Konfigurieren von IPSec zwischen einem Microsoft Windows 2000-Server und einem Cisco Gerät

Inhalt

Einführung Bevor Sie beginnen Konventionen Voraussetzungen Verwendete Komponenten Netzwerkdiagramm Konfigurieren des Microsoft Windows 2000-Servers für die Arbeit mit Cisco Geräten Durchgeführte Aufgaben Schrittweise Anleitung Konfigurieren der Cisco Geräte Konfigurieren des Cisco 3640 Routers Konfigurieren von PIX Konfigurieren des VPN 3000-Konzentrators Konfigurieren des VPN 500-Konzentrators Überprüfen Fehlerbehebung Befehle zur Fehlerbehebung Zugehörige Informationen

Einführung

In diesem Dokument wird veranschaulicht, wie ein IPSec-Tunnel mit vorinstallierten Schlüsseln erstellt wird, um zwei privaten Netzwerken beizutreten: ein privates Netzwerk (192.168.I.X) innerhalb eines Cisco Geräts und ein privates Netzwerk (10.32.50.X) innerhalb des Microsoft 2000-Servers. Wir gehen davon aus, dass der Datenverkehr vom Cisco Gerät und innerhalb des 2000-Servers zum Internet (hier durch die Netzwerke 172.18.124.X dargestellt) vor Beginn dieser Konfiguration fließt.

Ausführliche Informationen zur Konfiguration des Microsoft Windows 2000-Servers finden Sie auf der Microsoft-Website: <u>http://support.microsoft.com/support/kb/articles/Q252/7/35.ASP</u>

Bevor Sie beginnen

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den <u>Cisco Technical Tips</u> <u>Conventions</u>.

Voraussetzungen

Für dieses Dokument bestehen keine besonderen Voraussetzungen.

Verwendete Komponenten

Diese Konfigurationen wurden mit den unten stehenden Software- und Hardwareversionen entwickelt und getestet.

- Microsoft Windows 2000 Server 5.00.2195
- Cisco 3640 Router mit Cisco IOS® Software-Version c3640-ik2o3s-mz.121-5.T.bin
- Cisco Secure PIX Firewall mit PIX Software Version 5.2.1
- Cisco VPN 3000 Concentrator mit VPN 3000 Concentrator Software Version 2.5.2.F
- Cisco VPN 5000 Concentrator mit VPN 500 Concentrator Software Version 5.2.19

Die in diesem Dokument enthaltenen Informationen wurden aus Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Sie in einem Live-Netzwerk arbeiten, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen, bevor Sie es verwenden.

Netzwerkdiagramm

In diesem Dokument wird die im Diagramm unten dargestellte Netzwerkeinrichtung verwendet.



Konfigurieren des Microsoft Windows 2000-Servers für die Arbeit mit Cisco Geräten

Durchgeführte Aufgaben

Dieses Diagramm zeigt die in der Microsoft Windows 2000-Serverkonfiguration ausgeführten Aufgaben:



Schrittweise Anleitung

Wenn Sie die <u>Konfigurationsanweisungen</u> auf der Microsoft-Website befolgt haben, überprüfen Sie anhand der folgenden Schritte, ob Ihre Konfiguration mit Cisco Geräten kompatibel ist. Kommentare und Änderungen werden mit den Screenshots vermerkt.

 Klicken Sie auf dem Microsoft Windows 2000-Server auf Start > Ausführen > secpol.msc, und überprüfen Sie die Informationen auf den folgenden Bildschirmen.Nachdem die Anweisungen auf der Microsoft-Website zur Konfiguration eines 2000-Servers verwendet wurden, wurden die folgenden Tunnelinformationen angezeigt.Hinweis: Die Beispielregel heißt "to cisco".

bcal Security Settings				_ 🗆 ×
Action ⊻iew ↔	🗈 🔳 🗙 🗗 🗔	😢 🗋 🏦 🗍 🖺 🚨		
Tree	Name 🔺	Description	Policy Assigned	
Security Settings	Client (Respond Only)	Communicate normally (uns	No	
🗄 🧾 Account Policies	Secure Server (Requir	For all IP traffic, always req	No	
E Public Key Policies	to_cisco	Tor airse traine, aways roq	Yes	
IP Security Policies on				·
	l			

