

# Configurar el IPSec entre un router y un PIX usando el comando nat 0 access-list

## Contenido

[Introducción](#)

[Antes de comenzar](#)

[Convenciones](#)

[prerrequisitos](#)

[Componentes Utilizados](#)

[Teoría Precedente](#)

[Configurar](#)

[Diagrama de la red](#)

[Configuraciones](#)

[Verificación](#)

[Troubleshooting](#)

[Comandos para resolución de problemas](#)

[Ejemplo de resultado del comando debug](#)

[Información Relacionada](#)

## [Introducción](#)

Este documento ilustra una configuración de Seguridad IP (IPSec) entre un router y un Firewall PIX de Cisco Secure. Para el tráfico entre la LAN principal y las LAN remotas queremos usar direcciones IP privadas internas y también para los hosts de la LAN en direcciones IP enrutables cuando los usuarios acceden a Internet. Sin embargo, los usuarios también pueden acceder a las páginas públicas en Internet sin que el tráfico de las mismas atraviese el túnel utilizando el comando route-map.

Refiérase [ASA/PIX: Dispositivo de seguridad a un ejemplo de configuración del router IOS túnel ipsec de LAN a LAN](#) para aprender más sobre el escenario donde túneles de LAN a LAN entre un router y el PIX/ASA de los dispositivos del Cisco Security.

## [Antes de comenzar](#)

### [Convenciones](#)

Para obtener más información sobre las convenciones del documento, consulte [Convenciones de Consejos Técnicos de Cisco](#).

### [prerrequisitos](#)

No hay requisitos previos específicos para este documento.

## Componentes Utilizados

La información que contiene este documento se basa en las versiones de software y hardware indicadas a continuación.

- Router Cisco con la versión 12.0(7)T de software del IOS de Cisco
- Versión 5.1(1) del Cisco PIX Firewall

La información que se presenta en este documento se originó a partir de dispositivos dentro de 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 un comando antes de ejecutarlo.

## Teoría Precedente

En el PIX, los comandos `access-list` y `nat 0` funcionan de manera conjunta. Cuando un usuario en la red de 10.1.1.0 va a la red de 10.2.2.0, utilizamos la lista de acceso para permitir que el tráfico de la red de 10.1.1.0 sea cifrado sin el Network Address Translation (NAT). No obstante, cuando esos dos mismos usuarios se dirigen a cualquier otra parte, son traducidos a la dirección 172.17.63.210 mediante la traducción de dirección de puerto (PAT). En el router, utilizan a los **comandos `route-map` and `access-list`** de permitir que el tráfico de la red de 10.2.2.0 sea cifrado sin el NAT. No obstante, cuando esos dos mismos usuarios se dirigen a cualquier otra parte, son traducidos a la dirección 172.17.63.210 mediante la traducción de dirección de puerto (PAT).

A continuación se presentan los comandos de configuración requeridos en el Firewall de PIX para que el tráfico por el túnel no se ejecute a través de PAT y para que el tráfico a Internet se ejecute a través de PAT.

```
access-list nonat permit ip 10.1.1.0 255.255.255.0 10.2.2.0 255.255.255.0 nat (inside) 0 access-list nonat nat (inside) 1 10.1.1.0 255.255.255.0 0 0
```

