Implementación de teléfonos SIP IP Office remotos con un ASBCE

Versión 12.0
Edición 14
Abril de 2024

Aviso

Si bien se hicieron esfuerzos razonables para asegurar que la información contenida en este documento esté completa y sea exacta en el momento de su impresión, Avaya no se responsabiliza por los errores. Avaya se reserva el derecho de realizar cambios y correcciones a la información contenida en este documento sin la obligación de notificar a ninguna persona u organización dichos cambios.

Exención de responsabilidad con respecto a la documentación

“Documentación” hace referencia a la información publicada en diversos medios, que puede incluir información del producto, descripciones de suscripciones o servicios, instrucciones operativas y especificaciones de rendimiento, que se suelen poner a disposición de los usuarios de productos. La documentación no incluye material publicitario. Avaya no asume la responsabilidad por las modificaciones, adiciones o eliminaciones efectuadas en la versión original publicada de la Documentación, a menos que dichas modificaciones, adiciones o eliminaciones hayan sido realizadas por Avaya o expresamente a nombre de esta. El Usuario final acuerda indemnizar y eximir de toda responsabilidad a Avaya, agentes de Avaya y empleados con respecto a todo reclamo, acción judicial, demanda y juicio que surgiere de o en relación con modificaciones, incorporaciones o eliminaciones posteriores en esta documentación realizadas por el Usuario final.

Exención de responsabilidad con respecto a los vínculos

Avaya no asume la responsabilidad del contenido ni la fiabilidad de los enlaces a los sitios web incluidos en cualquier punto de este sitio o en la Documentación proporcionada por Avaya. Avaya no es responsable de la confiabilidad de ninguna información, instrucción ni contenido proporcionado en estos sitios y no necesariamente aprueba los productos, los servicios o la información que describen u ofrecen. Avaya no garantiza que estos vínculos funcionarán todo el tiempo ni tiene control de la disponibilidad de las páginas vinculadas.

Garantía

Avaya ofrece una garantía limitada para los productos de hardware y software de Avaya. Consulte su contrato con Avaya para establecer las condiciones de la garantía limitada. Además, el idioma de la garantía estándar de Avaya, así como la información relacionada con el soporte técnico para este producto durante el período de vigencia de la garantía, está disponible, tanto para los clientes de Avaya como para otras personas interesadas, en el sitio web del Soporte técnico de Avaya: https://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010 o en el enlace “Garantía y ciclo de vida del producto” o en el sitio web posterior designado por Avaya. Tenga en cuenta que si ha adquirido los productos de un Channel Partner de Avaya fuera de Estados Unidos y Canadá, la garantía es proporcionada por dicho Channel Partner de Avaya y no por Avaya.

“**Servicio alojado**” significa una suscripción de servicio alojado por Avaya que Usted adquiere ya sea de Avaya o de un Channel Partner de Avaya (según corresponda) y que se describe detalladamente en SAS alojado u otra documentación de descripción del servicio sobre el servicio alojado correspondiente. Si compra una suscripción de Servicio alojado, la garantía limitada anterior podría no ser aplicable, pero puede tener derecho a servicios de soporte técnico relacionados con el Servicio alojado como se describe más adelante en los documentos de descripción del servicio para el Servicio alojado correspondiente. Comuníquese con Avaya o el Channel Partner de Avaya (según corresponda) para obtener más información.

Servicio alojado

SE APLICA LO SIGUIENTE ÚNICAMENTE SI ADQUIERE UNA SUSCRIPCIÓN DE AVAYA A UN SERVICIO HOSPEDADO DE AVAYA O UN CHANNEL PARTNER DE AVAYA (SI CORRESPONDE), LOS TÉRMINOS DE USO PARA LOS SERVICIOS HOSPEDADOS ESTÁN DISPONIBLES EN EL SITIO WEB DE AVAYA HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO EN EL ENLACE “Avaya Terms of Use for Hosted Services” O EN LOS SITIOS FUTUROS QUE DESIGNE AVAYA, Y SE APLICAN A TODA PERSONA QUE TENGA ACCESO O USE EL SERVICIO HOSPEDADO. AL ACCEDER O USAR EL SERVICIO HOSPEDADO, O AL AUTORIZAR A TERCEROS A HACERLO, EN NOMBRE SUYO Y DE LA ENTIDAD PARA LA QUE ACCEDE O USA EL SERVICIO HOSPEDADO (EN ADELANTE, A LOS QUE SE HACE REFERENCIA INDISTINTAMENTE COMO “USTED” Y “USUARIO FINAL”), ACEPTA LOS TÉRMINOS DE USO. SI ACEPTA LOS TÉRMINOS DE USO EN NOMBRE DE UNA COMPAÑÍA U OTRA ENTIDAD LEGAL, USTED DECLARA QUE TIENE LA AUTORIDAD PARA VINCULAR A DICHA ENTIDAD CON LOS PRESENTES TÉRMINOS DE USO. SI NO CUENTA CON DICHA AUTORIDAD O SI NO ESTÁ DE ACUERDO CON LOS PRESENTES TÉRMINOS DE USO, NO DEBE ACCEDER NI USAR EL SERVICIO HOSPEDADO NI AUTORIZAR A TERCEROS A QUE ACCEDAN O USEN EL SERVICIO HOSPEDADO.

Licencias

Los Términos globales de licencia de software (“Términos de licencia de software”) están disponibles en el siguiente sitio web https://www.avaya.com/en/legal-license-terms/ o cualquier sitio posterios designado por Avaya. Estos Términos de licencia de software se aplican a cualquiera que instale, descargue o use Software o Documentación. Al instalar, descargar o usar el Software, o al autorizar a terceros a hacerlo, el usuario final acepta que estos Términos de licencia de software crean un contrato vinculante entre el usuario final y Avaya. Si el usuario final acepta estos Términos de licencia de software en nombre de una compañía u otra entidad legal, el usuario final declara que tiene la autoridad para vincular a dicha entidad con los presentes Términos de licencia de software.

Copyright

Excepto donde se indique expresamente lo contrario, no se debe hacer uso de los materiales de este sitio, de la Documentación, del Software, del Servicio alojado ni del hardware proporcionados por Avaya. Todo el contenido de este sitio, la documentación, el Servicio alojado y los productos proporcionados por Avaya, incluida la selección, la disposición y el diseño del contenido, son de propiedad de Avaya o de sus licenciantes y están protegidos por leyes de derecho de autor y otras leyes de propiedad intelectual, incluidos los derechos de su género relacionados con la protección de las bases de datos. No debe modificar, copiar, reproducir, reeditar, cargar, publicar, transmitir ni distribuir de ninguna manera el contenido, en su totalidad o en parte, incluidos los códigos y el software, a menos que posea una autorización expresa de Avaya. La reproducción, transmisión, difusión, almacenamiento o uso no autorizado sin el consentimiento expreso por escrito de Avaya puede considerarse un delito penal o civil según la ley vigente.

Virtualización

Si el producto se implementa en una máquina virtual, se aplica lo siguiente. Cada producto tiene su propio código de pedido y tipos de licencia. A menos que se indique lo contrario, cada instancia de un producto debe pedirse por separado y tener una licencia independiente. Por ejemplo, si el cliente usuario final o el Channel Partner de Avaya prefieren instalar dos Instancias del mismo tipo de producto, entonces se deben solicitar dos productos del mismo tipo.

Componentes de terceros

Lo siguiente corresponde solo si el códec H.264 (AVC) se distribuye con el producto. ESTE PRODUCTO ESTÁ SUJETO A LA LICENCIA DE CARTERA DE PATENTES AVC PARA EL USO PERSONAL DE UN CONSUMIDOR Y OTROS USOS QUE NO IMPLIQUEN REMUNERACIÓN PARA (i) CODIFICAR VIDEO QUE CUMPLA CON EL ESTÁNDAR AVC (“AVC VIDEO”) O (ii) DECODIFICAR VIDEO AVC QUE UN CLIENTE CODIFICÓ DURANTE UNA ACTIVIDAD PERSONAL U OBTENIDO A TRAVÉS DE UN PROVEEDOR DE VIDEO AUTORIZADO PARA SUMINISTRAR VIDEO AVC. NO SE OTORGA LICENCIA NI SE IMPLICA PARA CUALQUIER OTRO USO. PARA OBTENER INFORMACIÓN ADICIONAL, PUEDE CONSULTAR MPEG LA, L.L.C. VISITE HTTP://WWW.MPEGLA.COM.

Proveedor de servicio

CON RESPECTO A LOS CÓDECS, SI EL CHANNEL PARTNER DE AVAYA ALOJA PRODUCTOS QUE UTILIZAN O INCORPORAN LOS CÓDECS H.264 O H.265, EL CHANNEL PARTNER DE AVAYA RECONOCE Y MANIFIESTA ACUERDO CON QUE ES RESPONSABLE DE ASUMIR TODAS LAS TARIFAS Y/O REGALÍAS. EL CÓDEC H.264 (AVC) ESTÁ SUJETO A LA LICENCIA DE CARTERA DE PATENTES AVC PARA EL USO PERSONAL DE UN CONSUMIDOR Y OTROS USOS QUE NO IMPLIQUEN REMUNERACIÓN PARA (i) CODIFICAR VIDEO QUE CUMPLA CON EL ESTÁNDAR AVC (“AVC VIDEO”) O (ii) DECODIFICAR VIDEO AVC QUE UN CONSUMIDOR CODIFICÓ DURANTE UNA ACTIVIDAD

PERSONAL U OBTENIDO A TRAVÉS DE UN PROVEEDOR DE VIDEO AUTORIZADO PARA SUMINISTRAR VIDEO AVC. NO SE OTORGA LICENCIA NI SE IMPLICA PARA CUALQUIER OTRO USO. SE PODRÁ OBTENER INFORMACIÓN ADICIONAL SOBRE LOS CÓDECS H.264 (AVC) y H.265 (HEVC) DE MPEG LA, L.L.C. VISITE HTTP://WWW.MPEGLA.COM.

Cumplimiento de leyes

Usted reconoce y acepta que es su responsabilidad respetar las leyes y los reglamentos aplicables, incluidos, a mero título enunciativo, las leyes y los reglamentos relacionados con la grabación de llamadas, la privacidad de datos, la propiedad intelectual, el secreto comercial, el fraude, los derechos de interpretación musical, en el país o territorio en el cual se utiliza el producto de Avaya.

Prevención del fraude telefónico

El “fraude telefónico” se refiere al uso no autorizado de su sistema de telecomunicaciones por parte de un participante sin autorización (por ejemplo, una persona que no es un empleado, agente ni subcontratista corporativo o una persona que no trabaja en nombre de su compañía). Tenga en cuenta que pueden existir riesgos de Fraude telefónico asociados con su sistema y que, en tal caso, esto puede generar cargos adicionales considerables para sus servicios de telecomunicaciones.

Intervención en fraude telefónico de Avaya

Si sospecha que Usted está siendo victima de fraude telefónico y necesita asistencia o soporte técnico, comuníquese con su representante de ventas de Avaya.

Vulnerabilidades de seguridad

Puede encontrar información sobre las políticas de respaldo de seguridad de Avaya en la sección de Soporte técnico y políticas de seguridad de https://support.avaya.com/security.

Las sospechas de vulnerabilidades de la seguridad de productos de Avaya se manejan a través del Flujo de soporte técnico de seguridad de productos de Avaya (https://support.avaya.com/css/P8/documents/100161515).

Marcas registradas

Las marcas comerciales, logotipos y marcas de servicio (“Marcas”) que aparecen en este sitio, la Documentación, los Servicios alojados y los productos proporcionados por Avaya son Marcas registradas o no registradas de Avaya, sus afiliados, licenciantes, proveedores y otros terceros. Los usuarios no tienen permiso para usar dichas Marcas sin previo consentimiento por escrito de Avaya o dichos terceros que puedan ser propietarios de la Marca. Ningún contenido de este sitio, la Documentación, los Servicios alojados ni los productos deben considerarse como otorgamiento, por implicación, impedimento o de alguna otra forma, una licencia o derecho para usar las Marcas sin la autorización expresa por escrito de Avaya o del tercero correspondiente.

Avaya es una marca registrada de Avaya LLC.

Todas las demás marcas que no pertenecen a Avaya son propiedad de sus respectivos dueños.

Linux® es una marca comercial registrada de Linus Torvalds en EE. UU. y en otros países.

Descarga de documentación

Para obtener las versiones más actualizadas de la Documentación, visite el sitio web del Soporte técnico de Avaya: https://support.avaya.com o el sitio web posterior designado por Avaya.

Contacto con el soporte técnico de Avaya

Visite el sitio web del Soporte técnico de Avaya: https://support.avaya.com para obtener avisos y artículos sobre Productos o Servicios en la nube o para informar acerca de algún problema con su Producto o Servicio en la nube de Avaya. Para obtener una lista de los números de teléfono y las direcciones de contacto del soporte técnico, visite el sitio web del Soporte técnico de Avaya: https://support.avaya.com (o el sitio web posterior designado por Avaya); desplácese hasta la parte inferior de la página y seleccione Contacto con el Soporte técnico de Avaya.

Contenido

Parte 1: Compatibilidad con extensiones SIP remotas 6

Capítulo 1: Compatibilidad con extensiones SIP remotas en IP Office 7

Esquema de ejemplo 7

Consideraciones de seguridad 9

Capítulo 2: Configuración IP Office para extensiones SIP remotas 10

Lista de verificación de la configuración de IP Office 10

Licencias y suscripciones 11

Configuración de SIP VoIP de IP Office 11

Configurar los detalles del ASBCE transmitidos a extensiones remotas por el IP Office 13

Agregar configuración adicional para extensiones remotas 15

Lista blanca del ASBCE 16

Capítulo 3: Agregar certificados de IP Office al ASBCE 17

Lista de verificación del certificado ASBCE 17

Descarga del certificado raíz de IP Office 18

Agregar el certificado raíz de IP Office al ASBCE 19

Generación de un certificado de identidad de ASBCE usando IP Office Web Manager 20

Generación de un certificado de identidad de ASBCE usando Web Control (vista de plataforma) 21

División del certificado de identidad del ASBCE 22

Agregar el certificado de identidad al ASBCE 23

Capítulo 4: Configuración de ASBCE para extensiones SIP remotas 25

Resumen de flujo de llamadas de ASBCE 26

Clonar vs. Agregar 28

Lista de verificación de la configuración de ASBCE 28

Configuración de firewall 30

Configurar la interfaz de ASBCE externa 31

Configurar la interfaz de ASBCE interna 32

Creación de un perfil de cliente TLS 34

Creación de un perfil de servidor TLS 35

Creación de una interfaz de medios interna 37

Creación de una interfaz de medios externa 38

Creación de una interfaz de señalización interna 39

Creación de la interfaz de señalización externa 40

Creación de un perfil de servidor de ASBCE para el IP Office 41

Creación de un perfil de enrutamiento del servidor 43

Creación de una política de ocultamiento de topología de ASBCE 44

Creación de una lista de bloqueo de IP/URI 45

Creación de una regla de aplicación 46

Creación de una regla de medios 47

Creación de un grupo de políticas de terminal 50

Configuración de un perfil de agentes de usuario 51

Creación del flujo de suscriptor 52

Creación de un flujo de servidor ... 55
Agregar proxys inversos para solicitudes de archivos ... 57
Capítulo 5: Anulación de anclaje de medios de llamada desde el ASBCE ... 62
Creación de una política de sesión para un sitio remoto ... 62
Creación de un flujo de sesión para el sitio remoto ... 64
Capítulo 6: Compatibilidad con Client Avaya Workplace como extensión remota ... 66
Registro SIP de Client Avaya Workplace ... 66
Verificación de la configuración remota ... 67
Capítulo 7: Verificación del estado de la extensión remota en el ASBCE ... 69
Visualización de estadísticas SIP del ASBCE ... 69
Visualización de estadísticas de usuario de ASBCE ... 70
Visualización de incidentes de ASBCE ... 71
Parte 2: Compatibilidad con IPv6 ... 72
Capítulo 8: Compatibilidad con extensiones remotas IPv6 ... 73
Compatibilidad con extensión remota IPv6 ... 73
Esquema de extensión remota IPv6 ... 74
Limitaciones de extensión remota IPv6 ... 74
Configuración DNS para compatibilidad con extensiones remotas IPv6 ... 75
Configuración de certificado para compatibilidad con extensiones remotas IPv6 ... 75
Configuración de Avaya Spaces para compatibilidad con extensiones remotas IPv6 ... 76
Lista de verificación de configuración para extensiones remotas IPv6 ... 76
Lista de verificación de configuración para extensiones remotas IPv4 e IPv6 combinadas ... 77
Parte 3: Resiliencia ... 80
Capítulo 9: Resiliencia de ASBCE y IP Office ... 81
Ejemplo de esquema de resiliencia ... 81
Generación de un certificado de identidad para el IP Office secundario ... 82
Instalación del certificado de identidad de IP Office secundario ... 83
Configuración de IP Office para resiliencia de extensión remota ... 84
Configuración del Avaya one-X Portal ... 84
Configuración del ASBCE para resiliencia ... 85
Configuración de DNS para resiliencia ... 85
Capítulo 10: Verificación de la configuración de resiliencia ... 86
Verificación del enrutamiento DNS de resiliencia ... 86
Visualización del seguimiento del ASBCE ... 87
Verificación de las respuestas de Avaya one-X Portal ... 88
Parte 4: Información adicional ... 90
Capítulo 11: Ayuda y documentación adicionales ... 91
Manuales y guías de usuario adicionales ... 91
Obteniendo ayuda ... 91
Buscar un socio comercial de Avaya ... 92
Recursos adicionales de IP Office ... 92
Capacitación ... 93
Capítulo 12: Glosario ... 94

Parte 1: Compatibilidad con extensiones SIP remotas

Capítulo 1: Compatibilidad con extensiones SIP remotas en IP Office

Esta sección proporciona un proceso de ejemplo para admitir extensiones SIP remotas que se conectan a un IP Office a un Avaya Session Border Controller (ASBCE). El ASBCE proporciona una gama de funciones que proporcionan seguridad adicional al proceso de conexión.

- Este documento se basa en IP Office R11.1.3.1 y ASBCE R10.1.2.
- Para IP Office R11.1.3.1, IP Office admite extensiones Client Avaya Workplace remotas iOS y Android IPv6 usando IPv6. De lo contrario, IP Office solo admite extensiones remotas IPv4.

Extensiones SIP remotas compatibles

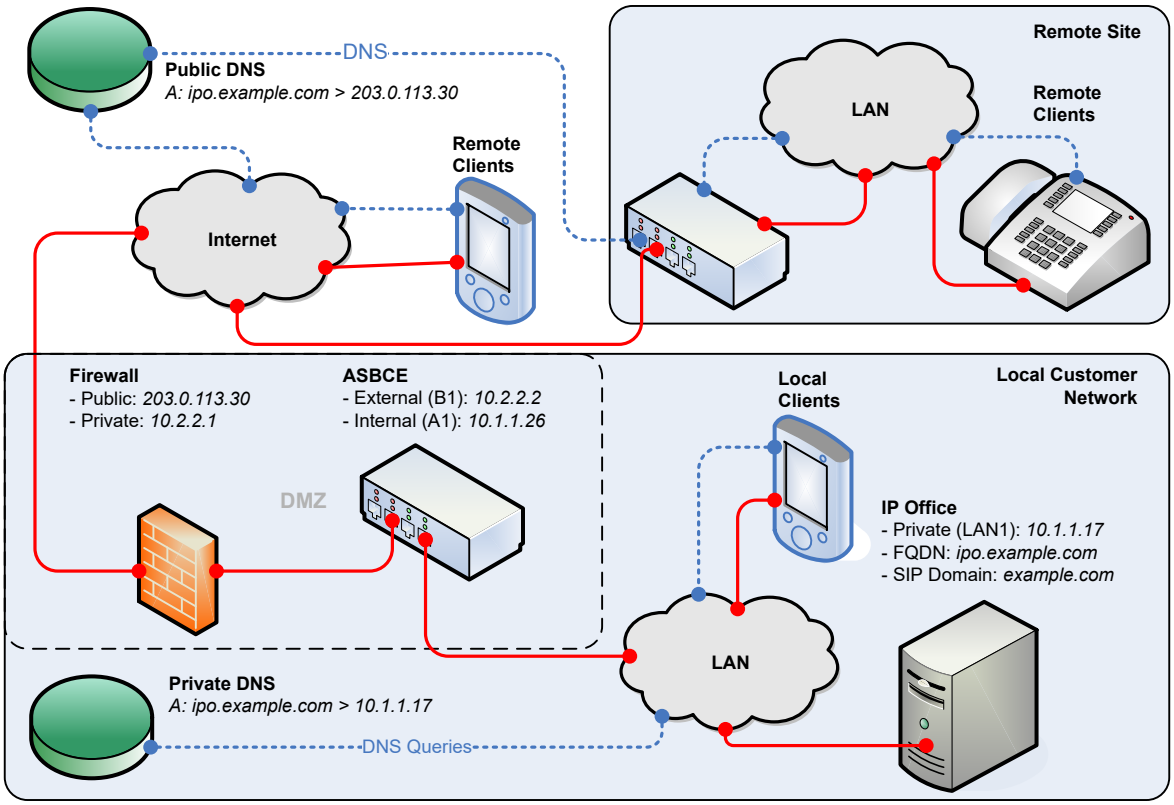
Teléfonos de escritorio SIP	Softphones SIP
• Teléfonos de la serie J100 • Teléfonos de la serie K100 (Avaya Vantage™)	• Client Avaya Workplace

Vínculos relacionados

Esquema de ejemplo en la página 7
Consideraciones de seguridad en la página 9

Esquema de ejemplo

Este esquema muestra el escenario de ejemplo utilizado en este documento:



- Para este escenario, las extensiones SIP son teléfonos J100 y softphones Client Avaya Workplace.
- IP Office es el registrador SIP.
  - Este ejemplo utiliza TLS para las conexiones SIP. Esto requiere la consideración de los certificados de IP Office y la provisión de certificados para el ASBCE.
- El ASBCE tiene interfaces IP públicas y privadas. Con estos, actúa como puerta de enlace para el tráfico SIP entre la red privada del cliente y la Internet pública.
  - Cuando se utilizan internamente, los clientes SIP se conectan directamente a IP Office.
  - Cuando se utilizan externamente, los clientes SIP se conectan a IP Office través del ASBCE.
  - El ASBCE también enruta solicitudes para archivos utilizados por las extensiones SIP remotas. Por ejemplo, solicitudes para los archivos `.txt` y `.xml`.
- La red del cliente incluye un firewall entre esta y la Internet pública. Avaya recomienda esto para mejorar la seguridad.
  - El firewall reenvía el tráfico de extensiones remotas al ASBCE.
- La solución DNS del cliente proporciona DNS de división. Es decir:
  - En la red privada del cliente, DNS resuelve el FQDN de IP Office a la dirección IP de IP Office.
  - En la Internet pública, DNS resuelve el FQDN de IP Office a la dirección IP pública del firewall del cliente.

Vínculos relacionados

Compatibilidad con extensiones SIP remotas en IP Office en la página 7

Consideraciones de seguridad

Cualquier escenario en el que conecte IP Office a la Internet pública debe incluir la consideración de la seguridad. Las opciones y requisitos de seguridad de IP Office se cubren en el manual Avaya Pautas de seguridad de IP Office™ Platform.

En este caso, la conexión mediante un ASBCE pone a disposición una gama de opciones de seguridad adicionales.

- **Coincidencia de agente de usuario**

  Puede configurar qué cadenas de agentes de usuario pueden conectarse a través del ASBCE. Esto le permite admitir únicamente conexiones de aplicaciones y dispositivos conocidos. Vea Configuración de un perfil de agentes de usuario en la página 51.

- **Reglas de aplicación**

  Puede utilizar reglas de aplicación para configurar qué tipo de medios admiten sus conexiones, el número máximo de conexiones y el número máximo de conexiones por extensión remota. Vea Creación de una regla de aplicación en la página 46.

- **Listas de bloqueo de IP/URL**

  Puede utilizarlos para bloquear direcciones IP o URL que fallan repetidamente en el registro de nombre de usuario o contraseña. Vea Creación de una lista de bloqueo de IP/URI en la página 45.

Vínculos relacionados

Compatibilidad con extensiones SIP remotas en IP Office en la página 7

Capítulo 2: Configuración IP Office para extensiones SIP remotas

Esta sección proporciona un resumen general de la configuración IP Office para admitir la conexión de extensiones SIP remotas a través de un ASBCE.

Vínculos relacionados

Lista de verificación de la configuración de IP Office en la página 10
Licencias y suscripciones en la página 11
Configuración de SIP VoIP de IP Office en la página 11
Configurar los detalles del ASBCE transmitidos a extensiones remotas por el IP Office en la página 13
Agregar configuración adicional para extensiones remotas en la página 15
Lista blanca del ASBCE en la página 16

Lista de verificación de la configuración de IP Office

#	Acción	Vínculo/notas	✔
1.	Verifique la configuración de SIP VoIP	Vea Configuración de SIP VoIP de IP Office en la página 11.	
2.	Agregar configuración para extensiones remotas	Vea Configurar los detalles del ASBCE transmitidos a extensiones remotas por el IP Office en la página 13.	
3.	Configure los números de origen NoUser	Vea Agregar configuración adicional para extensiones remotas en la página 15.	
4.	Lista blanca del ASBCE	Evite que IP Office bloquee el ASBCE. Vea Lista blanca del ASBCE en la página 16.	

Vínculos relacionados

Configuración IP Office para extensiones SIP remotas en la página 10

Licencias y suscripciones

IP Office no requiere ninguna licencia adicional para admitir la operación con un ASBCE. Los teléfonos y las aplicaciones conectados a IP Office usando un ASBCE utilizan las mismas licencias o suscripciones que para el funcionamiento local.

Vínculos relacionados

Configuración IP Office para extensiones SIP remotas en la página 10

Configuración de SIP VoIP de IP Office

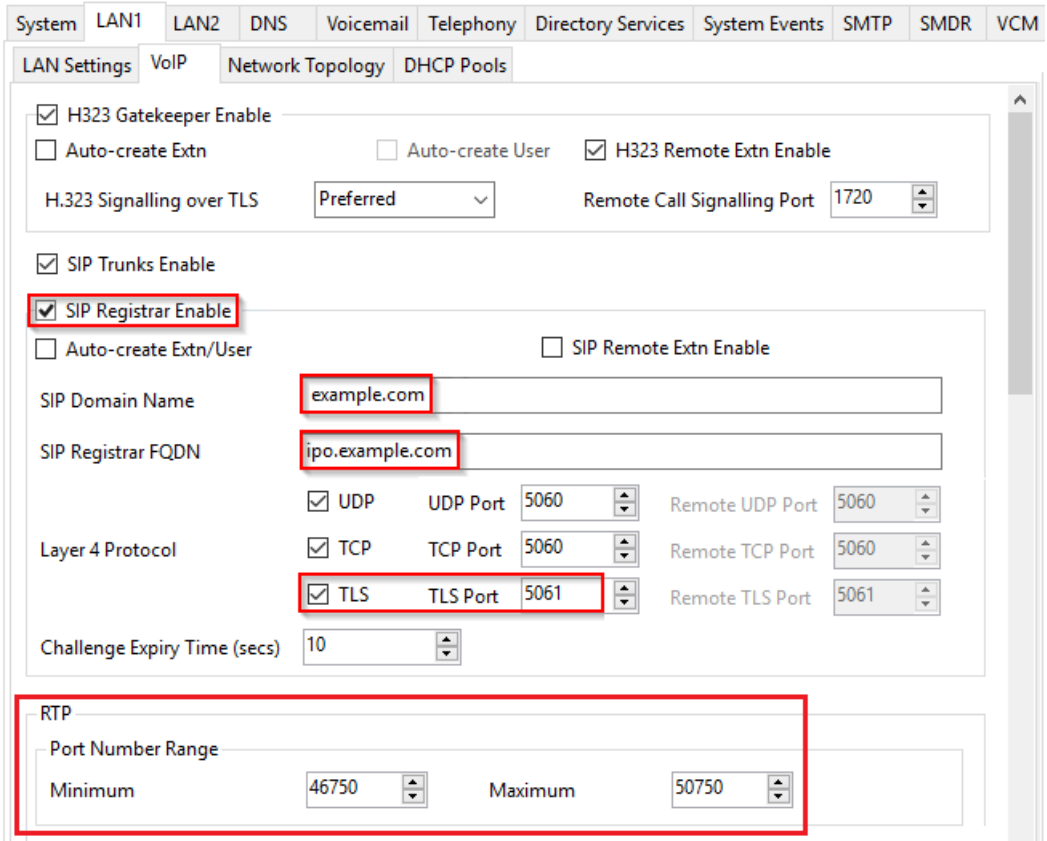
La siguiente es la configuración de IP Office utilizada para admitir extensiones SIP en el escenario de ejemplo. Esta configuración es la misma para extensiones SIP locales y remotas.

Importante:

- Al cambiar esta configuración, se debe reiniciar el sistema IP Office.

