

# Configuration de Cisco PIX en Cisco Secure VPN Client, avec clé générique pré-partagée et configuration de mode

## Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Conventions](#)

[Configurez](#)

[Diagramme du réseau](#)

[Configurations](#)

[Vérifiez](#)

[Dépannez](#)

[Dépannage des commandes](#)

[Informations connexes](#)

## Introduction

Cette configuration explique comment connecter un client vpn à un Pare-feu PIX à l'utilisation des masques, du mode-config, et de la commande d'**autorisation-ipsec de connexion de sysopt**. La commande d'**autorisation-ipsec de connexion de sysopt** permet implicitement n'importe quel paquet qui provient un tunnel d'IPSec. Cette commande saute également les contrôles d'une **liste d'accès**, d'un **conduit**, ou d'un appel de procédure associé d'**access-group** pour des connexions d'IPSec.

## Conditions préalables

### Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

### Composants utilisés

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

- Version du logiciel PIX Cisco Secure 6.3(3) avec le Cisco Secure VPN Client 1.0 (affiché en tant que 2.0.7 dans l'**aide > au sujet du menu**)

ou

- Version du logiciel PIX Cisco Secure 6.3(3) avec le Cisco Secure VPN Client 1.1 (affiché en tant que 2.1.12 dans l'**aide > au sujet du** menu)

Les informations présentées dans ce document ont été créées à partir de périphériques dans un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est vivant, assurez-vous que vous comprenez l'impact potentiel de n'importe quelle commande.

## Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous aux [Conventions relatives aux conseils techniques Cisco](#).

## Configurez

Dans cette section, vous êtes présenté avec les informations que vous pouvez employer pour configurer les caractéristiques décrites dans ce document.

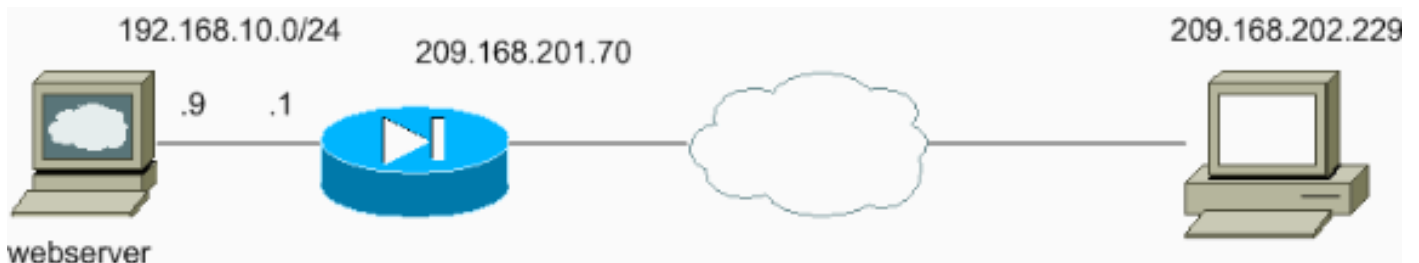
Un utilisateur avec un client vpn connecte et reçoit une adresse IP du fournisseur de services Internet (ISP). Ceci est remplacé par une adresse IP du groupe de mode-config sur le PIX (172.16.1.1 - 172.16.1.255). L'utilisateur a accès à tout sur l'intérieur du Pare-feu, qui inclut des réseaux. Les utilisateurs qui n'exécutent pas le client vpn peuvent se connecter au web server avec l'aide de l'adresse fournie par l'affectation statique. Le trafic des utilisateurs intérieurs ne passe pas par le tunnel d'IPSec quand l'utilisateur se connecte à l'Internet.

**Remarque:** La technologie de cryptage est sujette à des contrôles d'exportation. Il est de votre responsabilité de connaître la loi au sujet de l'exportation de la technologie de cryptage. Si vous avez n'importe quelles questions au sujet de contrôle d'exportation, envoyez un courrier électronique à [export@cisco.com](mailto:export@cisco.com).

