Configuration d'IPSec depuis un Client VPN Cisco (Solaris) 3.5 sur un concentrateur VPN 3000

Contenu

Introduction

Ce document explique comment configurer le client VPN 3.5 pour Solaris 2.6 pour la connexion à un concentrateur VPN 3000.

Conditions préalables

Conditions requises

Avant d'essayer cette configuration, veuillez vous assurer que vous remplissez les conditions préalables suivantes .

- Cet exemple utilise une clé pré-partagée pour l'authentification de groupe. Le nom d'utilisateur et le mot de passe (authentification étendue) sont vérifiés par rapport à la base de données interne du concentrateur VPN.
- Le client VPN doit être correctement installé. Référez-vous à Installation du client VPN pour Solaris pour plus de détails sur l'installation.
- La connectivité IP doit exister entre le client VPN et l'interface publique du concentrateur VPN. Le masque de sous-réseau et les informations de passerelle doivent être définis correctement.

Components Used

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

- Client VPN Cisco pour Solaris 2.6 version 3.5, image 3DES. (nom de l'image : vpnclient-solaris5.6-3.5.Rel-k9.tar.Z)
- Type de concentrateur VPN Cisco : 3005 Bootcode Rev : Altiga Networks/VPN Concentrator Version 2.2.int_9 Jan 19 2000 05:36:41 Software Rev : Cisco Systems, Inc./VPN série 3000 Concentrator Version 3.1.Rel 06 août 2001 13:47:37

Les informations présentées dans ce document ont été créées à partir de périphériques dans un environnement de laboratoire spécifique. All of the devices used in this document started with a cleared (default) configuration. Si vous travaillez dans un réseau opérationnel, assurez-vous de bien comprendre l'impact potentiel de toute commande avant de l'utiliser.

Conventions

Pour plus d'informations sur les conventions des documents, référez-vous aux Conventions utilisées pour les conseils techniques de Cisco.

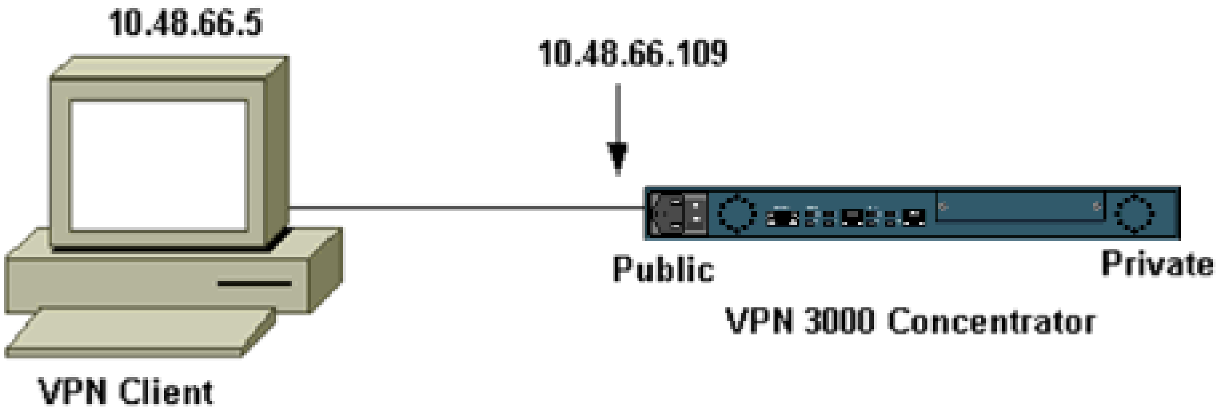
Configuration

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

Remarque : Pour en savoir plus sur les commandes utilisées dans le présent document, utilisez l'outil de recherche de commandes (clients inscrits seulement).

Diagramme du réseau

Ce document utilise la configuration réseau indiquée dans le diagramme suivant :



Remarque : pour que le client VPN 3.5 se connecte au concentrateur VPN, vous devez disposer de la version 3.0 ou ultérieure sur le concentrateur.

Configurations

Création d'un profil utilisateur pour la connexion

Les profils utilisateur sont stockés dans le répertoire /etc/CiscoSystemsVPNlient/Profiles. Ces fichiers texte ont une extension .pcf et contiennent les paramètres nécessaires pour établir une connexion à un concentrateur VPN. Vous pouvez créer un nouveau fichier ou en modifier un existant. Vous devez trouver un exemple de profil, sample.pcf, dans le répertoire des profils. Cet exemple suit l'utilisation de ce fichier pour créer un nouveau profil nommé toCORPORATE.pcf.

```
[cholera]: ~ > cd /etc/CiscoSystemsVPNClient/Profiles/
[cholera]: /etc/CiscoSystemsVPNClient/Profiles > cp sample.pcf toCORPORATE.pcf
```

Vous pouvez utiliser votre éditeur de texte préféré pour modifier ce nouveau fichier, toCORPORATE.pcf. Avant toute modification, le fichier ressemble à ce qui suit.

Remarque : si vous voulez utiliser IPSec sur la traduction d'adresses de réseau (NAT), l'entrée EnableNat dans la configuration ci-dessous doit indiquer « EnableNat=1 » au lieu de « EnableNat=0. »

```
[main]
Description=sample user profile
Host=10.7.44.1
AuthType=1
GroupName=monkeys
EnableISPConnect=0
ISPConnectType=0
ISPConnect=
ISPCommand=
Username=chimchim
SaveUserPassword=0
EnableBackup=0
BackupServer=
EnableNat=0
CertStore=0
CertName=
CertPath=
CertSubjectName=
CertSerialHash=00000000000000000000000000000000
DHGroup=2
ForceKeepAlives=0
```

Référez-vous à Profils utilisateur pour obtenir une description des mots clés du profil utilisateur.

Pour configurer correctement votre profil, vous devez connaître au minimum vos valeurs équivalentes pour les informations suivantes.

- Nom d'hôte ou adresse IP publique du concentrateur VPN (10.48.66.109)
- Nom du groupe (RemoteClient)
- Mot de passe du groupe (cisco)
- Nom d'utilisateur (joe)

Modifiez le fichier avec vos informations afin qu'il soit similaire à ce qui suit.

```
[main]
Description=Connection to the corporate
Host=10.48.66.109
AuthType=1
GroupName=RemoteClient
GroupPwd=cisco
```