2. Diese Beispielregel enthält zwei Filter: Microsoft-Cisco und Cisco-

to_cis	sco Properties		?)
Rule	es General		
į	Security rules f	or communicating with ot	her computers
<u>I</u> Ρ	Security Rules:		
1	P Filter List	Filter Action	Authentication Tu
	Z Microsoft-Cisco	Permit	Preshared Key 17
	Cisco-Microsoft	Permit	Preshared Key 17
	Oynamic>	Default Response	Preshared Key No
			Þ
	A <u>d</u> d <u>E</u> dit	<u>R</u> emove	Use Add <u>W</u> izard
0			ancel <u>Apply</u>
1			

3. Wählen Sie die Cisco-Microsoft IP-Sicherheitsregel aus, und klicken Sie dann auf **Bearbeiten**, um die IP-Filterlisten anzuzeigen/hinzuzufügen/zu

Edit Rule Properties	? ×
Authentication Methods Tu IP Filter List	nnel Setting Connection Type Filter Action
The selected IP filter lis secured with this rule.	t specifies which network traffic will be
IP Filter Lists:	
Name	Description
O All ICMP Traffic	Matches all ICMP packets betw
O All IP Traffic	Matches all IP packets from this
 Cisco-Microsoft Microsoft-Cisco 	
Add Edit	Remove
0	K Cancel Apply

bearbeiten.

4. Die Registerkarte **Allgemein > Erweitert** der Regel hat die **IKE-Lebensdauer** (480 Minuten = 28.800

to	_cisco Properties	? ×
	Rules General	
	Key Exchange Settings	Ă∥
	Master key Perfect Forward Secrecy	
	Authenticate and generate a new key after every:	
	480 minutes	
	Authenticate and generate a new key after every:	
	0 session(s)	
	Protect identities with these security methods:	
	Methods	
	Internet Key Exchange (IKE) for Windows 2000	
	Jointly developed by Microsoft and Cisco Systems, Inc.	
	OK Cancel	
	Advanced	
	OK Cancel Apply	,
Sekunden):		

5. Die Registerkarte Allgemein > Erweitert > Methoden enthält die IKE-Verschlüsselungsmethode (DES), IKE-Hashing (SHA1) und die Diffie-Helman-Gruppe



6. Jeder Filter hat fünf Registerkarten: Authentifizierungsmethoden (vorinstallierte Schlüssel für Internet Key Exchange

ne Kule Fro	Jertites		
	IP Filter List		Filter Action
Authentic	ation Methods	Tunnel Setting	Connection Type
	The authentication between the con authentication m another compute	on method specifies ł nputers. Offer and ac iethods when negotia ar.	how trust is established cept these sting security with
Authenticat	ion Method prefere	nce order:	
Method	C)etails	Add
Preshared	Key c	bisco123	Edit
			Remove
			Move up
			Move down
			ancel I Anniu

Authentication Methods Tunnel Setting Connection Type Image: Authentication Methods Tunnel Setting Connection Type Image: This rule only applies to network traffic over connections of the selected type. Image: Connections of the selected type. Image: All network connections Image: Connections Image: Local area network (LAN) Image: Connections Image: Remote access Image: Connection System Connections		IP Filter List		Filter Actio	n
 All network connections Local area network (LAN) Remote access 	Authentic	ation Methods	Tunnel Setting	; Conn	ection Type
 All network connections Local area network (LAN) Remote access 		This rule only app the selected type.	lies to network tra	affic over conr	ections of
 Local area network (LAN) Remote access 	C All net	work connections			
C Remote access	• Local a	area network (LAN)			
	C Remot	e access			

n

A 10 10		T 10			··
Authentica	tion Methods P Filter List	l unnel S	etting	Filter Action	tion Type
\times	The selected filte for secure netwo	er action spe rk traffic, and	cifies whe d how it w	ther this rule ill secure the	negotiates traffic.
Filter Action:	s:				
Name		Des	cription		
O IPSec t	unnel				
O Permit		Perr	mit unsecu	ured IP pack	ets to
O Reques	t Security (Option	al) Acc	epts unse:	cured comm	unicat
C Require	security	Acc	epts unse	cured comm	unicat
Add	Edit	Re	move	🗖 Use Ad	dd Wizard
			1	1	

Sie Filteraktion > IPSec-Tunnel > Bearbeiten > Bearbeiten, und klicken Sie auf Benutzerdefiniert:

