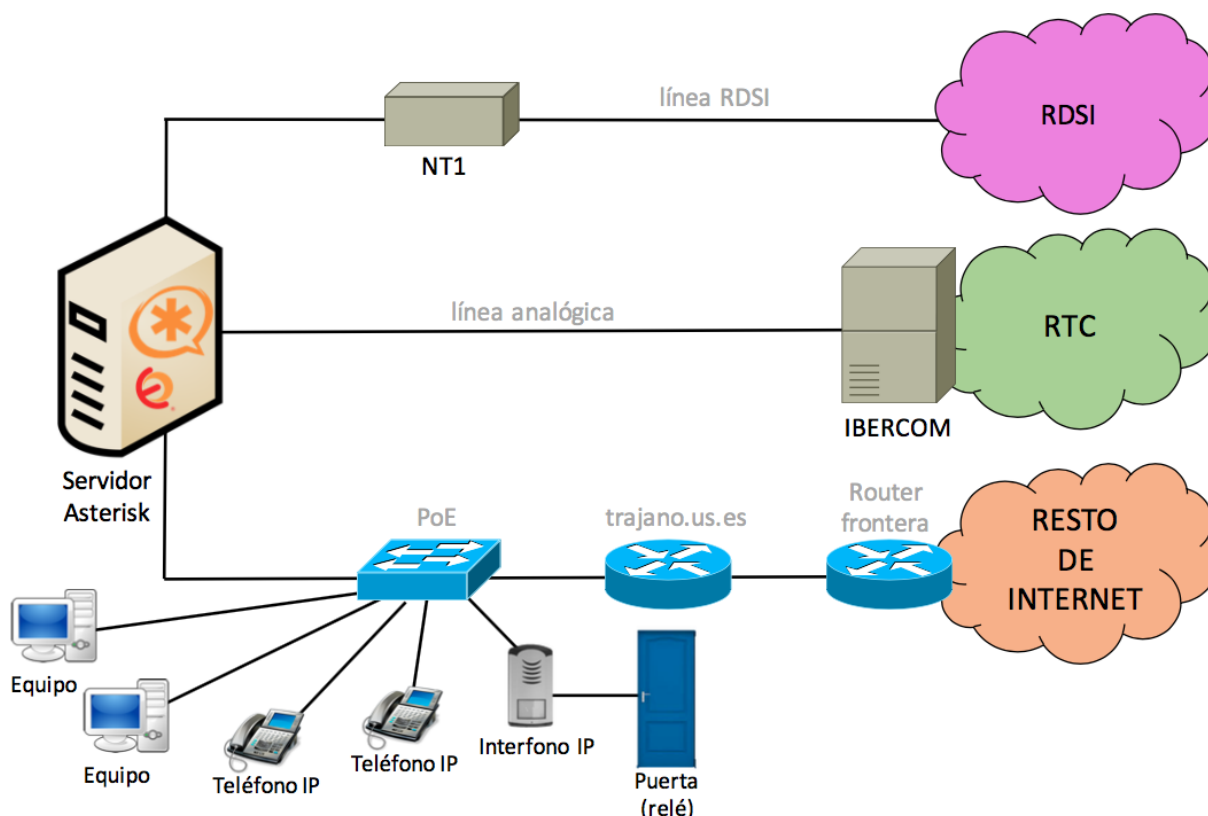


Figura 6: Esquema básico del nuevo sistema de telefonía del Departamento

2.7 Problemas

La configuración del servidor de VoIP del sistema de telefonía del Departamento ha tenido lugar manteniendo activas todas las funciones de éste, evitando así dejar sin servicio a todo el Departamento. Una vez realizada la configuración completa del nuevo escenario surgieron los siguientes problemas:

- Escaneo de puertos.
- Los teléfonos no dejaban de sonar.
- Aumento de tráfico no deseado en la red.
- Aparición de numerosas llamadas maliciosas.

A continuación se profundizará en los problemas mencionados una vez realizada la implementación.

2.7.1 Escaneo de puertos

Actualmente existen numerosas herramientas capaces de detectar y escanear servidores de VoIP en busca de extensiones SIP disponibles que permitan el acceso al sistema de telefonía.

Desde el momento que el servidor de VoIP del Departamento fue accesible desde Internet comenzaron a aparecer multitud de escaneos desde diversas herramientas y agentes de usuario, intentando averiguar el número de extensiones del servidor, la configuración de estas, la configuración del servidor, el sistema donde se hospeda el servidor, etc.

2.7.2 Teléfonos que no dejan de sonar

Por otra parte, un método que utilizan las herramientas anteriormente mencionadas para detectar y escanear servidores de VoIP es el envío continuo de mensajes INVITE al puerto SIP estándar (5060).

El envío de mensajes SIP INVITE a PBX o servidores VoIP vulnerables puede ser útil en algunas circunstancias para los ciberdelincuentes. Sin embargo, no hay forma de distinguir si el dispositivo que escucha en ese puerto es un servidor o un cliente. De este modo, es fácil confundir una PBX que escucha en el puerto SIP 5060 con un *softphone* que tiene abierto ese puerto para recibir y enviar tráfico de señalización. Esto produce que los mensajes no sólo vayan destinados a PBXs o servidores, sino también a *softphones*. Lamentablemente, a este problema se une que la mayoría de los teléfonos IP o *softphones* comienzan a sonar cuando reciben un mensaje INVITE dirigido a su dirección IP, aunque no sea destinado a su extensión o cuenta.

Teniendo el servidor accesible desde de Internet, los *softphones* conectados en la subred con direccionamiento público se veían afectados por el envío constante de estos mensajes, resultando muy molesto que no dejaran de sonar.

2.7.3 Tráfico no deseado en la red

Los ataques contra el servidor de telefonía del Departamento desencadenan un excesivo consumo de ancho de banda y tráfico malicioso entre las dos subredes del Departamento, impidiendo así la disponibilidad de otros servicios de la red. No debemos olvidar que el tráfico de voz y señalización llega hasta el servidor de VoIP ubicado en la subred interna y no solo hasta el servidor trajano.us.es.

2.7.4 Llamadas maliciosas

Las llamadas maliciosas son aquellas en las que usuarios no autorizados tratan de realizar llamadas de pago, principalmente llamadas internacionales y/o de larga distancia que no tienen permiso para realizar.

Al hacer accesible el servidor de VoIP desde el resto de Internet, se producían numerosos intentos de llamadas de este tipo. Estas llamadas no llegaban a realizarse satisfactoriamente debido a la configuración del plan de numeración del servidor de VoIP y la configuración de éste. No obstante, existía la posibilidad de que los atacantes descifrasen dicho plan de numeración, accedieran al sistema de telefonía y, finalmente, pudieran realizar las llamadas. Además, podrían incluso acceder a otros servicios dentro del sistema de telefonía sin autorización.

Este es el principal motivo que nos lleva a la implementación de mayor seguridad en el sistema de telefonía del Departamento.

3 ANÁLISIS DE VULNERABILIDADES

*Todos somos muy ignorantes. Lo que ocurre es que no todos ignoramos las mismas cosas.
- Albert Einstein -*

En este capítulo se describen las vulnerabilidades que sufre la tecnología VoIP, así como los mecanismos de prevención y protección contra ataques de los componentes claves (servidor, teléfonos IP y red IP) que conforman un sistema de telefonía con esta tecnología.

3.1 Seguridad en los componentes del sistema de telefonía

La tecnología VoIP, como ya se ha mencionado, tiene que lidiar con todos los problemas de seguridad de las redes tradicionales de datos además de nuevos riesgos provocados por los nuevos protocolos y componentes.

En comparación con los sistemas tradicionales de telefonía, es más sencillo interceptar una conversación telefónica en cualquiera de los muchos puntos del camino. Una llamada que ha sido interceptada puede ser escuchada, incluso en los casos en los que exista cifrado. Asimismo, debido a la facilidad de configurar pasarelas de VoIP, es relativamente fácil suplantar identidades de llamadas entrantes con intenciones fraudulentas.

Por estas razones es necesario añadir mayor seguridad en los sistemas de telefonía IP. Para ello, se han de proteger todos los componentes que integran el sistema desde los terminales IP hasta la red IP. A continuación se examinarán los elementos clave que componen el sistema de telefonía junto a algunas opciones que permiten protegerlos, previniendo las amenazas que puedan llegar a sufrir.

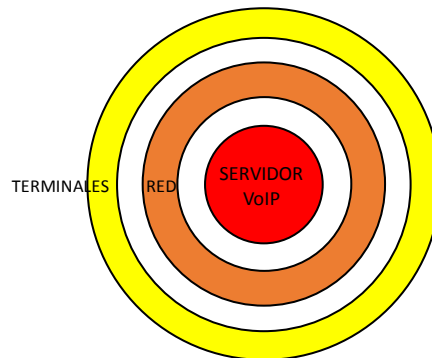


Figura 7: Componentes clave a proteger en un sistema de telefonía IP

3.1.1 Terminales

Un teléfono IP o *softphone* es un *software* que permite realizar llamadas a través de Internet o una red IP a otros *softphones* o a teléfonos convencionales. Este *software* es vulnerable a los mismos huecos de seguridad (*security hole*) que hacen que un sistema operativo pueda estar a plena disposición de un atacante. Es recomendable limitar, en la medida de lo posible, el uso de *softphones* instalados en PCs o *Smartphones*, ya que son más vulnerables a intrusiones por la propia naturaleza de sus sistemas operativos.

A continuación, se enumeran algunos de los ataques que pueden sufrir:

- Inundación de mensajes UDP (*Flood UDP*).
- Inundación de mensajes RTP (*Flood RTP*).
- Inundación de mensajes SIP INVITE (*Invite flood*).

Estos ataques son del tipo **SPIT** (*spam over IP telephone*) y, principalmente, consisten en enviar de forma continua mensajes al teléfono IP haciendo, en algunos casos, que éste no deje de sonar. Igualmente, estos ataques afectan a la red, ya que está siendo constantemente sobrecargada de tráfico no deseado.

También se puede comprometer la seguridad de estos terminales a causa de fallos en su configuración, servicios no desactivados o accesos no autorizados a sus ficheros de configuración vía TFTP/HTTP/HTTPS.

Las consecuencias de estas vulnerabilidades suelen ser la pérdida de servicio o la desconfiguración de los propios terminales.

Para protegerse es recomendable separar la red en distintas redes virtuales (una VLAN para voz y otra para datos). De esta forma, un posible ataque malicioso sobre una de las dos redes no afectaría a la otra.

Además de la precaución básica de mantener los *firmwares* de los dispositivos actualizados, es recomendable añadir un sistema de mitigación de ataques de denegación de servicio (DoS) y disponer de un sistema de autenticación en dos factores (2FA).

Un sistema de autenticación en dos factores ofrece seguridad adicional en el proceso de inicio de sesión. Se trata de una verificación en dos pasos basada en “algo” que el usuario sabe, como su usuario y contraseña, y “algo” que tiene, como podrían ser los certificados o un código de verificación.

3.1.2 Red

Debido al uso de redes IP como medio de transporte para la telefonía, esta tecnología presenta riesgos similares a los que sufren las redes de estas características en general, que van desde el espionaje hasta ataques de denegación de servicio.

Los ataques más significativos son los siguientes:

- Ataques de intermediario (*man-in-the-middle*).
- Ataques de escucha (*eavesdropping*), que permiten capturar la señalización y el flujo de audio dejando la privacidad del usuario comprometida.
- Ataques de denegación de servicio (DoS), que comprometen la disponibilidad del servicio.
- Ataques a servicios como TFTP, que permiten la descarga de la configuración de los equipos o DHCP, que pueden dejar sin direcciones IP a los terminales, debido al agotamiento de las direcciones destinadas para ello.

Como se puede comprobar, las consecuencias de estas vulnerabilidades pueden afectar a los principios fundamentales de la seguridad: confidencialidad, integridad y disponibilidad.

Para protegerse es recomendable, como se ha mencionado en el apartado anterior, separar el tráfico de la red en distintas VLANs (voz y datos), emplear sistemas de autenticación multifactorial y cifrar el audio con protocolos como SRTP (*Secure Real-time Transport Protocol* definido en RFC 3711) y ZRTP (extensión de RTP que describe el establecimiento de un intercambio de claves). Estos protocolos de cifrado permiten agregar funciones de seguridad como autenticación de mensajes, confidencialidad y protección de respuesta, reduciendo el riesgo de interceptación de comunicaciones o espionaje.

Además, conviene disponer de un cortafuegos que impida la descarga de los ficheros de configuración de los equipos a usuarios no autorizados.

La política de aplicar distintas capas de seguridad en los distintos estratos de la red (cortafuegos para el servidor, aislamiento del servidor del resto de la red, separación de redes de voz y datos) se denomina "defensa en profundidad" (*in-depth*), en oposición a la "defensa perimetral" empleada, por ejemplo, en NAT.

3.1.3 Servidor de VoIP

El servidor de VoIP o PBX es el componente más importante del sistema de telefonía IP que hay que proteger, ya que implementa el servicio de voz sobre IP y permite la gestión de las comunicaciones.

El ataque más común a una PBX es el sondeo inocuo conocido en inglés como *friendly-scanner*, que no es realmente un escáner "amigo" sino un tipo de *botnet*⁴. El ataque se lleva a cabo en los siguientes pasos:

1. Barrido de puertos (*scanning*).
2. Enumeración (*enumeration*).
3. Fuerza bruta (*brute force*).
4. Abuso (*abuse*).

Primero, escanea unos rangos de direcciones IP en busca de servidores SIP que se comuniquen a través del puerto 5060. Si encuentra el puerto abierto, trata de enumerar la configuración del servidor, las extensiones disponibles, etc. Posteriormente, intenta forzar bruscamente el servidor probando números secuenciales como extensiones SIP con nombres de usuarios y contraseñas comunes (débiles). Y una vez obtenido el acceso a una extensión del servidor, los atacantes tratan de realizar llamadas a través de la red telefónica conmutada, sobre todo para realizar llamadas internacionales, llamadas de pago.

Un *friendly-scanner* puede sondear la red una vez cada pocas horas o entrar en el modo DoS, enviando multitud de solicitudes SIP REGISTER por segundo, causando una enorme pérdida de ancho de banda.

Los ataques de estas características son del tipo **TOLL FRAUD** (fraude), ya que los atacantes usan el sistema de telefonía de forma fraudulenta para realizar llamadas de pago (llamadas internacionales y/o de larga distancia) que no tienen permiso para realizar.

⁴ Un *botnet* es un conjunto o red de robots informáticos que se ejecutan de manera autónoma y automática pudiendo controlar todos los equipos/servidores infectados de forma remota.

El uso fraudulento de los sistemas de telefonía refuerza la importancia de llevar a cabo buenas prácticas de seguridad a la hora de configurar las extensiones y proteger el servidor. Algunas de estas prácticas son:

- Proteger el servidor de Internet, siendo más restrictivo en términos de qué extensiones se pueden alcanzar desde direcciones IP externas.
- Utilizar contraseñas seguras, lo bastante largas y difíciles de adivinar. La mayoría de los clientes SIP requieren que la contraseña se introduzca sólo una vez, por lo que no es necesario crear contraseñas fáciles de recordar. La recomendación actual es usar al menos 12 caracteres, incluyendo números, símbolos y letras mayúsculas y minúsculas.
- Crear nombres de usuario distintos de las extensiones. La mayoría de los intentos de fuerza bruta prueban nombres de usuario que coinciden con los números de extensión.
- Supervisar el uso de SIP en la organización, monitorizando los registros del servidor de VoIP y comprobando la información de facturación telefónica, buscando llamadas interurbanas o internacionales.

Además de implementar buenas prácticas para proteger el sistema de telefonía IP, es recomendable dotar de seguridad al servidor de VoIP desde los diferentes puntos de vista que se detallan a continuación.

3.1.3.1 Seguridad en la configuración del servidor de VoIP

Un servidor de VoIP con una configuración segura puede evitar muchos de los ataques que sufre esta tecnología. Dotar de seguridad a un servidor desde su configuración consiste en ajustar sus parámetros para minimizar o impedir la realización de llamadas sin autenticación y sin registro previo de los clientes. De esta forma, los atacantes seguirán pudiendo acceder a la red donde se encuentre el servidor, pero no podrán acceder al sistema de telefonía sin autorización, es decir, sin una extensión SIP a la que tengan acceso.

Actualmente existen algunas herramientas como **SIPVicious** que permiten probar si la configuración SIP del servidor Asterisk es segura (para mayor detalle de esta herramienta véase el [ANEXO C. SIPVicious](#)). **SIPVicious** se compone principalmente de cinco programas escritos en Python:

- `svmap`. Es un escáner SIP. Se encarga de sondear una dirección o un rango de direcciones IP para averiguar si hay dispositivos SIP, ya sean servidores o *softphones*, que tengan abierto el puerto SIP estándar. Hoy en día, también permite el barrido de puertos no estándares.
- `svwar`. Este ejecutable sondea el servidor de VoIP buscando y enumerando las extensiones SIP que permiten registrarse. Además, indica si la extensión requiere o no autenticación.
- `svcrack`. Intenta obtener la contraseña de una extensión SIP o un servidor de registro. Los modos actuales de craqueo de contraseñas son rangos numéricos o palabras de archivos diccionario.
- `svreport`. Este programa es capaz de exportar la información de las sesiones creadas por el resto de herramientas a pdf, xml, csv y texto sin formato.
- `svcrash`. Responde a los mensajes `svwar` y `svcrack` SIP con un mensaje que hace que las versiones anteriores se bloqueen.

Dado que estas herramientas han sido muy explotadas por los ciberdelincuentes, los proveedores de PBX han actualizado su *software* para prohibir dichos sondeos, conocidos como "*friendly-scanner*". Sin

embargo, **SIPVicious** puede configurarse para que realice una exploración con mensajes INVITE, permitiendo así atacar a la PBX o servidor.

3.1.3.2 Seguridad en el perímetro del servidor de VoIP

Una vez protegido el servidor con una configuración segura, se debe complementar su protección incrementando la seguridad en la red donde se encuentra junto con el resto de elementos del sistema. Esta medida se lleva a cabo añadiendo *software* o *hardware* cerca del servidor de forma que se impida el acceso a usuarios no autorizados a la red.

El empleo de IPS, cortafuegos y análisis avanzados de protocolos son una técnica muy común que permite la mitigación de algunas de las vulnerabilidades de este servicio. Es una técnica que debe actualizarse continuamente para incorporar un nivel de seguridad proactivo.

3.1.3.3 Seguridad integrada en el servidor de VoIP

Por último, para incrementar la seguridad en el propio servidor es necesario la adición de *software* integrado que permita bloquear e impedir el acceso al servidor de direcciones IP maliciosas. Ejemplos son **Fail2ban** y **SecAst**.

Fail2ban es una herramienta que analiza los archivos de registro de un servicio y prohíbe las direcciones IP que muestran signos maliciosos (para más información véase el [ANEXO A. Guía De Instalación De Fail2ban](#)). Principalmente se usa para actualizar las reglas del cortafuegos rechazando o prohibiendo direcciones IP que tratan de hacer un uso fraudulento de un servicio. Cabe destacar que no se considera un sistema de seguridad, pues no analiza los paquetes, sólo analiza los mensajes de registro y depende completamente del servidor, en este caso de Asterisk, para detectar cualquier intruso o fallo en los registros sobre los que esta herramienta puede actuar.

Por un lado, **SecAst** es un sistema propietario de detección y prevención de fraudes e intrusiones diseñado específicamente para proteger los sistemas de telefonía basados en Asterisk. Utiliza una gran variedad de técnicas y bases de datos propietarias para detectar intentos de intrusión, detener ataques en curso y prevenir futuros ataques. Tras la detección del ataque, **SecAst** puede cancelar llamadas y/o bloquear al atacante desde Asterisk a nivel de red.

El uso de las bases de datos de números de teléfonos fraudulentos y direcciones IP de ciberdelincuentes le permite mitigar el riesgo de intrusión de los atacantes conocidos y reducir el riesgo de fraude por llamadas de pago no autorizadas. Asimismo, este sistema de seguridad permite monitorizar los intentos de conexión, las direcciones IP origen de los usuarios remotos, el número de canales en uso por usuario...

3.2 Ataques SIP

Previamente se han mencionado numerosos ataques que comprometen la seguridad en un sistema de telefonía IP a través de sus componentes. Ahora, se detallarán algunos ataques al protocolo SIP que afectan a la seguridad del servidor de VoIP directamente e indirectamente, al resto del sistema.

El protocolo SIP posee una sintaxis muy similar a la de los protocolos HTTP (utilizado en los servicios de páginas Web) y SMTP (para distribución de e-mails). Debido a esto y a que los mensajes SIP son transmitidos

en texto plano, hace que este protocolo sea muy atractivo desde el punto de vista de los atacantes. Los atacantes, principalmente, tratan de interceptar y manipular los mensajes SIP para diferentes fines. Estos ataques incluso pueden desencadenar un ataque de DoS contra el servidor en determinadas ocasiones.

Algunos de estos ataques son:

- Secuestro de registro (*registration hijacking*).
- Secuestro de sesión (*session hijacking*).
- Abandono de sesión (*tearing down sessions*).

3.2.1 Secuestro de registro

Se produce cuando un agente de usuario (teléfono IP o *softphone*) intenta registrarse en un proxy SIP o un servidor de registro. El atacante captura el mensaje de registro y suplanta al agente de usuario introduciendo su propia dirección. Este ataque hace que las llamadas entrantes, en lugar de ser destinadas al agente de usuario, sean destinadas hacia el atacante.

3.2.2 Secuestro de sesión

Este ataque consiste en la duplicación de las credenciales de autorización de una sesión ya establecida entre el servidor y el agente de usuario para permitir el acceso a los servicios prestados por el servidor.

3.2.3 Abandono de sesión

Este ataque intercepta las peticiones de un agente de usuario y envía un mensaje BYE como respuesta procedente de un proxy o servidor de VoIP. Esto provoca el cierre de la sesión establecida entre el cliente y el servidor.

Este tipo de ataques contra el protocolo SIP no suelen tener efectos graves, dado que es mucho más sencillo lanzar un ataque DoS contra la red o algún elemento de ésta que tenga consecuencias mayores que un simple cierre de sesión. Por ello, estos ataques son poco frecuentes y no suelen venir motivados por un afán de causar graves daños más allá de un simple cierre de sesión.

Además de todos estos ataques, existen los ataques tipo **VISHING**, que son similares a los tipo phishing. La diferencia es que la víctima proporciona su información personal por teléfono y no en el sitio web.

