

PIX 6.x : NAT により、スタティックにアドレス指定された PIX Firewall とダイナミックにアドレス指定された IOS ルータ間のダイナミック IPsec の設定例

目次

[はじめに](#)

[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](#)

[はじめに](#)

このドキュメントでは、PIX がダイナミック IPsec 接続を受け入れられるようにするための設定例について説明します。プライベート ネットワーク 10.1.1.x からインターネットにアクセスする場合は、リモート ルータがネットワーク アドレス変換 (NAT) を実行します。10.1.1.x から PIX の背後にあるプライベート ネットワーク 192.168.1.x へのトラフィックは、NAT プロセスからは除外されます。ルータは PIX への接続を開始できますが、PIX はルータへの接続を開始できません。

この設定は、パブリック インターフェイス (外部インターフェイス) でダイナミック IP アドレスを受信する Cisco IOS® ルータを使用してダイナミック IPsec LAN-to-LAN (L2L) トンネルを作成するために、PIX Firewall を使用します。IP アドレスをサービス プロバイダー (ISP) からダイナミックに割り当てるために、Dynamic Host Configuration Protocol (DHCP) はメカニズムを提供します。これにより、ホストで使用されなくなった IP アドレスを再利用できます。

ルータが 6.x を実行する PIX セキュリティ アプライアンスからのダイナミック IPsec 接続を受け入れるシナリオの詳細については、「[NAT による Dynamic-to-Static IPsec の設定例](#)」を参照してください。

PIX/ASA セキュリティ アプライアンスで Cisco IOS ルータからのダイナミック IPsec 接続を受け入れることができるようにするには、『[スタティック IOS ルータと NAT 付きダイナミック PIX/ASA 7.x の間の IPsec の設定例](#)』を参照してください。

PIX/ASA セキュリティ アプライアンスがソフトウェア バージョン 7.x 以降を実行している場合の同じシナリオについては、「[NAT による静的 PIX/ASA 7.x とダイナミック IOS ルータとの間の IPsec 設定](#)」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しては個別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 12.4
- Cisco PIX ファイアウォール ソフトウェア リリース 6.3.1
- Cisco Secure PIX Firewall 515E
- Cisco 7206 ルータ

本書の情報は、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、初期（デフォルト）設定の状態から起動しています。稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

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。

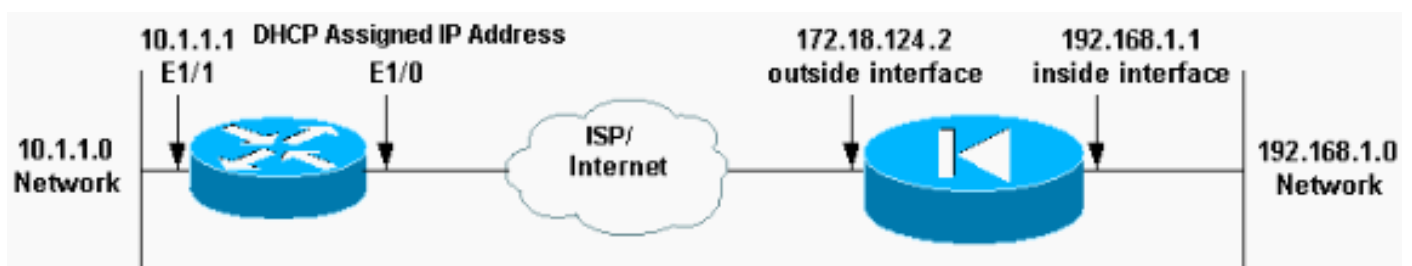
設定

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。



設定

このドキュメントでは、次の設定を使用します。

- [Elf \(PIX\)](#)
- [Mop \(Cisco 7204 ルータ \)](#)

