

IPSec entre dos routers IOS con el ejemplo de configuración de las redes privadas superpuestas

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Configurar](#)

[Diagrama de la red](#)

[Configuraciones](#)

[Verificación](#)

[Troubleshooting](#)

[Información Relacionada](#)

[Introducción](#)

Este documento describe cómo configurar al router del Cisco IOS en IPSec sitio a sitio un VPN con los direccionamientos de red privada superpuesta detrás de los gateways de VPN.

[prerrequisitos](#)

[Requisitos](#)

No hay requisitos específicos para este documento.

[Componentes Utilizados](#)

La información en este documento se basa en los Cisco IOS 3640 Router que funcionan con la versión de software 12.4.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

[Convenciones](#)

Consulte [Convenciones de Consejos Técnicos de Cisco](#) para obtener más información sobre las convenciones sobre documentos.

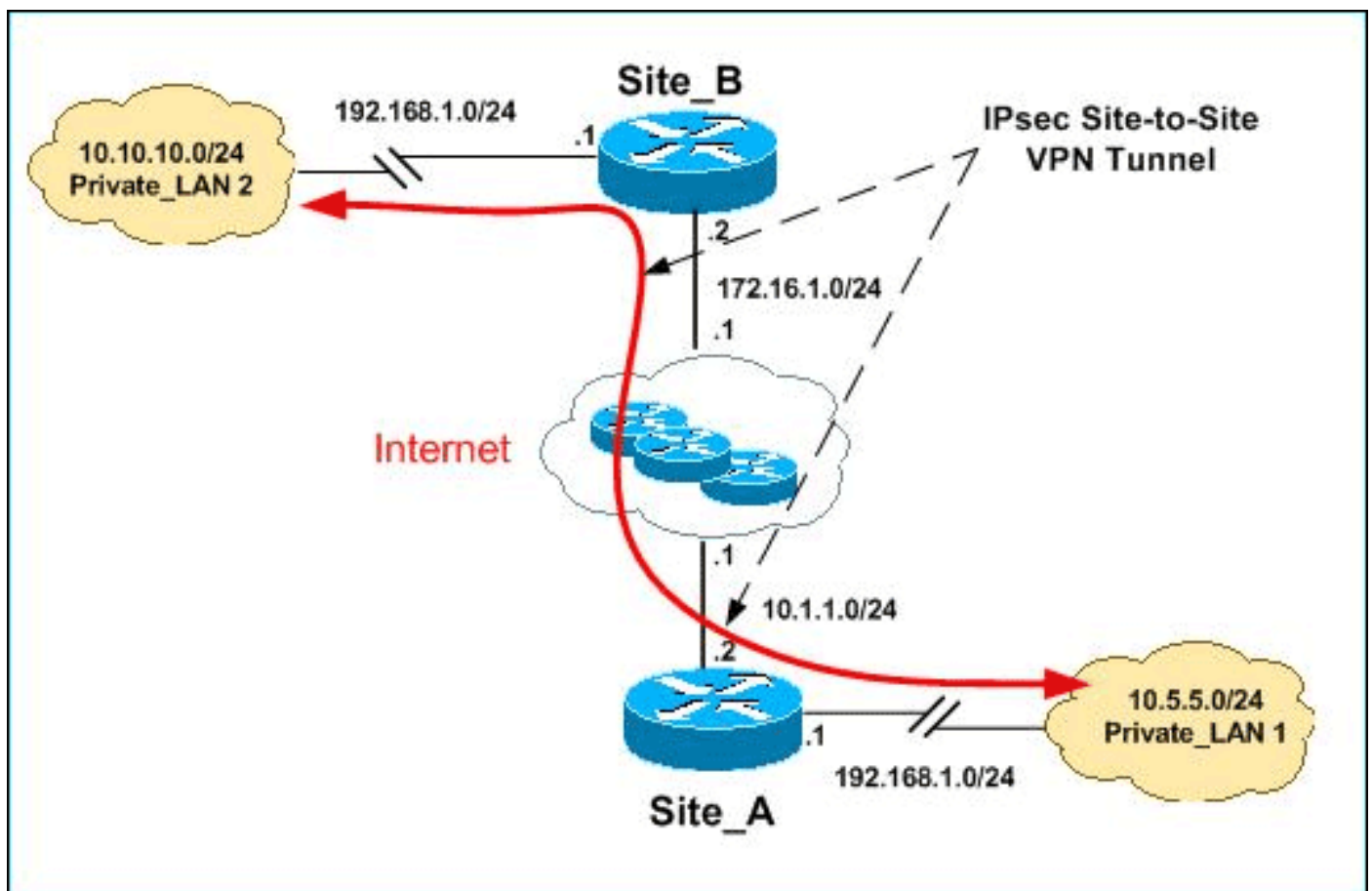
Configurar

En esta sección encontrará la información para configurar las funciones descritas en este documento.

Nota: Utilice la herramienta [Command Lookup Tool](#) ([clientes registrados solamente](#)) para obtener más información sobre los comandos utilizados en esta sección.

Diagrama de la red

En este documento, se utiliza esta configuración de red:



Nota: Los esquemas de direccionamiento IP usados en esta configuración no son legalmente enrutables en Internet. Son las direcciones RFC1918 que se han utilizado en un entorno de laboratorio.

El Private_LAN1 y Private_LAN2 tienen una subred IP de 192.168.1.0/24. Esto simula el espacio de dirección superpuesta detrás de cada lado del túnel IPsec.

En este ejemplo, el router del Site_A realiza una traducción bidireccional de modo que los dos LAN privados puedan comunicarse sobre el túnel IPsec. La traducción significa que el Private_LAN1 "ve" Private_LAN2 como 10.10.10.0/24 a través del túnel IPsec, y Private_LAN2 "ve" el Private_LAN1 como 10.5.5.0/24 a través del túnel IPsec.

