Konfigurieren eines IPsec-Tunnels - Cisco VPN 5000 Concentrator für Checkpoint 4.1-Firewall

Inhalt

Einführung Voraussetzungen Anforderungen Verwendete Komponenten Konventionen Konfigurieren Netzwerkdiagramm Konfigurationen **Checkpoint 4.1-Firewall** Überprüfen Fehlerbehebung Befehle zur Fehlerbehebung beim VPN 500 Concentrator Netzwerkzusammenfassung Checkpoint 4.1 Firewall-Fehlerbehebung Beispielausgabe für Debugging Zugehörige Informationen

Einführung

In diesem Dokument wird veranschaulicht, wie ein IPsec-Tunnel mit vorinstallierten Schlüsseln aufgebaut wird, um zwei private Netzwerke miteinander zu verbinden. Sie verbindet ein privates Netzwerk im Cisco VPN 500 Concentrator (192.168.1.x) mit einem privaten Netzwerk innerhalb der Checkpoint 4.1-Firewall (10.32.50.x). Es wird davon ausgegangen, dass der Datenverkehr aus dem Inneren des VPN-Konzentrators und innerhalb des Prüfpunkts zum Internet (dargestellt in diesem Dokument durch die Netzwerke 172.18.124.x) fließt, bevor Sie mit dieser Konfiguration beginnen.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und

Hardwareversionen:

- Cisco VPN 5000 Concentrator
- Cisco VPN 5000 Concentrator Software Version 5.2.19.0001
- Checkpoint 4.1-Firewall

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter <u>Cisco Technical Tips</u> <u>Conventions</u> (Technische Tipps zu Konventionen von Cisco).

Konfigurieren

In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

Hinweis: Verwenden Sie das <u>Command Lookup Tool</u> (nur <u>registrierte</u> Kunden), um weitere Informationen zu den in diesem Dokument verwendeten Befehlen zu erhalten.

Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



Konfigurationen

In diesem Dokument wird diese Konfiguration verwendet.

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]			
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.	

Checkpoint 4.1-Firewall

Führen Sie diese Schritte aus, um die Checkpoint 4.1-Firewall zu konfigurieren.

 Wählen Sie Eigenschaften > Verschlüsselung aus, um die IPsec-Lebensdauer des Prüfpunkts so festzulegen, dass sie mit dem Befehl KeyLifeSecs = 28800 VPN Concentrator übereinstimmt.Hinweis: Lassen Sie die Nutzungsdauer des Internet Key Exchange (IKE) des Prüfpunkts standardmäßig unverändert.

Properties Setup	×
High Availability IP Pool NAT Acces Security Policy Traffic Control Services L Authentication SYNDefender LDAP	ss Lists Desktop Security Log 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)	<u>Erom</u> 100
E⊻ery 10485760 Bytes (0 for infinity)	<u>I</u> o Ifff
Renegotiate I <u>K</u> E Security Associations every	1440 minutes
Renegotiate I <u>P</u> SEC Security Associations every	28800 seconds
OK Cancel	Help

2. Wählen Sie Verwalten > Netzwerkobjekte > Neu (oder Bearbeiten) > Netzwerk, um das Objekt f
ür das interne ("cpinside") Netzwerk hinter dem Pr
üfpunkt zu konfigurieren. Dies sollte mit dem Befehl "Peer = "10.32.50.0/24" VPN Concentrator

letwork Proper	ties			2
General NAT	1			
<u>N</u> ame:	cpinside]	
IP Address:	10.32.50.0		<u>G</u> et address	
Net <u>M</u> ask:	255.255.255.0]	
<u>C</u> omment:			Color:	•
Location:	O <u>E</u> xternal	Broadcast	t O <u>D</u> isallowed	
	<u></u>	11		

- übereinstimmen.
- 3. Wählen Sie Verwalten > Netzwerkobjekte > Bearbeiten, um das Objekt für den Gateway-Endpunkt ("RTPCPVPN"-Prüfpunkt) zu bearbeiten, auf den der VPN-Konzentrator im Partner = <ip>-Befehl verweist.Wählen Sie Interne unter Speicherort aus.Wählen Sie Gateway als Typ aus.Unter Installierte Module finden Sie Informationen zu VPN-1 und FireWall-1 und Managementkonsole.

