ASA/PIX： IOS ルータ LAN-to-LAN IPSec トンネルへのセキュリティ アプライアンス接続の設定例

目次

概要

このドキュメントでは、内部ネットワークが 1 つである PIX セキュリティ アプライアンス 7.x 以降または Adaptive Security Appliance (ASA) から、暗号イメージを実行する 2611 ルータへの IPSsec トンネルの設定方法を示します。 話を簡単にするため、スタティック ルートを使用します。

ルータと PIX の間の LAN-to-LAN トンネル設定の詳細については、『ルータから PIX へ間の IPSec の設定』を参照してください。

PIX ファイアウォールと Cisco VPN 3000 コンセントレータの間の LAN-to-LAN トンネル設定の詳細については、『Cisco VPN 3000 コンセントレータと PIX ファイアウォール間の LAN-to-LAN IPSec トンネルの設定例』を参照してください。

LAN-to-LAN トンネルが PIX と VPN コンセントレータの間に存在するシナリオの詳細については、『PIX 7.x および VPN 3000 コンセントレータ間の IPSec トンネルの設定例』を参照してください。

複数の PIX 間の LAN-to-LAN トンネルが、VPN クライアントがハブ PIX を介してスポーク PIX にアクセスすることを許可するシナリオの詳細については、『TACACS+ 認証を使用した PIX/ASA 7.x 拡張 Spoke-to-Client VPN の設定例』を参照してください。

PIX/ASA セキュリティ アプライアンスでソフトウェア バージョン 8.x が稼働している場合の同様のシナリオについては、『SDM: ASA/PIX および IOS ルータ間の Site-to-Site IPsec VPN の設定例』を参照してください。

ASA 関連の設定が ASDM GUI を使用して表示され、ルータ関連の設定が Cisco CP GUI を使用して表示される同様のシナリオについては、『Configuration Professional: ASA/PIX および IOS ルータ間の Site-to-Site IPsec VPN 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。

- PIX ソフトウェア バージョン 7.0 が稼働する PIX-525
- Cisco IOS(R) ソフトウェア リリース 12.2(15)T13 が稼働する Cisco 2611 ルータ

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。

背景説明

PIX では、**access-list** および **nat 0** コマンドが連携して機能します。 10.1.1.0 ネットワーク上のユーザが 10.2.2.0 ネットワークにアクセスする際には、10.1.1.0 ネットワークのトラフィックを Network Address Translation（NAT; ネットワーク アドレス変換）を行わずに暗号化することを許可するために、アクセス リストが使用されます。 ルータでは、10.2.2.0 ネットワークのトラフィックを NAT 変換せずに暗号化することを許可するために、**route-map** コマンドと **access-list** コマンドが使用されます。 しかし、同じユーザが他の場所にアクセスする際には、Port Address Translation（PAT; ポート アドレス変換）によりアドレス 172.17.63.230 に変換されます。

トラフィックがトンネルでは PAT を通過しないようにし、インターネットへのトラフィックは PAT を通過するようにするためには、PIX セキュリティ アプライアンスで次の設定コマンドが必要です。

```
access-list nonat permit ip 10.1.1.0 255.255.255.0 10.2.2.0 255.255.255.0 nat (inside) 0 access-list nonat nat (inside) 1 10.1.1.0 255.255.255.0 0 0
```

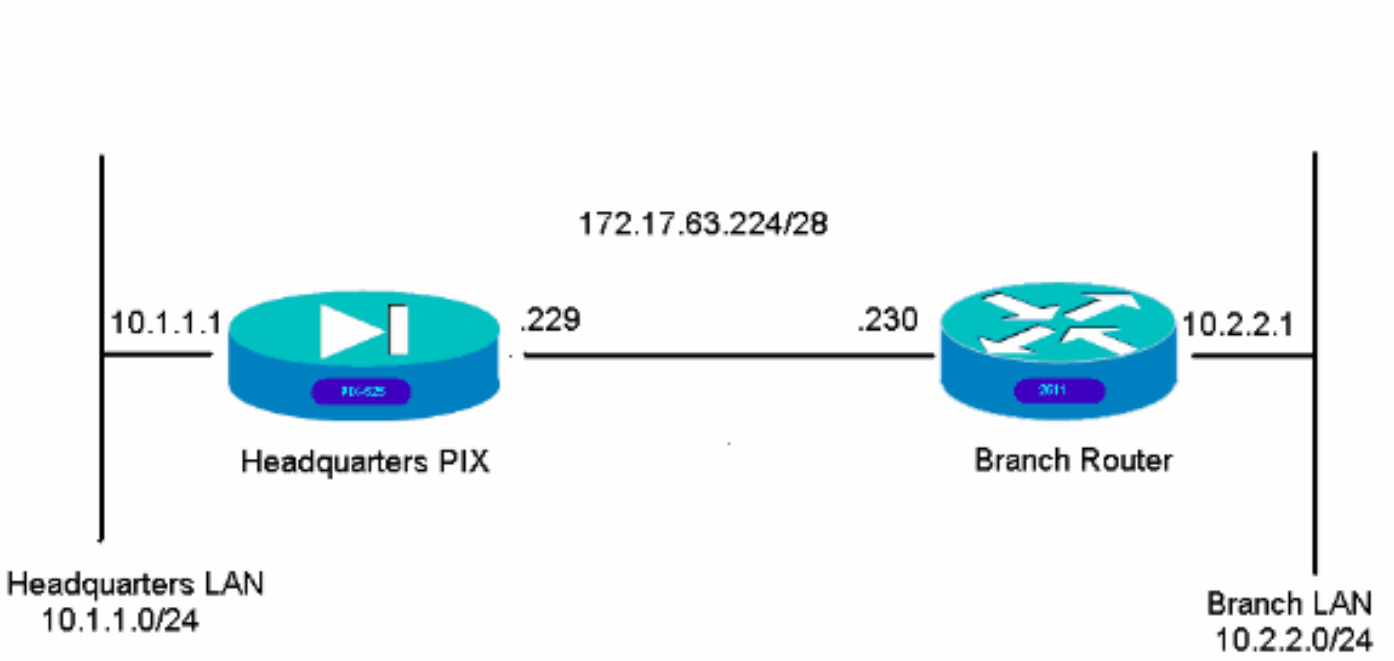
設定

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

これらの設定例は、コマンドライン インターフェイス用のものです。 ASDM を使用して設定する場合は、このドキュメントの「Adaptive Security Device Manager（ASDM）を使用した設定」を参照してください。

- 本社の PIX
- ブランチ ルータ

本社の PIX

```
HQPIX(config)#show run PIX Version 7.0(0)102 names !
interface Ethernet0 description WAN interface nameif
outside security-level 0 ip address 172.17.63.229
255.255.255.240 ! interface Ethernet1 nameif inside
security-level 100 ip address 10.1.1.1 255.255.255.0 !
interface Ethernet2 shutdown no nameif no security-level
no ip address ! interface Ethernet3 shutdown no nameif
no security-level no ip address ! interface Ethernet4
shutdown no nameif no security-level no ip address !
interface Ethernet5 shutdown no nameif no security-level
no ip address ! enable password 8Ry2YjIyt7RRXU24
encrypted passwd 2KFQnbNIdI.2KYOU encrypted hostname
HQPIX domain-name cisco.com ftp mode passive clock
```

