Guía de configuración del SIP trunk *net2phone*

Información para la configuración homologada del servicio de SIP Trunk ***net2phone*** , requerimientos y especificaciones.

Interconexión

La Autenticación se puede realizar por IP*, DIGEST (user y contraseña), IP+DIGEST ó IP/DIGEST.

- En caso que se utilice IP, deberá contar con una IP pública fija, la misma debe ser informada al equipo de ***net2phone***
- En caso de ser dinámica esta IP, se deberá utilizar autenticación DIGEST.

El dominio de destino de la señalización SIP para enviar llamadas:

- siptrunk.net2phone.com

Para llamadas entrantes se deberán crear 2 peers autorizando los 2 hosts desde donde recibirán las llamadas entrantes:

- 169.132.196.33:5060
- 206.20.196.19:5060

*En caso de que se autentique por validación IP se debe tener en cuenta lo siguiente, dependiendo de qué versión de **asterisk** se utilice, por favor configurar en trunk setup / incoming el campo “insecure” como se describe debajo:

- Versiones asterisk 1.6 y anteriores: Insecure=very
- Versiones asterisk superiores a 1.6: Insecure=invite

IP de media / Audio / RTP: (se negocia en la señalización)

Firewall

Se deben autorizar los siguientes rangos IP para la recepción de los paquetes RTP de media (UDP) como así los puertos que debajo se detallan, tanto para llamadas entrantes como salientes, desde los media proxy de ***net2phone***:

IP´s audio RTP:

- 204.13.140.0
- 216.53.0.0
- 66.33.128.0
- 206.20.0.0
- 169.132.0.0
- 66.33.160.0

IP de media:

- 200.115.186.65
- 200.115.187.65

Puertos:

- 5060 UDP
- 20000 al 24000 UDP

Se enviaran las llamadas al DID provisto por net2phone con un formato internacional y prefijo 011.
Ejemplo Argentina: 01154XXXXXXXXX

Plan de Discado

El equipo de net2phone le enviara el plan de discado asociado a su cuenta junto con las credenciales.

ANI

Por default ***net2phone*** envía sólo el ANI de cabecera de la cuenta, el cual será informado al cliente como también los adicionales si es que posee.

DTMF

Se deberán enviar los tonos DTMF en RFC 2833, payload 101.

- http://www.faqs.org/rfcs/rfc2833.ht

Requerimientos para un correcto funcionamiento del servicio Corporativo de SIP Trunk net2phone

Codecs

Para garantizar una buena calidad a cualquier destino es necesario que el Gateway o IP-PBX que origina las llamadas tenga soporte (en cualquier orden de prioridad) de los siguientes códecs = G729, G723, G711ulaw.

Recomendable:

- Códec Estándar de IDT: G729 ulaw y alaw

Latencia

Es recomendable que sea inferior a 100ms, máximo de 250ms.

Packet loss

No debe ser superior al 2%. Tanto en la red LAN como en el vínculo entre la IP-PBX del cliente y nuestra red.

Jitter

No debe ser superior a 30ms.

Ancho de Banda

Utilizando G729, se requiere un promedio de 30kbps simétricos por canal.

*En caso de que la interconexión entre el cliente y ***net2phone*** no sea dedicada y la visibilidad sea a través de Internet el cliente debe aplicar técnicas de priorización de tráfico para garantizar la conectividad entre el cliente y la red de ***net2phone*** (bloques mencionados anteriormente).

Canales Habilitados

Según el detalle de lo contratado se le habilitaran X cantidad de canales para llamadas entrantes o salientes concurrentes

Ejemplos de Configuración para centrales Asterisk

Autenticamos tráfico IP-PBX SIP Trunking por:

IP Authentication (IP address) o Digest Authentication (SIP account y SIP password)

Después de decidir qué tipo de autenticación usar, tendrá que establecer un SIP TRUNK con nuestro servidor proxy :

- siptrunk.net2phone.com

En el caso de haber optado por autenticación por ip deberá informar a ***net2phone*** la misma caso contrario registrar su SIP PBX con las credenciales provistas.

IP Authentication (IP Address)

El método de autenticación por IP es normalmente más sencillo y puede ser usada solamente cuando se tiene una dirección IP pública estática.
Aumenta la seguridad ya que su SIP Trunk sólo se podrá utilizar a partir de la dirección IP que proporcione.

A continuación detallamos una configuración básica para Asterisk para la autenticación por IP:

Outgoing Settings

[out-1]

type=peer
port=5060
username=<n° de cuenta>
fromuser=<n° de cuenta>
nat=auto
insecure=invite
ignoresdpversion=yes
host= siptrunk.net2phone.com
dtmfmode=rfc2833
context=from-trunk
canreinvite=no
disallow=all
allow=g729
allow=ulaw

qualify=no

Incoming Settings

[in-1]

disallow=all
type=peer
port=5060
nat=auto
insecure=invite
host=169.132.196.44
dtmfmode=rfc2833
context=from-trunk
canreinvite=no
allow=g729
allow=ulaw

[in-2]

disallow=all
type=peer
port=5060
nat=auto
insecure=invite
host=206.20.196.34
dtmfmode=rfc2833
context=from-trunk
canreinvite=no
allow=g729
allow=ulaw

* No es necesario "registration string" para IP Authentication.

Autenticación digest (usuario y contraseña)

A continuación detallamos una Configuración Básica para asterisk cuando utilizamos Digest Authentication (account y SIP Password):

Peer Detail

username=<account>
user=<account>
type=peer
secret= <password>
progressinband=never
fromuser=<account>
port=5060
nat=auto
insecure=very
ignoresdpversion=yes
host= siptrunk.net2phone.com
dtmfmode=rfc2833
context=from-trunk
canreinvite=no
disallow=all
allow=g729&ulaw

qualify=no

User Detail

username=<account>
user=<account>
type=user
port=5060
context=from-pstn
canreinvite=no
disallow=all
allow=g729&ulaw

Register String

Argentina:
register=>account:password@siptrunk.net2phone.com/siptrunking

Incoming Settings

[in-1]

disallow=all
type=peer
port=5060
nat=auto
insecure=invite
host=169.132.196.44
dtmfmode=rfc2833
context=from-trunk
canreinvite=no
allow=g729
allow=ulaw

[in-2]

disallow=all
type=peer
port=5060
nat=auto
insecure=invite
host=206.20.196.34
dtmfmode=rfc2833
context=from-trunk
canreinvite=no
allow=g729
allow=ulaw