ASA/PIX : Exemple de configuration d'adressage IP statique pour client VPN IPSec avec CLI et ASDM

Contenu

Introduction

Ce document décrit comment configurer l'appliance de sécurité adaptable de gamme Cisco 5500 (ASA) pour fournir l'IP address statique au client VPN avec Adaptive Security Device Manager (ASDM) ou le CLI. 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 avec le Client VPN Cisco.

Référez-vous à Exemple de configuration d'authentification PIX/ASA 7.x et Client VPN Cisco 4.x avec Windows 2003 RADIUS IAS (sur Active Directory) afin de configurer la connexion VPN d'accès à distance entre un client VPN Cisco (4.x pour Windows) et le dispositif de sécurité 7.x de le gamme PIX 500. L'utilisateur de client vpn distant authentifie contre le Répertoire actif avec un serveur de RAYON de Service d'authentification Internet de Microsoft Windows 2003 (IAS).

Référez-vous à PIX/ASA 7.x et Client VPN Cisco 4.x pour l'exemple de configuration d'authentification de Cisco Secure ACS afin d'installer une connexion VPN d'Accès à distance entre un Client VPN Cisco (4.x pour Windows) et l'appliance 7.x de Sécurité de gamme 500 PIX avec un Cisco Secure Access Control Server (version 3.2 ACS) pour l'authentification étendue

(Xauth).

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.

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 :

- Logiciel Cisco Adaptive Security Appliance versions 7.x et ultérieures
- Adaptive Security Device Manager Versions 5.x et ultérieures
- Client VPN Cisco Versions 4.x et ultérieures

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

Vous pouvez également utiliser cette configuration avec le dispositif de sécurité Cisco PIX Versions 7.x et ultérieures.

Conventions

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

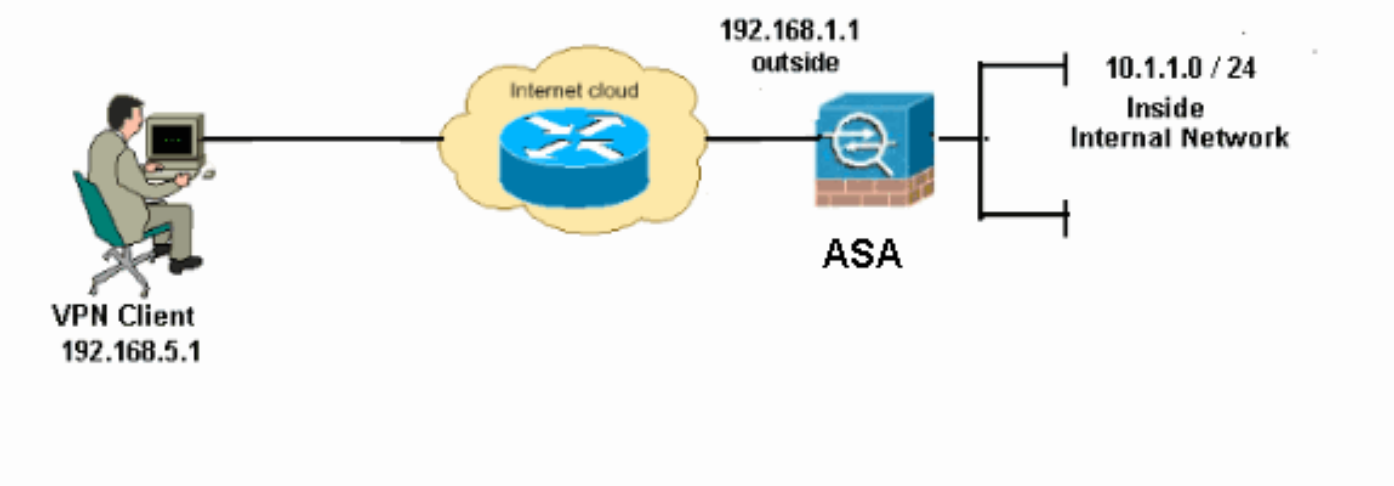
Configurez

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

Remarque: Utilisez l'Outil de recherche de commande (clients enregistrés seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



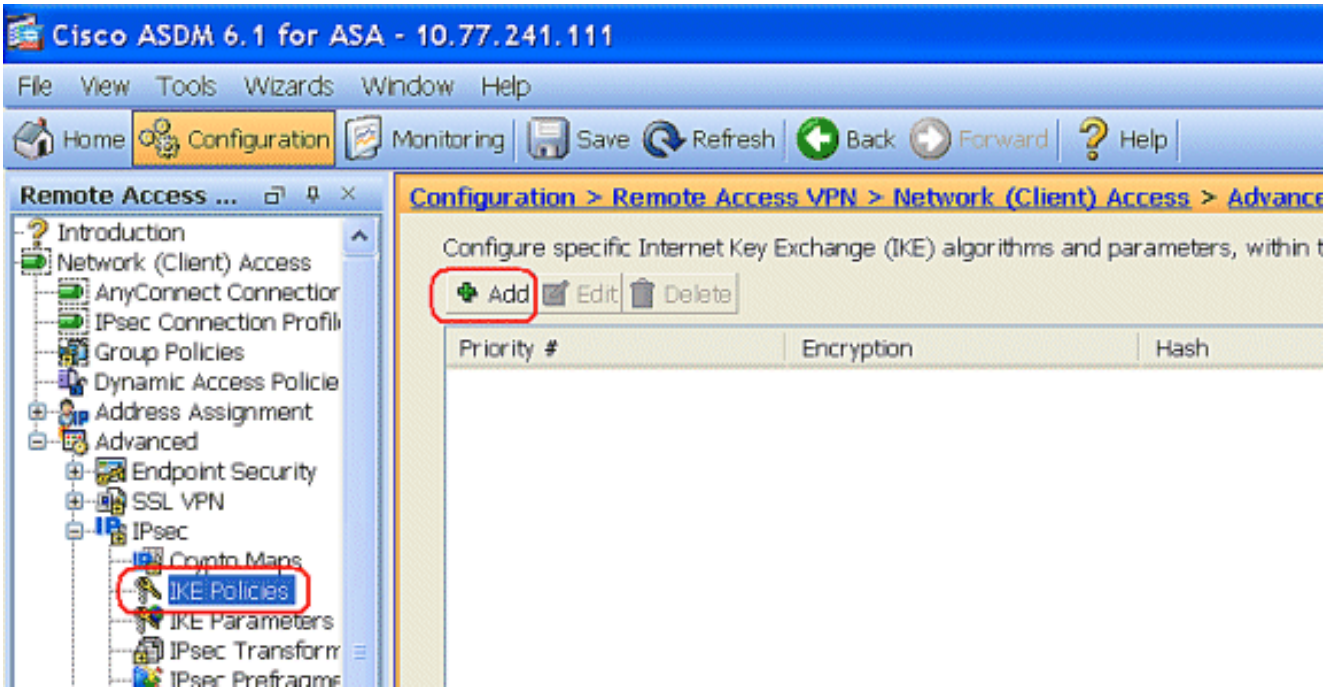
Remarque: Les schémas d'adressage d'IP utilisés dans cette configuration ne sont pas légalement routables sur Internet. Ils sont les adresses RFC 1918, qui ont été utilisées dans un environnement de travaux pratiques.

Configurez l'Accès à distance VPN (IPSec)

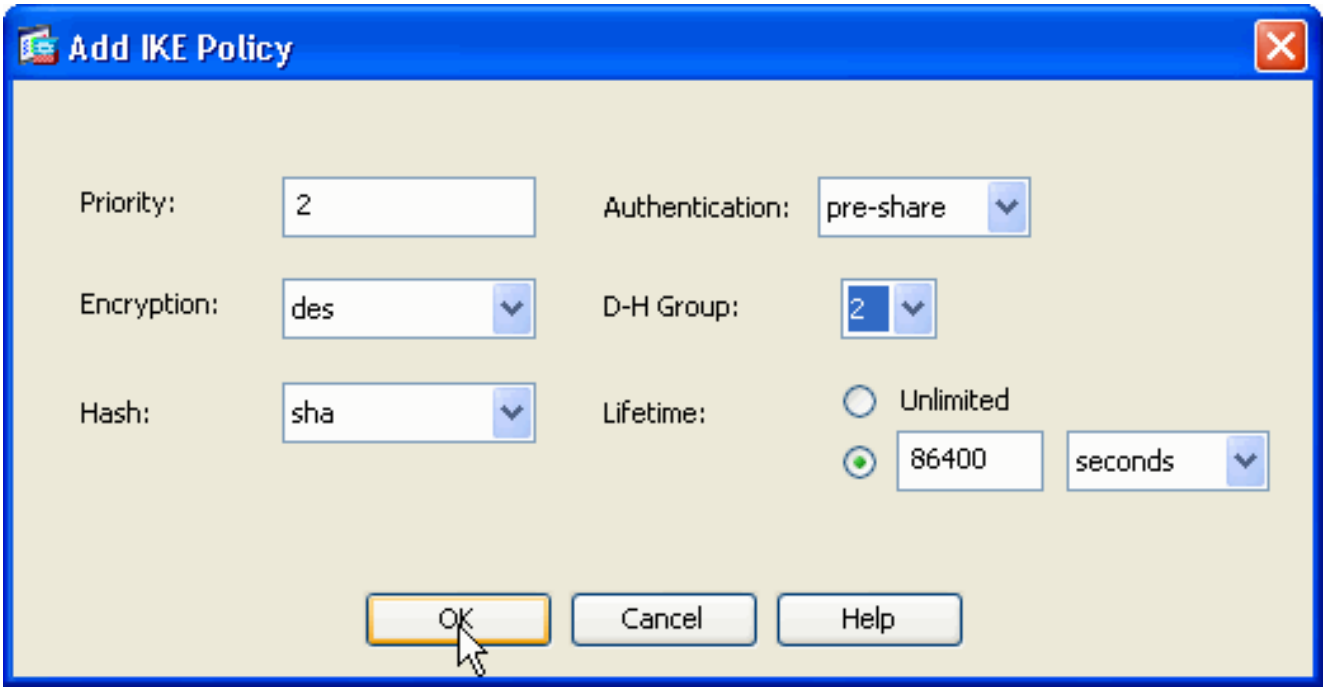
Procédure ASDM

Complétez ces étapes afin de configurer le VPN d'accès à distance :

