Configuring IPSec from VPN Client Version 3.5 Solaris to a VPN 3000 Concentrator

Document ID: 18886

Contents

Introduction Prerequisites Requirements Components Used Conventions Configure Network Diagram Configurations Verify Connecting to the VPN Concentrator Troubleshoot Debugs Related Information Introduction

This document illustrates how to configure the VPN Client 3.5 for Solaris 2.6 to connect to a VPN 3000 Concentrator.

Prerequisites

Requirements

Before attempting this configuration, please ensure that you meet the following prerequisites.

- This example uses pre-shared key for group authentication. The username and password (extended authentication) are checked against the internal database of the VPN Concentrator.
- The VPN Client must be correctly installed. Refer to Installing the VPN Client for Solaris for details on the installation.
- IP connectivity must exist between the VPN Client and the public interface of the VPN Concentrator. Subnet mask and gateway information must be set properly.

Components Used

The information in this document is based on these software and hardware versions.

- Cisco VPN Client for Solaris 2.6 version 3.5, 3DES image. (image name: 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

The information presented in this document was created from devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If you are working in a live

network, ensure that you understand the potential impact of any command before using it.

Conventions

For more information on document conventions, see the Cisco Technical Tips Conventions.

Configure

In this section, you are presented with the information to configure the features described in this document.

Note: To find additional information on the commands used in this document, use the Command Lookup Tool (registered customers only).

Network Diagram

This document uses the network setup shown in the diagram below.



Note: For the VPN Client 3.5 to connect to the VPN Concentrator, you need version 3.0 or later on the concentrator.

Configurations

Creating a User Profile for the Connection

The user profiles are stored in the /etc/CiscoSystemsVPNClient/Profiles directory. These text files have a .pcf extension and contain parameters needed to established a connection to a VPN Concentrator. You can create a new file or edit an existing one. You should find a sample profile, sample.pcf, in the profile directory. This example follows the use of that file to create a new profile named toCORPORATE.pcf.

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

You can use your favorite text editor to edit this new file, toCORPORATE.pcf. Before any modifications, the file looks like the following.

Note: If you want to use IPSec over Network Address Translation (NAT), the EnableNat entry in the configuration below must say "EnableNat=1" instead of "EnableNat=0."

```
[main]
Description=sample user profile
Host=10.7.44.1
AuthType=1
GroupName=monkeys
EnableISPConnect=0
ISPConnectType=0
```

Refer toUser Profiles for a description of the user profile keywords.

To successfully configure your profile, you need to know, as a minimum, your equivalent values for the following information.

- The host name or public IP address of the VPN Concentrator (10.48.66.109)
- The group name (RemoteClient)
- The group password (cisco)
- The username (joe)

Edit the file with your information so that it will be similar to the following.

```
[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=
DHGroup=2
ForceKeepAlives=0
```

Configuring the VPN Concentrator

Use the following steps to configure the VPN Concentrator.

Note: Because of space limitations, screen captures only show partial or relevant areas.

 Assign the pool of addresses. To assign an available range of IP addresses, point a browser to the inside interface of the VPN Concentrator and select **Configuration > System > Address Management >Pools**. Click **Add**. Specify a range of IP addresses that do not conflict with any other devices on the inside network.

VPN 3000 Concentrator Series Manager			
Conce	Configuration System Address Management Pools This section lets you configure IP Address Pools. Click the Add button to add a pool entry, or select a pool and click Moo IP Pool Entry 10 20 20 20 - 10 20 20 200	hify or Delete. Actions Add Modify Delete	

2. To tell the VPN Concentrator to use the pool, select **Configuration > System > Address Management > Assignment**, check the **Use Address Pools** box, and then click **Apply**.

VPN 3 Conce	000 ntrator Series Manager	
Configuration Interfaces System Devers Devevers Devers Devevers Devers Devers Devevers Devers Devers	Configuration System Address Manage This section presents Address Assignment Use Client Address F Use Address from Authentication Server Use DHCP F Use Address Pools F Apply	ement Assignment options. Each of the followir Check to use the IP addre user/group configuration. Check to use an IP addres Check to use DHCP to ob Check to use internal addr client.

