PIX/ASA : Exemple de configuration de la fonction de mise à jour automatique d'un client VPN IPsec

Contenu

Introduction

Ce document décrit comment configurer la caractéristique d'Automatique-mise à jour de Client VPN Cisco dans l'appliance de sécurité adaptatif de la gamme Cisco ASA 5500 et les Dispositifs de sécurité de la gamme Cisco PIX 500.

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 :

- Version 7.x et ultérieures de passages d'appliance de sécurité adaptatif de la gamme Cisco ASA 5500
- Version 7.x et ultérieures de passages de Dispositifs de sécurité de la gamme Cisco PIX 500
- Version 5.x et ultérieures du Cisco Adaptive Security Device Manager (ASDM)
- Client VPN Cisco 4.x et plus tard

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.

Comment configurer la mise à jour client pour Windows avec le CLI

La caractéristique de mise à jour client permet des administrateurs à un site central automatiquement d'informer des utilisateurs de client vpn quand il est temps de mettre à jour le logiciel de client VPN et l'image de client matériel VPN 3002.

Émettez la commande de **mise à jour client** dans le mode de configuration d'ipsec-`attributs de groupe de tunnels` afin de configurer la mise à jour client. Si le client exécute déjà une version de logiciel sur la liste de nombres de révision, elle n'a pas besoin de mettre à jour son logiciel. Si le client n'exécute pas une version de logiciel sur la liste, elle devrait mettre à jour. Vous pouvez spécifier jusqu'à quatre entrées de mise à jour du client.

La syntaxe de commande suit :

client-update type *type* {url *url-string*} {rev-nums *rev-nums*} no client-update *[type]*

- **Rév-nums** *Rév-nums* — Spécifie le logiciel ou les images de microprogramme pour ce client. Écrivez jusqu'à quatre, séparé par des virgules.
- *type* — Spécifie les systèmes d'exploitation pour annoncer d'une mise à jour client. La liste de systèmes d'exploitation comporte de ces derniers :Microsoft Windows : toutes les Plateformes basées sur WindowsWIN9X : Plateformes de Windows 95, de Windows 98, et de Windows MEWinNT : Plateformes de Windows NT 4.0, de Windows 2000, et de Windows XPvpn3002 : Client matériel VPN 3002
- *URL-chaîne* **URL** — Spécifie l'URL pour le logiciel/image de microprogramme. Cet URL doit indiquer un fichier approprié pour le client.

Cet exemple configure des paramètres de mise à jour client pour le groupe de tunnels de remote-access appelé le remotegrp. Il indique la révision le numéro 4.6.1 et l'URL pour la récupération de la mise à jour, qui est `https://support/updates`.

ASA
hostname(config)#**tunnel-group remotegrp type ipsec_ra** hostname(config)#**tunnel-group remotegrp ipsec-attributes** hostname(config-ipsec)#**client-update type windows url https://support/updates/rev-nums 4.6.1**

Comment configurer la mise à jour client pour Windows avec l'ASDM

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

Référez-vous à permettre à HTTPS Access pour l'ASDM afin de permettre l'ASA à configurer par l'ASDM

