

PIX/ASA 7.x:nat、global、static および access-list コマンドを使用したポート リダイレクション (フォワーディング)

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[関連製品](#)

[表記法](#)

[ネットワーク図](#)

[初期設定](#)

[アウトバウンド アクセスの許可](#)

[NAT を使用した inside ホストから outside ネットワークへのアクセスの許可](#)

[PAT を使用した Inside ホストから Outside ネットワークへのアクセスの許可](#)

[inside ホストから outside ネットワークへのアクセスの制限](#)

[信頼できないホストから信頼できるネットワーク上のホストへのアクセスの許可](#)

[PIX バージョン 7.0 以降での ACL の使用](#)

[特定のホストおよびネットワークでの NAT の無効化](#)

[static を使用したポート リダイレクション \(フォワーディング \)](#)

[ネットワーク ダイアグラム : ポート リダイレクション \(フォワーディング \)](#)

[PIX 部分設定 - ポートリダイレクション](#)

[static を使用した TCP/UDP セッションの制限](#)

[時間ベースのアクセス リスト](#)

[テクニカルサポートのサービス リクエストをオープンする際に収集する情報](#)

[関連情報](#)

概要

Cisco PIX セキュリティ アプライアンス バージョン 7.0 を実装した場合にセキュリティを最大限に実現するには、nat-control、nat、global、static、access-list、access-group の各コマンドを使用する際に、セキュリティの高いインターフェイスと低いインターフェイスの間をパケットが流れる仕組みを理解することが重要です。このドキュメントでは、これらのコマンドの違い、ポート リダイレクション (フォワーディング) の設定方法、コマンドライン インターフェイスまたは Adaptive Security Device Manager (ASDM) を使用した PIX ソフトウェア バージョン 7.x での Outside ネットワーク アドレス変換 (NAT) の機能について説明します。

注 : ASDM 5.2以降の一部のオプションは、ASDM 5.1のオプションとは異なる場合があります。詳細については、[ASDMのドキュメントを参照](#)してください。

[前提条件](#)

[要件](#)

ASDM でデバイスを設定できるようにする方法については、『[ASDM 用の HTTPS アクセスの許可](#)』を参照してください。

[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いています。

- Cisco PIX 500 シリーズ セキュリティ アプライアンス ソフトウェア バージョン 7.0 以降
- ASDM バージョン 5.x 以降

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ました。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。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

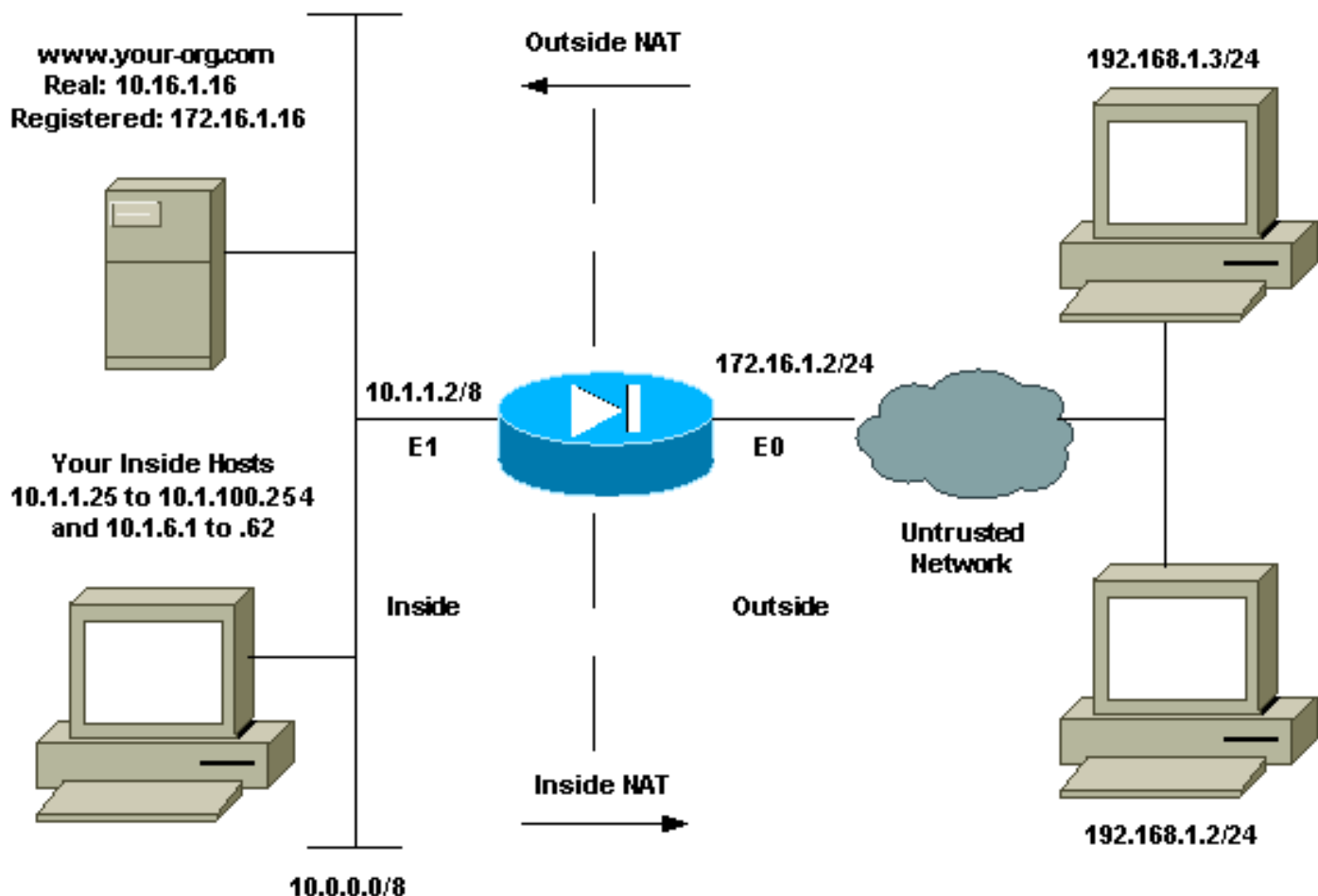
[関連製品](#)

この設定は、Cisco ASA セキュリティ アプライアンス バージョン 7.x 以降でも使用できます。

[表記法](#)

ドキュメント表記の詳細については、『[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。

[ネットワーク図](#)



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。

初期設定

インターフェイス名は次のとおりです。

- **interface ethernet 0** : Outside の nameif
- **interface ethernet 1** : Inside の nameif

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。

アウトバウンド アクセスの許可

アウトバウンド アクセスは、セキュリティ レベルの高いインターフェイスからセキュリティ レベルの低いインターフェイスへの接続を意味します。これには、inside から outside への接続、inside から非武装地帯 (DMZ) への接続、および DMZ から outside への接続が含まれます。発信元インターフェイスのセキュリティ レベルが宛先より高いという条件下では、ある DMZ から別の DMZ への接続もこれに含まれる可能性があります。これを確認するには、PIX インターフェイス上の「セキュリティ レベル」設定を確認します。

次の例は、セキュリティ レベルとインターフェイス名の設定を示しています。

```
pix(config)#interface ethernet 0
```

```
pix(config-if)#security-level 0
pix(config-if)#nameif outside
pix(config-if)#exit
```

PIX 7.0 では **nat-control** コマンドが導入されています。コンフィギュレーション モードで **nat-control** コマンドを使用すると、Outside 通信用に NAT が必要かどうかを指定できます。NAT 制御をイネーブルにすると、PIX ソフトウェアの以前のバージョンと同じように、アウトバウンドトラフィックを許可するために NAT ルールの設定が必要です。NAT 制御がディセーブルになっている場合 (**no nat-control**)、Inside ホストは、NAT ルールの設定なしで、Outside ネットワークと通信できません。ただし、パブリックアドレスを持たない Inside ホストがある場合は、これらのホスト用に NAT を設定する必要があります。

ASDM を使用して NAT 制御を設定するには、ASDM Home ウィンドウから Configuration タブを選択し、機能メニューから NAT を選択します。

Enable traffic through the firewall without translation: このオプションは PIX バージョン 7.0(1) で導入されました。このオプションにチェックマークが付いていると、コンフィギュレーションでは **nat-control** コマンドは発行されません。このコマンドは、ファイアウォールを通過するために変換が必要ではないことを意味します。通常、このオプションにチェックマークが付いているのは、内部ホストにパブリック IP アドレスがある場合、またはネットワークトポロジで内部ホストが IP アドレスに変換される必要がない場合だけです。

内部ホストにプライベート IP アドレスがある場合は、このオプションのチェックマークを外して、内部ホストをパブリック IP アドレスに変換でき、内部ホストがインターネットにアクセスできるようにする必要があります。

The screenshot displays the Cisco ASDM 5.1 for PIX - 10.1.1.1 interface. The main window is titled "Configuration > NAT > Translation Rules". The "Enable traffic through the firewall without address translation" checkbox is checked. Below this, there are radio buttons for "Translation Rules" (selected) and "Translation Exemption Rules". A dropdown menu shows "All Interfaces" and a "Show All" button. A table with columns "Rule", "Original", and "Translated" is shown. The "Original" column has sub-columns "Interface", "Source Network", and "Destination Network". The "Translated" column has sub-columns "Interface" and "Address". Buttons for "Add", "Edit", and "Delete" are on the right. At the bottom, there are buttons for "Static NAT", "Dynamic NAT", "Static Policy NAT", "Dynamic Policy NAT", and "Manage Pools...". The "Apply" and "Reset" buttons are at the bottom center. The status bar at the bottom shows "<admin> NA (15)" and the time "7/11/06 6:02:29 PM UTC".

