Application Note

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

Peering local de ZoomPhone (BYOC y BYOP)

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.

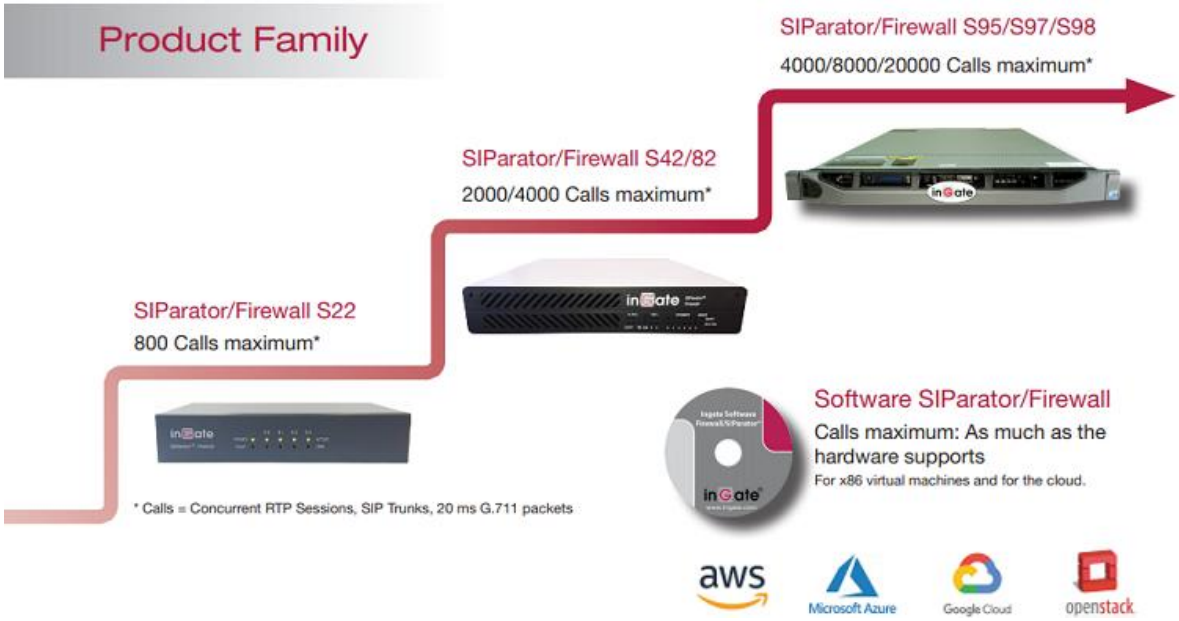
Acerca de la familia de productos SIParator® SBC de Ingate.

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.

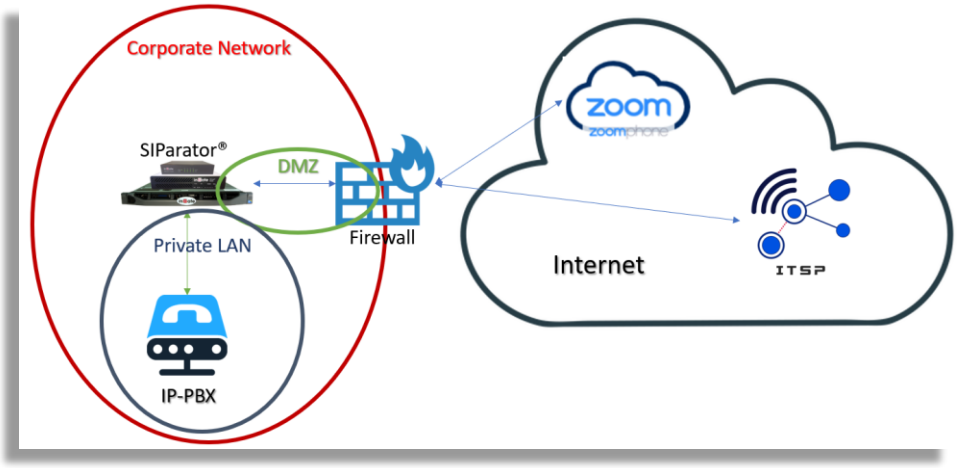


Figura 1: Diseño de implementación

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.

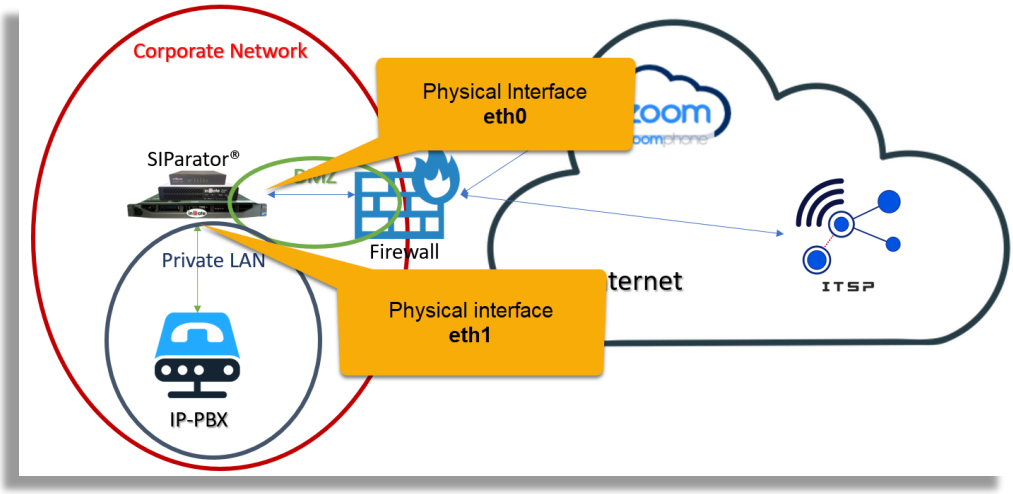
Configuración de interfaces de red IP

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.

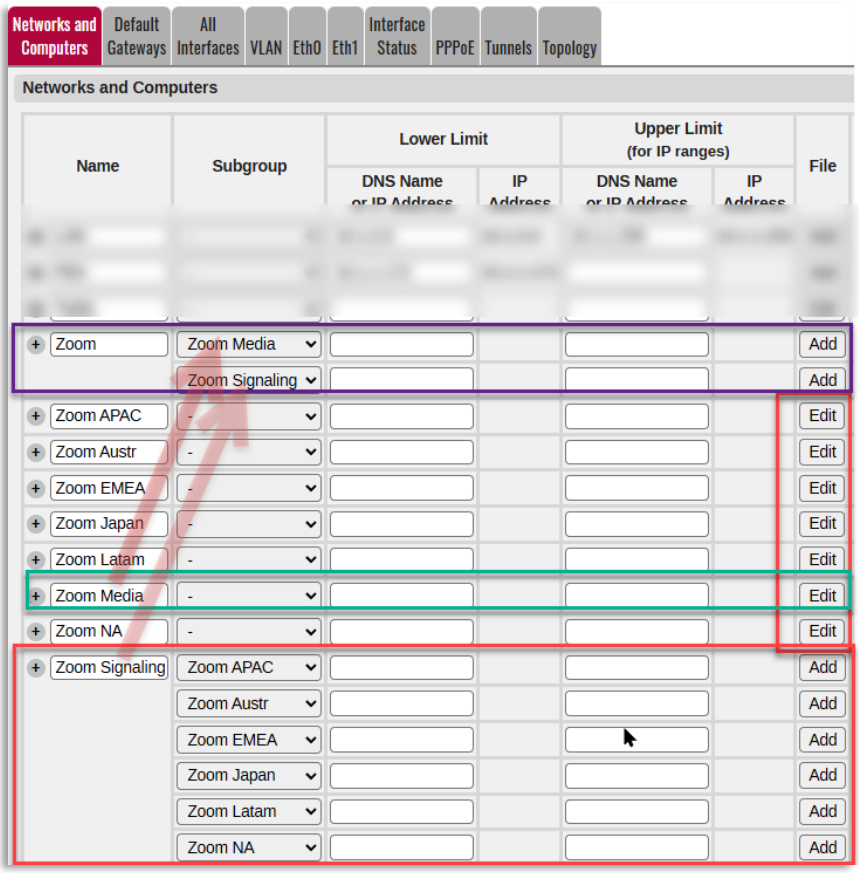
Para la señalización y Media se pueden obtener los detalles de las IPs en este link: [BYOC-P or BYOP-P migration to the Common Platform]

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 hace 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:



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:

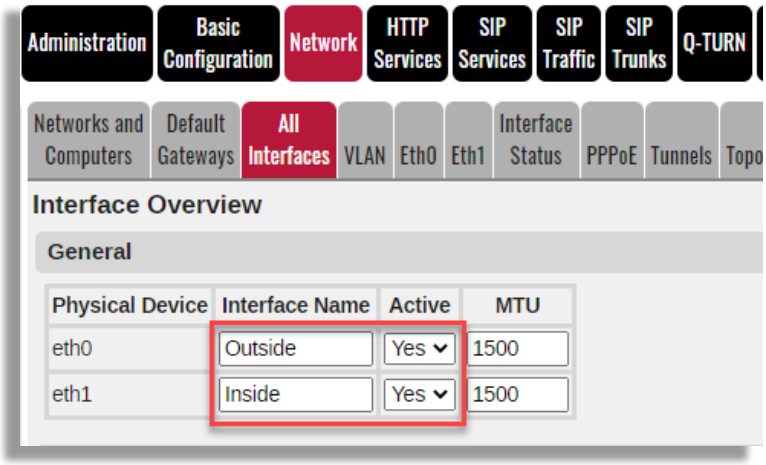
- APAC:
  #APAC Old
  149.137.41.246
  207.226.132.198
  #APAC New
  170.114.156.212
  170.114.185.212
- Australia:
  #Australia Old
  103.122.166.248
  103.122.167.248
  #Australia New
  159.124.96.84
  159.124.64.84
- EMEA:
  #EMEA Old
  213.19.144.198
  213.244.140.198
  #EMEA New
  159.124.0.84
  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

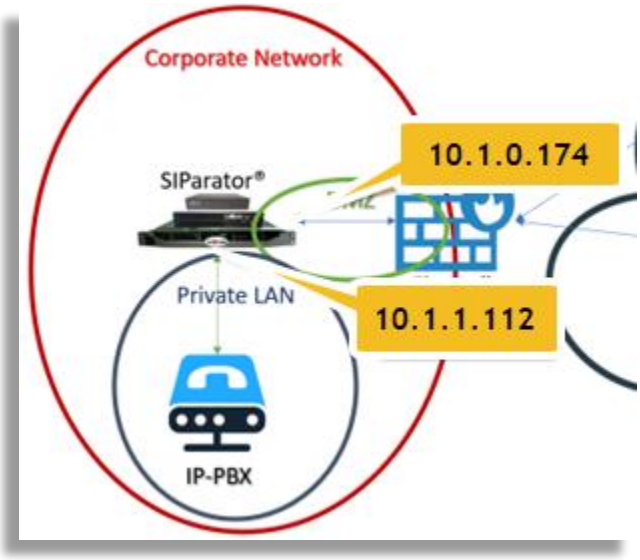
Por simplicidad para la Media hemos consolidado todas las IP de Media en un solo nombre (Resaltado en verde en la imagen arriba):

- 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)

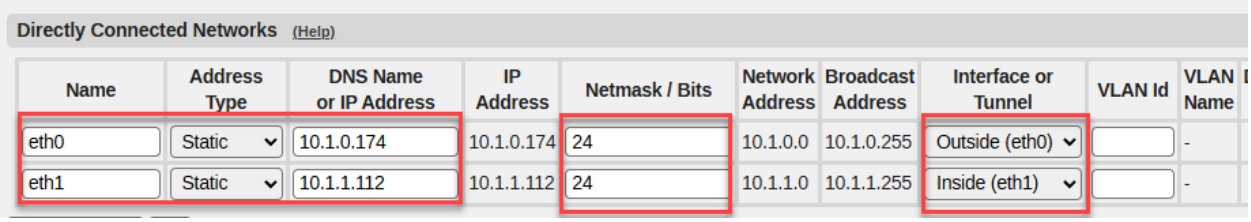


Mirando nuestra topología:

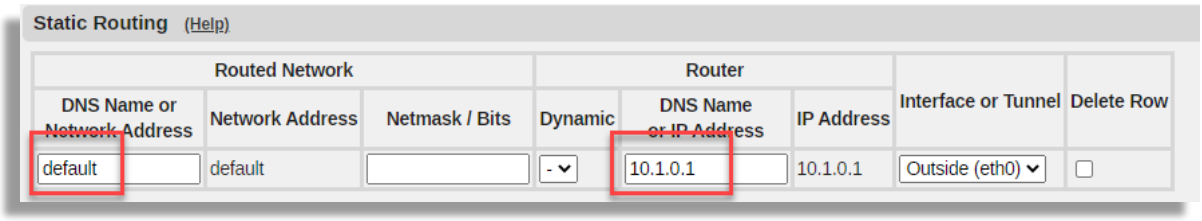


En nuestro caso,

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

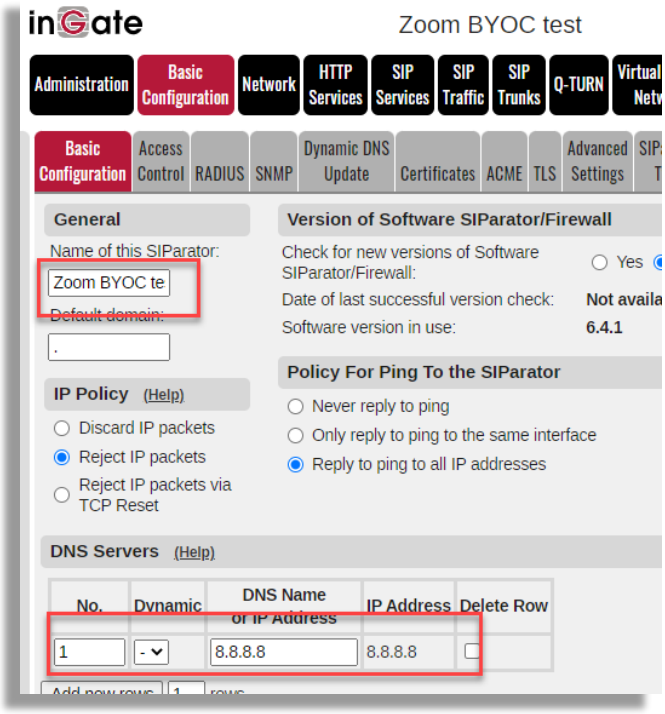


Ruta estática para la puerta de enlace predeterminada:



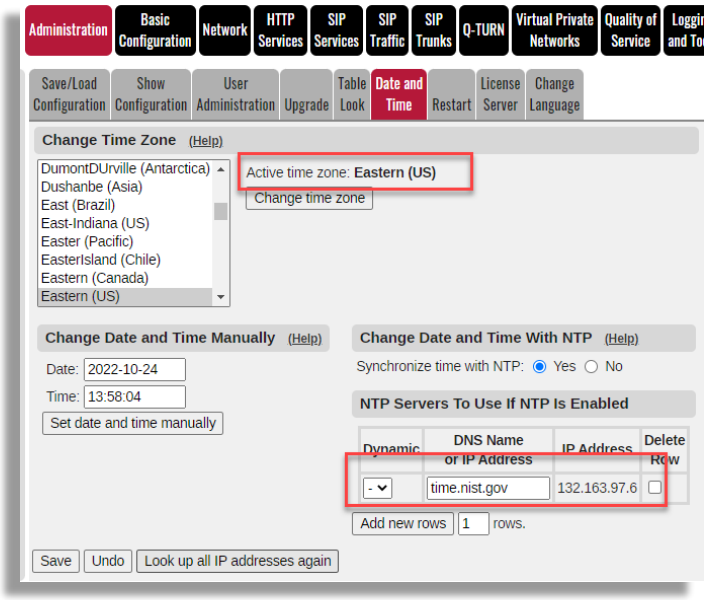
Otras configuraciones relacionadas con la red

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



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.

