# Configurazione di un tunnel IPSec tra un firewall Cisco Secure PIX e un firewall Checkpoint NG

### Sommario

Introduzione **Prerequisiti** Requisiti Componenti usati Esempio di rete Convenzioni Configurazione del PIX Configurazione del checkpoint NG Verifica Verifica della configurazione PIX Visualizza stato tunnel su checkpoint NG Risoluzione dei problemi Risoluzione dei problemi relativi alla configurazione PIX Riepilogo della rete Visualizza registri Checkpoint NG Informazioni correlate

### **Introduzione**

In questo documento viene illustrato come configurare un tunnel IPsec con chiavi già condivise per la comunicazione tra due reti private. Nell'esempio, le reti in comunicazione sono la rete privata 192.168.10.x all'interno di Cisco Secure PIX Firewall e la rete privata 10.32.x.x all'interno di Checkpoint<sup>TM</sup> Next Generation (NG) Firewall.

## **Prerequisiti**

### Requisiti

Prima di provare questa configurazione, accertarsi di soddisfare i seguenti requisiti:

- Il traffico tra il PIX e l'interno del <sup>checkpointTM</sup> NG e verso Internet (rappresentato qui dalle reti 172.18.124.x) deve scorrere prima di avviare questa configurazione.
- Gli utenti devono avere familiarità con la negoziazione IPSec. Questo processo può essere suddiviso in cinque fasi, incluse due fasi IKE (Internet Key Exchange).Un tunnel IPsec viene avviato da traffico interessante. Il traffico è considerato interessante quando avviene tra peer IPsec.Nella fase 1 di IKE, i peer IPsec negoziano il criterio di associazione di sicurezza (SA)

IKE stabilito. Dopo l'autenticazione dei peer, viene creato un tunnel protetto utilizzando Internet Security Association and Key Management Protocol (ISAKMP). In IKE fase 2, i peer IPsec utilizzano il tunnel autenticato e sicuro per negoziare le trasformazioni di associazione di sicurezza IPsec. La negoziazione del criterio condiviso determina la modalità di definizione del tunnel IPSec. Il tunnel IPSec viene creato e i dati vengono trasferiti tra i peer IPSec in base ai parametri IPSec configurati nei set di trasformazioni IPSec. Il tunnel IPsec termina quando le associazioni di protezione IPsec vengono eliminate o quando scade la loro durata.

#### Componenti usati

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

- Software PIX versione 6.2.1
- CheckpointTM NG Firewall

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

Nel documento viene usata questa impostazione di rete:



#### **Convenzioni**

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

# Configurazione del PIX

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

Configurazione PIX				
PIX Version 6.2(1)				
nameif ethernet0 outside security0				
nameif ethernet1 inside security100				
enable password 8Ry2YjIyt7RRXU24 encrypted				
passwd 2KFQnbNIdI.2KYOU encrypted				

hostname PIXRTPVPN domain-name cisco.com fixup protocol ftp 21 fixup protocol http 80 fixup protocol h323 h225 1720 fixup protocol h323 ras 1718-1719 fixup protocol ils 389 fixup protocol rsh 514 fixup protocol rtsp 554 fixup protocol smtp 25 fixup protocol sqlnet 1521 fixup protocol sip 5060 fixup protocol skinny 2000 names !--- Interesting traffic to be encrypted to the Checkpoint™ NG. access-list 101 permit ip 192.168.10.0 255.255.255.0 10.32.0.0 255.255.128.0 !--- Do not perform Network Address Translation (NAT) on traffic to the Checkpoint™ NG. access-list nonat permit ip 192.168.10.0 255.255.255.0 10.32.0.0 255.255.128.0 pager lines 24 interface ethernet0 10baset interface ethernet1 10full mtu outside 1500 mtu inside 1500 ip address outside 172.18.124.158 255.255.255.0 ip address inside 192.168.10.1 255.255.255.0 ip audit info action alarm ip audit attack action alarm pdm history enable arp timeout 14400 global (outside) 1 interface !--- Do not perform NAT on traffic to the Checkpoint™ NG. nat (inside) 0 access-list nonat nat (inside) 1 0.0.0.0 0.0.0.0 0 0 route outside 0.0.0.0 0.0.0.0 172.18.124.1 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 aaa-server LOCAL protocol local no snmp-server location no snmp-server contact snmp-server community public no snmp-server enable traps floodguard enable !--- Permit all inbound IPsec authenticated cipher sessions. sysopt connection permit-ipsec no sysopt route dnat !--- Defines IPsec encryption and authentication algorithms. crypto ipsec transform-set rtptac esp-3des esp-md5-hmac !--- Defines crypto map. crypto map rtprules 10 ipsecisakmp crypto map rtprules 10 match address 101 crypto map rtprules 10 set peer 172.18.124.157 crypto map rtprules 10 set transform-set rtptac !--- Apply crypto map on the outside interface. crypto map rtprules interface outside isakmp enable outside !--- Defines pre-shared secret used for IKE

```
authentication. isakmp key ******* address

172.18.124.157 netmask 255.255.255.255

!--- Defines ISAKMP policy. isakmp policy 1

authentication pre-share

isakmp policy 1 encryption 3des

isakmp policy 1 hash md5

isakmp policy 1 group 2

isakmp policy 1 lifetime 86400

telnet timeout 5

ssh timeout 5

terminal width 80

Cryptochecksum:089b038c8e0dbc38d8ce5ca72cf920a5

: end
```

