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

Contenu

Introduction

Ce document montre comment configurer le client vpn 3.5 pour que le Solaris 2.6 se connecte à un concentrateur VPN 3000.

Conditions préalables

Conditions requises

Avant de tenter cette configuration, assurez-vous s'il vous plaît que vous rencontrez les conditions préalables suivantes.

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

Composants utilisés

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

- Client VPN Cisco pour la version 3.5 de Solaris 2.6, image 3DES. (nom d'image : vpnclient-solaris5.6-3.5.Rel-k9.tar.Z)
- Type de concentrateur de Cisco VPN : 3005 Bootcode Rév : Logiciel Rév de la version 2.2.int_9 le 19 janvier 2000 05:36:41 de concentrateur d'Altiga Networks/VPN : Cisco Systems, Inc. /VPN 3000 gammes de concentrateurs de la version 3.1.Rel le 6 août 2001 13:47:37

Les informations présentées dans ce document ont été créées à partir de périphériques dans un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). 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.

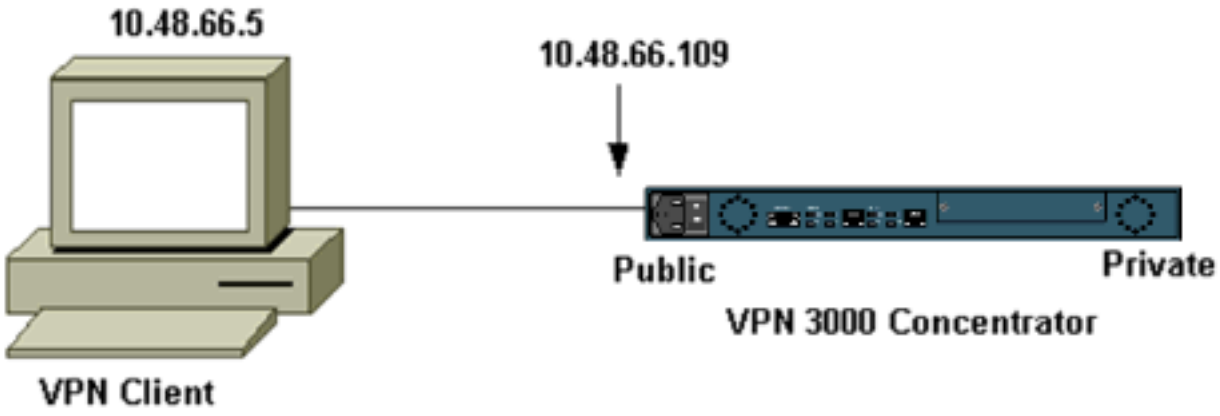
Configurez

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

Remarque: Pour obtenir des informations supplémentaires sur les commandes utilisées dans ce document, utilisez l'Outil de recherche de commande (clients enregistrés seulement).

Diagramme du réseau

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



Remarque: Pour le client 3.5 VPN à connecter au concentrateur VPN, vous avez besoin de la version 3.0 ou plus tard du concentrateur.

Configurations

Création d'un profil utilisateur pour la connexion

Les profils utilisateurs sont enregistrés dans le répertoire de /etc/CiscoSystemsVPNClient/Profiles. Ces fichiers texte ont une extension .pcf et contiennent des paramètres requis ont établi une connexion à un concentrateur VPN. Vous pouvez créer un nouveau fichier ou éditer existant. Vous devriez trouver un exemple de profil, sample.pcf, dans le répertoire de profil. Cet exemple suit l'utilisation de ce fichier de créer un nouveau profil nommé toCORPORATE.pcf.

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

Vous pouvez employer votre éditeur de texte préféré pour éditer ce nouveau fichier, toCORPORATE.pcf. Avant toutes les modifications, le fichier ressemble au suivant.

Remarque: Si vous voulez utiliser IPSec au-dessus de Traduction d'adresses de réseau (NAT), l'entrée d'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 les profils de toUser pour une description des mots clé de profil utilisateur.

Pour configurer avec succès votre profil, vous devez connaître, comme minimum, vos valeurs équivalentes pour les informations suivantes.

- Le nom d'hôte ou adresse IP publique du concentrateur VPN (10.48.66.109)
- Le nom de groupe (RemoteClient)
- Le mot de passe de groupe (Cisco)
- Le nom d'utilisateur (Joe)

Éditez le fichier avec vos informations de sorte qu'elles soient semblables au suivant.