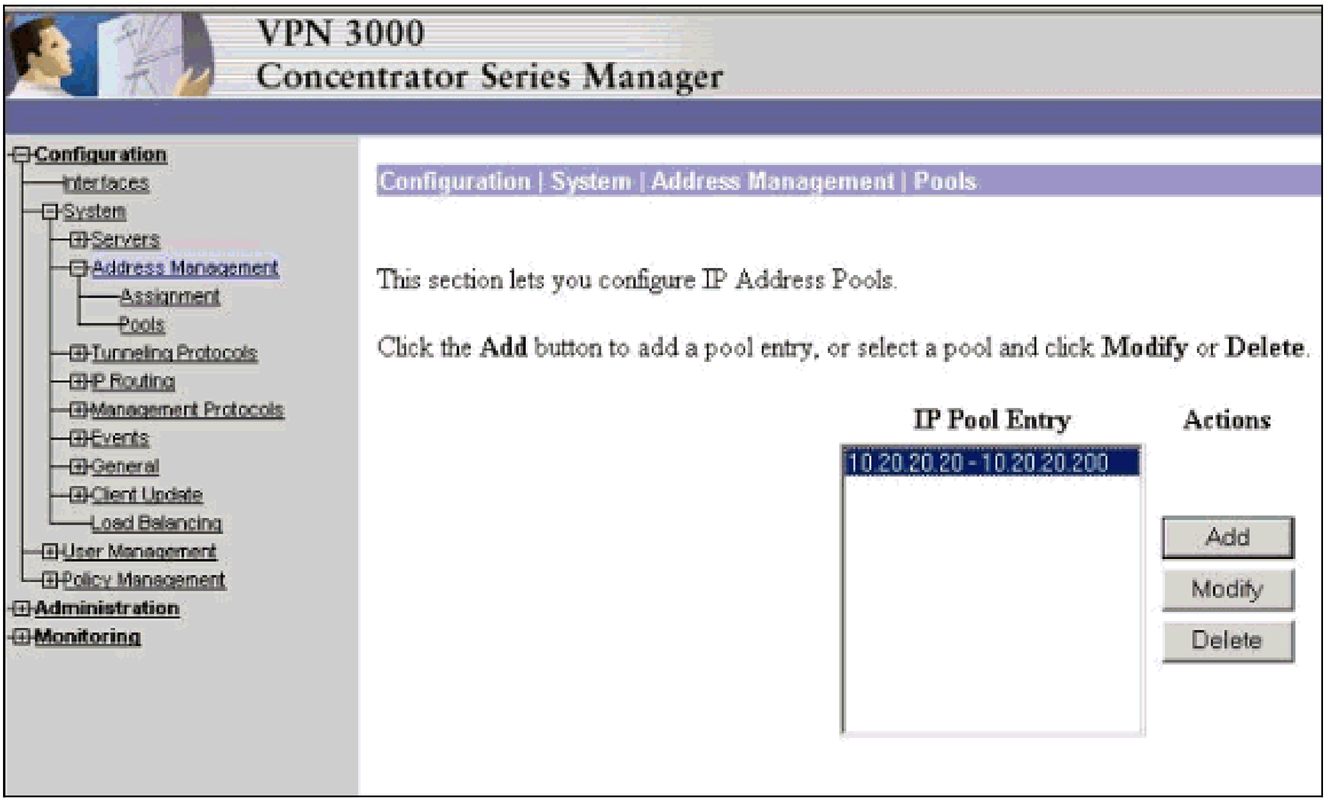
```
EnableISPConnect=0
ISPConnectType=0
ISPConnect=
ISPCommand=
Username=joe
SavePassword=0
EnableBackup=0
BackupServer=
EnableNat=0
CertStore=0
CertName=
CertPath=
CertSubjectName=
CertSerialHash=00000000000000000000000000000000
DHGroup=2
ForceKeepAlives=0
```

Configuration du concentrateur VPN

Procédez comme suit pour configurer le concentrateur VPN.

Remarque : En raison de l'espace limité, les captures d'écran ne montrent que des zones partielles ou pertinentes.

1. Attribuez le pool d'adresses. Pour attribuer une plage d'adresses IP disponible, pointez un navigateur sur l'interface interne du concentrateur VPN et sélectionnez **Configuration > System > Address Management > Pools**. Cliquez sur **Add**. Spécifiez une plage d'adresses IP qui ne sont en conflit avec aucun autre périphérique du réseau interne.

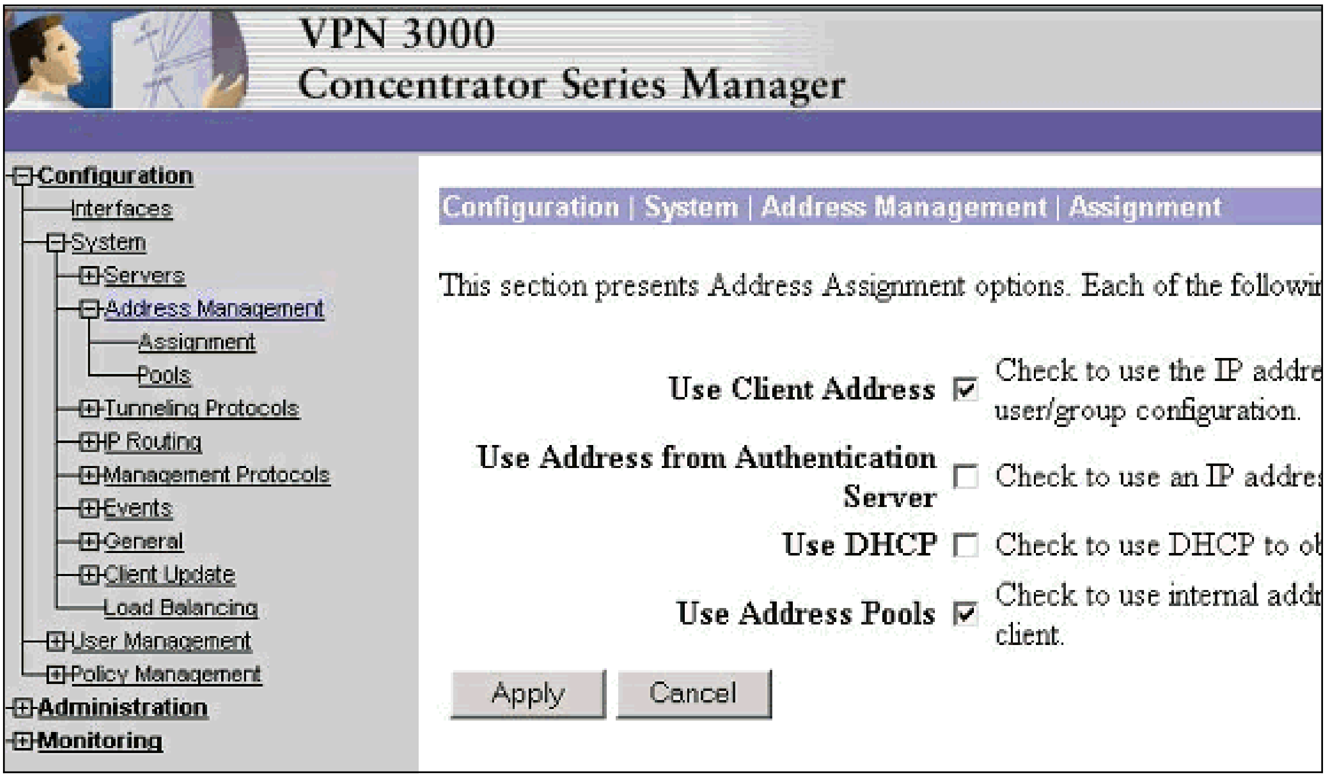


This section lets you configure IP Address Pools.

Click the **Add** button to add a pool entry, or select a pool and click **Modify** or **Delete**.

10.20.20.20 - 10.20.20.200

2. Pour indiquer au concentrateur VPN d'utiliser le pool, sélectionnez **Configuration > System > Address Management > Assignment**, cochez la case **Use Address Pools**, puis cliquez sur **Apply**.

