Deploying Avaya IP Office™ Platform SSL VPN Services

Issue 7
April 2023

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 Inc. 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.

Avis de limite de responsabilité en matière de documentation

Le terme « Documentation » désigne l'ensemble des informations publiées sur divers supports, notamment les informations relatives aux produits, les instructions d'utilisation et les spécifications techniques de performance mis généralement à la disposition des utilisateurs des produits. Le terme documentation n'inclut pas les documents 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 celles-ci sont effectuées par l'utilisateur final.

Avis de limite de 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 les documents fournis 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 Web en question.

Garantie

Avaya offre une garantie limitée sur le matériel et les logiciels Avaya. Consultez votre contrat de vente pour en connaître les termes. Vous trouverez 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 support technique d'Avaya à l'adresse suivante : https://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010 sous la rubrique « Warranty & Product Lifecycle », 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 DE LA LICENCE DU LOGICIEL DISPONIBLES SUR LE SITE INTERNET D'AVAYA (HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO) EN SUIVANT LE LIEN « CONDITIONS DE LA LICENCE DU LOGICIEL AVAYA (produits Avaya) » OU SUR LE SITE SUCCESSEUR DÉSIGNÉ PAR AVAYA, S'APPLIQUENT À QUICONQUE TÉLÉCHARGE, UTILISE ET/OU INSTALLE LE LOGICIEL AVAYA, ACQUIS AUPRÈS D'AVAYA INC., À TOUTE FILIALE D'AVAYA OU À TOUT PARTENAIRE DE DISTRIBUTION AVAYA (LE CAS ÉCHÉANT) SOUS CONTRAT COMMERCIAL AVEC AVAYA OU UN PARTENAIRE DE DISTRIBUTION AVAYA. SAUF STIPULATION CONTRAIRE ET SOUS RÉSERVE DE L'ACCORD ÉCRIT D'AVAYA, AVAYA NE PROPOSE PAS CETTE LICENCE SI LE LOGICIEL A ÉTÉ OBTENU AILLEURS QUE CHEZ AVAYA, UN AFFILIÉ AVAYA OU UN PARTENAIRE DE DISTRIBUTION AVAYA ; AVAYA SE RÉSERVE LE DROIT DE POURSUIVRE EN JUSTICE TOUTE PERSONNE UTILISANT OU VENDANT CE LOGICIEL SANS LICENCE. EN INSTALLANT, TÉLÉCHARGEANT OU UTILISANT LE LOGICIEL, OU EN AUTORISANT D'AUTRES PERSONNES À LE FAIRE, VOUS ACCEPTEZ, EN VOTRE PROPRE NOM ET AU NOM DE L'ENTITÉ POUR LAQUELLE VOUS INSTALLEZ, TÉLÉCHARGEZ OU UTILISEZ LE LOGICIEL (CI-APRÈS APPELÉE DE MANIÈRE INTERCHANGEABLE « VOUS » ET « UTILISATEUR FINAL »), CES CONDITIONS GÉNÉRALES ET D'ÊTRE LIÉ PAR CONTRAT AVEC AVAYA INC. OU L'AFFILIÉ D'AVAYA APPLICABLE (AVAYA). OU TOUTE AUTRE SOCIÉTÉ AFFILIÉE D'AVAYA CONCERNÉE (« AVAYA »).

Avaya vous accorde une licence d'exploitation couvrant les types de licence décrits ci-dessous, à l'exception des Logiciels Heritage Nortel, pour lequel le champ d'application de la licence est détaillé ci-dessous. Lorsque le type de licence n'est pas expressément indiqué dans le document de commande, la licence applicable se rapporte à la Licence Système Désigné, conformément aux termes de la Section Licence Systèmes désignés (SD) ci-dessous, selon le cas. Le nombre de licences et d'unités de capacité pour lesquelles la licence est accordée est de un (1), sauf si un nombre différent de licences ou d'unités de capacité est spécifié dans la documentation ou d'autres textes mis à votre disposition. Le terme « Logiciel » se rapporte aux programmes informatiques en code exécutable fournis par Avaya ou par un de ses partenaires de distribution, qu'il s'agisse de produits indépendants ou déjà installés sur du matériel ou de toute mise à niveau, mise à jour, correction de bogue ou version modifiée. « Processeur Désigné » désigne un unique ordinateur autonome. « Serveur » désigne un ensemble de Processeurs désignés hébergeant (de façon physique ou virtuelle) une application logicielle accessible par plusieurs utilisateurs. Le terme « Instance » désigne un exemplaire unique du Logiciel en cours d'exécution à un moment particulier : (i) sur une machine physique ; ou sur une machine virtuelle logicielle (« VM ») ou déploiement similaire.

Type(s) de licence

Licence de système(s) désigné(s) (DS). L'Utilisateur final peut installer et utiliser chaque copie ou une Instance du Logiciel uniquement : 1) sur un certain nombre de Processeurs désignés, dans la limite indiquée dans la commande ; ou 2) dans la limite du nombre d'Instances du Logiciel indiqué dans la commande ou la Documentation, ou conformément à l'autorisation écrite d'Avaya. Avaya peut exiger que le(s) Processeur(s) désigné(s) soit(soient) identifié(s) dans la commande par le type, le numéro de série, le code de caractéristique, l'Instance, l'emplacement ou toute autre désignation spécifique, ou fourni(s) par l'Utilisateur final à Avaya par des moyens électroniques mis en place par Avaya spécifiquement à cette fin.

Licence utilisateur simultané (CU). L'Utilisateur final peut installer et utiliser le Logiciel sur plusieurs Processeurs désignés ou un ou plusieurs Serveurs, à condition que seul le nombre d'Unités sous licence accède au Logiciel et l'utilise à tout moment, comme indiqué dans la commande, la Documentation ou l'autorisation écrite d'Avaya. Une « Unité » représente l'unité sur laquelle Avaya, à son entière discrétion, base la tarification de ses licences et peut être, entre autres, un agent, un port, un utilisateur, un compte de messagerie électronique ou vocale associé à un nom de personne ou à une fonction de l'entreprise (par ex., webmaster ou centre d'assistance) ou encore une entrée du répertoire dans la base de données d'administration utilisée par le Logiciel et autorisant un utilisateur à accéder à l'interface du Logiciel. Les Unités peuvent être associées à un Serveur identifié spécifique ou à une Instance du Logiciel.

Licence en Cluster (LC). L'Utilisateur final peut installer et utiliser chaque copie ou une Instance du Logiciel uniquement dans la limite du nombre de Clusters indiqué dans la commande, la Documentation ou l'autorisation écrite d'Avaya avec une valeur par défaut d'un (1) Cluster si cela n'est pas spécifié.

Licence Enterprise (EN). L'Utilisateur final peut installer et utiliser chaque copie ou une Instance du Logiciel uniquement dans le cadre d'une utilisation à l'échelle de l'entreprise d'un nombre illimité d'Instances du Logiciel, tel qu'indiqué dans la commande, la Documentation ou l'autorisation écrite d'Avaya.

Licence Utilisateur nommé (UN). L'Utilisateur final peut : (i) installer et utiliser chaque copie ou Instance du Logiciel sur un seul Processeur désigné ou un seul Serveur par Utilisateur nommé autorisé (tel que défini ci-après) ; ou (ii) installer et utiliser chaque copie ou Instance du Logiciel sur un Serveur dans la mesure où seuls les Utilisateurs nommés autorisés accèdent au Logiciel et l'utilisent tel qu'indiqué dans la commande, la Documentation ou l'autorisation écrite d'Avaya. Un « Utilisateur nommé » est un utilisateur ou un dispositif qui a été expressément autorisé par Avaya à accéder au Logiciel et à l'utiliser. Un « Utilisateur nommé » peut être, à la seule discrétion d'Avaya et sans limitation, désigné par son nom, sa fonction dans l'entreprise (par ex., webmaster ou centre d'assistance), un compte de messagerie électronique ou vocale au nom d'une personne ou d'une fonction de l'entreprise, ou d'une entrée de répertoire dans la base de données d'administration utilisée par le Logiciel et autorisant un utilisateur à accéder à l'interface du Logiciel.

Licence Shrinkwrap. L'Utilisateur final peut installer et utiliser le Logiciel en vertu des conditions générales des contrats de licence applicables, tels qu'une licence « shrinkwrap » (acceptée par rupture de l'emballage) ou « clickthrough » (acceptée par lecture du contrat avant téléchargement) accompagnant le Logiciel ou applicable à celui-ci (« Licence Shrinkwrap ») tel qu'indiqué dans la commande, la Documentation ou l'autorisation écrite d'Avaya.

Licence de transaction (TR) L'Utilisateur final peut utiliser le Logiciel dans la limite du nombre de Transactions spécifié pour une période de temps limitée et tel qu'indiqué dans la commande, la Documentation ou l'autorisation écrite d'Avaya. Une « Transaction » désigne l'unité par laquelle Avaya, à sa seule discrétion, base la tarification de ses licences. Elle peut, sans limitation, être mesurée en fonction de l'utilisation, de l'accès, des interactions (entre client/serveur ou client/entreprise) ou du fonctionnement du Logiciel dans une période de temps spécifiée (par ex., par heure, par jour, par mois). Certains exemples de Transactions incluent, sans y être limités, chaque message d'accueil/d'attente diffusé, chaque promotion personnalisée (sur n'importe quel canal), chaque opération de rappel, chaque agent en direct ou session de chat Web, chaque appel routé ou redirigé (sur n'importe quel canal). L'Utilisateur final ne peut pas dépasser le nombre de Transactions sans le consentement préalable d'Avaya et le paiement de frais supplémentaires.

Logiciels Heritage Nortel

La mention « Logiciels Heritage Nortel » signifie que le logiciel a été acheté par Avaya dans le cadre du rachat de Nortel Enterprise Solutions Business au mois de décembre 2009. Les Logiciels Nortel hérités sont ceux présents dans la liste des Produits Nortel hérités que vous trouverez à l'adresse https://support.avaya.com/LicenseInfo à l'aide du lien « Produits Nortel hérités » ou sur un site successeur désigné par Avaya. Pour les Logiciels Heritage Nortel, Avaya accorde au Client une licence d'utilisation des Logiciels Heritage Nortel fournis ci-dessous, uniquement pour le niveau d'activation ou d'utilisation autorisé, uniquement aux fins spécifiées dans la Documentation, et uniquement intégrés à, pour exécution sur ou pour communication avec les équipements Avaya. Les frais concernant les logiciels Heritage Nortel peuvent porter sur une extension d'activation ou d'utilisation autorisée telle que spécifiée dans un bon de commande ou un devis.

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 licence 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, télécharger, 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 et/ou l'utilisation non autorisés de cette documentation 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

Le terme « Composants tiers » signifie que certains logiciels ou certaines parties des logiciels inclus dans le Logiciel ou le Service hébergé peuvent contenir des composants logiciels (y compris des composants open source) distribués dans le cadre de contrats avec des tiers (« Composants tiers ») faisant l'objet de conditions quant aux droits d'utilisation de certaines parties du logiciel (« Conditions tierces »). Les informations portant sur le code source du SE Linux (pour les Produits ayant distribué le code source du SE Linux) et identifiant les titulaires de copyright des Composants tiers et les Termes tiers en vigueur sont disponibles dans les produits, dans la Documentation ou sur le site Web d'Avaya à l'adresse : https://support.avaya.com/Copyright ou tout site successeur désigné par Avaya. Les conditions de licence des logiciels libres fournies dans le cadre des Conditions Tierces sont cohérentes avec les droits de licence concédés dans ces Conditions de Licence de Logiciel, et peuvent vous accorder des droits supplémentaires tels que la modification et la distribution des logiciels libres. Les Conditions Tierces prévaudront sur les Conditions de Licence de Logiciel, uniquement en ce qui concerne les Composants Tiers applicables, si ces Conditions de Licence de Logiciel imposent des restrictions plus importantes que celles des Conditions Tierces applicables.

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

CELA S'APPLIQUE À L'HÉBERGEMENT DES PRODUITS OU SERVICES AVAYA PAR LES PARTENAIRES DE DISTRIBUTION D'AVAYA. LE PRODUIT OU SERVICE HÉBERGÉ PEUT UTILISER DES ÉLÉMENTS TIERS QUI SONT SUJETS À DES CONDITIONS DE TIERS ET QUI NÉCESSITENT

UN FOURNISSEUR DE SERVICES POUR OBTENIR LA LICENCE INDÉPENDAMMENT ET DIRECTEMENT AUPRÈS D'UN FOURNISSEUR TIERS. L'HÉBERGEMENT DES PRODUITS AVAYA PAR LES PARTENAIRES DE DISTRIBUTION D'AVAYA DOIT ÊTRE AUTORISÉ PAR ÉCRIT PAR AVAYA ET SI CES PRODUITS UTILISENT OU INCORPORENT CERTAINS LOGICIELS TIERS, Y COMPRIS, SANS S'Y LIMITER, LES LOGICIELS OU CODECS MICROSOFT, LE PARTENAIRE DE DISTRIBUTION D'AVAYA DOIT OBTENIR INDÉPENDAMMENT TOUT ACCORD DE LICENCE APPLICABLE, À SES FRAIS, DIRECTEMENT AUPRÈS DU FOURNISSEUR TIERS APPLICABLE.

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, 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 nécessitez une assistance technique ou autre, contactez l'assistance d'intervention en cas de fraude à la tarification au 1-800-643-2353 (États-Unis et Canada). Pour obtenir d'autres numéros de téléphone d'assistance, reportez-vous au site Web de support technique d'Avaya : https://support.avaya.com, ou au site successeur désigné par 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 de commerce

Les marques de commerce, les logos et les marques de service (« Marques ») figurant sur ce site, sur toute documentation, 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 Inc.

Toutes les autres marques commerciales 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.

Contents

Chapitre 1 : Modifications du document depuis la dernière version

Les modifications suivantes ont été apportées à ce document pour IP Office version 9.1.

Kit de développement logiciel (SDK)

Pour faciliter la configuration associée de SSL VPN, deux SDK sont proposés. Ils sont décrits dans la section Configuration de SSL VPN à l'aide d'un SDK à la page 53.

Assistant d'installation rapide AVG

L'assistant d'installation rapide AVG a été mis à jour. Voir Annexe A : Exemple d'assistant d'installation rapide AVG à la page 94.

Chapitre 2 : À propos du service SSL VPN

La solution d'accès à distance SSL VPN IP Office est un moyen facile et rapide de configurer un accès à distance sécurisé à haut débit. Cette solution est conçue pour fournir à Avaya et à ses partenaires un accès à distance fiable qui améliore la transmission de services tout en réduisant le coût relatif à la transmission de services sur site. Elle permet aux partenaires de toute taille de créer une infrastructure qui automatise la gestion et la maintenance des systèmes IP Office.

Services fournis par SSL VPN

Le service SSL VPN établit un véritable tunnel sécurisé entre le matériel Avaya IP Office installé sur le site client et un Avaya VPN Gateway (AVG) distant. Le personnel de support s'appuient sur ce tunnel sécurisé pour offrir aux clients des services de gestion à distance, tels que la gestion d'erreurs, la surveillance et l'administration. Il permet aux administrateurs de :

- transférer le trafic via le service SSL VPN par le biais de routes statiques et de tunnels distincts ;
- surveiller IP Office à distance sur le service SSL VPN connecté à un serveur AVG à l'aide de System Status Application (SSA) ou de SysMonitor ;
- gérer les systèmes IP Office à distance à l'aide d'Avaya IP Office Manager ou IP Office Manager for Server Edition ;
- recevoir des interruptions SNMP, des entrées syslog et des alarmes SMTP par courrier électronique de IP Office sur le service SSL VPN connecté à un serveur AVG ;
- activer et désactiver le tunnel à l'aide de Manager ou de IP Office Manager for Server Edition ;
- activer et désactiver le tunnel à l'aide de codes de fonction, d'un standard automatique ou d'une administration basée sur un poste téléphonique ;
- exécuter plusieurs instances de service SSL VPN simultanément.

Liens connexes

Options de déploiement à la page 10
Modes de fonctionnement à la page 10
Architecture du système à la page 13
Configuration système requise et restrictions à la page 16
Documentation associée à la page 17

Options de déploiement

Services d'assistance à distance Avaya

La solution SSL VPN fait partie intégrante de IP Office Support Services (IPOSS), ce qui permet à Avaya de proposer une assistance technique et un dépannage à distance de pointe. La fonction d'intégration automatisée simplifie grandement l'établissement de la connexion SSL VPN à Avaya. Le processus d'intégration comprend l'extraction de l'inventaire, l'enregistrement à GRT afin de créer l'enregistrement de base installée, ainsi que l'enregistrement technique pour la connectivité à distance à Avaya.

Pour de plus amples informations sur l'offre de maintenance IPOSS, consultez la page IP Office Support Services du portail des ventes Avaya.

Services d'assistance à distance fournis par les partenaires Avaya

Indépendamment de l'offre IPOSS, les partenaires peuvent utiliser le client SSL VPN en l'associant à la solution Avaya VPN Gateway (AVG) pour créer leur propre infrastructure SSL VPN. Ce document fournit des informations et décrit des procédures qui aideront les partenaires Avaya à établir leur propre solution SSL VPN pour un accès à distance, dans le cadre de leur programme de maintenance auprès de leurs clients.

La solution SSL VPN configurée par le partenaire est prise en charge par les systèmes IP Office Standard Edition et Server Edition.

Liens connexes

À propos du service SSL VPN à la page 9

Modes de fonctionnement

Modes de fonctionnement

Le service SSL VPN est pris en charge par le matériel IP500v2. Le module de contrôle IP500 n'est pas pris en charge.

Le service SSL VPN est pris en charge lorsque IP Office fonctionne dans l'un des modes suivants. Le mode Branch n'est pas pris en charge.

- IP Office Standard Edition (modes Essential, Advanced et Preferred)
- Server Edition
  - Server Edition primaire
  - Server Edition secondaire
- Système d'expansion Server Edition
  - Système d'expansion Server Edition(V2), un système d'expansion IP500v2
  - Système d'expansion Server Edition(L), un système d'expansion Linux
- Basic Edition

Remarque :

Basic Edition n'est pris en charge que pour les déploiements utilisant Avaya IP Office Support Services (IPOSS). Basic Edition n'est pas pris en charge avec un SSL VPN déployé pour les services d'assistance aux partenaires Avaya.

Fonctions prises en charge

La fonctionnalité disponible dépend du mode de fonctionnement utilisé. Cette section présente les fonctionnalités de SSL VPN et énumère les fonctions disponibles dans chaque mode.

Fonctions prises en charge	Mode de fonctionnement			
	Standard Edition	Server Edition	Système d'expansion Server Edition	Basic Edition
Connectivité				
Connexion SSL VPN continue au serveur AVG	✔	✔	✔	✔
Tunnels distincts	✔	✔	✔	✔
Routes statiques	✔	✔	✔	✔
Plusieurs instances de service SSL VPN exécutées simultanément	✔	✔	✔	✔
Accès au périphérique LAN (NAPT)	✔	✔	✔	—
Gestion des erreurs				
Génération d'interruptions SNMP	✔	✔	✔	✔
Génération d'entrées syslog	✔	✔	✔	—
Génération de notifications d'alarmes par courrier électronique	✔	✔	✔	—
Génération d'alarmes test	✔	✔	✔	✔
Surveillance et administration				
Gestion à distance à l'aide de Manager ou de IP Office Manager for Server Edition	✔	✔	✔	✔

Table continues…

Fonctions prises en charge	Mode de fonctionnement			
	Standard Edition	Server Edition	Système d'expansion Server Edition	Basic Edition
Surveillance à distance à l'aide de System Status Application	✔	✔	✔	✔
Surveillance à distance à l'aide de SysMonitor	✔	✔	✔	✔
Activation et désactivation du service SSL VPN par le biais de codes de fonction	✔	✔	✔	—
Activation et désactivation du service SSL VPN par le biais de menus basés sur un poste téléphonique	—	—	—	✔
Activation et désactivation du service SSL VPN par le biais de Manager ou IP Office Manager for Server Edition	✔	✔	✔	—
Activation et désactivation du service SSL VPN par le biais d'un standard automatique	✔	✔	✔	—
Activation et désactivation du service SSL VPN par le biais de touches programmables sur les téléphones Avaya	✔	✔	✔	✔
Mise à niveau à distance de l'application IP Office vers les nouvelles versions	✔	✔	✔	✔

Outils de surveillance et d'administration

Quand le service SSL VPN est connecté, vous pouvez gérer et surveiller le système IP Office à distance via le tunnel.

Les outils suivants sont conçus pour gérer, mettre à niveau et configurer à distance le système IP :

- IP Office Manager : application administrative qui permet de configurer les paramètres système des systèmes IP Office Essential Edition.
  - IP Office Manager for Server Edition : quand vous lancez IP Office Manager, vous pouvez choisir d'ouvrir une configuration à l'aide du mode IP Office Manager for Server Edition. Ce mode vous permet d'administrer les serveurs Server Edition et les systèmes d'expansion.
- IP Office Basic Edition – Web Manager : outil par navigateur qui permet de configurer les paramètres système du système IP Office.

Vous pouvez utiliser les outils suivants pour surveiller à distance le système IP Office :

- System Status Application(SSA) : l'application System Status Application est un outil de diagnostic qui permet de surveiller l'état des systèmes IP Office. SSA signale les événements historiques en temps réels ainsi que les données d'état et de configuration.
- SysMonitor : l'application SysMonitor affiche les informations relatives au fonctionnement du système IP Office. Elle permet de recueillir les informations dans des fichiers journaux en vue de les analyser.

Liens connexes

À propos du service SSL VPN à la page 9

Architecture du système

Le service SSL VPN établit un véritable tunnel sécurisé entre le matériel IP Office installé sur le site client et un système Avaya VPN Gateway (AVG) installé au niveau du site du fournisseur de services. Les informations de cette section permettent de comprendre l'architecture réseau utilisée par le service SSL VPN.

Cartes d'interface réseau

Avaya vous recommande de déployer le serveur AVG dans une configuration à deux branches avec deux cartes d'interface réseau. Une interface traite le trafic privé entre le service SSL VPN et l'intranet sécurisé. Cette connexion permet au service SSL VPN d'accéder aux ressources internes et vous permet de configurer et de gérer le système IP Office depuis un poste de gestion. La seconde interface traite le trafic vers et depuis Internet.

Routage

Au niveau du site du fournisseur de services, vous pouvez configurer un routage d'entreprise entre le AVG et son réseau privé. Au niveau du site client, vous pouvez placer chaque système IP Office du côté privé d'un routeur d'entreprise. Aucune modification de configuration du routeur d'entreprise n'est nécessaire pour faire fonctionner le service SSL VPN.

IP Officetransfère les données vers AVG via le service SSL VPN à l'aide de routes statiques ou de tunnels distincts. Pour envoyer le trafic via le tunnel SSL VPN, vous devez utiliser l'une des options suivantes :

- laisser IP Office installer de manière dynamique les tunnels distincts au moment de la connexion du service SSL VPN à AVG, et les supprimer à la déconnexion du service ;

- configurer une route statique dans IP Office Manager.

Tunnels distincts :

Lorsque vous installez et configurez AVG, vous pouvez ajouter des sous-réseaux distincts ou des adresses hôte à un groupe. Le système IP Office intègre les informations de routage du tunnel de manière dynamique quand le service SSL VPN établit une connexion avec AVG. Les routes de réseaux distinctes sont supprimées quand le service SSL VPN se déconnecte de AVG.

Pour plus d'informations sur les tunnels distincts dans AVG à l'aide de Net Direct, consultez le *guide Avaya VPN Gateway Administration Guide (Guide d'administration)* (NN46120-105) et le *guide Avaya VPN Gateway BBI Application Guide (Guide d'application BBI)* (NN46120-102). Pour plus d'informations sur la configuration de tunnels distincts à l'aide de l'interface de ligne de commande, consultez le *guide CLI Application Guide (Guide d'application CLI)* (NN46120-101).

Routes statiques :

Si vous n'utilisez pas des tunnels distincts, vous pouvez configurer une route statique directement sur le système IP Office. Lorsque vous configurez une route statique, le système détermine la destination du trafic transféré à partir des informations de la route IP configurée dans Manager. Vous devez définir le service SSL VPN en tant que destination.

Utilisez une route statique quand :

- les tunnels distincts ne sont pas proposés par le AVG et que vous devez envoyer le trafic via le tunnel ;
- le service SSL VPN n'est pas connecté à AVG et que vous souhaitez mettre en file d'attente le trafic devant être transféré via le tunnel une fois la connexion restaurée ; dans ce cas, IP Office met temporairement en file d'attente un petit nombre de paquets qui déclenche la connexion quand SSL VPN est en service mais qu'il est déconnecté.

Vous pouvez configurer plusieurs routes statiques sur le même système IP Office.

Authentification

Chaque système IP Office prend en charge plusieurs tunnels SSL VPN. Une adresse IP statique privée unique est attribuée à chaque instance de service SSL VPN. Lorsque vous connectez le service SSL VPN, AVG authentifie le système IP Office. Si les systèmes IP Office sont peu nombreux, vous pouvez utiliser la base de données locale Avaya VPN Gateway (AVG) pour créer les données utilisateur nécessaires à l'authentification. Pour les déploiements à plus grande échelle, il est recommandé d'utiliser un serveur RADIUS pour l'authentification.

Accès de l'agent du service

Les agents du service situés sur le site du fournisseur de services peuvent se connecter à n'importe quel système IP Office qui dispose d'une connexion SSL VPN à AVG en service. Ils peuvent surveiller et gérer le système IP Office à distance en contactant l'adresse IP du tunnel SSL VPN, et accéder aux adresses IP de plusieurs services SSL VPN simultanément.

AVG garantit que les tunnels SSL VPN ne communiquent pas entre eux. Vous n'avez pas besoin de configurer d'autres paramètres pour garantir l'indépendance et la sécurisation des tunnels.

Gestion des erreurs

Le serveur de gestion d'erreurs est un composant facultatif du service SSL VPN. Déployez un serveur de gestion d'erreurs sur le site du fournisseur de services et utilisez le service SSL VPN pour lui envoyer les erreurs système. Vous pouvez définir des filtres d'événements qui

déterminent les erreurs à signaler. Par exemple, vous pouvez définir des filtres pour signaler tout événement relatif au fonctionnement du système IP Office, et pour signaler également les erreurs propres au fonctionnement du service SSL VPN.

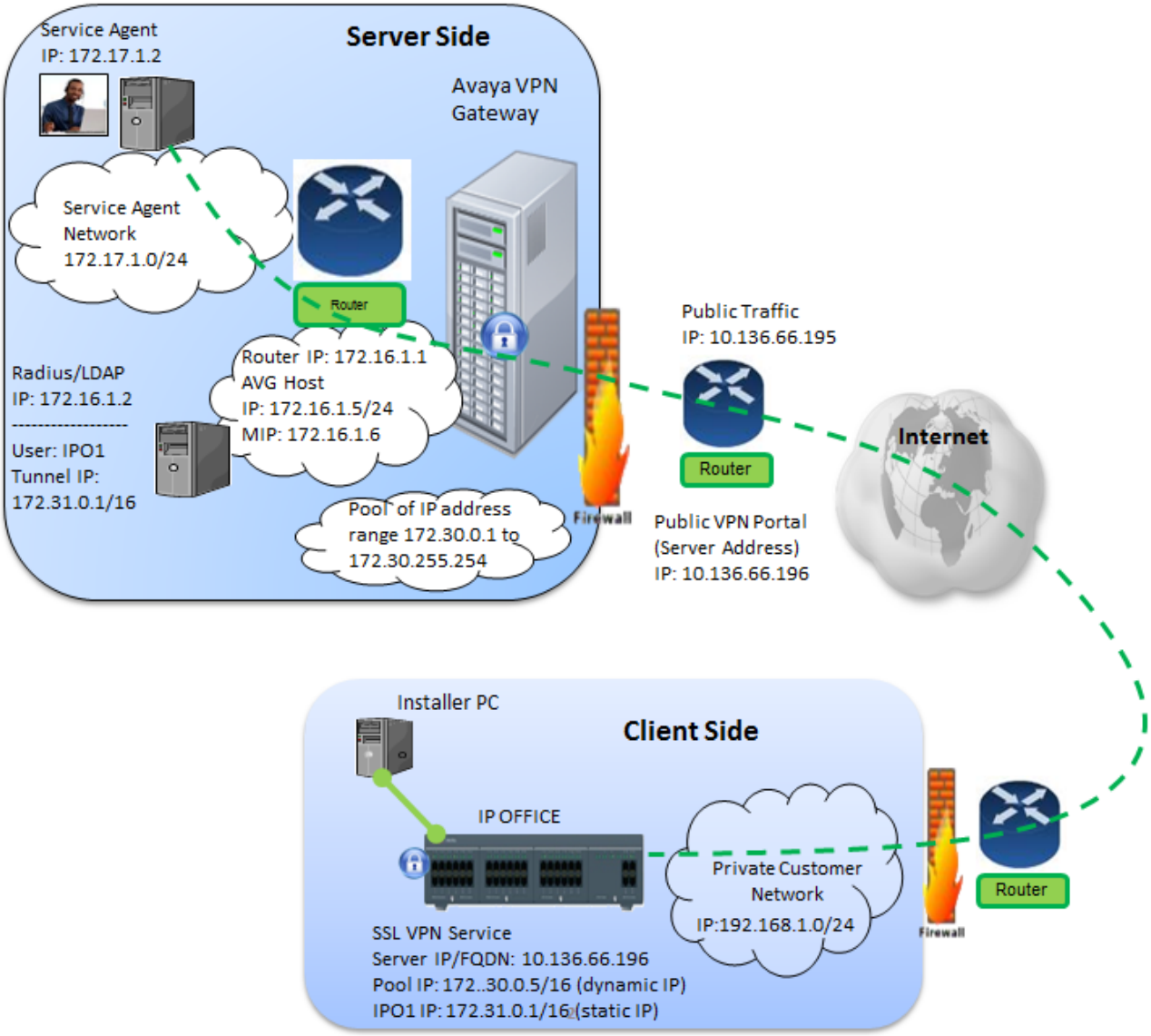
Avaya vous recommande de définir le nom de compte de services SSL VPN de manière à ce qu'il corresponde au nom d'ID de périphérique de l'agent SNMP. L'ID de périphérique de l'agent SNMP est configuré dans IP Office Manager, dans le formulaire **Système**, sous **Évènements système**, **Configuration**.

Traversée du pare-feu

Le service SSL VPN fonctionne en toute transparence à travers le pare-feu. Il n'est pas nécessaire de configurer votre routeur d'entreprise pour autoriser le service SSL VPN si vous l'avez déjà configuré pour le trafic HTTPS. Le service SSL VPN se sert du même port de destination pour le trafic TCP.

