

Esempio di configurazione di IPsec tra due router IOS con reti private sovrapposte

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Convenzioni](#)

[Configurazione](#)

[Esempio di rete](#)

[Configurazioni](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Informazioni correlate](#)

[Introduzione](#)

In questo documento viene descritto come configurare il router Cisco IOS in una VPN IPsec da sito a sito con indirizzi di rete privati sovrapposti dietro i gateway VPN.

[Prerequisiti](#)

[Requisiti](#)

Nessun requisito specifico previsto per questo documento.

[Componenti usati](#)

Per questo documento, sono stati usati router Cisco IOS 3640 con software versione 12.4.

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 [Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti](#).

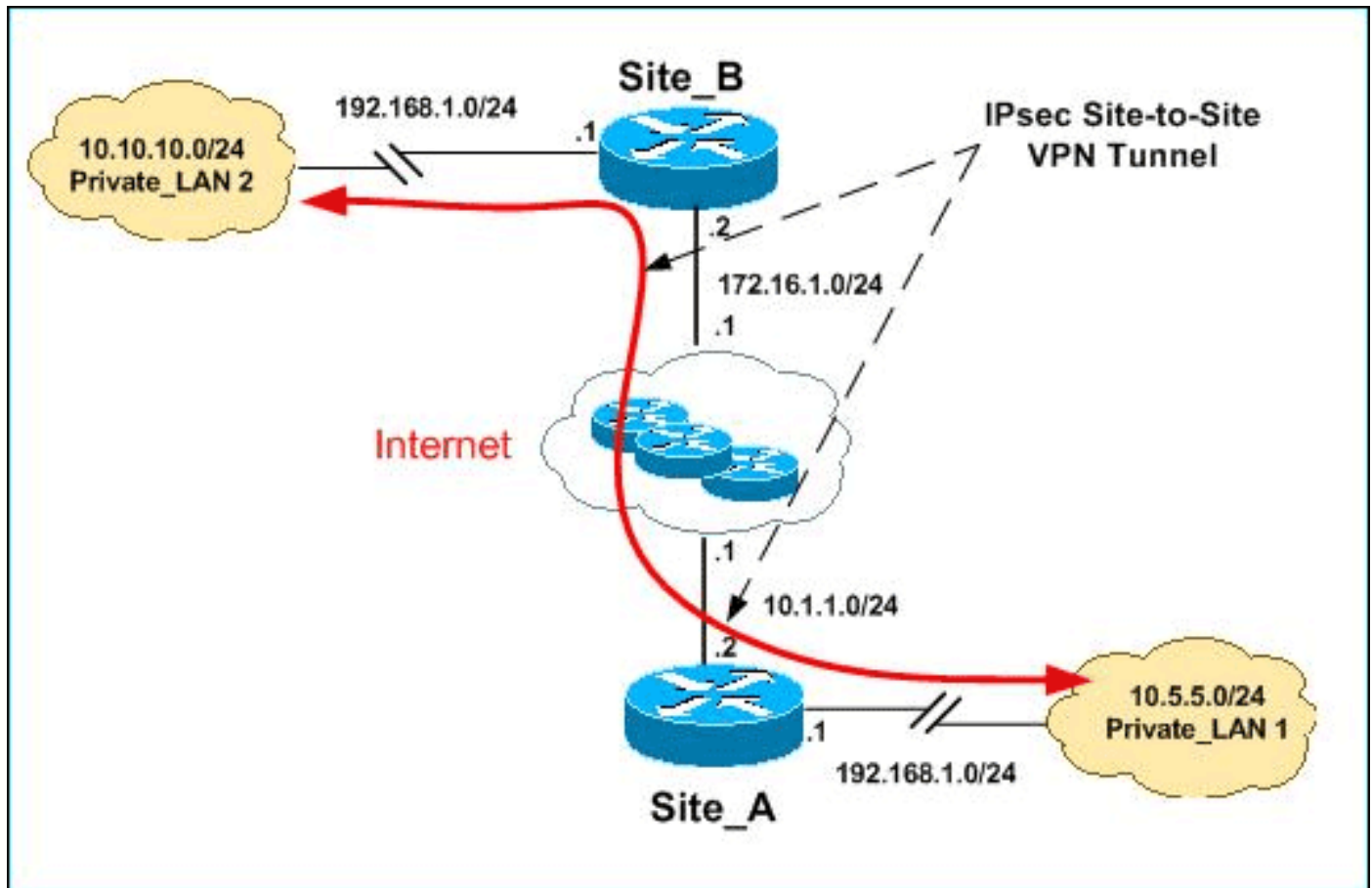
Configurazione

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 [strumento di ricerca](#) dei comandi (solo utenti [registrati](#)).

Esempio di rete

Nel documento viene usata questa impostazione di rete:



Nota: gli schemi di indirizzamento IP utilizzati in questa configurazione non sono legalmente instradabili su Internet. Si tratta degli indirizzi RFC 1918 utilizzati in un ambiente lab.

Sia Private_LAN1 che Private_LAN2 dispongono di una subnet IP di 192.168.1.0/24. In questo modo viene simulato lo spazio di indirizzi sovrapposto dietro ogni lato del tunnel IPsec.

Nell'esempio, il router Site_A esegue una conversione bidirezionale in modo che le due LAN private possano comunicare attraverso il tunnel IPsec. La conversione indica che per Private_LAN1 il valore di Private_LAN2 è 10.10.10.0/24 tramite il tunnel IPsec e per Private_LAN2 il valore di Private_LAN1 è 10.5.5.0/24 tramite il tunnel IPsec.

Configurazioni

Nel documento vengono usate queste configurazioni:

- [Configurazione SDM router A sito](#)
- [Configurazione CLI router A sito](#)
- [Configurazione router sito B](#)

