ASA/PIX : Exemple de configuration d'adressage client VPN IPSec à l'aide de serveur DHCP avec client ASDM

Contenu

Introduction

Ce document décrit comment configurer l'appliance de sécurité adaptable (ASA) de la gamme Cisco 5500 pour inciter le serveur DHCP à fournir l'adresse IP du client à tous les clients VPN en utilisant Adaptive Security Device Manager (ASDM) ou 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 Cisco ASA est complète, elle peut être vérifiée en utilisant 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 distant du Client VPN authentifie contre l'Active Directory en utilisant un serveur RADIUS du service d'authentification Internet (IAS) de Microsoft Windows 2003.

Référez-vous à PIX/ASA 7.x et Client VPN Cisco 4.x pour un exemple de configuration d'authentification Cisco secure ACS afin d´établir une 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 à l´aide d´un Cisco Secure Access Control Server (ACS version 3.2) 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.

Informations générales

Les VPN d'accès à distance adressent la condition requise du collaborateur mobile pour se connecter en toute sécurité au réseau de l'entreprise. Les utilisateurs mobiles peuvent configurer une connexion sécurisée à l'aide du logiciel client VPN installé sur leurs PC. Le client VPN initie une connexion au périphérique d'un site central configuré pour accepter ces requêtes. Dans cet exemple, le périphérique de lieu d'exploitation principal est une appliance de sécurité adaptable de la gamme ASA 5500 qui utilise des crypto-cartes dynamiques.

En gestion d'adresses de dispositifs de sécurité nous devons configurer les adresses IP qui connectent un client à une ressource sur le réseau privé, par le tunnel, et permettent le client de fonctionner comme si il ont été directement connectés au réseau privé. En outre, nous traitons seulement les adresses IP privées qui obtiennent assigné aux clients. Les adresses IP assignées à d'autres ressources sur votre réseau privé font partie de vos responsabilités d'administration réseau, pas une partie de Gestion VPN. Par conséquent, quand des adresses IP sont discutées ici, nous voulons dire ces adresses IP disponibles dans votre système d'adressage du réseau privé ce avons permis la fonction de client comme périphérique du tunnel.

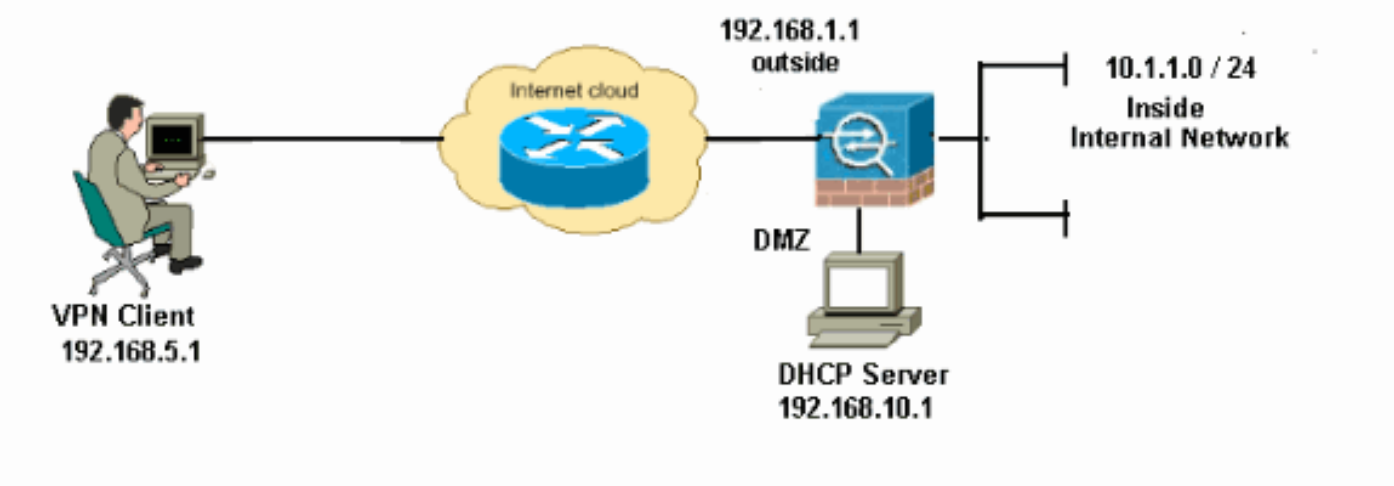
Configurez

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 :



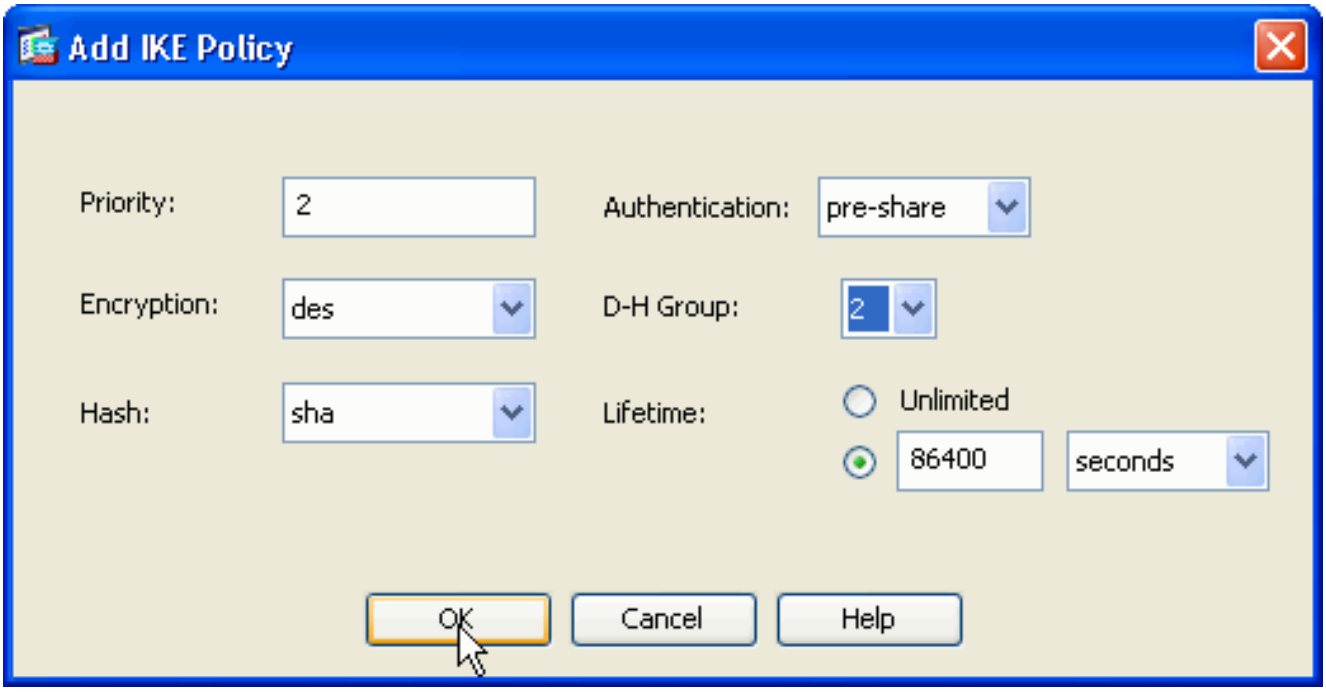
Remarque: Les schémas d'adressage d'IP utilisés dans cette configuration ne sont pas légalement routables sur Internet. Ce sont des adresses RFC 1918 qui ont été utilisées dans un environnement de laboratoire.

Configurez l'Accès à distance VPN (IPSec)

Procédure ASDM

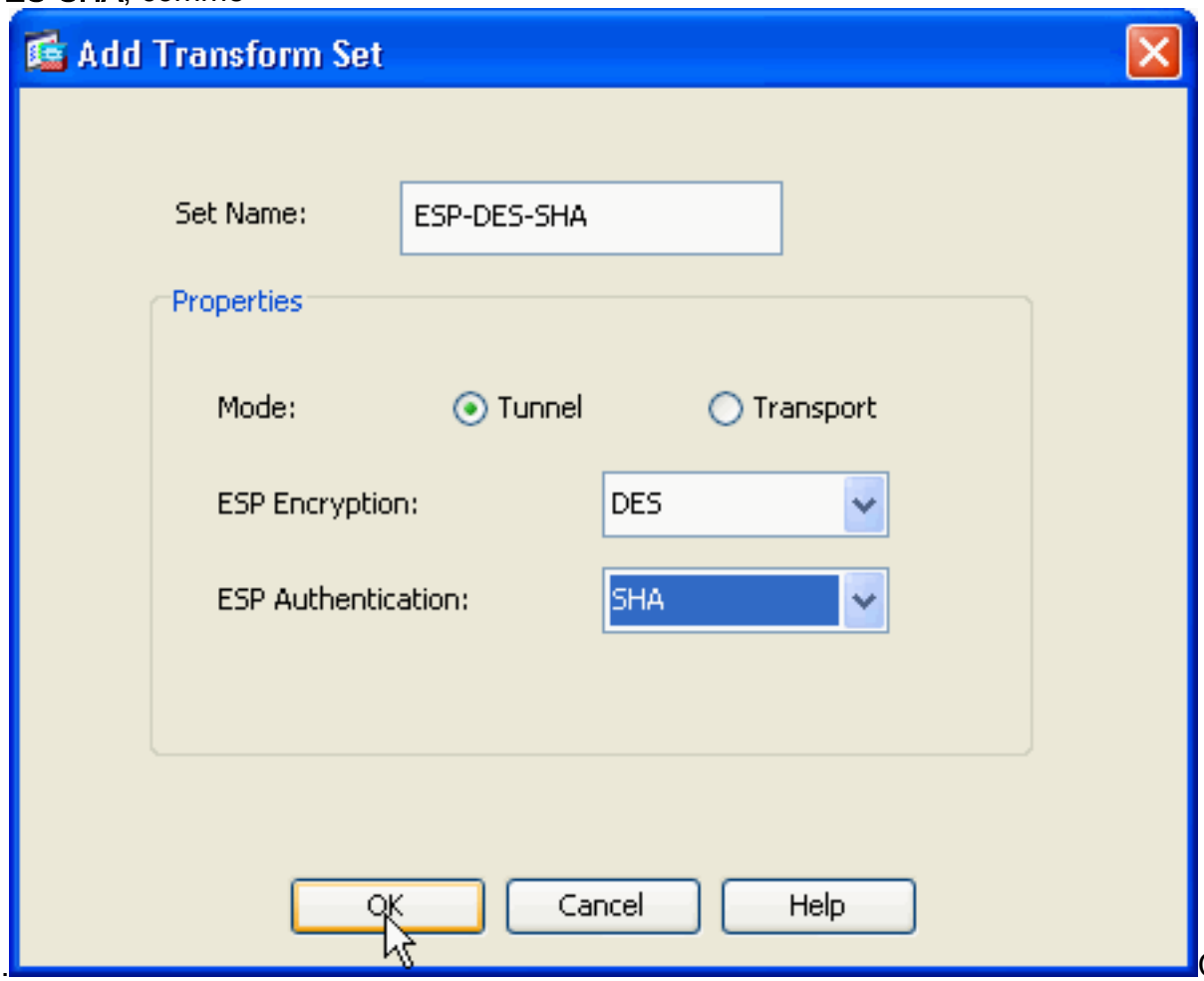
Complétez ces étapes afin de configurer le VPN d'accès à distance :

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, comme affiché.