### Configurazione del checkpoint NG

Gli oggetti e le regole di rete vengono definiti nel <sup>CheckpointTM</sup> NG per definire i criteri relativi alla configurazione VPN da configurare. Questo criterio viene quindi installato utilizzando <sup>CheckpointTM</sup> NG Policy Editor per completare il lato <sup>CheckpointTM</sup> NG della configurazione.

 Creare i due oggetti di rete per la rete del checkpoint e la rete del firewall PIX che crittografano il traffico interessante. A tale scopo, selezionare Gestisci > Oggetti di rete, quindi selezionare Nuovo > Rete. Immettere le informazioni di rete appropriate, quindi fare clic su OK.Questi esempi mostrano un set di oggetti di rete chiamati CP\_Inside (all'interno della rete di <sup>CheckpointTM</sup> NG) e PIXINSIDE (all'interno della rete di \_\_\_\_\_\_\_\_

Network Prope	ties - CP_inside		×
General NAT	]		
<u>N</u> ame:	CP_inside		
IP <u>A</u> ddress:	10.32.0.0		
Net <u>M</u> ask:	255.255.128.0		
<u>C</u> omment:	CPINSIDE		
Color:	<b></b> _		
Broadcas <u>Includ</u>	address: ed O <u>No</u> t included		
	OK Cancel	Help	

Network Prope	rties - PIXINSIDE	X
General NAT	]	
<u>N</u> ame:	PIXINSIDE	
IP <u>A</u> ddress:	192.168.10.0	
Net <u>M</u> ask:	255.255.255.0	
<u>C</u> omment:	Pixinside	
Co <u>l</u> or:	<b></b>	
Broadcas <u>I</u> nclud	t address: ed <u>O No</u> t included	
	OK Cancel Help	

2. Create gli oggetti della stazione di lavoro per <sup>CheckpointTM</sup> NG e PIX. A tale scopo, selezionare Gestisci > Oggetti di rete > Nuovo > Workstation.Èpossibile utilizzare l'oggetto stazione di lavoro <sup>CheckpointTM</sup> NG creato durante l'impostazione iniziale di <sup>CheckpointTM</sup> NG. Selezionare le opzioni per impostare la workstation come Gateway e Dispositivo VPN interoperabile e quindi fare clic su OK.Questi esempi mostrano una serie di oggetti chiamati ciscocp (CheckpointTM NG) e PIX (PIX Firewall).

Workstation Properties - o	ciscocp			×
Workstation Properties - o General Topology NAT VPN Authentication Management I Advanced	ciscocp General Name: IP Address: Color: Type:	ciscocp 172.18.124.157 Checkpoint External IP C Host © Gateway	<u>G</u> et address	X
	Check Point	Products int products installed: Version NG ireWall-1 o-1 ver anagement Station	i 🔽 Get Version	 ] ]
	Object Managed Managed Secure Interr Communic	gement	al) xtemal) cocppvzfoa	
		ОК	Cancel	Help

w	orkstation Properties -	PIX			X
	General — Topology	General			
	- NAT	<u>N</u> ame:	PIX		
	Advanced	IP <u>A</u> ddress:	172.18.124.158	<u>G</u> et address	
		Comment:	PIX Firewall		
		Color:			
		Туре:	⊂ <u>H</u> ost		
		Check Point P	Products		
		Check Po	int products installed: Version NG	Get Version	
		□VPN-1 & F □FloodGate □Policy Ser □Managem	ireWall-1 -1 ver ent Station		
		Object Manag	jement		
		C Managed	by this Management Server (Interna	el)	
		C Managed	by another Management Server (E)	ktemal)	
		✓ Interope	rable ⊻PN Device		
			OK	Cancel Help	

