Configurazione del tunnel IPSec LAN-LAN tra Cisco Pix Firewall e un firewall NetScreen

Sommario

Introduzione Prerequisiti Requisiti Componenti usati Convenzioni Configurazione Esempio di rete Configurazioni Verifica Comandi di verifica Output verifica Risoluzione dei problemi Comandi per la risoluzione dei problemi Output di esempio del comando debug Informazioni correlate

Introduzione

In questo documento viene descritta la procedura necessaria per creare un tunnel LAN-LAN IPsec tra un firewall Cisco PIX e un firewall NetScreen con il software più recente. Dietro ogni dispositivo è presente una rete privata che comunica con l'altro firewall tramite il tunnel IPsec.

Prerequisiti

Requisiti

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

- Il firewall NetScreen è configurato con gli indirizzi IP nelle interfacce trust/untrust.
- Viene stabilita la connessione a Internet.

Componenti usati

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

- Software PIX Firewall versione 6.3(1)
- Ultima revisione NetScreen

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>

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> <u>ricerca</u> dei comandi (solo utenti <u>registrati</u>).

Esempio di rete

Nel documento viene usata questa impostazione di rete:



Configurazioni

Nel documento vengono usate queste configurazioni:

- PIX Firewall
- <u>Firewall NetScreen</u>

Configurazione del firewall PIX

PIX Firewall PIX Version 6.3(1) interface ethernet0 10baset interface ethernet1 100full nameif ethernet0 outside security0 nameif ethernet1 inside security100 enable password 8Ry2YjIyt7RRXU24 encrypted

passwd 2KFQnbNIdI.2KYOU encrypted hostname pixfirewall domain-name cisco.com fixup protocol ftp 21 fixup protocol h323 h225 1720 fixup protocol h323 ras 1718-1719 fixup protocol http 80 fixup protocol ils 389 fixup protocol rsh 514 fixup protocol rtsp 554 fixup protocol sip 5060 fixup protocol sip udp 5060 fixup protocol skinny 2000 fixup protocol smtp 25 fixup protocol sqlnet 1521 names !--- Access control list (ACL) for interesting traffic to be encrypted and !--- to bypass the Network Address Translation (NAT) process. access-list nonat permit ip 10.0.25.0 255.255.255.0 10.0.3.0 255.255.255.0 pager lines 24 logging on logging timestamp logging buffered debugging icmp permit any inside mtu outside 1500 mtu inside 1500 !--- IP addresses on the interfaces. ip address outside 172.18.124.96 255.255.255.0 ip address inside 10.0.25.254 255.255.255.0 ip audit info action alarm ip audit attack action alarm pdm logging informational 100 pdm history enable arp timeout 14400 global (outside) 1 interface !--- Bypass of NAT for IPsec interesting inside network traffic. nat (inside) 0 access-list nonat nat (inside) 1 0.0.0.0 0.0.0.0 0 0 !--- Default gateway to the Internet. route outside 0.0.0.0 0.0.0.0 172.18.124.1 1 timeout xlate 0:05:00 timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h225 1:00:00 timeout h323 0:05:00 mgcp 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 http 10.0.0.0 255.0.0.0 inside no snmp-server location no snmp-server contact snmp-server community public no snmp-server enable traps floodguard enable !--- This command avoids applied ACLs or conduits on encrypted packets. sysopt connection permit-ipsec !--- Configuration of IPsec Phase 2. crypto ipsec transform-set mytrans esp-3des esp-sha-hmac crypto map mymap 10 ipsec-isakmp crypto map mymap 10 match address nonat crypto map mymap 10 set pfs group2 crypto map mymap 10 set peer 172.18.173.85



Configurazione del firewall NetScreen

Completare questa procedura per configurare il firewall NetScreen.

