

# VPN クライアントバージョン3.5 Solaris からの VPN 3000 コンセントレータへIPSec を設定する 方法

## 内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[設定](#)

[ネットワーク図](#)

[設定](#)

[確認](#)

[VPN コンセントレータへの接続](#)

[トラブルシューティング](#)

[デバッグ](#)

[関連情報](#)

## 概要

このドキュメントでは、VPN 3000 コンセントレータに接続するための VPN Client 3.5 for Solaris 2.6 の設定方法を説明します。

## 前提条件

### 要件

設定を開始する前に、次の前提条件を満たしていることを確認してください。

- この例では、グループ認証に事前共有キーを使用します。ユーザ名とパスワード（拡張認証）が、VPNコンセントレータの内部データベースと照合されます。
- VPN Clientが正しくインストールされている必要があります。インストールの詳細については、「[Solaris用VPN Clientのインストール](#)」を参照してください。
- VPN ClientとVPNコンセントレータのパブリックインターフェイスの間にIP接続が存在する必要があります。サブネットマスクとゲートウェイ情報を正しく設定する必要があります。

### [使用するコンポーネント](#)

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco VPN Client for Solaris 2.6バージョン3.5、3DESイメージ。(イメージ名称 : vpnclient-solaris5.6-3.5.Rel-k9.tar.Z)
- Cisco VPN Concentrator Type:3005 Bootcode Rev:Altiga Networks/VPN Concentrator Version 2.2.int\_9 Jan 19 2000 05:36:41 Software Rev:Cisco Systems, Inc./VPN 3000 Concentrator Series Version 3.1.Rel Aug 06 2001 13:47:37

このマニュアルの情報は、特定のラボ環境に置かれたデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期(デフォルト)設定の状態から起動しています。実稼動中のネットワークで作業をしている場合、実際にコマンドを使用する前に、その潜在的な影響について理解しておく必要があります。

## 表記法

ドキュメント表記の詳細は、『[シスコテクニカルティップスの表記法](#)』を参照してください。

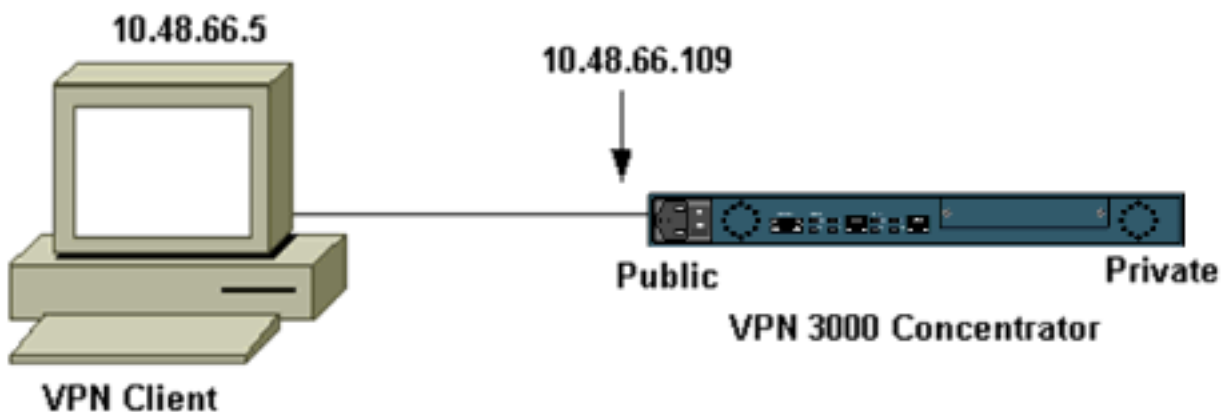
## 設定

このセクションでは、このドキュメントで説明する機能を設定するために必要な情報を提供しています。

注：この文書で使用されているコマンドの詳細を調べるには、「Command Lookup ツール」を使用してください(登録ユーザのみ)。

## ネットワーク図

このドキュメントでは次の図に示すネットワーク構成を使用しています。



注：VPN Client 3.5をVPNコンセントレータに接続するには、コンセントレータでバージョン3.0以降が必要です。

## 設定

### 接続用のユーザプロファイルの作成

ユーザプロファイルは/etc/CiscoSystemsVPNClient/Profilesディレクトリに保存されます。これらのテキストファイルには.pcf拡張子が付いており、VPNコンセントレータへの接続を確立するた