Modify Security Method	? ×
Security Method	
 High (ESP) Data will be encrypted, authentic and unmodified 	
 Medium (AH) Data will be authentic and unmodified, but will not be encrypted 	
 Custom (for expert users) Settings 	
OK Cancel Apply	

auf

Einstellungen - IPSec transformiert und IPSec-

Custom Security Method Settings	? ×
Specify the settings for this custom set	curity method.
Data and address integrity without Integrity algorithm:	encryption (AH) :
MD5 💌	
 Data integrity and encryption (ESP Integrity algorithm: MD5 	'):
Encryption algorithm:	
Session Key Settings:	
🔲 Generate a new key every:	🔽 Generate a new key every
100000 Kbytes	3600 seconds
	OK Cancel
	OK Cancel

Lebensdauer

Filterliste - Zu verschlüsselnde Quell- und Zielnetzwerke: Für Cisco-

Microsoft:

23 IP Filter I	List						?)
	An IP filter list is composed addresses and protocol	ed of multiple filters. In s can be combined into	this way multiple subnet one IP filter.	s, IP			
Name:							
Cisco-Mici	flosoft						
Description	ε						Add
			A				Edi
			v				Remove
Filters:			_			V (Jse Add Wizard
Mirrored	Description	Protocol	Source Port	Destination Port	Source DNS Name	Source Address	Source Ma
Yes		ANY	ANY	ANY	<a ip="" specific="" sub<="" td=""><td>192.168.1.0</td><td>255.255.25</td>	192.168.1.0	255.255.25
•							F
							Canad
						70	

Für Microsoft-Cisco:

ist					? >
n IP filter list is com ddresses and proto	nposed of multiple filte ocols can be combine	rs. In this way multiple su d into one IP filter.	bnets, IP		
ŭsco					
:					Add
		*			Edit
		_			Remove
				ᆔ	Use Add Wizard
Description	Protocol	Source Port	Destination Port	Source DNS Name	Source Address
	ANY	ANY	ANY	<a ip="" specific="" sub<="" td=""><td>10.32.50.0</td>	10.32.50.0
					•
	ist n IP filter list is con ddresses and proto isco	st n IP filter list is composed of multiple filte ddresses and protocols can be combine isco Description Protocol ANY	st n IP filter list is composed of multiple filters. In this way multiple su ddresses and protocols can be combined into one IP filter. isco isco Description Protocol Source Port ANY ANY	st n IP filter list is composed of multiple filters. In this way multiple subnets, IP ddresses and protocols can be combined into one IP filter. isco Description Protocol Source Port Destination Port ANY ANY ANY	st n IP filter list is composed of multiple filters. In this way multiple subnets, IP ddresses and protocols can be combined into one IP filter. isco Description Protocol Source Port Destination Port Source DNS Name ANY ANY ANY <a ip="" specific="" sub<="" td="">

Tunneleinstellung - Verschlüsselungs-Peers: Für Cisco-

Für

	Edit Rule Properties		? ×
	IP Filter List Authentication Methods	Tunnel Setting	Filter Action
	The tunnel en IP traffic destir List. It takes tw	e tunnel endpoint is the tunneling computer closest to the traffic destination, as specified by the associated IP Filter t. It takes two rules to describe an IPSec Tunnel.	
	 This rule does not specify an IPSec tunnel. The tunnel endpoint is specified by this IP Address: 172.18.124.35 		
Microsoft-Cisco [.]		OK Ca	ancel Apply

Konfigurieren der Cisco Geräte

Konfigurieren Sie die Cisco Router-, PIX- und VPN-Konzentratoren wie in den folgenden Beispielen gezeigt.

- <u>Cisco Router 3640</u>
- <u>PIX</u>
- <u>VPN 3000-Konzentrator</u>
- <u>VPN 5000 Concentrator</u>