- 1. Selezionare Elenchi > Indirizzo, andare alla scheda Attendibile e fare clic su Nuovo indirizzo.
- Aggiungere la rete interna NetScreen crittografata sul tunnel e fare clic su OK.Nota: assicurarsi che l'opzione Trust sia selezionata.Nell'esempio, viene usata la rete 10.0.3.0 con una maschera di

) Back + 🐑 - 💌 🛋 🏠 🔎 9	Search 👷 Favorites 🜒 Media 🥝 🔂 😓 🗟	8 - 💟 🎎	
aress 🗿 hetp://10.0.3.254/layout.html*6,1,1			💌 🛃 Go 🛛 Links
IETSCREEN'-5		• help • support	• about • logout
System Address Address Admin Interface	CONFIGURATION		
Network Policy VPN Mitbal IP Lists Address Service Schedble Users Monitor	Address Name IP Address/Domain Name Netmask Comment Location	[insideNetwork [10.0.3.0 [255.255.255.0	
Traffic Counters Alarm Log	1	OKCencel	
ceynight & 1968-2001 efformen Technologier Ind. All rightresterved.			

3. Selezionare Elenchi > Indirizzo, andare alla scheda Non attendibile e fare clic su Nuovo

indirizzo.

4. Aggiungere la rete remota utilizzata da NetScreen Firewall per crittografare i pacchetti e fare clic su OK.Nota: non utilizzare i gruppi di indirizzi quando si configura una VPN per un gateway non NetScreen. L'interoperabilità VPN non riesce se si utilizzano gruppi di indirizzi. Il gateway di protezione non NetScreen non è in grado di interpretare l'ID proxy creato da NetScreen quando viene utilizzato il gruppo di indirizzi.Per risolvere questo problema, sono disponibili due soluzioni:Separare i gruppi di indirizzi in singole voci della rubrica. Specificare i singoli criteri in base alla voce della rubrica.Se possibile, configurare l'ID proxy su 0.0.0/0 sul gateway non NetScreen (dispositivo firewall).Nell'esempio, viene usata la rete 10.0.25.0 con una maschera di

NetScreen Administration Tools - Microsoft	Internet Explorer		2181 ×
File Edit View Favorites Tools Help			2
🔇 Back + 🕑 - 💌 💈 🟠 🔎 Se	arch 🐈 Favorites 🜒 Media 🧭 🔂 - 🤳 🖩	8 - 🔁 🎎	
Address a http://10.0.3.254/kayout.html*6,1,1			💌 🛃 Go Links 🏁
NETSCREEN-5		help support	• about • logout
Suctom			1 8 8 C - 1 - 1 - 1 - 1 - 1 - 1 - 1 - 1 - 1 -
ADDRESS	CONFIGURATION		-
Admin			
Interface		î	
Network			
Policy	Address Name	Remoteblaturark	
VPN	Address Madre	Premolevenion	
Virtual IP	IP Address/Domain Name	10.0.25.0	
Lists			
Address	Netmask	255.255.255.0	
Service			
Users	Comment		
Monitor	Location	C Tout & Hebruit	
	Locaton	Tust - Onitust	
Counters		in or Louis I	
Alarm		UK Cancel	
Log			
Ceavilaht @ 1998-2001			
NetScreen Technologies			
All rights reserved.			
a) Go to the Units steel Addresses Configuration			a Internet
	a di di anti anti anti anti anti anti anti ant	- 1- 1- 1z	

- 5. Selezionare **Rete > VPN**, andare alla scheda Gateway e fare clic su **Nuovo gateway tunnel remoto** per configurare il gateway VPN (criteri IPsec fase 1 e fase 2).
- 6. Usare l'indirizzo IP dell'interfaccia esterna del PIX per terminare il tunnel e configurare le opzioni IKE della fase 1 da associare. Al termine, fare clic su OK.In questo esempio vengono utilizzati i campi e i valori seguenti.Nome gateway: A501Indirizzo IP statico: 172.18.124.96Modalità: Principale (protezione ID)Chiave già condivisa: "testme"Proposta fase 1: pre-g2-3des-sha