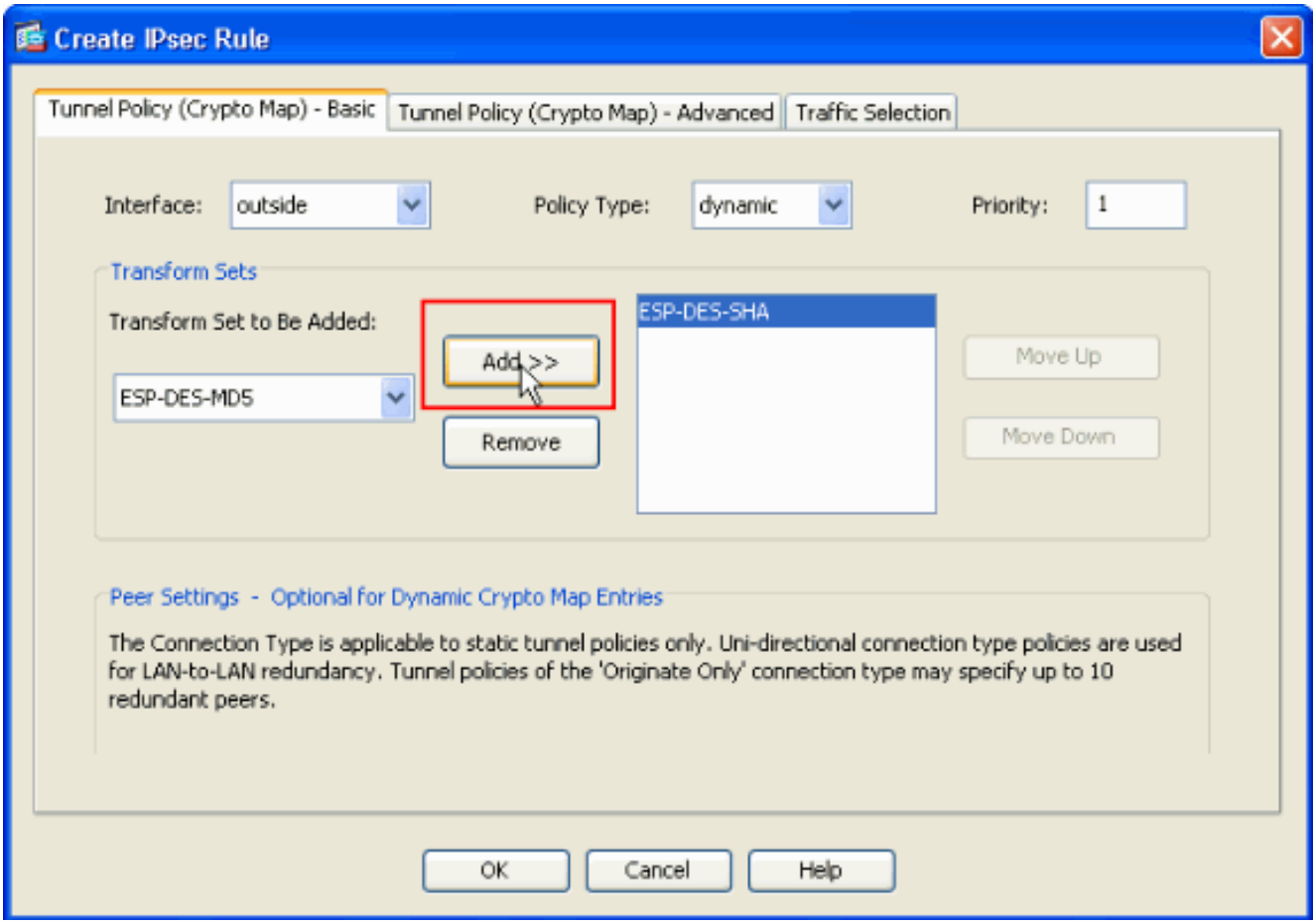
Cliquez sur **OK** et sur **Apply**.

2. 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.



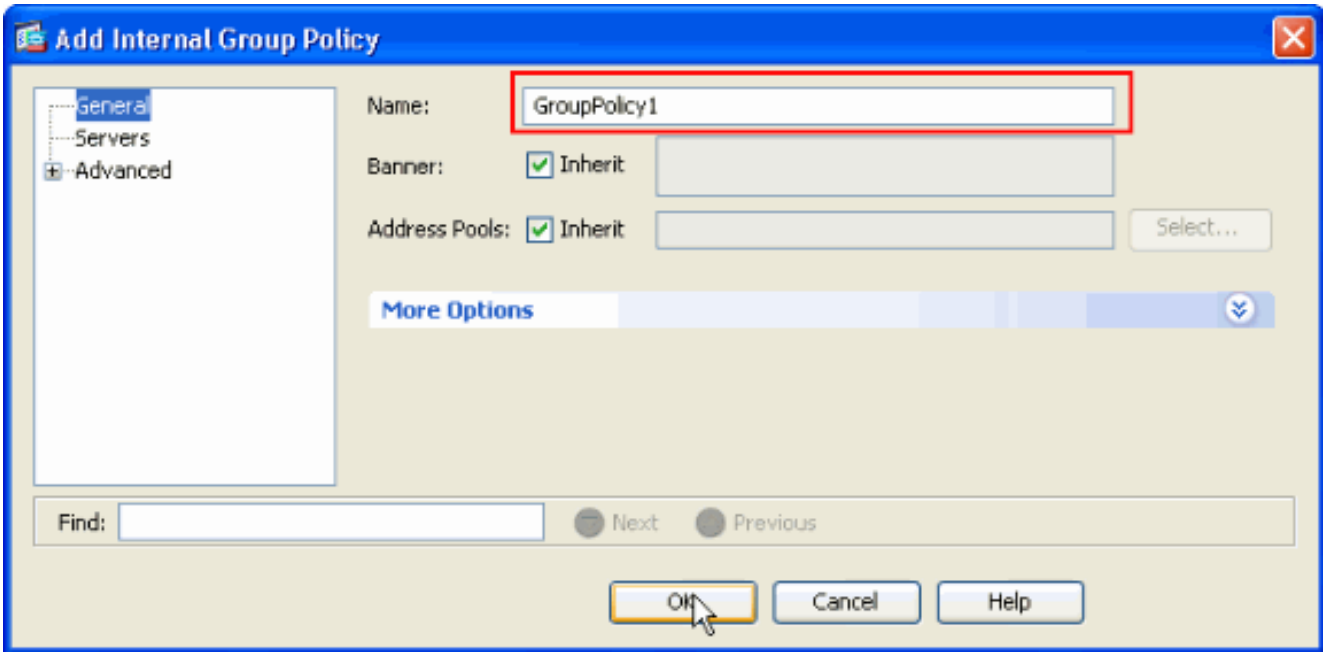
Cliquez sur **OK** et sur **Apply**.

3. 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.



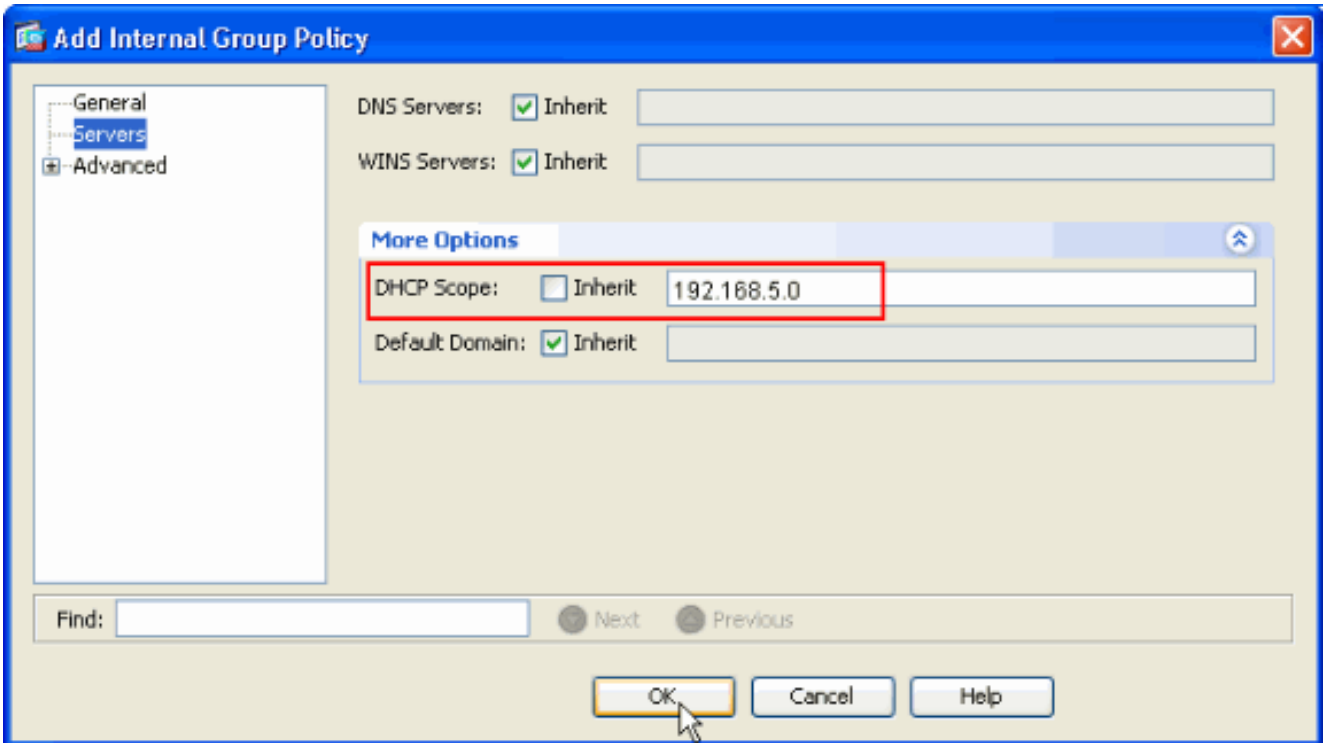
Cliquez sur **OK** et sur **Apply**.

4. Choisissez la **configuration > l'Accès à distance VPN > réseau (client) Access > a avancé > des stratégies de groupe > des stratégies de groupe d'Add>Internal** afin de créer une stratégie de groupe (par exemple **GroupPloicy1**), comme affiché.



