# Exemple de configuration de L2TP sur IPsec entre un PC Windows 2000/XP et PIX/ASA 7.2 à l'aide d'une clé prépartagée

## Contenu



## Introduction

Ce document décrit comment configurer le Layer 2 Tunneling Protocol (L2TP) au-dessus de la sécurité IP (IPsec) de Microsoft Windows distant 2000/2003 et des clients de XP à une entreprise de dispositifs de sécurité PIX utilisant des clés pré-partagées avec le serveur de RAYON de Service d'authentification Internet de Microsoft Windows 2003 (IAS) pour l'authentification de l'utilisateur. Consultez Microsoft - Liste de contrôle : Configurer IAS pour la connexion à distance et l'accès VPN pour plus d'informations sur IAS.

L'avantage primaire de configurer L2TP avec IPsec dans un scénario d'Accès à distance est que les utilisateurs distants peuvent accéder à un VPN au-dessus d'un réseau IP public sans

passerelle ou ligne dédiée. Ceci active l'Accès à distance de pratiquement n'importe quel endroit avec des POTS. Une allocation complémentaire est que la seule exigence de client pour l'accès VPN est l'utilisation du Windows 2000 avec le réseau commuté de Microsoft (DUN). Aucun logiciel client supplémentaire, tel que le logiciel de Client VPN Cisco, n'est exigé.

Ce document décrit également comment utiliser le Cisco Adaptive Security Device Manager (ASDM) afin de configurer l'appliance de Sécurité de gamme 500 PIX pour le L2TP sur IPsec.

**Remarque:** Le Layer 2 Tunneling Protocol (L2TP) au-dessus d'IPsec est pris en charge sur la version de logiciel 6.x et ultérieures de pare-feu Cisco Secure PIX.

Afin de configurer L2TP au-dessus d'IPsec entre le PIX 6.x et Windows 2000, référez-vous à configurer L2TP au-dessus d'IPsec entre le PC de Pare-feu et de Windows 2000 PIX utilisant des Certificats.

Afin de configurer le L2TP sur IPsec du Microsoft Windows 2000 à distance et des clients XP à un site entreprise suivre une méthode chiffrée, référez-vous au L2TP sur IPsec de configuration de l'Windows 2000 ou client XP à un Concentrateur de la série Cisco VPN 3000 utilisant des clés Pré-partagées.

# Conditions préalables

## Conditions requises

Avant que l'établissement sécurisé de tunnel, les besoins de connectivité IP d'exister entre les pairs.

Assurez-vous que le port UDP 1701 n'est pas bloqué n'importe où le long du chemin de la connexion.

Utilisez la stratégie par défaut seulement de tunnel de groupe et de groupe par défaut sur Cisco PIX/ASA. Les stratégies et les groupes définis par l'utilisateur ne fonctionnent pas.

**Remarque:** Les dispositifs de sécurité n'établissent pas un tunnel L2TP/IPsec avec le Windows 2000 si le Client VPN Cisco 3.x ou le Cisco VPN 3000 Client 2.5 est installé. Désactivez le service de Cisco VPN pour le Client VPN Cisco 3.x, ou le service d'ANetIKE pour le Cisco VPN 3000 Client 2.5 du panneau de services dans le Windows 2000. Afin de faire ceci choisissez le **Start > Programs > Administrative Tools > Services**, redémarrez le service d'agent de stratégie d'IPsec du panneau de services, et redémarrez l'ordinateur.

## Composants utilisés

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

- Appliance 515E de Sécurité PIX avec version de logiciel 7.2(1) ou plus tard
- Adaptive Security Device Manager 5.2(1) ou plus tard
- Microsoft Windows 2000 Server
- Professionnel de Microsoft Windows XP avec le SP2
- Serveur Windows 2003 avec IAS

**Remarque:** Si vous améliorez le PIX 6.3 à la version 7.x, assurez-vous que vous avez installé SP2 dans Windows XP (client L2TP).

**Remarque:** Les informations dans le document sont également valides pour des dispositifs de sécurité ASA.

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 l'appliance de Sécurité de gamme de Cisco ASA 5500 7.2(1) ou plus tard.

### Conventions

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

## Informations générales

Terminez-vous ces étapes afin de configurer le L2TP sur IPsec.

1. Configurez le mode de transport d'IPsec afin d'activer IPsec avec L2TP.Le client du Windows 2000 L2TP/IPsec utilise le mode de transport d'IPsec — seulement la charge utile d'IP est chiffrée, et les en-têtes IP d'original sont laissées intactes. Les avantages de ce mode sont qu'il ajoute seulement quelques octets à chaque paquet et permet à des périphériques sur le réseau public pour voir la source et la destination définitives du paquet. Par conséquent, pour que les clients du Windows 2000 L2TP/IPsec connectent aux dispositifs de sécurité, vous devez configurer le mode de transport d'IPsec pour une transformation (voir l'étape 2 dans la configuration ASDM). Avec cette capacité (transport), vous pouvez activer l'offre spéciale traitant (par exemple, QoS) sur le réseau intermédiaire basé sur les informations dans l'en-tête IP. Cependant, l'en-tête de la couche 4 est chiffrée, qui limite l'examen du paquet. Malheureusement, la transmission de l'en-tête IP en texte clair, mode de transport permet à un attaquant pour exécuter une certaine analyse du trafic.
2. Configurez L2TP avec un groupe de Réseau privé virtuel à accès commuté (VPDN).

La configuration de L2TP avec IPsec prend en charge les Certificats qui utilisent les clés ou les méthodes pré-partagées de signature RSA, et l'utilisation (par opposition à la charge statique) des crypto map dynamiques. La clé pré-partagée est utilisée comme authentification pour établir le tunnel de L2TP sur IPsec.

## Configurez

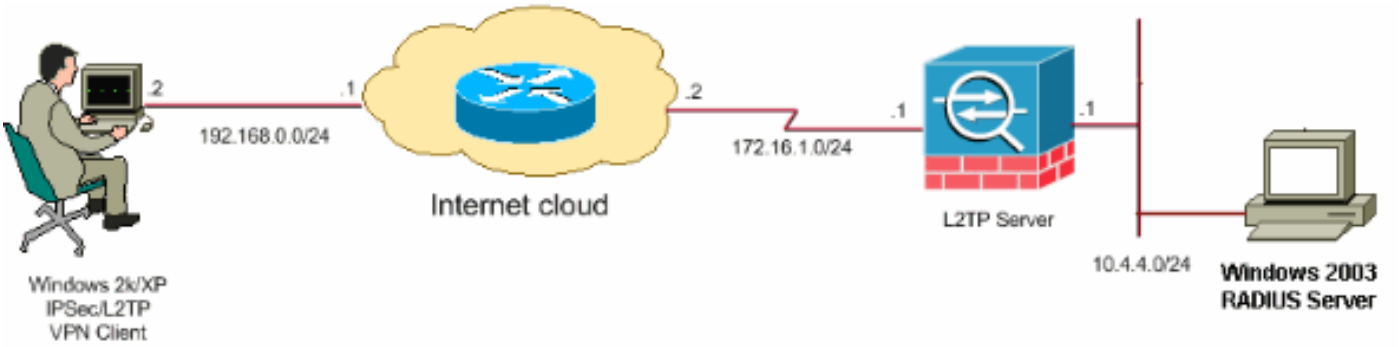
Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

**Remarque:** Utilisez l'outil Command Lookup Tool (clients enregistrés seulement) pour trouver plus d'informations sur les commandes utilisées dans ce document.

**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.

## Diagramme du réseau

Ce document utilise la configuration réseau suivante :




## Configurations

Ce document utilise les configurations suivantes :

- Configuration de client de Windows L2TP/IPsec
- Serveur L2TP dans la configuration PIX
- L2TP utilisant la configuration ASDM
- Configuration de Microsoft Windows Serveur 2003 avec IAS

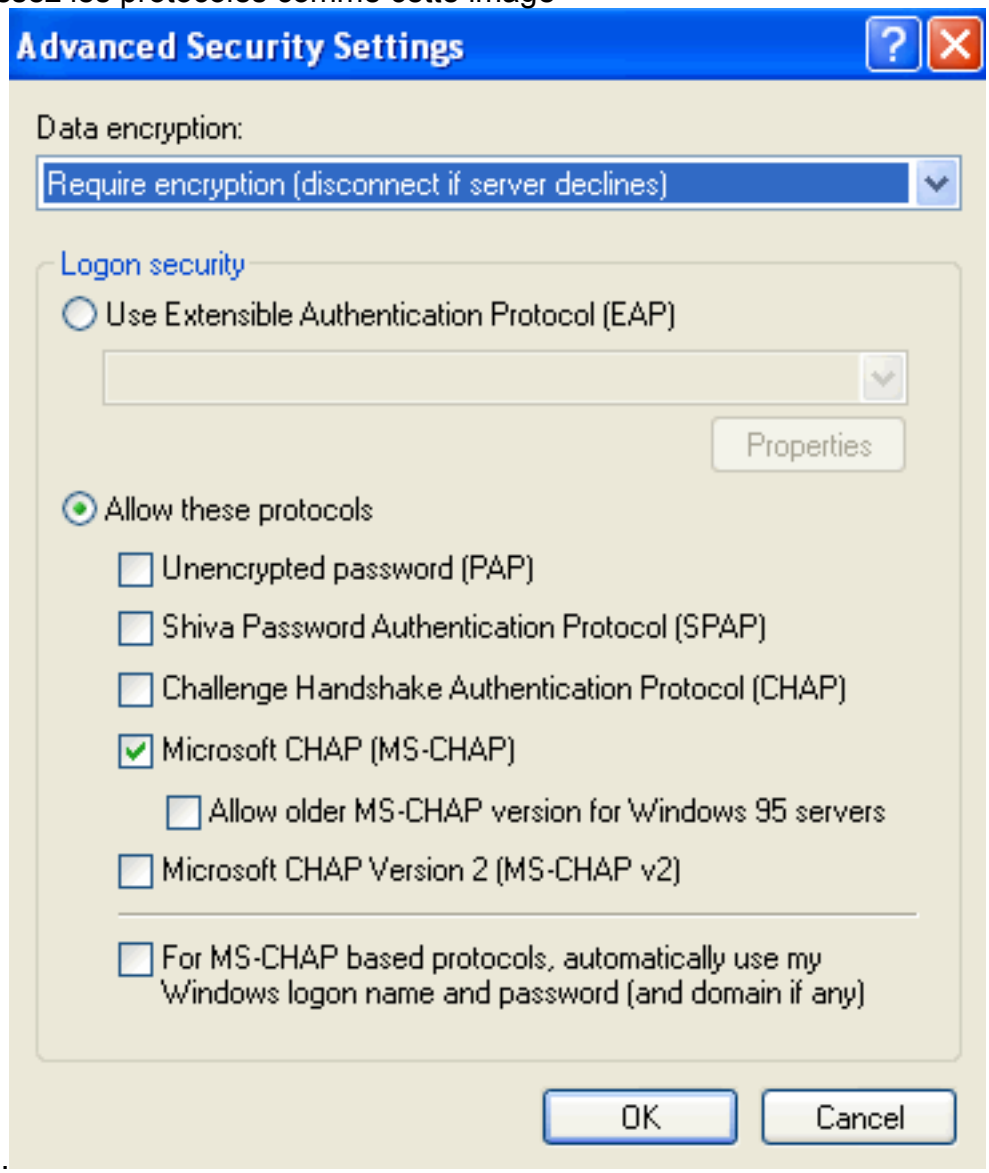
## Configuration de client de Windows L2TP/IPsec

Terminez-vous ces étapes afin de configurer le L2TP sur IPsec sur le Windows 2000. Pour des étapes 1 et 2 et début de saut de Windows XP de l'étape 3 :