NetScreen Administration	1 Tools - Microsoft Internet Explorer	1 al X
Elle Edit Yew Fgvarites	Ios He	2
🔾 Sack + 💭 🖉 📕	2 😚 🔎 Search 👷 Pavortes 😁 Media 🌮 🍰 🐨 🖓 🐨 🖓 🏅	
Aggress App://10.0.3.254/4	layout.htmi*6,1,1 💌 🛃 🐼	Links ³⁰
NETSCREEN'-5	help • support • about • log	out
System	REMOTE TUNNEL GATEWAY CONFIGURATION	-
Configure		
Interface		
Network	Gateway Name Toson	
Policy	Remote Gateway	
VPN VPNALTP	Static IP Address IP Address 17218.124.96	
Lists	Dynamic IP Address Peer ID (optional)	
Address	C Dialup User User/Group None -	
Gervice		
Users	Wiede (Instator) * Main (ID Protection) * Aggressive	
Monitor	Phase 1 Proposal	
Traffic	pre-g2-3des-sha r none	
Counters		
Log	Preshared Key	
Conversion in 1998 2001	Local ID (optional)	
NetScreen Technologies	Preferred Certificate (optional)	
All right: reserved,	Local Cert None -	
	Peer Type NONE *	
	OK Cancel	
		•
Go to the Gateway Configuration	Internet	1

Una volta creato il gateway del tunnel remoto, viene visualizzata una schermata simile a questa.



- 7. Andare alla scheda Proposta P1 e fare clic su **Nuova proposta fase 1** per configurare la proposta 1.
- Immettere le informazioni di configurazione per la proposta di fase 1 e fare clic su OK.In questo esempio vengono utilizzati questi campi e valori per lo scambio Fase 1.Nome: ToPix501Autenticazione: PrecondivisioneGruppo DH: Gruppo 2Crittografia: 3DES-CBCHash: SHA-1Durata: 3600 sec.

Quando la fase 1 è stata aggiunta correttamente alla configurazione NetScreen, viene visualizzata una schermata simile a

- 9. Andare alla scheda Proposta P2 e fare clic su **Nuova proposta fase 2** per configurare la fase 2.
- Immettere le informazioni di configurazione per la proposta per la fase 2 e fare clic su OK.In questo esempio vengono utilizzati questi campi e valori per lo scambio Fase 2.Nome: ToPix501Perfect Forward Secrecy: DH-2 (1024 bit)Algoritmo di crittografia: 3DES-CBCAlgoritmo di autenticazione: SHA-1Durata: 26400

sec			
NetScreen Administration Tools - Mic	rosoft Internet Explorer		-16 ×
Elle Edit Yew Figworites Iools He		a <u></u>	
😋 Back + 🐑 - 💌 😫 🐔 ,	🔎 Search 👷 Favorites 🜒 Media 🔗 🍰 🤤 🛛	🧾 🕹	
Address Attp://10.0.3.254/layout.html*6	1,1		🖸 🛃 Go 🛛 Links 🇯
NETSCREEN - 5		• help • support • ab	out logout
System PHA	ASE 2 PROPOSAL CONFIGURATION		
Admin	Shelf File Contraction (1986)		×.
Interface	[
Network	Name	ToPx501	
VEN	Perfect Forward Secrecy	DH Group 2 *	
Virtual IP	Encapsulation		
Lists	· Encryption (ESP)		
Service	Encryption Algorithm	3DES-CBC -	
Schedule	Authentication Algorithm	SHA-1 •	
Uters	C Authentication Only (AH)		
Monator	Authentication Algorithm	MD5 •	
Counters			
Alam	Lifetime	1 (D)	
E00	In Time	26400	
Copyright @ 1998-2001 NetScreen Technologies		Sec ∩ Min ∩ Hours ∩ Days	
Inc. All rights reserved.	In Kbytes	10 Rbytes	

Quando la fase 2 è stata aggiunta correttamente alla configurazione NetScreen, viene visualizzata una schermata simile a questa.

