

MANUAL DE CONFIGURACION DE TRIXBOX CON SIP TRUNKING DE VOZTELECOM (OIGAA DIRECT)

HISTÓRICO DE MODIFICACIONES

<u>Revisión</u>	<u>Fecha</u>	<u>Modificaciones</u>	<u>Pág. afectadas</u>

Índice

MANUAL DE CONFIGURACION DE TRIXBOX CON SIP TRUNKING DE VOZTELECOM	1
(OIGAA DIRECT)	1
1. Objetivo del documento	3
Plataforma validada	3
2. Datos de la cuenta SIP	4
Datos de la cuenta SIP proporcionados por el operador	4
3. Versiones de software Epygi	5
4. Entorno de validación y configuración	6
Esquema de la plataforma validada	6
Configuración	7

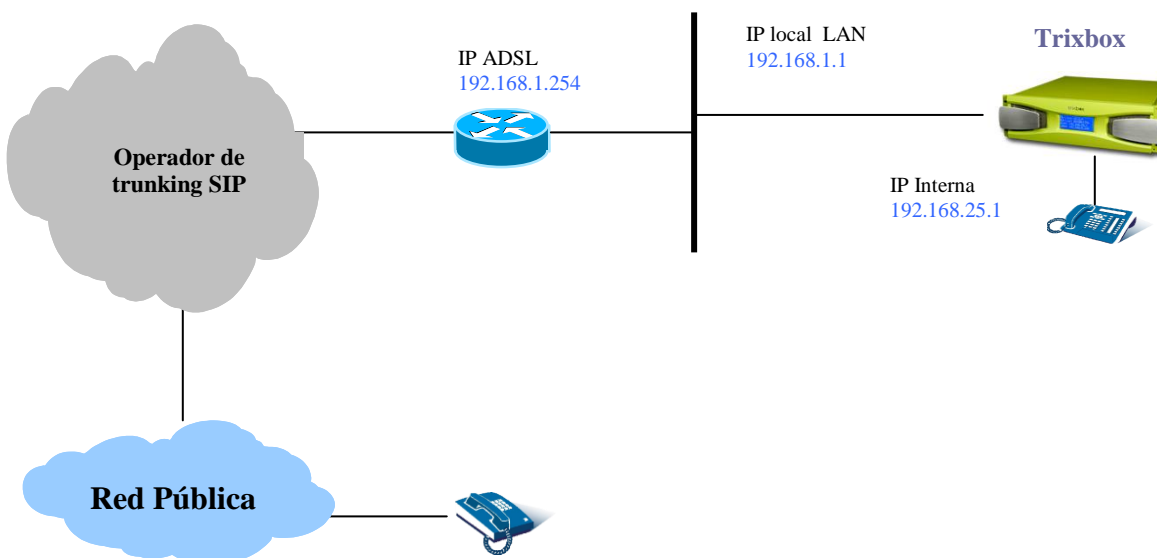
1. Objetivo del documento

El objetivo del documento es detallar el escenario, la programación y las prestaciones validadas en la interconexión entre una plataforma **Trixbox y Elastix** y un servicio de trunking IP. En este caso, el servicio de trunking es proporcionado por **Voz Telecom (servicio Oigaa Direct)**.

El servicio de trunking IP proporciona al usuario la posibilidad de realizar y recibir llamadas sobre una red IP.

Plataforma validada

Se ha validado la siguiente solución:



A continuación se indican los datos necesarios para configurar el sistema, así como las direcciones IP concretas utilizadas como ejemplo en esta nota.

IP pública estática	192.168.1.1
Gateway	192.168.1.254
Máscara de red	255.255.255.0
IP Interna	192.168.25.1
Servidor DNS	192.168.1.254

2. Datos de la cuenta SIP

Datos de la cuenta SIP proporcionados por el operador

Número de teléfono	885551703
Usuario de red	4455455573
Password de red	wRtVklGH
Proxy SIP	sip.voztele.com.mx
Supported codecs	G729, G711A/U, G723

