

# Exemple de configuration IPSec entre pare-feu PIX Firewall et concentrateur Cisco VPN 3000 avec chevauchement de réseaux privés

## Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Conventions](#)

[Configuration](#)

[Diagramme du réseau](#)

[Configurations](#)

[Vérification](#)

[PIX](#)

[Concentrateur VPN](#)

[Dépannage](#)

[Dépannage des commandes](#)

[Informations connexes](#)

## [Introduction](#)

Ce document décrit comment configurer le pare-feu Cisco Secure PIX Firewall dans un VPN IPSec site à site avec des adresses réseau privées qui se chevauchent derrière des passerelles VPN. La fonction NAT (Network Address Translation) améliorée introduite dans PIX 6.2 est utilisée dans cet exemple pour traduire les réseaux qui se chevauchent de chaque côté du tunnel VPN IPSec en espaces d'adresses qui ne se chevauchent pas.

## [Conditions préalables](#)

### [Conditions requises](#)

Aucune spécification déterminée n'est requise pour ce document.

### [Components Used](#)

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Cisco Secure PIX Firewall 506 avec version logicielle 6.3(3)

- Concentrateur VPN 3030 avec version logicielle 4.1(5)

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.

## Conventions

Pour plus d'informations sur les conventions des documents, référez-vous aux [Conventions utilisées pour les conseils techniques de Cisco](#).

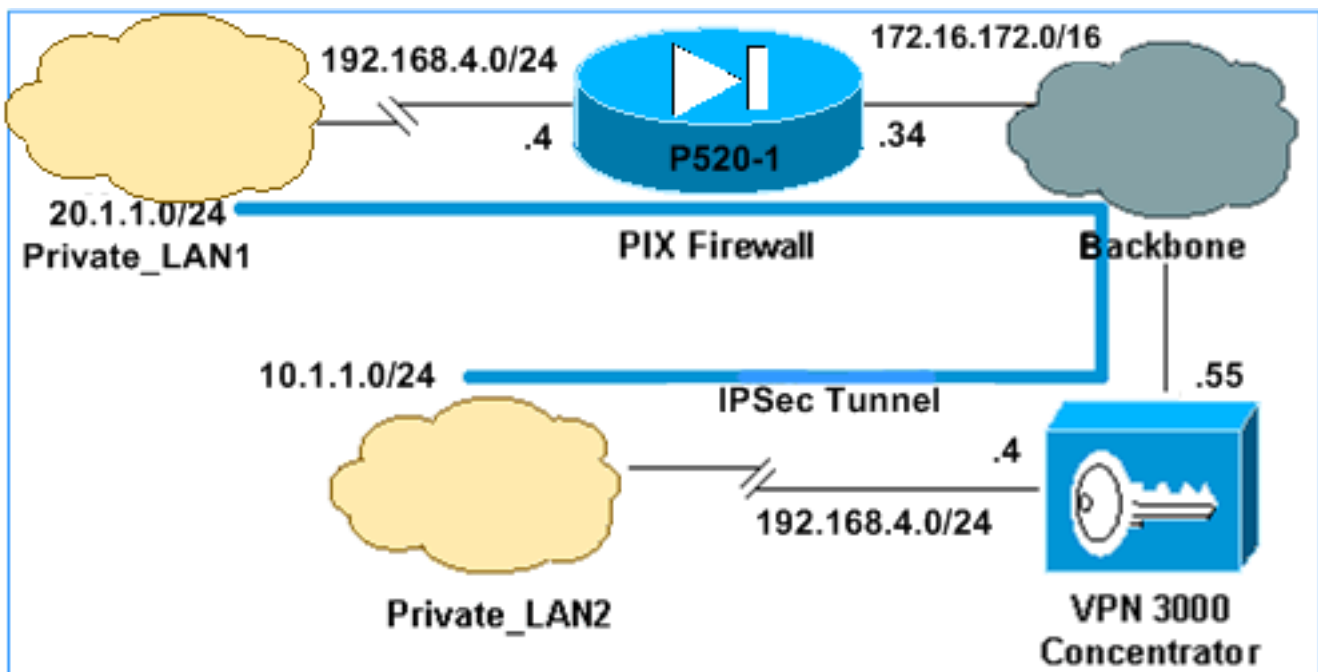
## Configuration

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

**Remarque :** Pour en savoir plus sur les commandes utilisées dans le présent document, utilisez [l'outil de recherche de commandes](#) (clients [inscrits](#) seulement).