Configuraciones

En este documento, se utilizan estas configuraciones:

- [Configuración de SDM del router del Site A](#)
- [Configuración CLI del router del Site A](#)
- [Configuración del router del Site B](#)

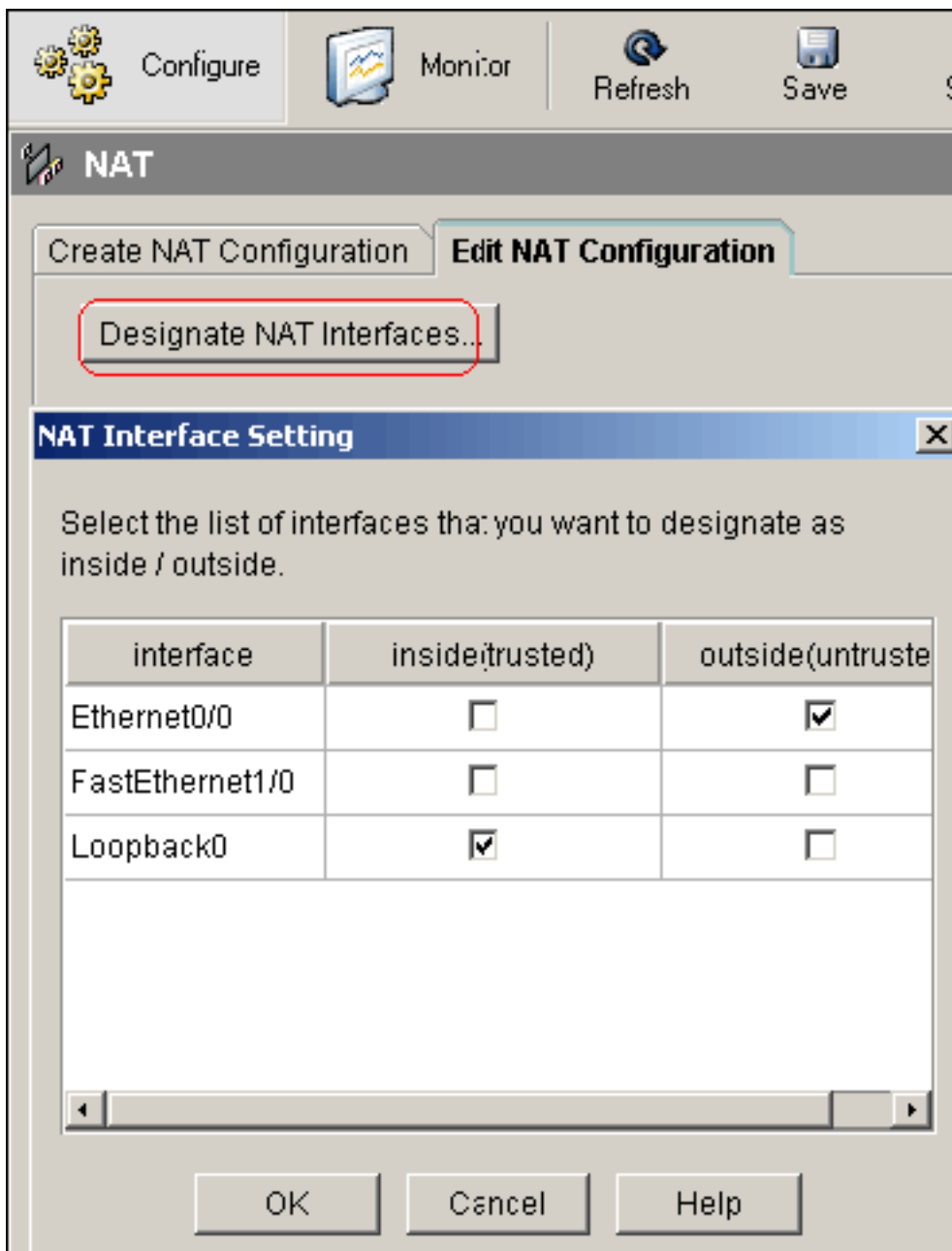
Configuración de SDM del router del Site A

Nota: Este documento asume que configuran al router con las configuraciones básicas como la configuración de la interfaz, etc. refiere a la [configuración básica del router usando el SDM](#) para más información.

Configuración de NAT

Complete estos pasos para utilizar el NAT para configurar el SDM en el router del Site_A:

1. Elija la **configuración > el NAT > editan la configuración del NAT**, y hacen clic las **interfaces designadas NAT** para definir confiado en y las interfaces no confiables como se



muestra.

2. Haga clic en OK.
3. El tecleo **agrega** para configurar la traducción de NAT desde adentro a la dirección exterior como se

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

muestra.

- Haga clic en OK.

Network Address Translation Rules

Inside Interface(s): Loopback0

Outside Interface(s): Ethernet0/0

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

- De nuevo, el tecleo **agrega** para configurar la traducción de NAT del exterior a la dirección interior como se

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

muestra.

- Haga clic en OK.

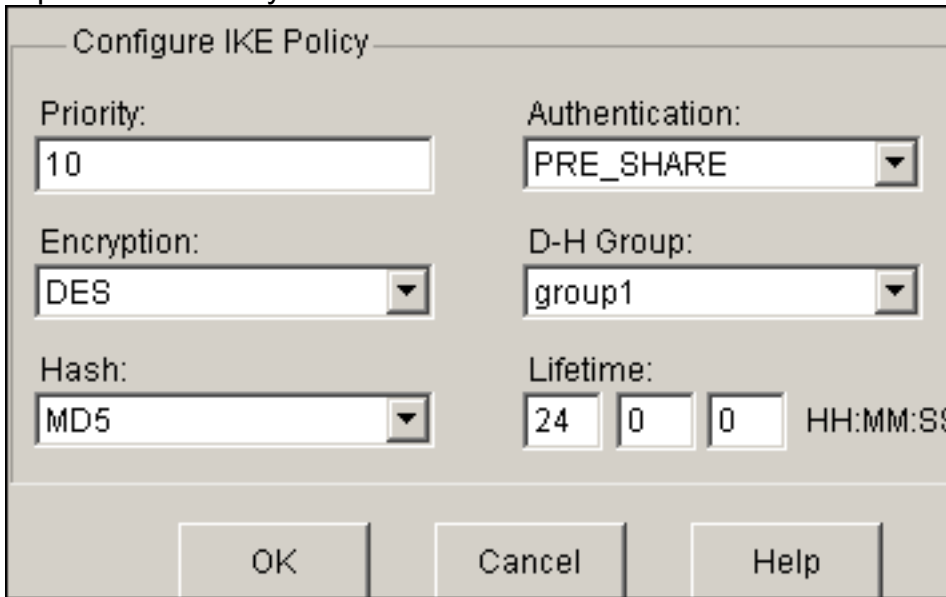
Network Address Translation Rules			
Inside Interface(s):		Loopback0	
Outside Interface(s):		Ethernet0/0	
Original address	Translated address	Rule Type	
192.168.1.0-192.168.1.255	10.5.5.0-10.5.5.255	Static	
192.168.1.0-192.168.1.255	10.10.10.0-10.10.10.255	Static	

