PIX 6.x： NAT を使用した、スタティックにアドレス指定された IOS ルータとダイナミックにアドレス指定された PIX ファイアウォール間のダイナミック IPSec の設定例

目次

はじめに

このドキュメントでは、IOS® ルータで PIX ファイアウォールからのダイナミック IPSec 接続を許可できるようにする設定例を紹介します。 リモート ルータは、プライベート ネットワーク 10.0.0.x がインターネットにアクセスする場合、Network Address Translation (NAT; ネットワーク アドレス変換) を行います。 10.0.0.x から PIX の背後にあるプライベート ネットワーク 10.1.0.x へのトラフィックは、NAT プロセスからは除外されます。 PIX ファイアウォールはルータへの接続を開始できますが、ルータが PIX への接続を開始することはできません。

この設定では、Cisco IOS ルータを使用して、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 PIX ファイアウォールを持つ IPsec LAN-to-LAN (L2L) トンネルを作成します。 Dynamic Host Configuration Protocol (DHCP) によって、IP アドレスをインターネット 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の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。

PIX がルータ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、『ACS 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』を参照してください。

Cisco PIX セキュリティ アプライアンス ソフトウェア バージョン 7.x または Cisco 適応型セキュリティ アプライアンス (ASA) で、Open Shortest Path First (OSPF) を使用して GRE トンネ

ルのない VPN/IPsec を設定する方法の詳細については、PIX/ASA 7.x 以降： 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』を参照してください。

Cisco PIX セキュリティ アプライアンス ソフトウェア バージョン 7.x または Cisco 適応型セキュリティ アプライアンス（ASA）で、Open Shortest Path First（OSPF）を使用して GRE トンネルのない VPN/IPsec を設定する方法の詳細については、PIX/ASA 7.x 以降： 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』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 Firewall ソフトウェア リリース 6.3.4
- Cisco Secure PIX Firewall 515E
- Cisco 2811 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。