Exemple d'architecture

Le schéma suivant présente un exemple de l'architecture utilisée par le service SSL VPN.



Liens connexes

[À propos du service SSL VPN](#) à la page 9

Configuration système requise et restrictions

Configuration requise

Bande passante :

Assurez-vous que la bande passante de chargement est d'au moins 90 kbit/s (720 kbit/s) avec un temps de latence inférieur à 150 ms (parcours circulaire). Cette spécification est nécessaire pour qu'Avaya Global Services puisse fournir une prise en charge à distance via le service SSL VPN.

Authentification :

- Si les systèmes IP Office sont peu nombreux, vous pouvez utiliser la base de données locale Avaya VPN Gateway (AVG) pour créer les données utilisateur nécessaires à l'authentification.
- Pour les déploiements à grande échelle, un serveur RADIUS est requis. Avaya recommande d'utiliser Avaya Identity Engines Ignition Server en tant que serveur RADIUS.
- À la fin du tunnel SSL VPN, le système IP Office vérifie l'identité de AVG à partir de certificats numériques. Vous devez configurer des certificats dans AVG et installer les certificats X.509 requis dans le magasin de certificats IP Office.

Licence :

Le service SSL VPN ne requiert aucune clé de licence.

Restrictions

Small Community Networks :

Si vous déployez des systèmes IP Office dans un réseau SCN (Small Community Network), vous pouvez configurer un service SSL VPN entre des nœuds spécifiques du SCN et de AVG. Vous ne pouvez pas utiliser la connexion SSL VPN pour accéder à distance aux autres nœuds de la topologie SCN : le service SSL VPN communique uniquement avec le système IP Office qui correspond à son extrémité. Vous devez configurer un service SSL VPN pour chaque nœud dans le SCN auquel vous voulez accéder à distance.

Certificats :

Le magasin de certificats approuvés IP Office permet de stocker jusqu'à 25 certificats.

Version HTTP :

Si vous utilisez un navigateur avec une version HTTP postérieure à 1.1, il est possible que vous ne puissiez pas vous connecter à un périphérique LAN à l'aide de NAPT SSL VPN. Si vous rencontrez des problèmes lors de la connexion à un périphérique LAN, modifiez les paramètres de votre navigateur afin d'utiliser HTML version 1.1.

Liens connexes

À propos du service SSL VPN à la page 9

Documentation associée

Pour installer, configurer et administrer la solution SSL VPN, vous devez vous reporter à la documentation relative au système Avaya IP Office, à Avaya VPN Gateway (AVG) et à Avaya Identity Engines Ignition Server. De plus, vous devez consulter la documentation fournie par les autres fournisseurs pour le support du matériel et des logiciels utilisés dans votre infrastructure réseau.

Procurez-vous la documentation Avaya suivante pour le support de la solution SSL VPN.

Documentation Avaya VPN Gateway

- *Avaya VMware Getting Started Guide (Guide de mise en route Avaya VMware) - Avaya VPN Gateway* (NN46120-302)
- *Avaya VPN Gateway User Guide* (guide de l'utilisateur) (NN46120-104)
- *Avaya VPN Gateway Administration Guide (guide d'administration*) (NN46120-105)
- *Avaya VPN Gateway BBI Application Guide (guide d'application BBI)* (NN46120-102)
- *Avaya VPN Gateway CLI Application Guide (guide d'application CLI)* (NN46120-101)

Documentation Avaya IP Office

- *Avaya IP Office Basic Edition – Web Manager*
- *Avaya IP Office Manager*
- *Administration de Voicemail Pro*
- *Installation de Embedded Voicemail*

Documentation Avaya Identity Engines Ignition Server

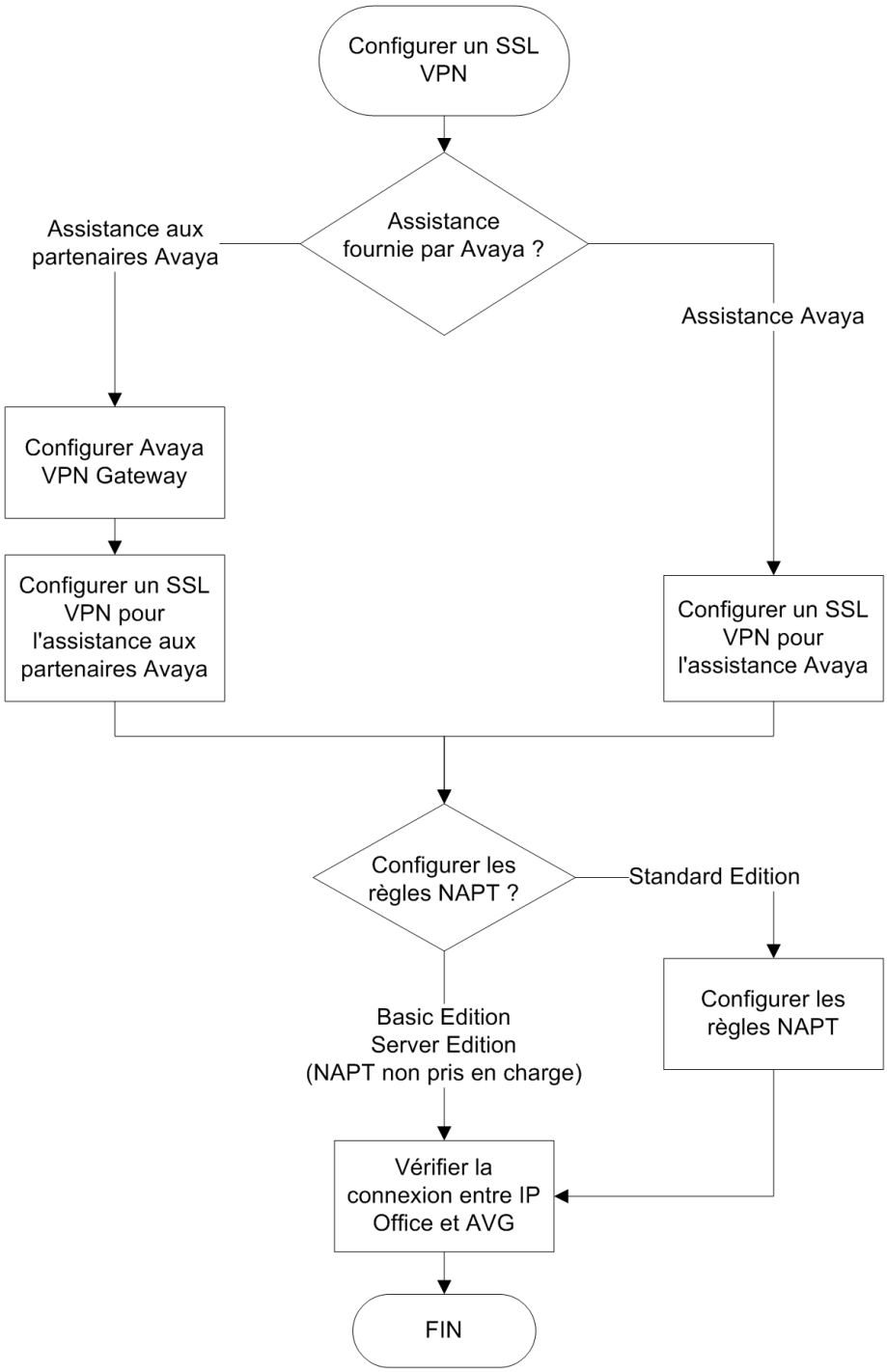
- *Avaya Identity Engines Ignition Server — Configuration Guide* (guide de configuration) (NN47280-500)

Liens connexes

À propos du service SSL VPN à la page 9

Chapitre 3 : Flux de travail de la configuration d'un SSL VPN

Le flux de travail de la page suivante indique la séquence de tâches à exécuter pour configurer un SSL VPN.



Navigation

- Configuration de à la page 22
- Configuration d'un SSL VPN pour l'assistance Avaya à la page 36
- Configuration d'un SSL VPN pour l'assistance aux partenaires Avaya à la page 39

- Règles NAPT à la page 60
- Vérification de la connexion entre et à la page 62

Chapitre 4 : Configuration d'Avaya VPN Gateway

Pour fournir les services d'assistance avec la solution SSL VPN, les partenaires Avaya doivent configurer Avaya VPN Gateway (AVG).

Cette section fournit des informations sur les tâches à effectuer pour installer et configurer un système AVG pour la prise en charge de la connexion SSL VPN pour un système IP Office.

Avant de configurer le système IP Office pour un service SSL VPN, vous devez configurer l'infrastructure à laquelle le service se connecte. Cette section traite de la configuration de l'interopération d'AVG avec un système IP Office. Pour exécuter ces tâches, vous devez consulter les différents documents relatifs à AVG, ainsi que la documentation fournie par les autres fournisseurs pour le support du matériel et des logiciels utilisés dans votre infrastructure réseau.

Les principales tâches requises pour le déploiement d'Avaya VPN Gateway sont décrites dans ce chapitre. Il ne s'agit cependant que de recommandations générales. Les détails exacts du déploiement peuvent varier en fonction de l'environnement du partenaire.

Liens connexes

Planification initiale et configuration

Environnement virtualisé

Le client SSL VPN nécessite qu'Avaya VPN Gateway (AVG) soit installé dans un environnement virtualisé comme serveur VPN Gateway. Les seuls environnements virtuels pris en charge sont les serveurs ESX et ESXi. Il existe trois modèles d'AVG : 3050–VM, 3070–VM et 3090–

VM. Pour connaître les spécifications matérielles de chaque modèle, consultez le document *VMware Getting Started Guide (Guide de mise en route VMware), Avaya VPN Gateway* (NN46120-302). Vous pouvez télécharger l'ensemble des documents relatifs à AVG depuis http://support.avaya.com.

D'autres informations sur les serveurs VMware ESXi sont disponibles à l'adresse http://www.vmware.com.

Configuration à deux branches

Installez Avaya VPN Gateway (AVG) dans une configuration à deux branches. Cela signifie que le serveur AVG doit être équipé de deux cartes d'interface réseau. Attribuez une adresse IP statique à chaque carte d'interface réseau.

- Une interface gère le trafic privé et sert d'interface de gestion.
- La deuxième interface gère l'accès Internet et les tunnels SSL VPN.

Logiciel AVG

Deux options permettent de déployer le logiciel AVG.

- Déploiement des dispositifs virtuels OVF AVG
- CD-ROM d'installation automatique

Pour obtenir des informations et connaître les procédures d'installation d'AVG, consultez le document *VMware Getting Started Guide (Guide de mise en route VMware), Avaya VPN Gateway* (NN46120-302).

PC de l'agent de service

Installez le PC de l'agent de service sur le réseau privé et définissez la passerelle par défaut sur l'adresse IP hôte d'Avaya VPN Gateway (AVG).

Sur le PC de l'agent de service

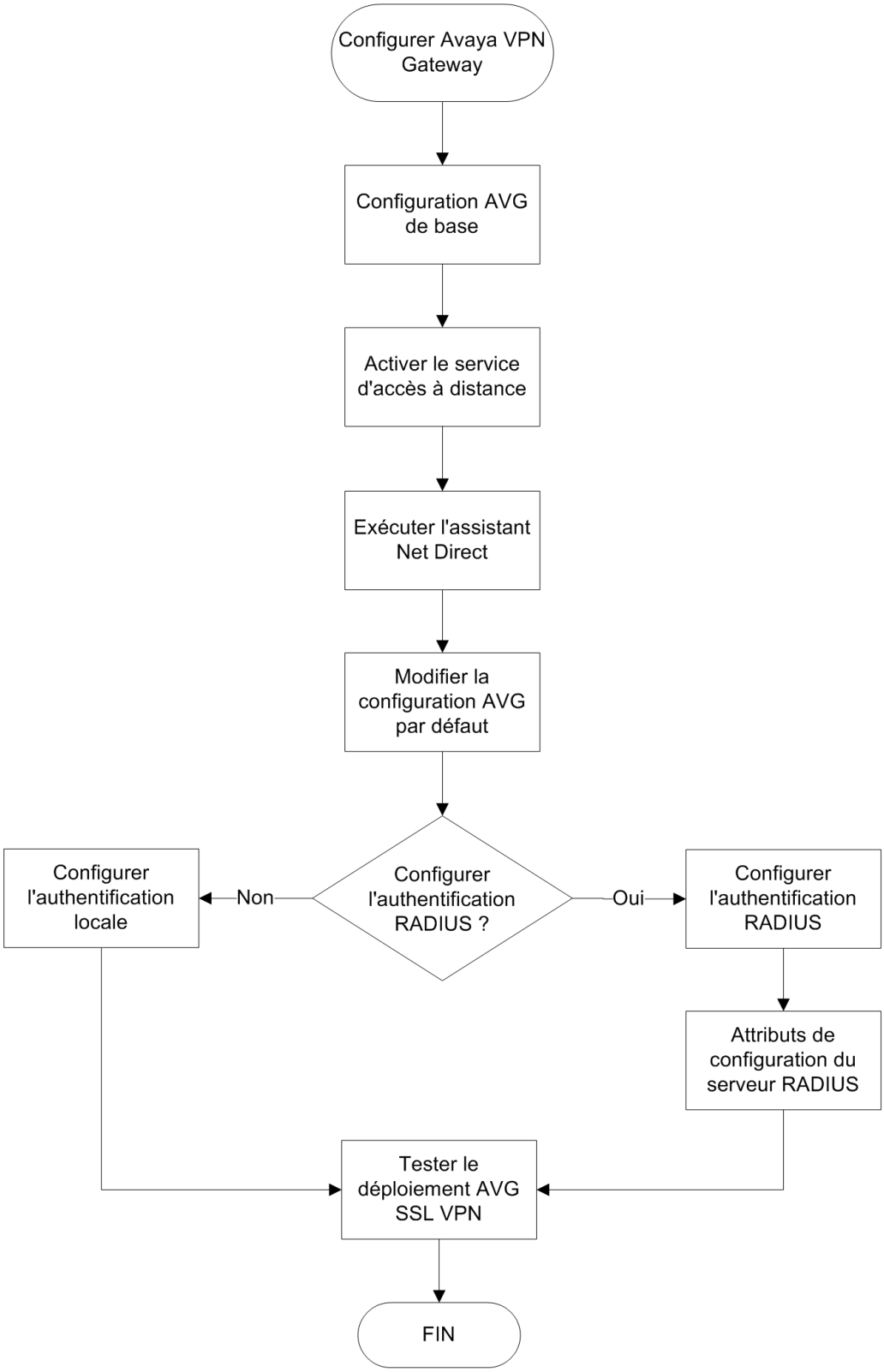
- L'adresse IP de l'interface de gestion (MIP) est utilisée pour démarrer une interface de gestion basée sur le navigateur (BBI) ou une interface de ligne de commande afin de configurer et de surveiller AVG.
- L'adresse IP du tunnel SSL VPN est utilisée pour gérer et surveiller à distance les systèmes IP Office.

Liens connexes

Configuration d'Avaya VPN Gateway à la page 22

Avaya VPN GatewayOrganigramme des tâches de la configuration

L'organigramme des tâches suivant indique la séquence de procédures à suivre pour configurer AVG.


Configurer Avaya VPN Gateway
Configuration AVG de base
Activer le service d'accès à distance
Exécuter l'assistant Net Direct
Modifier la configuration AVG par défaut
Configurer l'authentification RADIUS ?
Non
Configurer l'authentification locale
Oui
Configurer l'authentification RADIUS
Attributs de configuration du serveur RADIUS
Tester le déploiement AVG SSL VPN
FIN

Navigation

Liens connexes

Configuration d'Avaya VPN Gateway à la page 22

Configuration AVG de base

Configuration d'AVG sur le PC de l'agent de service

Lorsque vous démarrez VPN Gateway pour la première fois, le menu **Configuration** s'affiche. Ce menu contient la commande CLI **new**. Cet assistant de configuration initiale intuitif et basé sur l'interface CLI pour AVG propose des paramètres par défaut afin d'activer rapidement des connexions SSL depuis IP Office. Il est utile lors de la configuration initiale et de la phase de test. Il constitue le moyen le plus rapide de configurer AVG pour la première fois. Par la suite, l'interface de gestion basée sur le navigateur (BBI) peut être utilisée afin d'apporter à la connectivité SSL VPN les modifications recommandées. Pour de plus amples informations, consultez le document *User Guide Avaya VPN Gateway* (Guide d'utilisateur Avaya VPN Gateway) (NN46120-104).

Lorsque vous utilisez la commande new pour exécuter l'assistant d'installation rapide, les paramètres suivants sont créés :

- Un VPN. Le VPN est généralement défini pour l'accès à un intranet, à des sections d'un intranet ou à un extranet.
- Un serveur SSL virtuel du type du portail. Une adresse IP de portail y est affectée ; l'utilisateur distant doit s'y connecter pour accéder au portail. Si vous avez choisi d'utiliser la fonction VPN sans commutateur d'application, le serveur du portail est défini sur le mode autonome.
- Un certificat test a été installé et associé au serveur du portail.
- La méthode d'authentification est définie sur la base de données locale et un utilisateur test est configuré. L'utilisateur test appartient à un groupe appelé `trusted` dont les règles d'accès permettent d'accéder à tous les réseaux, services et chemins.
- Un ou plusieurs noms de domaine sont ajoutés à la liste de recherche DNS. Ainsi, l'utilisateur distant peut saisir un nom abrégé dans les différents champs d'adresse du portail (par exemple, inside au lieu de inside.exemple.com si exemple.com est ajouté à la liste de recherche).

- Si vous avez choisi d'activer la redirection de HTTP vers HTTPS, un serveur supplémentaire de type HTTP a été créé afin de rediriger vers HTTPS les requêtes effectuées avec HTTP. En effet, le serveur du portail nécessite une connexion SSL.

Une version imprimée des exemples de paramètres de configuration à partir du fichier journal Installation rapide est disponible à la section Annexe A : Exemple de fichier journal d'Installation rapide AVG à la page 94.

Liens connexes

Configuration d'Avaya VPN Gateway à la page 22

Activation des services d'accès à distance

En plus d'utiliser la console VM locale pour configurer VPN, l'administrateur doit aussi gérer le VPN à l'aide d'une session TELNET ou SSH ou via la BBI. Pour autoriser la configuration à distance de VPN Gateway, les services d'accès à distance doivent être activés.

Exécutez cette procédure à l'aide de l'interface de ligne de commande (CLI). Reportez-vous aux documents AVG suivants :

- *Command Reference Avaya VPN Gateway (Référence des commandes Avaya VPN Gateway)*
- *CLI Application Guide Avaya VPN Gateway (Guide d'application CLI Avaya VPN Gateway)*

Procédure

1. Connectez-vous à l'AVG.
2. Saisissez les commandes suivantes.

```
/cfg/sys/adm/.
        telnet on
        ssh on
/cfg/sys/adm/https/.
        cert 1
        ena true
/cfg/sys/adm/http/.
        ena true
apply
```

Liens connexes

Configuration d'Avaya VPN Gateway à la page 22

Exécution de l'assistant Net Direct

Grâce à l'assistant Net Direct, vous pouvez créer sur le portail un lien qui permet de télécharger et de lancer une version allégée du client Avaya VPN, à savoir le client Net Direct. Exécutez l'assistant Net Direct à partir de l'interface Manager basée sur le navigateur (BBI). Consultez

le document *Avaya VPN Gateway BBI Application Guide* (Guide d'application BBI Avaya VPN Gateway).

Procédure

1. Connectez-vous à l'AVG BBI.

   Dans le panneau de navigation à gauche, sélectionnez **Assistants**.
2. Cliquez sur **Assistant Net Direct**.
3. Sur la page **Paramètres Net Direct pour le VPN sélectionné**, activez la case d'option **Activer Net Direct pour ce VPN**.
4. Sur la page **Paramètres du pool IP par défaut** :
   - Pour **IPPool par défaut**, sélectionnez **Pool_local**.
   - Saisissez les adresses IP de début et de fin de la plage de pool.

Liens connexes

Configuration d'Avaya VPN Gateway à la page 22

Modification de l'AVG par défaut pour SSL VPN

Une fois les assistants de configuration Installation rapide et Net Direct exécutés, la configuration par défaut doit être modifiée afin de prendre en charge une connexion SSL VPN avec un système IP Office.

Exécutez cette procédure à l'aide de l'interface d'AVG basée sur le navigateur (BBI). Consultez le document *Avaya VPN Gateway BBI Application Guide* (Guide d'application BBI Avaya VPN Gateway).

Cette procédure est dupliquée à la section Annexe B : Modification de l'AVG par défaut pour SSL VPN (avec captures d'écran) à la page 98. Cette version de la procédure comprend des captures d'écran de l'interface utilisateur.

Préambules

Assurez-vous que la passerelle par défaut configurée sur l'AVG réponde aux requêtes ICMP. Si la passerelle par défaut ne répond pas aux requêtes ICMP, l'AVG ne peut pas fournir de services VPN.

Procédure

1. Connectez-vous à l'AVG BBI en tant qu'administrateur.
2. Dans le panneau de navigation à gauche, sélectionnez l'onglet **Config**, puis **Passerelle VPN** > **VPN 1** > **Pool IP**.
3. Il est possible que le VPN par défaut de la configuration AVG de base dispose déjà d'un pool local. Si ce n'est pas le cas, vous devez ajouter un pool local au VPN par défaut.

Sur la page **Ajouter un nouveau pool d'adresses IP**, ajoutez un pool local au VPN par défaut.

4. Sur la page **Modifier le pool d'adresses IP**, assurez-vous que les valeurs des champs **IP de début** et **IP de fin** correspondent aux valeurs définies via l'assistant de configuration Net Direct.
5. Sur la page **Pool IP** > **Paramètres des attributs du réseau**, sélectionnez l'onglet **Attributs du réseau** et saisissez les valeurs correspondant à votre réseau.
6. Sur la page **Pool IP**, définissez le pool local que vous avez créé à l'étape 3 comme **pool IP par défaut**.
7. Sur la page **Paramètres d'accès du client Net Direct**, vérifiez les paramètres créés via l'assistant de configuration Net Direct.
   - Assurez-vous que l'option **Vérification d'inactivité** est **désactivée**.
   - Assurez-vous que la bannière Net Direct est définie.
8. Définissez le lien du portail pour qu'il ouvre le client Net Direct. Sur la page **Configuration des liens du portail**, sélectionnez l'onglet **Lien du portail**. Dans le champ **Type de lien**, sélectionnez **Net Direct**.
9. Sur la page **Réseaux pour tunnels distincts** :
   - définissez **Mode de tunnels distincts** sur **activé** ;
   - définissez les routes de tunnels distincts pour atteindre l'agent de service sur le réseau privé.
10. Pour VPN 1, ouvrez la page des groupes et sélectionnez **Groupe 1**. Sur la page **Modifier un groupe**, définissez le pool local que vous avez créé à l'étape 3 comme pool IP.
11. Ouvrez la page **VPN 1** > **Groupe 1** > **Listes d'accès**. Sur la page **Liste d'accès de pare-feu**, créez une règle d'accès si elle n'a pas été créée par défaut.
12. Ouvrez la page **VPN 1** > **SSL**. Sur la page **Paramètres du serveur**, sous **Paramètres SSL**, définissez **Chiffrements** sur **AES256-SHA** pour un chiffrement renforcé.
13. Ouvrez la page **VPN 1** > **Autorisation** > **Services**. Supprimez tous les services définis dans la configuration par défaut car ils ne sont pas requis par SSL VPN.
14. Ouvrez la page **VPN 1** > **Autorisation** > **Réseaux**. Définissez le sous-réseau d'autorisation référencé dans l'une des règles d'accès et défini dans **VPN 1** > **Groupe 1** > **Listes d'accès**.

    Remarque :

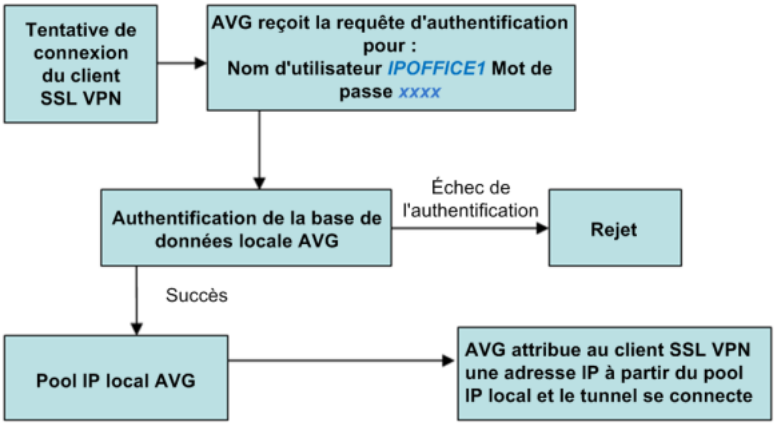
    Ce paramètre contrôle la communication entre les tunnels de SSL VPN. La communication est uniquement activée en spécifiant une liste autorisée de réseaux « intranet ». La communication entre clients VPN est bloquée par défaut.
15. Ouvrez la page **VPN 1** > **Paramètres généraux** > **Session**. Définissez la **période d'inactivité de la session** sur 2 minutes.

Liens connexes

Configuration d'Avaya VPN Gateway à la page 22

Configuration de l'authentification locale

Si les systèmes IP Office sont peu nombreux, vous pouvez utiliser la base de données locale Avaya VPN Gateway (AVG) pour créer les données utilisateur nécessaires à l'authentification. Ceci permet de configurer rapidement l'authentification alors qu'aucun serveur d'authentification RADIUS externe n'est disponible. Configurez un pool IP pour attribuer des adresses IP aux utilisateurs locaux de façon dynamique. Le schéma ci-après illustre le flux d'authentification du client SSL VPN ainsi que la méthode d'attribution des adresses du pool IP.



Cette procédure comporte les étapes manuelles permettant de configurer l'authentification locale. Vous pouvez aussi configurer l'authentification à l'aide de l'assistant d'authentification AVG.

Procédure

1. Pour **VPN 1**, ouvrez la page **Configuration du pool IP** et ajoutez un pool IP local.
2. Sélectionnez **VPN 1** > **Pool IP** > **Ajouter/Modifier**. Définissez la plage dynamique du pool IP en renseignant les champs **IP de début** et **IP de fin**.
3. Sélectionnez **VPN 1** > **Pool IP** > **Attribut du réseau**. Définissez le **masque de sous-réseau du client**.
4. Sur la page **Ajouter un groupe**, ajoutez un nouveau groupe à VPN 1.
5. Sélectionnez **VPN 1** > **<Nom_Groupe>** > **Modifier le groupe**. Sélectionnez l'onglet **Général** et attribuez un pool local au groupe en le sélectionnant dans le champ **Pool IP**.
6. Sélectionnez l'onglet **Listes d'accès** et indiquez la liste d'accès pour le groupe d'utilisateurs locaux.
7. Sélectionnez l'onglet **Liens** et attribuez les liens.

8. Modifiez les paramètres de l'authentification VPN. Sur la page **Serveurs d'authentification**, ajoutez un nouveau serveur d'authentification.
9. Sélectionnez **VPN 1** > **<Nom_Serveur_Auth>** > **Ajouter/Modifier des utilisateurs** et ajoutez des utilisateurs au groupe.
10. Modifiez le serveur d'authentification et définissez l'**ordre d'authentification**.

Liens connexes

Configuration d'Avaya VPN Gateway à la page 22

Configuration de l'authentification RADIUS

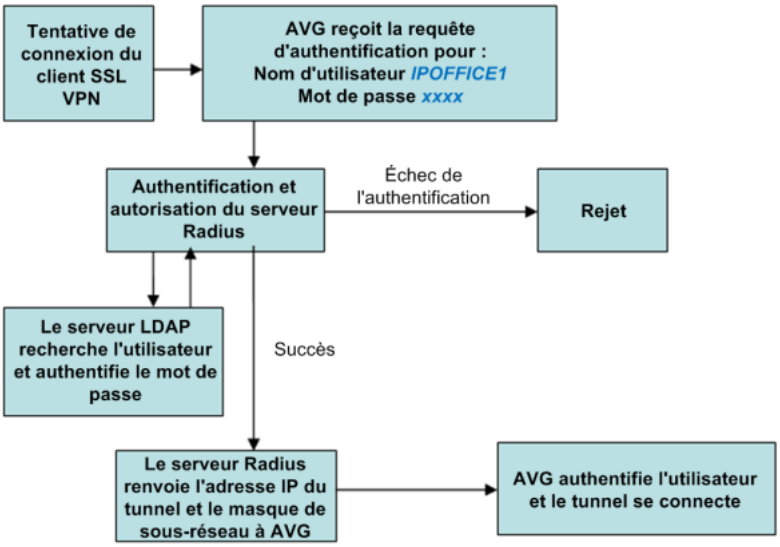
Le principal avantage de l'authentification RADIUS est que le service SSL VPN se voit toujours attribuer la même adresse IP de tunnel.

Pour configurer l'authentification RADIUS, vous devez installer un serveur RADIUS. Pour un serveur RADIUS, Avaya recommande Avaya Identity Engine. Pour obtenir des informations et télécharger le logiciel, rendez-vous à l'adresse http://support.avaya.com.

Les informations sur l'authentification du protocole RADIUS, telles que les informations sur le compte utilisateur, et les informations sur le tunnel SSL VPN, telles que l'adresse IP et le masque de sous-réseau, doivent être stockées dans une base de données. Deux options sont possibles :

- Utiliser la base de données locale d'Identity Engine pour stocker les informations sur l'utilisateur et fournir à la fois les services de recherche et d'authentification et d'autorisation. Cette option peut être utilisée pour un nombre peu élevé d'utilisateurs. Le nombre d'utilisateurs est limité dans Identity Engine. Reportez-vous à la documentation pour connaître le nombre exact.
- Utiliser un serveur LDAP pour stocker les informations d'identification utilisateur et les informations sur le tunnel SSL VPN, à la fois pour les services de recherche et d'authentification. Cette option convient aux déploiements impliquant un nombre élevé d'utilisateurs.

Pour l'installation du serveur LDAP, la documentation Avaya Identity Engine Radius Server contient les options de configuration pour les serveurs LDAP de différents fournisseurs. Le schéma ci-après illustre l'authentification RADIUS avec un serveur LDAP. Notez que dans cette procédure, cette configuration avec un serveur RADIUS ne nécessite pas de serveur LDAP.



Cette procédure comporte les étapes manuelles permettant de configurer l'authentification RADIUS. Vous pouvez aussi configurer l'authentification à l'aide de l'assistant d'authentification AVG.