(in)			~ ~ ~					-1.09
http://10.0.3.254	fayout.html*6,1,	1						<u></u> ⊻ 🔁 🕫
SCREEN -5						• help	• 90p	port • about •
System	VPN							17 Sept 2003 15
Configure								
Admin								1'age
Interface	Manu	al Key AutoKey DR Ga	teway P1 Pro	posal P2	Proposal Certificate	127	P	PPage
Network	and the second							1
Policy								
VPN								
Virtual IP	1		L'Annes I		Internet and the	240.20		a second second
The second second second		Name	PFS	Encap,	Encrypt/Autn.	Lifetime	Lifesize	Configure
Lists		AAAA 240 440 MAG	No PES	ESP	DES/MOS	3900	0	1.1.1.1.1.1.1
Lists		and be sub-sub-sub-			and the second se			
Lists Address		nopti-esp-dep-sha	No PFS	ESP	DES/SHA	3600	0	
Lists Address Service		nopti-esp-des-sha nopti-esp-des-md5	No PFS No PFS	ESP ESP	DES / SHA 30ES / MD5	3600 3600	0	
Lists Address Service Schedule		nopti-esp-3des-sha nopti-esp-3des-md5 nopti-esp-3des-sha	No PFS No PFS No PFS	ESP ESP ESP	DES / SHA 30ES / MD5 30ES / SHA	3600 3600 3600	0 0 0	
Lists Address Service Schedule Users Monitor		nopti-esp-des-sha nopti-esp-3des-sha nopti-esp-3des-sha g2-esp-des-md5	No PFS No PFS No PFS DH Group 2	ESP ESP ESP ESP	DES/SHA 3DES/MD5 3DES/SHA DES/MD6	3600 3600 3600 3600	0 0 0	
Lists Address Service Schedule Users Monitor		nopti-esp-des-sha nopti-esp-3des-md5 nopti-esp-3des-sha g2-esp-des-md5 g2-esp-des-md5	No PFS No PFS No PFS DH Group 2 DH Group 2	ESP ESP ESP ESP ESP	DES / SHA 30ES / MD5 30ES / SHA 0ES / M05 0ES / SHA	3600 3600 3600 3600 3600	0 0 0 0	
Lists Address Service Schedule Users Monitor Traffic		nopti-esp-3des-md5 nopti-esp-3des-md5 nopti-esp-3des-md5 g2-esp-des-md5 g2-esp-des-md5 g2-esp-3des-md5	No PFS No PFS No PFS DH Group 2 DH Group 2 DH Group 2	ESP ESP ESP ESP ESP ESP	0ES/SHA 30ES/M05 3DES/SHA 0ES/M05 0ES/SHA 30ES/M05	3600 3600 3600 3600 3600 3600	0 0 0 0 0	
Lists Address Service Schedule Users Monitor Traffic Counters Alarm		nopti-esp-des-sha nopti-esp-3des-sha g2-esp-des-sha g2-esp-des-sha g2-esp-des-sha g2-esp-3des-sha g2-esp-3des-sha	No PFS No PFS No PFS DH Group 2 DH Group 2 DH Group 2 DH Group 2	ESP ESP ESP ESP ESP ESP ESP	DES / SHA 30ES / MD5 3DES / SHA 0ES / M05 0ES / SHA 3DES / MD5 3DES / SHA	3800 3800 3800 3800 3800 3800 3800	0 0 0 0 0 0	
Lists Address Service Schedule Users Monitor Traffic Counters Alarm		nopti-esp-des-sha nopti-esp-3des-sha g2-esp-des-m05 g2-esp-des-m05 g2-esp-des-sha g2-esp-3des-sha g2-esp-3des-sha TsPro601	No PFS No PFS No PFS DH Group 2 DH Group 2 DH Group 2 DH Group 2 DH Group 2 DH Group 2	ESP ESP ESP ESP ESP ESP ESP ESP	DES / SHA 30ES / MD5 30ES / SHA 0ES / MD5 0ES / SHA 30ES / MD5 30ES / SHA	3600 3600 3600 3600 3600 3600 3600 26400	0 0 0 0 0 0 0	