timezone AEST 10 **access-list Ipsec-conn extended permit ip 10.1.1.0 255.255.255.0 10.2.2.0 255.255.255.0 access-list nonat extended permit ip 10.1.1.0 255.255.255.0 10.2.2.0 255.255.255.0** pager lines 24 logging enable logging buffered debugging mtu inside 1500 mtu outside 1500 no failover monitor-interface inside monitor-interface outside asdm image flash:/asdmfile.50073 no asdm history enable arp timeout 14400 **nat-control global (outside) 1 interface nat (inside) 0 access-list nonat nat (inside) 1 10.1.1.0 255.255.255.0 access-group 100 in interface inside** route outside 0.0.0.0 0.0.0.0 172.17.63.230 1 timeout xlate 3:00:00 timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02 sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 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 partner protocol tacacs+ **username cisco password 3USUcOPFUiMCO4Jk encrypted http server enable http 10.1.1.2 255.255.255.255 inside** no snmp-server location no snmp-server contact snmp-server community public snmp-server enable traps snmp **crypto ipsec transform-set avalanche esp-des esp-md5-hmac crypto ipsec security-association lifetime seconds 3600 crypto ipsec df-bit clear-df outside crypto map forsberg 21 match address Ipsec-conn crypto map forsberg 21 set peer 172.17.63.230 crypto map forsberg 21 set transform-set avalanche crypto map forsberg interface outside** isakmp identity address **isakmp enable outside isakmp policy 1 authentication pre-share isakmp policy 1 encryption 3des isakmp policy 1 hash sha isakmp policy 1 group 2** isakmp policy 1 lifetime 86400 isakmp policy 65535 authentication pre-share isakmp policy 65535 encryption 3des isakmp policy 65535 hash sha isakmp policy 65535 group 2 isakmp policy 65535 lifetime 86400 telnet timeout 5 ssh timeout 5 console timeout 0 **tunnel-group 172.17.63.230 type ipsec-l2l tunnel-group 172.17.63.230 ipsec-attributes pre-shared-key *** ! class-map inspection_default match default-inspection-traffic ! ! policy-map asa_global_fw_policy class inspection_default inspect dns maximum-length 512 inspect ftp inspect h323 h225 inspect h323 ras inspect netbios inspect rsh inspect rtsp inspect skinny inspect esmtp inspect sqlnet inspect sunrpc inspect tftp inspect sip inspect xdmcp inspect http ! service-policy asa_global_fw_policy global Cryptochecksum:3a5851f7310d14e82bdf17e64d638738 : end SV-2-8#

ブランチ ルータ

BranchRouter#**show run** Building configuration... Current configuration : 1719 bytes ! ! Last configuration change at 13:03:25 AEST Tue Apr 5 2005 ! NVRAM config last updated at 13:03:44 AEST Tue Apr 5 2005 ! version 12.2 service timestamps debug datetime msec service timestamps log uptime no service password-encryption ! hostname BranchRouter ! logging queue-limit 100 logging buffered 4096 debugging ! username cisco privilege 15 password 0 cisco memory-size iomem 15 clock timezone AEST 10 ip subnet-zero ! ! ! ip audit notify log ip audit po max-events 100 ! ! ! **crypto isakmp policy 11 encr 3des authentication pre-share group 2 crypto isakmp key cisco123 address 172.17.63.229** ! ! **crypto ipsec transform-set sharks esp-des esp-md5-hmac** ! **crypto map nolan 11 ipsec-isakmp set peer 172.17.63.229 set**

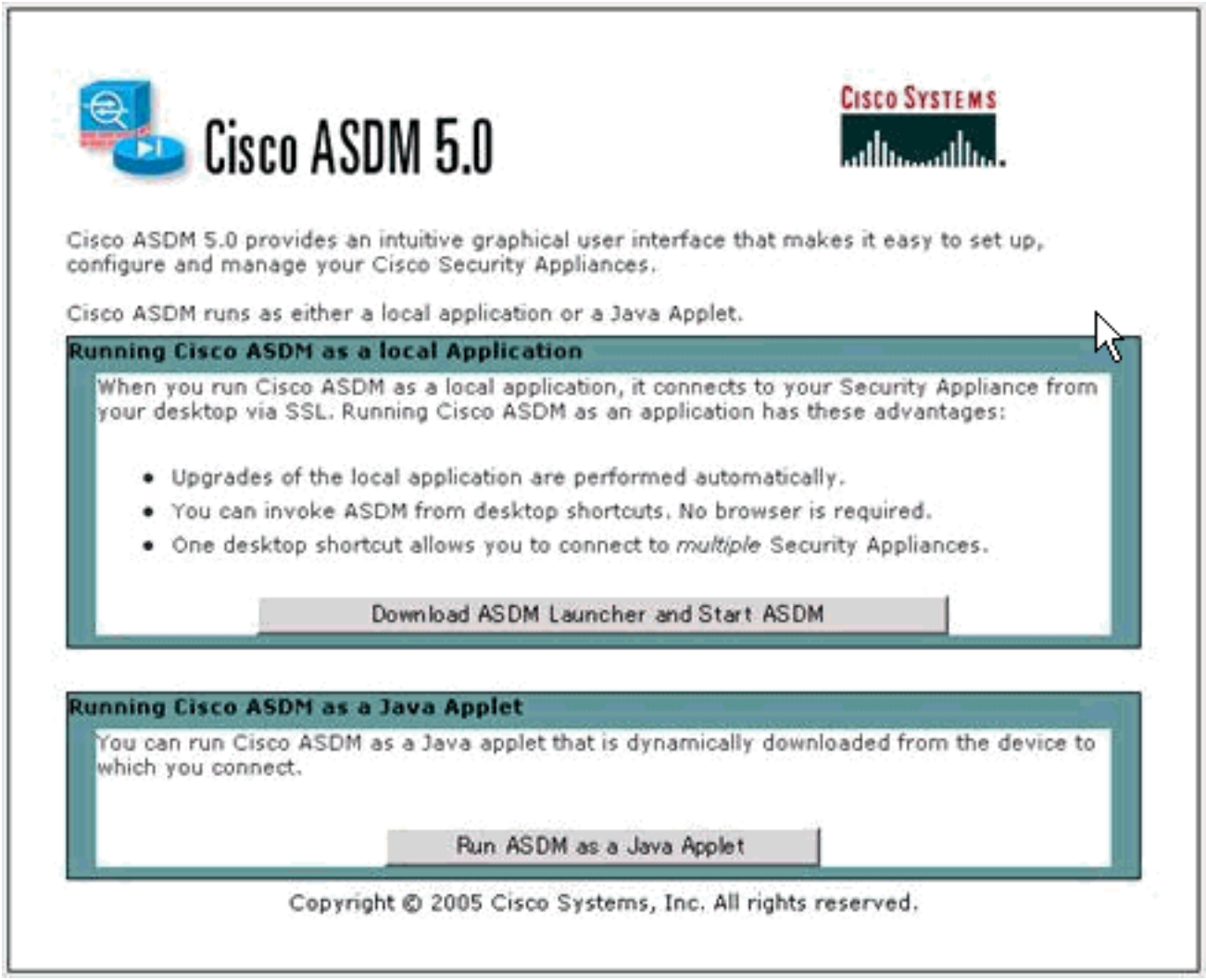
```
transform-set sharks match address 120 ! ! ! ! ! ! ! ! !
! no voice hpi capture buffer no voice hpi capture
destination ! ! mta receive maximum-recipients 0 ! ! ! !
interface Ethernet0/0 ip address 172.17.63.230
255.255.255.240 ip nat outside no ip route-cache no ip
mroute-cache half-duplex crypto map nolan ! interface
Ethernet0/1 ip address 10.2.2.1 255.255.255.0 ip nat
inside half-duplex ! ip nat pool branch 172.17.63.230
172.17.63.230 netmask 255.255.255.0 ip nat inside source
route-map nonat pool branch overload no ip http server
no ip http secure-server ip classless ip route 10.1.1.0
255.255.255.0 172.17.63.229 ! ! ! access-list 120 permit
ip 10.2.2.0 0.0.0.255 10.1.1.0 0.0.0.255 access-list 130
deny ip 10.2.2.0 0.0.0.255 10.1.1.0 0.0.0.255 access-
list 130 permit ip 10.2.2.0 0.0.0.255 any ! route-map
nonat permit 10 match ip address 130 ! call rsvp-sync !
! mgcp profile default ! dial-peer cor custom ! ! ! ! !
line con 0 line aux 0 line vty 0 4 login ! ! end
```