3.3 Detección de ataques al sistema de telefonía

Los signos de un ataque al sistema de telefonía IP incluyen problemas al registrar/conectar los teléfonos, conexiones de red extremadamente lentas y un uso continuo de ancho de banda.

Todas las medidas propuestas anteriormente proporcionan una solución válida a corto plazo ya que no son escalables ni suficientes para proteger el sistema de telefonía. Sin embargo, si se incorpora el uso de un

sistema de autenticación en dos factores (o multifactorial), sí es una solución válida a largo plazo. De esta manera, incluso si un atacante obtuviese la contraseña maestra de un usuario, se le bloquearía la entrada al no disponer de los certificados adecuados.

Otras soluciones intermedias son:

- Crear un señuelo (*honeypot*). Disponer de un servidor de VoIP que no requiera registro de los clientes para permitir que los ciberdelincuentes ataquen a ese sistema de telefonía falso, distrayéndolos así del sistema real.
- Enviar mensajes 200 OK en respuesta a los mensajes SIP REGISTER de los atacantes. Existen herramientas que utilizan secuencias de comandos automatizadas para detener estos ataques. Engañan al escáner haciéndole pensar que se ha realizado un intento de registro exitoso.
- Paquete Invalido. En casos excepcionales, puede bloquear el escáner y detener una inundación de paquetes enviando una respuesta SIP no válida.

3.4 Recomendaciones

La tecnología VoIP se enfrenta a varios problemas de seguridad, tanto los originados por su propio desarrollo como los provocados por los protocolos en las que se basa. A la hora de diseñar una política de seguridad es necesario plantearla a varios niveles, teniendo en cuenta los distintos elementos que componen el sistema: terminales, redes, dispositivos centrales (PBX o servidores) y el entorno de estos.

Tal y como se detalla en la referencia [3], una política de seguridad debe seguir las siguientes normas fundamentales:

1. Desarrollar una arquitectura de red apropiada.
 - Si es posible por los requisitos de calidad de servicio, es una buena práctica separar voz y datos en redes virtuales diferentes (VLAN), deshabilitando los protocolos de una red en la otra.
 - Se recomienda el empleo de autenticación robusta y control de accesos en la pasarela de voz.
 - Se aconseja disponer de un cortafuegos de estado (*stateful firewall* o *stateful packet filter*) que permita monitorizar el estado de las conexiones, rechazando paquetes originados por una llamada incorrecta.
 - Uso de protocolos IPSec o SSH para administración remota y proceso de auditoría.
2. Emplear cortafuegos preparados para voz sobre IP y otras medidas de protección adecuadas. Debido a las vulnerabilidades expuestas, los sistemas de VoIP deben incorporar un conjunto de medidas de seguridad y protocolos que formen una "defensa en profundidad"; unos cortafuegos preparados para esta tecnología son componentes esenciales en este sentido. Si es posible, añadir detección de intrusiones y sistemas de prevención.
3. Limitar en lo posible el uso de *softphones*, ya que están instalados en máquinas con sistemas operativos potencialmente no seguros y expuestos a virus y otros *softwares* maliciosos.

4. En el caso de utilizar *softphones*, no usar el puerto estándar SIP (5060). Es el puerto por defecto que utilizan las herramientas de sondeo.
5. Reforzar el control físico de seguridad. A menos que la red voz esté cifrada, el acceso físico a la red de área local permite la interceptación de comunicaciones telefónicas. Por lo tanto, un sistema de seguridad debe incluir la protección de los accesos físicos a la red.
6. Instalar sistemas anti-virus, tanto en el servidor como en los *softphones* empleados.
7. Mantener el *software* actualizado: sistemas operativos, servidor, clientes, antivirus y cortafuegos.
8. Aplicar encriptación. La encriptación protege al sistema de escuchas no deseadas; TLS e IPSec son dos opciones válidas.

4 SOLUCIÓN ADOPTADA

*Nuestra recompensa se encuentra en el esfuerzo y no en el resultado. Un esfuerzo total es una Victoria completa.
- Mahatma Gandhi -*

Este capítulo describe la solución propuesta para permitir el acceso al servidor de VoIP del Departamento de Ingeniería Telemática de la Escuela Superior de Ingenieros de forma segura desde el resto de Internet.

Además, incluye el diseño de una política de seguridad, planteada a varios niveles, teniendo en cuenta los distintos elementos que componen el sistema de telefonía IP y centrándose en el componente central de éste (el servidor de VoIP).

4.1 Accesibilidad del servidor de VoIP

Tal como se explica en el [Capítulo 2](#), la red IP del Departamento se compone de dos segmentos de red. Dentro del segmento de red del Departamento existen, entre otras, dos subredes: la subred con direccionamiento público, que da salida a Internet a través de su router frontera; y la subred interna con direccionamiento privado, donde actualmente se encuentra el servidor de VoIP del Departamento, Asterisk.

El router frontera de la subred con direccionamiento público dispone, además, de un cortafuegos basado en **iptables** que permite el filtrado IP y traducción de direcciones (NAT).

Para que el servidor de VoIP pueda ser accesible desde el resto de Internet, se plantean tres posibles soluciones:

- Ubicar el servidor y los clientes internos del Departamento en la subred de direccionamiento público, con direcciones IP públicas.
- Ubicar el servidor en la subred con direccionamiento público y los clientes internos en la subred con direccionamiento privado.
- Mantener tanto el servidor como los clientes internos dentro de la subred de direccionamiento privado y realizar una traducción de direcciones (NAT) en el router frontera.

En las circunstancias actuales resulta casi imposible posicionar todos los clientes internos del Departamento en la subred con direccionamiento público debido a la escasez de direcciones públicas de esta. Se trata de una red con máscara de 27 bits, es decir, solo dispone de 30 direcciones IP.

Tampoco resulta práctico ubicar el servidor en la subred con direccionamiento público mientras los clientes internos se ubican en la subred con direccionamiento privado, ya que causaría mucho tráfico entre ambas subredes.

Por lo tanto, se concluye que la solución más razonable es mantener el servidor junto a los clientes internos en la subred con direccionamiento privado, debido a que, si existe una hipotética caída de red o un ataque de DoS en la subred con direccionamiento público, los clientes podrían seguir manteniendo llamadas internas entre ellos y realizando llamadas hacia el exterior a través de las líneas troncales.

4.2 Adición de seguridad integrada en el servidor de VoIP

La política de seguridad que se ha planteado a varios niveles comienza con la adición de seguridad en el propio servidor de VoIP. Consiste en añadir *software* integrado que permita bloquear e impedir el acceso al servidor de usuarios no autorizados.

El *software* elegido para ello ha sido **Fail2ban** por su condición de *software* libre y gratuito, además de ser uno de los más usados comúnmente. No obstante, cabe citar que existen productos de *software* privativo más completos que el elegido, como por ejemplo *SecAst* (que dispone de una versión gratuita para su uso no comercial).

4.2.1 Fail2ban

Fail2ban es una herramienta que analiza los ficheros de registro de un servicio y bloquea las direcciones IP que muestran signos maliciosos. Una de sus principales funciones es la de añadir filtros al cortafuegos para diversos servicios como apache, ssh o asterisk.

En el caso del servidor Asterisk, **Fail2ban** es capaz de reducir la tasa de intentos de autenticaciones incorrectas. Sin embargo, no puede eliminar el riesgo que presenta la autenticación débil. Para garantizar la confidencialidad, como se ha mencionado previamente en este documento, es necesario configurar el servicio para que además use mecanismos de autenticación basados en dos factores.

Actualmente **Fail2ban** sigue siendo compatible con Asterisk, aunque debemos considerarlo como una solución a corto plazo, ya que esta herramienta es bastante limitada para detectar ataques contra dicho servicio.

Este *software* ya viene instalado y configurado en Elastix para ssh pero no para la señalización SIP. La configuración para Asterisk es muy sencilla (véase el [ANEXO A. Guía De Instalación De Fail2ban](#)), sólo hay que establecer los valores de los siguientes parámetros: `ignoreip`, `bantime`, `maxretry` y `findtime`.

Para la configuración de estos parámetros, **Fail2ban** dispone, entre otros, de dos ficheros de configuración importantes. Estos ficheros son los siguientes:

- ❖ `/etc/fail2ban/filter.d/asterisk.conf`. Es un fichero de configuración de patrones de bloqueo para Asterisk, es decir, un fichero de configuración que permite ajustar en qué formato se encuentra la dirección IP en los archivos de logs para que ésta pueda ser baneada.
- ❖ `/etc/fail2ban/jail.conf`. Es un fichero de configuración general de **Fail2ban** en el que se establecen los valores de los parámetros mencionados anteriormente.

Para configurar el fichero de registro de salida se encuentran dos opciones, o bien usar `syslog`, y que todos los mensajes vayan al fichero `/var/log/messages`, o bien usar su propio archivo de registro, por ejemplo `/var/log/fail2ban.log`. Para indicar qué opción se va a emplear, se hace uso del parámetro `logpath`.

4.3 Adición de seguridad en el perímetro del servidor de VoIP

Tal como se ha descrito en apartados anteriores, el Departamento dispone de un cortafuegos basado en `iptables` en el router frontera. Además, el servidor Asterisk está alojado en un sistema operativo Linux basado en CentOS que también permite uso de esta herramienta de filtrado de paquetes.

Con el fin de incrementar la seguridad en el perímetro del servidor de VoIP, se va a implementar un cortafuegos de aplicación en este mismo. De esta manera, el Departamento dispondrá, finalmente, de dos cortafuegos, uno a nivel de red en el router frontera y otro a nivel de aplicación en el servidor de VoIP Asterisk.

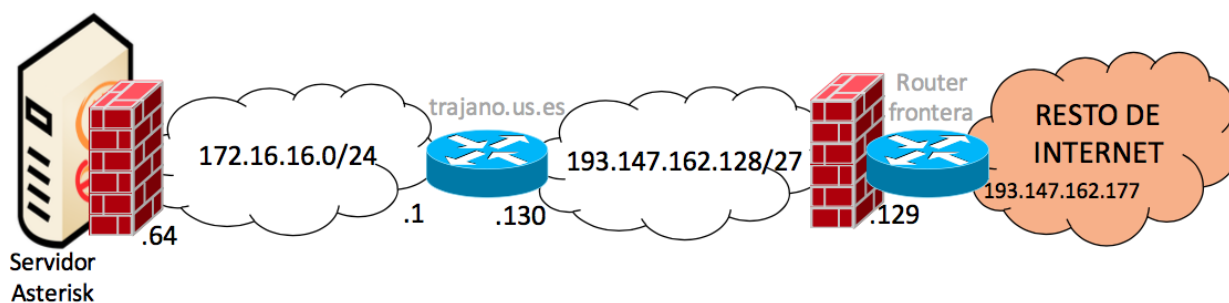


Figura 8: Cortafuegos de la red del Departamento

Para mantener la confidencialidad en el sistema de telefonía del Departamento se van a añadir una serie de reglas a estos cortafuegos, de forma que sólo permitan el acceso de determinados usuarios. Esto evitará los posibles daños e impedirá que las personas no autorizadas por puertos no autorizados puedan obtener acceso al servicio de telefonía.

4.3.1 Cortafuegos de aplicación

El nombre “cortafuegos de aplicación” resulta engañoso; un cortafuegos de aplicación es aquel que actúa sobre la capa de aplicación, mientras que el descrito en este apartado actúa sobre la capa de red. En este caso, ha recibido este nombre para diferenciarlo del cortafuegos instalado en el router frontera de la red.

Este cortafuegos contiene las cadenas creadas por `Fail2ban` para Asterisk y las reglas que esta herramienta introduce dinámicamente para bloquear las direcciones IP que considera atacantes. Sin embargo, para bloquear las direcciones IP de los atacantes, la solución más eficiente sería definir una política por defecto DROP (rechazar todo) que permitiera solo por excepción las direcciones IP fijas de los clientes. Pero, en realidad, muchos clientes SIP no tienen direcciones IP estáticas, debido a que estos, a menudo, se conectan dinámicamente a través de distintas redes WiFi u otras redes que cambian la dirección IP. Por tanto, bloquear el acceso por direcciones IP normalmente no es viable.

Fail2ban, como se ha indicado en apartados anteriores, es una herramienta a corto plazo que no garantiza totalmente la seguridad. Por ello, se han introducido ciertas reglas adicionales en el cortafuegos para impedir que agentes de usuario distintos a los empleados por los miembros del Departamento tengan acceso al sistema de telefonía. La forma más fácil de implementarlo es permitir sólo esos determinados agentes de usuario y prohibir todos los demás.

4.3.2 Cortafuegos de red

No es suficiente con cortar determinado tráfico en el cortafuegos de aplicación, debido a que éste se encuentra en la parte más interna del segmento de red del Departamento. Esto significa que seguiría habiendo tráfico SIP no deseado en la subred con direccionamiento público (subred PROFES). Además, los *softphones* ubicados en esta subred continuarían sufriendo sondeos “*friendly-scanner*”, que provocaría que no dejaran de sonar. Para impedir que este tráfico entre en la red, es necesario añadir otras reglas en el cortafuegos del router frontera.

Las reglas del cortafuegos de red se introducirán en la cadena FORWARD de la tabla FILTER, ya que es la cadena por la que pasan los paquetes destinados a otros equipos.

A la hora de introducir reglas **iptables** en el router frontera se debe tener en cuenta que este router es el encargado de realizar la traducción de direcciones. Por lo tanto, hay que considerar que:

- En la tabla NAT la cadena PREROUTING (encargada de la acción DNAT) se procesa antes que la cadena FORWARD de la tabla FILTER, es decir, la traducción de direcciones del destino se realiza antes de que el router frontera tome la decisión de encaminamiento.
- En la cadena POSTROUTING (encargada de la acción SNAT) se procesan las reglas después de la cadena FORWARD.

Seguidamente se muestra un diagrama que contiene todas las cadenas **iptables** por las que puede pasar un paquete dependiendo de su destino:

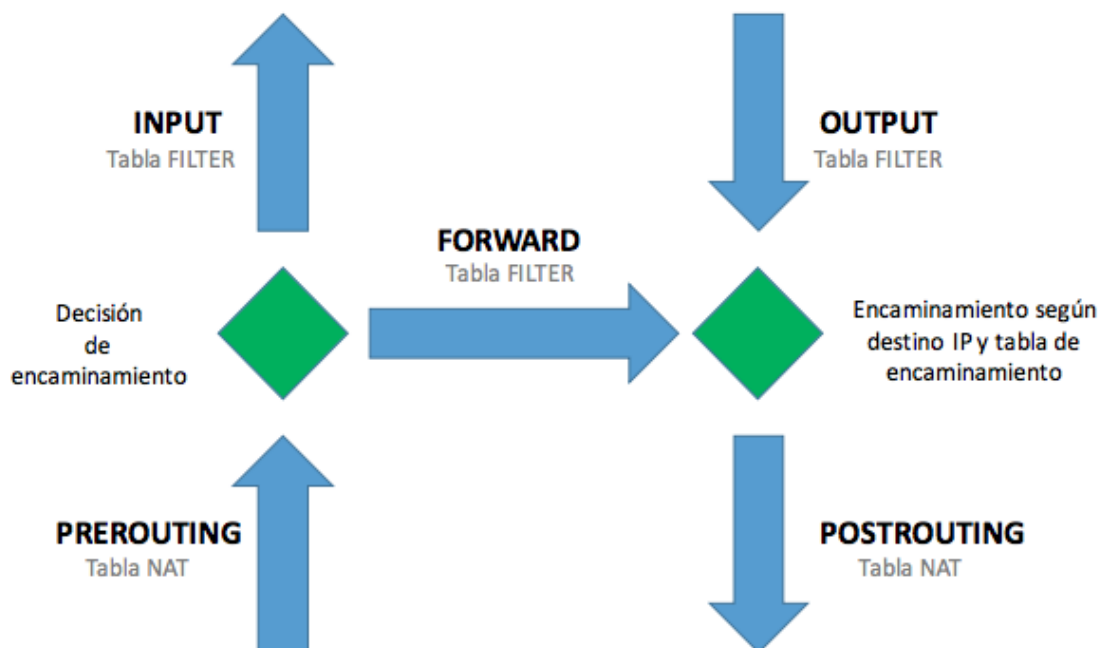


Figura 9: Camino que sigue un paquete IP en el cortafuegos de red

4.4 Adición de seguridad en la configuración del servidor de VoIP

En este apartado se indicará cómo ajustar algunos parámetros de configuración del servidor de VoIP para minimizar posibles ataques e impedir, en la medida de lo posible, la realización de llamadas sin autenticación y sin registro previo de los clientes.

Además, se describirán otras medidas para proteger el servidor de Internet, como el empleo de contraseñas más seguras o el establecimiento de qué extensiones pueden ser alcanzadas desde direcciones IP externas.

4.4.1 Configuraciones seguras

Los parámetros que conviene asegurar su valor de configuración para proteger el servidor de usuarios no autorizados son los siguientes:

- ❖ `alwaysauthreject=yes`. Ajustando este parámetro con el valor `yes`, Asterisk rechaza las autenticaciones erróneas tanto si el usuario es válido, como si no, respondiendo al atacante siempre con el mismo mensaje. Esto evita los ataques de fuerza bruta que permiten descubrir extensiones.
- ❖ `allowguest=no` (el valor por defecto es `yes`). Este parámetro deshabilita las llamadas SIP de clientes anónimos.
- ❖ `insecure=no`. Especifica cómo manejar las conexiones entre los clientes. Por defecto, el valor de este parámetro es `no`, lo que significa que autentica todas las conexiones.

El parámetro `type` establece en que momento de la comunicación el cliente SIP debe autenticarse para realizar una llamada. Los comportamientos que permite dicho parámetro son los siguientes:

- `type=peer`. Obliga a que el desafío para la autenticación del cliente se realice sólo en el mensaje REGISTER, nunca en el mensaje INVITE.
- `type=user`. Permite autenticar al cliente en los mensajes de INVITE mediante desafíos en cada llamada y no necesita que el cliente esté registrado previamente.
- `type=friend` (`peer + user`). Valor escogido por defecto en el que Asterisk crea dos instancias, un tipo `peer` y otro tipo `user`, con el mismo nombre de usuario. Esto quiere decir que el cliente puede ser autenticado cuando se registra o cuando va a iniciar una llamada.

Como resumen, se muestra la siguiente tabla que expone cómo puede autenticarse cada cliente según su tipo:

| type | REGISTER | INVITE |
|--------|----------|--------|
| peer | X | |
| user | | X |
| friend | X | X |

Tabla 4: Parámetro type

El problema de configurar las extensiones como `type=friend` (valor por defecto) es que este tipo de relación permite al usuario realizar llamadas sin registrarse. Además, Asterisk envía diferentes mensajes de error dependiendo de si el número de extensión es válido o no. Esto permitiría al atacante conocer los números de extensión válidos para concentrar su ataque de fuerza bruta.

Igualmente, Asterisk no incluye la dirección IP de los clientes que fallan al autenticarse mediante mensajes de tipo INVITE, lo que impide a **Fail2ban** detectarlo. Por estas razones, lo más seguro es utilizar `type=peer`, obligando a todos los clientes a registrarse y a autenticarse desde el primer momento.

4.4.2 Cambio de contraseña de los teléfonos IP

Anteriormente, el sistema de telefonía IP del Departamento no era accesible a través de Internet, con lo que los clientes SIP sólo tenían acceso a él mientras se encontraban en sus respectivos despachos. Por este motivo las contraseñas de sus cuentas eran muy sencillas.

Debido al objetivo de hacer el servidor público y accesible desde el exterior de la red del Departamento, se han visto en la necesidad de cambiar las contraseñas y emplear otras más seguras. Para ello, se ha seguido el estándar actual utilizando una contraseña de al menos 12 caracteres, incluyendo números, símbolos y letras mayúsculas y minúsculas.

Aunque la seguridad siempre implica incomodidad, este no es el caso, ya que la mayoría de los clientes SIP requieren que la contraseña se introduzca sólo una vez, por lo que no es necesario emplear contraseñas fáciles de recordar. Además, en el caso de las extensiones internas del Departamento, los teléfonos IP de los profesores se configuran vía TFTP, con lo que no es necesario ni siquiera introducir la contraseña manualmente.

4.4.3 Modificación del plan de extensiones

Para proteger el servidor de Internet se va a ser más restrictivo en cuanto a qué extensiones pueden ser accesibles desde direcciones IP externas.

Tal como se ha descrito en el Capítulo 2 del apartado [Plan de numeración](#), los prefijos '2X', '3X' y '4X' están reservados para las extensiones SIP internas. Estas extensiones se configurarán para que sólo sean accesibles desde el segmento de red del Departamento.

La modificación del plan de extensiones no afectará a los prefijos empleados para el establecimiento de llamadas tanto internas como externas.

Dado que una cuenta SIP o extensión no puede estar registrada en dos dispositivos a la vez, se ha decidido crear un conjunto de extensiones nuevas para que los profesores puedan acceder al sistema de telefonía desde el exterior sin necesidad de desconectar su teléfono IP del despacho. El nuevo plan de extensiones mantendrá las extensiones internas existentes e incluirá un conjunto de extensiones para cada profesor que sí serán accesibles desde Internet.

El nuevo conjunto de extensiones dispondrá del prefijo '1XX', siendo 'XX' el número de extensión correspondiente a cada profesor. Por ejemplo, en el caso del profesor cuya extensión interna sea la número '23', su extensión externa asignada será la '123'.

Como se ha comentado en otros apartados, **SIPVicious** comienza su sondeo de extensiones, por defecto, a partir de la extensión número '100' y suele llegar hasta la número '105', con lo que este nuevo plan de extensiones, en principio, no se vería afectado por el uso malicioso de esta herramienta (para más información

véase el [ANEXO C. SIPVicious](#)).

El nuevo plan de extensiones queda como sigue:

| EXTENSIÓN | ASIGNADA A ... |
|---------------------|--|
| 121-133, 135 | Extensiones SIP externas de profesores |
| 20 | Puerta |
| 21-33, 35 | Extensiones SIP internas de profesores |
| 34, 36-39 | Salas / Secretaría |
| 40 | FAX |

Tabla 5: Nuevo plan de extensiones SIP del Departamento

5 IMPLEMENTACIÓN

No harás nunca nada en este mundo sin coraje. Es la mayor cualidad mental junto al honor.
- Aristóteles -

Este capítulo describe el proceso de diseño e implementación de la nueva arquitectura de red que permite al servidor de VoIP del Departamento de Ingeniería Telemática de la Escuela Superior de Ingenieros ser accesible de forma segura desde el resto de Internet.

