

# Configuración del router para cliente VPN, configuración de modo, clave comodín previamente compartida con NAT

## Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Configurar](#)

[Diagrama de la red](#)

[Configuraciones](#)

[Verificación](#)

[Troubleshoot](#)

[Comandos para resolución de problemas](#)

[Ejemplo de resultado del comando debug](#)

[Información Relacionada](#)

## Introducción

Esta configuración de ejemplo ilustra un router configurado para la configuración de modo (el usuario consigue una dirección IP del conjunto), las claves comodín previamente compartidas (todos los clientes del PC comparten una clave común) y la Traducción de Dirección de Red (NAT). En esta configuración, un usuario fuera del sitio puede entrar la red y tener asignada una dirección IP interna del conjunto. Para los usuarios, aparece que están dentro de la red. Debido a que el direccionamiento privado, y por lo tanto la NAT, están implicados, se debe indicar al router qué debe traducir y qué no debe traducir.

## Prerequisites

### Requirements

No hay requisitos específicos para este documento.

### Componentes Utilizados

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

- Versión 12.0.7T o posterior del software del IOS® de Cisco
- Hardware compatible con esta revisión de software
- CiscoSecure VPN Client 1.0/10A o 1.1 (mostrado como 2.0.7/E o 2.1.12, respectivamente, vaya a **Ayuda > Acerca de** para verificar)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

## Convenciones

For more information on document conventions, refer to the [Cisco Technical Tips Conventions](#).

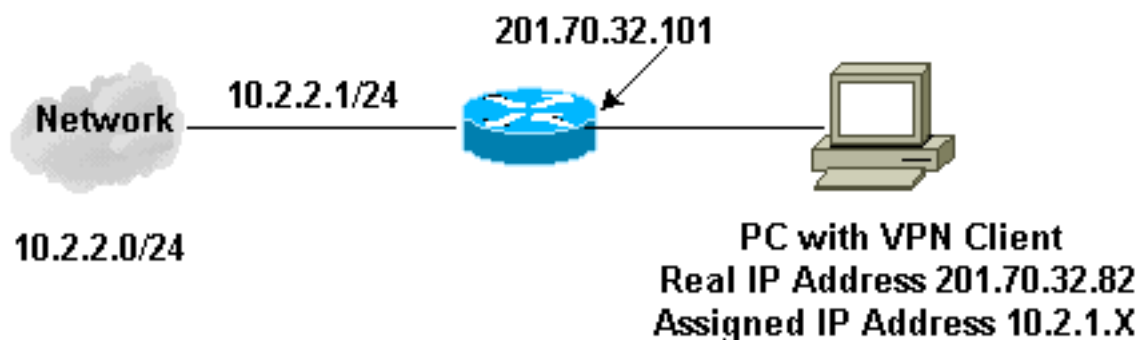
## Configurar

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

**Nota:** Para encontrar información adicional sobre los comandos usados en este documento, utilice la [Command Lookup Tool](#) (sólo clientes registrados) .

## Diagrama de la red

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



## Configuraciones

Este documento usa estas configuraciones.

- [Cliente VPN](#)
- [Router](#)

Configuración de cliente VPN
<pre> Network Security policy:  1- Myconn     My Identity = ip address         Connection security: Secure         Remote Party Identity and addressing             ID Type: IP subnet </pre>

```
10.2.2.0
Port all Protocol all
```

```
Connect using secure tunnel
ID Type: IP address
201.70.32.101
```

```
Authentication (Phase 1)
```

```
Proposal 1
```

```
Authentication method: pre-shared key
Encryp Alg: DES
Hash Alg: MD5
SA life: Unspecified
Key Group: DH 1
```

```
Key exchange (Phase 2)
```

```
Proposal 1
```

```
Encapsulation ESP
Encrypt Alg: DES
Hash Alg: MD5
Encap: tunnel
SA life: Unspecified
no AH
```

```
2- Other Connections
```

```
Connection security: Non-secure
```

```
Local Network Interface
```

```
Name: Any
```

```
IP Addr: Any
```

```
Port: All
```