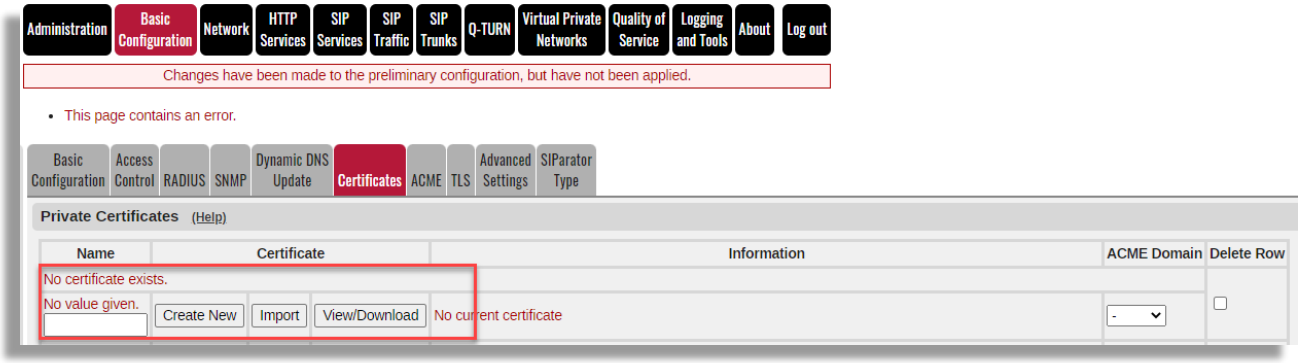
Para habilitar TLS, necesitaremos los certificados públicos adecuados. Con SIParator hay dos formas de adquirir, instalar y mantener certificados TLS.

- **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

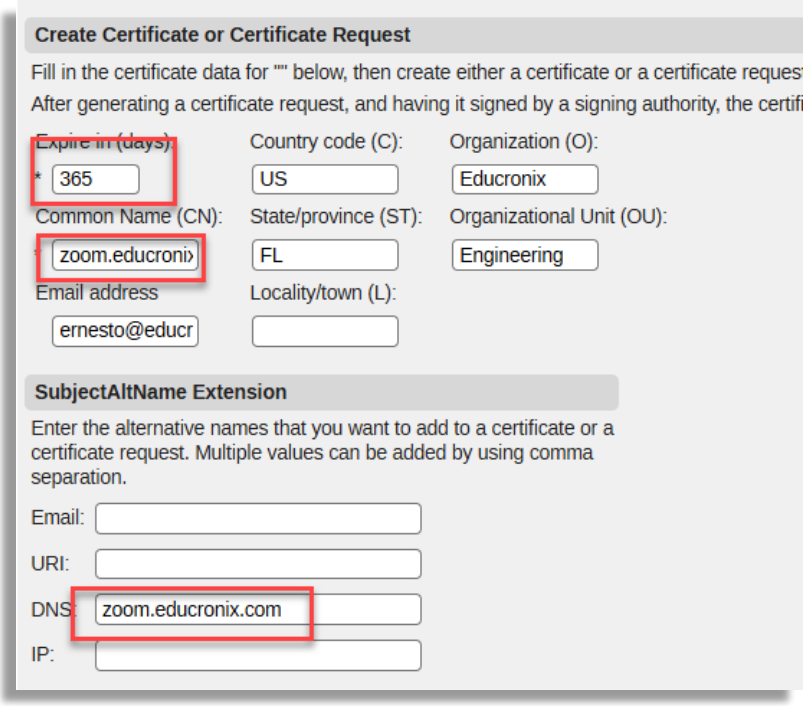
En primer lugar, tendremos que crear una CSR (Solicitud de Firma de Certificado).

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



Asigne un nombre y haga clic en "Crear nuevo"

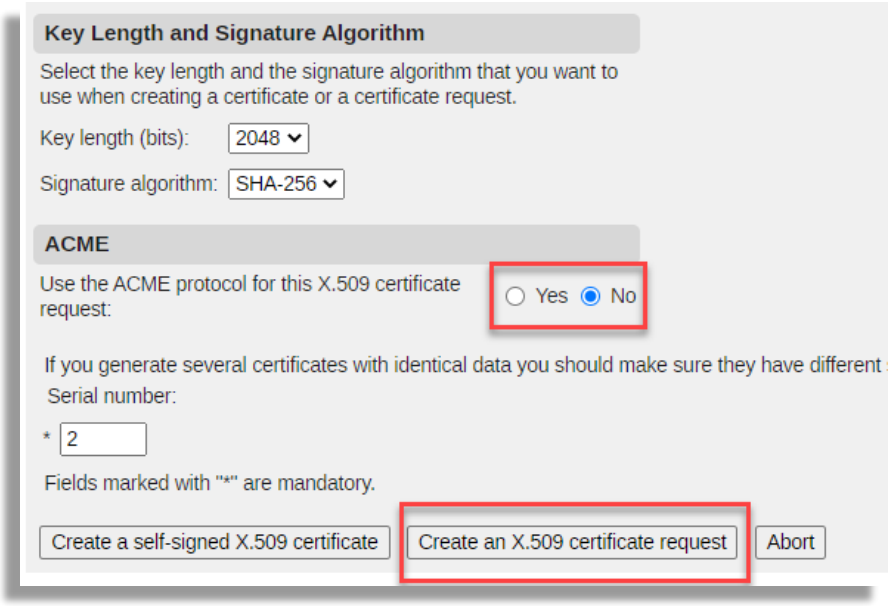
Rellene la información solicitada y asegúrese de que el DNS de la extensión Common Name y SubjectAltName apunte al FQDN de SIParator que se resuelve en la dirección IP pública asociada a la interfaz externa:



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

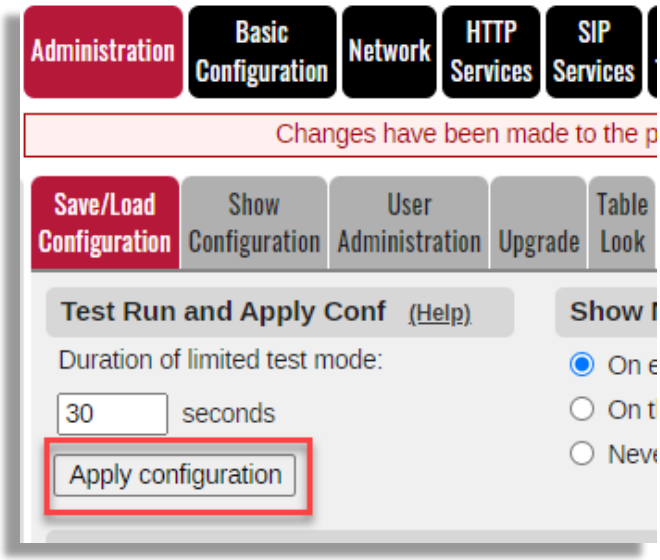
Todos los campos restantes se pueden dejar en los valores predeterminados.

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

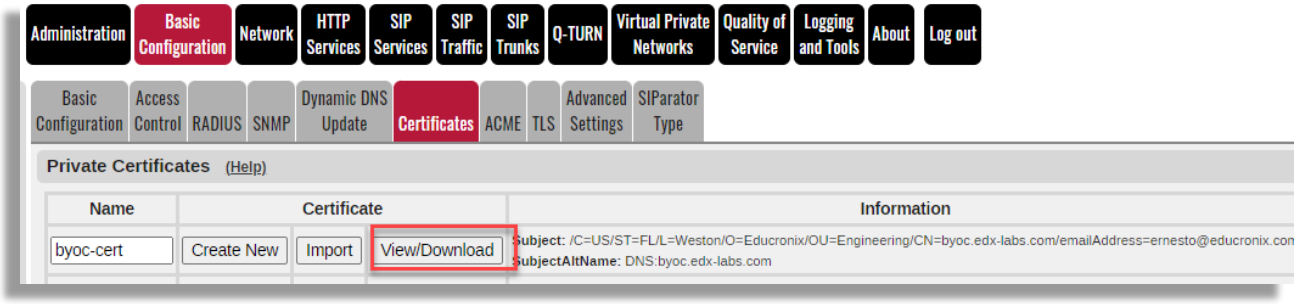


La solicitud de certificado se mostrará de la siguiente manera:

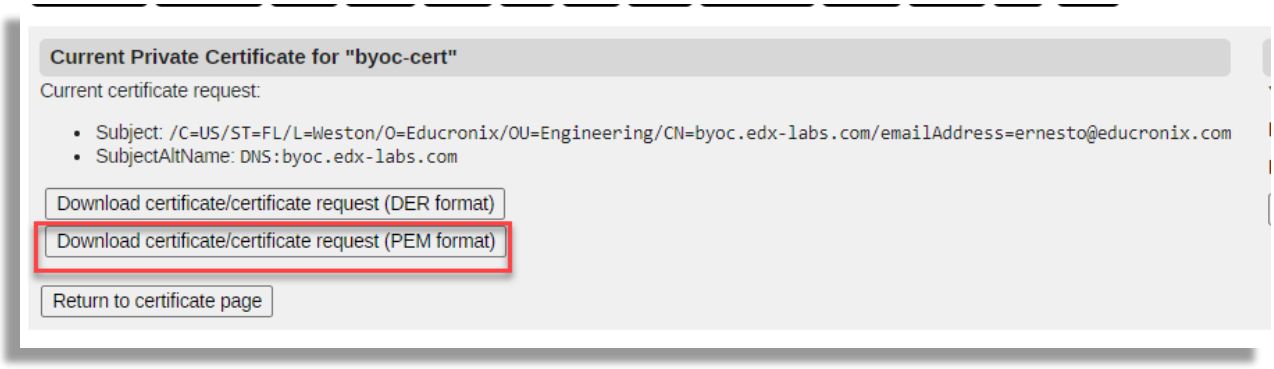
Aplicar cambios



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



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.



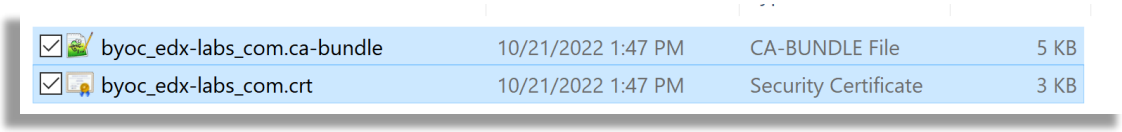
El archivo descargado debería verse así:

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

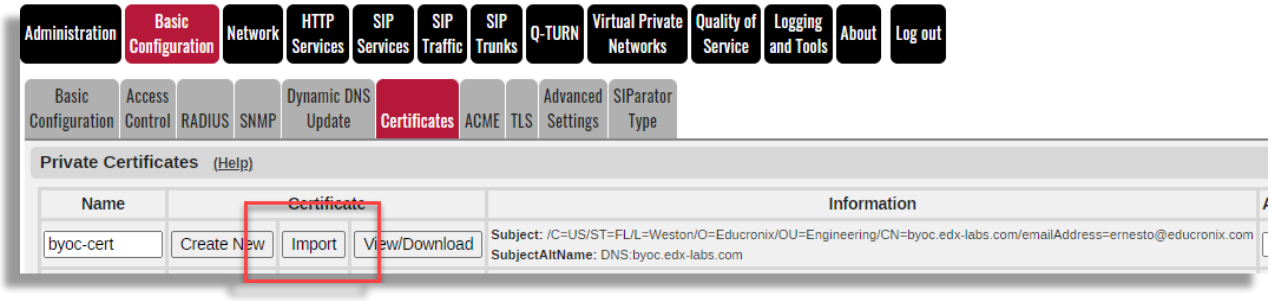
Una vez firmado te proporcionarán un conjunto de archivos, normalmente 2:

- Certificado firmado
- Certificados de paquete de intermediarios.

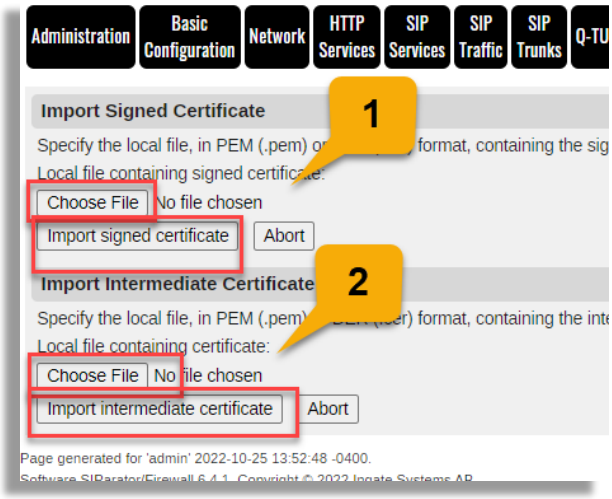
Similar a esto:



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

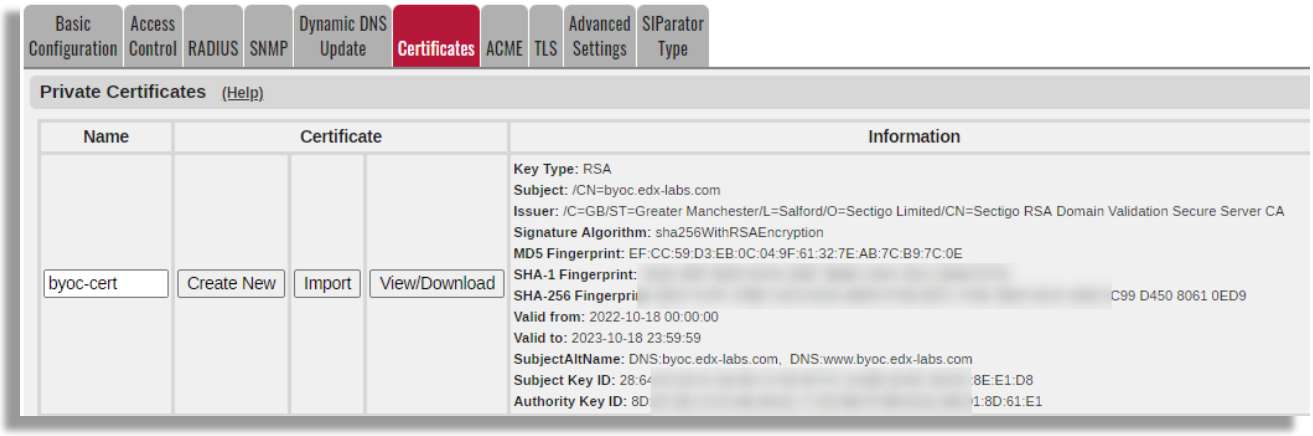


Primero importe el certificado, guárdelo y aplíquelo y, a continuación, cargue el paquete.