5.1 Traducción de direcciones (NAT)

Dada la situación existente, la solución óptima es mantener el servidor de VoIP en la subred con direccionamiento privado junto con los clientes internos. Para ello, se necesita que el router frontera realice una traducción de nombres para los puertos de audio y señalización en los que el servidor está escuchando. En nuestro caso el servidor escucha en el puerto UDP/TCP 5060 la señalización SIP y en el rango de puertos UDP 10.000-10100 el audio RTP en la dirección 172.16.16.64. Se configurará para que el sistema de telefonía IP del Departamento esté accesible desde el resto de Internet a través de la dirección de trajano.us.es (193.147.162.130).

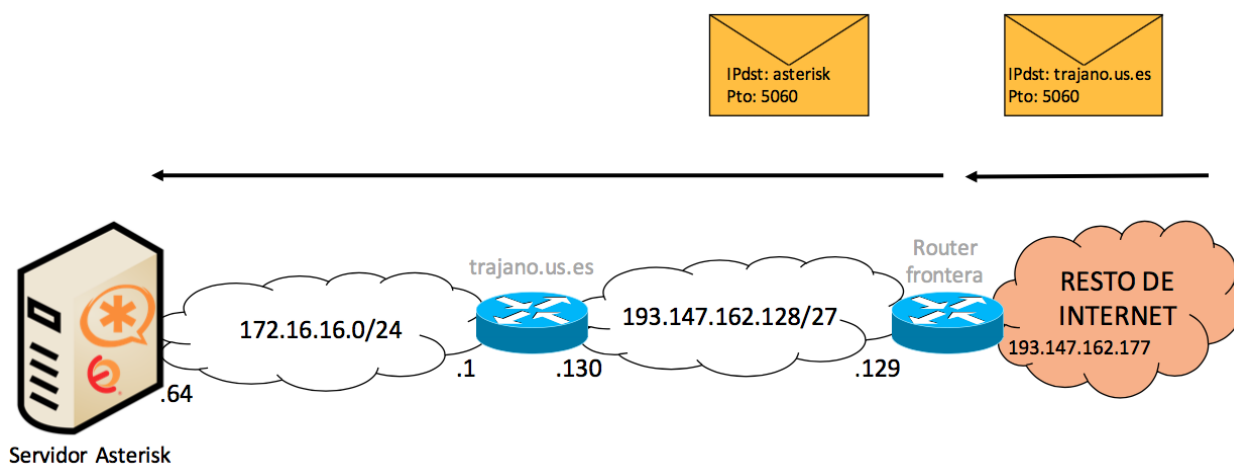


Figura 10: Esquema básico de la arquitectura de red del Departamento

En este escenario el NAT permite que sólo a través de algunos puertos el servidor sea accesible desde Internet, si bien existe la posibilidad de cambiar el puerto de escucha de la señalización SIP a un puerto no estándar, ya que la mayoría de los escáneres “amigo” sólo sondean, por defecto, el puerto 5060. Sin embargo, cambiar el número de puerto de escucha a un puerto no estándar puede ser difícil de configurar en los clientes SIP y muy fácil de mapear desde cualquier otra herramienta que enumere los puertos que un equipo tiene abiertos.

Por consiguiente, se han introducido las siguientes reglas DNAT (Destination NAT) en el cortafuegos del router frontera para el enmascaramiento del servidor:

```
# SIP
iptables -t nat -A PREROUTING -p udp -d 193.147.162.130 --dport 5060 -j DNAT --
to-destination 172.16.16.64:5060

iptables -t nat -A PREROUTING -p tcp -d 193.147.162.130 --dport 5060 -j DNAT --
to-destination 172.16.16.64:5060

# RTP
iptables -t nat -A PREROUTING -p udp -d 193.147.162.130 --dport 10000:10100 -j
DNAT --to-destination 172.16.16.64:10000-10100
```

Con estas reglas se obliga a que todo el tráfico con destino al servidor `trajano.us.es` (193.147.162.130) por los puertos de audio y señalización indicados anteriormente se redirijan a Asterisk (172.16.16.64).

5.1.1 Configuración NAT en Asterisk

Actualmente Asterisk no es compatible con el protocolo STUN (siglas en inglés de *Session Traversal Utilities for NAT*), por lo que toda la configuración NAT, tanto del servidor como de las extensiones, se debe hacer manualmente.

Es necesario realizar esta configuración para indicarle al servidor que no utilice la información de direccionamiento procedente de los mensajes SDP de los clientes SIP, sino la dirección IP y puerto de donde procede el mensaje. Igualmente, es necesario especificarle qué extensiones pueden ser accesibles desde Internet para que éste rellene correctamente su información de direccionamientos en los paquetes SDP.

5.1.1.1 Configuración de extensiones

La configuración necesaria, para que las extensiones puedan ser accesibles desde el exterior, se lleva a cabo mediante la interfaz web de Elastix con la herramienta “PBX Configuration”, que se trata de una herramienta incluida en FreePBX, en el apartado “Extensions”. Los únicos parámetros que se han de configurar son `nat=yes`, que indica que hay NAT entre el teléfono SIP y el servidor Asterisk, y `qualify=yes`, que se explicará a continuación.

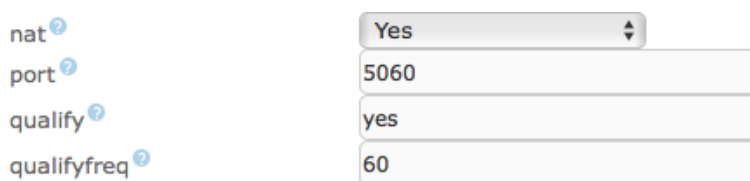
El parámetro `nat` sólo es necesario especificarlo cuando se trabaja con clientes SIP que no están en la misma red que el servidor. Este parámetro permite varios funcionamientos según sus valores:

- La opción `nat=no|rfc3581` es la opción que por defecto está configurada. Significa que no hay NAT entre el cliente y el servidor o que fuerza el comportamiento según la RFC3581. Esta opción es una solución híbrida, ya que el servidor coge la dirección IP de la cabecera de red (cabecera IP) y el puerto indicado en el mensaje SDP para enviar tráfico RTP. Asimismo, esta opción deshabilita el soporte RTP simétrico, es decir, un cliente SIP no usa el mismo puerto para enviar y recibir el flujo de datos. Sin embargo, este comportamiento no es deseable en muchos casos, por ejemplo, cuando el cliente está ubicado detrás de un NAT. En este caso, la respuesta no atravesará el NAT debido a que no coincidirá con la vinculación dirección IP/puerto establecida en la solicitud.
- La opción `nat = yes` es la combinación de `route` más el modo `rfc3581`. Este valor hace que Asterisk ignore siempre la información de direccionamiento de las cabeceras SDP del cliente y envíe los mensajes RTP a la dirección IP y al puerto desde donde se recibió el primer mensaje RTP. En nuestro caso, es la opción más conveniente.

Cabe destacar que, con la configuración del parámetro `nat=yes`, el cliente SIP no recibirá audio entrante hasta que Asterisk no haya recibido audio de ese cliente, ya que no sabe a qué dirección IP/puerto tiene que enviar dicho tráfico.

El parámetro `qualify` hace que Asterisk compruebe periódicamente la conexión con el dispositivo enviando mensajes SIP OPTIONS para que las sesiones UDP se mantengan y las traducciones de direcciones no se eliminen del cortafuegos. Si la conexión expirase, Asterisk no tendría forma de iniciar la llamada hacia el dispositivo.

Este parámetro puede tomar tres valores `xxx|no|yes` donde `xxx` es el número de milisegundos entre comprobaciones, `no` indica que no se comprueba si el dispositivo está disponible y el valor `yes` que establece que el tiempo entre comprobaciones por defecto sea 2 segundos. En nuestro caso, la opción `yes` es suficiente, ya que se comprueba la disponibilidad del dispositivo y no sobrecarga la red con mensajes SIP OPTIONS. Este parámetro, como ya se ha mencionado, es usado en conjunto con el parámetro `nat=yes`.



The image shows a configuration interface for NAT extensions. It consists of four rows, each with a parameter name on the left and a corresponding value in a text input field on the right. The parameters and their values are: `nat` with a dropdown menu set to 'Yes', `port` with the value '5060', `qualify` with the value 'yes', and `qualifyfreq` with the value '60'. Each parameter name has a small question mark icon next to it.

| | |
|--------------------------|------|
| <code>nat</code> | Yes |
| <code>port</code> | 5060 |
| <code>qualify</code> | yes |
| <code>qualifyfreq</code> | 60 |

Figura 11: Configuración NAT extensiones

5.1.1.2 Configuración del servidor

La configuración del servidor Asterisk para que rellene correctamente la información de direccionamiento de los mensajes SDP también se realiza mediante la interfaz web de Elastix. En la interfaz web, esta configuración se realiza dentro de la herramienta “PBX Configuration” en la pestaña “Settings” → “Asterisk SIP Settings”, disponible en “Unembedded FreePBX”. El valor de los parámetros de configuración que se han de asignar son los siguientes:

```

nat=yes
externhost=193.147.162.130
localnet=172.16.16.0/255.255.255.0
          193.147.162.128/255.255.255.224

```

Con esta configuración Asterisk utiliza la dirección IP definida en el parámetro `externip` para las llamadas entre clientes que están detrás de un NAT, es decir, para los clientes que estén accediendo al sistema de telefonía desde el exterior de la red del Departamento. A su vez utiliza la dirección local para los clientes que estén ubicados en las subredes locales del Departamento, conocidas por Asterisk mediante el parámetro `Local Networks`.

NAT Settings

NAT [?] yes no never route

IP Configuration [?] Public IP Static IP Dynamic IP

External IP [?]

Local Networks [?]

/

/

Figura 12: Configuración NAT del servidor

Con la configuración de estos parámetros siempre habrá un canal de comunicación entre Asterisk y el cliente SIP. Asterisk utilizará la dirección IP externa para rellenar el campo de información de direccionamiento del mensaje SDP para la comunicación con extensiones externas.

5.1.2 Problema de audio

Tal y como se ha mencionado, los mensajes SDP contienen información sobre los puntos finales de la conexión necesaria para permitir la comunicación de media entre ambos; esta información es rellena de acuerdo a lo que los extremos saben sobre sí mismos. Es por esto que, si el cliente SIP está detrás de un NAT, la información introducida en esos campos no será la correcta, lo que provocará que el tráfico RTP nunca llegue a su destino.

La siguiente figura muestra el campo del mensaje SDP del agente de usuario donde se indica la dirección IP donde éste quiere recibir el tráfico RTP. Como se puede observar, se trata de una dirección IP privada que no es encaminable desde Internet.

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|----------------|----------------|----------|--------|--|
| 68 | 9.734670 | 46.222.157.218 | 172.16.16.64 | SIP/SDP | 60 | Request: INVITE sip:46@193.147.162.130 |
| 69 | 9.736581 | 172.16.16.64 | 46.222.157.218 | SIP | 488 | Status: 100 Trying |
| 71 | 9.892841 | 172.16.16.64 | 217.217.55.150 | SIP/SDP | 896 | Request: INVITE sip:46@217.217.55.150:5060;t |

```

▶ Frame 68: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
▶ Ethernet II, Src: Dell_Ba:ee:3d (00:13:72:8a:ee:3d), Dst: HewlettP_3b:70:e8 (44:1e:a1:3b:70:e8)
▶ Internet Protocol Version 4, Src: 46.222.157.218, Dst: 172.16.16.64
▶ User Datagram Protocol, Src Port: 43127, Dst Port: 5060
▼ Session Initiation Protocol (INVITE)
  ▶ Request-Line: INVITE sip:46@193.147.162.130 SIP/2.0
  ▶ Message Header
  ▼ Message Body
    ▼ Session Description Protocol
      Session Description Protocol Version (v): 0
      ▶ Owner/Creator, Session Id (o): 45 3800 772 IN IP4 10.38.54.7
      Session Name (s): Talk
    ▶ Connection Information (c): IN IP4 10.38.54.7
    ▶ Bandwidth Information (b): AS:380
  
```

Figura 13: Mensaje SDP

En este tipo de escenarios, si no se lleva a cabo correctamente la configuración NAT, puede llevar a la ausencia de audio en las llamadas SIP externas, en otras palabras, que no haya tráfico de audio RTP cuando uno de los clientes está accediendo al sistema de telefonía desde el exterior de la red, es decir, desde Internet.

La configuración del NAT, tanto en el servidor como en las extensiones, soluciona el problema de encaminamiento de audio. Del mismo modo que el cliente SIP ve la dirección pública y el puerto correcto hacia donde tiene que enviar el tráfico RTP en el mensaje SDP, el servidor podrá enviar paquetes RTP basándose en la dirección IP y puerto desde donde ha recibido el primer mensaje de audio, incluso aunque el cliente haya rellenado incorrectamente la información de direccionamiento. Esto es posible gracias a la configuración del parámetro `nat=yes` que ignora todos esos campos de direccionamiento del mensaje SDP referentes al tráfico de media.

Es relativamente fácil detectar que los problemas en una llamada son de audio. Con *softphones* como **Linphone** o directamente capturando el tráfico de la red con **Wireshark**, se puede observar si los clientes SIP envían tráfico RTP, pero no reciben ningún flujo de audio. Sin embargo, sí reciben la señalización SIP correctamente.

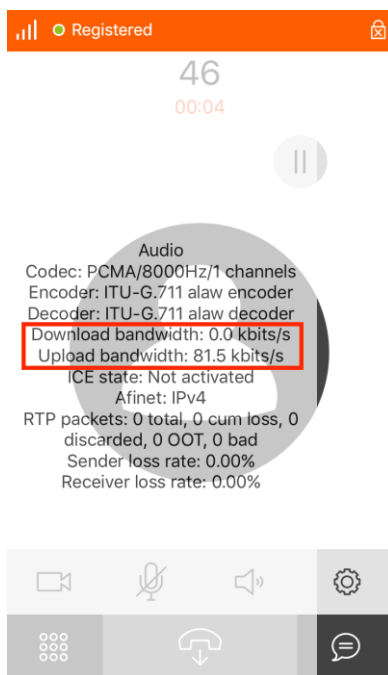


Figura 14: Ausencia de Audio en Linphone

5.2 Fail2ban

Una vez instalado el paquete **Fail2ban** (para más información véase el [ANEXO A. Guía De Instalación De Fail2ban](#)), se debe configurar el fichero `jail.conf` rellenando los parámetros `ignoreip`, `bantime`, `maxretry` y `findtime` en la sección `[Default]`, de forma que sean válidos para todos los servicios que **Fail2ban** examine.

Con estos parámetros se indica que las direcciones IP que se desea que no estén prohibidas (`ignoreip`) sean la dirección IP del servidor `trajano.us.es`, la subred de direccionamiento privado, puesto que es donde se encuentran los clientes SIP internos, y la subred local.

Debido a que el servidor de VoIP del Departamento se reinicia todos los días para evitar su degradación, se ha establecido un periodo de bloqueo de direcciones IP (`bantime`) de 10 horas (36000s), de forma que un cliente malicioso solo pueda realizar un máximo 3 ataques diarios. También, se ha dispuesto en 10 horas el espacio de tiempo en el que deben ocurrir todos los intentos de acceso al servidor (`findtime`).

Para activar el análisis y monitorización de Asterisk, se debe introducir en el fichero `jail.conf` dentro de la sección `[Default]` y justo antes de la sección `[ssh-iptables]` la sección `[asterisk-iptables]`.

En esta sección se establece un máximo de 5 intentos de acceso fallidos y se indica el uso de un fichero propio de registro denominado “`fail2ban`” (`logpath`), ubicado en el directorio `/var/log/asterisk`.

La configuración del parámetro `maxretry` en esta sección indica que éste sólo afecta a las reglas de análisis establecidas para Asterisk.

Una vez puesta en marcha la herramienta **Fail2ban**, ésta creará y añadirá una cadena al cortafuegos por cada servicio que analice, permitiendo así rechazar las direcciones IP con signos maliciosos. Por ello, no se debe olvidar que antes de iniciarla es necesario arrancar **iptables** en el servidor.

5.3 Cortafuegos

A continuación se detallarán las reglas introducidas en los cortafuegos de red y de aplicación del segmento de red del Departamento. Estas reglas permitirán sólo el acceso al sistema de determinados agentes de usuario, evitando así escaneos de puertos, tráfico SIP no deseado en las subredes internas e intentos de llamadas maliciosas.

5.3.1 Cortafuegos de aplicación

Analizar todos los paquetes que llegan al cortafuegos en busca de una cadena que se corresponda con el agente de usuario en cuestión es algo tedioso y consume mucha carga de procesamiento. Por este motivo, se ha implementado un algoritmo para gestionar el tráfico introduciendo reglas **iptables**. De esta manera, se reduce la carga de procesamiento haciendo que no todos los paquetes sean procesados por todas las reglas.

El algoritmo es el siguiente:

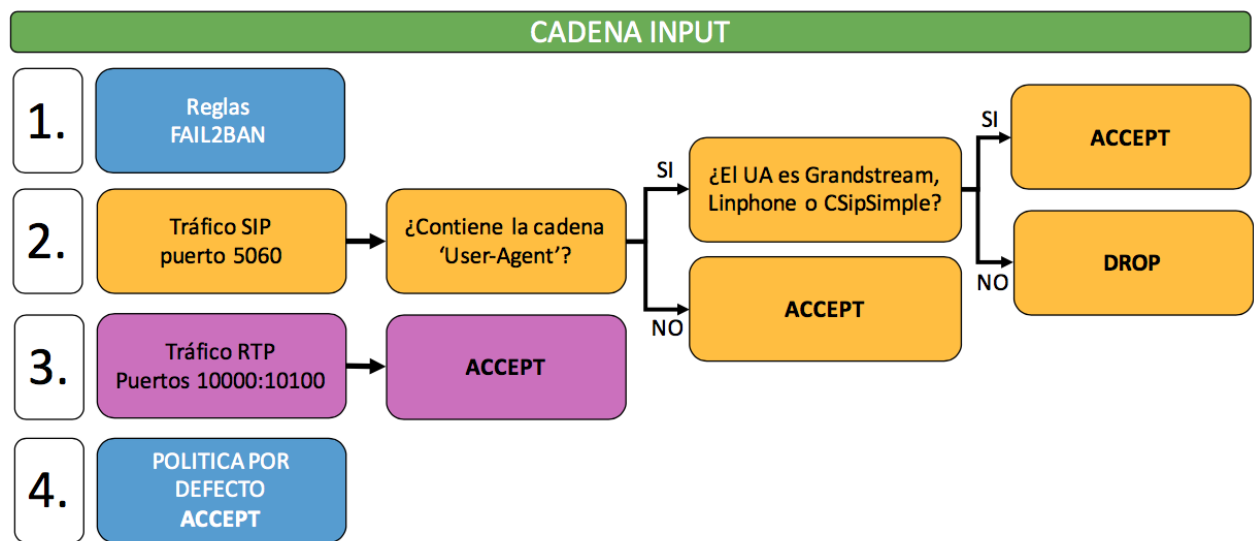


Figura 15: Algoritmo del cortafuegos de aplicación

Para implementar este algoritmo, se han creado tres cadenas **iptables**, una para el tráfico de señalización SIP, otra para el de audio y otra que será referenciada desde la cadena SIP.

#Creamos las cadenas nuevas

```
iptables -N SIP
iptables -N RTP
iptables -N UA
```

Debido a que todo el tráfico de telefonía va dirigido al servidor Asterisk, que es donde está instaurado el cortafuegos, todas estas cadenas serán referenciadas desde la cadena INPUT de la tabla FILTER.

#Cadena INPUT

```
iptables -A INPUT -p udp --dport 5060 -j SIP
iptables -A INPUT -p tcp --dport 5060 -j SIP
iptables -A INPUT -p udp --dport 10000:10100 -j RTP
```

Con las reglas introducidas en esta cadena se consigue que todo el tráfico con destino al puerto de señalización SIP sea procesado por la cadena SIP y todo el que vaya a los puertos de audio, por la cadena RTP (más adelante se hablará de la cadena UA)

A continuación se muestran las reglas de procesamiento de paquetes de cada una de las cadenas creadas:

```
#RTP
iptables -A RTP -j ACCEPT

#SIP
iptables -A SIP -m string --string 'User-Agent' --algo kmp -j UA
iptables -A SIP -j ACCEPT

#UA
iptables -A UA -m string --string 'Grandstream' --algo kmp -j ACCEPT
iptables -A UA -m string --string 'Linnphone' --algo kmp -j ACCEPT
iptables -A UA -m string --string 'CSipSimple' --algo kmp -j ACCEPT
iptables -A UA -m string --string 'CyberData 3x4 Keypad Intercom' --algo kmp -j
ACCEPT
iptables -A UA -j DROP
```

La cadena SIP hace referencia a la cadena UA (*user-agent*). Las reglas introducidas permiten la comprobación de la existencia de una cadena de texto “*user-agent*” que identifica al agente de usuario que realiza la comunicación. Si el paquete procesado contiene esa cadena de texto será desviado a la cadena UA. Si, por el contrario, no la contiene significará que se trata de mensajes de respuesta provisionales del servidor (100 Trying, 180 Ringing...) que indican que la llamada ya ha sido iniciada, con lo que el tráfico deberá ser aceptado.

Existen numerosos agentes de usuario maliciosos. Algunos de ellos son los siguientes: Sipcli, SIPVicious, sip-scan, sipsak, sundayaddr, friendly-scanner, iWar, SIVus, Gulp, sipv, smap, friendly-request, VaxIPUserAgent, VaxSIPUserAgent, siparmyknife... sería muy costoso introducir una regla para cada uno de ellos. Resulta más fácil poner una regla que permita sólo los agentes de usuario empleados en el Departamento.

En la cadena UA se rechazan todos los agentes de usuario que no sean los siguientes:

- Los únicos *softphones* permitidos en el Departamento: **Linnphone** y **CSipSimple**.
- Los teléfonos IP (agente de usuario denominado Granstream).
- El interfono IP (agente de usuario denominado Cyberdata).

Para permitir estos agentes de usuario se ha hecho uso del módulo *string* de **iptables**.

A la hora de introducir los agentes de usuario es necesario tener especial cuidado, debido a que la herramienta **iptables** distingue entre mayúsculas y minúsculas. Esto quiere decir que si un paquete contiene la cadena de texto “Cyberdata”, según las reglas introducidas, será rechazado mientras que con la cadena de texto “CyberData” sería aceptado.