めに必要なパラメータが含まれています。新しいファイルを作成したり、既存のファイルを編集したりできます。プロファイルのディレクトリには、サンプルのプロファイルsample.pcfがあります。この例では、そのファイルを使用してtoCORPORATE.pcfという名前の新しいプロファイルを作成します。

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

お気に入りのテキストエディタを使用して、この新しいファイルtoCORPORATE.pcfを編集できます。ファイルを変更する前は、次のようになります。

**注：IPSec over Network Address Translation(NAT)を使用する場合、次の設定のEnableNatエントリでは、「EnableNat=0」ではなく「EnableNat=1」と表示される必要があります。**

```
[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
```

ユーザプロファイル[キーワード](#)の詳細については、「ユーザプロファイル」を参照してください。

プロファイルを正しく設定するには、次の情報に対応する値を最小限に抑える必要があります。

- VPNコンセントレータのホスト名またはパブリックIPアドレス(10.48.66.109)
- グループ名(RemoteClient)
- グループパスワード(cisco)
- ユーザ名(joe)

ファイルを編集して、次のような情報を表示します。

```
[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

## VPN コンセントレータの設定

VPN コンセントレータを設定するには、次の手順を使用します。

注：スペースの制限により、スクリーンキャプチャは一部または関連エリアのみを表示します。

1. アドレスプールを割り当てます。使用可能な範囲のIPアドレスを割り当てるには、ブラウザでVPN コンセントレータの内部インターフェイスをポイントし、**[Configuration] > [System] > [Address Management] > [Pools]**を選択します。**[Add]** をクリックします。ネットワークの内側にある他のデバイスと競合しない IP アドレスの範囲を指定します。

The screenshot shows the web interface for the VPN 3000 Concentrator Series Manager. The breadcrumb navigation is Configuration | System | Address Management | Pools. The main content area contains the text: "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**." Below this text is a table with the following structure:

IP Pool Entry	Actions
10.20.20.20 - 10.20.20.200	<input type="button" value="Add"/> <input type="button" value="Modify"/> <input type="button" value="Delete"/>

2. VPN コンセントレータにプールを使用するように指示するには、**[Configuration] > [System] > [Address Management] > [Assignment]**を選択し、**[Use Address Pools]**ボックスをオンにし、**[Apply]** をクリックします。

**VPN 3000 Concentrator Series Manager**

**Configuration | System | Address Management | Assignment**

This section presents Address Assignment options. Each of the following

**Use Client Address**  Check to use the IP address user/group configuration.

**Use Address from Authentication Server**  Check to use an IP address

**Use DHCP**  Check to use DHCP to obtain

**Use Address Pools**  Check to use internal address client.

Apply Cancel

3. グループとパスワードを追加します。[Configuration] > [User Management] > [Groups]を選択し、[Add Group]をクリックします。正しい情報を入力し、[Add]をクリックして情報を送信してください。この例では、「RemoteClient」という名前のグループをパスワード「cisco」で使用しています。

**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 base **Inherit?** box and enter a new value to override base group values.

**Identity General IPsec Client FW PPTP/L2TP**

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 <input type="checkbox"/>	External groups are configured on an external authentication server. Internal groups are configured on the VPN 3000 Concentrator Series's Internal Database.

Add Cancel

4. グループの[IPsec]タブで、認証が[Internal]に設定されていることを確認します。

Configuration | User Management | Groups | Modify RemoteClient

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

Identity | General | **IPSec** | Client FW | PPTP/L2TP

IPSec Parameters		
Attribute	Value	Inherit?
IPSec SA	ESP-3DES-MD5	<input checked="" type="checkbox"/>
IKE Peer Identity Validation	If supported by certificate	<input checked="" type="checkbox"/>
