Een IPsec-tunnels configureren - Cisco VPN 5000 Concentrator om controlepunt 4.1-firewall te configureren

Inhoud

Inleiding Voorwaarden Vereisten Gebruikte componenten Conventies Configureren Netwerkdiagram Configuraties Control-point 4.1-firewall Verifiëren Problemen oplossen Opdrachten voor VPN 5000 Concentrator probleemoplossing Netwerksamenvatting Checkpoint 4.1 Firewall debug Voorbeeld van output van foutopsporing Gerelateerde informatie

Inleiding

Dit document toont aan hoe u een IPsec-tunnel met pre-Shared Toetsen kunt vormen om zich aan twee particuliere netwerken aan te sluiten. Het sluit zich aan bij een privaat netwerk binnen Cisco VPN 5000 Concentrator (192.168.1.x) aan een privaat netwerk binnen de Checkpoint 4.1 Firewall (10.32.50.x). Er wordt aangenomen dat het verkeer van binnen de VPN-centrator en binnen het checkpoint naar het internet (in dit document weergegeven door de 172.18.124.x-netwerken) toeneemt voordat u deze configuratie start.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

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

- Cisco VPN 5000 Concentrator
- Cisco VPN 5000 Concentrator-softwareversie 5.2.19.001
- Control-point 4.1-firewall

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

Raadpleeg <u>Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor</u> meer informatie over documentconventies.

Configureren

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

N.B.: Gebruik het <u>Opdrachtupgereedschap</u> (<u>alleen geregistreerde</u> klanten) om meer informatie te vinden over de opdrachten die in dit document worden gebruikt.

Netwerkdiagram

Het netwerk in dit document is als volgt opgebouwd:



Dit document gebruikt deze configuratie.

Cisco VPN 5000 Concentrator			
[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]			
KevLifeSecs	=	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 1131 out of 65500 bytes.			

Control-point 4.1-firewall

Volg deze stappen om de firewall van checkpoint 4.1 te configureren.

 Selecteer Properties > Encryption om het checkpoint IPsec-reddingstijden in te stellen om met de KeyLifeSecs-opdracht overeen te komen: 28800 VPN Concentrator.Opmerking: Laat de IKE (Checkpoint Internet Key Exchange)-levensduur bij de standaardinstelling

Properties Setup	×
High Availability IP Pool NAT Access L	Lists Desktop Security
Authentication SYNDefender LDAP Er	ncryption ConnectControl
SKIP Enable Exportable SKIP Change SKIP Session Key : Every 120 Seconds (0 for infinity) or Every 10485760 Bytes (0 for infinity)	Manual IPSEC SPI allocation range (hex): Erom 100 <u>I</u> o ffff
IKE Renegotiate IKE Security Associations every 144 Renegotiate IESEC Security Associations every 288	40 minutes 800 seconds
OK Cancel	Help

 Selecteer Manager > Netwerkobjecten > Nieuw (of Bewerken) > Netwerk om het object voor het interne netwerk ("component") achter het Selectieteken te configureren. Dit moet overeenkomen met de peer = "10.32.50.0/24" VPN Concentrator

N	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: Color:	•
	Location: Broadcast:	
	OK Cancel Help	

3. Selecteer Manager > Netwerkobjecten > Bewerken om het object te bewerken voor het eindpunt van de gateway ("RTPC VPN"-controle) waarnaar de VPN-Concentrator in de partner = <ip> opdracht wijst.Selecteer Intern onder Locatie.Selecteer Gateway voor type.Controleer VPN-1 en FireWall-1 en beheerstation onder de geïnstalleerde

Workstation Pro	operties			>
General Interfa	aces SNMP N	IAT Certifical	tes VPN	Authe
<u>N</u> ame:	RTPCPVPN			
IP <u>A</u> ddress:	172.18.124.157		<u>G</u> et addr	ess
<u>C</u> omment:	Firewalled gatew	ay to internet		
Location: -		Type:		_
Interna	I O <u>E</u> xternal		lost 💌	Gate <u>w</u> ay
- Modules Ins	talled			a.1
VPN-1	& <u>F</u> ireWall-1	Version: [4.1	_	Liet
FloodG	ate-1	Version: 4.1	<u>▼</u>	
	ession	Version: 4.1	7	
🔽 <u>M</u> anag	gement Station	Cojor:		•
				1
	OK	Cancel	Help	