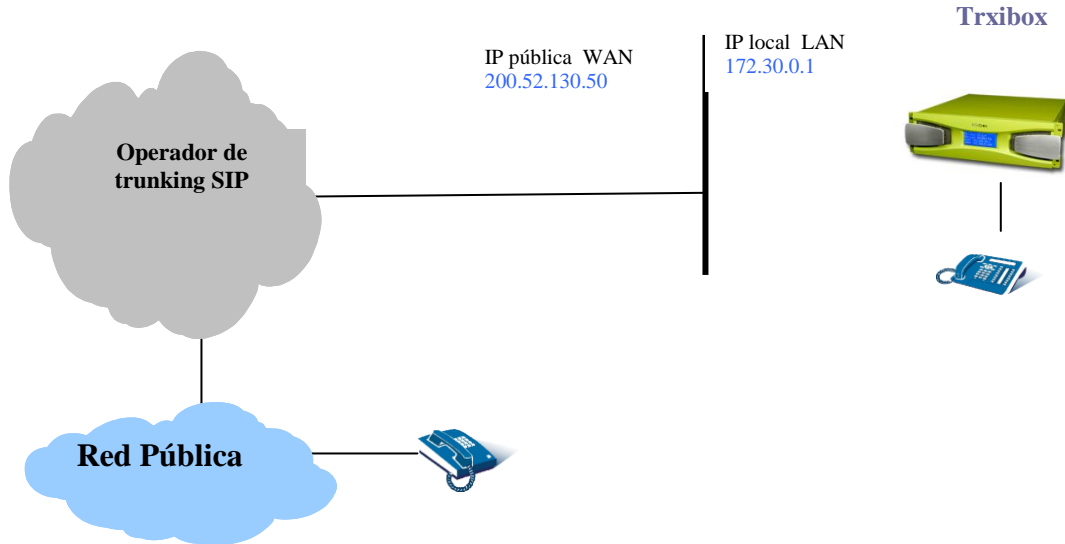
Los valores que aparecen en este apartado son ficticios y se utilizan como ejemplo durante la nota.

3. Versiones de software Trixbox

Versión: 2.6.1-13

4. Entorno de validación y configuración

Esquema de la plataforma validada

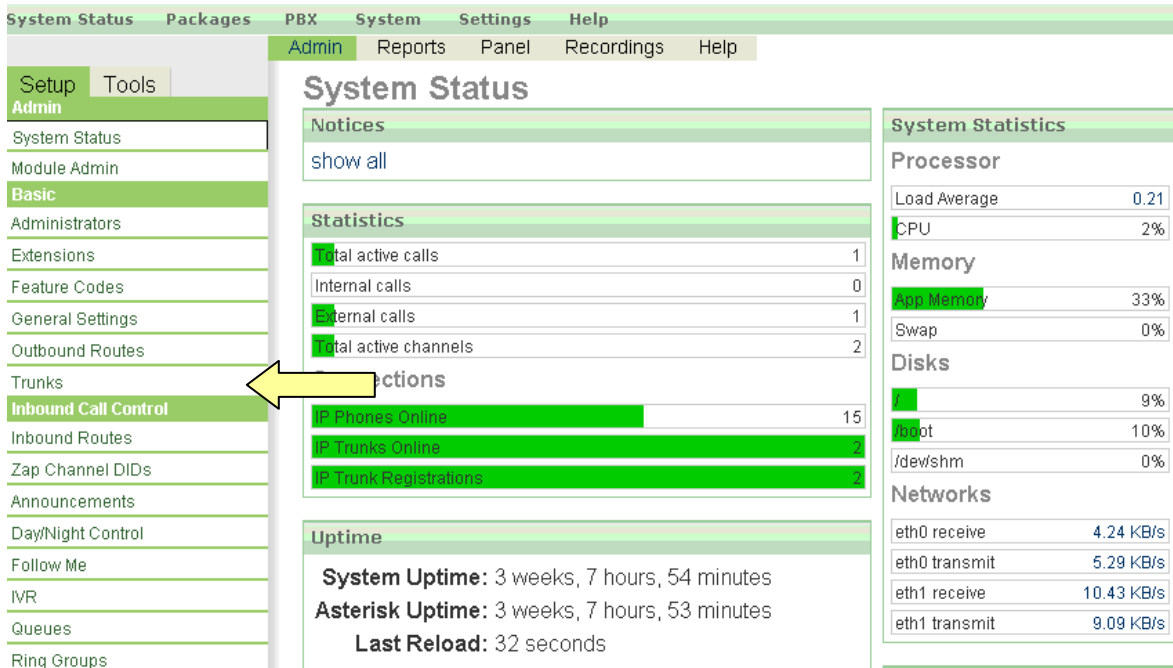


A continuación se indican los datos necesarios para configurar el sistema, así como las direcciones IP concretas utilizadas como ejemplo en esta nota.

