Configuración de IPSec de cliente VPN de Solaris versión 3.5 en un concentrador VPN 3000

Contenido

Introducción Prerequisites Requirements Componentes Utilizados Convenciones Configurar Diagrama de la red Configuraciones Verificación Conexión con el concentrador VPN Troubleshoot Depuraciones Información Relacionada

Introducción

Este documento ilustra cómo configurar VPN Client 3.5 para Solaris 2.6 para conectar con un VPN 3000 Concentrator.

Prerequisites

Requirements

Antes de utilizar esta configuración, asegúrese de que cumple con los siguientes requisitos previos.

- Este ejemplo utiliza una clave previamente compartida para la autenticación de grupo. El nombre de usuario y la contraseña (autenticación extendida) se comprueban con la base de datos interna del concentrador VPN.
- El VPN Client debe estar instalado correctamente. Refiérase a <u>Instalación del Cliente VPN</u> para Solaris para obtener detalles sobre la instalación.
- La conectividad IP debe existir entre el VPN Client y la interfaz pública del VPN Concentrator. La máscara de subred y la información de la puerta de enlace deben configurarse correctamente.

Componentes Utilizados

La información que contiene este documento se basa en estas versiones de software y hardware.

- Cisco VPN Client para Solaris 2.6 versión 3.5, imagen 3DES. (nombre de la imagen: vpnclient-solaris5.6-3.5.Rel-k9.tar.Z)
- Tipo de concentrador VPN de Cisco: 3005 Código de arranque Rev: Altiga Networks/VPN Concentrator Versión 2.2.int_9 19 ene 2000 05:36:41 Software Rev: Cisco Systems, Inc./VPN 3000 Concentrator Series Versión 3.1.Rel 06 Agosto 2001 13:47:37

La información que se presenta en este documento se originó a partir de dispositivos dentro de un ambiente de laboratorio específico. All of the devices used in this document started with a cleared (default) configuration. Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener un comando antes de ejecutarlo.

Convenciones

Para obtener más información sobre las convenciones del documento, consulte <u>Convenciones de</u> <u>Consejos Técnicos de Cisco</u>.

Configurar

En esta sección encontrará la información para configurar las funciones descritas en este documento.

Nota: Para encontrar información adicional sobre los comandos usados en este documento, utilice la <u>Command Lookup Tool</u> (<u>sólo</u> clientes registrados).

Diagrama de la red

Este documento utiliza la instalación de red que se muestra en el siguiente diagrama.



Nota: Para que VPN Client 3.5 se conecte al VPN Concentrator, necesita la versión 3.0 o posterior en el concentrador.

Configuraciones

Creación de un perfil de usuario para la conexión

Los perfiles de usuario se almacenan en el directorio /etc/CiscoSystemsVPNClient/Profiles. Estos archivos de texto tienen una extensión .pcf y contienen los parámetros necesarios para establecer una conexión a un concentrador VPN. Puede crear un archivo nuevo o editar uno existente. Debe encontrar un perfil de ejemplo, sample.pcf, en el directorio de perfiles. Este ejemplo sigue al uso de ese archivo para crear un nuevo perfil denominado toCORPORATE.pcf.

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

Puede utilizar su editor de texto favorito para editar este nuevo archivo, toCORPORATE.pcf. Antes de realizar cualquier modificación, el archivo tiene el aspecto siguiente.

Nota: Si desea utilizar IPSec sobre traducción de direcciones de red (NAT), la entrada EnableNat de la siguiente configuración debe decir "EnableNat=1" en lugar de "EnableNat=0".

```
[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
```

Consulte <u>Perfiles de usuario</u> para obtener una descripción de las palabras clave del perfil de usuario.

Para configurar correctamente el perfil, debe conocer, como mínimo, los valores equivalentes para la siguiente información.

- Nombre de host o dirección IP pública del concentrador VPN (10.48.66.109)
- El nombre del grupo (RemoteClient)
- La contraseña del grupo (cisco)
- El nombre de usuario (joe)

Edite el archivo con su información para que sea similar a lo siguiente.

[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=000000000000000000000000000000000000
DHGroup=2
ForceKeepAlives=0

Configuración del concentrador VPN

Utilice los siguientes pasos para configurar el concentrador VPN.

Nota: Debido a las limitaciones de espacio, las capturas de pantalla sólo muestran áreas parciales o relevantes.

 Asigne el conjunto de direcciones. Para asignar un rango disponible de direcciones IP, señale un buscador a la interfaz interna del VPN Concentrator y seleccione Configuration > System > Address Management >Pools . Haga clic en Add (Agregar). Especifique un rango de direcciones IP que no entren en conflicto con otros dispositivos de la red

100.		
VPN 3 Conce	3000 ntrator Series Manager	
	Configuration System Address Management Pools	
- CD-Servers		
	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 Delet	e.
- HP Routing		
DEvente	IP Pool Entry Actions	
	10 20 20 20 - 10 20 20 20	
- Client Update		
Load Balancing	Add	1
- Der Management	Cou	
Devicy Management	Modify	
	Delay	ŕ.
CONTRACTING IN	Delete	L.

 Para indicar al VPN Concentrator que utilice el conjunto, seleccione Configuration > System > Address Management > Assignment, active la casilla Use Address Pools y, a continuación, haga clic en Apply.

