ASA/PIX : Exemple de configuration de serveur VPN distant avec NAT entrant pour le trafic client VPN avec CLI et ASDM

Contenu

Introduction

Ce document décrit comment configurer le dispositif de sécurité adaptatif (ASA) de la gamme Cisco 5500 pour qu'il agisse en tant que serveur VPN distant à l'aide de l'Adaptive Security Device Manager (ASDM) ou du CLI et du NAT pour le trafic entrant du client VPN. L'ASDM fournit la gestion et la surveillance de la sécurité de classe mondiale par une interface de gestion basée sur le Web, intuitive et facile à utiliser. Une fois que la configuration de Cisco ASA est complète, elle peut être vérifiée par le Client VPN Cisco.

Conditions préalables

Conditions requises

Ce document suppose que l´ASA est complètement opérationnel et configuré pour permettre au Cisco ASDM ou CLI d'apporter des modifications de configuration. On assume qu'également L'ASA est configurée pour NAT sortant. Référez-vous permettent à des hôtes internes Access aux réseaux extérieurs avec l'utilisation de PAT pour plus d'informations sur la façon configurer NAT sortant.

Remarque: Référez-vous à Permettre l'accès HTTPS pour l'ASDM ou PIX/ASA 7.x : SSH dans l'exemple de configuration d'interface interne et externe pour permettre au périphérique d´être configuré à distance par l'ASDM ou Secure Shell (SSH).

Composants utilisés

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

- Version de logiciel 7.x d'appliance de sécurité adaptable Cisco et plus tard
- Version 5.x et ultérieures d'Adaptive Security Device Manager
- Version 4.x et ultérieures de Client VPN Cisco

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.

Produits connexes

Cette configuration peut également être utilisée avec la version 7.x et ultérieures d'appareils de Sécurité de Cisco PIX.

Conventions

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

Informations générales

Les configurations d'accès à distance fournissent un accès à distance sécurisé pour les Clients VPN Cisco, tels que les utilisateurs mobiles. Un VPN d'accès à distance permet aux utilisateurs distants d´accéder sécuritairement aux ressources réseau centralisées. Le Client VPN Cisco se conforme au protocole IPSec et est spécifiquement conçu pour fonctionner avec l'appareil de sécurité. Cependant, l'appareil de sécurité peut établir des connexions d'IPSec avec beaucoup de clients protocol-conformes. Référez-vous aux guides de configuration ASA pour plus d'informations sur IPSec.

Les groupes et les utilisateurs sont des concepts de noyau en Gestion de la Sécurité des VPN et dans la configuration de l'appareil de sécurité. Ils spécifient les attributs qui déterminent l'accès d'utilisateurs et l'utilisation du VPN. Un groupe est une collection d'utilisateurs traités comme entité unique. Les utilisateurs obtiennent leurs attributs dans les politiques de groupe. Les groupes de tunnel identifient la stratégie de groupe pour les connexions spécifiques. Si vous n'assignez pas une stratégie de groupe particulière aux utilisateurs, la stratégie de groupe par défaut pour la connexion s'applique.

Un groupe de tunnel se compose d'un ensemble d´enregistrements qui détermine les politiques de connexion de tunnel. Ces enregistrements identifient les serveurs auxquels les utilisateurs de tunnel sont authentifiés, aussi bien que les serveurs de comptabilité, le cas échéant, auxquels les informations de connexion sont envoyées. Ils identifient également une politique de groupe par défaut pour les connexions, et ils contiennent des paramètres protocol-spécifiques de connexion.

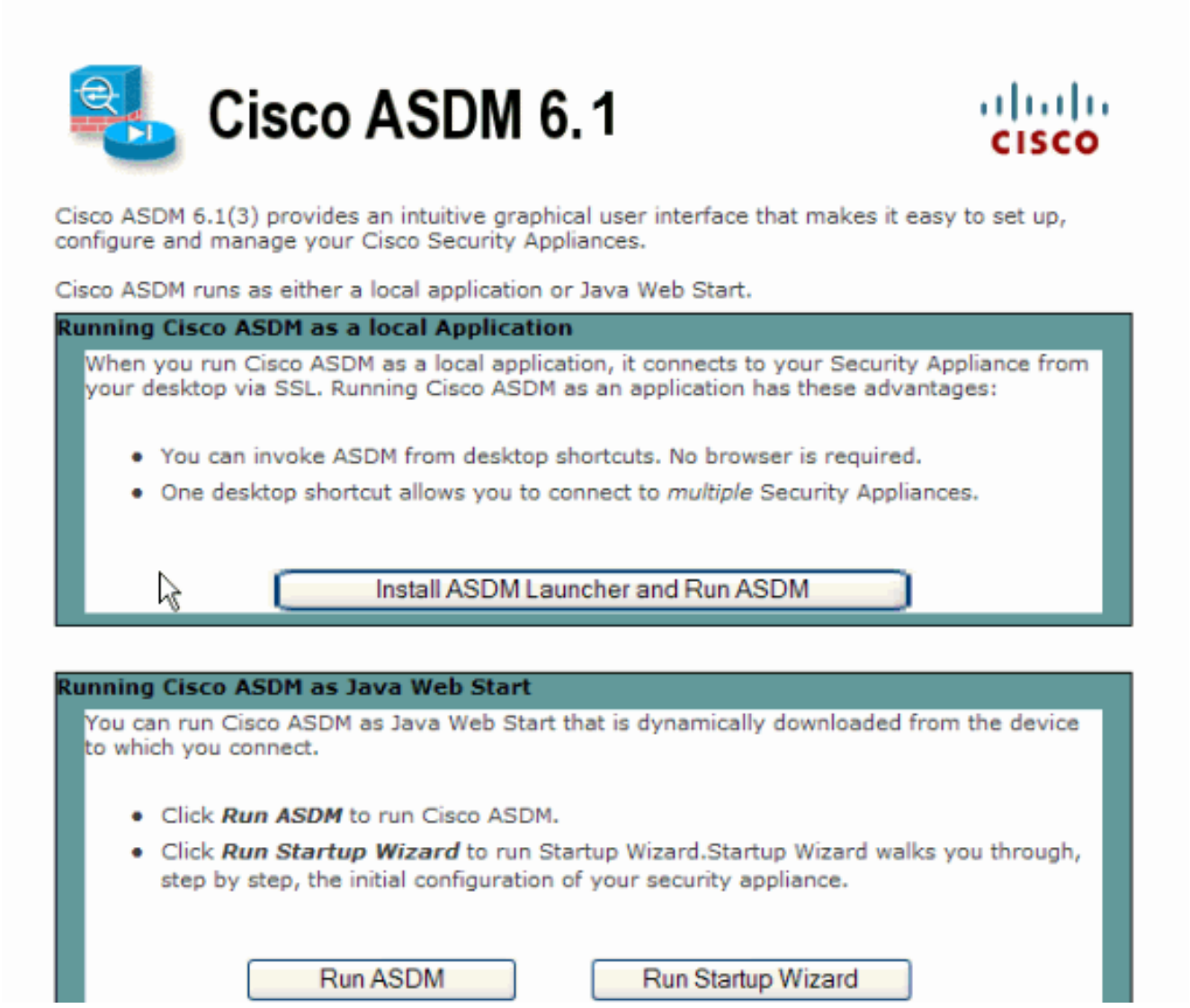
Les groupes de tunnel incluent un nombre restreint d'attributs qui concernent la création du tunnel elle-même. Les groupes de tunnel incluent un pointeur à une politique de groupe qui définit des attributs adaptés à l'utilisateur.

Configurations

Configurez l'ASA/PIX en tant que serveur VPN distant avec l'ASDM

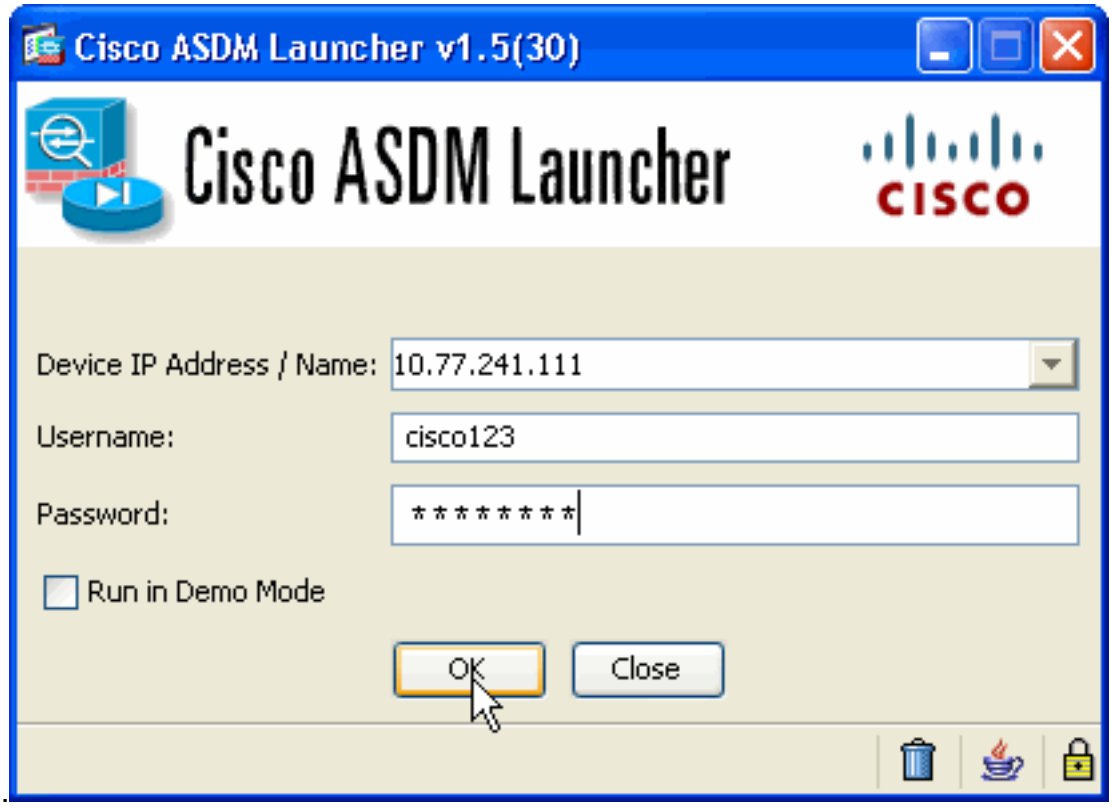
Terminez-vous ces étapes afin de configurer Cisco ASA en tant que serveur VPN distant avec l'ASDM :

1. Ouvrez votre navigateur et écrivez les **<IP_Address de https:// de l'interface de l'ASA qui a été configurée pour ASDM Access>** afin d'accéder à l'ASDM sur l'ASA.Prenez soin d'autoriser tous les avertissements que votre navigateur vous donne en ce qui concerne l'authenticité de certificat SSL. Le nom d'utilisateur par défaut et le mot de passe sont tous deux vides.L'ASA présente cette fenêtre pour permettre le téléchargement de l'application ASDM. Cet exemple charge l'application sur l'ordinateur local et ne fonctionne pas dans une applet
Java.

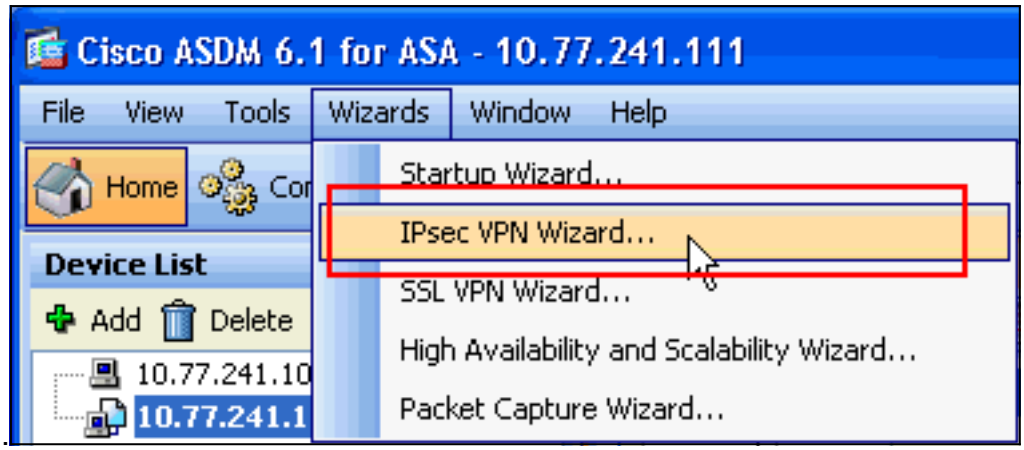


2. Cliquez sur **Download ASDM Launcher and Start ASDM** pour télécharger le programme d'installation de l'application ASDM.

