

PIX-to-PIX-to-PIX (ハブ・アンド・スポーク) IPSec 設定

目次

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[設定](#)

[ネットワーク図](#)

[設定](#)

[確認](#)

[トラブルシューティング](#)

[トラブルシューティングのためのコマンド](#)

[セキュリティ アソシエーションのクリア](#)

[関連情報](#)

概要

この設定は、中央の Cisco Secure PIX Firewall がインターネットまたはパブリック ネットワーク上で IPsec を使用して、VPN のトンネルを介して 2 つの他の PIX Firewall ボックスの背後にあるネットワークと通信できます。2 つの外部ネットワークは、相互に通信する必要はありませんが、中央ネットワークへの接続があります。2 つの外部ネットワークは、PIX はあるインターフェイスで受信したトラフィックを同じインターフェイスにはルーティングしないため、中央 PIX を介して、相互に通信できません。2 つの外部ネットワークが、相互に通信する必要がある場合は、このドキュメントで説明するハブ アンド スポーク構成ではなく、フルメッシュ構成が必要です。PIX 上にすでに、nat 1、static、および conduit 文が存在する場合があります。この例では、追加の暗号化だけが示されています。

前提条件

要件

はたらく IPsec に関してはこの設定を開始する前にトンネルエンドポイント間の接続を確立して下さい。

使用するコンポーネント

この文書に記載されている情報は PIXファイアウォール バージョン 5.1.x に、5.2.x および 6.3.3 基づいています。

注: show version コマンドは暗号化が有効になることを示す必要があります。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

[表記法](#)

ドキュメント表記の詳細は、『[シスコテクニカルティップスの表記法](#)』を参照してください。

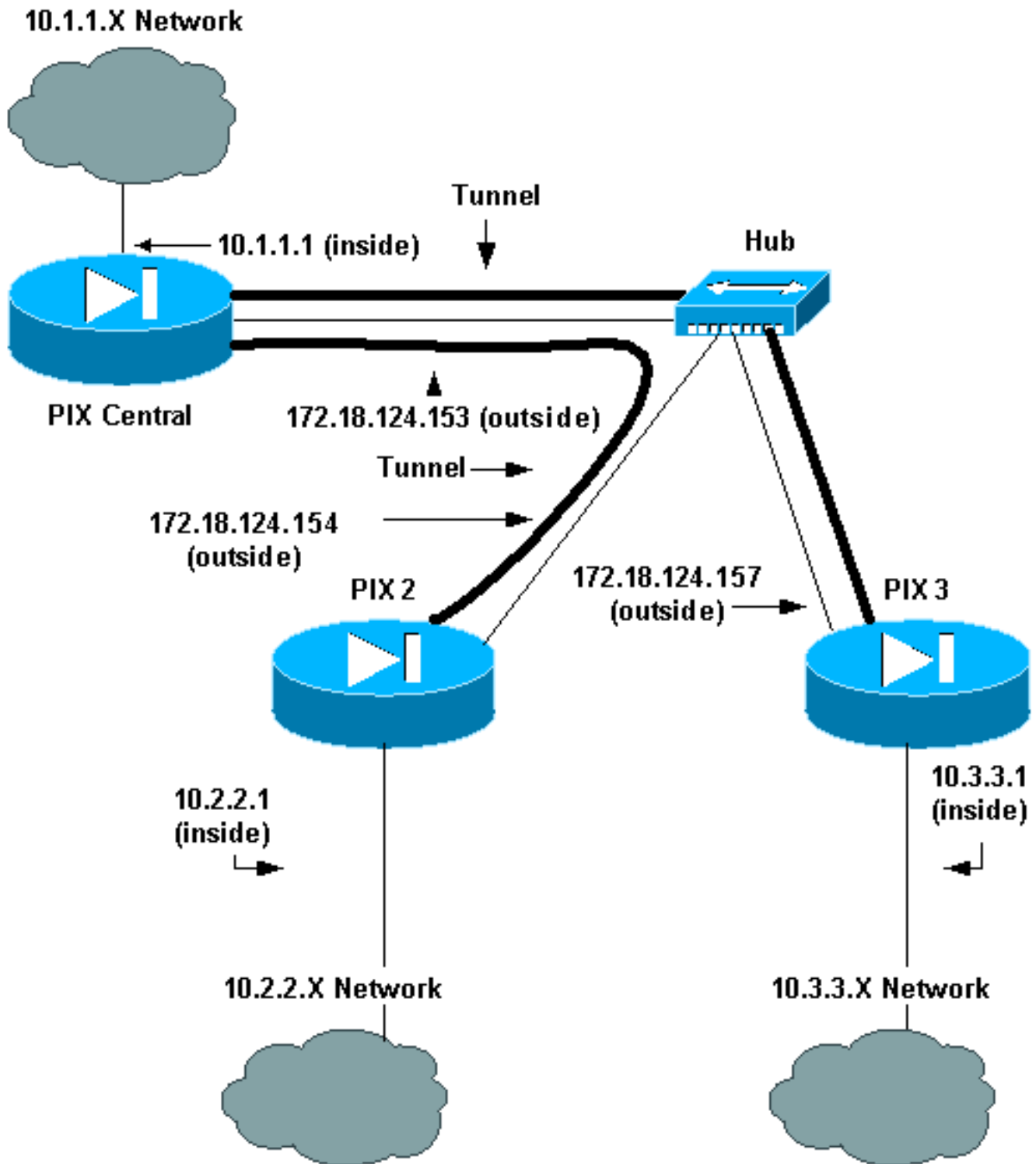
[設定](#)

