ASA : Exemple de configuration de tunnel SMART avec ASDM

Contenu

Introduction

Un tunnel intelligent est une connexion entre une application TCP et un site privé, qui utilise une session VPN SSL sans client (basée sur navigateur) avec l'appliance de sécurité comme chemin et l'appliance de sécurité comme serveur proxy. Vous pouvez identifier les applications auxquelles vous souhaitez accorder l'accès au tunnel intelligent et spécifier le chemin local vers chaque application. Pour les applications qui s'exécutent sous Microsoft Windows, vous pouvez également exiger une correspondance du hachage SHA-1 de la somme de contrôle comme condition pour l'octroi d'un accès au tunnel intelligent.

Lotus SameTime et *Microsoft Outlook Express* sont des exemples d'applications auxquelles vous pouvez accorder l'accès au tunnel intelligent.

Selon que l'application est un client ou une application Web, la configuration du tunnel intelligent nécessite l'une des procédures suivantes :

- Créez une ou plusieurs listes de tunnels intelligents des applications clientes, puis affectez la liste aux stratégies de groupe ou aux stratégies d'utilisateur local pour lesquelles vous souhaitez fournir un accès au tunnel intelligent.

- Créez une ou plusieurs entrées de liste de signets qui spécifient les URL des applications Web éligibles à l'accès Smart Tunnel, puis attribuez la liste aux DAP, aux stratégies de groupe ou aux stratégies d'utilisateur local pour lesquels vous souhaitez fournir un accès Smart Tunnel.Vous pouvez également répertorier les applications Web pour lesquelles automatiser l'envoi d'informations d'identification de connexion dans des connexions de tunnel intelligentes sur des sessions VPN SSL sans client.

Ce document suppose que la configuration du client VPN SSL Cisco AnyConnect est déjà effectuée et fonctionne correctement de sorte que la fonctionnalité de tunnel intelligent puisse être configurée sur la configuration existante. Pour plus d'informations sur la configuration du client VPN SSL Cisco AnyConnect, référez-vous à ASA 8.x : Exemple de configuration d'autorisation de la Transmission tunnel partagée pour un client VPN AnyConnect sur le dispositif ASA

Remarque : Assurez-vous que les étapes *4.b à 4.l* décrites dans la section Configuration ASA utilisant ASDM 6.0(2) de la *section ASA 8.x : Allow Split Tunneling for AnyConnect VPN Client on the ASA Configuration Example* n'est pas exécuté afin de configurer la fonctionnalité de tunnel intelligent.

Ce document décrit comment configurer un tunnel intelligent sur des dispositifs de sécurité adaptatifs dédiés de la gamme Cisco ASA 5500.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Appareils de sécurité adaptatifs de la gamme Cisco ASA 5500 qui exécutent le logiciel version 8.0(2)
- PC exécutant Microsoft Vista, Windows XP SP2 ou Windows 2000 Professionnel SP4 avec Microsoft Installer version 3.1
- Cisco Adaptive Security Device Manager (ASDM) version 6.0(2)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Informations générales

Configuration de l'accès au tunnel intelligent

La table Smart Tunnel affiche les listes Smart Tunnel, chacune d'elles identifiant une ou plusieurs applications pouvant bénéficier d'un accès Smart Tunnel et son système d'exploitation associé. Étant donné que chaque stratégie de groupe ou d'utilisateur local prend en charge une liste de tunnels intelligents, vous devez regrouper les applications non basées sur un navigateur pour qu'elles soient prises en charge dans une liste de tunnels intelligents. En suivant la configuration d'une liste, vous pouvez l'affecter à une ou plusieurs stratégies de groupe ou d'utilisateur local.

La fenêtre des tunnels intelligents (**Configuration > Remote Access VPN > Client SSL VPN Access > Portal > Smart Tunnels**) vous permet d'effectuer les procédures suivantes :

- **Ajouter une liste de tunnels intelligents et ajouter des applications à la liste**Complétez ces étapes afin d'ajouter une liste de tunnels intelligents et d'ajouter des applications à la liste :Cliquez sur **Add**.La boîte de dialogue Add Smart Tunnel List s'affiche.Entrez un nom pour la liste, et cliquez sur **Add**.ASDM ouvre la boîte de dialogue Ajouter une entrée de tunnel intelligente, qui vous permet d'affecter les attributs d'un tunnel intelligent à la liste.Après avoir affecté les attributs souhaités pour le tunnel intelligent, cliquez sur **OK**.ASDM affiche ces attributs dans la liste.Répétez ces étapes si nécessaire afin de compléter la liste, puis cliquez sur **OK** dans la boîte de dialogue Ajouter une liste de tunnels intelligents.
- **Modifier une liste de tunnels intelligents**Complétez ces étapes afin de modifier une liste de tunnels intelligents :Double-cliquez sur la liste ou choisissez la liste dans le tableau, puis cliquez sur **Modifier**.Cliquez sur **Ajouter** pour insérer un nouvel ensemble d'attributs de tunnel intelligent dans la liste ou choisissez une entrée dans la liste, puis cliquez sur **Modifier** ou **Supprimer**.
- **Supprimer une liste**Afin de supprimer une liste, choisissez la liste dans le tableau, puis cliquez sur **Supprimer**.
- **Ajouter un signet**Après la configuration et l'affectation d'une liste de tunnels intelligents, vous pouvez rendre un tunnel intelligent facile à utiliser en ajoutant un signet pour le service et en cliquant sur l'option **Activer le tunnel intelligent** dans la boîte de dialogue Ajouter ou modifier le signet.

