Configurazione di un tunnel IPsec - Da router Cisco a firewall checkpoint 4.1

Sommario

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

Introduzione

In questo documento viene illustrato come formare un tunnel IPsec con chiavi già condivise per collegarsi a due reti private: la rete privata 192.168.1.x all'interno del router Cisco e la rete privata 10.32.50.x all'interno del firewall del checkpoint.

Prerequisiti

Requisiti

In questa configurazione di esempio si presume che il traffico tra il router e l'interno del checkpoint e diretto a Internet (rappresentato qui dalle reti 172.18.124.x) scorra prima dell'avvio della configurazione.

Componenti usati

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

Cisco 3600 router

- Software Cisco IOS® (C3640-JO3S56I-M), versione 12.1(5)T, SOFTWARE RELEASE (fc1)
- Checkpoint Firewall 4.1

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

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

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 questo documento, 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.

- <u>Configurazione router</u>
- <u>Configurazione di Checkpoint Firewall</u>

Configurazione router

Cisco 3600 Router Configuration Current configuration : 1608 bytes !

```
version 12.1
no service single-slot-reload-enable
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname cisco_endpoint
!
logging rate-limit console 10 except errors
ip subnet-zero
no ip finger
!
ip audit notify log
ip audit po max-events 100
1
!--- Internet Key Exchange (IKE) configuration crypto
isakmp policy 1
authentication pre-share
crypto isakmp key ciscorules address 172.18.124.157
!
!--- IPsec configuration crypto ipsec transform-set
rtpset esp-des esp-sha-hmac
crypto map rtp 1 ipsec-isakmp
set peer 172.18.124.157
set transform-set rtpset
match address 115
!
call rsvp-sync
cns event-service server
1
controller T1 1/0
1
controller T1 1/1
!
interface Ethernet0/0
ip address 172.18.124.35 255.255.250.240
ip nat outside
no ip mroute-cache
half-duplex
crypto map rtp
1
interface Ethernet0/1
ip address 192.168.1.1 255.255.255.0
ip nat inside
half-duplex
1
interface FastEthernet1/0
no ip address
shutdown
duplex auto
speed auto
1
ip kerberos source-interface any
ip nat pool INTERNET 172.18.124.36 172.18.124.36 netmask
255.255.255.240
ip nat inside source route-map nonat pool INTERNET
ip classless
ip route 0.0.0.0 0.0.0.0 172.18.124.34
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
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
!
dial-peer cor custom
!
line con 0
transport input none
line aux 0
line vty 0 4
login
!
end
```

Configurazione di Checkpoint Firewall

Completare la procedura seguente per configurare Checkpoint Firewall.

 Poiché la durata predefinita di IKE e IPsec varia a seconda del fornitore, selezionare Proprietà > Crittografia per impostare la durata del checkpoint in modo che corrisponda alle impostazioni predefinite di Cisco.La durata predefinita di IKE di Cisco è 86400 secondi (= 1440 minuti) e può essere modificata dai seguenti comandi:criterio crypto isakmp #durata #La durata configurabile di Cisco IKE è compresa tra 60 e 86400 secondi. La durata predefinita di IPSec di Cisco è 3600 secondi e può essere modificata dal comando crypto ipsec security-association lifetime seconds #.La durata configurabile di Cisco IPsec è compresa tra 120 e 86400

	Properties Setup			×
	High Availability Security Policy 1 Authentication	IP Pool NAT Acc Traffic Control Services SYNDefender LDAP	ess Lists Log and Alert Encryption	Desktop Security Security Servers ConnectControl
	SKIP Enable Export Change SKIP Ses Every 120 or Every 1048	table SKIP sion Key : Seconds (0 for infinity 5760 Butes (0 for infinity	Manual IF SPI alloc) <u>E</u> rom	PSEC ation range (hex):
	IKE Renegotiate I <u>K</u> E S Renegotiate I <u>P</u> SE	ecurity Associations every C Security Associations every	1440 3600	minutes seconds
econdi.	WordPad	🗱 Command Prompt	TTPI	CPVPN - Check