NAT 制御を使用してアウトバウンド アクセスを許可するために必要な 2 つのポリシーがあります。最初のポリシーは変換方式です。変換方式は **static** コマンドを使用したスタティック変換、または **nat/global** ルールを使用したダイナミック変換のどちらかになります。NAT 制御がディセーブルになっていて、Inside ホストがパブリックアドレスを持っている場合、この変換方式は必要ありません。

(NAT 制御がイネーブルになっているかディセーブルになっているかに関係なく適用される) アウトバウンド アクセスのもう 1 つの要件は、Access Control List (ACL; アクセス コントロール リスト) が存在するかどうかです。ACL が存在する場合、ACL は特定のプロトコルとポートを使用して、発信元ホストが宛先ホストにアクセスするのを許可する必要があります。デフォルトでは、PIX 経由のアウトバウンド接続に対するアクセス制限はありません。これは、発信元インターフェイスに ACL が設定されていない場合、デフォルトでは、変換方式が設定されていればアウトバウンド接続が可能になることを意味します。

[NAT を使用した inside ホストから outside ネットワークへのアクセスの許可](#)

この設定では、サブネット 10.1.6.0/24 上のすべてのホストに外部へのアクセスが付与されます。これを行うには、手順で示すように、**nat** コマンドと **global** コマンドを使用します。

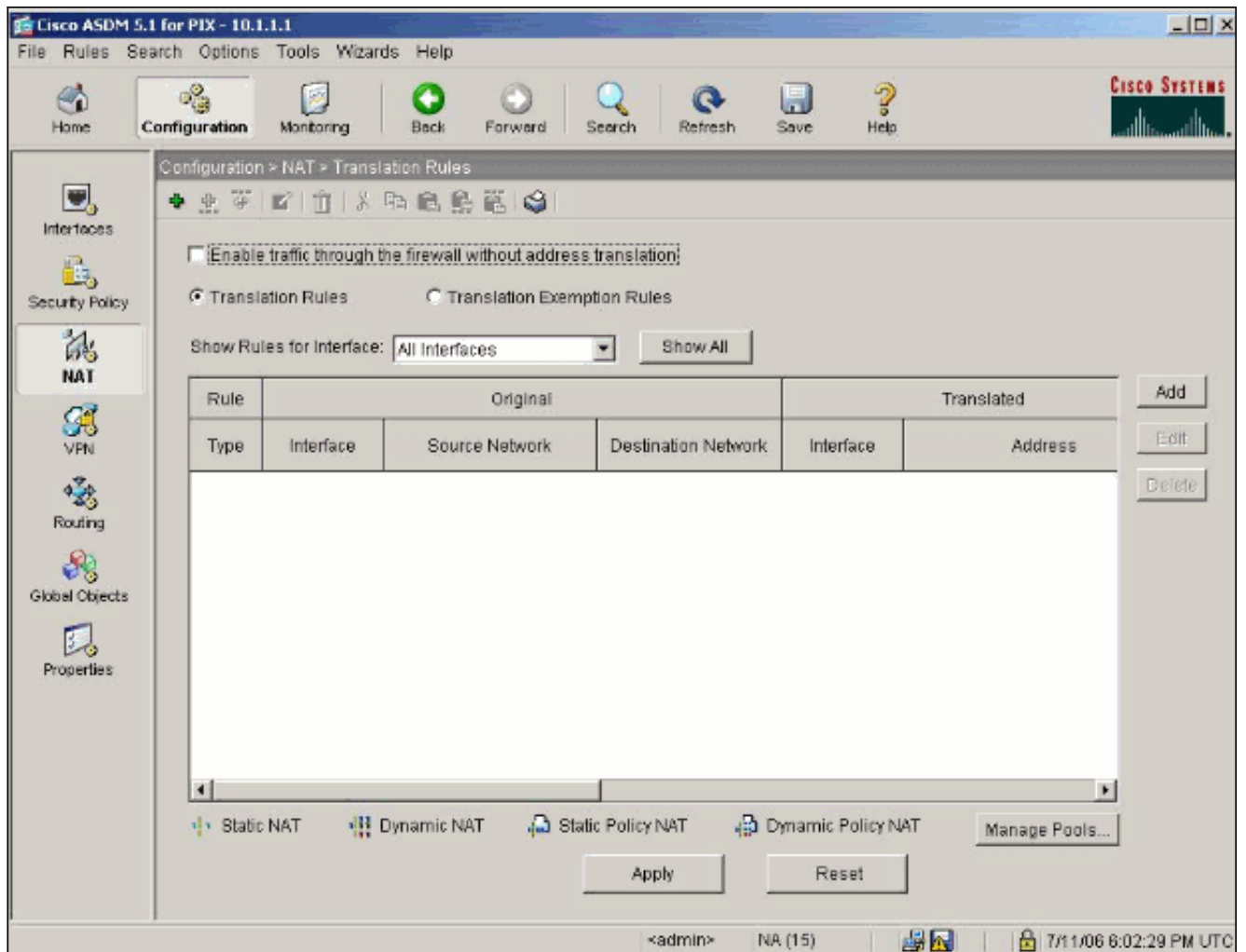
1. NAT に含める Inside グループを定義します。

```
nat (inside) 1 10.1.6.0 255.255.255.0
```

2. NAT文で定義されたホストが変換される外部インターフェイスのアドレスプールを指定します。

```
global (outside) 1 172.16.1.5-172.16.1.10 netmask 255.255.255.0
```

3. グローバル アドレス プールを作成するには、ASDM を使用します。Configuration > Features > NAT の順に選択し、Enable traffic through the firewall without address translation のチェックマークを外します。続いて Add をクリックして、NAT Rule を設定します。



4. [Manage Pools] をクリックして、NAT プール アドレスを定義します。

Edit 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

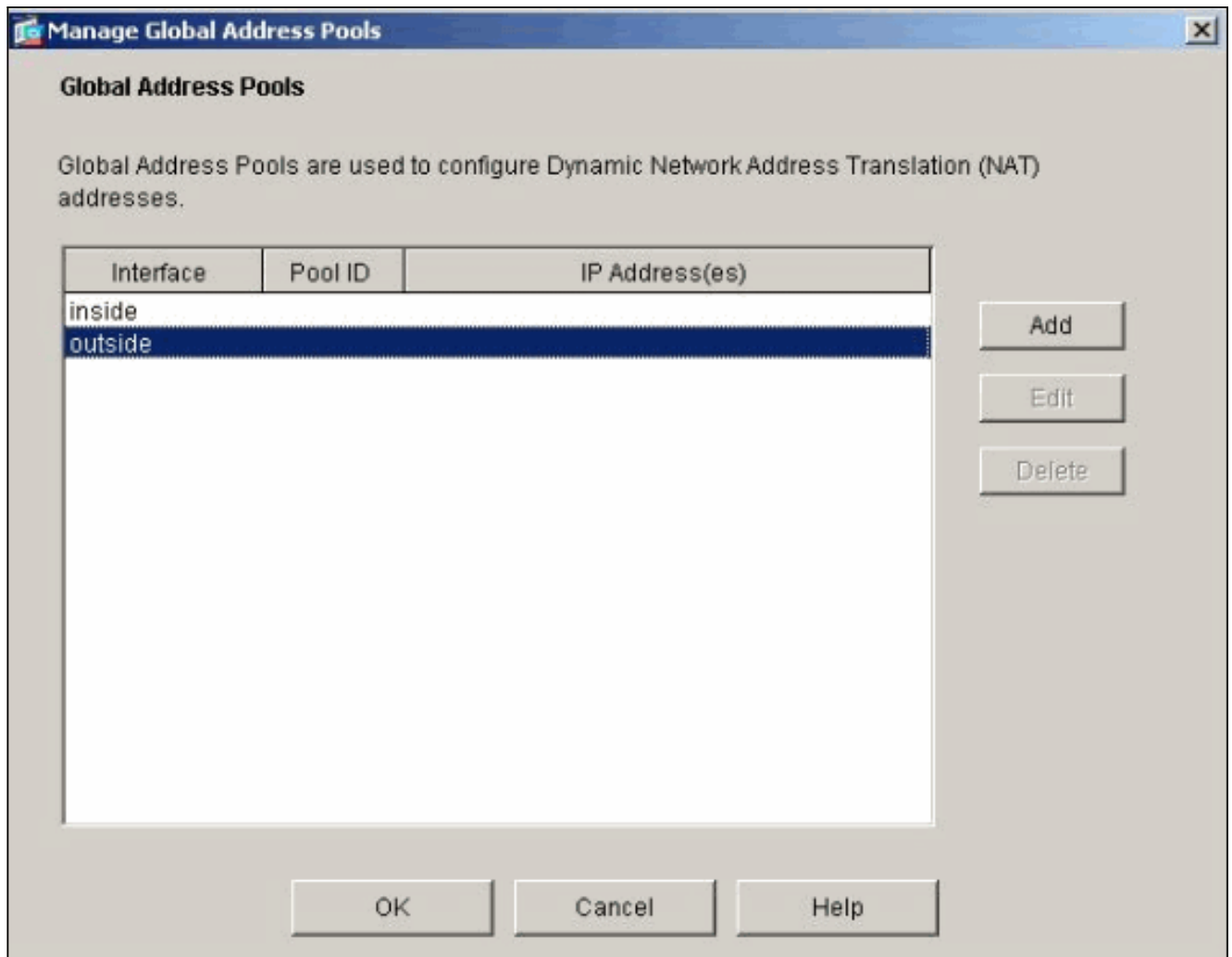
TCP Original port: Translated port:

UDP

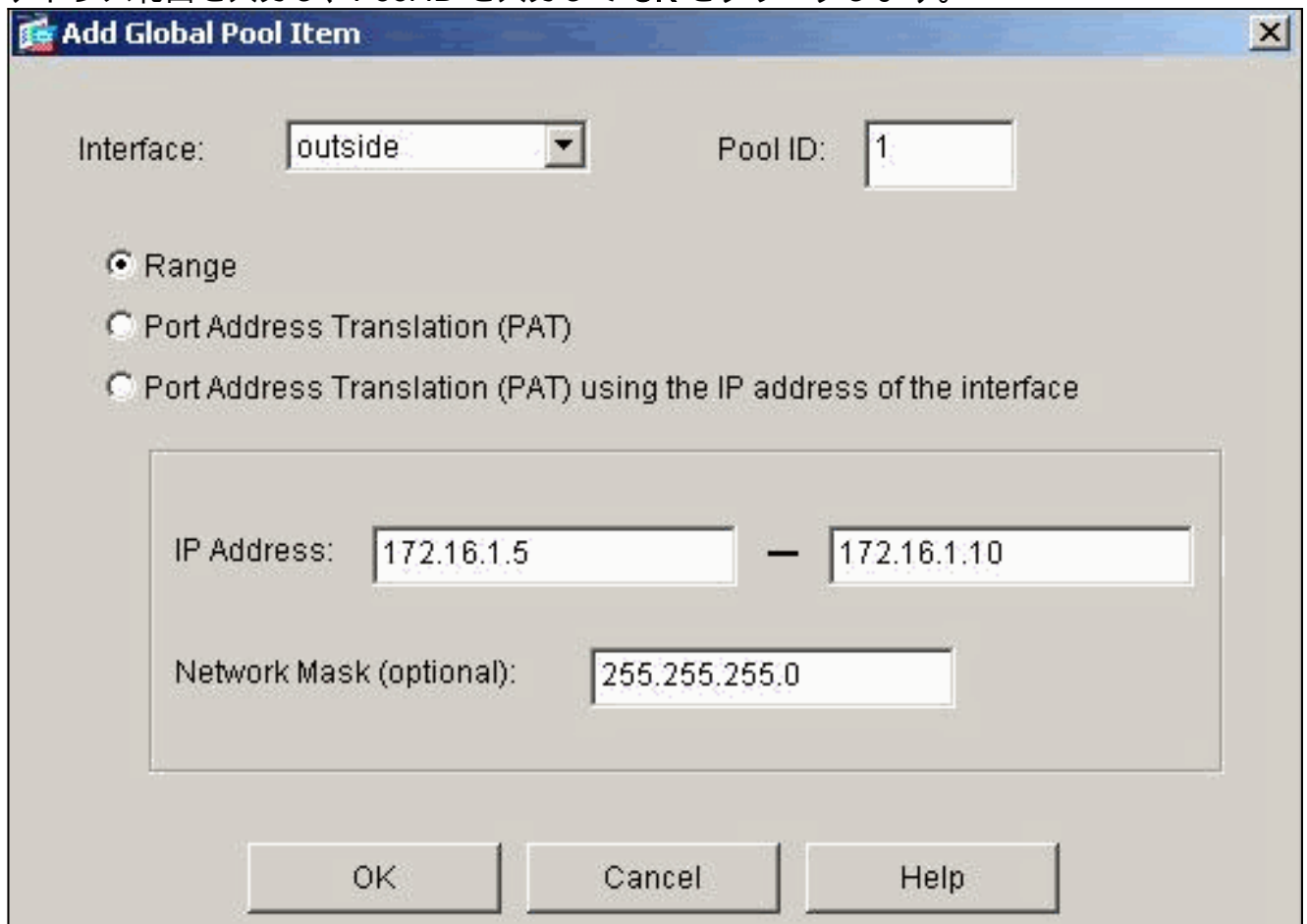
Dynamic Address Pool:

Pool ID	Address
N/A	No address pool defined

5. **Outside > Add** の順に選択して、範囲を選択し、アドレスのプールを指定します。



6. アドレス範囲を入力し、Pool ID を入力して OK をクリックします。



7. Configuration > Features > NAT > Translation Rules の順に選択して、変換ルールを作成します。
8. 発信元インターフェイスとして **Inside** を選択し、NAT を適用するアドレスを入力します。
9. Translate Address on Interface では、**Outside** を選択し、**Dynamic** を選択して、設定したアドレスプールを選択します。
10. [OK] をクリックします。

Edit 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

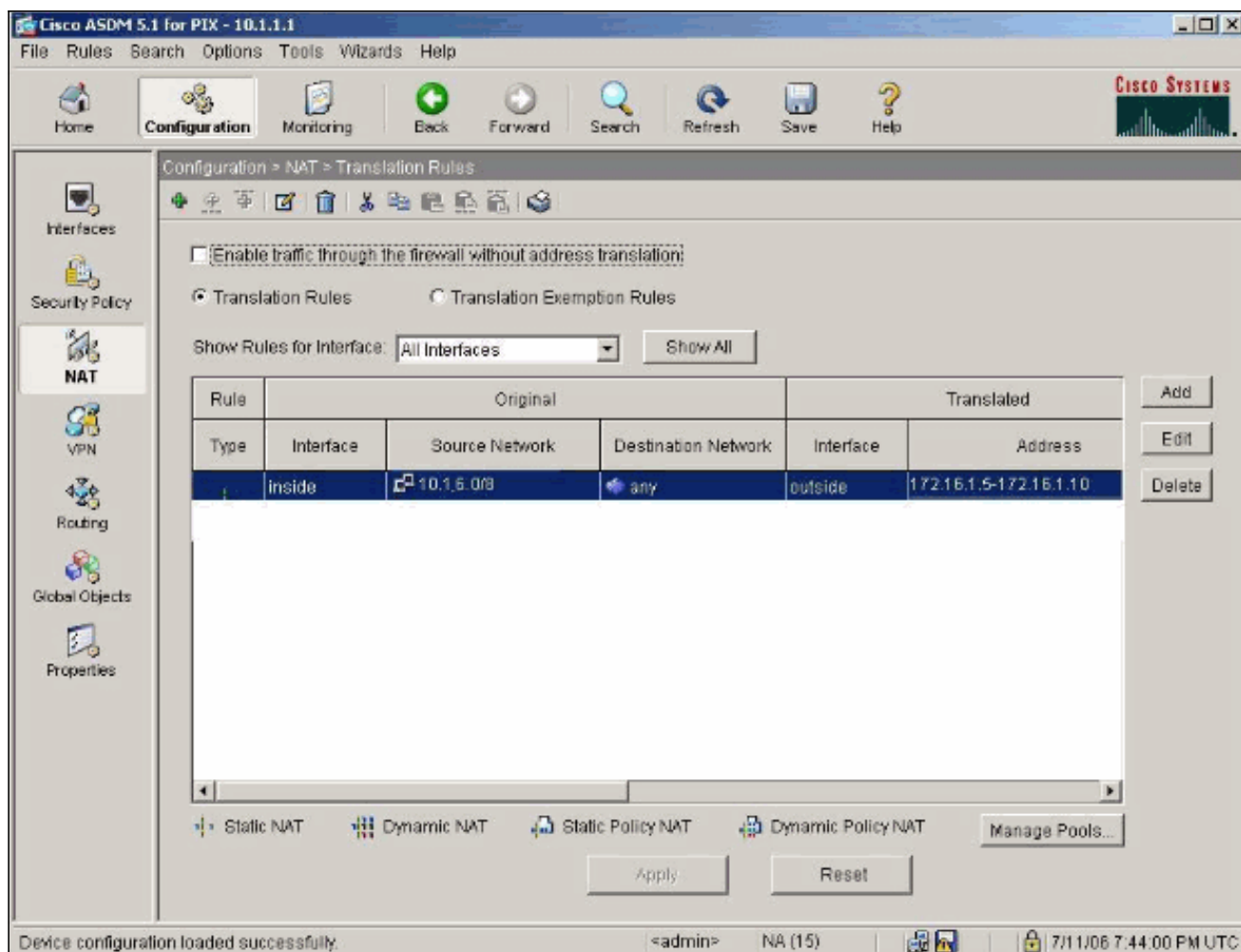
TCP Original port: Translated port:

UDP

Dynamic Address Pool:

Pool ID	Address
1	172.16.1.5-172.16.1.10

11. Configuration > Features > NAT > Translation Rules の順に選択すると、Translation Rules に変換が表示されます。



これで、内部のホストは外部ネットワークにアクセスできます。内部のホストは外部へ接続を開始すると、グローバルプールのアドレスに変換されます。アドレスは、先着順、先に変換される順に、グローバルプール内の一番低いアドレスから割り当てられます。たとえば、ホスト10.1.6.25が最初に外部への接続を開始する場合、アドレス172.16.1.5を受信します。次のホストが172.16.1.6を受信します。これはスタティック変換ではなく、**timeout xlate hh:mm:ss** コマンドで定義されている非アクティブ期間が過ぎると、タイムアウトします。プール内のアドレスよりも多くの Inside ホストが存在する場合、プールの最後のアドレスが Port Address Translation (PAT; ポート アドレス変換) に使用されます。

[PAT を使用した Inside ホストから Outside ネットワークへのアクセスの許可](#)

変換用に inside ホストで 1 つのパブリックアドレスを共有する場合は PAT を使用します。global ステートメントに 1 つのアドレスが指定されている場合、そのアドレスはポート変換されます。PIX ではインターフェイスごとに 1 つのポート変換が可能であり、この変換では、単一のグローバルアドレスへのアクティブな xlate オブジェクトが最大で 65,535 個サポートされます。PAT を使用して Inside ホストが Outside ネットワークにアクセスするのを許可するには、次の手順を実行します。

1. PAT に含める Inside グループを定義します (0 0 を使用すると、すべての Inside ホストを選択することになります)。

```
nat (inside) 1 10.1.6.0 255.255.255.0
```

2. PAT で使用するグローバルアドレスを指定します。このアドレスには、インターフェイスアドレスを使用できます。

```
global (outside) 1 172.16.1.4 netmask 255.255.255.0
```

- ASDM で **Configuration > Features > NAT** の順に選択し、**Enable traffic through the firewall without address translation** のチェックマークを外します。
- Add** をクリックして、NAT ルールを設定します。
- Manage Pools** をクリックして、PAT アドレスを設定します。
- Outside > Add** の順に選択し、**Port Address Translation (PAT)** をクリックして、PAT 用の 1 つのアドレスを設定します。
- アドレスを入力し、Pool ID を入力して、**OK** をクリックします。

The screenshot shows the 'Add Global Pool Item' dialog box. The 'Interface' dropdown is set to 'outside' and the 'Pool ID' text box contains '1'. There are three radio button options: 'Range', 'Port Address Translation (PAT)' (which is selected), and 'Port Address Translation (PAT) using the IP address of the interface'. Below these options is a section for IP address configuration. The 'IP Address' field contains '172.16.1.4' and the 'Network Mask (optional)' field contains '255.255.255.0'. At the bottom of the dialog are three buttons: 'OK', 'Cancel', and 'Help'.

- Configuration > Features > NAT > Translation Rules** の順に選択して、変換ルールを作成します。
- 発信元インターフェイスとして **inside** を選択し、NAT を適用するアドレスを入力します。
- Translate Address on Interface では、**Outside** を選択し、**Dynamic** を選択して、設定したアドレスプールを選択します。[OK] をクリックします。

Edit 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

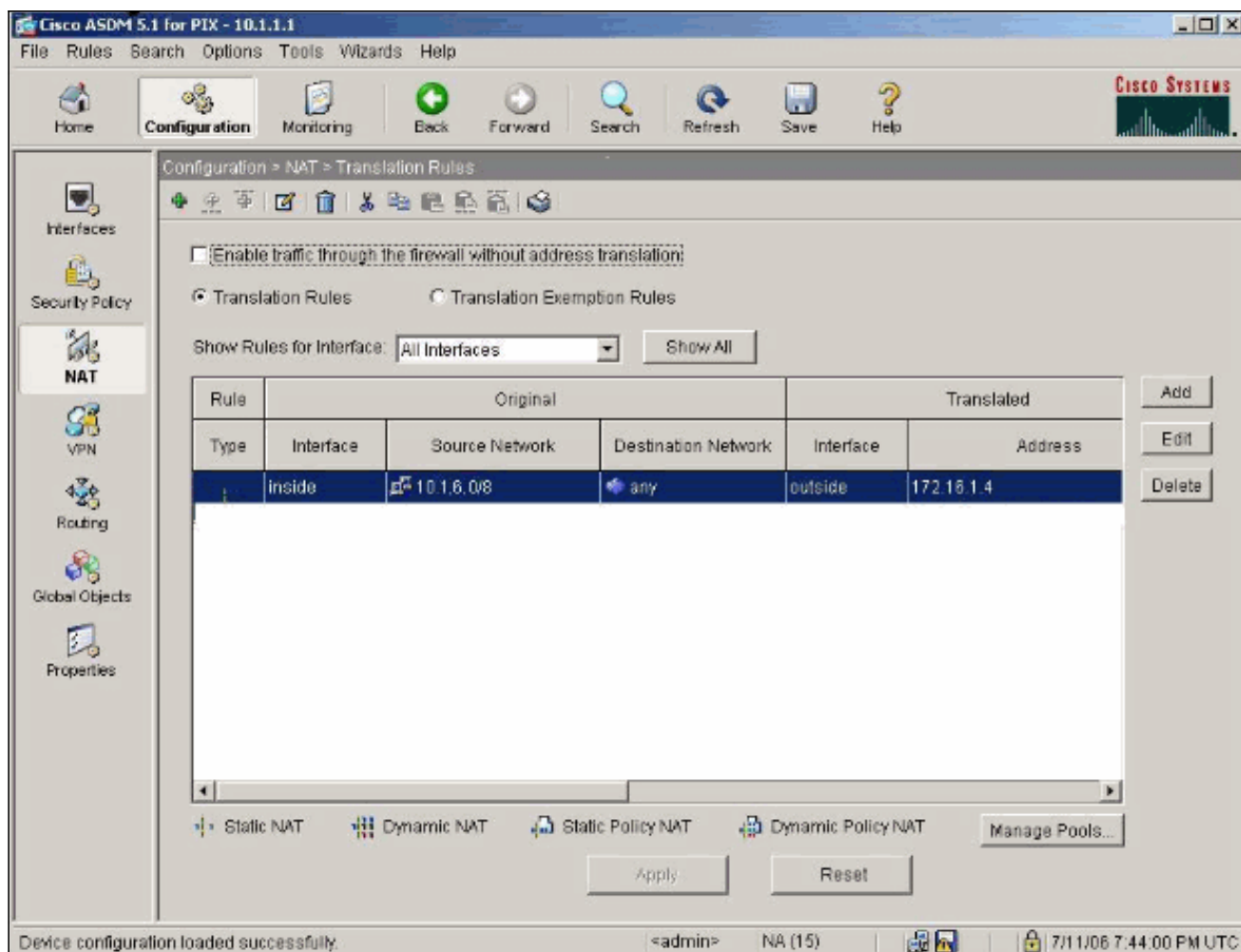
TCP Original port: Translated port:

UDP

Dynamic Address Pool:

Pool ID	Address
1	172.16.1.4

11. Configuration > Features > NAT > Translation Rules の順に選択すると、Translation Rules に変換が表示されます。



PAT を使用するときには、次の事項を考慮する必要があります。

- 別のグローバルアドレスプール内にある IP アドレスは PAT では指定できない。
- PAT は H.323 アプリケーション、キャッシング ネーム サーバ、および Point-to-Point Tunneling Protocol (PPTP; ポイントツーポイント トンネリング プロトコル) と連携して機能させることはできません。PAT は、Domain Name Service (DNS)、FTP と受動 FTP、HTTP、メール、Remote-Procedure Call (RPC; リモート プロシージャ コール)、rshell、Telnet、URL フィルタリング、および発信 traceroute とは連携します。
- ファイアウォール経由でマルチメディア アプリケーションを実行する必要があるときは、PAT を使用しない。マルチメディア アプリケーションは、PAT によって提供されるポート マッピングと競合する可能性があります。
- PIX ソフトウェア リリース 4.2(2) では、逆順で着信する IP データ パケットに対しては PAT 機能が働かない。PIX ソフトウェア リリース 4.2(3) ではこの問題が修正されています。
- **global** コマンドで指定されたグローバルアドレスのプール内の IP アドレスは、すべての外部ネットワークアドレスを PIX でアクセス可能にするために、逆 DNS エントリを必要とする。逆 DNS マッピングを作成するには、アドレスとホスト名のマッピング ファイルにある、各グローバルアドレスに対応する DNS Pointer (PTR) レコードを使用します。PTR エントリがない場合、サイトではインターネット接続が低速または断続的になる可能性があり、FTP 要求では常にエラーが発生します。たとえば、グローバル IP アドレスが 192.168.1.3 で PIX セキュリティ アプライアンスのドメイン名が pix.caguana.com の場合、PTR レコードは次のようになります。

```
3.1.1.175.in-addr.arpa. IN PTR
pix3.caguana.com
4.1.1.175.in-addr.arpa. IN PTR
pix4.caguana.com & so on.
```

[inside ホストから outside ネットワークへのアクセスの制限](#)

有効な変換方式が発信元ホストに対して定義されており、ACL が発信元 PIX インターフェイスに対して定義されていない場合、デフォルトでアウトバウンド接続が許可されます。ただし状況によっては、発信元、宛先、プロトコル、ポートのいずれかまたはすべてに基づいたアウトバウンドアクセス制限が必要です。そのためには、**access-list** コマンドで ACL を設定し、**access-group** コマンドでその ACL を接続発信元の PIX インターフェイスに適用する必要があります。PIX 7.0 ACL は、インバウンドとアウトバウンド両方の方向に適用できます。次に示す手順は、1つのサブネットに関してはアウトバウンド HTTP アクセスを許可する一方で、他のすべてのホストによる Outside への HTTP アクセスを拒否し、それ以外のすべての IP トラフィックをすべての人に対して許可する例です。

1. ACL を定義します。

```
access-list acl_outbound permit tcp 10.1.6.0 255.255.255.0 any eq www
access-list acl_outbound deny tcp any any eq www
access-list acl_outbound permit ip any any
```

注：PIX ACLはCisco IOS®ルータのACLとは異なり、PIXはCisco IOSのようなワイルドカードマスクを使用しません。その代わりに、正規のサブネットマスクを ACL 定義で使用します。Cisco IOS ルータと同様に、PIX の ACL には暗黙的な「deny all」が ACL の最後に存在します。**注：新しいアクセスリストエントリ**は、既存のACEの末尾に追加されます。最初に特定のACEを処理する必要がある場合は、アクセスリスlineキーワードを使用できます。次に、コマンドの要約の例を示します。

```
access-list acl_outbound line 1 extended permit tcp host 10.1.10.225 any
```

2. ACL を内部インターフェイスに適用します。

```
access-group acl_outbound in interface inside
```

3. ASDMを使用して、ステップ1の最初のアクセスリストエントリを設定し、10.1.6.0/24からのHTTPトラフィックを許可します。[Configuration] > [Features] > [Security Policy] > [Access Rules]を選択します。

4. Add をクリックし、このウィンドウに表示される情報を入力し、OK をクリックします。

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:

Time Range
 Time Range:

Syslog
 Default Syslog

Rule Flow Diagram
 Rule applied to traffic incoming to source interface

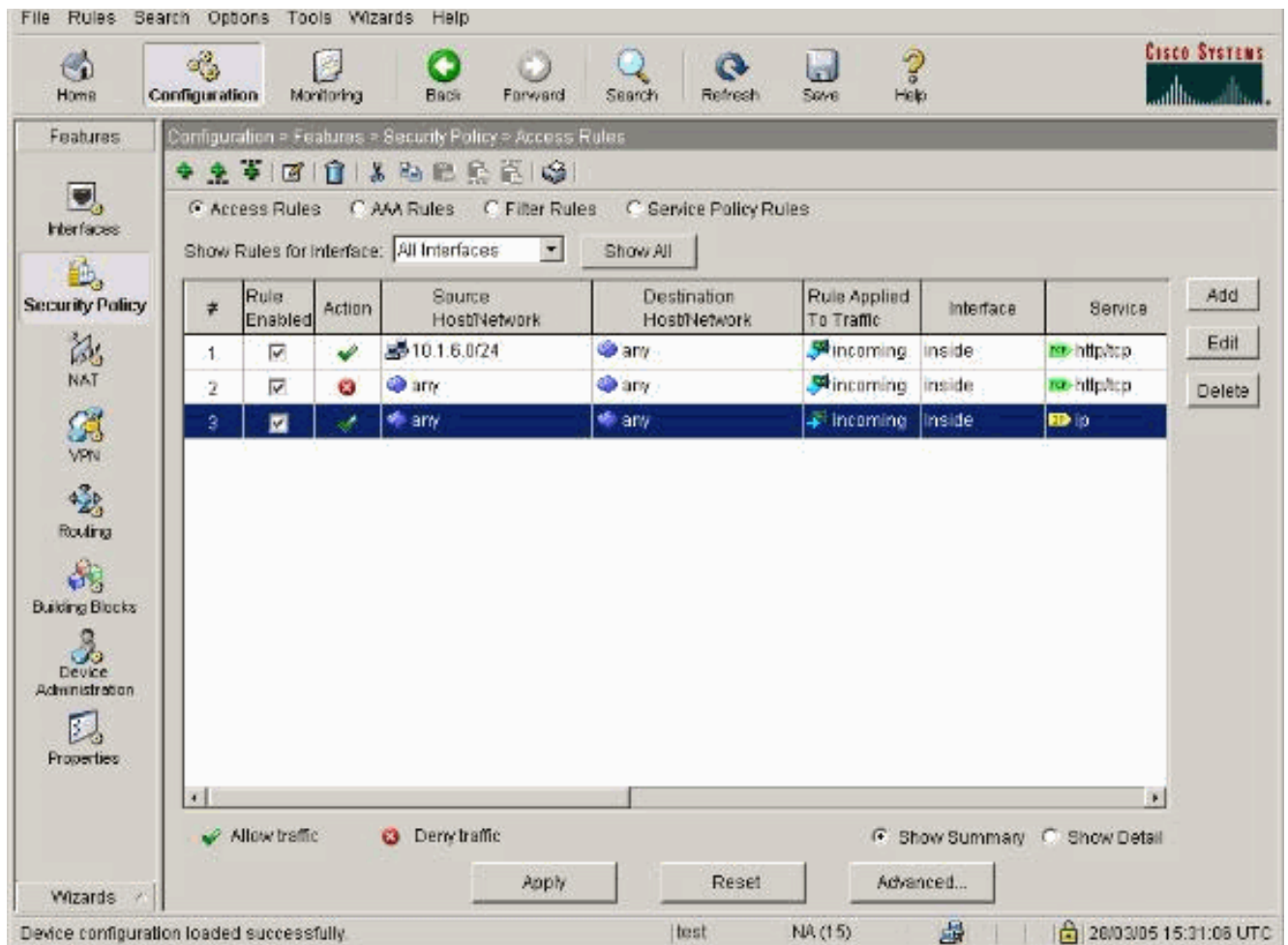
 10.1.6.0/24 → inside → outside → any
 Allow traffic

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

Destination Port
 Service = ...
 Service Group

Please enter the description below (optional):

5. 3 つの access-list エントリを入力したら、**Configuration > Feature > Security Policy > Access Rules** の順に選択し、これらのルールを表示します。



信頼できないホストから信頼できるネットワーク上のホストへのアクセスの許可

ほとんどの組織では、その組織の信頼できるネットワーク内にあるリソースに対して信頼できないホストのアクセスを許可する必要があります。その一般的な例は、社内 Web サーバです。デフォルトでは、PIX は外部ホストから内部ホストへの接続を拒否します。NAT 制御モードでこの接続を許可するには、**static** コマンドを **access-list** コマンドおよび **access-group** コマンドと組み合わせて使用します。NAT 制御がデisableになっている場合、変換を行わないのであれば、**access-list** コマンドと **access-group** コマンドのみが必要です。

access-group コマンドで ACL をインターフェイスに適用します。このコマンドにより ACL がインターフェイスに関連付けられ、特定の方向に流れるトラフィックが検査されます。

