

完全メッシュ PIX to PIX to PIX IPsec 設定

内容

[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](#)

[関連情報](#)

概要

この設定では、3つの Cisco Secure PIX Firewall ボックスの背後にあるプライベート ネットワークが、インターネットまたは IPsec を使用するパブリック ネットワークから VPN のトンネルで接続できるようになります。3つのネットワークにはそれぞれ、他の2つのネットワークに接続されています。このシナリオでは、パブリック インターネットへの接続にはネットワーク アドレス変換 (NAT) が必要です。ただし、3つのイントラネット間のトラフィックにはNATは必要ありません。これらのイントラネットは、パブリックインターネット上のVPNトンネルを使用して送信できます。

前提条件

要件

IPsecが機能するには、この設定を開始する前に、トンネルエンドポイントからトンネルエンドポイントへの接続が必要です。

使用するコンポーネント

この設定は、PIX Firewallバージョン6.1(2)で開発およびテストされています。

注： `show version` コマンドで、暗号化が有効になっていることが示されている必要があります。

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ました。このドキュメントで使用するすべてのデバイスは、初期 (デフォルト) 設定の状態から起動しています。対象のネットワークが稼働中である場合には、どのようなコマンドについても、その潜在的

な影響について確実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については、『[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。

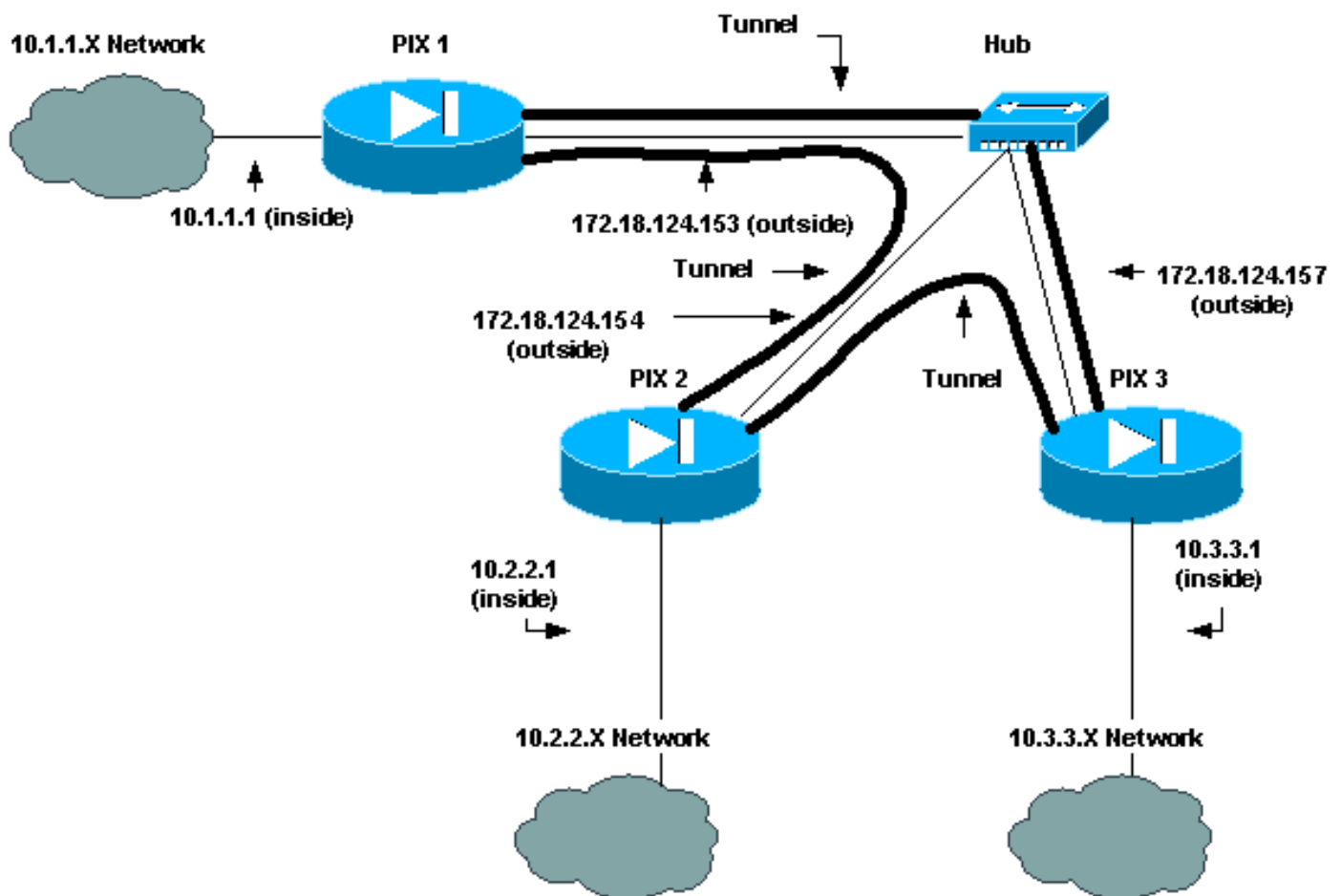
設定

このセクションでは、このドキュメントで説明する機能を設定するために必要な情報を提供しています。

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)を参照してください。一部ツールについては、ゲスト登録のお客様にはアクセスできない場合がありますことをご了承ください。

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 セットアップを使用します。



設定

このドキュメントでは、次の構成を使用します。

- [PIX 1](#)

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

PIX 1 の設定

```

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]

```

PIX 2 の設定

```

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
```

PIX 3 の設定

```
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]
```

確認

現在、この設定に使用できる確認手順はありません。

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使用できる情報を示します。詳細は、『[確立されたIPSecトンネルでデータトラフィックを通過させるPIXのトラブルシューティング](#)』を参照してください。

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。

デバッグ コマンド

logging monitor debuggingコマンドまたはlogging console debuggingコマンドを実行して、PIXでこれらのコマンドを使用します。

- **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。

clearコマンド

セキュリティアソシエーション(SA)をクリアするには、PIXのコンフィギュレーションモードで次のコマンドを使用します。

- **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] isakmp sa** : アクティブなインターネットキーエクスチェンジ(IKE)SAを削除します。crypto キーワードはオプションです。

注：IPsecが機能するには、この設定を開始する前に、トンネルエンドポイントからトンネルエンドポイントへの接続が必要です。

関連情報

- [確立されたIPSec トンネル上のパステータトラフィックへのPIX のトラブルシューティング](#)
- [Cisco PIX 500 シリーズ セキュリティ アプライアンス](#)
- [PIX コマンド リファレンス](#)
- [IPsecネゴシエーション/IKEプロトコル](#)
- [Requests for Comments \(RFCs\)](#)
- [テクニカル サポートとドキュメント - Cisco Systems](#)