Contenido

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.

prerrequisitos

Requisitos

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.

- Software Release 12.0.7T o Posterior de Cisco IOS®
- Hardware que soporta esta revisión del software
- CiscoSecure VPN cliente 1.0/10A o 1.1 (mostrado como 2.0.7/E o 2.1.12, vaya respectivamente al **Help (Ayuda) > About (Acerca de)** a marcar)

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

Para obtener más información sobre las convenciones del documento, consulte las Convenciones de Consejos Técnicos de Cisco.

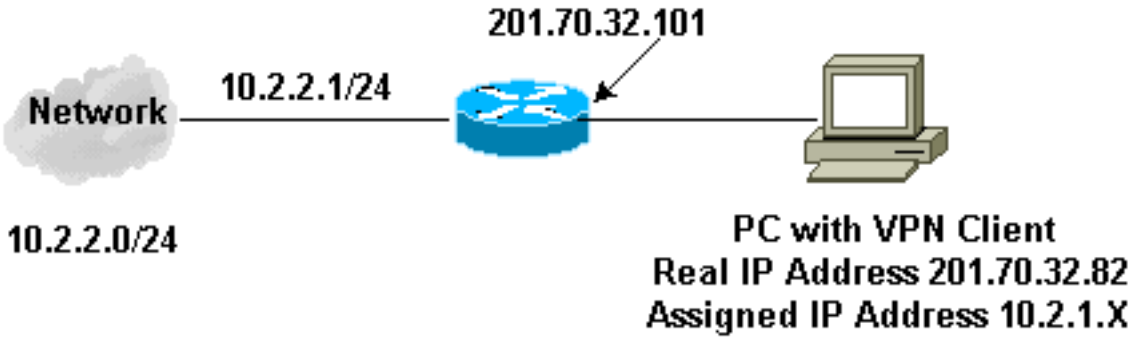
Configurar

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 Command Lookup Tool (solo para 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
Configuración del router
Current configuration:!version 12.0service timestamps debug uptimeservice timestamps log uptimeno service password-encryption!hostname Router!enable secret 5 1v5OP$mPuiEQn8ULa8hVMYVOV1D.enable password ww!ip subnet-zero!cns event-service server!*!--- IKE configuration.* **crypto isakmp policy 1hash md5authentication pre-sharecrypto isakmp key cisco123 address 0.0.0.0crypto isakmp client configuration address-pool local ourpool!***!--- IPSec configuration.***crypto ipsec transform-set trans1 esp-des esp-md5-hmac!crypto dynamic-map dynmap 10set transform-set trans1!crypto map intmap client configuration**

```
address initiatecrypto map intmap client configuration
address respondcrypto map intmap 10 ipsec-isakmp dynamic
dynmap ! interface Ethernet0ip address 201.70.32.101
255.255.255.0 no ip directed-broadcastip nat outsideno
ip route-cacheno ip mroute-cache crypto map intmap
!interface Serial1ip address 10.2.2.1 255.255.255.0no ip
directed-broadcastip nat inside! ip local pool ourpool
10.2.1.1 10.2.1.254ip 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 classlessip route 0.0.0.0 0.0.0.0
201.70.32.1no 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 0.0.0.255access-list 101 permit ip 10.2.2.0
0.0.0.255 anyroute-map nonat permit 10match ip address
101 !line con 0transport input noneline aux 0line vty 0
4password wwlogin!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.

- ¿**active del show crypto engine connections**? Muestra los paquetes encriptados y desencriptados.
- ¿**muestre IPSec crypto sa**? Muestra a fase 2 asociaciones de seguridad.
- ¿**muestre isakmp crypto sa**? Muestra las asociaciones de seguridad de la fase 1.

Troubleshooting

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

Comandos para resolución de problemas

Nota: Antes de ejecutar un comando de depuración, consulte Información importante sobre comandos de depuración.

