

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Configurar](#)

[Diagrama de la red](#)

[Configuraciones](#)

[Verificación](#)

[PIX](#)

[Concentrador VPN](#)

[Troubleshooting](#)

[Comandos para resolución de problemas](#)

[Información Relacionada](#)

[Introducción](#)

Este documento describe cómo configurar el Cisco Secure PIX Firewall en IPsec sitio a sitio un VPN con los direccionamientos de red privada superpuesta detrás de los gateways de VPN. La característica de la Traducción de dirección de red mejorada (NAT) introducida en PIX 6.2 se utiliza en este ejemplo para traducir las redes superpuestas en cada lado del túnel del IPsec VPN a los espacios de la dirección sin traslapo.

[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.

- Cisco Secure PIX Firewall 506 con la versión de software 6.3(3)
- Concentrador del VPN 3030 con la versión de software 4.1(5)

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 [Convenciones de Consejos Técnicos de Cisco](#).

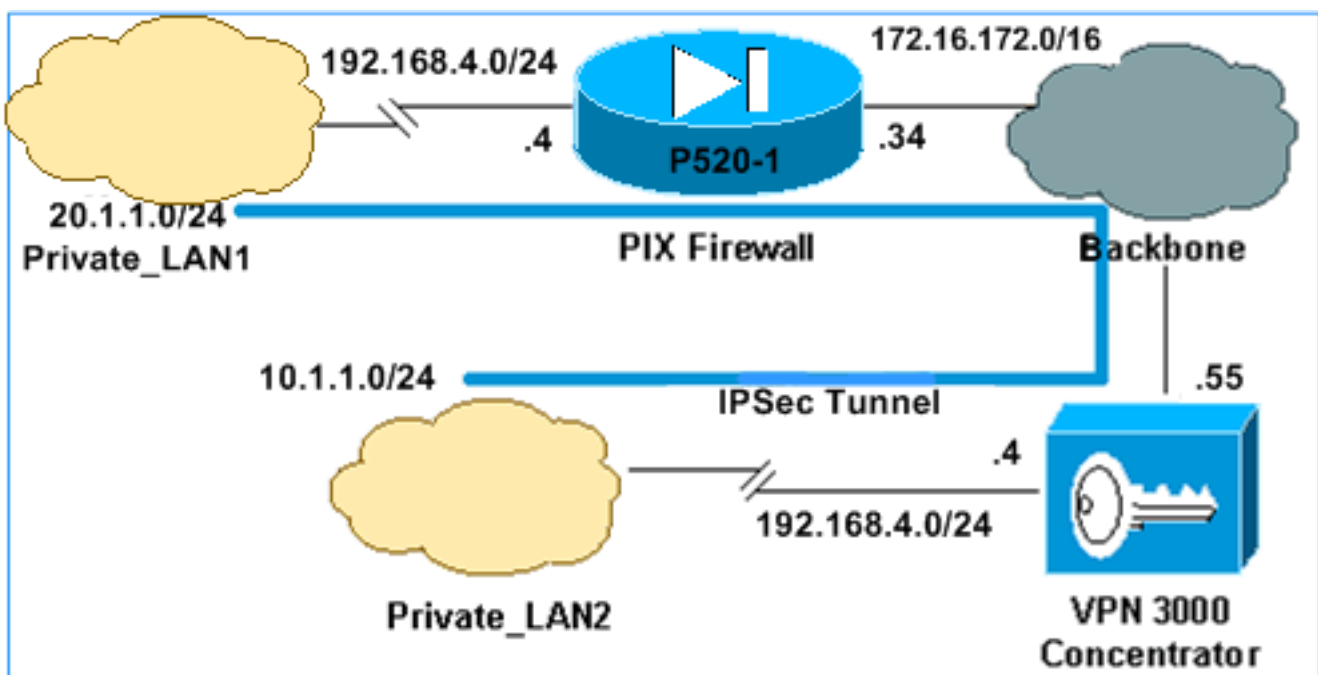
Configurar

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.



El Private_LAN1 y Private_LAN2 tienen una subred IP de 192.168.4.0/24. Esto simula el espacio de dirección superpuesta detrás de cada lado del túnel IPsec. El concentrador VPN 3000 se utiliza aquí como un ejemplo de un concentrador que no tenga las funciones del tráfico del NAT over VPN.

