Tunnel IPsec dinamico tra un'ASA con indirizzo statico e un router Cisco IOS con indirizzo dinamico che utilizza un esempio di configurazione CCP

Sommario

Introduzione Prerequisiti Requisiti Componenti usati Convenzioni Premesse Configurazione Esempio di rete Configurazioni Verifica Verifica Verifica dei parametri del tunnel tramite CCP Verifica dello stato del tunnel tramite la CLI di ASA Verificare i parametri del tunnel tramite la CLI del router Risoluzione dei problemi Informazioni correlate

Introduzione

In questo documento viene fornita una configurazione di esempio per abilitare le appliance di sicurezza PIX/ASA ad accettare le connessioni IPsec dinamiche dal router Cisco IOS[®]. In questo scenario, il tunnel IPsec viene stabilito quando il tunnel viene avviato solo dall'estremità del router. ASA: impossibile avviare un tunnel VPN a causa della configurazione IPsec dinamica.

Questa configurazione consente a PIX Security Appliance di creare un tunnel LAN-to-LAN (L2L) IPsec dinamico con un router VPN remoto. Il router riceve dinamicamente il proprio indirizzo IP pubblico esterno dal provider di servizi Internet. Il protocollo DHCP (Dynamic Host Configuration Protocol) fornisce questo meccanismo per allocare dinamicamente gli indirizzi IP dal provider. Questo consente di riutilizzare gli indirizzi IP quando gli host non ne hanno più bisogno.

La configurazione sul router viene effettuata con il software <u>Cisco Configuration Professional</u> (CCP). CCP è uno strumento di gestione dei dispositivi basato su GUI che consente di configurare i router basati su Cisco IOS. Per ulteriori informazioni su come configurare un router con CCP, fare riferimento a <u>Configurazione base del router con Cisco Configuration Professional</u>.

Per ulteriori informazioni e esempi di configurazione sulla creazione del tunnel IPsec che usa router ASA e Cisco IOS, fare riferimento a <u>VPN da sito a sito (L2L)</u> con ASA.

Per ulteriori informazioni e un esempio di configurazione della creazione di tunnel IPSec dinamici con l'uso di PIX e di un router Cisco IOS, fare riferimento a <u>VPN da sito a sito (L2L)</u> con IOS.

Prerequisiti

<u>Requisiti</u>

Prima di provare la configurazione, verificare che l'ASA e il router dispongano di connettività Internet per stabilire il tunnel IPSEC.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco IOS Router 1812 con software Cisco IOS versione 12.4
- Software Cisco ASA 5510 release 8.0.3

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.

Convenzioni

Fare riferimento a <u>Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni</u> <u>dei documenti.</u>

Premesse

In questo scenario, la rete 192.168.100.0 è dietro l'ASA e la rete 192.168.200.0 è dietro il router Cisco IOS. Si presume che il router ottenga il proprio indirizzo pubblico tramite DHCP dal proprio ISP. Poiché questo pone un problema nella configurazione di un peer statico sull'estremità ASA, è necessario adottare una configurazione crittografica dinamica per stabilire un tunnel tra il sito e il router Cisco IOS.

Gli utenti Internet sull'estremità ASA vengono tradotti nell'indirizzo IP dell'interfaccia esterna. Si presume che NAT non sia configurato sull'estremità del router Cisco IOS.

Di seguito sono riportati i passaggi principali da configurare sull'estremità ASA per stabilire un tunnel dinamico:

- 1. Configurazione relativa a ISAKMP fase 1
- 2. Configurazione esenzione NAT
- 3. Configurazione mappa crittografica dinamica

Sul router Cisco IOS è configurata una mappa crittografica statica perché si presume che l'ASA abbia un indirizzo IP pubblico statico. Di seguito vengono elencati i passaggi principali da

configurare sull'estremità del router Cisco IOS per stabilire un tunnel IPSEC dinamico.

- 1. Configurazione relativa a ISAKMP fase 1
- 2. Configurazione correlata alla mappa crittografica statica

Questi passaggi sono descritti in dettaglio in queste configurazioni.

Configurazione

In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

Nota: per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo <u>strumento di</u> ricerca dei comandi (solo utenti registrati).