Konfigurieren des Cisco 3640 Routers

Cisco Router 3640

```
Current configuration : 1840 bytes
```

```
!
version 12.1
no service single-slot-reload-enable
```

```
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
1
hostname moss
!
logging rate-limit console 10 except errors
!
ip subnet-zero
no ip finger
ip audit notify log
ip audit po max-events 100
crypto isakmp policy 1
!--- The following are IOS defaults so they do not
appear: !--- IKE encryption method encryption des !---
IKE hashing hash sha !--- Diffie-Hellman group group 1
!--- Authentication method authentication pre-share
!--- IKE lifetime lifetime 28800
!--- encryption peer crypto isakmp key cisco123 address
172.18.124.157
!--- The following is the IOS default so it does not
appear: !--- IPSec lifetime crypto ipsec security-
association lifetime seconds 3600 ! !--- IPSec
transforms crypto ipsec transform-set rtpset esp-des
esp-md5-hmac
crypto map rtp 1 ipsec-isakmp
!--- Encryption peer set peer 172.18.124.157
set transform-set rtpset
!--- Source/Destination networks defined match address
115
!
call rsvp-sync
interface Ethernet0/0
ip address 192.168.1.1 255.255.255.0
ip nat inside
half-duplex
interface Ethernet0/1
ip address 172.18.124.35 255.255.255.240
ip nat outside
half-duplex
crypto map rtp
1
ip nat pool INTERNET 172.18.124.35 172.18.124.35 netmask
255.255.255.240
ip nat inside source route-map nonat pool INTERNET
ip classless
ip route 0.0.0.0 0.0.0.0 172.18.124.36
no ip http server
1
access-list 101 deny ip 192.168.1.0 0.0.0.255 10.32.50.0
0.0.255
access-list 101 permit ip 192.168.1.0 0.0.0.255 any
!--- Source/Destination networks defined access-list 115
permit ip 192.168.1.0 0.0.0.255 10.32.50.0 0.0.0.255
access-list 115 deny ip 192.168.1.0 0.0.0.255 any
route-map nonat permit 10
match ip address 101
```

```
!
line con 0
transport input none
line 65 94
line aux 0
line vty 0 4
!
end
```

Konfigurieren von PIX

PIX			
PIX Version 5.2(1)			
nameif ethernet0 outside security0			
nameif ethernet1 inside security100			
enable password 8Rv2YiIvt7RRXU24 encrypted			
passwd 2KFOnbNIdI.2KYOU encrypted			
hostname pixfirewall			
fixup protocol ftp 21			
fixup protocol http 80			
fixup protocol h323 1720			
fixup protocol rsh 514			
fixup protocol smtp 25			
fixup protocol sqlnet 1521			
fixup protocol sip 5060			
names			
<pre>! Source/Destination networks defined access-list 115</pre>			
permit ip 192.168.1.0 255.255.255.0 10.32.50.0			
255.255.255.0			
access-list 115 deny ip 192.168.1.0 255.255.255.0 any			
pager lines 24			
logging on			
no logging timestamp			
no logging standby			
no logging console			
no logging monitor			
no logging buffered			
no logging trap			
no logging history			
logging facility 20			
logging queue 512			
interface ethernet0 auto			
interface ethernet1 10baset			
mtu outside 1500			
mtu inside 1500			
ip address outside 172.18.124.35 255.255.255.240			
ip address inside 192.168.1.1 255.255.255.0			
ip audit info action alarm			
ip audit attack action alarm			
no failover			
Tallover timeout 0:00:00			
Tallover poll 15			
Lallover ip address outside U.U.U.U			
Lallover 1p address inside U.U.U.U			
arp timeout 14400			
Except Source/Destination from Network Address			
Translation (NAT): nat (inside) 0 access-list 115			
timeout vlate 3:00:00			
timeout conn 1:00:00 half-closed 0:10:00 udn 0:02:00 rng			
cimeout comi 1.00.00 maii-ciosed 0.10.00 uap 0.02.00 rpc			

0:10:00 h323 0:05:00 sip 0:30:00 sip_media 0:02:00 timeout uauth 0:05:00 absolute aaa-server TACACS+ protocol tacacs+ aaa-server RADIUS protocol radius no snmp-server location no snmp-server contact snmp-server community public no snmp-server enable traps floodguard enable sysopt connection permit-ipsec no sysopt route dnat !--- IPSec transforms crypto ipsec transform-set myset esp-des esp-md5-hmac !--- IPSec lifetime crypto ipsec security-association lifetime seconds 3600 crypto map rtpmap 10 ipsec-isakmp !--- Source/Destination networks crypto map rtpmap 10 match address 115 !--- Encryption peer crypto map rtpmap 10 set peer 172.18.124.157 crypto map rtpmap 10 set transform-set myset crypto map rtpmap interface outside isakmp enable outside !--- Encryption peer isakmp key ******* address 172.18.124.157 netmask 255.255.255.240 isakmp identity address !--- Authentication method isakmp policy 10 authentication pre-share !--- IKE encryption method isakmp policy 10 encryption des !--- IKE hashing isakmp policy 10 hash sha !--- Diffie-Hellman group isakmp policy 10 group 1 !--- IKE lifetime isakmp policy 10 lifetime 28800 telnet timeout 5 ssh timeout 5 terminal width 80 Cryptochecksum:c237ed11307abea7b530bbd0c2b2ec08 : end

Konfigurieren des VPN 3000-Konzentrators

Verwenden Sie die Menüoptionen und Parameter unten, um den VPN Concentrator nach Bedarf zu konfigurieren.