3. Selezionare Gestisci > Oggetti di rete > Modifica per aprire la finestra Proprietà stazione di lavoro per la stazione di lavoro <sup>CheckpointTM</sup> NG (ciscocp in questo esempio).Selezionare Topologia dalle opzioni sul lato sinistro della finestra, quindi selezionare la rete da crittografare. Fare clic su Modifica per impostare le proprietà dell'interfaccia.

4. Selezionare l'opzione per designare la workstation come interna, quindi specificare l'indirizzo IP appropriato. Fare clic su OK.In questa configurazione, CP\_inside è la rete interna del checkpoint<sup>TM</sup> NG. Le selezioni di topologia mostrate di seguito designano la workstation come interna e specificano l'indirizzo

	Interface	Properties			X
	General	Topology Qo	5		_
	Topolo	gy			
	O <u>E</u> xt	ernal (leads out t	o the internet)		
	💿 Įnte	ernal (leads to the	local network)		
	IP /	Addresses behind	this interface:		
	0	0 <u>N</u> ot Defined			
	0	Ne <u>t</u> work defin	ed by the interface	IP and Net Mask	
	(	Specific:	+ CP_inside	•	
	Anti-Sp ☑ <u>P</u> er Spo	oofing form Anti-Spoofir oof Tracking: 〇	ig based on interfa N <u>o</u> ne	ce topology O <u>A</u> lert	
ide.	[	ОК	Cancel	Help	

5. Nella finestra Proprietà workstation, selezionare l'interfaccia esterna sul <sup>CheckpointTM</sup> NG che conduce a Internet, quindi fare clic su **Modifica** per impostare le proprietà dell'interfaccia. Selezionare l'opzione per designare la topologia come esterna, quindi fare clic su

Inte	erface Properties	×
G	ieneral Topology QoS	
	Topology	
	• External (leads out to the internet)	
	O Internal (leads to the local network)	
	IP Addresses behind this interface:	
	C Not Defined	
	C Network defined by the interface IP and Net Mask	
	O Specific:	
	Anti-Spoofing	
	Perform Anti-Spoofing based on interface topology	
	Spoof Tracking: 🔿 N <u>o</u> ne 💿 <u>L</u> og 🔿 <u>A</u> lert	
_	OK Cancel Help	

 Dalla finestra Workstation Properties sul <sup>CheckpointTM</sup> NG, selezionare VPN dalle opzioni sul lato sinistro della finestra, quindi selezionare i parametri IKE per gli algoritmi di crittografia e autenticazione. Fare clic su Modifica per configurare le proprietà IKE.

Workstation Properties - o	iscocp			×
General Topology NAT VPN Authentication Management ⊡ Advanced	VPN Encryption schemes	set default <u>I</u> KE pr	roperties	
	Nickname DN ▲dd	E@t	Certificate Authority ▶ ■ Remove	

7. Configurare le proprietà IKE:Selezionare l'opzione per la crittografia **3DES** in modo che le proprietà IKE siano compatibili con il comando **isakmp policy # encryption 3des**.Selezionare l'opzione **MD5** in modo che le proprietà IKE siano compatibili con il comando **crypto isakmp** 

IKE Properties	X
General	
Support key exchange encryption of DES	with: Support data integrity with: MD <u>5</u> ■ SHA <u>1</u>
Support authentication methods: — Pre-Shared Secret	Edit <u>S</u> ecrets
Public <u>K</u> ey Signatures <u>V</u> PN-1 & FireWall-1 authentica	Specify ation for SecuRemote (Hybrid Mode)
	<u>A</u> dvanced
OK Ca	ancel Help

policy # hash md5.