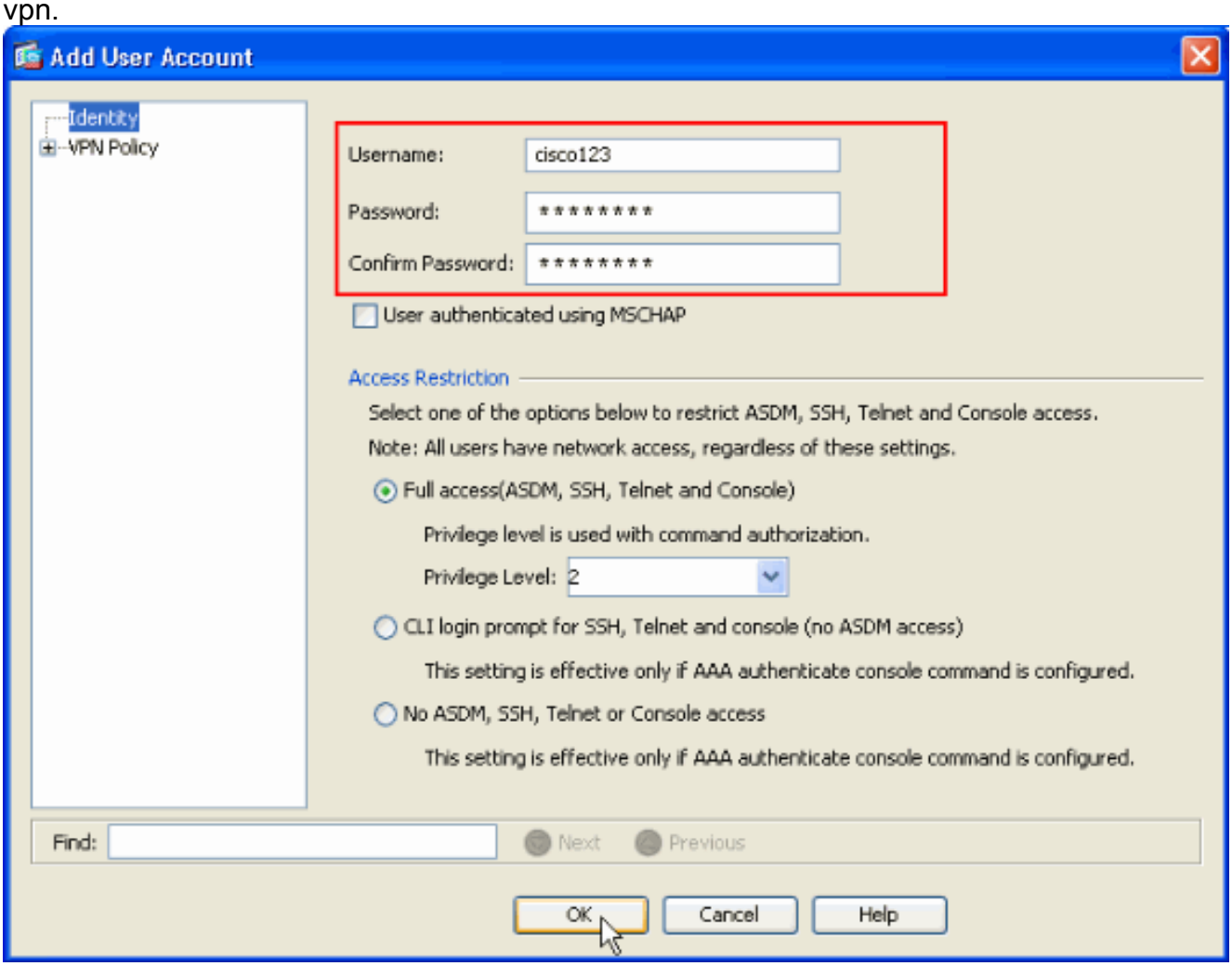
Cliquez sur **OK** et sur **Apply**.

5. Choisissez la **configuration > l'Accès à distance VPN > réseau (client) Access > a avancé > les stratégies de groupe > le groupe Policies>Servers>> d'Add>Internal** afin de configurer la **portée de DHCP** pour que les utilisateurs de client vpn soient assignés dynamiquement.



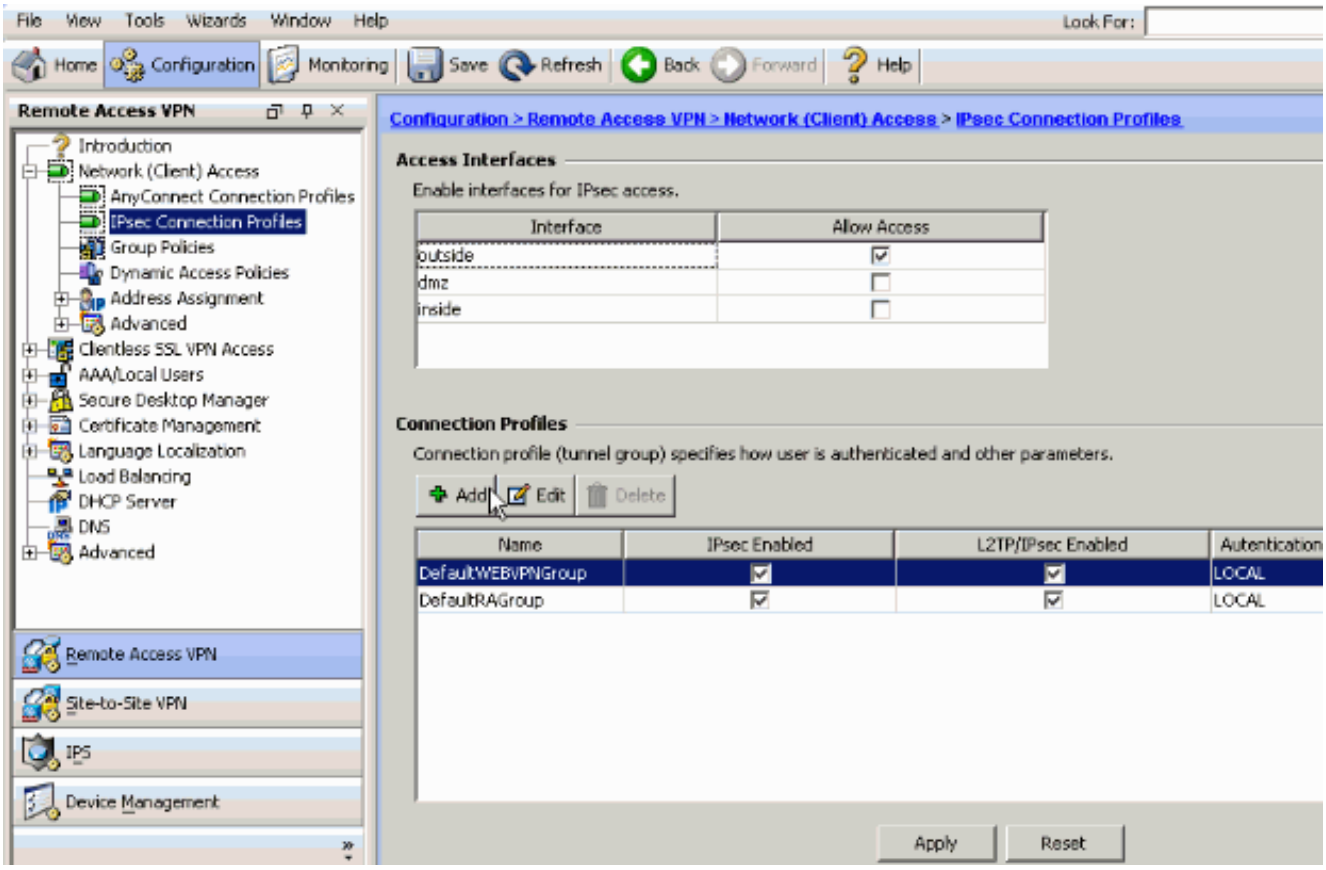
Cliquez sur **OK** et sur **Apply**.**Remarque:** La configuration de portée de DHCP est facultative. Référez-vous à [configurer le DHCP adressant le] pour en savoir plus.

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.

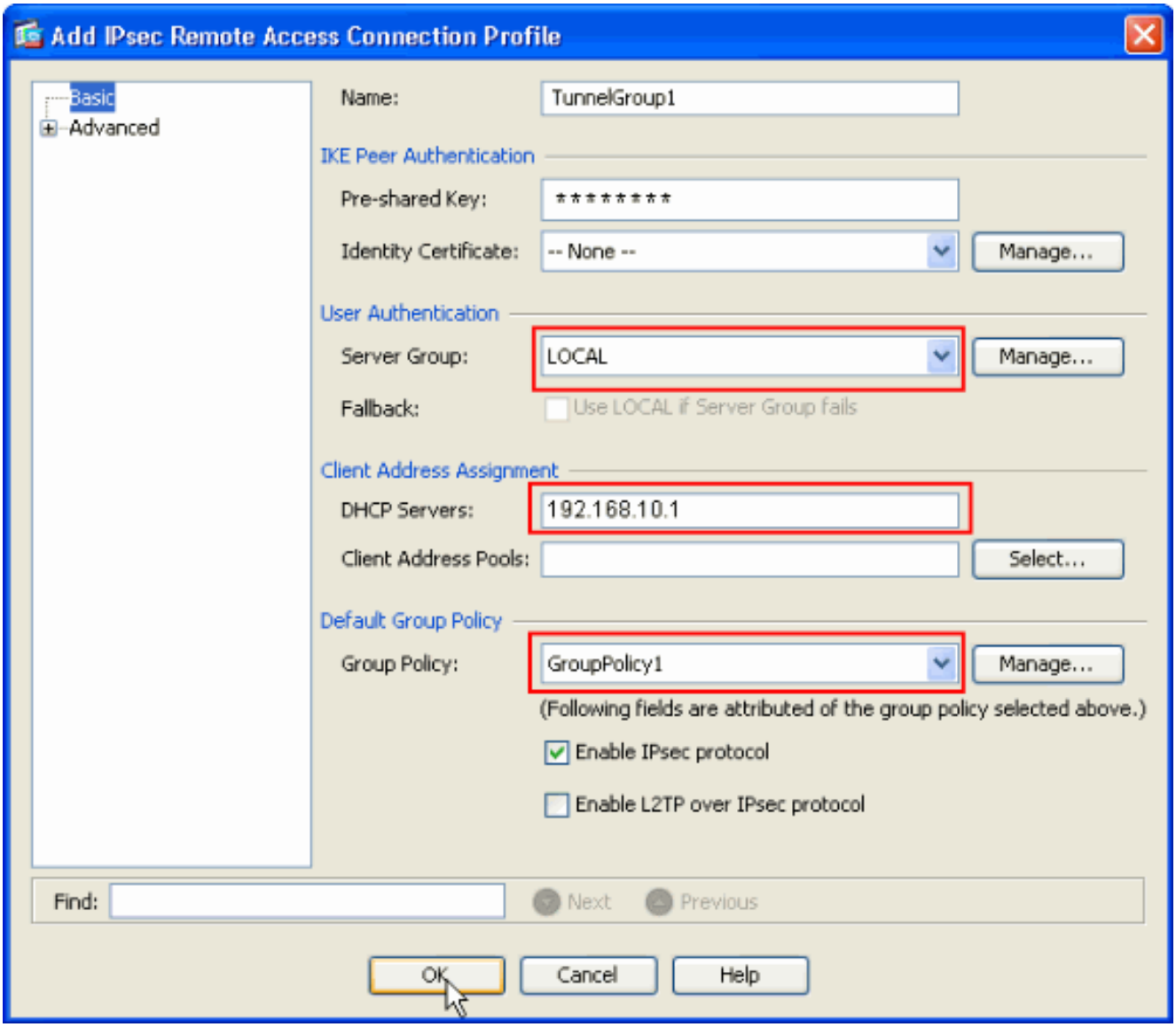


7. Choisissez la **configuration > l'Accès à distance VPN > réseau (client) Access > des profils >**

Add> de connexion d'IPSec afin d'ajouter un groupe de tunnel (par exemple, **TunnelGroup1** et la clé pré-partagée comme cisco123), comme
affiché.