Um ein IKE-Angebot hinzuzufügen, wählen Sie Configuration > System > Tunneling Protocols
 IPSec > IKE Proposals > Add a Proposal (Konfiguration > System > Tunneling-Protokolle > IPSec > IKE-Vorschläge) aus.

```
Proposal Name = DES-SHA

!--- Authentication method Authentication Mode = Preshared Keys !--- IKE hashing

Authentication Algorithm = SHA/HMAC-160 !--- IKE encryption method Encryption Algorithm =

DES-56 !--- Diffie-Hellman group Diffie Hellman Group = Group 1 (768-bits) Lifetime

Measurement = Time Date Lifetime = 10000 !--- IKE lifetime Time Lifetime = 28800
```

 Um den LAN-to-LAN-Tunnel zu definieren, wählen Sie Configuration > System > Tunneling Protocols > IPSec LAN-to-LAN aus.

```
Name = to_2000
Interface = Ethernet 2 (Public) 172.18.124.35/28
!--- Encryption peer Peer = 172.18.124.157 !--- Authentication method Digital Certs = none
(Use Pre-shared Keys) Pre-shared key = ciscol23 !--- IPSec transforms Authentication =
ESP/MD5/HMAC-128 Encryption = DES-56 !--- Use the IKE proposal IKE Proposal = DES-SHA
```

Autodiscovery = off !--- Source network defined Local Network Network List = Use IP Address/Wildcard-mask below IP Address 192.168.1.0 Wildcard Mask = 0.0.0.255 !---Destination network defined Remote Network Network List = Use IP Address/Wildcard-mask below IP Address 10.32.50.0 Wildcard Mask 0.0.0.255

 Um die Sicherheitszuordnung zu ändern, wählen Sie Configuration > Policy Management > Traffic Management > Security Associations > Modify aus.

SA Name = L2L-to_2000 Inheritance = From Rule IPSec Parameters /--- IPSec transforms Authentication Algorithm = ESP/MD5/HMAC-128 Encryption Algorithm = DES-56 Encapsulation Mode = Tunnel PFS = Disabled Lifetime Measurement = Time Data Lifetime = 10000 /--- IPSec lifetime Time Lifetime = 3600 Ike Parameters /--- Encryption peer IKE Peer = 172.18.124.157 Negotiation Mode = Main /--- Authentication method Digital Certificate = None (Use Preshared Keys) /--- Use the IKE proposal IKE Proposal DES-SHA

Konfigurieren des VPN 500-Konzentrators

VPN 5000 Concentrator [IP Ethernet 1:0] Mode = RoutedSubnetMask = 255.255.255.240IPAddress = 172.18.124.35[General] IPSecGateway = 172.18.124.36DeviceName = "cisco" EthernetAddress = 00:00:a5:f0:c8:00DeviceType = VPN 5002/8 Concentrator ConfiguredOn = Timeserver not configured ConfiguredFrom = Command Line, from Console [IP Ethernet 0:0] Mode = RoutedSubnetMask = 255.255.255.0 IPAddress = 192.168.1.1 [Tunnel Partner VPN 1] *!--- Encryption peer* Partner = 172.18.124.157 *!---*IPSec lifetime KeyLifeSecs = 3600 BindTo = "ethernet 1:0" !--- Authentication method SharedKey = "ciscol23" KeyManage = Auto !--- IPSec transforms Transform = esp(md5,des) Mode = Main !--- Destination network defined Peer = "10.32.50.0/24" !--- Source network defined LocalAccess = "192.168.1.0/24" [IP Static] 10.32.50.0 255.255.255.0 VPN 1 1 [IP VPN 1] Mode = Routed Numbered = Off [IKE Policy] !--- IKE hashing, encryption, Diffie-Hellman group Protection = SHA_DES_G1 Configuration size is 1088 out of 65500 bytes.

<u>Überprüfen</u>

Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

Fehlerbehebung

Dieser Abschnitt enthält Informationen zur Fehlerbehebung in Ihren Konfigurationen.

