

Application Note



Peering local de ZoomPhone (BYOC y BYOP) usando Ingate SIParator® SBC

Introducción.....	4
Acerca del sistema telefónico Zoom.....	4
Acerca de la familia de productos SIParator® SBC de Ingate.....	4
Escenarios de implementación	7
Topología de prueba de concepto	7
Configuración del sistema telefónico Zoom	8
Configuración de SIParator® SBC	8
Requisitos previos.....	8
Configuración de interfaces internas y externas	9
Otras configuraciones relacionadas con la red	14
Configuración de TLS para Zoom	15
Uso de la RSE.....	15
Uso de ACME.....	20
Adición de certificados de CA de Zoom para confiar en las conexiones TLS	24
Configurar el servidor NTP	25
Configuración de TLS con Zoom Versiones compatibles	26
Configuración de SIP en SIParator®	28
Configuración de la señalización TLS	28
Configuración de puertos SIP	29
Configurar el cifrado de medios.....	30
Definición de DNS Override para manejar trafico distribuido a Zoom con failover o balanceo	32
Configurar el enlace troncal SIP	33
Configuración del grupo troncal Zoom-PSTN.....	34
Configuración del grupo troncal PBX-PSTN	37
Configurar el plan de marcado	39
Habilitación de opciones SIP para solicitudes de Zoom.....	40
Ruta de salida de Zoom a PSTN.....	41
Ruta de salida de PBX a PSTN.....	43
Ruta PBX←→Zoom.....	43
Configuración de la transcodificación.....	45
Recomendaciones finales y otros puntos de interés	48
Documentación útil.....	48
Configuración y requisitos del teléfono Zoom.....	48

Grupos de rutas (Administrar)	49
Grupos SIP (Administrar).....	49
Reglas de enrutamiento (Administrar)	50
Declaraciones.....	50
Ayuda y soporte	50

Introducción

Acerca del sistema telefónico Zoom

Zoom Phone es un sistema telefónico en la nube creado de forma nativa para la plataforma Zoom. Zoom Phone, fluido y seguro, agiliza la experiencia de telecomunicaciones con funciones de clase empresarial en una plataforma unificada que incluye videoconferencias y chat de equipo. Ofrece una gestión centralizada, lo que permite a los equipos de TI aprovisionar y gestionar fácilmente a los usuarios, así como supervisar la calidad de las llamadas y los datos de uso en el portal de administración de Zoom.

Zoom Phone fluye fácilmente hacia otras soluciones de Zoom. Los usuarios de Zoom Phone pueden realizar y recibir llamadas telefónicas, trasladar la llamada a videoconferencia sin necesidad de que los participantes cuelguen o marquen a un puente separado, compartir contenido y enviar mensajes de chat desde las aplicaciones móviles y de escritorio de Zoom.

Zoom Phone, que funciona en la plataforma en la nube de Zoom distribuida por todo el mundo, está diseñado para ser fácil de usar y maximizar la calidad de voz y vídeo. Viene con numerosas características de seguridad y funciona con cifrado AES-GCM de 256 bits.

Zoom Phone ofrece una variedad de planes adaptados a las necesidades únicas de su negocio. Puede seleccionar un plan de precios que le permita pagar sobre la marcha o seleccionar entre números de teléfono locales y llamadas nacionales en 40+ países diferentes. También hay planes complementarios opcionales disponibles para las empresas que tienen al menos un usuario con licencia.

El peering de las instalaciones de Zoom Phone proporciona a las organizaciones flexibilidad y opciones fluidas para migrar sus cargas de trabajo de voz a la nube. Esto se logra proporcionando dos tipos de conexión; Premisa Peering de PSTN y/o PBX de peering local (formalmente denominado Bring Your Own PBX - BYOP). El peering PSTN de Zoom Phone permite a las organizaciones aprovechar el entorno PSTN de su operador de telefonía actual para la conectividad de Zoom Phone. Con esta funcionalidad, las organizaciones pueden conectar Zoom Phone con prácticamente cualquier operador de telefonía.

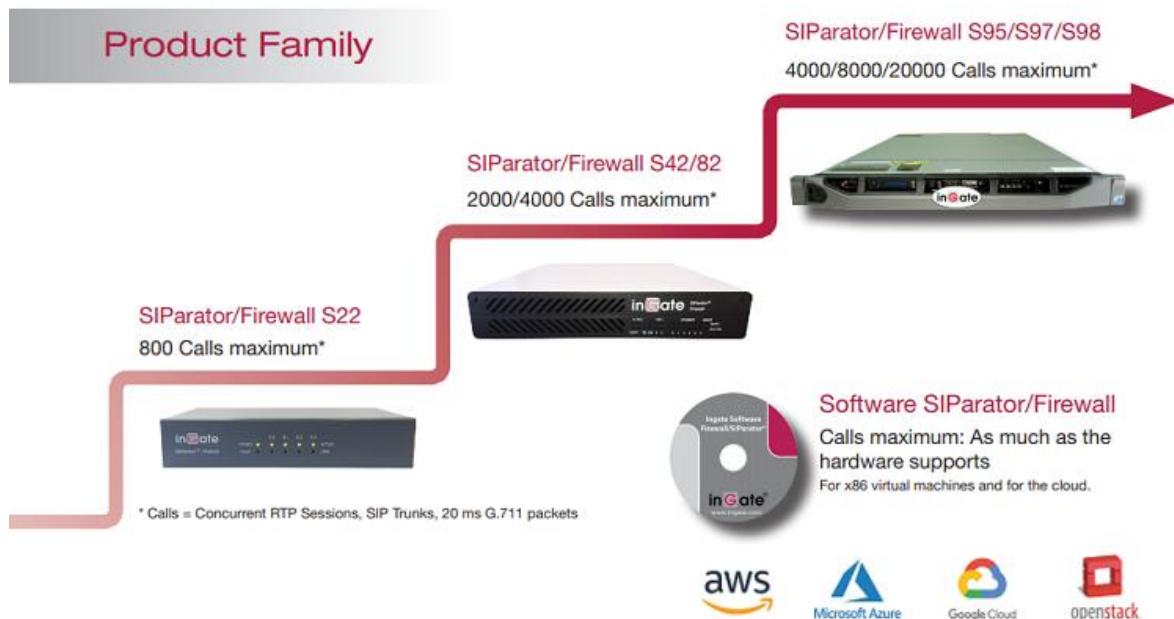
Acerca de la familia de productos SIParator® SBC de Ingate.

Un controlador de borde de sesión es un dispositivo que se conecta a un firewall de red existente para habilitar sin problemas las comunicaciones SIP (protocolo de inicio de sesión). Mientras que los firewalls tradicionales bloquean el tráfico SIP, incluidas las aplicaciones de misión crítica como la voz sobre IP (VoIP), el SBC de SIParator® de Ingate resuelve este problema, trabajando en conjunto con sus soluciones de seguridad actuales.

El SIParator® de Ingate es un controlador de borde de sesión empresarial (E-SBC) potente, flexible y rentable para la conectividad, la seguridad y la interoperabilidad SIP, como la conexión de PBX y soluciones de comunicaciones unificadas (UC) a proveedores de servicios de enlace troncal SIP.

El firewall® de Ingate, que siempre se incluye en el producto, convierte a Ingate SIParator en un dispositivo todo en uno para la seguridad de los datos, así como para el control de los bordes de las sesiones.

Los SIParators/Firewalls® de Ingate están disponibles en una amplia gama de modelos®:



El SIParator simplifica el enlace troncal SIP y facilita la conexión de puntos finales de UC remotos, la agregación de troncales SIP y la distribución de sesiones entre sitios y puntos de entrega de servicios. Se utiliza para la seguridad de las comunicaciones en tiempo real, la interoperabilidad SIP y la amplia conectividad. El SIParator® es compatible con todas las redes existentes y viene con un proxy SIP estándar y un registrador SIP. Tiene soporte para NAT y PAT, así como para TLS y SRTP para cifrar tanto la señalización SIP como los medios, eliminando el problema de seguridad más asociado con el uso de VoIP empresarial.

El sistema flexible de licencias complementarias permite a cualquier empresa mejorar la solución SIParator®/Firewall® para satisfacer sus necesidades en cualquier momento.

Con más de 10.000 instalaciones en todo el mundo, el SIParator® de Ingate viene en una amplia gama de capacidades y ha sido utilizado por empresas minoristas, instituciones financieras, empresas industriales, agencias gubernamentales, centros de llamadas y pequeñas y grandes empresas.

Escenarios de implementación

Topología de prueba de concepto

La interoperabilidad entre SIParator® SBC y Trunking con el sistema telefónico Zoom se ha probado en la siguiente configuración.

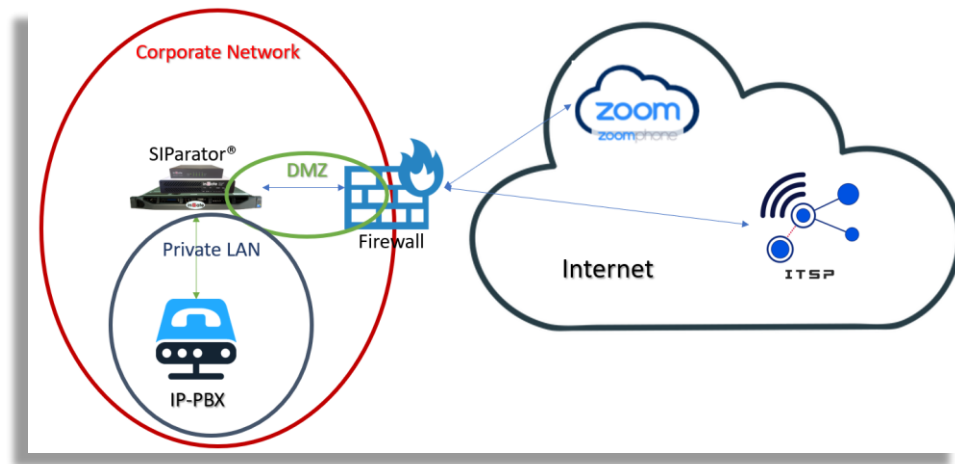


Figura 1: Diseño de implementación

La configuración de SIParator® en este documento mostrará cómo enrutar el tráfico PSTN hacia o desde el sistema Zoom Phone o la PBX del cliente existente. También se mostrará cómo enrutar llamadas entre usuarios de Zoom y usuarios de PBX (extensiones)

Suponemos que SIParator se ubicará detrás de un firewall existente en una DMZ.

Nuestro SIParator se configurará con 2 interfaces de red habilitadas (se recomienda encarecidamente no utilizar una sola interfaz), una estará en la DMZ mientras que la otra estará en la LAN privada interna donde se puede acceder a la IP PBX.

Tanto el sistema telefónico de Zoom como el proveedor de troncales SIP se encuentran en la WAN o en una red externa (Internet).

La IP-PBX se encuentra en la Red Privada

El sistema telefónico Zoom utiliza la señalización TLS, mientras que ITSP e IP-PBX utilizan SIP a través de UDP

El sistema telefónico Zoom funciona con medios cifrados (SRTP), mientras que ITSP e IP-PBX utilizan RTP simple para los medios.

Configuración del sistema telefónico Zoom

Para obtener instrucciones detalladas sobre cómo configurar el sistema telefónico de Zoom, puede consultar el Centro de ayuda de Zoom en

<https://support.zoom.us/hc/en-us/articles/360001297663-Getting-started-with-Zoom-Phone-admin->

NOTA: Antes de comenzar la configuración: ■ Póngase en contacto con su representante de Zoom para habilitar los grupos SIP y configurar troncales SIP que se dirijan a su SBC para su cuenta de Zoom Phone. ■ Asegúrese de tener credenciales de administrador de Zoom Portal. Tenga en cuenta que cada cliente debe tener una cuenta de administrador de Zoom Phone y que toda la configuración relacionada con Zoom Phone la realiza el cliente y no el operador.

Reemplazar con proceso de solicitud a soporte de la habilitación de BYOC y BYOP

Para mayor detalle revisar: [BYOC-P or BYOP-P deployment and connectivity options](#)

Configuración de SIParator® SBC

Requisitos previos

Para este caso de uso, la validación se ha realizado con la versión 6.4.1 de SIParator® y la licencia mínima necesaria debe incluir:

- Número de sesiones simultáneas de troncales sip. También se conoce como CCS y debe ser al menos el número máximo de sesiones SIP simultáneas que queremos que admita la solución asignada a 2 grupos troncales.
- Un grupo troncal admitirá llamadas simultáneas entre PBX y PSTN y el segundo troncal estará asociado a llamadas entre Zoom y PSTN
- También debemos tener en cuenta el número máximo de llamadas simultáneas entre Zoom y PBX, pero no usarán ningún grupo troncal.
- Esto se puede obtener con CCS compartido entre los 3 flujos (Zoom-PSTN, PBX-PSTN, Zoom-PBX). En este caso necesitarás:

CCS total necesario = Zoom-PSTN + PBX-PSTN + Zoom-PBX

Un grupo troncal adicional que comparte todos los CCS (licencia conocida como TGS)

Si tiene alguna duda o pregunta sobre las mejores opciones para obtener licencias, no dude en enviar sus preguntas a support@educronix.com

No se necesitan otras licencias para este caso de uso específico. Cuando se necesita transcodificación, no se necesita licencia, ya que la función de transcodificación es una funcionalidad incorporada puramente basada en software.

