PIX/ASA 7.x および FWSM： NAT および PAT ステートメント

目次

概要

このドキュメントでは、Cisco PIX/ASA セキュリティ アプライアンスでの基本的なネットワーク アドレス変換（NAT）とポート アドレス変換（PAT）の設定の例を紹介しています。 また、簡略化したネットワーク ダイアグラムも掲載されています。 詳細は、使用している PIX/ASA ソフトウェア バージョンの PIX/ASA のドキュメントを参照してください。

PIX 5.x 以降での **nat**、**global**、**static**、**conduit**、**access-list** の各コマンドおよびポート リダイレクション（フォワーディング）についての詳細は、『PIX での nat、global、static、conduit、および access-list の各コマンドとポート リダイレクション（フォワーディング）の使用方法』を参

照してください。

Cisco Secure PIX Firewall での基本的な NAT と PAT の設定例についての詳細は、『Cisco Secure PIX Firewall での NAT と PAT の使用』を参照してください。

ASA バージョン 8.3 以降での NAT 設定の詳細については、『NAT について』を参照してください。

注: 透過モードでの NAT は PIX/ASA バージョン 8.x 以降でサポートされています。 詳細は、『透過モードでの NAT』を参照してください。

前提条件

要件

このドキュメントの読者には、Cisco PIX/ASA セキュリティ アプライアンスに関する知識が必要です。

使用するコンポーネント

このドキュメントの情報は 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 以降に基づくものです。

注: このドキュメントは PIX/ASA バージョン 8.x で再検証されています。

注: このドキュメントで使用されているコマンドは、Firewall Service Module（FWSM）に適用可能です。

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。

nat-control コマンド

PIX/ASA での **nat-control** コマンドにより、ファイアウォールを通過するすべてのトラフィックには、特定の変換エントリ（マッチする **global** 設定がある **nat** 設定、または **static** 設定）が必要であることが指定されます。 **nat-control** コマンドを使用すると、変換の動作がバージョン 7.0 より前の PIX ファイアウォールと同じになります。 PIX/ASA バージョン 7.0 以降のデフォルト設定は、**no nat-control** コマンドの指定です。 PIX/ASA バージョン 7.0 以降では、**nat-control** コマンドを発行することにより動作を変更できます。

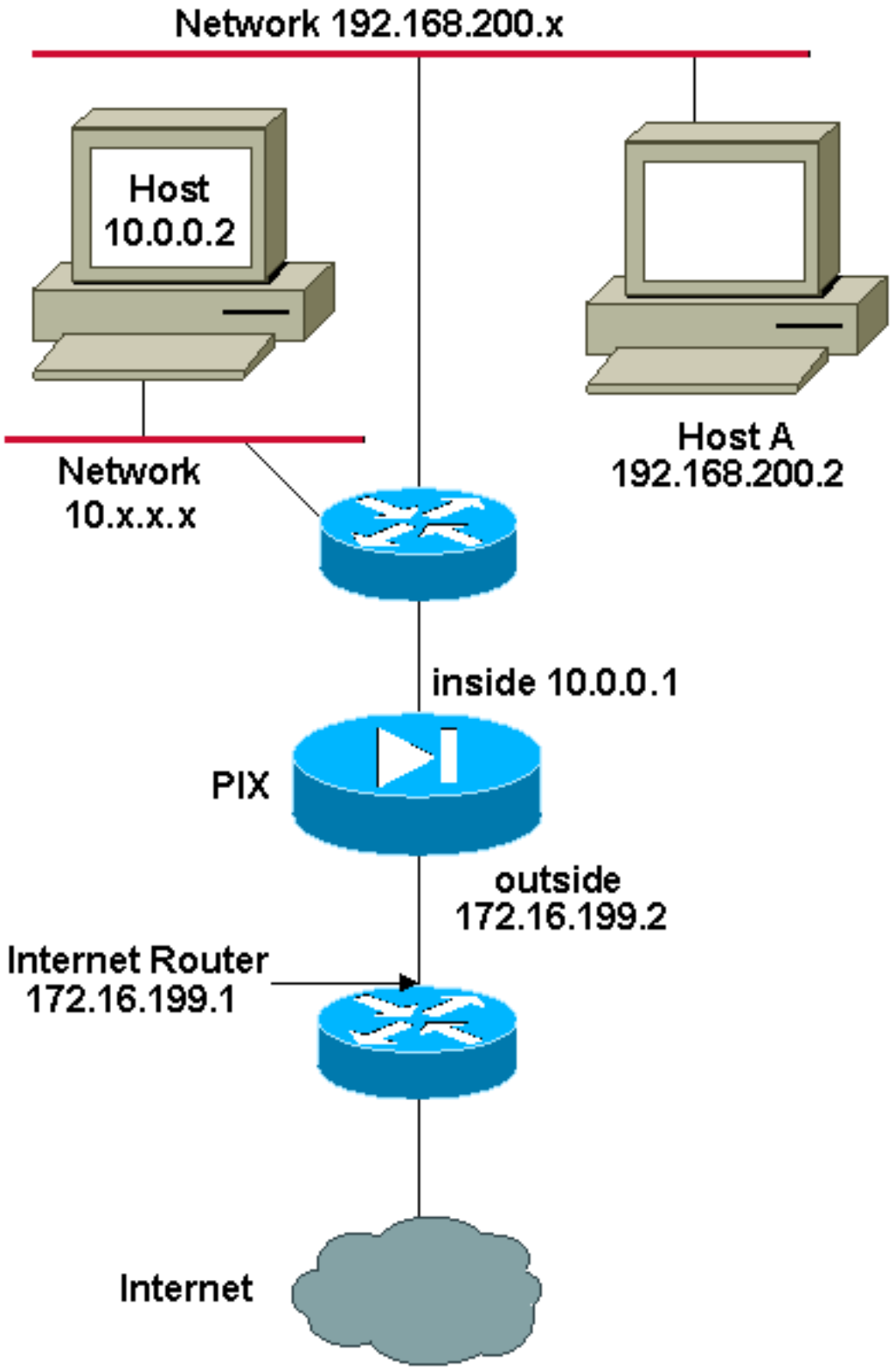
nat-control がディセーブルになっていると、コンフィギュレーションに特定の変換エントリがなくても、PIX/ASA ではより高セキュリティのインターフェイスから、より低セキュリティのインターフェイスにパケットの転送が行われます。 より低セキュリティのインターフェイスから、より高セキュリティのインターフェイスにトラフィックを渡すには、トラフィックの許可にアクセ

ス リストを使用します。 これで、PIX/ASA はトラフィックの転送を行います。 このドキュメントでは、**nat-control** がイネーブルにされた状態での PIX/ASA セキュリティ アプライアンスの動作に焦点を当てています。

注: PIX/ASA で nat-control 設定を削除または無効化するには、セキュリティ アプライアンスからすべての NAT 設定を削除する必要があります。 一般的には、NAT 制御をオフにする前に、NAT を削除する必要があります。 期待どおりに動作させるには、PIX/ASA で NAT を再設定する必要があります。

nat 0 を使用した複数の NAT 文

ネットワーク図



注: 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 RFC 1918 で、 ラボ環境で使用されたアドレスです。

この例では、172.16.199.1 ~ 172.16.199.63 のアドレス範囲が ISP からネットワーク管理者に提供されています。 ネットワーク管理者は、インターネット ルータの Inside インターフェイスに 172.16.199.1 を割り当て、PIX/ASA の Outside インターフェイスに 172.16.199.2 を割り当てると判断します。

ネットワーク管理者にはネットワーク 192.168.200.0/24 に割り当てられた Class C アドレスがあり、インターネットにアクセスするためにこれらのアドレスを使用する複数のワークステーショ

ンがあります。 これらのワークステーションはアドレス変換の対象ではありません。 ところが、新しいワークステーションには 10.0.0.0/8 ネットワークのアドレスが割り当てられるため、これらには変換が必要です。

このネットワーク設計を実現するには、次の出力に示されているように、ネットワーク管理者は PIX/ASA のコンフィギュレーションに 2 つの NAT 設定と 1 つのグローバル プールを使用する必要があります。

```
global (outside) 1 172.16.199.3-172.16.199.62 netmask 255.255.255.192

nat (inside) 0 192.168.200.0 255.255.255.0 0 0

nat (inside) 1 10.0.0.0 255.0.0.0 0 0
```

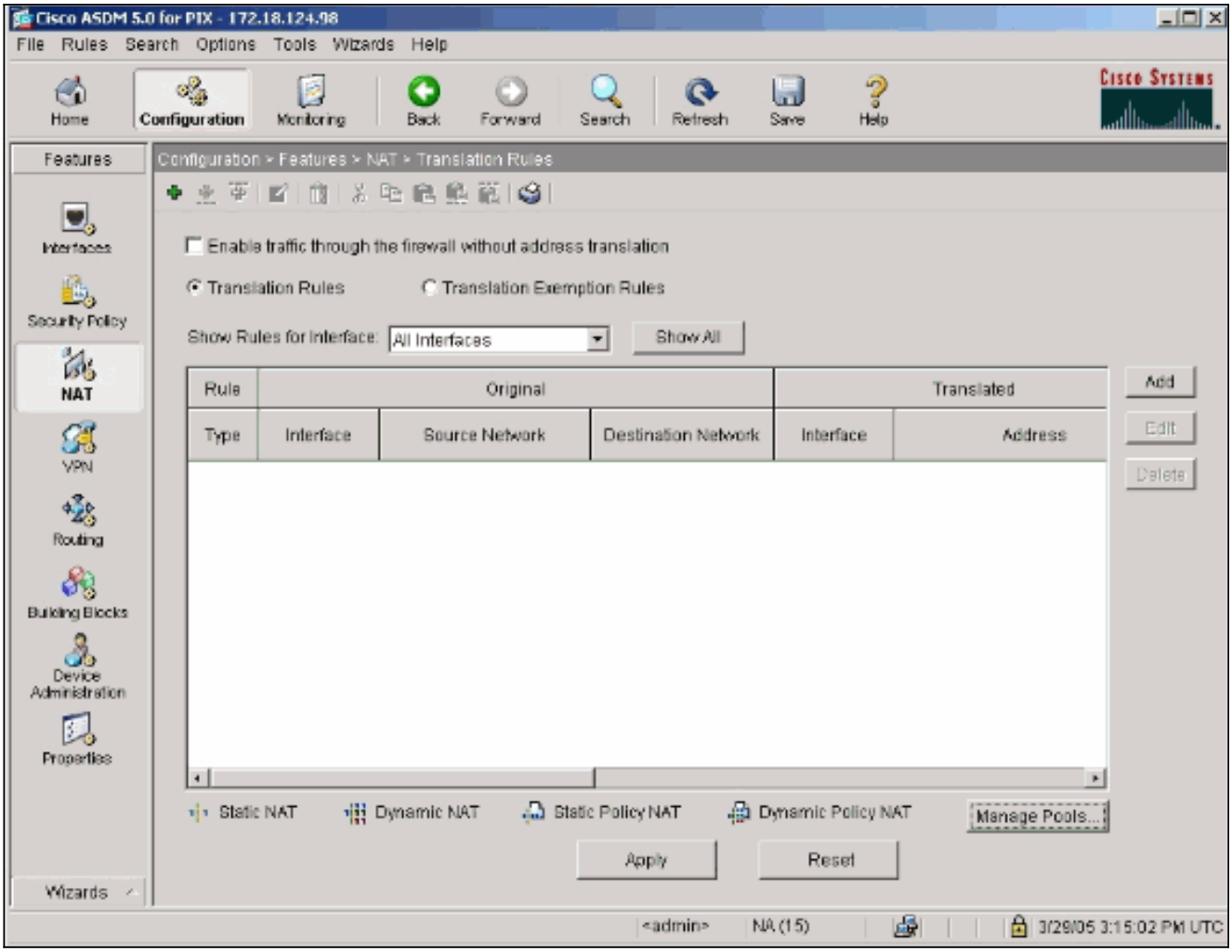
このコンフィギュレーションでは、192.168.200.0/24 ネットワークからのアウトバウンド トラフィックで送信元アドレスが変換されるものはありません。 この場合、10.0.0.0/8 ネットワークからの送信元アドレスが、172.16.199.3 ~ 172.16.199.62 の範囲からのアドレスに変換されます。

