Déploiement de téléphones SIP IP Office distants avec un ASBCE

Version 12.0
Édition 14
Avril 2024

Avis

Toutes les mesures nécessaires ont été prises pour garantir l'exactitude et la pertinence des informations contenues dans ce document au moment de son impression. Avaya ne peut cependant être tenu responsable des éventuelles erreurs ou omissions. Avaya se réserve le droit de modifier et de corriger les informations contenues dans ce document, sans devoir en informer qui que ce soit, ni quelque organisation que ce soit.

Clause de non-responsabilité en matière de documentation

Le terme « Documentation » désigne toute information publiée sur différents supports, pouvant inclure des informations sur les produits, des descriptions d'abonnements ou de services, des instructions sur le fonctionnement et des spécifications de performance généralement mises à la disposition des utilisateurs de ces produits. Le terme Documentation n'inclut pas les supports marketing. Avaya n'est pas responsable des modifications, ajouts ou suppressions réalisés par rapport à la version originale publiée de la Documentation, sauf si ces modifications, ajouts ou suppressions ont été effectués par Avaya ou expressément en son nom. L'utilisateur final accepte d'indemniser et de ne pas poursuivre Avaya, ses agents et ses employés pour toute plainte, action en justice, demande et jugement résultant de ou en rapport avec des modifications, ajouts ou suppressions dans la mesure où ceux-ci sont effectués par l'utilisateur final.

Clause de non-responsabilité en matière de liens hypertextes

Avaya décline toute responsabilité quant au contenu et à la fiabilité des sites Web indiqués sur ce site ou dans la Documentation fournie par Avaya. Avaya décline toute responsabilité quant à l'exactitude des informations, des affirmations ou du contenu fournis par ces sites et n'approuve pas nécessairement les produits, services ou informations qui y sont décrits ou proposés. Avaya ne garantit pas que ces liens fonctionnent en toute circonstance et n'a aucun contrôle sur la disponibilité des pages qui y sont associées.

Garantie

Avaya offre une garantie limitée sur le matériel et les logiciels Avaya. Veuillez vous référer à votre contrat avec Avaya pour en connaître les termes. Les clients d'Avaya trouveront également les conditions générales de garantie pratiquées par Avaya, ainsi que des informations relatives à la prise en charge du produit, pendant la période de garantie, sur le site Web de l'assistance technique Avaya à l'adresse suivante : https://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010 sous la rubrique « Garantie et cycle de vie du produit », ou sur le site successeur désigné par Avaya. Veuillez noter que si vous vous êtes procuré ce ou ces produits auprès d'un partenaire de distribution Avaya agréé en dehors des États-Unis et du Canada, la garantie vous est proposée par le partenaire de distribution Avaya agréé et non par Avaya.

Le terme « **Service hébergé** » désigne un abonnement à un service hébergé Avaya souscrit auprès d'Avaya ou d'un partenaire de distribution Avaya agréé (le cas échéant), décrit ci-après dans la section relative au SAS hébergé et dans tout autre document décrivant le service hébergé applicable. Si vous souscrivez un abonnement à un Service hébergé, la garantie limitée susmentionnée peut ne pas s'appliquer, mais vous pouvez avoir droit aux services d'assistance liés au Service hébergé, tels que décrits ci-après dans vos documents décrivant le Service hébergé applicable. Pour obtenir des informations complémentaires, contactez Avaya ou le partenaire de distribution Avaya (le cas échéant).

Service hébergé

LES CONDITIONS SUIVANTES S'APPLIQUENT UNIQUEMENT LORSQUE VOUS ACHETEZ UN ABONNEMENT DE SERVICE HÉBERGÉ AVAYA AUPRÈS D'AVAYA OU D'UN PARTENAIRE AVAYA (LE CAS ÉCHÉANT), LES CONDITIONS D'UTILISATION DES SERVICES HÉBERGÉS SONT DISPONIBLES SUR LE SITE AVAYA, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO SOUS LE LIEN « Avaya Terms Of Use For Hosted Services » OU UN AUTRE SITE SUCCESSEUR TEL QUE DÉSIGNÉ PAR AVAYA, ET SONT APPLICABLES À TOUTE PERSONNE QUI ACCÈDE AU SERVICE HÉBERGÉ OU L'UTILISE. EN ACCÉDANT AU SERVICE HÉBERGÉ OU EN L'UTILISANT, OU EN AUTORISANT D'AUTRES À LE FAIRE, VOUS, EN VOTRE NOM, ET L'ENTREPRISE AU NOM DE LAQUELLE VOUS LE FAITES (CI-APRÈS DÉNOMMÉ INDIFFÉREMMENT COMME « VOUS » ET « UTILISATEUR FINAL »), ACCEPTEZ LES CONDITIONS D'UTILISATION. SI VOUS ACCEPTEZ LES CONDITIONS D'UTILISATION AU NOM D'UNE ENTREPRISE OU AUTRE ENTITÉ JURIDIQUE, VOUS DÉCLAREZ QUE VOUS ÊTES HABILITÉ À LIER CETTE ENTITÉ À CES CONDITIONS D'UTILISATION. SI VOUS N'ÊTES PAS HABILITÉ À LE FAIRE OU SI VOUS NE SOUHAITEZ PAS ACCEPTER CES CONDITIONS D'UTILISATION, VOUS NE DEVEZ NI ACCÉDER AU SERVICE HÉBERGÉ, NI L'UTILISER, NI AUTORISER QUICONQUE À Y ACCÉDER OU À L'UTILISER.

Licences

Les Conditions générales de licence de logiciel (les « Conditions de licence de logiciel ») sont disponibles sur le site Web suivant : https://www.avaya.com/en/legal-license-terms/, ou sur tout site successeur désigné par Avaya. Les présentes Conditions de licence de logiciel s'appliquent à toute personne qui installe, télécharge et/ou utilise le Logiciel et/ou la Documentation. En installant, en téléchargeant ou en utilisant le Logiciel, ou en autorisant d'autres personnes à le faire, l'utilisateur final accepte que les présentes Conditions de licence de logiciel le lient par contrat à Avaya. Si l'utilisateur final accepte les présentes Conditions de licence de logiciel au nom d'une société ou d'une autre entité juridique, l'utilisateur final déclare avoir le pouvoir de lier ladite entité aux présentes Conditions de licence de logiciel.

Copyright

Sauf mention contraire explicite, il est interdit d'utiliser les documents disponibles sur ce site ou dans la Documentation, les Logiciels, le Service hébergé ou le matériel fournis par Avaya. Tout le contenu de ce site, toute documentation, Service hébergé et tout produit fournis par Avaya, y compris la sélection, la disposition et la conception du contenu, appartient à Avaya ou à ses concédants de licences et est protégé par les droits d'auteur et autres droits sur la propriété intellectuelle, y compris les droits sui generis de protection des bases de données. Vous ne pouvez pas modifier, copier, reproduire, republier, charger, déposer, transmettre ou distribuer, de quelque façon que ce soit, tout contenu, partiel ou intégral, y compris tout code et logiciel sans l'autorisation expresse d'Avaya. La reproduction, la transmission, la diffusion, le stockage ou l'utilisation non autorisés de ce contenu sans l'autorisation expresse d'Avaya peuvent constituer un délit passible de sanctions civiles ou pénales en vertu des lois en vigueur.

Virtualisation

Ce qui suit s'applique si le produit est déployé sur une machine virtuelle. Chaque produit possède un code de commande et des types de licence spécifiques. Sauf mention contraire, chaque Instance de produit doit faire l'objet d'une licence distincte et être commandée séparément. Par exemple, si l'utilisateur final ou le partenaire de distribution Avaya souhaite installer deux Instances du même type de produits, il est nécessaire de commander deux produits de ce type.

Composants tiers

Les dispositions suivantes s'appliquent uniquement lorsque le codec H.264 (AVC) est fourni avec le produit. CE PRODUIT FAIT L'OBJET D'UNE LICENCE DE PORTEFEUILLE DE BREVETS AVC POUR L'UTILISATION PERSONNELLE ET NON COMMERCIALE PAR UN PARTICULIER POUR (i) ENCODER DE LA VIDÉO SELON LA NORME AVC (« VIDÉO AVC ») ET/OU (ii) DÉCODER DE LA VIDÉO AVC ENCODÉE PAR UN PARTICULIER ENGAGÉ DANS UNE ACTIVITÉ PERSONNELLE ET/OU OBTENUE AUPRÈS D'UN FOURNISSEUR DE VIDÉOS HABILITÉ À FOURNIR DES VIDÉOS AVC. AUCUNE LICENCE N'EST OCTROYÉE DE FAÇON EXPLICITE OU IMPLICITE POUR TOUTE AUTRE UTILISATION. DES INFORMATIONS SUPPLÉMENTAIRES SONT DISPONIBLES AUPRÈS DE MPEG LA, L.L.C. (HTTP://WWW.MPEGLA.COM).

Fournisseur de service

CONCERNANT LES CODECS, SI LE PARTENAIRE DE DISTRIBUTION D'AVAYA HÉBERGE UN PRODUIT QUI UTILISE OU INCORPORE LE CODEC H.264 OU H.265, LE PARTENAIRE DE DISTRIBUTION D'AVAYA RECONNAÎT ET ACCEPTE QUE LE PARTENAIRE DE DISTRIBUTION D'AVAYA EST RESPONSABLE POUR TOUS LES FRAIS ET/OU DROITS D'AUTEUR RELATIFS. LE CODEC H.264 (AVC) FAIT L'OBJET D'UNE LICENCE DE PORTEFEUILLE DE BREVETS AVC POUR L'UTILISATION PERSONNELLE ET NON COMMERCIALE PAR UN PARTICULIER POUR (i) ENCODER DE LA VIDÉO SELON LA NORME AVC (« VIDÉO AVC ») ET/OU (ii) DÉCODER DE LA VIDÉO AVC ENCODÉE PAR UN PARTICULIER ENGAGÉ DANS UNE ACTIVITÉ PERSONNELLE ET/OU OBTENUE

AUPRÈS D'UN FOURNISSEUR DE VIDÉOS HABILITÉ À FOURNIR DES VIDÉOS AVC. AUCUNE LICENCE N'EST OCTROYÉE DE FAÇON EXPLICITE OU IMPLICITE POUR TOUTE AUTRE UTILISATION. VOUS POUVEZ OBTENIR DES INFORMATIONS SUPPLÉMENTAIRES POUR LES CODECS H.264 (AVC) ET H.265 (HEVC) DEPUIS MPEG LA, L.L.C. (HTTP://WWW.MPEGLA.COM).

Dans le respect des lois

Vous reconnaissez et acceptez être tenu responsable de vous conformer aux lois et règlements applicables, y compris, mais sans s'y limiter, les lois et règlements en lien avec l'enregistrement des appels, la confidentialité des données, la propriété intellectuelle, le secret commercial, la fraude et les droits d'interprétation musicale du pays ou du territoire dans lequel le produit Avaya est utilisé.

Lutte contre la fraude à la tarification

Le terme « fraude à la tarification » fait référence à l'usage non autorisé de votre système de télécommunication par un tiers non habilité (par exemple, une personne qui ne fait pas partie du personnel de l'entreprise, qui n'est ni agent, ni sous-traitant ou qui ne travaille pas pour le compte de votre société). Sachez que votre système peut faire l'objet d'une fraude à la tarification et qu'en cas de fraude, les frais supplémentaires pour vos services de télécommunications peuvent être importants.

Intervention en cas de fraude à la tarification

Si vous pensez être victime d'une fraude à la tarification et que vous avez besoin d'une assistance technique ou autre, veuillez contacter votre représentant commercial Avaya.

Failles de sécurité

Vous trouverez plus d'informations concernant la politique d'assistance d'Avaya en matière de sécurité dans la rubrique Politique de sécurité et assistance (https://support.avaya.com/security).

Les failles sécuritaires suspectées du produit sont traitées conformément au processus d'assistance sécuritaire pour les produits Avaya (https://support.avaya.com/css/P8/documents/100161515).

Marques commerciales

Les marques commerciales, les logos et les marques de service (« Marques ») figurant sur ce site, sur toute documentation, sur le ou les Services hébergés et sur tout produit fournis par Avaya sont des marques déposées ou non déposées d'Avaya, de ses sociétés affiliées, de ses concédants de licences, de ses fournisseurs ou de parties tierces. Les utilisateurs ne sont pas autorisés à utiliser ces Marques sans autorisation écrite préalable d'Avaya ou dudit tiers qui peut être propriétaire de la Marque. Rien de ce qui est contenu dans ce site, la Documentation, le ou les Services hébergés et le ou les produits ne saurait être interprété comme accordant, par implication, préclusion ou autrement, toute licence ou tout droit sur les Marques sans l'autorisation écrite expresse d'Avaya ou du tiers applicable.

Avaya est une marque commerciale déposée d'Avaya LLC.

Toutes les marques commerciales autres qu'Avaya sont la propriété de leurs détenteurs respectifs.

Linux® est une marque de commerce déposée de Linus Torvalds aux États-Unis et dans d'autres pays.

Téléchargement de la documentation

Pour obtenir les versions les plus récentes de la Documentation, reportez-vous au site Web de l'assistance technique Avaya : https://support.avaya.com, ou au site successeur désigné par Avaya.

Contacter l'assistance Avaya

Consultez le site Web de l'assistance technique Avaya : https://support.avaya.com pour obtenir des avis et des articles portant sur les produits ou les services cloud, ou pour signaler tout problème que vous pourriez rencontrer avec votre produit ou service cloud Avaya. Pour connaître nos coordonnées et obtenir la liste des numéros d'assistance, consultez le site Web de l'assistance technique Avaya à l'adresse : https://support.avaya.com (ou le site successeur désigné par Avaya), faites défiler la page jusqu'en bas, puis sélectionnez Contacter l'assistance Avaya.

Sommaire

Partie 1 : Prise en charge des extensions SIP distantes

Chapitre 1 : Prise en charge des extensions SIP distantes sur IP Office

Cette section fournit un exemple de procédure pour la prise en charge des extensions SIP distantes se connectant à IP Office via un Avaya Session Border Controller (ASBCE). L'ASBCE fournit une gamme de fonctions qui fournissent une sécurité supplémentaire au processus de connexion.

- Ce document est basé sur IP Office R11.1.3.1 et ASBCE R10.1.2.
- Pour IP Office R11.1.3.1, IP Office prend en charge les extensions distantes Client Avaya Workplace iOS et Android IPv6 en utilisant l'IPv6. Sinon, IP Office prend uniquement en charge les extensions distantes IPv4.

Extensions SIP distantes prises en charge

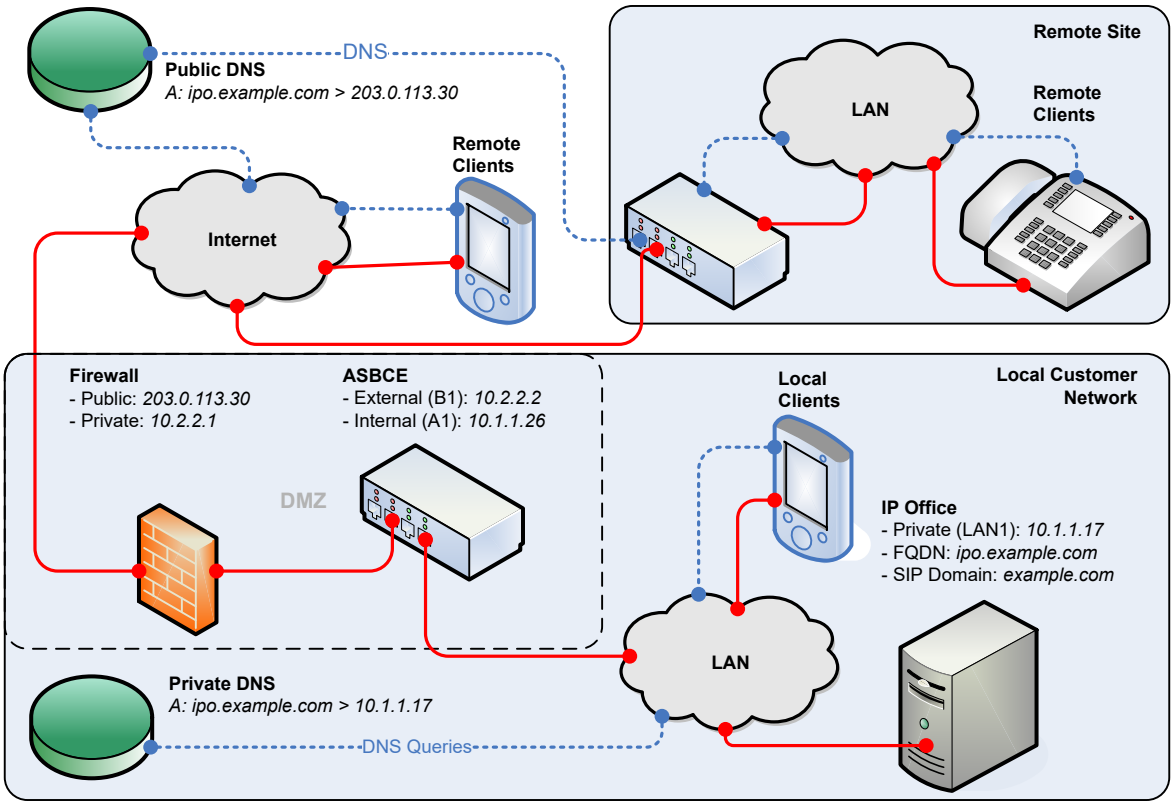
Téléphones de bureau SIP	Téléphones logiciels SIP
• Téléphones de la série J100 • Téléphones série K100 (Avaya Vantage™)	• Client Avaya Workplace

Liens connexes

Exemple de schéma à la page 7
Considérations relatives à la sécurité à la page 9

Exemple de schéma

Ce schéma présente l'exemple de scénario utilisé dans ce document :



- Pour ce scénario, les extensions SIP sont des téléphones de la série J100 et des téléphones logiciels Client Avaya Workplace.
- IP Office est le registrar SIP.
  - Cet exemple utilise TLS pour les connexions SIP. Cela nécessite de prendre en compte les certificats IP Office et de fournir des certificats pour l'ASBCE.
- L'ASBCE dispose d'interfaces IP publiques et privées. En les utilisant, il agit comme passerelle pour le trafic SIP entre le réseau privé du client et l'Internet public.
  - Lorsqu'ils sont utilisés en interne, les clients SIP se connectent directement à IP Office.
  - Lorsqu'ils sont utilisés en externe, les clients SIP se connectent à IP Office via l'ASBCE.
  - L'ASBCE achemine également les demandes de fichiers utilisés par les extensions SIP distantes. Par exemple, les demandes pour les fichiers `.txt` et `.xml`.
- Le réseau du client comprend un pare-feu entre lui-même et l'Internet public. Avaya recommande ceci pour une sécurité améliorée.
  - Le pare-feu transfère le trafic des extensions distantes vers l'ASBCE.
- La solution DNS du client fournit un DNS fractionné. C'est-à-dire :
  - Sur le réseau privé du client, le DNS résout le FQDN d'IP Office à l'adresse IP d'IP Office.
  - Sur l'Internet public, le DNS résout le FQDN d'IP Office à l'adresse IP publique du pare-feu du client.

Liens connexes

[Prise en charge des extensions SIP distantes sur IP Office](#) à la page 7

Considérations relatives à la sécurité

Tout scénario dans lequel vous connectez IP Office à l'Internet public doit prendre en compte la sécurité. Les options et exigences de sécurité d'IP Office sont abordées dans le manuel Directives de sécurité d'Avaya IP Office™ Platform.

Dans ce cas, la connexion à l'aide d'un ASBCE permet de disposer d'une série d'options de sécurité supplémentaires.

- **Correspondance de l'agent utilisateur**

  Vous pouvez configurer les chaînes d'agents utilisateur pouvant se connecter via l'ASBCE. Cela vous permet de ne prendre en charge que les connexions à partir d'applications et d'appareils connus. Voir la section Configuration d'un profil d'agents utilisateurs à la page 51.

- **Règles d'application**

  Vous pouvez utiliser les règles d'application pour configurer le type de média pris en charge par vos connexions, le nombre maximum de connexions et le nombre maximum de connexions par extension distante. Voir la section Création d'une règle d'application à la page 46.

- **Listes de blocage IP/URL**

  Vous pouvez les utiliser pour bloquer les adresses IP ou les URL qui échouent de façon répétée à l'enregistrement du nom d'utilisateur ou du mot de passe. Voir la section Création d'une liste de blocage IP/URI à la page 45.

Liens connexes

Prise en charge des extensions SIP distantes sur IP Office à la page 7

Chapitre 2 : Configuration d'IP Office pour les extensions SIP distantes

Cette section fournit un résumé général de la configuration d'IP Office pour la prise en charge de la connexion des extensions SIP distantes via un ASBCE.

Liens connexes

Liste de contrôle de la configuration d'IP Office à la page 10
Licences et abonnements à la page 11
Configuration VoIP SIP d'IP Office à la page 11
Définition des détails de l'ASBCE transmis aux extensions distantes par IP Office à la page 13
Ajout de paramètres supplémentaires pour les extensions distantes à la page 15
Mise en liste blanche de l'ASBCE à la page 16

Liste de contrôle de la configuration d'IP Office

#	Action	Lien/Remarques	✔
1.	Vérifier les paramètres VoIP SIP	Voir la section Configuration VoIP SIP d'IP Office à la page 11.	
2.	Ajouter un paramètre pour les extensions distantes	Voir la section Définition des détails de l'ASBCE transmis aux extensions distantes par IP Office à la page 13.	
3.	Définir les numéros source NoUser	Voir la section Ajout de paramètres supplémentaires pour les extensions distantes à la page 15.	
4.	Mettre l'ASBCE en liste blanche	Empêchez IP Office de bloquer l'ASBCE. Voir la section Mise en liste blanche de l'ASBCE à la page 16.	

Liens connexes

Configuration d'IP Office pour les extensions SIP distantes à la page 10

Licences et abonnements

IP Office ne nécessite aucune licence supplémentaire pour prendre en charge le fonctionnement avec un ASBCE. Les téléphones et les applications connectés à IP Office à l'aide d'un ASBCE utilisent les mêmes licences ou abonnements que pour le fonctionnement local.

Liens connexes

Configuration d'IP Office pour les extensions SIP distantes à la page 10

Configuration VoIP SIP d'IP Office

Voici la configuration d'IP Office utilisée pour prendre en charge les extensions SIP dans l'exemple de scénario. Cette configuration est la même pour les extensions SIP locales et distantes.

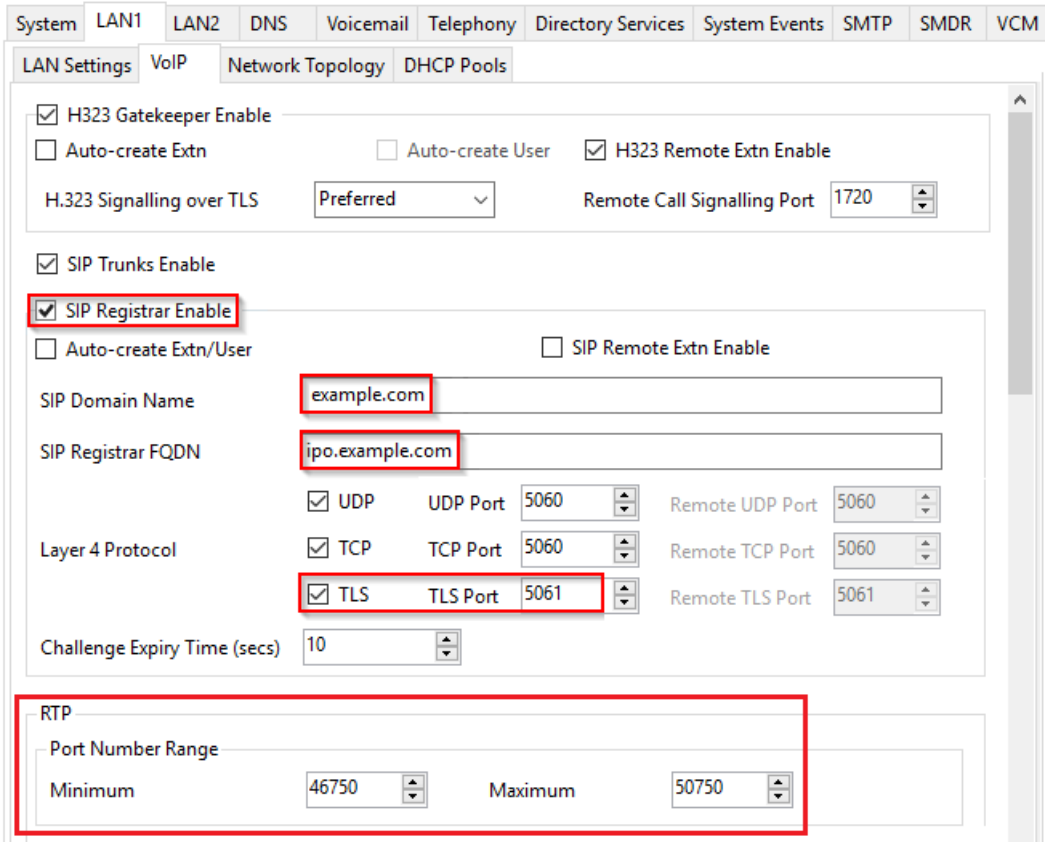
Important :

- La modification de ces paramètres nécessite un redémarrage d'IP Office.

Procédure

1. Connectez-vous à IP Office à l'aide d'IP Office Manager ou de IP Office Web Manager.
2. Sélectionnez **Système** ou **Paramètres du système** > **Système**.

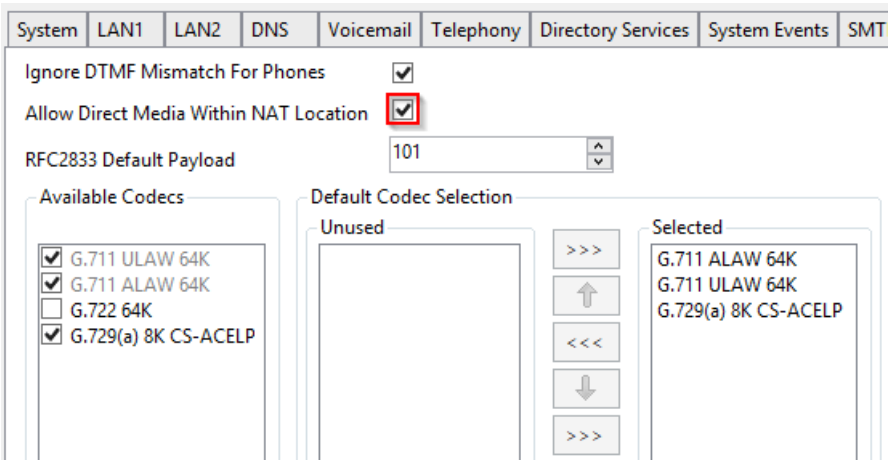
3. Sélectionnez l'onglet **LAN1**.



Champ	Description
Activer le Registrar SIP	Permet aux extensions SIP de s'enregistrer auprès d'IP Office.
Activer l'extension distante SIP	Désactivez. L'ASBCE gère les connexions NAT des extensions distantes.
Nom de domaine SIP	Définit le domaine que les clients SIP doivent utiliser pour l'enregistrement.
FQDN du Registrar SIP	Définit le nom de domaine complet pour le routage des connexions SIP vers IP Office.
Protocole de couche 4	Définit les protocoles de couche 4 et les ports sur lesquels IP Office écoute le trafic des extensions SIP.
Plage de numéros de ports	Définit la plage de numéros de port qu'IP Office utilise pour le trafic RTP et RTCP.

4. Sélectionnez le sous-onglet **VoIP**.

   Cochez la case **Autoriser le média direct dans l'emplacement NAT**.



