Configuración de un túnel IPSec – Concentrador VPN 5000 de Cisco al firewall de punto de control 4.1

Contenido

Introducción **Prerequisites** Requirements **Componentes Utilizados** Convenciones Configurar Diagrama de la red Configuraciones Escudo de protección de punto de control 4.1 Verificación Troubleshoot Comandos de resolución de problemas del concentrador de la VPN 5000 Resumen de la red Depuración del Checkpoint 4.1 Firewall Ejemplo de resultado del comando debug Información Relacionada

Introducción

Este documento muestra cómo formar un túnel IPsec con claves previamente compartidas para unir dos redes privadas. Se une a una red privada dentro del Cisco VPN 5000 Concentrator (192.168.1.x) a una red privada dentro del Checkpoint 4.1 Firewall (10.32.50.x). Se supone que el tráfico desde el interior del concentrador VPN y dentro del punto de control a Internet (representado en este documento por las redes 172.18.124.x) fluye antes de iniciar esta configuración.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

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

- Concentrador Cisco VPN 5000
- Software Cisco VPN 5000 Concentrator versión 5.2.19.0001
- Escudo de protección de punto de control 4.1

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Convenciones

Consulte <u>Convenciones de Consejos TécnicosCisco para obtener más información sobre las</u> <u>convenciones del documento.</u>

<u>Configurar</u>

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

Nota: Use la <u>Command Lookup Tool</u> (sólo <u>clientes registrados</u>) para obtener más información sobre los comandos utilizados en este documento.

Diagrama de la red

En este documento, se utiliza esta configuración de red:



Este documento usa esta configuración.

Concentrador Cisco VPN 5000		
[IP Ethernet 0:0]		
Mode	= Routed	
SubnetMask	= 255.255.255.0	
IPAddress	= 192.168.1.1	
[General]		
EthernetAddress	= 00:00:a5:e9:c8:00	
DeviceType	= VPN 5002/8 Concentrator	
ConfiguredOn	= Timeserver not configured	
ConfiguredFrom	= Command Line, from Console	
DeviceName	= "cisco_endpoint"	
IPSecGateway	= 172.18.124.34	
[IKE Policy]		
Protection	= SHA_DES_G2	
[Tunnel Partner VPN 1]		
KeyLifeSecs	= 28800	
LocalAccess	= "192.168.1.0/24"	
Peer	= "10.32.50.0/24"	
BindTo	= "ethernet 1:0"	
SharedKey	= "ciscorules"	
KeyManage	= Auto	
Transform	= esp(sha,des)	
Partner	= 172.18.124.157	
Mode	= Main	
[IP VPN 1]		
Numbered	= Off	
Mode	= Routed	
[IP Ethernet 1:0]		
IPAddress	= 172.18.124.35	
SubnetMask	= 255.255.255.240	
Mode	= Routed	
[IP Static]		
10.32.50.0 255.255.255.0	VPN 1 1	
Configuration size is 11	31 out of 65500 bytes.	

Escudo de protección de punto de control 4.1

Complete estos pasos para configurar el firewall Checkpoint 4.1.

 Seleccione Properties > Encryption para establecer los tiempos de vida de IPSec de punto de control para coincidir con el comando KeyLifeSecs = 28800 VPN Concentrator.Nota: Deje las duraciones del intercambio de claves de Internet (IKE) del punto de control en el valor predeterminado.

Properties Setup	×
High Availability IP Pool NAT Acces Security Policy Traffic Control Services L Authentication SYNDefender LDAP	s Lists Desktop Security .og and Alert Security Servers Encryption ConnectControl
SKIP Enable Exportable SKIP Change SKIP Session Key :	Manual IPSEC SPI allocation range (hex):
Every 120 Seconds (0 for infinity) or Every 10495790 Dates (0 for infinity)	Erom 100
IKE Renegotiate I <u>K</u> E Security Associations every	440 minutes
Renegotiate I <u>P</u> SEC Security Associations every	28800 seconds
OK Cancel	Help

 Seleccione Manage (Administración) > Network Objects (Objetos de red) > New (o Edit) Nuevo (o Editar) > Network (Red) para configurar el objeto para la red interna ("cpinside") detrás del punto de control. Esto debe coincidir con el comando Peer = "10.32.50.0/24" VPN

	Network Properties
	General NAT
	<u>N</u> ame: cpinside
	IP Address: 10.32.50.0 Get address
	Net <u>M</u> ask: 255.255.255.0
	Color:
	Location: Broadcast:
	● Internal ○ External ● Allowed ○ Disallowed
	OK Cancel Help
Concentrator.	