L'accès Smart Tunnel permet à une application TCP cliente d'utiliser une connexion VPN basée sur navigateur pour se connecter à un service. Il offre les avantages suivants aux utilisateurs, par rapport aux modules externes et à la technologie héritée, le transfert de port :

- Le tunnel intelligent offre de meilleures performances que les plug-ins.
- Contrairement au transfert de port, le tunnel intelligent simplifie l'expérience utilisateur en ne nécessitant pas la connexion utilisateur de l'application locale au port local.
- Contrairement au transfert de port, le tunnel intelligent n'exige pas que les utilisateurs disposent de privilèges d'administrateur.

Exigences, restrictions et limites du tunnel intelligent

Exigences générales et limites

Les conditions générales et les limites du tunnel intelligent sont les suivantes :

- L'hôte distant à l'origine du tunnel intelligent doit exécuter une version 32 bits de Microsoft Windows Vista, Windows XP ou Windows 2000 ; ou Mac OS 10.4 ou 10.5.
- La connexion automatique au tunnel intelligent prend uniquement en charge Microsoft Internet

Explorer sous Windows.
- Le navigateur doit être activé avec Java, Microsoft ActiveX ou les deux.
- Le tunnel intelligent prend uniquement en charge les serveurs proxy placés entre les ordinateurs exécutant Microsoft Windows et l'appliance de sécurité. Le tunnel intelligent utilise la configuration d'Internet Explorer (c'est-à-dire celle destinée à une utilisation à l'échelle du système sous Windows). Si l'ordinateur distant a besoin d'un serveur proxy pour atteindre l'appliance de sécurité, l'URL de la fin de la connexion doit figurer dans la liste des URL exclues des services proxy. Si la configuration du proxy spécifie que le trafic destiné à l'ASA passe par un proxy, tout le trafic du tunnel intelligent passe par le proxy.Dans un scénario d'accès distant basé sur HTTP, un sous-réseau ne fournit parfois pas d'accès utilisateur à la passerelle VPN. Dans ce cas, un proxy placé devant l'ASA pour acheminer le trafic entre le Web et l'emplacement de l'utilisateur final fournit un accès Web. Cependant, seuls les utilisateurs VPN peuvent configurer des proxys placés devant l'ASA. Ce faisant, ils doivent s'assurer que ces proxys prennent en charge la méthode CONNECT. Pour les serveurs proxy qui nécessitent une authentification, le tunnel intelligent prend uniquement en charge le type d'authentification digest de base.
- Lorsque le tunnel intelligent démarre, l'appliance de sécurité envoie tout le trafic du processus du navigateur utilisé par l'utilisateur pour lancer la session sans client. Si l'utilisateur démarre une autre instance du processus du navigateur, il transmet tout le trafic au tunnel. Si le processus du navigateur est identique et que l'appliance de sécurité ne fournit pas l'accès à une URL donnée, l'utilisateur ne peut pas l'ouvrir. Comme solution de contournement, l'utilisateur peut utiliser un navigateur différent de celui utilisé pour établir la session sans client.
- Un basculement dynamique ne conserve pas les connexions de tunnel intelligent. Les utilisateurs doivent se reconnecter après un basculement.

Configuration requise et limites de Windows

Les conditions et limitations suivantes s'appliquent uniquement à Windows :

- Seules les applications Winsock 2 basées sur TCP peuvent accéder à un tunnel intelligent.
- L'appliance de sécurité ne prend pas en charge le proxy Microsoft Outlook Exchange (MAPI). Ni le transfert de port ni le tunnel intelligent ne prennent en charge MAPI. Pour les communications Microsoft Outlook Exchange utilisant le protocole MAPI, les utilisateurs distants doivent utiliser AnyConnect.
- Les utilisateurs de Microsoft Windows Vista qui utilisent le tunnel intelligent ou le transfert de port doivent ajouter l'URL de l'ASA à la zone Site approuvé. Pour accéder à la zone Site approuvé, démarrez Internet Explorer, sélectionnez **Outils > Options Internet**, puis cliquez sur l'onglet **Sécurité**. Les utilisateurs de Vista peuvent également désactiver le mode protégé afin de faciliter l'accès intelligent au tunnel ; Cisco recommande toutefois de ne pas utiliser cette méthode car elle augmente la vulnérabilité aux attaques.

Exigences et limites de Mac OS

Ces exigences et limitations s'appliquent uniquement à Mac OS :

- Safari 3.1.1 ou ultérieur ou Firefox 3.0 ou ultérieur
- Sun JRE 1.5 ou version ultérieure

- Seules les applications démarrées à partir de la page du portail peuvent établir des connexions de tunnel intelligentes. Cette exigence inclut la prise en charge de tunnel intelligent pour Firefox. L'utilisation de Firefox pour démarrer une autre instance de Firefox lors de la première utilisation d'un tunnel intelligent nécessite le profil utilisateur csco_st. Si ce profil utilisateur n'est pas présent, la session invite l'utilisateur à en créer un.
- Les applications utilisant le protocole TCP qui sont liées dynamiquement à la bibliothèque SSL peuvent fonctionner via un tunnel intelligent.
- Le tunnel intelligent ne prend pas en charge ces fonctionnalités et applications sur Mac OS :Services proxyConnexion automatiqueApplications qui utilisent des espaces de noms à deux niveauxApplications basées sur la console, telles que Telnet, SSH et cURLApplications utilisant dlopen ou dlsym pour localiser les appels libsocketApplications liées de manière statique pour localiser les appels libsocket

Configuration

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Ajouter ou modifier une liste de tunnels intelligents

La boîte de dialogue Ajouter une liste de tunnels intelligents vous permet d'ajouter une liste d'entrées de tunnels intelligents à la configuration de l'appliance de sécurité. La boîte de dialogue Modifier la liste de tunnels intelligents vous permet de modifier le contenu de la liste.