この項では、このドキュメントで説明する機能の設定に必要な情報を提供します。

注: このセクションで使用されているコマンドの詳細を調べるには、[Command Lookup Tool](#) ([登録ユーザ専用](#)) を使用してください。

[ネットワーク図](#)

このドキュメントでは、次のネットワーク構成を使用しています。



設定

このドキュメントでは、次の設定を使用します。

- [PIX 本部](#)
- [PIX2](#)
- [PIX3](#)

PIX 本部

```
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

```

確認

ここでは、設定が正常に動作していることを確認します。

[Output Interpreter Tool](#) (OIT) ([登録ユーザ専用](#)) では、特定の **show** コマンドがサポートされています。OIT を使用して、**show** コマンド出力の解析を表示できます。

- **show crypto ipsec sa** — IPsecセキュリティアソシエーション結合 (SA) の現在のステータスを表示する、トラフィックが暗号化されたかどうか確認で役立ちます。
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: 3bc6913 *!--- 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: 0x3bc6913(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** — インターネット キー エクスチェンジ (IKE) SA の現在のステータスを示します。
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

[トラブルシューティング](#)

ここでは、設定のトラブルシューティングに役立つ情報について説明します。

[トラブルシューティングのためのコマンド](#)

注: [debug](#) コマンドを使用する前に、『[debug コマンドの重要な情報](#)』を参照してください。

PIX (動作する logging monitor debugging か logging console debugging コマンドと) :

- **debug crypto ipsec** — IPsec 処理をデバッグします。
- **debug crypto isakmp** — Internet Security Association and Key Management Protocol (ISAKMP) 処理をデバッグします。

- **debug crypto engine** : 暗号化と復号化を行う暗号化エンジンに関するデバッグ メッセージを表示します。

[セキュリティ アソシエーションのクリア](#)

PIX のコンフィギュレーションモードでこれらのコマンドを使用して下さい:

- **clear [crypto] ipsec sa** : アクティブな IPSec SA を削除します。 crypto キーワードはオプションです。
- **clear [crypto] ipsec sa** : アクティブな IKE SA を削除します。 crypto キーワードはオプションです。

[関連情報](#)

- [Cisco PIX Firewall ソフトウェア](#)
- [Cisco Secure PIX ファイアウォール コマンド リファレンス](#)
- [セキュリティ製品に関する Field Notice \(PIX を含む \)](#)
- [Requests for Comments \(RFC \)](#)
- [IPSec ネゴシエーション/IKE プロトコル](#)
- [テクニカルサポートとドキュメント - Cisco Systems](#)