

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](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Produits connexes](#)

[Conventions](#)

[Informations générales](#)

[Configuration](#)

[Diagramme du réseau](#)

[Configurations](#)

[Configuration du client L2TP/IPsec Windows](#)

[Serveur L2TP dans la configuration PIX](#)

[L2TP avec configuration ASDM](#)

[Configuration de Microsoft Windows Serveur 2003 avec IAS](#)

[Authentification étendue pour L2TP sur IPsec à l'aide d'Active Directory](#)

[Vérification](#)

[Dépannage](#)

[Dépannage des commandes](#)

[Exemple de sortie de débogage](#)

[Dépannage à l'aide d'ASDM](#)

[Problème : Déconnexions fréquentes](#)

[Dépannage de Windows Vista](#)

[Informations connexes](#)

Introduction

Ce document décrit comment configurer le protocole L2TP (Layer 2 Tunneling Protocol) sur IP Security (IPsec) à partir de clients Microsoft Windows 2000/2003 et XP distants vers un bureau d'entreprise PIX Security Appliance à l'aide de clés pré-partagées avec le serveur RADIUS de Microsoft Windows 2003 Internet Authentication Service (IAS) pour l'authentification des utilisateurs. Consultez [Microsoft - Liste de contrôle : Configuration d'IAS pour l'accès à distance et VPN](#) pour plus d'informations sur IAS.

Le principal avantage de la configuration de L2TP avec IPsec dans un scénario d'accès à distance est que les utilisateurs distants peuvent accéder à un VPN sur un réseau IP public sans passerelle

ou ligne dédiée. Cela permet un accès à distance depuis pratiquement n'importe quel endroit avec POTS. Un autre avantage est que la seule condition requise pour l'accès VPN est l'utilisation de Windows 2000 avec la mise en réseau à distance Microsoft (DUN). Aucun logiciel client supplémentaire, tel que Cisco VPN Client, n'est requis.

Ce document décrit également comment utiliser Cisco Adaptive Security Device Manager (ASDM) afin de configurer le dispositif de sécurité de la gamme PIX 500 pour L2TP sur IPsec.

Remarque : le [protocole L2TP \(Layer 2 Tunneling Protocol\) sur IPsec](#) est pris en charge par le logiciel pare-feu Cisco Secure PIX version 6.x et ultérieure.

Afin de configurer L2TP sur IPsec entre PIX 6.x et Windows 2000, référez-vous à [Configuration L2TP sur IPsec entre PIX Firewall et Windows 2000 PC à l'aide de certificats](#).

Afin de configurer L2TP sur IPsec à partir de clients Microsoft Windows 2000 et XP distants vers un site d'entreprise à l'aide d'une méthode chiffrée, référez-vous à [Configuration de L2TP sur IPsec à partir d'un client Windows 2000 ou XP vers un concentrateur Cisco VPN 3000 à l'aide de clés prépartagées](#).

Conditions préalables

Conditions requises

Avant l'établissement du tunnel sécurisé, la connectivité IP doit exister entre les homologues.

Assurez-vous que le port UDP 1701 n'est pas bloqué sur le chemin de la connexion.

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

Remarque : L'apppliance de sécurité n'établit pas de tunnel L2TP/IPsec avec Windows 2000 si le Client VPN Cisco 3.x ou le Client VPN Cisco 3000 2.5 est installé. Désactivez le service VPN Cisco pour Cisco VPN Client 3.x ou le service ANetIKE pour Cisco VPN 3000 Client 2.5 à partir du panneau Services de Windows 2000. Pour ce faire, choisissez **Démarrer > Programmes > Outils d'administration > Services**, redémarrez le service Agent de stratégie IPsec à partir du panneau Services et redémarrez l'ordinateur.

Components Used

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

- Dispositif de sécurité PIX 515E avec logiciel version 7.2(1) ou ultérieure
- Adaptive Security Device Manager 5.2(1) ou version ultérieure
- Microsoft Windows 2000 Server
- Microsoft Windows XP Professionnel avec SP2
- Serveur Windows 2003 avec IAS

Remarque : si vous mettez à niveau PIX 6.3 vers la version 7.x, assurez-vous que vous avez installé SP2 dans Windows XP (Client L2TP).

Remarque : Les informations du document sont également valides pour l'appliance de sécurité ASA.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Produits connexes

Cette configuration peut également être utilisée avec le dispositif de sécurité de la gamme Cisco ASA 5500 7.2(1) ou version ultérieure.

Conventions

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

Informations générales

Complétez ces étapes afin de configurer L2TP sur IPsec.

1. Configurez le mode de transport IPsec afin d'activer IPsec avec L2TP. Le client L2TP/IPsec de Windows 2000 utilise le mode de transport IPsec : seule la charge utile IP est chiffrée et les en-têtes IP d'origine restent intacts. Ce mode présente les avantages suivants : il ajoute seulement quelques octets à chaque paquet et permet aux périphériques du réseau public de voir la source et la destination finales du paquet. Par conséquent, pour que les clients L2TP/IPsec Windows 2000 se connectent à l'appliance de sécurité, vous devez configurer le mode de transport IPsec pour une transformation (voir l'étape 2 de la [configuration ASDM](#)). Avec cette fonctionnalité (transport), vous pouvez activer le traitement spécial (par exemple, QoS) sur le réseau intermédiaire en fonction des informations de l'en-tête IP. Cependant, l'en-tête de couche 4 est chiffré, ce qui limite l'examen du paquet. Malheureusement, la transmission de l'en-tête IP en texte clair, mode transport, permet à un attaquant d'effectuer une analyse du trafic.
2. Configurez L2TP avec un groupe VPDN (Virtual Private Dial Network).

La configuration de L2TP avec IPsec prend en charge les certificats qui utilisent les clés pré-partagées ou les méthodes de signature RSA, ainsi que l'utilisation de cartes de chiffrement dynamiques (par opposition aux cartes statiques). La clé pré-partagée est utilisée comme authentification pour établir le tunnel L2TP sur IPsec.

Configuration

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

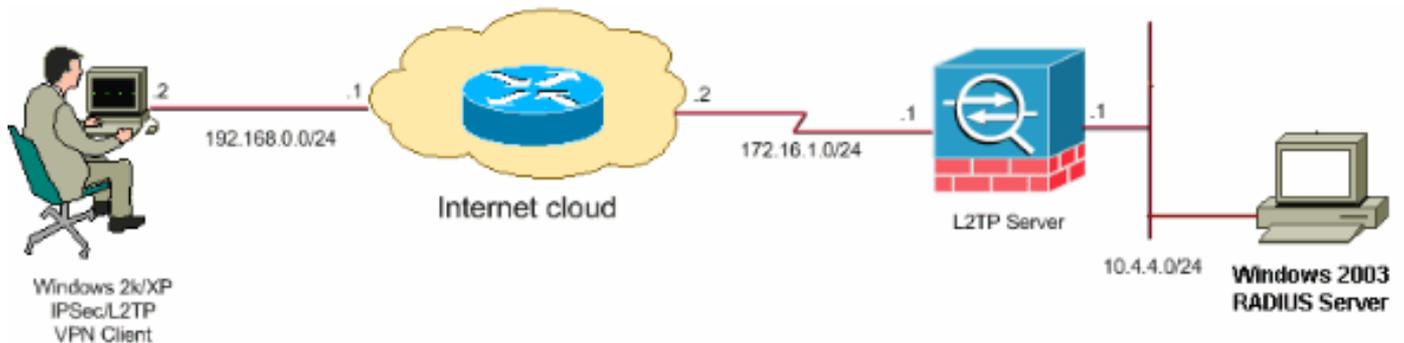
Remarque : Utilisez [l'outil de recherche de commandes](#) (clients [inscrits](#) seulement) pour en savoir plus sur les commandes figurant dans le présent document.

Remarque : les schémas d'adressage IP utilisés dans cette configuration ne sont pas routables

légalement sur Internet. Ce sont des adresses RFC 1918 qui ont été utilisés dans un environnement de laboratoire.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



Configurations

Ce document utilise les configurations suivantes :

- [Configuration du client L2TP/IPsec Windows](#)
- [Serveur L2TP dans la configuration PIX](#)
- [L2TP avec configuration ASDM](#)
- [Configuration de Microsoft Windows Serveur 2003 avec IAS](#)

Configuration du client L2TP/IPsec Windows

Complétez ces étapes afin de configurer L2TP sur IPsec sur Windows 2000. Pour Windows XP, ignorez les étapes 1 et 2 et commencez à l'étape 3 :

1. Ajoutez cette valeur de Registre à votre ordinateur 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 rompre la connexion car elle fait que la boîte XP négocie L2TP uniquement plutôt qu'une L2TP avec une connexion IPsec. Il est obligatoire d'ajouter une stratégie IPsec associée à cette clé de Registre. Si vous recevez une `erreur 800` lorsque vous essayez d'établir une connexion, supprimez la clé (Valeur : 1) afin que la connexion fonctionne. **Remarque :** Vous devez redémarrer l'ordinateur Windows 2000/2003 ou XP pour que les modifications prennent effet. Par défaut, le client Windows tente d'utiliser IPsec avec une autorité de certification. La configuration de cette clé de Registre empêche cela. Vous pouvez maintenant configurer une stratégie IPsec sur la station Windows pour qu'elle corresponde aux paramètres que vous voulez sur PIX/ASA. Référez-vous à [Configuration d'une connexion L2TP/IPSec à l'aide de l'authentification de clé pré-partagée \(Q240262\)](#) pour une

configuration étape par étape de la stratégie IPsec Windows. Référez-vous à [Configurer une clé prépartagée pour une utilisation avec des connexions de protocole de tunnellation de couche 2 dans Windows XP \(Q281555\)](#) pour plus d'informations.

