NAT の ASA バージョン 9.x ポート転送を設定する

目次

概要

このドキュメントでは、ポート リダイレクション（フォワーディング）の設定方法、および CLI または Adaptive Security Device Manager（ASDM）を使用した、適応型セキュリティ アプライアンス（ASA）ソフトウェア バージョン 9.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。

詳細については、『Cisco ASA シリーズ ファイアウォール ASDM 設定ガイド』を参照してください。

前提条件

要件

デバイスを ASDM で設定できるようにするには、『管理アクセスの設定』を参照してください。

使用するコンポーネント

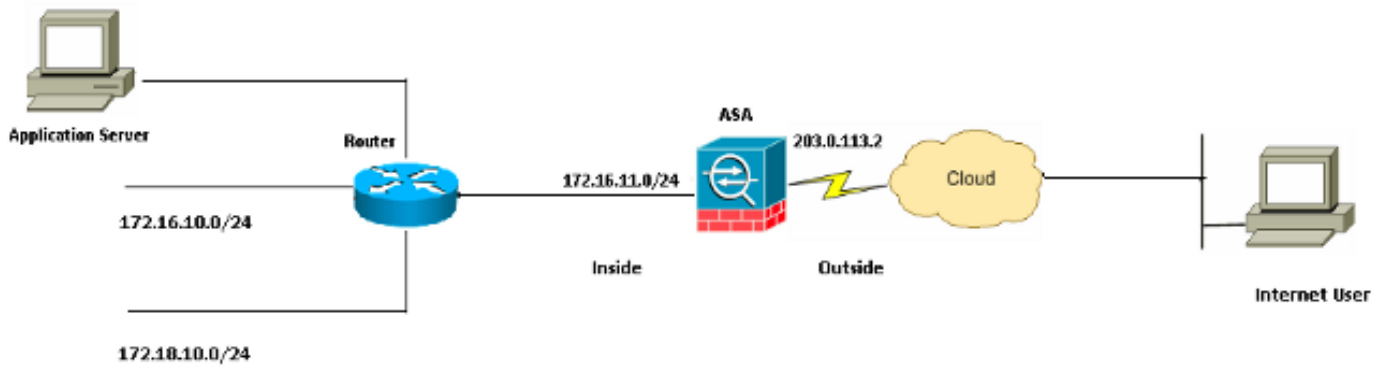
このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Cisco ASA 5525 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 9.x 以降
- ASDM バージョン 7.x 以降

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。

設定

ネットワーク図



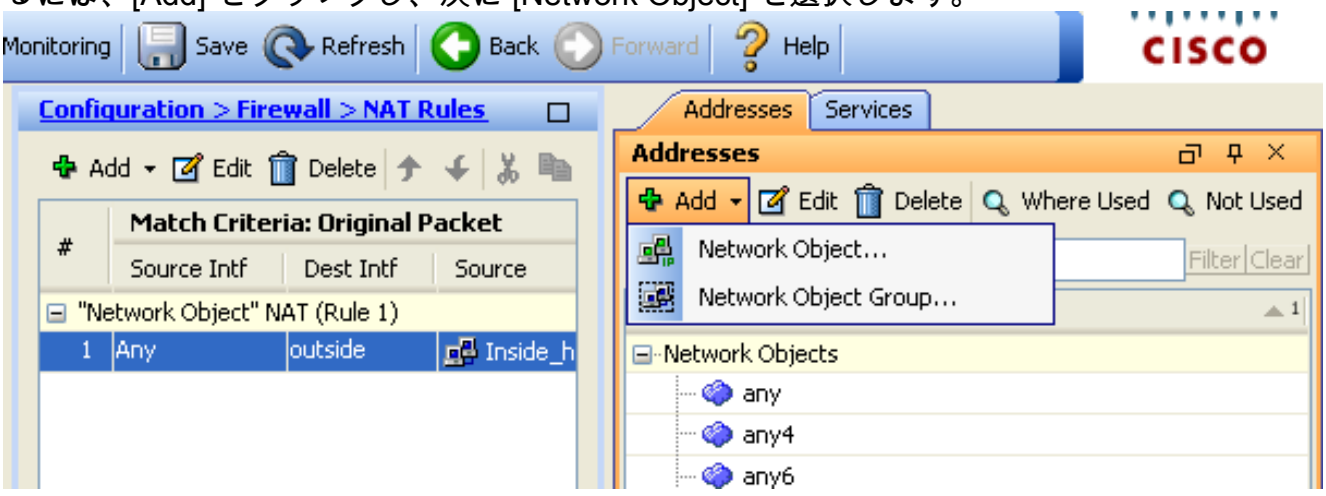
この設定で使用している IP アドレス スキームは、インターネット上で正式にルーティング可能なものではありません。 これらはラボ環境で使用された RFC 1918 でのアドレスです。

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

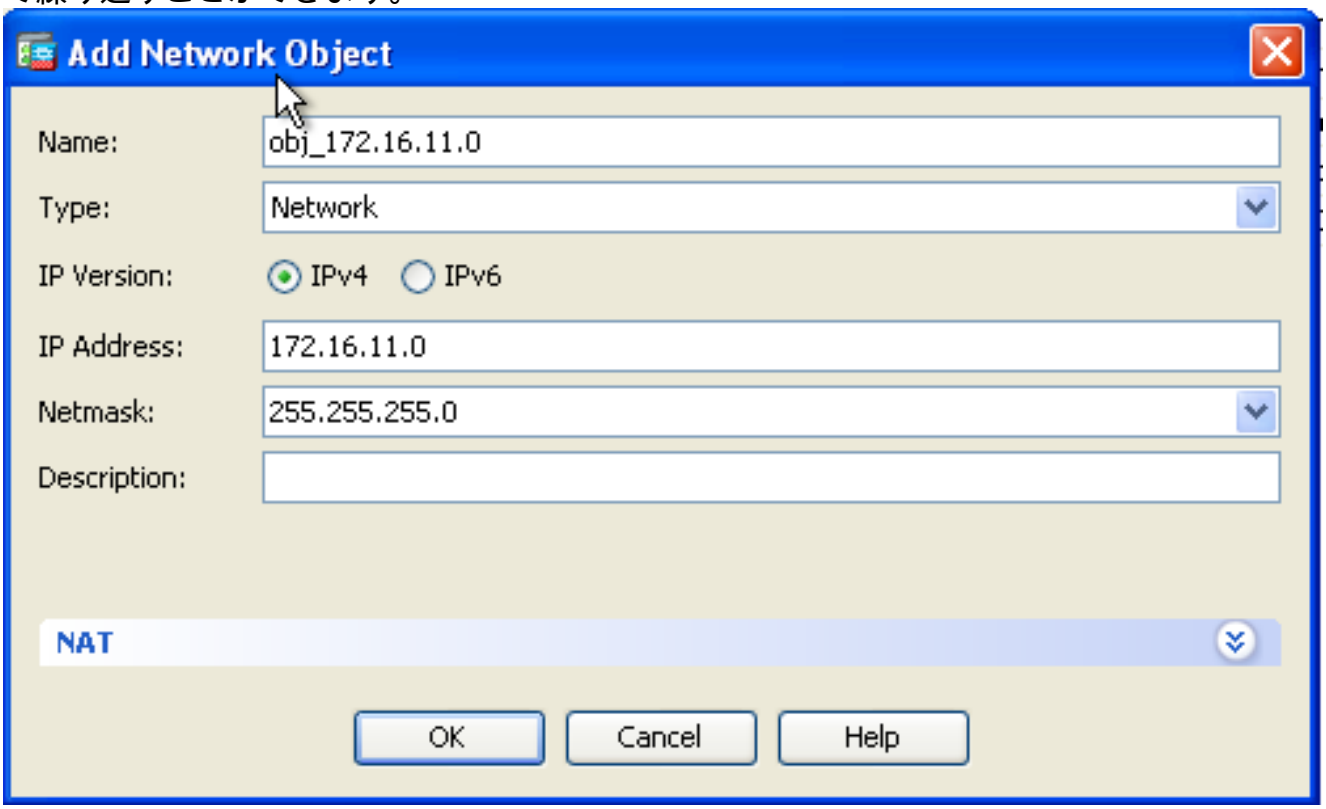
変換用に inside ホストで 1 つのパブリック アドレスを共有する場合は、ポート アドレス変換（PAT）を使用します。 PAT の最も単純な設定の 1 つに、すべての内部ホストを、外部インターフェイスの IP アドレスのように見えるよう変換することが含まれます。 これは、ISP から使用できるルーティング可能な IP アドレスの数が制限されているか少数、あるいはわずか 1 つの場合に使われる、一般的な PAT の設定です。

PAT を使用して inside ホストから outside ネットワークへのアクセスを許可するには、次の手順を実行します。

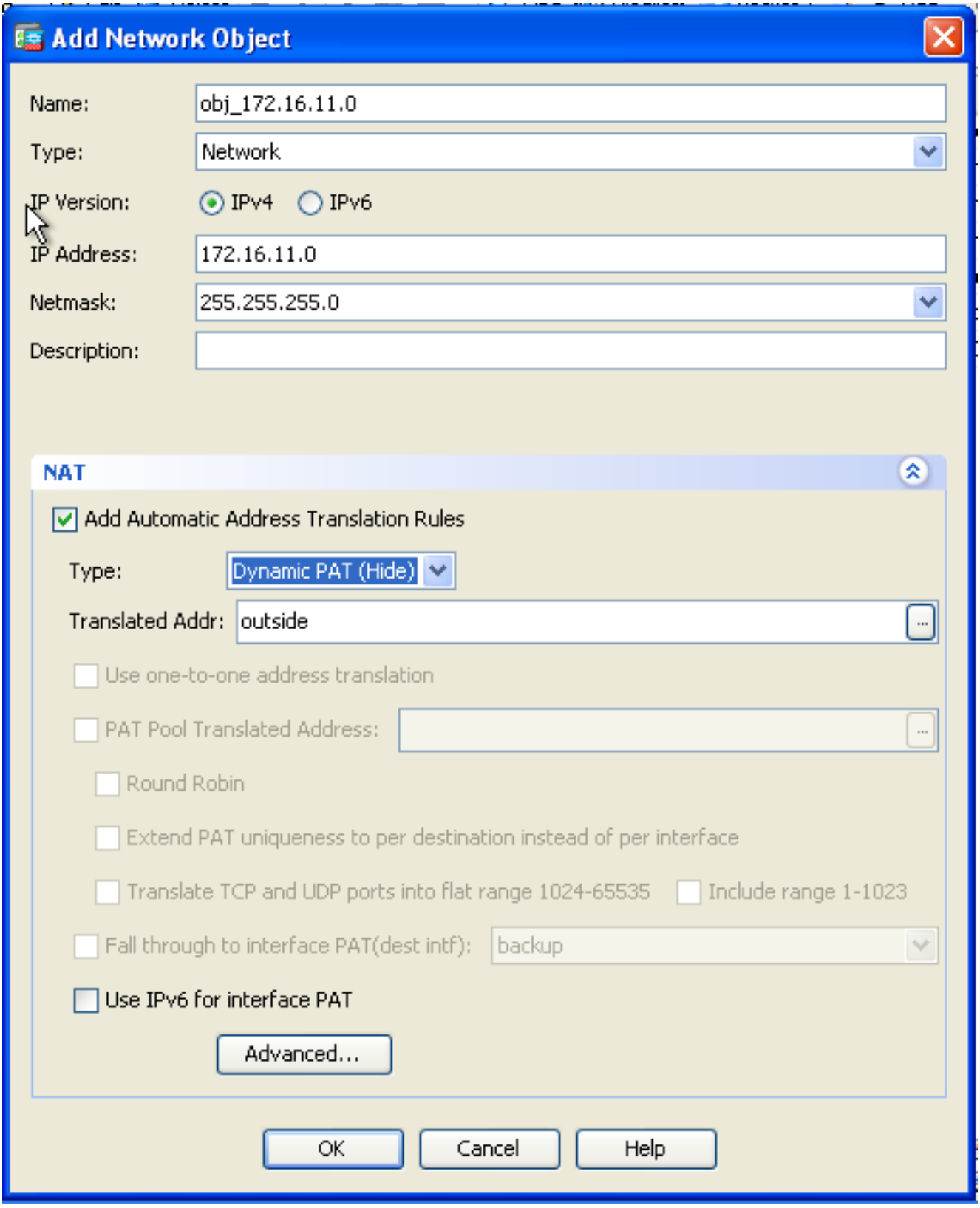
1. [Configuration] > [Firewall]> [NAT Rules] を選択します。 ダイナミック NAT ルールを設定するには、[Add] をクリックし、次に [Network Object] を選択します。