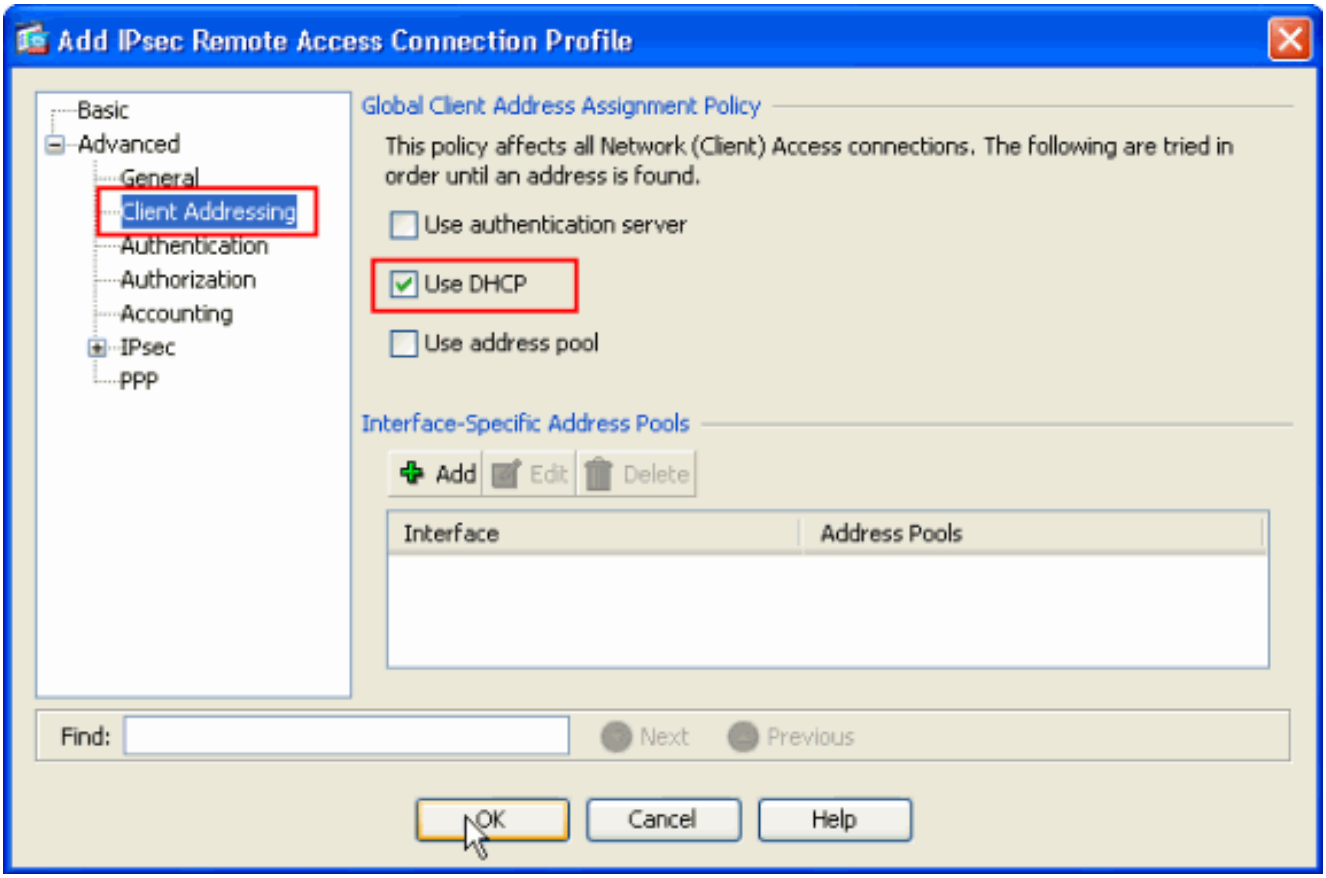


Sous l'onglet **de base** choisissez le groupe de serveurs comme **GENS DU PAYS** pour le champ d'authentification de l'utilisateur.Choisissez **Grouppolicy1** comme stratégie de groupe pour le champ de stratégie de groupe par défaut.Fournissez l'adresse IP de serveur DHCP dans l'espace prévu pour des **serveurs**
DHCP.



Cliquez sur **OK**.

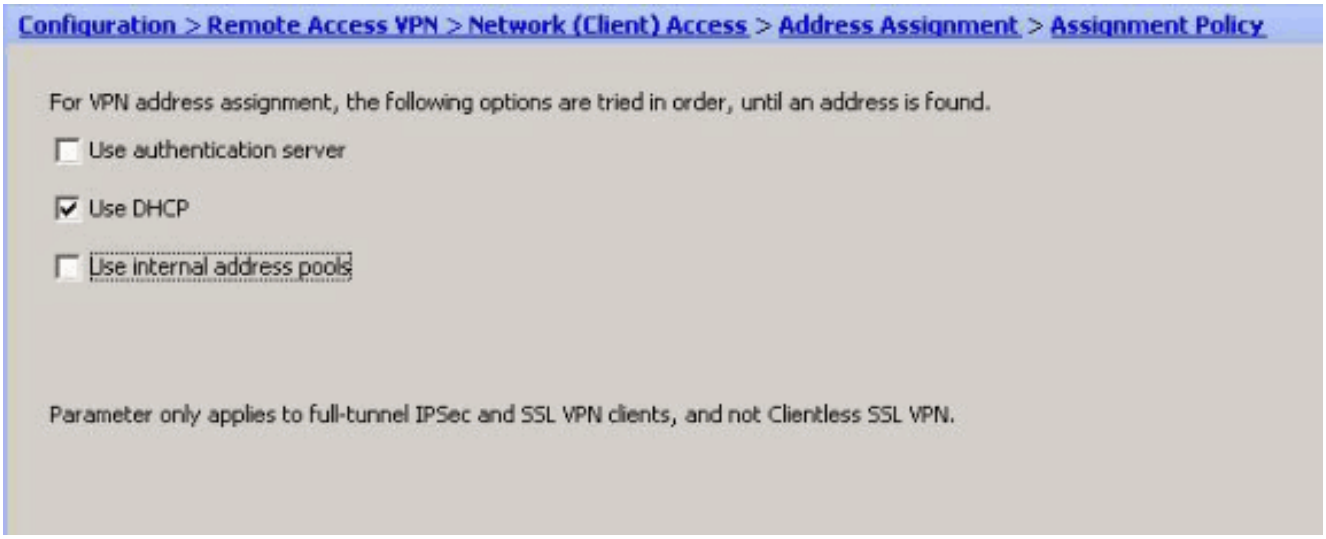
8. Choisissez **avancé > client adressant >** et vérifiez la case à cocher **DHCP d'utilisation** pour le serveur DHCP pour assigner l'adresse IP aux clients vpn.**Remarque:** Veillez à décocher les cases pour le **serveur d'authentification d'utilisation** et **à utiliser le pool d'adresses**.



Configuration pour ASDM 6.x

La même configuration ASDM fonctionne bien avec la version 6.x ASDM, excepté quelques modifications mineures en termes de chemins ASDM. Les chemins ASDM à certains champs ont eu une variance de version 6.2 et ultérieures ASDM. Les modifications avec les chemins existants sont répertoriées ci-dessous. Ici les images graphiques ne sont pas reliées dans les cas où elles demeurent les mêmes pour toutes les versions du commandant ASDM.

1. La configuration > l'Accès à distance VPN > réseau (client) Access > ont avancé > IPSec > stratégies IKE > ajoutent
2. La configuration > l'Accès à distance VPN > réseau (client) Access > ont avancé > IPSec > jeux de transformations d'IPSec > ajoutent
3. La configuration > l'Accès à distance VPN > réseau (client) Access > ont avancé > IPSec > crypto map > ajoutent
4. Choisissez le Configuration > Remote Access VPN > Network (Client) Access > Group Policies > ajoutent > des stratégies de groupe internes
5. Choisissez le Configuration > Remote Access VPN > Network (Client) Access > Group Policies > ajoutent des stratégies de groupe > des serveurs de >Internal
6. Choisissez la configuration > l'Accès à distance VPN > AAA installé/utilisateurs locaux > utilisateurs locaux > ajoutent
7. La configuration > l'Accès à distance VPN > réseau (client) Access > des profils de connexion d'IPSec > ajoutent
8. Choisissez la configuration > l'Accès à distance VPN > réseau (client) Access > stratégie d'affectation d'adresses >
   d'affectation



Toutes ces trois options sont activées par défaut. Cisco ASA suit la même commande pour assigner des adresses aux clients vpn. Quand vous décochez les deux autres options, Cisco ASA ne vérifie pas les options de serveur d'AAA et de groupe local. Les options activées par défaut peuvent être vérifiées par l'**exposition exécutent tous | dans VPN-ajoutez la** commande. C'est un résultat témoin pour votre référence :`vpn-addr-assign aaa`
`vpn-addr-assign dhcp`
`vpn-addr-assign local reuse-delay 0`Pour plus d'informations sur cette commande, référez-vous VPN-adr-assignent.

Configurez l'ASA/PIX utilisant le CLI

Terminez-vous ces étapes afin de configurer le serveur DHCP pour fournir l'adresse 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.