Cette procédure est dupliquée à la section Annexe C : Configuration de l'authentification RADIUS (avec captures d'écran) à la page 104. Cette version de la procédure comprend des captures d'écran de l'interface utilisateur.

Procédure

1. Connectez-vous à l'AVG BBI en tant qu'administrateur.
2. Sur la page **Configuration du pool IP**, ajoutez un nouveau pool d'adresses IP pour l'authentification RADIUS.
3. Sur la page **Pool IP**, définissez le pool d'adresses IP de l'authentification RADIUS que vous avez créé à l'étape 2 comme **pool IP par défaut**.
4. Modifiez le VPN. Sur la page **Serveurs d'authentification** > **Ajouter un nouveau serveur d'authentification**, renseignez les champs correspondant au serveur RADIUS.
5. Définissez les paramètres du serveur d'authentification RADIUS. Notez que l'ID fournisseur 1872 est associé à Alteon et identifie AVG. Sélectionnez l'onglet **Paramètres** et renseignez les champs suivants.
   - **ID fournisseur : 1872**
   - **Type de fournisseur : 1**
   - **Délai d'expiration : 10**
   - **ID fournisseur pour ID VPN : 1872**
   - **Type de fournisseur pour ID VPN : 3**
6. Définissez les paramètres du réseau RADIUS. Sélectionnez l'onglet **Attributs du réseau** et renseignez les champs suivants.

Paramètres de l'ID fournisseur	Paramètres du type de fournisseur
Adresse IP du client : 1872	Adresse IP du client : 4
Masque de sous-réseau du client : 1872	Masque de sous-réseau du client : 5
Serveur NBNS principal : 1872	Serveur NBNS principal : 6
Serveur NBNS secondaire : 1872	Serveur NBNS secondaire : 7
Serveur DNS principal : 1872	Serveur DNS principal : 8

7. Définissez les attributs du filtre. Sélectionnez l'onglet Attributs du filtre et renseignez les champs suivants.
   - **Attribut du filtre Radius : désactivé**
   - **ID fournisseur pour l'attribut du filtre : 9**
   - **Type de fournisseur pour l'attribut du filtre : 1**
8. Indiquez l'adresse du serveur Radius. Sur la page **Serveurs RADIUS**, sélectionnez l'onglet **Serveurs**.
9. Cliquez sur **Ajouter**. Sur la page **Modifier le serveur RADIUS**, saisissez l'adresse IP et le mot de passe du serveur RADIUS.
10. Sélectionnez l'onglet **Ordre de l'authentification** et indiquez l'ordre préféré des méthodes d'authentification.

Liens connexes

Configuration d'Avaya VPN Gateway à la page 22

Attributs de configuration du serveur RADIUS

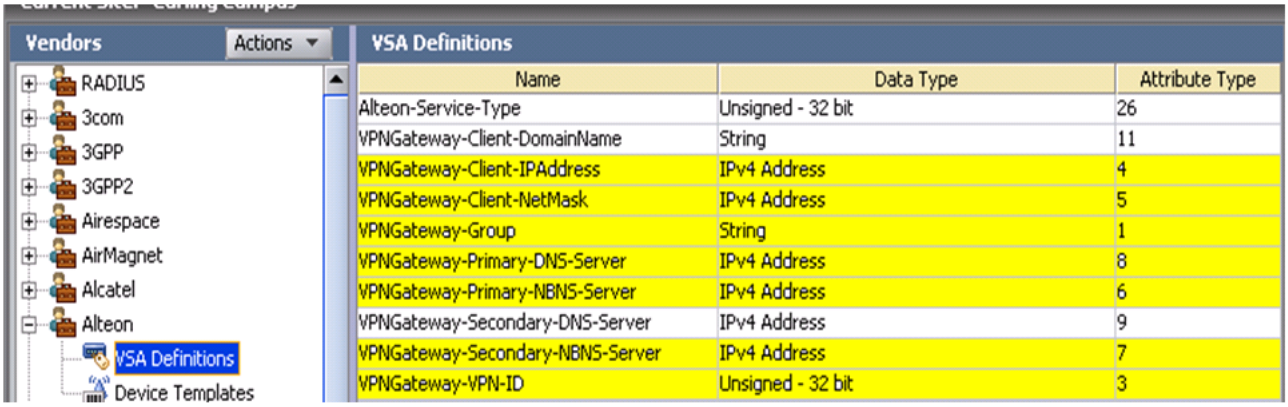
Le service SSL VPN nécessite un serveur RADIUS. Avaya recommande d'utiliser Avaya Identity Engines Ignition Server en tant que serveur RADIUS.

Lorsque vous connectez le service SSL VPN, Avaya VPN Gateway (AVG) authentifie le système IP Office en envoyant une requête à un serveur RADIUS externe. Cette section répertorie les attributs que vous devez configurer sur le serveur RADIUS.

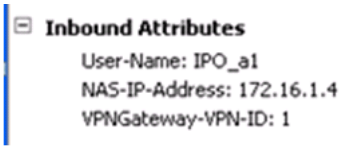
Mappage des attributs du serveur RADIUS

La liste ci-dessous répertorie le nom des attributs Radius spécifiques à chaque fournisseur, les types de données associés et les codes de type de fournisseur pour Alteon (AVG).

Les exemples suivants ont été obtenus à l'aide d'un serveur RADIUS Avaya Identity Engines. Les attributs en surbrillance ont été configurés comme **Attributs du réseau** et **Paramètres** dans la configuration du serveur RADIUS AVG.



• Les attributs entrants allant de l'AVG vers le serveur Radius au cours de la requête d'authentification sont indiqués ci-dessous.



Les attributs Radius envoyés par l'AVG sont les suivants :

- o NAS-IP-Address (attribut de radius générique) correspond à l'adresse IP de l'AVG.
- User-Name (attribut de radius générique) correspond au nom du compte de l'utilisateur.
- VPNGateway-VPN-ID est un attribut Alteon.

Le serveur Radius IDEngine possède un mappage interne par défaut pour les attributs Radius les plus courants, comme indiqué dans le tableau ci-dessous. Les lignes en surbrillance correspondent aux attributs Radius contenus dans la REQUÊTE Radius ci-dessus.

Inbound Attributes

Name	Vendor	Attribute Mapping
Inbound-Digest-Auth-Param	RADIUS	Digest-Auth-Param
Inbound-Digest-Domain	RADIUS	Digest-Domain
Inbound-Digest-Method	RADIUS	Digest-Method
Inbound-Digest-Nonce-Count	RADIUS	Digest-Nonce-Count
Inbound-Digest-Opaque	RADIUS	Digest-Opaque
Inbound-Digest-Qop	RADIUS	Digest-Qop
Inbound-Digest-Realm	RADIUS	Digest-Realm
Inbound-Digest-SIP-AOR	RADIUS	Digest-SIP-AOR
Inbound-Digest-URI	RADIUS	Digest-URI
Inbound-Digest-Username	RADIUS	Digest-Username
Inbound-Framed-Compression	RADIUS	Framed-Compression
Inbound-Framed-Interface-Id	RADIUS	Framed-Interface-Id
Inbound-Framed-IP-Address	RADIUS	Framed-IP-Address
Inbound-Framed-IP-Netmask	RADIUS	Framed-IP-Netmask
Inbound-Framed-MTU	RADIUS	Framed-MTU
Inbound-Framed-Pool	RADIUS	Framed-Pool
Inbound-Framed-Protocol	RADIUS	Framed-Protocol
Inbound-Login-IP-Host	RADIUS	Login-IP-Host
Inbound-NAS-Identifier	RADIUS	NAS-Identifier
Inbound-NAS-IP-Address	RADIUS	NAS-IP-Address
Inbound-NAS-Port	RADIUS	NAS-Port
Inbound-NAS-Port-Id	RADIUS	NAS-Port-Id
Inbound-NAS-Port-Type	RADIUS	NAS-Port-Type
Inbound-Port-Limit	RADIUS	Port-Limit
Inbound-Service-Type	RADIUS	Service-Type
Inbound-Tunnel-Client-Auth-Id	RADIUS	Tunnel-Client-Auth-Id
Inbound-Tunnel-Client-Endpoint	RADIUS	Tunnel-Client-Endpoint
Inbound-Tunnel-Medium-Type	RADIUS	Tunnel-Medium-Type
Inbound-Tunnel-Preference	RADIUS	Tunnel-Preference
Inbound-Tunnel-Private-Group-Id	RADIUS	Tunnel-Private-Group-Id
Inbound-Tunnel-Server-Auth-Id	RADIUS	Tunnel-Server-Auth-Id
Inbound-Tunnel-Server-Endpoint	RADIUS	Tunnel-Server-Endpoint
Inbound-Tunnel-Type	RADIUS	Tunnel-Type
Inbound-User-Name	RADIUS	User-Name

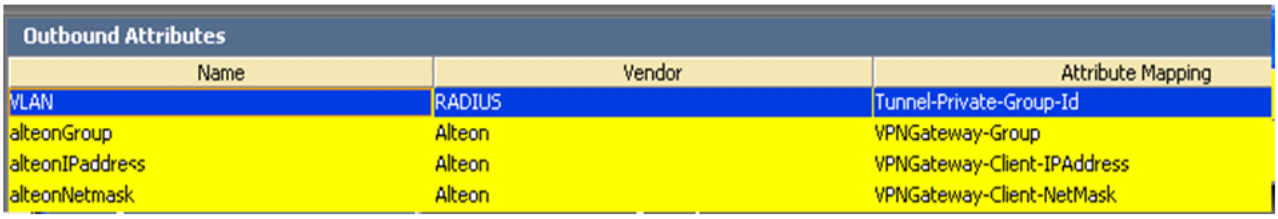
Les serveurs Radius évaluent les attributs entrants à l'aide de règles d'autorisation. La règle peut utiliser un attribut entrant pour vérifier une condition ou peut renvoyer l'attribut entrant dans une RÉPONSE Radius comme valeur sortante. Si un attribut entrant envoyé par l'AVG nécessite une évaluation mais qu'il ne fait pas partie de l'ensemble par défaut du serveur Radius, il doit être défini comme nouvel attribut entrant sur le serveur Radius. Pour consulter des exemples de règles d'authentification, reportez-vous au document *Administration IDEngine*.

• Les attributs sortants envoyés vers l'AVG depuis le serveur Radius au cours d'une RÉPONSE d'authentification sont indiqués ci-dessous :

Outbound Attributes

alteonNetmask (VPNGateway-Client-NetMask): 255.255.0.0
alteonGroup (VPNGateway-Group): IPoffice
alteonIPaddress (VPNGateway-Client-IPAddress): 10.1.0.1

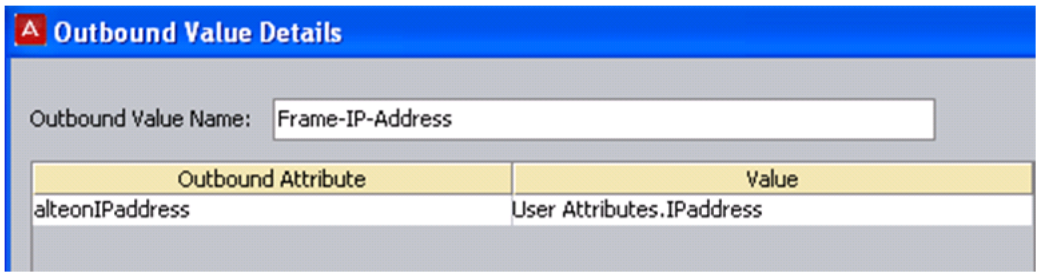
Les attributs sortants sont les champs de données utilisés par le serveur Radius pour transmettre les données de mise en service à VPN Gateway. Les attributs sortants sont des attributs de protocole Radius génériques ou du type du fournisseur. À l'image des attributs entrants, les attributs sortants doivent être créés s'ils ne font pas partie de l'ensemble par défaut du serveur Radius. Dans l'exemple ci-dessus, les trois attributs sortants Alteon (spécifiques à AVG) "alteonGroup", "alteonIPaddress" et "alteonNetmask" doivent être créés dans le serveur Radius selon l'exemple ci-après :



Outbound Attributes

Name	Vendor	Attribute Mapping
VLAN	RADIUS	Tunnel-Private-Group-Id
alteonGroup	Alteon	VPNGateway-Group
alteonIPaddress	Alteon	VPNGateway-Client-IPAddress
alteonNetmask	Alteon	VPNGateway-Client-NetMask

La valeur des attributs sortants peut être statique ou associée à des attributs utilisateur dans la base de données locale du serveur Radius ou dans un référentiel LDAP. Vous trouverez ci-dessous un exemple de valeur d'attribut sortant associée à un attribut de l'utilisateur de la base de données :



Outbound Value Details

Outbound Value Name: Frame-IP-Address

Outbound Attribute	Value
alteonIPaddress	User Attributes.IPaddress

Les valeurs sortantes sont associées à des règles d'authentification et sont envoyées vers VPN Gateway en tant qu'attributs Radius lorsque la règle est évaluée. Si la règle donne "Autoriser", les valeurs sortantes sont utilisées pour définir les caractéristiques de la session de l'utilisateur. Lorsque la règle donne "Refuser", les valeurs sortantes renvoyées sont généralement utilisées pour fournir des informations sur la cause du refus. Pour plus d'informations, reportez-vous à la documentation IDEngine.

Liens connexes

Configuration d'Avaya VPN Gateway à la page 22

Chapitre 5 : Configuration d'un SSL VPN pour l'assistance Avaya

Cette section fournit des informations sur la procédure de configuration pour IP Office lorsqu'Avaya est le fournisseur de services. Vous pouvez automatiquement configurer SSL VPN à l'aide du processus d'intégration.

Vous pouvez configurer plusieurs instances du service SSL VPN et les exécuter simultanément.

Prérequis

Lorsque vous configurez un service SSL VPN, l'adresse de la passerelle VPN peut être une adresse FQDN. Vous devez configurer le serveur DNS pour résoudre les adresses FQDN. Configurez les paramètres DSN dans le formulaire **Système** d'IP Office Manager, sous **DNS**.

Liens connexes

[Configuration d'un SSL VPN à l'aide d'un fichier d'intégration](#) à la page 36
[Modification d'un service existant à l'aide du fichier d'intégration](#) à la page 37

Configuration d'un SSL VPN à l'aide d'un fichier d'intégration

Le fichier d'intégration XML est disponible auprès d'Avaya. Il contient les paramètres requis pour établir un tunnel sécurisé entre IP Office et un serveur AVG. Une fois importé, le fichier d'intégration XML applique les paramètres et installe un ou plusieurs certificats TLS.

Pour configurer le service SSL VPN sur un nouveau système, vous devez commencer par générer un fichier d'inventaire du système IP Office. Quand vous enregistrez votre système IP Office, le fichier d'inventaire que vous avez généré est chargé dans le GRT et les données d'inventaire sont intégrées à la base de données Avaya Customer Support (ACS). Après avoir activé la prise en charge à distance, vous pouvez télécharger le fichier d'intégration XML du site Web GRT et le charger sur votre système IP Office.

Le processus d'intégration configure les éléments suivants :

- Configuration du service VPN SSL
- Codes courts permettant d'activer et de désactiver le service SSL VPN
- Interruptions des alarmes SNMP

- Un ou plusieurs certificats TLS dans le magasin de certificats approuvés IP Office.

Exécutez cette procédure à l'aide du client Avaya IP Office Web Manager.

Avertissement :

Le processus d'enregistrement en ligne crée automatiquement un service VPN SSL dans la configuration système lors du téléchargement du fichier d'enregistrement en ligne sur le système. Veillez à ne pas supprimer ou modifier ces services, sauf si Avaya vous invite à la faire.

Préambules

Avant de commencer, munissez-vous des codes produit et de la description figurant dans le catalogue de votre système IP Office. Par exemple, « IP OFFICE 500 VERSION 2 CONTROL UNIT TAA ».

Procédure

1. Sélectionnez **Outils > Intégration**.

   La boîte de dialogue Intégration s'ouvre.

2. Si le code matériel de votre système IP Office se termine par les lettres TAA, cochez la case située en regard de la question **Utilisez-vous le matériel de la gamme TAA ?**
3. Cliquez sur **Obtenir le fichier d'inventaire** pour générer un inventaire de votre système IP Office.
4. Cliquez sur **Enregistrer IP Office**.

   Un navigateur s'ouvre ; accédez au site Web GRT.

5. Connectez-vous au site Web, puis saisissez les données requises du système IP Office.
6. Sélectionnez **Remote Support** (Prise en charge à distance) pour le système IP Office.
7. Cliquez sur **Download** (Télécharger) et enregistrez le fichier d'intégration.
8. Accédez à l'emplacement où vous avez enregistré le fichier d'intégration et cliquez sur **Télécharger vers**.

   Un message s'affiche pour confirmer que le fichier d'intégration a été correctement installé.

Liens connexes

Configuration d'un SSL VPN pour l'assistance Avaya à la page 36

Modification d'un service existant à l'aide du fichier d'intégration

Vous pouvez utiliser le fichier d'intégration pour configurer le service SSL VPN. Le fichier d'intégration contient les paramètres requis pour établir un tunnel sécurisé entre IP Office et un serveur AVG. Suivez cette procédure quand vous avez déjà configuré le service SSL VPN sur un

système IP Office et que vous avez besoin de mettre à jour ou de modifier la configuration SSL VPN.

Vous pouvez l'exécuter depuis l'interface Avaya IP Office Web Manager.

Préambules

Avant de commencer, munissez-vous des codes produit et de la description figurant dans le catalogue de votre système IP Office. Par exemple, « IP OFFICE 500 VERSION 2 CONTROL UNIT TAA ».

Procédure

1. Sélectionnez **Outils > Intégration**.

   La boîte de dialogue Intégration s'ouvre.

2. Cette étape est facultative. Pour générer un inventaire de votre système IP Office, procédez comme suit :

   - Si le code matériel de votre système IP Office se termine par les lettres TAA, cochez la case située en regard de la question **Utilisez-vous le matériel de la gamme TAA ?**
   - Cliquez sur **Obtenir le fichier d'inventaire**.

3. Cliquez sur **Modifier**.

   Un navigateur s'ouvre ; accédez au site Web Avaya.

4. Connectez-vous au site Web.

   La page Connectivité à distance IP Office / Gestion de mot de passe s'ouvre.

5. Cliquez sur **Existing IP Office SSL VPN Remote Connectivity** (Connectivité à distance SSL VPN IP Office existante).

6. Sélectionnez **Regenerate on-boarding file (existing properties)** (Générer à nouveau le fichier d'intégration (avec les propriétés existantes)).

7. Saisissez le nom du service SSL VPN et le nom du compte SSL VPN dans les champs appropriés.

8. Cliquez sur **Submit** (Envoyer).

9. Choisissez si vous voulez recevoir le fichier d'intégration mis à jour par courrier électronique, ou si vous voulez le télécharger et suivre les indications qui s'affichent à l'écran.

10. Une fois le fichier téléchargé ou reçu par courrier électronique, enregistrez-le dans votre système local.

11. Accédez à l'emplacement où vous avez enregistré le fichier d'intégration et cliquez sur **Télécharger vers** depuis l'interface Web Manager.

    Un message s'affiche pour confirmer que le fichier d'intégration a été correctement installé.

Liens connexes

Configuration d'un SSL VPN pour l'assistance Avaya à la page 36

Chapitre 6 : Configuration d'un SSL VPN pour l'assistance aux partenaires Avaya

Ces prestataires de service tiers peuvent utiliser leur propre portail Avaya VPN pour porter assistance à un client distant en utilisant la technologie IP Office SSL VPN.

Pour l'assistance d'un fournisseur de services tiers, SSL VPN peut être configuré manuellement à l'aide de l'application Manager. Vous pouvez configurer un système standard ou un Server Edition système. La configuration manuelle n'est pas prise en charge par le mode Basic Edition.

Vous pouvez configurer plusieurs instances du service SSL VPN et les exécuter simultanément.

Prérequis

Lorsque vous configurez un service SSL VPN, l'adresse de la passerelle VPN peut être une adresse FQDN. Vous devez configurer le serveur DNS pour résoudre les adresses FQDN. Configurez les paramètres DNS dans le formulaire **Système** d'IP Office Manager, sous **DNS**.

Procédures de configuration d'un SSL VPN pour l'assistance aux partenaires Avaya

La liste ci-dessous indique la séquence de procédures à suivre pour configurer un SSL VPN pour l'assistance aux partenaires.

- Configuration du service SSL VPN à la page 40
- Installation d'un certificat à la page 42
- Configuration des codes de fonction à la page 43
- Configuration des notifications d'alarmes à la page 47
- Configuration d'une route statique à la page 51
- Vérification de la connexion à l'aide de à la page 62
- Envoi d'une alarme test à la page 64

Liens connexes

Configuration du service SSL VPN à la page 40
Installation d'un certificat à la page 42
Configuration des codes de fonction à la page 43
Configuration des notifications d'alarmes à la page 47
Configuration d'une route statique à la page 51

Configuration du service SSL VPN

Suivez cette procédure pour configurer le service SSL VPN.

Exécutez cette procédure depuis l'interface Manager. Si vous configurez un système Server Edition, utilisez le mode IP Office Manager for Server Edition.

Préambules

Vous devez connaître la valeur des variables de configuration suivantes.

Tableau 1 : onglet Service

Variable	Description
Nom du service	Saisissez un nom pour le nouveau service SSL VPN.
Nom du compte	Saisissez le nom du compte du service SSL VPN. Ce nom de compte permet d'authentifier le service SSL VPN lorsqu'il tente de se connecter à l'aide de AVG. **Systèmes Server Edition :** Si vous configurez un système Server Edition, Avaya vous recommande de définir le même nom pour le compte de service SSL VPN et pour l'ID de périphérique de l'agent SNMP. Quand ces paramètres correspondent, le personnel du support technique peut identifier les adresses du tunnel SSL VPN grâce à ces informations. Vous pouvez configurer un seul ID de périphérique d'agent SNMP par système. Si vous configurez plusieurs instances du service SSL VPN, choisissez l'un des noms de compte de service SSL VPN à associer à celui de l'ID de périphérique de l'agent SNMP en fonction de vos besoins en matière de support technique à distance. Vous pouvez également afficher l'ID du périphérique en sélectionnant **Réseau** dans la liste de navigation et en choisissant un système Server Edition ; un récapitulatif des paramètres du système sélectionné s'affiche.
Mot de passe du compte	Saisissez le mot de passe du compte de service SSL VPN.
Confirmer le mot de passe	Confirmez le mot de passe du compte de service SSL VPN.
Adresse du serveur	Saisissez l'adresse de la passerelle VPN. L'adresse peut être de type FQDN ou IPv4.
Type de serveur	Sélectionnez AVG.
Numéro de port du serveur	Sélectionnez un numéro de port. Le numéro de port par défaut est 443.

Tableau 2 : onglet Session

Variable	Description
Protocole de transfert de données préféré	Sélectionnez TCP ; il s'agit du protocole utilisé par le service SSL VPN pour le transfert de données. Si vous sélectionnez le protocole UDP lorsque vous configurez la connexion, UDP s'affiche dans ce champ mais le service SSL VPN le remplace par TCP.
Intervalle d'interrogation	Saisissez la durée, en secondes, de l'intervalle entre chaque message d'interrogation. La valeur par défaut est 30 secondes.
Tentatives d'interrogation	Saisissez le nombre de messages d'interrogation ignorés envoyés par IP Office à AVG avant de déterminer qu'AVG a cessé de répondre. Quand le nombre de messages d'interrogation consécutifs est atteint et qu'AVG n'en a pas accusé réception, IP Office interrompt la connexion. La valeur par défaut est 4.
Intervalle de reconnexion en cas d'échec	Il s'agit de la période d'attente avant que le service SSL VPN ne tente d'établir à nouveau une connexion avec AVG. Cette période commence au moment où le tunnel SSL VPN est en service et que sa tentative de connexion à AVG échoue, ou lorsque la connexion à AVG est perdue. La valeur par défaut est définie sur 60 secondes.

Procédure

1. Dans la liste de navigation, cliquez avec le bouton droit de la souris sur **Service**.
2. Sélectionnez **Nouveau** > **Service VPN SSL**.
3. Sous l'onglet **Service**, configurez les paramètres répertoriés dans le tableau ci-dessous.
4. Sélectionnez l'onglet **Session** et configurez les paramètres énumérés dans le tableau ci-dessous.
5. Sélectionnez l'onglet **Remplacement** et choisissez l'une des options suivantes :
   - pour activer le service et établir une connexion VPN SSL, veillez à ce que l'option **Service Remplacement activé** soit désélectionnée ;
   - pour configurer le service sans établir de connexion VPN SSL, sélectionnez l'option **Service Remplacement activé**.
6. Cliquez sur **OK**.
7. Cliquez sur l'icône **Enregistrer** pour enregistrer la configuration.

Liens connexes

Configuration d'un SSL VPN pour l'assistance aux partenaires Avaya à la page 39

Installation d'un certificat

Le service SSL VPN vérifie l'identité des périphériques à chaque extrémité du tunnel SSL VPN à partir de certificats numériques. Cette procédure décrit la méthode d'installation d'un certificat dans le magasin de certificats approuvés IP Office.

Manager intègrent une option de menu vous permettant de rétablir les paramètres de sécurité par défaut dans IP Office. Si vous restaurez vos paramètres de sécurité par défaut, et que le service SSL VPN ne se reconnecte pas avec l'AVG après quelques minutes, vous avez alors besoin d'ajouter à nouveau le certificat à l'emplacement de stockage du certificat approuvé.

De même, l'application Security Manager vous permet de supprimer le certificat du magasin de certificats approuvés. Si vous supprimez le certificat en utilisant Security Manager et que le service SSL VPN était déjà connecté avec AVG, le SSL VPN se déconnectera la prochaine fois que le tunnel renégociera la question secrète. Par défaut, cette renégociation a lieu toutes les 8 heures ; cet intervalle peut varier en fonction des paramètres configurés dans AVG. Lorsque le service SSL VPN est déconnecté au cours d'une renégociation, ou si vous désactivez le service avant que la renégociation suivante ait lieu, vous ne pouvez pas réactiver le service SSL VPN tant que vous n'avez pas installé le certificat requis dans le magasin de certificats approuvés.

Préambules

Vous devez installer un des types de certificat suivants :

- le certificat auto-signé AVG du portail du VPN auquel le service IP Office SSL VPN se connecte
- le certificat de l'autorité de certification qui a signé le certificat AVG.

Procédure

1. Sélectionnez **Fichier > Avancé > Paramètres de sécurité**.

   Une boîte de dialogue énumère les systèmes IP Office.
2. Cochez la case en regard du système IP Office sur lequel vous voulez installer le certificat.
3. Cliquez sur **OK**.

   Une boîte de dialogue s'ouvre.
4. Dans le champ **Nom d'utilisateur du service**, saisissez le nom d'utilisateur de l'administrateur IP Office.
5. Dans le champ **Mot de passe de l'utilisateur du service**, saisissez le mot de passe de l'administrateur IP Office.
6. Cliquez sur **OK**.

   Les informations d'identification sont acceptées.
7. Dans le volet de navigation, sélectionnez **Sécurité > Système**, puis le nom de configuration.
8. Sous l'onglet **Certificats**, cliquez sur **Ajouter**.

   Une boîte de dialogue s'ouvre, vous invitant à sélectionner la source du certificat.

9. Sélectionnez **Coller depuis le Presse-papiers** et cliquez sur **OK**.

   Une boîte de dialogue permettant de capturer le texte du certificat s'ouvre.

10. Copiez votre certificat et collez le texte dans la fenêtre ouverte. Vous devez inclure les lignes `-----BEGIN CERTIFICATE-----` et `-----END CERTIFICATE-----`.

11. Cliquez sur **OK**.

    Le nom du certificat s'affiche dans la liste des certificats installés.

Liens connexes

Configuration d'un SSL VPN pour l'assistance aux partenaires Avaya à la page 39

Configuration des codes de fonction

Le système IP Office permet de configurer des codes de fonction. Ces codes de fonction déclenchent une action spécifique quand vous les composez sur un téléphone connecté au système IP Office. Pour obtenir des informations sur la programmation des touches de téléphone avec des codes de fonction, consultez le document IP Office Manager.

Vous pouvez configurer des codes de fonction et les utiliser pour activer et désactiver le service SSL VPN. Lorsque le service SSL VPN est activé ou désactivé par le biais des codes de fonction, il reste provisionné dans le système ; les codes de fonction mettent le tunnel en service ou en état de remplacement.

Le système IP Office propose un ensemble de fonctions prédéfinies, accessibles par le biais des codes de fonction. Les fonctions prédéfinies ci-dessous permettent de créer des codes de fonction qui activent ou désactivent le service SSL VPN :

- Désactiver le mode Service de nuit du groupe de recherche de ligne : active le service SSL VPN
- Définir le groupe de recherche de ligne sur Service de nuit : désactive le service SSL VPN

Ces codes de fonction sont disponibles en interne et vous devez les composer depuis un téléphone de bureau connecté au système IP Office. Pour pouvoir les utiliser depuis un téléphone externe, vous pouvez configurer un standard automatique. Le standard automatique vous permet de composer un numéro pour accéder au système IP Office depuis un téléphone externe et d'activer les codes de fonction à l'aide d'un système de menu.

Liens connexes

Configuration d'un SSL VPN pour l'assistance aux partenaires Avaya à la page 39
Configuration d'un code de fonction pour activer le service SSL VPN à la page 44
Configuration d'un code de fonction pour désactiver le service SSL VPN à la page 44
Configuration d'un standard automatique à la page 45

Configuration d'un code de fonction pour activer le service SSL VPN

Suivez cette procédure pour configurer un code de fonction qui active le service SSL VPN quand le numéro est composé depuis un téléphone connecté au système IP Office.

Procédure

1. Dans la liste de navigation, sélectionnez **Code de fonction**.

   La liste des codes de fonction définis par défaut s'affiche.

2. Cliquez avec le bouton droit de la souris et sélectionnez **Nouveau**.

   L'onglet Code de fonction s'affiche.

3. Dans le champ **Code**, saisissez ***775*x*1**, où *x* représente une instance du service SSL VPN, dans une plage de 1 à 9. Par exemple, si deux instances de service SSL VPN sont configurées, et que vous définissez des codes de fonction pour la première instance, saisissez ***77511**.

   Remarque :

   Vous pouvez attribuer différents numéros aux codes de fonctions. Dans le but de vous simplifier la tâche, Avaya vous recommande d'utiliser *775, qui représente *SSL sur un clavier.