 Seleccione Administrar > Objetos de red > Editar para editar el objeto para el punto de control de gateway ("RTPCVPN" Checkpoint) al que el concentrador VPN señala en el comando Partner = <ip>.Seleccione Interno en Ubicación.Seleccione Gateway para Type (Tipo).Verifique VPN-1 y FireWall-1 y Management Station en Módulos

Wo	rkstation Properties		×
G	ieneral Interfaces SNMP N	IAT Certificates VPN	Authe
	Name: RTPCPVPN		
	IP Address: 172.18.124.157	<u>G</u> et addre	155
	Comment: Firewalled gatew	vay to internet	
	Location: O <u>I</u> nternal O <u>E</u> xternal	Type: O <u>H</u> ost ⊙ I	Gate <u>w</u> ay
	Modules Installed		
	VPN-1 & EireWall-1	Version: 4.1	Get
	FloodGate-1	Version: 4.1	
	Compregsion	Version: 4.1	
	Management Station	Color:	•
		_	
	ОК	Cancel Help	1
os.			1

4. Seleccione Administrar > Objetos de red > Nuevo (o Editar) > Red para configurar el objeto para la red externa ("inside_cisco") detrás del concentrador VPN.Esto debe coincidir con el comando LocalAccess = <192.168.1.0/24> VPN

General NAT
<u>N</u> ame: inside_cisco
IP Address: 192.168.1.0 Get address
Net <u>Mask:</u> 255.255.255.0
Color: Color:
Location: Broadcast:
○ Internal ● External ● Allowed ○ Disallowed
OK Cancel Help

5. Seleccione Administrar > Objetos de red > Nuevo > Estación de trabajo para agregar un objeto para el gateway del concentrador VPN externo ("cisco_terminal").Esta es la interfaz "externa" del concentrador VPN con conectividad al punto de control (en este documento, 172.18.124.35 es la dirección IP en el comando IPAddress = <ip>).Seleccione External en Location. Seleccione Gateway para Type (Tipo).Nota: No verifique VPN-1/FireWall-

Workstation Properties	×
General Interfaces SNMP N	IAT VPN
<u>N</u> ame: cisco_endpoint	
IP Address: 172.18.124.35	<u>G</u> et address
Comment:	
Location:	Type:
O <u>I</u> nternal ⊙ <u>E</u> xternal	<u>○ H</u> ost
Modules Installed	
VPN-1 & <u>F</u> ireWall-1	Version: 4.1 🔽 Ge <u>t</u>
FloodGate-1	Version: 4.1
Compression	Version: 4.1
Management Station	Color:
ОК	Cancel Help

6. Seleccione Manage (Administración) > Network objects (Objetos de red) > Edit (Editar) para editar la ficha VPN del punto final del punto de control Gateway (denominado"RTPCPVPN"). En Domain (Dominio), seleccione Other (Otro) y luego, seleccione el interior de la red de Punto de control (denominado "cpinside") en la lista desplegable. Bajo los esquemas de encripción definidos, seleccione IKE y luego haga clic en Edit

General Interfaces SNMP NAT Certificates VPN Authe Domain: Encryption schemes defined: O Disabled Image: ME
Domain: Encryption schemes defined: O Disabled Image: Method schemes defined:
○ Valid Addresses(of Interfaces) □ Manual IPSEC ○ Other: □ Manual IPSEC □ Cpinside □ Manual IPSEC □ Exportable for SecuRemote Edit

7. Cambie las propiedades IKE a encripción DES y hash SHA1 para coincidir con el comando SHA_DES_G2 VPN Concentrator.Nota: El "G2" se refiere al grupo Diffie-Hellman 1 ó 2. En las pruebas, se descubrió que el punto de control acepta "G2" o "G1".Cambie esta configuración:Cancelar la selección del modo agresivoMarque Compatible con subredes.Verifique Pre-Shared Secret bajo Authentication