 Selezionare Gestisci > Oggetti di rete > Nuovo (o Modifica) > Rete per configurare l'oggetto per la rete interna (denominata "cpinside") dietro il checkpoint. In questo caso, la porta deve essere concordata con la rete di destinazione (seconda) indicata nel comando Cisco accesslist 115 allow ip 192.168.1.0.0.0.255 10.32.50.0 0.0.0.255. Selezionare Interno in

Network Properties
General NAT
<u>N</u> ame: cpinside
IP Address: 10.32.50.0 <u>G</u> et address
Net <u>M</u> ask: 255.255.255.0
Color:
Location: Broadcast: Disallowed
OK Cancel Help

 Selezionare Gestisci > Oggetti di rete > Modifica per modificare l'oggetto per l'endpoint di checkpoint (gateway) RTPVPN a cui punta il router Cisco nel comando set peer 172.18.124.157.Selezionare Interno in Posizione. Per Tipo, selezionare Gateway. In Moduli installati selezionare la casella di controllo VPN-1 e FireWall-1 e selezionare anche la casella di controllo Stazione di

Workstation P	operties			×
General Inter	faces SNMP N	IAT Certifical	tes VPN	Authe
<u>N</u> ame:	RTPCPVPN			
IP <u>A</u> ddress:	172.18.124.157		<u>G</u> et addr	ess
<u>C</u> omment:	Firewalled gatew	ay to internet		
Location:		Type:		<u>.</u>
• Intern	al () <u>E</u> xternal		iost 💌	Gate <u>w</u> ay
- Modules In	stalled			Get
	l & <u>F</u> ireWall-I	Version: 4.1		
	uate-1	Version: 4.1		
	icasion			
I ⊻ <u>M</u> ana	agement Station	Co <u>l</u> or:		•
	ОК	Cancel	Help	

4. Selezionare Gestisci > Oggetti di rete > Nuovo > Rete per configurare l'oggetto per la rete esterna (chiamata "inside_cisco") dietro il router Cisco.In questo caso, la licenza deve essere conforme alla rete di origine (prima) specificata nel comando Cisco access-list 115 allow ip 192.168.1.0.0.0.255 10.32.50.0.0.255.Selezionare Esterno in

Network Properties
General NAT
<u>Name:</u> inside_cisco
IP Address: 192.168.1.0
Net <u>M</u> ask: 255.255.255.0
Color:
Location: Broadcast:
○ Internal
UK Cancel Help

5. Selezionare Gestisci > Oggetti di rete > Nuovo > Workstation per aggiungere un oggetto per il gateway router Cisco esterno (chiamato "cisco_endpoint"). Questa è l'interfaccia Cisco a cui viene applicato il comando crypto map name.Selezionare Esterno in Posizione. Per Tipo, selezionare Gateway.Nota: non selezionare la casella di controllo VPN-1/FireWall-

Workstation Properties	×
General Interfaces SNMP N	IAT VPN
<u>N</u> ame: <mark>cisco_endpoint</mark>	
IP Address: 172.18.124.35	<u>G</u> et address
<u>C</u> omment:	
Location:	Type:
<u>Internal</u>	<u>O Host</u> O Gate <u>w</u> ay
Modules Installed	
VPN-1 & <u>F</u> ireWall-1	Version: 4.1 Cleg
FloodGate-1	Version: 4.1
Compre <u>s</u> sion	Version: 4.1
Management Station	Color:
OK	Cancel Help

6. Selezionare Gestisci > Oggetti di rete > Modifica per modificare la scheda VPN dell'endpoint del gateway del checkpoint (chiamata "RTPCPVPN"). In Dominio selezionare Altro, quindi selezionare dall'elenco a discesa l'interno della rete del checkpoint (denominata "cpinside"). In Definizione schemi di crittografia selezionare IKE, quindi fare clic su

Workstation Properties	×
General Interfaces SNMP NAT	Certificates VPN Authe
Domain: Disabled Valid Addresses(of Interfaces) Dither: Exportable for SecuRemote	Encryption schemes defined:
Traffic Control Logging	
Image: March M)g
OK Car	ncel Help

Modifica.

