Pare-feu Cisco Secure PIX Firewall 6.x et client VPN Cisco 3.5 pour Windows avec authentification RADIUS du service IAS de Microsoft Windows 2000 et 2003

Contenu

Introduction
Conditions préalables
Conditions requises
Components Used
Conventions
Configuration
Diagramme du réseau
Configurations
Vérification
Dépannage
Dépannage des commandes
Exemple de sortie de débogage
Informations connexes

Introduction

Cet exemple de configuration montre comment configurer Cisco VPN Client version 3.5 pour Windows et Cisco Secure PIX Firewall pour une utilisation avec Microsoft Windows 2000 et 2003 Internet Authentication Service (IAS) RADIUS Server. Consultez Microsoft - Liste de contrôle : Configuration d'IAS pour l'accès à distance et VPN pour plus d'informations sur IAS.

Référez-vous à Exemple de configuration d'authentification PIX/ASA 7.x et Cisco VPN Client 4.x pour Windows avec Microsoft Windows 2003 IAS RADIUS afin d'en savoir plus sur le même paysage dans PIX/ASA 7.0 avec Cisco VPN Client 4.x.

Conditions préalables

Conditions requises

Assurez-vous que vous répondez à ces exigences avant d'essayer cette configuration :

- Le logiciel Cisco Secure PIX Firewall version 6.0 prend en charge les connexions VPN à partir du client VPN Cisco 3.5 pour Windows.

- Cet exemple de configuration suppose que le PIX fonctionne déjà avec la statique, les conduits ou les listes d'accès appropriés. Le document actuel n'a pas l'intention d'illustrer ces concepts de base, mais de montrer la connectivité au PIX à partir d'un client VPN Cisco.

Components Used

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

- Logiciel pare-feu PIX version 6.1.1**Note :** Ceci a été testé sur le logiciel PIX version 6.1.1, mais devrait fonctionner sur toutes les versions 6.x.
- Client VPN Cisco version 3.5 pour Windows
- Windows 2000 et 2003 Server avec IAS

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.

Conventions

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

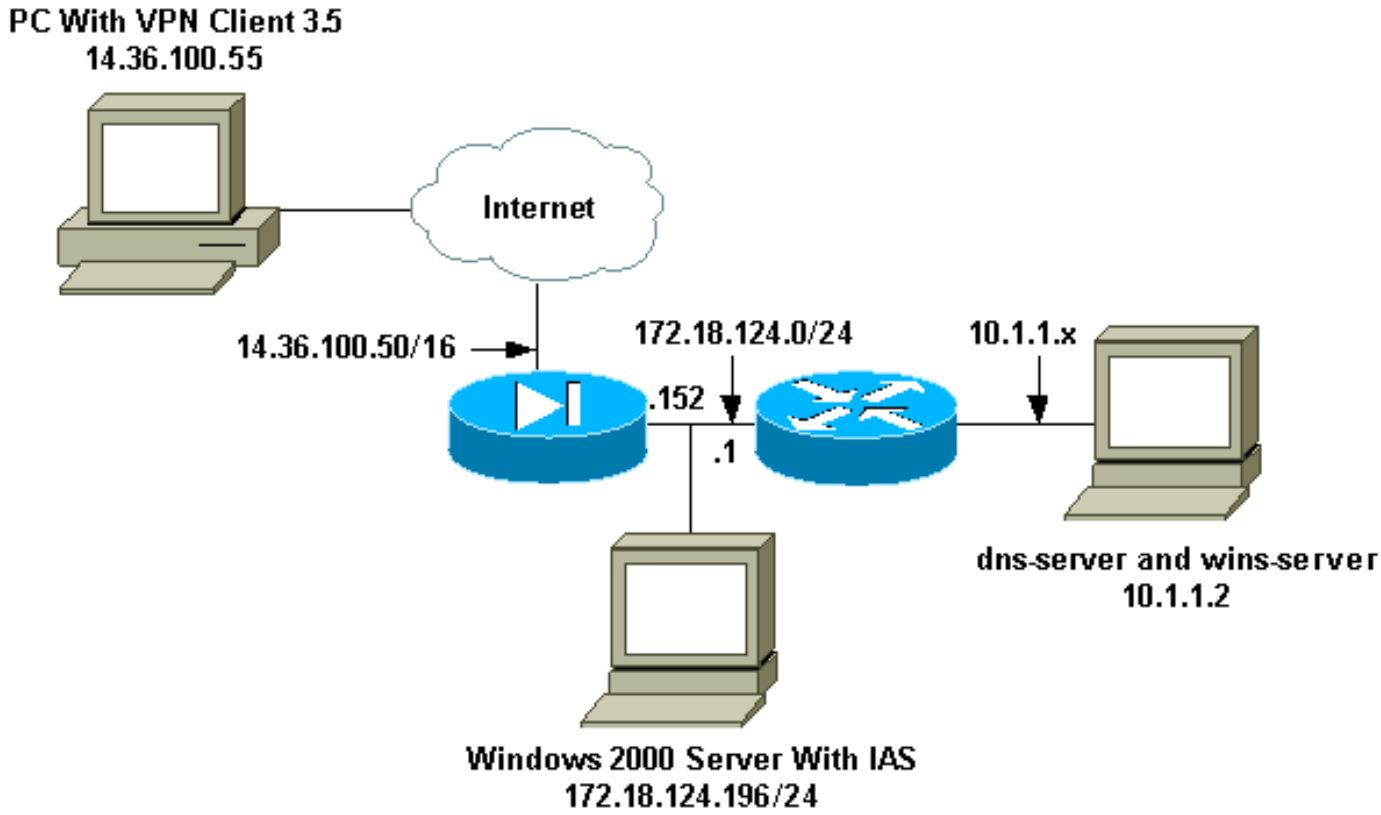
Configuration

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

Remarque : utilisez l'outil de recherche de commandes (clients enregistrés uniquement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



Configurations

Ce document utilise les configurations suivantes.

- Pare-feu PIX
- Client VPN Cisco 3.5 pour Windows
- Microsoft Windows 2000 Server avec IAS
- Microsoft Windows 2003 Server avec IAS

Pare-feu PIX

Pare-feu PIX

```
pixfirewall(config)#write terminal
Building configuration...
: Saved
:
PIX Version 6.1(1)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname pixfirewall
fixup protocol ftp 21
fixup protocol http 80
fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
fixup protocol skinny 2000
```

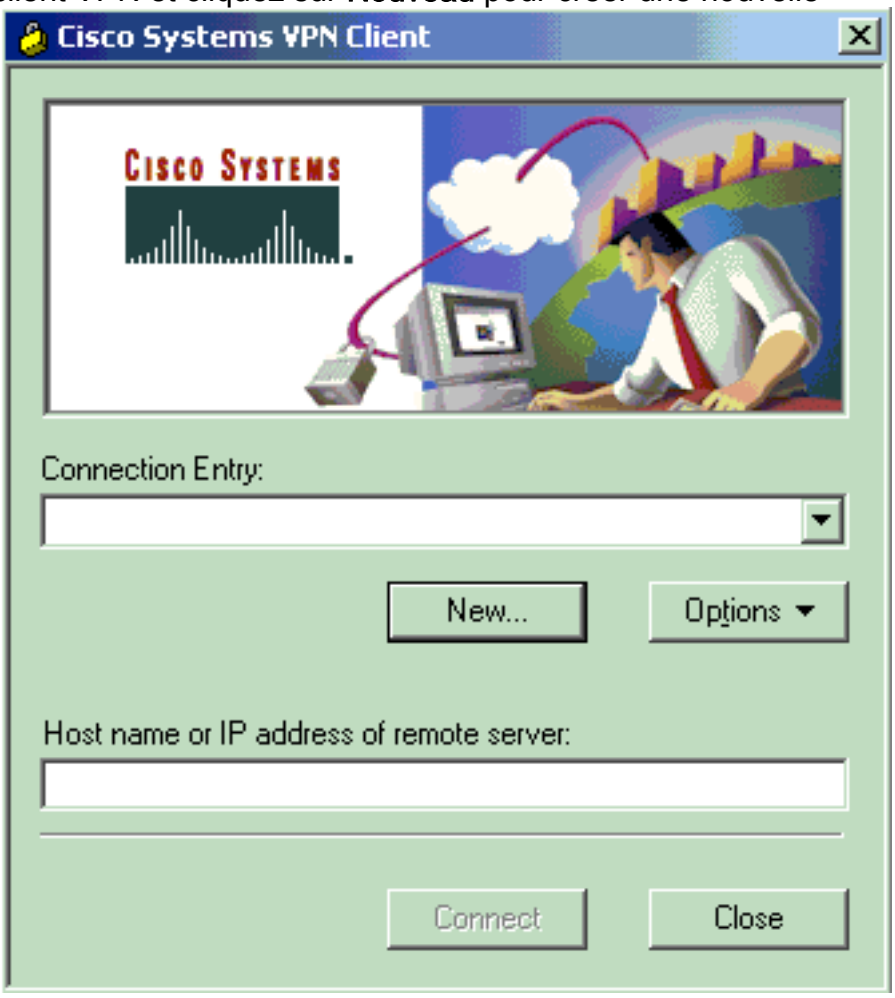
```
names
!--- Issue the access-list command to avoid !--- Network
Address Translation (NAT) on the IPsec packets.

access-list 101 permit ip 10.1.1.0 255.255.255.0
10.1.2.0
  255.255.255.0
pager lines 24
interface ethernet0 auto
interface ethernet1 auto
mtu outside 1500
mtu inside 1500
ip address outside 14.36.100.50 255.255.0.0
ip address inside 172.18.124.152 255.255.255.0
ip audit info action alarm
ip audit attack action alarm
ip local pool ippool 10.1.2.1-10.1.2.254
pdm history enable
arp timeout 14400
global (outside) 1 14.36.100.51
!--- Binding access list 101 to the NAT statement to
avoid !--- NAT on the IPsec packets. nat (inside) 0
access-list 101
Nat (inside) 1 0.0.0.0 0.0.0.0 0 0
route outside 0.0.0.0 0.0.0.0 14.36.1.1 1
route inside 10.1.1.0 255.255.255.0 172.18.124.1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00
   rpc 0:10:00 h323 0:05:00 sip 0:30:00 sip_media
0:02:00
timeout uauth 0:05:00 absolute
!--- Enable access to the RADIUS protocol.
aaa-server RADIUS protocol radius
!--- Associate the partnerauth protocol to RADIUS. aaa-
server partnerauth protocol radius
aaa-server partnerauth (inside) host 172.18.124.196
cisco123
   timeout 5
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
!--- Tell PIX to implicitly permit IPsec traffic. sysopt
connection permit-ipsec
no sysopt route dnat
!--- Configure a transform set that defines how the
traffic is protected. crypto ipsec transform-set myset
esp-des esp-md5-hmac
!--- Create a dynamic crypto map and specify which !---
transform sets are allowed for this dynamic crypto map
entry. crypto dynamic-map dynmap 10 set transform-set
myset
!--- Add the dynamic crypto map set into a static crypto
map set. crypto map mymap 10 ipsec-isakmp dynamic dynmap
!--- Enable the PIX to launch the Xauth application on
the VPN Client. crypto map mymap client authentication
partnerauth
!--- Apply the crypto map to the outside interface.
crypto map mymap interface outside
!--- IKE Policy Configuration. isakmp enable outside
isakmp identity address
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption des
```

```
isakmp policy 10 hash md5
isakmp policy 10 group 2
isakmp policy 10 lifetime 86400
!--- IPsec group configuration for VPN Client. vpngroup
vpn3000 address-pool ippool
vpngroup vpn3000 dns-server 10.1.1.2
vpngroup vpn3000 wins-server 10.1.1.2
vpngroup vpn3000 default-domain cisco.com
vpngroup vpn3000 idle-time 1800
vpngroup vpn3000 password ********
telnet timeout 5
ssh timeout 5
terminal width 80
Cryptochecksum:3f9e31533911b8a6bb5c0f06900c2dbc
: end
[OK]
pixfirewall(config)#
```