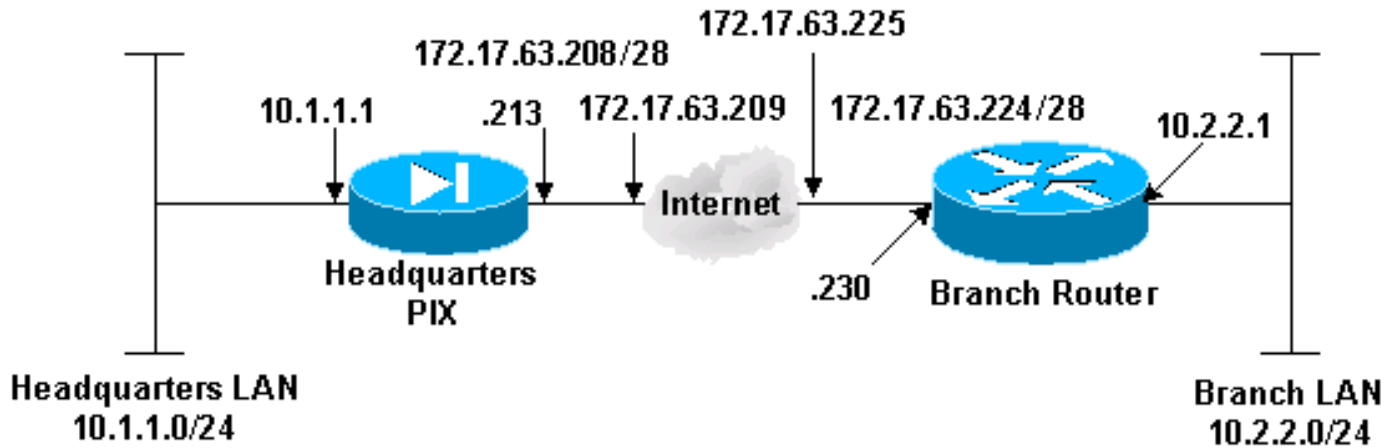
## Configurar

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

**Nota:** Para obtener información adicional sobre los comandos que se utilizan en este documento, use la herramienta Command Lookup del IOS.

## Diagrama de la red

Este documento utiliza la instalación de red que se muestra en el siguiente diagrama.



## Configuraciones

Este documento usa las configuraciones detalladas a continuación.

### PIX principal

```

PIX Version 5.1(1)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
!--- Traffic to the router: access-list ipsec permit ip
10.1.1.0 255.255.255.0 10.2.2.0 255.255.255.0 !--- Do
not Network Address Translate (NAT) traffic to the
router: access-list nonat permit ip 10.1.1.0
255.255.255.0 10.2.2.0 255.255.255.0 enable password
8Ry2YjIyt7RRXU24 encrypted passwd 2KFQnbNIdI.2KYOU
encrypted hostname HQ_PIX fixup protocol ftp 21 fixup
protocol http 80 fixup protocol smtp 25 fixup protocol
h323 1720 fixup protocol rsh 514 fixup protocol sqlnet
1521 names pager lines 24 no logging timestamp no
logging standby no logging console no logging monitor no
logging buffered no logging trap no logging history
logging facility 20 logging queue 512 interface
ethernet0 auto interface ethernet1 auto mtu outside 1500
mtu inside 1500 ip address outside 172.17.63.213
255.255.255.240 ip address inside 10.1.1.1 255.255.255.0
no failover failover timeout 0:00:00 failover ip address
outside 0.0.0.0 failover ip address inside 0.0.0.0 arp
timeout 14400 global (outside) 1 172.17.63.210 !--- Do
not NAT traffic to the router: nat (inside) 0 access-
list nonat nat (inside) 1 10.1.1.0 255.255.255.0 0 0
conduit permit icmp any any route outside 0.0.0.0
0.0.0.0 172.17.63.209 1 timeout xlate 3:00:00 conn
1:00:00 half-closed 0:10:00 udp 0:02:00 timeout rpc
0:10:00 h323 0:05:00 timeout uauth 0:05:00 absolute aaa-
server TACACS+ protocol tacacs+ aaa-server RADIUS
protocol radius aaa-server partner protocol tacacs+ no
snmp-server location no snmp-server contact snmp-server
community public no snmp-server enable traps floodguard
enable !--- IPSec policies: sysopt connection permit-
ipsec crypto ipsec transform-set avalanche esp-des esp-
md5-hmac crypto ipsec security-association lifetime
seconds 3600 crypto map forsberg 21 ipsec-isakmp crypto
map forsberg 21 match address ipsec crypto map forsberg
21 set peer 172.17.63.230 crypto map forsberg 21 set
transform-set avalanche crypto map forsberg interface
outside !--- IKE policies: isakmp enable outside isakmp