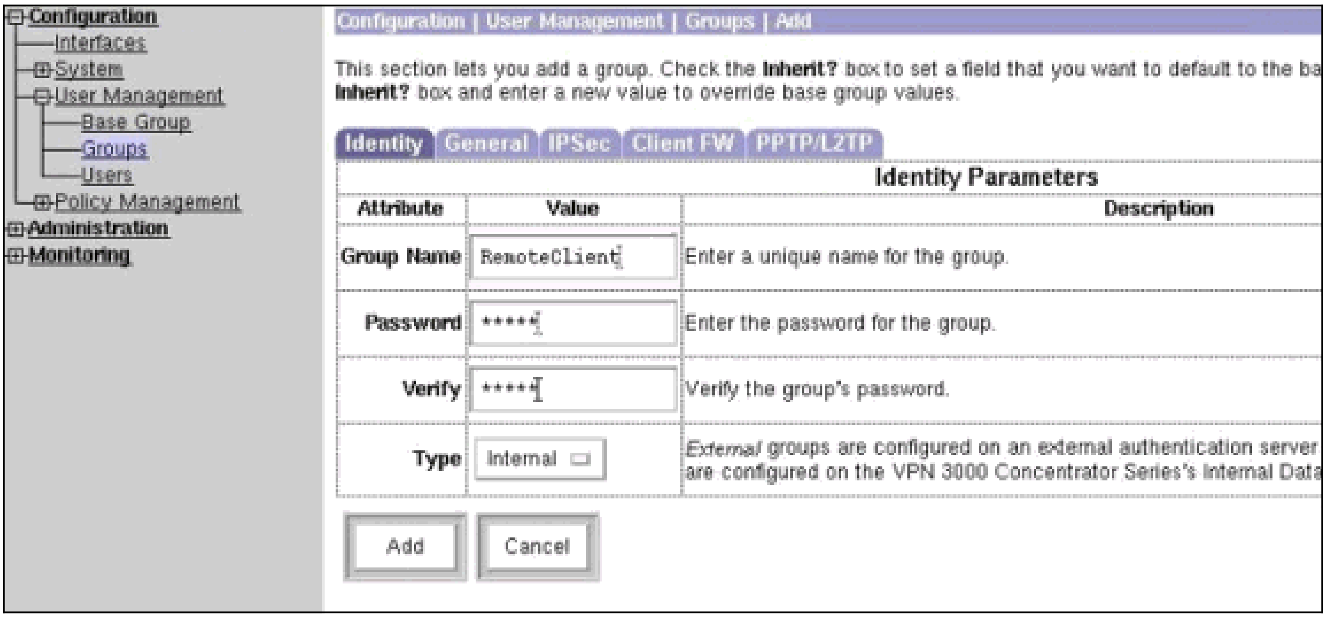


Configuration | System | Address Management | Assignment

This section presents Address Assignment options. Each of the followi

Use Client Address	☑	Check to use the IP addre user/group configuration.
Use Address from Authentication Server	□	Check to use an IP addres
Use DHCP	□	Check to use DHCP to ol
Use Address Pools	☑	Check to use internal addr client.

3. Ajoutez un groupe et un mot de passe. Sélectionnez **Configuration > User Management > Groups**, puis cliquez sur **Add Group**. Entrez les informations correctes, puis cliquez sur **Ajouter** pour soumettre les informations.Cet exemple utilise un groupe nommé « RemoteClient » avec le mot de passe « cisco ».

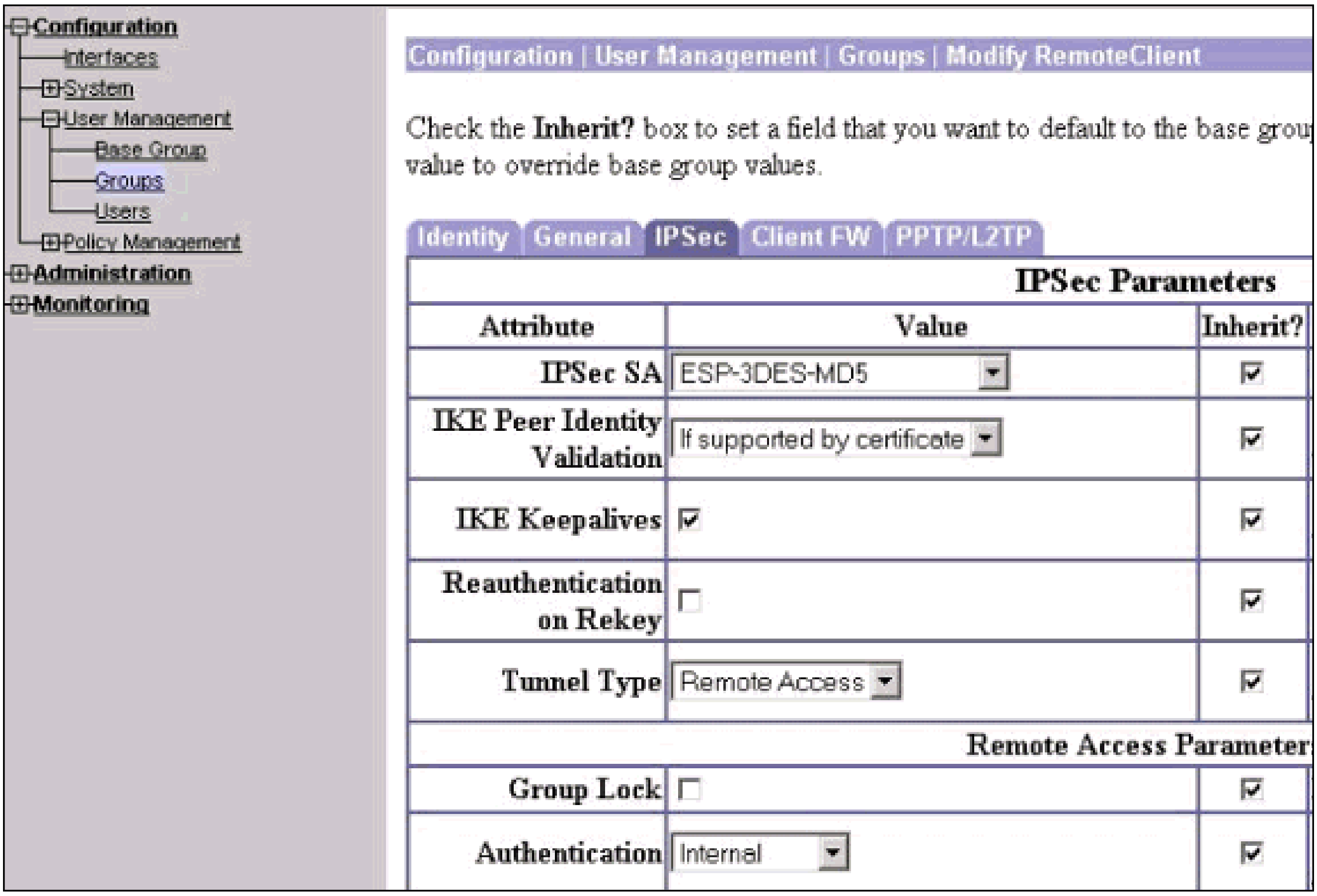


Configuration | User Management | Groups | Add

This section lets you add a group. Check the **Inherit?** box to set a field that you want to default to the ba **Inherit?** box and enter a new value to override base group values.