3. Créez votre connexion.
4. Sous Connexions réseau et accès à distance, cliquez avec le bouton droit sur la connexion et sélectionnez **Propriétés**. Accédez à l'onglet Sécurité et cliquez sur **Avancé**. Sélectionnez les protocoles comme le montre cette

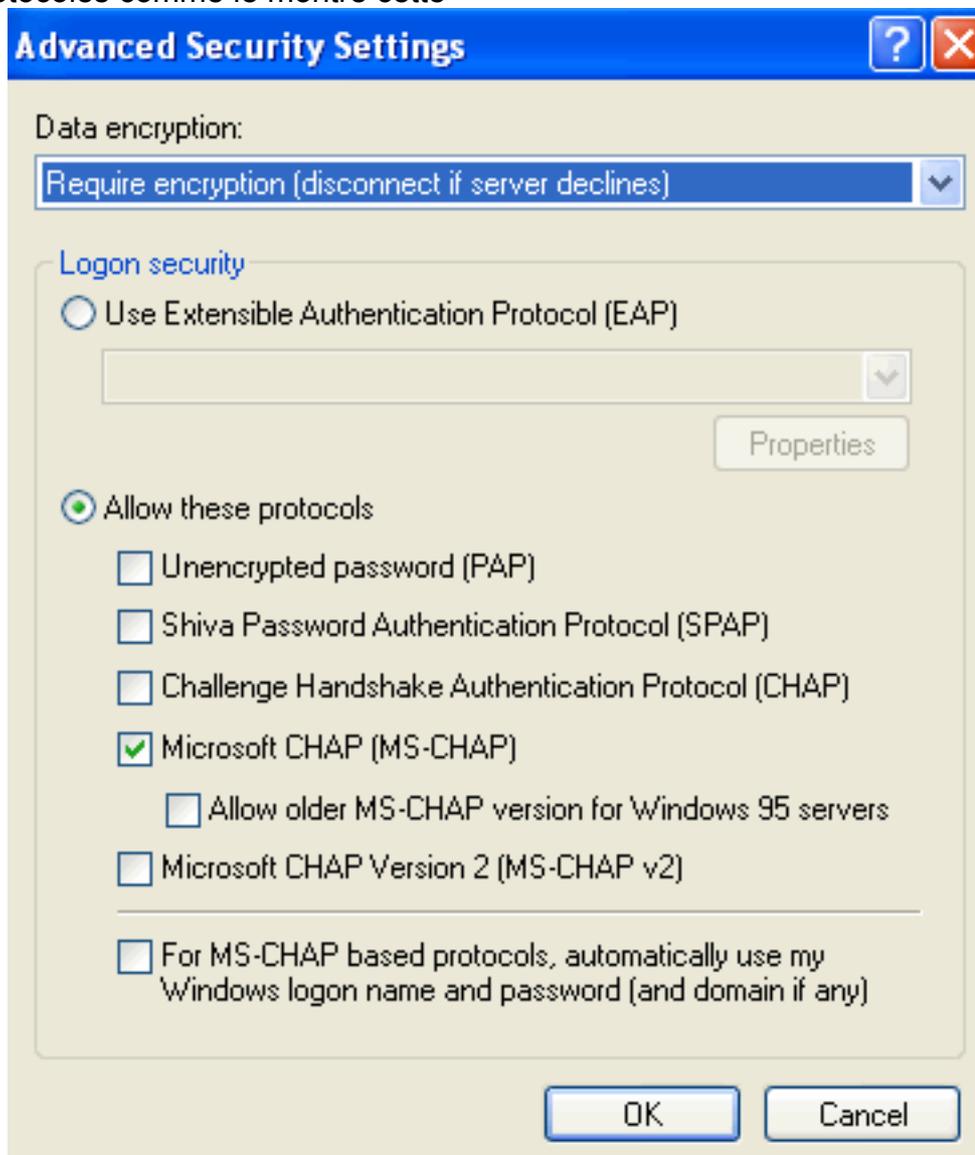
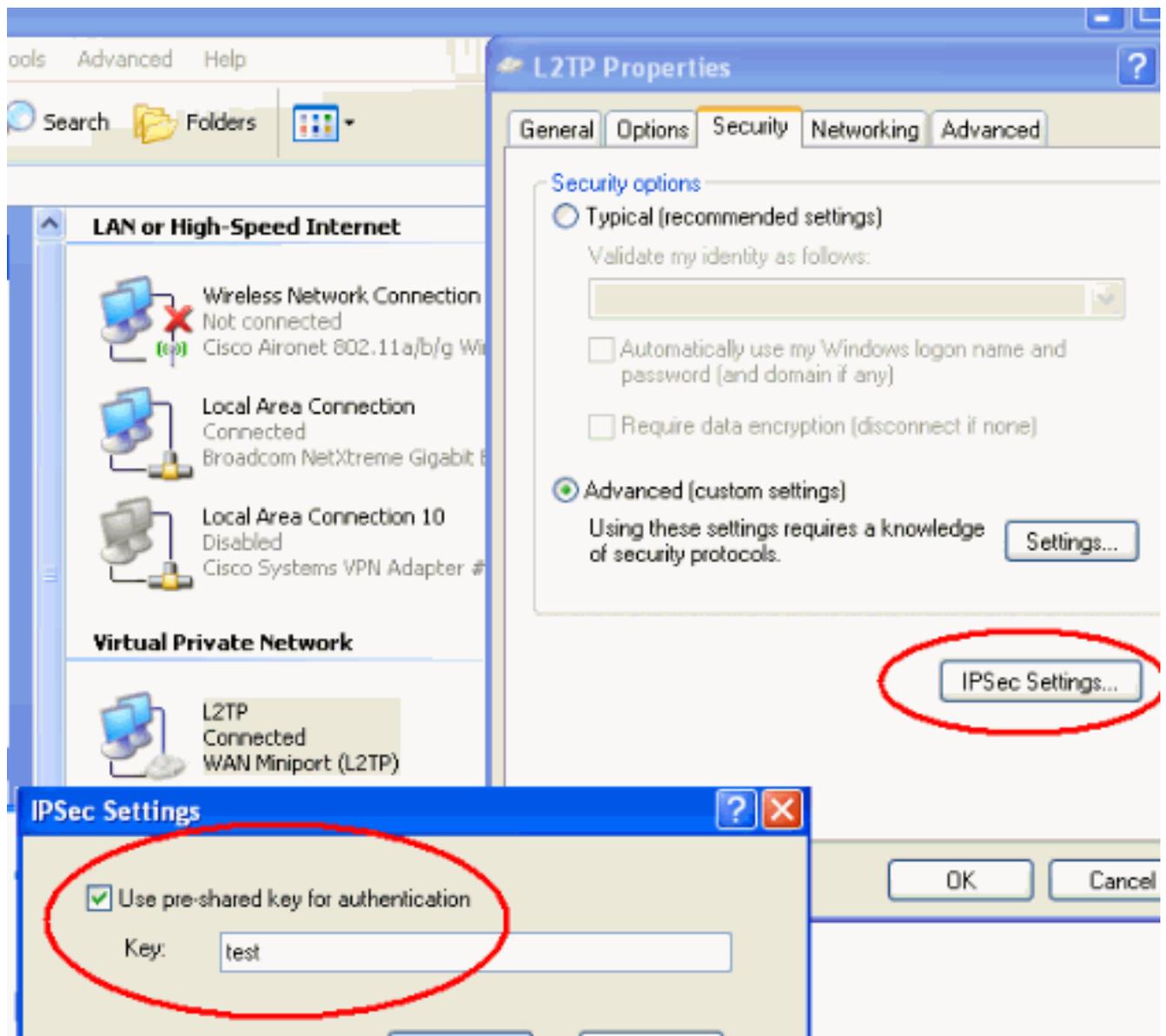


image.