Procedimiento

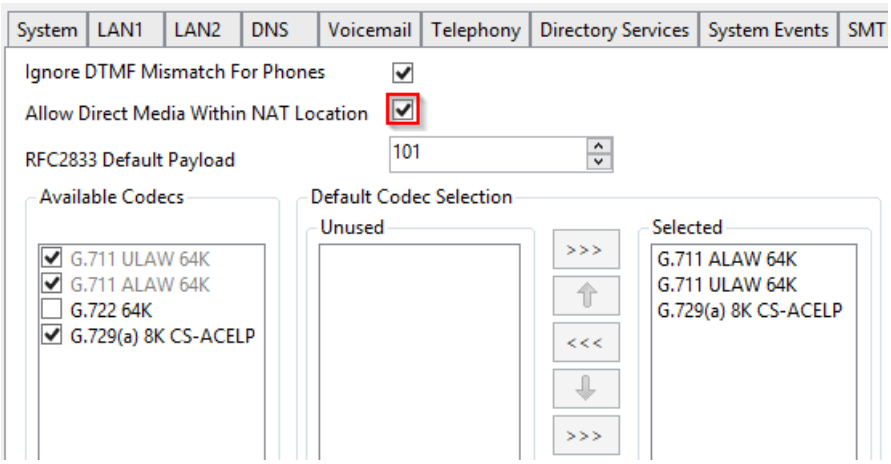
1. Inicie sesión en IP Office con IP Office Manager o IP Office Web Manager.
2. Seleccione **Sistema** o **Configuración del sistema** > **Sistema**.
3. Seleccione la pestaña **LAN1**.



Campo	Descripción
Habilitar registrador SIP	Permite que las extensiones SIP se registren en IP Office.
Habilitar extensión remota SIP	Deshabilitar. El ASBCE administra conexiones NAT de extensión remota.
Nombre de dominio SIP	Establece el dominio que los clientes SIP deben utilizar para el registro.
FQDN de registrador SIP	Establece el nombre de dominio completo para enrutar conexiones SIP a IP Office.
Protocolo de capa 4	Establece los protocolos y puertos de capa 4 en los que IP Office escucha el tráfico de extensiones SIP.
Rango de número de puerto	Establece el rango de números de puerto que IP Office utiliza para el tráfico RTP y RTCP.

4. Seleccione la subpestaña **VoIP**.

   Habilite la casilla de verificación **Permitir medios directos con Localización NAT**.



   - Al habilitar esto, los medios directos entre dispositivos que residen en la misma subred que se conecta a IP Office usando NAT. Para admitir esto a través del ASBCE se requiere una configuración adicional para que el ASBCE se desancle de los medios de llamada. Consulte Anulación de anclaje de medios de llamada desde el ASBCE en la página 62.

5. Haga clic en **Aceptar** o **Actualizar**.
6. Guarde la configuración y reinicie el sistema IP Office:
   - Si utiliza IP Office Manager, guarde la configuración y reinicie el sistema.
   - Si utiliza IP Office Web Manager, haga clic en **Guardar en IP Office** y reinicie el sistema.

Vínculos relacionados

Configuración IP Office para extensiones SIP remotas en la página 10

Configurar los detalles del ASBCE transmitidos a extensiones remotas por el IP Office

Antes de registrarse con IP Office, las extensiones de Avaya solicitan el archivo `46xxsettings.txt`. Este archivo contiene la configuración que utilizan las extensiones.

Para extensiones remotas, el archivo `46xxsettings.txt` generado automáticamente por IP Office debe contener la información de direcciones que la extensión remota puede utilizar para conectarse al ASBCE.

- Las extensiones solicitan el archivo `46xxsettings.txt` cuando se registran por primera vez en IP Office.
- Después de recibir el archivo `46xxsettings.txt`, las extensiones predeterminadas solicitan el archivo nuevamente cada 24 horas para aplicar cualquier cambio.
- Las extensiones también solicitan el archivo cada vez que se reinician. Puede reiniciarlos de manera remota usando SysMonitor o System Status Application.

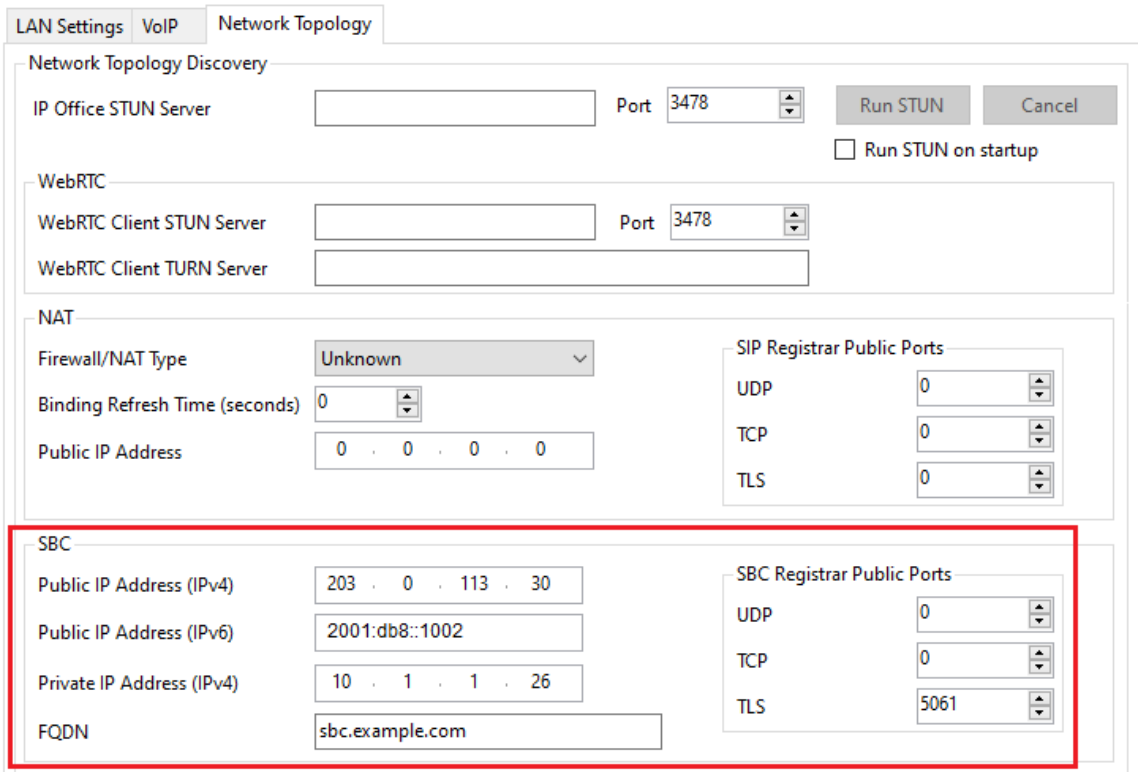
Importante:

- Al cambiar esta configuración, se debe reiniciar el sistema IP Office.

Procedimiento

1. Inicie sesión en IP Office con IP Office Manager o IP Office Web Manager.
2. Seleccione **Sistema** o **Configuración del sistema** > **Sistema**.
3. Seleccione la LAN (**LAN1** o **LAN2**) conectada a la misma red que el ASBCE.
4. Seleccione **Topología de red**.
   - Si utiliza IP Office Web Manager, solo puede cambiar esta configuración en modo desconectado. Haga clic en el ícono y seleccione **Modo desconectado**.

5. En la sección **SBC**, ingrese la siguiente información:



Configuración	Descripción
Dirección IP pública (IPv4)	La dirección IPv4 pública para el tráfico entrante del cliente SIP en la red del cliente. • Esta es la dirección IPv4 pública del ASBCE o del servicio de Internet, como el firewall del cliente. • DNS externo debe resolver el FQDN de IP Office a esta dirección cuando lo solicite una extensión remota IPv4.
Dirección IP pública (IPv6)	La dirección IPv6 pública para el tráfico entrante del cliente SIP a la red del cliente como se mencionó anteriormente. Para obtener más información, consulte Compatibilidad con extensiones remotas IPv6 en la página 73. • Esta es la dirección IPv6 pública del ASBCE o del servicio de Internet, como el firewall del cliente. • DNS externo debe resolver el FQDN de IP Office a esta dirección cuando lo solicite una extensión remota IPv6.
Dirección IP privada (IPv4)	La dirección IPv4 privada/interna del ASBCE. • DNS interno debe resolver el **FQDN** abajo a esta dirección.
FQDN	El nombre de dominio completo del ASBCE. DNS debe resolver este FQDN a las direcciones IPv6 que se utilizan (IPv4 utiliza el FQDN de registrador SIP de IP Office).
Puertos públicos de registrador SIP	Los puertos públicos (externos) **UDP**, **TCP** y/o **TLS** que los clientes SIP externos deben utilizar para conectarse al ASBCE.

6. Haga clic en **Aceptar** o **Actualizar**.
7. Guarde la configuración y reinicie el sistema IP Office:
   - Si utiliza IP Office Manager, guarde la configuración y reinicie el sistema.

- Si utiliza IP Office Web Manager, haga clic en **Guardar en IP Office** y reinicie el sistema.

Vínculos relacionados

Configuración IP Office para extensiones SIP remotas en la página 10

Agregar configuración adicional para extensiones remotas

Puede utilizar los siguientes números de origen **NoUser** para tener valores adicionales establecidos en el archivo `46xxsettings.txt` generado automáticamente que IP Office suministra a extensiones remotas.

Procedimiento

1. Inicie sesión en IP Office con IP Office Manager o IP Office Web Manager.
2. Haga clic en **Usuario** o **Administración de llamadas** > **Usuario**.
3. Ubique la configuración para el usuario llamado *NoUser*.
4. Seleccione **Números de origen**.
5. Agregue los números de origen *NoUser* adicionales requeridos:
   - **SET_STIMULUS_SBC_REG_INTERVAL=**`<seconds>`

     Este número de origen *NoUser* establece el intervalo de registro utilizado por los teléfonos de la serie J100. El valor predeterminado es de 3600 segundos (1 hora). Cuando se admiten teléfonos a través de un ASBCE, el valor recomendado es 180 segundos. El rango admitido es de 180 a 3600 segundos.
   - **PUBLIC_HTTP=**`<file server address>`

     Cuando utiliza la configuración de **Dirección IP del servidor HTTP** y **Redirección HTTP**, IP Office utiliza este valor para configurar la dirección del servidor de archivos público dada a extensiones remotas.
6. Haga clic en **Aceptar** o **Actualizar**.
7. Guarde la configuración y reinicie el sistema IP Office:
   - Si utiliza IP Office Manager, guarde la configuración y reinicie el sistema.
   - Si utiliza IP Office Web Manager, haga clic en **Guardar en IP Office** y reinicie el sistema.

Vínculos relacionados

Configuración IP Office para extensiones SIP remotas en la página 10

Lista blanca del ASBCE

Con la extensión remota conectada a IP Office a través del ASBCE, los intentos de registro incorrectos pueden hacer que IP Office bloquee la dirección IP del ASBCE.

Procedimiento

1. Inicie sesión en IP Office con IP Office Manager o IP Office Web Manager.
2. Seleccione **Sistema** o **Configuración del sistema** > **Sistema**.
3. Seleccione **VoIP** > **Listas de control de acceso**.
4. Agregue la dirección IP interna del ASBCE al **Lista blanca de IP**.
5. Haga clic en **Aceptar** o **Actualizar**.
6. Si utiliza IP Office Manager, guarde la configuración en el sistema de IP Office.

Vínculos relacionados

Configuración IP Office para extensiones SIP remotas en la página 10

Capítulo 3: Agregar certificados de IP Office al ASBCE

Para el escenario de ejemplo, IP Office está usando su certificado autofirmado. En ese caso, el ASBCE requiere:

- Una copia del certificado raíz de IP Office. Esta es la Autoridad de certificado (Certificate Authority, CA).
- Un certificado de identidad para el ASBCE emitido por IP Office.
  - **Para IPv4:** el certificado debe incluir el FQDN de IP Office (CN o SAN) y la dirección IPv4 (SAN).
  - **Para IPv6:** además del FQDN de IP Office y la dirección IPv4, el certificado de identidad del ASBCE debe incluir el FQDN del ASBCE y la dirección IPv6.

Uso de certificados de terceros

Si IP Office utiliza certificados emitidos por una CA de terceros, entonces esa CA debe emitir los certificados raíz e identidad requeridos por el ASBCE. Sin embargo, los principios para los detalles requeridos en el certificado de identidad siguen siendo los mismos que se describen en esta sección de la documentación.

Vínculos relacionados

Lista de verificación del certificado ASBCE en la página 17
Descarga del certificado raíz de IP Office en la página 18
Agregar el certificado raíz de IP Office al ASBCE en la página 19
Generación de un certificado de identidad de ASBCE usando IP Office Web Manager en la página 20
Generación de un certificado de identidad de ASBCE usando Web Control (vista de plataforma) en la página 21
División del certificado de identidad del ASBCE en la página 22
Agregar el certificado de identidad al ASBCE en la página 23

Lista de verificación del certificado ASBCE

#	Acción	Vínculo/notas	✔
1.	Descargue el certificado raíz de IP Office	Vea Descarga del certificado raíz de IP Office en la página 18.	

La tabla continúa…

#	Acción	Vínculo/notas	✔
2.	Agregue el certificado raíz al ASBCE	Vea Agregar el certificado raíz de IP Office al ASBCE en la página 19.	
3.	Generar un certificado de identidad para el ASBCE	Vea Generación de un certificado de identidad de ASBCE usando IP Office Web Manager en la página 20.	
4.	Dividir el certificado	Extraiga archivos de certificado y clave privada separados del certificado de identidad. Vea División del certificado de identidad del ASBCE en la página 22.	
5.	Agregue los archivos al ASBCE	Agregue el certificado de identidad y los archivos de clave privada al ASBCE Vea Agregar el certificado de identidad al ASBCE en la página 23.	

Vínculos relacionados

Agregar certificados de IP Office al ASBCE en la página 17

Descarga del certificado raíz de IP Office

Siga este procedimiento para descargar una copia del certificado raíz IP Office.

Procedimiento

1. Inicie sesión en IP Office con IP Office Web Manager.
   - Para un IP500 V2, ingrese la dirección del sistema seguida de `:8443/WebMgmtEE/WebManagerment.html`.
   - Para un servidor basado en Linux, ingrese la dirección del sistema seguida de `:7070/WebManagement/WebManagement.html`.
2. Seleccione **Seguridad** > **Configuración de seguridad**.
3. Si IP Office está en una red multisitio, haga clic en junto al correspondiente IP Office.
4. Seleccione **Certificados**.
5. En **Tienda de certificado de confianza**, ubique el certificado raíz que utiliza el sistema IP Office.
6. Haga clic en junto al certificado.
7. Haga clic en **Sí**.
8. Cambie el nombre del archivo `IPO_RootCA.crt`.

Pasos siguientes

- Vaya a Agregar el certificado raíz de IP Office al ASBCE en la página 19.

Vínculos relacionados

Agregar certificados de IP Office al ASBCE en la página 17

Agregar el certificado raíz de IP Office al ASBCE

Siga este procedimiento para cargar la copia del certificado raíz de IP Office al ASBCE.

Antes de empezar

- Descargue el certificado raíz de IP Office. Vea Descarga del certificado raíz de IP Office en la página 18.

Procedimiento

1. Vaya a **Administración de TLS** > **Certificados**.
2. Haga clic en **Instalar**.
3. Establezca **Tipo** en **Certificado CA**.
4. Ingrese un nombre descriptivo para el certificado.
5. Habilite **Permitir certificado débil/clave**.
6. Haga clic en **Elegir archivo** y seleccione el archivo `IPO_RootCA.crt`.
7. Haga clic en **Cargar**. El menú muestra una advertencia de que este es un certificado autofirmado.
8. Haga clic en **Continuar**. El menú muestra el certificado.
9. Haga clic en **Instalar**.
10. Haga clic en **Terminar**.

Pasos siguientes

- Utilice IP Office para crear un certificado de identidad para el ASBCE:
  - Para sistemas de suscripción, consulte Generación de un certificado de identidad de ASBCE usando IP Office Web Manager en la página 20.
  - Para otros sistemas, consulte Generación de un certificado de identidad de ASBCE usando Web Control (vista de plataforma) en la página 21.

Vínculos relacionados

Agregar certificados de IP Office al ASBCE en la página 17

Generación de un certificado de identidad de ASBCE usando IP Office Web Manager

Este proceso genera un certificado de identidad para el ASBCE usando IP Office Web Manager.

- Este proceso es para sistemas IP Office en modo de suscripción que utilizan **Administración automática de certificados** . Para otros sistemas, consulte Generación de un certificado de identidad de ASBCE usando Web Control (vista de plataforma) en la página 21.

Procedimiento

1. Inicie sesión en el sistema con IP Office Web Manager.
   - Para un IP500 V2, ingrese la dirección del sistema seguida de `:8443/WebMgmtEE/WebManagerment.html`.
   - Para un servidor basado en Linux, ingrese la dirección del sistema seguida de `:7070/WebManagement/WebManagement.html`.
2. Seleccione **Seguridad** > **Configuración de seguridad**.
3. Si IP Office está en una red multisitio, haga clic en junto al correspondiente IP Office.
4. Seleccione **Certificados**.
5. Haga clic en **Regenerar**.
6. Seleccione **Crear certificado para una máquina diferente**.
7. En **Nombre de asunto**, ingrese el FQDN del ASBCE.
8. En **Nombre(s) alternativos de asunto**, ingrese cualquier valor adicional para otros servidores y servicios a los que el ASBCE necesita conectarse.
   - **Para IPv4:** el certificado debe incluir la dirección FQDN e IPv4 de IP Office.
   - **Para IPv6:** además del FQDN de IP Office y la dirección IPv4, el certificado de identidad del ASBCE debe incluir el FQDN del ASBCE y la dirección IPv6.
   - Utilice valores separados por comas para las entradas *DNS:<FQDN>* y *IP:<IP address>* requeridas.
   - Si utiliza diferentes FQDN para el dominio Avaya one-X® Portal XMPP, ingrese todos los FQDN como una lista separada por comas de entradas DNS.
9. Haga clic en **Aceptar**. Espere hasta un minuto mientras IP Office genera el certificado.
10. Cuando se le solicite, configure una contraseña de cifrado para el certificado de identidad y haga clic en **Sí** .
11. El navegador le pedirá que descargue y guarde el archivo de certificado.
12. Cambie el nombre del archivo descargado a `SBCE_ID.p12`.

Pasos siguientes

- Vea División del certificado de identidad del ASBCE en la página 22.

Vínculos relacionados

Agregar certificados de IP Office al ASBCE en la página 17

Generación de un certificado de identidad de ASBCE usando Web Control (vista de plataforma)

Este proceso genera un certificado de identidad para el ASBCE usando los menús de Web Control del servidor de IP Office.

Procedimiento

1. Inicie sesión en los menús de IP Office Web Control de la siguiente manera:
   - Desde dentro de IP Office Web Manager, seleccione el servidor primario. Haga clic en ☰ y seleccione **Vista de plataforma**.
   - Navegue hasta `https://<IP Office IP address>:7071` e inicie sesión.
2. Seleccione la pestaña **Configuración** y desplácese hacia abajo hasta **Certificados**.
3. Seleccione **Crear certificado para una máquina diferente**.
4. Introduzca los siguientes datos:
5. En **IP de máquina**, ingrese la dirección IP externa del ASBCE.
6. En **Contraseña**, ingrese una contraseña para cifrar el certificado y la clave.
7. En **Nombre de asunto**, ingrese el FQDN del ASBCE.
8. En **Nombre(s) alternativos de asunto**, ingrese cualquier valor adicional para otros servidores y servicios a los que el ASBCE necesita conectarse.
   - **Para IPv4:** el certificado debe incluir la dirección FQDN e IPv4 de IP Office.
   - **Para IPv6:** además del FQDN de IP Office y la dirección IPv4, el certificado de identidad del ASBCE debe incluir el FQDN del ASBCE y la dirección IPv6.
   - Utilice valores separados por comas para las entradas *DNS:<FQDN>* y *IP:<IP address>* requeridas.
   - Si utiliza diferentes FQDN para el dominio Avaya one-X® Portal XMPP, ingrese todos los FQDN como una lista separada por comas de entradas DNS.
9. Haga clic en **Regenerar**.
10. Haga clic en el enlace en la ventana emergente y guarde el archivo.
11. Cambie el nombre del archivo descargado a `SBCE_ID.p12`.

Pasos siguientes

- Vea División del certificado de identidad del ASBCE en la página 22.

Vínculos relacionados

Agregar certificados de IP Office al ASBCE en la página 17

División del certificado de identidad del ASBCE

El certificado de identidad creado para el ASBCE por IP Office es un solo archivo. Contiene el certificado y la clave privada. Para la configuración del ASBCE, debe dividir el certificado de identidad en certificados separados y archivos de clave privada.

Antes de empezar

- Utilice IP Office para crear un certificado de identidad para el ASBCE:
  - Para sistemas de suscripción, consulte Generación de un certificado de identidad de ASBCE usando IP Office Web Manager en la página 20.
  - Para otros sistemas, consulte Generación de un certificado de identidad de ASBCE usando Web Control (vista de plataforma) en la página 21.

Procedimiento

1. Con WinSCP, conéctese a la dirección IP de administración del ASBCE usando el puerto 222 y el inicio de sesión de ipcs.
2. Copie el certificado de identidad de IP Office creado para el ASBCE (`SBCE_ID.p12`) en el directorio ASBCE **`/home/ipcs`**.
3. SSH a la IP de administración del ASBCE usando el puerto 222 e inicio de sesión de ipcs.
4. Ingrese el comando **su root** o **su -root** y escriba la contraseña raíz del ASBCE.
5. Ingrese los siguientes comandos. El comando que se utilizará depende de si generó el certificado usando los menús de IP Office Web Manager o de Web Control (vista de plataforma).

   Nota:

   - Cuando se le solicite una contraseña o frase de contraseña PEM, ingrese la contraseña especificada cuando genere el certificado de identidad para el ASBCE.
   - Si la contraseña incluye caracteres especiales, debe anteponerles `\` cuando los ingresa en la línea de comandos. Por ejemplo, en la línea de comandos, ingrese un `@` en la contraseña como `\@`.

   - **Certificado de IP Office Web Control:**

     Siga los siguientes pasos con un certificado generado usando los menús de IP Office Web Control.

     ```
     openssl pkcs12 -in SBCE_ID.p12 -out SBCE_ID.crt -nokeys -clcerts
     openssl pkcs12 -in SBCE_ID.p12 -out SBCE_ID.key -nocerts
     ```

   - **Certificado de IP Office Web Manager:**

     Siga los siguientes pasos con un certificado generado usando IP Office Web Manager.

     ```
     openssl enc -base64 -d -in SBCE_ID.p12 -out SBCE_ID_BIN.p12 -A
     openssl pkcs12 -in SBCE_ID_BIN.p12 -out SBCE_ID.crt -nokeys -clcerts
     openssl pkcs12 -in SBCE_ID_BIN.p12 -out SBCE_ID.key -nocerts
     ```

6. Copie los archivos `SBCE_ID.crt` y `SBCE_ID.key` nuevos desde el ASBCE a su PC

7. El archivo `SBCE_ID.crt` aún contiene el certificado CA raíz de IP Office, la clave privada y el certificado de Id. de ASBCE. Para poder importar el archivo al ASBCE, debe eliminar el certificado CA y la clave privada del archivo.
   a. Abra `SBCE_ID.crt` en WordPad en su PC.
   b. Elimine todas las líneas excepto las que están entre las primeras líneas **BEGIN CERTIFICATE** y **END CERTIFICATE**. Por ejemplo:

```
-----BEGIN CERTIFICATE-----
MIIEYjCCA0qgAwIBAgIGYCZWOINgMA0GCSqGSIb3DQEBCwUAMIGtMQswCQYDVQQG
EwJVUzETMBEGA1UECAwKTmV3IEplcnNleTEWMBQGA1UEBwwNQmFza2luZyBSaWRn
ZTESMBAGA1UECgwJQXZheWEgSW5jMQwwCgYDVQQLDANHQ1MxLTArBgNVBAMMJGlw
b2ZmaWNlLXJvb3QtMDAwQzI5RDJDRTQ2LmF2YXlhLmNvbTEgMB4GCSqGSIb3DQEJ
ARYRc3VwcG9ydEBhdmF5YS5jb20wHhcNMTUxMjA5MTMyNTQ5WhcNMjIxMjA5MTIy
NTQ5WjCBlzELMAkGA1UEBhMCVVMxEzARBgNVBAgMCk5ldyBKZXJzZXkxFjAUBgNV
BAcMDUJhc2tpbmcgUmlkZ2UxEjAQBgNVBAoMCUF2YXlhIEluYzEMMAoGA1UECwwD
R0NTMRcwFQYDVQQDDA5zYmNlLmJ1bmR5LmNvbTEgMB4GCSqGSIb3DQEJARYRc3Vw
cG9ydEBhdmF5YS5jb20wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDE
XivTfA4Q/w/oMlnojSnOyE51Yzk3d84L1FPHtzfj6IZlfE3w0LAv/7uQl1AljRlc
diiZctJQw2puwnkdhsKzi+GQRaHzKoc+cb+tUhMRrrFBIvnnZ9yy0D1CW+iVp8z9
TO8Tce7G9vMgiRjRnZL7UfesqWigkuySpXMcDUKivlnTuYeOuP8znbu9620xrcCO
/w36qhOB2BcE3jGFn7Iv69hiol2ifHqAWhDcatwvQQahTf85Uka5hVoRetwdT9ys
mk1nnMJ913UyN8DlvXoqnWUav9rQVZKpnQMSOERw9w8n0sb5dXNOqxaV3G2zyHPq
psUHEYKc7bk2haooIvifAgMBAAGjgZswgZgwCQYDVR0TBAIwADALBgNVHQ8EBAMC
A/gwHwYDVR0RBBgwFoIOc2JjZS5idW5keS5jb22HBId88iIwHwYDVR0jBBgwFoAU
8AJiRrTa38gHJzRg4wpAX0Oc7SgwHQYDVR0OBBYEFApovB6QMB8amPZdmppIjaZ3
HO39MB0GA1UdJQQWMBQGCCsGAQUFBwMBBggrBgEFBQcDAjANBgkqhkiG9w0BAQsF
AAOCAQEAOG2tfwKeBPaLX0aef35pDzdPjck6qFnZwV3BQFHCz3C3P0RxcLXdC+us
tk/UH71440h8yVhCqLwkQmHuoDK+8ofmuHOlvhnGK8d+lWPWJwImLrIk5PI5ZsXC
4n/9ZKQzibeylfblRQpiCgAaT6L2lvQvZfuETAfSYk4TwZUdMja8JGYDIkNqHBNp
FPb+W1/cPimututLyJYRVCGpkM6bGfmpyMbS3JDGtYWhb7uq19XqlMdZAVWtL5a1
Bxe1kwNfsYIOQGPDiOO9nO1s+9i2pcIUQ1BchpA2yUphvtwS2KrNMhOkG3mcpWHB
9a2PMn1DMM3PXMfyRh9vL00fMRSNVA==
-----END CERTIFICATE-----
```

Pasos siguientes

- Vaya al Agregar el certificado de identidad al ASBCE en la página 23

Vínculos relacionados

Agregar certificados de IP Office al ASBCE en la página 17

Agregar el certificado de identidad al ASBCE

Siga este proceso para cargar el certificado de identidad al ASBCE.

Antes de empezar

- División del certificado de identidad del ASBCE en la página 22

Procedimiento

1. Vaya a **Administración de TLS** > **Certificados**.
2. Haga clic en **instalación**.
3. En **Tipo**, seleccione **Certificado**.
4. Ingrese un nombre descriptivo para el certificado.
5. Haga clic en **Elegir archivo** y seleccione el archivo `SBCE_ID.crt`.
6. Seleccione **Cargar archivo clave**.
7. Haga clic en **Elegir archivo** y seleccione el archivo `SBCE_ID.key`.
8. Haga clic en **Cargar**. El menú muestra el certificado.
9. Haga clic en **instalación**.

10. Haga clic en **Terminar**.
11. Con SSH, acceda a la dirección IP de administración del ASBCE usando el puerto 222 y el inicio de sesión de ipcs.
    a. Ingrese `su root` o `su -root` y la contraseña de raíz del ASBCE.
    b. Ingrese los siguientes comandos, reemplazando `********` con la contraseña establecida cuando genera el certificado de identidad:

    ```
    cd /usr/local/ipcs/cert/key
    enc_key SBCE_ID.key ********
    ```

    - Debe anteponer caracteres especiales en la contraseña con una `\`. Por ejemplo, para ingresar una `@`, escriba `\@`.

Vínculos relacionados

Agregar certificados de IP Office al ASBCE en la página 17

Capítulo 4: Configuración de ASBCE para extensiones SIP remotas

Esta sección analiza la configuración del ASBCE para enrutar llamadas SIP entre las extensiones remotas y IP Office.

- **Compatibilidad con IPv6:** para obtener detalles sobre la compatibilidad con extensiones remotas IPv6, consulte Compatibilidad con extensiones remotas IPv6 en la página 73.
  - **Si solo admite extensiones remotas IPv6:** siga el proceso de configuración en esta sección para IPv4, pero reemplace las direcciones IPv4 externas con direcciones IPv6 cuando corresponda.
  - **Si es compatible con extensiones remotas IPv4 e IPv6:** debe realizar pasos de configuración adicionales después de completar la configuración de IPv4. Vea Lista de verificación de configuración para extensiones remotas IPv4 e IPv6 combinadas en la página 77.

