

Konfigurieren von IPSec von VPN Client Version 3.5 Solaris zu einem VPN 3000-Konzentrator

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konventionen](#)

[Konfigurieren](#)

[Netzwerkdiagramm](#)

[Konfigurationen](#)

[Überprüfen](#)

[Herstellen einer Verbindung mit dem VPN Concentrator](#)

[Fehlerbehebung](#)

[Debugger](#)

[Zugehörige Informationen](#)

[Einführung](#)

In diesem Dokument wird veranschaulicht, wie der VPN-Client 3.5 für Solaris 2.6 für die Verbindung mit einem VPN 300-Konzentrator konfiguriert wird.

[Voraussetzungen](#)

[Anforderungen](#)

Bevor Sie diese Konfiguration versuchen, stellen Sie sicher, dass Sie die folgenden Voraussetzungen erfüllen.

- In diesem Beispiel wird der vorinstallierte Schlüssel für die Gruppenauthentifizierung verwendet. Benutzername und Kennwort (erweiterte Authentifizierung) werden mit der internen Datenbank des VPN Concentrator abgeglichen.
- Der VPN-Client muss korrekt installiert sein. Weitere Informationen zur Installation finden Sie unter [Installieren des VPN-Clients für Solaris](#).
- Es muss eine IP-Verbindung zwischen dem VPN-Client und der öffentlichen Schnittstelle des VPN-Concentrators bestehen. Die Subnetzmaske und die Gateway-Informationen müssen korrekt eingestellt sein.

[Verwendete Komponenten](#)

Die Informationen in diesem Dokument basieren auf diesen Software- und Hardwareversionen.

- Cisco VPN Client für Solaris 2.6 Version 3.5, 3DES-Image (Bildname: vpnclient-solaris5.6-3.5.Rel-k9.tar.Z)
- Cisco VPN Concentrator-Typ: 3005 Bootcode Rev: Altiga Networks/VPN Concentrator Version 2.2.int_9 Jan 19 200 05:36:41 Software Rev: Cisco Systems, Inc./VPN Concentrator der Serie 3.1.Rel. Aug. 2001 13:47:37

Die in diesem Dokument enthaltenen Informationen wurden aus Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Sie in einem Live-Netzwerk arbeiten, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen, bevor Sie es verwenden.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den [Cisco Technical Tips Conventions](#).

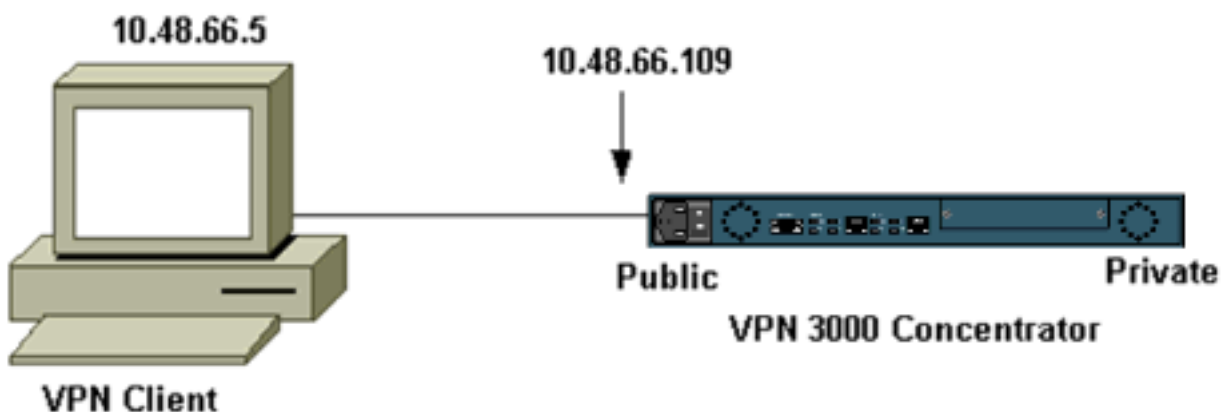
Konfigurieren

In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

Hinweis: Um weitere Informationen zu den in diesem Dokument verwendeten Befehlen zu erhalten, verwenden Sie das [Command Lookup Tool](#) ([nur registrierte Kunden](#)).