Asegúrese de que está utilizando uno de los dispositivos SIParator® de acuerdo con la carga de trabajo esperada, o una máquina virtual con el tamaño adecuado si está utilizando SIParator® de software

Antes de iniciar la implementación, asegúrese de que tiene:

- Una dirección IP pública que se utilizará exclusivamente para su SBC. Se puede asignar en su firewall y enrutar correctamente a la dirección IP de SIParator® DMZ.
- Certificados públicos emitidos por una de las CA compatibles con Zoom.

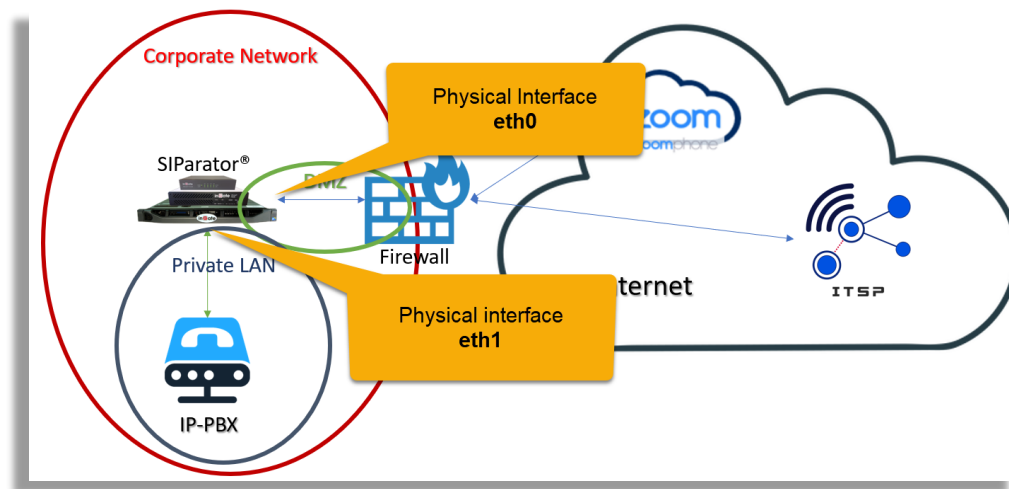
Configuración de interfaces de red IP

A las interfaces SBC se les asignarán direcciones IP para

- Interfaz externa. Que se encuentra en la DMZ y está asociado a la dirección IP pública.
- Interfaz interna. Que se utilizará para el acceso de gestión a SIParator® y también para llegar a los recursos SIP internos (p.e, IP-PBX).

SBC, en nuestro caso, está conectado a la WAN/Internet a través de una conexión DMZ.

En nuestro caso, todas las interfaces son puertos ethernet dedicados.



Configuración de interfaces internas y externas

Puede utilizar las tablas proporcionadas por Zoom para los medios y las IP de señalización. Utilizaremos las tablas disponibles en el momento en que se creó este documento para la documentación de Zoom.

Para la señalización y Media se pueden obtener los detalles de las IPs en este link: [BYOC-P or BYOP-P migration to the Common Platform](#)

Peering local de ZoomPhone (BYOC y BYOP)

A los efectos de este documento, seleccionaremos solo la región de Sur America, ya que nuestro laboratorio se está implementando para América Latina, sin embargo, puede usar las secciones apropiadas de la tabla según la región en la que se encuentre o se implemente.

Current Zoom Data Centers	Proposed new Zoom Data Centers
US01 - South America (SP/QR) Mexico and Central America (Querétaro, MX) Signaling IP: 149.137.69.247 Port: TCP/5061 Media Subnet: 149.137.69.0/24 Port: UDP/20000-64000 South America (São Paulo) Signaling IP: 64.211.144.247 Port: TCP/5061 Media Subnet: 64.211.144.0/24 Port: UDP/20000-64000	Zoom Common Platform - Central and South America Querétaro, MX Signaling IP: 159.124.128.84 Port: 5061 Media Subnet: 159.124.128.80/28 Port: 10000-65000 Dulles, VA, US Signaling IP: 206.247.121.212 Port: 5061 Media Subnet: 206.247.121.208/28 Port: 10000-65000

Dado que el momento de preparar este documento los datacenter están en transición de la localidad actual a la nueva, usaremos ambos grupos de IPs para nuestra configuración y así no tener dependencia alguna de cuando la migración se efectúe.

Para hacer más genérico este documento y facilitar al lector la implementación en cualquier región, tomando ventaja de nuevas funcionalidades del Ingate que permiten cargar las tablas de IPs como texto plano, estructuraremos los nombres de redes de esta forma:

Name	Subgroup	Lower Limit		Upper Limit (for IP ranges)		File
		DNS Name or IP Address	IP Address	DNS Name or IP Address	IP Address	
+ Zoom	Zoom Media					Add
	Zoom Signaling					Add
+ Zoom APAC	-					Edit
+ Zoom Austr	-					Edit
+ Zoom EMEA	-					Edit
+ Zoom Japan	-					Edit
+ Zoom Latam	-					Edit
+ Zoom Media	-					Edit
+ Zoom NA	-					Edit
+ Zoom Signaling	Zoom APAC					Add
	Zoom Austr					Add
	Zoom EMEA					Add
	Zoom Japan					Add
	Zoom Latam					Add
	Zoom NA					Add

Se puede observar que hay una línea para cada región, y cada una de ellas tiene habilitado un botón de "edit". Ese botón se habilita cuando para cualquier nombre de red escogemos el botón de "add" y

agregamos una tabla con un formato explicado en el manual de configuración de ingate acá: [Ingate Reference Guide](#)

Acá la lista de todos los archivos de texto que contienen dichas configuraciones de direcciones IP:

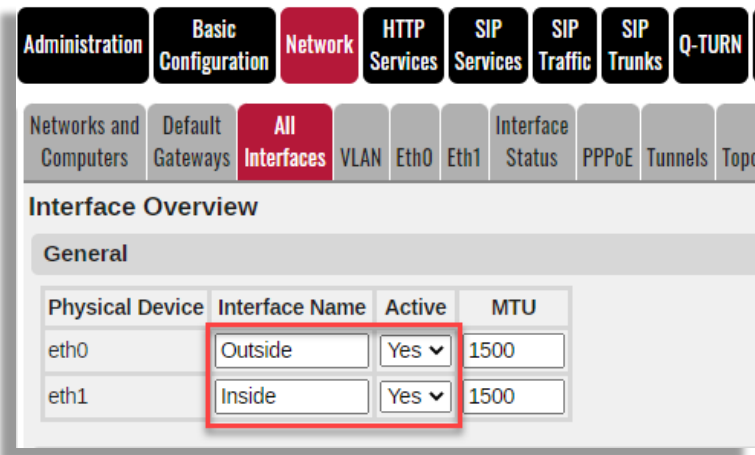
- APAC:
#APAC Old
149.137.41.246
207.226.132.198
#APAC New
170.114.156.212
170.114.185.212
- Australia:
#Australia Old
103.122.166.248
103.122.167.248
#Australia New
159.124.96.84
159.124.64.84
- EMEA:
#EMEA Old
213.19.144.198
213.244.140.198
#EMEA New
159.124.0.84
159.124.32.84
- Japan:
#Japan Old
209.9.211.198 #HK
101.36.167.237 #HK2
149.137.25.246
207.226.132.198
#Japan New
170.114.156.212
170.114.185.212
147.124.96.84
- Latam
#Latam Old
64.211.144.247
149.137.69.247
#Latam New
159.124.128.84
206.247.121.212
- North America NA
#North America Old

162.12.233.59
162.12.232.59
162.12.235.85
#North America New
144.195.121.212
206.247.121.212

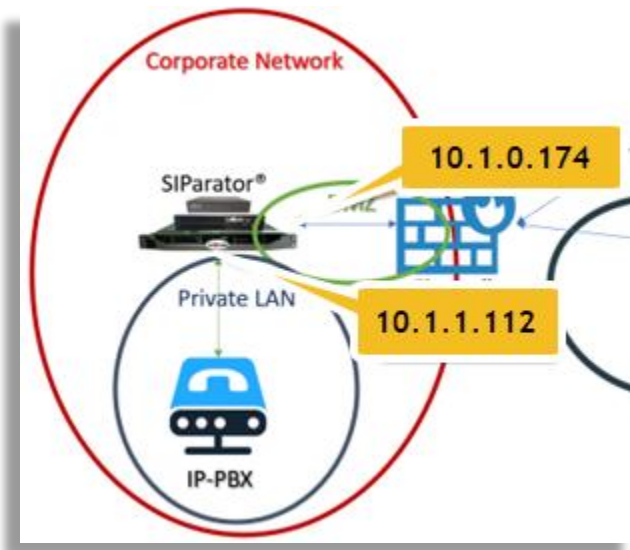
Por simplicidad para la Media hemos consolidado todas las IP de Media en un solo nombre (Resaltado en verde en la imagen arriba):

- Media
 - #North America
 - 162.12.232.0/24
 - 162.12.233.0/24
 - 162.12.235.0/24
 - #LATAM
 - 64.211.144.0/24
 - 149.137.69.0/24
 - #EMEA
 - 213.19.144.128/25
 - 213.244.140.0/24
 - #Australia
 - 103.122.166.0/24
 - 103.122.167.0/24
 - #APAC
 - 149.137.41.0/24
 - 207.226.132.0/24
 - #HK
 - 209.9.211.192/26
 - 101.36.167.0/24
 - #Japan
 - 207.226.132.0/24
 - 149.137.25.0/24
 - #New Media IP
 - 159.124.128.80/28
 - 101.36.167.0/24
 - 206.247.121.208/28
 - 144.195.121.208/28
 - 170.114.156.208/28
 - 170.114.185.208/28
 - 147.124.96.80/28
 - 159.124.96.80/28
 - 159.124.64.80/28
 - 159.124.0.80/28
 - 159.124.32.80/28

Asegúrese de que 2 interfaces estén habilitadas (activas). En nuestro caso también estamos asignando un nombre a cada uno (inside para eth1 y Outside para eth0)



Mirando nuestra topología:



En nuestro caso,

- Red DMZ: 10.1.0.0/24
- Red LAN: 10.1.1.0/24
- Puerta de enlace predeterminada: 10.1.0.1

Peering local de ZoomPhone (BYOC y BYOP)

Directly Connected Networks (Help)									
Name	Address Type	DNS Name or IP Address	IP Address	Netmask / Bits	Network Address	Broadcast Address	Interface or Tunnel	VLAN Id	VLAN Name
eth0	Static	10.1.0.174	10.1.0.174	24	10.1.0.0	10.1.0.255	Outside (eth0)		-
eth1	Static	10.1.1.112	10.1.1.112	24	10.1.1.0	10.1.1.255	Inside (eth1)		-

Ruta estática para la puerta de enlace predeterminada:

Static Routing (Help)							
Routed Network				Router		Interface or Tunnel	Delete Row
DNS Name or Network Address	Network Address	Netmask / Bits	Dynamic	DNS Name or IP Address	IP Address		
default	default		-	10.1.0.1	10.1.0.1	Outside (eth0)	☐

Otras configuraciones relacionadas con la red

Asignemos la dirección del servidor DNS. En nuestro caso vamos a utilizar Google DNS 8.8.8.8

inGate Zoom BYOC test

Administration **Basic Configuration** **Network** **HTTP Services** **SIP Services** **SIP Traffic** **SIP Trunks** **Q-TURN** **Virtual Network**

Basic Configuration **Access Control** **RADIUS** **SNMP** **Dynamic DNS Update** **Certificates** **ACME** **TLS** **Advanced Settings** **SIP Trunk**

General

Name of this SIParator: Zoom BYOC te

Default domain: .