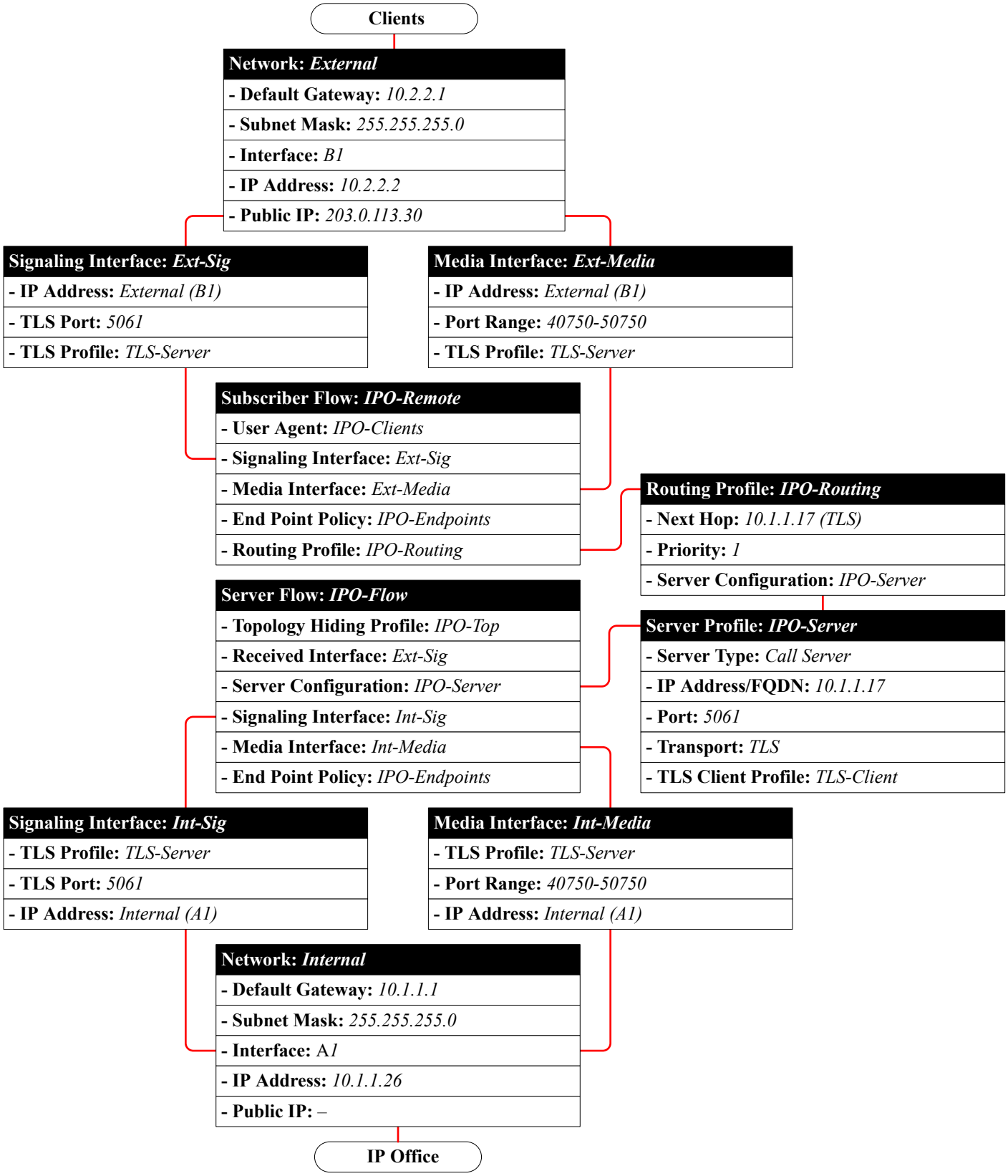
Vínculos relacionados

Resumen de flujo de llamadas de ASBCE en la página 26
Clonar vs. Agregar en la página 28
Lista de verificación de la configuración de ASBCE en la página 28
Configuración de firewall en la página 30
Configurar la interfaz de ASBCE externa en la página 31
Configurar la interfaz de ASBCE interna en la página 32
Creación de un perfil de cliente TLS en la página 34
Creación de un perfil de servidor TLS en la página 35
Creación de una interfaz de medios interna en la página 37
Creación de una interfaz de medios externa en la página 38
Creación de una interfaz de señalización interna en la página 39
Creación de la interfaz de señalización externa en la página 40
Creación de un perfil de servidor de ASBCE para el IP Office en la página 41
Creación de un perfil de enrutamiento del servidor en la página 43
Creación de una política de ocultamiento de topología de ASBCE en la página 44
Creación de una lista de bloqueo de IP/URI en la página 45
Creación de una regla de aplicación en la página 46
Creación de una regla de medios en la página 47
Creación de un grupo de políticas de terminal en la página 50
Configuración de un perfil de agentes de usuario en la página 51
Creación del flujo de suscriptor en la página 52
Creación de un flujo de servidor en la página 55

Agregar proxys inversos para solicitudes de archivos en la página 57

Resumen de flujo de llamadas de ASBCE

Esta imagen resume los componentes de configuración del ASBCE utilizados para la conexión entre las extensiones remotas IPv4 y IP Office.



Vínculos relacionados

Configuración de ASBCE para extensiones SIP remotas en la página 25

Clonar vs. Agregar

Importante:

Varios procesos en este documento le indican que cree nuevos elementos clonando una plantilla existente en lugar de agregar una nueva entrada. Es decir, hacer clic en **Clonar** en lugar de **Agregar**.

- Debe utilizar **Clonar** cuando se indica en un proceso y debe clonar el perfil existente indicado en las instrucciones.
- El uso de **Agregar** creará una nueva entrada que tiene una configuración predeterminada diferente del clon esperado. Esto provocará un funcionamiento incorrecto.

Vínculos relacionados

Configuración de ASBCE para extensiones SIP remotas en la página 25

Lista de verificación de la configuración de ASBCE

#	Acción	Vínculo/notas	✔
1.	Configurar reenvío de puertos de firewall	Enrutar tráfico externo desde los clientes al ASBCE. Vea Configuración de firewall en la página 30.	
2.	Configurar la interfaz de red de ASBCE externa	Configure las direcciones IP externas que utiliza el ASBCE. Vea Configurar la interfaz de ASBCE externa en la página 31.	
3.	Configure la interfaz de red de ASBCE interna.	Configure las direcciones IP internas que utiliza el ASBCE. Vea Configurar la interfaz de ASBCE interna en la página 32.	
4.	Crear un perfil de cliente TLS	Esto establece la configuración de TLS que utiliza ASBCE cuando se conecta al IP Office. Vea Creación de un perfil de cliente TLS en la página 34.	
5.	Crear un perfil de servidor TLS	Esto establece la configuración de TLS utilizada por el ASBCE cuando los clientes y IP Office se conectan a él. Vea Creación de un perfil de servidor TLS en la página 35.	
6.	Crear una interfaz de medios SIP interna	Defina los puertos y direcciones en los que el ASBCE escucha medios SIP desde IP Office. Vea Creación de una interfaz de señalización interna en la página 39.	

La tabla continúa…

#	Acción	Vínculo/notas	✔
7.	Crear una interfaz de medios SIP externa	Defina los puertos y direcciones en los que el ASBCE escucha medios SIP para las extensiones remotas. Vea Creación de la interfaz de señalización externa en la página 40.	
8.	Crear una interfaz de señalización SIP interna	Defina los puertos y direcciones en los que el ASBCE escucha la señalización de llamadas SIP desde IP Office. Vea Creación de una interfaz de señalización interna en la página 39.	
9.	Crear una interfaz de señalización SIP externa	Defina los puertos y direcciones en los que el ASBCE escucha la señalización de llamadas SIP desde las extensiones remotas. Vea Creación de la interfaz de señalización externa en la página 40.	
10.	Crear un perfil de servidor	Vea Creación de un perfil de servidor de ASBCE para el IP Office en la página 41.	
11.	Crear enrutamiento del servidor	Vea Creación de un perfil de enrutamiento del servidor en la página 43.	
12.	Configurar ocultamiento de topología	Defina las conversiones de información de encabezado SIP que el ASBCE debe realizar . Vea Creación de una política de ocultamiento de topología de ASBCE en la página 44.	
13.	Cree una lista de bloqueo de IP/URL.	Configure los tipos de medios compatibles y el número máximo de conexiones. Vea Creación de una lista de bloqueo de IP/URI en la página 45.	
14.	Crear una regla de aplicación	Configure el tipo y el número de conexiones de medios compatibles. Vea Creación de una regla de aplicación en la página 46.	
15.	Crear una regla de medios	Vea Creación de una regla de medios en la página 47.	
16.	Crear una política de terminal	Una política de terminal agrupa las reglas de aplicación y medios. Vea Creación de un grupo de políticas de terminal en la página 50.	
17.	Agregar un perfil de agente de usuario	Defina los valores de AU para las extensiones remotas que el ASBCE debe permitir conectar. Vea Configuración de un perfil de agentes de usuario en la página 51.	
18.	Crear un flujo de suscriptor	Vea Creación del flujo de suscriptor en la página 52.	

La tabla continúa…

#	Acción	Vínculo/notas	✔
19.	Crear un flujo de servidor	Vea Creación de un flujo de servidor en la página 55.	
20.	Agregar un proxy inverso para Client Avaya Workplace	Enrutar solicitudes de archivos de configuración por parte de los clientes a IP Office. Vea Agregar proxys inversos para solicitudes de archivos en la página 57.	

Vínculos relacionados

Configuración de ASBCE para extensiones SIP remotas en la página 25

Configuración de firewall

Debe configurar el equipo de red del cliente en el borde de su red para enrutar el tráfico de extensión remota externa al ASBCE. El proceso real varía según la red y el equipo del cliente. Las siguientes son solo pautas.

Procedimiento

1. Habilite solo **NAT de capa 3**.
2. Deshabilitar todas las funcionalidades de conocimiento SIP como ALG.
3. Reenvíe los siguientes puertos a la dirección IP de la interfaz B1 del ASBCE.
   - **Para teléfonos Client Avaya Workplace de la serie J100:**

Protocolo de transporte/aplicación		Puerto	Utilización
tcp	tls	5061	Conexión SIP TLS para registro.
	http	80	Solicitudes de archivos generales y seguros desde teléfonos y clientes si **Usar puertos de teléfono preferidos** no está habilitado en IP Office.
	https	443	
	http	8411	Solicitudes de archivos generales y seguros desde teléfonos y clientes si **Usar puertos de teléfono preferidos** está habilitado en IP Office.
	https	411	
udp	rtp	40750 to 50750	El rango de puertos utilizado para el tráfico de medios de llamada (RTP) y de control de llamadas (RTCP).
	rtcp		

Pasos siguientes

- Vaya a Configurar la interfaz de ASBCE externa en la página 31.

Vínculos relacionados

Configuración de ASBCE para extensiones SIP remotas en la página 25

Configurar la interfaz de ASBCE externa

Agregue detalles para la red del cliente entre el firewall del cliente y el ASBCE.

- **Compatibilidad con IPv4/IPv6 dual:** para admitir extensiones remotas IPv4 e IPv6, debe crear entradas separadas para IPv4 e IPv6:
  - La **Dirección IP** para cada una debe utilizar la dirección *B1* IPv4 o IPv6 correspondiente.

Importante:

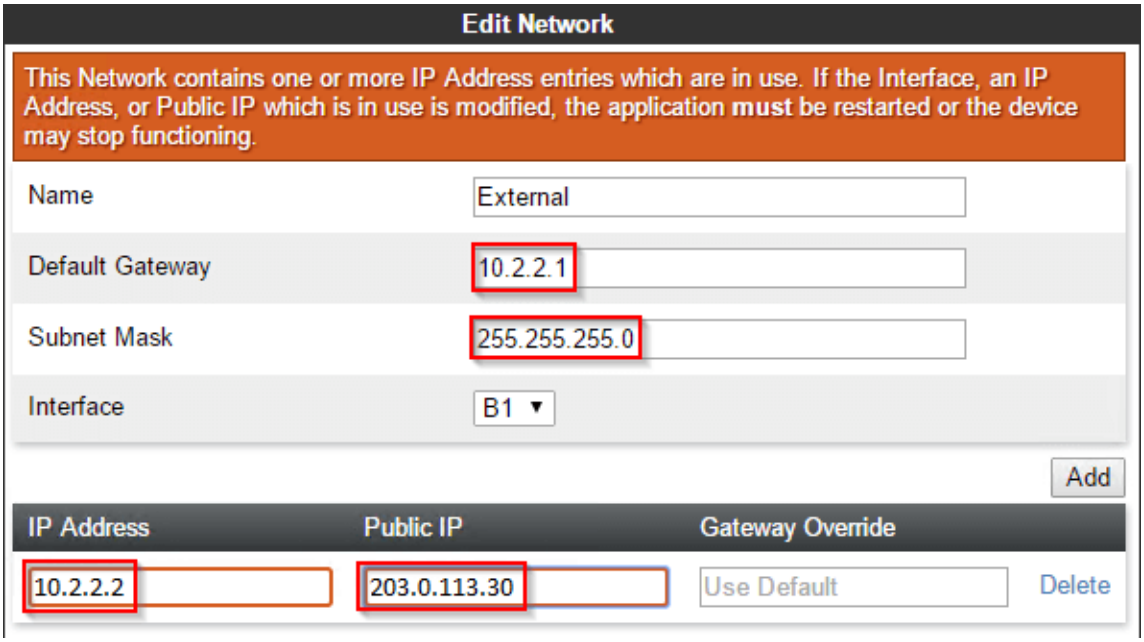
- Este proceso requiere que reinicie el ASBCE. Si lo hace, se finalizarán todas las conexiones actuales usando el ASBCE.

Antes de empezar

- Configuración de firewall en la página 30

Procedimiento

1. Vaya a **Configuración específica del dispositivo** > **Administración de red**.
2. Seleccione la pestaña **Redes** y haga clic en **Agregar**.
3. Introduzca los siguientes datos:



Campo	Descripción
Nombre	Este nombre se utiliza en otros menús para seleccionar la red.
Puerta de enlace predeterminada	La dirección IP interna del equipo que enruta el tráfico entre la red del cliente y la Internet pública. Para el escenario de ejemplo, esta es la dirección interna del firewall.
Máscara de subred	La máscara IP para la red de la **Puerta de enlace predeterminada**.
interfaces	Seleccione la interfaz pública del ASBCE.

4. Haga clic en **Agregar** e ingrese una dirección IP que el ASBCE utiliza en esta interfaz de red.

Campo	Descripción
Dirección IP	Ingrese la dirección IP de la interfaz del ASBCE conectada al firewall.
IP pública	Ingrese la dirección IP pública del firewall. Esto debe coincidir con la dirección IP a la que DNS dirige la extensión remota cuando realiza la búsqueda de DNS del nombre de dominio completo de IP Office.

5. Si admite extensiones remotas IPv4 e IPv6, repita el proceso para crear las entradas IPv6.

Pasos siguientes

- Vaya a Configurar la interfaz de ASBCE interna en la página 32.

Vínculos relacionados

Configuración de ASBCE para extensiones SIP remotas en la página 25

Configurar la interfaz de ASBCE interna

Agregue detalles para la red del cliente entre el ASBCE y IP Office.

- **Compatibilidad con IPv4/IPv6 dual:** puede utilizar la misma entrada para extensiones remotas IPv4 e IPv6.

Importante:

- Este proceso requiere que reinicie el ASBCE. Si lo hace, se finalizarán todas las conexiones actuales usando el ASBCE.

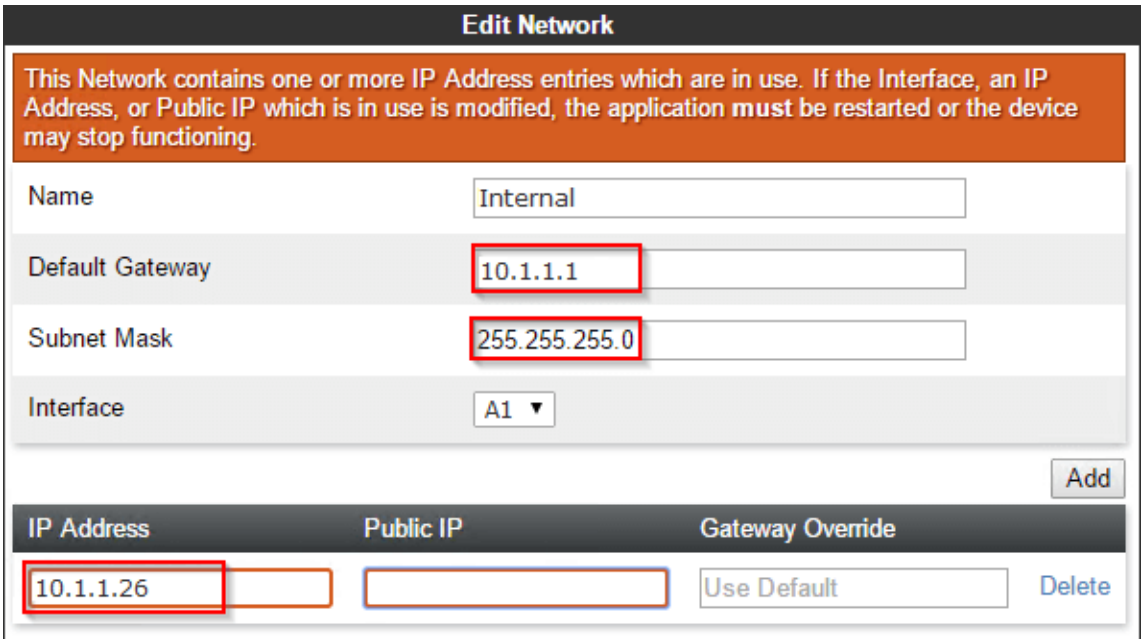
Antes de empezar

- Configurar la interfaz de ASBCE externa en la página 31

Procedimiento

1. Vaya a **Configuración específica del dispositivo** > **Administración de red**.
2. Seleccione la pestaña **Redes** y haga clic en **Agregar**.

3. Introduzca los siguientes datos:



Campo	Descripción
Nombre	Este nombre se utiliza en otros menús para seleccionar la red.
Puerta de enlace predeterminada	La dirección IP y la puerta de enlace predeterminada para el tráfico dentro de la red del cliente.
Máscara de subred	
interfaces	Seleccione la interfaz privada del ASBCE.

4. Haga clic en **Agregar** e ingrese una dirección IP que el ASBCE utiliza en esta interfaz de red.

Campo	Descripción
Dirección IP	Ingrese la dirección IP para la interfaz del ASBCE conectada a la red del cliente. Esta es la dirección IP de la interfaz A1.

5. Vaya a **Administración del sistema** y haga clic en **Reiniciar aplicación**.

Pasos siguientes

- Vaya a Creación de un perfil de cliente TLS en la página 34.

Vínculos relacionados

Configuración de ASBCE para extensiones SIP remotas en la página 25

Creación de un perfil de cliente TLS

Para conexiones TLS desde el ASBCE, actúa como cliente TLS. Por ejemplo, para conexiones a IP Office y a los clientes externos. El perfil del cliente TLS utilizado para cada conexión define los certificados utilizados y otros ajustes de TLS.

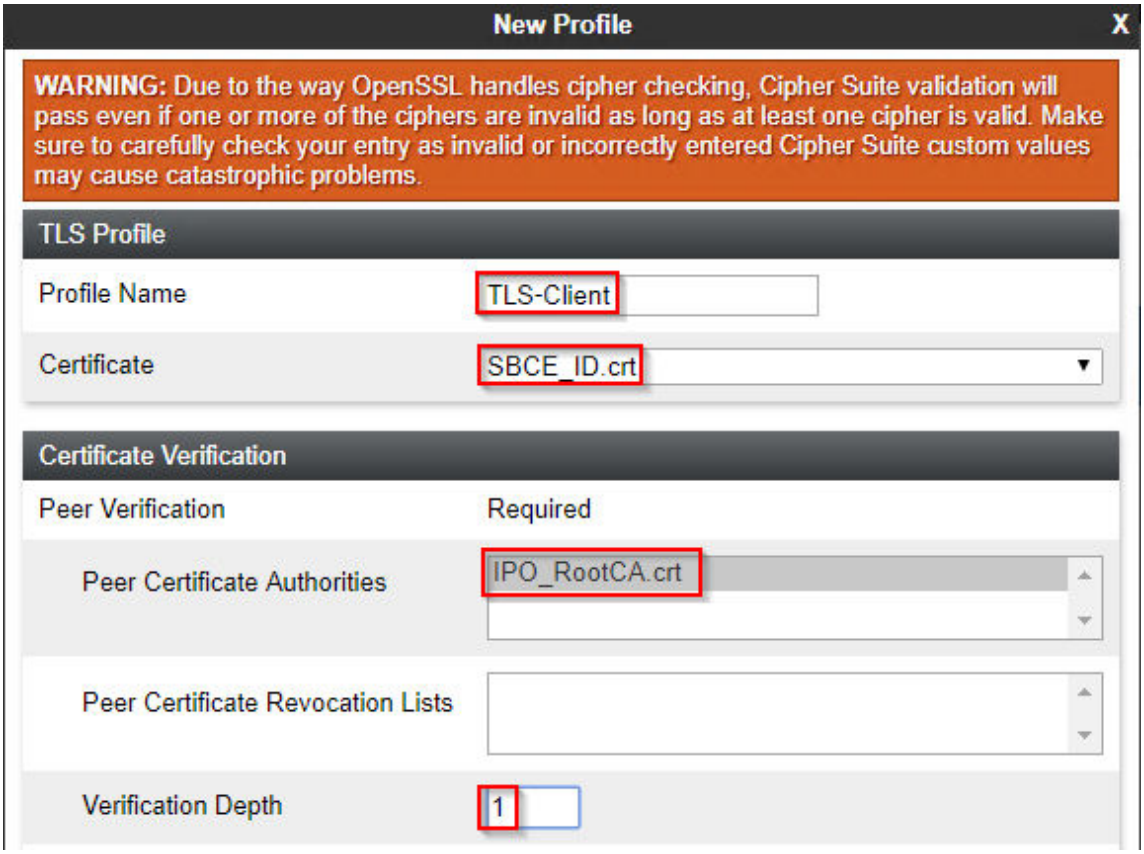
- **Compatibilidad con IPv4/IPv6 dual:** puede utilizar la misma entrada para extensiones remotas IPv4 e IPv6.

Antes de empezar

- Configurar la interfaz de ASBCE interna en la página 32.

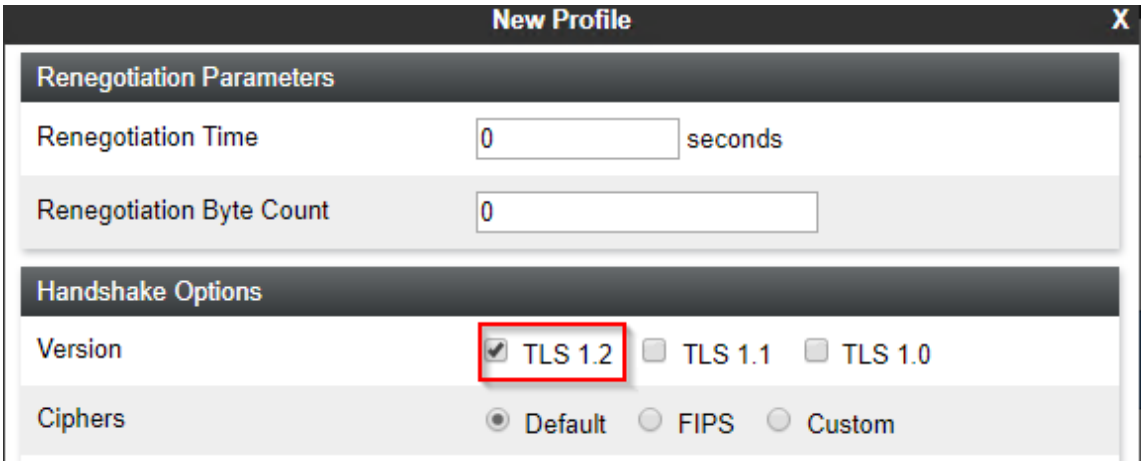
Procedimiento

1. Seleccione **Administración de TLS** > **Perfiles de cliente**.
2. Haga clic en **Agregar**.



3. Introduzca un nombre. Luego, puede utilizar esto para seleccionar la política en otros menús.
4. En **Certificado**, seleccione el certificado de identidad creado para el ASBCE.
5. En **Autoridades de certificado de pares**, seleccione el certificado raíz utilizado para crear el certificado de identidad. Para el escenario de ejemplo, este es el archivo `IPO_RootCA.crt` cargado en el ASBCE.
6. En **Profundidad de verificación**, ingrese **1**.

7. Haga clic en **Siguiente**.



8. Habilite **TLS 1.2**.
9. Haga clic en **Terminar**.

Pasos siguientes

- Vaya a Creación de un perfil de servidor TLS en la página 35.

Vínculos relacionados

Configuración de ASBCE para extensiones SIP remotas en la página 25

Creación de un perfil de servidor TLS

Para conexiones TLS al ASBCE, actúa como servidor TLS. Por ejemplo, para conexiones desde IP Office y desde clientes externos. El perfil del cliente TLS utilizado para cada conexión define los certificados utilizados y otros ajustes de TLS.

- **Compatibilidad con IPv4/IPv6 dual:** puede utilizar la misma entrada para extensiones remotas IPv4 e IPv6.

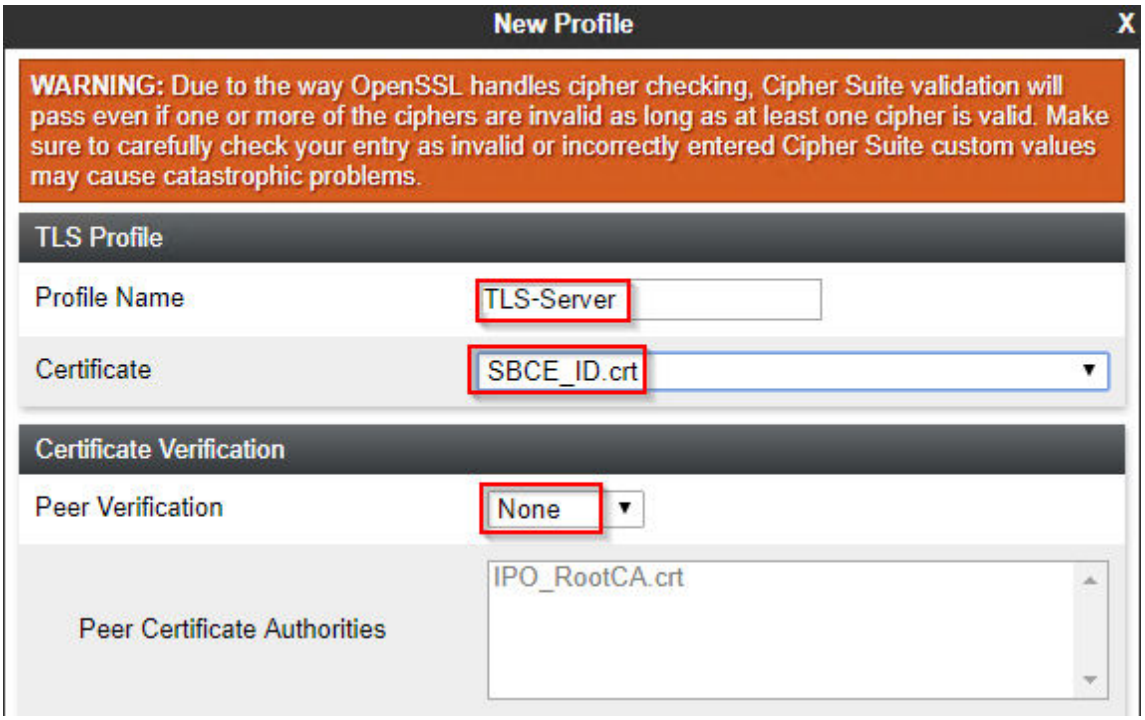
Antes de empezar

- Creación de un perfil de cliente TLS en la página 34.