4. Dans la liste **Fonction**, sélectionnez **Désactiver le mode Service de nuit du groupe de recherche de ligne**.

5. Dans le champ **Numéro de téléphone**, saisissez le nom du service SSL VPN entre guillemets. Par exemple, pour le nom de service Service1, saisissez `"Service1"`.

   Utilisez le nom de service SSL VPN que vous avez saisi lors de la création du service SSL VPN. Pour de plus amples informations sur ce paramètre, consultez la section Configuration du service SSL VPN à la page 40.

6. Cliquez sur **OK**.

7. Cliquez sur l'icône **Enregistrer** pour enregistrer les modifications apportées à la configuration.

Liens connexes

Configuration des codes de fonction à la page 43

Configuration d'un code de fonction pour désactiver le service SSL VPN

Suivez cette procédure pour configurer un code de fonction qui désactive le service SSL VPN quand le numéro est composé depuis un téléphone connecté au système IP Office.

Procédure

1. Dans la liste de navigation, sélectionnez **Code de fonction**.

La liste des codes de fonction définis par défaut s'affiche.

2. Cliquez avec le bouton droit de la souris et sélectionnez **Nouveau**.

   L'onglet Code de fonction s'affiche.

3. Dans le champ **Code**, saisissez ***775*x*0**, où *x* représente une instance du service SSL VPN, dans une plage de 1 à 9. Par exemple, si deux instances de service SSL VPN sont configurées, et que vous définissez des codes de fonction pour la première instance, saisissez ***77510**.

   Remarque :

   Vous pouvez attribuer différents numéros aux codes de fonctions. Dans le but de vous simplifier la tâche, Avaya vous recommande d'utiliser *775, qui représente *SSL sur un clavier.

4. Dans la liste **Fonction**, sélectionnez **Définir le groupe de recherche de ligne sur Service de nuit**.

5. Dans le champ **Numéro de téléphone**, saisissez le nom du service SSL VPN entre guillemets. Par exemple, pour le nom de service Service1, saisissez `"Service1"`.

   Utilisez le nom de service SSL VPN que vous avez saisi lors de la création du service SSL VPN. Pour de plus amples informations sur ce paramètre, consultez la section Configuration du service SSL VPN à la page 40.

6. Cliquez sur **OK**.

7. Cliquez sur l'icône **Enregistrer** pour enregistrer les modifications apportées à la configuration.

Liens connexes

Configuration des codes de fonction à la page 43

Configuration d'un standard automatique

La procédure ci-dessous explique comment configurer un standard automatique. Le standard automatique vous permet d'accéder au système IP Office depuis un numéro de téléphone interne ou externe et d'utiliser un système de menu pour activer ou désactiver le service SSL VPN.

Préambules

Vous devez configurer des codes de fonction. Voir Configuration des codes de fonction à la page 43.

Si vous utilisez Avaya Voicemail Pro, vous devez définir un module qui permet d'aider le transfert avant de commencer cette procédure. Pour plus d'informations, voir *Administration de Voicemail Pro* (15–601063).

À propos de cette tâche

Dans cette procédure, vous créez un standard automatique, puis mappez les appels entrants au standard automatique. Cet exemple utilise la valeur 0 pour activer le service SSL VPN et la valeur 1 pour le désactiver, mais vous pouvez attribuer ces fonctions à n'importe quelle touche du clavier.

Procédure

1. Sélectionnez l'une des options suivantes :
   - Si vous utilisez Embedded Voicemail, sélectionnez **Standard automatique** dans la liste de navigation.
   - Si vous utilisez Voicemail Pro, commencez cette procédure à l'étape 12 à la page 46.
2. Cliquez avec le bouton droit de la souris et sélectionnez **Nouveau**.
3. Dans le champ **Nom**, saisissez le nom à attribuer au standard automatique.
4. Sélectionnez l'onglet **Actions**.
5. Choisissez l'entrée de la touche **0** et cliquez sur le bouton **Modifier**.
6. Dans la liste **Action**, sélectionnez une des options suivantes :
   - Sélectionnez **Transfert normal**.
   - Sélectionnez **Transfert**.
7. Dans la liste **Destination**, saisissez le code de fonction que vous avez configuré pour activer le service et cliquez sur **OK**.
8. Choisissez l'entrée de la touche **1** et cliquez sur le bouton **Modifier**.
9. Dans la liste **Action**, sélectionnez une des options suivantes :
   - Sélectionnez **Transfert normal**.
   - Sélectionnez **Transfert**.
10. Dans la liste **Destination**, saisissez le code de fonction que vous avez configuré pour désactiver le service et cliquez sur **OK**.
11. Cliquez sur l'icône **Enregistrer** pour enregistrer les modifications apportées à la configuration.
12. Dans la liste de navigation, sélectionnez **Route des appels entrants**.
13. Sous l'onglet **Standard**, définissez le champ **Capacité de support** sur **Toute voix**.
14. Dans la liste **ID du groupe de lignes**, sélectionnez la ligne que vous souhaitez utiliser pour l'activation et la désactivation du service SSL VPN.
15. Sélectionnez l'onglet **Destination**.
16. Choisissez l'une des options suivantes :
    - Si vous utilisez Embedded Voicemail, dans la liste **Destination,** sélectionnez le standard automatique que vous avez configuré.
    - Si vous utilisez Voicemail Pro, saisissez `VM:<nom>` dans la liste **Destination**, où `<nom>` désigne le nom du module Voicemail Pro.
17. Cliquez sur **OK**.
18. Cliquez sur l'icône **Enregistrer** pour enregistrer les modifications apportées à la configuration.

Étapes suivantes

Vous pouvez enregistrer des invites pour le standard automatique. Pour plus d'informations sur l'enregistrement des invites, consultez la documentation de votre système de messagerie vocale. Si vous utilisez Embedded Voicemail, consultez le *Installation de Embedded Voicemail*. Si vous utilisez Voicemail Pro, consultez le document *Administration de Voicemail Pro*.

Liens connexes

Configuration des codes de fonction à la page 43

Configuration des notifications d'alarmes

La configuration de la gestion des erreurs du service SSL VPN est facultative. Si vous configurez la gestion des erreurs, vous pouvez définir des filtres afin de déterminer les types d'événements pour lesquels vous voulez être notifié. Vous pouvez par exemple recevoir des notifications relatives aux erreurs liées au service SSL VPN, ou relatives aux erreurs liées au système IP Office.

Pour configurer la gestion des erreurs, vous devez définir la destination des alarmes pour le signalement des erreurs système. Vous pouvez définir les destinations suivantes pour la consignation des alarmes :

- Interruptions SNMP signalées sur un réseau LAN local ou sur un serveur distant
- Notifications par courrier électronique signalées sur un serveur SMTP d'un réseau LAN local ou un serveur SMTP distant
- Entrées syslog signalées sur un réseau LAN local, ou sur un serveur distant

Les destinations d'alarmes pouvant être configurées dépendent du mode de fonctionnement utilisé. Le tableau ci-dessous répertorie les destinations d'alarmes prises en charge pour chaque mode.

Destination d'alarmes	Mode de fonctionnement			
	Essential Edition	IP Office Server Edition	Système d'expansion Server Edition	Basic Edition
Interruptions SNMP				
SNMP sur un réseau LAN local	✔	✔	✔	✔
SNMP sur un service SSL VPN	✔	✔	✔	✔
Notifications par courrier électronique				
Serveur SMTP sur un réseau LAN local	✔	✔	✔	—

Table continues…

Destination d'alarmes	Mode de fonctionnement			
	Essential Edition	IP Office Server Edition	Système d'expansion Server Edition	Basic Edition
Serveur SMTP sur un tunnel SSL VPN	✔	✔	✔	—
Entrées syslog				
Serveur Syslog sur un réseau LAN local	✔	✔	✔	—
Serveur Syslog sur un tunnel SSL VPN	✔	✔	✔	—

Liens connexes

Configuration d'un SSL VPN pour l'assistance aux partenaires Avaya à la page 39
Configuration des destinations des interruptions SNMP à la page 48
Configuration des notifications d'alarmes par courrier électronique à la page 49
Configuration des entrées syslog à la page 50

Configuration des destinations des interruptions SNMP

Suivez la procédure ci-dessous pour signaler des erreurs système sous forme d'interruptions SNMP. Vous pouvez définir des filtres afin de déterminer les types d'événements qui génèrent des interruptions SNMP. Par exemple, vous pouvez générer des interruptions SNMP pour des erreurs liées au service SSL VPN ou pour des erreurs liées au système IP Office.

Préambules

Quand vous définissez une adresse IP de destination pour un événement d'erreur, le système s'appuie sur un tableau de routage IP pour déterminer quelle interface servira à envoyer l'événement d'erreur. La destination doit correspondre à une adresse IPv4 pour que l'interruption SNMP soit correctement acheminée vers le serveur de gestion des erreurs.

Vous devez configurer un dispositif d'écoute d'interruption sur l'ordinateur de destination où les interruptions SNMP sont signalées.

Procédure

1. Dans la liste de navigation, cliquez sur **Système** et sélectionnez l'onglet **Événements système**.

   Manager affiche les onglets **Configuration** et **Alarmes**.
2. Sous l'onglet **Configuration**, sélectionnez l'option **SNMP activé**.
3. Dans le champ **Communauté**, saisissez `public`.
4. Dans l'onglet **Alarmes**, cliquez sur **Ajouter**.
5. Sélectionnez **Interruption** et saisissez une adresse de destination pour les interruptions SNMP dans le champ **Adresse IP**. .

6. Saisissez un numéro de port ou utilisez le numéro de port par défaut (162).
7. Dans le champ **Communauté**, saisissez `public`.
8. Dans la liste **Événements**, choisissez le filtre d'événements :
   - Sélectionnez **Service** pour générer les interruptions SNMP concernant les erreurs liées au service SSL VPN.
   - Sélectionnez tout événement lié au fonctionnement du système IP Office pour lequel vous souhaitez générer des interruptions SNMP. Pour plus d'informations sur ces options, reportez-vous à *IP Office Manager*.
9. Cliquez sur **OK** pour fermer la boîte de dialogue.
10. Cliquez sur **OK** dans l'onglet Alarmes.
11. Cliquez sur l'icône **Enregistrer** pour enregistrer les modifications apportées à la configuration.

Liens connexes

Configuration des notifications d'alarmes à la page 47

Configuration des notifications d'alarmes par courrier électronique

Suivez la procédure ci-dessous pour recevoir par courrier électronique les notifications des erreurs lorsqu'elles surviennent. Vous pouvez définir des filtres afin de déterminer les types d'événements pour lesquels vous voulez être notifié. Vous pouvez par exemple recevoir des notifications relatives aux erreurs liées au service SSL VPN, ou relatives aux erreurs liées au système IP Office.

Préambules

Vous devez configurer un serveur de messagerie SMTP sur l'ordinateur qui sert à la gestion des erreurs. Vous devez également configurer un client de messagerie sur l'ordinateur sur lequel vous voulez recevoir les notifications par courrier électronique.

Quand vous définissez une adresse de destination pour un événement d'erreur, le système s'appuie sur un tableau de routage IP pour déterminer quelle interface servira à envoyer l'événement d'erreur. La destination doit correspondre à une adresse IPv4 pour que la notification soit correctement acheminée vers le serveur de gestion des erreurs.

Procédure

1. Dans la liste de navigation, cliquez sur **Système** et sélectionnez l'onglet **Événements système**.

   Manageraffiche les onglets **Configuration** et **Alarmes**.
2. Dans l'onglet **Alarmes**, cliquez sur **Ajouter**.
3. Sélectionnez l'option **Courrier électronique** et saisissez l'adresse souhaitée pour la réception des notifications dans le champ **Courrier électronique**.

4. Dans la liste **Événements**, choisissez le filtre d'événements :
   - Sélectionnez **Service** pour recevoir des notifications concernant les erreurs liées au service SSL VPN.
   - Sélectionnez tout événement lié au fonctionnement du système IP Office pour lequel vous souhaitez recevoir des notifications. Pour plus d'informations sur ces options, reportez-vous à *IP Office Manager*.
5. Cliquez sur **OK** pour fermer la boîte de dialogue.
6. Cliquez sur **OK** dans l'onglet Alarmes.
7. Sélectionnez l'onglet **SMTP**.
8. Dans le champ **Adresse IP**, saisissez l'adresse IP du serveur SMTP.
9. Dans le champ **Port**, saisissez le numéro de port du serveur SMTP.
10. Dans le champ **Adresse e-mail d'expéditeur**, saisissez l'adresse e-mail que le système IP Office doit utiliser pour envoyer les notifications.
11. Sélectionnez **Le serveur nécessite une authentification**.
12. Dans les champs **Nom d'utilisateur** et **Mot de passe**, saisissez les informations d'identification nécessaires pour se connecter au serveur SMTP.
13. Cliquez sur **OK**.
14. Cliquez sur l'icône **Enregistrer** pour enregistrer les modifications apportées à la configuration.

Liens connexes

Configuration des notifications d'alarmes à la page 47

Configuration des entrées syslog

Suivez la procédure ci-dessous pour signaler des erreurs système sous forme d'entrées syslog. Vous pouvez définir des filtres afin de déterminer les types d'événements signalés. Par exemple, vous pouvez signaler des erreurs liées au service SSL VPN ou liées au système IP Office.

Préambules

Vous devez configurer un client syslog sur le serveur où vous souhaitez que les erreurs systèmes soient signalées.

Quand vous définissez une adresse IP de destination pour un événement d'erreur, le système s'appuie sur un tableau de routage IP pour déterminer quelle interface servira à envoyer l'événement d'erreur. La destination doit correspondre à une adresse IPv4 pour que la notification soit correctement acheminée vers le serveur de gestion des erreurs.

Procédure

1. Dans la liste de navigation, cliquez sur **Système** et sélectionnez l'onglet **Événements système**.

   Manager affiche les onglets **Configuration** et **Alarmes**.

2. Dans l'onglet **Alarmes**, cliquez sur **Ajouter**.
3. Sélectionnez l'option **Syslog** et, dans le champ **Adresse IP**, saisissez l'adresse IP du serveur où le client syslog est configuré.
4. Dans le champ **Port**, saisissez le numéro de port du serveur où le client syslog est configuré.
5. Dans la liste **Événements**, choisissez le filtre d'événements :
   - Sélectionnez **Service** pour signaler les erreurs liées au service SSL VPN.
   - Sélectionnez tout événement lié au fonctionnement du système IP Office pour lequel vous souhaitez recevoir des notifications. Pour plus d'informations sur ces options, reportez-vous à *IP Office Manager*.
6. Cliquez sur **OK** pour fermer la boîte de dialogue.
7. Cliquez sur **OK** dans l'onglet **Alarmes.**
8. Cliquez sur l'icône **Enregistrer** pour enregistrer les modifications apportées à la configuration.

Liens connexes

Configuration des notifications d'alarmes à la page 47

Configuration d'une route statique

Quand vous configurez des routes de tunnel distinct sur AVG, le système IP Office intègre les informations de routage du tunnel de manière dynamique quand le service SSL VPN établit une connexion avec AVG. Toutefois, il est également possible de configurer une route statique. Cette section fournit des informations sur les situations propices à la configuration d'une route statique et explique la procédure de configuration.

Lorsque vous configurez une route statique, le système détermine la destination du trafic transféré à partir des informations de la route IP configurée dans Manager. Vous pouvez définir le service SSL VPN en tant que destination.

Utilisez une route statique quand :

- les tunnels distincts ne sont pas proposés par le AVG et que vous devez envoyer le trafic via le tunnel ;
- le service SSL VPN n'est pas connecté à AVG et que vous souhaitez mettre en file d'attente le trafic devant être transféré via le tunnel une fois la connexion restaurée.

Préambules

Vous devez vous munir tout d'abord des informations suivantes :

- l'adresse du sous-réseau distant ; il s'agit du sous-réseau situé dans le réseau privé où est installé AVG ;

- le masque de sous-réseau appliqué à l'adresse du sous-réseau ;
- le nom du service SSL VPN que vous souhaitez utiliser pour envoyer le trafic vers ce sous-réseau distant.

Procédure

1. Dans la liste de navigation, sélectionnez **Route IP**.
2. Cliquez avec le bouton droit de la souris et sélectionnez **Nouveau**.
3. Dans le champ **Adresse IP**, saisissez l'adresse du sous-réseau distant situé sur le site d'installation d'AVG.
4. Dans le champ **Masque de sous-réseau**, saisissez le masque de sous-réseau appliqué au sous-réseau distant.
5. Dans le champ **Adresse IP de la passerelle**, vérifiez que l'adresse IP de la passerelle est définie sur 0.0.0.0.
6. Dans la liste **Destination**, sélectionnez le nom du service SSL VPN.

Liens connexes

Configuration d'un SSL VPN pour l'assistance aux partenaires Avaya à la page 39

Chapitre 7 : Configuration d'un Partenaire Avaya SSL VPN en utilisant un SDK

Ces prestataires de service tiers peuvent utiliser leur propre portail Avaya VPN pour porter assistance à un client distant en utilisant la technologie IP Office SSL VPN.

Pour l'assistance d'un prestataire de service, le SSL VPN cpeut être configuré en utilisant un Software Development Kit (SDK). Le SDK est conçu pour permettre à des partenaires de paramétrer leur propre AVG en automatisant certains ou tous les aspects de l'enregistrement IP Office et du processus d'intégration. Le processus d'automatisation remplace les procédures utilisées pour une configuration manuelle.

Options SDK

Il existe deux intégrations des SDK.

- On-boarding SDK
- On-boarding Express SDK

On-boarding SDK :

Pour chaque nouvelle installation d'IP Office, On-boarding SDK est exécuté sur le serveur web du partenaire pour générer un fichier xml d'intégration qui est chargé sur IP Office via Web Manager. Ce processus paramètre le tunnel SSL VPN de l'IP Office du client au partenaire AVG.

On-boarding Express SDK :

Le On-boarding Express SDK peut être exécuté hors ligne sans connexion à Internet. Lorsque vous exécutez le SDK, IP Office est immédiatement intégré puis collecte tous les fichiers et identifiants concernés par le processus d'intégration dans un fichier zip. A ce stade, le tunnel SSL VPN tente de se connecter avec l'AVG mais n'arrive pas à être authentifié. Lorsque le partenaire traite le contenu du fichier zip pour créer les permissions SSL VPN du site client associé, l'AVG accepte la mise en place du tunnel SSL VPN.

Codes de fonction

IP Office supporte de nombreux services SSL VPN. Cela signifie qu'il peut y avoir deux services SSL VPN concurrents et activement connectés, l'un au Avaya Support AVG et l'autre au partenaire AVG. Lorsque deux services SSL VPN sont configurés sur IP Office, Avaya recommande de les nommer et de suivre une convention de codification courte expliquée ci-dessous pour le service Avaya Support SSL VPN et leur service Partner SSL VPN. Les conventions sont basées sur :

- Les chiffres 775 = SSL sur le cadran d'un téléphone.

- Le quatrième chiffre, 1 ou 2 est pour l'instance du service.
- Pour le cinquième chiffre, 1 = activé et 0 = désactivé.

Service Support Avaya SSL-VPN :

- Nom du service : AVAYA_SUPPORT
- Code court pour activer le service AVAYA_SUPPORT: 77511
- Code court pour désactiver service AVAYA_SUPPORT : 77510

Service partenaire SSL VPN :

- Nom du service : BP_SUPPORT
- Code court pour activer le service BP_SUPPORT: 77521
- Code court pour désactiver le service BP_SUPPORT: 77520

Prérequis

- Sur l'ordinateur sur lequel vous exécuterez le SDK, vous devez avoir Java 1,6 ou plus.
- L'adresse IP du tunnel ne doit pas être entre 172,22.0,0 et 172,25.255,255. Ce lot d'adresse est réservé à Avaya support.

Liens connexes

Téléchargement de SDK à la page 54
Téléchargement du fichier d'inventaire IP Office à la page 54
Utilisation de On-boarding SDK à la page 55
Utilisation de On-boarding Express SDK à la page 58

Téléchargement de SDK

Vous pouvez télécharger le On-boarding SDK et le On-Boarding Express SDK sur le site Internet Avaya DevConnect sur http://www.devconnectprogram.com/

Liens connexes

Configuration d'un Partenaire Avaya SSL VPN en utilisant un SDK à la page 53

Téléchargement du fichier d'inventaire IP Office

Cette procédure décrit la méthode manuelle pour le téléchargement du fichier d'inventaire IP Office en utilisant Web Manager. Le On-boarding Express SDK fournit des outils pour automatiser le téléchargement sans utiliser Web Manager. Pour plus d'informations, consulter la documentation incluse dans le On-boarding Express SDK.

Procédure

1. Connectez-vous à Web Manager. Dans un navigateur Web, entrez l'adresse IP du système IP Office au format `http://<ip_address>/index.html`.

   La page d'index du serveur s'ouvre.
2. Cliquez sur **IP Office Web Manager**.
3. Sur la page de connexion, entrez le nom d'utilisateur et le mot de passe, puis cliquez sur **Connexion**.
4. Sur la page Solution, cliquez sur le menu du serveur à droite du serveur et sélectionnez **On-boarding**.
5. Sur la page On-Boarding, cliquez sur **Obtenir le fichier d'inventaire**.

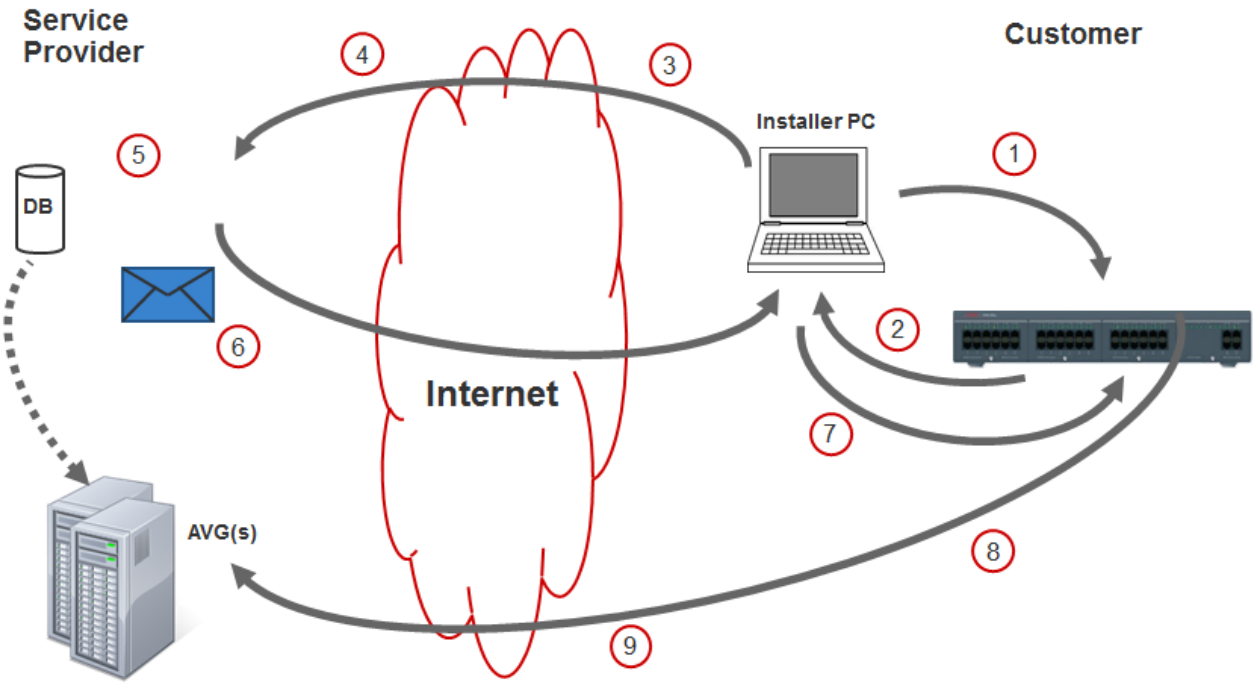
   Le fichier d'inventaire est téléchargé sur le programme d'installation du PC.

Liens connexes

[Configuration d'un Partenaire Avaya SSL VPN en utilisant un SDK](#) à la page 53

Utilisation de On-boarding SDK

Processus de configuration de SSL VPN en utilisant le On-boarding SDK



1	Configurez les paramètres IP Office suivants. • ID système • Licences • Interfaces LAN • Serveur DNS
2	Sur le site client, téléchargez le fichier d'inventaire XML à partir d'IP Office sur le programme d'installation du PC.
3	Chargez le fichier d'inventaire sur le site Partenaire.
4	Enregistrez les permissions VPN SSL dans la base de données.
5	Utilisez l'outil On-boarding SDK.
6	Envoyez par courrier électronique ou chargez le fichier xml on-boarding sur le programme d'installation du PC.
7	Chargez le fichier xml on-boarding sur l'IP Office.
8	Le service SSL VPN se connecte à l'AVG.
9	Utilisez SSA pour vérifier la connectivité SSL VPN.

Liens connexes

Configuration d'un Partenaire Avaya SSL VPN en utilisant un SDK à la page 53
Enregistrez les permissions VPN SSL dans la base de données AVG. à la page 56
Utilisation de On-boarding SDK à la page 56
Chargement du fichier d'intégration et vérification du SSL VPN à la page 57

Enregistrez les permissions VPN SSL dans la base de données AVG.

Si vous utilisez la base de données locale AVG, ajoutez les permissions sur l'interface de configuration de l'AVG.

Si vous utilisez une base de données LDAP ou une base de données RADIUS, utilisez l'interface appropriée pour ajouter les permissions dans la base de données.

Liens connexes

Utilisation de On-boarding SDK à la page 55

Utilisation de On-boarding SDK

Vous pouvez utiliser le SDK d deux façons.

- Utilisez le dossier de délivrance du script de commande d'intégration DOS avec les paramètres pertinents et les noms de fichier d'entrée/de sortie.
- Utilisez les JAVA API publiés.

Pour plus d'informations, consultez le guide du développeur SDK inclus dans le fichier zip SDK.

La sortie du SDK est le fichier d'intégration xml. Transférer le fichier sur le programme d'installation du PC sur le site client.

Liens connexes

Utilisation de On-boarding SDK à la page 55

Chargement du fichier d'intégration et vérification du SSL VPN

Procédure

1. Connectez-vous à Web Manager. Dans un navigateur Web, entrez l'adresse IP du système IP Office au format `http://<ip_address>/index.html`.

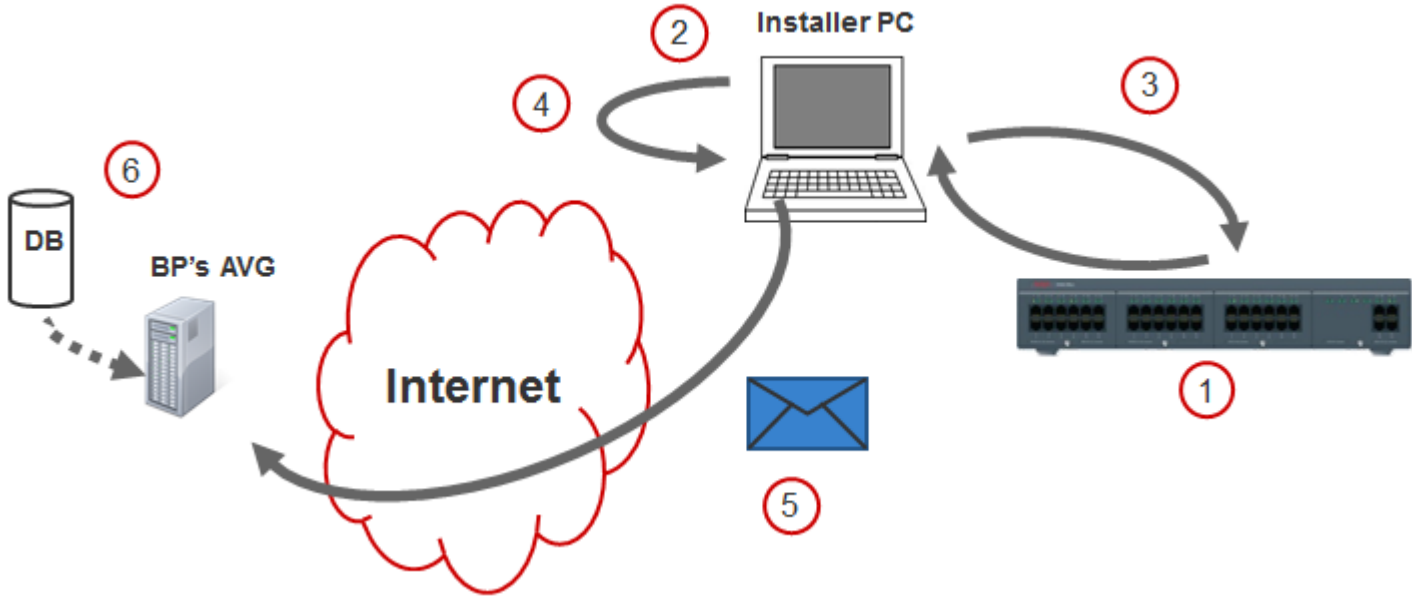
   La page d'index du serveur s'ouvre.
2. Cliquez sur **IP Office Web Manager**.
3. Sur la page de connexion, entrez le nom d'utilisateur et le mot de passe, puis cliquez sur **Connexion**.
4. Sur la page Solution, cliquez sur le menu du serveur à droite du serveur et sélectionnez **On-boarding**.
5. Sur la page On-Boarding, dans le panneau numéro 3, cliquez sur **Rechercher** et recherchez l'emplacement du fichier d'intégration xml.
6. Cliquez sur **Charger**.
7. Vérifiez la connectivité du SSL VPN en utilisant l'application SSA.

Liens connexes

Utilisation de On-boarding SDK à la page 55

Utilisation de On-boarding Express SDK

Processus de configuration de SSL VPN en utilisant le On-boarding Express SDK



1	Configuration des paramètres IP Office suivants. • ID système • Licences • Interfaces LAN • Serveur DNS
2	Exécutez l'outil On-boarding Express SDK.
3	L'outil On-boarding Express SDK échange des fichiers avec IP Office.
4	L'outil On-boarding Express SDK crée un fichier zip qui contient tous les fichiers requis pour l'intégration. Reprenez les étapes 1–3 pour tous les systèmes IP Office.
5	Transférez en toute sécurité les fichiers zippés sur le site partenaire. Par exemple, utilisez un service d'hébergement de fichiers ou un service de stockage sur le cloud pour transférer le fichier.
6	Traitez tous les fichiers d'intégration pour créer un tunnel SSL VPN.