5. **Note:** Cette étape s'applique uniquement à Windows XP. Cliquez sur **Paramètres IPsec**, cochez **Utiliser la clé pré-partagée pour l'authentification** et saisissez la clé pré-partagée afin de définir la clé pré-partagée. Dans cet exemple, 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 test password DLauiaX3178qgoB5c7iVNw== 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.
```

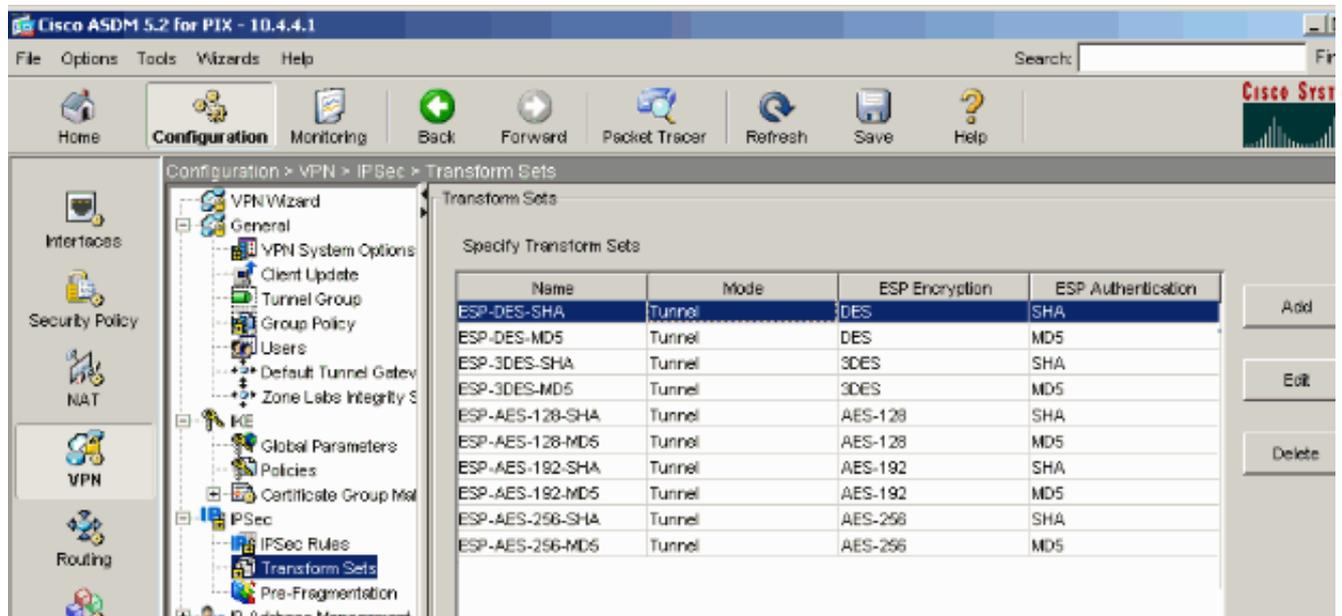
```
tunnel-group DefaultRAGroup ppp-attributes
no authentication chap
authentication ms-chap-v2
```

