# Configuración de PIX a PIX a PIX IPSec totalmente mallado

## Contenido



## Introducción

Esta configuración permite que las redes privadas detrás de tres cuadros del Cisco Secure PIX Firewall sean conectadas por los túneles VPN sobre Internet o cualquier red pública que utilice el IPSec. Cada uno de las tres redes tiene Conectividad a las otras dos redes. En este escenario, el Network Address Translation (NAT) se requiere para las conexiones al Internet pública. Sin embargo, el NAT no se requiere para el tráfico entre los tres intranets, que se pueden transmitir usando un túnel VPN sobre el Internet pública.

## prerrequisitos

### Requisitos

Para que el IPSec trabaje, usted debe tener Conectividad del punto final del túnel al punto final del túnel antes de que usted comience esta configuración.

### Componentes Utilizados

Esta configuración fue desarrollada y probada con la versión 6.1(2) del firewall PIX.

**Nota: El comando show version** debe mostrar que el cifrado está habilitado.

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

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

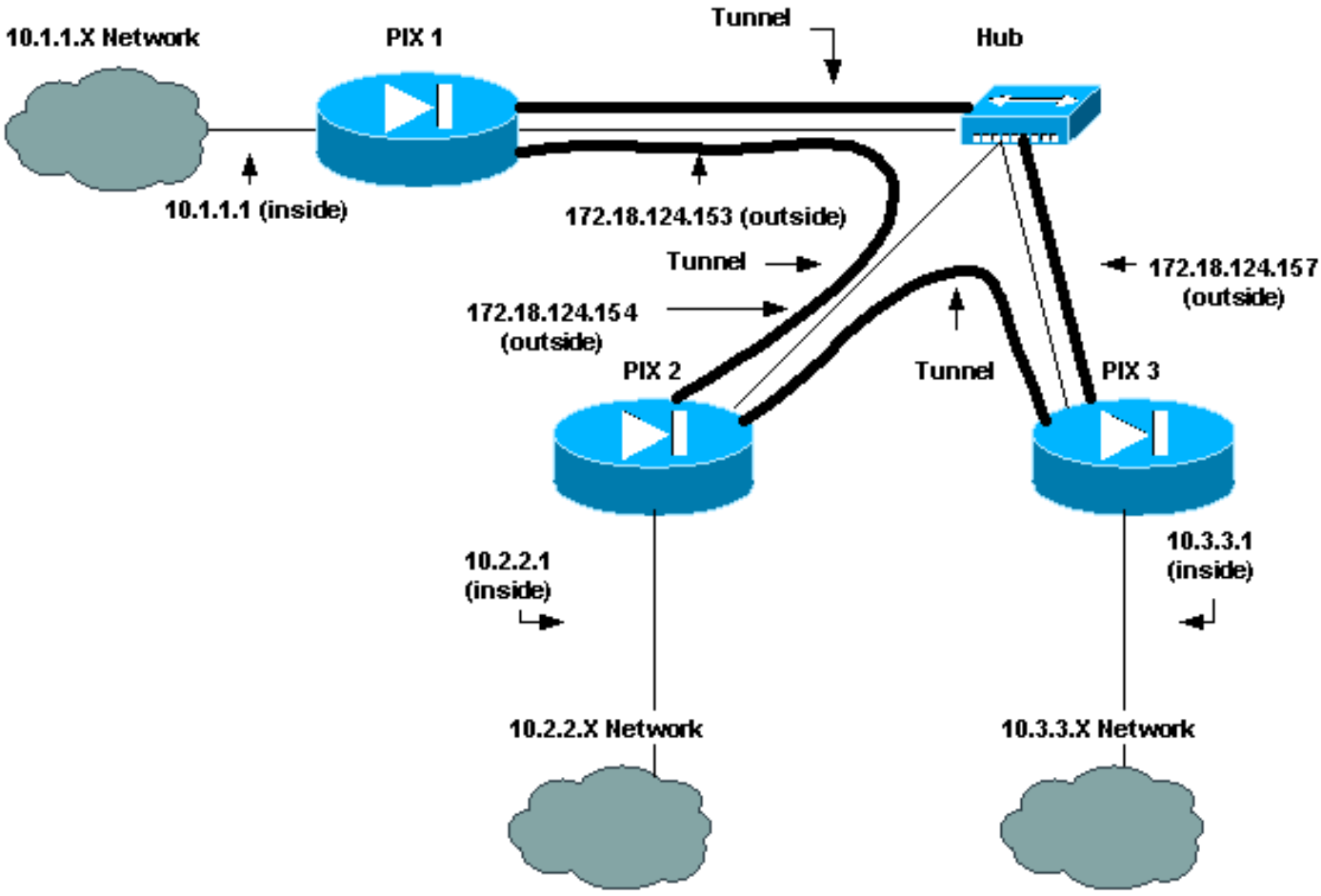
# Configurar

En esta sección encontrará la información para configurar las funciones descritas en este documento.

**Nota:** Utilice la herramienta Command Lookup Tool (clientes registrados solamente) para obtener más información sobre los comandos utilizados en esta sección.

