Configuración de PIX a PIX a PIX IPSec (concentrador y radio)

Contenido

Introducción

Esta configuración permite que un Cisco Secure PIX Firewall central se comunique con las redes detrás de otras dos cajas PIX Firewall a través de túneles VPN a través de Internet o cualquier red pública que utilice IPsec. Las dos redes periféricas no necesitan comunicarse entre sí, pero hay conectividad a la red central. Las dos redes de salida no pueden comunicarse entre sí atravesando el PIX central porque el PIX no rutea el tráfico recibido en una interfaz de regreso a la misma interfaz. Si hay necesidad de que las redes externas se comuniquen entre sí, necesita una configuración de malla completa, en lugar de la configuración de hub y spoke que se muestra en este documento. Puede que ya haya **declaraciones nat 1**, **global**, **static** y **conduit** presentes en los PIX. Este ejemplo sólo muestra la adición de cifrado.

Prerequisites

Requirements

Para que IPsec funcione, *debe* establecer la conectividad entre los puntos finales del túnel antes de iniciar esta configuración.

Componentes Utilizados

La información en este documento se basa en las versiones 5.1.x, 5.2.x y 6.3.3 de PIX Firewall.

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

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.

Convenciones

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

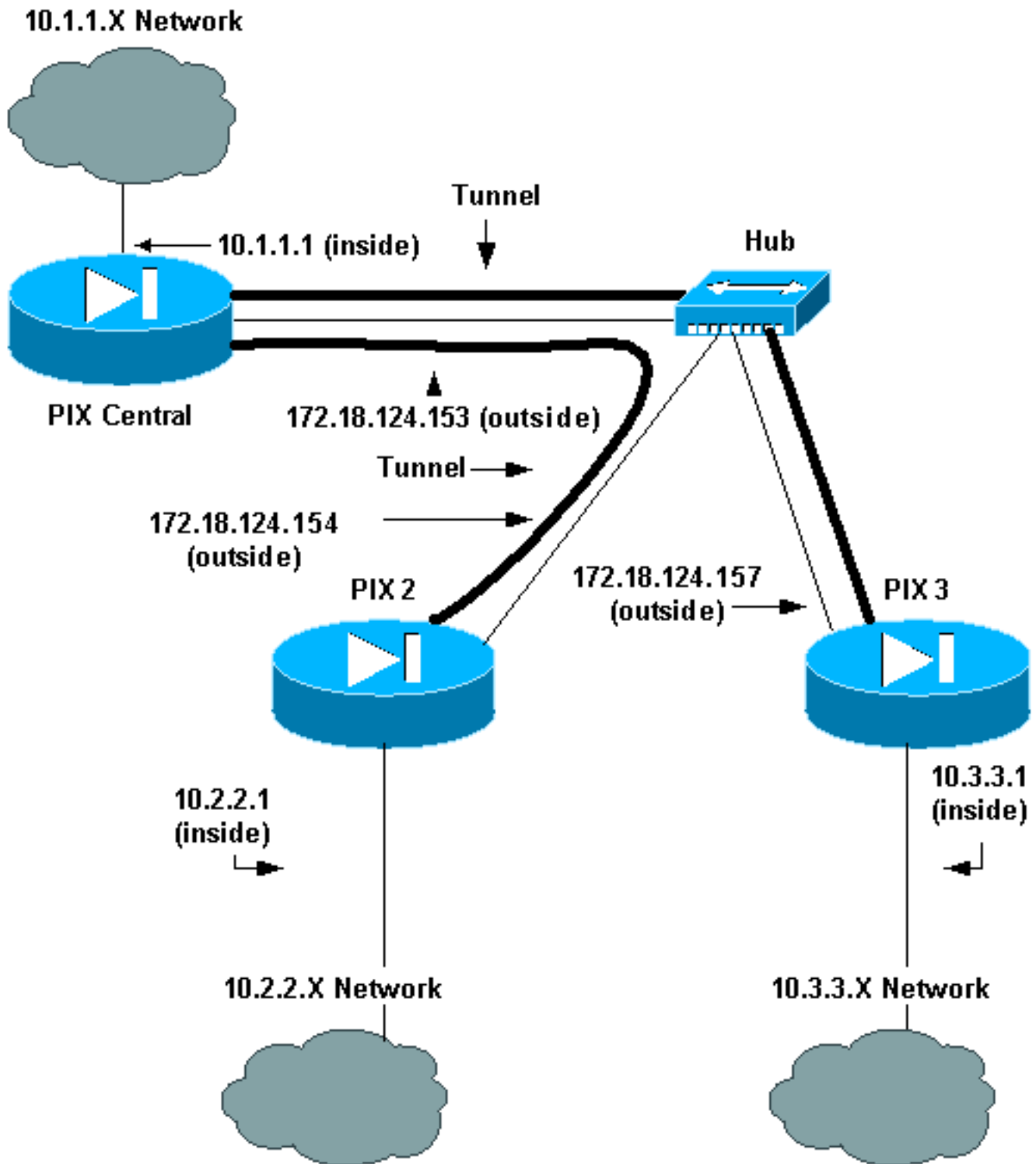# Configurar

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

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

Diagrama de la red

En este documento, se utiliza esta configuración de red:

10.1.1.X Network

Tunnel

10.1.1.1 (inside)

Hub

PIX Central

172.18.124.153 (outside)

Tunnel →

172.18.124.154
(outside)

PIX 2

172.18.124.157
(outside) →

PIX 3

10.3.3.1
(inside)

10.2.2.1
(inside)

10.2.2.X Network

10.3.3.X Network

Configuraciones

En este documento, se utilizan estas configuraciones:

- Central PIX
- PIX 2
- PIX 3

Central PIX
`Building configuration...` `: 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 pix-central
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
```
!--- This is traffic to PIX 2. **access-list 120 permit ip
10.1.1.0 255.255.255.0 10.2.2.0 255.255.255.0**
!--- This is traffic to PIX 3. **access-list 130 permit ip
10.1.1.0 255.255.255.0 10.3.3.0 255.255.255.0**
*!--- Do not do Network Address Translation (NAT) on
traffic to other PIXes.* **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
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
pdm history enable
arp timeout 14400
```
!--- Do not do NAT on traffic to other PIXes. **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 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
snmp-server enable traps
floodguard enable
```
sysopt connection permit-ipsec