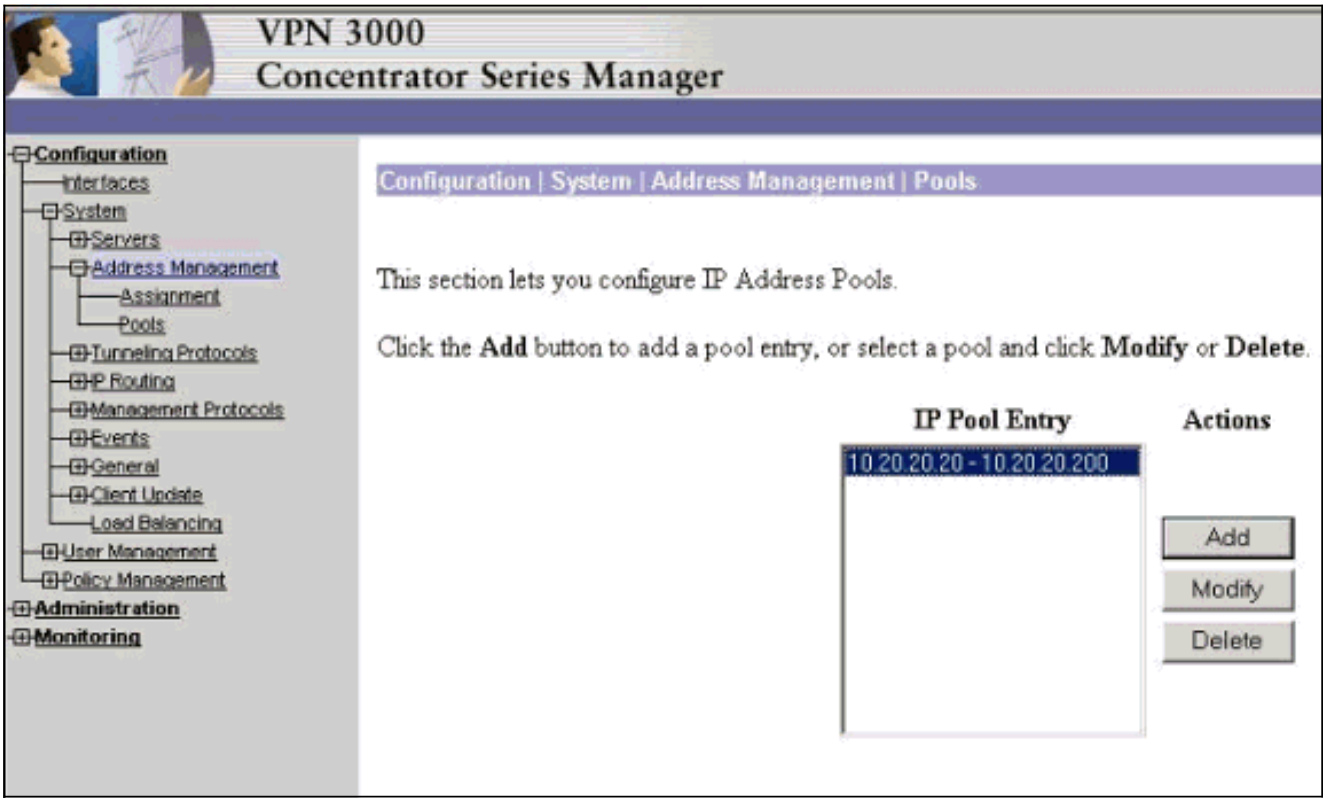
```
[main]
Description=Connection to the corporate
Host=10.48.66.109 AuthType=1 GroupName=RemoteClient GroupPwd=cisco EnableISPConnect=0
ISPConnectType=0 ISPConnect= ISPCommand= Username=joe SaveUserPassword=0 EnableBackup=0
BackupServer= EnableNat=0 CertStore=0 CertName= CertPath= CertSubjectName=
CertSerialHash=00000000000000000000000000000000 DHGroup=2 ForceKeepAlives=0
```

