

PIX/ASA (バージョン 7.x 以降) ネットワーク アドレス変換を使用した IPsec VPN 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](#)

[関連製品](#)

[設定](#)

[ネットワーク図](#)

[設定](#)

[PIX セキュリティ アプライアンスとアクセスリストの設定](#)

[PIX セキュリティ アプライアンスおよび MPF \(モジュラ ポリシー フレームワーク\) の設定](#)

[確認](#)

[トラブルシューティング](#)

[ルータ IPsec のトラブルシューティング コマンド](#)

[セキュリティ アソシエーションのクリア](#)

[PIX のトラブルシューティング コマンド](#)

[関連情報](#)

概要

この設定例では、ネットワーク アドレス変換 (NAT) を実行するファイアウォール経由の IPsec VPN トンネルを示します。Cisco IOS® ソフトウェアの 12.2(13)T より前のリリースを使用している場合、この設定はポート アドレス変換 (PAT) では動作しません。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。総称ルーティング カプセル化 (GRE) トンネリングの方が適しています。この例で、Cisco 2621 ルータおよび 3660 ルータは 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 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またはアクセス コントロール リスト (ACL) 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 の動作と設定についての詳細は、『[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](#)』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 デバイスが PAT で動作するかどうかを判断するには、ベンダーにお問い合わせください。また、Cisco IOS ソフトウェア リリース 12.2(13)T 以降では、PAT に対して NAT 透過機能を使用できます。詳細については、『[IPSec NAT 透過](#)』を参照してください。Cisco IOS ソフトウェア リリース 12.2(13)T 以降のこれらの機能についての詳細は、『[NAT を使用した IPSec ESP のサポート](#)』を参照してください。

注: Cisco テクニカル サポートでサービス 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 バージョン 6.x 以前の NAT を使用したファイアウォール経由の IPSec トンネルを設定する方法の詳細については、『[NAT を使用したファイアウォール経由の IPSec トンネルの設定](#)』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 (Cisco IOS ソフトウェア リリース 12.2(13)T より前) 最新の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 3660 ルータ
- 7.x 以降が稼働する Cisco PIX 500 シリーズ セキュリティ アプライアンス

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。

[関連製品](#)

このドキュメントは、ソフトウェア バージョン 7.x 以降を実行する Cisco 5500 シリーズ適応型 セキュリティ アプライアンス (ASA) でも使用できます。

[設定](#)

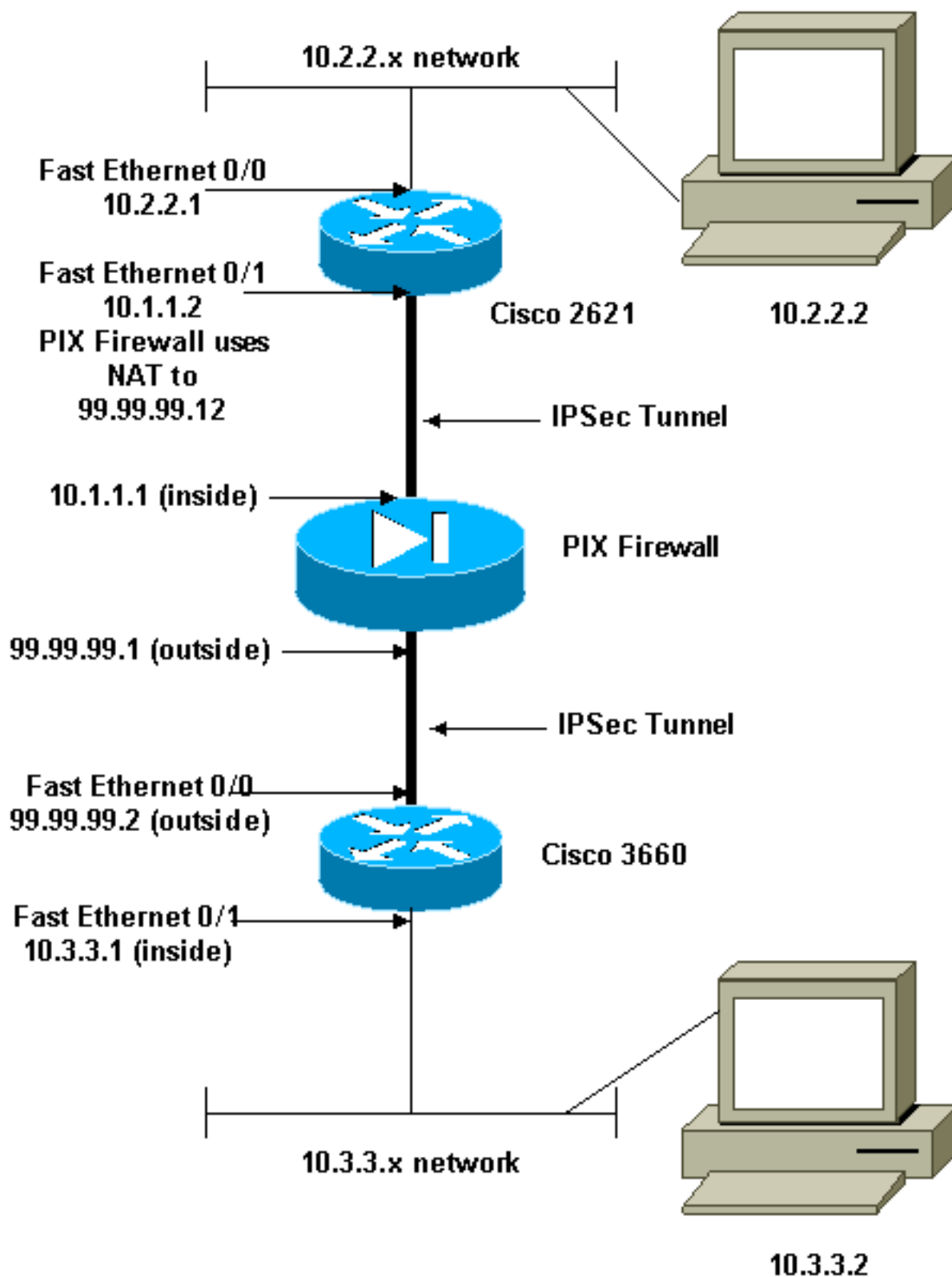
このセクションでは、このドキュメントで説明している機能の設定に使用するための情報を説明します。

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、[コマンド検索ツール](#) ([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。

- [Cisco 2621 の設定](#)
- [Cisco 3660 の設定](#)
- [PIX セキュリティ アプライアンスとアクセス リストの設定Advanced Security Device Manager GUI \(ASDM \) の設定コマンドライン インターフェイス \(CLI \) の設定](#)
- [PIX セキュリティ アプライアンスおよび MPF \(モジュラ ポリシー フレームワーク \) の設定](#)

Cisco 2621

```
Current configuration:
!
version 12.0
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
!
!--- The IKE policy. crypto isakmp policy 10 hash md5
authentication pre-share crypto isakmp key cisco123
address 99.99.99.2 ! 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 99.99.99.2 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 the 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 3660

