Exemple de configuration d'IPSec avec un client VPN (adresse IP affectée de manière statique/dynamique) en concentrateur VPN 3000

Contenu

Introduction

Cet exemple de configuration montre comment former un tunnel IPsec à partir d'un PC qui exécute le client VPN Cisco (4.x et versions ultérieures) (adresse IP attribuée statique/dynamique) vers un concentrateur VPN Cisco 3000 afin de permettre à l'utilisateur d'accéder en toute sécurité au réseau à l'intérieur du concentrateur VPN.

Référez-vous à Utilisation de Cisco Secure ACS pour Windows avec le concentrateur VPN 3000 - IPSec afin d'en savoir plus sur le même scénario avec l'authentification RADIUS à l'aide de Cisco ACS. Référez-vous à Configuration du concentrateur Cisco VPN 3000 avec MS RADIUS afin d'en savoir plus sur le même scénario avec MS-RADIUS Authentication.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

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

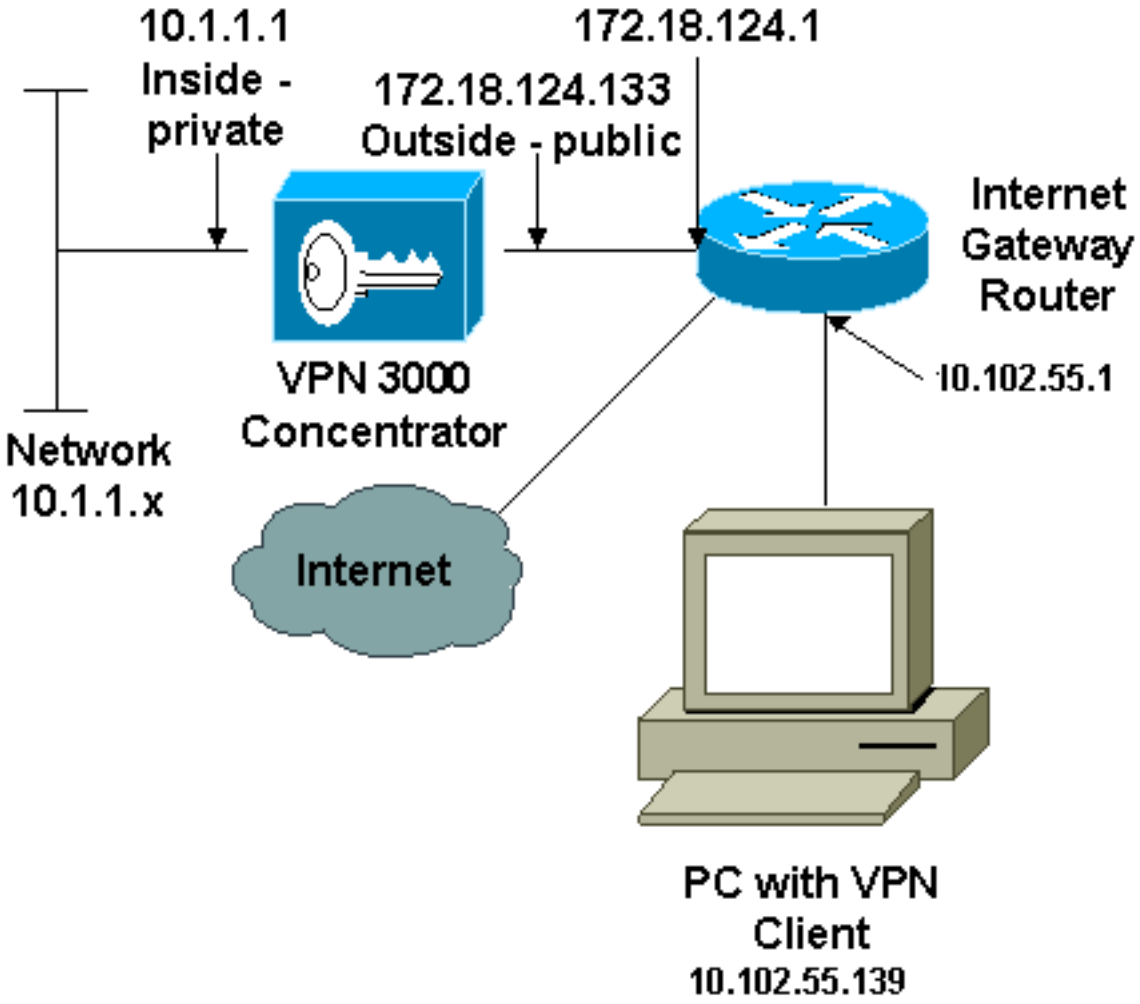
- Concentrateur VPN Cisco 3030 version 4.1.7.A
- Client VPN Cisco Versions 4.x et ultérieures

Remarque : Cette configuration a été récemment testée à l'aide de la version 4.7.2.H du concentrateur VPN Cisco.

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.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



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 utilisées dans un environnement de travaux pratiques.

Conventions

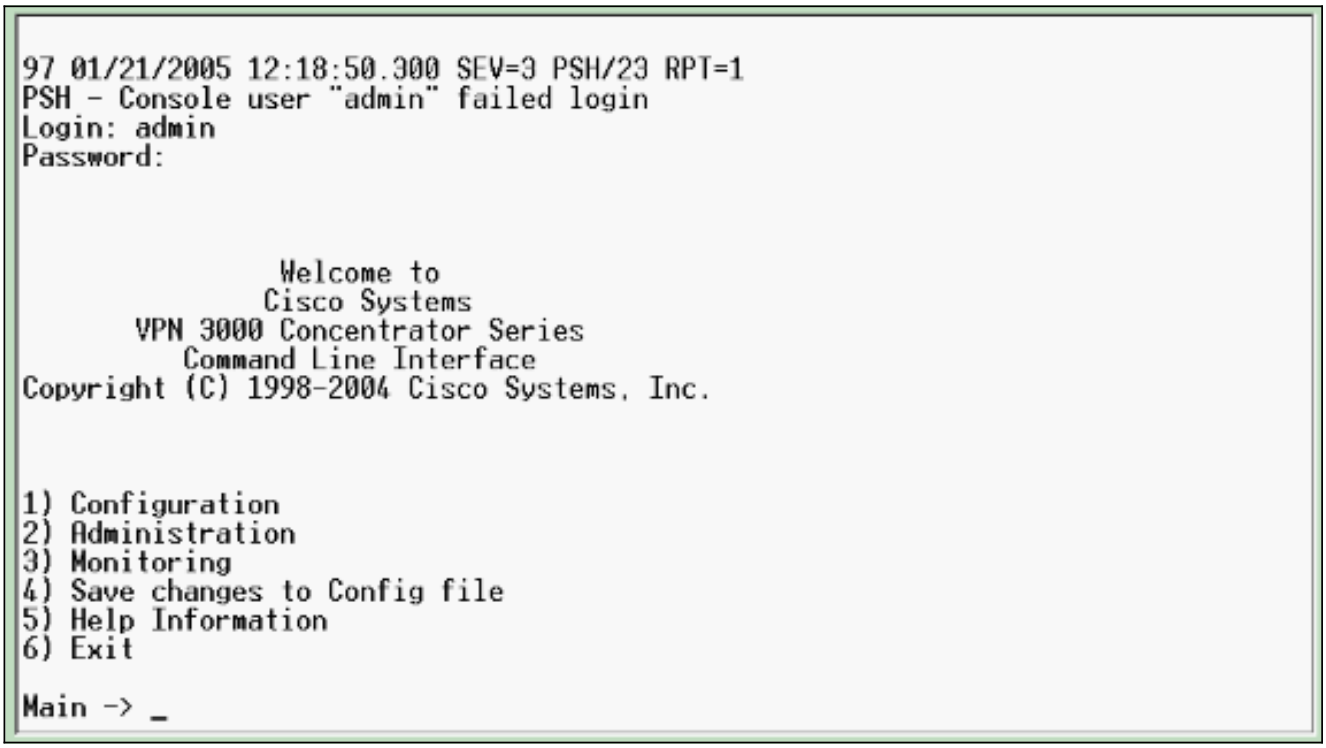
Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Configurer le concentrateur VPN 3000

Complétez ces étapes afin de configurer le concentrateur VPN 3000.

Remarque : en raison de l'espace limité, certaines captures d'écran n'affichent que des écrans partiels.

1. Connectez-vous au port de console du concentrateur VPN et vérifiez que des adresses IP sont attribuées aux interfaces privées (internes) et publiques (externes).En outre, vérifiez qu'une passerelle par défaut est attribuée afin que le concentrateur VPN puisse transférer les paquets pour les destinations qu'il ne connaît pas à la passerelle par défaut (généralement le routeur de passerelle Internet)
   :



```
               Cisco Systems
       VPN 3000 Concentrator Series
          Command Line Interface
Copyright (C) 1998-2004 Cisco Systems, Inc.



1) Configuration
2) Administration
3) Monitoring
4) Save changes to Config file
5) Help Information
6) Exit

Main -> 1

1) Interface Configuration
2) System Management
3) User Management
4) Policy Management
5) Tunneling and Security
6) Back

Config -> 1
```

Ce tableau présente les adresses IP actuelles.

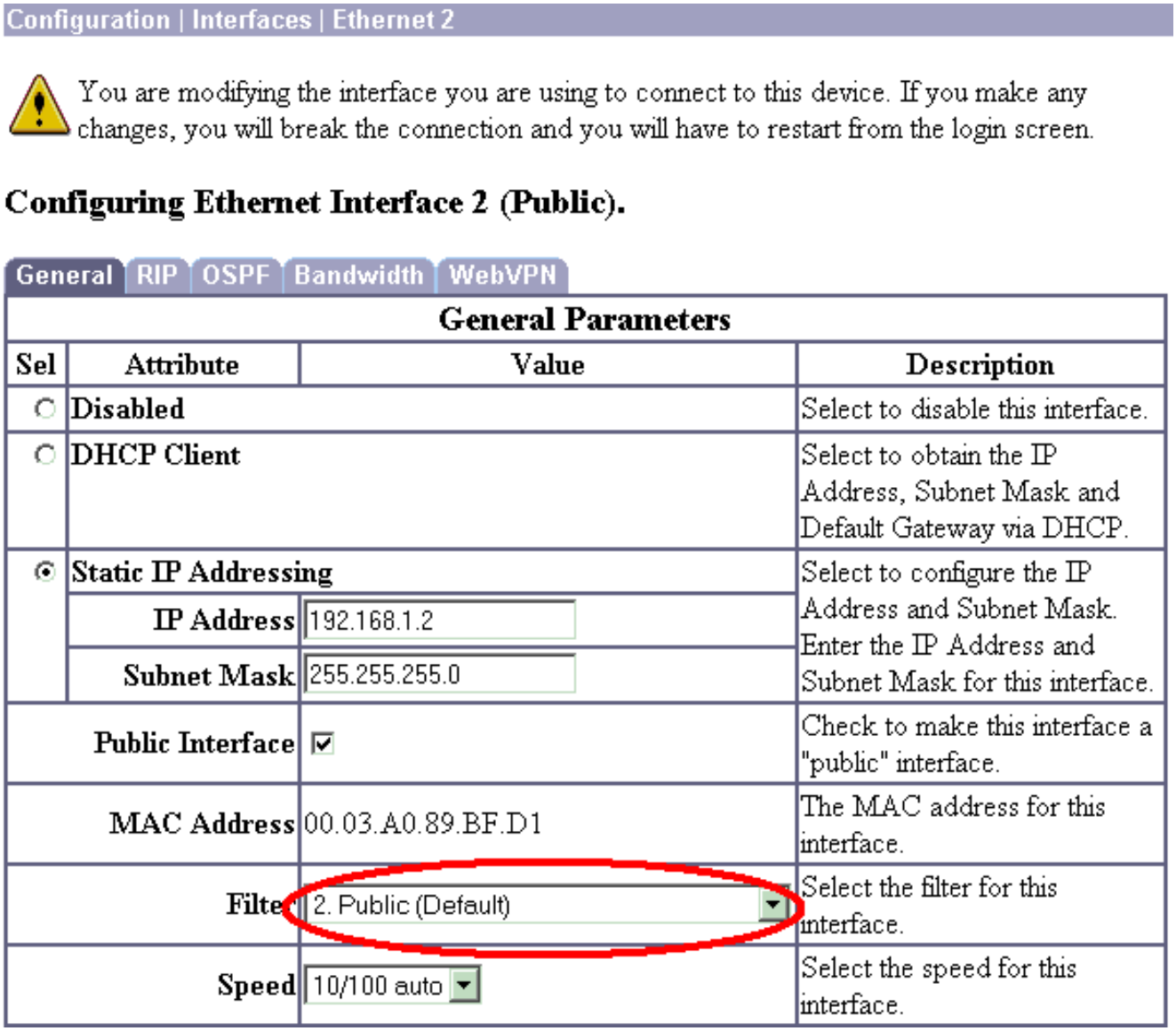
```
5) Tunneling and Security
6) Back

Config -> 1

This table shows current IP addresses.

  Intf          Status       IP Address/Subnet Mask          MAC Address
--------------------------------------------------------------------------------
Ether1-Pri|      UP      |       10.1.1.1/255.255.255.0  | 00.90.A4.00.06.94
Ether2-Pub|      UP      | 172.18.124.133/255.255.255.0  | 00.90.A4.00.06.95
Ether3-Ext|Not Configured|        0.0.0.0/0.0.0.0        |
--------------------------------------------------------------------------------
DNS Server(s): 10.1.0.121, 10.1.0.122
DNS Domain Name:
Default Gateway: 172.18.124.1

1) Configure Ethernet #1 (Private)
2) Configure Ethernet #2 (Public)
3) Configure Ethernet #3 (External)
4) Configure Power Supplies
5) Back

Interfaces ->
```

```
DNS Domain Name:
Default Gateway: 172.18.124.1

1) Configure Ethernet #1 (Private)
2) Configure Ethernet #2 (Public)
3) Configure Ethernet #3 (External)
4) Configure Power Supplies
5) Back

Interfaces -> 5

1) Interface Configuration
2) System Management
3) User Management
4) Policy Management
5) Tunneling and Security
6) Back

Config -> 2

1) Servers (Authentication, Authorization, Accounting, DNS, DHCP, etc.)
2) Address Management
3) IP Routing (static routes, OSPF, etc.)
4) Management Protocols (Telnet, TFTP, FTP, etc.)
5) Event Configuration
6) General Config (system name, time, etc.)
7) Client Update
8) Load Balancing Configuration
9) Back

System -> 3_
```