General Interfaces SNMP NAT Certificates	VPN Authe
KE Properties	×
General	
Key <u>N</u> egotiation Encryption Method(s):	- <u>H</u> ash Method: -
	□ MD <u>5</u>
□ 📾 CAST □ 🖾 3DES	☑ SHA <u>1</u>
Authentication Method:	
✓ Pre-Shared Secret Edit S	ecrets
Public Key Signatures <u>Con</u>	ïgure
☐ Supports Aggresive <u>M</u> ode ☑ Support	s Su <u>b</u> nets
OK Cancel	Help
Method	

8. Haga clic en **Editar secretos** para establecer la clave previamente compartida de acuerdo con el comando **SharedKey = <key>** Concentrador

Workstation Properties
General Interfaces SNMP NAT Certificates VPN Authe
IKE Properties
General
Shared Secret
Shared Secrets List:
Peer Name Shared Secret
cisco_endpoint **** <u>E</u> dit
Bemove
OK Cancel
OK Cancel Help
OK Cancel Help

9. Seleccione Manage (Administración) > Network Objects (Objetos de red) > Edit (Editar) para editar la ficha VPN de "cisco_endpoint". En Dominio, seleccione Otro y, a continuación, seleccione el interior de la red del concentrador VPN (Ilamada "inside_cisco"). Bajo los esquemas de encripción definidos, seleccione IKE y luego haga clic en Edit

Workstation Properties	>
General Interfaces SNMP NAT	VPN
Domain:	Encryption schemes defined:
O <u>D</u> isabled	Manual IPSEC
○ <u>V</u> alid Addresses(of Interfaces)	
	🗆 🔝 SKIP
🛱 inside_cisco 🔻	
Exportable for SecuRemote	<u>E</u> dit
Traffic Control Logging	
Image: March M	9
OK Can	cel Help

10. Cambie las propiedades IKE a encripción DES y hash SHA1 para coincidir con el comando SHA_DES_G2 VPN Concentrator.Nota: El "G2" se refiere al grupo Diffie-Hellman 1 ó 2. En las pruebas, se encontró que el punto de control acepta "G2" o "G1".Cambie esta configuración:Cancelar la selección del modo agresivoMarque Compatible con subredes.Verifique Pre-Shared Secret bajo Authentication

General Interfaces SNMP NAT Certificates	VPN	Authe	•
KE Properties			×
General			
Key <u>N</u> egotiation Encryption Method(s):	⊢ <u>H</u> ash M	Method: -	
DES DES	E M	1D <u>5</u>	
CAST	.	UA1	
L L Marine 3DES	1. 0	nA <u>r</u>	
- Authentication Method:			
✓ Pre-Shared Secret Edit S	ecrets		
Public Key Signatures <u>Conf</u>	ïgure		
Supports Aggresive <u>M</u> ode 🔽 Support	s Su <u>b</u> net	'S	
OK Cancel H	Help]	
/ethod.			

11. Haga clic en **Editar secretos** para establecer la clave previamente compartida de acuerdo con el comando **SharedKey = <key>** Concentrador

- 1	IKE Properties	x
	General	
	Shared Secret	×
	Shared Secrets List: Peer Name Shared Secret RTPCPVPN **** Edit Remove	
/PN	OK Cancel OK Cancel Help	

 En la ventana del editor de políticas, ingrese una ventana tanto con el origen como con el destino, como en "inside_cisco" y "cpinside" (bidireccional). Set Service=Any, Action=Encrypt, y

Tr	ack=L	_ong.						
Ĩ	RTPO	CPVPN - Check P	oint Policy Editor					_ 🗆 🗙
E	ile <u>E</u> di	it ⊻iew <u>M</u> anage	Policy <u>W</u> indow <u>H</u>	elp				
l	- 5	🗟 🔉 🏅 🖻	🖻 💁 👼 🧖	0. 🕫 🕼	😭 📒 💕	æ 🖷 1	L 🔫 🍽 🛙	🕈 🖫 🖓 🖡
Å	Sec	urity Policy - Standard	l 📩 Address Trans	slation - Standar	d 🏽 🥐 Bandwidth	Policy - Sta	ndard	
	No.	Source	Destination	Servic	e Act	ion	Track	In
\$	1	👷 inside_cisco	👷 cpinside	Any		crypt	Long	
	•							•
F	or Help,	press F1			RTPCPVPN	Read	Write	