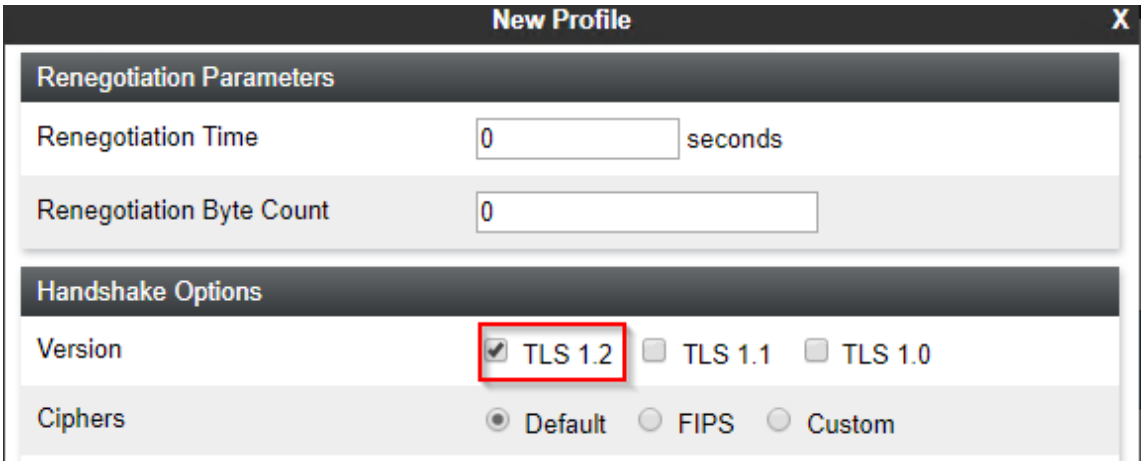
Procedimiento

1. Seleccione **Administración de TLS** > **Perfiles de cliente**.

2. Haga clic en **Agregar**.



3. Introduzca un nombre. Luego, puede utilizar esto para seleccionar la política en otros menús.
4. En **Certificado**, seleccione el certificado de identidad creado para el ASBCE.
5. En **Autoridades de certificado de pares**, seleccione **Ninguno**.
6. Haga clic en **Siguiente**.



7. Habilite **TLS 1.2**.
8. Haga clic en **Terminar**.

Pasos siguientes

- Vaya a Creación de una interfaz de medios interna en la página 37.

Vínculos relacionados

Configuración de ASBCE para extensiones SIP remotas en la página 25

Creación de una interfaz de medios interna

Debe crear una interfaz de medios interna. El ASBCE utiliza esto para escuchar medios de llamada SIP desde IP Office.

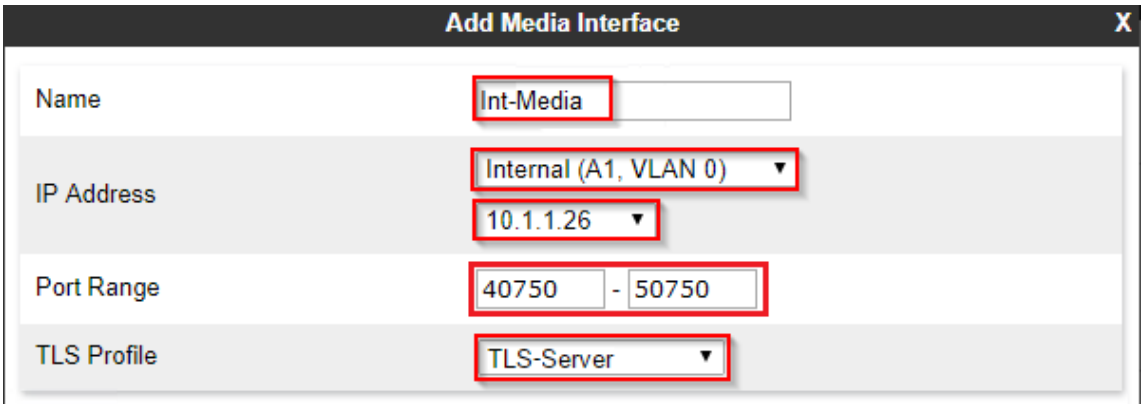
- **Compatibilidad con IPv4/IPv6 dual:** puede utilizar la misma entrada para extensiones remotas IPv4 e IPv6.

Antes de empezar

- Creación de un perfil de cliente TLS en la página 34.

Procedimiento

1. Seleccione **Configuración específica del dispositivo** > **interfaz de medios**.
2. Haga clic en **Agregar**.



3. Introduzca un nombre. Luego, puede utilizar esto para seleccionar la política en otros menús.
4. Seleccione la interfaz interna del ASBCE.
5. Para **Perfil TLS**, seleccione el perfil del servidor TLS que creó para el tráfico al ASBCE.
6. Haga clic en **Terminar**.

Pasos siguientes

- Vaya a Creación de una interfaz de medios externa en la página 38.

Vínculos relacionados

Configuración de ASBCE para extensiones SIP remotas en la página 25

Creación de una interfaz de medios externa

Debe crear una interfaz de medios externa. El ASBCE utiliza esto para escuchar medios de llamada SIP de las extensiones remotas.

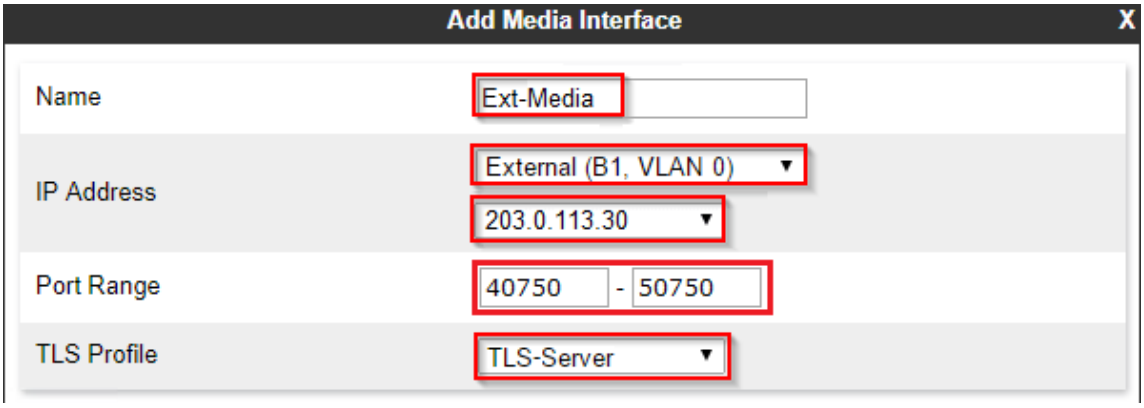
- **Compatibilidad con IPv4/IPv6 dual:** para admitir extensiones remotas IPv4 e IPv6, debe crear entradas separadas para IPv4 e IPv6:
  - La **Dirección IP** para cada una debe utilizar la dirección *B1* IPv4 o IPv6 correspondiente.

Antes de empezar

- Creación de una interfaz de medios interna en la página 37.

Procedimiento

1. Vaya a **Configuración específica del dispositivo** > **interfaz de medios**.
2. Haga clic en **Agregar**.



3. Introduzca un nombre. Luego, puede utilizar esto para seleccionar la política en otros menús.
4. Seleccione la interfaz externa y la dirección IP del ASBCE.
5. Para **Perfil TLS**, seleccione el perfil del servidor TLS que creó para el tráfico al ASBCE.
6. Haga clic en **Terminar**.
7. Si admite extensiones remotas IPv4 e IPv6, repita el proceso para crear las entradas IPv6.

Pasos siguientes

- Vaya a Creación de una interfaz de señalización interna en la página 39.

Vínculos relacionados

Configuración de ASBCE para extensiones SIP remotas en la página 25

Creación de una interfaz de señalización interna

Debe crear una interfaz de señalización interna. El ASBCE utiliza esto para escuchar la señalización de llamadas SIP desde IP Office.

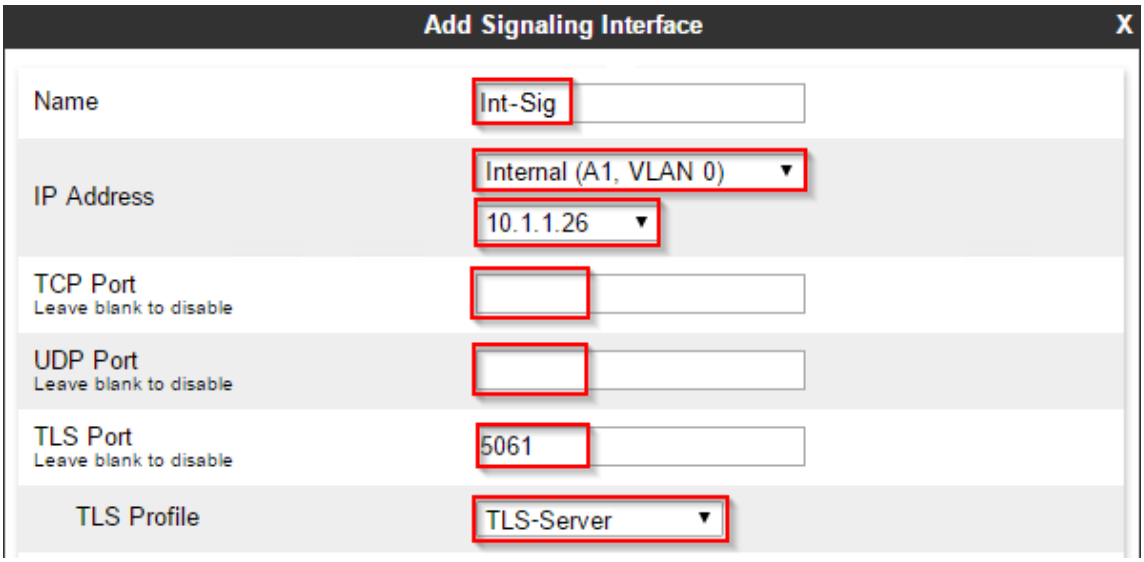
- **Compatibilidad con IPv4/IPv6 dual:** puede utilizar la misma entrada para extensiones remotas IPv4 e IPv6.

Antes de empezar

- Creación de una interfaz de medios externa en la página 38.

Procedimiento

1. Seleccione **Configuración específica del dispositivo** > **Interfaz de señalización**.
2. Haga clic en **Agregar**.



3. Introduzca un nombre. Luego, puede utilizar esto para seleccionar la política en otros menús.
4. Elija *A1* de la lista desplegable **Dirección IP**.
5. Deje el espacio **Puerto TCP** en blanco para deshabilitar TCP.
6. Deje **Puerto UDP** en blanco para deshabilitar UDP.
7. Configure **Puerto TLS** para que coincida con el puerto TLS de IP Office.
8. Para **Perfil TLS**, seleccione el perfil del servidor TLS que creó para el tráfico al ASBCE.
9. Haga clic en **Terminar**.

Pasos siguientes

- Vaya a Creación de la interfaz de señalización externa en la página 40.

Vínculos relacionados

Configuración de ASBCE para extensiones SIP remotas en la página 25

Creación de la interfaz de señalización externa

Debe crear una interfaz de señalización externa. El ASBCE utiliza esto para escuchar mensajes de registro SIP de las extensiones remotas.

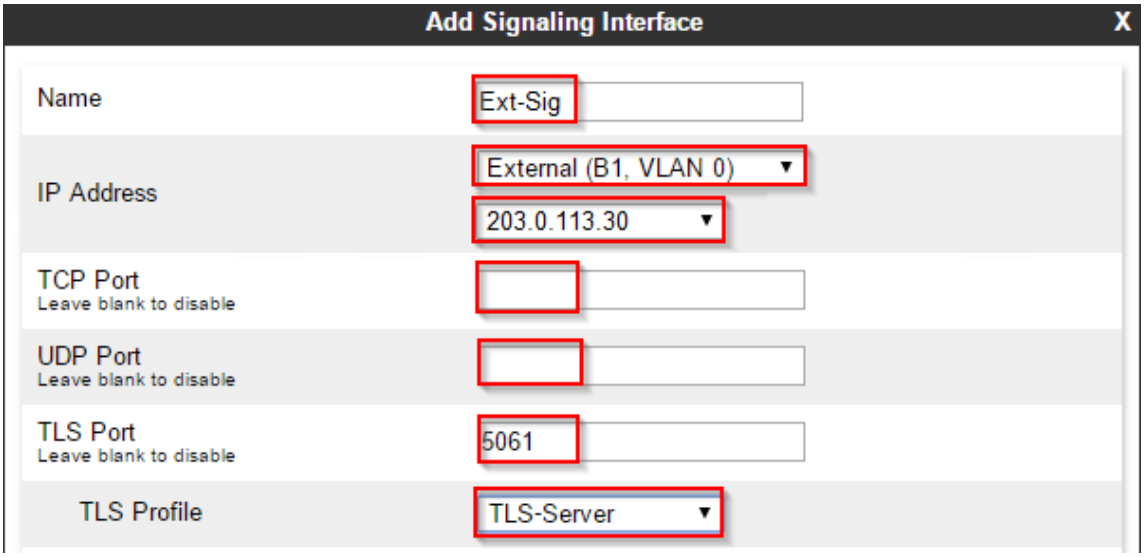
- **Compatibilidad con IPv4/IPv6 dual:** para admitir extensiones remotas IPv4 e IPv6, debe crear entradas separadas para IPv4 e IPv6:
  - La **Dirección IP** para cada una debe utilizar la dirección *B1* IPv4 o IPv6 correspondiente.

Antes de empezar

- Creación de una interfaz de señalización interna en la página 39.

Procedimiento

1. Seleccione **Configuración específica del dispositivo** > **Interfaz de señalización**.
2. Haga clic en **Agregar**.



3. Introduzca un nombre. Luego, puede utilizar esto para seleccionar la política en otros menús.
4. Elija *B1* de la lista desplegable **Dirección IP**.
5. Deje el espacio **Puerto TCP** en blanco para deshabilitar TCP.
6. Deje **Puerto UDP** en blanco para deshabilitar UDP.
7. Configure **Puerto TLS** para que coincida con el puerto TLS de IP Office.
8. Para **Perfil TLS**, seleccione el perfil del servidor TLS que creó para el tráfico al ASBCE.
9. Haga clic en **Terminar**.
10. Si admite extensiones remotas IPv4 e IPv6, repita el proceso para crear las entradas IPv6.

Pasos siguientes

- Vaya a Creación de un perfil de servidor de ASBCE para el IP Office en la página 41.

Vínculos relacionados

Configuración de ASBCE para extensiones SIP remotas en la página 25

Creación de un perfil de servidor de ASBCE para el IP Office

Debe crear un perfil de servidor en el ASBCE que coincida con la configuración de IP Office, consulte Configuración de SIP VoIP de IP Office en la página 11.

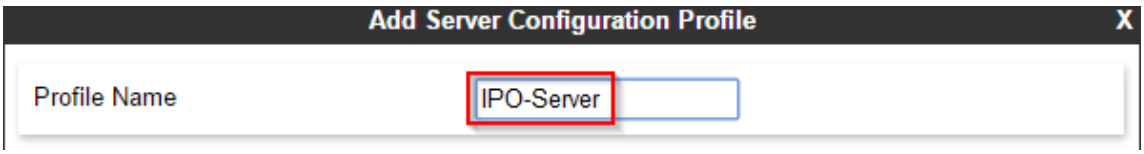
- **Compatibilidad con IPv4/IPv6 dual:** puede utilizar la misma entrada para extensiones remotas IPv4 e IPv6.

Antes de empezar

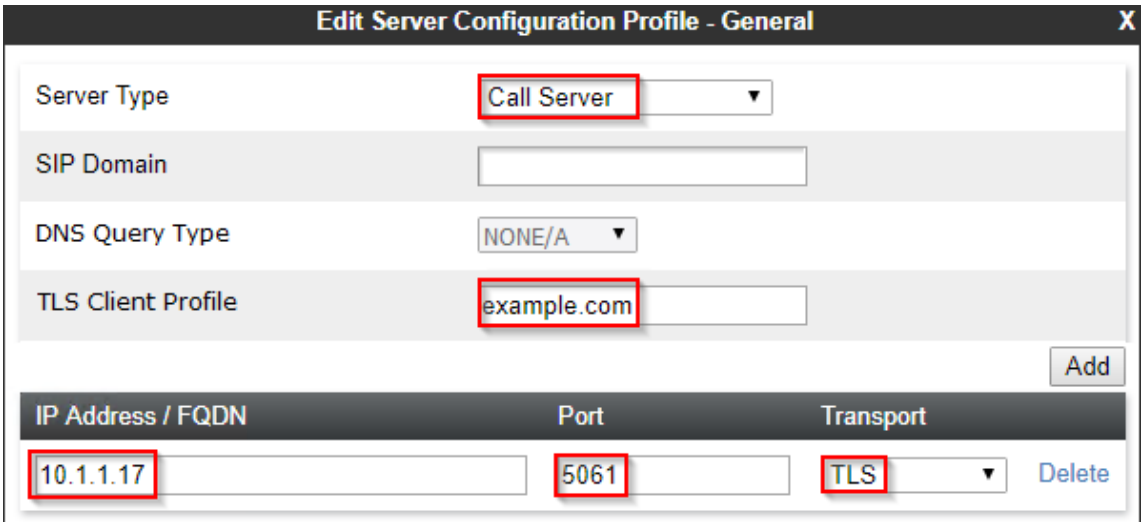
- Creación de una interfaz de señalización interna en la página 39.

Procedimiento

1. Seleccione **Perfiles globales** > **Configuración del servidor**.
2. Haga clic en **Agregar**.
3. Introduzca un nombre. Luego, puede utilizar esto para seleccionar la política en otros menús.



4. Haga clic en **Siguiente**.

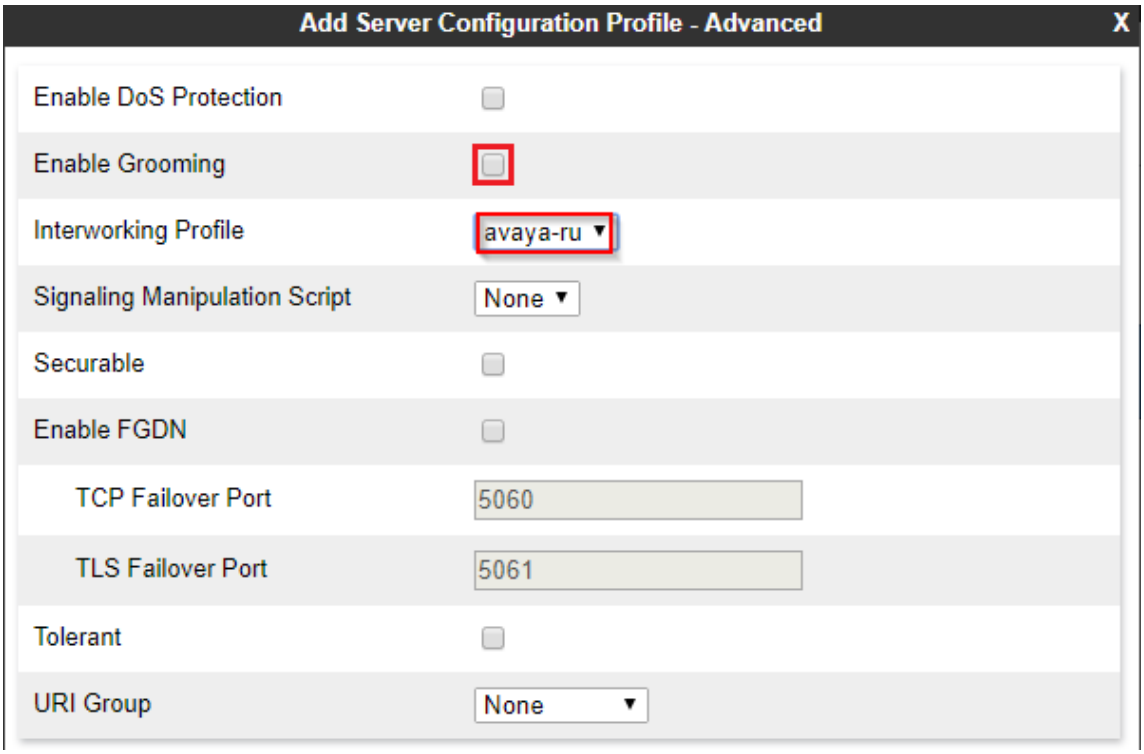


   a. Para **Tipo de servidor** seleccione **Servidor de llamadas**.
   b. Configure el **Dominio SIP** para que coincida con el utilizado por IP Office para el registro SIP.
   c. Para el **Perfil de cliente TLS** seleccione el perfil de cliente TLS que creó.

d. Haga clic en **Agregar** e ingrese los detalles para las conexiones SIP de cuatro puertos de capa establecidas en la configuración de IP Office.
   - Configure el **Dirección/FQDN IP** a la dirección IP del IP Office.
   - Configure el **Puerto** y el **Transporte** para que coincidan con la configuración de IP Office.

e. Haga clic en **Siguiente**.

5. Haga clic en **Siguiente** para omitir la configuración de **Autenticación**.
6. Haga clic en **Siguiente** para omitir la configuración de **Latido**.
7. Ajuste la configuración avanzada de la siguiente manera:



a. Desactive la casilla de verificación **Habilitar grooming**.

b. Configure **Perfil de interconexión** en *avaya-ru*.

8. Haga clic en **Terminar**.

Pasos siguientes

- Vaya a Creación de un perfil de enrutamiento del servidor en la página 43.

Vínculos relacionados

Configuración de ASBCE para extensiones SIP remotas en la página 25

Creación de un perfil de enrutamiento del servidor

El ASBCE utiliza un perfil de enrutamiento del servidor para enrutar el tráfico entrante coincidente al servidor o servidores correspondientes. En este caso, debe crear un perfil que enrute el tráfico a IP Office.

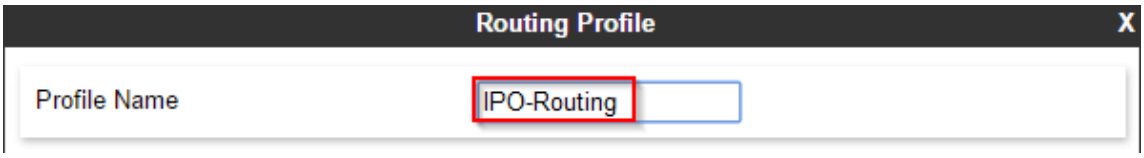
- **Compatibilidad con IPv4/IPv6 dual:** puede utilizar la misma entrada para extensiones remotas IPv4 e IPv6.

Antes de empezar

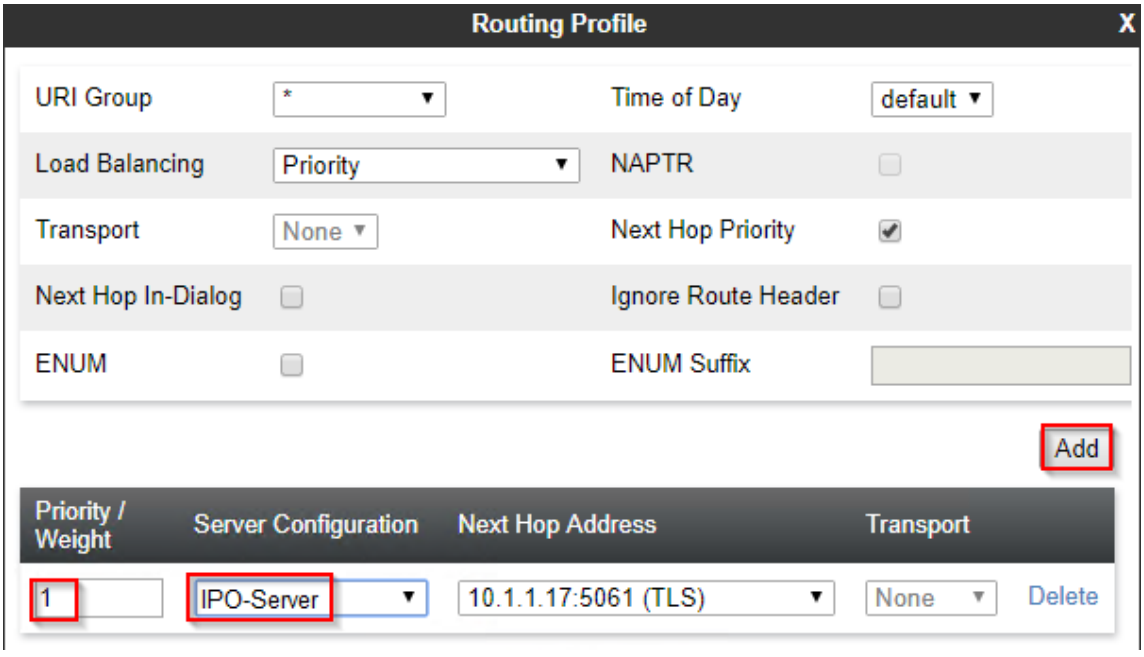
- Creación de un perfil de servidor de ASBCE para el IP Office en la página 41.

Procedimiento

1. Seleccione **Perfiles globales** > **Enrutamiento**.
2. Haga clic en **Agregar**.
3. Introduzca un nombre. Luego, puede utilizar esto para seleccionar la política en otros menús.



4. Haga clic en **Siguiente**.



5. Haga clic en **Agregar**.
6. Configure la **Prioridad** en 1.
7. Configure la **Configuración del servidor** en el perfil del servidor creado para IP Office.
8. En **Dirección de siguiente Hop**, seleccione la dirección IP de IP Office.
9. Haga clic en **Terminar**.

Pasos siguientes

- Vaya a Creación de una política de ocultamiento de topología de ASBCE en la página 44.

Vínculos relacionados

Configuración de ASBCE para extensiones SIP remotas en la página 25

Creación de una política de ocultamiento de topología de ASBCE

El ASBCE puede utilizar la configuración de ocultamiento de topología para eliminar o reemplazar valores en mensajes SIP. Por ejemplo, reemplace una dirección IP en un encabezado SIP con un nombre de dominio completo.

- **Compatibilidad con IPv4/IPv6 dual:** puede utilizar la misma entrada para extensiones remotas IPv4 e IPv6.

Antes de empezar

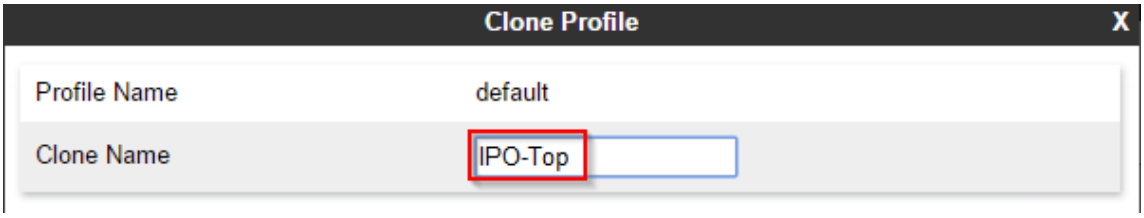
- Creación de un perfil de enrutamiento del servidor en la página 43.

Procedimiento

1. Seleccione **Perfiles globales** > **Ocultamiento de topología**.
2. Seleccione el perfil predeterminado y haga clic en **Clonar**.

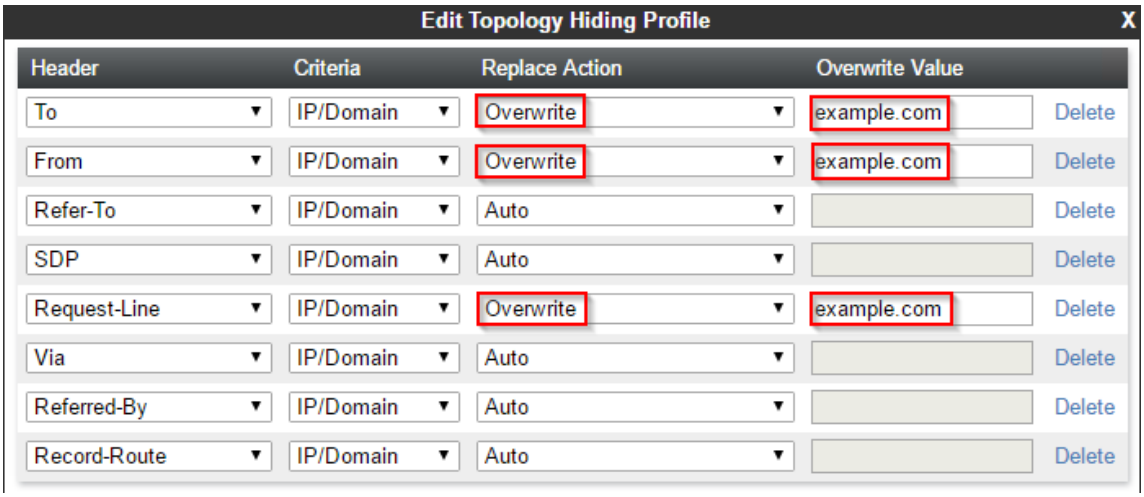
   Importante:

   - Debe utilizar **Clonar** y el perfil o la política indicados. El uso de **Agregar** creará un nuevo perfil o política con diferentes configuraciones predeterminadas.
3. Introduzca un nombre. Luego, puede utilizar esto para seleccionar la política en otros menús.



4. Haga clic en **Terminar**.

5. Seleccione el nuevo perfil y haga clic en **Editar**.



6. Para los campos **A**, **Desde**, **SDP**, **Referencia a** y **Línea de solicitud**:
   a. Establezca **Reemplazar acción** en **Sobrescribir**.
   b. Ingrese el dominio IP Office como **Sobrescribir valor**.
7. Haga clic en **Terminar**.

Pasos siguientes

- Vaya a Creación de una lista de bloqueo de IP/URI en la página 45.

Vínculos relacionados

Configuración de ASBCE para extensiones SIP remotas en la página 25

Creación de una lista de bloqueo de IP/URI

Puede utilizar una lista de bloqueo para que el ASBCE bloquee las direcciones IP y URI que sean el origen de solicitudes de registro fallidas. Luego, puede agregar la lista de bloqueo a cualquier flujo de suscriptor y proxys inversos que cree.

- **Compatibilidad con IPv4/IPv6 dual:** puede utilizar la misma entrada para extensiones remotas IPv4 e IPv6.