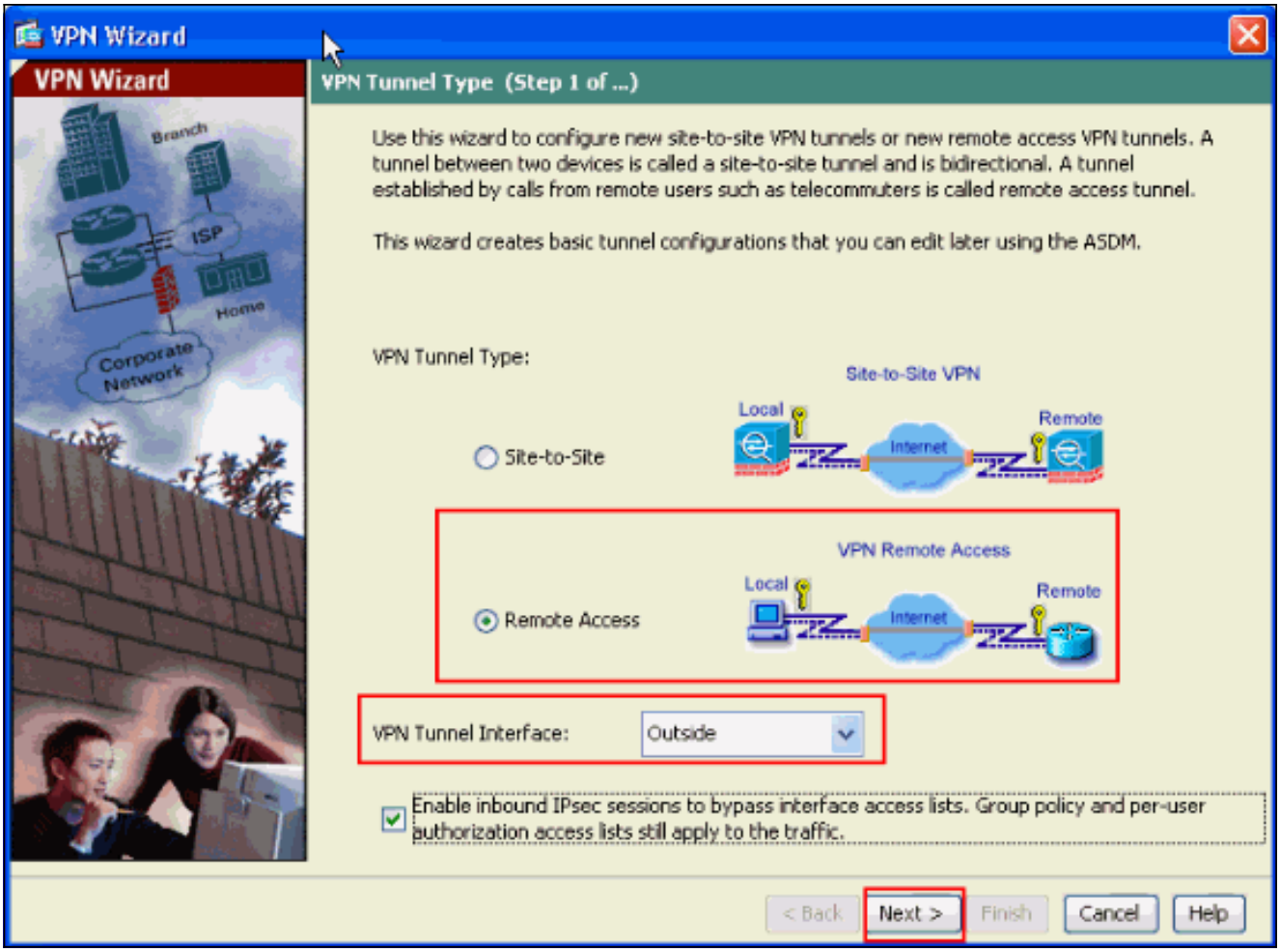
3. Une fois le lanceur d'ASDM téléchargé, exécutez les étapes stipulées par les invites afin d'installer le logiciel et d'exécuter le lanceur de Cisco ASDM.
4. Entrez l'adresse IP pour l'interface que vous avez configurée avec la commande **http -**, ainsi qu'un nom d'utilisateur et un mot de passe, le cas échéant.Cet exemple utilise **cisco123** comme nom d'utilisateur et **cisco123** comme mot de passe.



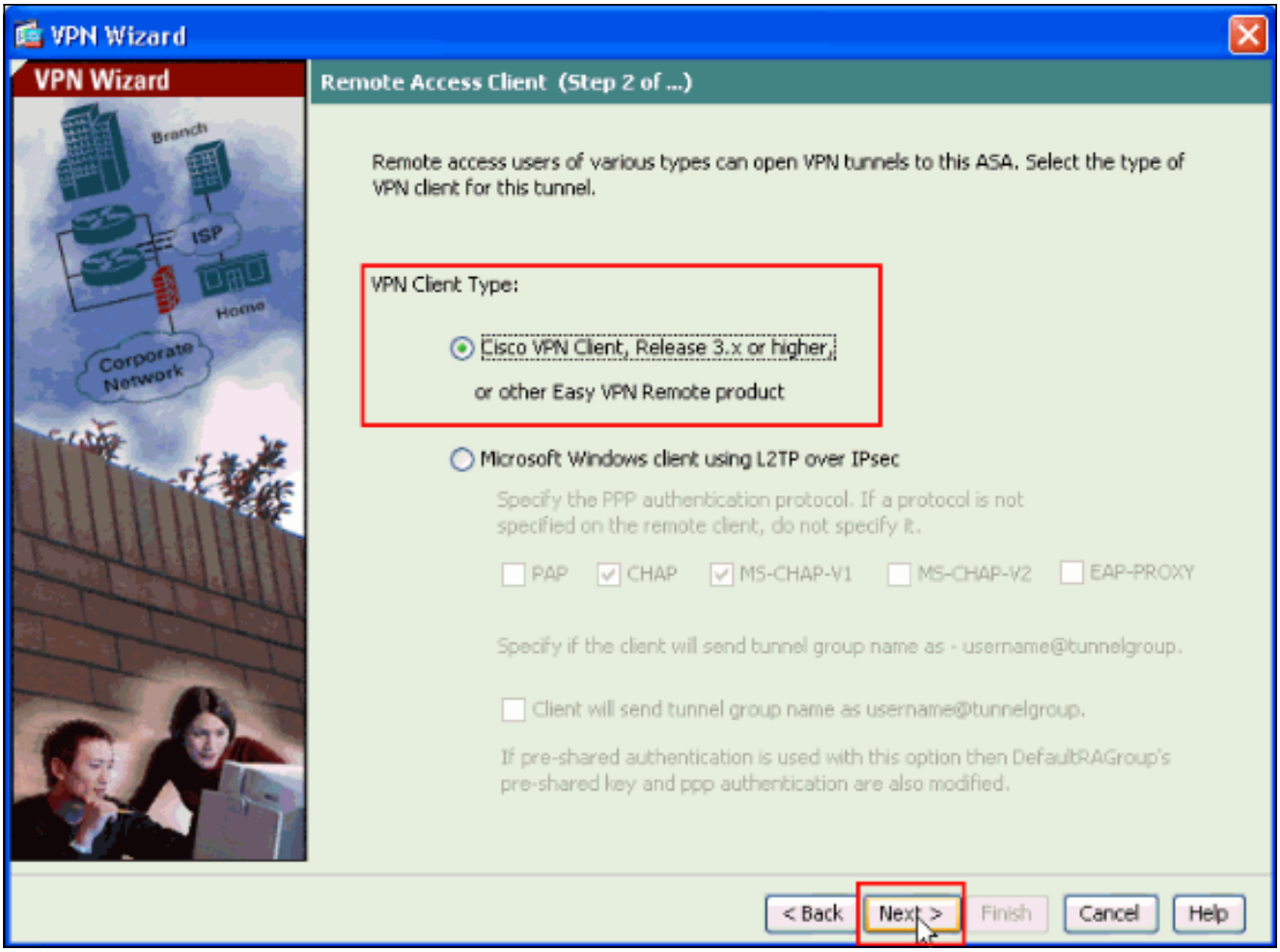
5. **Assistants** choisis **> assistant d'IPsec VPN de la** fenêtre d'accueil.



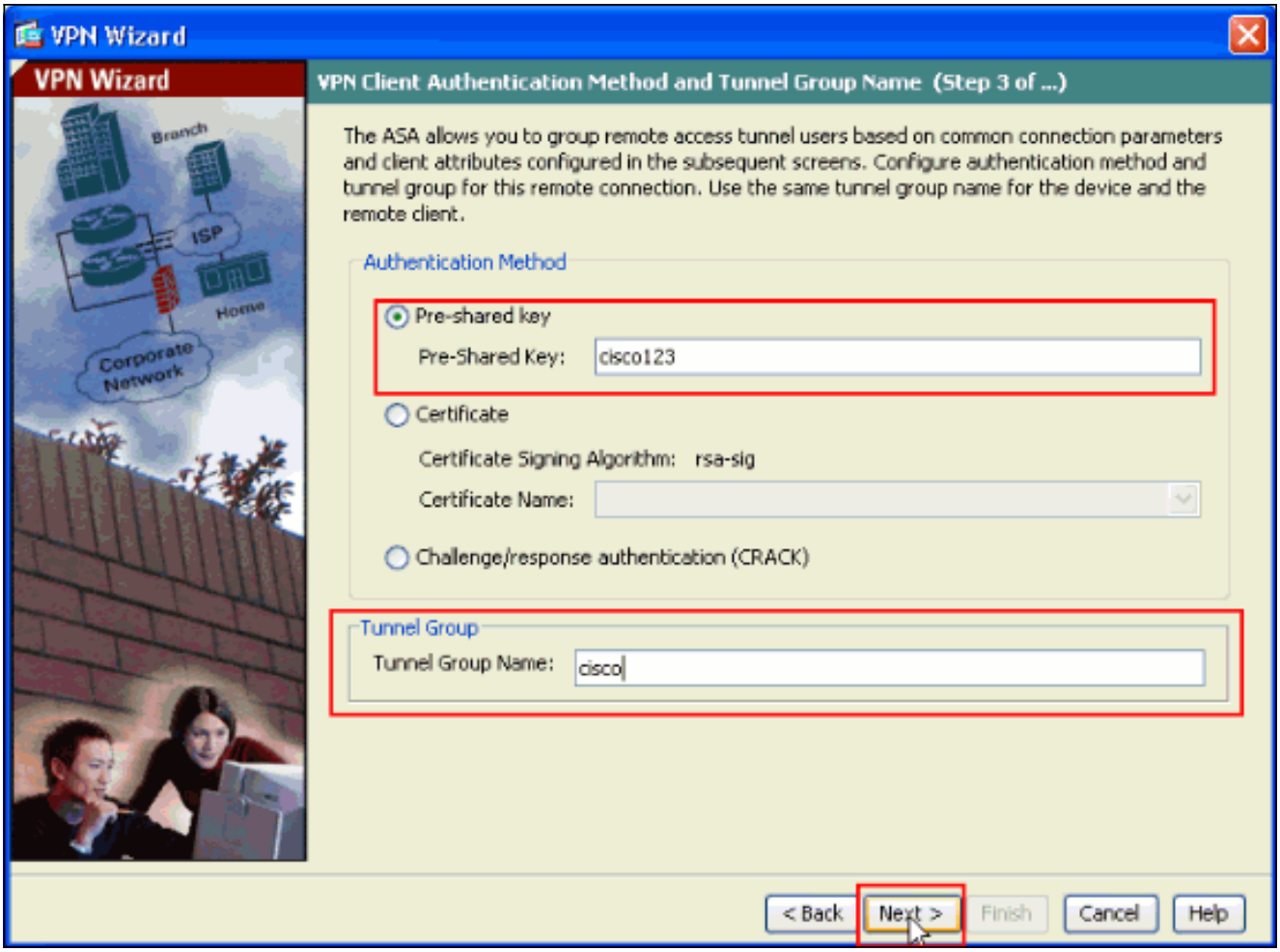
6. Sélectionnez le type de tunnel VPN d'**Accès à distance** et assurez-vous que l'interface de tunnel VPN est placée comme désirée, et cliquez sur Next comme affiché ici.



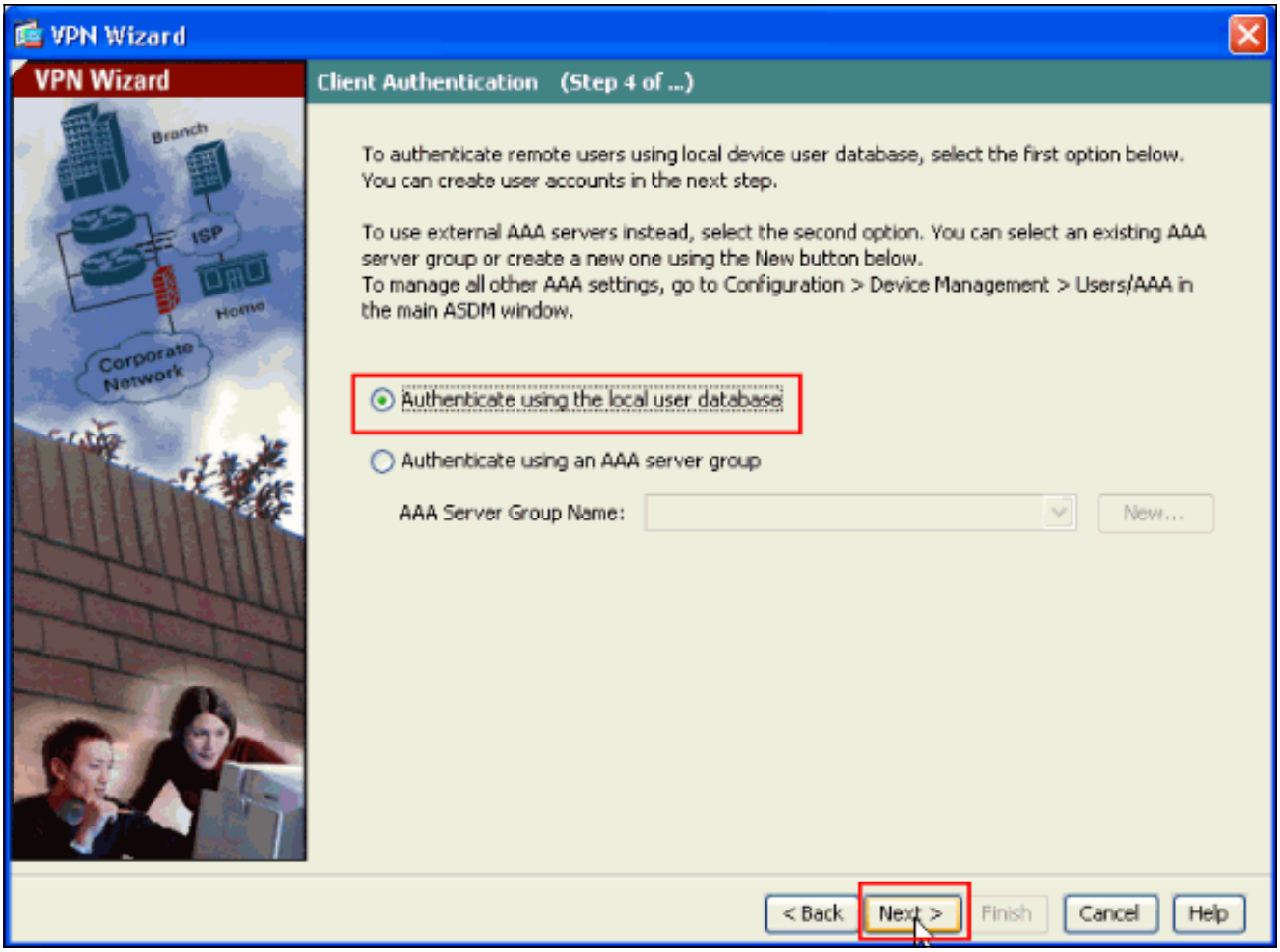
7. Le type de client vpn est choisi, comme affiché. **Le Client VPN Cisco** est choisi ici. Cliquez sur **Next**
(Suivant).



