IPsec configureren van VPN-client versie 3.5 Solaris naar een VPN-Concentrator 3000

Inhoud

Inleiding Voorwaarden Vereisten Gebruikte componenten Conventies Configureren Netwerkdiagram Configuraties Verifiëren Aansluiten op de VPN-centrator Problemen oplossen Debugs Gerelateerde informatie

Inleiding

Dit document illustreert hoe u de VPN-client 3.5 kunt configureren voor Solaris 2.6 om verbinding te maken met een VPN-Concentrator 3000.

Voorwaarden

Vereisten

Zorg er voordat u deze configuratie probeert, voor dat u aan de volgende voorwaarden voldoet.

- In dit voorbeeld wordt gebruik gemaakt van een vooraf gedeelde sleutel voor groepsidentificatie. De gebruikersnaam en het wachtwoord (uitgebreide authenticatie) worden gecontroleerd aan de hand van de interne database van de VPN Concentrator.
- De VPN-client moet correct geïnstalleerd zijn. Raadpleeg <u>De VPN-client installeren voor</u> <u>Solaris</u> voor meer informatie over de installatie.
- IP-connectiviteit moet bestaan tussen de VPN-client en de openbare interface van de VPNcentrator. Subnetmasker en informatie over de poort moeten goed worden ingesteld.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies.

- Cisco VPN-client voor Solaris 2.6, versie 3.5, 3DES-afbeelding. (beeldnaam: vpnclient-solaris5.6-3.5.Rel-k9.tar.Z)
- Cisco VPN-centrator type: 3005 Bootcode Rev.: Altiga Networks/VPN Concentrator versie 2.2.int_9 Jan 19 2000 05:36:41 Software Rev.: Cisco Systems, Inc./VPN 3000 Concentrator Series versie 3.1.Rel augustus 2001 13:47:37

De informatie in dit document is gebaseerd op apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als u in een levend netwerk werkt, zorg er dan voor dat u de potentiële impact van om het even welke opdracht begrijpt alvorens het te gebruiken.

Conventies

Zie de <u>Cisco Technical Tips Convention</u> voor meer informatie over documentconventies.

Configureren

Deze sectie bevat informatie over het configureren van de functies die in dit document worden beschreven.

N.B.: Als u aanvullende informatie wilt vinden over de opdrachten in dit document, gebruikt u het <u>Opdrachtplanningprogramma</u> (alleen <u>geregistreerd</u> klanten).

Netwerkdiagram

Dit document gebruikt de netwerkinstellingen die in het onderstaande schema zijn weergegeven.



VPN Client

Opmerking: Voor VPN-client 3.5 om verbinding te maken met de VPN-Concentrator hebt u versie 3.0 of hoger op de concentrator nodig.

Configuraties

Een gebruikersprofiel maken voor de verbinding

De gebruikersprofielen worden opgeslagen in de map /etc/CiscoSystemsVPN/Profiles. Deze tekstbestanden hebben een .pcf-extensie en bevatten parameters die nodig zijn om een verbinding met een VPN-centrator te maken. U kunt een nieuw bestand maken of een bestaand bestand bewerken. U zou een voorbeeldprofiel, Samsfp.pcf, in de profielfolder moeten vinden. Dit

voorbeeld volgt het gebruik van dat bestand om een nieuw profiel te maken dat naar CORPORATE.pcf wordt genoemd.

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

U kunt uw favoriete teksteditor gebruiken om dit nieuwe bestand, naar CORPORATE.pcf, te bewerken. Voordat er wijzigingen worden aangebracht, ziet het bestand er als volgt uit.

N.B.: Als u IPSec over Network Address Translation (NAT) wilt gebruiken, moet in de configuratie hieronder "EnableNat=1" in plaats van "EnableNat=0" betekenen.

[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= DHGroup=2 ForceKeepAlives=0

Raadpleeg <u>Gebruikersprofielen</u> voor een beschrijving van de sleutelwoorden van het gebruikersprofiel.

Om uw profiel met succes te configureren moet u minimaal uw equivalente waarden voor de volgende informatie weten.

- De naam van de host of het openbare IP-adres van de VPN-Concentrator (10.48.6.109)
- De groepsnaam (RemoteClient)
- Het groepswachtwoord (cisco)
- De gebruikersnaam (joe)

Bewerk het bestand met uw informatie zodat het op het volgende lijkt.

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

De VPN-centrator configureren

Gebruik de volgende stappen om de VPN-centrator te configureren.

Opmerking: vanwege ruimtebeperkingen geeft het scherm alleen gedeeltelijke of relevante gebieden weer.

 Pas de adressen toe. Om een beschikbaar bereik van IP-adressen toe te wijzen, richt u een browser op de interne interface van VPN Concentrator en selecteert u Configuration > System > Address Management >Pools. Klik op Add (Toevoegen). Specificeer een bereik van IP-adressen die niet met andere apparaten op het binnennetwerk botsen.

VPN 3 Conce	000 ntrator Series Manager	
Configuration Interfaces Configuration Conf	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 Mool IP Pool Entry 10 20 20 20 - 10 20 20 200	dify or Delete Actions Add Modify Delete

 Als u de VPN-Concentrator wilt vertellen dat hij de pool moet gebruiken, selecteert u Configuration > System > Address Management > Asmission, controleert u het vakje Adres Pools en vervolgens klikt u op Toepassen.