En este ejemplo, el PIX 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 10.1.1.0/24 a través del túnel IPsec, y Private_LAN2 “ve” el Private_LAN1 como 20.1.1.0/24 a través del túnel IPsec.

Configuraciones

PIX

```
P520-1(config)#show run: Saved:PIX Version
6.3(3)interface ethernet0 autointerface ethernet1
autonameif ethernet0 outside security0nameif ethernet1
inside security100enable password 8Ry2YjIyt7RRXU24
encryptedpasswd 2KFQnbNIdI.2KYOU encryptedhostname P520-
```

```

1domain-name bru-ch.comfixup protocol dns maximum-length
512fixup protocol ftp 21fixup protocol h323 h225
1720fixup protocol h323 ras 1718-1719fixup protocol http
80fixup protocol rsh 514fixup protocol rtsp 554fixup
protocol sip 5060fixup protocol sip udp 5060fixup
protocol skinny 2000fixup protocol smtp 25fixup protocol
sqlnet 1521fixup protocol tftp 69names !--- Defines
IPSec interesting traffic. !--- Note that the host
behind PIX communicates !--- to Private_LAN1 using
10.1.1.0/24. !--- When the packets arrive at the PIX,
they are first !--- translated to 192.168.4.0/24 and
then encrypted by IPSec.access-list 101 permit ip
20.1.1.0 255.255.255.0 192.168.4.0 255.255.255.0 pager
lines 24mtu outside 1500mtu inside 1500ip address
outside 172.16.172.34 255.255.255.0ip address inside
192.168.4.4 255.255.255.0ip audit info action alarmip
audit attack action alarmpdm history enablearp timeout
14400!--- Static translation defined to translate
Private_LAN2 !--- from 192.168.4.0/24 to
10.1.1.0/24.static (outside,inside) 10.1.1.0 192.168.4.0
netmask 255.255.255.0 0 0!--- Static translation defined
to translate Private_LAN1 !--- from 192.168.4.0/24 to
20.1.1.0/24. !--- 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 PIX), is !---
required if Private_LAN1 also needs internal
access.static (inside,outside) 20.1.1.0 192.168.4.0
netmask 255.255.255.0 0 0route outside 0.0.0.0 0.0.0.0
172.16.172.55 1timeout xlate 3:00:00timeout conn 1:00:00
half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h225
1:00:00timeout h323 0:05:00 mgcp 0:05:00 sip 0:30:00
sip_media 0:02:00timeout uauth 0:05:00 absoluteaaa-
server TACACS+ protocol tacacs+ aaa-server RADIUS
protocol radius aaa-server LOCAL protocol local no snmp-
server locationno snmp-server contactsnmp-server
community publicno snmp-server enable trapsfloodguard
enablesysopt connection permit-ipsec!--- Defines IPSec
encryption and authentication algorithms.crypto ipsec
transform-set myset esp-des esp-md5-hmac!--- Defines
crypto map.crypto map vpn 10 ipsec-isakmpcrypto map vpn
10 match address 101crypto map vpn 10 set peer
172.16.172.55crypto map vpn 10 set transform-set myset!-
-- Apply crypto map on the outside interface.crypto map
vpn interface outsideisakmp enable outside!--- Defines
pre-shared secret (cisco123) used for IKE
authentication.isakmp key ***** address 172.16.172.55
netmask 255.255.255.255 isakmp identity address!---
Defines ISAKMP policy.isakmp policy 1 authentication
pre-shareisakmp policy 1 encryption desisakmp policy 1
hash md5isakmp policy 1 group 1isakmp policy 1 lifetime
86400telnet timeout 5ssh timeout 5console timeout
0terminal width
80Cryptochecksum:6cc25fc2fea20958dfe74c1fca45ada2: end

```

[Concentrador VPN 3000 configuración del túnel de LAN a LAN](#)

Para la dirección destino 20.1.1.0 /24 (Private_LAN1) usted necesita tener una Static ruta en el VPN 3000. Para hacer, seleccionar **Configuration > System > el Routing IP > las Static rutas y elegir agregan**. Una vez que usted es relleno hecho hacia fuera los campos, haga click en Add

Utilice las configuraciones en estas imágenes para configurar su concentrador VPN 3000.

Configuration | Tunneling and Security | IPsec | LAN-to-LAN | Add

Add a new IPsec LAN-to-LAN connection.

Enable

Check to enable this LAN-to-LAN connection.

Name ToPIX

Enter the name for this LAN-to-LAN connection.