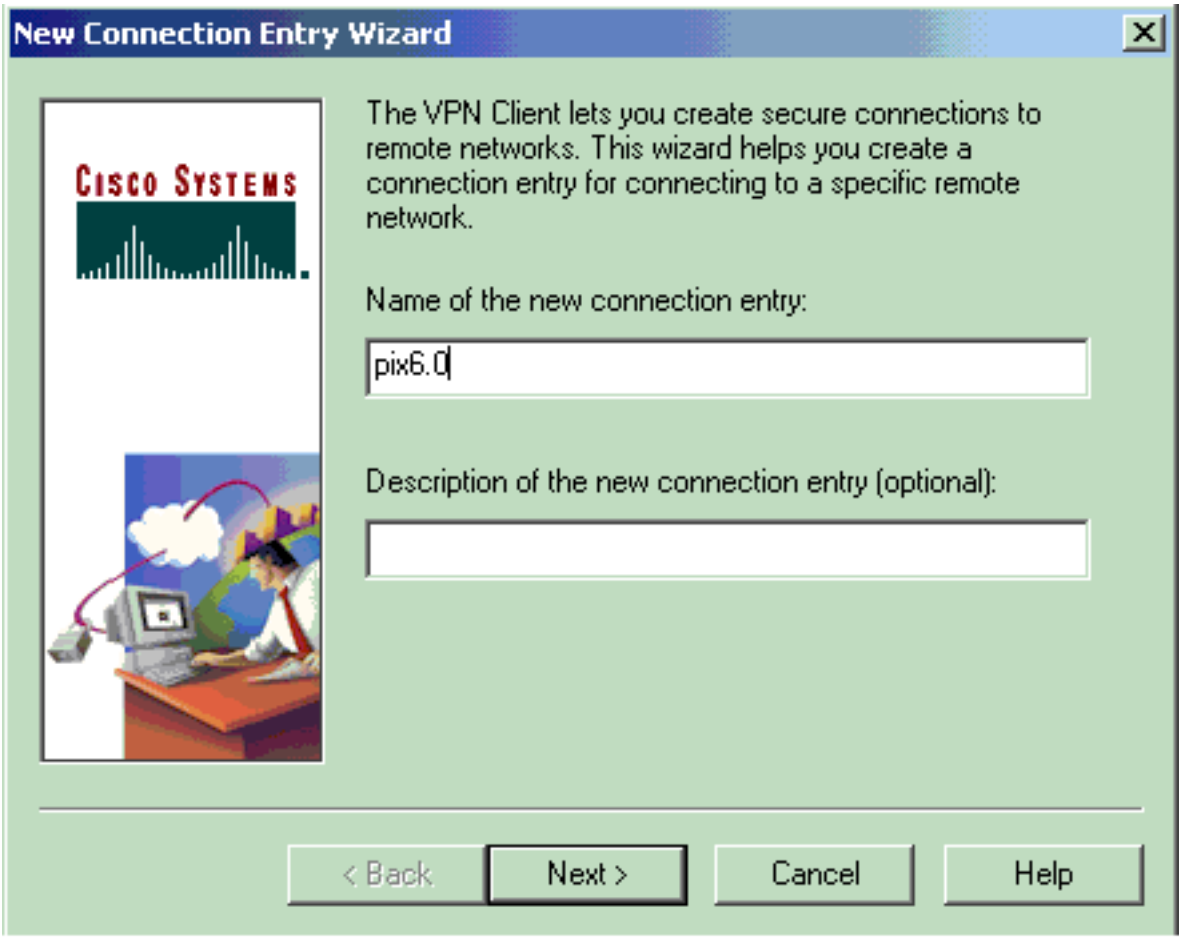
Client VPN Cisco 3.5 pour Windows

Cette section explique comment configurer le client VPN Cisco 3.5 pour Windows.

1. Lancez le client VPN et cliquez sur **Nouveau** pour créer une nouvelle connexion.

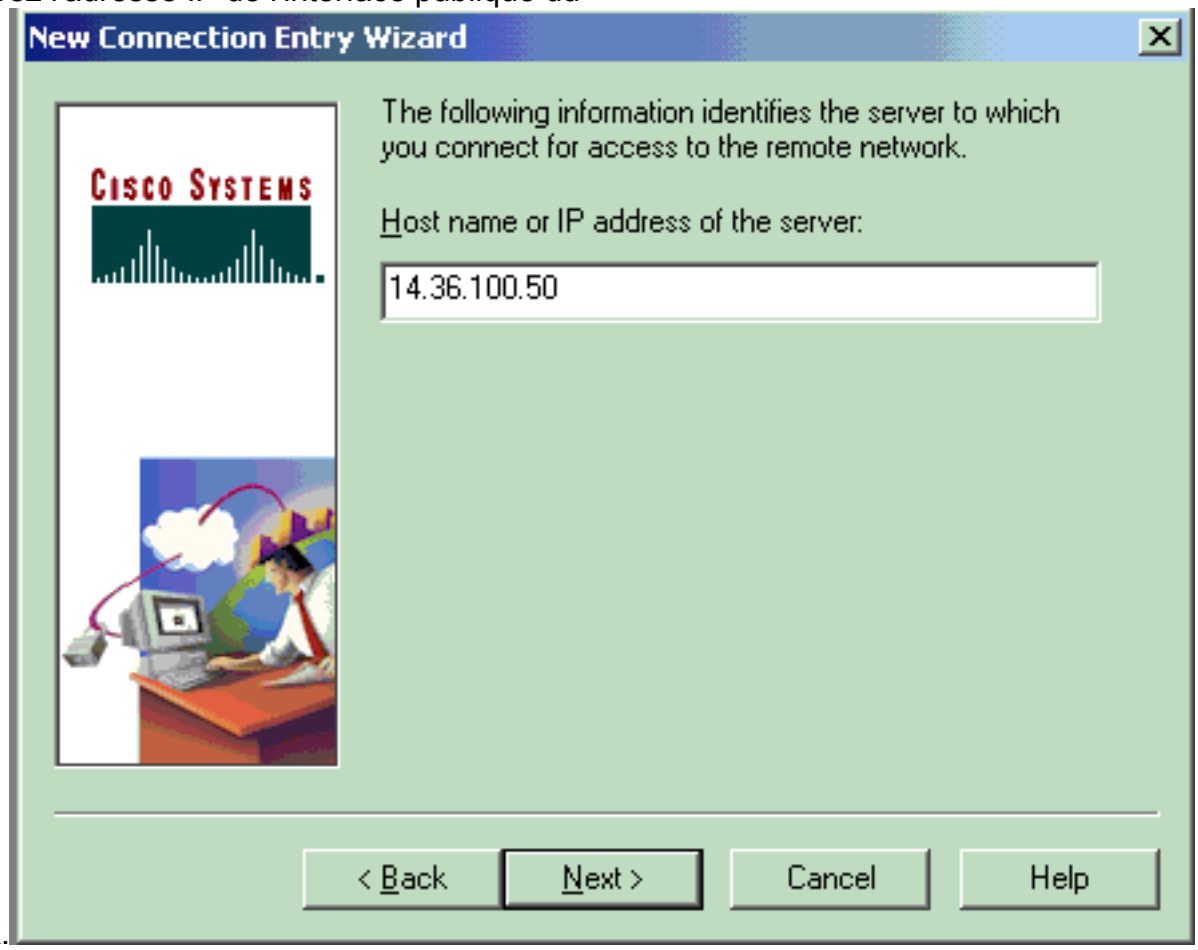


2. Dans la zone **Entrée de connexion**, attribuez un nom à votre



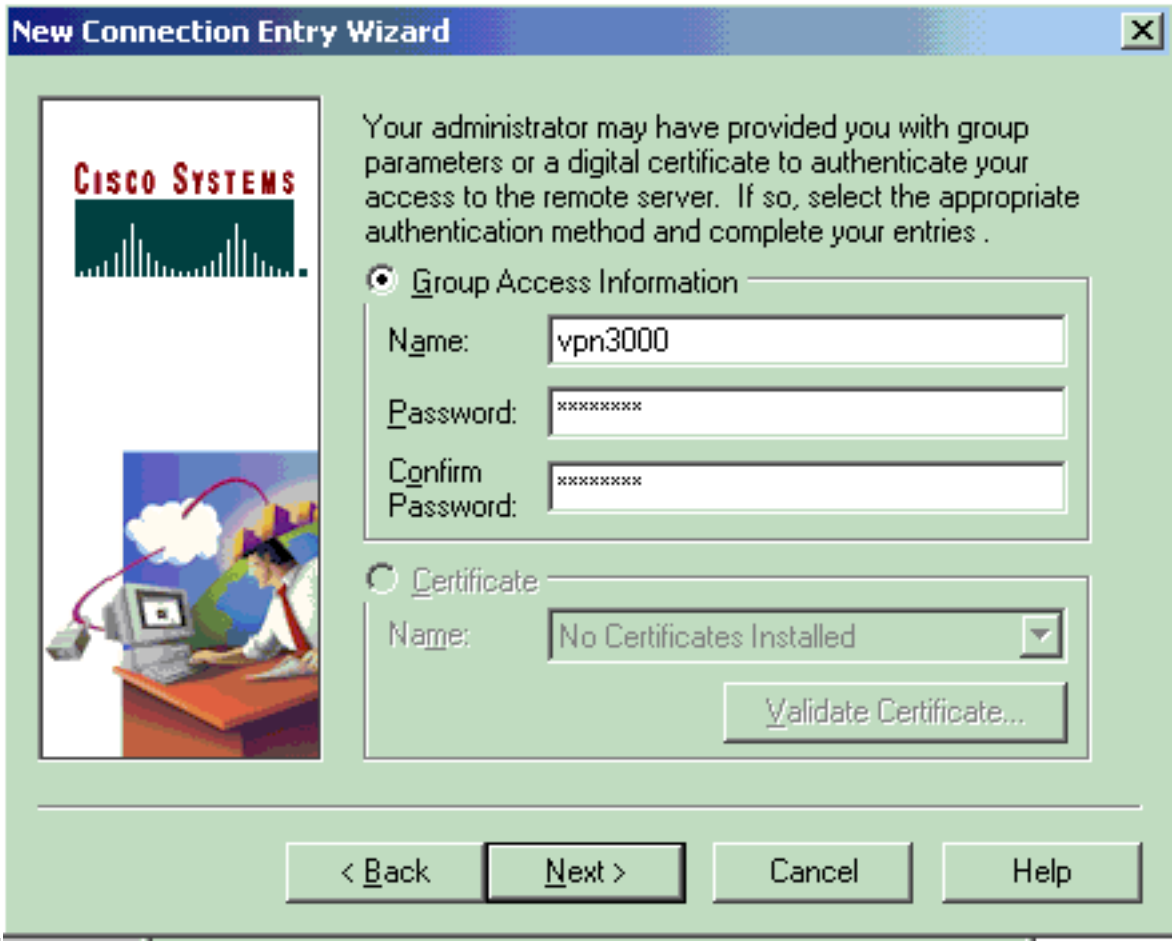
entrée.