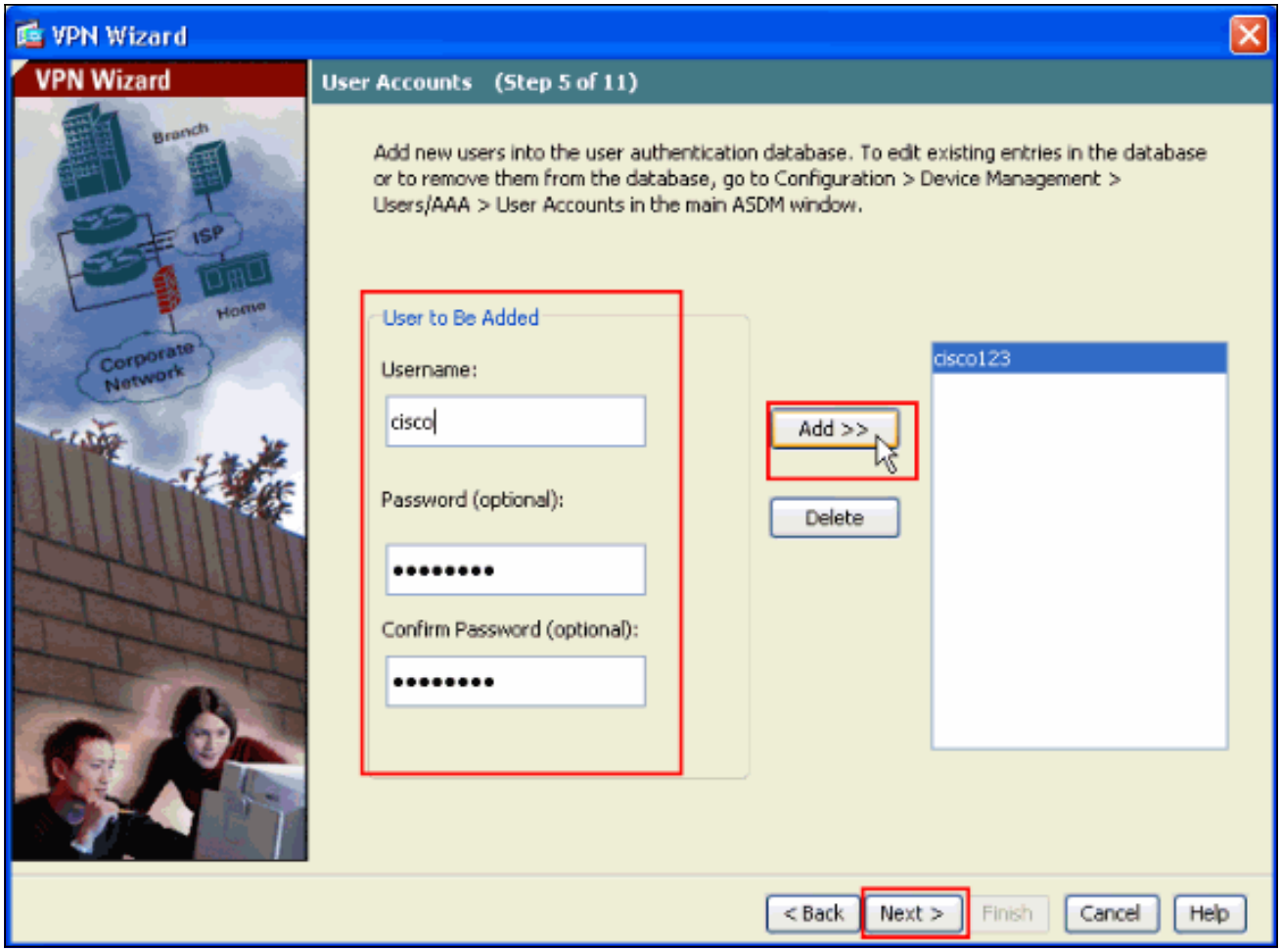
8. Écrivez un nom pour le nom du groupe tunnel. Entrez les informations d'authentification à utiliser, qui sont la clé pré-partagée dans cet exemple. La clé pré-partagée utilisée dans cet exemple est **cisco123**. Le Tunnel Group Name utilisé dans cet exemple est **Cisco**. Cliquez sur **Next**
(Suivant).



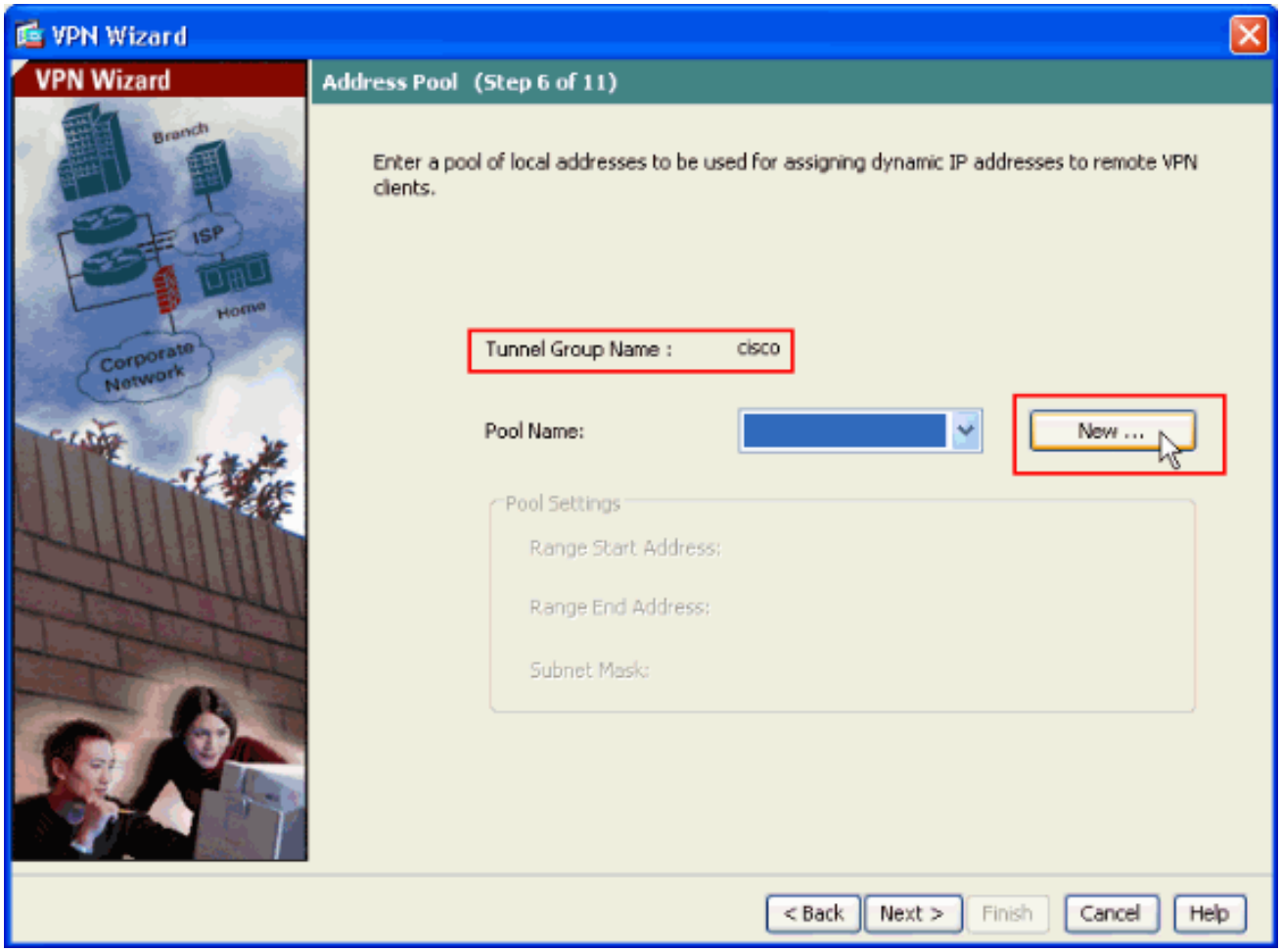
9. Choisissez si vous voulez que des utilisateurs distants soient authentifiés à la base de données des utilisateurs locaux ou à un groupe de serveurs AAA externe.**Remarque:** Vous ajoutez des utilisateurs à la base de données locale des utilisateurs dans l'étape 10.**Remarque:** Référez-vous aux groupes de serveurs d'authentification et d'autorisation PIX/ASA 7.x pour des utilisateurs VPN par l'intermédiaire de l'exemple de configuration ASDM pour les informations sur la façon dont configurer un Groupe de serveurs AAA externe avec
l'ASDM.



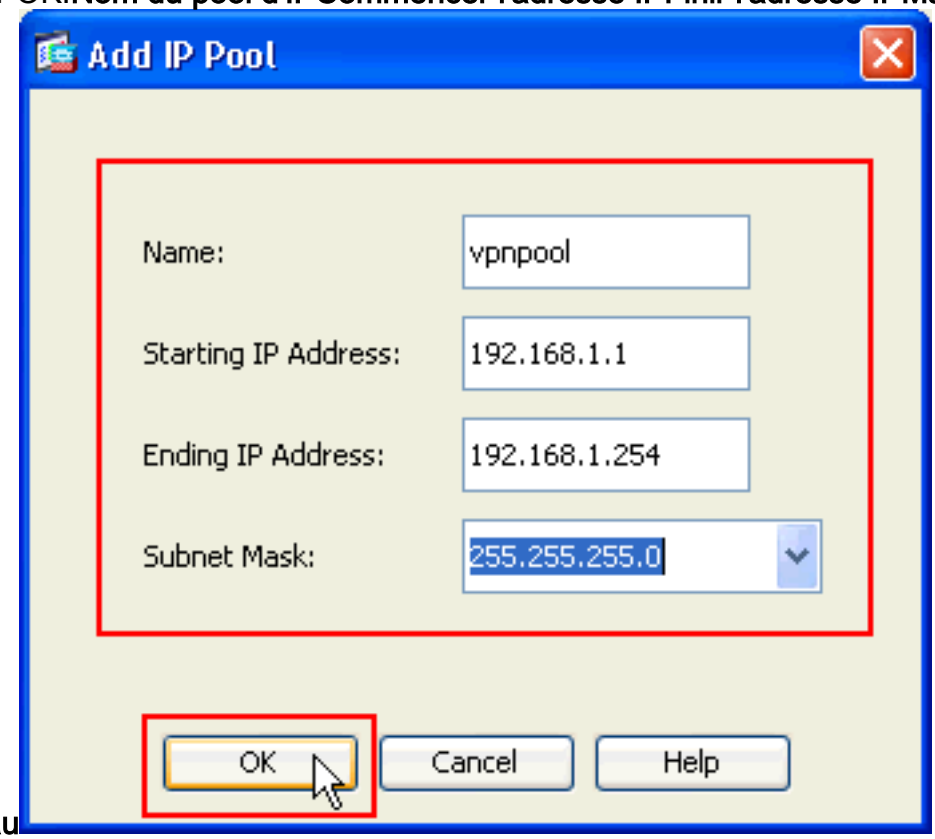
10. Fournissez un **nom d'utilisateur** et un **mot de passe** facultatif et cliquez sur Add afin d'ajouter de nouveaux utilisateurs à la base de données d'authentification de l'utilisateur. Cliquez sur **Next** (Suivant).**Remarque:** Ne pas supprimer les utilisateurs existants de cette fenêtre. **Configuration > Device Management > Users/AAA > User Accounts** choisi dans la fenêtre principale ASDM pour éditer les entrées existantes dans la base de données ou pour les retirer de la base de
données.



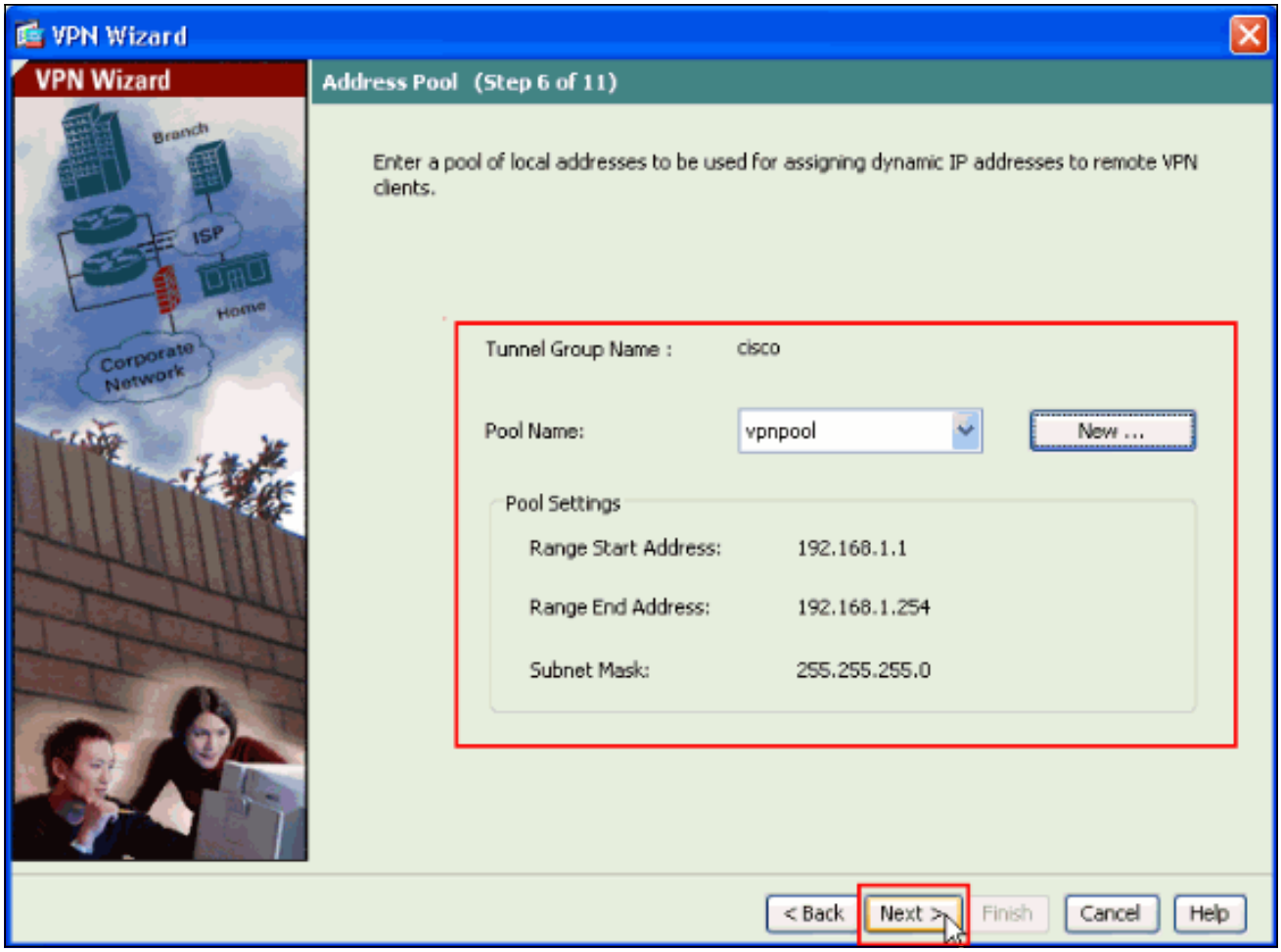
11. Afin de définir un groupe d'adresses locales à assigner dynamiquement aux clients vpn distants, cliquez sur New pour créer un nouveau **pool d'IP**.