4. Selecteer Manager > Netwerkobjecten > Nieuw (of Bewerken) > Netwerk om het object voor het externe netwerk ("interne_cisco") achter de VPN-centrator te configureren.Dit moet overeenkomen met de opdracht LocalAccess = <192.168.1.0/24>VPN

	Network Properties
	General NAT
	<u>Name:</u> inside_cisco
	IP Address: 192.168.1.0 Get address
	Net <u>M</u> ask: 255.255.255.0
	Color: Color:
	Location: Broadcast:
	○ Internal ● External ● Allowed ● Disallowed
	OK Cancel Help
trator.	

5. Selecteer Manager > Netwerkobjecten > Nieuw > Workstation om een object voor de externe ("cisco_endpoints") VPN Concentrator-gateway toe te voegen.Dit is de "buiten" interface van de VPN-Concentrator met connectiviteit op het Selectieteken (in dit document is 172.18.124.35 het IP-adres in het IPA-adres = <ip>opdracht).Selecteer Extern onder Locatie. Selecteer Gateway voor type.Opmerking: controleer VPN-1/FireWall-1

Workstation Properties	×
General Interfaces SNMP NAT VPN	
Name: cisco_endpoint	
IP <u>A</u> ddress: 172.18.124.35 <u>G</u> e	t address
<u>C</u> omment:	
Location: □ Internal	● Gate <u>w</u> ay
Modules Installed	
VPN-1 & FireWall-1 Version: 4.1	Get
FloodGate-1 Version: 4.1	3
Compression Version: 4.1	3
Management Station Color:	
OK Cancel He	elp

niet

6. Selecteer Manager > Netwerkobjecten > Bewerken om het tabblad Selectiepunt te bewerken (genaamd "RTPVPN") VPN-tabblad. Selecteer onder Domain, Andere en selecteer dan de binnenkant van het Checkpoint netwerk (genoemd "component") in de vervolgkeuzelijst. Selecteer onder Encryption schemes die worden gedefinieerd IKE en klik vervolgens op

Workstation Properties	×			
General Interfaces SNMP NAT	Certificates VPN Authe			
Domain: Disabled Valid Addresses(of Interfaces) Disabled Line Line Line Line Line Line Line Line	Encryption schemes defined:			
- Troffic Control Logging				
I Tame Control Logging I Ium on Traffic Control Loggi	ng			
OK Car	ncel Help			

- Bewerken.
- 7. Verander de IKE eigenschappen in **DES** encryptie en **SHA1** hashing om met de opdracht **SHA_DES_G2** VPN Concentrator akkoord te gaan.**Opmerking:** The "G2" verwijst naar Diffie-Hellman groep 1 of 2. Bij testen werd ontdekt dat het checkpoint ofwel "G2" ofwel "G1" accepteert.Wijzig deze instellingen:De selectie van de **aggregatieroute** opheffen.Controleer **Ondersteunen subnetten**.Controleer **vooraf gedeeld geheim** onder

	General Interfaces SNMP NAT Certificates VPN Authe
	KE Properties 🚬 🔁
	General
	Key <u>N</u> egotiation Encryption Method(s): <u>H</u> ash Method: _
	I SHA1
	Authentication Method:
	✓ Pre-Shared Secret Edit Secrets
	Public Key Signatures <u>Configure</u>
	Supports Aggresive <u>M</u> ode 🔽 Supports Su <u>b</u> nets
	OK Cancel Help
vernicatiemethode.	

8. Klik op **Geheimen bewerken** om de voorgedeelde toets in te stellen om met de **SharedKey =** <**key**>VPN Concentrator-opdracht akkoord te

Workstation Properties
General Interfaces SNMP NAT Certificates VPN Authe
IKE Properties
General
Shared Secret
- Shared Secrets List:
Peer Name Shared Secret cisco_endpoint **** Edit Remove
OK Cancel Help
Qaan.