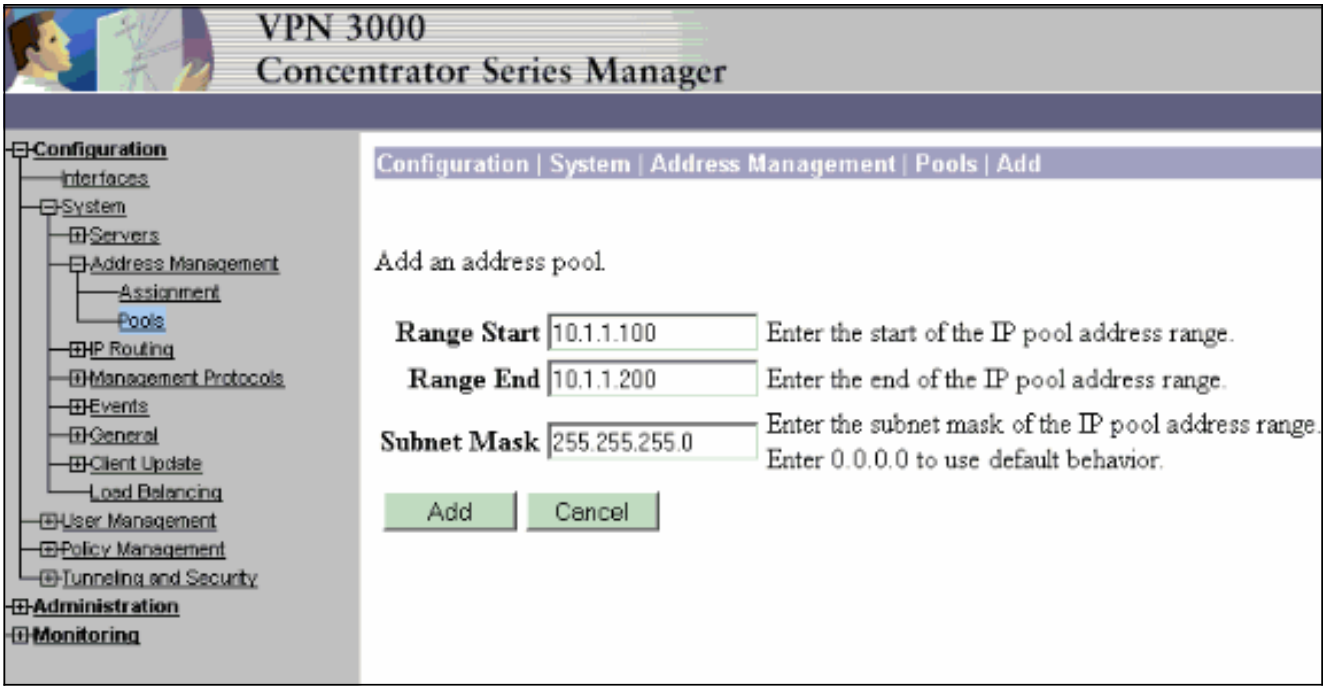
```
8) Load Balancing Configuration
9) Back

System -> 3

1) Static Routes
2) Default Gateways
3) OSPF
4) OSPF Areas
5) DHCP Parameters
6) Redundancy
7) Reverse Route Injection
8) DHCP Relay
9) Back

Routing -> 1

Static Routes
-------------
Destination     Mask            Metric Destination
-----------------------------------------------------------
0.0.0.0         0.0.0.0              1 172.18.124.1
10.0.0.0        255.0.0.0           10 10.1.16.111
192.168.0.0     255.255.0.0         10 10.1.16.111

1) Add Static Route
2) Modify Static Route
3) Delete Static Route
4) Back

Routing ->
```

```
 8) Load Balancing Configuration
 9) Back

 System -> 3

 1) Static Routes
 2) Default Gateways
 3) OSPF
 4) OSPF Areas
 5) DHCP Parameters
 6) Redundancy
 7) Reverse Route Injection
 8) DHCP Relay
 9) Back

 Routing -> 1

 Static Routes
 -------------
 Destination     Mask            Metric Destination
 ------------------------------------------------------------
 0.0.0.0         0.0.0.0              1 172.18.124.1



 1) Add Static Route
 2) Modify Static Route
 3) Delete Static Route
 4) Back

 Routing ->
```

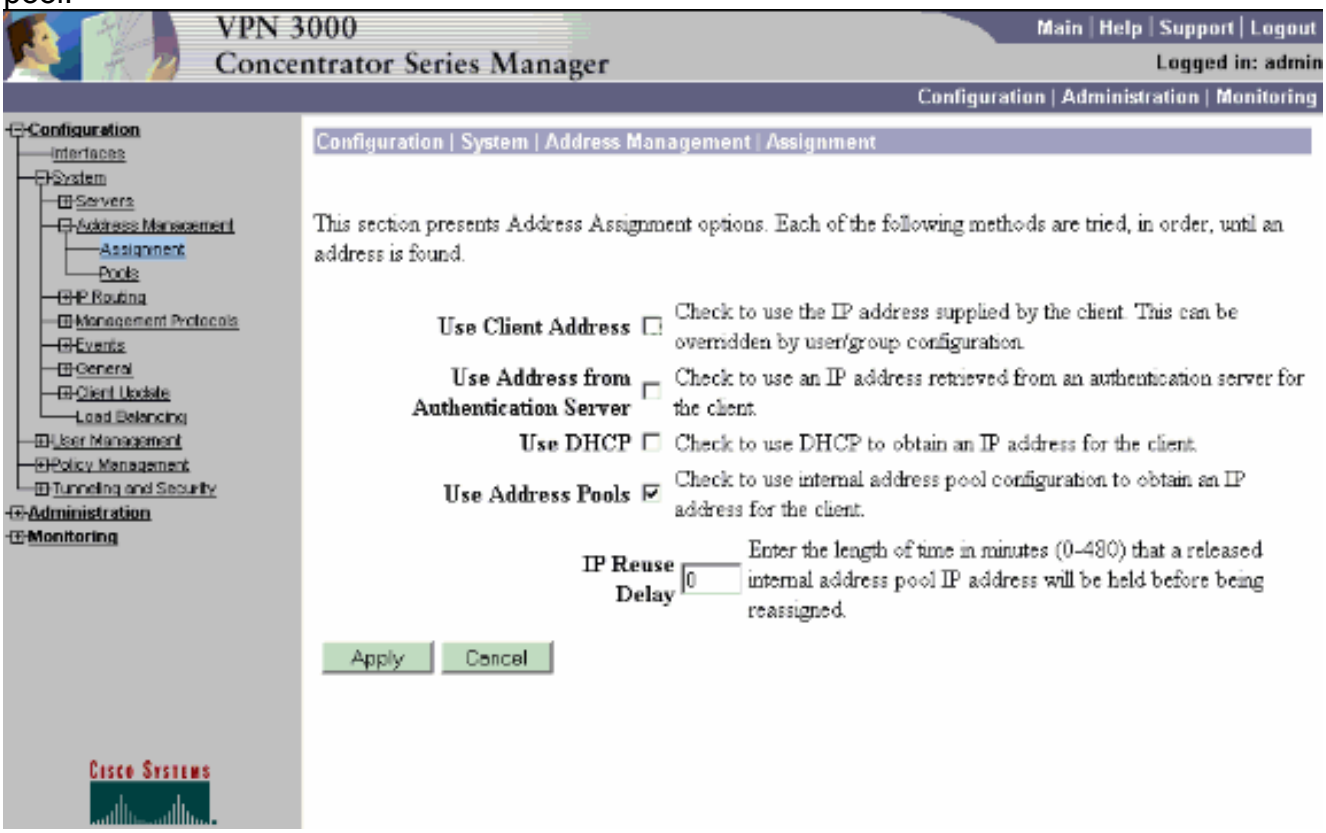
2. Assurez-vous de sélectionner l'option de filtre **public** pour l'interface publique.



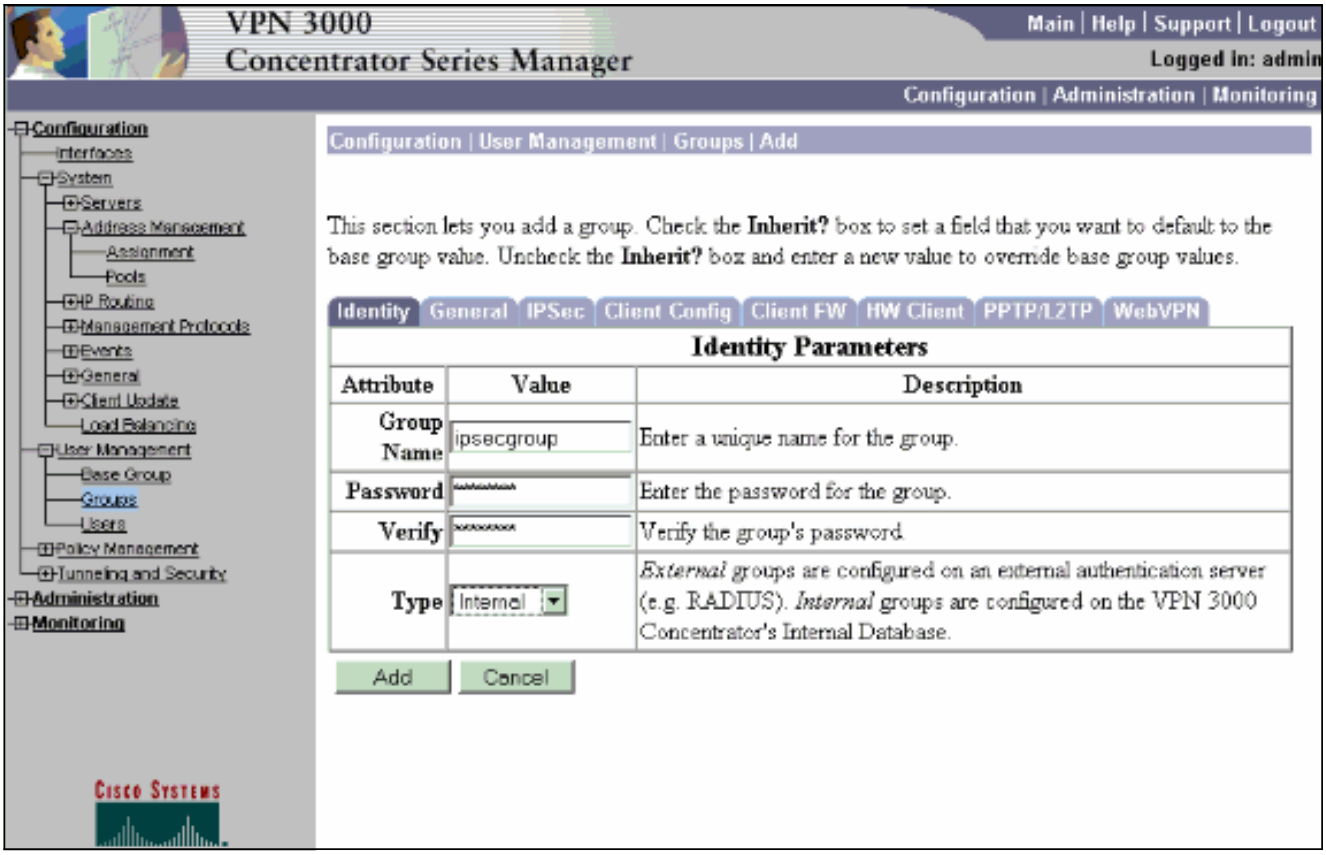
3. Pointez un navigateur vers l'interface interne du concentrateur VPN et choisissez Configuration > **System** > **Address Management** > **Address Pools** > **Add** afin d'attribuer une plage d'adresses IP disponible.Spécifiez une plage d'adresses IP qui ne sont en conflit avec aucun autre périphérique du réseau interne :**Remarque :** ces captures d'écran montrent la gestion des interfaces externes-publiques car des filtres ont été ajoutés pour autoriser cette opération dans un paramètre de TP
uniquement.



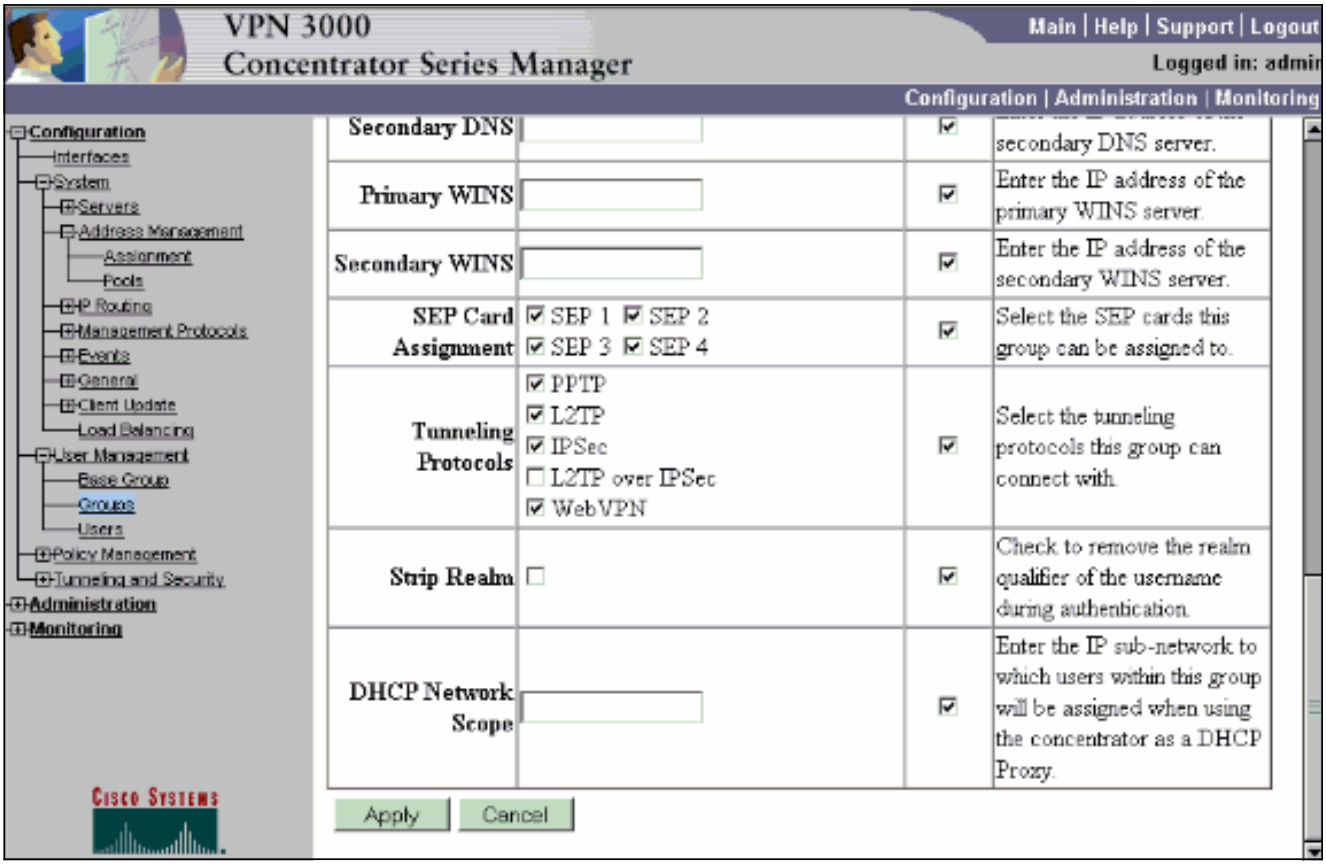
4. Choisissez Configuration > System > Address Management > **Assignment**, cochez la **case Use Address Pools** et cliquez sur **Apply** afin de demander au concentrateur VPN d'utiliser le pool.