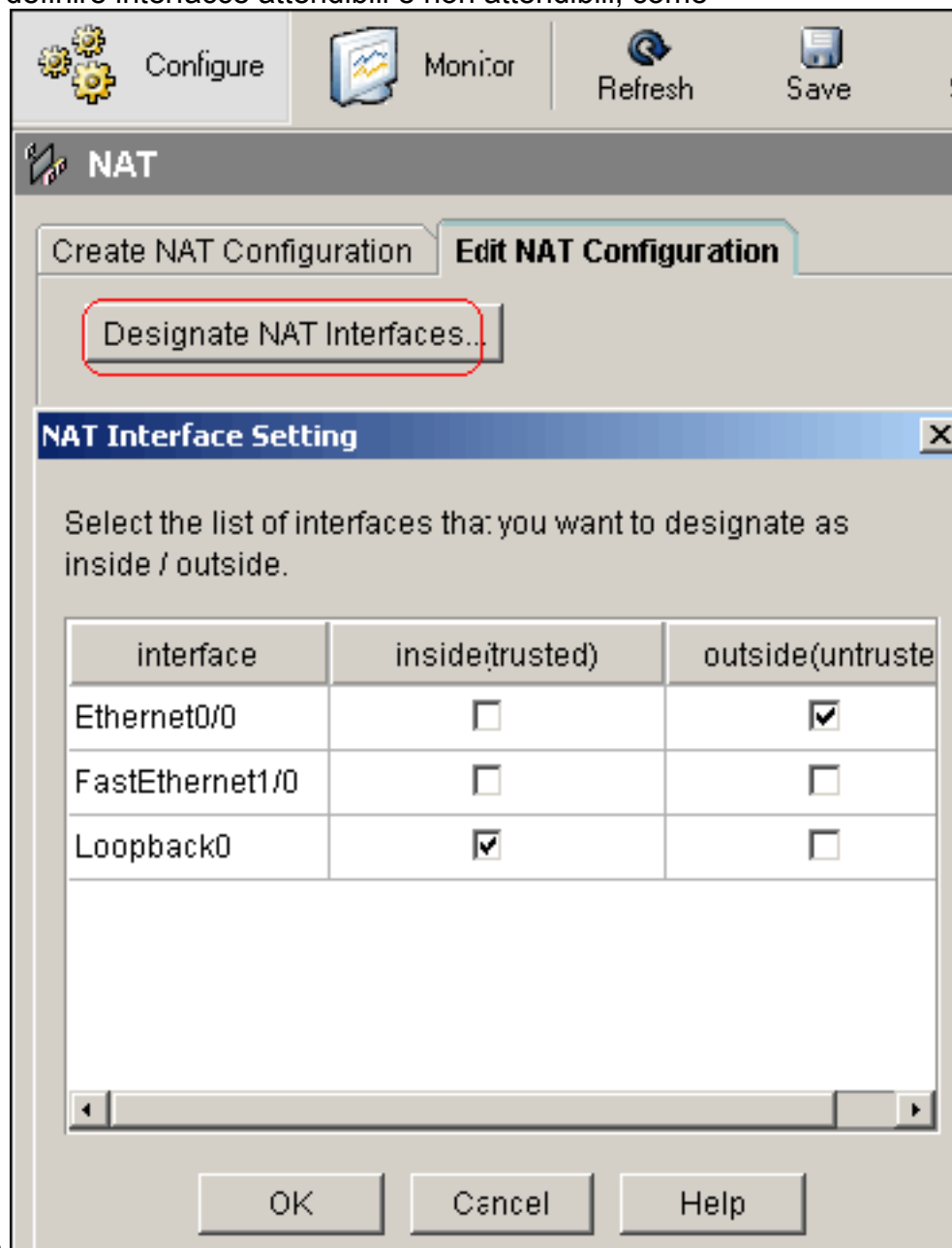
[Configurazione SDM router A sito](#)

Nota: in questo documento si presume che il router sia configurato con impostazioni di base come la configurazione dell'interfaccia, ecc. Per ulteriori informazioni, fare riferimento a [Configurazione base del router con SDM](#).

Configurazione NAT

Per utilizzare NAT per configurare il modello SDM sul router Site_A, completare la procedura seguente:

1. Scegliere **Configura > NAT > Modifica configurazione NAT** e fare clic su **Designa interfacce NAT** per definire interfacce attendibili e non attendibili, come



mostrato.

2. Fare clic su **OK**.

3. Per configurare la conversione NAT dall'interno all'esterno, fare clic su **Add** (Aggiungi) come

Add Address Translation Rule

Static Dynamic

Direction: From inside to outside

Translate from interface

Inside Interface(s): Loopback0

IP address: 192.168.1.0

Network Mask(optional): 255.255.255.0 or 24

Translate to interface

Outside Interface(s): Ethernet0/0

Type: IP address

Interface: Ethernet0/0

IP address: 10.5.5.0

Redirect Port

TCP UDP

Original Port: Translated Port:

OK Cancel Help

mostrato.

4. Fare clic su **OK**.

Network Address Translation Rules

Inside Interface(s): Loopback0

Outside Interface(s): Ethernet0/0

Original address	Translated address	Rule Type
192.168.1.0-192.168.1.255	10.5.5.0-10.5.5.255	Static

Add...

5. Ancora una volta, fare clic su **Add** (Aggiungi) per configurare la conversione NAT dall'esterno verso l'interno, come

Add Address Translation Rule

Static Dynamic

Direction: From outside to inside

Translate from interface

Outside Interface(s): Ethernet0/0

IP address: 10.10.10.0

Network Mask(optional): 255.255.255.0 or 24

Translate to interface

Inside Interface(s): Loopback0

IP address: 192.168.1.0

Redirect Port

TCP UDP

Original Port: Translated Port:

OK Cancel Help

mostrato.

- Fare clic su **OK**.

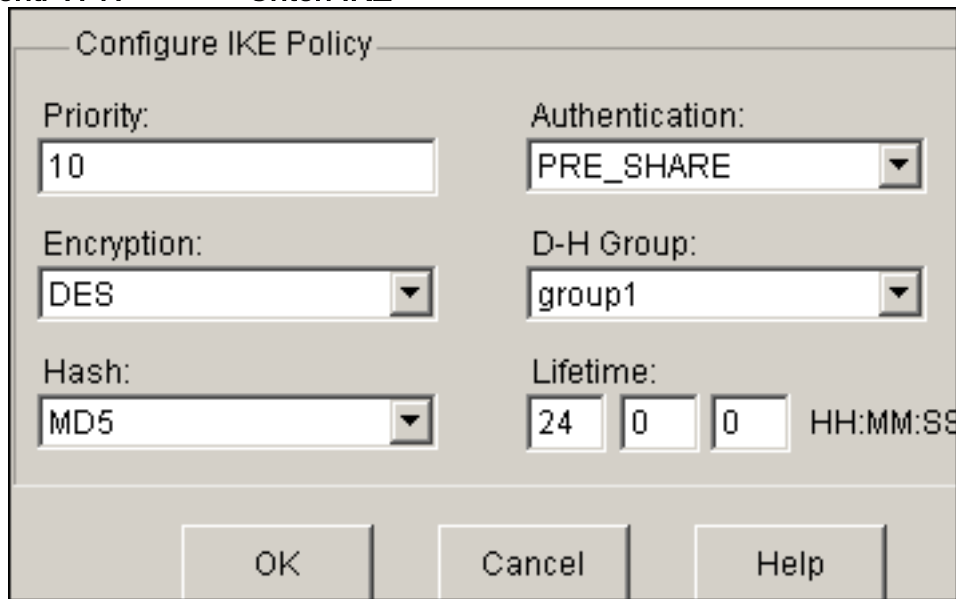
Network Address Translation Rules			
Inside Interface(s):		Loopback0	
Outside Interface(s):		Ethernet0/0	
	Original address	Translated address	Rule Type
	192.168.1.0-192.168.1.255	10.5.5.0-10.5.5.255	Static
	192.168.1.0-192.168.1.255	10.10.10.0-10.10.10.255	Static

Nota: ecco la configurazione CLI equivalente:

Configurazione VPN

Per utilizzare la VPN per configurare il modello SDM sul router Site_A, completare la procedura seguente:

1. Per definire i criteri IKE come mostrato in questa immagine, scegliere **Configura > VPN > Componenti VPN > IKE > Criteri IKE >**



Configure IKE Policy

Priority: 10

Authentication: PRE_SHARE

Encryption: DES

D-H Group: group1

Hash: MD5

Lifetime: 24 0 0 HH:MM:SS

OK Cancel Help

Aggiungi.