下記の手順は、Adaptive Security Device Manager（ASDM）を使用して同じ設定を適用する方法を示しています。

注: 設定の変更には CLI または ASDM のいずれかを使用します。 CLI と ASDM の両方を設定の変更に使用すると、ASDM によって適用される設定に関して重大な誤動作が発生します。 これは不具合ではなく、ASDM の動作によるものです。

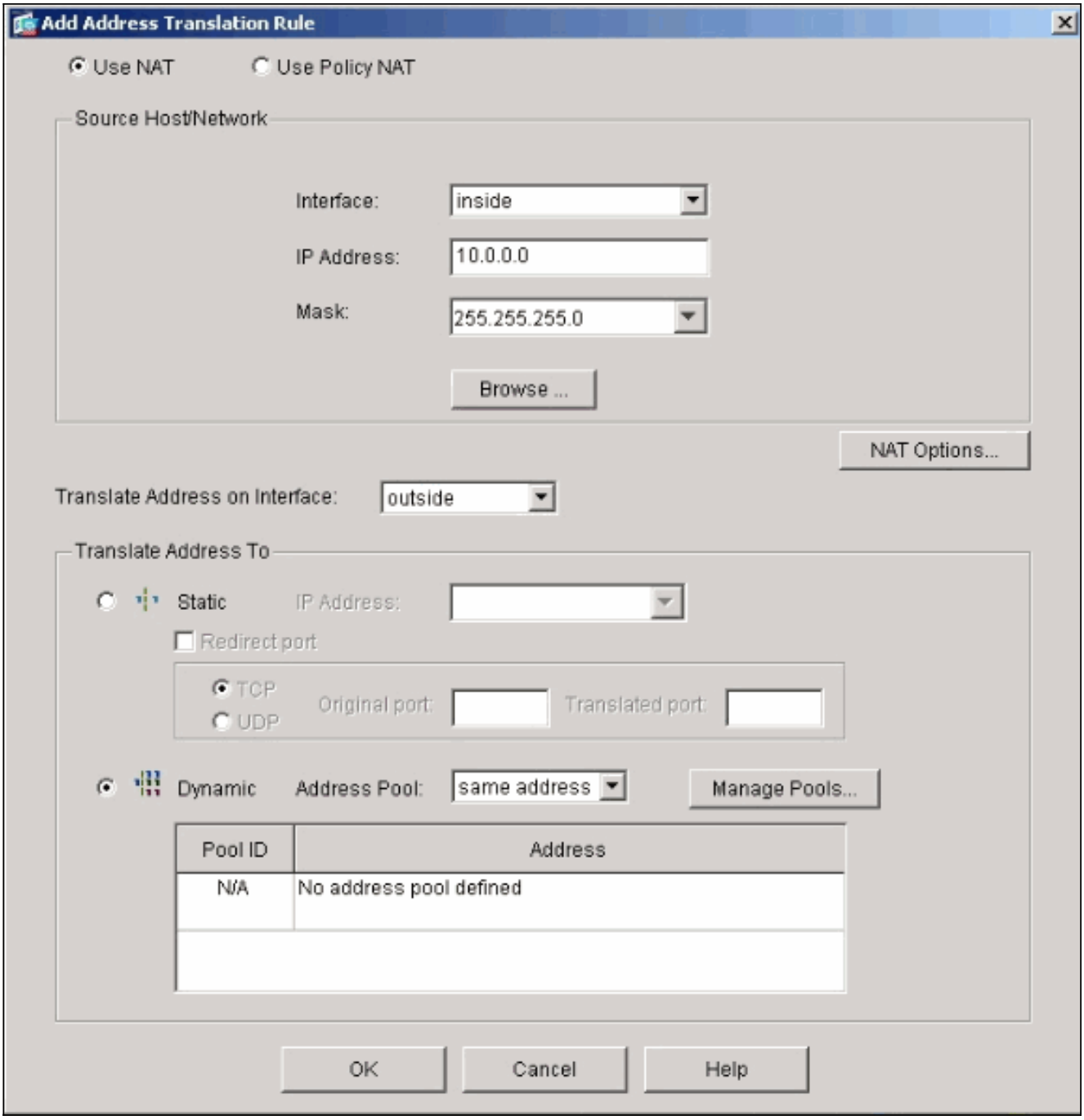
注: ASDM をオープンすると、PIX/ASA から現在のコンフィギュレーションがインポートされ、変更の作成や適用を行った際には、そのコンフィギュレーションに基づいて動作します。 ASDM セッションがオープンしている場合に PIX/ASA に変更が加えられると、ASDM は、PIX/ASA の現在のコンフィギュレーションと見なしているものでは動作しなくなります。 CLI でコンフィギュレーションを変更する場合は、必ず ASDM セッションをすべてクローズするようにしてください。 GUI で作業する場合には、ASDM を再オープンします。

1. ASDM を起動して、Configuration タブに移動し、**NAT** をクリックします。
2. [**Add**] をクリックして新しいルールを作成します。

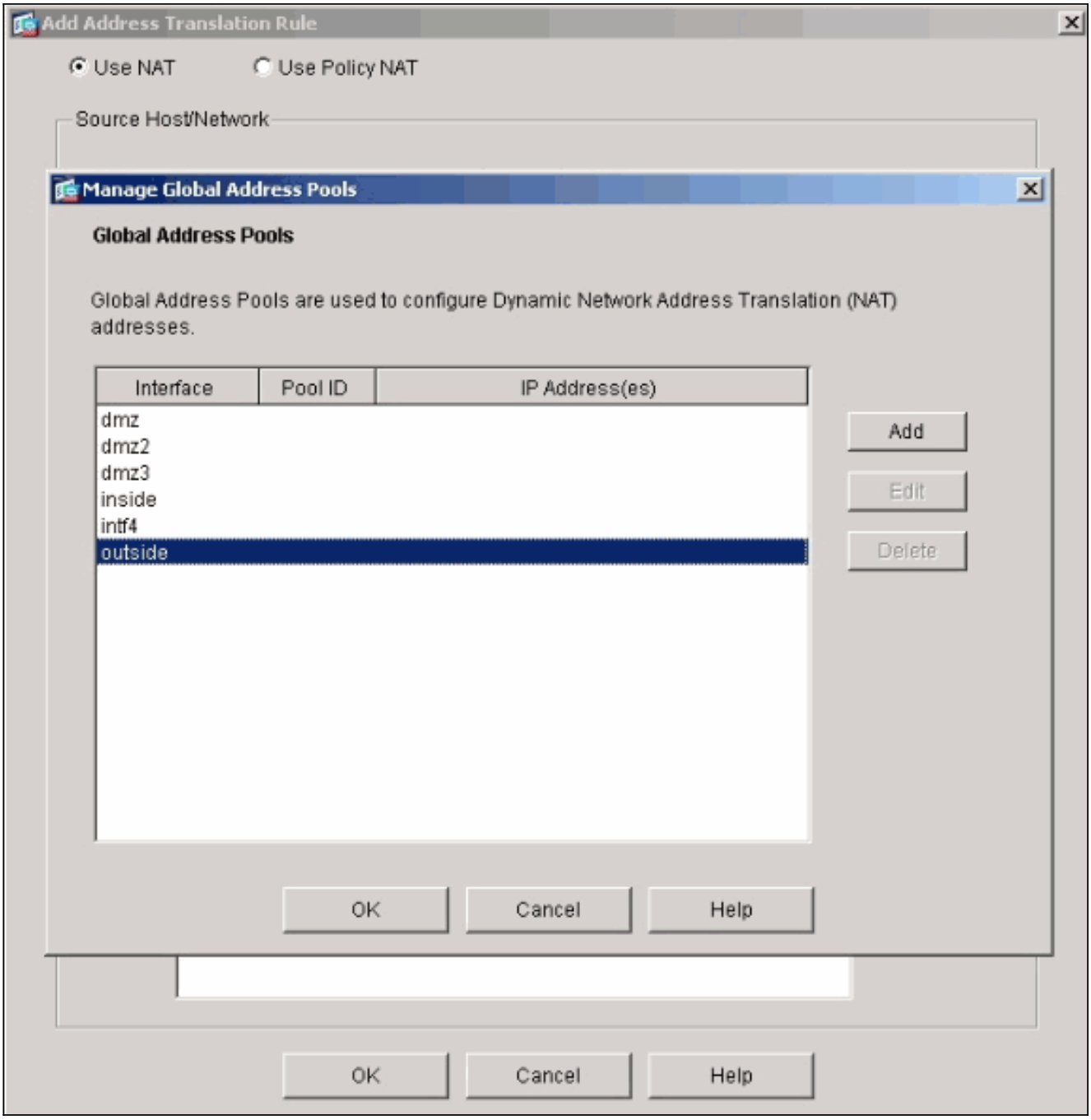


新しいウィンドウが表示され、ここからこの NAT エントリの NAT オプションを変更できます。 この例では、特定の 10.0.0.0/24 のネットワークから発信され、Inside インターフェイスに到達したパケットに対して NAT が実行されます。PIX/ASA では、これらのパケットが、Outside インターフェイスのダイナミック IP プールに変換されます。 NAT を適用するトラフィックについての情報を入力したら、変換済みトラフィック用の IP アドレスのプールを定義します。