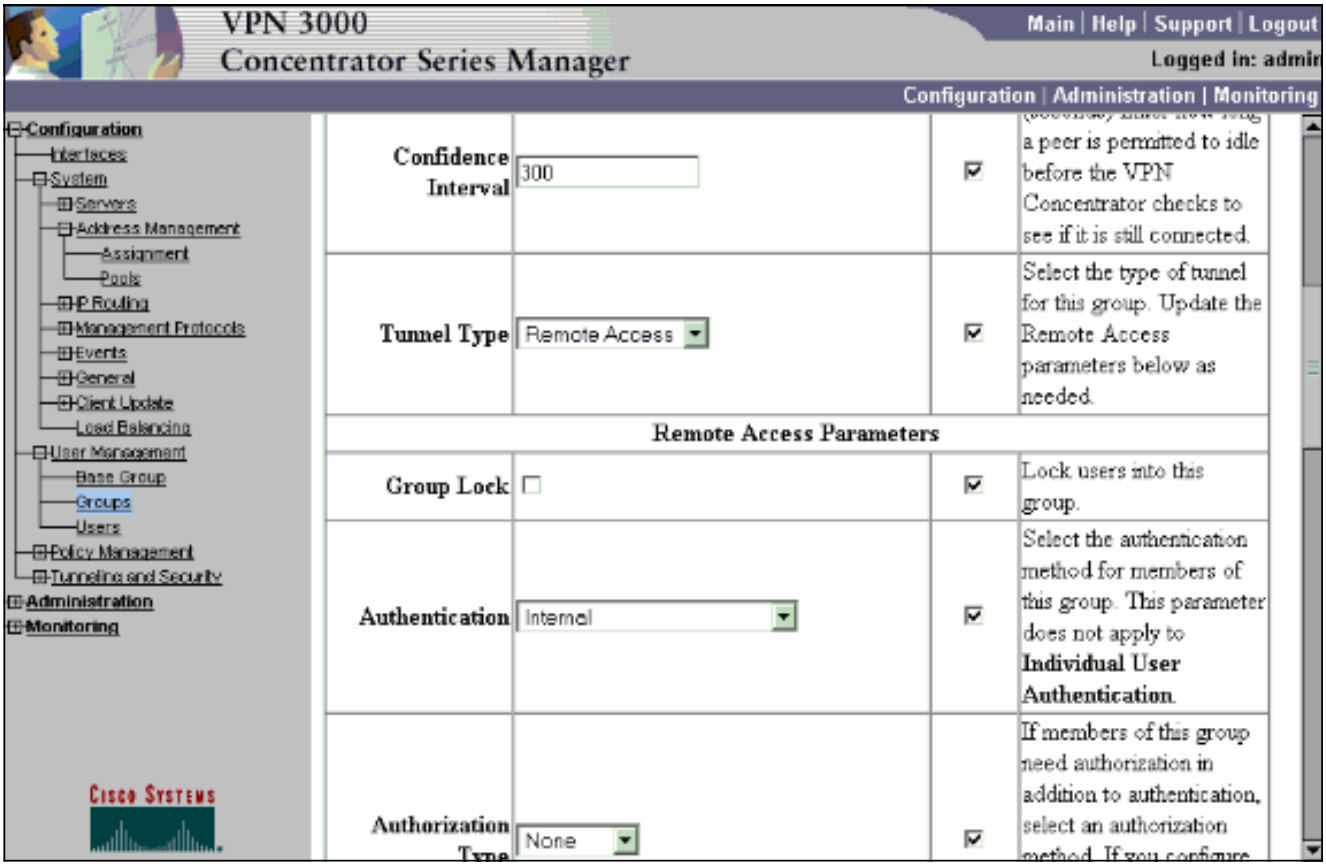
5. Choisissez **Configuration > User Management > Groups > Add Group** afin de configurer un groupe IPsec pour les utilisateurs et de définir un nom de groupe et un mot de passe.Cet exemple utilise group=« ipsecgroup » avec password/verify=« cisco123 »
:



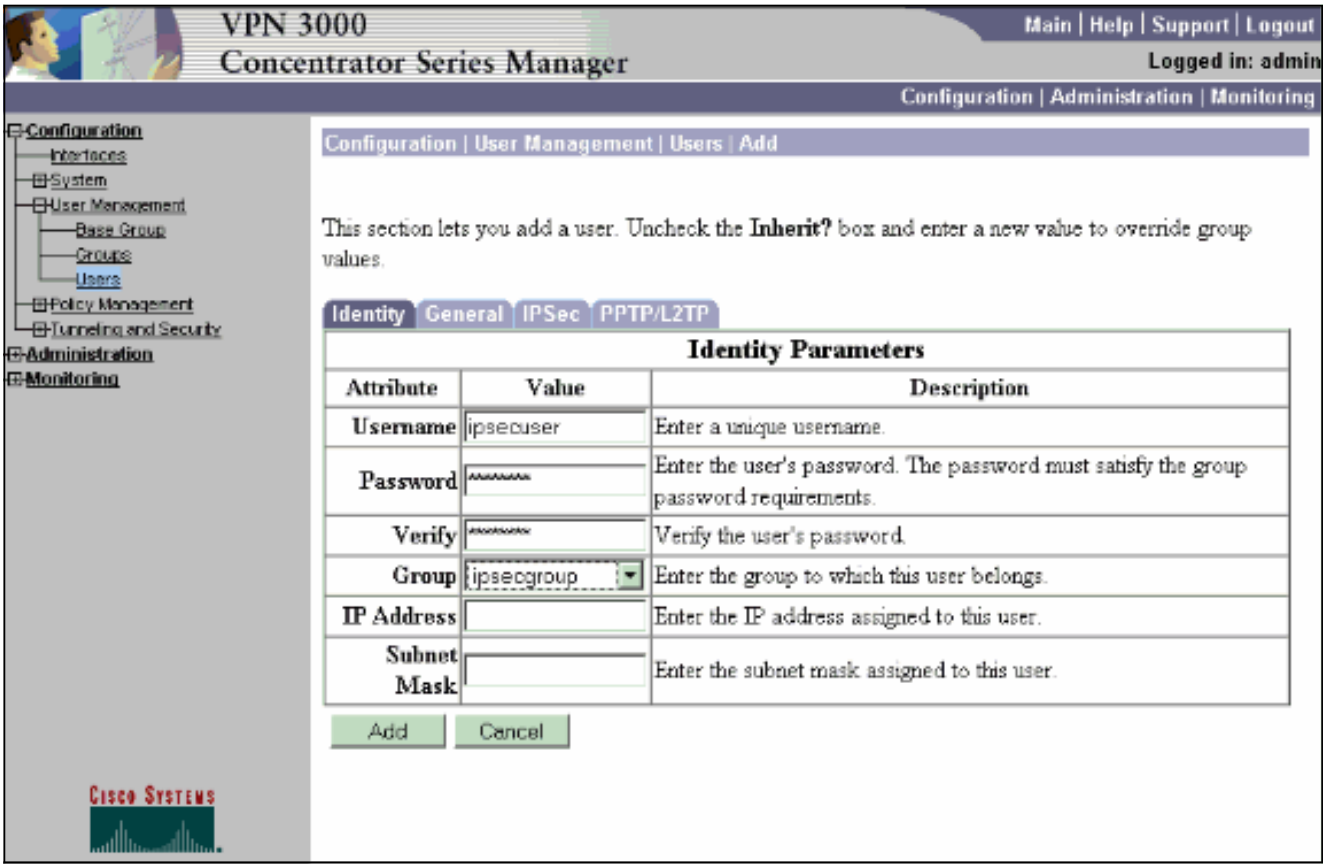
6. Dans l'onglet Général du groupe, vérifiez que **IPSec** est sélectionné.



7. Dans l'onglet IPSec du groupe, vérifiez que l'authentification est définie sur **Interne**. Choisissez **Configuration > User Management > Groups > Modify Group** et sélectionnez **ipsecgroup** dans l'option Current Groups afin d'effectuer cette opération.

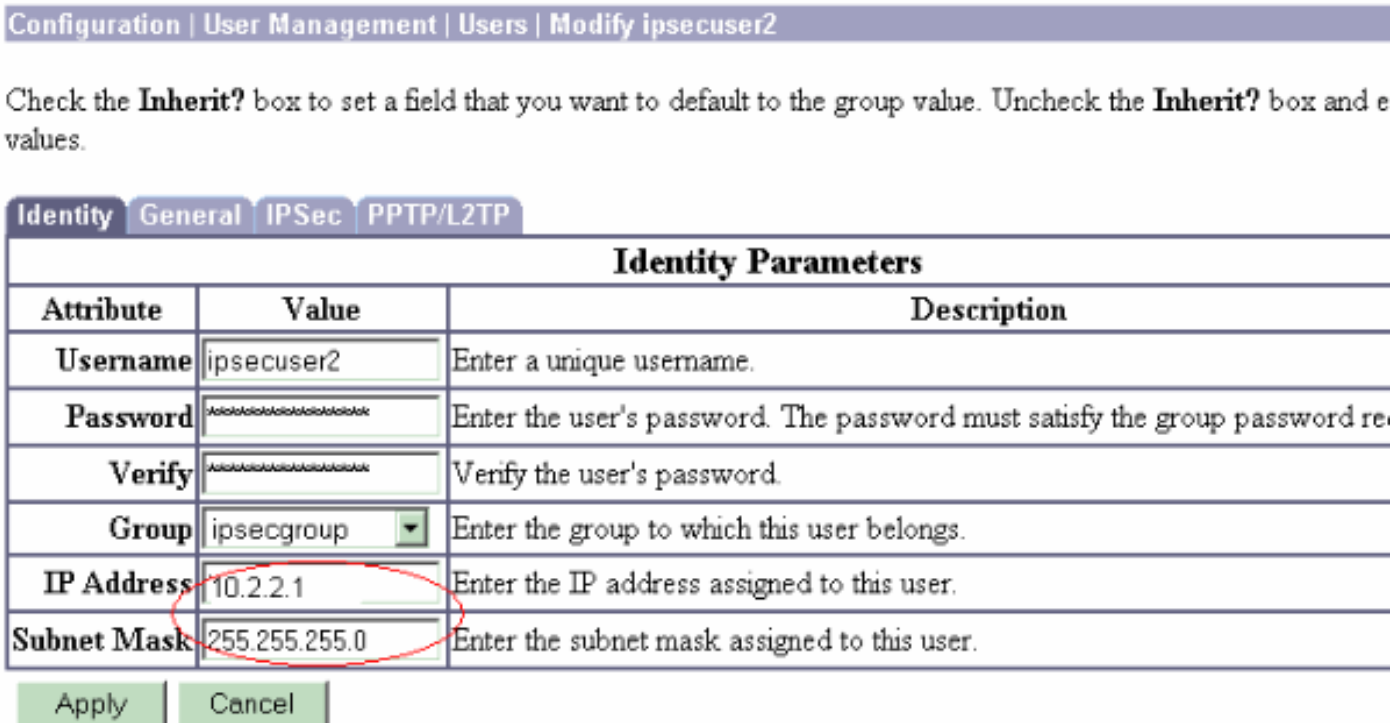


8. Choisissez **Configuration > User Management > Users > Add** et ajoutez un utilisateur au groupe précédemment défini.Dans cet exemple, l'utilisateur est « ipsecuser » avec le mot de passe « xyz12345 » dans le groupe « ipsecgroup »
:

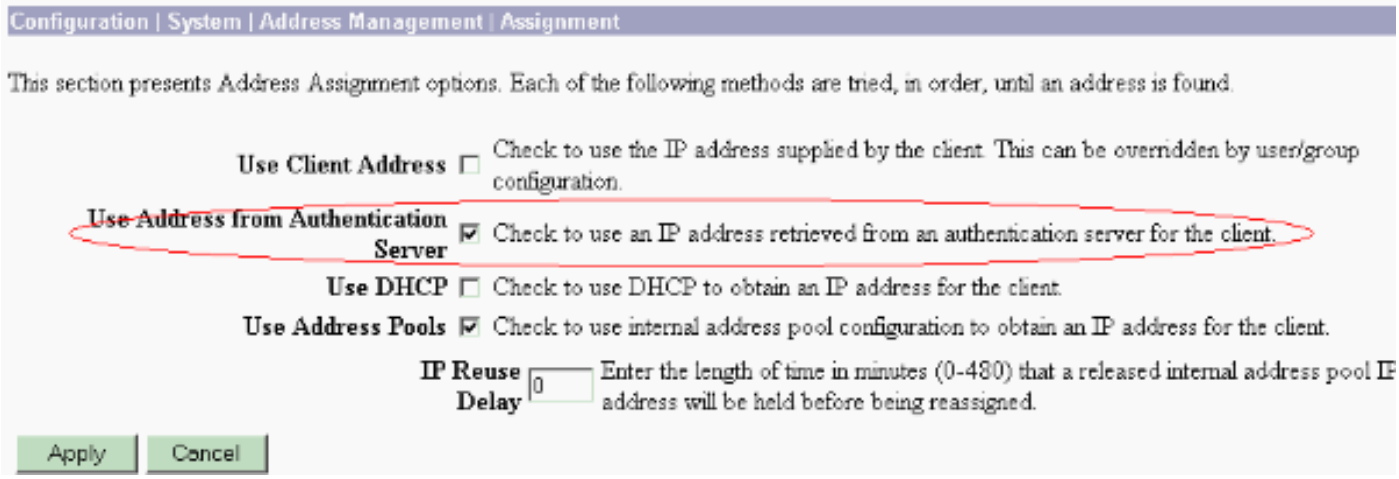


Attribuer une adresse IP statique à un utilisateur

Afin d'attribuer une adresse IP statique à l'utilisateur VPN distant chaque fois qu'il se connecte au concentrateur de la gamme VPN 3000, choisissez **Configuration > User Management > Users > Modify ipsecuser2 > identity**. Dans cette configuration pour l'utilisateur (ipsecuser2), l'adresse IP statique 10.2.2.1/24 est attribuée chaque fois que l'utilisateur se connecte.