1. Choisissez la **configuration > l'Accès à distance VPN > réseau (client) Access > a avancé > IPSec > stratégies IKE > ajoutent** afin de créer une stratégie ISAKMP.

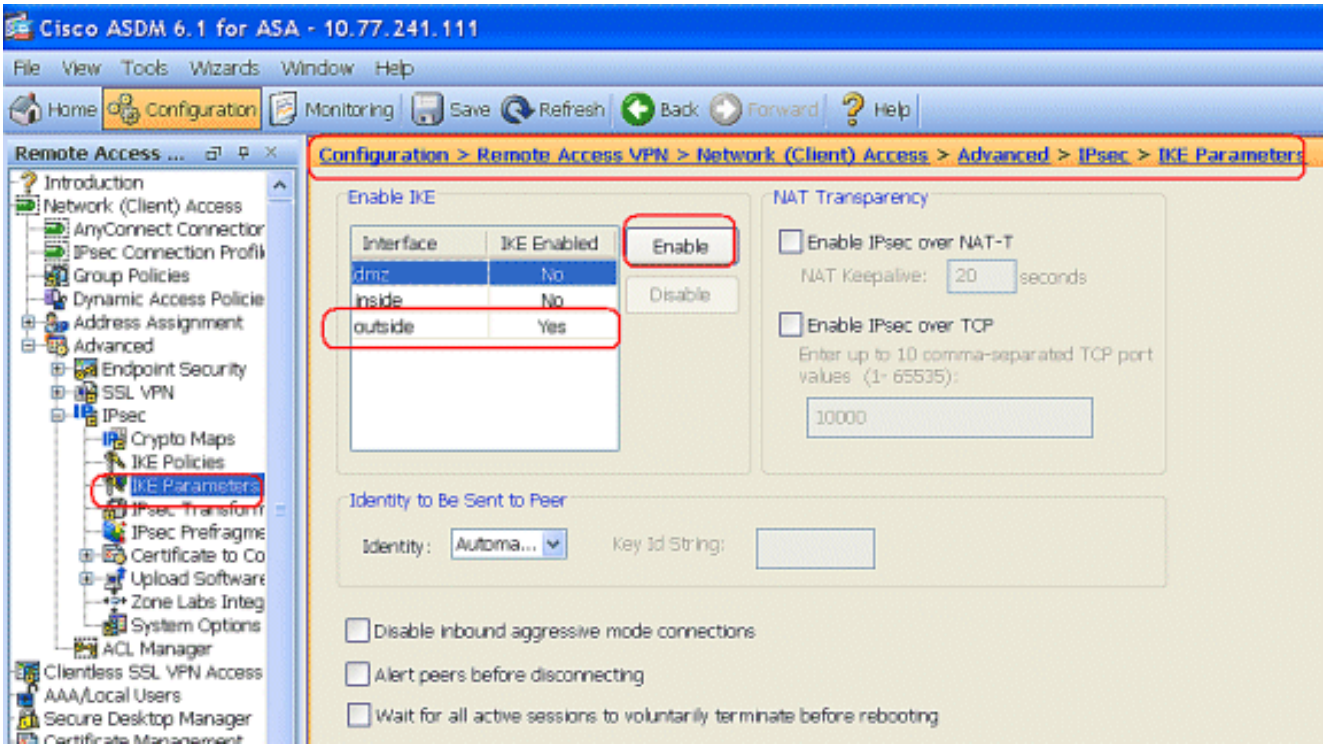


2. Fournissez les détails de stratégie ISAKMP.

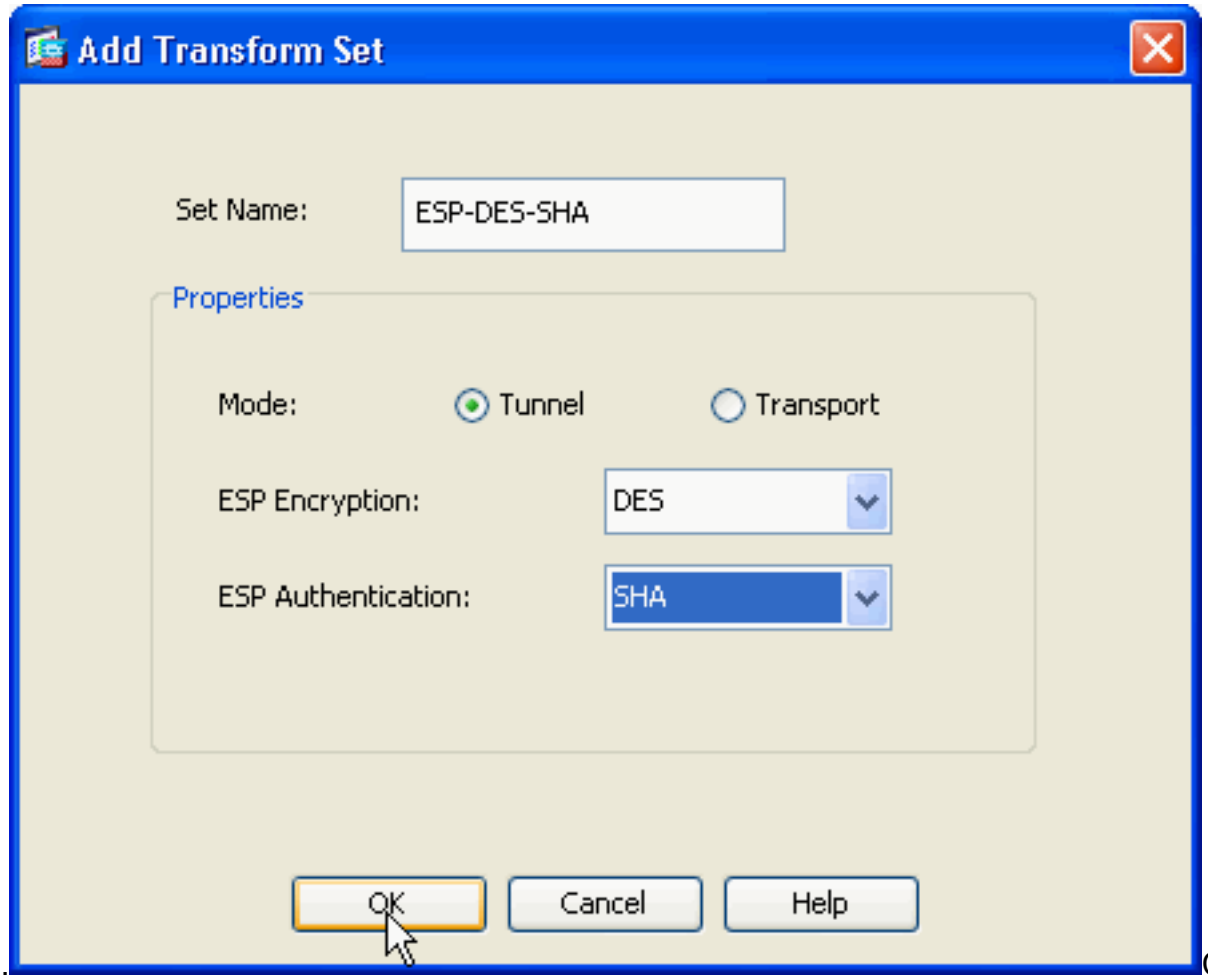


Cliquez sur **OK** et sur **Apply**.

3. Choisissez la **configuration > l'Accès à distance VPN > réseau (client) Access > a avancé > IPSec > paramètres d'IKE** pour activer l'IKE sur l'interface extérieure.