## Diagrama de la red

En este documento, se utiliza esta configuración de red:




## Configuraciones

En este documento, se utilizan estas configuraciones:

- PIX1

- PIX2
- PIX3

## Configuración del PIX1

```
PIX Version 6.1(2)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname pix_1
fixup protocol ftp 21
fixup protocol http 80
fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
names
!--- Traffic to PIX 2 private network: access-list 120
permit ip 10.1.1.0 255.255.255.0 10.2.2.0 255.255.255.0
!--- Traffic to PIX 3 private network: access-list 130
permit ip 10.1.1.0 255.255.255.0 10.3.3.0 255.255.255.0
!--- Do not perform NAT for traffic to !--- other PIX
Firewall private networks: access-list 100 permit ip
10.1.1.0 255.255.255.0 10.2.2.0 255.255.255.0 access-
list 100 permit ip 10.1.1.0 255.255.255.0 10.3.3.0
255.255.255.0 pager lines 24 logging on no logging
timestamp no logging standby no logging console no
logging monitor no logging buffered no logging trap no
logging history logging facility 20 logging queue 512
interface ethernet0 auto interface ethernet1 auto mtu
outside 1500 mtu inside 1500 ip address outside
172.18.124.153 255.255.255.0 ip address inside 10.1.1.1
255.255.255.0 ip audit info action alarm ip audit attack
action alarm no failover failover timeout 0:00:00
failover poll 15 failover ip address outside 0.0.0.0
failover ip address inside 0.0.0.0 arp timeout 14400 !--
- Do not perform NAT for traffic to other PIX Firewalls:
nat (inside) 0 access-list 100 route outside 0.0.0.0
0.0.0.0 172.18.124.1 1 timeout xlate 3:00:00 timeout
conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00
h323 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 no snmp-server
location no snmp-server contact snmp-server community
public snmp-server enable traps floodguard enable sysopt
connection permit-ipsec no sysopt route dnat crypto
ipsec transform-set myset esp-des esp-md5-hmac !---
IPsec configuration for tunnel to PIX 2: crypto map
newmap 20 ipsec-isakmp crypto map newmap 20 match
address 120 crypto map newmap 20 set peer 172.18.124.154
crypto map newmap 20 set transform-set myset !--- IPsec
configuration for tunnel to PIX 3: crypto map newmap 30
ipsec-isakmp crypto map newmap 30 match address 130
crypto map newmap 30 set peer 172.18.124.157 crypto map
newmap 30 set transform-set myset crypto map newmap
interface outside isakmp enable outside isakmp key
******** address 172.18.124.154 netmask 255.255.255.255
no-xauth no-config-mode isakmp key ******** address
172.18.124.157 netmask 255.255.255.255 no-xauth no-
config-mode isakmp identity address 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 1000 telnet timeout 5 ssh
timeout 5 terminal width 80
Cryptochecksum:436c96500052d0276324b9ef33221b2d : end
[OK]
```

## Configuración del PIX2

```
PIX Version 6.1(2)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname pix_2
fixup protocol ftp 21
fixup protocol http 80
fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
names
!--- Traffic to PIX 1: access-list 110 permit ip
10.2.2.0 255.255.255.0 10.1.1.0 255.255.255.0 !---
Traffic to PIX 3: access-list 130 permit ip 10.2.2.0
255.255.255.0 10.3.3.0 255.255.255.0 !--- Do not perform
NAT for traffic to other PIX Firewalls: access-list 100
permit ip 10.2.2.0 255.255.255.0 10.1.1.0 255.255.255.0
access-list 100 permit ip 10.2.2.0 255.255.255.0
10.3.3.0 255.255.255.0 pager lines 24 logging on no
logging timestamp no logging standby no logging console
no logging monitor no logging buffered no logging trap
no logging history logging facility 20 logging queue 512
interface ethernet0 auto interface ethernet1 auto mtu
outside 1500 mtu inside 1500 ip address outside
172.18.124.154 255.255.255.0 ip address inside 10.2.2.1
255.255.255.0 ip audit info action alarm ip audit attack
action alarm no failover failover timeout 0:00:00
failover poll 15 failover ip address outside 0.0.0.0
failover ip address inside 0.0.0.0 arp timeout 14400 !--
- Do not perform NAT for traffic to other PIX Firewalls:
nat (inside) 0 access-list 100 route outside 0.0.0.0
0.0.0.0 172.18.124.1 1 timeout xlate 3:00:00 timeout
conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00
h323 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 no snmp-server
location no snmp-server contact snmp-server community
public no snmp-server enable traps floodguard enable
sysopt connection permit-ipsec no sysopt route dnat
crypto ipsec transform-set myset esp-des esp-md5-hmac !-
-- IPsec configuration for tunnel to PIX 1: crypto map
newmap 10 ipsec-isakmp crypto map newmap 10 match
address 110 crypto map newmap 10 set peer 172.18.124.153
crypto map newmap 10 set transform-set myset !--- IPsec
configuration for tunnel to PIX 3: crypto map newmap 30
ipsec-isakmp crypto map newmap 30 match address 130
crypto map newmap 30 set peer 172.18.124.157 crypto map
newmap 30 set transform-set myset crypto map newmap
interface outside isakmp enable outside isakmp key
******** address 172.18.124.153 netmask 255.255.255.255
no-xauth no-config-mode isakmp key ******** address
172.18.124.157 netmask 255.255.255.255 no-xauth no-
config-mode isakmp identity address 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 1000 telnet timeout 5 ssh
timeout 5 terminal width 80
Cryptochecksum:aef12453a0ea29b592dd0d395de881f5 : end
```

