# Configurazione di IPSec tra un server Microsoft Windows 2000 e un dispositivo Cisco

## Sommario

Introduzione Operazioni preliminari Convenzioni Prerequisiti Componenti usati Esempio di rete Configurazione di Microsoft Windows 2000 Server per l'utilizzo con i dispositivi Cisco Attività eseguite Istruzioni dettagliate Configurazione dei dispositivi Cisco Configurazione del router Cisco 3640 Configurazione di PIX Configurazione di VPN 3000 Concentrator Configurazione di VPN 5000 Concentrator Verifica Risoluzione dei problemi Comandi per la risoluzione dei problemi Informazioni correlate

## **Introduzione**

In questo documento viene illustrato come formare un tunnel IPSec con chiavi già condivise per collegarsi a 2 reti private: una rete privata (192.168.I.X) all'interno di un dispositivo Cisco e una rete privata (10.32.50.X) all'interno di Microsoft 2000 Server. Si presume che il traffico tra il dispositivo Cisco e l'interno del server 2000 e Internet (rappresentato qui dalle reti 172.18.124.X) scorra prima di iniziare questa configurazione.

Per informazioni dettagliate sulla configurazione del server di Microsoft Windows 2000, visitare il sito Web Microsoft: <u>http://support.microsoft.com/support/kb/articles/Q252/7/35.ASP</u>

## Operazioni preliminari

### **Convenzioni**

Per ulteriori informazioni sulle convenzioni usate, consultare il documento <u>Cisco sulle convenzioni</u> <u>nei suggerimenti tecnici</u>.

### **Prerequisiti**

Non sono previsti prerequisiti specifici per questo documento.

### Componenti usati

Queste configurazioni sono state sviluppate e testate utilizzando le versioni software e hardware riportate di seguito.

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

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

### Esempio di rete

Questo documento utilizza le impostazioni di rete mostrate nel diagramma sottostante.



## <u>Configurazione di Microsoft Windows 2000 Server per l'utilizzo</u> <u>con i dispositivi Cisco</u>

### Attività eseguite

Il diagramma mostra le attività eseguite nella configurazione del server di Microsoft Windows 2000:



### Istruzioni dettagliate

Dopo aver seguito le <u>istruzioni</u> di configurazione sul sito Web Microsoft, eseguire la procedura seguente per verificare che la configurazione funzioni con i dispositivi Cisco. I commenti e le modifiche vengono annotati con le immagini acquisite.

 Fare clic su Start > Esegui > secpol.msc in Microsoft Windows 2000 Server e verificare le informazioni nelle schermate seguenti.Dopo aver utilizzato le istruzioni sul sito Web Microsoft per configurare un server 2000, sono state visualizzate le seguenti informazioni sul tunnel.Nota: la regola di esempio è chiamata "to\_cisco".

📑 Local Security Settings				_ 🗆 ×
Action ⊻iew ← →	🗈 🔟 🗙 🗗 🗔	😤 ] 🛍 🏦 🗍 🖺 🚨		
Tree	Name 🔺	Description	Policy Assigned	
Security Settings	Client (Respond Only) Secure Server (Requir Server (Request Secu to_cisco	Communicate normally (uns For all IP traffic, always req For all IP traffic, always req	No No No Yes	
	-			

2. Questa regola di esempio contiene due filtri: Microsoft-Cisco e Cisco-

to_cis	sco Properties		?
Rule	es General		
ų	Security rule:	s for communicating with o	ther computers
ĪP	Security Rules:		
	P Filter List	Filter Action	Authentication Tu
	Z Microsoft-Cisco	Permit	Preshared Key 17
	Cisco-Microsoft	Permit	Preshared Key 17
	<pre>&gt;</pre>	Default Response	Preshared Key No
•			Þ
	A <u>d</u> d <u>E</u>	dit <u>R</u> emove	Use Add Wizard
		Close	Cancel <u>A</u> pply

3. Selezionare la regola di sicurezza IP Cisco-Microsoft, quindi fare clic su **Modifica** per visualizzare/aggiungere/modificare gli elenchi filtri

Authentication Methods	Tunnel Setting Connection Type
IP Filter List	Filter Action
The selected If secured with the	P filter list specifies which network traffic will be his rule.
IP Filter Lists:	
Name	Description
O All ICMP Traffic	Matches all ICMP packets betw
O All IP Traffic	Matches all IP packets from this
	I Demons I

to_cisco Properties ?×
Rules General
Key Exchange Settings
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 Kan Eucleanes (IKE) (as ) (in dama 2000
Jointly developed by Microsoft and Cisco Systems, Inc.
Advanced
OK Cancel Apply
secondi):