Interface Ethernet 2 (Public) (172.16.172.55)

Select the interface for this LAN-to-LAN connection.

Connection Type Bi-directional

Choose the type of LAN-to-LAN connection. An *Originate-Only* connection may have multiple peers specified below.

Peers
172.16.172.34

Enter the remote peer IP addresses for this LAN-to-LAN connection. *Originate-Only* connection may specify up to ten peer IP addresses. Enter one IP address per line.

Digital Certificate None (Use Preshared Keys)

Select the digital certificate to use.

Certificate Transmission Entire certificate chain
 Identity certificate only

Choose how to send the digital certificate to the IKE peer.

Preshared Key cisco123

Enter the preshared key for this LAN-to-LAN connection.

Authentication ESP/MD5/HMAC-128

Specify the packet authentication mechanism to use.

Encryption DES-56

Specify the encryption mechanism to use.

IKE Proposal IKE-DES-MD5

Select the IKE Proposal to use for this LAN-to-LAN connection.

Filter -None-

Choose the filter to apply to the traffic that is tunneled through this LAN-to-LAN connection.

IPsec NAT-T

Check to let NAT-T compatible IPsec peers establish this LAN-to-LAN connection through a NAT device. You must also enable IPsec over NAT-T under NAT Transparency.

Bandwidth Policy -None-

Choose the bandwidth policy to apply to this LAN-to-LAN connection.

Routing None

Choose the routing mechanism to use. **Parameters below are ignored if Network Autodiscovery is chosen.**

Local Network: If a LAN-to-LAN NAT rule is used, this is the Trusted Network address.
Network List (Use IP Address/Wildcardmask below): Specify the local network address list or the IP address and wildcard mask for the LAN-to-LAN connection.
IP Address: 192.168.0
Wildcard Mask: 0.0.255
Note: Enter a wildcard mask, which is the reverse of a subnet mask. A wildcard mask has 0 in bit positions to ignore, 0 in bit positions to match. For example, 10.10.1.0/0.0.255 = all 10.10.1.x addresses.

Remote Network: If a LAN-to-LAN NAT rule is used, this is the Remote Network address.
Network List (Use IP Address/Wildcardmask below): Specify the remote network address list or the IP address and wildcard mask for the LAN-to-LAN connection.
IP Address: 192.168.0
Wildcard Mask: 0.0.255
Note: Enter a wildcard mask, which is the reverse of a subnet mask. A wildcard mask has 0 in bit positions to ignore, 0 in bit positions to match. For example, 10.10.1.0/0.0.255 = all 10.10.1.x addresses.

Add Cancel

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.

- **muestre isakmp crypto sa** - Visualice todas las asociaciones de seguridad actuales del Internet Key Exchange (IKE) (SA) en un par.
- **muestre el detalle crypto isakmp sa** - Visualice los detalles de todo el IKE actual SA en un par.
- **muestre IPsec crypto sa** - Visualiza las configuraciones usadas por los SA actuales.
- **muestre el detalle del xlate** - Visualiza la información del slot de traducción.

PIX

```
P520-1(config)# P520-1(config)#show crypto isakmp saTotal      : 1Embryonic : 0      dst
src      state      pending      created      172.16.172.55      172.16.172.34      QM_IDLE      0
1P520-1(config)#show crypto isakmp sa detailTotal      : 1Embryonic : 0      Local
Remote      Encr Hash      Auth State      Lifetime      172.16.172.34:500      172.16.172.55:500
des md5      psk QM_IDLE      86211P520-1(config)# P520-1(config)#show crypto ipsec
sainterface: outside      Crypto map tag: vpn, local addr. 172.16.172.34      local ident
(addr/mask/prot/port): (20.1.1.0/255.255.255.0/0/0)      remote ident (addr/mask/prot/port):
(192.168.4.0/255.255.255.0/0/0)      current_peer: 172.16.172.55:500      PERMIT,
flags={origin_is_acl,}      #pkts encaps: 4, #pkts encrypt: 4, #pkts digest 4      #pkts decaps: 4,
#pkts decrypt: 4, #pkts verify 4      #pkts compressed: 0, #pkts decompressed: 0      #pkts not
compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0      #send errors 1, #recv
errors 0      local crypto endpt.: 172.16.172.34, remote crypto endpt.: 172.16.172.55      path
mtu 1500, ipsec overhead 56, media mtu 1500      current outbound spi: 734575cb      inbound esp
sas:      spi: 0xe028850d(3760751885)      transform: esp-des esp-md5-hmac ,      in use
settings = {Tunnel, }      slot: 0, conn id: 1, crypto map: vpn      sa timing: remaining key
lifetime (k/sec): (4607999/28751)      IV size: 8 bytes      replay detection support: Y
inbound ah sas:      inbound pcp sas:      outbound esp sas:      spi: 0x734575cb(1933931979)
transform: esp-des esp-md5-hmac ,      in use settings = {Tunnel, }      slot: 0, conn id: 2,
crypto map: vpn      sa timing: remaining key lifetime (k/sec): (4607999/28751)      IV
size: 8 bytes      replay detection support: Y      outbound ah sas:P520-1(config)#show xlate
detail2 in use, 2 most usedFlags: D - DNS, d - dump, I - identity, i - inside, n - no random,
o - outside, r - portmap, s - staticNAT from inside:192.168.4.1 to outside:20.1.1.1 flags sNAT
from outside:192.168.4.1 to inside:10.1.1.1 flags s
```