Netzwerkdiagramm

In diesem Dokument wird die im Diagramm unten dargestellte Netzwerkeinrichtung verwendet.



Hinweis: Für die Verbindung des VPN-Clients 3.5 mit dem VPN-Konzentrator benötigen Sie Version 3.0 oder höher auf dem Konzentrator.

Konfigurationen

Erstellen eines Benutzerprofils für die Verbindung

Die Benutzerprofile werden im Verzeichnis /etc/CiscoSystemsVPNClient/Profiles gespeichert.

Diese Textdateien haben die Erweiterung .pcf und enthalten Parameter, die zum Herstellen einer Verbindung mit einem VPN-Konzentrator erforderlich sind. Sie können eine neue Datei erstellen oder eine vorhandene bearbeiten. Sie sollten ein Beispielprofil, sample.pcf, im Profilverzeichnis finden. Dieses Beispiel folgt der Verwendung dieser Datei, um ein neues Profil mit dem Namen CORPORATE.pcf zu erstellen.

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

Sie können diese neue Datei mit Ihrem bevorzugten Texteditor in CORPORATE.pcf bearbeiten. Vor Änderungen sieht die Datei wie folgt aus.

Hinweis: Wenn Sie IPSec über Network Address Translation (NAT) verwenden möchten, muss der EnableNat-Eintrag in der Konfiguration unten "EnableNat=1" statt "EnableNat=0" heißen.

```
[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
```

Eine Beschreibung der Schlüsselwörter für Benutzerprofile [finden Sie](#) unter Benutzerprofile.

Um Ihr Profil erfolgreich konfigurieren zu können, müssen Sie mindestens die entsprechenden Werte für die folgenden Informationen kennen.

- Der Hostname oder die öffentliche IP-Adresse des VPN Concentrator (10.48.66.109)
- Gruppenname (RemoteClient)
- Das Gruppenkennwort (cisco)
- Der Benutzername (joe)

Bearbeiten Sie die Datei mit Ihren Informationen, sodass sie der folgenden ähnelt.

```
[main]  
Description=Connection to the corporate  
Host=10.48.66.109  
AuthType=1  
GroupName=RemoteClient  
GroupPwd=cisco  
EnableISPConnect=0
```

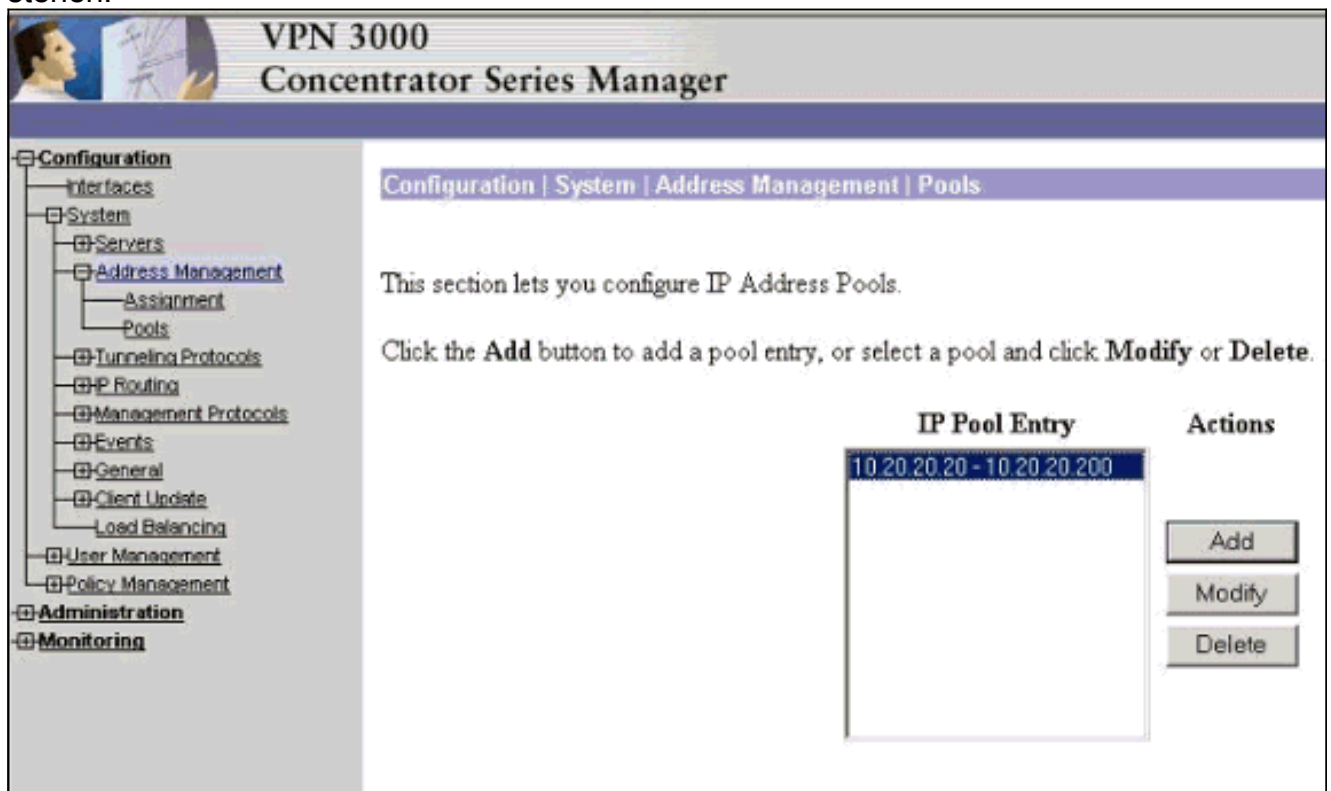
ISPConnectType=0
ISPConnect=
ISPCommand=
Username=joe
SaveUserPassword=0
EnableBackup=0
BackupServer=
EnableNat=0
CertStore=0
CertName=
CertPath=
CertSubjectName=
CertSerialHash=00000000000000000000000000000000
DHGroup=2
ForceKeepAlives=0