9. Selecteer Manager > Netwerkobjecten > Bewerken om het tabblad "cisco_end" VPN te bewerken. Selecteer onder Domain, Andere, en selecteer dan de binnenkant van het netwerk van de VPN Concentrator (genoemd "binnenkant_cisco"). Selecteer onder Encryption schemes die worden gedefinieerd IKE en klik vervolgens op

Workstation Properties	×		
General Interfaces SNMP NAT	VPN		
Domain:	Encryption schemes defined:		
C Disabled	Manual IPSEC		
○ Valid Addresses(of Interfaces)			
	SKIP		
🖳 inside_cisco 💌			
Exportable for SecuRemote	<u>E</u> dit		
Traffic Control Logging	ng		
OK Ca	ncel Help		

- Bewerken.
- 10. Verander de IKE eigenschappen in DES encryptie en SHA1 hashing om met de opdracht SHA_DES_G2 VPN Concentrator akkoord te gaan.Opmerking: The "G2" verwijst naar Diffie-Hellman groep 1 of 2. Bij testen bleek dat het checkpoint ofwel "G2" ofwel "G1" accepteert.Wijzig deze instellingen:De selectie van de aggregatieroute opheffen.Controleer Ondersteunen subnetten.Controleer vooraf gedeeld geheim onder

KE Properties
General
Key Negotiation Encryption Method(s): Hash Method: Image: Destination Encryption Method(s): Image: MD5 Image: Destination Encryption Method(s): Image: Method(s): Image: Destination Encryption Method(s): Image: Method(s): Image: Destination Encryption Method(s): Image: Method(s):
Authentication Method:
☐ Public Key Signatures Configure ☐ Supports Aggresive Mode ✓ Supports Subnets
OK Cancel Help

verificatiemethode.

11. Klik op **Geheimen bewerken** om de voorgedeelde toets in te stellen om met de **SharedKey** = <key>VPN Concentrator-opdracht akkoord te

IKE Properties	×
General	
Shared Secret	×
Shared Secrets List: Peer Name Shared Secret RTPCPVPN **** <u>Ec</u> <u>R</u> em	lit Iove
OK Cancel Help	

 Typ in het venster Policy Editor een regel met zowel Bron als Destination als "interne_cisco" en "cpinto" (bidirectioneel). Service=Any instellen, Action=Encrypt en Track=Long.

ľ	RTPO	CPVPN - Check P	oint Policy Editor				- 🗆 ×
E	ile <u>E</u> di	t <u>V</u> iew <u>M</u> anage	Policy <u>W</u> indow <u>H</u>	elp			
	- 5	🖪 🕹 🕻 🖻	E 💁 🕉 🕉	B. 🐬 🌆 🖆	🗏 🖀 🖷 🖦	u 🖡 🖃 📑	😓 🍸 🚯
	😫 Secu	urity Policy - Standard	🕂 🖶 Address Trans	slation - Standard 🛛 😿	Bandwidth Policy - St	andard	
I	No.	Source	Destination	Service	Action	Track	ln <mark></mark> ≜
1	1	🚆 inside_cisco	👷 cpinside 👷 inside_cisco	Any	Encrypt	Long	
l	•						•
F	or Help,	press F1		RTPC	PVPN Read	I/Write	

13. Klik onder het kopje Actie op het pictogram groene **versleuteling** en selecteer **Eigenschappen bewerken** om het coderingsbeleid te

configureren.				
rrity Policy - Standard	🛃 Address Translation	- Standard 👭 Ban	dwidth Policy - Standard	
∼ FVV1 Host	∼ Ldap-Servers	🕑 Idap	accept	
∼ FVV1 Host	∼ Logical-Servers	∼ load_agent	accept	5
💂 inside_cisco	🖶 cpinside 🚆 inside_cisco	Any	dit properties	hg .
		dest-unreach	Edit Encryption	
		echo-reply		
		icmp. proto	accept	ern i
		icmp info-reply		
		icmp info-reg	drop	
😑 Any	Any	imp mask-reply	7 🦰 reject	
41		imp meet ransact		
•				