## Configuración del router

```
Current configuration:
```

```
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Router
!
enable secret 5 $1$v50P$mPuiEQn8ULa8hVMYVOV1D.
enable password ww
!
ip subnet-zero
!
cns event-service server
!
!--- IKE configuration. crypto isakmp policy 1
hash md5
authentication pre-share
crypto isakmp key cisco123 address 0.0.0.0
crypto isakmp client configuration address-pool local
ourpool
!
!--- IPsec configuration. crypto ipsec transform-set
trans1 esp-des esp-md5-hmac
!
crypto dynamic-map dynmap 10
set transform-set trans1
!
crypto map intmap client configuration address initiate
```

```

crypto map intmap client configuration address respond
crypto map intmap 10 ipsec-isakmp dynamic dynmap
!
interface Ethernet0
ip address 201.70.32.101 255.255.255.0
no ip directed-broadcast
ip nat outside
no ip route-cache
no ip mroute-cache
crypto map intmap
!
interface Serial1
ip address 10.2.2.1 255.255.255.0
no ip directed-broadcast
ip nat inside
!
ip local pool ourpool 10.2.1.1 10.2.1.254
ip nat pool outsidepool 201.70.32.150 201.70.32.160
netmask 255.255.255.0
!--- Except the private network to private network
traffic !--- from the NAT process. ip nat inside source
route-map nonat pool outsidepool
ip classless
ip route 0.0.0.0 0.0.0.0 201.70.32.1
no ip http server
!--- Except the private network to private network
traffic !--- from the NAT process. access-list 101 deny
ip 10.2.2.0 0.0.0.255 10.2.1.0 0.0.0.255 access-list 101
permit ip 10.2.2.0 0.0.0.255 any route-map nonat permit
10 match ip address 101 ! line con 0 transport input
none line aux 0 line vty 0 4 password ww login ! end

```

## Verificación

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

La herramienta [Output Interpreter](#) (sólo para clientes registrados) permite utilizar algunos comandos “show” y ver un análisis del resultado de estos comandos.

- **show crypto engine connections active:** muestra los paquetes cifrados y descifrados.
- **show crypto ipsec sa:** muestra las asociaciones de seguridad de la fase 2.
- **show crypto isakmp sa** — Muestra las asociaciones de seguridad de la fase 1.

## Troubleshoot

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

### Comandos para resolución de problemas

**Nota:** Antes de ejecutar un comando **debug**, consulte [Información Importante sobre Comandos Debug](#).

Estas depuraciones deben ejecutarse en ambos routers IPSec (peers). La verificación de las

asociaciones de seguridad se debe realizar en ambos pares

- **debug crypto ipsec** — Muestra los IPSec Negotiations de la Fase 2.
- **debug crypto isakmp** — Muestra las negociaciones ISAKMP para la fase 1.
- **debug crypto engine**: muestra el tráfico cifrado.
- **clear crypto isakmp** — Borra las asociaciones de seguridad relacionadas con la fase 1.
- **clear crypto sa**: borra las asociaciones de seguridad relacionadas con la fase 2.