## Diagramme du réseau

Ce document utilise la configuration réseau indiquée dans le diagramme suivant.



Private\_LAN1 et Private\_LAN2 ont tous deux un sous-réseau IP de 192.168.4.0/24. Cela simule l'espace d'adressage qui se chevauche derrière chaque côté du tunnel IPsec. Le concentrateur VPN 3000 est utilisé ici comme exemple d'un concentrateur qui n'a pas la fonctionnalité NAT sur le trafic VPN.

Dans cet exemple, le PIX effectue une traduction bidirectionnelle afin que les deux réseaux locaux privés puissent communiquer via le tunnel IPsec. La traduction signifie que Private\_LAN1 « voit » Private\_LAN2 comme 10.1.1.0/24 via le tunnel IPsec, et Private\_LAN2 « voit » Private\_LAN1 comme 20.1.1.0/24 via le tunnel IPsec.

## Configurations

### PIX

```
P520-1(config)#show run
: Saved
:
PIX Version 6.3(3)
interface ethernet0 auto
interface ethernet1 auto
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname P520-1
domain-name bru-ch.com
fixup protocol dns maximum-length 512
fixup protocol ftp 21
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol http 80
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol sip 5060
fixup protocol sip udp 5060
fixup protocol skinny 2000
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol tftp 69
names
!--- 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 24
mtu outside 1500
mtu inside 1500
ip address outside 172.16.172.34 255.255.255.0
ip address inside 192.168.4.4 255.255.255.0
ip audit info action alarm
ip audit attack action alarm
pdm history enable
arp 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 0
route outside 0.0.0.0 0.0.0.0 172.16.172.55 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc
0:10:00 h225 1:00:00
```

```

timeout h323 0:05:00 mgcp 0:05:00 sip 0:30:00 sip_media
0:02:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
aaa-server LOCAL protocol local
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
sysopt 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-isakmp
crypto map vpn 10 match address 101
crypto map vpn 10 set peer 172.16.172.55
crypto map vpn 10 set transform-set myset
!--- Apply crypto map on the outside interface. crypto
map vpn interface outside
isakmp 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-share
isakmp policy 1 encryption des
isakmp policy 1 hash md5
isakmp policy 1 group 1
isakmp policy 1 lifetime 86400
telnet timeout 5
ssh timeout 5
console timeout 0
terminal width 80
Cryptochecksum:6cc25fc2fea20958dfe74c1fca45ada2
: end

```

## [Configuration du tunnel LAN à LAN du concentrateur VPN 3000](#)

Pour l'adresse de destination 20.1.1.0 /24 (Private\_LAN1), vous devez disposer d'une route statique sur le VPN 3000. Pour ce faire, sélectionnez **Configuration > System > IP Routing > Static Routes** et choisissez **Add**. Une fois les champs remplis, cliquez sur **Ajouter**.

Configuration | System | IP Routing | Static Routes | Add

Configure and add a static route.

|                        |   |   |
|------------------------|---|---|
| <b>Network Address</b> | 20.1.1.0  | Enter the network address.                              |
| <b>Subnet Mask</b>     | 255.255.255.0   | Enter the subnet mask.                                  |
| <b>Metric</b>          | 1   | Enter the numeric metric for this route (1 through 16). |
| <b>Destination</b>     |   |   |
| <b>Router Address</b>  | 172.16.172.34   | Enter the router/gateway IP address.                    |
| <b>Interface</b>       | <input type="radio"/> Ethernet 2 (Public) (172.16.172.55) | Select the interface to route to.                       |

Utilisez les paramètres de ces images pour configurer votre concentrateur VPN 3000.

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

Add a new IPsec LAN-to-LAN connection.

|   |   |
|---|---|
| <b>Enable</b> <input checked="" type="checkbox"/>                                 | Check to enable this LAN-to-LAN connection.   |
| <b>Name</b> <input type="text" value="ToPIX"/>                                    | Enter the name for this LAN-to-LAN connection.  |
| <b>Interface</b> <input type="text" value="Ethernet 2 (Public) (172.16.172.55)"/> | Select the interface for this LAN-to-LAN connection.  |
| <b>Connection Type</b> <input type="text" value="Bi-directional"/>                | Choose the type of LAN-to-LAN connection. An <i>Originate-Only</i> connection may have multiple peers specified below.  |
| <b>Peers</b><br><input type="text" value="172.16.172.34"/>                        | Enter the remote peer IP addresses for this LAN-to-LAN connection. <i>Originate-Only</i> connection may specify up to ten peer IP addresses. Enter one IP address per line. |
| <b>Digital Certificate</b> <input type="text" value="None (Use Preshared Keys)"/> | Select the digital certificate to use.  |