IKE Keepalives	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Reauthentication on Rekey	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Tunnel Type	Remote Access	<input checked="" type="checkbox"/>
Remote Access Parameter		
Group Lock	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Authentication	Internal	<input checked="" type="checkbox"/>

5. グループの[General]タブで、トンネリングプロトコルとして[IPSec]が選択されていることを確認します。

General Parameters			
Attribute	Value	Inherit?	
Access Hours	-No Restrictions-	<input checked="" type="checkbox"/>	Select the
Simultaneous Logins	3	<input checked="" type="checkbox"/>	Enter the r
Minimum Password Length	8	<input checked="" type="checkbox"/>	Enter the r
Allow Alphabetic-Only Passwords	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Enter whe be added
Idle Timeout	30	<input checked="" type="checkbox"/>	(minutes) l
Maximum Connect Time	0	<input checked="" type="checkbox"/>	(minutes) l
Filter	-None-	<input checked="" type="checkbox"/>	Enter the f
Primary DNS		<input checked="" type="checkbox"/>	Enter the l
Secondary DNS		<input checked="" type="checkbox"/>	Enter the l
Primary WINS		<input checked="" type="checkbox"/>	Enter the l
Secondary WINS		<input checked="" type="checkbox"/>	Enter the l
Tunneling Protocols	<input type="checkbox"/> PPTP <input type="checkbox"/> L2TP <input checked="" type="checkbox"/> IPSec <input type="checkbox"/> L2TP over IPSec	<input type="checkbox"/>	Select the
			Check to

6. ユーザをVPNコンソントレータに追加するには、[Configuration] > [User Management] > [Users]を選択し、[Add]をクリックします。

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	<input type="button" value="Add"/> <input type="button" value="Modify"/> <input type="button" value="Delete"/>

7. グループの正しい情報を入力し、[適用]をクリックして情報を送信してください。

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 **Inherit?** box to set a field that you want to default to the user value.

**Identity** | General | IPSec | PPTP/L2TP

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 <input type="checkbox"/>	Enter the group to which this user belongs.
IP Address	<input type="text"/>	Enter the IP address assigned to this user.
Subnet Mask	<input type="text"/>	Enter the subnet mask assigned to this user.

## 確認

### [VPN コンセントレータへの接続](#)

VPN Clientとコンセントレータを設定したので、新しいプロファイルはVPNコンセントレータに接続できます。

```
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 >
```

## トラブルシューティング

ここでは、設定のトラブルシューティングに使用できる情報を示します。

### デバッグ

デバッグを有効にするには、`ipsecclog`コマンドを使用します。次に例を示します。

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

### コンセントレータへの接続時のクライアントのデバッグ

```
[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

## [VPNコンセントレータのデバッグ](#)

イベント接続の失敗が発生した場合は、[Configuration] > [System] > [Events] > [Classes]を選択して、次のデバッグをオンにします。

- AUTH : ログ1-13の重大度
- IKE : ログの重大度1 ~ 6
- IPSEC : ログ1 ~ 6の重大度

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.](#)

Configured Event Classes	Actions
AUTH	<input type="button" value="Add"/> <input type="button" value="Modify"/> <input type="button" value="Delete"/>
IKE	
IPSEC	

ログを表示するには、[Monitoring] > [Event Log]を選択します。

## 関連情報

- [Cisco VPN 3000 シリーズ コンセントレータに関するサポート ページ](#)
- [Cisco VPN 3000 シリーズ クライアントに関するサポート ページ](#)
- [IPSec に関するサポート ページ](#)
- [テクニカルサポート - Cisco Systems](#)