ASDM を使用した設定

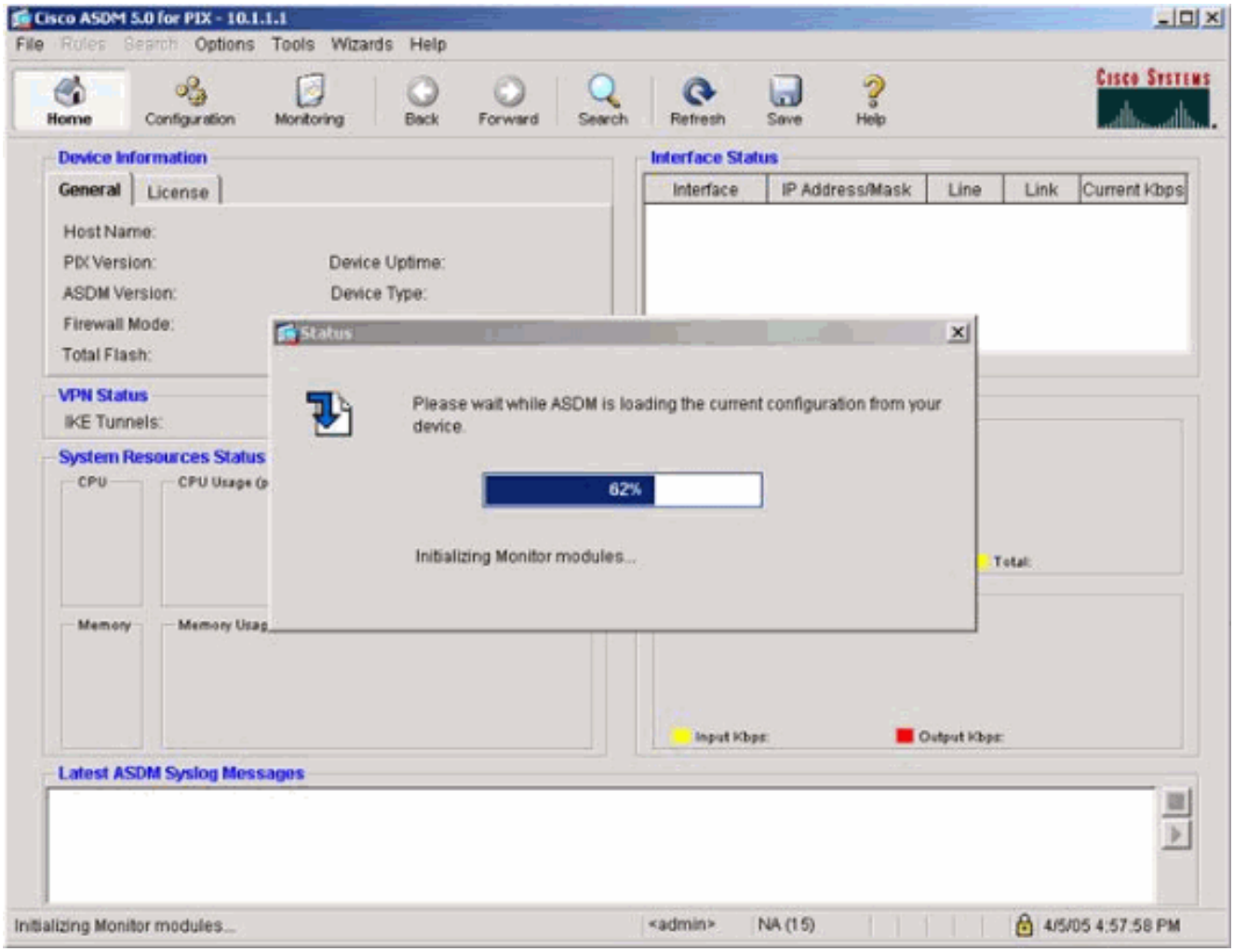
この例では、ASDM GUI を使用した PIX の設定方法を示します。 ブラウザを搭載し、IP アドレスが 10.1.1.2 である PC が、PIX の内部インターフェイス e1 に接続されています。 PIX で http が有効であることを確認します。