Liens connexes

Configuration d'un Partenaire Avaya SSL VPN en utilisant un SDK à la page 53
Exécution du On-boarding Express SDK à la page 59
Processus Fichiers zip On-boarding Express SDK à la page 59

Exécution du On-boarding Express SDK

Cette procédure fournit des informations sur l'interface utilisateur de la ligne de commande par défaut. Un JAVA API est également fourni pour faciliter la création d'une interface utilisateur alternative. L'interface de ligne de commande par défaut collecte les données utilisées pour créer le fichier de propriétés en tant qu'entrée sur le JAVA API.

Par exemple, une application mobile pourrait être créée sous une forme permettant de collecter les données nécessaires. Puis utiliser le JAVA API qui contacte ensuite l'IP Office qui termine le processus d'enregistrement et crée le fichier zip qui en résulte.

Procédure

1. Modifiez le `default_parameters.txt` fichier.
2. Exécutez le fichier On-boarding Express SDK `sslvpnOnboardingExpress.bat` en utilisant les paramètres de commande appropriées.

   Le On-boarding Express SDK crée un fichier zip qui contient les fichiers requis pour configurer le SSL VPN pour l'IP Office. Le fichier zip est enregistré dans le `sslvpn_OUTPUT` dossier.

Étapes suivantes

Transférez en toute sécurité les fichiers zippés sur le site partenaire. Par exemple, utilisez un service d'hébergement de fichiers ou un service de stockage sur le cloud pour transférer le fichier.

Liens connexes

Utilisation de On-boarding Express SDK à la page 58

Processus Fichiers zip On-boarding Express SDK

Une fois que le fichier zip généré a été transféré au site partenaire, les permissions du tunnel SSL VPN pour l'installation client sont configurées sur AVG, Radius ou LDAP. Une fois cela terminé, le tunnel SSL VPN se connecte avec succès à AVG.

Si vous utilisez un service de stockage partagé sur le cloud, le traitement du fichier zip sur le site Partenaire peut être fait en quelques secondes. Cela permet au programme d'installation de lancer SSA immédiatement après avoir exécuté le script on-boarding express pour vérifier que la connectivité du tunnel SSL VPN fonctionne.

Liens connexes

Utilisation de On-boarding Express SDK à la page 58

Chapitre 8 : Règles NAPT

Utilisez un service SSL VPN et des règles NAPT (Network Address and Port Translation, adresse réseau et traduction de ports) pour établir des sessions de communication à distance avec des périphériques LAN tels qu'un module IP Office UCM. Pour établir la connexion à un périphérique LAN sur le réseau IP Office privé, le fournisseur de services d'assistance démarre une application de communication sur un ordinateur situé sur son site distant et définit les paramètres de configuration suivants pour la session :

- l'adresse IP d'un tunnel SSL VPN ;
- le numéro de port externe du périphérique LAN.

IP Office utilise les règles NAPT pour associer l'adresse IP du tunnel et le numéro de port externe à l'adresse IP et au numéro de port sur le réseau privé.

Liens connexes

Configuration des règles NAPT à la page 60
Suppression d'une règle NAPT à la page 61

Configuration des règles NAPT

Exécutez cette procédure depuis l'interface Manager. Vous pouvez configurer jusqu'à 64 règles.

Lorsque vous configurez une règle NAPT, vous devez sélectionner un type d'application. Les options d'application suivantes sont disponibles :

- Personnalisé
- VMPro
- one-X Portal
- SSH
- TELNET
- RDP (Remote Desktop Protocol)
- Web Control

Vous pouvez utiliser le paramètre **Personnalisé** afin de configurer une règle NAPT pour un nouveau type d'application. Vous pouvez également utiliser le paramètre **Personnalisé** avec un **numéro de port externe** modifié pour ouvrir simultanément deux sessions de communication en utilisant la même application pour établir une connexion au même périphérique LAN. Par

exemple, afin d'activer deux sessions SSH simultanées pour la même adresse IP, les deux règles NAPT ressembleraient à ceci.

Application	Protocole	Numéro de port externe	Adresse IP interne	Numéro de port interne
SSH	TCP	22	192.168.40.1	22
Personnalisé	TCP	221	192.168.40.1	22

Procédure

1. Dans la liste de navigation, sélectionnez **Service**.
2. Dans la liste **Service**, sélectionnez le service SSL VPN à partir duquel vous voulez configurer des règles NAPT.
3. Dans le volet des détails du service, sélectionnez l'onglet **NAPT**.
4. Sous **Application**, ouvrez la liste déroulante et sélectionnez un type d'application.

   Le champ **Protocole** et les champs **Numéro de port** sont automatiquement renseignés avec les valeurs par défaut.
5. (Facultatif) Si vous souhaitez configurer une application de type **Personnalisé**, modifiez le champ **Numéro de port externe**.
6. Pour configurer d'autres règles, répétez les étapes 4 et 5.

Liens connexes

Règles NAPT à la page 60

Suppression d'une règle NAPT

Procédure

Pour supprimer une règle NAPT, utilisez la colonne vide à gauche du tableau. Faites un clic droit sur la cellule vide en regard de la règle à supprimer, puis cliquez sur l'icône de suppression.

Liens connexes

Règles NAPT à la page 60

Chapitre 9 : Vérification de la connexion entre IP Office et AVG

Les procédures répertoriées dans ce chapitre permettent de tester la connexion entre le système IP Office et AVG.

Liens connexes

[Vérification de la connexion à l'aide de SysMonitor](#) à la page 62
[Vérification du déploiement SSL VPN AVG à l'aide de System Status Application](#) à la page 63
[Vérification de la connexion à l'aide d'AVG BBI](#) à la page 63
[Envoi d'une alarme test](#) à la page 64

Vérification de la connexion à l'aide de SysMonitor

Vous pouvez utiliser System Status Application (SSA) pour vous assurer que le tunnel SSL VPN est en service. Démarrez SSA et assurez-vous que les paramètres de configuration du tunnel sont affichés.

Vous pouvez également effectuer les étapes ci-dessous pour utiliser SysMonitor afin de vérifier la connexion SSL VPN entre le système IP Office et AVG.

Procédure

1. Sélectionnez **Démarrer > Programmes > IP Office > Monitor**.

   L'application SysMonitor se connecte au serveur IP Office et affiche un journal système.

2. Sélectionnez les options **Filters > Trace** (Filtres > Suivi) et cliquez sur l'onglet **VPN**.
3. Dans la zone SSL VPN, vérifiez que les options **Session** et **Session State** (État de la session) sont activées. Cliquez sur **OK**.

   Le journal SysMonitor énumère les activités du service SSL VPN sous le nom que vous avez attribué au service.

4. Localisez le nom de service et vérifiez les informations suivantes :

Changement d'état de la session	Quand vous activez le service SSL VPN, l'état de la session passe par les phases suivantes : • résolution du nom de domaine ; • démarrage de la session ; • connexion de l'adresse IP de IP Office à l'adresse IP de la passerelle VPN. Si IP Office n'est pas en mesure de résoudre le nom de domaine, le message d'erreur suivant s'affiche : "DNS failed to resolve host name <x.x.x> and reached MAX retries. Restart session." (La résolution du nom d'hôte <x.x.x> par le DNS a échoué et le nombre maximum de tentatives a été atteint. Redémarrez la session.)

Liens connexes

Vérification de la connexion entre IP Office et AVG à la page 62

Vérification du déploiement SSL VPN AVG à l'aide de System Status Application

Pour tester le déploiement SSL AVG, procédez comme suit.

1. Démarrez IP Office System Status Application (SSA) et assurez-vous que le tunnel SSL VPN est **en service** et que l'**adresse IP du tunnel** est affichée.
2. Envoyez un ping à IP Office à distance. Sur l'ordinateur de l'agent de service, ouvrez une fenêtre de commande et exécutez une commande ping à l'aide de l'adresse IP du tunnel. La commande ping devrait aboutir.

Liens connexes

Vérification de la connexion entre IP Office et AVG à la page 62

Vérification de la connexion à l'aide d'AVG BBI

Procédure

1. Connectez-vous à l'AVG BBI.
2. Dans le panneau de navigation à gauche, développez **Monitor**.
3. Sous **Monitor**, sélectionnez **Utilisateurs**.
4. La colonne **IP source** affiche :
   - l'adresse IP d'IP Office ;

- l'adresse IP du tunnel SSL VPN attribuée à l'utilisateur local.

Liens connexes

Vérification de la connexion entre IP Office et AVG à la page 62

Envoi d'une alarme test

Suivez cette procédure pour envoyer une alarme test à partir de System Status Application (SSA). Cette alarme test vous permet de générer un événement d'erreur.

Préambules

Il est nécessaire de définir une destination pour l'alarme. Quand vous définissez une adresse IP de destination pour l'événement d'erreur, le système s'appuie sur un tableau de routage IP pour déterminer quelle interface servira à envoyer l'événement d'erreur.

Procédure

1. Lancez SSA à l'aide d'une des méthodes suivantes :
   - Lancez SSA à partir du DVD IP Office Admin.
   - Sélectionnez **Démarrer > Programmes > IP Office > System Status**.
   - Depuis Manager ou IP Office Manager for Server Edition, sélectionnez **Fichier > Avancé > System Status**.
2. Sélectionnez **Alarmes > Service** dans la liste de navigation.
3. Cliquez sur le bouton **Alarme test**.

   Le tableau affiche les résultats du test :

Valeur	Description
Date et heure de la dernière erreur	Il s'agit de la date et de l'heure auxquelles l'alarme s'est produite.
Occurrences	Désigne le nombre de fois où l'alarme s'est produite depuis le dernier redémarrage de l'unité de contrôle ou depuis le moment où elle a été effacée la dernière fois.
Description de l'erreur	Les alarmes test affichent le message "Test de l'alarme initié par l'opérateur."

   Si vous avez configuré une destination d'alarme pour une interruption SNMP, l'alarme test génère les informations suivantes :

```
Enterprise: ipoGenTraps
Bindings (8)
Binding #1: ipoGTEventStdSeverity.0 *** (int32) major(4)
Binding #2: ipoGTEventDateTime.0 *** (octets)
Binding #3: ipoGTEventDevID.0 *** (octets)
Binding #4: sysDescr.0 *** (octets)
Binding #5: ipoGTEventReason.0 *** (int32) testAlarm(39)
Binding #6: ipoGTEventData.0 *** (octets)
```

```
Binding #7: ipoGTEventAlarmDescription.0 *** (octets) Operator initiated test
alarm - do not process
Binding #8: ipoGTEventAlarmRemedialAction.0 *** (octets) (zero-length)
```

Liens connexes

[Vérification de la connexion entre IP Office et AVG](#) à la page 62

Chapitre 10 : Surveillance et gestion du système IP Office

Quand le service SSL VPN est connecté, vous pouvez surveiller le système IP Office à distance via le tunnel. Vous pouvez également gérer et mettre à niveau le système IP Office à distance. Le service SSL VPN vous permet d'utiliser des applications lourdes et des applications Web comme si elles étaient directement connectées à une interface LAN locale. Cette section fournit des informations sur les applications prises en charge et sur leur utilisation.

Outils de surveillance

Vous pouvez utiliser les outils suivants pour surveiller à distance le système IP Office :

- System Status Application(SSA) : l'application System Status Application est un outil de diagnostic qui permet de surveiller l'état des systèmes IP Office. SSA signale les événements historiques en temps réels ainsi que les données d'état et de configuration.
- SysMonitor : l'application SysMonitor affiche les informations relatives au fonctionnement du système IP Office. Elle permet de recueillir les informations dans des fichiers journaux en vue de les analyser.

Outils de gestion

Les outils suivants sont conçus pour gérer, mettre à niveau et configurer à distance le système IP Office :

- IP Office Manager : application administrative qui permet de configurer les paramètres système des systèmes IP Office Essential Edition.
  - IP Office Manager for Server Edition : quand vous lancez IP Office Manager, vous pouvez choisir d'ouvrir une configuration à l'aide du mode IP Office Manager for Server Edition. Ce mode vous permet d'administrer les serveurs Server Edition et les systèmes d'expansion.
- IP Office Basic Edition – Web Manager : outil par navigateur qui permet de configurer les paramètres système du système IP Office.

Signalement des erreurs

Le service SSL VPN permet d'envoyer les erreurs système vers un serveur de gestion d'erreurs distant situé au niveau du site du fournisseur de services où est installé AVG. Vous pouvez définir des filtres d'événements qui déterminent les erreurs à signaler et configurer les destinations où les envoyer.

Pour plus d'informations sur le signalement des erreurs, reportez-vous à la section Configuration des notifications d'alarmes à la page 47

Modes de fonctionnement

Les outils disponibles pour la surveillance et la gestion à distance du système IP Office dépendent du mode de fonctionnement utilisé. Le tableau ci-dessous répertorie les outils pris en charge pour chaque mode.

Outils	Mode de fonctionnement			
	Essential Edition	IP Office Server Edition	Système d'expansion Server Edition	Basic Edition
SSA	✔	✔	✔	✔
SysMonitor	✔	✔	✔	✔
Manager(simplifié)	—	—	—	✔
Manager(standard) et IP Office Manager for Server Edition	✔	✔	✔	—
Web Manager	—	—	—	✔
Signalement des erreurs	✔	✔	✔	✔

Liens connexes

Surveillance d'IP Office à distance à l'aide de SSA à la page 67
Surveillance d'IP Office à distance à l'aide de SysMonitor à la page 68
Surveillance à distance de périphériques LAN à l'aide du tunnel SSL VPN à la page 69
Configuration d'IP Office à distance à l'aide de Web Manager à la page 70
Configuration d'IP Office à distance à l'aide de Manager à la page 70
Configuration de systèmes Server Edition à l'aide d'IP Office Manager for Server Edition à la page 71
Configuration de systèmes Server Edition à l'aide de Web Control à la page 73

Surveillance d'IP Office à distance à l'aide de SSA

Suivez cette procédure pour connecter l'application System Status Application (SSA) à IP Office via le tunnel SSL VPN.

Préambules

Le tunnel SSL VPN doit être en service et vous devez vous munir des informations suivantes :

- l'adresse IP du tunnel SSL VPN ;
- le nom d'utilisateur du compte administrateur IP Office ;
- le mot de passe du compte administrateur IP Office.

Procédure

1. Lancez SSA à l'aide d'une des méthodes suivantes :
   - Lancez SSA à partir du DVD IP Office Admin.
   - Sélectionnez **Démarrer > Programmes > IP Office > System Status**.
   - Depuis Manager ou IP Office Manager for Server Edition, sélectionnez **Fichier > Avancé > System Status**.
2. Dans le champ **Adresse IP de l'unité de contrôle**, saisissez l'adresse IP du tunnel SSL VPN.
3. Dans le champ **Nom d'utilisateur**, saisissez le nom d'utilisateur du compte administrateur IP Office.
4. Dans le champ **Mot de passe**, saisissez le mot de passe du compte administrateur IP Office.
5. Cliquez sur **Connexion**.

Liens connexes

Surveillance et gestion du système IP Office à la page 66

Surveillance d’IP Office à distance à l'aide de SysMonitor

Suivez cette procédure pour connecter l'application SysMonitor à IP Office via le tunnel SSL VPN.

Préambules

Le tunnel SSL VPN doit être en service et vous devez vous munir des informations suivantes :

- l'adresse IP du tunnel SSL VPN ;
- le mot de passe du compte administrateur IP Office.

Procédure

1. Sélectionnez **Démarrer > Programmes > IP Office > Monitor**.
2. Cliquez sur l'icône **Sélectionner l'unité**.

   Une boîte de dialogue s'ouvre.
3. Dans le champ **Adresse IP de l'unité de contrôle**, saisissez l'adresse IP du tunnel SSL VPN.

4. Dans le champ **Password** (Mot de passe), saisissez le mot de passe du compte administrateur IP Office.
5. Cliquez sur le bouton de navigation situé en regard du champ **Trace Log Settings Filename** (Suivre le nom de fichier des paramètres du journal) et accédez à l'emplacement où vous avez enregistré le journal de suivi, puis cliquez sur **Open** (Ouvrir).
6. Cliquez sur **OK**.

Liens connexes

Surveillance et gestion du système IP Office à la page 66

Surveillance à distance de périphériques LAN à l'aide du tunnel SSL VPN

La procédure ci-dessous vous permet de vous connecter à un périphérique LAN sur le réseau IP Office via le tunnel SSL VPN en utilisant l'adresse réseau et la traduction de ports (NAPT). Vous pouvez vous connecter à un périphérique LAN à l'aide d'une application de communication pour laquelle une règle NAPT est configurée. Pour plus d'informations sur la configuration des règles NAPT, consultez la section NAPT (Network Address and Port Translation, adresse réseau et traduction de ports) à la page 60.

Préambules

Le tunnel SSL VPN doit être en service et vous devez vous munir des informations suivantes :

- l'adresse IP du tunnel SSL VPN ;
- le numéro de port externe configuré dans la règle NAPT pour le périphérique LAN auquel vous vous connectez.

Procédure

1. Ouvrez l'application de communication que vous utilisez pour vous connecter à un périphérique LAN via le tunnel SSL VPN.
2. Établissez une session de communication à l'aide de l'adresse IP du tunnel SSL VPN et du numéro de port externe du périphérique LAN.

Liens connexes

Surveillance et gestion du système IP Office à la page 66

Configuration d'IP Office à distance à l'aide de Web Manager

Suivez cette procédure pour connecter l'application Web Manager à IP Office via le tunnel SSL VPN.

Pour plus d'informations sur l'utilisation de l'application Web Manager pour configurer le système IP Office, reportez-vous à *Avaya IP Office Basic Edition – Web Manager.*

Préambules

Le tunnel SSL VPN doit être en service et vous devez vous munir des informations suivantes :

- l'adresse IP du tunnel SSL VPN ;
- le nom du compte administrateur IP Office ;
- le mot de passe du compte administrateur IP Office.

Procédure

1. Dans un navigateur, saisissez l'adresse IP pour la gestion Web en respectant le format suivant : `https://10.0.0.1:8443/webmanagement/WebManagement.html`, où *10.0.0.1* correspond à l'adresse IP du tunnel SSL VPN.

   Si le navigateur renvoie un avertissement de sécurité, suivez les paramètres de menu affichés pour poursuivre la connexion.
2. Lorsque le menu de connexion s'affiche, saisissez le nom d'utilisateur et le mot de passe de l'administration système.
3. Cliquez sur **Connexion**.

   La page d'accueil de la gestion Web du système s'affiche.

Liens connexes

Surveillance et gestion du système IP Office à la page 66

Configuration d'IP Office à distance à l'aide de Manager

Vous pouvez utiliser Manager pour administrer le système IP Office à distance via le tunnel SSL VPN. Quand vous utilisez Manager via le tunnel SSL VPN, la détection automatique des systèmes IP Office n'est pas prise en charge. Vous devez configurer l'adresse IP du système auquel vous voulez vous connecter. Suivez cette procédure pour connecter l'application Manager à IP Office via le tunnel SSL VPN.

Pour plus d'informations sur la procédure de configuration de Manager, et sur la manière de l'utiliser pour administrer un système IP Office, reportez-vous à *Avaya IP Office Manager*.

Préambules

Le tunnel SSL VPN doit être en service et vous devez vous munir des informations suivantes :

- l'adresse IP du tunnel SSL VPN ;
- le nom du compte administrateur IP Office ;
- le mot de passe du compte administrateur IP Office.

Procédure

1. Sélectionnez **Démarrer > Programmes > IP Office > Manager**.
2. Cliquez sur l'icône **Ouvrir la configuration à partir d'IP Office**.

   La boîte de dialogue Sélectionner IP Office s'ouvre.
3. Saisissez l'adresse IP du tunnel SSL VPN dans le champ **Adresse de l'unité/de diffusion** et cliquez sur **Actualiser**.
4. Sélectionnez le système IP Office que vous souhaitez configurer et cliquez sur **OK**.

   La boîte de dialogue Connexion utilisateur au service de configuration s'ouvre.
5. Saisissez le nom d'utilisateur du compte administrateur IP Office dans le champ **Nom d'utilisateur du service**, puis saisissez le mot de passe du compte administrateur IP Office dans le champ **Mot de passe de l'utilisateur du service**. Cliquez sur **OK**.

Liens connexes

Surveillance et gestion du système IP Office à la page 66

Configuration de systèmes Server Edition à l'aide d'IP Office Manager for Server Edition

Vous pouvez utiliser IP Office Manager for Server Edition pour administrer à distance les systèmes suivants via le tunnel SSL VPN :

- Server Edition primaire
- Server Edition secondaire
- Système d'expansion Server Edition

Préambules

Le tunnel SSL VPN doit être en service et vous devez vous munir des informations suivantes :

- l'adresse IP du tunnel SSL VPN ;
- le nom du compte administrateur IP Office Manager for Server Edition ;
- le mot de passe du compte administrateur IP Office Manager for Server Edition.

À propos de cette tâche

Pour configurer les systèmes Server Edition à distance, vous devez configurer un service SSL VPN entre AVG et le Server Edition primaire. Il est ensuite possible de modifier la configuration

des systèmes Server Edition qui sont connectés au serveur principal. Vous devez commencer par configurer un service SSL VPN entre chaque système Server Edition et AVG.

Suivez cette procédure pour connecter IP Office Manager for Server Edition à un serveur Server Edition primaire via le tunnel SSL VPN.

Pour plus d'informations sur l'utilisation de IP Office Manager for Server Edition, reportez-vous à *Avaya IP Office Manager*.

Procédure

1. Sélectionnez **Démarrer > Programmes > IP Office > Manager**.
2. Sélectionnez **Fichier > Préférences**.
3. Sélectionnez **Utiliser l'accès à distance pour Multi-Site** et cliquez sur **OK**.
4. Cliquez sur l'icône **Ouvrir la configuration à partir d'IP Office**.

   La boîte de dialogue Sélectionner IP Office s'ouvre.
5. Saisissez l'adresse IP du tunnel SSL VPN dans le champ **Adresse de l'unité/de diffusion** et cliquez sur **Actualiser**.
6. Sélectionnez le système Server Edition que vous souhaitez configurer.

   Lorsque le système Server Edition est sélectionné, l'option Ouvrir avec Server Edition s'affiche et est activée par défaut.
7. Si vous vous connectez à un serveur Server Edition primaire et que vous souhaitez modifier la configuration des systèmes Server Edition qui y sont connectés, sélectionnez **Utiliser l'accès à distance**. Si vous vous connectez directement à un système Server Edition que vous souhaitez configurer, il n'est pas nécessaire de sélectionner cette option.
8. Cliquez sur **OK**.

   La boîte de dialogue Connexion utilisateur au service de configuration s'ouvre.
9. Saisissez le nom d'utilisateur du compte administrateur IP Office Manager for Server Edition dans le champ **Nom d'utilisateur du service**, puis saisissez le mot de passe du compte administrateur IP Office Manager for Server Edition dans le champ **Mot de passe de l'utilisateur du service**. Cliquez sur **OK**.
10. Dans la liste de navigation, sélectionnez **Réseau**.

    L'écran Récapitulatif s'ouvre. Un tableau affiché dans le bas de l'écran répertorie tous les systèmes Server Edition.
11. Sélectionnez le système Server Edition que vous souhaitez configurer.

    L'écran Récapitulatif affiche les informations de configuration relatives au système sélectionné.

Liens connexes

Surveillance et gestion du système IP Office à la page 66

Configuration de systèmes Server Edition à l'aide de Web Control

L'interface Web Control est conçue pour lancer IP Office Manager for Server Edition et administrer les systèmes Server Edition à distance via le tunnel SSL VPN.

Vous pouvez utiliser IP Office Manager for Server Edition pour administrer à distance les systèmes suivants via le tunnel SSL VPN :

- Server Edition primaire
- Server Edition secondaire
- Système d'expansion Server Edition

Préambules

Le tunnel SSL VPN doit être en service et vous devez vous munir des informations suivantes :

- l'adresse IP du tunnel SSL VPN ;
- le nom du compte administrateur Web Control ;
- le mot de passe du compte administrateur Web Control.

À propos de cette tâche

Pour configurer les systèmes Server Edition à distance, vous devez configurer un service SSL VPN entre AVG et le Server Edition primaire. Il est ensuite possible de modifier la configuration des systèmes Server Edition qui sont connectés au serveur principal. Vous devez commencer par configurer un service SSL VPN entre chaque système Server Edition et AVG.

Suivez cette procédure pour lancer IP Office Manager for Server Edition depuis l'interface Web Control et l'utiliser pour se connecter à Server Edition primaire via le tunnel SSL VPN.

Pour plus d'informations sur l'utilisation de IP Office Manager for Server Edition, reportez-vous à *Avaya IP Office Manager*.

Procédure

1. Ouvrez un navigateur et saisissez l'adresse `https://<adresse IP>:7070`, où *<adresse IP>* désigne l'adresse du tunnel SSL VPN configuré pour Server Edition primaire.
2. Saisissez les informations d'identification de l'administrateur dans les champs **Connexion** et **Mot de passe** et cliquez sur **Connexion**.

   L'écran d'accueil s'ouvre et affiche la liste des serveurs Server Edition et des systèmes d'expansion.
3. Cliquez sur **Gérer**.

   IP Office Manager for Server Edition s'ouvre sur l'écran Récapitulatif.
4. Sélectionnez **Fichier > Fermer** pour fermer la configuration.
5. Sélectionnez **Fichier > Préférences**.
6. Sélectionnez **Utiliser l'accès à distance pour Multi-Site** et cliquez sur **OK**.

7. Cliquez sur l'icône **Ouvrir la configuration à partir d'IP Office**.

   La boîte de dialogue Sélectionner IP Office s'ouvre.

8. Saisissez l'adresse IP du tunnel SSL VPN dans le champ **Adresse de l'unité/de diffusion** et cliquez sur **Actualiser**.

9. Sélectionnez le serveur Server Edition.

   Lorsque le système Server Edition est sélectionné, l'option Ouvrir avec Server Edition s'affiche et est activée par défaut.

10. Sélectionnez **Utiliser l'accès à distance** et cliquez sur **OK**.

    La boîte de dialogue Connexion utilisateur au service de configuration s'ouvre.

11. Saisissez le nom d'utilisateur du compte administrateur IP Office Manager for Server Edition dans le champ **Nom d'utilisateur du service**, puis saisissez le mot de passe du compte administrateur IP Office Manager for Server Edition dans le champ **Mot de passe de l'utilisateur du service**. Cliquez sur **OK**.

    IP Office Manager for Server Edition s'ouvre sur l'écran Récapitulatif.

12. Dans le tableau situé au bas de l'écran, sélectionnez le serveur Server Edition primaire.

13. Dans la liste **Ouvrir. . .** située sur côté droit de l'écran, cliquez sur **Configuration**.

    Une arborescence du système s'affiche.

14. Après avoir configuré le système sélectionné et enregistré les modifications, sélectionnez **Réseau** dans la liste de navigation pour revenir à l'écran **Récapitulatif**.

15. Pour configurer un autre système Server Edition connecté au serveur Server Edition primaire, accédez au tableau situé en bas de l'écran Récapitulatif pour le sélectionner.

    L'écran Récapitulatif affiche les informations de configuration relatives au système sélectionné.

Liens connexes

Surveillance et gestion du système IP Office à la page 66

Chapitre 10 : Mise à niveau d'IP Office à distance

Le tunnel SSL VPN permet de mettre à niveau le système IP Office depuis le site du fournisseur de services. Cette fonction est disponible quand vous mettez à niveau un système de version 8.1 vers une version de logiciel plus récente.

Quand vous utilisez Manager via le tunnel SSL VPN, la détection automatique des systèmes IP Office n'est pas prise en charge.

Suivez cette procédure au niveau du site du fournisseur de services, depuis l'interface Manager installée sur le serveur Service Agent. Si vous configurez un système Server Edition, utilisez le mode IP Office Manager for Server Edition.

Préambules

Au niveau du site du fournisseur de services, il est nécessaire d'installer le DVD IP Office Admin contenant la nouvelle version de logiciel sur le PC Service Agent.

Le tunnel SSL VPN doit être en service et vous devez vous munir des informations suivantes :

- l'adresse IP du tunnel SSL VPN ;

Procédure

1. Sélectionnez **Fichier > Préférences > Détection**.
2. Dans le champ **Critères de recherche IP**, saisissez l'adresse IP du tunnel SSL VPN et cliquez sur **OK**.
3. Sélectionnez **Fichier > Avancé > Mettre à niveau**.

   L'assistant de mise à niveau s'ouvre.

   Remarque :

   Si une boîte de dialogue s'ouvre et vous invite à ouvrir un fichier de configuration, cliquez sur Annuler et poursuivez cette étape. Il n'est pas nécessaire d'ouvrir un fichier de configuration avant d'effectuer une mise à niveau.
4. Dans le champ **Adresse de l'unité/de diffusion**, saisissez l'adresse IP du tunnel SSL VPN et cliquez sur **Actualiser**.

   Ne saisissez pas d'adresse de diffusion. Les adresses de diffusion ne sont pas prises en charge pour les mises à niveau à distance via une connexion SSL VPN.

5. Cochez la case en regard du système que vous souhaitez mettre à niveau, puis cliquez sur **Mettre à niveau**.

   Une fois la mise à niveau terminée, IP Office redémarre et le service SSL VPN se reconnecte automatiquement.

Chapitre 11 : Surveillance du service SSL VPN

Outre la surveillance du système IP Office, vous pouvez également surveiller le tunnel SSL VPN. Cette section fournit des informations sur les outils de surveillance disponibles pour le service SSL VPN et sur leur utilisation.

Vous pouvez surveiller le service SSL VPN à l'aide des outils suivants :

- System Status Application(SSA) : l'application System Status Application est un outil de diagnostic qui permet de surveiller l'état du tunnel SSL VPN. SSA signale les événements historiques en temps réels.
- SysMonitor : l'application SysMonitor affiche les informations relatives au fonctionnement du tunnel SSL VPN. Elle permet de recueillir les informations dans des fichiers journaux en vue de les analyser. Utilisez cet outil pour recueillir des informations uniquement lorsqu'elles sont demandées par le personnel du support technique.
- Signalement des erreurs : quand des problèmes surviennent, le service SSL VPN génère des erreurs concernant ses propres composants. Vous pouvez définir des filtres d'événements qui génèrent l'envoi de notifications quand les erreurs concernées se produisent. Vous pouvez également configurer la destination de l'envoi des notifications. Pour plus d'informations sur le processus de définition des filtres d'événements et de configuration des destinations d'alarmes, reportez-vous à la section Configuration des notifications d'alarmes à la page 47.

