ASA : Exemple de configuration de tunnel SMART avec ASDM

Contenu

Introduction

Un tunnel intelligent est une connexion entre une application basée sur le protocole TCP et un site privé, utilisant une session (basée sur navigateur) sans client de VPN SSL avec les dispositifs de sécurité comme voie et les dispositifs de sécurité en tant que serveur proxy. Vous pouvez identifier les applications auxquelles vous voulez accorder l'accès intelligent de tunnel et spécifier le chemin local à chaque application. Pour les applications qui fonctionnent sur Microsoft Windows, vous pouvez également avoir besoin d'une correspondance des informations parasites SHA-1 de la somme de contrôle comme condition pour accorder l'accès intelligent de tunnel.

Les Lotus Sametime et le *Microsoft Outlook Express* sont des exemples des applications auxquelles vous pourriez vouloir accorder l'accès intelligent de tunnel.

La personne à charge en fonction si l'application est un client ou est une application Web-activée, configuration intelligente de tunnel a besoin d'une de ces procédures :

- Créez un ou plusieurs listes intelligentes de tunnel des applications cliente, et puis assignez la

liste aux stratégies de groupe ou aux stratégies d'utilisateur local pour qui vous voulez fournir l'accès intelligent de tunnel.
- Créez un ou plusieurs entrées de la liste de signet qui spécifient l'URLs des applications Web-activées habilitées à l'accès intelligent de tunnel, et assignent alors la liste au DAPs, les stratégies de groupe, ou des stratégies d'utilisateur local pour qui vous veulent fournir l'accès intelligent de tunnel.Vous pouvez également répertorier les applications Web-activées pour que lesquelles automatisent l'envoi des qualifications de procédure de connexion dans les connexions en tunnel intelligentes au-dessus des sessions sans client de VPN SSL.

Ce document suppose que la configuration de client de VPN SSL de Cisco AnyConnect est déjà faite et fonctionne correctement de sorte que la caractéristique intelligente de tunnel puisse être configurée sur la configuration existante. Pour plus d'informations sur la façon configurer le client de VPN SSL de 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

Référez-vous à configurer une stratégie intelligente de tunnel de tunnel pour plus d'informations sur la façon configurer la Segmentation de tunnel avec le tunnel intelligent.

Remarque: Assurez-vous que les étapes *4.b à 4.l* décrit dans la configuration ASA utilisant la section ASDM 6.0(2) de l'*ASA 8.x : Permettez la Segmentation de tunnel pour l'AnyConnect VPN Client sur l'exemple de configuration ASA* n'est pas exécuté afin de configurer la caractéristique intelligente de tunnel.

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.

Composants utilisés

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

- Dispositifs de sécurité adaptatifs dédiés de la gamme Cisco ASA 5500 qui exécute la version de logiciel 8.0(2)
- PC qui exécute Microsoft Vista, Windows XP SP2, ou le professionnel SP4 de Windows 2000 avec la version 3.1 d'installateur de Microsoft
- Cisco Adaptive Security Device Manager (ASDM) version 6.0(2)

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

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

Informations générales

Configuration intelligente d'Access de tunnel

La table intelligente de tunnel affiche les listes intelligentes de tunnel, qui identifie un ou plusieurs applications habilitées à l'accès intelligent de tunnel et à son système d'exploitation associé (SYSTÈME D'EXPLOITATION). Puisque chaque stratégie de groupe ou stratégie d'utilisateur local prend en charge une liste intelligente de tunnel, vous devez grouper les applications basées sur nonbrowser à prendre en charge dans une liste intelligente de tunnel. Après la configuration d'une liste, vous pouvez l'assigner à un ou plusieurs groupe maintient l'ordre ou à stratégies d'utilisateur local.

Remarque: Pour plus d'informations sur la configuration intelligente de tunnel, référez-vous à configurer le tunnel intelligent Access.