Version of Software SIParator/Firewall

Check for new versions of Software SIParator/Firewall: ☐ Yes ☒ No

Date of last successful version check: Not available

Software version in use: 6.4.1

Policy For Ping To the SIParator

☐ Never reply to ping

☐ Only reply to ping to the same interface

☒ Reply to ping to all IP addresses

IP Policy (Help)

☐ Discard IP packets

☒ Reject IP packets

☐ Reject IP packets via TCP Reset

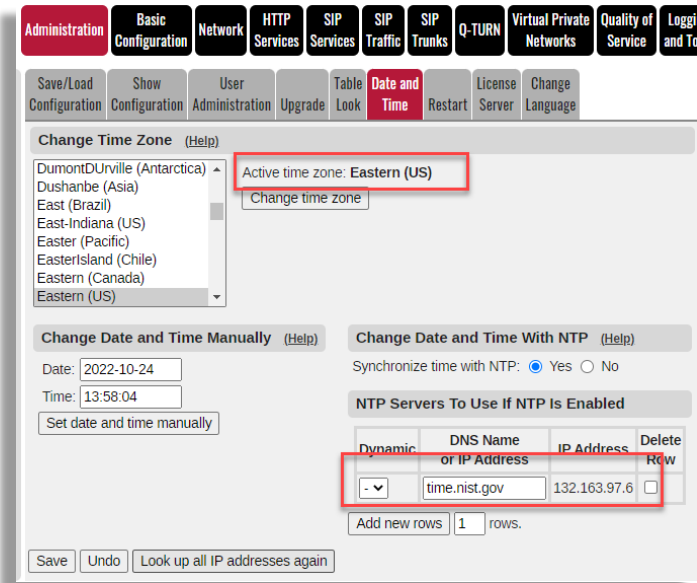
DNS Servers (Help)

No.	Dynamic	DNS Name or IP Address	IP Address	Delete Row
1	-	8.8.8.8	8.8.8.8	☐

Add new rows: 1 rows

También puede asignar un nombre a este SIParator. El nombre se mostrará en las etiquetas de su navegador.

Asignemos también un servidor NTP y un tiempo de configuración para el SIParator®. Suponemos que se encuentra en la zona horaria EST.



Configuración de TLS para Zoom

En esta sección, habilitaremos TLS para configurar la conectividad con el sistema telefónico Zoom.

Para habilitar TLS, necesitaremos los certificados públicos adecuados. Con SIParator hay dos formas de adquirir, instalar y mantener certificados TLS.

- **Uso CSR.** Generando la Solicitud de Firma desde el SIParator, envíela a la Autoridad de Certificación para obtener el certificado firmado y los certificados intermedios (si es necesario) e instalarlos en el SIParator®.
- **Uso de ACME.** Usar SIParator integrado en el cliente ACME y usar la autoridad habilitada para ACME adecuada de conformidad con las CA aceptadas por Zoom.

Uso de la RSE

En primer lugar, tendremos que crear una CSR (Solicitud de Firma de Certificado).

En Certificados de configuración básica → Certificados → privados, agregue una nueva fila:

Asigne un nombre y haga clic en "Crear nuevo"

Rellene la información solicitada y asegúrese de que el DNS de la extensión Common Name y SubjectAltName apunte al FQDN de SIParator que se resuelve en la dirección IP pública asociada a la interfaz externa:

Expire in (days) y Common Name (CN) son campos obligatorios.

Todos los campos restantes se pueden dejar en los valores predeterminados.

Haga clic en "Crear una solicitud de certificado X.509"

Key Length and Signature Algorithm

Select the key length and the signature algorithm that you want to use when creating a certificate or a certificate request.

Key length (bits):

Signature algorithm:

ACME

Use the ACME protocol for this X.509 certificate request: ☐ Yes ☒ No

If you generate several certificates with identical data you should make sure they have different Serial number:

*

Fields marked with "*" are mandatory.

La solicitud de certificado se mostrará de la siguiente manera:

Subject: /C=US/ST=FL/L=Weston/O=Educronix/OU=Engineering/CN=byoc.edx-labs.com/emailAddress=ernesto@educronix.com
SubjectAltName: DNS:byoc.edx-labs.com

Aplicar cambios

Administration **Basic Configuration** **Network** **HTTP Services** **SIP Services**

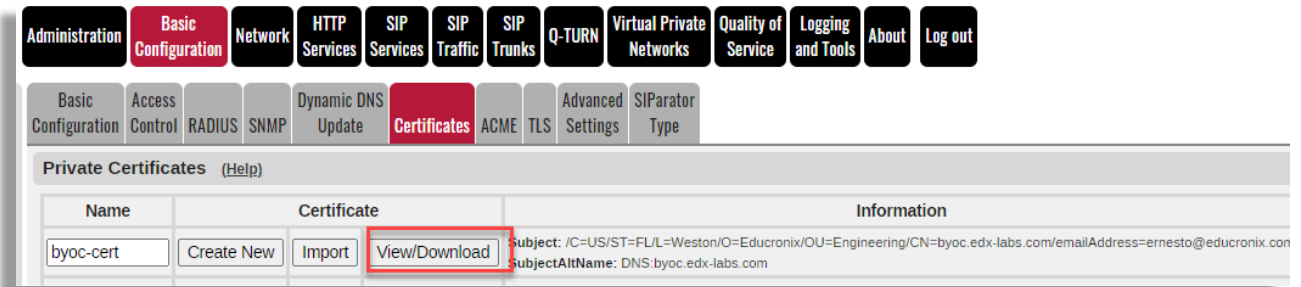
Changes have been made to the p

Save/Load Configuration seconds

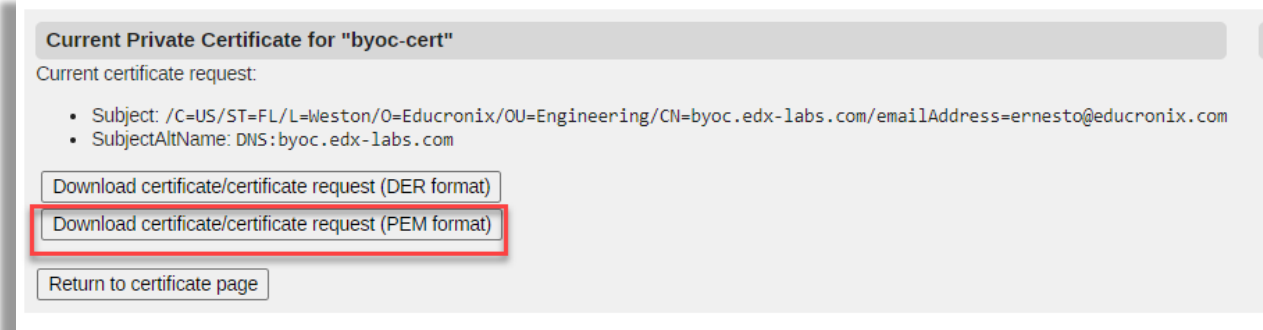
☐ On e
☐ On t
☐ Neve

Vuelva al certificado y haga clic en "Ver/Descargar"

Peering local de ZoomPhone (BYOC y BYOP)



Descargue el certificado en formato PEM o DER. Dependerá de la CA que vayas a utilizar para firmarlo y cuál le queda mejor. Usaremos PEM para nuestro ejemplo.



El archivo descargado debería verse así:

```
-----BEGIN CERTIFICATE REQUEST-----
MIIDDDCCAFQCAQAwgZcxZAJBgNVBAYTA1VTMQswCQYDVQQIEwJGTDEPMA0GA1UE
kAI2B3mQyjs2J4Ac65G548HEhmIkGx94oIhjQ60Kgx47aDYQVQV263OYq6+8NV35
s7b+UOfjqGsz7+m/g/PZiw6Rvh2fVM2V+Uuj5d9j3TTweRjhb7V325NEmdw/SXCr
SO6K0CZWyl5sr5mv6FQUNw==
-----END CERTIFICATE REQUEST-----
```

Utilícelo para solicitar el certificado firmado a la autoridad de certificación que haya seleccionado.

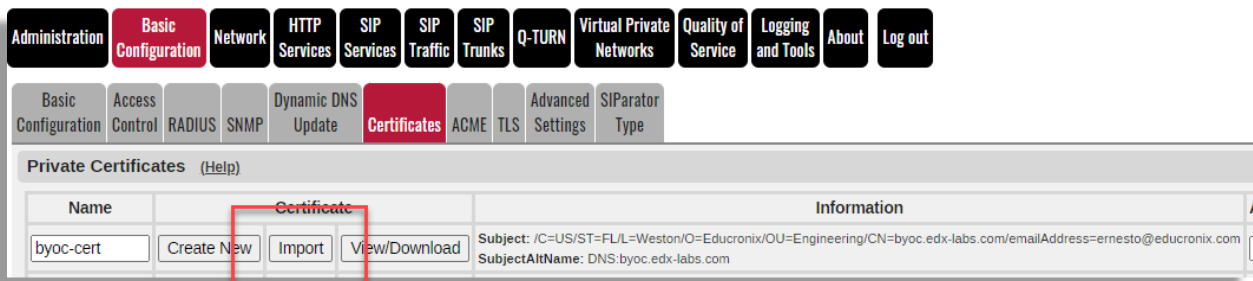
Una vez firmado te proporcionarán un conjunto de archivos, normalmente 2:

- Certificado firmado
- Certificados de paquete de intermediarios.

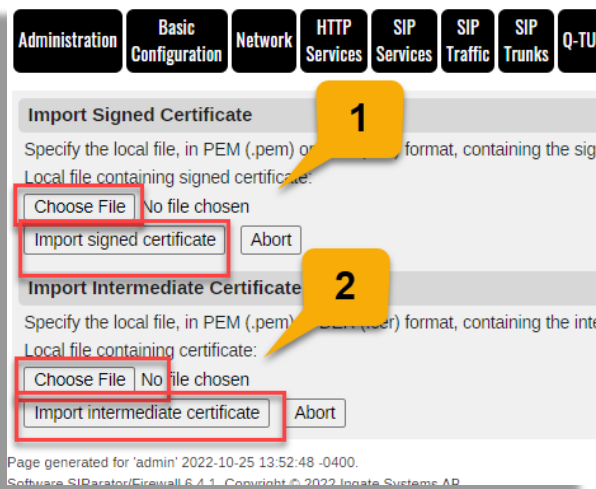
Similar a esto:

☒		byoc_edx-labs_com.ca-bundle	10/21/2022 1:47 PM	CA-BUNDLE File	5 KB
☒		byoc_edx-labs_com.crt	10/21/2022 1:47 PM	Security Certificate	3 KB

Deberá cargar el certificado firmado, así como el paquete de CA como certificados intermedios. Utilice el botón "Importar" para hacerlo:

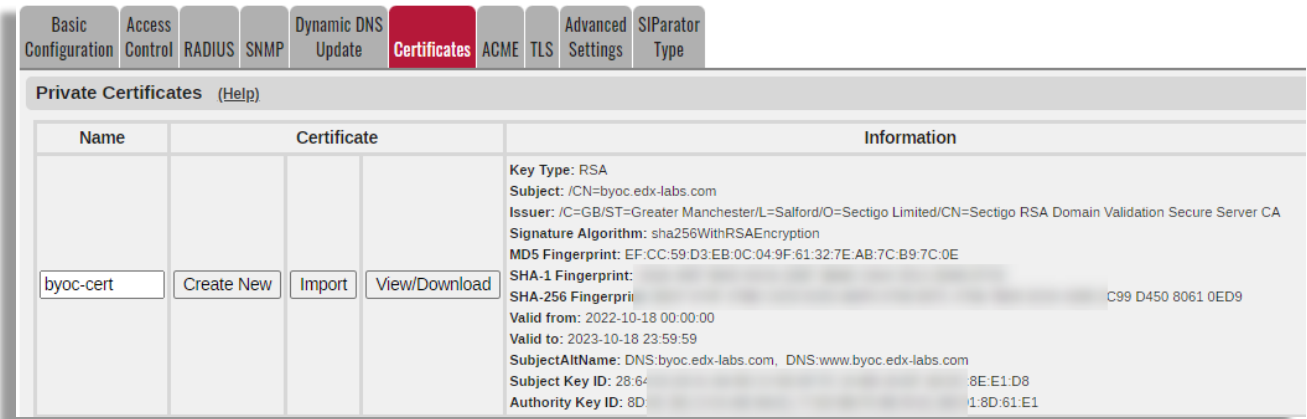


Primero importe el certificado, guárdelo y aplíquelo y, a continuación, cargue el paquete.