この手順は、本社の PIX の ASDM 設定を示しています。

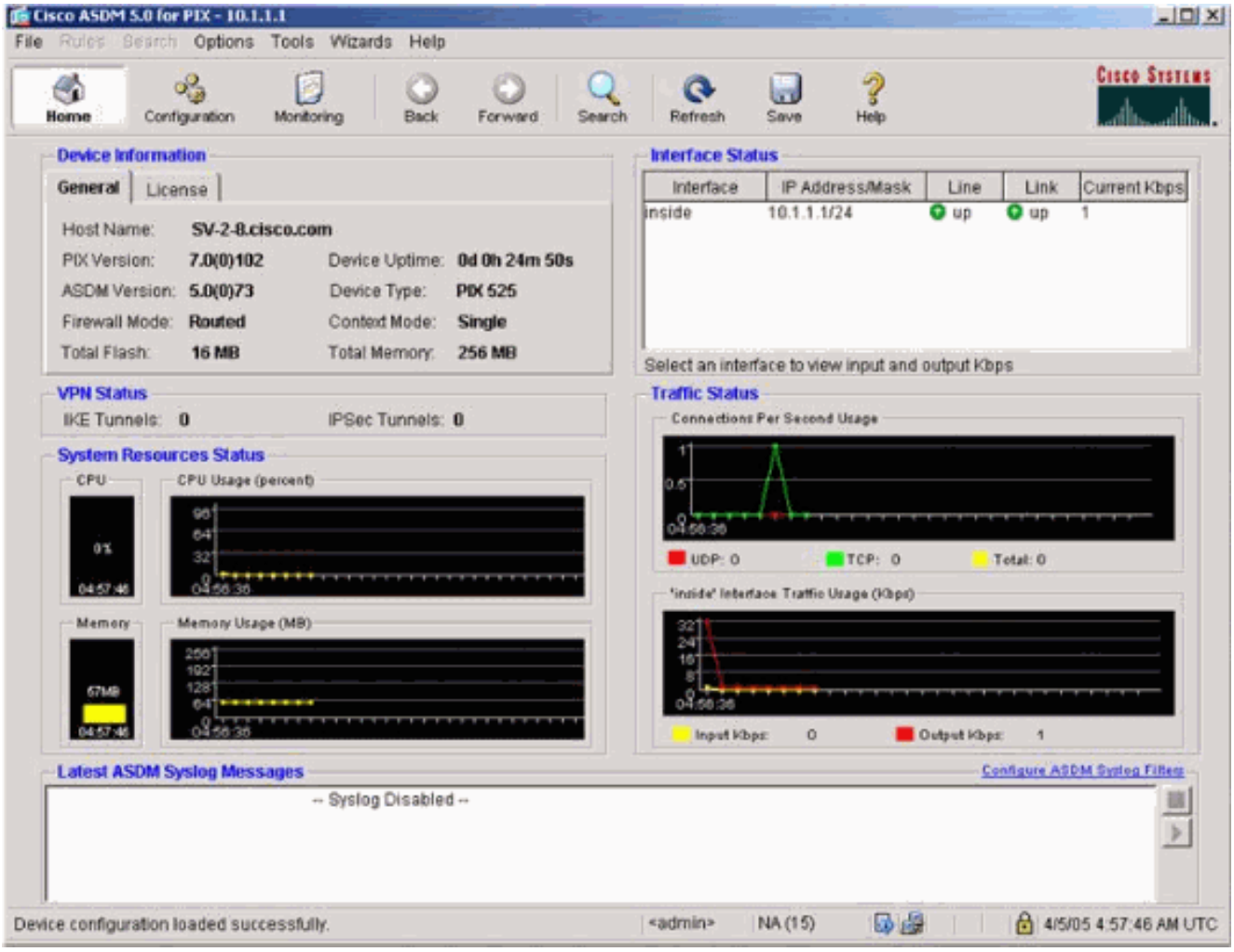
1. PC を PIX に接続し、ダウンロード方式を選択します。



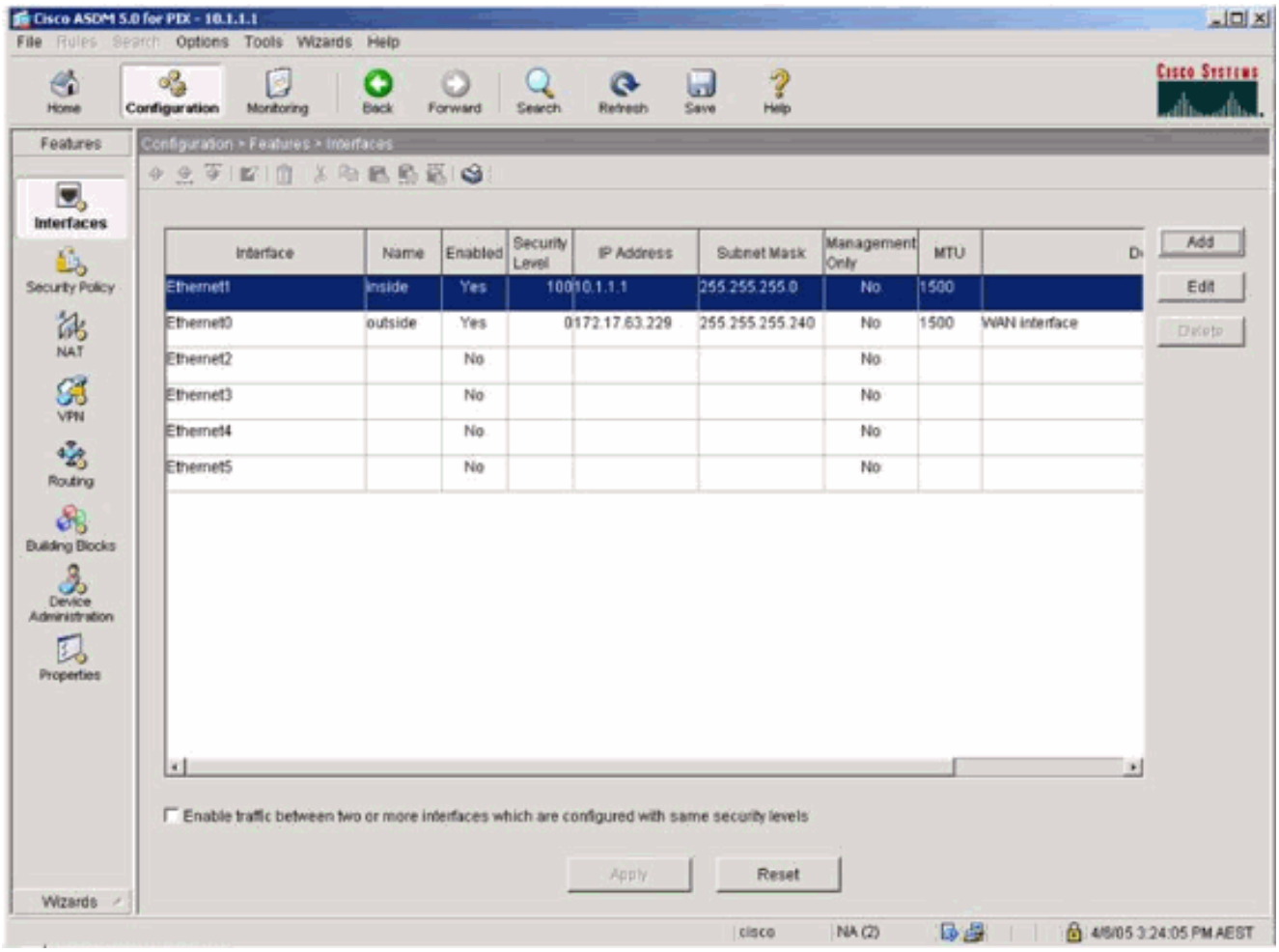
ASDM は、PIX から既存の設定をロードします。



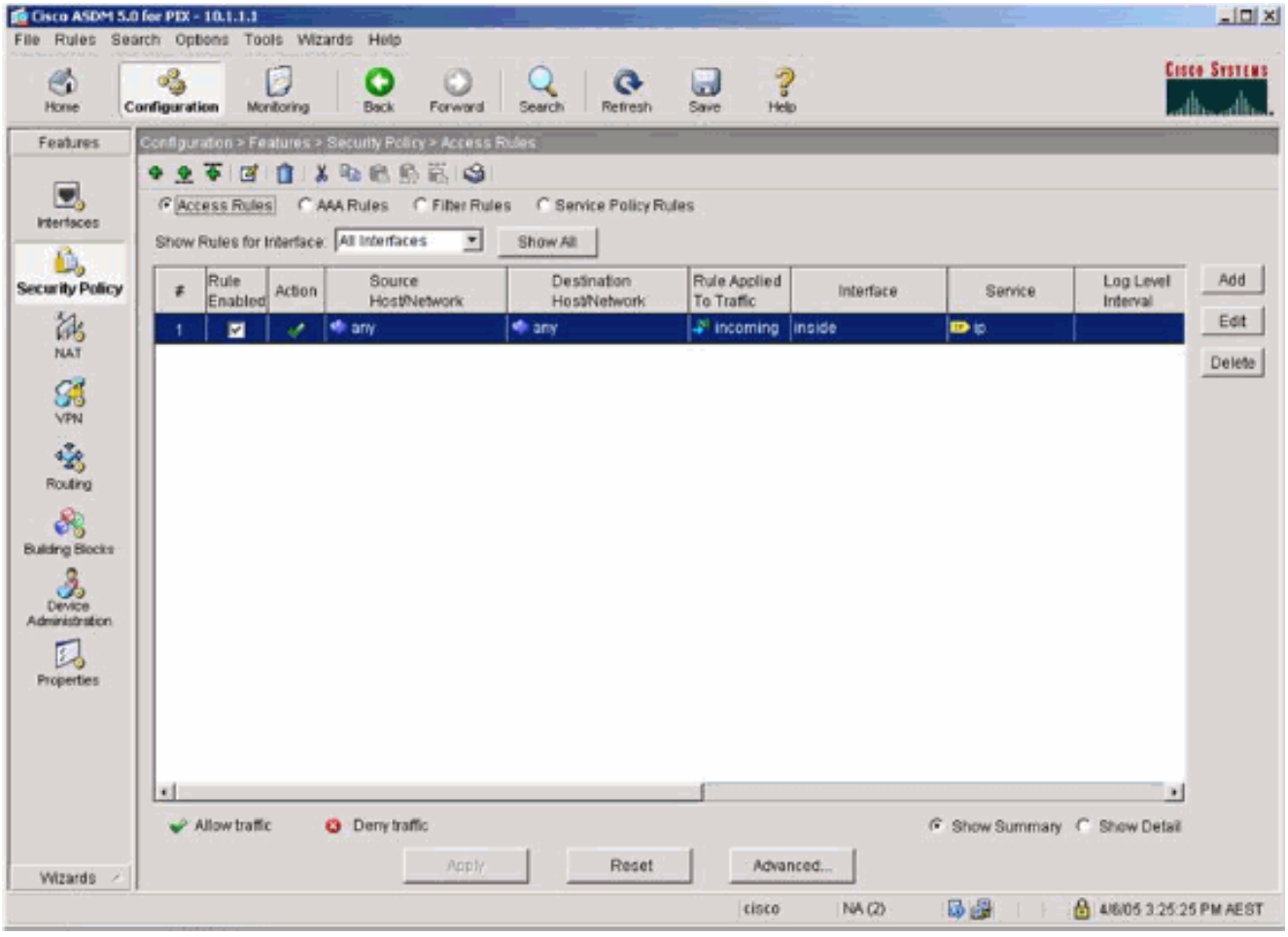
次のウィンドウでは、監視ツールとメニューが示されます。



2. [Configuration] > [Features] > [Interfaces] の順に選択して、新しいインターフェイスの場合は [Add] を、既存の設定の場合は [Edit] を選択します。