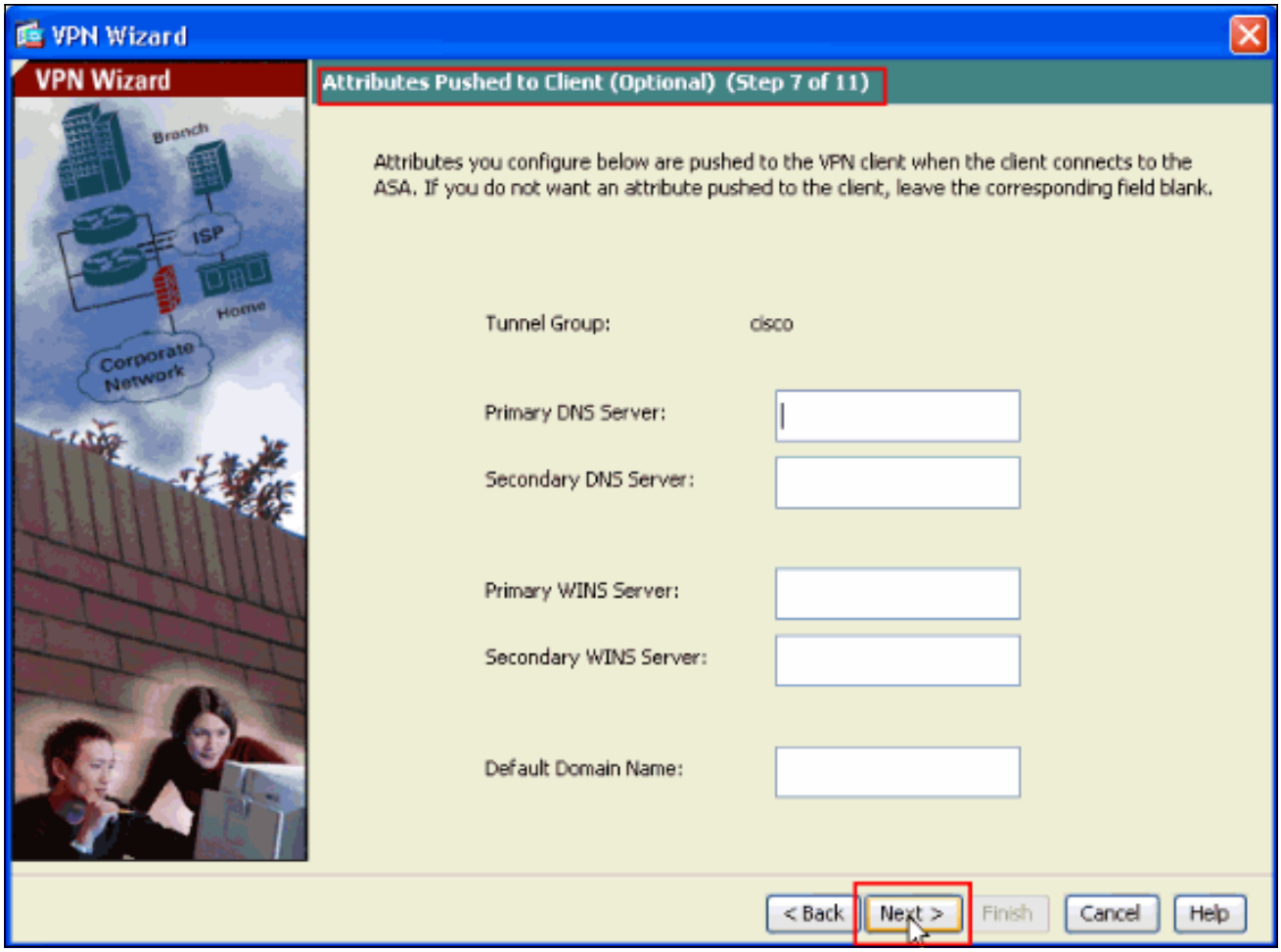
12. Dans la nouvelle fenêtre intitulée **ajoutez le pool d'IP** fournissent ces informations, et cliquent sur OK.**Nom du pool d'IPCommencer l'adresse IPFinir l'adresse IPMasque de sous-réseau**



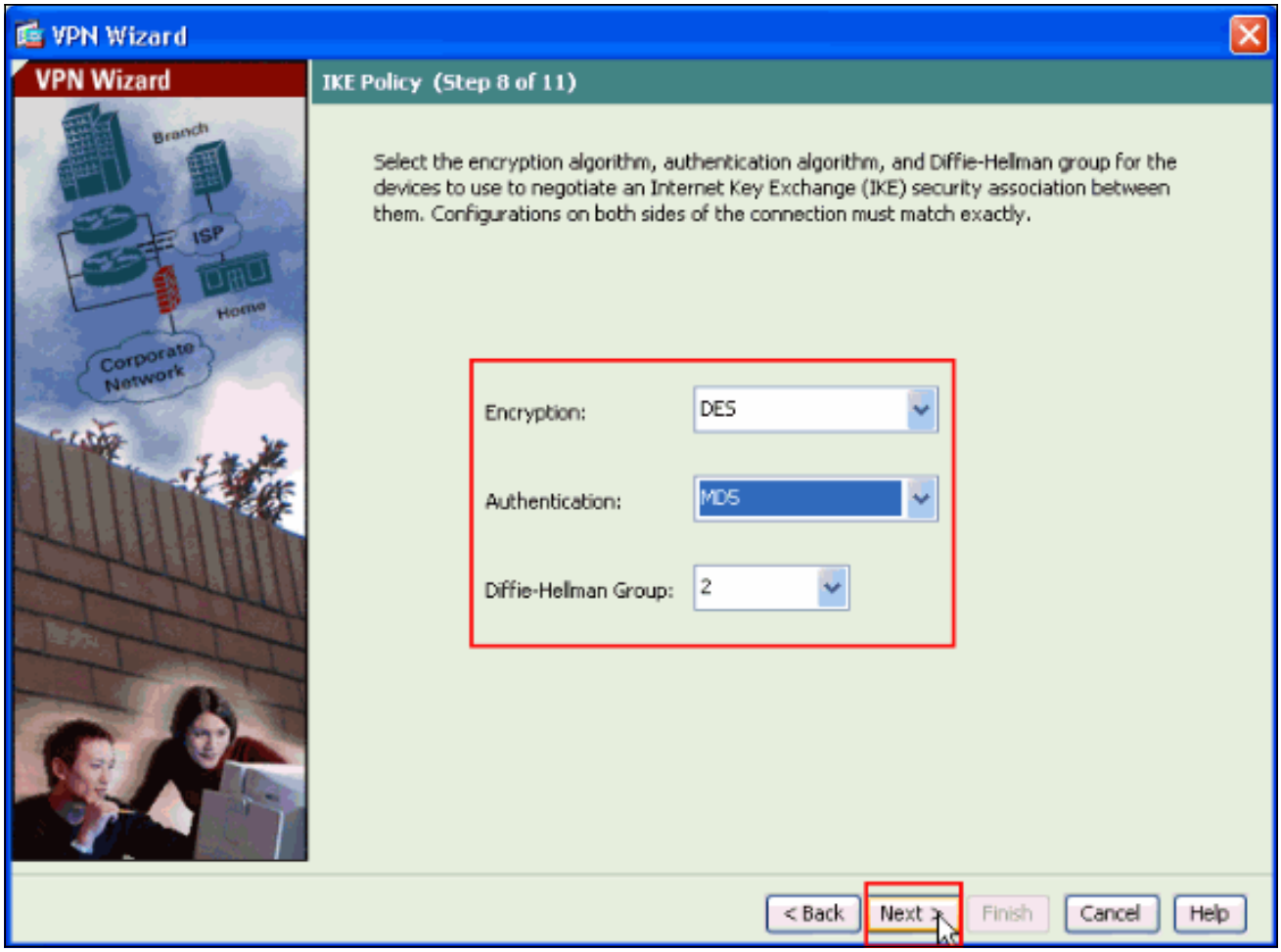
13. Après que vous définissiez le groupe d'adresses locales à assigner dynamiquement aux clients vpn distants quand ils se connectent, cliquez sur Next.



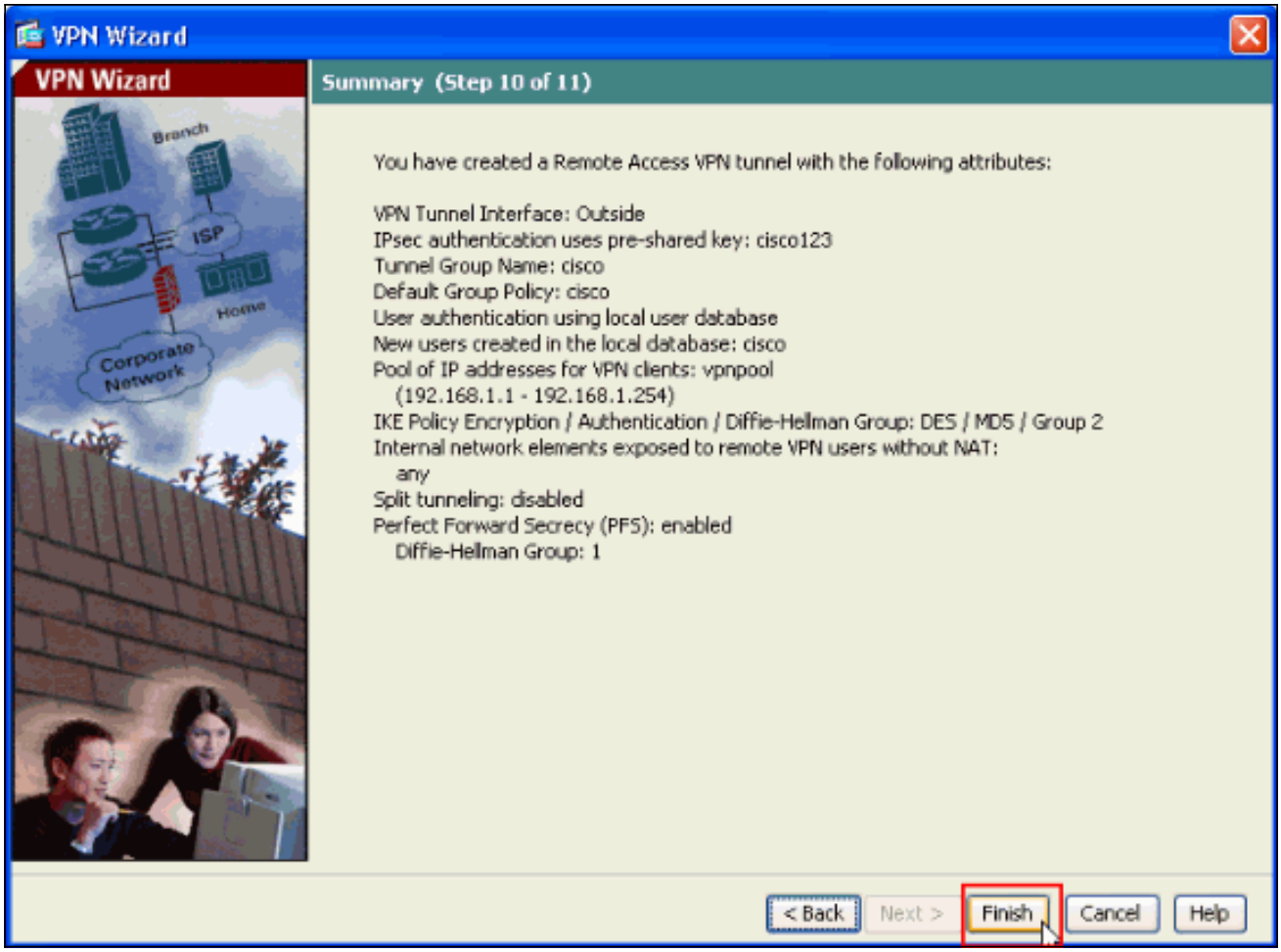
14. *Facultatif :* Spécifiez les informations du serveur DNS et WINS et un nom de Domaine par défaut à diffuser aux clients VPN
distants.



15. Spécifiez les paramètres pour l'IKE, également connus sous le nom de IKE phase 1.Les configurations des deux côtés du tunnel doivent correspondre exactement. Cependant, le Client VPN Cisco sélectionne automatiquement la configuration appropriée pour lui-même. Par conséquent, aucun configuration d´IKE n'est nécessaire sur le PC Client.



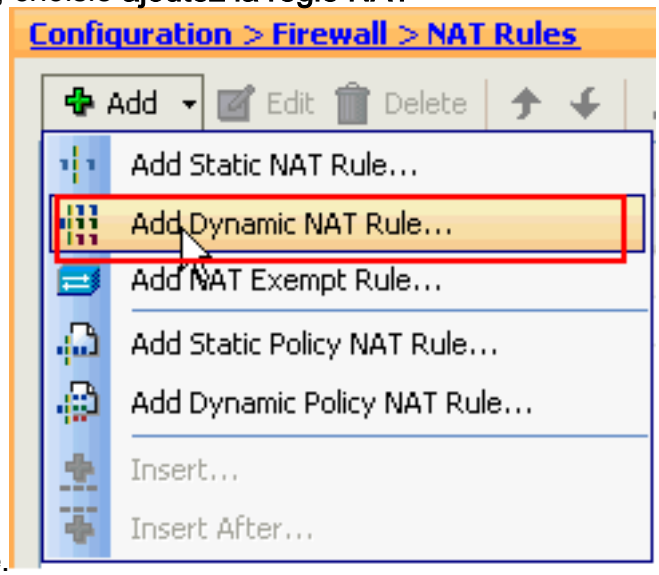
16. Cette fenêtre montre un résumé des actions que vous avez prises. Cliquez sur **Finish** si vous êtes satisfait de votre configuration.