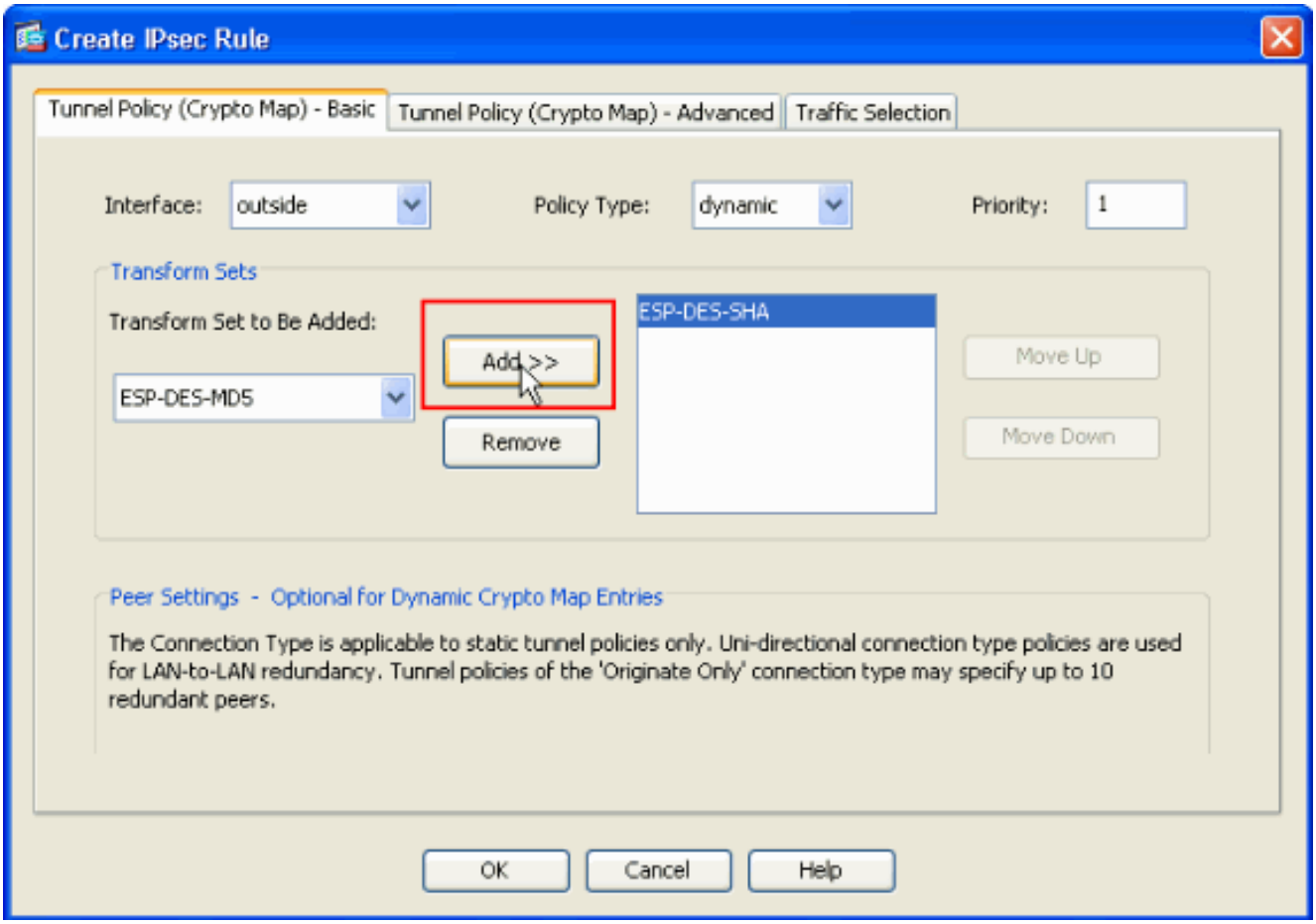


4. Choisissez la **configuration > l'Accès à distance VPN > réseau (client) Access > a avancé > IPSec > jeux de transformations d'IPSec > ajoutent** afin de créer le jeu de transformations **ESP-DES-SHA**, comme



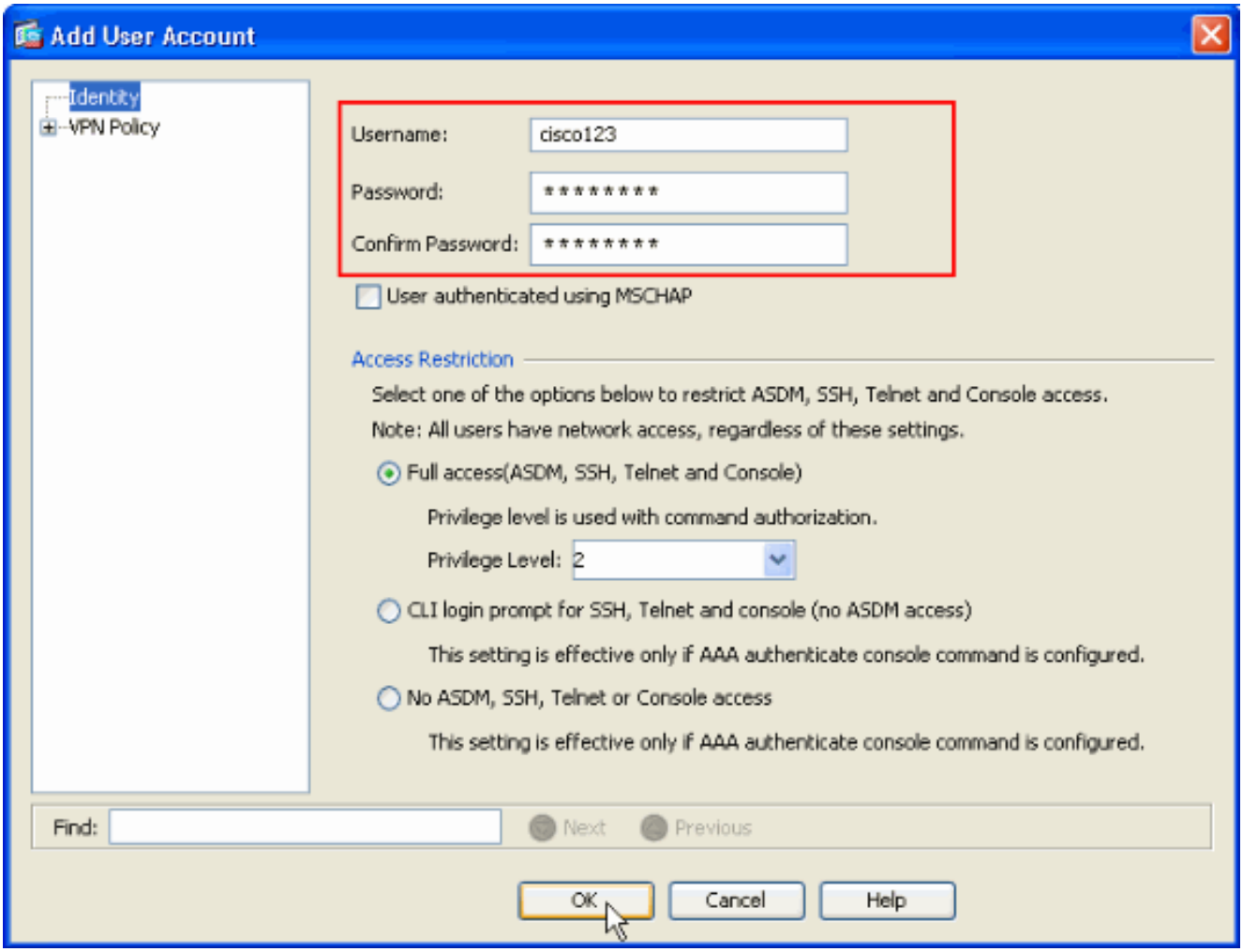
affiché. Cliquez sur **OK** et sur **Apply**.

5. Choisissez la **configuration > l'Accès à distance VPN > réseau (client) Access > a avancé > IPSec > crypto map > ajoutent** afin de créer un crypto map avec la stratégie dynamique de la priorité 1, comme
affiché.

