Настройка PIX-to-PIX-to-PIX IPSec (Hub и Spoke)

Содержание

Введение

Эта конфигурация позволяет центральному межсетевому экрану Cisco Secure PIX связываться с сетями позади двух других коробок Межсетевого экрана PIX через VPN-туннели по Интернету или любой открытой сети с помощью IPsec. Эти две удаленных сети не имеют никакой потребности связаться друг с другом, но существует подключение к центральной сети. Эти две удаленных сети не в состоянии связаться друг с другом путем прохождения через центрального PIX (межсетевой экран), потому что PIX не направляет трафик, полученный на одном интерфейсе, отступают тот же интерфейс. Если существует потребность в удаленных сетях для передачи друг с другом, вам нужна полностью решетчатая конфигурация вместо концентратора и конфигурации оконечного устройства, показанной в этом документе. Там могло бы уже быть **nat 1**, **глобальным**, **статичным**, и подарок **инструкций канала передачи данных** на PIX. Данный пример только показывает добавление шифрования.

Предварительные условия

Требования

Для IPsec для работы *необходимо* установить подключение между оконечными точками туннеля перед началом этой конфигурации.

Используемые компоненты

Сведения в этом документе основываются на версиях 5.1.x, 5.2.x Межсетевого экрана PIX, и 6.3.3.

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.

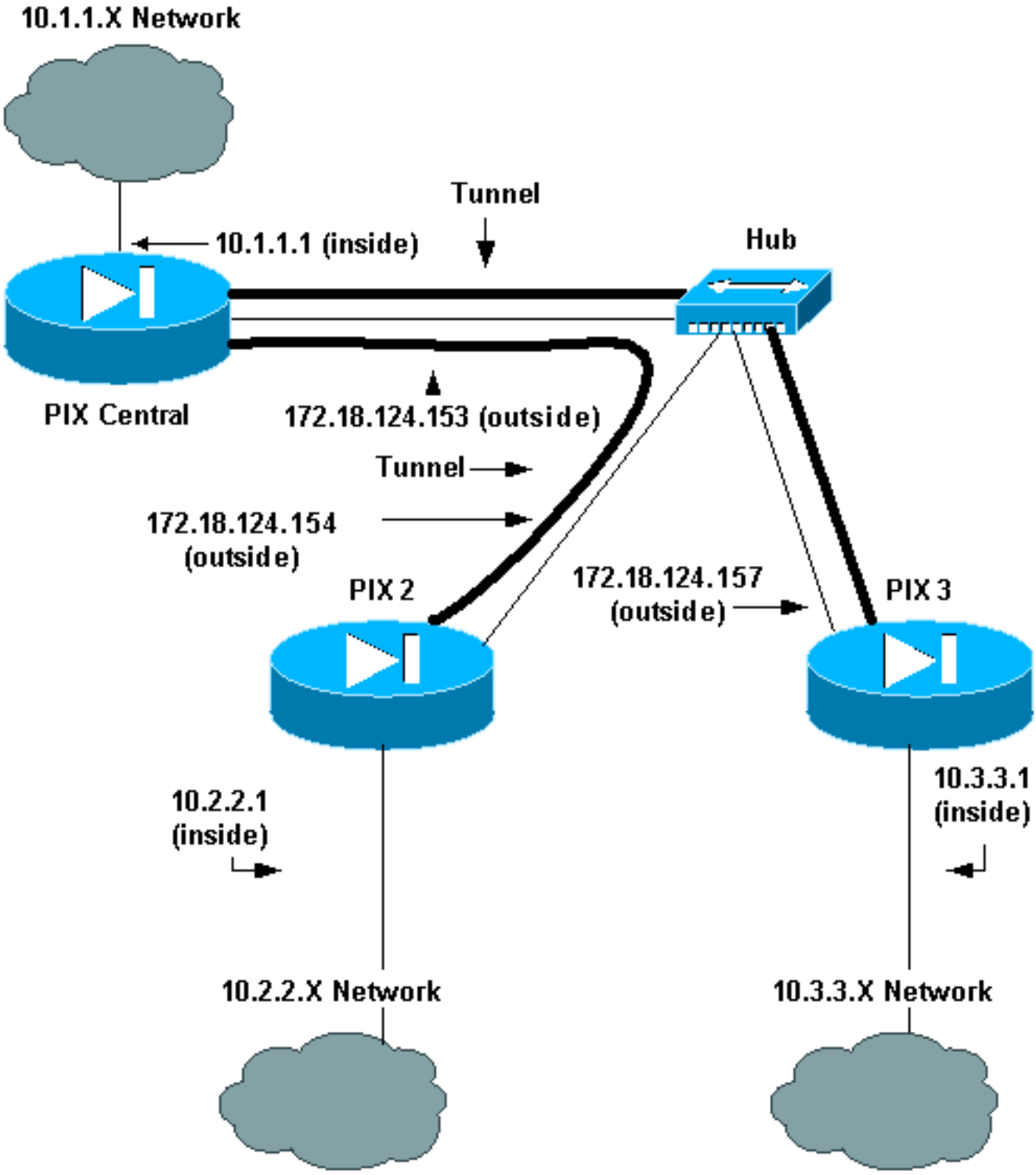
Настройка

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:

- Центральный PIX
- PIX 2
- PIX 3

Центральный 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
```

Проверка

Этот раздел позволяет убедиться, что конфигурация работает правильно.

Средство Output Interpreter (OIT) (только для зарегистрированных клиентов) поддерживает определенные команды show. **Посредством OIT можно анализировать выходные данные команд show.**

- **show crypto ipsec sa** Если трафик зашифрован, отображает текущий статус Сопоставлений безопасности IPSec (SA) и полезен в определении.
```
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** текущее состояние SA Протокола 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
```

Устранение неполадок

В этом разделе описывается процесс устранения неполадок конфигурации.

Команды для устранения неполадок

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

На PIX (с **logging monitor debugging** или выполнением **команд logging console 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.

Очистка ассоциаций безопасности

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 ассоциации безопасности IKE. Ключевое слово crypto является необязательным.**

Дополнительные сведения

- Cisco PIX Firewall Software
- Справочники по командам для межсетевого экрана PIX Cisco Secure
- Уведомления о дефектах продуктов по безопасности (включая PIX)
- Запросы комментариев (RFC)
- Согласование IPsec/Протоколы IKE
- Cisco Systems – техническая поддержка и документация