Estos debugs deben ejecutarse en ambos routeres IPSec (pares). La verificación de las asociaciones de seguridad se debe realizar en ambos pares

- ¿**IPSec del debug crypto**? Visualiza los IPSec Negotiations de la fase 2.
- ¿**isakmp del debug crypto**? Visualiza negociaciones ISAKMP de la fase 1.
- ¿**motor del debug crypto**? Visualiza el tráfico se cifra que.
- ¿**borre el isakmp crypto**? Borra las asociaciones de seguridad relacionadas con la fase 1.
- ¿**borre el sa crypto**? 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_STATEApr 18 15:17:59: ISAKMP (4):
received packet from     201.70.32.82 (R) MM_NO_STATEApr
18 15:18:03: ISAKMP (0): received packet from
201.70.32.82 (N) NEW SAApr 18 15:18:03: ISAKMP (0:5):
processing SA payload.     message ID = 0Apr 18
15:18:03: ISAKMP (0:5): Checking ISAKMP transform 1
against priority 1 policyApr 18 15:18:03: ISAKMP:
encryption DES-CBCApr 18 15:18:03: ISAKMP:      hash
MD5Apr 18 15:18:03: ISAKMP:      default group 1Apr 18
15:18:03: ISAKMP:      auth pre-shareApr 18 15:18:03:
ISAKMP (0:5): atts are acceptable.     Next payload is
0Apr 18 15:18:03: CryptoEngine0: generate alg
parameterApr 18 15:18:05: CRYPTO_ENGINE: Dh phase 1
status: 0Apr 18 15:18:05: CRYPTO_ENGINE: Dh phase 1
status: 0Apr 18 15:18:05: ISAKMP (0:5): SA is doing pre-
shared     key authenticationApr 18 15:18:05: ISAKMP
(5): SA is doing pre-shared     key authentication using
id type ID_IPV4_ADDRApr 18 15:18:05: ISAKMP (5): sending
packet to     201.70.32.82 (R) MM_SA_SETUPApr 18
15:18:05: ISAKMP (5): received packet from
201.70.32.82 (R) MM_SA_SETUPApr 18 15:18:05: ISAKMP
(0:5): processing KE payload.     message ID = 0Apr 18
15:18:05: CryptoEngine0: generate alg parameterApr 18
15:18:05: CRYPTO_ENGINE: Dh phase 1 status: 0Apr 18
15:18:05: CRYPTO_ENGINE: Dh phase 1 status: 0Apr 18
15:18:05: ISAKMP (0:5): SA is doing pre-shared     key
authenticationApr 18 15:18:05: ISAKMP (5): SA is doing
pre-shared     key authentication using idtype
ID_IPV4_ADDRApr 18 15:18:05: ISAKMP (5): sending packet
to     201.70.32.82 (R) MM_SA_SETUPApr 18 15:18:05:
ISAKMP (5): received packet from     201.70.32.82 (R)
MM_SA_SETUPApr 18 15:18:05: ISAKMP (0:5): processing KE
payload.     message ID = 0Apr 18 15:18:05:
CryptoEngine0: generate alg parameterApr 18 15:18:07:
ISAKMP (0:5): processing NONCE payload.     message ID =
0Apr 18 15:18:07: CryptoEngine0: create ISAKMP SKEYID
for     conn id 5Apr 18 15:18:07: ISAKMP (0:5): SKEYID
state generatedApr 18 15:18:07: ISAKMP (0:5): processing
vendor id payloadApr 18 15:18:07: ISAKMP (0:5):
processing vendor id payloadApr 18 15:18:07: ISAKMP (5):
sending packet to 201.70.32.82     (R) MM_KEY_EXCHApr 18
15:18:07: ISAKMP (0:4): purging SA.Apr 18 15:18:07:
ISAKMP (0:4): purging node -1412157317Apr 18 15:18:07:
ISAKMP (0:4): purging node 1875403554Apr 18 15:18:07:
CryptoEngine0: delete connection 4Apr 18 15:18:08:
ISAKMP (5): received packet from     201.70.32.82 (R)
MM_KEY_EXCHApr 18 15:18:08: ISAKMP (0:5): processing ID
payload.     message ID = 0Apr 18 15:18:08: ISAKMP
(0:5): processing HASH payload.     message ID = 0Apr 18
15:18:08: CryptoEngine0: generate hmac context     for
conn id 5Apr 18 15:18:08: ISAKMP (5): processing NOTIFY
payload     24578 protocol 1 spi 0, message ID = 0Apr 18
15:18:08: ISAKMP (0:5): SA has been authenticated
with 201.70.32.82Apr 18 15:18:08: ISAKMP (5): ID payload
next-payload : 8        type         : 1        protocol
: 17        port         : 500        length       :
8Apr 18 15:18:08: ISAKMP (5): Total payload length:
12Apr 18 15:18:08: CryptoEngine0: generate hmac context
```

```
for conn id 5Apr 18 15:18:08: CryptoEngine0: clear dh
number     for conn id 1Apr 18 15:18:08: ISAKMP (5):
sending packet to     201.70.32.82 (R) QM_IDLEApr 18
15:18:08: ISAKMP (5): received packet from
201.70.32.82 (R) QM_IDLEApr 18 15:18:08: ISAKMP (0:5):
Locking struct 14D0DC     on allocationApr 18 15:18:08:
ISAKMP (0:5): allocating address     10.2.1.1Apr 18
15:18:08: CryptoEngine0: generate hmac context     for
conn id 5Apr 18 15:18:08: ISAKMP (0:5): initiating peer
config to     201.70.32.82. message ID = 1226793520Apr
18 15:18:08: ISAKMP (5): sending packet to 201.70.32.82
(R) QM_IDLEApr 18 15:18:09: ISAKMP (5): received packet
from 201.70.32.82     (R) QM_IDLEApr 18 15:18:09: ISAKMP
(0:5): processing transaction payload     from
201.70.32.82. message ID = 1226793520Apr 18 15:18:09:
ISAKMP: recieved config from 201.70.32.82   .Apr 18
15:18:09: CryptoEngine0: generate hmac context     for
conn id 5Apr 18 15:18:09: ISAKMP:     Config payload
type: 4Apr 18 15:18:09: ISAKMP (0:5): peer accepted the
address!Apr 18 15:18:09: ISAKMP (0:5): adding static
route for 10.2.1.1Apr 18 15:18:09: ISAKMP (0:5):
deleting node 1226793520Apr 18 15:18:09: CryptoEngine0:
generate hmac context for     conn id 5Apr 18 15:18:09:
ISAKMP (0:5): processing SA payload.     message ID = -
617682048Apr 18 15:18:09: ISAKMP (0:5): Checking IPSec
proposal 1Apr 18 15:18:09: ISAKMP: transform 1,
ESP_DESApr 18 15:18:09: ISAKMP:   attributes in
transform:Apr 18 15:18:09: ISAKMP:      authenticator is
HMAC-MD5Apr 18 15:18:09: ISAKMP:      encaps is 1Apr 18
15:18:09: validate proposal 0Apr 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= 0x4Apr 18 15:18:09: validate
proposal request 0Apr 18 15:18:09: ISAKMP (0:5):
processing NONCE payload.     message ID = -617682048Apr
18 15:18:09: ISAKMP (0:5): processing ID payload.
message ID = -617682048Apr 18 15:18:09: ISAKMP (5):
ID_IPV4_ADDR src 10.2.1.1     prot 0 port 0Apr 18