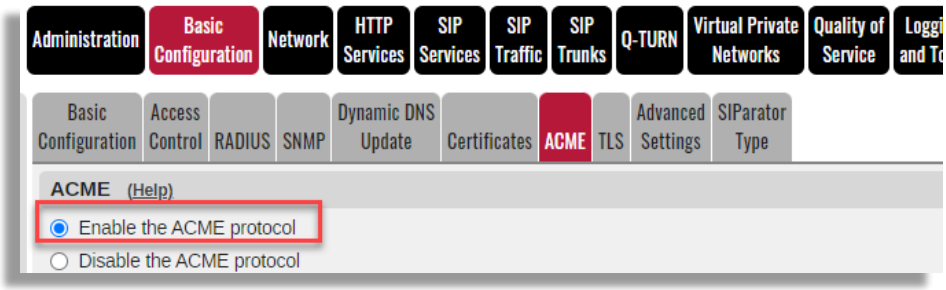
Guarde y vuelva a aplicar los cambios.

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



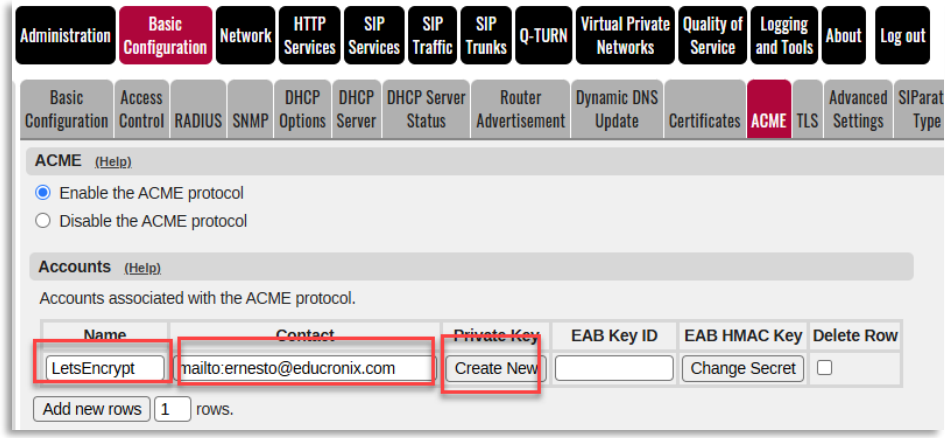
Uso de ACME

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

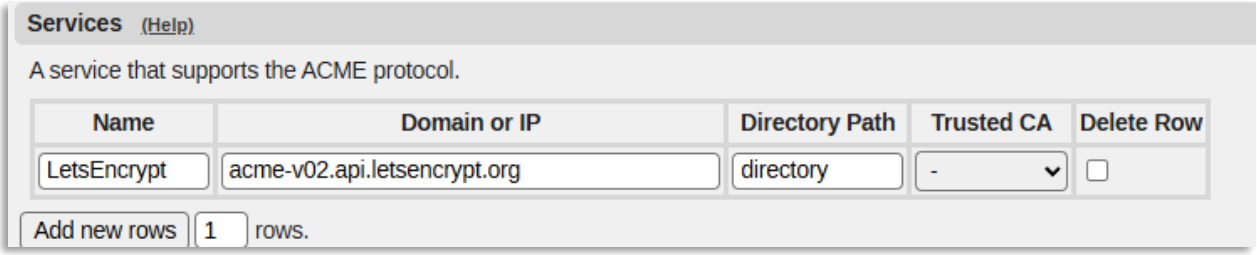
En nuestro caso usaremos Let's Encrypt que hemos confirmado que funciona correctamente con Zoom.



- Asignar nombre

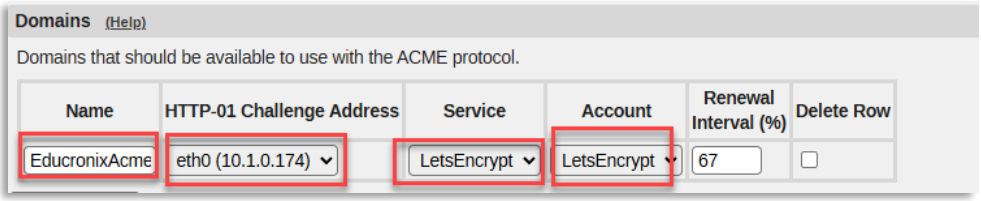
- Agregue información de contacto con el formato mailto:xxxxx@yyyy.zzz para proporcionar quién recibirá actualizaciones y notificaciones de la CA.
- Genere una "Clave privada" presionando "Crear nueva"

Agregar el servicio



- Asignar un nombre
- Introduzca el dominio proporcionado por la CA (para Lest'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.

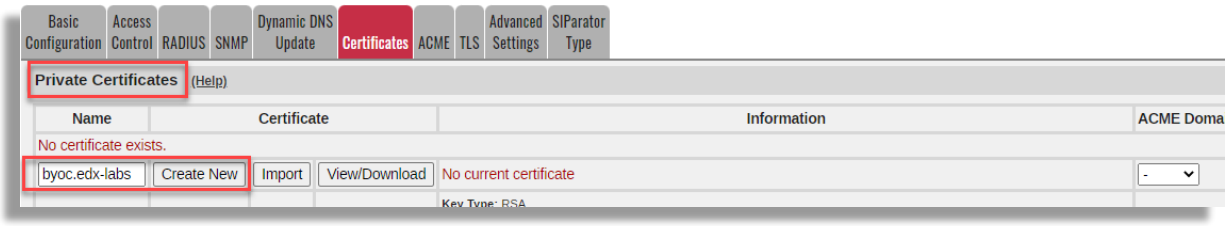


- Asignar un nombre
- Seleccione la interfaz que estará orientada hacia el exterior (Internet)
- Seleccione el servicio y la cuenta (creados anteriormente).
- Mantenga el valor predeterminado del 67% para establecer cuándo se activará la solicitud de renovación

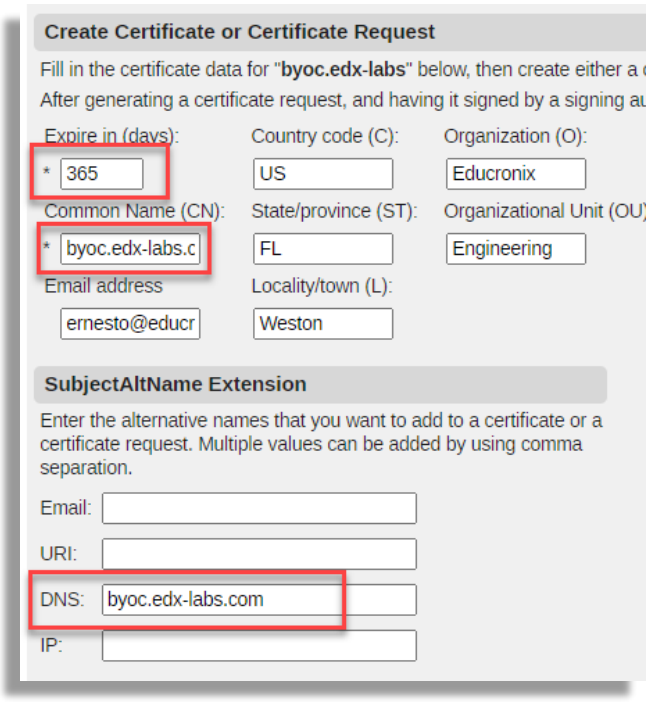
Ahora estamos listos para crear el certificado usando ACME.

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":

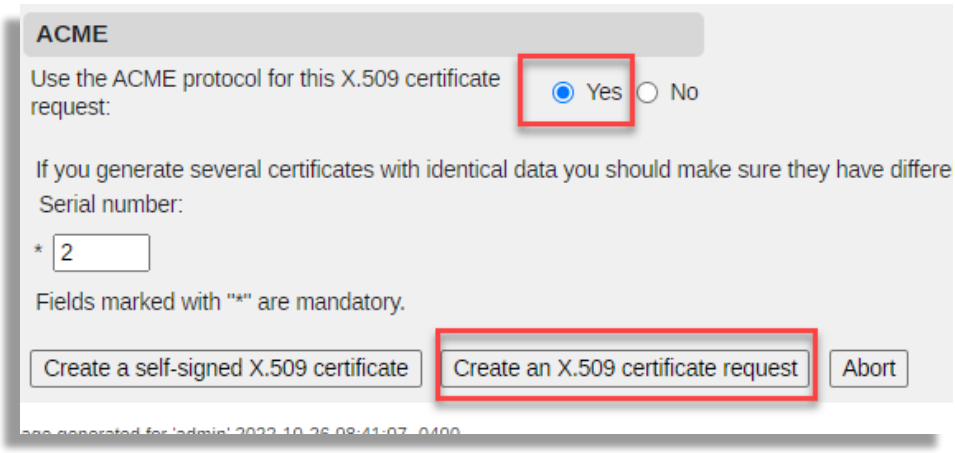


Completa la información aquí:



Notar:

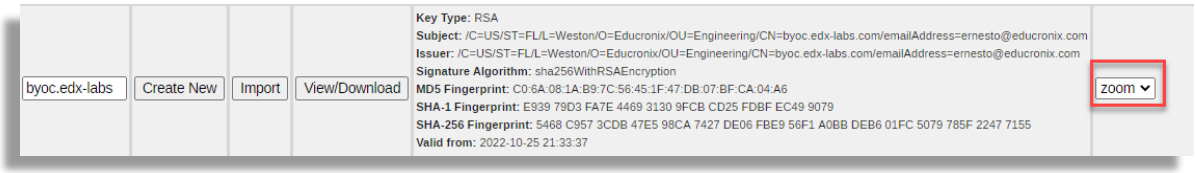
- Caducidad y Nombre común son campos obligatorios, sin embargo, la autoridad de certificación definirá Caducidad independientemente del valor que introduzca.
- El nombre común y el DNS deben coincidir con el FQDN asociado a la dirección IP pública de SIParator®.



- Seleccione "Sí" en la sección ACME
- Pulse en "Crear una solicitud de certificado X.509.

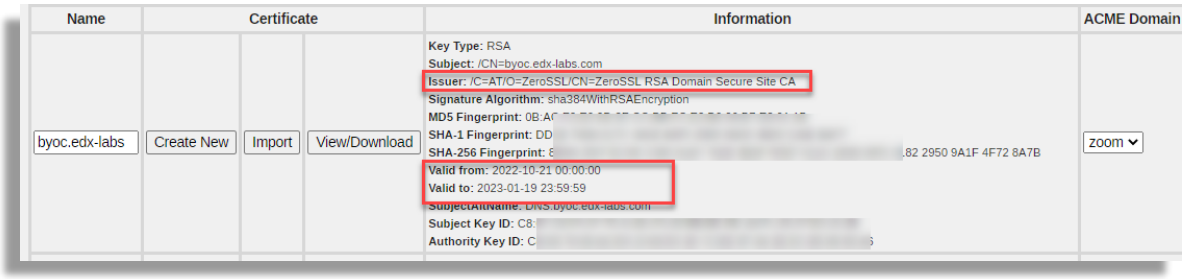
Esto crea un certificado autofirmado temporal hasta que la CA proporciona el nuevo certificado firmado.

Asegúrese de asociar el dominio ACME a este nuevo certificado.