3. Entrez l'adresse IP de l'interface publique du



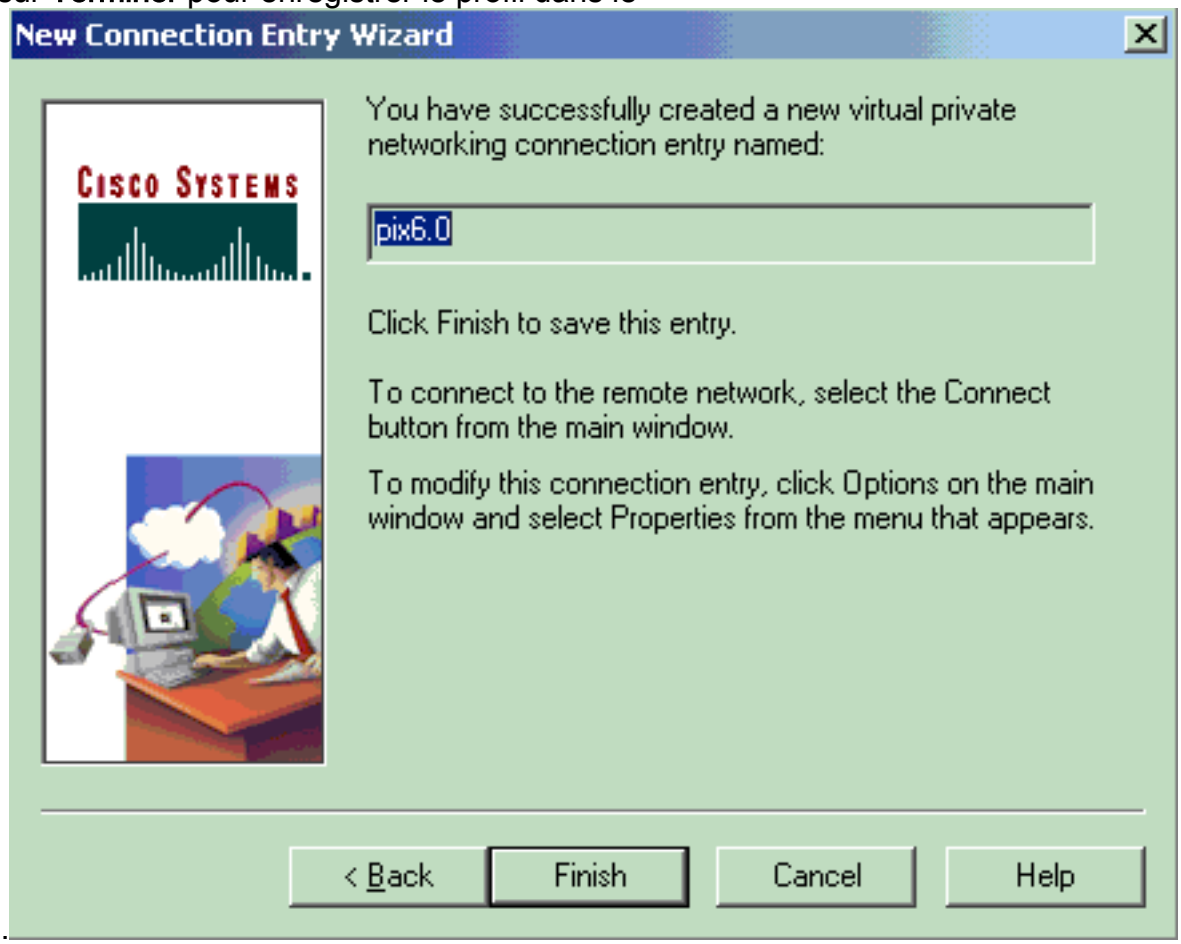
PIX.

4. Sous **Informations d'accès au groupe**, saisissez le nom du groupe et le mot de passe du



groupe.

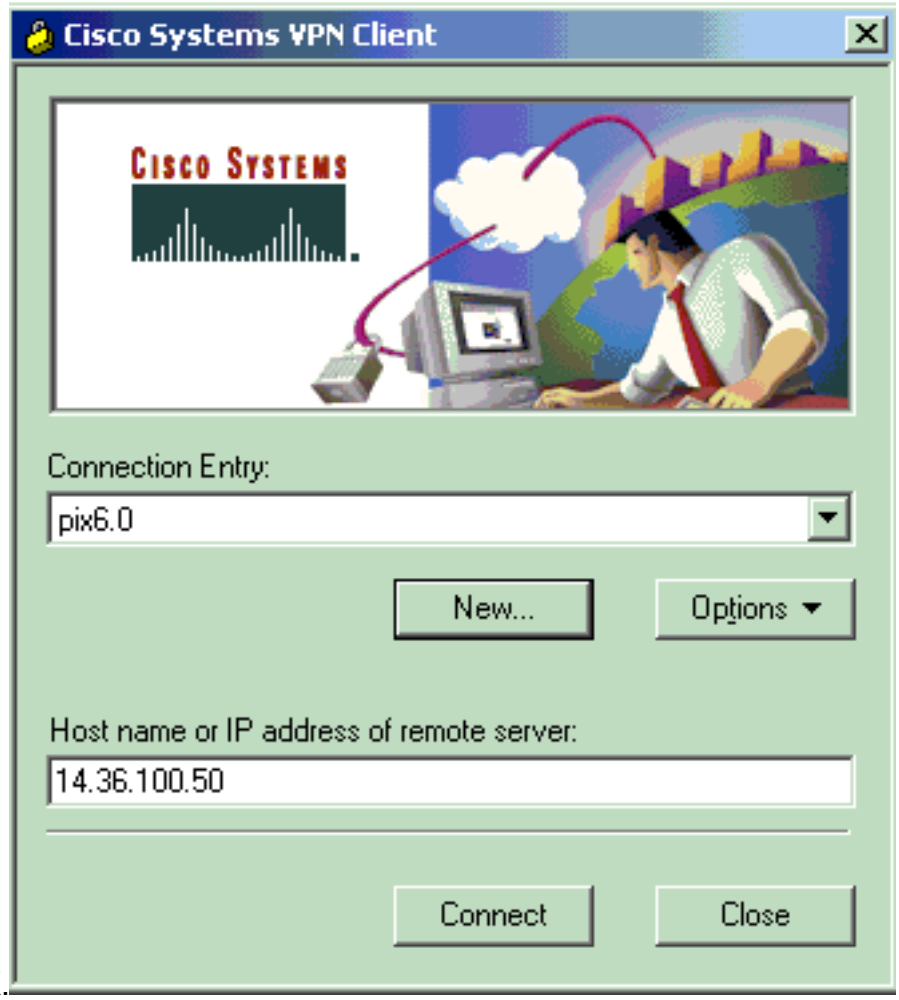
5. Cliquez sur **Terminer** pour enregistrer le profil dans le



Registre.

6. Cliquez sur **Connect** pour vous connecter au

PIX.