```

```
key westernfinal2000 address 172.17.63.230 netmask
255.255.255.255 isakmp identity address isakmp policy 21
authentication pre-share isakmp policy 21 encryption des
isakmp policy 21 hash md5 isakmp policy 21 group 1
telnet timeout 5 terminal width 80
Cryptochecksum:e36245da9428c4c07b489f787c8ccd3b : end
```

## Router de rama

```
Current configuration:
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Branch_Router
!
!
!
!
!
!
ip subnet-zero
!
!
!--- IKE policies: crypto isakmp policy 11 hash md5
authentication pre-share crypto isakmp key
westernfinal2000 address 172.17.63.213 ! ! !--- IPsec
policies: crypto ipsec transform-set sharks esp-des esp-
md5-hmac ! ! crypto map nolan 11 ipsec-isakmp set peer
172.17.63.213 set transform-set sharks !--- Include the
private-network-to-private-network traffic !--- in the
encryption process. match address 120 ! ! ! interface
Ethernet0 ip address 172.17.63.230 255.255.255.240 no ip
directed-broadcast ip nat outside no ip route-cache
crypto map nolan ! interface Ethernet1 ip address
10.2.2.1 255.255.255.0 no ip directed-broadcast ip nat
inside ! interface Serial0 no ip address no ip directed-
broadcast no ip mroute-cache shutdown no fair-queue !
interface Serial1 no ip address no ip directed-broadcast
shutdown ! ip nat pool branch 172.17.63.230
172.17.63.230 netmask 255.255.255.240 !--- Except the
private network from the NAT process: ip nat inside
source route-map nonat pool branch overload ip classless
ip route 0.0.0.0 0.0.0.0 172.17.63.225 no ip http server
!--- Include the private-network-to-private-network
traffic !--- in the encryption process: access-list 120
permit ip 10.2.2.0 0.0.0.255 10.1.1.0 0.0.0.255 !---
Except the private network from the NAT process: access-
list 130 deny ip 10.2.2.0 0.0.0.255 10.1.1.0 0.0.0.255
access-list 130 permit ip 10.2.2.0 0.0.0.255 any !---
Except the private network from the NAT process: route-
map nonat permit 10 match ip address 130 ! ! line con 0
transport input none line 1 16 line aux 0 line vty 0 4 !
end
```

## Verificación

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

La herramienta del Output Interpreter soportan a los ciertos comandos show, que permite que usted vea una análisis de la salida del comando show.

- show crypto isakmp sa: Ver todas las asociaciones actuales de seguridad IKE (SAs) de un par.
- **muestre IPSec crypto sa** - Muestra las configuraciones usadas por las asociaciones de seguridad actuales del [IPSec].
- show crypto engine connections active: (sólo el router) muestra las conexiones actuales y la información sobre los paquetes encriptación y desencriptación.

## Troubleshooting

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

### Comandos para resolución de problemas

La herramienta del Output Interpreter soportan a los ciertos comandos show, que permite que usted vea una análisis de la salida del comando show.

**Nota: Antes de ejecutar un comando debug, consulte Información Importante sobre Comandos Debug.**

Las siguientes depuraciones deben estar ejecutándose en ambos pares IPSec.

- **isakmp del debug crypto** - (router y PIX) visualiza los errores durante la fase 1.
- **IPSec del debug crypto** - (router y PIX) visualiza los errores durante la fase 2.
- debug crypto engine – (sólo router) Muestra información del motor crypto.

La verificación de las asociaciones de seguridad se debe realizar en ambos pares Realizan a los comandos pix en el enable mode; los comandos del router se ejecutan en el modo non-enable (no habilitar).