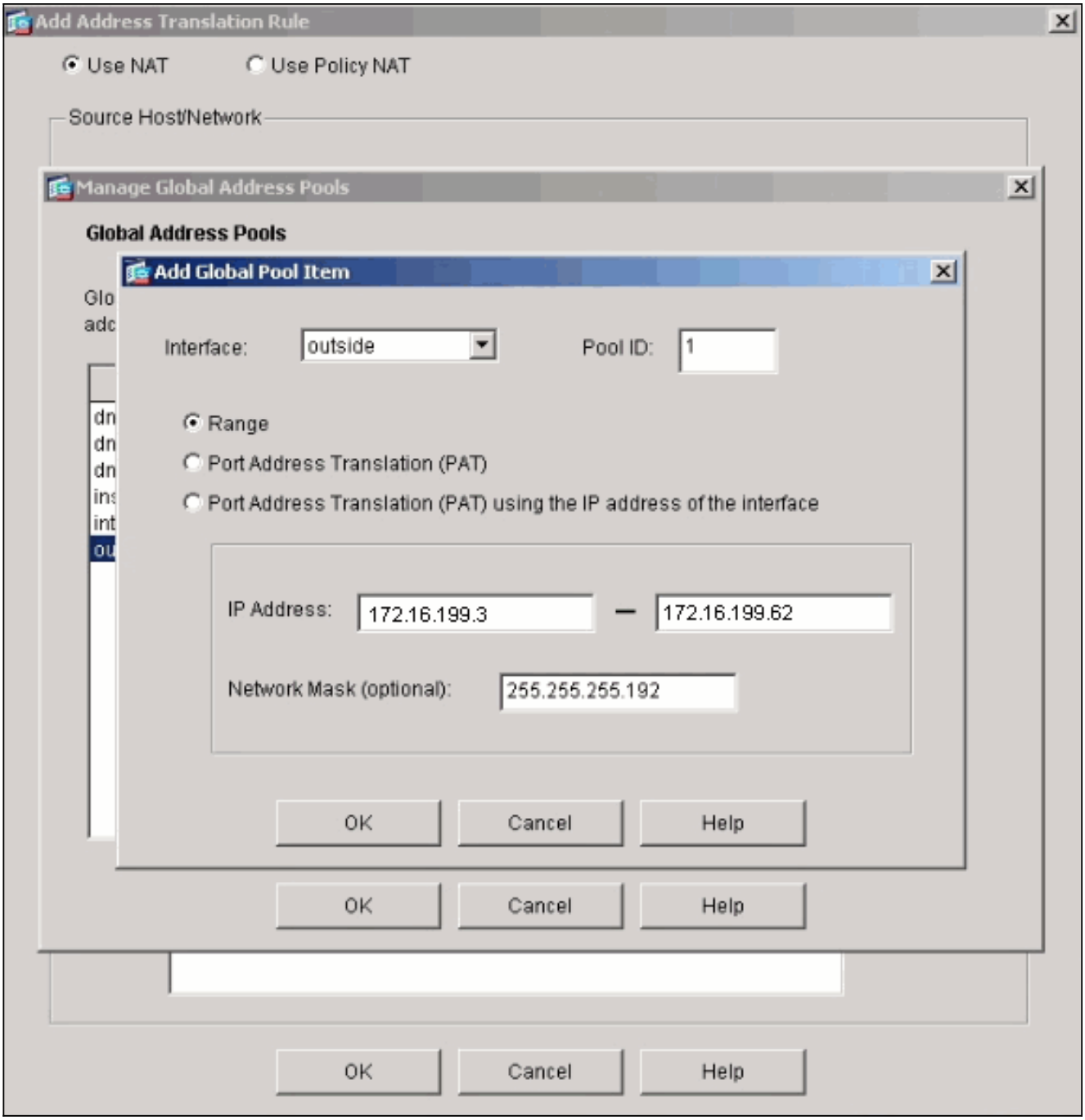
3. 新しい IP プールを追加するには **[Manage Pools]** をクリックします。