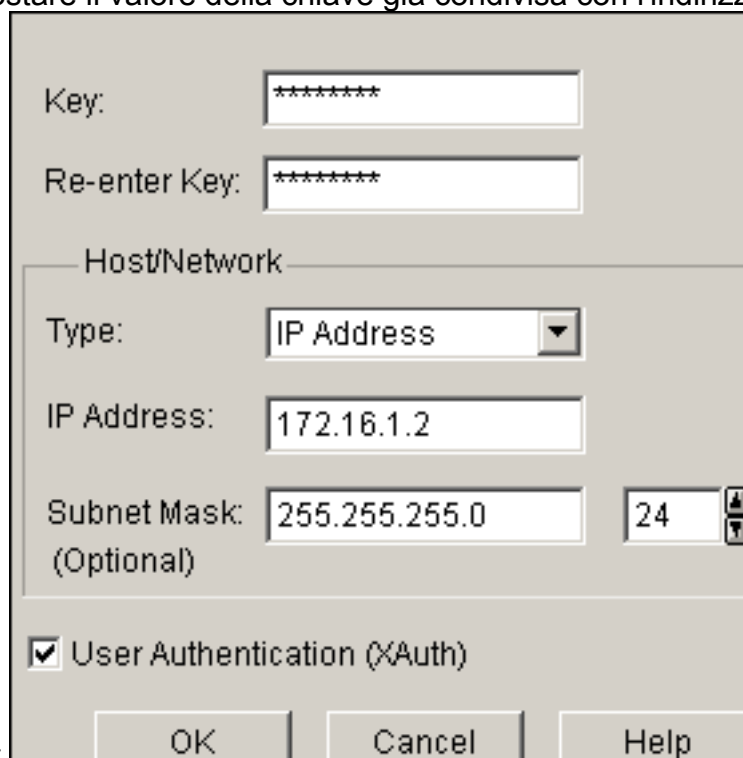
2. Fare clic su **OK**.



Priority	Encryption	Hash	D-H Group	Authentication	Type
10	DES	MD5	group1	PRE SHARE	User Defined

Nota: ecco la configurazione CLI equivalente:

3. Scegliere **Configura > VPN > Componenti VPN > IKE > Chiavi già condivise > Aggiungi** per impostare il valore della chiave già condivisa con l'indirizzo IP del



Key: *****

Re-enter Key: *****

Host/Network

Type: IP Address

IP Address: 172.16.1.2

Subnet Mask: 255.255.255.0 24

(Optional)

User Authentication (XAuth)

OK Cancel Help

peer.

4. Fare clic su **OK**.

Pre-shared Keys			Add...
Peer IP/Name	Subnet Mask	pre-shared key	
172.16.1.2	255.255.255.0	*****	

Nota: ecco la configurazione CLI equivalente:

- Scegliere **Configura > VPN > Componenti VPN > IPSec > Set di trasformazioni > Aggiungi** per creare un set di trasformazioni *myset* come mostrato in questa

immagine.

- Fare clic su **OK**.

Transform Set				Add...
Name	ESP Encryption	ESP Integrity	AH Integrity	
myset	ESP_DES	ESP_MD5_HMAC		

Nota: ecco la configurazione CLI equivalente:

- Per creare un Access Control List (ACL) crittografico di *101*, scegliere **Configura > VPN > Componenti VPN > IPSec > Regole IPSec (ACL) >**

Add a Rule

Name/Number: Type:

Description:

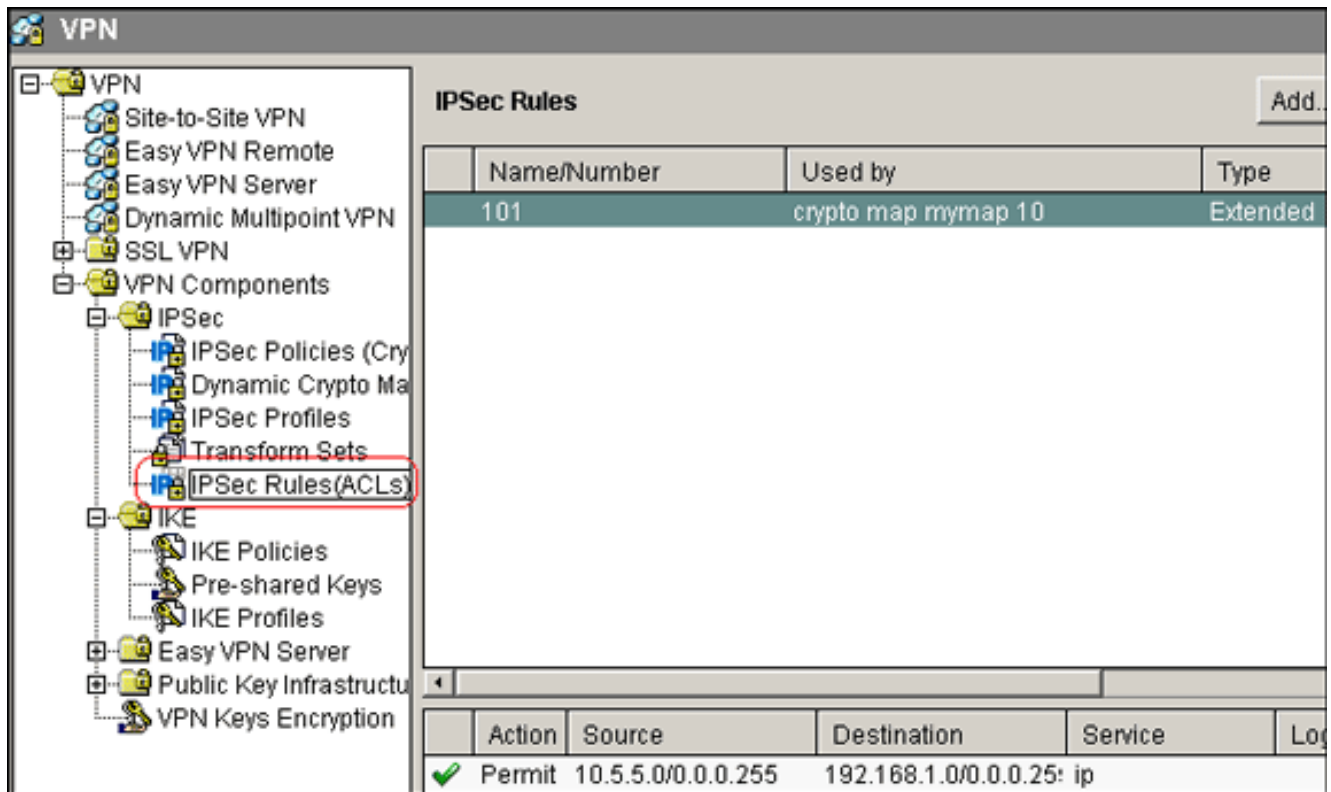
Rule Entry

```
permit ip 10.5.5.0 0.255.255.255 192.168.1.0 0.255.
```

Interface Association
None.