   - L'activation de cette option permet un média direct entre les appareils résidant sur le même sous-réseau qui se connectent à IP Office à l'aide du NAT. La prise en charge de cette fonction via l'ASBCE nécessite une configuration supplémentaire pour que l'ASBCE se désancre du média d'appel, voir Désancrage des médias d'appel de l'ASBCE à la page 62.

5. Cliquez sur **OK** ou **Mettre à jour**.
6. Enregistrez les paramètres et redémarrez le système IP Office :
   - Si vous utilisez IP Office Manager, enregistrez les paramètres et redémarrez le système.
   - Si vous utilisez IP Office Web Manager, cliquez sur **Enregistrer sur IP Office** et redémarrez le système.

Liens connexes

Configuration d'IP Office pour les extensions SIP distantes à la page 10

Définition des détails de l'ASBCE transmis aux extensions distantes par IP Office

Avant de s'enregistrer auprès d'IP Office, les extensions Avaya demandent le fichier `46xxsettings.txt`. Ce fichier contient les paramètres utilisés par les extensions.

Pour les extensions distantes, le fichier `46xxsettings.txt` généré automatiquement par IP Office doit contenir les informations d'adresse que l'extension distante peut utiliser pour se connecter à l'ASBCE.

- Les extensions demandent le fichier `46xxsettings.txt` lorsqu'elles s'enregistrent pour la première fois auprès d'IP Office.
- Après avoir reçu le fichier `46xxsettings.txt`, les extensions redemandent par défaut le fichier toutes les 24 heures pour appliquer les modifications.

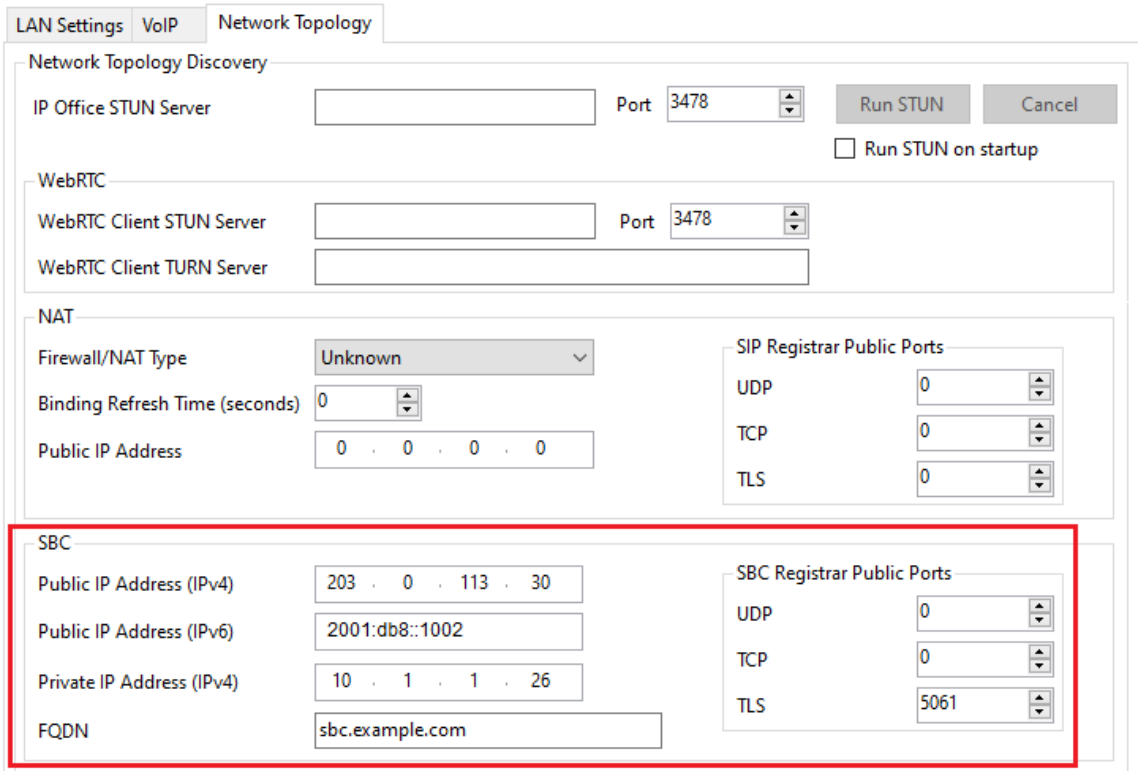
- Les extensions demandent également le fichier à chaque redémarrage. Vous pouvez les redémarrer à distance à l'aide de SysMonitor ou System Status Application.

Important :

- La modification de ces paramètres nécessite un redémarrage d'IP Office.

Procédure

1. Connectez-vous à IP Office à l'aide d'IP Office Manager ou de IP Office Web Manager.
2. Sélectionnez **Système** ou **Paramètres du système** > **Système**.
3. Sélectionnez le LAN (**LAN1** ou **LAN2**) connecté au même réseau que l'ASBCE.
4. Sélectionnez **Topologie réseau**.
   - Si vous utilisez IP Office Web Manager, vous ne pouvez modifier ces paramètres qu'en mode hors ligne. Cliquez sur l'icône et sélectionnez **Mode Hors ligne**.
5. Dans la section **SBC**, saisissez les informations suivantes :



Paramètre	Description
Adresse IP publique (IPv4)	L'adresse IPv4 publique pour le trafic de client SIP entrant dans le réseau du client. • Il s'agit de l'adresse IPv4 publique de l'ASBCE ou du service faisant face à l'Internet, tel que le pare-feu du client. • Le DNS externe doit résoudre le FQDN d'IP Office à cette adresse lorsqu'il est demandé par une extension distante IPv4.

Le tableau continue …

Paramètre	Description
Adresse IP publique (IPv6)	L'adresse IPv6 publique pour le trafic de client SIP entrant dans le réseau du client, comme ci-dessus. Pour plus d'informations, veuillez consulter Prise en charge des extensions distantes IPv6 à la page 73. • Il s'agit de l'adresse IPv6 publique de l'ASBCE ou du service faisant face à l'Internet, tel que le pare-feu du client. • Le DNS externe doit résoudre le FQDN d'IP Office à cette adresse lorsqu'il est demandé par une extension distante IPv6.
Adresse IP privée (IPv4)	L'adresse IPv4 privée/interne de l'ASBCE. • Le DNS interne doit résoudre le **FQDN** ci-dessous à cette adresse.
FQDN	Le nom de domaine complet de l'ASBCE. Le DNS doit résoudre ce FQDN aux adresses IPv6 utilisées (l'IPv4 utilise le FQDN du registrar SIP IP Office).
Ports publics du Registrar SIP	Les ports publics (externes) **UDP**, **TCP** et/ou **TLS** que les clients SIP externes doivent utiliser pour se connecter à l'ASBCE.

6. Cliquez sur **OK** ou **Mettre à jour**.
7. Enregistrez les paramètres et redémarrez le système IP Office :
   - Si vous utilisez IP Office Manager, enregistrez les paramètres et redémarrez le système.
   - Si vous utilisez IP Office Web Manager, cliquez sur **Enregistrer sur IP Office** et redémarrez le système.

Liens connexes

Configuration d'IP Office pour les extensions SIP distantes à la page 10

Ajout de paramètres supplémentaires pour les extensions distantes

Vous pouvez utiliser les numéros source **NoUser** suivants pour définir des valeurs supplémentaires dans le fichier `46xxsettings.txt` généré automatiquement qu'IP Office fournit aux extensions distantes.

Procédure

1. Connectez-vous à IP Office à l'aide d'IP Office Manager ou de IP Office Web Manager.
2. Cliquez sur **Utilisateur** ou **Gestion des appels** > **Utilisateur**.
3. Localisez les paramètres de l'utilisateur nommé *NoUser*.
4. Sélectionnez **Numéros source**.
5. Ajoutez les numéros source *NoUser* supplémentaires requis :
   - **SET_STIMULUS_SBC_REG_INTERVAL=**`<seconds>`

     Ce numéro source *NoUser* définit l'intervalle d'enregistrement utilisé par les téléphones de la série J100. La valeur par défaut est de 3600 secondes (1 heure). Lorsque vous prenez en charge des téléphones via un ASBCE, la valeur

recommandée est de 180 secondes. La plage prise en charge est comprise entre 180 et 3 600 secondes.

- **PUBLIC_HTTP=**`<file server address>`

  Lorsque vous utilisez les paramètres **Adresse IP du serveur HTTP** et **Redirection HTTP**, IP Office utilise cette valeur pour définir l'adresse du serveur de fichiers public donnée aux extensions distantes.

6. Cliquez sur **OK** ou **Mettre à jour**.
7. Enregistrez les paramètres et redémarrez le système IP Office :
   - Si vous utilisez IP Office Manager, enregistrez les paramètres et redémarrez le système.
   - Si vous utilisez IP Office Web Manager, cliquez sur **Enregistrer sur IP Office** et redémarrez le système.

Liens connexes

Configuration d'IP Office pour les extensions SIP distantes à la page 10

Mise en liste blanche de l'ASBCE

Lorsqu'une extension distante se connecte à IP Office via l'ASBCE, des tentatives d'enregistrement incorrectes peuvent entraîner le blocage de l'adresse IP de l'ASBCE par IP Office.

Procédure

1. Connectez-vous à IP Office à l'aide d'IP Office Manager ou de IP Office Web Manager.
2. Sélectionnez **Système** ou **Paramètres du système** > **Système**.
3. Sélectionnez **VoIP** > **Listes de contrôle d'accès**.
4. Ajoutez l'adresse IP interne de l'ASBCE à la **Liste blanche des IP**.
5. Cliquez sur **OK** ou **Mettre à jour**.
6. Si vous utilisez IP Office Manager, enregistrez les paramètres dans le système IP Office.

Liens connexes

Configuration d'IP Office pour les extensions SIP distantes à la page 10

Chapitre 3 : Ajout de certificats IP Office à l'ASBCE

Dans l'exemple de scénario, IP Office utilise son certificat auto-signé. Dans ce cas, l'ASBCE a besoin :

- D'une copie du certificat racine d'IP Office. Il s'agit de l'Autorité de Certification (« Certificate Authority » ou « CA »).
- D'un certificat d'identité pour l'ASBCE émis par IP Office.
  - **Pour l'IPv4 :** Le certificat doit inclure les adresse FQDN (CN ou SAN) et IPv4 (SAN) d'IP Office.
  - **Pour l'IPv6 :** En plus des adresses FQDN et IPv4 d'IP Office, le certificat d'identité de l'ASBCE doit inclure les adresses FQDN et IPv6 de l'ASBCE.

Utilisation de certificats tiers

Si IP Office utilise des certificats émis par une Autorité de Certification tierce, les certificats racine et d'identité requis pour l'ASBCE doivent être émis par cette Autorité de Certification. Cependant, les principes relatifs aux détails requis dans le certificat d'identité restent les mêmes que ceux décrits dans cette section de la documentation.

Liens connexes

Liste de vérification du certificat de l'ASBCE à la page 17
Téléchargement du certificat racine IP Office à la page 18
Ajout du certificat racine IP Office à l'ASBCE à la page 19
Génération d'un certificat d'identité ASBCE à l'aide d'IP Office Web Manager à la page 19
Génération d'un certificat d'identité ASBCE à l'aide de Web Control (Affichage de la plateforme) à la page 21
Fractionnement du certificat d'identité de l'ASBCE à la page 22
Ajout du certificat d'identité au ASBCE à la page 23

Liste de vérification du certificat de l'ASBCE

#	Action	Lien/Remarques	✔
1.	Télécharger le certificat racine IP Office	Voir la section Téléchargement du certificat racine IP Office à la page 18.	

Le tableau continue …

#	Action	Lien/Remarques	✔
2.	Ajouter le certificat racine à l'ASBCE	Voir la section Ajout du certificat racine IP Office à l'ASBCE à la page 19.	
3.	Générer un certificat d'identité pour l'ASBCE	Voir la section Génération d'un certificat d'identité ASBCE à l'aide d'IP Office Web Manager à la page 19.	
4.	Fractionner le certificat	Extrayez des fichiers de certificat et de clé privée distincts du certificat d'identité. Voir la section Fractionnement du certificat d'identité de l'ASBCE à la page 22.	
5.	Ajouter les fichiers à l'ASBCE	Ajoutez le certificat d'identité et les fichiers de clé privée à l'ASBCE Voir la section Ajout du certificat d'identité au ASBCE à la page 23.	

Liens connexes

Ajout de certificats IP Office à l'ASBCE à la page 17

Téléchargement du certificat racine IP Office

Suivez cette procédure pour télécharger une copie du certificat racine IP Office.

Procédure

1. Connectez-vous à IP Office à l'aide d'IP Office Web Manager.
   - Pour un IP500 V2, saisissez l'adresse du système, suivie de `:8443/WebMgmtEE/WebManagerment.html`.
   - Pour un serveur basé sur Linux, saisissez l'adresse système, suivie de `:7070/WebManagement/WebManagement.html`.
2. Sélectionnez **Sécurité** > **Paramètres de sécurité**.
3. Si IP Office se trouve dans un réseau multi-sites, cliquez sur en regard de l'IP Office requis.
4. Sélectionnez **Certificats**.
5. Dans le **Magasin de certificats approuvés**, localisez le certificat racine que le système IP Office utilise.
6. Cliquez sur en regard du certificat.
7. Cliquez sur **Oui**.
8. Renommez le fichier `IPO_RootCA.crt`.

Étapes suivantes

- Allez à Ajout du certificat racine IP Office à l'ASBCE à la page 19.

Liens connexes

Ajout de certificats IP Office à l'ASBCE à la page 17

Ajout du certificat racine IP Office à l'ASBCE

Suivez cette procédure pour charger la copie du certificat racine IP Office sur l'ASBCE.

Préambules

- Téléchargez le certificat racine IP Office. Voir la section Téléchargement du certificat racine IP Office à la page 18.

Procédure

1. Accédez à **Gestion TLS** > **Certificats**.
2. Cliquez sur **Installer**.
3. Définissez le **Type** sur **Certificat CA**.
4. Entrez un nom descriptif pour le certificat.
5. Activez **Autoriser un certificat ou une clé faible**.
6. Cliquez sur **Choisir un fichier** et sélectionnez le fichier `IPO_RootCA.crt`.
7. Cliquez sur **Charger**. Le menu affiche un avertissement indiquant qu'il s'agit d'un certificat auto-signé.
8. Cliquez sur **Continuer** . Le menu affiche le certificat.
9. Cliquez sur **Installer**.
10. Cliquez sur **Terminer**.

Étapes suivantes

- Utilisez IP Office pour créer un certificat d'identité pour l'ASBCE :
  - Pour les systèmes avec abonnement, reportez-vous à la section Génération d'un certificat d'identité ASBCE à l'aide d'IP Office Web Manager à la page 19.
  - Pour les autres systèmes, reportez-vous à la section Génération d'un certificat d'identité ASBCE à l'aide de Web Control (Affichage de la plateforme) à la page 21.

Liens connexes

Ajout de certificats IP Office à l'ASBCE à la page 17

Génération d'un certificat d'identité ASBCE à l'aide d'IP Office Web Manager

Cette procédure génère un certificat d'identité pour l'ASBCE à l'aide d'IP Office Web Manager.

- Cette procédure concerne les systèmes IP Office en mode abonnement utilisant la **Gestion automatique des certificats**. Pour les autres systèmes, reportez-vous à la

section Génération d'un certificat d'identité ASBCE à l'aide de Web Control (Affichage de la plateforme) à la page 21.

Procédure

1. Connectez-vous au système à l'aide d'IP Office Web Manager.
   - Pour un IP500 V2, saisissez l'adresse du système, suivie de `:8443/WebMgmtEE/WebManagerment.html`.
   - Pour un serveur basé sur Linux, saisissez l'adresse système, suivie de `:7070/WebManagement/WebManagement.html`.
2. Sélectionnez **Sécurité** > **Paramètres de sécurité**.
3. Si IP Office se trouve dans un réseau multi-sites, cliquez sur en regard de l'IP Office requis.
4. Sélectionnez **Certificats**.
5. Cliquez sur **Renouveler**.
6. Sélectionnez **Créer un certificat pour un autre ordinateur**.
7. Dans **Nom du sujet**, saisissez le FQDN de l'ASBCE.
8. Dans **Autre(s) nom(s) de l'objet**, saisissez des valeurs supplémentaires pour les autres serveurs et services auxquels l'ASBCE doit se connecter.
   - **Pour IPv4 :** Le certificat doit inclure le FQDN IP Office et l'adresse IPv4.
   - **Pour l'IPv6 :** En plus des adresses FQDN et IPv4 d'IP Office, le certificat d'identité de l'ASBCE doit inclure les adresses FQDN et IPv6 de l'ASBCE.
   - Utilisez des valeurs séparées par des virgules pour les entrées *DNS:<FQDN>* et *IP:<IP address>* requises.
   - Si vous utilisez des FQDN différents pour le domaine XMPP Avaya one-X® Portal, saisissez tous les FQDN sous forme de liste d'entrées DNS séparée par des virgules.
9. Cliquez sur **OK**. Attendez une minute pendant que IP Office génère le certificat.
10. Lorsque vous y êtes invité, définissez un mot de passe de chiffrement pour le certificat d'identité et cliquez sur **Oui** .
11. Le navigateur vous invitera à télécharger et enregistrer le fichier de certificat.
12. Renommez le fichier téléchargé en `SBCE_ID.p12`.

Étapes suivantes

- Voir la section Fractionnement du certificat d'identité de l'ASBCE à la page 22.

Liens connexes

Ajout de certificats IP Office à l'ASBCE à la page 17

Génération d'un certificat d'identité ASBCE à l'aide de Web Control (Affichage de la plateforme)

Cette procédure génère un certificat d'identité pour l'ASBCE à l'aide des menus Web Control du serveur IP Office.

Procédure

1. Connectez-vous aux menus Web Control d'IP Office en procédant de l'une des manières suivantes :
   - À partir d'IP Office Web Manager, sélectionnez le serveur principal. Cliquez sur ☰ et sélectionnez **Affichage de la plateforme**.
   - Accédez à `https://<IP Office IP address>:7071` et connectez-vous.
2. Sélectionnez l'onglet **Paramètres** et faites défiler jusqu'à **Certificats**.
3. Sélectionnez **Créer un certificat pour un autre ordinateur**.
4. Entrez les données suivantes :
5. Dans **Adresse IP de l'ordinateur**, saisissez l'adresse IP externe de l'ASBCE.
6. Dans **Mot de passe**, saisissez un mot de passe pour chiffrer le certificat et la clé.
7. Dans **Nom du sujet**, saisissez le FQDN de l'ASBCE.
8. Dans **Autre(s) nom(s) de l'objet**, saisissez des valeurs supplémentaires pour les autres serveurs et services auxquels l'ASBCE doit se connecter.
   - **Pour IPv4 :** Le certificat doit inclure le FQDN IP Office et l'adresse IPv4.
   - **Pour l'IPv6 :** En plus des adresses FQDN et IPv4 d'IP Office, le certificat d'identité de l'ASBCE doit inclure les adresses FQDN et IPv6 de l'ASBCE.
   - Utilisez des valeurs séparées par des virgules pour les entrées *DNS:<FQDN>* et *IP:<IP address>* requises.
   - Si vous utilisez des FQDN différents pour le domaine XMPP Avaya one-X® Portal, saisissez tous les FQDN sous forme de liste d'entrées DNS séparée par des virgules.
9. Cliquez sur **Renouveler**.
10. Cliquez sur le lien dans la fenêtre contextuelle et enregistrez le fichier.
11. Renommez le fichier téléchargé en `SBCE_ID.p12`.

Étapes suivantes

- Voir la section Fractionnement du certificat d'identité de l'ASBCE à la page 22.

Liens connexes

Ajout de certificats IP Office à l'ASBCE à la page 17

Fractionnement du certificat d'identité de l'ASBCE

Le certificat d'identité créé pour l'ASBCE par IP Office est un fichier unique. Il contient à la fois le certificat et la clé privée. Pour la configuration de l'ASBCE, vous devez fractionner le certificat d'identité en fichiers de certificat et de clé privée distincts.

Préambules

- Utilisez IP Office pour créer un certificat d'identité pour l'ASBCE :
  - Pour les systèmes avec abonnement, reportez-vous à la section Génération d'un certificat d'identité ASBCE à l'aide d'IP Office Web Manager à la page 19.
  - Pour les autres systèmes, reportez-vous à la section Génération d'un certificat d'identité ASBCE à l'aide de Web Control (Affichage de la plateforme) à la page 21.

Procédure

1. À l'aide de WinSCP, connectez-vous à l'adresse IP de gestion de l'ASBCE en utilisant le port 222 et l'identifiant ipcs.
2. Copiez le certificat d'identité IP Office créé pour l'ASBCE (`SBCE_ID.p12`) dans le répertoire **`/home/ipcs`** de l'ASBCE .
3. À l'aide du SSH, accédez à l'adresse IP de gestion de l'ASBCE en utilisant le port 222 et l'identifiant ipcs.
4. Saisissez la commande **su root** ou **su -root** et saisissez le mot de passe racine de l'ASBCE.
5. Saisissez les commandes suivantes. La commande à utiliser varie selon que vous avez généré le certificat à l'aide d'IP Office Web Manager ou des menus Web Control (Affichage de la plateforme).

   Remarque :

   - Lorsque vous êtes invité à saisir un mot de passe ou une phrase secrète PEM, saisissez le mot de passe spécifié lors de la génération du certificat d'identité pour l'ASBCE.
   - Si le mot de passe contient des caractères spéciaux, vous devez les faire précéder du préfixe `\` lorsque vous les saisissez sur la ligne de commande. Par exemple, sur la ligne de commande, saisissez un `@` dans le mot de passe sous la forme `\@`.

   - **Certificat Web Control d'IP Office :**

     Suivez les étapes suivantes avec un certificat généré à l'aide des menus Web Control d'IP Office.

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

   - **Certificat IP Office Web Manager :**

     Suivez les étapes suivantes avec un certificat généré à l'aide d'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. Copiez les nouveaux fichiers `SBCE_ID.crt` et `SBCE_ID.key` de l'ASBCE sur votre PC.
7. Le fichier `SBCE_ID.crt` contient toujours le certificat AC racine d'IP Office, la clé privée et le certificat d'identité de l'ASBCE. Pour pouvoir importer le fichier dans l'ASBCE, vous devez supprimer le certificat AC et la clé privée du fichier .
   a. Ouvrez `SBCE_ID.crt` dans WordPad sur votre PC.
   b. Supprimez toutes les lignes sauf celles situées entre les premières lignes **BEGIN CERTIFICATE** et **END CERTIFICATE**. Par exemple :

```
-----BEGIN CERTIFICATE-----
MIIEYjCCA0qgAwIBAgIGYCZWOINgMA0GCSqGSIb3DQEBCwUAMIGtMQswCQYDVQQG
EwJVUzETMBEGA1UECAwKTmV3IEplcnNleTEWMBQGA1UEBwwNQmFza2luZyBSaWRn
ZTESMBAGA1UECgwJQXZheWEgSW5jMQwwCgYDVQQLDANHQ1MxLTArBgNVBAMMJGlw
b2ZmaWNlLXJvb3QtMDAwQzI5RDJDRTQ2LmF2YXlhLmNvbTEgMB4GCSqGSIb3DQEJ
ARYRc3VwcG9ydEBhdmF5YS5jb20wHhcNMTUxMjA5MTMyNTQ5WhcNMjIxMjA5MTIy
NTQ5WjCBlzELMAkGA1UEBhMCVVMxEzARBgNVBAgMCk5ldyBKZXJzZXkxFjAUBgNV
BAcMDUJhc2tpbmcgUmlkZ2UxEjAQBgNVBAoMCUF2YXlhIEluYzEMMAoGA1UECwwD
R0NTMRcwFQYDVQQDDA5zYmNlLmJ1bmR5LmNvbTEgMB4GCSqGSIb3DQEJARYRc3Vw
cG9ydEBhdmF5YS5jb20wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDE
XivTfA4Q/w/oMlnojSnOyE51Yzk3dS4L1FPHtzfj6IZlfE3w0LAv/7uQl1AljRlc
dii2ctJQw2puwnkdhsKzi+GQRaHzKoc+cb+tUhMRrrFBIvnnZ9yy0D1CW+iVp8z9
TO8Tce7G9vMgiRjRnZL7UfesqWigkuySpXMcDUKivlnTuYeOuP8znbu9620xrcCO
/w36qhOB2BcE3jGFn7Iv69hiol2ifHqAWhDcatwvQQahTf85Uka5hVoRetwdT9ys
mk1nnMJ913UyN8DlvXoqnWUav9rQVZKpnQMSOERw9w8n0sb5dXNOqxaV3G2zyHPq
psUHEYKc7bk2haooIvifAgMBAAGjgZswgZgwCQYDVR0TBAIwADALBgNVHQ8EBAMC
A/gwHwYDVR0RBBgwFoIOc2JjZS5idW5keS5jb22HBId88iIwHwYDVR0jBBgwFoAU
8AJiRrTa38gHJzRg4wpAX0Oc7SgwHQYDVR0OBBYEFApovB6QMB8amPZdmppIjaZ3
HO39MB0GA1UdJQQWMBQGCCsGAQUFBwMBBggrBgEFBQcDAjANBgkqhkiG9w0BAQsF
AAOCAQEAOG2tfwKeBPaLX0aef35pDzdPjck6qFnZwV3BQFHCz3C3P0RxcLXdC+us
tk/UH71440h8yVhCqLwkQmHuoDK+8ofmuHOlvhnGK8d+lWPWJwImLrIk5PI5zsXC
4n/9ZKQzibeylfblRQpiCgAaT6L2lvQvZfuETAfSYk4Tw2UdMja8JGYDIkNqHBNp
FPb+W1/cPimututLyJYRVCGpkM6bGfmpyMbS3JDGtYWhb7uq19XqlMdZAVWtL5a1
Bxe1kwNfsYIOQGPDiOO9nO1s+9i2pcIUQ1BchpA2yUphvtwS2KrNMhOkG3mcpWHB
9a2PMn1DMM3PXMfyRh9vL00fMRSNVA==
-----END CERTIFICATE-----
```

Étapes suivantes

- Allez à Ajout du certificat d'identité au ASBCE à la page 23

Liens connexes

Ajout de certificats IP Office à l'ASBCE à la page 17

Ajout du certificat d'identité au ASBCE

Suivez cette procédure pour charger le certificat d'identité sur l'ASBCE.

Préambules

- Fractionnement du certificat d'identité de l'ASBCE à la page 22

Procédure

1. Accédez à **Gestion TLS** > **Certificats**.
2. Cliquez sur **Installer**.
3. Dans **Type**, sélectionnez **Certificat**.
4. Entrez un nom descriptif pour le certificat.
5. Cliquez sur **Choisir un fichier** et sélectionnez le fichier `SBCE_ID.crt`.
6. Sélectionnez **Charger le fichier de clé**.
7. Cliquez sur **Choisir un fichier** et sélectionnez le fichier `SBCE_ID.key`.

8. Cliquez sur **Charger**. Le menu affiche le certificat.
9. Cliquez sur **Installer**.
10. Cliquez sur **Terminer**.
11. À l'aide du SSH, accédez à l'adresse IP de gestion de l'ASBCE en utilisant le port 222 et l'identifiant ipcs.
    a. Saisissez `su root` ou `su -root` et le mot de passe racine de l'ASBCE.
    b. Saisissez les commandes suivantes, en remplaçant `********` par le mot de passe défini lors de la génération du certificat d'identité :

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

    - Vous devez faire précéder les caractères spéciaux dans le mot de passe de `\`. Par exemple, pour entrer `@`, saisissez `\@`.