Liens connexes

Affichage de l'état du tunnel à la page 77
Surveillance des alarmes à l'aide de SSA à la page 80
Résolution des problèmes liés au service SSL VPN à la page 82

Affichage de l'état du tunnel

Suivez cette procédure pour afficher l'état du tunnel SSL VPN à l'aide de System Status Application (SSA).

Procédure

1. Lancez SSA à l'aide d'une des méthodes suivantes :
   - Lancez SSA à partir du DVD IP Office Admin.

- Sélectionnez **Démarrer > Programmes > IP Office > System Status**.
- Depuis Manager, sélectionnez **Fichier > Avancé > System Status**.

2. Sélectionnez **Réseau IP > SSL VPN** dans la liste de navigation.

   Un tableau récapitulatif fournit des informations propres à chaque service SSL VPN configuré.

3. Pour afficher des informations détaillées relatives à un service SSL VPN particulier, mettez le service SSL VPN en surbrillance et cliquez sur **Sélectionner**.

   Un tableau détaillé fournit les informations sur l'état du service SSL VPN sélectionné.

Liens connexes

Surveillance du service SSL VPN à la page 77
Description des champs État du tunnel : tableau récapitulatif à la page 78
Description des champs État du tunnel : tableau détaillé à la page 79

Description des champs État du tunnel : tableau récapitulatif

System Status Application(SSA) affiche les informations récapitulatives suivantes concernant le service SSL VPN :

Valeur	Description
Nom	Nom du service SSL VPN configuré dans IP Office.
État de service	Indique si le service SSL VPN est en service ou affiche l'état Service Remplacement activé.
Dernier temps de connexion	Horodatage de la dernière connexion établie.
Dernier temps de déconnexion	Horodatage de la dernière déconnexion.
Adresse IP du tunnel	Adresse IP du tunnel SSL VPN.
Total des battements de cœur manqués	Nombre cumulé des signaux d'interrogation manqués. Le total est réinitialisé à 0 au redémarrage de IP Office, ou lors de l'annulation de l'approvisionnement du service SSL VPN dans Manager.
Total des entretiens manqués	Les entretiens sont utilisés dans les connexions UDP. UDP n'est pas pris en charge pour le service SSL VPN ; la valeur est définie sur 0.
Point de terminaison TCP local	Adresse TCP IP et numéro de port d'IP Office.
Point de terminaison TCP distant	Adresse publique et numéro de port d'AVG. VIP d'AVG.
Point de terminaison UDP local	UDP n'est pas pris en charge pour le service SSL VPN ; la valeur est définie sur 0.
Point de terminaison UDP distant	UDP n'est pas pris en charge pour le service SSL VPN ; la valeur est définie sur 0.

Liens connexes

Affichage de l'état du tunnel à la page 77

Description des champs État du tunnel : tableau détaillé

System Status Application(SSA) affiche les informations détaillées suivantes concernant le service SSL VPN :

Valeur	Description
Nom du service	Nom du service configuré dans IP Office.
État de service	Indique si le service SSL VPN est en service ou affiche l'état Service Remplacement activé.
Nom du compte	Nom du compte du service SSL VPN. Ce nom de compte permet d'authentifier le service SSL VPN lorsqu'il tente de se connecter à l'aide de AVG.
Adresse du serveur	Adresse du serveur de passerelle VPN au niveau du site du fournisseur de services. L'adresse affichée peut être de type IPv4 ou FQDN (Fully Qualified Domain Name).
Type de serveur	Le service SSL VPN est pris en charge par Avaya VPN Gateway. Le serveur est de type AVG.
Protocole	Le service SSL VPN utilise le protocole TCP pour le transfert de données. Si vous sélectionnez le protocole UDP lorsque vous configurez la connexion, UDP s'affiche dans ce champ mais le service SSL VPN le remplace par TCP.
Date et heure de la dernière connexion	Horodatage de la dernière connexion établie.
Date et heure de la dernière déconnexion	Horodatage de la dernière déconnexion.
Adresse IP du tunnel	Adresse IP du tunnel SSL VPN.
Masque de sous-réseau du tunnel	Masque de sous-réseau du tunnel SSL VPN.
Adresse IP de la passerelle du tunnel	Adresse IP de la passerelle par défaut d'IP Office.
Domaine du tunnel	Adresse de domaine du tunnel.
Adresse TCP IP locale	Adresse TCP IP d'IP Office.
Port TCP local	Port TCP de IP Office. Le numéro de port est dynamique.
Adresse TCP IP distante	Adresse TCP IP du serveur AVG.
Port TCP distant	Le port TCP du serveur AVG. Le numéro de port par défaut est 443.
Adresse IP UDP locale	UDP n'est pas pris en charge pour le service SSL VPN ; la valeur est définie sur 0.
Port UDP local	UDP n'est pas pris en charge pour le service SSL VPN ; la valeur est définie sur 0.

Table continues…

Valeur	Description
Adresse IP UDP distante	UDP n'est pas pris en charge pour le service SSL VPN ; la valeur est définie sur 0.
Port UDP distant	UDP n'est pas pris en charge pour le service SSL VPN ; la valeur est définie sur 0.
DNS primaire	Adresse du serveur DNS principal configuré sur AVG. Cette adresse, fournie à titre d'information, n'est pas utilisée par IP Office.
DNS secondaire	Adresse du serveur DNS secondaire configuré sur AVG. Cette adresse, fournie à titre d'information, n'est pas utilisée par IP Office.
WINS primaire	WINS primaire configuré sur AVG. Cette adresse, fournie à titre d'information, n'est pas utilisée par IP Office.
WINS secondaire	WINS secondaire configuré sur AVG. Cette adresse, fournie à titre d'information, n'est pas utilisée par IP Office.
Total des battements de cœur manqués	Nombre cumulé des signaux d'interrogation manqués. Le total est réinitialisé à 0 au redémarrage de IP Office, ou lors de l'annulation de l'approvisionnement du service SSL VPN dans Manager.
Total des entretiens manqués	Les entretiens sont utilisés dans les connexions UDP. UDP n'est pas pris en charge pour le service SSL VPN ; la valeur est définie sur 0.

Liens connexes

[Affichage de l'état du tunnel](#) à la page 77

Surveillance des alarmes à l'aide de SSA

Suivez cette procédure pour afficher les erreurs système liées au service SSL VPN qui sont signalées dans System Status Application (SSA).

Procédure

1. Lancez SSA à l'aide d'une des méthodes suivantes :
   - Lancez SSA à partir du DVD IP Office Admin.
   - Sélectionnez **Démarrer > Programmes > IP Office > System Status**.
   - Depuis Manager, sélectionnez **Fichier > Avancé > System Status**.
2. Sélectionnez **Alarmes > Service** dans la liste de navigation.

Les erreurs système sont répertoriées dans un tableau. Lorsqu'elles sont liées au service SSL VPN, les erreurs système sont identifiées par le nom du service.

Liens connexes

Surveillance du service SSL VPN à la page 77
Description des alarmes SSA à la page 81

Description des alarmes SSA

Les erreurs système suivantes sont liées au service SSL VPN et sont signalées dans System Status Application (SSA).

Nom	Description
Date et heure de la dernière erreur	Il s'agit de la date et de l'heure auxquelles l'alarme s'est produite.
Occurrences	Désigne le nombre de fois où l'alarme s'est produite depuis le dernier redémarrage de l'unité de contrôle ou depuis le moment où elle a été effacée la dernière fois.

Table continues…

Nom	Description
Description de l'erreur	Les alarmes liées au service SSL VPN génèrent l'affichage des messages d'erreur suivants, suivis par le nom du service SSL VPN : • VPN SSL hors service en raison d'une maintenance planifiée. • VPN SSL hors service en raison de l'inaccessibilité du serveur ou d'un problème de réseau • VPN SSL hors service en raison de l'échec de la négociation de la session TLS. • VPN SSL hors service en raison de l'échec de la renégociation de la clé de session TLS. • VPN SSL hors service en raison d'un manque de ressources sur IP Office. • VPN SSL hors service en raison d'une erreur interne d'IP Office. • VPN SSL hors service en raison d'un trop grand nombre de messages de pulsation manqués. • VPN SSL hors service en raison de l'échec de la résolution du serveur FQDN. • VPN SSL hors service en raison de la détection d'un doublon d'adresse IP sur une autre interface IP Office. • VPN SSL hors service en raison d'un échec d'authentification. • VPN SSL hors service en raison d'une erreur de protocole SOCKS. • VPN SSL hors service en raison du signalement d'une erreur par le serveur.

Liens connexes

Surveillance des alarmes à l'aide de SSA à la page 80

Résolution des problèmes liés au service SSL VPN

Vous pouvez vous servir des informations recueillies par SysMonitor pour résoudre les problèmes de connectivité. SysMonitor recueille des informations utiles pour résoudre les problèmes du service SSL VPN quand il ne parvient pas à se connecter à AVG et que System Status Application (SSA) ne fournit pas suffisamment d'informations pour identifier l'origine de l'échec.

Suivez cette procédure pour recueillir des informations uniquement lorsqu'elles sont demandées par le personnel du support technique.

Procédure

1. Sélectionnez **Démarrer > Programmes > IP Office > Monitor**.

   L'application SysMonitor se connecte au serveur IP Office et affiche un journal système.
2. Sélectionnez les options **Filters > Trace** (Filtres > Suivi) et cliquez sur l'onglet **VPN**.
3. Dans la zone SSL VPN, sélectionnez les filtres spécifiés par le support technique.
4. Cliquez sur **OK**

   Le journal SysMonitor énumère les activités du service SSL VPN sous le nom que vous avez attribué au service.

Liens connexes

[Surveillance du service SSL VPN](#) à la page 77
[Description de la sortie SysMonitor](#) à la page 83

Description de la sortie SysMonitor

Le tableau suivant énumère les filtres que vous pouvez sélectionner dans SysMonitor, et décrit les sorties générées par chaque filtre. Ces informations sont destinées à aider le personnel du support technique lors de la résolution des problèmes liés au service SSL VPN.

Nom	Description
Configuration	Affiche les informations relatives à la date d'ajout, de modification ou de suppression du service SSLVPN.
Session	Affiche les informations relatives à l'état du service SSL VPN, à savoir si le tunnel est en service ou s'il affiche l'état Service Remplacement activé, ou s'il tente de se connecter. Lorsque le service SSL VPN est connecté, ce sont les paramètres du tunnel SSL VPN négocié avec AVG qui s'affichent.
SessionState	Affiche les informations relatives à l'état lorsque survient un événement. Les états définis sont les suivants : Idle (Inactif), Connecting (Connexion en cours), Connected (Connecté), Disconnecting (Déconnexion en cours), WaitingToStart (En attente de démarrage) et NeedsRestart (Redémarrage requis).
Fsm	Utilisé pour les connexions UDP. UDP n'est pas pris en charge pour le service SSL VPN ; aucune sortie n'est générée.
Socks	Affiche les événements de pile SOCKS déclenchés par des messages de signalement.

Table continues…

Nom	Description
SocksState	Affiche les états internes de la pile SOCKS quand SOCKS5 signale que les messages sont traités.
Heartbeat	Affiche les informations relatives à la période d'envoi et de réception des messages d'interrogation.
Keepalive	Utilisé pour les connexions UDP. UDP n'est pas pris en charge pour le service SSL VPN ; aucune sortie n'est générée.
SignalingPktRx	Affiche un flux d'octet de SOCKS signalant la réception de paquets en provenance d'AVG.
SignalingPktTx	Affiche un flux d'octet de SOCKS signalant l'envoi de paquets vers AVG.
DataPktRx	Affiche un sous-ensemble de datagrammes, en commençant par le paquet de données reçu par le tunnel SSL VPN en provenance d'AVG et transféré vers le système IP Office.
DataPktTx	Affiche un sous-ensemble de datagrammes, commençant par le paquet de données envoyé par l'interface du tunnel SSL VPN à AVG.
TunnelInterface	Affiche les informations relatives aux interactions entre l'interface du tunnel SSL VPN et la pile IP IP Office.
TunnelRoutes	Affiche les informations relatives aux tunnels distincts installés dans le tableau de routage IP Office, ou supprimés de ce tableau.

Liens connexes

[Résolution des problèmes liés au service SSL VPN](#) à la page 82

Chapitre 12 : Entretien du service SSL VPN

Cette section décrit les tâches que vous devez exécuter régulièrement une fois que le service SSL VPN est configuré et connecté.

Les informations de cette section vous aident à exécuter les tâches de maintenance suivantes :

- mettre le tunnel hors service, puis le remettre en service ;
- modifier le mot de passe du compte SSL VPN.

Liens connexes

Activation et désactivation du service à la page 85
Réinitialisation du mot de passe à la page 91

Activation et désactivation du service

Après avoir configuré le service SSL VPN, vous pouvez vous servir des interfaces suivantes pour activer ou désactiver le tunnel.

- Manager
- System Status Application(SSA)
- codes de fonction composés sur les téléphones Avaya
- touches programmables des téléphones Avaya pris en charge
- standard automatique configuré sur des systèmes Embedded Voicemail ou Voicemail Pro
- administration basée sur un poste téléphonique parmi les téléphones Avaya pris en charge

Les méthodes disponibles dépendent du mode de fonctionnement utilisé.

Le tableau ci-dessous énumère les méthodes prises en charge dans chaque mode de fonctionnement :

Méthode	Mode de fonctionnement			
	Essential Edition	IP Office Server Edition	Système d'expansion Server Edition	Basic Edition
Manager	✔	✔	✔	—
SSA	✔	✔	✔	—
Codes de fonction composés sur les téléphones Avaya	✔	✔	✔	—
Touches programmables des téléphones Avaya	✔	✔	✔	—
Standard automatique sur des systèmes Embedded Voicemail ou Voicemail Pro	✔	✔	✔	—
Administration basée sur un poste téléphonique	—	—	—	✔

Liens connexes

Entretien du service SSL VPN à la page 85
Activation du service à l'aide de Manager à la page 86
Désactivation du service à l'aide de Manager à la page 87
Activation du service à l'aide de SSA à la page 87
Désactivation du service à l'aide de SSA à la page 88
Activation du service à l'aide d'un code de fonction à la page 88
Désactivation du service à l'aide d'un code de fonction à la page 89
Activation et désactivation du service à l'aide de l'administration basée sur un poste de téléphonique à la page 89
Activation et désactivation du service à l'aide des touches programmables à la page 90

Activation du service à l'aide de Manager

Suivez cette procédure pour activer le service SSL VPN depuis l'interface Manager. Si vous configurez un système Server Edition, utilisez le mode IP Office Manager for Server Edition.

Avant de commencer, le service SSL VPN doit afficher l'état Service Remplacement activé.

Procédure

1. Dans la liste de navigation, cliquez avec le bouton droit de la souris sur **Service**.

   La liste affiche la liste des services configurés sur le système.
2. Sélectionnez le service SSL VPN que vous souhaitez activer.
3. Sous l'onglet **Remplacement,** décochez l'option **Service Remplacement activé**.
4. Cliquez sur **OK**.
5. Cliquez sur l'icône **Enregistrer** pour enregistrer la configuration.

Liens connexes

Activation et désactivation du service à la page 85

Désactivation du service à l'aide de Manager

Suivez cette procédure pour désactiver le service SSL VPN depuis l'interface Manager. Si vous configurez un système Server Edition, utilisez le mode IP Office Manager for Server Edition.

Avant de commencer, le service SSL VPN doit afficher l'état En service.

Procédure

1. Dans la liste de navigation, cliquez avec le bouton droit de la souris sur **Service**.

   La liste affiche la liste des services configurés sur le système.
2. Sélectionnez le service SSL VPN que vous souhaitez désactiver.
3. Sous l'onglet **Remplacement,** cochez l'option **Service Remplacement activé**.
4. Cliquez sur **OK**.
5. Cliquez sur l'icône **Enregistrer** pour enregistrer la configuration.

Liens connexes

Activation et désactivation du service à la page 85

Activation du service à l'aide de SSA

Suivez cette procédure pour activer le service SSL VPN depuis System Status Application (SSA). Avant de commencer, le service SSL VPN doit afficher l'état Service Remplacement activé.

Procédure

1. Lancez SSA à l'aide d'une des méthodes suivantes :
   - Lancez SSA à partir du DVD IP Office Admin.
   - Sélectionnez **Démarrer > Programmes > IP Office > System Status**.
   - Depuis Manager, sélectionnez **Fichier > Avancé > System Status**.
2. Sélectionnez **Réseau IP > SSL VPN** dans la liste de navigation.
3. Sélectionnez dans la liste le service SSL VPN que vous souhaitez activer.

4. Cliquez sur le bouton **Réglé sur En service**.

   L'état devient alors En service.

Liens connexes

Activation et désactivation du service à la page 85

Désactivation du service à l'aide de SSA

Suivez cette procédure pour désactiver le service SSL VPN depuis System Status Application (SSA). Avant de commencer, le service SSL VPN doit afficher l'état En service.

Procédure

1. Lancez SSA à l'aide d'une des méthodes suivantes :
   - Lancez SSA à partir du DVD IP Office Admin.
   - Sélectionnez **Démarrer > Programmes > IP Office > System Status**.
   - Depuis Manager ou IP Office Manager for Server Edition, sélectionnez **Fichier > Avancé > System Status**.
2. Sélectionnez **Réseau IP > SSL VPN** dans la liste de navigation.
3. Sélectionnez dans la liste le service SSL VPN que vous souhaitez activer.
4. Cliquez sur le bouton **Réglé sur Remplacement actif**.

   Une boîte de dialogue de confirmation s'ouvre.
5. Cliquez sur **Oui**.

   Le système génère une alarme pour confirmer que le service SSL VPN est désactivé.
6. Pour afficher l'alarme, sélectionnez **Alarmes > Service** depuis la liste de navigation.

   L'alarme affiche le message suivant : "VPN SSL hors service en raison d'une maintenance planifiée" suivi du nom du service.

Liens connexes

Activation et désactivation du service à la page 85

Activation du service à l'aide d'un code de fonction

Suivez cette procédure pour activer le service SSL VPN en composant un code de fonction sur un téléphone. Avant de commencer, le service SSL VPN doit afficher l'état Service Remplacement activé.

Préambules

Cette fonction est disponible uniquement si l'administrateur système a configuré des codes de fonction sur le système IP Office. Pour plus d'informations, consultez la section Configuration des codes de fonction à la page 43. Avant de commencer, vous devez connaître le numéro que l'administrateur système a configuré dans le code de fonction pour identifier le service SSL VPN.

Procédure

Depuis un téléphone connecté au système IP Office, saisissez ***775x1**, où *x* correspond à une instance du service SSL VPN, dans une plage de 1 à 9. Par exemple, si l'administrateur système a configuré le code de fonction avec le chiffre **1** pour identifier le service SSL VPN, saisissez ***77511**.

La connexion SSL VPN est alors en service.

Liens connexes

Activation et désactivation du service à la page 85

Désactivation du service à l'aide d'un code de fonction

Suivez cette procédure pour désactiver le service SSL VPN en composant un code de fonction sur un téléphone. Avant de commencer, le service SSL VPN doit afficher l'état En service.

Préambules

Cette fonction est disponible uniquement si l'administrateur système a configuré des codes de fonction sur le système IP Office. Pour plus d'informations, consultez la section Configuration des codes de fonction à la page 43. Avant de commencer, vous devez connaître le numéro que l'administrateur système a configuré dans le code de fonction pour identifier le service SSL VPN.

Procédure

Depuis un téléphone connecté au système IP Office, saisissez ***775x0**, où *x* correspond à une instance du service SSL VPN, dans une plage de 1 à 9. Par exemple, si l'administrateur système a configuré le code de fonction avec le chiffre **1** pour identifier le service SSL VPN, saisissez ***77510**.

La connexion SSL VPN affiche alors l'état Service Remplacement activé.

Liens connexes

Activation et désactivation du service à la page 85

Activation et désactivation du service à l'aide de l'administration basée sur un poste de téléphonique

Sur certains modèles de téléphone Avaya, vous pouvez activer et désactiver le service SSL VPN à l'aide de touches programmables. Cette section fournit des informations sur cette fonction et sur les téléphones qui la prennent en charge.

Préambules

Vous devez tout d'abord configurer les droits du terminal système de l'utilisateur avant qu'il puisse accéder à cette fonction. Pour plus d'informations sur la procédure de configuration de ces droits du terminal système, reportez-vous à *IP Office Manager*.

Les téléphones doivent être branchés dans le premier des deux premiers ports de la première carte de la plate-forme IP500 V2.

À propos de cette tâche

Vous pouvez utiliser les touches programmables pour activer et désactiver le service SSL VPN sur les téléphones Avaya suivants :

- Téléphones de bureau ETR 18D et ETR 34D
- Téléphone de bureau numérique 1416
- Téléphone de bureau numérique 1408
- Téléphone de bureau numérique 9504
- Téléphone de bureau numérique 9508
- Téléphones de bureau numérique T7316 et 7316E
- Téléphone de bureau numérique M7310 et M7324

La procédure suivante permet de vous guider pour accéder à la fonction SSL VPN sur ces téléphones. Pour obtenir des informations détaillées sur les options de menu, reportez-vous au guide de l'utilisateur de votre téléphone.

Procédure

1. Les menus dont vous avez besoin pour accéder à la fonction SSL VPN dépendent du modèle de votre téléphone. Appliquez l'une des méthodes ci-dessous pour accéder à la fonction SSL VPN :
   - Sélectionnez **Admin > Administration système > Paramètres système** et faites défiler la liste pour accéder au service SSL VPN.
   - Sélectionnez **Admin > Fonction** et faites-défiler la liste pour accéder au service SSL VPN.
   - Sélectionnez **Admin** et appuyez sur **#775** pour accéder au menu SSL VPN.
2. Appuyez sur la touche programmable appropriée pour activer ou désactiver le service.

Liens connexes

[Activation et désactivation du service](#) à la page 85

Activation et désactivation du service à l'aide des touches programmables

Certains modèles de téléphone Avaya offrent des touches programmables. Ces touches programmables se comportent comme des raccourcis et vous évitent de saisir un code de fonction ou de parcourir les menus depuis l'interface du téléphone pour activer une fonction. Votre administrateur système peut configurer une touche programmable pour activer et désactiver le service SSL VPN.

Si votre administrateur système a configuré une touche programmable sur votre téléphone pour le service SSL VPN, un libellé s'affiche en regard de la touche programmée sur votre téléphone.

Appuyez sur cette touche pour faire basculer l'état du service SSL VPN sur activé (en service) et désactivé (service remplacement activé).

L'état du service SSL VPN s'affiche en regard de la touche du téléphone. L'affichage de l'état dépend du modèle du téléphone. Par exemple, certains téléphones affichent une icône, tandis

que d'autres utilisent des voyants pour indiquer l'état d'une fonction. Quand l'icône s'affiche ou que le voyant s'allume, cela signifie que le service SSL VPN est activé.

Quand vous appuyez sur la touche pour désactiver le service SSL VPN, l'icône ne s'affiche plus et le voyant s'éteint.

Liens connexes

Activation et désactivation du service à la page 85

Réinitialisation du mot de passe

Cette section décrit les différentes méthodes qui permettent de réinitialiser le mot de passe pour le service SSL VPN.

La réinitialisation du mot de passe du service SSL VPN peut s'effectuer de deux manières.

- Vous pouvez modifier le mot de passe dans le fichier d'intégration, puis le réimporter.
- Vous pouvez modifier le mot de passe à l'aide de Manager.

Quelle que soit la méthode, il est nécessaire de modifier également le mot de passe qui est configuré pour le service SSL VPN sur le serveur RADIUS.

Liens connexes

Entretien du service SSL VPN à la page 85
Réinitialisation du mot de passe à l'aide d'un fichier d'intégration à la page 91
Réinitialisation du mot de passe à l'aide de Manager à la page 92

Réinitialisation du mot de passe à l'aide d'un fichier d'intégration

Suivez cette procédure quand vous avez déjà configuré le service SSL VPN sur un système IP Office et que vous avez besoin de modifier le mot de passe du service SSL VPN.

Suivez cette procédure depuis l'interface Avaya IP Office Web Manager au niveau du site client.

Préambules

Vous devez vous munir tout d'abord des informations suivantes :

- le nom du service SSL VPN ;
- le nom de compte utilisé pour authentifier le service SSL VPN lorsqu'il tente de se connecter à l'aide de AVG.

Vous pouvez rechercher le nom du compte et le nom du service SSL VPN à l'aide de l'application System Status Application (SSA). Pour plus d'informations, consultez la section Affichage de l'état du tunnel à la page 77.

Vous devez également réinitialiser le mot de passe du service SSL VPN sur le serveur RADIUS.

Procédure

1. Sélectionnez **Outils > Intégration**.

   La boîte de dialogue Intégration s'ouvre.

2. Cliquez sur **Modifier**.

   Un navigateur s'ouvre ; accédez au site Web Avaya.

3. Connectez-vous au site Web.

   La page Connectivité à distance IP Office / Gestion de mot de passe s'ouvre.

4. Cliquez sur **Existing IP Office SSL VPN Remote Connectivity** (Connectivité à distance SSL VPN IP Office existante).

5. Sélectionnez **Réinitialiser le mot de passe**.

   Le nom du service SSL VPN par défaut s'affiche.

6. Vérifiez que le nom du service affiché correspond au nom du service SSL VPN dont vous souhaitez modifier le mot de passe. Si le nom du service par défaut ne correspond pas, saisissez le nom du service.

7. Saisissez le nom du compte SSL VPN.

8. Cliquez sur **Submit** (Envoyer).

9. Choisissez si vous voulez recevoir le fichier d'intégration mis à jour par courrier électronique, ou si vous voulez le télécharger et suivre les indications qui s'affichent à l'écran.

10. Une fois le fichier téléchargé ou reçu par courrier électronique, enregistrez-le dans votre système local.

11. Accédez à l'emplacement où vous avez enregistré le fichier d'intégration et cliquez sur **Télécharger vers** depuis l'interface Web Manager.

    Un message s'affiche pour confirmer que le fichier d'intégration a été correctement installé.

Étapes suivantes

Après avoir réinitialisé le mot de passe, assurez-vous que le service SSL VPN s'est correctement reconnecté à AVG en suivant la procédure décrite à la section Affichage de l'état du tunnel à la page 77.

Liens connexes

Réinitialisation du mot de passe à la page 91

Réinitialisation du mot de passe à l'aide de Manager

Suivez cette procédure pour modifier le mot de passe du service SSL VPN. Suivez cette procédure depuis l'interface Manager au niveau du site client. Si vous configurez un système Server Edition, utilisez le mode IP Office Manager for Server Edition.

Préambules

Vous devez également réinitialiser le mot de passe du service SSL VPN sur le serveur RADIUS.

Procédure

1. Dans la liste de navigation, sélectionnez **Service**.
2. Sélectionnez le nom du service SSL VPN.
3. Dans l'onglet **Session**, saisissez le nouveau mot de passe pour le compte de service SSL VPN dans le champ **Mot de passe du compte**.
4. Saisissez de nouveau le mot de passe dans le champ **Confirmer le mot de passe**.
5. Cliquez sur **OK**.
6. Cliquez sur l'icône **Enregistrer** pour enregistrer la configuration.

Liens connexes

Réinitialisation du mot de passe à la page 91

Chapitre 13 : Annexe A : Exemple d'assistant d'installation rapide AVG

Pour lancer l'assistant, redémarrez une nouvelle image AVG. Sur la console, lorsque le message `localhost login:` s'affiche, indentifez-vous avec le nom d'utilisateur "admin" et le mot de passe "admin". Le menu de l'assistant s'ouvre. Sélectionnez `new` et suivez les instructions.

