Exemple de configuration d'un VPN SSL client léger (WebVPN) sur ASA avec ASDM

Contenu

Introduction

La technologie Thin-Client VPN SSL permet l'accès sécurisé pour certaines applications dotées de ports statiques, telles que Telnet(23), SSH(22), POP3(110), IMAP4(143) et SMTP(25). Vous pouvez utiliser Thin-Client VPN SSL en tant qu'application déterminée axée sur l'utilisateur, axée sur la politique, ou les deux à la fois. C'est-à-dire que vous pouvez configurer l'accès selon chaque utilisateur, ou que vous pouvez créer des Politiques collectives auxquelles vous ajoutez un ou plusieurs utilisateurs.

- **VPN SSL sans client (WebVPN) - Fournit un client distant nécessitant un navigateur Web compatible SSL pour accéder à des serveurs Web HTTP ou HTTPS sur un réseau local d'entreprise (LAN).** En outre, le VPN SSL sans client permet l'exploration de fichiers Windows via le protocole Common Internet File System (CIFS). Outlook Web Access (OWA) est un exemple d'accès HTTP.Consultez l'Exemple de configuration d'un VPN SSL sans client

(WebVPN) sur une ASA afin d'en savoir plus sur le VPN SSL sans client.

- **VPN SSL client léger (redirection de port) - Fournit un client distant qui télécharge un petit applet basé sur Java et permet l'accès sécurisé aux applications de Protocole de contrôle de transmissions (TCP) qui utilisent des numéros de port statiques.** Le Post Office Protocol (POP3), le Simple Mail Transfer Protocol (SMTP), le Protocole de messagerie IMAP, le Secure shell (SSH) et le telnet sont des exemples d'accès sécurisé. Puisque les fichiers sur l'ordinateur local changent, les utilisateurs doivent avoir des privilèges d'administrateur locaux pour utiliser cette méthode. Cette méthode de VPN SSL ne fonctionne pas avec les applications qui utilisent des affectations de ports dynamiques, telles que certaines applications de protocole de transfert de fichiers (FTP).**Remarque :** le protocole UDP (User Datagram Protocol) n'est pas pris en charge.
- **Client VPN SSL (Mode Tunnel) — Télécharge un petit client sur le poste de travail distant et permet un accès entièrement sécurisé aux ressources d'un réseau d'entreprise interne.** Vous pouvez télécharger de manière permanente le client VPN SSL (SVC) sur une station de travail distante ou supprimer le client une fois la session sécurisée fermée.Référez-vous à Exemple de configuration du client VPN SSL (SVC) sur ASA avec ASDM afin d'en savoir plus sur le client VPN SSL.

Ce document présente une configuration simple pour le VPN SSL client léger sur l'appareil de sécurité adaptatif (ASA). La configuration permet à un utilisateur d'établir une connexion Telnet sécurisée à un routeur situé à l'intérieur de l'ASA. La configuration de ce document est prise en charge pour ASA version 7.x et ultérieure.

Conditions préalables

Conditions requises

Avant de tenter cette configuration, assurez-vous de respecter les conditions suivantes pour les stations clientes distantes :

- Navigateur Web compatible SSL
- SUN Java JRE version 1.4 ou ultérieure
- Cookies activés
- Bloqueurs de fenêtres publicitaires intempestives désactivés
- Privilèges administratifs locaux (non requis mais fortement suggéré)

Note : La dernière version de SUN Java JRE est disponible en téléchargement gratuit sur le site Java.

Components Used

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

- Dispositif de sécurité adaptatif de la gamme Cisco 5510
- Cisco Adaptive Security Device Manager (ASDM) 5.2(1)**Remarque :** référez-vous à Autoriser l'accès HTTPS pour ASDM afin de permettre à l'ASA d'être configuré par l'ASDM.
- Logiciel Cisco Adaptive Security Appliance Version 7.2(1)
- Client distant Microsoft Windows XP Professionnel (SP 2)

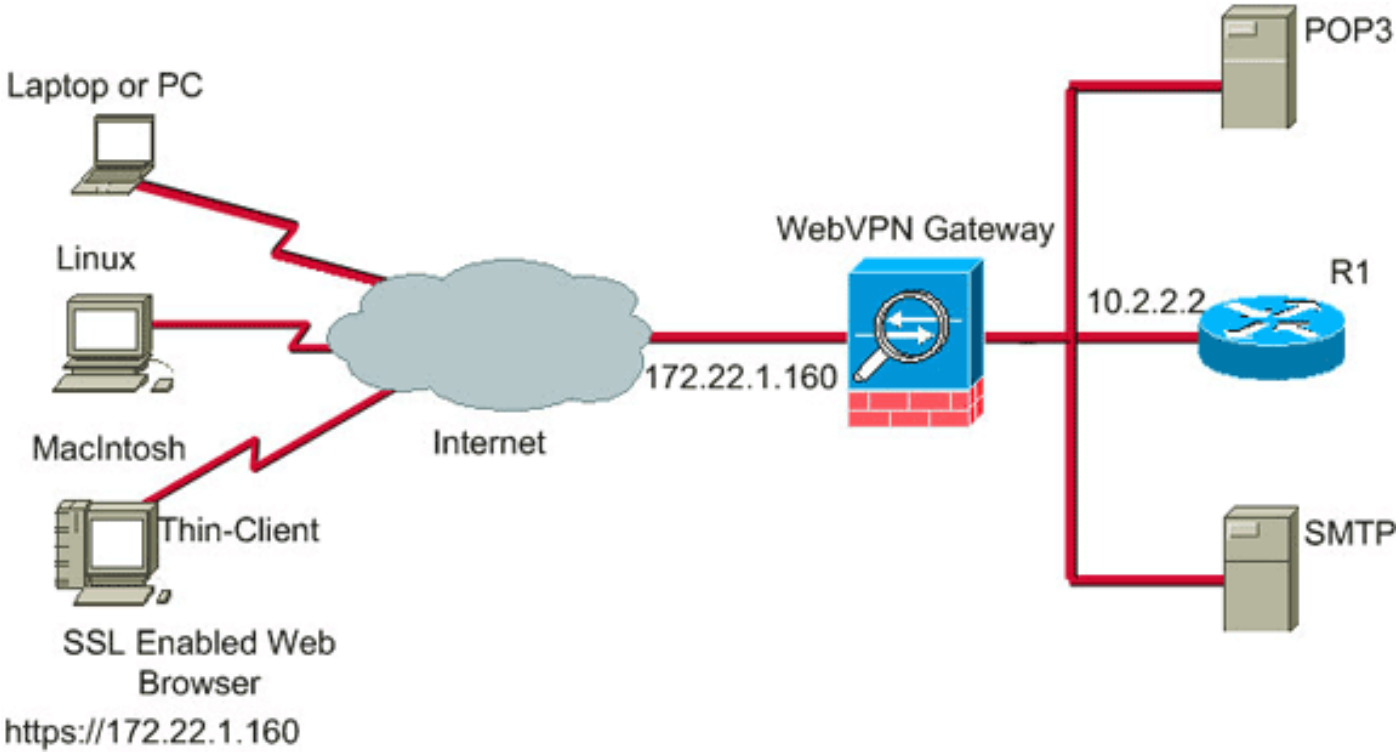
Les informations de ce document ont été élaborées dans un environnement de laboratoire. Tous

les périphériques utilisés dans ce document ont été réinitialisés à leur configuration par défaut. Si votre réseau est opérationnel, assurez-vous que vous comprenez l'impact potentiel de toute commande. Toutes les adresses IP utilisées dans cette configuration ont été sélectionnées à partir d'adresses RFC 1918 dans un environnement de laboratoire ; ces adresses IP ne sont pas routables sur Internet et sont utilisées à des fins de test uniquement.

Diagramme du réseau

Ce document utilise la configuration réseau décrite dans cette section.

Lorsqu'un client distant lance une session avec l'ASA, le client télécharge une petite applet Java sur la station de travail. Une liste des ressources préconfigurées est présentée au client.



Conventions

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

Informations générales

Afin de démarrer une session, le client distant ouvre un navigateur SSL à l'interface externe de l'ASA. Une fois la session établie, l'utilisateur peut utiliser les paramètres configurés sur l'ASA pour appeler n'importe quel accès Telnet ou d'application. L'ASA proxie la connexion sécurisée et permet à l'utilisateur d'accéder au périphérique.

Remarque : Les listes d'accès entrantes ne sont pas nécessaires pour ces connexions car l'ASA est déjà conscient de ce qui constitue une session juridique.

Configuration VPN SSL client léger à l'aide d'ASDM

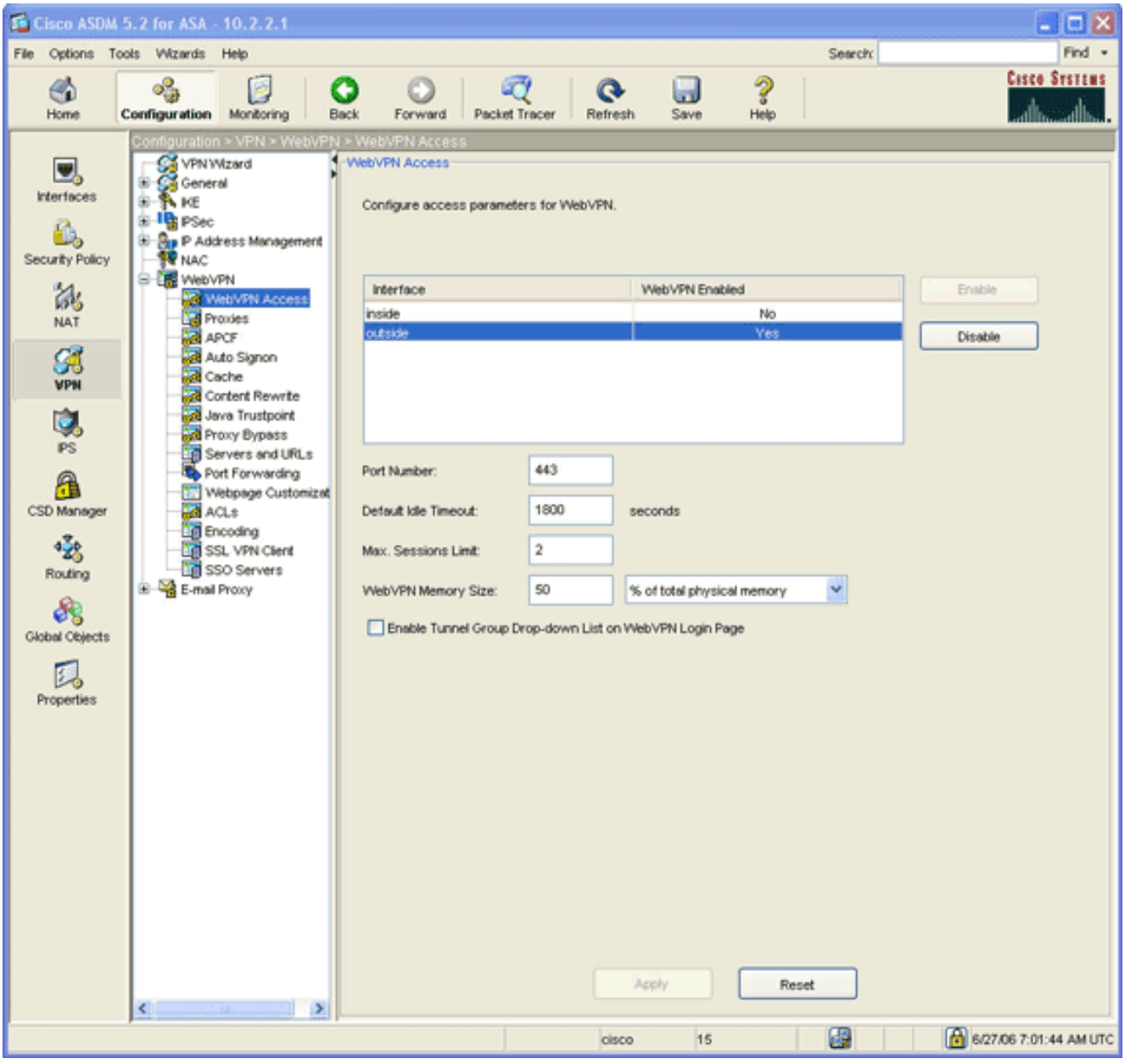
Afin de configurer le VPN SSL client léger sur l'ASA, procédez comme suit :