Nota: Aquí está la configuración CLI equivalente:

Configuración VPN

Complete estos pasos para utilizar el VPN para configurar el SDM en el router del Site_A:

1. Elija la configuración > los componentes VPN > VPN >IKE > las políticas IKE > Add para definir las políticas IKE tal y como se muestra en de esta



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

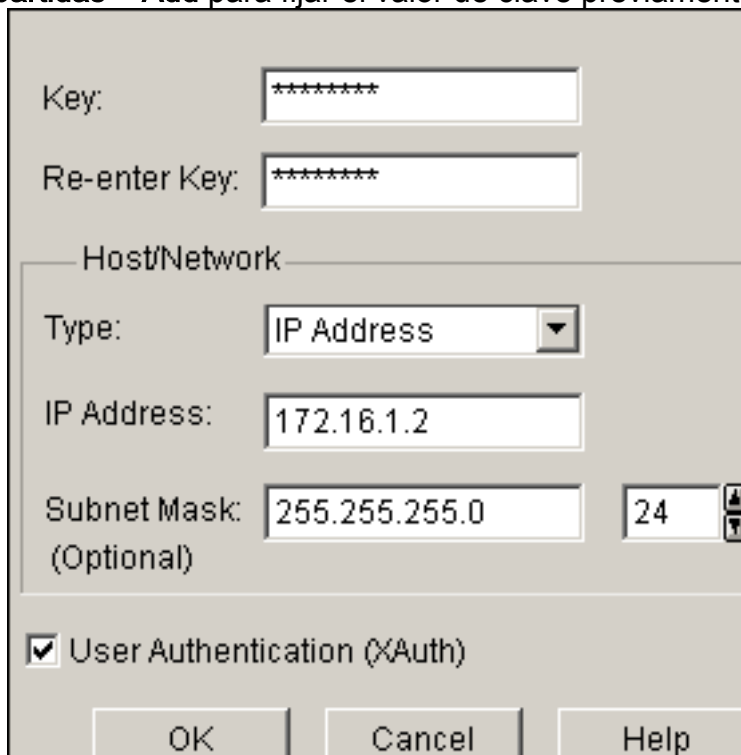
imagen.

2. Haga clic en OK.

IKE Políticas							Add...	Edit...	Del
Priority	Encryption	Hash	D-H Group	Authentication	Type				
10	DES	MD5	group1	PRE SHARE	User Defined				

Nota: Aquí está la configuración CLI equivalente:

3. Elija la configuración > los componentes VPN > VPN >IKE > las claves previamente compartidas > Add para fijar el valor de clave previamente compartida con el IP Address de



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. Haga clic en OK.

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

Nota: Aquí está la configuración CLI equivalente:

- Elija la configuración > el VPN > los componentes > el IPSec VPN > transforman los conjuntos > Add para crear un *myset* determinado de la transformación tal y como se

Add Transform Set

Name:

Data integrity with encryption (ESP)

Integrity Algorithm:

Encryption Algorithm:

Show Advanced

muestra en de esta imagen.

- Haga clic en OK.

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

Nota: Aquí está la configuración CLI equivalente:

- Elija la configuración > el VPN > los componentes > el IPSec > el IPSec Rules(ACLs) VPN > Add para crear un Access Control List(ACL) crypto

Add a Rule

Name/Number: Type:

Description:

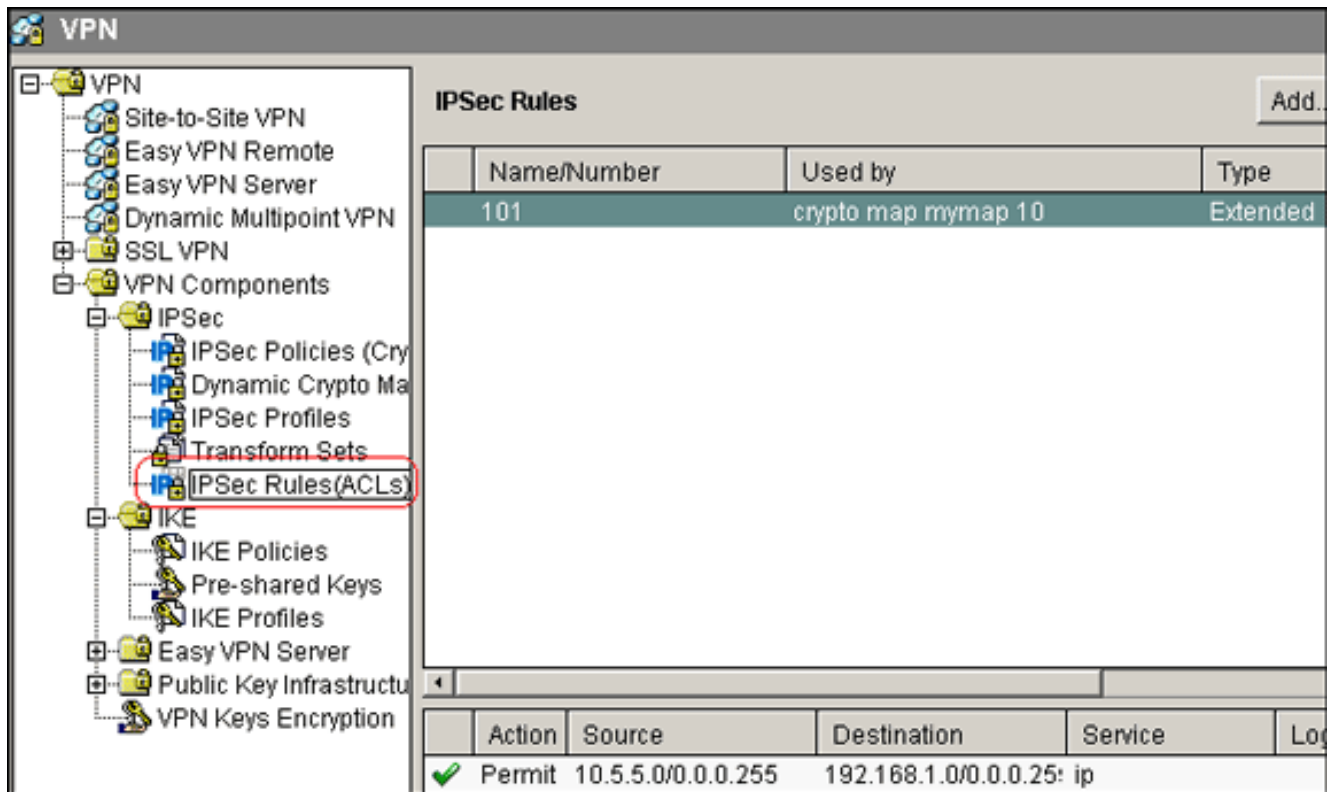
Rule Entry

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

Interface Association
None.