|  |  |
|--|--|
| <b>Certificate Transmission</b> <input type="radio"/> Entire certificate chain<br><input checked="" type="radio"/> Identity certificate only | Choose how to send the digital certificate to the IKE peer.  |
| <b>Preshared Key</b> <input type="text" value="cisco123"/>   | Enter the preshared key for this LAN-to-LAN connection.  |
| <b>Authentication</b> <input type="text" value="ESP/MD5/HMAC-128"/>  | Specify the packet authentication mechanism to use.  |
| <b>Encryption</b> <input type="text" value="DES-56"/>  | Specify the encryption mechanism to use.   |
| <b>IKE Proposal</b> <input type="text" value="IKE-DES-MD5"/>   | Select the IKE Proposal to use for this LAN-to-LAN connection.   |
| <b>Filter</b> <input type="text" value="-None-"/>  | Choose the filter to apply to the traffic that is tunneled through this LAN-to-LAN connection.   |
| <b>IPsec NAT-T</b> <input type="checkbox"/>  | 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. |
| <b>Bandwidth Policy</b> <input type="text" value="-None-"/>  | Choose the bandwidth policy to apply to this LAN-to-LAN connection.  |
| <b>Routing</b> <input type="text" value="None"/>   | Choose the routing mechanism to use. <b>Parameters below are ignored if Network Autodiscovery is chosen.</b>   |

**Local Network:** If a LAN-to-LAN NAT rule is used, this is the Translated Network address.

Network List

Specify the local network address list or the IP address and wildcard mask for this LAN-to-LAN connection.

IP Address

**Note: Enter a *wildcard* mask, which is the reverse of a subnet mask. A wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match. For example, 10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses.**

Wildcard Mask

**Remote Network:** If a LAN-to-LAN NAT rule is used, this is the Remote Network address.

Network List

Specify the remote network address list or the IP address and wildcard mask for this LAN-to-LAN connection.

IP Address

**Note: Enter a *wildcard* mask, which is the reverse of a subnet mask. A wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match. For example, 10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses.**

Wildcard Mask

Add

Cancel

## Vérification

Cette section présente des informations que vous pouvez utiliser pour vous assurer que votre configuration fonctionne correctement.

Certaines commandes **show** sont prises en charge par l'[Output Interpreter Tool](#) (clients enregistrés uniquement), qui vous permet de voir une analyse de la sortie de la commande show.

- **show crypto isakmp sa** - Affiche toutes les associations de sécurité IKE (Internet Key Exchange) actuelles sur un homologue.
- **show crypto isakmp sa detail** - Affiche les détails de toutes les SA IKE actuelles sur un homologue.
- **show crypto ipsec sa** - Affiche les paramètres utilisés par les SA actuelles.
- **show xlate detail** - Affiche les informations relatives aux emplacements de traduction.

## PIX

```
P520-1(config)#
P520-1(config)#show crypto isakmp sa
Total      : 1
Embryonic  : 0
      dst          src          state    pending    created
      172.16.172.55 172.16.172.34  QM_IDLE      0          1
```

```
P520-1(config)#show crypto isakmp sa detail
Total      : 1
Embryonic  : 0
      Local          Remote          Encr Hash    Auth    State    Lifetime
```

```
172.16.172.34:500 172.16.172.55:500 des md5 psk QM_IDLE 86211
P520-1(config)#
```

```
P520-1(config)#show crypto ipsec sa
```

```
interface: 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 detail
```

```
2 in use, 2 most used
```

```
Flags: D - DNS, d - dump, I - identity, i - inside, n - no random,
```

```
o - outside, r - portmap, s - static
```

```
NAT from inside:192.168.4.1 to outside:20.1.1.1 flags s
```

```
NAT from outside:192.168.4.1 to inside:10.1.1.1 flags s
```

Utilisez le trafic ping pour vérifier le tunnel. Cette sortie de suivi icmp de débogage collectée sur le PIX illustre comment les paquets sont traduits par NAT.

