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 de datagramme utilisateur (UDP) 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 de VPN SSL (SVC) à une station distante, ou vous pouvez retirer le client une fois que la session sécurisée est fermée.Référez-vous au client de VPN SSL (SVC) sur l'ASA avec l'exemple de configuration ASDM afin de se renseigner plus sur le client de VPN SSL.

Ce document explique une configuration simple pour le VPN SSL de client léger sur l'appliance de sécurité adaptable (ASA). La configuration permet un utilisateur au telnet sécurisé à un routeur situé sur l'intérieur de l'ASA. La configuration dans ce document est prise en charge pour la version 7.x et ultérieures ASA.

Conditions préalables

Conditions requises

Avant que vous tentiez cette configuration, assurez-vous que vous répondez à ces exigences pour les stations de client distant :

- navigateur Web SSL-activé
- Version 1.4 ou ultérieures de Javas JRE de SUN
- Témoins activés
- Bloqueurs de fenêtres instantanées désactivés
- Privilèges d'administrateur locaux (non exigés mais fortement suggérés)

Remarque: La dernière version de Javas JRE de SUN est disponible comme téléchargement gratuit du site Web de Javas .

Composants utilisés

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 Permettre l'accès HTTPS pour l'ASDM afin de permettre l'ASA d'être configuré par l'ASDM.
- Logiciel Cisco Adaptive Security Appliance Version 7.2(1)
- Professionnel de Microsoft Windows XP (client distant de fournisseur de services 2)

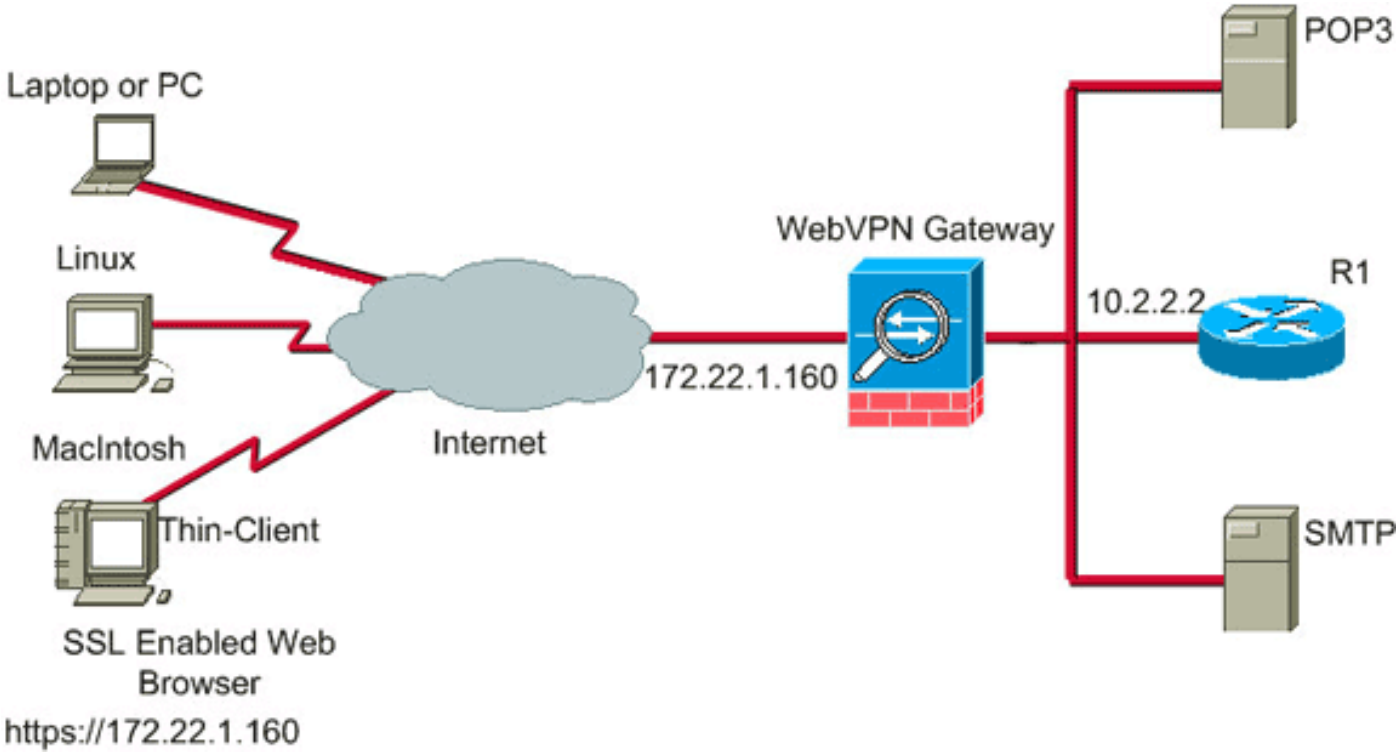
Les informations de ce document ont été élaborées dans un environnement de laboratoire. Tous

les périphériques utilisés dans ce document ont été remis à l'état initial 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.

Quand un client distant initie une session avec l'ASA, le client télécharge un petit applet Java au poste de travail. Le client est présenté avec une liste de ressources préconfigurées.



Conventions

Pour plus d'informations sur les conventions de documents, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Informations générales

Afin de commencer une session, le client distant ouvre un navigateur SSL à l'interface extérieure de l'ASA. Après que la session soit établie, l'utilisateur peut utiliser les paramètres configurés sur l'ASA pour appeler n'importe quel telnet ou accès d'application. Les proxys ASA la connexion sécurisée et permet l'accès client au périphérique.

Remarque: Les listes d'accès en entrée ne sont pas nécessaires pour ces connexions parce que l'ASA se rend déjà compte de ce qui constitue une session juridique.

Configuration de VPN SSL de client léger utilisant l'ASDM

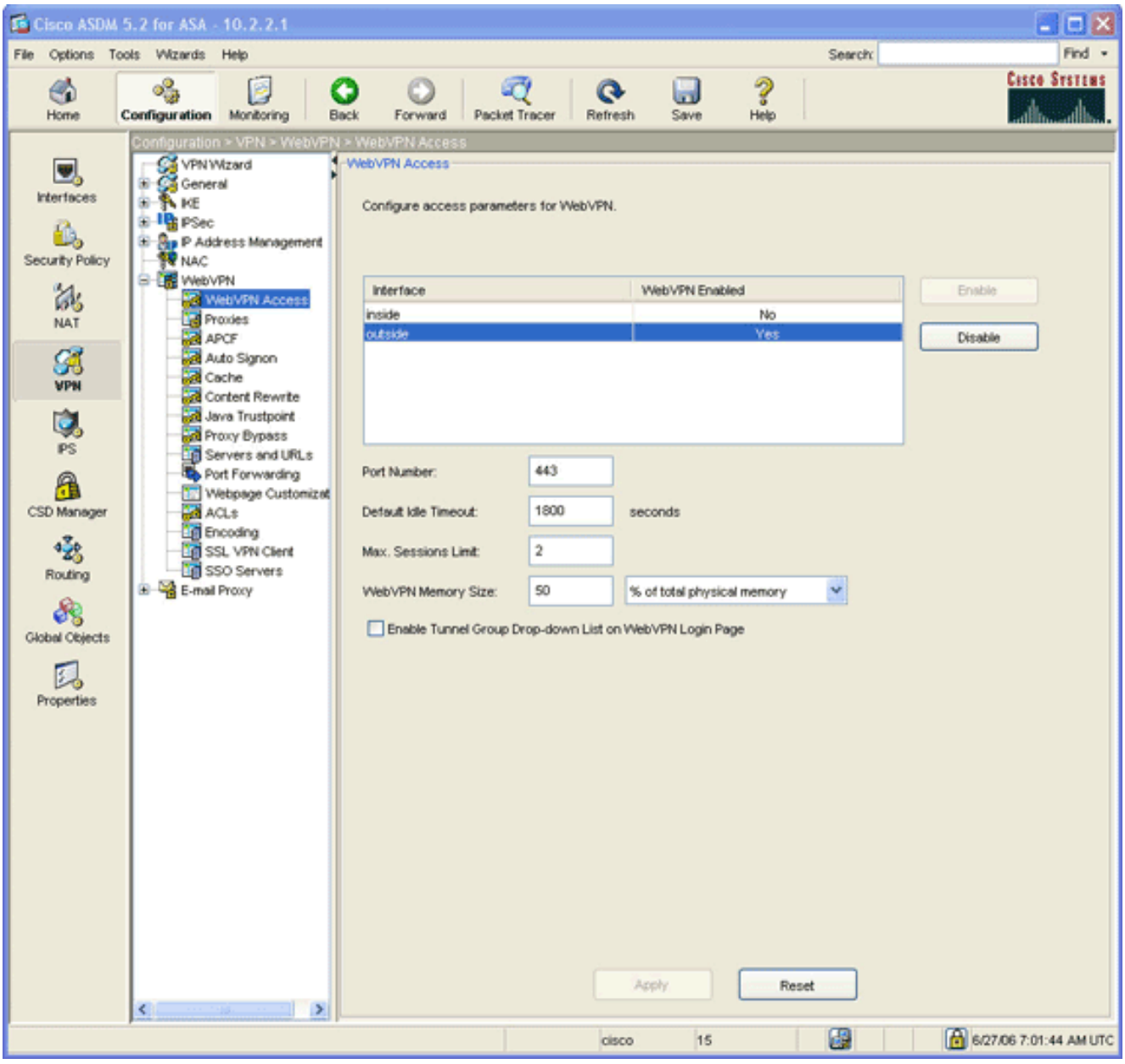
Afin de configurer le VPN SSL de client léger sur l'ASA, terminez-vous ces étapes :