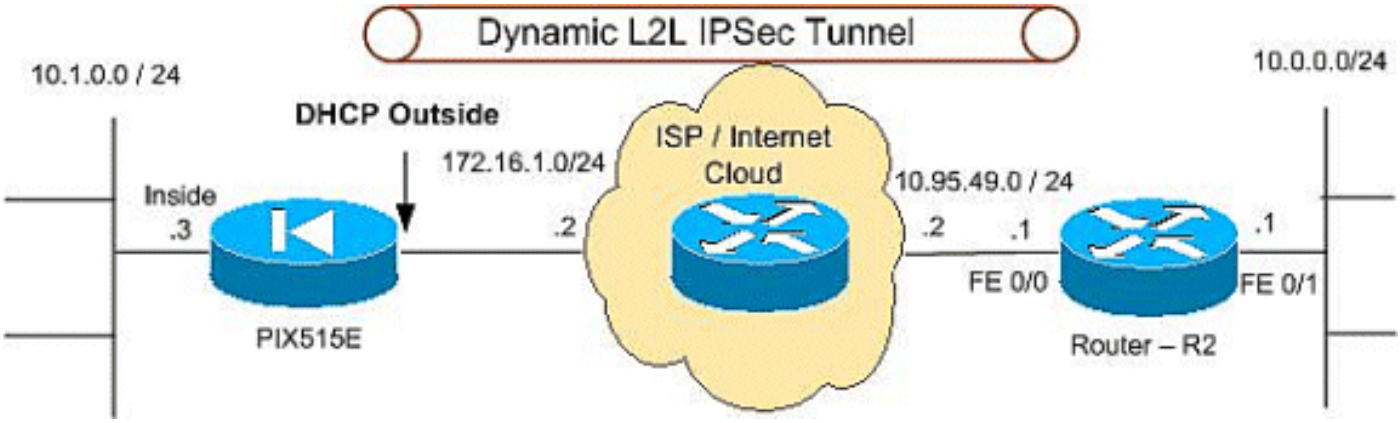
設定

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。

- PIX 515E
- R2（Cisco 2811 ルータ）

PIX 515E

```
PIX Version 6.3(4)
interface ethernet0 100full
interface ethernet1 100full
interface ethernet2 shut
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 intf2 security4
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname PIX515E
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

!--- The access control list (ACL) to avoid NAT on the
IPsec packets. access-list NO-NAT permit ip 10.1.0.0
255.255.255.0 10.0.0.0 255.255.255.0
!--- The ACL to apply on crypto map. !--- Include the
private-network-to-private-network traffic !--- in the
encryption process. access-list 101 permit ip 10.1.0.0
255.255.255.0 10.0.0.0 255.255.255.0
pager lines 24
logging on
mtu outside 1500
mtu inside 1500
mtu intf2 1500
!--- ISP will providthe the Outside IP address.
```

```
ip address outside dhcp

ip address inside 10.1.0.3 255.255.255.0
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
no failover ip address intf2
pdm history enable
arp timeout 14400
global (outside) 1 interface
nat (inside) 0 access-list NO-NAT
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
route outside 10.0.0.0 255.255.255.0 172.16.1.5 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 TACACS+ max-failed-attempts 3
aaa-server TACACS+ deadtime 10
aaa-server RADIUS protocol radius
aaa-server RADIUS max-failed-attempts 3
aaa-server RADIUS deadtime 10
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

!--- IPsec configuration, Phase 2. crypto ipsec
transform-set DYN-TS esp-des esp-md5-hmac
crypto map IPSEC 10 ipsec-isakmp
crypto map IPSEC 10 match address 101
crypto map IPSEC 10 set peer 10.95.49.1
crypto map IPSEC 10 set transform-set DYN-TS
crypto map IPSEC interface outside
!--- Internet Security Association and Key Management
Protocol (ISAKMP) !--- policy, Phase 1. !--- Note: In
real show run output, the pre-shared key appears as
*******.

isakmp enable outside
isakmp key cisco123 address 10.95.49.1 netmask
255.255.255.255
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
console timeout 0
terminal width 80
Cryptochecksum:f0294298e214a947fc2e03f173e4a405
: end
```

R2（Cisco 2811 ルータ）

```
R2#show running-configuration
Building configuration...

Current configuration : 1916 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname r1800
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
!
resource policy
!
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip subnet-zero
ip cef
!
!
no ip dhcp use vrf connected
!
!
no ip ips deny-action ips-interface
!
no ftp-server write-enable
!
!
!--- ISAKMP policy, Phase 1. crypto isakmp policy 10
hash md5
authentication pre-share
crypto isakmp key 6 cisco123 address 0.0.0.0 0.0.0.0
!
!
!--- IPsec policy, Phase 2. crypto ipsec transform-set
DYN-TS esp-des esp-md5-hmac
!
crypto dynamic-map DYN 10
set transform-set DYN-TS
match address 101
!
!
crypto map IPSEC 10 ipsec-isakmp dynamic DYN
!
!
!
interface FastEthernet0/0
ip address 10.95.49.1 255.255.255.0
ip nat outside
ip virtual-reassembly
load-interval 30
duplex auto
speed auto
```

```
crypto map IPSEC
!
interface FastEthernet0/1
ip address 10.0.0.1 255.255.255.0
ip nat inside
ip virtual-reassembly
duplex auto
speed auto
!
ip classless
ip route 10.1.0.0 255.255.255.0 10.95.49.2
!
ip http server
no ip http secure-server
!--- Except the private network from the NAT process. ip
nat inside source list 102 interface FastEthernet0/0
overload
!
!--- Include the private-network-to-private-network !---
traffic in the encryption process. access-list 101
permit ip 10.0.0.0 0.0.0.255 10.1.0.0 0.0.0.255

!--- Except the private network from the NAT process.
access-list 102 deny ip 10.0.0.0 0.0.0.255 10.1.0.0
0.0.0.255
access-list 102 permit ip 10.0.0.0 0.0.0.255 any
!
!
control-plane
!
!
line con 0
exec-timeout 0 0
line aux 0
line vty 0 4
exec-timeout 0 0
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。

- **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。

設定モードで、次の PIX コマンドを実行します。

- **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。

イネーブル モードで、次のルータ コマンドを実行します。

- **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

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

- 一般的な L2L およびリモート アクセス IPSec VPN のトラブルシューティング方法について
- 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
- Requests for Comments（RFC）
- IPSec ネゴシエーション/IKE プロトコル