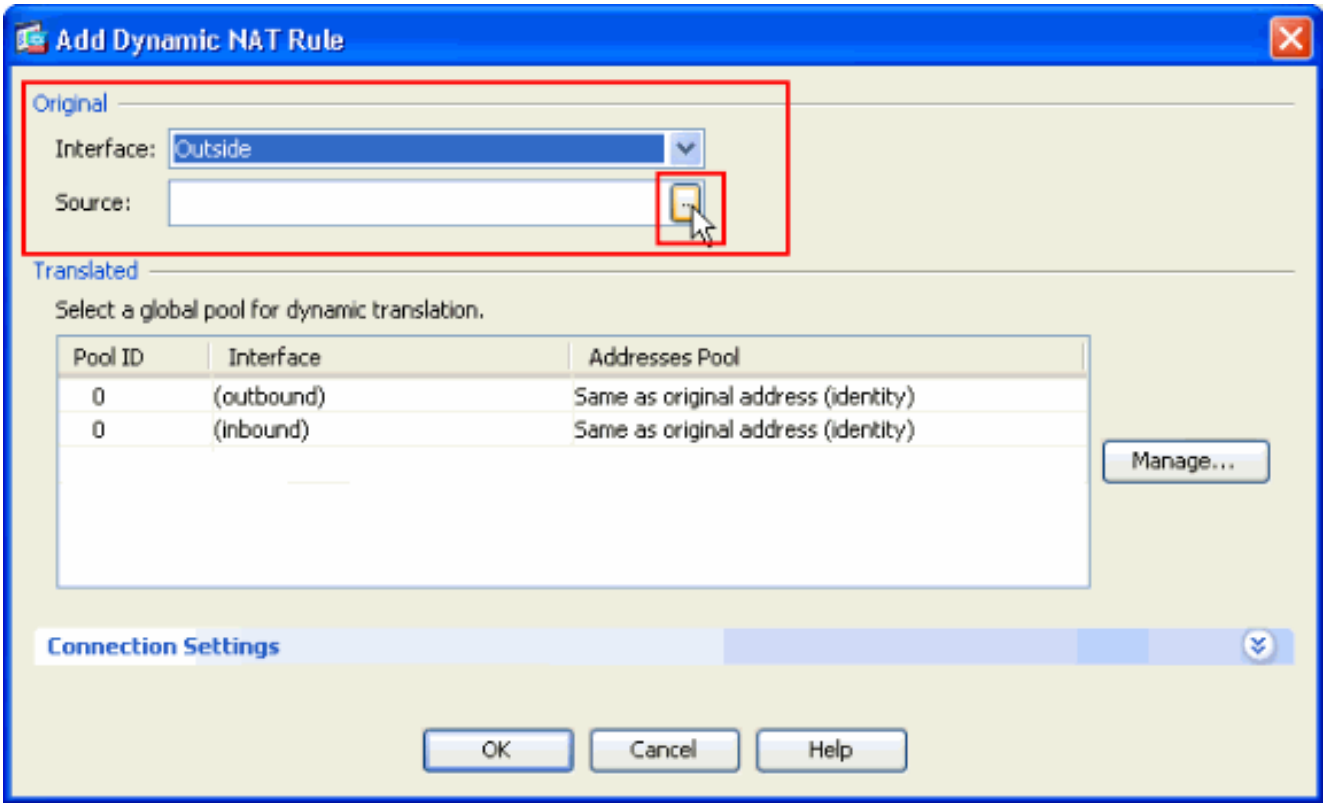
Configurez l'ASA/PIX au trafic d'arrivée NAT de client vpn avec l'ASDM

Terminez-vous ces étapes afin de configurer Cisco ASA au trafic d'arrivée NAT de client vpn avec l'ASDM :

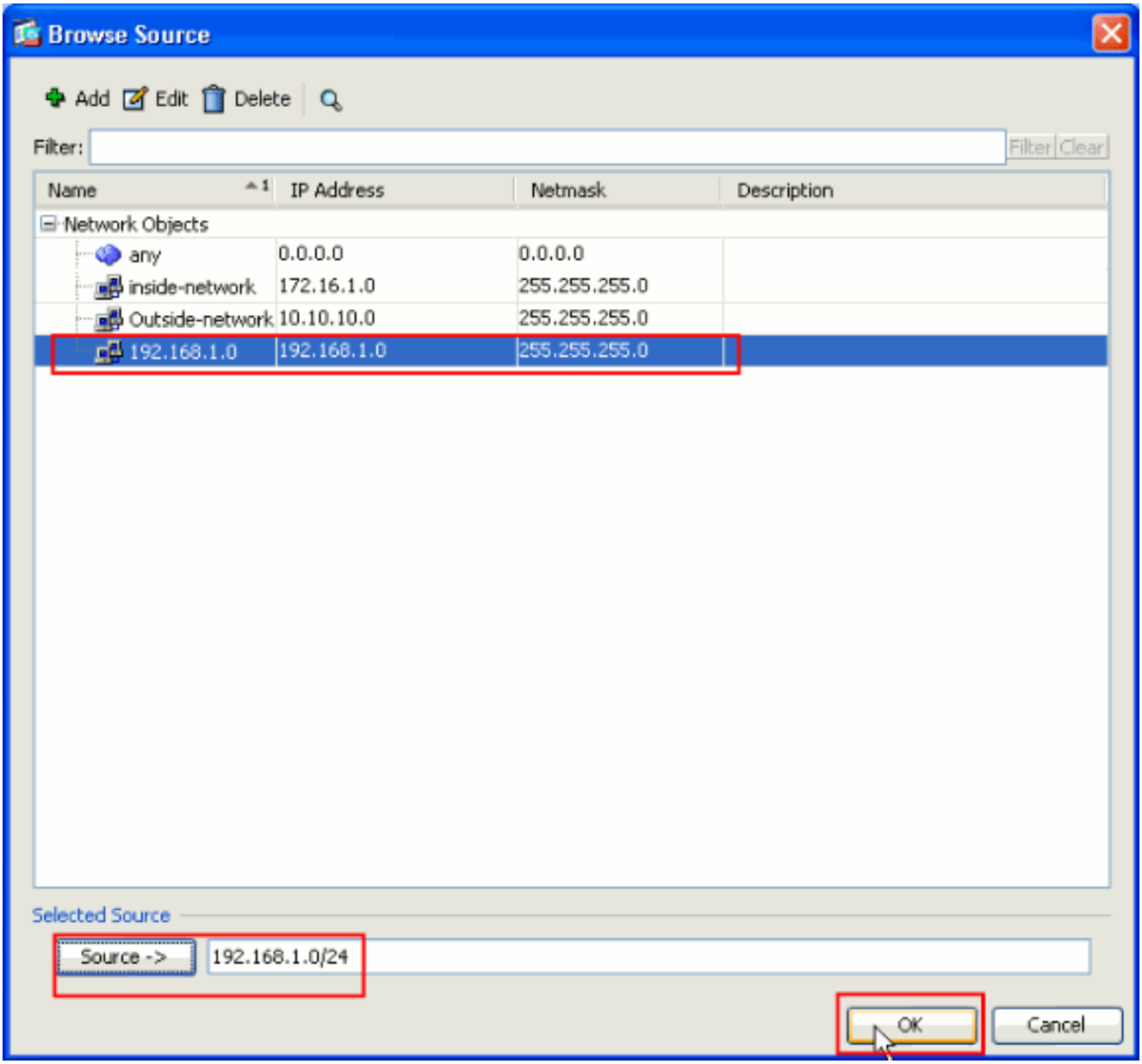
1. Choisissez la **configuration > le Pare-feu > des règles nat**, et cliquez sur Add. Dans la liste déroulante, choisie **ajoutez la règle NAT dynamique**.



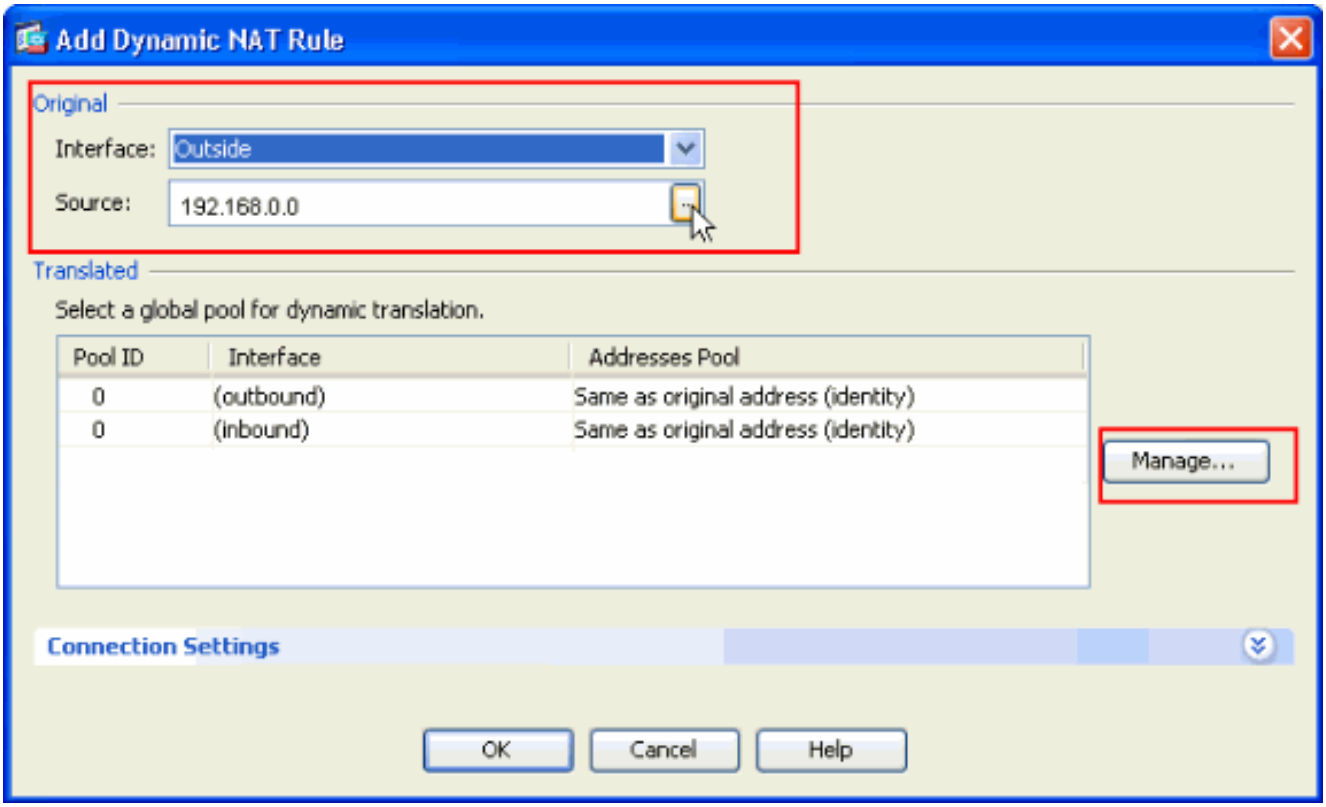
2. Dans la fenêtre **dynamique de règle NAT d'ajouter**, choisissez l'**extérieur** comme interface, et cliquez sur le bouton de furetage à côté de la case de **source**.



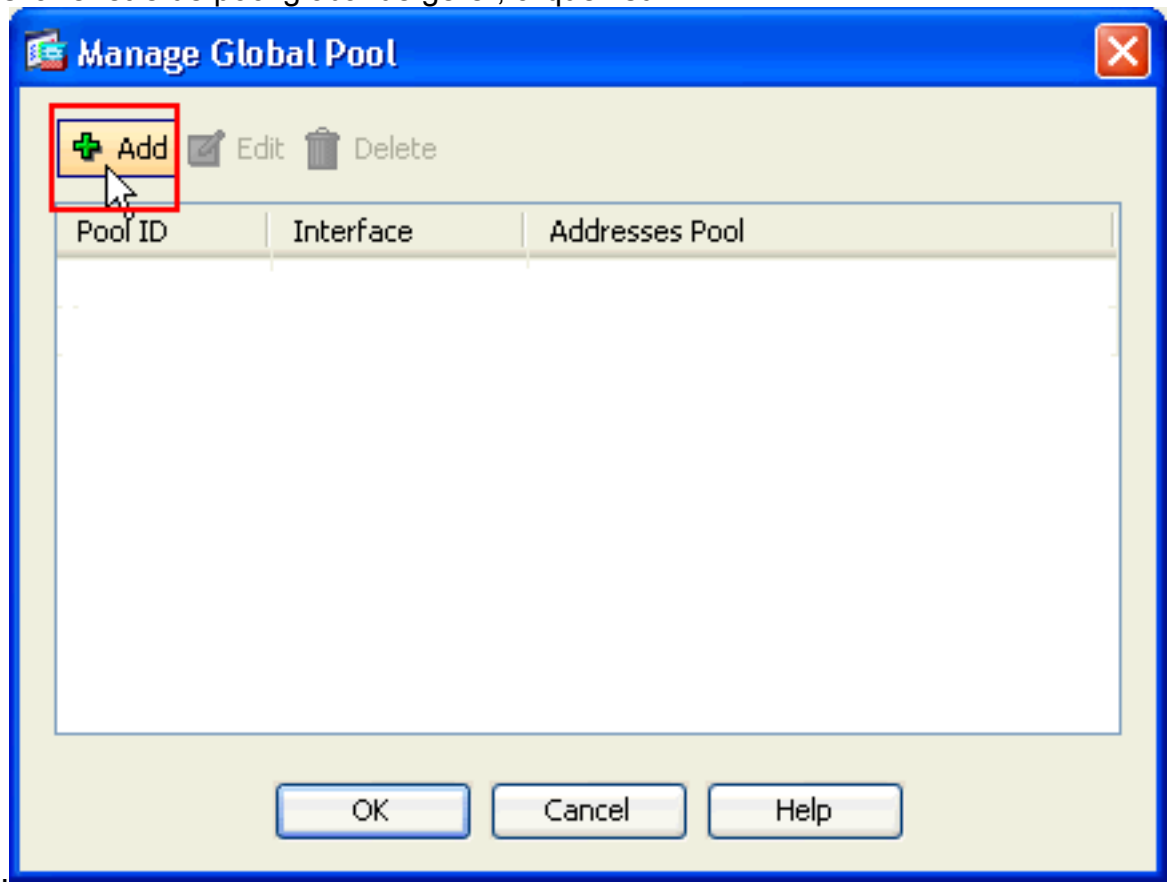
3. Dans la fenêtre de source de furetage, sélectionnez les objets de réseau appropriés et choisissez également la **source** sous la section sélectionnée de source, et cliquez sur OK. Ici l'objet de réseau de 192.168.1.0 est
choisi.