crypto ipsec transform-set myset esp-des esp-md5-hmac
!--- This is traffic 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
!--- This is traffic 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
console timeout 0
terminal width 80
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e
: end
```

PIX 2

```
Building configuration...
: 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 pix2
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
!--- This is traffic to PIX Central. access-list 110
permit ip 10.2.2.0 255.255.255.0 10.1.1.0 255.255.255.0
!--- Do not do NAT on traffic to PIX Central. access-
list 100 permit ip 10.2.2.0 255.255.255.0 10.1.1.0
255.255.255.0
pager lines 24
logging on
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
no failover ip address outside
no failover ip address inside
pdm history enable
arp timeout 14400
```
!--- Do not do NAT on traffic to PIX Central. **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 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
crypto ipsec transform-set myset esp-des esp-md5-hmac
!--- This is traffic to PIX Central. **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
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 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
console timeout 0
terminal width 80
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e
: end
```

PIX 3

```
Building configuration...
: 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 pix3
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
```
!--- This is traffic to PIX Central. **access-list 110**
permit ip 10.3.3.0 255.255.255.0 10.1.1.0 255.255.255.0
!--- Do not do NAT on traffic to PIX Central. **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
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
no failover ip address outside
no failover ip address inside
pdm history enable
arp timeout 14400
```
!--- Do not do NAT on traffic to PIX Central. **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 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
crypto ipsec transform-set myset esp-des esp-md5-hmac
!--- This is traffic to PIX Central. **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
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 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
console timeout 0
terminal width 80
Cryptochecksum:aa3bbd8c6275d214b153e1e0bc0173e4
: end
```

Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

[La herramienta Output Interpreter Tool (clientes registrados solamente) (OIT) soporta ciertos comandos show.](#) Utilice la OIT para ver un análisis del resultado del comando show.

- **show crypto ipsec sa**: muestra el estado actual de las asociaciones de seguridad IPsec (SA) y es útil para determinar si el tráfico está cifrado.