- 7. Modificare le proprietà IKE della crittografia DES in modo che corrispondano ai comandi seguenti: **criterio crypto isakmp #codificaNota:** la crittografia DES è l'impostazione predefinita, quindi non è visibile nella configurazione Cisco.
- 8. Modificare le proprietà IKE in hashing SHA1 per accettare i seguenti comandi:criterio crypto isakmp #hash shaNota: l'algoritmo hash SHA è l'impostazione predefinita e non è visibile nella configurazione Cisco.Cambia le impostazioni:Deselezionare Modalità aggressiva.Selezionare Supporta le subnet.Selezionare Segreto precondiviso in Metodo di autenticazione. Il risultato è conforme ai seguenti comandi:criterio crypto isakmp #pre-condivisione di

6	General Interfaces SNMP NAT Certificates VPN Authe	•
KE	Properties	>
G	General	
	Key Negotiation Encryption Method(s):Hash Method:	
	CAST	
	Authentication Method:	
	Pre-Shared Secret Edit Secrets	
	Public Key Signatures <u>Configure</u>	
	Europette Aggregius Made - El Supporte Submate	
	□ Supports Aggresive Mode V Supports Suphets	
autenticazione		

9. Fare clic su **Edit Secrets** (Modifica segreti) per impostare la chiave già condivisa in modo che concordi con il comando **crypto isakmp key** *key*

Workstation Properties
General Interfaces SNMP NAT Certificates VPN Authe
IKE Properties
General
Shared Secret
Shared Secrets List:
Peer Name Shared Secret
<u>E</u> dit <u>R</u> emove
OK Cancel
OK Cancel Help
OK Cancel Help

- address:
- Selezionare Gestisci > Oggetti di rete > Modifica per modificare la scheda VPN
 "cisco_endpoint". In Dominio, selezionare Altro, quindi selezionare l'interno della rete Cisco
 (chiamata "inside_cisco"). In Definizione schemi di crittografia selezionare IKE, quindi fare

General Interfaces SNMP NAT VPN Domain: Encryption schemes defined: Disabled Manual IPSEC Valid Addresses(of Interfaces) Manual IPSEC Dther: Manual IPSEC Inside_cisco SKIP Egportable for SecuRemote Edit	General Interfaces SNMP NAT VPN Domain: Disabled Valid Addresses(of Interfaces) Other: Image: Inside_cisco Image: Exportable for SecurRemote Traffic Control Logging Image: Ima	General Interfaces SNMP NAT VPN Domain:	orkstation Properties	
Domain: Encryption schemes defined: ○ Disabled Manual IPSEC ○ Valid Addresses(of Interfaces) Image: Manual IPSEC ○ Dther: Image: Manual IPSEC Image: Inside_cisco Image:	Domain: Disabled Valid Addresses(of Interfaces) Dther: Image: Inside_cisco Image: Inside_cisco<	Domain: Disabled Valid Addresses(of Interfaces) ther: inside_cisco Exportable for SecuPremote Traffic Control Logging Image: Interface Control Logging	General Interfaces SNMP NAT	VPN
Uther: Inside_cisco Exportable for SecuRemote Edit	Uther: Image: Skip Imag	Image: Control Logging Image: Traffic Control Logging Image: Traffic Control Logging Image: Traffic Control Logging	C Quiantian C Qui	Encryption <u>s</u> chemes defined: —
	Traffic Control Logging	Traffic Control Logging	<u>U</u> ther: <u>Inside_cisco</u> Exportable for SecuRemote	
■ Traffic Control Logging ■ <u>1</u> um on Traffic Control Logging			Traffic Control Logging ⊥um on Traffic Control Loggin	g

clic su Modifica.