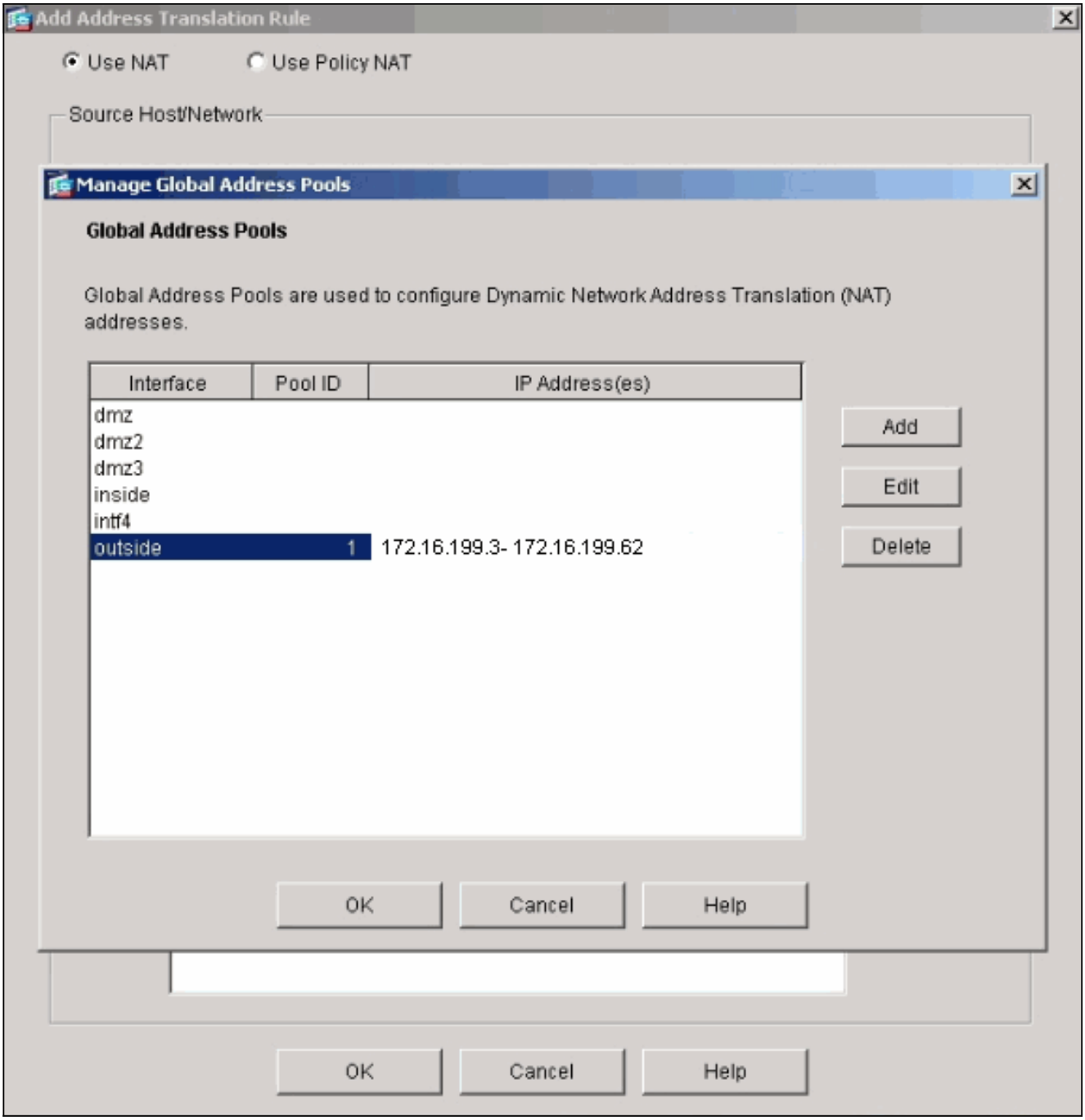
4. outside を選択して、Add をクリックします。



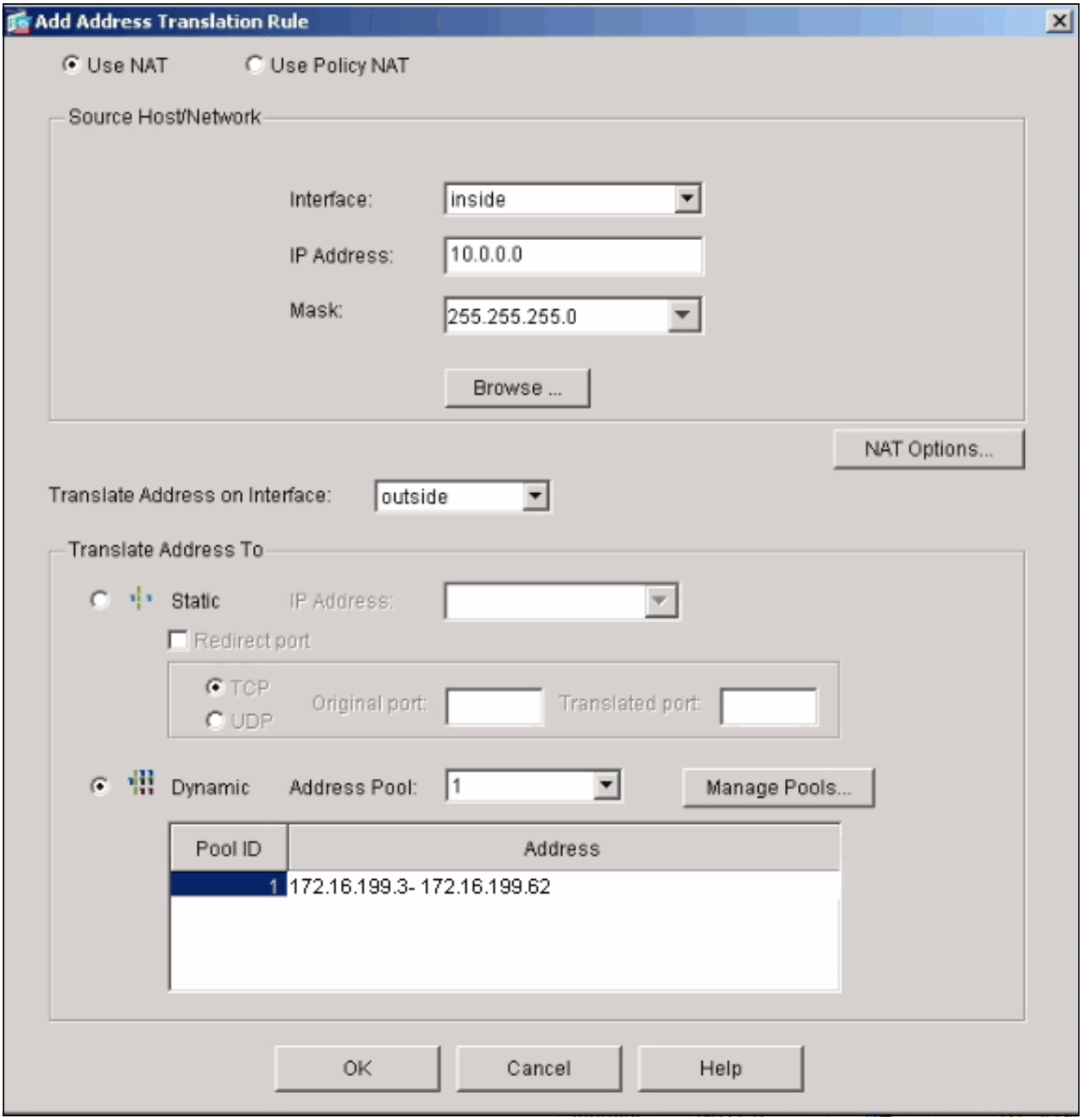
5. プールの IP 範囲を指定し、プールに一意の ID 番号を割り当てます。



6. 適切な値を選択して、**OK** をクリックします。Outside インターフェイスに新しいプールが定義されます。

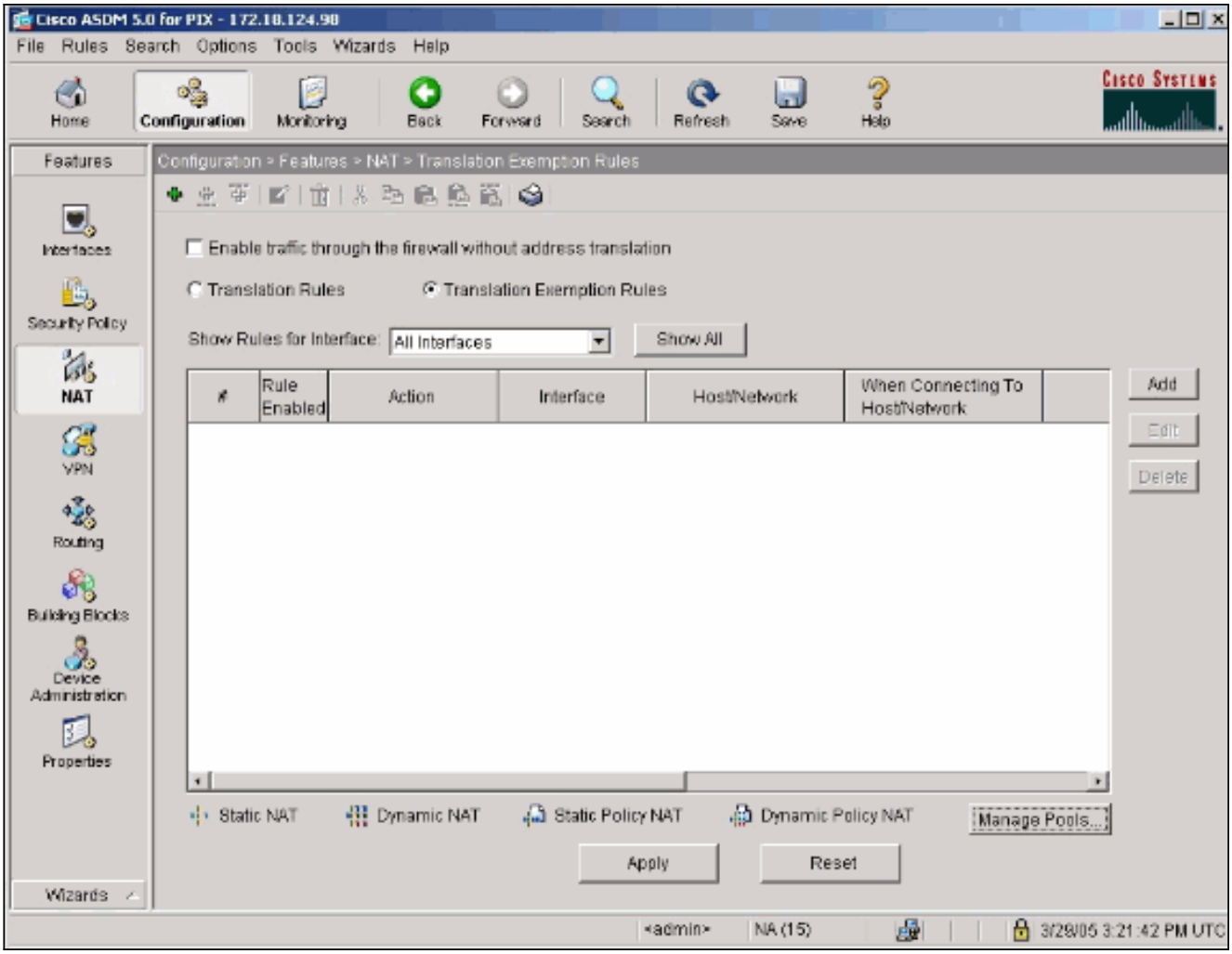


7. プールを定義したら、[**OK**] をクリックして、NAT ルール設定ウィンドウに戻ります。必ず、Address Pool ドロップダウン リストで作成したばかりの正しいプールを選択するようにしてください。

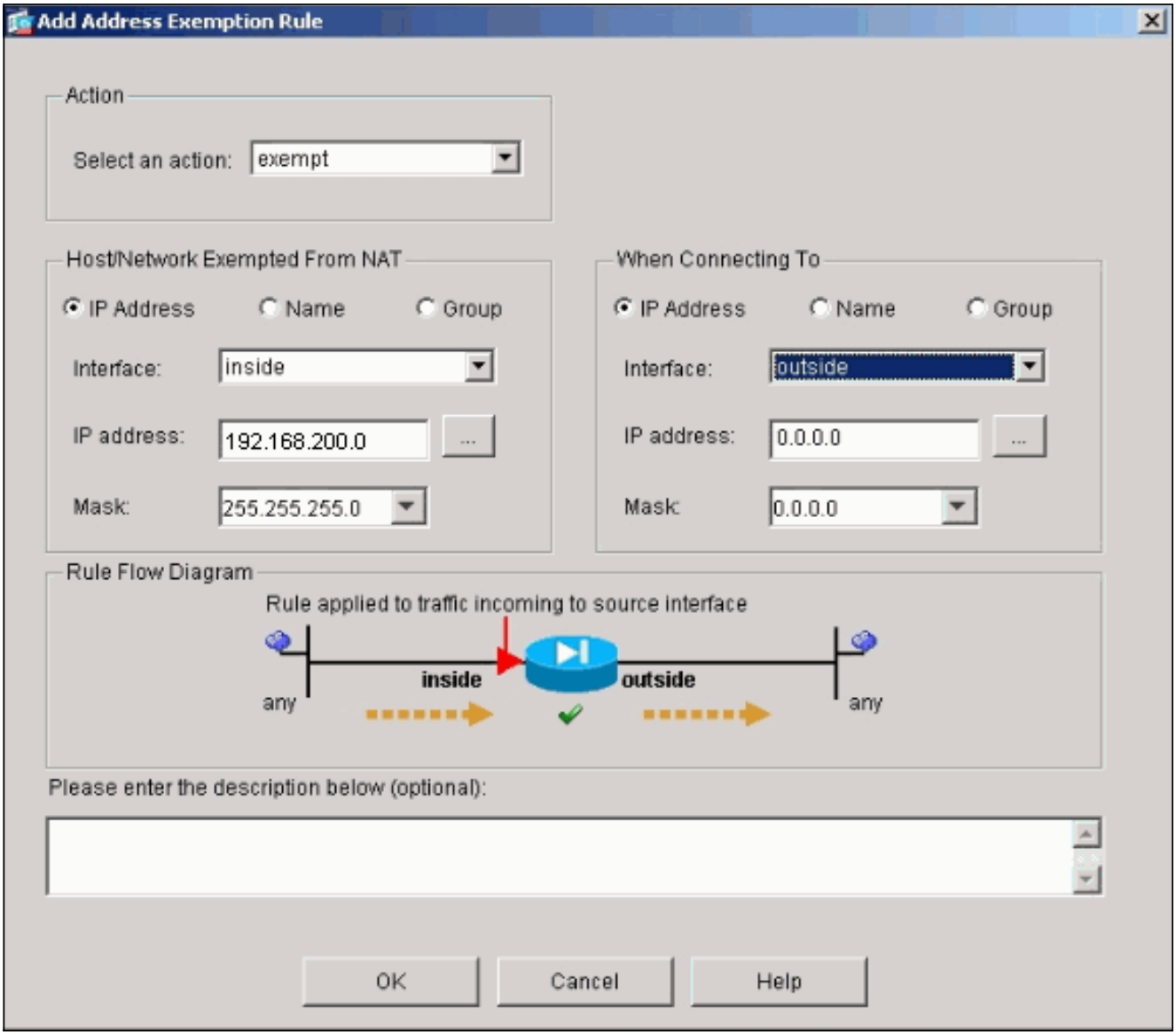


これで、セキュリティ アプライアンスを経由する NAT 変換が作成されました。 ところが、NAT を行わないトラフィックを指定する NAT エントリをさらに作成する必要があります。

8. 新しいルールを作成するには、ウィンドウの最上段にある **Translation Exemption Rules** をクリックして、**Add** をクリックする必要があります。



9. 送信元に *inside* インターフェイスを選択し、**192.168.200.0/24** サブネットを指定します。「When connecting」の値はデフォルト設定のままにしておきます。