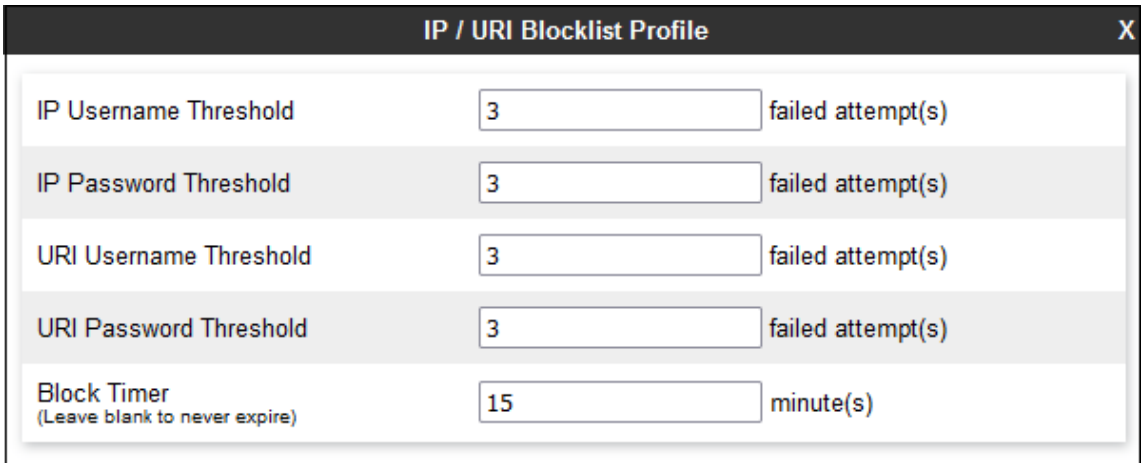
Antes de empezar

- Creación de una política de ocultamiento de topología de ASBCE en la página 44.

Procedimiento

1. Seleccione **Políticas de dominio** > **Perfil de lista de bloqueo de IP/URI**.

2. Haga clic en **Agregar**.



3. Introduzca un nombre. Luego, puede utilizar esto para seleccionar la política en otros menús.
4. Establezca el número de intentos fallidos de nombre y contraseña permitidos.
5. Establezca cuánto tiempo se bloquea una dirección IP o URI después de exceder cualquiera de los límites establecidos.
6. Haga clic en **Terminar**.

Pasos siguientes

- Continúe a Creación de una regla de aplicación en la página 46.

Vínculos relacionados

Configuración de ASBCE para extensiones SIP remotas en la página 25

Creación de una regla de aplicación

Puede utilizar una regla de aplicación para restringir el tipo de conexiones de medios que permite el ASBCE. También puede configurar el número máximo de dichas conexiones y el número máximo de conexiones por extensión remota.

- **Compatibilidad con IPv4/IPv6 dual:** puede utilizar la misma entrada para extensiones remotas IPv4 e IPv6.

Antes de empezar

- Creación de una lista de bloqueo de IP/URI en la página 45.

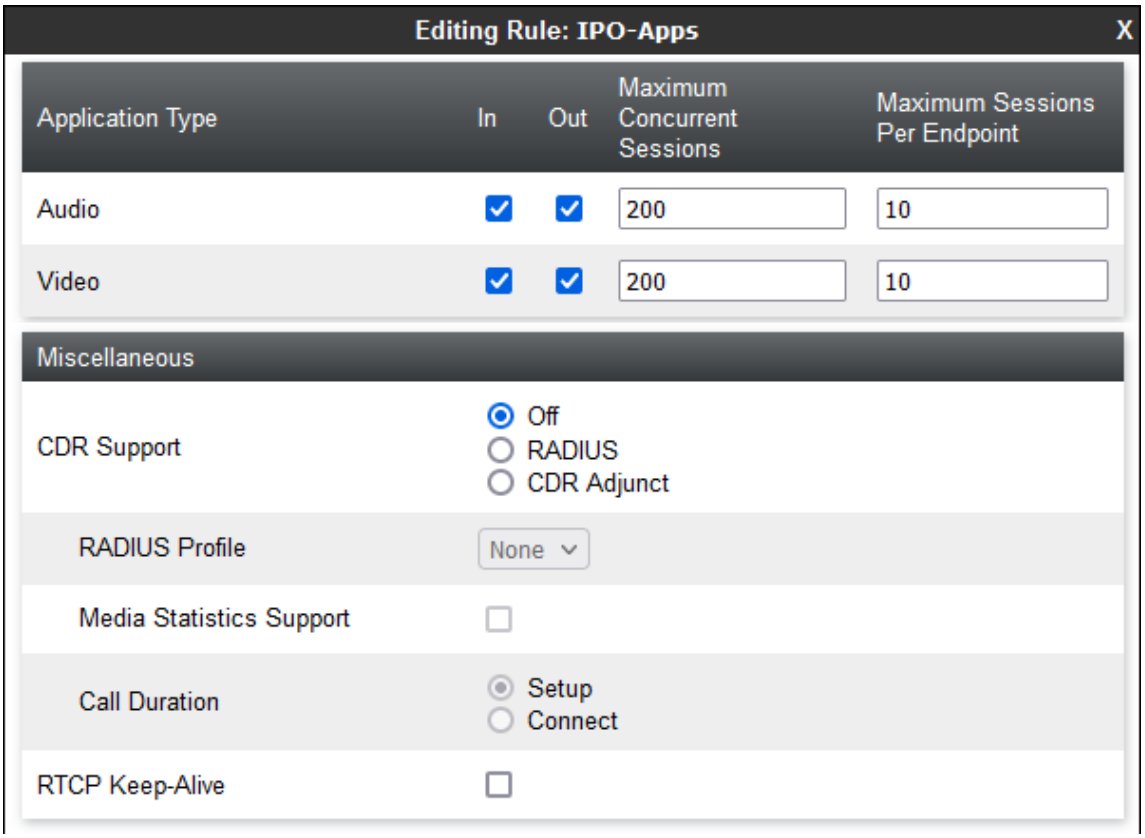
Procedimiento

1. Seleccione **Políticas de dominio** > **Reglas de aplicación**.
2. Seleccione la política *default-low* y haga clic en **Clonar**.

Importante:

- Debe utilizar **Clonar** y el perfil o la política indicados. El uso de **Agregar** creará un nuevo perfil o política con diferentes configuraciones predeterminadas.

3. Introduzca un nombre. Luego, puede utilizar esto para seleccionar la política en otros menús.
4. Haga clic en **Terminar**.
5. Seleccione la nueva política y haga clic en **Editar**.
6. Seleccione si desea permitir **Audio** y/o **Video**.



7. Para cada una de las anteriores, configure **Máximo de sesiones concurrentes** y **Máximo de sesiones por terminal**.
8. Haga clic en **Terminar**.

Pasos siguientes

- Continúe a Creación de una regla de medios en la página 47.

Vínculos relacionados

Configuración de ASBCE para extensiones SIP remotas en la página 25

Creación de una regla de medios

Puede utilizar una regla de medios para definir diferentes configuraciones de medios.

- **Compatibilidad con IPv4/IPv6 dual:** puede utilizar la misma entrada para extensiones remotas IPv4 e IPv6.

Antes de empezar

- Creación de una regla de aplicación en la página 46.

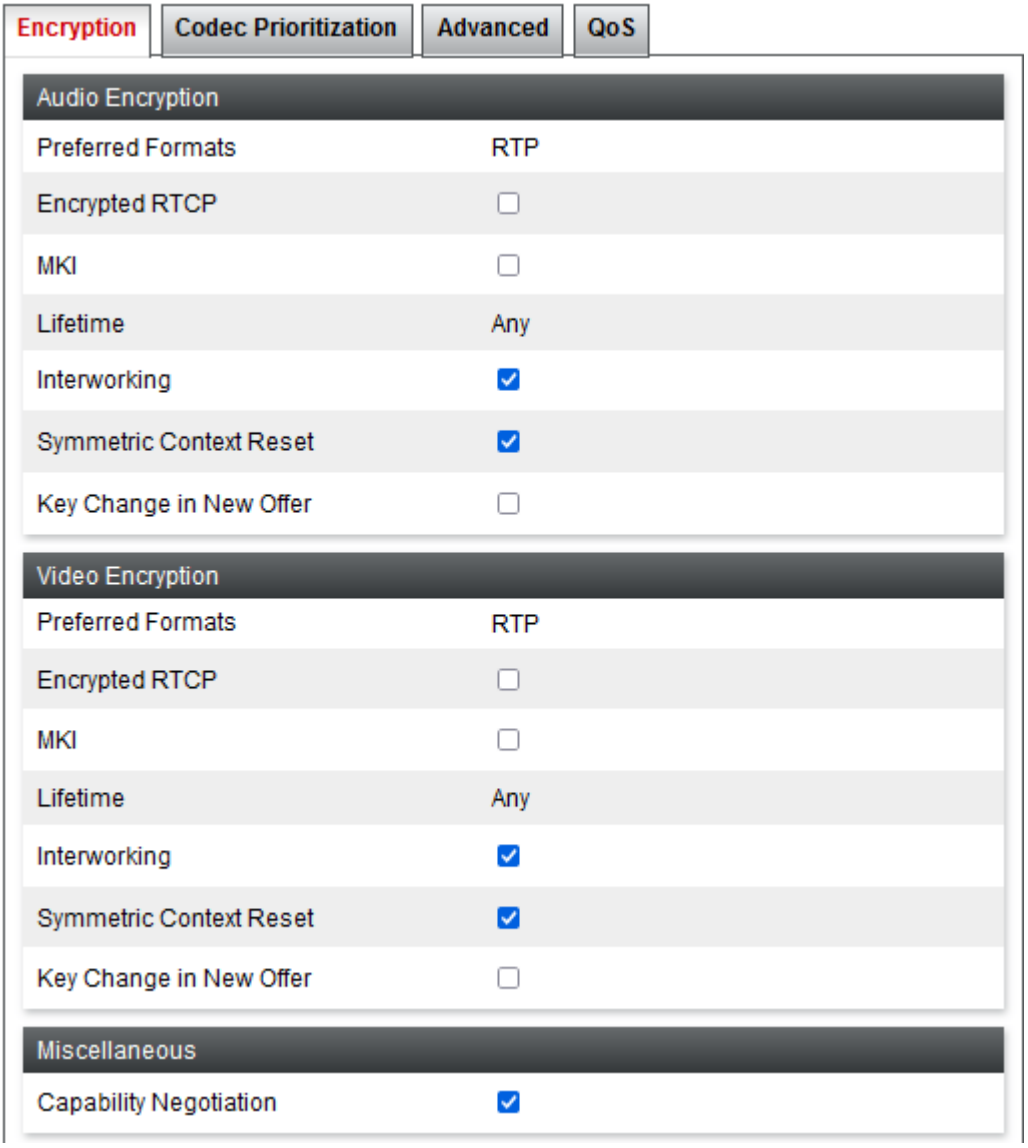
Procedimiento

1. Seleccione **Políticas de dominio** > **Reglas de medios**.
2. Seleccione la política *avaya-low-med-enc* y haga clic en **Clonar**.

   Importante:

   - Debe utilizar **Clonar** y el perfil o la política indicados. El uso de **Agregar** creará un nuevo perfil o política con diferentes configuraciones predeterminadas.
3. Introduzca un nombre. Luego, puede utilizar esto para seleccionar la política en otros menús.
4. Haga clic en **Terminar**.
5. Seleccione la nueva política y haga clic en **Editar**.

6. Para las opciones **Cifrado de audio** y **Cifrado de video**, configure **Formatos preferidos** en *RTP*.



   - Si utiliza SRTP, configure los valores **Formatos preferidos** y **RTCP cifrado** para que coincidan con la configuración de **Seguridad de VoIP** establecida en IP Office.
7. Compruebe que la configuración **Opciones avanzadas** > **ANAT habilitada** no esté seleccionada.
8. Haga clic en **Terminar**.

Pasos siguientes

- Continúe a Creación de un grupo de políticas de terminal en la página 50.

Vínculos relacionados

Configuración de ASBCE para extensiones SIP remotas en la página 25

Creación de un grupo de políticas de terminal

Una política de terminal agrupa reglas como reglas de medios y aplicaciones. Después de crear una política de terminal, puede asociarla con los flujos de suscriptor y servidor que crea.

- **Compatibilidad con IPv4/IPv6 dual:** puede utilizar la misma entrada para extensiones remotas IPv4 e IPv6.

Antes de empezar

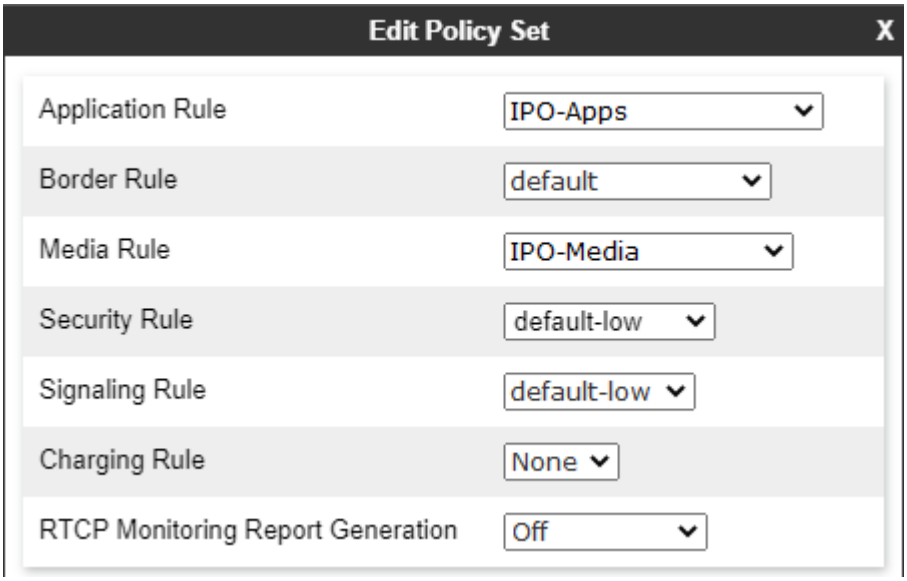
- Creación de una regla de medios en la página 47.

Procedimiento

1. Seleccione **Políticas de dominio** > **Grupos de políticas de terminal**.
2. Seleccione la política *default-low* y haga clic en **Clonar**.

   Importante:

   - Debe utilizar **Clonar** y el perfil o la política indicados. El uso de **Agregar** creará un nuevo perfil o política con diferentes configuraciones predeterminadas.
3. Introduzca un nombre. Luego, puede utilizar esto para seleccionar la política en otros menús.
4. Haga clic en **Terminar**.
5. Seleccione la nueva política y haga clic en **Editar**.
6. En **Regla de aplicación**, seleccione las reglas de medios y aplicaciones que creó para las extensiones remotas.



7. En **Regla de medios**, seleccione la regla de medios que creó.
8. Haga clic en **Terminar**.

Pasos siguientes

- Continúe a Configuración de un perfil de agentes de usuario en la página 51.

Vínculos relacionados

Configuración de ASBCE para extensiones SIP remotas en la página 25

Configuración de un perfil de agentes de usuario

Puede utilizar **Agentes de usuario** para restringir la conexión del ASBCE a aquellos clientes y teléfonos que envían una cadena *User Agent* (*UA*) coincidente. De lo contrario, cualquier teléfono o cliente puede conectarse.

- **Compatibilidad con IPv4/IPv6 dual:** puede utilizar la misma entrada para extensiones remotas IPv4 e IPv6.

Los siguientes son ejemplos de cadenas *UA* enviadas por clientes de Avaya.

Teléfono o cliente de Avaya	Agente de usuario
Teléfonos Avaya de la serie 9600	*Avaya one-X Deskphone*
Avaya J159	*Avaya J159 IP Phone 4.0.10.3.2*
Client Avaya Workplace - Android	*Avaya Communicator Android/3.35.2 (FA-RELEASE80-BUILD.18; Pixel 8 Pro)*
Client Avaya Workplace - Windows	*Avaya Communicator/3.0 (3.33.0.96.6; Avaya SDK; Microsoft Windows NT 10.0.19045.0)*

- Como se muestra en los ejemplos anteriores, la cadena de *UA* puede variar según la versión y/o plataforma del software.
- Puede ver la *UA* enviado por un teléfono o softphone en particular en SysMonitor después de registrar el teléfono o el cliente.

La coincidencia de AU utiliza una coincidencia de cadena de expresión regular (regex). Los siguientes son ejemplos de cadenas regex:

Expresión regular	Descripción
`Avaya.*`	Coincide con cualquier *UA* que comienza con *Avaya*. El `.` coincide con cualquier carácter. El `.*` coincide con cualquier número de caracteres.
`Avaya J1.*`	Coincide con la cadena *UA* de cualquier teléfono de la serie J100.
`Avaya (J1|Communicator).*`	Coincide con la cadena *UA* de teléfonos de la serie J100 y Client Avaya Workplace. Los paréntesis `( )` encierran las coincidencias potenciales, cada coincidencia potencial separada por un carácter `|`.
`Avaya Communicator\/3\.0\(3\.33.*`	Coincide con la cadena *UA* de solo la versión de Windows 3.33 de Client Avaya Workplace. La expresión regex utiliza la `\` par anteponer caracteres que de lo contrario se tratarían como comandos regex. Por ejemplo, `.` coincide con cualquier carácter mientras que `\.` coincide solo con un carácter `.` literal.

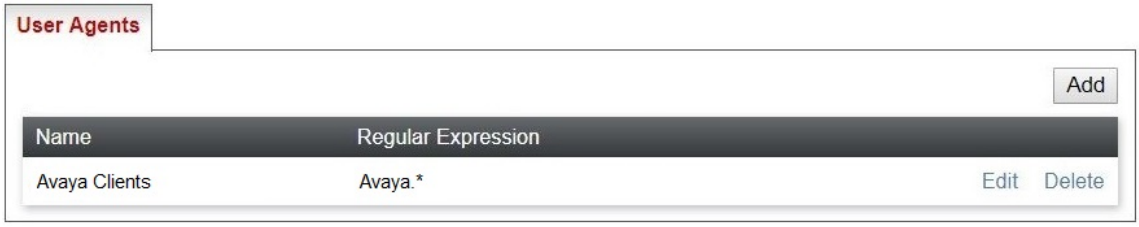
Para obtener más información sobre cómo crear cadenas regex, consulte https://learn.microsoft.com/en-us/dotnet/standard/base-types/regular-expression-language-quick-reference y https://regex101.com.

Antes de empezar

- Creación de una política de ocultamiento de topología de ASBCE en la página 44.

Procedimiento

1. Seleccione **Administración del sistema** > **Parámetros globales** > **Agentes de usuario**.
2. Haga clic en **Agregar**.



3. Introduzca un nombre. Luego, puede utilizar esto para seleccionar la política en otros menús.
4. Ingrese la expresión regular para la cadena o cadenas del agente del usuario que desea que coincidan.
5. Haga clic en **Terminar**.

Pasos siguientes

- Vaya a Creación del flujo de suscriptor en la página 52.

Vínculos relacionados

Configuración de ASBCE para extensiones SIP remotas en la página 25

Creación del flujo de suscriptor

El ASBCE utiliza un flujo de suscriptor para manejar conexiones entrantes desde extensiones remotas.

- **Compatibilidad con IPv4/IPv6 dual:** para admitir extensiones remotas IPv4 e IPv6, debe crear entradas separadas para IPv4 e IPv6:
  - Las interfaces **Interfaz de señalización** y **interfaz de medios** para cada una deben utilizar las interfaces IPv4 o IPv6 externas respectivas.

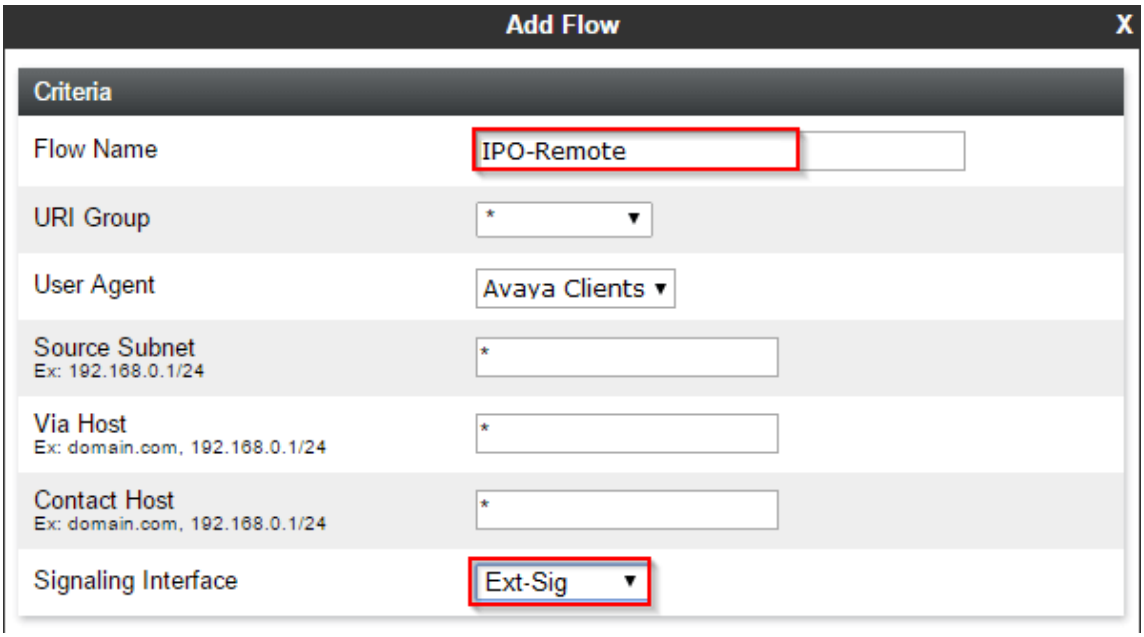
Antes de empezar

- Configuración de un perfil de agentes de usuario en la página 51.

Procedimiento

1. Seleccione **Configuración específica del dispositivo** > **Flujos de punto final**.

2. Seleccione la pestaña **Flujos de suscriptor** y haga clic en **Agregar**.

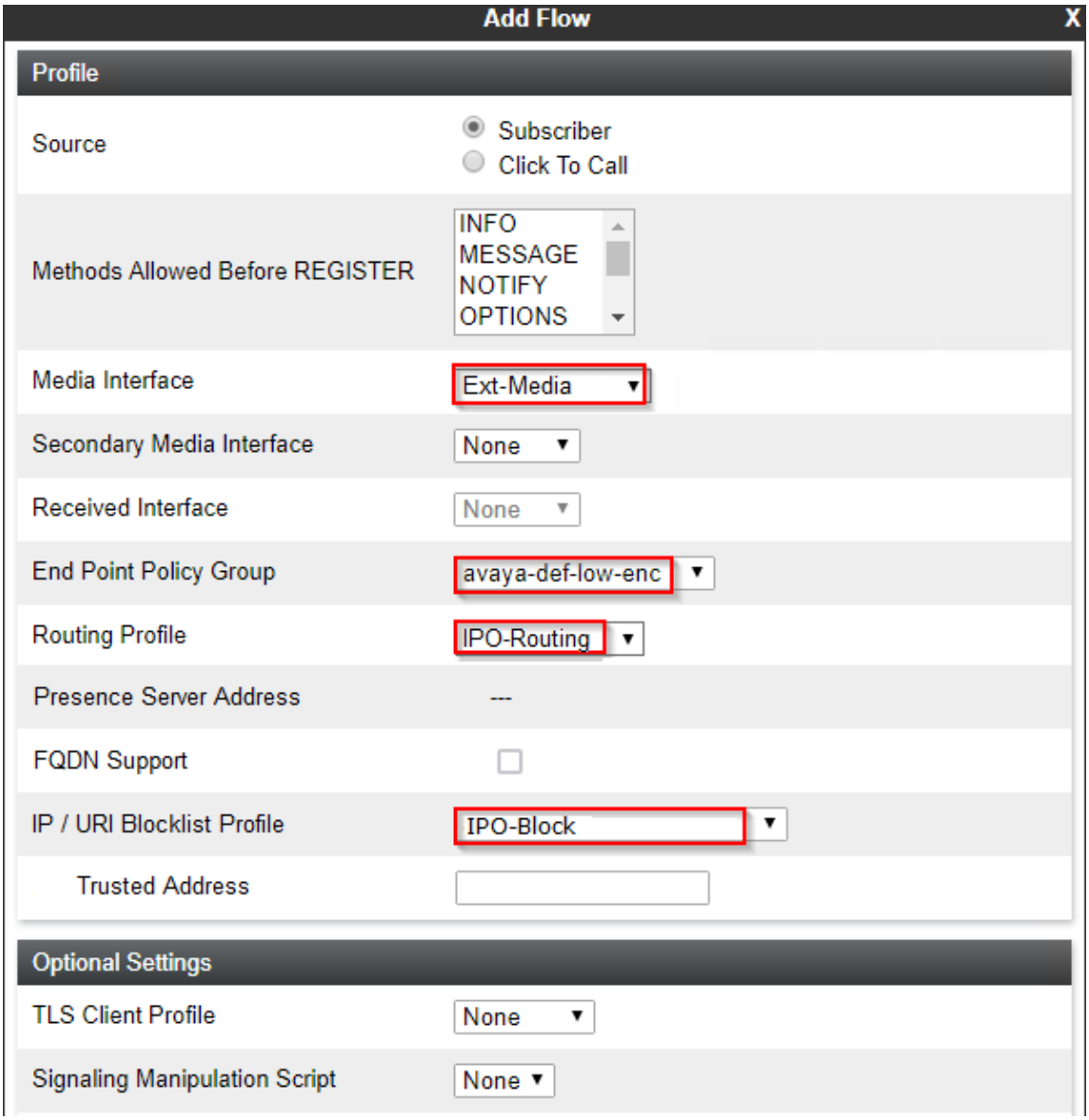


a. Introduzca un nombre. Luego, puede utilizar esto para seleccionar la política en otros menús.

b. Si es necesario, seleccione el perfil **Agente de usuario** que creó para que coincida con la AU de clientes que pueden utilizar el flujo de suscriptor.

c. Seleccione la **Interfaz de señalización** externa creada para las extensiones remotas.

3. Haga clic en **Siguiente**.



   a. En **interfaz de medios**, seleccione la interfaz de medios externos creada para las extensiones remotas.
   b. En **Grupo de políticas de terminal**, seleccione *avaya-def-low-enc*.
   c. En **Perfil de enrutamiento**, seleccione el perfil de enrutamiento del servidor creado para IP Office.
   d. Si creó un perfil de lista de bloques, selecciónelo usando el menú desplegable **Perfil de lista de bloqueo de IP/URI**.

4. Haga clic en **Terminar**.
5. Si admite extensiones remotas IPv4 e IPv6, repita el proceso para crear las entradas IPv6.

Pasos siguientes

- Vaya a Creación de un flujo de servidor en la página 55.

Vínculos relacionados

Configuración de ASBCE para extensiones SIP remotas en la página 25

Creación de un flujo de servidor

El ASBCE utiliza un flujo de servidor para manejar conexiones entrantes desde el servidor de IP Office.

- **Compatibilidad con IPv4/IPv6 dual:** para admitir extensiones remotas IPv4 e IPv6, debe crear entradas separadas para IPv4 e IPv6:
  - La **Interfaz recibida** para cada flujo del servidor debe utilizar la interfaz de señalización externa IPv4 o IPv6 correspondiente.

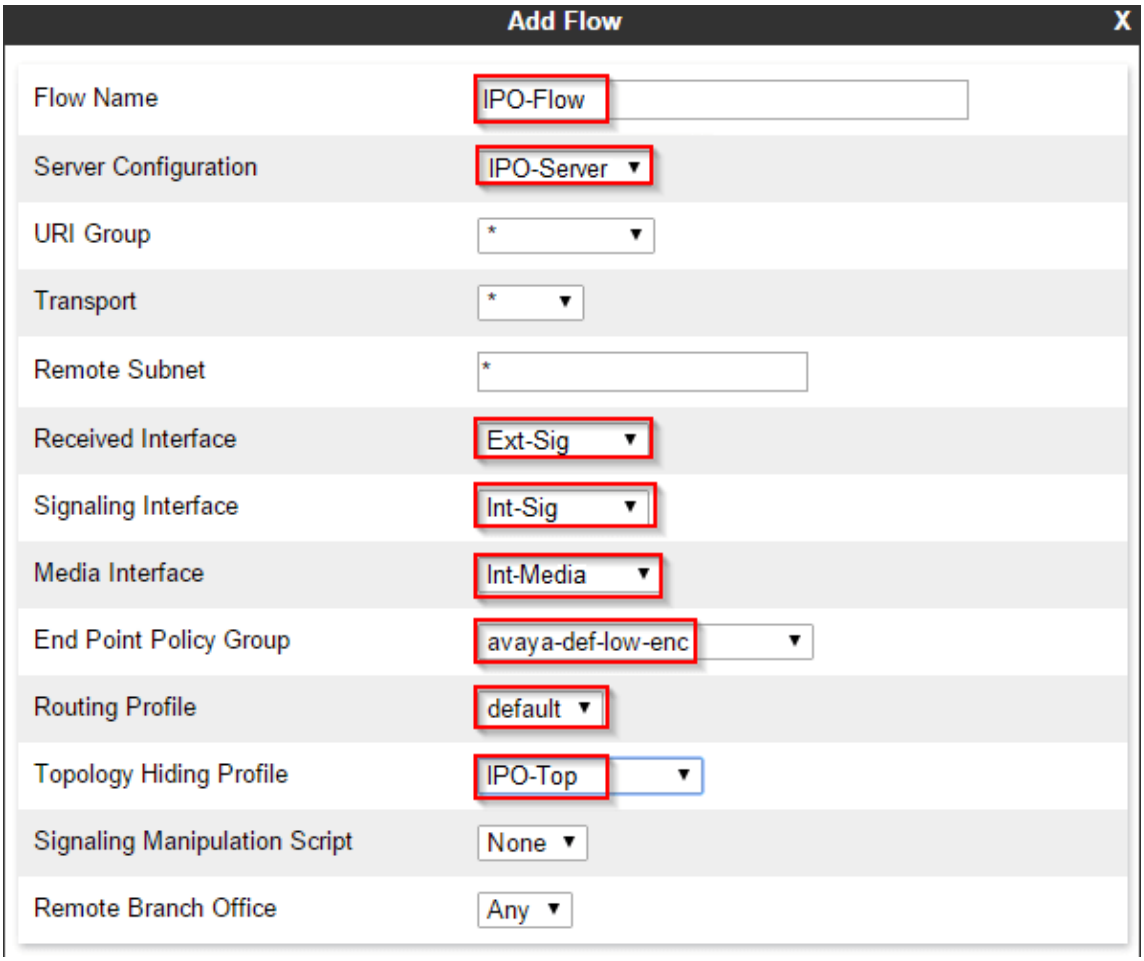
Antes de empezar

- Creación del flujo de suscriptor en la página 52.