- 11. Modificare la crittografia DES delle proprietà IKE per accettare i seguenti comandi:**criterio crypto isakmp #codificaNota:** la crittografia DES è l'impostazione predefinita, quindi non è visibile nella configurazione Cisco.
- 12. Modificare le proprietà IKE in hashing SHA1 per accettare i seguenti comandi:criterio crypto isakmp #hash shaNota: l'algoritmo hash SHA è l'impostazione predefinita e non è visibile nella configurazione Cisco.Cambia le impostazioni:Deselezionare Modalità aggressiva.Selezionare Supporta le subnet.Selezionare Segreto precondiviso in Metodo di autenticazione. Il risultato è conforme ai seguenti comandi:criterio crypto isakmp #pre-condivisione di

General Interfaces SNMP NAT Cer	ertificates VPN Authe
KE Properties 📐	2
General	
Key <u>N</u> egotiation Encryption Metho	od(s): - <u>H</u> ash Method: -
Authentication Method:	
I Pre-Shared Secret □ Public Key Signatures	Edit <u>S</u> ecrets <u>C</u> onfigure
Supports Aggresive <u>M</u> ode	Supports Su <u>b</u> nets
OK Cancel	Help
Itenticazione	

13. Fare clic su **Edit Secrets** (Modifica segreti) per impostare la chiave già condivisa in modo che concordi con il comando Cisco **crypto isakmp key** *key*

[IKE Properties	×
	General	
	Shared Secret ×	
	Shared Secrets List:	
	Peer Name Shared Secret	
	RTPCPVPN **** <u>E</u> dit	
	Bemove	
	OK Cancel	
		4
	OK Cancel Help	
address.		

14. Nella finestra Editor dei criteri inserire una regola con Origine e Destinazione come "inside_cisco" e "cpinside" (bidirezionale). Set **Service=Any**, **Action=Encrypt** e **Track=Long**.

1	RTPO	CPVPN - Check P	oint Policy Editor				_ 🗆 🗵
Ē	ile <u>E</u> di	it ⊻iew <u>M</u> anage	Policy <u>W</u> indow <u>H</u>	elp			
	- 5	🖪 🎗 🕒	E 💁 🕉 🕉	B. 🌮 🗽 😭	🗏 🖀 🖷 🖦	u, 🖡 🍽 📑	😓 🍸 🚯
	😫 Sec	urity Policy - Standard	🖥 🖶 Address Trans	slation - Standard 🛛 😿	Bandwidth Policy - St	andard	
	No.	Source	Destination	Service	Action	Track	In
ţ	1	👷 inside_cisco	👷 cpinside	Any	Encrypt	Long	6
jl.	•						•
F	or Help,	press F1		RTPC	PVPN Read	I/Write	1.

15. Fare clic sull'icona verde **Encrypt** e selezionare **Modifica proprietà** per configurare i criteri di crittografia sotto l'intestazione

AZIUNE.				
irity Policy - Standard 🛔	Address Translation -	Standard 🧱 Band	width Policy - Standard	^
∼ FVV1 Host	∼ Ldap-Servers	19 Idap	accept	
∼ FVV1 Host	∼ Logical-Servers	∼ load_agent	accept	5
💼 inside_cisco	문화 cpinside 문화 inside_cisco	Any	dit properties	hg .
~~		ICMD at at an and	Remove Encryption	
		gen dest-unreach	Edit Encryption	
		echo-reply		
		icmp isome meete	accept	
		icmp-proto		
		imp info reply	(PROF) drop	
Anu	a Any	icmp mask ranky		
	- Any	icmp mack request	🔟 🧲 reject	
•				

16. Selezionare IKE, quindi fare clic su

	Encryption Properties	×
	General Encryption schemes defined:	
Modifica	OK Cancel Help	

17. Nella finestra Proprietà IKE modificare queste proprietà in modo che corrispondano alle trasformazioni IPsec di Cisco nel comando crypto ipsec transform-set rtpset esp-des espsha-hmac:In Trasforma, selezionare Crittografia + integrità dei dati (ESP). L'algoritmo di crittografia deve essere DES, l'integrità dei dati SHA1 e il gateway peer consentito deve essere il gateway del router esterno (chiamato "cisco endpoint"). Fare clic su

IKE Pro	perties	X
Genera	al	
R	 <u>I</u>ransform: ⊙ Encryption + Data Integrity (ESP) ○ Data Integrity Only (AH) 	
-	Encryption Algorithm: DES	
	Data Integrity SHA1	
	Allowed Peer Gateway:	
	Use Perfect Forward Secrecy	
	OK Cancel Help	

18. Dopo aver configurato il checkpoint, selezionare **Criterio > Installa** nel menu del checkpoint per rendere effettive le modifiche.