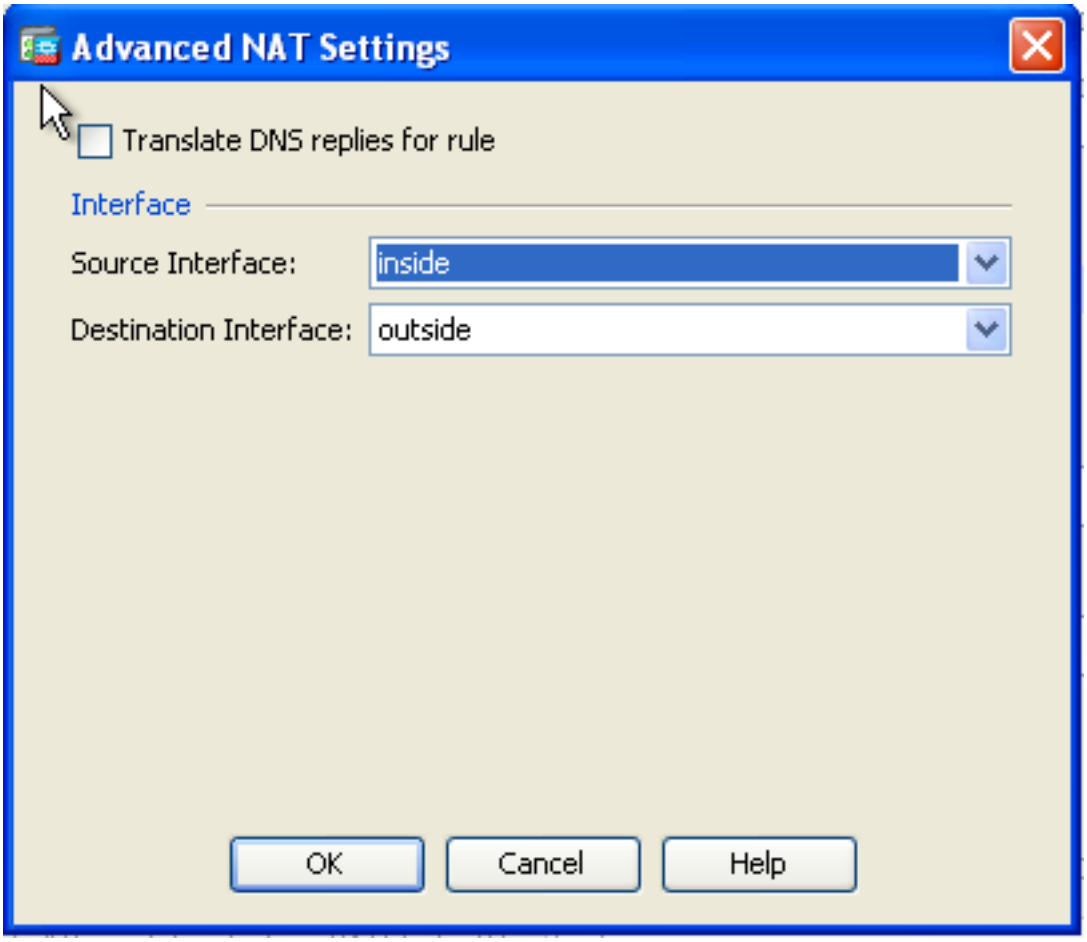
2. **Dynamic PAT** が必要なネットワーク/ホスト/範囲を設定します。 この例では、内部サブネットの 1 つが選択されました。 このプロセスは、次のように変換する他のサブネットに対して繰り返すことができます。



3. [NAT] を展開します。 [Add Automatic Address Translation Rules] チェックボックスをオンにします。 [Type] ドロップダウン リストから [Dynamic PAT (Hide)] を選択します。 [Translated Addr] フィールドで、外部インターフェイスを反映するオプションを選択します。 [Advanced] をクリックします。



4. [Source Interface] および [Destination Interface] のドロップダウン リストで、適切なインターフェイスを選択します。 [OK] をクリックし、次に [Apply] をクリックし、変更を有効にします。



この PAT 設定に対応する CLI 出力を以下に示します。

```
object network obj_172.16.11.0
subnet 172.16.11.0 255.255.255.0
nat (inside,outside) dynamic interface
```

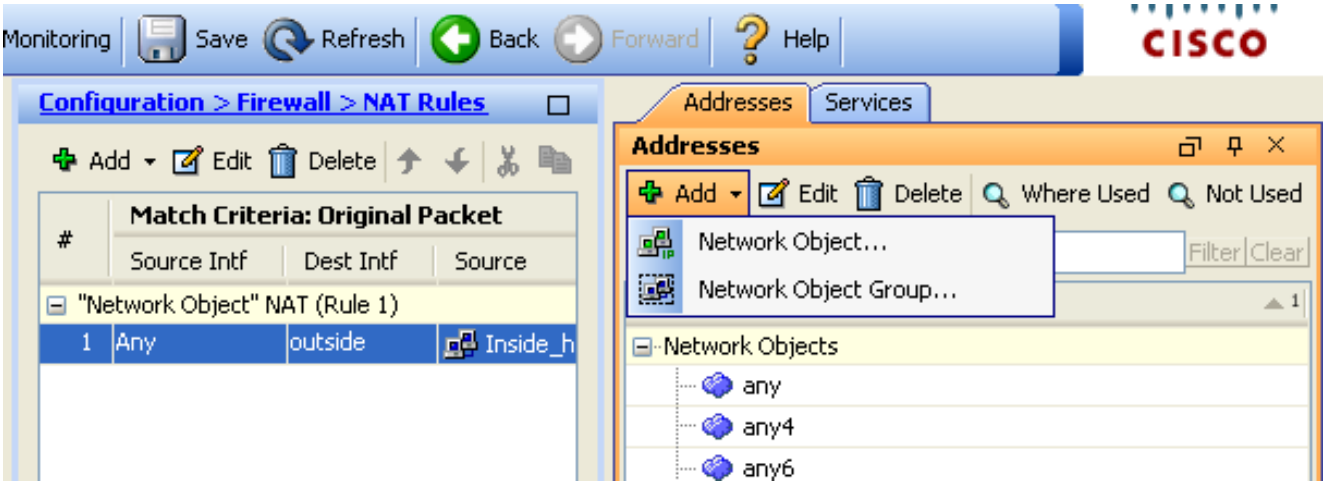
NAT を使用した inside ホストから outside ネットワークへのアクセスの許可

inside ホスト/ネットワークのグループに対して outside ネットワークへのアクセスを許可するには、ダイナミック NAT ルールを設定します。 PAT とは異なり、ダイナミック NAT はアドレスプールから変換されたアドレスを割り当てます。 その結果、ホストは自身の変換された IP アドレスにマッピングされ、2 つのホストが同じ変換された IP アドレスを共有することはできません。

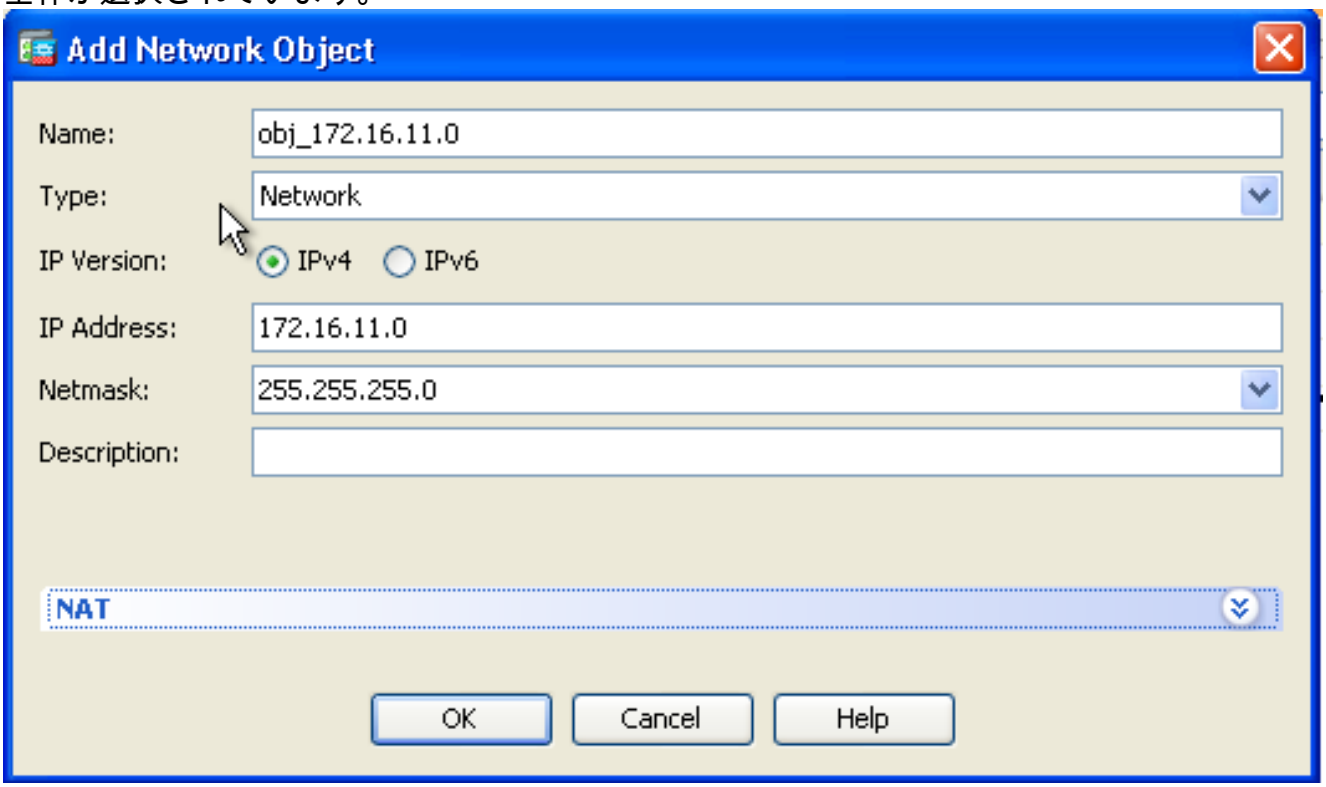
このためには、アクセスを許可するホスト/ネットワークの実アドレスを選択し、変換 IP アドレスのプールにマップする必要があります。

NAT を使用して inside ホストから outside ネットワークへのアクセスを許可するには、次の手順を実行します。

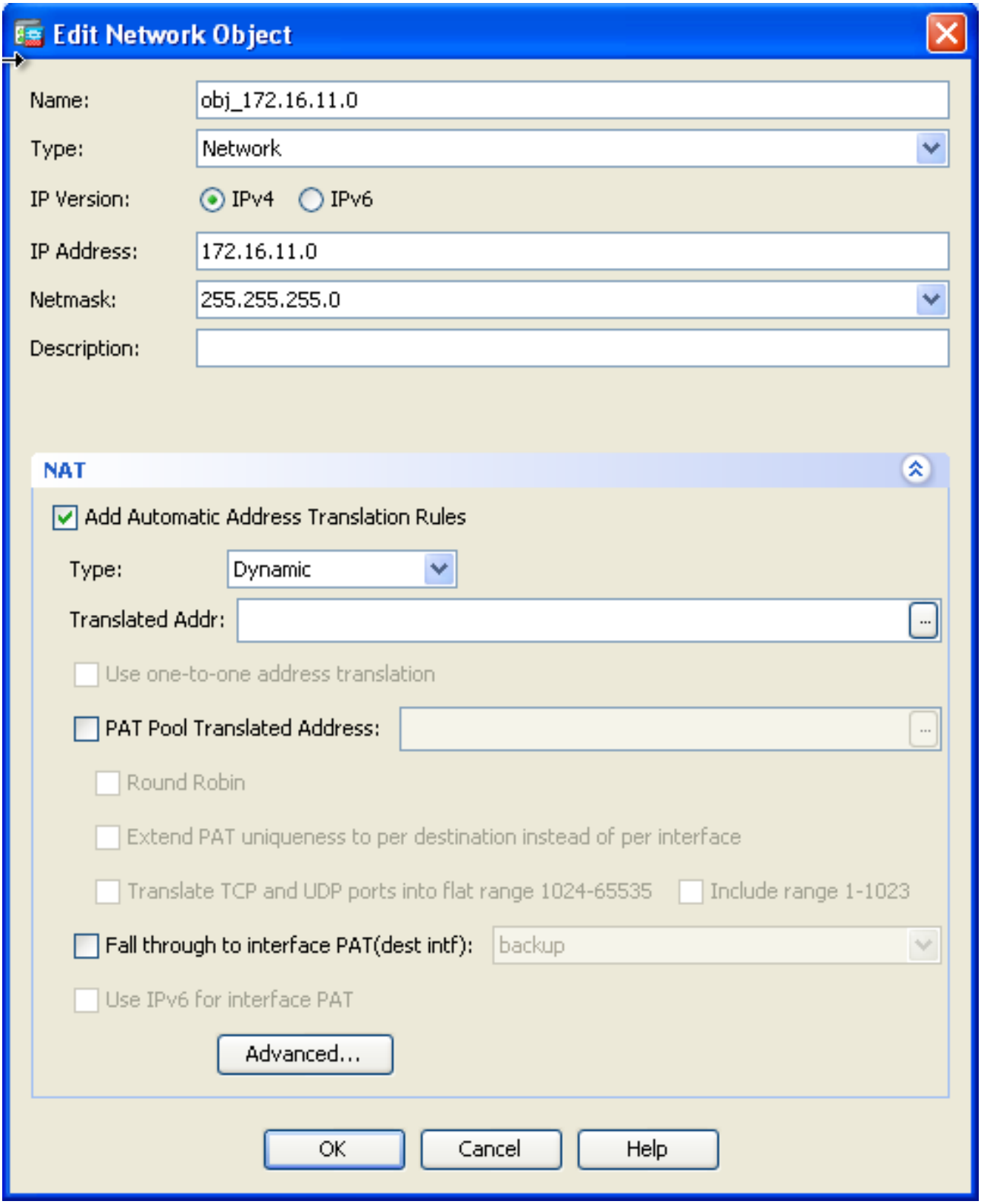
1. [Configuration] > [Firewall]> [NAT Rules] を選択します。 ダイナミック NAT ルールを設定するには、[Add] をクリックし、次に [Network Object] を選択します。