3. Add a group and a password. Select **Configuration > User Management > Groups**, and then click **Add Group**. Enter the correct information, and then click **Add** to submit the information.

This example uses a group named "RemoteClient" with a password of "cisco."

Configuration Interfaces Bystem Base Group Groups	Configuration This section le Inherit? box a	User Managements ts you add a group, nd enter a new valu eneral IPSec Cl	It Groups Add Check the Inherit? box to set a field that you want to default to the ba ie to override base group values. ient FW PPTP/L2TP
Users			Identity Parameters
Policy Management	Attribute	Value	Description
	Group Name	RemoteClient	Enter a unique name for the group.
	Password	******	Enter the password for the group.
	Verify	****4	Verify the group's password.
	Туре	Internal 🗆	External groups are configured on an external authentication server are configured on the VPN 3000 Concentrator Series's Internal Data
	Add	Cancel	

4. On the group's IPSec tab, verify that authentication is set to **Internal**.

Configuration	Configuration lieor	Managament Croune Madify DomateClier		
	Conliguration User i	aanagement Groups wouny Remotecher	it.	
Users	Check the Inherit? be value to override base Identity General I	Check the Inherit? box to set a field that you want to default to the base group value to override base group values.		
- Administration		IPSec Para	neters	
- Monitoring	Attribute	Value	Inherit?	
	IPSec SA	ESP-3DES-MD5	N	
	IKE Peer Identity Validation	If supported by certificate	N.	
	IKE Keepalives	ч	N	
	Reauthentication on Rekey		N	
	Tunnel Type	Remote Access 💌	<u>s</u>	
	······································	Remote Access I	Parameter	
	Group Lock		ঘ	
	Authentication	Internal	R	

5. On the group's General tab, verify that **IPSec** is selected as the tunneling protocols.

- Configuration		Ģ	eneral	Paramet
Interfaces System User Management Base Group	Attribute	Value	Inherit?	
	Access Hours	-No Restrictions- 💌	V	Select the
	Simultaneous Logins	3	V	Enter the r
	Minimum Password Length	8	V	Enter the r
Depolicy Management D	Allow Alphabetic-Only Passwords	N	•	Enter whe be added
	Idle Timeout	30	•	(minutes)]
	Maximum Connect Time	0	V	(minutes) l
	Filter	-None- 💌	V	Enter the f
	Primary DNS		•	Enter the I
	Secondary DNS		V	Enter the I
	Primary WINS		V	Enter the I
	Secondary WINS		V	Enter the I
	Tunneling Protocols	□ PPTP □ L2TP ☑ IPSec □ L2TP over IPSec		Select the
				Check to r

6. To add the user to the VPN Concentrator, select **Configuration > User Management > Users**, and then click **Add**.

- Configuration Interfaces	Configuration User Management Users		
Crowning action Crowning action Crowning Crowning Crowning Crowning Crowning	Configuration User Management Users This section lets you configure users. Click the Add button to add a user, or select a user and Current Bredford itmcs-80	l click M nt Users ¹⁻³⁰⁰²	odify or Delete. Actions Add Modify
			Delete

7. Enter the correct information for the group, and then click **Apply** to submit the information.

Configuration Interfaces Osystem OServers OAddress Management OTunneling Protocols	Configuration Check the Inhe group values.	User Management Us rrit? box to set a field the neral IPSec PPTP/L	sers Modify joe at you want to default to the group value. Uncheck the Inhe 2TP
PPTP			Identity Parameters
L2TP	Attribute	Value	Description
- Management	User Name	ljoe	Enter a unique user name.
Protocols DEvents General	Password		Enter the user's password. The password must satisfy the
	Verify	[*******	Verify the user's password.
Base Group Groups	Group	RemoteClient 🗆	Enter the group to which this user belongs.
Users 	IP Address	I	Enter the IP address assigned to this user.
Administration Monitoring Routing Table	Subnet Mask	T.	Enter the subnet mask assigned to this user.
System Status 	Apply	Cancel	