5. La scheda Generale > Avanzate > Metodi della regola contiene il metodo di crittografia IKE (DES), l'hashing IKE (SHA1) e il gruppo Diffie-Helman

IncryptionIntegrityDiffie-HellmanDESSHA1Low (1)DESSHA1Low (1)DESMD5Medium (2)DESMD5Low (1)	644
DES SHA1 Low (1) DES SHA1 Low (1) BDES MD5 Medium (2) DES MD5 Low (1)	Aug
DES SHA1 Low (1) BDES MD5 Medium (2)	
DES MDS Medium (2)	Edit
	Remov
	Move u
	Move do

(Low(1)):
6. Ogni filtro dispone di 5 schede: Metodi di autenticazione (chiavi già condivise per IKE [Internet Key

IF	P Filter List	Filter Acti	on
Authenticat	ion Methods Tunne	l Setting Conr	nection Type
	The authentication method between the computers. O authentication methods wh another computer.	d specifies how trust is ffer and accept these nen negotiating securi	established ty with
Authenticatio	n Method preference order	:	
Method	Details		Add
Preshared N	ey cisco123		Edit
			Remove
			Move up
			Move down
	OK	Connect	0 b.

dit Rule Properties		? ×
IP Filter List	Tunnel Setting	Filter Action
This rule only ap the selected type	plies to network tra	affic over connections of
C All network connections		
<ul> <li>Local area network (LAN)</li> </ul>		
C Hemote access		
	ОК	Cancel Apply

IP Filter List The selected filter a for secure network	Filter Action action specifies whether this rule negotiates traffic, and how it will secure the traffic.
The selected filter a for secure network	action specifies whether this rule negotiates . traffic, and how it will secure the traffic.
Filter Actions:	
Filer Actions.	
Name	Description
O IPSec tunnel	
O Permit	Permit unsecured IP packets to
O Request Security (Optional)	Accepts unsecured communicat
C Require Security	Accepts unsecured communicat
Add Edit	Remove Use Add Wizard

are Operazione filtro > Tunnel IPSec > Modifica > Modifica, quindi fare clic su

	Modify Security Method
	Security Method
	<ul> <li>High (ESP)</li> <li>Data will be encrypted, authentic and unmodified</li> </ul>
	Medium (AH) Data will be authentic and unmodified, but will not be encrypted
	Custom (for expert users) Settings
	OK Cancel Apply
ato:	

are clic su Impostazioni - Trasformazioni IPSec e Durata

ustom Security Method Settings	? ×
Specify the settings for this custom secu	rity method.
Data and address integrity without en Integrity algorithm:	ncryption (AH) :
MD5 💌	
<ul> <li>Data integrity and encryption (ESP):</li> <li>Integrity algorithm:</li> <li>MD5</li> </ul>	
Encryption algorithm: DES	
- Session Key Settings:	
Generate a new key every: 100000 Kbytes	Generate a new key every 3600 seconds
	OK Cancel

- reti di origine e destinazione da crittografare:Per Cisco-

#### Microsoft:

🕄 IP Filter l	list						?
	An IP filter list is composed addresses and protocols	ed of multiple filters. In can be combined into	this way multiple subnet one IP filter.	s, IP			
Name:							
Cisco-Micr	rosoft						
Description	r						Add
			A				Edit
			<b>T</b>				Remove
Filters:			_				Use 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></a>	192.168.1.0	255.255.25
•							Þ
						04	Carred
						- 10	Lancel



Cisco:

IP Filter I	List					? ×
	An IP filter list is comp addresses and protoc	osed of multiple filters. Ir ols can be combined int	n this way multiple subne o one IP filter.	ts, IP		
Name:						
Microsoft-	Cisco					
, Description	r.					Add
			*			Edit
			<b>•</b>			Remove
Filters:					<b>T</b>	Use Add Wizard
Mirrored	Description	Protocol	Source Port	Destination Port	Source DNS Name	Source Address
Yes		ANY	ANY	ANY	<a ip="" specific="" sub<="" td=""><td>10.32.50.0</td></a>	10.32.50.0
•						Þ
					OK	Cancel