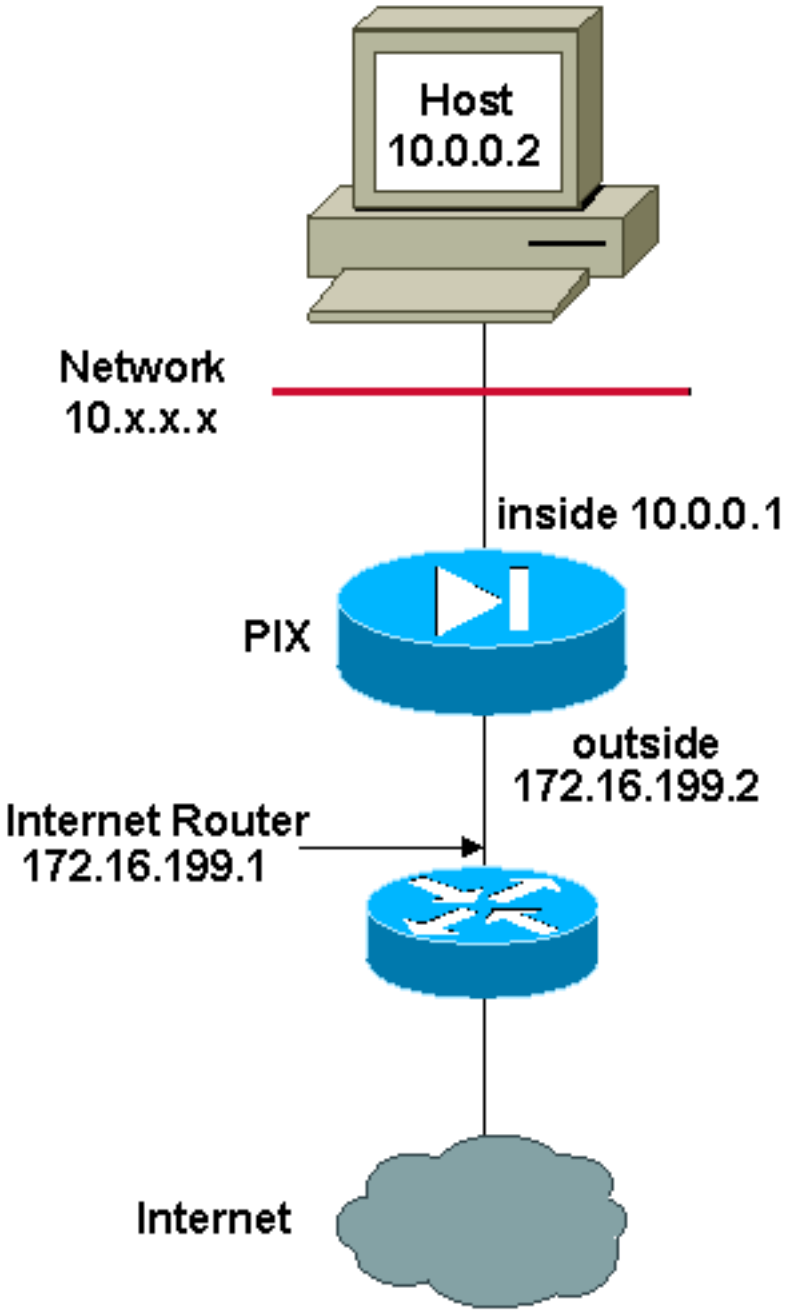
これで、NAT ルールが定義されました。

10. セキュリティ アプライアンスの現在の実行コンフィギュレーションにこの変更を適用するには、**Apply** をクリックします。次の出力には、PIX/ASA のコンフィギュレーションに適用される実際の追加部分が示されています。 これらは手動で入力するコマンドとは多少異なりますが、効果は同じです。

```
access-list inside_nat0_outbound extended permit
ip 192.168.200.0 255.255.255.0 any

global (outside) 1 172.16.199.3-172.16.199.62 netmask 255.255.255.192

nat (inside) 0 access-list inside_nat0_outbound
nat (inside) 1 10.0.0.0 255.255.255.0
```

複数のグローバル プール

ネットワーク図



注: 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 RFC 1918 で、 ラボ環境で使用されたアドレスです。

この例では、インターネットに登録されている 2 つの IP アドレス範囲がネットワーク管理者に提供されています。 ネットワーク管理者は、10.0.0.0/8 の範囲にあるすべての内部アドレスを登録アドレスに変換する必要があります。 ネットワーク管理者が使用する必要のある IP アドレスの範囲は、172.16.199.1 ~ 172.16.199.62 と 192.168.150.1 ~ 192.168.150.254 です。 ネットワーク管理者は、次の方法でこれを実現できます。

```
global (outside) 1 172.16.199.3-172.16.199.62 netmask 255.255.255.192

global (outside) 1 192.168.150.1-192.168.150.254 netmask 255.255.255.0

nat (inside) 1 0.0.0.0 0.0.0.0 0 0
```

ダイナミック NAT では、より限定的な設定が、同じインターフェイス上でグローバル設定を使用する場合に優先されます。

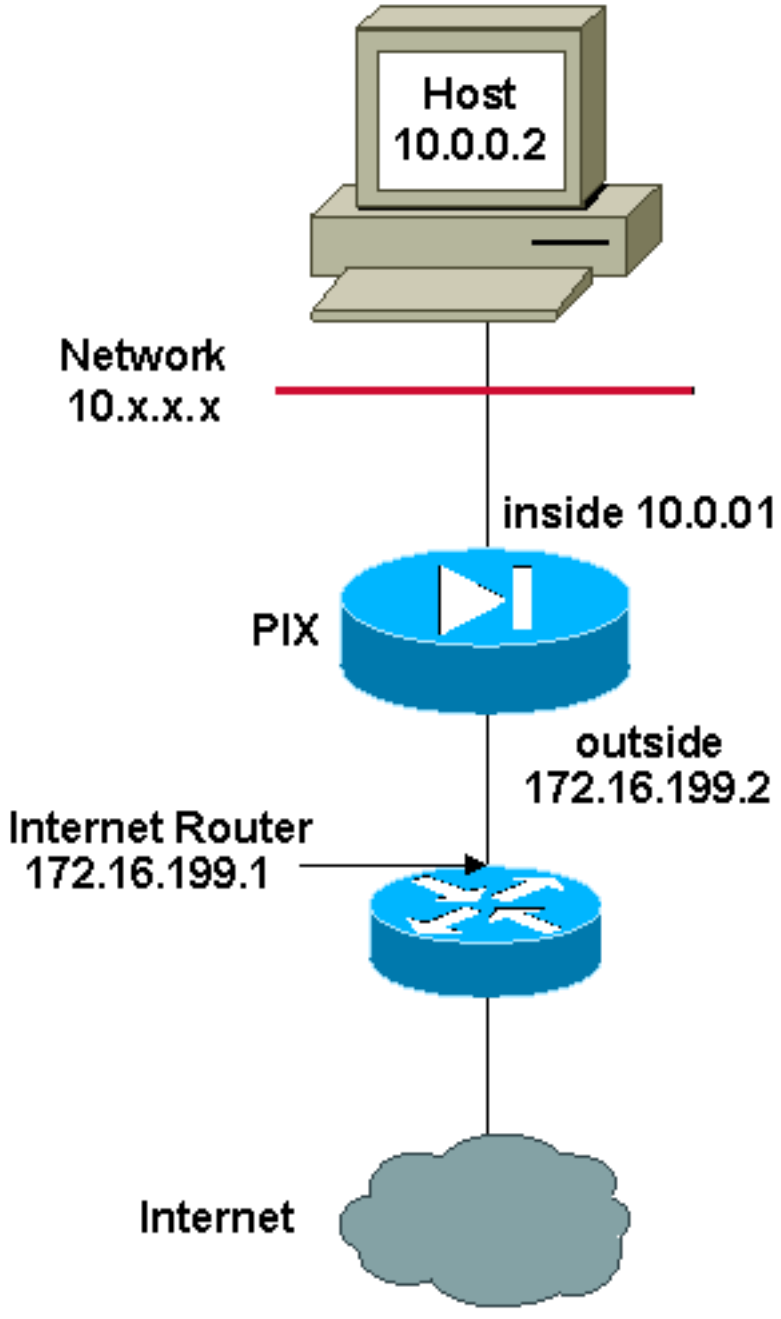
```
nat (inside) 1 10.0.0.0 255.0.0.0
nat (inside) 2 10.1.0.0 255.255.0.0
```

```
global (outside) 1 172.16.1.1
global (outside) 2 192.168.1.1
```
内部ネットワークが 10.1.0.0 の場合、NAT global 2 は 1 よりも変換に関して限定的なので、global 2 が 1 より優先されます。

注: NAT ステートメントでは、ワイルドカード アドレッシング方式が使用されています。 この設定では、内部送信元アドレスがインターネットに送出される際に、PIX/ASA で内部送信元アドレスをすべて変換するように指定されています。 必要な場合は、このコマンドのアドレスをさらに絞り込むことができます。

NAT グローバル文と PAT グローバル文の混在

ネットワーク図



注: 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 RFC 1918 で、 ラボ環境で使用されたアドレスです。

この例では、会社で使用するように、172.16.199.1 ~ 172.16.199.63 のアドレス範囲が ISP からネットワーク管理者に提供されています。 ネットワーク管理者は、インターネット ルータの Inside インターフェイスに 172.16.199.1 を使用し、PIX/ASA の Outside インターフェイスに 172.16.199.2 を使用すると判断します。 NAT プールの用途には、172.16.199.3 ~ 172.16.199.62 が残されています。 ところが、ネットワーク管理者には、一時点で 60 人を超えるユーザが PIX/ASA からの外部アクセスを試みる可能性があることがわかっています。 そのため、ネットワーク管理者は 172.16.199.62 を使用して、これを PAT アドレスにすると判断します。これにより、複数のユーザが同時に 1 つのアドレスを共用できます。