Configurer le concentrateur VPN

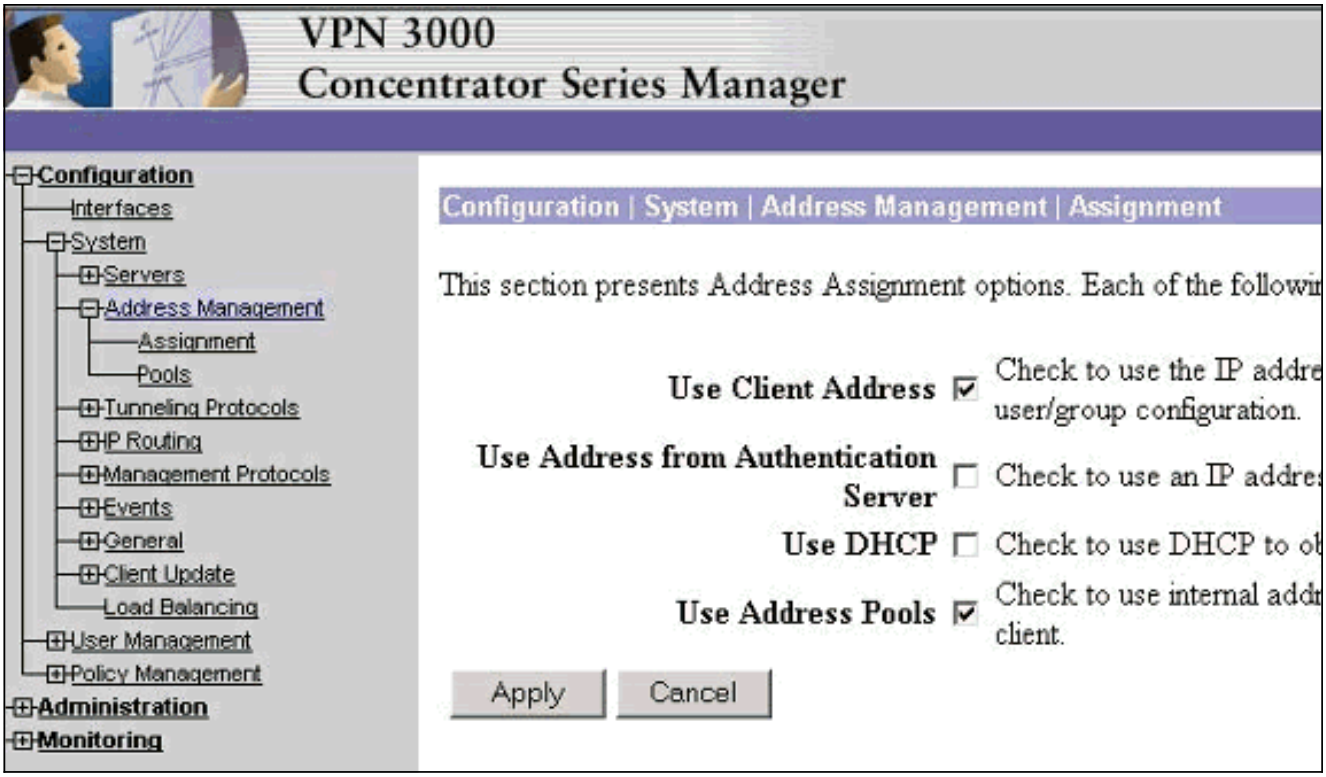
Employez les étapes suivantes pour configurer le concentrateur VPN.

Remarque: En raison des limites de l'espace, les captures d'écran affichent seulement des zones partielles ou appropriées.