14. Selecteer IKE en klik op

	Encryption Properties
	General Encryption schemes defined:
verken	OK Cancel Help

15. Wijzig deze eigenschappen in het venster IKE Properties om het af te stemmen met de opdracht Transformer = SSP(sha,des) VPN Concentrator.Selecteer onder Omzetten de optie Encryption + Data Integrity (ESP). Het Encryption Algorithm moet DES zijn, de gegevensintegriteit moet SHA1 zijn en de toegestane peer Gateway moet de externe VPN Concentrator-gateway (aangeduid als "cisco_endpoints") zijn. Klik op

IKE Properties	×
General	1
 Iransform: Encryption + Data Integr Data Integrity Only (AH) 	ity (ESP)
Encryption Algorithm:	DES
<u>D</u> ata Integrity	SHA1
Allowed Peer Gateway:	cisco_endpo
Use Perfect Forward See	crecy
	Cancel Help

16. Nadat u het selectieteken aanpast, selecteert u **Beleidsbeleid > Installatie** in het menu Selectieteken om de wijzigingen van kracht te laten worden.

Verifiëren

Er is momenteel geen verificatieprocedure beschikbaar voor deze configuratie.

Problemen oplossen

Opdrachten voor VPN 5000 Concentrator probleemoplossing

Het <u>Uitvoer Tolk</u> (<u>uitsluitend geregistreerde</u> klanten) (OIT) ondersteunt bepaalde **show** opdrachten. Gebruik de OIT om een analyse van **tonen** opdrachtoutput te bekijken.

Opmerking: Raadpleeg <u>Belangrijke informatie over debug Commands</u> voordat u **debug**opdrachten gebruikt.

- vpn-scan-alles-Geeft informatie over alle bijbehorende VPN-verbindingen, inclusief informatie over de tijd, het VPN-nummer, het echte IP-adres van de peer, de scripts die zijn uitgevoerd, en in het geval van een fout, het routine- en regelnummer van de software code waar de fout is opgetreden.
- Geeft de systeemlogbuffer weer toont de inhoud van de interne logbuffer.
- vpn statistieken tonen toont deze informatie voor gebruikers, partners, en het totaal voor beide. (Voor modulaire modellen bevat de weergave een gedeelte voor elke modulesleuf. Raadpleeg het gedeelte <u>Uitvoer van monster</u>.)Huidige actieve-de huidige actieve verbindingen.In het niets—de op dit moment onderhandelende verbindingen.Hoog water: het hoogste aantal gelijktijdige actieve verbindingen sinds de laatste herstart.Totaal uitvoeren: het totale aantal succesvolle verbindingen sinds de laatste herstart.Tunnel ok - Het aantal tunnels waarvoor geen fouten waren.Tunnel start—het aantal tunnels start.Tunnelfout-het aantal tunnels met fouten.
- toon VPN statistiek breedband toont ISAKMP onderhandelingsstatistieken, en veel meer actieve verbindingsstatistieken.

Netwerksamenvatting

Wanneer meerdere aangrenzende interne netwerken zijn geconfigureerd in het encryptiedomein op het Selectieteken, kan het apparaat deze automatisch samenvatten met betrekking tot interessant verkeer. Als de VPN Concentrator niet is geconfigureerd om aan elkaar te koppelen, zal de tunnel waarschijnlijk falen. Als bijvoorbeeld de binnennetwerken van 10.0.0.0/24 en 10.0.1.0/24 zodanig zijn geconfigureerd dat ze in de tunnel worden opgenomen, kunnen ze worden samengevat tot 10.0.0.0/23.

Checkpoint 4.1 Firewall debug

Dit was een Microsoft Windows NT-installatie. Omdat de tracering lang is ingesteld in het venster Policy Editor (zoals weergegeven in <u>Stap 12</u>), moet het ontkende verkeer in het logvenster rood verschijnen. Meer breedaardige debug is te verkrijgen door:

C:\WINNT\FW1\4.1\fwstop C:\WINNT\FW1\4.1\fw d -d en in een ander venster: 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
Antwoord ja op de Zijn jullie zeker?.