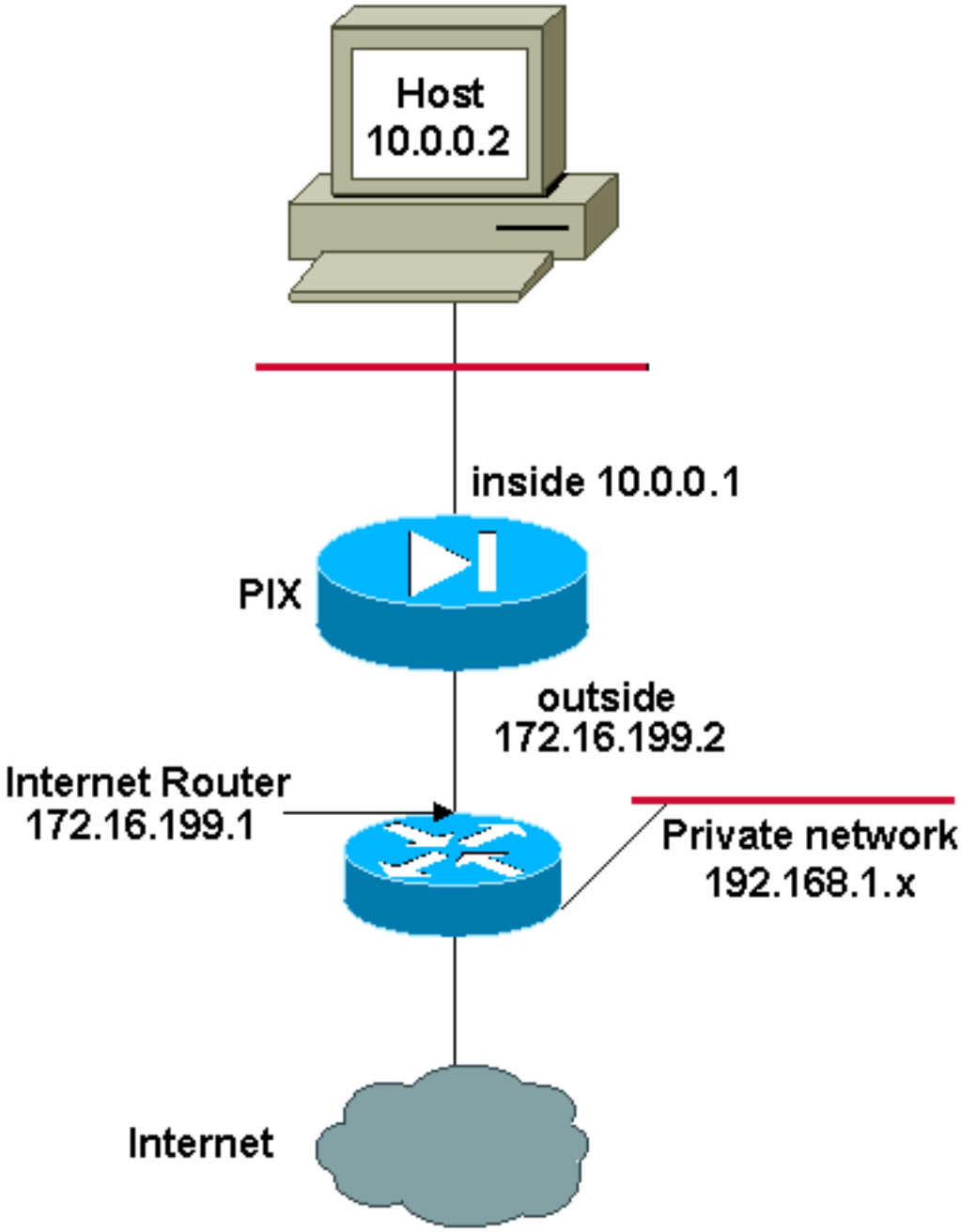
```
global (outside) 1 172.16.199.3-172.16.199.61 netmask 255.255.255.192

global (outside) 1 172.16.199.62 netmask 255.255.255.192

nat (inside) 1 0.0.0.0 0.0.0.0 0 0
```

これらのコマンドでは、PIX/ASA に対して、最初の 59 人の内部ユーザが PIX/ASA を通過するために送信元アドレスを 172.16.199.3 ~ 172.16.199.61 に変換するように指示されています。 これらのアドレスが使い果たされると、PIX では、NAT プール内のアドレスの 1 つが解放されるまで、後続の送信元アドレスすべてを 172.16.199.62 に変換することになります。

注: NAT ステートメントでは、ワイルドカード アドレッシング方式が使用されています。 この設定では、内部送信元アドレスがインターネットに送出される際に、PIX/ASA で内部送信元アドレスをすべて変換するように指定されています。 必要な場合は、このコマンドのアドレスをさらに限定的にすることができます。

nat 0 アクセスリストを使用した複数の NAT 文

ネットワーク図



注: 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 RFC 1918 で、 ラボ環境で使用されたアドレスです。

この例では、172.16.199.1 ~ 172.16.199.63 のアドレス範囲が ISP からネットワーク管理者に提供されています。 ネットワーク管理者は、インターネット ルータの Inside インターフェイスに 172.16.199.1 を割り当て、PIX/ASA の Outside インターフェイスに 172.16.199.2 を割り当てると判断します。

ただし、このシナリオでは、インターネット ルータの外に別のプライベート LAN セグメントが存在しています。 ネットワーク管理者は、これら 2 つのネットワーク内のホストどうしが通信するときに、グローバル プールのアドレスを無駄に使用しないようにする必要があります。 ただし、内部ユーザ (10.0.0.0/8) がインターネットにアクセスする場合は、内部ユーザの発信元アドレスを変換する必要があります。

```
access-list 101 permit ip 10.0.0.0 255.0.0.0 192.168.1.0 255.255.255.0

global (outside) 1 172.16.199.3-172.16.199.62 netmask 255.255.255.192
```

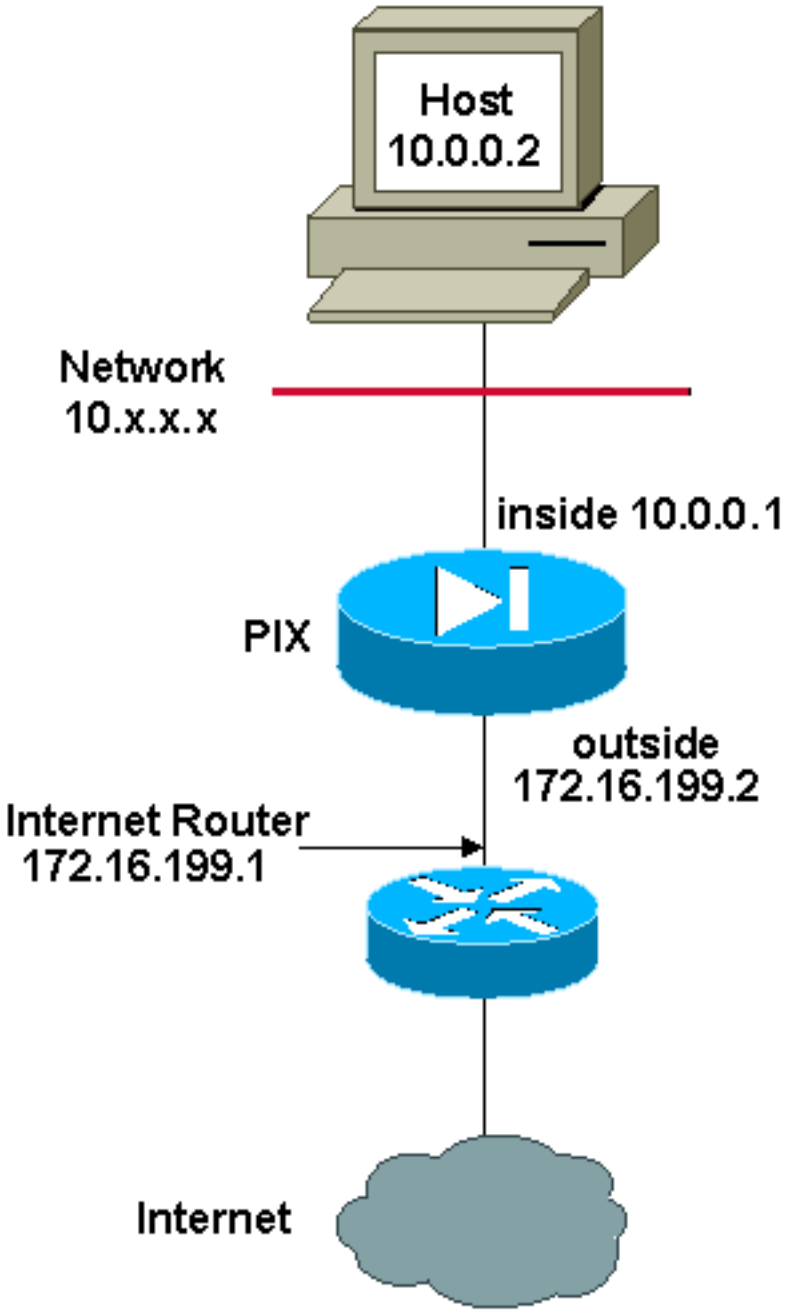
```
nat (inside) 0 access-list 101

nat (inside) 1 10.0.0.0 255.0.0.0 0 0
```

このコンフィギュレーションでは、送信元アドレスが 10.0.0.0/8 の範囲で宛先アドレスが 192.168.1.0/24 の範囲のアドレスは変換されません。 この場合、10.0.0.0/8 のネットワーク内から開始され、192.168.1.0/24 以外のいずれかを宛先とする送信元アドレスが、172.16.199.3 ~ 172.16.199.62 の範囲にあるアドレスに変換されます。

使用中の Cisco デバイスからの **write terminal** コマンドの出力がある場合は、アウトプット インタープリタ（登録ユーザ専用）を使用できます。

ポリシー NAT の使用

ネットワーク図



注: 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 RFC 1918 アドレスであり、ラボ環境で使用されたものです

。

0 以外の NAT ID の **nat** コマンドでアクセス リストを使用すると、ポリシー NAT が有効になります。

注: ポリシー NAT はバージョン 6.3.2 で導入されました。

ポリシー NAT を使用すると、アクセス リストで発信元と宛先のアドレス (またはポート) を指定する際に、アドレス変換対象のローカル トラフィックを識別できます。 通常の NAT で使用されるのは発信元のアドレス/ポートのみですが、ポリシー NAT では発信元と宛先の両方のアドレス/ポートが使用されます。

注: NAT 免除 (**nat 0 access-list**) 以外のすべてのタイプの NAT で、ポリシー NAT がサポートされています。 NAT 例外では、ローカル アドレスの識別にアクセス コントロール リストが使用されますが、ポートは考慮されないという点がポリシー NAT と異なります。

ポリシー NAT では、発信元/ポートと宛先/ポートの組み合わせが設定ごとに一意である限り、同じローカル アドレスを識別する複数の NAT 設定やスタティック設定を作成できます。 これにより、それぞれの送信元ポートと宛先ポートのペアに対して異なるグローバル アドレスを対応させることができます。