Liens connexes

Ajout de certificats IP Office à l'ASBCE à la page 17

Chapitre 4 : Configuration de l'ASBCE pour les extensions SIP distantes

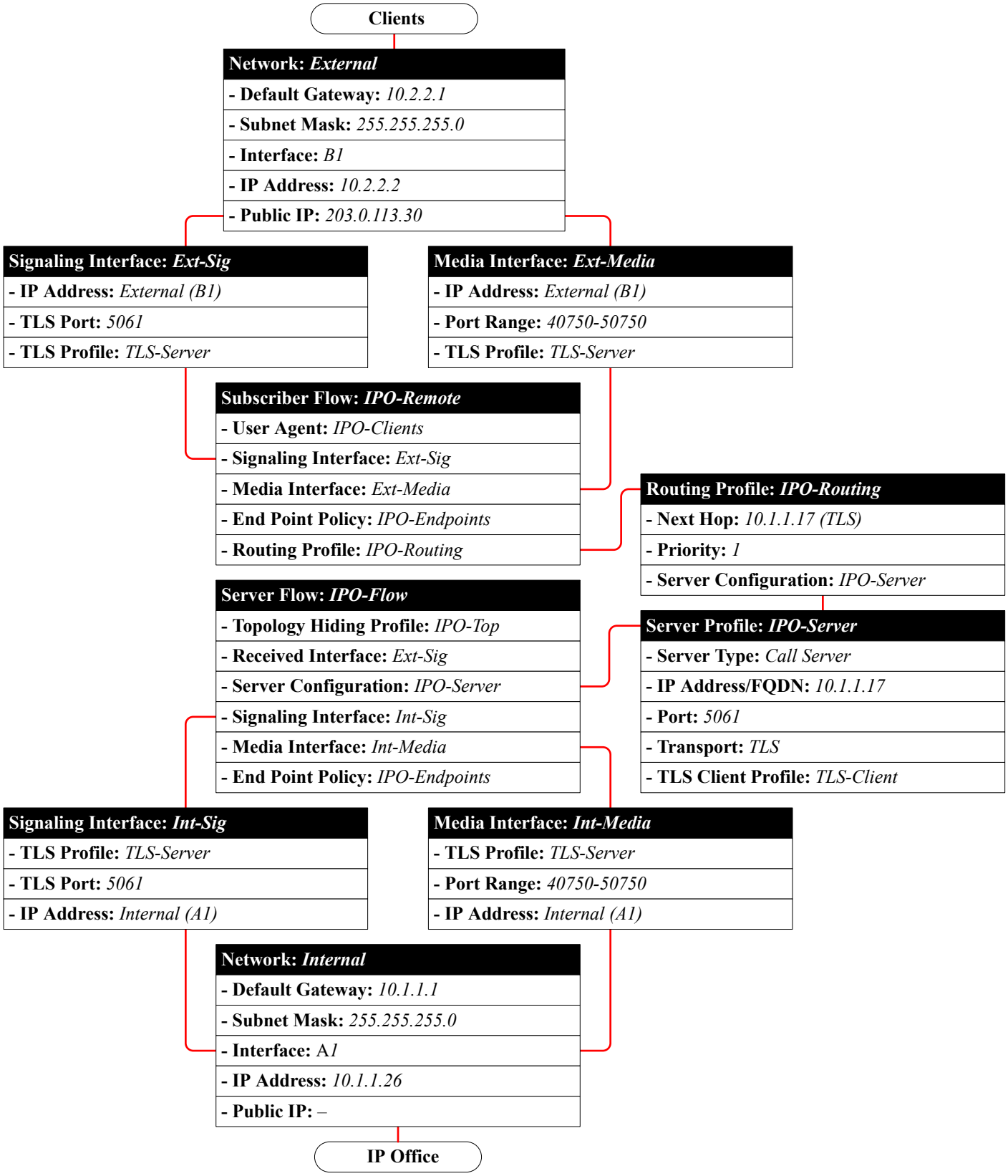
Cette section traite de la configuration de l'ASBCE pour acheminer les appels SIP entre les extensions distantes et IP Office.

- **Prise en charge de l'IPv6 :** Pour plus de détails sur la prise en charge des extensions distantes IPv6, reportez-vous à la section Prise en charge des extensions distantes IPv6 à la page 73.
  - **Si vous ne prenez en charge que les extensions distantes IPv6 :** Suivez la procédure de configuration de cette section pour l'IPv4, mais remplacez les adresses IPv4 externes par des adresses IPv6, le cas échéant.
  - **Si les extensions distantes IPv4 et IPv6 sont prises en charge :** Vous devez effectuer des étapes de configuration supplémentaires après avoir terminé la configuration de l'IPv4. Voir la section Liste de vérification de configuration pour les extensions distantes IPv4 et IPv6 combinées à la page 77.

Liens connexes

Résumé du flux d'appels de l'ASBCE

Cette image résume les éléments de configuration de l'ASBCE utilisés pour la connexion entre les extensions distantes IPv4 et IP Office.



Liens connexes

Configuration de l'ASBCE pour les extensions SIP distantes à la page 25

Clone ou Ajouter

Important :

Plusieurs procédures de ce document vous indiquent de créer de nouveaux éléments en clonant un modèle existant plutôt qu'en ajoutant une nouvelle entrée. Autrement dit, vous devez cliquer sur **Clone** plutôt que sur **Ajouter**.

- Vous devez utiliser **Clone** lorsque cela est indiqué dans une procédure et cloner le profil existant indiqué dans les instructions.
- L'utilisation d'**Ajouter** créera une nouvelle entrée avec des paramètres par défaut différents du clone attendu. Cela entraînera un fonctionnement incorrect.

Liens connexes

Configuration de l'ASBCE pour les extensions SIP distantes à la page 25

Liste de contrôle de la configuration de l'ASBCE

#	Action	Lien/Remarques	✔
1.	Configurer le transfert du port du pare-feu	Acheminez le trafic externe des clients vers l'ASBCE. Voir la section Configuration du pare-feu à la page 30.	
2.	Configurer l'interface réseau ASBCE externe	Définissez les adresses IP externes utilisées par l'ASBCE. Voir la section Configurer l'interface ASBCE externe à la page 31.	
3.	Configurez l'interface réseau ASBCE interne.	Définissez les adresses IP internes utilisées par l'ASBCE. Voir la section Configurer l'interface ASBCE interne à la page 32.	
4.	Créer un profil de client TLS	Ceci définit les paramètres TLS utilisés par l'ASBCE lorsqu'il se connecte à IP Office. Voir la section Création d'un profil de client TLS à la page 34.	
5.	Créer un profil de serveur TLS	Ceci définit les paramètres TLS utilisés par l'ASBCE lorsque les clients et le IP Office s'y connectent. Voir la section Création d'un profil de serveur TLS à la page 35.	
6.	Créer une interface média SIP interne	Définissez les ports et les adresses sur lesquels l'ASBCE écoute les médias SIP provenant d'IP Office. Voir la section Création d'une interface de signalisation interne à la page 39.	

Le tableau continue …

#	Action	Lien/Remarques	✔
7.	Créer une interface média SIP externe	Définissez les ports et les adresses sur lesquels l'ASBCE écoute les médias SIP pour les extensions distantes. Voir la section Création d'une interface de signalisation externe à la page 40.	
8.	Créer une interface de signalisation SIP interne	Définissez les ports et les adresses sur lesquels l'ASBCE écoute la signalisation d'appel SIP provenant d'IP Office. Voir la section Création d'une interface de signalisation interne à la page 39.	
9.	Créer une interface de signalisation SIP externe	Définissez les ports et les adresses sur lesquels l'ASBCE écoute la signalisation d'appel SIP provenant des extensions distantes. Voir la section Création d'une interface de signalisation externe à la page 40.	
10.	Créer un profil de serveur	Voir la section Création d'un profil de serveur ASBCE pour IP Office à la page 41.	
11.	Créer un routage de serveur	Voir la section Création d'un profil de routage de serveur à la page 43.	
12.	Configurer le masquage de topologie	Définissez les conversions des informations d'en-tête SIP que l'ASBCE doit effectuer. Voir la section Création d'une politique de masquage de la topologie de l'ASBCE à la page 44.	
13.	Créer une liste de blocage IP/URL.	Définissez les types de médias pris en charge et le nombre maximal de connexions. Voir la section Création d'une liste de blocage IP/URI à la page 45.	
14.	Créer une règle d'application	Définissez le type et le nombre de connexions média prises en charge. Voir la section Création d'une règle d'application à la page 46.	
15.	Créer une règle de média	Voir la section Création d'une règle de média à la page 48.	
16.	Créer une politique de point d'extrémité	Une politique de point d'extrémité regroupe les règles d'application et de média. Voir la section Création d'un groupe de politique de point d'extrémité à la page 50.	
17.	Ajouter un profil d'agent utilisateur	Définissez les valeurs UA pour les extensions distantes que l'ASBCE doit autoriser à connecter. Voir la section Configuration d'un profil d'agents utilisateurs à la page 51.	
18.	Créer un flux d'abonnés	Voir la section Création du flux d'abonnés à la page 52.	

Le tableau continue …

#	Action	Lien/Remarques	✔
19.	Créer un flux de serveur	Voir la section Création d'un flux de serveur à la page 55.	
20.	Ajouter un proxy inverse pour Client Avaya Workplace	Acheminez les demandes de fichiers de paramètres par les clients vers IP Office. Voir la section Ajout de proxy inverses pour les demandes de fichiers à la page 57.	

Liens connexes

Configuration de l'ASBCE pour les extensions SIP distantes à la page 25

Configuration du pare-feu

Vous devez configurer l'équipement du réseau du client à la périphérie de son réseau pour acheminer le trafic externe des extensions distantes vers l'ASBCE. La procédure réelle varie en fonction du réseau et de l'équipement du client. Les indications suivantes ne sont que des lignes directrices.

Procédure

1. Activez le **NAT de couche 3** uniquement.
2. Désactivez toutes les fonctionnalités compatibles SIP telles que l'ALG.
3. Transférez les ports suivants vers l'adresse IP de l'interface B1 de l'ASBCE.
   - **Pour Client Avaya Workplace et les téléphones de la série J100 :**

Protocole de transport/application		Port	Utilisation
tcp	tls	5061	Connexion SIP TLS pour l'enregistrement.
	http	80	Demandes de fichiers générales et sécurisées provenant des téléphones et des clients si l'option **Utiliser les ports téléphoniques préférés** n'est pas activée sur IP Office.
	https	443	
	http	8411	Demandes de fichiers générales et sécurisées provenant des téléphones et des clients si l'option **Utiliser les ports téléphoniques préférés** est activée sur IP Office.
	https	411	
udp	rtp	40750 to 50750	La plage de ports utilisée pour le trafic RTP (médias d'appel) et RTCP (contrôle d'appel).
	rtcp		

Étapes suivantes

- Allez à Configurer l'interface ASBCE externe à la page 31.

Liens connexes

Configuration de l'ASBCE pour les extensions SIP distantes à la page 25

Configurer l'interface ASBCE externe

Ajoutez des détails pour le réseau du client entre le pare-feu client et l'ASBCE.

- **Prise en charge IPv4/IPv6 double :** Pour prendre en charge les postes distants IPv4 et IPv6, vous devez créer des entrées distinctes pour IPv4 et IPv6 :
  - L'**Addresse IP** pour chacune doit utiliser l'adresse *B1* IPv4 ou IPv6 correspondante.

Important :

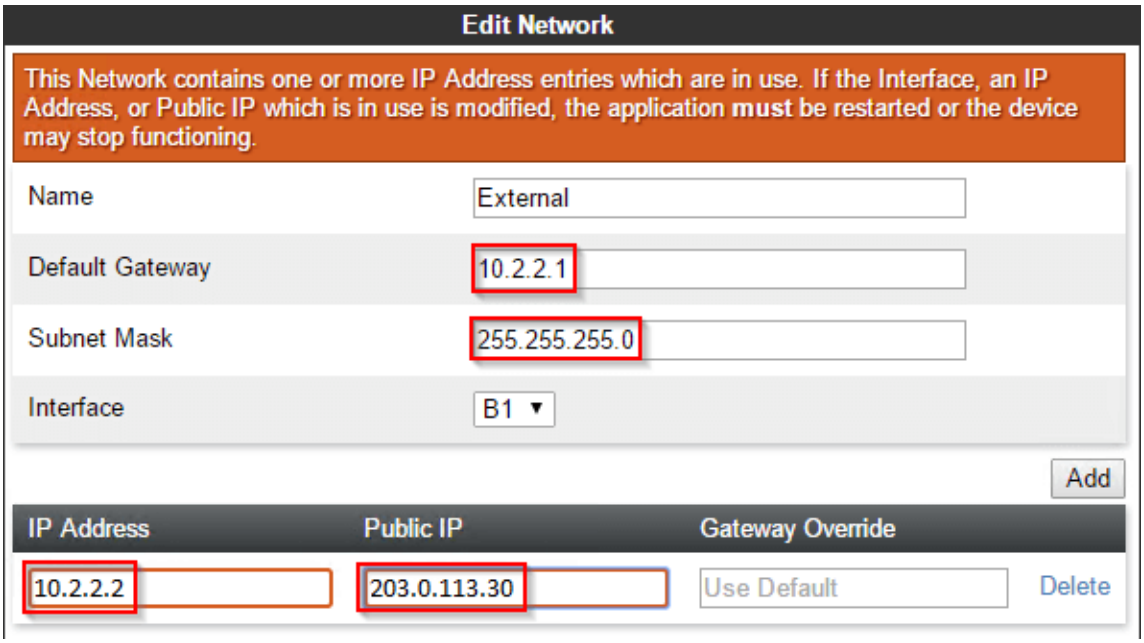
- Cette procédure nécessite le redémarrage de l'ASBCE. Cela mettra fin à toutes les connexions en cours utilisant l'ASBCE.

Préambules

- Configuration du pare-feu à la page 30

Procédure

1. Accédez à **Paramètres spécifiques à l'appareil** > **Gestion de réseau**.
2. Sélectionnez l'onglet **Réseaux** et cliquez sur **Ajouter**.
3. Entrez les données suivantes :



Champ	Description
Nom	Vous utilisez ce nom dans d'autres menus pour sélectionner le réseau.
Passerelle par défaut	L'adresse IP interne de l'équipement qui achemine le trafic entre le réseau du client et l'Internet public. Dans l'exemple de scénario, il s'agit de l'adresse interne du pare-feu.
Masque de sous-réseau	Le masque IP pour le réseau de la **Passerelle par défaut**.
Interface	Sélectionnez l'interface publique de l'ASBCE.

4. Cliquez sur **Ajouter** et saisissez une adresse IP que l'ASBCE utilise sur cette interface réseau.

Champ	Description
Adresse IP	Saisissez l'adresse IP de l'interface ASBCE connectée au pare-feu.
IP publique	Saisissez l'adresse IP publique du pare-feu. Elle doit correspondre à l'adresse IP vers laquelle le DNS dirige l'extension distante lors de la recherche DNS du nom de domaine complet d'IP Office.

5. Si vous prenez en charge les extensions distantes IPv4 et IPv6, répétez la procédure pour créer les entrées IPv6.

Étapes suivantes

- Allez à Configurer l'interface ASBCE interne à la page 32.

Liens connexes

Configuration de l'ASBCE pour les extensions SIP distantes à la page 25

Configurer l'interface ASBCE interne

Ajoutez des détails pour le réseau du client entre l'ASBCE et IP Office.

- **Prise en charge IPv4/IPv6 double :** Vous pouvez utiliser la même entrée pour les postes distants IPv4 et IPv6.

Important :

- Cette procédure nécessite le redémarrage de l'ASBCE. Cela mettra fin à toutes les connexions en cours utilisant l'ASBCE.

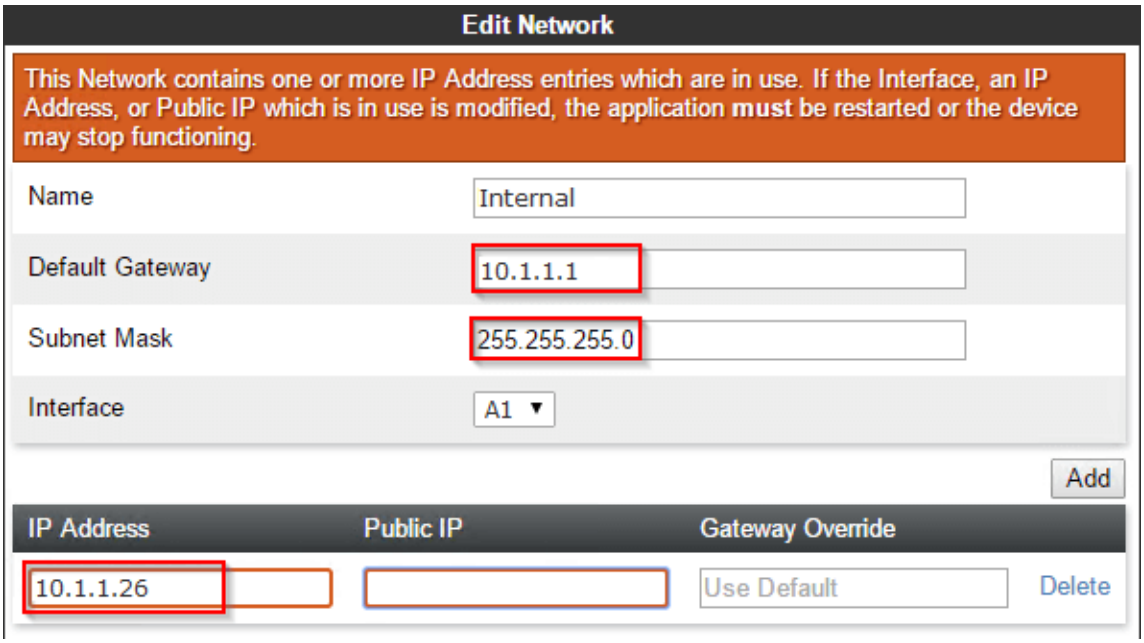
Préambules

- Configurer l'interface ASBCE externe à la page 31

Procédure

1. Accédez à **Paramètres spécifiques à l'appareil** > **Gestion de réseau**.
2. Sélectionnez l'onglet **Réseaux** et cliquez sur **Ajouter**.

3. Entrez les données suivantes :



Champ	Description
Nom	Vous utilisez ce nom dans d'autres menus pour sélectionner le réseau.
Passerelle par défaut	L'adresse IP et la passerelle par défaut pour le trafic à l'intérieur du réseau du client.
Masque de sous-réseau	
Interface	Sélectionnez l'interface privée de l'ASBCE.

4. Cliquez sur **Ajouter** et saisissez une adresse IP que l'ASBCE utilise sur cette interface réseau.

Champ	Description
Adresse IP	Saisissez l'adresse IP de l'interface ASBCE connectée au réseau du client. Il s'agit de l'adresse IP de l'interface A1.

5. Accédez à **Gestion du système** et cliquez sur **Redémarrage de l'application...**.

Étapes suivantes

- Allez à Création d'un profil de client TLS à la page 34.

Liens connexes

Configuration de l'ASBCE pour les extensions SIP distantes à la page 25

Création d'un profil de client TLS

Pour les connexions TLS à partir de l'ASBCE, celui-ci agit en tant que client TLS. Par exemple, pour les connexions à IP Office et aux clients externes. Le profil de client TLS utilisé pour chaque connexion définit les certificats utilisés et les autres paramètres TLS.

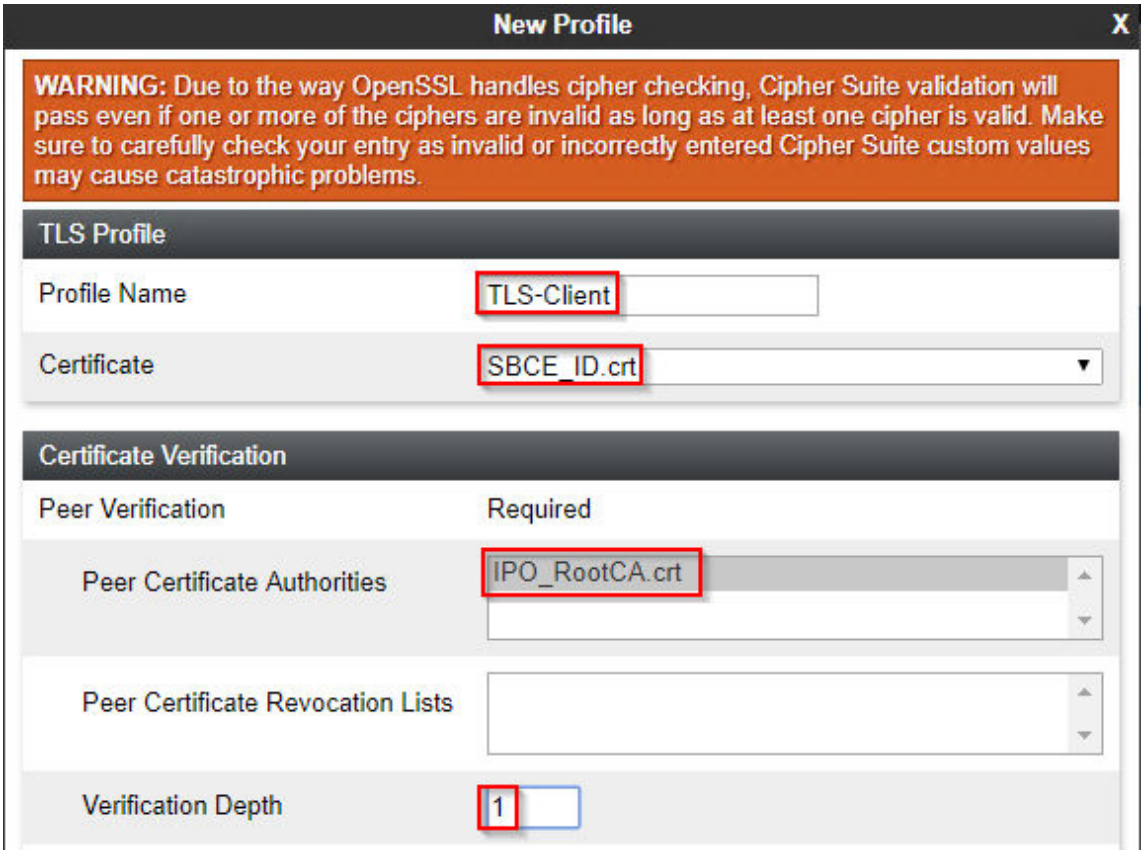
- **Prise en charge IPv4/IPv6 double :** Vous pouvez utiliser la même entrée pour les postes distants IPv4 et IPv6.

Préambules

- Configurer l'interface ASBCE interne à la page 32.

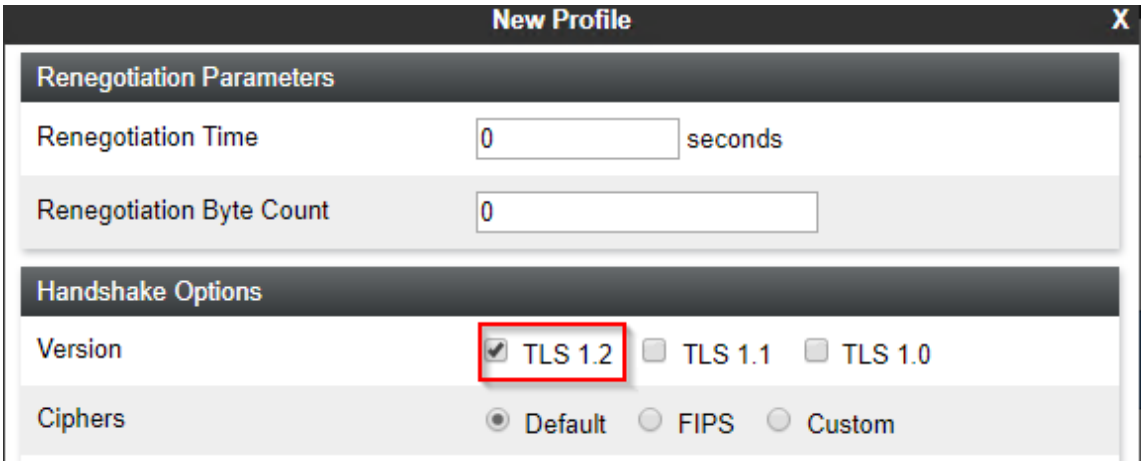
Procédure

1. Sélectionnez **Gestion TLS** > **Profils de client**.
2. Cliquez sur **Ajouter**.



3. Saisissez un nom. Vous pouvez ensuite l'utiliser pour sélectionner la politique dans d'autres menus.
4. Dans **Certificat**, sélectionnez le certificat d'identité créé pour l'ASBCE.
5. Dans **Autorités de certification homologues**, sélectionnez le certificat racine utilisé pour créer le certificat d'identité. Dans l'exemple de scénario, il s'agit du fichier `IPO_RootCA.crt` chargé sur l'ASBCE.
6. Dans **Profondeur de vérification**, saisissez **1**.

7. Cliquez sur **Suivant**.



8. Activez **TLS 1.2**.
9. Cliquez sur **Terminer**.

Étapes suivantes

- Allez à Création d'un profil de serveur TLS à la page 35.

Liens connexes

Configuration de l'ASBCE pour les extensions SIP distantes à la page 25

Création d'un profil de serveur TLS

Pour les connexions TLS à l'ASBCE, celui-ci agit en tant que serveur TLS. Par exemple, pour les connexions à partir d'IP Office et à partir de clients externes. Le profil de client TLS utilisé pour chaque connexion définit les certificats utilisés et les autres paramètres TLS.

- **Prise en charge IPv4/IPv6 double :** Vous pouvez utiliser la même entrée pour les postes distants IPv4 et IPv6.

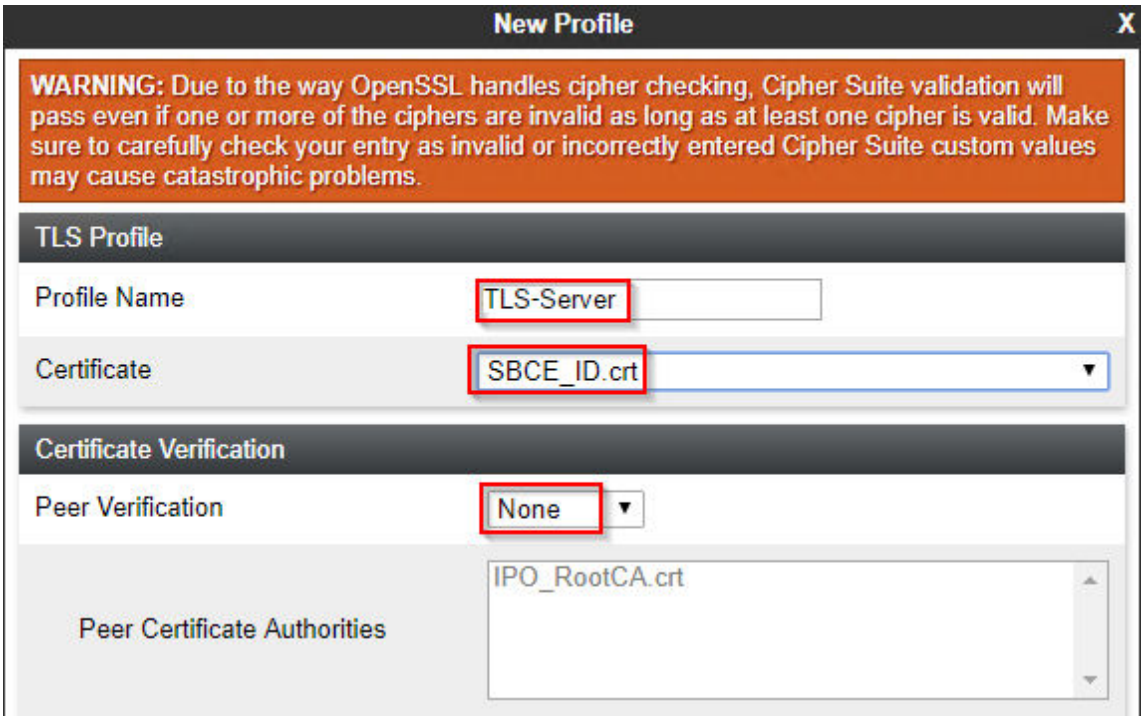
Préambules

- Création d'un profil de client TLS à la page 34.