Konfigurieren des VPN Concentrator

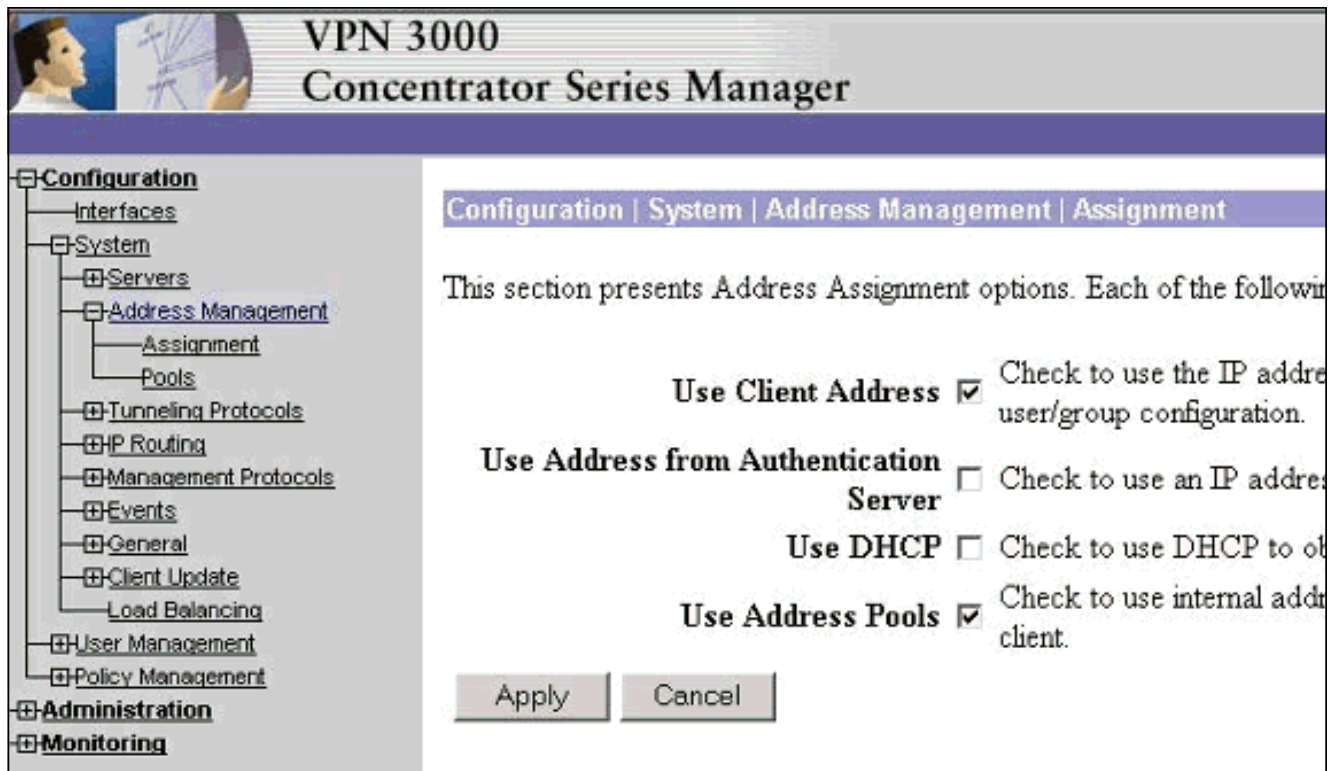
Führen Sie die folgenden Schritte aus, um den VPN-Konzentrator zu konfigurieren.