## Configuración del PIX3

```
PIX Version 6.1(2)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname pix_3
fixup protocol ftp 21
fixup protocol http 80
fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
names
!--- IPsec configuration for tunnel to PIX 1: access-
list 110 permit ip 10.3.3.0 255.255.255.0 10.1.1.0
255.255.255.0 !--- IPsec configuration for tunnel to PIX
2: access-list 120 permit ip 10.3.3.0 255.255.255.0
10.2.2.0 255.255.255.0 !--- Do not perform NAT for
traffic to other PIX Firewalls: access-list 100 permit
ip 10.3.3.0 255.255.255.0 10.2.2.0 255.255.255.0 access-
list 100 permit ip 10.3.3.0 255.255.255.0 10.1.1.0
255.255.255.0 pager lines 24 logging on no logging
timestamp no logging standby no logging console no
logging monitor no logging buffered no logging trap no
logging history logging facility 20 logging queue 512
interface ethernet0 auto interface ethernet1 auto mtu
outside 1500 mtu inside 1500 ip address outside
172.18.124.157 255.255.255.0 ip address inside 10.3.3.1
255.255.255.0 ip audit info action alarm ip audit attack
action alarm no failover failover timeout 0:00:00
failover poll 15 failover ip address outside 0.0.0.0
failover ip address inside 0.0.0.0 arp timeout 14400 !--
- Do not perform NAT for traffic to other PIX Firewalls:
nat (inside) 0 access-list 100 route outside 0.0.0.0
0.0.0.0 172.18.124.1 1 timeout xlate 3:00:00 timeout
conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00
h323 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 no snmp-server
location no snmp-server contact snmp-server community
public no snmp-server enable traps floodguard enable
sysopt connection permit-ipsec no sysopt route dnat
crypto ipsec transform-set myset esp-des esp-md5-hmac !-
-- IPsec configuration for tunnel to PIX 1: crypto map
newmap 10 ipsec-isakmp crypto map newmap 10 match
address 110 crypto map newmap 10 set peer 172.18.124.153
crypto map newmap 10 set transform-set myset !--- IPsec
configuration for tunnel to PIX 2: crypto map newmap 20
ipsec-isakmp crypto map newmap 20 match address 120
crypto map newmap 20 set peer 172.18.124.154 crypto map
newmap 20 set transform-set myset crypto map newmap
interface outside isakmp enable outside isakmp key
******** address 172.18.124.153 netmask 255.255.255.255
no-xauth no-config-mode isakmp key ******** address
172.18.124.154 netmask 255.255.255.255 no-xauth no-
config-mode isakmp identity address 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 1000 telnet timeout 5 ssh
timeout 5 terminal width 80
Cryptochecksum:e6ad75852dff21efdb2d24cc95ffbe1c : end
[OK]
```

# Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

# Troubleshooting

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración. Refiera a resolver problemas el PIX para pasar el tráfico de datos en un túnel de IPSec establecido para más información.

## Comandos para resolución de problemas

**Nota:** Consulte Información Importante sobre Comandos de Debug antes de usar un **comando debug**.

**comandos debug**

Utilice estos comandos en el PIX, con el **logging monitor debugging** o ejecutarse de los **comandos logging console debugging**.

- **IPSec del debug crypto** — Procesamiento IPSec de los debugs.
- **isakmp del debug crypto** — Proceso del Internet Security Association and Key Management Protocol (ISAKMP) de los debugs.
- **motor del debug crypto** — Mensajes del debug de las visualizaciones sobre los motores de criptografía, que realizan el cifrado y el desciframiento.

**comandos clear**

Para borrar las asociaciones de seguridad (SA), utilice estos comandos en el modo de configuración del PIX.

- **clear [crypto] ipsec sa** — Borra el IPSec activo SA. La palabra clave crypto es opcional.
- **clear [crypto] isakmp sa** — Borra el Internet Key Exchange (IKE) activo SA. La palabra clave crypto es opcional.

**Nota:** Para que el IPSec trabaje, usted debe tener Conectividad del punto final del túnel al punto final del túnel antes de que usted comience esta configuración.

# Información Relacionada

- Resolución de problemas de PIX para pasar el tráfico de datos en un túnel IPSec establecido
- Dispositivos de seguridad Cisco PIX de la serie 500
- Referencias de Comando PIX
- Protocolos del IPSec Negotiations/IKE

- Solicitudes de Comentarios (RFC)
- Soporte Técnico y Documentación - Cisco Systems