

# PIX 6.x : アクセス リストと NAT を使用して PIX Firewall をパススルーする IPSec トンネルの設定例

## 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

このドキュメントでは、Network Address Translation ( NAT; ネットワーク アドレス変換 ) を実行するファイアウォール経由での IPSec トンネルの設定例を示しています。この設定はポートアドレス変換 ( PAT ) と 12.2(13)T より前に Cisco IOS® ソフトウェア リリースを使用する場合機能しません。この種の設定は、IP トラフィックのトンネル伝送に使用できます。IPX やルーティング アップデートなど、ファイアウォールを経由しないトラフィックの暗号化には、この設定は使用できません。このような種類の設定には、Generic Routing Encapsulation ( GRE; 総称ルーティング カプセル化 ) トンネル伝送が適しています。このドキュメントの例では、Cisco 2621 ルータと 3660 ルータが 2 つのプライベート ネットワークを結合する IPSec トンネルのエンドポイントで、中間の PIX に IPSec トラフィックを許可するためのコンジット ( conduit ) または Access Control List ( ACL; アクセス コントロール リスト ) があります。

注: NAT は 1 対 1 のアドレス変換です。多 ( ファイアウォールの Inside ) 対 1 の変換である PAT と混同しないでください。 [NAT の動作と設定の詳細は、『NAT オペレーションの検証と NAT の基本的なトラブルシューティング』](#) または [『NAT の動作の仕組み』](#) を参照してください。

注: PAT を使用する IPsec は、トンネル外部のエンドポイントのデバイスが 1 つの IP アドレスからの複数のトンネルを処理できないために、正しく動作しない場合があります。トンネルのエンドポイントのデバイスが PAT で動作するかどうかを、ベンダーに問い合わせて確認する必要があります。また、バージョン 12.2(13)T 以降では、PAT に対して NAT 透過機能も使用できます。 [詳細は、『IPSec NAT 透過』](#) を参照してください。 [バージョン 12.2\(13\)T 以降でのこれらの機能の詳細は、『NAT を使用した IPSec ESP のサポート』](#) を参照してください。 [また、TAC でサービ](#)

[スリクエストをオープンする前に、『NATに関するFAQ』](#)を参照してください。よくある質問に対する多くの回答があります。

[PIX/ASA バージョン 7.x で NAT を使用してファイアウォールを通過する IPSec トンネルを設定する方法の詳細は、『アクセスリストと MPF を使用した NAT を使用するセキュリティ アプリアンスをパススルーする IPSec トンネルの設定例』](#)を参照してください。

## [前提条件](#)

### [要件](#)

このドキュメントに関する固有の要件はありません。

### [使用するコンポーネント](#)

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Cisco IOS ソフトウェア リリース 12.0.7.T ( 12.2(13)T よりも前 ) [さらに新しいバージョンについては、『IPSec NAT 透過』](#)を参照してください。
- Cisco 2621 ルータ Cisco IOS ソフトウェア リリース 12.4 実行する
- Cisco 3660 ルータ Cisco IOS ソフトウェア リリース 12.4 実行する
- Cisco PIX Firewall 6.x を実行する