8. Selezionare l'opzione di autenticazione per Segreti già condivisi, quindi fare clic su Modifica segreti per impostare la chiave già condivisa come compatibile con il comando PIX **isakmp** chiave chiave indirizzo netmask netmask . Fare clic su Edit (Modifica) per immettere la chiave, come mostrato di seguito, e fare clic su Set (Imposta),

Shar	ed Secret		
	Shared Secrets List:		
	Peer Name	Shared Secret	
	PIX	XXXX	<u>E</u> dit
			Bamaua
			<u>– Femove</u>
	r Entre courts [		
	Enter secier. Icisc	ortpi	
		Canaal	

9. Dalla finestra delle proprietà di IKE, fare clic su **Avanzate...** e modificare le seguenti impostazioni:Deselezionare l'opzione **Supporto modalità aggressiva**.Selezionare l'opzione **Supporta scambio chiave per le subnet**.Al termine, fare clic su

Advanced IKE properties			×
Use <u>UDP</u> encapsulation			
Support Diffie-Hellman groups ———		EC_encapsi 🔽	
	Group 1 (768	3 bit) 24 bit)	
	Group 5 (153	36 bit)	
Rekeying Parameters			- 
Renegotiate IKE security associa	tions	1440 🔅	Minutes
Renegotiate IPSEC Security asso	ciations every	3600 🕂	Seconds
Renegotiate IPSEC Security a	associations ever	ry 50000 🚊	KBytes
Misc			
Support IP <u>compression</u> for Support aggressive mode	ecureUlient		
Support key exchange for sul	onets		
	ancel	Help	

10. Selezionare Gestisci > Oggetti di rete > Modifica per aprire la finestra Proprietà stazione di lavoro per il PIX. Selezionare Topologia dalle opzioni sul lato sinistro della finestra per definire manualmente il dominio VPN.In questa configurazione, PIXINSIDE (all'interno della rete PIX) è definito come dominio VPN.

Workstation Properties - PIX	k internet				×
General	Topology	1			
- NAT	<u>G</u> et Interfaces				
- VPN - Advanced	Name	IP Address	Network Mask		
	Add	Edit	<u>B</u> emove	Show	- -
	Show all IPs beh	ind Gateway es <u>b</u> ehind Gateway b	ased on Topology	Show	-
	<ul> <li>Manually Defin</li> </ul>		•	Show	
	Egportable for \$	SecuRemote			
			OK C	Cancel Help	

11. Selezionare **VPN** dalle opzioni sul lato sinistro della finestra, quindi selezionare IKE come schema di crittografia. Fare clic su **Modifica** per configurare le proprietà IKE.

Workstation Properties - I	PIX			×
General - Topology - NAT - Advanced	VPN			
		OK	Cancel He	lp

12. Configurare le proprietà IKE come illustrato di seguito:Selezionare l'opzione per la crittografia 3DES in modo che le proprietà IKE siano compatibili con il comando isakmp policy # encryption 3des.Selezionare l'opzione MD5 in modo che le proprietà IKE siano compatibili con il comando crypto isakmp policy # hash

IKE Properties	
General	
Support key exchange encryptic	on with: – – Support data integrity with: –
DES DES	
CAST	
	I SHA <u>I</u>
Support authentication methods	[
✓ Pre-Shared Secret	Edit Secrets
Public Key Signatures	Matching Criteria
VPN 1.8 Firsty all 1 authors	Fighting Concerns (Hubrid Mode)
	tication for securitemote (Hybrid Mode)
	Advanced
	<u>A</u> dvanced
ОК	Cancel Help

 Selezionare l'opzione di autenticazione per Segreti già condivisi, quindi fare clic su Modifica segreti per impostare la chiave già condivisa come compatibile con il comando PIX isakmp key key address address netmask netmask. Fare clic su Modifica per immettere la chiave, quindi su Imposta,

×
e

14. Nella finestra delle proprietà di IKE fare clic su Avanzate e modificare le impostazioni.Selezionare il gruppo Diffie-Hellman appropriato per le proprietà IKE.Deselezionare l'opzione Supporto modalità aggressiva.Selezionare l'opzione Supporta scambio chiave per le subnet.Al termine, fare clic su OK,

Advanced IKE properties			×
Use UDP encapsulation			
o	UDP VPN1_IP	SEC_encapsi 💌	
Support Diffie-Hellman groups —		01.33	1
	Group 1 (76	8 bit) 124 hit)	
	Group 5 (15	i36 bit)	
Rekeying Parameters			
Renegotiate IKE security asso	ociations	1440 🕂	Minutes
Renegotiate IPSEC Security a	associations every	3600 🕂	Seconds
🔲 Renegotiate IPSEC Secu	rity associations eve	ery   50000 🚊	KBytes
Misc			
Support IP compression fo	or SecureClient		
Support <u>agg</u> resive mode			
Support key exchange for	r <u>s</u> ubnets		
ОК	Cancel	Help	

15. Selezionare Regole > Aggiungi regole > In alto per configurare le regole di crittografia per il criterio.Nella finestra Editor dei criteri, inserire una regola con un'origine CP\_inside (all'interno della rete del checkpoint <sup>TM</sup> NG) e PIXINSIDE (all'interno della rete del PIX) sia sulle colonne di origine che di destinazione. Impostare i valori per Service = Any, Action = Encrypt e Track = Log. Dopo aver aggiunto la sezione Azione crittografia della regola, fare clic con il pulsante destro del mouse su Azione, quindi selezionare Modifica proprietà.