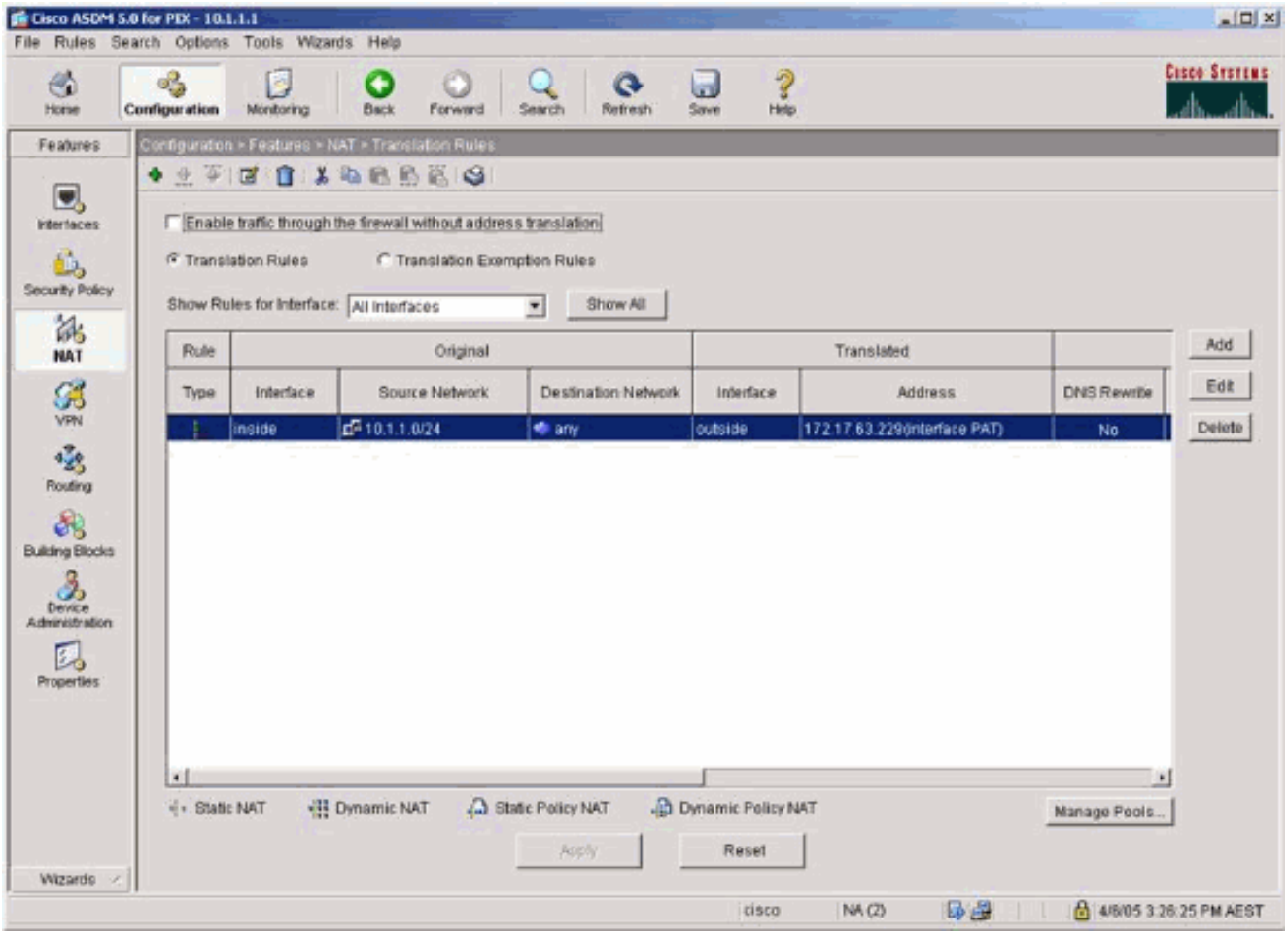


3. 内部インターフェイスのセキュリティ オプションを選択します。

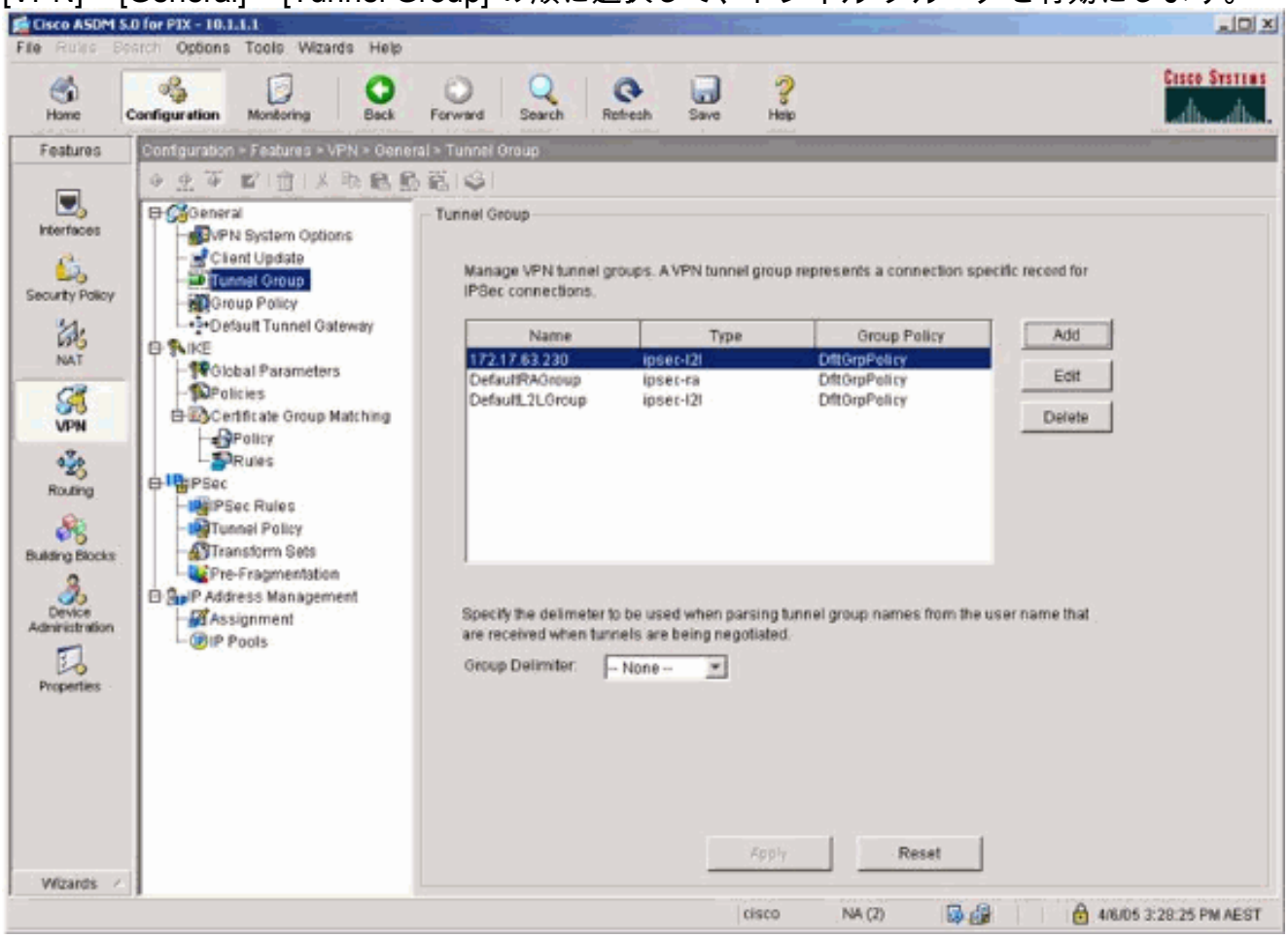


4. NAT 設定では、暗号化されたトラフィックは NAT の対象外になり、それ以外のすべてのト

ラフィックは外部インターフェイスに対しては NAT/PAT の対象です。

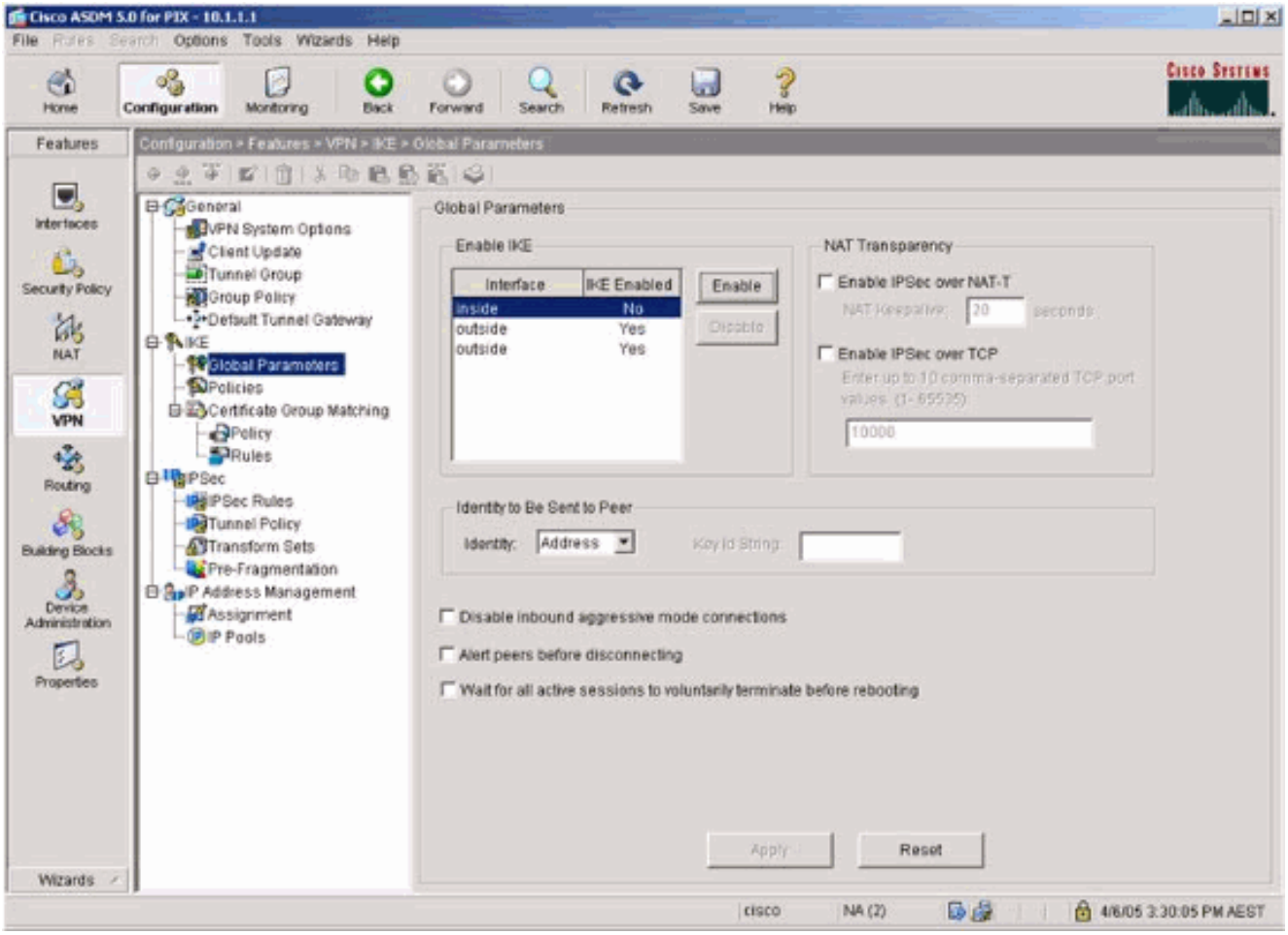


5. [VPN] > [General] > [Tunnel Group] の順に選択して、トンネル グループを有効にします。

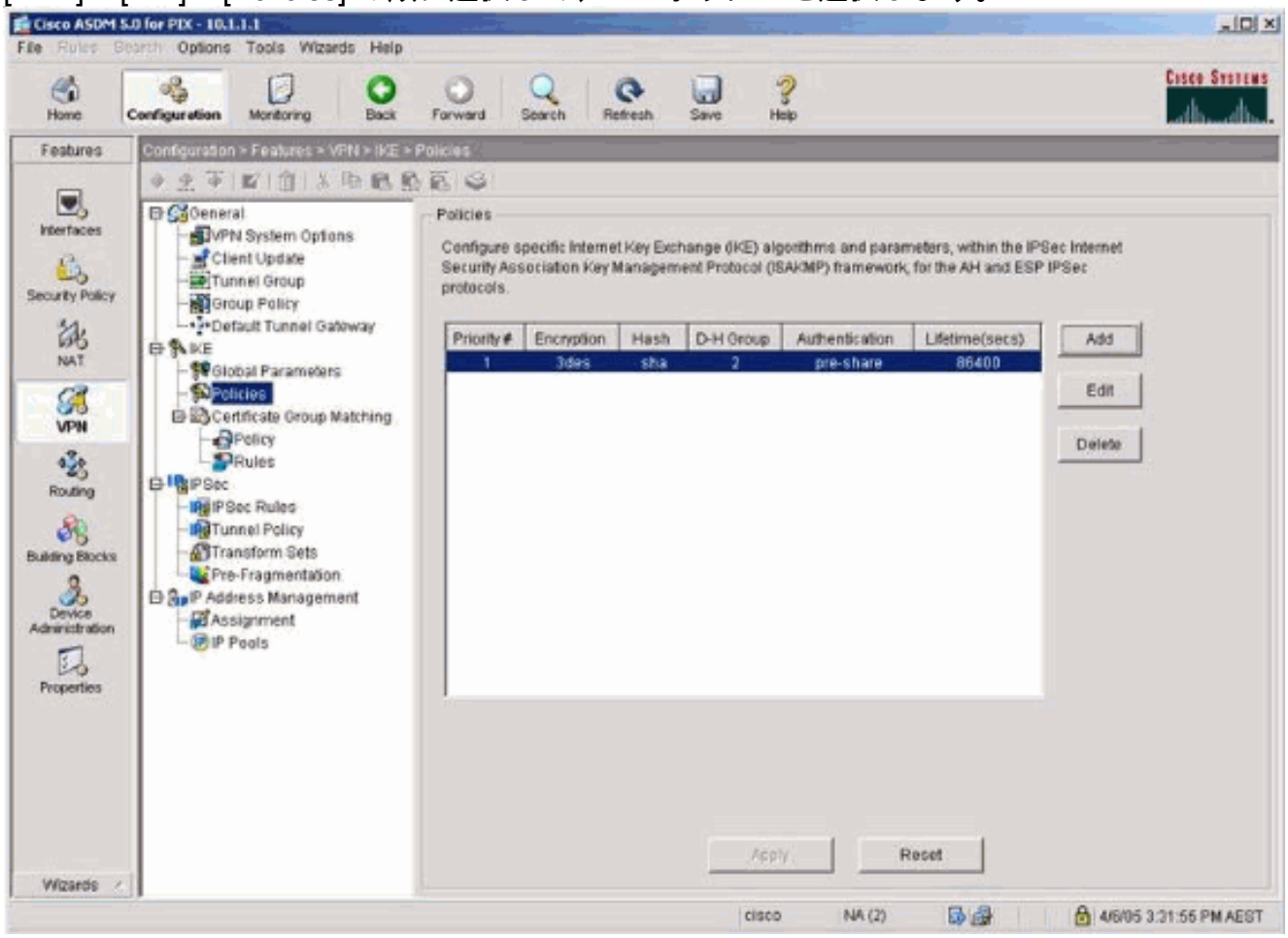


6. [VPN] > [IKE] > [Global Parameters] の順に選択して、外部インターフェイス上で IKE を有

効にします。

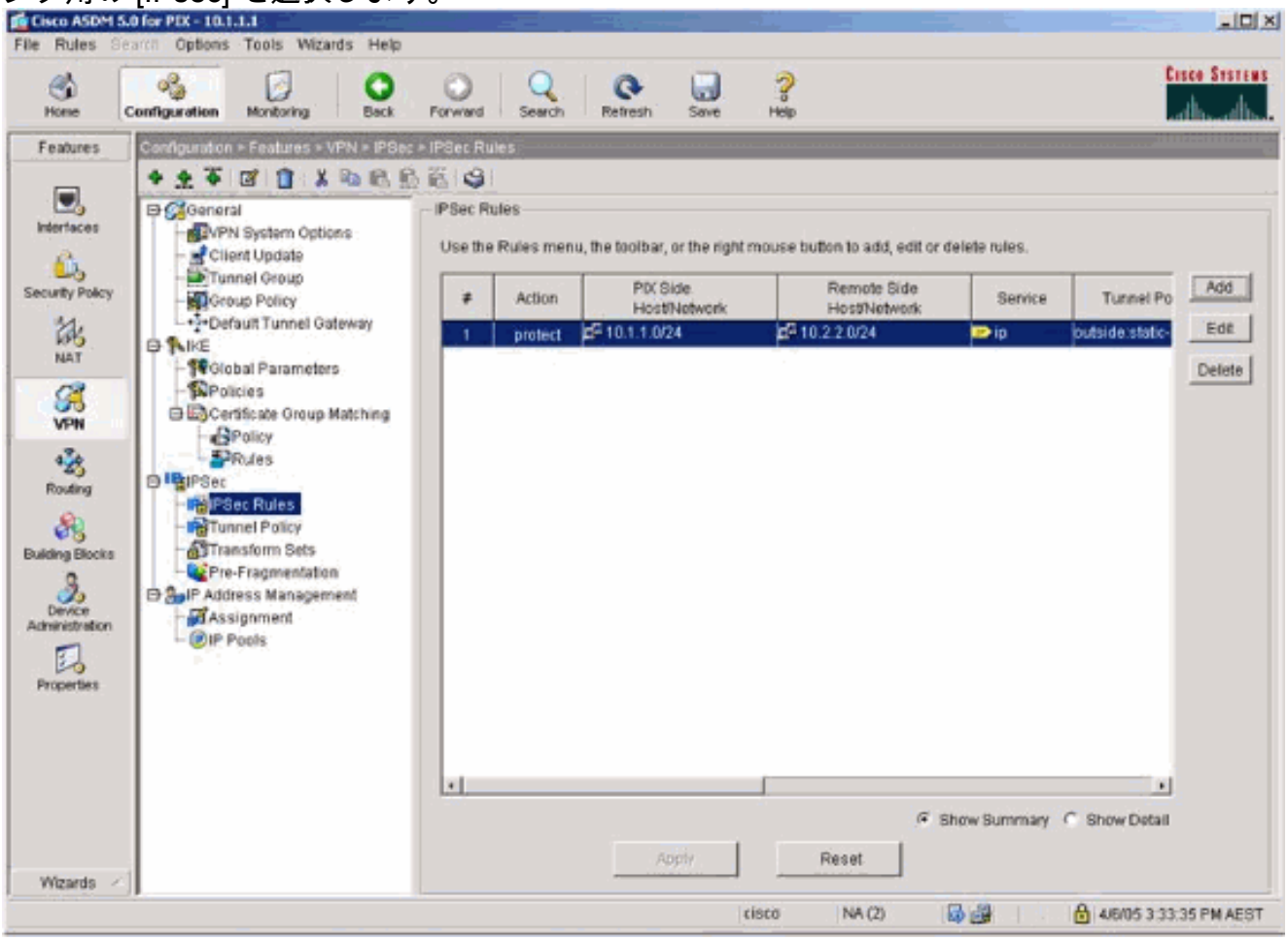


7. [VPN] > [IKE] > [Policies] の順に選択して、IKE ポリシーを選択します。