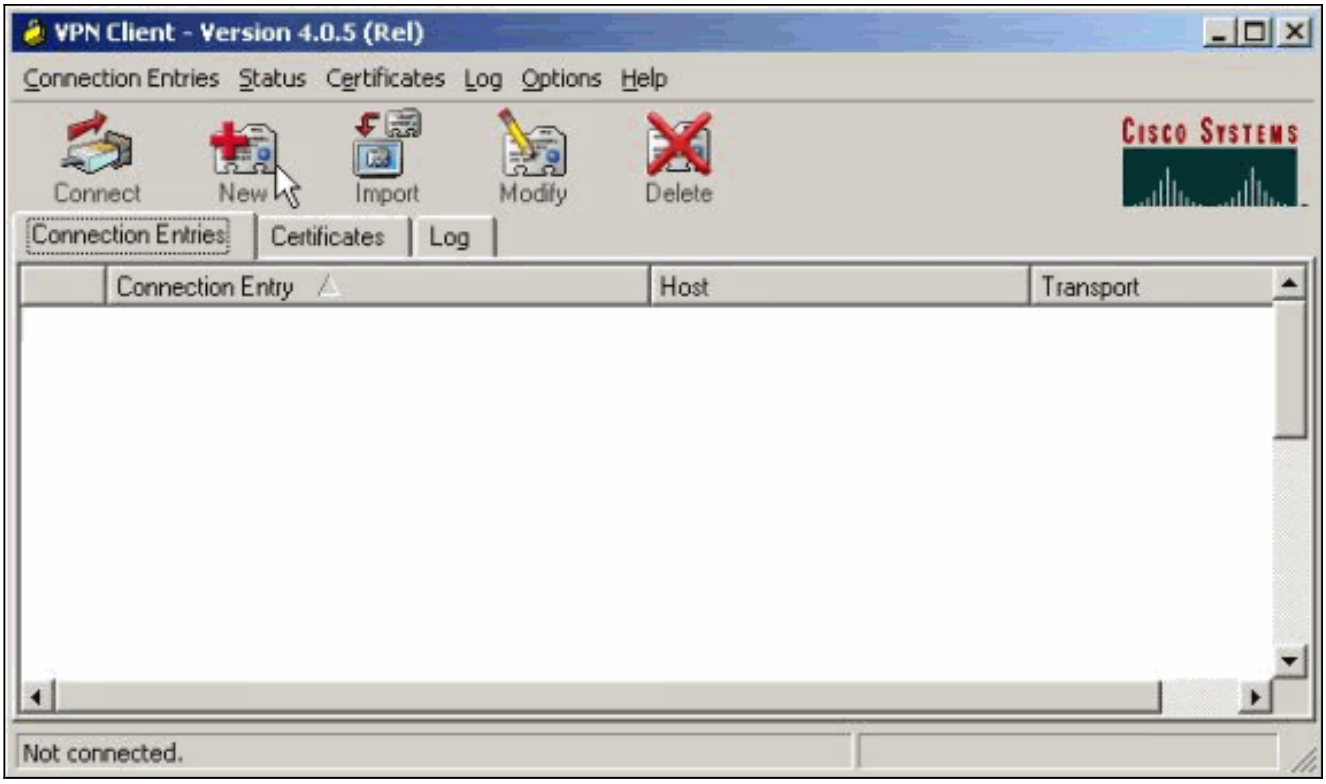
Remarque : veillez à accéder à **Configuration > System > Address Management > Assignment** afin de vous assurer que le concentrateur VPN réserve l'adresse IP attribuée. Cochez la case **Utiliser l'adresse du serveur d'authentification** pour attribuer les adresses IP extraites d'un serveur d'authentification par utilisateur. L'adresse IP et le masque de sous-réseau saisis dans l'onglet Paramètres d'identité de la fenêtre **User Management > Users > Add or Modify** sont considérés comme se trouvant dans le serveur d'authentification interne.



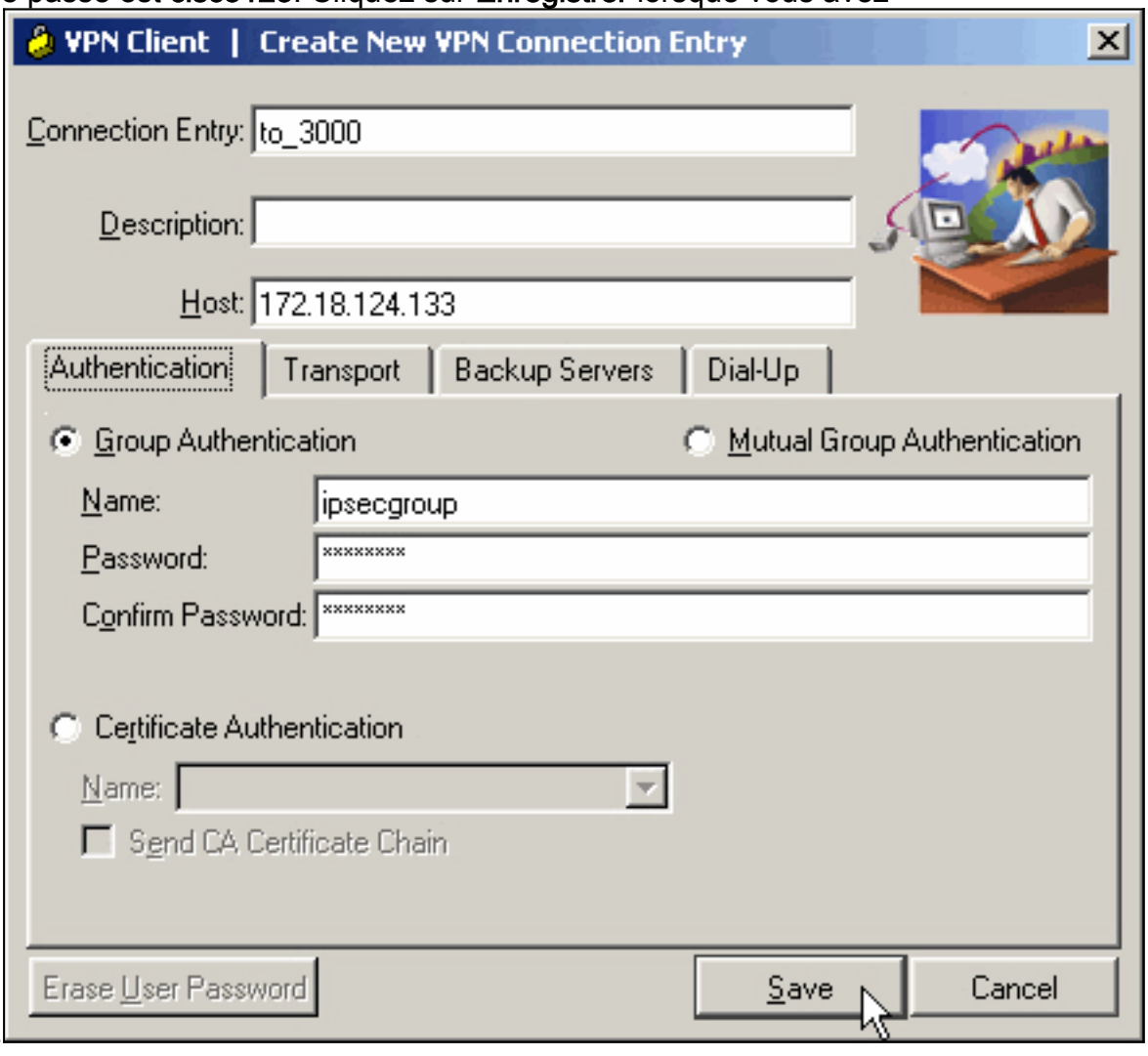
Configurer le client VPN

Exécutez les étapes suivantes afin de configurer le client VPN.

1. Cliquez sur **Nouveau** afin de créer une nouvelle entrée de connexion.



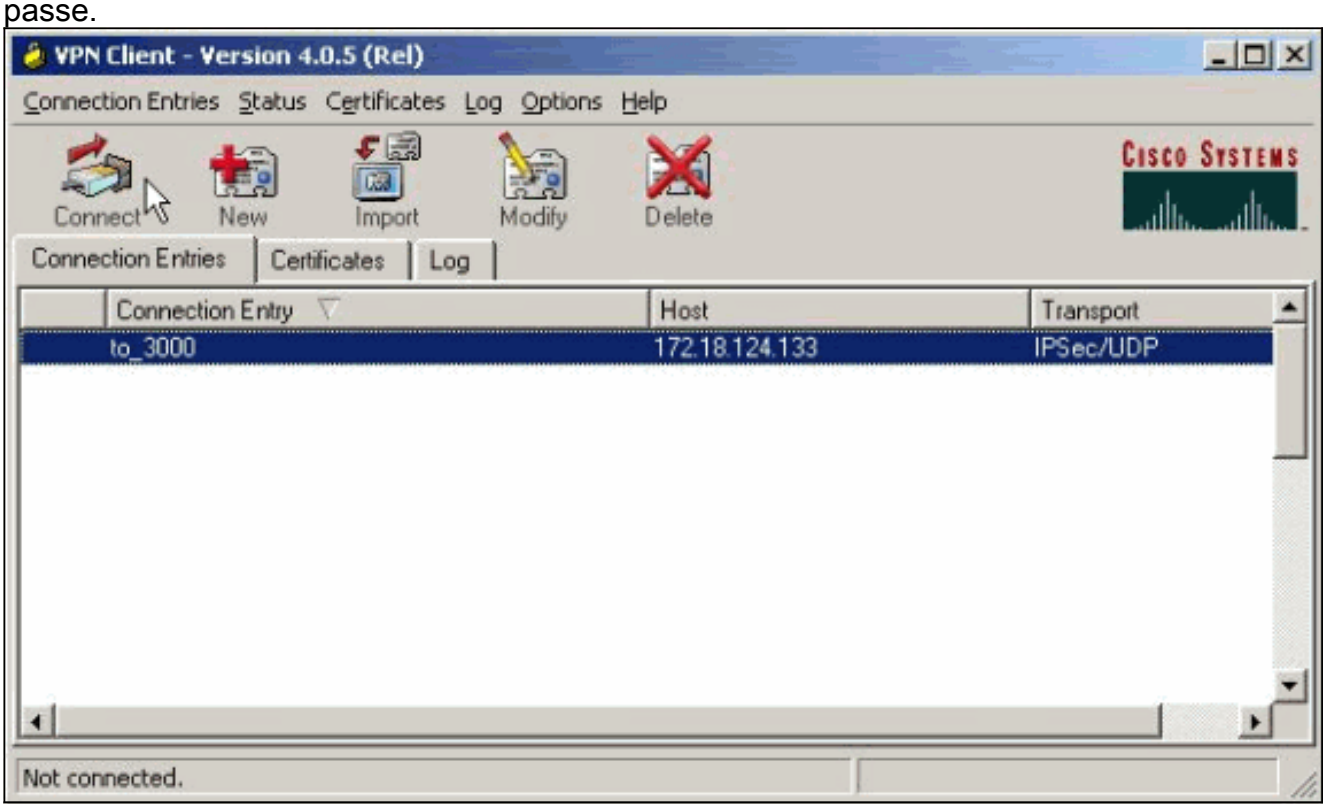
2. Nommez la connexion, entrez l'adresse IP de l'interface publique du concentrateur VPN et fournissez les informations d'identification du groupe. Dans ce cas, le nom est **ipsecgroup** et le mot de passe est **cisco123**. Cliquez sur **Enregistrer** lorsque vous avez



terminé.

3. Sélectionnez l'entrée de connexion dans la liste et cliquez sur **Connect**. Lorsque vous y êtes invité, entrez votre nom d'utilisateur/mot de

passe.



Vérification

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépannage

Ces sections fournissent des informations que vous pouvez utiliser pour dépanner 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 .**

Remarque : reportez-vous à Informations importantes sur les commandes de débogage avant d'émettre des commandes de débogage.

Causes de problèmes potentiels

Ce sont des erreurs potentielles qui peuvent se produire. Reportez-vous aux sections Client VPN et Concentrateur VPN pour connaître les résolutions de ces erreurs.

- Un utilisateur reçoit le message `Impossible de négocier IPSec ou l'hôte n'a pas répondu.`Le débogage VPN 3000 indique :
  ```
  14 02/20/2001 08:59:29.100 SEV=4 IKE/22 RPT=5 10.102.55.139
  No Group found matching badgroup for Pre-shared key peer 10.102.55.139
  ```
  Cause habituelle : L'utilisateur tente de se connecter avec un nom de groupe qui n'est pas configuré.
- Un utilisateur ne peut pas se connecter et le débogage VPN 3000 indique :
  ```
  Filter missing on interface 2, IKE data from Peer x.x.x.x dropped
  ```

Cause habituelle : Le filtre est manquant dans l'interface publique. Il s'agit généralement du filtre « public » (mais il peut s'agir du filtre privé); « aucun » n'est valide). Choisissez **Configuration > Interfaces > Ethernet 2 > Filter** et définissez le filtre « public » ou une autre valeur (c'est-à-dire pas « aucun »). Reportez-vous à la section Configuration de ce document pour plus d'informations sur la façon de configurer le filtre.