Inside ホストの外部へのアクセスを許可する **nat** および **global** コマンドとは対照的に、**static** コマンドでは、適切な ACL/グループが追加されている場合、両方向の変換が作成され、Inside ホストによる外部へのアクセスと Outside ホストによる内部へのアクセスが許可されます。

このドキュメントで示した PAT の設定例では、Outside ホストからのグローバルアドレスへの接続が試みられると、そのアドレスが多数の Inside ホストに使用されてしまう可能性があります。**static** コマンドでは 1 対 1 のマッピングが作成されます。**access-list** コマンドでは Inside ホストに許可される接続のタイプが定義され、これはセキュリティレベルの低いホストが高いホストに接続する場合には常に必要です。**access-list** コマンドはポートとプロトコルの両方に基づき、またシステム管理者の裁量に基づいてアクセスを緩やかに許容したり、逆に厳しく制限したりできます。

このドキュメント内の「[ネットワークダイアグラム](#)」では、これらのコマンドを使用して、すべての信頼できないホストが Inside Web サーバに接続でき、信頼できないホスト 192.168.1.1 が同じマシン上の FTP サービスにアクセスできるように PIX を設定する例を示しています。

[PIX バージョン 7.0 以降での ACL の使用](#)

PIX ソフトウェア バージョン 7.0 以降で、ACL を使用して次の手順を実行します。

1. NAT 制御がイネーブルになっている場合、Inside Web サーバに対して、Outside アドレスまたはグローバルアドレスへのスタティックアドレス変換を定義します。

```
static (inside, outside) 172.16.1.16 10.16.1.16
```

2. どのホストがどのポートを使用して Web/FTP サーバに接続できるかを定義します。

```
access-list 101 permit tcp any host 172.16.1.16 eq www
access-list 101 permit tcp host 192.168.1.1 host 172.16.1.16 eq ftp
```

3. アクセスリストを、アクセスグループを使って外部インターフェイスに適用します。

```
access-group 101 in interface outside
```

4. ASDM を使用してこのスタティック変換を作成するには、**Configuration > Features > NAT** の順に選択して、**Add** をクリックします。
5. 発信元インターフェイスとして **inside** を選択し、スタティック変換を作成する対象である内部アドレスを入力します。
6. **Static** を選択し、変換先 Outside アドレスを IP address フィールドに入力します。[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

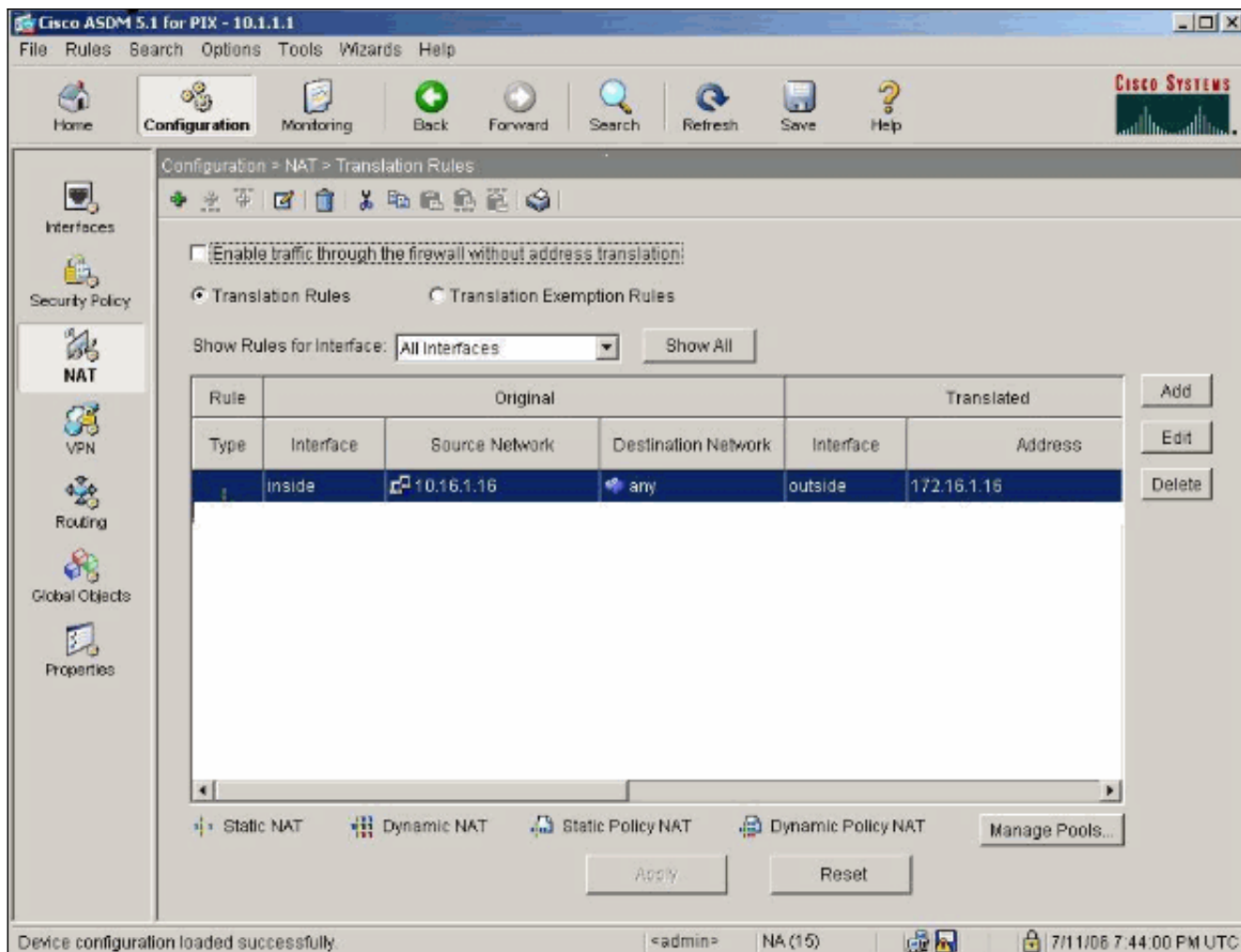
TCP Original port: Translated port:

UDP

 Dynamic Address Pool:

Pool ID	Address

7. Configuration > Features > NAT > Translation Rules の順に選択すると、Translation Rules に変換が表示されます。



8. 「[Inside ホストから Outside ネットワークへのアクセスの制限](#)」の手順を使用して、**access-list** のエントリを入力します。注：これらのコマンドを実装する場合は注意してください。**access-list 101 permit ip any any** コマンドを実装すると、アクティブな変換がある限り、信頼できないネットワーク上の任意のホストが、信頼できるネットワークの任意のホストに IP を使用してアクセスできます。

特定のホストおよびネットワークでの NAT の無効化

NAT 制御を使用し、Inside ネットワーク上にパブリックアドレスが存在し、特定の Inside ホストが変換なしで Outside にアクセスできるようにする必要がある場合は、**nat 0** または **static** コマンドを使用して、これらのホストに対して NAT をディセーブルにすることができます。

nat コマンドの例を次に示します。

```
nat (inside) 0 10.1.6.0 255.255.255.0
```

ASDM を使用して特定のホスト/ネットワークに対して NAT をディセーブルにするには、次の手順を実行します。

1. **Configuration > Features > NAT** の順に選択し、**Add** をクリックしします。
2. 発信元インターフェイスとして **inside** を選択し、スタティック変換を作成する対象である内部アドレス/ネットワークを入力します。
3. **Dynamic** を選択し、Address Pool には同じアドレスを選択します。[OK] をクリックします。

Edit 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

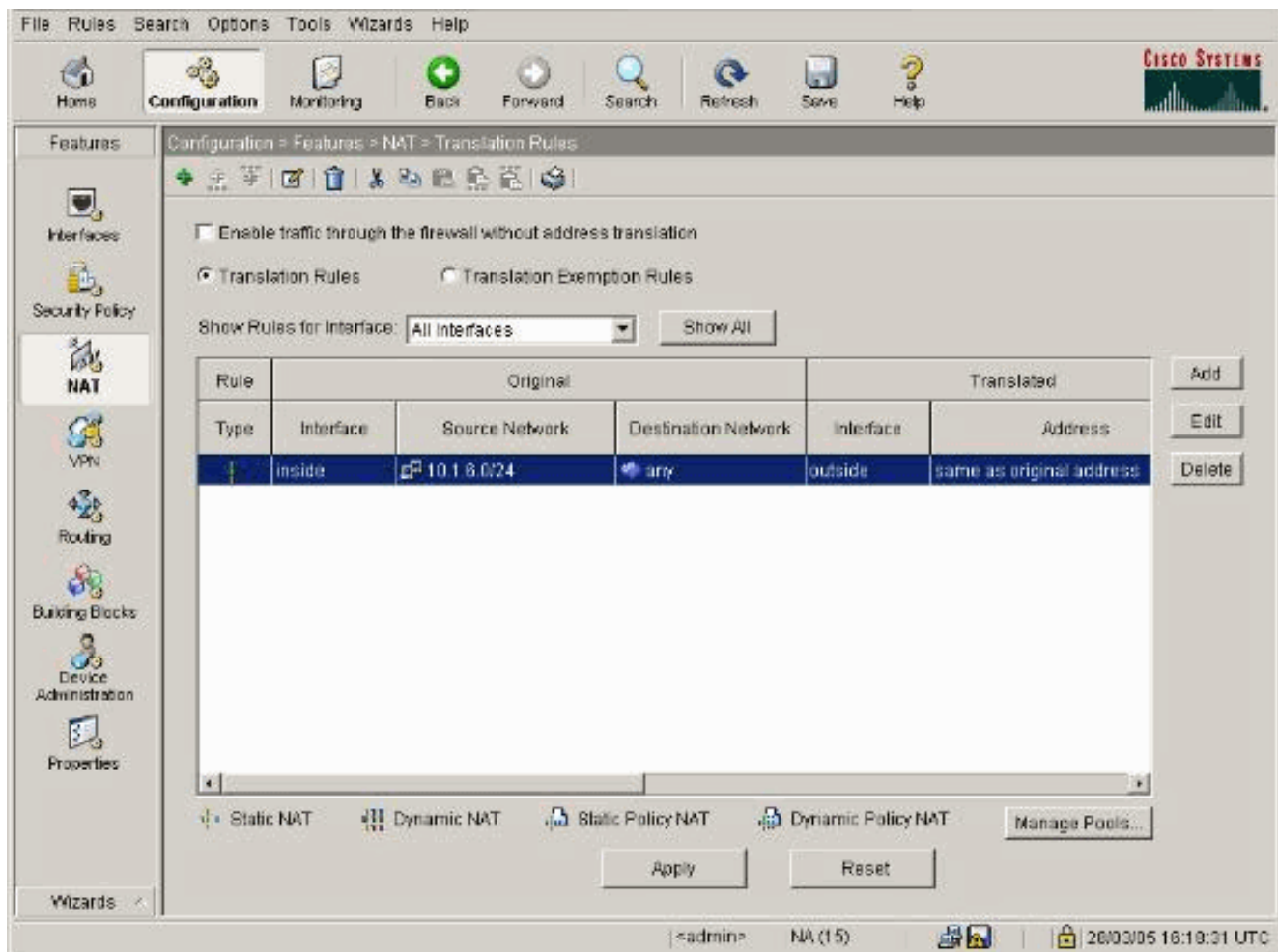
TCP Original port: Translated port:

UDP

Dynamic Address Pool:

Pool ID	Address
N/A	No address pool defined

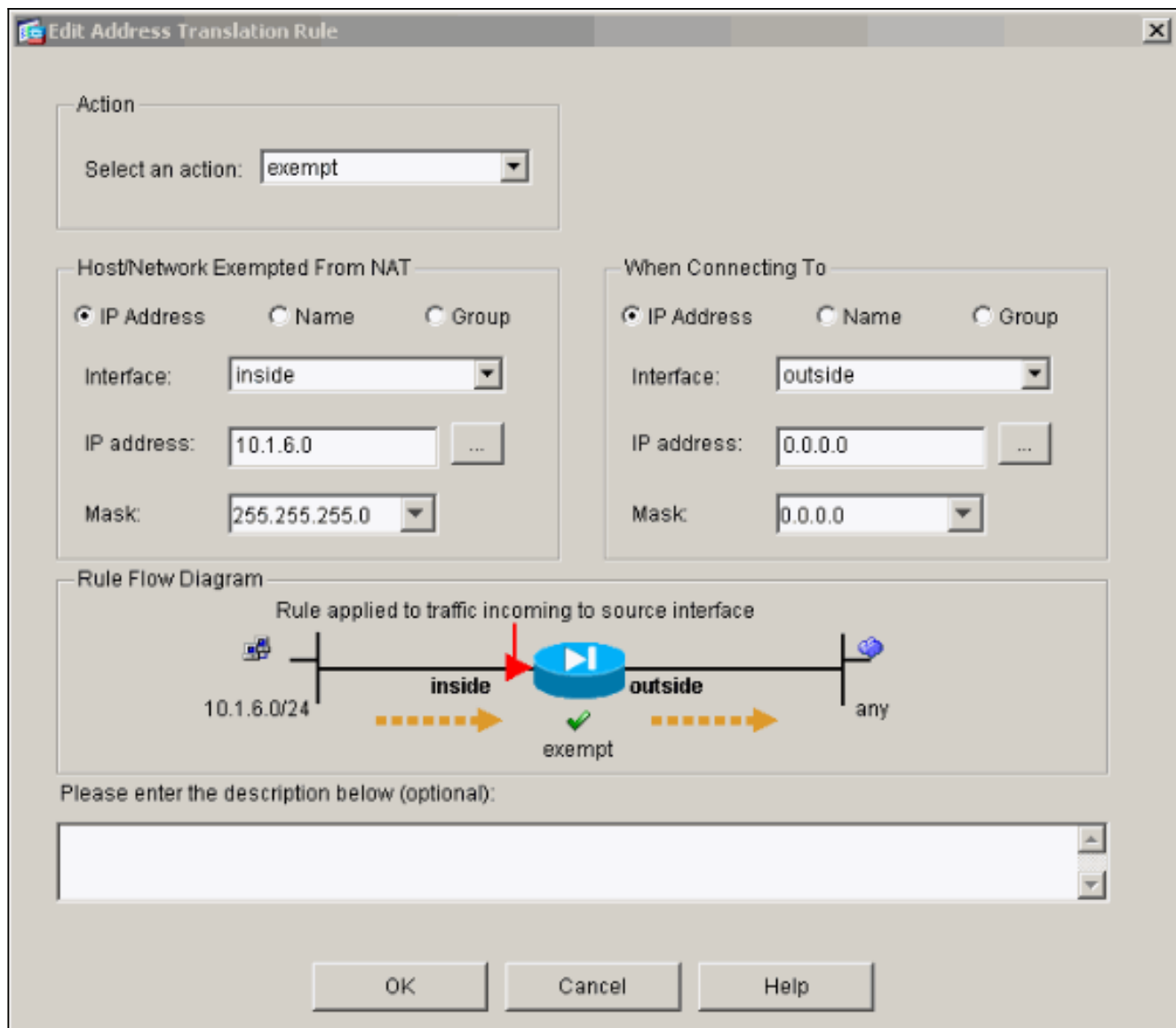
4. Configuration > Features > NAT > Translation Rules の順に選択すると、Translation Rules に新しいルールが表示されます。



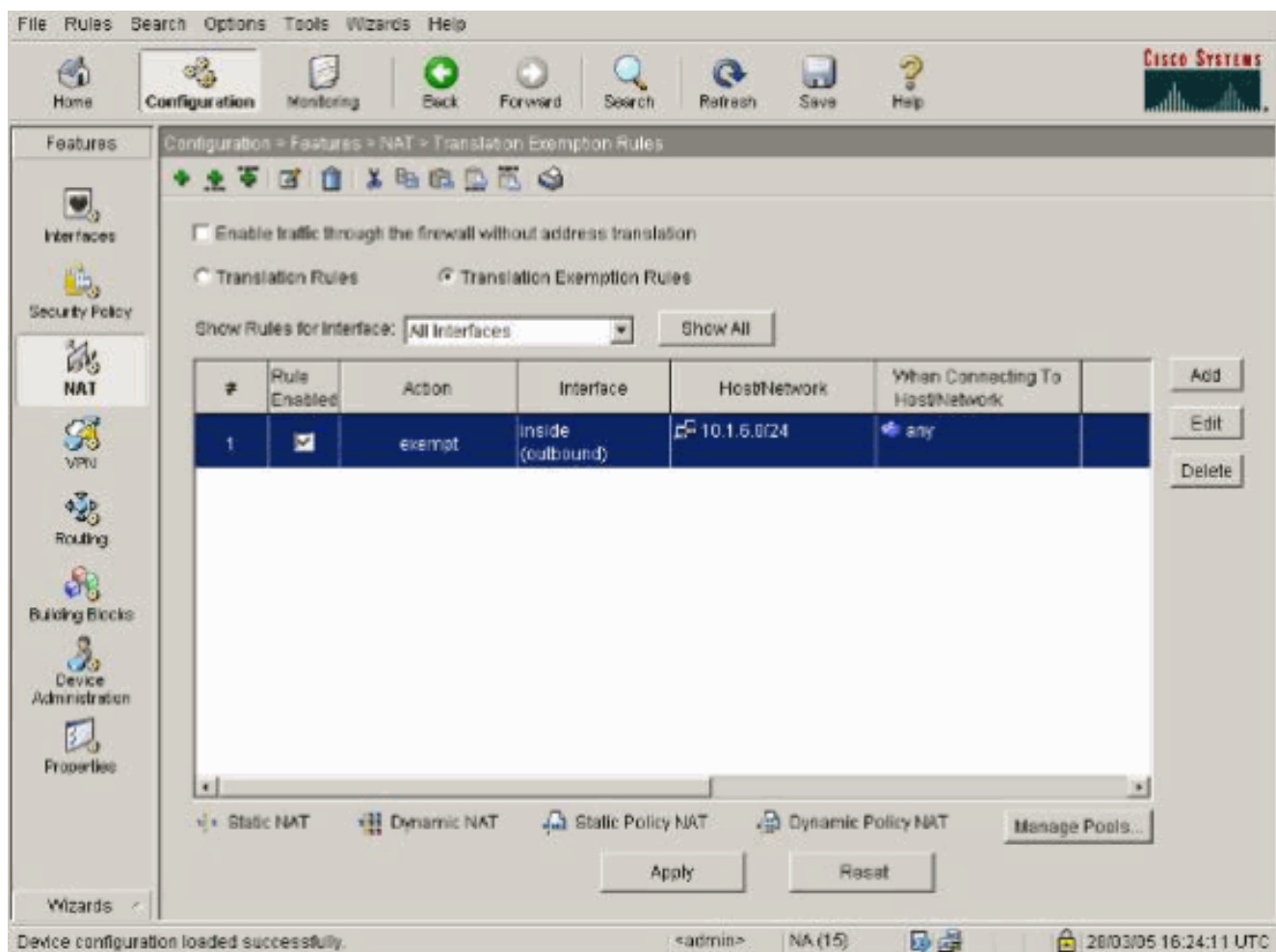
5. (発信元と宛先に基づいて) 変換しないトラフィックをより細かく制御できる ACL を使用する場合は、次のコマンドを使用します。

```
access-list 103 permit ip 10.1.6.0 255.255.255.0 any
nat (inside) 0 access-list 103
```

6. ASDM を使用し、**Configuration > Features > NAT > Translation Rules** の順に選択します。
 7. **Translation Exemption Rules** を選択し、**Add** をクリックしします。次の例に、10.1.6.0/24 ネットワークから任意の場所へのトラフィックを変換から除外する方法を示します。



8. Configuration > Features > NAT > Translation Exemption Rules の順に選択して、新しいルールを表示します。



9. Web サーバに対する **static** コマンドは、次の例に示すように変わります。

```
static (inside, outside) 10.16.1.16 10.16.1.16
```

10. ASDM から、**Configuration > Features > NAT > Translation Rules** の順に選択します。

11. **Translation Rules** を選択し、**Add** をクリックしします。発信元アドレス情報を入力し、**Static** を選択します。IP Address フィールドに同じアドレスを入力します。