Configurez les interfaces AVG

```
localhost login: admin
Password:
Alteon iSD SSL
Hardware platform: 3050-VM
Software version: 10.0.1.0

------------------------------------------------------------
[Setup Menu]
      join        - Join an existing cluster
      new         - Initialize host as a new installation
      boot        - Boot menu
      info        - Information menu
      exit        - Exit  [global command, always available]

>> Setup# new

Setup will guide you through the initial configuration.
```

```
Enter port number for the management interface [1-4]: 1
Enter IP address for this machine (on management interface): 172.16.1.5
Enter network mask [255.255.255.0]:
Enter VLAN tag id (or zero for no VLAN) [0]:
Setup a two armed configuration (yes/no) [yes]:
Enter port number for the traffic interface [1-4]: 2
Enter IP address for this machine (on traffic interface): 10.136.66.195
Enter network mask [255.255.255.0]:
Enter VLAN tag id (or zero for no VLAN) [0]:
Enter default gateway IP address (on the traffic interface): 10.136.66.1
Enter the Management IP (MIP) address: 172.16.1.6
Making sure the MIP does not exist...ok
Trying to contact gateway...ok
```

Configurez le certificat Self-Signed

```
Enter a timezone or 'UTC' or 'select' [select]: UTC
Enter the current date (YYYY-MM-DD) [2014-11-20]:
Enter the current time (HH:MM:SS) [23:54:18]:
Enter NTP server address (or blank to skip):
Enter DNS server address: 198.152.7.12
   Enabled SSH (allow CLI access).
Enter a password for the "admin" user:
Re-enter to confirm:
Run VPN quick setup wizard [yes]:
Enter VPN Portal IP address: 10.136.66.196
   Using VPN device without an Alteon switch.
   Using empty DNS search list.
   Creating HTTP to HTTPS redirect server.
   Enabling HTTPS BBI on port 443.
Use self-signed certificate (yes/no) [yes]:
!!!The combined length of the following parameters may not exceed 225 bytes!!!
Country Name (2 letter code): ca
State or Province Name (full name): on
Locality Name (eg, city): ottawa
Organization Name (eg, company): smec
Organizational Unit Name (eg, section):
Common Name (eg, your name or your server's hostname): testavg
Email Address:
Subject alternative name (blank or comma separated list of
URI:<uri>, DNS:<fqdn>, IP:<ip-address>, otherName:<string>, email:<email-address
>):
Valid for days [2556 (7 years)]:
Key size (512/1024/2048/4096) [2048]:
```

Option 1 : Configurer 'IP Pool local

```
Use RADIUS authentication server (yes/no) [yes]: no
   Using LOCAL authentication.
Enter Lower IP address in pool range: 172.30.0.1
Enter Upper IP address in pool range: 172.30.255.254
Enter Network mask for the pool range [255.255.255.0]: 255.255.0.0
```

Option 2 : Configurer le serveur RADIUS

```
Use RADIUS authentication server (yes/no) [yes]:
Use generic RADIUS server configuration parameters (yes/no) [yes]:
Enter RADIUS server IP address: 172.16.1.2
Enter shared secret:
Re-enter to confirm:
```

Configurer le sous-réseau Service Agent

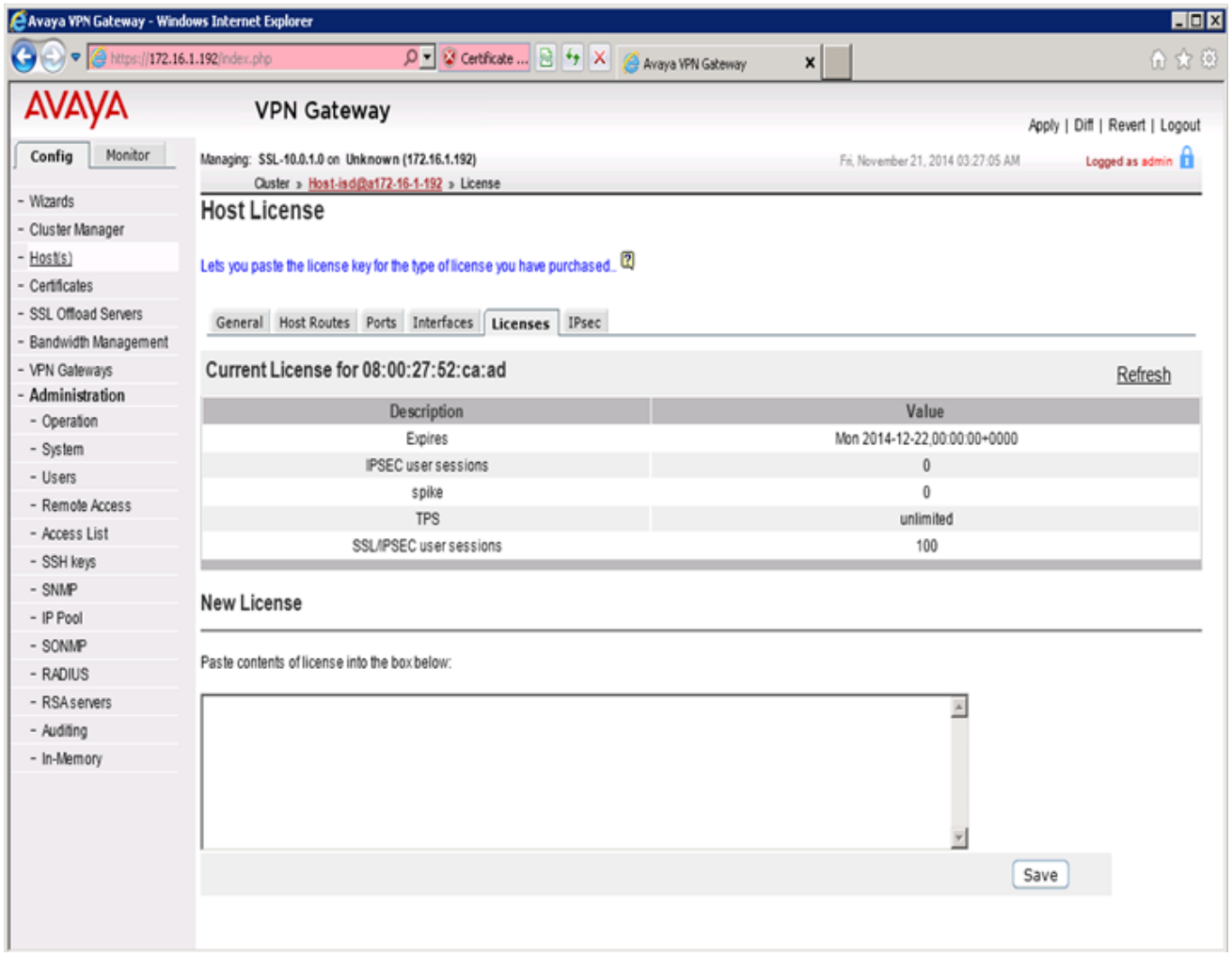
Remarque :

Si le sous-réseau service agent est sur le même sous-réseau que l'interface hôte AVG, par exemple 172,16.1,0 netmask 255,255.255,0, vous recevez un message pour le portail même s'il n'est pas configuré ou utilisé. Si le sous-réseau de l'interface hôte a un portail ar défaut disponible, utilisez l'adresse IP de ce portail (par ex, 172,16.1,1). Sinon, saisissez l'adresse du sous-réseau à nouveau (par ex. : 172,16.1,0).

```
Enter intranet network address: 172.17.1.0
Enter intranet network mask [255.255.255.0]:
Enter intranet gateway: 172.16.1.1
   Enabling network attributes.
   Enabling NetDirect.
   Enabling Split Tunnel Mode.
   Set splittun based on intranet network.
   Added a static route with intranet network.
   Creating empty portal linkset 'base-links'.
   Creating group 'trusted' with secure access.
   Creating network access rule to allow only intranet network for group 'truste
d'.
   Asigning portal linkset 'base-links' to group 'trusted'.
   Creating group 'ipoffice' with secure access.
   Creating network access rule to allow only intranet network for group 'ipoffi
ce'.
   Asigning portal linkset 'base-links' to group 'ipoffice'.
Initializing system.....
```

Ajout de la licence SSL VPN

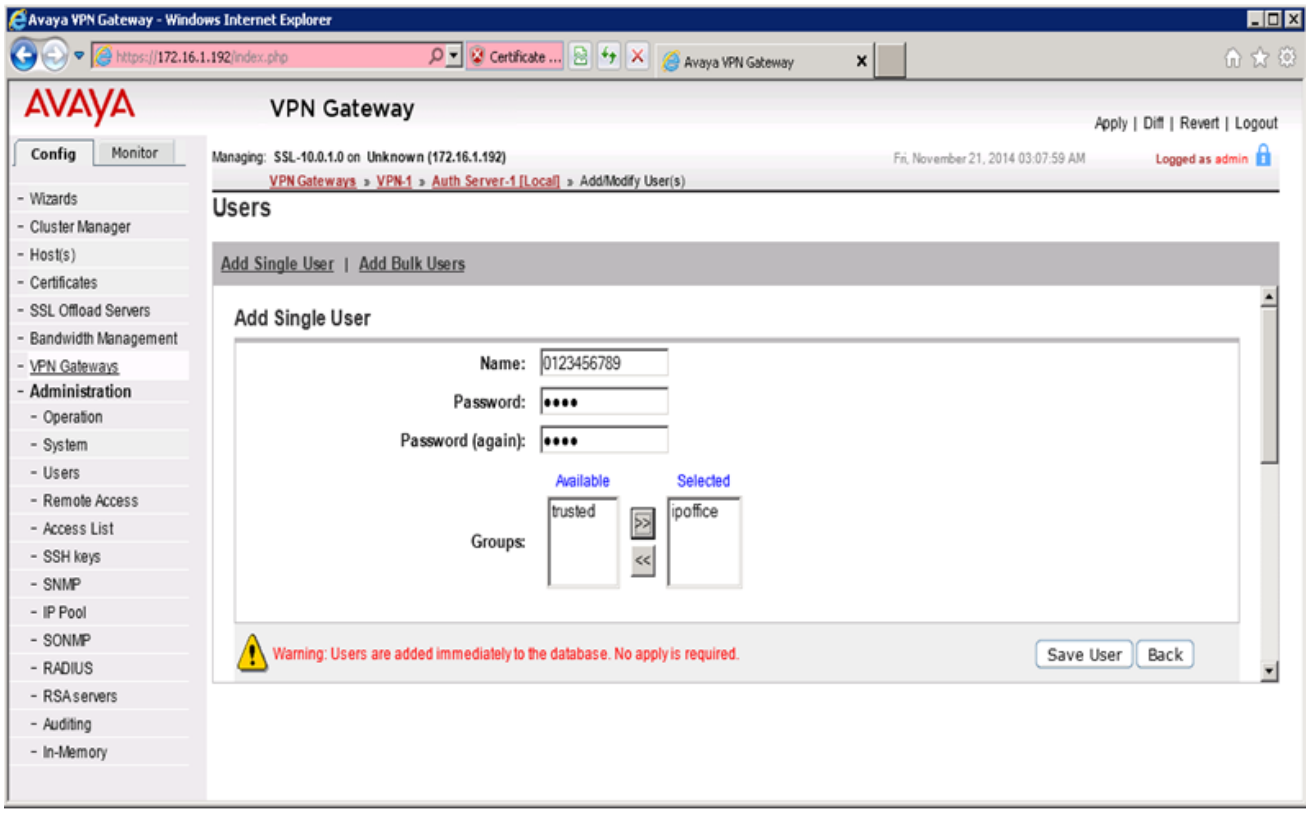
Identifiez-vous sur l'interface AVG pour ajouter une licence.



Ajout d'un utilisateur

La configuration est terminée.

Si vous utilisez l'option 1, configurer l'IP Pool local, vous pouvez maintenant ajouter des utilisateur dans la base de données locale AVG. Les utilisateurs doivent faire partie du groupe **ipoffice**.



Chapitre 14 : Annexe B : Modification de l'AVG par défaut pour SSL VPN (avec captures d'écran)

Une fois les assistants de configuration Installation rapide et Net Direct exécutés, la configuration par défaut doit être modifiée afin de prendre en charge une connexion SSL VPN avec un système IP Office.

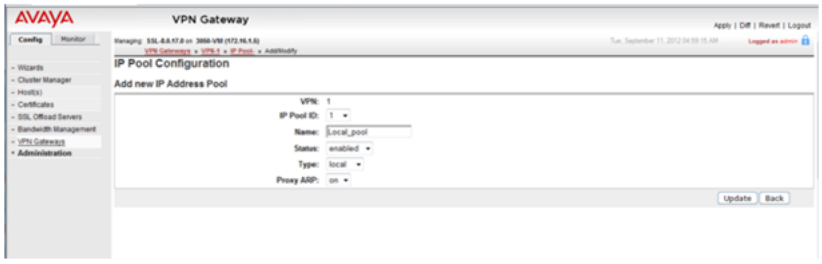
Exécutez cette procédure à l'aide de l'interface d'AVG basée sur le navigateur (BBI). Consultez le document *Avaya VPN Gateway BBI Application Guide* (Guide d'application BBI Avaya VPN Gateway).

Préambules

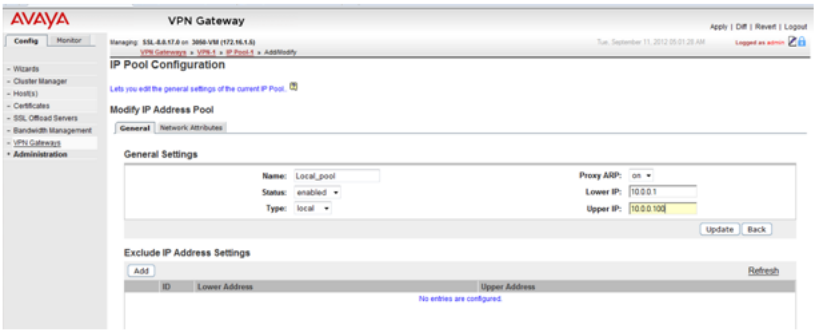
Assurez-vous que la passerelle par défaut configurée sur l'AVG réponde aux requêtes ICMP. Si la passerelle par défaut ne répond pas aux requêtes ICMP, l'AVG ne peut pas fournir de services VPN.

Procédure

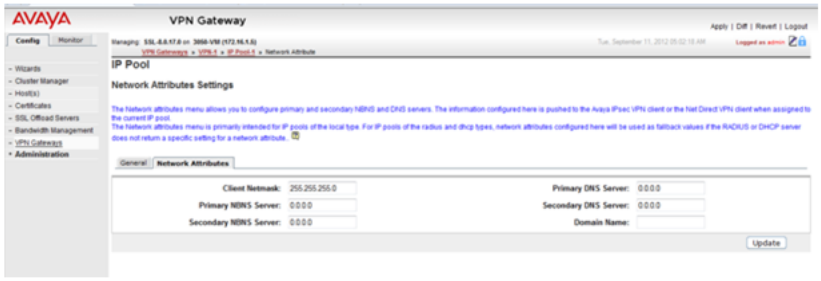
1. Connectez-vous à l'AVG BBI en tant qu'administrateur.
2. Dans le panneau de navigation à gauche, sélectionnez l'onglet **Config**, puis **Passerelle VPN** > **VPN 1** > **Pool IP**.
3. Il est possible que le VPN par défaut de la configuration AVG de base dispose déjà d'un pool local. Si ce n'est pas le cas, vous devez ajouter un pool local au VPN par défaut. Sur la page **Ajouter un nouveau pool d'adresses IP**, ajoutez un pool local au VPN par défaut.



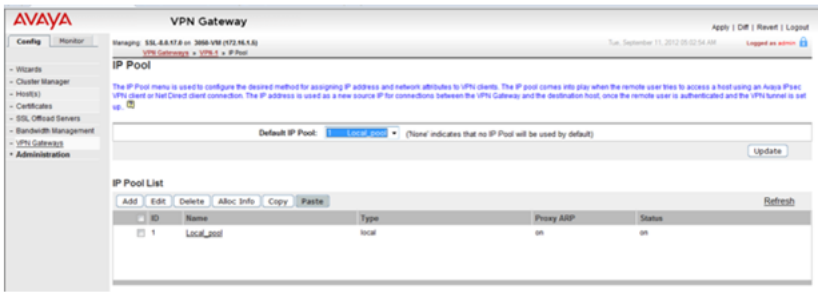
4. Sur la page **Modifier le pool d'adresses IP**, assurez-vous que les valeurs des champs **IP de début** et **IP de fin** correspondent aux valeurs définies via l'assistant de configuration Net Direct.



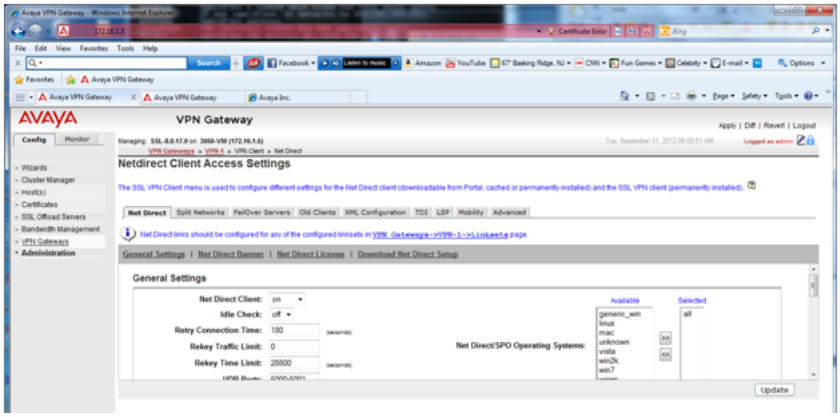
5. Sur la page **Pool IP** > **Paramètres des attributs du réseau**, sélectionnez l'onglet **Attributs du réseau** et saisissez les valeurs correspondant à votre réseau.



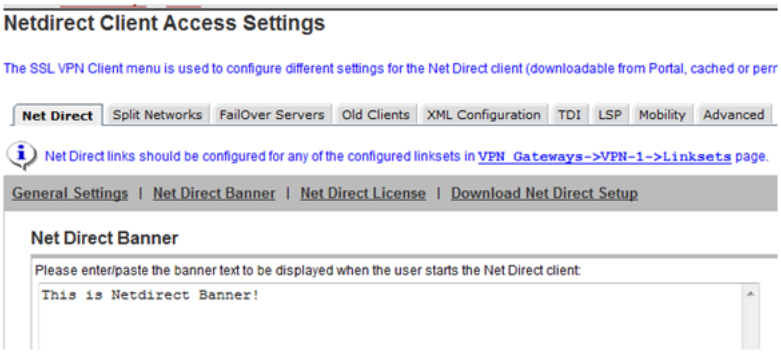
6. Sur la page **Pool IP**, définissez le pool local que vous avez créé à l'étape 3 comme **pool IP par défaut**.



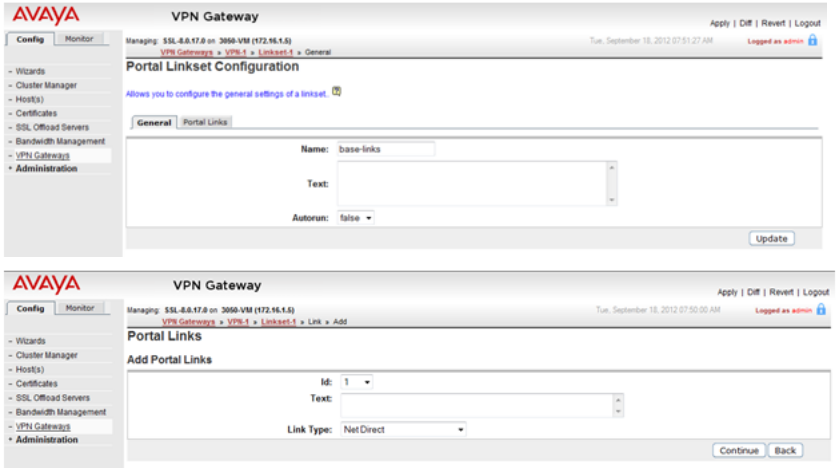
7. Sur la page **Paramètres d'accès du client Net Direct**, vérifiez les paramètres créés via l'assistant de configuration Net Direct.
   a. Assurez-vous que l'option **Vérification d'inactivité** est **désactivée**.



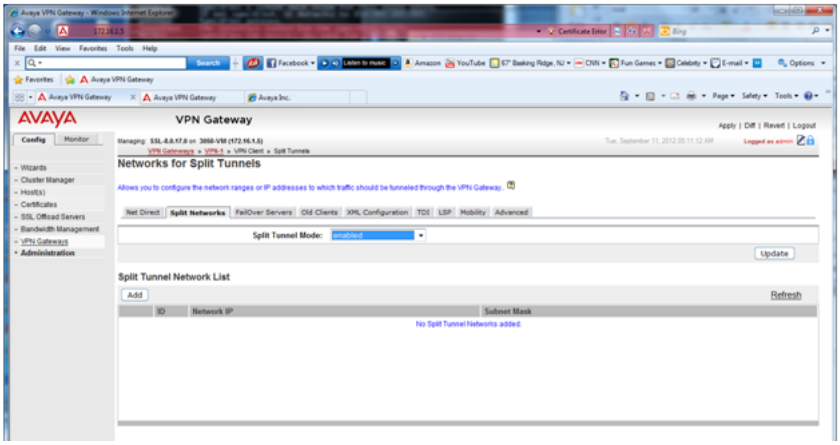
b. Assurez-vous que la bannière Net Direct est définie.



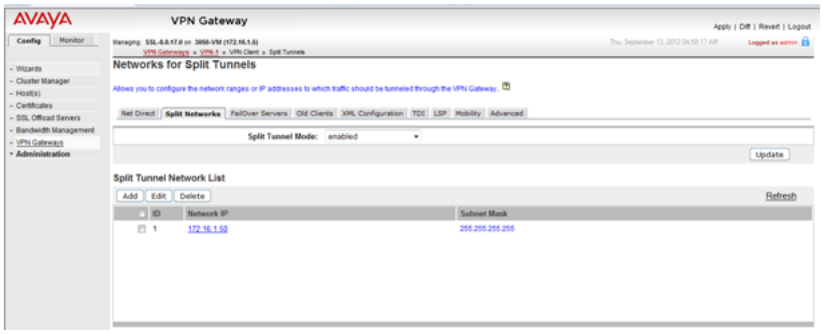
8. Définissez le lien du portail pour qu'il ouvre le client Net Direct. Sur la page **Configuration des liens du portail**, sélectionnez l'onglet **Lien du portail**. Dans le champ **Type de lien**, sélectionnez **Net Direct**.



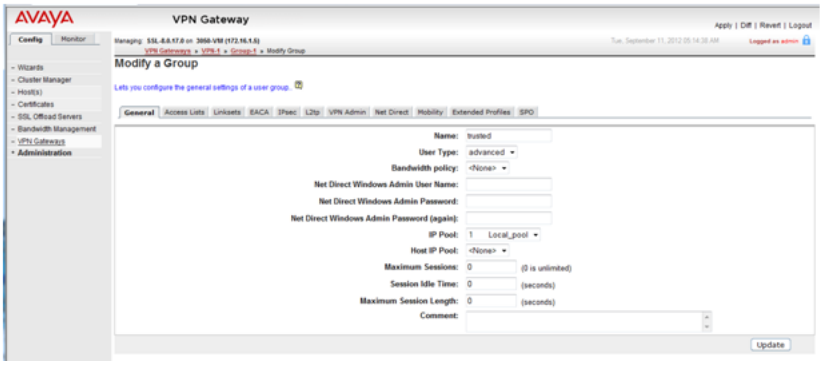
9. Sur la page **Réseaux pour tunnels distincts** :
   a. Définissez **Mode de tunnels distincts** sur **activé**.



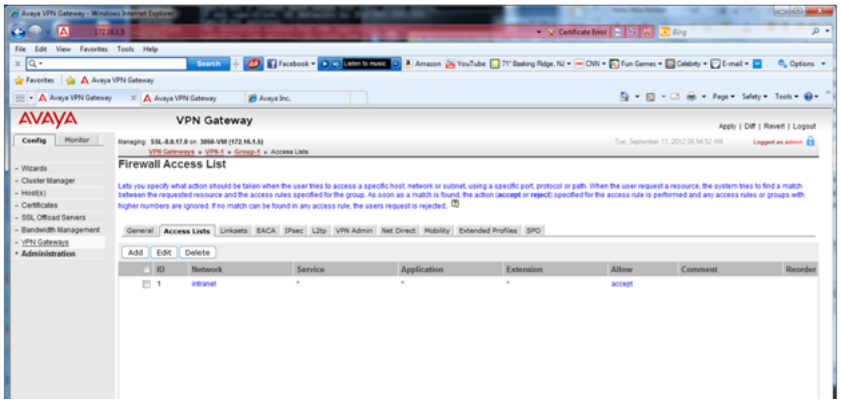
b. Définissez les routes de tunnels distincts pour atteindre l'agent de service sur le réseau privé.



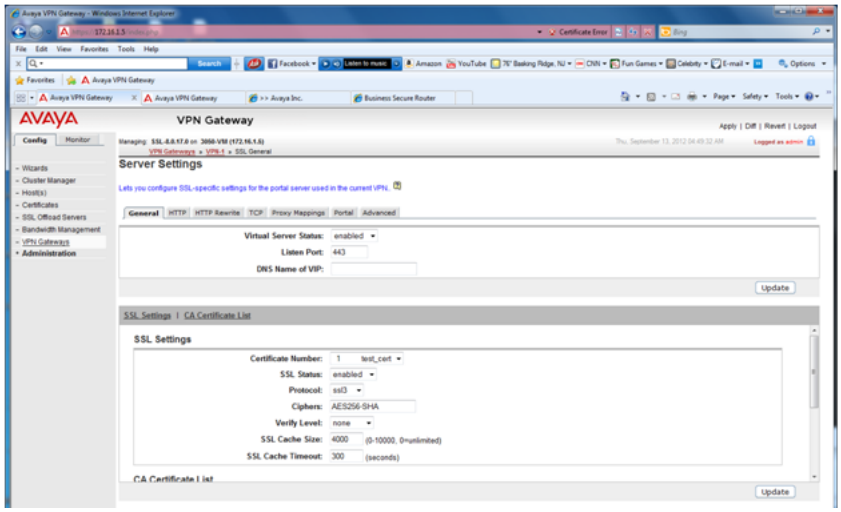
10. Pour VPN 1, ouvrez la page des groupes et sélectionnez **Groupe 1**. Sur la page **Modifier un groupe**, définissez le pool local que vous avez créé à l'étape 3 comme pool IP.



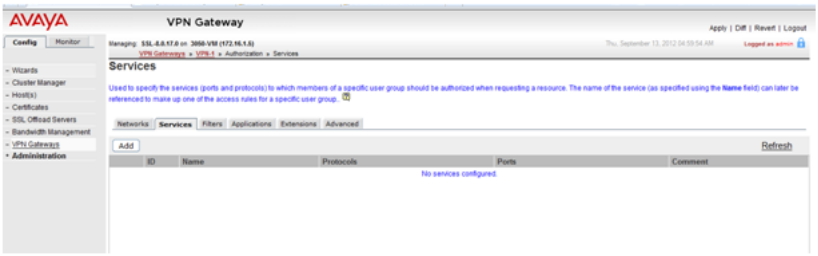
11. Ouvrez la page **VPN 1** > **Groupe 1** > **Listes d'accès**. Sur la page **Liste d'accès de pare-feu**, créez une règle d'accès si elle n'a pas été créée par défaut.



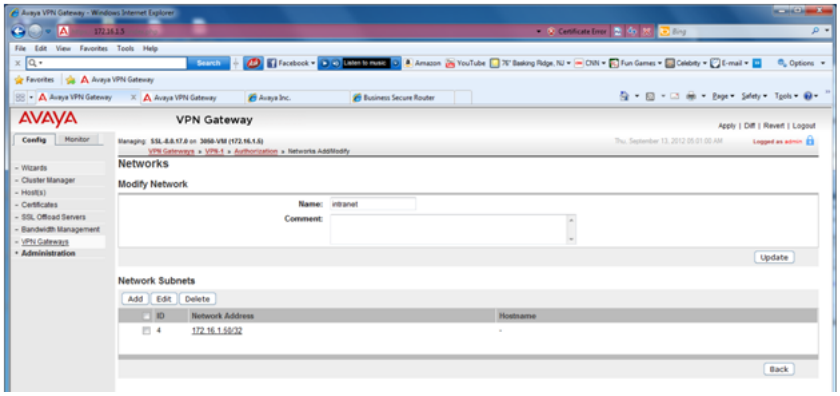
12. Ouvrez la page **VPN 1** > **SSL**. Sur la page **Paramètres du serveur**, sous **Paramètres SSL**, définissez **Chiffrements** sur **AES256-SHA** pour un chiffrement renforcé.



13. Ouvrez la page **VPN 1** > **Autorisation** > **Services**. Supprimez tous les services définis dans la configuration par défaut car ils ne sont pas requis par SSL VPN.



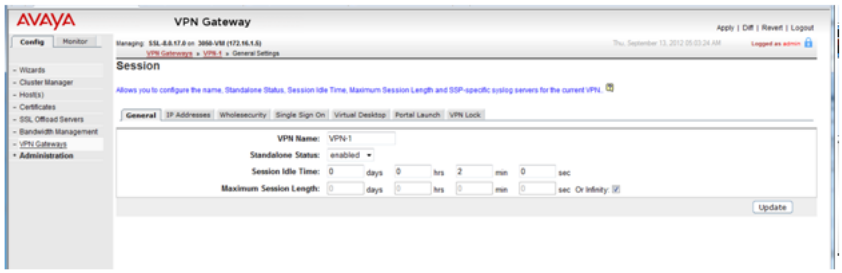
14. Ouvrez la page **VPN 1** > **Autorisation** > **Réseaux**. Définissez le sous-réseau d'autorisation référencé dans l'une des règles d'accès et défini dans **VPN 1** > **Groupe 1** > **Listes d'accès**.



Remarque :

Ce paramètre contrôle la communication entre les tunnels de SSL VPN. La communication est uniquement activée en spécifiant une liste autorisée de réseaux « intranet ». La communication entre clients VPN est bloquée par défaut.

15. Ouvrez la page **VPN 1** > **Paramètres généraux** > **Session**. Définissez la **période d'inactivité de la session** sur 2 minutes.



Chapitre 15 : Annexe C : Configuration de l'authentification RADIUS (avec captures d'écran)

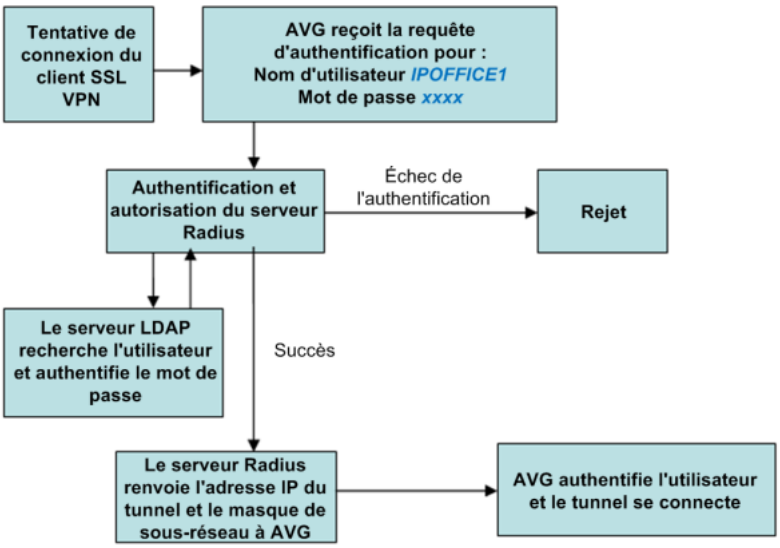
Le principal avantage de l'authentification RADIUS est que le service SSL VPN se voit toujours attribuer la même adresse IP de tunnel.

Pour configurer l'authentification RADIUS, vous devez installer un serveur RADIUS. Pour un serveur RADIUS, Avaya recommande Avaya Identity Engine. Pour obtenir des informations et télécharger le logiciel, rendez-vous à l'adresse http://support.avaya.com.

Les informations sur l'authentification du protocole RADIUS, telles que les informations sur le compte utilisateur, et les informations sur le tunnel SSL VPN, telles que l'adresse IP et le masque de sous-réseau, doivent être stockées dans une base de données. Deux options sont possibles :

- Utiliser la base de données locale d'Identity Engine pour stocker les informations sur l'utilisateur et fournir à la fois les services de recherche et d'authentification et d'autorisation. Cette option peut être utilisée pour un nombre peu élevé d'utilisateurs. Le nombre d'utilisateurs est limité dans Identity Engine. Reportez-vous à la documentation pour connaître le nombre exact.
- Utiliser un serveur LDAP pour stocker les informations d'identification utilisateur et les informations sur le tunnel SSL VPN, à la fois pour les services de recherche et d'authentification. Cette option convient aux déploiements impliquant un nombre élevé d'utilisateurs.

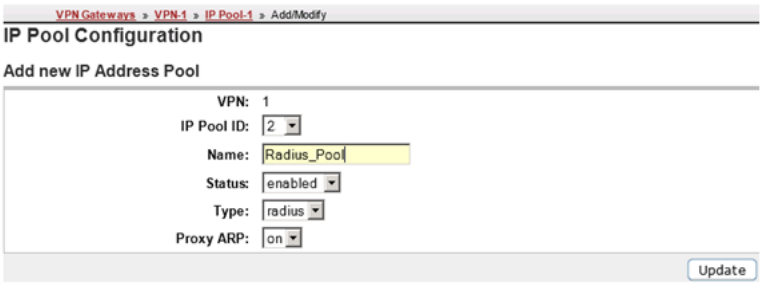
Pour l'installation du serveur LDAP, la documentation Avaya Identity Engine Radius Server contient les options de configuration pour les serveurs LDAP de différents fournisseurs. Le schéma ci-après illustre l'authentification RADIUS avec un serveur LDAP. Notez que dans cette procédure, cette configuration avec un serveur RADIUS ne nécessite pas de serveur LDAP.