Finalmente, con la regla introducida en la cadena RTP se permite todo el tráfico de audio sin importar su origen o destino, ya que para que se envíe tráfico de estas características es necesario haber establecido la llamada previamente, siendo los paquetes de señalización correspondientes a esa llamada procesados por las otras cadenas.

Es posible eliminar esta última cadena, ya que con ella lo único que obtenemos es que los paquetes de audio no sean procesados por el resto de reglas de la cadena INPUT, permitiendo así disminuir el retardo en el audio de la llamada.

El servidor de VoIP está programado para que se reinicie a diario, dado que el uso continuado sin reinicios periódicos podría provocar la degradación del sistema. Con cada reinicio se borran todas las reglas del cortafuegos introducidas, incluidas las dinámicas incluidas por **Fail2ban**.

El borrado de las reglas introducidas por **Fail2ban** no supone un problema, ya que este las va a seguir introduciendo dinámicamente; sin embargo, podría resultar farragoso tener que introducir diariamente el resto de las reglas, orientadas a aceptar tráfico sólo de determinados agentes de usuario.

La solución al problema es guardar las reglas del cortafuegos (a excepción de las reglas incluidas por **Fail2ban**, considerando que son siempre las mismas) y recargarlas al arrancar el sistema. Para guardar las reglas se debe ejecutar el siguiente comando:

```
service iptables save
```

Una vez guardadas las reglas, se debe modificar el fichero iptables-config ubicado en /etc/sysconfig/ para indicar al sistema operativo que se recarguen las reglas después de un reinicio.

Además, en este fichero se pueden configurar otros parámetros como contadores, estado...

/etc/sysconfig/iptables-config

```
# Value: yes|no, default: no
# Saves all firewall rules to /etc/sysconfig/iptables if firewall gets
# restarted.
iptables_save_on_restart="yes"

# Save (and restore) rule and chain counter.
# Value: yes|no, default: no
# Save counters for rules and chains to /etc/sysconfig/iptables if
# 'service iptables save' is called or on stop or restart if SAVE_ON_STOP or
# SAVE_ON_RESTART is enabled.
iptables_save_counter="no"

# Numeric status output
# Value: yes|no, default: yes
# Print IP addresses and port numbers in numeric format in the status output.
iptables_status_numeric="yes"
```

```
# Verbose status output
# Value: yes|no, default: yes
# Print info about the number of packets and bytes plus the "input-" and
# "outputdevice" in the status output.
IPTABLES_STATUS_VERBOSE="no"

# Status output with numbered lines
# Value: yes|no, default: yes
# Print a counter/number for every rule in the status output.
IPTABLES_STATUS_LINENUMBERS="yes"

# Reload sysctl settings on start and restart
# Default: -none-
# Space separated list of sysctl items which are to be reloaded on start.
# List items will be matched by fgrep.
#IPTABLES_SYSCTL_LOAD_LIST=".ip_contrack .bridge-nf"
```

5.3.2 Cortafuegos de red

Debido a que el tráfico de red en el router frontera del Departamento es elevado y existen multitud de reglas en este cortafuegos para otros servicios, se quiere evitar que todos los paquetes destinados al servicio de telefonía tengan que ser procesados por todas las reglas **iptables**. Para ello, al igual que en el cortafuegos de aplicación, se han creado tres cadenas **iptables** para el tráfico SIP y RTP.

#Creamos las cadenas nuevas

```
iptables -N SIP
iptables -N RTP
iptables -N UA
```

Para priorizar de alguna forma el tráfico de voz y señalización SIP, manteniendo una cierta calidad de servicio (*Quality of Service* - QoS), se han introducido las reglas referentes al sistema de telefonía al principio de la cadena FORWARD de la tabla FILTER, haciendo éstas referencia a las cadenas creadas anteriormente:

Cadena FORWARD

```
iptables -I FORWARD -p udp --dport 10000:10100 -j RTP
iptables -I FORWARD -p tcp --dport 5060 -j SIP
iptables -I FORWARD -p udp --dport 5060 -j SIP
```

De este modo, las primeras reglas serán las destinadas al servicio de telefonía. Así se permite que sólo los paquetes con destino a los puertos de audio y señalización se deriven a las cadenas creadas, siendo el resto

de paquetes procesados por las reglas de la cadena FORWARD restantes.

La única diferencia entre estas reglas y las reglas introducidas en el cortafuegos de aplicación es la cadena donde van a ser procesadas. En el caso del cortafuegos de aplicación son introducidas en la cadena INPUT, porque todo el tráfico va hacia el servidor, y en el caso del cortafuegos de red en la cadena FORWARD, porque se trata de un router más en el camino.

A continuación se muestran las reglas de procesamiento de paquetes de cada una de las cadenas creadas:

```
#Cadena RTP
iptables -A RTP -j ACCEPT

#Cadena SIP
iptables -A SIP -m string --string 'User-Agent' --algo kmp -j UA
iptables -A SIP -j ACCEPT

#Cadena UA
iptables -A UA -m string --string 'Linphone' --algo kmp -j ACCEPT
iptables -A UA -m string --string 'CSipSimple' --algo kmp -j ACCEPT
iptables -A UA -j DROP
```

La desigualdad con respecto al cortafuegos de red es la cadena UA, que rechaza a todos los agentes de usuario que no sean **CSipSimple** y **Linphone**, los únicos *softphones* permitidos en el Departamento. En este caso, no es necesario permitir los agentes de usuario Granstream o Cyberdata, porque estos acceden al sistema de telefónica desde la red interna del Departamento y no desde el exterior.

Al igual que en el cortafuegos de aplicación, es posible eliminar la cadena RTP.

Seguidamente se muestra en un diagrama todas las cadenas **iptables** del router frontera de la red del Departamento por las que puede pasar un paquete dependiendo de su destino:

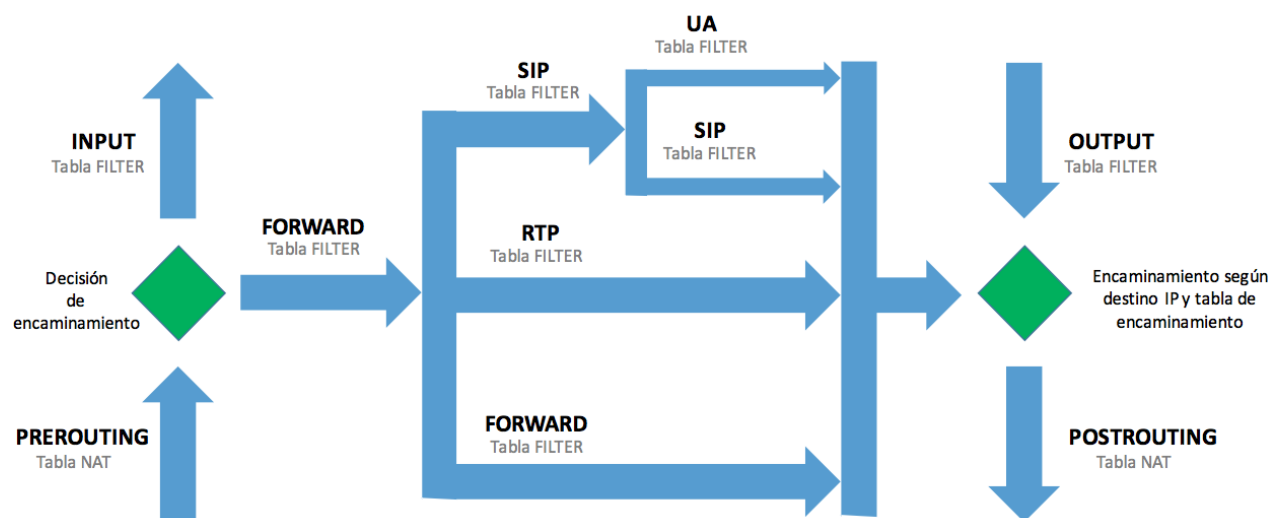


Figura 16: Nuevo camino que sigue un paquete IP en el cortafuegos de red

Una vez establecidas las reglas **iptables**, es necesario guardarlas de modo que, cuando el equipo se reinicie, estas reglas se mantengan. El router frontera contiene todas sus reglas en un *script* denominado `rc.firewall`, ubicado en el directorio `/root/` que es llamado al arrancar el sistema. Se ha editado este *script* para que llame a otros dos *scripts*, `nat-sip.sh` y `drop-ua.sh`, con el fin de que se introduzcan las nuevas reglas.

El *script* `nat-sip.sh` contiene las reglas necesarias para realizar el DNAT; mientras que el `drop-ua.sh`, las reglas mencionadas que permiten crear las nuevas cadenas y las reglas para aceptar sólo determinados agentes de usuario.

Es cierto que una vez introducidas estas reglas en el cortafuegos de red no debería ser necesario introducirlas en el cortafuegos de aplicación. Sin embargo, no se puede perder de vista la posibilidad de un ataque originado desde el interior de la red, por lo que finalmente se ha decidido mantener estas reglas en ambos cortafuegos.

5.4 Establecimiento de las configuraciones seguras

Los parámetros `alwaysauthreject` y `allowguest` en Elastix vienen configurados por defecto a los valores deseados. Se encuentran en el archivo `sip_general_additional.conf` del directorio `/etc/asterisk/`.

Sin embargo, el parámetro `insecure` no está configurado por defecto. Éste puede ser configurado a través de la interfaz web de Elastix con la herramienta “PBX Configuration” en “Unembedded FreePBX”, posicionándose en la pestaña “Settings” → “Asterisk SIP Settings”:

| Parameter | Value |
|-------------|--------------|
| tcpenable | yes |
| tcpbindaddr | 0.0.0.0/5060 |
| realm | asterisk |
| allowguest | no |

[Add Field](#)

Figura 17: Elastix. Configuraciones seguras

Los parámetros que pueden ser configurados en esta sección son los denominados parámetros de configuración general SIP.

Por otra parte, el parámetro `type` se configura para cada extensión por separado desde “PBX Configuration” en la sección “Extensions”.



Figura 18: Elastix. Type peer

Para evitar lo engorroso que sería realizar este cambio en todas las extensiones del sistema de telefonía del Departamento por separado, se ha realizado a través de la base de datos de Elastix. Esta base de datos dispone de una interfaz web accesible desde la dirección IP del servidor (<https://172.16.16.64/phpmyadmin/>) o desde la terminal de comandos ejecutando lo siguiente:

```
mysql -u asteriskuser -p
passwd
mysql> use asterisk;
```

Los parámetros de configuración de extensiones y de configuración general SIP se encuentra en la tabla “sip” de la base de datos “asterisk”.

La tabla “sip” contiene cuatro atributos: el **ID** que corresponde al número de extensión, **keyword** que identifica el parámetro de configuración, **data** que indica el valor del parámetro y **flags**.

Con la siguiente instrucción se realiza el cambio del valor del parámetro `type` para todas las extensiones:

```
UPDATE `sip` SET data=peer WHERE keyword='type';
```

Finalmente, se ha configurado el parámetro `nat` para que las extensiones internas (pertenecientes a los teléfonos IP) no sean accesibles desde el exterior del segmento de red del Departamento. Para ello, se ha ejecutado la siguiente sentencia:

```
UPDATE 'sip' SET data='no' WHERE keyword='nat' AND id>20 AND id<40
```

5.5 Cambio de contraseña de los teléfonos IP

Para realizar el cambio de contraseñas de los teléfonos IP del Departamento es necesario la realización de dos pasos:

- Cambiar la contraseña de las extensiones en el servidor.
- Modificar los ficheros de configuración que los teléfonos se descargan vía TFTP cuando se inician para indicarles su nueva contraseña.

De igual forma que el parámetro `type`, las contraseñas de las extensiones SIP en el servidor de VoIP se configuran por separado en el apartado de cada extensión dentro de la interfaz web. Para evitar cambiarlas una a una, se ha ejecutado la siguiente sentencia en la base de datos de Elastix:

```
UPDATE `sip` SET data=CONCAT('xxxxxxxxxx', id) WHERE data LIKE 'abc%' AND keyword='secret';
```

donde 'xxxxxxxxxx' es la nueva contraseña e 'id' es el número de cada extensión.

Una vez configurada la nueva contraseña en el servidor de VoIP es necesario cambiar el archivo de configuración `reconf.sh`, que genera los ficheros de configuración de los teléfonos IP, estableciendo la nueva contraseña.

5.6 Creación de extensiones para el nuevo plan

Para facilitar la configuración de las nuevas extensiones se han creado todas de forma individual con la configuración por defecto desde la interfaz web. Después se han modificado los parámetros de relevancia desde la base de datos.

Seguidamente se muestran las sentencias empleadas para la configuración de las nuevas extensiones:

- Establecimiento del parámetro `type`:

```
UPDATE `sip` SET data='peer' WHERE keyword='type';
```

- Establecimiento de contraseña (`secret`):

```
UPDATE sip SET data=CONCAT('xxxxxxxxxx',id) WHERE keyword='secret' AND id>120 AND id<=135
```

- Establecimiento del parámetro `nat`, que hace que estas nuevas extensiones puedan ser accesibles desde el exterior de la red del Departamento:

```
UPDATE `sip` SET data='yes' WHERE keyword='nat' AND id>120 AND id<=135
```

6 PROBLEMAS FRECUENTES

*Si los problemas llegan cuando menos te lo esperas, tal vez la clave sea esperarlos siempre.
- Cormac McCarthy -*

Este capítulo está dedicado a la acotación de fallos. En él se describen los problemas más frecuentes y sus soluciones a la hora de hacer accesible desde Internet un servidor de telefonía IP y dotar de seguridad el entorno de éste.

6.1 Se ha hecho NAT en el servidor Asterisk y no hay audio

Este problema es uno de los más importantes que se han resuelto en este proyecto. La solución se detalla en el apartado [5.1.2 Configuración NAT en Asterisk](#).

Si una vez realizada la configuración NAT en el servidor y en las extensiones el problema sigue existiendo, deberá comprobar lo siguiente:

- Los códecs.
- Los puertos de audio.

Ambos, *softphones* o teléfonos IP, deben disponer de al menos un códec en común con el servidor Asterisk para la realización de la llamada. Si no es así, añada los códecs necesarios desde los ajustes de audio de su *softphone* o en "Asterisk SIP Settings" desde "Unembedded FreePBX" en el servidor.

En el caso de que el parámetro `canreinvite` esté activado en el servidor, deberá comprobar que ambos *softphones* tiene códecs en común, ya que en este caso el tráfico de audio no pasa por Asterisk, la comunicación de audio es de extremo a extremo.

Tampoco debe olvidarse de indicarle al servidor qué puertos de audio debe utilizar (deben ser los mismos que los que ha abierto en el cortafuegos para hacer DNAT). Estos ajustes se encuentran en "Asterisk SIP Settings" :



Figura 19: Asterisk. Ajuste de puertos de audio

6.2 La aplicación de telefonía no se registra

Este problema aparece cuando un primer registro falla y el cliente de telefonía no permite, por un fallo de implementación, un segundo registro.

La única forma de conseguir que el usuario pueda registrarse de nuevo es borrando la cuenta y creándola de nuevo con los mismos datos.

En el caso de **Linphone** de escritorio es más complicado, ya que es necesario cerrar completamente la aplicación, borrar los archivos ocultos que ésta genera en el directorio del usuario y, posteriormente, volver a crear la cuenta. Para borrar los archivos ocultos desde la terminal de comandos bastaría con ejecutar la siguiente sentencia:

```
rm .linphone*
```

Para configurar correctamente estas aplicaciones véase el [ANEXO B. Configuración de Softphones](#).

6.3 Ha introducido mal la contraseña de la cuenta SIP y no puedo registrarse

Si ha introducido mal la contraseña más de 5 veces, la herramienta **Fail2ban** le habrá bloqueado la dirección IP del dispositivo desde donde esté intentando registrarse. Si captura el tráfico con **Wireshark**, le aparecerán mensajes **403 forbidden** en respuesta a su solicitud de registro.

Puede comprobar si su dirección IP ha sido bloqueada ejecutando el siguiente comando en el servidor Asterisk:

```
iptables -L -n
```

Si su dirección IP ha sido bloqueada, aparecerá en la cadena fail2ban-ASTERISK.

La solución a este problema es cambiar la dirección IP del dispositivo, ya que desde la dirección IP que ha estado intentando registrarse estará bloqueada durante 10 horas. Si está usando datos móviles, basta con reiniciar el Smartphone. Si está conectado a través de WiFi, deberá reiniciar el router.

Fail2ban lee de los archivos de registro durante un tiempo determinado (especificado mediante un parámetro de configuración). Aunque reinicie la herramienta, el temporizador no se reactiva, de este modo sigue

leyendo los registros de las últimas horas o minutos (según el temporizador). Es por ello que, si no cambia la dirección IP de su dispositivo, no podrá acceder al sistema de telefonía durante las horas establecidas en la herramienta.

Otra solución sería reiniciar el servidor Asterisk, ya que este no guarda las direcciones introducidas por **Fail2ban**.

Debe recordar que **Fail2ban** permite configurar qué direcciones IP no quiere que sean bloqueadas o cuánto tiempo quiere que lo estén (para más información véase el [ANEXO A. Guía De Instalación De Fail2ban](#)).

6.4 No puede registrar su extensión desde una de sus subredes locales

Si desde la subred donde se encuentra el servidor Asterisk puede registrar su extensión, y sin embargo, desde otra subred local no, lo más probable es que haya olvidado introducir la subred local en el parámetro `Local Networks` de la configuración del servidor (para entrar en detalle véase el apartado de [Configuración NAT del servidor](#)). Este parámetro hace que Asterisk rellene los campos de información de direccionamiento (mensaje SDP) con la dirección IP privada para clientes situados en las subredes locales, mientras que, para el resto de Internet, usaría la dirección IP pública del NAT.

También debe tener en cuenta la arquitectura de su red para decidir con qué dirección IP debe Asterisk rellenar los mensajes SDP, que le permiten recibir correctamente el tráfico de audio.

6.5 Cuando inicia una llamada, al principio recibe audio del otro extremo pero después no

Tal como se ha mencionado en este proyecto, Asterisk no es compatible con el protocolo STUN, por tanto, es necesario desactivar esta opción de los *softphones*.

Cuando un *softphone* tiene activado el protocolo STUN no es capaz de rellenar correctamente la información de direccionamiento del mensaje SDP para el servidor, enviándole dos direcciones IP (la dirección pública con la que sale a Internet y la dirección privada que el router le da).

```
▼ Message Body
  ▼ Session Description Protocol
    Session Description Protocol Version (v): 0
    ▶ Owner/Creator, Session Id (o): 45 1069 1778 IN IP4 192.168.1.45
    Session Name (s): Talk
    ▶ Connection Information (c): IN IP4 192.168.1.45
    ▶ Bandwidth Information (b): AS:380
    ▶ Time Description, active time (t): 0 0
    ▶ Session Attribute (a): ice-pwd:7478308332a7512722c9672a
    ▶ Session Attribute (a): ice-ufrag:3e43c84c
    ▶ Session Attribute (a): rtcp-xr:rcvr-rtt=all:10000 stat-summary=loss,dup,jitt,TTL voip-metrics
    ▶ Media Description, name and address (m): audio 7230 RTP/AVP 96 97 98 99 0 8 18 101 100 102
    ▶ Connection Information (c): IN IP4 83.55.107.254
    ▶ Media Attribute (a): rtpmap:96 opus/48000/2
```

Figura 20: Problema STUN. Doble información de direccionamiento

Esto confunde a Asterisk, que no espera a recibir audio del cliente para conocer su verdadera información de direccionamiento, sino que envía inmediatamente el tráfico RTP a la dirección pública especificada en el mensaje SDP. Se producen entonces dos flujos de audio, uno con la dirección pública especificada en el mensaje SDP y otro con la dirección IP pública con la que el *softphone* envía su primer mensaje de tráfico RTP.

Debe recordarse que, con el parámetro `nat=yes` de la configuración del servidor, se permite a Asterisk enviar paquetes RTP a la dirección IP y puerto desde donde ha recibido el primer mensaje de audio del cliente, incluso si el cliente ha rellenado incorrectamente la información de direccionamiento.

Finalmente, sólo queda el flujo de audio correspondiente a la dirección especificada en el mensaje SDP. Esto explica por qué al principio el *softphone* sí recibe audio del otro extremo y, momentáneamente, deja de recibirlo. El cliente no recibe tráfico RTP del flujo iniciado por el servidor al no haber una correspondencia con los puertos que el cliente ha establecido para ello.

Para desactivar esta opción de los *softphones*, simplemente, hay que dejar vacío el campo “STUN server” de los ajustes de red.

6.6 Tiene un softphone que no deja de sonar en una subred con direccionamiento público

Por defecto los *softphones* tienen configurado el puerto estándar SIP (5060) para recibir y enviar tráfico SIP. El uso de este puerto no es el más recomendable, puesto que el cliente, al estar conectado a través de una dirección pública, está expuesto a los sondeos que se producen en Internet en busca de servidores de VoIP vulnerables (para más información véase el [ANEXO C. SIPVicious](#)).

Estos escáneres provocan el envío constante de mensajes INVITE a cualquier dirección IP que tenga abierto el puerto 5060, haciendo, en este caso, que los teléfonos no dejen de sonar.

Se recomienda cambiar en los *softphones* el puerto de señalización SIP. Para ello, solo hay que activar la opción “random” del puerto de escucha en los parámetros de configuración (como ayuda puede consultar el [ANEXO B. Configuración De Softphones](#)).

6.7 Guía de pasos a seguir ante un problema en el sistema de telefonía IP

6.7.1 Guía de resolución de problemas de tráfico SIP

A continuación se describirán los pasos a seguir para la resolución de problemas de tráfico de señalización SIP en un sistema de telefonía IP:

1. Compruebe que el tráfico SIP llega al servidor Asterisk. Para ello, capture tráfico con **Wireshark** en la subred con direccionamiento privado.
 - Si el tráfico SIP no llega al servidor, compruebe si llega al router que hace NAT.
 - Si el tráfico SIP llega por una las interfaces del router y éste no lo reenvía por la interfaz que debería, se trata de un problema de puertos. Deberá comprobar las reglas **iptables** encargadas de la traducción de direcciones.