Workstation Properties
General Interfaces SNMP NAT Certificates VPN Authe
Name: RTPCPVPN
IP <u>A</u> ddress: 172.18.124.157 <u>G</u> et address
Comment: Firewalled gateway to internet
Location:Type:
O <u>I</u> nternal O <u>E</u> xternal O <u>H</u> ost O Gate <u>w</u> ay
Modules Installed
VPN-1 & EireWall-1 Version: 4.1 Cet
FloodGate-1 Version: 4.1
Compression Version: 4.1
Management Station Color:
OK Cancel Help

4. Wählen Sie Verwalten > Netzwerkobjekte > Neu (oder Bearbeiten) > Netzwerk, um das Objekt für das externe ("inside_cisco") Netzwerk hinter dem VPN-Konzentrator zu konfigurieren.Dies sollte mit dem Befehl LocalAccess = <192.168.1.0/24> VPN Concentrator

	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:	
	<u>○ Internal</u> <u>○ External</u> <u>○ Allowed</u> <u>○ D</u> isallowed	
	OK Cancel Help	
ubereinstimmen.		

5. Wählen Sie Verwalten > Netzwerkobjekte > Neu > Workstation, um ein Objekt für das externe VPN-Concentrator-Gateway ("cisco_endpoint") hinzuzufügen.Dies ist die "externe" Schnittstelle des VPN Concentrator mit Verbindung zum Checkpoint (in diesem Dokument ist 172.18.124.35 die IP-Adresse im IPAddress = <ip>-Befehl).Wählen Sie Extern unter Speicherort aus. Wählen Sie Gateway als Typ aus.Hinweis: Aktivieren Sie VPN-1/FireWall-1

Workstation Properties
General Interfaces SNMP NAT VPN
<u>N</u> ame: cisco_endpoint
IP <u>A</u> ddress: 172.18.124.35 <u>G</u> et address
<u>C</u> omment:
Location: Type: O Internal O External Most O Gateway
Modules Installed
✓ VPN-1 & FireWall-1 Version: 4.1 ✓ Get
FloodGate-1 Version: 4.1
Compression Version: 4.1
Management Station Color: ▼
OK Cancel Help

nicht.

6. Wählen Sie Verwalten > Netzwerkobjekte > Bearbeiten, um die Registerkarte f
ür das Checkpoint Gateway-Endger
ät (RTPCPVPN genannt) zu bearbeiten. W
ählen Sie unter Domain (Dom
äne) die Option Other (Andere) aus, und w
ählen Sie dann die Innenseite des Checkpoint-Netzwerks (als "cpinside" bezeichnet) aus der Dropdown-Liste aus. W
ählen Sie unter Definierte Verschl
üsselungsschemata die Option IKE aus, und klicken Sie dann auf

Workstation Properties	×
General Interfaces SNMP NAT	Certificates VPN Authe
Domain: ○ Disabled ○ Valid Addresses(of Interfaces) ○ Dther: Image: cpinside Image: cpinside </td <td>Encryption <u>s</u>chemes defined:</td>	Encryption <u>s</u> chemes defined:
OK Ca	ncel Help

Bearbeiten.

7. Ändern Sie die IKE-Eigenschaften in DES-Verschlüsselung und SHA1-Hashing, um mit dem Befehl SHA_DES_G2 VPN Concentrator zu übereinstimmen.Hinweis: "G2" bezieht sich auf die Diffie-Hellman-Gruppe 1 oder 2. Beim Testen wurde entdeckt, dass der Prüfpunkt entweder "G2" oder "G1" akzeptiert.Ändern Sie diese Einstellungen:Deaktivieren Sie die Option Aggressiver Modus.Aktivieren Sie Subnetze unterstützen.Aktivieren Sie Pre-Shared Secret unter Authentication

General Interfaces SNMP NAT Certificates	VPN Authe
KE Properties	×
General	
Key Negotiation Encryption Method(s):	Hash Method: -
Pre-Shared Secret Edit Secret Public Key Signatures Config	gure
Supports Aggresive Mode Supports	Su <u>b</u> nets
OK Cancel H	elp
Method.	

8. Klicken Sie auf **Edit Secrets** (Geheimnisse **bearbeiten**), um den vorinstallierten Schlüssel so festzulegen, dass er mit dem Befehl **SharedKey = <key>** VPN Concentrator

Workstation Properties
General Interfaces SNMP NAT Certificates VPN Authe
IKE Properties
General
Shared Secret 🗙
Shared Secrets List:
Peer Name Shared Secret
<u>R</u> emove
OK Cancel
OK Cancel Help

übereinstimmt.

9. Wählen Sie Verwalten > Netzwerkobjekte > Bearbeiten, um die Registerkarte "cisco_endpoint" für VPN zu bearbeiten. Wählen Sie unter Domain (Domäne) die Option Other (Andere) aus, und wählen Sie dann die interne Komponente des VPN Concentrator-Netzwerks aus (die Bezeichnung "inside_cisco"). Wählen Sie unter Definierte Verschlüsselungsschemata die Option IKE aus, und klicken Sie dann auf

Workstation Properties	×
General Interfaces SNMP NAT	VPN
Domain:	Encryption schemes defined:
○ <u>D</u> isabled ○ <u>V</u> alid Addresses(of Interfaces)	Manual IPSEC
• <u>O</u> ther:	🗖 🖬 SKIP
inside_cisco 🔽	
Exportable for SecuRemote	<u>E</u> dit
Traffic Control Logging	Ig
OK Car	ncel Help

Bearbeiten.