La fenêtre intelligente de tunnels (**configuration > Accès à distance VPN > VPN SSL sans client Access > portail > les tunnels intelligents**) te permet pour remplir ces procédures :

- **Ajoutez une liste intelligente de tunnel et ajoutez les applications à la liste**Terminez-vous ces étapes afin d'ajouter une liste intelligente de tunnel et ajouter des applications à la liste :Cliquez sur **Add**.La boîte de dialogue intelligente de liste de tunnel d'ajouter apparaît.Entrez un nom pour la liste, et cliquez sur **Add**.L'ASDM ouvre la boîte de dialogue intelligente d'entrée de tunnel d'ajouter, qui te permet pour assigner les attributs d'un tunnel intelligent à la liste.Après que vous assigniez les attributs désirés pour le tunnel intelligent, cliquez sur OK.L'ASDM affiche ces attributs dans la liste.Répétez ces étapes selon les besoins afin de remplir la liste, et cliquez sur OK alors dans la boîte de dialogue intelligente de liste de tunnel d'ajouter.
- **Changez une liste intelligente de tunnel**Terminez-vous ces étapes afin de changer une liste intelligente de tunnel :Double-cliquer la liste ou choisissez la liste dans la table, et cliquez sur Edit.Cliquez sur Add pour insérer un nouvel ensemble d'attributs intelligents de tunnel dans la liste ou pour choisir une entrée dans la liste, et cliquez sur Edit ou **supprimez**.
- **Retirez une liste**Afin de retirer une liste, choisissez la liste dans la table, et cliquez sur Delete.
- **Ajoutez un signet**Après la configuration et l'attribution d'une liste intelligente de tunnel, vous pouvez rendre un tunnel intelligent facile à utiliser en ajoutant un signet pour le service et en cliquant sur l'option **intelligente de tunnel d'enable** dans l'ajouter ou éditer la boîte de dialogue de signet.

L'accès intelligent de tunnel permet une application basée sur le protocole TCP de client d'employer une connexion VPN basée sur navigateur pour se connecter à un service. Il offre les avantages suivants aux utilisateurs, comparés aux modules d'extension et à la technologie existante, transmission du port :

- Le tunnel intelligent offre une meilleure représentation que des connexions.
- Àla différence de la transmission du port, le tunnel intelligent simplifie l'expérience utilisateur par n'exige pas la connexion utilisateur de l'application locale au port local.
- Àla différence de la transmission du port, le tunnel intelligent n'exige pas des utilisateurs d'avoir des privilèges d'administrateur.

Conditions requises, restrictions, et limites intelligentes de tunnel

Conditions générales et limites

Le tunnel intelligent a les conditions générales et les limites suivantes :

- Le serveur distant lançant le tunnel intelligent doit exécuter une version 32 bits de Microsoft Windows Vista, de Windows XP, ou de Windows 2000 ; ou Mac OS 10.4 ou 10.5.
- L'ouverture de session automatique de tunnel intelligent prend en charge seulement Microsoft Internet Explorer sur Windows.
- Le navigateur doit être activé avec Javas, Microsoft ActiveX, ou chacun des deux.
- Le tunnel intelligent prend en charge seulement des proxys placés entre les ordinateurs qui exécutent Microsoft Windows et les dispositifs de sécurité. Le tunnel intelligent utilise la configuration d'Internet Explorer (c'est-à-dire, celle destinée au niveau système à l'utilisation dans Windows). Si l'ordinateur distant exige d'un serveur proxy d'atteindre les dispositifs de sécurité, l'URL de l'extrémité de terminaison de la connexion doit être dans la liste d'URLs exclue des services proxys. Si la configuration de proxy spécifie ce trafic destiné pour l'ASA passe par un proxy, tout le trafic du tunnel intelligent passe par le proxy.Dans un scénario basé sur HTTP d'Accès à distance, parfois un sous-réseau ne permet pas d'accéder l'accès client à la passerelle VPN. Dans ce cas, un proxy placé devant l'ASA pour conduire le trafic entre le Web et l'emplacement de l'utilisateur final fournit l'accès de Web. Cependant, seulement les utilisateurs VPN peuvent configurer des proxys placés devant l'ASA. En faire ainsi, ils doivent s'assurer que ces proxys prennent en charge la méthode de CONNECTER. Pour les proxys qui exigent l'authentification, le tunnel intelligent prend en charge seulement le type de base d'authentification de condensé.
- Si intelligents les débuts de tunnel, les dispositifs de sécurité perce un tunnel tout le trafic du processus de navigateur l'utilisateur utilisé pour initier la session sans client. Si l'utilisateur commence un autre exemple du processus de navigateur, il passe tout le trafic au tunnel. Si le processus de navigateur est identique et les dispositifs de sécurité ne permettent pas d'accéder à un URL donné, l'utilisateur ne peut pas l'ouvrir. Comme contournement, l'utilisateur peut utiliser un navigateur différent de celui utilisé pour établir la session sans client.
- Un basculement dynamique ne retient pas les connexions en tunnel intelligentes. Les utilisateurs doivent rebrancher après un Basculement.