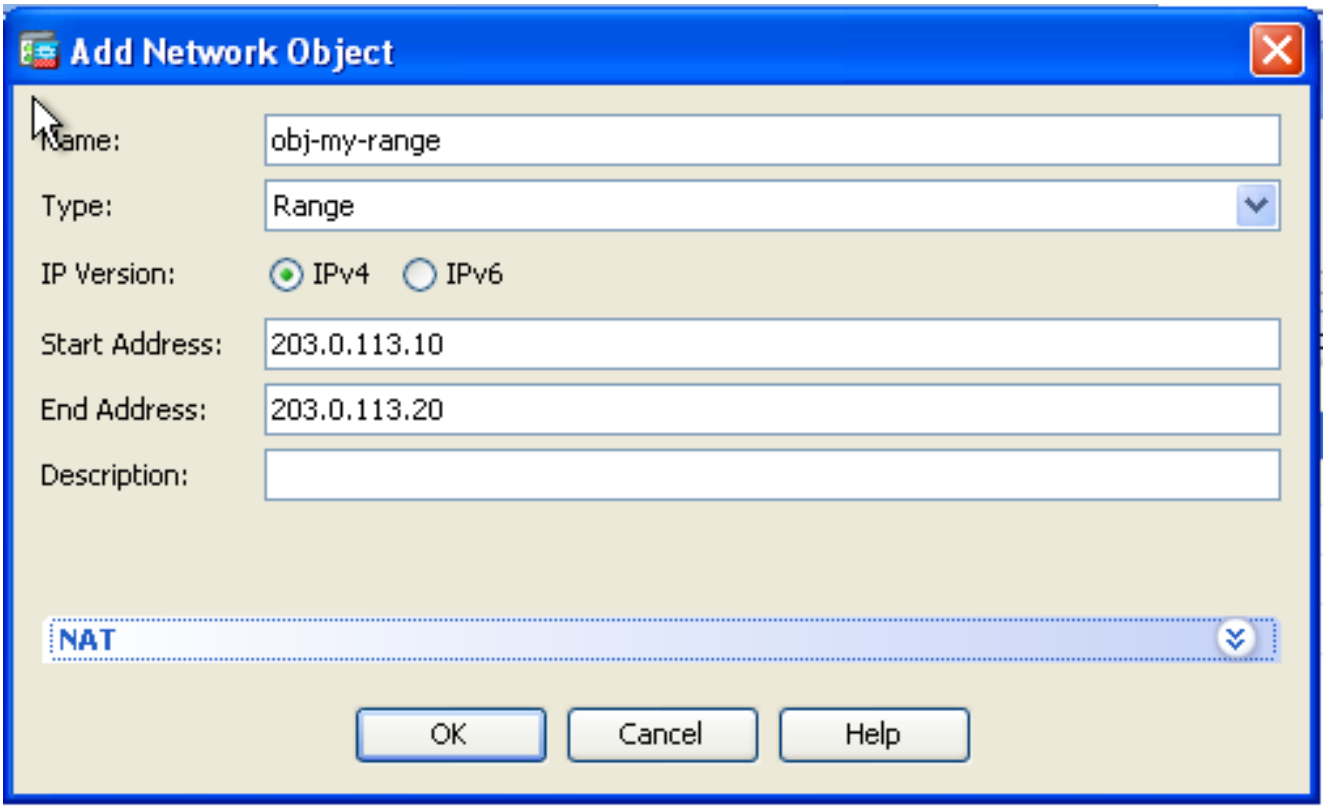
2. Dynamic PAT が必要なネットワーク/ホスト/範囲を設定します。 この例では *inside-network* 全体が選択されています。



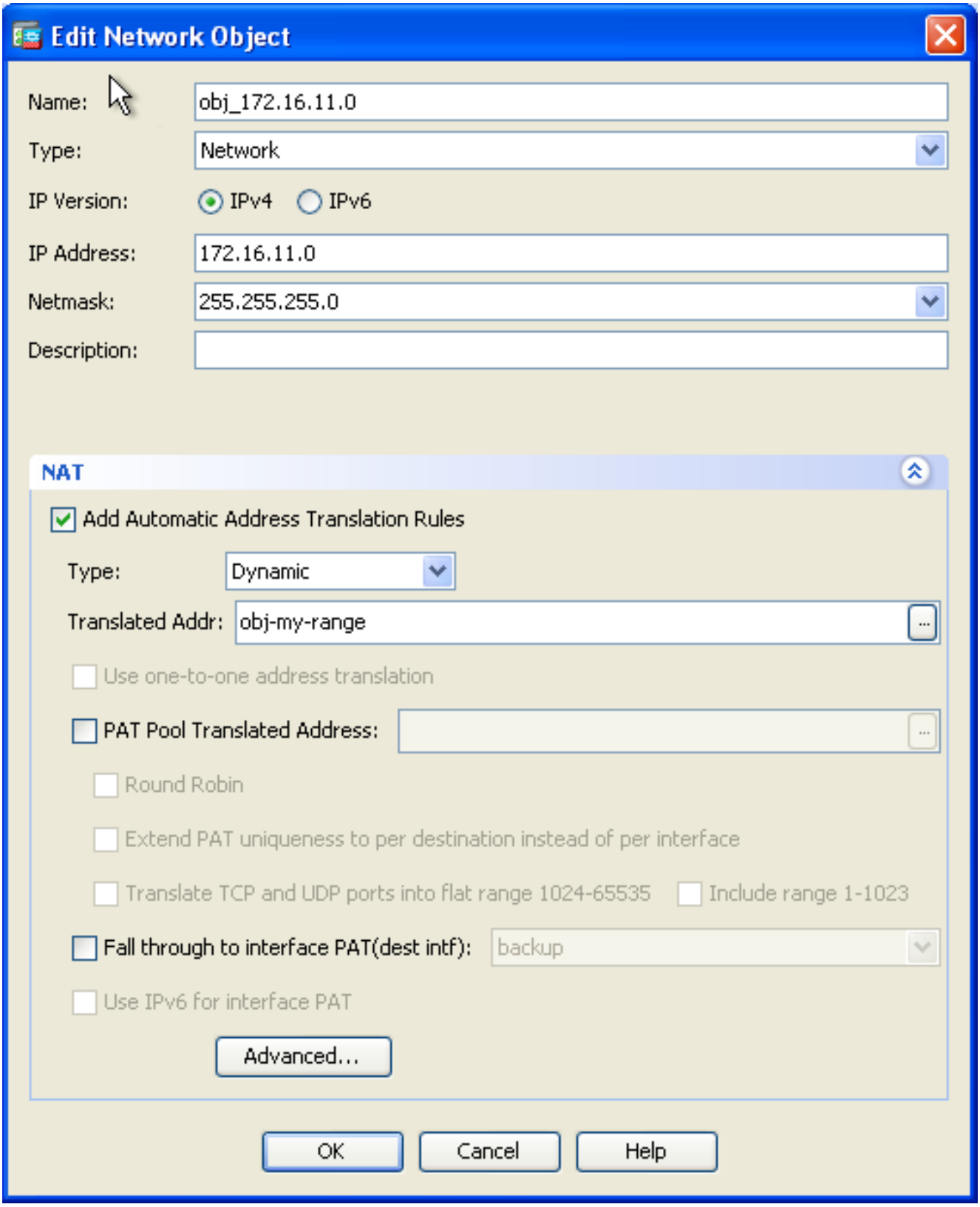
3. [NAT] を展開します。 [Add Automatic Address Translation Rules] チェックボックスをオンにします。 [Type] ドロップダウン リストから、[Dynamic] を選択します。 [Translated Addr] フィールドで、適切なオプションを選択します。 [Advanced] をクリックします。



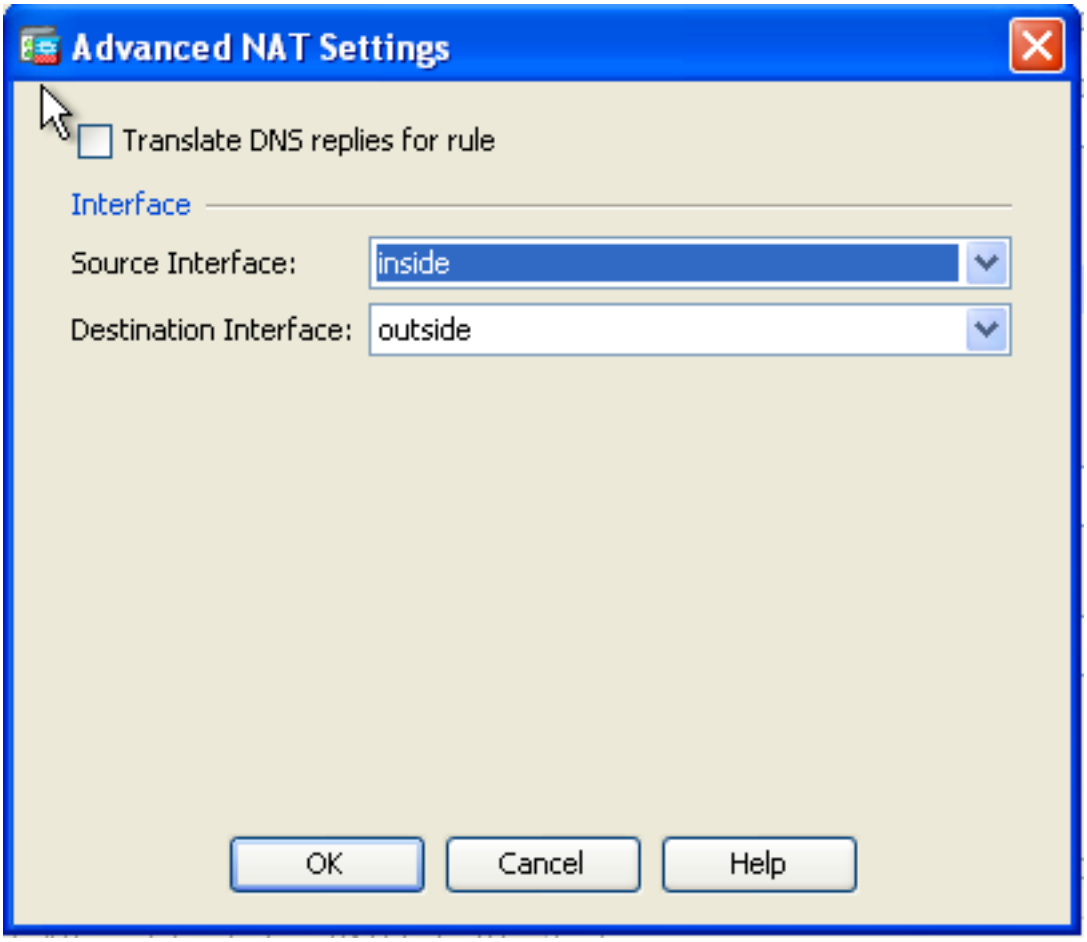
4. [Add] をクリックして、ネットワーク オブジェクトを追加します。 [Type] ドロップダウン リストから、[Range] を選択します。 [Start Address] および [End Address] フィールドに、PAT IP アドレスの開始と終了を入力します。 [OK] をクリックします。



5. [Translated Addr] フィールドで、アドレス オブジェクトを選択します。 送信元と宛先インターフェイスを選択するには、[Advanced] をクリックします。



6. [Source Interface] および [Destination Interface] のドロップダウン リストで、適切なインターフェイスを選択します。 [OK] をクリックし、次に [Apply] をクリックし、変更を有効にします。

