Configurando o IPsec PIX-à-PIX-À-PIX (hub and spoke)

Índice

Introdução

Esta configuração permite que um firewall PIX segura Cisco central comunique-se com as redes atrás outras de duas caixas do PIX Firewall através dos túneis VPN sobre o Internet ou toda a rede pública usando o IPsec. As duas redes remotas não têm nenhuma necessidade de comunicar-se um com o otro, mas há uma Conectividade à rede central. As duas redes remotas não podem comunicar-se um com o otro atravessando o PIX central porque o PIX não distribui o tráfego recebido em uma relação traseira para fora a mesma relação. Se há uma necessidade para que as redes remotas se comuniquem um com o otro, você precisa uma configuração inteiramente engrenada, em vez da configuração do hub and spoke mostrada neste documento. Pôde já haver um **nat 1**, **global**, um **estático**, e umas **indicações de canalização** atuais nas PIXes. Este exemplo mostra somente a adição de criptografia.

Pré-requisitos

Requisitos

Para que o IPsec trabalhe, você *deve* estabelecer a Conectividade entre pontos finais de túnel antes que você comece esta configuração.

Componentes Utilizados

A informação neste documento é baseada em versões 5.1.x do PIX Firewall, 5.2.x, e 6.3.3.

Nota: O comando show version deve mostrar que a criptografia está permitida.

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 a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

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

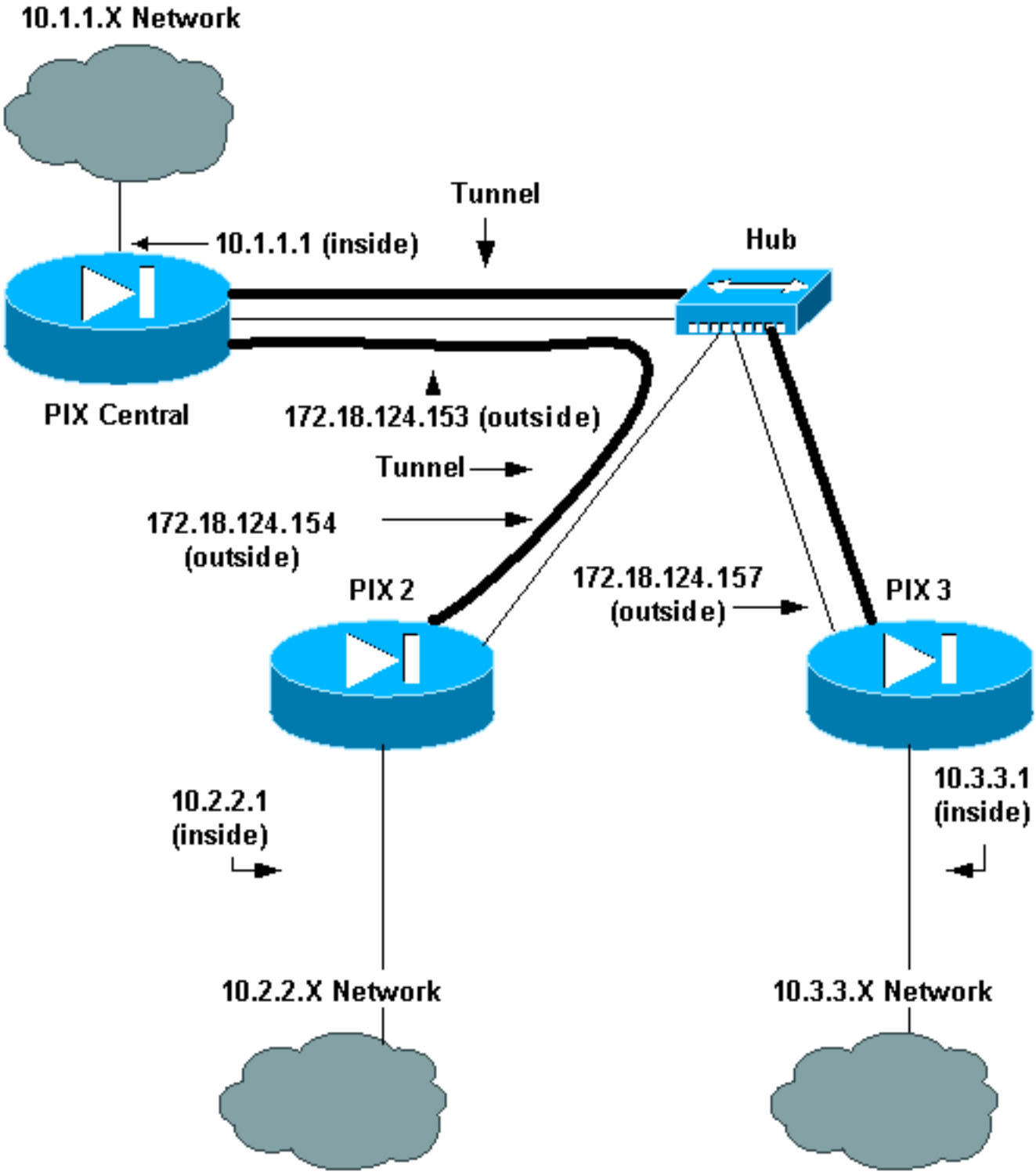
Configurar

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
- PIX2
- PIX3

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
```

PIX2

```
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
```

PIX3

```
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 (apenas para clientes registrados) (OIT) suporta determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

- **mostre IPsec cripto sa** — Indica o status atual das associações de segurança IPSec (SA) e é útil em determinar se o tráfego é 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:
```
- **mostre isakmp cripto sa** — Mostra o estado atual do Internet Key Exchange (IKE) SA.
```
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
```

Troubleshooting

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 o **logging monitor debugging** ou os **comandos logging console debugging que** são executado):

- **IPsec do debug crypto** — Debuga o processamento de IPSec.

- **isakmp do debug crypto** — Debuga o processamento do Internet Security Association and Key Management Protocol (ISAKMP).
- **motor do debug crypto** — Os indicadores debugam mensagens sobre as crypto-engines, que executam a criptografia e a descriptografia.

Cancele associações de segurança

Use estes comandos no modo de configuração do PIX:

- **clear [crypto] ipsec sa** — Suprime do IPSec ativo SA. As palavras-chave crypto são opcionais.
- **clear [crypto] isakmp sa** — Suprime do IKE ativo SA. As palavras-chave crypto são opcionais.

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