## Ejemplo de resultado del comando debug

### Depuración del router

```
Apr 18 15:17:59: ISAKMP (4): received packet from
201.70.32.82 (R) MM_NO_STATE
Apr 18 15:17:59: ISAKMP (4): received packet from
201.70.32.82 (R) MM_NO_STATE
Apr 18 15:18:03: ISAKMP (0): received packet from
201.70.32.82 (N) NEW SA
Apr 18 15:18:03: ISAKMP (0:5): processing SA payload.
message ID = 0
Apr 18 15:18:03: ISAKMP (0:5): Checking ISAKMP transform
1
against priority 1 policy
Apr 18 15:18:03: ISAKMP: encryption DES-CBC
Apr 18 15:18:03: ISAKMP: hash MD5
Apr 18 15:18:03: ISAKMP: default group 1
Apr 18 15:18:03: ISAKMP: auth pre-share
Apr 18 15:18:03: ISAKMP (0:5): atts are acceptable.
Next payload is 0
Apr 18 15:18:03: CryptoEngine0: generate alg parameter
Apr 18 15:18:05: CRYPTO_ENGINE: Dh phase 1 status: 0
Apr 18 15:18:05: CRYPTO_ENGINE: Dh phase 1 status: 0
Apr 18 15:18:05: ISAKMP (0:5): SA is doing pre-shared
key authentication
Apr 18 15:18:05: ISAKMP (5): SA is doing pre-shared
key authentication using id type ID_IPV4_ADDR
Apr 18 15:18:05: ISAKMP (5): sending packet to
201.70.32.82 (R) MM_SA_SETUP
Apr 18 15:18:05: ISAKMP (5): received packet from
201.70.32.82 (R) MM_SA_SETUP
Apr 18 15:18:05: ISAKMP (0:5): processing KE payload.
message ID = 0
Apr 18 15:18:05: CryptoEngine0: generate alg parameter
Apr 18 15:18:05: CRYPTO_ENGINE: Dh phase 1 status: 0
Apr 18 15:18:05: CRYPTO_ENGINE: Dh phase 1 status: 0
Apr 18 15:18:05: ISAKMP (0:5): SA is doing pre-shared
key authentication
Apr 18 15:18:05: ISAKMP (5): SA is doing pre-shared
key authentication using id
type ID_IPV4_ADDR
Apr 18 15:18:05: ISAKMP (5): sending packet to
201.70.32.82 (R) MM_SA_SETUP
Apr 18 15:18:05: ISAKMP (5): received packet from
201.70.32.82 (R) MM_SA_SETUP
Apr 18 15:18:05: ISAKMP (0:5): processing KE payload.
message ID = 0
Apr 18 15:18:05: CryptoEngine0: generate alg parameter
Apr 18 15:18:07: ISAKMP (0:5): processing NONCE payload.
message ID = 0
```

```
Apr 18 15:18:07: CryptoEngine0: create ISAKMP SKEYID for
conn id 5
Apr 18 15:18:07: ISAKMP (0:5): SKEYID state generated
Apr 18 15:18:07: ISAKMP (0:5): processing vendor id
payload
Apr 18 15:18:07: ISAKMP (0:5): processing vendor id
payload
Apr 18 15:18:07: ISAKMP (5): sending packet to
201.70.32.82
(R) MM_KEY_EXCH
Apr 18 15:18:07: ISAKMP (0:4): purging SA.
Apr 18 15:18:07: ISAKMP (0:4): purging node -1412157317
Apr 18 15:18:07: ISAKMP (0:4): purging node 1875403554
Apr 18 15:18:07: CryptoEngine0: delete connection 4
Apr 18 15:18:08: ISAKMP (5): received packet from
201.70.32.82 (R) MM_KEY_EXCH
Apr 18 15:18:08: ISAKMP (0:5): processing ID payload.
message ID = 0
Apr 18 15:18:08: ISAKMP (0:5): processing HASH payload.
message ID = 0