- Si el tráfico SIP no llega a ninguna de las interfaces, posiblemente su cliente SIP no tenga salida a Internet.
- 2. Compruebe si la dirección IP del cliente SIP está bloqueada por **Fail2ban**.
 - Si está bloqueada, la solución se encuentra en el apartado [6.3](#).
- 3. Compruebe si el agente de usuario está permitido en el sistema de telefonía. Debe verificar que la cadena de texto “user-agent” de los mensajes SIP corresponde con la cadena de texto introducida en las reglas del cortafuegos (debe tener en cuenta las mayúsculas y minúsculas).
- 4. Compruebe que los dos cortafuegos reciben paquetes del agente de usuario en cuestión. Puede verse con el siguiente comando:

```
iptables -L -v -n
```

- Deberá observar si el contador de las reglas que hacen referencia a dicho agente de usuario está a cero.
- Si el contador está a cero, vuelva al paso anterior.
- 5. Borre y vuelva a crear la cuenta en su *softphone*. Solución detallada en el apartado [6.4](#).
- 6. Pruebe a intentar registrarse desde otra extensión.
 - Si desde otra extensión es posible registrarse, el problema está en la configuración de la extensión en el servidor.
- 7. Pruebe a registrarse desde otro dispositivo.
 - Si es posible, el problema estará en la configuración de los parámetros de la extensión en el *softphone*.
- 8. Capture tráfico con herramientas como **Wireshark** o **sngrep**, compruebe dónde se queda la comunicación y analice todos los paquetes.

6.7.2 Guía de resolución de problemas de tráfico RTP

A continuación se detallarán los pasos a seguir para la resolución de problemas de tráfico de audio RTP en un sistema de telefonía IP:

1. Compruebe que el tráfico RTP llega al servidor Asterisk. Para ello, capture tráfico con **Wireshark** en la subred con direccionamiento privado.
 - Si el tráfico RTP no llega al servidor, compruebe si llega al router que hace NAT.
 - Si el tráfico RTP llega por una de las interfaces del router y éste no lo reenvía por la interfaz que debería, se trata de un problema de puertos. Deberá comprobar las reglas **iptables** encargadas de la traducción de direcciones.
2. Compruebe las direcciones IP origen y destino de los paquetes.
 - Si el *softphone* está accediendo al sistema de telefonía desde el exterior, compruebe que el servidor nunca intenta enviar un paquete con dirección IP destino privada (con destino al *softphone*). Si es así, el problema está en la configuración NAT de las extensiones. Probablemente, esa extensión no pueda ser accesible desde el exterior.

- Compruebe que el servidor envía los mensajes RTP basándose:
 - En la dirección IP y puerto desde donde ha recibido el primer mensaje de audio del cliente en el caso de que el éste accediendo desde el exterior.
 - En la dirección de direccionamiento contenida en el mensaje SDP en el caso de que la extensión solo pueda ser accesible desde el interior del sistema de telefonía.
 - Compruebe que no tiene el problema: [Doble flujo RTP](#).
3. Pruebe a intentar realizar una llamada desde otra extensión.
 - Si es posible, el problema está en la configuración de la extensión en el servidor.
 4. Pruebe a intentar realizar una llamada desde otro dispositivo.
 - Si es posible, el problema estará en la configuración de los parámetros de la extensión en el *softphone*.
 5. Capture tráfico con **Wireshark**, analice todos los paquetes y observe con atención las direcciones IP y puerto de los paquetes RTP y en los mensajes SDP; concretamente, los campos que muestran la dirección IP y puerto donde el cliente espera el tráfico RTP.

7 CONCLUSIONES

No hay dificultad en comenzar; el problema es terminar.

- Henry James -

En este apartado se detallan las conclusiones a las que se ha llegado con la realización de este proyecto y se proponen futuras mejoras que podrían realizarse sobre el mismo, aumentando su funcionalidad o seguridad.

7.1 Conclusiones

En general, este proyecto permite a los miembros del Departamento usar el sistema de telefónica desde el exterior de la red del Departamento de forma segura a través de una aplicación o teléfono IP.

Actualmente existen numerosos puntos de ataque contra la tecnología VoIP. La solución adoptada cubre un número aceptable de vulnerabilidades y debilidades de la misma. Pese a que existen otras mejoras en la actualidad, no se han llegado a implementar, debido a que el *software* sobre el que se ha realizado el proyecto no las soporta.

Como medida de protección de la red interna se ha optado por el uso de una política de seguridad en el cortafuegos del router frontera basadas en **iptables** y por la incorporación de la herramienta **Fail2ban** en el servidor Asterisk, que añade un grado más de seguridad. La elección de estas medidas ha sido acertada, dado que poseen una sintaxis clara de configuración, existe una amplia documentación al respecto y con ella se ha evitado colocar equipos adicionales, como proxy o servidores VPN que aumentarían la latencia en las llamadas.

Tras la implementación de este proyecto cualquier miembro del Departamento podrá acceder al sistema de telefonía con su extensión sin ningún problema, siempre que utilice una aplicación *softphone* instalada en su ordenador o un teléfono IP. En el caso de utilizar una aplicación *softphone* en un *Smartphone*, las prestaciones serían las mismas, pero durante un tiempo establecido, debido a las limitaciones de las aplicaciones gratuitas. Esto no supone un problema si el usuario mantiene la aplicación en primer plano, dado que el registro se mantiene, cosa que no ocurre cuando la aplicación pasa a un segundo plano.

Durante la realización de este proyecto sólo se han permitido dos agentes de usuario, **Linphone** y **CSipSimple**. Sin embargo, sería sencillo permitir otros agentes, ya que no habría que alterar la configuración del servidor de VoIP ni las herramientas empleadas, bastaría con añadir nuevas reglas de **iptables** a los cortafuegos en los *scripts* correspondiente.

7.2 Líneas de continuación

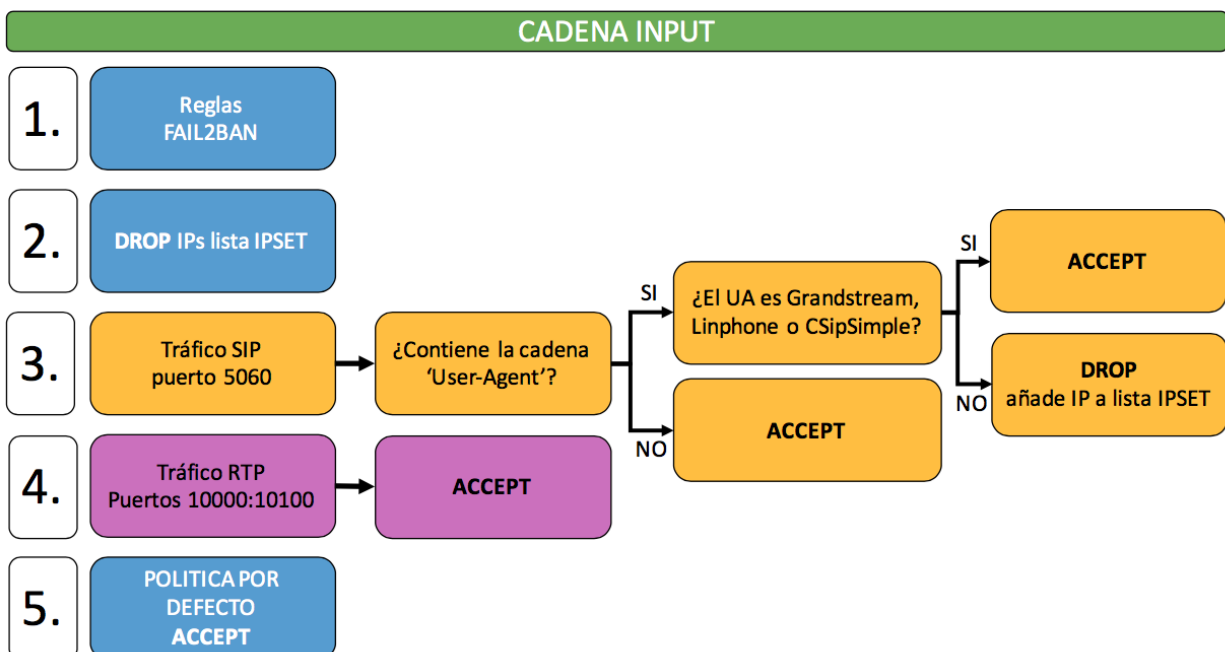
La implementación que se ha llevado a cabo en este proyecto cumple con la funcionalidad y requisitos especificados en éste. Sin embargo, debido al limitado tiempo de desarrollo y a la desactualización de *software* de algunos equipos, se pueden encontrar algunas mejoras que implantar en el sistema de telefonía del Departamento.

A continuación se detallan algunas de las mejoras que podrían llevarse a cabo, bien para solucionar otros problemas, bien para incrementar la seguridad en este sistema.

7.2.1 IPSET

Tal como se ha mencionado en este documento, analizar todos los paquetes que llegan al cortafuegos en busca de una cadena de texto que se corresponda con un agente de usuario determinado es algo tedioso y consume mucha carga de procesamiento. A pesar de haber implementado un algoritmo para la gestión del tráfico, la carga de procesamiento sigue siendo elevada. Se podría plantear una solución de mejora que haga uso de un módulo no muy común de **iptables**, el módulo **ipset**.

Este módulo permite crear una lista dinámica de direcciones IP que estén creando demasiado tráfico o que cumplan unas determinadas condiciones. Posteriormente permite aplicar a esa lista una política de seguridad (DROP, REJECT...). De esta forma, el algoritmo implementado en el apartado [5.3.1 Cortafuegos de aplicación](#) quedaría como sigue:



A continuación se muestra el *script* que implementa este algoritmo:

```
#!/bin/bash

#Creamos la lista dinamica de direcciones IP
ipset create myset hash:ip

#Creamos las cadenas nuevas
iptables -N SIP
iptables -N RTP
iptables -N UA

iptables -A INPUT -m set --match-set myset src -j DROP
iptables -A INPUT -p udp --dport 5060 -j SIP
iptables -A INPUT -p tcp --dport 5060 -j SIP
iptables -A INPUT -p udp --dport 10000:10100 -j RTP

#RTP
iptables -A RTP -j ACCEPT

#SIP
iptables -A SIP -m string --string 'User-Agent' --algo kmp -j UA
iptables -A SIP -j ACCEPT

#UA
iptables -A UA -m string --string 'Grandstream' --algo kmp -j ACCEPT
iptables -A UA -m string --string 'Linphone' --algo kmp -j ACCEPT
iptables -A UA -m string --string 'CSipSimple' --algo kmp -j ACCEPT
iptables -A UA -m string --string 'CyberData 3x4 Keypad Intercom' --algo kmp -j
ACCEPT

iptables -A UA -j SET --add-set myset src,dst
iptables -A UA -j DROP
```

Como se puede observar, el *script* es muy similar al descrito en el apartado mencionado. Con él se consigue que, cuando un paquete no provenga de los agentes de usuario permitidos en el sistema de telefonía, se introduzca su dirección IP origen en una lista dinámica (ipset), permitiendo posteriormente bloquearla.

De esta forma, cuando vuelva a llegar un paquete con esa misma dirección IP será bloqueado desde el primer momento sin necesidad de ser procesado por el resto de reglas.

Seguidamente se muestra el comando que permite ver las direcciones IP que han sido prohibidas:

```
ipset list myset
```

dónde `myset`, en este caso, es el nombre de la lista dinámica de direcciones IP.

El uso de este módulo de **iptables** sería válido tanto para el cortafuegos de red como para el cortafuegos de aplicación en un segmento de red como el del Departamento. Sin embargo, esta solución no ha podido llevarse a cabo debido a la desactualización del router frontera de la red y del servidor de VoIP. Este módulo sólo está disponible a partir de la versión Debian Jessie o CentOS 6.

No obstante, esta solución ha sido probada en otro sistema de telefonía IP satisfactoriamente, donde el servidor de VoIP está alojado en un sistema operativo CentOS 7.

7.2.2 Autenticación basada en dos factores

Como se ha descrito en este proyecto, un sistema de autenticación basado en dos factores (2FA) consiste en la verificación en dos pasos del proceso de inicio de sesión. Un paso está basado en “algo” que el usuario sabe, como su usuario y contraseña y el otro en “algo” que el usuario tiene, como podrían ser certificados.

Se puede añadir una mejora a este proyecto usando mecanismos de autenticación basado en dos factores. Para ello, se podría emplear SIPS (*SIP over TLS*). Esto impediría el acceso de usuarios no autorizados al servidor de VoIP. Sin embargo, no sería una solución válida por sí sola, ya que seguiría existiendo tráfico SIP no deseado entre las subredes del segmento de red del Departamento.

Realmente llevar a cabo esta solución es algo complejo, ya que se tienen que seguir los siguientes pasos:

1. Creación de un certificado para el servidor Asterisk.
2. Cambio en los ajustes de configuración general SIP.
3. Configuración de los clientes para usar TLS.
4. Creación de los certificados de los clientes e introducción de estos en el dispositivo.

Para la creación de los certificados, Asterisk cuenta con una herramienta denominada `ast_tls_cert` ubicada en el directorio `/usr/share/doc/asterisk-11.20.0/contrib/scripts`. Esta utilidad es válida tanto para la creación de certificados de los clientes como los del servidor.

Con esta solución, la torre de protocolos del plano de control del servidor de VoIP quedaría así:

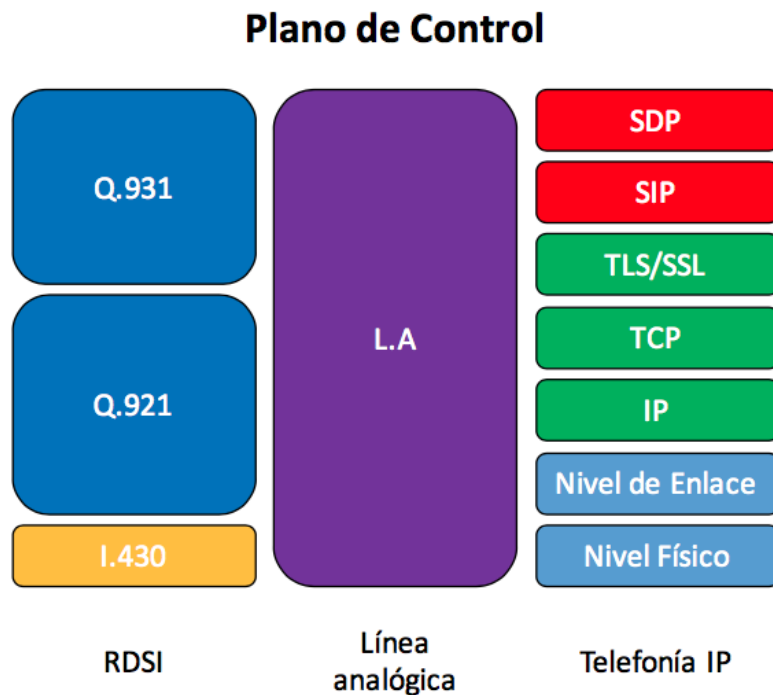


Figura 21: Torre del plano de control de un sistema de telefonía de autenticación basada en dos factores

El inconveniente de esta solución es que no todos los *softphones* soportan estos mecanismos de autenticación, la mayoría son de pago. Además, ningún mecanismo asegura que todas las entidades participantes en una conexión utilicen TLS.

7.2.3 Cifrado del audio RTP

Los ataques de escucha (*eavesdropping*) permiten capturar la señalización SIP y el flujo de audio de una llamada dejando la privacidad del usuario comprometida. Se podría plantear una solución a este problema cifrando el audio con un protocolo como SRTP (*Secure Real-time Transport Protocol* definido en RFC 3711).

SRTP es un protocolo de voz que añade confidencialidad, autenticación de mensajes y protección ante la reproducción del audio. Debido a que el tráfico RTP tiene como factor crítico el retardo de tiempo, SRTP proporciona un alto rendimiento y una baja expansión de paquetes.

La capa SRTP que se encuentra justo debajo del RTP en la torre de protocolos, se encarga de interceptar el paquete RTP, modificarlo y enviarlo a la capa UDP.

Con la implantación de este protocolo en el sistema de telefonía del Departamento la torre de protocolos de la capa de usuario del servidor de VoIP quedaría como sigue:

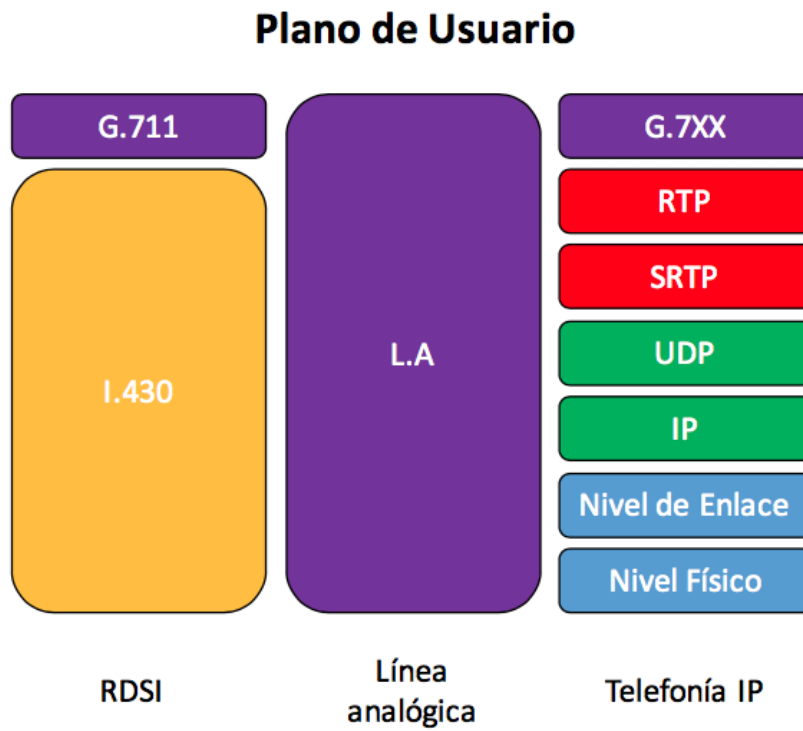


Figura 22: Torre del plano de usuario de un sistema de telefonía con cifrado de audio

ANEXOS

ÍNDICE DE ANEXOS

| | |
|--|-----------|
| ANEXO A. Guía De Instalación De Fail2ban | 65 |
| A.1 <i>Herramienta iptables</i> | 65 |
| A.2 <i>Configuración de Asterisk para guardar los logs</i> | 65 |
| A.3 <i>Configuración de fail2ban</i> | 66 |
| A.4 <i>Arranque de fail2ban</i> | 67 |
| A.5 <i>Comprobación de funcionamiento</i> | 68 |
| ANEXO B. Configuración De Softphones | 71 |
| B.1 <i>Configuración de un cliente Linphone de escritorio</i> | 72 |
| B.2 <i>Configuración de un cliente Linphone en un teléfono móvil</i> | 76 |
| B.3 <i>Configuración de un cliente CSipSimple en un teléfono móvil</i> | 81 |
| B.4 <i>Duración del registro</i> | 87 |
| ANEXO C. SIPVicious | 89 |
| C.1 <i>Introducción a SIPVicious</i> | 89 |
| C.2 <i>Descarga de los ejecutables SIPVicious</i> | 90 |
| C.3 <i>Pruebas</i> | 90 |

ANEXO A. GUÍA DE INSTALACIÓN DE FAIL2BAN

En este manual se detallan las instrucciones para la instalación y la administración de la herramienta **Fail2ban** instalada en el servidor Asterisk del Departamento de Ingeniería Telemática de la Escuela Superior de Ingenieros de Sevilla.

Fail2ban es una herramienta que analiza los ficheros de registro de un servicio. Si encuentra algún signo malicioso en estos ficheros, prohíbe la dirección IP de la que procede el mensaje. Para ello, depende completamente del servidor Asterisk, ya que es el servidor quién escribe en los mensajes de registro. Principalmente esta herramienta permite añadir reglas **iptables** al cortafuegos para diversos servicios.

El único requisito para la instalación de esta herramienta es tener instalado el paquete **Python** en una versión igual o superior a la v2.6. Aunque **Fail2ban** ya está instalado y configurado en Elastix para el servicio ssh, no viene para la señalización SIP. Se detalla a continuación la configuración para el servidor Asterisk.

A.1 Herramienta iptables

Antes de comenzar con la configuración de **Fail2ban** para Asterisk, se debe comprobar que la herramienta **iptables** está configurada para arrancar en el servidor. Para ello, se debe ejecutar el siguiente comando con permisos de superusuario:

```
service iptables status
```

Una vez comprobado que la herramienta se encuentra activa, debe asegurarse de que se inicia al arrancar la máquina:

```
chkconfig iptables on
```

A.2 Configuración de Asterisk para guardar los logs

Para configurar que Asterisk guarde los logs en un archivo específico y con un formato de hora correcto, se debe editar el fichero `/etc/asterisk/logger.conf` agregando las siguientes líneas en cada sección:

```
[general]
dateformat=%F %T

[logfiles]
fail2ban => notice
```

A.3 Configuración de fail2ban

Tal como se ha mencionado, **Fail2ban** ya se encuentra instalado en el sistema Elastix a partir de la versión 2.4. Si excepcionalmente no se encontrara en el sistema, se puede instalar con el comando:

```
yum install fail2ban
```

Fail2ban dispone, entre otros, de dos ficheros de configuración importantes:

- ❖ `/etc/fail2ban/filter.d/asterisk.conf`.
- ❖ `/etc/fail2ban/jail.conf`.

El fichero `asterisk.conf` contiene la configuración de patrones de bloqueo para Asterisk, el cual permite ajustar en que formato se encuentra la dirección IP en los archivos de registro para que la herramienta pueda bloquearla.

A su vez el fichero `jail.conf` es el fichero de configuración más importante de **Fail2ban**. En él se configuran los parámetros que se describen a continuación:

- `ignoreip`. Este parámetro sirve para agregar direcciones IP que no se quiere que sean bloqueadas por error, como por ejemplo nuestra propia dirección IP, evitando así perder el acceso al servidor. Permite introducir tantas direcciones IP como se necesiten separándolas por un espacio.
- `Bantime`. Este parámetro establece el número de segundos que una dirección IP estará bloqueada en caso de que se incumplan las reglas o se supere el número máximo de intentos de acceso permitidos.
- `maxretry`. Este parámetro especifica el número de intentos de acceso fallidos antes de que la dirección IP del equipo sea bloqueada.
- `findtime`. Este parámetro fija el espacio de tiempo en el que deben ocurrir todos los intentos especificados en `maxretry` para que la cuenta sea bloqueada.

Una vez instalado el paquete debe configurarse el fichero `jail.conf` rellenando los parámetros anteriormente descritos. Estos parámetros deben introducirse en la sección `[Default]`, en el caso de que sean válidos para todos los servicios que analiza **Fail2ban**, o debajo de la sección del servicio en concreto que se desea analizar con esas reglas y condiciones.