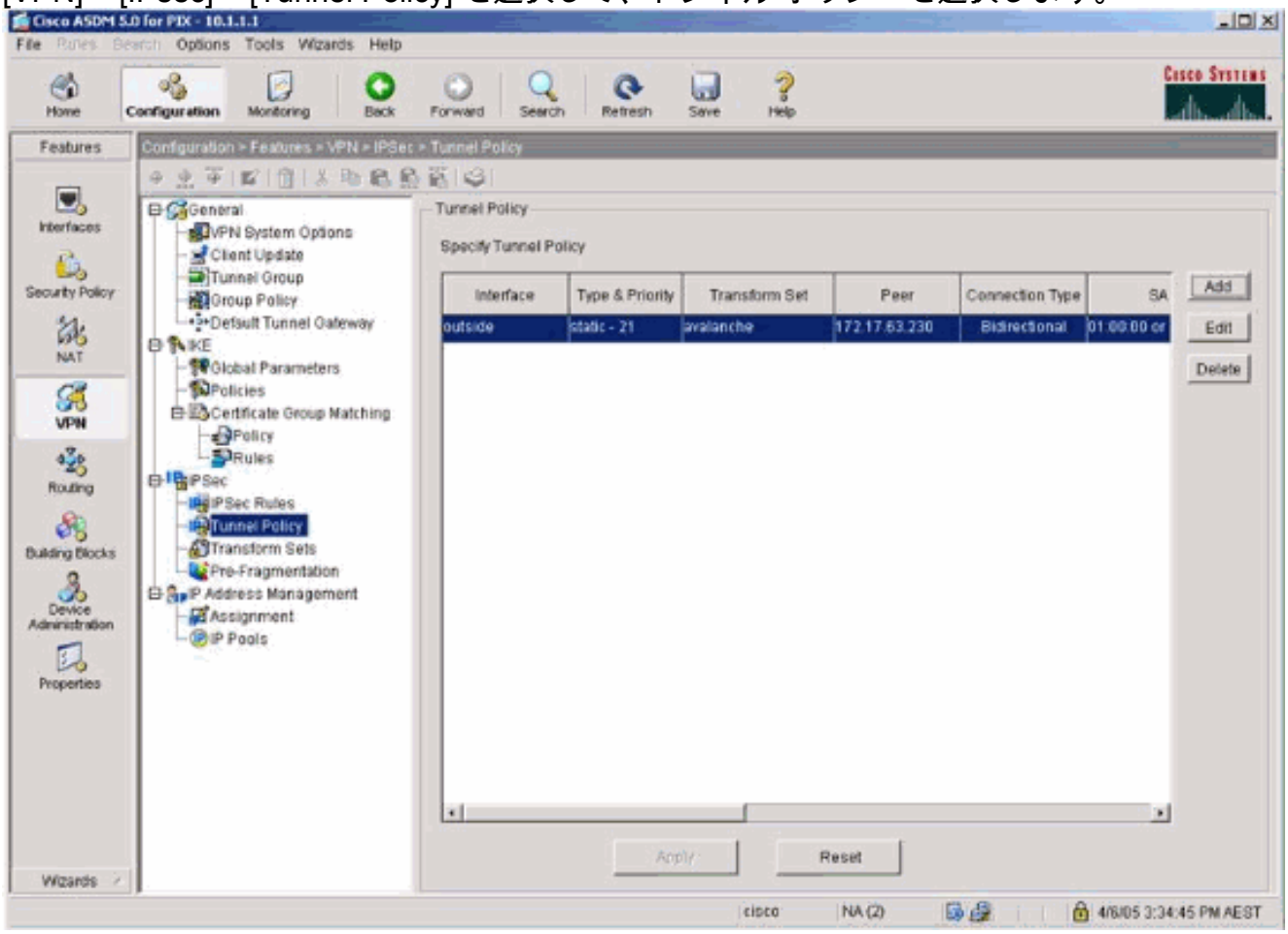


8. [VPN] > [IPsec] > [IPsec Rules] の順に選択して、ローカル トンネルとリモート アドレッシ

ング用の [IPsec] を選択します。

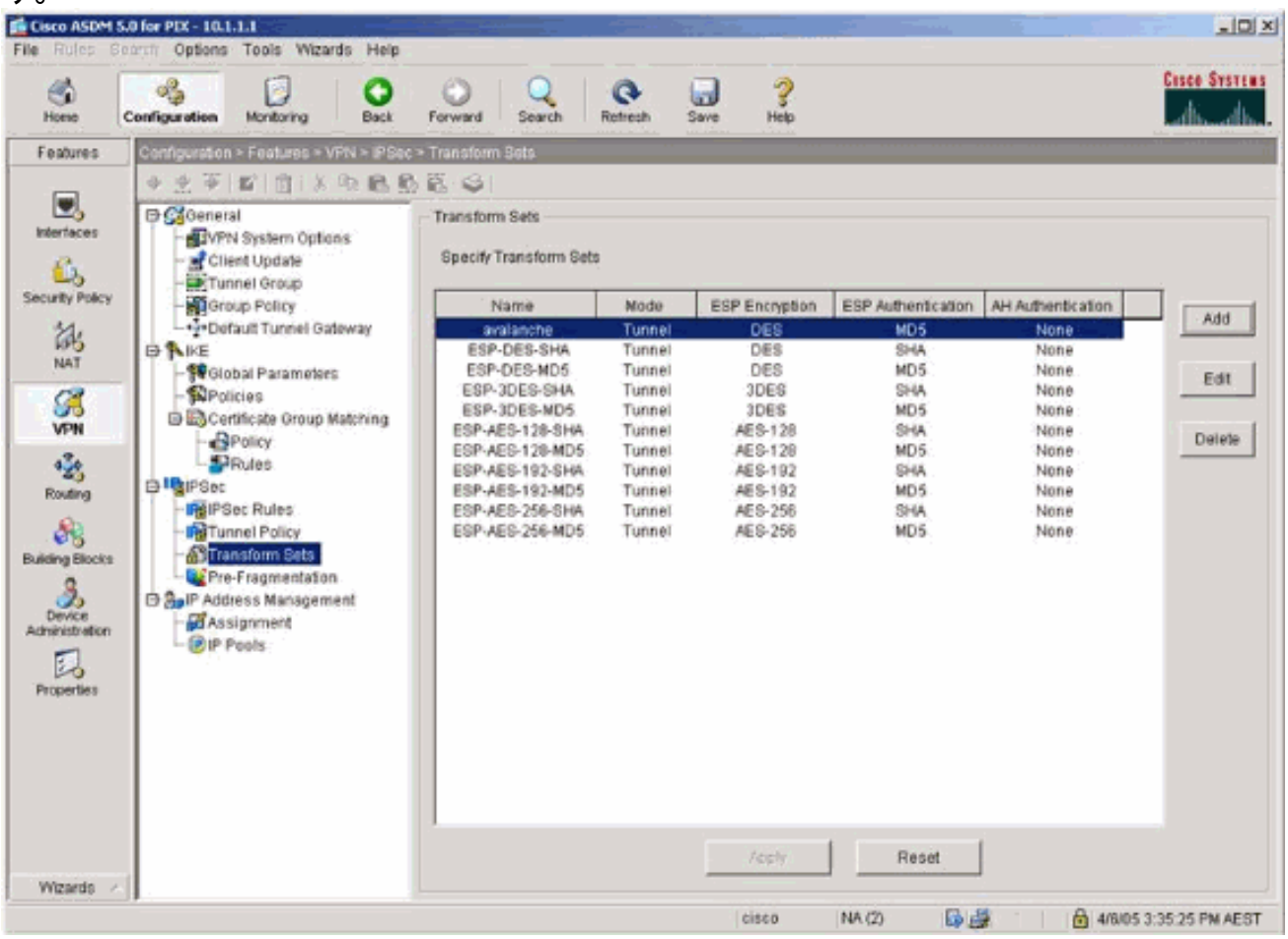


9. [VPN] > [IPsec] > [Tunnel Policy] を選択して、トンネル ポリシーを選択します。

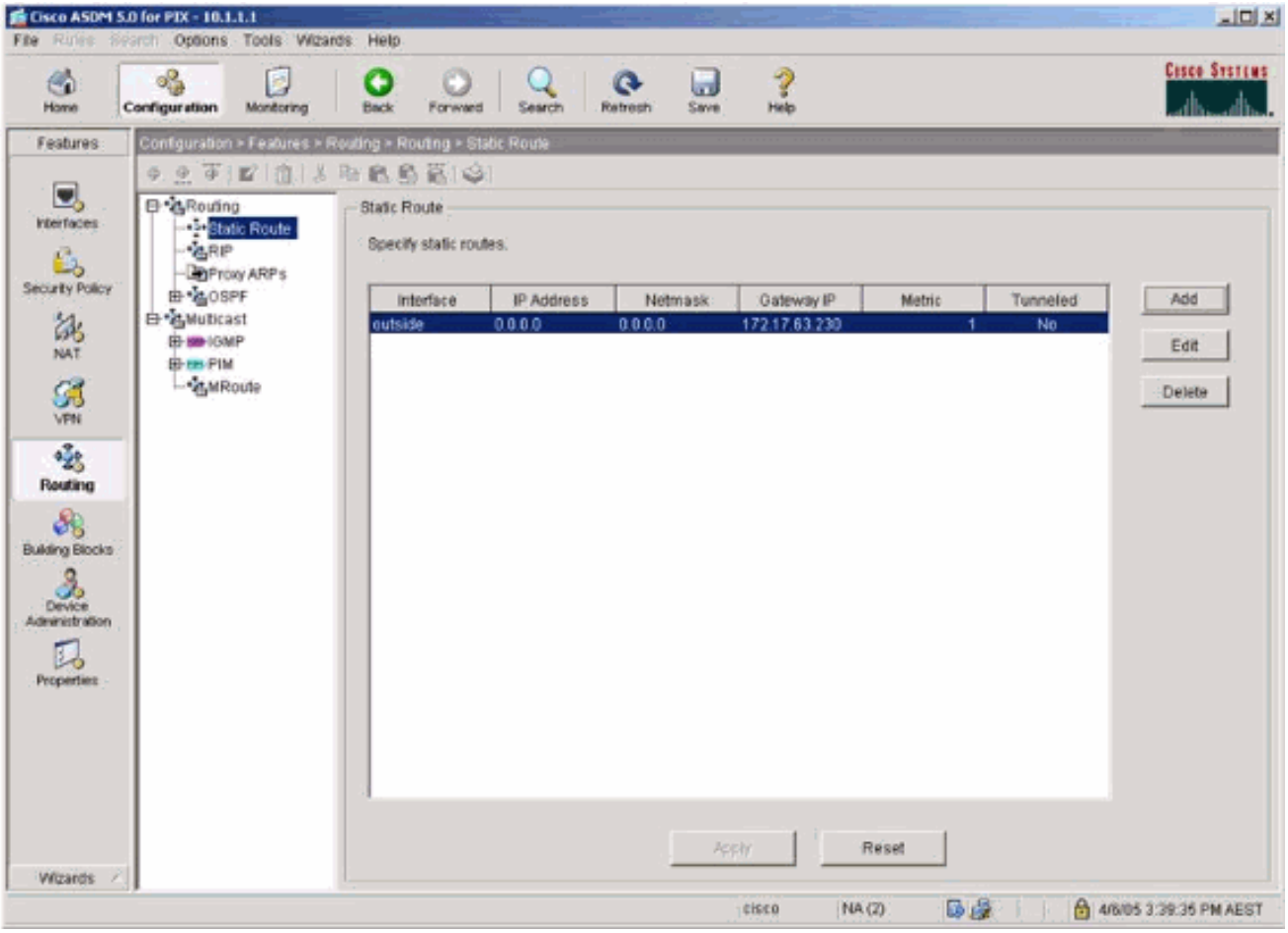


10. [VPN] > [IPsec] > [Transform Sets] の順に選択して、トランスフォーム セットを選択しま

す。



11. [Routing] > [Routing] > [Static Route] の順に選択して、ゲートウェイ ルータへのスタティック ルートを選択します。 この例では、簡単にするため、スタティック ルートはリモート VPN ピアを指します。