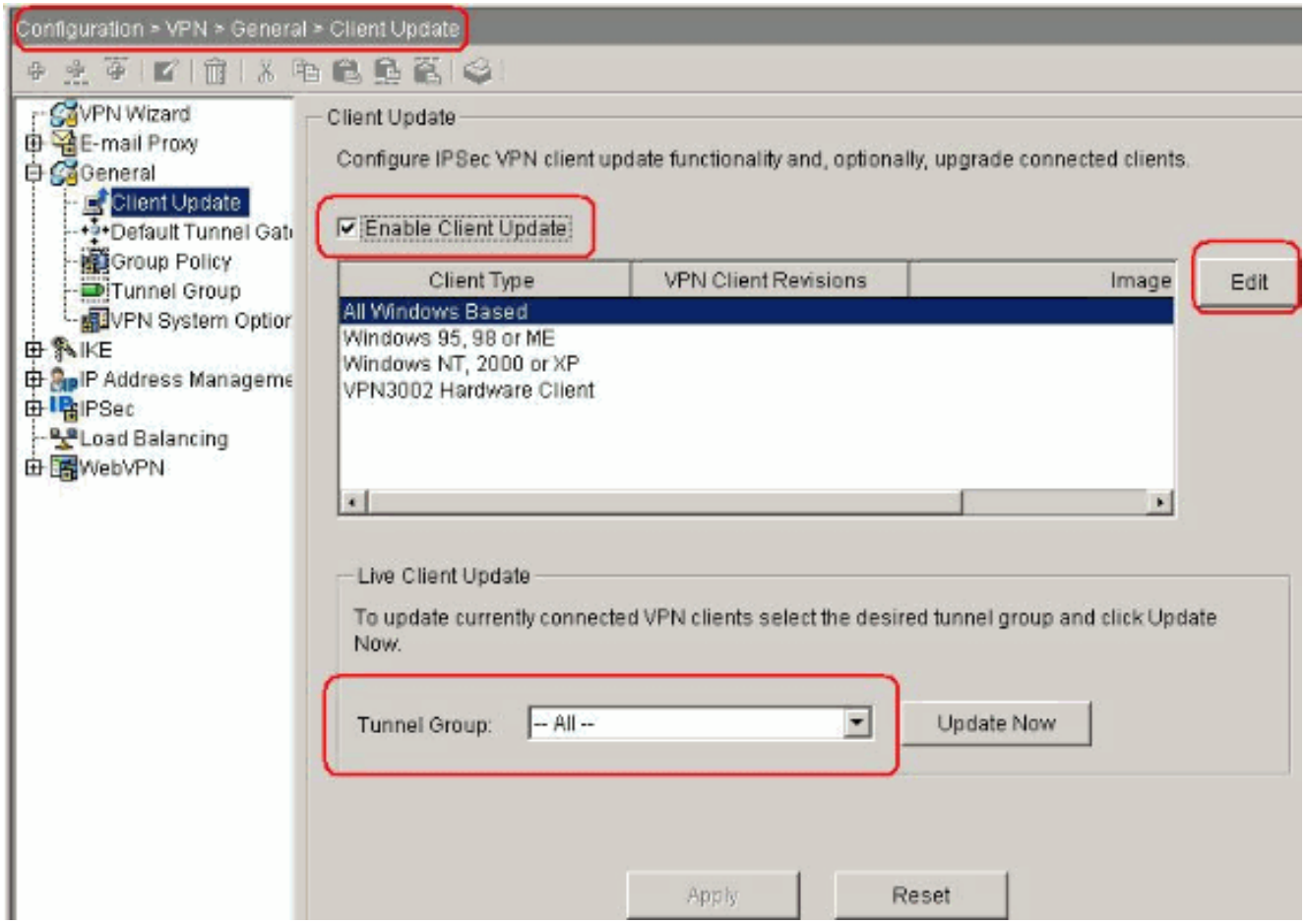
L'ASDM entoure deux genres de mise à jour client : un qui prend en charge des clients Windows et des clients matériels VPN 3002 par un groupe de tunnel, et l'autre qui prennent en charge des périphériques ASA agissant en tant que serveur d'automatique-mise à jour.

Les utilisateurs distants peuvent utiliser des versions périmées de logiciel VPN ou de client matériel. Vous pouvez exécuter une mise à jour client à tout moment pour faire ces fonctions :