En el caso del Departamento, todos los parámetros, a excepción del parámetro `maxretry`, se han introducido en la sección `[Default]`. Se ha establecido que las direcciones IP que se desea que no estén prohibidas (`ignoreip`), sean la IP del servidor `trajano.us.es`, la subred de direccionamiento privado, puesto que es donde se encuentran los clientes SIP internos, y la subred local.

El servidor VoIP del Departamento se reinicia todos los días. Debido a esto se ha establecido un periodo de bloqueo de dirección IP (`bantime`) de 10 horas (36000s), de forma que un cliente malicioso solo pueda realizar un máximo 3 ataques diarios. También, se ha dispuesto en 10 horas el espacio de tiempo en el que deben ocurrir todos los intentos de acceso al servidor (`findtime`).

A continuación se muestra como queda la sección [Default] :

/etc/fail2ban/jail.conf

```
[DEFAULT]
bantime = 36000
findtime = 36000
ignoreip = 127.0.0.1/8 193.147.162.130 172.16.16.0/24
```

Para configurar el fichero de registro de salida se tienen dos opciones, o bien usar syslog, y que todos los mensajes vayan al registro /var/log/messages, o bien usar su propio fichero de registro, por ejemplo /var/log/fail2ban.log. Para indicar qué opción se va a emplear, se hace uso del parámetro logpath. Este parámetro se encuentra en la sección específica de cada servicio.

Para activar la inspección del servicio deseado, debe introducirse en el fichero jail.conf dentro de la sección [Default] y justo antes de la sección [ssh-iptables] las siguientes líneas:

```
[asterisk-iptables]
enabled = true
filter = asterisk
action = iptables-allports[name=ASTERISK, protocol=all]
sendmail-whois[name=ASTERISK, dest=root, sender=fail2ban@localhost]
logpath = /var/log/asterisk/fail2ban
maxretry=5
```

En estas líneas, además de activar la herramienta **Fail2ban** para Asterisk, se ha establecido un maxretry de 5 intentos para este servicio y se ha indicado el uso de un fichero propio de registro denominado “fail2ban”, ubicado en el directorio /var/log/asterisk.

A.4 Arranque de fail2ban

Una vez configurado **Fail2ban**, se procede a la validación de la configuración de éste. Para ello, se arranca el servicio mediante el siguiente comando:

```
service fail2ban start
```

Si el resultado es exitoso, se configura su arranque tras un reinicio:

```
chkconfig fail2ban on
```

Para comprobar si la herramienta **Fail2ban** está funcionando, se pueden mostrar las reglas **iptables** y comprobar que **Fail2ban** ha creado y añadido una cadena al cortafuegos en la tabla FILTER por cada servicio que se ha activado en el fichero de configuración `jail.conf`.

```
[root@asterisk] iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source                destination
fail2ban-SSH tcp  --  anywhere              anywhere
fail2ban-ASTERISK all  --  anywhere              anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination

Chain fail2ban-ASTERISK (1 references)
target     prot opt source                destination
RETURN    all  --  anywhere              anywhere

Chain fail2ban-SSH (1 references)
target     prot opt source                destination
RETURN    all  --  anywhere              anywhere
```

Como se puede observar en el servidor del Departamento, **Fail2ban** ha añadido la cadena `fail2ban-ASTERISK`.

A.5 Comprobación de funcionamiento

Para comprobar el correcto funcionamiento de **Fail2ban** se va a verificar que, al realizar más de 5 intentos de acceso fallidos desde un *softphone*, es capaz de registrarlo en el fichero de log correspondiente; además de bloquear la dirección IP del cliente en la cadena **iptables**, creada al arrancarse el sistema.

Para llevar a cabo esta prueba se ha introducido 5 veces mal la contraseña de una extensión desde un *softphone* que está accediendo desde Internet, ya que en la red interna del Departamento los clientes no pueden ser bloqueados gracias al parámetro `ignoreip`. Se recuerda que se ha establecido el parámetro `maxentry` a 5 en la configuración de **Fail2ban** para Asterisk.

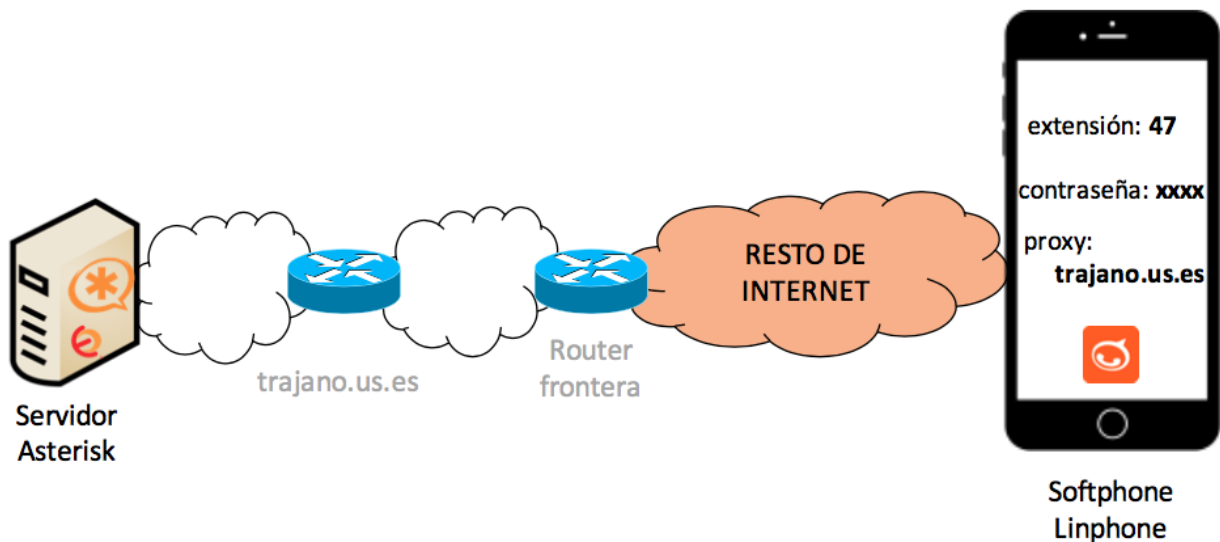


Figura 23: Prueba de funcionamiento Fail2ban y softphone Linphone

Como se puede observar en la figura, **Fail2ban** ha bloqueado la dirección IP “46.222.254.243” correspondiente al cliente SIP que ha intentado el registro de la extensión en el sistema de telefonía.

```
[root@asterisk ~]# iptables -L -n
Chain INPUT (policy ACCEPT)
target     prot opt source                destination            tcp dpt:22
fail2ban-SSH tcp  --  0.0.0.0/0             0.0.0.0/0
fail2ban-ASTERISK all  --  0.0.0.0/0             0.0.0.0/0

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination

Chain fail2ban-ASTERISK (1 references)
target     prot opt source                destination
REJECT    all  --  46.222.254.243       0.0.0.0/0             reject-with icmp-port-unreachable
RETURN    all  --  0.0.0.0/0             0.0.0.0/0

Chain fail2ban-SSH (1 references)
target     prot opt source                destination
RETURN    all  --  0.0.0.0/0             0.0.0.0/0
[root@asterisk ~]#
```

Figura 24: Dirección IP maliciosa bloqueada en la cadena fail2ban-Asterisk creada por fail2ban

También, se puede observar como **Fail2ban** ha registrado en el fichero de registro la incidencia.

```
NOTICE[3765][C-00000458] chan_sip.c: Failed to authenticate device <sip:47@193.147.162.130>;tag=7GZMLk2CR
NOTICE[3765] chan_sip.c: Registration from 'sip:47@193.147.162.130' failed for '46.222.254.243:61890' - Wrong password
NOTICE[3765] chan_sip.c: Registration from 'sip:47@193.147.162.130' failed for '46.222.254.243:62025' - Wrong password
NOTICE[3765] chan_sip.c: Registration from 'sip:47@193.147.162.130' failed for '46.222.254.243:62025' - Wrong password
NOTICE[3765] chan_sip.c: Registration from 'sip:47@193.147.162.130' failed for '46.222.254.243:62025' - Wrong password
NOTICE[3765] chan_sip.c: Registration from 'sip:47@193.147.162.130' failed for '46.222.254.243:62025' - Wrong password
NOTICE[18396] pbx_spool.c: Call completed to Local/s@tc-maint
```

Figura 25: Fichero Fail2ban de registro

No se debe olvidar que **Fail2ban** depende totalmente de Asterisk para detectar cualquier intruso o fallo en la autenticación de usuarios. Desafortunadamente, Asterisk solo registra en los archivos de logs determinados eventos, como fallos en la autenticación de los mensajes REGISTER. De esta forma, si un atacante envía un mensaje INVITE con autenticación y falla, Asterisk no lo registrará, con lo que **Fail2ban** no podrá detectarlo ni bloquearlo. Es por esto que, por ejemplo, **Fail2ban** no puede parar los “*friendly-scanner*” procedentes de la aplicación **SIPvicious**, ya que éste emplea mensajes INVITE para intentar acceder al sistema de telefonía.

ANEXO B. CONFIGURACIÓN DE SOFTPHONES

En este manual se detallan las instrucciones para la configuración y uso de los diferentes *softphones* permitidos en el sistema de telefonía del Departamento de Ingeniería Telemática de la Escuela Técnica Superior de Ingenieros de Sevilla. Los *softphone* autorizados son **Linphone** y **CSipSimple**.

Linphone es una aplicación de telefonía de código abierto que permite la comunicación de voz, vídeo y mensajería instantánea a través de Internet o de cualquier red IP. Esta aplicación hace uso del protocolo SIP y permite también utilizar cualquier operador de VoIP. Además, la organización dispone de un servicio de audio y video SIP gratuito.

Linphone fue la primera aplicación de código abierto con *software* SIP en GNU/Linux y actualmente está disponible para:

- Windows phone y escritorio
- Android e iOS
- OSX



Figura 26: Logo de Linphone

CSipSimple también es una aplicación de telefonía de código abierto, pero sólo disponible para el sistema operativo Android. Esta aplicación permite la comunicación de voz a través de Internet o cualquier red IP haciendo uso del protocolo SIP.



Figura 27: Logo de CSipSimple

B.1 Configuración de un cliente Linphone de escritorio

Una vez descargada la aplicación, se detallarán los pasos a realizar para la configuración rápida de una cuenta SIP en un cliente **Linphone** de escritorio.

Al abrir la aplicación le aparecerá un cuadro con un asistente de configuración de cuenta.

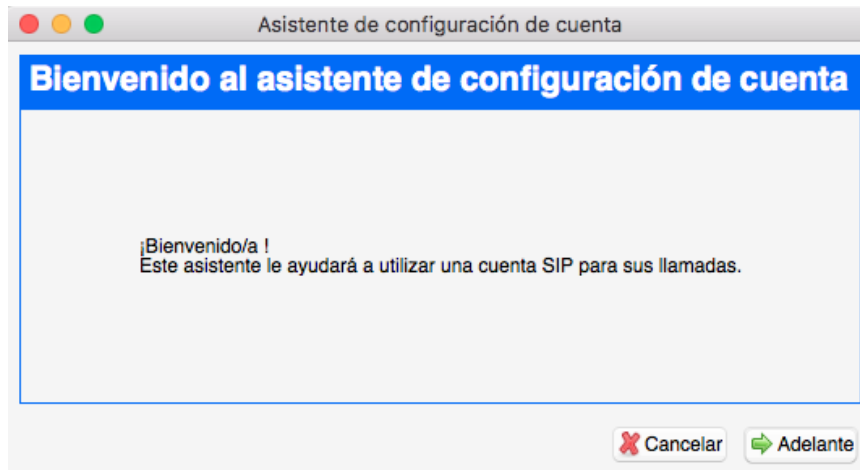


Figura 28: Linphone escritorio. Asistente de configuración

Debe seleccionar **Adelante**. A continuación, en la siguiente pantalla le aparecerán los tipos de cuentas que **Linphone** permite configurar. Deberá marcar “**Ya tengo una cuenta SIP y quiero usarla**”.

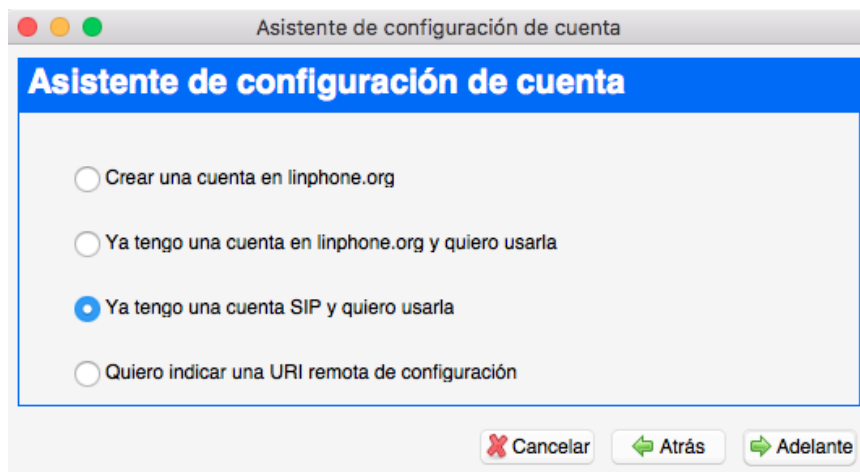


Figura 29: Linphone escritorio. Usar cuenta SIP

En esta pantalla se procede a la configuración de la cuenta. En ella debe introducir los siguientes campos:

- **Nombre de usuario:** su extensión SIP.
- **Contraseña:** su clave SIP.
- **Dominio:** su servidor VoIP.
- **Proxy:** si su sistema de telefonía usa proxy. No debe rellenarlo si no procede.

Normalmente las extensiones SIP suelen ser numéricas. **Linphone** de escritorio no permite en una primera instancia utilizar una cuenta SIP con un nombre de usuario numérico. Sin embargo, una vez configurada la cuenta, sí permite cambiar el nombre de usuario a un usuario numérico. En estas circunstancias, primero ha de rellenarse el campo “**Nombre de usuario**” con un carácter alfabético y posteriormente se procede a su modificación.

En la siguiente imagen se muestra un ejemplo de configuración de la extensión 47, que tiene como servidor de telefonía la dirección IP 193.147.162.130. Como **Linphone** no permite un nombre de cuenta numérico, se ha introducido una letra ‘p’ antes del número de extensión para que nos permita avanzar en la configuración.

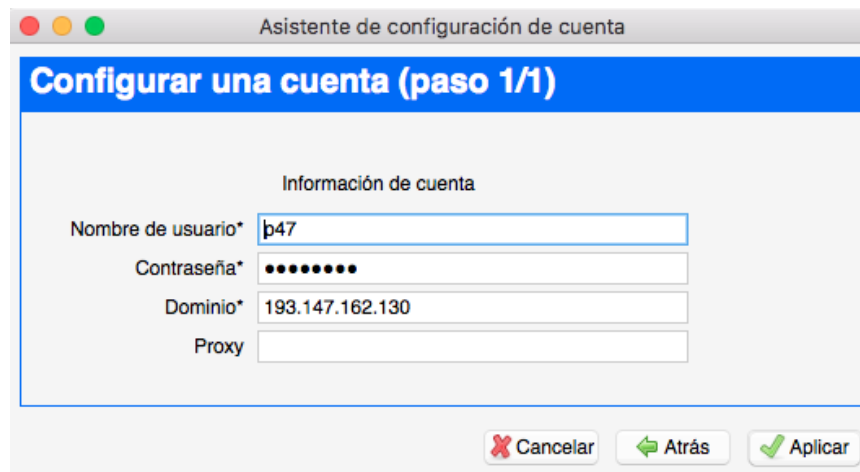


Figura 30: Linphone escritorio. Configuración de una cuenta

Para finalizar la configuración de la cuenta SIP debe hacer click en **Aplicar** y, posteriormente, **cerrar** la ventana del asistente de configuración.

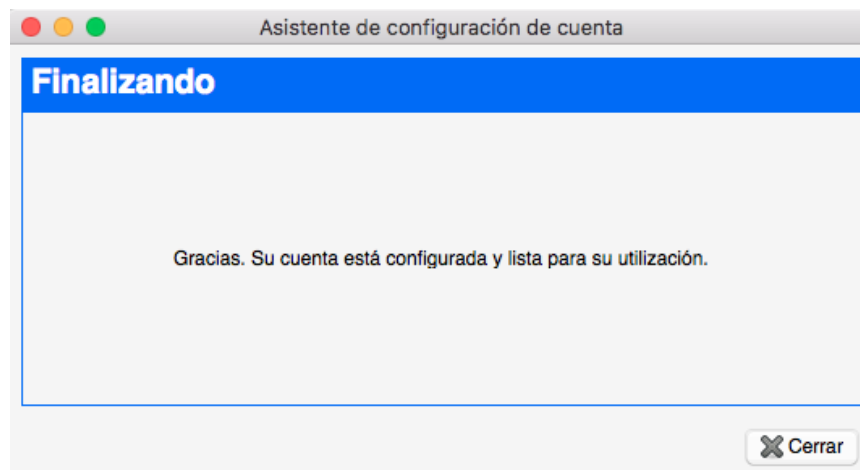


Figura 31: Linphone escritorio. Configuración de cuenta finalizada

Tal como se ha mencionado anteriormente, es necesario editar la cuenta SIP para cambiar el nombre de usuario al nombre de usuario real, numérico. Para ello, debe seleccionar **Opciones** en el menú de herramientas y a continuación, en el desplegable, seleccionar **Preferencias**.

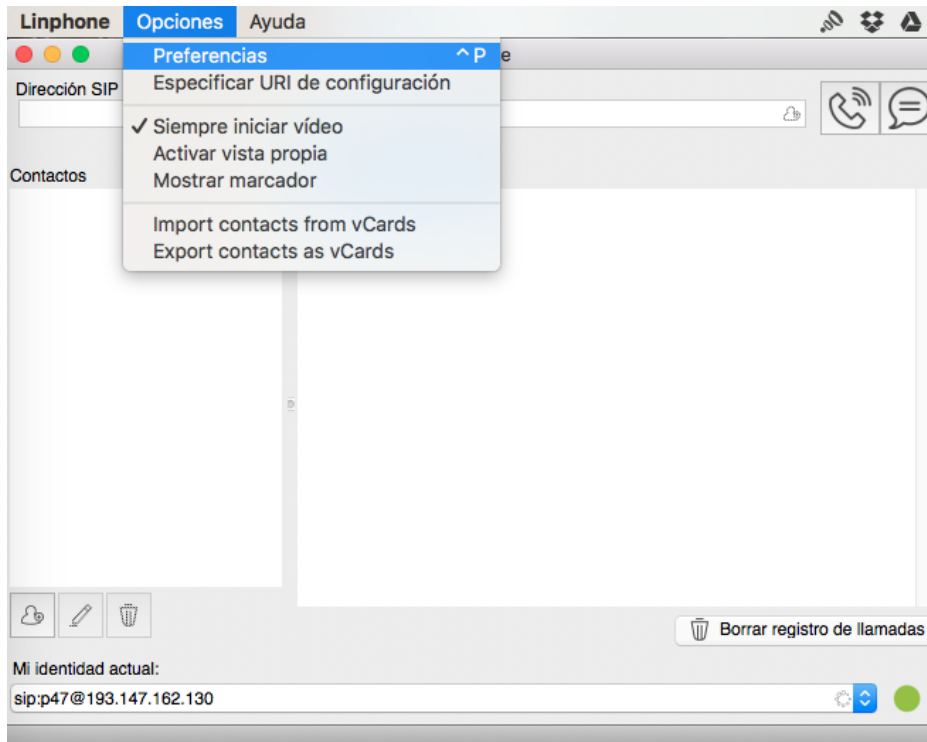


Figura 32: Linphone escritorio. Preferencias

Después le aparecerá una ventana tal como se muestra en la siguiente imagen.

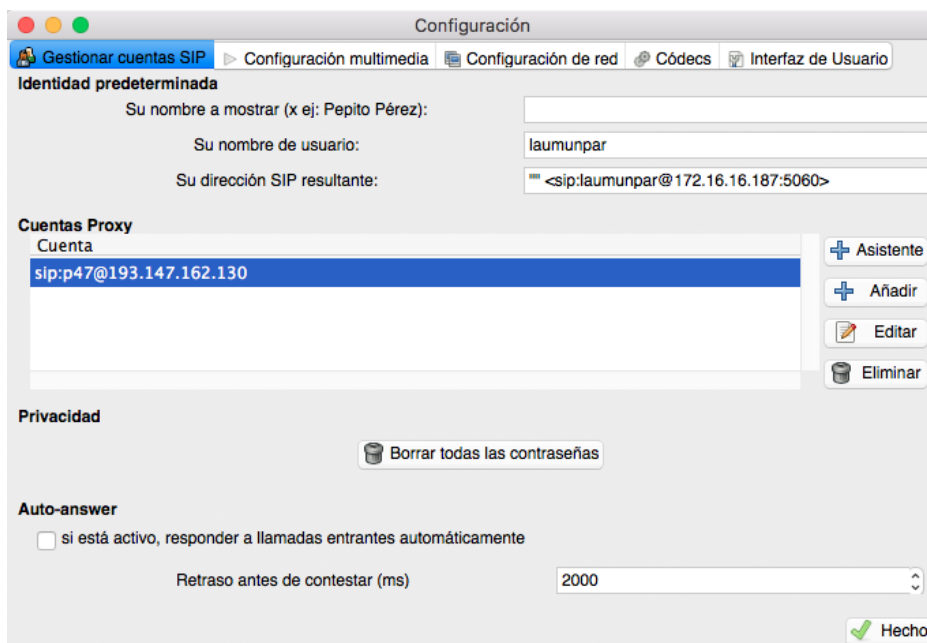


Figura 33: Linphone escritorio. Configuración

Esta ventana permite la configuración multimedia, de red, elección de códecs... Para editar la cuenta SIP pulse **Editar**, ubicado en la parte derecha de la ventana de la pestaña **Gestionar cuentas SIP**.