Utilice el tráfico de ping para verificar el túnel. Este resultado de la traza ICMP del debug recogido en el PIX ilustra cómo los paquetes son traducidos por el NAT.

```
P520-1(config)# debug icmp traceICMP trace onWarning: this may cause problems on busy
networksP520-1(config)# 1: ICMP echo-request from inside:192.168.4.1 to 10.1.1.1 ID=3060
seq=4391 length=802: ICMP echo-request: translating inside:192.168.4.1 to outside:20.1.1.13:
ICMP echo-request: untranslating inside:10.1.1.1 to outside:192.168.4.14: ICMP echo-reply from
outside:192.168.4.1 to 20.1.1.1 ID=3060 seq=4391 length=805: ICMP echo-reply: translating
outside:192.168.4.1 to inside:10.1.1.16: ICMP echo-reply: untranslating outside:20.1.1.1 to
inside:192.168.4.17: ICMP echo-request from inside:192.168.4.1 to 10.1.1.1 ID=3061 seq=4391
length=808: ICMP echo-request: translating inside:192.168.4.1 to outside:20.1.1.19: ICMP echo-
request: untranslating inside:10.1.1.1 to outside:192.168.4.110: ICMP echo-reply from
outside:192.168.4.1 to 20.1.1.1 ID=3061 seq=4391 length=8011: ICMP echo-reply: translating
outside:192.168.4.1 to inside:10.1.1.112: ICMP echo-reply: untranslating outside:20.1.1.1 to
inside:192.168.4.113: ICMP echo-request from inside:192.168.4.1 to 10.1.1.1 ID=3062 seq=4391
length=8014: ICMP echo-request: translating inside:192.168.4.1 to outside:20.1.1.115: ICMP echo-
request: untranslating inside:10.1.1.1 to outside:192.168.4.116: ICMP echo-reply from
```

```

outside:192.168.4.1 to 20.1.1.1 ID=3062 seq=4391 length=8017: ICMP echo-reply: translating
outside:192.168.4.1 to inside:10.1.1.118: ICMP echo-reply: untranslating
outside:20.1.1.1 to
inside:192.168.4.119: ICMP echo-request from inside:192.168.4.1 to 10.1.1.1 ID=3063 seq=4391
length=8020: ICMP echo-request: translating
inside:192.168.4.1 to outside:20.1.1.121: ICMP echo-
request: untranslating
inside:10.1.1.1 to outside:192.168.4.122: ICMP echo-reply from
outside:192.168.4.1 to 20.1.1.1 ID=3063 seq=4391 length=8023: ICMP echo-reply: translating
outside:192.168.4.1 to inside:10.1.1.124: ICMP echo-reply: untranslating
outside:20.1.1.1 to
inside:192.168.4.125: ICMP echo-request from inside:192.168.4.1 to 10.1.1.1 ID=3064 seq=4391
length=8026: ICMP echo-request: translating
inside:192.168.4.1 to outside:20.1.1.127: ICMP echo-
request: untranslating
inside:10.1.1.1 to outside:192.168.4.128: ICMP echo-reply from
outside:192.168.4.1 to 20.1.1.1 ID=3064 seq=4391 length=8029: ICMP echo-reply: translating
outside:192.168.4.1 to inside:10.1.1.130: ICMP echo-reply: untranslating
outside:20.1.1.1 to
inside:192.168.4.1P520-1(config)#

```

[Concentrador VPN](#)

Seleccione el **Monitoring (Monitoreo) > Sessions (Sesiones) > Detail (Detalle)** para verificar su configuración concentradora VPN 3000.