- clear crypto isakmp sa - (PIX) Elimina las asociaciones de seguridad de la Fase 1.
- clear crypto isakmp – (PIX) Elimina las asociaciones de seguridad de la Fase 2.
- clear crypto isakmp – (Router) Elimina las asociaciones de seguridad de la Fase 1.
- clear crypto sa – (Router) Elimina las asociaciones de seguridad de la Fase 2.

### Ejemplo de resultado del comando debug

- [Depuraciones de Headquarters PIX](#)
- [Depuraciones del router de sucursal](#)

### Depuraciones de Headquarters PIX

```
ISAKMP (0): beginning Main Mode exchange
IPSEC(ipsec_encap): crypto map check deny
```

```
02303: sa_request,
(key eng. msg.) src= 172.17.63.213, dest= 172.17.63.230,
src_proxy= 10.1.1.0/255.255.255.0/0/0 (type=4),
```

dest\_proxy= 10.2.2.0/255.255.255.0/0/0 (type=4),  
protocol= ESP, transform= esp-des esp-md5-hmac ,  
lifedur= 28800s and 4608000kb,  
spi= 0x0(0), conn\_id= 0, keysize= 0, flags= 0x4004

crypto\_isakmp\_process\_block: src 172.17.63.230,  
dest 172.17.63.213

OAK\_MM exchange

ISAKMP (0): processing SA payload. message ID = 0

ISAKMP (0): Checking ISAKMP transform 1 against priority  
21 policy

ISAKMP: encryption DES-CBC

ISAKMP: hash MD5

ISAKMP: default group 1

ISAKMP: auth pre-share

ISAKMP: life type in seconds

ISAKMP: life duration (basic) of 3600

ISAKMP (0): atts are acceptable. Next payload is 0

ISAKMP (0): SA is doing pre-shared key authentication  
using id type ID\_IPV4\_ADDR

return status is IKMP\_NO\_ERRORIPSEC(ipsec\_encap): crypto  
map check deny

crypto\_isakmp\_process\_block: src 172.17.63.230,  
dest 172.17.63.213

OAK\_MM exchange

ISAKMP (0): processing KE payload. message ID = 0

ISAKMP (0): processing NONCE payload. message ID = 0

ISAKMP (0): processing vendor id payload

ISAKMP (0): speaking to another IOS box!

ISAKMP (0): ID payload

next-payload : 8

type : 1

protocol : 17

port : 500

length : 8

ISAKMP (0): Total payload length: 12

return status is IKMP\_NO\_ERRORIPSEC(ipsec\_encap):  
crypto map check deny

crypto\_isakmp\_process\_block: src 172.17.63.230,  
dest 172.17.63.213

OAK\_MM exchange

ISAKMP (0): processing ID payload. message ID = 0

ISAKMP (0): processing HASH payload. message ID = 0

ISAKMP (0): SA has been authenticated

ISAKMP (0): beginning Quick Mode exchange, M-ID of  
-1448244754:a9ad89eeIPSEC(key\_engine): got a  
queue even

IPSEC(spi\_response): getting spi 0x5cfcf6e9(1560082153)  
for SA from 172.17.63.230 to  
172.17.63.213 for prot 3