- 11. Selezionare la scheda **AutoKey IKE**, quindi fare clic su **Nuova voce IKE AutoKey** per creare e configurare AutoKey IKE.
- 12. Immettere le informazioni di configurazione per AutoKey IKE e quindi fare clic su OK.In questo esempio vengono utilizzati questi campi e valori per AutoKey IKE.Nome: VPN-1Nome tunnel gateway remoto: A501Questa opzione è stata creata in precedenza nella scheda Gateway.Proposta fase 2: ToPix501Questa opzione è stata creata in precedenza nella scheda Proposta P2.Monitor VPN: Attivaln questo modo il dispositivo NetScreen può impostare le trap SNMP (Simple Network Management Protocol) per monitorare le condizioni del monitor

VPN.

NetScreen Administrati	ion Tools - Microsoft Internet Explorer	_ 6 ×
Ele Edit Yew Favorite	tes Tools Help	2
😮 Back + 🕑 - 💌	😰 🐔 🔎 Search 🐈 Favorites 🜒 Media 🥝 🍰 - 🤪 🗟 - 📴 🚳	
Address http://10.0.3.25	S4/Jayout. Honi*6,1,1	🔁 Go Links »
NETSCREEN-5	• help)• support • about	• logout
System Configure	AUTOKEY IKE CONFIGURATION	
Admin Interface		
Policy	Name VPN-1	
Virtual IP	Remote Gateway Tunnel Name To501 Ust Gateways	
Address	Phase 2 Proposal ToPb501	
Schedule	none T	
Monitor	none	
Counters	VPN Monitor 🗟 Enable	
Log	Transport Mode Enable (For L2TP-over-IPSec only)	
Copyright © 1995-2001 NetScreen Technologies Inc.	OK Cencel	

Una volta configurata correttamente la regola VPN-1, viene visualizzata una schermata simile a quella dell'esempio.

NetScreen Administration	Tools - Microsoft Inter	net Explorer	<u>.</u>			-		_ 5 X
Ele Edit Yew Favorites	Icols the							1
🕒 Back + 🕤 - 💽	🕈 🔥 🔎 Search	📌 Favorites 📢	Media 🚱	🔗 · 冯 🖩 · 📴	3			
Address 1 http://10.0.3.254/0	nyout.html*6,1,1						•	🔁 Go Links »
NETSCREEN'-5						• hilp •	support • abou	t Flogout
System	VPN						17 Sept 2	003 15:46:06
Configure								2.1.4
Admin								Page 1 of 1
Interface	Nanual Key	AutoKey IKE	ateway P1	Proposal P2 Proposa	Certificates	LITP	IPPool	
Network								
Policy	Name	Gateway	Replay	P2 Proposals	Monitor	Transport	Configure	i I
Virtual IP	VPN-1	To501	No	ToPix501	On	Off	List	
Lists								-*
Address								
Service								
Schedule								
Users								
Monitor								
Traffic								
Counters								
- Hann								
Section in case of								
Copyright @ 1999-2001 NetSchen Technologies								
inc.								

- 13. Selezionare **Rete > Criterio**, andare alla scheda In uscita e fare clic su **Nuovo criterio** per configurare le regole che consentono la crittografia del traffico IPSec.
- 14. Immettere le informazioni di configurazione per il criterio e fare clic su OK. In questo esempio vengono utilizzati questi campi e valori per il criterio. Il campo Name (Nome) è facoltativo e non viene utilizzato in questo esempio. Source address: All'interno della reteQuesta impostazione è stata definita in precedenza nella scheda Attendibile.Indirizzo di destinazione: ReteRemotaQuesta impostazione è stata definita in precedenza nella scheda non attendibile.Servizio: QualsiasiAzione: TunnelTunnel VPN: VPN-1(precedentemente definito come tunnel VPN nella scheda AutoKey IKE).Modifica criterio VPN in ingresso corrispondente: ControllatoQuesta opzione crea automaticamente una regola in entrata che corrisponde al traffico VPN della rete esterna.