VPN 3 Conce	3000 ntrator Series Manager
- <u>Configuration</u>	
Interfaces	Configuration System Address Management Assignment
	This section presents Address Assignment options. Each of the followir
Pools ————————————————————————————————————	Use Client Address 🔽 Check to use the IP addre user/group configuration.
	Use Address from Authentication \Box Check to use an IP address Server
- D General	Use DHCP □ Check to use DHCP to ob
Load Balancing	Use Address Pools 🔽 Check to use internal address
	Apply Cancel

3. Agregue un grupo y una contraseña. Seleccione Configuration > User Management > Groups y luego haga clic en Add Group. Introduzca la información correcta y, a continuación, haga clic en Agregar para enviar la información.Este ejemplo utiliza un grupo denominado "RemoteClient" con una contraseña de

"cisco".					
Configuration Interfaces System User Management Base Group Groups	Configuration This section le Inherit? box a Identity Go	User Management ts you add a group, nd enter a new value eneral TPSec Cli	Groups Add Check the Inherit? box to set a field that you want to default to the ba to override base group values. ent FW PPTP/L2TP		
Users		Identity Parameters			
Policy Management Administration	Attribute	Value	Description		
-Monitoring	Group Name	RemoteClient	Enter a unique name for the group.		
	Password	******	Enter the password for the group.		
	Verify	*****1	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. En la ficha IPSec del grupo, verifique que la autenticación esté establecida en **Interna**.

Configuration Interfaces DSystem Duser Management Base Group Groups Users DPolicy Management	Configuration User f Check the Inherit? be value to override base Identity General I	Management Groups Modify RemoteClien ox to set a field that you want to default to the group values. PSec Client FW PPTP/L2TP	t base grouj
Administration		IPSec Parar	neters
ter monitor init	Attribute	Value	Inherit?
	IPSec SA	ESP-3DES-MD5	N
	IKE Peer Identity Validation	If supported by certificate 💌	9
	IKE Keepalives	N	ঘ
	Reauthentication on Rekey		ঘ
	Tunnel Type	Remote Access 💌	
	· · · · · · · · · · · · · · · · · · ·	Remote Access P	arameter
	Group Lock		N
	Authentication	Internal 💌	J

5. En la ficha General del grupo, verifique que **IPSec** esté seleccionado como protocolos de tunelización.

			Feneral	Paramet
	Attribute	Value	Inherit?	
—⊞ <u>System</u> —⊡User Management	Access Hours	-No Restrictions- 💌	v	Select the
Base Group Groups	Simultaneous Logins	3		Enter the r
	Minimum Password Length	8	V	Enter the r
<u>Administration</u> <u>Monitoring</u>	Allow Alphabetic-Only Passwords	N	2	Enter whe be added
	Idle Timeout	30	V	(minutes) I
	Maximum Connect Time	0	V	(minutes) I
	Filter	-None-	V	Enter the f
	Primary DNS		•	Enter the I
	Secondary DNS		V	Enter the I
	Primary WINS	[•	Enter the I
	Secondary WINS		V	Enter the I
	Tunneling Protocols	□ PPTP □ L2TP ☑ IPSec □ L2TP over IPSec		Select the
				Check to :

6. Para agregar el usuario al VPN Concentrator, seleccione Configuration > User Management
 > Users y luego haga clic en



7. Introduzca la información correcta para el grupo y, a continuación, haga clic en **Aplicar** para enviar la

-Configuration	Configuration	User Management U	sers Modify joe
	Check the Inherit? box to set a field that you want to default to the group value. Uncheck the Inhe group values.		
PPTP			Identity Parameters
	Attribute	Value	Description
	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.
	Group	RemoteClient 🗆	Enter the group to which this user belongs.
	IP Address	I	Enter the IP address assigned to this user.
<u> Monitoring</u> Routing Table	Subnet Mask	The second secon	Enter the subnet mask assigned to this user.
Filterable Event Log Live Event Log System Status Sessions Sessions Statistics	Apply	Cancel	

Verificación

Conexión con el concentrador VPN

Ahora que el VPN Client y el concentrador están configurados, el nuevo perfil debe funcionar para conectarse al 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 > bq [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

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

Depuraciones

Para habilitar las depuraciones, utilice el comando **ipseclog**. Se presenta un ejemplo a continuación:

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

Depurar en el cliente cuando se conecta al concentrador

[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, 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</pre>

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 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

111 17:09:17.376 01/25/2002 Sev=Info/4 IPSEC/0x43700014 Deleted all keys

Depuraciones en el concentrador VPN

Seleccione **Configuration > System > Events > Classes** para activar la siguiente depuración si hay fallas de conexión a eventos.

IPSEC/0x43700009

IPSEC/0x43700014

- AUTH Gravedad para registrar 1-13
- IKE: gravedad para registrar 1-6
- IPSEC: gravedad para registrar 1-6



Puede ver el registro seleccionando Monitoring > Event Log.

Información Relacionada

- Página de soporte del concentrador de la serie Cisco VPN 3000
- Página de soporte al cliente Serie Cisco VPN 3000
- Página de soporte de IPSec
- <u>Soporte Técnico Cisco Systems</u>