Impostazione tunnel - peer crittografia:Per Cisco-

<ul> <li>IP Filter List</li> <li>Authentication Methods</li> <li>Tunnel Setting</li> <li>Connection Type</li> <li>The tunnel endpoint is the tunneling computer closest to the IP traffic destination, as specified by the associated IP Filter List. It takes two rules to describe an IPSec Tunnel.</li> <li>This rule does not specify an IPSec tunnel.</li> <li>The tunnel endpoint is specified by this IP Address:</li> <li>172.18.124.157</li> </ul>	<ul> <li>IP Filter List Filter Action</li> <li>Authentication Methods Tunnel Setting Connection Type</li> <li>The tunnel endpoint is the tunneling computer closest to the IP traffic destination, as specified by the associated IP Filter List. It takes two rules to describe an IPSec Tunnel.</li> <li>This rule does not specify an IPSec tunnel.</li> <li>The tunnel endpoint is specified by this IP Address:</li> <li>172.18.124.157</li> </ul>	Edi	t Rule Pr	operties		
<ul> <li>The tunnel endpoint is the tunneling computer closest to the IP traffic destination, as specified by the associated IP Filter List. It takes two rules to describe an IPSec Tunnel.</li> <li>This rule does not specify an IPSec tunnel.</li> <li>The tunnel endpoint is specified by this IP Address:</li> <li>172.18.124.157</li> </ul>	<ul> <li>The tunnel endpoint is the tunneling computer closest to the IP traffic destination, as specified by the associated IP Filter List. It takes two rules to describe an IPSec Tunnel.</li> <li>This rule does not specify an IPSec tunnel.</li> <li>The tunnel endpoint is specified by this IP Address:</li> <li>172.18.124.157</li> </ul>	à	Authent	IP Filter List ication Methods	) Tunnel Setting	Filter Action
<ul> <li>This rule does not specify an IPSec tunnel.</li> <li>The tunnel endpoint is specified by this IP Address:</li> <li>172.18.124.157</li> </ul>	<ul> <li>This rule does not specify an IPSec tunnel.</li> <li>The tunnel endpoint is specified by this IP Address:</li> <li>172.18.124.157</li> </ul>			The tunnel endp IP traffic destina List. It takes two	point is the tunneling tion, as specified by rules to describe a	g computer closest to th y the associated IP Filte an IPSec Tunnel.
172.18.124.157	172.18.124.157		C This r	ule does not specify	an IPSec tunnel.	lden av
			• The ti	unnel endpoint is sp 72 . 18 . 124 .	ecified by this IP Ad 157	ldress:
		_				

Edit Rule Pro	operties				?	x
Authenti	IP Filter List cation Methods	 Tunnel Sel	Filt tting	ter Actio Conne	n ection Type	
	The tunnel end IP traffic destin List. It takes tw	point is the tunn ation, as specific o rules to descri	heling comp ed by the a be an IPS(	puter clo associati ec Tunn	osest to the ed IP Filter hel.	
⊂ This n ⊙ The tu 17	ule does not specify unnel endpoint is sp 2 . 18 .124 .	y an IPSec tunn becified by this If	el. P Address:			
,						
				. 1		
		UK	Land	ser	Арріу	

#### Microsoft-Cisco:

## Configurazione dei dispositivi Cisco

Configurare i Cisco router, PIX e VPN concentrator come mostrato negli esempi seguenti.

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

### Configurazione del router Cisco 3640

#### Cisco 3640 Router

```
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
hostname moss
!
logging rate-limit console 10 except errors
ip subnet-zero
!
no ip finger
1
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
1
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
0.0.0.255
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
```

## Configurazione di 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 salnet 1521
fixup protocol sip 5060
names
Source/Destination networks defined access-list 115
permit in 192.168.1.0 255.255 255 0 10 32 50 0
access-list 115 denv in 192 168 1 0 255 255 255 0 anv
nager lines 24
logging on
no logging timogtamp
no logging standby
no logging scalaby
no logging console
no logging huffored
no logging bullered
no logging trap
logging history
logging facility 20
interface athermatic sub-
interface ethernett auto
interiace etherneti lubaset
mtu outside 1500
mtu inside 1500
1p address outside 172.18.124.35 255.255.255.240
1p address inside 192.168.1.1 255.255.255.0
ip audit into action alarm
ip audit attack action alarm
no fallover
failover timeout 0:00:00
Tallover poll 15
Tallover ip address outside U.U.U.U
Tallover ip address inside U.U.U.U
arp timeout 14400
! Except Source/Destination from Network Address
Translation (NAT): nat (inside) 0 access-list 115
route outside 0.0.0.0 0.0.0.0 172.18.124.36 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 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

#### Configurazione di VPN 3000 Concentrator

Utilizzare le opzioni di menu e i parametri mostrati di seguito per configurare VPN Concentrator in base alle esigenze.

 Per aggiungere una proposta IKE, selezionare Configurazione > Sistema > Protocolli di tunneling > IPSec > Proposte IKE > Aggiungi proposta.

```
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
```

 Per definire il tunnel da LAN a LAN, selezionare Configurazione > Sistema > Protocolli di tunneling > IPSec da LAN a LAN.

```
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

 Per modificare l'associazione di protezione, selezionare Configurazione > Gestione criteri > Gestione traffico > Associazioni di protezione > Modifica.