Esempio di rete

Nel documento viene usata questa impostazione di rete:



Configurazioni

Questa è la configurazione della VPN IPsec sul router VPN con CCP. Attenersi alla seguente procedura:

 Aprire l'applicazione CCP e scegliere Configura > Sicurezza > VPN > VPN da sito a sito. Fare clic su Avvia la scheda selezionata.



2. Scegliere Procedura guidata dettagliata e quindi fare clic su



3. Immettere l'indirizzo IP peer remoto insieme ai dettagli di autenticazione.

Site-to-Site VPN Wiza	rd	× * * * * * * * * * * * * * * * * * * *
VPN Wizard	VPN Connection Information Select the interface for this VPN connection:	FastEthemet1 😿 Details
	Peer Identity Select the type of peer(s) used for this VP connection: Briter the IP address of the renote peer.	N Peer with static P address 💉
	Authentication Authentication ensures that each end of th key.	e VPN connection uses the same secret
KA	Pre-shared Keys pre-shared keys Re-enter Key:	C Digital Certificates
		< Back Next > Firmsh Cancel Help

4. Scegliere le proposte IKE e fare clic su

VPN Wizard	IKE Proposals					
THE THEORY	IKE proposals	specify the er	cryption algo	withm, authentical	tion algorithm an	d ixey exchange
	method that is	used by this r	outer when n	egotiating a VPN	connection with t	the remote
	device should I	be configured	with at least	one of the policie	rs listed below.	e remote.
$\sim \wedge$	a survey mana					
	Click the Add.	button to ad	d more polici	es and the Edit	button to edit an o	existing policy
	Evicette	Eccention	Mach	DHOme	Authoritication	Turio
A	enong	3DES	SHA 1	aroun?	PRE SHARE	Cisco CP Def
		DES	MD5	group2	PRE SHARE	User Defined
Re			1			
Re	Add.	Edit.				
R	Add.	Edit				
	Add.	Edit.				
	Add_	Edit				

5. Definite i dettagli del set di trasformazioni e fate clic su Avanti

Site-to-Site VPN Wiza	rd					
VPN Wizard	A transform A transform data in the communit one select Click the <i>i</i> transform Select Tr	m Set m set specifie e VPN tunnel. icate, the remo ted below. Add button to i set. ansform Set:	s the encryption and aut Since the two devices mu te device must be config add a new transform se	tenscation algo ust use the san ured with the s t and the Edit	rithms used to prote te algorithms to ame transform set ar button to edit the spi	ctilhe silhe acified
	m	set	~			-
	Detail	s of the specif	ied transform set			
		Name	ESP Encryption	ESP Integrity	AH Integrity	
						2
	Ad	id	:dit	Back Next >	First Cancel	Help

(Next).

6. Definire il traffico da crittografare e fare clic su

IPSec rules define the traffic, such as file trans protected by this VPN connection. Other data to device. You can protect all traffic between a pa specify an IPSec rule that defines the traffic typ	fers (FTP) and e-mail (SMTP) that will be affic will be sent unprotected to the remol dicular source and destination subnet, or es to be protected.
Protect all traffic between the following subm	ets
Local Network	Remote Network
Enter the IP address and subnet mask of the network where IPSec traffic originates.	Enter the IP Address and Subnet Mas the destination Network
IP Address:	IP Address:
192 168 200.0	192.168.100.0
Subnet Mask:	Subnet Mask
255.255.255.0 or 24	255.255.255.0 or 24
Create/Select an access-list for IPSec traffic	