Guardar y aplicar cambios

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



En el caso de ZeroSSL, puede ver el certificado y el intermedio (cadena de confianza) seleccionando "Ver/Descargar"

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:

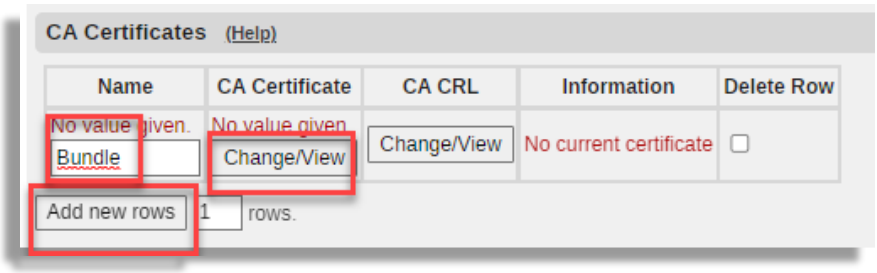
https://cacerts.digicert.com/DigiCertGlobalRootCA.crt.pem

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

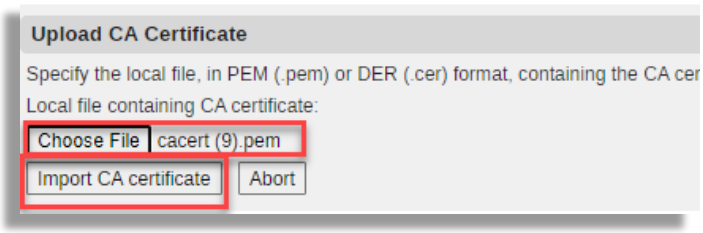
https://cacerts.digicert.com/DigiCertGlobalRootG3.crt.pem

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:

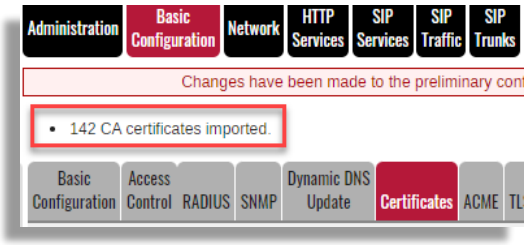


- Asigna un nombre (Bundle en nuestro caso)
- Haga clic en Certificado de CA "Cambiar/Ver"



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

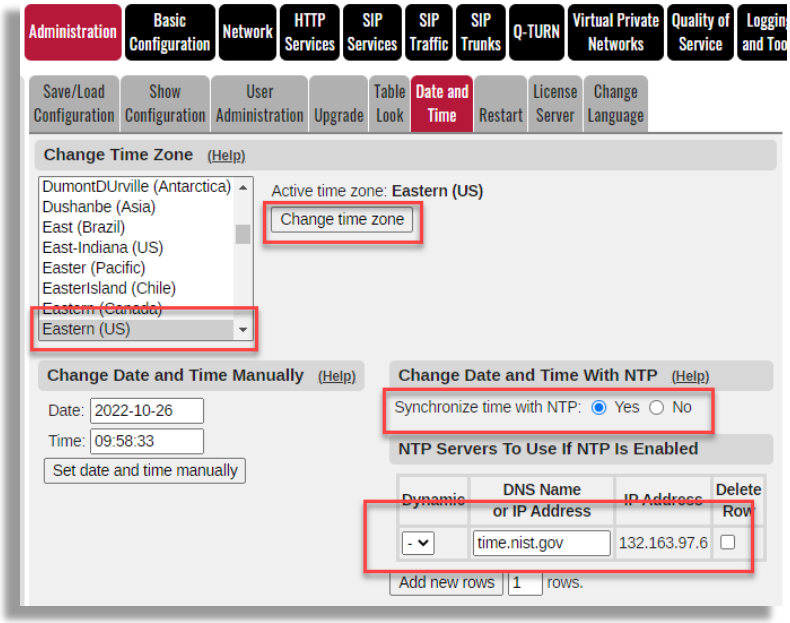
En el caso del paquete, verá alrededor de 142 certificados cargados con el mismo nombre.



Aplique y guarde los cambios.

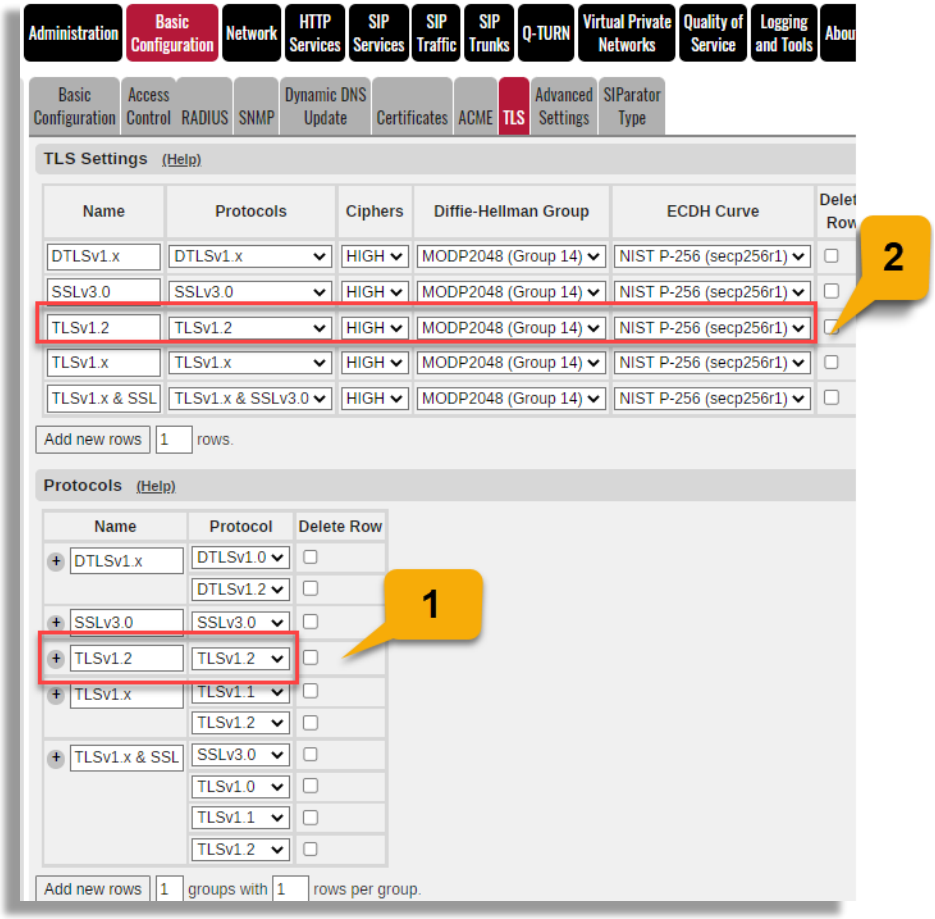
Configurar el servidor NTP

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



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.

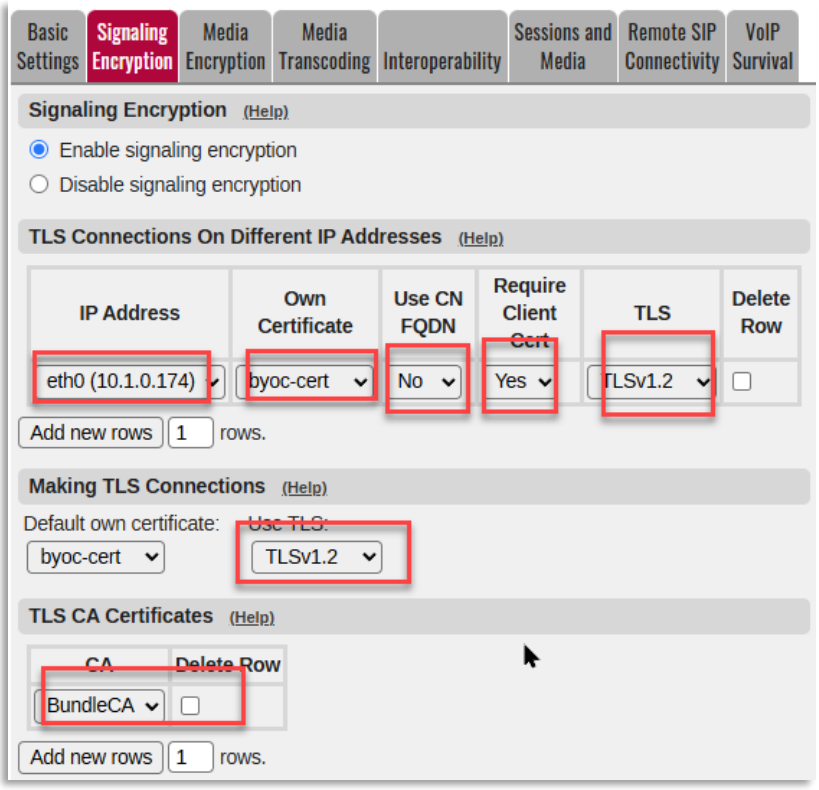


- Agregue una nueva entrada en la sección Protocolos que incluya solo TLSv1.2, lo llamamos "TLSv1.2
- Guarde y, a continuación, agregue una nueva entrada en la tabla Configuración de TLS, como se muestra en la imagen anterior. También lo llamamos "TLSv1.2"

Configuración de SIP en SIParator®

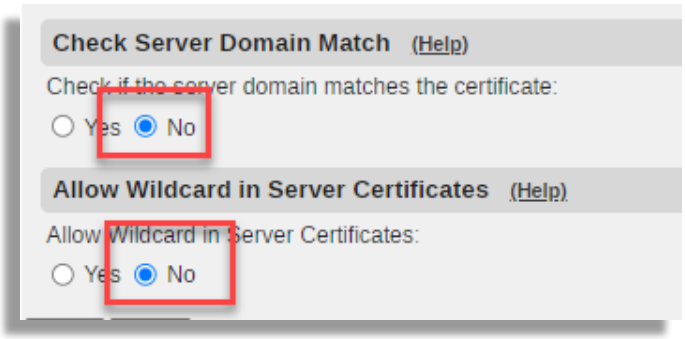
Ahora configuraremos toda la configuración relacionada con la señalización para SIP.

Configuración de la señalización TLS



- 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.

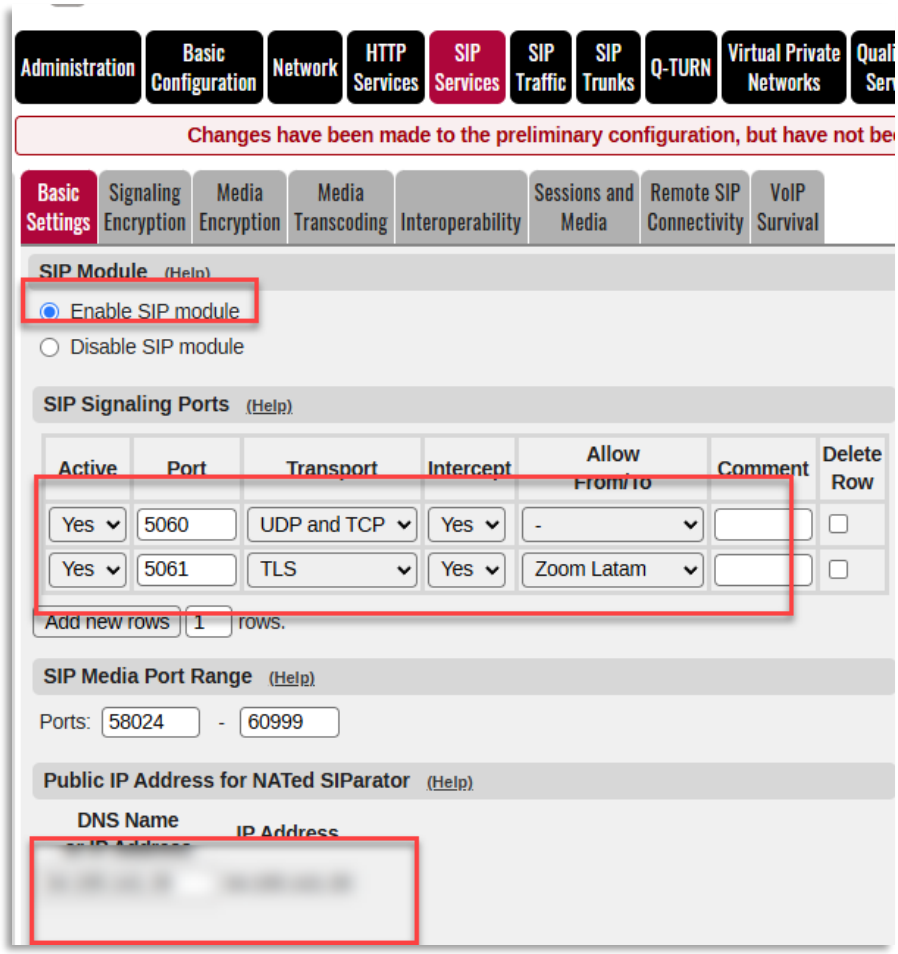
También dejará los siguientes dos ajustes en "No" como se muestra aquí:



Configuración de puertos SIP

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

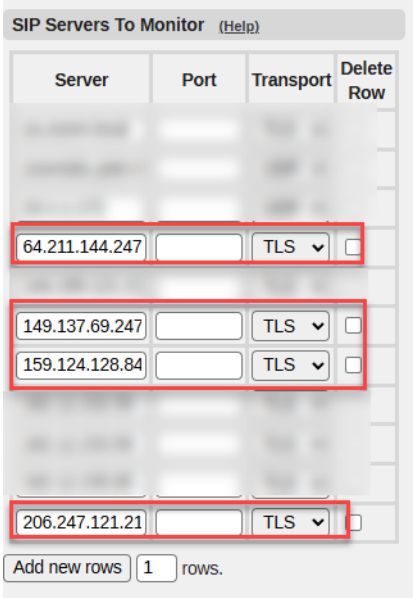
Vaya a Configuración básica de servicios SIP →



- 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.



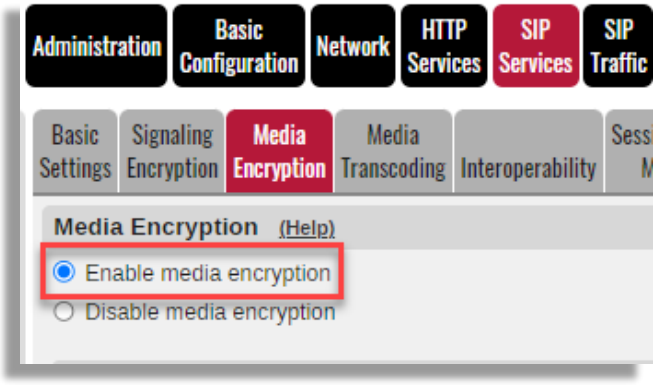
Estamos monitoreando entonces los nodos correspondientes a Latam según se explico inicialmente.

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.