Verifica

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

funzioni correttamente.

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**.

- show crypto isakmp sa: visualizza tutte le associazioni di sicurezza IKE (SA) correnti in un peer.
- **show crypto ipsec sa**: visualizza le impostazioni utilizzate dalle associazioni di protezione correnti.

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 di debug sui motori di crittografia, che eseguono la crittografia e la decrittografia.
- debug crypto isakmp: visualizza i messaggi sugli eventi IKE.
- debug crypto ipsec: visualizza gli eventi IPsec.
- clear crypto isakmp: cancella tutte le connessioni IKE attive.
- clear crypto sa: cancella tutte le SA IPsec.

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 il router non è configurato per corrispondere, è probabile che il tunnel non riesca. 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.

Checkpoint

Poiché il rilevamento è stato impostato per Long nella finestra Editor dei criteri, il traffico negato dovrebbe essere visualizzato in rosso nel Visualizzatore log. Per ottenere un debug più dettagliato, usare:

C:\WINNT\FW1\4.1\fwstop C:\WINNT\FW1\4.1\fw d -d e in un'altra finestra: Utilizzare i seguenti comandi per cancellare le associazioni di protezione sul checkpoint:

fw tab -t IKE_SA_table -x
fw tab -t ISAKMP_ESP_table -x
fw tab -t inbound_SPI -x
fw tab -t ISAKMP_AH_table -x
Rispondere sì al questionario..