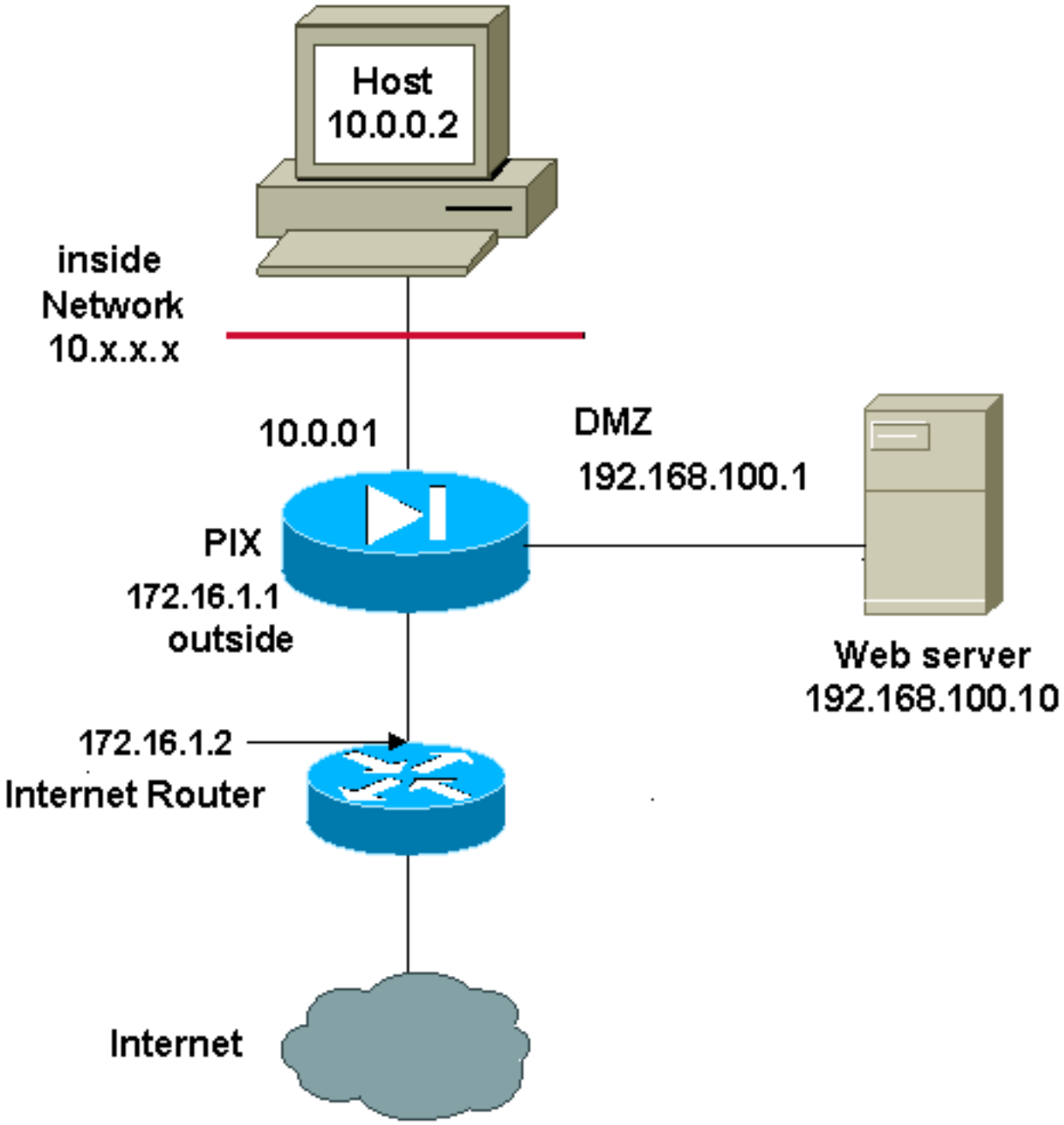
この例では、ネットワーク管理者からはポート 80 (Web) とポート 23 (Telnet) に宛先 IP アドレス 192.168.201.11 へのアクセスが割り当てられていますが、送信元アドレスには 2 つの異なる IP アドレスを使用する必要があります。 IP アドレス 172.16.199.3 が Web への送信元アドレスに使用されます。 Telnet には IP アドレス 172.16.199.4 が使用され、10.0.0.0/8 の範囲にあるすべての内部アドレスは変換が必要です。 ネットワーク管理者は、次の方法でこれを実現できます。

```
access-list WEB permit tcp 10.0.0.0 255.0.0.0 192.168.201.11
255.255.255.255 eq 80

access-list TELNET permit tcp 10.0.0.0 255.0.0.0 192.168.201.11
255.255.255.255 eq 23

nat (inside) 1 access-list WEB

nat (inside) 2 access-list TELNET

global (outside) 1 172.16.199.3 netmask 255.255.255.192

global (outside) 2 172.16.199.4 netmask 255.255.255.192
```

可能性のある問題と修正を表示するには、 アウトプットインタープリタ ツール (登録ユーザ専用) を使用できます。

スタティック NAT

ネットワーク図



注: 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 RFC 1918 で、 ラボ環境で使用されたアドレスです。

スタティック NAT 設定では、1 対 1 のマッピングが作成され、特定のアドレスが別のアドレスに変換されます。 このタイプの設定では、設定が存在する限り、NAT テーブルに恒久的なエントリが作成され、内部ホストと外部ホストの両方から接続を開始できます。 これは、主にメール、Web、FTP などのアプリケーション サービスを提供するホストで便利な設定です。 この例では、内部と外部のユーザが DMZ 上の Web サーバにアクセスできるようにスタティック NAT 設定を設定します。

次の出力は、スタティック文の作成方法を示しています。 マッピングされる IP アドレスと実際の IP アドレスの順序に注意してください。

`static (real_interface,mapped_interface) mapped_ip real_ip netmask mask`
これは、Inside インターフェイス上のユーザが DMZ 上のサーバにアクセスできるように作成されたスタティック変換です。 これにより、内部のアドレスと DMZ 上のサーバのアドレスとのマッピングが作成されます。 これで、Inside のユーザは、Inside のアドレスを使用して DMZ 上の

サーバにアクセスできるようになります。

```
static (DMZ,inside) 10.0.0.10 192.168.100.10 netmask 255.255.255.255
```

これは、Outside インターフェイス上のユーザが DMZ 上のサーバにアクセスできるように作成されたスタティック変換です。 これにより、外部のアドレスと DMZ 上のサーバのアドレスとのマッピングが作成されます。 これで、外部のユーザは、外部アドレスを使用して DMZ 上のサーバにアクセスできるようになります。

```
static (DMZ,outside) 172.16.1.5 192.168.100.10 netmask 255.255.255.255
```

注: 外側インターフェイスのセキュリティ レベルは DMZ よりも低いため、外部のユーザが DMZ 上のサーバにアクセスできるようにするには、アクセス リストを作成する必要もあります。 このアクセス リストでは、スタティック変換で**マッピングされるアドレス**へのアクセスをユーザに許可する必要があります。 このアクセス リストはできるだけ詳細に作成することを推奨します。 この場合、いずれのホストも、Web サーバのポート 80（www/http）およびポート 443（https）以外へのアクセスは許可されません。

```
access-list OUTSIDE extended permit tcp any host 172.16.1.5 eq www
access-list OUTSIDE extended permit tcp any host 172.16.1.5 eq https
```

ここで、Outside インターフェイスにアクセス リストを適用する必要があります。

```
access-group OUTSIDE in interface outside
```

access-list コマンドと **access-group** コマンドについての詳細は、『拡張アクセスリスト』と『アクセスグループ』を参照してください。

NAT をバイパスする方法

ここでは、NAT のバイパス方法について説明します。 NAT 制御をイネーブルにするときに、NAT をバイパスできます。 NAT をバイパスするには、アイデンティティ NAT、スタティック アイデンティティ NAT、あるいは、NAT 免除を使用できます。

アイデンティティ NAT の設定

アイデンティティ NAT では、実 IP アドレスが同じ IP アドレスに変換されます。 NAT 変換を作成できるのは「変換対象」ホストだけであり、応答トラフィックを返すことが可能です。

注: NAT 設定を変更する場合に、新しい NAT 情報が使用される前に既存の変換がタイムアウトになるのを待たない場合は、**clear xlate** コマンドを使用して変換テーブルをクリアできます。 ところが、変換を使用している既存の接続は、変換テーブルをクリアする際に、すべて接続解除されます。

アイデンティティ NAT を設定するには、次のコマンドを入力します。

```
hostname(config)#nat (real_interface) 0 real_ip [mask [dns] [outside] [norandomseq] [[tcp]
tcp_max_conns [emb_limit]] [udp udp_max_conns]
```

たとえば、Inside の 10.1.1.0/24 のネットワークにアイデンティティ NAT を使用するには、次のコマンドを入力します。

```
hostname(config)#nat (inside) 0 10.1.1.0 255.255.255.0
```

nat コマンドの詳細は、『Cisco セキュリティ アプライアンス コマンド リファレンス、バージョン 7.2』を参照してください。

スタティック アイデンティティ NAT の設定

スタティック アイデンティティ NAT では、実 IP アドレスが同じ IP アドレスに変換されます。変換は常にアクティブで、「変換対象」のホストとリモートのホストでは、どちらも接続の開始が可能です。 スタティック アイデンティティ NAT では、標準 NAT またはポリシー NAT を使用できます。 ポリシー NAT では、変換する実際のアドレスを決定するときに、実際のアドレスと宛先アドレスを指定できます (ポリシー NAT の詳細については、「ポリシー NAT の使用」の項を参照)。 たとえば、Outside の宛先サーバ A にアクセスする場合は、Inside アドレスに対してポリシー スタティック アイデンティティ NAT を使用し、Outside のサーバ Bにアクセスする場合には、通常の変換を使用することも可能です。

注: スタティック コマンドを削除しても、変換を使用している現在の接続への影響はありません。 これらの接続を削除する場合は、clear local-host コマンドを入力します。 変換テーブルのクリアは、**clear xlate** コマンドを使用して実行できます。 代わりに static コマンドを削除します。 clear xlate コマンドで削除できるのは、nat コマンドと global コマンドで作成されたダイナミック変換だけです。

ポリシー スタティック アイデンティティ NAT を設定するには、次のコマンドを入力します。

```
hostname(config)#static (real_interface,mapped_interface) real_ip access-list acl_id [dns]
[norandomseq] [[tcp] tcp_max_conns [emb_limit]] [udp udp_max_conns]
```