```
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:ele0730fa260244caa2e2784f632accd
: end
```

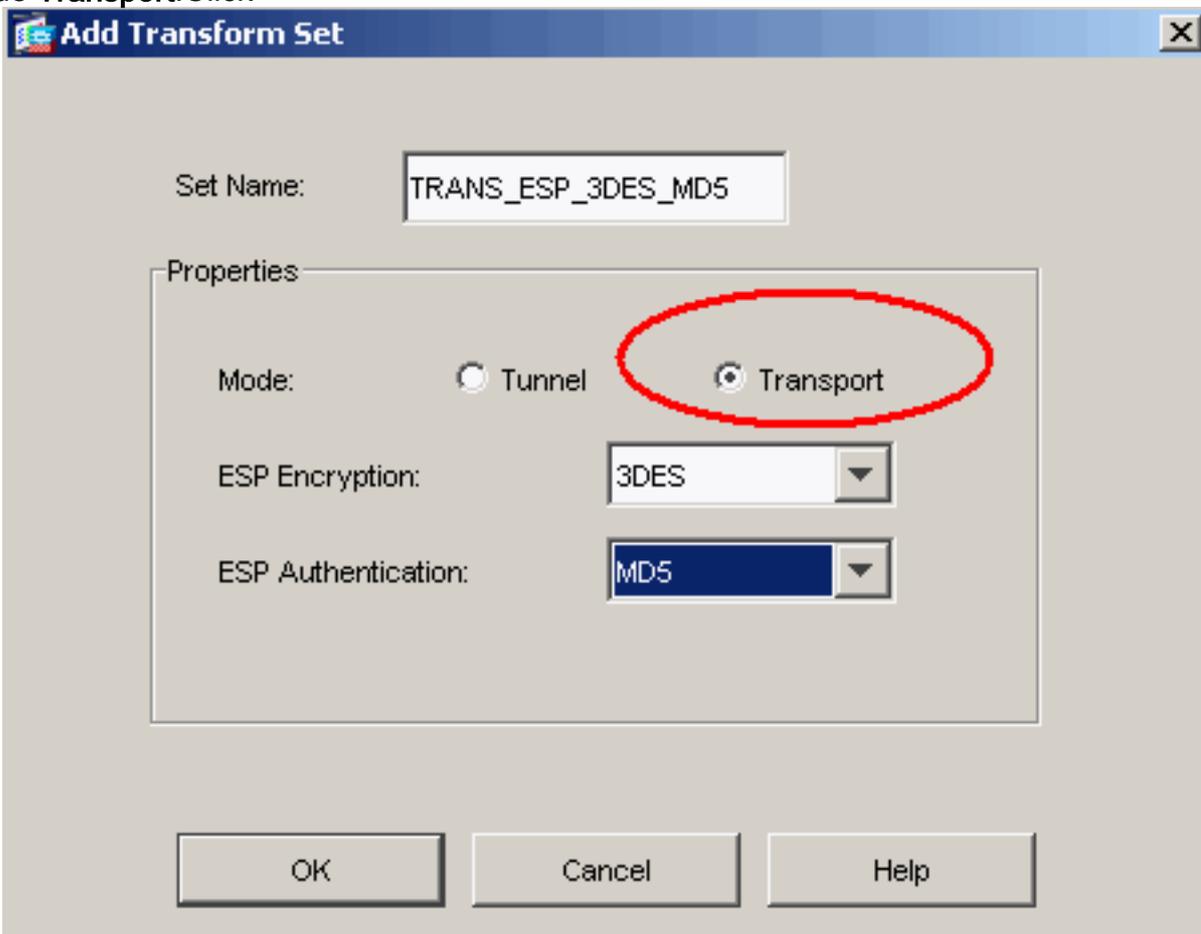
[L2TP avec configuration ASDM](#)

Complétez ces étapes afin de configurer l'appliance de sécurité pour accepter les connexions L2TP sur IPsec :

1. Ajoutez un jeu de transformation IPsec et spécifiez IPsec pour utiliser le mode transport plutôt que le mode tunnel. Pour ce faire, choisissez **Configuration > VPN > IPsec > Transform Sets** et cliquez sur **Add**. Le volet Jeux de transformation s'affiche.

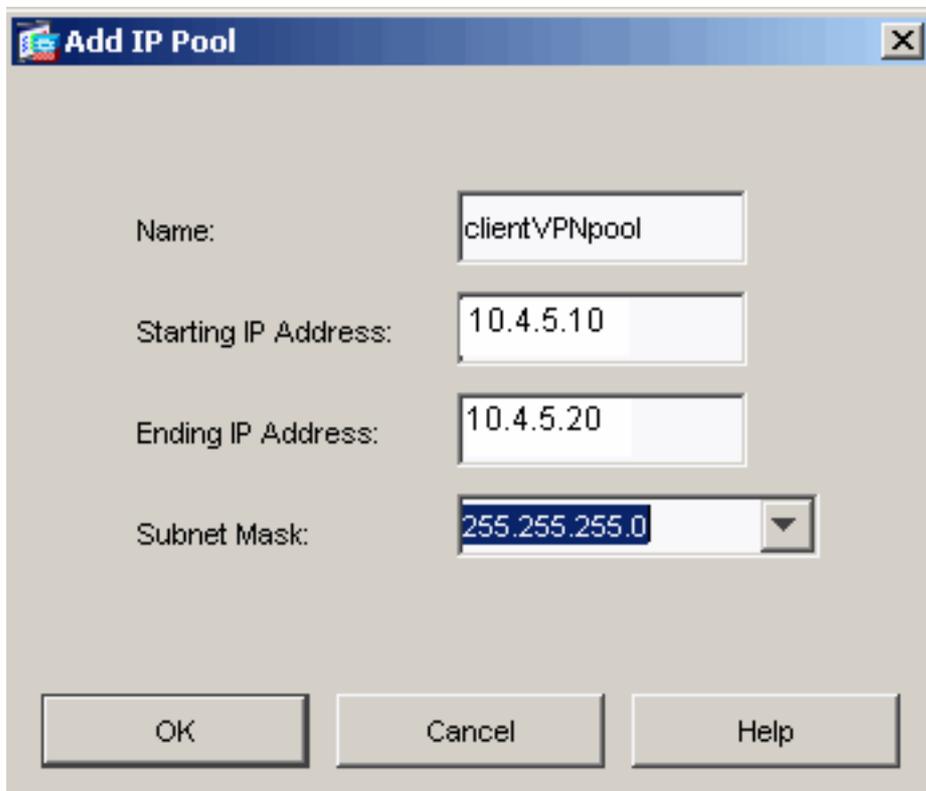


2. Complétez ces étapes afin d'ajouter un jeu de transformation :Entrez un nom pour le jeu de transformation.Choisissez les méthodes ESP Encryption et ESP Authentication.Choisissez le mode **Transport**.Click



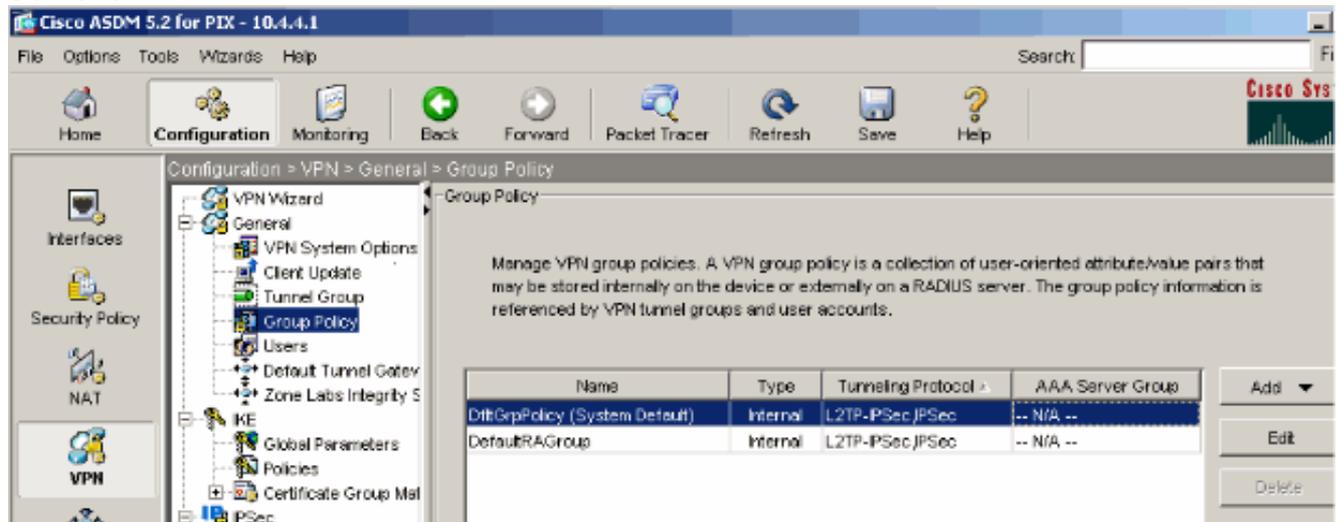
OK.

3. Complétez ces étapes afin de configurer une méthode d'attribution d'adresse. Cet exemple utilise des pools d'adresses IP.Choisissez **Configuration > VPN > IP Address Management > IP Pools**.Cliquez sur **Add**. La boîte de dialogue Add IP Pool apparaît.Saisissez le nom du nouveau pool d'adresses IP.Entrez les adresses IP de début et de fin.Entrez le masque de sous-réseau et cliquez sur

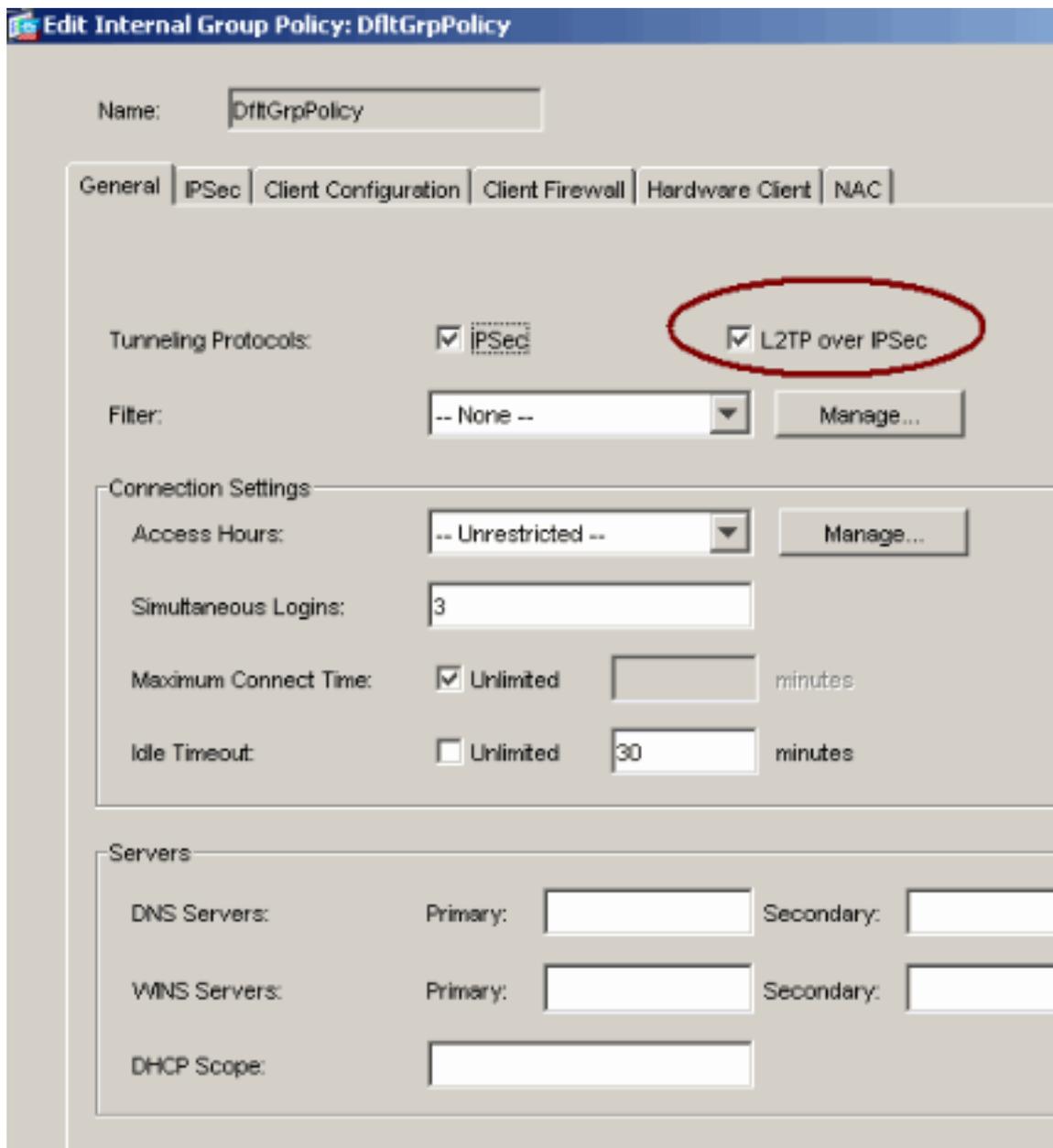


OK.

4. Choisissez **Configuration > VPN > General > Group Policy** afin de configurer L2TP sur IPsec comme protocole de tunnellation VPN valide pour la stratégie de groupe. Le volet Stratégie de groupe s'affiche.

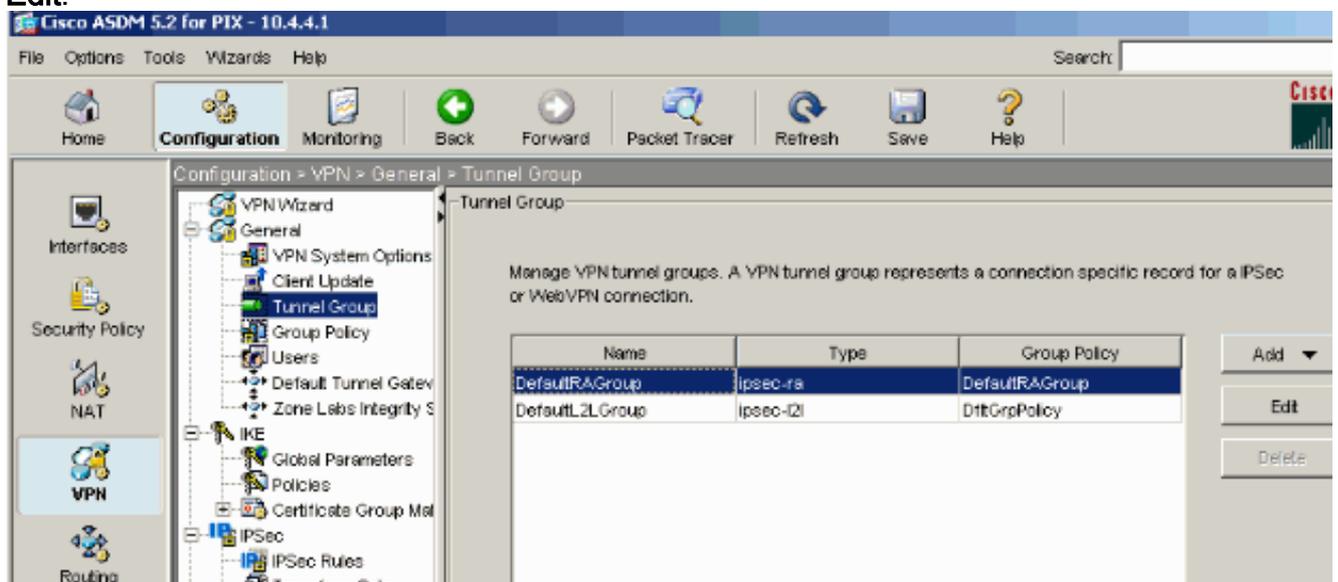


5. Sélectionnez une stratégie de groupe (DiffGrpPolicy) et cliquez sur **Modifier**. La boîte de dialogue Modifier la stratégie de groupe s'affiche. Vérifiez **L2TP sur IPsec** afin d'activer le protocole pour la stratégie de groupe, puis cliquez sur

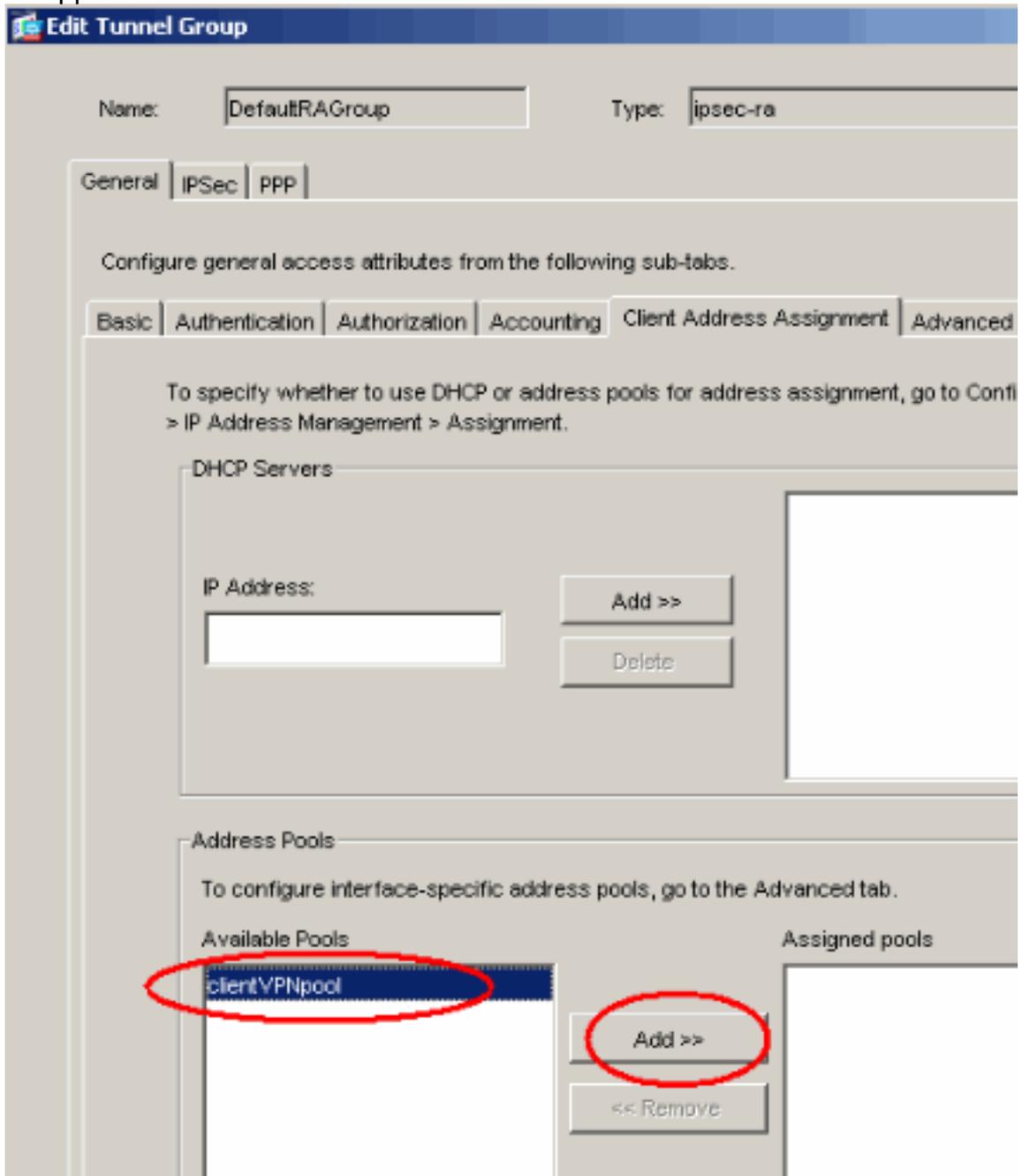


OK.

6. Complétez ces étapes afin d'affecter le pool d'adresses IP à un groupe de tunnels :Choisissez **Configuration > VPN > General > Tunnel Group**.Une fois le volet Groupe de tunnels affiché, sélectionnez un groupe de tunnels (DefaultRAGroup) dans le tableau.Cliquez sur **Edit**.

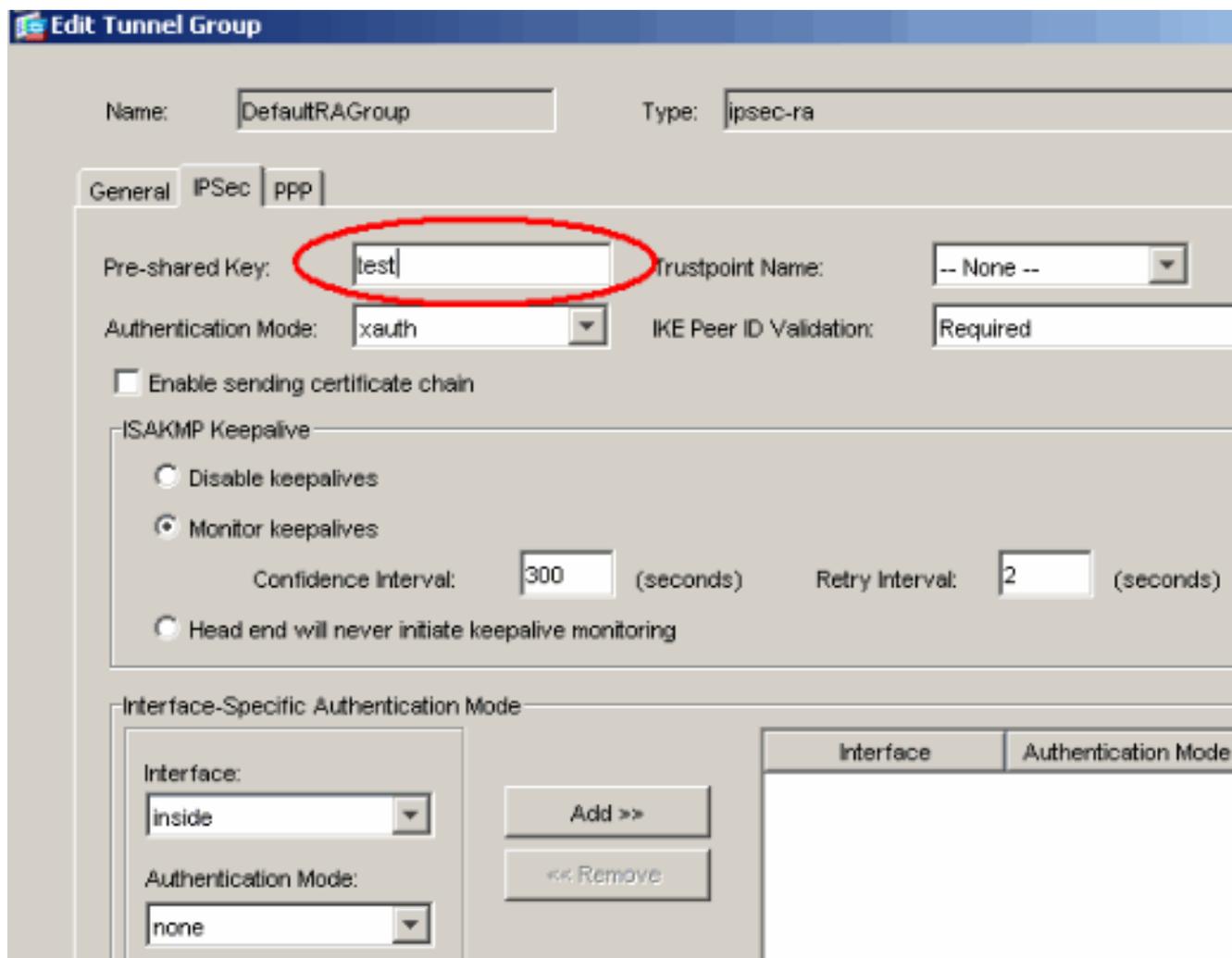


7. Effectuez ces étapes lorsque la fenêtre Modifier le groupe de tunnels apparaît : Dans l'onglet Général, accédez à l'onglet Attribution d'adresse client. Dans la zone Pools d'adresses, sélectionnez un pool d'adresses à attribuer au groupe de tunnels. Cliquez sur **Add**. Le pool d'adresses apparaît dans la zone Pools