Output di esempio del comando debug

```
Configuration register is 0x2102
```

```
cisco_endpoint#debug crypto isakmp
Crypto ISAKMP debugging is on
cisco_endpoint#debug crypto isakmp
Crypto IPSEC debugging is on
cisco_endpoint#debug crypto engine
Crypto Engine debugging is on
cisco_endpoint#
20:54:06: IPSEC(sa_request): ,
  (key eng. msg.) src= 172.18.124.35, dest= 172.18.124.157,
    src_proxy= 192.168.1.0/255.255.255.0/0/0 (type=4),
    dest_proxy= 10.32.50.0/255.255.255.0/0/0 (type=4),
   protocol= ESP, transform= esp-des esp-sha-hmac ,
   lifedur= 3600s and 4608000kb,
    spi= 0xA29984CA(2727969994), conn_id= 0, keysize= 0, flags= 0x4004
20:54:06: ISAKMP: received ke message (1/1)
20:54:06: ISAKMP: local port 500, remote port 500
20:54:06: ISAKMP (0:1): beginning Main Mode exchange
20:54:06: ISAKMP (0:1): sending packet to 172.18.124.157 (I) MM_NO_STATE
20:54:06: ISAKMP (0:1): received packet from 172.18.124.157 (I) MM_NO_STATE
20:54:06: ISAKMP (0:1): processing SA payload. message ID = 0
20:54:06: ISAKMP (0:1): found peer pre-shared key matching 172.18.124.157
20:54:06: ISAKMP (0:1): Checking ISAKMP transform 1 against priority 1 policy
20:54:06: ISAKMP: encryption DES-CBC
20:54:06: ISAKMP:hash SHA20:54:06: ISAKMP:default group 120:54:06: ISAKMP:auth pre-share
20:54:06: ISAKMP (0:1): atts are acceptable. Next payload is 0
20:54:06: CryptoEngine0: generate alg parameter
20:54:06: CRYPTO_ENGINE: Dh phase 1 status: 0
20:54:06: CRYPTO_ENGINE: Dh phase 1 status: 0
20:54:06: ISAKMP (0:1): SA is doing pre-shared key authentication
   using id type ID_IPV4_ADDR
20:54:06: ISAKMP (0:1): sending packet to 172.18.124.157 (I) MM_SA_SETUP
20:54:06: ISAKMP (0:1): received packet from 172.18.124.157 (I) MM_SA_SETUP
20:54:06: ISAKMP (0:1): processing KE payload. message ID = 0
20:54:06: CryptoEngine0: generate alg parameter
20:54:06: ISAKMP (0:1): processing NONCE payload. message ID = 0
20:54:06: ISAKMP (0:1): found peer pre-shared key matching 172.18.124.157
20:54:06: CryptoEngine0: create ISAKMP SKEYID for conn id 1
20:54:06: ISAKMP (0:1): SKEYID state generated
20:54:06: ISAKMP (1): ID payload
        next-payload : 8
        type : 1
                   : 17
        protocol
        port
                     : 500
                     : 8
        length
20:54:06: ISAKMP (1): Total payload length: 12
```

```
20:54:06: CryptoEngine0: generate hmac context for conn id 1
20:54:06: ISAKMP (0:1): sending packet to 172.18.124.157 (I) MM_KEY_EXCH
20:54:06: ISAKMP (0:1): received packet from 172.18.124.157 (I) MM_KEY_EXCH
20:54:06: ISAKMP (0:1): processing ID payload. message ID = 0
20:54:06: ISAKMP (0:1): processing HASH payload. message ID = 0
20:54:06: CryptoEngine0: generate hmac context for conn id 1
20:54:06: ISAKMP (0:1): SA has been authenticated with 172.18.124.157
20:54:06: ISAKMP (0:1): beginning Quick Mode exchange, M-ID of 1855173267
20:54:06: CryptoEngine0: generate hmac context for conn id 1
20:54:06: ISAKMP (0:1): sending packet to 172.18.124.157 (I) QM_IDLE
20:54:06: CryptoEngine0: clear dh number for conn id 1
20:54:06: ISAKMP (0:1): received packet from 172.18.124.157 (I) QM_IDLE
20:54:06: CryptoEngine0: generate hmac context for conn id 1
20:54:06: ISAKMP (0:1): processing HASH payload. message ID = 1855173267
20:54:06: ISAKMP (0:1): processing SA payload. message ID = 1855173267
20:54:06: ISAKMP (0:1): Checking IPSec proposal 1
20:54:06: ISAKMP: transform 1, ESP_DES
20:54:06: ISAKMP: attributes in transform:
20:54:06:ISAKMP:encaps is 120:54:06:ISAKMP:SA life type in seconds20:54:06:ISAKMP:SA life duration (basic) of 360020:54:06:ISAKMP:SA life type in kilobytes20:54:06:ISAKMP:SA life duration (VPI) of 0x0 0x46 0x50 0x020:54:06:ISAKMP:authenticator is HMAC-SHA
20:54:06: validate proposal 0
20:54:06: ISAKMP (0:1): atts are acceptable.
20:54:06: IPSEC(validate_proposal_request): proposal part #1,
  (key eng. msg.) dest= 172.18.124.157, src= 172.18.124.35,
    dest_proxy= 10.32.50.0/255.255.255.0/0/0 (type=4),
    src_proxy= 192.168.1.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= esp-des esp-sha-hmac ,
    lifedur= 0s and 0kb,
    spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