- Un utilisateur ne peut pas se connecter et voit `Incapable de négocier IPSec ou l'hôte n'a pas répondu`.Le débogage VPN 3000 indique :
  `Terminating connection attempt: IPSEC not permitted for group >group<`
  Cause habituelle : IPsec n'est pas sélectionné sur le groupe. Choisissez Configuration > User Management > Groups > <group> > Modify > **General** et vérifiez que **IPSec** est sélectionné sous Tunneling Protocols.
- Un utilisateur ne peut pas se connecter après de nombreuses tentatives et voit `l'authentification de l'utilisateur échouer`.Le débogage VPN 3000 indique :
  `Authentication rejected: Reason = User was not found handle = 14, server = Internal, user = <user>`
  Cause habituelle : L'utilisateur n'existe pas dans la base de données des utilisateurs. Assurez-vous d'entrer le nom d'utilisateur correct lorsque la fenêtre d'authentification de l'utilisateur s'affiche.
- Les utilisateurs ne peuvent pas se connecter et le débogage VPN 3000 indique :
  `Filter missing on interface 0, IKE data from Peer x.x.x.x dropped`
  Cause habituelle : La route par défaut est manquante. Assurez-vous qu'il existe une route par défaut dans la configuration. Choisissez **Configuration > System > IP routing > Default Gateway** et spécifiez la passerelle par défaut.
- Un utilisateur ne peut pas se connecter et voit `que votre connexion IPSec a été interrompue par l'homologue distant`.Le débogage VPN 3000 indique :
  `User [ <user> ]`
  `IKE rcv'd FAILED IP Addr status!`
  Cause habituelle : Aucune option n'est cochée pour attribuer une adresse IP au client VPN. Choisissez **Configuration > System > Address Management > Address Assignment** et sélectionnez une option.
- Un utilisateur ne peut pas se connecter et voit `l'authentification de l'utilisateur échouer`.Le débogage VPN 3000 indique :
  `The calculated HASH doesn't match the received value`
  Cause habituelle : Le mot de passe de groupe sur le client VPN est différent du mot de passe configuré sur le concentrateur VPN. Vérifiez le mot de passe sur le client VPN et le concentrateur.
- Vous avez configuré le pool VPN pour les ressources derrière le concentrateur VPN. Vous pouvez accéder aux ressources, mais vous ne pouvez pas leur envoyer de requête ping.**Cause habituelle :** Il y a un PIX derrière le concentrateur VPN qui bloque les paquets ICMP. Connectez-vous à ce PIX et appliquez une **liste d'accès** pour activer les paquets ICMP.
- Il n'y a pas de débogages de concentrateur VPN et tous ou certains utilisateurs ne peuvent pas se connecter.Le filtre public du concentrateur VPN par défaut contient des règles pour autoriser ce trafic :Protocole = UDP, port = 500Protocole = UDP, port = 10000Protocole = ESPProtocole = AHSi les filtres du concentrateur VPN autorisent ce trafic, alors un périphérique entre le client VPN et le concentrateur VPN peut bloquer certains de ces ports (peut-être un pare-feu). Afin de vérifier, essayez de vous connecter au concentrateur VPN à partir du réseau immédiatement en dehors du concentrateur VPN. Si cela fonctionne, un périphérique entre le PC client VPN et le concentrateur VPN bloque le trafic.
- Un utilisateur ne peut pas se connecter et voit ces journaux :
  `07/10/2006 11:48:59.280 SEV=4 IKE/0 RPT=141 10.86.190.92`

```
Group [NYMVPN]
received an unencrypted packet when crypto active!! Dropping packet
```

Cause habituelle : Nom ou mot de passe de groupe mal défini. Recréez le nouveau nom de groupe et le nouveau mot de passe sur le concentrateur VPN 3000 pour le client VPN.

- Un utilisateur peut envoyer une requête ping ou établir une connexion Telnet à un hôte situé derrière le concentrateur VPN, mais il ne peut pas utiliser le Remote Desktop 9RDP (Remote Desktop 9RDP) ou des applications similaires.**Cause courante :** Le filtre Public n'est pas activé sur l'interface Public. Reportez-vous à l'étape 2 de la section Configurer le concentrateur VPN 3000 de ce document.
- Un utilisateur peut se connecter, mais aucun trafic ne passe par le tunnel VPN.**Cause habituelle :** NAT-Transparency n'est pas activé. Dans de nombreux cas, le client VPN se trouve derrière un périphérique PAT. La fonction PAT repose sur les numéros de port TCP et UDP pour conserver l'espace d'adressage. Mais ESP, qui encapsule le trafic VPN, est un protocole distinct de TCP ou UDP. Cela signifie que de nombreux périphériques PAT ne peuvent pas gérer le trafic ESP. NAT-T encapsule les paquets ESP dans des paquets UDP, ce qui leur permet de passer facilement par un périphérique PAT. Ainsi, pour permettre au trafic ESP de circuler via un périphérique PAT, vous devez activer NAT-T sur le concentrateur. Référez-vous à Configuration du mode transparent NAT pour IPSec sur le concentrateur VPN 3000 pour plus d'informations.

Client VPN

Choisissez **Start > Programs > Cisco Systems VPN 3000 Client > Log Viewer** afin d'afficher la visionneuse de journal.

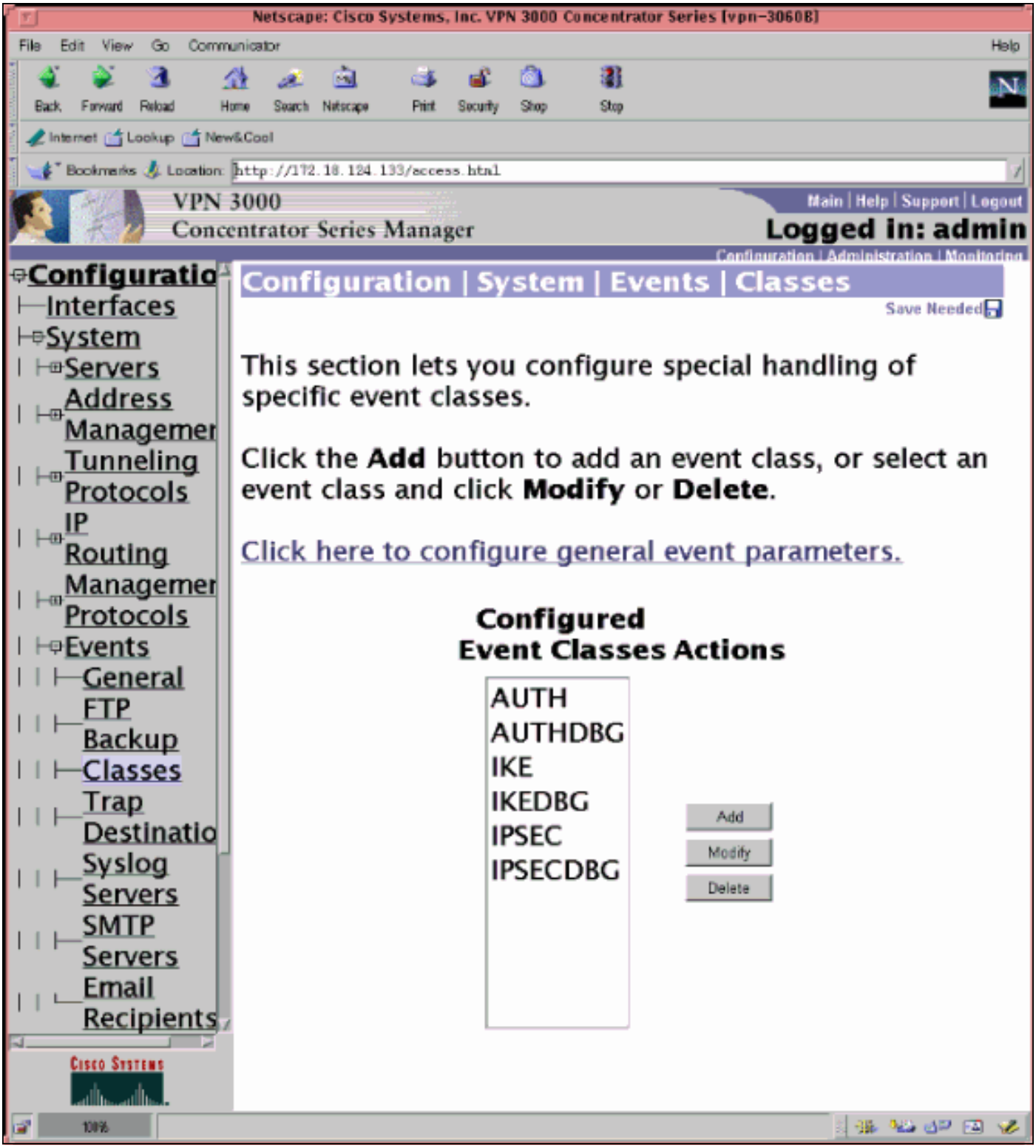
Concentrateur VPN

Choisissez **Configuration > System > Events > Classes** afin d'activer ce débogage en cas d'échec de connexion d'événement :

- AUTH - Gravité du journal 1-13
- AUTHDBG - Gravité du journal 1-13
- IKE - Gravité du journal 1-13
- IKEDBG - Gravité du journal 1-13
- IPSEC - Gravité du journal 1-13
- IPSECDBG - Gravité du journal 1-13

Note : Si nécessaire, AUTHDECODE, IKEDECODE, IPSECDECODE peuvent être ajoutés ultérieurement.

Référez-vous à Dépannage des problèmes de connexion sur le concentrateur VPN 3000 pour plus de détails sur le dépannage.



Choisissez **Monitoring > Filterable Event Log** afin d'afficher le journal.