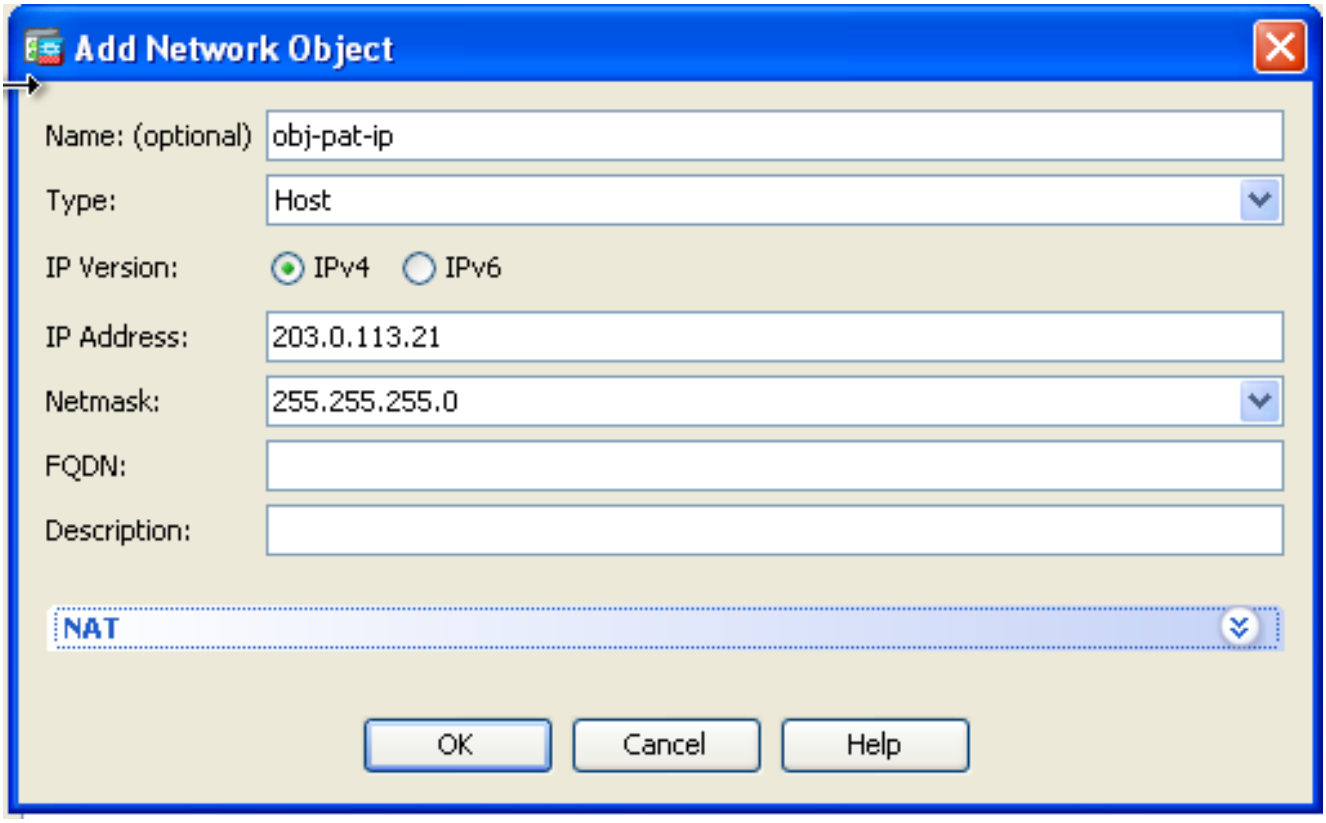


この ASDM 設定に対応する CLI 出力を以下に示します。

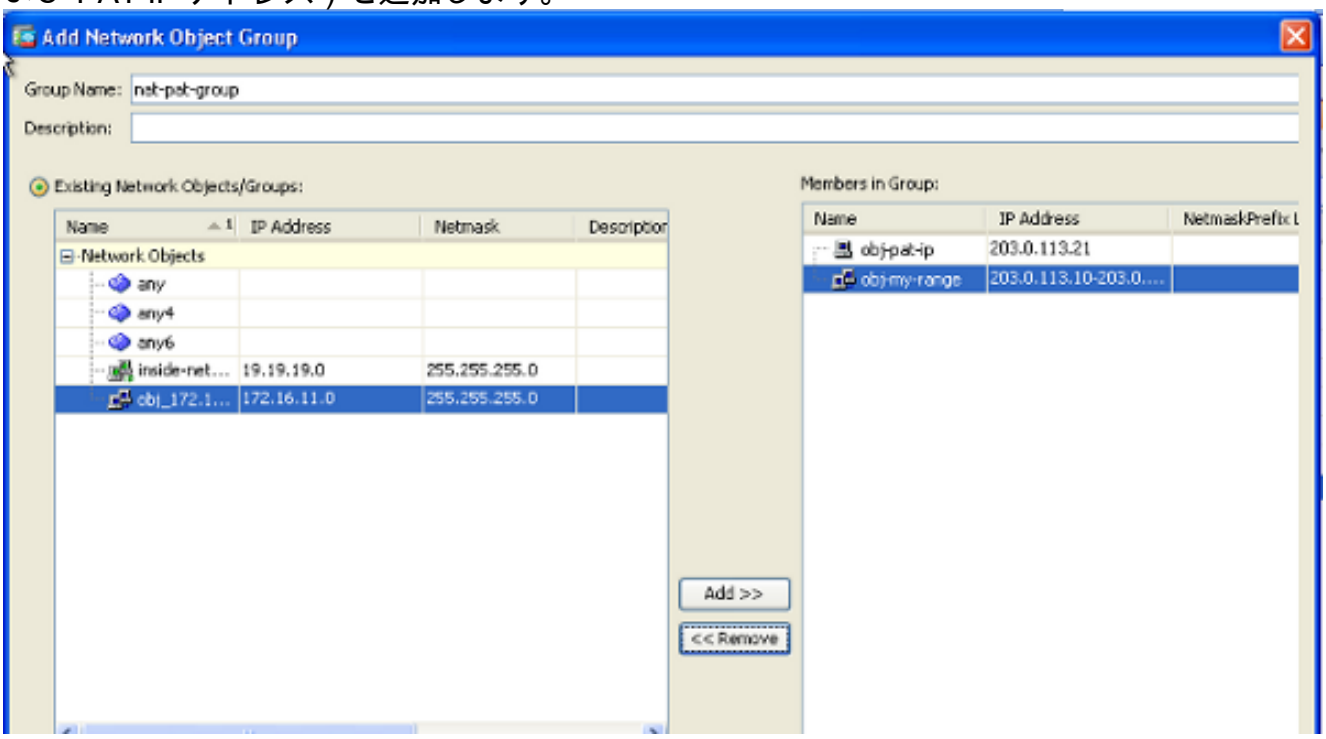
```
object network obj-my-range
range 203.0.113.10 203.0.113.20

object network obj_172.16.11.0
subnet 172.16.11.0 255.255.255.0
nat(inside,outside) dynamic obj-my-range
```

この設定では 172.16.11.0 ネットワークのホストは NAT プールの IP アドレス (203.0.113.10 ~ 203.0.113.20) のいずれかに変換されます。 マッピングされたプールにあるアドレスが実際のグループより少ない場合、アドレスが不足する可能性があります。 その結果、ダイナミック PAT バックアップを備えたダイナミック NAT を実装するか、既存のプールの拡張を試すことができます。

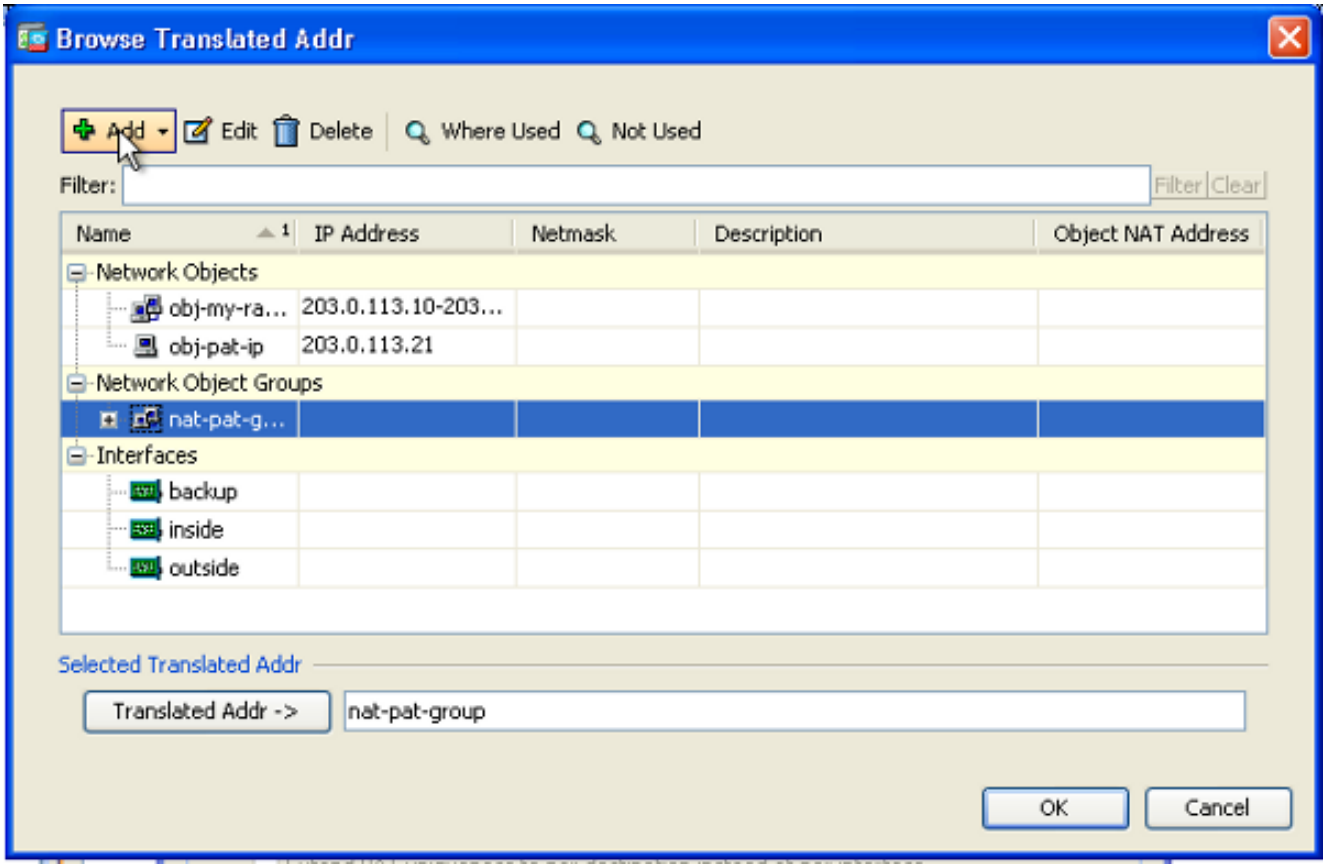
1. ネットワーク オブジェクトを追加するには、前の設定の手順 1 ~ 3 を繰り返し、[Add] をもう一度クリックします。 [Type] ドロップダウン リストから、[Host] を選択します。 [IP Address] フィールドに、PAT バックアップの IP アドレスを入力します。 [OK] をクリックします。



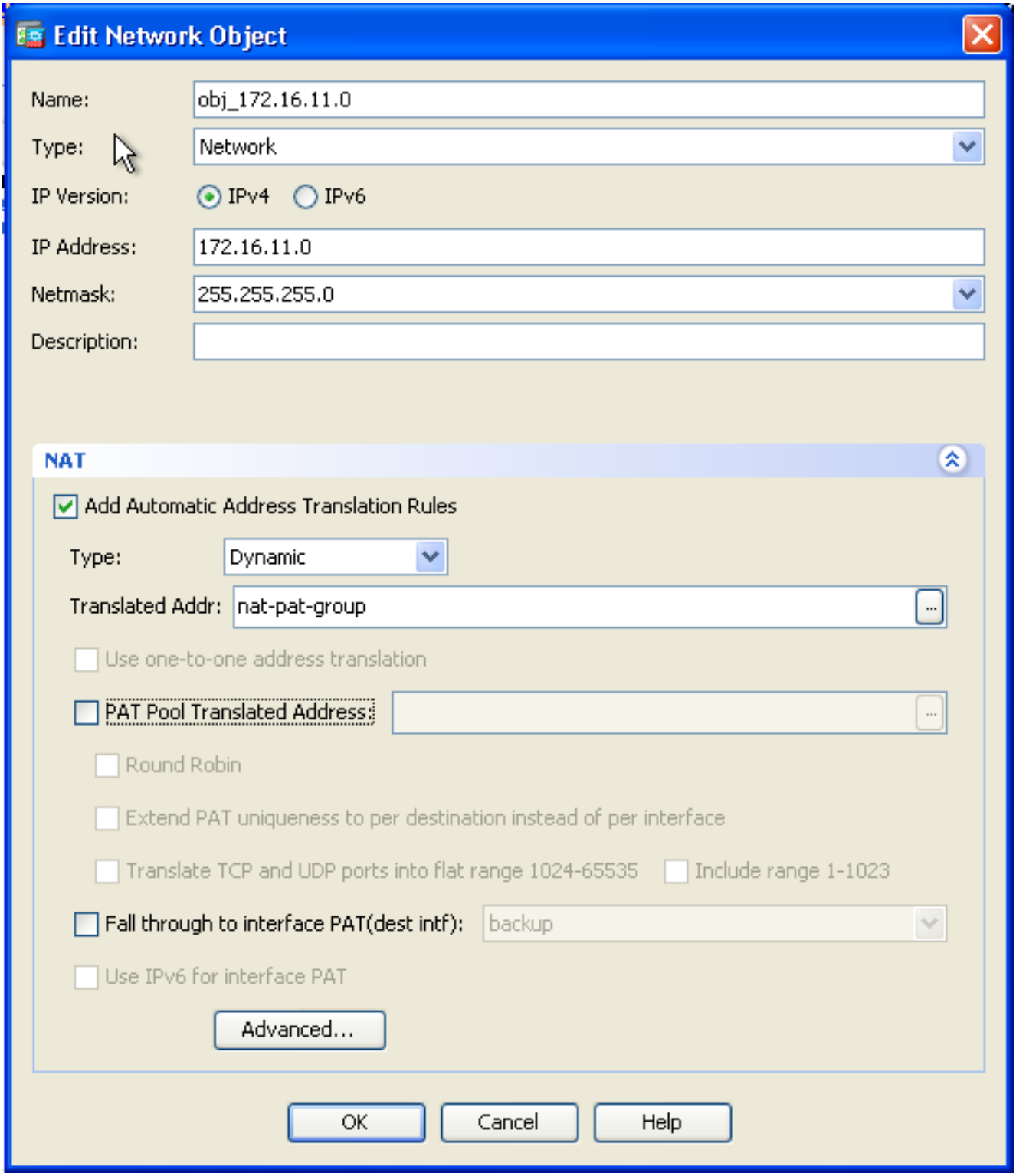
2. [Add] をクリックして、ネットワーク オブジェクト グループを追加します。 [Group Name] フィールドにグループ名を入力し、グループの両方のアドレス オブジェクト（NAT 範囲および PAT IP アドレス）を追加します。