1. Webvpn d'enable sur l'ASA
2. Configurez les caractéristiques de transmission du port
3. Créez une stratégie de groupe et liez-la à la liste de transmission du port (créée dans étape 2)
4. Créez un groupe de tunnel et liez-le à la stratégie de groupe (créée dans étape 3)
5. Créez un utilisateur et ajoutez qu'utilisateur à la stratégie de groupe (créée dans étape 3)

Étape 1. Webvpn d'enable sur l'ASA

Afin d'activer le webvpn sur l'ASA, terminez-vous ces étapes :

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

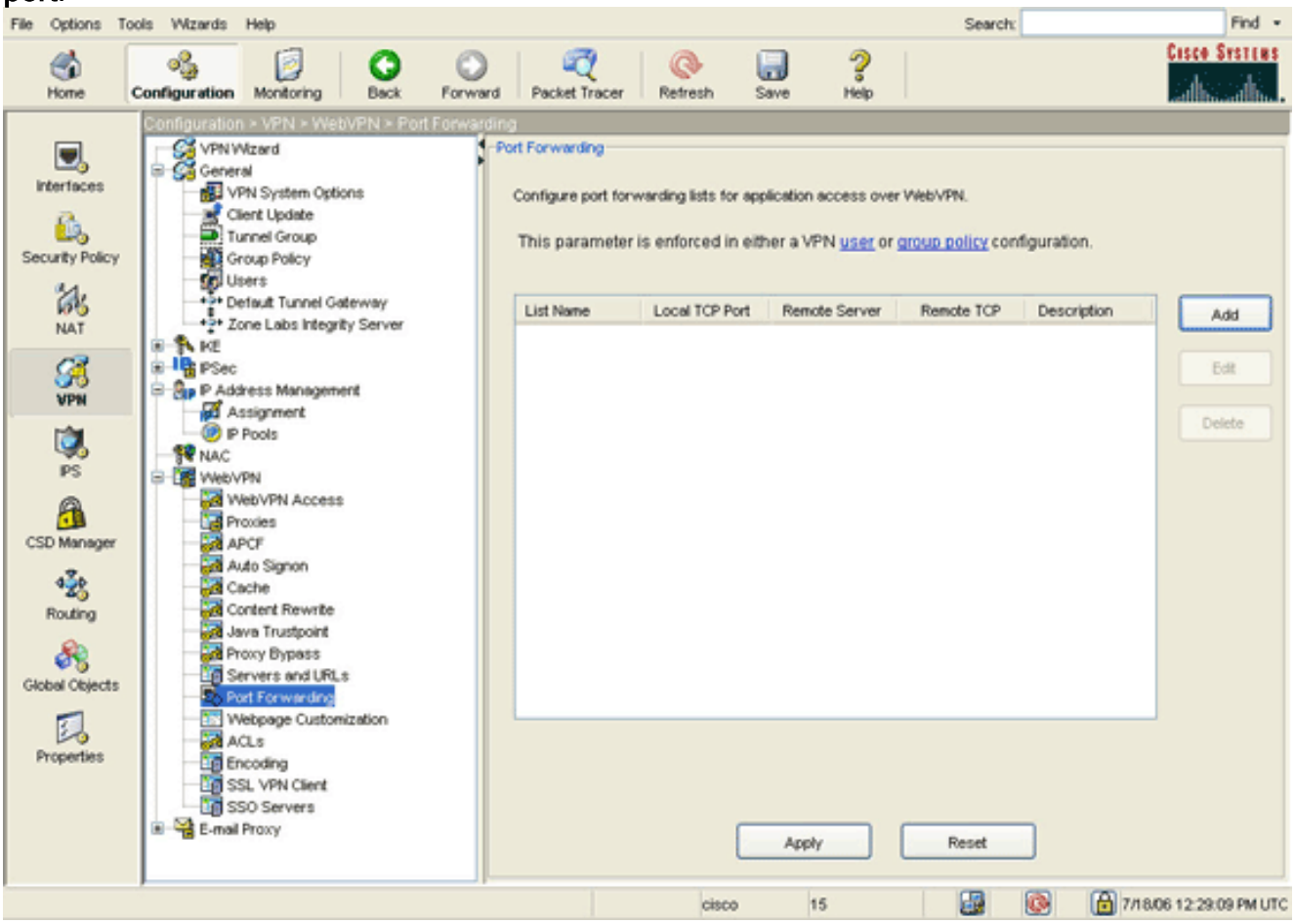


3. Mettez en valeur l'interface, et cliquez sur l'**enable**.
4. Cliquez sur Apply, cliquez sur la **sauvegarde**, et puis cliquez sur **oui** pour recevoir les modifications.

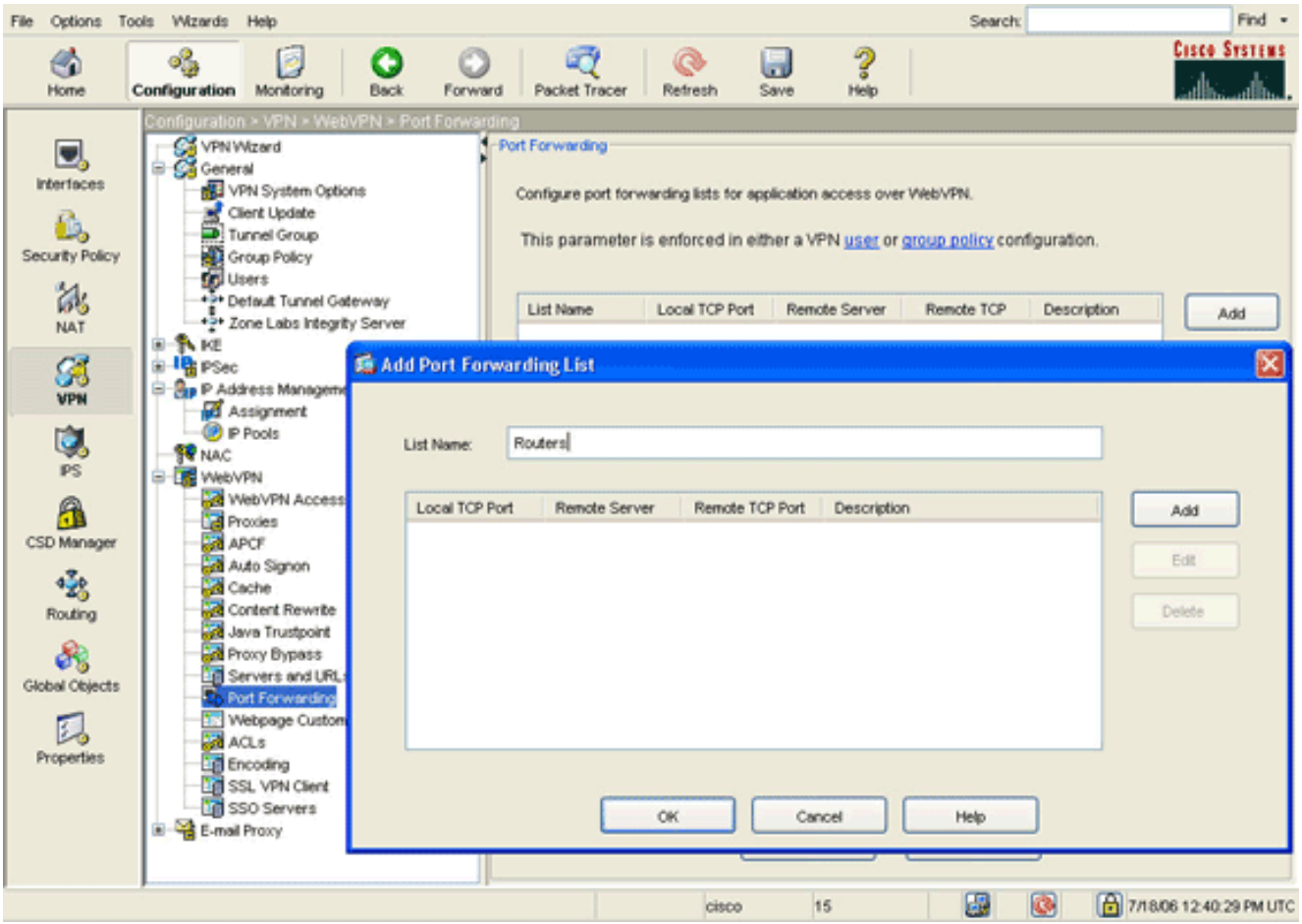
Étape 2. Configurez les caractéristiques de transmission du port

Afin de configurer des caractéristiques de transmission du port, terminez-vous ces étapes :