1. Activer WebVPN sur l'ASA
2. Configuration des caractéristiques de transfert de port
3. Créer une stratégie de groupe et la lier à la liste de transfert de port (créée à l'étape 2)
4. Créer un groupe de tunnels et le lier à la stratégie de groupe (créé à l'étape 3)
5. Créer un utilisateur et ajouter cet utilisateur à la stratégie de groupe (créée à l'étape 3)

Étape 1. Activer WebVPN sur l'ASA

Pour activer WebVPN sur l'ASA, procédez comme suit :

1. Dans l'application ASDM, cliquez sur **Configuration**, puis cliquez sur **VPN**.
2. Développez **WebVPN**, puis sélectionnez **WebVPN Access**.

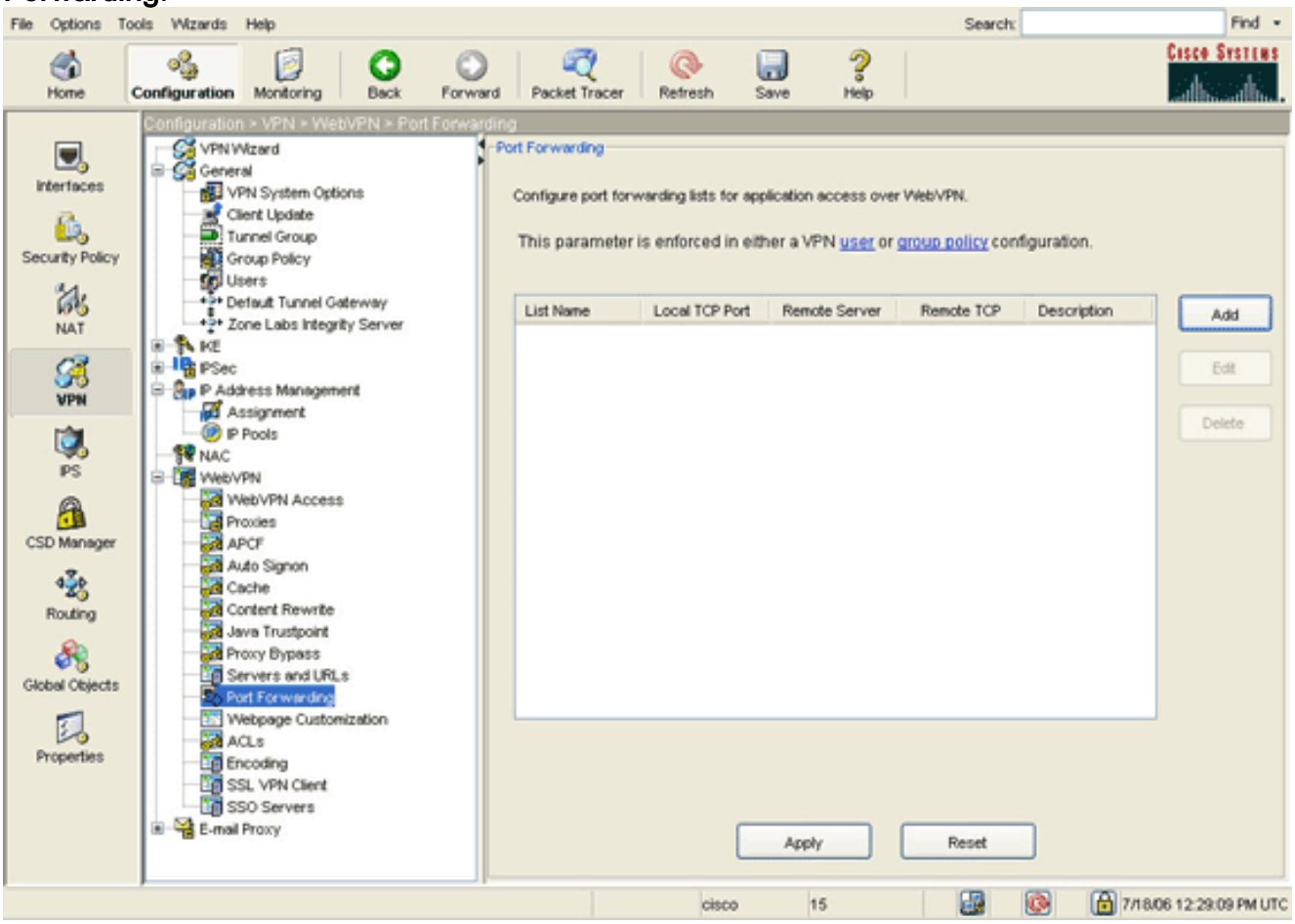


3. Mettez l'interface en surbrillance, puis cliquez sur **Enable**.
4. Cliquez sur **Apply**, sur **Save**, puis sur **Yes** pour accepter les modifications.

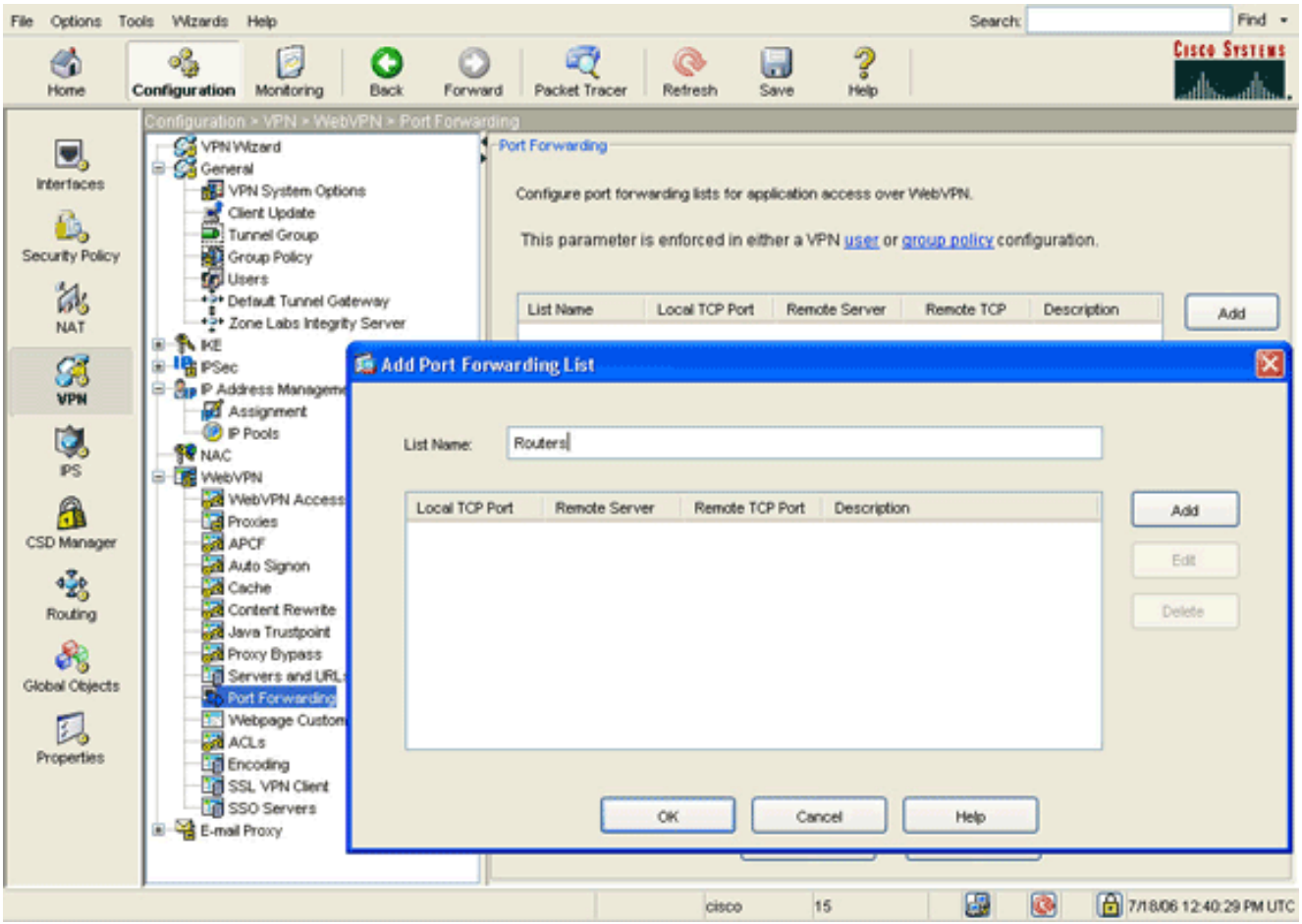
Étape 2. Configuration des caractéristiques de transfert de port

Afin de configurer les caractéristiques de transfert de port, procédez comme suit :