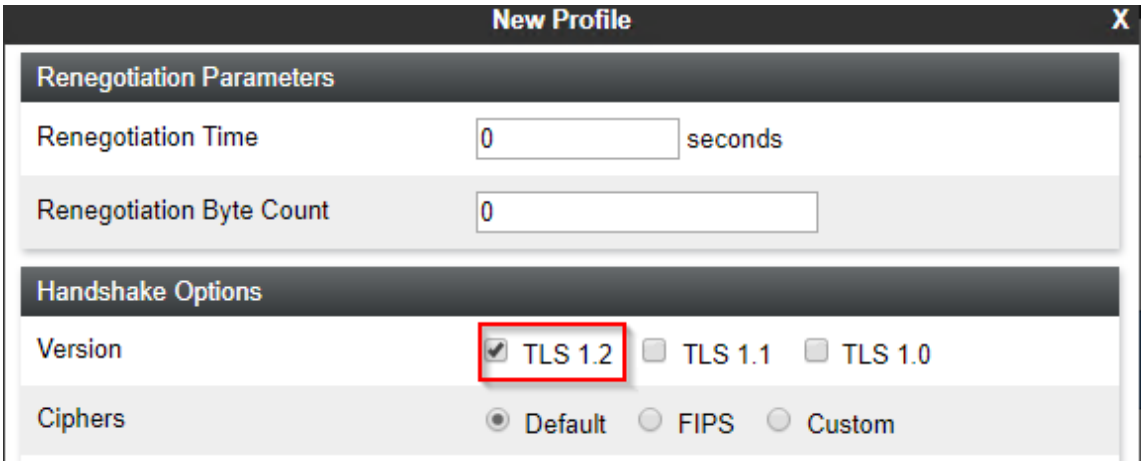
Procédure

1. Sélectionnez **Gestion TLS** > **Profils de client**.

2. Cliquez sur **Ajouter**.



3. Saisissez un nom. Vous pouvez ensuite l'utiliser pour sélectionner la politique dans d'autres menus.
4. Dans **Certificat**, sélectionnez le certificat d'identité créé pour l'ASBCE.
5. Dans **Autorités de certification homologues**, sélectionnez **Aucun**.
6. Cliquez sur **Suivant**.



7. Activez **TLS 1.2**.
8. Cliquez sur **Terminer**.

Étapes suivantes

- Allez à Création d'une interface média interne à la page 37.

Liens connexes

Configuration de l'ASBCE pour les extensions SIP distantes à la page 25

Création d'une interface média interne

Vous devez créer une interface média interne. L'ASBCE l'utilise pour écouter les média d'appel SIP provenant d'IP Office.

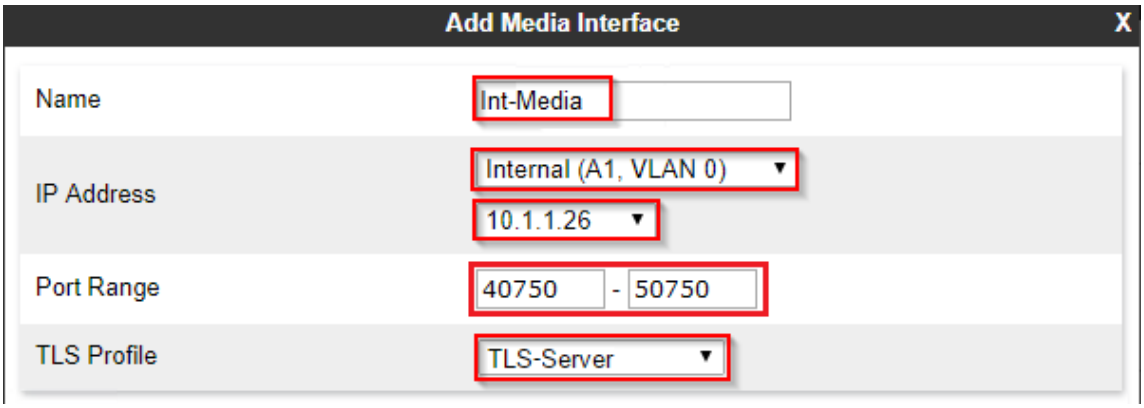
- **Prise en charge IPv4/IPv6 double :** Vous pouvez utiliser la même entrée pour les postes distants IPv4 et IPv6.

Préambules

- Création d'un profil de client TLS à la page 34.

Procédure

1. Sélectionnez **Paramètres spécifiques à l'appareil** > **Interface média**.
2. Cliquez sur **Ajouter**.



3. Saisissez un nom. Vous pouvez ensuite l'utiliser pour sélectionner la politique dans d'autres menus.
4. Sélectionnez l'interface interne de l'ASBCE.
5. Pour **Profil TLS**, sélectionnez le profil de serveur TLS que vous avez créé pour le trafic vers l'ASBCE.
6. Cliquez sur **Terminer**.

Étapes suivantes

- Allez à Création d'une interface média externe à la page 38.

Liens connexes

Configuration de l'ASBCE pour les extensions SIP distantes à la page 25

Création d'une interface média externe

Vous devez créer une interface média externe. L'ASBCE l'utilise pour écouter les médias d'appel SIP provenant des extensions distantes.

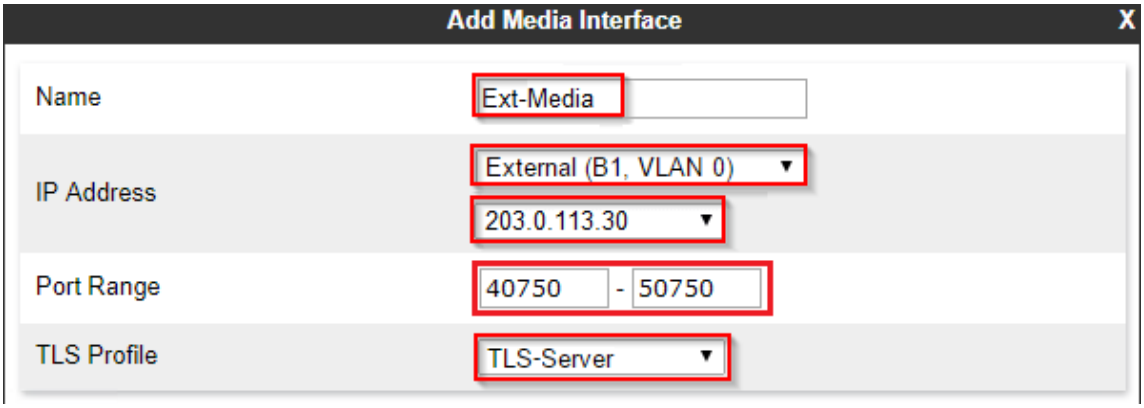
- **Prise en charge IPv4/IPv6 double :** Pour prendre en charge les postes distants IPv4 et IPv6, vous devez créer des entrées distinctes pour IPv4 et IPv6 :
  - L'**Addresse IP** pour chacune doit utiliser l'adresse *B1* IPv4 ou IPv6 correspondante.

Préambules

- Création d'une interface média interne à la page 37.

Procédure

1. Accédez à **Paramètres spécifiques à l'appareil** > **Interface média**.
2. Cliquez sur **Ajouter**.



3. Saisissez un nom. Vous pouvez ensuite l'utiliser pour sélectionner la politique dans d'autres menus.
4. Sélectionnez l'interface externe et l'adresse IP de l'ASBCE.
5. Pour **Profil TLS**, sélectionnez le profil de serveur TLS que vous avez créé pour le trafic vers l'ASBCE.
6. Cliquez sur **Terminer**.
7. Si vous prenez en charge les extensions distantes IPv4 et IPv6, répétez la procédure pour créer les entrées IPv6.

Étapes suivantes

- Allez à Création d'une interface de signalisation interne à la page 39.

Liens connexes

Configuration de l'ASBCE pour les extensions SIP distantes à la page 25

Création d'une interface de signalisation interne

Vous devez créer une interface de signalisation interne. L'ASBCE l'utilise pour écouter la signalisation d'appel SIP provenant d'IP Office.

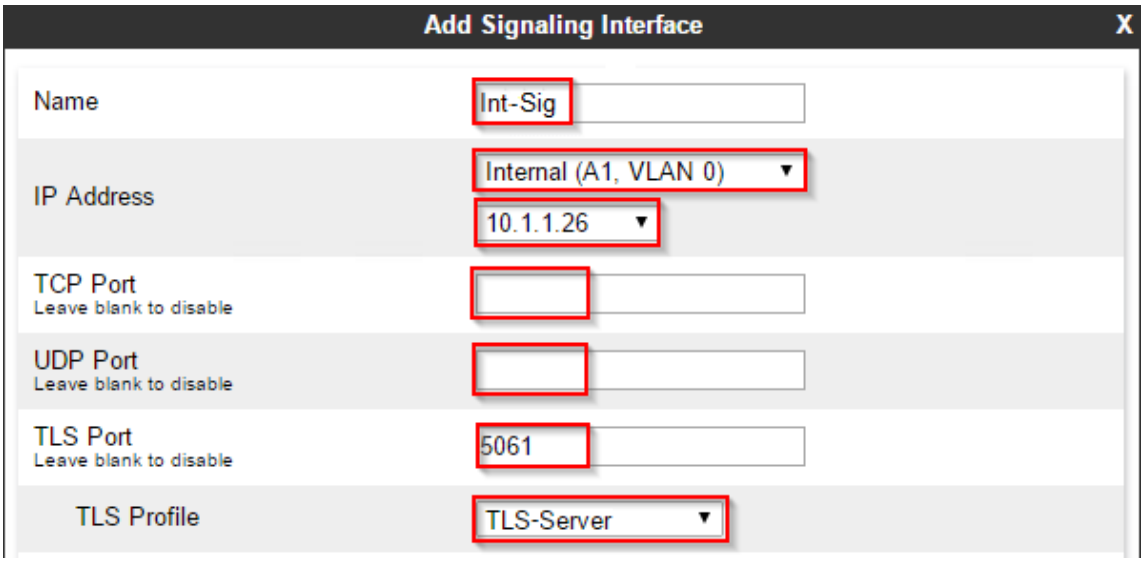
- **Prise en charge IPv4/IPv6 double :** Vous pouvez utiliser la même entrée pour les postes distants IPv4 et IPv6.

Préambules

- Création d'une interface média externe à la page 38.

Procédure

1. Sélectionnez **Paramètres spécifiques à l'appareil** > **Interface de signalisation**.
2. Cliquez sur **Ajouter**.



3. Saisissez un nom. Vous pouvez ensuite l'utiliser pour sélectionner la politique dans d'autres menus.
4. Choisissez *A1* dans la liste déroulante **Addresse IP**.
5. Laissez le champ **Port TCP** vide pour désactiver le TCP.
6. Laissez le champ **Port UDP** vide pour désactiver l'UDP.
7. Définissez le **Port TLS** pour qu'il correspondre au port TLS d'IP Office.
8. Pour **Profil TLS**, sélectionnez le profil de serveur TLS que vous avez créé pour le trafic vers l'ASBCE.
9. Cliquez sur **Terminer**.

Étapes suivantes

- Allez à Création d'une interface de signalisation externe à la page 40.

Liens connexes

Configuration de l'ASBCE pour les extensions SIP distantes à la page 25

Création d'une interface de signalisation externe

Vous devez créer une interface de signalisation externe. L'ASBCE l'utilise pour écouter les messages d'enregistrement SIP provenant des extensions distantes.

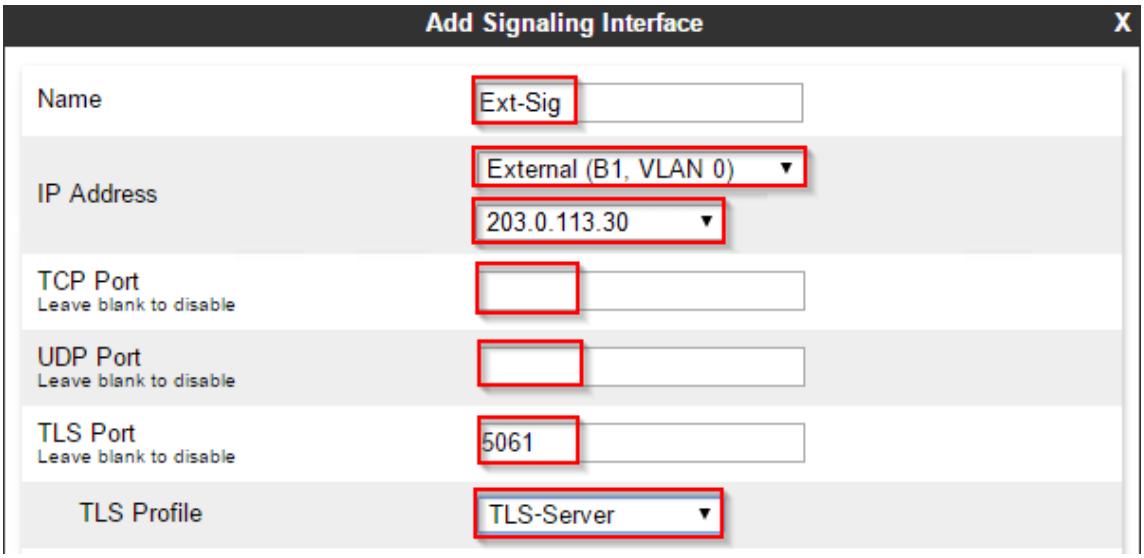
- **Prise en charge IPv4/IPv6 double :** Pour prendre en charge les postes distants IPv4 et IPv6, vous devez créer des entrées distinctes pour IPv4 et IPv6 :
  - L'**Addresse IP** pour chacune doit utiliser l'adresse *B1* IPv4 ou IPv6 correspondante.

Préambules

- Création d'une interface de signalisation interne à la page 39.

Procédure

1. Sélectionnez **Paramètres spécifiques à l'appareil** > **Interface de signalisation**.
2. Cliquez sur **Ajouter**.



3. Saisissez un nom. Vous pouvez ensuite l'utiliser pour sélectionner la politique dans d'autres menus.
4. Choisissez *B1* dans la liste déroulante **Addresse IP**.
5. Laissez le champ **Port TCP** vide pour désactiver le TCP.
6. Laissez le champ **Port UDP** vide pour désactiver l'UDP.
7. Définissez le **Port TLS** pour qu'il correspondre au port TLS d'IP Office.
8. Pour **Profil TLS**, sélectionnez le profil de serveur TLS que vous avez créé pour le trafic vers l'ASBCE.
9. Cliquez sur **Terminer**.
10. Si vous prenez en charge les extensions distantes IPv4 et IPv6, répétez la procédure pour créer les entrées IPv6.

Étapes suivantes

- Allez à Création d'un profil de serveur ASBCE pour IP Office à la page 41.

Liens connexes

Configuration de l'ASBCE pour les extensions SIP distantes à la page 25

Création d'un profil de serveur ASBCE pour IP Office

Vous devez créer un profil de serveur sur l'ASBCE qui correspond à la configuration d'IP Office, voir Configuration VoIP SIP d'IP Office à la page 11.

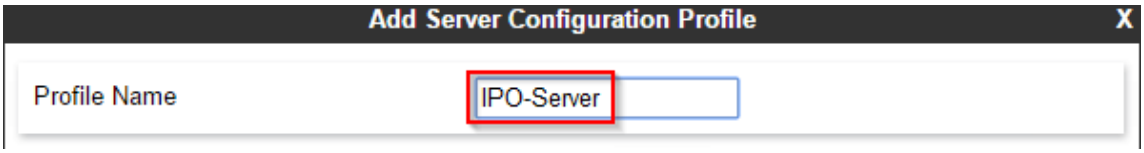
- **Prise en charge IPv4/IPv6 double :** Vous pouvez utiliser la même entrée pour les postes distants IPv4 et IPv6.

Préambules

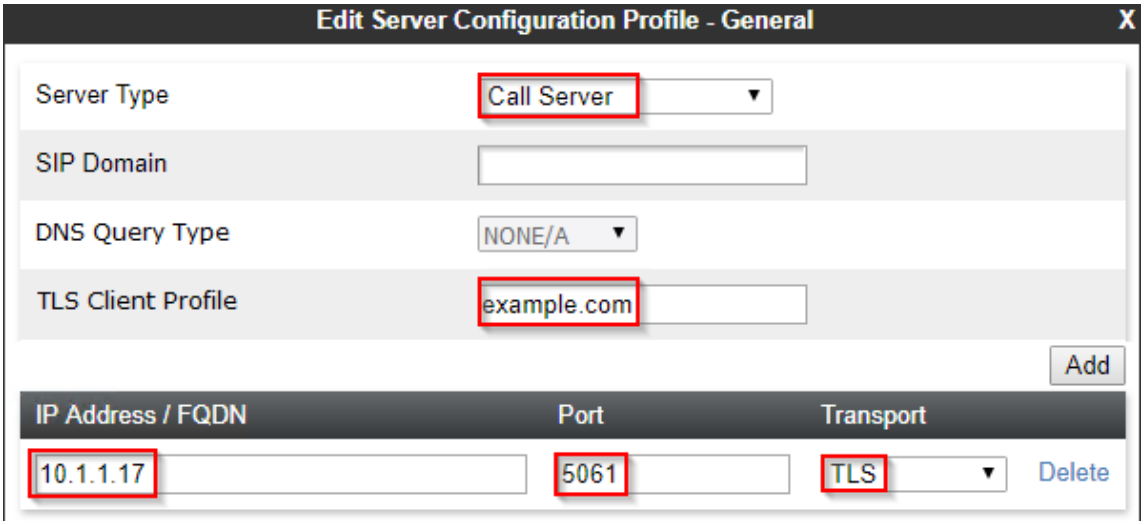
- Création d'une interface de signalisation interne à la page 39.

Procédure

1. Sélectionnez **Profils globaux** > **Configuration du serveur**.
2. Cliquez sur **Ajouter**.
3. Saisissez un nom. Vous pouvez ensuite l'utiliser pour sélectionner la politique dans d'autres menus.



4. Cliquez sur **Suivant**.

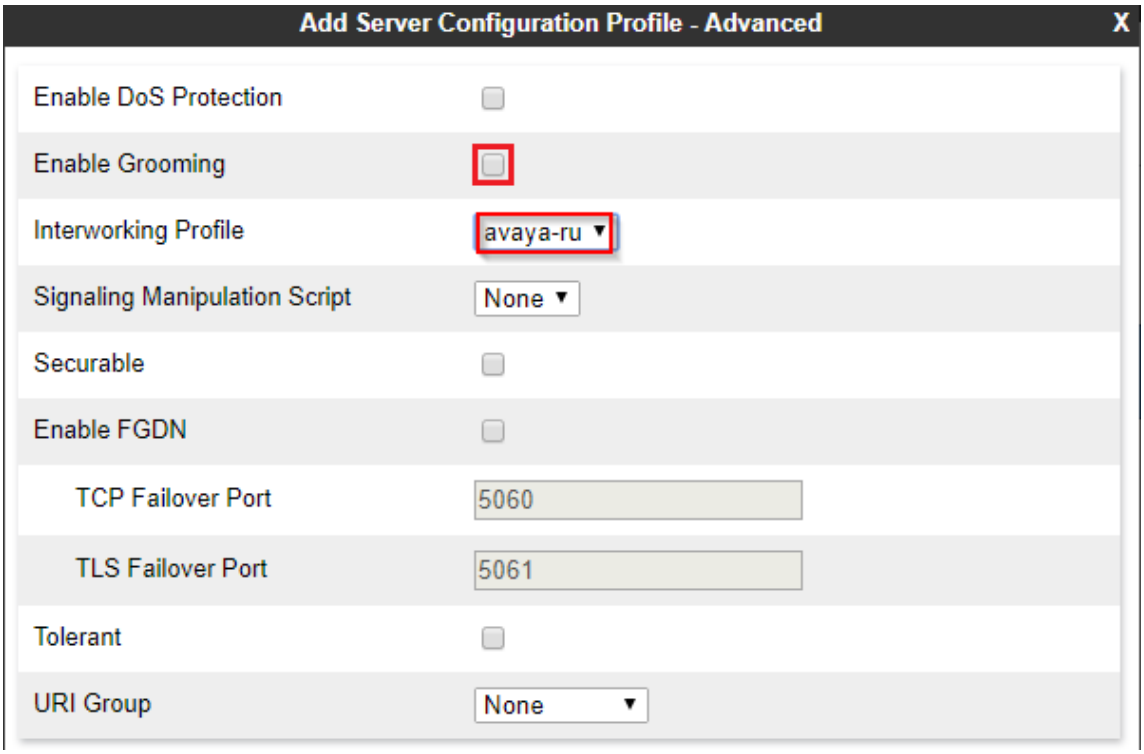


   a. Pour le **Type de serveur**, sélectionnez **Serveur d'appels**.
   b. Définissez le **Domaine SIP** pour qu'il corresponde à celui utilisé par IP Office pour l'enregistrement SIP.
   c. Pour le **Profil de client TLS**, sélectionnez le profil de client TLS que vous avez créé.

d. Cliquez sur **Ajouter** et saisissez les détails des connexions SIP de port de couche 4 définies dans la configuration d'IP Office.
   - Définissez l'**Adresse IP/FQDN** sur l'adresse IP d'IP Office.
   - Définissez le **Port** et le **Transport** pour qu'ils correspondent aux paramètres d'IP Office.

e. Cliquez sur **Suivant**.

5. Cliquez sur **Suivant** pour ignorer les paramètres d'**Authentification**.
6. Cliquez sur **Suivant** pour ignorer les paramètres de **Pulsation**.
7. Réglez les paramètres avancés comme suit :



a. Décochez la case **Activer l'entretien**.

b. Définissez **Profil d'interfonctionnement** sur *avaya-ru*.

8. Cliquez sur **Terminer**.

Étapes suivantes

- Allez à Création d'un profil de routage de serveur à la page 43.

Liens connexes

Configuration de l'ASBCE pour les extensions SIP distantes à la page 25

Création d'un profil de routage de serveur

L'ASBCE utilise un profil de routage de serveur pour acheminer le trafic entrant correspondant vers le ou les serveurs appropriés. Dans ce cas, vous devez créer un profil qui achemine le trafic vers IP Office.

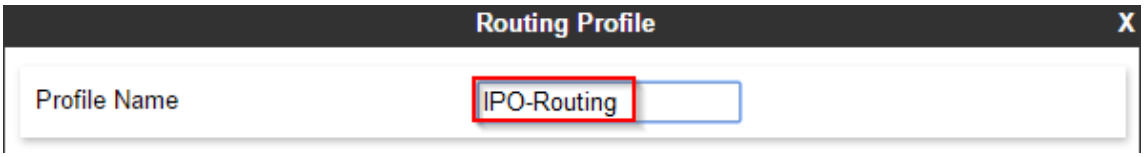
- **Prise en charge IPv4/IPv6 double :** Vous pouvez utiliser la même entrée pour les postes distants IPv4 et IPv6.

Préambules

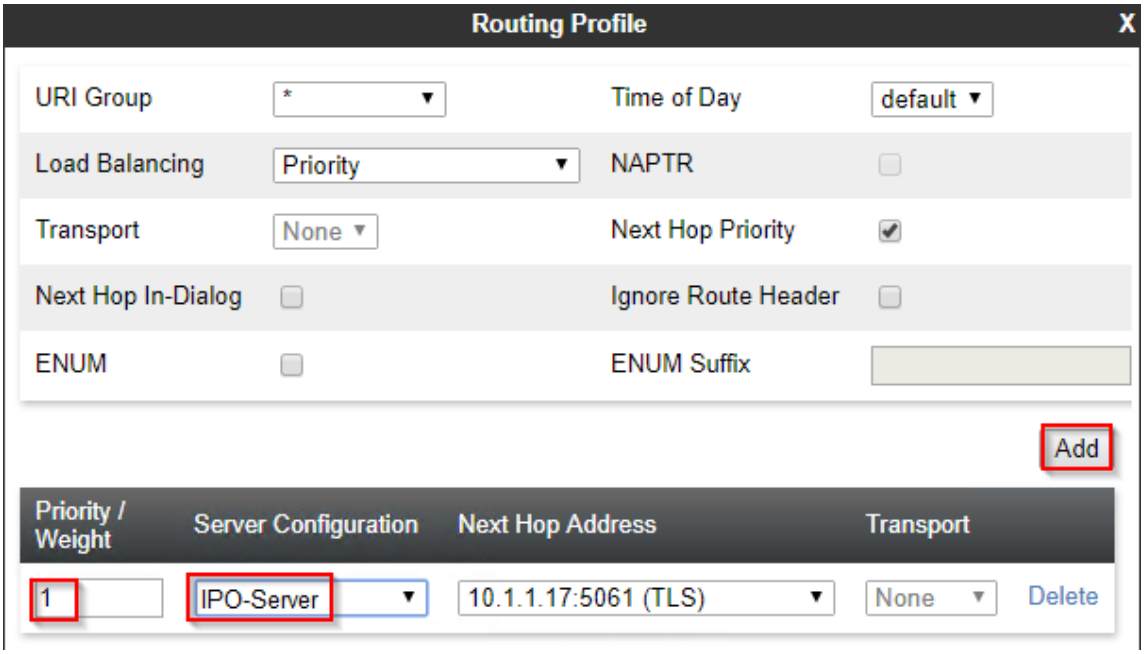
- Création d'un profil de serveur ASBCE pour IP Office à la page 41.

Procédure

1. Sélectionnez **Profils globaux** > **Routage**.
2. Cliquez sur **Ajouter**.
3. Saisissez un nom. Vous pouvez ensuite l'utiliser pour sélectionner la politique dans d'autres menus.



4. Cliquez sur **Suivant**.



5. Cliquez sur **Ajouter**.
6. Définissez la **Priorité** sur 1.
7. Définissez la **Configuration du serveur** sur le profil de serveur créé pour IP Office.
8. Dans **Adresse de saut suivant**, sélectionnez l'adresse IP d'IP Office.
9. Cliquez sur **Terminer**.

Étapes suivantes

- Allez à Création d'une politique de masquage de la topologie de l'ASBCE à la page 44.

Liens connexes

Configuration de l'ASBCE pour les extensions SIP distantes à la page 25

Création d'une politique de masquage de la topologie de l'ASBCE

L'ASBCE peut utiliser le paramètre de masquage de la topologie pour supprimer ou remplacer des valeurs dans les messages SIP. Par exemple, remplacez une adresse IP dans un en-tête SIP par un nom de domaine complet requis.

- **Prise en charge IPv4/IPv6 double :** Vous pouvez utiliser la même entrée pour les postes distants IPv4 et IPv6.

Préambules

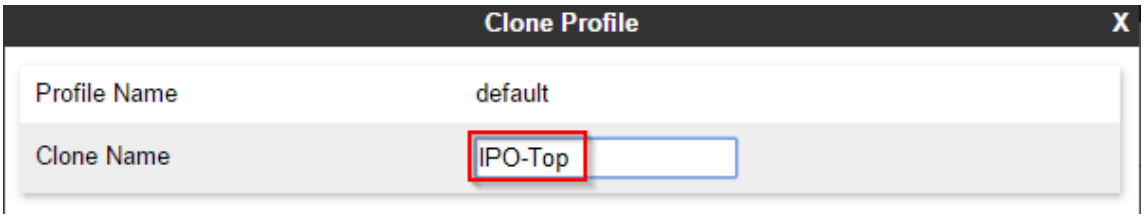
- Création d'un profil de routage de serveur à la page 43.

Procédure

1. Sélectionnez **Profils globaux** > **Masquage de topologie**.
2. Sélectionnez le profil par défaut et cliquez sur **Clone**.