7. Verificare il riepilogo della configurazione IPsec di crittografia e fare clic su

Click Finish to deliver the configuration to the router. Image: Click Finish to deliver the configuration to the router. Image: Click Finish to deliver the configuration to the router. Image: Click Finish to deliver the configuration to the router. Image: Click Finish to deliver the configuration to the router. Image: Click Finish to deliver the configuration to the router. Image: Click Finish to deliver the configuration to the router. Image: Click Finish to deliver the configuration to the router. Image: Click Finish to deliver the configuration to the router. Image: Click Finish to deliver the configuration to the router. Image: Click Finish to deliver the configuration to the router. Image: Click Finish to deliver the configuration to the router. Image: Click Finish to deliver the configuration to the router. Image: Click Finish to deliver the configuration to the router. Image: Click Finish to deliver the configuration to the router. Image: Click Finish to deliver the configuration to the router. Image: Click Finish to deliver the configuration to the router. Image: Click Finish to deliver the configuration to the router. Image: Click Finish to deliver the configuration to the router. Image: Click Finish to deliver to the router. Image: Click Finish to deliver to the router.	VPN Wizard	Summary of the	Configuration			
IVE*Shareu ney. IVE Policies: Hash DH Group Authentication Encryption MD5 group2 PRE_SHARE DES SH4_1 group2 PRE_SHARE DES Transform Sets: Name:myset ESP Encryption.ESP_DES ESP Integrity.ESP_MD5_HMAC Mode:TUNNEL IPSec Rule: permit all ip traffic from 192.168.200.0 0.0.0.265 to 192.168.100.0 0.0		Click Finish to d	eliver the configuration	on to the router.		
Hash DH Group Authentication Encryption MD5 group2 PRE_SHARE DES SH4_1 group2 PRE_SHARE 3DES Transform Sets: Name myset ESP Encryption.ESP_DES ESP Integrity.ESP_MD5_HMAC Mode: TUNNEL IPSec Rule: permit all ip traffic from 192.168.200.0 0.0.0.255 to 192.188.100.0 0.0.0		pre-snareu key. IKE Policies:				~
MD5 group2 PRE_SHARE DES SH4_1 group2 PRE_SHARE 3DES Transform Sets: Name:myset ESP Encryption:ESP_DES ESP Integrity:ESP_MD5_HMAC Mode:TUNNEL IPSec Rule: permit all ip traffic from 192.168.200.0 0.0.0.255 to 192.168.100.0.0.0		Hash	DH Group	Authentication	Encryption	
Transform Sets: Name:myset ESP Encryption:ESP_DES ESP Integrity:ESP_MD5_HMAC Mode:TUNNEL IPSec Rule: permit all ip traffic from 192.168.200.0 0.0.0.265 to 192.168.100.0 0.0		MD5 SHA_1	group2 group2	PRE_SHARE PRE_SHARE	DES 3DES	
IPSec Rule: permit all ip traffic from 192.168.200.0 0.0.0.255 to 192.168.100.0 0.0	D-	Transform Sets Name ESP Er ESP In Mode:1	: myset httpption:ESP_DES tegrity:ESP_MD5_Ht TUNNEL	MAC .		1
	KA	IPSec Rule: permit	all ip traffic from 192	.168.200.0 0.0.0.255 to	192.168.100.0 0	•
IF [Test VPN connectivity after configuring.]		Test VPN con	nectivity after configu	uting.]		

8. Per inviare la configurazione al router VPN, fare clic su

Delivery.

Deliver Configuration to Router	
Deliver delta commands to the router's running config.	
Preview commands that will be delivered to the router's running configuration.	
crypto ipsec transform-set inyset esp-ind5-himac esp-des mode tunnel exit crypto map SDM_CMAP_1 1 ipsec-isakmp description Tunnel to209.165.201.2 set transform-set myset set peer 209.165.201.2	
match address 101 exit interface FastEthernet1	
The differences between the running configuration and the startup configuration a the router is turned off.	ire lost whenever
This operation can take several minutes.	
Deliver Cancel Save to file Help	