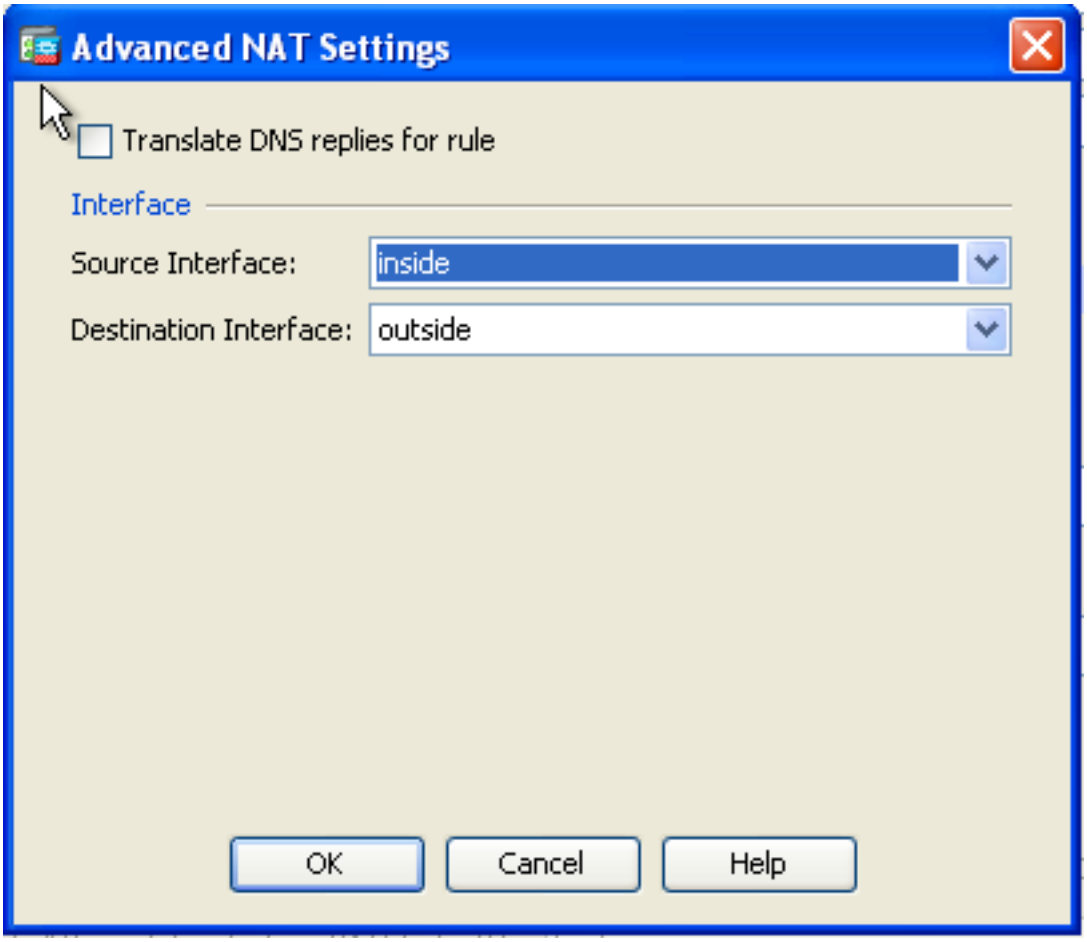
3. 設定した NAT ルールを選択し、[Translated Addr] を新しく設定されたグループ「nat-pat-group」（以前は「obj-my-range」だった）に変更します。 [OK] をクリックします。



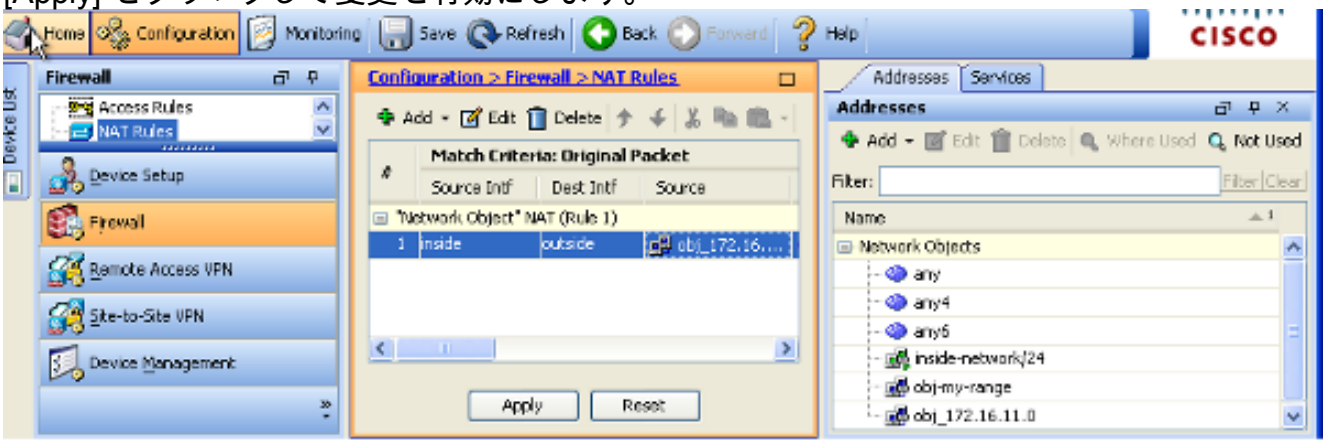
4. NAT ルールを追加するには、[OK] をクリックします。 送信元と宛先インターフェイスを選択するには、[Advanced] をクリックします。



5. [Source Interface] および [Destination Interface] のドロップダウン リストで、適切なインターフェイスを選択します。 [OK] をクリックします。



6. [Apply] をクリックして変更を有効にします。



この ASDM 設定に対応する CLI 出力を以下に示します。

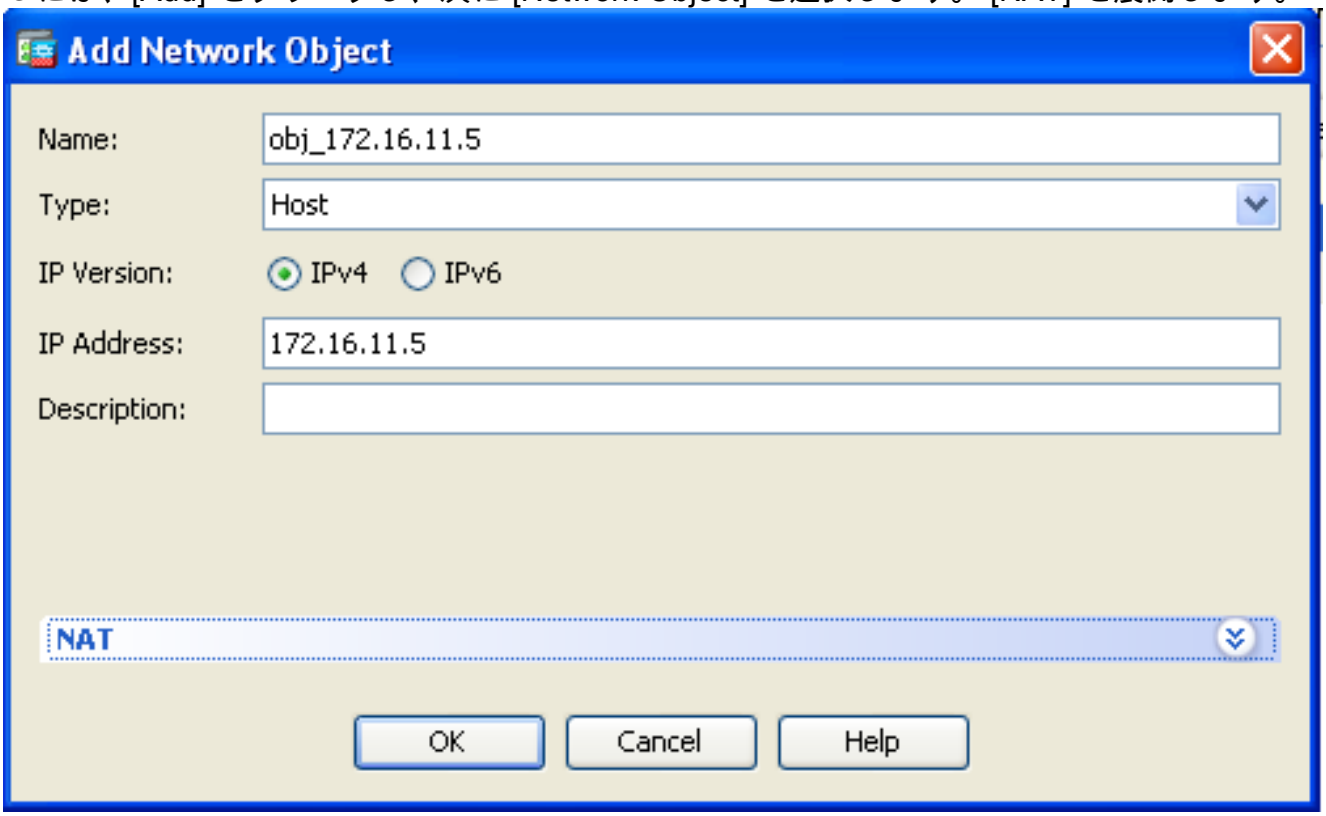
```
object network obj-my-range
range 203.0.113.10 203.0.113.20

object network obj-pat-ip
host 203.0.113.21

object-group network nat-pat-group
network-object object obj-my-range
network-object object obj-pat-ip

object network obj_172.16.11.0
subnet 172.16.11.0 255.255.255.0
```

```
nat (inside,outside) dynamic nat-pat-group
```

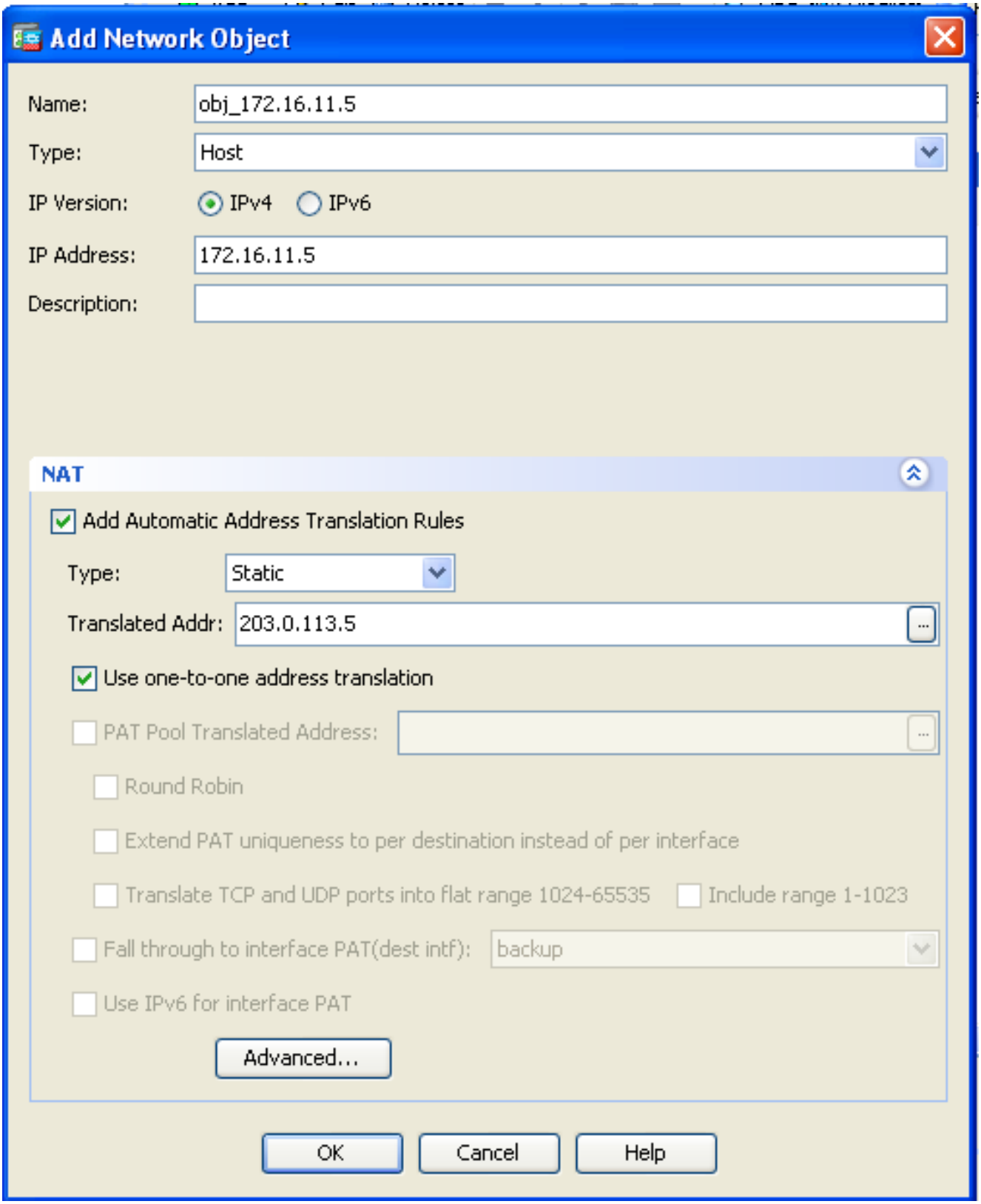
信頼できないホストから信頼できるネットワーク上のホストへのアクセスの許可

スタティック NAT 変換とアクセス ルールを適用して、これらのホストに対しアクセスを許可します。 外部ユーザが内部ネットワーク上の任意のサーバにアクセスできるようにするには、このように設定する必要があります。 内部ネットワークのサーバにはプライベート IP アドレスが設定されます。このプライベート IP アドレスは、インターネット上でルーティング不可能です。このため、スタティック NAT ルールを使用してプライベート IP アドレスをパブリック IP アドレスに変換する必要があります。 1 つの内部サーバ (172.16.11.5) があるとします。 このようにアクセスを許可するには、このプライベート サーバ IP アドレスをパブリック IP アドレスに変換する必要があります。 この例では、172.16.11.5 を 203.0.113.5 に変換するために双方向スタティック NAT を実装する方法を説明します。