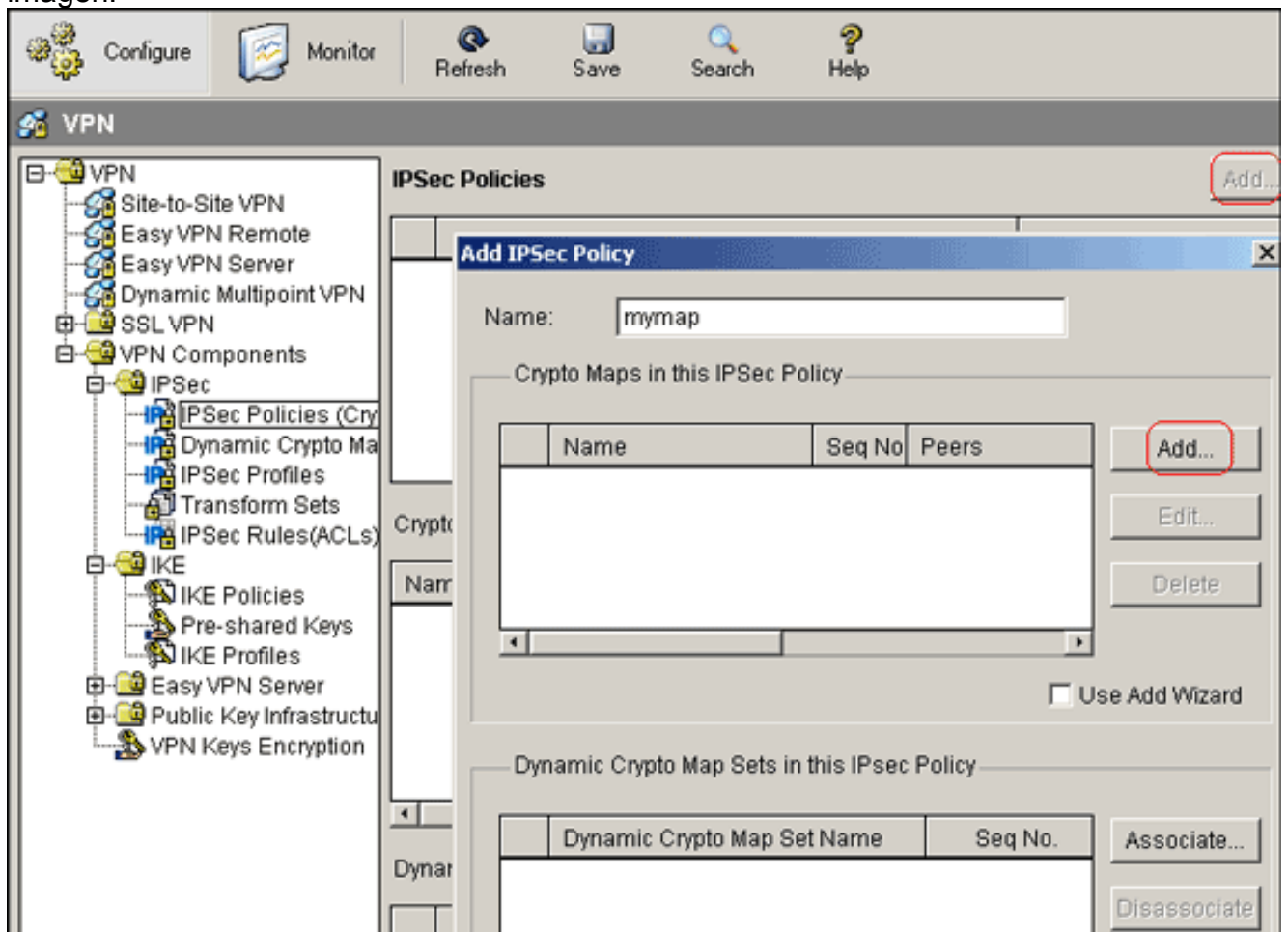
101.

8. Haga clic en OK.



Nota: Aquí está la configuración CLI equivalente:

- Elija la configuración > el VPN > los componentes > el IPsec > las políticas IPsec VPN > Add en order para crear el *mymap* de la correspondencia del crypto tal y como se muestra en de esta imagen.



- Haga clic en Add (Agregar).Haga clic la **ficha general** y conserve las configuraciones