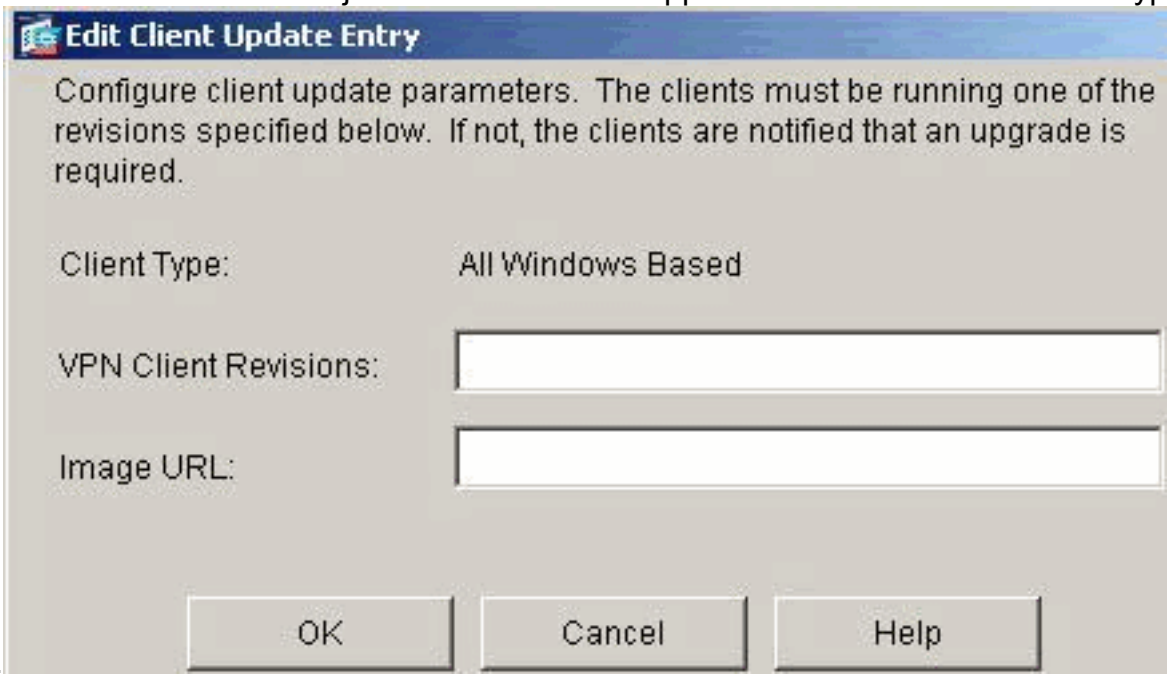
- Enable mettant à jour des révisions de client.
- Spécifiez les types et les nombres de révision de clients auxquels la mise à jour s'applique.
- Fournissez un URL ou une adresse IP dont pour obtenir la mise à jour.
- Informez sur option les utilisateurs de client Windows qu'ils devraient mettre à jour leur version de client vpn.
- Pour des clients Windows, vous pouvez fournir un mécanisme pour que les utilisateurs accomplissent la mise à jour.
- Pour des utilisateurs de client matériel VPN 3002, la mise à jour se produit automatiquement, sans la notification.

Terminez-vous ces étapes afin de configurer une mise à jour client :

1. Choisissez la **configuration > le VPN > le général > la mise à jour client** afin d'aller à la fenêtre de mise à jour client. La fenêtre de mise à jour client s'ouvre.Cochez la case de **mise à jour client d'enable** afin d'activer la mise à jour client.Choisissez le type de client auquel vous voulez appliquer la mise à jour client. Les types disponibles sont **tous de** client **basés sur Windows, le Windows 95, 98 ou le client matériel MOI, de Windows NT 4.0, de 2000 ou de XP, et VPN 3002.**Si le client exécute déjà une version de logiciel sur la liste de nombres de révision, elle n'a pas besoin de mettre à jour son logiciel. Si le client n'exécute pas une version de logiciel sur la liste, elle devrait mettre à jour. Vous pouvez spécifier jusqu'à trois de ces entrées de mise à jour du client. La toute la sélection basée sur Windows couvre toutes les plates-formes Windows permises. Si vous sélectionnez ceci, ne spécifiez pas les différents types de client Windows.Cliquez sur Edit afin de spécifier les révisions acceptables de client et la source pour le logiciel ou l'image de microprogramme mis à jour pour la mise à jour
client.