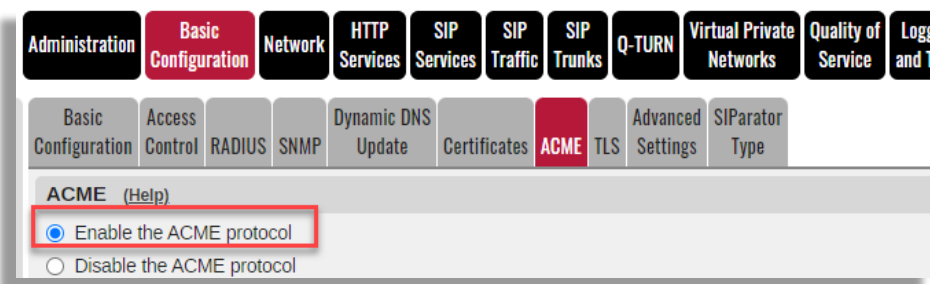
Guarde y vuelva a aplicar los cambios.

Debería poder ver el nuevo certificado firmado de forma similar a este:



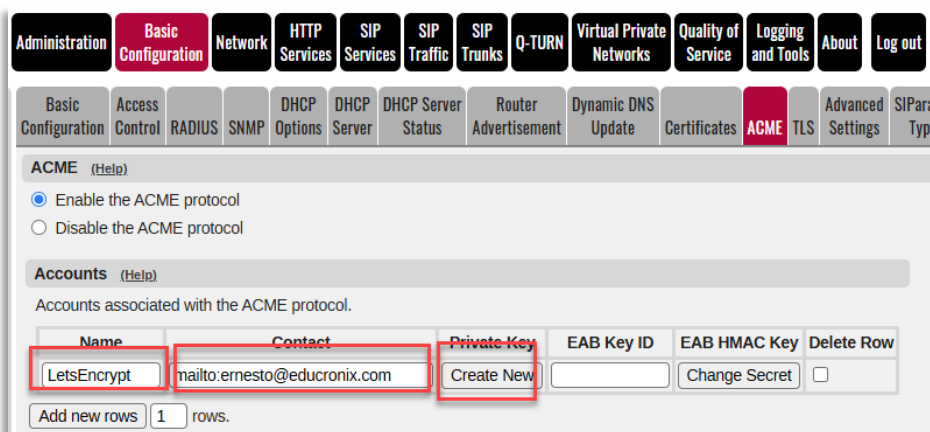
Uso de ACME

Antes de crear el certificado, necesitaremos tener habilitada y configurada correctamente la función SIPParator® ACME.



A los efectos de este documento, hemos seleccionado una Autoridad de Certificación que admita el protocolo ACME y que cumpla con los requisitos de Zoom.

En nuestro caso usaremos Let's Encrypt que hemos confirmado que funciona correctamente con Zoom.



- Asignar nombre

- Agregue información de contacto con el formato <mailto:xxxxx@yyyy.zzz> para proporcionar quién recibirá actualizaciones y notificaciones de la CA.
- Genere una "Clave privada" presionando "Crear nueva"

Agregar el servicio

Services (Help)

A service that supports the ACME protocol.

Name	Domain or IP	Directory Path	Trusted CA	Delete Row
LetsEncrypt	acme-v02.api.letsencrypt.org	directory	-	☐

Add new rows 1 rows.

- Asignar un nombre
- Introduzca el dominio proporcionado por la CA (para Let's Encrypt es "acme-v02.api.letsencrypt.org")
- Introduzca la ruta del directorio según lo proporcionado por la CA (para Let's Encrypt es "directory")

Agregue un nombre de dominio que se utilizará y al que se hará referencia al crear nuevos certificados administrados por ACME.

Domains (Help)

Domains that should be available to use with the ACME protocol.

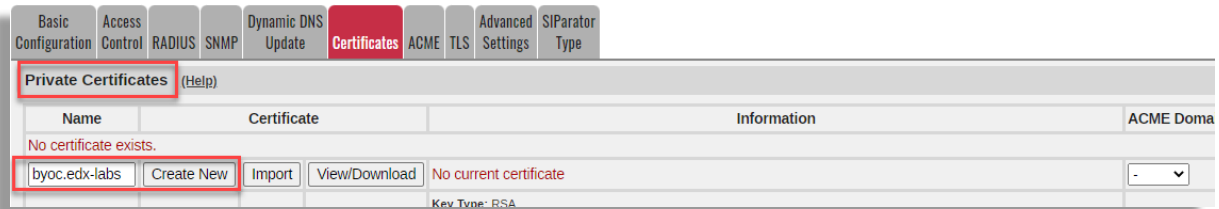
Name	HTTP-01 Challenge Address	Service	Account	Renewal Interval (%)	Delete Row
EducronixAcme	eth0 (10.1.0.174)	LetsEncrypt	LetsEncrypt	67	☐

- Asignar un nombre
- Seleccione la interfaz que estará orientada hacia el exterior (Internet)
- Seleccione el servicio y la cuenta (creados anteriormente).
- Mantenga el valor predeterminado del 67% para establecer cuándo se activará la solicitud de renovación

Ahora estamos listos para crear el certificado usando ACME.

Al igual que en "Uso de CSR" crearemos una Solicitud de Firma de Certificado, pero en este caso seleccionaremos la etiqueta ACME.

Agregue una nueva fila en Certificados Privados y asigne un nombre, haga clic en "Crear Nuevo":



Completa la información aquí:

Create Certificate or Certificate Request

Fill in the certificate data for "byoc.edx-labs" below, then create either a certificate or a certificate request. After generating a certificate request, and having it signed by a signing authority, you can import it back into SIParator.

Expire in (days): Country code (C): Organization (O):

Common Name (CN): State/province (ST): Organizational Unit (OU):

Email address: Locality/town (L):

SubjectAltName Extension

Enter the alternative names that you want to add to a certificate or a certificate request. Multiple values can be added by using comma separation.

Email:

URI:

DNS:

IP:

Notar:

- Caducidad y Nombre común son campos obligatorios, sin embargo, la autoridad de certificación definirá Caducidad independientemente del valor que introduzca.
- El nombre común y el DNS deben coincidir con el FQDN asociado a la dirección IP pública de SIParator®.

- Esto crea un certificado autofirmado temporal hasta que la CA proporciona el nuevo certificado firmado.
- Asegúrese de asociar el dominio ACME a este nuevo certificado.

[illegible]

En unos segundos más, verá el nuevo certificado ya firmado por la CA compatible con ACME de su elección.

[illegible]



Aviso La autoridad de certificación USERTrust RSA está incluida en las CA aceptadas por Zoom.

Si tiene preguntas sobre otras opciones de ACME, no dude en enviar sus consultas a support@educronix.com

Adición de certificados de CA de Zoom para confiar en las conexiones TLS

En el momento en que se publica este documento, todos los certificados de Zoom están firmados por DigiCert. Debe agregar todos los certificados raíz de DigiCert en la sección CA de la configuración básica de SIParator®.

Aquí solo tiene que añadir un paquete que incluya certificados raíz DigiCert. Una buena fuente para este paquete se puede encontrar aquí: <https://curl.se/docs/caextract.html>

O puede descargar todos los certificados raíz de CA necesarios para DigiCert directamente aquí:

<https://cacerts.digicert.com/DigiCertGlobalRootCA.crt.pem>

<https://cacerts.digicert.com/DigiCertGlobalRootG2.crt.pem>

<https://cacerts.digicert.com/DigiCertGlobalRootG3.crt.pem>

En cualquier caso, para instalar cualquiera de los Bundle o certificados Cas específicos mencionados anteriormente, puedes hacerlo aquí:

En Certificados de configuración básica → , en la sección Certificado de CA:

Name	CA Certificate	CA CRL	Information	Delete Row
No value given. Bundle	No value given. Change/View	Change/View	No current certificate	☐

Add new rows 1 rows.

- Asigna un nombre (Bundle en nuestro caso)
- Haga clic en Certificado de CA "Cambiar/Ver"

Specify the local file, in PEM (.pem) or DER (.cer) format, containing the CA certificate.

Local file containing CA certificate:

Choose File cacert (9).pem

Import CA certificate Abort

- Selecciona el archivo que descargas en la sección anterior
- Haga clic en "Importar certificado de CA"

En el caso del paquete, verá alrededor de 142 certificados cargados con el mismo nombre.

Administration Basic Configuration Network HTTP Services SIP Services SIP Traffic SIP Trunks

Changes have been made to the preliminary configuration.

- 142 CA certificates imported.

Basic Configuration Access Control RADIUS SNMP Dynamic DNS Update Certificates ACME TL

Aplique y guarde los cambios.

Configurar el servidor NTP

Para tener SIParator® bien sincronizado con su zona horaria, haga la configuración correcta aquí:

Administration **Basic Configuration** **Network** **HTTP Services** **SIP Services** **SIP Traffic** **SIP Trunks** **Q-TURN** **Virtual Private Networks** **Quality of Service** **Logging and Tools**

Save/Load Configuration Show Configuration User Administration Upgrade Table Look **Date and Time** Restart License Server Change Language

Change Time Zone (Help)

DumontDURville (Antarctica) Dushanbe (Asia) East (Brazil) East-Indiana (US) Easter (Pacific) EasterIsland (Chile) **Eastern (Canada)** **Eastern (US)**

Active time zone: **Eastern (US)**

Change time zone

Change Date and Time Manually (Help)

Date: 2022-10-26 Time: 09:58:33 Set date and time manually

Change Date and Time With NTP (Help)

Synchronize time with NTP: ☒ Yes ☐ No

NTP Servers To Use If NTP Is Enabled

Dynamic	DNS Name or IP Address	IP Address	Delete Row
☒	time.nist.gov	132.163.97.6	☐

Add new rows 1 rows.

Configuración de TLS con Zoom Versiones compatibles

Se sabe que Zoom solo admite TLS v1.2. En esta sección, crearemos un perfil TLS que incluya solo TLSv1.2 y se utilizará en la configuración de TLS para SIP más adelante en este documento.

The screenshot shows the SIPParator configuration interface. The top navigation bar includes tabs for Administration, Basic Configuration (selected), Network, HTTP Services, SIP Services, SIP Traffic, SIP Trunks, Q-TURN, Virtual Private Networks, Quality of Service, Logging and Tools, and About. Below this, a sub-navigation bar includes Basic Configuration, Access Control, RADIUS, SNMP, Dynamic DNS Update, Certificates, ACME, TLS (selected), Advanced Settings, and SIPParator Type.

The main content area is divided into two sections: TLS Settings and Protocols.

TLS Settings (Help)

Name	Protocols	Ciphers	Diffie-Hellman Group	ECDH Curve	Delete Row
DTLSv1.x	DTLSv1.x	HIGH	MODP2048 (Group 14)	NIST P-256 (secp256r1)	☐
SSLv3.0	SSLv3.0	HIGH	MODP2048 (Group 14)	NIST P-256 (secp256r1)	☐
TLSv1.2	TLSv1.2	HIGH	MODP2048 (Group 14)	NIST P-256 (secp256r1)	☐
TLSv1.x	TLSv1.x	HIGH	MODP2048 (Group 14)	NIST P-256 (secp256r1)	☐
TLSv1.x & SSL	TLSv1.x & SSLv3.0	HIGH	MODP2048 (Group 14)	NIST P-256 (secp256r1)	☐

Add new rows rows.

Protocols (Help)

Name	Protocol	Delete Row
+ DTLSv1.x	DTLSv1.0	☐
	DTLSv1.2	☐
+ SSLv3.0	SSLv3.0	☐
+ TLSv1.2	TLSv1.2	☐
+ TLSv1.x	TLSv1.1	☐
	TLSv1.2	☐
+ TLSv1.x & SSL	SSLv3.0	☐
	TLSv1.0	☐
	TLSv1.1	☐
	TLSv1.2	☐

Add new rows groups with rows per group.

- Agregue una nueva entrada en la sección Protocolos que incluya solo TLSv1.2, lo llamamos "TLSv1.2"
- Guarde y, a continuación, agregue una nueva entrada en la tabla Configuración de TLS, como se muestra en la imagen anterior. También lo llamamos "TLSv1.2"

Configuración de SIP en SIParator®

Ahora configuraremos toda la configuración relacionada con la señalización para SIP.

Configuración de la señalización TLS

Signaling Encryption (Help)

☒ Enable signaling encryption
☐ Disable signaling encryption

TLS Connections On Different IP Addresses (Help)

IP Address	Own Certificate	Use CN FQDN	Require Client Cert	TLS	Delete Row
eth0 (10.1.0.174)	byoc-cert	No	Yes	TLSv1.2	☐

Add new rows 1 rows.

Making TLS Connections (Help)

Default own certificate: byoc-cert Use TLS: TLSv1.2

TLS CA Certificates (Help)

CA	Delete Row
BundleCA	☐

Add new rows 1 rows.