Befehle zur Fehlerbehebung

Bestimmte **show**-Befehle werden vom <u>Output Interpreter Tool</u> unterstützt (nur <u>registrierte</u> Kunden), mit dem Sie eine Analyse der **show**-Befehlsausgabe anzeigen können.

Hinweis: Bevor Sie Debugbefehle ausgeben, lesen Sie <u>Wichtige Informationen über Debug-</u> Befehle.

Cisco Router 3640

- debug crypto engine Zeigt Debugmeldungen über Krypto Engines, die Verschlüsselung und Entschlüsselung durchführen.
- debug crypto isakmp Zeigt Meldungen über IKE-Ereignisse an.
- debug crypto ipsec Zeigt IPSec-Ereignisse an.
- show crypto isakmp sa Zeigt alle aktuellen IKE-Sicherheitszuordnungen (SAs) in einem Peer an.
- **show crypto ipsec sa** Zeigt die Einstellungen an, die von aktuellen Sicherheitszuordnungen verwendet werden.
- clear crypto isakmp (aus Konfigurationsmodus) Löscht alle aktiven IKE-Verbindungen.
- clear crypto sa (aus dem Konfigurationsmodus) Löscht alle IPSec-Sicherheitszuordnungen.

<u>PIX</u>

- debug crypto ipsec Zeigt die IPSec-Verhandlungen von Phase 2 an.
- debug crypto isakmp Zeigt die Verhandlungen der Internet Security Association und des Key Management Protocol (ISAKMP) über Phase 1.
- debug crypto engine Zeigt den verschlüsselten Datenverkehr an.
- show crypto ipsec sa Zeigt die Sicherheitszuordnungen für Phase 2 an.
- show crypto isakmp sa Zeigt die Sicherheitszuordnungen für Phase 1 an.
- clear crypto isakmp (aus dem Konfigurationsmodus) Löscht die Sicherheitszuordnungen für Internet Key Exchange (IKE).
- clear crypto ipsec sa (aus dem Konfigurationsmodus) Löscht IPSec-Sicherheitszuordnungen.

VPN 3000-Konzentrator

- Starten Sie den VPN 300 Concentrator-Debugging, indem Sie Configuration > System > Events > Classes > Modify auswählen (Severity to Log=1-13, Severity to Console=1-3): IKE, IKEDBG, IKEDECODE, IPSEC, IPSECDBG, IPSECDECODE
- Das Ereignisprotokoll kann gelöscht oder abgerufen werden, indem Sie Monitoring > Event Log (Überwachung > Ereignisprotokoll) auswählen.
- - Der LAN-zu-LAN-Tunnelverkehr kann unter Überwachung > Sitzungen überwacht werden.
- Der Tunnel kann unter Administration > Administration Sessions > LAN-to-LAN Sessions > Actions Logout gelöscht werden.

- 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 die Leitungsnummer des Software-Codes, in dem der Fehler aufgetreten ist.
- show vpn statistics Zeigt die folgenden Informationen f
 ür Benutzer, Partner und die Gesamtsumme f
 ür beide an. (Bei modularen Modellen umfasst die Anzeige einen Abschnitt f
 ür jeden Modulsteckplatz.) Current Active - Die aktuell aktiven Verbindungen. In Negot - Die derzeit verhandelnden Verbindungen. High Water - Die h
 öchste Anzahl gleichzeitiger aktiver Verbindungen seit dem letzten Neustart. Running Total (Gesamt ausf
 ühren) - Die Gesamtzahl erfolgreicher Verbindungen seit dem letzten Neustart. Tunnel Starts (Tunnel wird gestartet) -Die Anzahl der Tunnelstarts. Tunnel OK - Die Anzahl der Tunnel, f
 ür die keine Fehler aufgetreten sind. Tunnel Error (Tunnelfehler): Die Anzahl der Tunnel mit Fehlern.
- **show vpn statistics ausführliche** Zeigt Statistiken zur ISAKMP-Aushandlung und viele weitere aktive Verbindungsstatistiken an.

Zugehörige Informationen

- <u>Cisco VPN Concentrators der Serie 5000 Ankündigung des Vertriebsendes</u>
- Konfigurieren der IPSec-Netzwerksicherheit
- Konfigurieren des Internet Key Exchange Security Protocol
- <u>Technischer Support Cisco Systems</u>