Hinweis: Aufgrund von Platzbeschränkungen zeigen Screenshots nur teilweise oder relevante Bereiche an.

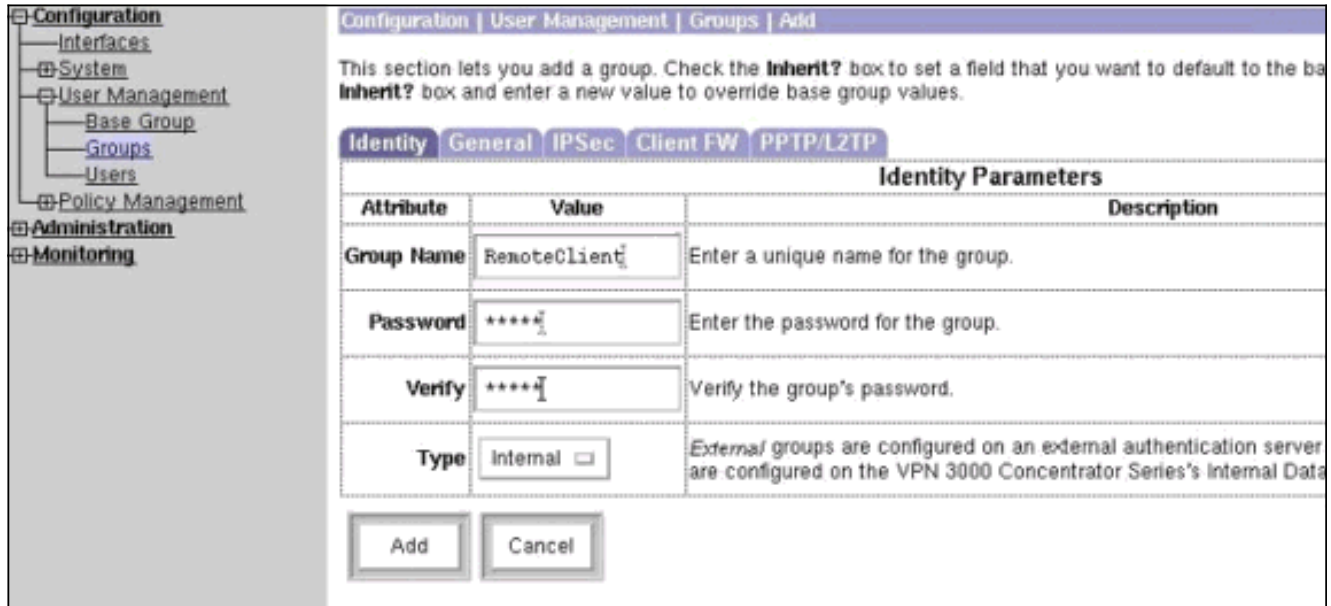
1. Weisen Sie den Adresspool zu. Um einen verfügbaren IP-Adressbereich zuzuweisen, verweisen Sie einen Browser auf die interne Schnittstelle des VPN Concentrator, und wählen Sie **Configuration > System > Address Management > Pools (Konfiguration > System > Adressverwaltung > Pools)**. Klicken Sie auf **Hinzufügen**. Geben Sie einen Bereich von IP-Adressen an, die nicht mit anderen Geräten im internen Netzwerk in Konflikt stehen.