Conditions requises et limites de Windows

Les conditions requises et les limites suivantes s'appliquent à Windows seulement :

- Seulement le Winsock 2, des applications basées sur le protocole TCP sont habilité à l'accès intelligent de tunnel.
- Les dispositifs de sécurité ne prennent en charge pas le proxy de l'échange de Microsoft Outlook (MAPI). Ni la transmission du port ni le tunnel intelligent ne prend en charge MAPI. Pour la transmission d'échange de Microsoft Outlook utilisant le protocole MAPI, les utilisateurs distants doivent utiliser AnyConnect.
- Les utilisateurs de la Microsoft Windows Vista qui utilisent le tunnel intelligent ou la transmission du port doivent ajouter l'URL de l'ASA à la zone de confiance de site. Afin

d'accéder à la zone de confiance de site, commencez l'Internet Explorer, et choisissez les **outils > les options Internet**, et cliquez sur les utilisateurs de vista de tableau de **Sécurité** peut également désactiver le mode protégé afin de faciliter l'accès intelligent de tunnel ; cependant, Cisco recommande contre cette méthode parce qu'elle augmente la vulnérabilité pour attaquer.

Conditions requises et limites de Mac OS

Ces conditions requises et limites appliquent à Mac OS seulement :

- Safari 3.1.1 ou plus tard ou Firefox 3.0 ou plus tard
- Sun JRE 1.5 ou plus tard
- Seulement les applications commencées de la page du portail peuvent établir les connexions en tunnel intelligentes. Cette condition requise inclut le soutien intelligent de tunnel de Firefox. Utilisant Firefox commencer un autre exemple de Firefox pendant la première utilisation d'un tunnel intelligent exige le profil utilisateur nommé csco_st. Si ce profil utilisateur n'est pas présent, la session incite l'utilisateur à créer un.
- Les applications utilisant le TCP qui sont dynamiquement liées à la bibliothèque SSL peuvent fonctionner au-dessus d'un tunnel intelligent.
- Le tunnel intelligent ne prend en charge pas ces caractéristiques et applications sur Mac OS :Services proxysOuverture de session automatiqueApplications qui utilisent des espaces de nom à deux niveauxapplications basées sur console, telles que le telnet, le SSH, et la boucleLes applications utilisant dlopen ou dlsym pour localiser des appels de libsocketApplications statiquement jointes pour localiser des appels de libsocket

Configurez

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

Remarque: Utilisez l'outil Command Lookup Tool (clients enregistrés seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Ajoutez ou éditez la liste intelligente de tunnel

La boîte de dialogue intelligente de liste de tunnel d'ajouter vous permet d'ajouter une liste d'entrées intelligentes de tunnel à la configuration de dispositifs de sécurité. La boîte de dialogue intelligente de liste de tunnel d'éditer vous permet de modifier le contenu de la liste.

Champ

Nom de liste — Écrivez un nom unique pour la liste des applications ou les programmes. Il n'y a aucune restriction sur le nombre de caractères dans le nom. N'utilisez pas les espaces. Après la configuration de la liste intelligente de tunnel, le nom de liste apparaît à côté de l'attribut intelligent de liste de tunnel dans les stratégies de groupe de VPN SSL et les stratégies sans client d'utilisateur local. Assignez un nom qui vous aidera à distinguer son contenu ou le but d'autre le répertorie que vous êtes susceptible de configurer.

Ajoutez ou éditez l'entrée intelligente de tunnel

L'ajouter ou éditent la boîte de dialogue intelligente d'entrée de tunnel vous permet de spécifier les attributs d'une application dans une liste intelligente de tunnel.