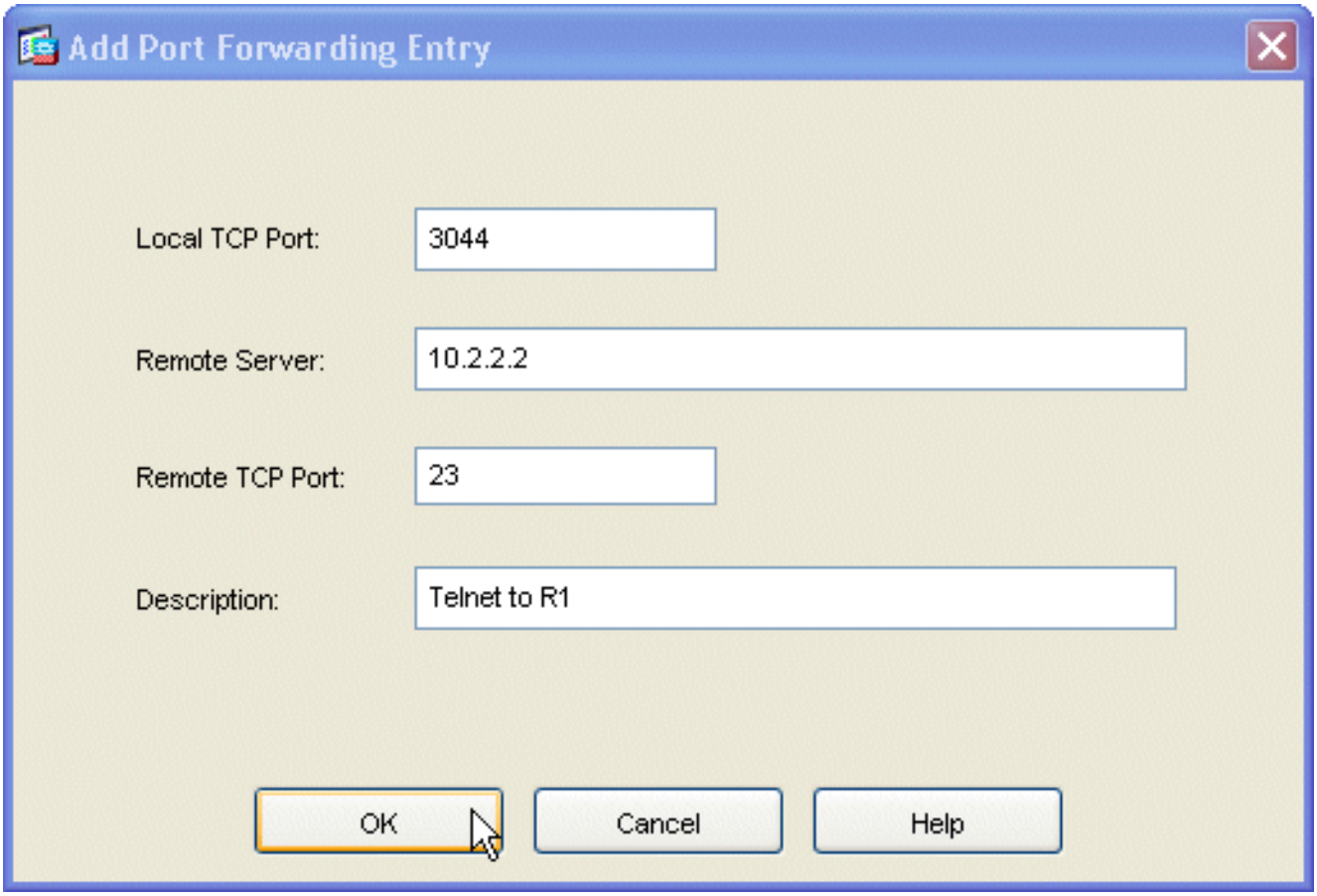
1. Développez **WebVPN**, puis choisissez **Port Forwarding**.



2. Cliquez sur le bouton **Add.**



3. Dans la boîte de dialogue Ajouter une liste de transfert de port, entrez un nom de liste, puis cliquez sur **Ajouter**.La boîte de dialogue Ajouter une entrée de transfert de port s'affiche.



4. Dans la boîte de dialogue Ajouter une entrée de transfert de port, entrez les options suivantes :Dans le champ Local TCP Port, saisissez un numéro de port ou acceptez la

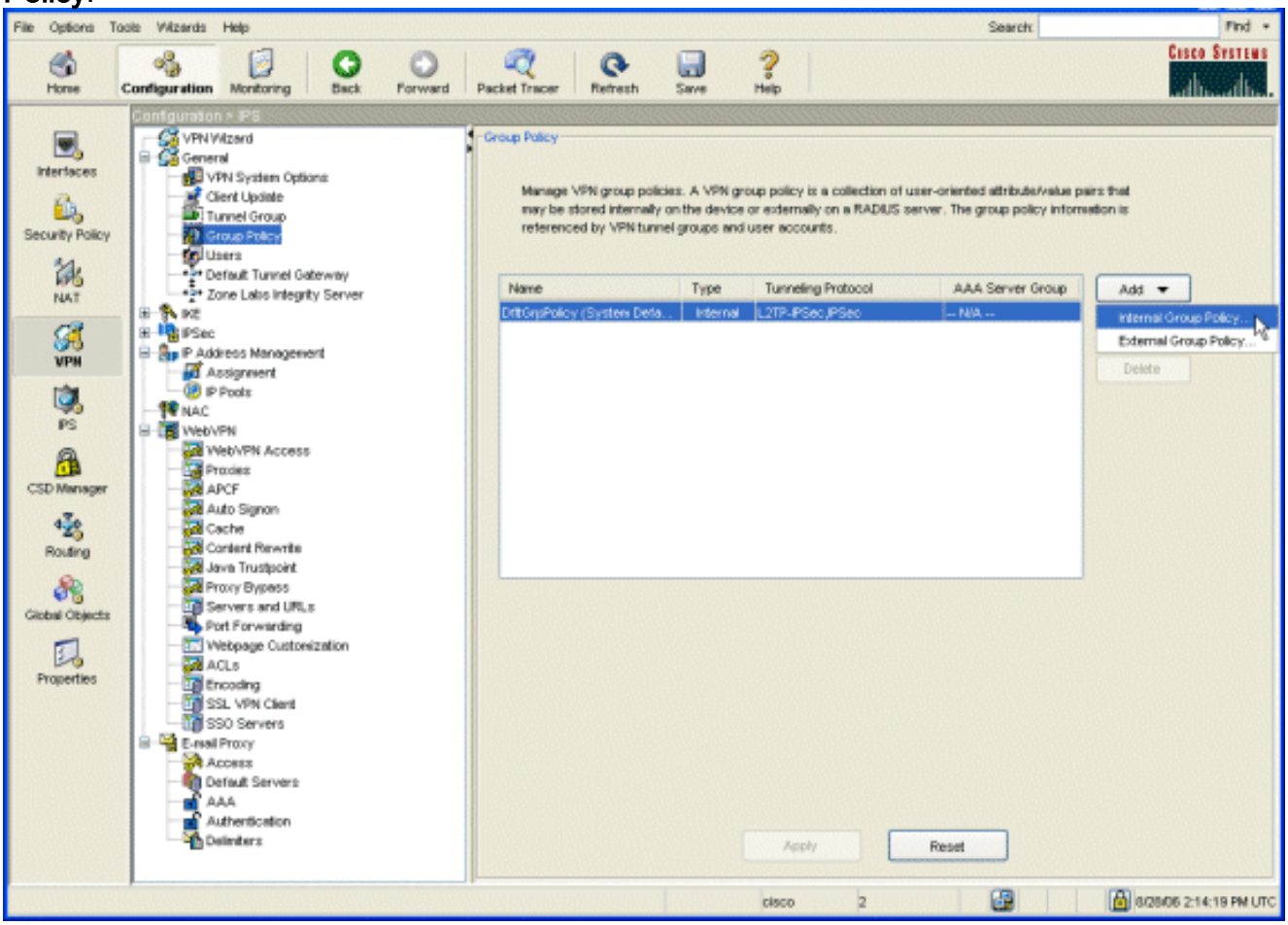
valeur par défaut.La valeur que vous entrez peut être n'importe quel nombre compris entre 1024 et 65535.Dans le champ Remote Server, saisissez une adresse IP.Cet exemple utilise l'adresse du routeur.Dans le champ Remote TCP Port, saisissez un numéro de port.Cet exemple utilise le port 23.Dans le champ Description, saisissez une description, puis cliquez sur **OK**.

