

Настройка полностью сцепленных PIX к PIX к PIX IPSec

Содержание

[Введение](#)

[Предварительные условия](#)

[Требования](#)

[Используемые компоненты](#)

[Условные обозначения](#)

[Настройка](#)

[Схема сети](#)

[Конфигурации](#)

[Проверка](#)

[Устранение неполадок](#)

[Команды для устранения неполадок](#)

[Дополнительные сведения](#)

Введение

Эта конфигурация позволяет частным сетям позади трех коробок межсетевого экрана Cisco Secure PIX быть связанными VPN-туннелями по Интернету или любой открытой сети, которая использует IPsec. Каждая из этих трех сетей имеет подключение к другим двум сетям. В этом сценарии Технология NAT требуется для соединений с общедоступным Интернетом. Однако NAT не требуется для трафика между этими тремя интранет, которые могут быть переданы с помощью VPN-туннеля по общедоступному Интернету.

Предварительные условия

Требования

Для IPsec для работы у вас должно быть подключение от конечной точки туннеля до конечной точки туннеля перед началом этой конфигурации.

Используемые компоненты

Эта конфигурация разрабатывалась и проверялась с версией 6.1 (2) Межсетевого экрана PIX.

Примечание: Команда `Show version` должна показать, что включено шифрование.

Сведения, представленные в этом документе, были получены от устройств, работающих в

специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Условные обозначения

[Более подробную информацию о применяемых в документе обозначениях см. в описании условных обозначений, используемых в технической документации Cisco.](#)