Verify

Connecting to the VPN Concentrator

Now that the VPN Client and Concentrator are configured, the new profile should work to connect to the VPN Concentrator.

```
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.
^{\rm 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 >

Troubleshoot

This section provides information you can use to troubleshoot your configuration.

Debugs

To enable debugs, use the **ipseclog** command. An example is shown below.

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

Debug on the Client When Connecting to the Concentrator

```
[cholera]: /etc/CiscoSystemsVPNClient > cat /tmp/clientlog
      17:08:49.821 01/25/2002 Sev=Info/4 CLI/0x43900002
1
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
      17:08:49.855 01/25/2002 Sev=Info/4 CVPND/0x4340000F
2
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
      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
      17:08:49.858 01/25/2002 Sev=Info/4
6
                                             IPSEC/0x4370000C
Key deleted by SPI 0x637377d3
      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
```

17:08:49.860 01/25/2002 Sev=Info/4 10 IPSEC/0x4370000C Key deleted by SPI 0x5facd5bf IPSEC/0x43700009 17:08:49.860 01/25/2002 Sev=Info/4 11 IPSec driver already started 17:08:49.861 01/25/2002 Sev=Info/4 IPSEC/0x43700014 12 Deleted all keys 17:08:49.861 01/25/2002 Sev=Info/4 13 IPSEC/0x43700014 Deleted all keys 17:08:49.862 01/25/2002 Sev=Info/4 IPSEC/0x43700009 14 IPSec driver already started 17:08:49.863 01/25/2002 Sev=Info/4 IPSEC/0x43700009 15 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 17:08:50.883 01/25/2002 Sev=Info/4 19 CM/0x43100026Attempt 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. 17:08:51.099 01/25/2002 Sev=Info/4 21 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 17:08:51.400 01/25/2002 Sev=Info/5 IKE/0x4300002F 24 Received ISAKMP packet: peer = 10.48.66.109 17:08:51.400 01/25/2002 Sev=Info/4 IKE/0x43000014 25 RECEIVING <<< ISAKMP OAK AG (SA, KE, NON, ID, HASH, VID, VID, VID, VID) from 10.48.66.109 17:08:51.400 01/25/2002 Sev=Info/5 26 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 17:08:51.400 01/25/2002 Sev=Info/5 IKE/0x43000059 29 Vendor ID payload = AFCAD71368A1F1C96B8696FC77570100 17:08:51.400 01/25/2002 Sev=Info/5 IKE/0x43000001 30

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

47 17:08:56.646 01/25/2002 Sev=Info/5 IKE/0x430000D
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
 IPSec/0x43700014
 IPSEC/0x43700014
 IPSEC/0x43700014

Debugs on the VPN Concentrator

Select **Configuration > System > Events > Classes** to turn on the following debug if there are event connection failures.

- AUTH Severity to log 1–13
- IKE Severity to log 1–6
- **IPSEC** Severity to log 1–6

- Configuration	
Interfaces	Configuration System Events Classes
GSystem	
- Bervers	
	This section late you configure energial handling of energific event classes
	This section less you compute special nationing of special event classes.
- Management Protocols	Click the Add button to add an event class, or select an event class and click Mod
General	Click here to configure general event parameters.
FTP Backup	
Classes	Configured
	Event Classes Actions
Syslog Servers	Event Classes Actions
SMIP Servers	AUTH
Enal Recipients	IKE
	IPSEC
L and Balancing	Add
Eddu Datarici Itu	Modify
ElPoicy Management	(nowny)
- Administration	Delete
- Monitoring	

You can view the log by selecting **Monitoring > Event Log**.

Related Information

- Cisco VPN 3000 Series Concentrator Support Page
- Cisco VPN 3000 Series Client Support Page
- IPSec Support Page
- Technical Support Cisco Systems

Contacts & Feedback | Help | Site Map

© 2014 – 2015 Cisco Systems, Inc. All rights reserved. Terms & Conditions | Privacy Statement | Cookie Policy | Trademarks of Cisco Systems, Inc.

Updated: Jan 14, 2008

Document ID: 18886