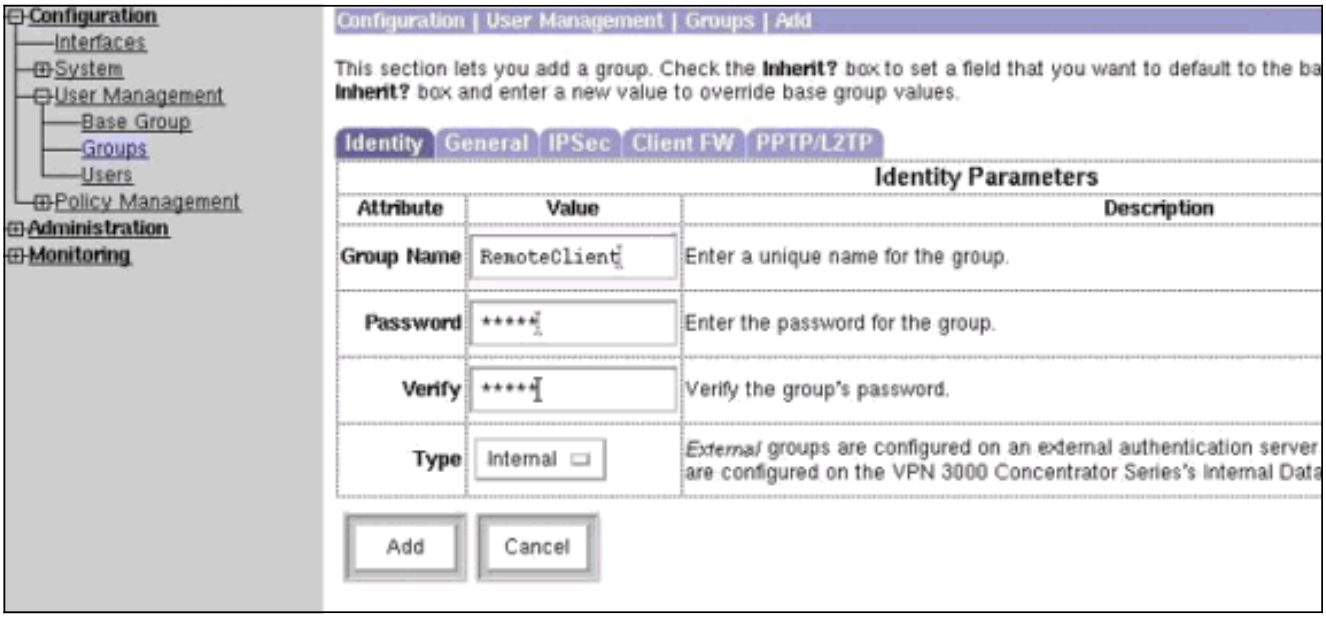
1. Affectez le groupe d'adresses. Pour assigner une plage disponible des adresses IP, indiquez un navigateur l'interface interne du concentrateur VPN et sélectionnez les **>Pools de configuration > de système > de gestion d'adresses**. Cliquez sur **Add**. Spécifiez une plage des adresses IP qui ne sont en conflit avec aucun autre périphérique sur le réseau intérieur.



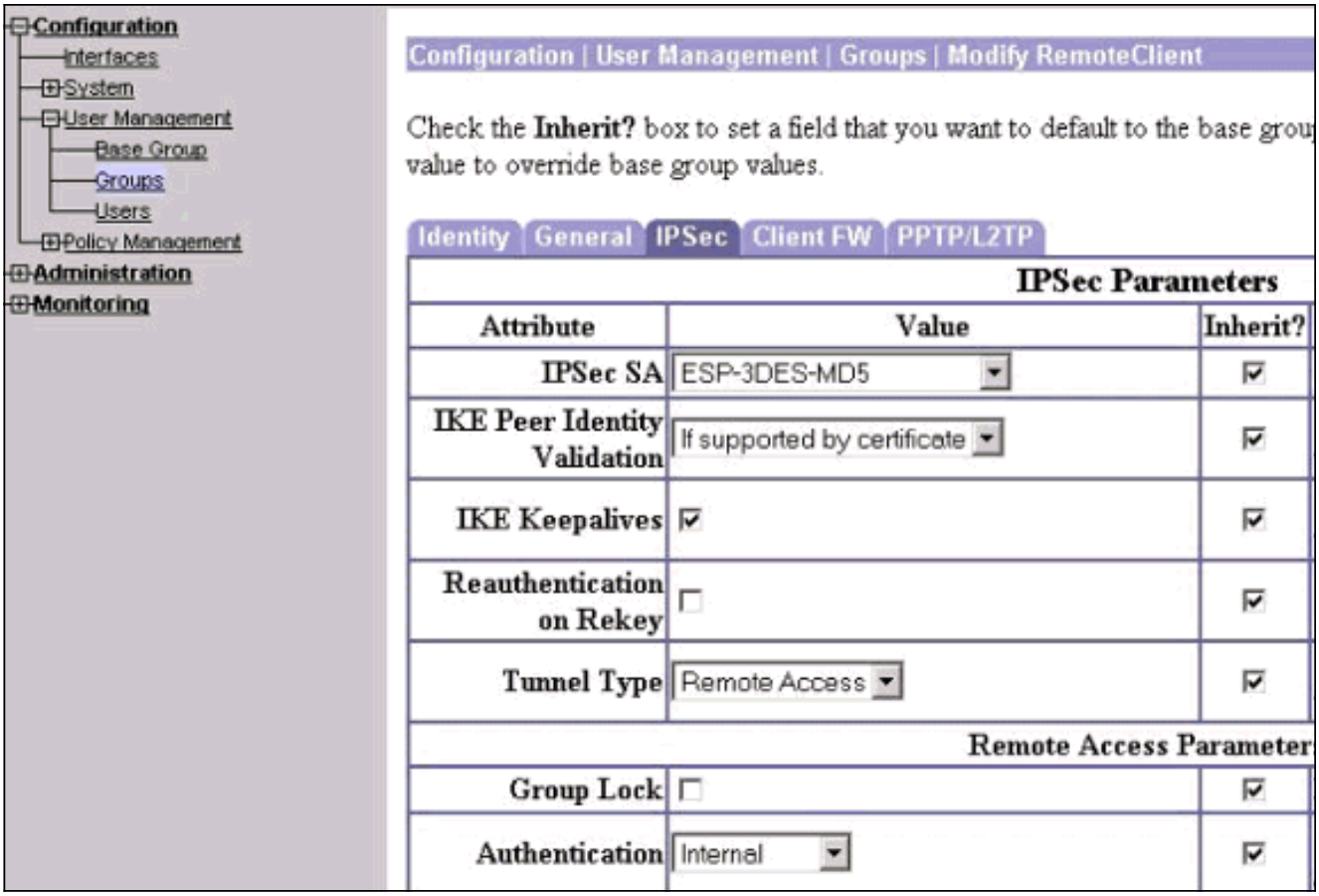
2. Pour dire le concentrateur VPN d'utiliser le groupe, la **configuration** choisie **> le système > la gestion d'adresses > l'affectation**, cochent la case de **pools d'adresses d'utilisation**, et puis cliquent sur
Apply.