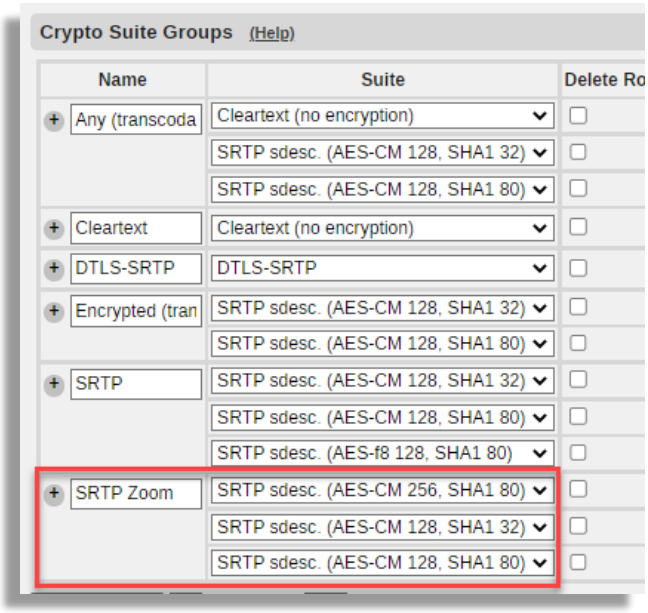
Configurar el cifrado de medios

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:

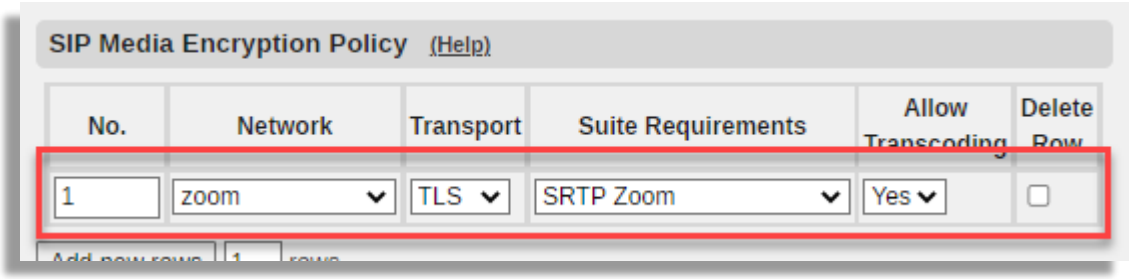


Luego crearemos un grupo de Crypto Suite específicamente para Zoom



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

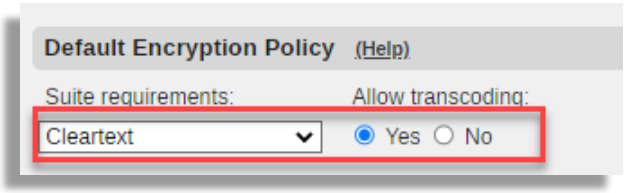
Agregue una política de cifrado de medios:



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

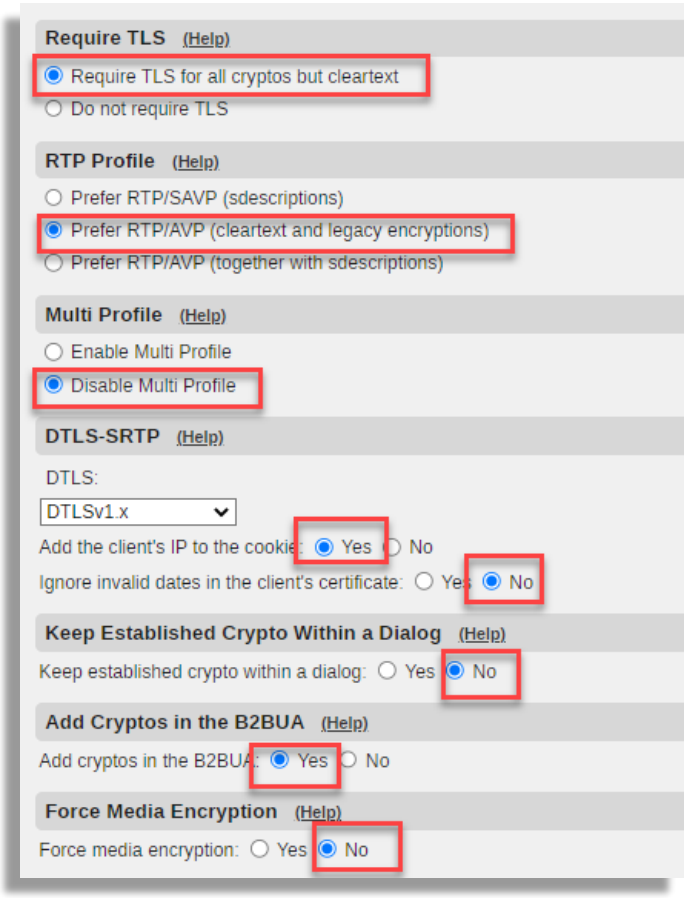
- Asocie la suite recientemente creada llamada "SRTP Zoom"
- Habilitar "Permitir transcodificación"

Defina una política de cifrado predeterminada para todo lo demás:



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

Establezca los parámetros restantes como se muestra:

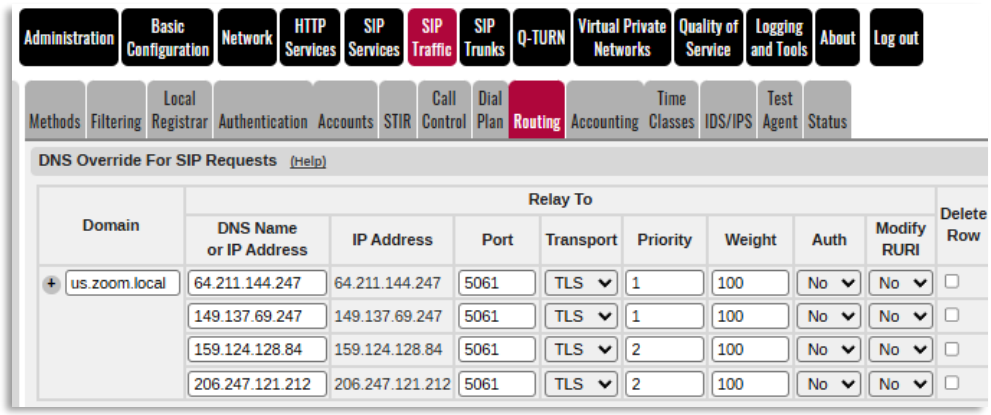


Definición de DNS Override para manejar trafico distribuido a Zoom con failover o balanceo

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

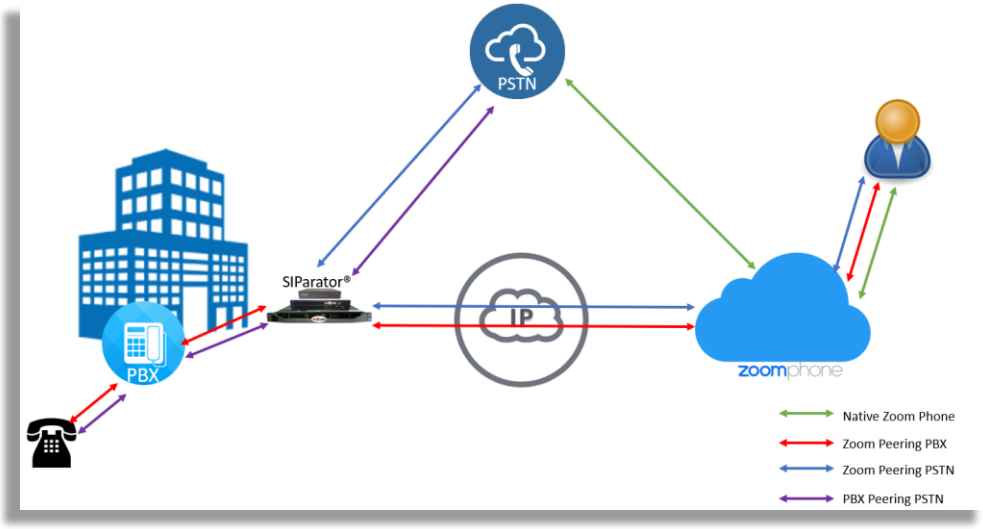


Acá hemos creado un destino (url) llamado us.zoom.local el cual distribuye con 2 diferentes prioridades (1 y 2) and grupos de proxys a los que se les va a distribuir en round-robin usando los pesos indicados.

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

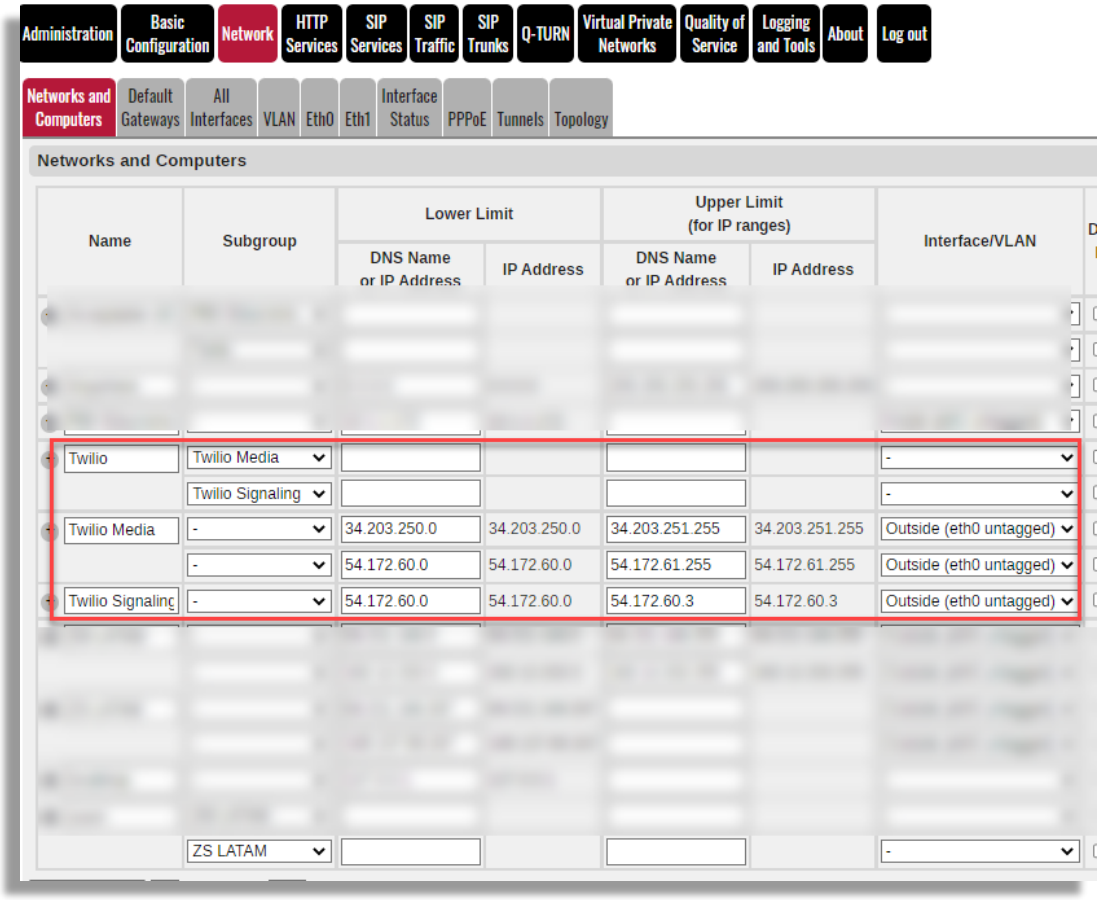
Entendamos cómo se ven los flujos SIP en nuestro caso:



Configuración del grupo troncal Zoom-PSTN

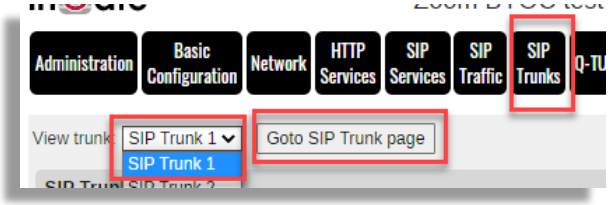
En nuestro caso, estamos utilizando el servicio de enlace troncal SIP de Twilio con fines de demostración.

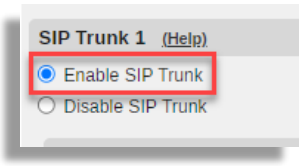
Primero, debemos agregar un nombre de red para las direcciones IP proporcionadas por Twilio. Se pueden encontrar en el sitio web de Twilio (https://www.twilio.com/docs/sip-trunking/ip-addresses). Incluiremos solo las IP de Virginia de América del Norte, ya que el SIParator está alojado en la región de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



Vamos a configurar el grupo troncal

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

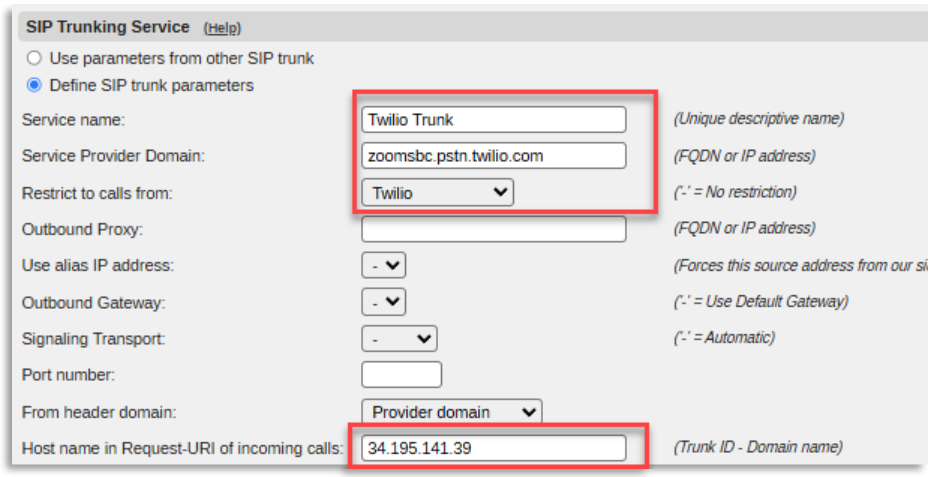




Haga clic en "Ir a la página de troncales SIP" y habilite el grupo de troncales

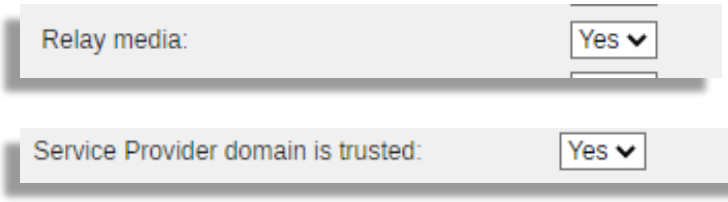
Estamos utilizando el servicio troncal SIP elástico de Twilio y tenemos como FQDN asignado: zoompeering.pstn.twilio.com

Para no definir el troncal:

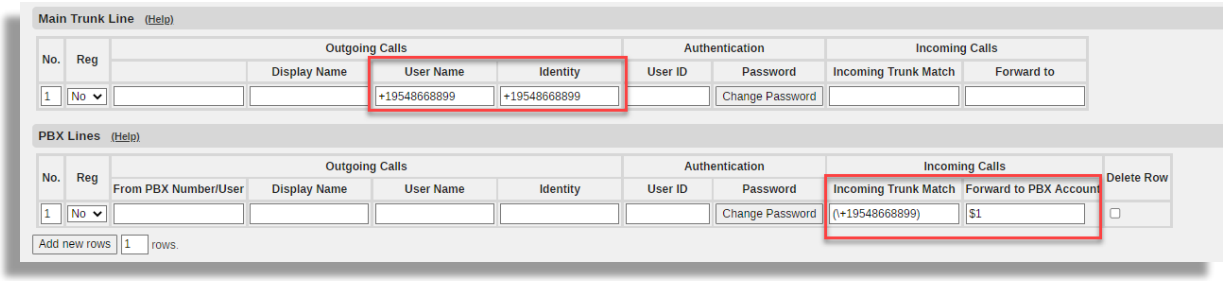


- Asignar un nombre al grupo de troncales
- Utilice el FQDN de proxy proporcionado como dominio del proveedor de servicios.
- Como nuestro SIParator® está detrás de un firewall (DMZ), necesitaremos ingresar la IP pública en el nombre de host en Request-URI.