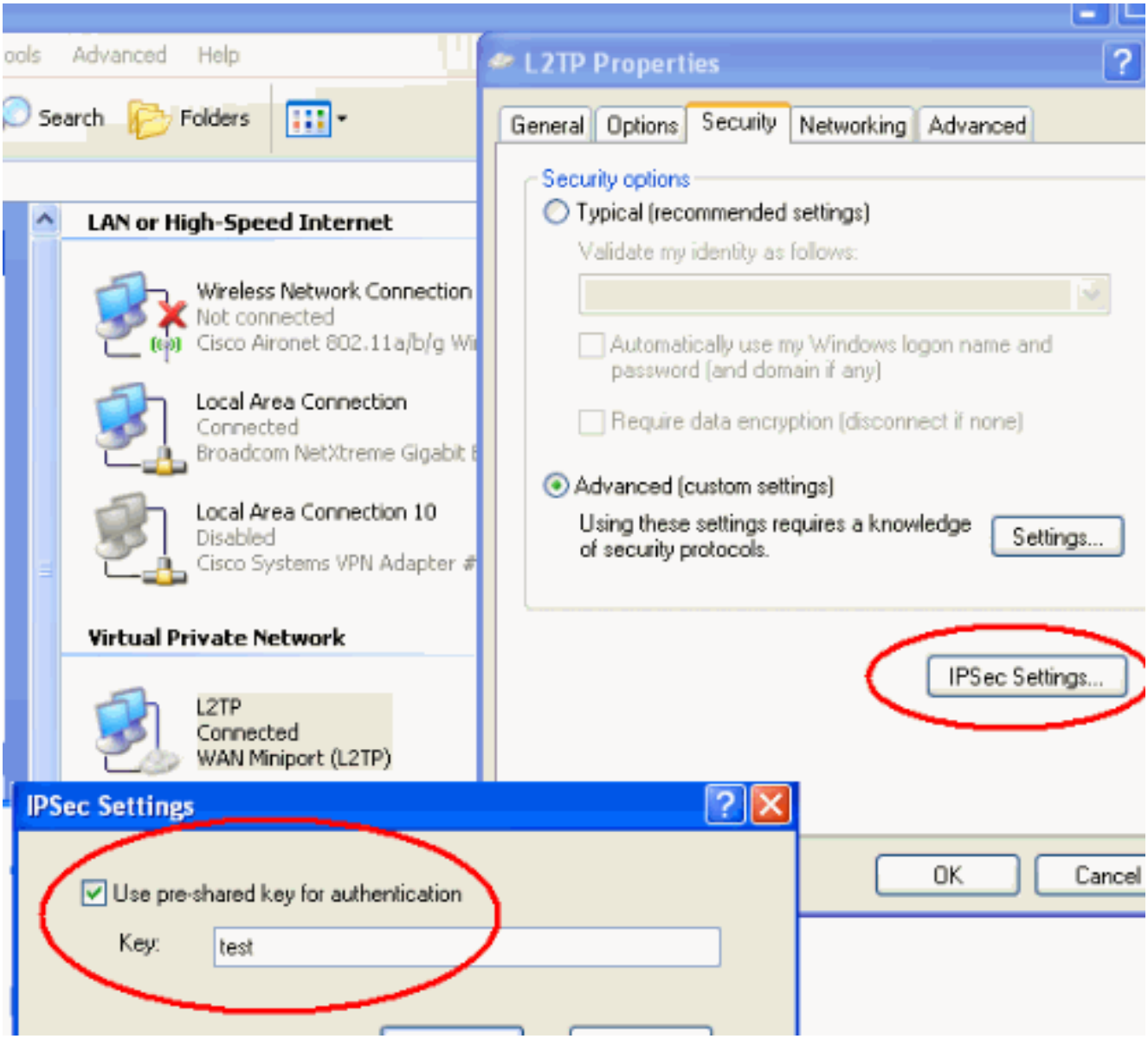
1. Ajoutez cette valeur de registre à votre ordinateur de Windows 2000 :`HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Rasman\Parameters`
2. Ajoutez cette valeur de registre à cette clé :`Value Name: ProhibitIpSec`
   `Data Type: REG_DWORD`
   `Value: 1`**Remarque:** Dans certains cas (Windows XP Sp2), l'ajout de cette clé **(valeur : 1)** semble casser la connexion pendant qu'il fait la case de XP négocier L2TP seulement plutôt qu'un L2TP avec la connexion d'IPsec. Il est obligatoire d'ajouter une stratégie d'IPsec en même temps que cette clé de registre. Si vous recevez une `erreur 800` quand vous essayez d'établir une connexion, retirez la clé (valeur : 1) afin d'obtenir la connexion pour fonctionner.**Remarque:** Vous devez redémarrer Windows 2000/2003 ou l'ordinateur de XP pour que les modifications les prennent effet. Par défaut le client Windows tente d'utiliser IPsec avec un Autorité de certification (CA). La configuration de cette clé de registre empêche ceci de se produire. Maintenant vous pouvez configurer une stratégie d'IPsec sur

la station de Windows pour apparier les paramètres que vous voulez sur le PIX/ASA. Référez-vous à comment configurer une connexion L2TP/IPSec utilisant l'authentification principale pré-partagée (Q240262) pour une configuration pas à pas de la stratégie de Windows IPsec.Référez-vous configurent une clé pré-partagée pour l'usage avec des connexions de Layer 2 Tunneling Protocol dans Windows XP (pour en savoir plus Q281555)\.

3. Créez votre connexion.
4. Sous des connexions de réseau et de connexion à distance, cliquez avec le bouton droit sur la connexion et choisissez Properties.Allez à l'onglet Sécurité et cliquez sur **avancé**. Choisissez les protocoles comme cette image affiche.




5. **Remarque:** Cette étape s'applique seulement pour Windows XP.Cliquez sur les **configurations d'IPSec**, vérifiez la **clé pré-partagée d'utilisation pour l'authentification** et saisissez la clé pré-partagée afin de placer la clé pré-partagée.Dans cet exemple, le test est utilisé comme clé pré-
partagée.




## Serveur L2TP dans la configuration PIX

| PIX 7.2 |
| --- |
| pixfirewall#**show run** PIX Version 7.2(1) ! hostname pixfirewall domain-name default.domain.invalid enable password 8Ry2YjIyt7RRXU24 encrypted names ! *!--- Configures the outside and inside interfaces.* interface Ethernet0 nameif outside security-level 0 ip address 172.16.1.1 255.255.255.0 ! interface Ethernet1 nameif inside security-level 100 ip address 10.4.4.1 255.255.255.0 ! passwd 2KFQnbNIdI.2KYOU encrypted ftp mode passive dns server-group DefaultDNS domain-name default.domain.invalid **access-list nonat extended permit ip 10.4.4.0 255.255.255.0 10.4.5.0 255.255.255.0 nat (inside) 0 access-list nonat** pager lines 24 logging console debugging mtu outside 1500 mtu inside 1500 *!--- Creates a pool of addresses from which IP addresses are assigned !--- dynamically to the remote VPN Clients.* **ip local pool clientVPNpool 10.4.5.10-10.4.5.20 mask 255.255.255.0** no failover **asdm image flash:/asdm-521.bin** no asdm history enable arp timeout 14400 *!--- The **global** and **nat** command enable !--- the Port Address Translation (PAT) using an outside interface IP !--- address for all outgoing traffic.* **global (outside) 1 interface nat** |

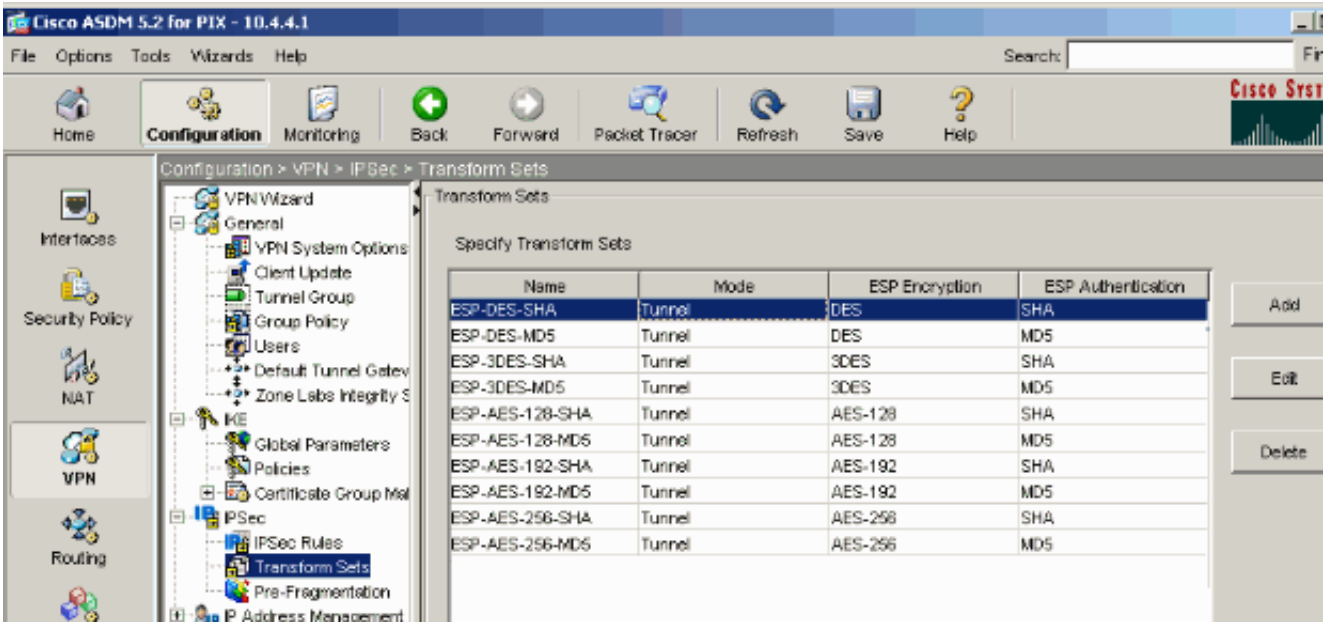
```
(inside) 1 0.0.0.0 0.0.0.0 route outside 0.0.0.0 0.0.0.0
172.16.1.2 1 timeout xlate 3:00:00 timeout conn 1:00:00
half-closed 0:10:00 udp 0:02:00 icmp 0:00:02 timeout
sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00
mgcp-pat 0:05:00 timeout sip 0:30:00 sip_media 0:02:00
sip-invite 0:03:00 sip-disconnect 0:02:00 timeout uauth
0:05:00 absolute !--- Create the AAA server group "vpn"
and specify its protocol as RADIUS. !--- Specify the IAS
server as a member of the "vpn" group and provide its !-
-- location and key. aaa-server vpn protocol radius aaa-
server vpn host 10.4.4.2 key radiuskey !--- Identifies
the group policy as internal. group-policy
DefaultRAGroup internal !--- Instructs the security
appliance to send DNS and !--- WINS server IP addresses
to the client. group-policy DefaultRAGroup attributes
wins-server value 10.4.4.99 dns-server value 10.4.4.99
!--- Configures L2TP over IPsec as a valid VPN tunneling
protocol for a group. vpn-tunnel-protocol IPSec l2tp-
ipsec default-domain value cisco.com !--- Configure
usernames and passwords on the device !--- in addition
to using AAA. !--- If the user is an L2TP client that
uses Microsoft CHAP version 1 or !--- version 2, and the
security appliance is configured !--- to authenticate
against the local !--- database, you must include the
mschap keyword. !--- For example, username <username>
password <password> mschap. username test password
DLaUiAX3l78qgoB5c7iVNw== nt-encrypted vpn-tunnel-
protocol l2tp-ipsec 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 !--- Identifies the IPsec
encryption and hash algorithms !--- to be used by the
transform set. crypto ipsec transform-set
TRANS_ESP_3DES_MD5 esp-3des esp-md5-hmac !--- Since the
Windows 2000 L2TP/IPsec client uses IPsec transport
mode, !--- set the mode to transport. !--- The default
is tunnel mode. crypto ipsec transform-set
TRANS_ESP_3DES_MD5 mode transport !--- Specifies the
transform sets to use in a dynamic crypto map entry.
crypto dynamic-map outside_dyn_map 20 set transform-set
TRANS_ESP_3DES_MD5 !--- Requires a given crypto map
entry to refer to a pre-existing !--- dynamic crypto
map. crypto map outside_map 20 ipsec-isakmp dynamic
outside_dyn_map !--- Applies a previously defined crypto
map set to an outside interface. crypto map outside_map
interface outside crypto isakmp enable outside crypto
isakmp nat-traversal 20 !--- Specifies the IKE Phase I
policy parameters. crypto isakmp policy 10
authentication pre-share encryption 3des hash md5 group
2 lifetime 86400 !--- Creates a tunnel group with the
tunnel-group command, and specifies the local !---
address pool name used to allocate the IP address to the
client. !--- Associate the AAA server group (VPN) with
the tunnel group. tunnel-group DefaultRAGroup general-
attributes address-pool clientVPNpool authentication-
server-group vpn !--- Link the name of the group policy
to the default tunnel !--- group from tunnel group
general-attributes mode. default-group-policy
DefaultRAGroup !--- Use the tunnel-group ipsec-
attributes command !--- in order to enter the ipsec-
attribute configuration mode. !--- Set the pre-shared
key. !--- This key should be the same as the key
configured on the Windows machine. tunnel-group
DefaultRAGroup ipsec-attributes pre-shared-key * !---
```

```
Configures the PPP authentication protocol with the
authentication type !--- command from tunnel group ppp-
attributes mode. tunnel-group DefaultRAGroup ppp-
attributes no authentication chap authentication ms-
chap-v2 telnet timeout 5 ssh timeout 5 console timeout 0
! class-map inspection_default match default-inspection-
traffic ! ! policy-map type inspect dns preset_dns_map
parameters message-length maximum 512 policy-map
global_policy class inspection_default inspect dns
preset_dns_map inspect ftp inspect h323 h225 inspect
h323 ras inspect netbios inspect rsh inspect rtsp
inspect skinny inspect esmtp inspect sqlnet inspect
sunrpc inspect tftp inspect sip inspect xdmcp ! service-
policy global_policy global prompt hostname context
Cryptochecksum:e1e0730fa260244caa2e2784f632accd : end
```