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

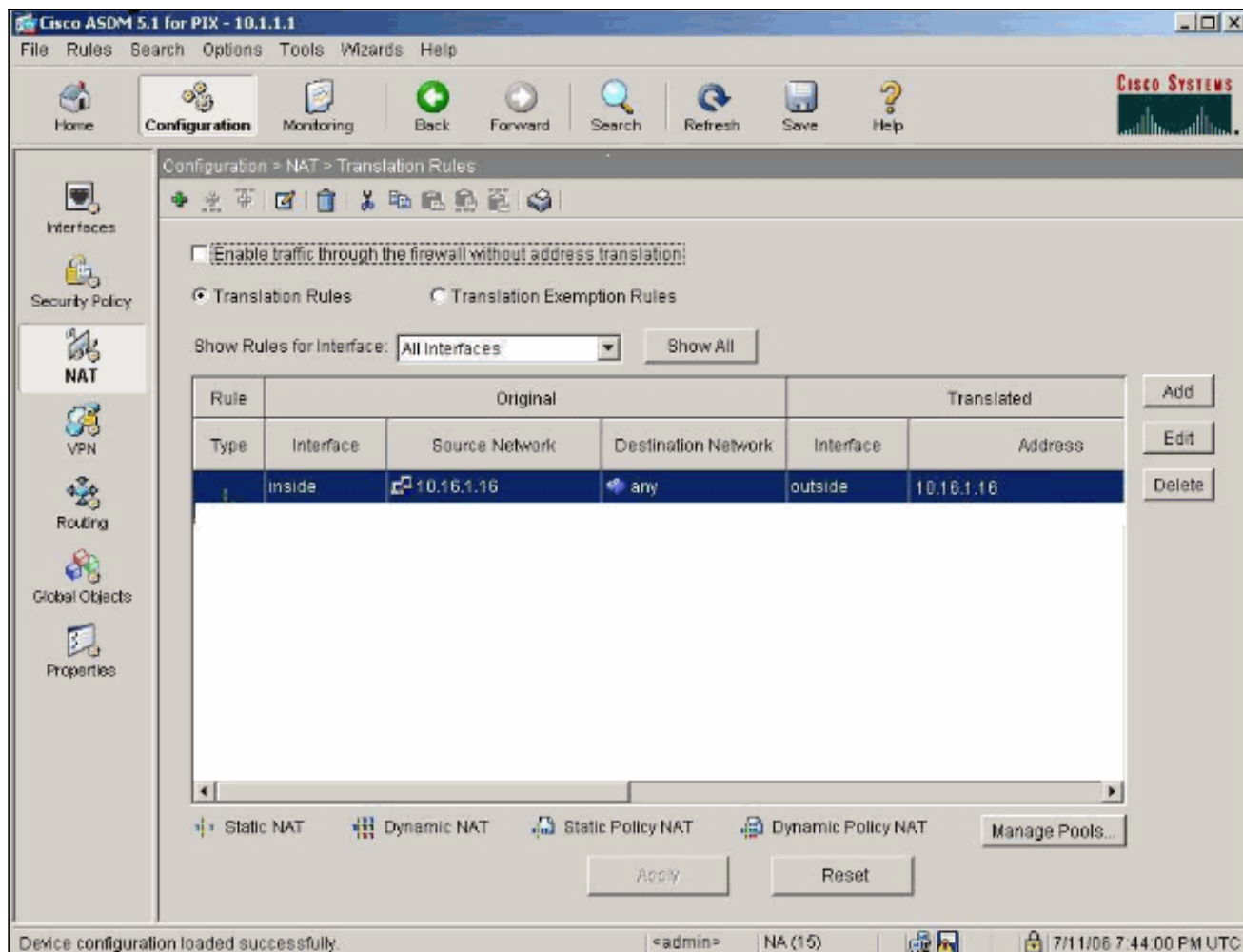
TCP Original port: Translated port:

UDP

 Dynamic Address Pool:

Pool ID	Address

12. Configuration > Features > NAT > Translation Rules の順に選択すると、Translation Rules に変換が表示されます。



13. ACL を使用する場合は、次のコマンドを使用します。

```
access-list 102 permit tcp any host 10.16.1.16 eq www
access-group 102 in interface outside
```

ASDM での ACL の設定についての詳細は、このドキュメントの「[Inside ホストから Outside ネットワークへのアクセスの制限](#)」セクションを参照してください。ネットワーク/マスクを指定しながら nat 0 を使用する場合と、Inside からのみの接続開始を許可するネットワーク/マスクを使う ACL を使用する場合の違いに注意してください。nat 0 とともに ACL を使用すると、インバウンドまたはアウトバウンドトラフィックによる接続の開始が可能になります。PIX インターフェイスを別のサブネットに配置して、到達可能性に問題が発生しないようにする必要があります。

[static を使用したポート リダイレクション \(フォワーディング\)](#)

PIX 6.0 では、ポート リダイレクション (フォワーディング) 機能が追加されたことにより、Outside ユーザが特定の IP アドレス/ポートに接続し、PIX がトラフィックを適切な Inside サーバ/ポートにリダイレクトすることが可能になりました。また、static コマンドが変更されています。共有アドレスを一意のアドレスまたは共有アウトバウンド PAT アドレスにしたり、外部インターフェイスと共有させることができます。この機能は、PIX 7.0 で利用できます。

注：スペースの制限により、コマンドは2行で表示されます。

```
static [(internal_if_name, external_if_name)] {global_ip/interface}local_ip [netmask mask]
[max_conns [emb_limit [norandomseq]]]
```

```
static [(internal_if_name, external_if_name)] {tcp|udp} {global_ip/interface} global_port
local_ip local_port [netmask mask] [max_conns [emb_limit [norandomseq]]]
```

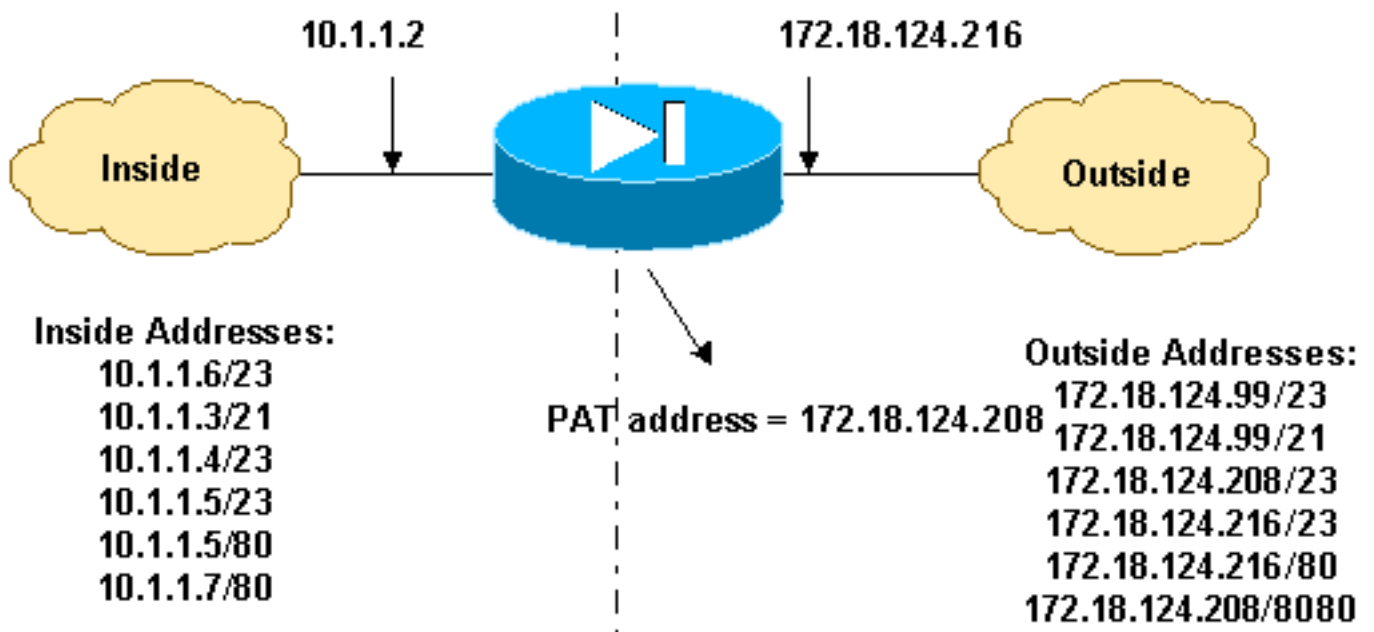
注：スタティックNATが外部IP(global_IP)アドレスを変換に使用する場合、変換が発生する可能性があります。そのため、スタティック変換では IP アドレスではなくキーワード **interface** を使用します。

このネットワークの例でのポート リダイレクション (フォワーディング) は次のようになります。

- 外部ユーザは Telnet 要求を一意的 IP アドレス 172.18.124.99 に送り、PIX はこれを 10.1.1.6 にリダイレクトする。
- 外部ユーザは FTP 要求を一意的 IP アドレス 172.18.124.99 に送り、PIX はこれを 10.1.1.3 にリダイレクトする。
- 外部ユーザは Telnet 要求を PAT アドレス 172.18.124.208 に送り、PIX はこれを 10.1.1.4 にリダイレクトする。
- 外部ユーザは Telnet 要求を PIX Outside IP アドレス 172.18.124.216 に送り、PIX はこれを 10.1.1.5 にリダイレクトする。
- 外部ユーザは HTTP 要求を PIX 外部 IP アドレス 172.18.124.216 に送り、PIX はこれを 10.1.1.5 にリダイレクトする。
- 外部ユーザは HTTP ポート 8080 要求を PAT アドレス 172.18.124.208 に送り、PIX はこれを 10.1.1.7 のポート 80 にリダイレクトする。

この例では、ACL 100を使用して、内部から外部への一部のユーザのアクセスをブロックします。この手順はオプションです。ACL を設定しなければ、すべてのトラフィックは発信が許可されます。

ネットワークダイアグラム：ポートリダイレクション (フォワーディング)



PIX 部分設定 - ポートリダイレクション

次に抜粋した設定では、スタティック ポート リダイレクション (フォワーディング) の使用方法を示しています。「[ポート リダイレクション \(フォワーディング \) のネットワークダイアグラ](#)

[△](#)」を参照してください。

PIX 7.x 設定の抜粋：ポートリダイレクション (フォワーディング)

```
fixup protocol ftp 21
!--- Use of an outbound ACL is optional. access-list 100
permit tcp 10.1.1.0 255.255.255.128 any eq www access-
list 100 deny tcp any any eq www access-list 100 permit
tcp 10.0.0.0 255.0.0.0 any access-list 100 permit udp
10.0.0.0 255.0.0.0 host 172.18.124.100 eq domain access-
list 101 permit tcp any host 172.18.124.99 eq telnet
access-list 101 permit tcp any host 172.18.124.99 eq ftp
access-list 101 permit tcp any host 172.18.124.208 eq
telnet access-list 101 permit tcp any host
172.18.124.216 eq telnet access-list 101 permit tcp any
host 172.18.124.216 eq www access-list 101 permit tcp
any host 172.18.124.208 eq 8080 interface Ethernet0
nameif outside security-level 0 ip address
172.18.124.216 255.255.255.0 ! interface Ethernet1
nameif inside security-level 100 ip address 10.1.1.2
255.255.255.0 ! global (outside) 1 172.18.124.208 nat
(outside) 1 0.0.0.0 0.0.0.0 0 0 static (inside,outside)
tcp 172.18.124.99 telnet 10.1.1.6 telnet netmask
255.255.255.255 0 0 static (inside,outside) tcp
172.18.124.99 ftp 10.1.1.3 ftp netmask 255.255.255.255 0
0 static (inside,outside) tcp 172.18.124.208 telnet
10.1.1.4 telnet netmask 255.255.255.255 0 0 static
(outside) tcp interface telnet 10.1.1.5 telnet
netmask 255.255.255.255 0 0 static (inside,outside) tcp
interface www 10.1.1.5 www netmask 255.255.255.255 0 0
static (inside,outside) tcp 172.18.124.208 8080 10.1.1.7
www netmask 255.255.255.255 0 0 !!--- Use of an outbound
ACL is optional. access-group 100 in interface inside
access-group 101 in interface outside
```