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

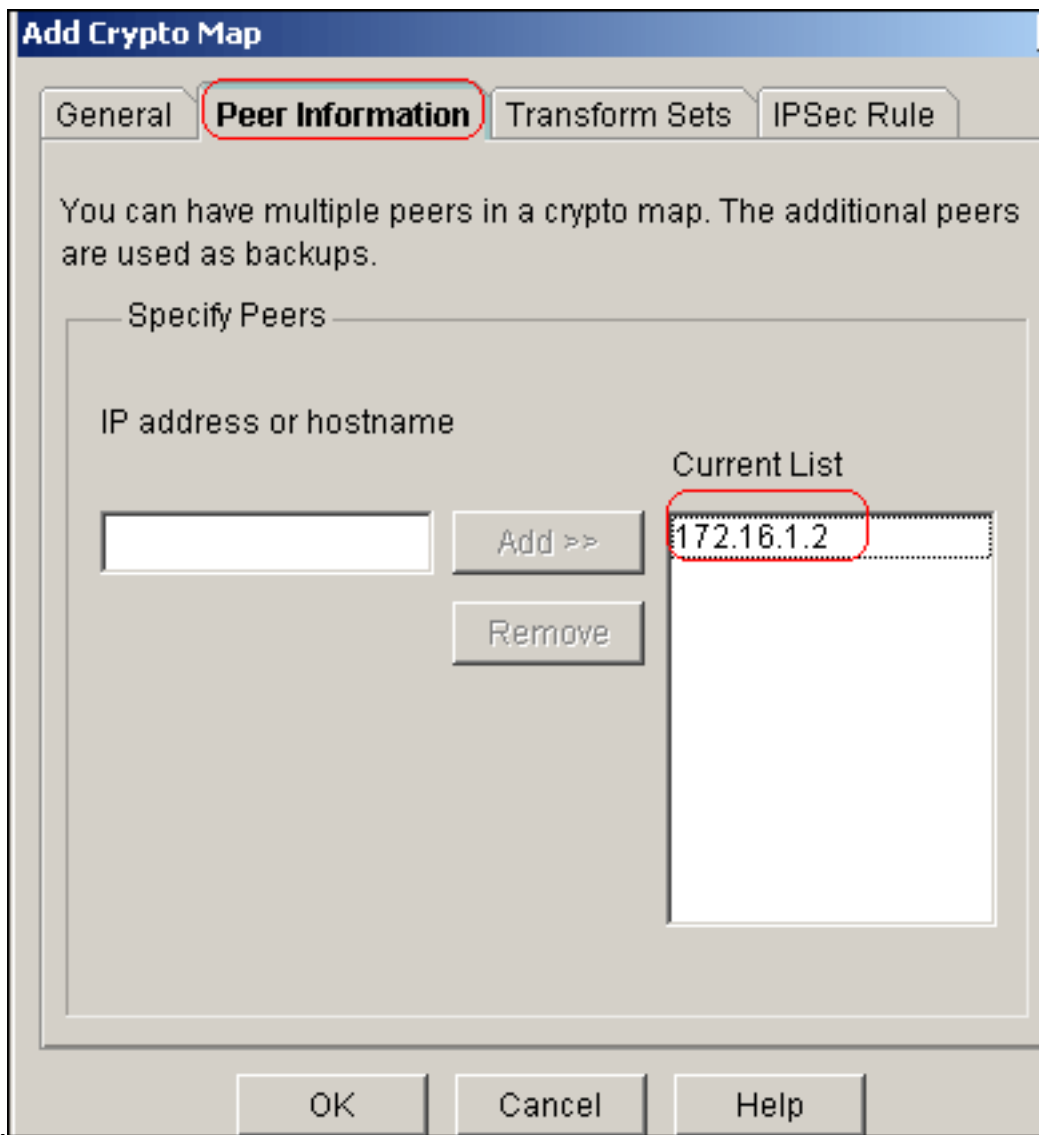
Reverse Route Injection

OK Cancel Help

predeterminadas.

clique la pestaña de la **información de peer** para agregar el IP Address de Peer

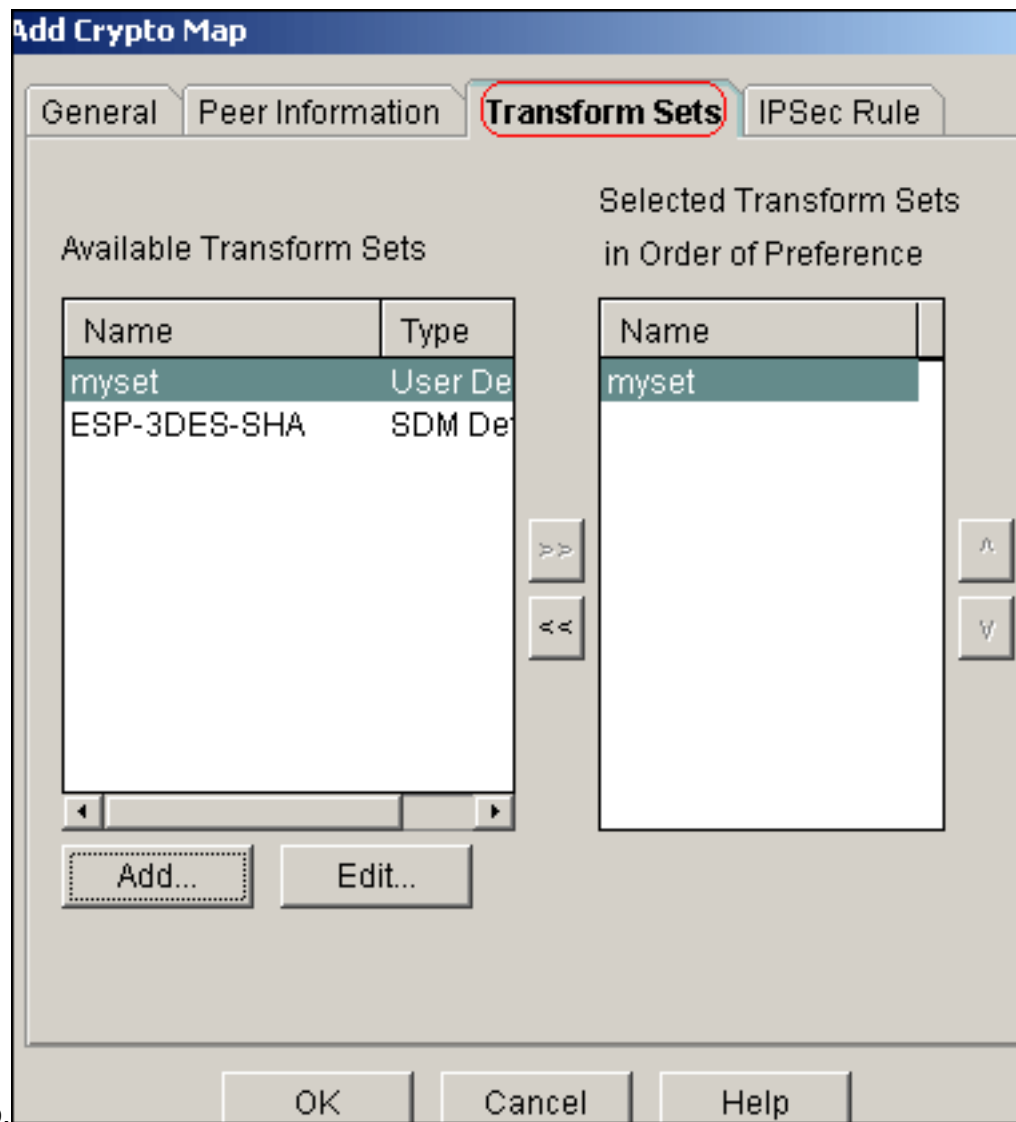
Haga



172.16.1.2.