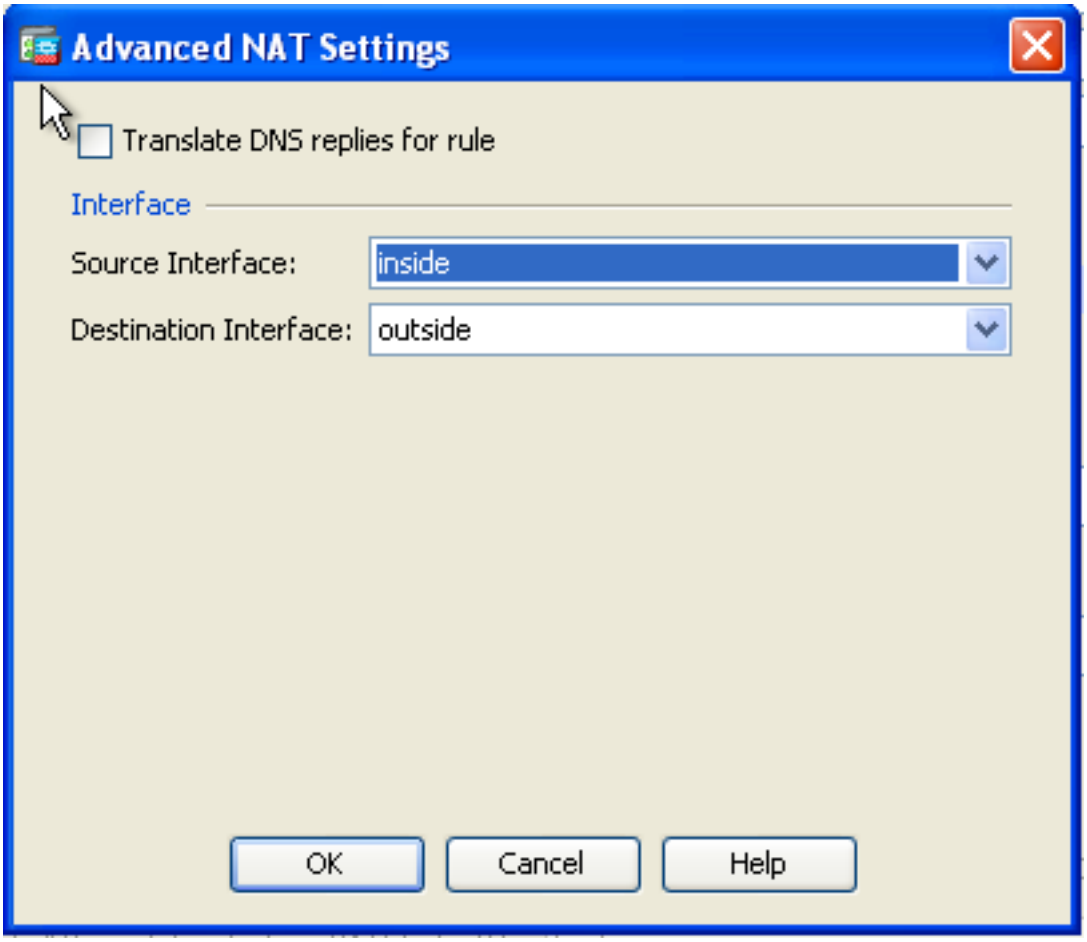
1. [Configuration] > [Firewall]> [NAT Rules] を選択します。 スタティック NAT ルールを設定するには、[Add] をクリックし、次に [Network Object] を選択します。 [NAT] を展開します。



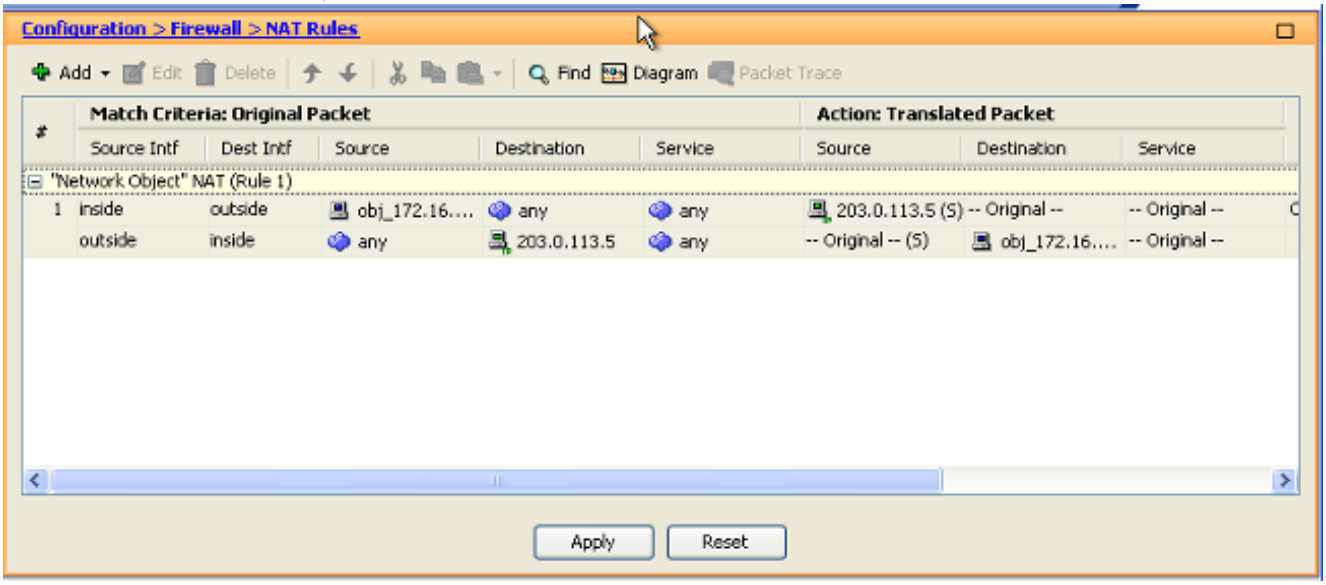
2. [Add Automatic Address Translation Rules] チェックボックスをオンにします。 [Type] ドロップダウン リストから、[Static] を選択します。 [Translated Addr] フィールドに、IP アドレスを入力します。 送信元と宛先インターフェイスを選択するには、[Advanced] をクリックします。



3. [Source Interface] および [Destination Interface] のドロップダウン リストで、適切なインターフェイスを選択します。 [OK] をクリックします。



4. 設定したスタティック NAT エントリは次のように表示されます。 [Apply] をクリックしてこれを ASA に送信します。



この NAT 設定に対応する CLI 出力を以下に示します。

```
object network obj_172.16.11.5
host 172.16.11.5
nat (inside,outside) static 203.0.113.5
```

スタティック アイデンティティ NAT

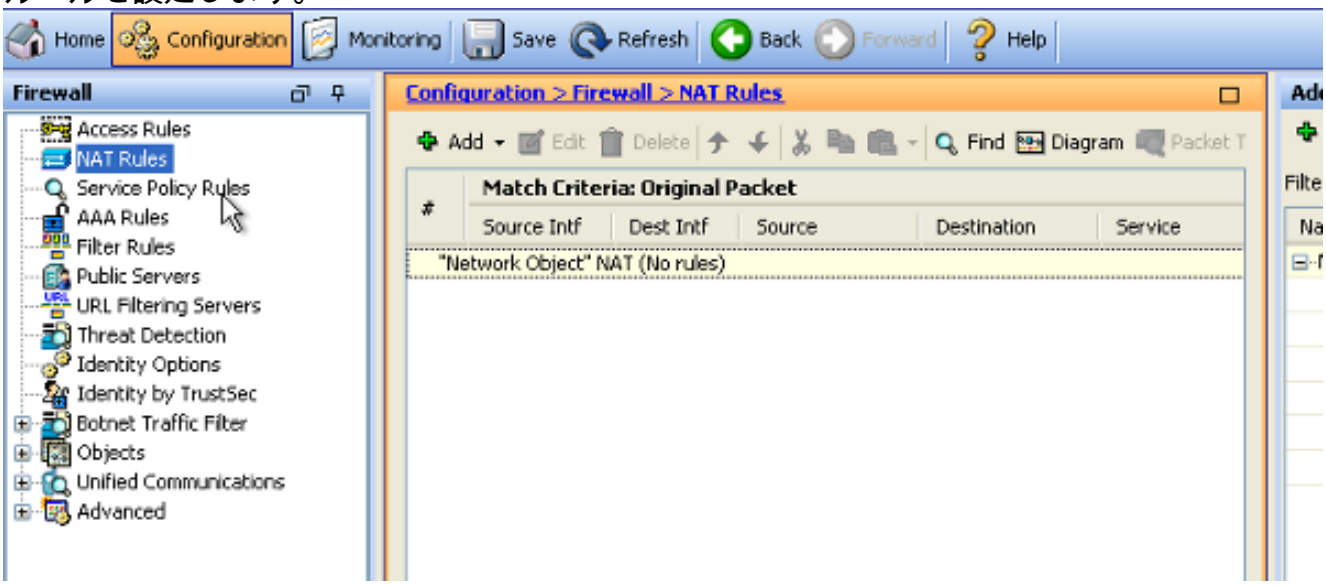
NAT 免除は、内部のユーザが NAT の完了なしに、リモート VPN ホスト/サーバ、または ASA の他のインターフェイスの背後にあるホスト/サーバにアクセスしようとする場合に便利な機能です

。 このためには、プライベート IP アドレスをもつ内部サーバが、それ自身に変換されるアイデンティティになり、代わりに NAT を実行する宛先へのアクセスを許可されます。

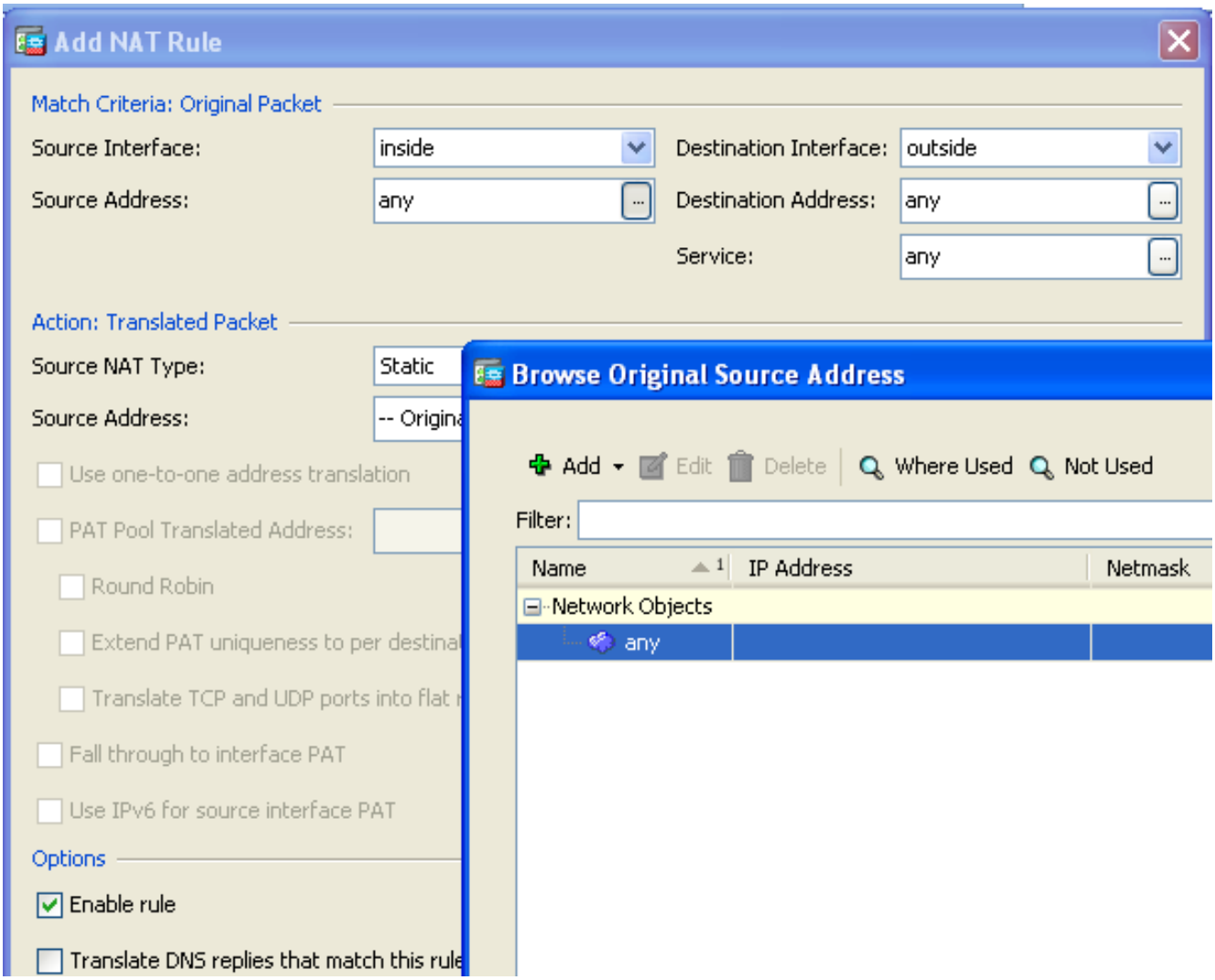
この例では、内部ホスト 172.16.11.15 は、リモート VPN サーバの 172.20.21.15 にアクセスする必要があります。