Champ

List Name : saisissez un nom unique pour la liste des applications ou programmes. Il n'y a aucune restriction quant au nombre de caractères dans le nom. N'utilisez pas d'espaces. Après la configuration de la liste de tunnels intelligents, le nom de la liste apparaît en regard de l'attribut Liste de tunnels intelligents dans les stratégies de groupe VPN SSL sans client et les stratégies d'utilisateur local. Attribuez un nom qui vous aidera à distinguer son contenu ou sa fonction des autres listes que vous êtes susceptible de configurer.

Ajouter ou modifier une entrée de tunnel intelligent

La boîte de dialogue Ajouter ou modifier une entrée de tunnel dynamique vous permet de spécifier les attributs d'une application dans une liste de tunnels intelligents.

- **ID d'application** : saisissez une chaîne de nom pour l'entrée dans la liste des tunnels intelligents. La chaîne est unique pour le système d'exploitation. En règle générale, il nomme l'application à laquelle l'accès au tunnel intelligent doit être accordé. Afin de prendre en charge plusieurs versions d'une application pour laquelle vous choisissez de spécifier différents chemins ou valeurs de hachage, vous pouvez utiliser cet attribut pour différencier les entrées, en spécifiant le système d'exploitation et le nom et la version de l'application prise en charge par chaque entrée de liste. La chaîne peut contenir jusqu'à 64 caractères.
- **Process Name** : saisissez le nom du fichier ou le chemin d'accès à l'application. La chaîne peut contenir jusqu'à 128 caractèresWindows requiert une correspondance exacte de cette valeur avec le côté droit du chemin d'application sur l'hôte distant pour qualifier l'application

pour l'accès intelligent au tunnel. Si vous spécifiez uniquement le nom de fichier pour Windows, le VPN SSL n'applique pas de restriction d'emplacement sur l'hôte distant pour qualifier l'application pour l'accès au tunnel intelligent.Si vous spécifiez un chemin d'accès et que l'utilisateur a installé l'application dans un autre emplacement, cette application n'est pas éligible. L'application peut résider sur n'importe quel chemin tant que le côté droit de la chaîne correspond à la valeur que vous entrez.Afin d'autoriser une application pour l'accès au tunnel intelligent si elle est présente sur l'un des chemins de l'hôte distant, spécifiez uniquement le nom et l'extension de l'application dans ce champ ou créez une entrée de tunnel intelligent unique pour chaque chemin.Pour Windows, si vous voulez ajouter l'accès Smart Tunnel à une application démarrée à partir de l'invite de commandes, vous devez spécifier « cmd.exe » dans le nom de processus d'une entrée de la liste Smart Tunnel et spécifier le chemin d'accès à l'application elle-même dans une autre entrée car « cmd.exe » est le parent de l'application.Mac OS nécessite le chemin complet du processus et respecte la casse. Afin d'éviter de spécifier un chemin pour chaque nom d'utilisateur, insérez un tilde (~) avant le chemin partiel (par exemple, ~/bin/vnc).

- **OS** : cliquez sur Windows ou Mac afin de spécifier le système d'exploitation hôte de l'application.
- **Hash** —(*Facultatif et applicable uniquement pour Windows*) Afin d'obtenir cette valeur, entrez la somme de contrôle du fichier exécutable dans un utilitaire qui calcule un hash à l'aide de l'algorithme SHA-1. Un exemple de cet utilitaire est le Vérificateur d'intégrité de la somme de contrôle des fichiers (FCIV) de Microsoft, disponible à la disponibilité et à la description de l'utilitaire Vérificateur d'intégrité de la somme de contrôle des fichiers. Après avoir installé FCIV, placez une copie temporaire de l'application à hacher sur un chemin qui ne contient aucun espace (par exemple, c : /fciv.exe), puis entrez l'application fciv.exe -sha1 sur la ligne de commande (par exemple, fciv.exe -sha1 c:\msimn.exe) pour afficher le hachage SHA-1.Le hachage SHA-1 comporte toujours 40 caractères hexadécimaux.Avant d'autoriser une application pour l'accès au tunnel intelligent, le VPN SSL sans client calcule le hachage de l'application correspondant à l'ID de l'application. Il qualifie l'application pour l'accès au tunnel intelligent si le résultat correspond à la valeur du hachage.La saisie d'un hachage fournit une assurance raisonnable que le VPN SSL ne qualifie pas un fichier illégitime qui correspond à la chaîne que vous avez spécifiée dans l'ID de l'application. Comme la somme de contrôle varie selon la version ou le correctif d'une application, le hachage que vous entrez ne peut correspondre qu'à une seule version ou à un seul correctif sur l'hôte distant. Afin de spécifier un hachage pour plusieurs versions d'une application, créez une entrée de tunnel intelligent unique pour chaque valeur de hachage.**Remarque :** Vous devez mettre à jour la liste des tunnels intelligents à l'avenir si vous entrez des valeurs de hachage et que vous voulez prendre en charge les versions futures ou les correctifs d'une application avec accès aux tunnels intelligents. Un problème soudain lié à l'accès au tunnel intelligent peut indiquer que l'application qui contient des valeurs de hachage n'est pas à jour avec une mise à niveau d'application. Vous pouvez éviter ce problème en ne saisissant pas de hachage.
- Une fois que vous avez configuré la liste de tunnels intelligents, vous devez l'affecter à une stratégie de groupe ou d'utilisateur local pour qu'elle devienne active de la manière suivante :Afin d'affecter la liste à une stratégie de groupe, choisissez **Config > Remote Access VPN > Client SSL VPN Access > Group Policies > Add or Edit > Portal**, puis choisissez le nom du tunnel intelligent dans la liste déroulante en regard de l'attribut Smart Tunnel List.Afin d'affecter la liste à une stratégie d'utilisateur local, choisissez **Config > Remote Access VPN > AAA Setup > Local Users > Add or Edit > VPN Policy > Clientless SSL VPN**, puis choisissez le nom du tunnel intelligent dans la liste déroulante en regard de l'attribut Smart Tunnel List.