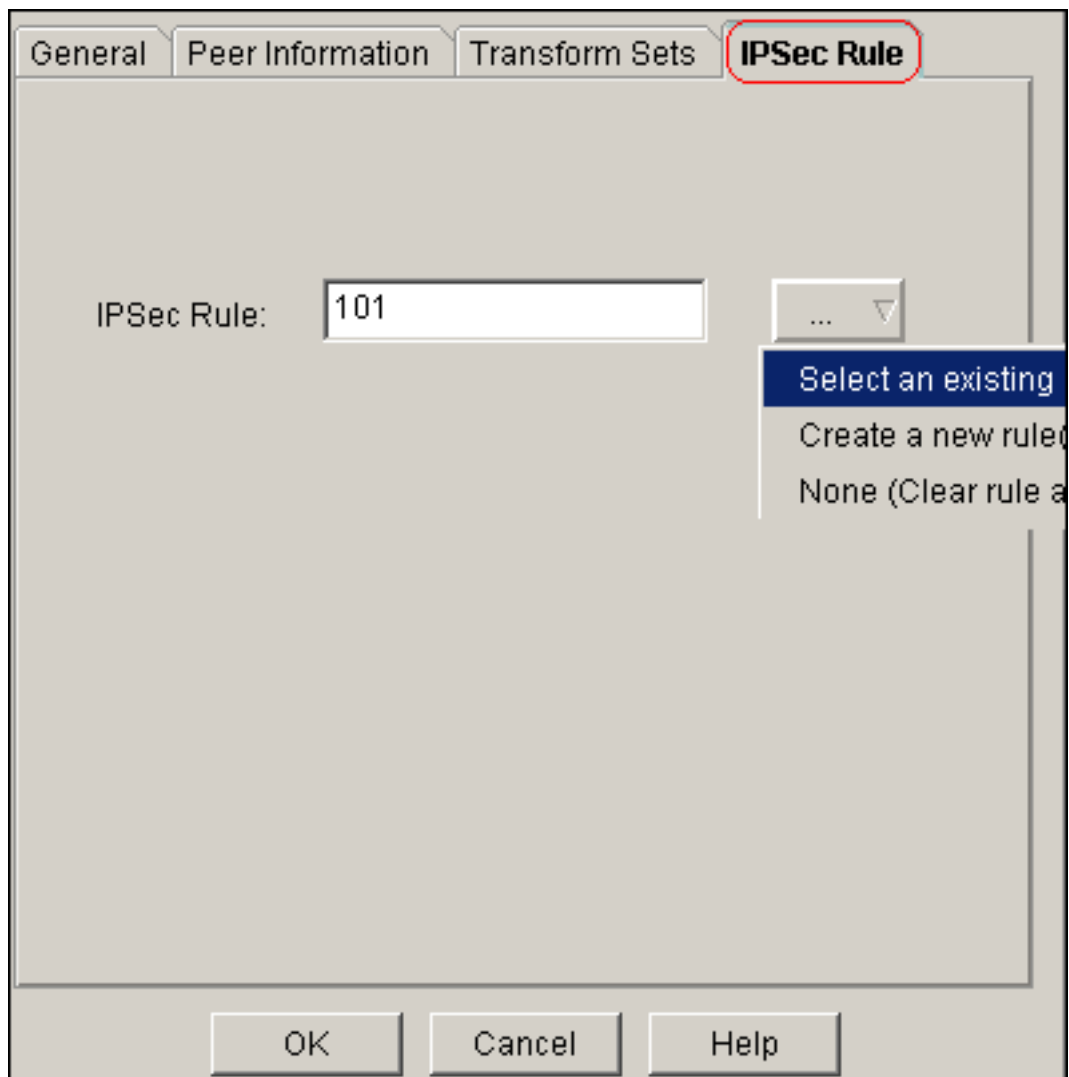
Haga

clic la lengüeta de los conjuntos de la transformación para seleccionar deseado transforman el *myset*



determinado.

Haga clic la lengüeta de la **regla del IPSec** para seleccionar el ACL 101 crypto