10. Ändern Sie die IKE-Eigenschaften in DES-Verschlüsselung und SHA1-Hashing, um mit dem Befehl SHA_DES_G2 VPN Concentrator zu übereinstimmen.Hinweis: "G2" bezieht sich auf die Diffie-Hellman-Gruppe 1 oder 2. Im Test wurde festgestellt, dass der Prüfpunkt entweder "G2" oder "G1" akzeptiert.Ändern Sie diese Einstellungen:Deaktivieren Sie die Option Aggressiver Modus.Aktivieren Sie Subnetze unterstützen.Aktivieren Sie Pre-Shared Secret unter Authentication

General Interfaces SNMP NAT Certificates	VPN Authe
KE Properties	
General	
Key <u>N</u> egotiation Encryption Method(s):	Hash Method: -
I I I CAST	□ MD <u>5</u>
D 🖾 3DES	I SHA <u>1</u>
Authentication Method:	
Pre-Shared Secret Edit S	ecrets
Public Key Signatures <u>Conf</u>	figure
Supports Aggresive <u>M</u> ode 🔽 Support	ts Su <u>b</u> nets
OK Cancel H	Help
Vethod.	

11. Klicken Sie auf **Edit Secrets** (Geheimnisse **bearbeiten**), um den vorinstallierten Schlüssel so festzulegen, dass er mit dem Befehl **SharedKey = <key>** VPN Concentrator

	IKE Properties	×
	General	
	Shared Secret	×
	Shared Secret Peer Name Shared Secret RTPCPVPN **** Edit Edit Remove Emove	
	OK Cancel	
übereinstimmt.	OK Cancel Help	

 Fügen Sie im Fenster des Richtlinien-Editors eine Regel mit Quelle und Ziel als "inside_cisco" und als "cpinside" (bidirektional) ein. Set Service=Any, Action=Encrypt und Track=Long.

ľ	RTPC	PVPN - Check P	oint Policy Editor				- 🗆 🗵
E	ile <u>E</u> di	t ⊻iew <u>M</u> anage	<u>Policy W</u> indow <u>H</u>	elp			
	- 5	🖻 🎗 🔍 🔊	🖻 🚇 😽 🕉	B. 🐬 🌌 😭	📙 🖀 🖷 🖕	u, 🖡 🕪 📑	😓 🍸 🚯
😸 Security Policy - Standard 📩 Address Translation - Standard 😨 Bandwidth Policy - Standard							
I	No.	Source	Destination	Service	Action	Track	In
1	1	🚆 inside_cisco	👷 cpinside 👷 inside_cisco	Any	Encrypt	Long	GV
l	•						▶
F	or Help, j	press F1		RTPC	PVPN Read	Write	

13. Klicken Sie unter der Überschrift Aktion auf das grüne Symbol Verschlüsselung, und wählen Sie Eigenschaften bearbeiten aus, um Verschlüsselungsrichtlinien zu konfigurieren

rity Policy - Standard	📇 Address Translation	- Standard 报 Ban	dwidth Policy - Standard	
~ FVV1 Host	∼ Ldap-Servers	10 Idap	accept	
∼ FVV1 Host	∼ Logical-Servers	∼ load_agent	accept	5
💂 inside_cisco	🚑 cpinside 🚆 inside_cisco	Any	dit properties	T ig
		icmp dest-unreach icmp echo-reply icmp echo-request	Edit Encryption	
		icmp-proto	drop	
Any	Any	imp mask-reply	🚺 😑 reject	
•				

14. Wählen Sie IKE aus, und klicken Sie auf

Encryption Properties	×
General	
Encryption schemes defined:	
OK Cancel Help	

- Bearbeiten.
- 15. Ändern Sie im Fenster IKE-Eigenschaften diese Eigenschaften, um mit dem Befehl Transform = esp(sha,des) VPN Concentrator zuzustimmen.Wählen Sie unter Transform (Transform) Encryption + Data Integrity (ESP) aus. Der Verschlüsselungsalgorithmus muss DES sein, die Datenintegrität muss SHA1 sein, und das zulässige Peer-Gateway muss das externe VPN-Concentrator-Gateway sein (der Name lautet "cisco_endpoint"). Klicken Sie

IKE Properties	
General	
- Transform:	
Encryption + Data Integri	ty (ESP)
C Data Integrity Only (AH)	
Encryption Algorithm:	DES
<u>D</u> ata Integrity	SHA1 🔽
Allowed Peer Gateway:	cisco endpo
Lise Perfect Forward Sec	
	accy.
	ancel Help

16. Nachdem Sie den Checkpoint konfiguriert haben, wählen Sie im Checkpoint-Menü **Richtlinien > Installieren**, damit die Änderungen wirksam werden.