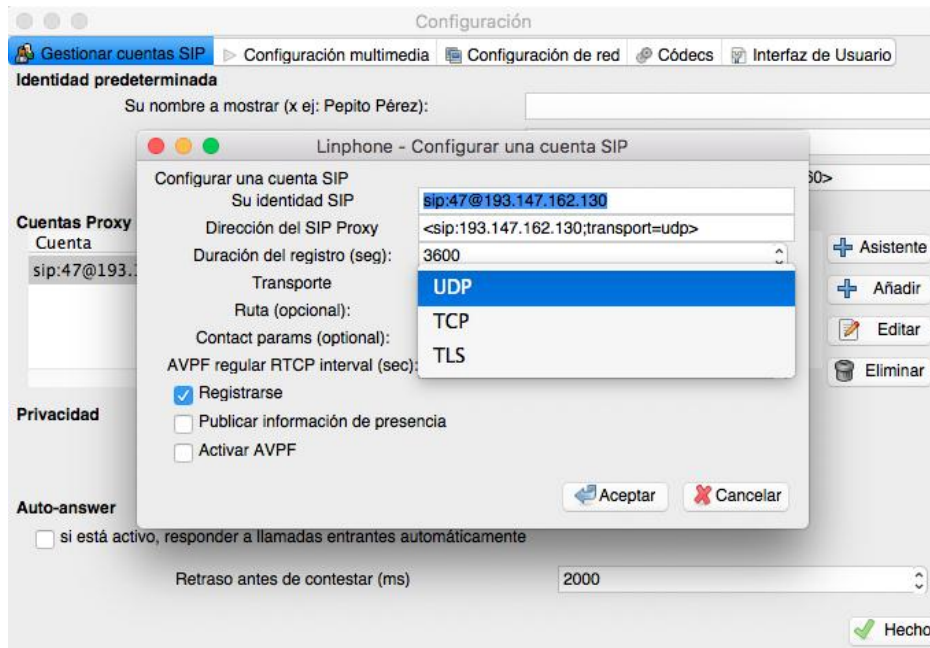


Figura 34: Linphone escritorio. Ajustes de una cuenta SIP

Una vez dentro, permite configurar y editar, además del nombre de usuario, algunos otros parámetros como el protocolo de transporte, la duración del registro de la cuenta, etc. El nombre de usuario se cambia en el campo “**Su identidad SIP**”. En este caso, solo es necesario quitarle el carácter extra introducido en la fase de configuración inicial. Tras ello escoja **Aceptar** e, inmediatamente después, **Hecho**.

Quando la cuenta esté configurada, **Linphone** le pedirá que introduzca de nuevo su contraseña. Esto es debido al cambio de nombre de usuario. Si le aparece este mensaje antes, ignórelo, seleccione **Cancelar** y no lo rellene hasta que no haya editado la cuenta.

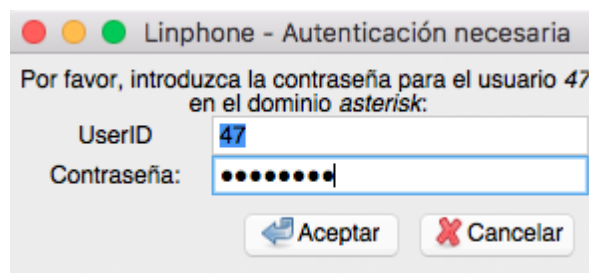


Figura 35: Linphone escritorio. Autenticación necesaria

A continuación se muestran las pestañas de **Configuración de red** y **Códex** con los ajustes por defecto.

Un campo que puede resultar útil es el número de puerto SIP que el cliente emplea para recibir y enviar tráfico SIP. Con los ajustes por defecto, el puerto seleccionado es el 5060. Tal como se ha descrito en el proyecto, el uso de este puerto no es el más recomendable, puesto que resulta atacado con frecuencia, provocando llamadas indeseadas.

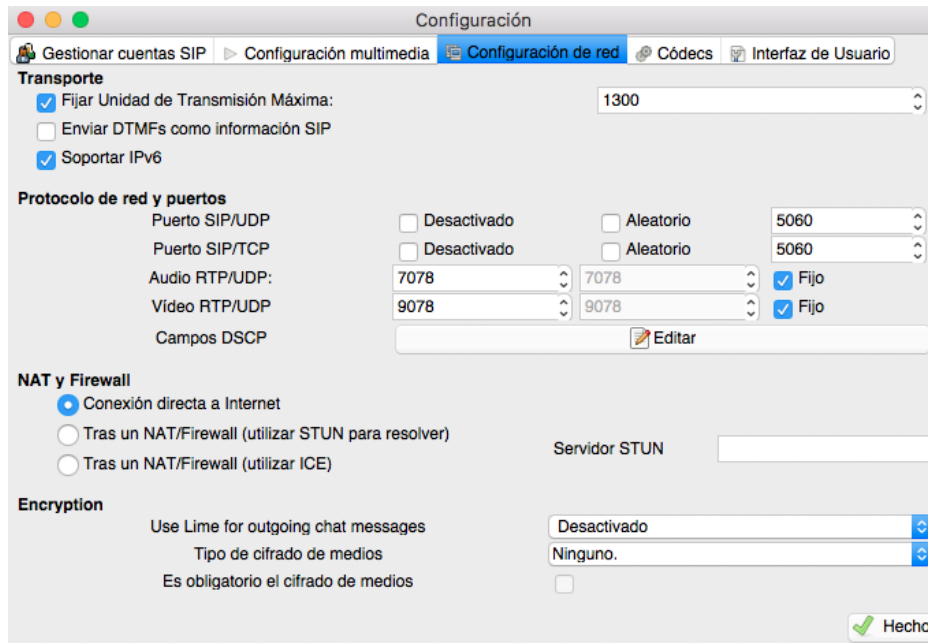


Figura 36: Linphone escritorio. Configuración de red

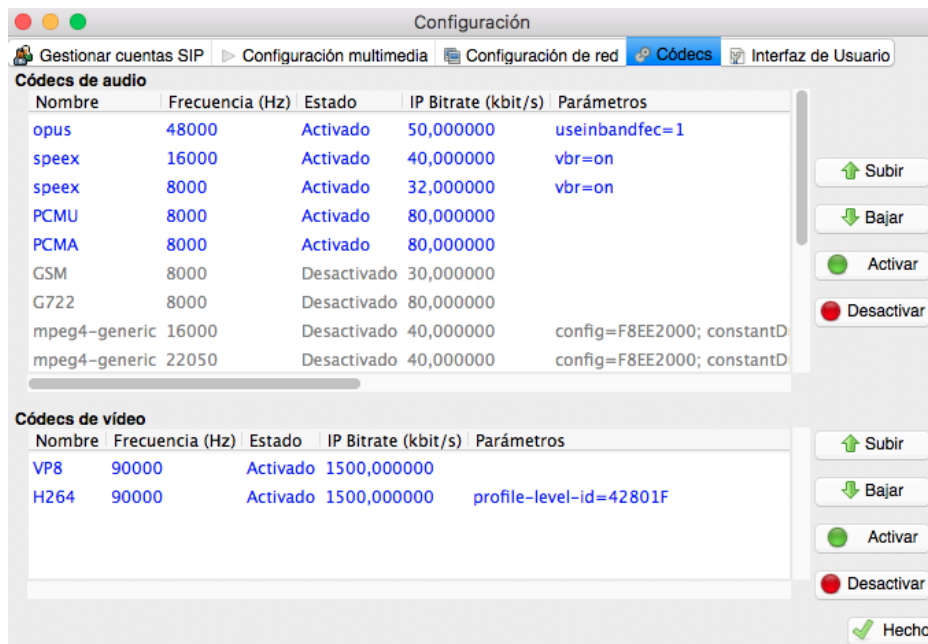


Figura 37: Linphone escritorio. Códex

B.2 Configuración de un cliente Linphone en un teléfono móvil

Una vez descargada la aplicación en el teléfono, se describirán los pasos a realizar para la configuración rápida de una cuenta SIP en un cliente **Linphone**. Este manual sirve tanto para clientes Android como iOS.

Al abrir la aplicación le aparecerá un asistente de configuración de cuentas. Este asistente dispondrá de un menú con los diferentes tipos de cuentas que **Linphone** permite configurar. Deberá seleccionar “**USE SIP ACCOUNT**” para hacer uso de una cuenta SIP.

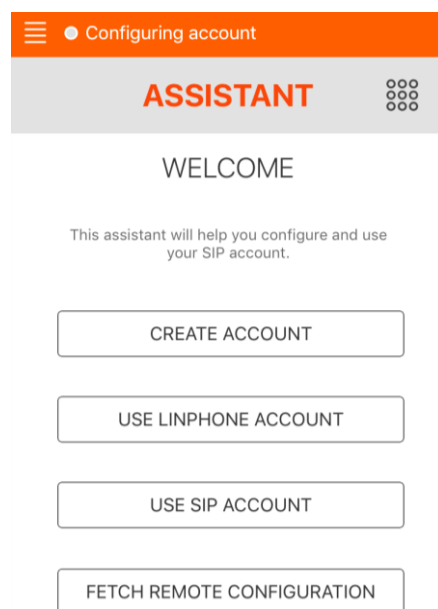


Figura 38: Linphone Smartphone. Asistente de configuración

En la siguiente pantalla se procederá a la configuración de la cuenta SIP. En ella debe introducir los siguientes campos:

- **Username:** su extensión SIP.
- **Password:** su clave SIP.
- **Domain:** su servidor VoIP.
- **Display name:** nombre de la cuenta (opcional).
- **Transport:** protocolo de transporte que desea utilizar. Debe recordar que el protocolo de transporte que emplee debe ser el mismo que el configurado en el servidor para esta extensión.

Configuring account

← ASSISTANT

Enter your username and password with your SIP domain.

USERNAME
45

PASSWORD (OPTIONAL)
●●●●●●●

DOMAIN
193.147.162.130

DISPLAY NAME (OPTIONAL)

TRANSPORT
 UDP TCP TLS

LOGIN

Figura 39: Linphone Smartphone. Configuración de una cuenta

En el caso de este cliente **Linphone** no es necesario que el nombre de usuario sea alfanumérico, con lo que permite realizar la configuración de la cuenta SIP de una vez.

En la imagen superior se muestra un ejemplo de configuración de la extensión 45, que tiene como servidor de telefonía la dirección IP 193.147.162.130 y utiliza el protocolo de transporte UDP.

Una vez configurada la cuenta debe pulsar **LOGIN** para finalizar. Si la configuración es correcta y la extensión ha logrado registrarse en el servidor, **Linphone** mostrará en la parte superior un círculo verde indicando que el resultado ha sido exitoso.

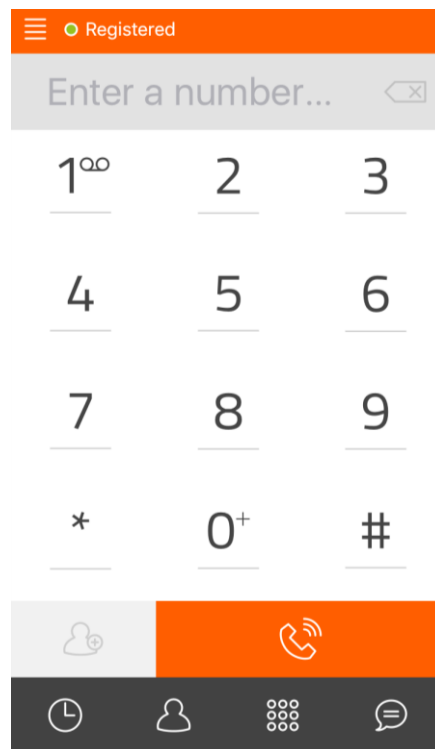



Figura 40. Linphone Smartphone. Cuenta registrada

Si posteriormente quiere añadir otra cuenta, puede llegar al menú principal pulsando en el símbolo  situado arriba a la izquierda en la pantalla y seleccionar **Assistant**.

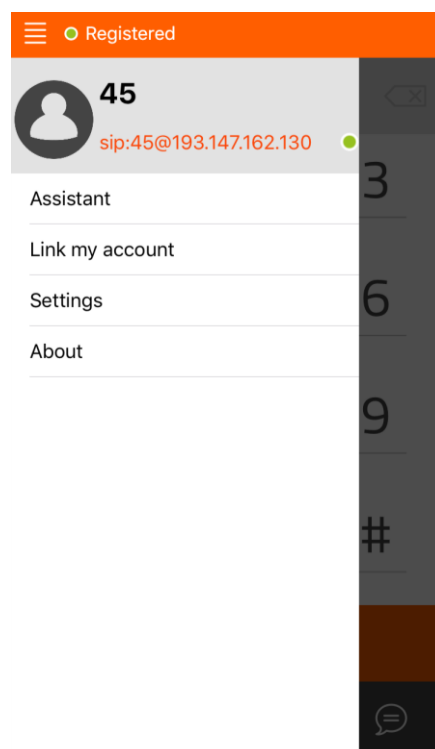


Figura 41: Linphone Smartphone. Menú principal

Si desea realizar configuraciones avanzadas, deberá seleccionar **Settings** en el menú principal.

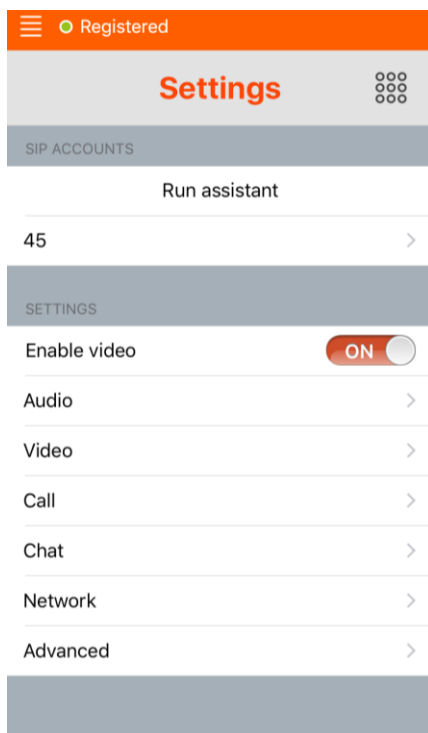


Figura 42: Linphone Smartphone. Ajustes

Desde esta pantalla se puede realizar tanto ajustes a las cuentas asociadas como ajustes generales de red, voz, audio, vídeo...

A continuación se muestran los ajustes de la cuenta/extensión 45.

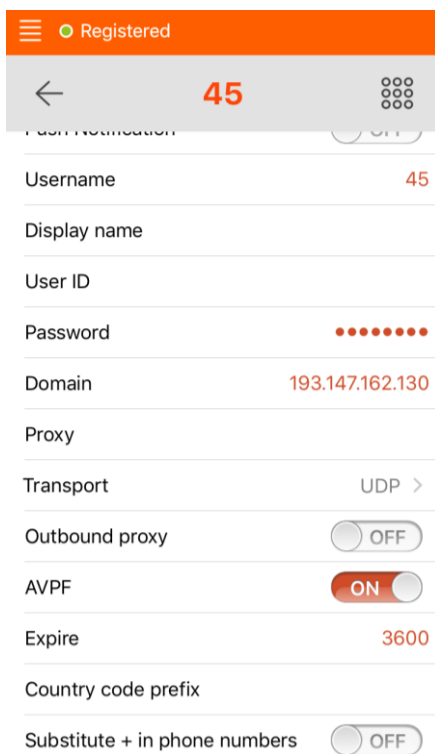


Figura 43: Linphone Smartphone. Ajuste de cuenta

La configuración de puertos, tanto de audio y vídeo como de señalización SIP, se encuentra en los ajustes de red (Menú principal → Network). El puerto SIP debe configurarse con la opción **Random Port**. Si esta opción está desactivada, el puerto por defecto para recibir y enviar tráfico SIP será el 5060. Si, por el contrario, el campo está activado, como es el caso, el puerto empleado será aleatorio.

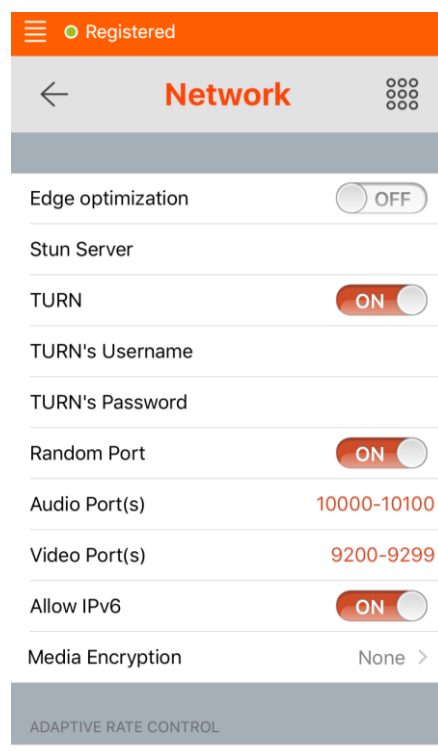


Figura 44: Linphone Smartphone. Ajustes de red

B.3 Configuración de un cliente CSipSimple en un teléfono móvil

Una vez descargada la aplicación en el teléfono móvil Android, se detallarán los pasos a realizar para la configuración rápida de una cuenta SIP en un cliente **CSipSimple**.

Al abrir la aplicación le aparecerá una pantalla con un botón en el centro que le permitirá añadir una cuenta.

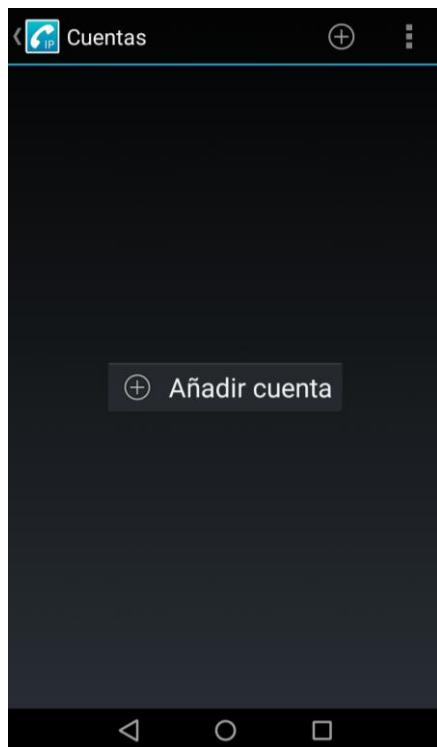


Figura 45: CSipSimple. Añadir cuenta

Justo después le aparecerá una lista con todos los tipos de cuenta que **CSipSimple** permite asociar al *softphone*. Se podría escoger el asistente de configuración **Básico**, pero, en este caso, se ha elegido el **Avanzado** para mostrar todas las opciones de configuración posibles.

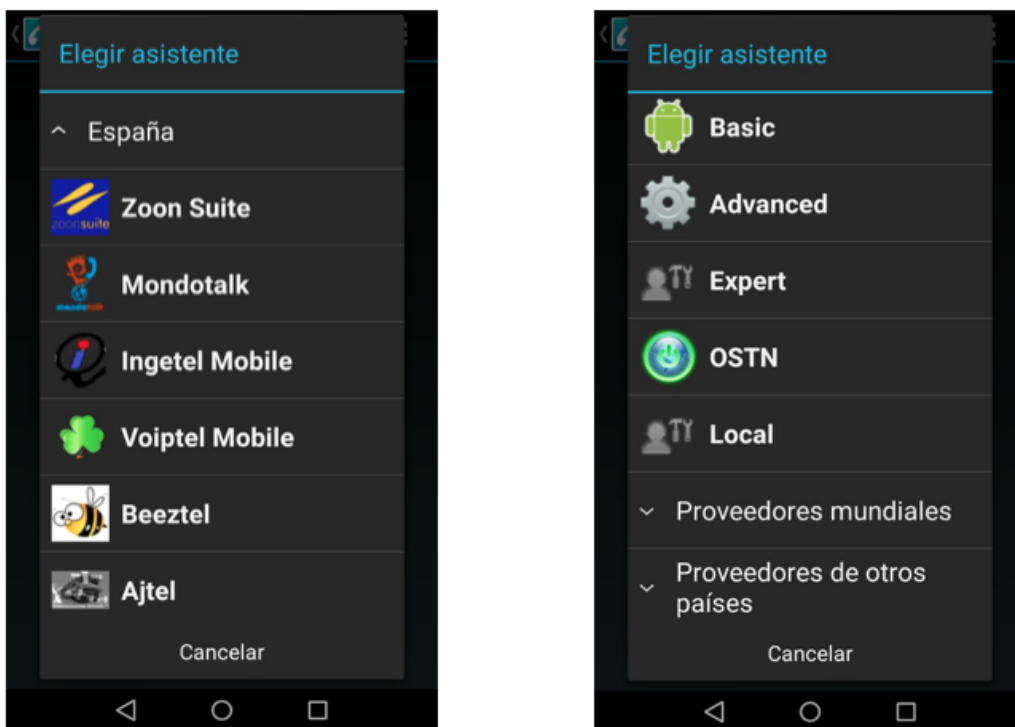


Figura 46. CSipSimple. Asistentes de configuración

Una vez seleccionado el asistente de configuración, debe aparecer una pantalla con los campos que se han de introducir obligatoriamente en color naranja para asociar la extensión o cuenta SIP al *softphone*.

A continuación, en la siguiente pantalla, se procederá a la configuración de la cuenta SIP rellenando los campos obligatorios:

- **Nombre de la cuenta:** nombre a mostrar para esta cuenta.
- **Servidor:** su servidor VoIP.
- **Nombre de usuario:** su extensión SIP.
- **Contraseña:** su clave SIP.



Figura 47: CSipSimple. Configuración de una cuenta SIP

En la imagen superior se muestra un ejemplo de configuración de la extensión 47, que tiene como servidor de telefonía la dirección IP 193.147.162.130 y utiliza el protocolo de transporte UDP.

Una vez configurada la cuenta, debe pulsar **Guardar** para finalizar. Si la configuración es correcta y la extensión ha logrado registrarse en el servidor, **CSipSimple** mostrará una lista con todas las cuentas configuradas y en color verde indicará si el resultado ha sido exitoso.

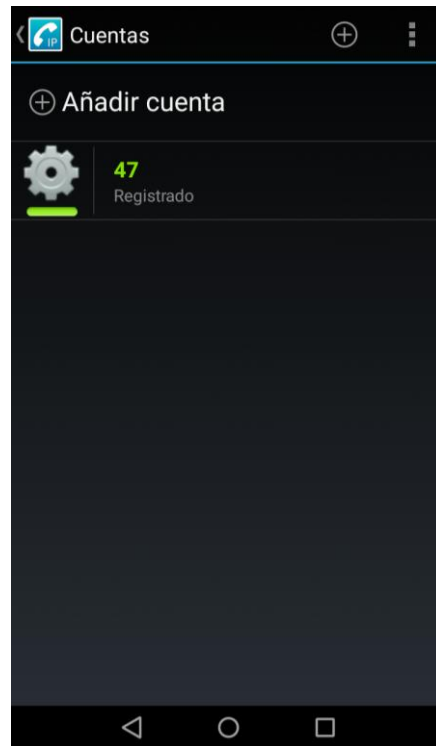



Figura 48: CSipSimple. Cuenta registrada

CSipSimple dispone de un menú de ajustes accesible desde el marcador pulsando en el botón  y seleccionando la opción **Ajustes**.