15:18:09: ISAKMP (0:5): processing ID payload.
message ID = -617682048Apr 18 15:18:09: ISAKMP (5):
ID_IPV4_ADDR_SUBNET dst     10.2.2.0/255.255.255.0 prot
0 port 0Apr 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 3Apr 18 15:18:09:
CryptoEngine0: generate hmac context     for conn id
5Apr 18 15:18:09: ISAKMP (5): sending packet to
201.70.32.82     (R) QM_IDLEApr 18 15:18:09: ISAKMP (5):
received packet from 201.70.32.82     (R) QM_IDLEApr 18
15:18:09: CryptoEngine0: generate hmac context     for
conn id 5Apr 18 15:18:09: ISAKMP (0:5): processing SA
payload.     message ID = -1078114754Apr 18 15:18:09:
ISAKMP (0:5): Checking IPSec proposal 1Apr 18 15:18:10:
ISAKMP: transform 1, ESP_DESApr 18 15:18:10: ISAKMP:
attributes in transform:Apr 18 15:18:10: ISAKMP:
authenticator is HMAC-MD5Apr 18 15:18:10: ISAKMP:
encaps is 1Apr 18 15:18:10: validate proposal 0Apr 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= 0x4Apr 18 15:18:10: validate
proposal request 0Apr 18 15:18:10: ISAKMP (0:5):
processing NONCE payload.     message ID = -
1078114754Apr 18 15:18:10: ISAKMP (0:5): processing ID
payload.     message ID = -1078114754Apr 18 15:18:10:
ISAKMP (5): ID_IPV4_ADDR src 10.2.1.1     prot 0 port
0Apr 18 15:18:10: ISAKMP (0:5): processing ID payload.
message ID = -1078114754Apr 18 15:18:10: ISAKMP (5):
ID_IPV4_ADDR_SUBNET dst     10.2.2.0/255.255.255.0 prot
0 port 0Apr 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 3Apr 18 15:18:10:
CryptoEngine0: generate hmac context     for conn id
5Apr 18 15:18:10: ISAKMP (5): sending packet to
201.70.32.82     (R) QM_IDLEApr 18 15:18:10: ISAKMP (5):
received packet from 201.70.32.82     (R) QM_IDLEApr 18
15:18:10: CryptoEngine0: generate hmac context     for
conn id 5Apr 18 15:18:10: ipsec allocate flow 0Apr 18
15:18:10: ipsec allocate flow 0Apr 18 15:18:10: ISAKMP
(0:5): Creating IPSec SAsApr 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 4Apr 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 4Apr 18 15:18:10: ISAKMP
(0:5): deleting node -1078114754Apr 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= 0x4Apr 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= 0x4Apr 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= 2000Apr 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= 2001Apr 18 15:18:10: ISAKMP:
Locking struct 14D0DC for IPSECApr 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_IDLERouter#show crypto ipsecApr 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      sainterface: 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        02000
Ethernet0       201.70.32.101   set
HMAC_MD5+DES_56_CB  0        72001 Ethernet0
201.70.32.101   set    HMAC_MD5+DES_56_CB  7
0Crypto adjacency count : Lock: 0, Unlock: 0
```