5. Cliquez sur **OK**, puis sur **Apply**.
6. Cliquez sur **Save**, puis sur **Yes pour accepter les modifications.**

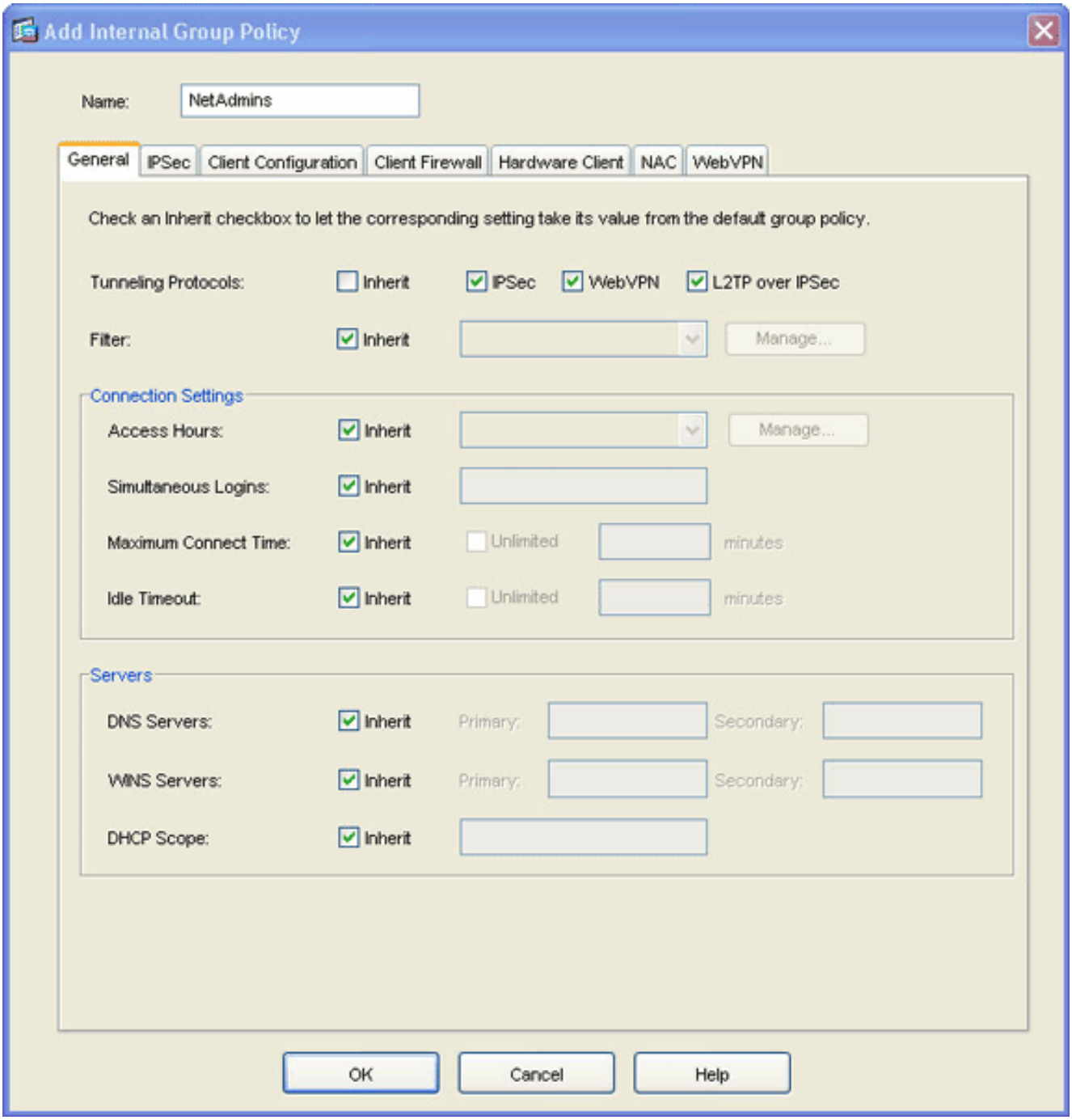
Étape 3. Créer une stratégie de groupe et la lier à la liste de transfert de port

Afin de créer une stratégie de groupe et de la lier à la liste de transfert de port, procédez comme suit :

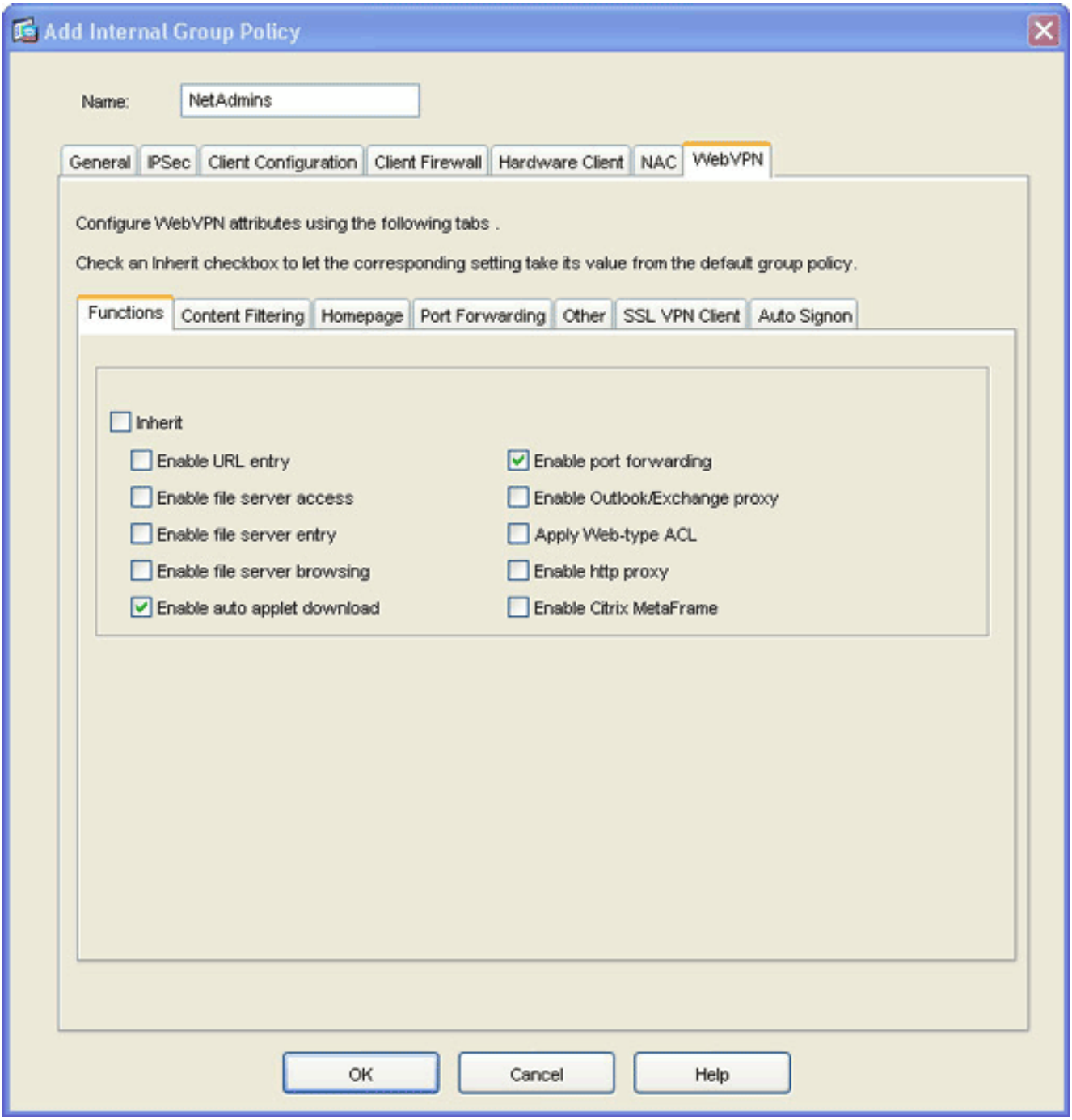
1. Développez **General**, puis choisissez **Group Policy**.



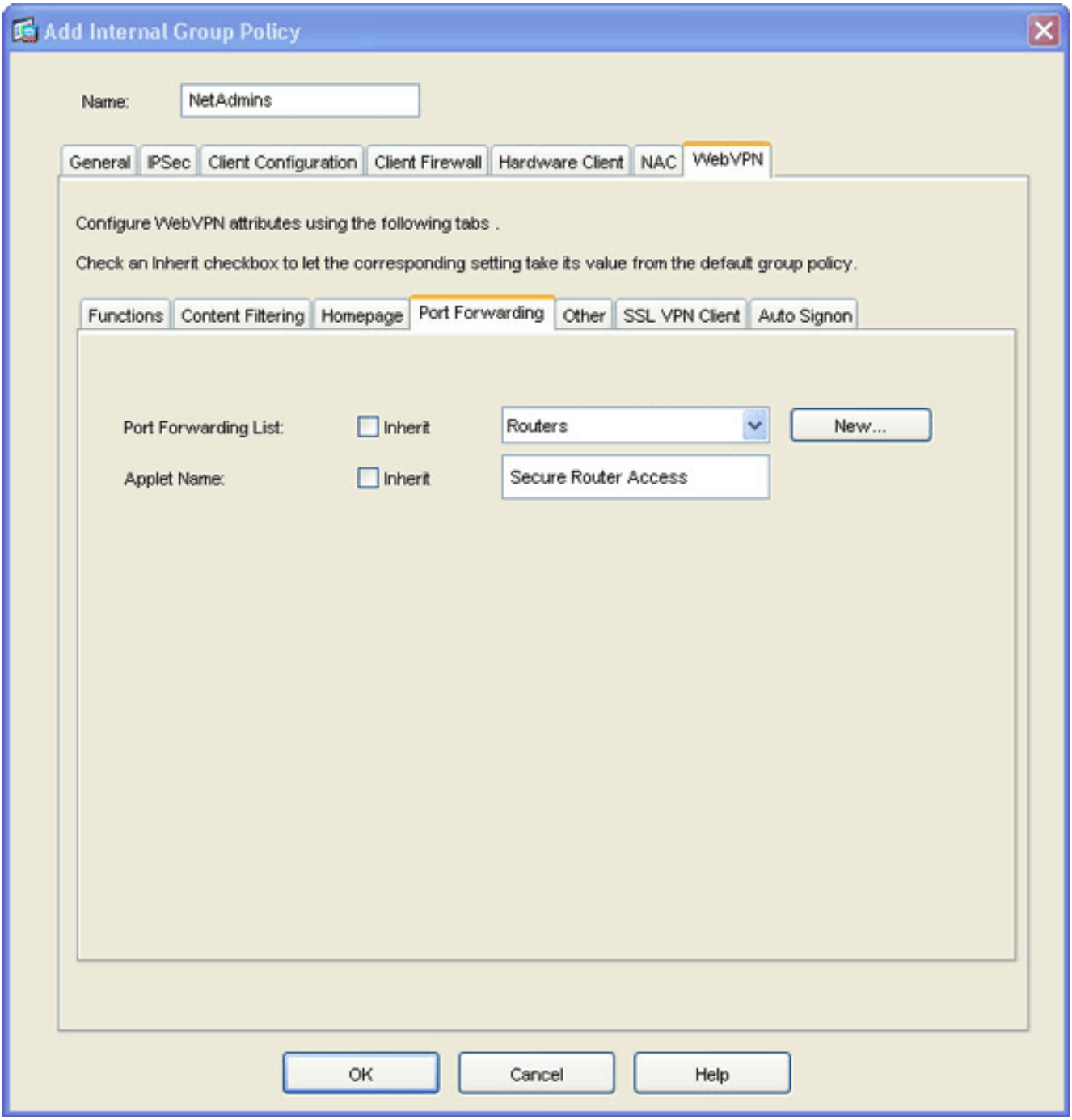
2. Cliquez sur **Add**, puis sélectionnez **Internal Group Policy**.La boîte de dialogue Ajouter une stratégie de groupe interne s'affiche.



3. Entrez un nom ou acceptez le nom de stratégie de groupe par défaut.
4. Décochez la case Tunneling Protocols **Inherit** et cochez la case **WebVPN**.
5. Cliquez sur l'onglet **WebVPN** situé en haut de la boîte de dialogue, puis cliquez sur l'onglet **Fonctions**.
6. Décochez la case **Hériter** et cochez les cases **Activer le téléchargement automatique des applets** et **Activer le transfert de port** comme indiqué dans cette image
   :



7. Également dans l'onglet WebVPN, cliquez sur l'onglet **Port Forwarding** et décochez la case Port Forwarding List
Inherit.