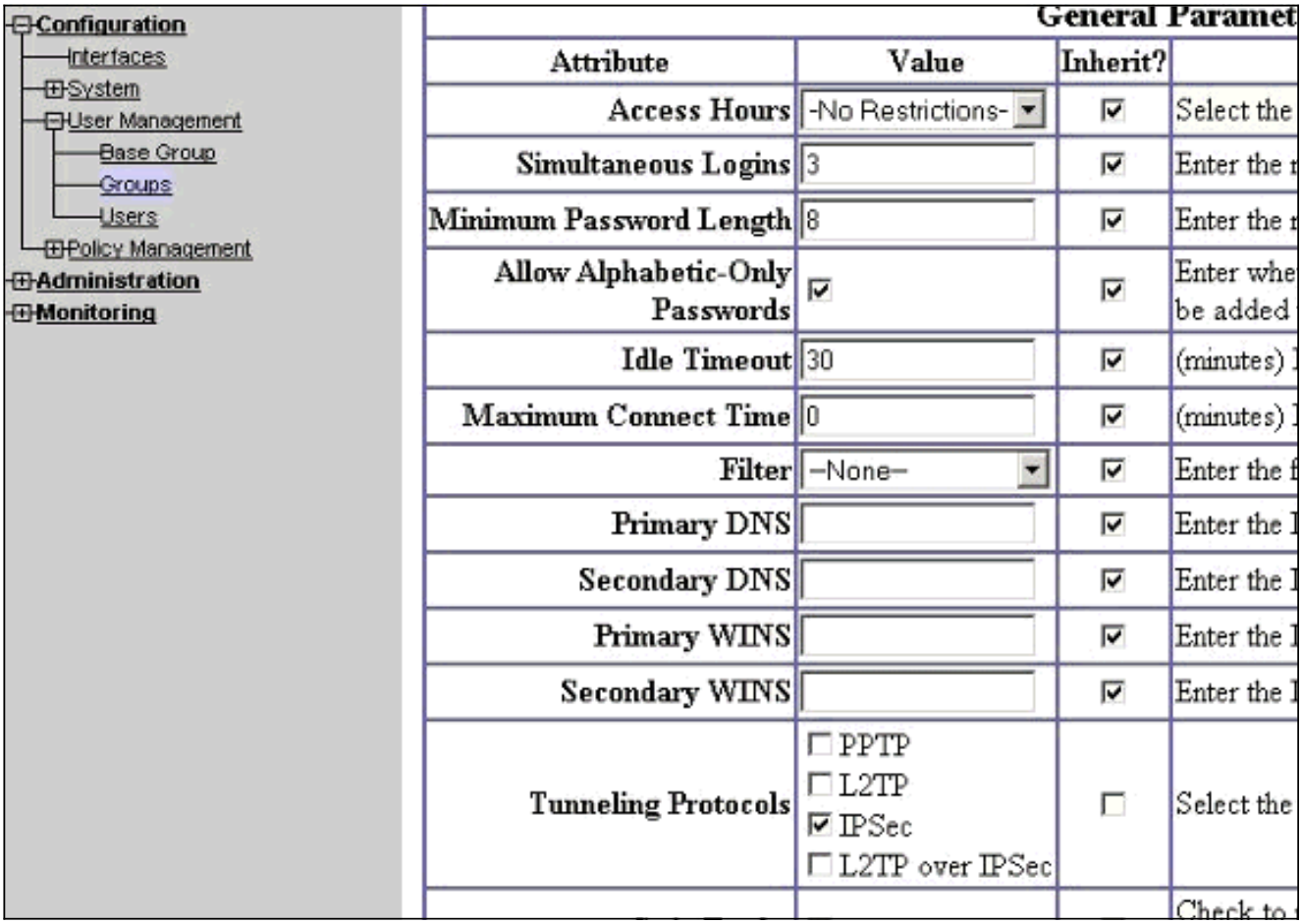
3. Ajoutez un groupe et un mot de passe. **Le Configuration > User Management > Groups** choisi, et cliquent sur Add alors le **groupe**. Écrivez les informations correctes, et puis cliquez sur Add pour soumettre les informations.Cet exemple utilise un groupe nommé « RemoteClient » avec un mot de passe de « Cisco. »