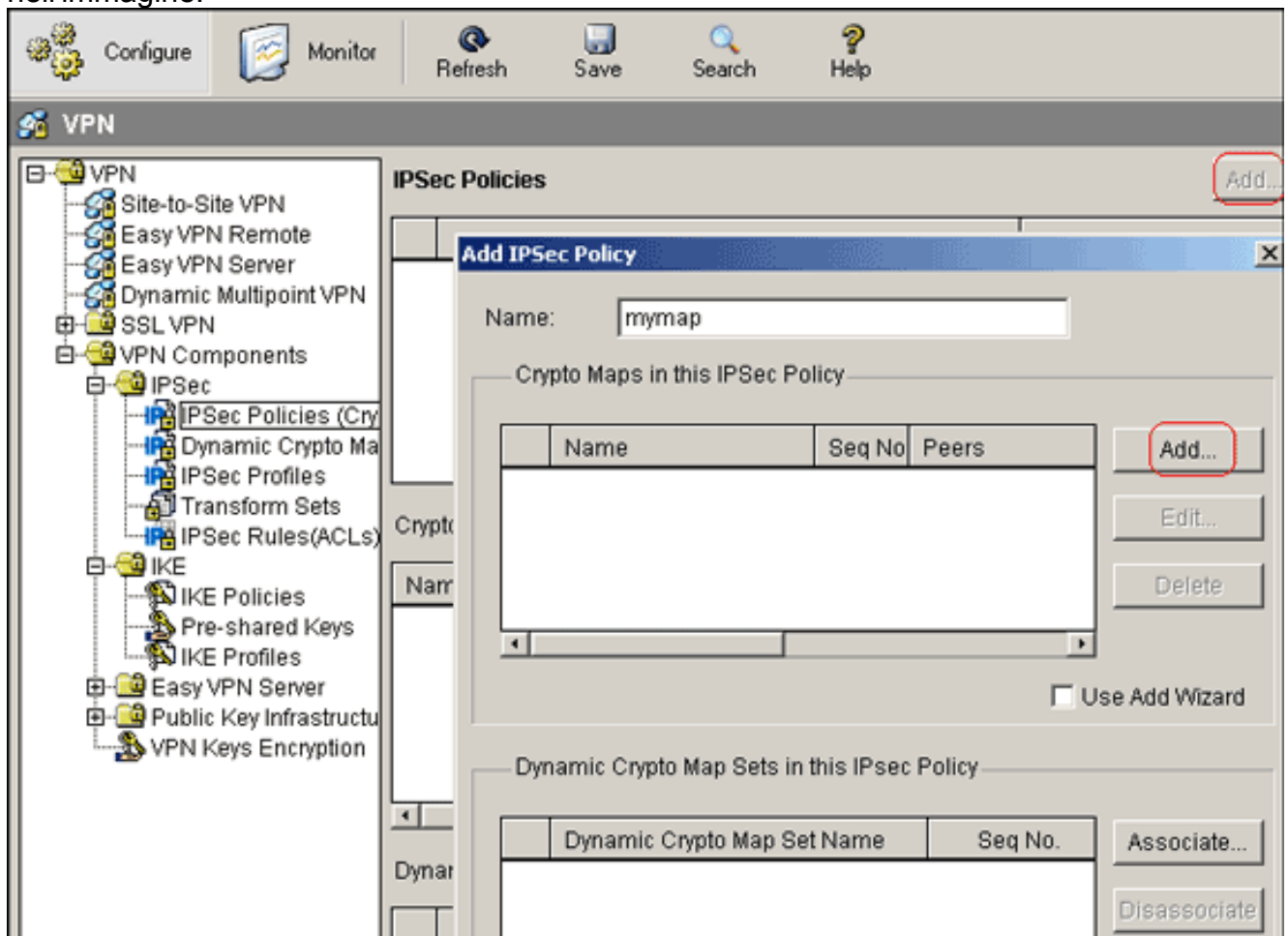
Aggiungi.

8. Fare clic su **OK**.



Nota: ecco la configurazione CLI equivalente:

- Scegliere **Configura > VPN > Componenti VPN > IPsec > Criteri IPsec > Aggiungi** per creare una mappa crittografica di *mymap*, come mostrato nell'immagine.



- Fare clic su **Add**. Fare clic sulla scheda **General** (Generale) e mantenere le impostazioni

Add Crypto Map

General Peer Information Transform Sets IPsec Rule

Name of IPsec Policy: mymap

Description:

Sequence Number: 1

Security Association Lifetime:
1 0 0 HH:MM:SS 4608000 Kilobytes

Idle Time:
HH:MM:SS

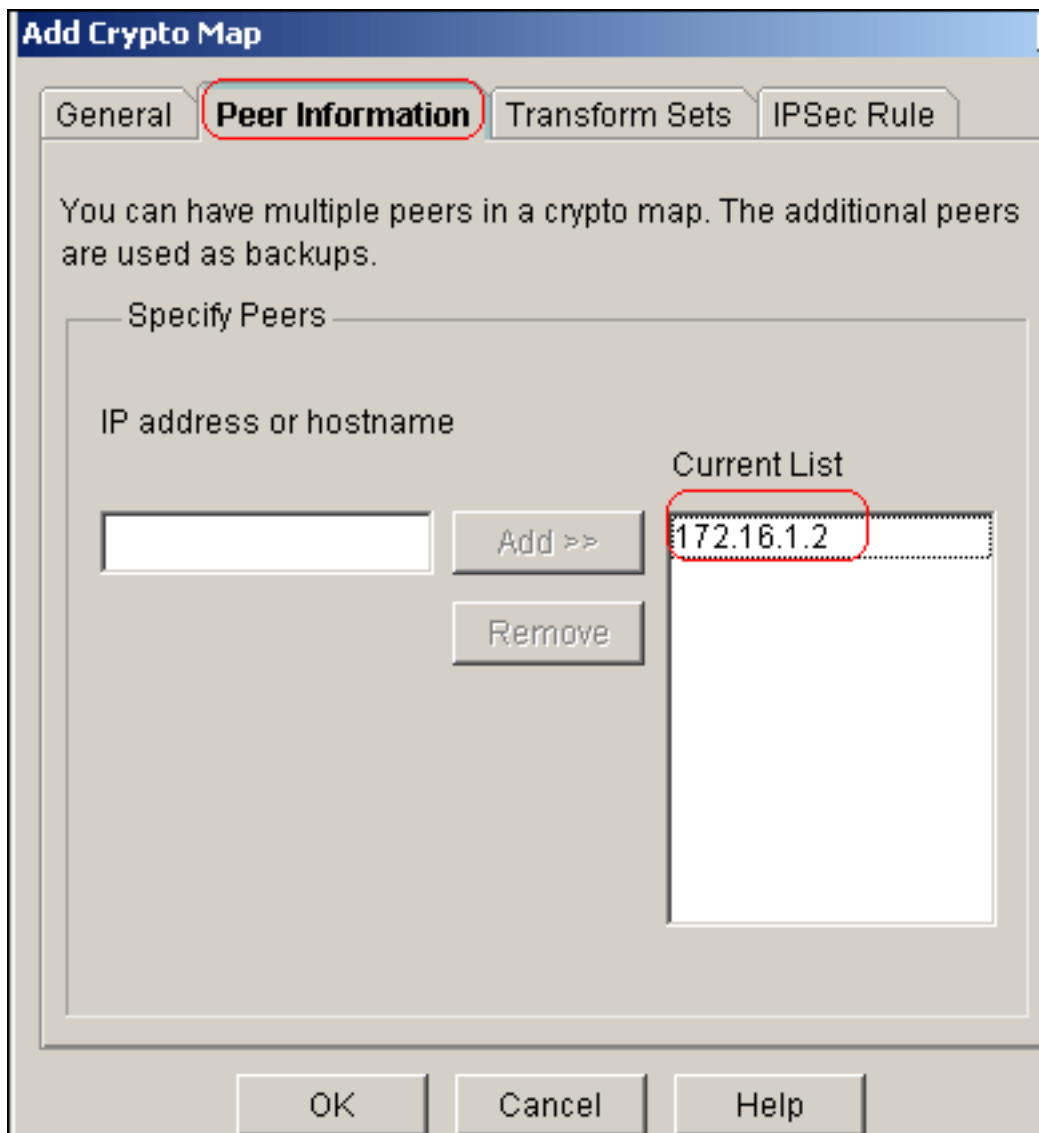
Perfect Forward Secrecy group1

Reverse Route Injection

OK Cancel Help

predefinite.