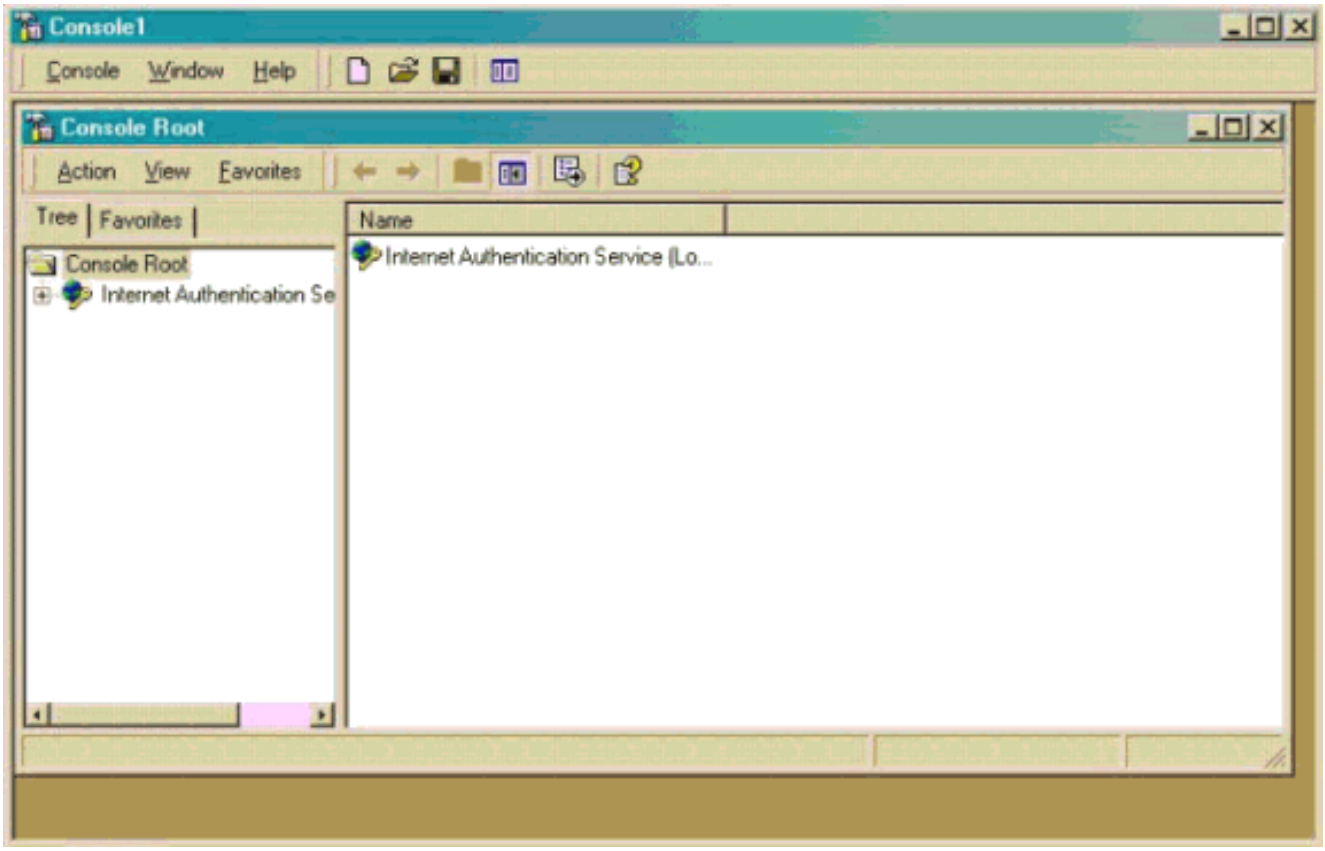


Microsoft Windows 2000 Server avec IAS

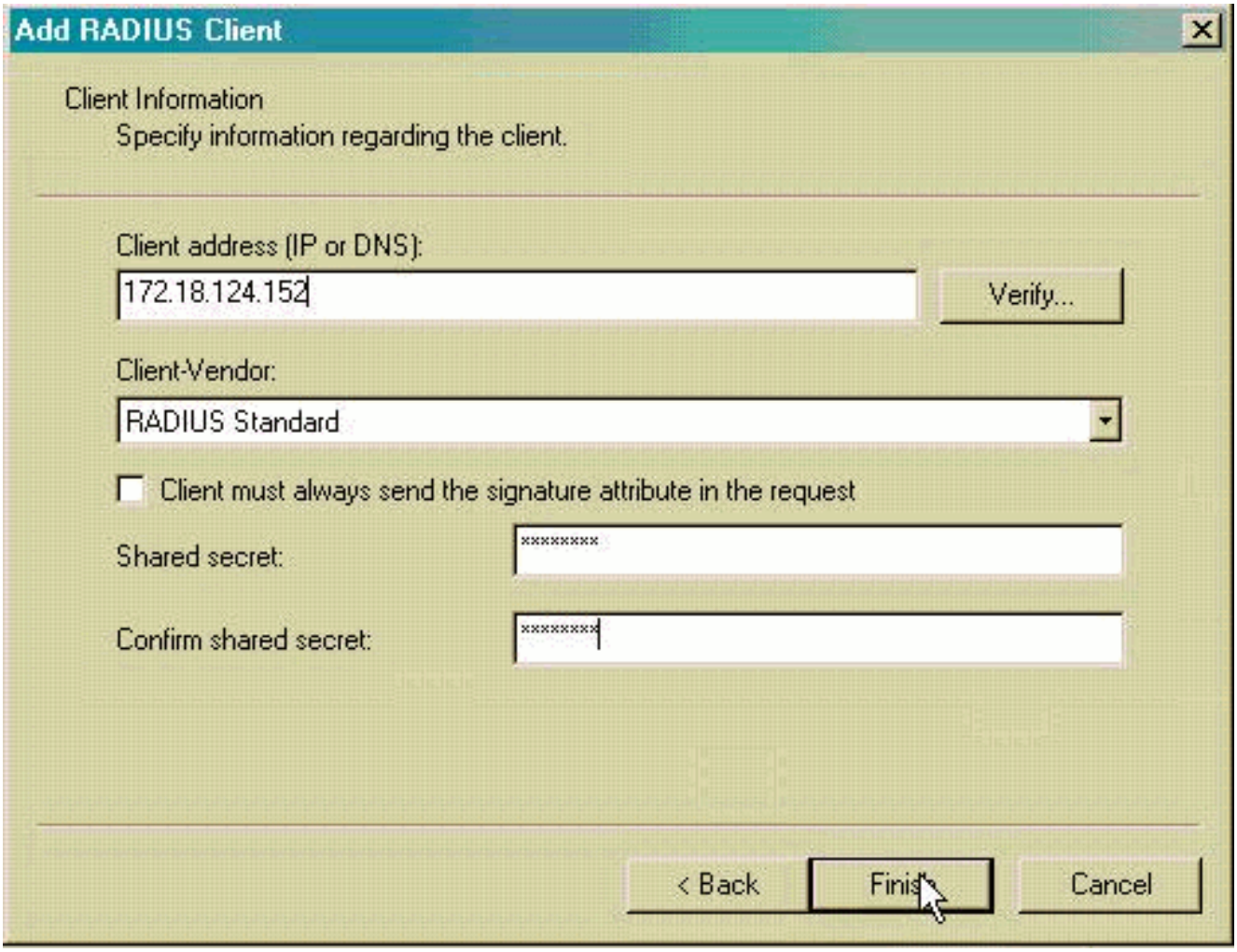
Complétez ces étapes pour configurer le serveur Microsoft Windows 2000 avec IAS. Il s'agit d'une configuration de base pour utiliser un serveur IAS Windows 2000 pour l'authentification RADIUS des utilisateurs VPN. Si vous avez besoin d'une conception plus complexe, contactez Microsoft pour obtenir de l'aide.

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

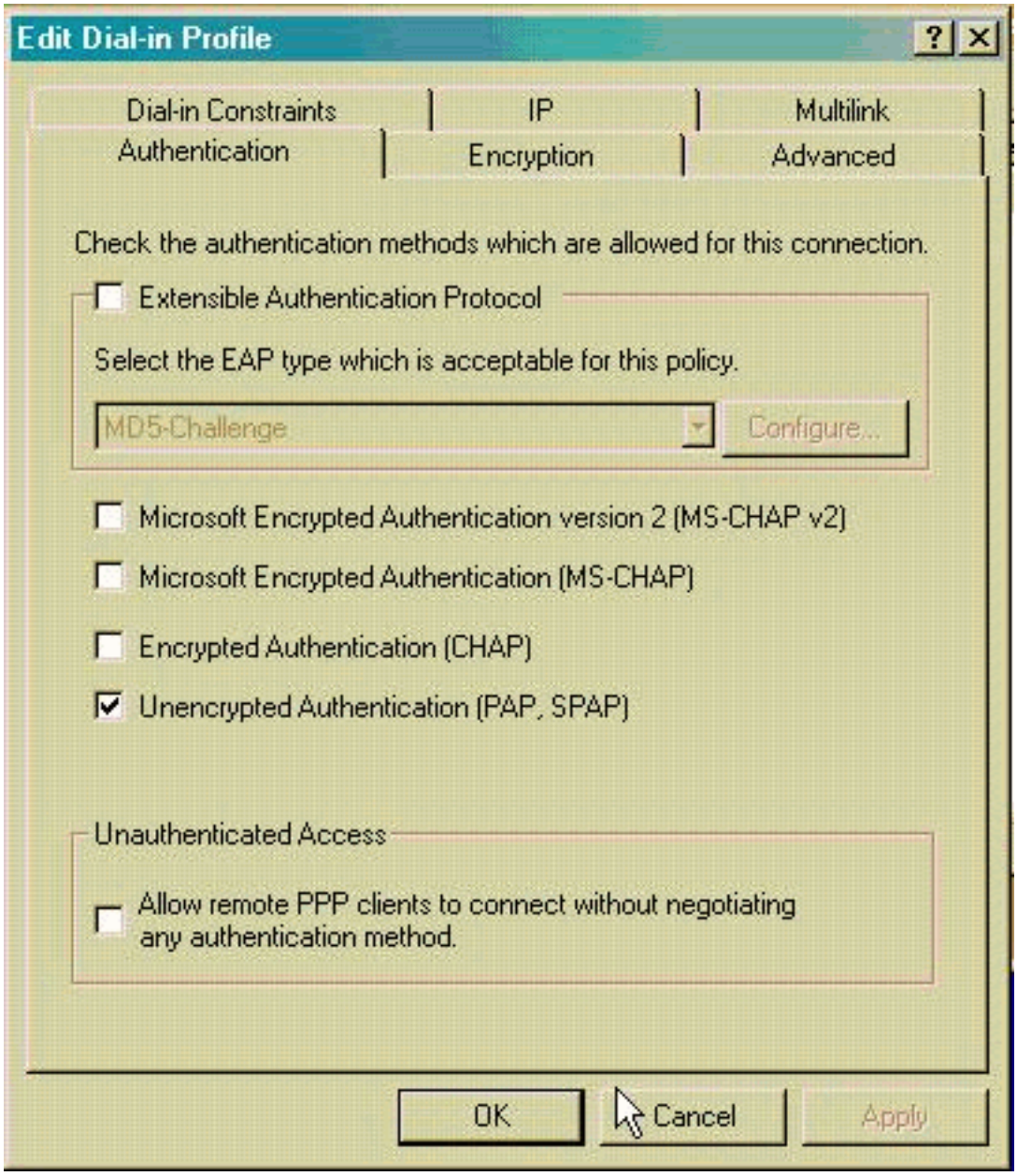
1. Lancez la console de gestion Microsoft. Choisissez **Démarrer > Exécuter** et tapez **mmc.** Cliquez ensuite sur **OK**.
2. Choisissez **Console > Ajouter Supprimer le composant logiciel enfichable....** afin d'ajouter le service IAS à cette console.
3. Cliquez sur **Add** afin de lancer une nouvelle fenêtre avec tous les composants logiciels enfichables autonomes disponibles. Cliquez sur **Internet Authentication Service (IAS)** et cliquez sur **Add**.
4. Vérifiez que **Local Computer** est sélectionné et cliquez sur **Finish**. Cliquez ensuite sur **Fermer**.
5. Notez que IAS est maintenant ajouté. Cliquez sur **OK** pour voir qu'il a été ajouté à la racine de la
console.



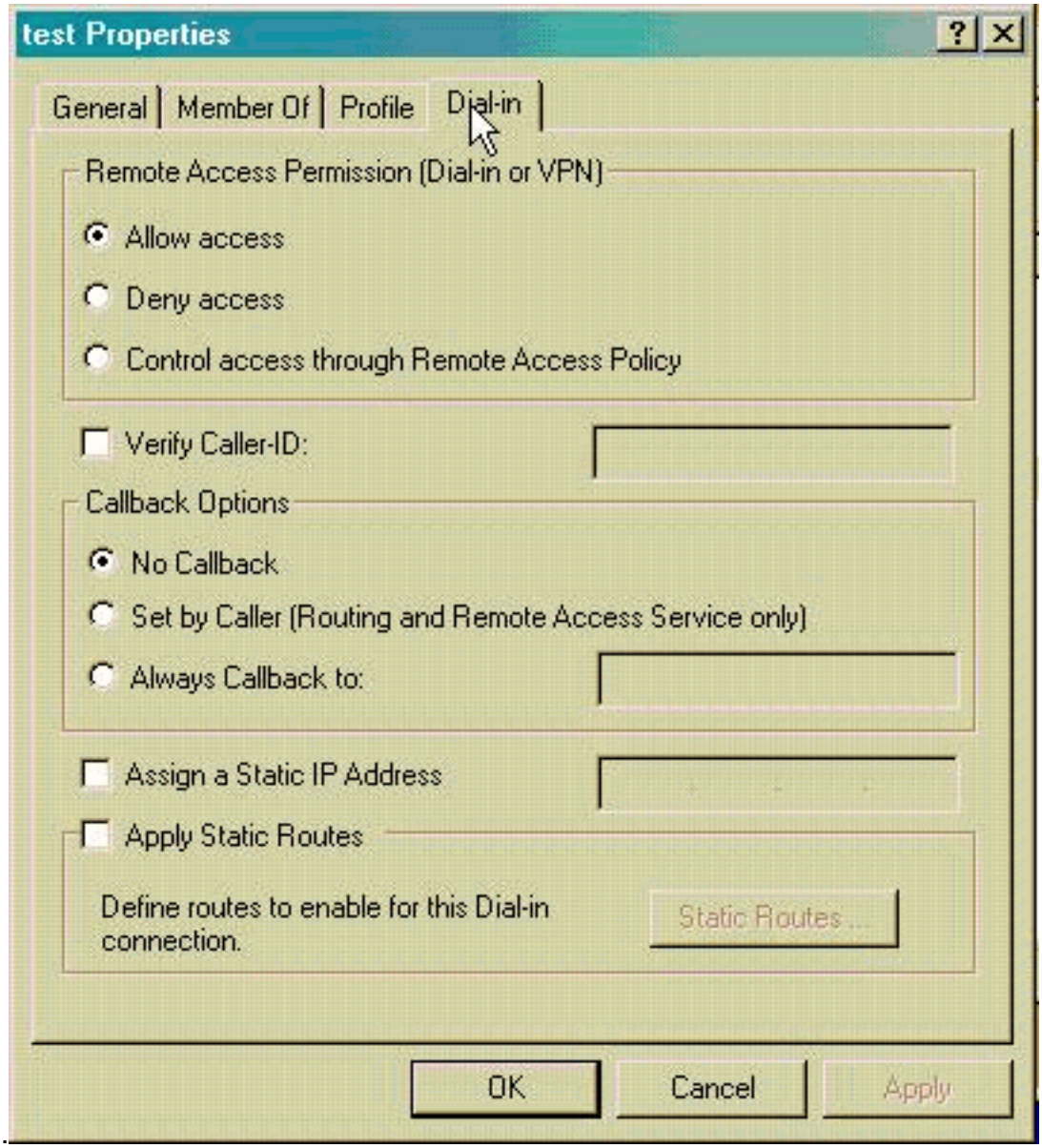
6. Développez le **service d'authentification Internet** et cliquez avec le bouton droit sur **Clients**. Cliquez sur **Nouveau client** et saisissez un nom. Le choix du nom n'a pas vraiment d'importance ; c'est ce que vous verrez dans ce point de vue. Veillez à sélectionner **RADIUS** et cliquez sur **Suivant**.
7. Complétez l'**adresse du client** avec l'adresse de l'interface PIX à laquelle le serveur IAS est connecté. Assurez-vous de sélectionner **RADIUS Standard** et d'ajouter le secret partagé pour correspondre à la commande que vous avez entrée sur le PIX :
   ```
   aaa-server partnerauth (inside) host 172.18.124.196 cisco123 timeout 5
   ```
   Remarque : dans cet exemple, « cisco123 » est le secret partagé.