Identity Parameters		
Attribute	**Value**	**Description**
Group Name	RemoteClient	Enter a unique name for the group.
Password	*****	Enter the password for the group.
Verify	*****	Verify the group's password.
Type	Internal	*External* groups are configured on an external authentication server are configured on the VPN 3000 Concentrator Series's Internal Data

4. Dans l'onglet IPSec du groupe, vérifiez que l'authentification est définie sur **Interne**.

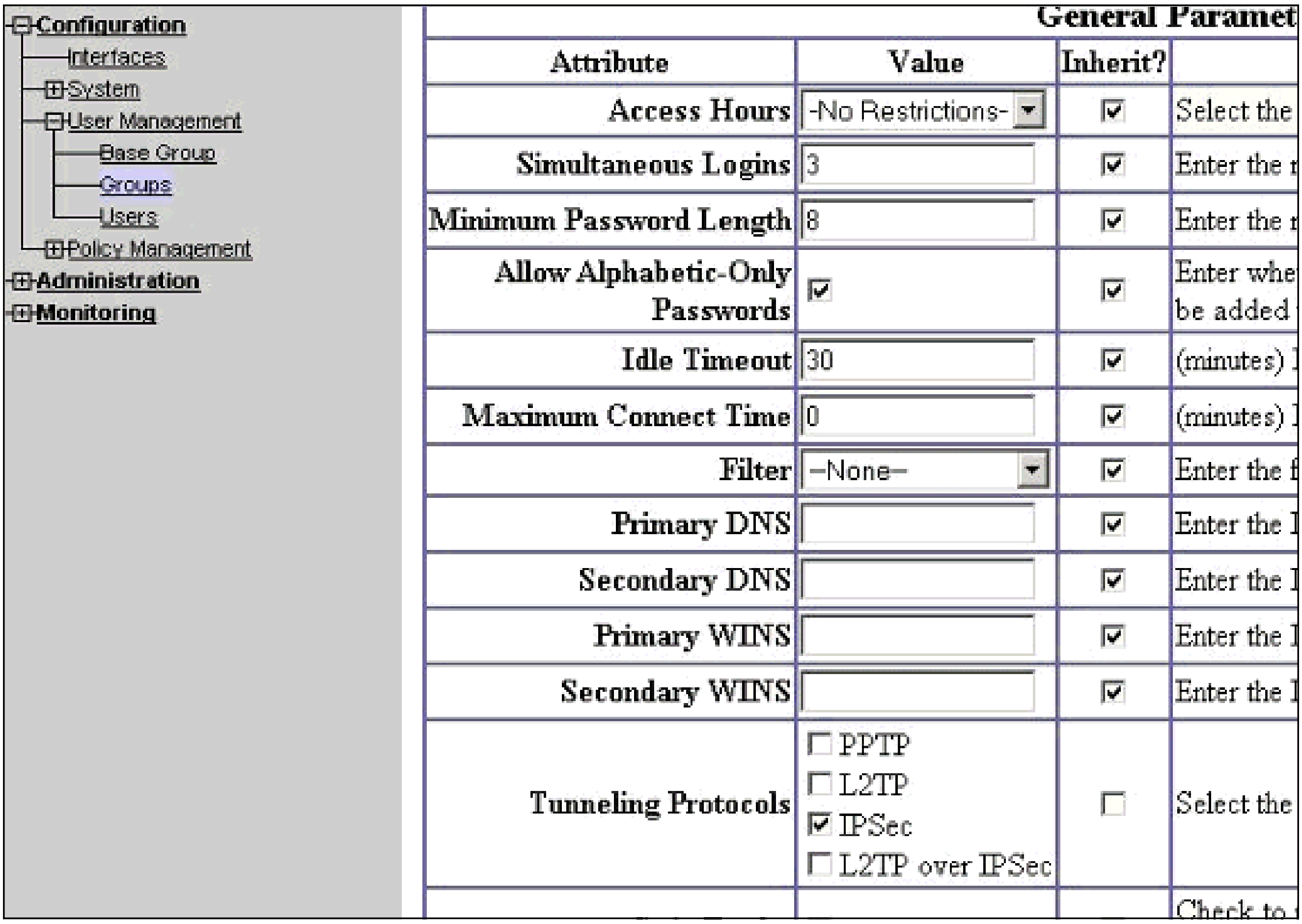


Configuration | User Management | Groups | Modify RemoteClient

Check the **Inherit?** box to set a field that you want to default to the base grou value to override base group values.

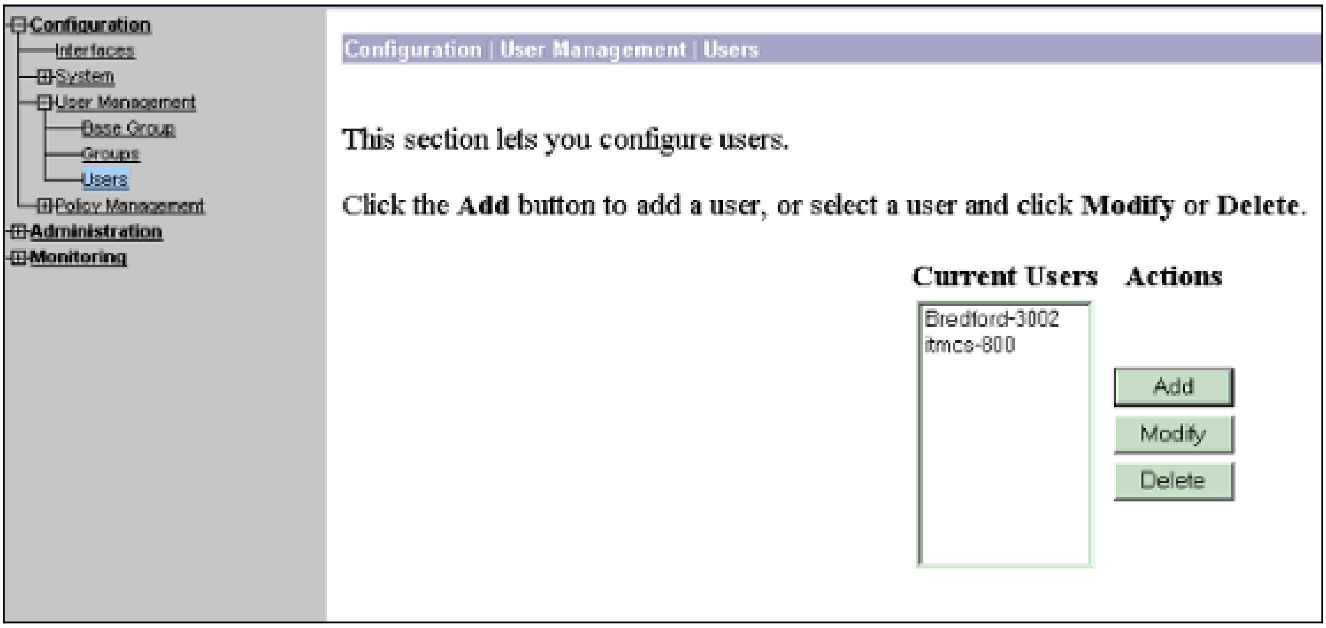
IPSec Parameters		
Attribute	**Value**	**Inherit?**
IPSec SA	ESP-3DES-MD5	☑
IKE Peer Identity Validation	If supported by certificate	☑
IKE Keepalives	☑	☑
Reauthentication on Rekey	□	☑
Tunnel Type	Remote Access	☑
Remote Access Parameter		
Group Lock	□	☑
Authentication	Internal	☑

5. Dans l'onglet Général du groupe, vérifiez que **IPSec** est sélectionné comme protocole de tunnellisation.



General Paramet			
Attribute	**Value**	**Inherit?**	
Access Hours	-No Restrictions-	☑	Select the
Simultaneous Logins	3	☑	Enter the
Minimum Password Length	8	☑	Enter the
Allow Alphabetic-Only Passwords	☑	☑	Enter whe be added
Idle Timeout	30	☑	(minutes)
Maximum Connect Time	0	☑	(minutes)
Filter	--None--	☑	Enter the
Primary DNS		☑	Enter the
Secondary DNS		☑	Enter the
Primary WINS		☑	Enter the
Secondary WINS		☑	Enter the
Tunneling Protocols	□ PPTP □ L2TP ☑ IPSec □ L2TP over IPSec	□	Select the
			Check to

6. Pour ajouter l'utilisateur au concentrateur VPN, sélectionnez **Configuration > User Management > Users**, puis cliquez sur **Add**.