CISCOCP - Check Point Policy Editor	- Standar	d g									
File Edit Wew Manage Rules Policy Topology Search Window Help											
1 📽 🛅 📰 🌮 1 94 84   🖪 🤇	°°S 🗃 S= 🕼 94 84   ▶ Q. Q. Q. Q. S. I 🕆 🖻 🖃										
\$ < < < < < < < < < < < < < < < < < < <	Sec.	urity - Standard 🔠	Address Translation - St	andard 🙀 QoS - S	tandard 🛄 Desktop S	ecurity - Standard					
Retwork Objects	NU.	SOURCE	DESTINATION	SERVICE	ACTION	TRACK	INSTALL				
	1			* Any	Edit prop	erties	🔝 Gateway:				
- ++ OP_inside	2	+ CP_inside	* Any	* Any	ece Ecit Entre	spilor	Gateway:				
Prodeside     Prodeside		ne	P 172.10.1 172.10.1	Comment 24.157 Chedipoi 24.158 PDX Pirew	Accept     Accept     Accept     Accept     Accept     Clert A     Clert B	iéh uéh n Audh ncrypt	1				
					Query Co Clear Qu	olunin ery					

16. Con IKE selezionato ed evidenziato, fare clic su

E	Encryption Properties	×
	General Encryption schemes defined: Image: KE Image: FVVZ	
	OK Cancel	Help

17. Nella finestra Proprietà IKE modificare le proprietà in modo che corrispondano alle trasformazioni IPSec PIX nel comando crypto ipsec transform-set rtptac esp-3des esp-md5-hmac.Impostare l'opzione Transform su Encryption + Data Integrity (ESP), impostare Encryption Algorithm su 3DES, impostare Data Integrity su MD5 e impostare Allowed Peer Gateway in modo che corrisponda al gateway PIX esterno (qui denominato PIX). Fare clic

IKE Properties	
General	
Transform	
Encryption + Data Integri	ty (ESP)
O Data Integrity Only (AH)	
Encryption Algorithm:	3DES 💌
Data Integrity	MD5
Compression method:	None
<u>A</u> llowed Peer Gateway:	PIX 💌
Use Perfect Forward Secrecy	
Use DH <u>G</u> roup:	Group 1 (768 bit) 🗾 💌
Perform IP <u>P</u> ool NAT	
ОКС	ancel Help

18. Dopo aver configurato il file <sup>CheckpointTM</sup> NG, salvare il criterio e selezionare Criterio > Installa per

attivarlo.	
allivano.	

CISCOCP - Check Point Policy E	ditor - Standard		10.00		· · · · · · · · · · · · · · · · · · ·	
File Edit View Manage Rules I	Policy Topology Search Window	Help				
	Verify Install Uninstall View	Address Translation - St	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	tandard 📅 Desitop S	eurty - Sandard	
	PRAEBS LOUS-					
Ketwork Objects	Install Users Database	DESTINATION	SERVICE	ACTION	TION TRACK	INSTALL
E Workstation	Management High Availability					
D PIX	Global Properties	+ PRONSIDE	* Any	C Encryst	🔳 Log	Gateway:
Network.						The second se
	2 + CP_inside	* Any	* Any	G accept	E Log	Gateway:
PDONSIDE						
- 😥 Domain						
OSE Device						
- Embedded Device						
- III Group						
- B Address Range				TRADE DE LA COMPANY		
Gateway Cluster		· · · · · · · · · · · · · · · · · · ·	ana ar ar			
Dynamic Object	Name	1P	Commerk			
	ciscocp	172.18.1	24.157 Checkpoir	nt External IP		
	D PDK	172.18.1	24.158 PEX Firew	al		
	CP_inside	10.32.0.0	O OPINSIDE	1		
	PDONSIDE	192.168.	10.0 Picinside			

Durante la compilazione del criterio, nella finestra di installazione vengono visualizzate note sullo stato di

avanzamento.



o la finestra di installazione indica che l'installazione dei criteri è stata completata. Fare clic su **Chiudi** per completare la

 Install Policy

 Standard.W: Security Policy Script generated into Standard.pf

 Standard:

 Compiled OK.