**Remarque:** Afin de trouver les informations complémentaires sur les commandes utilisées dans ce document, référez-vous au [Command Lookup Tool](#) (clients [enregistrés](#) seulement).

## Diagramme du réseau

Ce document utilise cette configuration du réseau.



## Configurations

Ce document utilise les configurations suivantes.

- [Configuration PIX](#)
- [Configuration du client VPN](#)

## Configuration PIX

```
sv2-5(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 sv2-5
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
!--- Access-list defined for nat 0. access-list 101
permit ip 192.168.10.0 255.255.255.0 172.16.1.0
255.255.255.0
!--- Access-list applied on the outside interface.
access-list 102 permit tcp any host 209.168.201.9 eq www
access-list 102 permit icmp any any
pager lines 24
logging on
logging buffered debugging
mtu outside 1500
mtu inside 1500
ip address outside 209.168.201.70 255.255.255.0
ip address inside 192.168.10.1 255.255.255.0
ip audit info action alarm
ip audit attack action alarm
!--- Set up the mode-config pool. ip local pool test
172.16.1.1-172.16.1.255
no failover
failover timeout 0:00:00
failover poll 15
no failover ip address outside
no failover ip address inside
pdm history enable
arp timeout 14400
global (outside) 1 interface
!--- Do not do Network Address Translation (NAT) for the
VPN Client pool. nat (inside) 0 access-list 101
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
!--- Also allow *unencrypted* communication if desired.
static (inside,outside) 209.168.201.9 192.168.10.9
netmask 255.255.255.255 0 0
access-group 102 in interface outside
route outside 0.0.0.0 0.0.0.0 209.168.201.1 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 mqcp 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
!--- These are IPSec parameters. crypto ipsec transform-
set myset esp-des esp-md5-hmac
crypto dynamic-map dynmap 10 set transform-set myset
crypto map mymap 10 ipsec-isakmp dynamic dynmap
crypto map mymap client configuration address initiate
crypto map mymap client configuration address respond
crypto map mymap interface outside
!--- These are IKE parameters. isakmp enable outside
isakmp key ***** address 0.0.0.0 netmask 0.0.0.0
isakmp identity address
isakmp client configuration address-pool local test
outside
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption des
isakmp policy 10 hash md5
isakmp policy 10 group 1
isakmp policy 10 lifetime 86400
telnet timeout 5
ssh timeout 5
console timeout 0
vpdn username cisco password ***** store-local
terminal width 80
Cryptochecksum:4f21dc73759ffae29935430132e662ef
: end
```

## Configuration du client VPN

```
sv2-5(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 sv2-5
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
!--- Access-list defined for nat 0. access-list 101
permit ip 192.168.10.0 255.255.255.0 172.16.1.0
```

```
255.255.255.0
!--- Access-list applied on the outside interface.
access-list 102 permit tcp any host 209.168.201.9 eq www
access-list 102 permit icmp any any
pager lines 24
logging on
logging buffered debugging
mtu outside 1500
mtu inside 1500
ip address outside 209.168.201.70 255.255.255.0
ip address inside 192.168.10.1 255.255.255.0
ip audit info action alarm
ip audit attack action alarm
!--- Set up the mode-config pool. ip local pool test
172.16.1.1-172.16.1.255
no failover
failover timeout 0:00:00
failover poll 15
no failover ip address outside
no failover ip address inside
pdm history enable
arp timeout 14400
global (outside) 1 interface
!--- Do not do Network Address Translation (NAT) for the
VPN Client pool. nat (inside) 0 access-list 101
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
!--- Also allow *unencrypted* communication if desired.
static (inside,outside) 209.168.201.9 192.168.10.9
netmask 255.255.255.255 0 0
access-group 102 in interface outside
route outside 0.0.0.0 0.0.0.0 209.168.201.1 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 mcp 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
!--- These are IPsec parameters. crypto ipsec transform-
set myset esp-des esp-md5-hmac
crypto dynamic-map dynmap 10 set transform-set myset
crypto map mymap 10 ipsec-isakmp dynamic dynmap
crypto map mymap client configuration address initiate
crypto map mymap client configuration address respond
crypto map mymap interface outside
!--- These are IKE parameters. isakmp enable outside
isakmp key ***** address 0.0.0.0 netmask 0.0.0.0
isakmp identity address
isakmp client configuration address-pool local test
outside
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption des
isakmp policy 10 hash md5
isakmp policy 10 group 1
isakmp policy 10 lifetime 86400
telnet timeout 5
```

```
ssh timeout 5
console timeout 0
vpdn username cisco password ***** store-local
terminal width 80
Cryptochecksum:4f21dc73759ffae29935430132e662ef
: end
```