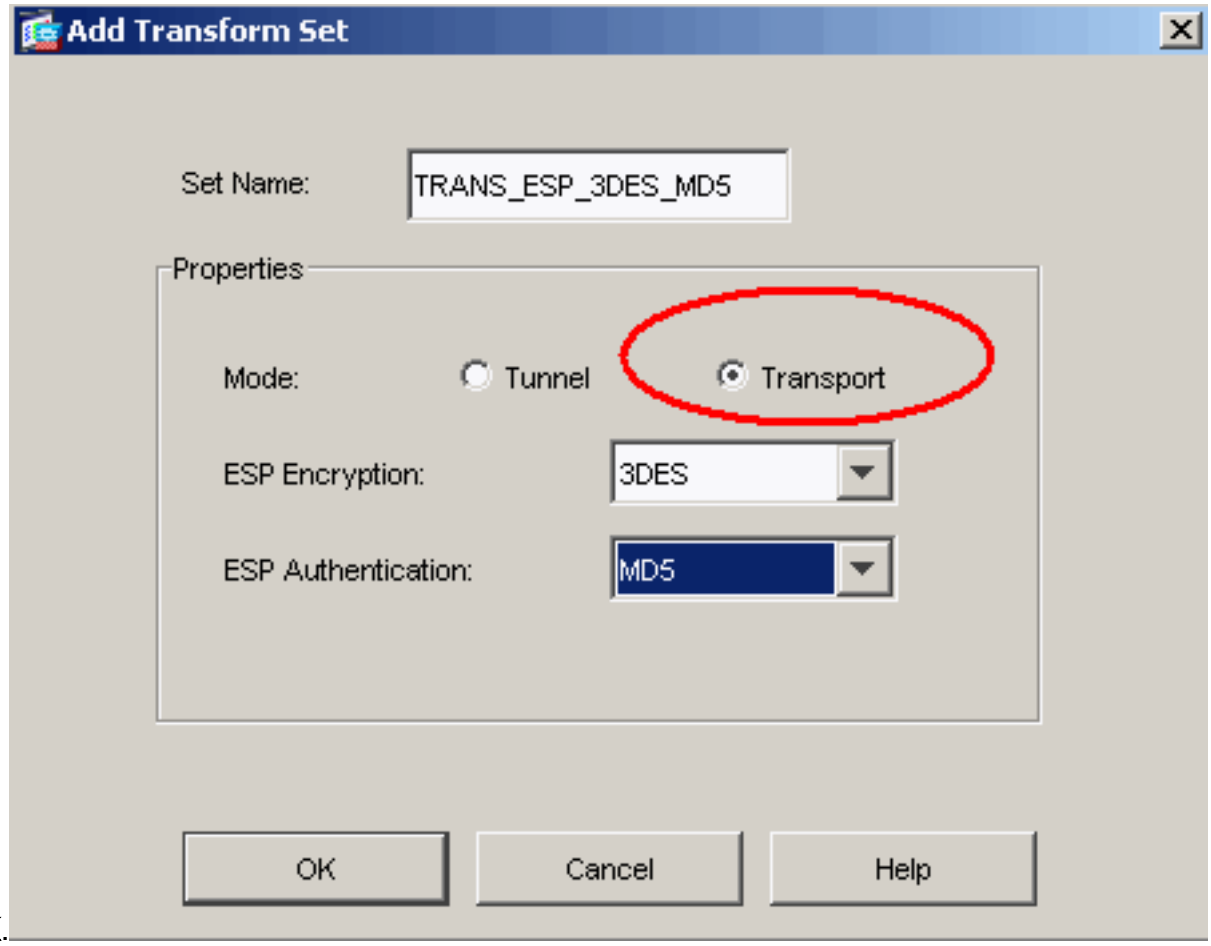
## L2TP utilisant la configuration ASDM

Terminez-vous ces étapes afin de configurer les dispositifs de sécurité pour recevoir des connexions de L2TP sur IPsec :

1. Ajoutez un jeu de transformations d'IPsec et spécifiez IPsec pour utiliser le mode de transport plutôt que le tunnel mode. Afin de faire ceci, choisissez la **configuration > le VPN > l'IPSec > les jeux de transformations** et cliquez sur Add. Les affichages de volet de jeux de transformations.

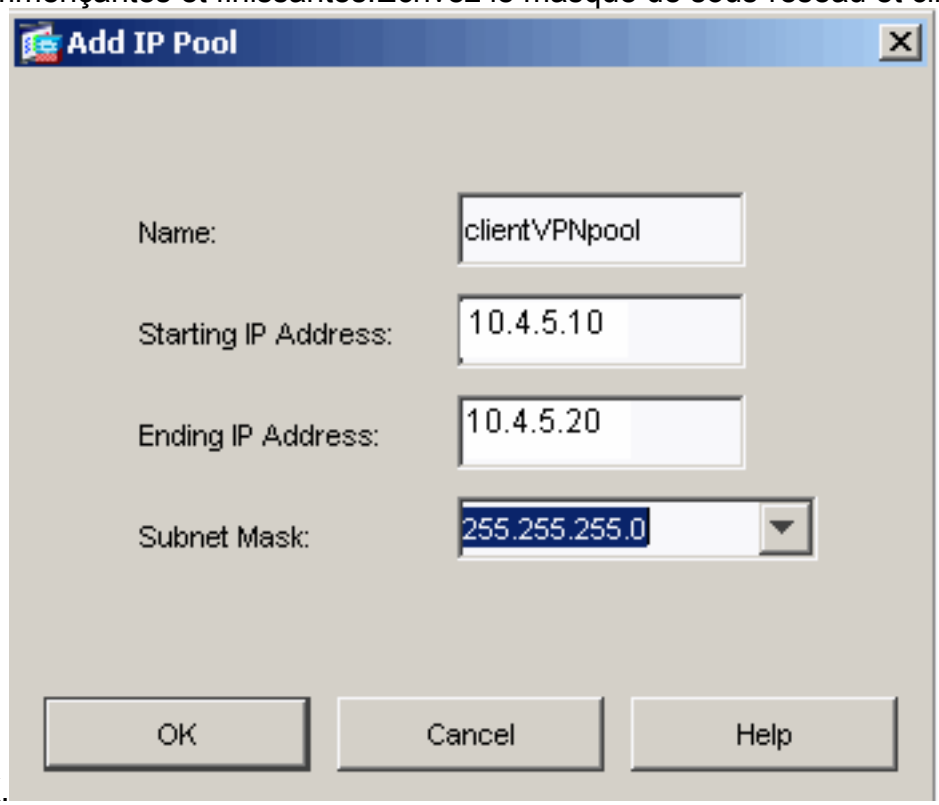



2. Terminez-vous ces étapes afin d'ajouter un jeu de transformations :Écrivez un nom pour le jeu de transformations.Choisissez les méthodes de cryptage de l'ESP et d'authentification de l'ESP.Choisissez le mode en tant que **transport**.Cliquez sur




**OK**.

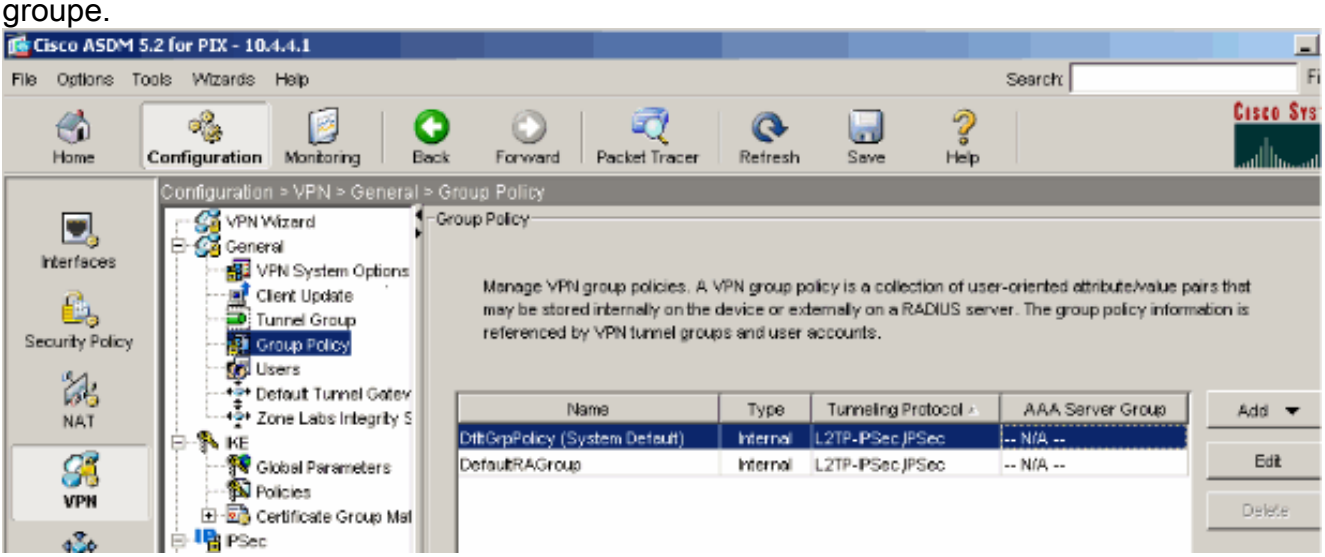
3. Terminez-vous ces étapes afin de configurer une méthode d'affectation d'adresses. Cet exemple utilise des groupes d'adresse IP.Choisissez la **configuration > le VPN > la gestion d'adresse IP > les groupes IP**.Cliquez sur **Add**. La boîte de dialogue Add IP Pool apparaît.Écrivez le nom du nouveau groupe d'adresse IP.Écrivez les adresses IP commençantes et finissantes.Écrivez le masque de sous-réseau et cliquez sur



