

Configurando o Cisco PIX para a configuração de modo, pré-compartilhada e de caractere geral do Cisco Secure VPN Client

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenções](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configurações](#)

[Verificar](#)

[Troubleshooting](#)

[Comandos de solução de problemas](#)

[Informações Relacionadas](#)

[Introdução](#)

Esta configuração demonstra como conectar um cliente VPN a um PIX Firewall com o uso dos convites, do config de modo, e do **comando sysopt connection permit-ipsec**. O **comando sysopt connection permit-ipsec** permite implicitamente todo o pacote que vier de um túnel de IPsec. Este comando igualmente contorneia as verificações de uma indicação de **comando access-list, conduit, ou access-group** associada para conexões IPsec.

[Pré-requisitos](#)

[Requisitos](#)

Não existem requisitos específicos para este documento.

[Componentes Utilizados](#)

As informações neste documento são baseadas nestas versões de software e hardware.

- Software Release 6.3(3) do PIX seguro Cisco com o Cisco Secure VPN Client 1.0 (mostrado como 2.0.7 no menu do **ajuda > sobre**)

ou

- Software Release 6.3(3) do PIX seguro Cisco com o Cisco Secure VPN Client 1.1 (mostrado como 2.1.12 no menu do **ajuda > sobre**)

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se sua rede está viva, assegure-se de que você compreenda o impacto potencial do comando any.

Convenções

Para obter mais informações sobre convenções de documento, consulte as [Convenções de dicas técnicas Cisco](#).

Configurar

Nesta seção, você é apresentado com a informação que você pode se usar para configurar as características descritas neste documento.

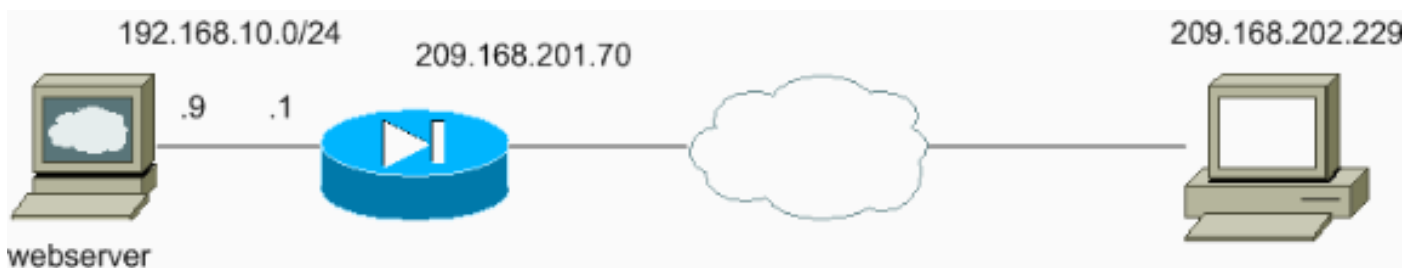
Um usuário com um cliente VPN se conecta e recebe um endereço IP do ISP. Isto é substituído por um endereço IP de Um ou Mais Servidores Cisco ICM NT do pool de configuração de modo no PIX (172.16.1.1 - 172.16.1.255). O usuário tem o acesso a tudo no interior do Firewall, que inclui redes. Os usuários que não executam o cliente VPN podem conectar ao servidor de Web com a ajuda do endereço fornecido pela atribuição estática. O tráfego de usuários internos não passa no túnel de IPsec quando o usuário conectar-se à Internet.

Nota: A tecnologia de criptografia está sujeita a controles de exportação. É sua responsabilidade conhecer a lei sobre a exportação de tecnologia de criptografia. Se você tem quaisquer perguntas sobre o controle de exportação, envie um email a export@cisco.com.

Nota: A fim encontrar a informação adicional nos comandos usados neste documento, refira a [ferramenta de consulta de comandos \(clientes registrados somente\)](#).

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede.



Configurações

Este documento utiliza estas configurações.

- [Configuração de PIX](#)
- [Configuração de cliente de VPN](#)

Configuração de 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 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
!--- 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

```

Configuração de cliente de 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 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
!--- 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
```

Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

Troubleshooting

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

Comandos de solução de problemas

A [Output Interpreter Tool \(somente clientes registrados\)](#) oferece suporte a determinados comandos show, o que permite exibir uma análise da saída do comando show.

Nota: Antes que você emita **comandos debug**, refira a [informação importante em comandos Debug](#).

A fim ver os debug do lado do cliente VPN, permita o visor do Log seguro da Cisco.

- **debug crypto ipsec sa** — Indica as negociações de IPSEC de fase 2.
- **isakmp do debug crypto** — Indica as negociações do Internet Security Association and Key Management Protocol (ISAKMP) da fase 1.

Veja este **resultado do debug**:

```
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#
```

[Informações Relacionadas](#)

- [Página de suporte do IPSec](#)
- [Introdução ao IPSec](#)
- [Estabelecendo conectividade através de firewalls do Cisco PIX](#)
- [Referências de comando PIX](#)
- [Página de suporte do PIX](#)
- [Solicitações de Comentários \(RFCs\)](#)
- [Suporte Técnico - Cisco Systems](#)