Apr 18 15:18:08: CryptoEngine0: generate hmac context
for conn id 5
Apr 18 15:18:08: ISAKMP (5): processing NOTIFY payload
24578 protocol 1 spi 0, message ID = 0
Apr 18 15:18:08: ISAKMP (0:5): SA has been authenticated
with 201.70.32.82
Apr 18 15:18:08: ISAKMP (5): ID payload
next-payload : 8
type : 1
protocol : 17
port : 500
length : 8
Apr 18 15:18:08: ISAKMP (5): Total payload length: 12
Apr 18 15:18:08: CryptoEngine0: generate hmac context
for conn id 5
Apr 18 15:18:08: CryptoEngine0: clear dh number
for conn id 1
Apr 18 15:18:08: ISAKMP (5): sending packet to
201.70.32.82 (R) QM_IDLE
Apr 18 15:18:08: ISAKMP (5): received packet from
201.70.32.82 (R) QM_IDLE
Apr 18 15:18:08: ISAKMP (0:5): Locking struct 14D0DC
on allocation
Apr 18 15:18:08: ISAKMP (0:5): allocating address
10.2.1.1
Apr 18 15:18:08: CryptoEngine0: generate hmac context
for conn id 5
Apr 18 15:18:08: ISAKMP (0:5): initiating peer config to
201.70.32.82. message ID = 1226793520
Apr 18 15:18:08: ISAKMP (5): sending packet to
201.70.32.82
(R) QM_IDLE
Apr 18 15:18:09: ISAKMP (5): received packet from
201.70.32.82
(R) QM_IDLE
Apr 18 15:18:09: ISAKMP (0:5): processing transaction
payload
from 201.70.32.82. message ID = 1226793520
Apr 18 15:18:09: ISAKMP: recieved config from
201.70.32.82 .
Apr 18 15:18:09: CryptoEngine0: generate hmac context
for conn id 5
Apr 18 15:18:09: ISAKMP: Config payload type: 4
Apr 18 15:18:09: ISAKMP (0:5): peer accepted the
```

```
address!
Apr 18 15:18:09: ISAKMP (0:5): adding static route for
10.2.1.1
Apr 18 15:18:09: ISAKMP (0:5): deleting node 1226793520
Apr 18 15:18:09: CryptoEngine0: generate hmac context
for
    conn id 5
Apr 18 15:18:09: ISAKMP (0:5): processing SA payload.
    message ID = -617682048
Apr 18 15:18:09: ISAKMP (0:5): Checking IPsec proposal 1
Apr 18 15:18:09: ISAKMP: transform 1, ESP_DES
Apr 18 15:18:09: ISAKMP:   attributes in transform:
Apr 18 15:18:09: ISAKMP:     authenticator is HMAC-MD5
Apr 18 15:18:09: ISAKMP:     encaps is 1
Apr 18 15:18:09: validate proposal 0
Apr 18 15:18:09: ISAKMP (0:5): atts are acceptable.
Apr 18 15:18:09: IPSEC(validate_proposal_request):
    proposal part #1, (key eng. msg.) dest=
201.70.32.101,
    src= 201.70.32.82, dest_proxy=
10.2.2.0/255.255.255.0/0/0
    (type=4), src_proxy= 10.2.1.1/255.255.255.255/0/0
(type=1),
    protocol= ESP, transform= esp-des esp-md5-hmac ,
    lifedur= 0s and 0kb, spi= 0x0(0), conn_id= 0,
keysize= 0,
    flags= 0x4
Apr 18 15:18:09: validate proposal request 0
Apr 18 15:18:09: ISAKMP (0:5): processing NONCE payload.
    message ID = -617682048
Apr 18 15:18:09: ISAKMP (0:5): processing ID payload.
    message ID = -617682048
Apr 18 15:18:09: ISAKMP (5): ID_IPV4_ADDR src 10.2.1.1