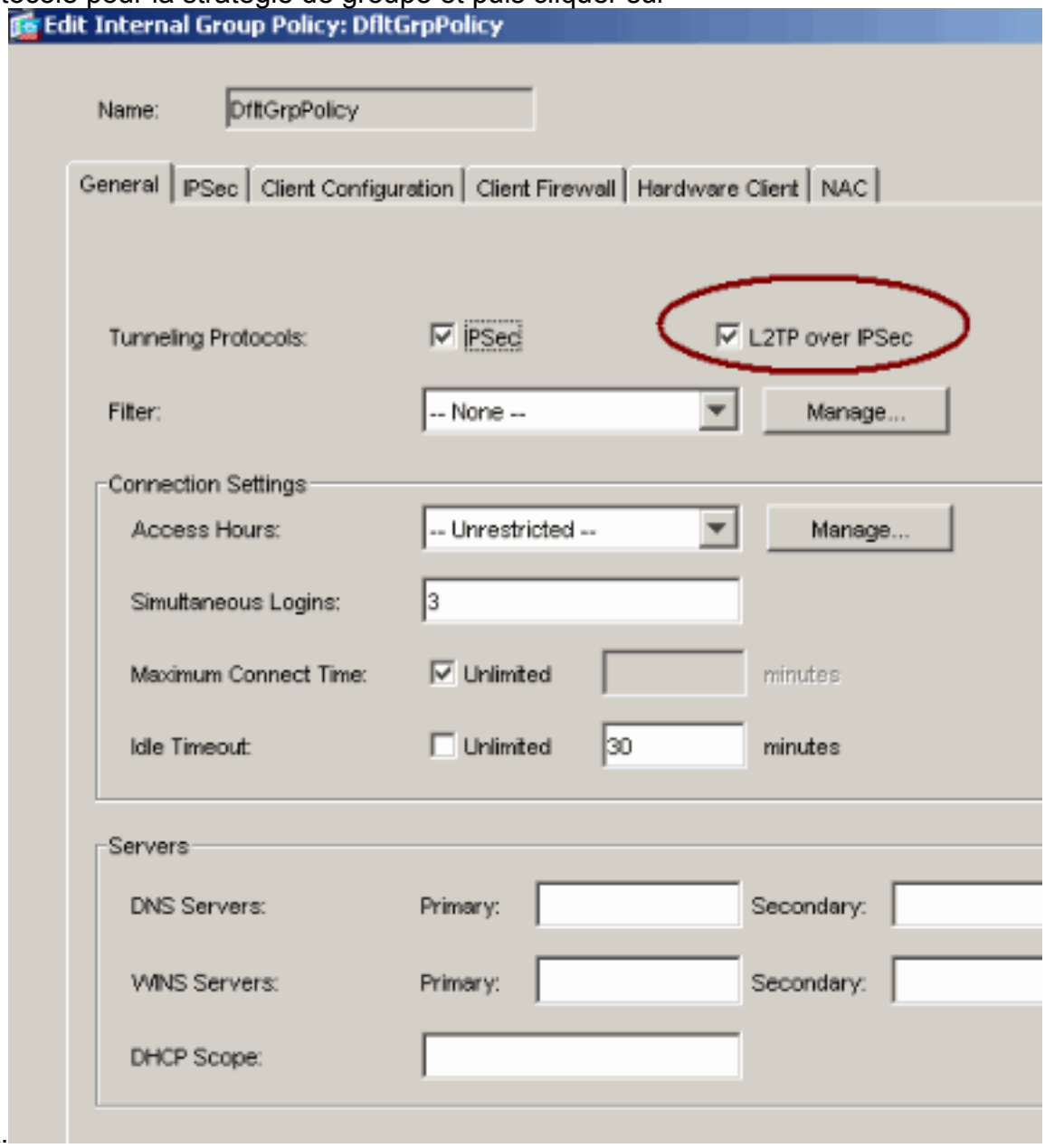

OK.

4. Choisissez le **Configuration > VPN > General > Group Policy** afin de configurer le L2TP sur IPsec comme protocole valide de tunnellisation VPN pour la stratégie de groupe. Les

affichages de volet de stratégie de groupe.



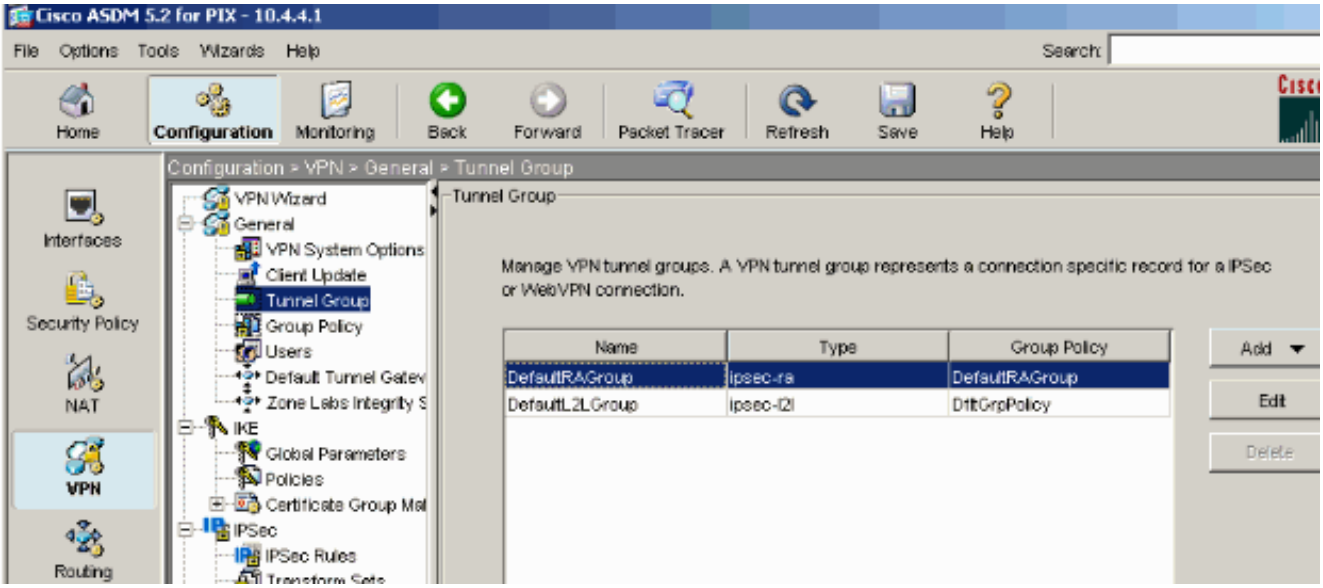

5. Sélectionnez une stratégie de groupe (DiffGrpPolicy) et cliquez sur Edit.Les affichages de dialogue de stratégie de groupe d'éditer. Vérifiez **L2TP au-dessus d'IPSec** afin d'activer le protocole pour la stratégie de groupe et puis cliquer sur



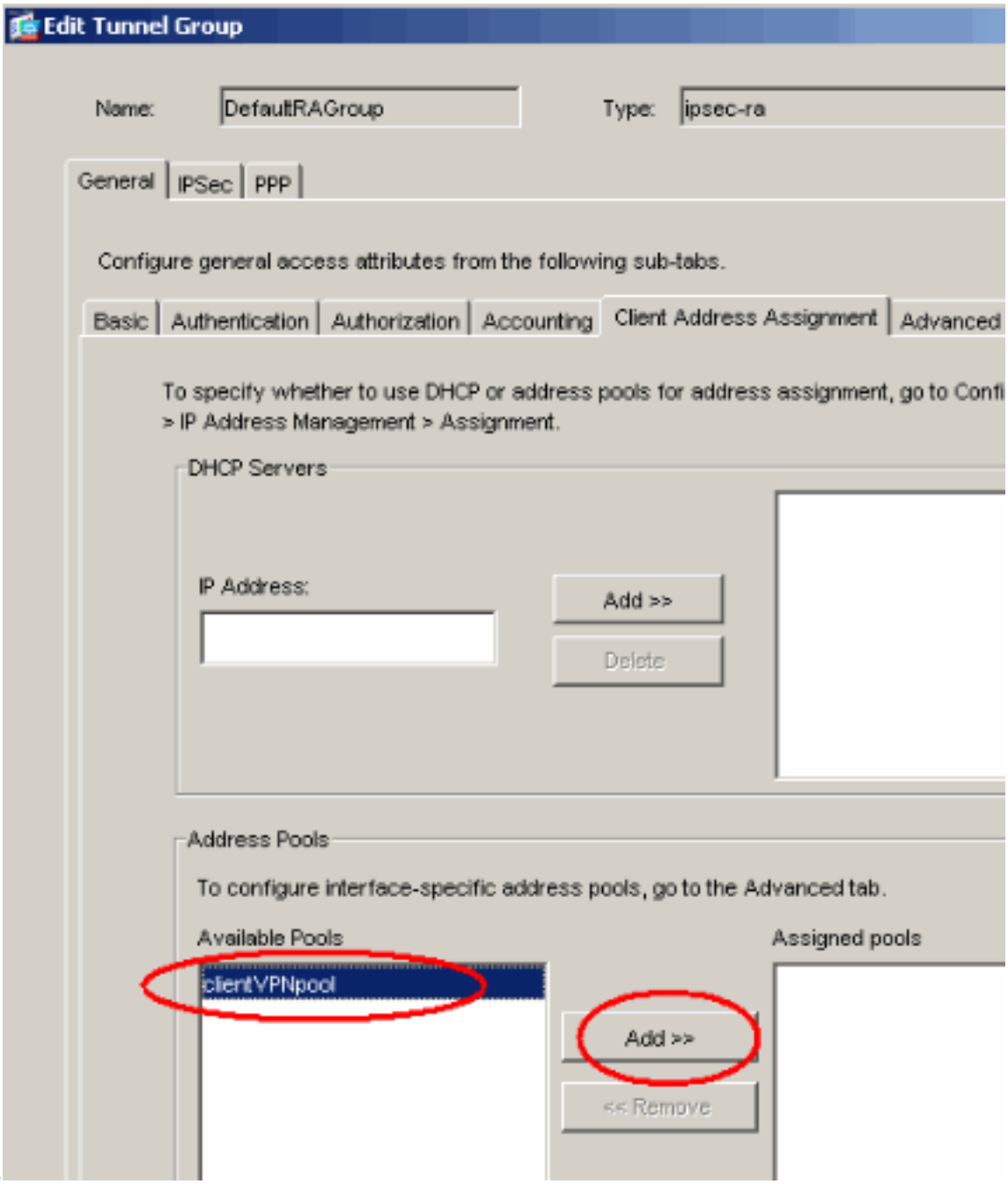

OK.

6. Terminez-vous ces étapes afin d'affecter le groupe d'adresse IP à un groupe de tunnel

:Choisissez la **configuration > le VPN > le groupe de général > de tunnel**.Après que le volet de groupe de tunnel apparaisse, sélectionnez un groupe de tunnel (DefaultRAGroup) dans la table.Cliquez sur
**Edit**.

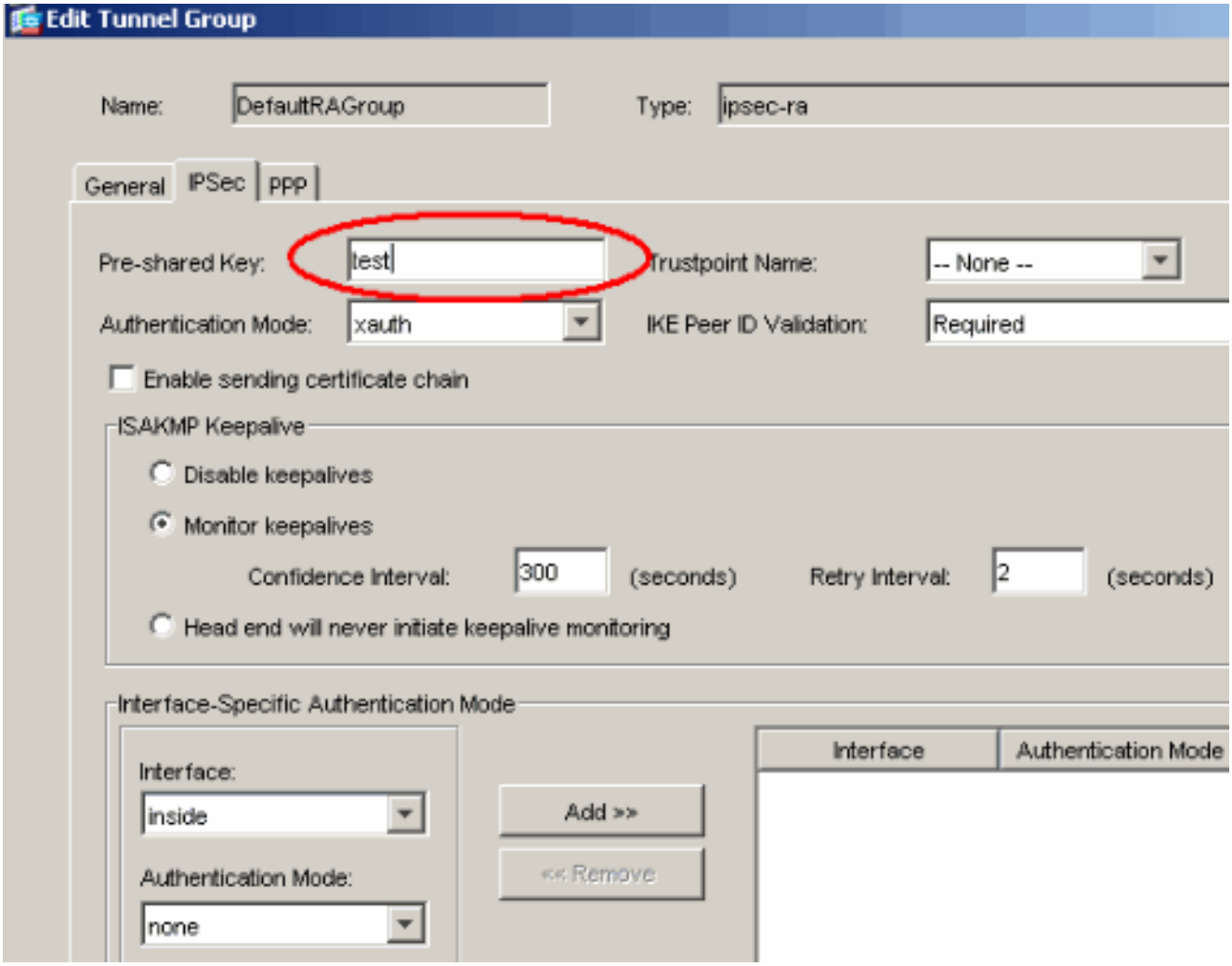



7. Terminez-vous ces étapes quand la fenêtre de groupe de tunnel d'éditer apparaît :De l'onglet Général, allez à l'onglet Client Address Assignment.Dans la région de pools d'adresses, choisissez un pool d'adresses pour assigner au groupe de tunnel.Cliquez sur **Add**. Le pool d'adresses semble dans les groupes assignés