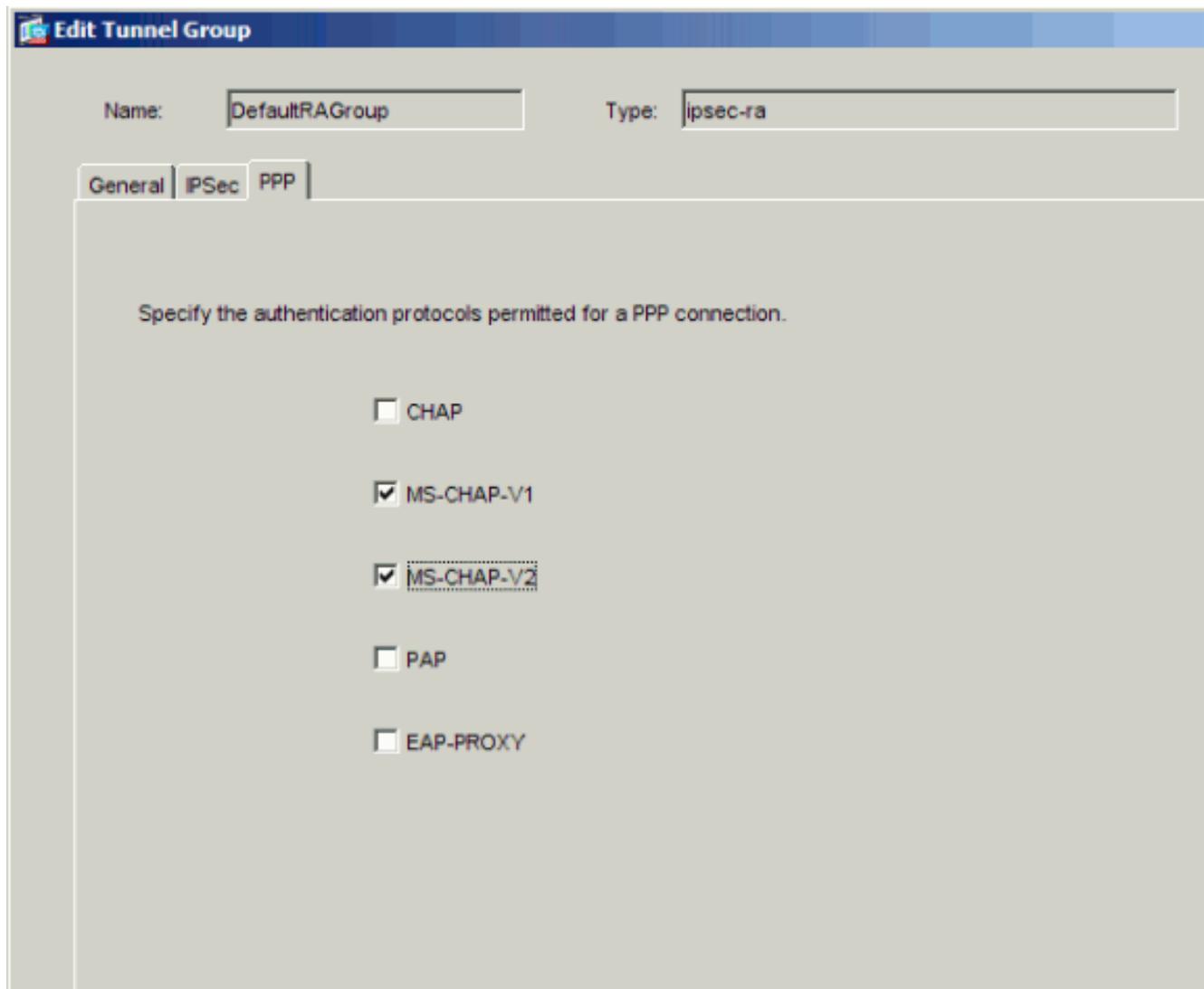


affectés.

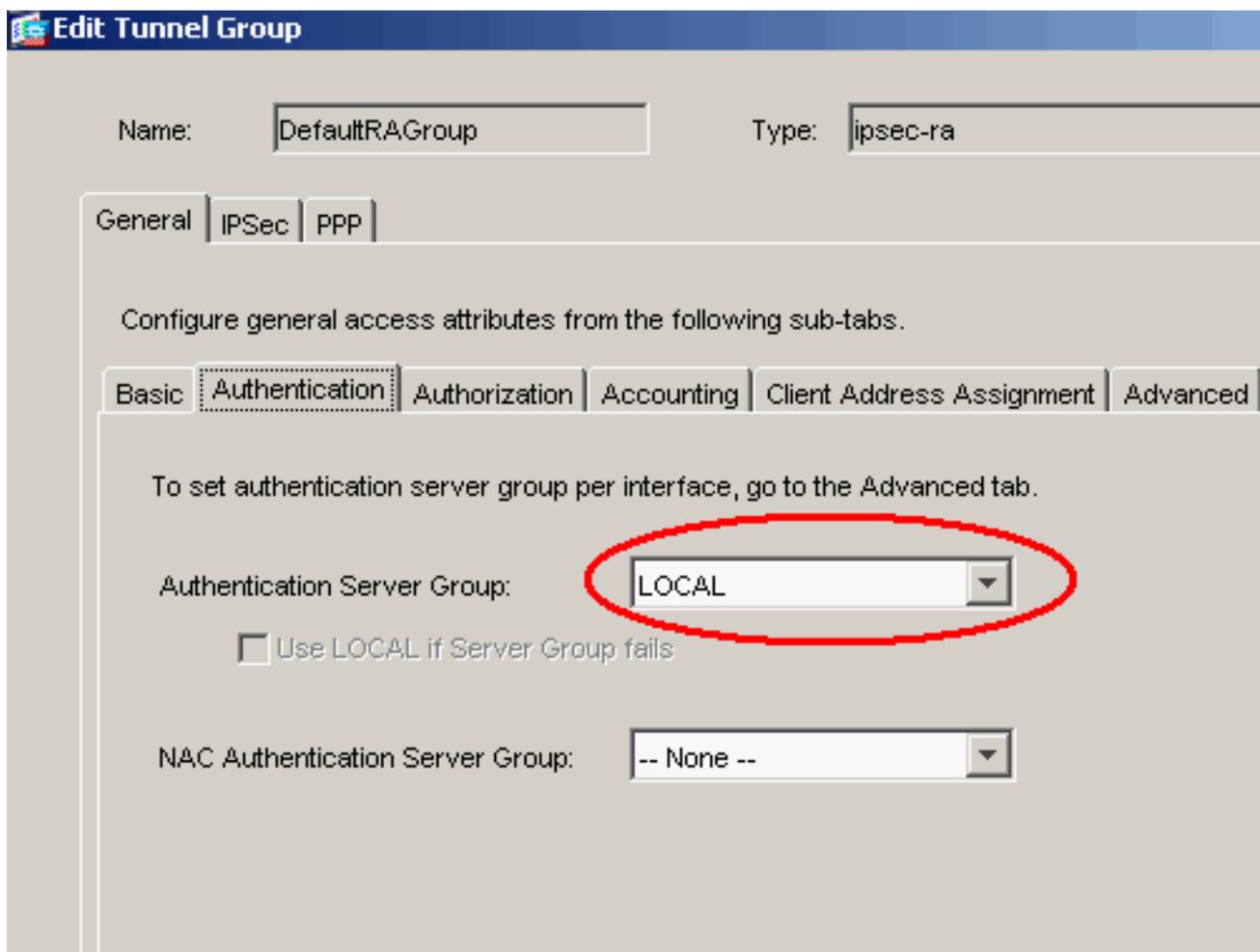
8. Afin de définir la clé pré-partagée, accédez à l'onglet IPSec, saisissez votre **clé pré-partagée**, puis cliquez sur **OK**.



9. L2TP sur IPsec utilise des protocoles d'authentification PPP. Spécifiez les protocoles autorisés pour les connexions PPP dans l'onglet PPP du groupe de tunnels. Sélectionnez le protocole **MS-CHAP-V1** pour l'authentification.



10. Spécifiez une méthode pour authentifier les utilisateurs qui tentent des connexions L2TP sur IPsec. Vous pouvez configurer l'appliance de sécurité pour qu'elle utilise un serveur d'authentification ou sa propre base de données locale. Pour ce faire, accédez à l'onglet Authentification du groupe de tunnels. Par défaut, l'appliance de sécurité utilise sa base de données locale. La liste déroulante Authentication Server Group affiche LOCAL. Pour utiliser un serveur d'authentification, sélectionnez-en un dans la liste. **Remarque** : l'appliance de sécurité prend uniquement en charge les authentifications PPP PAP et Microsoft CHAP versions 1 et 2 sur la base de données locale. Les protocoles EAP et CHAP sont exécutés par des serveurs d'authentification par proxy. Par conséquent, si un utilisateur distant appartient à un groupe de tunnels configuré avec EAP ou CHAP et que l'appliance de sécurité est configurée pour utiliser la base de données locale, cet utilisateur ne peut pas se connecter.



Remarque : Choisissez **Configuration > VPN > General > Tunnel Group** afin de revenir à la configuration du groupe de tunnels afin que vous puissiez lier la stratégie de groupe au groupe de tunnels et activer la commutation de groupe de tunnels (facultatif). Lorsque le volet Groupe de tunnels apparaît, sélectionnez le groupe de tunnels et cliquez sur **Modifier**.

Remarque : La commutation de groupe de tunnels permet à l'appliance de sécurité d'associer différents utilisateurs qui établissent des connexions L2TP sur IPsec à différents groupes de tunnels. Puisque chaque groupe de tunnels a son propre groupe de serveurs AAA et ses propres pools d'adresses IP, les utilisateurs peuvent être authentifiés par des méthodes spécifiques à leur groupe de tunnels. Avec cette fonctionnalité, au lieu d'envoyer uniquement un nom d'utilisateur, l'utilisateur envoie un nom d'utilisateur et un nom de groupe au format `username@group_name`, où "@" représente un délimiteur que vous pouvez configurer, et le nom de groupe est le nom d'un groupe de tunnels configuré sur l'appliance de sécurité.