- **ID de la demande** — Écrivez une chaîne pour nommer l'entrée dans la liste intelligente de tunnel. La chaîne est seule pour le SYSTÈME D'EXPLOITATION. Typiquement, il nomme l'application pour accorder l'accès intelligent de tunnel. Afin de prendre en charge des plusieurs versions d'une application pour laquelle vous choisissez de spécifier des différents chemins ou des valeurs de hachage, vous pouvez employer cet attribut pour différencier des entrées, spécifiant le SYSTÈME D'EXPLOITATION et le nom et la version de l'application prise en charge par chaque entrée de la liste. La chaîne peut être jusqu'à 64 caractères.
- **Nom du processus** — Entrez dans le nom du fichier ou le chemin à l'application. La chaîne peut être jusqu'à 128 caractèresWindows exige un précis - correspondance de cette valeur au côté droit du chemin d'application sur le serveur distant pour qualifier l'application pour l'accès intelligent de tunnel. Si vous spécifiez seulement le nom du fichier pour Windows, le VPN SSL n'impose pas une restriction d'emplacement sur le serveur distant pour qualifier l'application pour l'accès intelligent de tunnel.Si vous spécifiez un chemin et l'utilisateur installait l'application dans un autre emplacement, cette application ne qualifie pas. L'application peut résider sur n'importe quel chemin tant que le côté droit des vérifications de la chaîne la valeur que vous écrivez.Afin d'autoriser une demande d'accès intelligent de tunnel s'il est présent sur un de plusieurs chemins sur le serveur distant, ou spécifiez seulement le nom et l'extension de l'application dans ce domaine ou créez une seule entrée intelligente de tunnel pour chaque chemin.Pour Windows, si vous voulez ajouter l'accès intelligent de tunnel à une application commencée de l'invite de commande, vous devez spécifier « cmd.exe » dans le nom du processus d'une entrée dans la liste intelligente de tunnel et spécifier le chemin à l'application lui-même dans une autre entrée parce que « cmd.exe » est le parent de l'application.Mac OS exige le chemin d'accès complet au processus et distingue les majuscules et minuscules. Afin d'éviter de spécifier un chemin pour chaque nom d'utilisateur, insérez un tilde (|) avant le chemin partiel (par exemple, ~/bin/vnc).
- **SYSTÈME D'EXPLOITATION** — Clic Windows ou MAC afin de spécifier le SYSTÈME D'EXPLOITATION d'hôte de l'application.
- **Informations parasites** — (*facultatif et applicable seulement pour Windows*) afin d'obtenir cette valeur, écrivez la somme de contrôle du fichier exécutable dans un utilitaire qui calcule des informations parasites utilisant l'algorithme SHA-1. Un exemple d'un tel utilitaire est le vérificateur d'intégrité de somme de contrôle de fichier de Microsoft (FCIV), qui est disponible chez http://support.microsoft.com/kb/841290/ . Après avoir installé FCIV, placez une copie provisoire de l'application à hacher sur un chemin qui ne contient aucun espace (par exemple, c : /fciv.exe), entrent dans alors l'application fciv.exe -sha1 à la ligne de commande (par exemple, fciv.exe -sha1 c:\msimn.exe) pour afficher les informations parasites SHA-1.Les informations parasites SHA-1 sont toujours 40 caractères hexadécimaux.Avant d'autoriser une demande d'accès intelligent de tunnel, le VPN SSL sans client calcule les informations parasites de l'application appariant l'ID de la demande. Il qualifie l'application pour l'accès intelligent de tunnel si le résultat apparie la valeur des informations parasites.Entrer dans des informations parasites fournit une assurance raisonnable que le VPN SSL ne qualifie pas un fichier illégitime qui apparie la chaîne que vous avez spécifiée dans l'ID de la demande. Puisque la somme de contrôle varie avec chaque version ou correctif d'une application, les informations parasites que vous entrez peuvent seulement apparier un version ou correctif sur

le serveur distant. Afin de spécifier des informations parasites pour plus d'une version d'une application, créez une seule entrée intelligente de tunnel pour chaque valeur de hachage.**Remarque:** Vous devez mettre à jour la liste intelligente de tunnel à l'avenir si vous écrivez des valeurs de hachage et vous voulez prendre en charge des versions futures ou des correctifs d'une application avec l'accès intelligent de tunnel. Un problème soudain avec l'accès intelligent de tunnel pourrait être une indication que l'application qui contient des valeurs de hachage n'est pas à jour avec une mise à jour d'application. Vous pouvez éviter ce problème en n'entrant pas dans des informations parasites.

- Une fois que vous configurez la liste intelligente de tunnel, vous devez l'assigner à une stratégie de groupe ou à une stratégie d'utilisateur local pour qu'elle devienne actif comme suit :Afin d'assigner la liste à une stratégie de groupe, choisir le **VPN SSL sans client Access > stratégies de groupe de config > d'Accès à distance VPN> > ajoutent ou éditent > portail**, et choisissent le nom intelligent de tunnel de la liste déroulante à côté de l'attribut intelligent de liste de tunnel.Afin d'assigner la liste à une stratégie d'utilisateur local, choisir l'**AAA de config > d'Accès à distance VPN> installé > les utilisateurs locaux > ajoutent ou éditent > règle VPN > VPN SSL sans client**, et choisissent le nom intelligent de tunnel de la liste déroulante à côté de l'attribut intelligent de liste de tunnel.