20:54:06: validate proposal request 0
20:54:06: ISAKMP (0:1): processing NONCE payload. message ID = 1855173267
20:54:06: ISAKMP (0:1): processing ID payload. message ID = 1855173267
20:54:06: ISAKMP (0:1): processing ID payload. message ID = 1855173267
20:54:06: CryptoEngine0: generate hmac context for conn id 1
20:54:06: ipsec allocate flow 0
20:54:06: ipsec allocate flow 0
20:54:06: ISAKMP (0:1): Creating IPSec SAs
                  inbound SA from 172.18.124.157 to 172.18.124.35
20:54:06:
        (proxy 10.32.50.0 to 192.168.1.0)
20:54:06: has spi 0xA29984CA and conn_id 2000 and flags 4
20:54:06:
                  lifetime of 3600 seconds
20:54:06:
                  lifetime of 4608000 kilobytes
20:54:06:
                  outbound SA from 172.18.124.35
                                                    to 172.18.124.157
   (proxy 192.168.1.0 to 10.32.50.0)
20:54:06:
                 has spi 404516441 and conn_id 2001 and flags 4
20:54:06:
                  lifetime of 3600 seconds
                  lifetime of 4608000 kilobytes
20:54:06:
20:54:06: ISAKMP (0:1): sending packet to 172.18.124.157 (I) QM_IDLE
20:54:06: ISAKMP (0:1): deleting node 1855173267 error FALSE reason ""
20:54:06: IPSEC(key_engine): got a queue event...
20:54:06: IPSEC(initialize_sas): ,
  (key eng. msg.) dest= 172.18.124.35, src= 172.18.124.157,
    dest_proxy= 192.168.1.0/255.255.255.0/0/0 (type=4),
    src_proxy= 10.32.50.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= esp-des esp-sha-hmac ,
    lifedur= 3600s and 4608000kb,
    spi= 0xA29984CA(2727969994), conn_id= 2000, keysize= 0, flags= 0x4
20:54:06: IPSEC(initialize_sas): ,
  (key eng. msg.) src= 172.18.124.35, dest= 172.18.124.157,
    src_proxy= 192.168.1.0/255.255.255.0/0/0 (type=4),
```

```
dest_proxy= 10.32.50.0/255.255.255.0/0/0 (type=4),
   protocol= ESP, transform= esp-des esp-sha-hmac ,
   lifedur= 3600s and 4608000kb,
    spi= 0x181C6E59(404516441), conn_id= 2001, keysize= 0, flags= 0x4
20:54:06: IPSEC(create_sa): sa created,
  (sa) sa_dest= 172.18.124.35, sa_prot= 50,
    sa_spi= 0xA29984CA(2727969994),
    sa_trans= esp-des esp-sha-hmac , sa_conn_id= 2000
20:54:06: IPSEC(create_sa): sa created,
  (sa) sa_dest= 172.18.124.157, sa_prot= 50,
    sa_spi= 0x181C6E59(404516441),
    sa_trans= esp-des esp-sha-hmac , sa_conn_id= 2001
cisco_endpoint#sho cry ips sa
interface: Ethernet0/0
   Crypto map tag: rtp, local addr. 172.18.124.35
   local ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (10.32.50.0/255.255.255.0/0/0)
   current_peer: 172.18.124.157
    PERMIT, flags={origin_is_acl,}
    #pkts encaps: 14, #pkts encrypt: 14, #pkts digest 14
    #pkts decaps: 14, #pkts decrypt: 14, #pkts verify 14
    #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.: 172.18.124.35, remote crypto endpt.: 172.18.124.157
     path mtu 1500, media mtu 1500
     current outbound spi: 181C6E59
     inbound esp sas:
     spi: 0xA29984CA(2727969994)
       transform: esp-des esp-sha-hmac ,
       in use settings ={Tunnel, }
       slot: 0, conn id: 2000, flow_id: 1, crypto map: rtp
                         sa timing: remaining key lifetime (k/sec):
 --More--
    (4607998/3447)
       IV size: 8 bytes
       replay detection support: Y
     inbound ah sas:
     inbound pcp sas:
     outbound esp sas:
     spi: 0x181C6E59(404516441)
       transform: esp-des esp-sha-hmac ,
       in use settings ={Tunnel, }
       slot: 0, conn id: 2001, flow_id: 2, crypto map: rtp
       sa timing: remaining key lifetime (k/sec): (4607997/3447)
       IV size: 8 bytes
       replay detection support: Y
     outbound ah sas:
     outbound pcp sas:
cisco_endpoint#show crypto isakmp sa
   dst src state
                                          conn-id slot
172.18.124.157 172.18.124.35 QM_IDLE
                                             1
                                                       0
```

Informazioni correlate

- Negoziazione IPSec/protocolli IKE
- <u>Configurazione della protezione di rete IPsec</u>
- <u>Configurazione del protocollo di protezione di Internet Key Exchange</u>
- Documentazione e supporto tecnico Cisco Systems