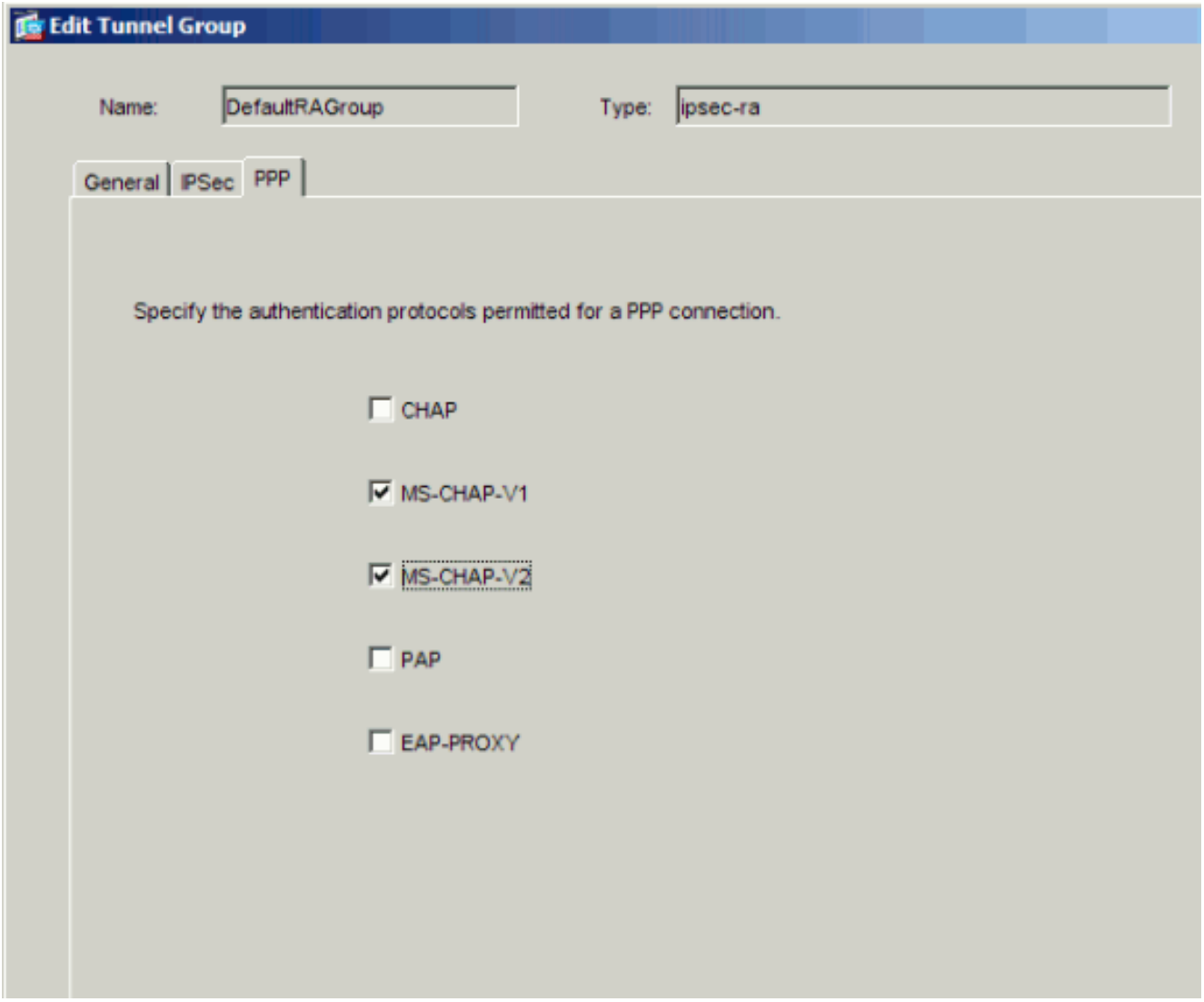


case.

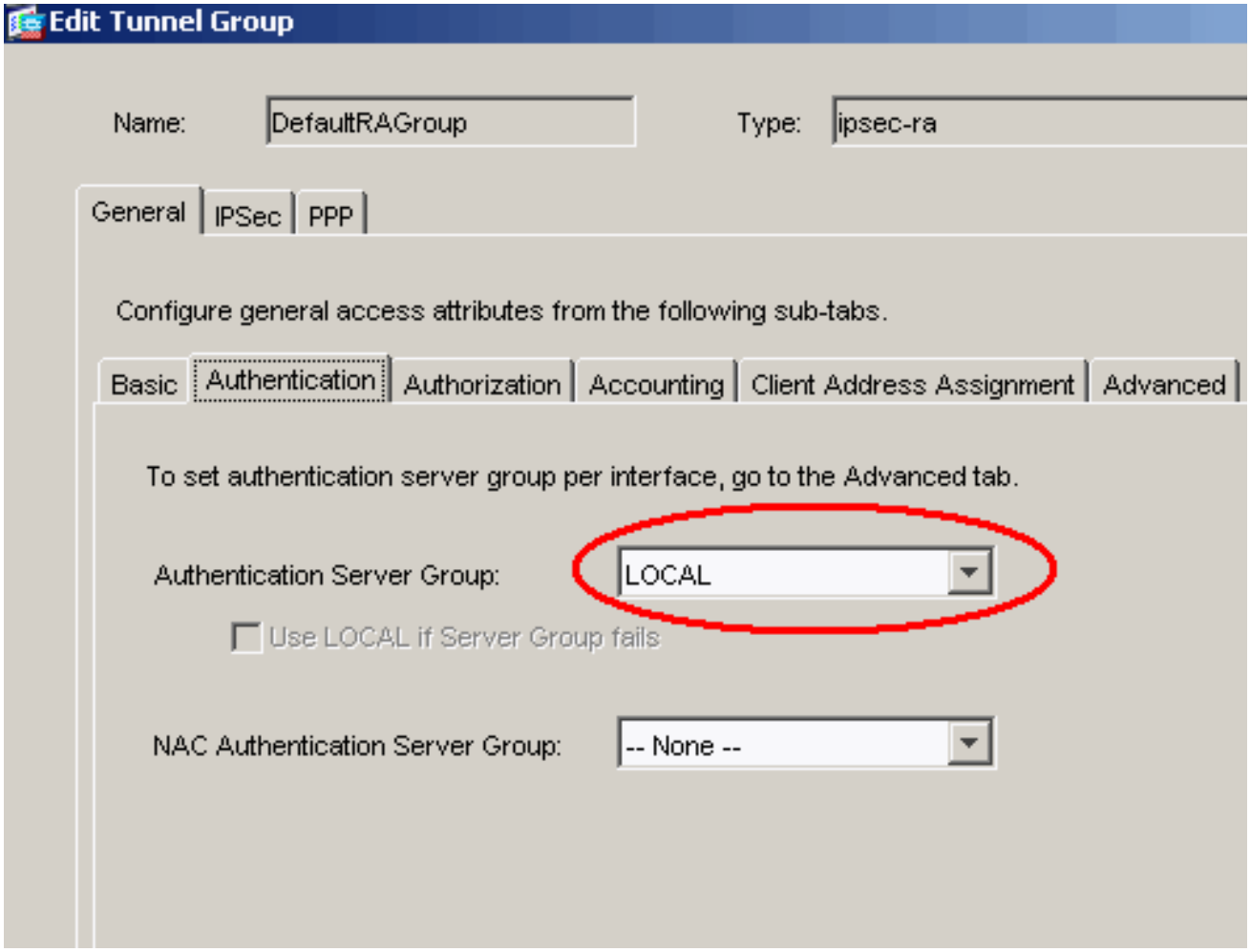
8. Afin de placer la clé pré-partagée, allez à l'onglet d'IPSec, introduisez votre **clé pré-partagée**, et cliquez sur
OK.




9. Le L2TP sur IPsec utilise des Protocoles d'authentification de PPP. Spécifiez les protocoles qui sont permis pour des connexions PPP sur l'onglet de PPP du groupe de tunnel. Sélectionnez le protocole **MS-CHAP-V1** pour l'authentification.