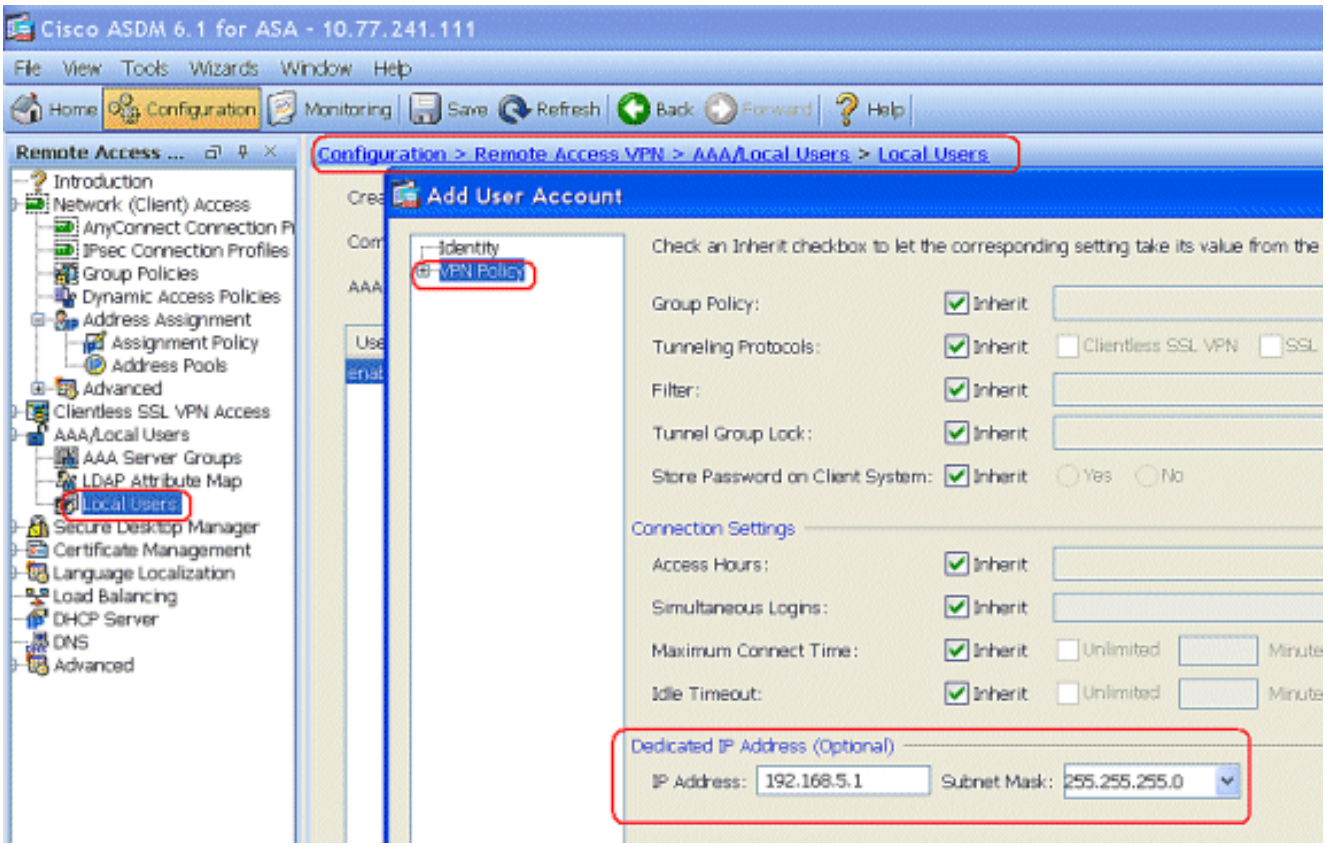


Cliquez sur **OK** et sur **Apply**.

6. Choisissez la **configuration > l'Accès à distance VPN > AAA installé > des utilisateurs locaux > ajoutent** afin de créer le compte utilisateur (par exemple, nom d'utilisateur - cisco123 et mot de passe - cisco123) pour l'accès de client
vpn.

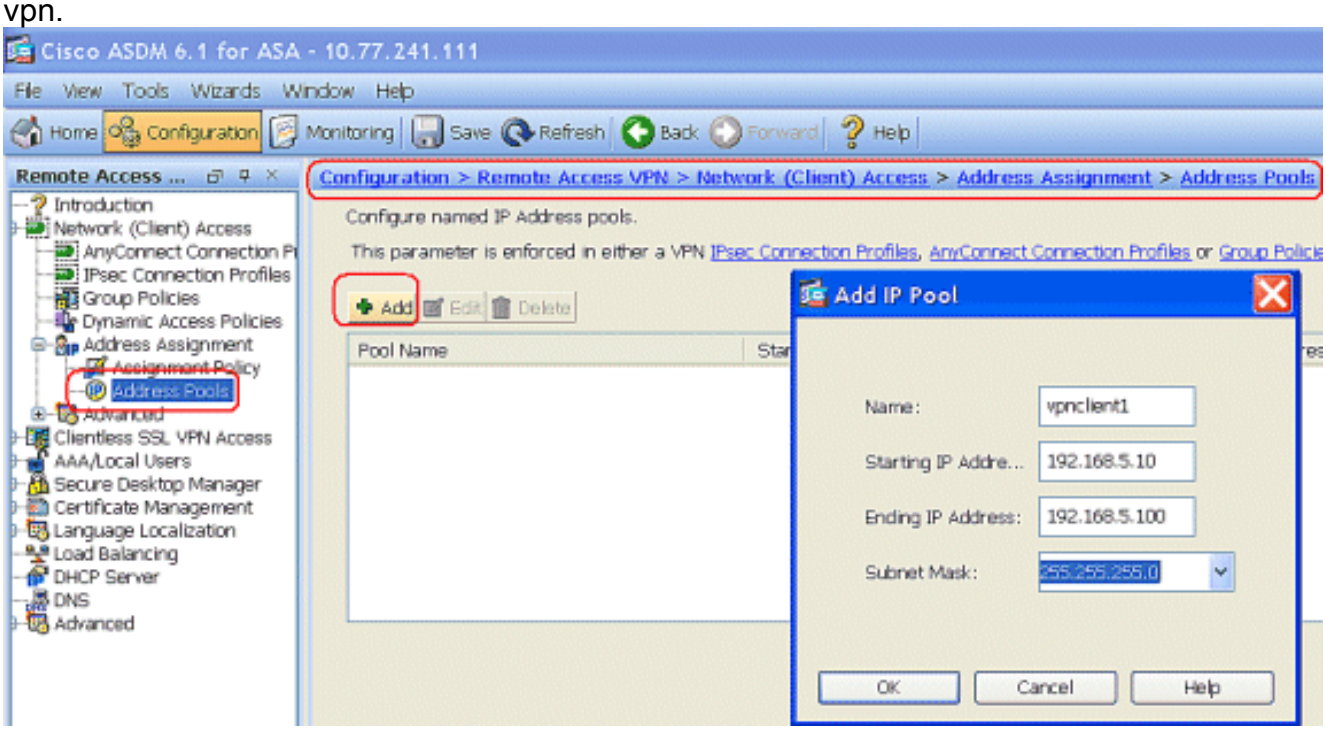


7. Allez à la **règle VPN** et ajoutez la **charge statique/avez dédié l'adresse IP** pour l'utilisateur "cisco123," comme
suit.