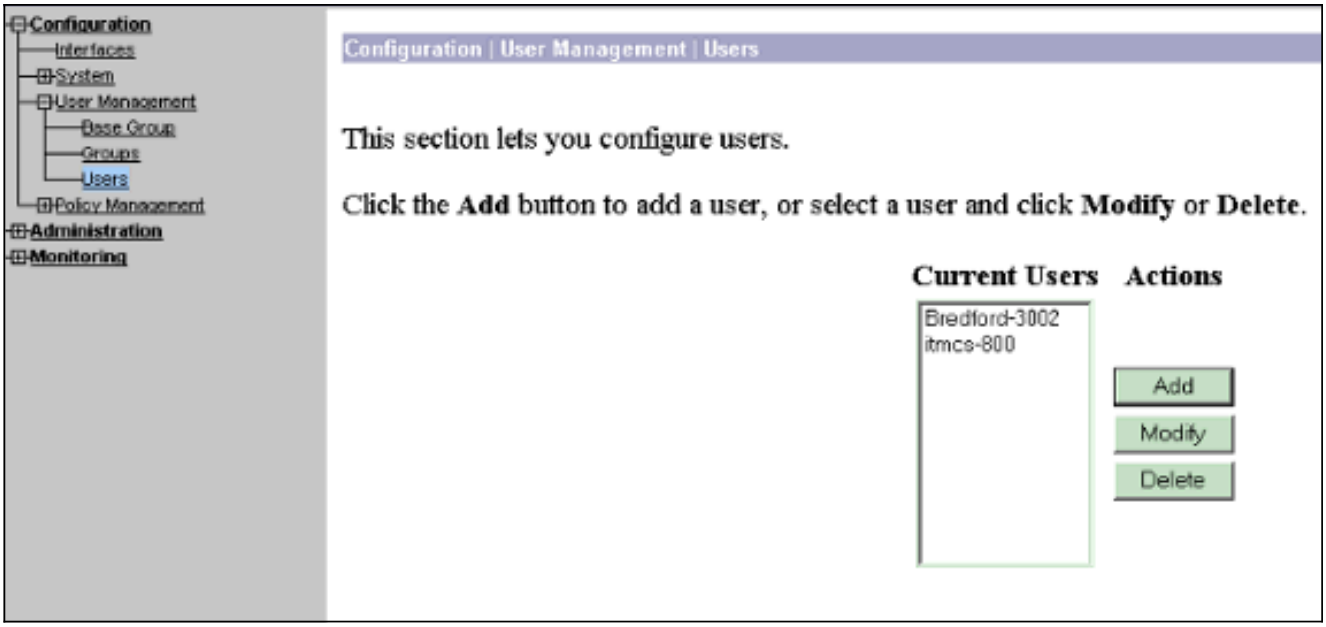
4. Sur l'onglet d'IPSec du groupe, vérifiez que l'authentification est placée à **interne**.