```
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname goss-3660
!
ip subnet-zero
!
cns event-service server
!
!--- The IKE policy. crypto isakmp policy 10 hash md5
authentication pre-share crypto isakmp key cisco123
address 99.99.99.12 ! crypto ipsec transform-set myset
esp-des esp-md5-hmac ! crypto map mymap local-address
FastEthernet0/0 !--- The IPsec policy. crypto map mymap
```

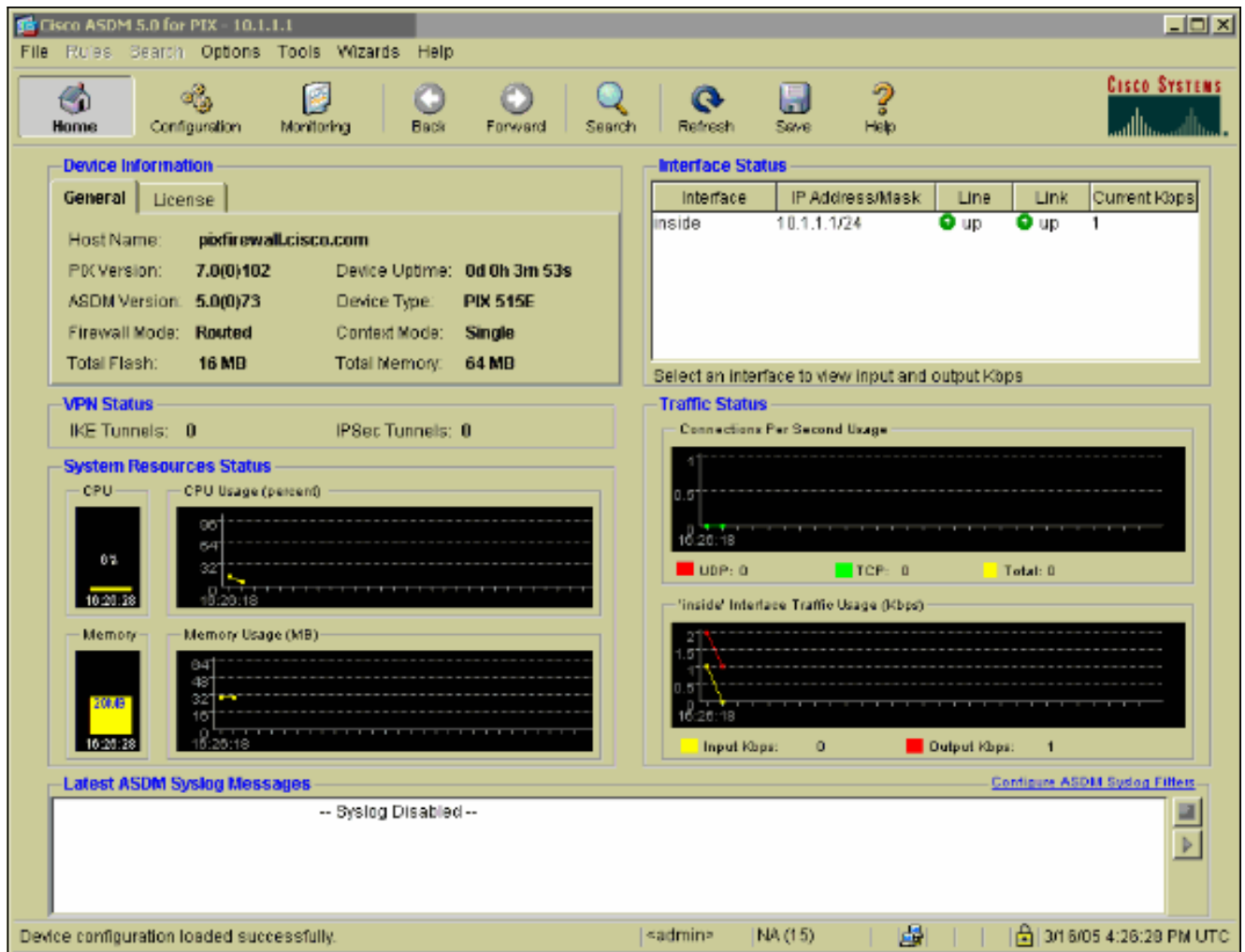
```
10 ipsec-isakmp set peer 99.99.99.12 set transform-set
myset !--- Include the private-network-to-private-
network traffic !--- in the encryption process. match
address 101 ! interface FastEthernet0/0 ip address
99.99.99.2 255.255.255.0 no ip directed-broadcast ip nat
outside duplex auto speed auto !--- Apply to the
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 ! !--- The pool from which inside hosts translate to
!--- the globally unique 99.99.99.0/24 network. ip nat
pool OUTSIDE 99.99.99.70 99.99.99.80 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 99.99.99.1
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
```

PIX セキュリティ アプライアンスとアクセス リストの設定

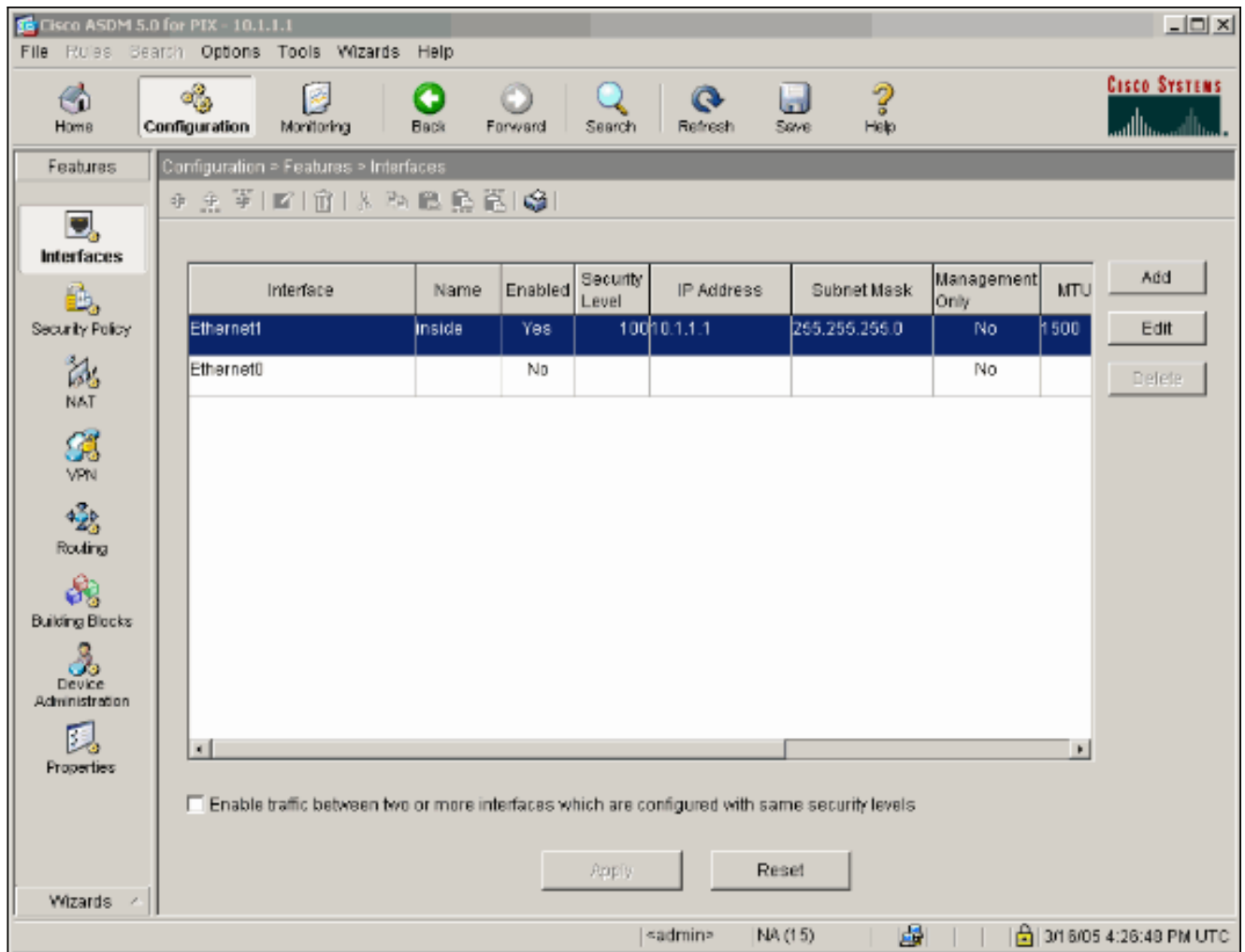
ASDM 5.0 の設定

ASDM を使用して PIX Firewall バージョン 7.0 を設定するには、次の手順を実行します。

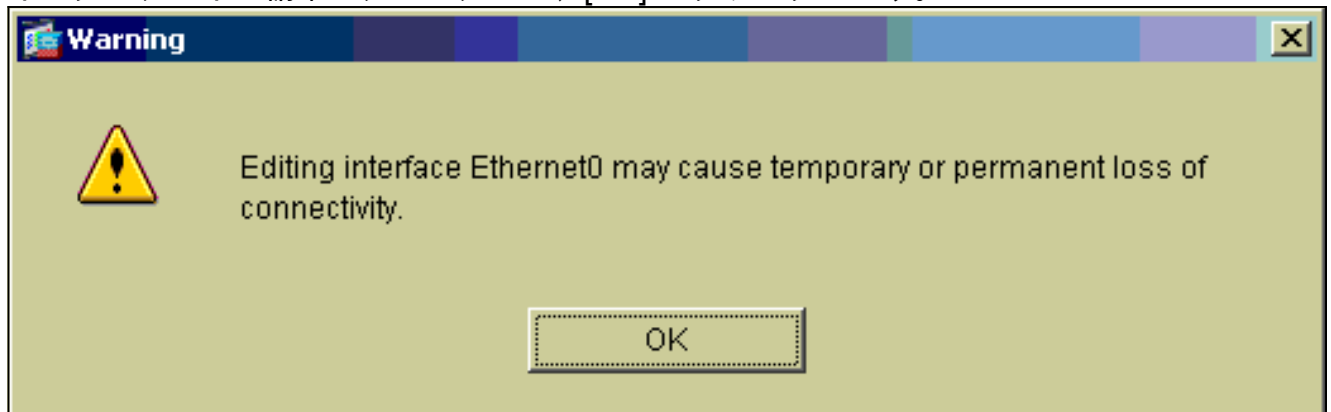