return status is IKMP\_NO\_ERROR

crypto\_isakmp\_process\_block: src 172.17.63.230,

```
dest 172.17.63.213
OAK_QM exchange
oakley_process_quick_mode:
OAK_QM_IDLE
ISAKMP (0): processing SA payload. message ID =
    -1448244754

ISAKMP : Checking IPsec proposal 1

ISAKMP: transform 1, ESP_DES
ISAKMP:  attributes in transform:
ISAKMP:      encaps is 1
ISAKMP:      SA life type in seconds
ISAKMP:      SA life duration (basic) of 28800
ISAKMP:      SA life type in kilobytes
ISAKMP:      SA life duration (VPI) of  0x0
    0x46 0x50 0x0
ISAKMP:      authenticator is HMAC-MD5
ISAKMP (0): atts are acceptable.IPSEC
(validate_proposal_request):
proposal part #1,
(key eng. msg.) dest= 172.17.63.230,
src= 172.17.63.213,
dest_proxy= 10.2.2.0/255.255.255.0/0/0 (type=4),
src_proxy= 10.1.1.0/255.255.255.0/0/0 (type=4),
protocol= ESP, transform= esp-des esp-md5-hmac ,
lifedur= 0s and 0kb,
spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4

ISAKMP (0): processing NONCE payload. message ID =
    -1448244754

ISAKMP (0): processing ID payload. message ID =
    -1448244754
ISAKMP (0): processing ID payload. message ID =
    -1448244754
ISAKMP (0): processing NOTIFY payload 96 protocol 3
    spi 1510339082, message ID = -1448244754
ISAKMP (0): processing responder lifetime
ISAKMP (0): responder lifetime of
    3600sIPSEC(map_alloc_entry):
    allocating entry 3

IPSEC(map_alloc_entry): allocating entry 4

ISAKMP (0): Creating IPsec SAs
    inbound SA from  172.17.63.230 to
    172.17.63.213
    (proxy 10.2.2.0 to 10.1.1.0)
    has spi 1560082153 and conn_id 3 and flags 4
    lifetime of 3600 seconds
    lifetime of 4608000 kilobytes
    outbound SA from  172.17.63.213 to
    172.17.63.230
    (proxy 10.1.1.0 to 10.2.2.0)
    has spi 183633242 and conn_id 4 and flags 4
    lifetime of 3600 seconds
    lifetime of 4608000 kilobytesIPSEC(key_engine):
    got a queue event...
IPSEC(initialize_sas): ,
(key eng. msg.) dest= 172.17.63.213, src=
    172.17.63.230,
dest_proxy= 10.1.1.0/255.255.255.0/0/0 (type=4),
```

```
src_proxy= 10.2.2.0/255.255.255.0/0/0 (type=4),
protocol= ESP, transform= esp-des esp-md5-hmac ,
lifedur= 3600s and 4608000kb,
spi= 0x5cfcf6e9(1560082153), conn_id= 3, keysize= 0,
flags= 0x4
IPSEC(initialize_sas): ,
(key eng. msg.) src= 172.17.63.213, dest=
172.17.63.230,
src_proxy= 10.1.1.0/255.255.255.0/0/0 (type=4),
dest_proxy= 10.2.2.0/255.255.255.0/0/0 (type=4),
protocol= ESP, transform= esp-des esp-md5-hmac ,
lifedur= 3600s and 4608000kb,
spi= 0xaf2055a(183633242), conn_id= 4, keysize= 0,
flags= 0x4

return status is IKMP_NO_ERROR602301: sa created,
(sa) sa_dest= 172.17.63.213, sa_prot= 50,
sa_spi= 0x5cfcf6e9(1560082153),
sa_trans= esp-des esp-md5-hmac , sa_conn_id= 3
602301: sa created,
(sa) sa_dest= 172.17.63.230, sa_prot= 50,
sa_spi= 0xaf2055a(183633242),
sa_trans= esp-des esp-md5-hmac , sa_conn_id= 4
```