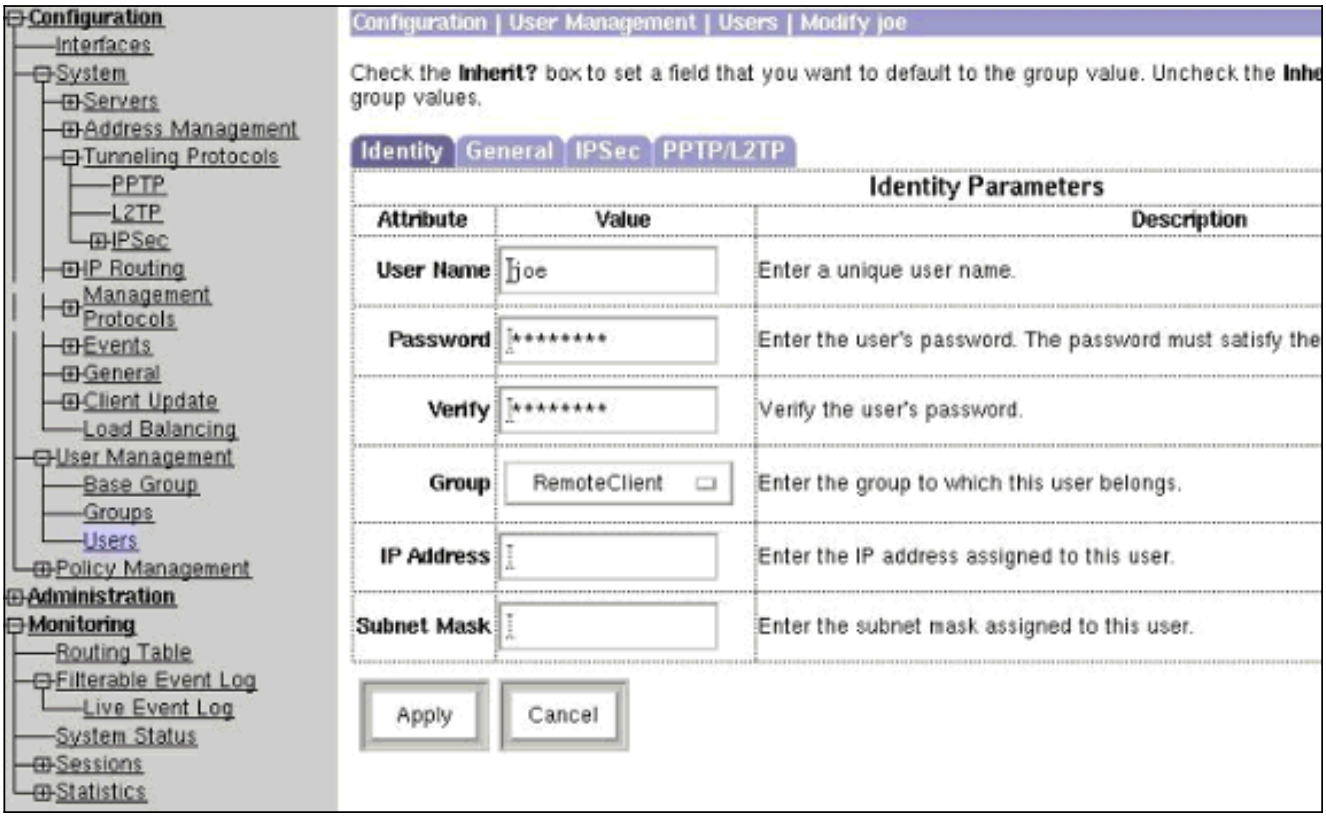
5. Sur l'onglet Général du groupe, vérifiez qu'**IPSec** est sélectionné comme protocoles de Tunnellisation.



6. Pour ajouter l'utilisateur au concentrateur VPN, au **Configuration > User Management** choisi **> aux utilisateurs**, et puis cliquer sur
Add.



7. Écrivez les informations correctes pour le groupe, et puis cliquez sur Apply pour soumettre les
informations.