Procedimiento

1. Seleccione **Configuración específica del dispositivo** > **Flujos de punto final**.

2. Seleccione la pestaña **Flujos del servidor** y haga clic en **Agregar**.



   a. En **Nombre de flujo**, ingrese un nombre descriptivo.
   b. En **Configuración del servidor**, seleccione el perfil de servidor creado para el servidor de IP Office.
   c. En **Interfaz recibida**, seleccione la interfaz de señalización externa creada para las extensiones remotas.
   d. En **Interfaz de señalización**, seleccione la interfaz de señalización interna creada para las extensiones remotas.
   e. En **interfaz de medios**, seleccione la interfaz de medios internos creada para las extensiones remotas.
   f. En **Grupo de políticas de terminal**, seleccione *avaya-def-low-enc*.
   g. En **Perfil de enrutamiento**, seleccione *default*.
   h. En **Perfil de ocultamiento de topología**, seleccione el perfil de ocultamiento de topología creado para extensiones remotas de IP Office.

3. Haga clic en **Terminar**.
4. Si admite extensiones remotas IPv4 e IPv6, repita el proceso para crear las entradas IPv6.

Pasos siguientes

- Vaya a Agregar proxys inversos para solicitudes de archivos en la página 57.

Vínculos relacionados

Configuración de ASBCE para extensiones SIP remotas en la página 25

Agregar proxys inversos para solicitudes de archivos

El siguiente es un ejemplo para crear proxys inversos para extensiones remotas. Estos permiten que las extensiones remotas soliciten archivos de IP Office. Por ejemplo, solicitar los archivos `46xxspecials.txt` y `46xxsettings.txt`.

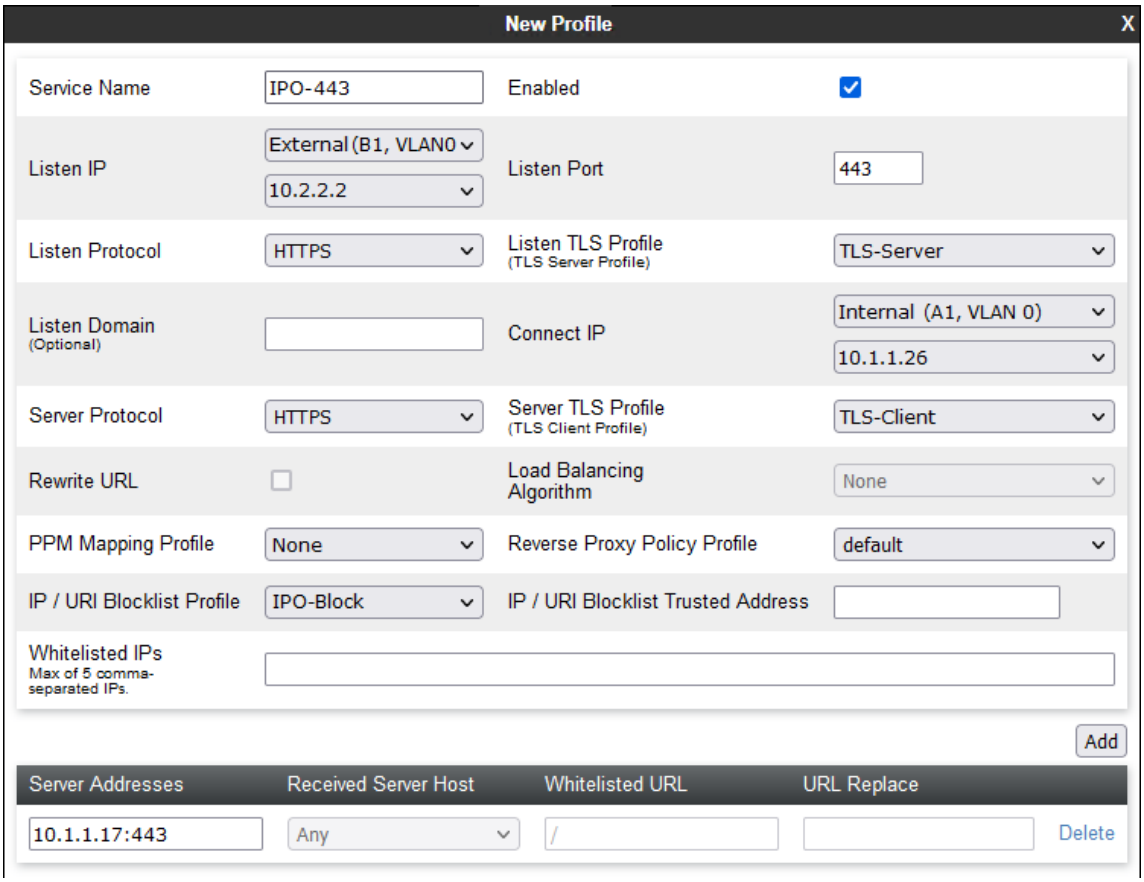
Los puertos y el protocolo requeridos dependen de los requisitos del tipo de extensión remota.

- De manera predeterminada, para la conexión inicial al IP Office para solicitar el archivo `46xxsettings.txt`, las extensiones utilizan `http` o `https`. IP Office utiliza puerto `80` y puerto `443` respectivamente.
- La configuración `46xxsettings.txt` le indica a la extensión remota qué puertos y protocolos utilizar para conexiones futuras.
- Si **Sistema** > **Sistema** > **Usar puertos de teléfono preferidos** está habilitado, `46xxsettings.txt` indica a los teléfonos y clientes que utilicen el puerto `8411` para solicitudes de archivos HTTP y el puerto `411` para solicitudes de archivos HTTPS, y esos puertos están habilitados en IP Office.
  - Con **Usar puertos de teléfono preferidos** habilitado, IP Office aún permite conexiones en el puerto `80` y el puerto `443`. IP Office requiere esto para la conexión inicial y para clientes heredados.
- **Compatibilidad con IPv4/IPv6 dual:** para admitir extensiones remotas IPv4 e IPv6, debe crear entradas separadas para IPv4 e IPv6. Cada una usando las interfaces externas IPv4 e IPv6 respectivas.

Procedimiento

1. Seleccione **Configuración específica del dispositivo** > **Servicios DMZ** > **Servicios de relé**.

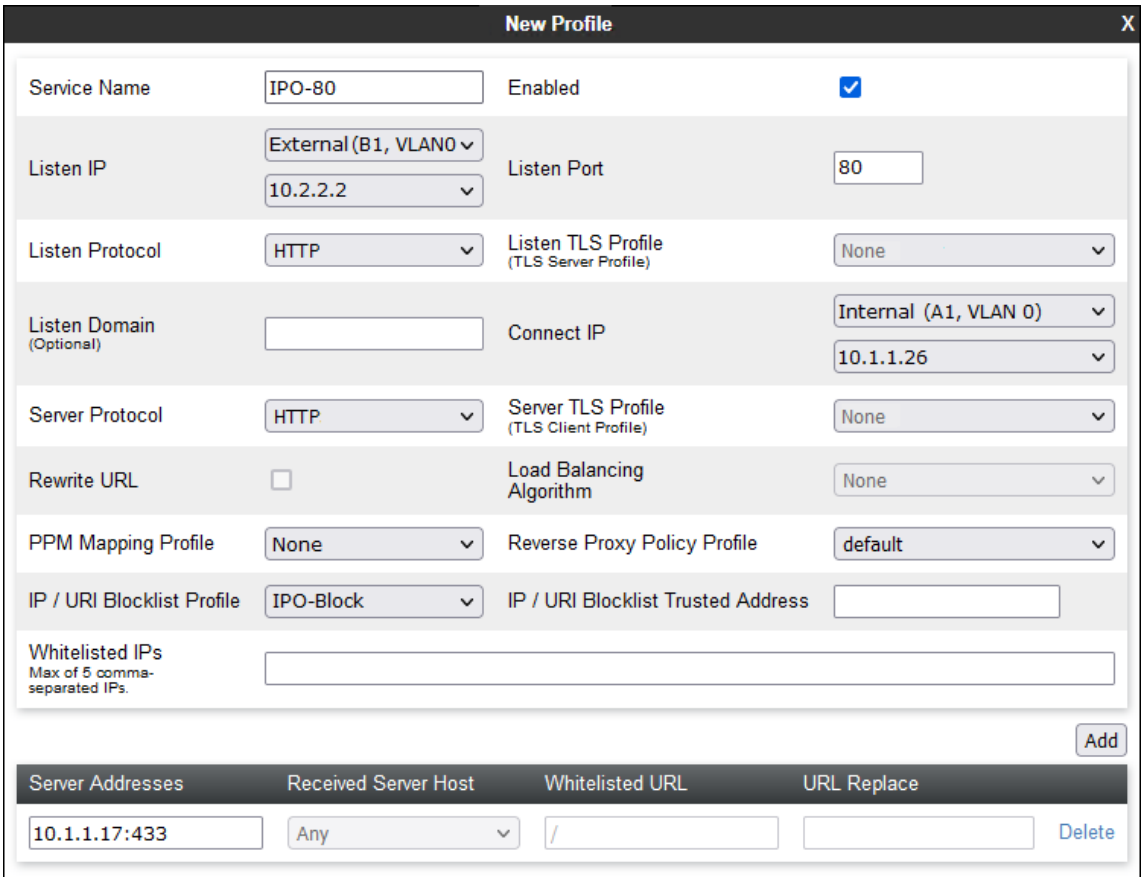
2. Seleccione la pestaña **Proxy inverso** y haga clic en **Agregar**.



   a. En **Nombre de servicio** ingrese un nombre descriptivo para el proxy inverso.
   b. En **Escucha IP**, seleccione la interfaz *B1* externa y la dirección IP.
   c. Establezca **Puerto de escucha** en `443`.
   d. Establezca **Protocolo de escucha** en **HTTPS**.
   e. En **Perfil de TLS de escucha**, seleccione el perfil del servidor TLS.
   f. En **IP de conexión**, seleccione la interfaz *A1* interna y la dirección IP.
   g. En **Servidor de protocolo**, seleccione **HTTPS**.
   h. En **Perfil de servidor TLS**, seleccione el perfil del cliente TLS.
   i. Si creó una lista de bloqueo, selecciónela usando el **Perfil de lista de bloqueo de IP/URI** menú desplegable.
   j. Haga clic en **Agregar**:
   k. Para **Dirección del servidor**, ingrese la dirección IP de IP Office seguida de `:443`.

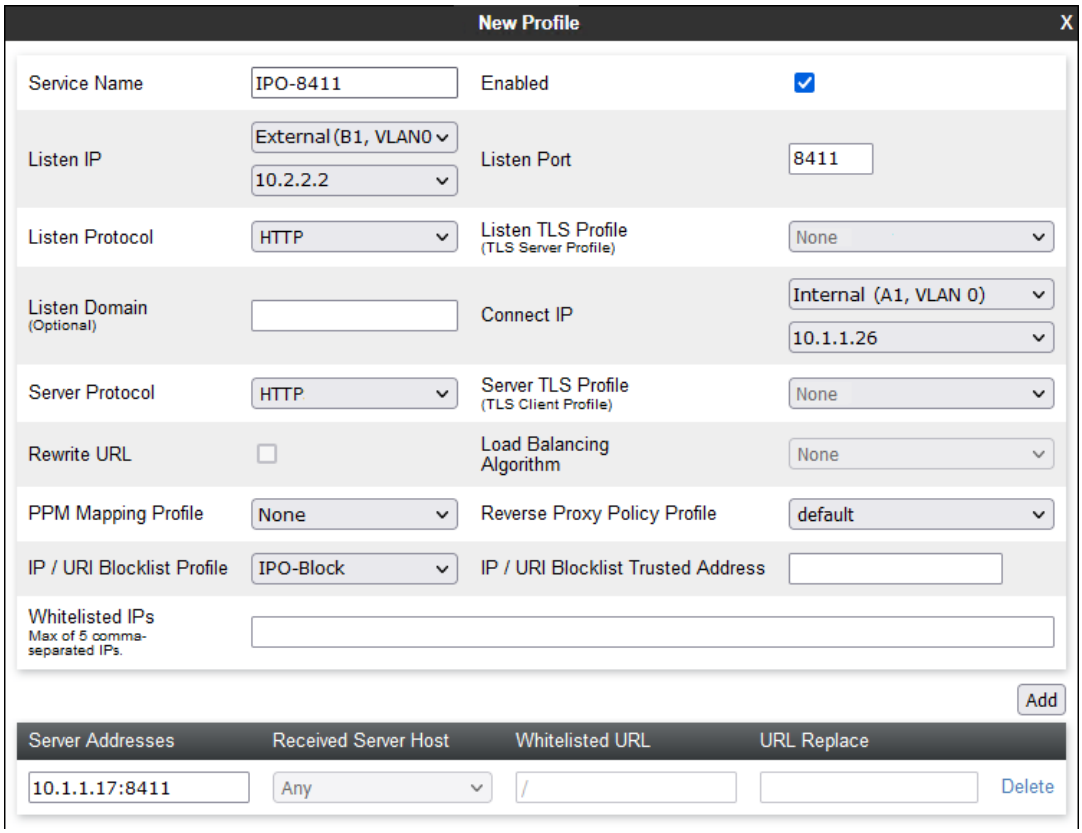
3. Haga clic en **Terminar**.

4. Repita el procedimiento para agregar un proxy para solicitudes de archivo HTTP de puerto `80`. Este proxy no utiliza ningún perfil TLS.

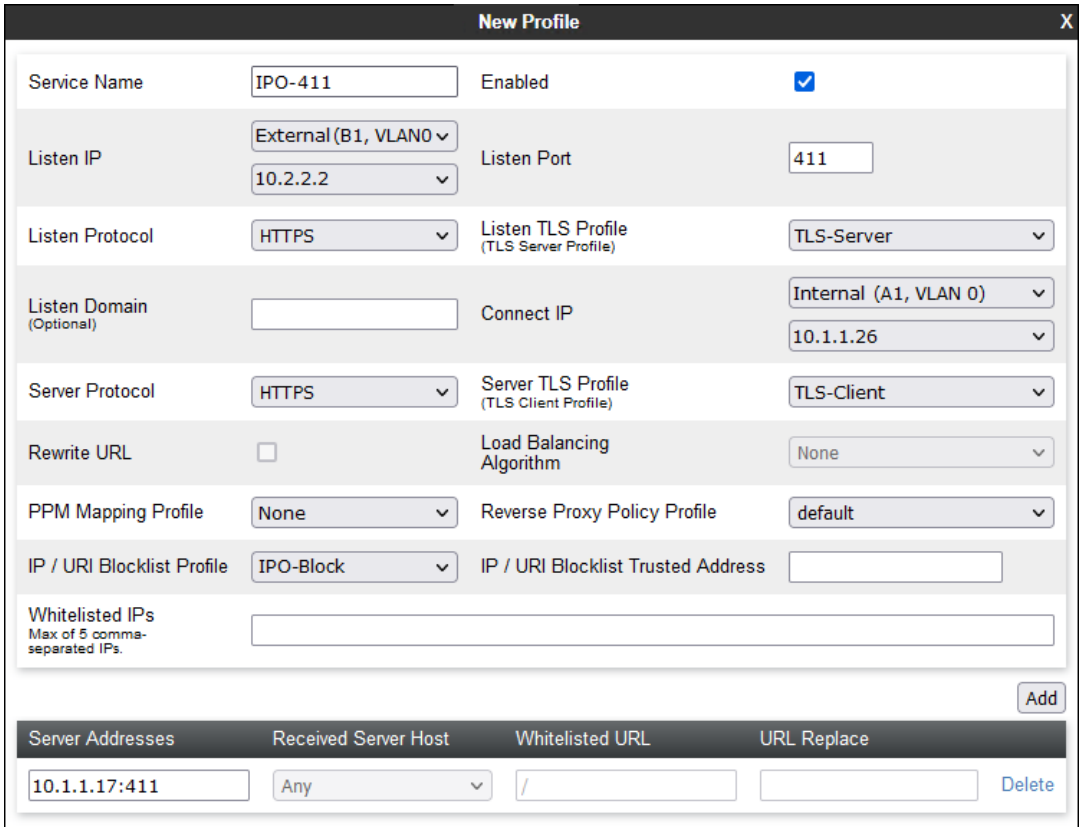


5. Haga clic en **Terminar**.

6. Si **Usar puertos de teléfono preferidos** está habilitado en IP Office:
   a. Agregue un proxy inverso para HTTP en el puerto `8411`.



b. Agregue un proxy inverso para HTTPS en el puerto `411`.



7. Si admite extensiones remotas IPv4 e IPv6, repita el proceso para crear las entradas IPv6.

Vínculos relacionados

Configuración de ASBCE para extensiones SIP remotas en la página 25

Capítulo 5: Anulación de anclaje de medios de llamada desde el ASBCE

ASBCE normalmente sigue siendo parte de todas las llamadas que enruta. Todos los medios de llamada y la señalización de llamadas permanecen anclados al ASBCE y, por lo tanto, requieren ancho de banda y procesamiento desde el ASBCE.

En escenarios donde las redes involucradas admiten el enrutamiento directo entre todos los extremos de la llamada, puede desanclar los medios de llamada desde ASBCE. La cancelación de anclaje reduce el ancho de banda y los recursos requeridos por el ASBCE. El ASBCE sigue manejando la señalización de llamadas.

- Para extensiones remotas en la misma subred remota, al desanclar el ASBCE permite medios directos entre las extensiones remotas en esa subred.
- También puede utilizar la anulación de anclaje en otros escenarios. Por ejemplo, entre extensiones remotas en dos subredes separadas. Para obtener más información, consulte https://documentation.avaya.com/bundle/GUID-416B16B1-7DB4-4C01-A966-3E62EFEA4D43/page/Media_Unanchoring_scenarios.html.

La anulación de anclaje utiliza los siguientes elementos de configuración de ASBCE adicionales:

- **Flujo de sesión**

  Un flujo de sesión define un par de rangos de direcciones de red y qué política de sesión el ASBCE debe aplicar para el tráfico entre esas redes. Para medios directos en un sitio remoto, el rango de direcciones de sitios se configura para ambas redes en el flujo de sesión.

- **Política de sesión**

  Una política de sesión establece cómo el ASBCE debe tratar los medios de llamada. Puede utilizar la misma política de sesión para varios flujos de sesión.

Vínculos relacionados

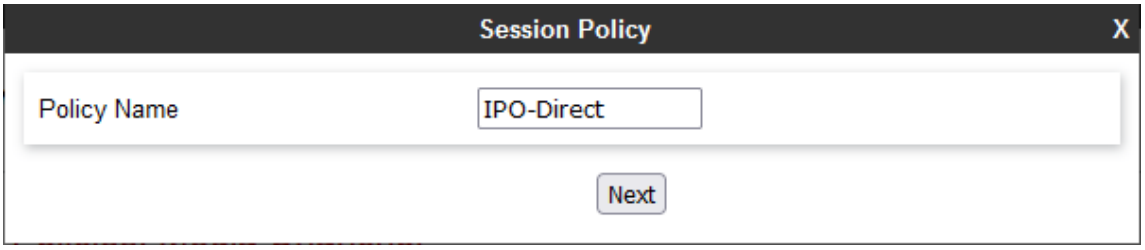
Creación de una política de sesión para un sitio remoto en la página 62
Creación de un flujo de sesión para el sitio remoto en la página 64

Creación de una política de sesión para un sitio remoto

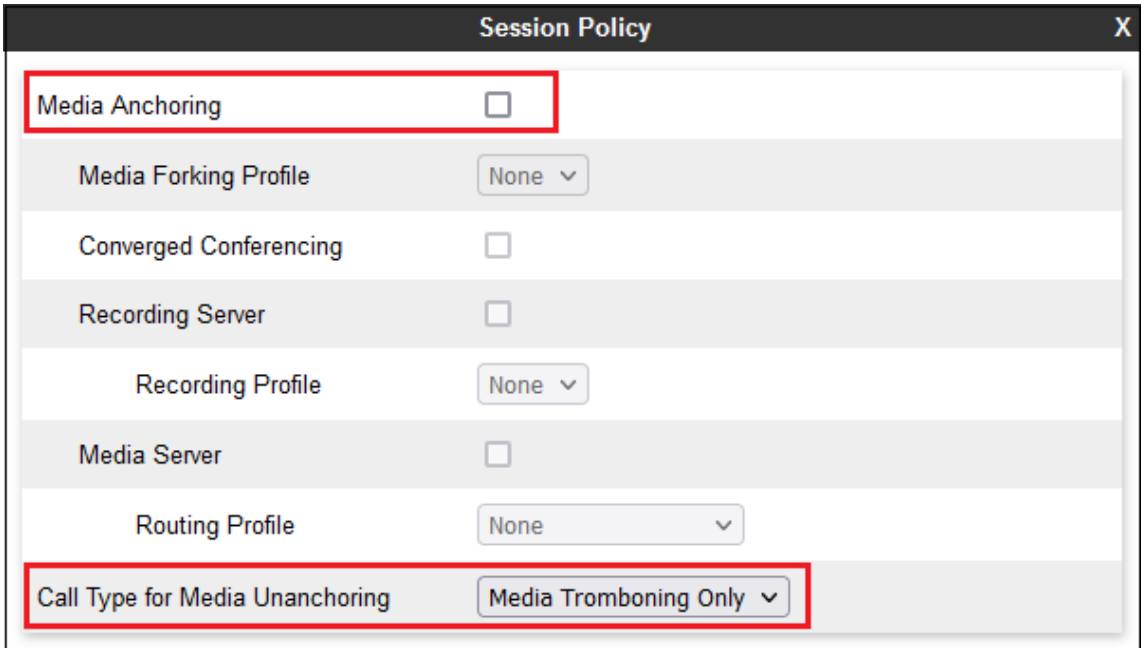
Una política de sesión establece cómo el ASBCE debe tratar el tráfico entre sitios coincidentes con cualquier flujo de sesión que utilice la política. Puede utilizar la misma política para múltiples flujos de sesión. Es decir, para múltiples sitios remotos.

Procedimiento

1. Seleccione **Políticas de dominio** > **Políticas de sesión**.
2. Haga clic en **Agregar**.
3. Introduzca un nombre. Luego, puede utilizar esto para seleccionar la política en otros menús.



4. Haga clic en **Siguiente**.



5. Cancele la selección de **Anclaje de medios**.
6. Establezca **Tipo de llamada para desanclar medios** en **Solo tromboning de medios**.
7. Haga clic en **Terminar**.

Pasos siguientes

- Vaya a Creación de un flujo de sesión para el sitio remoto en la página 64.

Vínculos relacionados

Anulación de anclaje de medios de llamada desde el ASBCE en la página 62

Creación de un flujo de sesión para el sitio remoto

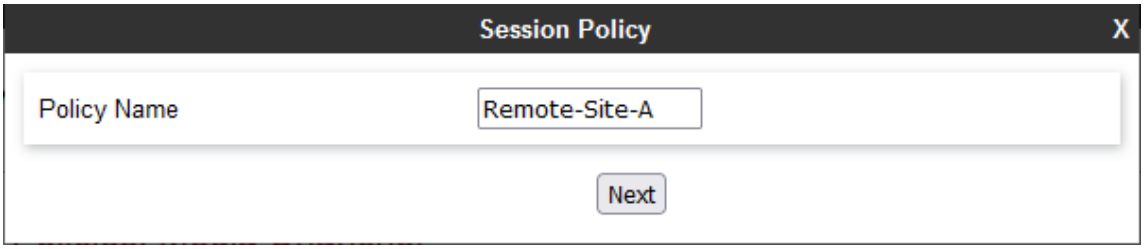
Un flujo de sesión define intervalos de direcciones entre los cuales el ASBCE debe aplicar una política de sesión. Para una subred remota, los intervalos de dirección en ambos lados son los mismos.

Antes de empezar

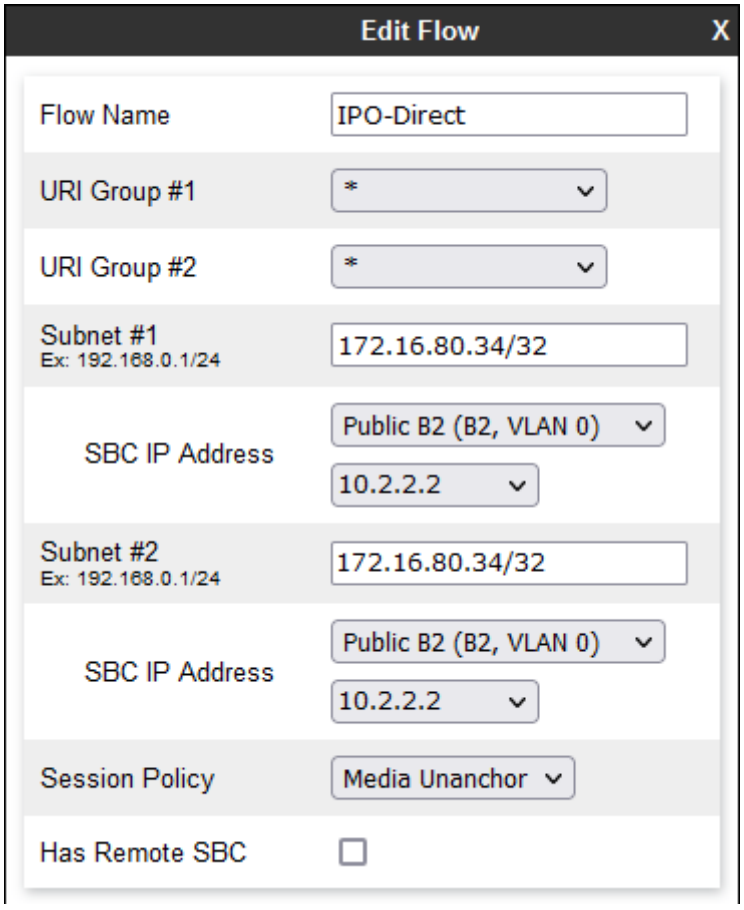
- Creación de una política de sesión para un sitio remoto en la página 62.

Procedimiento

1. Seleccione **Red y flujos** > **Flujos de sesión**.
2. Haga clic en **Agregar**.
3. Introduzca un nombre. Luego, puede utilizar esto para seleccionar la política en otros menús.



4. Haga clic en **Siguiente**.



5. Para **Subred#1** configure el rango de direcciones IP utilizado por extensiones remotas en el sitio remoto. Configure la **Dirección IP SBC** en la interfaz externa del ASBCE.
6. Establezca los mismos valores para **Subred#2**.
7. Para **Política de sesión**, seleccione la política de sesión que creó.
8. Haga clic en **Terminar**.

Vínculos relacionados

Anulación de anclaje de medios de llamada desde el ASBCE en la página 62

Capítulo 6: Compatibilidad con Client Avaya Workplace como extensión remota

Esta sección proporciona notas sobre el funcionamiento de Client Avaya Workplace cuando se utiliza como extensión SIP remota para IP Office.