9. Fare clic su **OK**.

Configurazione CLI

- <u>Ciscoasa</u>
- VPN-Router

Ciscoasa

```
ciscoasa(config)#show run
: Saved
:
ASA Version 8.0(3)
1
hostname ciscoasa
enable password 8Ry2YjIyt7RRXU24 encrypted
names
1
interface Ethernet0/0
nameif outside
security-level 0
ip address 209.165.201.2 255.255.255.224
!
interface Ethernet0/1
nameif inside
 security-level 100
ip address 192.168.100.1 255.255.255.0
1
interface Ethernet0/2
shutdown
no nameif
no security-level
no ip address
!
interface Ethernet0/3
shutdown
no nameif
no security-level
no ip address
I
interface Management0/0
shutdown
no nameif
no security-level
no ip address
!
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
   - Output suppressed access-list nonat extended permit
```

```
ip 192.168.100.0 255.255.255.0 192.168.200.0
255.255.255.0
no pager
mtu outside 1500
mtu inside 1500
icmp unreachable rate-limit 1 burst-size 1
asdm image disk0:/asdm-613.bin
no asdm history enable
arp timeout 14400
!!--- Define the nat-translation for Internet users
global (outside) 1 interface
nat (inside) 1 192.168.100.0 255.255.255.0
!!--- Define the nat-exemption policy for VPN traffic
nat (inside) 0 access-list nonat
route outside 0.0.0.0 0.0.0.0 209.165.201.1 1
1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00
icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp
0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00
sip-disconnect 0:02:00
timeout uauth 0:05:00 absolute
dynamic-access-policy-record DfltAccessPolicy
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup
linkdown coldstart
!!--- Configure the IPsec transform-set crypto ipsec
transform-set myset esp-des esp-md5-hmac
!!--- Configure the dynamic crypto map crypto dynamic-
map mymap 1 set transform-set myset
crypto dynamic-map mymap 1 set reverse-route
crypto map dyn-map 10 IPSec-isakmp dynamic mymap
crypto map dyn-map interface outside
!!--- Configure the phase I ISAKMP policy crypto isakmp
policy 10
authentication pre-share
encryption des
hash md5
group 2
lifetime 86400
!!--- Configure the default L2L tunnel group parameters
tunnel-group DefaultL2LGroup IPSec-attributes
pre-shared-key *
1
class-map inspection_default
match default-inspection-traffic
1
1
policy-map type inspect dns preset_dns_map
parameters
 message-length maximum 512
policy-map global_policy
class inspection_default
 inspect dns preset_dns_map
 inspect ftp
 inspect h323 h225
```

inspect	h323 ras
inspect	netbios
inspect	rsh
inspect	rtsp
inspect	skinny
inspect	esmtp
inspect	sqlnet
inspect	sunrpc
inspect	tftp
inspect	sip
inspect	xdmcp
!	
service-po	licy global_policy global
prompt hos	tname context
Cryptochec	ksum:d41d8cd98f00b204e9800998ecf8427e
: end	
ciscoasa(c	onfig)#

La CCP crea questa configurazione sul router VPN.

```
VPN-Router
VPN-Router#show run
Building configuration...
1
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname VPN-Router
1
Ţ
username cisco privilege 15 secret 5
$1$UQxM$WvwDZbfDhK3wS26C9xYns/
username test12 privilege 15 secret 5
$1$LC0U$ex3tp4hM8CYD.HJSRDfQ01
1
!!--- Output suppressed no aaa new-model ip subnet-zero
! ip cef ! crypto isakmp enable outside
!
crypto isakmp policy 1
encrypt 3des
 authentication pre-share
group 2
!
crypto isakmp policy 2
hash md5
authentication pre-share
group 2
!
1
crypto isakmp key cisco123 address 209.165.201.2
1
!
crypto ipsec transform-set myset esp-des esp-md5-hmac
1
1
crypto map SDM_CMAP_1 1 IPSec-isakmp
description Tunnel to209.165.201.2
 set peer 209.165.201.2
 set transform-set myset
```

```
match address 101
1
1
interface BRI0
no ip address
shutdown
!
interface Dot11Radio0
no ip address
shutdown
speed basic-1.0 basic-2.0 basic-5.5 6.0 9.0 basic-11.0
12.0 18.0 24.0 36.0 48.0 54.0
station-role root
!
interface Dot11Radio1
no ip address
 shutdown
speed basic-6.0 9.0 basic-12.0 18.0 basic-24.0 36.0
48.0 54.0
station-role root
!
interface FastEthernet0
ip address 192.168.200.1 255.255.255.0
 duplex auto
speed auto
1
interface FastEthernet1
ip address dhcp
duplex auto
 speed auto
 crypto map SDM_CMAP_1
!
interface FastEthernet2
no ip address
shutdown
!
interface FastEthernet3
no ip address
shutdown
!
interface FastEthernet4
no ip address
shutdown
interface FastEthernet5
no ip address
shutdown
1
interface FastEthernet6
no ip address
shutdown
1
interface FastEthernet7
no ip address
shutdown
!
interface FastEthernet8
no ip address
shutdown
ļ
interface FastEthernet9
no ip address
 shutdown
```

```
interface Vlan1
no ip address
!
ip classless
ip route 0.0.0.0 0.0.0.0 209.165.200.1
!
!!--- Output suppressed ! ip http server ip http
authentication local ip http secure-server ! access-list
100 permit ip 0.0.0.0 255.255.255.0 0.0.0.0
255.255.255.0
access-list 101 remark CCP_ACL Category=4
access-list 101 remark IPSEC Rule
access-list 101 permit ip 192.168.200.0 0.0.0.255
192.168.100.0 0.0.0.255
1
!
!
!
control-plane
!
!
line con 0
line aux 0
line vty 0 4
privilege level 15
login local
transport input telnet ssh
line vty 5 15
privilege level 15
login local
transport input telnet ssh
1
no scheduler allocate
end
```