1. PIX にコンソール接続します。クリアな設定から、インタラクティブなプロンプトを使用して、Workstation 10.1.1.3 から **Advanced Security Device Manager GUI (ASDM)** で PIX を管理できるようにします。
2. Workstation 10.1.1.3 から、Web ブラウザを開いて、ASDM を使用します (この例では <https://10.1.1.1>)。
3. 認証のプロンプトで [Yes] を選択し、[PIX Firewall ASDM のブートストラップ構成](#) で設定されているイネーブル パスワードでログインします。
4. PC 上で初めて ASDM を実行する場合は、ASDM Launcher を使用するのかわ、それとも Java App として ASDM を使用するのかわを尋ねるプロンプトが出ます。この例では、ASDM Launcher が選択され、インストールされます。
5. [ASDM Home] ウィンドウに移動して、[Configuration] タブを選択します。



- イーサネット 0 インターフェイスを強調表示し、[Edit] をクリックして外部インターフェイスを設定します。



7. インターフェイス編集のプロンプトで、[OK] をクリックします。



8. インターフェイスの詳細を入力し、完了したら [OK] をクリックします。

Hardware Port: **Ethernet0** Configure Hardware Properties...

Enable Interface Dedicate this interface to management only

Interface Name:

Security Level:

IP Address

Use Static IP Obtain Address via DHCP

IP Address:


Subnet Mask:

MTU:

Description:

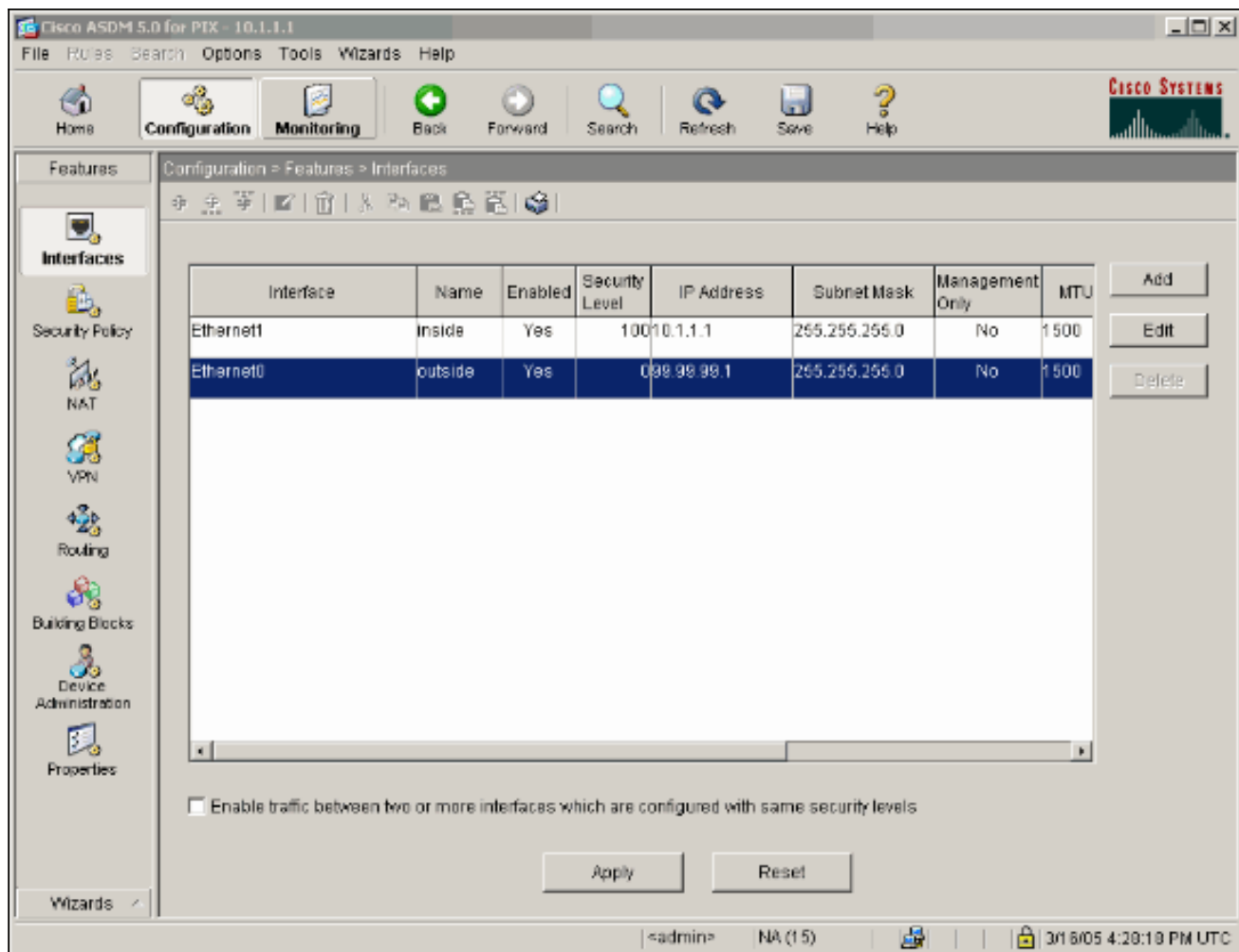
OK Cancel Help

9. インターフェイス変更のプロンプトで、[OK] をクリックします。

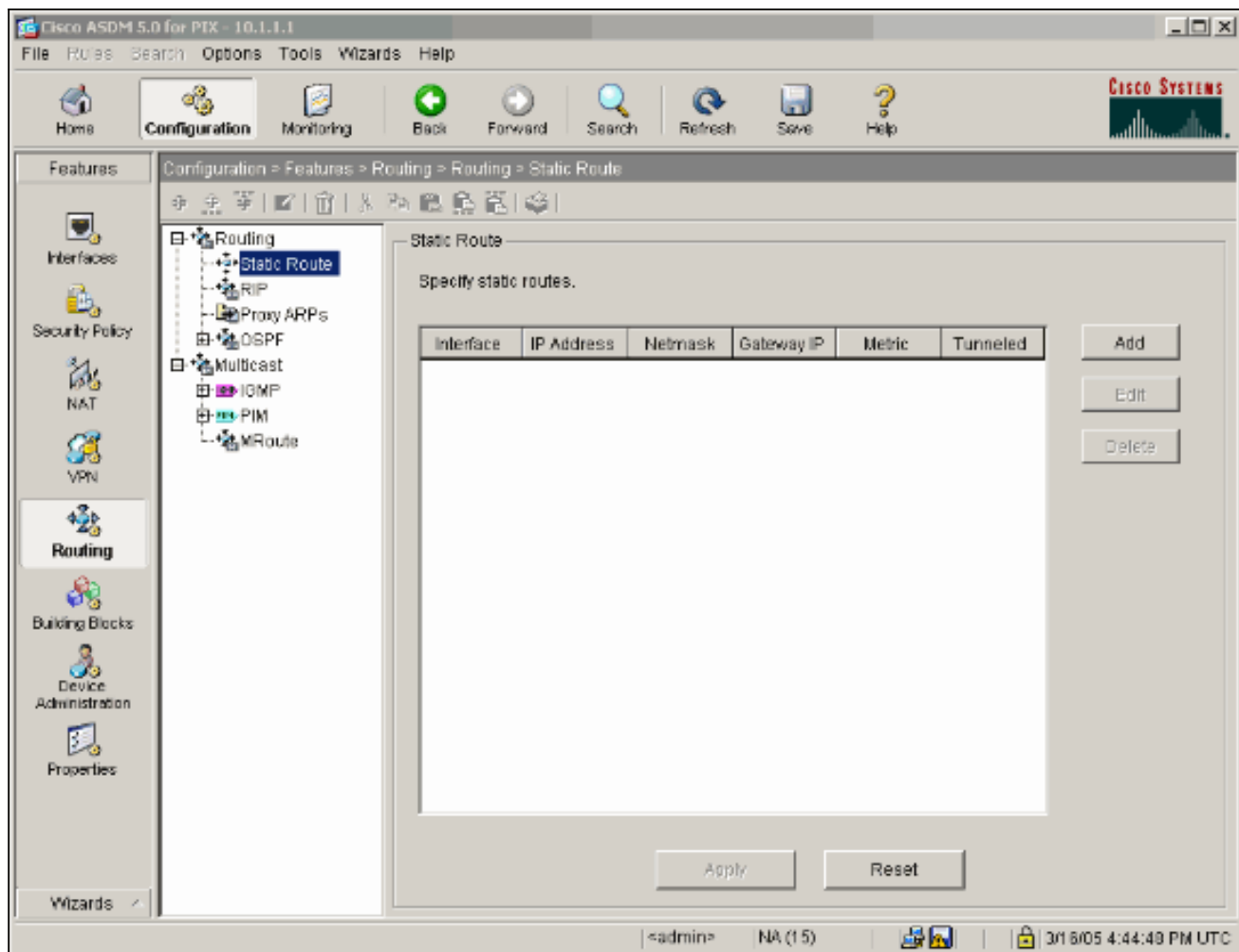
 Changing an interface's security level may cause your PIX configuration to become invalid, causing the PIX to drop legal traffic or allow illegal traffic to pass through. Do you still wish to proceed?