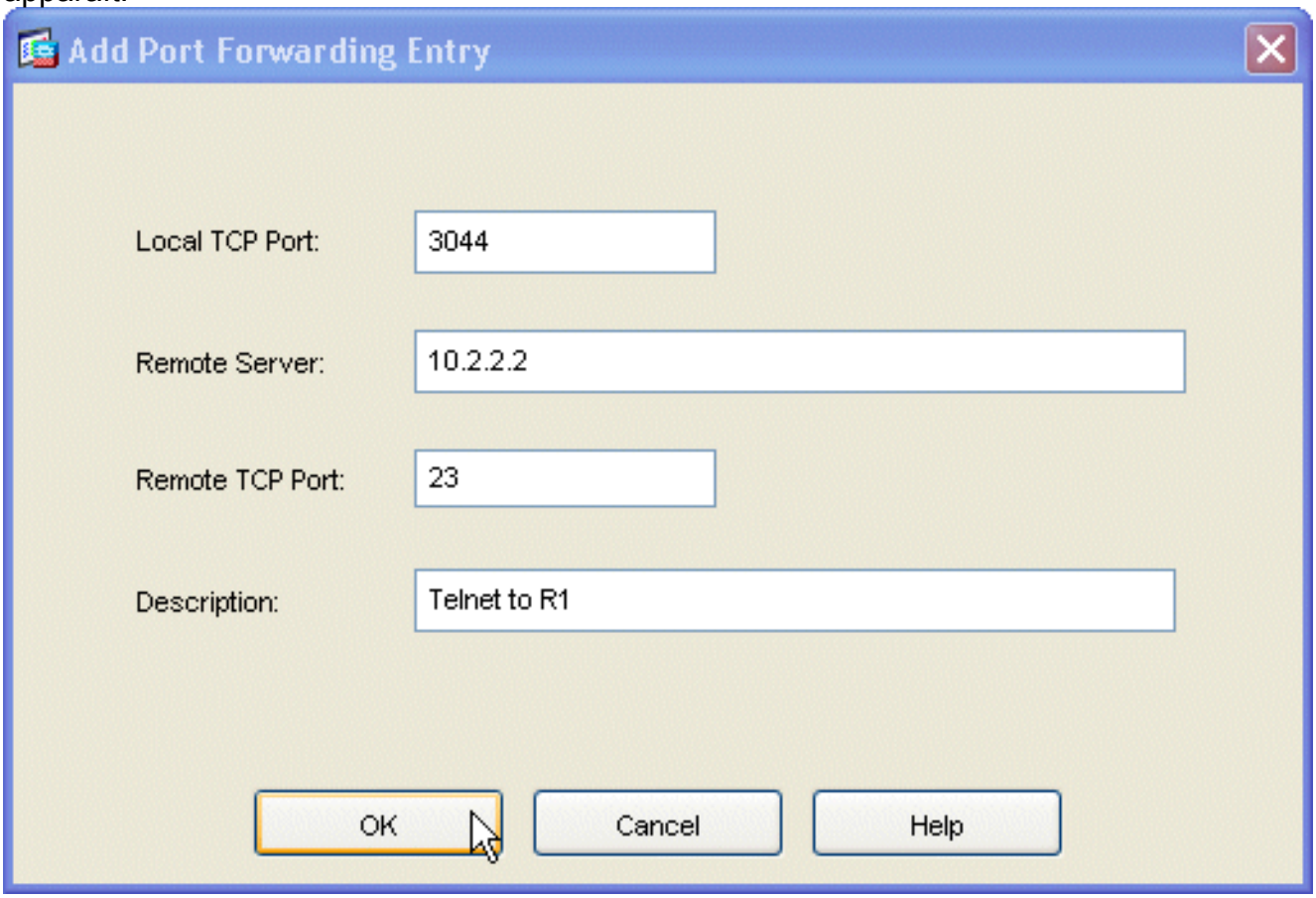
1. Développez le **webvpn**, et choisissez la **transmission du port**.



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



3. Dans la boîte de dialogue de liste de transmission du port d'ajouter, écrivez un nom de liste, et cliquez sur Add.La boîte de dialogue d'entrée de transmission du port d'ajouter apparaît.



4. Dans la boîte de dialogue d'entrée de transmission du port d'ajouter, entrez ces options :Dans le domaine de port TCP local, introduisez un numéro de port ou recevez la valeur par

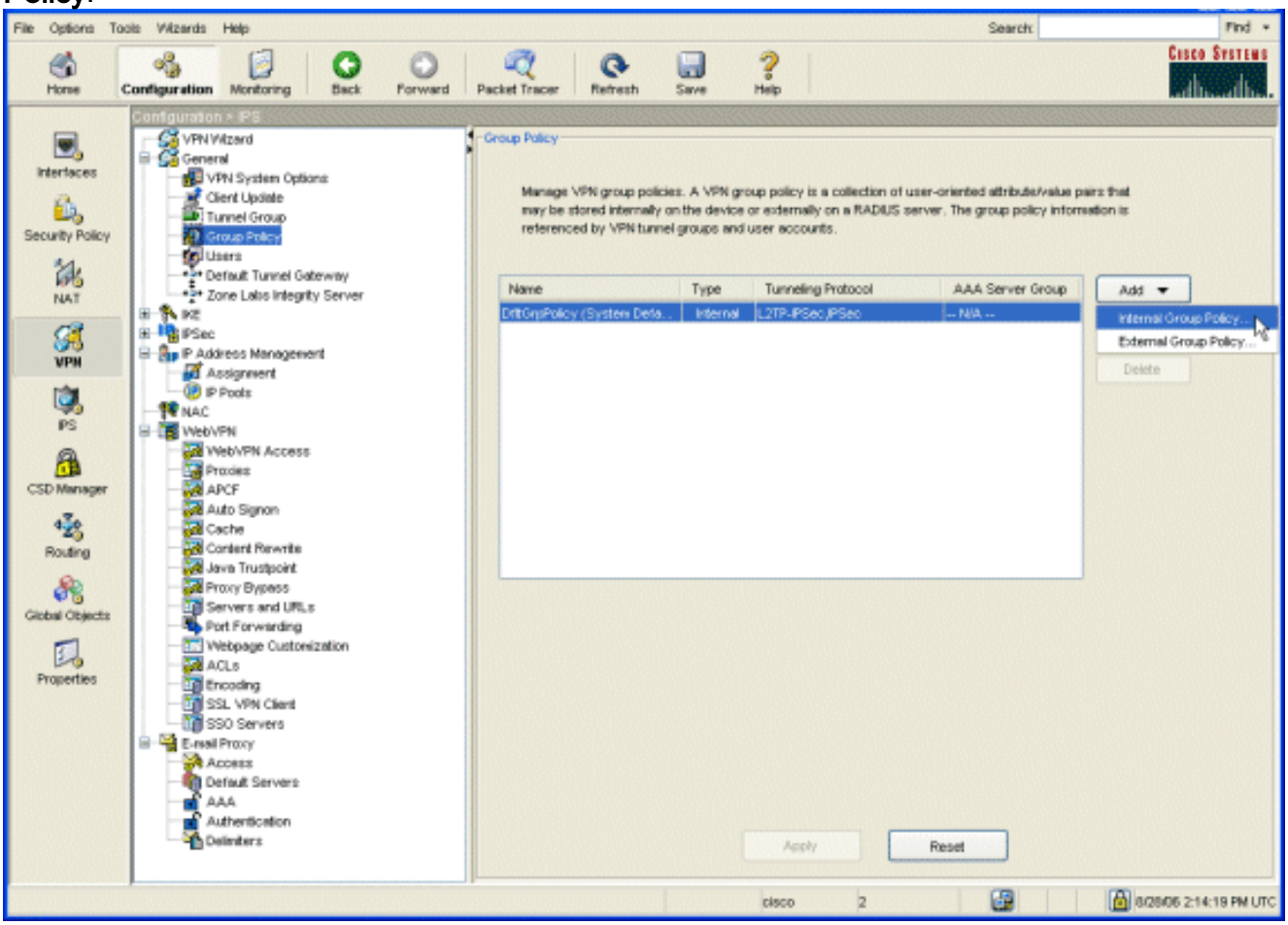
défaut.La valeur que vous écrivez peut être tout nombre à partir de 1024 à 65535.Dans le domaine de serveur distant, écrivez une adresse IP.Cet exemple utilise l'adresse du routeur.Dans le domaine de port TCP distant, introduisez un numéro de port.Cet exemple utilise le port 23.Dans le champ description, écrivez une description, et cliquez sur OK.

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

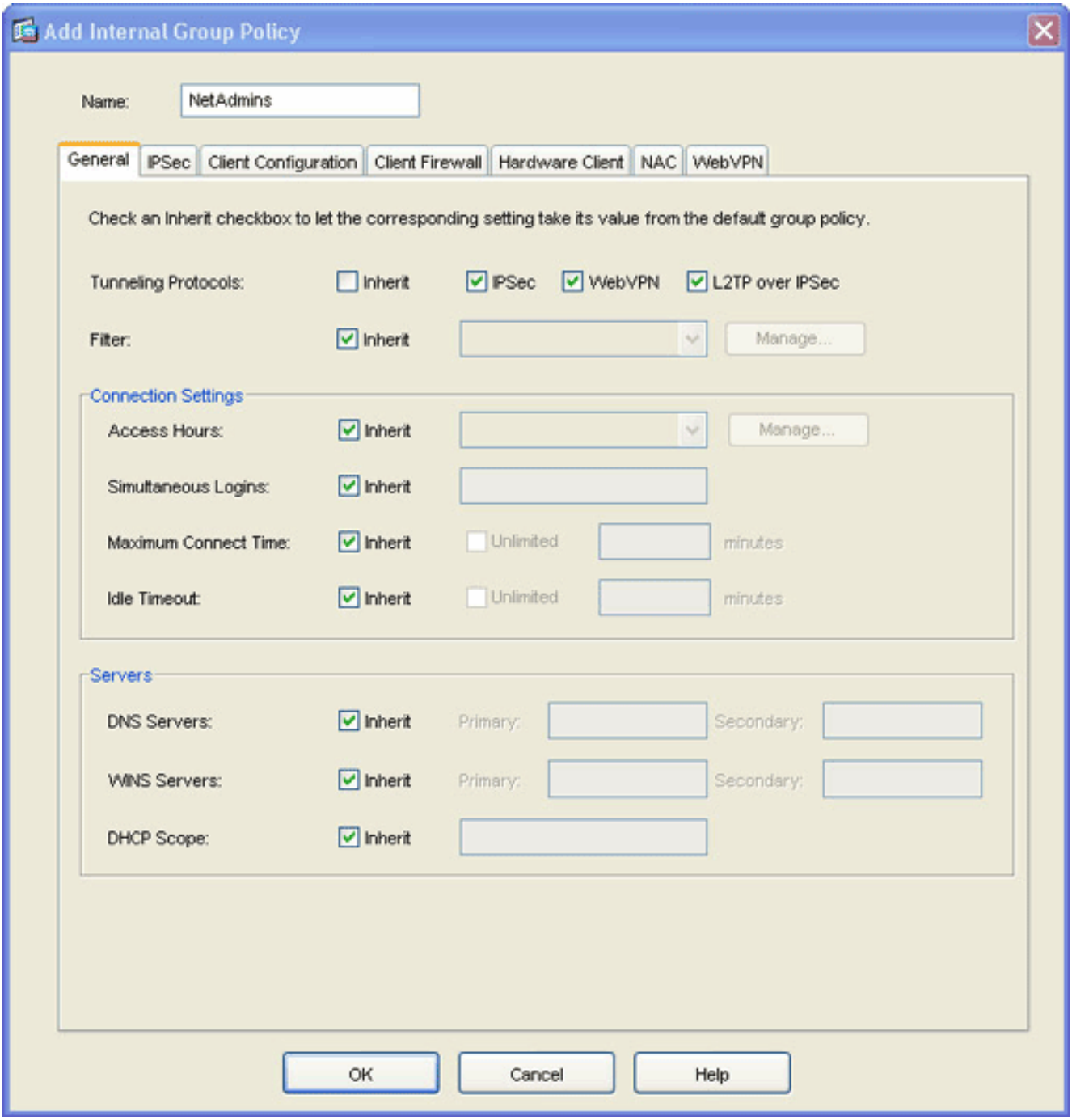
Étape 3. Créez une stratégie de groupe et liez-la à la liste de transmission du port