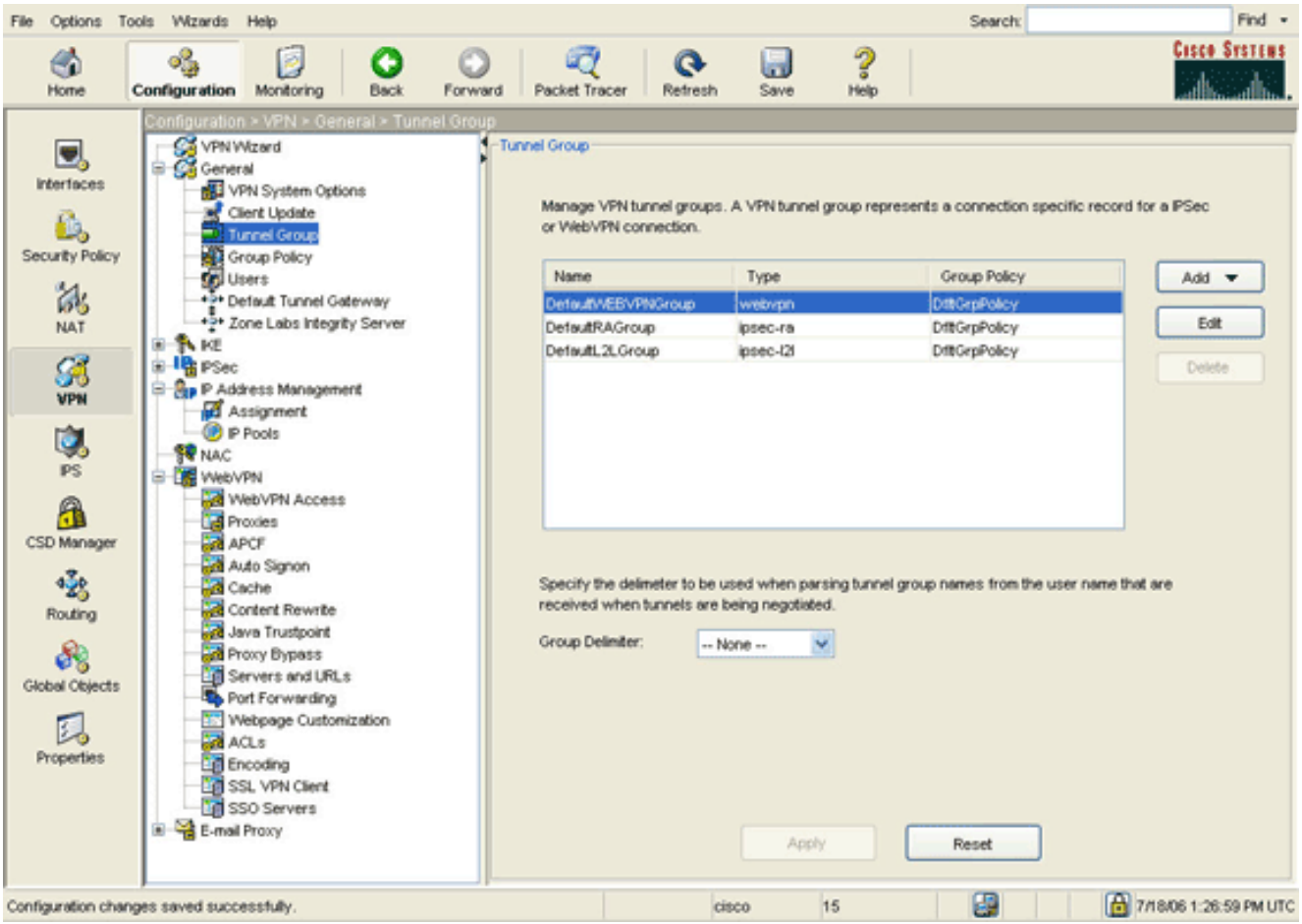
8. Cliquez sur la flèche de la liste déroulante **Port Forwarding List**, puis sélectionnez la liste de transfert de port que vous avez créée à l'étape 2.
9. Décochez la case **Hériter** le nom de l'applet et modifiez le nom dans le champ de texte.Le client affiche le nom de l'applet lors de la connexion.
10. Cliquez sur **OK**, puis sur **Apply**.
11. Cliquez sur **Save**, puis sur **Yes pour accepter les modifications.**

Étape 4. Créer un groupe de tunnels et le lier à la stratégie de groupe

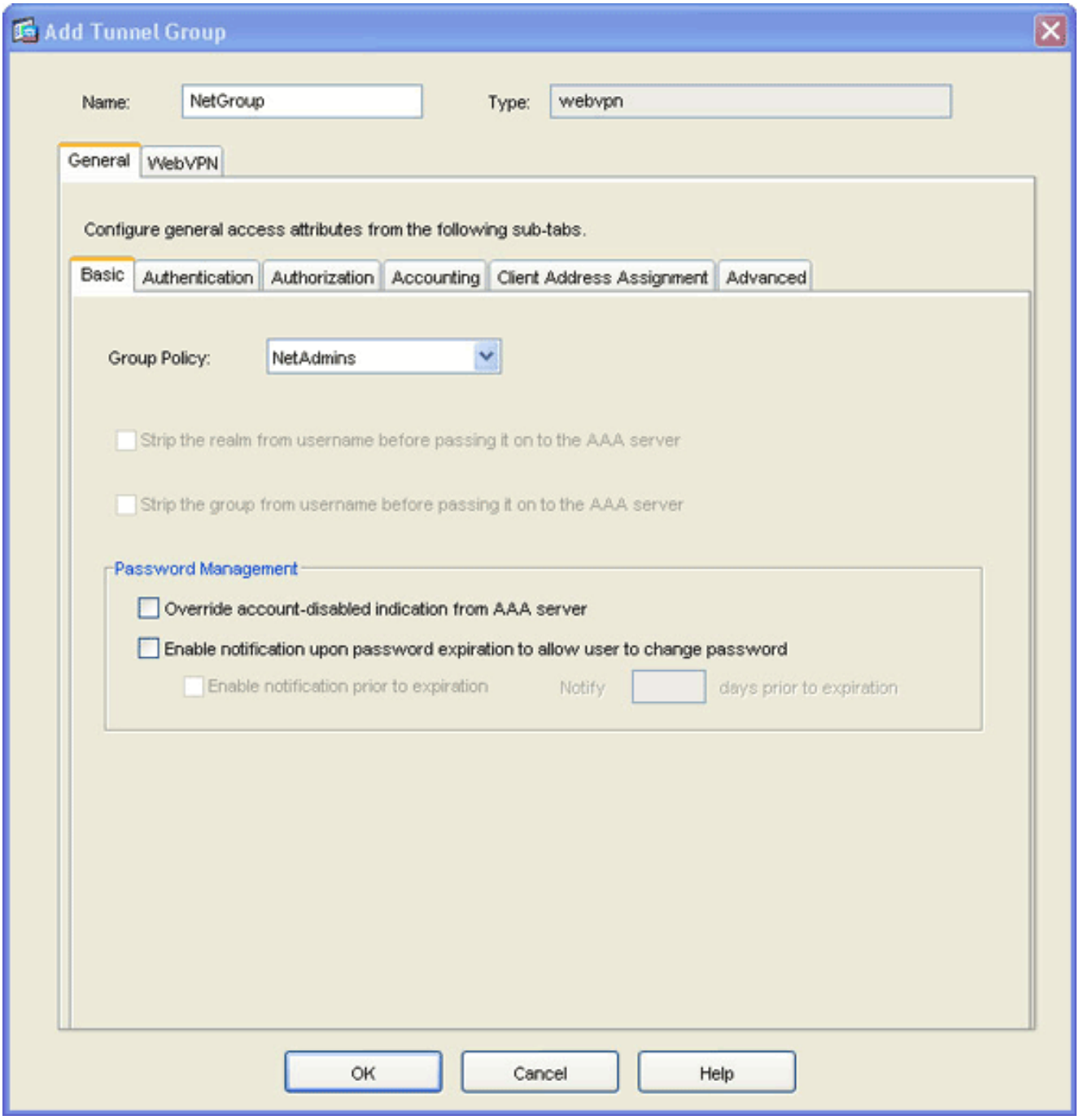
Vous pouvez modifier le groupe de tunnels *DefaultWebVPNroup* par défaut ou créer un nouveau groupe de tunnels.

Pour créer un nouveau groupe de tunnels, procédez comme suit :