Exécution de Config sur le périphérique ASA

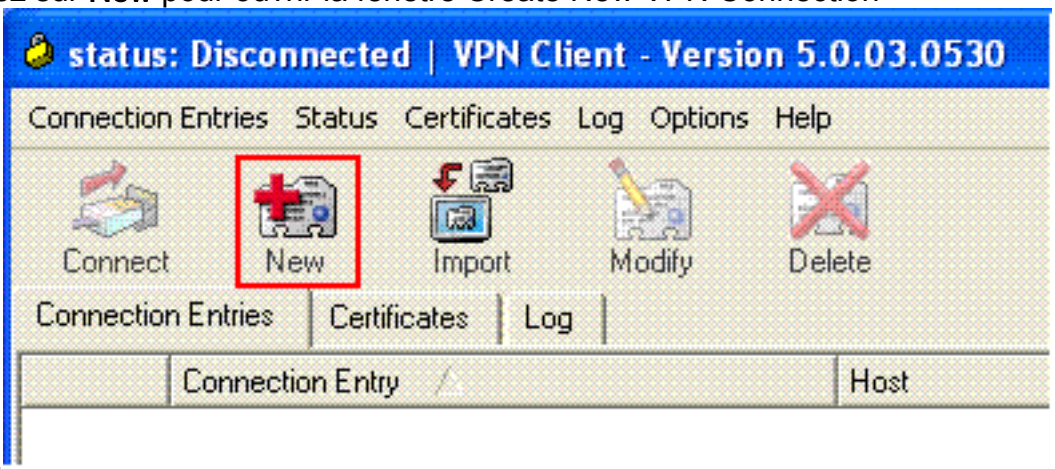
```
ASA# sh run
ASA Version 8.0(2)
!
!--- Specify the hostname for the Security Appliance.
hostname ASA enable password 8Ry2YjIyt7RRXU24 encrypted
names ! !--- Configure the outside and inside
interfaces. interface Ethernet0/0 nameif inside
security-level 100 ip address 10.1.1.1 255.255.255.0 !
interface 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 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 DHCP Server and now by AAA or the Local
pool.The CLI vpn-addr-assign dhcp for VPN address
assignment through DHCP Server is hidden in the CLI
provided by show run command. no vpn-addr-assign aaa no
vpn-addr-assign local 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 GroupPolicy1 internal group-policy
GroupPolicy1 attributes !--- define the DHCP network
scope in the group policy.This configuration is Optional
dhcp-network-scope 192.168.5.0 !--- In order to identify
remote access users to the Security Appliance, !--- you
can also configure usernames and passwords on the
device. username cisco123 password ffIRPGpDSOJh9YLq
encrypted !--- Create a new tunnel group and set the
connection !--- type to remote-access. tunnel-group
TunnelGroup1 type remote-access !--- Define the DHCP
server address to the tunnel group. tunnel-group
TunnelGroup1 general-attributes default-group-policy
GroupPolicy1 dhcp-server 192.168.10.1 !--- 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#
```

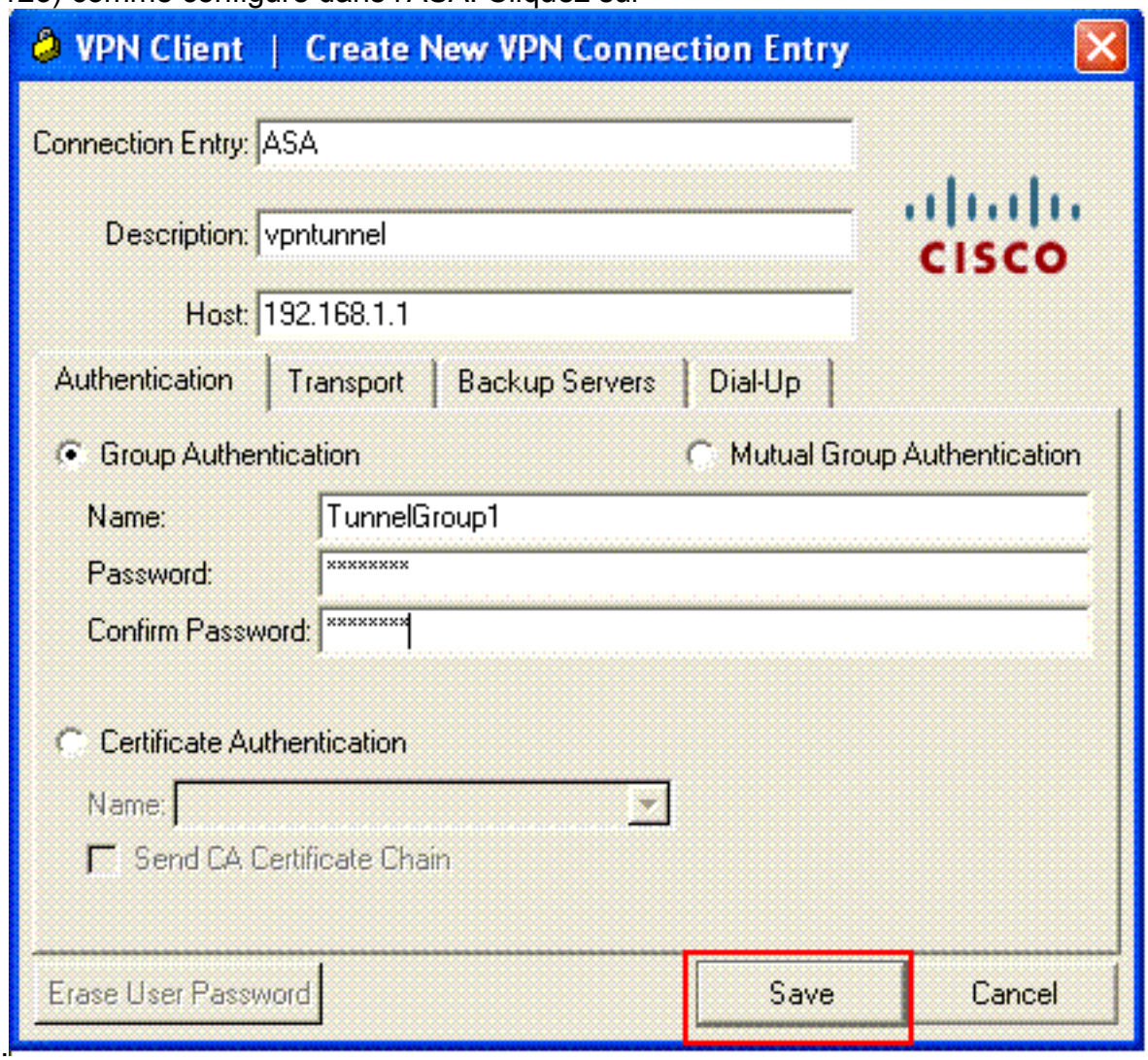
Configuration de Client VPN Cisco

Essayez de vous connecter à Cisco ASA en utilisant le Client VPN Cisco afin de vérifier que l'ASA est configuré avec succès.

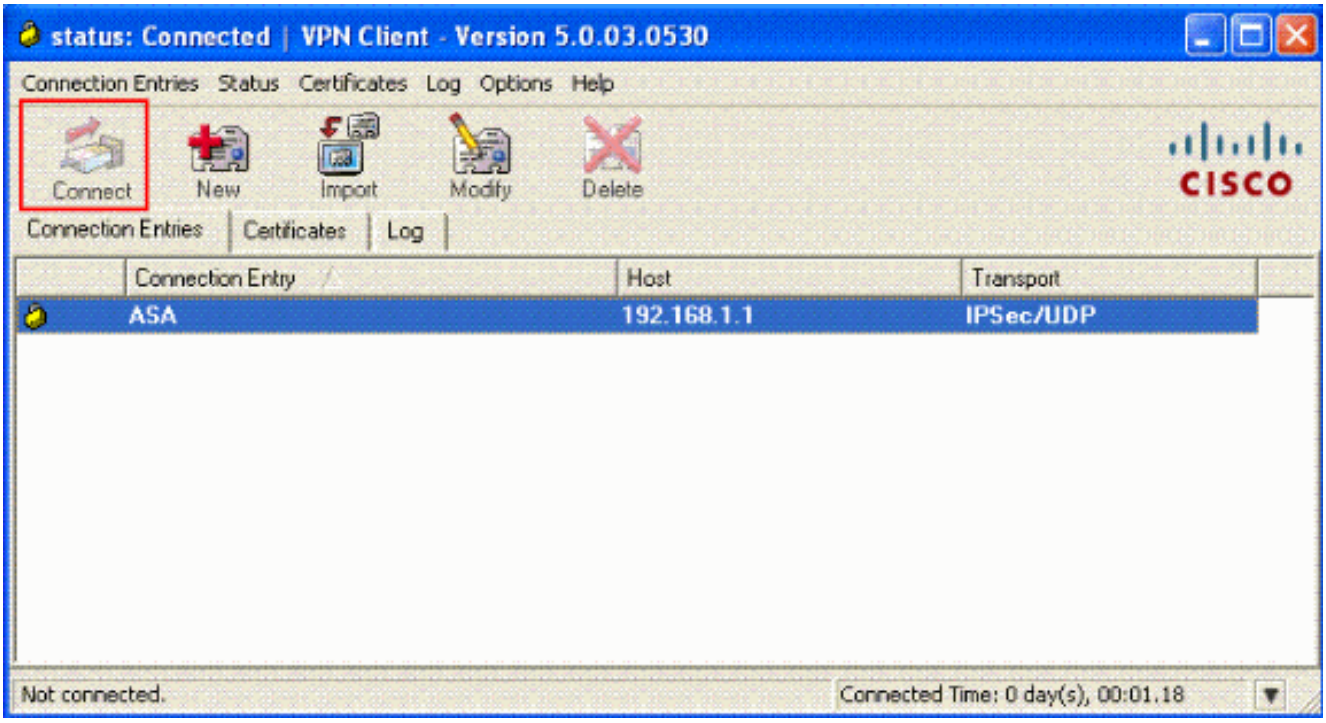
1. Sélectionnez **Démarrer > Programmes > Client VPN Cisco Systems > Client VPN**.
2. Cliquez sur **New** pour ouvrir la fenêtre Create New VPN Connection Entry.