NetScreen Administration Tools - Microsoft .	Internet Explorer	_16 X
Elle Edit Vew Favorites Icols Help		
🔇 Back + 🕑 - 🖹 🗟 🏠 🔎 Sea	arch 👷 Favorites 😵 Media 🥙 🍰 😳 🚱 - 🗾 🍪	
Address) http://10.0.3.254/Jayout.html*6,1,1		💌 🛃 Go 🛛 Links 🇯
NETSCREEN -5	🧶 bitp	• support • about • logout
System Dor tow oo	NUCLIDATION	-
Configure	MIGURATION	
Admin	1	
Interface		
Network	Name (optional)	
Policy	Source Address InsideNetwork *	
Ven	Destination Address RemoteNetwork *	
Liete	Service ANY	
Address	NAT & OF	
Service	C	
Schedule	⊂ DI₽ Off	
Users	C DIP On	
Monitor		
Traffic	A. HOMMAN	
Counters	Action Tunnel 1	
Alarm	VPN Tunnel VPN-1	
	Andify matching incoming VPN policy	
Cepyright @ 1999-2001 NetScreen Technologies	L2TP None •	
inc. All rights paramed	Authentication	

15. Quando il criterio viene aggiunto, verificare che la regola VPN in uscita sia la prima nell'elenco dei criteri. La regola creata automaticamente per il traffico in entrata si trova nella scheda In entrata.Completare questi passaggi se è necessario modificare l'ordine dei criteri:Fare clic sulla scheda In uscita.Fare clic sulle frecce circolari nella colonna Configura per visualizzare la finestra Sposta macro criteri.Modificare l'ordine dei criteri in modo che il criterio VPN sia superiore all'ID criterio 0 (in modo che il criterio VPN sia in cima all'elenco).

Andare alla scheda In entrata per visualizzare la regola per il traffico in entrata.

Verifica

Le informazioni contenute in questa sezione permettono di verificare che la configurazione funzioni correttamente.

Comandi di verifica

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**.

- ping Esegue la diagnosi della connettività di rete di base.
- show crypto ipsec sa: visualizza le associazioni di sicurezza della fase 2.
- show crypto isakmp sa: visualizza le associazioni di sicurezza della fase 1.

Output verifica

Di seguito è riportato un esempio di output dei comandi ping e show.

Il ping viene avviato da un host dietro il firewall NetScreen.

```
C:\>ping 10.0.25.1 -t
Request timed out.
Request timed out.
Reply from 10.0.25.1: bytes=32 time<105ms TTL=128
Reply from 10.0.25.1: bytes=32 time<114ms TTL=128
Reply from 10.0.25.1: bytes=32 time<106ms TTL=128
Reply from 10.0.25.1: bytes=32 time<121ms TTL=128
Reply from 10.0.25.1: bytes=32 time<110ms TTL=128
Reply from 10.0.25.1: bytes=32 time<116ms TTL=128
Reply from 10.0.25.1: bytes=32 time<109ms TTL=128
Reply from 10.0.25.1: bytes=32 time<110ms TTL=128
Reply from 10.0.25.1: bytes=32 time<118ms TTL=128
Di seguito è riportato l'output del comando show crypto ipsec sa.
pixfirewall(config)#show crypto ipsec sa
interface: outside
    Crypto map tag: mymap, local addr. 172.18.124.96
   local ident (addr/mask/prot/port):
      (10.0.25.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port):
      (10.0.3.0/255.255.255.0/0/0)
   current_peer: 172.18.173.85:500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 11, #pkts encrypt: 11, #pkts digest 11
    #pkts decaps: 11, #pkts decrypt: 13, #pkts verify 13
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0,
    #pkts decompress failed: 0, #send errors 0, #recv errors 1
     local crypto endpt.: 172.18.124.96,
        remote crypto endpt.: 172.18.173.85
     path mtu 1500, ipsec overhead 56, media mtu 1500
     current outbound spi: f0f376eb
     inbound esp sas:
      spi: 0x1225ce5c(304467548)
        transform: esp-3des esp-sha-hmac ,
        in use settings ={Tunnel, }
       slot: 0, conn id: 3, crypto map: mymap
       sa timing: remaining key lifetime (k/sec):
         (4607974/24637)
       IV size: 8 bytes
       replay detection support: Y
    inbound ah sas:
    inbound pcp sas:
    outbound esp sas:
     spi: 0xf0f376eb(4042487531)
       transform: esp-3des esp-sha-hmac ,
       in use settings ={Tunnel, }
       slot: 0, conn id: 4, crypto map: mymap
       sa timing: remaining key lifetime (k/sec):
         (4607999/24628)
       IV size: 8 bytes
```

```
replay detection support: Y
```