1. Développez **General**, puis sélectionnez **Tunnel Group**.



2. Cliquez sur **Add**, puis sélectionnez **WebVPN Access**.La boîte de dialogue Ajouter un groupe de tunnels
s'affiche.

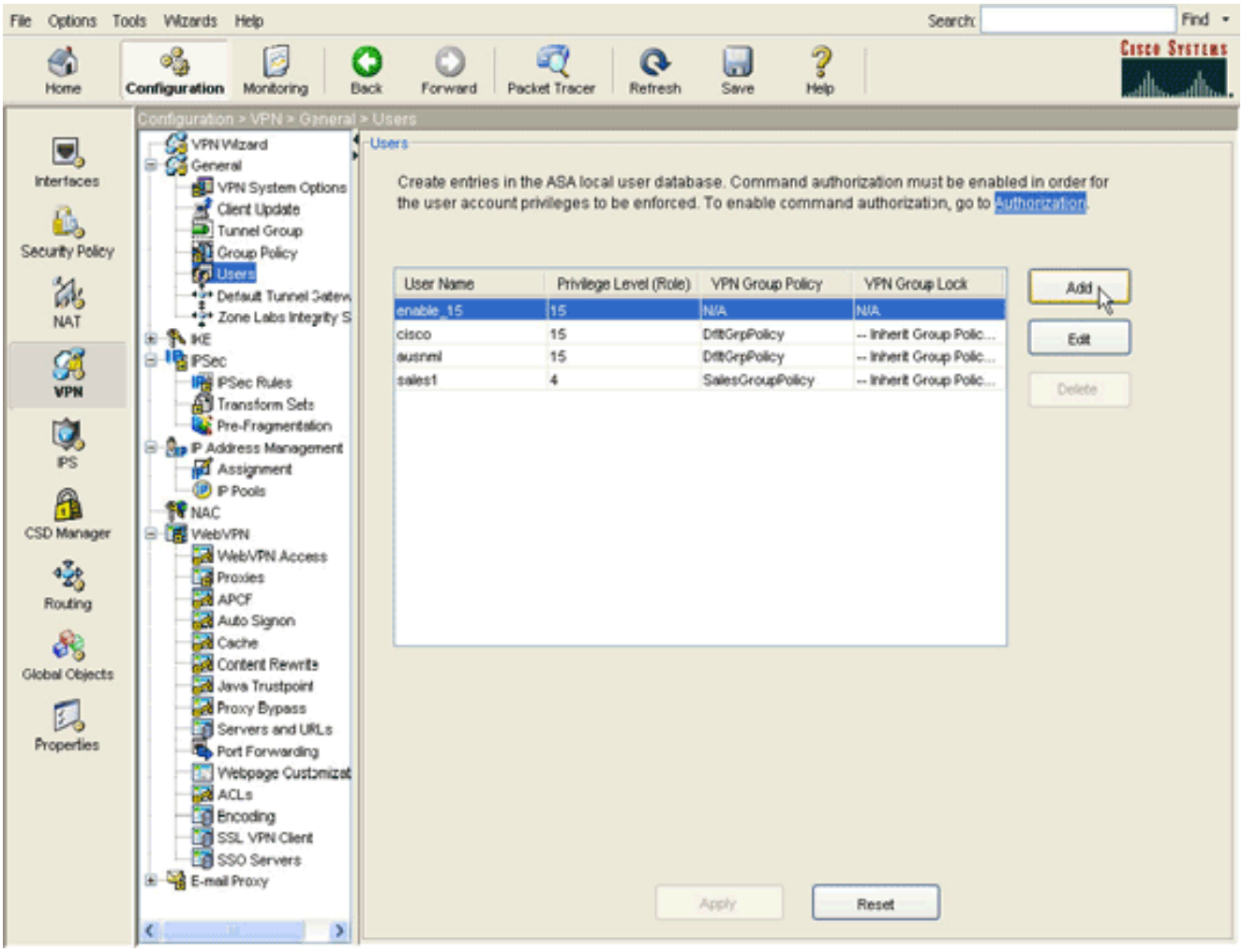


3. Saisissez un nom dans le champ Nom.
4. Cliquez sur la flèche de la liste déroulante **Stratégie de groupe**, puis sélectionnez la stratégie de groupe que vous avez créée à l'étape 3.
5. Cliquez sur **OK**, puis sur **Apply**.
6. Cliquez sur **Save**, puis sur **Yes pour accepter les modifications.**Le groupe de tunnels, la stratégie de groupe et les caractéristiques de transfert de port sont maintenant liés.

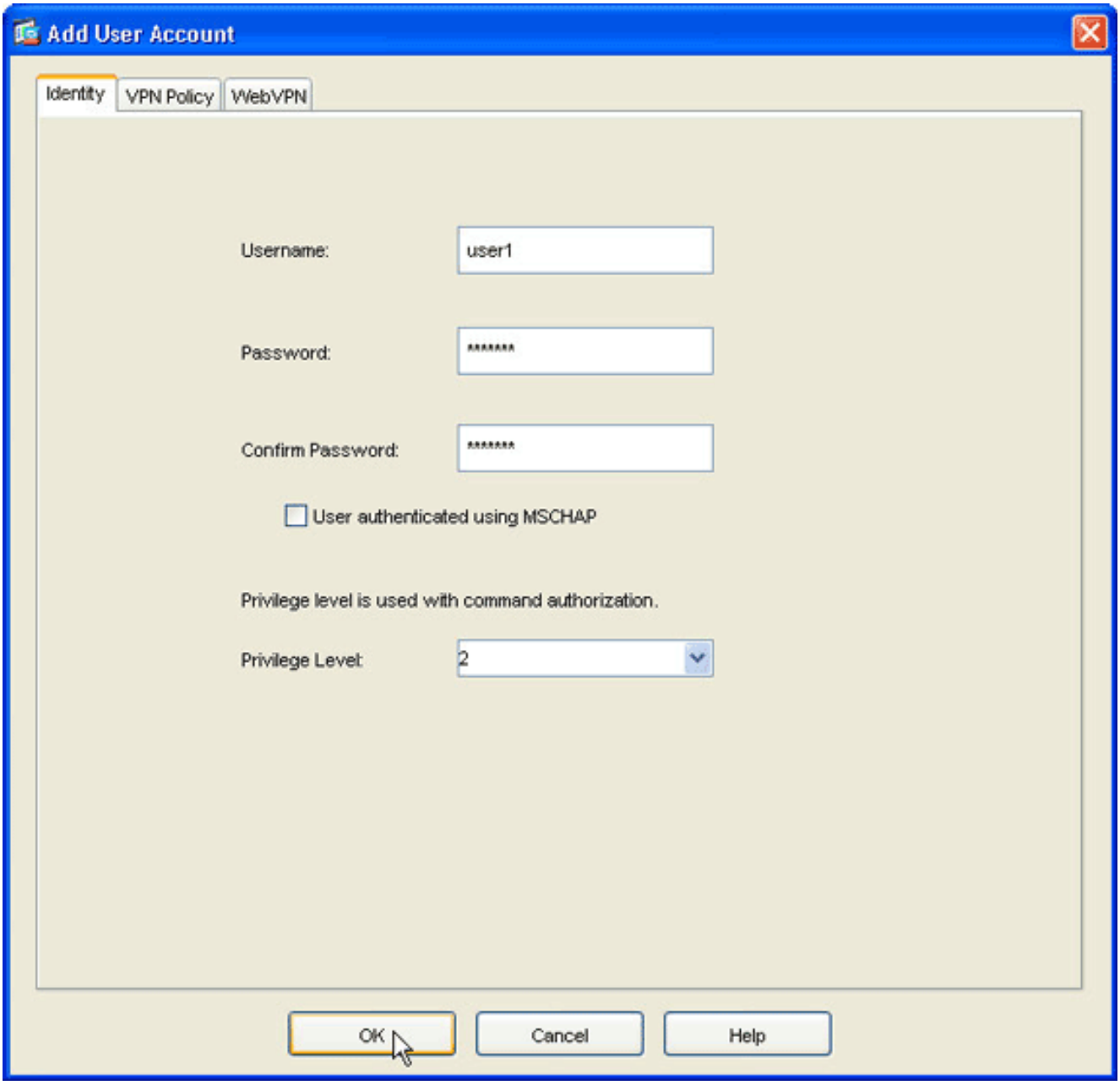
Étape 5. Créer un utilisateur et ajouter cet utilisateur à la stratégie de groupe

Pour créer un utilisateur et l'ajouter à la stratégie de groupe, procédez comme suit :

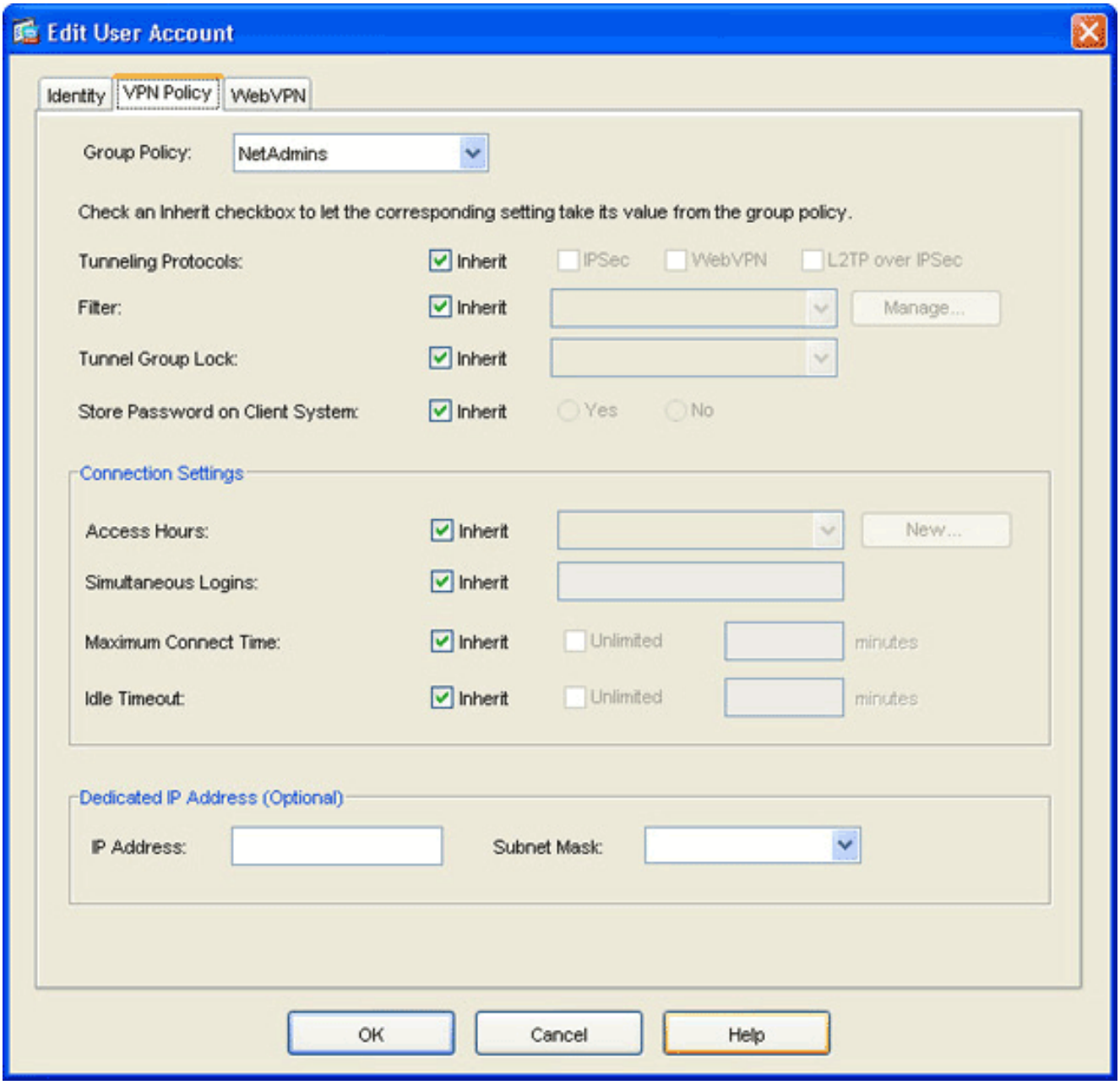
1. Développez **General**, puis choisissez **Users**.



2. Cliquez sur le bouton **Add.**La boîte de dialogue Ajouter un compte d'utilisateur s'affiche.



3. Entrez les valeurs du nom d'utilisateur, du mot de passe et des informations de privilège, puis cliquez sur l'onglet **Stratégie VPN**.