OK Cancel

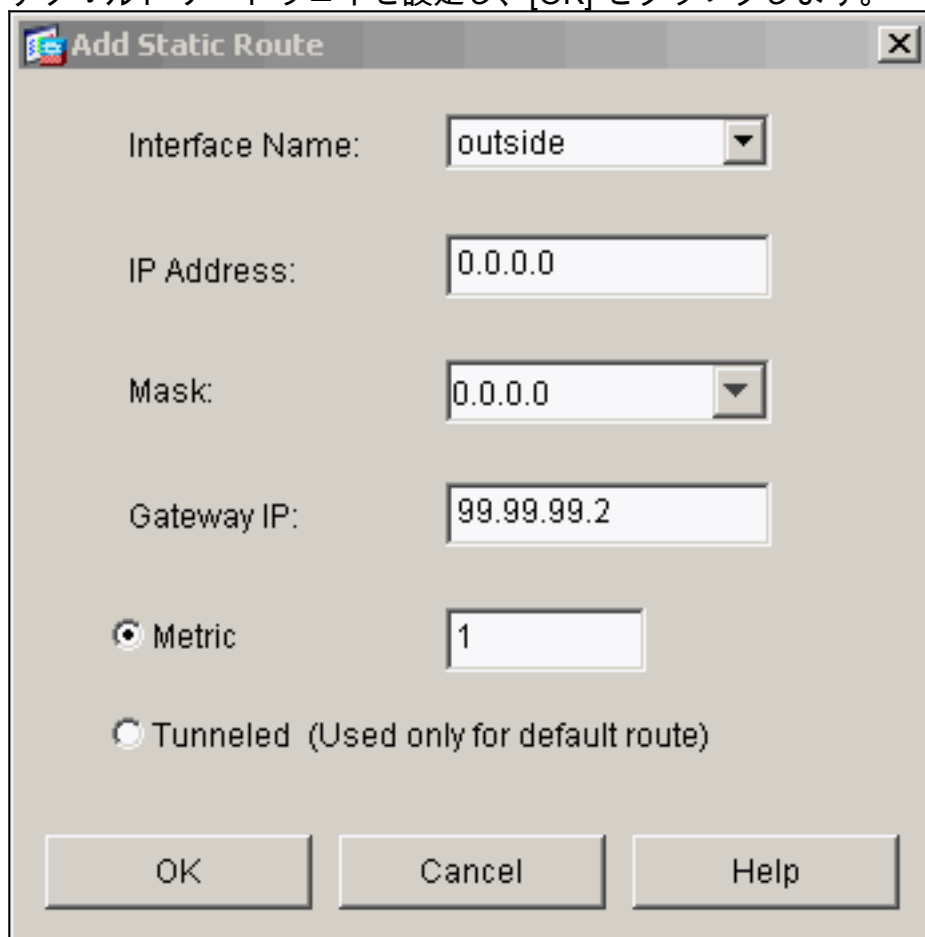
10. [Apply] をクリックして、インターフェイス設定を承認します。設定内容は PIX にもプッシュされます。この例ではスタティック ルートを使用します。



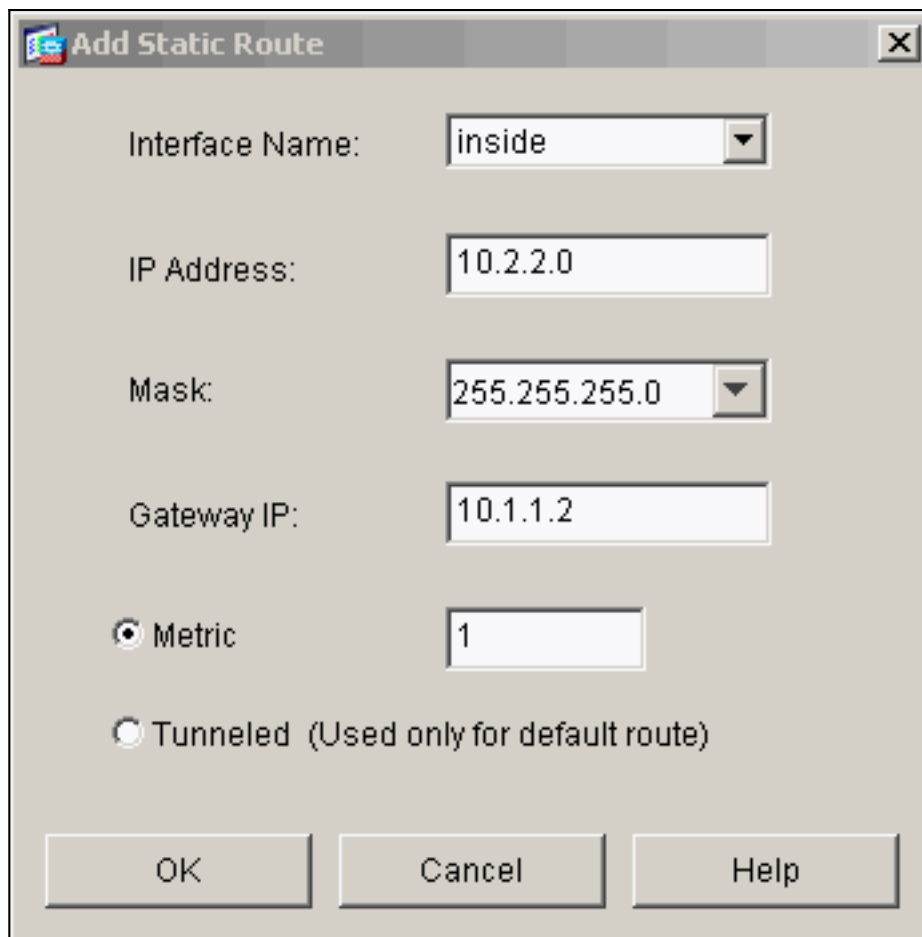
11. [Features] タブの下で [Routing] をクリックし、[Static Route] を強調表示し、[Add] をクリックします。



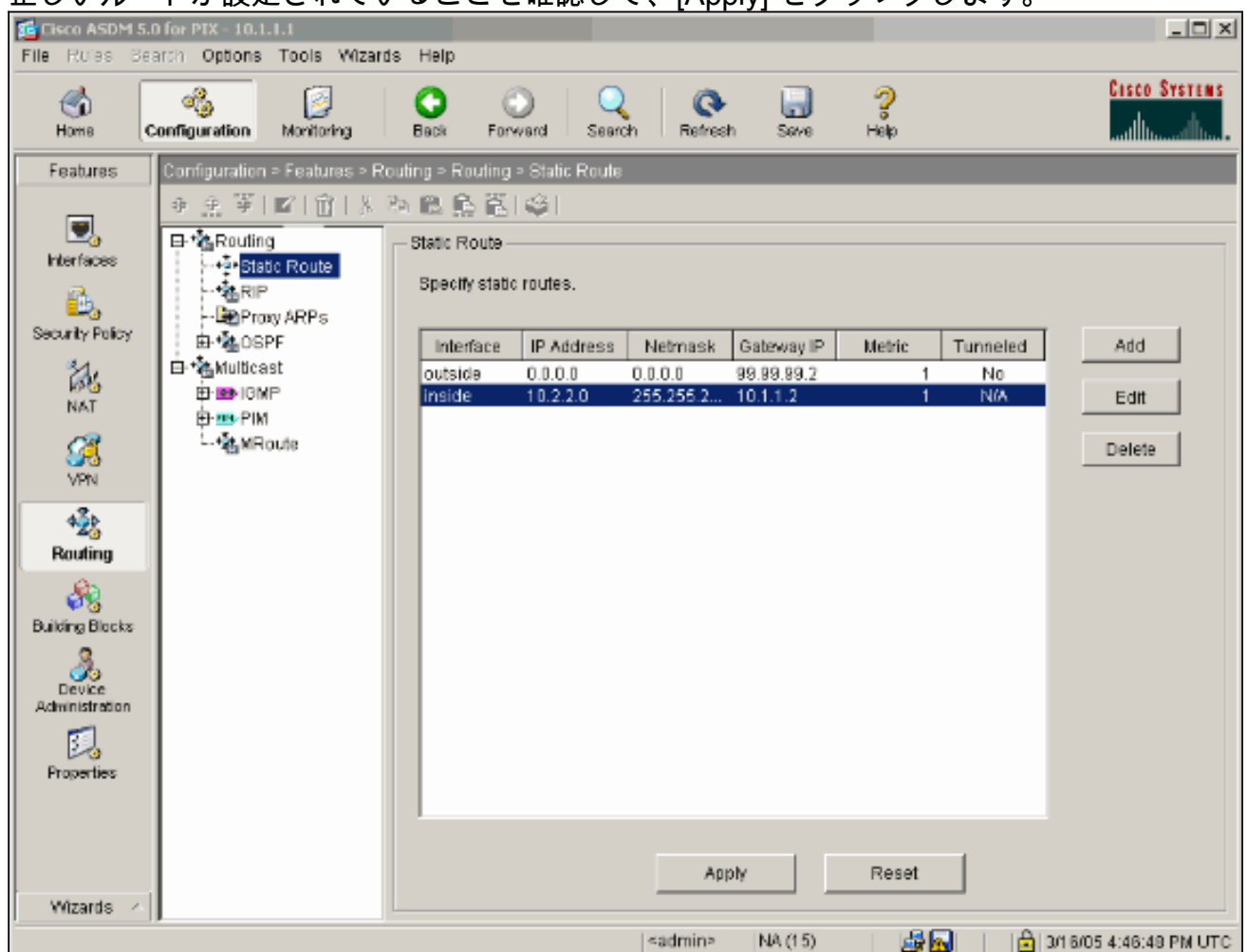
12. デフォルト ゲートウェイを設定し、[OK] をクリックします。



13. [Add] をクリックして、inside ネットワークにルートを追加します。

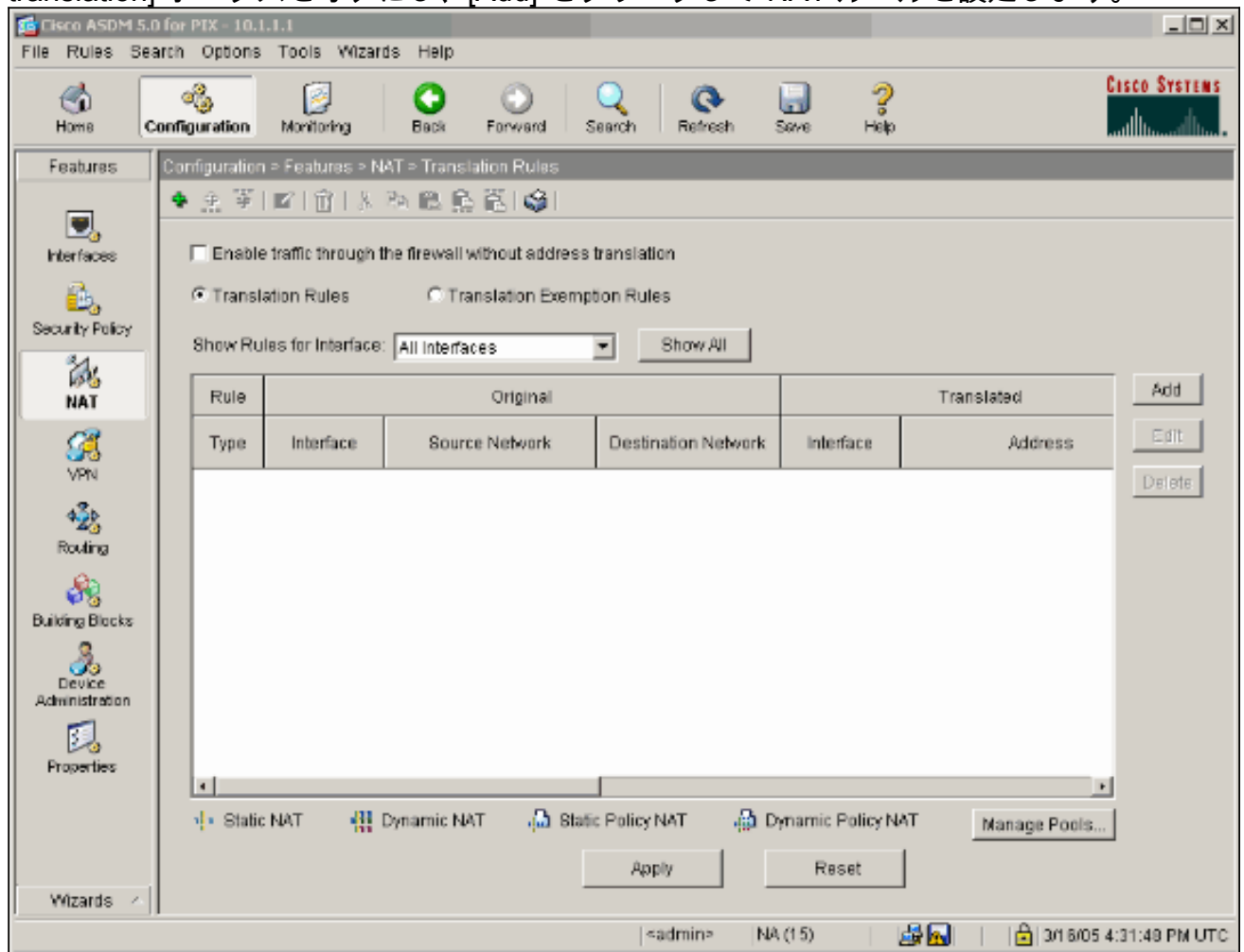


14. 正しいルートが設定されていることを確認して、[Apply] をクリックします。



15. この例では、NAT を使用します。[Enable traffic through the firewall without address

translation] ボックスをオフにし、[Add] をクリックして NAT ルールを設定します。



- 送信元ネットワーク (この例のみで使用) を設定します。次に、PAT を定義するため、[Manage Pools] をクリックします。

Add Address Translation Rule

Use NAT Use Policy NAT

Source Host/Network


Interface:

IP Address:

Mask:

Translate Address on Interface:


Translate Address To

 **Static** IP Address:

Redirect port

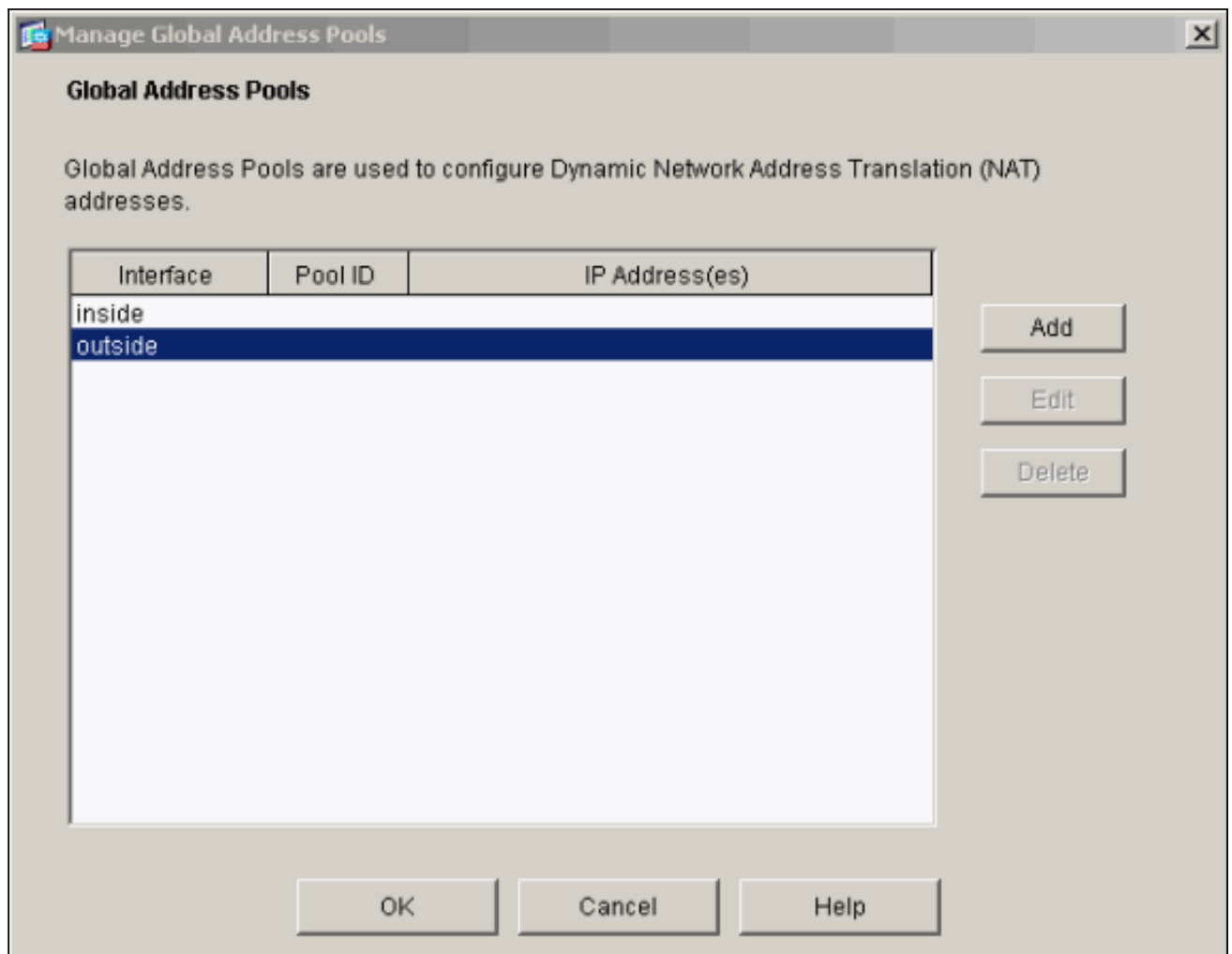
TCP Original port: Translated port:

UDP

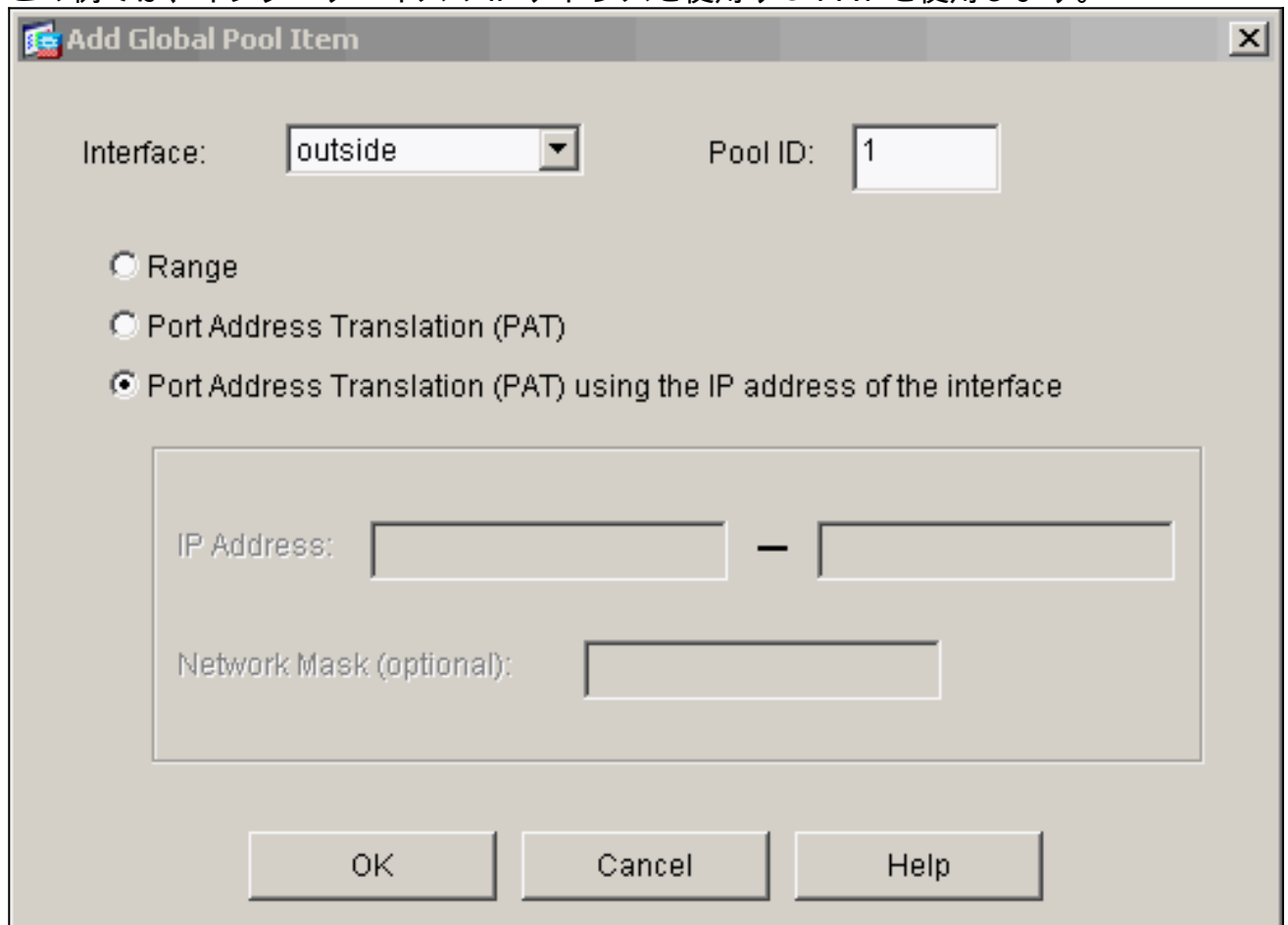
 **Dynamic** Address Pool:

Pool ID	Address
N/A	No address pool defined

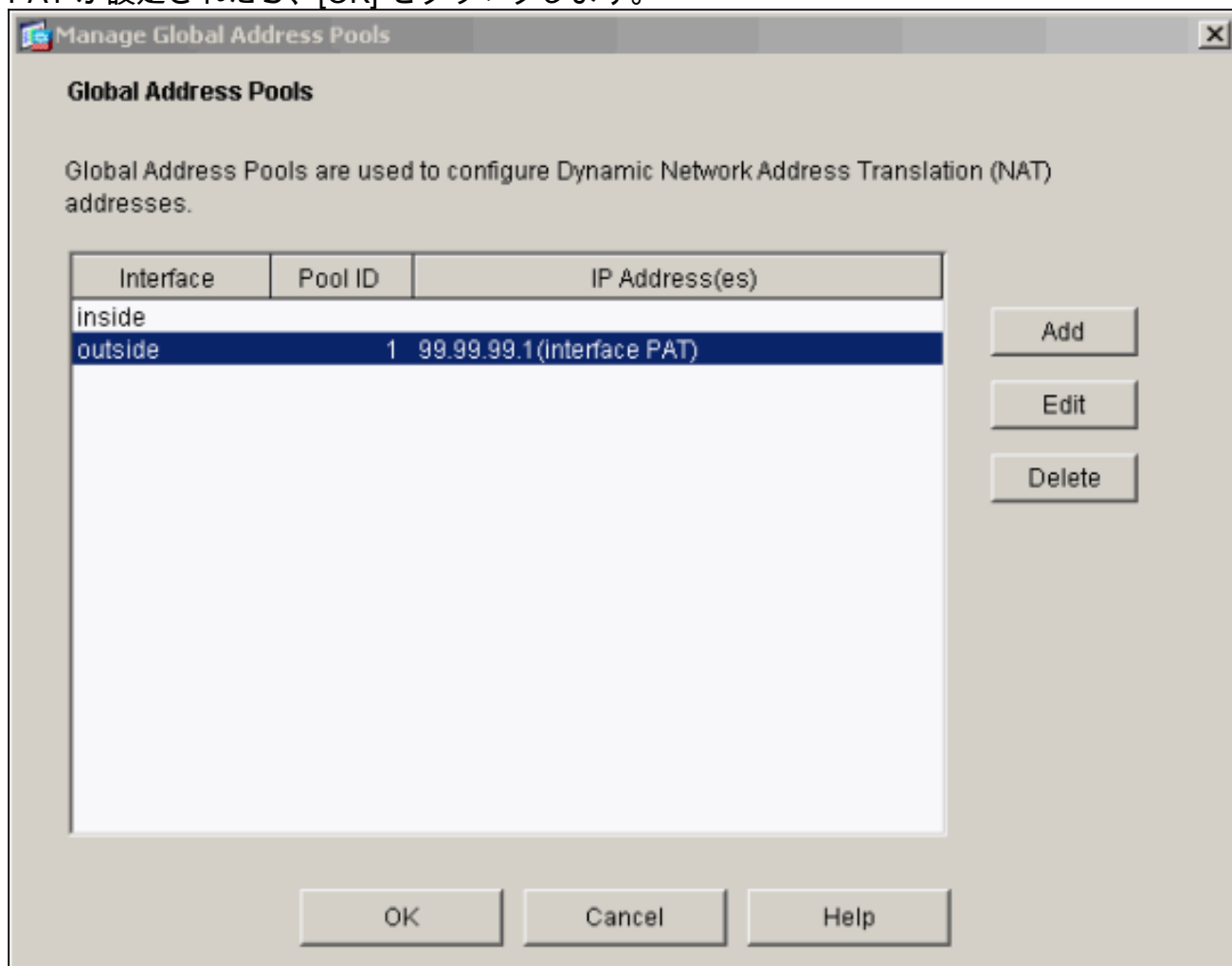
17. outside インターフェイスを選択し、[Add] をクリックします。



この例では、インターフェイスの IP アドレスを使用する PAT を使用します。



18. PAT が設定されたら、[OK] をクリックします。