Configuration | User Management | Users

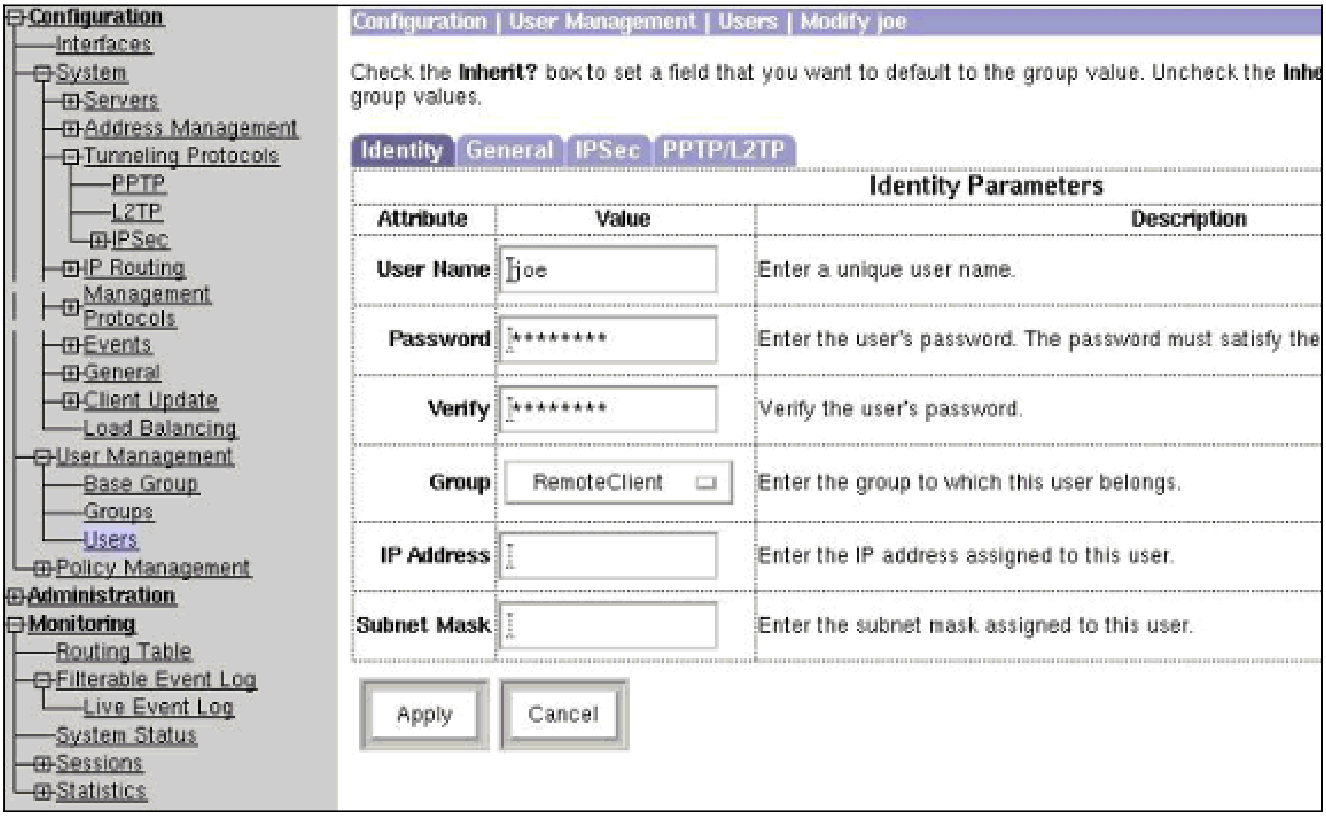
This section lets you configure users.

Click the **Add** button to add a user, or select a user and click **Modify** or **Delete**.

Current Users **Actions**

Bredford-3002
itmcs-800

7. Entrez les informations correctes pour le groupe, puis cliquez sur **Apply** pour soumettre les informations.



Configuration | User Management | Users | Modify joe

Check the **Inherit?** box to set a field that you want to default to the group value. Uncheck the **Inhe** group values.

Identity Parameters

Attribute	Value	Description
User Name	joe	Enter a unique user name.
Password	********	Enter the user's password. The password must satisfy the
Verify	********	Verify the user's password.
Group	RemoteClient	Enter the group to which this user belongs.
IP Address		Enter the IP address assigned to this user.
Subnet Mask		Enter the subnet mask assigned to this user.

Vérification

Connexion au concentrateur VPN

Maintenant que le client VPN et le concentrateur sont configurés, le nouveau profil doit fonctionner pour se connecter au concentrateur VPN.

```
91 [cholera]: /etc/CiscoSystemsVPNClient > vpnclient connect toCORPORATE
Cisco Systems VPN Client Version 3.5 (Rel)
Copyright (C) 1998-2001 Cisco Systems, Inc. All Rights Reserved.
Client Type(s): Solaris
```

```
Running on: SunOS 5.6 Generic_105181-11 sun4u

Initializing the IPSec link.
Contacting the security gateway at 10.48.66.109
Authenticating user.
User Authentication for toCORPORATE...

Enter Username and Password.

Username [Joe]:
Password []:
Contacting the security gateway at 10.48.66.109
Your link is secure.
IPSec tunnel information.
Client address: 10.20.20.20
Server address: 10.48.66.109
Encryption: 168-bit 3-DES
Authentication: HMAC-MD5
IP Compression: None
NAT passthrough is inactive.
Local LAN Access is disabled.

^Z
Suspended

[cholera]: /etc/CiscoSystemsVPNClient > bg
[1]    vpnclient connect toCORPORATE &
(The process is made to run as background process)

[cholera]: /etc/CiscoSystemsVPNClient > vpnclient disconnect

Cisco Systems VPN Client Version 3.5 (Rel)
Copyright (C) 1998-2001 Cisco Systems, Inc. All Rights Reserved.
Client Type(s): Solaris
Running on: SunOS 5.6 Generic_105181-11 sun4u

Your IPSec link has been disconnected.
Disconnecting the IPSEC link.
[cholera]: /etc/CiscoSystemsVPNClient >
[1]    Exit -56                      vpnclient connect toCORPORATE

[cholera]: /etc/CiscoSystemsVPNClient >
```

Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Déboguages

Pour activer les débogages, utilisez la commande **ipseclog**. Un exemple est présenté ci-dessous.

```
[cholera]: /etc/CiscoSystemsVPNClient > ipseclog /tmp/clientlog
```