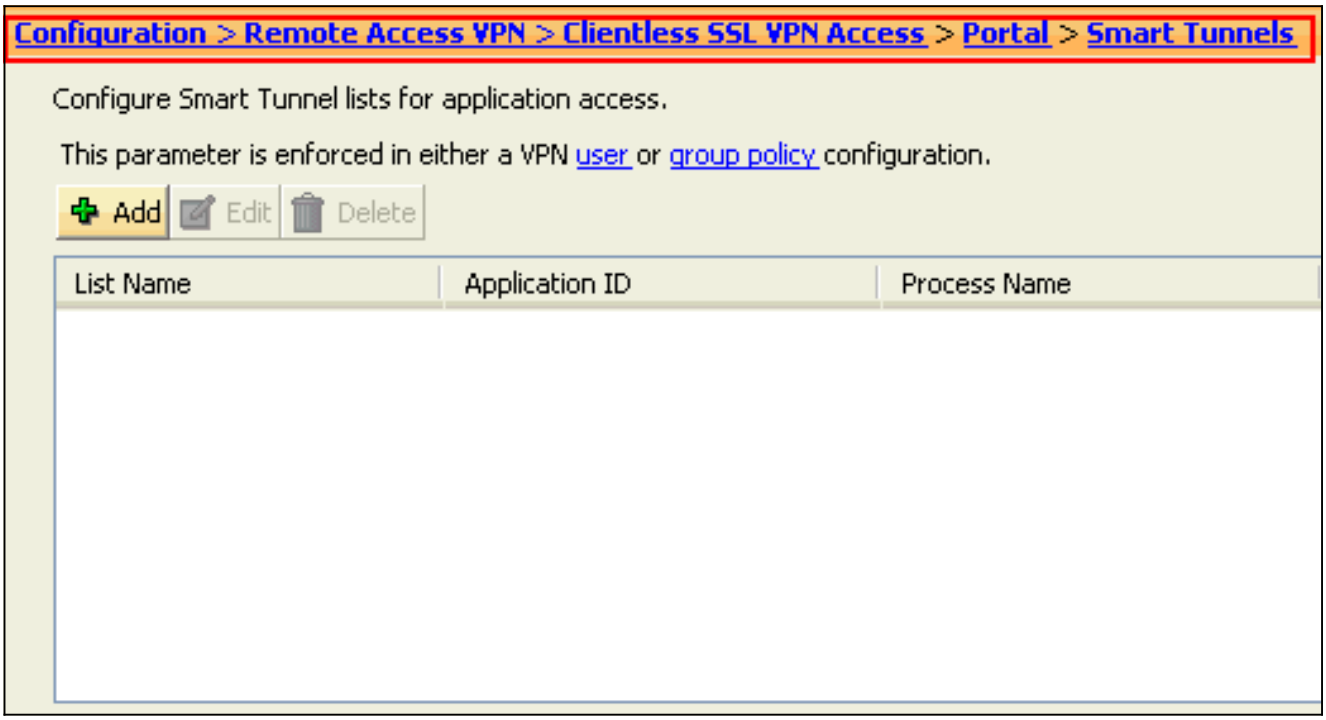
Configuration du tunnel intelligent ASA (exemple Lotus) à l'aide de ASDM 6.0(2)

Ce document suppose que la configuration de base, telle que la configuration d'interface, est terminée et fonctionne correctement.

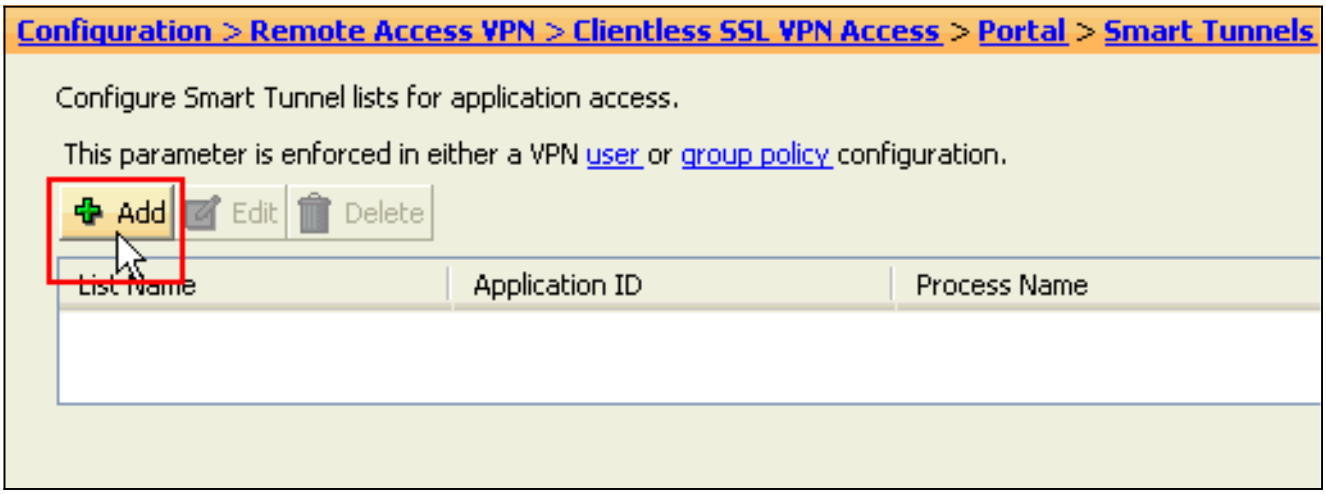
Complétez ces étapes afin de configurer un tunnel intelligent :