Elf (PIX)

```
Building configuration...
: Saved
:
PIX Version 6.3(1)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 intf2 security10
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname elf
fixup protocol ftp 21
fixup protocol http 80
fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
fixup protocol skinny 2000
names
!--- Access control list (ACL) to avoid NAT on the IPsec
packets. access-list nonat permit ip 192.168.1.0
255.255.255.0 10.1.1.0 255.255.255.0
pager lines 24
logging on
logging buffered debugging
interface ethernet0 auto
interface ethernet1 auto
interface ethernet2 auto shutdown
mtu outside 1500
mtu inside 1500
mtu intf2 1500
ip address outside 172.18.124.2 255.255.255.0
ip address inside 192.168.1.1 255.255.255.0
ip address intf2 127.0.0.1 255.255.255.255
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
failover ip address intf2 0.0.0.0
pdm history enable
arp timeout 14400
global (outside) 1 interface
!-- Binds ACL nonat to the NAT statement to avoid NAT on
the IPsec packets nat (inside) 0 access-list nonat
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
!--- Permits Internet Control Message Protocol (ICMP)
traffic for testing. !--- Do not enable it in a live
network. conduit permit icmp any any
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
aaa-server LOCAL protocol tacacs+
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
!--- IPsec configuration crypto ipsec transform-set
router-set esp-des esp-md5-hmac
crypto dynamic-map cisco 1 set transform-set router-set
crypto map dyn-map 10 ipsec-isakmp dynamic cisco
crypto map dyn-map interface outside
isakmp enable outside
!--- Internet Security Association and Key Management
Protocol (ISAKMP) !--- policy for accepting dynamic
connections from remote PIX. !--- Note: In real show run
output, the pre-shared key appears as *****. isakmp
key cisco123 address 0.0.0.0 netmask 0.0.0.0
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 86400
telnet timeout 5
ssh timeout 5
terminal width 80
Cryptochecksum:eeb67d5df47045f7e6ac4aa090aab683
: end
[OK]
elf#
```

Mop (Cisco 7204 ルータ)

```
mop#show running-configuration
Building configuration...

Current configuration : 1916 bytes
!
version 12.4
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname mop
!
!
ip subnet-zero
!
!
no ip domain-lookup
!
ip cef
ip audit notify log
ip audit po max-events 100
!
!--- Internet Key Exchange (IKE) policies crypto isakmp
```

```

policy 1
  hash md5
  authentication pre-share
crypto isakmp key cisco123 address 172.18.124.2
!
!
!---- IPsec policies crypto ipsec transform-set pix-set
esp-des esp-md5-hmac
!
crypto map pix 10 ipsec-isakmp
  set peer 172.18.124.2
  set transform-set pix-set
  match address 101
!
interface FastEthernet0/0
  no ip address
  shutdown
  duplex half
!
interface Ethernet1/0
ip address dhcp
ip nat outside
duplex half
crypto map pix
!
interface Ethernet1/1
ip address 10.1.1.1 255.255.255.0
ip nat inside
duplex half
!
!---- Except the private network from the NAT process. ip
nat inside source route-map nonat interface Ethernet1/0
overload
ip classless
ip route 0.0.0.0 0.0.0.0 Ethernet1/0
no ip http server
ip pim bidir-enable
!
!---- Include the private-network-to-private-network !---
traffic in the encryption process. access-list 101
permit ip 10.1.1.0 0.0.0.255 192.168.1.0 0.0.0.255
!---- Except the private network from the NAT process.
access-list 110 deny ip 10.1.1.0 0.0.0.255 192.168.1.0
0.0.0.255
access-list 110 permit ip 10.1.1.0 0.0.0.255 any
!
route-map nonat permit 10
  match ip address 110
!
line con 0
  exec-timeout 0 0
line aux 0
line vty 0 4
  login
!
!
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。

これらの **show** コマンドは、PIX およびルータ上で実行できます。

- **show crypto isakmp sa** : ピアにおける現在の IKE セキュリティ アソシエーション (SA) をすべて表示します。
- **show crypto ipsec sa** : 現在の (IPSec) SA で使用されている設定を表示します。
- **show crypto engine connections active** : 現在の接続と、暗号化および復号化されたパケットの情報 (ルータのみ) を表示します。

両方のピアで SA をクリアする必要があります。

- PIX コマンドは、設定モードで実行されます。**clear crypto isakmp sa** : フェーズ 1 SA をクリアします。**clear crypto ipsec sa** : フェーズ 2 SA をクリアします。
- ルータのコマンドは、イネーブル モードで実行されます。**clear crypto isakmp** : フェーズ 1 SA をクリアします。**clear crypto sa** : フェーズ 2 SA をクリアします。

[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](#)

[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。

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。

- **show crypto isakmp sa** : 現在ピアにあるすべての IKE SA を表示します。
- **show crypto ipsec sa** : 現在の (IPSec) SA で使用されている設定を表示します。
- **show crypto engine connections active** : 現在の接続と、暗号化および復号化されたパケットの情報 (ルータのみ) を表示します。

[関連情報](#)

- [IPSec ネゴシエーション/IKE プロトコルに関するサポート ページ](#)
- [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](#)
- [Requests for Comments \(RFC \)](#)
- [テクニカル サポートとドキュメント – Cisco Systems](#)