P520-1(config)# **debug icmp trace**

ICMP trace on

Warning: this may cause problems on busy networks



P520-1(config)#

```
1: ICMP echo-request from inside:192.168.4.1 to 10.1.1.1 ID=3060 seq=4391 length=80
2: ICMP echo-request: translating inside:192.168.4.1 to outside:20.1.1.1
3: ICMP echo-request: untranslating inside:10.1.1.1 to outside:192.168.4.1
4: ICMP echo-reply from outside:192.168.4.1 to 20.1.1.1 ID=3060 seq=4391 length=80
5: ICMP echo-reply: translating outside:192.168.4.1 to inside:10.1.1.1
6: ICMP echo-reply: untranslating outside:20.1.1.1 to inside:192.168.4.1
7: ICMP echo-request from inside:192.168.4.1 to 10.1.1.1 ID=3061 seq=4391 length=80
8: ICMP echo-request: translating inside:192.168.4.1 to outside:20.1.1.1
9: ICMP echo-request: untranslating inside:10.1.1.1 to outside:192.168.4.1
10: ICMP echo-reply from outside:192.168.4.1 to 20.1.1.1 ID=3061 seq=4391 length=80
11: ICMP echo-reply: translating outside:192.168.4.1 to inside:10.1.1.1
12: ICMP echo-reply: untranslating outside:20.1.1.1 to inside:192.168.4.1
13: ICMP echo-request from inside:192.168.4.1 to 10.1.1.1 ID=3062 seq=4391 length=80
14: ICMP echo-request: translating inside:192.168.4.1 to outside:20.1.1.1
15: ICMP echo-request: untranslating inside:10.1.1.1 to outside:192.168.4.1
16: ICMP echo-reply from outside:192.168.4.1 to 20.1.1.1 ID=3062 seq=4391 length=80
17: ICMP echo-reply: translating outside:192.168.4.1 to inside:10.1.1.1
18: ICMP echo-reply: untranslating outside:20.1.1.1 to inside:192.168.4.1
19: ICMP echo-request from inside:192.168.4.1 to 10.1.1.1 ID=3063 seq=4391 length=80
20: ICMP echo-request: translating inside:192.168.4.1 to outside:20.1.1.1
21: ICMP echo-request: untranslating inside:10.1.1.1 to outside:192.168.4.1
22: ICMP echo-reply from outside:192.168.4.1 to 20.1.1.1 ID=3063 seq=4391 length=80
23: ICMP echo-reply: translating outside:192.168.4.1 to inside:10.1.1.1
24: ICMP echo-reply: untranslating outside:20.1.1.1 to inside:192.168.4.1
25: ICMP echo-request from inside:192.168.4.1 to 10.1.1.1 ID=3064 seq=4391 length=80
26: ICMP echo-request: translating inside:192.168.4.1 to outside:20.1.1.1
27: ICMP echo-request: untranslating inside:10.1.1.1 to outside:192.168.4.1
28: ICMP echo-reply from outside:192.168.4.1 to 20.1.1.1 ID=3064 seq=4391 length=80
29: ICMP echo-reply: translating outside:192.168.4.1 to inside:10.1.1.1
30: ICMP echo-reply: untranslating outside:20.1.1.1 to inside:192.168.4.1
```

P520-1(config)#

## [Concentrateur VPN](#)

Sélectionnez **Monitoring > Sessions > Detail** pour vérifier la configuration de votre concentrateur VPN 3000.

| Monitoring   Sessions   Detail   |               | Wednesday, 07 July 2004 18:17:33  |            |                 |          |          |          |
|----------------------------------|---------------|---|------------|-----------------|----------|----------|----------|
|                                  |               | Reset  Refresh  |            |                 |          |          |          |
| <a href="#">Back to Sessions</a> |               |   |            |                 |          |          |          |
| Connection Name                  | IP Address    | Protocol  | Encryption | Login Time      | Duration | Bytes Tx | Bytes Rx |
| ToPIX                            | 172.16.172.34 | IPSec/LAN-to-LAN  | DES-56     | Jul 07 18:09:20 | 0:08:13  | 416      | 416      |



| 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                |

## Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration. Vous trouverez des informations supplémentaires sur le dépannage dans les documents suivants :

- [Résolution des problèmes de connexion sur le concentrateur VPN 3000](#)
- [Dépannage de sécurité IP - Comprendre et utiliser les commandes de dépannage](#)
- [Dépannage de PIX de sorte qu'il permette le passage du trafic de données sur un tunnel IPSec établi](#)

## Dépannage des commandes

Certaines commandes **show** sont prises en charge par l'[Output Interpreter Tool](#) (clients enregistrés uniquement), qui vous permet de voir une analyse de la sortie de la commande show.

**Note :** Avant d'émettre des commandes **debug**, consultez [Informations importantes sur les commandes de débogage](#).