 Installing VPN-1/FireWall-1 policy On: ciscocp ...

 VPN-1/FireWall-1 policy installed successfully on ciscocp...

 VPN-1/FireWall-1 policy Installation for all modules was successful

## **Verifica**

### Verifica della configurazione PIX

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**.

Eseguire il ping tra una delle reti private e l'altra per verificare la comunicazione tra le due reti private. In questa configurazione, è stato inviato un ping dal lato PIX (192.168.10.2) alla rete interna di <sup>CheckpointTM</sup> NG (10.32.50.51).

• show crypto isakmp sa: visualizza tutte le SA IKE correnti in un peer.

```
show crypto isakmp sa
 Total
        : 1
 Embryonic : 0
             dst
                                        src
                                                                state
                                                                         pending created
   172.18.124.157 172.18.124.158 QM_IDLE
                                                      0
                                                                 1

    show crypto ipsec sa: visualizza le impostazioni utilizzate dalle associazioni di protezione

 correnti.
 PIX501A#show cry ipsec sa
 interface: outside
     Crypto map tag: rtprules, local addr. 172.18.124.158
    local ident (addr/mask/prot/port): (192.168.10.0/255.255.255.0/0/0)
    remote ident (addr/mask/prot/port): (10.32.0.0/255.255.128.0/0/0)
    current_peer: 172.18.124.157
      PERMIT, flags={origin_is_acl,}
     #pkts encaps: 19, #pkts encrypt: 19, #pkts digest 19
     #pkts decaps: 19, #pkts decrypt: 19, #pkts verify 19
     #pkts compressed: 0, #pkts decompressed: 0
     #pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0
     #send errors 1, #recv errors 0
      local crypto endpt.: 172.18.124.158, remote crypto endpt.: 172.18.124.157
      path mtu 1500, ipsec overhead 56, media mtu 1500
      current outbound spi: 6b15a355
      inbound esp sas:
       spi: 0xced238c7(3469883591)
         transform: esp-3des esp-md5-hmac ,
         in use settings ={Tunnel, }
         slot: 0, conn id: 3, crypto map: rtprules
         sa timing: remaining key lifetime (k/sec): (4607998/27019)
         IV size: 8 bytes
         replay detection support: Y
      inbound ah sas:
      inbound pcp sas:
      outbound esp sas:
       spi: 0x6b15a355(1796580181)
         transform: esp-3des esp-md5-hmac ,
         in use settings ={Tunnel, }
         slot: 0, conn id: 4, crypto map: rtprules
         sa timing: remaining key lifetime (k/sec): (4607998/27019)
         IV size: 8 bytes
         replay detection support: Y
      outbound ah sas:
      outbound pcp sas:
```

#### Visualizza stato tunnel su checkpoint NG

Andare all'Editor criteri e selezionare **Finestra > Stato sistema** per visualizzare lo stato del tunnel.

🐺 CISCOCP - Check Point System Status									
<u>File View M</u> odules <u>P</u> roducts <u>T</u> ools <u>W</u> indow <u>H</u> elp									
) 🖸 🗉   🗛 🔢 🔦 🎫 🇞 📾 🚅 🍥 😪	<b>於</b>								
Modules IP Address	VPN-1 Details								
E-12 CISCOCP	Status: OK								
E ciscocp 172.18.124.157	Packets								
FireWall-1	Encrypted: 20								
FloodGate-1	Decrypted: 20								
Management	Errors								
SVN Foundation	Encryption errors: 0								
MPIN-1	Decryption errors: 0								
	IKE events errors: 0								
	Hardware								
	HW Vendor Name: none								
	HW Status: none								

## Risoluzione dei problemi

#### Risoluzione dei problemi relativi alla configurazione PIX

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**.

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

Utilizzare questi comandi per abilitare i debug sul firewall PIX.