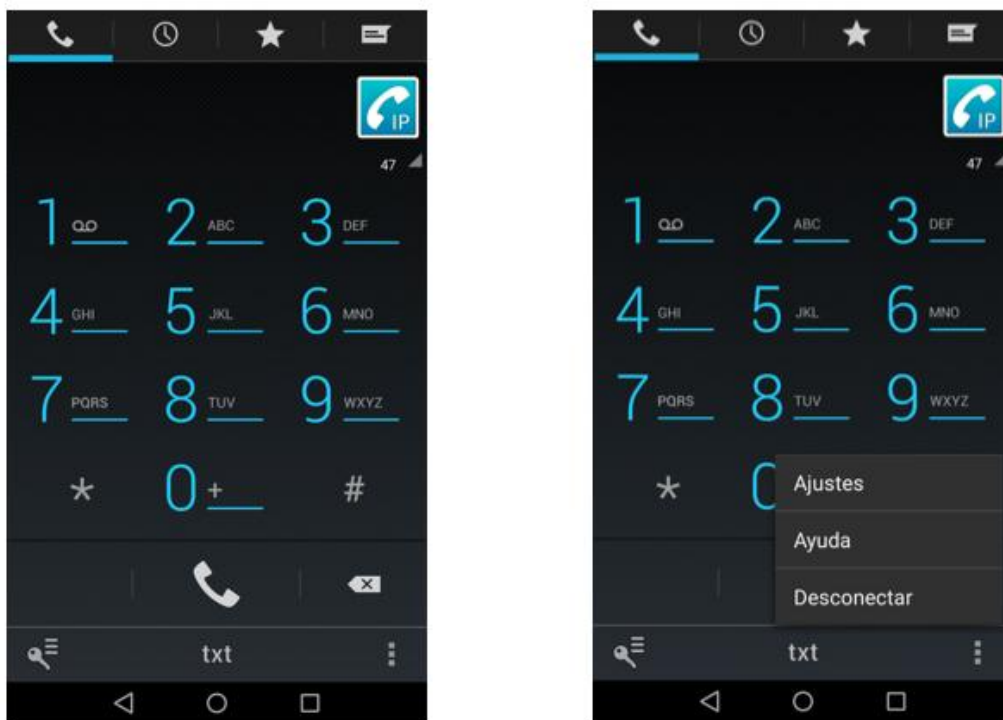


Figura 49: CSipSimple. Marcador telefónico

La siguiente imagen muestra el menú de ajustes.



Figura 50: CSipSimple. Ajustes

Este menú permite la configuración de numerosas funcionalidades. Por ejemplo, si marcamos la opción **“Integrar con Android”** en el apartado de **“Configuración sencilla”** del menú de ajustes, permite la integración de la aplicación con el marcador telefónico.

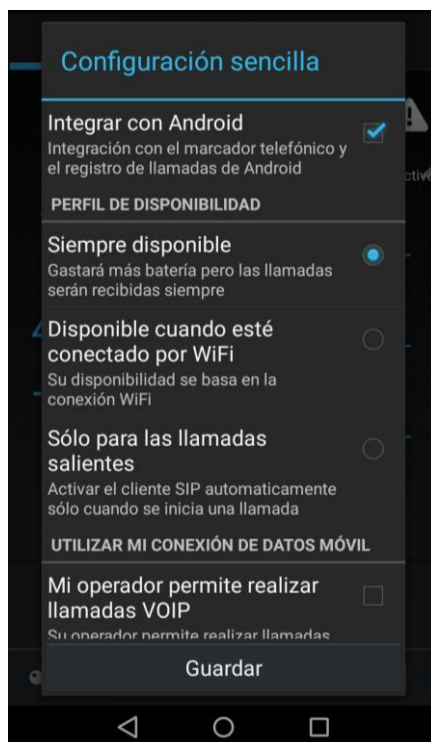


Figura 51: CSipSimple. Configuración Sencilla

En los ajustes de red, por defecto, viene desactivado el uso de datos móviles para la aplicación. Si quiere utilizar la aplicación sin estar conectado a una red WiFi puede cambiar la configuración desde el menú de ajustes seleccionando **Red**.

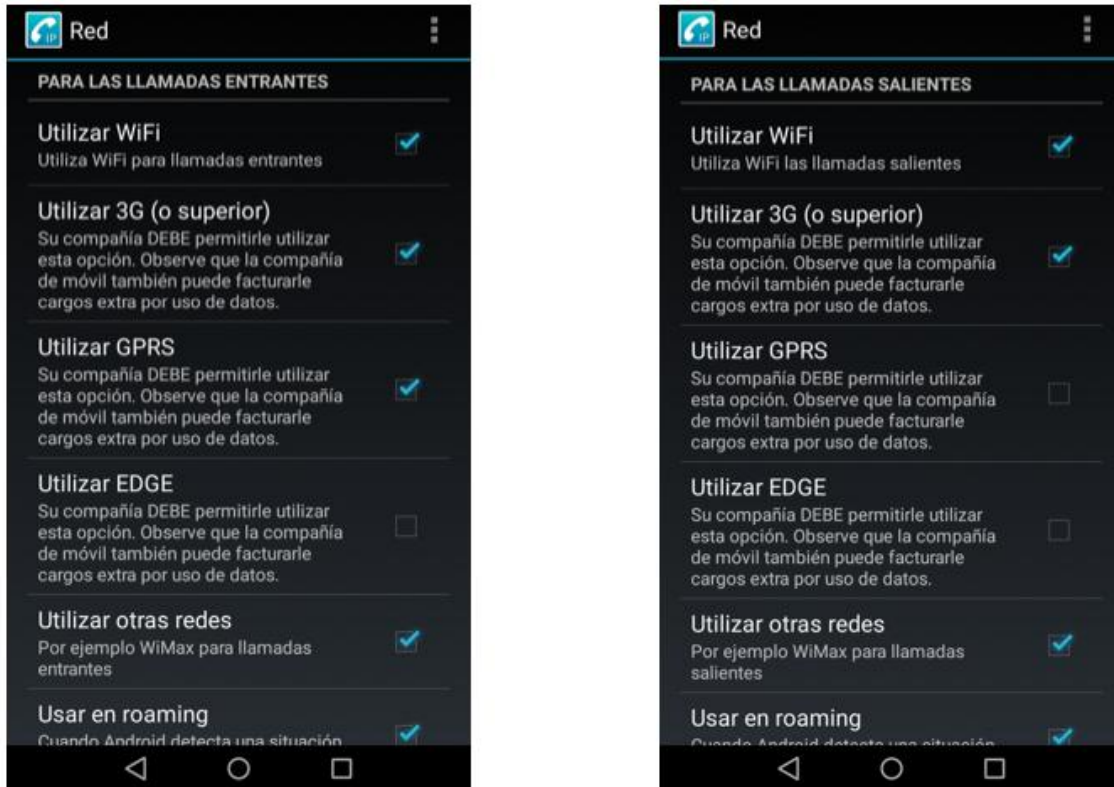


Figura 52: CSipSimple. Configuración de red

Tal como se ha mencionado anteriormente, existe una opción que permite la integración del marcador telefónico con el de la aplicación. En la siguiente imagen se puede apreciar como, al realizar una llamada, el dispositivo nos pregunta qué cuenta deseamos utilizar.

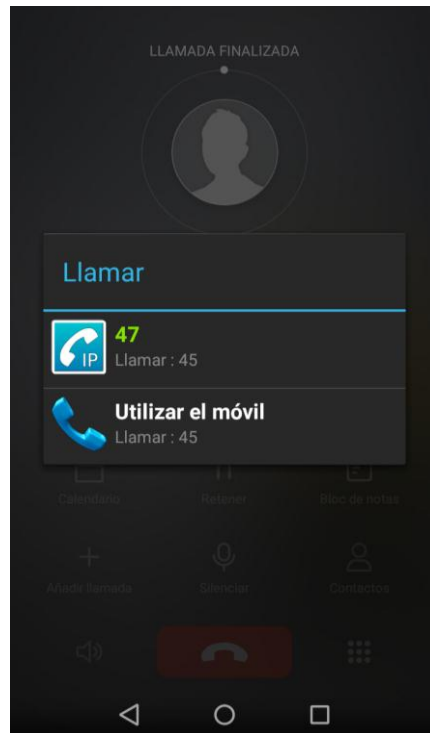


Figura 53: CSipSimple. Llamada

B.4 Duración del registro

Las aplicaciones móviles que implementan *softphones* tienen el problema de que el registro de la extensión no se mantiene durante mucho tiempo. Esto quiere decir que, si la aplicación está abierta y en primer plano, se pueden recibir llamadas sin ningún problema. Sin embargo, si la aplicación está en segundo plano, se pueden recibir llamadas SIP sólo mientras que la extensión se encuentre registrada. En el caso de **CSipSimple** el registro de una extensión puede durar hasta una hora, mientras que en el caso de **Linphone** sólo dura minutos. Para volver a registrar la extensión lo único que hay que hacer es volver a entrar en la aplicación.

Con las aplicaciones *softphone* de escritorio esto no ocurre. El cliente se mantiene registrado hasta que se fuerza el cierre de la aplicación, permitiendo así recibir llamadas SIP en cualquier momento.

ANEXO C. SIPVICIOUS

En este manual se describen las instrucciones de uso de la herramienta **SIPVicious** que permite probar si la configuración SIP del servidor Asterisk del sistema de telefonía del Departamento de Ingeniería Telemática de la Escuela Técnica Superior de Ingenieros de Sevilla es segura.



Figura 54: Logo de SIPVicious

SIPVicious se compone de varios programas en **Python**, con lo que el único requisito para la instalación y uso de esta herramienta es tener instalado el paquete **Python**.

C.1 Introducción a SIPVicious

SIPVicious es una herramienta de código abierto que realiza barrido inocuo de puertos, conocido como “*friendly-scanner*”, que como se ha descrito en el proyecto, no es realmente un sondeo de puertos “amigo”, sino un tipo de *botnet*. Actualmente existen numerosas herramientas similares a ésta que tratan de acceder a los sistemas de telefonía IP para intentar realizar llamadas de pago a través de la red telefónica conmutada.

Estas herramientas tratan de explorar rangos de direcciones IP identificando a los servidores SIP que encuentran en su camino. Por defecto, sólo comprueban las comunicaciones a través del puerto SIP estándar (5060), pero algunas ya permiten sondear en otros rangos de puertos.

Una vez que han detectado un dispositivo SIP, intentan enumerar su configuración, averiguar las extensiones SIP, etc. Posteriormente intentan forzar bruscamente el servidor probando números secuenciales como extensiones SIP con nombres de usuarios y contraseñas comunes (débiles).

En el caso de **SIPVicious**, siempre comienza su exploración probando con la extensión ‘100’, con lo que se recomienda no utilizar dicha extensión en el plan de numeración del sistema de telefonía. En cuanto a las contraseñas débiles, **SIPVicious** utiliza palabras y claves comunes de archivos diccionario.

Finalmente, obtenido el acceso a una extensión del servidor de VoIP, los atacantes tratan de realizar llamadas a través de la red telefónica conmutada.

SIPVicious, al ser de código abierto, permite a cualquier proveedor de un sistema de telefonía IP comprobar si la configuración de su servidor SIP es segura realizando este tipo de pruebas.

A continuación se detallarán los programas de los que se compone **SIPVicious** (todos los programas están escritos en **Python**):

| PROGRAMA | DESCRIPCIÓN |
|-----------------|--|
| svmap | Es un escáner SIP. Se encarga de escanear una dirección o un rango de direcciones IP para averiguar si existen dispositivos SIP, ya sean servidores o teléfonos IP, escuchando en el puerto SIP estándar. Actualmente, también permite el sondeo de puertos no estándares. |
| svwar | Escanea el servidor de VoIP buscando y enumerando las extensiones SIP que permiten registrarse. Además, indica si la extensión requiere o no autenticación. |
| svcrack | Intenta obtener la contraseña de una extensión SIP o un servidor de registro. Los modos actuales de craqueo de contraseñas son rangos numéricos o palabras de archivos diccionario. |
| svreport | Exporta la información de las sesiones creadas por el resto de herramientas a pdf, xml, csv y texto sin formato. |
| svcrash | Responde a los mensajes svwar y svcrack SIP con un mensaje que hace que las versiones anteriores se bloqueen. |

Tabla 6: Programas SIPVicious

C.2 Descarga de los ejecutables SIPVicious

Se pueden descargar los ejecutables de **SIPVicious** del siguiente repositorio:

<https://github.com/EnableSecurity/sipvicious>

Se descargará un ZIP que contendrá un directorio llamado `sipvicious-master`. Dentro del directorio se encontrará otro denominado `SIPVicious`, donde se hallarán los cinco programas de **SIPVicious**.

C.3 Pruebas

A continuación se mostrarán las pruebas realizadas al servidor de VoIP del sistema de telefonía del Departamento para demostrar que su configuración es segura.

Todas las pruebas que se detallan a partir de ahora se han realizado sin implementar la solución que se ha adoptado en este proyecto con el fin de poder observar las diferencias que se producen en el sistema de telefonía IP.

Primero se ha hecho uso del comando `svmap` para escanear un rango de direcciones IP y comprobar si existen servidores SIP escuchando. El comando es el siguiente:

```
./svmap.py x.x.x.x/y
```


donde x.x.x.x es la dirección de la red que se desea escanear e 'y' la máscara. En este caso queda como sigue:

```
MacBook-Pro-de-LAURA:sipvicius laumunpar$ ./svmap.py 193.147.162.128/27
| SIP Device      | User Agent      | Fingerprint |
|-----|-----|-----|
| 193.147.162.130:5060 | FPBX-2.11.0(11.24.0) | disabled |
```

Figura 55: SIPVicious-svmap

Como se puede observar, **SIPVicious** ha detectado al servidor de VoIP del Departamento en la dirección 193.147.162.130 y la versión que corre.

Seguidamente, se ha realizado un intento de enumeración de extensiones. El comando empleado para ello es el siguiente:

```
./svwar.py 193.147.162.130 -m INVITE --force
```

Se debe especificar el uso de mensajes INVITE, ya que por lo que se ha mencionado anteriormente los proveedores de *software* PBX han bloqueado el sondeo de puertos con mensajes REGISTER.

Tal como se ha mencionado en este proyecto, **SIPVicious** comienza el escaneo de extensiones en la extensión '100'. En el caso del Departamento, éste no dispone de ninguna extensión en ese rango, con lo que la herramienta no puede detectar ninguna extensión disponible.

```
MacBook-Pro-de-LAURA:sipvicius laumunpar$ ./svwar.py 193.147.162.130 -m INVITE --force
WARNING:TakeASip:using an INVITE scan on an endpoint (i.e. SIP phone) may cause it to ring and wake up people in the
middle of the night
WARNING:TakeASip:Bad user = SIP/2.0 401 - svwar will probably not work!
WARNING:TakeASip:We got an unknown response
ERROR:TakeASip:Response: 'SIP/2.0 401 Unauthorized\r\nVia: SIP/2.0/UDP 127.0.0.1:5060;branch=z9hG4bK-1202379558;rece
ived=79.156.46.88;rport=5060\r\nFrom: "100"<sip:100@193.147.162.130>;tag=31303001393132333037393639\r\nTo: "100"<sip
:100@193.147.162.130>;tag=as71ad2fbf\r\nCall-ID: 1572605004\r\nCSeq: 1 INVITE\r\nServer: FPBX-2.11.0(11.24.0)\r\nAll
ow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY, INFO, PUBLISH, MESSAGE\r\nSupported: replaces, time
r\r\nWWW-Authenticate: Digest algorithm=MD5, realm="asterisk", nonce="6641ce4f"\r\nContent-Length: 0\r\n\r\n'
WARNING:TakeASip:We got an unknown response
ERROR:TakeASip:Response: 'SIP/2.0 401 Unauthorized\r\nVia: SIP/2.0/UDP 127.0.0.1:5060;branch=z9hG4bK-2371968319;rece
ived=79.156.46.88;rport=5060\r\nFrom: "101"<sip:101@193.147.162.130>;tag=31303101333037323533313232\r\nTo: "101"<sip
:101@193.147.162.130>;tag=as7de4d5d0\r\nCall-ID: 2577772552\r\nCSeq: 1 INVITE\r\nServer: FPBX-2.11.0(11.24.0)\r\nAll
ow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY, INFO, PUBLISH, MESSAGE\r\nSupported: replaces, time
r\r\nWWW-Authenticate: Digest algorithm=MD5, realm="asterisk", nonce="1c46048e"\r\nContent-Length: 0\r\n\r\n'
WARNING:TakeASip:We got an unknown response
ERROR:TakeASip:Response: 'SIP/2.0 401 Unauthorized\r\nVia: SIP/2.0/UDP 127.0.0.1:5060;branch=z9hG4bK-1612017730;rece
ived=79.156.46.88;rport=5060\r\nFrom: "102"<sip:102@193.147.162.130>;tag=3130320132353933303630343337\r\nTo: "102"<s
ip:102@193.147.162.130>;tag=as32f29b15\r\nCall-ID: 4049548551\r\nCSeq: 1 INVITE\r\nServer: FPBX-2.11.0(11.24.0)\r\nA
llow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY, INFO, PUBLISH, MESSAGE\r\nSupported: replaces, ti
mer\r\nWWW-Authenticate: Digest algorithm=MD5, realm="asterisk", nonce="17b5f3fa"\r\nContent-Length: 0\r\n\r\n'
WARNING:TakeASip:We got an unknown response
```

Figura 56: SIPVicious-svwar sin opciones

Se podría afinar un poco más la búsqueda de extensiones indicándole en qué rango se encuentran estas:

```
./svwar.py -e 21-25 193.147.162.130 -m INVITE --force
```

```
MacBook-Pro-de-LAURA:sipvicious laumunpar$ ./svwar.py -e 21-25 193.147.162.130 -m INVITE --force
WARNING:TakeASip:using an INVITE scan on an endpoint (i.e. SIP phone) may cause it to ring and wake up people in the
middle of the night
| Extension | Authentication |
|-----|-----|
| 24        | reqauth        |
| 25        | reqauth        |
| 1550411336 | reqauth        |
| 22        | reqauth        |
| 23        | reqauth        |
| 21        | reqauth        |
```

Figura 57: SIPVicious-svwar

En este caso **SIPVicious** sí detecta las extensiones e indica si requieren autenticación o no. Todas las extensiones del Departamento requieren autenticación.

Finalmente, existe un comando que permite obtener la contraseña de las extensiones disponibles. Para ello, se ha creado un archivo diccionario con las contraseñas más comunes. El resultado ha sido el siguiente:

```
./svcrack.py 193.147.162.130 -u 45 -d contraseñas.txt
```

```
MacBook-Pro-de-LAURA:sipvicious laumunpar$ ./svcrack.py 193.147.162.130 -u 45 -d contraseñas.txt
ERROR:ASipOfRedWine:We got an unknown response
| Extension | Password |
|-----|-----|
| 45        | XXXXXXXX |
```

Figura 58: SIPVicious-svcrack

Una vez implementada la solución adoptada de este proyecto se puede comprobar como **SIPVicious** no tiene acceso al sistema de telefonía del Departamento, siendo imposible obtener resultados de los comandos anteriormente ejecutados.

```
MacBook-Pro-de-LAURA:sipvicious laumunpar$ ./svmap.py 193.147.162.128/27
WARNING:root:found nothing
MacBook-Pro-de-LAURA:sipvicious laumunpar$ ./svwar.py 193.147.162.130 --force
ERROR:TakeASip:socket error: timed out
WARNING:root:found nothing
MacBook-Pro-de-LAURA:sipvicious laumunpar$ ./svwar.py -e 21-25 193.147.162.130 -m INVITE --force
WARNING:TakeASip:using an INVITE scan on an endpoint (i.e. SIP phone) may cause it to ring and wake up people in the
middle of the night
ERROR:TakeASip:socket error: timed out
WARNING:root:found nothing
```

Figura 59: SIPVicious una vez implementada la solución adoptada de este proyecto

REFERENCIAS

- [1] José Carlos Moral Cuevas, «Instalación del sistema de telefonía VoIP del Departamento de Ingeniería Telemática de la Escuela Superior de Ingenieros» Proyecto Fin de Carrera, 2012.
- [2] João Marcelo Ceron, klaus Stending-Jessen and Cristine Hoepers, «Anatomy of SIP Attacks» ;login: THE USENIX MAGAZINE, vol. 37, nº 6, 2012.
- [3] Jianqiang Xin, «Security Issues and Countermeasure for VoIP» SANS Institute InfoSec Reading Room, 2007.
- [4] Asterisk: Open Source Communications Software: <http://www.asterisk.org/>.
- [5] Elastix: Your Linux PBX Unified Communications Solution: <http://www.elastix.org/>.
- [6] Tutoriales de Elastix: Telefonía IP Asterisk Elastix: <http://www.elastixtech.com/>.
- [7] Fail2ban: <https://www.fail2ban.org/>.
- [8] VoIP Info: <https://www.voip-info.org/>.
- [9] Asterisk Forums: <http://www.forums.asterisk.org/>.
- [10] SIPVicious: Tools for auditing SIP-based VoIP systems: <http://blog.sipvicious.org/>.
- [11] Gerardo Barajas Puente, «Securing Your Elastix System» Elastix Unified Communications Server Cookbook, 2015.
- [12] Asterisk Wiki: <https://wiki.asterisk.org/>.
- [13] Wired Magazine, «Danny Cohen engineered Internet take flight», 2012.
- [14] Joe Hallock, «A brief history of VoIP» University of Washington, vol I: The Past, 2004.
- [15] RFC2235: <http://www.faqs.org/rfcs/rfc2235.html>
- [16] David Endler and Mark Collier, «Hacking Exposed VoIP: Voice over IP Security Secrets & Solutions», 2006
- [17] Cisco, «How to protect your voice: Tips on IP Phone Security»
- [18] David Piscitello, «How to protect your VoIP network», Network World, 2006

[19] Peter Cox, «VoIP toll fraud attack racks up a £57k bill in two days», 2009