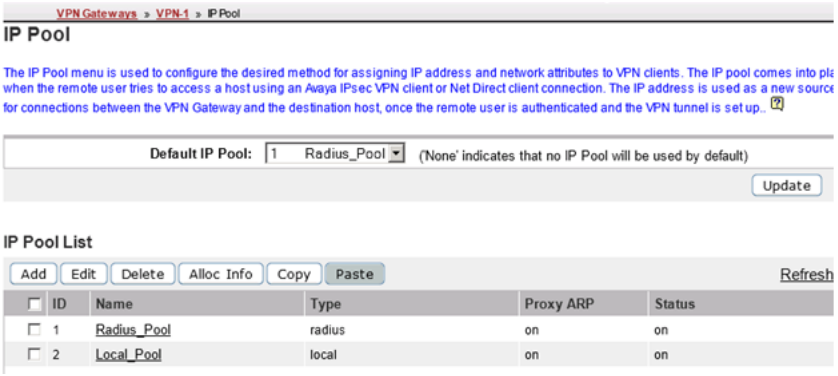
Cette procédure comporte les étapes manuelles permettant de configurer l'authentification RADIUS. Vous pouvez aussi configurer l'authentification à l'aide de l'assistant d'authentification AVG.

Procédure

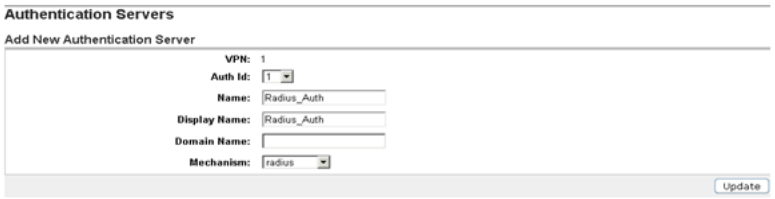
1. Connectez-vous à l'AVG BBI en tant qu'administrateur.
2. Sur la page **Configuration du pool IP**, ajoutez un nouveau pool d'adresses IP pour l'authentification RADIUS.



3. Sur la page **Pool IP**, définissez le pool d'adresses IP de l'authentification RADIUS que vous avez créé à l'étape 2 comme **pool IP par défaut**.

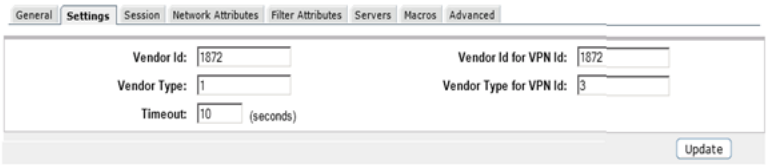


4. Modifiez le VPN. Sur la page **Serveurs d'authentification** > **Ajouter un nouveau serveur d'authentification**, renseignez les champs correspondant au serveur RADIUS.



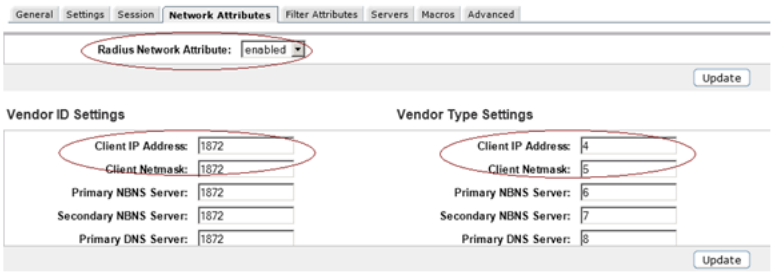
5. Définissez les paramètres du serveur d'authentification RADIUS. Notez que l'ID fournisseur 1872 est associé à Alteon et identifie AVG. Sélectionnez l'onglet **Paramètres** et renseignez les champs suivants.

   - **ID fournisseur : 1872**
   - **Type de fournisseur : 1**
   - **Délai d'expiration : 10**
   - **ID fournisseur pour ID VPN : 1872**
   - **Type de fournisseur pour ID VPN : 3**

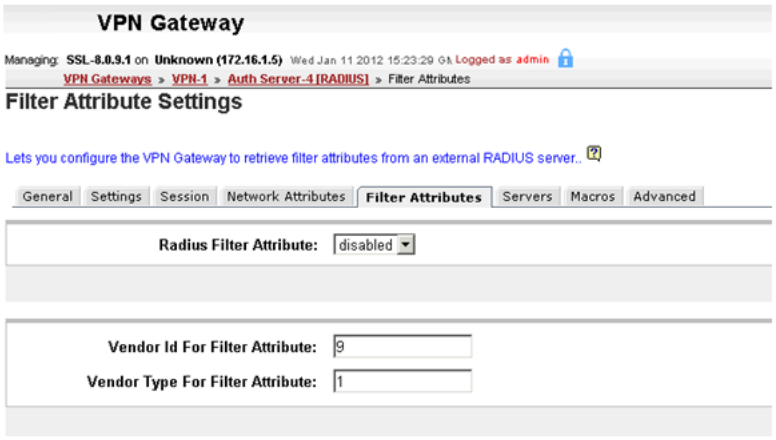


6. Définissez les paramètres du réseau RADIUS. Sélectionnez l'onglet **Attributs du réseau** et renseignez les champs suivants.

Paramètres de l'ID fournisseur	Paramètres du type de fournisseur
Adresse IP du client : 1872	Adresse IP du client : 4
Masque de sous-réseau du client : 1872	Masque de sous-réseau du client : 5
Serveur NBNS principal : 1872	Serveur NBNS principal : 6
Serveur NBNS secondaire : 1872	Serveur NBNS secondaire : 7
Serveur DNS principal : 1872	Serveur DNS principal : 8

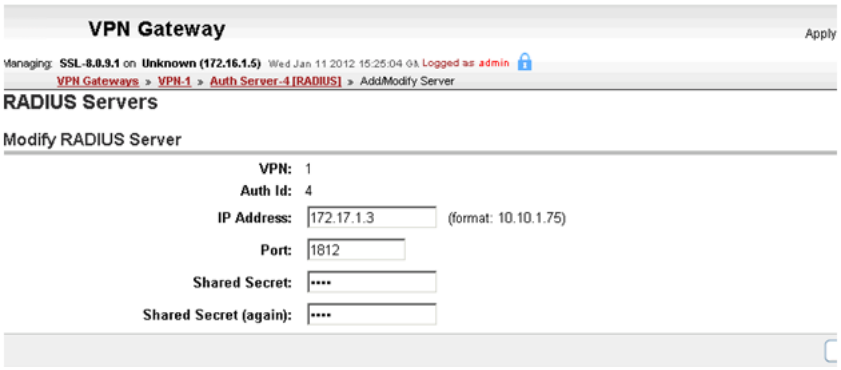


7. Définissez les attributs du filtre. Sélectionnez l'onglet Attributs du filtre et renseignez les champs suivants.
   - **Attribut du filtre Radius : désactivé**
   - **ID fournisseur pour l'attribut du filtre : 9**
   - **Type de fournisseur pour l'attribut du filtre : 1**

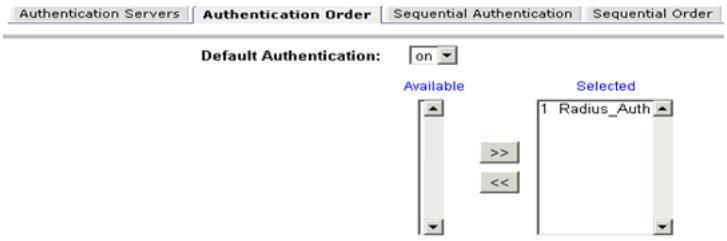


8. Indiquez l'adresse du serveur Radius. Sur la page **Serveurs RADIUS**, sélectionnez l'onglet **Serveurs**.

9. Cliquez sur **Ajouter**. Sur la page **Modifier le serveur RADIUS**, saisissez l'adresse IP et le mot de passe du serveur RADIUS.



10. Sélectionnez l'onglet **Ordre de l'authentification** et indiquez l'ordre préféré des méthodes d'authentification.



Chapitre 16 : Annexe D : Paramètres de configuration AVG

```
[Main Menu]       info       - Information menu       stats      -
Statistics menu       cfg        - Configuration menu       boot
     - Boot menu       maint      - Maintenance menu       diff
    - Show pending config changes   [global command]       apply
    - Apply pending config changes  [global command]       revert
    - Revert pending config changes [global command]       paste
    - Restore saved config with key [global command]       help
    - Show command help             [global command]       exit
    - Exit  [global command, always available]

>> Main# cfg

------------------------------------------------------------
[Configuration Menu]
      ssl        - SSL offload menu
      cert       - Certificate menu
      vpn        - VPN menu
      test       - Create test vpn, portal and certificate
      quick      - Quick vpn setup wizard
      sys        - System-wide parameter menu
      lang       - Language support
      bwm        - Bandwidth management menu
      log        - logging system menu
      ptcfg      - Backup configuration to TFTP/FTP/SCP/SFTP server
      gtcfg      - Restore configuration from TFTP/FTP/SCP/SFTP server
      dump       - Dump configuration on screen for copy-and-paste

>> Configuration# dump
Dump private/secret keys (yes/no) [no]:
Collecting data, please wait...
/*
/*
/* Alteon iSD SSL
/* Configuration dump taken Tue Sep 18 08:40:50 EDT 2012
/* Hardware Platform: 3050-VM
/* Software Version: 8.0.17.0
/* Uptime:  8 days 3 hours 59 minutes
/* IP Address: 172.16.1.4
/* Hardware Address: 00:0c:29:e0:d8:73
/* Disk space:   config         10110  386513  3 %
  user_content   32832  6015488  1 %

/*
/*
/cfg/.
/cfg/ssl/.
/cfg/ssl/server 1/.
        name "Redirect to VPN 1"
        vips 216.13.56.91
```

```
        standalone off
        port "80 (http)"
        rip 0.0.0.0
        rport 81
        type http
        proxy on
        loopback on
        fastfin off
        ena enabled
/cfg/ssl/server 1/trace/.
/cfg/ssl/server 1/ssl/.
        cert 1
        cachesize 4000
        cachettl 5m
        renegotiate legacy
        protocol ssl3
        verify none
        log none
        verifylog none
        ciphers ALL:-EXPORT:-LOW!ADH
        ena disabled
/cfg/ssl/server 1/tcp/.
        cwrite 15m
        ckeep 15m
        swrite 15m
        sconnect 30s
        csendbuf auto
        crecbuf auto
        ssendbuf auto
        srecbuf 6000
/cfg/ssl/server 1/http/.
        httpsredir on
        redirect on
        downstatus unavailable
        securecookie off
        certcard off
        cookieonce off
        sslheader on
        sslxheader off
        sslsidheader off
        addxfor off
        addvia on
        addxisd off
        addfront off
        addbeassl off
        addbeacli off
        addclicert off
        addnostore off
        nocachehdr off
        compress off
        cmsie on
        rhost off
        maxrcount 40
        maxline 16384
        urlobscure off
        sessionhdr off
/cfg/ssl/server 1/http/redirmap/.
/cfg/ssl/server 1/http/dynheader/.
/cfg/ssl/server 1/http/rewrite/.
        paramtag none
        urldeferattr on
        rewrite off
        ciphers HIGH:MEDIUM
        response iSD
        URI "/cgi-bin/weakcipher"
```

```
/cfg/ssl/server 1/http/auth/.
        mode basic
        realm Xnet
        proxy off
        ena disabled
/cfg/ssl/server 1/dns/.
/cfg/ssl/server 1/adv/.
/cfg/ssl/server 1/adv/pool/.
        timeout 15s
        ena disabled
/cfg/ssl/server 1/adv/traflog/.
        protocol bsd
        sysloghost 0.0.0.0
        udpport 514
        priority info
        facility local4
        ena disabled
/cfg/ssl/server 1/adv/loadbalancing/.
        type all
        persistence none
        metric hash
        health auto
        interval 10s
        grace on
        ena disabled
/cfg/ssl/server 1/adv/loadbalancing/script/.
/cfg/ssl/server 1/adv/loadbalancing/remotessl/.
        protocol ssl3
        ciphers ALL
/cfg/ssl/server 1/adv/loadbalancing/remotessl/verify/.
        verify none
/cfg/ssl/server 1/adv/sslconnect/.
        protocol ssl3
        cachemode on
        ciphers EXP-RC4-MD5:ALL!DH
        ena disabled
/cfg/ssl/server 1/adv/sslconnect/verify/.
        verify none
/cfg/cert 1/.
        name test_cert
        cert
-----BEGIN CERTIFICATE-----
MIIEejCCA+OgAwIBAgIJAODDyCE7V9E3MA0GCSqGSIb3DQEBBAUAMIG/MQswCQYD
VQQGEwJVUzETMBEGA1UECBMKQ2FsaWZvcm5pYTEQMA4GA1UEBxMHVGVzdGluZzEo
MCYGA1UEChMfVGVzdCBJbmMuIDEgMDQ6Mzc6MjEgMjAxMi0wOS0xMDESMBAGA1UE
CxMJdGVzdCBkZXB0MSAwHgYDVQQDExd3d3cuZHVtbXlzc2x0ZXN0aW5nLmNvbTEp
MCcGCSqGSIb3DQEJARYadGVzdGVyQGR1bW15c3NsdGVzdGluZy5jb20wHhcNMTIw
OTEwMDgzNzIyWhcNMTMwOTEwMDgzNzIyWjCBvzELMAkGA1UEBhMCVVMxEzARBgNV
BAgTCkNhbGlmb3JuaWExEDAOBgNVBAcTB1Rlc3RpbmcxKDAmBgNVBAoTH1Rlc3Qg
SW5jLiAxIDA0OjM3OjIxIDIwMTItMDktMTAxEjAQBgNVBAsTCXRlc3QgZGVwdDEg
MB4GA1UEAxMXd3d3LmR1bW15c3NsdGVzdGluZy5jb20xKTAnBgkqhkiG9w0BCQEW
GnRlc3RlckBkdW1teXNzbHRlc3RpbmcuY29tMIGfMA0GCSqGSIb3DQEBAQUAA4GN
ADCBiQKBgQCyw80A6VzNwFRpizR9iWJnvZziAgwJZBmI7V2QjtQD+7tMwZA1mNZf
JohYRRS24WGOerGJd3YtAkQHv3yWSo6NiQ5X0Ng8ou4wvg7nlhsqSjeReSn7RUPV
Jl7L45MySiLI5iKWH2j+i1NxLfLbtkqO7+RVAlM3lL4T0Lsjg4RiswIDAQABo4IB
ejCCAXYwDAYDVR0TBAUwAwEB/zARBglghkgBhvhCAQEEBAMCAkQwMgYJYIZIAYb4
QgENBCUWI0FsdGVvbi9Ob3J0ZWwgR2VuZXJhdGVkIENlcnRpZmljYXRlMB0GA1Ud
DgQWBBSGR0w74d4NpcyEeYyLayjiBtRc9DCB9AYDVR0jBIHsMIHpgBSGR0w74d4N
pcyEeYyLayjiBtRc9KGBxaSBwjCBvzELMAkGA1UEBhMCVVMxEzARBgNVBAgTCkNh
bGlmb3JuaWExEDAOBgNVBAcTB1Rlc3RpbmcxKDAmBgNVBAoTH1Rlc3QgSW5jLiAx
IDA0OjM3OjIxIDIwMTItMDktMTAxEjAQBgNVBAsTCXRlc3QgZGVwdDEgMB4GA1UE
AxMXd3d3LmR1bW15c3NsdGVzdGluZy5jb20xKTAnBgkqhkiG9w0BCQEWGnRlc3Rl
ckBkdW1teXNzbHRlc3RpbmcuY29tggkA4MPIITtX0TcwCQYDVR0SBAIwADANBgkq
hkiG9w0BAQQFAAOBgQAMw7vnW4aWgwQZEpjWEYxzRkbAD1+vWYbtdNix9kPtHzWu
e5Fr9c4iuzSHW6cC8natTQc+8iAUNjokBpZ2PT62mENRsNjfj2Ov3/OzXuUYtwkt
```

```
OtOCddd5gM1DL6ovxM4k59VLkDYdn5p0kwknSAGHJyoUjQ3g7XWGAOffJy+Wbw==
-----END CERTIFICATE-----
...
/cfg/cert 1/revoke/.
/cfg/cert 1/revoke/automatic/.
        anonymous false
        interval 1d
        verify off
        ena disabled
/cfg/vpn 1/.
        name VPN-1
        ips 216.13.56.91
        standalone on
        hostippool false
/cfg/vpn 1/aaa/.
        idlettl 2m
        sessionttl infinity
        authorder 1
        defauth on
        defippool 1
/cfg/vpn 1/aaa/tg/.
        ena disabled
        recheck 15m
        action teardown
        details on
        runonce off
        logmode off
        loglevel info
        bypass off
/cfg/vpn 1/aaa/tg/agent/.
        timeout 2s
        minver 0.0.0.0
/cfg/vpn 1/aaa/nap/.
        autorem false
/cfg/vpn 1/aaa/nap/probation/.
        ena false
/cfg/vpn 1/aaa/nap/servers/.
/cfg/vpn 1/aaa/nap/shvs/.
        add 311 128 wshv
        add 40082 0 nshv
/cfg/vpn 1/aaa/nap/wshv/.
        firewall on
        autoupdate on
/cfg/vpn 1/aaa/nap/wshv/virus/.
        enabled false
/cfg/vpn 1/aaa/nap/wshv/spyware/.
        enabled false
/cfg/vpn 1/aaa/nap/wshv/secupdates/.
        enabled false
/cfg/vpn 1/aaa/wholesec/.
        ena false
/cfg/vpn 1/aaa/auth 1/.
        type local
        name local
/cfg/vpn 1/aaa/auth 1/local/.
        pwdage 0
        expirewarn 15
/cfg/vpn 1/aaa/auth 1/adv/.
/cfg/vpn 1/aaa/seqauth/.
        ena false
        copyuser off
        usesecond off
        retries 3
/cfg/vpn 1/aaa/network 1/.
        name intranet
```

```
/cfg/vpn 1/aaa/network 1/subnet 4/.
        net 172.16.1.50
        mask 255.255.255.255
/cfg/vpn 1/aaa/group 1/.
        name trusted
        restrict 0
        usertype advanced
        idlettl 0
        sessionttl 0
        ippool 1
/cfg/vpn 1/aaa/group 1/access 1/.
        network intranet
        service *
        appspec *
        extspec *
        action accept
/cfg/vpn 1/aaa/group 1/linkset/.
        add base-links
/cfg/vpn 1/aaa/group 1/l2tp/.
/cfg/vpn 1/aaa/group 1/ipsec/.
/cfg/vpn 1/aaa/ssodomains/.
/cfg/vpn 1/aaa/ssoheaders/.
/cfg/vpn 1/aaa/radacct/.
        ena false
/cfg/vpn 1/aaa/radacct/servers/.
/cfg/vpn 1/aaa/radacct/vpnattribute/.
        vendorid "1872 (alteon)"
        vendortype 3
/cfg/vpn 1/aaa/adv/.
/cfg/vpn 1/aaa/adv/unmatchgrp/.
        ena disabled
/cfg/vpn 1/server/.
        port "443 (https)"
        loopback on
        fastfin off
        ena enabled
/cfg/vpn 1/server/trace/.
/cfg/vpn 1/server/ssl/.
        cert 1
        cachesize 4000
        cachettl 5m
        renegotiate legacy
        protocol ssl3
        log none
        verifylog none
        ciphers AES256-SHA
        verify none
        ena enabled
/cfg/vpn 1/server/tcp/.
        cwrite 15m
        ckeep 15m
        skeep 2m
        sinterval 1m
        swrite 15m
        sconnect 30s
        csendbuf auto
        crecbuf auto
        ssendbuf auto
        srecbuf 6000
/cfg/vpn 1/server/http/.
        downstatus unavailable
        securecookie on
        certcard off
        cookieonce off
        sslheader off
```

```
        sslxheader off
        sslsidheader off
        addxfor off
        addvia on
        addxisd off
        addclicert off
        addnostore on
        nocachehdr off
        compress off
        allowimage on
        allowdoc off
        allowscript off
        allowica on
        cmsie on
        maxrcount 40
        maxline 16384
        urlobscure off
        sessionhdr off
/cfg/vpn 1/server/http/rewrite/.
        paramtag none
        urldeferattr on
        rewrite off
        ciphers HIGH:MEDIUM
        response iSD
        URI "/cgi-bin/weakcipher"
/cfg/vpn 1/server/proxymap/.
/cfg/vpn 1/server/portal/.
        wipecookies on
        cookiedb on
        resetcookie off
        persistent off
/cfg/vpn 1/server/portal/urlrewrite/.
        rewrite on
        jrewrite on
        cssrewrite on
        gziprewrite on
        ena enabled
/cfg/vpn 1/server/adv/.
/cfg/vpn 1/server/adv/traflog/.
        protocol bsd
        sysloghost 0.0.0.0
        udpport 514
        priority info
        facility local4
        ena disabled
/cfg/vpn 1/server/adv/sslconnect/.
        protocol ssl23
        cachemode on
        ciphers EXP-RC4-MD5:ALL!DH
/cfg/vpn 1/server/adv/sslconnect/verify/.
        verify none
/cfg/vpn 1/l2tp/.
        ena disabled
        cert unset
        authorder mschapv2,pap
        groupmatch true
/cfg/vpn 1/ipsec/.
        ena disabled
        cert unset
        groupmatch true
        groupbind off
/cfg/vpn 1/ipsec/sys/.
/cfg/vpn 1/ipsec/sys/failover/.
        primary 0.0.0.0
        secondary 0.0.0.0
```

```
        tertiary 0.0.0.0
/cfg/vpn 1/ipsec/sys/nat-t/.
        udpport 10001
        portswitch off
        ena false
/cfg/vpn 1/ippool 1/.
        type local
        name Local_pool
        lowerip 10.0.0.1
        upperip 10.0.0.100
        proxyarp on
        ena enabled
/cfg/vpn 1/ippool 1/exclude/.
/cfg/vpn 1/ippool 1/netattr/.
        netmask 255.255.255.0
        primnbns 0.0.0.0
        secnbns 0.0.0.0
        primdns 0.0.0.0
        secdns 0.0.0.0
/cfg/vpn 1/portal/.
        logintext
This is a configurable text.
...
        seclogtext
This is a configurable text.
...
        iconmode fancy
        linktext

...
        linkurl on
        punblock off
        linkcols 2
        linkwidth 100%
        companyname "Avaya Inc."
        smbworkgrp WORKGROUP
        autojre on
        applet on
        wiper on
        rsaauto off
        ieclear on
        citrix off
        clientauth off
        trustsite off
/cfg/vpn 1/portal/colors/.
        color1 #ececec
        color2 #ececec
        color3 #cc0000
        color4 #cc0000
/cfg/vpn 1/portal/content/.
        ena disabled
/cfg/vpn 1/portal/faccess/.
        ena disabled
        ipsecmode native
        contip 0.0.0.0
        portalmsg
From this page you can gain full network access. This
requires that Net Direct is enabled or
that you have either Avaya's IPSEC client (version 4.89 or better)
and/or SSL-VPN (TDI version 1.1 or better) client installed. If the Net Direct
installable client is installed it will be used if Net Direct is enabled.
Note: Your browser must support Java. If not download SUN's
J2SE JRE from
class="white_link" href="javascript:download_jre()">www.java.com.
Remember: You can only access resources on the network as defined by
```

```
your access rights. Contact your network operator if you are
dissatisfied with your current access rights.
...
appletmsg
The quest for full network access has started._The outcome of the quest will be indicated
in the progress bar and console window below.
...
/cfg/vpn 1/portal/lang/.
        setlang en
/cfg/vpn 1/portal/lang/beconv/.
/cfg/vpn 1/portal/whitelist/.
        ena disabled
/cfg/vpn 1/portal/whitelist/domains/.
/cfg/vpn 1/portal/blacklist/.
        ena disabled
/cfg/vpn 1/portal/blacklist/domains/.
/cfg/vpn 1/portal/usertype/.
/cfg/vpn 1/portal/usertype/novice/.
        sysinfo off
/cfg/vpn 1/linkset 1/.
        name base-links
        autorun false
/cfg/vpn 1/linkset 1/link 1/.
        href <netdirect>
        NetdirectFlag off
        type netdirect
/cfg/vpn 1/linkset 1/link 1/netdirect/.
/cfg/vpn 1/vdesktop/.
        ena off
        prelogon off
        always off
        force off
        switch off
        secure off
        persist off
        filesep off
        remdisk off
        print off
        netshare off
        cryptlevel 128
        timeout 5
        conncntrl off
/cfg/vpn 1/vdesktop/mcd/.
        ena disabled
        keylogger off
        scrscrap off
        acntcreate off
/cfg/vpn 1/vdesktop/mcd/vkeyboard/.
        ena disabled
/cfg/vpn 1/sslclient/.
        ippool off
        netdirect on
        caching off
        ndbanner
This is Netdirect Banner!
...
ndlicense
END USER LICENSE AGREEMENT
FOR AVAYA VPN CLIENT
This Software License Agreement ('Agreement') is between you, ('User') and Avaya
Corporation and its subsidiaries and affiliates ('Avaya').  PLEASE READ THE FOLLOWING
CAREFULLY.
BY CLICKING ON THE 'YES' BUTTON OR USING THIS SOFTWARE, YOU ('USER') ARE CONSENTING TO BE
BOUND BY THIS AGREEMENT BETWEEN YOURSELF AND AVAYA.  IF YOU DO NOT AGREE TO BE BOUND BY
THIS AGREEMENT, CLICK 'NO' AND DO NOT USE THIS SOFTWARE.
```

```
LICENSE GRANT: This Agreement shall govern the licensing of Avaya and Avaya licensor's
software and the accompanying user manuals, on line help services, Avaya Web Site and
other instructions (collectively, the 'Software') provided or made available to User.
The Software includes client software, which resides on the computers of User, to access
Sublicensor's networks (the 'Client Software').  The Software provided under this License
is proprietary to Avaya and to third parties from whom Avaya has acquired license
rights.  This Software was licensed in conjunction with the purchase of a 'Avaya VPN
Gateway' or other Avaya VPN device, that will give the User access to the Sublicensor's
purchaser's network and may only be used for this purpose by you.  User is hereby granted
a nonexclusive object code only license to use the Software under the following terms:
- User shall use the Software only in conjunction with the Avaya VPN Gateway or other
Avaya VPN device with which the Software was distributed.
- User may make one copy of the Software only for safekeeping (archives) or backup
purposes.
- User may not modify, translate, adapt, decompile, disassemble, decrypt, extract,
or otherwise reverse engineer or attempt to discover the source code and techniques
incorporated in the Software.  User may not create derivative works based on the Software
or any trade secret or proprietary information of Avaya.
- Title to Software shall not pass to User.
- User shall not provide, or otherwise make available, any Software, in whole or in part,
in any form, to any third party, nor shall User sublicense, rent or lease the Software.
- Upon termination or breach of this Agreement, or in the event that the Avaya device
with which it was distributed is no longer in use, User will immediately cease use of
and destroy all copies of the Software and  return the Software to Avaya or certify as
to such destruction to Avaya that is has been destroyed. Avaya and Third-party owners
from whom Avaya has acquired license rights to material that is incorporated into the
Software shall have the right to enforce the provisions of this Agreement against User.
IN NO EVENT SHALL AVAYA OR ITS  AGENTS, SUPPLIERS, MANUFACTURERS OR DISTRIBUTORS BE
LIABLE FOR ANY DAMAGES WHATSOEVER, INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF
BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION OR DATA, DAMAGES
BASED ON ANY THIRD PARTY CLAIM,  OR, OR ANY OTHER PECUNIARY LOSS ARISING OUT OF THE USE
OR INABILITY TO USE THE SOFTWARE, EVEN IF SUCH PARTY HAS BEEN ADVISED OF THE POSSIBILITY
OF SUCH DAMAGES.  SOME JURISDICTIONS DO NOT ALLOW THESE LIMITATIONS OR EXCLUSIONS AND IN
SUCH EVENT THEY MAY NOT APPLY.
User agrees to comply with all export restrictions regarding the Software, and shall not
export, directly or indirectly, any Software or related technical data or information
without first obtaining any required export licenses or other governmental approvals. THE
SOFTWARE IS PROVIDED 'AS IS' WITHOUT WARRANTY OR CONDITION OF ANY KIND, EITHER EXPRESS
OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY,
FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. THE ENTIRE RISK ARISING OUT OF
USE OR PERFORMANCE OF THE SOFTWARE REMAINS WITH USER.  Avaya is not obligated to User
to provide support of any kind for the Software, and in the event it chooses to do
so, such support is subject to the terms of this Agreement.  Some jurisdictions do not
allow exclusion of implied warranties and, in such event, the above exclusions may not
apply. If User is the United States Government, the following paragraph shall apply:
All Software provided hereunder is commercial computer software and commercial computer
software documentation, as applicable, and in the event Software is licensed for or
on behalf of the United States Government, the respective rights to the Software is
governed by Avaya standard commercial license in accordance with U.S. Federal Regulations
at 48 C.F.R. Sections 12.212 (for non-DoD entities) and  48 C.F.R. 227.7202 (for DoD
entities). Software contains trade secrets and copyrighted material and User agrees to
treat the Software as confidential information using a reasonable standard of care.  User
shall not remove or obscure any copyright, patent, trademark, trade secret, or similar
intellectual property or restricted rights notice within or affixed to any Software and
shall reproduce and affix such notices on any backup copy of software. User may terminate
this Agreement at any time.  Avaya may terminate this Agreement if User fails to comply
with any of its terms.  This Agreement is the complete and exclusive agreement between
the parties hereto regarding its subject matter, and shall be governed solely by the laws
of the state of New York, without regard to its rules governing conflicts of law.
...
          oslist all
        udpports 5000-5001
        rekeytraf 0
        rekeytime 8h
        portalbind on
```

```
        idlecheck off
        keepalive 0
        recncttime 3m
        clampmss on
        splittun enabled
        tdiclient off
        lspclient off
        oldclients false
/cfg/vp
```

Index

R

S

T

V