Cette sortie illustre un débogage fonctionnel de la négociation IKE. Voici les sorties des commandes **debug crypto isakmp** et **debug crypto ipsec**.

```
P520-1(config)#show debug
debug crypto ipsec 1
debug crypto isakmp 1
P520-1(config)#
ISAKMP (0): beginning Main Mode exchange

crypto_isakmp_process_block:src:172.16.172.55, dest:172.16.172.34 spt:500 dpt:500
OAK_MM exchange
ISAKMP (0): processing SA payload. message ID = 0

ISAKMP (0): Checking ISAKMP transform 1 against priority 1 policy
ISAKMP:      encryption DES-CBC
ISAKMP:      hash MD5
```

```
ISAKMP:      default group 1
ISAKMP:      auth pre-share
ISAKMP:      life type in seconds
ISAKMP:      life duration (VPI) of  0x0 0x1 0x51 0x80
ISAKMP (0): atts are acceptable. Next payload is 0
ISAKMP (0): processing vendor id payload

ISAKMP (0): SA is doing pre-shared key authentication using id type ID_IPV4_ADDR
return status is IKMP_NO_ERROR
crypto_isakmp_process_block:src:172.16.172.55, dest:172.16.172.34 spt:500 dpt:500
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): processing vendor id payload
ISAKMP (0): received xauth v6 vendor id
ISAKMP (0): processing vendor id payload
ISAKMP (0): speaking to another IOS box!
ISAKMP (0): processing vendor id payload
ISAKMP (0): speaking to a VPN3000 concentrator
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_ERROR
crypto_isakmp_process_block:src:172.16.172.55, dest:172.16.172.34 spt:500 dpt:500
OAK_MM exchange
ISAKMP (0): processing ID payload. message ID = 0
ISAKMP (0): processing HASH payload. message ID = 0
ISAKMP (0): processing vendor id payload
ISAKMP (0): remote peer supports dead peer detection
ISAKMP (0): SA has been authenticated

ISAKMP (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 3

return status is IKMP_NO_ERROR
ISAKMP (0): sending INITIAL_CONTACT notify
ISAKMP (0): sending NOTIFY message 24578 protocol 1
VPN Peer: ISAKMP: Added new peer: ip:172.16.172.55/500 Total VPN Peers:1
VPN Peer: ISAKMP: Peer ip:172.16.172.55/500 Ref cnt incremented to:1 Total
VPN Peers:1
crypto_isakmp_process_block:src:172.16.172.55, dest:172.16.172.34 spt:500 dpt:500
OAK_QM exchange
oakley_process_quick_mode:
OAK_QM_IDLE
ISAKMP (0): processing SA payload. message ID = 3299905691
ISAKMP : Checking IPsec proposal 1
ISAKMP: transform 1, ESP_DES
ISAKMP:  attributes in transform:
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:      encaps is 1
ISAKMP:      authenticator is HMAC-MD5
ISAKMP (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= 0x4
```

```
ISAKMP (0): processing NONCE payload. message ID = 3299905691
```

```
ISAKMP (0): processing ID payload. message ID = 3299905691
```

```
ISAKMP (0): processing ID payload. message ID = 3299905691
```

**ISAKMP (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= 0x4
```

```
IPSEC(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= 0x4
```

```
VPN Peer: IPSEC: Peer ip:172.16.172.55/500 Ref cnt incremented to:2 Total VPN Peers:1
```

```
VPN Peer: IPSEC: Peer ip:172.16.172.55/500 Ref cnt incremented to:3 Total VPN Peers:1
```

```
return status is IKMP_NO_ERROR
```

```
P520-1(config)#
```

```
P520-1(config)#
```

```
crypto_isakmp_process_block:src:172.16.172.55, dest:172.16.172.34 spt:500 dpt:500
```

```
ISAKMP (0): processing NOTIFY payload 36136 protocol 1
```

```
spi 0, message ID = 1690390088
```

```
ISAKMP (0): received DPD_R_U_THERE from peer 172.16.172.55
```

```
ISAKMP (0): sending NOTIFY message 36137 protocol 1
```

```
return status is IKMP_NO_ERR_NO_TRANS
```

```
P520-1(config)#
```

## [Informations connexes](#)

- [Pages d'assistance sur les produits de sécurité et VPN](#)
- [Pages d'assistance pour la sécurité et la technologie VPN](#)
- [Page d'assistance IPsec](#)
- [Support technique - Cisco Systems](#)