IP pública estática	200.52.130.50
IP privada del Epygi	172.30.0.1
Máscara de red	255.255.0.0
Servidor DNS	200.52.130.1

Configuración

Para configurar una SIP tenemos que seleccionar Trunks y agregar [SIP Trunk SIP](#)



System Status

Notices
show all

Statistics

Total active calls	1
Internal calls	0
External calls	1
Total active channels	2

Actions

IP Phones Online	15
IP Trunks Online	2
IP Trunk Registrations	0

Uptime

System Uptime: 3 weeks, 7 hours, 54 minutes
Asterisk Uptime: 3 weeks, 7 hours, 53 minutes
Last Reload: 32 seconds

System Statistics

Processor

Load Average	0.21
CPU	2%

Memory

App Memory	33%
Swap	0%

Disks

SATA	9%
Xvopt	10%
/dev/shm	0%

Networks

eth0 receive	4.24 KB/s
eth0 transmit	5.29 KB/s
eth1 receive	10.43 KB/s
eth1 transmit	9.09 KB/s

Agregamos los siguientes datos:

Outbound Caller ID = DID

Trunk Name = 8780035

Peer Details

```
username=8780035
user=8780035
type=peer
secret=qMqTLKs
host=sip.voztele.com.mx
fromusername=8780035
fromuser=8780035
fromdomain=sip.voztele.com.mx
dtmfmode=auto
disallow=all
context=from-trunk
canreinvite=no
allow=g729&alaw&ulaw
```

PEER Details:

```
username=8780055
user=8780055
type=peer
secret=UtieKYXn
host=sip.voztele.com.mx
fromusername=8780055
fromuser=8780055
fromdomain=sip.voztele.com.mx
dtmfmode=auto
disallow=all
```

Incoming Settings

```
type=peer
insecure=port&port,invite
host=193.22.119.20
dtmfmode=auto
disallow=all
context=from-trunk
allow=g729&alaw&ulaw
```

Registration
RegisterString

Username:password@voztele.com.mx:5062/Username

8780035:qMqTLKs@sip.voztele.com.mx:5062/8780035

Incoming Settings

USER Context:

USER Details:

```
type=peer
insecure=port&port,invite
host=193.22.119.20
dtmfmode=auto
disallow=all
context=from-trunk
allow=g729&alaw&ulaw
```

Con nuestra troncal configurada es necesario dirigir las llamadas de entrada a alguna extensión válida o a algún IVR para lo cual ingresaremos a la opción [Inbound Routes](#) y seleccionaremos la opción que deseemos que sea nuestro destino para las llamadas que ingresen por nuestra línea OIGAA Direct, proporcionando como único dato el mismo DID que configuramos en nuestra línea de registro.

Ej. 8780035

Add Incoming Route

Add Incoming Route

Description:

DID Number:

Caller ID Number:

Para finalizar tenemos que seleccionar General Settings y en el apartado Security Settings seleccionar "Yes" para poder recibir llamadas desde cualquier troncal SIP.

System Status Packages PBX System Settings Help

Admin Reports Panel Recordings Help

Setup Tools

Admin

- System Status
- Module Admin
- Basic
- Administrators
- Extensions
- Feature Codes
- General Settings
- Outbound Routes
- Trunks
- Inbound Call Control
- Inbound Routes
- Zap Channel DIDs
- Announcements
- Day/Night Control
- Follow Me
- IVR
- Queues
- Ring Groups

System Status

Notices

show all

Statistics

Total active calls	1
Internal calls	0
External calls	1
Total active channels	2

Connections

IP Phones Online	15
IP Trunks Online	2
IP Trunk Registrations	2

Uptime

System Uptime: 3 weeks, 7 hours, 54 minutes
Asterisk Uptime: 3 weeks, 7 hours, 53 minutes
Last Reload: 32 seconds

System Statistics

Processor

Load Average	0.21
CPU	2%

Memory

App Memory	33%
Swap	0%

Disks

/	9%
/boot	10%
/devshm	0%

Networks

eth0 receive	4.24 KB/s
eth0 transmit	5.29 KB/s
eth1 receive	10.43 KB/s
eth1 transmit	9.09 KB/s

Security Settings

Allow Anonymous Inbound SIP Calls?