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。

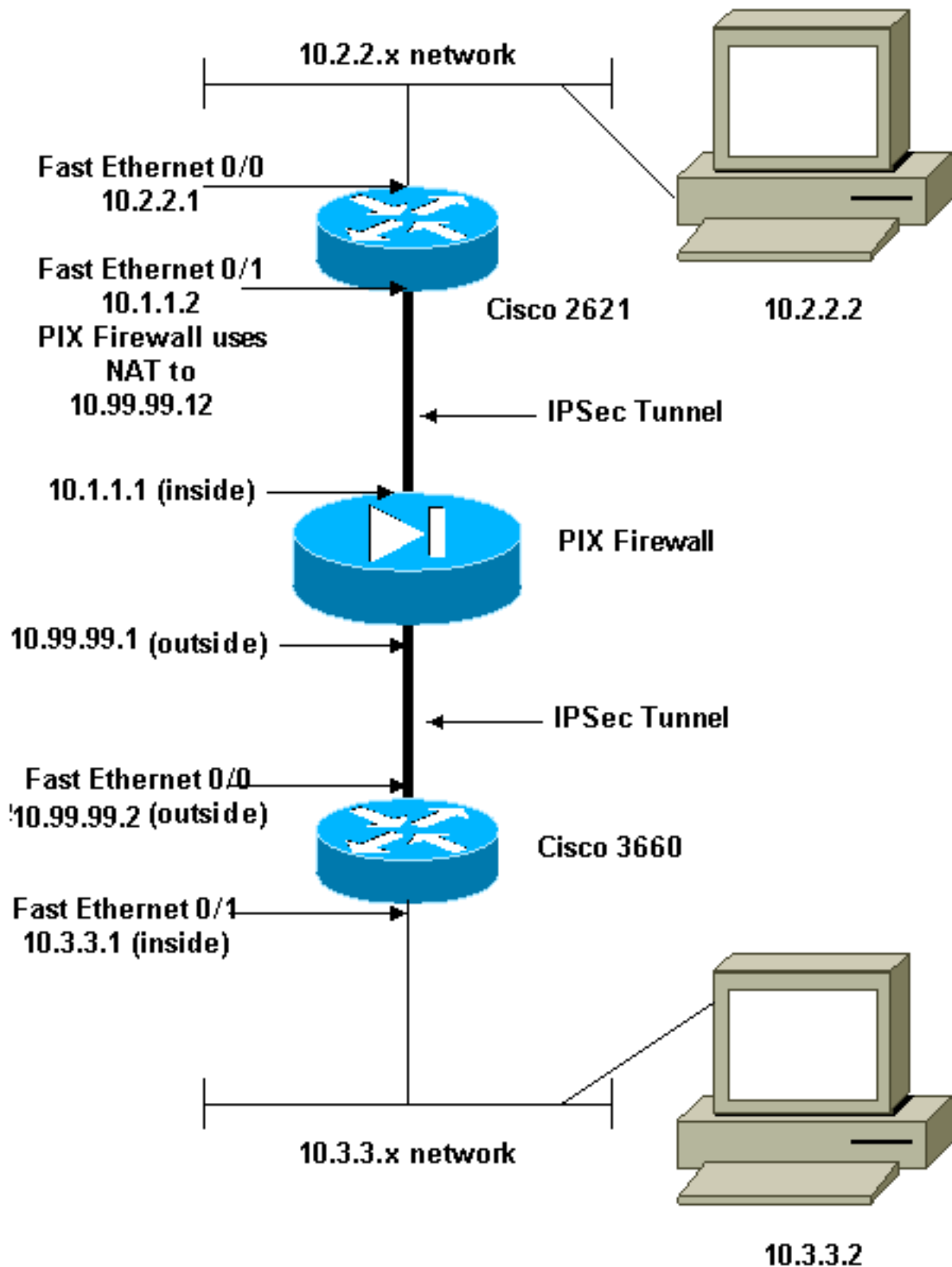
## [設定](#)

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: このドキュメント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。



注: この設定で使用している IP アドレススキームは、インターネット上で正式にルーティング可能なものではありません。これらは、ラボ環境で使用された [RFC 1918](#) のアドレスです。

## 設定

このドキュメントでは、次の設定を使用します。

- [Cisco 2621 の設定](#)
- [Cisco PIX Firewall の部分設定](#)
- [Cisco 3660 の設定](#)

## Cisco 2621 の設定

Current configuration:

```
!  
version 12.4  
service timestamps debug uptime  
service timestamps log uptime  
no service password-encryption  
!  
hostname goss-2621  
!  
ip subnet-zero  
!  
ip audit notify log  
ip audit po max-events 100  
isdn voice-call-failure 0  
cns event-service server  
!  
!--- IKE Policy crypto isakmp policy 10 hash md5  
authentication pre-share crypto isakmp key cisco123  
address 10.99.99.2 ! crypto ipsec transform-set myset  
esp-des esp-md5-hmac ! crypto map mymap local-address  
FastEthernet0/1 !--- IPSec Policy crypto map mymap 10  
ipsec-isakmp set peer 10.99.99.2 set transform-set myset  
!--- Include the private-network-to-private-network  
traffic !--- in the encryption process. match address  
101 ! controller T1 1/0 ! interface FastEthernet0/0 ip  
address 10.2.2.1 255.255.255.0 no ip directed-broadcast  
duplex auto speed auto ! interface FastEthernet0/1 ip  
address 10.1.1.2 255.255.255.0 no ip directed-broadcast  
duplex auto speed auto !--- Apply to interface. crypto  
map mymap ! ip classless ip route 0.0.0.0 0.0.0.0  
10.1.1.1 no ip http server !--- Include the private-  
network-to-private-network traffic !--- in the  
encryption process. access-list 101 permit ip 10.2.2.0  
0.0.0.255 10.3.3.0 0.0.0.255 line con 0 transport input  
none line aux 0 line vty 0 4 ! no scheduler allocate end
```

## Cisco PIX Firewall の部分設定

```
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  
!--- The fixup protocol esp-ike command is disabled by  
default. fixup protocol esp-ike ip address outside  
10.99.99.1 255.255.255.0 ip address inside 10.1.1.1  
255.255.255.0 !--- Range of registered IP addresses for  
use. global (outside) 1 10.99.99.50-10.99.99.60 !---  
Translate any internal source address when !--- going  
out to the Internet. nat (inside) 1 0.0.0.0 0.0.0.0 0 0  
static (inside,outside) 10.99.99.12 10.1.1.2 netmask  
255.255.255.255 0 0 !--- or access-list acl-out permit  
esp host 10.99.99.2 host 10.99.99.12 access-list acl-out  
permit udp host 10.99.99.2 host 10.99.99.12 eq isakmp  
access-list acl-out permit udp host 10.99.99.2 host
```

```
10.99.99.12 eq 4500 !--- It is important to permit UDP
port 4500 for NAT-T because the PIX is acting !--- as a
NAT device between the routers. access-group acl-out in
interface outside isakmp enable outside isakmp enable
inside Command configured in order to enable NAT-T
isakmp nat-traversal 20 route outside 0.0.0.0 0.0.0.0
99.99.99.2 1 route inside 10.2.2.0 255.255.255.0
10.1.1.2 1
```