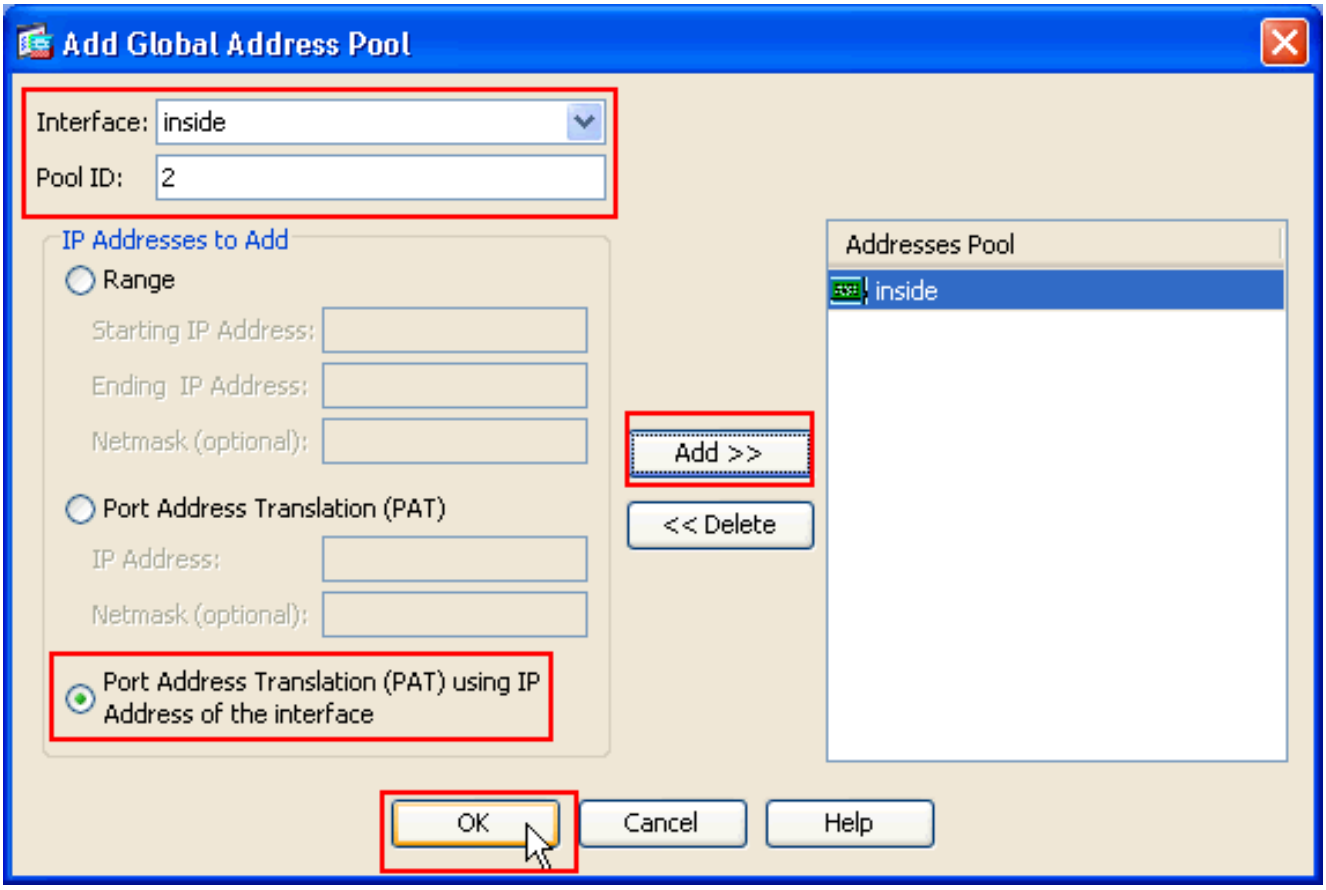
4. Le clic
gèrent.



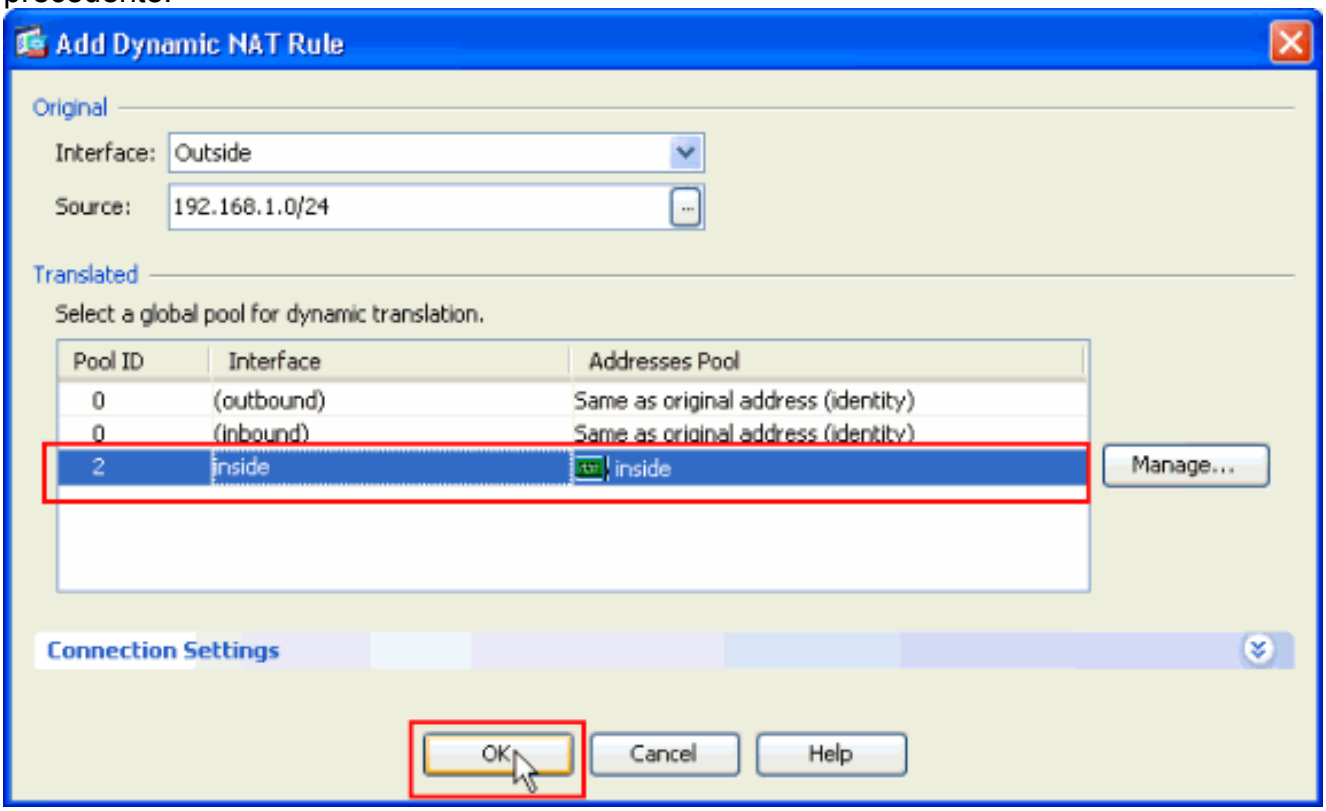
5. Dans la fenêtre de pool global de gérer, cliquez sur Add.



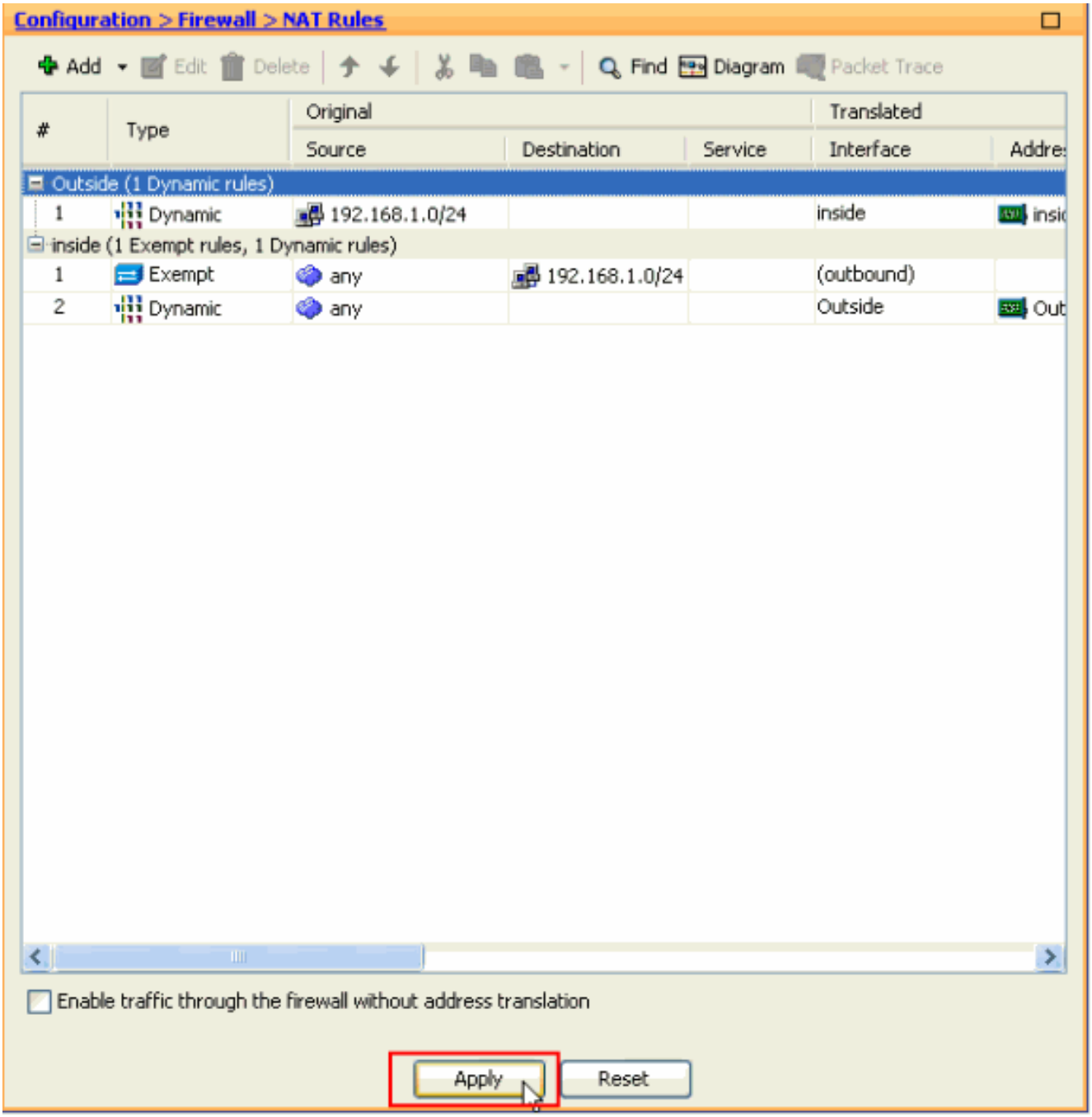
6. Dans la fenêtre de pool d'adresses globales d'ajouter, choisissez l'**intérieur** comme interface et **2** comme **ID de groupe**. Assurez-vous également que la case d'option à côté de **PAT utilisant l'adresse IP de l'interface** est sélectionnée. Cliquez sur **Add>>**, et puis cliquez sur OK.



7. Cliquez sur OK après que vous sélectionniez le pool global avec l'**ID 2 de groupe** configuré dans l'étape précédente.



8. Cliquez sur Apply maintenant de sorte que la configuration soit appliquée à l'ASA.This se termine la configuration.



Configurez l'ASA/PIX en tant que serveur VPN distant et pour NAT d'arrivée avec le CLI

Exécution de Config sur le périphérique ASA
ciscoasa#**show running-config** : Saved ASA Version 8.0(3) ! hostname ciscoasa enable password 8Ry2YjIyt7RRXU24 encrypted names ! interface Ethernet0/0 nameif Outside security-level 0 ip address 10.10.10.2 255.255.255.0 ! interface Ethernet0/1 nameif inside security-level 100 ip address 172.16.1.2 255.255.255.0 ! ! passwd 2KFQnbNIdI.2KYOU encrypted boot system disk0:/asa803-k8.bin ftp mode passive access-list inside_nat0_outbound extended permit ip any 192.168.1.0 255.255.255 0 pager lines 24 logging enable mtu Outside 1500 mtu inside 1500 **ip local pool vpnpool 192.168.1.1-192.168.1.254 mask 255.255.255.0** no failover icmp unreachable rate-limit 1 burst-size 1 asdm image disk0:/asdm-615.bin asdm history enable arp timeout 14400 nat-control **global (Outside) 1 interface global (inside) 2 interface nat (Outside) 2**