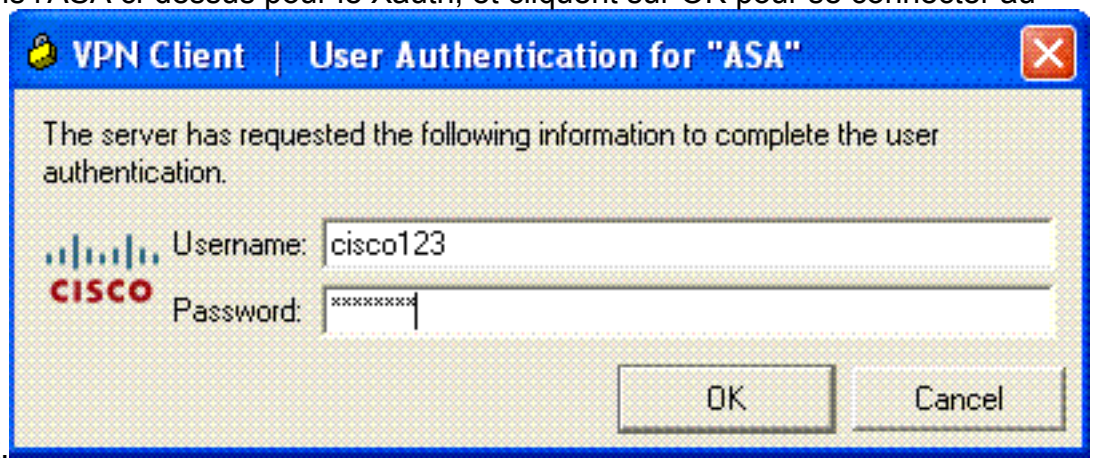
3. Complétez les détails de votre nouvelle connexion.Entrez le nom de l'entrée de connexion avec une description. Écrivez l'**adresse IP extérieure de l'ASA** dans la case d'hôte. Entrez alors le groupe de tunnel VPN name(TunnelGroup1) et le mot de passe (clé pré-partagée - cisco123) comme configuré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



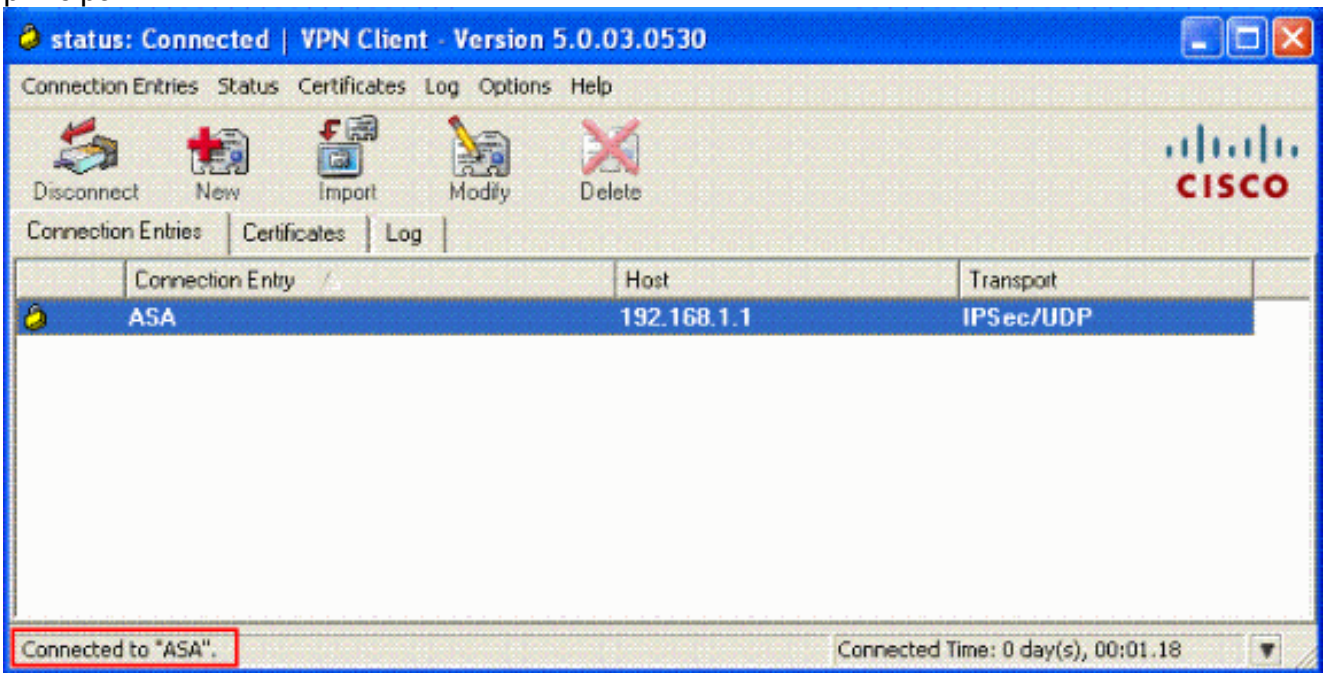
4. Cliquez sur en fonction la connexion que vous voulez au clic d'utiliser-et **vous connectez de la** fenêtre principale de client vpn.



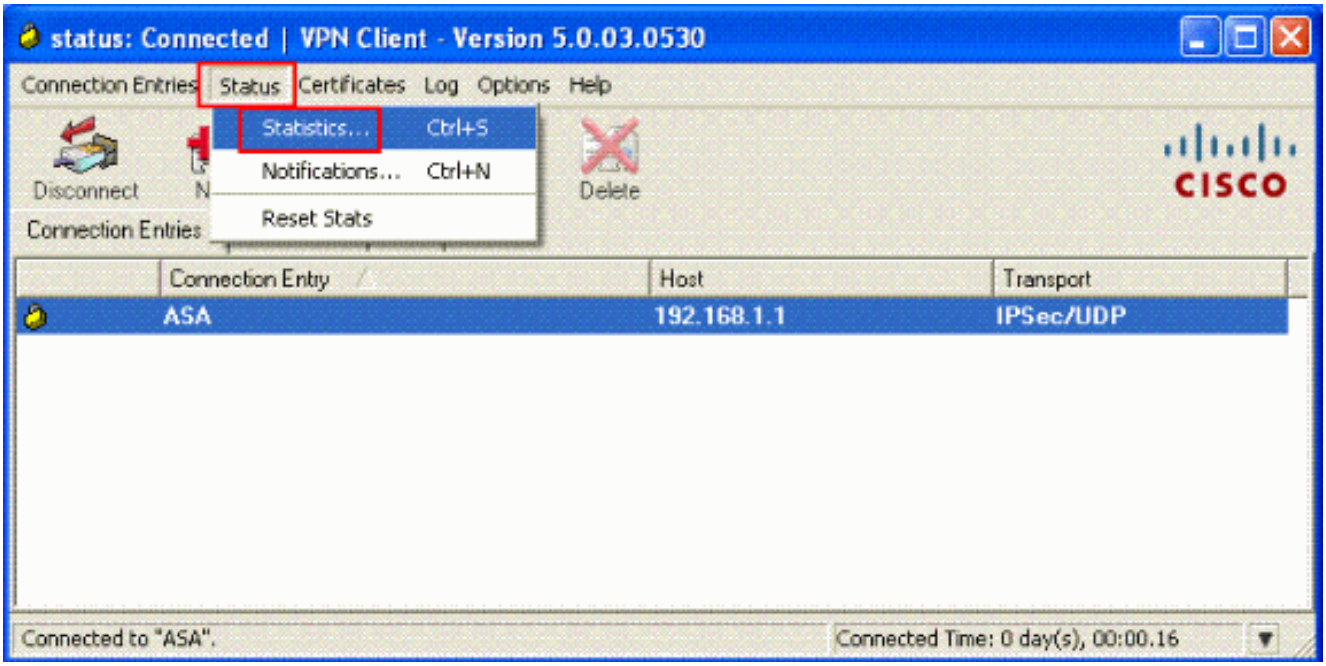
5. Une fois incité, écrivez le **nom d'utilisateur : cisco123** et **mot de passe : cisco123** comme configurés dans l'ASA ci-dessus pour le Xauth, et cliquent sur OK pour se connecter au réseau distant.



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



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



Vérifiez

Commandes show

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

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.

```
ASA #show crypto ipsec sa interface: outside Crypto map tag: dynmap, seq num: 10, local addr:
192.168.1.1 local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0) remote ident
(addr/mask/prot/port): (192.168.5.1/255.255.255.255/0/0) current_peer: 192.168.1.2, username:
cisco123 dynamic allocated peer ip: 192.168.5.1 #pkts encaps: 55, #pkts encrypt: 55, #pkts
digest: 55 #pkts decaps: 55, #pkts decrypt: 55, #pkts verify: 55 #pkts compressed: 0, #pkts
decompressed: 0 #pkts not compressed: 0, #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.:
192.168.1.1, remote crypto endpt.: 192.168.1.2 path mtu 1500, ipsec overhead 58, media mtu 1500
current outbound spi: C2C25E2B inbound esp sas: spi: 0x69F8C639 (1777911353) transform: esp-des
esp-md5-hmac none in use settings ={RA, Tunnel, } slot: 0, conn_id: 40960, crypto-map: dynmap sa
timing: remaining key lifetime (sec): 28337 IV size: 8 bytes replay detection support: Y
outbound esp sas: spi: 0xC2C25E2B (3267517995) transform: esp-des esp-md5-hmac none in use
settings ={RA, Tunnel, } slot: 0, conn_id: 40960, crypto-map: dynmap sa timing: remaining key
lifetime (sec): 28337 IV size: 8 bytes replay detection support: Y 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: 192.168.1.2 Type : user Role : responder Rekey : no State : AM_ACTIVE
```

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.

Exemple de sortie de débogage

- ASA 8.0
- Client vpn 5.0 pour Windows

ASA 8.0

```
ASA#debug crypto isakmp 7 Jan 22 22:21:24 [IKEv1]: IP = 192.168.1.2, IKE_DECODE RECEIVED Message
(msgid=0) with payloads : HDR + SA (1) + KE (4) + NONCE (10) + ID (5) + VENDOR (13) + VENDOR
(13) + VENDOR (13) + VENDOR (13) + VENDOR (13) + NONE (0) total le ngth : 856 Jan 22 22:21:24
[IKEv1 DEBUG]: IP = 192.168.1.2, processing SA payload Jan 22 22:21:24 [IKEv1 DEBUG]: IP =
192.168.1.2, processing ke payload Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, processing
ISA_KE payload Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, processing nonce payload Jan 22
22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, processing ID payload Jan 22 22:21:24 [IKEv1 DEBUG]:
IP = 192.168.1.2, processing VID payload Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2,
Received xauth V6 VID Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, processing VID payload
Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, Received DPD VID Jan 22 22:21:24 [IKEv1 DEBUG]:
IP = 192.168.1.2, processing VID payload Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2,
Received Fragmentation VID Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, IKE Peer included
IKE fragmenta tion capability flags: Main Mode: True Aggressive Mode: False Jan 22 22:21:24
[IKEv1 DEBUG]: IP = 192.168.1.2, processing VID payload Jan 22 22:21:24 [IKEv1 DEBUG]: IP =
192.168.1.2, Received NAT-Traversal ver 02 V ID Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2,
processing VID payload Jan 22 22:21:24 [IKEv1 DEBUG]: IP = 192.168.1.2, Received Cisco Unity
client VID Jan 22 22:21:24 [IKEv1]: IP = 192.168.1.2, Connection landed on tunnel_group Tun
nelGroup1 Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, processin g IKE
SA payload Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, IKE SA Pr
oposal # 1, Transform # 13 acceptable Matches global IKE entry # 2 Jan 22 22:21:24 [IKEv1
DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, construct ing ISAKMP SA payload Jan 22 22:21:24
[IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, construct ing ke payload Jan 22 22:21:24
```

[IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, construct ing nonce payload Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, Generatin g keys for Responder... Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, construct ing ID payload Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, construct ing hash payload Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, Computing hash for ISAKMP Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, construct ing Cisco Unity VID payload Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, construct ing xauth V6 VID payload Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, construct ing dpd vid payload Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, construct ing Fragmentation VID + extended capabilities payload Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, construct ing VID payload Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, Send Alti ga/Cisco VPN3000/Cisco ASA GW VID Jan 22 22:21:24 [IKEv1]: IP = 192.168.1.2, IKE_DECODE SENDING Message (msgid=0) with payloads : HDR + SA (1) + KE (4) + NONCE (10) + ID (5) + HASH (8) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) + NONE (0) total le ngth : 368 Jan 22 22:21:24 [IKEv1]: IP = 192.168.1.2, IKE_DECODE RECEIVED Message (msgid=0) with payloads : HDR + HASH (8) + NOTIFY (11) + VENDOR (13) + VENDOR (13) + NONE (0) total length : 116 Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, processin g hash payload Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, Computing hash for ISAKMP Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, processin g notify payload Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, processin g VID payload Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, Processin g IOS/PIX Vendor ID payload (version: 1.0.0, capabilities: 00000408) Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, processin g VID payload Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, Received Cisco Unity client VID Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, construct ing blank hash payload Jan 22 22:21:24 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, construct ing qm hash payload Jan 22 22:21:24 [IKEv1]: IP = 192.168.1.2, IKE_DECODE SENDING Message (msgid=e8a 1816d) with payloads : HDR + HASH (8) + ATTR (14) + NONE (0) total length : 68 Jan 22 22:21:31 [IKEv1]: IP = 192.168.1.2, IKE_DECODE RECEIVED Message (msgid=e8 a1816d) with payloads : HDR + HASH (8) + ATTR (14) + NONE (0) total length : 84 Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, process_a ttr(): Enter! Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, IP = 192.168.1.2, Processin g MODE_CFG Reply attributes. Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, IKEGetUserAttributes: primary DNS = cleared Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, IKEGetUserAttributes: secondary DNS = cleared Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, IKEGetUserAttributes: primary WINS = cleared Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, IKEGetUserAttributes: secondary WINS = cleared Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, IKEGetUserAttributes: IP Compression = disabled Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, IKEGetUserAttributes: Split Tunneling Policy = Disabled Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, IKEGetUserAttributes: Browser Proxy Setting = no-modify Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, IKEGetUserAttributes: Browser Proxy Bypass Local = disable Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP = 192.168 .1.2, User (cisco123) authenticated. Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, constructing blank hash payload Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, constructing qm hash payload Jan 22 22:21:31 [IKEv1]: IP = 192.168.1.2, IKE_DECODE SENDING Message (msgid=143 60de6) with payloads : HDR + HASH (8) + ATTR (14) + NONE (0) total length : 60 Jan 22 22:21:31 [IKEv1]: IP = 192.168.1.2, IKE_DECODE RECEIVED Message (msgid=14 360de6) with payloads : HDR + HASH (8) + ATTR (14) + NONE (0) total length : 56 Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, process_attr(): Enter! Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, Processing cfg ACK attributes Jan 22 22:21:31 [IKEv1]: IP = 192.168.1.2, IKE_DECODE RECEIVED Message (msgid=26 63a1dd) with payloads : HDR + HASH (8) + ATTR (14) + NONE (0) total length : 193 Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, process_attr(): Enter! Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, Processing cfg Request attributes Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, MODE_CFG: Received request for IPV4 address! Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, MODE_CFG: Received request for IPV4 net mask! Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, MODE_CFG: Received request for DNS server address! Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username =

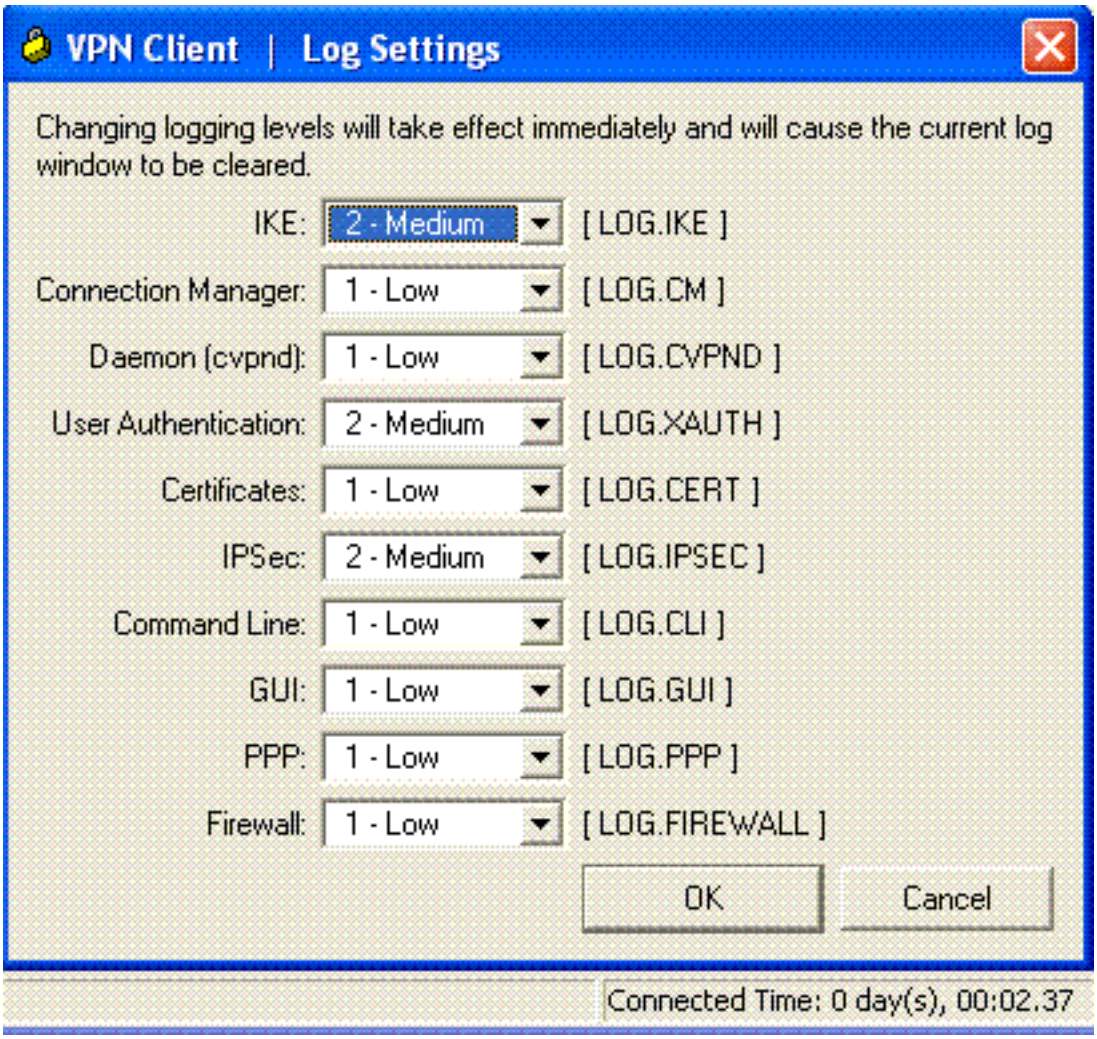
cisco123, IP = 1 92.168.1.2, MODE_CFG: Received request for WINS server address! Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP = 192.168 .1.2, Received unsupported transaction mode attribute: 5 Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, MODE_CFG: Received request for Banner! Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, MODE_CFG: Received request for Save PW setting! Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, MODE_CFG: Received request for Default Domain Name! Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, MODE_CFG: Received request for Split Tunnel List! Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, MODE_CFG: Received request for Split DNS! Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, MODE_CFG: Received request for PFS setting! Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, MODE_CFG: Received request for Client Browser Proxy Setting! Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, MODE_CFG: Received request for backup ip-sec peer list! Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP = 192.168 .1.2, Received unknown transaction mode attribute: 28684 Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, MODE_CFG: Received request for Application Version! Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP = 192.168 .1.2, Client Type: WinNT Client Application Version: 5.0.03.0530 Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, MODE_CFG: Received request for FWTYPE! Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, MODE_CFG: Received request for DHCP hostname for DDNS is: Wireless12 3! Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, MODE_CFG: Received request for UDP Port! Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, Obtained IP addr (192.168.5.1) prior to initiating Mode Cfg (XAuth e nabled) Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP = 192.168 .1.2, Assigned private IP address 192.168.5.1 to remote user Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, constructing blank hash payload Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, Send Client Browser Proxy Attributes! Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, Browser Proxy set to No-Modify. Browser Proxy data will NOT be inclu ded in the mode-cfg reply Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, constructing qm hash payload Jan 22 22:21:31 [IKEv1]: IP = 192.168.1.2, IKE_DECODE SENDING Message (msgid=266 3a1dd) with payloads : HDR + HASH (8) + ATTR (14) + NONE (0) total length : 158 Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, Delay Quick Mode processing, Cert/Trans Exch/RM DSID in progress Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, Resume Quick Mode processing, Cert/Trans Exch/RM DSID completed Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP = 192.168 .1.2, **PHASE 1 COMPLETED** Jan 22 22:21:31 [IKEv1]: IP = 192.168.1.2, Keep-alive type for this connection: DPD Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, Starting P1 rekey timer: 950 seconds. Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, sending notify message Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, constructing blank hash payload Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, constructing qm hash payload Jan 22 22:21:31 [IKEv1]: IP = 192.168.1.2, IKE_DECODE SENDING Message (msgid=f44 35669) with payloads : HDR + HASH (8) + NOTIFY (11) + NONE (0) total length : 84 Jan 22 22:21:31 [IKEv1]: IP = 192.168.1.2, IKE_DECODE RECEIVED Message (msgid=54 1f8e43) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0) total length : 1022 Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, processing hash payload Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, processing SA payload Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, processing nonce payload Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, processing ID payload Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP = 192.168 .1.2, Received remote Proxy Host data in ID Payload: Address 192.168.5.1, Proto col 0, Port 0 Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, processing ID payload Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP = 192.168 .1.2, Received local IP Proxy Subnet data in ID Payload: Address 0.0.0.0, Mask 0.0.0.0, Protocol 0, Port 0 Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP = 192.168 .1.2, QM IsRekeyed old sa not found by addr Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP = 192.168 .1.2, IKE Remote Peer configured for crypto map: dynmap Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, processing IPSec SA payload Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, IPSec SA