```
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
```

### Configurazione di VPN 5000 Concentrator

#### VPN 5000 Concentrator

```
[ IP Ethernet 1:0 ]
Mode = Routed
SubnetMask = 255.255.255.240
IPAddress = 172.18.124.35
[ General ]
IPSecGateway = 172.18.124.36
DeviceName = "cisco"
EthernetAddress = 00:00:a5:f0:c8:00
DeviceType = VPN 5002/8 Concentrator
ConfiguredOn = Timeserver not configured
ConfiguredFrom = Command Line, from Console
[ IP Ethernet 0:0 ]
Mode = Routed
SubnetMask = 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.
```

## **Verifica**

Attualmente non è disponibile una procedura di verifica per questa configurazione.

## Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alle configurazioni.

### Comandi per la risoluzione dei problemi

Alcuni comandi **show sono supportati dallo** <u>strumento Output Interpreter (solo utenti registrati); lo</u> <u>strumento permette di visualizzare un'analisi dell'output del comando</u> **show.** 

**Nota:** prima di usare i comandi di **debug**, consultare le <u>informazioni importanti sui comandi di</u> <u>debug</u>.

#### Cisco 3640 Router

- debug crypto engine: visualizza i messaggi di debug sui motori di crittografia, che eseguono la crittografia e la decrittografia.
- debug crypto isakmp: visualizza i messaggi relativi agli eventi IKE.
- debug crypto ipsec Visualizza gli eventi IPSec.
- show crypto isakmp sa: visualizza tutte le associazioni di sicurezza IKE correnti in un peer.
- **show crypto ipsec sa**: visualizza le impostazioni utilizzate dalle associazioni di sicurezza correnti.
- clear crypto isakmp (dalla modalità di configurazione) Cancella tutte le connessioni IKE attive.
- clear crypto sa (dalla modalità di configurazione) Elimina tutte le associazioni di protezione IPSec.

#### <u>PIX</u>

- debug crypto ipsec: visualizza le negoziazioni IPSec della fase 2.
- **debug crypto isakmp**: visualizza le negoziazioni ISAKMP (Internet Security Association and Key Management Protocol) della fase 1.
- debug crypto engine: visualizza il traffico crittografato.
- show crypto ipsec sa: visualizza le associazioni di sicurezza della fase 2.
- show crypto isakmp sa: visualizza le associazioni di sicurezza della fase 1.
- clear crypto isakmp (dalla modalità di configurazione) Cancella le associazioni di protezione IKE (Internet Key Exchange).
- clear crypto ipsec sa (dalla modalità di configurazione) Cancella le associazioni di protezione IPSec.

#### VPN 3000 Concentrator

- Avviare il debug di VPN 3000 Concentrator selezionando Configurazione > Sistema > Eventi > Classi > Modifica (gravità da registro=1-13, gravità da console=1-3): IKE, IKEDBG, IKEDECODE, IPSEC, IPSECDBG, IPSECDECODE
- Il registro eventi può essere cancellato o recuperato selezionando Monitoraggio > Registro eventi.
- - Il traffico del tunnel LAN-LAN può essere monitorato in Monitoraggio > Sessioni.
- Il tunnel può essere cancellato in Amministrazione > Amministra sessioni > Sessioni LAN-to-LAN > Azioni - Disconnessione.

- vpn trace dump all: visualizza le informazioni su tutte le connessioni VPN corrispondenti, incluse le informazioni sull'ora, il numero VPN, l'indirizzo IP reale del peer, gli script eseguiti e, in caso di errore, la routine e il numero di riga del codice software in cui si è verificato l'errore.
- show vpn statistics: visualizza le informazioni seguenti per Users, Partners e il totale per entrambi. Per i modelli modulari, il display include una sezione per ogni slot del modulo. Corrente attiva - Le connessioni attive correnti. In Negot - Connessioni attualmente in fase di negoziazione. High Water - Numero massimo di connessioni attive simultanee dall'ultimo riavvio. Totale in esecuzione: il numero totale di connessioni riuscite dall'ultimo riavvio. Avvio del tunnel: numero di avvii del tunnel. Tunnel OK: il numero di tunnel per i quali non sono stati rilevati errori. Errore tunnel: numero di tunnel con errori.
- **show vpn statistics verbose**: visualizza le statistiche di negoziazione ISAKMP e molte altre statistiche di connessione attive.

## Informazioni correlate

- <u>Cisco VPN serie 5000 concentrator: annuncio di fine vendita</u>
- <u>Configurazione di IPSec Network Security</u>
- Configurazione del protocollo di protezione di Internet Key Exchange
- <u>Supporto tecnico Cisco Systems</u>