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

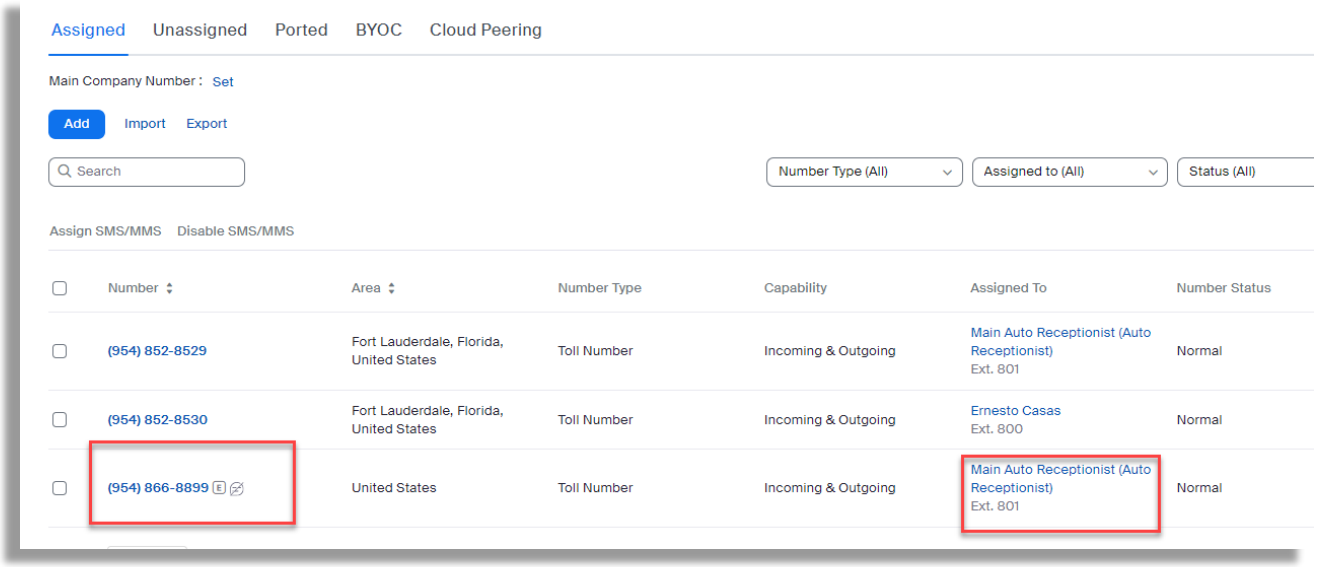


Ahora configuraremos las reglas de coincidencia para enrutar los DID entrantes designados para los usuarios de Zoom o el operador automático:



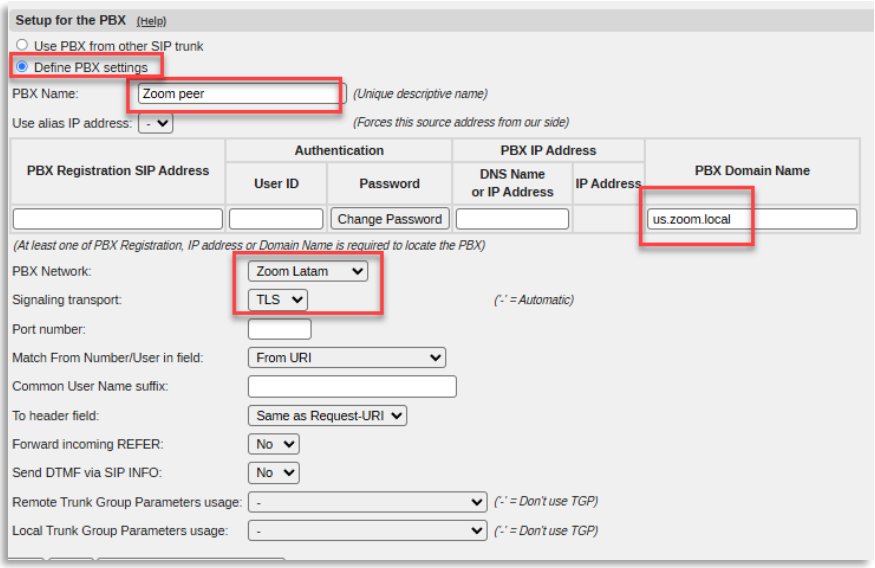
Si tiene más de un DID, puede seguir agregando filas a la tabla de líneas PBX y hacer coincidir DID adicionales. También puede utilizar expresiones regulares para la coincidencia.

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.



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 ",".



- 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

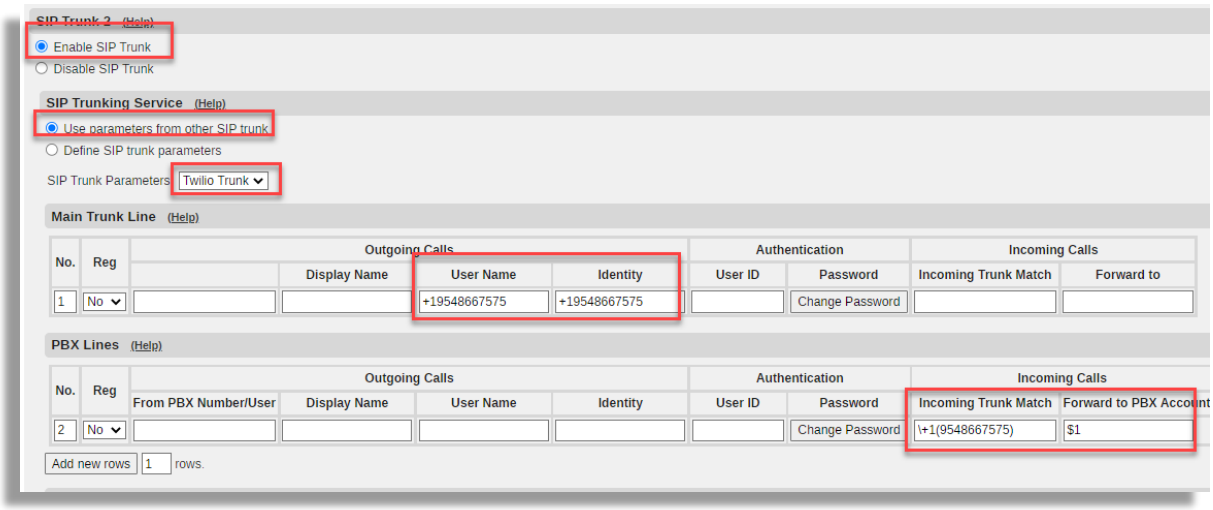
- Seleccione la Red (ZS LATAM), creada previamente en → Redes de Red y Computadoras
- Seleccione Señalización TLS.
- Deje los campos restantes con valores predeterminados.

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.

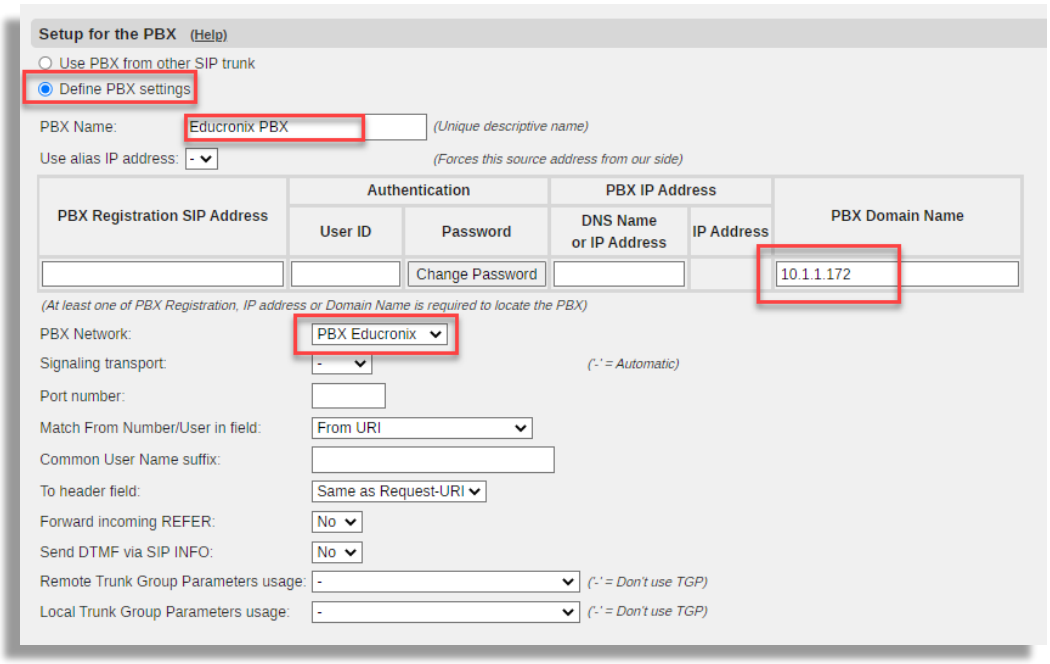
Necesitaremos agregar una nueva página de grupo troncal

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.

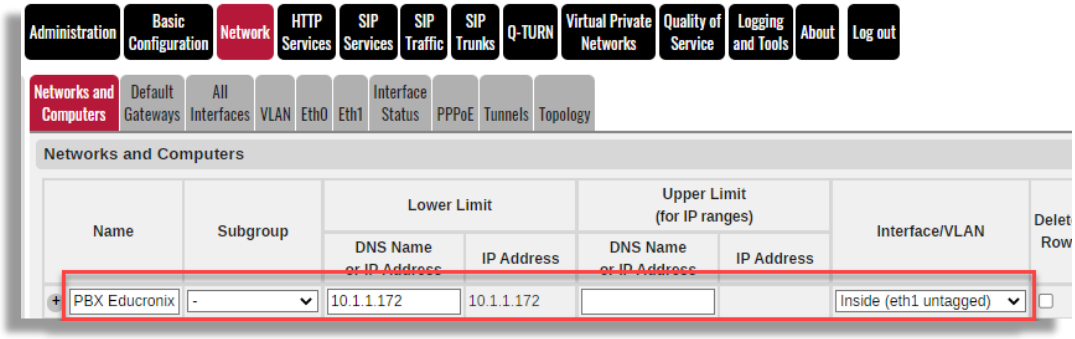


- Habilitar el troncal
- Utilice parámetros de otro troncal SIP y elija Troncal de Twilio (configurado en la sección anterior)
- Wi utilizará un DID diferente y lo agregará al nombre de usuario e identidad salientes para fines de identificación de llamadas.
- Para la llamada entrante coincidirá con el 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



- 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:

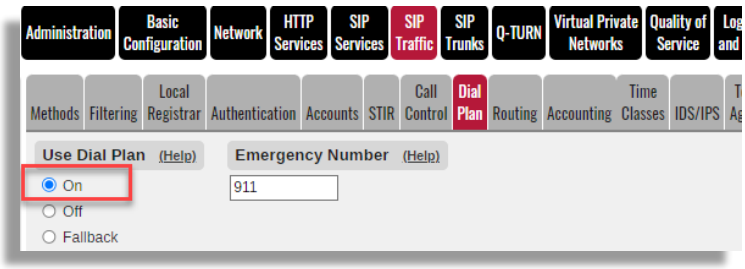


- Deje los campos restantes con los valores predeterminados.

Configurar el plan de marcado

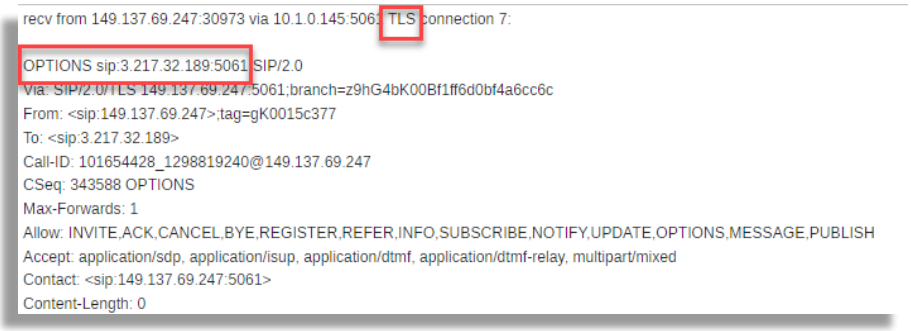
Con el plan de marcado, podremos enrutar el tráfico saliente, el tráfico entre Zoom y PBX y también habilitar el SIParator® para responder a las solicitudes de opciones de Zoom.

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



Habilitación de opciones SIP para solicitudes de Zoom

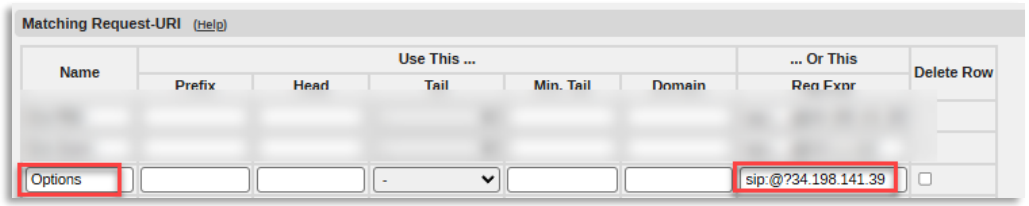
Necesitaremos detectar las solicitudes de OPTIONS que aterrizan en la interfaz externa. Las opciones de SP envían solicitudes a la IP pública externa de forma similar a esta:



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

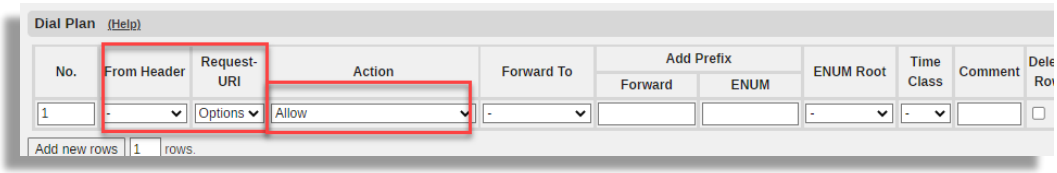
sip:@?34.195.141.39

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 trafico proveniente de la PBX o de Zoom usando la sección de matching From Header.