19. スタティック変換を設定するため、[Add] をクリックします。

Add Address Translation Rule

Use NAT Use Policy NAT

Source Host/Network


Interface:

IP Address:

Mask:

Translate Address on Interface:


Translate Address To

 **Static** IP Address:

Redirect port

TCP Original port: Translated port:

UDP

 **Dynamic** Address Pool:

Pool ID	Address
1	99.99.99.1 (interface PAT)

20. [Interface] ドロップダウンで [inside] を選択した後、IP アドレス 10.1.1.2 とサブネットマスク 255.255.255.255 を入力してから、[Static] を選択し、[IP Address] フィールドに外部アドレス 99.99.99.12 を入力します。完了したら、[OK] をクリックします。

Add Address Translation Rule

Use NAT Use Policy NAT

Source Host/Network


Interface:

IP Address:

Mask:

Translate Address on Interface:


Translate Address To

 Static IP Address:

Redirect port

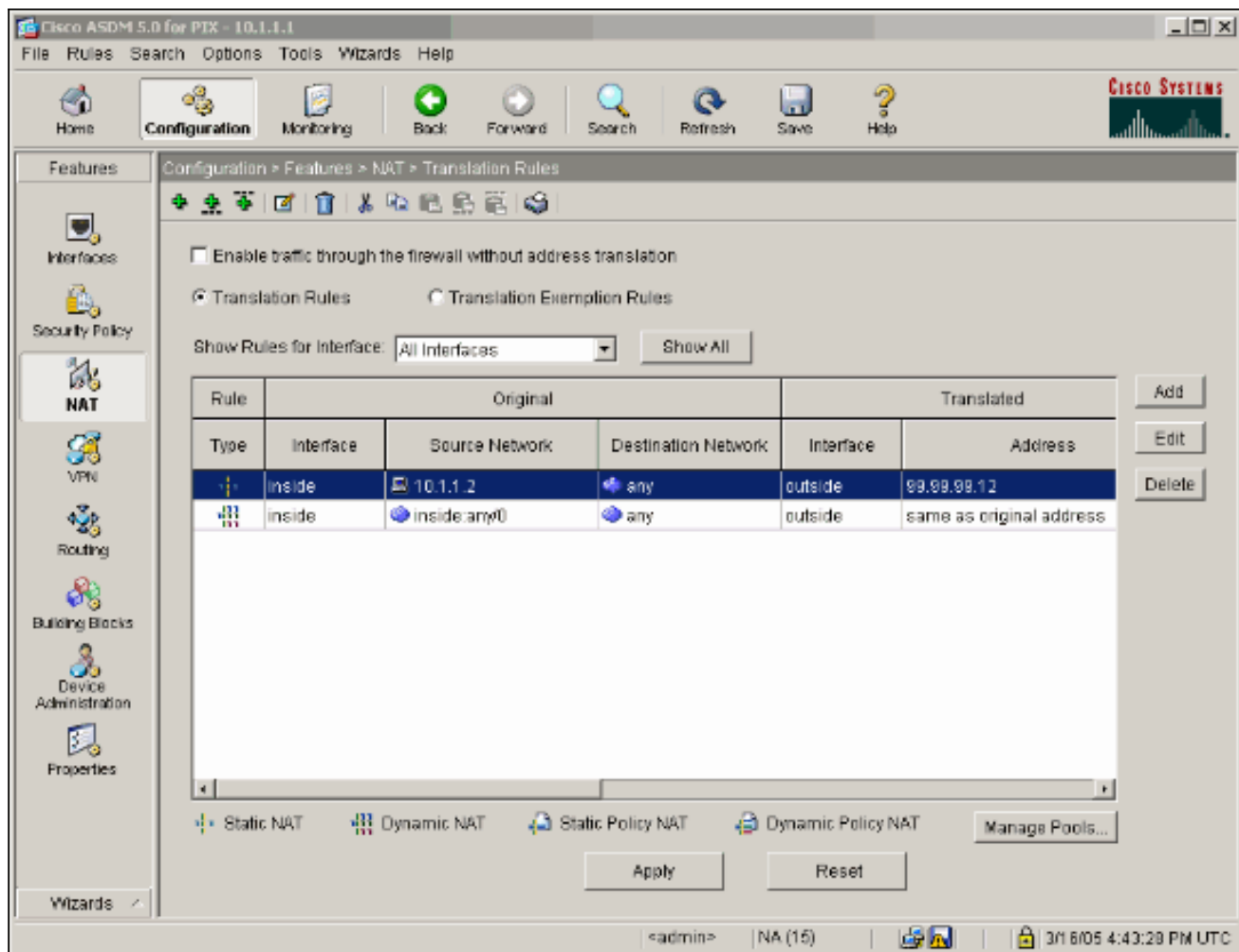
TCP Original port: Translated port:

UDP

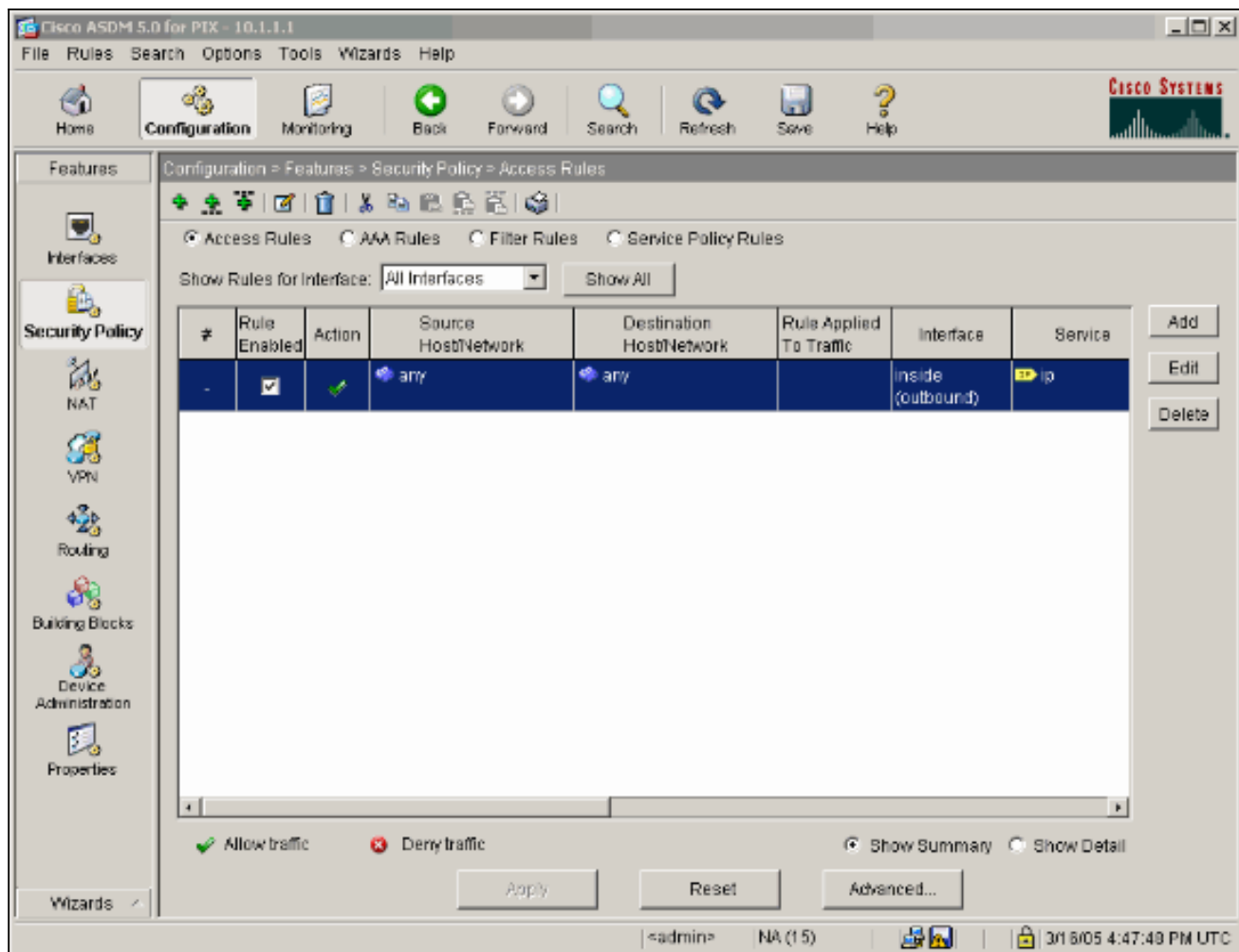
 Dynamic Address Pool:

Pool ID	Address

21. [Apply] をクリックして、インターフェイスの設定を承認します。設定内容は PIX にもブッシュュされます。



22. [Features] タブの [Security Policy] を選択して、セキュリティ ポリシー ルールを設定します。



23. [Add] をクリックして esp トラフィックを許可し、[OK] をクリックして続行します。

Add Access Rule


Action
 Select an action:
 Apply to Traffic:

Source Host/Network
 IP Address Name Group
 Interface:
 IP address: ...
 Mask:

Destination Host/Network
 IP Address Name Group