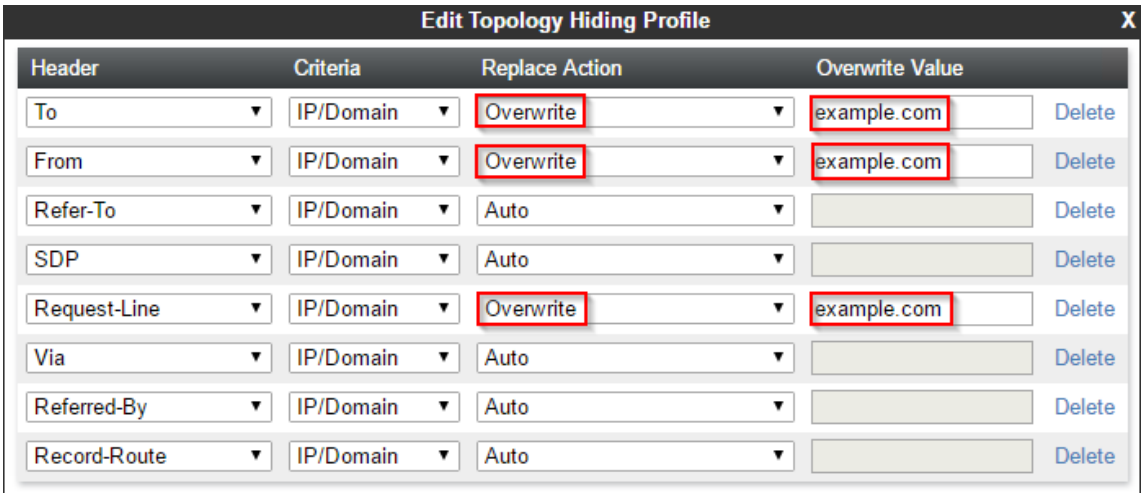
   Important :

   - Vous devez utiliser **Clone** et le profil ou la politique indiqués. L'utilisation de **Ajouter** permet de créer un nouveau profil ou une nouvelle politique avec différents paramètres par défaut.
3. Saisissez un nom. Vous pouvez ensuite l'utiliser pour sélectionner la politique dans d'autres menus.



4. Cliquez sur **Terminer**.

5. Sélectionnez le nouveau profil et cliquez sur **Modifier**.



6. Pour les champs **À**, **De**, **Refer-To**, **SDP**, et **Request-Line** :
   a. Définissez le **Action de remplacement** sur **Remplacer**.
   b. Entrez le domaine IP Office en tant que **Valeur de remplacement**.
7. Cliquez sur **Terminer**.

Étapes suivantes

- Allez à Création d'une liste de blocage IP/URI à la page 45.

Liens connexes

Configuration de l'ASBCE pour les extensions SIP distantes à la page 25

Création d'une liste de blocage IP/URI

Vous pouvez utiliser une liste de blocage pour que l'ASBCE bloque les adresses IP et les URI à l'origine des demandes d'enregistrement ayant échoué. Vous pouvez ensuite ajouter la liste de blocage à tout flux d'abonnés et proxy inverses que vous créez.

- **Prise en charge IPv4/IPv6 double :** Vous pouvez utiliser la même entrée pour les postes distants IPv4 et IPv6.

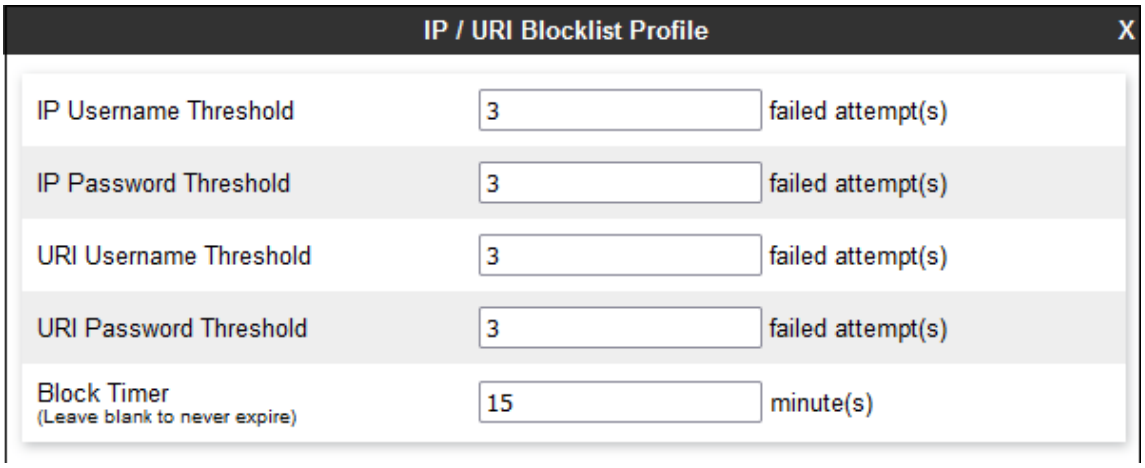
Préambules

- Création d'une politique de masquage de la topologie de l'ASBCE à la page 44.

Procédure

1. Sélectionnez **Politiques de domaine** > **Profil de la liste de blocage IP/URI**.

2. Cliquez sur **Ajouter**.



3. Saisissez un nom. Vous pouvez ensuite l'utiliser pour sélectionner la politique dans d'autres menus.
4. Définissez le nombre d'échecs de tentatives de nom et de mot de passe autorisés.
5. Définissez la durée pendant laquelle une adresse IP ou un URI est bloqué après avoir dépassé l'une des limites définies.
6. Cliquez sur **Terminer**.

Étapes suivantes

- Passez à Création d'une règle d'application à la page 46.

Liens connexes

Configuration de l'ASBCE pour les extensions SIP distantes à la page 25

Création d'une règle d'application

Vous pouvez utiliser une règle d'application pour restreindre le type de connexions média autorisées par l'ASBCE. Elle peut également définir le nombre maximal de ces connexions et le nombre maximal de connexions par extension distante.

- **Prise en charge IPv4/IPv6 double :** Vous pouvez utiliser la même entrée pour les postes distants IPv4 et IPv6.

Préambules

- Création d'une liste de blocage IP/URI à la page 45.

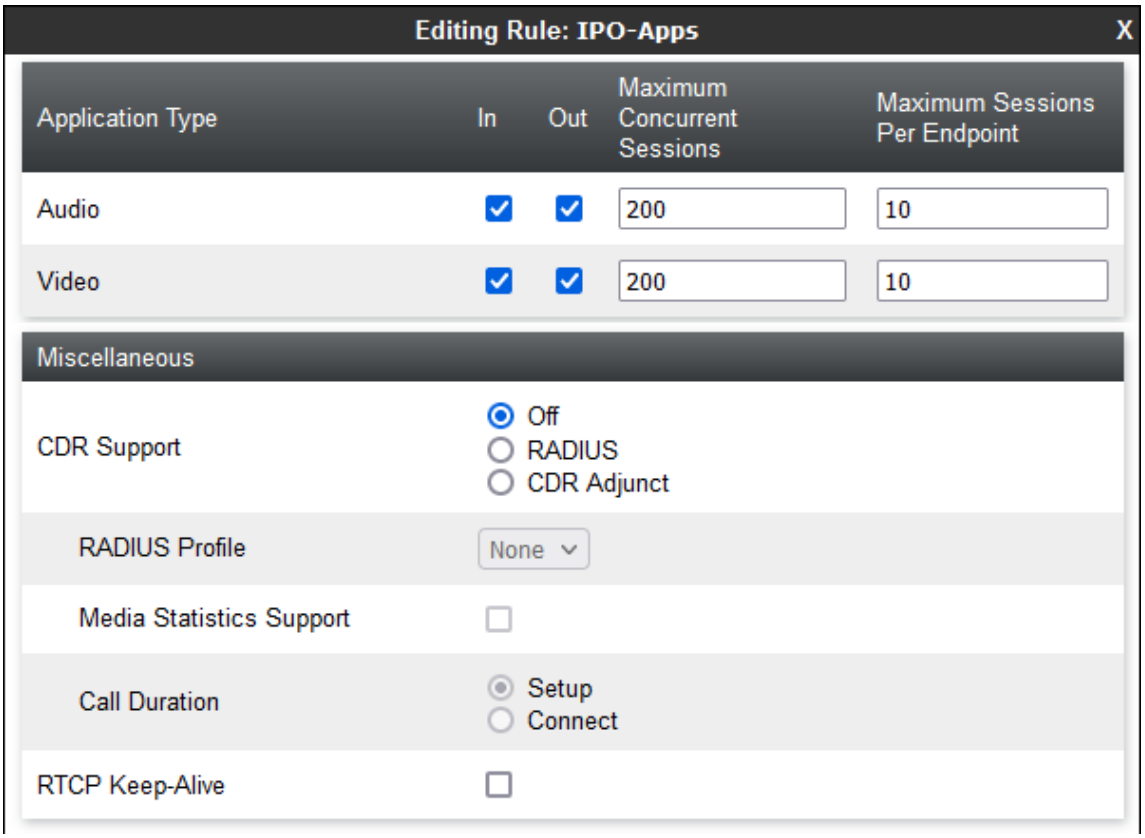
Procédure

1. Sélectionnez **Politiques de domaine** > **Règles d'application**.
2. Sélectionnez la politique *default-low* et cliquez sur **Clone**.

Important :

- Vous devez utiliser **Clone** et le profil ou la politique indiqués. L'utilisation de **Ajouter** permet de créer un nouveau profil ou une nouvelle politique avec différents paramètres par défaut.

3. Saisissez un nom. Vous pouvez ensuite l'utiliser pour sélectionner la politique dans d'autres menus.
4. Cliquez sur **Terminer**.
5. Sélectionnez la nouvelle politique et cliquez sur **Modifier**.
6. Sélectionnez si vous souhaitez autoriser l'**Audio** et/ou la **Vidéo**.



7. Pour chacun des éléments ci-dessus, définissez le **Nombre maximal de sessions simultanées** et le **Nombre maximal de sessions par point d'extrémité**.
8. Cliquez sur **Terminer**.

Étapes suivantes

- Passez à Création d'une règle de média à la page 48.

Liens connexes

Configuration de l'ASBCE pour les extensions SIP distantes à la page 25

Création d'une règle de média

Vous pouvez utiliser une règle de média pour définir différents paramètres de média.

- **Prise en charge IPv4/IPv6 double :** Vous pouvez utiliser la même entrée pour les postes distants IPv4 et IPv6.

Préambules

- Création d'une règle d'application à la page 46.

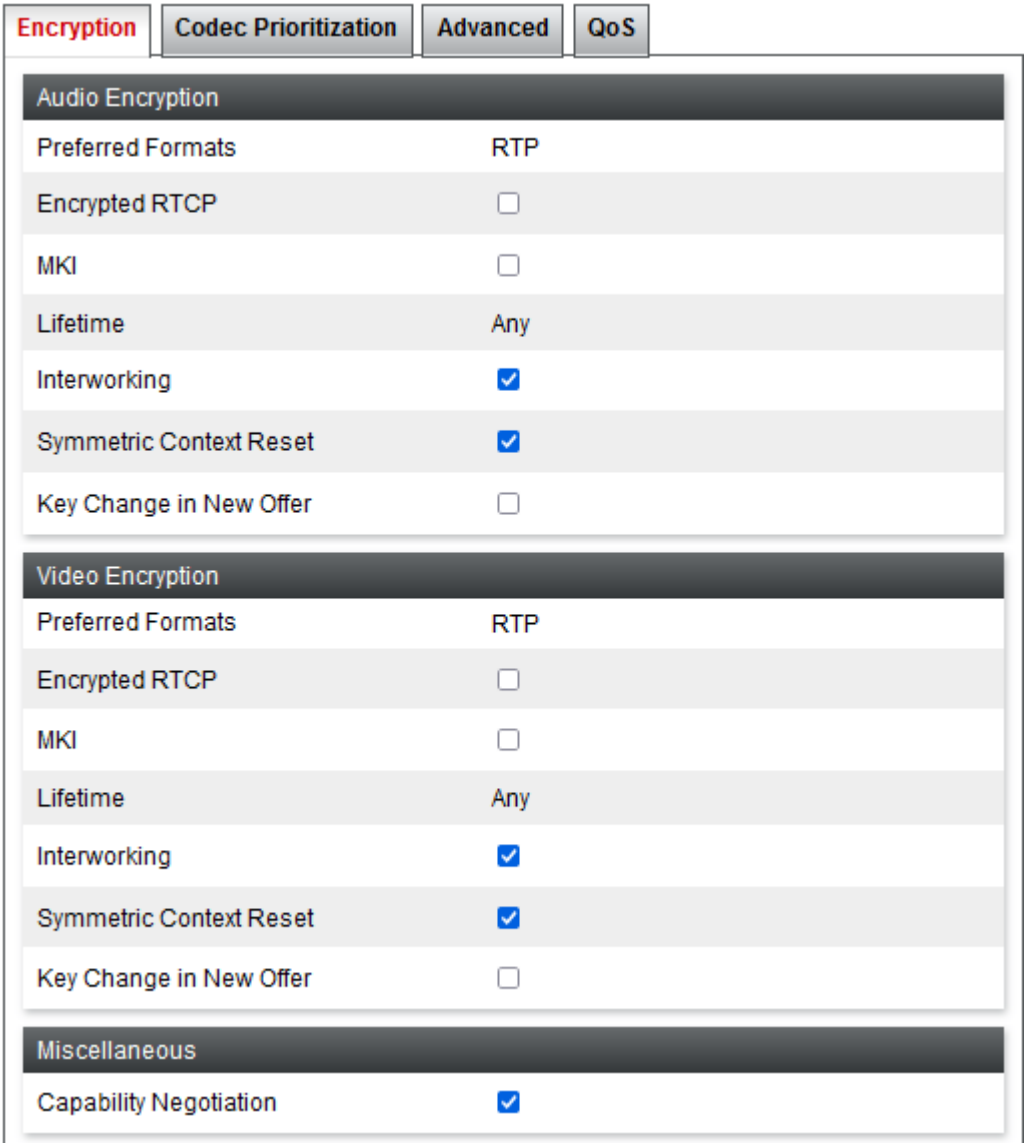
Procédure

1. Sélectionnez **Politiques de domaine** > **Règles de média**.
2. Sélectionnez la politique *avaya-low-med-enc* et cliquez sur **Clone**.

   Important :

   - Vous devez utiliser **Clone** et le profil ou la politique indiqués. L'utilisation de **Ajouter** permet de créer un nouveau profil ou une nouvelle politique avec différents paramètres par défaut.
3. Saisissez un nom. Vous pouvez ensuite l'utiliser pour sélectionner la politique dans d'autres menus.
4. Cliquez sur **Terminer**.
5. Sélectionnez la nouvelle politique et cliquez sur **Modifier**.

6. Pour les options **Chiffrement audio** et **Chiffrement vidéo**, définissez les **Formats préférés** sur *RTP*.



   - Si vous utilisez SRTP, définissez les valeurs **Formats préférés** et **RTCP chiffré** pour qu'elles correspondent aux paramètres **Sécurité VoIP** définis sur IP Office.
7. Vérifiez que le paramètre **Options avancées** > **ANAT activé** n'est pas sélectionné.
8. Cliquez sur **Terminer**.

Étapes suivantes

- Passez à Création d'un groupe de politique de point d'extrémité à la page 50.

Liens connexes

Configuration de l'ASBCE pour les extensions SIP distantes à la page 25

Création d'un groupe de politique de point d'extrémité

Une politique de point d'extrémité regroupe les règles telles que les règles de média et d'applications. Après avoir créé une politique de point d'extrémité, vous pouvez l'associer aux flux d'abonnés et de serveur que vous créez.

- **Prise en charge IPv4/IPv6 double :** Vous pouvez utiliser la même entrée pour les postes distants IPv4 et IPv6.

Préambules

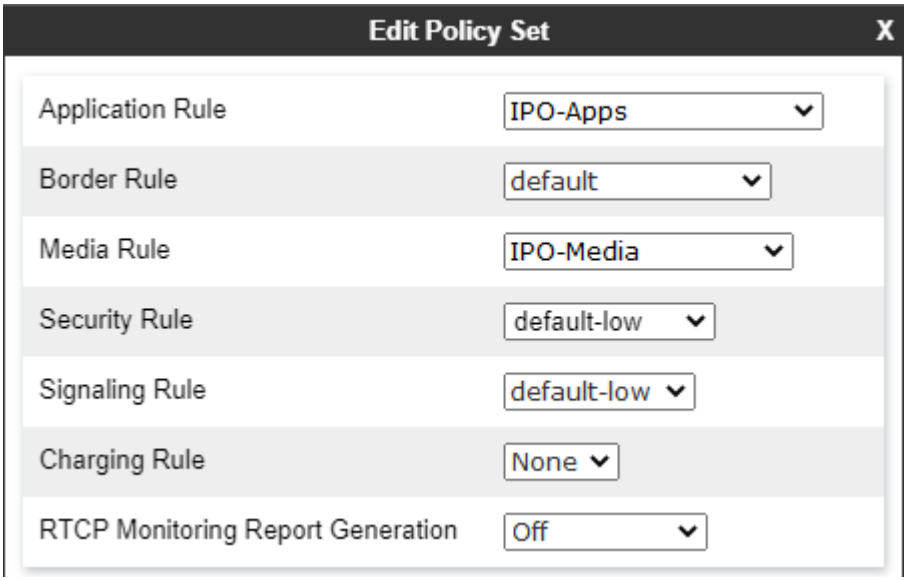
- Création d'une règle de média à la page 48.

Procédure

1. Sélectionnez **Politiques de domaine** > **Groupes de politiques de points d'extrémité**.
2. Sélectionnez la politique *default-low* et cliquez sur **Clone**.

   Important :

   - Vous devez utiliser **Clone** et le profil ou la politique indiqués. L'utilisation de **Ajouter** permet de créer un nouveau profil ou une nouvelle politique avec différents paramètres par défaut.
3. Saisissez un nom. Vous pouvez ensuite l'utiliser pour sélectionner la politique dans d'autres menus.
4. Cliquez sur **Terminer**.
5. Sélectionnez la nouvelle politique et cliquez sur **Modifier**.
6. Dans **Règle d'application**, sélectionnez les règles d'application et de média que vous avez créées pour les extensions distantes.



7. Dans **Règle de média**, sélectionnez la règle de média que vous avez créée.
8. Cliquez sur **Terminer**.

Étapes suivantes

- Passez à Configuration d'un profil d'agents utilisateurs à la page 51.

Liens connexes

Configuration de l'ASBCE pour les extensions SIP distantes à la page 25

Configuration d'un profil d'agents utilisateurs

Vous pouvez utiliser les **Agents utilisateurs** pour restreindre la connexion ASBCE aux clients et aux téléphones qui envoient une chaîne d'*User Agent* (*UA*) appropriée. Sinon, tout téléphone ou client peut se connecter.

- **Prise en charge IPv4/IPv6 double :** Vous pouvez utiliser la même entrée pour les postes distants IPv4 et IPv6.

Voici des exemples de chaînes *UA* envoyées par les clients Avaya.

Téléphone ou client Avaya	Agent utilisateur
Téléphones Avaya série 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)*

- Comme illustré dans les exemples ci-dessus, la chaîne *UA* peut varier en fonction de la version du logiciel et/ou de la plateforme.
- Vous pouvez afficher l'*UA* envoyée par un téléphone ou un téléphone logiciel particulier dans SysMonitor après avoir enregistré le téléphone ou le client.

La correspondance UA utilise une correspondance de chaîne d'expression régulière (regex). Voici des exemples de chaînes regex :

Expression régulière	Description
`Avaya.*`	Correspond à tout *UA* commençant par *Avaya*. *.* correspond à n'importe quel caractère. *.** correspond à n'importe quel nombre de caractères.
`Avaya J1.*`	Correspond à la chaîne *UA* de tout téléphone de la série J100.
`Avaya (J1|Communicator).*`	Correspond à la chaîne *UA* des téléphones de la série J100 et d'Client Avaya Workplace. Les parenthèses *( )* encadrent les correspondances potentielles, chaque correspondance potentielle étant séparée par un caractère |.
`Avaya Communicator\/3\.0 \(3\.33.*`	Correspond à la chaîne *UA* de la version Windows 3.33 d'Client Avaya Workplace uniquement. L'expression regex utilise le caractère \ pour préfixer les caractères qui seraient autrement traités comme des commandes regex. Par exemple, *.* correspond à n'importe quel caractère tandis que *\.* correspond uniquement au caractère *.* littéral.

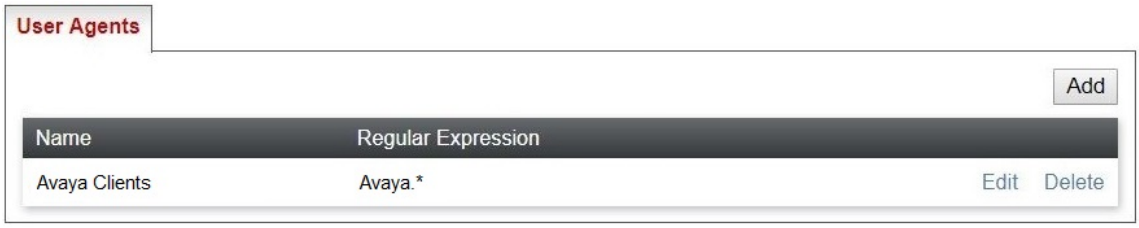
Pour plus d'informations sur la création de chaînes regex, reportez-vous à https://learn.microsoft.com/en-us/dotnet/standard/base-types/regular-expression-language-quick-reference et à https://regex101.com.

Préambules

- Création d'une politique de masquage de la topologie de l'ASBCE à la page 44.

Procédure

1. Sélectionnez **Gestion du système** > **Paramètres globaux** > **Agents utilisateurs**.
2. Cliquez sur **Ajouter**.



3. Saisissez un nom. Vous pouvez ensuite l'utiliser pour sélectionner la politique dans d'autres menus.
4. Entrez l'expression régulière pour la ou les chaînes d'agent utilisateur que vous souhaitez faire correspondre.
5. Cliquez sur **Terminer**.

Étapes suivantes

- Allez à Création du flux d'abonnés à la page 52.

Liens connexes

Configuration de l'ASBCE pour les extensions SIP distantes à la page 25

Création du flux d'abonnés

L'ASBCE utilise un flux d'abonnés pour traiter les connexions entrantes à partir des extensions distantes.

- **Prise en charge IPv4/IPv6 double :** Pour prendre en charge les postes distants IPv4 et IPv6, vous devez créer des entrées distinctes pour IPv4 et IPv6 :
  - L'**Interface de signalisation** et l'**Interface média** pour chacune doivent utiliser les interfaces IPv4 ou IPv6 externes correspondantes.

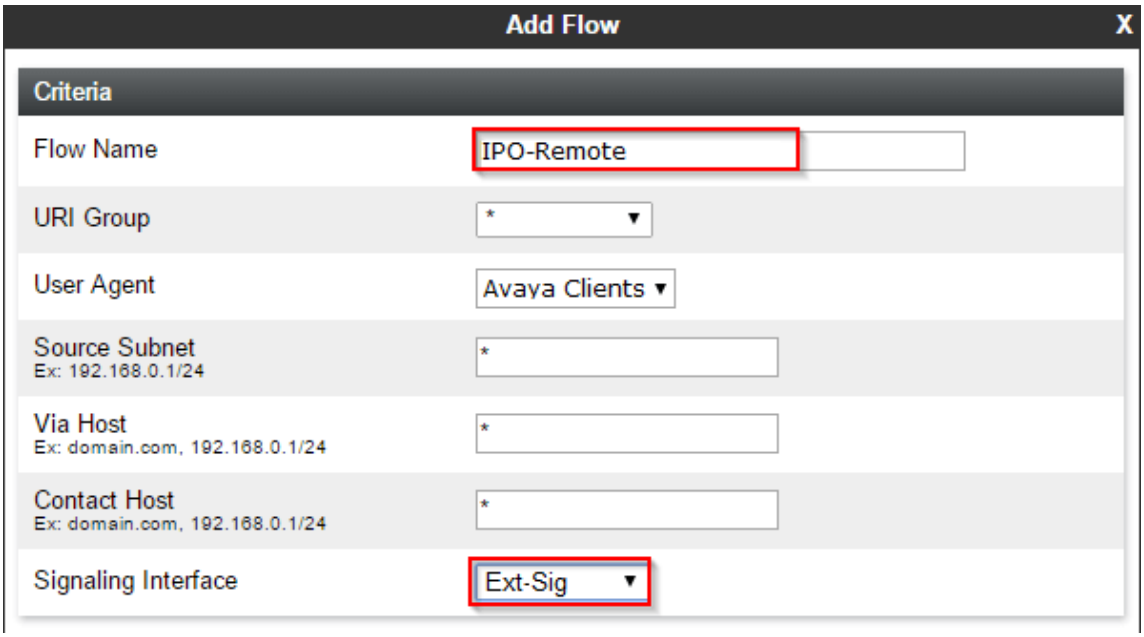
Préambules

- Configuration d'un profil d'agents utilisateurs à la page 51.

Procédure

1. Sélectionnez **Paramètres spécifiques à l'appareil** > **Flux de points d'extrémité**.

2. Sélectionnez l'onglet **Flux d'abonnés** et cliquez sur **Ajouter**.

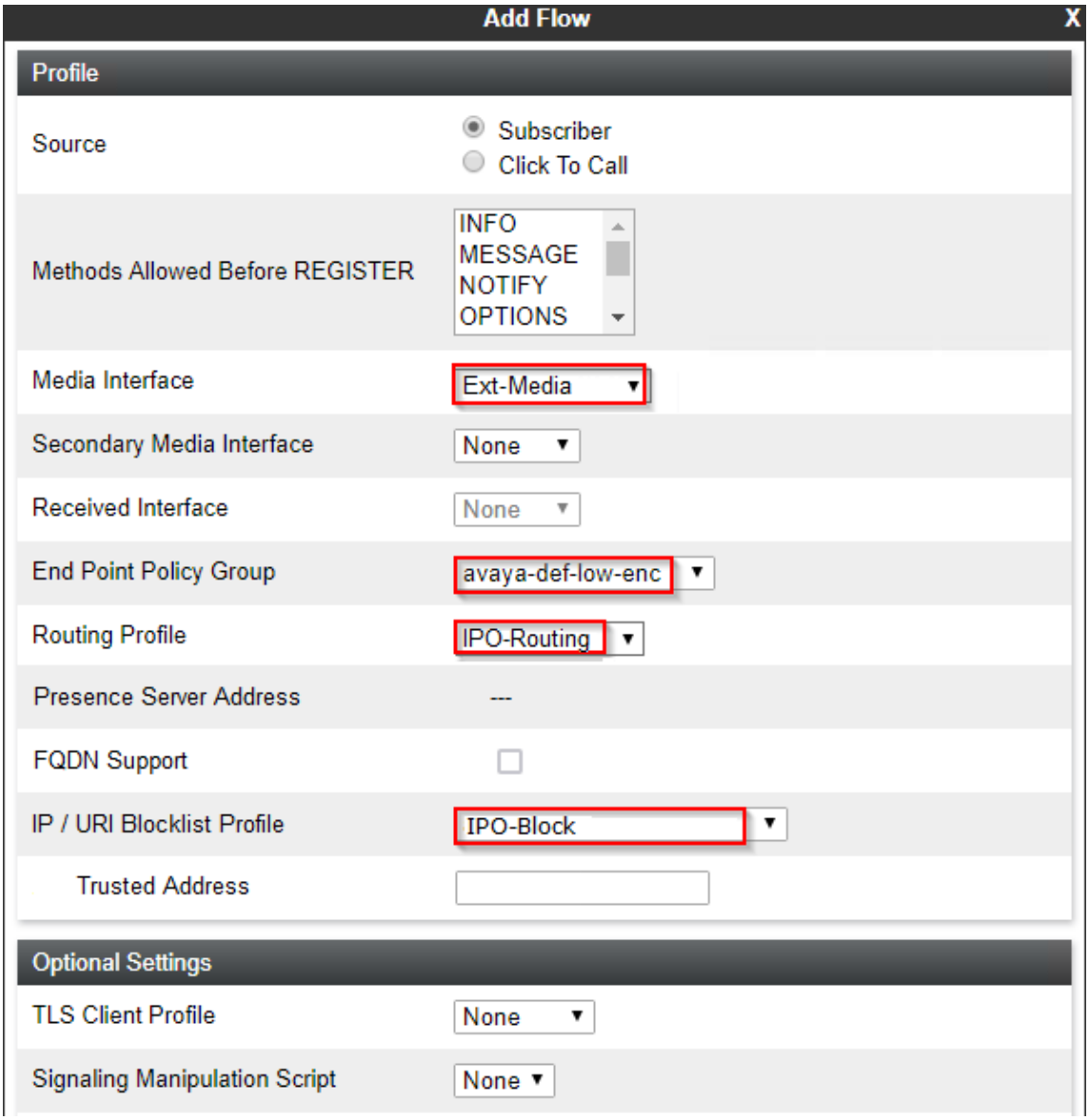


a. Saisissez un nom. Vous pouvez ensuite l'utiliser pour sélectionner la politique dans d'autres menus.

b. Si nécessaire, sélectionnez le profil d'**Agent utilisateur** que vous avez créé pour correspondre à l'agent utilisateur des clients autorisés à utiliser le flux d'abonnés.

c. Sélectionnez l'**Interface de signalisation** externe créé pour les extensions distantes.