注：PIX/ASAにsysopt noproxyarp outsideコマンドが設定されている場合、ファイアウォールはPIX/ASAでproxyarpおよびスタティックNAT変換を実行できません。これを解決するには、PIX/ASA設定でsysopt noproxyarp outsideコマンドを削除し、gratuitous ARPを使用してARPエントリを更新します。これにより、スタティックNATエントリが正常に動作できるようになります。

この手順は、ポートリダイレクション (フォワーディング) を設定する方法の例で、外部ユーザはTelnet 要求を一意的 IP アドレス 172.18.124.99 に送信でき、PIX はこれを 10.1.1.6 にリダイレクトします。

1. ASDM を使用し、**Configuration > Features > NAT > Translation Rules** の順に選択します。
2. **Translation Rules** を選択し、**Add** をクリックします。
3. Source Host/Network には、Inside IP アドレスの情報を入力します。
4. Translate Address To では、**Static** を選択し、Outside IP アドレスを入力して、**Redirect port** にチェックマークを付けます。
5. 変換前および変換後のポート情報を入力します (この例ではポート 23 が維持されます)。
[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

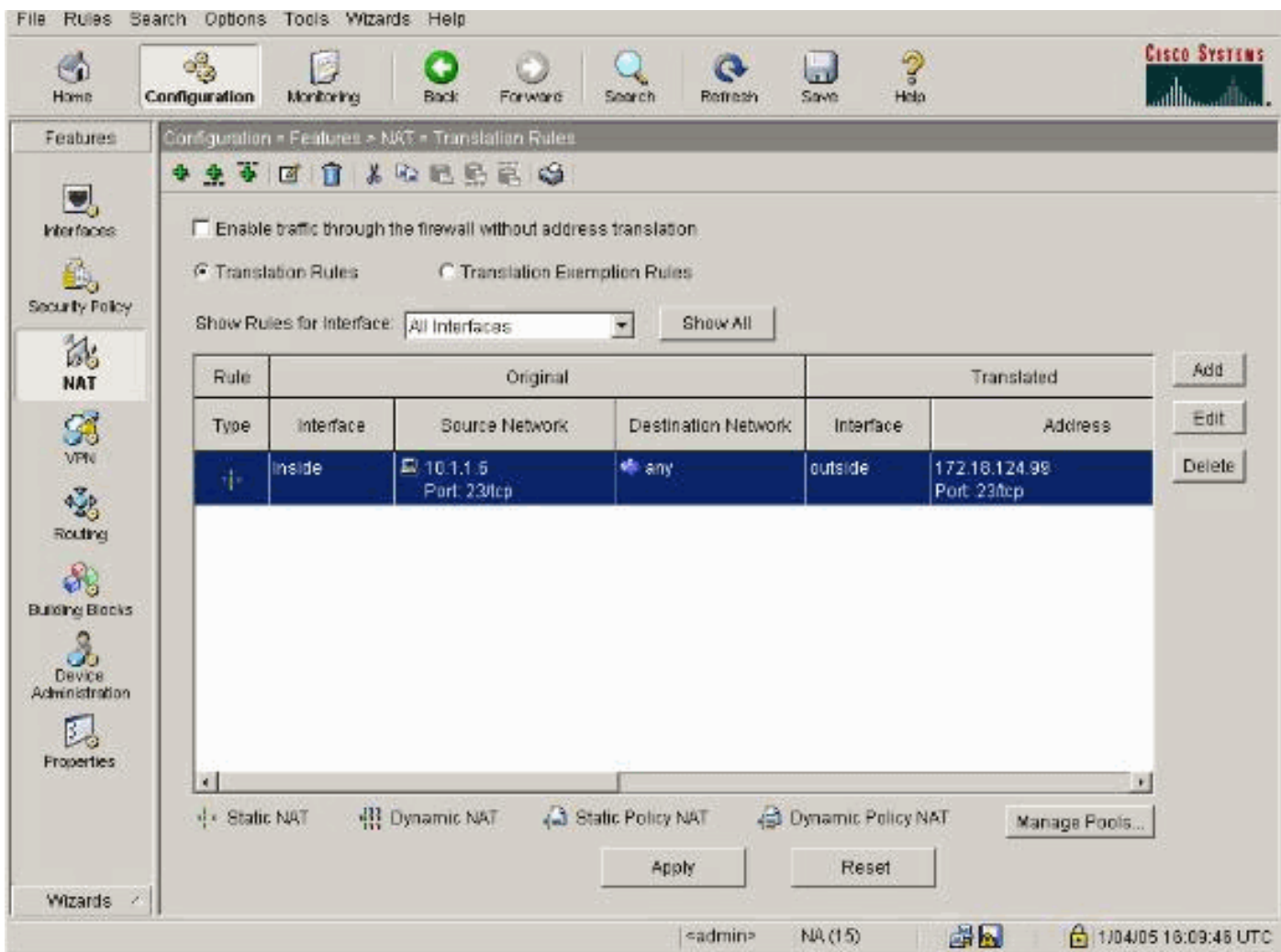
TCP Original port: Translated port:

UDP

 Dynamic Address Pool:

Pool ID	Address

Configuration > Features > NAT > Translation Rules の順に選択すると、Translation Rules に変換が表示されます。



static を使用した TCP/UDP セッションの制限

TCP または UDP セッションを PIX/ASA 内に配置されている内部サーバに制限する必要がある場合は、**static** コマンドを使用します。

サブネット全体の同時 TCP および UDP 接続の最大数を指定します。デフォルトは 0 で、接続が無制限であることを意味します (アイドル状態の接続は、**timeout conn** コマンドにより指定されたアイドル タイムアウトが経過した後に関閉じられます)。このオプションは、Outside NAT に適用されません。セキュリティ アプライアンスは、セキュリティ レベルの高いインターフェイスからセキュリティ レベルの低いインターフェイスへの接続のみを追跡します。

初期接続数を制限すると、DoS 攻撃からの保護になります。セキュリティ アプライアンスは、初期制限を使用して TCP インターセプトをトリガします。これにより、TCP SYN パケットでインターフェイスをフラグディングすることにより行われる DoS 攻撃から Inside システムが保護されます。初期接続は、発信元と宛先の間で必要なハンドシェイクを完了していない接続要求です。このオプションは、Outside NAT に適用されません。TCP インターセプト機能は、セキュリティ レベルの高いホストまたはサーバにのみ適用されます。Outside NAT に初期制限を設定した場合、初期制限は無視されます。

以下に、いくつかの例を示します。

```
ASA(config)#static (inside,outside) tcp 10.1.1.1 www 10.2.2.2 www tcp 500 100
!--- The maximum number of simultaneous tcp connections the local IP !--- hosts are to allow is
500, default is 0 which means unlimited !--- connections. Idle connections are closed after the
```


time specified !--- by the **timeout conn** command !--- The maximum number of embryonic connections per host is **100**.

%PIX-3-201002:{static|xlate} global_addressの接続が多すぎます！ ens nconns

これは接続に関連したメッセージです。このメッセージがログに記録されるのは、指定のスタティック アドレスへの最大接続数を超えた場合です。econns 変数は初期接続の最大数で、nconns は static または xlate に許可されている接続の最大数です。

スタティック アドレスへの接続に課せられている制限を確認するには、**show static** コマンドを使用することを推奨いたします。この制限は設定可能です。

%ASA-3-201011:インターフェイスOutsideの10.1.26.51/2393から10.0.86.155/135への着信パケットの接続制限が1000/1000を超えました

このエラーメッセージは、Cisco Bug ID [CSCsg52106\(登録ユーザ専用\)](#)に起因します。詳細は、このバグを参照してください。

時間ベースのアクセス リスト

時間範囲を作成してもデバイスへのアクセスは制限されません。**time-range** コマンドで定義されるのは時間範囲だけです。時間範囲を定義してから、これをトラフィック ルールやアクションに適用できます。

時間ベース ACL を実装するには、**time-range** コマンドを使用して、日および曜日の特定の時間を定義します。続いて **with the access-list extended time-range** コマンドを使用して、その時間範囲を ACL にバインドします。

時間範囲はセキュリティ アプライアンスのシステム クロックに基づきます。ただし、この機能は NTP 同期とともに使用すると最も効果的です。

時間範囲を作成し、時間範囲の設定モードに入ると、**absolute** および **periodic** コマンドを使用して時間範囲のパラメータを定義できます。**time-range** コマンドの **absolute** キーワードと **periodic** キーワードをデフォルト設定に復元するには、時間範囲設定モードで **default** コマンドを使用します。

時間ベース ACL を実装するには、**time-range** コマンドを使用して、日および曜日の特定の時間を定義します。続いて **with the access-list extended** コマンドを使用して、時間範囲を ACL にバインドします。次の例では、「Sales」という名前の ACL を「New York Minute」という名前の時間範囲にバインドしています。

この例では、「New York Minute」という名前の時間範囲を作成し、時間範囲設定モードに入ります。

```
hostname(config)#time-range New_York_Minute
hostname(config-time-range)#periodic weekdays 07:00 to 19:00
hostname(config)#access-list Sales line 1 extended deny ip any any time-range New_York_Minute
hostname(config)#access-group Sales in interface inside
```

テクニカルサポートのサービス リクエストをオープンする際に

収集する情報

依然としてサポートが必要で、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場合は、ご使用の PIX セキュリティ アプライアンスのトラブルシューティングのために、必ず下記の情報を添付するようにしてください。

- 問題の説明と関連するトポロジの詳細
- サービス リクエストをオープンする前のトラブルシューティングに使用した手順
- `show tech-support` コマンドの出力
- `logging buffered debugging` コマンド実行後の `show log` コマンドの出力、あるいは、問題を示す画面キャプチャ (採取されている場合)

収集したデータは、圧縮しないプレーン テキスト形式 (.txt) でサービス リクエストに添付してください。情報をサービス リクエストに添付するには、[TAC Service Request Tool](#) (登録ユーザ専用) を使用します。[TAC Service Request Tool](#) (登録ユーザ専用) にアクセスできない場合は、情報を Eメールの添付ファイルとし、メッセージの件名にサービス リクエスト番号を付けて attach@cisco.com 宛てに送信してください。一部ツールについては、ゲスト登録のお客様にはアクセスできない場合がありますことを、ご了承ください。

関連情報

- [PIX セキュリティ アプライアンスに関するサポート ページ](#)
- [PIX コマンド リファレンス](#)
- [Cisco Adaptive Security Device Manager \(ASDM\) Troubleshoot and Alerts](#)
- [Requests for Comments \(RFCs\)](#)
- [テクニカル サポートとドキュメント – Cisco Systems](#)