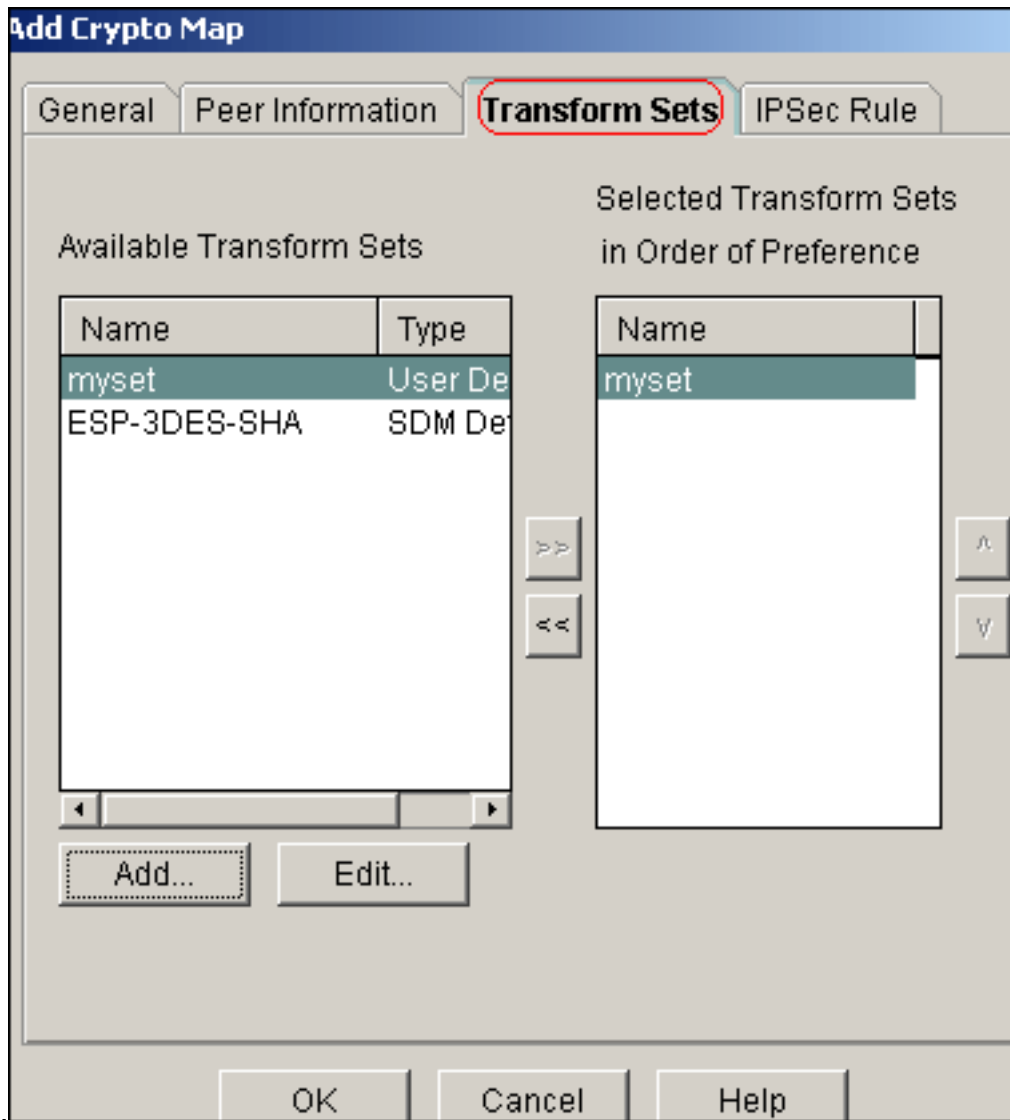
Fare clic sulla scheda **Peer Information** (Informazioni peer) per aggiungere l'indirizzo IP del peer



172.16.1.2.

Fare

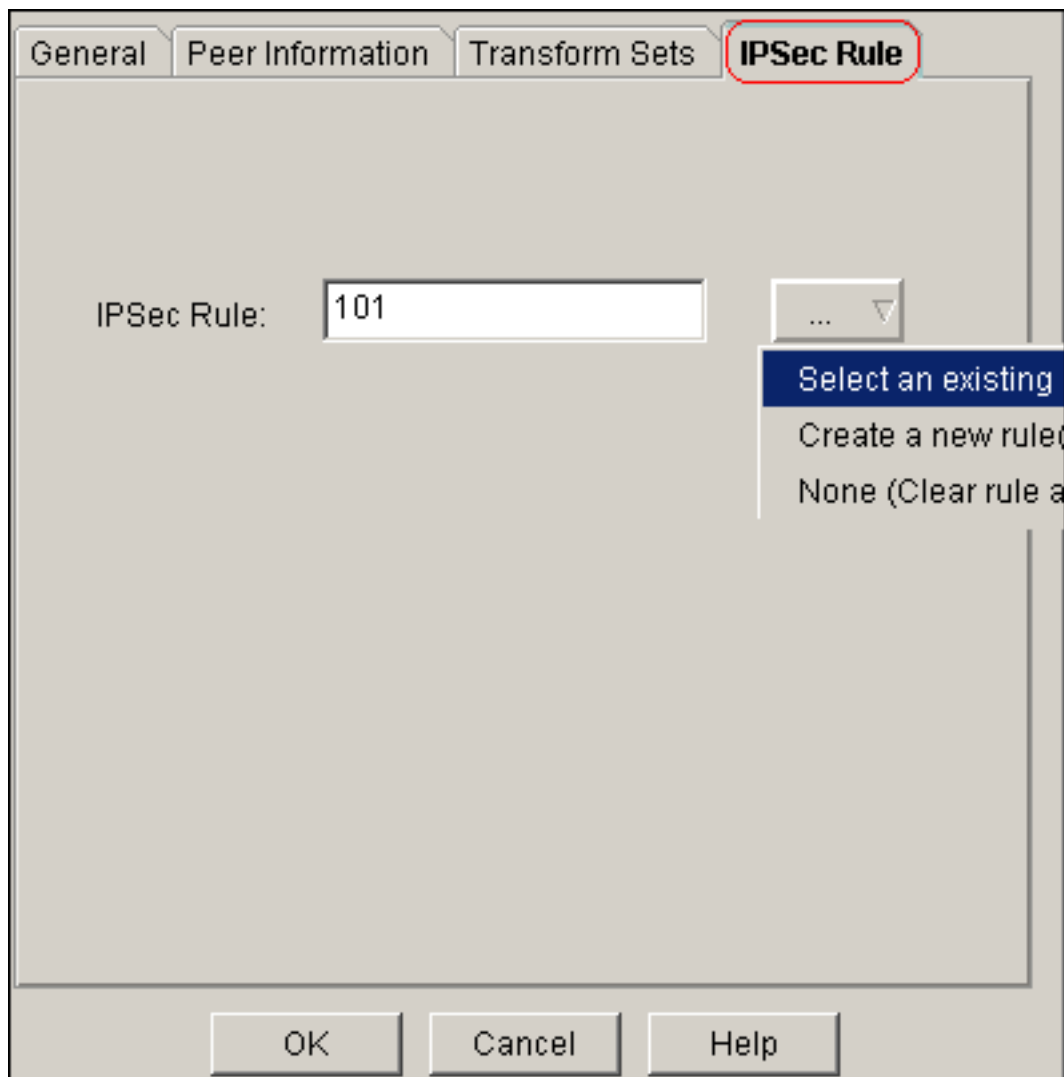
clic sulla scheda **Set di trasformazioni** per selezionare il set di trasformazioni *myset*



desiderato.