Voorbeeld van output van foutopsporing

```
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 l2lp_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 Active	In Negot	High Water	Running Total	Tunnel Starts	Tunnel OK	Tunnel 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_end	point# sho	w vpn sta	t verb				
	Current	In	High	Running	Tunnel	Tunnel	Tunnel
	Current Active	In Negot	High Water	Running Total	Tunnel Starts	Tunnel OK	Tunnel Error
	Current Active	In Negot	High Water 	Running Total	Tunnel Starts	Tunnel OK	Tunnel Error
Users	Current Active 0	In Negot 	High Water 	Running Total 	Tunnel Starts 	Tunnel OK 	Tunnel Error
Users Partners	Current Active 0 1	In Negot 0 0	High Water 0 1	Running Total 0 1	Tunnel Starts 0 1	Tunnel OK 0 0	Tunnel Error 0 0
Users Partners Total	Current Active 0 1 1	In Negot 0 0 0	High Water 0 1 1	Running Total 0 1 1	Tunnel Starts O 1 1	Tunnel OK 0 0 0 0	Tunnel Error 0 0 0
Users Partners Total	Current Active 0 1 1	In Negot 0 0 0	High Water 0 1 1	Running Total 0 1 1	Tunnel Starts 0 1 1	Tunnel OK 0 0 0	Tunnel Error 0 0 0
Users Partners Total Stats	Current Active 0 1 1	In Negot 0 0 0 VPN0:1	High Water 0 1 1	Running Total 0 1 1	Tunnel Starts 0 1 1	Tunnel OK 0 0 0	Tunnel Error 0 0 0

9 Unwrapped 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 No cookie found 0 Can't insert cookie 0 Inserted cookie(L) 1 0 Inserted cookie(R) Cookie not inserted(L) 0 Cookie not inserted(R) 0 Cookie conn changed 0 Cookie already inserted 0 Deleted cookie(L) 0 Deleted cookie(R) 0 Cookie not deleted(L) 0 0 Cookie not deleted(R) Forwarded to RP 0 0 Forwarded to IOP Bad UDP checksum 0 Not fastswitched 0 Bad Initiator cookie 0 0 Bad Responder cookie 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

IOP slot 1:

	Current Active	In Negot	High Water	Running Total	Tunnel Starts	Tunnel OK	Tunnel Error
IIaana							
Users	0	0	0	0	0	0	0
Total	0	0	0	0	0	0	0
IOCAL	0	0	0	0	0	0	0
Stats Wrapped Unwrapped BadEncap BadAuth BadEncryp rx IP rx IPX rx Other tx IP tx IPX tx Other IKE rekey	t						
Input VPN	pkts dro	pped due	to no SA	: 0			
Input VPN	pkts dro	opped due	to no fr	ee queue e	ntries: ()	
ISAKMP Ne	gotiation	n stats					
Admin pac	kets in	0					
Fastswitc	h packets	s in 3					
No cookie	found	0					
Can't ins	ert cooki	.e 0					
Inserted	cookie(L)	0					
Inserted	cookie(R)	1					
Cookie no	t inserte	ed(L) 0					
Cookie no	t inserte	ed(R) 0					
Cookie co	nn change	ed 0					
Cookie al	ready ins	serted 0					
Deleted c	ookie(L)	0					
Deleted c	ookie(R)	0					
Cookie no	t deleted	l(L) 0					
Cookie no	t deleted	l(R) 0					
Forwarded	to RP	0					
Forwarded	to IOP	3					
Bad UDP c	hecksum	0					
Not fasts	witched	0					
Bad Initi	ator cook	tie O					
Bad Respo	nder cook	tie O					
Has Respo	nder cook	tie O					
No Respon	der cooki	.e 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

Gerelateerde informatie

- <u>Cisco VPN 5000 Series Concentrators end-of-sale aankondiging</u>
- IPsec-onderhandeling/IKE-protocollen
- Technische ondersteuning en documentatie Cisco Systems