Configurando IPSec PIX para PIX para PIX (Hub e Spoke)

Contents

Introduction

Essa configuração permite que um Cisco Secure PIX Firewall central se comunique com redes atrás de duas outras caixas PIX Firewall através de túneis VPN pela Internet ou qualquer rede pública usando IPsec. As duas redes externas não precisam se comunicar entre si, mas há conectividade com a rede central. As duas redes externas não conseguem se comunicar entre si através do PIX central porque o PIX não roteia o tráfego recebido em uma interface de volta para a mesma interface. Se houver necessidade de comunicação entre as redes externas, você precisará de uma configuração totalmente em malha, em vez da configuração de hub e spoke mostrada neste documento. Pode já haver **instruções nat 1**, **global**, **estático** e **conduit** presentes nos PIXes. Este exemplo mostra apenas a adição de criptografia.

Prerequisites

Requirements

Para que o IPsec funcione, você *deve* estabelecer conectividade entre os pontos finais do túnel antes de iniciar esta configuração.

Componentes Utilizados

As informações neste documento são baseadas no PIX Firewall versões 5.1.x, 5.2.x e 6.3.3.

Observação: o comando **show version** deve mostrar que a criptografia está habilitada.

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

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

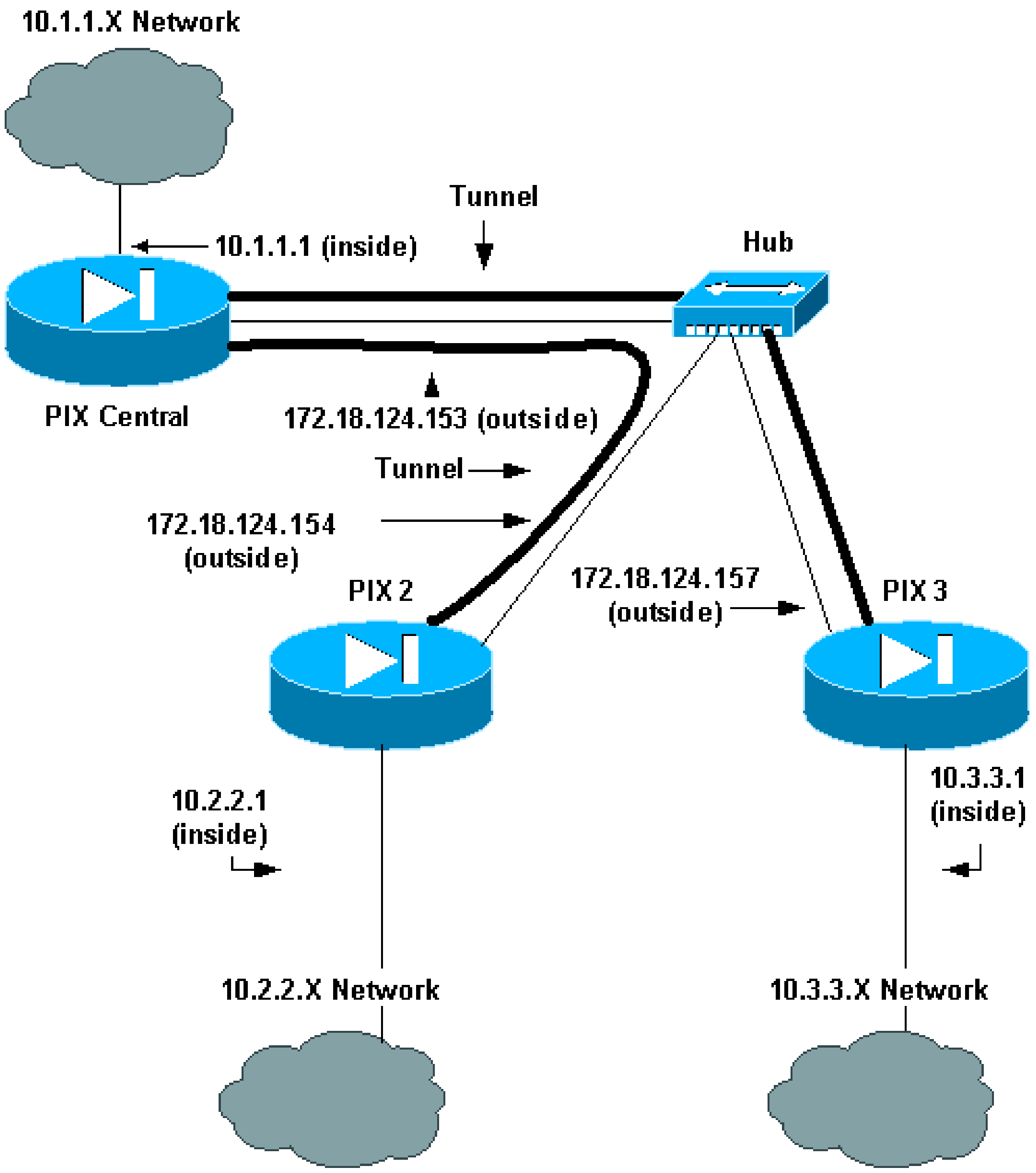
Configurar

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

Nota: Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



Configurações

Este documento utiliza as seguintes configurações:

- Central de PIX
- PIX 2
- PIX 3

Central de 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
```

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

A Output Interpreter Tool (somente clientes registrados) (OIT) oferece suporte a determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

- **show crypto ipsec sa** — Exibe o status atual das associações de segurança (SAs) IPsec e é útil para determinar se o tráfego é criptografado.

```
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** — Mostra o estado atual das SAs do Internet Key Exchange (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

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

Comandos para Troubleshooting

Nota:Consulte Informações Importantes sobre Comandos de Depuração antes de usar comandos debug.

No PIX (com os comandos **logging monitor debugging** ou **logging console debugging** em execução):

- **debug crypto ipsec** — Depura o processamento do IPsec.
- **debug crypto isakmp** — Depura o processamento do ISAKMP (Internet Security Association and Key Management Protocol).
- **debug crypto engine** — Exibe mensagens de depuração sobre mecanismos de criptografia, que executam criptografia e descriptografia.

Cancele associações de segurança

Use estes comandos no modo de configuração do PIX:

- **clear [crypto] ipsec sa** — Exclui as SAs IPsec ativas. A palavra-chave **crypto** é opcional.
- **clear [crypto] isakmp sa** — Exclui as SAs IKE ativas. A palavra-chave **crypto** é opcional.

Informações Relacionadas

- Cisco PIX Firewall Software
- Referências do comando Cisco Secure PIX Firewall
- Avisos de campo de produto de segurança (incluindo PIX)
- Solicitações de Comentários (RFCs)
- Negociação IPsec/Protocolos IKE
- Suporte Técnico e Documentação - Cisco Systems