Remarque : La commutation de groupe de tunnels est activée par le traitement du groupe de bandes, ce qui permet à l'appliance de sécurité de sélectionner le groupe de tunnels pour les connexions utilisateur en obtenant le nom du groupe à partir du nom d'utilisateur présenté par le client VPN. L'appliance de sécurité envoie ensuite uniquement la partie utilisateur du nom d'utilisateur pour l'autorisation et l'authentification. Sinon (si cette option est désactivée), l'appliance de sécurité envoie le nom d'utilisateur entier, y compris le domaine. Afin d'activer la commutation de groupe de tunnels, cochez la case **Dégagez le domaine du nom d'utilisateur avant de le transmettre au serveur AAA**, et cochez la case **Dégagez le groupe du nom d'utilisateur avant de le transmettre au serveur AAA**. Cliquez ensuite sur **OK**.

11. Complétez ces étapes afin de créer un utilisateur dans la base de données locale : Choisissez **Configuration > Properties > Device Administration > User Accounts**. Cliquez

sur **Add**. Si l'utilisateur est un client L2TP qui utilise Microsoft CHAP version 1 ou 2 et que l'appliance de sécurité est configurée pour s'authentifier sur la base de données locale, vous devez vérifier **User Authenticated** à l'aide de **MSCHAP** afin d'activer le MSCHAP. Cliquez sur **OK**.

Add User Account

Identity | VPN Policy

Username: test

Password: ****

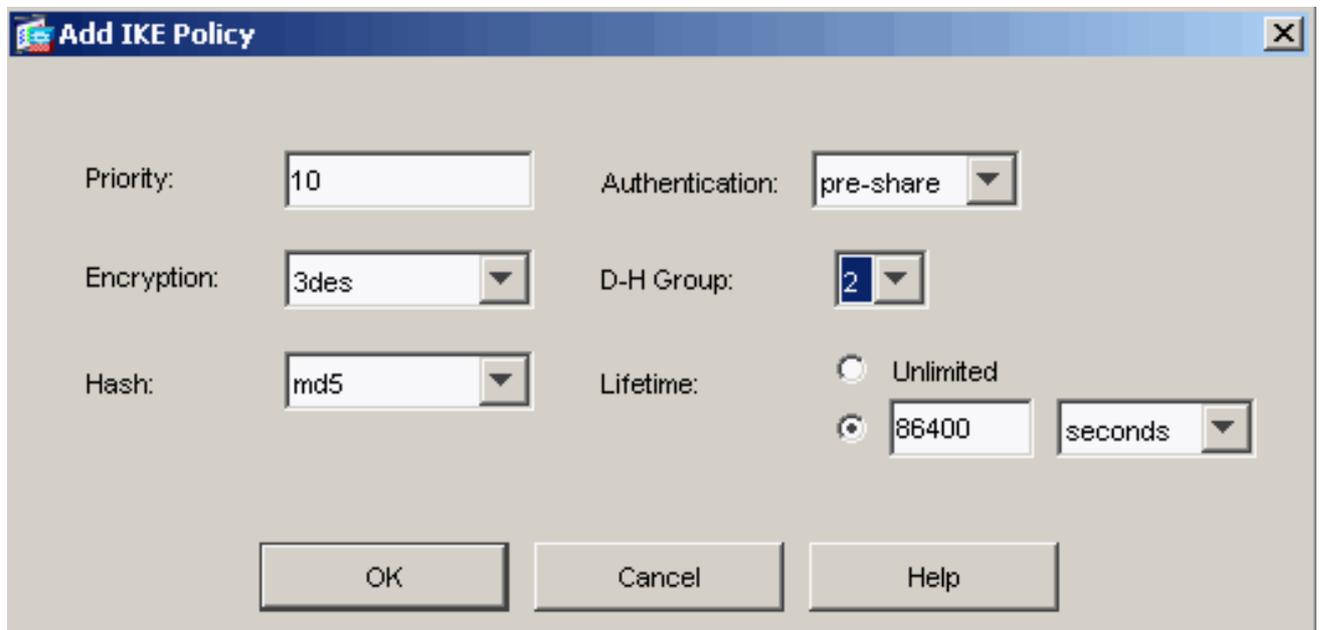
Confirm Password: ****

User authenticated using MSCHAP

Privilege level is used with command authorization.

Privilege Level: 2

12. Choisissez **Configuration > VPN > IKE > Politiques** et cliquez sur **Add** afin de créer une stratégie IKE pour la phase I. Cliquez sur **OK** pour continuer.



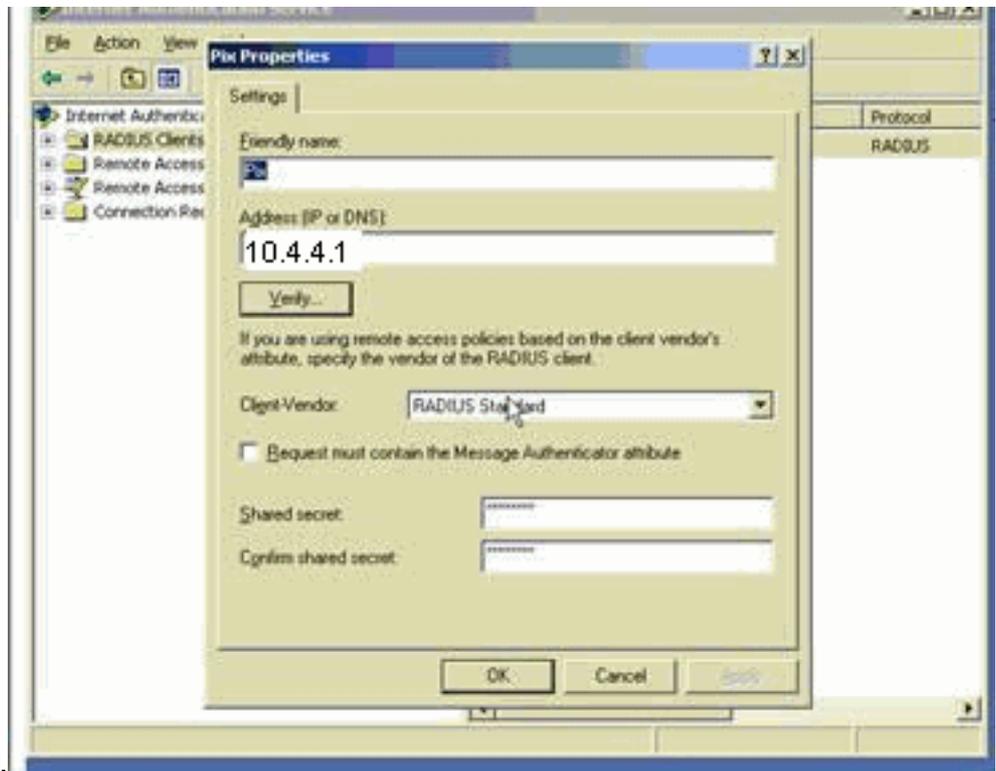
13. (Facultatif) Si vous prévoyez que plusieurs clients L2TP derrière un périphérique NAT tentent des connexions L2TP sur IPsec vers l'appliance de sécurité, vous devez activer la traversée NAT afin que les paquets ESP puissent traverser un ou plusieurs périphériques NAT. Pour ce faire, exécutez ces étapes: Choisissez **Configuration > VPN > IKE > Global Parameters**. Assurez-vous que **ISAKMP** est activé sur une interface. Cochez **Enable IPsec over NAT-T**. Cliquez OK.