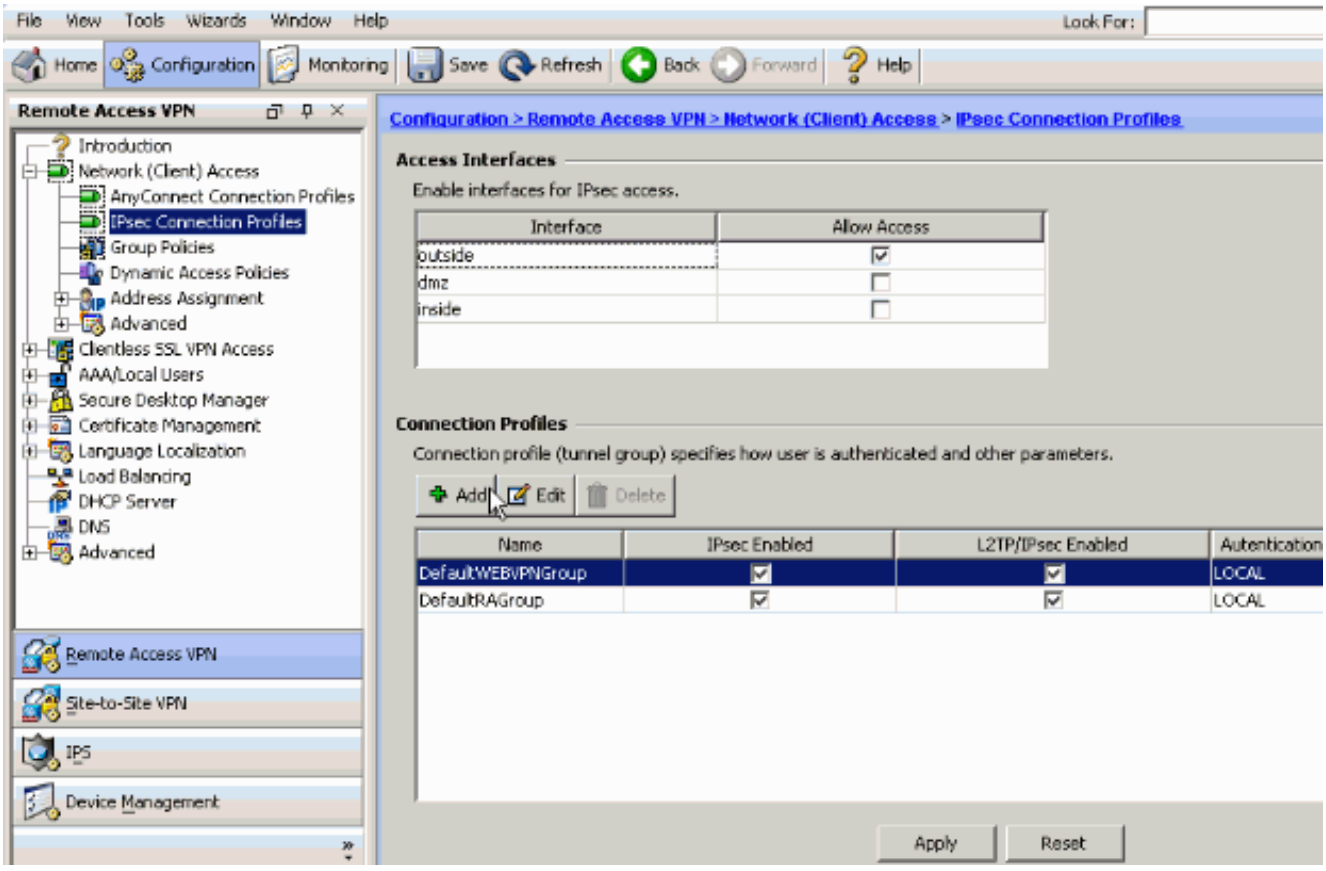


8. Choisissez la **configuration > l'Accès à distance VPN > réseau (client) Access > affectation**

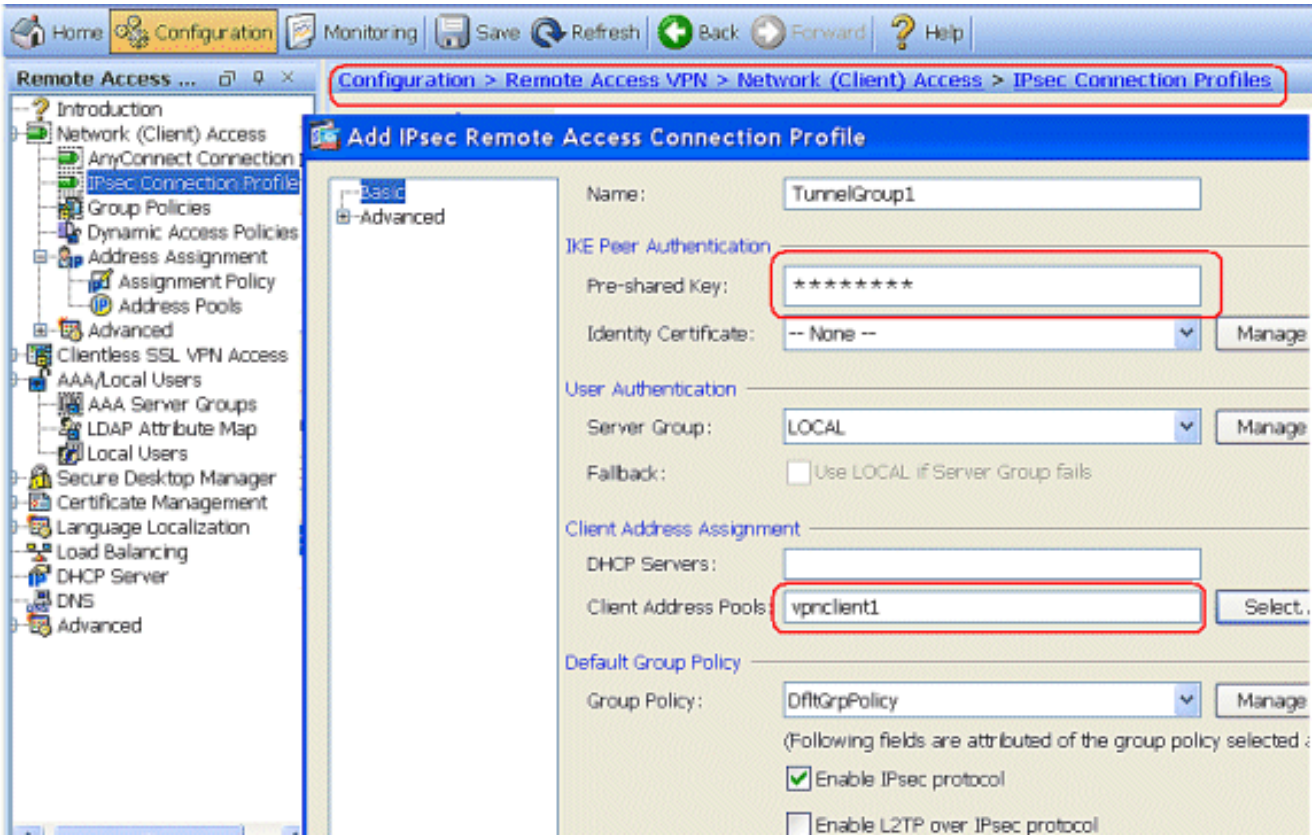
d'adresses > pools d'adresses et cliquez sur Add pour ajouter le client vpn pour des utilisateurs de client
vpn.



9. Choisissez la **configuration > l'Accès à distance VPN > réseau (client) Access > des profils de connexion d'IPSec > ajoutent** afin d'ajouter un groupe de tunnel (par exemple, TunnelGroup1 et la clé pré-partagée comme cisco123), comme
affiché.

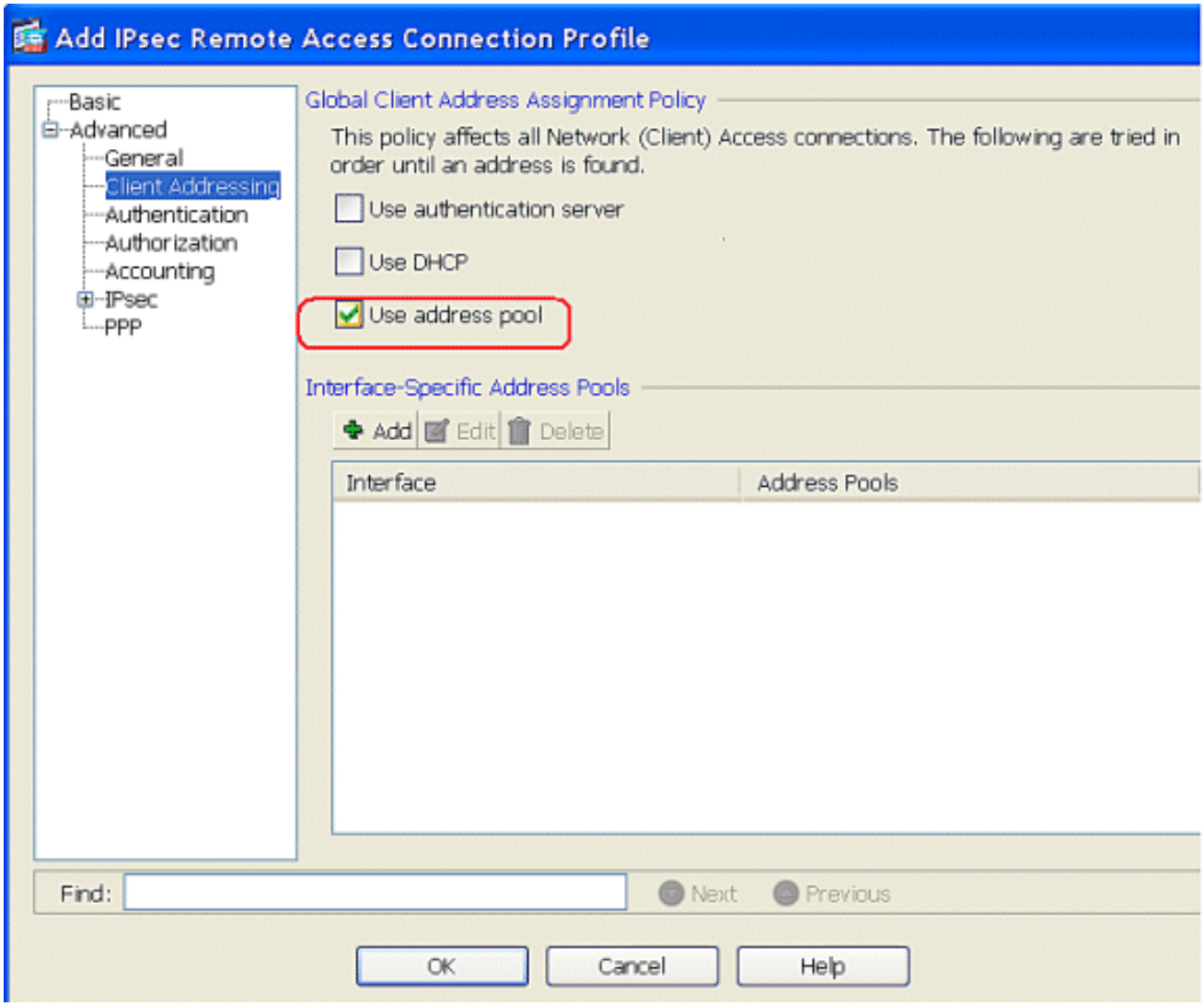


Sous l'onglet **de base**, choisissez le groupe de serveurs comme **GENS DU PAYS** pour le champ d'authentification de l'utilisateur.Choisissez **vpnclient1** en tant que groupes d'adresse du client pour les utilisateurs de client
vpn.