- **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 sugli eventi IKE.

```
VPN Peer: ISAKMP: Added new peer: ip:172.18.124.157 Total VPN Peers:1
VPN Peer: ISAKMP: Peer ip:172.18.124.157 Ref cnt incremented to:1 Total VPN Peers:1
ISAKMP (0): beginning Main Mode exchange
crypto_isakmp_process_block: src 172.18.124.157, dest 172.18.124.158
OAK_MM exchange
ISAKMP (0): processing SA payload. message ID = 0
ISAKMP (0): Checking ISAKMP transform 1 against priority 1 policy
ISAKMP: encryption 3DES-CBC
ISAKMP: hash MD5
ISAKMP: default group 2
ISAKMP: auth pre-share
ISAKMP: life type in seconds
ISAKMP: life duration (VPI) of 0x0 0x1 0x51 0x80
ISAKMP (0): atts are acceptable. Next payload is 0
```

```
ISAKMP (0): SA is doing pre-shared key authentication using id type ID_IPV4_ADDR
return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 172.18.124.157, dest 172.18.124.158
OAK_MM exchange
ISAKMP (0): processing KE payload. message ID = 0
ISAKMP (0): processing NONCE payload. message ID = 0
ISAKMP (0): ID payload
next-payload : 8
type : 1
protocol : 17
port : 500
length : 8
ISAKMP (0): Total payload length: 12
return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 172.18.124.157, dest 172.18.124.158
OAK_MM exchange
ISAKMP (0): processing ID payload. message ID = 0
ISAKMP (0): processing HASH payload. message ID = 0
ISAKMP (0): SA has been authenticated
ISAKMP (0): beginning Quick Mode exchange, M-ID of 322868148:133e93b4 IPSEC(key_engine): got a
queue event...
IPSEC(spi_response): getting spi 0xced238c7(3469883591) for SA
from 172.18.124.157 to 172.18.124.158 for prot 3
return status is IKMP_NO_ERROR
ISAKMP (0): sending INITIAL_CONTACT notify
ISAKMP (0): sending NOTIFY message 24578 protocol 1
ISAKMP (0): sending INITIAL_CONTACT notify
crypto_isakmp_process_block: src 172.18.124.157, dest 172.18.124.158
OAK_QM exchange
oakley_process_quick_mode:
OAK OM IDLE
ISAKMP (0): processing SA payload. message ID = 322868148
ISAKMP : Checking IPSec proposal 1
ISAKMP: transform 1, ESP_3DES
ISAKMP: attributes in transform:
ISAKMP: encaps is 1
ISAKMP: SA life type in seconds
ISAKMP: SA life duration (basic) of 28800
ISAKMP: SA life type in kilobytes
ISAKMP: SA life duration (VPI) of 0x0 0x46 0x50 0x0
ISAKMP: authenticator is HMAC-MD5
ISAKMP (0): atts are acceptable. IPSEC(validate_proposal_request): proposal part #1,
(key eng. msg.) dest= 172.18.124.157, src= 172.18.124.158,
dest_proxy= 10.32.0.0/255.255.128.0/0/0 (type=4),
src_proxy= 192.168.10.0/255.255.255.0/0/0 (type=4),
protocol= ESP, transform= esp-3des esp-md5-hmac ,
lifedur= 0s and 0kb,
spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
ISAKMP (0): processing NONCE payload. message ID = 322868148
ISAKMP (0): processing ID payload. message ID = 322868148
ISAKMP (0): processing ID payload. message ID = 322868148
ISAKMP (0): processing NOTIFY payload 24576 protocol 3
spi 3469883591, message ID = 322868148
ISAKMP (0): processing responder lifetime
ISAKMP (0): processing NOTIFY payload 24576 protocol 3
spi 3469883591, message ID = 322868148
ISAKMP (0): processing responder lifetime
ISAKMP (0): Creating IPSec SAs
inbound SA from 172.18.124.157 to 172.18.124.158 (proxy 10.32.0.0 to 192.168.10.0)
has spi 3469883591 and conn_id 3 and flags 4
lifetime of 28800 seconds
lifetime of 4608000 kilobytes
outbound SA from 172.18.124.158 to 172.18.124.157 (proxy 192.168.10.0 to 10.32.0.0)
has spi 1796580181 and conn_id 4 and flags 4
```