Información del cliente VPN

```
Apr 18 15:17:59: ISAKMP (4): received packet from
201.70.32.82 (R) MM_NO_STATEApr 18 15:17:59: ISAKMP (4):
received packet from     201.70.32.82 (R) MM_NO_STATEApr
18 15:18:03: ISAKMP (0): received packet from
201.70.32.82 (N) NEW SAApr 18 15:18:03: ISAKMP (0:5):
processing SA payload.     message ID = 0Apr 18
15:18:03: ISAKMP (0:5): Checking ISAKMP transform 1
against priority 1 policyApr 18 15:18:03: ISAKMP:
encryption DES-CBCApr 18 15:18:03: ISAKMP:      hash
MD5Apr 18 15:18:03: ISAKMP:      default group 1Apr 18
15:18:03: ISAKMP:      auth pre-shareApr 18 15:18:03:
ISAKMP (0:5): atts are acceptable.     Next payload is
0Apr 18 15:18:03: CryptoEngine0: generate alg
parameterApr 18 15:18:05: CRYPTO_ENGINE: Dh phase 1
status: 0Apr 18 15:18:05: CRYPTO_ENGINE: Dh phase 1
status: 0Apr 18 15:18:05: ISAKMP (0:5): SA is doing pre-
shared     key authenticationApr 18 15:18:05: ISAKMP
(5): SA is doing pre-shared     key authentication using
id type ID_IPV4_ADDRApr 18 15:18:05: ISAKMP (5): sending
packet to     201.70.32.82 (R) MM_SA_SETUPApr 18
15:18:05: ISAKMP (5): received packet from
201.70.32.82 (R) MM_SA_SETUPApr 18 15:18:05: ISAKMP
(0:5): processing KE payload.     message ID = 0Apr 18
15:18:05: CryptoEngine0: generate alg parameterApr 18
15:18:05: CRYPTO_ENGINE: Dh phase 1 status: 0Apr 18
15:18:05: CRYPTO_ENGINE: Dh phase 1 status: 0Apr 18
```

```
15:18:05: ISAKMP (0:5): SA is doing pre-shared     key
authenticationApr 18 15:18:05: ISAKMP (5): SA is doing
pre-shared     key authentication using idtype
ID_IPV4_ADDRApr 18 15:18:05: ISAKMP (5): sending packet
to     201.70.32.82 (R) MM_SA_SETUPApr 18 15:18:05:
ISAKMP (5): received packet from     201.70.32.82 (R)
MM_SA_SETUPApr 18 15:18:05: ISAKMP (0:5): processing KE
payload.     message ID = 0Apr 18 15:18:05:
CryptoEngine0: generate alg parameterApr 18 15:18:07:
ISAKMP (0:5): processing NONCE payload.     message ID =
0Apr 18 15:18:07: CryptoEngine0: create ISAKMP SKEYID
for     conn id 5Apr 18 15:18:07: ISAKMP (0:5): SKEYID
state generatedApr 18 15:18:07: ISAKMP (0:5): processing
vendor id payloadApr 18 15:18:07: ISAKMP (0:5):
processing vendor id payloadApr 18 15:18:07: ISAKMP (5):
sending packet to 201.70.32.82     (R) MM_KEY_EXCHApr 18
15:18:07: ISAKMP (0:4): purging SA.Apr 18 15:18:07:
ISAKMP (0:4): purging node -1412157317Apr 18 15:18:07:
ISAKMP (0:4): purging node 1875403554Apr 18 15:18:07:
CryptoEngine0: delete connection 4Apr 18 15:18:08:
ISAKMP (5): received packet from     201.70.32.82 (R)
MM_KEY_EXCHApr 18 15:18:08: ISAKMP (0:5): processing ID
payload.     message ID = 0Apr 18 15:18:08: ISAKMP
(0:5): processing HASH payload.     message ID = 0Apr 18
15:18:08: CryptoEngine0: generate hmac context     for
conn id 5Apr 18 15:18:08: ISAKMP (5): processing NOTIFY
payload     24578 protocol 1 spi 0, message ID = 0Apr 18
15:18:08: ISAKMP (0:5): SA has been authenticated
with 201.70.32.82Apr 18 15:18:08: ISAKMP (5): ID payload
next-payload : 8        type         : 1        protocol
: 17        port         : 500        length       :
8Apr 18 15:18:08: ISAKMP (5): Total payload length:
12Apr 18 15:18:08: CryptoEngine0: generate hmac context
for conn id 5Apr 18 15:18:08: CryptoEngine0: clear dh
number     for conn id 1Apr 18 15:18:08: ISAKMP (5):
sending packet to     201.70.32.82 (R) QM_IDLEApr 18
15:18:08: ISAKMP (5): received packet from
201.70.32.82 (R) QM_IDLEApr 18 15:18:08: ISAKMP (0:5):
Locking struct 14D0DC     on allocationApr 18 15:18:08:
ISAKMP (0:5): allocating address     10.2.1.1Apr 18
15:18:08: CryptoEngine0: generate hmac context     for
conn id 5Apr 18 15:18:08: ISAKMP (0:5): initiating peer
config to     201.70.32.82. message ID = 1226793520Apr
18 15:18:08: ISAKMP (5): sending packet to 201.70.32.82
(R) QM_IDLEApr 18 15:18:09: ISAKMP (5): received packet
from 201.70.32.82     (R) QM_IDLEApr 18 15:18:09: ISAKMP
(0:5): processing transaction payload     from