Vínculos relacionados

[Registro SIP de Client Avaya Workplace](#) en la página 66
[Verificación de la configuración remota](#) en la página 67

Registro SIP de Client Avaya Workplace

1. Los usuarios pueden utilizar los siguientes métodos para registrar su Client Avaya Workplace cuando se inicia:
   - **Registro directo:**

     El usuario ingresa la dirección de IP Office de la forma `https://<IPOffice_FQDN>/46xxsettings.txt` cuando `://<IPOffice_FQDN>/` es el FQDN del registrador SIP configurado en IP Office.
     - Para extensiones remotas, DNS público resuelve el FQDN a la dirección IP pública del firewall de la red del cliente.
     - Para IPv6, el usuario debe utilizar `https://<SBC_FQDN>/46xxsettings.txt` donde <SBC_FQDN> es el FQDN del ASBCE.
   - **Registro de dirección basado en correo electrónico:**

     El usuario ingresa su dirección de correo electrónico. El cliente se comunica con Avaya Spaces, donde el perfil configurado para el dominio de correo electrónico del cliente proporciona la dirección FQDN del sistema IP Office.
     - Este método de registro no es compatible con extensiones remotas IPV6.
   - **Inicio de sesión de SSO**

     Este método de inicio de sesión utilizó la misma información de perfil de Avaya Spaces que el registro basado en correo electrónico anterior.
     - Este método de registro no es compatible con extensiones remotas IPV6.

2. Después de recibir un archivo `46xxsettings.txt` desde IP Office, Client Avaya Workplace envía una consulta DNS para la dirección IP del FQDN que se le proporcionó en **SIP_CONTROLLER_LIST** en el archivo `46xxsettings.txt`.
   - Para extensiones remotas, los valores utilizados en el archivo `46xxsettings.txt` generado automáticamente se establecen en los ajustes de **Sistema** > **LAN1** > **Topología de red** > **SBC** en la configuración de IP Office.
3. El cliente luego intenta registrarse como una extensión SIP usando la dirección IP devuelta por el servidor DNS. Para una extensión remota, esa es la dirección IP pública del cliente para su firewall de red o ASBCE.

Vínculos relacionados

[Compatibilidad con Client Avaya Workplace como extensión remota](#) en la página 66

Verificación de la configuración remota

Con una PC remota, puede ver y verificar la configuración dada a las extensiones remotas.

Procedimiento

1. Utilice **nslookup** para verificar que DNS resuelve el FQDN para IP Office a las direcciones IP correctas.

```
C:\ nslookup ipo.example.com
Server:  Unknown
Address: 203.0.113.30
```

2. Con un navegador, solicite el archivo `46xxsettings.txt` desde IP Office. Por ejemplo, ingrese `ipo.example.com/46xxsettings.txt`.
3. Verifique el rango de puertos que se muestra. Client Avaya Workplace puede utilizar puertos RTP/RTCP en el rango `40750 to 50750`.

```
# SIPXAUTOGENERATEDSETTINGS
IF $SIG_IN_USE SEQ H323 GOTO 96X1AUTOGENERATEDSETTINGS
SET RTP_PORT_LOW 40750
SET RTP_PORT_RANGE 10002
SET TLSSRVRID 1
```

4. Otros ajustes muestran los valores que utiliza Client Avaya Workplace para conectarse a servicios de IP Office:

```
# K1EXAUTOGENERATEDSETTINGS
SET ENABLE_AVAYA_CLOUD_ACCOUNTS 1
SET SIP_CONTROLLER_LIST ipo.example.com:5061;transport=tls
SET CONFERENCE_FACTORY_URI "ConfServer@ipo.example.com"
SET PSTN_VM_NUM "VM.user@ipo.example.com"
SET SETTINGS_FILE URL "https://ipo.example.com:411/46xxsettings.txt"
SET FQDN IP MAP "ipo.example.com=10.1.1.17"
```

5. Para contactos y servicios de presencia, verifique si los valores `IPO_PRESENCE_ENABLED` y `IPO_CONTACTS_ENABLED` están configurados en `1`.

```
# SETTINGSK1EX
SET SSOENABLED 0
SET EWSSSO 0
SET SIPREGPROXYPOLICY "alternate"
SET IPO_PRESENCE_ENABLED 1
SET IPO_CONTACTS_ENABLED 1
SET DND_SAC_LINK 1
SET POUND_KEY_AS_CALL_TRIGGER 0
```

Vínculos relacionados

Compatibilidad con Client Avaya Workplace como extensión remota en la página 66

Capítulo 7: Verificación del estado de la extensión remota en el ASBCE

ASBCE proporciona un conjunto de menús que muestran el estado de las conexiones e intenta crear conexiones.

Vínculos relacionados

Visualización de estadísticas SIP del ASBCE en la página 69
Visualización de estadísticas de usuario de ASBCE en la página 70
Visualización de incidentes de ASBCE en la página 71

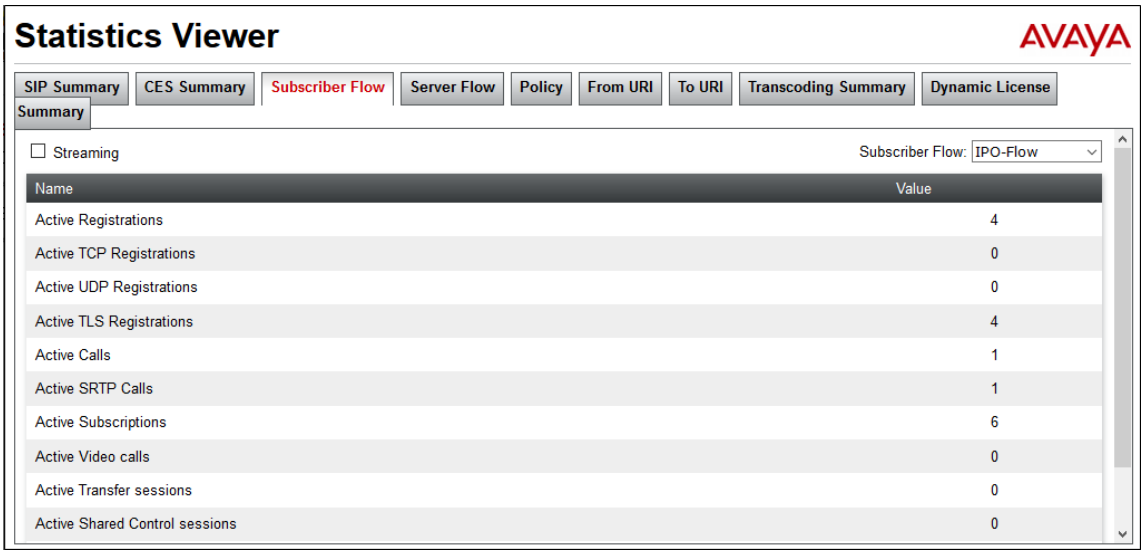
Visualización de estadísticas SIP del ASBCE

Visor de estadísticas puede mostrar detalles sobre el número de conexiones y llamadas de extensión remota.

Procedimiento

1. Seleccione **Estado** > **Estadísticas SIP**
2. Seleccione **Flujo de suscriptor** y en el menú desplegable seleccione el flujo creado para extensiones remotas.

3. El visor muestra detalles como el número de registros, el número de llamadas, etc.



Vínculos relacionados

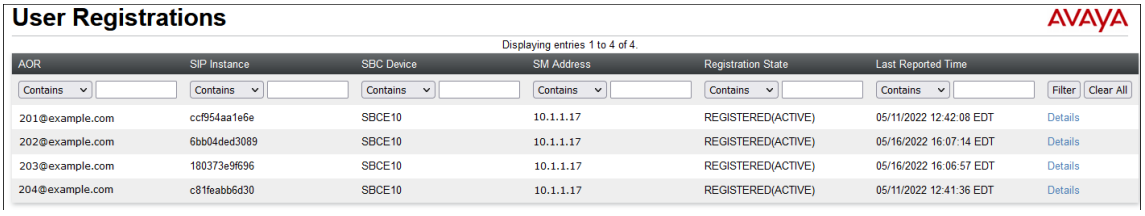
[Verificación del estado de la extensión remota en el ASBCE](#) en la página 69

Visualización de estadísticas de usuario de ASBCE

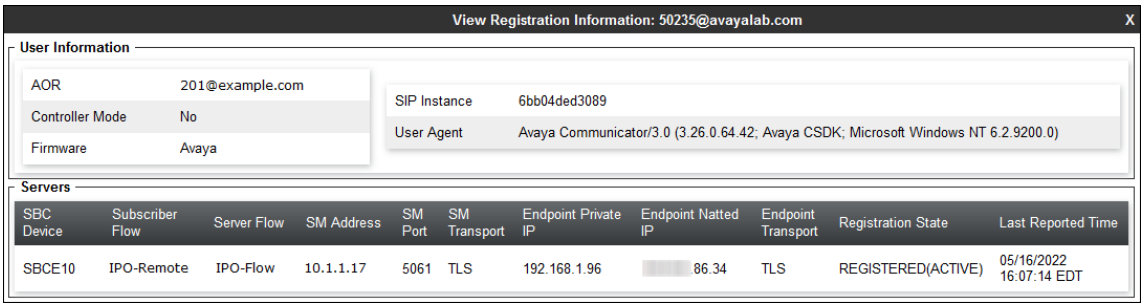
Visor de estadísticas puede mostrar detalles de extensiones remotas individuales.

Procedimiento

1. Seleccione **Estado** > **Registros de usuario**
2. El visor muestra detalles de clientes SIP registrados a través del ASBCE.



3. Para mostrar información adicional para un usuario en particular, haga clic en **Detalles**.



Vínculos relacionados

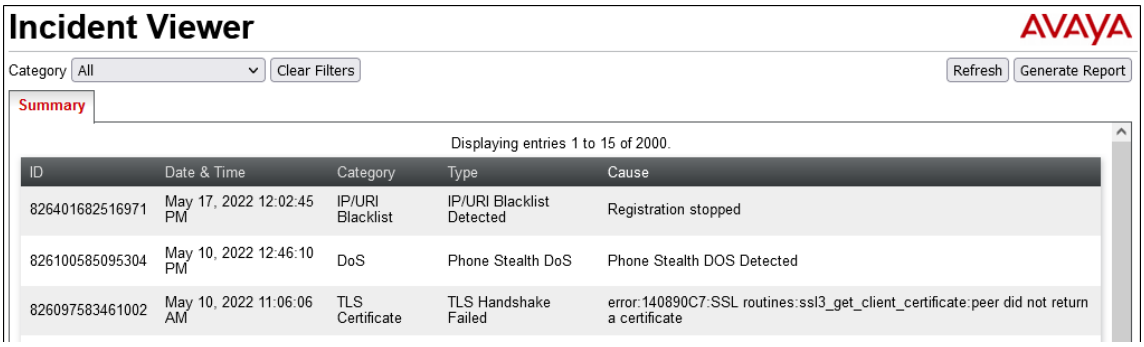
Verificación del estado de la extensión remota en el ASBCE en la página 69

Visualización de incidentes de ASBCE

El ASBCE puede mostrar detalles de problemas como errores de certificado y problemas de registro. Si las extensiones remotas experimentan problemas al conectarse a IP Office, esto puede mostrar el motivo si el problema en el ASBCE.

Procedimiento

1. Seleccione **Incidentes**.
2. El visor muestra los detalles de los incidentes.



Vínculos relacionados

Verificación del estado de la extensión remota en el ASBCE en la página 69

Parte 2: Compatibilidad con IPv6

Capítulo 8: Compatibilidad con extensiones remotas IPv6

Para IP Office R11.1.3.1 y versiones posteriores, IP Office admite extensiones remotas de Client Avaya Workplace en iOS y Android usando IPv6.

Vínculos relacionados

Compatibilidad con extensión remota IPv6 en la página 73
Esquema de extensión remota IPv6 en la página 74
Limitaciones de extensión remota IPv6 en la página 74
Configuración DNS para compatibilidad con extensiones remotas IPv6 en la página 75
Configuración de certificado para compatibilidad con extensiones remotas IPv6 en la página 75
Configuración de Avaya Spaces para compatibilidad con extensiones remotas IPv6 en la página 76
Lista de verificación de configuración para extensiones remotas IPv6 en la página 76
Lista de verificación de configuración para extensiones remotas IPv4 e IPv6 combinadas en la página 77

Compatibilidad con extensión remota IPv6

Para IP Office R11.1.3.1 y versiones posteriores, el teléfono móvil remoto Client Avaya Workplace puede utilizar IPv6.

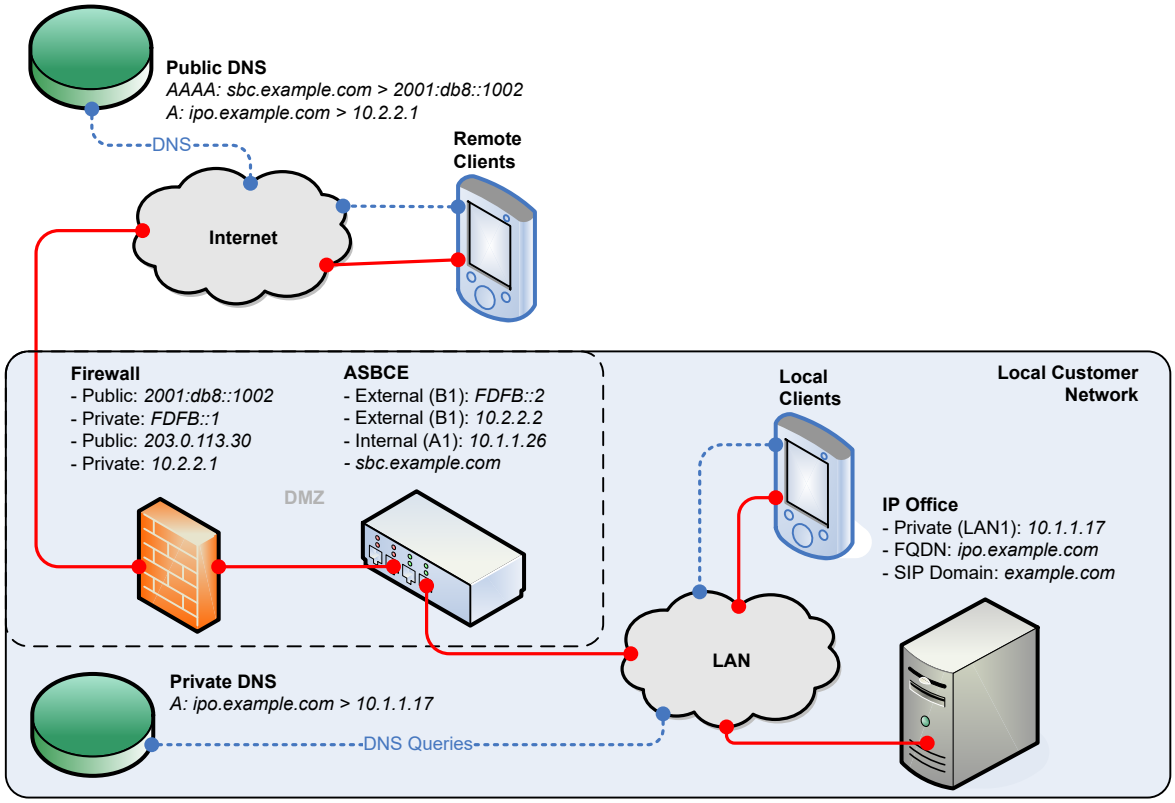
- Puede configurar IP Office para que proporcione al teléfono móvil remoto Client Avaya Workplace el FQDN del ASBCE en el archivo `46xxsettings.txt` generado automáticamente.
- La conexión requiere un ASBCE R10.1.2 instalado en una instalación de doble pila. El ASBCE realiza el enrutamiento entre los clientes IPv6 e IP Office IPv4.
- Client Avaya Workplace:
  - iOS: Client Avaya Workplace R3.35 y posteriores.
  - Android: Client Avaya Workplace R3.35.1 y posteriores.
  - Los dispositivos iPad y Vantage no están incluidos en la compatibilidad con IPv6.
- Los clientes y teléfonos SIP en la red privada del cliente aún utilizan IPv4 para conectarse directamente a IP Office.
- Si la red a la que Client Avaya Workplace está conectado admite IPv4 e IPv6, el Client Avaya Workplace predeterminado es IPv4.

Vínculos relacionados

Compatibilidad con extensiones remotas IPv6 en la página 73

Esquema de extensión remota IPv6

El siguiente esquema es un ejemplo para admitir extensiones remotas IPv6.



- IP Office proporciona a las extensiones remotas el FQDN del ASBCE.
- El DNS público resuelve el FQDN del ASBCE a la dirección IPv6 pública del firewall del cliente.
- El firewall reenvía los puertos utilizados por las extensiones remotas a la interfaz externa del ASBCE.
- La doble pila ASBCE maneja el enrutamiento entre direcciones IPv6 e IPv4.
- Para extensiones internas, el DNS privado resuelve el FQDN de a la dirección IPv4 del IP Officesistema de IP Office.

Vínculos relacionados

Compatibilidad con extensiones remotas IPv6 en la página 73

Limitaciones de extensión remota IPv6

- Si bien existe firmware para el funcionamiento de IPv6 de los teléfonos de la serie J100, deben utilizar IPv4 para la conexión de extensión remota a IP Office.

- Avaya Spaces no es compatible con IPv6. Por lo tanto, un Client Avaya Workplace que utiliza IPv6 no admite funciones proporcionadas por Avaya Spaces. Por ejemplo:
  - No hay registro de cliente usando correo electrónico o inicio de sesión SSO.
  - Sin mensajería instantánea si IP Office está configurado para usar Avaya Spaces como su servidor de mensajería.
- Si la red a la que Client Avaya Workplace está conectado admite IPv4 e IPv6, el Client Avaya Workplace predeterminado es IPv4.

Vínculos relacionados

Compatibilidad con extensiones remotas IPv6 en la página 73

Configuración DNS para compatibilidad con extensiones remotas IPv6

Para admitir IPv6, el DNS debe resolver el FQDN del ASBCE además del FQDN de IP Office:

- El DNS público para el FQDN de IP Office aún debe resolverse a una dirección IPv4.
- El DNS público también debe resolver el FQDN del ASBCE a una dirección IPv6. Para ello, el cliente debe agregar registros `AAAA` a su servicio DNS público.
- Las extensiones locales continúan conectándose directamente a IP Office usando direcciones IPv4. Esto lo resuelve el DNS privado del cliente.

Vínculos relacionados

Compatibilidad con extensiones remotas IPv6 en la página 73

Configuración de certificado para compatibilidad con extensiones remotas IPv6

Cuando se admiten extensiones remotas IPv6, además de la dirección FQDN e IPv4 de IP Office, el certificado de identidad del ASBCE debe incluir la dirección FQDN e IPv6 del ASBCE.

- El FQDN del ASBCE puede agregarse como parte del nombre común (CN) del certificado o el nombre alternativo del asunto (SAN).
- La dirección IPv6 debe agregarse al SAN.

Vínculos relacionados

Compatibilidad con extensiones remotas IPv6 en la página 73

Configuración de Avaya Spaces para compatibilidad con extensiones remotas IPv6

Avaya Spaces no es compatible con IPv6. Por lo tanto, un Client Avaya Workplace que utiliza IPv6 no admite funciones proporcionadas por Avaya Spaces. Por ejemplo:

- No hay registro de cliente usando correo electrónico o inicio de sesión SSO.
- Sin mensajería instantánea si IP Office está configurado para usar Avaya Spaces como su servidor de mensajería.

Página de inicio de sesión en blanco

Si no deshabilita la compatibilidad con SSO, al iniciar sesión, usuarios del cliente IPv6, verán una página en blanco. Para iniciar sesión, debe cerrar la página en blanco y luego iniciar sesión directamente usando la dirección de archivo IP Office `46xxsettings.txt`.

- Si desea que los usuarios del cliente IPv4 aún puedan utilizar SSO, debe indicar a los usuarios de la extensión remota IPv6 que cierren la página en blanco e inicien sesión con la dirección de archivo IP Office `46xxsettings.txt`.
- De lo contrario, para evitar que la página en blanco se inicie cuando el usuario inicia Client Avaya Workplace, debe agregar un archivo `46xxspecials.txt` con la configuración `SET SIPSSO 0` a IP Office. Tenga en cuenta que esto afectará a todos los usuarios de Client Avaya Workplace.

```
...
SETTINGSEQNX
SET SIPSSO 0
GOTO GENERALSPECIALS
```

Vínculos relacionados

Compatibilidad con extensiones remotas IPv6 en la página 73

Lista de verificación de configuración para extensiones remotas IPv6

Si solo admite extensiones remotas IPv6, siga el mismo proceso de configuración que para IPv4, pero reemplace las direcciones IPv4 externas con direcciones IPv6 cuando corresponda. Vea Configuración de ASBCE para extensiones SIP remotas en la página 25.

#	Acción	Vínculo/notas	✔
1.	Configurar compatibilidad con DNS público para IPv6	DNS debe resolver el FQDN del ASBCE a la dirección IPv6 para el tráfico al ASBCE. Vea Configuración DNS para compatibilidad con extensiones remotas IPv6 en la página 75.	
2.	Incluya el FQDN del ASBCE y la dirección IPv6 en el certificado de identidad del ASBCE.	Vea Configuración de certificado para compatibilidad con extensiones remotas IPv6 en la página 75.	

La tabla continúa…

#	Acción	Vínculo/notas	✔
3.	Deshabilitar compatibilidad con Avaya Spaces.	Vea Configuración de Avaya Spaces para compatibilidad con extensiones remotas IPv6 en la página 76.	
4.	Configure la dirección IPv6 pública en IP Office	Debe proporcionar a las extensiones remotas la dirección IPv6 para utilizar para el registro y las llamadas SIP. Vea Configurar los detalles del ASBCE transmitidos a extensiones remotas por el IP Office en la página 13.	
5.	Configurar el flujo de llamada del ASBCE	Siga el mismo proceso de configuración de ASBCE utilizado para IPv4 pero usando direcciones IPv6 cuando corresponda. Vea Lista de verificación de la configuración de ASBCE en la página 28.	

Vínculos relacionados

Compatibilidad con extensiones remotas IPv6 en la página 73

Lista de verificación de configuración para extensiones remotas IPv4 e IPv6 combinadas

Esta lista de verificación asume que ha completado la configuración de ASBCE para admitir extensiones remotas IPv4. Vea Lista de verificación de la configuración de ASBCE en la página 28. Las notas indican dónde el ASBCE requiere configuración adicional para admitir extensiones remotas IPv4 e IPv6.

#	Acción	Vínculo/notas	✔
1.	Configurar compatibilidad con DNS público para IPv6	DNS debe resolver el FQDN del ASBCE a la dirección IPv6 para el tráfico al ASBCE. Vea Configuración DNS para compatibilidad con extensiones remotas IPv6 en la página 75.	
2.	Incluya el FQDN del ASBCE y la dirección IPv6 en el certificado de identidad del ASBCE.	La identidad del ASBCE debe incluir el FQDN de IP Office y la dirección IPv4, más el FQDN del ASBCE y la dirección IPv6. Vea Configuración de Avaya Spaces para compatibilidad con extensiones remotas IPv6 en la página 76.	
3.	Deshabilitar compatibilidad con Avaya Spaces.	Avaya Spaces no es compatible con IPv6. Vea Configuración de Avaya Spaces para compatibilidad con extensiones remotas IPv6 en la página 76.	

La tabla continúa…

#	Acción	Vínculo/notas	✔
4.	Configure la dirección IPv6 pública en IP Office	Debe proporcionar a las extensiones remotas la dirección IPv6 para utilizar para el registro y las llamadas SIP. Vea Configurar los detalles del ASBCE transmitidos a extensiones remotas por el IP Office en la página 13.	
5.	Configurar reenvío de puertos de firewall	Agregue una nueva entrada, como la entrada IPv4, pero usando las direcciones IPv6 cuando corresponda. Vea Configuración de firewall en la página 30.	
6.	Configurar la interfaz de red de ASBCE externa	Agregue una nueva entrada para la interfaz externa pero usando las direcciones IPv6. Vea Configurar la interfaz de ASBCE externa en la página 31.	
7.	Configurar la interfaz de red de ASBCE interna	Utilice la entrada IPv4 existente. Vea Configurar la interfaz de ASBCE interna en la página 32.	
8.	Crear un perfil de cliente TLS	Utilice la entrada IPv4 existente. Vea Creación de un perfil de cliente TLS en la página 34.	
9.	Crear un perfil de servidor TLS	Utilice la entrada IPv4 existente. Vea Creación de un perfil de servidor TLS en la página 35.	
10.	Crear una interfaz de medios SIP interna	Utilice la entrada IPv4 existente. Vea Creación de una interfaz de medios interna en la página 37.	
11.	Crear una interfaz de medios SIP externa	Agregue una nueva entrada, como la entrada IPv4, pero usando las direcciones IPv6 cuando corresponda. Vea Creación de una interfaz de medios externa en la página 38.	
12.	Crear una interfaz de señalización de llamadas SIP interna	Utilice la entrada IPv4 existente. Vea Creación de una interfaz de señalización interna en la página 39.	
13.	Crear una interfaz de señalización de llamadas SIP externa	Agregue una nueva entrada, como la entrada IPv4, pero usando las direcciones IPv6 cuando corresponda. Vea Creación de la interfaz de señalización externa en la página 40.	
14.	Crear un perfil de servidor	Utilice la entrada IPv4 existente. Vea Creación de un perfil de servidor de ASBCE para el IP Office en la página 41.	

La tabla continúa…

#	Acción	Vínculo/notas	✔
15.	Crear enrutamiento del servidor	Utilice la entrada IPv4 existente. Vea Creación de un perfil de enrutamiento del servidor en la página 43.	
16.	Configurar ocultamiento de topología	Utilice la entrada IPv4 existente. Vea Creación de una política de ocultamiento de topología de ASBCE en la página 44.	
17.	Cree una lista de bloqueo de IP/URL.	Utilice la entrada IPv4 existente. Vea Creación de una lista de bloqueo de IP/URI en la página 45.	
18.	Crear una regla de aplicación	Utilice la entrada IPv4 existente. Vea Creación de una regla de aplicación en la página 46.	
19.	Crear una regla de medios	Utilice la entrada IPv4 existente. • Asegúrese de que **Opciones avanzadas** > **ANAT habilitada** no esté seleccionado. Vea Creación de una regla de medios en la página 47.	
20.	Crear una política de terminal	Utilice la entrada IPv4 existente. Vea Creación de un grupo de políticas de terminal en la página 50.	
21.	Agregar un perfil de agentes de usuario	Utilice la entrada IPv4 existente. Vea Configuración de un perfil de agentes de usuario en la página 51.	
22.	Crear un flujo de suscriptor	Agregue una nueva entrada, como la entrada IPv4: • Configure las interfaces de medios y señalización para utilizar las interfaces IPv6 externas. Vea Creación del flujo de suscriptor en la página 52.	
23.	Crear un flujo de servidor	Agregue una nueva entrada, como la entrada IPv4: • Configure la interfaz de señalización externa IPv6 como **Interfaz recibida**. Vea Creación de un flujo de servidor en la página 55.	
24.	Agregar un proxy inverso para Client Avaya Workplace	Agregue nuevos proxies usando la interfaz B1 externa configurada para direcciones IPv6. Vea Agregar proxys inversos para solicitudes de archivos en la página 57.	

Vínculos relacionados

Compatibilidad con extensiones remotas IPv6 en la página 73

Parte 3: Resiliencia

Capítulo 9: Resiliencia de ASBCE y IP Office

IP Office admite una gama de opciones de resiliencia, incluida la resiliencia para teléfonos SIP y aplicaciones de softphone SIP. Para obtener más información, consulte el manual IP Office Descripción general de la resistencia.

Esta sección de este documento proporciona una descripción general de la configuración adicional requerida para agregar compatibilidad con resiliencia a una configuración existente. Los pasos adicionales principales son los siguientes:

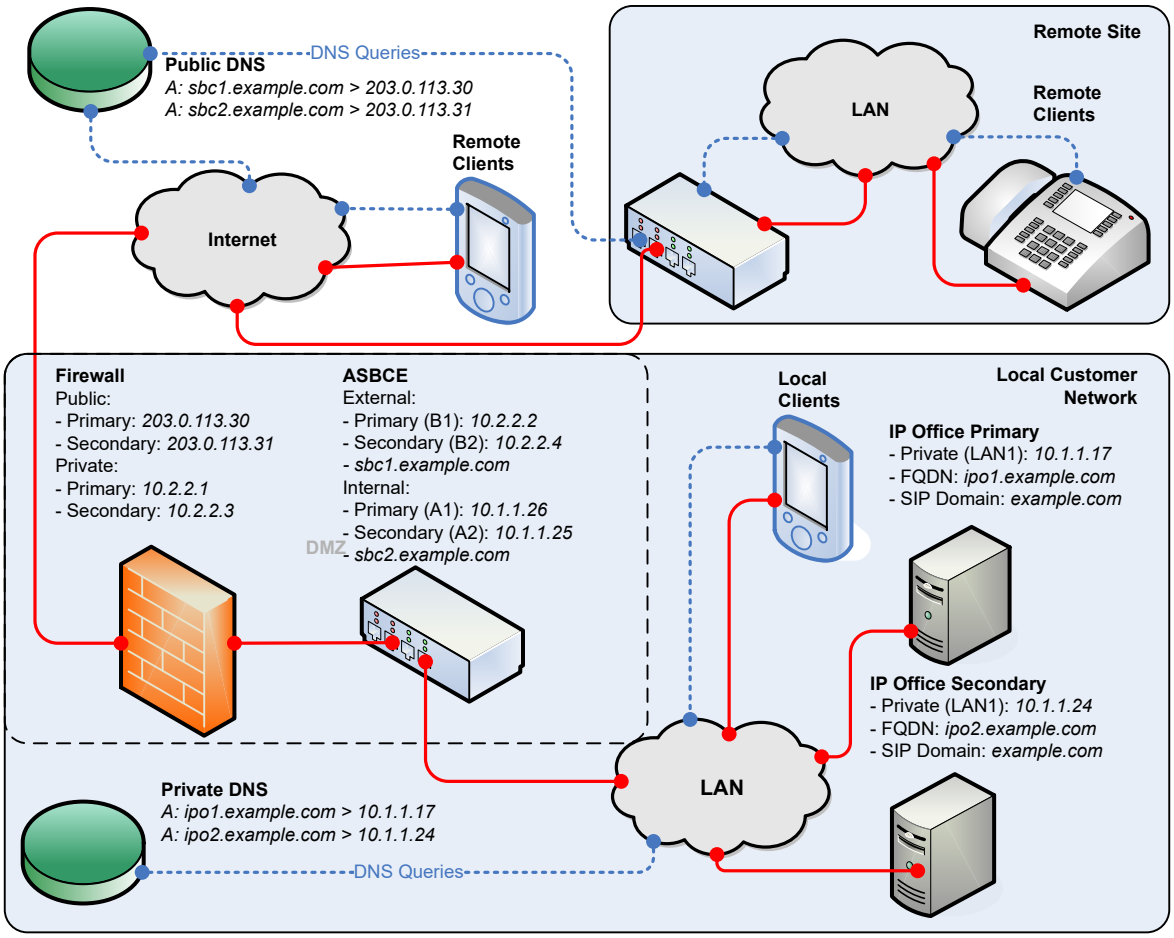
- IP Office no puede utilizar la dirección IP de la extensión remota para que coincida con una ubicación en la configuración de IP Office. Por lo tanto, para utilizar los ajustes de ubicación en resiliencia, debe configurar la ubicación en la configuración de extensión.