<u>Überprüfen</u>

Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

Fehlerbehebung

Befehle zur Fehlerbehebung beim VPN 500 Concentrator

Das <u>Output Interpreter Tool</u> (nur <u>registrierte</u> Kunden) (OIT) unterstützt bestimmte **show**-Befehle. Verwenden Sie das OIT, um eine Analyse der **Ausgabe des** Befehls **show anzuzeigen**.

Hinweis: Beachten Sie <u>vor der</u> Verwendung von **Debug-**Befehlen die <u>Informationen</u> zu <u>Debug-</u><u>Befehlen</u>.

- vpn trace dump all Zeigt Informationen über alle übereinstimmenden VPN-Verbindungen an, einschließlich Informationen über die Zeit, die VPN-Nummer, die tatsächliche IP-Adresse des Peers, die ausgeführten Skripts und im Falle eines Fehlers die Routine und Leitungsnummer des Software-Codes, in dem der Fehler aufgetreten ist.
- **show system log buffer** (Systemprotokollpuffer anzeigen) Zeigt den Inhalt des internen Protokollpuffers an.
- show vpn statistics Zeigt diese Informationen für Benutzer, Partner und die Gesamtsumme für beide. (Bei modularen Modellen umfasst das Display einen Bereich für jeden Modulsteckplatz. Weitere Informationen finden Sie im Abschnitt Beispieldebugausgabe.)Current Active - Die aktuell aktiven Verbindungen.In Negot - Die derzeit verhandelnden Verbindungen.High Water - Die höchste Anzahl gleichzeitiger aktiver Verbindungen seit dem letzten Neustart.Running Total (Gesamt ausführen): Die Gesamtzahl erfolgreicher Verbindungen seit dem letzten Neustart.Tunnel ok (Tunnel OK): Die Anzahl der Tunnel, für die keine Fehler aufgetreten sind.Tunnel starts (Tunnel wird gestartet): Die Anzahl der Tunnelstarts.Tunnel Error (Tunnel-Fehler): Die Anzahl der Tunnel mit Fehlern.
- show vpn statistics ausführliche Zeigt Statistiken zur ISAKMP-Aushandlung und viele weitere aktive Verbindungsstatistiken an.

Netzwerkzusammenfassung

Wenn mehrere benachbarte Netzwerke in der Verschlüsselungsdomäne am Checkpoint konfiguriert sind, kann das Gerät diese automatisch in Bezug auf interessanten Datenverkehr zusammenfassen. Wenn der VPN-Concentrator nicht für eine Übereinstimmung konfiguriert ist, schlägt der Tunnel wahrscheinlich fehl. Wenn beispielsweise die internen Netzwerke 10.0.0.0 /24 und 10.0.1.0 /24 so konfiguriert sind, dass sie in den Tunnel eingeschlossen werden, können sie in 10.0.0.0 /23 zusammengefasst werden.

Checkpoint 4.1 Firewall-Fehlerbehebung

Dies war eine Microsoft Windows NT-Installation. Da die Verfolgung im Fenster des Policy Editor (wie in <u>Schritt 12</u> gezeigt) für Long festgelegt wurde, sollte der abgelehnte Datenverkehr in der Protokollanzeige rot angezeigt werden. Ausführlichere Debugging-Informationen finden Sie unter:

C:\WINNT\FW1\4.1\fwstop C:\WINNT\FW1\4.1\fw d -d und in einem anderen Fenster: $C:\WINNT\FW1\4.1\fwstart$

Führen Sie diese Befehle aus, um die Sicherheitszuordnungen (SAs) am Prüfpunkt zu löschen:

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
Beantworten Sie mit Ja im Fenster Sind Sie sicher? eingeben.

Beispielausgabe für Debugging

```
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	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 tx IP tx IPX tx Other IKE rekey Input VPN Input VPN ISAKMP Ne Admin pac Fastswitc No cookie Can't ins Inserted Inserted Cookie no Cookie no Cookie al Deleted c	0 0 0 t pkts dro pkts dro gotiation kets in h packets found ert cooki cookie(L) cookie(R) t inserte t inserte nn change ready ins ookie(L)	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	0 0 0 to no SA: to no fre	0 0 0	0 0 entries: (0 0
Deleted c	ookie(L)	0					
Deleted c	ookie(R)	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	U					
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

Zugehörige Informationen

- Cisco VPN Concentrators der Serie 5000 Ankündigung des Vertriebsendes
- IPsec-Aushandlung/IKE-Protokolle
- <u>Technischer Support und Dokumentation Cisco Systems</u>