Remarque : Dans cet exemple de configuration, le tunnel intelligent est configuré pour l'application Lotus.

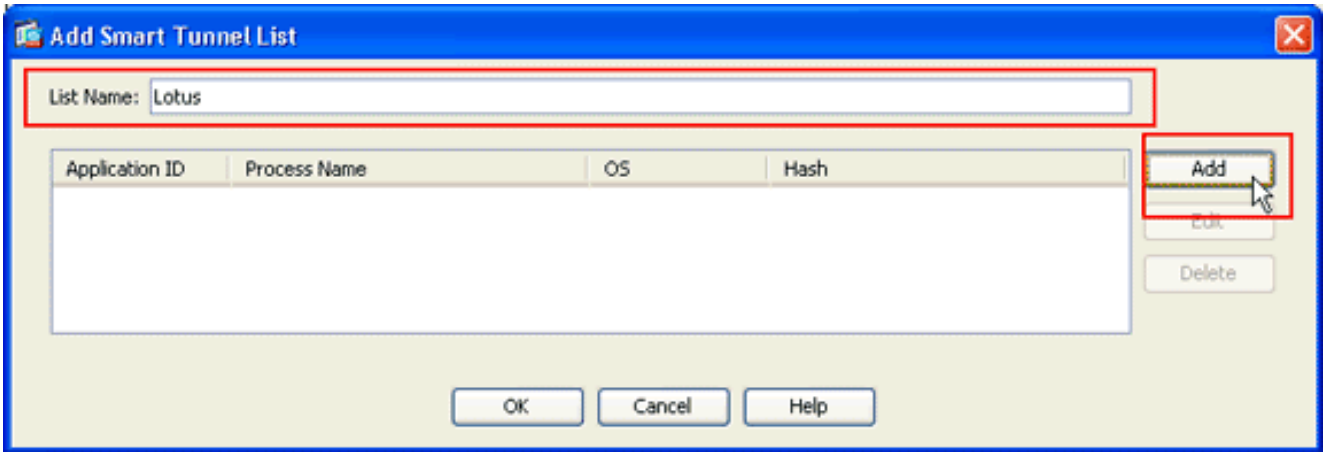
1. Choisissez **Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Smart Tunnels** afin de démarrer la configuration Smart Tunnel.



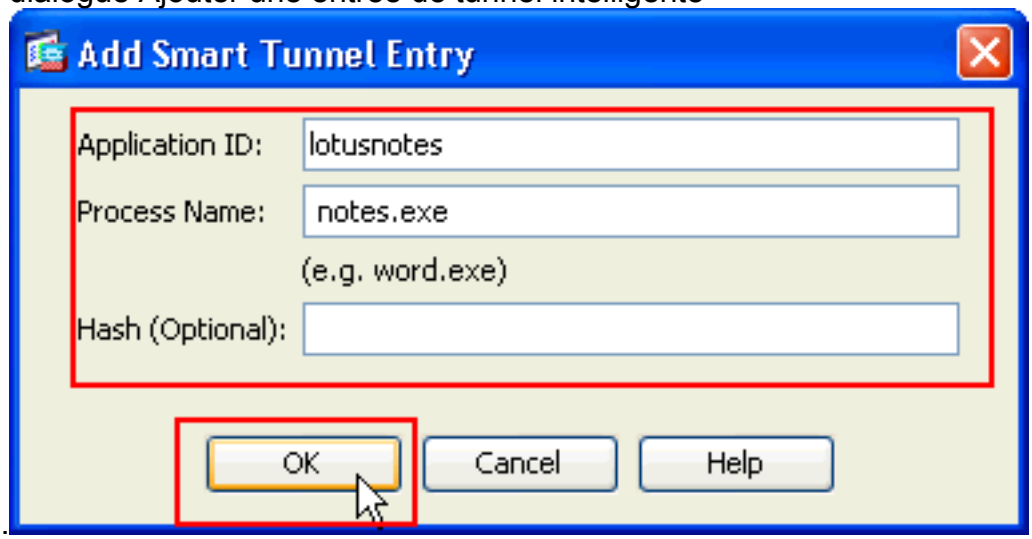
2. Cliquez sur **Add**.