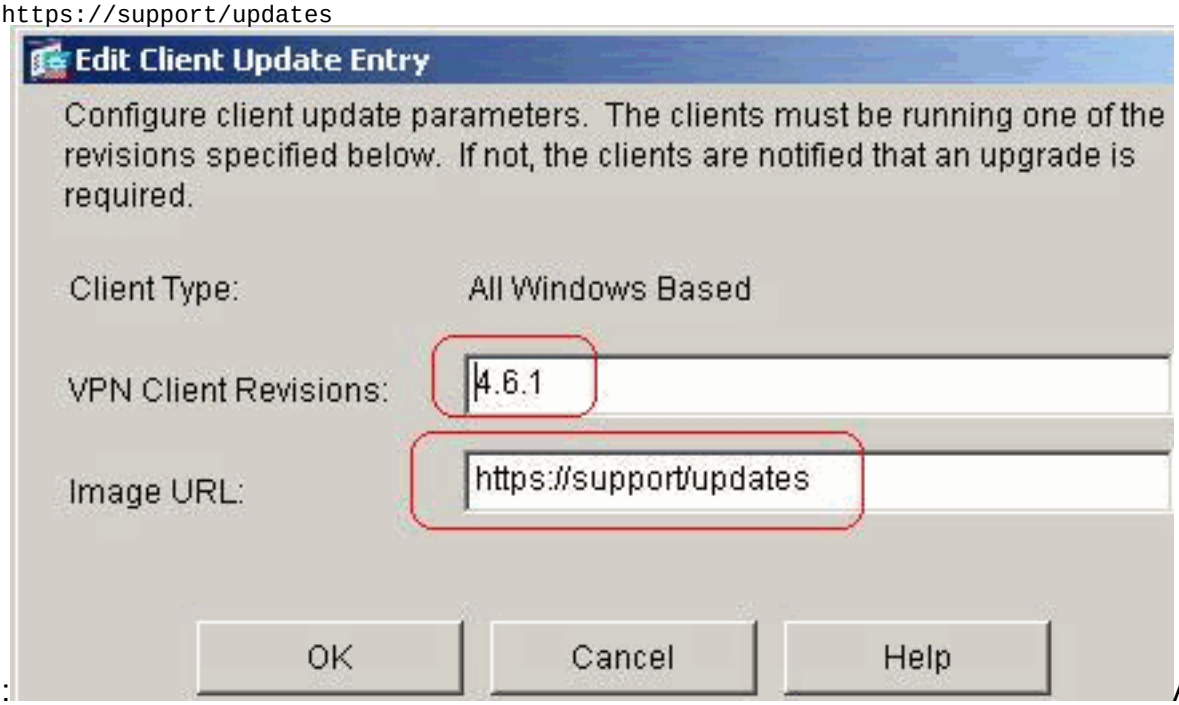


2. La fenêtre d'entrée de mise à jour du client d'éditer apparaît et affiche la sélection de type de client.



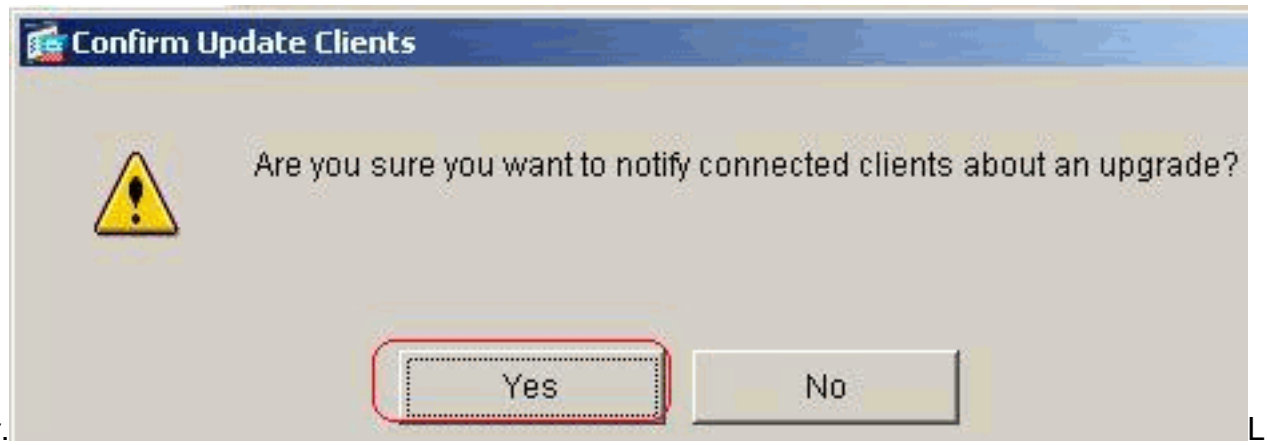
3. Spécifiez la mise à jour client que vous voulez appliquer à tous les clients du type sélectionné à travers les dispositifs de sécurité entiers. C'est-à-dire, spécifiez le type dont de client, l'URL ou l'adresse IP pour obtenir l'image mise à jour, et le nombre ou les nombres de révision acceptables pour ce client. Vous pouvez spécifier jusqu'à quatre nombres de révision, séparés par des virgules. Vos entrées semblent dans les colonnes appropriées la table sur la fenêtre de mise à jour de client après que vous cliquiez sur OK.Si le nombre de révision de client apparie un des nombres de révision spécifiés, il n'y a aucun besoin de mettre à jour le client.**Remarque:** Pour tous les clients Windows, vous devez utiliser le protocole http:// ou https:// comme préfixe pour l'URL. Pour le client matériel VPN 3002, vous

devez spécifier le protocole tftp:// à la place.Il initie une mise à jour client pour tous les clients Windows pour des révisions courantes d'un groupe de tunnels de remote-access plus anciennes que 4.6.1 et spécifie l'URL pour la récupération de la mise à jour comme `https://support/updates`



: Alternativement, vous pouvez configurer la mise à jour client juste pour différents types de client, plutôt que pour tous les clients Windows, que vous pouvez voir si l'étape 1-c.La mise à jour de clients VPN 3002 sans intervention de l'utilisateur et les utilisateurs ne reçoivent aucun message de notification.Vous pouvez faire commencer au navigateur automatiquement une application si vous incluez le nom d'application à l'extrémité de l'URL ; par exemple : **https://support/updates/vpnclient.exe.**