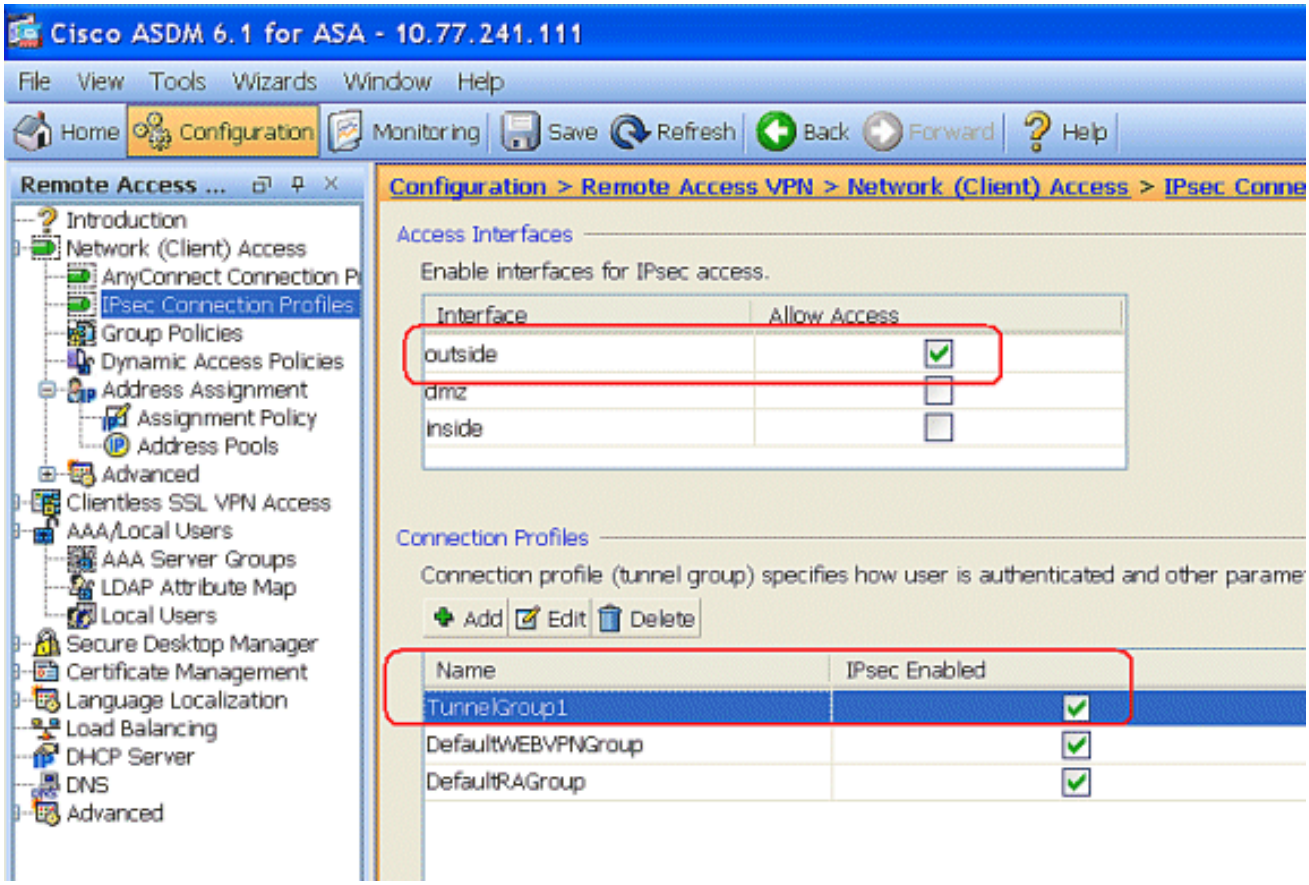
Cliquez sur **OK**.

10. Choisissez **avancé > client adressant** et cochez la case de **pool d'adresses d'utilisation** pour assigner l'adresse IP aux clients vpn.**Remarque:** Veillez à décocher les cases pour le **serveur d'authentification d'utilisation** et **à utiliser le DHCP**.



Cliquez sur **OK**.

11. Activez l'interface **extérieure** pour IPSec Access. Cliquez sur Apply pour poursuivre.



Configurer ASA/PIX avec CLI

Terminez-vous ces étapes afin de configurer le serveur DHCP pour fournir des adresses IP aux clients vpn de la ligne de commande. Référez-vous à Configurer les vpn d'accès à distance ou Dispositifs de sécurité adaptatifs dédiés de la gamme Cisco ASA 5505-Références de commande pour plus d'informations sur chaque commande qui est utilisée.

Configuration en cours sur le périphérique ASA

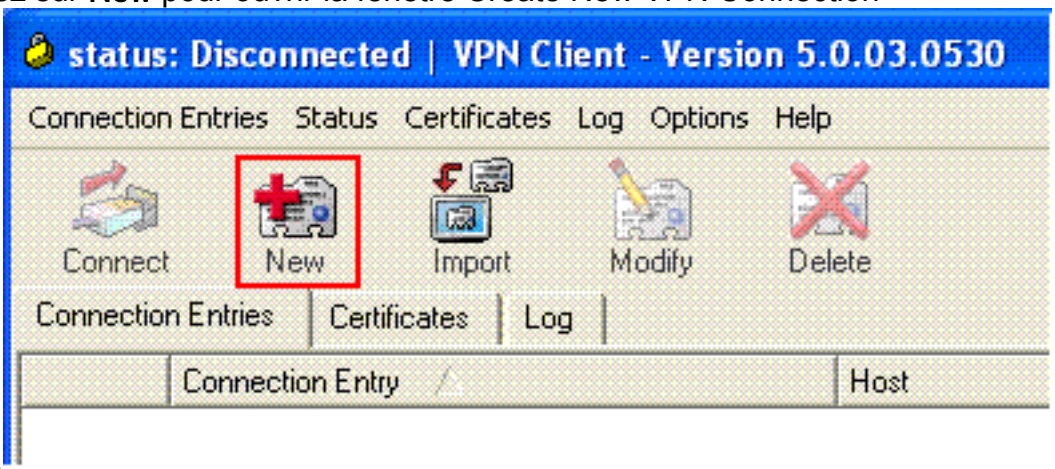
```
ASA# sh run
ASA Version 8.0(2)
!
!--- Specify the hostname for the Security Appliance.
hostname ASA enable password 8Ry2YjIyt7RRXU24 encrypted
names ! !--- Configure the outside and inside
interfaces. interface Ethernet0/0 nameif inside
security-level 100 ip address 10.1.1.1 255.255.255.0 !
interface Ethernet0/1 nameif outside security-level 0 ip
address 192.168.1.1 255.255.255.0 ! interface
Ethernet0/2 nameif DMZ security-level 50 ip address
192.168.10.2 255.255.255.0 !--- Output is suppressed.
passwd 2KFQnbNIdI.2KYOU encrypted boot system
disk0:/asa802-k8.bin ftp mode passive access-list 101
extended permit ip 10.1.1.0 255.255.255.0 192.168.5.0
255.255.255.0 pager lines 24 logging enable logging asdm
informational mtu inside 1500 mtu outside 1500 mtu dmz
1500 ip local pool vpnclient1 192.168.5.10-192.168.5.100
mask 255.255.255.0 no failover icmp unreachable rate-
limit 1 burst-size 1 !--- Specify the location of the
ASDM image for ASA to fetch the image for ASDM access.
asdm image disk0:/asdm-613.bin no asdm history enable
arp timeout 14400 global (outside) 1 192.168.1.5 nat
(inside) 0 access-list 101 nat (inside) 1 0.0.0.0
```

```
0.0.0.0 route outside 0.0.0.0 0.0.0.0 192.168.1.2 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 http 0.0.0.0 0.0.0.0 inside no snmp-server
location no snmp-server contact snmp-server enable traps
snmp authentication linkup linkdown coldstart crypto
ipsec transform-set ESP-DES-SHA esp-des esp-sha-hmac
crypto dynamic-map outside_dyn_map 1 set transform-set
ESP-DES-SHA crypto map outside_map 1 ipsec-isakmp
dynamic outside_dyn_map !--- Specifies the interface to
be used with !--- the settings defined in this
configuration. crypto map outside_map interface outside
!--- PHASE 1 CONFIGURATION ---! !--- This configuration
uses ISAKMP policy 2. !--- The configuration commands
here define the Phase !--- 1 policy parameters that are
used. crypto isakmp enable outside crypto isakmp policy
2 authentication pre-share encryption des hash sha group
2 lifetime 86400 no crypto isakmp nat-traversal !---
Specifies that the IP address to the vpn clients are
assigned by the local and not by AAA or dhcp. The CLI
vpn-addr-assign local for VPN address assignment through
ASA is hidden in the CLI provided by show run command.
no vpn-addr-assign aaa no vpn-addr-assign dhcp telnet
timeout 5 ssh timeout 5 console timeout 0 threat-
detection basic-threat threat-detection statistics
access-list ! 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 ! group-policy DfltGrpPolicy
attributes vpn-tunnel-protocol IPSec webvpn group-policy
GroupPolicy1 internal !--- In order to identify remote
access users to the Security Appliance, !--- you can
also configure usernames and passwords on the device. !-
-- specify the IP address to assign to a particular
user, use the vpn-framed-ip-address command !--- in
username mode username cisco123 password
ffIRPGpDSOJh9YLq encrypted username cisco123 attributes
vpn-framed-ip-address 192.168.5.1 255.255.255.0 !---
Create a new tunnel group and set the connection !---
type to remote-access. tunnel-group TunnelGroup1 type
remote-access tunnel-group TunnelGroup1 general-
attributes address-pool vpnclient1 !--- Enter the pre-
shared-key to configure the authentication method.
tunnel-group TunnelGroup1 ipsec-attributes pre-shared-
key * prompt hostname context
Cryptochecksum:e0725ca9ccc28af488ded9ee36b7822d : end
ASA#
```