201.70.32.82. message ID = 1226793520Apr 18 15:18:09:
ISAKMP: recieved config from 201.70.32.82   .Apr 18
15:18:09: CryptoEngine0: generate hmac context     for
conn id 5Apr 18 15:18:09: ISAKMP:     Config payload
type: 4Apr 18 15:18:09: ISAKMP (0:5): peer accepted the
address!Apr 18 15:18:09: ISAKMP (0:5): adding static
route for 10.2.1.1Apr 18 15:18:09: ISAKMP (0:5):
deleting node 1226793520Apr 18 15:18:09: CryptoEngine0:
generate hmac context for     conn id 5Apr 18 15:18:09:
ISAKMP (0:5): processing SA payload.     message ID = -
617682048Apr 18 15:18:09: ISAKMP (0:5): Checking IPSec
proposal 1Apr 18 15:18:09: ISAKMP: transform 1,
ESP_DESApr 18 15:18:09: ISAKMP:   attributes in
transform:Apr 18 15:18:09: ISAKMP:      authenticator is
HMAC-MD5Apr 18 15:18:09: ISAKMP:      encaps is 1Apr 18
15:18:09: validate proposal 0Apr 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= 0x4Apr 18 15:18:09: validate
proposal request 0Apr 18 15:18:09: ISAKMP (0:5):
processing NONCE payload.     message ID = -617682048Apr
18 15:18:09: ISAKMP (0:5): processing ID payload.
message ID = -617682048Apr 18 15:18:09: ISAKMP (5):
ID_IPV4_ADDR src 10.2.1.1     prot 0 port 0Apr 18
15:18:09: ISAKMP (0:5): processing ID payload.
message ID = -617682048Apr 18 15:18:09: ISAKMP (5):
ID_IPV4_ADDR_SUBNET dst     10.2.2.0/255.255.255.0 prot
0 port 0Apr 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 3Apr 18 15:18:09:
CryptoEngine0: generate hmac context     for conn id
5Apr 18 15:18:09: ISAKMP (5): sending packet to
201.70.32.82     (R) QM_IDLEApr 18 15:18:09: ISAKMP (5):
received packet from 201.70.32.82     (R) QM_IDLEApr 18
15:18:09: CryptoEngine0: generate hmac context     for
conn id 5Apr 18 15:18:09: ISAKMP (0:5): processing SA
payload.     message ID = -1078114754Apr 18 15:18:09:
ISAKMP (0:5): Checking IPSec proposal 1Apr 18 15:18:10:
ISAKMP: transform 1, ESP_DESApr 18 15:18:10: ISAKMP:
attributes in transform:Apr 18 15:18:10: ISAKMP:
authenticator is HMAC-MD5Apr 18 15:18:10: ISAKMP:
encaps is 1Apr 18 15:18:10: validate proposal 0Apr 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= 0x4Apr 18 15:18:10: validate
proposal request 0Apr 18 15:18:10: ISAKMP (0:5):
processing NONCE payload.     message ID = -
1078114754Apr 18 15:18:10: ISAKMP (0:5): processing ID
payload.     message ID = -1078114754Apr 18 15:18:10:
ISAKMP (5): ID_IPV4_ADDR src 10.2.1.1     prot 0 port
0Apr 18 15:18:10: ISAKMP (0:5): processing ID payload.
message ID = -1078114754Apr 18 15:18:10: ISAKMP (5):
ID_IPV4_ADDR_SUBNET dst     10.2.2.0/255.255.255.0 prot
0 port 0Apr 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 3Apr 18 15:18:10:
CryptoEngine0: generate hmac context     for conn id
5Apr 18 15:18:10: ISAKMP (5): sending packet to
201.70.32.82     (R) QM_IDLEApr 18 15:18:10: ISAKMP (5):
received packet from 201.70.32.82     (R) QM_IDLEApr 18
15:18:10: CryptoEngine0: generate hmac context     for
conn id 5Apr 18 15:18:10: ipsec allocate flow 0Apr 18
15:18:10: ipsec allocate flow 0Apr 18 15:18:10: ISAKMP
(0:5): Creating IPSec SAsApr 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 4Apr 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 4Apr 18 15:18:10: ISAKMP
(0:5): deleting node -1078114754Apr 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= 0x4Apr 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= 0x4Apr 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= 2000Apr 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= 2001Apr 18 15:18:10: ISAKMP:
Locking struct 14D0DC for IPSECApr 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_IDLERouter#show crypto ipsecApr 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      sainterface: 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         02000
Ethernet0       201.70.32.101   set
HMAC_MD5+DES_56_CB  0         72001 Ethernet0
201.70.32.101   set    HMAC_MD5+DES_56_CB  7
0Crypto adjacency count : Lock: 0, Unlock: 0
```

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