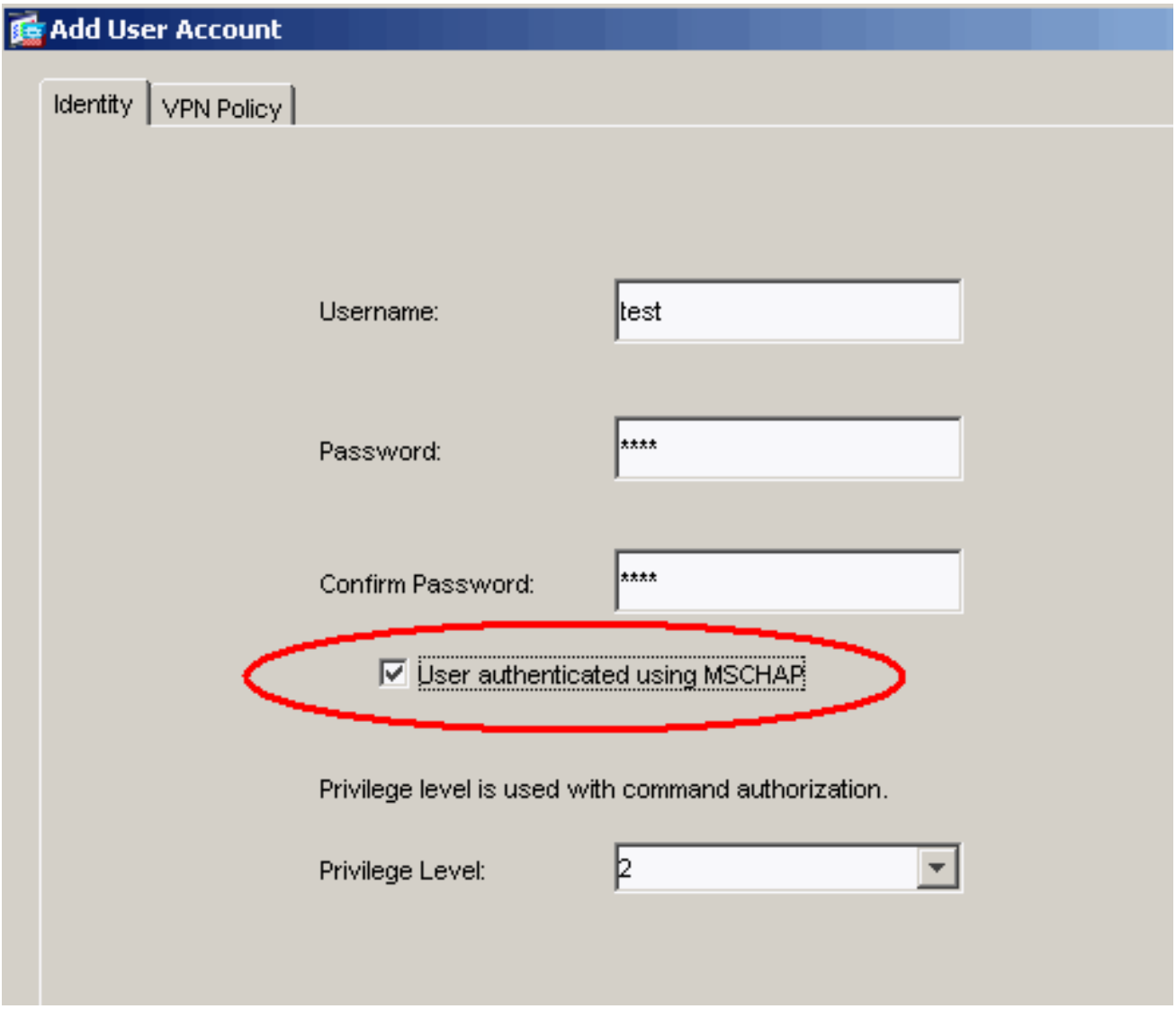

10. Spécifiez une méthode pour authentifier les utilisateurs qui tentent des connexions de L2TP sur IPsec.Vous pouvez configurer les dispositifs de sécurité pour utiliser un serveur d'authentification ou sa propre base de données locale. Afin de faire ceci, allez à l'onglet d'authentification du groupe de tunnel. Par défaut, les dispositifs de sécurité utilisent sa base de données locale. La liste déroulante de groupe de serveurs d'authentification affiche des GENS DU PAYS. Afin d'utiliser un serveur d'authentification, sélectionnez un de la liste.**Remarque:** L'appliance de Sécurité prend en charge seulement les authentifications PAP de PPP et des versions 1 et 2 de CHAP de Microsoft sur la base de données locale. L'EAP et le CHAP sont exécutés par des serveurs d'authentification de proxy. Par conséquent, si un utilisateur distant appartient à un groupe configuré de tunnel avec l'EAP ou le CHAP, et les dispositifs de sécurité est configuré pour utiliser la base de données locale, que l'utilisateur ne peut pas se
connecter.



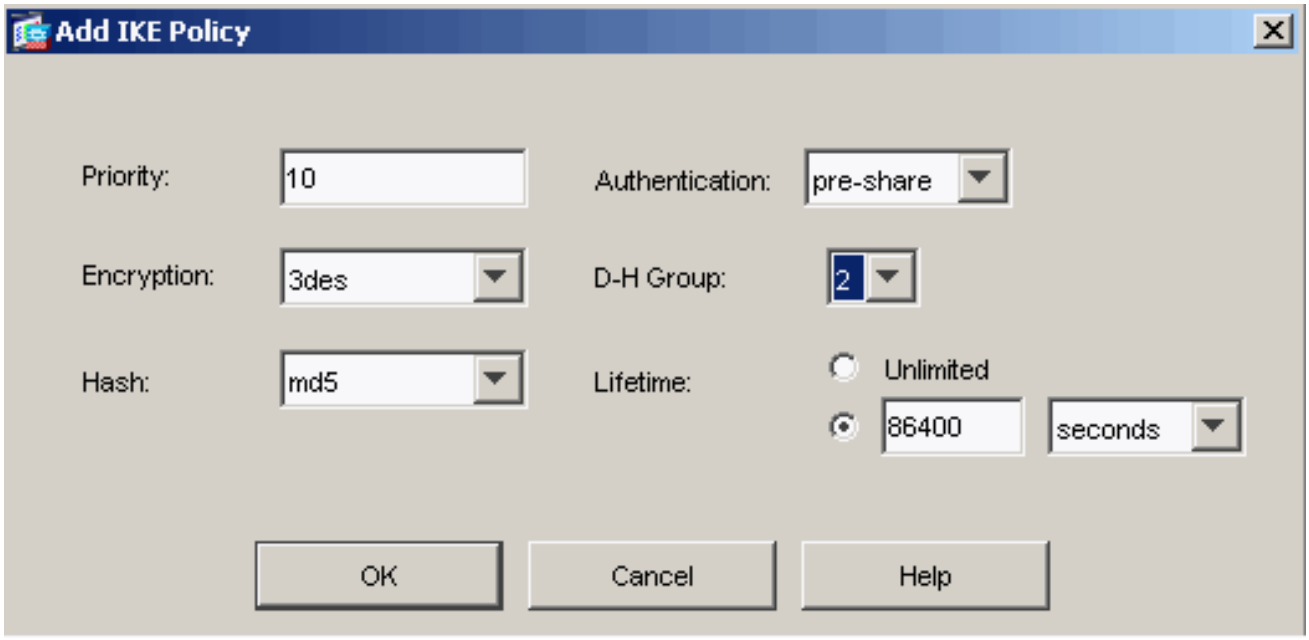

**Remarque:** Choisissez la **configuration > le VPN > le groupe de général > de tunnel** afin de retourner à la configuration de groupe de tunnel de sorte que vous puissiez lier la stratégie de groupe au groupe de tunnel et activer la commutation de groupe de tunnel (facultative). Quand le volet de groupe de tunnel apparaît, choisissez le groupe de tunnel et cliquez sur Edit.**Remarque:** Percez un tunnel le groupe que la commutation permet aux dispositifs de sécurité d'associer les différents utilisateurs qui établissent des connexions de L2TP sur IPsec avec différents groupes de tunnel. Puisque chaque groupe de tunnel a ses propres groupes de Groupe de serveurs AAA et d'adresse IP, des utilisateurs peuvent être authentifiés par des méthodes spécifiques à leur groupe de tunnel. Avec cette configuration, au lieu d'envoyer juste un nom d'utilisateur, l'utilisateur envoie un nom d'utilisateur et un nom de groupe dans le format username@group_name, où « @ » représente un délimiteur que vous pouvez configurer, et le nom de groupe est le nom d'un groupe de tunnel qui est configuré sur les dispositifs de sécurité.**Remarque:** La commutation de groupe de tunnel est activée par le groupe de bande traitant, qui permet aux dispositifs de sécurité de sélectionner le groupe de tunnel pour des connexions utilisateur en obtenant le nom de groupe du nom d'utilisateur présenté par le client vpn. Les dispositifs de sécurité envoient alors seulement la pièce d'utilisateur du nom d'utilisateur pour l'autorisation et l'authentification. Autrement (si handicapé), les dispositifs de sécurité envoient le nom d'utilisateur entier, y compris le royaume. Afin d'activer la commutation de groupe de tunnel, la **bande de** contrôle le **royaume du nom d'utilisateur avant de le transmettre au serveur d'AAA**, et la **bande de** contrôle le **groupe du nom d'utilisateur avant de le transmettre au serveur d'AAA**. Cliquez ensuite sur **OK**.

11. Terminez-vous ces étapes afin de créer un utilisateur dans la base de données locale :Choisissez les **>Properties de configuration > la gestion > les comptes utilisateurs de**

**périphérique**.Cliquez sur **Add**.Si l'utilisateur est un client L2TP qui utilise la version 1 ou 2 de CHAP de Microsoft, et l'appliance de Sécurité est configuré pour authentifier contre la base de données locale, vous devez vérifier l'**utilisateur authentifié utilisant MSCHAP** afin d'activer le MSCHAP.Cliquez sur
**OK**.




12. Choisissez la **configuration > le VPN > l'IKE > les stratégies** et cliquez sur Add afin de créer une stratégie IKE pour la phase I. cliquent sur OK pour
continuer.



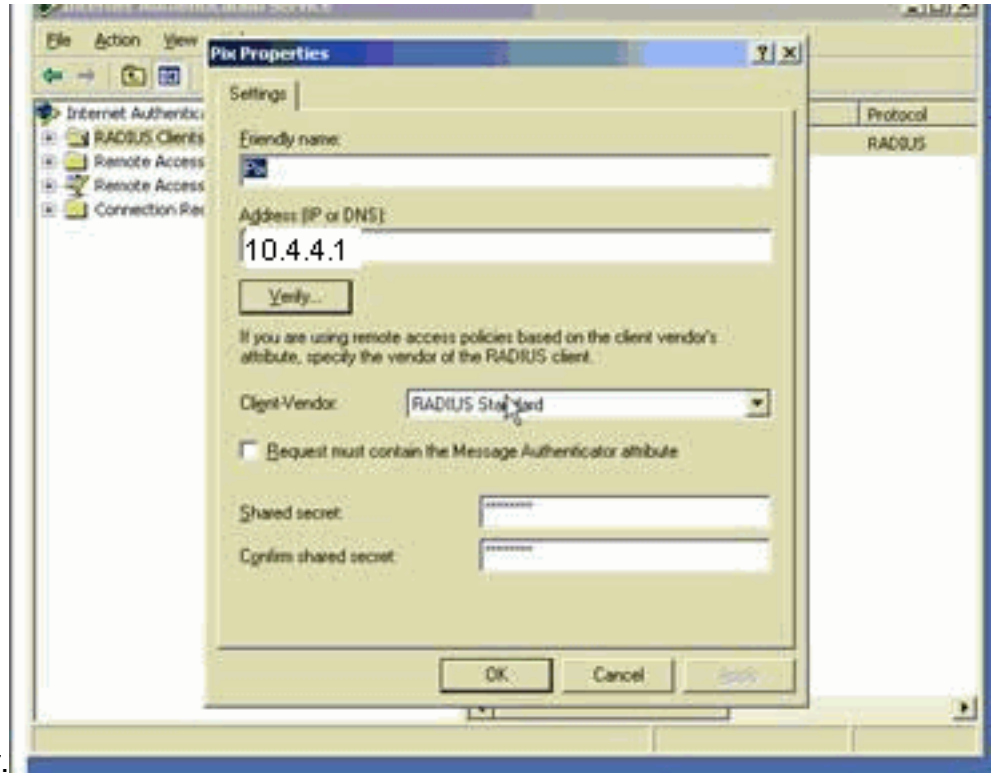

13. (Facultatif) si vous vous attendez à ce que les plusieurs clients L2TP derrière un périphérique NAT tentent des connexions de L2TP sur IPsec aux dispositifs de sécurité, vous devez activer le NAT Traversal de sorte que les paquets de l'ESP puissent traverser un ou plusieurs périphériques NAT. Pour ce faire, exécutez ces étapes:Choisissez la **configuration > le VPN > l'IKE > les paramètres globaux**.Assurez-vous que l'**ISAKMP** est activé sur une interface.**Enable IPSec de** contrôle **au-dessus de NAT-T**.Cliquez sur **OK**.

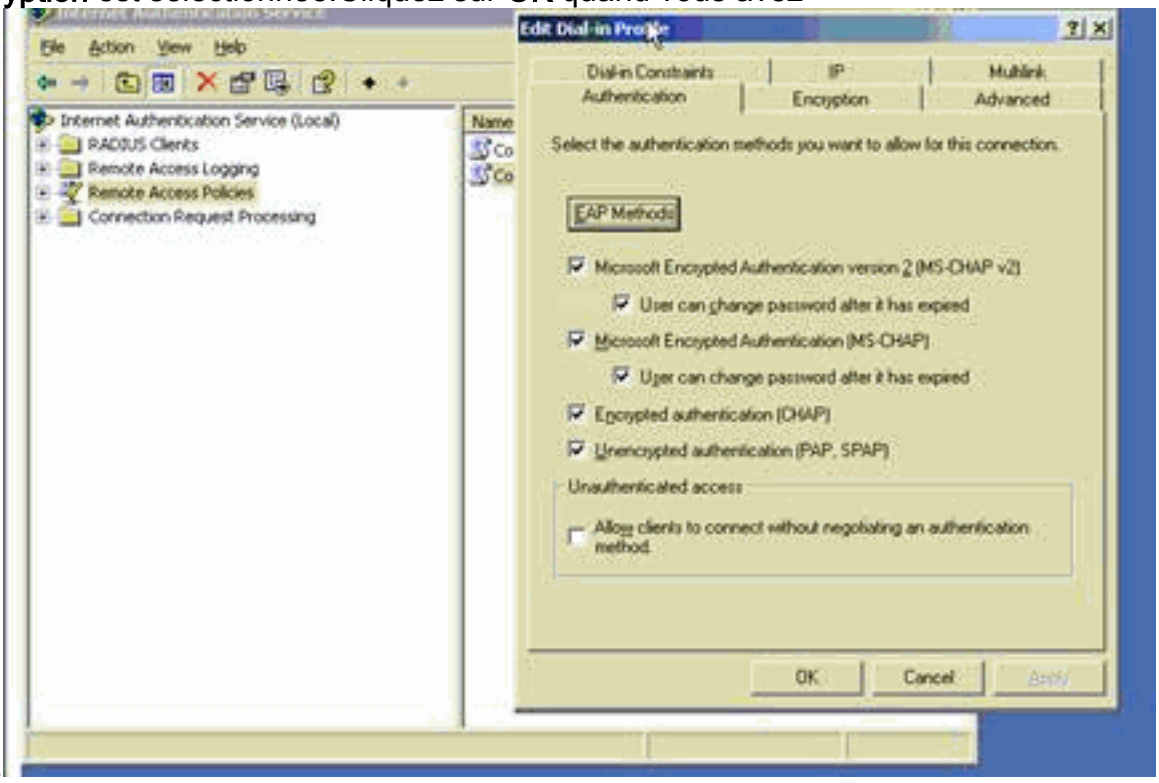
## Configuration de Microsoft Windows Serveur 2003 avec IAS

Terminez-vous ces étapes afin de configurer le serveur de Microsoft Windows 2003 avec IAS.