    prot 0 port 0
Apr 18 15:18:09: ISAKMP (0:5): processing ID payload.
    message ID = -617682048
Apr 18 15:18:09: ISAKMP (5): ID_IPV4_ADDR_SUBNET dst
    10.2.2.0/255.255.255.0 prot 0 port 0
Apr 18 15:18:09: IPSEC(key_engine): got a queue event...
Apr 18 15:18:09: IPSEC(spi_response): getting spi
    153684796 for SA from 201.70.32.82   to
201.70.32.101
    for prot 3
Apr 18 15:18:09: CryptoEngine0: generate hmac context
for conn id 5
Apr 18 15:18:09: ISAKMP (5): sending packet to
201.70.32.82
    (R) QM_IDLE
Apr 18 15:18:09: ISAKMP (5): received packet from
201.70.32.82
    (R) QM_IDLE
Apr 18 15:18:09: CryptoEngine0: generate hmac context
for conn id 5
Apr 18 15:18:09: ISAKMP (0:5): processing SA payload.
    message ID = -1078114754
Apr 18 15:18:09: ISAKMP (0:5): Checking IPsec proposal 1
Apr 18 15:18:10: ISAKMP: transform 1, ESP_DES
Apr 18 15:18:10: ISAKMP:   attributes in transform:
Apr 18 15:18:10: ISAKMP:     authenticator is HMAC-MD5
Apr 18 15:18:10: ISAKMP:     encaps is 1
Apr 18 15:18:10: validate proposal 0
Apr 18 15:18:10: ISAKMP (0:5): atts are acceptable.
Apr 18 15:18:10: IPSEC(validate_proposal_request):
    proposal part #1, (key eng. msg.) dest=
```

```
201.70.32.101,
  src= 201.70.32.82, dest_proxy=
10.2.2.0/255.255.255.0/0/0
  (type=4), src_proxy= 10.2.1.1/255.255.255.255/0/0
(type=1),
  protocol= ESP, transform= esp-des esp-md5-hmac ,
  lifedur= 0s and 0kb, spi= 0x0(0), conn_id= 0,
keysize= 0,
  flags= 0x4
Apr 18 15:18:10: validate proposal request 0
Apr 18 15:18:10: ISAKMP (0:5): processing NONCE payload.
  message ID = -1078114754
Apr 18 15:18:10: ISAKMP (0:5): processing ID payload.
  message ID = -1078114754
Apr 18 15:18:10: ISAKMP (5): ID_IPV4_ADDR src 10.2.1.1
  prot 0 port 0
Apr 18 15:18:10: ISAKMP (0:5): processing ID payload.
  message ID = -1078114754
Apr 18 15:18:10: ISAKMP (5): ID_IPV4_ADDR_SUBNET dst
  10.2.2.0/255.255.255.0 prot 0 port 0
Apr 18 15:18:10: IPSEC(key_engine): got a queue event...
Apr 18 15:18:10: IPSEC(spi_response): getting spi
224008976
  for SA from 201.70.32.82   to 201.70.32.101
  for prot 3
Apr 18 15:18:10: CryptoEngine0: generate hmac context
  for conn id 5
Apr 18 15:18:10: ISAKMP (5): sending packet to
201.70.32.82
  (R) QM_IDLE
Apr 18 15:18:10: ISAKMP (5): received packet from
201.70.32.82
  (R) QM_IDLE
Apr 18 15:18:10: CryptoEngine0: generate hmac context
  for conn id 5
Apr 18 15:18:10: ipsec allocate flow 0
Apr 18 15:18:10: ipsec allocate flow 0
Apr 18 15:18:10: ISAKMP (0:5): Creating IPsec SAs
Apr 18 15:18:10:      inbound SA from 201.70.32.82
  to 201.70.32.101  (proxy 10.2.1.1   to
10.2.2.0)
Apr 18 15:18:10:      has spi 224008976 and conn_id
2000