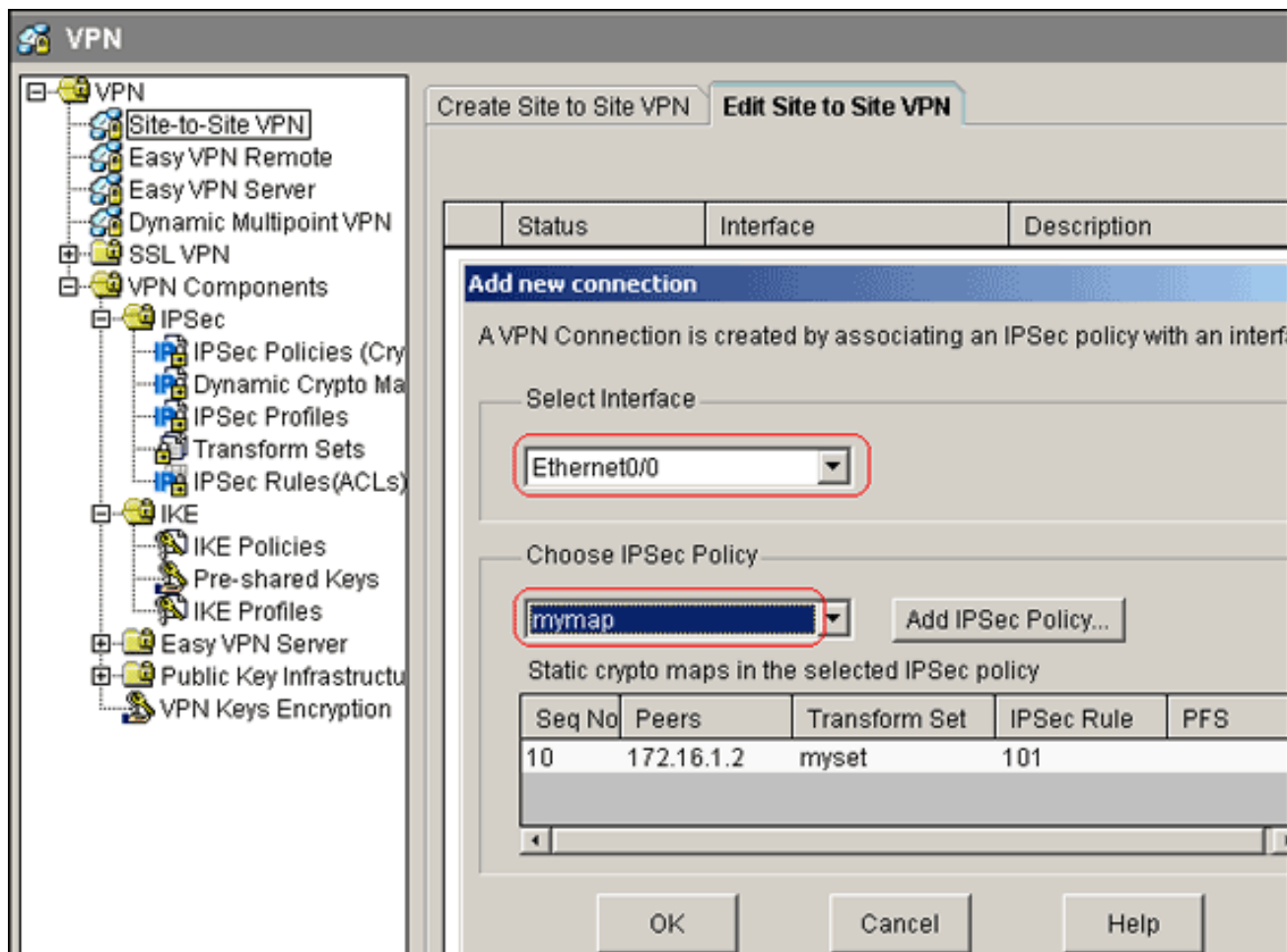


existente.

Haga

clic en OK. **Nota:** Aquí está la configuración CLI equivalente:

11. Elija la configuración > el VPN > el VPN de sitio a sitio > editan el VPN de sitio a sitio > Add para aplicar el *mymap de la* correspondencia de criptografía al Ethernet0/0 de la interfaz.



12. Haga clic en OK. **Nota:** Aquí está la configuración CLI equivalente:

Configuración CLI del router del Site_A

Router del Site_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#

```

Configuración CLI del router del Site B

Router del Site_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#

```

Verificación

En esta sección encontrará información que puede utilizar para confirmar que su configuración esté funcionando correctamente.

[La herramienta Output Interpreter Tool \(clientes registrados solamente\)](#) (OIT) soporta ciertos comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

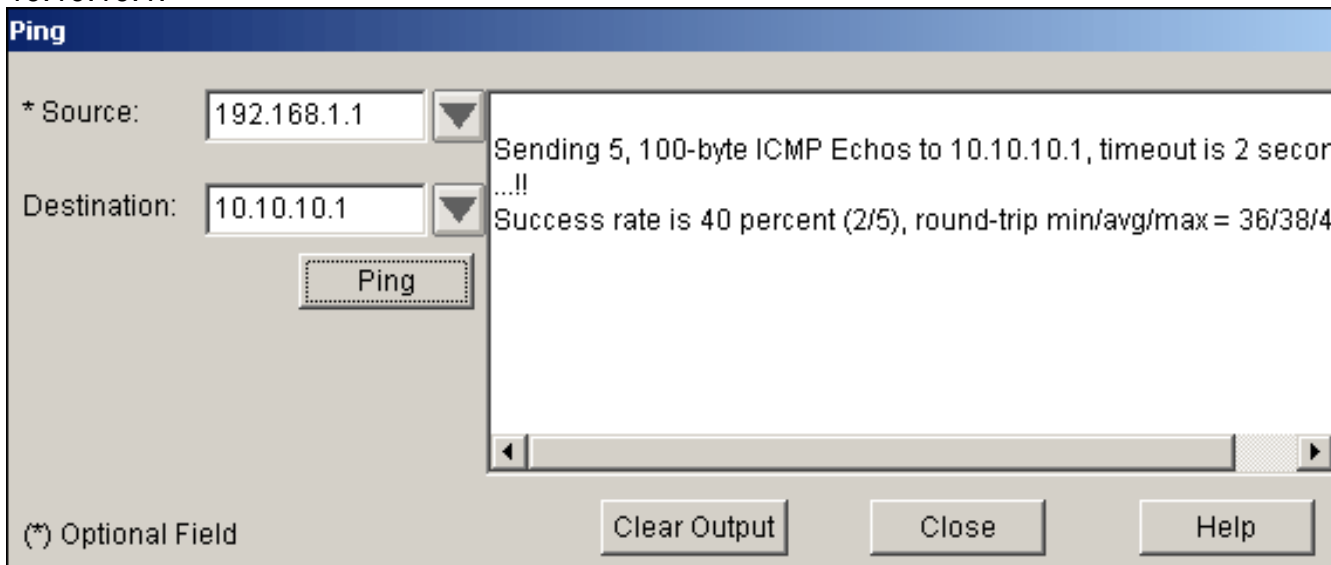
- **muestre isakmp crypto sa** — Visualiza todas las asociaciones de seguridad actuales del Internet Key Exchange (IKE) (SA) en un par. `par.Site_A#show crypto isakmp sa dst src state conn-id slot status 172.16.1.2 10.1.1.2 QM_IDLE 1 0 ACTIVE`
- **muestre el detalle crypto isakmp sa** — Visualiza los detalles de todo el IKE actual SA en un par. `par.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** — Muestra la configuración actual utilizada por las SA actuales. `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#
```

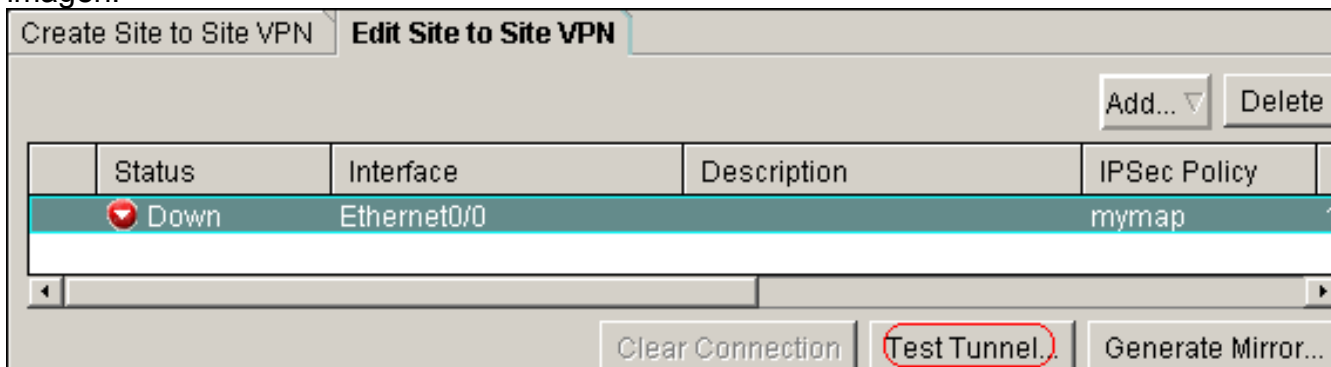
- **muestre a IP las traducciones nacionales** — Visualiza la información del slot de