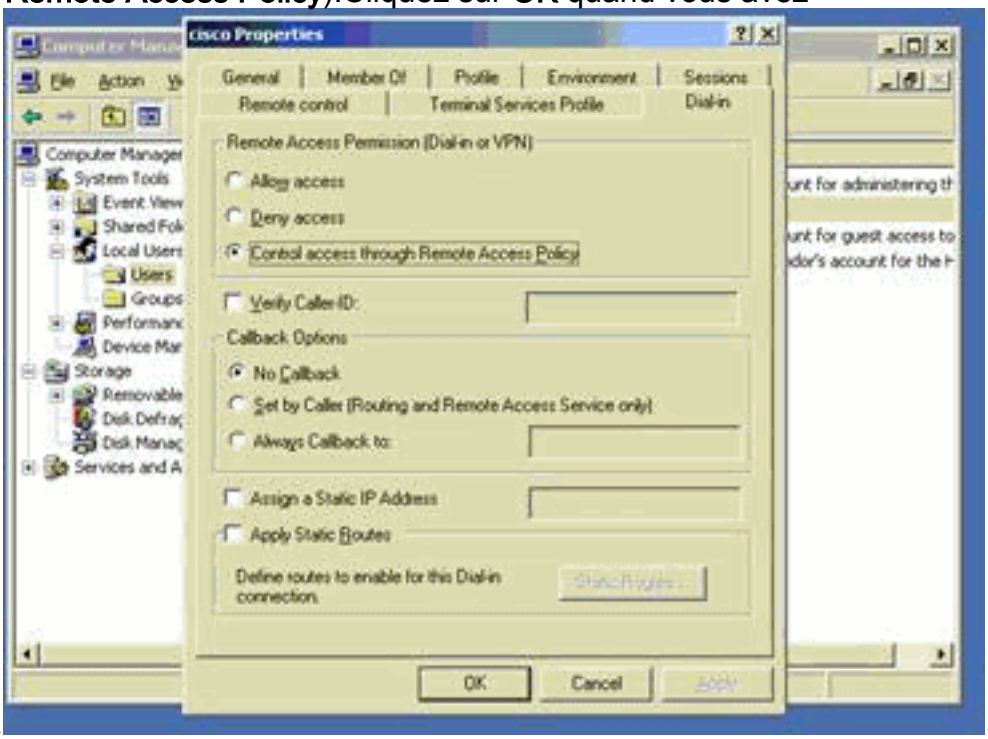
**Remarque:** ces étapes supposent que IAS est déjà installé sur l'ordinateur local. Sinon, ajoutez ce composant via **Control Panel > Add/Remove Programs**.

1. Choisissez les **outils d'administration > le Service d'authentification Internet** et cliquez avec le bouton droit sur le **client RADIUS** afin d'ajouter un nouveau client RADIUS. Après que vous tapiez les informations de client, cliquez sur OK.Cet exemple affiche un client nommé « Pix » avec une adresse IP de 10.4.4.1. Le Client-constructeur est placé au **RADIUS Standard**, et le secret partagé est

radiuskey. 


2. Choisissez les **stratégies d'accès à distance**, cliquez avec le bouton droit sur des **connexions à d'autres serveurs d'accès**, et sélectionnez **Properties**.
3. Assurez-vous que l'option **Grant Remote Access Permissions** est sélectionnée.
4. Cliquez sur **Edit Profile** et vérifiez ces paramètres :Sur l'onglet d'authentification, vérifiez l'**authentification décryptée (PAP, SPAP)**.Dans l'onglet Encryption, assurez-vous que l'option **No Encryption** est sélectionnée.Cliquez sur **OK** quand vous avez terminé. 


5. Choisissez l'**Administrative Tools > Computer Management > System Tools > Local Users and Groups**, cliquez avec le bouton droit sur des **utilisateurs** et de **nouveaux utilisateurs** choisis afin d'ajouter un utilisateur en compte d'ordinateur local.
6. Ajoutez un utilisateur avec le mot de passe Cisco **password1** et vérifiez les informations de son profil :Dans l'onglet General, assurez-vous que l'option **Password Never Expired** est

sélectionnée au lieu de l'option User Must Change Password.Dans l'onglet Dial-in, sélectionnez l'option **Allow access** (ou conservez la configuration par défaut **Control access through Remote Access Policy**).Cliquez sur **OK** quand vous avez terminé. 


## Authentification étendue pour L2TP au-dessus d'IPSec utilisant le Répertoire actif

Employez cette configuration sur l'ASA afin de permettre à l'authentification pour que la connexion L2tp ait lieu à partir du Répertoire actif :

```
ciscoasa(config-tunnel-general)# tunnel-group DefaultRAGroup ppp-attributes ciscoasa(config-ppp)# authentication pap
```

En outre, sur le client L2tp, allez aux **configurations de sécurité avancée (coutume)** et choisissez seulement l'option pour le **mot de passe non chiffré (PAP)**.

# Vérifiez

Cette section présente des informations que vous pouvez utiliser pour vous assurer que votre configuration fonctionne correctement.

Certaines commandes **show** sont prises en charge par l'Output Interpreter Tool (clients enregistrés uniquement), qui vous permet de voir une analyse de la sortie de la commande show.

- **show crypto ipsec sa** — Affiche toutes les associations de sécurité en cours d'IKE (SAS) à un pair.`pixfirewall#show crypto ipsec sa interface: outside Crypto map tag: outside_dyn_map, seq num: 20, local addr: 172.16.1.1 access-list 105 permit ip host 172.16.1.1 host 192.168.0.2 local ident (addr/mask/prot/port): (172.16.1.1/255.255.255.255/17/0) remote ident (addr/mask/prot/port): (192.168.0.2/255.255.255.255/17/1701) current_peer: 192.168.0.2, username: test dynamic allocated peer ip: 10.4.5.15 #pkts encaps: 23, #pkts encrypt: 23, #pkts digest: 23 #pkts decaps: 93, #pkts decrypt: 93, #pkts verify: 93 #pkts compressed: 0, #pkts decompressed: 0 #pkts not compressed: 23, #pkts comp failed: 0, #pkts decomp failed: 0 #post-frag successes: 0, #post-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.: 172.16.1.1, remote crypto endpt.: 192.168.0.2 path mtu 1500, ipsec overhead 58, media mtu 1500 current outbound spi: C16F05B8 inbound esp sas: spi: 0xEC06344D`

```
(3959829581) transform: esp-3des esp-md5-hmac in use settings ={RA, Transport, } slot: 0,
conn_id: 3, crypto-map: outside_dyn_map sa timing: remaining key lifetime (sec): 3335 IV
size: 8 bytes replay detection support: Y outbound esp sas: spi: 0xC16F05B8 (3245278648)
transform: esp-3des esp-md5-hmac in use settings ={RA, Transport, } slot: 0, conn_id: 3,
crypto-map: outside_dyn_map sa timing: remaining key lifetime (sec): 3335 IV size: 8 bytes
replay detection support: Y
```

- **show crypto isakmp sa** — Affiche toutes les SA IKE en cours au niveau d'un homologue.`pixfirewall#`**`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: 192.168.0.2 Type : user Role : responder Rekey : no State : MM_ACTIVE`
- **exposition VPN-sessiondb** — Inclut les filtres de protocole que vous pouvez utiliser afin de visualiser les informations détaillées au sujet des connexions de L2TP sur IPsec. La pleine commande du mode de configuration globale est le **protocole distant l2tpOverIpsec de filtre détaillé par VPN-sessoindb d'exposition**.Cet exemple affiche les détails d'une connexion simple de L2TP sur IPsec :`pixfirewall#`**`show vpn-sessiondb detail remote filter protocol L2TPOverIPSec`** `Session Type: Remote Detailed Username : test Index : 1 Assigned IP : 10.4.5.15 Public IP : 192.168.0.2 Protocol : L2TPOverIPSec Encryption : 3DES Hashing : MD5 Bytes Tx : 1336 Bytes Rx : 14605 Client Type : Client Ver : Group Policy : DefaultRAGroup Tunnel Group : DefaultRAGroup Login Time : 18:06:08 UTC Fri Jan 1 1993 Duration : 0h:04m:25s Filter Name : NAC Result : N/A Posture Token: IKE Sessions: 1 IPSec Sessions: 1 L2TPOverIPSec Sessions: 1 IKE: Session ID : 1 UDP Src Port : 500 UDP Dst Port : 500 IKE Neg Mode : Main Auth Mode : preSharedKeys Encryption : 3DES Hashing : MD5 Rekey Int (T): 28800 Seconds Rekey Left(T): 28536 Seconds D/H Group : 2 IPSec: Session ID : 2 Local Addr : 172.16.1.1/255.255.255.255/17/1701 Remote Addr : 192.168.0.2/255.255.255.255/17/1701 Encryption : 3DES Hashing : MD5 Encapsulation: Transport Rekey Int (T): 3600 Seconds Rekey Left(T): 3333 Seconds Idle Time Out: 30 Minutes Idle TO Left : 30 Minutes Bytes Tx : 1336 Bytes Rx : 14922 Pkts Tx : 25 Pkts Rx : 156 L2TPOverIPSec: Session ID : 3 Username : test Assigned IP : 10.4.5.15 Encryption : none Auth Mode : msCHAPV1 Idle Time Out: 30 Minutes Idle TO Left : 30 Minutes Bytes Tx : 378 Bytes Rx : 13431 Pkts Tx : 16 Pkts Rx : 146`

# Dépannez

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

## Dépannage des commandes

Certaines commandes sont prises en charge par l'Output Interpreter Tool (clients enregistrés seulement), qui te permet pour visualiser une analyse de sortie de commande show.

**Remarque:** Consultez Informations importantes sur les commandes debug et Dépannage de la sécurité IP - Présentation et utilisation des commandes debug avant d'utiliser les commandes **debug**.