 Interface:
 IP address: ...
 Mask:

Syslog
 Default Syslog

Time Range
 Time Range:

Rule Flow Diagram
 Rule applied to traffic incoming to source interface

 99.99.99.2 outside inside 99.99.99.12
 Allow traffic

Protocol and Service
 TCP UDP ICMP IP
 IP Protocol
 IP protocol: ...

Please enter the description below (optional):


24. ISAKMP トラフィックを許可するため、[Add] をクリックした後、[OK] をクリックして続行します。

Edit Access Rule

Action
 Select an action:
 Apply to Traffic:

Source Host/Network
 IP Address Name Group
 Interface:
 IP address: ...
 Mask:

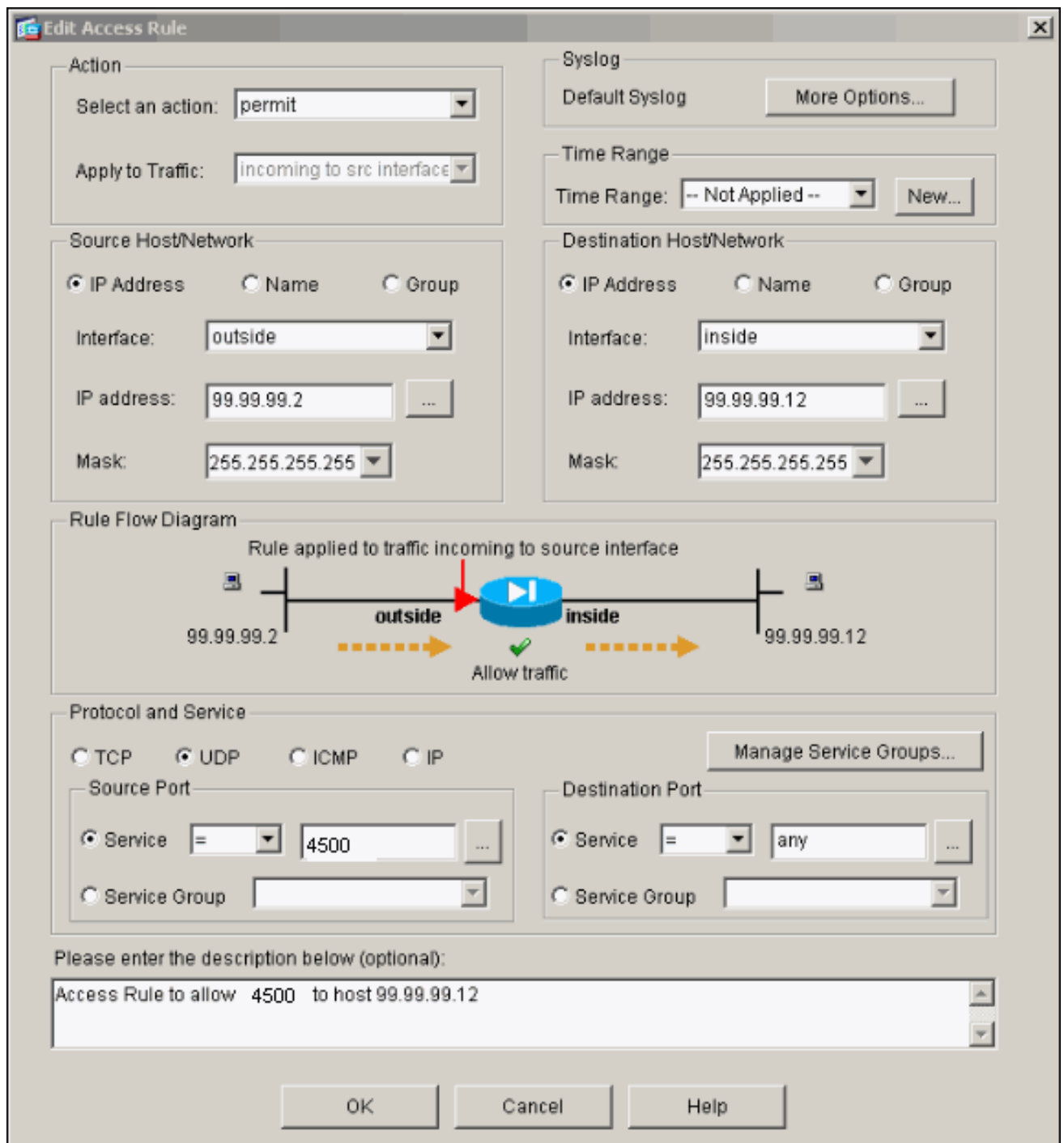
Destination Host/Network
 IP Address Name Group
 Interface:
 IP address: ...
 Mask:

Rule Flow Diagram
 Rule applied to traffic incoming to source interface


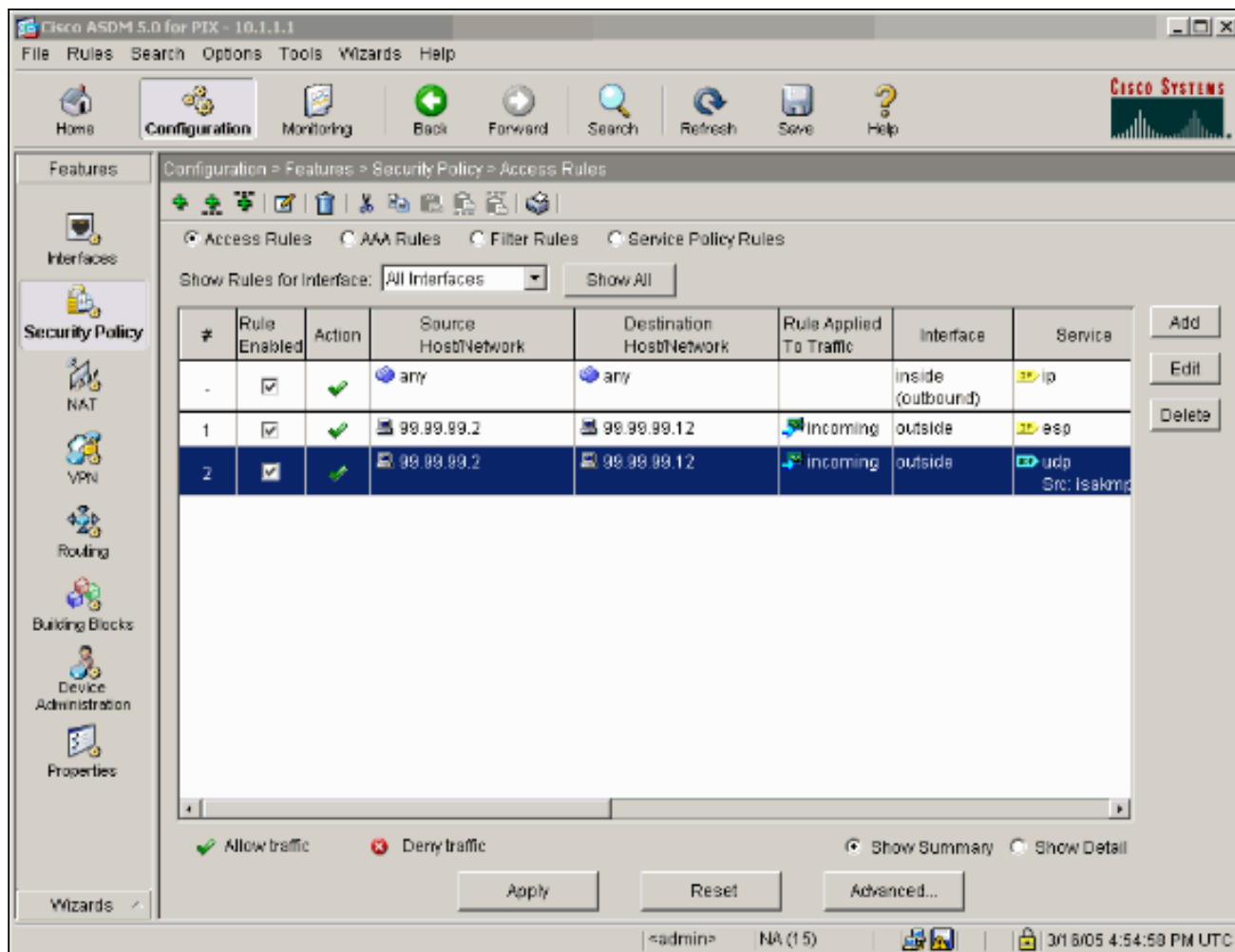
Protocol and Service
 TCP UDP ICMP IP
Source Port
 Service = ...
 Service Group
Destination Port
 Service = ...
 Service Group

Please enter the description below (optional):

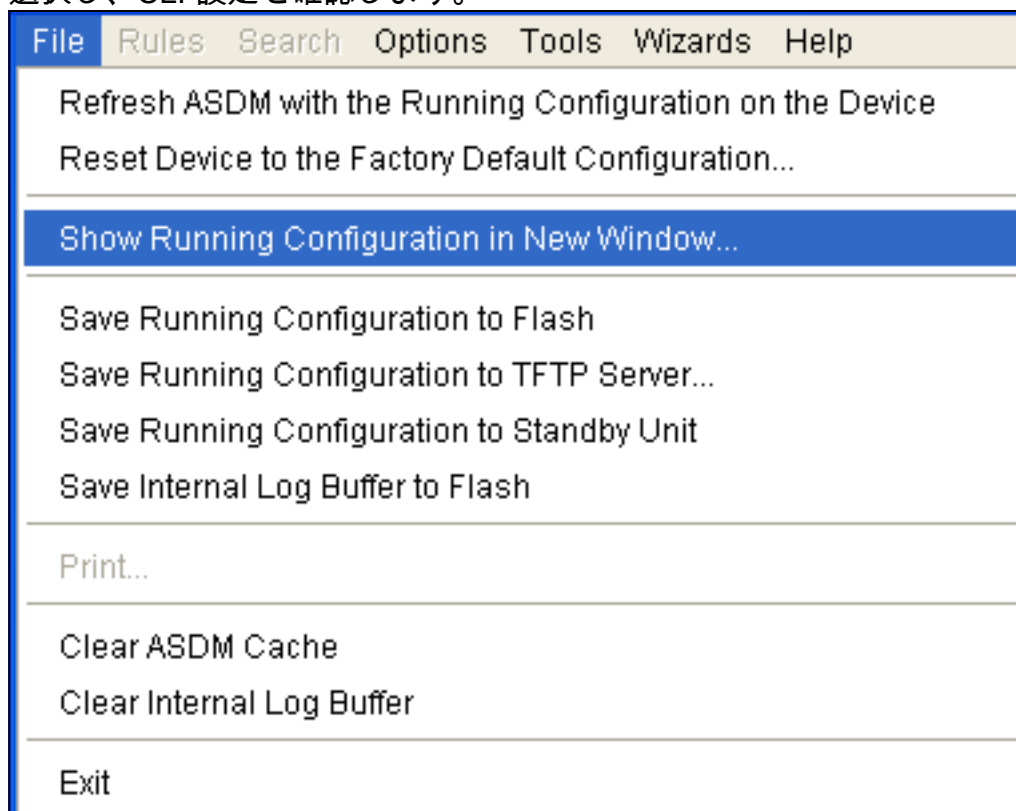
25. [Add] をクリックして NAT-T のための UDP ポート 4500 トラフィックを許可し、[OK] をクリックして続行します。



26. [Apply] をクリックして、インターフェイス設定を承認します。設定内容は PIX にもプッシュされます。



27. 設定はこれで完了しました。[File] > [Show Running Configuration in New Windows] の順に選択し、CLI 設定を確認します。



PIX ファイアウォール