Concentrateur VPN 3000 - bon exemple de débogage

```
1 02/07/2002 08:00:13.320 SEV=8 IKEDBG/0 RPT=69 172.18.124.241
RECEIVED Message (msgid=0) with payloads :
HDR + SA (1) + KE (4) + NONCE (10) + ID (5) + VENDOR (13) + VENDOR (13) + VENDOR
 (13) + NONE (0) ... total length : 562

4 02/07/2002 08:00:13.320 SEV=9 IKEDBG/0 RPT=70 172.18.124.241
processing SA payload
```

```
5 02/07/2002 08:00:13.320 SEV=9 IKEDBG/0 RPT=71 172.18.124.241
processing ke payload

6 02/07/2002 08:00:13.320 SEV=9 IKEDBG/0 RPT=72 172.18.124.241
processing ISA_KE

7 02/07/2002 08:00:13.320 SEV=9 IKEDBG/1 RPT=7 172.18.124.241
processing nonce payload

8 02/07/2002 08:00:13.320 SEV=9 IKEDBG/1 RPT=8 172.18.124.241
Processing ID

9 02/07/2002 08:00:13.320 SEV=9 IKEDBG/47 RPT=4 172.18.124.241
processing VID payload

10 02/07/2002 08:00:13.320 SEV=9 IKEDBG/49 RPT=4 172.18.124.241
Received xauth V6 VID

11 02/07/2002 08:00:13.320 SEV=9 IKEDBG/47 RPT=5 172.18.124.241
processing VID payload

12 02/07/2002 08:00:13.320 SEV=9 IKEDBG/49 RPT=5 172.18.124.241
Received DPD VID

13 02/07/2002 08:00:13.320 SEV=9 IKEDBG/47 RPT=6 172.18.124.241
processing VID payload

14 02/07/2002 08:00:13.320 SEV=9 IKEDBG/49 RPT=6 172.18.124.241
Received Cisco Unity client VID

15 02/07/2002 08:00:13.320 SEV=9 IKEDBG/23 RPT=2 172.18.124.241
Starting group lookup for peer 172.18.124.241

16 02/07/2002 08:00:13.320 SEV=8 AUTHDBG/1 RPT=2
AUTH_Open() returns 136

17 02/07/2002 08:00:13.320 SEV=7 AUTH/12 RPT=2
Authentication session opened: handle = 136

18 02/07/2002 08:00:13.320 SEV=8 AUTHDBG/3 RPT=2
AUTH_PutAttrTable(136, 728a84)

19 02/07/2002 08:00:13.320 SEV=8 AUTHDBG/6 RPT=2
AUTH_GroupAuthenticate(136, 9b143bc, 482fb0)

20 02/07/2002 08:00:13.320 SEV=8 AUTHDBG/59 RPT=2
AUTH_BindServer(9a08630, 0, 0)

21 02/07/2002 08:00:13.320 SEV=9 AUTHDBG/69 RPT=2
Auth Server 16b3fa0 has been bound to ACB 9a08630, sessions = 1

22 02/07/2002 08:00:13.320 SEV=8 AUTHDBG/65 RPT=2
AUTH_CreateTimer(9a08630, 0, 0)

23 02/07/2002 08:00:13.320 SEV=9 AUTHDBG/72 RPT=2
Reply timer created: handle = 3B2001B

24 02/07/2002 08:00:13.320 SEV=8 AUTHDBG/61 RPT=2
AUTH_BuildMsg(9a08630, 0, 0)

25 02/07/2002 08:00:13.320 SEV=8 AUTHDBG/64 RPT=2
AUTH_StartTimer(9a08630, 0, 0)

26 02/07/2002 08:00:13.320 SEV=9 AUTHDBG/73 RPT=2
```

```
Reply timer started: handle = 3B2001B, timestamp = 10085308, timeout = 30000

27 02/07/2002 08:00:13.320 SEV=8 AUTHDBG/62 RPT=2
AUTH_SndRequest(9a08630, 0, 0)

28 02/07/2002 08:00:13.320 SEV=8 AUTHDBG/50 RPT=3
IntDB_Decode(62b6d00, 115)

29 02/07/2002 08:00:13.320 SEV=8 AUTHDBG/47 RPT=3
IntDB_Xmt(9a08630)

30 02/07/2002 08:00:13.320 SEV=9 AUTHDBG/71 RPT=2
xmit_cnt = 1

31 02/07/2002 08:00:13.320 SEV=8 AUTHDBG/47 RPT=4
IntDB_Xmt(9a08630)

32 02/07/2002 08:00:13.420 SEV=8 AUTHDBG/49 RPT=2
IntDB_Match(9a08630, 2ebe71c)

33 02/07/2002 08:00:13.420 SEV=8 AUTHDBG/63 RPT=2
AUTH_RcvReply(9a08630, 0, 0)

34 02/07/2002 08:00:13.420 SEV=8 AUTHDBG/50 RPT=4
IntDB_Decode(2ebe71c, 44)

35 02/07/2002 08:00:13.420 SEV=8 AUTHDBG/48 RPT=2
IntDB_Rcv(9a08630)

36 02/07/2002 08:00:13.420 SEV=8 AUTHDBG/66 RPT=2
AUTH_DeleteTimer(9a08630, 0, 0)

37 02/07/2002 08:00:13.420 SEV=9 AUTHDBG/74 RPT=2
Reply timer stopped: handle = 3B2001B, timestamp = 10085318

38 02/07/2002 08:00:13.420 SEV=8 AUTHDBG/58 RPT=2
AUTH_Callback(9a08630, 0, 0)

39 02/07/2002 08:00:13.420 SEV=6 AUTH/41 RPT=2 172.18.124.241
Authentication successful: handle = 136, server = Internal, group = ipsecgroup

40 02/07/2002 08:00:13.420 SEV=7 IKEDBG/0 RPT=73 172.18.124.241
Group [ipsecgroup]
Found Phase 1 Group (ipsecgroup)

41 02/07/2002 08:00:13.420 SEV=8 AUTHDBG/4 RPT=2
AUTH_GetAttrTable(136, 728c4c)

42 02/07/2002 08:00:13.420 SEV=7 IKEDBG/14 RPT=2 172.18.124.241
Group [ipsecgroup]
Authentication configured for Internal

43 02/07/2002 08:00:13.420 SEV=8 AUTHDBG/2 RPT=2
AUTH_Close(136)

44 02/07/2002 08:00:13.420 SEV=9 IKEDBG/0 RPT=74 172.18.124.241
Group [ipsecgroup]
processing IKE SA

45 02/07/2002 08:00:13.420 SEV=8 IKEDBG/0 RPT=75 172.18.124.241
Group [ipsecgroup]
Proposal # 1, Transform # 1, Type ISAKMP, Id IKE
Parsing received transform:
  Phase 1 failure against global IKE proposal # 1:
```

```
  Mismatched attr types for class Hash Alg:
    Rcv'd: SHA
    Cfg'd: MD5

50 02/07/2002 08:00:13.420 SEV=8 IKEDBG/0 RPT=76 172.18.124.241
Group [ipsecgroup]
  Phase 1 failure against global IKE proposal # 2:
  Mismatched attr types for class Hash Alg:
    Rcv'd: SHA
    Cfg'd: MD5

53 02/07/2002 08:00:13.420 SEV=8 IKEDBG/0 RPT=77 172.18.124.241
Group [ipsecgroup]
  Phase 1 failure against global IKE proposal # 3:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 2
    Cfg'd: Oakley Group 1

57 02/07/2002 08:00:13.420 SEV=8 IKEDBG/0 RPT=78 172.18.124.241
Group [ipsecgroup]
  Phase 1 failure against global IKE proposal # 4:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 2
    Cfg'd: Oakley Group 1

61 02/07/2002 08:00:13.420 SEV=8 IKEDBG/0 RPT=79 172.18.124.241
Group [ipsecgroup]
  Phase 1 failure against global IKE proposal # 5:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 2
    Cfg'd: Oakley Group 7

65 02/07/2002 08:00:13.420 SEV=8 IKEDBG/0 RPT=80 172.18.124.241
Group [ipsecgroup]
  Phase 1 failure against global IKE proposal # 6:
  Mismatched attr types for class Hash Alg:
    Rcv'd: SHA
    Cfg'd: MD5

68 02/07/2002 08:00:13.420 SEV=7 IKEDBG/28 RPT=2 172.18.124.241
Group [ipsecgroup]
IKE SA Proposal # 1, Transform # 2 acceptable
Matches global IKE entry # 1

70 02/07/2002 08:00:13.420 SEV=8 AUTHDBG/60 RPT=2
AUTH_UnbindServer(9a08630, 0, 0)

71 02/07/2002 08:00:13.420 SEV=9 AUTHDBG/70 RPT=2
Auth Server 16b3fa0 has been unbound from ACB 9a08630, sessions = 0

72 02/07/2002 08:00:13.420 SEV=8 AUTHDBG/10 RPT=2
AUTH_Int_FreeAuthCB(9a08630)

73 02/07/2002 08:00:13.420 SEV=7 AUTH/13 RPT=2
Authentication session closed: handle = 136

74 02/07/2002 08:00:13.450 SEV=9 IKEDBG/0 RPT=81 172.18.124.241

Group [ipsecgroup]
constructing ISA_SA for isakmp

75 02/07/2002 08:00:13.450 SEV=9 IKEDBG/0 RPT=82 172.18.124.241
Group [ipsecgroup]
constructing ke payload
```

```
76 02/07/2002 08:00:13.450 SEV=9 IKEDBG/1 RPT=9 172.18.124.241
Group [ipsecgroup]
constructing nonce payload

77 02/07/2002 08:00:13.450 SEV=9 IKEDBG/0 RPT=83 172.18.124.241
Group [ipsecgroup]
Generating keys for Responder...

78 02/07/2002 08:00:13.450 SEV=9 IKEDBG/1 RPT=10 172.18.124.241
Group [ipsecgroup]
constructing ID

79 02/07/2002 08:00:13.450 SEV=9 IKEDBG/0 RPT=84
Group [ipsecgroup]
construct hash payload

80 02/07/2002 08:00:13.450 SEV=9 IKEDBG/0 RPT=85 172.18.124.241
Group [ipsecgroup]
computing hash

81 02/07/2002 08:00:13.450 SEV=9 IKEDBG/46 RPT=5 172.18.124.241
Group [ipsecgroup]
constructing Cisco Unity VID payload

82 02/07/2002 08:00:13.450 SEV=9 IKEDBG/46 RPT=6 172.18.124.241
Group [ipsecgroup]
constructing xauth V6 VID payload

83 02/07/2002 08:00:13.450 SEV=9 IKEDBG/46 RPT=7 172.18.124.241
Group [ipsecgroup]
constructing dpd vid payload

84 02/07/2002 08:00:13.450 SEV=9 IKEDBG/46 RPT=8 172.18.124.241
Group [ipsecgroup]
constructing VID payload

85 02/07/2002 08:00:13.450 SEV=9 IKEDBG/48 RPT=2 172.18.124.241
Group [ipsecgroup]
Send Altiga GW VID

86 02/07/2002 08:00:13.450 SEV=8 IKEDBG/0 RPT=86 172.18.124.241
SENDING Message (msgid=0) with payloads :
HDR + SA (1) + KE (4) + NONCE (10) + ID (5) + HASH (8) + VENDOR (13) + VENDOR (1
3) + VENDOR (13) + VENDOR (13) + NONE (0) ... total length : 344

89 02/07/2002 08:00:13.480 SEV=8 IKEDBG/0 RPT=87 172.18.124.241
RECEIVED Message (msgid=0) with payloads :
HDR + HASH (8) + NOTIFY (11) + NONE (0) ... total length : 76

91 02/07/2002 08:00:13.480 SEV=9 IKEDBG/0 RPT=88 172.18.124.241
Group [ipsecgroup]
processing hash

92 02/07/2002 08:00:13.480 SEV=9 IKEDBG/0 RPT=89 172.18.124.241
Group [ipsecgroup]
computing hash

93 02/07/2002 08:00:13.480 SEV=9 IKEDBG/0 RPT=90 172.18.124.241
Group [ipsecgroup]
Processing Notify payload

94 02/07/2002 08:00:13.480 SEV=9 IKEDBG/0 RPT=91 172.18.124.241
Group [ipsecgroup]
```

```
constructing blank hash

95 02/07/2002 08:00:13.480 SEV=9 IKEDBG/0 RPT=92 172.18.124.241
Group [ipsecgroup]
constructing qm hash

96 02/07/2002 08:00:13.480 SEV=8 IKEDBG/0 RPT=93 172.18.124.241
SENDING Message (msgid=ec88ba81) with payloads :
HDR + HASH (8) + ATTR (14) + NONE (0) ... total length : 100

98 02/07/2002 08:00:21.810 SEV=8 IKEDBG/0 RPT=94 172.18.124.241
RECEIVED Message (msgid=ec88ba81) with payloads :
HDR + HASH (8) + ATTR (14) + NONE (0) ... total length : 85

100 02/07/2002 08:00:21.810 SEV=9 IKEDBG/1 RPT=11
process_attr(): Enter!

101 02/07/2002 08:00:21.810 SEV=9 IKEDBG/1 RPT=12
Processing MODE_CFG Reply attributes.

102 02/07/2002 08:00:21.810 SEV=8 AUTHDBG/1 RPT=3
AUTH_Open() returns 137

103 02/07/2002 08:00:21.810 SEV=7 AUTH/12 RPT=3
Authentication session opened: handle = 137

104 02/07/2002 08:00:21.810 SEV=8 AUTHDBG/3 RPT=3
AUTH_PutAttrTable(137, 728a84)

105 02/07/2002 08:00:21.810 SEV=8 AUTHDBG/5 RPT=1
AUTH_Authenticate(137, 50093bc, 4b5708)

106 02/07/2002 08:00:21.810 SEV=8 AUTHDBG/59 RPT=3
AUTH_BindServer(9b1544c, 0, 0)

107 02/07/2002 08:00:21.810 SEV=9 AUTHDBG/69 RPT=3
Auth Server 16b3fa0 has been bound to ACB 9b1544c, sessions = 1

108 02/07/2002 08:00:21.810 SEV=8 AUTHDBG/65 RPT=3
AUTH_CreateTimer(9b1544c, 0, 0)

109 02/07/2002 08:00:21.810 SEV=9 AUTHDBG/72 RPT=3
Reply timer created: handle = 3B4001A

110 02/07/2002 08:00:21.810 SEV=8 AUTHDBG/61 RPT=3
AUTH_BuildMsg(9b1544c, 0, 0)

111 02/07/2002 08:00:21.810 SEV=8 AUTHDBG/64 RPT=3
AUTH_StartTimer(9b1544c, 0, 0)

112 02/07/2002 08:00:21.810 SEV=9 AUTHDBG/73 RPT=3
Reply timer started: handle = 3B4001A, timestamp = 10086157, timeout = 30000

113 02/07/2002 08:00:21.810 SEV=8 AUTHDBG/62 RPT=3
AUTH_SndRequest(9b1544c, 0, 0)

114 02/07/2002 08:00:21.810 SEV=8 AUTHDBG/50 RPT=5
IntDB_Decode(62b6d00, 102)

115 02/07/2002 08:00:21.810 SEV=8 AUTHDBG/47 RPT=5
IntDB_Xmt(9b1544c)

116 02/07/2002 08:00:21.810 SEV=9 AUTHDBG/71 RPT=3
xmit_cnt = 1
```

```
117 02/07/2002 08:00:21.810 SEV=8 AUTHDBG/47 RPT=6
IntDB_Xmt(9b1544c)

118 02/07/2002 08:00:21.910 SEV=8 AUTHDBG/49 RPT=3
IntDB_Match(9b1544c, 2ebe71c)

119 02/07/2002 08:00:21.910 SEV=8 AUTHDBG/63 RPT=3
AUTH_RcvReply(9b1544c, 0, 0)

120 02/07/2002 08:00:21.910 SEV=8 AUTHDBG/50 RPT=6
IntDB_Decode(2ebe71c, 62)

121 02/07/2002 08:00:21.910 SEV=8 AUTHDBG/48 RPT=3
IntDB_Rcv(9b1544c)

122 02/07/2002 08:00:21.910 SEV=8 AUTHDBG/66 RPT=3
AUTH_DeleteTimer(9b1544c, 0, 0)

123 02/07/2002 08:00:21.910 SEV=9 AUTHDBG/74 RPT=3
Reply timer stopped: handle = 3B4001A, timestamp = 10086167

124 02/07/2002 08:00:21.910 SEV=8 AUTHDBG/58 RPT=3
AUTH_Callback(9b1544c, 0, 0)

125 02/07/2002 08:00:21.910 SEV=6 AUTH/4 RPT=1 172.18.124.241
Authentication successful: handle = 137, server = Internal, user = ipsecuser

126 02/07/2002 08:00:21.910 SEV=8 AUTHDBG/3 RPT=4
AUTH_PutAttrTable(137, 1861c60)

127 02/07/2002 08:00:21.910 SEV=8 AUTHDBG/60 RPT=3
AUTH_UnbindServer(9b1544c, 0, 0)

128 02/07/2002 08:00:21.910 SEV=9 AUTHDBG/70 RPT=3
Auth Server 16b3fa0 has been unbound from ACB 9b1544c, sessions = 0

129 02/07/2002 08:00:21.910 SEV=8 AUTHDBG/59 RPT=4
AUTH_BindServer(9b1544c, 0, 0)

130 02/07/2002 08:00:21.910 SEV=9 AUTHDBG/69 RPT=4
Auth Server 16b3fa0 has been bound to ACB 9b1544c, sessions = 1

131 02/07/2002 08:00:21.910 SEV=8 AUTHDBG/65 RPT=4
AUTH_CreateTimer(9b1544c, 0, 0)

132 02/07/2002 08:00:21.910 SEV=9 AUTHDBG/72 RPT=4
Reply timer created: handle = 3B5001A

133 02/07/2002 08:00:21.910 SEV=8 AUTHDBG/61 RPT=4
AUTH_BuildMsg(9b1544c, 0, 0)

134 02/07/2002 08:00:21.910 SEV=8 AUTHDBG/64 RPT=4
AUTH_StartTimer(9b1544c, 0, 0)

135 02/07/2002 08:00:21.910 SEV=9 AUTHDBG/73 RPT=4
Reply timer started: handle = 3B5001A, timestamp = 10086167, timeout = 30000

136 02/07/2002 08:00:21.910 SEV=8 AUTHDBG/62 RPT=4
AUTH_SndRequest(9b1544c, 0, 0)

137 02/07/2002 08:00:21.910 SEV=8 AUTHDBG/50 RPT=7
IntDB_Decode(2ec5350, 44)
```

```
138 02/07/2002 08:00:21.910 SEV=8 AUTHDBG/47 RPT=7