- **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

### Pare-feu PIX

```
PIX#debug crypto isakmp 7 pixfirewall# Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, IKE_DECODE
RECEIVED Mess age (msgid=0) with payloads : HDR + SA (1) + VENDOR (13) + VENDOR (13) + VENDOR
(13) + NONE (0) total length : 256 Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, processing
```

SA payload Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, Oakley proposal is acceptable Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, processing VID payload Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, processing VID payload Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, Received Fragmentation VID Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, processing VID payload Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, Received NAT-Traversal ver 02 V ID Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, processing IKE SA payload Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, IKE SA Proposal # 1, Transform # 2 acceptable Matches global IKE entry # 2 Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, constructing ISAKMP SA payload Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, constructing Fragmentation VID + extended capabilities payload Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, IKE_DECODE SENDING Message (msgid=0) with payloads : HDR + SA (1) + VENDOR (13) + NONE (0) total length : 104 Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, IKE_DECODE RECEIVED Message (msgid=0) with payloads : HDR + KE (4) + NONCE (10) + NONE (0) total length : 184 Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, processing ke payload Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, processing ISA_KE payload Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, processing nonce payload Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, constructing ke payload Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, constructing nonce payload Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, constructing Cisco Unity VID pa yload Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, constructing xauth V6 VID paylo ad Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, Send IOS VID Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, Constructing ASA spoofing IOS V endor ID payload (version: 1.0.0, capabilities: 20000001) Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, constructing VID payload Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, Send Altiga/Cisco VPN3000/Cisco ASA GW VID Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, Connection landed on tunnel_group Def aultRAGroup Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, Generat ing keys for Responder... Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, IKE_DECODE SENDING Message (msgid=0) with payloads : HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) + VENDOR ( 13) + VENDOR (13) + NONE (0) total length : 256 Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, IKE_DECODE RECEIVED Message (msgid=0) with payloads : HDR + ID (5) + HASH (8) + NONE (0) total length : 60 Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, process ing ID payload Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, process ing hash payload Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, Computi ng hash for ISAKMP Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, Connection landed on tunnel_group Def aultRAGroup Jan 02 18:26:44 [IKEv1]: Group = DefaultRAGroup, IP = 192.168.0.2, Freeing previ ously allocated memory for authorization-dn-attributes Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, constru cting ID payload Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, constru cting hash payload Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, Computi ng hash for ISAKMP Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, constru cting dpd vid payload Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, IKE_DECODE SENDING Message (msgid=0) with payloads : HDR + ID (5) + HASH (8) + VENDOR (13) + NONE (0) total length : 80 *!--- Phase 1 completed succesfully.* Jan 02 18:26:44 [IKEv1]: Group = DefaultRAGroup, IP = 192.168.0.2, **PHASE 1 COMPL ETED** Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, Keep-alive type for this connection: None Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, Keep-alives configured on but peer do es not support keep-alives (type = None) Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, Startin g P1 rekey timer: 21600 seconds. Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, IKE_DECODE RECEIVED Message (msgid=e1 b84b0) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0) total length : 164 Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, process ing hash payload Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, process ing SA payload Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, process ing nonce payload Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, process ing ID payload Jan 02 18:26:44 [IKEv1]: Group = DefaultRAGroup, IP = 192.168.0.2, Received remo te Proxy Host data in ID Payload: Address 192.168.0.2, Protocol 17, Port 1701 Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, process ing ID payload Jan 02 18:26:44 [IKEv1]: Group = DefaultRAGroup, IP = 192.168.0.2, Received loca l Proxy Host data in ID Payload: Address 172.16.1.1, Protocol 17, Port 1701 *!--- PIX identifies the L2TP/IPsec session.* Jan 02 18:26:44 [IKEv1]: Group = DefaultRAGroup, IP = 192.168.0.2, **L2TP/IPSec se ssion detected.** Jan 02 18:26:44 [IKEv1]: Group = DefaultRAGroup, IP = 192.168.0.2, QM IsRekeyed old sa not found by addr Jan 02 18:26:44 [IKEv1]: Group = DefaultRAGroup, IP = 192.168.0.2, IKE Remote Pe er configured for crypto map: outside_dyn_map Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, process ing IPSec SA payload Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, IPSec S A Proposal # 1, Transform # 1 acceptable Matches global IPSec SA entry # 20 Jan 02 18:26:44 [IKEv1]: Group = DefaultRAGroup, IP = 192.168.0.2, IKE: requesti ng SPI! Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, IKE got SPI from key engine:

SPI = 0xce9f6e19 *!--- Constructs Quick mode in Phase 2.* Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, **oakley constucting quick mode** Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, constru cting blank hash payload Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, constru cting IPSec SA payload Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, constru cting IPSec nonce payload Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, constru cting proxy ID Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, Transmi tting Proxy Id: Remote host: 192.168.0.2 Protocol 17 Port 1701 Local host: 172.16.1.1 Protocol 17 Port 1701 Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, constru cting qm hash payload Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, IKE_DECODE SENDING Message (msgid=e1b 84b0) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + N ONE (0) total length : 144 Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, IKE_DECODE RECEIVED Message (msgid=e1 b84b0) with payloads : HDR + HASH (8) + NONE (0) total length : 48 Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, process ing hash payload Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, loading all IPSEC SAs Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, Generat ing Quick Mode Key! Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, Generat ing Quick Mode Key! Jan 02 18:26:44 [IKEv1]: Group = DefaultRAGroup, IP = 192.168.0.2, Security nego tiation complete for User () Responder, Inbound SPI = 0xce9f6e19, Outbound SPI = 0xd08f711b Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, IKE got a KEY_ADD msg for SA: SPI = 0xd08f711b Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, Pitcher : received KEY_UPDATE, spi 0xce9f6e19 Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, Startin g P2 rekey timer: 3059 seconds. *!--- Phase 2 completes succesfully.* Jan 02 18:26:44 [IKEv1]: Group = DefaultRAGroup, IP = 192.168.0.2, PHASE 2 COMPL ETED (msgid=0e1b84b0) Jan 02 18:26:44 [IKEv1]: IKEQM_Active() Add L2TP classification rules: ip <192.1 68.0.2> mask <0xFFFFFFFF> port <1701> PIX#**debug crypto ipsec 7** pixfirewall# IPSEC: Deleted inbound decrypt rule, SPI 0x71933D09 Rule ID: 0x028D78D8 IPSEC: Deleted inbound permit rule, SPI 0x71933D09 Rule ID: 0x02831838 IPSEC: Deleted inbound tunnel flow rule, SPI 0x71933D09 Rule ID: 0x029134D8 IPSEC: Deleted inbound VPN context, SPI 0x71933D09 VPN handle: 0x0048B284 IPSEC: Deleted outbound encrypt rule, SPI 0xAF4DA5FA Rule ID: 0x028DAC90 IPSEC: Deleted outbound permit rule, SPI 0xAF4DA5FA Rule ID: 0x02912AF8 IPSEC: Deleted outbound VPN context, SPI 0xAF4DA5FA VPN handle: 0x0048468C IPSEC: New embryonic SA created @ 0x01BFCF80, SCB: 0x01C262D0, Direction: inbound SPI : 0x45C3306F Session ID: 0x0000000C VPIF num : 0x00000001 Tunnel type: ra Protocol : esp Lifetime : 240 seconds IPSEC: New embryonic SA created @ 0x0283A3A8, SCB: 0x028D1B38, Direction: outbound SPI : 0x370E8DD1 Session ID: 0x0000000C VPIF num : 0x00000001 Tunnel type: ra Protocol : esp Lifetime : 240 seconds IPSEC: Completed host OBSA update, SPI 0x370E8DD1 IPSEC: Creating outbound VPN context, SPI 0x370E8DD1 Flags: 0x00000205 SA : 0x0283A3A8 SPI : 0x370E8DD1 MTU : 1500 bytes VCID : 0x00000000 Peer : 0x00000000 SCB : 0x028D1B38 Channel: 0x01693F08 IPSEC: Completed outbound VPN context, SPI 0x370E8DD1 VPN handle: 0x0048C164 IPSEC: New outbound encrypt rule, SPI 0x370E8DD1 Src addr: 172.16.1.1 Src mask: 255.255.255.255 Dst addr: 192.168.0.2 Dst mask: 255.255.255.255 Src ports Upper: 1701 Lower: 1701 Op : equal Dst ports Upper: 1701 Lower: 1701 Op : equal Protocol: 17 Use protocol: true SPI: 0x00000000 Use SPI: false IPSEC: Completed outbound encrypt rule, SPI 0x370E8DD1 Rule ID: 0x02826540 IPSEC: New outbound permit rule, SPI 0x370E8DD1 Src addr: 172.16.1.1 Src mask: 255.255.255.255 Dst addr: 192.168.0.2 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: 0x370E8DD1 Use SPI: true IPSEC: Completed outbound permit rule, SPI 0x370E8DD1 Rule ID: 0x028D78D8 IPSEC: Completed host IBSA update, SPI 0x45C3306F IPSEC: Creating inbound VPN context, SPI 0x45C3306F Flags: 0x00000206 SA : 0x01BFCF80 SPI : 0x45C3306F MTU : 0 bytes VCID : 0x00000000 Peer : 0x0048C164 SCB : 0x01C262D0 Channel: 0x01693F08 IPSEC: Completed inbound VPN context, SPI 0x45C3306F VPN handle: 0x0049107C IPSEC: Updating outbound VPN context 0x0048C164, SPI 0x370E8DD1 Flags: 0x00000205 SA : 0x0283A3A8 SPI : 0x370E8DD1 MTU : 1500 bytes VCID : 0x00000000 Peer : 0x0049107C SCB : 0x028D1B38 Channel: 0x01693F08 IPSEC: Completed outbound VPN context, SPI 0x370E8DD1 VPN handle: 0x0048C164 IPSEC: Completed outbound inner rule, SPI 0x370E8DD1 Rule ID: 0x02826540 IPSEC: Completed outbound outer SPD rule, SPI 0x370E8DD1 Rule ID: 0x028D78D8 IPSEC: New inbound tunnel flow rule, SPI 0x45C3306F Src addr: 192.168.0.2 Src mask: 255.255.255.255 Dst addr: 172.16.1.1 Dst mask: 255.255.255.255 Src ports Upper: 1701 Lower: 1701 Op : equal Dst ports Upper: 1701 Lower: 1701 Op : equal Protocol: 17 Use protocol: true SPI: 0x00000000 Use SPI: false IPSEC: Completed inbound tunnel flow rule, SPI 0x45C3306F Rule ID: 0x02831838 IPSEC: New inbound decrypt rule, SPI 0x45C3306F Src addr: 192.168.0.2 Src mask: 255.255.255.255 Dst addr: 172.16.1.1 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: 0x45C3306F Use SPI: true IPSEC: Completed inbound decrypt rule, SPI 0x45C3306F Rule ID: 0x028DAC90 IPSEC: New inbound permit rule, SPI 0x45C3306F Src addr: 192.168.0.2 Src mask: 255.255.255.255 Dst

```
addr: 172.16.1.1 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: 0x45C3306F Use SPI: true
IPSEC: Completed inbound permit rule, SPI 0x45C3306F Rule ID: 0x02912E50
```

## Dépannez utilisant l'ASDM

Vous pouvez employer l'ASDM afin d'activer se connecter et visualiser les logs.

1. Choisissez la **configuration > le Properties > en se connectant > en se connectant l'installation**, sélectionnez l'**enable se connectant** et cliquez sur Apply afin d'activer se connecter.
2. Choisissez la **surveillance > en se connectant > mémoire tampon de log > sur se connecter le niveau**, le **tampon de journalisation** choisi, et la **vue de** clic afin de visualiser les logs.

## Problème : Fréquentez les débranchements

### Inactif/Session Timeout

Si le délai d'attente de veille est placé à 30 minutes (par défaut), il signifie qu'il relâche le tunnel après qu'aucun trafic ne le traverse pendant 30 minutes. Le client vpn obtient déconnecté après 30 minutes indépendamment de la configuration du délai d'attente de veille et rencontre le message d'erreur `PEER_DELETE-IKE_DELETE_UNSPECIFIED`.

Configurez **idle timeout** et **session timeout** sur **none** afin que le tunnel **fonctionne** toujours et de sorte qu'il ne soit jamais supprimé.

Saisissez la commande **vpn-idle-timeout** dans le mode de configuration de la stratégie de groupe ou de configuration du nom d'utilisateur afin de configurer le délai d'attente de l'utilisateur :

```
hostname(config)#group-policy DfltGrpPolicy attributes hostname(config-group-policy)#vpn-idle-timeout none
```

Configurez une durée maximale pour des connexions de VPN avec la commande **vpn-session-timeout** dans le mode de configuration de la stratégie de groupe ou de configuration du nom d'utilisateur :

```
hostname(config)#group-policy DfltGrpPolicy attributes hostname(config-group-policy)#vpn-session-timeout none
```

## Dépannez les Windows Vista

### Utilisateur simultané

Les Windows Vista L2TP/IPsec ont introduit quelques modifications architecturales qui ont interdit plus d'un utilisateur simultané d'être connecté à une tête de réseau PIX/ASA. Ce comportement ne se produit pas sur Windows 2K/XP. Cisco a mis en application un contournement pour cette modification en date de la version 7.2(3) et plus grand.

### PC de vista non capable se connecter

Si l'ordinateur de Windows Vista ne peut pas connecter le serveur L2TP, alors vérifiez que vous avez configuré SEULEMENT mschap-v2 sous les ppp-attributs sur le DefaultRAGroup.

# Informations connexes

- Solutions de dépannage les plus fréquentes concernant un VPN IPsec LAN à LAN et d'accès à distance
- Dispositifs de sécurité de la gamme Cisco PIX 500
- Dispositifs de sécurité adaptatifs de la gamme Cisco ASA 5500
- Support produit de Logiciels pare-feu Cisco PIX
- Références des commandes du pare-feu Cisco Secure PIX
- Page d'assistance RADIUS
- Page de support de la négociation IPSec/des protocoles IKE
- Demandes de commentaires (RFC)
- Protocole L2TP (Layer Two Tunnel Protocol)
- Support et documentation techniques - Cisco Systems