Vínculos relacionados

Ejemplo de esquema de resiliencia en la página 81
Generación de un certificado de identidad para el IP Office secundario en la página 82
Instalación del certificado de identidad de IP Office secundario en la página 83
Configuración de IP Office para resiliencia de extensión remota en la página 84
Configuración del Avaya one-X Portal en la página 84
Configuración del ASBCE para resiliencia en la página 85
Configuración de DNS para resiliencia en la página 85

Ejemplo de esquema de resiliencia

El siguiente es un esquema de ejemplo para una configuración resistente.



Para la compatibilidad resiliente de extensiones remotas, el ASBCE utiliza 2 conjuntos de direcciones IP públicas/privadas:

- El ASBCE enruta un grupo al servidor primario de IP Office y el otro grupo al servidor secundario de IP Office.
- Esta lógica es la misma independientemente de la instalación del ASBCE: Simplex, HA, dos servidores separados de ASBCE o doble pila.

Vínculos relacionados

Resiliencia de ASBCE y IP Office en la página 81

Generación de un certificado de identidad para el IP Office secundario

El IP Office secundario requiere un certificado de identidad emitido por el IP Office primario.

Procedimiento

1. Inicie sesión en los menús de IP Office Web Control de la siguiente manera:
   - Desde dentro de IP Office Web Manager, seleccione el servidor primario. Haga clic en ☰ y seleccione **Vista de plataforma**.

- Navegue hasta `https://<IP Office IP address>:7071` e inicie sesión.

2. Vaya a la pestaña **Configuración** y desplácese hacia abajo hasta **Certificados**.
3. Introduzca los siguientes datos:

Valor	Descripción
IP de máquina	Ingrese la dirección IP del servidor secundario.
Contraseña	Ingrese una contraseña para cifrar el certificado y la clave.
Nombre del asunto	Ingrese el FQDN del IP Office secundario.
Nombre(s) alternativo(s) del asunto	Enumerar el FQDN del IP Office secundario, el dominio XMPP secundario, el dominio SIP y las direcciones IP internas y externas del IP Office secundario.

4. Haga clic en **Regenerar** y **Aplicar**.
5. En la ventana emergente, haga clic en el enlace para descargar el certificado.
6. Haga clic en **Aceptar**.
7. Cambie el nombre del archivo descargado a `IPOSEC_ID.p12`.

Pasos siguientes

- Instalación del certificado de identidad de IP Office secundario en la página 83.

Vínculos relacionados

Resiliencia de ASBCE y IP Office en la página 81

Instalación del certificado de identidad de IP Office secundario

Debe agregar el certificado de identidad creado para el IP Office secundario.

Antes de empezar

- Generación de un certificado de identidad para el IP Office secundario en la página 82.

Procedimiento

1. Inicie sesión en el sistema con IP Office Web Manager.
   - Para un IP500 V2, ingrese la dirección del sistema seguida de `:8443/WebMgmtEE/WebManagerment.html`.
   - Para un servidor basado en Linux, ingrese la dirección del sistema seguida de `:7070/WebManagement/WebManagement.html`.
2. Vaya a **Administrador de seguridad** > **Certificados**.
3. Haga clic en el ícono junto al servidor secundario.
4. Haga clic en **Establecer**.
5. Navegue hasta el archivo de certificado de identidad y selecciónelo.
6. Ingrese la contraseña.
7. Haga clic en **Cargar**.

Vínculos relacionados

Resiliencia de ASBCE y IP Office en la página 81

Configuración de IP Office para resiliencia de extensión remota

Además de la configuración estándar para resiliencia (consulte IP Office Descripción general de la resistencia), debe configurar el IP Office secundario de la siguiente manera:

- Establezca la configuración del registrador SIP, excepto **FQDN de registrador SIP**, en la misma configuración que se utiliza en el servidor IP Office primario. Esto incluye hacer coincidir el **Nombre de dominio SIP**. Vea Configuración de SIP VoIP de IP Office en la página 11.
- Configure el **FQDN de registrador SIP** para que coincida con el FQDN configurado en DNS para enrutar el tráfico SIP al servidor IP Office secundario.
- Establezca la configuración de **SBC** en la que las extensiones remotas deben utilizar para conectarse al ASBCE configurado para enrutar llamadas SIP al ASBCE secundario. Vea Configurar los detalles del ASBCE transmitidos a extensiones remotas por el IP Office en la página 13.

Vínculos relacionados

Resiliencia de ASBCE y IP Office en la página 81

Configuración del Avaya one-X Portal

Debe configurar el servicio Avaya one-X Portal con el nombre de dominio del IP Office secundario.

Procedimiento

1. Inicie sesión en los menús del administrador de Avaya one-X Portal, ya sea:
   - Dentro de IP Office Manager, seleccione **Aplicaciones** > **one-X Portal** > .
   - Navegue hasta `https://<portal IP address>:9443/onexportal-admin.html` e inicie sesión como administrador.
2. Seleccione **Configuración** > **Nombre de dominio del host**.
   a. Configure el **Nombre de dominio de host secundario** en el FQDN del Avaya one-X Portal secundario.
   b. Haga clic en **Guardar**.
3. Haga clic en el ícono en la parte superior de los menús para reiniciar Avaya one-X Portal.

Vínculos relacionados

Resiliencia de ASBCE y IP Office en la página 81

Configuración del ASBCE para resiliencia

Los pasos de la configuración del ASBCE son como los de la configuración de un solo servidor. El requisito es crear entradas adicionales, pero usando las direcciones IP públicas y privadas del servidor secundario de IP Office.

Vínculos relacionados

Resiliencia de ASBCE y IP Office en la página 81

Configuración de DNS para resiliencia

La configuración del servidor DNS es como la de un solo servidor IP Office. DNS requiere registros adicionales del FQDN del servidor secundario IP Office y ASBCE.

Vínculos relacionados

Resiliencia de ASBCE y IP Office en la página 81

Capítulo 10: Verificación de la configuración de resiliencia

Puede utilizar los siguientes métodos para verificar la información de resiliencia que IP Office proporciona a las extensiones remotas.

Vínculos relacionados

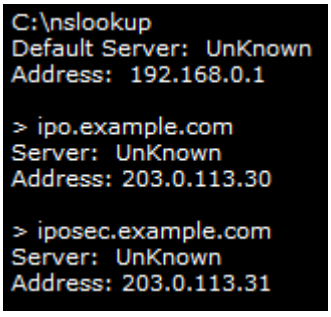
Verificación del enrutamiento DNS de resiliencia en la página 86
Visualización del seguimiento del ASBCE en la página 87
Verificación de las respuestas de Avaya one-X Portal en la página 88

Verificación del enrutamiento DNS de resiliencia

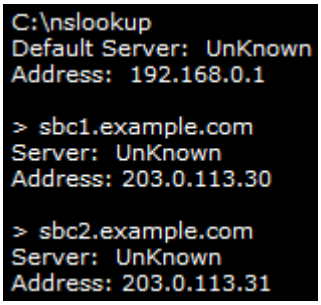
Con una PC remota, puede verificar que DNS esté resolviendo correctamente las solicitudes.

Procedimiento

1. Utilice el comando `nslookup` para verificar que DNS resuelva los FQDN del IP Office primario e IP Office secundario a las direcciones IP correctas. Por ejemplo:



2. Utilice el comando `nslookup` para verificar que DNS resuelva los FQDN del ASBCE primario y secundario.



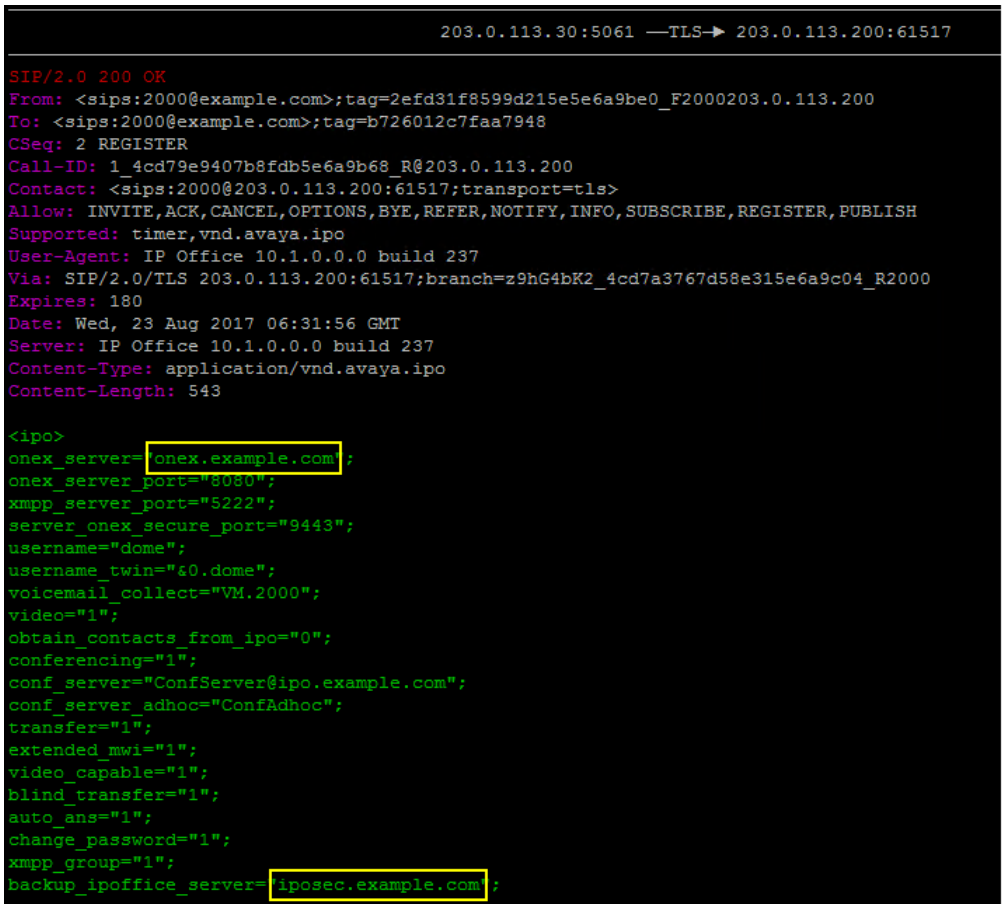
Vínculos relacionados

Verificación de la configuración de resiliencia en la página 86

Visualización del seguimiento del ASBCE

El siguiente es un ejemplo de sesión traceSBC para el registro de un cliente. Muestra la respuesta *200 OK* SIP enviada al cliente.

La respuesta contiene una cantidad de ajustes de configuración. Para extensiones remotas, la respuesta incluirá el FQDN de SBC que configuró en el IP Office secundario.



```
                                    203.0.113.30:5061 ──TLS─▶ 203.0.113.200:61517
SIP/2.0 200 OK
From: <sips:2000@example.com>;tag=2efd31f8599d215e5e6a9be0_F2000203.0.113.200
To: <sips:2000@example.com>;tag=b726012c7faa7948
CSeq: 2 REGISTER
Call-ID: 1_4cd79e9407b8fdb5e6a9b68_R@203.0.113.200
Contact: <sips:2000@203.0.113.200:61517;transport=tls>
Allow: INVITE,ACK,CANCEL,OPTIONS,BYE,REFER,NOTIFY,INFO,SUBSCRIBE,REGISTER,PUBLISH
Supported: timer,vnd.avaya.ipo
User-Agent: IP Office 10.1.0.0.0 build 237
Via: SIP/2.0/TLS 203.0.113.200:61517;branch=z9hG4bK2_4cd7a3767d58e315e6a9c04_R2000
Expires: 180
Date: Wed, 23 Aug 2017 06:31:56 GMT
Server: IP Office 10.1.0.0.0 build 237
Content-Type: application/vnd.avaya.ipo
Content-Length: 543

<ipo>
onex_server="onex.example.com";
onex_server_port="8080";
xmpp_server_port="5222";
server_onex_secure_port="9443";
username="dome";
username_twin="&0.dome";
voicemail_collect="VM.2000";
video="1";
obtain_contacts_from_ipo="0";
conferencing="1";
conf_server="ConfServer@ipo.example.com";
conf_server_adhoc="ConfAdhoc";
transfer="1";
extended_mwi="1";
video_capable="1";
blind_transfer="1";
auto_ans="1";
change_password="1";
xmpp_group="1";
backup_ipoffice_server="iposec.example.com";
```

- **Durante el funcionamiento normal:**

  La respuesta *200 OK* muestra los valores *onex_server* y *backup_ipoffice_server* establecidos con los servidores primario y secundario respectivamente.

- **Durante la resiliencia:**

  onex_server contiene el FQDN del portal secundario y *backup_ipoffice_server* es *0.0.0.0*.

Vínculos relacionados

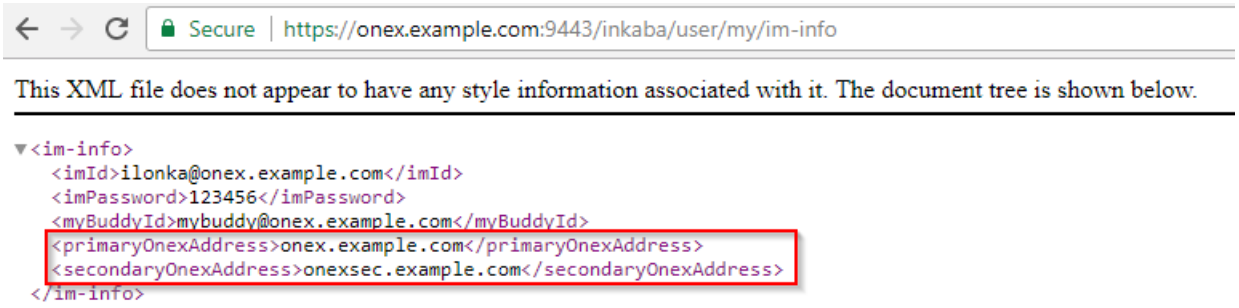
Verificación de la configuración de resiliencia en la página 86

Verificación de las respuestas de Avaya one-X Portal

Cuando un cliente solicita información XMPP del servicio primario de Avaya one-X Portal, la respuesta incluye las direcciones del servidor XMPP primario y secundario.

Procedimiento

1. Durante el funcionamiento normal, con un navegador, ingrese `https://<FQDN>:9443/inkaba/user/my/im-info` dónde *<FQDN>* es el FQDN del servicio primario de Avaya one-X Portal.



2. Verifique que la respuesta incluya los FQDN de los servicios primario y secundario de Avaya one-X Portal.
   a.
   b. La respuesta debe incluir el FQDN del servidor primario de IP Office.

3. Con un navegador, ingrese `https://<FQDN>:9443/inkaba/user/my/sip-info` dónde *<FQDN>* es el FQDN del servicio primario de Avaya one-X Portal.

4. Si repite los pasos durante la resiliencia, utilice el FQDN del servidor secundario de Avaya one-X Portal.
   - La información `im-info` será la misma.
   - La información `sip-info` mostrará el FQDN del servidor secundario de IP Office.

Vínculos relacionados

Verificación de la configuración de resiliencia en la página 86

Parte 4: Información adicional

Capítulo 11: Ayuda y documentación adicionales

Las siguientes páginas proporcionan fuentes de ayuda adicional.

Vínculos relacionados

Manuales y guías de usuario adicionales en la página 91
Obteniendo ayuda en la página 91
Buscar un socio comercial de Avaya en la página 92
Recursos adicionales de IP Office en la página 92
Capacitación en la página 93

Manuales y guías de usuario adicionales

El sitio web de Avaya Centro de Documentación contiene guías de usuario y manuales para productos Avaya, lo que incluye IP Office.

- Para obtener una lista de los manuales y guías de usuario actuales de IP Office, consulte el documento Avaya Manuales y guías del usuario de la IP Office™ Platform.
- Los sitios web de Avaya IP Office Knowledgebase y Avaya Soporte técnico también proporcionan acceso a los manuales técnicos y guías de usuario de IP Office.
  - Tenga en cuenta que, cuando sea posible, estos sitios redirigen a los usuarios a la versión del documento alojado por Avaya Centro de Documentación.

Para otros tipos de documentos y otros recursos, visite los diferentes sitios web de Avaya (consulte Recursos adicionales de IP Office en la página 92).

Vínculos relacionados

Ayuda y documentación adicionales en la página 91

Obteniendo ayuda

Avaya vende IP Office a través de socios comerciales acreditados. Esos socios comerciales proporcionan soporte técnico directo a sus clientes y pueden escalar problemas a Avaya si es necesario.

Si su sistema IP Office actualmente no tiene un socio comercial Avaya que le proporcione soporte y mantenimiento, puede utilizar la herramienta Avaya Partner Locator para encontrar un socio comercial. Vea Buscar un socio comercial de Avaya en la página 92.

Vínculos relacionados

Ayuda y documentación adicionales en la página 91

Buscar un socio comercial de Avaya

Si su sistema IP Office actualmente no tiene un socio comercial Avaya que le proporcione soporte y mantenimiento, puede utilizar la herramienta Avaya Partner Locator para encontrar un socio comercial.

Procedimiento

1. Con un navegador, vaya a Sitio web de Avaya en https://www.avaya.com
2. Seleccione **Socios** y luego **Buscar un socio**.
3. Ingrese la información de su ubicación.
4. Para socios comerciales IP Office, con el **Filtro**, seleccione **Pequeña/mediana empresa**.

Vínculos relacionados

Ayuda y documentación adicionales en la página 91

Recursos adicionales de IP Office

Además del sitio web de documentación (consulte Manuales y guías de usuario adicionales en la página 91), hay una gama de sitios web que proporcionan información sobre productos y servicios de Avaya, lo que incluye IP Office.

- Sitio web de Avaya (https://www.avaya.com)

  Este es el sitio web oficial de Avaya. La página principal proporciona acceso a sitios Web individuales de Avaya para los distintos países y regiones.

- **Ventas de Avaya y portal para socios** *(*https://sales.avaya.com*)*

  Este es el sitio Web oficial de todos los socios de negocios Avaya. Este sitio requiere del registro de un nombre y contraseña de usuario. Una vez que accede, puede personalizar el portal para que muestre productos específicos y el tipo de información que desea ver.

- **Avaya IP Office Knowledgebase** *(*https://ipofficekb.avaya.com*)*

  Este sitio proporciona acceso a una versión en línea y actualizada regularmente de guías del usuario y manual técnico IP Office.

- **Avaya Soporte técnico** *(*https://support.avaya.com*)*

  Este sitio proporciona acceso al software del producto Avaya, a la documentación y a otros servicios para instaladores y mantenedores de productos Avaya.

  - **Avaya Foros de soporte** *(*https://support.avaya.com/forums/index.php*)*

    Este sitio proporciona foros para analizar problemas de producto.

- **Grupo de usuarios internacionales de Avaya** *(*https://www.iuag.org*)*

  Esta es la organización para los clientes Avaya. Proporciona foros y grupos de conversación.

- **Avaya DevConnect** *(*https://www.devconnectprogram.com/*)*

  Este sitio proporciona detalles sobre API y SDK para productos Avaya, incluido IP Office. El sitio también proporciona notas de aplicación para productos de terceros que no son de Avaya, que interoperan con IP Office usando esas API y SDK.

- **Aprendizaje Avaya** *(*https://www.avaya-learning.com/*)*

  Este sitio proporciona acceso a cursos de capacitación y programas de acreditación para productos Avaya.

Vínculos relacionados

Ayuda y documentación adicionales en la página 91

Capacitación

Las credenciales y capacitación de Avaya garantizan que todos nuestros socios comerciales tengan las capacidades y habilidades para vender e implementar las soluciones Avaya y brindar soporte técnico para ellas, además de superar las expectativas de los clientes. Se encuentran disponibles las siguientes credenciales:

- Avaya Certified Sales Specialist (APSS) (Especialista en ventas certificado por Avaya)
- Avaya Implementation Professional Specialist (AIPS) (Especialista profesional en implementación de Avaya)
- Avaya Certified Support Specialist (ACSS) (Especialista en soporte técnico certificado por Avaya)

En el sitio web de Aprendizaje Avaya, encontrará los mapas de credenciales.

Vínculos relacionados

Ayuda y documentación adicionales en la página 91

Capítulo 12: Glosario

Las siguientes son definiciones para los términos utilizados dentro de este documento.

Vínculos relacionados

Un registro en la página 94
Registro AAAA en la página 94
ASBCE en la página 95
DNS en la página 95
Nombre de dominio en la página 95
FQDN en la página 95
IP de administración en la página 96
SBC en la página 96
DNS de división en la página 96
Registro SRV en la página 96
XMPP en la página 97

Un registro

"Registro de dirección". Un registro DNS básico que asigna un nombre de dominio o FQDN a una dirección IPv4. Para direcciones IPv6, DNS utiliza registros `AAAA`.

Vínculos relacionados

Glosario en la página 94

Registro AAAA

También denominado "registro Quad-A". Los servicios DNS utilizan registros `AAAA` para asignar un nombre de dominio o FQDN a una dirección IPv6. Estos son como los registros `A` utilizados para direcciones IPv4.

Vínculos relacionados

Glosario en la página 94

ASBCE

"Avaya Session Border Controller for Enterprise". La plataforma Avaya para proporcionar servicios SBC para una red de clientes.

Vínculos relacionados

Glosario en la página 94

DNS

"Servidor de nombre de dominio". Un servidor o servicio que proporciona información de dirección IP en respuesta a una consulta de nombre de dominio o de FQDN. Por ejemplo, cuando una aplicación intenta conectarse a `www.example.com`, primero contacta al servidor DNS en su red. El servidor DNS resuelve la dirección de texto `www.example.com` a la dirección IP numérica correspondiente. El proceso implica que el servidor DNS verifique los registros DNS que conserva y, si es necesario, los que conservan otros servidores DNS en la red o en Internet.

Vínculos relacionados

Glosario en la página 94

Nombre de dominio

La dirección de texto utilizada para identificar una red de dispositivos. Un servidor DNS traduce el nombre de dominio y los nombres de dominio completo a direcciones IP específicas.

Vínculos relacionados

Glosario en la página 94

FQDN

"Nombre de dominio completo". La dirección de texto completa asignada a un servidor, servicio o cliente específico dentro de un dominio.

Vínculos relacionados

Glosario en la página 94

IP de administración

La dirección IP utilizada para el acceso del administrador al servidor del ASBCE. Esta es una dirección diferente de la utilizada para las interfaces de tráfico de red internas y externas proporcionadas por el ASBCE.

Vínculos relacionados

Glosario en la página 94

SBC

"Session Border Controller". Un SBC es un dispositivo que controla la señalización de llamadas SIP y los medios entre dos redes.

Vínculos relacionados

Glosario en la página 94

DNS de división

El uso de FQDN y servidores DNS para enrutar el tráfico dentro y entre redes simplifica el mantenimiento de la red. Sin embargo, pueden surgir problemas cuando utiliza el enrutamiento FQDN para el tráfico de red interno y externo. Puede hacer que la red enrute el tráfico interno a servicios internos externamente. Esto expone las direcciones y los servicios internos que deben permanecer ocultos.

El DNS de división utiliza un servicio DNS público para el tráfico externo a la red del cliente y un servicio DNS privado para el tráfico interno dentro de la red del cliente.

Los clientes pueden configurar DNS de división usando un solo servidor DNS en el borde de la red del cliente o servidores DNS públicos y privados separados.

Vínculos relacionados

Glosario en la página 94

Registro SRV

"Registro de servicio". Para dominios que admiten múltiples servicios, por ejemplo `www.example.com` o `sip.example.com`, es posible que los registros `A` de DNS no sean suficientes para el enrutamiento requerido. Los registros `SRV` de DNS proporcionan asignación para servicios específicos que se ejecutan dentro de un dominio.

Vínculos relacionados

Glosario en la página 94

XMPP

“Protocolo de mensajería y presencia extensible”. XMPP es un protocolo de estándares abierto que permite que los dispositivos intercambien información de mensajes instantáneos, presencia y contactos.

Vínculos relacionados

Glosario en la página 94

Índice

A

a través de 44
Administrador 91
Administrador del sistema 91
agente de usuario 51, 52
alg 30
alg de SIP 30
anular anclaje 62
API 92
ASBCE
    certificado de identidad 20
audio 46
autoridades de certificados 34
Avaya Spaces
    IPv6 76
Ayuda 91

B

Boletines técnicos 92

C

cadena de AU 51
capacitación 92, 93
certificado 34, 35
    IPv6 75
certificado de identidad
    agregar a ASBCE 23
    generar 20, 21
    IPv6 75
certificado raíz
    cargar 19
    descargar 18
cifrados 34, 35
clave privada
    extraer 22
cliente tls 34, 41
clonar 28
códec 47
CONFIGURAR SIPSSO 76
cursos 92

D

de 44
dirección IP 31, 32
    lista blanca 16
Dirección IP pública 75
Distribuidor 91
DNS
    IPv6 75

E

encabezados 44
encabezados sip 44
enrutamiento del servidor 43
esquema
    extensiones SIP 7
    IPv6 74
estado 69
expresión regular 51
extensiones SIP
    esquema 7

F

firewall 30
flujo de servidor 55
    política de terminal 50
flujo de sesión 64
flujo de suscriptor 52
    lista de bloqueo 45
    política de terminal 50
foros 92
fqdn 11

G

glosario 94
grupo de políticas 50
grupo de políticas de terminal 50
Guías de referencia rápida 91
Guías de usuario 91

H

hasta 44

I

intentos fallidos 45
intentos fallidos de contraseña 45
intentos fallidos de nombre de usuario 45
interfaces de medios 37
interfaz
    externa 31
    interno 32
interfaz de medios 38
interfaz de señalización 39
    externa 40
intervalo de registro 15
IP pública 31, 32
IPv6 73
    certificado 75
    DNS 75
    Espacio 76
    esquema 74

L

licencias 11
línea de solicitud 44
lista blanca 16
lista de bloqueo 45, 52, 57
Lista de bloqueo de IP/URL 45, 52, 57
localizador de socios comerciales 92

M

Manuales 91
máscara 31, 32
máscara de subred 31, 32
máximo de sesiones 46
medios directos 62

N

nat 30
nat de capa 3 30
nombre de dominio 11
Notas de la aplicación 92
nouser 15
números de origen 15

O

ocultamiento de topología 44

P

página en blanco 76
peer ca 34
perfil del servidor 41
peso 43
política de sesión 62
prioridad 43
profundidad de verificación 34
protocolo de capa 4 11
proxy 57
proxy de archivo 57
proxy inverso 57
    lista de bloqueo 45
puerta de enlace 31, 32
puerta de enlace predeterminada 31, 32
puerto tls 40
puertos de teléfono preferidos 57

Q

QOS 47

R

rango de números de puerto 11
rango de puertos rtp 11
redes 31, 32
reemplazar 44
referido por 44
referir a 44
registrador sip 11
regla de aplicación 46
    política de terminal 50
regla de medios 47
    política de terminal 50
ruta de registro 44

S

SDK 92
sdp 44
seguridad 9
servidor de archivos 15
servidor de llamadas 41
servidor tls 35
sesiones
    máximo 46
sesiones concurrentes 46
siguiente salto 43
SIPSSO 76
sitios Web 92
sobrescribir 44
soporte técnico 92
Spaces
    IPv6 76
SRTP 47
suscripciones 11

T

temporizador de bloqueo 45
terminal
    sesiones por 46
tipo de servidor 41

U

usar puertos de teléfono preferidos 57

V

ventas 92
verificación de pares 34, 35
versión tls 34, 35
video 46

W

weblm 11