Verifica

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

Lo <u>strumento Output Interpreter</u> (solo utenti <u>registrati</u>) (OIT) supporta alcuni comandi **show**. Usare l'OIT per visualizzare un'analisi dell'output del comando **show**.

- Verifica dei parametri del tunnel tramite CCP
- Verifica dello stato del tunnel tramite la CLI di ASA
- Verifica dei parametri del tunnel tramite la CLI del router

Verifica dei parametri del tunnel tramite CCP

 Monitorare il traffico che attraversa il tunnel IPsec.

incarcating deation into less that			<u>(8)</u>
Application Help		Cisc	o Configuration Professional
Select Coversarity Hember)	R Nonitor > Security > VPN Stud	ui > 1Fsec Tuenelli	
C Router Stopaty Change Status a Cost Status I Marc Turnels	VPH Scaus Off Ph Scaus Off Ph Turnes Off Ph Turnes	Each row represents one POic Tunnel Each row represents one POic Tunnel Local P Pointob P Peer 200 100 20012 201 100 2001 2000 200 100 201 2000	Stop Wonitoring Tent Tannel. Update Select Item to Nonitar Color Co
Deferm Typedi Defer State Def Ale Def State Def States	- PS on an architer	-Turnel Salar	P Send Errar Packets P Received Errar Packets
Care of the		Vew Hervel Positive data every 13 coc M Encapsainton Pacinty Decapsain at 19	tion Packets Sensitives Packets
		This (Add MASS)	The Decent 20

Monitorare lo stato della fase I di ISAKMP



SA.

Verifica dello stato del tunnel tramite la CLI di ASA

Verificare lo stato della fase I di ISAKMP SA.

ciscoasa#show crypto isakmp sa

```
Active SA: 1

Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)

Total IKE SA: 1

1 IKE Peer: 209.165.200.12

Type : L2L Role : responder

Rekey : no State : MM_ACTIVE

ciscoasa#
```

Nota: osservare che il ruolo di risponditore indica che l'iniziatore del tunnel è all'altra estremità, ad esempio il router VPN.

```
    Verificare i parametri di IPSEC SA fase II.

 ciscoasa#show crypto ipsec sa
 interface: outside
     Crypto map tag: mymap, seq num: 1, local addr: 209.165.201.2
       local ident (addr/mask/prot/port): (192.168.100.0/255.255.255.0/0/0)
       remote ident (addr/mask/prot/port): (192.168.200.0/255.255.255.0/0/0)
       current_peer: 209.165.200.12
       #pkts encaps: 29, #pkts encrypt: 29, #pkts digest: 29
       #pkts decaps: 29, #pkts decrypt: 29, #pkts verify: 29
       #pkts compressed: 0, #pkts decompressed: 0
       #pkts not compressed: 29, #pkts comp failed: 0, #pkts decomp failed: 0
       #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
       #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
       #send errors: 0, #recv errors: 0
       local crypto endpt.: 209.165.201.2, remote crypto endpt.: 209.165.200.12
       path mtu 1500, IPSec overhead 58, media mtu 1500
       current outbound spi: E7B37960
     inbound esp sas:
       spi: 0xABB49C64 (2880740452)
          transform: esp-des esp-md5-hmac none
          in use settings ={L2L, Tunnel, }
          slot: 0, conn_id: 4096, crypto-map: mymap
          sa timing: remaining key lifetime (kB/sec): (4274997/3498)
          IV size: 8 bytes
          replay detection support: Y
     outbound esp sas:
       spi: 0xE7B37960 (3887298912)
          transform: esp-des esp-md5-hmac none
          in use settings ={L2L, Tunnel, }
          slot: 0, conn_id: 4096, crypto-map: mymap
          sa timing: remaining key lifetime (kB/sec): (4274997/3498)
          IV size: 8 bytes
          replay detection support: Y
```