```
pixfirewall# show run : Saved : PIX Version 7.0(0)102
names ! interface Ethernet0 nameif outside security-
level 0 ip address 99.99.99.1 255.255.255.0 ! interface
Ethernet1 nameif inside security-level 100 ip address
10.1.1.1 255.255.255.0 ! enable password
2KFQnbNIdI.2KYOU encrypted passwd 2KFQnbNIdI.2KYOU
encrypted hostname pixfirewall domain-name cisco.com ftp
mode passive access-list outside_access_in remark Access
Rule to Allow ESP traffic access-list outside_access_in
extended permit esp host 99.99.99.2 host 99.99.99.12
access-list outside_access_in remark Access Rule to
allow ISAKMP to host 99.99.99.12 access-list
outside_access_in extended permit udp host 99.99.99.2 eq
isakmp host 99.99.99.12 access-list outside_access_in
remark Access Rule to allow port 4500 (NAT-T) to host
99.99.99.12 access-list outside_access_in extended
permit udp host 99.99.99.2 eq 4500 host 99.99.99.12
pager lines 24 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 0.0.0.0 0.0.0.0 static
(inside,outside) 99.99.99.12 10.1.1.2 netmask
255.255.255.255 access-group outside_access_in in
interface outside route inside 10.2.2.0 255.255.255.0
10.1.1.2 1 route outside 0.0.0.0 0.0.0.0 99.99.99.2 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
http server enable http 10.1.1.3 255.255.255.255 inside
no snmp-server location no snmp-server contact snmp-
server enable traps snmp telnet timeout 5 ssh timeout 5
console timeout 0 ! 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 ! service-
policy asa_global_fw_policy global
Cryptochecksum:0a12956036ce4e7a97f351cde61fba7e : end
```

[PIX セキュリティ アプライアンスおよび MPF \(モジュラ ポリシー フレームワーク\) の設定](#)

アクセス リストの代わりに、MPF (モジュラ ポリシー フレームワーク) でコマンド `inspect ipsec-pass-thru` を使用し、PIX/ASA セキュリティ アプライアンス経由で IPsec トラフィックを渡します。

この検査は ESP トラフィックのピンホールを開くように設定されています。転送フローが存在していて、かつ許容できる最大接続数に制限がない場合、ESP データ フローのすべてが許可されます。AH は許可されません。ESP データ フローのデフォルト アイドル タイムアウトは、デフォルトで 10 分に設定されています。この検査は、クラスおよび一致コマンド モードを含め、他の検査を適用できるすべての場所に適用可能です。IPSec パススルー アプリケーション インспекションは、IKE UDP ポート 500 接続に関連付けられた ESP (IP プロトコル 50) トラフィックを簡単に横断できます。このインспекションは、冗長なアクセス リスト コンフィギュレーションを回避して ESP トラフィックを許可し、タイムアウトと最大接続数によりセキュリティも

確保します。 `class-map`、`policy-map`、および `service-policy` の各コマンドを使用してトラフィックのクラスを定義し、`inspect` コマンドをクラスに適用して、ポリシーを 1 つまたは複数のインターフェイスに適用します。有効にした場合、`inspect IPsec-pass-thru` コマンドでは、タイムアウト 10 分の無制限 ESP トラフィックが可能になります。これは設定不可能です。NAT および非 NAT トラフィックは許可されます。