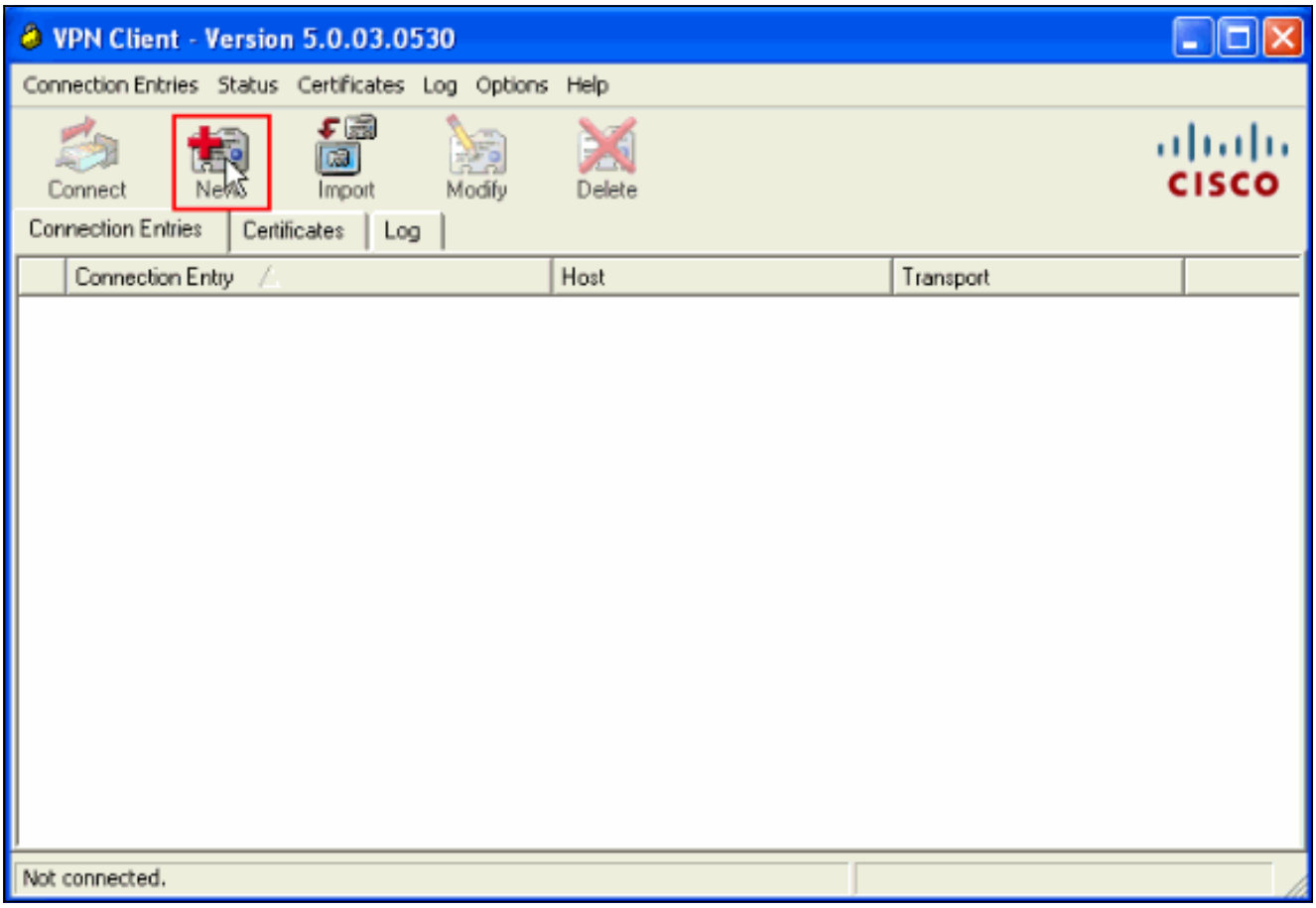
```
192.168.1.0 255.255.255.0 outside nat (inside) 0 access-
list inside_nat0_outbound nat (inside) 1 0.0.0.0 0.0.0.0
route Outside 0.0.0.0 0.0.0.0 10.10.10.3 1 timeout xlate
3:00:00 timeout conn 1:00:00 half-closed 0:10:00 udp
0:02:00 icmp 0:00:02 timeout sunrpc 0:10:00 h323 0:05:00
h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00 timeout sip
0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-
disconnect 0:02:00 timeout uauth 0:05:00 absolute
dynamic-access-policy-record DfltAccessPolicy http
server enable no snmp-server location no snmp-server
contact !--- Configuration for IPsec policies. !---
Enables the crypto transform configuration mode, !---
where you can specify the transform sets that are used
!--- during an IPsec negotiation. crypto ipsec
transform-set ESP-DES-SHA esp-des esp-sha-hmac crypto
ipsec transform-set ESP-DES-MD5 esp-des esp-md5-hmac
crypto dynamic-map SYSTEM_DEFAULT_CRYPTO_MAP 65535 set
pfs group1 crypto dynamic-map SYSTEM_DEFAULT_CRYPTO_MAP
65535 set transform-set ESP-DES-SH ESP-DES-MD5 crypto
map Outside_map 65535 ipsec-isakmp dynamic
SYSTEM_DEFAULT_CRYPTO_MAP crypto map Outside_map
interface Outside crypto isakmp enable Outside !---
Configuration for IKE policies. !--- Enables the IKE
policy configuration (config-isakmp) !--- command mode,
where you can specify the parameters that !--- are used
during an IKE negotiation. Encryption and !--- Policy
details are hidden as the default values are chosen.
crypto isakmp policy 10 authentication pre-share
encryption des hash sha group 2 lifetime 86400 crypto
isakmp policy 30 authentication pre-share encryption des
hash md5 group 2 lifetime 86400 telnet timeout 5 ssh
timeout 60 console timeout 0 management-access inside
threat-detection basic-threat threat-detection
statistics access-list group-policy cisco internal
group-policy cisco attributes vpn-tunnel-protocol IPSec
!--- Specifies the username and password with their !---
respective privilege levels username cisco123 password
ffIRPGpDSOJh9YLq encrypted privilege 15 username cisco
password ffIRPGpDSOJh9YLq encrypted privilege 0 username
cisco attributes vpn-group-policy cisco tunnel-group
cisco type remote-access tunnel-group cisco general-
attributes address-pool vpnpool default-group-policy
cisco !--- Specifies the pre-shared key "cisco123" which
must !--- be identical at both peers. This is a global
!--- configuration mode command. tunnel-group cisco
ipsec-attributes pre-shared-key * ! class-map
inspection_default match default-inspection-traffic ! !
policy-map type inspect dns migrated_dns_map_1
parameters message-length maximum 512 policy-map
global_policy class inspection_default inspect dns
migrated_dns_map_1 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 prompt hostname context
Cryptochecksum:f2ad6f9d5bf23810a26f5cb464e1fdf3 : end
ciscoasa#
```

Vérifiez

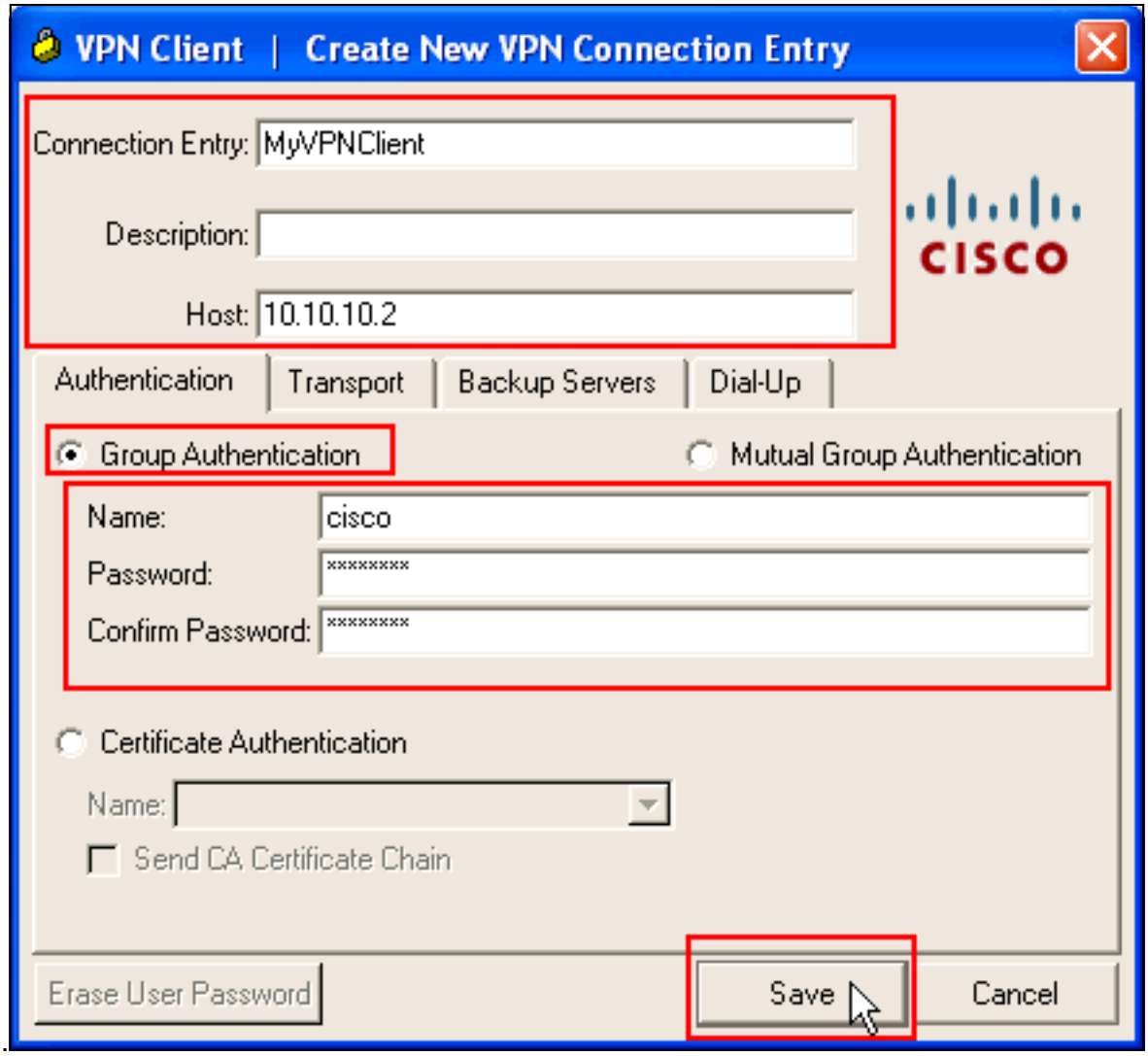
Tentez de se connecter à Cisco ASA par le Client VPN Cisco afin de vérifier que l'ASA est avec

succès configurée.

1. Cliquez sur
   New.

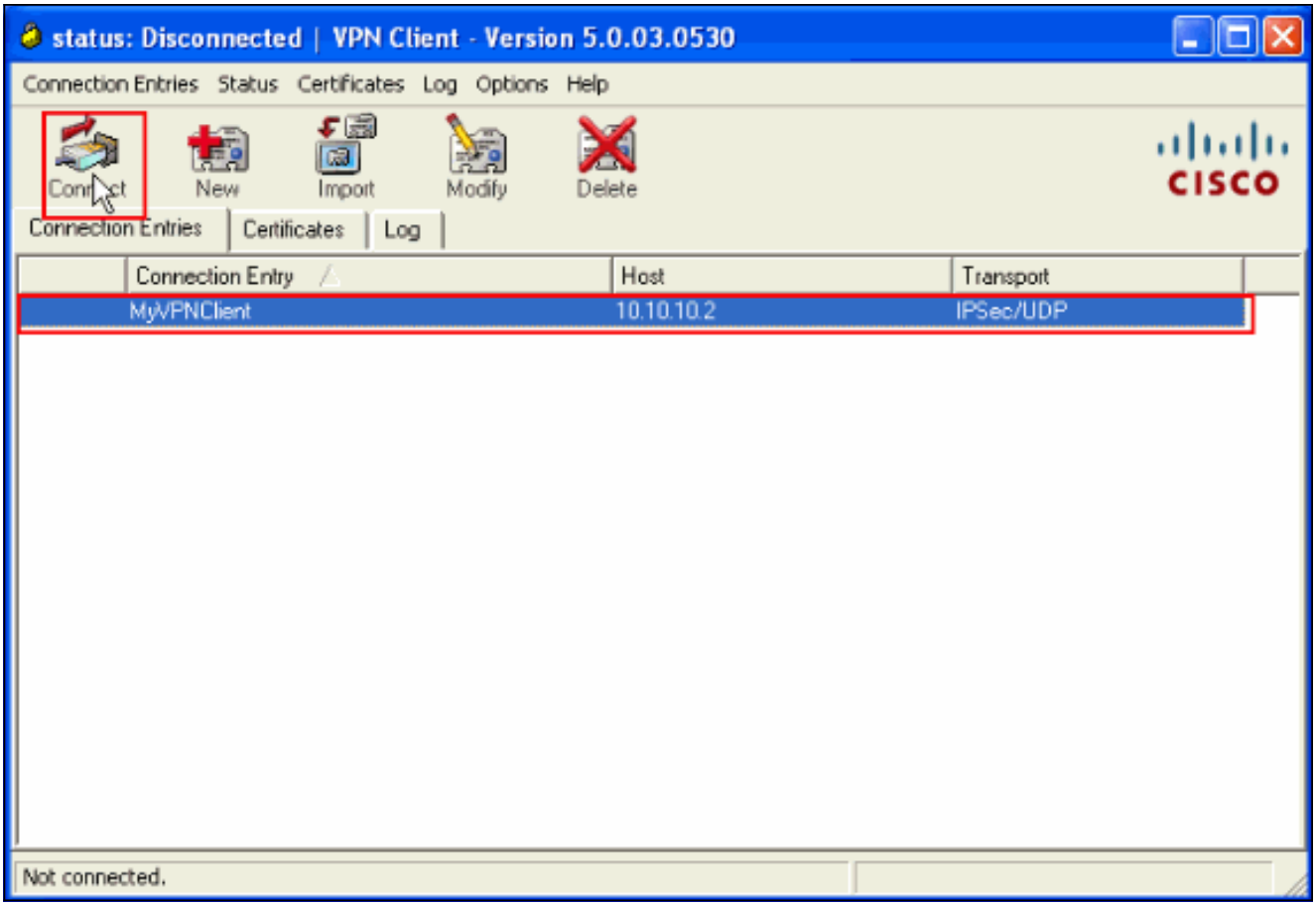


2. Complétez les détails de votre nouvelle connexion.Le champ Host doit contenir l'adresse IP ou l'adresse Internet de Cisco précédemment configuré ASA. Les informations d'authentification de groupe doivent correspondre à cela utilisé dans la **sauvegarde de** clic d'**étape 4.** quand vous êtes de

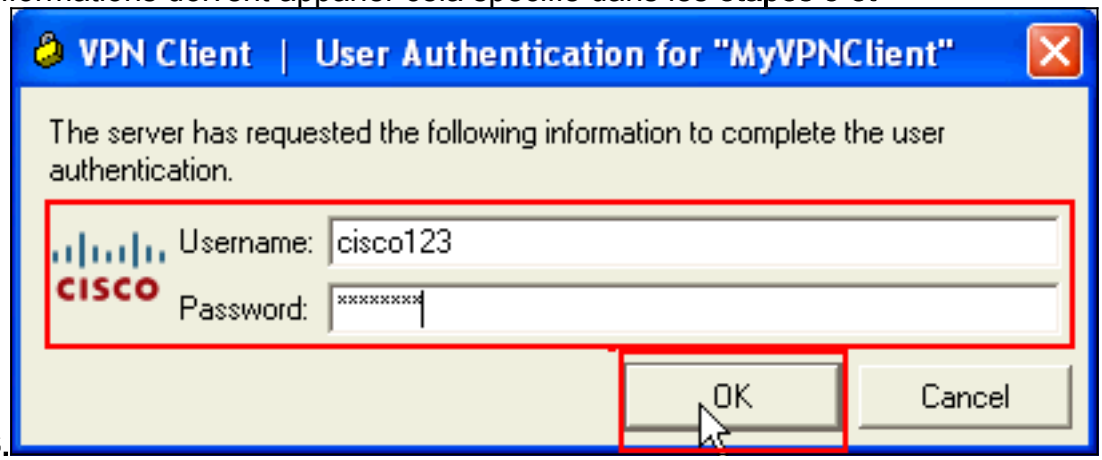


finition.