Déboguer sur le client lors de la connexion au concentrateur

```
[cholera]: /etc/CiscoSystemsVPNClient > cat /tmp/clientlog
```

```
1      17:08:49.821  01/25/2002  Sev=Info/4     CLI/0x43900002
Started vpnclient:
Cisco Systems VPN Client Version 3.5 (Rel)
Copyright (C) 1998-2001 Cisco Systems, Inc. All Rights Reserved.
Client Type(s): Solaris
Running on: SunOS 5.6 Generic_105181-11 sun4u

2      17:08:49.855  01/25/2002  Sev=Info/4     CVPND/0x4340000F
Started cvpnd:
Cisco Systems VPN Client Version 3.5 (Rel)
Copyright (C) 1998-2001 Cisco Systems, Inc. All Rights Reserved.
Client Type(s): Solaris
Running on: SunOS 5.6 Generic_105181-11 sun4u

3      17:08:49.857  01/25/2002  Sev=Info/4     IPSEC/0x43700013
Delete internal key with SPI=0xb0f0d0c0

4      17:08:49.857  01/25/2002  Sev=Info/4     IPSEC/0x4370000C
Key deleted by SPI 0xb0f0d0c0

5      17:08:49.858  01/25/2002  Sev=Info/4     IPSEC/0x43700013
Delete internal key with SPI=0x637377d3

6      17:08:49.858  01/25/2002  Sev=Info/4     IPSEC/0x4370000C
Key deleted by SPI 0x637377d3

7      17:08:49.859  01/25/2002  Sev=Info/4     IPSEC/0x43700013
Delete internal key with SPI=0x9d4d2b9d

8      17:08:49.859  01/25/2002  Sev=Info/4     IPSEC/0x4370000C
Key deleted by SPI 0x9d4d2b9d

9      17:08:49.859  01/25/2002  Sev=Info/4     IPSEC/0x43700013
Delete internal key with SPI=0x5facd5bf

10     17:08:49.860  01/25/2002  Sev=Info/4     IPSEC/0x4370000C
Key deleted by SPI 0x5facd5bf

11     17:08:49.860  01/25/2002  Sev=Info/4     IPSEC/0x43700009
IPSec driver already started

12     17:08:49.861  01/25/2002  Sev=Info/4     IPSEC/0x43700014
Deleted all keys

13     17:08:49.861  01/25/2002  Sev=Info/4     IPSEC/0x43700014
Deleted all keys

14     17:08:49.862  01/25/2002  Sev=Info/4     IPSEC/0x43700009
IPSec driver already started

15     17:08:49.863  01/25/2002  Sev=Info/4     IPSEC/0x43700009
IPSec driver already started

16     17:08:49.863  01/25/2002  Sev=Info/4     IPSEC/0x43700014
Deleted all keys

17     17:08:50.873  01/25/2002  Sev=Info/4     CM/0x43100002
Begin connection process

18     17:08:50.883  01/25/2002  Sev=Info/4     CM/0x43100004
Establish secure connection using Ethernet

19     17:08:50.883  01/25/2002  Sev=Info/4     CM/0x43100026
Attempt connection with server "10.48.66.109"
```

```
20     17:08:50.883  01/25/2002  Sev=Info/6     IKE/0x4300003B
Attempting to establish a connection with 10.48.66.109.

21     17:08:51.099  01/25/2002  Sev=Info/4     IKE/0x43000013
SENDING >>> ISAKMP OAK AG (SA, KE, NON, ID, VID, VID, VID) to
10.48.66.109

22     17:08:51.099  01/25/2002  Sev=Info/4     IPSEC/0x43700009
IPSec driver already started

23     17:08:51.100  01/25/2002  Sev=Info/4     IPSEC/0x43700014
Deleted all keys

24     17:08:51.400  01/25/2002  Sev=Info/5     IKE/0x4300002F
Received ISAKMP packet: peer = 10.48.66.109

25     17:08:51.400  01/25/2002  Sev=Info/4     IKE/0x43000014
RECEIVING <<< ISAKMP OAK AG (SA, KE, NON, ID, HASH, VID, VID, VID,
VID) from 10.48.66.109

26     17:08:51.400  01/25/2002  Sev=Info/5     IKE/0x43000059
Vendor ID payload = 12F5F28C457168A9702D9FE274CC0100

27     17:08:51.400  01/25/2002  Sev=Info/5     IKE/0x43000001
Peer is a Cisco-Unity compliant peer

28     17:08:51.400  01/25/2002  Sev=Info/5     IKE/0x43000059
Vendor ID payload = 09002689DFD6B712

29     17:08:51.400  01/25/2002  Sev=Info/5     IKE/0x43000059
Vendor ID payload = AFCAD71368A1F1C96B8696FC77570100

30     17:08:51.400  01/25/2002  Sev=Info/5     IKE/0x43000001
Peer supports DPD

31     17:08:51.400  01/25/2002  Sev=Info/5     IKE/0x43000059
Vendor ID payload = 1F07F70EAA6514D3B0FA96542A500301

32     17:08:51.505  01/25/2002  Sev=Info/4     IKE/0x43000013
SENDING >>> ISAKMP OAK AG *(HASH, NOTIFY:STATUS_INITIAL_CONTACT)
to 10.48.66.109

33     17:08:51.510  01/25/2002  Sev=Info/5     IKE/0x4300002F
Received ISAKMP packet: peer = 10.48.66.109

34     17:08:51.511  01/25/2002  Sev=Info/4     IKE/0x43000014
RECEIVING <<< ISAKMP OAK TRANS *(HASH, ATTR) from 10.48.66.109

35     17:08:51.511  01/25/2002  Sev=Info/4     CM/0x43100015
Launch xAuth application

36     17:08:56.333  01/25/2002  Sev=Info/4     CM/0x43100017
xAuth application returned

37     17:08:56.334  01/25/2002  Sev=Info/4     IKE/0x43000013
SENDING >>> ISAKMP OAK TRANS *(HASH, ATTR) to 10.48.66.109

38     17:08:56.636  01/25/2002  Sev=Info/5     IKE/0x4300002F
Received ISAKMP packet: peer = 10.48.66.109

39     17:08:56.637  01/25/2002  Sev=Info/4     IKE/0x43000014
RECEIVING <<< ISAKMP OAK TRANS *(HASH, ATTR) from 10.48.66.109
```

```
40     17:08:56.637  01/25/2002  Sev=Info/4     CM/0x4310000E
Established Phase 1 SA.  1 Phase 1 SA in the system

41     17:08:56.639  01/25/2002  Sev=Info/4     IKE/0x43000013
SENDING >>> ISAKMP OAK TRANS *(HASH, ATTR) to 10.48.66.109

42     17:08:56.639  01/25/2002  Sev=Info/4     IKE/0x43000013
SENDING >>> ISAKMP OAK TRANS *(HASH, ATTR) to 10.48.66.109

43     17:08:56.645  01/25/2002  Sev=Info/5     IKE/0x4300002F
Received ISAKMP packet: peer = 10.48.66.109

44     17:08:56.646  01/25/2002  Sev=Info/4     IKE/0x43000014
RECEIVING <<< ISAKMP OAK TRANS *(HASH, ATTR) from 10.48.66.109

45     17:08:56.646  01/25/2002  Sev=Info/5     IKE/0x43000010