5. Seguridad

Sistema Operativo

- Sistemas Operativos Recomendados: Centos (en todas sus Versiones), Red Hat (en todas sus versiones).
- Actualizar el sistema operativo según se vayan haciendo liberaciones a versiones recientes. Esta función se conoce como *YUM UPDATE*.
- Tener actualizado el KERNEL del sistema operativo a la última versión.
- Desinstalar *portmap* y servicios asociados (*rpc, statd, nfs-kernel-server, etc.*).
- Habilitar el firewall del sistema operativo, instalar otro firewall (se han tenido buenos resultados utilizando *SHOREWALL*) o instalar un dispositivo externo equivalente.
- En el firewall, cerrar el acceso a todos los puertos que no deben estar permitidos. Esto es todos los que están por debajo del puerto 1024.
- Deshabilitar los servicios no necesarios (*Ej. Telnet, FTP, STP, SCP, PING*)
- Recomendamos no instalar otro software adicional a la aplicación de Voz.
- Realizar Cambios constantes del passwd de root, y que este sea manejado únicamente por el Administrador del equipo.
- Creación de cuentas por Usuario con sus permisos correspondientes. Ninguna deberá tener permiso de administrador.
- Desinstalar el servicio SSH puerto 22, o en caso de ser imposible, cambiar el puerto hacia cualquier otro. Esto únicamente será necesario si necesita acceder a la maquina de forma local.
- Utilizar IP tables o Netfilter para la creación de listas de acceso. Definir en estos las direcciones IP desde las cuales se podrá acceder remotamente (en caso de que asi lo requiera).
- Tener el sistema operativo Actualizado

Para la aplicación de ASTERISK

- Cambiar el PWD de la aplicación de voz. Los passwords deben de ser alfanuméricos y de no menos de 12 caracteres. Combinar letras, símbolos y números en cadenas de Mayúsculas y minúsculas aleatoriamente. (Ej. → Yg7#pQ1=fdHH)
- Cambiar el PWD del FREEPBX. Este password es diferente que el del punto anterior. OJO, este es uno de los errores más comunes tanto en TRIXBOX como en ELASTIX. Seguir las recomendaciones para creación del password del punto anterior.
- No utilizar el PWD de una extensión como la misma Extensión.
- Evitar la conexión en SSH utilizando exploradores de carpetas.

Siete pasos para mejorar la seguridad en SIP con Asterisk

- No aceptar SIP Authentication Request desde cualquier dirección: usar permit y deny en el sip.conf para permitir solo el pool de IP's que sepamos que van a intentar registrarse. Poner allowguest=no, en el sip.conf.
- Poner alwaysauthreject=yes en el sip.conf: Esta opción esta por defecto en "no", lo que va a permitir fugas de información de extensiones. Poniéndolo en "yes" vamos a denegar las bad authentication requests en usernames validos, denegando así a los atacantes remotos la habilidad de detectar extensiones con ataques de fuerza bruta.
- Usar passwords fuertes: Usar símbolos, números, y mezclar con letras mayúsculas y minúsculas, por lo menos que sean passwords de 12 dígitos de largo.
- Bloquear los puertos del AMI manager: Usar las líneas "permit=" y "deny=" en el manager.conf para reducir la cantidad de petición de conexiones sabiendo unicamente el host. Seguir Recomendaciones anteriores para creación de passwords.
- Permitir solo una o dos llamadas a la vez para usuarios SIP: usar la expresión call-limit=2.
- Crear los usuarios SIP diferentes de las extensiones: usar la dirección MAC de la tarjeta de red, o alguna combinación de una frase común + el hash de la extensión en MD5 (ejemplo: escribimos en el shell, "md5 -s elpassword 2550" 2550 sería la extensión?).
- Asegurarse que el contexto [default] es seguro: No permitir que llamantes no autenticados puedan llegar a algun contexto que permita realizar llamadas. Prohibir llamadas sin autenticación permanentemente poniendo "allowguest=no" en la sección [general] del sip.conf.

Otras Recomendaciones

- Evitar en la medida de lo posible utilizar direccionamiento homologado.
 - IP Privada
 - No hacer forwarding de puertos
 - No hacer DMZ
- Revisar frecuentemente el log de accesos en busca de intentos de conexión desconocidos
- Revisar frecuentemente los archivos que contiene los CDR's (Call Detail Records) en busca de llamadas desconocidas.

La mejor medida para evitar accesos a sus equipos es el control de usuarios y passwords. El administrador deberá ser responsable de esta información así como de la supervisión para acceso al servidor y también del usuario SIP y password de cada línea.