## Depuraciones del router de sucursal

```
Branch_Router#
01:27:08: ISAKMP (0): received packet from 172.17.63.213
(N) NEW SA
01:27:08: ISAKMP (0:1): processing SA payload.
message ID = 0
01:27:08: ISAKMP (0:1): Checking ISAKMP transform 1
against priority 11 policy
01:27:08: ISAKMP: encryption DES-CBC
01:27:08: ISAKMP: hash MD5
01:27:08: ISAKMP: default group 1
01:27:08: ISAKMP: auth pre-share
01:27:08: ISAKMP: life type in seconds
01:27:08: ISAKMP: life duration (basic) of 3600
01:27:08: ISAKMP (0:1): atts are acceptable. Next
payload is 0
01:27:08: CryptoEngine0: generate alg parameter
01:27:10: CRYPTO_ENGINE: Dh phase 1 status: 0
01:27:10: CRYPTO_ENGINE: Dh phase 1 status: 0
01:27:10: ISAKMP (0:1): SA is doing pre-shared key
authentication
01:27:10: ISAKMP (1): SA is doing pre-shared key
authentication using id type ID_IPV4_ADDR
01:27:10: ISAKMP (1): sending packet to 172.17.63.213
(R) MM_SA_SETUP
01:27:10: ISAKMP (1): received packet from 172.17.63.213
(R) MM_SA_SETUP
01:27:10: ISAKMP (0:1): processing KE payload. message
ID = 0
01:27:10: CryptoEngine0: generate alg parameter
01:27:12: ISAKMP (0:1): processing NONCE payload.
message ID = 0
01:27:12: CryptoEngine0: create ISAKMP SKEYID for
conn id 1
01:27:12: ISAKMP (0:1): SKEYID state generated
01:27:12: ISAKMP (0:1): processing vendor id payload
01:27:12: ISAKMP (0:1): speaking to another IOS box!
01:27:12: ISAKMP (1): sending packet to 172.17.63.213 (R)
MM_KEY_EXCH
```