3. Cliquez sur **Suivant**.



   a. Dans **Interface média**, sélectionnez l'interface média externe créée pour les extensions distantes.
   b. Dans **Groupe de politiques de points d'extrémité**, sélectionnez *avaya-def-low-enc*.
   c. Dans **Profil de routage**, sélectionnez le profil de routage du serveur créé pour IP Office.
   d. Si vous avez créé un profil de liste de blocage, sélectionnez-le à l'aide de la liste déroulante **Profil de la liste de blocage IP/URI**.

4. Cliquez sur **Terminer**.
5. Si vous prenez en charge les extensions distantes IPv4 et IPv6, répétez la procédure pour créer les entrées IPv6.

Étapes suivantes

- Allez à Création d'un flux de serveur à la page 55.

Liens connexes

Configuration de l'ASBCE pour les extensions SIP distantes à la page 25

Création d'un flux de serveur

L'ASBCE utilise un flux de serveur pour traiter les connexions entrantes à partir du serveur IP Office.

- **Prise en charge IPv4/IPv6 double :** Pour prendre en charge les postes distants IPv4 et IPv6, vous devez créer des entrées distinctes pour IPv4 et IPv6 :
  - L'**Interface reçue** pour chaque flux de serveur doit utiliser l'interface de signalisation externe IPv4 ou IPv6 correspondante.

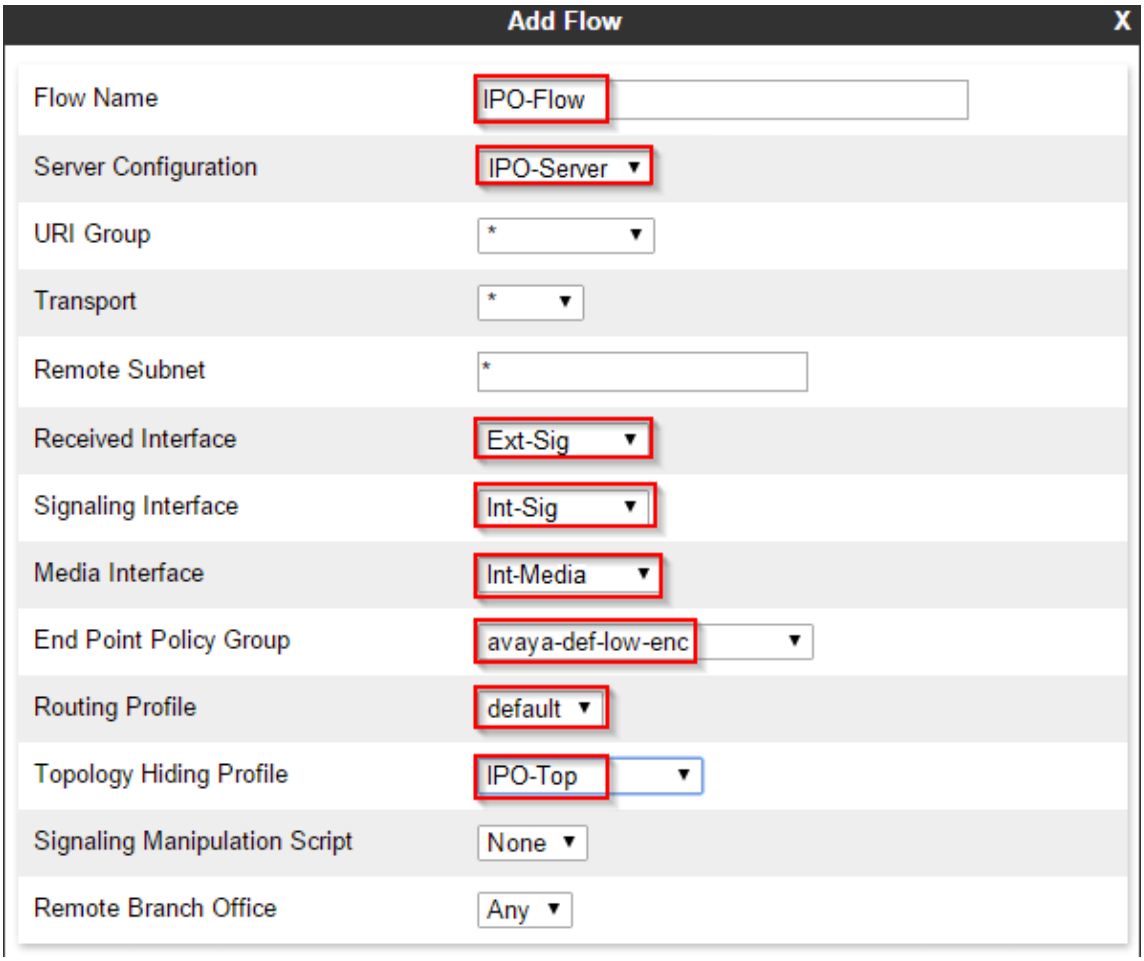
Préambules

- Création du flux d'abonnés à la page 52.

Procédure

1. Sélectionnez **Paramètres spécifiques à l'appareil** > **Flux de points d'extrémité**.

2. Sélectionnez l'onglet **Flux de serveur** et cliquez sur **Ajouter**.



   a. Dans **Nom de flux**, saisissez un nom descriptif.
   b. Dans **Configuration du serveur**, sélectionnez le profil de serveur créé pour le serveur IP Office.
   c. Dans **Interface reçue**, sélectionnez l'interface de signalisation externe créée pour les extensions distantes.
   d. Dans **Interface de signalisation**, sélectionnez l'interface de signalisation interne créée pour les extensions distantes.
   e. Dans **Interface média**, sélectionnez l'interface média interne créée pour les extensions distantes.
   f. Dans **Groupe de politiques de points d'extrémité**, sélectionnez *avaya-def-low-enc*.
   g. Dans **Profil de routage**, sélectionnez *default*.
   h. Dans **Topologie de profil de marquage**, sélectionnez le profil de masquage de topologie créé pour les extensions distantes IP Office.
3. Cliquez sur **Terminer**.
4. Si vous prenez en charge les extensions distantes IPv4 et IPv6, répétez la procédure pour créer les entrées IPv6.

Étapes suivantes

- Allez à Ajout de proxy inverses pour les demandes de fichiers à la page 57.

Liens connexes

Configuration de l'ASBCE pour les extensions SIP distantes à la page 25

Ajout de proxy inverses pour les demandes de fichiers

Voici un exemple de création de proxy inverses pour les extensions distantes. Ils permettent aux extensions distantes de demander des fichiers à IP Office. Par exemple, la demande des fichiers `46xxsettings.txt` et `46xxspecials.txt`.

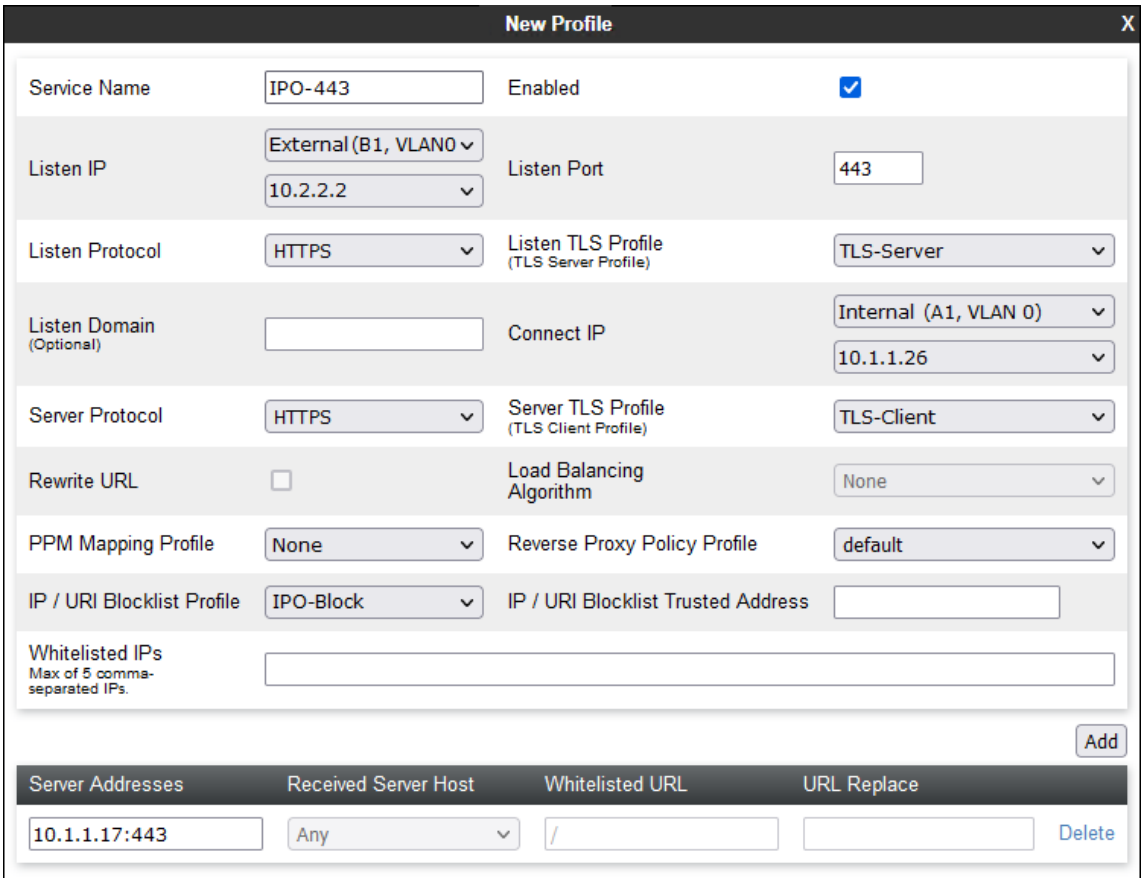
Les ports et le protocole requis dépendent des exigences du type d'extension distante.

- Par défaut, pour que la connexion initiale à IP Office demande le fichier `46xxsettings.txt`, les extensions utilisent soit `http`, soit `https`. IP Office utilise respectivement le port `80` et le port `443`.
- Les paramètres du fichier `46xxsettings.txt` indiquent à l'extension distante les ports et protocoles à utiliser pour les connexions futures.
- Si l'option **Système** > **Système** > **Utiliser les ports téléphoniques préférés** est activée, le fichier `46xxsettings.txt` indique aux téléphones et aux clients d'utiliser le port `8411` pour HTTP et le port `411` pour les requêtes de fichiers HTTPS, et ces ports sont activés sur IP Office.
  - Lorsque l'option **Utiliser les ports téléphoniques préférés** est activée, IP Office autorise toujours les connexions sur le port `80` et le port `443`. IP Office requiert cela pour la connexion initiale et pour les clients hérités.
- **Prise en charge IPv4/IPv6 double :** Pour prendre en charge les postes distants IPv4 et IPv6, vous devez créer des entrées distinctes pour IPv4 et IPv6. Chacune utilise les interfaces externes IPv4 et IPv6 respectives.

Procédure

1. Sélectionnez **Paramètres spécifiques à l'appareil** > **Services DMZ** > **Services de relais**.

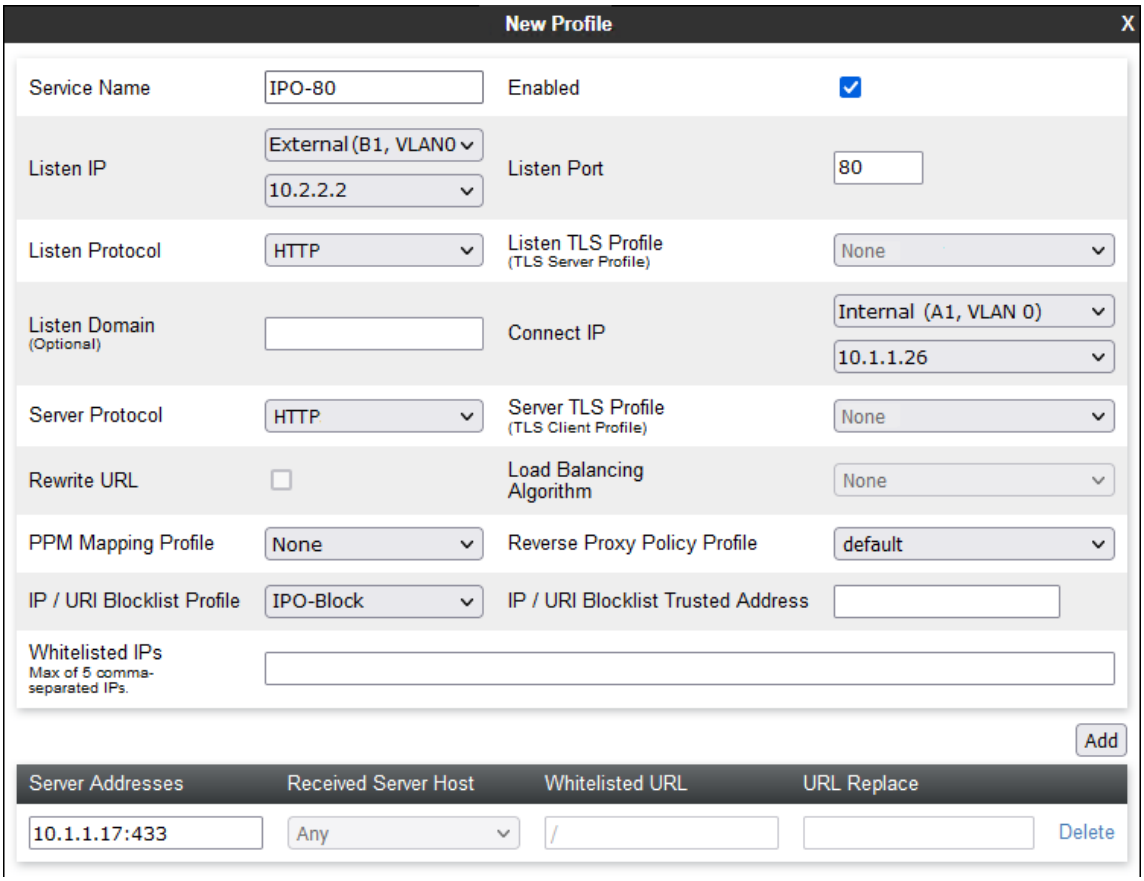
2. Sélectionnez l'onglet **Proxy inverse** et cliquez sur **Ajouter**.



   a. Dans **Nom de service**, saisissez un nom descriptif pour le proxy inverse.
   b. Dans **IP d'écoute**, sélectionnez l'interface *B1* externe et l'adresse IP.
   c. Définissez le **Port d'écoute** sur `443`.
   d. Définissez le **Protocole d'écoute** sur **HTTPS**.
   e. Dans **Profil TLS d'écoute**, sélectionnez le profil du serveur TLS.
   f. Dans **IP de connexion**, sélectionnez l'interface *A1* interne et l'adresse IP.
   g. Dans **Protocole du serveur**, sélectionnez **HTTPS**.
   h. Dans **Profile TLS du serveur**, sélectionnez le profil du client TLS.
   i. Si vous avez créé une liste de blocage, sélectionnez-la à l'aide de la liste déroulante **Profil de la liste de blocage IP/URI**.
   j. Cliquez sur **Ajouter** :
   k. Pour **Adresse du serveur**, saisissez l'adresse IP d'IP Office suivie de `:443`.

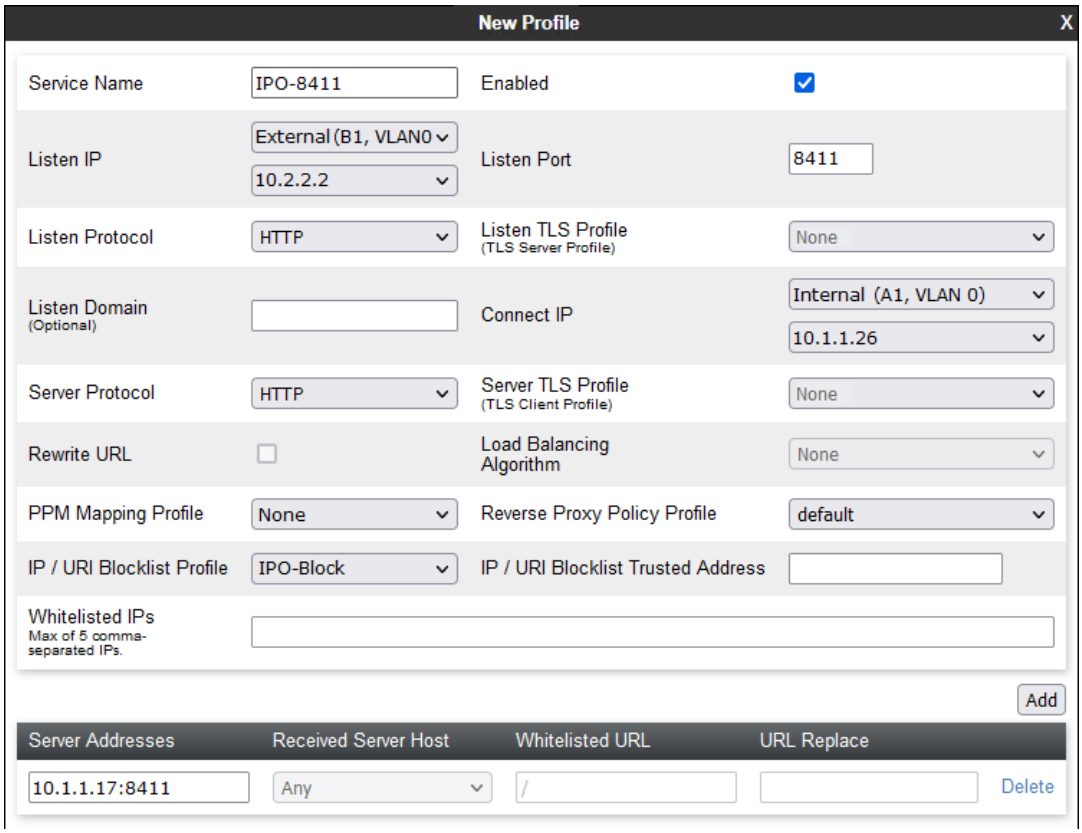
3. Cliquez sur **Terminer**.

4. Répétez la procédure pour ajouter un proxy pour les requêtes de fichiers HTTP de port `80`. Ce proxy n'utilise aucun profil TLS.

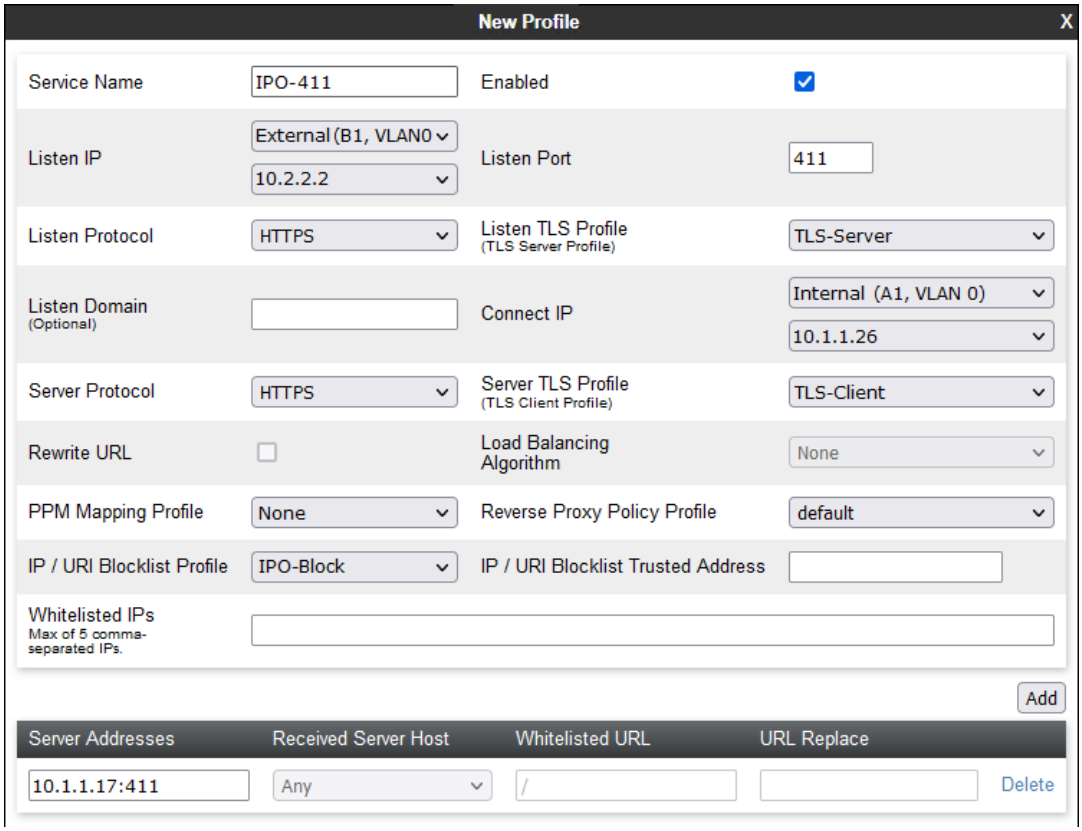


5. Cliquez sur **Terminer**.

6. Si l'option **Utiliser les ports téléphoniques préférés** est activée sur IP Office :
   a. Ajoutez un proxy inverse pour HTTP sur le port `8411`.



b. Ajoutez un proxy inverse pour HTTPS sur le port `411`.



7. Si vous prenez en charge les extensions distantes IPv4 et IPv6, répétez la procédure pour créer les entrées IPv6.

Liens connexes

Configuration de l'ASBCE pour les extensions SIP distantes à la page 25

Chapitre 5 : Désancrage des médias d'appel de l'ASBCE

L'ASBCE reste normalement partie prenante de tous les appels qu'il achemine. Tous les médias d'appel et la signalisation d'appel restent ancrés à l'ASBCE, et nécessitent donc une bande passante et un traitement de la part de l'ASBCE.

Dans les scénarios où les réseaux impliqués prennent en charge le routage direct entre toutes les extrémités de l'appel, vous pouvez désancrer le média d'appel de l'ASBCE. Le désancrage réduit la bande passante et les ressources requises par l'ASBCE. L'ASBCE continue à traiter la signalisation d'appel.

- Pour les extensions distantes sur le même sous-réseau distant, le désancrage de l'ASBCE permet un support direct entre les extensions distantes sur ce sous-réseau.
- Vous pouvez également utiliser le désancrage dans d'autres scénarios. Par exemple, entre des extensions distantes sur deux sous-réseaux distincts. Pour plus d'informations, voir https://documentation.avaya.com/bundle/GUID-416B16B1-7DB4-4C01-A966-3E62EFEA4D43/page/Media_Unanchoring_scenarios.html.

Le désancrage utilise les éléments de configuration de l'ASBCE supplémentaires suivants :

- **Flux de session**

  Un flux de session définit une paire de plages d'adresses réseau et la politique de session que l'ASBCE doit appliquer pour le trafic entre ces réseaux. Pour les supports directs sur un site distant, la plage d'adresses du site est définie pour les deux réseaux dans le flux de session.

- **Politique de session**

  Une politique de session définit la manière dont l'ASBCE doit traiter les médias d'appel. Vous pouvez utiliser la même politique de session pour plusieurs flux de session.

Liens connexes

Création d'une politique de session pour un site distant à la page 62
Création d'un flux de session pour le site distant à la page 64

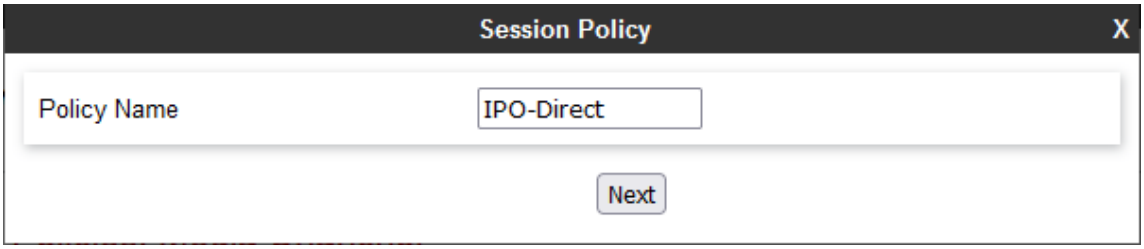
Création d'une politique de session pour un site distant

Une politique de session définit la manière dont l'ASBCE doit traiter le trafic entre les sites correspondant à tout flux de session qui utilise la politique. Vous pouvez utiliser la même politique pour plusieurs flux de session. Autrement dit, pour plusieurs sites distants.

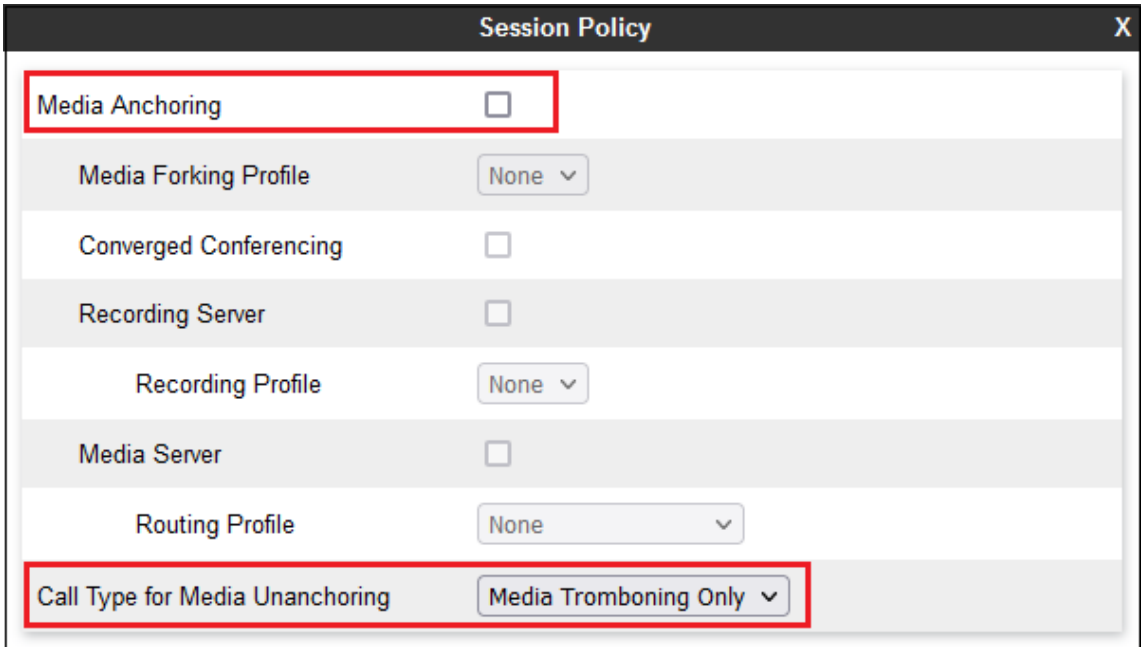
Procédure

1. Sélectionnez **Politiques de domaine** > **Politiques de session**.

2. Cliquez sur **Ajouter**.
3. Saisissez un nom. Vous pouvez ensuite l'utiliser pour sélectionner la politique dans d'autres menus.