## Vérifiez

Aucune procédure de vérification n'est disponible pour cette configuration.

## Dépannez

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

### 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.

**Remarque:** Avant d'émettre des commandes **debug**, reportez-vous à [Informations importantes sur les commandes de débogage](#).

Afin de voir le côté client VPN met au point, active le visualiseur Cisco Secure de log.

- **debug crypto ipsec SA** — Affiche les négociations IPSecs de la phase 2.
- **debug crypto isakmp** — Affiche les négociations de Protocole ISAKMP (Internet Security Association and Key Management Protocol) de la phase 1.

Voir la cette **sortie de débogage** :

```
crypto_isakmp_process_block:src:209.168.202.229,
dest:209.168.201.70 spt:500 dpt:500
OAK_MM exchange
ISAKMP (0): processing SA payload. message ID = 0

ISAKMP (0): Checking ISAKMP transform 1 against priority 10 policy
ISAKMP: encryption DES-CBC
ISAKMP: hash MD5
ISAKMP: default group 1
ISAKMP: auth pre-share
ISAKMP (0): atts are acceptable. Next payload is 0
ISAKMP (0): SA is doing pre-shared key authentication
using id type ID_IPV4_ADDR
return status is IKMP_NO_ERROR
crypto_isakmp_process_block:src:209.168.202.229,
dest:209.168.201.70 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

return status is IKMP\_NO\_ERROR

crypto\_isakmp\_process\_block:src:209.168.202.229,  
dest:209.168.201.70 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 NOTIFY payload 24578 protocol 1  
spi 0, message ID = 0

ISAKMP (0): processing notify INITIAL\_CONTACTIPSEC(key\_engine):  
got a queue event...

IPSEC(key\_engine\_delete\_sas): rec'd delete notify from ISAKMP

IPSEC(key\_engine\_delete\_sas): delete all SAs shared with 209.168.202.229

**ISAKMP (0): SA has been authenticated**

*!--- Phase 1 is complete.* 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 ISAKMP (0):  
sending phase 1 RESPONDER\_LIFETIME notify ISAKMP (0): sending NOTIFY message 24576 protocol 1  
VPN Peer: ISAKMP: Added new peer: ip:209.168.202.229/500 Total VPN Peers:1 VPN Peer: ISAKMP:  
Peer ip:209.168.202.229/500 Ref cnt incremented to:1 Total VPN Peers:1  
crypto\_isakmp\_process\_block:src:209.168.202.229, dest:209.168.201.70 spt:500 dpt:500 OAK\_QM  
exchange **ISAKMP (0:0): Need config/address**

*!--- Mode configuration.* ISAKMP (0:0): initiating peer config to 209.168.202.229. ID =  
2521514930 (0x964b43b2) return status is IKMP\_NO\_ERROR  
crypto\_isakmp\_process\_block:src:209.168.202.229, dest:209.168.201.70 spt:500 dpt:500  
ISAKMP\_TRANSACTION exchange ISAKMP (0:0): processing transaction payload from 209.168.202.229.  
message ID = 16133588 ISAKMP: Config payload CFG\_ACK ISAKMP (0:0): peer accepted the address!  
return status is IKMP\_NO\_ERROR crypto\_isakmp\_process\_block:src:209.168.202.229,  
dest:209.168.201.70 spt:500 dpt:500 OAK\_QM exchange oakley\_process\_quick\_mode: OAK\_QM\_IDLE  
ISAKMP (0): processing SA payload. message ID = 1524017329 ISAKMP : Checking IPsec proposal 1  
ISAKMP: transform 1, ESP\_DES ISAKMP: attributes in transform: ISAKMP: authenticator is HMAC-MD5  
ISAKMP: encaps is 1 *!--- Phase 2 starts.* **ISAKMP (0): atts are**

**acceptable.IPSEC(validate\_proposal\_request):  
proposal part #1,**

(key eng. msg.) dest= 209.168.201.70, src= 209.168.202.229,  
dest\_proxy= 192.168.10.0/255.255.255.0/0/0 (type=4),  
src\_proxy= 172.16.1.1/255.255.255.255/0/0 (type=1),  
protocol= ESP, transform= esp-des esp-md5-hmac ,  
lifedur= 0s and 0kb,  
spi= 0x0(0), conn\_id= 0, keysize= 0, flags= 0x4

ISAKMP (0): processing NONCE payload. message ID = 1524017329

ISAKMP (0): processing ID payload. message ID = 1524017329

ISAKMP (0): ID\_IPV4\_ADDR src 172.16.1.1 prot 0 port 0

ISAKMP (0): processing ID payload. message ID = 1524017329

ISAKMP (0): ID\_IPV4\_ADDR\_SUBNET dst 192.168.10.0/255.255.255.0 prot 0 port  
0IPSEC(key\_engine): got a queue event...

IPSEC(spi\_response): getting spi 0x9f068383(2668004227) for SA  
from 209.168.202.229 to 209.168.201.70 for prot 3

return status is IKMP\_NO\_ERROR

crypto\_isakmp\_process\_block:src:209.168.202.229,  
dest:209.168.201.70 spt:500 dpt:500

OAK\_QM exchange

oakley\_process\_quick\_mode:

OAK\_QM\_AUTH\_AWAIT

*!--- Phase 2 complete IPsec SAs are created.* **ISAKMP (0): Creating IPsec SAs**

inbound SA from 209.168.202.229 to 209.168.201.70  
(proxy 172.16.1.1 to 192.168.10.0)

has spi 2668004227 and conn\_id 2 and flags 4

outbound SA from 209.168.201.70 to 209.168.202.229

(proxy 192.168.10.0 to 172.16.1.1)