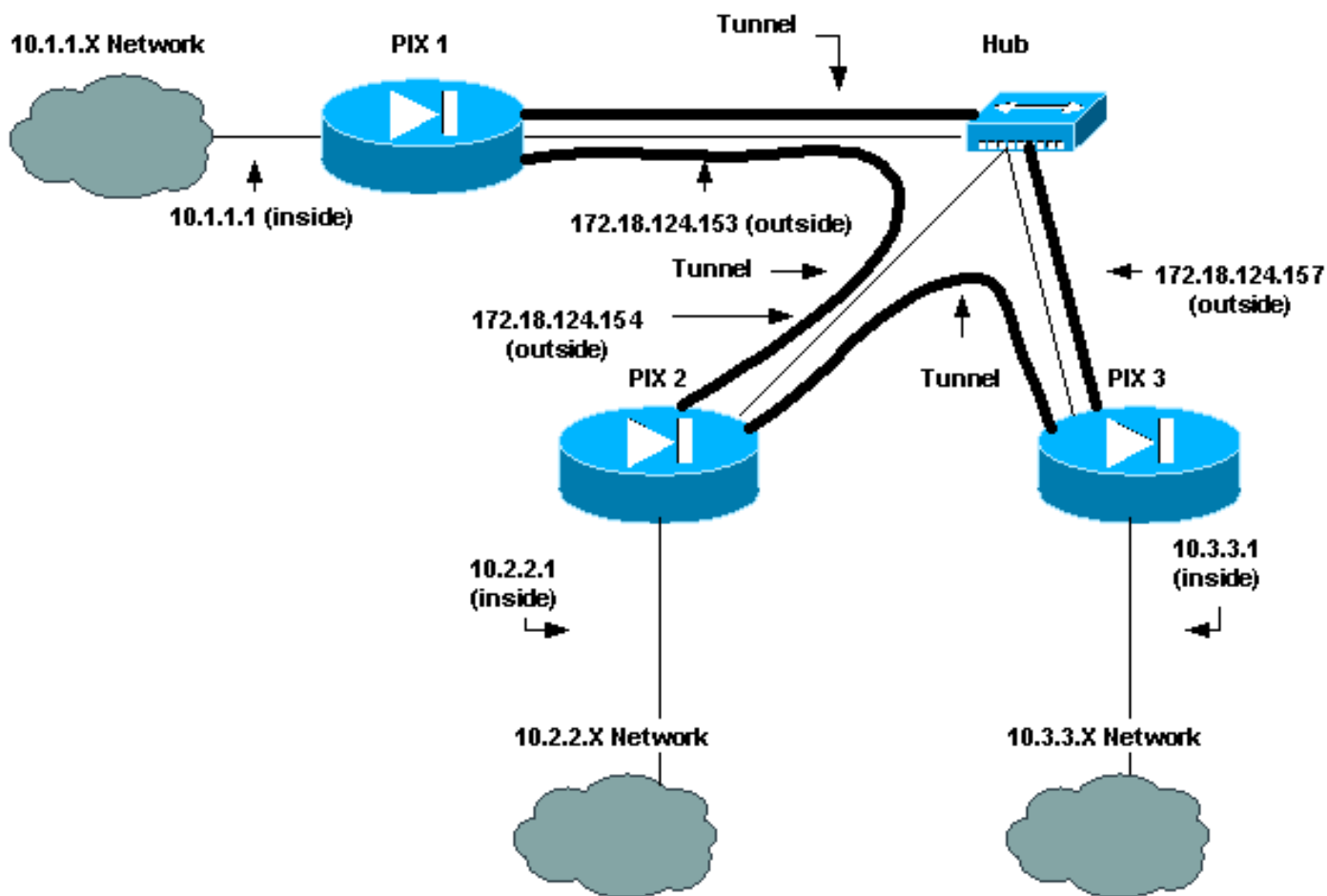
Настройка

В этом разделе содержатся сведения о настройке функций, описанных в этом документе.

Примечание: [Используйте инструмент Command Lookup \(только для зарегистрированных пользователей\) для того, чтобы получить более подробную информацию о командах, использованных в этом разделе.](#)

Схема сети

В настоящем документе используется следующая схема сети:



Конфигурации

Эти конфигурации используются в данном документе:

- [PIX 1](#)
- [PIX 2](#)
- [PIX 3](#)

Конфигурация PIX 1

```

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]
```

Конфигурация PIX 2

```
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
```

Конфигурация PIX 3

```
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]
```

Проверка

В настоящее время для этой конфигурации нет процедуры проверки.

Устранение неполадок

В этом разделе описывается процесс устранения неполадок конфигурации. См. [Устранение проблем PIX для Передачи Трафика данных Установке туннеля IPSec](#) для получения дополнительной информации.

Команды для устранения неполадок

Примечание: [Прежде чем выполнять какие-либо команды отладки , ознакомьтесь с документом "Важные сведения о командах отладки"](#).

команды "debug"

Используйте эти команды на PIX с выполнением команд `logging console debugging` или `logging monitor debugging`.

- `debug crypto ipsec` Обработка IPSEC Отладок.
- `debug crypto isakmp` Обработка Протокола ISAKMP Отладок.
- `debug crypto engine` сообщения отладки о ядрах шифрования, которые выполняют шифрование и расшифровку.

Команды clear

Чтобы к очистке сопоставлений безопасности (SA), используйте эти команды в режиме конфигурации PIX.

- `clear [crypto] ipsec sa`— удаляет все активные ассоциации безопасности IPSec. Ключевое слово `crypto` является необязательным.
- `clear [crypto] isakmp sa` — Удаляет активные SA Протокола IKE. Ключевое слово `crypto` является необязательным.

Примечание: Для IPsec для работы у вас должно быть подключение от конечной точки туннеля до конечной точки туннеля перед началом этой конфигурации.

Дополнительные сведения

- [Устранение неполадок PIX при передаче трафика по установленному туннелю IPSec](#)
- [Cisco PIX 500 Series Security Appliances](#)
- [Справочник по командам PIX](#)
- [Протоколы Согласований/IKE IPsec](#)

- [Запросы комментариев \(RFC\)](#)
- [Cisco Systems – техническая поддержка и документация](#)