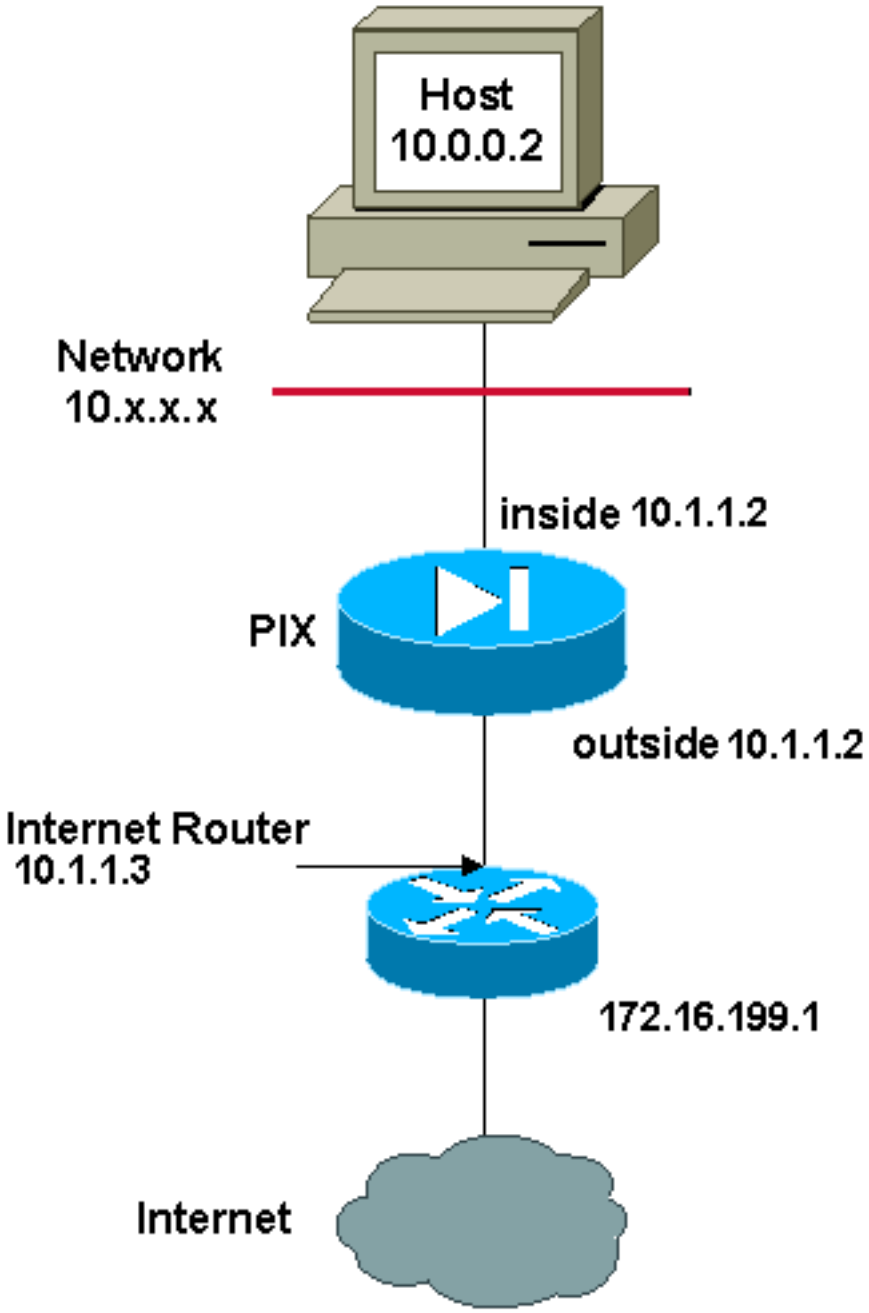
拡張アクセス リストを作成するには、**access-list extended** コマンドを使用します。 このアクセス リストに記載できるのは許可 ACE だけです。 アクセス リスト内の送信元アドレスが、このコマンドの real_ip に一致していることを確認してください。 ポリシー NAT では、inactive キーワードや time-range キーワードは考慮されません。 ポリシー NAT の設定では、すべての ACE はアクティブであると見なされます。 詳細は、「ポリシー NAT の使用」の項を参照してください。

通常のスタティック アイデンティティ NAT を設定するには、次のコマンドを入力します。

```
hostname(config)#static (real_interface,mapped_interface) real_ip real_ip [netmask mask] [dns]
[norandomseq] [[tcp] tcp_max_conns [emb_limit]] [udp udp_max_conns]
```

両方の real_ip 引数に同じ IP アドレスを指定します。

ネットワーク図



注: 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 RFC 1918 で、 ラボ環境で使用されたアドレスです。

たとえば、次のコマンドでは、Outside からアクセスされる際の Inside の IP アドレス（ 10.1.1.2 ）にはスタティック アイデンティティ NAT が使用されています。

```
hostname(config)#static (inside,outside) 10.1.1.2 10.1.1.2 netmask 255.255.255.255
```

static コマンドの詳細は、『Cisco セキュリティ アプライアンス コマンド リファレンス、バージョン 7.2』を参照してください。

次のコマンドでは、Inside からアクセスされる際の Outside の IP アドレス（ 172.16.199.1 ）にはスタティック アイデンティティ NAT が使用されています。

```
hostname(config)#static (outside,inside) 172.16.199.1 172.16.199.1 netmask 255.255.255.255
```

次のコマンドでは、サブネット全体がスタティックにマッピングされます。

```
hostname(config)#static (inside,dmz) 10.1.1.2 10.1.1.2 netmask 255.255.255.0
```

次のスタティック アイデンティティ ポリシー NAT の例には、1 つの宛先アドレスにアクセスす

る際のアイデンティティ NAT を使用する単一の実アドレス、および、それ以外にアクセスする際の変換が示されています。

```
hostname(config)#access-list NET1 permit ip host 10.1.1.3 172.16.199.0 255.255.255.224
hostname(config)#access-list NET2 permit ip host 10.1.1.3 172.16.199.224 255.255.255.224
hostname(config)#static (inside,outside) 10.1.1.3 access-list NET1 hostname(config)#static
(inside,outside) 172.16.199.1 access-list NET2
```

注: static コマンドについての詳細は、『Cisco ASA 5580 適応型セキュリティ アプライアンス コマンド リファレンス、バージョン 8.1』を参照してください。

注: アクセスリストについての詳細は、『Cisco ASA 5580 適応型セキュリティ アプライアンス コマンド ライン コンフィギュレーション ガイド、バージョン 8.1』を参照してください。

NAT 免除の設定

NAT 免除により、アドレスの変換が免除され、実ホストとリモート ホストの両方で接続を開始できます。 NAT 除外では、（ポリシー NAT と同様）除外する実トラフィックを決定するときに実アドレスと宛先アドレスを指定できるので、アイデンティティ NAT を使用するよりも NAT 除外を使用する方がきめ細かい制御が行えます。 その反面、ポリシー NAT と異なり、NAT 免除ではアクセス リストのポートが考慮されません。 アクセス リスト内のポートを検討するには、スタティック アイデンティティ NAT を使用します。

注: NAT 免除を削除しても、NAT 免除を使用している既存の接続への影響はありません。 これらの接続を削除するには、clear local-host コマンドを入力します。

NAT 免除を設定するには、次のコマンドを入力します。

```
hostname(config)#nat (real_interface) 0 access-list acl_name [outside]
```

access-list extended コマンドを使用して、拡張アクセス リストを作成します。 このアクセス リストには許可 ACE と拒否 ACE の両方を記載できます。 アクセス リストには実ポートと宛先ポートは指定しないでください。 NAT 免除ではポートは考慮されません。 NAT 免除では、inactive キーワードや time-range キーワードも考慮されません。 NAT 免除の設定では、すべての ACE はアクティブであると見なされます。

デフォルトでは、このコマンドで免除対象になるのは、Inside から Outside へのトラフィックです。 outside から inside へのトラフィックが NAT をバイパスするようにするには、**nat コマンド**を追加して outside を入力し、NAT インスタンスを outside NAT として識別します。 外部インターフェイスに対してダイナミック NAT を設定して、他のトラフィックを除外する場合は、外部 NAT 除外を使用できます。

たとえば、すべての宛先アドレスにアクセスする際に Inside のネットワークを免除するには、次のコマンドを入力します。

```
hostname(config)#access-list EXEMPT permit ip 10.1.1.0 255.255.255.0 any hostname(config)#nat
(inside) 0 access-list EXEMPT
```

ある DMZ ネットワークにダイナミック Outside NAT を使用して、他の DMZ ネットワークを免除するには、次のコマンドを入力します。

```
hostname(config)#nat (dmz) 1 10.1.1.0 255.255.255.0 outside dns hostname(config)#global
(inside) 1 10.1.1.2 hostname(config)#access-list EXEMPT permit ip 10.1.1.0 255.255.255.0 any
hostname(config)#nat (dmz) 0 access-list EXEMPT
```

たとえば、2 つの異なる宛先アドレスにアクセスする際に 1 つの Inside のアドレスを免除するには、次のコマンドを入力します。

```
hostname(config)#access-list NET1 permit ip 10.1.1.0 255.255.255.0 172.16.199.0 255.255.255.224
hostname(config)#access-list NET1 permit ip 10.1.1.0 255.255.255.0 172.16.199.224
255.255.255.224 hostname(config)#nat (inside) 0 access-list NET1
```

確認

セキュリティ アプライアンスを通過するトラフィックは、ほとんどが NAT の対象になります。Cisco ASA をバージョン 8.2 以前と同じ構成にする場合は、『PIX/ASA： パフォーマンスの問題の監視とトラブルシューティング』を参照してください。

show xlate count コマンドは、PIX を経由した変換の現在数と最大数を表示します。 変換は外部アドレスへの内部アドレスのマッピングで、1 対 1 のマッピングになる場合（NAT など）と多対 1 のマッピングになる場合（PAT など）があります。 このコマンドは show xlate コマンドのサブセットで、PIX 経由の各変換を出力します。 コマンド出力に表示される「in use」の変換は、コマンドの発行時点で PIX 内に存在するアクティブな変換の数を表します。 「most used」は、PIX の電源オン以降に PIX で見られた変換の最大数を表します。

トラブルシューティング

ポート 443 のスタティック PAT 追加時にエラー メッセージが表示される

問題

ポート 443 のスタティック PAT の追加時に、次のエラー メッセージが表示されます。

```
[[ERROR] static (INSIDE,OUTSIDE) tcp interface 443 192.168.1.87 443 netmask 255.255.255.255 tcp
0 0 udp 0

unable to reserve port 443 for static PAT

ERROR: unable to download policy
```

解決策

このエラー メッセージは、ASDM または WEBVPN が 443 ポートで動作している場合に表示されます。 この問題を解決するには、ファイアウォールにログインし、次のいずれかの手順を実行します。

- ASDM ポートを 443 以外に変更するには、次のコマンドを実行します。`ASA(config)#no http server enable ASA(config)#http server enable 8080`
- WEBVPN ポートを 443 以外に変更するには、次のコマンドを実行します。`ASA(config)#webvpn ASA(config-webvpn)#enable outside ASA(config-webvpn)#port 65010`

これらのコマンドの実行後には、別のサーバに対するポート 443 で NAT/PAT を追加できます。将来 ASA を管理する目的で ASDM を使用するときには、新しいポートとして 8080 を指定します。

エラー： mapped-address conflict with existing static

問題

ASA のスタティック設定の追加時に次のエラーが表示されます。

```
ERROR: mapped-address conflict with existing static
```

解決策

追加するスタティック ソースのエントリがまだ存在していないことを確認します。

関連情報

- PIX に関するサポート ページ
- PIX コマンド リファレンス
- ASA に関するサポート ページ
- ASA のコマンド 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