8. Cliquez sur **Terminer** pour revenir à la racine de la console.
9. Cliquez sur **Stratégies d'accès à distance** dans le volet gauche et double-cliquez sur la stratégie **Autoriser l'accès si l'autorisation de connexion à distance est activée**.
10. Cliquez sur **Modifier le profil** et accédez à l'onglet Authentification. Sous **Méthodes d'authentification**, assurez-vous que seule **l'authentification non chiffrée (PAP, SPAP)** est cochée.**Remarque :** le client VPN ne peut utiliser cette méthode que pour l'authentification.



11. Cliquez sur **Apply**, puis **OK** deux fois.
12. Afin de modifier les utilisateurs pour autoriser la connexion, choisissez **Console > Ajouter/Supprimer un composant logiciel enfichable**. Cliquez sur **Ajouter**, puis sélectionnez le **composant logiciel enfichable Utilisateurs et groupes locaux**. Cliquez sur **Add**. Veillez à sélectionner **Ordinateur local** et cliquez sur **Terminer**. Click OK.
13. Développez **Utilisateurs et groupes locaux** et cliquez sur le dossier **Utilisateurs** dans le volet gauche. Dans le volet droit, double-cliquez sur l'utilisateur auquel vous souhaitez autoriser l'accès.
14. Cliquez sur l'onglet Composer et sélectionnez **Autoriser l'accès** sous **Autorisation d'accès à distance (Composer ou**



VPN).

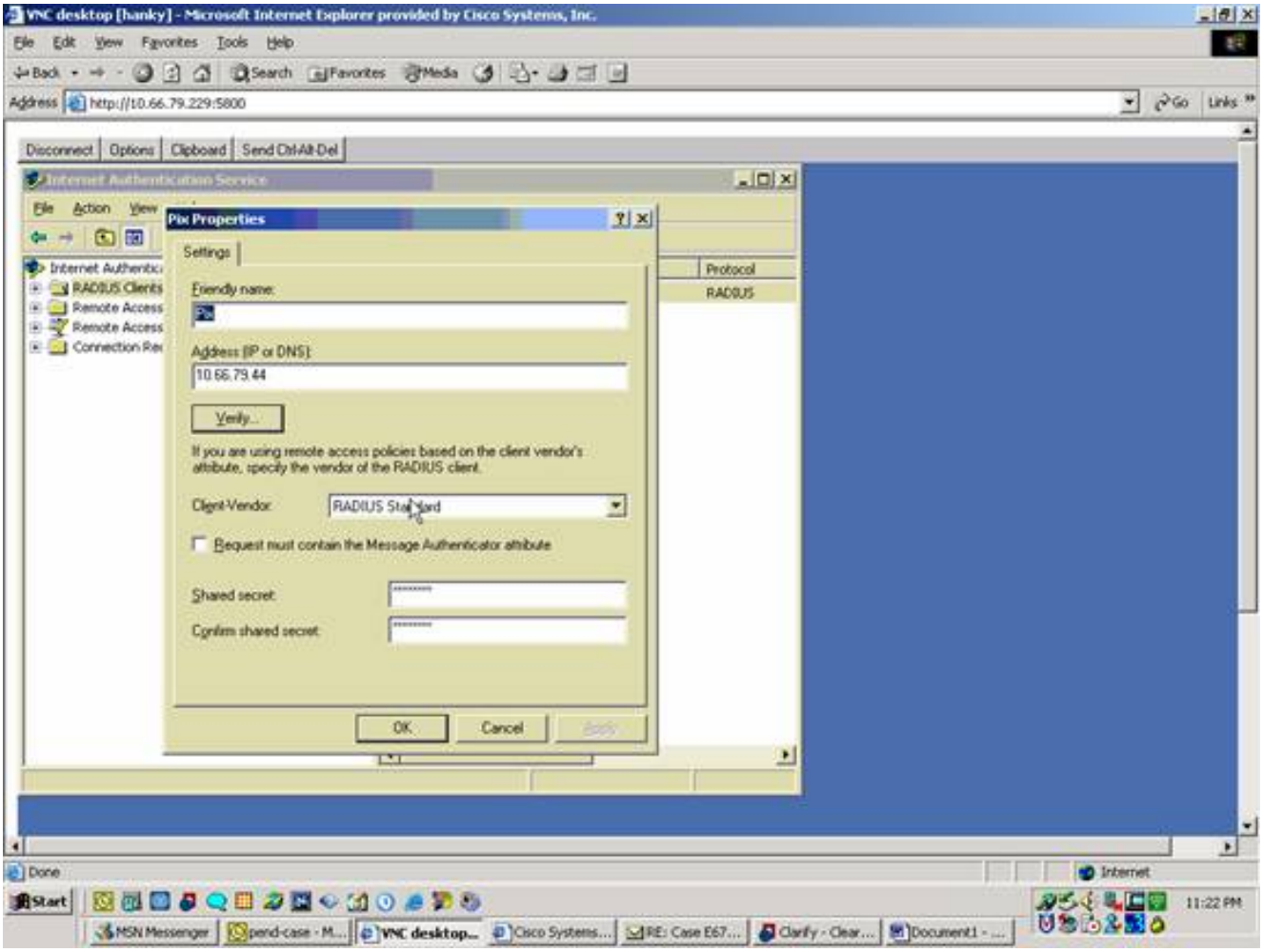
15. Cliquez sur **Apply** et **OK** pour terminer l'action. Vous pouvez fermer l'écran **Console Management** et enregistrer la session, si vous le souhaitez.
16. Les utilisateurs que vous avez modifiés doivent maintenant pouvoir accéder au PIX avec le client VPN 3.5. N'oubliez pas que le serveur IAS authentifie uniquement les informations utilisateur. Le PIX effectue toujours l'authentification de groupe.

Microsoft Windows 2003 Server avec IAS

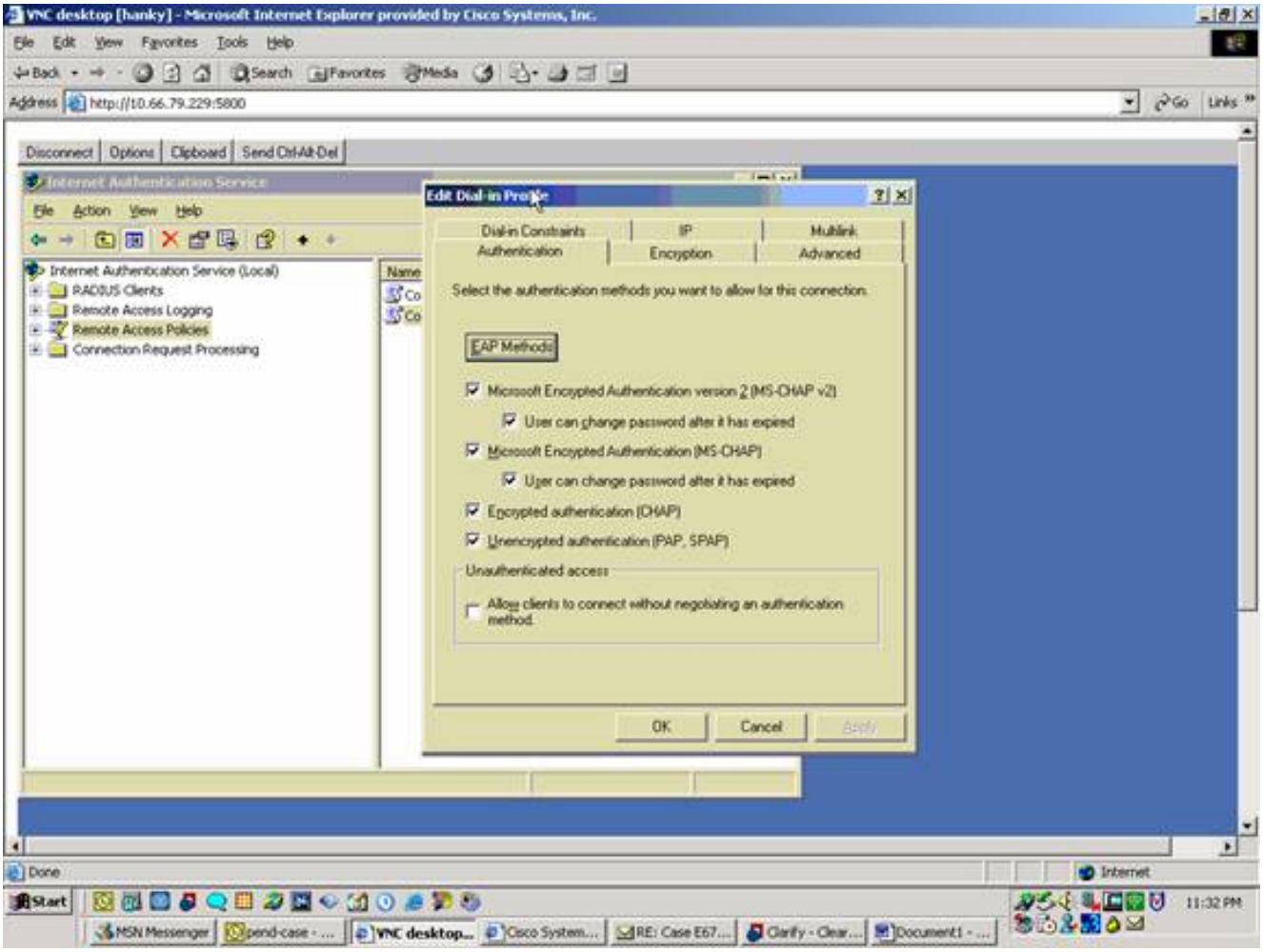
Complétez ces étapes pour configurer le serveur Microsoft Windows 2003 avec IAS.