selezionare l'ACL crittografico esistente 101, fare clic sulla scheda **IPSec**

Per

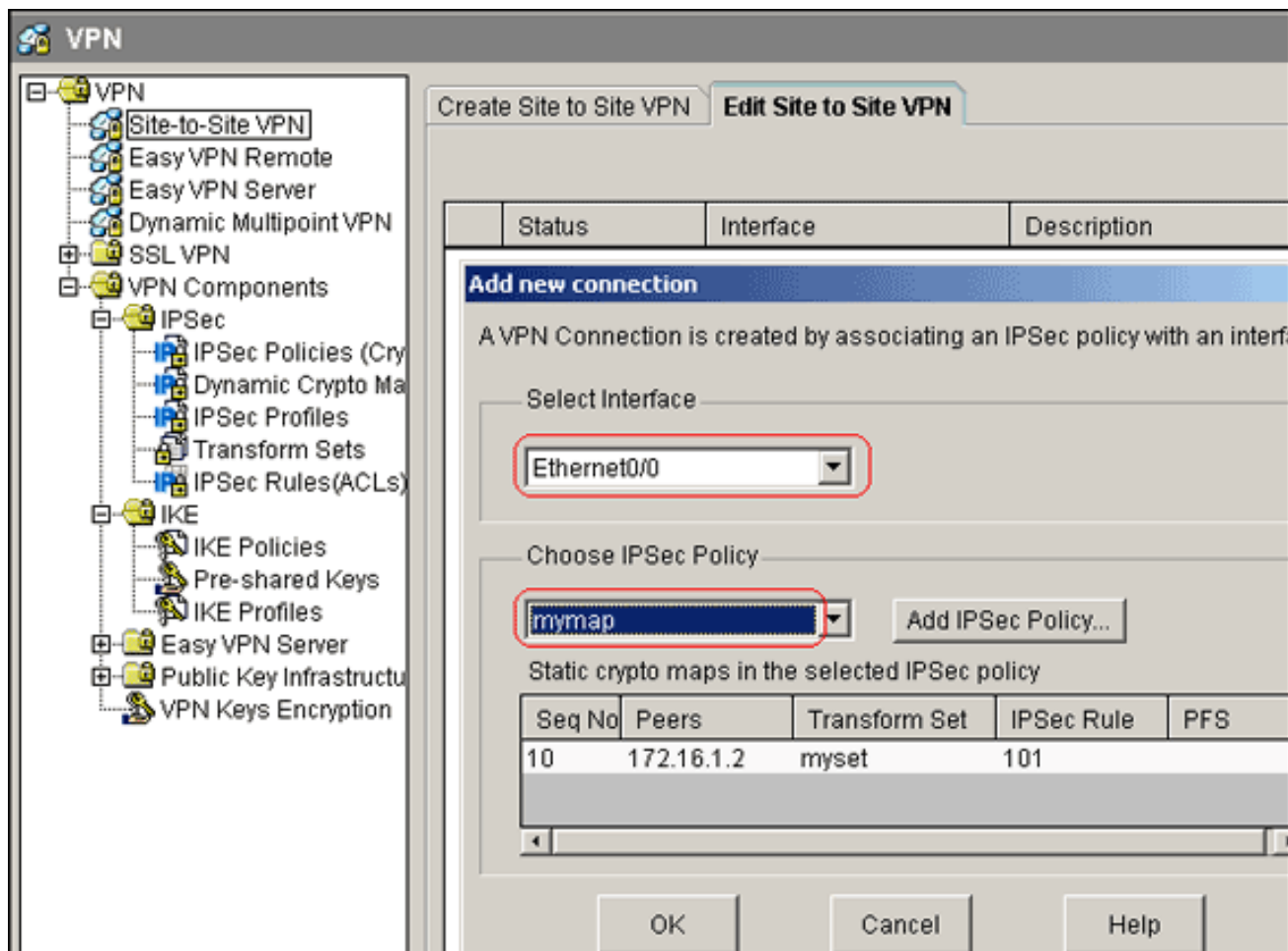


Rule.

Fare clic su

OK.Nota: ecco la configurazione CLI equivalente:

11. Scegliere **Configura > VPN > VPN da sito a sito > Modifica VPN da sito a sito > Aggiungi** per applicare la mappa crittografica *mymap* all'interfaccia Ethernet0/0.



12. Fare clic su **OK**. **Nota:** ecco la configurazione CLI equivalente:

[Configurazione CLI router A sito](#)

```

Router sito_A

Site_A#show running-config
*Sep 25 21:15:58.954: %SYS-5-CONFIG_I: Configured from console by console
Building configuration...

Current configuration : 1545 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Site_A
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
!
resource policy
!
!
!
ip cef

```

```

!
!
crypto isakmp policy 10
  hash md5
  authentication pre-share
!--- Defines ISAKMP policy. crypto isakmp key 6 L2L12345
address 172.16.1.2 255.255.255.0

!--- Defines pre-shared secret used for IKE
authentication !! crypto ipsec transform-set myset esp-
des esp-md5-hmac
!--- Defines IPSec encryption and authentication
algorithms. ! crypto map mymap 10 ipsec-isakmp
  set peer 172.16.1.2
  set transform-set myset
  match address 101
!--- Defines crypto map. !!!! interface Loopback0 ip
address 192.168.1.1 255.255.255.0 ip nat inside
  ip virtual-reassembly
!
interface Ethernet0/0
  ip address 10.1.1.2 255.255.255.0
  ip nat outside
  ip virtual-reassembly
  half-duplex
  crypto map mymap
!--- Apply crypto map on the outside interface. !! !---
Output Suppressed ! ip http server no ip http secure-
server ! ip route 0.0.0.0 0.0.0.0 10.1.1.1
!
ip nat inside source static network 192.168.1.0 10.5.5.0
/24

!--- Static translation defined to translate
Private_LAN1 !--- from 192.168.1.0/24 to 10.5.5.0/24. !-
-- Note that this translation is used for both !--- VPN
and Internet traffic from Private_LAN1. !--- A routable
global IP address range, or an extra NAT !--- at the ISP
router (in front of Site_A router), is !--- required if
Private_LAN1 also needs internal access. ip nat outside
source static network 192.168.1.0 10.10.10.0 /24

!--- Static translation defined to translate
Private_LAN2 !--- from 192.168.1.0/24 to 10.10.10.0/24.
! access-list 101 permit ip 10.5.5.0 0.0.0.255
192.168.1.0 0.0.0.255

!--- Defines IPSec interesting traffic. !--- Note that
the host behind Site_A router communicates !--- to
Private_LAN2 using 10.10.10.0/24. !--- When the packets
arrive at the Site_A router, they are first !---
translated to 192.168.1.0/24 and then encrypted by
IPSec. !! control-plane !! line con 0 line aux 0 line
vty 0 4 !! end Site_A#

```

Configurazione CLI router Site B

Router sito_B

```

Site_B#show running-config
Building configuration...

```

```

Current configuration : 939 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Site_B
!
!
ip subnet-zero
!
!
crypto isakmp policy 10
  hash md5
  authentication pre-share
crypto isakmp key L2L12345 address 10.1.1.2
255.255.255.0
!
!
crypto ipsec transform-set myset esp-des esp-md5-hmac
!
crypto map mymap 10 ipsec-isakmp
  set peer 10.1.1.2
  set transform-set myset
  match address 101
!
!
!
!
interface Ethernet0
 ip address 192.168.1.1 255.255.255.0
!
interface Ethernet1
 ip address 172.16.1.2 255.255.255.0
  crypto map mymap
!
!--- Output Suppressed ! ip classless ip route 0.0.0.0
0.0.0.0 172.16.1.1
ip http server
!
access-list 101 permit ip 192.168.1.0 0.0.0.255 10.5.5.0
0.0.0.255
!
line con 0
line aux 0
line vty 0 4
!
end

Site_B#

```

Verifica

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

Lo [strumento Output Interpreter](#) (solo utenti [registrati](#)) (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 (SA) IKE (Internet Key Exchange) correnti in un peer.

```
Site_A#show crypto isakmp sa
dst          src          state          conn-id slot status
172.16.1.2   10.1.1.2     QM_IDLE        1      0 ACTIVE
```