01:27:12: ISAKMP (1): received packet from 172.17.63.213  
(R) MM\_KEY\_EXCH  
01:27:12: ISAKMP (0:1): processing ID payload.  
message ID = 0  
01:27:12: ISAKMP (0:1): processing HASH payload.  
message ID = 0  
01:27:12: CryptoEngine0: generate hmac context for  
conn id 1  
01:27:12: ISAKMP (0:1): SA has been authenticated  
with 172.17.63.213  
01:27:12: ISAKMP (1): ID payload  
next-payload : 8  
type : 1  
protocol : 17  
port : 500  
length : 8  
01:27:12: ISAKMP (1): Total payload length: 12  
01:27:12: CryptoEngine0: generate hmac context  
for conn id 1  
01:27:12: CryptoEngine0: clear dh number for  
conn id 1  
01:27:12: ISAKMP (1): sending packet to  
172.17.63.213 (R) QM\_IDLE  
01:27:12: ISAKMP (1): received packet from  
172.17.63.213 (R) QM\_IDLE  
01:27:12: CryptoEngine0: generate hmac context for  
conn id 1  
01:27:12: ISAKMP (0:1): processing SA payload.  
message ID = -1448244754  
01:27:12: ISAKMP (0:1): Checking IPsec proposal 1  
01:27:12: ISAKMP: transform 1, ESP\_DES  
01:27:12: ISAKMP: attributes in transform:  
01:27:12: ISAKMP: encaps is 1  
01:27:12: ISAKMP: SA life type in seconds  
01:27:12: ISAKMP: SA life duration (basic)  
of 28800  
01:27:12: ISAKMP: SA life type in kilobytes  
01:27:12: ISAKMP: SA life duration (VPI) of  
0x0 0x46 0x50 0x0  
01:27:12: ISAKMP: authenticator is HMAC-MD5  
01:27:12: validate proposal 0  
01:27:12: ISAKMP (0:1): atts are acceptable.  
01:27:12: IPSEC(validate\_proposal\_request):  
proposal part #1, (key eng. msg.)  
dest= 172.17.63.230, src= 172.17.63.213,  
dest\_proxy= 10.2.2.0/255.255.255.0/0/0 (type=4),  
src\_proxy= 10.1.1.0/255.255.255.0/0/0 (type=4),  
protocol= ESP, transform= esp-des esp-md5-hmac ,  
lifedur= 0s and 0kb,  
spi= 0x0(0), conn\_id= 0, keysize= 0, flags= 0x4  
01:27:13: validate proposal request 0  
01:27:13: ISAKMP (0:1): processing NONCE payload.  
message ID = -1448244754  
01:27:13: ISAKMP (0:1): processing ID payload.  
message ID = -1448244754  
01:27:13: ISAKMP (1): ID\_IPV4\_ADDR\_SUBNET src  
10.1.1.0/255.255.255.0 prot 0 port 0  
01:27:13: ISAKMP (0:1): processing ID payload.  
message ID = -1448244754  
01:27:13: ISAKMP (1): ID\_IPV4\_ADDR\_SUBNET dst  
10.2.2.0/255.255.255.0 prot 0 port 0  
01:27:13: IPSEC(key\_engine): got a queue event...  
01:27:13: IPSEC(spi\_response): getting spi 183633242  
for SA

```
from 172.17.63.213 to 172.17.63.230 for prot 3
01:27:13: CryptoEngine0: generate hmac context for
conn id 1
01:27:13: ISAKMP (1): sending packet to 172.17.63.213
(R) QM_IDLE
01:27:13: ISAKMP (1): received packet from 172.17.63.213
(R) QM_IDLE
01:27:13: CryptoEngine0: generate hmac context
for conn id 1
01:27:13: ipsec allocate flow 0
01:27:13: ipsec allocate flow 0
01:27:13: ISAKMP (0:1): Creating IPSec SAs
01:27:13: inbound SA from 172.17.63.213
to 172.17.63.230 (proxy 10.1.1.0 to 10.2.2.0)
01:27:13: has spi 183633242 and conn_id 2000
and flags 4
01:27:13: lifetime of 28800 seconds
01:27:13: lifetime of 4608000 kilobytes
01:27:13: outbound SA from 172.17.63.230
to 172.17.63.213 (proxy 10.2.2.0 to 10.1.1.0)
01:27:13: has spi 1560082153 and conn_id
2001 and flags 4
01:27:13: lifetime of 28800 seconds
01:27:13: lifetime of 4608000 kilobytes
01:27:13: ISAKMP (0:1): deleting node -1448244754
01:27:13: IPSEC(key_engine): got a queue event...
01:27:13: IPSEC(initialize_sas): ,
(key eng. msg.) dest= 172.17.63.230, src=
172.17.63.213,
dest_proxy= 10.2.2.0/255.255.255.0/0/0 (type=4),
src_proxy= 10.1.1.0/255.255.255.0/0/0 (type=4),
protocol= ESP, transform= esp-des esp-md5-hmac ,
lifedur= 28800s and 4608000kb,
spi= 0xAF2055A(183633242), conn_id= 2000,
keysize= 0, flags= 0x4
01:27:13: IPSEC(initialize_sas): ,
(key eng. msg.) src= 172.17.63.230,
dest= 172.17.63.213,
src_proxy= 10.2.2.0/255.255.255.0/0/0 (type=4),
dest_proxy= 10.1.1.0/255.255.255.0/0/0 (type=4),
protocol= ESP, transform= esp-des esp-md5-hmac ,
lifedur= 28800s and 4608000kb,
spi= 0x5CFCF6E9(1560082153), conn_id= 2001,
keysize= 0, flags= 0x4
01:27:13: IPSEC(create_sa): sa created,
(sa) sa_dest= 172.17.63.230, sa_prot= 50,
sa_spi= 0xAF2055A(183633242),
sa_trans= esp-des esp-md5-hmac , sa_conn_id= 2000
01:27:13: IPSEC(create_sa): sa created,
(sa) sa_dest= 172.17.63.213, sa_prot= 50,
sa_spi= 0x5CFCF6E9(1560082153),
sa_trans= esp-des esp-md5-hmac , sa_conn_id= 2001
```

## [Información Relacionada](#)

- [Solicitudes de Comentarios \(RFC\)](#)
- [Soporte Técnico - Cisco Systems](#)