3. Sélectionnez la connexion de création récente, et cliquez sur **Connect**.

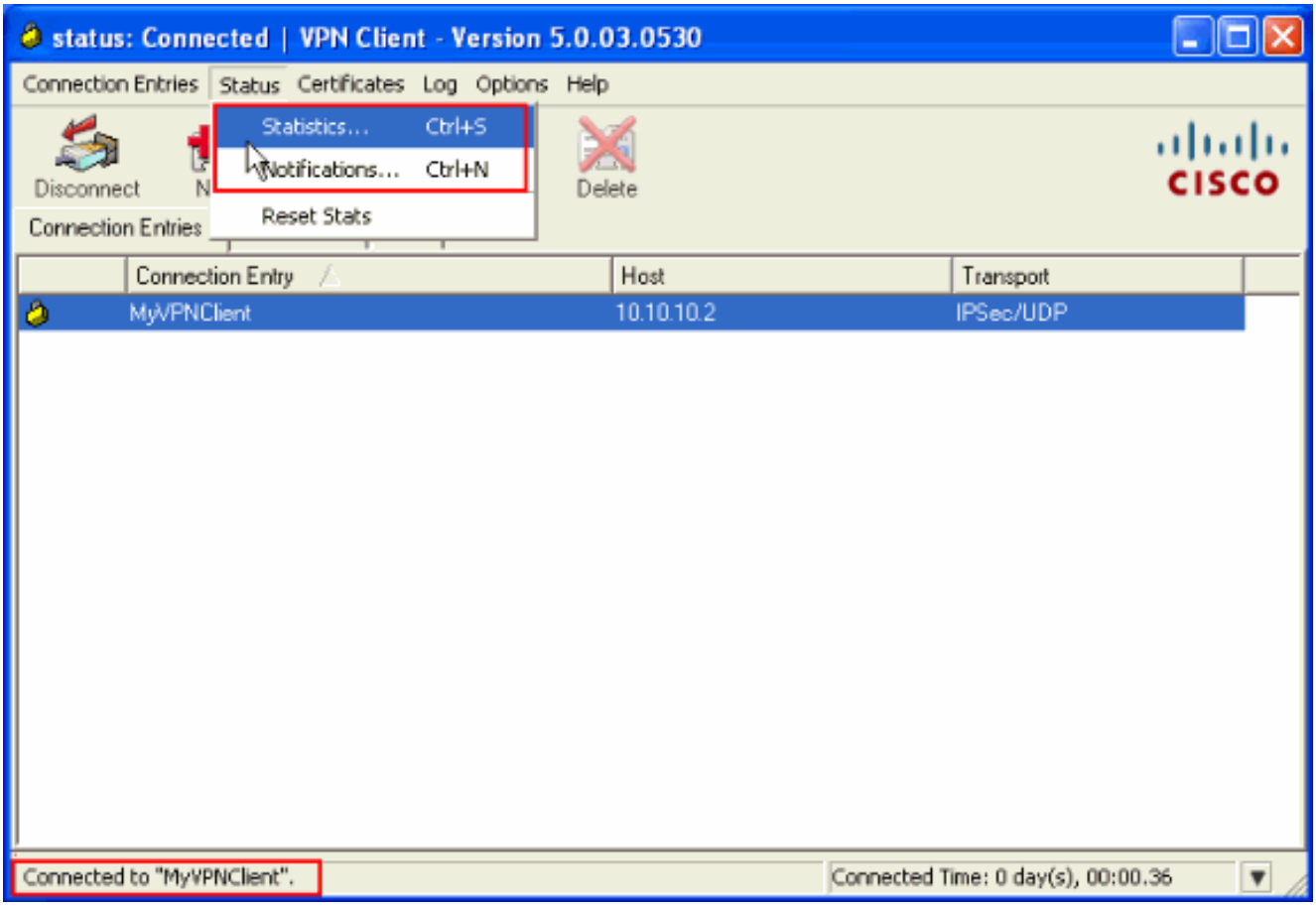


4. Saisissez un nom utilisateur et un mot de passe pour l'authentification étendue. Ces informations doivent apparier cela spécifié dans les **étapes 5 et**

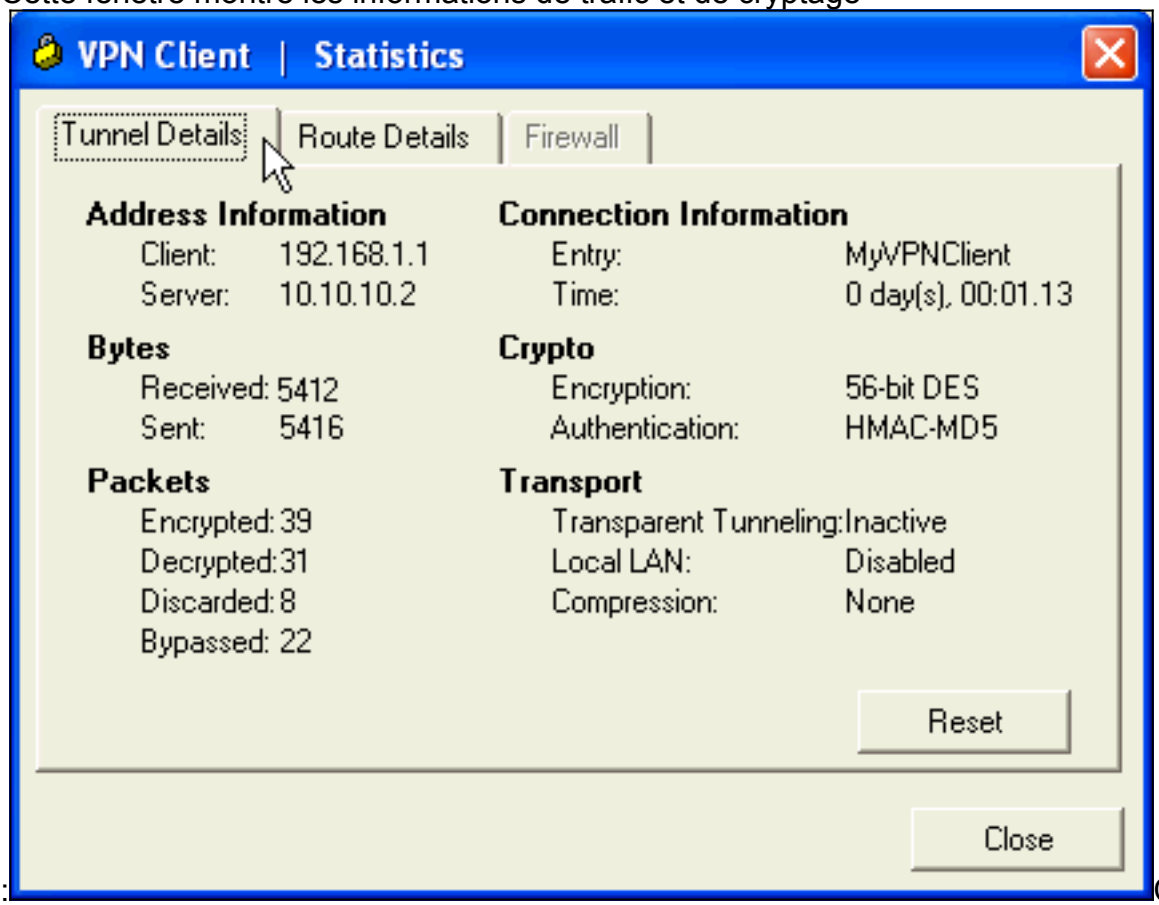


6.

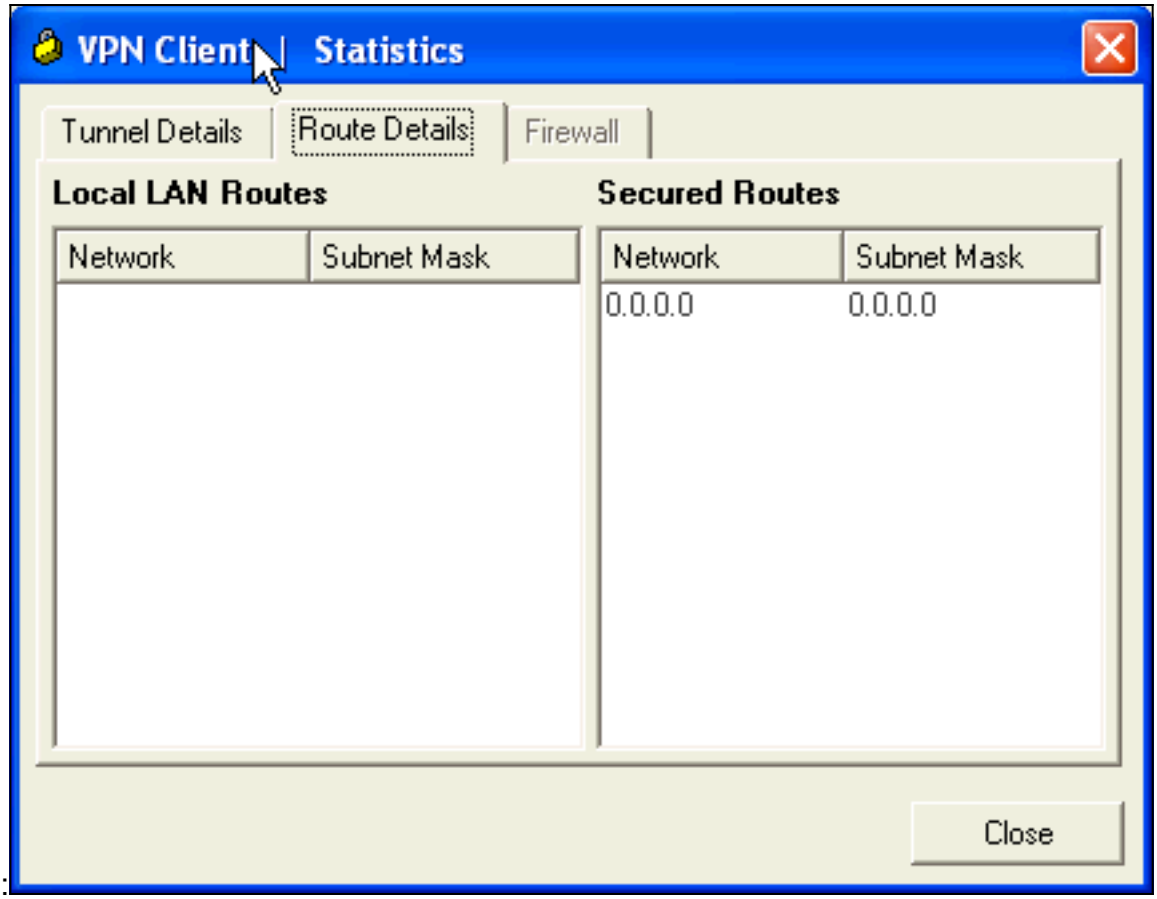
5. Une fois que la connexion est avec succès établie, choisissez les **statistiques du** menu d'état afin de vérifier les détails du
tunnel.



Cette fenêtre montre les informations de trafic et de cryptage



: Cette fenêtre montre les informations de split tunneling



:

Dispositif de sécurité ASA/PIX - Commandes show

- **show crypto isakmp sa** — Affiche toutes les SA IKE en cours au niveau d'un homologue.ASA#**show crypto isakmp sa** Active SA: 1 Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey) Total IKE SA: 1 1 IKE Peer: 10.10.10.1 Type : user Role : responder Rekey : no State : AM_ACTIVE
- **show crypto ipsec sa** — Affiche toutes les SA IPsec en cours au niveau d'un homologue.ASA#**show crypto ipsec sa** interface: Outside **Crypto map tag: SYSTEM_DEFAULT_CRYPTO_MAP, seq num: 65535, local addr: 10.10 .10.2 local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0) remote ident (addr/mask/prot/port): (192.168.1.1/255.255.255.255/0/0) current_peer: 10.10.10.1, username: cisco123 dynamic allocated peer ip: 192.168.1.1 #pkts encaps: 20, #pkts encrypt: 20, #pkts digest: 20 #pkts decaps: 74, #pkts decrypt: 74, #pkts verify: 74 #pkts compressed: 0, #pkts decompressed: 0 #pkts not compressed: 20, #pkts comp failed: 0, #pkts decomp failed: 0** #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0 #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0 #send errors: 0, #recv errors: 0 **local crypto endpt.: 10.10.10.2, remote crypto endpt.: 10.10.10.1** path mtu 1500, ipsec overhead 58, media mtu 1500 current outbound spi: F49F954C inbound esp sas: spi: 0x3C10F9DD (1007745501) transform: esp-des esp-md5-hmac none in use settings ={RA, Tunnel, } slot: 0, conn_id: 24576, crypto-map: SYSTEM_DEFAULT_CRYPTO_MAP sa timing: remaining key lifetime (sec): 27255 IV size: 8 bytes replay detection support: Y outbound esp sas: spi: 0xF49F954C (4104099148) transform: esp-des esp-md5-hmac none in use settings ={RA, Tunnel, } slot: 0, conn_id: 24576, crypto-map: SYSTEM_DEFAULT_CRYPTO_MAP sa timing: remaining key lifetime (sec): 27255 IV size: 8 bytes replay detection support: Y
- ciscoasa(config)#**debug icmp trace** *!--- Inbound Nat Translation is shown below for Outside to Inside* **ICMP echo request translating Outside:192.168.1.1/768 to inside:172.16.1.2/1** ICMP echo reply from inside:172.16.1.3 to Outside:172.16.1.2 ID=1 seq=7936 len=3 2 *!--- Inbound Nat Translation is shown below for Inside to Outside* **ICMP echo reply untranslating inside:172.16.1.2/1 to Outside:192.168.1.1/768** ICMP echo request from Outside:192.168.1.1 to inside:172.16.1.3 ID=768 seq=8192 len=32 ICMP echo request translating Outside:192.168.1.1/768 to inside:172.16.1.2/1 ICMP echo reply from inside:172.16.1.3 to Outside:172.16.1.2 ID=1 seq=8192 len=3 2 ICMP echo reply untranslating inside:172.16.1.2/1

```
to Outside:192.168.1.1/768 ICMP echo request from 192.168.1.1 to 172.16.1.2 ID=768 seq=8448
len=32 ICMP echo reply from 172.16.1.2 to 192.168.1.1 ID=768 seq=8448 len=32 ICMP echo
request from 192.168.1.1 to 172.16.1.2 ID=768 seq=8704 len=32 ICMP echo reply from
172.16.1.2 to 192.168.1.1 ID=768 seq=8704 len=32 ICMP echo request from 192.168.1.1 to
172.16.1.2 ID=768 seq=8960 len=32 ICMP echo reply from 172.16.1.2 to 192.168.1.1 ID=768
seq=8960 len=32
```

Dépannez

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

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** .

Référez-vous à la plupart des L2L et solutions communs de dépannage VPN d'IPSec d'Accès à distance pour plus d'informations sur la façon dépanner le Site-site VPN.

Informations connexes

- Dispositifs de sécurité adaptatifs de la gamme Cisco ASA 5500
- Cisco Adaptive Security Device Manager
- Dépannage et alertes des dispositifs de sécurité adaptatifs de la gamme Cisco ASA 5500
- Support et documentation techniques - Cisco Systems