Configurando PIX para PIX para PIX IPSec totalmente integrado

Índice

Introdução
Pré-requisitos
Requisitos
Componentes Utilizados
Convenções
Configurar
Diagrama de Rede
Configurações
Verificar
Troubleshooting
Comandos para Troubleshooting
Informações Relacionadas

Introdução

Esta configuração permite que as redes privadas atrás de três caixas do firewall PIX segura Cisco sejam conectadas por túneis VPN sobre o Internet ou toda a rede pública que usar o IPsec. Cada um das três redes tem a Conectividade a outras duas redes. Nesta encenação, o Network Address Translation (NAT) é exigido para conexões aos Internet públicas. Contudo, o NAT não é exigido para o tráfego entre os três intranet, que podem ser transmitidos usando um túnel VPN sobre os Internet públicas.

Pré-requisitos

Requisitos

Para que o IPsec trabalhe, você deve ter a Conectividade do ponto final de túnel ao ponto final de túnel antes que você comece esta configuração.

Componentes Utilizados

Esta configuração foi desenvolvida e testada com versão 6.1(2) do PIX Firewall.

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.

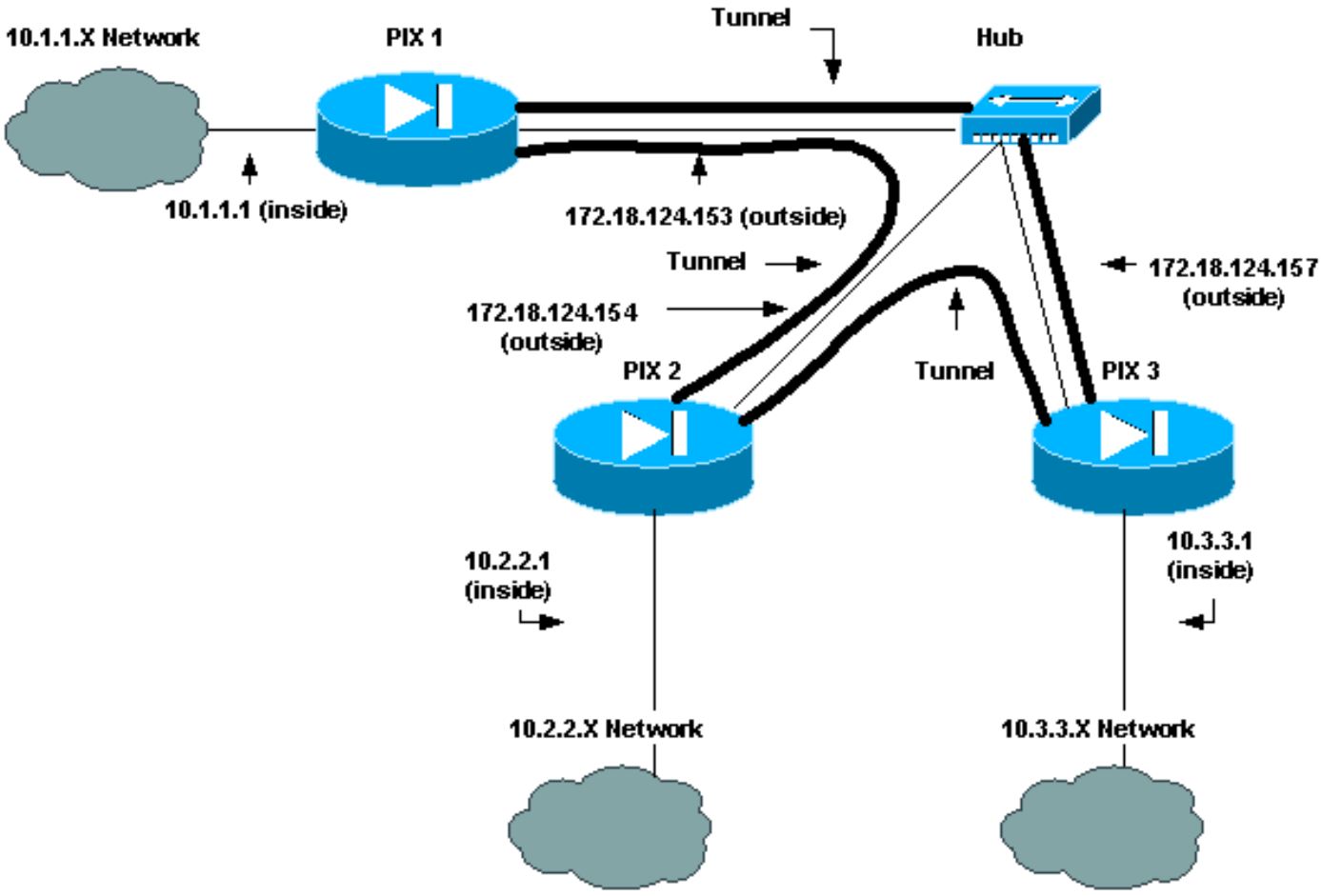
Configurar

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:

- PIX1

- PIX2
- PIX3

Configuração 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]
```

Configuração 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
```

Configuração 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]
```

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. Refira a pesquisa de defeitos do PIX para passar o tráfego de dados em um túnel IPSec estabelecido para mais informação.

Comandos para Troubleshooting

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

Comandos debug

Use estes comandos no PIX, com o **logging monitor debugging** ou ser executado dos **comandos logging console debugging**.

- **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.

comandos clear

A fim cancelar as associações de segurança (SA), 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 Internet Key Exchange (IKE) ativo SA. As palavras-chave crypto são opcionais.

Nota: Para que o IPsec trabalhe, você deve ter a Conectividade do ponto final de túnel ao ponto final de túnel antes que você comece esta configuração.

Informações Relacionadas

- Troubleshooting de PIX para Passagem de Tráfego de Dados em um Túnel de IPSec Estabelecido
- Cisco PIX 500 Series Security Appliances

- Referências de comando PIX
- Protocolos do IPsec Negotiations/IKE
- Solicitações de Comentários (RFCs)
- Suporte Técnico e Documentação - Cisco Systems