NAT を完了して inside ホストから リモート VPN ネットワークへのアクセスを許可するには、次の手順を実行します。

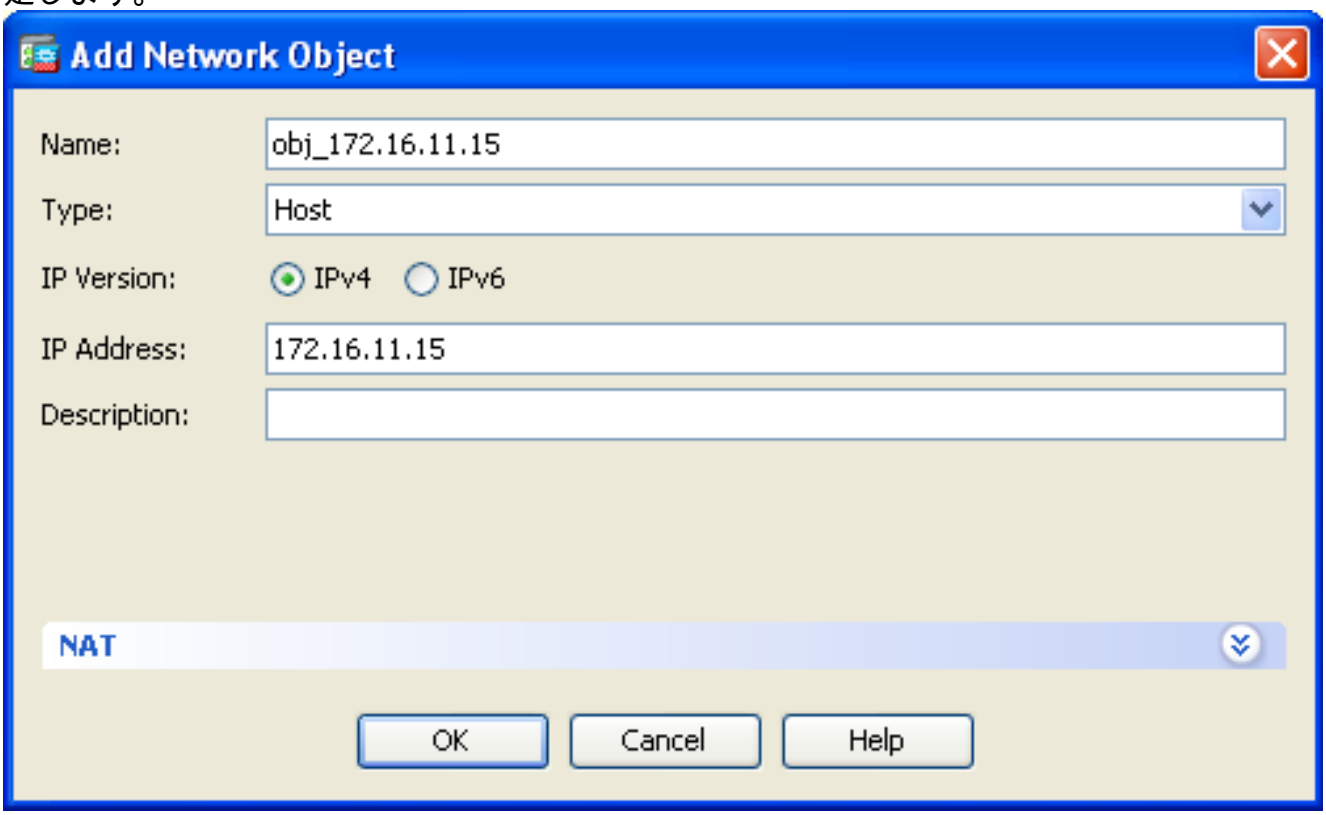
1. [Configuration] > [Firewall]> [NAT Rules] を選択します。 **[Add]** をクリックして、NAT 免除ルールを設定します。



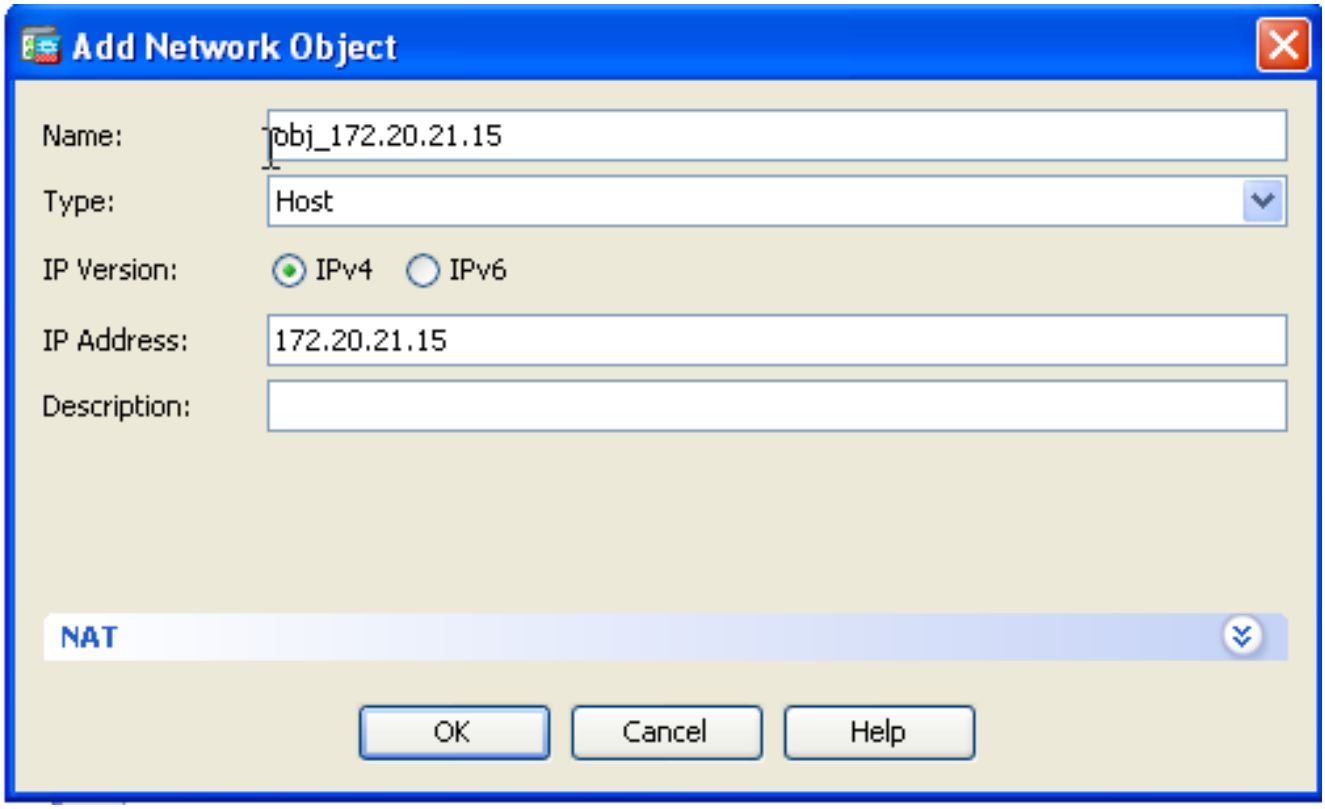
2. [Source Interface] および [Destination Interface] のドロップダウン リストで、適切なインターフェイスを選択します。 [Source Address] フィールドで、適切なエントリを選択します。



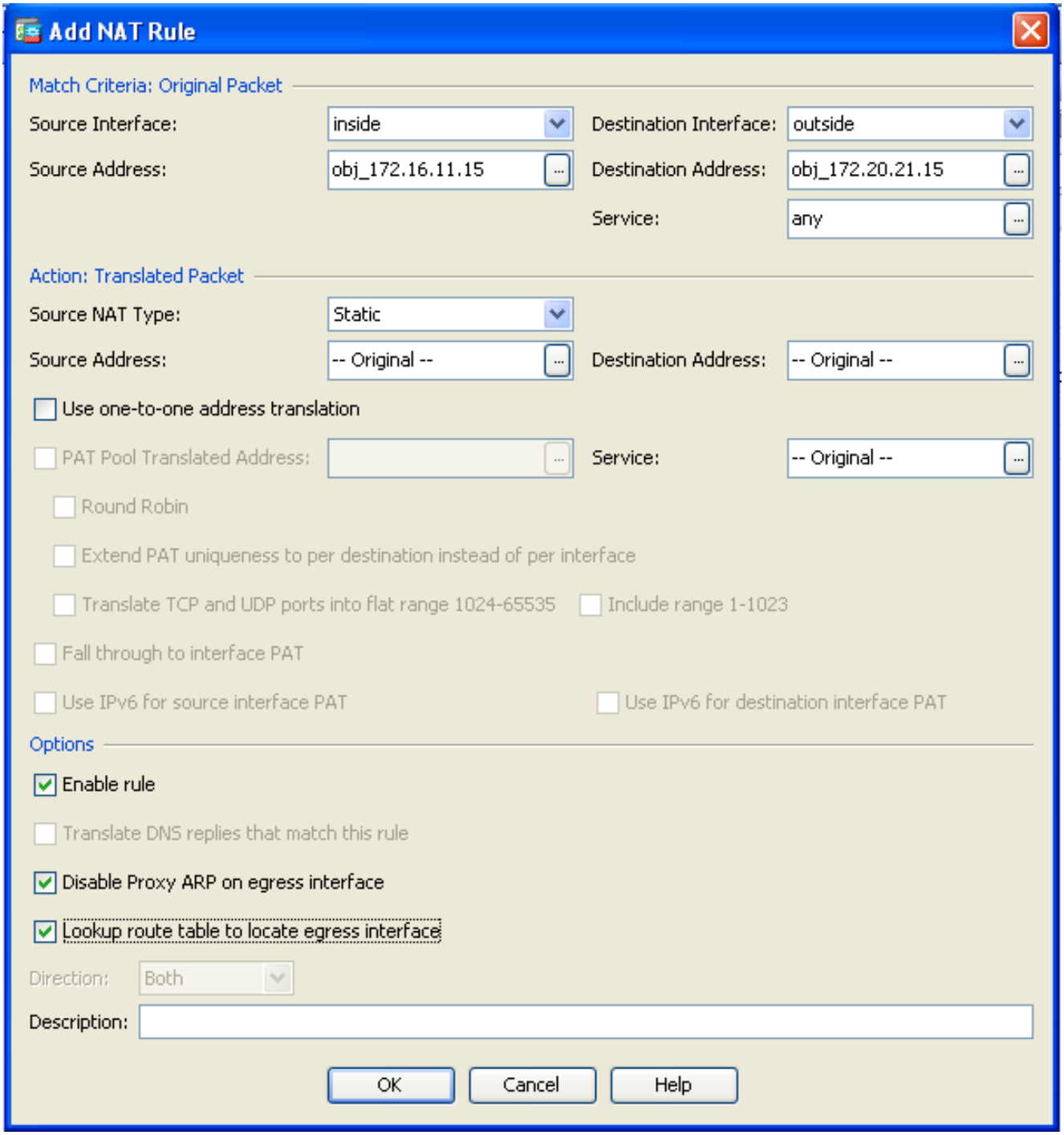
3. [Add] をクリックして、ネットワーク オブジェクトを追加します。 ホスト IP アドレスを設定します。



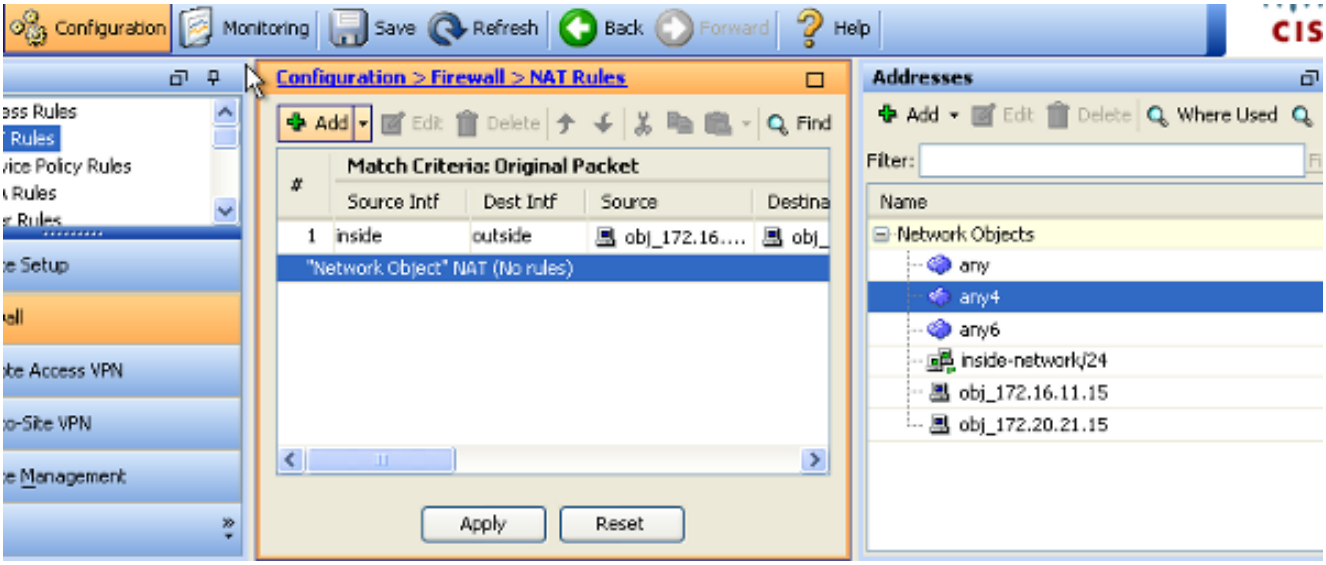
4. 同様に、[Destination Address] を検索します。 [Add] をクリックして、ネットワーク オブジェクトを追加します。 ホスト IP アドレスを設定します。



5. 設定された [Source Address] および [Destination Address] オブジェクトを選択します。 [Disable Proxy ARP on egress interface] および [Lookup route table to locate egress interface] のチェックボックスをオンにします。 [OK] をクリックします。



6. [Apply] をクリックして変更を有効にします。



この NAT 免除またはアイデンティティ NAT 設定に対応する CLI 出力を以下に示します。

```
object network obj_172.16.11.15
host 172.16.11.15
object network obj_172.20.21.15
host 172.20.21.15

nat (inside,outside) source static obj_172.16.11.15 obj_172.16.11.15
destination static obj_172.20.21.15 obj_172.20.21.15 no-proxy-arp route-lookup
```

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)