Afin de créer une stratégie de groupe et la lier à la liste de transmission du port, terminez-vous ces étapes :

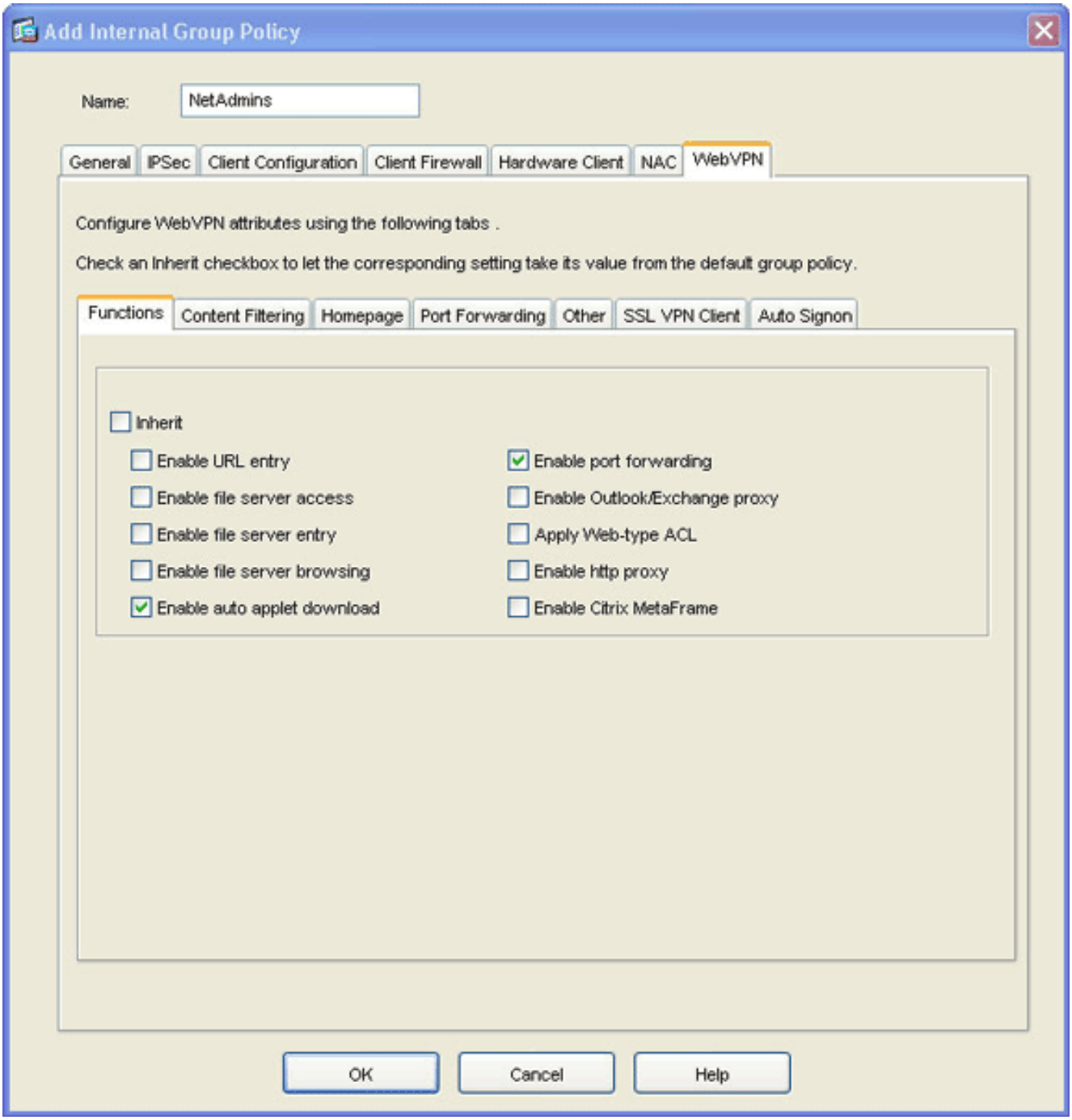
1. Développez **General**, puis choisissez **Group Policy**.



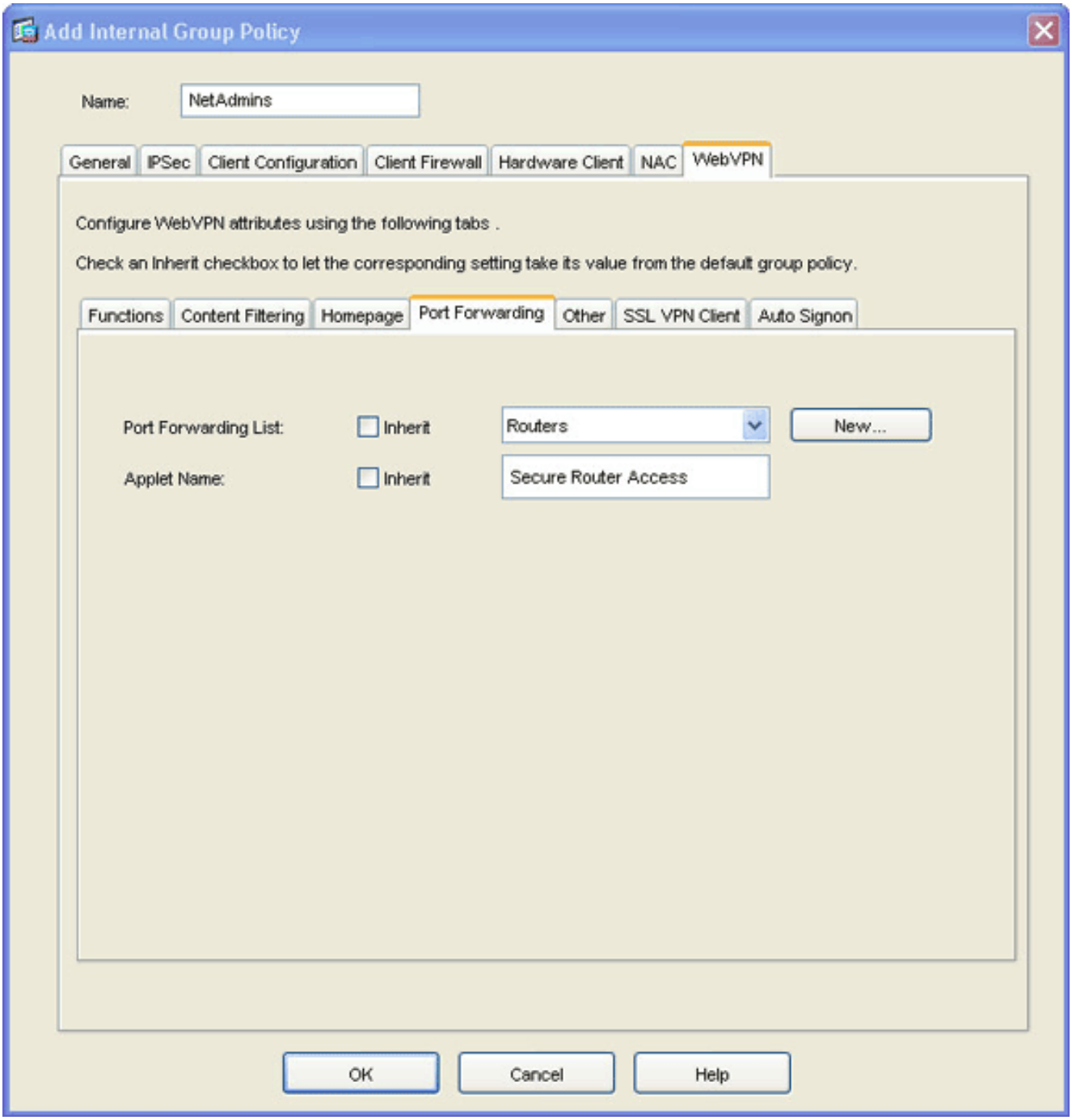
2. Cliquez sur **Add**, puis sélectionnez **Internal Group Policy**.La boîte de dialogue d'Add Internal Group Policy apparaît.



3. Écrivez un nom ou recevez le nom de stratégie de groupe par défaut.
4. Décochez la case Tunneling Protocols Inherit, et cochez la case de **webvpn**.
5. Cliquez sur l'onglet de **webvpn** situé en haut de la boîte de dialogue, et puis cliquez sur l'onglet de **fonctions**.
6. Décochez la case d'**héritage**, et cochez le **téléchargement automatique d'applet d'enable** et **activez les** cases de **transmission du port** suivant les indications de cette image :



7. Également dans l'onglet de webvpn, cliquez sur l'onglet de **transmission du port**, et décochez la liste de transmission du port **héritent de la**
case.