- Agregue un nuevo raw en "Conexiones TLS en diferentes direcciones IP"
- Asocie su interfaz externa (eth0) para recibir y generar tráfico TLS
- Seleccione el certificado a presentar por SIParator® (el que creamos anteriormente).
- Deshabilite "Usar FQDN de CN" y habilite "Requerir certificado de cliente" para que cumpla con los requisitos de soporte de Zoom MTLS.
- Seleccione el perfil creado recientemente para TLSv1.2
- Utilice el mismo certificado que el predeterminado para cualquier otra conexión TLS
- Agregue los certificados raíz de CA de confianza en función de lo que configuró anteriormente.

También dejará los siguientes dos ajustes en "No" como se muestra aquí:

Check Server Domain Match [\(Help\)](#)

Check if the server domain matches the certificate:

☐ Yes ☒ No

Allow Wildcard in Server Certificates [\(Help\)](#)

Allow Wildcard in Server Certificates:

☐ Yes ☒ No

Configuración de puertos SIP

Ahora necesitaremos asociar los puertos que se usarán para SIP (UDP/TCP y/o TLS)

Vaya a Configuración básica de servicios SIP →

Administration **Basic Configuration** **Network** **HTTP Services** **SIP Services** **SIP Traffic** **SIP Trunks** **Q-TURN** **Virtual Private Networks** **Quality of Service**

Changes have been made to the preliminary configuration, but have not been saved.

Basic Settings **Signaling Encryption** **Media Encryption** **Media Transcoding** **Interoperability** **Sessions and Media** **Remote SIP Connectivity** **VoIP Survival**

SIP Module [\(Help\)](#)

☒ Enable SIP module

☐ Disable SIP module

SIP Signaling Ports [\(Help\)](#)

Active	Port	Transport	Intercept	Allow From/to	Comment	Delete Row
Yes	5060	UDP and TCP	Yes	-		☐
Yes	5061	TLS	Yes	Zoom Latam		☐

Add new rows rows.

SIP Media Port Range [\(Help\)](#)

Ports: -

Public IP Address for NATed SIP Parator [\(Help\)](#)

DNS Name	IP Address

- Asegúrese de que el módulo SIP esté habilitado
- De forma predeterminada, el puerto de señalización SIP 5060 para UDP y TCP ya está habilitado y "Permitir desde" habilita el acceso desde cualquier red. Más adelante, podemos restringir esto solo para las fuentes en las que confiamos para UDP o TCP.

- Activa el puerto 5061 para TLS, habilita Intercept a restrict para el tráfico que solo proviene de la zona de Zoom que has definido anteriormente (en nuestro caso creamos un nombre de red "ZS LATAM" y restringiremos o permitiremos solo desde esas IP's.
- Como nuestro SIParator® se encuentra en una DMZ, la IP pública está NATed y debemos anotar la dirección IP pública como se indica.

En este punto, también queremos monitorear las direcciones IP de proxy SIP de Zoom. En nuestro caso sabemos que LATAM utiliza los que se indican a continuación. SIParator® monitoreará esas IP's mediante el envío periódico de OPCIONES SIP.

Server	Port	Transport	Delete Row
64.211.144.247		TLS	☐
149.137.69.247		TLS	☐
159.124.128.84		TLS	☐
206.247.121.21		TLS	☐

Add new rows 1 rows.

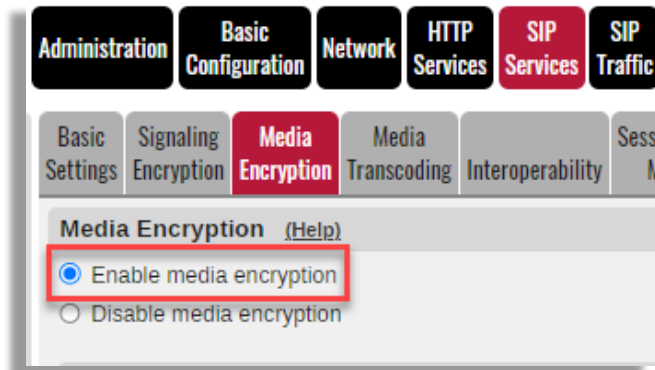
Estamos monitoreando entonces los nodos correspondientes a Latam según se explico inicialmente.

Como Zoom utiliza el puerto 5061, no es necesario indicar explícitamente ningún puerto para supervisar (5061 es el valor predeterminado para TLS). Solo tenemos que seleccionar TLS.

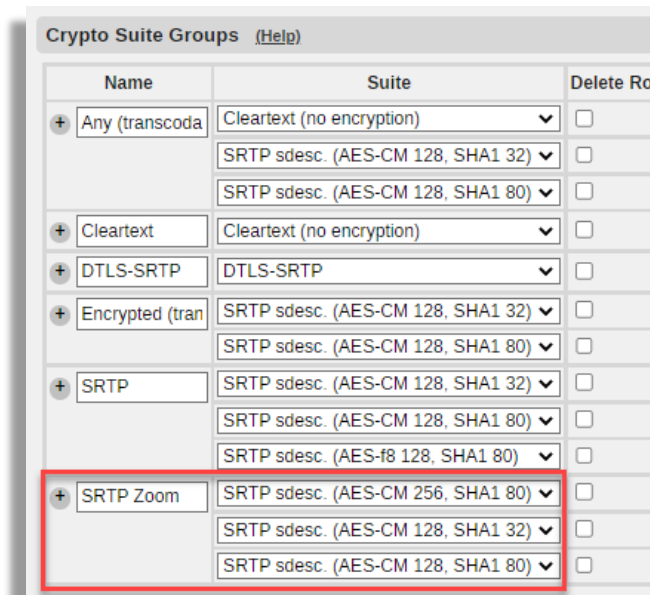
Configurar el cifrado de medios

Zoom requiere, además de TLS como cifrado de señalización, los medios que también se van a cifrar (SRTP)

Para configurar el cifrado de medios, asegúrese de que esté habilitado:

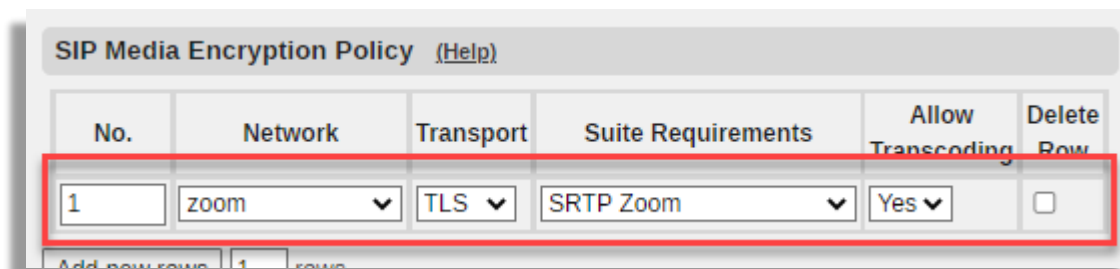


Luego crearemos un grupo de Crypto Suite específicamente para Zoom



- Agregue una fila con 3 subfilas
- Seleccione cada subfila asociada a las suites que se muestran en la imagen

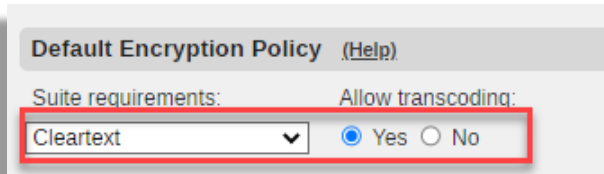
Agregue una política de cifrado de medios:



- Agregar una nueva fila
- Seleccione la red agregada llamada "zoom"
- Seleccione TLS para el protocolo de transporte

- Asocie la suite recientemente creada llamada "SRTP Zoom"
- Habilitar "Permitir transcodificación"

Defina una política de cifrado predeterminada para todo lo demás:



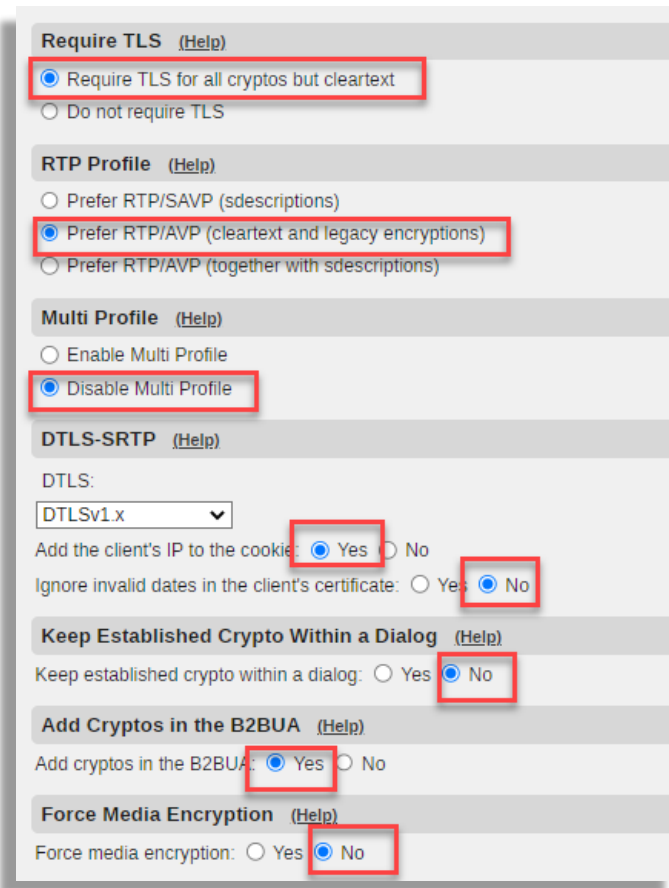
Default Encryption Policy (Help)

Suite requirements: Cleartext ▼

Allow transcoding: ☒ Yes ☐ No

- Seleccione "Texto sin cifrar" como política predeterminada (Texto sin cifrar significa "Sin cifrado")
- Permitir la transcodificación

Establezca los parámetros restantes como se muestra:



Require TLS (Help)

☒ Require TLS for all cryptos but cleartext

☐ Do not require TLS

RTP Profile (Help)

☐ Prefer RTP/SAVP (sdescriptions)

☒ Prefer RTP/AVP (cleartext and legacy encryptions)

☐ Prefer RTP/AVP (together with sdescriptions)

Multi Profile (Help)

☐ Enable Multi Profile

☒ Disable Multi Profile

DTLS-SRTP (Help)

DTLS: DTLSv1.x ▼

Add the client's IP to the cookie: ☒ Yes ☐ No

Ignore invalid dates in the client's certificate: ☐ Yes ☒ No

Keep Established Crypto Within a Dialog (Help)

Keep established crypto within a dialog: ☐ Yes ☒ No

Add Cryptos in the B2BUA (Help)

Add cryptos in the B2BUA: ☒ Yes ☐ No

Force Media Encryption (Help)

Force media encryption: ☐ Yes ☒ No

Definición de DNS Override para manejar trafico distribuido a Zoom con failover o balanceo

En esta sección tomaremos ventaja de una funcionalidad del SBC que permite definir un url y asociar una tabla de distribución muy similar a una tabla de direcciones IP con registros tipo SRV.

Esto nos permite apuntar a todos los proxy de Zoom que queremos usar como posibles destino y nos permite establecer pesos y prioridades para la distribución del tráfico.

Veamos un ejemplo de la tabla que se ubica en la sección SIP Traffic → Routing

AdministrationBasic ConfigurationNetworkHTTP ServicesSIP ServicesSIP TrafficSIP TrunksQ-TURNVirtual Private NetworksQuality of ServiceLogging and ToolsAboutLog out

MethodsFilteringLocal RegistrarAuthenticationAccountsSTIRCall ControlDial PlanRoutingAccountingClassesIDS/IPSTest AgentStatus

DNS Override For SIP Requests (Help)

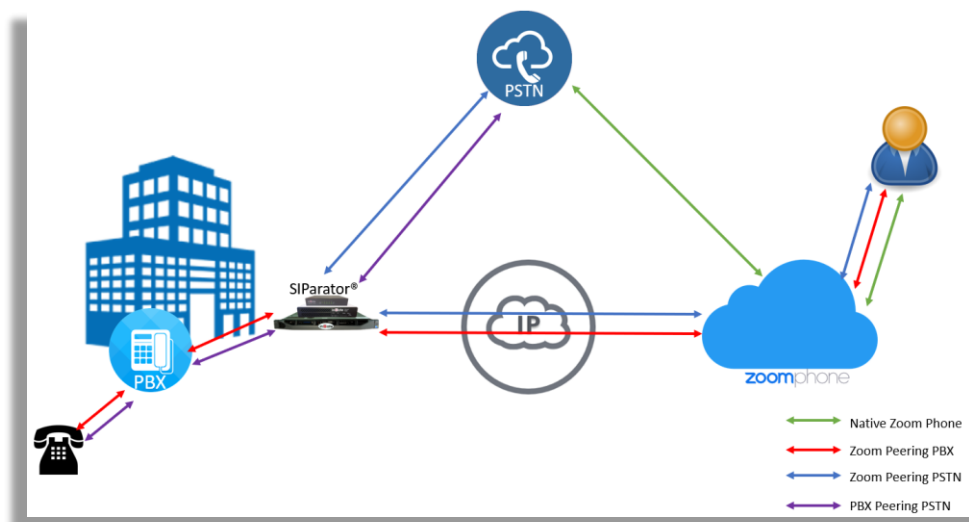
Domain	Relay To								Delete Row
	DNS Name or IP Address	IP Address	Port	Transport	Priority	Weight	Auth	Modify RURI	
+ us.zoom.local	64.211.144.247	64.211.144.247	5061	TLS	1	100	No	No	☐
	149.137.69.247	149.137.69.247	5061	TLS	1	100	No	No	☐
	159.124.128.84	159.124.128.84	5061	TLS	2	100	No	No	☐
	206.247.121.212	206.247.121.212	5061	TLS	2	100	No	No	☐

Acá hemos creado un destino (url) llamado us.zoom.local el cual distribuye con 2 diferentes prioridades (1 y 2) and grupos de proxys a los que se les va a distribuir en round-robin usando los pesos indicados.