13. En el encabezado Acción, haga clic en el icono verde **Cifrar** y seleccione **Editar propiedades** para configurar las políticas de cifrado

cinado.				
urity Policy - Standard	🛃 Address Translation	- Standard 👭 Band	dwidth Policy - Standard	^
∼ FVV1 Host	∼ Ldap-Servers	🗐 Idap	accept	
∼ FW1 Host	∼ Logical-Servers	∼ load_agent	accept	
💂 inside_cisco	💂 cpinside	A APV		ha
🛱 cpinside	🚆 inside_cisco	- Ally	dit properties	- •
		om dest-unreach	Edit Encryption	
		Comp echo-reply		
		echo-request	accept	am 🦳
		icmp-proto		
		info-reply	drop	
		info-req		
🔁 Any	🔁 Any	mask-reply	🚺 🦰 reject	hg L
•		imp mark ramart		

14. Seleccione IKE y haga clic en

	Encryption Properties	×
	General Encryption schemes defined: C M RE C Manual IPSEC C M SKIP C M FVVZ Edit	
dit	OK Cancel Help	

15. En la ventana IKE Properties, cambie estas propiedades para coincidir con el comando Transform = esp(sha,des) VPN Concentrator.En Transform (Transformar), seleccione Encryption (Encriptación) + Data Integrity (ESP) (Integridad de datos (ESP)). El algoritmo de cifrado debe ser DES, la integridad de los datos debe ser SHA1 y la puerta de enlace de par permitida debe ser la puerta de enlace del concentrador VPN externo (denominada "cisco_endpoint"). Click

IKE	Properties	X
Ge	eneral	
	 Transform: Encryption + Data Integrity (ESP) Data Integrity Only (AH) 	
	Encryption Algorithm: DES	
	Data Integrity SHA1	
	Allowed Peer Gateway:	
	Use Perfect Forward Secrecy	
ок	OK Cancel Help	

16. Después de configurar el punto de control, seleccione **Policy > Install** en el menú Checkpoint para que los cambios surtan efecto.



Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

Troubleshoot

Comandos de resolución de problemas del concentrador de la VPN 5000

La herramienta Output Interpreter Tool (clientes registrados solamente) (OIT) soporta ciertos comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

Nota: Consulte <u>Información Importante sobre Comandos Debug</u> antes de utilizar los comandos **debug**.

- vpn trace dump all: muestra información sobre todas las conexiones VPN coincidentes, incluida información sobre la hora, el número VPN, la dirección IP real del par, los scripts que se han ejecutado y, en caso de error, la rutina y el número de línea del código de software donde se produjo el error.
- show system log buffer: muestra el contenido del búfer de registro interno.
- **show vpn statistics**: muestra esta información para usuarios, socios y el total para ambos. (Para los modelos modulares, la pantalla incluye una sección para cada ranura de módulo. Consulte la sección <u>Salida de Debug de Ejemplo</u>).Activo actual: las conexiones activas actuales.En Negot: las conexiones que están negociando actualmente.Agua alta: el mayor número de conexiones activas simultáneas desde el último reinicio.Total en ejecución: el número total de conexiones exitosas desde el último reinicio.Túnel oK: el número de túneles para los que no hubo errores.Comienza el túnel: se inicia el número de túnel.Error de túnel: el número de túneles con errores.
- show vpn statistics verbose: muestra las estadísticas de negociación ISAKMP y muchas más estadísticas de conexión activas.

Resumen de la red

Cuando se configuran varias redes internas adyacentes en el dominio de cifrado en el punto de control, el dispositivo podría resumirlas automáticamente con respecto al tráfico interesante. Si el concentrador VPN no está configurado para coincidir, es probable que el túnel falle. Por ejemplo, si las redes internas de 10.0.0.0 /24 y 10.0.1.0 /24 están configuradas para ser incluidas en el túnel, podrían resumirse en 10.0.0.0 /23.