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

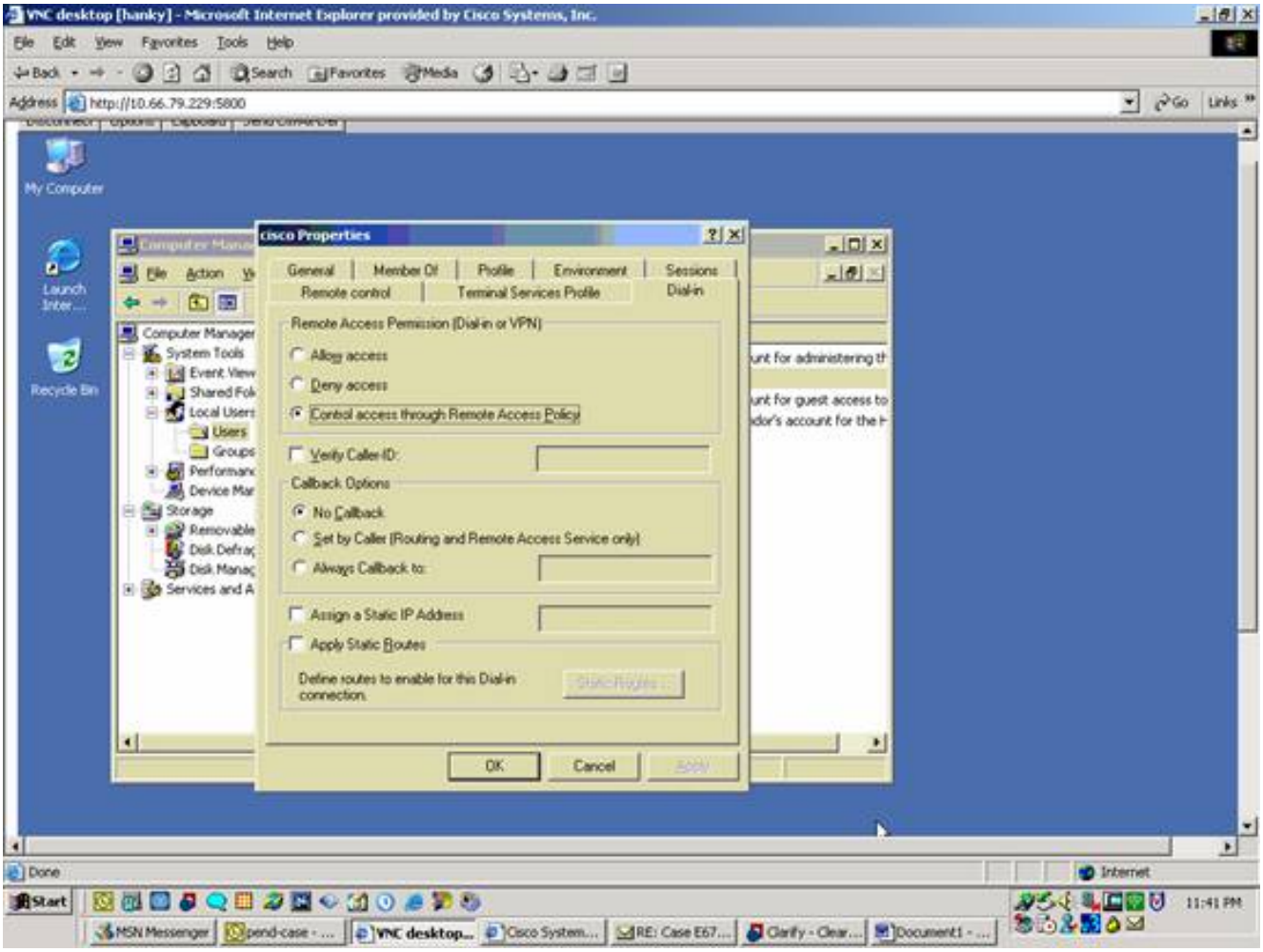
1. Choisissez **Outils d'administration > Service d'authentification Internet** et cliquez avec le bouton droit sur **Client RADIUS** pour ajouter un nouveau client RADIUS. Après avoir tapé les informations sur le client, cliquez sur **OK**.Cet exemple montre un client nommé « Pix » avec l'adresse IP 10.66.79.44. Client-Vendor est défini sur RADIUS Standard et le secret partagé est « cisco123
   ».



2. Accédez à **Remote Access Policies**, cliquez avec le bouton droit de la souris sur **Connections to Other Access Servers** et sélectionnez **Properties**.
3. Assurez-vous que l'option Grant Remote Access Permissions est sélectionnée.
4. Cliquez sur **Modifier le profil** 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. Ajoutez un utilisateur au compte d'ordinateur local. Pour ce faire, 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**.
6. Ajoutez un utilisateur avec le mot de passe Cisco « cisco123 » et vérifiez ces informations de 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 Composer, sélectionnez l'option **Autoriser l'accès** (ou laissez le paramètre par défaut de Contrôle de l'accès via la stratégie d'accès à distance).Cliquez sur **OK quand vous avez terminé.**



Vérification

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

L'Outil Interpréteur de sortie (clients enregistrés uniquement) (OIT) prend en charge certaines commandes show. Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show .**

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

Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration. Pour plus d'informations, référez-vous à Dépannage du PIX pour passer le trafic de données sur un tunnel IPSec établi.

Dépannage des commandes

Certaines commandes sont prises en charge par l'outil Output Interpreter (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 avant d'utiliser les commandes **debug** et reportez-vous à Résolution des problèmes de sécurité IP - Compréhension et utilisation des commandes de débogage.

- **debug crypto ipsec** - Affichez les négociations IPSec de la phase 2.
- **debug crypto isakmp** - Affichez les négociations ISAKMP de la phase 1.
- **debug crypto engine** - Affichez le trafic chiffré.