Esto deberá ajustarse en su caso particular a la estrategia de distribución de trafico hacia Zoom que mejor se ajuste a su estrategia.

Configurar el enlace troncal SIP

Entendamos cómo se ven los flujos SIP en nuestro caso:



Configuración del grupo troncal Zoom-PSTN

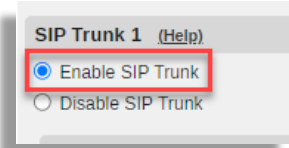
En nuestro caso, estamos utilizando el servicio de enlace troncal SIP de Twilio con fines de demostración.

Primero, debemos agregar un nombre de red para las direcciones IP proporcionadas por Twilio. Se pueden encontrar en el sitio web de Twilio (<https://www.twilio.com/docs/sip-trunking/ip-addresses>). Incluiremos solo las IP de Virginia de América del Norte, ya que el SIParator está alojado en la región de AWS Virginia.

Name	Subgroup	Lower Limit		Upper Limit (for IP ranges)		Interface/VLAN
		DNS Name or IP Address	IP Address	DNS Name or IP Address	IP Address	
Twilio	Twilio Media					-
	Twilio Signaling					-
Twilio Media	-	34.203.250.0	34.203.250.0	34.203.251.255	34.203.251.255	Outside (eth0 untagged)
	-	54.172.60.0	54.172.60.0	54.172.61.255	54.172.61.255	Outside (eth0 untagged)
Twilio Signaling	-	54.172.60.0	54.172.60.0	54.172.60.3	54.172.60.3	Outside (eth0 untagged)

Vamos a configurar el grupo troncal

En primer lugar, habilitaremos un nuevo grupo de troncales habilitando desde las opciones desplegables:



Haga clic en "Ir a la página de troncales SIP" y habilite el grupo de troncales

Estamos utilizando el servicio troncal SIP elástico de Twilio y tenemos como FQDN asignado: zoompeering.pstn.twilio.com

Para no definir el troncal:

- Asignar un nombre al grupo de troncales
- Utilice el FQDN de proxy proporcionado como dominio del proveedor de servicios.
- Como nuestro SIParator® está detrás de un firewall (DMZ), necesitaremos ingresar la IP pública en el nombre de host en Request-URI.

Configure la siguiente opción en el troncal y deje todo lo demás con valores predeterminados:

Ahora configuraremos las reglas de coincidencia para enrutar los DID entrantes designados para los usuarios de Zoom o el operador automático:

Peering local de ZoomPhone (BYOC y BYOP)

The screenshot shows the Zoom Phone configuration interface. The top section is 'Main Trunk Line' with a 'Help' link. It contains a table with columns: No., Reg., Display Name, User Name, Identity, User ID, Password, Incoming Trunk Match, and Forward to. The 'User Name' and 'Identity' fields are highlighted with a red box. Below this is the 'PBX Lines' section with a 'Help' link. It contains a table with columns: No., Reg., From PBX Number/User, Display Name, User Name, Identity, User ID, Password, Incoming Trunk Match, Forward to PBX Account, and Delete Row. The 'Incoming Trunk Match' and 'Forward to PBX Account' fields are highlighted with a red box. At the bottom of the PBX Lines section, there is a button 'Add new rows' and a text '1 rows'.

Si tiene más de un DID, puede seguir agregando filas a la tabla de líneas PBX y hacer coincidir DID adicionales. También puede utilizar expresiones regulares para la coincidencia.

La configuración DID (formato E164) en la línea troncal principal (usuario e identidad) se utilizará para fines de identificación de llamadas en las llamadas salientes. En nuestro caso, estamos utilizando el DID asignado al operador automático en Zoom.

The screenshot shows the 'Assigned' tab in the Zoom Phone configuration interface. It includes a 'Main Company Number' field set to 'Set', buttons for 'Add', 'Import', and 'Export', a search bar, and filters for 'Number Type (All)', 'Assigned to (All)', and 'Status (All)'. Below these are links for 'Assign SMS/MMS' and 'Disable SMS/MMS'. The main table lists assigned numbers with columns: Number, Area, Number Type, Capability, Assigned To, and Number Status. The number (954) 866-8899 is highlighted with a red box, and its assigned user 'Main Auto Receptionist (Auto Receptionist)' is also highlighted with a red box.

Number	Area	Number Type	Capability	Assigned To	Number Status
(954) 852-8529	Fort Lauderdale, Florida, United States	Toll Number	Incoming & Outgoing	Main Auto Receptionist (Auto Receptionist) Ext. 801	Normal
(954) 852-8530	Fort Lauderdale, Florida, United States	Toll Number	Incoming & Outgoing	Ernesto Casas Ext. 800	Normal
(954) 866-8899	United States	Toll Number	Incoming & Outgoing	Main Auto Receptionist (Auto Receptionist) Ext. 801	Normal

Ahora estamos configurando la conexión de este grupo troncal a Zoom.

Si el destino del zoom no es más de dos direcciones IP o FQDN, entonces podemos usar la sección PBX para el troncal asignando ambos al campo de dominio separados por ",".

Setup for the PBX (help)

☐ Use PBX from other SIP trunk

☒ Define PBX settings

PBX Name: (Unique descriptive name)

Use alias IP address: (Forces this source address from our side)

PBX Registration SIP Address	Authentication		PBX IP Address		PBX Domain Name
	User ID	Password	DNS Name or IP Address	IP Address	
					us.zoom.local
Change Password					

(At least one of PBX Registration, IP address or Domain Name is required to locate the PBX)

PBX Network:

Signaling transport: (* = Automatic)

Port number:

Match From Number/User in field:

Common User Name suffix:

To header field:

Forward incoming REFER:

Send DTMF via SIP INFO:

Remote Trunk Group Parameters usage: (* = Don't use TGP)

Local Trunk Group Parameters usage: (* = Don't use TGP)

- Seleccione "Definir la configuración de PBX"
- Asignar un nombre
- En "Nombre de dominio PBX" ingrese el url que creamos para definir la estrategia de distribución de tráfico hacia Zoom (us.zoom.local)

#Latam Old
64.211.144.247
149.137.69.247
#Latam New
159.124.128.84
206.247.121.212

- Seleccione la Red (ZS LATAM), creada previamente en → Redes de Red y Computadoras
- Seleccione Señalización TLS.
- Deje los campos restantes con valores predeterminados.

Configuración del grupo troncal PBX-PSTN

En esta sección asumimos que el ITSP también proporcionará servicio para Trunking con DID's asociados al PBX; de esta manera, puede utilizar un único SIParator® para administrar el tráfico PSTN para los usuarios de Zoom, así como su PBX existente.

Necesitaremos agregar una nueva página de grupo troncal

View trunk: SIP Trunk 1: Twilio Trunk; Zoom Peer
 SIP Trunk 1: Twilio Trunk; Zoom Peer
SIP Trunk 2
 SIP Trunk 3

☐ Enable SIP Trunk
☒ Disable SIP Trunk

Save Undo Look up all IP addresses again

Habilite Tunk Group y seleccione "Usar parámetros de otro troncal SIP". De esta forma utilizaremos el mismo Trunk que ya configuramos en el apartado anterior.

SIP Trunk 2 (Help)
☒ Enable SIP Trunk
☐ Disable SIP Trunk

SIP Trunking Service (Help)
☒ Use parameters from other SIP trunk
☐ Define SIP trunk parameters
 SIP Trunk Parameters: Twilio Trunk

Main Trunk Line (Help)						
Outgoing Calls					Authentication	Incoming Calls
No.	Reg	Display Name	User Name	Identity	User ID	Forward to
1	No		+19548667575	+19548667575	Change Password	

PBX Lines (Help)						
Outgoing Calls					Authentication	Incoming Calls
No.	Reg	From PBX Number/User	Display Name	User Name	Identity	Forward to
2	No					

Add new rows 1 rows.

- Habilitar el troncal
- Utilice parámetros de otro troncal SIP y elija Troncal de Twilio (configurado en la sección anterior)
- Wi utilizará un DID diferente y lo agregará al nombre de usuario e identidad salientes para fines de identificación de llamadas.
- Para la llamada entrante coincidirá con el DID asignado a PBX Trunking. Si tienes mora tan un DID puedes seguir añadiendo filas en las líneas de la centralita.

Ahora configuraremos la conectividad PBX

Setup for the PBX (Help)

☐ Use PBX from other SIP trunk

☒ Define PBX settings

PBX Name: (Unique descriptive name)

Use alias IP address: (Forces this source address from our side)

PBX Registration SIP Address	Authentication		PBX IP Address		PBX Domain Name
	User ID	Password	DNS Name or IP Address	IP Address	
		Change Password		10.1.1.172	

(At least one of PBX Registration, IP address or Domain Name is required to locate the PBX)

PBX Network:

Signaling transport: ('-' = Automatic)

Port number:

Match From Number/User in field:

Common User Name suffix:

To header field:

Forward incoming REFER:

Send DTMF via SIP INFO:

Remote Trunk Group Parameters usage: ('-' = Don't use TGP)

Local Trunk Group Parameters usage: ('-' = Don't use TGP)

- Seleccione "Definir la configuración de PBX"
- Asignar un nombre a la centralita
- En Dominio PBX introduzca la dirección IP de su PBX (En nuestro caso 10.1.1.172)
- Seleccione el nombre de red agregado anteriormente a → Redes de red y equipos. Si aún no lo ha hecho, vea el siguiente ejemplo:

Administration **Basic Configuration** **Network** **HTTP Services** **SIP Services** **SIP Traffic** **SIP Trunks** **Q-TURN** **Virtual Private Networks** **Quality of Service** **Logging and Tools** **About** **Log out**

Networks and Computers **Default Gateways** **All Interfaces** **VLAN** **Eth0** **Eth1** **Interface Status** **PPPoE** **Tunnels** **Topology**

Networks and Computers

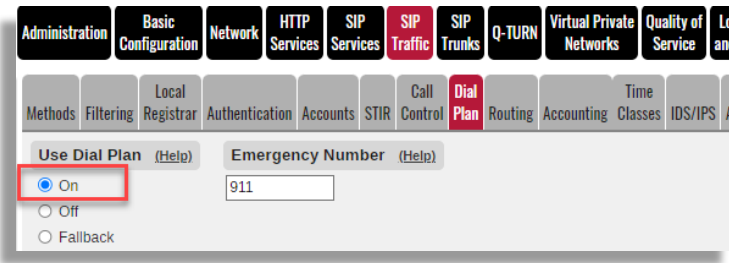
Name	Subgroup	Lower Limit		Upper Limit (for IP ranges)		Interface/VLAN	Delete Row
		DNS Name or IP Address	IP Address	DNS Name or IP Address	IP Address		
PBX Educronix	-	10.1.1.172	10.1.1.172			Inside (eth1 untagged)	☐

- Deje los campos restantes con los valores predeterminados.

Configurar el plan de marcado

Con el plan de marcado, podremos enrutar el tráfico saliente, el tráfico entre Zoom y PBX y también habilitar el SIParator® para responder a las solicitudes de opciones de Zoom.

En primer lugar, tendrás que activar el plan de marcado.



