Configuration d'un réseau PIX-to-PIX-to-PIX IPSec (topologie Hub and Spoke)

Contenu

Introduction

Cette configuration permet à un pare-feu Cisco Secure PIX Firewall central de communiquer avec des réseaux derrière deux autres boîtes de pare-feu PIX via des tunnels VPN sur Internet ou tout réseau public utilisant IPsec. Les deux réseaux périphériques n'ont pas besoin de communiquer entre eux, mais il existe une connectivité au réseau central. Les deux réseaux périphériques ne peuvent pas communiquer entre eux en passant par le PIX central, car le PIX ne route pas le trafic reçu sur une interface vers la même interface. Si les réseaux périphériques doivent communiquer entre eux, vous devez disposer d'une configuration entièrement maillée, au lieu de la configuration en étoile et en étoile illustrée dans ce document. Il peut déjà y avoir des instructions **nat 1**, **global**, **static** et **conduit** sur les PIXes. Cet exemple montre uniquement l'ajout du chiffrement.

Conditions préalables

Conditions requises

Pour qu'IPsec fonctionne, vous *devez* établir la connectivité entre les points d'extrémité du tunnel avant de commencer cette configuration.

Components Used

Les informations de ce document sont basées sur les versions 5.1.x, 5.2.x et 6.3.3 du pare-feu PIX.

Remarque : La commande **show version** doit indiquer que le chiffrement est activé.

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

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

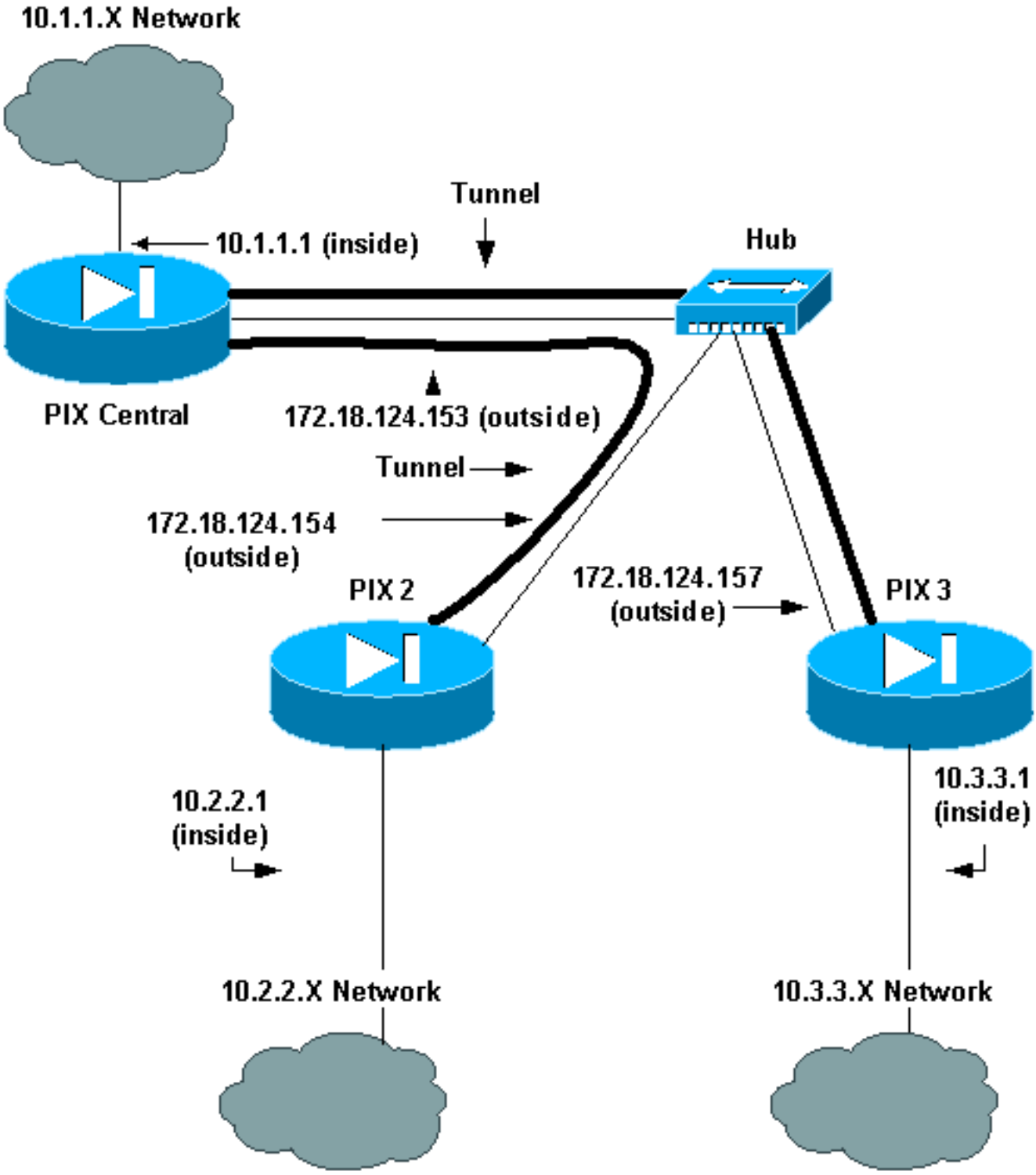
Configuration

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Remarque : utilisez l'outil de recherche de commandes (clients enregistrés uniquement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



Configurations

Ce document utilise les configurations suivantes :

- PIX Central
- PIX 2
- PIX 3

PIX Central
`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
```

Vérification

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

L'Outil Interpréteur de sortie (clients enregistrés uniquement) (OIT) prend en charge certaines commandes show. Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show .**

- **show crypto ipsec sa** - Affiche l'état actuel des associations de sécurité (SA) IPsec et permet de déterminer si le trafic est chiffré.

```
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** - Affiche l'état actuel des SA IKE (Internet Key Exchange).

```
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
```

Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Dépannage des commandes

Remarque : Consulter les renseignements importants sur les commandes de débogage avant d'utiliser les commandes de **débogage**.

Sur le PIX (avec les commandes **logging monitor debugging** ou **logging console debugging** en cours d'exécution) :

- **debug crypto ipsec** - Débogue le traitement IPsec.
- **debug crypto isakmp** - Débogue le traitement ISAKMP (Internet Security Association and Key Management Protocol).
- **debug crypto engine** - Affiche les messages de débogage sur les moteurs de chiffrement, qui effectuent le chiffrement et le déchiffrement.

Suppression des associations de sécurité

Utilisez ces commandes en mode de configuration du PIX :

- **clear [crypto] ipsec sa - Supprime les SA IPSec actives.** Le mot clé **crypto est facultatif.**
- **clear [crypto] isakmp sa — supprime les SA IKE actives.** Le mot clé **crypto est facultatif.**

Informations connexes

- Logiciels pare-feu Cisco PIX
- Références des commandes du pare-feu Cisco Secure PIX
- Notices de champs relatives aux produits de sécurité (y compris PIX)
- Demandes de commentaires (RFC)
- Négociation IPSec/Protocoles IKE
- Support et documentation techniques - Cisco Systems