注: フィックスアッププロトコル **esp-ike** コマンドはデフォルトでディセーブルにされます。フィックスアッププロトコル **esp-ike** コマンドが発行される場合、フィックスアップはつき、PIXファイアウォールはインターネット キー エクスチェンジ (IKE) の送信元ポートを維持します。それはまた ESP トラフィックのための PAT 変換を作成します。esp-ike フィックスアップがオンになっていればさらに、Internet Security Association and Key Management Protocol (ISAKMP) はあらゆるインターフェイスで有効にすることができません。

### Cisco 3660 の設定

```
version 12.4
 service timestamps debug uptime
 service timestamps log uptime
 no service password-encryption
 !
 hostname goss-3660
 !
 ip subnet-zero
 !
 cns event-service server
 !
 !--- IKE Policy crypto isakmp policy 10 hash md5
 authentication pre-share crypto isakmp key cisco123
 address 10.99.99.12 ! crypto ipsec transform-set myset
 esp-des esp-md5-hmac ! crypto map mymap local-address
 FastEthernet0/0 !--- IPSec Policy crypto map mymap 10
 ipsec-isakmp set peer 10.99.99.12 set transform-set
 myset !--- Include the private-network-to-private-
 network traffic !--- in the encryption process. match
 address 101 ! interface FastEthernet0/0 ip address
 10.99.99.2 255.255.255.0 no ip directed-broadcast ip nat
 outside duplex auto speed auto !--- Apply to interface.
 crypto map mymap ! interface FastEthernet0/1 ip address
 10.3.3.1 255.255.255.0 no ip directed-broadcast ip nat
 inside duplex auto speed auto ! interface Ethernet3/0 no
 ip address no ip directed-broadcast shutdown ! interface
 Serial3/0 no ip address no ip directed-broadcast no ip
 mroute-cache shutdown ! interface Ethernet3/1 no ip
 address no ip directed-broadcast interface Ethernet4/0
 no ip address no ip directed-broadcast shutdown !
 interface TokenRing4/0 no ip address no ip directed-
 broadcast shutdown ring-speed 16 ! !--- Pool from which
 inside hosts translate to !--- the globally unique
 10.99.99.0/24 network. ip nat pool OUTSIDE 10.99.99.70
 10.99.99.80 netmask 255.255.255.0 !--- Except the
 private network from the NAT process. ip nat inside
 source route-map nonat pool OUTSIDE ip classless ip
 route 0.0.0.0 0.0.0.0 10.99.99.1 no ip http server ! !--
 - Include the private-network-to-private-network traffic
 !--- in the encryption process. access-list 101 permit
 ip 10.3.3.0 0.0.0.255 10.2.2.0 0.0.0.255 access-list 101
 deny ip 10.3.3.0 0.0.0.255 any !--- Except the private
 network from the NAT process. access-list 110 deny ip
 10.3.3.0 0.0.0.255 10.2.2.0 0.0.0.255 access-list 110
```

```
permit ip 10.3.3.0 0.0.0.255 any route-map nonat permit
10 match ip address 110 ! line con 0 transport input
none line aux 0 line vty 0 4 ! 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** : フェーズ 2 のセキュリティ アソシエーションを表示します。
- **show crypto isakmp sa** : フェーズ 1 のセキュリティ アソシエーションを表示します。
- **show crypto engine connections active** : 暗号化パケットおよび復号化パケットを表示します。

## トラブルシューティング

ここでは、設定に関するトラブルシューティング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。

- **debug crypto engine** : 暗号化されたトラフィックを表示します。
- **debug crypto ipsec** : フェーズ 2 の IPsec ネゴシエーションを表示します。
- **debug crypto isakmp** — フェーズ 1 の ISAKMP ネゴシエーションを見るのに使用して下さい。

### セキュリティ アソシエーションのクリア

- **clear crypto isakmp** — IKE セキュリティ結合をクリアします。
- **clear crypto ipsec sa** - IPsec のセキュリティ アソシエーションをクリアします。

## 関連情報

- [Cisco PIX 500 シリーズ セキュリティ アプライアンス](#)
- [Cisco Secure PIX ファイアウォール コマンド リファレンス](#)
- [NAT に関するサポートページ](#)
- [Request for Comments \( RFC \)](#)
- [テクニカルサポートとドキュメント - Cisco Systems](#)