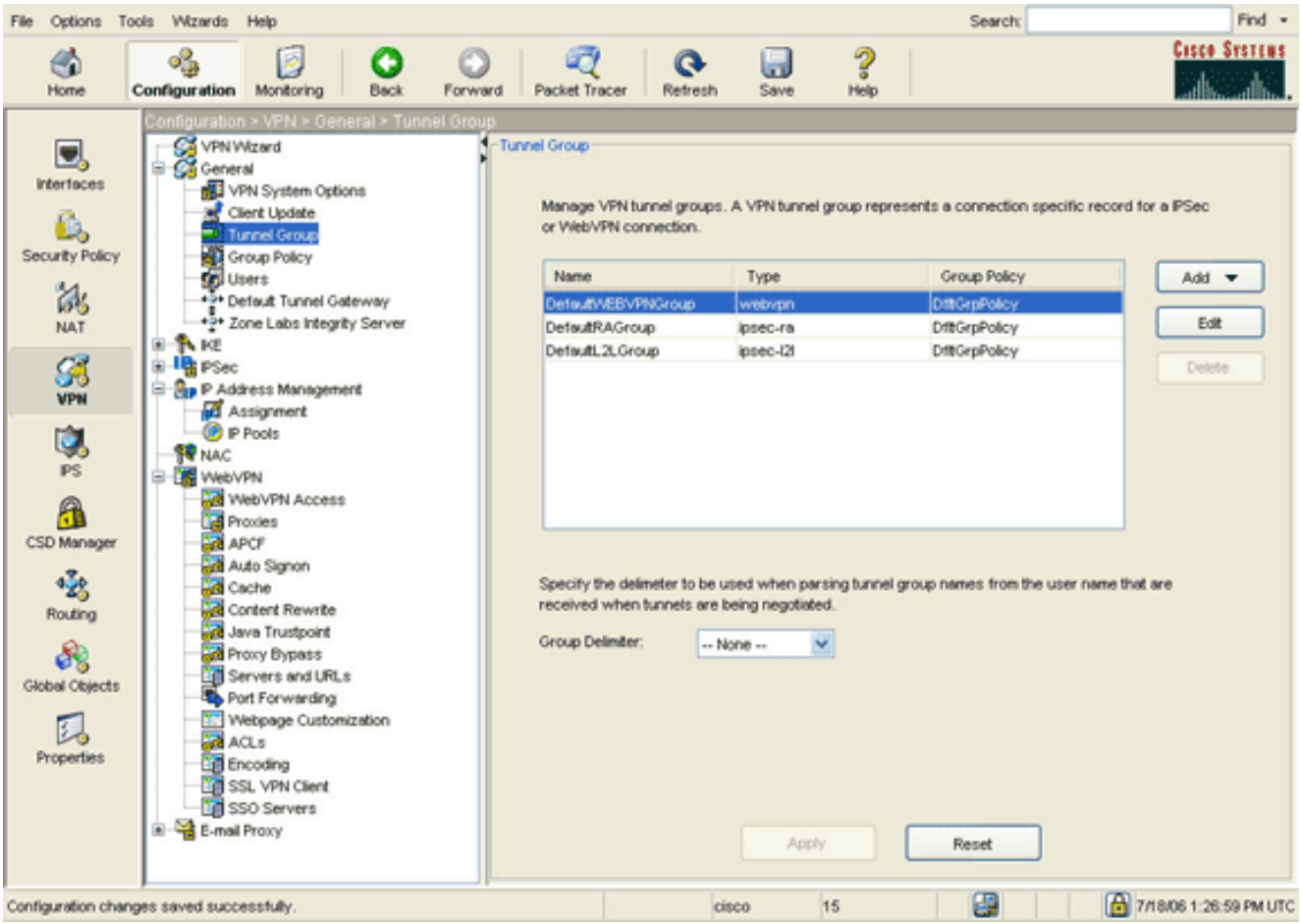
8. Cliquez sur la flèche déroulante de **liste de transmission du port**, et choisissez la liste de transmission du port que vous avez créée dans l'étape 2.
9. Décochez le nom d'applet **héritent de la** case, et changent le nom dans le champ texte.Le client affiche le nom d'applet sur la connexion.
10. Cliquez sur **OK**, puis sur **Apply**.
11. Cliquez sur **Save**, puis sur **Yes** pour accepter les modifications.

Étape 4. Créez un groupe de tunnel et liez-le à la stratégie de groupe

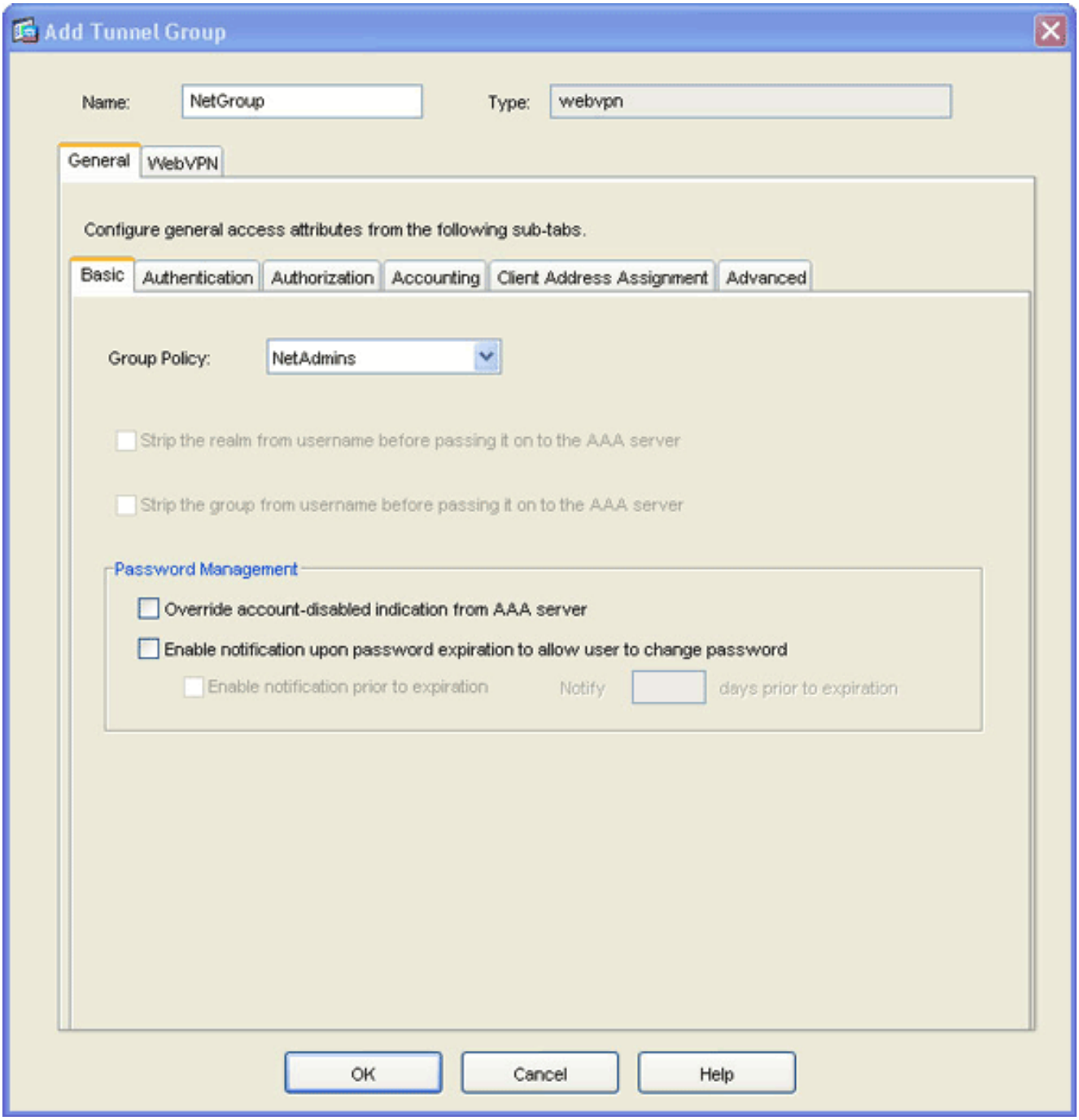
Vous pouvez éditer le groupe par défaut de tunnel de *DefaultWebVPNGroup* ou créer un nouveau groupe de tunnel.