MODE_CFG_REPLY: Attribute = INTERNAL_IPV4_ADDRESS: ,
value = 10.20.20.20

46     17:08:56.646  01/25/2002  Sev=Info/5     IKE/0x4300000D
MODE_CFG_REPLY: Attribute = MODECFG_UNITY_SAVEPWD: ,
value = 0x00000000

47     17:08:56.646  01/25/2002  Sev=Info/5     IKE/0x4300000D
MODE_CFG_REPLY: Attribute = MODECFG_UNITY_PFS: ,
value = 0x00000000

48     17:08:56.646  01/25/2002  Sev=Info/5     IKE/0x4300000E
MODE_CFG_REPLY: Attribute = APPLICATION_VERSION,
value = Cisco Systems, Inc./VPN 3000 Concentrator Series
Version 3.1.Rel built by vmurphy on Aug 06 2001 13:47:37

49     17:08:56.648  01/25/2002  Sev=Info/4     CM/0x43100019
Mode Config data received

50     17:08:56.651  01/25/2002  Sev=Info/5     IKE/0x43000055
Received a key request from Driver for IP address 10.48.66.109,
GW IP = 10.48.66.109

51     17:08:56.652  01/25/2002  Sev=Info/4     IKE/0x43000013
SENDING >>> ISAKMP OAK QM *(HASH, SA, NON, ID, ID) to 10.48.66.109

52     17:08:56.653  01/25/2002  Sev=Info/5     IKE/0x43000055
Received a key request from Driver for IP address 10.10.10.255,
GW IP = 10.48.66.109

53     17:08:56.653  01/25/2002  Sev=Info/4     IKE/0x43000013
SENDING >>> ISAKMP OAK QM *(HASH, SA, NON, ID, ID) to 10.48.66.109

54     17:08:56.663  01/25/2002  Sev=Info/5     IKE/0x4300002F
Received ISAKMP packet: peer = 10.48.66.109

55     17:08:56.663  01/25/2002  Sev=Info/4     IKE/0x43000014
RECEIVING <<< ISAKMP OAK INFO *(HASH, NOTIFY:STATUS_RESP_LIFETIME)
from 10.48.66.109

56     17:08:56.663  01/25/2002  Sev=Info/5     IKE/0x43000044
RESPONDER-LIFETIME notify has value of 86400 seconds

57     17:08:56.663  01/25/2002  Sev=Info/5     IKE/0x43000046
This SA has already been alive for 6 seconds, setting expiry
to 86394 seconds from now

58     17:08:56.666  01/25/2002  Sev=Info/5     IKE/0x4300002F
```

```
Received ISAKMP packet: peer = 10.48.66.109

59     17:08:56.666  01/25/2002  Sev=Info/4     IKE/0x43000014
RECEIVING <<< ISAKMP OAK QM *(HASH, SA, NON, ID, ID,
NOTIFY:STATUS_RESP_LIFETIME) from 10.48.66.109

60     17:08:56.667  01/25/2002  Sev=Info/5     IKE/0x43000044
RESPONDER-LIFETIME notify has value of 28800 seconds

61     17:08:56.667  01/25/2002  Sev=Info/4     IKE/0x43000013
SENDING >>> ISAKMP OAK QM *(HASH) to 10.48.66.109

62     17:08:56.667  01/25/2002  Sev=Info/5     IKE/0x43000058
Loading IPsec SA (Message ID = 0x4CEF4B32 OUTBOUND SPI =
0x5EAD41F5 INBOUND SPI = 0xE66C759A)

63     17:08:56.668  01/25/2002  Sev=Info/5     IKE/0x43000025
Loaded OUTBOUND ESP SPI: 0x5EAD41F5

64     17:08:56.669  01/25/2002  Sev=Info/5     IKE/0x43000026
Loaded INBOUND ESP SPI: 0xE66C759A

65     17:08:56.669  01/25/2002  Sev=Info/4     CM/0x4310001A
One secure connection established

66     17:08:56.674  01/25/2002  Sev=Info/5     IKE/0x4300002F
Received ISAKMP packet: peer = 10.48.66.109

67     17:08:56.675  01/25/2002  Sev=Info/4     IKE/0x43000014
RECEIVING <<< ISAKMP OAK QM *(HASH, SA, NON, ID, ID,
NOTIFY:STATUS_RESP_LIFETIME) from 10.48.66.109

68     17:08:56.675  01/25/2002  Sev=Info/5     IKE/0x43000044
RESPONDER-LIFETIME notify has value of 28800 seconds

69     17:08:56.675  01/25/2002  Sev=Info/4     IKE/0x43000013
SENDING >>> ISAKMP OAK QM *(HASH) to 10.48.66.109

70     17:08:56.675  01/25/2002  Sev=Info/5     IKE/0x43000058
Loading IPsec SA (Message ID = 0x88E9321A OUTBOUND SPI =
0x333B4239 INBOUND SPI = 0x6B040746)

71     17:08:56.677  01/25/2002  Sev=Info/5     IKE/0x43000025
Loaded OUTBOUND ESP SPI: 0x333B4239

72     17:08:56.677  01/25/2002  Sev=Info/5     IKE/0x43000026
Loaded INBOUND ESP SPI: 0x6B040746

73     17:08:56.678  01/25/2002  Sev=Info/4     CM/0x43100022
Additional Phase 2 SA established.

74     17:08:57.752  01/25/2002  Sev=Info/4     IPSEC/0x43700014
Deleted all keys

75     17:08:57.752  01/25/2002  Sev=Info/4     IPSEC/0x43700010
Created a new key structure

76     17:08:57.752  01/25/2002  Sev=Info/4     IPSEC/0x4370000F
Added key with SPI=0x5ead41f5 into key list

77     17:08:57.753  01/25/2002  Sev=Info/4     IPSEC/0x43700010
Created a new key structure

78     17:08:57.753  01/25/2002  Sev=Info/4     IPSEC/0x4370000F
```

```
Added key with SPI=0xe66c759a into key list

79     17:08:57.754  01/25/2002  Sev=Info/4     IPSEC/0x43700010
Created a new key structure

80     17:08:57.754  01/25/2002  Sev=Info/4     IPSEC/0x4370000F
Added key with SPI=0x333b4239 into key list

81     17:08:57.754  01/25/2002  Sev=Info/4     IPSEC/0x43700010
Created a new key structure

82     17:08:57.755  01/25/2002  Sev=Info/4     IPSEC/0x4370000F
Added key with SPI=0x6b040746 into key list

83     17:09:13.752  01/25/2002  Sev=Info/6     IKE/0x4300003D
Sending DPD request to 10.48.66.109, seq# = 2948297981

84     17:09:13.752  01/25/2002  Sev=Info/4     IKE/0x43000013
SENDING >>> ISAKMP OAK INFO *(HASH, NOTIFY:DPD_REQUEST)
to 10.48.66.109

85     17:09:13.758  01/25/2002  Sev=Info/5     IKE/0x4300002F
Received ISAKMP packet: peer = 10.48.66.109

86     17:09:13.758  01/25/2002  Sev=Info/4     IKE/0x43000014
RECEIVING <<< ISAKMP OAK INFO *(HASH, NOTIFY:DPD_ACK)
from 10.48.66.109

87     17:09:13.759  01/25/2002  Sev=Info/5     IKE/0x4300003F
Received DPD ACK from 10.48.66.109, seq# received = 2948297981,
seq# expected = 2948297981
```