Verificare i parametri del tunnel tramite la CLI del router

 Verificare lo stato della fase I di ISAKMP SA. 								
VPN-Router# shc	ow crypto isakmp s	a						
dst	src	state	conn-id	slot	status			
209.165.201.2	209.165.200.12	QM_IDLE	1	0	ACTIVE			

```
    Verificare i parametri di IPSEC SA fase II.

 VPN-Router#show crypto ipsec sa
 interface: FastEthernet1
     Crypto map tag: SDM_CMAP_1, local addr 209.165.200.12
    protected vrf: (none)
    local ident (addr/mask/prot/port): (192.168.200.0/255.255.255.0/0/0)
    remote ident (addr/mask/prot/port): (192.168.100.0/255.255.255.0/0/0)
    current_peer 209.165.201.2 port 500
      PERMIT, flags={origin_is_acl,}
     #pkts encaps: 39, #pkts encrypt: 39, #pkts digest: 39
     #pkts decaps: 39, #pkts decrypt: 39, #pkts verify: 39
     #pkts compressed: 0, #pkts decompressed: 0
     #pkts not compressed: 0, #pkts compr. failed: 0
     #pkts not decompressed: 0, #pkts decompress failed: 0
     #send errors 6, #recv errors 0
      local crypto endpt.: 209.165.200.12, remote crypto endpt.: 209.165.201.2
      path mtu 1500, ip mtu 1500
      current outbound spi: 0xABB49C64(2880740452)
      inbound esp sas:
       spi: 0xE7B37960(3887298912)
         transform: esp-des esp-md5-hmac ,
         in use settings ={Tunnel, }
         conn id: 2001, flow_id: C18XX_MBRD:1, crypto map: SDM_CMAP_1
         sa timing: remaining key lifetime (k/sec): (4481818/3375)
         IV size: 8 bytes
         replay detection support: Y
         Status: ACTIVE
      inbound ah sas:
      inbound pcp sas:
      outbound esp sas:
       spi: 0xABB49C64(2880740452)
         transform: esp-des esp-md5-hmac ,
         in use settings ={Tunnel, }
         conn id: 2002, flow_id: C18XX_MBRD:2, crypto map: SDM_CMAP_1
         sa timing: remaining key lifetime (k/sec): (4481818/3371)
         IV size: 8 bytes
         replay detection support: Y
         Status: ACTIVE
      outbound ah sas:
      outbound pcp sas:
```

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

• Annullamento delle connessioni crittografiche esistenti in corso. ciscoasa#clear crypto ipsec sa ciscoasa#clear crypto isakmp sa Usare i comandi debug per risolvere i problemi del tunnel VPN.Nota: se si abilita il debug, è
possibile che il funzionamento del router venga interrotto quando il carico di lavoro nelle reti
interne è elevato.Usare con cautela i comandi di debug. In generale, si consiglia di utilizzare
questi comandi solo sotto la direzione del rappresentante del supporto tecnico del router per
la risoluzione di problemi specifici.

```
ciscoasa#debug crypto engine
ciscoasa#debug crypto isakmp
ciscoasa#debug crypto IPSec
ciscoasa#
VPN-Router#debug crypto engine
Crypto Engine debugging is on
VPN-Router#debug crypto isakmp
Crypto ISAKMP debugging is on
VPN-Router#debug crypto ipsec
Crypto IPSEC debugging is on
VPN-Router#
```

Per ulteriori informazioni sui comandi di debug, fare riferimento a <u>debug crypto isakmp</u> in <u>Descrizione e uso dei comandi di debug</u>.

Informazioni correlate

- Pagina di supporto per la negoziazione IPSEC/protocolli IKE
- Documentazione per il software del sistema operativo di Cisco ASA Security Appliance
- Soluzioni più comuni per la risoluzione dei problemi delle VPN IPSEC
- RFC (Requests for Comments)