Configuration intelligente de tunnel ASA (exemple de Lotus) utilisant l'ASDM 6.0(2)

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

Remarque: Référez-vous à Permettre l'accès HTTPS pour l'ASDM afin de permettre l'ASA d'être configuré par l'ASDM.

Remarque: Le WebVPN et l'ASDM ne peuvent pas être activés sur la même interface ASA à moins que vous changiez les numéros de port. Référez-vous à ASDM et WebVPN activés sur la même interface d'ASA pour plus d'informations.

Terminez-vous ces étapes afin de configurer un tunnel intelligent :

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

1. Choisissez la **configuration > l'Accès à distance VPN > VPN SSL sans client Access > portail > les tunnels intelligents** afin de commencer la configuration intelligente de tunnel.
2. Cliquez sur **Add**.La boîte de dialogue intelligente de liste de tunnel d'ajouter apparaît.
3. Dans la boîte de dialogue intelligente de liste de tunnel d'ajouter, cliquez sur Add.La boîte de dialogue intelligente d'entrée de tunnel d'ajouter apparaît.
4. Dans le domaine d'ID de la demande, écrivez une chaîne pour identifier l'entrée dans la liste intelligente de tunnel.
5. Écrivez un nom du fichier et une extension pour l'application, et cliquez sur OK.
6. Dans la boîte de dialogue intelligente de liste de tunnel d'ajouter, cliquez sur OK.**Remarque:** Voici la commande de configuration équivalente CLI :
7. Assignez la liste aux stratégies de groupe et aux stratégies d'utilisateur local auxquelles vous voulez fournir l'accès intelligent de tunnel aux applications associées comme suit :Afin d'assigner la liste à une stratégie de groupe, choisir le **VPN SSL sans client Access > stratégies de groupe de configuration > d'Accès à distance VPN>**, et cliquer sur Add ou

l'éditer. La boîte de dialogue d'Add Internal Group Policy apparaît.

8. Dans la boîte de dialogue d'Add Internal Group Policy, cliquez sur le **portail**, choisissez le nom intelligent de tunnel de la liste déroulante intelligente de liste de tunnel, et cliquez sur OK.**Remarque:** Cet exemple utilise *Lotus* comme nom de liste intelligent de tunnel.
9. Afin d'assigner la liste à une stratégie d'utilisateur local, choisissez l'**AAA de configuration > d'Accès à distance VPN> installé > des utilisateurs locaux**, et cliquez sur Add pour configurer configurent un nouvel utilisateur ou cliquent sur Edit pour éditer un utilisateur existant.La boîte de dialogue de compte utilisateur d'éditer apparaît.
10. Dans la boîte de dialogue de compte utilisateur d'éditer, cliquez sur le **VPN SSL sans client**, choisissez le nom intelligent de tunnel de la liste déroulante intelligente de liste de tunnel, et cliquez sur OK.**Remarque:** Cet exemple utilise *Lotus* comme nom de liste intelligent de tunnel.

La configuration intelligente de tunnel est complète.

Dépannez

Je ne peux pas se connecter utilisant un URL intelligent bookmarked de tunnel dans le portail sans client. Pourquoi cette question peux se produit-elle, et est-ce que comment je la résoudre ?

Cette question se produit en raison du problème décrit dans l'ID de bogue Cisco CSCsx05766 **(clients enregistrés seulement)**. Afin de résoudre ce problème, déclassifiez le module d'extension d'exécution de Javas à une version plus ancienne.

Est-ce que je peux déformer l'URL d'un lien intelligent de tunnel configuré dans le webvpn ?

Quand le tunnel intelligent est utilisé sur l'ASA, vous ne pouvez pas déformer l'URL ou masquer la barre d'adresses du navigateur. Les utilisateurs peuvent visualiser l'URLs des liens configurés dans le webvpn qui utilisent le tunnel intelligent. En conséquence, ils peuvent changer le port et accéder au serveur pour un autre service.

Afin de résoudre ce problème, utilisation WebType ACLs. Référez-vous à créer le pour en savoir plus de WebType ACLs.

Informations connexes

- Dispositifs de sécurité adaptatifs de la gamme Cisco ASA 5500
- Notes en version pour l'AnyConnect VPN Client, version 2.3
- Exemple de configuration d'un client VPN SSL (SVC) sur ASA avec ASDM
- Support et documentation techniques - Cisco Systems