```
has spi 3326135849 and conn_id 1 and flags 4IPSEC
(key_engine): got a queue event...
IPSEC(initialize_sas): ,
(key eng. msg.) dest= 209.168.201.70, src= 209.168.202.229,
dest_proxy= 192.168.10.0/255.255.255.0/0/0 (type=4),
src_proxy= 172.16.1.1/0.0.0.0/0/0 (type=1),
protocol= ESP, transform= esp-des esp-md5-hmac ,
lifedur= 0s and 0kb,
spi= 0x9f068383(2668004227), conn_id= 2, keysize= 0, flags= 0x4
IPSEC(initialize_sas): ,
(key eng. msg.) src= 209.168.201.70, dest= 209.168.202.229,
src_proxy= 192.168.10.0/255.255.255.0/0/0 (type=4),
dest_proxy= 172.16.1.1/0.0.0.0/0/0 (type=1),
protocol= ESP, transform= esp-des esp-md5-hmac ,
lifedur= 0s and 0kb,
spi= 0xc640ce29(3326135849), conn_id= 1, keysize= 0, flags= 0x4

VPN Peer: IPSEC: Peer ip:209.168.202.229/500 Ref cnt
incremented to:2 Total VPN Peers:1
VPN Peer: IPSEC: Peer ip:209.168.202.229/500 Ref cnt
incremented to:3 Total VPN Peers:1
return status is IKMP_NO_ERROR
sv2-5#
```

## [Informations connexes](#)

- [Page d'assistance IPsec](#)
- [Introduction à IPsec](#)
- [Établissement de la Connectivité par des Pare-feu de Cisco PIX](#)
- [Référence des commandes PIX](#)
- [Page de support PIX](#)
- [Demandes de commentaires \(RFC\)](#)
- [Support technique - Cisco Systems](#)