Exemple de sortie de débogage

- Pare-feu PIX
- Client VPN 3.5 pour Windows

Pare-feu PIX

```
pixfirewall(config)#
crypto_isakmp_process_block: src 14.36.100.55, dest 14.36.100.50
VPN Peer: ISAKMP: Added new peer: ip:14.36.100.55 Total VPN Peers:1
VPN Peer: ISAKMP: Peer ip:14.36.100.55 Ref cnt incremented to:1
   Total VPN Peers:1
OAK_AG exchange
ISAKMP (0): processing SA payload. message ID = 0

ISAKMP (0): Checking ISAKMP transform 1 against priority 10 policy
ISAKMP:      encryption 3DES-CBC
ISAKMP:      hash SHA
ISAKMP:      default group 2
ISAKMP:      extended auth pre-share
ISAKMP:      life type in seconds
ISAKMP:      life duration (VPI) of  0x0 0x20 0xc4 0x9b
ISAKMP (0): atts are not acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 2 against priority 10 policy
ISAKMP:      encryption 3DES-CBC
ISAKMP:      hash MD5
ISAKMP:      default group 2
ISAKMP:      extended auth pre-share
ISAKMP:      life type in seconds
ISAKMP:      life duration (VPI) of  0x0 0x20 0xc4 0x9b
ISAKMP (0): atts are not acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 3 against priority 10 policy
ISAKMP:      encryption 3DES-CBC
ISAKMP:      hash SHA
ISAKMP:      default group 2
ISAKMP:      auth pre-share
ISAKMP:      life type in seconds
ISAKMP:      life duration (VPI) of  0x0 0x20 0xc4 0x9b
ISAKMP (0): atts are not acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 4 against priority 10 policy
ISAKMP:      encryption 3DES-CBC
ISAKMP:      hash MD5
ISAKMP:      default group 2
ISAKMP:      auth pre-share
ISAKMP:      life type in seconds
ISAKMP:      life duration (VPI) of  0x0 0x20 0xc4 0x9b
ISAKMP (0): atts are not acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 5 against priority 10 policy
ISAKMP:      encryption DES-CBC
ISAKMP:      hash SHA
```

```
ISAKMP:      default group 2
ISAKMP:      extended auth pre-share
ISAKMP:      life type in seconds
ISAKMP:      life duration (VPI) of  0x0 0x20 0xc4 0x9b
ISAKMP (0): atts are not acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 6 against priority 10 policy
ISAKMP:      encryption DES-CBC
ISAKMP:      hash MD5
ISAKMP:      default group 2
ISAKMP:      extended auth pre-share
ISAKMP:      life type in seconds
ISAKMP:      life duration (VPI) of  0x0 0x20 0xc4 0x9b
ISAKMP (0): atts are acceptable. Next payload is 3
ISAKMP (0): processing KE payload. message ID = 0

ISAKMP (0): processing NONCE payload. message ID = 0

ISAKMP (0): processing ID payload. message ID = 0
ISAKMP (0): processing vendor id payload

ISAKMP (0): processing vendor id payload

ISAKMP (0): remote peer supports dead peer detection

ISAKMP (0): processing vendor id payload

ISAKMP (0): speaking to a Unity client

ISAKMP: Created a peer node for 14.36.100.55
ISAKMP (0): ID payload
        next-payload : 10
        type         : 1
        protocol     : 17
        port         : 500
        length       : 8
ISAKMP (0): Total payload length: 12
return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 14.36.100.55, dest 14.36.100.50
OAK_AG exchange
ISAKMP (0): processing HASH payload. message ID = 0
ISAKMP (0): processing NOTIFY payload 24578 protocol 1
        spi 0, message ID = 0
ISAKMP (0): processing notify INITIAL_CONTACTIPSEC(key_engine): got
   a queue event...
IPSEC(key_engine_delete_sas): rec'd delete notify from ISAKMP
IPSEC(key_engine_delete_sas): delete all SAs shared with 14.36.100.55

ISAKMP (0): SA has been authenticated
return status is IKMP_NO_ERROR
ISAKMP/xauth: request attribute XAUTH_TYPE
ISAKMP/xauth: request attribute XAUTH_USER_NAME
ISAKMP/xauth: request attribute XAUTH_USER_PASSWORD
ISAKMP (0:0): initiating peer config to 14.36.100.55. ID = 3870616596
   (0xe6b4ec14)
crypto_isakmp_process_block: src 14.36.100.55, dest 14.36.100.50
ISAKMP_TRANSACTION exchange
ISAKMP (0:0): processing transaction payload from 14.36.100.55.
   message ID = 84
ISAKMP: Config payload CFG_REPLY
return status is IKMP_ERR_NO_RETRANS
ISAKMP (0:0): initiating peer config to 14.36.100.55. ID = 3612718114
   (0xd755b422)
crypto_isakmp_process_block: src 14.36.100.55, dest 14.36.100.50
ISAKMP_TRANSACTION exchange
```

```
ISAKMP (0:0): processing transaction payload from 14.36.100.55.
   message ID = 60
ISAKMP: Config payload CFG_ACK
return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 14.36.100.55, dest 14.36.100.50
ISAKMP_TRANSACTION exchange
ISAKMP (0:0): processing transaction payload from 14.36.100.55.
   message ID = 0
ISAKMP: Config payload CFG_REQUEST
ISAKMP (0:0): checking request:
ISAKMP: attribute    IP4_ADDRESS (1)
ISAKMP: attribute    IP4_NETMASK (2)
ISAKMP: attribute    IP4_DNS (3)
ISAKMP: attribute    IP4_NBNS (4)
ISAKMP: attribute    ADDRESS_EXPIRY (5)
        Unsupported Attr: 5
ISAKMP: attribute    APPLICATION_VERSION (7)
        Unsupported Attr: 7
ISAKMP: attribute    UNKNOWN (28672)
        Unsupported Attr: 28672
ISAKMP: attribute    UNKNOWN (28673)
        Unsupported Attr: 28673
ISAKMP: attribute    UNKNOWN (28674)
ISAKMP: attribute    UNKNOWN (28676)
ISAKMP: attribute    UNKNOWN (28679)
        Unsupported Attr: 28679
ISAKMP: attribute    UNKNOWN (28680)
        Unsupported Attr: 28680
ISAKMP: attribute    UNKNOWN (28677)
        Unsupported Attr: 28677
ISAKMP (0:0): responding to peer config from 14.36.100.55.
   ID = 3979868003
return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 14.36.100.55, dest 14.36.100.50
OAK_QM exchange
oakley_process_quick_mode:
OAK_QM_IDLE
ISAKMP (0): processing SA payload. message ID = 1527320241

ISAKMP : Checking IPSec proposal 1

ISAKMP: transform 1, ESP_3DES
ISAKMP:   attributes in transform:
ISAKMP:      authenticator is HMAC-MD5
ISAKMP:      encaps is 1
ISAKMP:      SA life type in seconds
ISAKMP:      SA life duration (VPI) of  0x0 0x20 0xc4 0x9b
   IPSEC(validate_proposal): transform proposal (prot 3, trans
3, hmac_alg 1) not supported

ISAKMP (0): atts not acceptable. Next payload is 0
ISAKMP (0): skipping next ANDed proposal (1)
ISAKMP : Checking IPSec proposal 2

ISAKMP: transform 1, ESP_3DES
ISAKMP:   attributes in transform:
ISAKMP:      authenticator is HMAC-SHA
ISAKMP:      encaps is 1
ISAKMP:      SA life type in seconds
ISAKMP:      SA life duration (VPI) of  0x0 0x20 0xc4 0x9b
   IPSEC(validate_proposal): transform proposal (prot 3, trans
3, hmac_alg 2) not supported

ISAKMP (0): atts not acceptable. Next payload is 0
```

```
ISAKMP (0): skipping next ANDed proposal (2)
ISAKMP : Checking IPSec proposal 3

ISAKMP: transform 1, ESP_3DES
ISAKMP:   attributes in transform:
ISAKMP:      authenticator is HMAC-MD5
ISAKMP:      encaps is 1
ISAKMP:      SA life type in seconds
ISAKMP:      SA life duration (VPI) of  0x0 0x20 0xc4 0x9b
   IPSEC(validate_proposal): transform proposal (prot 3, trans
3, hmac_alg 1) not supported

ISAKMP (0): atts not acceptable. Next payload is 0
ISAKMP : Checking IPSec proposal 4

ISAKMP: transform 1, ESP_3DES
ISAKMP:   attributes in transform:
ISAKMP:      authenticator is HMAC-SHA
ISAKMP:      encaps is 1
ISAKMP:      SA life type in seconds
ISAKMP:      SA life duration (VPI) of  0x0 0x20 0xc4 0x9b
   IPSEC(validate_proposal): transform proposal (prot 3, trans
3, hmac_alg 2) not supported

ISAKMP (0): atts not acceptable. Next payload is 0
ISAKMP : Checking IPSec proposal 5

ISAKMP: transform 1, ESP_DES
ISAKMP:   attributes in transform:
ISAKMP:      authenticator is HMAC-MD5
ISAKMP:      encaps is 1
ISAKMP:      SA life type in seconds
ISAKMP:      SA life duration (VPI) of  0x0 0x20 0xc4 0x9b
ISAKMP (0): atts are acceptable.
ISAKMP (0): bad SPI size of 2 octets!
ISAKMP : Checking IPSec proposal 6

ISAKMP: transform 1, ESP_DES
ISAKMP:   attributes in transform:
ISAKMP:      authenticator is HMAC-SHA
ISAKMP:      encaps is 1
ISAKMP:      SA life type in seconds
ISAKMP:      SA life duration (VPI) of  0x0 0x20 0xc4 0x9b
   IPSEC(validate_proposal): transform proposal (prot 3, trans
2, hmac_alg 2) not supported

ISAKMP (0): atts not acceptable. Next payload is 0
ISAKMP (0): skipping next ANDed proposal (6)
ISAKMP : Checking IPSec proposal 7

ISAKMP: transform 1, ESP_DES
ISAKMP:   attributes in transform:
ISAKMP:      authenticator is HMAC-MD5
ISAKMP:      encaps is 1
ISAKMP:      SA life type in seconds
ISAKMP:      SA life duration (VPI) of  0x0 0x20 0xc4 0x9b
ISAKMP (0): atts are acceptable.IPSEC(validate_proposal_request):
   proposal part #1,
  (key eng. msg.) dest= 14.36.100.50, src= 14.36.100.55,
    dest_proxy= 14.36.100.50/255.255.255.255/0/0 (type=1),
    src_proxy= 10.1.2.1/255.255.255.255/0/0 (type=1),
    protocol= ESP, transform= esp-des esp-md5-hmac ,
    lifedur= 0s and 0kb,
    spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
```

```
ISAKMP (0): processing NONCE payload. message ID = 1527320241

ISAKMP (0): processing ID payload. message ID = 1527320241
ISAKMP (0): ID_IPV4_ADDR src 10.1.2.1 prot 0 port 0
ISAKMP (0): processing ID payload. message ID = 1527320241
ISAKMP (0): ID_IPV4_ADDR dst 14.36.100.50 prot 0 port
   0IPSEC(key_engine): got a queue event...
IPSEC(spi_response): getting spi 0xf39c2217(4087095831) for SA
        from    14.36.100.55 to    14.36.100.50 for prot 3

return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 14.36.100.55, dest 14.36.100.50
OAK_QM exchange
oakley_process_quick_mode:
OAK_QM_IDLE
ISAKMP (0): processing SA payload. message ID = 3487980779

ISAKMP : Checking IPSec proposal 1

ISAKMP: transform 1, ESP_3DES
ISAKMP:   attributes in transform:
ISAKMP:      authenticator is HMAC-MD5
crypto_isakmp_process_block: src 14.36.100.55, dest 14.36.100.50
OAK_QM exchange
oakley_process_quick_mode:
OAK_QM_AUTH_AWAIT
ISAKMP (0): Creating IPSec SAs
        inbound SA from    14.36.100.55 to    14.36.100.50
             (proxy        10.1.2.1 to    14.36.100.50)
        has spi 4087095831 and conn_id 1 and flags 4
        lifetime of 2147483 seconds
        outbound SA from    14.36.100.50 to    14.36.100.55
             (proxy    14.36.100.50 to        10.1.2.1)
        has spi 1929305241 and conn_id 2 and flags 4
        lifetime of 2147483 secondsIPSEC(key_engine): got a queue event...
IPSEC(initialize_sas): ,
  (key eng. msg.) dest= 14.36.100.50, src= 14.36.100.55,
    dest_proxy= 14.36.100.50/0.0.0.0/0/0 (type=1),
    src_proxy= 10.1.2.1/0.0.0.0/0/0 (type=1),
    protocol= ESP, transform= esp-des esp-md5-hmac ,
    lifedur= 2147483s and 0kb,
    spi= 0xf39c2217(4087095831), conn_id= 1, keysize= 0, flags= 0x4
IPSEC(initialize_sas): ,
  (key eng. msg.) src= 14.36.100.50, dest= 14.36.100.55,
    src_proxy= 14.36.100.50/0.0.0.0/0/0 (type=1),
    dest_proxy= 10.1.2.1/0.0.0.0/0/0 (type=1),
    protocol= ESP, transform= esp-des esp-md5-hmac ,
    lifedur= 2147483s and 0kb,
    spi= 0x72fedc99(1929305241), conn_id= 2, keysize= 0, flags= 0x4

VPN Peer: IPSEC: Peer ip:14.36.100.55 Ref cnt incremented to:2
   Total VPN Peers:1
VPN Peer: IPSEC: Peer ip:14.36.100.55 Ref cnt incremented to:3
   Total VPN Peers:1
return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 14.36.100.55, dest 14.36.100.50
OAK_QM exchange
oakley_process_quick_mode:
OAK_QM_AUTH_AWAIT
ISAKMP (0): Creating IPSec SAs
        inbound SA from    14.36.100.55 to    14.36.100.50
             (proxy        10.1.2.1 to         0.0.0.0)
        has spi 1791135440 and conn_id 3 and flags 4
```

```
        lifetime of 2147483 seconds
        outbound SA from    14.36.100.50 to    14.36.100.55
             (proxy         0.0.0.0 to        10.1.2.1)
        has spi 173725574 and conn_id 4 and flags 4
        lifetime of 2147483 secondsIPSEC(key_engine): got a queue event...
IPSEC(initialize_sas): ,
  (key eng. msg.) dest= 14.36.100.50, src= 14.36.100.55,
    dest_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4),
    src_proxy= 10.1.2.1/0.0.0.0/0/0 (type=1),
    protocol= ESP, transform= esp-des esp-md5-hmac ,
    lifedur= 2147483s and 0kb,
    spi= 0x6ac28ed0(1791135440), conn_id= 3, keysize= 0, flags= 0x4
IPSEC(initialize_sas): ,
  (key eng. msg.) src= 14.36.100.50, dest= 14.36.100.55,
    src_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4),
    dest_proxy= 10.1.2.1/0.0.0.0/0/0 (type=1),
    protocol= ESP, transform= esp-des esp-md5-hmac ,
    lifedur= 2147483s and 0kb,
    spi= 0xa5ad786(173725574), conn_id= 4, keysize= 0, flags= 0x4

VPN Peer: IPSEC: Peer ip:14.36.100.55 Ref cnt incremented to:4
   Total VPN Peers:1
VPN Peer: IPSEC: Peer ip:14.36.100.55 Ref cnt incremented to:5
   Total VPN Peers:1
return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 14.36.100.55, dest 14.36.100.50
ISAKMP (0): processing NOTIFY payload 36136 protocol 1
        spi 0, message ID = 3443334051
ISAMKP (0): received DPD_R_U_THERE from peer 14.36.100.55
ISAKMP (0): sending NOTIFY message 36137 protocol 1
return status is IKMP_NO_ERR_NO_TRANS
```