Vérifiez

Se connecter au concentrateur VPN

Maintenant que le client vpn et le concentrateur sont configurés, le nouveau profil devrait 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 >
```

Dépannez

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

Debugs

Pour activer met au point, utilise la commande d'**ipseclog**. Un exemple est affiché ci-dessous.

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

Debug sur le client en se connectant 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
```

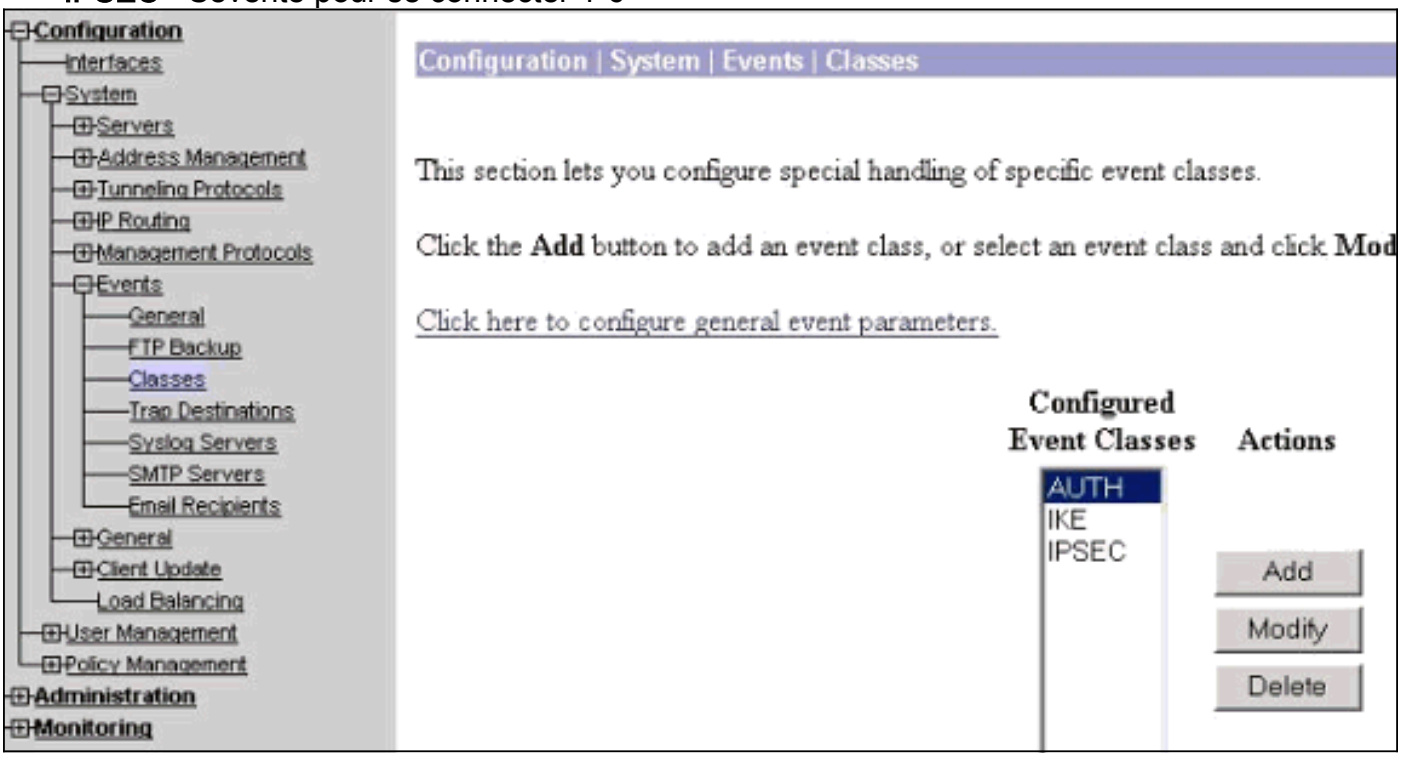
01/25/2002 Sev=Info/4 IKE/0x43000014 RECEIVING <<< ISAKMP OAK TRANS *(HASH, ATTR) from 10.48.66.109 35 17:08:51.511 01/25/2002 Sev=Info/4 CM/0x43100015 Launch xAuth application 36 17:08:56.333 01/25/2002 Sev=Info/4 CM/0x43100017 xAuth application returned 37 17:08:56.334 01/25/2002 Sev=Info/4 IKE/0x43000013 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
```

Debugs sur le concentrateur VPN

La configuration > le système > les événements > les classes choisis pour activer le suivant mettent au point s'il y a des défaillances de connexion d'événement.

- **AUTHENTIQUE** - Sévérité pour se connecter 1-13
- **IKE** - Sévérité pour se connecter 1-6
- **IPSEC** - Sévérité pour se connecter 1-6



Vous pouvez visualiser le log en sélectionnant la **surveillance > le journal d'événements**.

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