[Configuration de Microsoft Windows Serveur 2003 avec IAS](#)

Complétez ces étapes afin de configurer le serveur Microsoft Windows 2003 avec IAS.

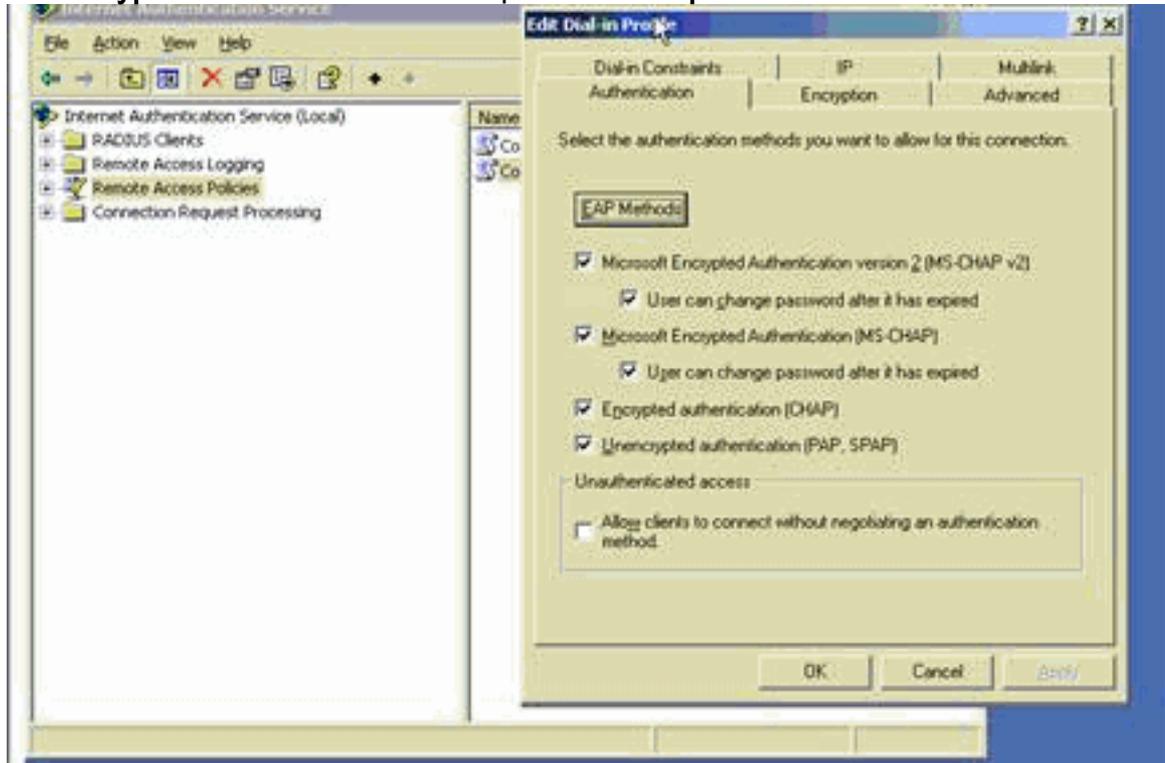
Remarque : Ces étapes supposent que IAS est déjà installé sur l'ordinateur local. Sinon, ajoutez ce composant via **Control Panel > Add/Remove Programs**.

1. Choisissez **Outils d'administration > Service d'authentification Internet** et cliquez avec le bouton droit sur **Client RADIUS** afin d'ajouter un nouveau client RADIUS. Après avoir tapé les informations sur le client, cliquez sur **OK**. Cet exemple montre un client nommé « Pix » avec l'adresse IP 10.4.4.1. Client-Vendor est défini sur **RADIUS Standard**, et le secret



partagé est radiuskey.

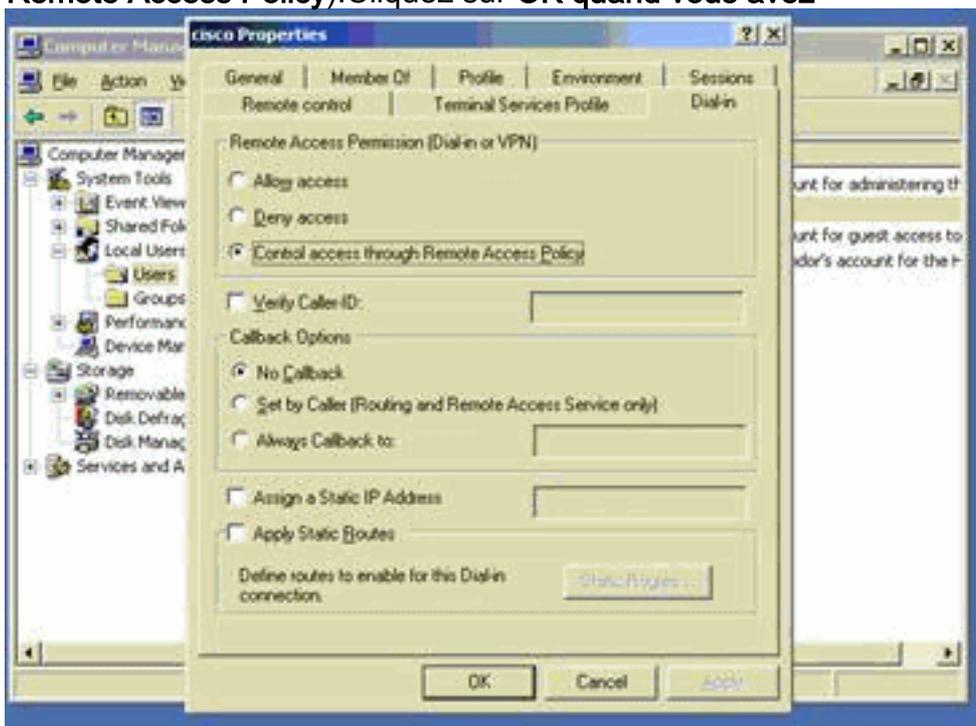
2. Choisissez **Remote Access Policies**, cliquez avec le bouton droit sur **Connexions à d'autres serveurs d'accès**, puis sélectionnez **Propriétés**.
3. Assurez-vous que l'option **Grant Remote Access Permissions** est sélectionnée.
4. Cliquez sur **Edit Profile** et vérifiez ces paramètres : Dans l'onglet **Authentification**, cochez la case **Authentification non chiffrée (PAP, SPAP)**. Dans l'onglet **Encryption**, assurez-vous que l'option **No Encryption** est sélectionnée. Cliquez sur **OK** quand vous avez



terminé.

5. Choisissez **Outils d'administration > Gestion de l'ordinateur > Outils système > Utilisateurs et groupes locaux**, cliquez avec le bouton droit sur **Utilisateurs** et sélectionnez **Nouveaux utilisateurs** afin d'ajouter un utilisateur au 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 sur IPsec à l'aide d'Active Directory](#)

Utilisez cette configuration sur l'ASA afin de permettre l'authentification de la connexion L2tp à partir d'Active Directory :

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

En outre, sur le client L2tp, accédez à **Paramètres de sécurité avancés (Personnalisés)** et choisissez uniquement l'option **Mot de passe non chiffré (PAP)**.

[Vérification](#)

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 IKE (SA) actuelles sur un homologue.