IntDB_Xmt(9b1544c)

139 02/07/2002 08:00:21.910 SEV=9 AUTHDBG/71 RPT=4
xmit_cnt = 1

140 02/07/2002 08:00:21.910 SEV=8 AUTHDBG/47 RPT=8
IntDB_Xmt(9b1544c)

141 02/07/2002 08:00:22.010 SEV=8 AUTHDBG/49 RPT=4
IntDB_Match(9b1544c, 2ec3f64)

142 02/07/2002 08:00:22.010 SEV=8 AUTHDBG/63 RPT=4
AUTH_RcvReply(9b1544c, 0, 0)

143 02/07/2002 08:00:22.010 SEV=8 AUTHDBG/50 RPT=8
IntDB_Decode(2ec3f64, 44)

144 02/07/2002 08:00:22.010 SEV=8 AUTHDBG/48 RPT=4
IntDB_Rcv(9b1544c)

145 02/07/2002 08:00:22.010 SEV=8 AUTHDBG/66 RPT=4
AUTH_DeleteTimer(9b1544c, 0, 0)

146 02/07/2002 08:00:22.010 SEV=9 AUTHDBG/74 RPT=4
Reply timer stopped: handle = 3B5001A, timestamp = 10086177

147 02/07/2002 08:00:22.010 SEV=8 AUTHDBG/58 RPT=4
AUTH_Callback(9b1544c, 0, 0)

148 02/07/2002 08:00:22.010 SEV=6 AUTH/41 RPT=3 172.18.124.241
Authentication successful: handle = 137, server = Internal, group = ipsecgroup

149 02/07/2002 08:00:22.010 SEV=8 AUTHDBG/3 RPT=5
AUTH_PutAttrTable(137, 1861c60)

150 02/07/2002 08:00:22.010 SEV=8 AUTHDBG/60 RPT=4
AUTH_UnbindServer(9b1544c, 0, 0)

151 02/07/2002 08:00:22.010 SEV=9 AUTHDBG/70 RPT=4
Auth Server 16b3fa0 has been unbound from ACB 9b1544c, sessions = 0

152 02/07/2002 08:00:22.010 SEV=8 AUTHDBG/59 RPT=5
AUTH_BindServer(9b1544c, 0, 0)

153 02/07/2002 08:00:22.010 SEV=9 AUTHDBG/69 RPT=5
Auth Server 16b3fa0 has been bound to ACB 9b1544c, sessions = 1

154 02/07/2002 08:00:22.010 SEV=8 AUTHDBG/65 RPT=5
AUTH_CreateTimer(9b1544c, 0, 0)

155 02/07/2002 08:00:22.010 SEV=9 AUTHDBG/72 RPT=5
Reply timer created: handle = 3B6001A

156 02/07/2002 08:00:22.010 SEV=8 AUTHDBG/61 RPT=5
AUTH_BuildMsg(9b1544c, 0, 0)

157 02/07/2002 08:00:22.010 SEV=8 AUTHDBG/64 RPT=5
AUTH_StartTimer(9b1544c, 0, 0)

158 02/07/2002 08:00:22.010 SEV=9 AUTHDBG/73 RPT=5
Reply timer started: handle = 3B6001A, timestamp = 10086177, timeout = 30000
```

```
159 02/07/2002 08:00:22.010 SEV=8 AUTHDBG/62 RPT=5
AUTH_SndRequest(9b1544c, 0, 0)

160 02/07/2002 08:00:22.010 SEV=8 AUTHDBG/50 RPT=9
IntDB_Decode(2ec39ec, 44)

161 02/07/2002 08:00:22.010 SEV=8 AUTHDBG/47 RPT=9
IntDB_Xmt(9b1544c)

162 02/07/2002 08:00:22.010 SEV=9 AUTHDBG/71 RPT=5
xmit_cnt = 1

163 02/07/2002 08:00:22.010 SEV=8 AUTHDBG/47 RPT=10
IntDB_Xmt(9b1544c)

164 02/07/2002 08:00:22.110 SEV=8 AUTHDBG/49 RPT=5
IntDB_Match(9b1544c, 2ec5350)

165 02/07/2002 08:00:22.110 SEV=8 AUTHDBG/63 RPT=5
AUTH_RcvReply(9b1544c, 0, 0)

166 02/07/2002 08:00:22.110 SEV=8 AUTHDBG/50 RPT=10
IntDB_Decode(2ec5350, 44)

167 02/07/2002 08:00:22.110 SEV=8 AUTHDBG/48 RPT=5
IntDB_Rcv(9b1544c)

168 02/07/2002 08:00:22.110 SEV=8 AUTHDBG/66 RPT=5
AUTH_DeleteTimer(9b1544c, 0, 0)

169 02/07/2002 08:00:22.110 SEV=9 AUTHDBG/74 RPT=5
Reply timer stopped: handle = 3B6001A, timestamp = 10086187

170 02/07/2002 08:00:22.110 SEV=8 AUTHDBG/58 RPT=5
AUTH_Callback(9b1544c, 0, 0)

171 02/07/2002 08:00:22.110 SEV=6 AUTH/41 RPT=4 172.18.124.241
Authentication successful: handle = 137, server = Internal, group = ipsecgroup

172 02/07/2002 08:00:22.110 SEV=8 AUTHDBG/4 RPT=3
AUTH_GetAttrTable(137, 729c04)

173 02/07/2002 08:00:22.110 SEV=8 AUTHDBG/4 RPT=4
AUTH_GetAttrTable(137, 728c4c)

174 02/07/2002 08:00:22.110 SEV=7 IKEDBG/14 RPT=3 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
Authentication configured for Internal

175 02/07/2002 08:00:22.110 SEV=8 AUTHDBG/2 RPT=3
AUTH_Close(137)

176 02/07/2002 08:00:22.110 SEV=4 IKE/52 RPT=61 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
User (ipsecuser) authenticated.

177 02/07/2002 08:00:22.110 SEV=9 IKEDBG/0 RPT=95 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
constructing blank hash

178 02/07/2002 08:00:22.110 SEV=9 IKEDBG/0 RPT=96 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
constructing qm hash
```

```
179 02/07/2002 08:00:22.110 SEV=8 IKEDBG/0 RPT=97 172.18.124.241
SENDING Message (msgid=4cc78f4e) with payloads :
HDR + HASH (8) + ATTR (14) + NONE (0) ... total length : 60

181 02/07/2002 08:00:22.110 SEV=8 AUTHDBG/60 RPT=5
AUTH_UnbindServer(9b1544c, 0, 0)

182 02/07/2002 08:00:22.110 SEV=9 AUTHDBG/70 RPT=5
Auth Server 16b3fa0 has been unbound from ACB 9b1544c, sessions = 0

183 02/07/2002 08:00:22.110 SEV=8 AUTHDBG/10 RPT=3
AUTH_Int_FreeAuthCB(9b1544c)

184 02/07/2002 08:00:22.110 SEV=7 AUTH/13 RPT=3
Authentication session closed: handle = 137

185 02/07/2002 08:00:22.110 SEV=8 IKEDBG/0 RPT=98 172.18.124.241
RECEIVED Message (msgid=4cc78f4e) with payloads :
HDR + HASH (8) + ATTR (14) + NONE (0) ... total length : 56

187 02/07/2002 08:00:22.110 SEV=9 IKEDBG/1 RPT=13
process_attr(): Enter!

188 02/07/2002 08:00:22.110 SEV=9 IKEDBG/1 RPT=14
Processing cfg ACK attributes

189 02/07/2002 08:00:22.180 SEV=8 IKEDBG/0 RPT=99 172.18.124.241
RECEIVED Message (msgid=38a7c320) with payloads :
HDR + HASH (8) + ATTR (14) + NONE (0) ... total length : 154

191 02/07/2002 08:00:22.180 SEV=9 IKEDBG/1 RPT=15
process_attr(): Enter!

192 02/07/2002 08:00:22.180 SEV=9 IKEDBG/1 RPT=16
Processing cfg Request attributes

193 02/07/2002 08:00:22.180 SEV=9 IKEDBG/53 RPT=1
MODE_CFG: Received request for IPV4 address!

194 02/07/2002 08:00:22.180 SEV=9 IKEDBG/53 RPT=2
MODE_CFG: Received request for IPV4 net mask!

195 02/07/2002 08:00:22.180 SEV=9 IKEDBG/53 RPT=3
MODE_CFG: Received request for DNS server address!

196 02/07/2002 08:00:22.180 SEV=9 IKEDBG/53 RPT=4
MODE_CFG: Received request for WINS server address!

197 02/07/2002 08:00:22.180 SEV=6 IKE/130 RPT=1 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
Received unsupported transaction mode attribute: 5

199 02/07/2002 08:00:22.180 SEV=9 IKEDBG/53 RPT=5
MODE_CFG: Received request for Application Version!

200 02/07/2002 08:00:22.180 SEV=9 IKEDBG/53 RPT=6
MODE_CFG: Received request for Banner!

201 02/07/2002 08:00:22.180 SEV=9 IKEDBG/53 RPT=7
MODE_CFG: Received request for Save PW setting!

202 02/07/2002 08:00:22.180 SEV=9 IKEDBG/53 RPT=8
MODE_CFG: Received request for Default Domain Name!
```

```
203 02/07/2002 08:00:22.180 SEV=9 IKEDBG/53 RPT=9
MODE_CFG: Received request for Split Tunnel List!

204 02/07/2002 08:00:22.180 SEV=9 IKEDBG/53 RPT=10
MODE_CFG: Received request for PFS setting!

205 02/07/2002 08:00:22.180 SEV=9 IKEDBG/53 RPT=11
MODE_CFG: Received request for FWTYPE!

206 02/07/2002 08:00:22.180 SEV=9 IKEDBG/53 RPT=12
MODE_CFG: Received request for UDP Port!

207 02/07/2002 08:00:22.180 SEV=9 IKEDBG/31 RPT=1 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
Obtained IP addr (10.1.1.100) prior to initiating Mode Cfg (XAuth enabled)

209 02/07/2002 08:00:22.180 SEV=9 IKEDBG/0 RPT=100 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
constructing blank hash

210 02/07/2002 08:00:22.180 SEV=9 IKEDBG/0 RPT=101 172.18.124.241
0000: 00010004 0A010164 F0010000 F0070000     .......d........
0010: 00070062 43697363 6F205379 7374656D     ...bCisco System
0020: 732C2049 6E632E2F 56504E20 33303030     s, Inc./VPN 3000
0030: 20436F6E 63656E74 7261746F 72205665      Concentrator Ve
0040: 7273696F 6E20332E 352E5265 6C206275     rsion 3.5.Rel bu
0050: 696C7420 62792076 6D757270 6879206F     ilt by vmurphy o

216 02/07/2002 08:00:22.180 SEV=9 IKEDBG/0 RPT=102 172.18.124.241
0000: 6E204E6F 76203237 20323030 31203131     n Nov 27 2001 11
0010: 3A32323A 3331                           :22:31

218 02/07/2002 08:00:22.180 SEV=9 IKEDBG/0 RPT=103 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
constructing qm hash

219 02/07/2002 08:00:22.180 SEV=8 IKEDBG/0 RPT=104 172.18.124.241
SENDING Message (msgid=38a7c320) with payloads :
HDR + HASH (8) + ATTR (14) + NONE (0) ... total length : 174

221 02/07/2002 08:00:22.190 SEV=9 IKEDBG/21 RPT=1 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
Delay Quick Mode processing, Cert/Trans Exch/RM DSID in progress

223 02/07/2002 08:00:22.190 SEV=4 AUTH/22 RPT=86
User ipsecuser connected

224 02/07/2002 08:00:22.190 SEV=7 IKEDBG/22 RPT=1 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
Resume Quick Mode processing, Cert/Trans Exch/RM DSID completed

226 02/07/2002 08:00:22.200 SEV=4 IKE/119 RPT=68 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
PHASE 1 COMPLETED

227 02/07/2002 08:00:22.200 SEV=6 IKE/121 RPT=1 172.18.124.241
Keep-alive type for this connection: DPD

228 02/07/2002 08:00:22.200 SEV=7 IKEDBG/0 RPT=105 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
Starting phase 1 rekey timer: 82080000 (ms)

229 02/07/2002 08:00:22.200 SEV=9 IKEDBG/0 RPT=106 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
```

```
sending notify message

230 02/07/2002 08:00:22.200 SEV=9 IKEDBG/0 RPT=107 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
constructing blank hash

231 02/07/2002 08:00:22.200 SEV=9 IKEDBG/0 RPT=108 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
constructing qm hash

232 02/07/2002 08:00:22.200 SEV=8 IKEDBG/0 RPT=109 172.18.124.241
SENDING Message (msgid=be237358) with payloads :
HDR + HASH (8) + NOTIFY (11) + NONE (0) ... total length : 88

234 02/07/2002 08:00:22.200 SEV=8 IKEDBG/0 RPT=110 172.18.124.241
RECEIVED Message (msgid=472c326b) with payloads :
HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0) ... total leng
th : 792

237 02/07/2002 08:00:22.200 SEV=9 IKEDBG/0 RPT=111 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
processing hash

238 02/07/2002 08:00:22.200 SEV=9 IKEDBG/0 RPT=112 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
processing SA payload

239 02/07/2002 08:00:22.200 SEV=9 IKEDBG/1 RPT=17 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
processing nonce payload

240 02/07/2002 08:00:22.200 SEV=9 IKEDBG/1 RPT=18 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
Processing ID

241 02/07/2002 08:00:22.200 SEV=5 IKE/25 RPT=62 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
Received remote Proxy Host data in ID Payload:
Address 10.1.1.100, Protocol 0, Port 0

244 02/07/2002 08:00:22.200 SEV=9 IKEDBG/1 RPT=19 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
Processing ID

245 02/07/2002 08:00:22.200 SEV=5 IKE/24 RPT=61 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
Received local Proxy Host data in ID Payload:
Address 172.18.124.133, Protocol 0, Port 0

248 02/07/2002 08:00:22.200 SEV=8 IKEDBG/0 RPT=113
QM IsRekeyed old sa not found by addr

249 02/07/2002 08:00:22.200 SEV=5 IKE/66 RPT=121 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
IKE Remote Peer configured for SA: ESP-3DES-MD5

251 02/07/2002 08:00:22.200 SEV=9 IKEDBG/0 RPT=114 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
processing IPSEC SA

252 02/07/2002 08:00:22.200 SEV=8 IKEDBG/0 RPT=115
Proposal # 2, Transform # 1, Type ESP, Id Triple-DES
Parsing received transform:
  Phase 2 failure:
```

```
  Mismatched attr types for class HMAC Algorithm:
    Rcv'd: SHA
    Cfg'd: MD5

256 02/07/2002 08:00:22.200 SEV=7 IKEDBG/27 RPT=1 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
IPSec SA Proposal # 3, Transform # 1 acceptable

258 02/07/2002 08:00:22.200 SEV=7 IKEDBG/0 RPT=116 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
IKE: requesting SPI!

259 02/07/2002 08:00:22.200 SEV=9 IPSECDBG/6 RPT=1
IPSEC key message parse - msgtype 6, len 200, vers 1, pid 00000000, seq 129, err
 0, type 2, mode 0, state 32, label 0, pad 0, spi 00000000, encrKeyLen 0, hashKe
yLen 0, ivlen 0, alg 0, hmacAlg 0, lifetype 0, lifetime1 708648, lifetime2 0, ds
Id 300

263 02/07/2002 08:00:22.200 SEV=9 IPSECDBG/1 RPT=1
Processing KEY_GETSPI msg!

264 02/07/2002 08:00:22.200 SEV=7 IPSECDBG/13 RPT=1
Reserved SPI 1037485220

265 02/07/2002 08:00:22.200 SEV=8 IKEDBG/6 RPT=1
IKE got SPI from key engine: SPI = 0x3dd6c4a4

266 02/07/2002 08:00:22.200 SEV=9 IKEDBG/0 RPT=117 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
oakley constucting quick mode

267 02/07/2002 08:00:22.200 SEV=9 IKEDBG/0 RPT=118 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
constructing blank hash

268 02/07/2002 08:00:22.200 SEV=9 IKEDBG/0 RPT=119 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