lifetime of 28800 seconds lifetime of 4608000 kilobytesIPSEC(key\_engine): got a queue event... IPSEC(initialize\_sas): , (key eng. msg.) dest= 172.18.124.158, src= 172.18.124.157, dest\_proxy= 192.168.10.0/255.255.255.0/0/0 (type=4), src\_proxy= 10.32.0.0/255.255.128.0/0/0 (type=4), protocol= ESP, transform= esp-3des esp-md5-hmac , lifedur= 28800s and 4608000kb, spi= 0xced238c7(3469883591), conn\_id= 3, keysize= 0, flags= 0x4 IPSEC(initialize\_sas): , (key eng. msg.) src= 172.18.124.158, dest= 172.18.124.157, src\_proxy= 192.168.10.0/255.255.255.0/0/0 (type=4), dest\_proxy= 10.32.0.0/255.255.128.0/0/0 (type=4), protocol= ESP, transform= esp-3des esp-md5-hmac , lifedur= 28800s and 4608000kb, spi= 0x6b15a355(1796580181), conn\_id= 4, keysize= 0, flags= 0x4 VPN Peer: IPSEC: Peer ip:172.18.124.157 Ref cnt incremented to:2 Total VPN Peers:1 VPN Peer: IPSEC: Peer ip:172.18.124.157 Ref cnt incremented to:3 Total VPN Peers:1 return status is IKMP\_NO\_ERROR

#### **Riepilogo della rete**

Quando più reti interne adiacenti sono configurate nel dominio di crittografia sul checkpoint, il dispositivo potrebbe riepilogarle automaticamente in relazione al traffico interessante. Se l'elenco di controllo di accesso (ACL) crittografico sul PIX non è configurato per corrispondere, è probabile che il tunnel abbia esito negativo. Ad esempio, se le reti interne 10.0.0.0 /24 e 10.0.1.0 /24 sono configurate per essere incluse nel tunnel, è possibile riepilogarle in 10.0.0.0 /23.

#### Visualizza registri Checkpoint NG

1	CISCOCP - Check Point Log Viewer - [fwJog]												
64	jele Mode Edit Selection 19ew Iools Window Help												
Ó	9 🤹 🙀	Log	*	*	A 1	F 🛓	۵ ک	<b>1</b> 2 👼	📑 🚟 🛱	🇞 🔛 😘	80	目	
1	Date	Time	Produc	t	::fiii	Inter.	Orig	Туре	Action	Source	Destina		into.
0	23Aug2002	17:32:47	WE VPN-	1 8 Fin	el/Vall	💽 da.	. ciscocp	🔳 log	Ow key install	PDC	ciscocp		IKE: Main Mode completion.
1	23Aug2002	17:32:47	VPN-	1 8 Fin	eiVal	🕒 de.	. ciscocp	🗐 log	Dw key install	PX	ciscocp		IKE: Quick Mode Received Notification from Peer: Initial Contact
2	23Aug2002	17:32:47	VPN-	1 & Fin	ei/Vall	💽 da.	. ciecocp	🔳 log	Ore key install	PIX	ciscocp		IKE: Guick Mode completion IKE IDs: subnet: 10.32.0.0 (mosk= 255.2)
з	23Aug2002	17:32:48	BE VPN-	t à Fin	el/Vall	E 11.	ciscoop	🔳 log	😡 decrypt	192:168 10:2	10.32.50.51	0	iomp-type 0 iomp-code 0
4	23Aug2002	17:32:48	器 VPN-	1 å Fin	el/Vall	🕒 E1.	. ciscoop	📕 log	🞑 decrypt	192.168.10.2	10.32.50.51	0	icmp-type 8 icmp-code 0
5	23Aug2002	17:32:48	R VPN-	18.50	elVal	🕒 E1.	clecoop	Iog	🔒 decrypt	192:168:10:2	10.32.50.51	0	icmp-type 8 icmp-code 8
6	23Aug2002	17:32:48	VPN-	1 8 Fin	elVal	🕒 E1.	ciscoop	🔳 log	😡 decrypt	192.168.10.2	10.32.50.51	0	iomp-type 8 iomp-code 8
l l													
5	23Aug2002 23Aug2002	17:32:48 17:32:48	VPN-	1 & Fin 1 & Fin	erval eiVal	C (1). C (1).	ciscoop	🔳 log	ideorypt decrypt	192.168.10.2	10.32.50.51	0	iomp-type 8 iomp-code 0 iomp-type 8 iomp-code 0

Selezionare Finestra > Visualizzatore log per visualizzare i log.

### Informazioni correlate

- <u>Software Cisco PIX Firewall</u>
- Riferimenti per i comandi di Cisco Secure PIX Firewall
- Avvisi sui prodotti per la sicurezza (inclusi PIX)
- <u>RFC (Requests for Comments)</u>
- Documentazione e supporto tecnico Cisco Systems