2. Um dem VPN-Concentrator mitzuteilen, dass er den Pool verwenden soll, wählen Sie **Configuration > System > Address Management > Assignment** aus, aktivieren Sie das Kontrollkästchen **Use Address Pools (Adresspools verwenden)**, und klicken Sie dann auf **Apply (Übernehmen)**.



3. Fügen Sie eine Gruppe und ein Kennwort hinzu. Wählen Sie **Konfiguration > Benutzerverwaltung > Gruppen aus**, und klicken Sie dann auf **Gruppe hinzufügen**. Geben Sie die richtigen Informationen ein, und klicken Sie dann auf **Hinzufügen**, um die Informationen zu senden. In diesem Beispiel wird eine Gruppe mit dem Namen "RemoteClient" und dem Kennwort "cisco" verwendet.



4. Überprüfen Sie auf der Registerkarte "IPSec" der Gruppe, ob die Authentifizierung auf "Intern" eingestellt ist.

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. Überprüfen Sie auf der Registerkarte Allgemein der Gruppe, ob IPSec als Tunneling-Protokolle ausgewählt ist.

Configuration | User Management | Groups | Modify RemoteClient

General Parameters

Attribute	Value	Inherit?	
Access Hours	-No Restrictions-	<input checked="" type="checkbox"/>	Select the
Simultaneous Logins	3	<input checked="" type="checkbox"/>	Enter the
Minimum Password Length	8	<input checked="" type="checkbox"/>	Enter the
Allow Alphabetic-Only Passwords	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Enter whe be added
Idle Timeout	30	<input checked="" type="checkbox"/>	(minutes) I
Maximum Connect Time	0	<input checked="" type="checkbox"/>	(minutes) I
Filter	-None-	<input checked="" type="checkbox"/>	Enter the f
Primary DNS		<input checked="" type="checkbox"/>	Enter the I
Secondary DNS		<input checked="" type="checkbox"/>	Enter the I
Primary WINS		<input checked="" type="checkbox"/>	Enter the I
Secondary WINS		<input checked="" type="checkbox"/>	Enter the I
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. Um den Benutzer dem VPN-Konzentrator hinzuzufügen, wählen Sie **Konfiguration > Benutzerverwaltung > Benutzer** aus, und klicken Sie dann auf

Hinzufügen.

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. Geben Sie die richtigen Informationen für die Gruppe ein, und klicken Sie dann auf **Apply**, um die Informationen zu senden.

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.

Überprüfen

[Herstellen einer Verbindung mit dem VPN Concentrator](#)

Nachdem der VPN-Client und der Concentrator konfiguriert wurden, sollte das neue Profil für die Verbindung mit dem VPN-Konzentrator verwendet werden.

```
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 >
```

Fehlerbehebung

Dieser Abschnitt enthält Informationen zur Fehlerbehebung in Ihrer Konfiguration.

Debugger

Um das Debuggen zu aktivieren, verwenden Sie den Befehl `ipsecclog`. Ein Beispiel ist unten dargestellt.

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

[Debuggen auf dem Client beim Herstellen einer Verbindung mit dem Concentrator](#)

[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

[Debuggen auf dem VPN Concentrator](#)

Wählen Sie **Configuration > System > Events > Classes (Konfiguration > System > Ereignisse > Klassen)** aus, um das folgende Debugging zu aktivieren, wenn Fehler bei der Verbindung auftreten.

- **AUTH** - Schweregrad für Protokoll 1-13
- **IKE** - Schweregrad für Protokoll 1-6

- IPSEC - Schweregrad für Protokoll 1-6

Configuration | System | Events | Classes

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

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

[Click here to configure general event parameters.](#)

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

Sie können das Protokoll anzeigen, indem Sie **Überwachung > Ereignisprotokoll** auswählen.

Zugehörige Informationen

- [Support-Seite für Cisco VPN Concentrator der Serie 3000](#)
- [Cisco VPN Client Support-Seite der Serie 3000](#)
- [IPSec-Support-Seite](#)
- [Technischer Support - Cisco Systems](#)