4. Cliquez sur la flèche de la liste déroulante **Stratégie de groupe**, puis sélectionnez la stratégie de groupe que vous avez créée à l'étape 3.Cet utilisateur hérite des caractéristiques et des stratégies WebVPN de la stratégie de groupe sélectionnée.
5. Cliquez sur **OK**, puis sur **Apply**.
6. Cliquez sur **Enregistrer**, puis **Oui** pour accepter les modifications.

Configuration VPN SSL client léger à l'aide de l'interface de ligne de commande

ASA
ASA Version 7.2(1) ! hostname ciscoasa domain-name default.domain.invalid enable password 8Ry2YjIyt7RRXU24 encrypted names ! interface Ethernet0/0

```
 nameif inside
 security-level 100
 ip address 10.1.1.1 255.255.255.0
!--- Output truncated  port-forward portforward 3044
10.2.2.2 telnet Telnet to R1
!--- Configure the set of applications that WebVPN
users !--- can access over forwarded TCP ports group-
policy NetAdmins internal
!--- Create a new group policy for enabling WebVPN
access group-policy NetAdmins attributes
 vpn-tunnel-protocol IPSec l2tp-ipsec webvpn
!--- Configure group policy attributes webvpn
  functions port-forward auto-download
!--- Configure group policies for WebVPN   port-forward
value portforward
!--- Configure port-forward to enable WebVPN
application access !--- for the new group policy  port-
forward-name value Secure Router Access
!--- Configure the display name that identifies TCP
port !--- forwarding to end users username user1
password tJsDL6po9m1UFs.h encrypted
username user1 attributes
 vpn-group-policy NetAdmins
!--- Create and add User(s) to the new group policy
http server enable http 0.0.0.0 0.0.0.0 DMZ no snmp-
server location no snmp-server contact snmp-server
enable traps snmp authentication linkup linkdown
coldstart tunnel-group NetGroup type webvpn
tunnel-group NetGroup general-attributes
 default-group-policy NetAdmins
!--- Create a new tunnel group and link it to the group
policy telnet timeout 5 ssh timeout 5 console timeout 0
! class-map inspection_default match default-
inspection-traffic ! ! policy-map type inspect dns
preset_dns_map parameters message-length maximum 512
policy-map global_policy class inspection_default
inspect dns preset_dns_map inspect ftp inspect h323
h225 inspect h323 ras inspect netbios inspect rsh
inspect rtsp inspect skinny inspect esmtp inspect
sqlnet inspect sunrpc inspect tftp inspect sip inspect
xdmcp ! service-policy global_policy global webvpn
 enable outside
!--- Enable Web VPN on Outside interface port-forward
portforward 3044 10.2.2.2 telnet Telnet to R1 prompt
hostname context
```

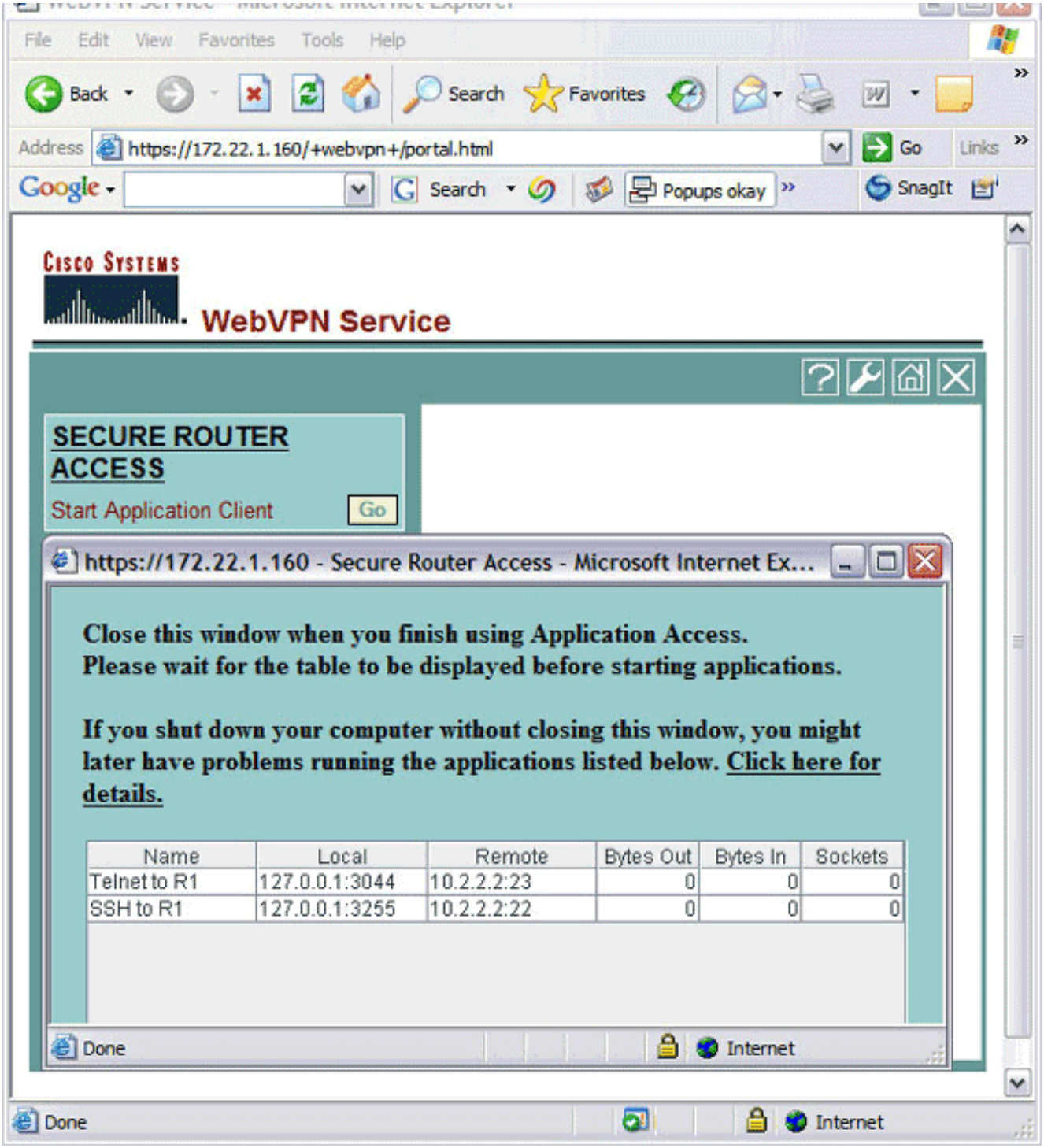
Vérification

Utilisez cette section pour vérifier que votre configuration fonctionne correctement.

Procédure

Cette procédure décrit comment déterminer la validité de la configuration et comment la tester.

1. Àpartir d'une station de travail client, saisissez **https:// *outside_ASA_IP Address*** ; où *outside_ASA_IPAddress* est l'URL SSL de l'ASA.Une fois le certificat numérique accepté et l'utilisateur authentifié, la page Web du service Web WebVPN s'affiche.

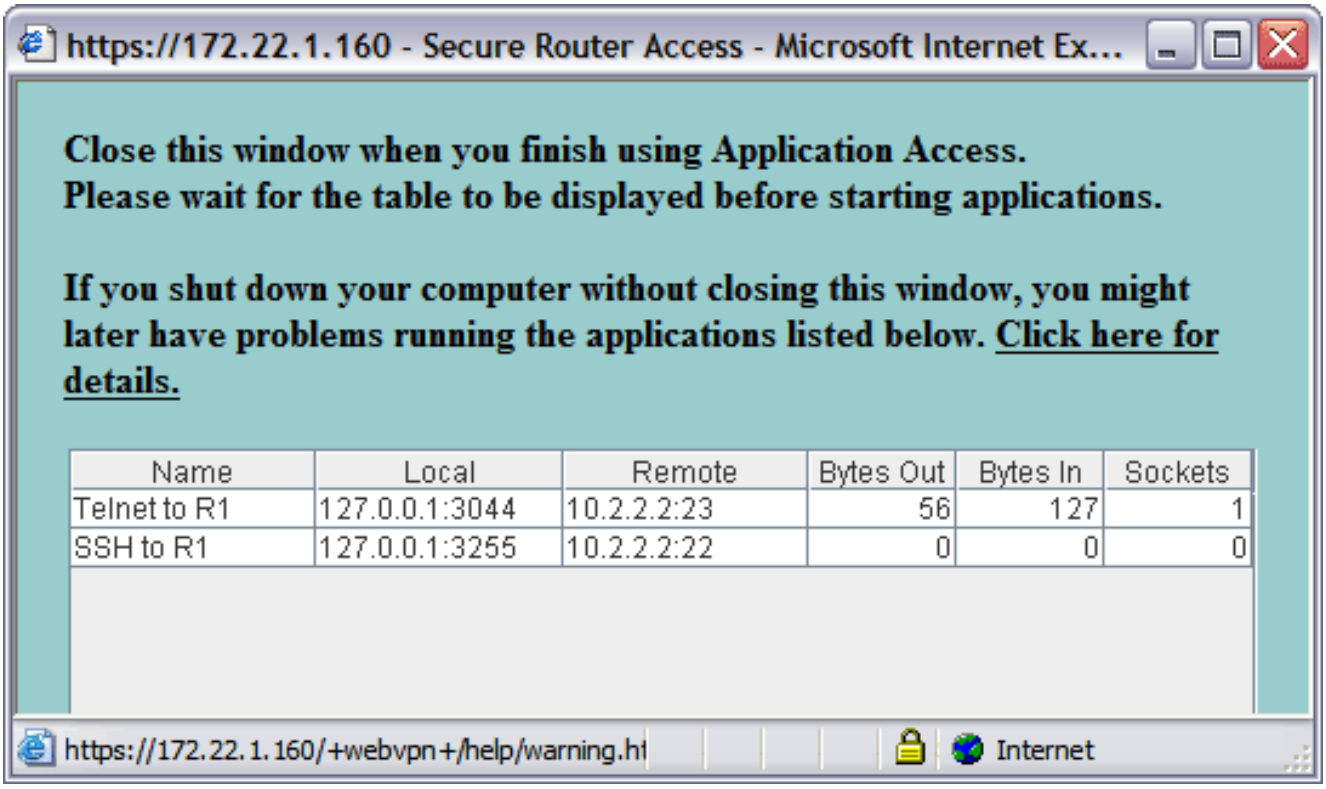


L'adresse et les informations de port nécessaires pour accéder à l'application apparaissent dans la colonne locale. Les colonnes Octets sortants et Octets entrants n'affichent aucune activité car l'application n'a pas été appelée pour le moment.