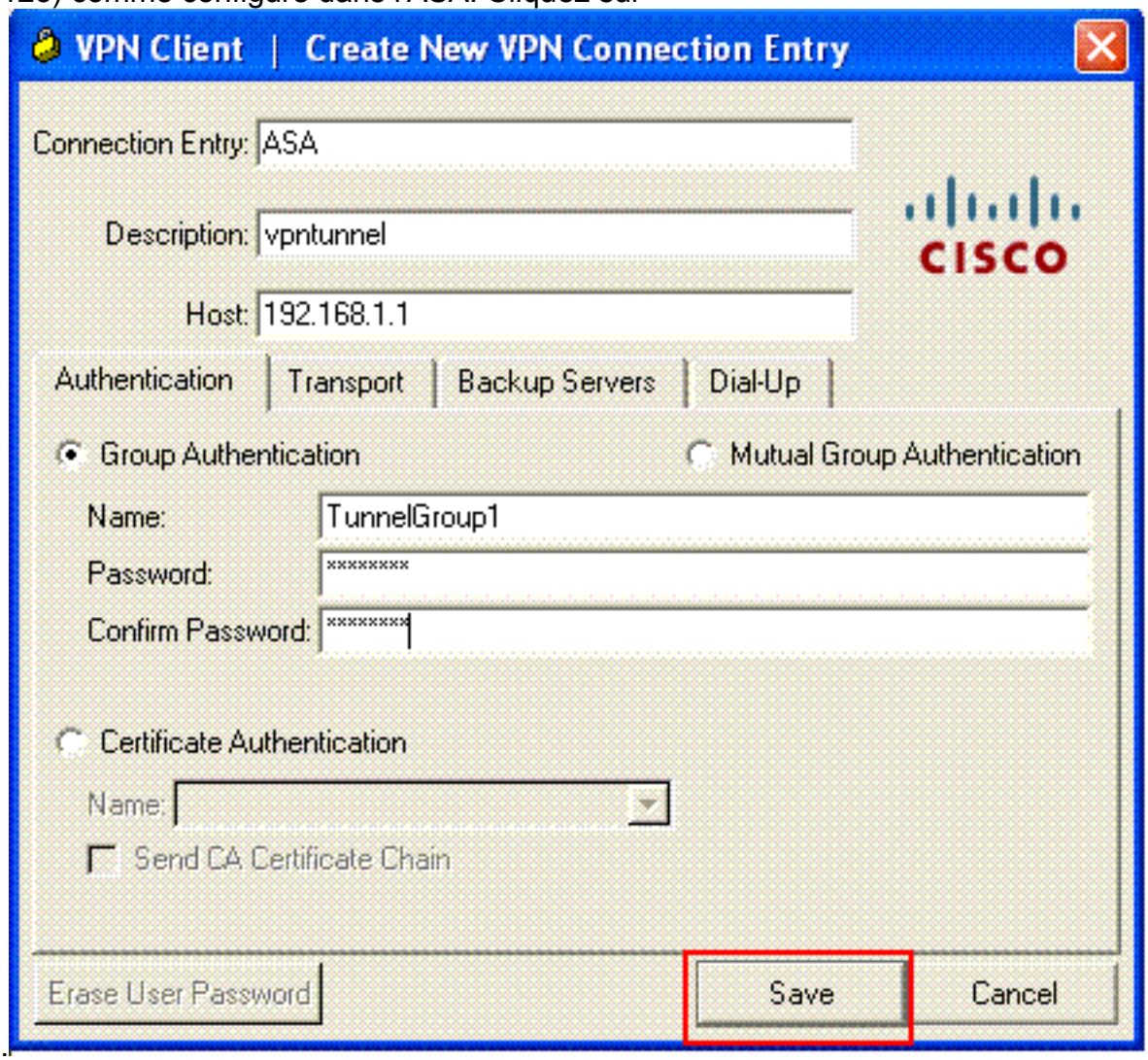
Configuration de Client VPN Cisco

Tentez de se connecter à Cisco ASA au Client VPN Cisco afin de vérifier que l'ASA est avec succès configurée.

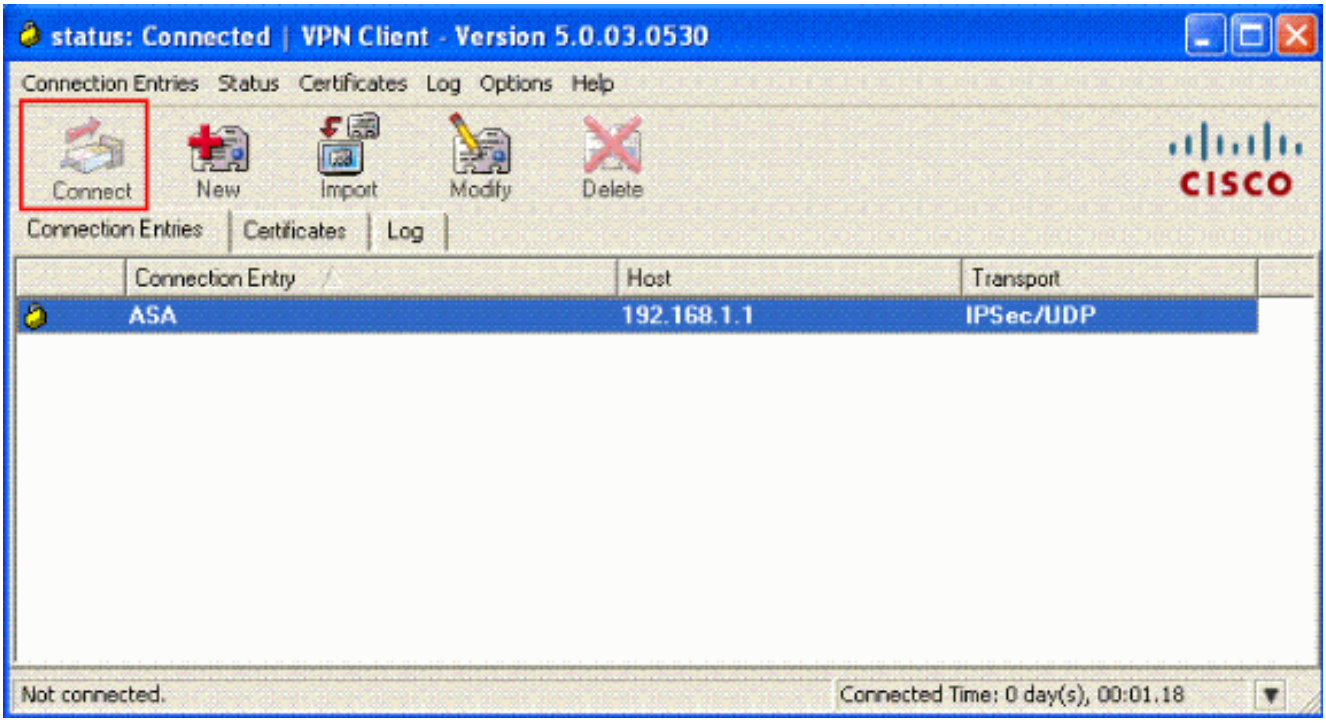
1. Choisissez le **début > les programmes > le client vpn de Cisco Systems > le client vpn**.
2. Cliquez sur **New** pour ouvrir la fenêtre Create New VPN Connection



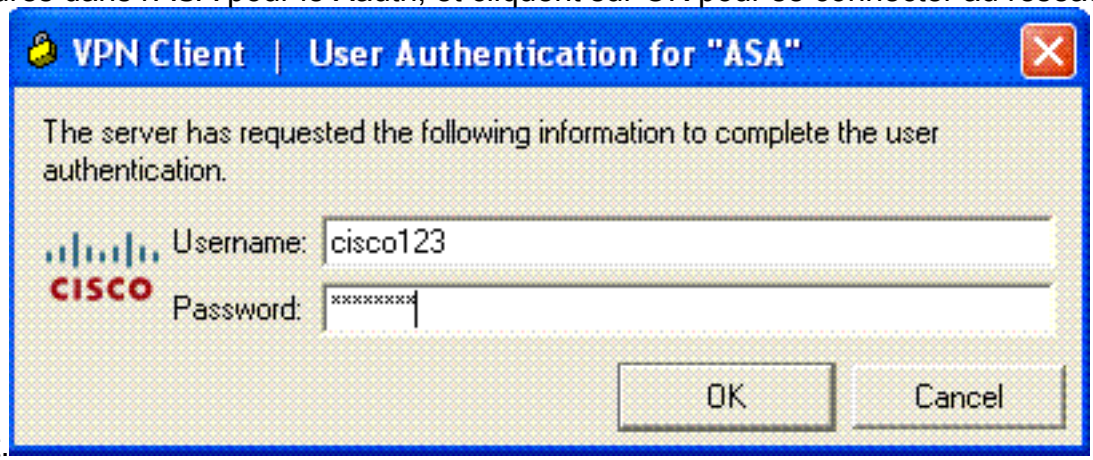
Entry.
3. Complétez les détails de votre nouvelle connexion.Entrez le nom de l'entrée de connexion avec une description. Écrivez l'**adresse IP extérieure de l'ASA** dans la case d'hôte. Entrez alors le nom de groupe de tunnel VPN (TunnelGroup1) et le mot de passe (clé pré-partagée - cisco123) comme configuré dans l'ASA. Cliquez sur