4. Sur option, vous pouvez envoyer un avis aux utilisateurs actifs avec les clients Windows périmés qui doivent mettre à jour leur client. Employez la région vivante de mise à jour client de la fenêtre de mise à jour client afin d'envoyer cet avis. Choisissez le groupe de tunnel (ou tous) et cliquez sur la **mise à jour maintenant**. Une boîte de dialogue est évident dans la figure et te demande de confirmer que vous voulez informer les clients connectés au sujet de la mise à



jour. Les utilisateurs indiqués voient une fenêtre externe, qui leur donne l'occasion de lancer un navigateur et de télécharger le logiciel mis à jour du site que vous avez spécifié dans l'URL. La seule partie de ce message que vous pouvez configurer est l'URL. (Voir les étapes 1B ou 1-c.) Les utilisateurs qui ne sont pas en activité reçoivent un message de notification la prochaine fois qu'ils ouvrent une session. Vous pouvez envoyer cet avis à tous les clients actifs sur tous les groupes de tunnel, ou vous pouvez l'envoyer aux clients sur un groupe

particulier de tunnel.Si le nombre de révision de client apparie un des nombres de révision spécifiés, il n'y a aucun besoin de mettre à jour le client, et aucun message de notification n'est envoyé à l'utilisateur. La mise à jour de clients VPN 3002 sans intervention de l'utilisateur et les utilisateurs ne reçoivent aucun message de notification.

Vérifiez

Aucune procédure de vérification n'est disponible pour cette configuration.

Informations connexes

- Support et documentation techniques - Cisco Systems