```
traducción.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 --- ---
```

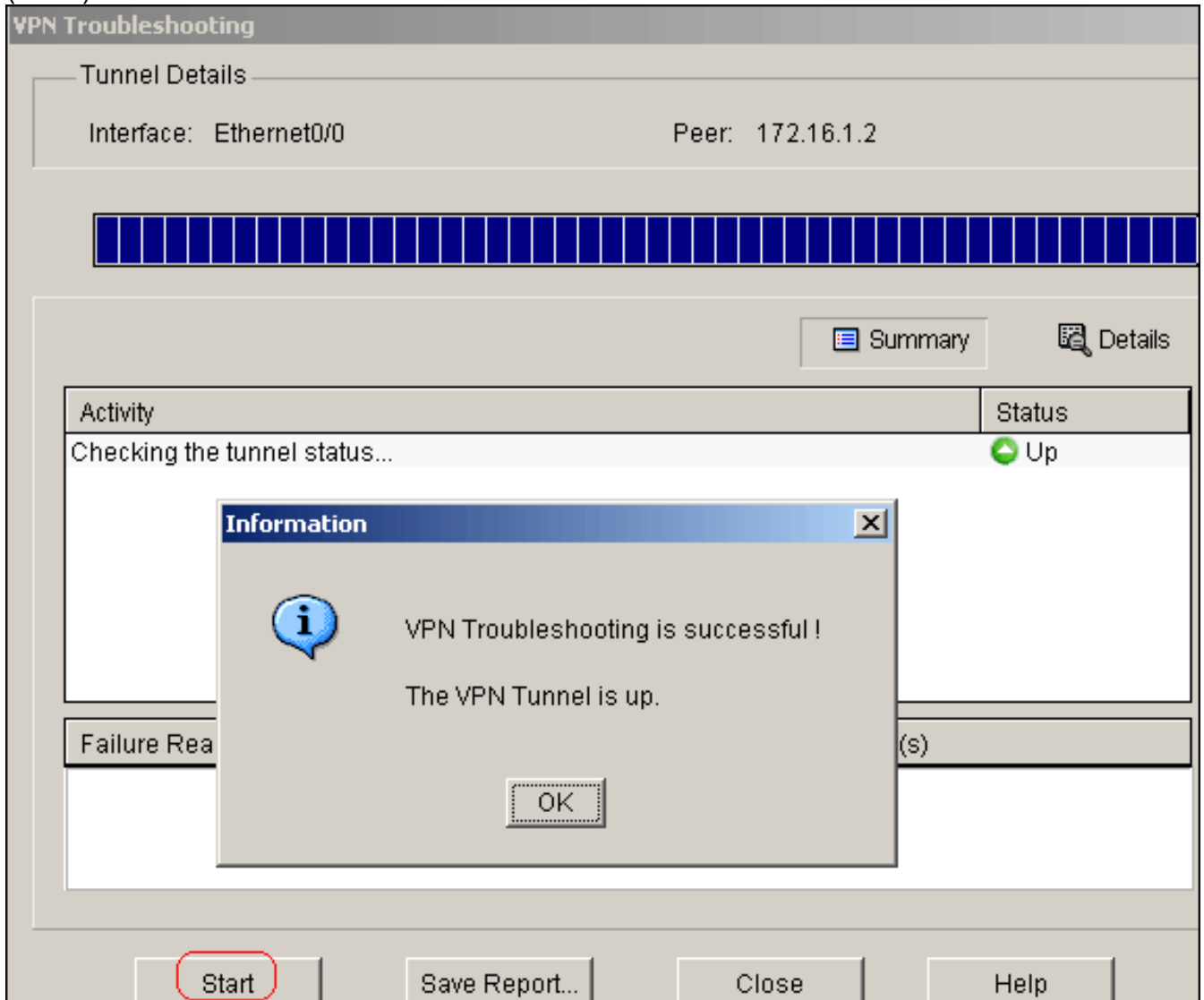
- **show ip nat statistics** — Visualiza la información estática sobre la traducción.Site_A#show ip nat statistics Total active translations: 4 (2 static, 2 dynamic; 0 extended) Outside interfaces: Ethernet0/0 Inside interfaces: Loopback0 Hits: 42 Misses: 2 CEF Translated packets: 13, CEF Punted packets: 0 Expired translations: 7 Dynamic mappings: Queued Packets: 0 Site_A#
- Complete estos pasos para verificar la conexión:En el SDM, elija las **herramientas > el ping** para establecer el túnel del IPsec VPN con el IP de la fuente como 192.168.1.1 y el IP de destino como 10.10.10.1.



Haga clic el **túnel de la prueba** para marcar el túnel del IPsec VPN se establece tal y como se muestra en de esta imagen.



Haga clic en Start (Inicio).



Troubleshooting

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

```
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, rc
vd 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, rc vd 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, rc vd 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, rc vd 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, rc vd 4

[Información Relacionada](#)

- [Soluciones a los Problemas más frecuentes de IPSec VPN L2L y de Acceso Remoto](#)
- [IPSec entre ASA/PIX y Cisco VPN 3000 Concentrator con el ejemplo de configuración de las redes privadas superpuestas](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)