Proposal # 14, Transform # 1 acceptable Matches global IPS ec SA entry # 10 Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP = 192.168 .1.2, IKE: requesting SPI! Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, IKE got SPI from key engine: SPI = 0x31de01d8 Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, oakley constucting quick mode Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, constructing blank hash payload Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, constructing IPSec SA payload Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP = 192.168 .1.2, Overriding Initiator's IPSec rekeying duration from 2147483 to 28800 secon ds Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, constructing IPSec nonce payload Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, constructing proxy ID Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, Transmitting Proxy Id: Remote host: 192.168.5.1 Protocol 0 Port 0 Local subnet: 0.0.0.0 mask 0.0.0.0 Protocol 0 Port 0 Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, Sending RESPONDER LIFETIME notification to Initiator Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, constructing qm hash payload Jan 22 22:21:31 [IKEv1]: IP = 192.168.1.2, IKE_DECODE SENDING Message (msgid=541 f8e43) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NOTIFY (11) + NONE (0) total length : 176 Jan 22 22:21:31 [IKEv1]: IP = 192.168.1.2, IKE_DECODE RECEIVED Message (msgid=54 1f8e43) with payloads : HDR + HASH (8) + NONE (0) total length : 48 Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, processing hash payload Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, loading all IPSEC SAs Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, Generating Quick Mode Key! Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, Generating Quick Mode Key! Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP = 192.168 .1.2, Security negotiation complete for User (cisco123) Responder, Inbound SPI = 0x31de01d8, Outbound SPI = 0x8b7597a9 Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, IKE got a KEY_ADD msg for SA: SPI = 0x8b7597a9 Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, Pitcher: received KEY_UPDATE, spi 0x31de01d8 Jan 22 22:21:31 [IKEv1 DEBUG]: Group = TunnelGroup1, Username = cisco123, IP = 1 92.168.1.2, Starting P2 rekey timer: 27360 seconds. Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP = 192.168 .1.2, Adding static route for client address: 192.168.5.1 Jan 22 22:21:31 [IKEv1]: Group = TunnelGroup1, Username = cisco123, IP = 192.168 .1.2, **PHASE 2 COMPLETED** (msgid=541f8e43) Jan 22 22:21:41 [IKEv1]: IP = 192.168.1.2, IKE_DECODE RECEIVED Message (msgid=78 f7d3ae) with payloads : HDR + HASH (8) + NOTIFY (11) + NONE (0) total length : 8 0 ASA#**debug crypto ipsec 7** *!--- Deletes the old SAs.* ASA# IPSEC: Deleted inbound decrypt rule, SPI 0x7F3C985A Rule ID: 0xD5567DB0 IPSEC: Deleted inbound permit rule, SPI 0x7F3C985A Rule ID: 0xD4EF1DF0 IPSEC: Deleted inbound tunnel flow rule, SPI 0x7F3C985A Rule ID: 0xD556AF60 IPSEC: Deleted inbound VPN context, SPI 0x7F3C985A VPN handle: 0x0004678C IPSEC: Deleted outbound encrypt rule, SPI 0xC921E280 Rule ID: 0xD517EE30 IPSEC: Deleted outbound permit rule, SPI 0xC921E280 Rule ID: 0xD5123250 IPSEC: Deleted outbound VPN context, SPI 0xC921E280 VPN handle: 0x00040AB4 *!--- Creates new SAs.* ASA# IPSEC: New embryonic SA created @ 0xD4EF2390, SCB: 0xD4EF22C0, Direction: inbound SPI : 0x7F3C985A Session ID: 0x0000F000 VPIF num : 0x00000002 Tunnel type: ra Protocol : esp Lifetime : 240 seconds IPSEC: New embryonic SA created @ 0xD556B118, SCB: 0xD556B048, Direction: outbound SPI : 0xC921E280 Session ID: 0x0000F000 VPIF num : 0x00000002 Tunnel type: ra Protocol : esp Lifetime : 240 seconds IPSEC: Completed host OBSA update, SPI 0xC921E280 IPSEC: Creating outbound VPN context, SPI 0xC921E280 Flags: 0x00000005 SA : 0xD556B118 SPI : 0xC921E280 MTU : 1500 bytes VCID : 0x00000000 Peer : 0x00000000 SCB : 0x0133B741 Channel: 0xD4160FA8 IPSEC: Completed outbound VPN context, SPI 0xC921E280 VPN handle: 0x00040AB4 IPSEC: New outbound encrypt rule, SPI 0xC921E280 Src addr: 0.0.0.0 Src mask: 0.0.0.0 Dst addr: 192.168.5.1 Dst mask: 255.255.255.255 Src ports Upper: 0 Lower: 0 Op : ignore Dst ports Upper: 0 Lower: 0 Op : ignore Protocol: 0 Use protocol: false SPI: 0x00000000 Use SPI: false IPSEC: Completed outbound encrypt rule, SPI 0xC921E280 Rule ID: 0xD517EE30 IPSEC: New outbound permit rule, SPI 0xC921E280 Src addr: 192.168.1.1 Src mask: 255.255.255.255 Dst addr: 192.168.1.2 Dst mask: 255.255.255.255 Src ports Upper: 0 Lower: 0 Op : ignore Dst ports Upper: 0 Lower: 0 Op : ignore Protocol: 50 Use protocol: true SPI: 0xC921E280 Use SPI: true IPSEC: Completed outbound permit rule, SPI 0xC921E280 Rule ID: 0xD5123250 IPSEC: Completed host IBSA update, SPI 0x7F3C985A IPSEC: Creating inbound VPN context, SPI 0x7F3C985A Flags: 0x00000006 SA : 0xD4EF2390 SPI : 0x7F3C985A MTU : 0 bytes VCID : 0x00000000 Peer : 0x00040AB4 SCB : 0x0132B2C3 Channel: 0xD4160FA8 IPSEC: Completed inbound VPN context, SPI 0x7F3C985A VPN handle: 0x0004678C IPSEC: Updating outbound VPN context 0x00040AB4, SPI 0xC921E280 Flags: 0x00000005 SA : 0xD556B118 SPI : 0xC921E280 MTU : 1500 bytes VCID : 0x00000000

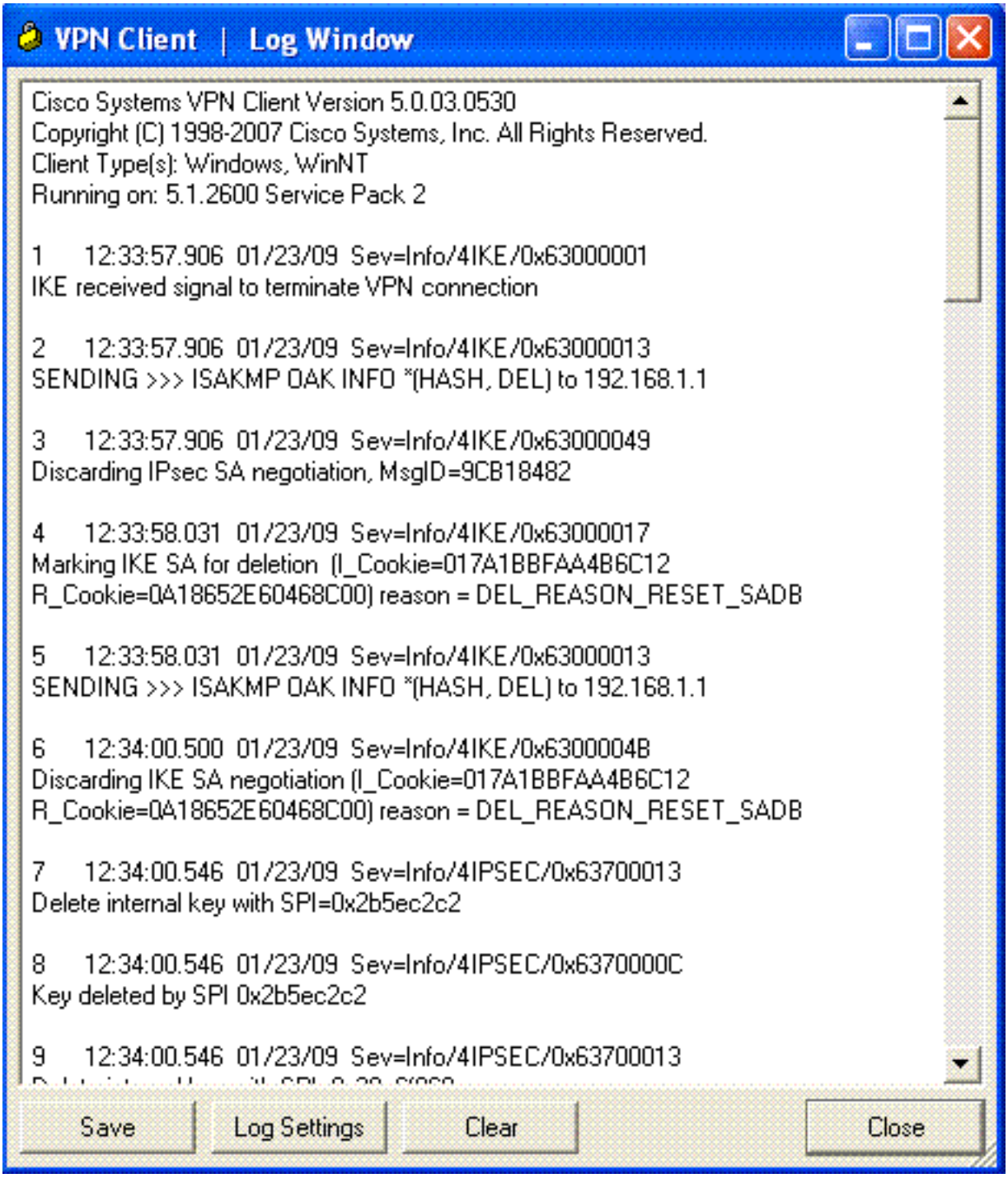
```
Peer : 0x0004678C SCB : 0x0133B741 Channel: 0xD4160FA8 IPSEC: Completed outbound VPN context,
SPI 0xC921E280 VPN handle: 0x00040AB4 IPSEC: Completed outbound inner rule, SPI 0xC921E280 Rule
ID: 0xD517EE30 IPSEC: Completed outbound outer SPD rule, SPI 0xC921E280 Rule ID: 0xD5123250
IPSEC: New inbound tunnel flow rule, SPI 0x7F3C985A Src addr: 192.168.5.1 Src mask:
255.255.255.255 Dst addr: 0.0.0.0 Dst mask: 0.0.0.0 Src ports Upper: 0 Lower: 0 Op : ignore Dst
ports Upper: 0 Lower: 0 Op : ignore Protocol: 0 Use protocol: false SPI: 0x00000000 Use SPI:
false IPSEC: Completed inbound tunnel flow rule, SPI 0x7F3C985A Rule ID: 0xD556AF60 IPSEC: New
inbound decrypt rule, SPI 0x7F3C985A Src addr: 192.168.1.2 Src mask: 255.255.255.255 Dst addr:
192.168.1.1 Dst mask: 255.255.255.255 Src ports Upper: 0 Lower: 0 Op : ignore Dst ports Upper: 0
Lower: 0 Op : ignore Protocol: 50 Use protocol: true SPI: 0x7F3C985A Use SPI: true IPSEC:
Completed inbound decrypt rule, SPI 0x7F3C985A Rule ID: 0xD5567DB0 IPSEC: New inbound permit
rule, SPI 0x7F3C985A Src addr: 192.168.1.2 Src mask: 255.255.255.255 Dst addr: 192.168.1.1 Dst
mask: 255.255.255.255 Src ports Upper: 0 Lower: 0 Op : ignore Dst ports Upper: 0 Lower: 0 Op :
ignore Protocol: 50 Use protocol: true SPI: 0x7F3C985A Use SPI: true IPSEC: Completed inbound
permit rule, SPI 0x7F3C985A Rule ID: 0xD4EF1DF0
```

[Client vpn 5.0 pour Windows]

Sélectionnez **Log > Log settings** pour activer les niveaux de log dans le client VPN.



Sélectionnez **Log > Log Window** pour afficher les entrées de journal dans le client VPN.



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
- Support et documentation techniques - Cisco Systems