debug on the client when disconnecting

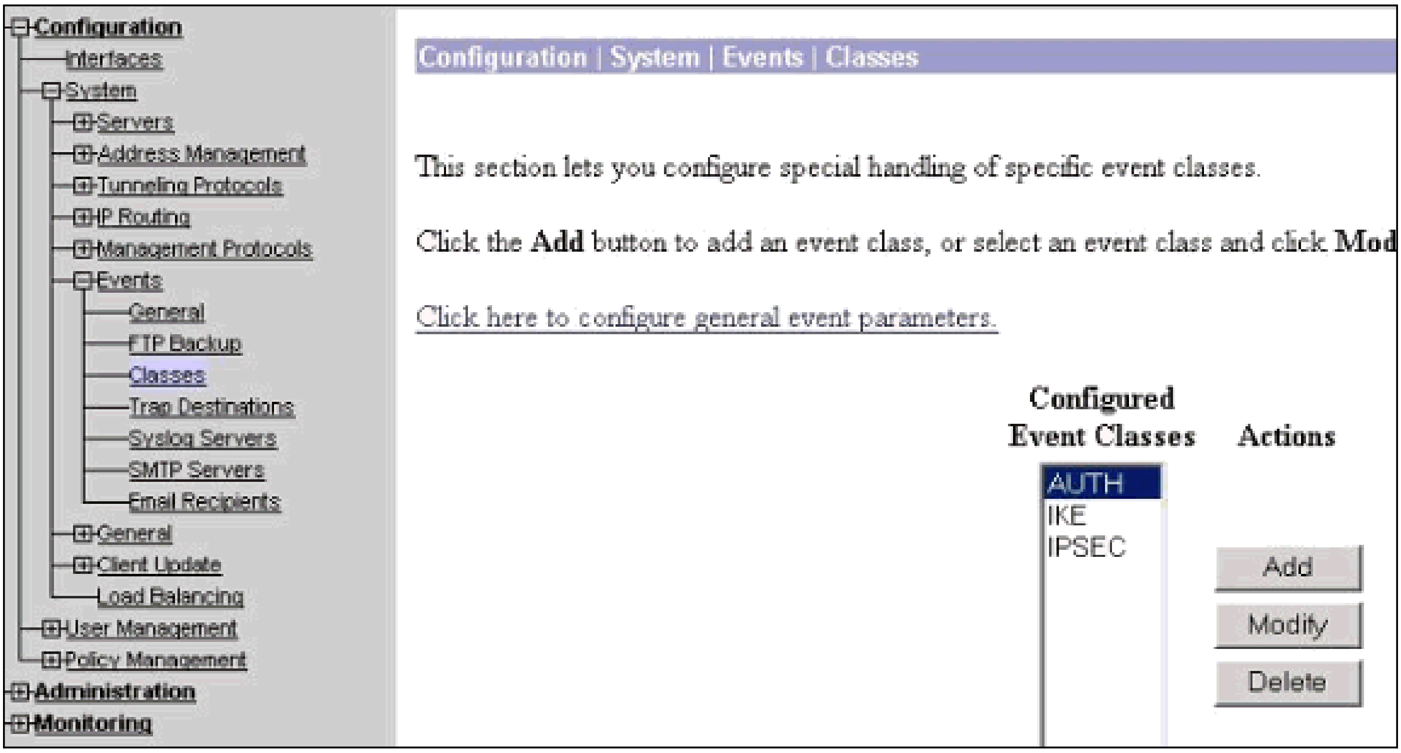
```
88     17:09:16.366  01/25/2002  Sev=Info/4     CLI/0x43900002
Started vpnclient:
Cisco Systems VPN Client Version 3.5 (Rel)
Copyright (C) 1998-2001 Cisco Systems, Inc. All Rights Reserved.
Client Type(s): Solaris
Running on: SunOS 5.6 Generic_105181-11 sun4u

89     17:09:16.367  01/25/2002  Sev=Info/4     CM/0x4310000A
Secure connections terminated

90     17:09:16.367  01/25/2002  Sev=Info/5     IKE/0x43000018
Deleting IPsec SA: (OUTBOUND SPI = 333B4239 INBOUND SPI = 6B040746)

91     17:09:16.368  01/25/2002  Sev=Info/4     IKE/0x43000013
SENDING >>> ISAKMP OAK INFO *(HASH, DEL) to 10.48.66.109

92     17:09:16.369  01/25/2002  Sev=Info/5     IKE/0x43000018
Deleting IPsec SA: (OUTBOUND SPI = 5EAD41F5 INBOUND SPI = E66C759A)

93     17:09:16.369  01/25/2002  Sev=Info/4     IKE/0x43000013
SENDING >>> ISAKMP OAK INFO *(HASH, DEL) to 10.48.66.109

94     17:09:16.370  01/25/2002  Sev=Info/4     IKE/0x43000013
SENDING >>> ISAKMP OAK INFO *(HASH, DEL) to 10.48.66.109

95     17:09:16.371  01/25/2002  Sev=Info/4     CM/0x43100013
Phase 1 SA deleted cause by DEL_REASON_RESET_SADB.
0 Phase 1 SA currently in the system
```

```
96     17:09:16.371  01/25/2002  Sev=Info/5     CM/0x43100029
Initializing CVPNDrv

97     17:09:16.371  01/25/2002  Sev=Info/6     CM/0x43100035
Tunnel to headend device 10.48.66.109 disconnected:
duration: 0 days 0:0:20

98     17:09:16.375  01/25/2002  Sev=Info/5     CM/0x43100029
Initializing CVPNDrv

99     17:09:16.377  01/25/2002  Sev=Info/5     IKE/0x4300002F
Received ISAKMP packet: peer = 10.48.66.109

100    17:09:16.377  01/25/2002  Sev=Warning/2  IKE/0x83000061
Attempted incoming connection from 10.48.66.109. Inbound
connections are not allowed.

101    17:09:17.372  01/25/2002  Sev=Info/4     IPSEC/0x43700013
Delete internal key with SPI=0x6b040746

102    17:09:17.372  01/25/2002  Sev=Info/4     IPSEC/0x43700013
Delete internal key with SPI=0x333b4239

103    17:09:17.373  01/25/2002  Sev=Info/4     IPSEC/0x43700013
Delete internal key with SPI=0xe66c759a

104    17:09:17.373  01/25/2002  Sev=Info/4     IPSEC/0x43700013
Delete internal key with SPI=0x5ead41f5

105    17:09:17.373  01/25/2002  Sev=Info/4     IPSEC/0x43700014
Deleted all keys

106    17:09:17.374  01/25/2002  Sev=Info/4     IPSEC/0x43700009
IPSec driver already started

107    17:09:17.374  01/25/2002  Sev=Info/4     IPSEC/0x43700014
Deleted all keys

108    17:09:17.375  01/25/2002  Sev=Info/4     IPSEC/0x43700009
IPSec driver already started

109    17:09:17.375  01/25/2002  Sev=Info/4     IPSEC/0x43700014
Deleted all keys

110    17:09:17.375  01/25/2002  Sev=Info/4     IPSEC/0x43700009
IPSec driver already started

111    17:09:17.376  01/25/2002  Sev=Info/4     IPSEC/0x43700014
Deleted all keys
```

Débogues sur le concentrateur VPN

Sélectionnez **Configuration > System > Events > Classes** pour activer le débogage suivant en cas d'échec de connexion d'événement.

- **AUTH** - Gravité du journal 1-13
- **IKE** - Gravité du journal 1-6
- **IPSEC** - Gravité du journal 1-6



Configuration | System | Events | Classes

This section lets you configure special handling of specific event classes.

Click the **Add** button to add an event class, or select an event class and click **Mod**

Click here to configure general event parameters.

Vous pouvez afficher le journal en sélectionnant **Monitoring > Event Log**.

Informations connexes

- Page d'assistance des concentrateurs VPN Cisco 3000
- Page d'assistance du Client VPN 3000 Series Cisco
- Page d'assistance IPsec
- Support technique - Cisco Systems