```
pix-central#show crypto ipsec sa

interface: outside
    Crypto map tag: newmap, local addr. 172.18.124.153

    local  ident (addr/mask/prot/port): (10.1.1.0/255.255.255.0/0/0)
    remote ident (addr/mask/prot/port): (10.3.3.0/255.255.255.0/0/0)
    current_peer: 172.18.124.157:500
      PERMIT, flags={origin_is_acl,}
!--- This verifies that encrypted packets are sent !--- and received without any errors.
    #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 0, #recv errors 0

       local crypto endpt.: 172.18.124.153,
       remote crypto endpt.: 172.18.124.157
       path mtu 1500, ipsec overhead 56, media mtu 1500
       current outbound spi: 3bcb6913
!--- Shows inbound SAs that are established. inbound esp sas:
       spi: 0x3efbe540(1056695616)
         transform: esp-des esp-md5-hmac ,
         in use settings ={Tunnel, }
         slot: 0, conn id: 3, crypto map: newmap
         sa timing: remaining key lifetime (k/sec): (4607999/27330)
         IV size: 8 bytes
         replay detection support: Y

       inbound ah sas:
       inbound pcp sas:
!--- Shows outbound SAs that are established. outbound esp sas:
       spi: 0x3bcb6913(1003186451)
         transform: esp-des esp-md5-hmac ,
         in use settings ={Tunnel, }
```

```
          slot: 0, conn id: 4, crypto map: newmap
          sa timing: remaining key lifetime (k/sec): (4607999/27321)
          IV size: 8 bytes
          replay detection support: Y

      outbound ah sas:

      outbound pcp sas:

 local  ident (addr/mask/prot/port): (10.1.1.0/255.255.255.0/0/0)
 remote ident (addr/mask/prot/port): (10.2.2.0/255.255.255.0/0/0)
 current_peer: 172.18.124.154:500
   PERMIT, flags={origin_is_acl,}
```
!--- This verifies that encrypted packets are sent !--- and received without any errors.
#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 0, #recv errors 0

  local crypto endpt.: 172.18.124.153,
  remote crypto endpt.: 172.18.124.154
  path mtu 1500, ipsec overhead 56, media mtu 1500
  current outbound spi: da8d556
```
!--- Shows inbound SAs that are established. inbound esp sas: spi: 0x53835c96(1401117846)
```
transform: esp-des esp-md5-hmac ,
      in use settings ={Tunnel, }
      slot: 0, conn id: 1, crypto map: newmap
      sa timing: remaining key lifetime (k/sec): (4607999/27319)
      IV size: 8 bytes
      replay detection support: Y

   inbound ah sas:

   inbound pcp sas:
```
!--- Shows outbound SAs that are established. outbound esp sas: spi: 0xda8d556c(3666695532)
```
transform: esp-des esp-md5-hmac ,
      in use settings ={Tunnel, }
      slot: 0, conn id: 2, crypto map: newmap
      sa timing: remaining key lifetime (k/sec): (4607999/27319)
      IV size: 8 bytes
      replay detection support: Y

   outbound ah sas:

   outbound pcp sas:
```

- **show crypto isakmp sa**: muestra el estado actual de las SA de Intercambio de claves de Internet (IKE).

```
pix-central#show crypto isakmp sa
Total     : 2
Embryonic : 0
        dst              src         state     pending    created

   172.18.124.153   172.18.124.154   QM_IDLE          0          0
   172.18.124.153   172.18.124.157   QM_IDLE          0          0
```

Troubleshoot

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

Comandos para resolución de problemas

Nota: Consulte [Información Importante sobre Comandos Debug](#) antes de utilizar los comandos **debug**.

En el PIX (con los comandos **logging monitor debugging** o **logging console debugging** ejecutándose):

- **debug crypto ipsec**: Depura el procesamiento IPsec.
- **debug crypto isakmp**: depura el procesamiento de la Asociación de seguridad de Internet y del protocolo de administración de claves (ISAKMP).
- **debug crypto engine**: muestra los mensajes de depuración sobre los motores criptográficos, que realizan el cifrado y el descifrado.

Despeje las asociaciones de seguridad

Utilice estos comandos en el modo de configuración del PIX:

- **clear [crypto] ipsec sa**: elimina las SAs IPsec activas. La palabra clave **crypto** es opcional.
- **clear [crypto] isakmp sa**: elimina las SA IKE activas. La palabra clave **crypto** es opcional.

Información Relacionada

- [Cisco PIX Firewall Software](#)
- [Referencias de Comandos de Cisco Secure PIX Firewall](#)
- [Avisos de campos de productos de seguridad (incluido PIX)](#)
- [Solicitudes de Comentarios (RFC)](#)
- [Negociación IPSec/Protocolos IKE](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)