Afin de créer un nouveau groupe de tunnel, terminez-vous ces étapes :

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



2. Cliquez sur **Add**, puis sélectionnez **WebVPN Access**.La boîte de dialogue de groupe de tunnel d'ajouter
apparaît.

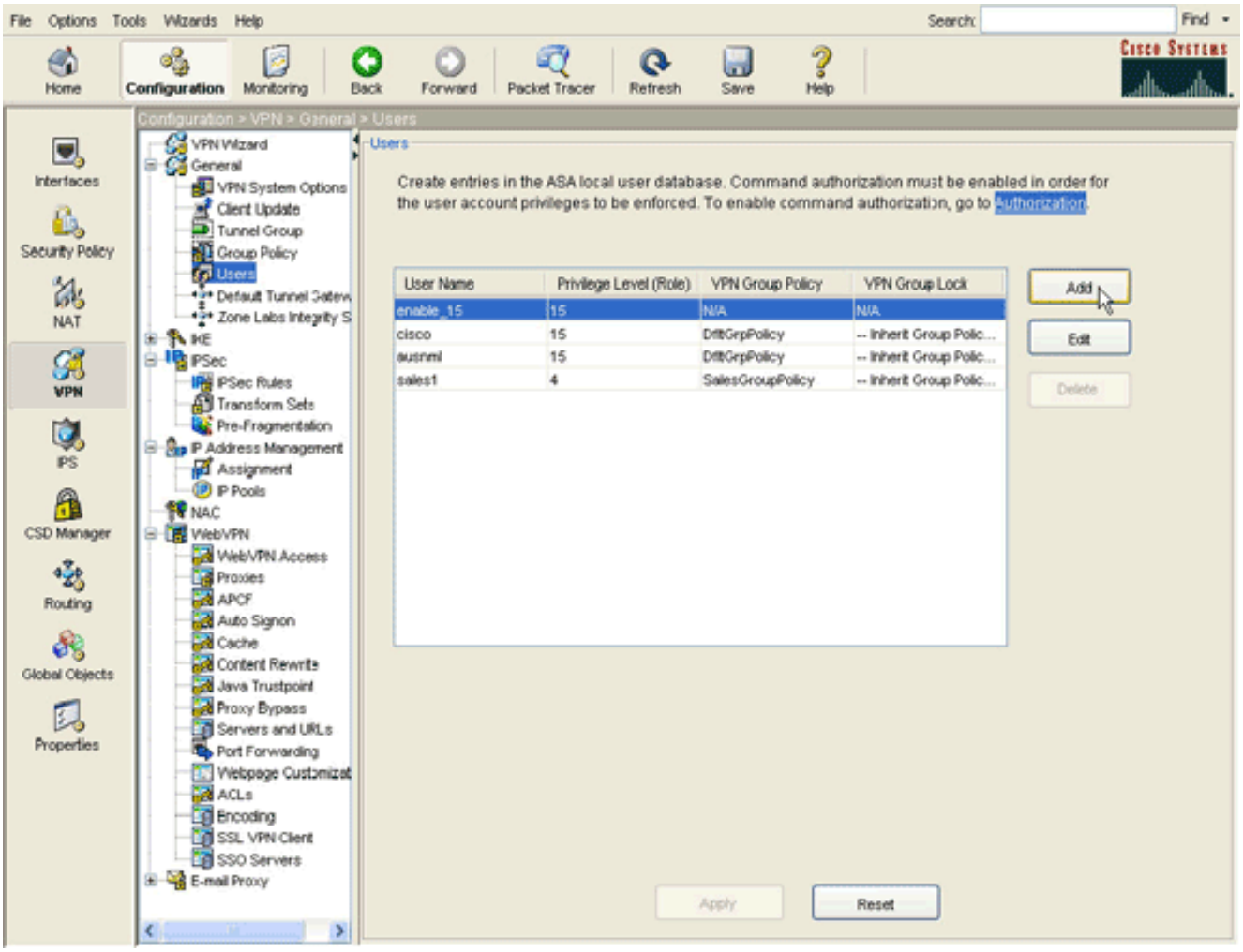


3. Écrivez un nom dans la zone d'identification.
4. Cliquez sur la flèche déroulante de **stratégie de groupe**, et choisissez la stratégie de groupe que vous avez créée dans l'étape 3.
5. Cliquez sur **OK**, puis sur **Apply**.
6. Cliquez sur **Save**, puis sur **Yes** pour accepter les modifications.Le groupe de tunnel, la stratégie de groupe, et les caractéristiques de transmission du port sont maintenant joints.

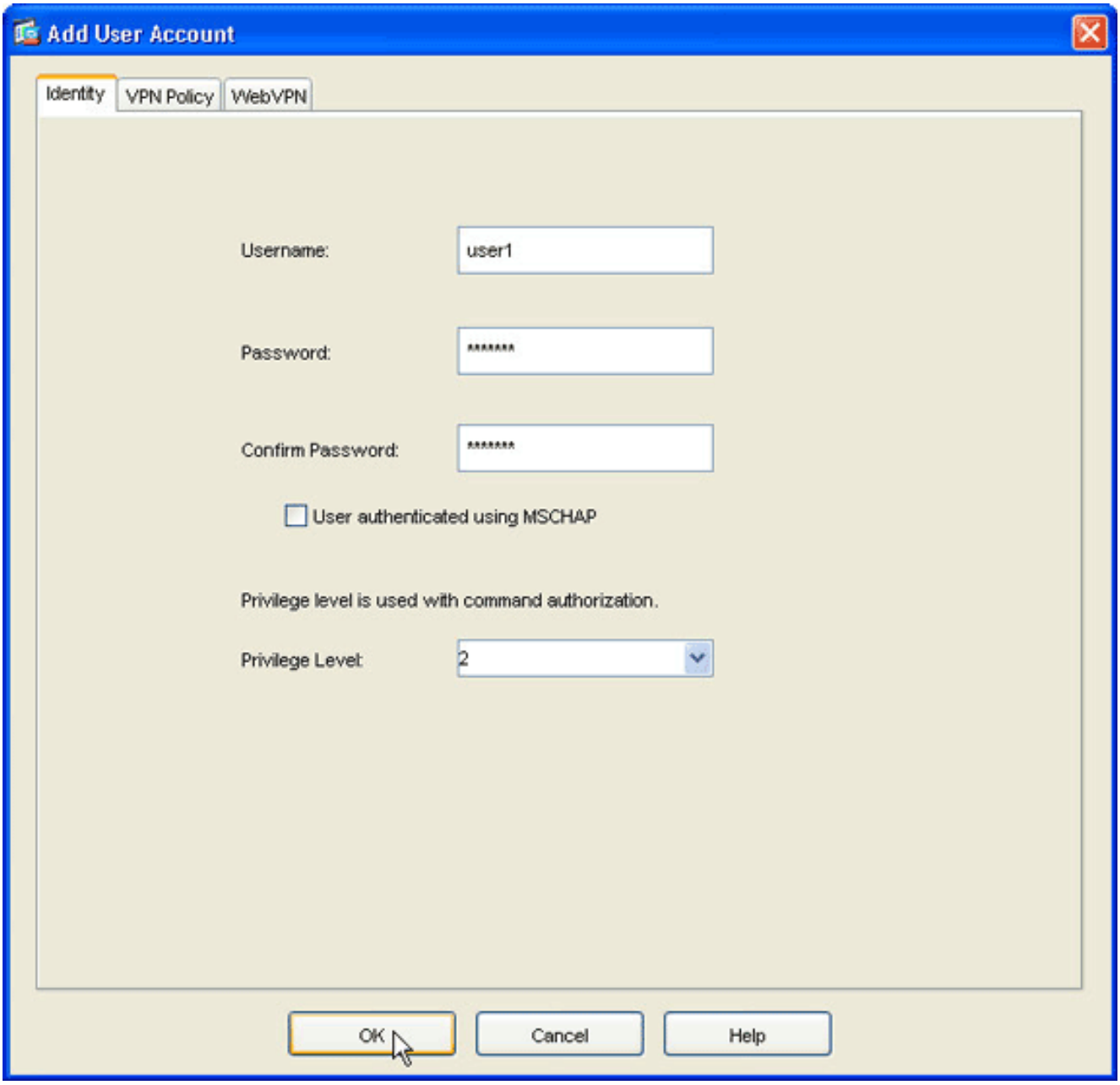
Étape 5. Créez un utilisateur et ajoutez cet utilisateur à la stratégie de groupe

Afin de créer un utilisateur et ajouter cet utilisateur à la stratégie de groupe, terminez-vous ces étapes :

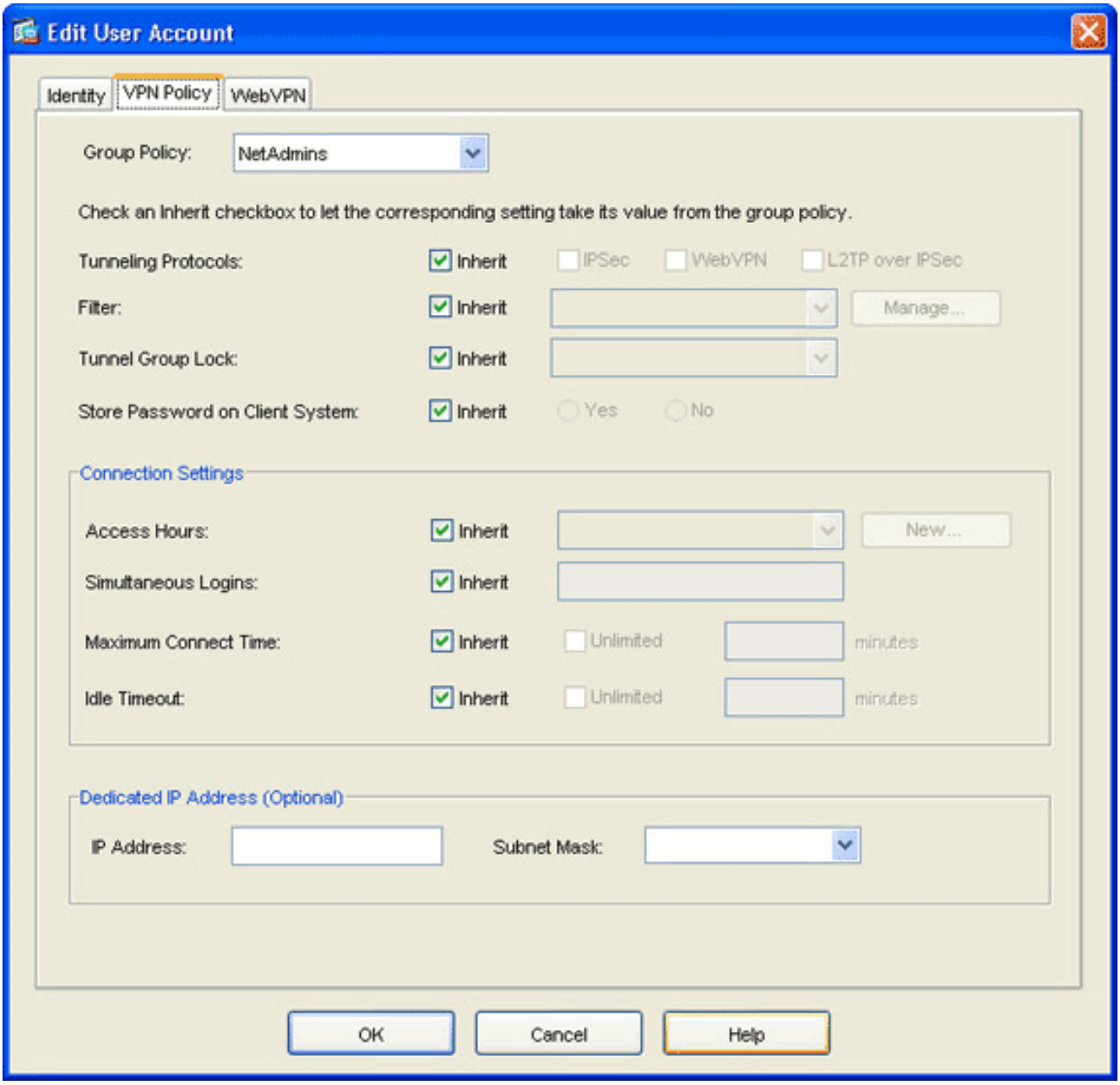
1. Développez **General**, puis choisissez **Users**.