Habilitación de opciones SIP para solicitudes de Zoom

Necesitaremos detectar las solicitudes de OPTIONS que aterrizan en la interfaz externa. Las opciones de SP envían solicitudes a la IP pública externa de forma similar a esta:

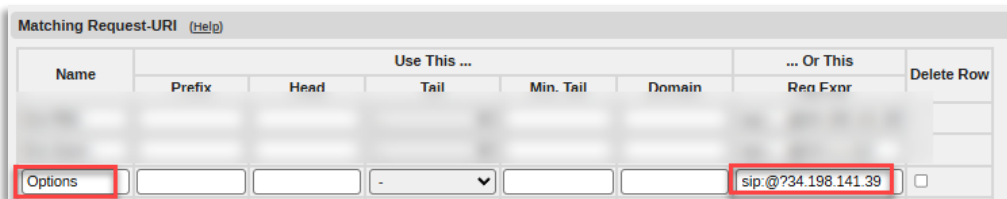
```

recv from 149.137.69.247:30973 via 10.1.0.145:5061 TLS connection 7:
OPTIONS sip:3.217.32.189:5061 SIP/2.0
Via: SIP/2.0/TLS 149.137.69.247:5061;branch=z9hG4bK00Bf1ff6d0bf4a6cc6c
From: <sip:149.137.69.247>;tag=gK0015c377
To: <sip:3.217.32.189>
Call-ID: 101654428_1298819240@149.137.69.247
CSeq: 343588 OPTIONS
Max-Forwards: 1
Allow: INVITE,ACK,CANCEL,BYE,REGISTER,REFER,INFO,SUBSCRIBE,NOTIFY,UPDATE,OPTIONS,MESSAGE,PUBLISH
Accept: application/sdp, application/isup, application/dtmf, application/dtmf-relay, multipart/mixed
Contact: <sip:149.137.69.247:5061>
Content-Length: 0
    
```

Usaremos una expresión regular para hacer coincidir el r-uri con una dirección IP, como esta:

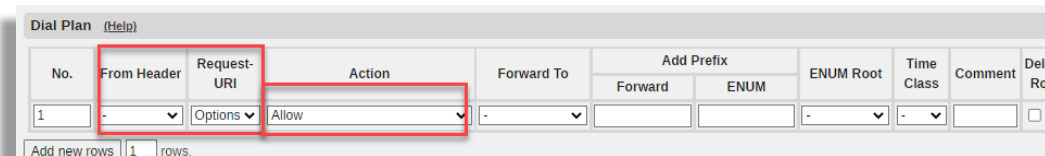
sip:@?34.195.141.39

En Dial Plan, hagamos coincidir el URI de solicitud con la expresión:



- Asignar un nombre a la regla
- Introduzca la expresión regular.

En Plan → de marcado, agregue la regla a "permitir" Opciones.



Ingresaremos reglas de identificación de tráfico proveniente de la PBX o de Zoom usando la sección de matching From Header.

Name	Use This ...		... Or This	Transport	Network	Delete Row
	Username	Domain	Reg Expr			
From LAN	*	*		UDP	LAN	☐
Zoom Latam	*	*		TLS	Zoom Latam	☐

La regla From LAN identifica todo tráfico proveniente de la red Interna y eso incluye la PBX y Zoom Latam identifica tráfico proveniente de Zoom. EN ambos casos se usa la red de origen para hacer el match.

A continuación, utilizaremos el Plan de Marcación para 3 propósitos principales:

- Enrutar el tráfico saliente a PSTN desde Zoom
- Enrutar el tráfico saliente a PSTN desde PBX
- Enrutar llamadas dentro de la red entre usuarios de Zoom y usuarios de PBX en ambos sentidos

Ruta de salida de Zoom a PSTN

Para detectar/hacer coincidir el tráfico proveniente de Zoom, agregaremos una regla en la sección de encabezado match From

Name	Use This ...		... Or This	Transport	Network	Delete Row
	Username	Domain	Reg Expr			
Zoom Latam	*	*		TLS	Zoom Latam	☐

- Agregar una fila en el encabezado Coincidencia desde
- Asignar un nombre a la regla
- Utilice el comodín "*" para el nombre de usuario y el dominio.
- Seleccione el protocolo de transporte que se va a detectar (TLS)
- Seleccione la red de la que provendrá el tráfico (fuentes de señalización de Zoom)

Agregue una regla de URI de solicitud para que coincida con el tráfico recibido para avanzar más adelante a PSTN. Acá debemos tomar en cuenta que llamadas hacia la PSTN pueden llegar tanto desde Zoom como desde la PBX por lo tanto usaremos una expresión regular que valide que el destino es de en formato E.164 de 10 dígitos y que llega ya sea por la interface interna como por la IP Publica:

sip:(\+1.....)@(10.1.1.112/34.195.141.39)

Name	Use This ...					... Or This	Delete Row
	Prefix	Head	Tail	Min. Tail	Domain	Reg Expr	
PSTN			-			sip:(\+1.....)@(10.1.1.112/34.195.141.39)	☐

- Agregue una nueva fila en "Matching Request-URI"
- Asignar un nombre a la nueva regla
- Haga coincidir las solicitudes SIP con [***sip:\(\+1.....\)@\(10.1.1.112/34.195.141.39\)***](#)
- Ahora definiremos el destino al troncal PSTN (reenviar a) utilizando el grupo de troncales Zoon-PSTN

Name	No.	Use This ...	... Or This			... Or This	... Or This	Use Alias IP	Delete Row
		Account	Replacement Domain	Port	Transport	Reg Expr	Trunk		
PSTN Zoom		-			-		SIP Trunk 2: Twilio Zoom peer	☐	☐

- Agregar una nueva fila en la tabla "Reenviar a"
- Asignar un nombre a la regla
- Selecciona Trunk 2 como destino (el que creamos con el ISTP para Zoom DID)

A continuación, definamos la regla del plan de marcado real para enviar tráfico saliente a PSTN procedente de Zoom.

No.	From Header	Request-URI	Action	Forward To	Add Prefix		ENUM Root	Time Class	Comment	Delete Row
					Forward	ENUM				
5	Zoom Latam	PSTN	Forward	PSTN Zoom				-		☐

- Cree una regla en la que Si **el encabezado From** coincide con "Zoom Latam" y **el URI de solicitud** coincide con "PSTN", hace un **Forward** a "PSTN Zoom"

Ruta de salida de PBX a PSTN

Ahora estamos listos para agregar reglas de plan de marcado para enrutar la salida a RTC procedente de PBX.

Agregue una regla "Reenviar a" que apunte al troncal que creamos para la conectividad PBX – PSTN.

Name	No.	Use This ...	... Or This	... Or This	... Or This	Trunk	Use Alias IP	Delete Row
PSTN PBX	1	-				SIP Trunk 1: Twilio,PBX	-	☐
						P Trunk 2: Twilio,Zoom peer	-	☐

- Agregue una nueva fila en la tabla "Reenviar a".
- Asignar un nombre a la nueva regla
- Seleccione Trunk 1 (el que creamos anteriormente para la conectividad PSTN para el PBX)

Agregue la regla de enrutamiento del plan de marcado real:

No.	From Header	Request-URI	Action	Forward To	Add Prefix	ENUM Root	Time Class	Comment
1	-	Options	Allow	-		-	-	
4	From LAN	PSTN	Forward	PSTN PBX		-	-	
5	Zoom Latam	PSTN	Forward	PSTN Zoom		-	-	

- Agregar una nueva fila a "Plan de marcado"
- Haga coincidir **el encabezado From** con la regla "From PBX" y **el URI de solicitud** con "To PSTN" y "Forward" a la ruta creada anteriormente denominada "To ITSP PBX"

El siguiente paso será agregar las reglas de enrutamiento necesarias para mover el tráfico

Usuarios/Extensiones de Zoom ↔ Usuarios/Extensiones de PBX

Ruta PBX ↔ Zoom

Aquí detectaremos las llamadas a las extensiones de Zoom haciendo coincidir con un número de 4 dígitos que llega a SIParator® desde la PBX, o haciendo coincidir con un número de 4 dígitos que llega a SIParator® desde Zoom.

Matching Request-URI (Help)

Name	Use This ...					... Or This	Delete Row
	Prefix	Head	Tail	Min. Tail	Domain	Reg Expr	
Ext PBX			-			sip:(...)@34.195.141.39	☐
Ext Zoom			-			sip:(...)@10.1.1.112	☐

- Agregue una nueva fila para hacer coincidir la marcación con una extensión PBX. Esta llamada llegará a la interfaz externa a la dirección IP pública del SIParator®.
- Asigne un nombre a la nueva fila.
- Introduzca la cadena coincidente " sip:(...)@34.195.141.39"
- Agregue una nueva fila para hacer coincidir la marcación con una extensión de Zoom. Esta llamada llegará a la interfaz interna a la dirección IP privada del SIParator®.
- Asigne un nombre a la nueva fila.
- Introduzca la cadena coincidente " sip:(...)@10.1.1.112"

Agregue los destinos "Forward To" para la llamada enrutada directamente a la PBX o a Zoom.

Forward To (Help)

Name	No.	Use This ... Account	... Or This			Reg Expr	Trunk	Use Alias IP	Delete Row
			Replacement Domain	Port	Transport				
+ PBX	1	-			-	sip:\$1@10.1.1.	-	-	☐
+ PSTN PBX	1	-			-		SIP Trunk 1: Twilio;PBX	-	☐
+ PSTN Zoom	1	-			-		SIP Trunk 2: Twilio;Zoom peer	-	☐
+ zoom	1	-			-	sip:\$1@us.zoo	-	-	☐

- Agregue una nueva fila para definir una ruta para llegar a la PBX
- Asignar un nombre a la nueva fila
- Utilice RegExp para definir el destino: "sip:\$1@10.1.1.172;transport=udp;b2buawm"
- Asegure que añadió "; transporte=udp; b2buawm" al final de la expresión.
- Agregue una nueva fila en la que usaremos el url que creamos con DNS Override, para distribuir el trafico hacia extensiones de Zoom con la misma estrategia que definimos para tráfico desde la PSTN. Usemos: "sip:\$1@us.zoom.local;b2buawm"

Definamos ahora las reglas en el plan de marcación real

Dial Plan (Help)

No.	From Header	Request-URI	Action	Forward To	Add Prefix		ENUM Root	Time Class	Comment	Delete Row
					Forward	ENUM				
1	-	Options	Allow	-			-	-		☐
2	From LAN	Ext Zoom	Forward	zoom			-	-		☐
3	Zoom Latam	Ext PBX	Forward	PBX			-	-		☐
4	From LAN	PSTN	Forward	PSTN PBX			-	-		☐
5	Zoom Latam	PSTN	Forward	PSTN Zoom			-	-		☐

- Agregue 2 nuevas filas, una para enrutar llamadas de Zoom a PBX y la segunda para enrutar llamadas de PBX a Zoom.
- Al hacer coincidir **From Header** con "Zoom Latam" y **Request-URI** con "Ext PBX", reenvíe la llamada a "PBX"
- Al hacer coincidir **From Header** con "From LAN" y **Request-URI** con "Ext Zoom", reenvíe la llamada a "zoom"
- Asegúrese de que las reglas para extensión la extensión tengan un valor n el orden de numeración inferior al de la regla correspondiente para PSTN (como se muestra en la imagen anterior)

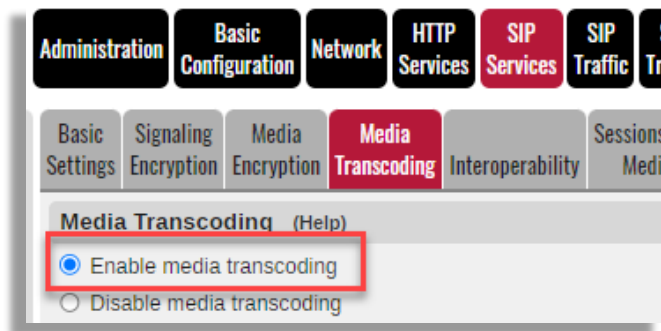
Configuración de la transcodificación

Las conexiones de peering local, tanto a través de Internet como de las opciones de circuito privado, preferirán los siguientes códecs en el orden de preferencia que se indica a continuación:

- OPUS
- G.722
- G.711A-ley/ μ -ley
- G.729

SIParator® tiene transcodificación basada en software incorporada sin necesidad de licencia adicional.

Tendrás que habilitar la transcodificación:



Primero crearemos los grupos de códecs necesarios:

Codecs [\(Help\)](#)

Name	No.	Codec	Parameters	Delete Row
+ Anyother	1	-	-	☐
+ Zoom	1	OPUS	-	☐
	2	G722	-	☐
	3	PCMU	-	☐
	4	PCMA	-	☐
	5	G729A	-	☐
	6	G729B	-	☐
	7	-	-	☐

Add new rows groups with rows per group.