4. Cliquez sur **Suivant**.



5. Désélectionnez **Ancrage des médias**.
6. Définissez le **Type d'appel pour le désancrage des médias** sur **Tromboning des médias uniquement**.
7. Cliquez sur **Terminer**.

Étapes suivantes

- Allez à Création d'un flux de session pour le site distant à la page 64.

Liens connexes

Désancrage des médias d'appel de l'ASBCE à la page 62

Création d'un flux de session pour le site distant

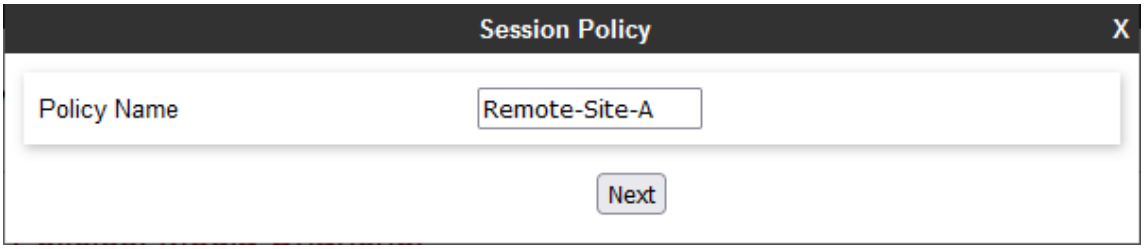
Un flux de session définit les plages d'adresses entre lesquelles l'ASBCE doit appliquer une politique de session. Pour un sous-réseau distant, les plages d'adresses des deux côtés sont les mêmes.

Préambules

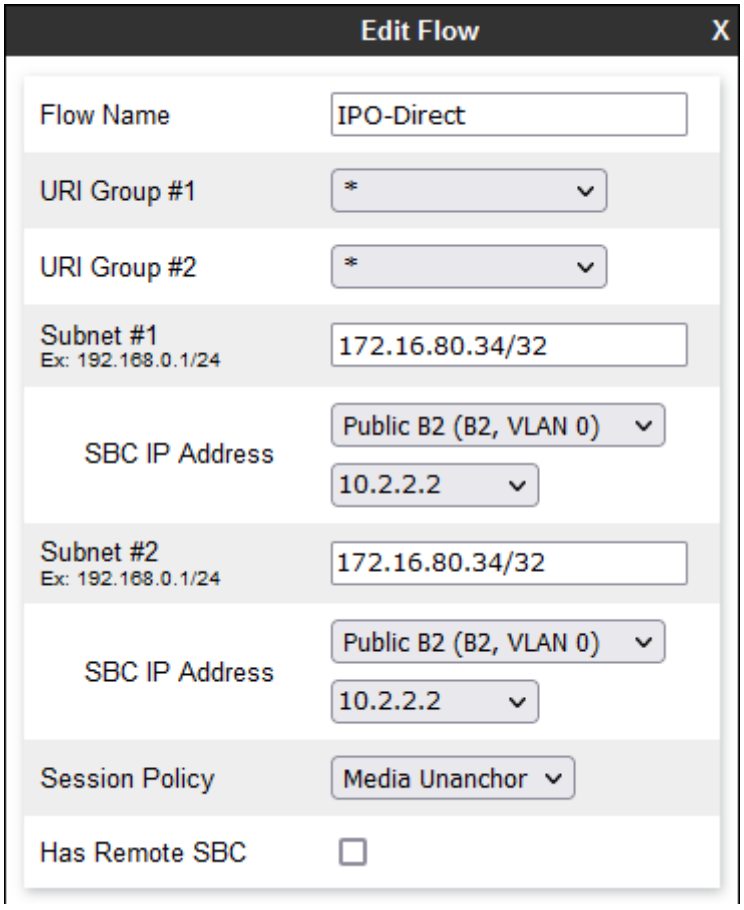
- Création d'une politique de session pour un site distant à la page 62.

Procédure

1. Sélectionnez **Réseau et flux** > **Flux de sessions**.
2. Cliquez sur **Ajouter**.
3. Saisissez un nom. Vous pouvez ensuite l'utiliser pour sélectionner la politique dans d'autres menus.



4. Cliquez sur **Suivant**.



5. Pour **Subnet#1**, définissez la plage d'adresses IP utilisée par les extensions distantes sur le site distant. Définissez l'**Adresse IP SBC** sur l'interface externe de l'ASBCE.
6. Définissez les mêmes valeurs pour **Subnet#2**.
7. Pour la **Politique de session**, sélectionnez la politique de session que vous avez créée.
8. Cliquez sur **Terminer**.

Liens connexes

Désancrage des médias d'appel de l'ASBCE à la page 62

Chapitre 6 : Prise en charge d'Client Avaya Workplace en tant qu'extension distante

Cette section fournit des remarques sur le fonctionnement d'Client Avaya Workplace lorsqu'il est utilisé comme extension SIP distante pour IP Office.

Liens connexes

[Enregistrement SIP d'Client Avaya Workplace](#) à la page 66
[Vérification des paramètres distants](#) à la page 67

Enregistrement SIP d'Client Avaya Workplace

1. Les utilisateurs peuvent utiliser les méthodes suivantes pour enregistrer leur Client Avaya Workplace au démarrage :
   - **Enregistrement direct :**

     L'utilisateur saisit l'adresse d'IP Office sous la forme `https://<IPOffice_FQDN>/46xxsettings.txt` où `://<IPOffice_FQDN>/` est le FQDN du registrar SIP configuré sur IP Office.

     - Pour les extensions distantes, le DNS public résout le FQDN à l'adresse IP publique du pare-feu réseau du client.
     - Pour l'IPv6, l'utilisateur doit utiliser `https://<SBC_FQDN>/46xxsettings.txt` où <SBC_FQDN> est le FQDN de l'ASBCE.
   - **Enregistrement de l'adresse par e-mail :**

     L'utilisateur saisit son adresse e-mail. Le client contacte Avaya Spaces, où le profil configuré pour le domaine de messagerie du client fournit l'adresse FQDN du système IP Office.

     - Cette méthode d'enregistrement n'est pas prise en charge pour les postes distants IPv6.
   - **Connexion SSO :**

     Cette méthode de connexion utilise les mêmes informations de profil Avaya Spaces que celles utilisées pour l'enregistrement par e-mail ci-dessus.

     - Cette méthode d'enregistrement n'est pas prise en charge pour les postes distants IPv6.

2. Après avoir reçu un fichier `46xxsettings.txt` de la part d'IP Office, Client Avaya Workplace envoie une requête DNS pour l'adresse IP du FQDN qui lui est attribué dans la liste **SIP_CONTROLLER_LIST** du fichier `46xxsettings.txt`.
   - Pour les extensions distantes, les valeurs utilisées dans le fichier `46xxsettings.txt` généré automatiquement sont définies par les paramètres **Système** > **LAN1** > **Topologie réseau** > **SBC** dans la configuration d'IP Office.
3. Le client tente ensuite de s'enregistrer en tant qu'extension SIP en utilisant l'adresse IP renvoyée par le serveur DNS. Pour une extension distante, il s'agit de l'adresse IP publique du client pour son pare-feu réseau ou son ASBCE.

Liens connexes

Prise en charge d'Client Avaya Workplace en tant qu'extension distante à la page 66

Vérification des paramètres distants

À l'aide d'un PC distant, vous pouvez voir et vérifier les paramètres donnés aux extensions distantes.

Procédure

1. Utilisez **nslookup** pour vérifier que le DNS résout le FQDN pour IP Office aux adresses IP correctes.

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

2. À l'aide d'un navigateur, demandez le fichier `46xxsettings.txt` à IP Office. Par exemple, saisissez `ipo.example.com/46xxsettings.txt`.
3. Vérifiez la plage de ports indiquée. Client Avaya Workplace peut utiliser des ports RTP/RTCP dans la plage `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. Les autres paramètres affichent les valeurs utilisées par Client Avaya Workplace pour se connecter aux services 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. Pour les contacts et les services de présence, vérifiez si les valeurs `IPO_PRESENCE_ENABLED` et `IPO_CONTACTS_ENABLED` sont définies sur `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
```

Liens connexes

Prise en charge d'Client Avaya Workplace en tant qu'extension distante à la page 66

Chapitre 7 : Vérification de l'état de l'extension distante dans l'ASBCE

L'ASBCE fournit un ensemble de menus qui affichent l'état des connexions et des tentatives de création de connexions.

Liens connexes

Affichage des statistiques SIP de l'ASBCE à la page 69
Affichage des statistiques des utilisateurs de l'ASBCE à la page 70
Affichage des incidents de l'ASBCE à la page 71

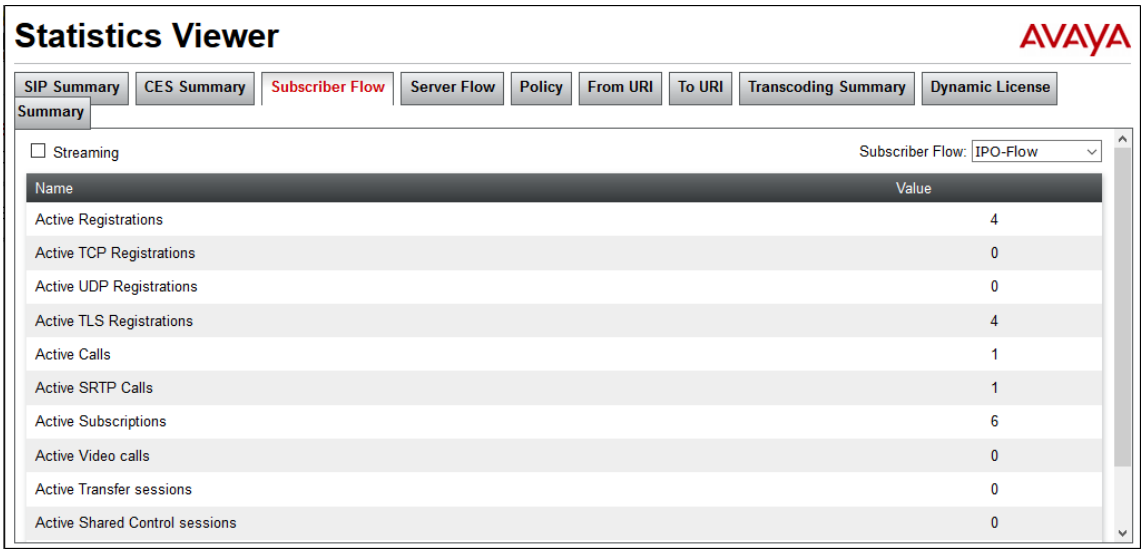
Affichage des statistiques SIP de l'ASBCE

La **Visionneuse de statistiques** peut afficher des détails sur le nombre de connexions et d'appels d'extensions distantes.

Procédure

1. Sélectionnez **État** > **Statistiques SIP**
2. Sélectionnez **Flux d'abonnés** et dans la liste déroulante , sélectionnez le flux créé pour les extensions distantes.

3. La visionneuse affiche des détails tels que le nombre d'enregistrements, le nombre d'appels, etc.



Liens connexes

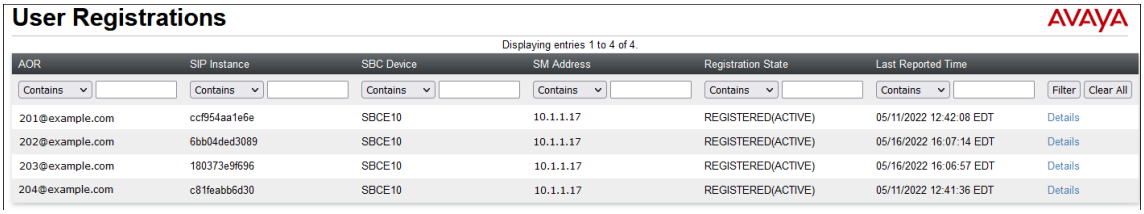
Vérification de l'état de l'extension distante dans l'ASBCE à la page 69

Affichage des statistiques des utilisateurs de l'ASBCE

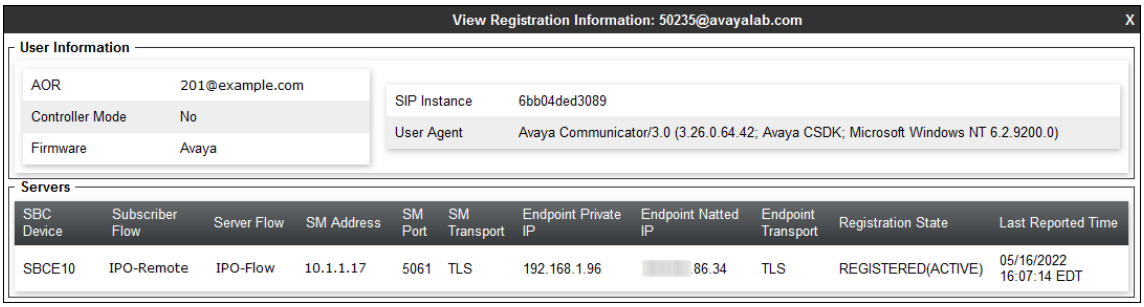
La **Visionneuse de statistiques** peut afficher les détails des extensions distantes individuelles.

Procédure

1. Sélectionnez **État** > **Détails**
2. La visionneuse affiche les détails des clients SIP enregistrés via l'ASBCE.



3. Pour afficher des informations supplémentaires sur un utilisateur particulier, cliquez sur **Inscription des utilisateurs**.



Liens connexes

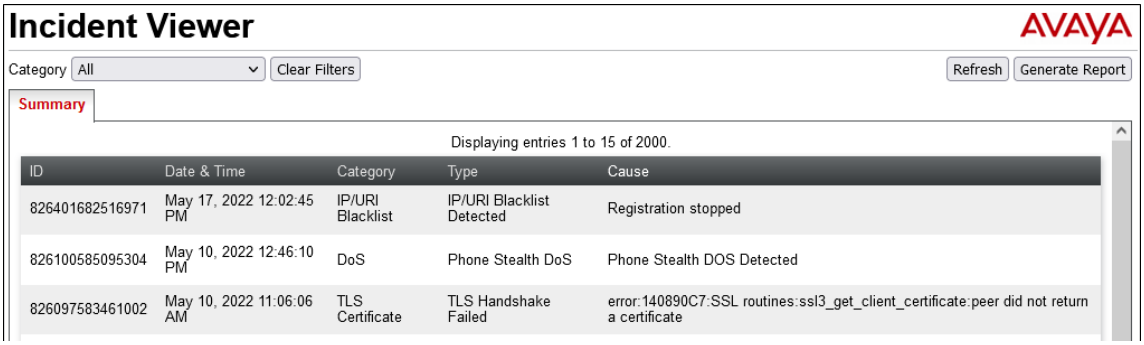
Vérification de l'état de l'extension distante dans l'ASBCE à la page 69

Affichage des incidents de l'ASBCE

L'ASBCE peut afficher des détails sur des incidents tels que des erreurs de certificat et des problèmes d'enregistrement. Si des extensions distantes rencontrent des problèmes lors de la connexion à IP Office, cela peut indiquer la raison si le problème se produit sur l'ASBCE.

Procédure

1. Sélectionnez **Incidents**.
2. La visionneuse affiche les détails des incidents.



Liens connexes

Vérification de l'état de l'extension distante dans l'ASBCE à la page 69

Partie 2 : Prise en charge d'IPv6

Chapitre 8 : Prise en charge des extensions distantes IPv6

Pour IP Office 11.1.3.1 et supérieur, IP Office prend en charge les extensions distantes Client Avaya Workplace sur iOS et Android en utilisant l'IPv6.

Liens connexes

Prise en charge des extensions distantes IPv6

Pour IP Office R11.1.3.1 et supérieur, un Client Avaya Workplace mobile distant peut utiliser l'IPv6.

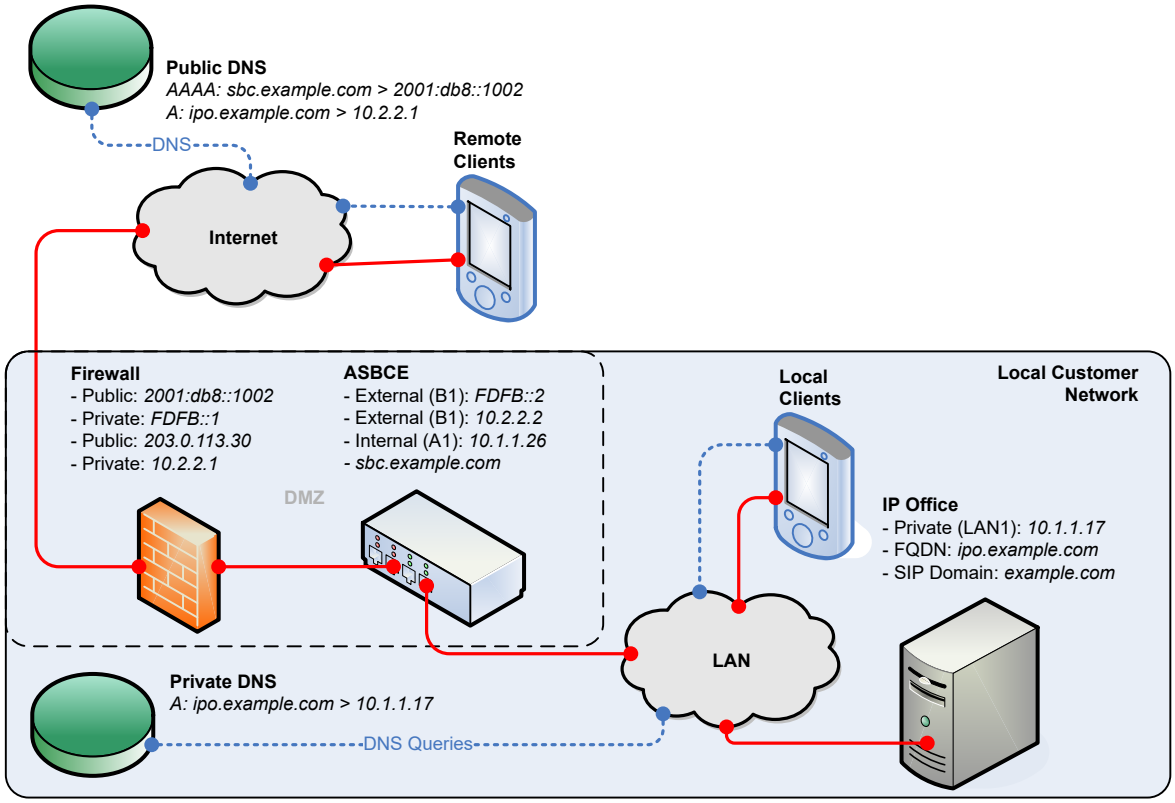
- Vous pouvez configurer IP Office pour qu'il fournisse à l'Client Avaya Workplace mobile distant le FQDN de l'ASBCE dans le fichier `46xxsettings.txt` généré automatiquement.
- La connexion nécessite un ASBCE R10.1.2 installé dans une installation à deux piles. L'ASBCE effectue le routage entre les clients IPv6 et l'IP Office IPv4 .
- Client Avaya Workplace:
  - iOS : Client Avaya Workplace R3.35 et supérieur.
  - Android : Client Avaya Workplace R3.35.1 et supérieur.
  - Les appareils iPad et Vantage ne sont pas inclus dans la prise en charge de l'IPv6.
- Les téléphones SIP et les clients sur le réseau privé du client utilisent toujours IPv4 pour se connecter directement à IP Office.
- Si le réseau auquel Client Avaya Workplace est connecté prend en charge l'IPv4 et l'IPv6, Client Avaya Workplace utilise par défaut l'IPv4.

Liens connexes

Prise en charge des extensions distantes IPv6 à la page 73

Schéma d'extensions distantes IPv6

Le schéma suivant est un exemple de prise en charge des extensions distantes IPv6.



- IP Office fournit aux extensions distantes le FQDN de l'ASBCE.
- Le DNS public résout le FQDN de l'ASBCE à l'adresse IPv6 publique du pare-feu du client.
- Le pare-feu transfère les ports utilisés par les extensions distantes vers l'interface externe de l'ASBCE.
- L'ASBCE à double pile gère le routage entre les adresses IPv6 et IPv4.
- Pour les extensions internes, le DNS privé résout le FQDN d'IP Office à l'adresse IPv4 du système IP Office.

Liens connexes

Prise en charge des extensions distantes IPv6 à la page 73

Limites des extensions distantes IPv6

- Bien qu'un micrologiciel existe pour le fonctionnement en IPv6 des téléphones de la série J100, ils doivent utiliser l'IPv4 pour la connexion d'extension distante à IP Office.

- Avaya Spaces ne prend pas en charge IPv6. Par conséquent, un Client Avaya Workplace utilisant IPv6 ne prend pas en charge les fonctions fournies par Avaya Spaces. Par exemple :
  - Aucun enregistrement client à l'aide de l'e-mail ou de la connexion SSO.
  - Pas de messagerie instantanée si IP Office est configuré pour utiliser Avaya Spaces comme serveur de messagerie.
- Si le réseau auquel Client Avaya Workplace est connecté prend en charge l'IPv4 et l'IPv6, Client Avaya Workplace utilise par défaut l'IPv4.

Liens connexes

Prise en charge des extensions distantes IPv6 à la page 73

Configuration DNS pour la prise en charge des extensions distantes IPv6

Pour prendre en charge l'IPv6, le DNS doit résoudre le FQDN de l'ASBCE en plus du FQDN d'IP Office :

- Le DNS public pour le FQDN d'IP Office doit toujours résoudre à une adresse IPv4.
- Le DNS public doit également résoudre le FQDN de l'ASBCE à une adresse IPv6. Pour ce faire, le client doit ajouter des enregistrements `AAAA` à son service DNS public.
- Les extensions locales continuent de se connecter directement à IP Office en utilisant des adresses IPv4. Ces adresses sont résolues par le DNS privé du client.

Liens connexes

Prise en charge des extensions distantes IPv6 à la page 73

Configuration des certificat pour la prise en charge des extrensions distantes IPv6

Lorsque vous prenez en charge les extensions distantes IPv6, en plus des adresses FQDN et IPv4 d'IP Office, le certificat d'identité de l'ASBCE doit inclure les adresses FQDN et IPv6 d'ASBCE.

- Le FQDN de l'ASBCE peut être ajouté comme partie du nom commun du certificat (CN) ou du nom alternatif de l'objet (SAN).
- L'adresse IPv6 doit être ajoutée au SAN.

Liens connexes

Prise en charge des extensions distantes IPv6 à la page 73

Configuration d'Avaya Spaces pour la prise en charge des extensions distantes IPv6

Avaya Spaces ne prend pas en charge IPv6. Par conséquent, un Client Avaya Workplace utilisant IPv6 ne prend pas en charge les fonctions fournies par Avaya Spaces. Par exemple :

- Aucun enregistrement client à l'aide de l'e-mail ou de la connexion SSO.
- Pas de messagerie instantanée si IP Office est configuré pour utiliser Avaya Spaces comme serveur de messagerie.

Page de connexion vierge

Si vous ne désactivez pas la prise en charge SSO, les utilisateurs de clients IPv6 voient une page blanche lorsqu'ils se connectent. Pour se connecter, ils doivent fermer la page vierge, puis se connecter directement à l'aide de l'adresse du fichier `46xxsettings.txt` d'IP Office.

- Si vous souhaitez que les utilisateurs du client IPv4 puissent toujours utiliser le SSO, vous devez demander aux utilisateurs d'extension distante IPv6 de fermer la page vierge et de se connecter à l'aide de l'adresse du fichier`46xxsettings.txt` d'IP Office.
- Sinon, pour empêcher le lancement de la page vierge lorsque l'utilisateur démarre Client Avaya Workplace, vous devez ajouter un fichier `46xxspecials.txt` avec le paramètre `SET SIPSSO 0` à IP Office. Remarque : cela affectera tous les utilisateurs d'Client Avaya Workplace.

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

Liens connexes

Prise en charge des extensions distantes IPv6 à la page 73

Liste de vérification de configuration pour les extensions distantes IPv6

Si vous ne prenez en charge que les extensions distantes IPv6, suivez la même procédure de configuration que pour IPv4, mais remplacez les adresses IPv4 externes par des adresses IPv6, le cas échéant. Voir la section Configuration de l'ASBCE pour les extensions SIP distantes à la page 25.

#	Action	Lien/Remarques	✔
1.	Configurer la prise en charge du DNS public pour l'IPv6	Le DNS doit résoudre le FQDN de l'ASBCE à l'adresse IPv6 pour le trafic vers l'ASBCE. Voir la section Configuration DNS pour la prise en charge des extensions distantes IPv6 à la page 75.	
2.	Inclure le FQDN de l'ASBCE et l'adresse IPv6 dans le certificat d'identité de l'ASBCE.	Voir la section Configuration des certificat pour la prise en charge des extrensions distantes IPv6 à la page 75.	

Le tableau continue …

#	Action	Lien/Remarques	✔
3.	Désactiver la prise en charge d'Avaya Spaces.	Voir la section Configuration d'Avaya Spaces pour la prise en charge des extensions distantes IPv6 à la page 76.	
4.	Définir l'adresse IPv6 publique dans IP Office	Vous devez donner aux extensions distantes l'adresse IPv6 à utiliser pour l'enregistrement SIP et les appels. Voir la section Définition des détails de l'ASBCE transmis aux extensions distantes par IP Office à la page 13.	
5.	Configurer le flux d'appels de l'ASBCE	Suivez le même processus de configuration de l'ASBCE que celui utilisé pour l'IPv4, mais en utilisant les adresses IPv6, le cas échéant. Voir la section Liste de contrôle de la configuration de l'ASBCE à la page 28.	

Liens connexes

Prise en charge des extensions distantes IPv6 à la page 73

Liste de vérification de configuration pour les extensions distantes IPv4 et IPv6 combinées

Cette liste de vérification suppose que vous avez terminé la configuration de l'ASBCE pour prendre en charge les extensions distantes IPv4. Voir la section Liste de contrôle de la configuration de l'ASBCE à la page 28. Les notes indiquent où l'ASBCE requiert une configuration supplémentaire pour prendre en charge les extensions distantes IPv4 et IPv6.

#	Action	Lien/Remarques	✔
1.	Configurer la prise en charge du DNS public pour l'IPv6	Le DNS doit résoudre le FQDN de l'ASBCE à l'adresse IPv6 pour le trafic vers l'ASBCE. Voir la section Configuration DNS pour la prise en charge des extensions distantes IPv6 à la page 75.	
2.	Inclure le FQDN de l'ASBCE et l'adresse IPv6 dans le certificat d'identité de l'ASBCE.	L'identité de l'ASBCE doit inclure les adresses FQDN et IPv4 d'IP Office, ainsi que les adresses FQDN et IPv6 de l'ASBCE. Voir la section Configuration d'Avaya Spaces pour la prise en charge des extensions distantes IPv6 à la page 76.	
3.	Désactiver la prise en charge d'Avaya Spaces.	Avaya Spaces n'est pas pris en charge avec l'IPv6. Voir la section Configuration d'Avaya Spaces pour la prise en charge des extensions distantes IPv6 à la page 76.	

Le tableau continue …

#	Action	Lien/Remarques	✔
4.	Définir l'adresse IPv6 publique dans IP Office	Vous devez donner aux extensions distantes l'adresse IPv6 à utiliser pour l'enregistrement SIP et les appels. Voir la section Définition des détails de l'ASBCE transmis aux extensions distantes par IP Office à la page 13.	
5.	Configurer le transfert du port du pare-feu	Ajoutez une nouvelle entrée, comme l'entrée IPv4, mais en utilisant les adresses IPv6, le cas échéant. Voir la section Configuration du pare-feu à la page 30.	
6.	Configurer l'interface réseau ASBCE externe	Ajoutez une nouvelle entrée pour l'interface externe mais en utilisant les adresses IPv6. Voir la section Configurer l'interface ASBCE externe à la page 31.	
7.	Configurer l'interface réseau ASBCE interne	Utilisez l'entrée IPv4 existante. Voir la section Configurer l'interface ASBCE interne à la page 32.	
8.	Créer un profil de client TLS	Utilisez l'entrée IPv4 existante. Voir la section Création d'un profil de client TLS à la page 34.	
9.	Créer un profil de serveur TLS	Utilisez l'entrée IPv4 existante. Voir la section Création d'un profil de serveur TLS à la page 35.	
10.	Créer une interface média SIP interne	Utilisez l'entrée IPv4 existante. Voir la section Création d'une interface média interne à la page 37.	
11.	Créer une interface média SIP externe	Ajoutez une nouvelle entrée, comme l'entrée IPv4, mais en utilisant les adresses IPv6, le cas échéant. Voir la section Création d'une interface média externe à la page 38.	
12.	Créer une interface de signalisation d'appel SIP interne	Utilisez l'entrée IPv4 existante. Voir la section Création d'une interface de signalisation interne à la page 39.	
13.	Créer une interface de signalisation d'appel SIP externe	Ajoutez une nouvelle entrée, comme l'entrée IPv4, mais en utilisant les adresses IPv6, le cas échéant. Voir la section Création d'une interface de signalisation externe à la page 40.	
14.	Créer un profil de serveur	Utilisez l'entrée IPv4 existante. Voir la section Création d'un profil de serveur ASBCE pour IP Office à la page 41.	

Le tableau continue …

#	Action	Lien/Remarques	✔
15.	Créer un routage de serveur	Utilisez l'entrée IPv4 existante. Voir la section Création d'un profil de routage de serveur à la page 43.	
16.	Configurer le masquage de topologie	Utilisez l'entrée IPv4 existante. Voir la section Création d'une politique de masquage de la topologie de l'ASBCE à la page 44.	
17.	Créer une liste de blocage IP/URL.	Utilisez l'entrée IPv4 existante. Voir la section Création d'une liste de blocage IP/URI à la page 45.	
18.	Créer une règle d'application	Utilisez l'entrée IPv4 existante. Voir la section Création d'une règle d'application à la page 46.	
19.	Créer une règle de média	Utilisez l'entrée IPv4 existante. • Assurez-vous que l'option **Options avancées** > **ANAT activé** n'est pas sélectionnée. Voir la section Création d'une règle de média à la page 48.	
20.	Créer une politique de point d'extrémité	Utilisez l'entrée IPv4 existante. Voir la section Création d'un groupe de politique de point d'extrémité à la page 50.	
21.	Ajouter un profil d'agents utilisateurs	Utilisez l'entrée IPv4 existante. Voir la section Configuration d'un profil d'agents utilisateurs à la page 51.	
22.	Créer un flux d'abonnés	Ajoutez une nouvelle entrée, comme l'entrée IPv4 : • Configurez les interfaces de média et de signalisation pour utiliser les interfaces IPv6 externes. Voir la section Création du flux d'abonnés à la page 52.	
23.	Créer un flux de serveur	Ajoutez une nouvelle entrée, comme l'entrée IPv4 : • Définissez l'interface de signalisation externe IPv6 comme **Interface reçue**. Voir la section Création d'un flux de serveur à la page 55.	
24.	Ajouter un proxy inverse pour Client Avaya Workplace	Ajoutez de nouveaux proxy à l'aide de l'interface B1 externe configurée pour les adresses IPv6. Voir la section Ajout de proxy inverses pour les demandes de fichiers à la page 57.	

Liens connexes

Prise en charge des extensions distantes IPv6 à la page 73

Partie 3 : Résilience

Chapitre 9 : Résilience ASBCE et IP Office

IP Office prend en charge une gamme d'options de résilience, y compris la résilience pour les téléphones SIP et les applications de téléphone logiciel SIP. Pour plus d'informations, reportez-vous au manuel Présentation de la résilience IP Office.

Cette section de ce document donne un aperçu de la configuration supplémentaire requise pour ajouter la prise en charge de la résilience à une configuration existante. Les principales étapes supplémentaires sont les suivantes :

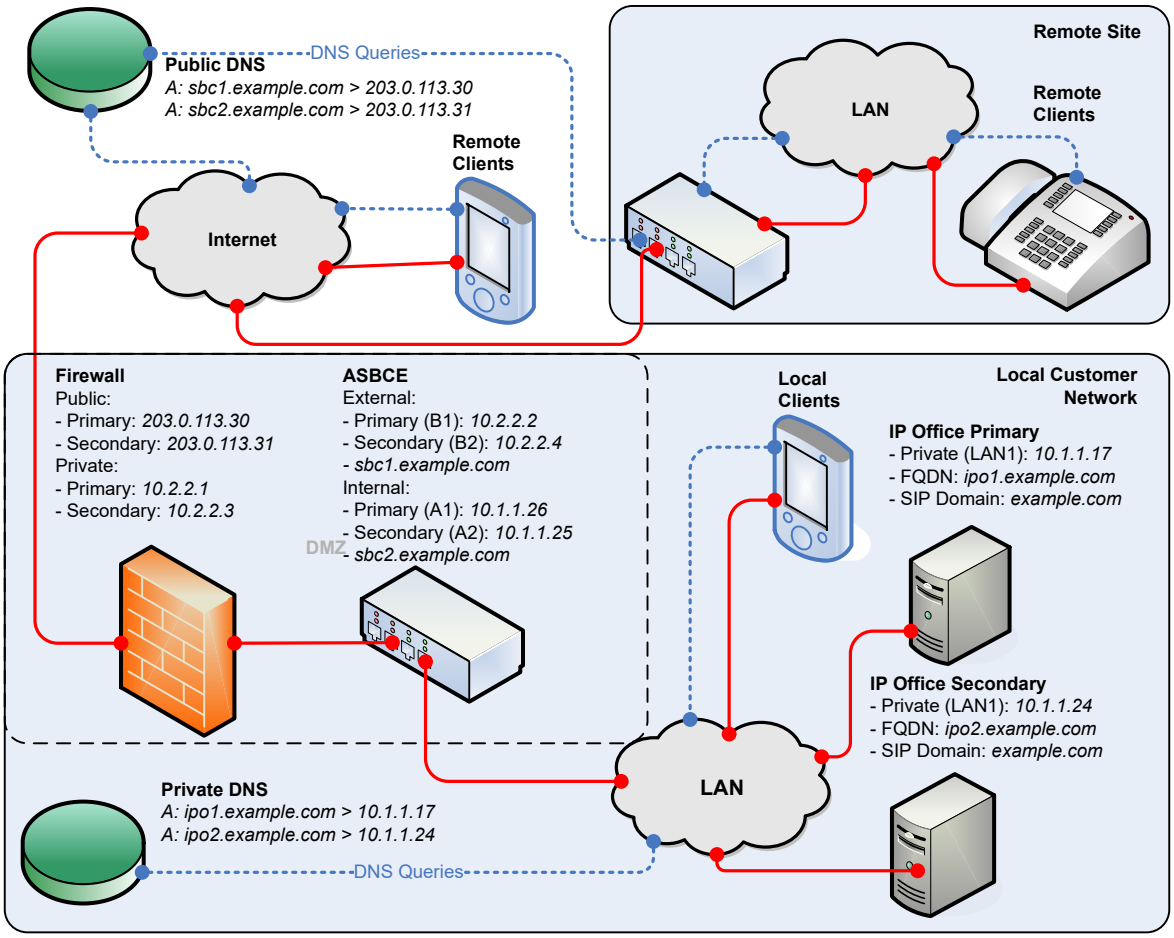
- IP Office ne peut pas utiliser l'adresse IP de l'extension distante pour correspondre à un emplacement dans la configuration d'IP Office. Par conséquent, pour utiliser les paramètres d'emplacement dans la résilience, vous devez configurer l'emplacement dans la configuration de l'extension.

Liens connexes

Exemple de schéma de résilience à la page 81
Génération d'un certificat d'identité pour l'IP Office secondaire à la page 82
Installation du certificat d'identité de l'IP Office secondaire à la page 83
Configuration d'IP Office pour la résilience des extensions distantes à la page 84
Configuration d'Avaya one-X Portal à la page 84
Configuration de l'ASBCE pour la résilience à la page 85
Configuration du DNS pour la résilience à la page 85

Exemple de schéma de résilience

Voici un exemple de schéma pour une configuration résiliente.



Pour une prise en charge résiliente des extensions distants, l'ASBCE utilise 2 jeux d'adresses IP publiques/privées :

- L'ASBCE route un jeu vers le serveur IP Office principal et l'autre vers le serveur IP Office secondaire.
- Cette logique est la même quelle que soit l'installation de l'ASBCE : Simplex, HA, deux serveurs ASBCE distincts ou double pile.

Liens connexes

[Résilience ASBCE et IP Office](#) à la page 81

Génération d'un certificat d'identité pour l'IP Office secondaire

L'IP Office secondaire nécessite un certificat d'identité émis par l'IP Office principal.

Procédure

1. Connectez-vous aux menus Web Control d'IP Office en procédant de l'une des manières suivantes :
   - À partir d'IP Office Web Manager, sélectionnez le serveur principal. Cliquez sur ☰ et sélectionnez **Affichage de la plateforme**.
   - Accédez à `https://<IP Office IP address>:7071` et connectez-vous.
2. Accédez à l'onglet **Paramètres** et faites défiler l'écran jusqu'à **Certificats**.
3. Entrez les données suivantes :

Valeur	Description
Adresse IP de l'ordinateur	Saisissez l'adresse IP du serveur secondaire.
Mot de passe	Saisissez un mot de passe pour chiffrer le certificat et la clé.
Nom de l'objet	Saisissez le FQDN de l'IP Office secondaire.
Autre nom(s) de l'objet	Indiquez le FQDN de l'IP Office secondaire, le domaine XMPP secondaire, le domaine SIP et les adresses IP IP Office internes et externes secondaires.

4. Cliquez sur **Régénérer** et **Appliquer** .
5. Dans la fenêtre contextuelle, cliquez sur le lien pour télécharger le certificat.
6. Cliquez sur **OK**.
7. Renommez le fichier téléchargé en `IPOSEC_ID.p12`.

Étapes suivantes

- Installation du certificat d'identité de l'IP Office secondaire à la page 83.

Liens connexes

Résilience ASBCE et IP Office à la page 81

Installation du certificat d'identité de l'IP Office secondaire

Vous devez ajouter le certificat d'identité créé pour l'IP Office secondaire.

Préambules

- Génération d'un certificat d'identité pour l'IP Office secondaire à la page 82.

Procédure

1. Connectez-vous au système à l'aide d'IP Office Web Manager.
   - Pour un IP500 V2, saisissez l'adresse du système, suivie de `:8443/WebMgmtEE/WebManagerment.html`.
   - Pour un serveur basé sur Linux, saisissez l'adresse système, suivie de `:7070/WebManagement/WebManagement.html`.
2. Accédez à **Security Manager** > **Certificats**.

3. Cliquez sur l'icône en regard du serveur secondaire.
4. Cliquez sur **Définir** .
5. Recherchez et sélectionnez le fichier de certificat d'identité.
6. Saisissez le mot de passe.
7. Cliquez sur **Charger**.

Liens connexes

Résilience ASBCE et IP Office à la page 81

Configuration d'IP Office pour la résilience des extensions distantes

En plus de la configuration standard pour la résilience (voir Présentation de la résilience IP Office), vous devez configurer l'IP Office secondaire comme suit :

- Définissez les paramètres du registrar SIP, à l'exception du **FQDN du Registrar SIP**, sur les mêmes paramètres que ceux utilisés sur le serveur IP Office principal. Cela inclut la correspondance du **Nom de domaine SIP**. Voir la section Configuration VoIP SIP d'IP Office à la page 11.
- Définissez le **FQDN du Registrar SIP** pour qu'il corresponde au FQDN configuré dans le DNS pour acheminer le trafic SIP vers le serveur IP Office secondaire.
- Définissez les paramètres **SBC** sur ceux que les extensions distantes doivent utiliser pour se connecter à l'ASBCE configuré pour acheminer les appels SIP vers l'ASBCE secondaire. Voir la section Définition des détails de l'ASBCE transmis aux extensions distantes par IP Office à la page 13.

Liens connexes

Résilience ASBCE et IP Office à la page 81

Configuration d'Avaya one-X Portal

Vous devez configurer le service Avaya one-X Portal avec le nom de domaine de l'IP Office secondaire .

Procédure

1. Connectez-vous aux menus de l'administrateur d'Avaya one-X Portal, de l'une des manières suivantes :
   - Dans IP Office Manager, sélectionnez **Applications** > **One-X Portal** > .
   - Accédez à `https://<portal IP address>:9443/onexportal-admin.html` et connectez-vous en tant qu'administrateur.

2. Sélectionnez **Configuration** > **Nom de domaine de l'hôte**.
    a. Définissez le **Nom de domaine de l'hôte secondaire** sur le FQDN de l'Avaya one-X Portal secondaire.
    b. Cliquez sur **Enregistrer**.
3. Cliquez sur l'icône en haut des menus pour redémarrer Avaya one-X Portal.

Liens connexes

Résilience ASBCE et IP Office à la page 81

Configuration de l'ASBCE pour la résilience

Les étapes de configuration de l'ASBCE sont similaires à celles de la configuration d'un serveur unique. Il est nécessaire de créer des entrées supplémentaires, mais en utilisant les adresses IP publiques et privées du serveur IP Office secondaire.

Liens connexes

Résilience ASBCE et IP Office à la page 81

Configuration du DNS pour la résilience

La configuration du serveur DNS est similaire à celle d'un serveur IP Office unique. Le DNS requiert les enregistrements supplémentaires du FQDN des serveurs IP Office et ASBCE secondaires.

Liens connexes

Résilience ASBCE et IP Office à la page 81

Chapitre 10 : Vérification de la configuration de résilience

Vous pouvez utiliser les méthodes suivantes pour vérifier les informations de résilience fournies par IP Office aux extensions distantes.

Liens connexes

[Vérification du routage DNS de résilience](#) à la page 86
[Affichage du suivi ASBCE](#) à la page 87
[Vérification des réponses Avaya one-X Portal](#) à la page 88

Vérification du routage DNS de résilience

À l'aide d'un PC distant, vous pouvez vérifier que le DNS résout correctement les requêtes.

Procédure

1. Utilisez la commande `nslookup` pour vérifier que le DNS résout les FQDN de l'IP Office principal et de l'IP Office secondaire aux adresses IP correctes. Par exemple :