2. Utilisez l'invite DOS ou une autre application Telnet pour démarrer une session Telnet.
3. À l'invite de commandes, entrez **telnet 127.0.0.1 3044**.**Remarque :** cette commande fournit un exemple de la façon d'accéder au port local affiché dans l'image de page Web du service Web Web WebVPN de ce document. *La commande n'inclut pas de deux-points (:).* Tapez la commande comme décrit dans ce document.L'ASA reçoit la commande sur la session sécurisée, et comme il stocke une carte des informations, l'ASA sait immédiatement ouvrir la session Telnet sécurisée sur le périphérique
mappé.

Une fois que vous avez entré votre nom d'utilisateur et votre mot de passe, l'accès au périphérique est terminé.

4. Afin de vérifier l'accès au périphérique, vérifiez les colonnes Octets sortants et Octets entrants, comme indiqué dans cette image
:



Commandes

Plusieurs **commandes show sont associées à WebVPN.** Vous pouvez exécuter ces commandes dans l'interface de ligne de commande (CLI) afin d'afficher les statistiques et autres informations. Pour obtenir des informations détaillées à propos des commandes **show, reportez-vous à** Vérification de la configuration de WebVPN.

Note : L'outil Interpréteur de sortie (clients enregistrés uniquement) (OIT) prend en charge

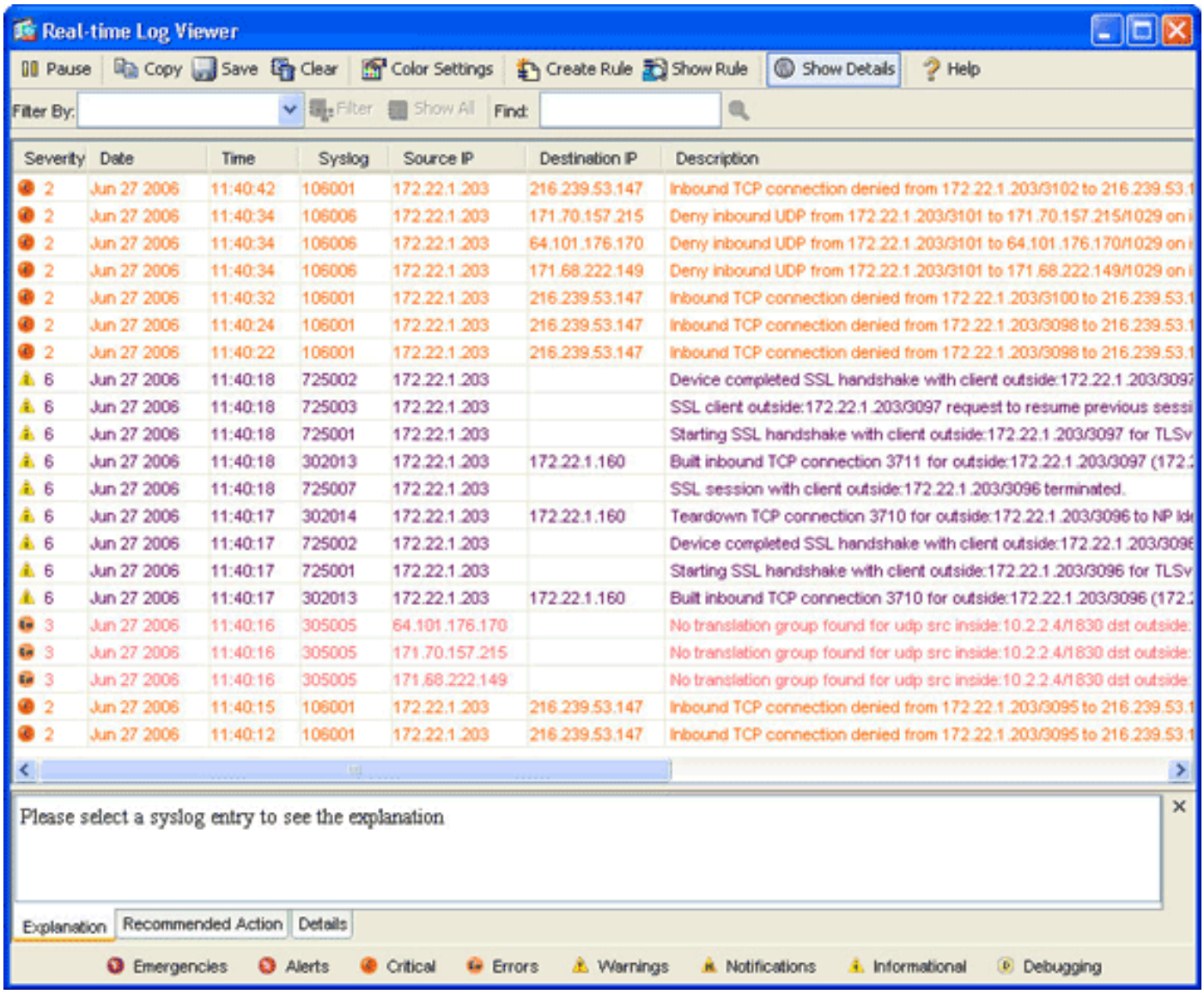
certaines commandes **show**. Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show .**

Dépannage

Utilisez cette section pour dépanner votre configuration.

Le processus de connexion SSL est-il terminé ?

Une fois que vous vous connectez à l'ASA, vérifiez si le journal en temps réel indique la fin de la connexion SSL.

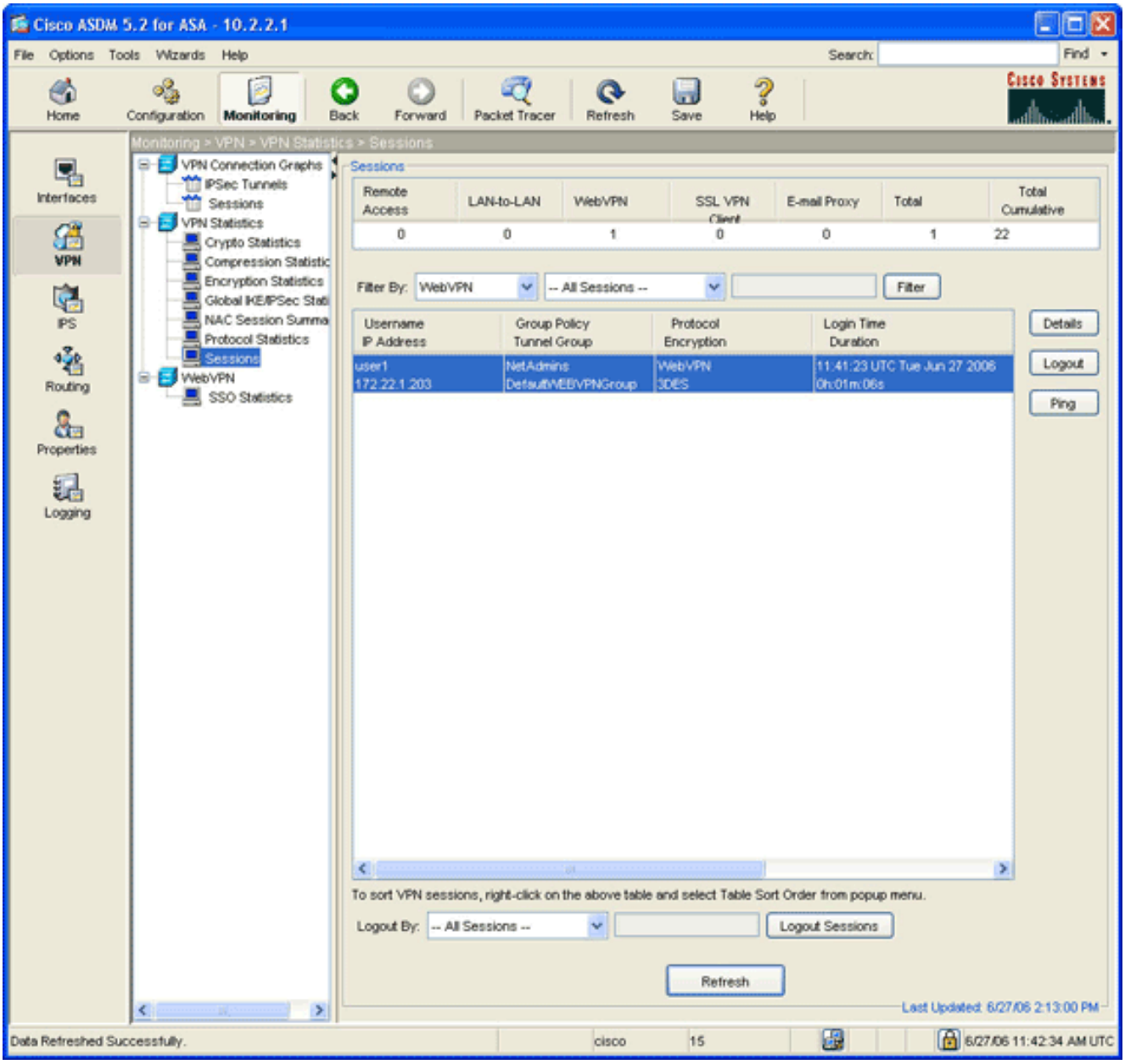


Le client léger VPN SSL est-il fonctionnel ?

Afin de vérifier que le client léger VPN SSL fonctionne, procédez comme suit :

1. Cliquez sur **Surveillance**, puis sur **VPN**.
2. Développez **VPN Statistics**, puis cliquez sur **Sessions**.Votre session client léger VPN SSL doit apparaître dans la liste des sessions. Assurez-vous de filtrer par WebVPN comme indiqué dans cette image

:



Commandes

Plusieurs commandes **debug sont associées à WebVPN.** Pour obtenir des informations détaillées à propos de ces commandes, reportez-vous à Utilisation des commandes Debug WebVPN.

Remarque : l'utilisation des commandes **debug** peut avoir un impact négatif sur votre périphérique Cisco. Avant d'utiliser les commandes **debug , référez-vous à la section** Informations importantes sur les commandes Debug.

Informations connexes

- Exemple de configuration d'un VPN SSL sans client (WebVPN) sur ASA
- Exemple de configuration d'un client VPN SSL (SVC) sur ASA avec ASDM
- Dispositifs de sécurité adaptatifs de la gamme Cisco ASA 5500
- Exemple de configuration d'ASA avec WebVPN et authentification unique à l'aide d'ASDM et de NTLMv1

- Support et documentation techniques - Cisco Systems