2. Cliquez sur le bouton **Add**.La boîte de dialogue de compte utilisateur d'ajouter apparaît.



3. Écrivez les valeurs pour le nom d'utilisateur, le mot de passe, et les informations de privilège, et puis cliquez sur l'onglet de **règle VPN**.



4. Cliquez sur la flèche déroulante de **stratégie de groupe**, et choisissez la stratégie de groupe que vous avez créée dans l'étape 3.Cet utilisateur hérite des caractéristiques de webvpn et des stratégies de la stratégie de groupe sélectionné.
5. Cliquez sur **OK**, puis sur **Apply**.
6. **Sauvegarde de** clic, et recevoir alors **oui les** modifications.

Configuration de VPN SSL de client léger utilisant le CLI

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
```

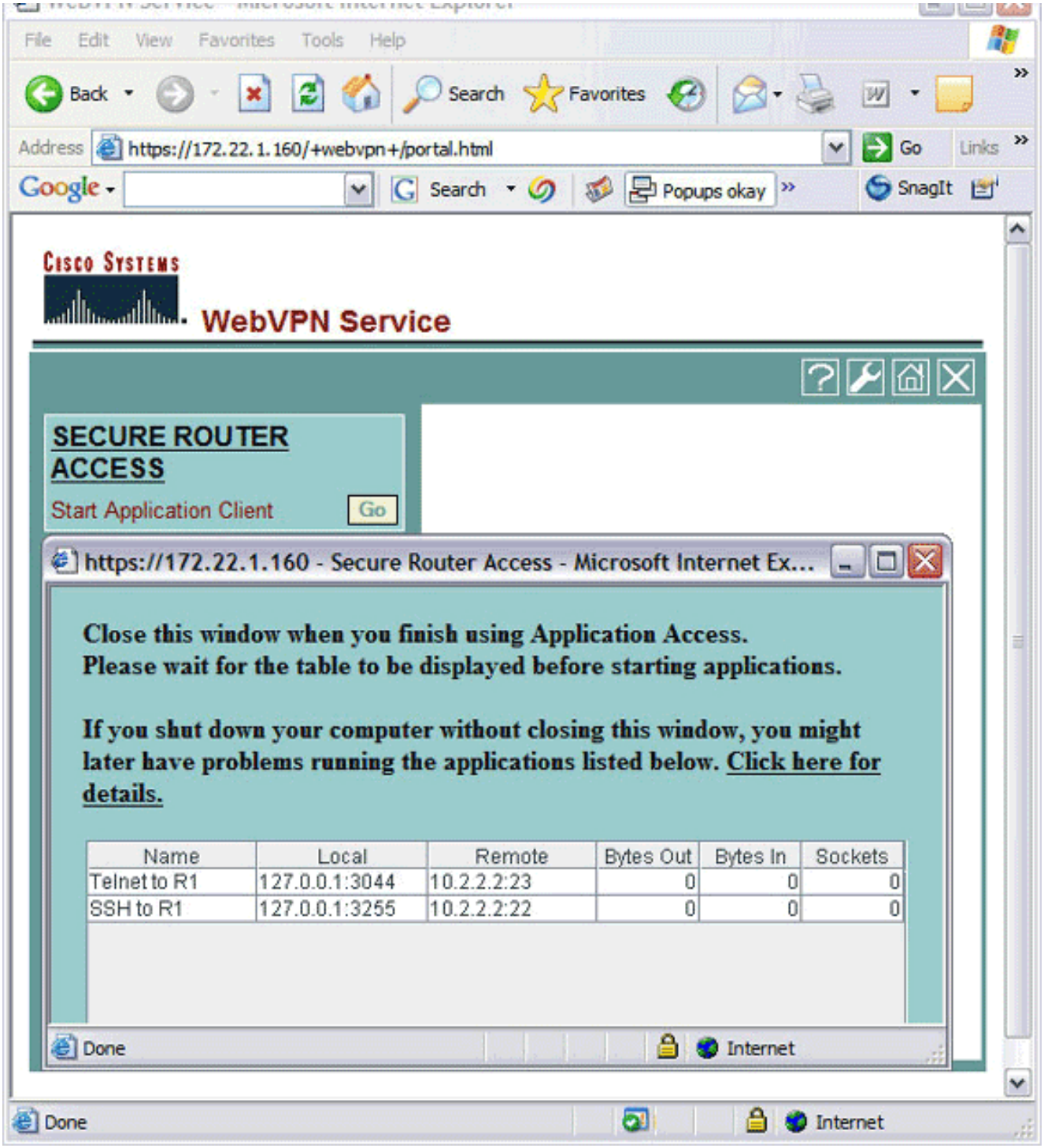
Vérifiez

Employez cette section pour vérifier que votre configuration fonctionne correctement.

Procédure

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

1. D'un poste de travail de client, introduisez l'***adresse d'outside_ASA_IP de*** **https://** ; là où les *outside_ASA_IPAddress* est l'URL SSL de l'ASA.Une fois que le certificat numérique est reçu, et l'utilisateur est authentifié, la page Web de service de webvpn paraît.

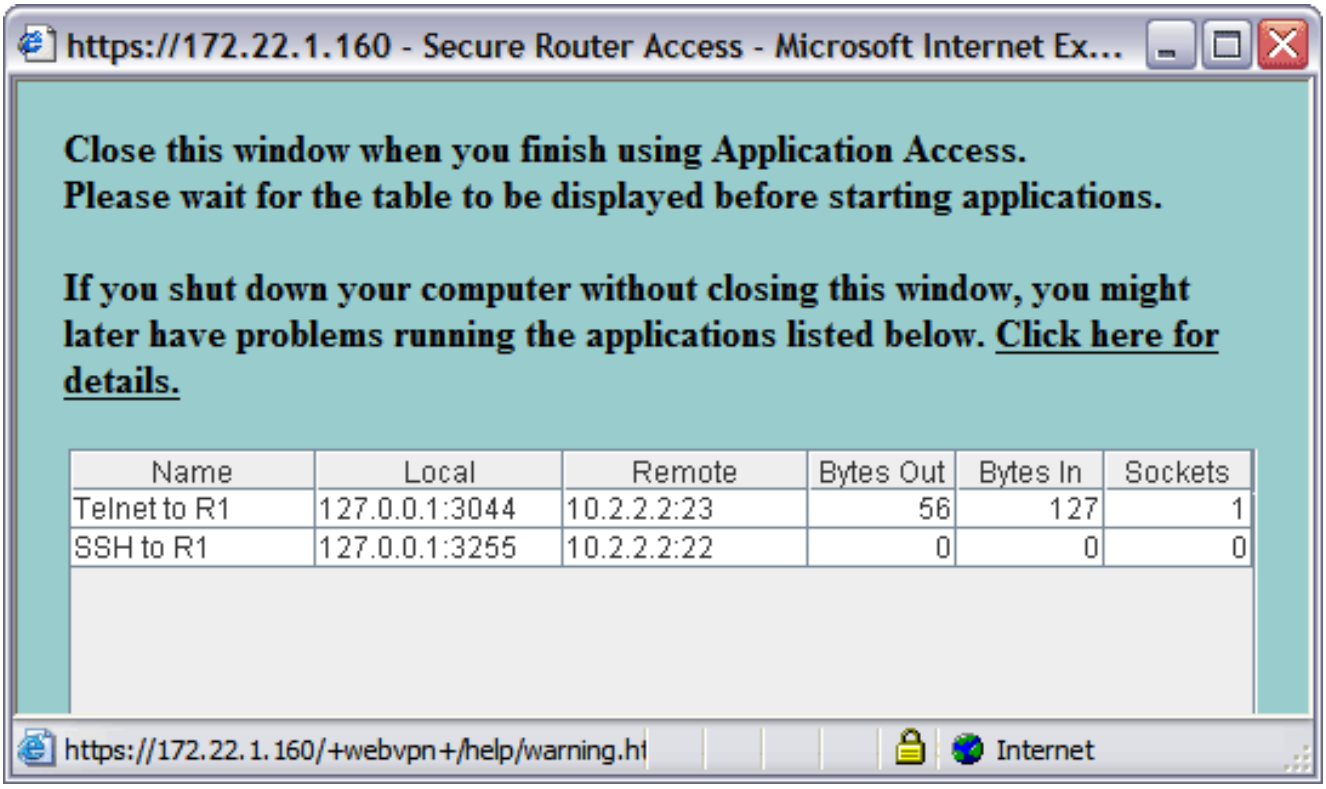


L'adresse et les informations requises de port pour accéder à l'application apparaît dans la colonne locale. Les octets et les octets dans les colonnes n'affichent aucune activité parce que l'application n'a pas été appelée à ce moment.

2. Utilisez l'invite DOS ou toute autre application telnet de commencer une session de telnet.