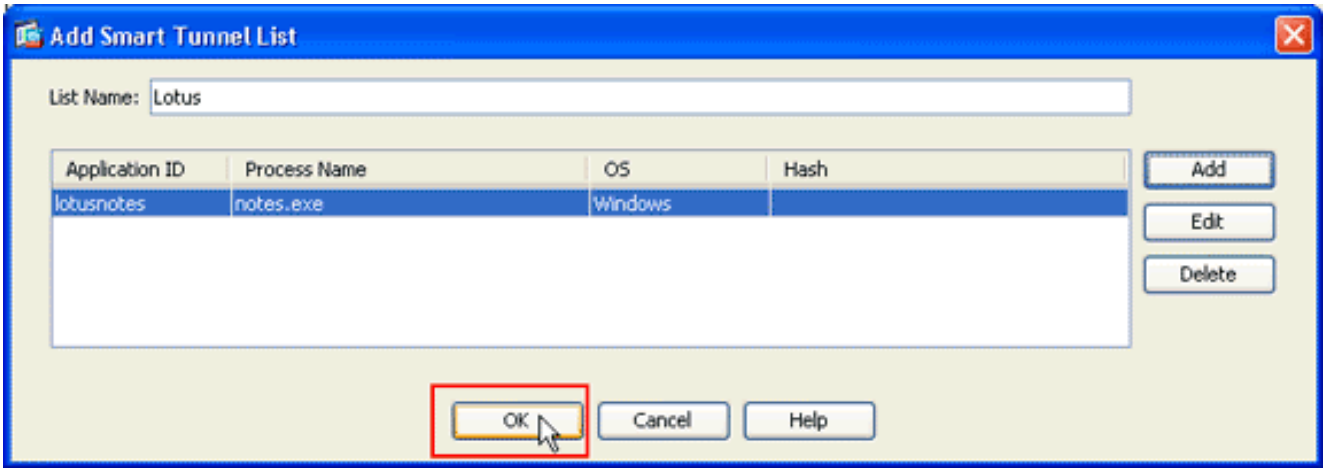
La boîte de dialogue Add Smart Tunnel List s'affiche.



3. Dans la boîte de dialogue Ajouter une liste de tunnels intelligents, cliquez sur **Ajouter**.La boîte de dialogue Ajouter une entrée de tunnel intelligente s'affiche.

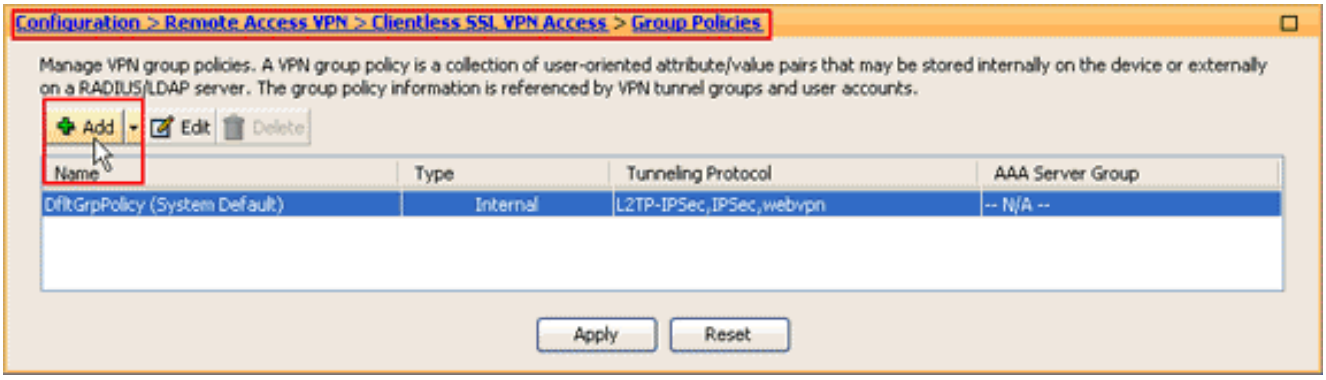


4. Dans le champ ID d'application, entrez une chaîne pour identifier l'entrée dans la liste de tunnels intelligents.
5. Entrez un nom de fichier et une extension pour l'application, puis cliquez sur **OK**.
6. Dans la boîte de dialogue Ajouter une liste de tunnels intelligents, cliquez sur **OK**.