- **show crypto isakmp sa detail:** visualizza i dettagli di tutte le associazioni di protezione IKE correnti in un peer.

```
Site_A#show crypto isakmp sa detail
Codes: C - IKE configuration mode, D - Dead Peer Detection
       K - Keepalives, N - NAT-traversal
       X - IKE Extended Authentication
       psk - Preshared key, rsig - RSA signature
       renc - RSA encryption
```

```
C-id Local          Remote          I-VRF          Status Encr Hash Auth DH Lifetime
Cap.
1     10.1.1.2         172.16.1.2     ACTIVE des  md5  psk  1  23:59:42
```

```
Connection-id:Engine-id = 1:1(software)
```

- **show crypto ipsec sa:** visualizza le impostazioni utilizzate dalle associazioni di protezione correnti.

```
Site_A#show crypto ipsec sa
```

```
interface: Ethernet0/0
Crypto map tag: mymap, local addr 10.1.1.2

protected vrf: (none)
local ident (addr/mask/prot/port): (10.5.5.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
current_peer 172.16.1.2 port 500
  PERMIT, flags={origin_is_acl,}
#pkts encaps: 2, #pkts encrypt: 2, #pkts digest: 2
#pkts decaps: 2, #pkts decrypt: 2, #pkts verify: 2
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 3, #recv errors 0

local crypto endpt.: 10.1.1.2, remote crypto endpt.: 172.16.1.2
path mtu 1500, ip mtu 1500, ip mtu idb Ethernet0/0
current outbound spi: 0x1A9CDC0A(446487562)

inbound esp sas:
spi: 0x99C7BA58(2580003416)
  transform: esp-des esp-md5-hmac ,
  in use settings ={Tunnel, }
  conn id: 2002, flow_id: SW:2, crypto map: mymap
  sa timing: remaining key lifetime (k/sec): (4478520/3336)
  IV size: 8 bytes
  replay detection support: Y
  Status: ACTIVE

inbound ah sas:

inbound pcp sas:

outbound esp sas:
spi: 0x1A9CDC0A(446487562)
  transform: esp-des esp-md5-hmac ,
  in use settings ={Tunnel, }
```

```
conn id: 2001, flow_id: SW:1, crypto map: mymap
sa timing: remaining key lifetime (k/sec): (4478520/3335)
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE
```

outbound ah sas:

outbound pcp sas:

Site_A#

- **show ip nat translation:** visualizza le informazioni sullo slot di conversione.

Site_A#**show ip nat translations**

Pro	Inside global	Inside local	Outside local	Outside global
---	---	---	10.10.10.1	192.168.1.1
---	---	---	10.10.10.0	192.168.1.0
---	10.5.5.1	192.168.1.1	---	---
---	10.5.5.0	192.168.1.0	---	---

- **show ip nat statistics:** visualizza informazioni statistiche sulla traduzione.

Site_A#**show ip nat statistics**

Total active translations: 4 (2 static, 2 dynamic; 0 extended)

Outside interfaces:

Ethernet0/0

Inside interfaces:

Loopback0

Hits: 42 Misses: 2

CEF Translated packets: 13, CEF Punted packets: 0

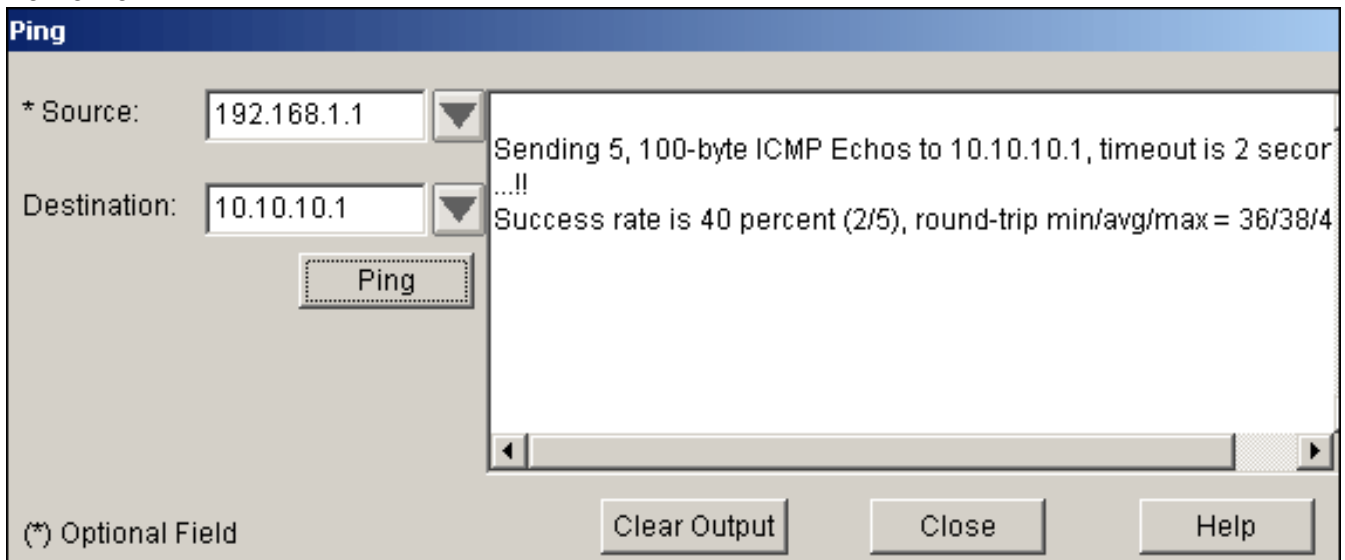
Expired translations: 7

Dynamic mappings:

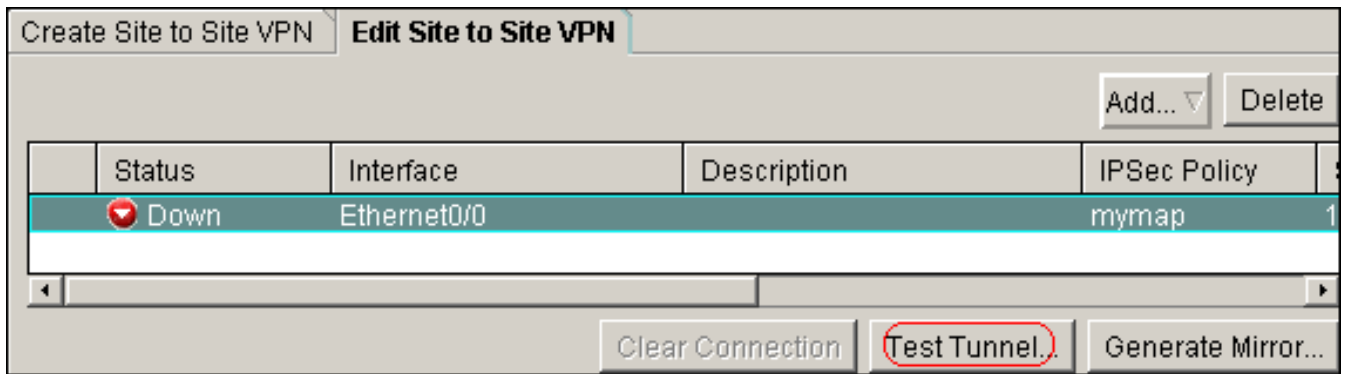
Queued Packets: 0

Site_A#

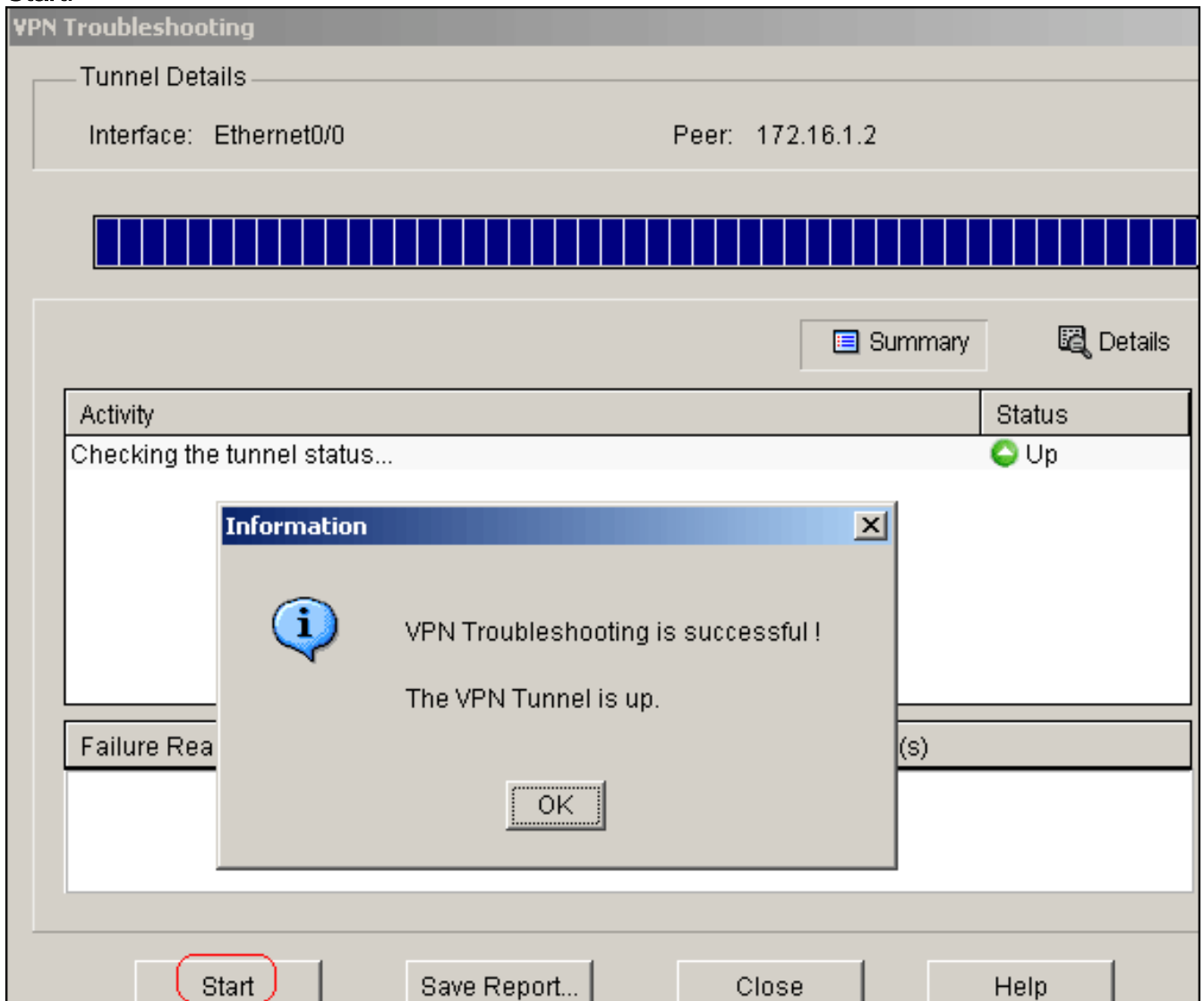
- Per verificare la connessione, completare i seguenti passaggi: In SDM, selezionare **Strumenti** > **Ping** per stabilire il tunnel VPN IPsec con l'IP di origine come 192.168.1.1 e l'IP di destinazione come 10.10.10.1.



Fare clic su **Test tunnel** per verificare che il tunnel VPN IPsec sia stato stabilito come mostrato in questa immagine.



Fare clic su
Start.



Risoluzione dei problemi

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

```
Site_A#debug ip packet
IP packet debugging is on
Site_A#ping
Protocol [ip]:
Target IP address: 10.10.10.1
```

```
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 192.168.1.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.1.1
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 40/45/52 ms
Site_A#
*Sep 30 18:08:10.601: IP: tableid=0, s=192.168.1.1 (local), d=10.10.10.1 (Ethernet0/0), routed via FIB
*Sep 30 18:08:10.601: IP: s=192.168.1.1 (local), d=10.10.10.1 (Ethernet0/0), len 100, sending
*Sep 30 18:08:10.641: IP: tableid=0, s=10.10.10.1 (Ethernet0/0), d=192.168.1.1 (Loopback0), routed via RIB
*Sep 30 18:08:10.641: IP: s=10.10.10.1 (Ethernet0/0), d=192.168.1.1, len 100, rcvd 4
*Sep 30 18:08:10.645: IP: tableid=0, s=192.168.1.1 (local), d=10.10.10.1 (Ethernet0/0), routed via FIB
*Sep 30 18:08:10.645: IP: s=192.168.1.1 (local), d=10.10.10.1 (Ethernet0/0), len 100, sending
*Sep 30 18:08:10.685: IP: tableid=0, s=10.10.10.1 (Ethernet0/0), d=192.168.1.1 (Loopback0), routed via RIB
*Sep 30 18:08:10.685: IP: s=10.10.10.1 (Ethernet0/0), d=192.168.1.1, len 100, rcvd 4
*Sep 30 18:08:10.685: IP: tableid=0, s=192.168.1.1 (local), d=10.10.10.1 (Ethernet0/0), routed via FIB
*Sep 30 18:08:10.689: IP: s=192.168.1.1 (local), d=10.10.10.1 (Ethernet0/0), len 100, sending
*Sep 30 18:08:10.729: IP: tableid=0, s=10.10.10.1 (Ethernet0/0), d=192.168.1.1 (Loopback0), routed via RIB
*Sep 30 18:08:10.729: IP: s=10.10.10.1 (Ethernet0/0), d=192.168.1.1, len 100, rcvd 4
*Sep 30 18:08:10.729: IP: tableid=0, s=192.168.1.1 (local), d=10.10.10.1 (Ethernet0/0), routed via FIB
*Sep 30 18:08:10.729: IP: s=192.168.1.1 (local), d=10.10.10.1 (Ethernet0/0), len 100, sending
*Sep 30 18:08:10.769: IP: tableid=0, s=10.10.10.1 (Ethernet0/0), d=192.168.1.1 (Loopback0), routed via RIB
*Sep 30 18:08:10.769: IP: s=10.10.10.1 (Ethernet0/0), d=192.168.1.1, len 100, rcvd 4
*Sep 30 18:08:10.773: IP: tableid=0, s=192.168.1.1 (local), d=10.10.10.1 (Ethernet0/0), routed via FIB
*Sep 30 18:08:10.773: IP: s=192.168.1.1 (local), d=10.10.10.1 (Ethernet0/0), len 100, sending
*Sep 30 18:08:10.813: IP: tableid=0, s=10.10.10.1 (Ethernet0/0), d=192.168.1.1 (Loopback0), routed via RIB
*Sep 30 18:08:10.813: IP: s=10.10.10.1 (Ethernet0/0), d=192.168.1.1, len 100, rcvd 4
```

[Informazioni correlate](#)

- [Soluzioni per la risoluzione dei problemi più comuni di VPN IPsec di L2L e ad accesso remoto](#)
- [Esempio di configurazione di IPsec tra ASA/PIX e Cisco VPN 3000 Concentrator con reti](#)

private sovrapposte

- Documentazione e supporto tecnico – Cisco Systems