constructing ISA_SA for ipsec

269 02/07/2002 08:00:22.200 SEV=5 IKE/75 RPT=121 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
Overriding Initiator's IPSec rekeying duration from 2147483 to 28800 seconds

271 02/07/2002 08:00:22.200 SEV=9 IKEDBG/1 RPT=20 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
constructing ipsec nonce payload

272 02/07/2002 08:00:22.200 SEV=9 IKEDBG/1 RPT=21 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
constructing proxy ID

273 02/07/2002 08:00:22.200 SEV=7 IKEDBG/0 RPT=120 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
Transmitting Proxy Id:
  Remote host: 10.1.1.100  Protocol 0  Port 0
  Local host:  172.18.124.133  Protocol 0  Port 0

277 02/07/2002 08:00:22.200 SEV=7 IKEDBG/0 RPT=121 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
Sending RESPONDER LIFETIME notification to Initiator

279 02/07/2002 08:00:22.200 SEV=9 IKEDBG/0 RPT=122 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
constructing qm hash
```

```
280 02/07/2002 08:00:22.200 SEV=8 IKEDBG/0 RPT=123 172.18.124.241
SENDING Message (msgid=472c326b) with payloads :
HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NOTIFY (11) + NONE (0)
... total length : 172

283 02/07/2002 08:00:22.210 SEV=8 IKEDBG/0 RPT=124 172.18.124.241
RECEIVED Message (msgid=64c59a32) with payloads :
HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0) ... total leng
th : 796

286 02/07/2002 08:00:22.210 SEV=9 IKEDBG/0 RPT=125 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
processing hash

287 02/07/2002 08:00:22.210 SEV=9 IKEDBG/0 RPT=126 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
processing SA payload

288 02/07/2002 08:00:22.210 SEV=9 IKEDBG/1 RPT=22 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
processing nonce payload

289 02/07/2002 08:00:22.210 SEV=9 IKEDBG/1 RPT=23 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
Processing ID

290 02/07/2002 08:00:22.210 SEV=5 IKE/25 RPT=63 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
Received remote Proxy Host data in ID Payload:
Address 10.1.1.100, Protocol 0, Port 0

293 02/07/2002 08:00:22.210 SEV=9 IKEDBG/1 RPT=24 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
Processing ID

294 02/07/2002 08:00:22.210 SEV=5 IKE/34 RPT=61 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
Received local IP Proxy Subnet data in ID Payload:
 Address 0.0.0.0, Mask 0.0.0.0, Protocol 0, Port 0

297 02/07/2002 08:00:22.210 SEV=8 IKEDBG/0 RPT=127
QM IsRekeyed old sa not found by addr

298 02/07/2002 08:00:22.210 SEV=5 IKE/66 RPT=122 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
IKE Remote Peer configured for SA: ESP-3DES-MD5

300 02/07/2002 08:00:22.210 SEV=9 IKEDBG/0 RPT=128 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
processing IPSEC SA

301 02/07/2002 08:00:22.210 SEV=8 IKEDBG/0 RPT=129
Proposal # 2, Transform # 1, Type ESP, Id Triple-DES
Parsing received transform:
  Phase 2 failure:
  Mismatched attr types for class HMAC Algorithm:
    Rcv'd: SHA
    Cfg'd: MD5

305 02/07/2002 08:00:22.210 SEV=7 IKEDBG/27 RPT=2 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
IPSec SA Proposal # 3, Transform # 1 acceptable
```

```
307 02/07/2002 08:00:22.210 SEV=7 IKEDBG/0 RPT=130 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
IKE: requesting SPI!

308 02/07/2002 08:00:22.210 SEV=9 IPSECDBG/6 RPT=2
IPSEC key message parse - msgtype 6, len 200, vers 1, pid 00000000, seq 130, err
 0, type 2, mode 0, state 32, label 0, pad 0, spi 00000000, encrKeyLen 0, hashKe
yLen 0, ivlen 0, alg 0, hmacAlg 0, lifetype 0, lifetime1 708648, lifetime2 0, ds
Id 300

312 02/07/2002 08:00:22.210 SEV=9 IPSECDBG/1 RPT=2
Processing KEY_GETSPI msg!

313 02/07/2002 08:00:22.210 SEV=7 IPSECDBG/13 RPT=2
Reserved SPI 1517437317

314 02/07/2002 08:00:22.210 SEV=8 IKEDBG/6 RPT=2
IKE got SPI from key engine: SPI = 0x5a724185

315 02/07/2002 08:00:22.210 SEV=9 IKEDBG/0 RPT=131 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
oakley constucting quick mode

316 02/07/2002 08:00:22.210 SEV=9 IKEDBG/0 RPT=132 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
constructing blank hash

317 02/07/2002 08:00:22.210 SEV=9 IKEDBG/0 RPT=133 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
constructing ISA_SA for ipsec

318 02/07/2002 08:00:22.210 SEV=5 IKE/75 RPT=122 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
Overriding Initiator's IPSec rekeying duration from 2147483 to 28800 seconds

320 02/07/2002 08:00:22.210 SEV=9 IKEDBG/1 RPT=25 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
constructing ipsec nonce payload

321 02/07/2002 08:00:22.210 SEV=9 IKEDBG/1 RPT=26 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
constructing proxy ID

322 02/07/2002 08:00:22.210 SEV=7 IKEDBG/0 RPT=134 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
Transmitting Proxy Id:
  Remote host: 10.1.1.100  Protocol 0  Port 0
  Local subnet:  0.0.0.0  mask 0.0.0.0 Protocol 0  Port 0

326 02/07/2002 08:00:22.210 SEV=7 IKEDBG/0 RPT=135 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
Sending RESPONDER LIFETIME notification to Initiator

328 02/07/2002 08:00:22.210 SEV=9 IKEDBG/0 RPT=136 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
constructing qm hash

329 02/07/2002 08:00:22.220 SEV=8 IKEDBG/0 RPT=137 172.18.124.241
SENDING Message (msgid=64c59a32) with payloads :
HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NOTIFY (11) + NONE (0)
... total length : 176

332 02/07/2002 08:00:22.220 SEV=8 IKEDBG/0 RPT=138 172.18.124.241
RECEIVED Message (msgid=472c326b) with payloads :
```

```
HDR + HASH (8) + NONE (0) ... total length : 48

334 02/07/2002 08:00:22.220 SEV=9 IKEDBG/0 RPT=139 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
processing hash

335 02/07/2002 08:00:22.220 SEV=9 IKEDBG/0 RPT=140 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
loading all IPSEC SAs

336 02/07/2002 08:00:22.220 SEV=9 IKEDBG/1 RPT=27 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
Generating Quick Mode Key!

337 02/07/2002 08:00:22.220 SEV=9 IKEDBG/1 RPT=28 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
Generating Quick Mode Key!

338 02/07/2002 08:00:22.220 SEV=7 IKEDBG/0 RPT=141 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
Loading host:
  Dst: 172.18.124.133
  Src: 10.1.1.100

340 02/07/2002 08:00:22.220 SEV=4 IKE/49 RPT=129 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
Security negotiation complete for User (ipsecuser)
Responder, Inbound SPI = 0x3dd6c4a4, Outbound SPI = 0x8104887e

343 02/07/2002 08:00:22.220 SEV=9 IPSECDBG/6 RPT=3
IPSEC key message parse - msgtype 1, len 624, vers 1, pid 00000000, seq 0, err 0
, type 2, mode 1, state 64, label 0, pad 0, spi 8104887e, encrKeyLen 24, hashKey
Len 16, ivlen 8, alg 2, hmacAlg 3, lifetype 0, lifetime1 708648, lifetime2 0, ds
Id 0

347 02/07/2002 08:00:22.220 SEV=9 IPSECDBG/1 RPT=3
Processing KEY_ADD msg!

348 02/07/2002 08:00:22.220 SEV=9 IPSECDBG/1 RPT=4
key_msghdr2secassoc(): Enter

349 02/07/2002 08:00:22.220 SEV=7 IPSECDBG/1 RPT=5
No USER filter configured

350 02/07/2002 08:00:22.220 SEV=9 IPSECDBG/1 RPT=6
KeyProcessAdd: Enter

351 02/07/2002 08:00:22.220 SEV=8 IPSECDBG/1 RPT=7
KeyProcessAdd: Adding outbound SA

352 02/07/2002 08:00:22.220 SEV=8 IPSECDBG/1 RPT=8
KeyProcessAdd: src 172.18.124.133 mask 0.0.0.0, dst 10.1.1.100 mask 0.0.0.0

353 02/07/2002 08:00:22.220 SEV=8 IPSECDBG/1 RPT=9
KeyProcessAdd: FilterIpsecAddIkeSa success

354 02/07/2002 08:00:22.220 SEV=9 IPSECDBG/6 RPT=4
IPSEC key message parse - msgtype 3, len 336, vers 1, pid 00000000, seq 0, err 0
, type 2, mode 1, state 32, label 0, pad 0, spi 3dd6c4a4, encrKeyLen 24, hashKey
Len 16, ivlen 8, alg 2, hmacAlg 3, lifetype 0, lifetime1 708648, lifetime2 0, ds
Id 0

358 02/07/2002 08:00:22.220 SEV=9 IPSECDBG/1 RPT=10
Processing KEY_UPDATE msg!
```

```
359 02/07/2002 08:00:22.220 SEV=9 IPSECDBG/1 RPT=11
Update inbound SA addresses

360 02/07/2002 08:00:22.220 SEV=9 IPSECDBG/1 RPT=12
key_msghdr2secassoc(): Enter

361 02/07/2002 08:00:22.220 SEV=7 IPSECDBG/1 RPT=13
No USER filter configured

362 02/07/2002 08:00:22.220 SEV=9 IPSECDBG/1 RPT=14
KeyProcessUpdate: Enter

363 02/07/2002 08:00:22.220 SEV=8 IPSECDBG/1 RPT=15
KeyProcessUpdate: success

364 02/07/2002 08:00:22.220 SEV=8 IKEDBG/7 RPT=1
IKE got a KEY_ADD msg for SA: SPI = 0x8104887e

365 02/07/2002 08:00:22.220 SEV=8 IKEDBG/0 RPT=142
pitcher: rcv KEY_UPDATE, spi 0x3dd6c4a4

366 02/07/2002 08:00:22.220 SEV=4 IKE/120 RPT=129 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
PHASE 2 COMPLETED (msgid=472c326b)

367 02/07/2002 08:00:22.280 SEV=8 IKEDBG/0 RPT=143 172.18.124.241
RECEIVED Message (msgid=64c59a32) with payloads :
HDR + HASH (8) + NONE (0) ... total length : 48

369 02/07/2002 08:00:22.280 SEV=9 IKEDBG/0 RPT=144 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
processing hash

370 02/07/2002 08:00:22.280 SEV=9 IKEDBG/0 RPT=145 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
loading all IPSEC SAs

371 02/07/2002 08:00:22.280 SEV=9 IKEDBG/1 RPT=29 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
Generating Quick Mode Key!

372 02/07/2002 08:00:22.280 SEV=9 IKEDBG/1 RPT=30 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
Generating Quick Mode Key!

373 02/07/2002 08:00:22.280 SEV=7 IKEDBG/0 RPT=146 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
Loading subnet:
  Dst: 0.0.0.0  mask: 0.0.0.0
  Src: 10.1.1.100

375 02/07/2002 08:00:22.280 SEV=4 IKE/49 RPT=130 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
Security negotiation complete for User (ipsecuser)
Responder, Inbound SPI = 0x5a724185, Outbound SPI = 0x285e6ed0

378 02/07/2002 08:00:22.280 SEV=9 IPSECDBG/6 RPT=5
IPSEC key message parse - msgtype 1, len 624, vers 1, pid 00000000, seq 0, err 0
, type 2, mode 1, state 64, label 0, pad 0, spi 285e6ed0, encrKeyLen 24, hashKey
Len 16, ivlen 8, alg 2, hmacAlg 3, lifetype 0, lifetime1 708648, lifetime2 0, ds
Id 0

382 02/07/2002 08:00:22.280 SEV=9 IPSECDBG/1 RPT=16
```

```
Processing KEY_ADD msg!

383 02/07/2002 08:00:22.280 SEV=9 IPSECDBG/1 RPT=17
key_msghdr2secassoc(): Enter

384 02/07/2002 08:00:22.280 SEV=7 IPSECDBG/1 RPT=18
No USER filter configured

385 02/07/2002 08:00:22.280 SEV=9 IPSECDBG/1 RPT=19
KeyProcessAdd: Enter

386 02/07/2002 08:00:22.280 SEV=8 IPSECDBG/1 RPT=20
KeyProcessAdd: Adding outbound SA

387 02/07/2002 08:00:22.280 SEV=8 IPSECDBG/1 RPT=21
KeyProcessAdd: src 0.0.0.0 mask 255.255.255.255, dst 10.1.1.100 mask 0.0.0.0

388 02/07/2002 08:00:22.280 SEV=8 IPSECDBG/1 RPT=22
KeyProcessAdd: FilterIpsecAddIkeSa success

389 02/07/2002 08:00:22.280 SEV=9 IPSECDBG/6 RPT=6
IPSEC key message parse - msgtype 3, len 336, vers 1, pid 00000000, seq 0, err 0
, type 2, mode 1, state 32, label 0, pad 0, spi 5a724185, encrKeyLen 24, hashKey
Len 16, ivlen 8, alg 2, hmacAlg 3, lifetype 0, lifetime1 708648, lifetime2 0, ds
Id 0

393 02/07/2002 08:00:22.280 SEV=9 IPSECDBG/1 RPT=23
Processing KEY_UPDATE msg!

394 02/07/2002 08:00:22.280 SEV=9 IPSECDBG/1 RPT=24
Update inbound SA addresses

395 02/07/2002 08:00:22.280 SEV=9 IPSECDBG/1 RPT=25
key_msghdr2secassoc(): Enter

396 02/07/2002 08:00:22.280 SEV=7 IPSECDBG/1 RPT=26
No USER filter configured

397 02/07/2002 08:00:22.280 SEV=9 IPSECDBG/1 RPT=27
KeyProcessUpdate: Enter

398 02/07/2002 08:00:22.280 SEV=8 IPSECDBG/1 RPT=28
KeyProcessUpdate: success

399 02/07/2002 08:00:22.280 SEV=8 IKEDBG/7 RPT=2
IKE got a KEY_ADD msg for SA: SPI = 0x285e6ed0

400 02/07/2002 08:00:22.280 SEV=8 IKEDBG/0 RPT=147
pitcher: rcv KEY_UPDATE, spi 0x5a724185

401 02/07/2002 08:00:22.280 SEV=4 IKE/120 RPT=130 172.18.124.241
Group [ipsecgroup] User [ipsecuser]
PHASE 2 COMPLETED (msgid=64c59a32)
```

Informations connexes

- Page d'assistance des concentrateurs VPN Cisco 3000
- Page d'assistance du Client VPN 3000 Series Cisco
- Négociation IPSec/Protocoles IKE
- Support et documentation techniques - Cisco Systems