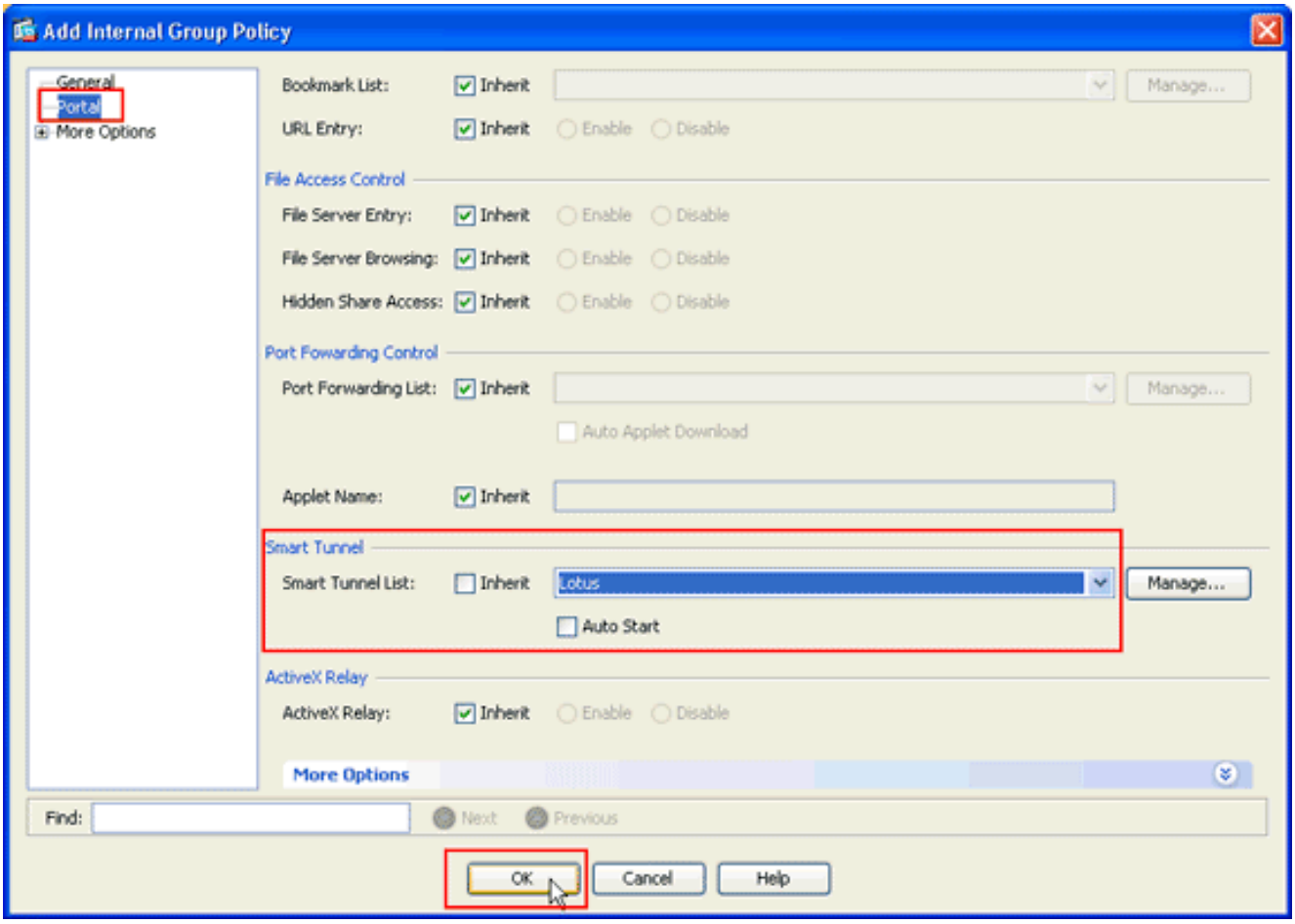


Remarque : Voici la commande de configuration CLI équivalente :

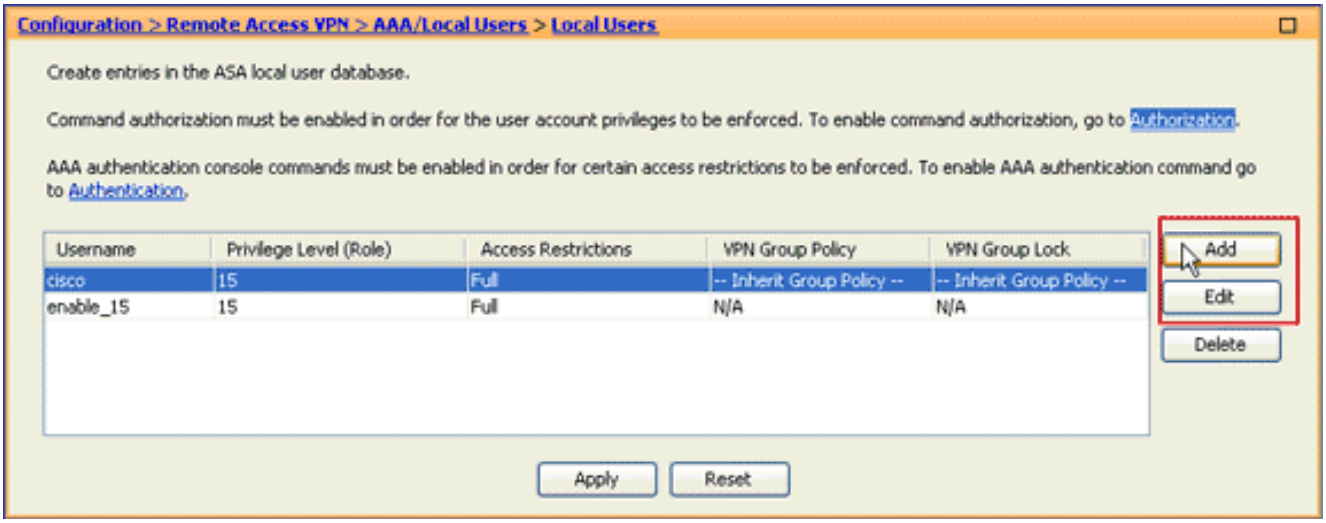
7. Affectez la liste aux stratégies de groupe et aux stratégies d'utilisateur local auxquelles vous souhaitez fournir un accès par tunnel intelligent aux applications associées comme suit :Afin d'affecter la liste à une stratégie de groupe, choisissez **Configuration > Remote Access VPN > Clientless SSL VPN Access > Group Policies**, puis cliquez sur **Add** or **Edit.**