- Agregue 1 fila y 1 fila adicional con 7 subfilas.
- La primera fila, denominada Cualquier otro en nuestro ejemplo, no tendrá ninguna selección en la columna Códec. Esto significa que cualquier códec es compatible con el grupo.
- La segunda fila, denominada Zoom, tiene una subfila por cada códec compatible con Zoom, como se mencionó anteriormente

Asociemos qué códecs están asociados a qué red de señalización:

Rules [\(Help\)](#)

No.	Destination	Transport	Codecs	Options	Delete Row
1	Zoom Latam	TLS	Zoom	-	☐
2	Twilio	-	Anyother	-	☐
3	PBX	-	Anyother	-	☐

Add new rows rows.

- En el caso de la red de señalización de Zoom, cuando utilice el transporte TLS, asocie el grupo de códecs de Zoom.
- Para Twilio (ISTP), para cualquier transporte, asocie el grupo de códecs "Cualquierotro".
- Lo mismo para "PBX Educronix".

Asegúrese de que el proxy multimedia esté habilitado:

The screenshot displays the SIPParator configuration web interface. At the top, there is a row of navigation tabs: Administration, Basic Configuration, Network, HTTP Services, SIP Services (highlighted in red), SIP Traffic, SIP Trunks, Q-TURN, Virtual Private Networks, and Quality of Service. Below this is a second row of sub-tabs: Basic Settings, Signaling Encryption, Media Encryption, Media Transcoding, Interoperability, Sessions and Media (highlighted in red), Remote SIP Connectivity, and VoIP Survival. The main content area is titled 'Session Configuration' and contains the following settings:

- Session timer:** A text input field containing '14400' followed by 'seconds'.
- Allowed amount of concurrent sessions (leave blank for no limit):** A text input field that is currently empty, with '(max 15)' indicated to its right.
- Timeout for SIP over TCP/TLS:** A text input field containing '90' followed by 'seconds'.

Below the session configuration is a section titled 'Media Proxy (Help)'. It contains two radio buttons: 'Enable Media Proxy' (which is selected and highlighted with a red rectangle) and 'Disable Media Proxy'. At the bottom of this section, there is a label 'Always use the Media Proxy:' followed by two radio buttons: 'Yes' and 'No' (which is selected).

Recomendaciones finales y otros puntos de interés

Documentación útil

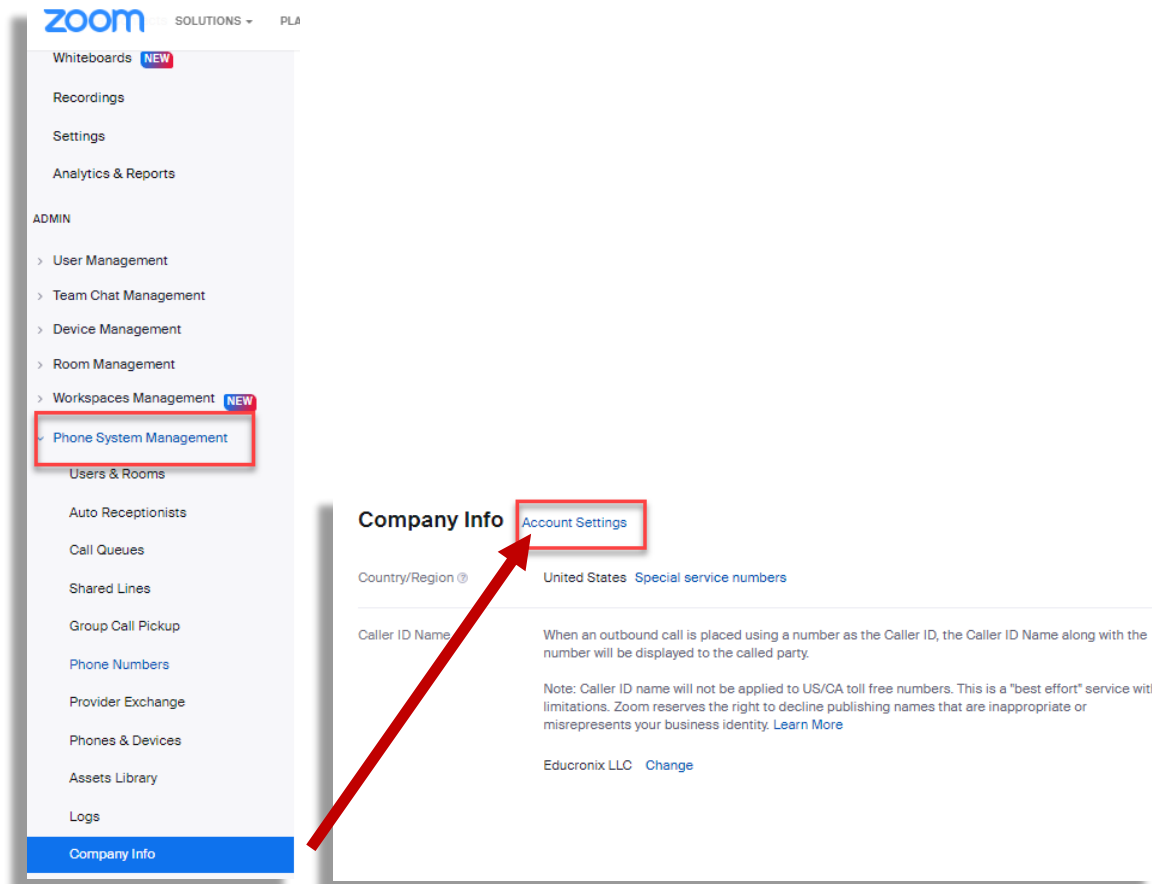
- [SIParator® reference Guide v 7.0.2](#)
- [Cómo usar la manipulación de encabezados genéricos](#)
- [Orientación e instalación – Ingate Software SIParator® Firewall/SIParator](#)

Configuración y requisitos del teléfono Zoom

El requisito más importante es tener su cuenta de Zoom habilitada para el teléfono Zoom con las funciones BYOC y BYOP habilitadas. Esto se puede hacer poniéndose en contacto con su representante de ventas de Zoom y averigüe los requisitos comerciales para tenerlos habilitados.

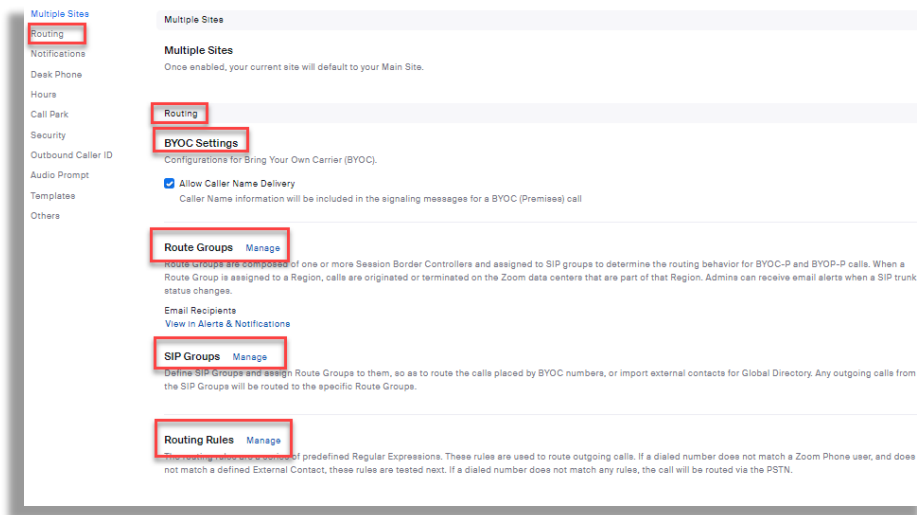
Una vez que lo tenga habilitado, notará el siguiente hecho en el panel de control de su cuenta de Zoom.

En primer lugar, verás una sección de Administración del sistema telefónico:



Seleccione Información de la empresa y, a continuación, **Configuración de la cuenta**

Hay 4 secciones importantes a las que debes prestar atención:



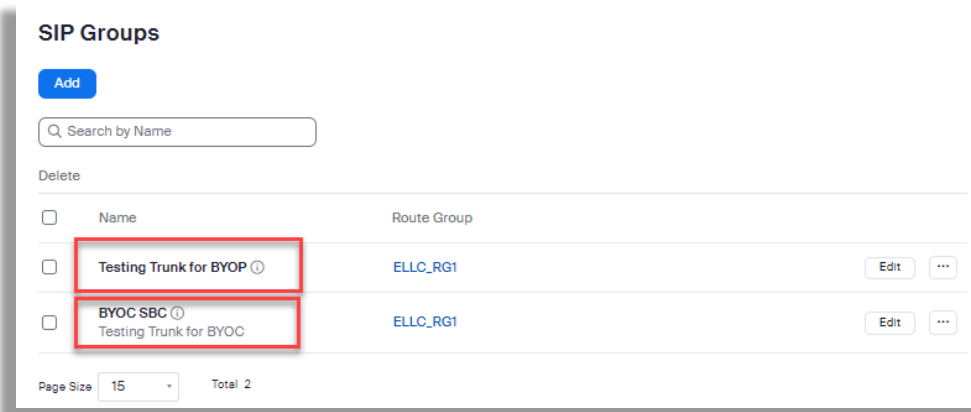
Grupos de rutas (Administrar)

Podrás ver el estado de la conexión de ambos servicios (BYOC y BYOP)

Route Group				
Last Updated Time: 07:23 PM, Nov 01, 2022				
Search by Name Type (				
Display Name	Session Border Controllers	Type	Backup Route Group	Provision Status
ELLC_RG1				
Region	Sequential:			
South America (São Paulo)	3.217.32.189:5061	BYOP-P	--	--
Mexico and Central America (Queretaro, MX)	3.217.32.189:5061			
ELLC_RG1				
Region	Sequential:			
South America (São Paulo)	3.217.32.189:5061	BYOC-P	--	--
Mexico and Central America (Queretaro, MX)	3.217.32.189:5061			

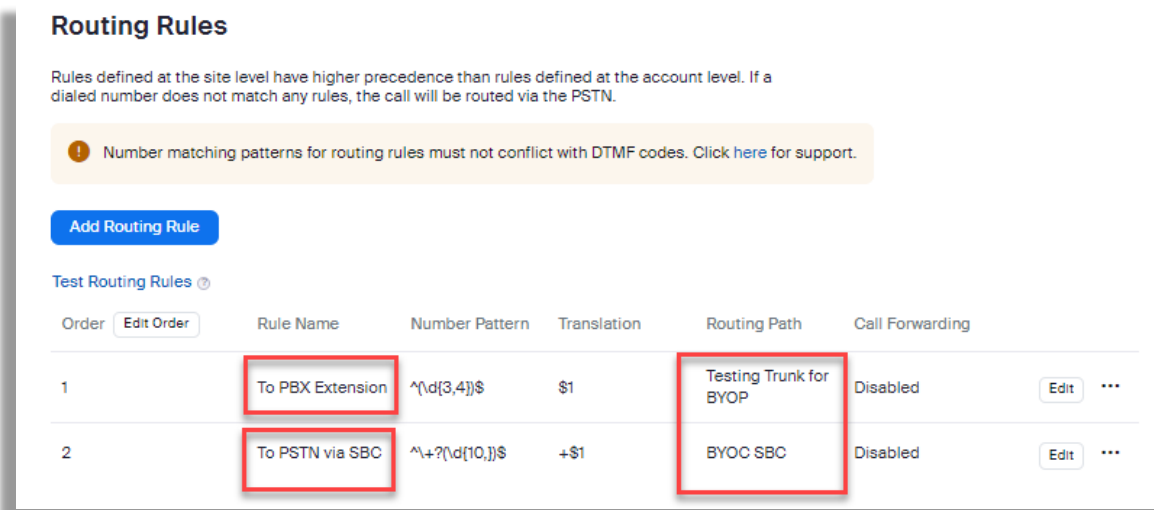
Grupos SIP (Administrar)

Deberá tener al menos un grupo SIP para BYOC y uno para BYOP como este:



Reglas de enrutamiento (Administrar)

Aquí debería haber definido las reglas de enrutamiento para llamar a extensiones PBX (BYOP) o marcar a PSTN a través de su SBC (BYOC).



Declaraciones

SIParator® e Ingate® son marcas comerciales de Ingate System AB

Zoom® y Zoom Phone® son marcas comerciales de Zoom Video Communications, Inc.

Esta documentación es propiedad intelectual de Educronix LLC y está protegida por derechos de autor

Ayuda y soporte

En caso de necesitar información adicional, asesoramiento o cualquier tipo de apoyo respecto al contenido de este documento, póngase en contacto con:

Educronix LLC
1331 St Tropez Cir #601
Weston, FL 33326
+1 954 866 8884
support@educronix.com