3. Àl'invite de commande, entrez dans le **telnet 127.0.0.1 3044**.**Remarque:** Cette commande fournit un exemple de la façon accéder au port local affiché dans l'image de page Web de service de webvpn dans ce document. *La commande n'inclut pas des deux points (:).* Introduisez la commande comme décrit dans ce document.L'ASA reçoit la maîtrise de la session sécurisée, et parce qu'elle enregistre une carte des informations, l'ASA sait immédiatement pour ouvrir la session de telnet sécurisée au périphérique mappé.

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

4. Afin de vérifier l'accès au périphérique, vérifiez les octets et les octets dans les colonnes suivant les indications de cette image
:



Commandes

Plusieurs commandes **show** sont associées au 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.

Remarque: L'Outil Interpréteur de sortie (clients enregistrés uniquement) (OIT) prend en charge

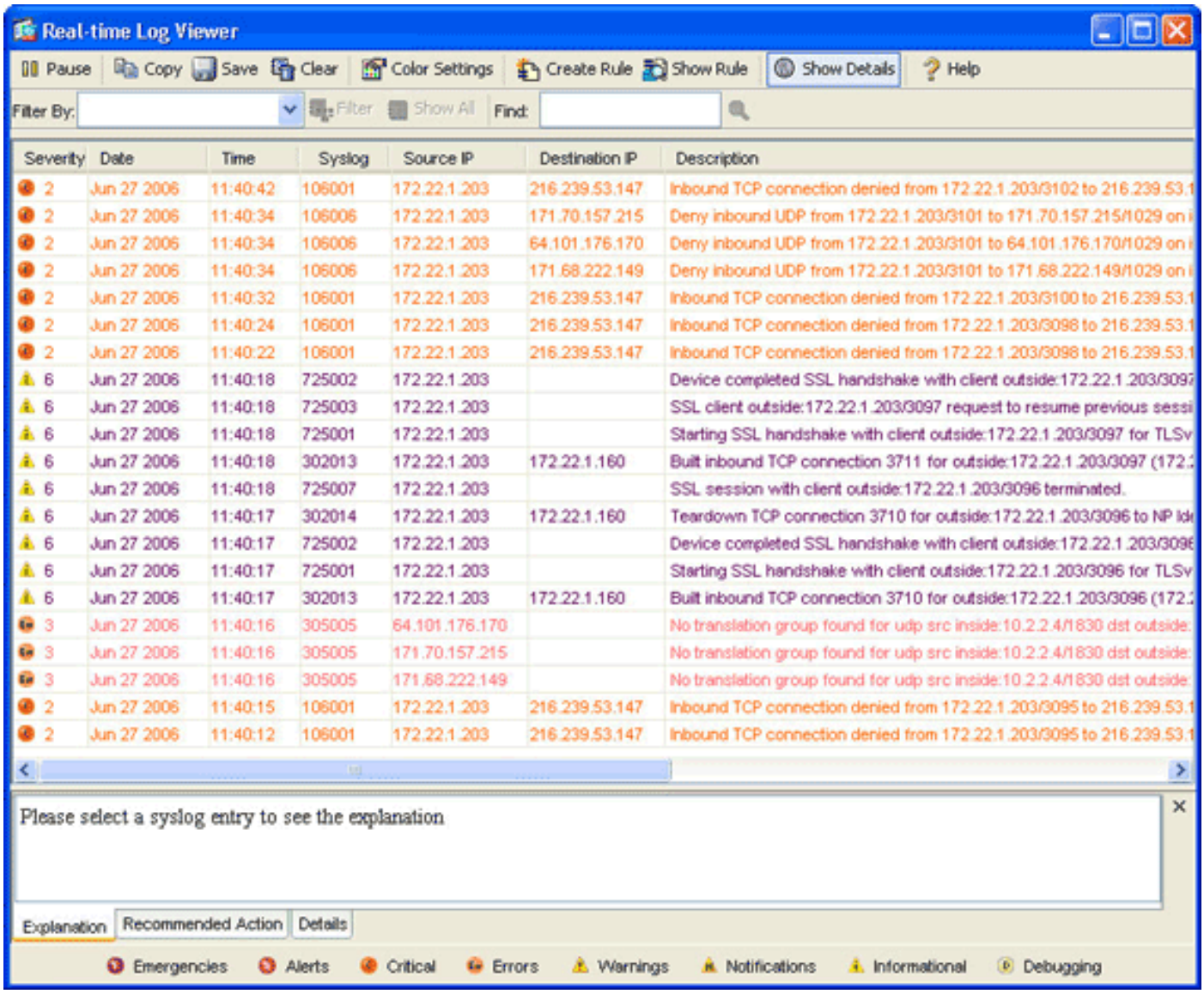
certaines commandes **show**. Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show** .

Dépannez

Utilisez cette section pour dépanner votre configuration.

Le SSL est-il processus de prise de contact complet ?

Une fois que vous vous connectez à l'ASA, vérifiez si le log en temps réel affiche la fin de la prise de contact SSL.

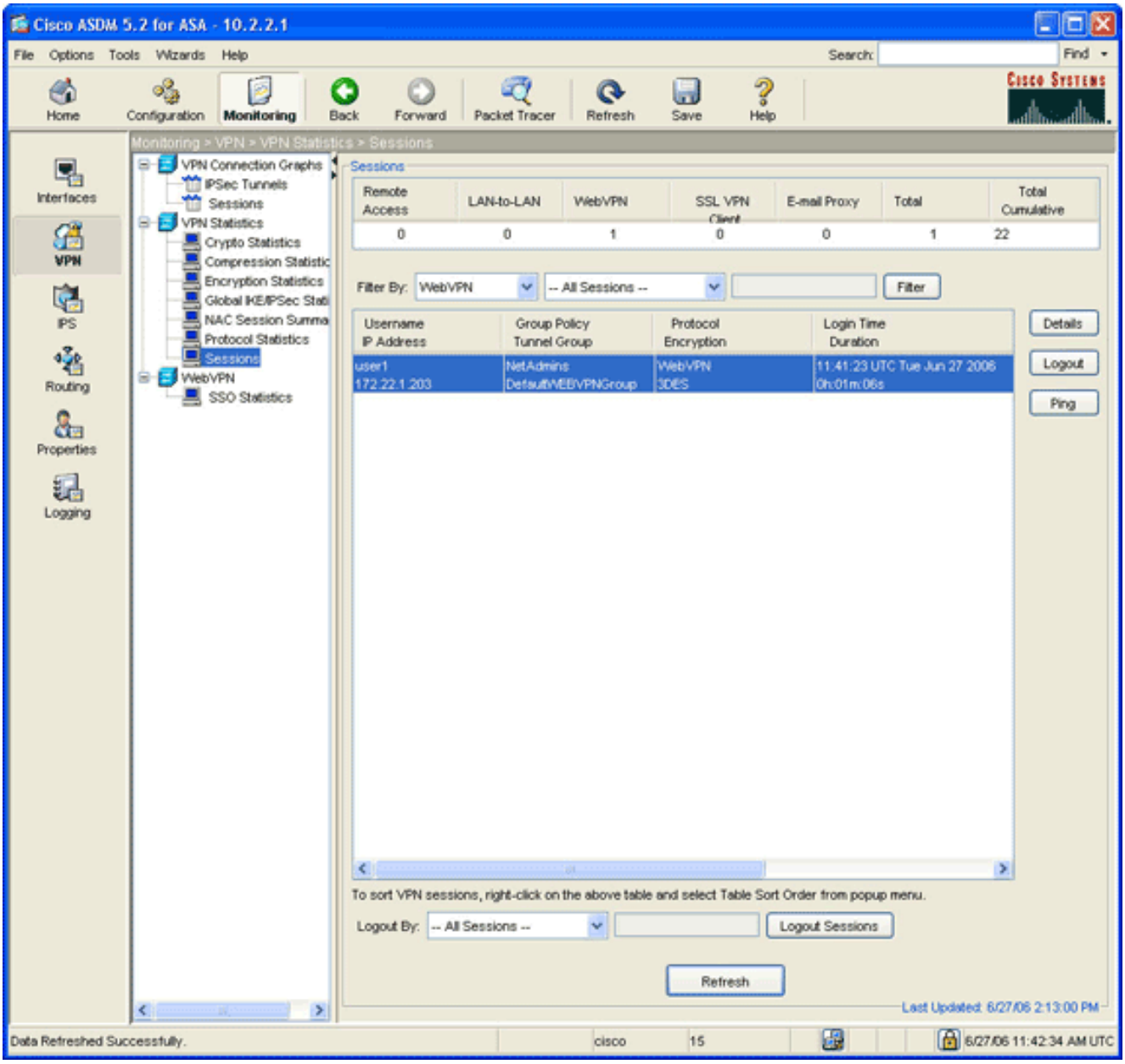


Le client léger de VPN SSL est-il fonctionnel ?

Afin de vérifier que le client léger de VPN SSL est fonctionnel, terminez-vous ces étapes :

1. **La surveillance de** clic, et cliquent sur alors le **VPN**.
2. Développez les **statistiques VPN**, et cliquez sur les **sessions**.Votre session de client léger de VPN SSL devrait apparaître dans la liste de sessions. Soyez sûr de filtrer par webvpn suivant les indications de 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