```
C:\nslookup
Default Server:  UnKnown
Address:  192.168.0.1

> ipo.example.com
Server:  UnKnown
Address: 203.0.113.30

> iposec.example.com
Server:  UnKnown
Address: 203.0.113.31
```

2. Utilisez la commande `nslookup` pour vérifier que le DNS résout les FQDN des ASBCE principal et du secondaire.

```
C:\nslookup
Default Server:  UnKnown
Address:  192.168.0.1

> sbc1.example.com
Server:  UnKnown
Address: 203.0.113.30

> sbc2.example.com
Server:  UnKnown
Address: 203.0.113.31
```

Liens connexes

Vérification de la configuration de résilience à la page 86

Affichage du suivi ASBCE

Voici un exemple de session traceSBC pour l'enregistrement d'un client. Il montre la réponse SIP *200 OK* envoyée au client.

La réponse contient un certain nombre de paramètres de configuration. Pour les extensions distantes, la réponse inclura le FQDN SBC que vous avez configuré sur l'IP Office secondaire.

```
                                    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";
```

- **En fonctionnement normal :**

  La réponse *200 OK* affiche les valeurs *onex_server* et *backup_ipoffice_server* définies avec les serveurs principal et secondaire respectivement.

- **Pendant la résilience :**

  onex_server contient le FQDN du portail secondaire et *backup_ipoffice_server* est *0.0.0.0*.

Liens connexes

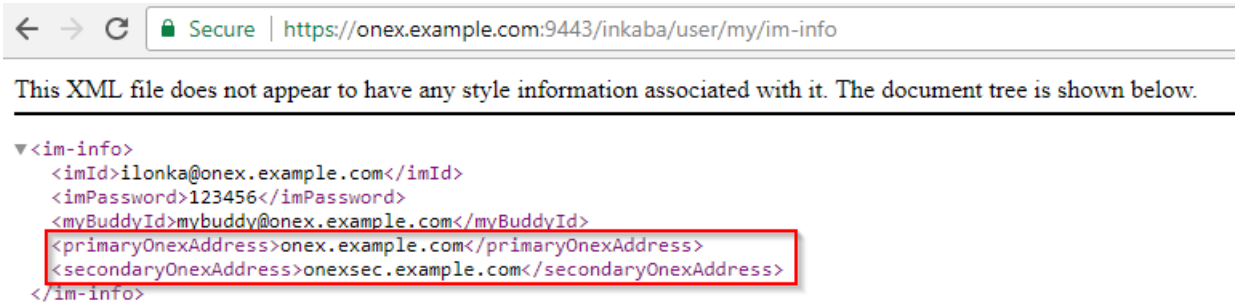
Vérification de la configuration de résilience à la page 86

Vérification des réponses Avaya one-X Portal

Lorsqu'un client demande des informations XMPP au service Avaya one-X Portal principal, la réponse inclut les adresses du serveur XMPP principal et secondaire.

Procédure

1. En mode de fonctionnement normal, à l'aide d'un navigateur, saisissez `https://<FQDN>:9443/inkaba/user/my/im-info` où *<FQDN>* est le FQDN du service Avaya one-X Portal principal.



2. Vérifiez que la réponse inclut les FQDN des services Avaya one-X Portal principal et secondaire.
   a.
   b. La réponse doit inclure le FQDN du serveur IP Office principal.

3. À l'aide d'un navigateur, saisissez `https://<FQDN>:9443/inkaba/user/my/sip-info` où *<FQDN>* est le FQDN du service Avaya one-X Portal principal.

4. Si vous répétez les étapes pendant la résilience, utilisez le FQDN du serveur Avaya one-X Portal secondaire.
   - Les informations `im-info` seront les mêmes.
   - Les informations `sip-info` indiqueront le FQDN du serveur IP Office secondaire.

Liens connexes

Vérification de la configuration de résilience à la page 86

Partie 4 : Informations complémentaires

Chapitre 11 : Aide et documentation supplémentaires

Les pages suivantes fournissent des sources d'aide supplémentaire.

Liens connexes

Manuels et guides de l'utilisateur supplémentaires à la page 91
Obtenir de l'aide à la page 91
Recherche d'un partenaire commercial Avaya à la page 92
Ressources IP Office complémentaires à la page 92
Formation à la page 93

Manuels et guides de l'utilisateur supplémentaires

Le site Web de l'Centre de documentation Avaya contient des guides de l'utilisateur et des manuels pour les produits Avaya, dont IP Office.

- Pour obtenir la liste des manuels et guides de l'utilisateur actuels d'IP Office, consultez le document Manuels et guides d'utilisation d'Avaya IP Office™ Platform.
- Les sites Web de l'Base de connaissances Avaya IP Office et de l'Support Avaya permettent également d'accéder aux guides de l'utilisateur et aux manuels techniques d'IP Office.
  - Notez que, dans la mesure du possible, ces sites redirigent les utilisateurs vers la version du document hébergée par l'Centre de documentation Avaya.

Pour d'autres types de documents et d'autres ressources, consultez les différents sites Web d'Avaya (voir la section Ressources IP Office complémentaires à la page 92).

Liens connexes

Aide et documentation supplémentaires à la page 91

Obtenir de l'aide

Avaya vend IP Office par le biais de partenaires commerciaux accrédités. Ces partenaires commerciaux fournissent une assistance directe à leurs clients et peuvent faire remonter les problèmes à Avaya si nécessaire.

Si votre système IP Office ne dispose pas actuellement d'un partenaire commercial Avaya assurant l'assistance et la maintenance, vous pouvez utiliser l'outil Avaya Partner Locator

pour trouver un partenaire commercial. Voir Recherche d'un partenaire commercial Avaya à la page 92.

Liens connexes

Aide et documentation supplémentaires à la page 91

Recherche d'un partenaire commercial Avaya

Si votre système IP Office ne dispose pas actuellement d'un partenaire commercial Avaya assurant l'assistance et la maintenance, vous pouvez utiliser l'outil Avaya Partner Locator pour trouver un partenaire commercial.

Procédure

1. Au moyen d'un navigateur, accédez à l'Site Web Avaya à l'adresse https://www.avaya.com.
2. Sélectionnez **Partenaires**, puis **Rechercher un partenaire**.
3. Saisissez vos informations d'emplacement.
4. Pour les partenaires commerciaux IP Office, à l'aide du **Filtre**, sélectionnez **Petites et moyennes entreprises**.

Liens connexes

Aide et documentation supplémentaires à la page 91

Ressources IP Office complémentaires

En plus du site Web de la documentation (voir la section Manuels et guides de l'utilisateur supplémentaires à la page 91), il existe une série de sites Web qui fournissent des informations sur les produits et les services Avaya, notamment IP Office.

- Site Web Avaya (https://www.avaya.com)

  Il s'agit du site Web officiel d'Avaya. La page principale permet également d'accéder aux sites web Avaya individuels pour des régions et pays différents.

- **Portail des ventes et partenaires Avaya** *(https://sales.avaya.com)*

  Il s'agit du site Web officiel pour tous les partenaires commerciaux d'Avaya. Le site requière l'enregistrement d'un nom d'utilisateur et d'un mot de passe. Une fois que vous y avez accédé, vous pouvez personnaliser le portail pour afficher des produits spécifiques et le type d'informations que vous souhaitez voir.

- **Base de connaissances Avaya IP Office** *(https://ipofficekb.avaya.com)*

  Ce site donne accès à une version en ligne, régulièrement mise à jour, du manuel technique et des guides de l'utilisateur IP Office.

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

Ce site permet aux installateurs et aux responsables de la maintenance des produits Avaya d'accéder aux logiciels, à la documentation et aux autres services de ces produits Avaya.

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

  Ce site propose des forums pour discuter des problèmes liés aux produits.

- **Groupe d'utilisateurs internationaux Avaya** *(*https://www.iuag.org*)*

  Il s'agit de l'organisation pour les clients Avaya. Elle propose des groupes de discussion et des forums.

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

  Ce site fournit des détails sur les API et les SDK pour les produits Avaya, notamment IP Office. Le site fournit également des notes d'application pour les produits tiers non-Avaya qui interagissent avec IP Office en utilisant ces API et SDK.

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

  Ce site donne accès à des cours de formation et à des programmes d'accréditation pour les produits Avaya.

Liens connexes

Aide et documentation supplémentaires à la page 91

Formation

La formation et les accréditations Avaya garantissent que nos partenaires commerciaux disposent des capacités et des compétences requises pour vendre, mettre en œuvre et appuyer les solutions Avaya et dépasser les attentes des clients avec succès. Les accréditations suivantes sont disponibles :

- Spécialiste de ventes certifié d'Avaya (APSS)
- Spécialiste professionnel de mise en œuvre d'Avaya (AIPS)
- Spécialiste d'assistance technique certifié d'Avaya (ACSS)

Les cartes d'identifiants sont disponibles sur le site Internet Formation Avaya.

Liens connexes

Aide et documentation supplémentaires à la page 91

Chapitre 12 : Glossaire

Vous trouverez ci-dessous les définitions des termes utilisés dans ce document.

Liens connexes

Enregistrement A

« Enregistrement d'adresse ». Un enregistrement DNS de base qui mappe un nom de domaine ou un FQDN à une adresse IPv4. Pour les adresses IPv6, le DNS utilise des enregistrements `AAAA`.

Liens connexes

Glossaire à la page 94

Enregistrement AAAA

Également appelé « Enregistrement Quad-A ». Les services DNS utilisent des enregistrements `AAAA` pour mapper un nom de domaine ou un FQDN à une adresse IPv6. Il s'agit des enregistrements `A` utilisés pour les adresses IPv4.

Liens connexes

Glossaire à la page 94

ASBCE

« Avaya Session Border Controller for Enterprise ». La plateforme Avaya permettant de fournir des services SBC pour un réseau de client.

Liens connexes

Glossaire à la page 94

DNS

« Serveur de noms de domaine ». Un serveur ou service qui fournit des informations sur l'adresse IP en réponse à une requête de nom de domaine ou de FQDN. Par exemple, lorsqu'une application tente de se connecter à l'adresse `www.example.com`, elle contacte d'abord le serveur DNS sur son réseau. Le serveur DNS résout l'adresse textuelle `www.example.com` à l'adresse IP numérique requise. Le processus implique que le serveur DNS vérifie les enregistrements DNS qu'il détient et, si nécessaire, ceux détenus par d'autres serveurs DNS du réseau ou sur Internet.

Liens connexes

Glossaire à la page 94

Nom de domaine

L'adresse textuelle utilisée pour identifier un réseau d'appareils. Un serveur DNS convertit le nom de domaine et les noms de domaine complets en adresses IP spécifiques.

Liens connexes

Glossaire à la page 94

FQDN

« Nom de domaine complet ». L'adresse textuelle complète attribuée à un serveur, service ou client spécifique au sein d'un domaine.

Liens connexes

Glossaire à la page 94

IP de gestion

L'adresse IP utilisée pour l'accès administrateur au serveur ASBCE. Il s'agit d'une adresse différente de celle utilisée pour les interfaces de trafic réseau internes et externes fournies par l'ASBCE.

Liens connexes

Glossaire à la page 94

SBC

« Session Border Controller ». Un SBC est un périphérique qui contrôle la signalisation et les médias d'appel SIP entre deux réseaux.

Liens connexes

Glossaire à la page 94

DNS fractionné

L'utilisation de FQDN et de serveurs DNS pour acheminer le trafic à l'intérieur et entre les réseaux simplifie la maintenance du réseau. Cependant, des problèmes peuvent survenir lorsque vous utilisez le routage FQDN pour le trafic réseau interne et externe. Cela peut amener le réseau à acheminer le trafic interne vers des services internes de manière externe. Cela expose les services et des adresses internes qui doivent rester masqués.

Le DNS fractionné utilise un service DNS public pour le trafic externe vers le réseau du client et un service DNS privé pour le trafic interne au sein du réseau du client.

Les clients peuvent configurer le DNS fractionné à l'aide d'un seul serveur DNS à la périphérie du réseau du client ou de serveurs DNS publics et privés distincts.

Liens connexes

Glossaire à la page 94

Enregistrement SRV

« Enregistrement de service ». Pour les domaines prenant en charge plusieurs services, par exemple `www.example.com` ou `sip.example.com`, les enregistrements DNS `A` peuvent ne pas être suffisants pour le routage requis. Les enregistrements DNS `SRV` fournissent un mappage pour des services spécifiques fonctionnant au sein d'un domaine.

Liens connexes

Glossaire à la page 94

XMPP

« Protocole extensible de messagerie et de présence ». XMPP est un protocole de normes ouvertes qui permet aux appareils d'échanger des informations de messagerie instantanée, de présence et de contacts.

Liens connexes

Glossaire à la page 94

Index

O

P

Q

R

S

T

U

V

W