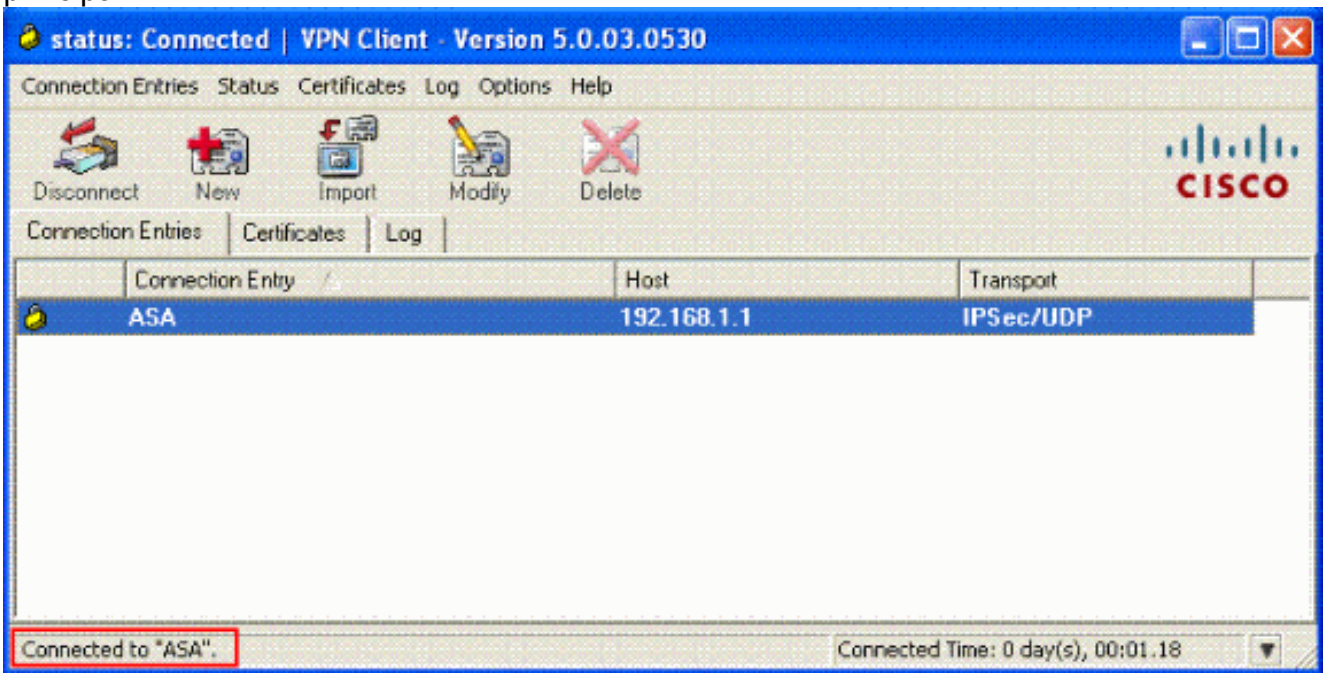
Save.
4. Cliquez sur la connexion que vous voulez utiliser, et le clic **se connectent de la** fenêtre principale de client
vpn.



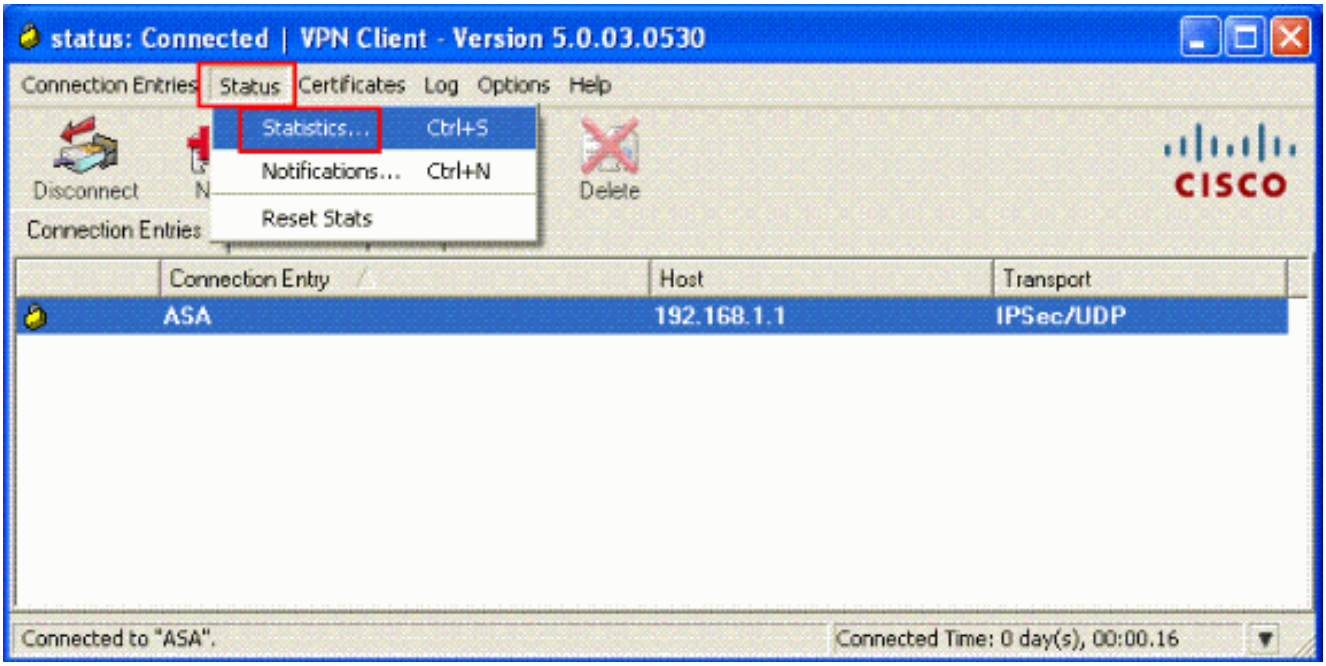
5. Une fois incité, écrivez le **nom d'utilisateur : cisco123** et **mot de passe : cisco123** comme configurés dans l'ASA pour le Xauth, et cliquent sur OK pour se connecter au réseau distant.



6. Le client vpn est connecté à l'ASA au lieu d'exploitation principal.



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



Vérifiez

Commandes show

Référez-vous à cette section pour vous assurer du bon fonctionnement de 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** .

- **show crypto isakmp sa** — Affiche toutes les associations de sécurité actuelles IKE (SA) sur un homologue.
- **show crypto ipsec sa** — Affiche les paramètres utilisés par les SA en cours.

Dépannez

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration. L'exemple de sortie Debug est également affiché.

Remarque: Pour plus d'informations sur l'Accès à distance IPSec VPN de dépannage référez-vous la plupart des solutions communes de dépannage VPN d'IPSec L2L et d'Accès à distance.

Suppression des associations de sécurité

Quand vous dépannez, veillez à autoriser les associations de sécurité existantes après que vous apportiez une modification. En mode privilégiée du PIX, utilisez les commandes suivantes :

- **clear [crypto] ipsec sa** - Supprime les SA IPSec actives. Le mot clé crypto est facultatif.
- **clear [crypto] isakmp sa** — supprime les SA IKE actives. Le mot clé crypto est facultatif.

Dépannage des commandes

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** .

Remarque: Référez-vous aux informations importantes sur les commandes de débogage avant d'utiliser les commandes de **débogage**.

- **debug crypto ipsec 7** — Affiche les négociations IPsec de la phase 2.
- **debug crypto isakmp 7** — Affiche les négociations ISAKMP de la phase 1.

Informations connexes

- Page d'assistance des appliances de sécurité adaptables de la gamme Cisco ASA 5500
- Références de commandes de Dispositifs de sécurité adaptatifs dédiés de la gamme Cisco ASA 5500
- Page de support pour serveurs de sécurité de la gamme Cisco PIX 500
- Référence de commandes de Dispositifs de sécurité de la gamme Cisco PIX 500
- Cisco Adaptive Security Device Manager
- Page de support de la négociation IPSec/des protocoles IKE
- Cisco VPN Client Support Page
- Logiciels pare-feu Cisco PIX
- Références des commandes du pare-feu Cisco Secure PIX
- Notices de champs relatives aux produits de sécurité (y compris PIX)
- Demandes de commentaires (RFC)
- Support et documentation techniques - Cisco Systems