outbound ah sas:

outbound pcp sas:

Di seguito è riportato l'output del comando show crypto isakmp sa.

Risoluzione dei problemi

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

Comandi per la risoluzione dei problemi

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

- debug crypto engine: visualizza i messaggi relativi ai motori di crittografia.
- debug crypto ipsec: visualizza le informazioni sugli eventi IPsec.
- debug crypto isakmp: visualizza i messaggi sugli eventi IKE.

Output di esempio del comando debug

Di seguito è riportato un esempio di output del comando debug per il firewall PIX.

```
debug crypto engine
debug crypto ipsec
debug crypto isakmp
crypto_isakmp_process_block:src:172.18.173.85,
 dest:172.18.124.96 spt:500 dpt:500
OAK_MM exchange
ISAKMP (0): processing SA payload. message ID = 0
ISAKMP (0): Checking ISAKMP transform 1 against priority 10 policy
ISAKMP:
           encryption 3DES-CBC
           hash SHA
ISAKMP:
          default group 2
ISAKMP:
ISAKMP:
          auth pre-share
ISAKMP:
           life type in seconds
ISAKMP:
           life duration (basic) of 28800
ISAKMP (0): atts are acceptable. Next payload is 0
ISAKMP (0): processing vendor id payload
ISAKMP (0): processing vendor id payload
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:172.18.173.85,
  dest:172.18.124.96 spt:500 dpt:500
OAK_MM exchange
ISAKMP (0): processing KE payload. message ID = 0
ISAKMP (0): processing NONCE payload. message ID = 0
return status is IKMP_NO_ERROR
crypto_isakmp_process_block:src:172.18.173.85,
  dest:172.18.124.96 spt:500 dpt:500
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): ID payload
       next-payload : 8
                 : 1
       type
       protocol
                   : 17
       port
                   : 500
                   : 8
       length
ISAKMP (0): Total payload length: 12
return status is IKMP_NO_ERROR
ISAKMP (0): sending INITIAL_CONTACT notify
ISAKMP (0): sending NOTIFY message 24578 protocol 1
VPN Peer: ISAKMP: Added new peer: ip:172.18.173.85/500
  Total VPN Peers:1
VPN Peer: ISAKMP: Peer ip:172.18.173.85/500 Ref cnt
  incremented to:1
   Total VPN Peers:1
crypto_isakmp_process_block:src:172.18.173.85,
  dest:172.18.124.96 spt:500 dpt:500
ISAKMP (0): processing DELETE payload. message ID = 534186807,
  spi size = 4IPSEC(key_engin
e): got a queue event...
IPSEC(key_engine_delete_sas): rec'd delete notify from ISAKMP
IPSEC(key_engine_delete_sas):
   delete all SAs shared with 172.18.173.85
return status is IKMP_NO_ERR_NO_TRANS
crypto_isakmp_process_block:src:172.18.173.85,
  dest:172.18.124.96 spt:500 dpt:500
OAK_QM exchange
oakley_process_quick_mode: OAK_QM_IDLE
ISAKMP (0): processing SA payload. message ID = 4150037097
ISAKMP : Checking IPSec proposal 1
ISAKMP: transform 1, ESP_3DES
ISAKMP: attributes in transform:
         SA life type in seconds
ISAKMP:
           SA life duration (VPI) of 0x0 0x0 0x67 0x20
ISAKMP:
ISAKMP:
           encaps is 1
ISAKMP:
           authenticator is HMAC-SHA
           group is 2
ISAKMP:
ISAKMP (0): atts are acceptable.
IPSEC(validate_proposal_request): proposal part #1,
  (key eng. msg.) dest= 172.18.124.96, src= 172.18.173.85,
   dest_proxy= 10.0.25.0/255.255.255.0/0/0 (type=4),
   src_proxy= 10.0.3.0/255.255.255.0/0/0 (type=4),
   protocol= ESP, transform= esp-3des esp-sha-hmac ,
   lifedur= 0s and 0kb,
    spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x24
```

```
ISAKMP (0): processing NONCE payload. message ID = 4150037097
ISAKMP (0): processing KE payload. message ID = 4150037097
ISAKMP (0): processing ID payload. message ID = 4150037097
ISAKMP (0): ID_IPV4_ADDR_SUBNET src 10.0.3.0/255.255.255.0
  prot 0 port 0
ISAKMP (0): processing ID payload. message ID = 4150037097
ISAKMP (0): ID_IPV4_ADDR_SUBNET dst 10.0.25.0/255.255.255.0
  prot 0 port 0IPSEC(key_engine)
: got a queue event...
IPSEC(spi_response): getting spi 0x1225ce5c(304467548) for SA
        from 172.18.173.85 to 172.18.124.96 for prot 3
return status is IKMP_NO_ERROR
crypto_isakmp_process_block:src:172.18.173.85,
  dest:172.18.124.96 spt:500 dpt:500
OAK_QM exchange
oakley_process_quick_mode:
OAK_QM_AUTH_AWAITmap_alloc_entry: allocating entry 3
map_alloc_entry: allocating entry 4
ISAKMP (0): Creating IPSec SAs
        inbound SA from 172.18.173.85 to 172.18.124.96
          (proxy 10.0.3.0 to 10.0.25.0)
        has spi 304467548 and conn_id 3 and flags 25
        lifetime of 26400 seconds
        outbound SA from 172.18.124.96 to 172.18.173.85
          (proxy 10.0.25.0 to 10.0.3.0)
       has spi 4042487531 and conn_id 4 and flags 25
        lifetime of 26400 secondsIPSEC(key_engine): got a queue event...
IPSEC(initialize_sas): ,
  (key eng. msg.) dest= 172.18.124.96, src= 172.18.173.85,
   dest_proxy= 10.0.25.0/255.255.255.0/0/0 (type=4),
   src_proxy= 10.0.3.0/255.255.255.0/0/0 (type=4),
   protocol= ESP, transform= esp-3des esp-sha-hmac ,
   lifedur= 26400s and 0kb,
   spi= 0x1225ce5c(304467548), conn_id= 3,
      keysize= 0, flags= 0x25
IPSEC(initialize_sas): ,
  (key eng. msg.) src= 172.18.124.96, dest= 172.18.173.85,
    src_proxy= 10.0.25.0/255.255.255.0/0/0 (type=4),
   dest_proxy= 10.0.3.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= esp-3des esp-sha-hmac ,
    lifedur= 26400s and 0kb,
    spi= 0xf0f376eb(4042487531), conn_id= 4, keysize= 0, flags= 0x25
VPN Peer: IPSEC: Peer ip:172.18.173.85/500 Ref cnt
  incremented to:2 Total VPN Peers:1
VPN Peer: IPSEC: Peer ip:172.18.173.85/500 Ref cnt
   incremented to:3 Total VPN Peers:1
```

```
return status is IKMP_NO_ERROR
```

Informazioni correlate

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