  and flags 4
Apr 18 15:18:10:      outbound SA from 201.70.32.101
  to 201.70.32.82  (proxy 10.2.2.0   to
10.2.1.1)
Apr 18 15:18:10:      has spi -1084694986 and conn_id
2001
  and flags 4
Apr 18 15:18:10: ISAKMP (0:5): deleting node -1078114754
Apr 18 15:18:10: IPSEC(key_engine): got a queue event...
Apr 18 15:18:10: IPSEC(initialize_sas): ,
  (key eng. msg.) dest= 201.70.32.101, src=
201.70.32.82,
  dest_proxy= 10.2.2.0/255.255.255.0/0/0 (type=4),
  src_proxy= 10.2.1.1/0.0.0.0/0/0 (type=1),
  protocol= ESP, transform= esp-des esp-md5-hmac ,
  lifedur= 0s and 0kb,
  spi= 0xD5A1B10(224008976), conn_id= 2000, keysize=
0,
  flags= 0x4
Apr 18 15:18:10: IPSEC(initialize_sas): ,
  (key eng. msg.) src= 201.70.32.101, dest=
```



```

201.70.32.82,
  src_proxy= 10.2.2.0/255.255.255.0/0/0 (type=4),
  dest_proxy= 10.2.1.1/0.0.0.0/0/0 (type=1),
  protocol= ESP, transform= esp-des esp-md5-hmac ,
  lifedur= 0s and 0kb,
  spi= 0xBF58DE36(3210272310), conn_id= 2001, keysize=
0,
  flags= 0x4
Apr 18 15:18:10: IPSEC(create_sa): sa created,
  (sa) sa_dest= 201.70.32.101, sa_prot= 50,
  sa_spi= 0xD5A1B10(224008976),
  sa_trans= esp-des esp-md5-hmac , sa_conn_id= 2000
Apr 18 15:18:10: IPSEC(create_sa): sa created,
  (sa) sa_dest= 201.70.32.82, sa_prot= 50,
  sa_spi= 0xBF58DE36(3210272310),
  sa_trans= esp-des esp-md5-hmac , sa_conn_id= 2001
Apr 18 15:18:10: ISAKMP: Locking struct 14D0DC for IPSEC
Apr 18 15:18:24: ISAKMP (0:5): retransmitting
  phase 2 -617682048 ...
Apr 18 15:18:24: ISAKMP (5): sending packet to
201.70.32.82
  (R) QM_IDLE

Router#show crypto ipsec
Apr 18 15:18:39: ISAKMP (0:5): retransmitting
  phase 2 -617682048 ...
Apr 18 15:18:39: ISAKMP (5): sending packet to
201.70.32.82
  (R) QM_IDLE      sa

interface: Ethernet0
  Crypto map tag: intmap, local addr. 201.70.32.101

  local ident (addr/mask/prot/port):
  (10.2.2.0/255.255.255.0/0/0)
  remote ident (addr/mask/prot/port):
  (10.2.1.1/255.255.255.255/0/0)
  current_peer: 201.70.32.82
  PERMIT, flags={}
  #pkts encaps: 7, #pkts encrypt: 7, #pkts digest 7
  #pkts decaps: 7, #pkts decrypt: 7, #pkts verify 7
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 0, #pkts compr. failed: 0,
  #pkts decompress failed: 0
  #send errors 0, #recv errors 0

  local crypto endpt.: 201.70.32.101, remote
  crypto endpt.: 201.70.32.82
  path mtu 1500, media mtu 1500
  current outbound spi: BF58DE36

  inbound esp sas:
  spi: 0xD5A1B10(224008976)
  transform: esp-des esp-md5-hmac ,
  in use settings = {Tunnel, }
  slot: 0, conn id: 2000, flow_id: 1,
  crypto map: intmap
  sa timing: remaining key lifetime
  (k/sec): (4607999/3500)
  IV size: 8 bytes
  replay detection support: Y

  inbound ah sas:

```

inbound pcp sas:

outbound esp sas:

```
spi: 0xBF58DE36(3210272310)
transform: esp-des esp-md5-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 2001, flow_id: 2,
crypto map: intmap
sa timing: remaining key lifetime
(k/sec): (4607999/3500)
IV size: 8 bytes
replay detection support: Y
```

outbound ah sas:

outbound pcp sas:

Router#**sho crypto engine connections active**

ID	Interface	IP-Address	State	Algorithm
Encrypt	Decrypt			
5		set		HMAC_MD5+DES_56_CB
0	0			
2000	Ethernet0	201.70.32.101	set	
HMAC_MD5+DES_56_CB	0	7		
2001	Ethernet0	201.70.32.101	set	
HMAC_MD5+DES_56_CB	7	0		

Crypto adjacency count : Lock: 0, Unlock: 0

## Información del Cliente VPN

Client configuration:

C:\>ping -t 10.2.2.5

Reply from 10.2.2.5: bytes=32 time<0ms TTL=352

Reply from 10.2.2.5: bytes=32 time<10ms TTL=352

From Logview:

14:25:34.044 New Connection - Initiating IKE  
Phase 1 (IP ADDR=201.70.32.101)

14:25:34.144 New Connection - SENDING>>>> ISAKMP  
OAK MM (SA)

14:25:35.886 New Connection - RECEIVED<<< ISAKMP  
OAK MM (SA)

14:25:36.067 New Connection - SENDING>>>> ISAKMP  
OAK MM (KE, NON, VID, VID)

14:25:38.310 New Connection - RECEIVED<<< ISAKMP  
OAK MM (KE, NON, VID)

14:25:38.460 New Connection - SENDING>>>> ISAKMP  
OAK MM \*(ID, HASH, NOTIFY:STATUS\_INITIAL\_CONTACT)

14:25:38.610 New Connection - RECEIVED<<< ISAKMP  
OAK MM \*(ID, HASH)

14:25:38.710 New Connection - Established IKE SA

14:25:38.811 New Connection - Initiating IKE Phase  
2 with Client IDs (message id  
: B01876)

14:25:38.911 Initiator = IP ADDR=201.70.32.82,  
prot = 0 port = 0

```
14:25:39.011 Responder = IP
SUBNET/MASK=10.2.2.0/255.255.255.0,
  prot = 0 port = 0

14:25:39.111 New Connection - SENDING>>>>
  ISAKMP OAK QM *(HASH, SA, NON, ID, ID)
14:25:39.251 New Connection - RECEIVED<<< ISAKMP
  OAK TRANS *(HASH, ATTR)
14:25:39.351 New Connection - Received Private IP
  Address = IP ADDR=10.2.1.1

14:25:39.451 New Connection - Discarding IPSec SA
  negotiation (message id: B01876)
14:25:39.552 New Connection - SENDING>>>> ISAKMP OAK
  TRANS *(HASH, ATTR)
14:25:40.022 New Connection - Received message for
  discarded
  IPSec SA negotiation (message id: B01876)
14:25:40.122 New Connection - Initiating IKE Phase 2
  with
  Client IDs (message id: C8CB0CE)
14:25:40.223 Initiator = IP ADDR=10.2.1.1, prot = 0
  port = 0
14:25:40.323 Responder = IP
SUBNET/MASK=10.2.2.0/255.255.255.0,
  prot = 0 port = 0
14:25:40.423 New Connection - SENDING>>>> ISAKMP OAK
  QM *(HASH, SA, NON, ID, ID)
14:25:40.873 New Connection - RECEIVED<<< ISAKMP OAK
  QM *(HASH, SA, NON, ID, ID,
  NOTIFY:STATUS_RESP_LIFETIME)
14:25:40.974 New Connection - SENDING>>>> ISAKMP OAK
  QM *(HASH)
14:25:41.074 New Connection - Loading IPSec SA
  (Message ID = C8CB0CE OUTBOUND SPI = 19A22423
  INBOUND SPI = E4829433)
14:25:41.174
```

## [Información Relacionada](#)

- [Configuración de seguridad de red IPSec](#)
- [Configuración del protocolo de seguridad de intercambio de claves de Internet](#)
- [Presentación del IPSec](#)
- [Páginas de soporte de productos de seguridad IP \(IPSec\)](#)
- [Soporte Técnico - Cisco Systems](#)