```
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
```

- **show vpn-sessiondb** - Inclut des filtres de protocole que vous pouvez utiliser afin d'afficher des informations détaillées sur les connexions L2TP sur IPsec. La commande full du mode de configuration globale est **show vpn-sessiondb remote filter protocol l2tpOverIpsec**. Cet exemple montre les détails d'une connexion L2TP sur IPsec unique :

```
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

Dépannage

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'[outil Interpréteur de sortie](#) (clients [enregistrés](#) uniquement) , qui vous permet d'afficher une analyse de la sortie de la commande **show**.

Remarque : reportez-vous à [Informations importantes sur les commandes de débogage](#) et [Dépannage de la sécurité IP - Compréhension et utilisation des 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

Pare-feu PIX

PIX#**debug crypto isakmp 7**

```
pixfirewall# Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, IKE_DECODE RECEIVED Message (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 VID
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 payload
Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, constructing xauth V6 VID payload
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 Vendor 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 DefaultRAGroup
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, Generating 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, processing ID payload
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, processing hash payload
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, Computing hash for ISAKMP
Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, Connection landed on tunnel_group DefaultRAGroup
Jan 02 18:26:44 [IKEv1]: Group = DefaultRAGroup, IP = 192.168.0.2, Freeing previously allocated memory for authorization-dn-attributes
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, constructing ID payload
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, constructing hash payload
```

Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, Computing hash for ISAKMP
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, constructing 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 does not support keep-alives (type = None)
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, Starting P1 rekey timer: 21600 seconds.
Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, IKE_DECODE RECEIVED Message (msgid=e1b84b0) 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, processing hash payload
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, processing SA payload
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, processing nonce payload
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, processing ID payload
Jan 02 18:26:44 [IKEv1]: Group = DefaultRAGroup, IP = 192.168.0.2, Received remote 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, processing ID payload
Jan 02 18:26:44 [IKEv1]: Group = DefaultRAGroup, IP = 192.168.0.2, Received local 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 session 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 Peer configured for crypto map: outside_dyn_map
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, processing IPsec SA payload
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, IPsec SA 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: requesting 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 constructing quick mode**

Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, constructing blank hash payload
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, constructing IPsec SA payload
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, constructing IPsec nonce payload
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, constructing proxy ID
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, Transmitting 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, constructing qm hash payload
Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, IKE_DECODE SENDING Message (msgid=elb84b0) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0) total length : 144
Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, IKE_DECODE RECEIVED Message (msgid=elb84b0) with payloads : HDR + HASH (8) + NONE (0) total length : 48
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, processing 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, Generating Quick Mode Key!
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, Generating Quick Mode Key!
Jan 02 18:26:44 [IKEv1]: Group = DefaultRAGroup, IP = 192.168.0.2, Security negotiation 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, Starting P2 rekey timer: 3059 seconds.

!--- Phase 2 completes successfully. Jan 02 18:26:44 [IKEv1]: Group = DefaultRAGroup, IP = 192.168.0.2, PHASE 2 COMPLETED (msgid=0elb84b0) Jan 02 18:26:44 [IKEv1]: IKEQM_Active() Add L2TP classification rules: ip <192.168.0.2> 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 : 0x01BF8CF80
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
```

Dépannage à l'aide d'ASDM

Vous pouvez utiliser ASDM afin d'activer la journalisation et d'afficher les journaux.

1. Choisissez **Configuration > Properties > Logging > Logging Setup**, sélectionnez **Enable Logging** et cliquez sur **Apply** afin d'activer la journalisation.
2. Choisissez **Monitoring > Logging > Log Buffer > On Logging Level**, sélectionnez **Logging Buffer**, puis cliquez sur **View** afin d'afficher les journaux.

Problème : Déconnexions fréquentes

Délai d'inactivité/de session

Si le délai d'inactivité est défini sur 30 minutes (par défaut), cela signifie qu'il abandonne le tunnel après qu'aucun trafic ne le traverse pendant 30 minutes. Le client VPN est déconnecté après 30 minutes, quel que soit le paramètre du délai d'inactivité, 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
```

Dépannage de Windows Vista

Utilisateur simultané

Windows Vista L2TP/IPsec a introduit quelques modifications architecturales qui interdisaient à plusieurs utilisateurs simultanés d'être connectés à un PIX/ASA de tête de réseau. Ce comportement ne se produit pas sous Windows 2K/XP. Cisco a mis en oeuvre une solution de contournement pour cette modification à partir de la version 7.2(3) et ultérieure.

PC Vista non connecté

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

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](#)
- [Assistance produit du logiciel Cisco PIX Firewall](#)
- [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](#)