Depuración del Checkpoint 4.1 Firewall

Se trataba de una instalación de Microsoft Windows NT. Debido a que el seguimiento se configuró para Long en la ventana del Editor de políticas (como se ve en el Paso 12), el tráfico denegado debería aparecer en rojo en el Visor de registros. Se puede obtener una depuración más detallada mediante:

C:\WINNT\FW1\4.1\fwstop C:\WINNT\FW1\4.1\fw d -d **y en otra ventana**. C:\WINNT\FW1\4.1\fwstart

Ejecute estos comandos para borrar las asociaciones de seguridad (SA) en el punto de control:

fw tab -t IKE_SA_table -x
fw tab -t ISAKMP_ESP_table -x
fw tab -t inbound_SPI -x
fw tab -t ISAKMP_AH_table -x
Conteste sí al ;Está seguro? mensaje

Ejemplo de resultado del comando debug

```
cisco_endpoint#vpn trac dump all
         4 seconds -- stepmngr trace enabled --
  new script: lan-lan primary initiator for <no id> (start)
manage @ 38 seconds :: lan-lan-VPN0:1:[172.18.124.157] (start)
        38 seconds doing l2lp_init, (0 @ 0)
        38 seconds doing l2lp_do_negotiation, (0 @ 0)
  new script: ISAKMP secondary Main for lan-lan-VPN0:1:[172.18.124.157] (start)
        38 seconds doing isa_i_main_init, (0 @ 0)
manage @ 38 seconds :: lan-lan-VPN0:1:[172.18.124.157] (done)
manage @ 38 seconds :: lan-lan-VPN0:1:[172.18.124.157] (start)
        38 seconds doing isa_i_main_process_pkt_2, (0 @ 0)
manage @ 38 seconds :: lan-lan-VPN0:1:[172.18.124.157] (done)
manage @ 38 seconds :: lan-lan-VPN0:1:[172.18.124.157] (start)
         38 seconds doing isa_i_main_process_pkt_4, (0 @ 0)
manage @ 38 seconds :: lan-lan-VPN0:1:[172.18.124.157] (done)
manage @ 39 seconds :: lan-lan-VPN0:1:[172.18.124.157] (start)
         39 seconds doing isa_i_main_process_pkt_6, (0 @ 0)
         39 seconds doing isa_i_main_last_op, (0 @ 0)
   end script: ISAKMP secondary Main for lan-lan-VPN0:1:[172.18.124.157], (0 @ 0)
   next script: lan-lan primary initiator for lan-lan-VPN0:1:[172.18.124.157], (0 @ 0)
         39 seconds doing l2lp_phase_1_done, (0 @ 0)
         39 seconds doing l2lp_start_phase_2, (0 @ 0)
  new script: phase 2 initiator for lan-lan-VPN0:1:[172.18.124.157] (start)
         39 seconds doing iph2_init, (0 @ 0)
         39 seconds doing iph2_build_pkt_1, (0 @ 0)
         39 seconds doing iph2_send_pkt_1, (0 @ 0)
manage @ 39 seconds :: lan-lan-VPN0:1:[172.18.124.157] (done)
manage @ 39 seconds :: lan-lan-VPN0:1:[172.18.124.157] (start)
         39 seconds doing iph2_pkt_2_wait, (0 @ 0)
         39 seconds doing ihp2_process_pkt_2, (0 @ 0)
         39 seconds doing iph2_build_pkt_3, (0 @ 0)
         39 seconds doing iph2_config_SAs, (0 @ 0)
         39 seconds doing iph2_send_pkt_3, (0 @ 0)
        39 seconds doing iph2_last_op, (0 @ 0)
   end script: phase 2 initiator for lan-lan-VPN0:1:[172.18.124.157], (0 @ 0)
   next script: lan-lan primary initiator for lan-lan-VPN0:1:[172.18.124.157], (0 @ 0)
         39 seconds doing 121p_open_tunnel, (0 @ 0)
         39 seconds doing l2lp_start_i_maint, (0 @ 0)
   new script: initiator maintenance for lan-lan-VPN0:1:[172.18.124.157] (start)
        39 seconds doing imnt_init, (0 @ 0)
manage @ 39 seconds :: lan-lan-VPN0:1:[172.18.124.157] (done)
```

cisco_endpoint#show vpn stat

Current	In	High	Running	Tunnel	Tunnel	Tunnel
Active	Negot	Water	Total	Starts	OK	Error