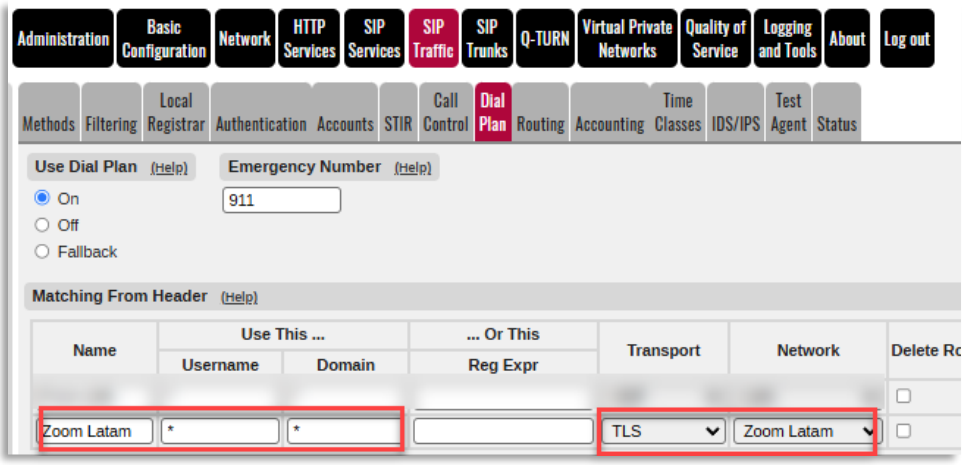
La regla From LAN identifica todo tráfico proveniente de la red Interna y eso incluye la PBX y Zoom Latam identifica tráfico proveniente de Zoom. EN ambos casos se usa la red de origen para hacer el match.

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

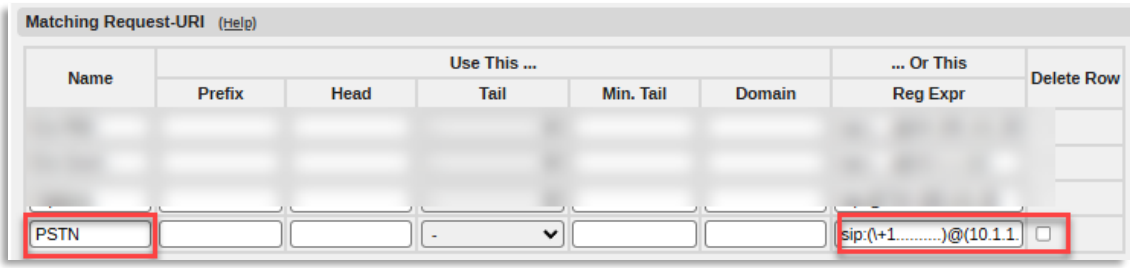
Para detectar/hacer coincidir el tráfico proveniente de Zoom, agregaremos una regla en la sección de encabezado match From



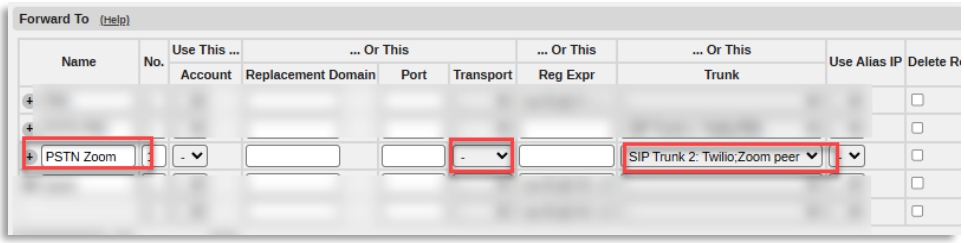
- Agregar una fila en el encabezado Coincidencia desde
- Asignar un nombre a la regla
- Utilice el comodín "*" para el nombre de usuario y el dominio.
- Seleccione el protocolo de transporte que se va a detectar (TLS)
- Seleccione la red de la que provendrá el tráfico (fuentes de señalización de Zoom)

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)

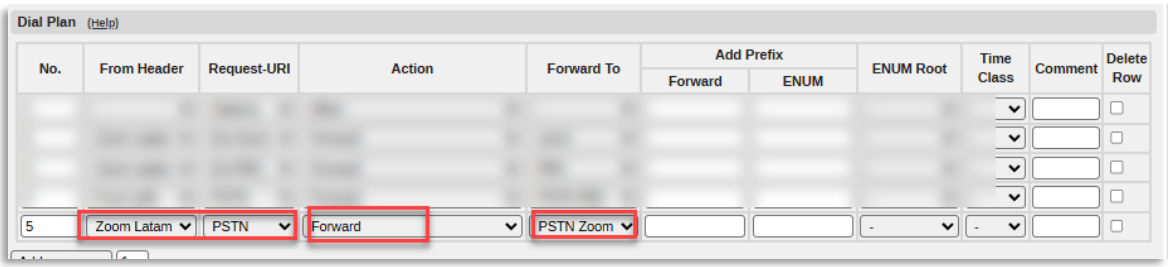


- Agregue una nueva fila en "Matching Request-URI"
- Asignar un nombre a la nueva regla
- Haga coincidir las solicitudes SIP con ***sip:(\+1.....)@(10.1.1.112|34.195.141.39)***
- Ahora definiremos el destino al troncal PSTN (reenviar a) utilizando el grupo de troncales Zoon-PSTN



- 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 DIDs)

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

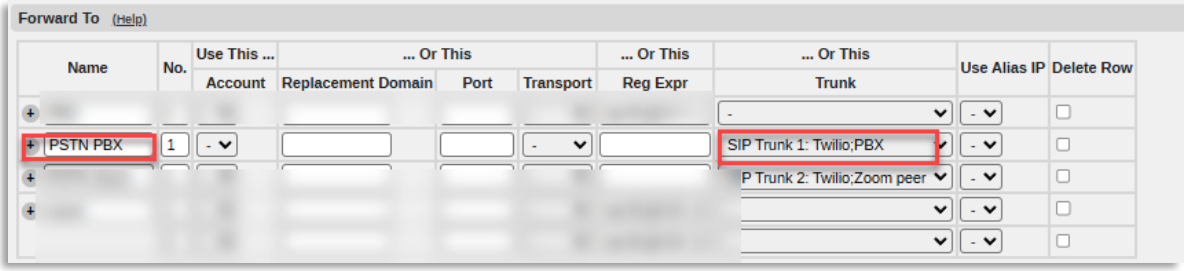


- Cree una regla en la que Si **el encabezado From** coincide con "Zoom Latam" y el **URI de solicitud** coincide con "PSTN", hace un **Forward** a "PSTN Zoom"

Ruta de salida de PBX a PSTN

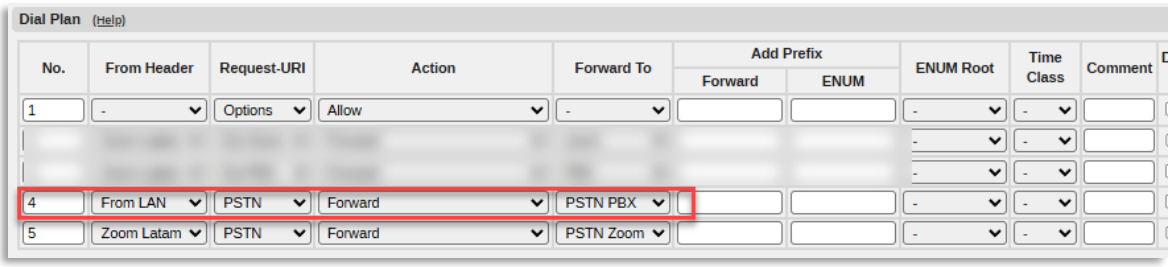
Ahora estamos listos para agregar reglas de plan de marcado para enrutar la salida a RTC procedente de PBX.

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



- 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:

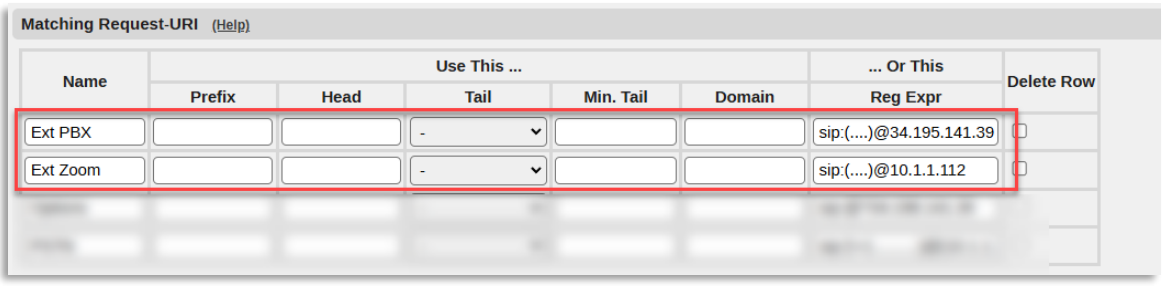


- Agregar una nueva fila a "Plan de marcado"
- Haga coincidir **el encabezado From** con la regla "From PBX" y **el URI de solicitud** con "To PSTN" y "Forward" a la ruta creada anteriormente denominada "To ITSP PBX"

El siguiente paso será agregar las reglas de enrutamiento necesarias para mover el tráfico Usuarios/Extensiones de Zoom ←→ Usuarios/Extensiones de PBX

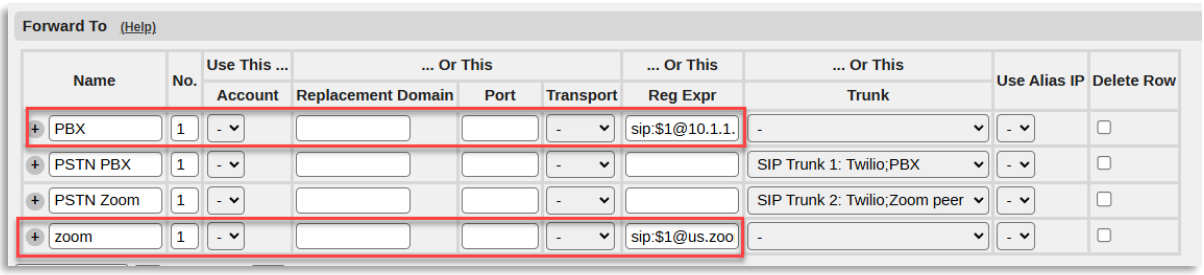
Ruta PBX←→Zoom

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.



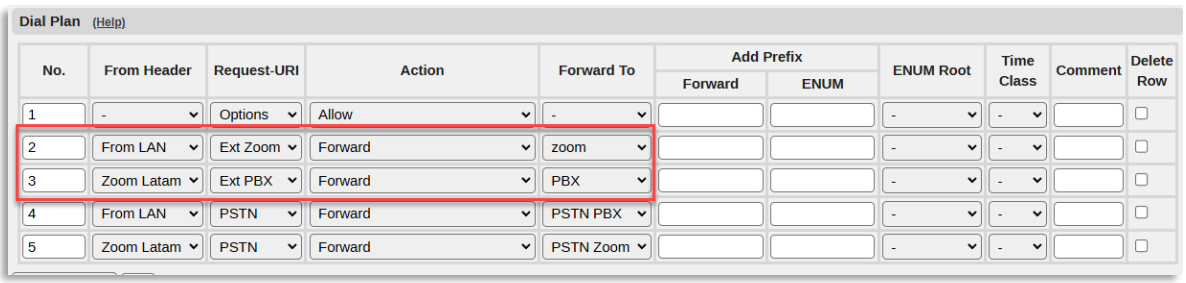
- Agregue una nueva fila para hacer coincidir la marcación con una extensión PBX. Esta llamada llegará a la interfaz externa a la dirección IP pública del SIParator®.
- Asigne un nombre a la nueva fila.
- Introduzca la cadena coincidente " sip:(....)@34.195.141.39”
- Agregue una nueva fila para hacer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



- 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



- 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)

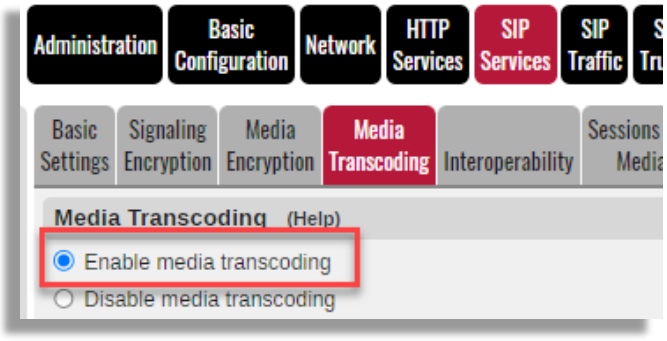
Configuración de la transcodificación

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:

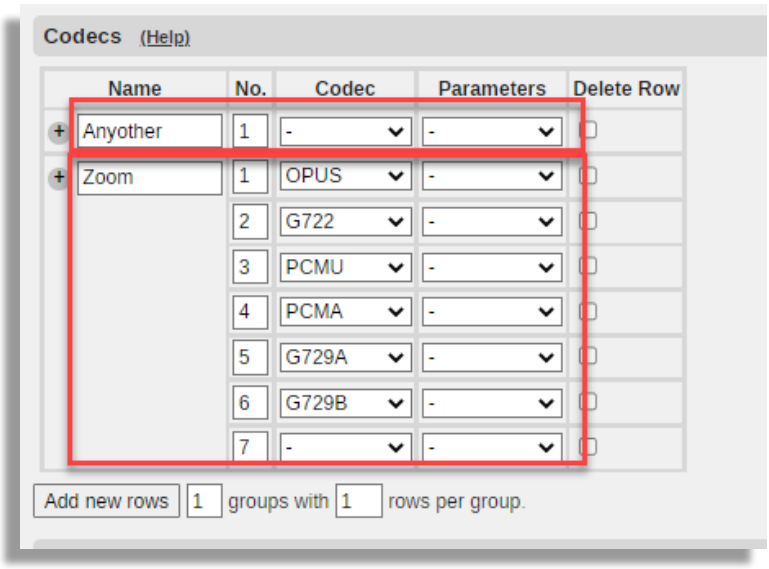
- OPUS
- G.722
- G.711A-ley/μ-ley
- G.729

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

Tendrás que habilitar la transcodificación:

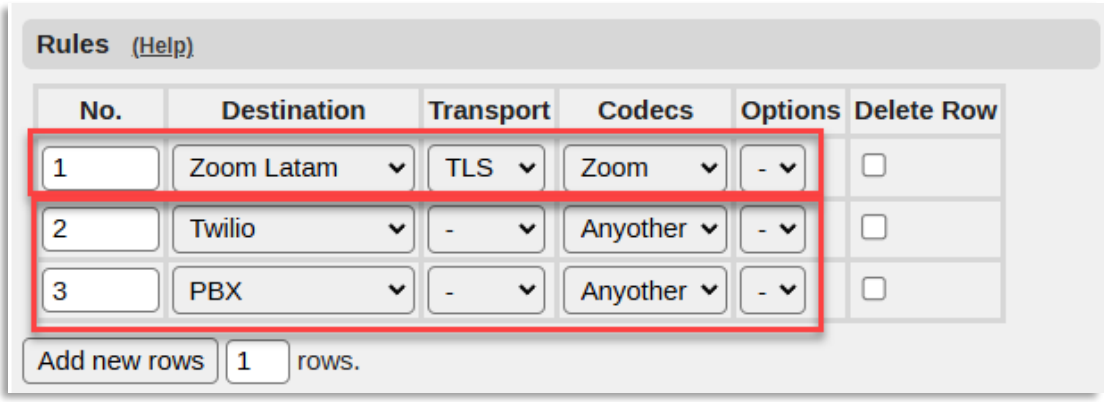


Primero crearemos los grupos de códecs necesarios:



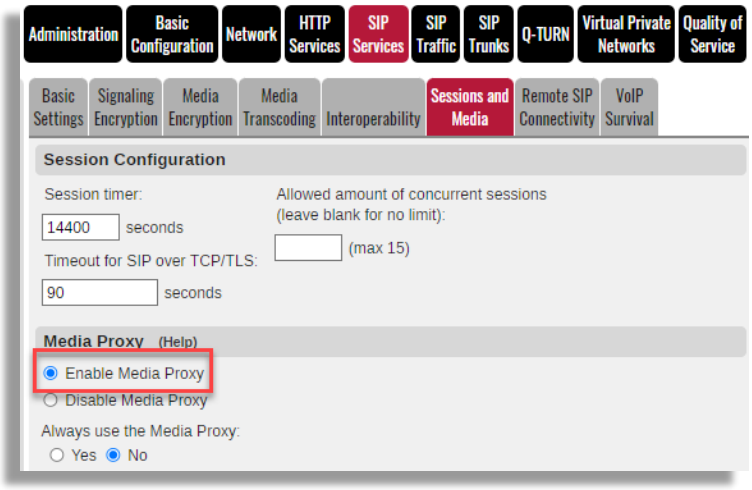
- Agregue 1 fila y 1 fila adicional con 7 subfilas.
- La primera fila, denominada Cualquier otro en nuestro ejemplo, no tendrá ninguna selección en la columna Códec. Esto significa que cualquier códec es compatible con el grupo.
- La segunda fila, denominada Zoom, tiene una subfila por cada códec compatible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

Asociemos qué códecs están asociados a qué red de señalización:



- 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:


Administration
Basic Configuration
Network
HTTP Services
SIP Services
SIP Traffic
SIP Trunks
Q-TURN
Virtual Private Networks
Quality of Service
Basic Settings
Signaling Encryption
Media Encryption
Media Transcoding
Interoperability
Sessions and Media
Remote SIP Connectivity
VoIP Survival
Session Configuration
Session timer:
14400
seconds
Timeout for SIP over TCP/TLS:
90
seconds
Allowed amount of concurrent sessions
(leave blank for no limit):
(max 15)
Media Proxy (Help)
Enable Media Proxy
Disable Media Proxy
Always use the Media Proxy:
Yes
No

Recomendaciones finales y otros puntos de interés

Documentación útil

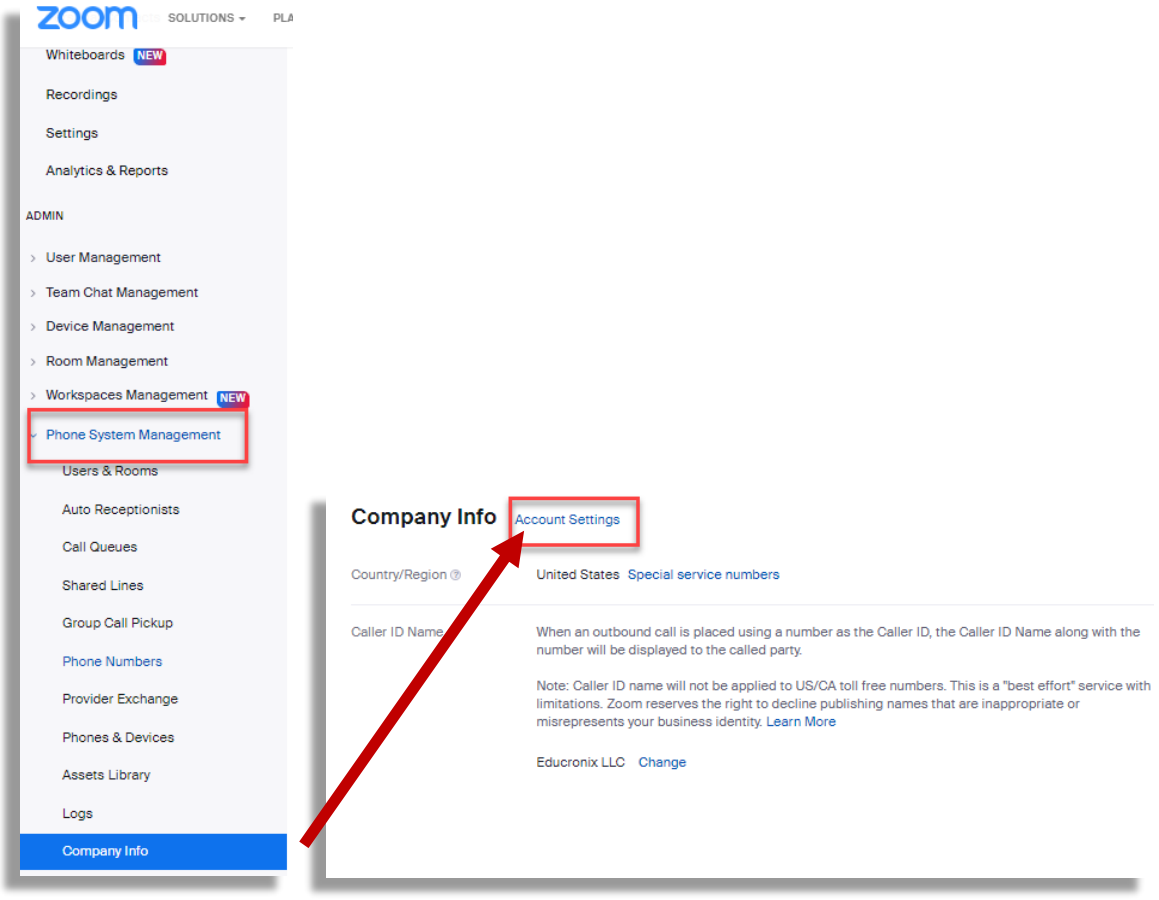
- SIParator® reference Guide v 7.0.2
- Cómo usar la manipulación de encabezados genéricos
- Orientación e instalación – Ingate Software SIParator® Firewall/SIParator

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.

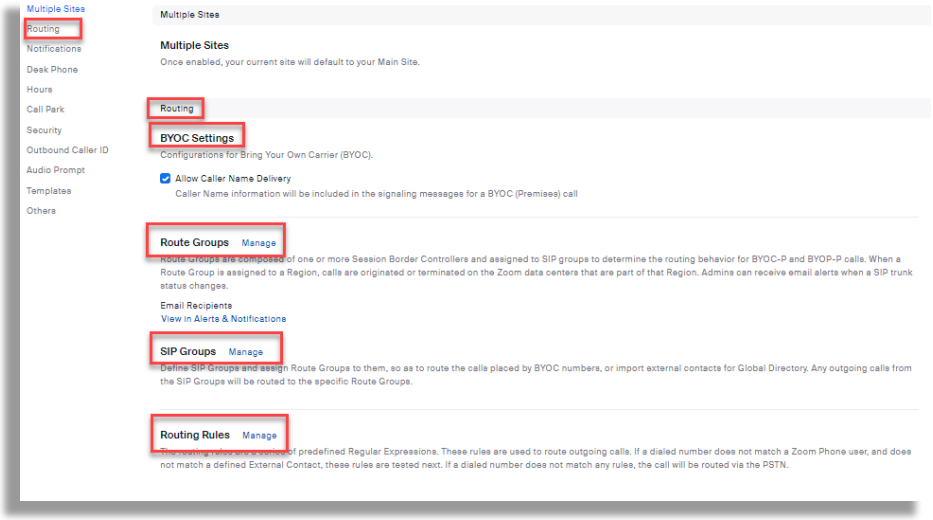
Una vez que lo tenga habilitado, notará el siguiente hecho en el panel de control de su cuenta de Zoom.

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



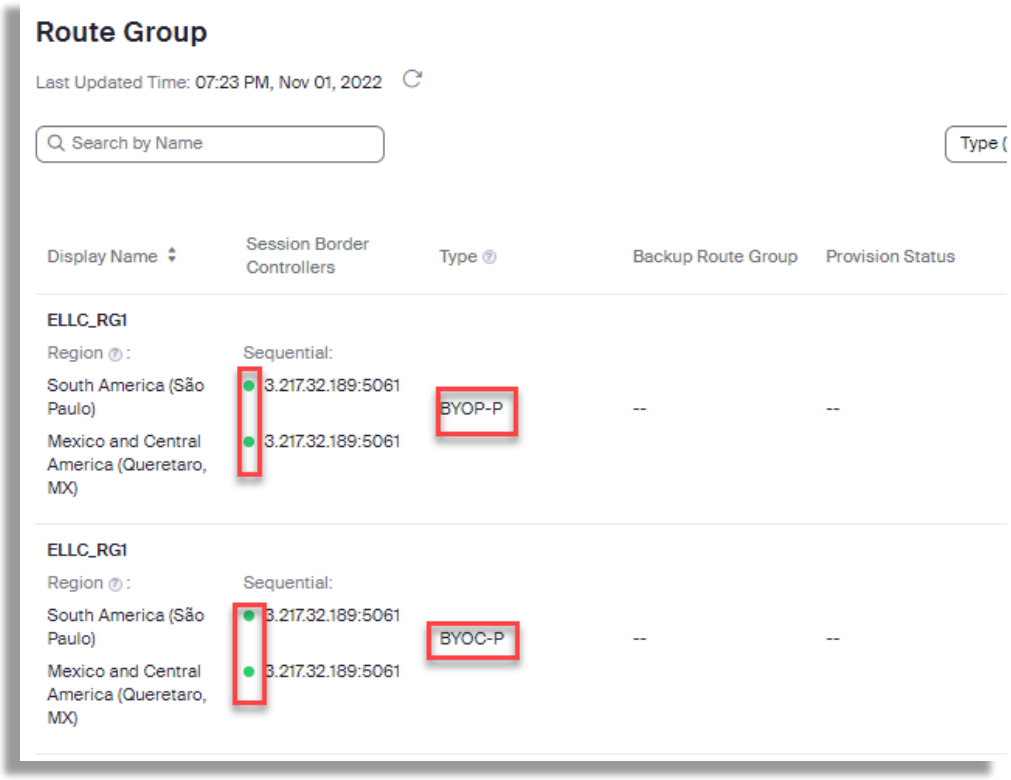
Seleccione Información de la empresa y, a continuación, **Configuración de la cuenta**

Hay 4 secciones importantes a las que debes prestar atención:



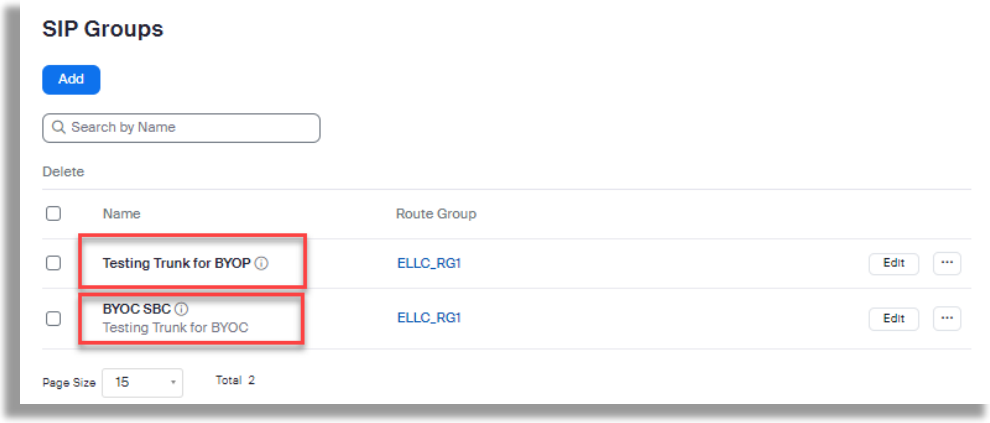
Grupos de rutas (Administrar)

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



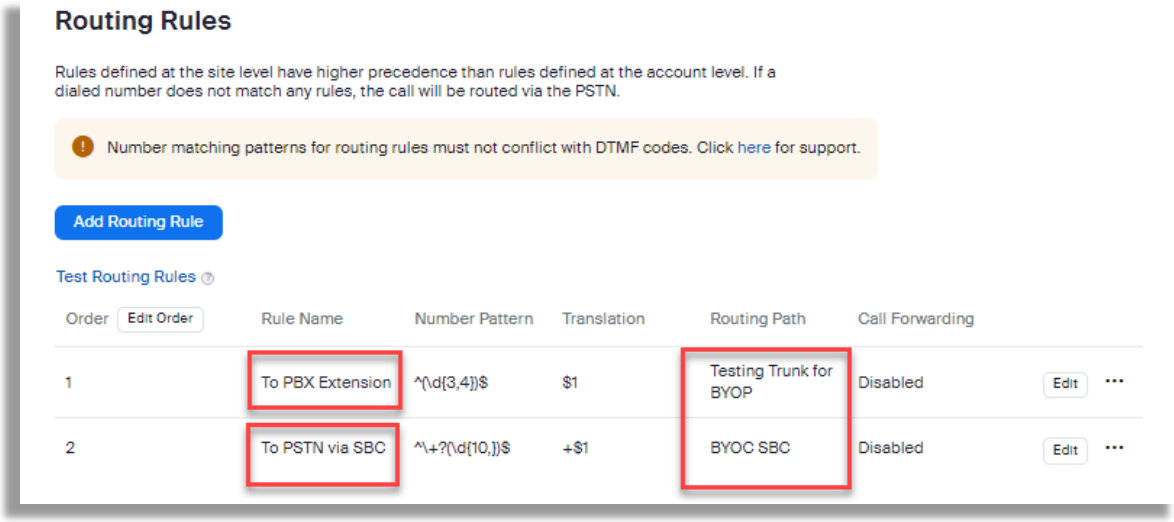
Grupos SIP (Administrar)

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

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