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。

トラブルシューティング

ASDM を使用すると、ロギングを有効にしてログを表示できます。

- [Configuration] > [Properties] > [Logging] > [Logging Setup]の順に選択して、[Enable Logging] を選択し、[Apply] をクリックしてロギングを有効にします。
- [Monitoring] > [Logging] > [Log Buffer] > [On Logging Level] の順に選択して、[Logging Buffer] を選択し、[View] をクリックしてログを表示します。

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。

- **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表示します。
- **debug crypto engine**：暗号化されたトラフィックを表示します。
- **clear crypto isakmp**：フェーズ 1 に関連したセキュリティ アソシエーションをクリアします。
- **clear crypto sa**：フェーズ 2 に関連したセキュリティ アソシエーションをクリアします。
- **debug icmp trace**：ホストからの ICMP 要求が PIX に到達するかどうかを示します。 このデバッグを実行するには、**access-list** コマンドを設定に追加して、ICMP を許可する必要があります。
- **logging buffer debugging**：PIX を通過する、ホストへの確立された接続と拒否された接続を表示します。 情報は PIX ログ バッファに保存され、**show log** コマンドで出力を表示できます。

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
- セキュリティ製品に関する Field Notice（PIX を含む）
- Requests for Comments（RFC）
- テクニカルサポートとドキュメント - Cisco Systems