Users	0	0	0	0	0	0	0
Partners	1	0	1	1	1	0	0
Total	1	0	1	1	1	0	0

IOP slot 1:

	Current	In	High	Running	Tunnel	Tunnel	Tunnel
	Active	Negot	Water	Total	Starts	OK	Error
Users	0	0	0	0	0	0	0
Partners	0	0	0	0	0	0	0
Total	0	0	0	0	0	0	0

cisco_endpoint#**show vpn stat verb**

	Current	In	High	Running	Tunnel	Tunnel	Tunnel
	Active	Negot	Water	Total	Starts	OK	Error
Users	0	0	0	0	0	0	0
Partners	1	0	1	1	1	0	0
Total	1	0	1	1	1	0	0

Stats	VPN0:1
Wrapped	13
Unwrapped	9
BadEncap	0
BadAuth	0
BadEncrypt	0
rx IP	9
rx IPX	0
rx Other	0
tx IP	13
tx IPX	0
tx Other	0
IKE rekey	0

Input VPN pkts dropped due to no SA: 0

Input VPN pkts dropped due to no free queue entries: 0

ISAKMP Negotiation stats Admin packets in 4 Fastswitch packets in 0 0 No cookie found Can't insert cookie 0 1 Inserted cookie(L) 0 Inserted cookie(R) Cookie not inserted(L) 0 Cookie not inserted(R) 0 Cookie conn changed 0 Cookie already inserted 0 0 Deleted cookie(L) 0 Deleted cookie(R) Cookie not deleted(L) 0 Cookie not deleted(R) 0 Forwarded to RP 0 0 Forwarded to IOP Bad UDP checksum 0 Not fastswitched 0 Bad Initiator cookie 0 Bad Responder cookie 0 Has Responder cookie 0 No Responder cookie 0 No SA 0

Bad find conn	0
Admin queue full	0
Priority queue full	0
Bad IKE packet	0
No memory	0
Bad Admin Put	0
IKE pkt dropped	0
No UDP PBuf	0
No Manager	0
Mgr w/ no cookie	0
Cookie Scavenge Add	1
Cookie Scavenge Rem	0
Cookie Scavenged	0
Cookie has mgr err	0
New conn limited	0

Bad Initiator cookie 0 Bad Responder cookie 0

IOP slot 1:

	Current Active	In Negot	High Water	Running Total	Tunnel Starts	Tunnel OK	Tunnel Error
Users	0	0	0	0	0	0	0
Partners	0	0	0	0	0	0	0
Total	0	0	0	0	0	0	0
Users Partners Total Stats Wrapped Unwrapped BadEncap BadAuth BadEncryp rx IP rx IPX rx Other tx IP tx IPX tx Other IKE rekey Input VPN INPUT VPN ISAKMP Ne Admin pac Fastswitc No cookie Can't ins Inserted Cachie pac	0 0 0 t pkts dro pkts dro gotiation kets in h packets found ert cooki cookie(L) cookie(R)	0 0 0 0 spped due stats 0 in 3 0 e 0 0 1 d(I) 0	0 0 0 to no SA to no fre	0 0 0 : 0 ee queue e	0 0 entries: (
Cookie no	t inserte	a(L) ()					
Cookie no	t inserte	a(K) U a 0					
Cookie al	nn change ready ing	a u					
Deleted c	ookie(L)	erced 0					
Deleted c	ookie(B)	0					
Cookie no	t deleted	(L) 0					
Cookie no	t deleted	(R) 0					
Forwarded	to RP	0					
Forwarded	to IOP	3					
Bad UDP c	hecksum	0					
Not fasts	witched	0					

Has Responder cookie	0
No Responder cookie	0
No SA	0
Bad find conn	0
Admin queue full	0
Priority queue full	0
Bad IKE packet	0
No memory	0
Bad Admin Put	0
IKE pkt dropped	0
No UDP PBuf	0
No Manager	0
Mgr w/ no cookie	0
Cookie Scavenge Add	1
Cookie Scavenge Rem	0
Cookie Scavenged	0
Cookie has mgr err	0
New conn limited	0

Información Relacionada

- Anuncio de fin de venta de los concentradores Serie VPN 5000 de Cisco
- <u>Negociación IPSec/Protocolos IKE</u>
- Soporte Técnico y Documentación Cisco Systems