```
hostname(config)#access-list test-udp-acl extended permit udp any any eq 500
hostname(config)#class-map test-udp-class hostname(config-cmap)#match access-list test-udp-acl
hostname(config)#policy-map test-udp-policy hostname(config-pmap)#class test-udp-class
hostname(config-pmap-c)#inspect ipsec-pass-thru hostname(config)#service-policy test-udp-policy
interface outside
```

確認

このセクションでは、設定が正常に動作しているかどうかを確認する際に役立つ情報を示しています。

特定の `show` コマンドは、[Output Interpreter Tool](#) ([登録ユーザ専用](#)) によってサポートされています。このツールを使用すると、`show` コマンド出力の分析を表示できます。

- `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。

[ルータ IPsec のトラブルシューティング 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 Internet Security Association and Key Management Protocol (ISAKMP) ネゴシエーションを表示します。

[セキュリティ アソシエーションのクリア](#)

- `clear crypto isakmp` - インターネット キー交換 (IKE) のセキュリティ アソシエーションをクリアします。
- `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。

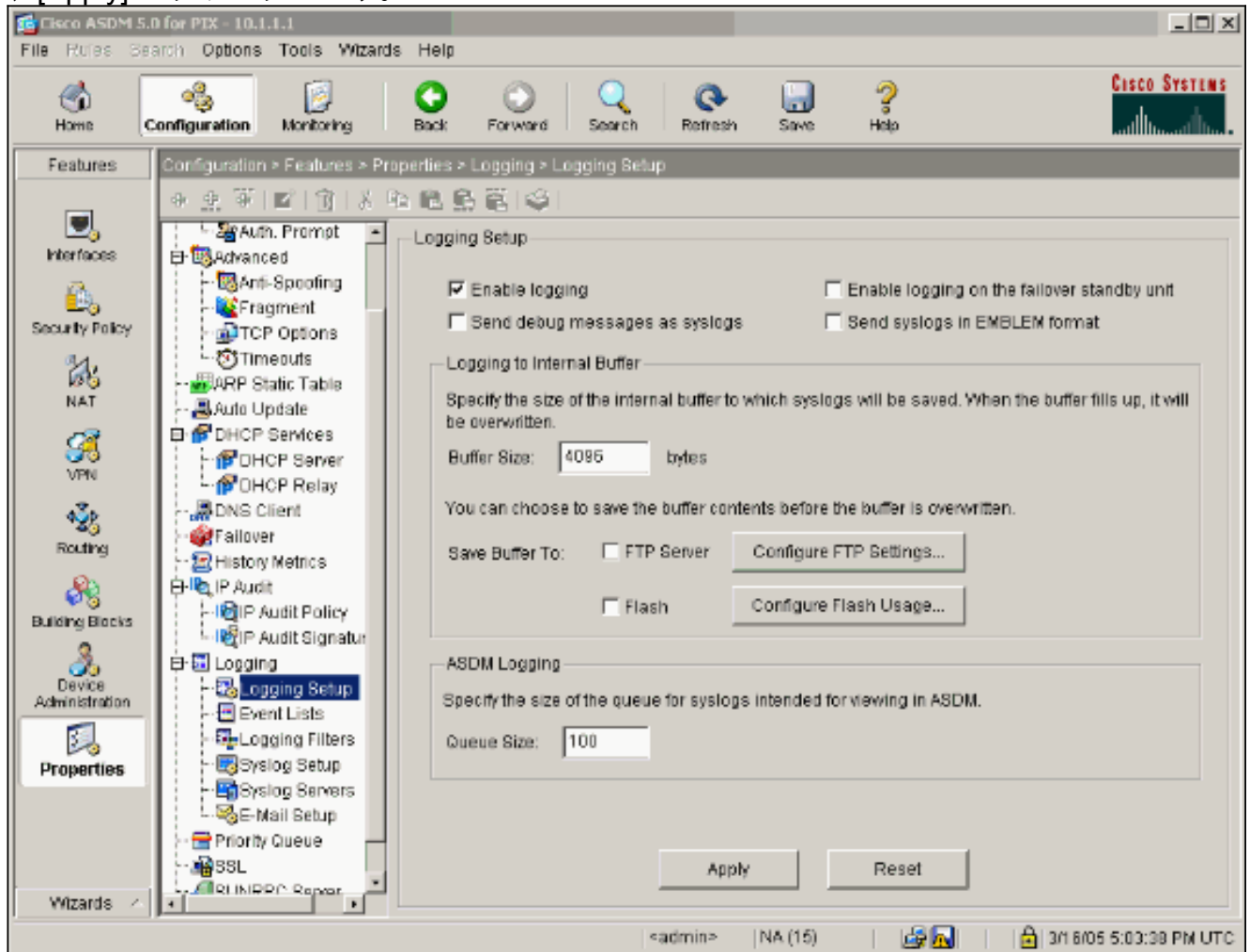
[PIX のトラブルシューティング コマンド](#)

特定の `show` コマンドは、[Output Interpreter Tool](#) ([登録ユーザ専用](#)) によってサポートされています。このツールを使用すると、`show` コマンド出力の分析を表示できます。

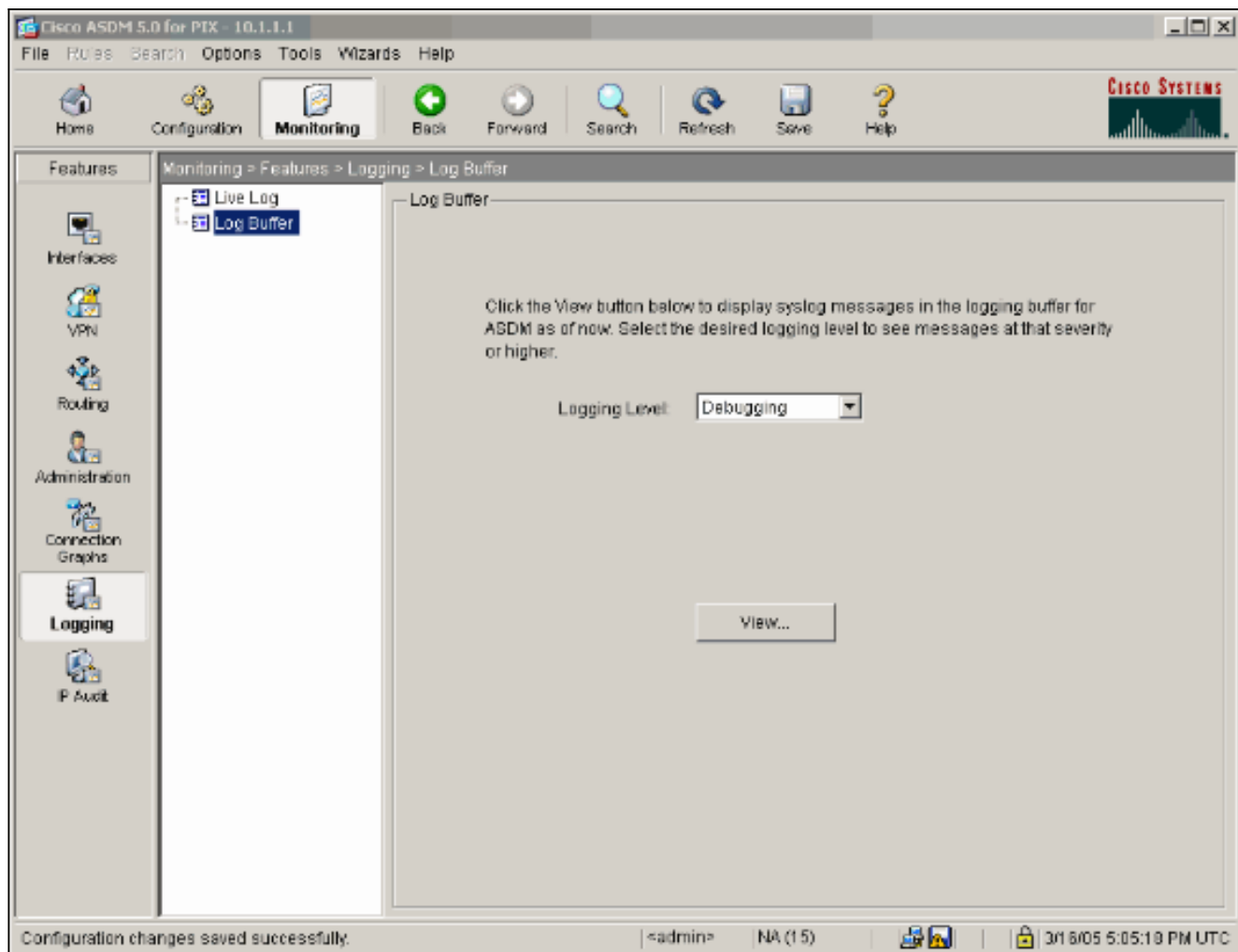
注: `debug` コマンドを使用する前に、『[debug コマンドの重要な情報](#)』を参照してください。

- **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。この情報は PIX ログ バッファに保存されており、**show log** コマンドを使用して表示できます。
- ASDM を使用してロギングを有効にし、以下の手順で示されているようにログを表示できます。

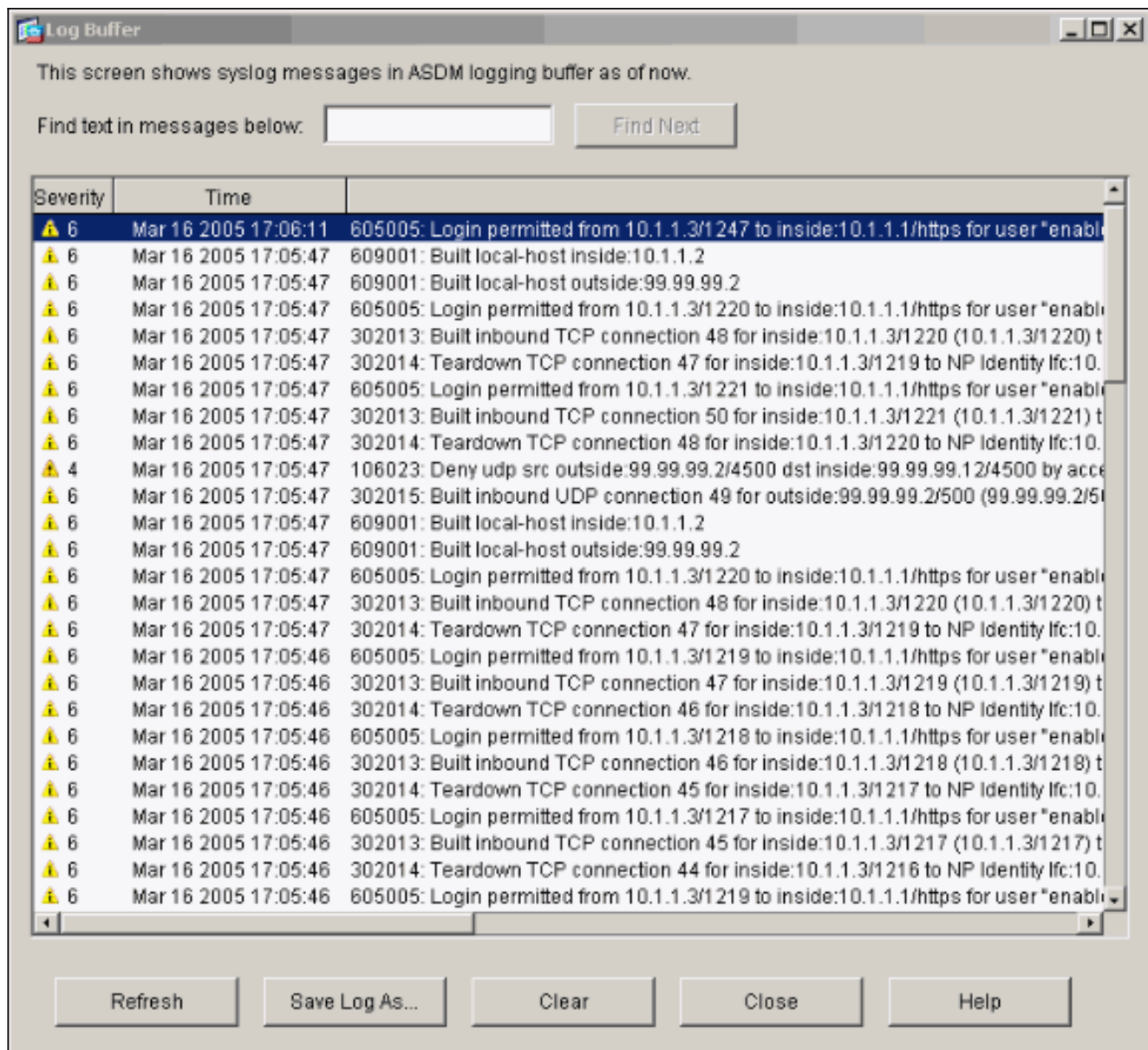
1. [Configuration] > [Properties] > [Logging] > [Logging Setup] > [Enable Logging] を選択した後、[Apply] をクリックします。



2. [Monitoring] > [Logging] > [Log Buffer] > [On Logging Level] > [Logging Buffer] を選択してから、[View] をクリックします。



ログバッファの例を次に示します。



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 に関するサポート ページ](#)
- [PIX コマンド リファレンス](#)
- [NAT に関するサポートページ](#)
- [Requests for Comments \(RFC \)](#)
- [テクニカルサポートとドキュメント - Cisco Systems](#)