Monitoring | Sessions | Detail
Wednesday, 07 July 2004 18:17:33

[Reset](#) [Refresh](#)

[Back to Sessions](#)

Connection Name	IP Address	Protocol	Encryption	Login Time	Duration	Bytes Tx	Bytes Rx
ToPDK	172.16.172.34	IPSec/LAN-to-LAN	DES-56	Jul 07 18:09:20	0:08:13	416	416

IKE Sessions: 1
IPSec Sessions: 1

IKE Session			
Session ID	1	Encryption Algorithm	DES-56
Hashing Algorithm	MD5	Diffie-Hellman Group	Group 1 (768-bit)
Authentication Mode	Pre-Shared Keys	IKE Negotiation Mode	Main
Rekey Time Interval	86400 seconds		
IPSec Session			
Session ID	2	Remote Address	20.1.1.0/0.0.0.255
Local Address	192.168.4.0/0.0.0.255	Encryption Algorithm	DES-56
Hashing Algorithm	MD5	SEP	1
Encapsulation Mode	Tunnel	Rekey Time Interval	28800 seconds
Rekey Data Interval	4608000 KBytes		
Bytes Received	416	Bytes Transmitted	416

[Troubleshooting](#)

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración. La información adicional en el troubleshooting se puede encontrar en los documentos siguientes:

- [Resolución de problemas de conexión en el concentrador VPN 3000](#)
- [Resolución de problemas de seguridad de IP – Información y uso de los comandos de depuración](#)

- [Resolución de problemas de PIX para pasar el tráfico de datos en un túnel IPsec establecido](#)

Comandos para resolución de problemas

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

Nota:

Esta salida demuestra un debug de trabajo de la negociación IKE. Se muestran aquí las salidas de los **comandos debug crypto isakmp y debug crypto ipsec**.

```
P520-1(config)#show debugdebug crypto ipsec ldebug crypto isakmp 1P520-1(config)# ISAKMP (0):
beginning Main Mode exchangecrypto_isakmp_process_block:src:172.16.172.55, dest:172.16.172.34
spt:500 dpt:500OAK_MM exchangeISAKMP (0): processing SA payload. message ID = 0ISAKMP (0):
Checking ISAKMP transform 1 against priority 1 policyISAKMP: encryption DES-CBCISAKMP:
hash MD5ISAKMP: default group 1ISAKMP: auth pre-shareISAKMP: life type in
secondsISAKMP: life duration (VPI) of 0x0 0x1 0x51 0x80 ISAKMP (0): atts are acceptable.
Next payload is 0ISAKMP (0): processing vendor id payloadISAKMP (0): SA is doing pre-shared key
authentication using id type ID_IPV4_ADDRreturn status is
IKMP_NO_ERRORcrypto_isakmp_process_block:src:172.16.172.55, dest:172.16.172.34 spt:500
dpt:500OAK_MM exchangeISAKMP (0): processing KE payload. message ID = 0ISAKMP (0): processing
NONCE payload. message ID = 0ISAKMP (0): processing vendor id payloadISAKMP (0): processing
vendor id payloadISAKMP (0): received xauth v6 vendor idISAKMP (0): processing vendor id
payloadISAKMP (0): speaking to another IOS box!ISAKMP (0): processing vendor id payloadISAKMP
(0): speaking to a VPN3000 concentratorISAKMP (0): ID payload next-payload : 8
type : 1 protocol : 17 port : 500 length :
8ISAKMP (0): Total payload length: 12return status is
IKMP_NO_ERRORcrypto_isakmp_process_block:src:172.16.172.55, dest:172.16.172.34 spt:500
dpt:500OAK_MM exchangeISAKMP (0): processing ID payload. message ID = 0ISAKMP (0): processing
HASH payload. message ID = 0ISAKMP (0): processing vendor id payloadISAKMP (0): remote peer
supports dead peer detectionISAKMP (0): SA has been authenticatedISAKMP (0): beginning Quick
Mode exchange, M-ID of -995061605:c4b0909bIPSEC(key_engine): got a queue
event...IPSEC(spi_response): getting spi 0xe028850d(3760751885) for SA from
172.16.172.55 to 172.16.172.34 for prot 3return status is IKMP_NO_ERRORISAKMP (0): sending
INITIAL_CONTACT notifyISAKMP (0): sending NOTIFY message 24578 protocol 1VPN Peer: ISAKMP: Added
new peer: ip:172.16.172.55/500 Total VPN Peers:1VPN Peer: ISAKMP: Peer ip:172.16.172.55/500 Ref
cnt incremented to:1 Total VPN Peers:1crypto_isakmp_process_block:src:172.16.172.55,
dest:172.16.172.34 spt:500 dpt:500OAK_QM exchangeoakley_process_quick_mode:OAK_QM_IDLEISAKMP
(0): processing SA payload. message ID = 3299905691ISAKMP : Checking IPsec proposal 1ISAKMP:
transform 1, ESP_DESISAKMP: attributes in transform:ISAKMP: SA life type in
secondsISAKMP: SA life duration (basic) of 28800ISAKMP: SA life type in
kilobytesISAKMP: SA life duration (VPI) of 0x0 0x46 0x50 0x0 ISAKMP: encaps is
1ISAKMP: authenticator is HMAC-MD5ISAKMP (0): atts are
acceptable.IPSEC(validate_proposal_request): proposal part #1, (key eng. msg.) dest=
172.16.172.55, src= 172.16.172.34, dest_proxy= 192.168.4.0/255.255.255.0/0/0 (type=4),
src_proxy= 20.1.1.0/255.255.255.0/0/0 (type=4), protocol= ESP, transform= esp-des esp-md5-
hmac , lifedur= 0s and 0kb, spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4ISAKMP (0):
processing NONCE payload. message ID = 3299905691ISAKMP (0): processing ID payload. message ID =
3299905691ISAKMP (0): processing ID payload. message ID = 3299905691ISAKMP (0): Creating IPsec
SAs inbound SA from 172.16.172.55 to 172.16.172.34 (proxy 192.168.4.0 to
20.1.1.0) has spi 3760751885 and conn_id 1 and flags 4 lifetime of 28800 seconds
lifetime of 4608000 kilobytes outbound SA from 172.16.172.34 to 172.16.172.55
(proxy 20.1.1.0 to 192.168.4.0) has spi 1933931979 and conn_id 2 and flags 4
lifetime of 28800 seconds lifetime of 4608000 kilobytesIPSEC(key_engine): got a queue
event...IPSEC(initialize_sas): , (key eng. msg.) dest= 172.16.172.34, src= 172.16.172.55,
dest_proxy= 20.1.1.0/255.255.255.0/0/0 (type=4), src_proxy= 192.168.4.0/255.255.255.0/0/0
(type=4), protocol= ESP, transform= esp-des esp-md5-hmac , lifedur= 28800s and 4608000kb,
spi= 0xe028850d(3760751885), conn_id= 1, keysize= 0, flags= 0x4IPSEC(initialize_sas): , (key
eng. msg.) src= 172.16.172.34, dest= 172.16.172.55, src_proxy= 20.1.1.0/255.255.255.0/0/0
(type=4), dest_proxy= 192.168.4.0/255.255.255.0/0/0 (type=4), protocol= ESP, transform=
```

```
esp-des esp-md5-hmac ,      lifedur= 28800s and 4608000kb,      spi= 0x734575cb(1933931979),
conn_id= 2, keysize= 0, flags= 0x4VPN Peer: IPSEC: Peer ip:172.16.172.55/500 Ref cnt incremented
to:2 Total VPN Peers:1VPN Peer: IPSEC: Peer ip:172.16.172.55/500 Ref cnt incremented to:3 Total
VPN Peers:1return status is IKMP_NO_ERRORP520-1(config)# P520-1(config)#
crypto_isakmp_process_block:src:172.16.172.55, dest:172.16.172.34 spt:500 dpt:500ISAKMP (0):
processing NOTIFY payload 36136 protocol 1      spi 0, message ID = 1690390088ISAKMP (0):
received DPD_R_U_THERE from peer 172.16.172.55ISAKMP (0): sending NOTIFY message 36137 protocol
1return status is IKMP_NO_ERR_NO_TRANSP520-1(config)#
```

[Información Relacionada](#)

- [Páginas de soporte del producto de la Seguridad y VPN](#)
- [Páginas de soporte de la tecnología de la Seguridad y VPN](#)
- [Página de soporte de IPSec](#)
- [Soporte Técnico - Cisco Systems](#)