Client VPN 3.5 pour Windows

```
193    19:00:56.073  01/24/02  Sev=Info/6       DIALER/0x63300002
Initiating connection.

194    19:00:56.073  01/24/02  Sev=Info/4       CM/0x63100002
Begin connection process

195    19:00:56.083  01/24/02  Sev=Info/4       CM/0x63100004
Establish secure connection using Ethernet

196    19:00:56.083  01/24/02  Sev=Info/4       CM/0x63100026
Attempt connection with server "14.36.100.50"

197    19:00:56.083  01/24/02  Sev=Info/6       IKE/0x6300003B
Attempting to establish a connection with 14.36.100.50.

198    19:00:56.124  01/24/02  Sev=Info/4       IKE/0x63000013
SENDING >>> ISAKMP OAK AG (SA, KE, NON, ID, VID, VID, VID)
to 14.36.100.50

199    19:00:56.774  01/24/02  Sev=Info/4       IPSEC/0x63700014
Deleted all keys

200    19:00:59.539  01/24/02  Sev=Info/5       IKE/0x6300002F
Received ISAKMP packet: peer = 14.36.100.50

201    19:00:59.539  01/24/02  Sev=Info/4       IKE/0x63000014
RECEIVING <<< ISAKMP OAK AG (SA, VID, VID, VID, KE, ID, NON, HASH)
from 14.36.100.50
```

```
202    19:00:59.539  01/24/02  Sev=Info/5       IKE/0x63000059
Vendor ID payload = 12F5F28C457168A9702D9FE274CC0100

203    19:00:59.539  01/24/02  Sev=Info/5       IKE/0x63000001
Peer is a Cisco-Unity compliant peer

204    19:00:59.539  01/24/02  Sev=Info/5       IKE/0x63000059
Vendor ID payload = AFCAD71368A1F1C96B8696FC77570100

205    19:00:59.539  01/24/02  Sev=Info/5       IKE/0x63000001
Peer supports DPD

206    19:00:59.539  01/24/02  Sev=Info/5       IKE/0x63000059
Vendor ID payload = 6D761DDC26ACECA1B0ED11FABBB860C4

207    19:00:59.569  01/24/02  Sev=Info/4       IKE/0x63000013
SENDING >>> ISAKMP OAK AG *(HASH, NOTIFY:STATUS_INITIAL_CONTACT)
to 14.36.100.50

208    19:00:59.569  01/24/02  Sev=Info/5       IKE/0x6300002F
Received ISAKMP packet: peer = 14.36.100.50

209    19:00:59.569  01/24/02  Sev=Info/4       IKE/0x63000014
RECEIVING <<< ISAKMP OAK TRANS *(HASH, ATTR) from 14.36.100.50

210    19:00:59.569  01/24/02  Sev=Info/4       CM/0x63100015
Launch xAuth application

211    19:01:04.236  01/24/02  Sev=Info/4       CM/0x63100017
xAuth application returned

212    19:01:04.236  01/24/02  Sev=Info/4       IKE/0x63000013
SENDING >>> ISAKMP OAK TRANS *(HASH, ATTR) to 14.36.100.50

213    19:01:04.496  01/24/02  Sev=Info/5       IKE/0x6300002F
Received ISAKMP packet: peer = 14.36.100.50

214    19:01:04.496  01/24/02  Sev=Info/4       IKE/0x63000014
RECEIVING <<< ISAKMP OAK TRANS *(HASH, ATTR) from 14.36.100.50

215    19:01:04.496  01/24/02  Sev=Info/4       CM/0x6310000E
Established Phase 1 SA.  1 Phase 1 SA in the system

216    19:01:04.506  01/24/02  Sev=Info/4       IKE/0x63000013
SENDING >>> ISAKMP OAK TRANS *(HASH, ATTR) to 14.36.100.50

217    19:01:04.516  01/24/02  Sev=Info/5       IKE/0x6300005D
Client sending a firewall request to concentrator

218    19:01:04.516  01/24/02  Sev=Info/5       IKE/0x6300005C
Firewall Policy: Product=Cisco Integrated Client, Capability=
(Centralized Policy Push).

219    19:01:04.516  01/24/02  Sev=Info/4       IKE/0x63000013
SENDING >>> ISAKMP OAK TRANS *(HASH, ATTR) to 14.36.100.50

220    19:01:04.586  01/24/02  Sev=Info/5       IKE/0x6300002F
Received ISAKMP packet: peer = 14.36.100.50

221    19:01:04.586  01/24/02  Sev=Info/4       IKE/0x63000014
RECEIVING <<< ISAKMP OAK TRANS *(HASH, ATTR) from 14.36.100.50

222    19:01:04.586  01/24/02  Sev=Info/5       IKE/0x63000010
MODE_CFG_REPLY: Attribute = INTERNAL_IPV4_ADDRESS: ,
```

```
value = 10.1.2.1

223    19:01:04.586  01/24/02  Sev=Info/5       IKE/0x63000010
MODE_CFG_REPLY: Attribute = INTERNAL_IPV4_DNS(1): ,
value = 10.1.1.2

224    19:01:04.586  01/24/02  Sev=Info/5       IKE/0x63000010
MODE_CFG_REPLY: Attribute = INTERNAL_IPV4_NBNS(1) (a.k.a. WINS)
: , value = 10.1.1.2

225    19:01:04.586  01/24/02  Sev=Info/5       IKE/0x6300000E
MODE_CFG_REPLY: Attribute = MODECFG_UNITY_DEFDOMAIN: ,
value = cisco.com

226    19:01:04.586  01/24/02  Sev=Info/4       CM/0x63100019
Mode Config data received

227    19:01:04.606  01/24/02  Sev=Info/5       IKE/0x63000055
Received a key request from Driver for IP address 14.36.100.50,
GW IP = 14.36.100.50

228    19:01:04.606  01/24/02  Sev=Info/4       IKE/0x63000013
SENDING >>> ISAKMP OAK QM *(HASH, SA, NON, ID, ID) to 14.36.100.50

229    19:01:04.606  01/24/02  Sev=Info/5       IKE/0x63000055
Received a key request from Driver for IP address 10.10.10.255,
GW IP = 14.36.100.50

230    19:01:04.606  01/24/02  Sev=Info/4       IKE/0x63000013
SENDING >>> ISAKMP OAK QM *(HASH, SA, NON, ID, ID) to 14.36.100.50

231    19:01:04.786  01/24/02  Sev=Info/4       IPSEC/0x63700014
Deleted all keys

232    19:01:05.948  01/24/02  Sev=Info/5       IKE/0x6300002F
Received ISAKMP packet: peer = 14.36.100.50

233    19:01:05.948  01/24/02  Sev=Info/4       IKE/0x63000014
RECEIVING <<< ISAKMP OAK QM *(HASH, SA, NON, ID, ID,
NOTIFY:STATUS_RESP_LIFETIME) from 14.36.100.50

234    19:01:05.948  01/24/02  Sev=Info/5       IKE/0x63000044
RESPONDER-LIFETIME notify has value of 28800 seconds

235    19:01:05.948  01/24/02  Sev=Info/5       IKE/0x63000045
RESPONDER-LIFETIME notify has value of 4608000 kb

236    19:01:05.948  01/24/02  Sev=Info/4       IKE/0x63000013
SENDING >>> ISAKMP OAK QM *(HASH) to 14.36.100.50

237    19:01:05.948  01/24/02  Sev=Info/5       IKE/0x63000058
Loading IPsec SA (Message ID = 0x5B090EB1 OUTBOUND SPI =
0xF39C2217 INBOUND SPI = 0x72FEDC99)

238    19:01:05.948  01/24/02  Sev=Info/5       IKE/0x63000025
Loaded OUTBOUND ESP SPI: 0xF39C2217

239    19:01:05.948  01/24/02  Sev=Info/5       IKE/0x63000026
Loaded INBOUND ESP SPI: 0x72FEDC99

240    19:01:05.948  01/24/02  Sev=Info/4       CM/0x6310001A
One secure connection established

241    19:01:05.988  01/24/02  Sev=Info/6       DIALER/0x63300003
```

```
Connection established.

242    19:01:06.078  01/24/02  Sev=Info/6       DIALER/0x63300008
MAPI32 Information - Outlook not default mail client

243    19:01:06.118  01/24/02  Sev=Info/5       IKE/0x6300002F
Received ISAKMP packet: peer = 14.36.100.50

244    19:01:06.118  01/24/02  Sev=Info/4       IKE/0x63000014
RECEIVING <<< ISAKMP OAK QM *(HASH, SA, NON, ID, ID,
NOTIFY:STATUS_RESP_LIFETIME) from 14.36.100.50

245    19:01:06.118  01/24/02  Sev=Info/5       IKE/0x63000044
RESPONDER-LIFETIME notify has value of 28800 seconds

246    19:01:06.118  01/24/02  Sev=Info/5       IKE/0x63000045
RESPONDER-LIFETIME notify has value of 4608000 kb

247    19:01:06.118  01/24/02  Sev=Info/4       IKE/0x63000013
SENDING >>> ISAKMP OAK QM *(HASH) to 14.36.100.50

248    19:01:06.118  01/24/02  Sev=Info/5       IKE/0x63000058
Loading IPsec SA (Message ID = 0xCFE65CEB OUTBOUND SPI =
0x6AC28ED0 INBOUND SPI = 0x0A5AD786)

249    19:01:06.118  01/24/02  Sev=Info/5       IKE/0x63000025
Loaded OUTBOUND ESP SPI: 0x6AC28ED0

250    19:01:06.118  01/24/02  Sev=Info/5       IKE/0x63000026
Loaded INBOUND ESP SPI: 0x0A5AD786

251    19:01:06.118  01/24/02  Sev=Info/4       CM/0x63100022
Additional Phase 2 SA established.

252    19:01:07.020  01/24/02  Sev=Info/4       IPSEC/0x63700010
Created a new key structure

253    19:01:07.020  01/24/02  Sev=Info/4       IPSEC/0x6370000F
Added key with SPI=0x17229cf3 into key list

254    19:01:07.020  01/24/02  Sev=Info/4       IPSEC/0x63700010
Created a new key structure

255    19:01:07.020  01/24/02  Sev=Info/4       IPSEC/0x6370000F
Added key with SPI=0x99dcfe72 into key list

256    19:01:07.020  01/24/02  Sev=Info/4       IPSEC/0x63700010
Created a new key structure

257    19:01:07.020  01/24/02  Sev=Info/4       IPSEC/0x6370000F
Added key with SPI=0xd08ec26a into key list

258    19:01:07.020  01/24/02  Sev=Info/4       IPSEC/0x63700010
Created a new key structure

259    19:01:07.020  01/24/02  Sev=Info/4       IPSEC/0x6370000F
Added key with SPI=0x86d75a0a into key list

260    19:01:15.032  01/24/02  Sev=Info/6       IKE/0x6300003D
Sending DPD request to 14.36.100.50, seq# = 152233542

261    19:01:15.032  01/24/02  Sev=Info/4       IKE/0x63000013
SENDING >>> ISAKMP OAK INFO *(HASH, NOTIFY:DPD_REQUEST)
to 14.36.100.50
```

```
262    19:01:15.032  01/24/02  Sev=Info/5       IKE/0x6300002F
Received ISAKMP packet: peer = 14.36.100.50

263    19:01:15.032  01/24/02  Sev=Info/4       IKE/0x63000014
RECEIVING <<< ISAKMP OAK INFO *(HASH, NOTIFY:DPD_ACK)
from 14.36.100.50

264    19:01:15.032  01/24/02  Sev=Info/5       IKE/0x6300003F
Received DPD ACK from 14.36.100.50, seq# received = 152233542,
seq# expected = 152233542
```

Informations connexes

- Page de support PIX
- Références des commandes du pare-feu PIX
- Page d'assistance RADIUS
- Page d'assistance des concentrateurs VPN Cisco 3000
- Page d'assistance du Client VPN 3000 Series Cisco
- Page de support pour Protocole IKE/Négociation Ipsec
- Demandes de commentaires (RFC)
- Support technique - Cisco Systems