3. Voeg een groep en een wachtwoord toe. Selecteer Configuratie > Gebruikersbeheer > Groepen en klik vervolgens op Groep toevoegen. Voer de juiste informatie in en klik vervolgens op Toevoegen om de informatie in te sturen.Dit voorbeeld gebruikt een groep genaamd "RemoteClient" met een wachtwoord van

"cisco."				
Configuration	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 ba Inherit? box and enter a new value to override base group values.			
Groups	Identity General IPSec Client FW PPTP/L2TP			
Users	Identity Parameters			
Generation Gener	Attribute	Value	Description	
	Group Name	RemoteClient	Enter a unique name for the group.	
	Password	*****4	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. Controleer op het tabblad IPSec van de groep of de verificatie is ingesteld op **Interne**.

Configuration Interfaces User Management Groups Users Users Users	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			
Administration	IPSec Parameters			
the monitoring	Attribute	Value	Inherit?	
	IPSec SA	ESP-3DES-MD5	N	
	IKE Peer Identity Validation	If supported by certificate 💌	N	
	IKE Keepalives	ч	9	
	Reauthentication on Rekey		R	
	Tunnel Type	Remote Access 💌		
	Remote Access Parameter			
	Group Lock		N	
	Authentication	Internal 💌	T	

5. Controleer op het tabblad General of the group of **IPSec** is geselecteerd als de tunnelprotocollen.

			eneral	Paramet
Interfaces	Attribute	Value	Inherit?	
Base Group	Access Hours	-No Restrictions- 💌	9	Select the
	Simultaneous Logins	3	V	Enter the r
Users	Minimum Password Length	8	V	Enter the r
<u>Olicy Management</u> <u>Administration</u> <u>Monitoring</u>	Allow Alphabetic-Only Passwords	ঘ	V	Enter whe be added
	Idle Timeout	30	V	(minutes)]
	Maximum Connect Time	0	V	(minutes)]
	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 a

 Als u de gebruiker aan de VPN-Concentrator wilt toevoegen, selecteert u Configuration > User Management > Gebruikers en vervolgens klikt u op Add.



7. Voer de juiste informatie voor de groep in en klik vervolgens op **Toepassen** om de informatie in te

Configuration	onfiguration	User Management U:	sers Modify joe	
	heck the Inho roup values. Identity Ge	mit? box to set a field th	at you want to default to the group value. Uncheck the Inhe	
PPTP.	Identity Parameters			
L2TP	Attribute	Value	Description	
	User Name	ljoe	Enter a unique user name.	
	Password	J*****	Enter the user's password. The password must satisfy the	
Client Update Load Balancing	Verify	·····	Verify the user's password.	
Base Group Groups	Group	RemoteClient 🗆	Enter the group to which this user belongs.	
Users 	IP Address	Į.	Enter the IP address assigned to this user.	
Monitoring Southing Table	Subnet Mask	I	Enter the subnet mask assigned to this user.	
Filterable Event Log Live Event Log System Status Greating Statistics	Apply	Cancel		

<u>Verifiëren</u>

Aansluiten op de VPN-centrator

Nu de VPN-client en de Concentrator zijn geconfigureerd moet het nieuwe profiel werken om verbinding te maken met de VPN-Concentrator.

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. 7 Suspended [cholera]: /etc/CiscoSystemsVPNClient > bg vpnclient connect toCORPORATE & [1] (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 >

Problemen oplossen

Deze sectie bevat informatie waarmee u problemen met de configuratie kunt oplossen.

Debugs

Gebruik de opdracht ipseclog. Hieronder wordt een voorbeeld gegeven.

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

bug in de client bij aansluiting op de centrator

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, 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

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 Deleted all keys

110 17:09:17.375 01/25/2002 Sev=Info/4 IPSEC/0x43700009 IPSec driver already started

11117:09:17.37601/25/2002Sev=Info/4IPSEC/0x43700014Deleted all keysDebugs in de VPN-concentratie

Selecteer **Configuration > System > Events > Classes** om het volgende debug in te schakelen als er problemen zijn met de verbinding.

IPSEC/0x43700014

- AUTH Severity to log 1-13
- IKE Ernst tot log 1-6
- IPSEC Ernst naar log 1-6

<u>Interfaces</u>	Configuration System Events Classes	
- El-Servers		
	This section lets you configure special handling of specific event of	ACCPC
D-Tunneling Protocols	The section for you could a shoot a unitally of shoots even of	
- CHP Routing		
Management Protocols	Click the Add button to add an event class, or select an event clas	s and click Mod
General	Click here to configure general event parameters.	
FTP Backup		
Classes	Configurad	
Trap Destinations	Comigureu Event Classes	A
Syslog Servers	Event Classes	Actions
SMTP Servers	AUTH	
	IKE	
	IPSEC	4.4.4
Lood Balancing		Add
Coad Datancing		Modify
- All Policy Management		wouny
El Administration		Delete
E Monitoring		
(Dimonitoring		

U kunt het logbestand weergeven door **Monitoring > Event Log** te selecteren.

Gerelateerde informatie

- Ondersteuning van Cisco VPN 3000 Series Concentrator-pagina
- <u>Cisco VPN 3000 Series clientondersteuningspagina</u>
- IPsec-ondersteuningspagina
- Technische ondersteuning Cisco-systemen