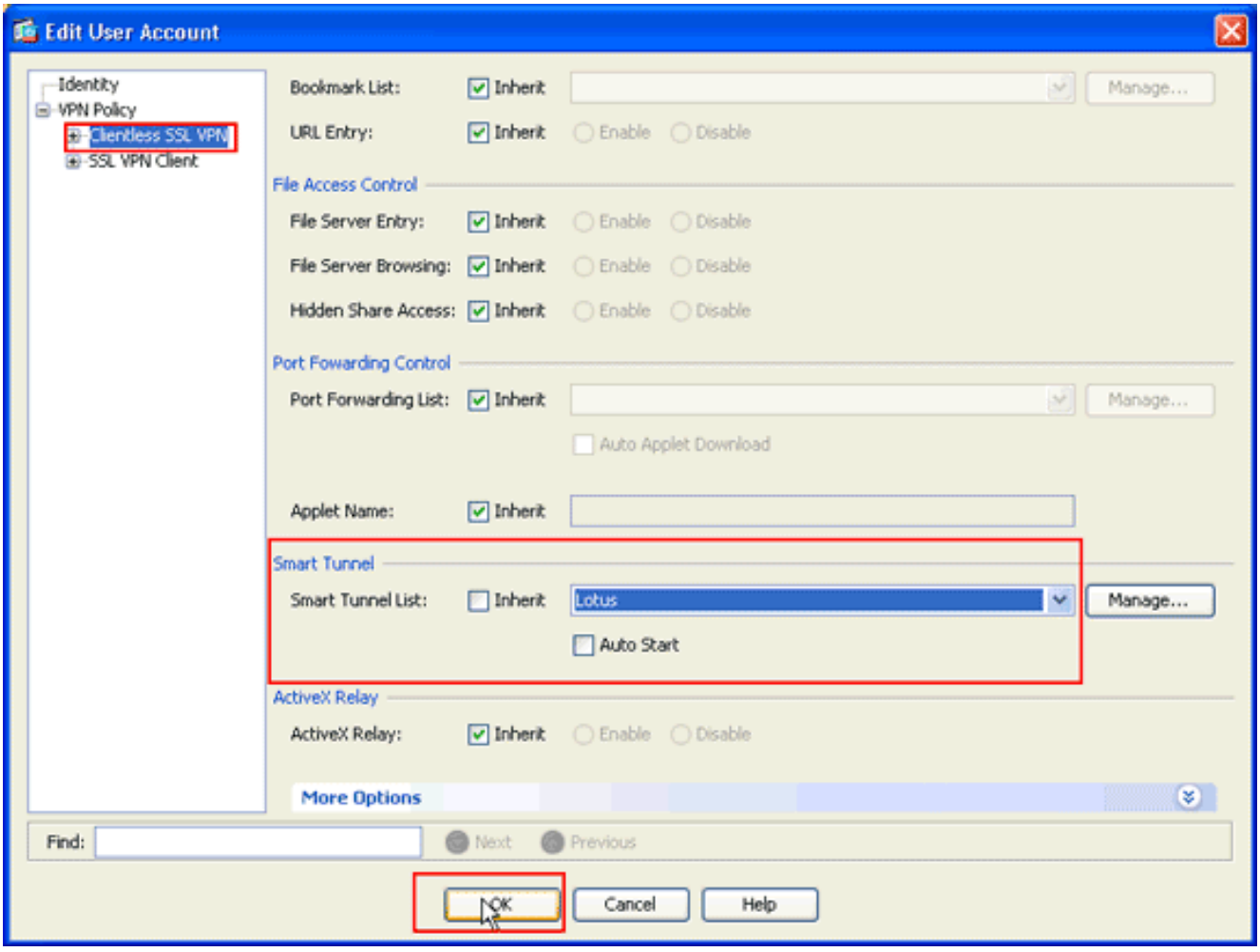
La boîte de dialogue Ajouter une stratégie de groupe interne s'affiche.



8. Dans la boîte de dialogue Ajouter une stratégie de groupe interne, cliquez sur **Portal**, choisissez le nom du tunnel intelligent dans la liste déroulante Smart Tunnel List, puis cliquez sur **OK**.**Remarque :** Cet exemple utilise *Lotus* comme nom de liste de tunnels intelligents.
9. Afin d'affecter la liste à une stratégie d'utilisateur local, choisissez **Configuration > Remote Access VPN> AAA Setup > Local Users**, puis cliquez sur **Add** pour configurer un nouvel utilisateur ou cliquez sur **Edit** pour modifier un utilisateur existant.



La boîte de dialogue Modifier le compte d'utilisateur s'affiche.



10. Dans la boîte de dialogue Modifier le compte d'utilisateur, cliquez sur **VPN SSL sans client**, choisissez le nom du tunnel intelligent dans la liste déroulante Smart Tunnel List, puis cliquez sur **OK**.**Remarque :** Cet exemple utilise *Lotus* comme nom de liste de tunnels intelligents.

La configuration du tunnel intelligent est terminée.

Dépannage

Je ne parviens pas à me connecter à l'aide d'une URL Smart Tunnel marquée

comme favori dans le portail sans client. Pourquoi ce problème se produit-il et comment puis-je le résoudre ?

Ce problème se produit en raison du problème décrit dans l'ID de bogue Cisco CSCsx05766 **(clients enregistrés uniquement)** . Afin de résoudre ce problème, rétrogradez le plug-in Java Runtime à une version antérieure.

Puis-je supprimer l'URL d'une liaison de tunnel intelligente configurée dans WebVPN ?

Lorsque le tunnel intelligent est utilisé sur l'ASA, vous ne pouvez pas masquer l'URL ou masquer la barre d'adresse du navigateur. Les utilisateurs peuvent afficher les URL des liens configurés dans WebVPN qui utilisent un tunnel intelligent. Par conséquent, ils peuvent modifier le port et accéder au serveur pour un autre service.

Afin de résoudre ce problème, utilisez des listes de contrôle d'accès WebType. Référez-vous à Listes de contrôle d'accès WebType pour plus d'informations.

Informations connexes

- Dispositifs de sécurité adaptatifs de la gamme Cisco ASA 5500
- Exemple de configuration d'un client VPN SSL (SVC) sur ASA avec ASDM
- Support et documentation techniques - Cisco Systems