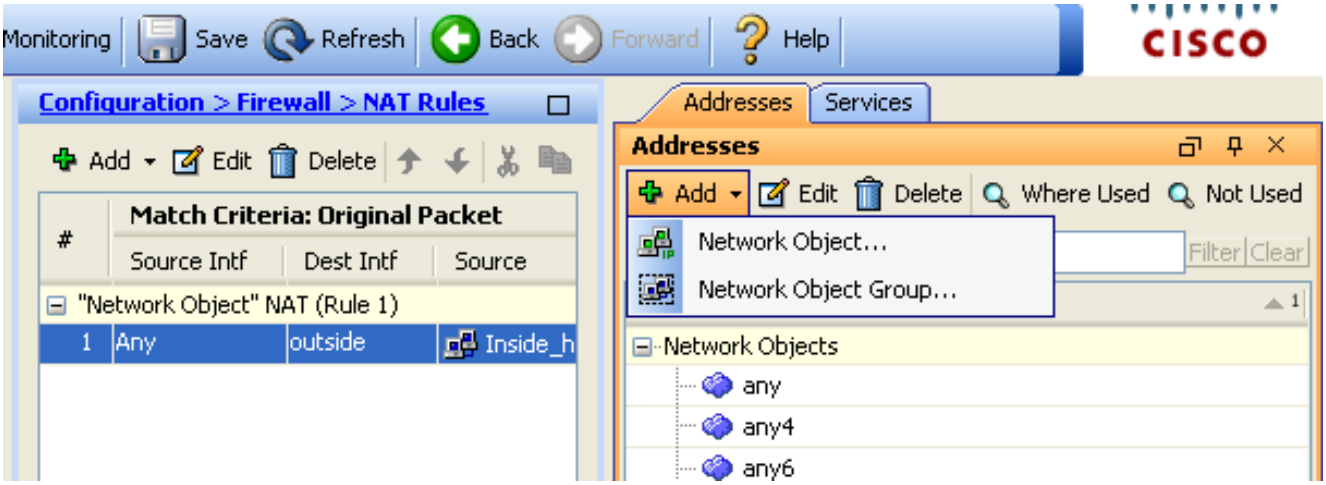
ポート フォワーディング (ポート リダイレクション) は、外部ユーザが特定ポートから内部サーバにアクセスする場合に便利な機能です。 このためには、内部サーバに設定されているプライベート IP アドレスをパブリック IP アドレスに変換し、特定のポートでのアクセスを許可します。

以下の例では、外部ユーザが SMTP サーバ 203.0.115.15 にポート 25 でアクセスすることを求めています。 このためには次の 2 つの手順を実行します。

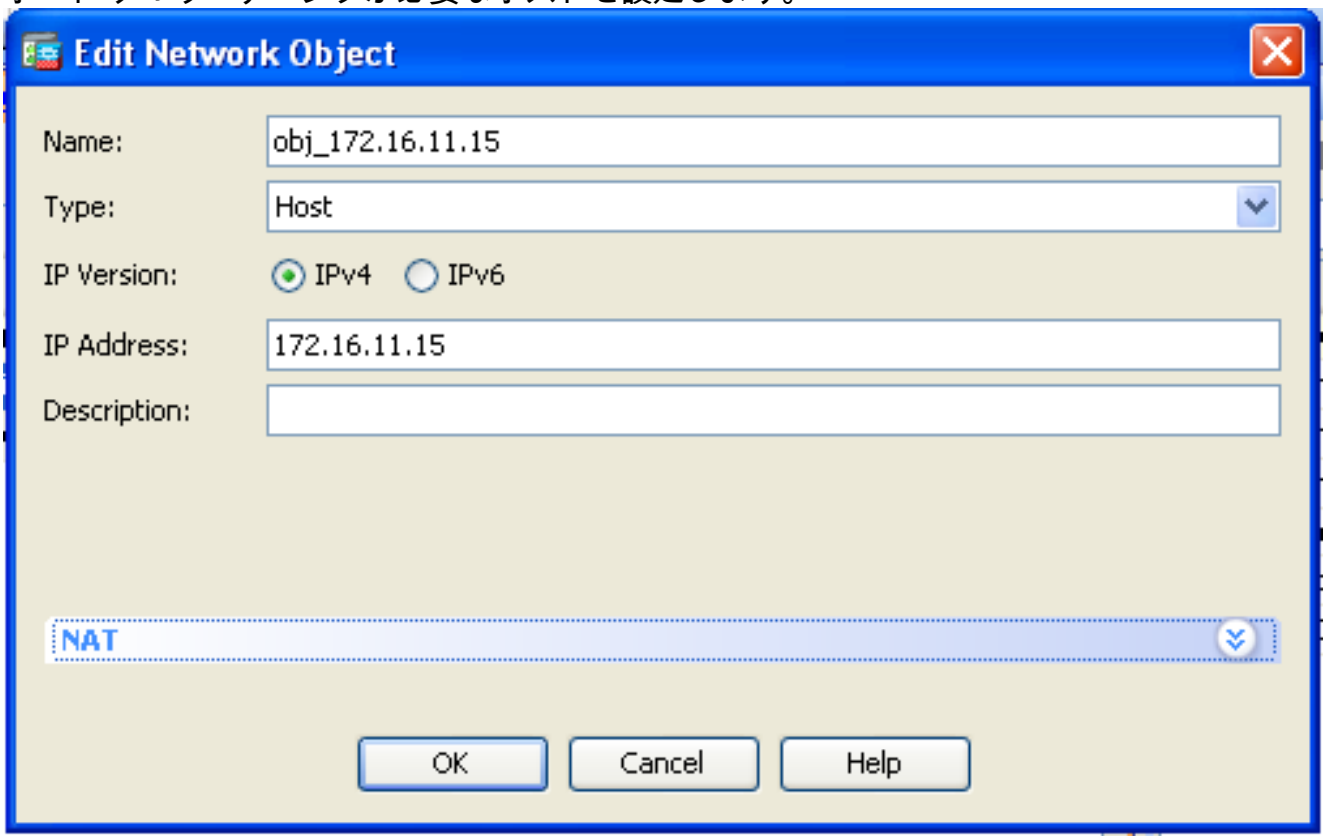
1. 内部メール サーバ 172.16.11.15、ポート 25 をパブリック IP アドレス 203.0.115.15、ポート 25 に変換します。
2. パブリック メール サーバ 203.0.115.15 へのポート 25 でのアクセスを許可します。

外部ユーザがこのサーバ 203.0.115.15、ポート 25 にアクセスしようとすると、このトラフィックは内部メール サーバ 172.16.11 15、ポート 25 にリダイレクトされます。

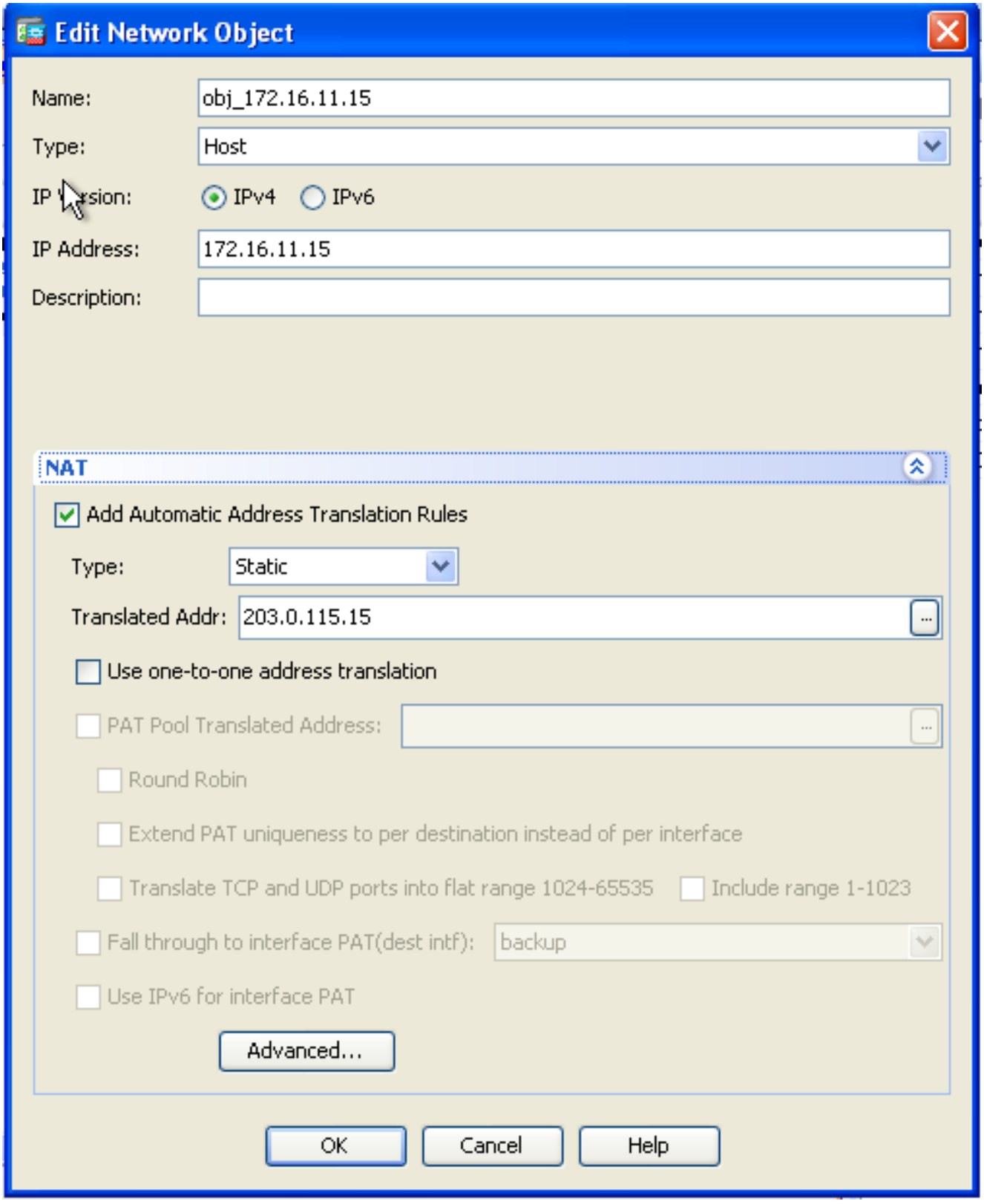
1. [Configuration] > [Firewall] > [NAT Rules] を選択します。 スタティック NAT ルールを設定するには、[Add] をクリックし、次に [Network Object] を選択します。



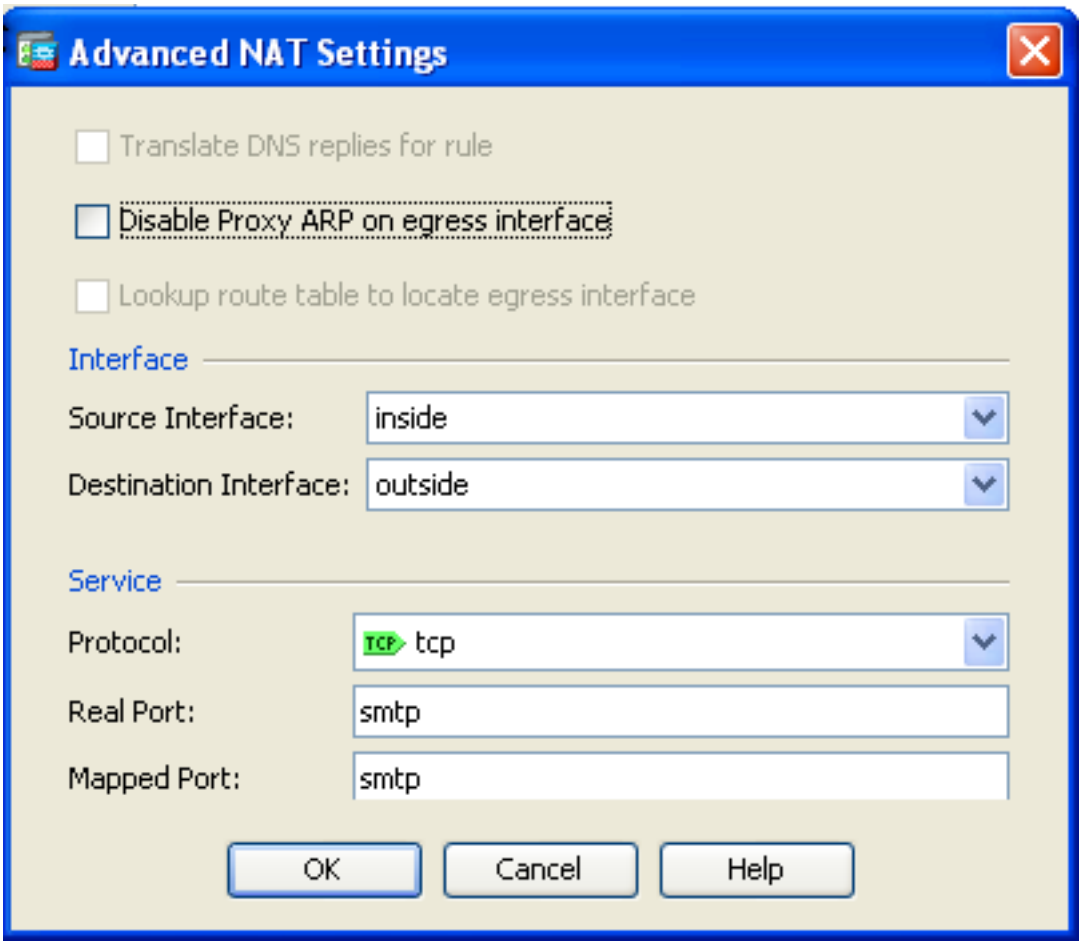
2. ポート フォワーディングが必要なホストを設定します。



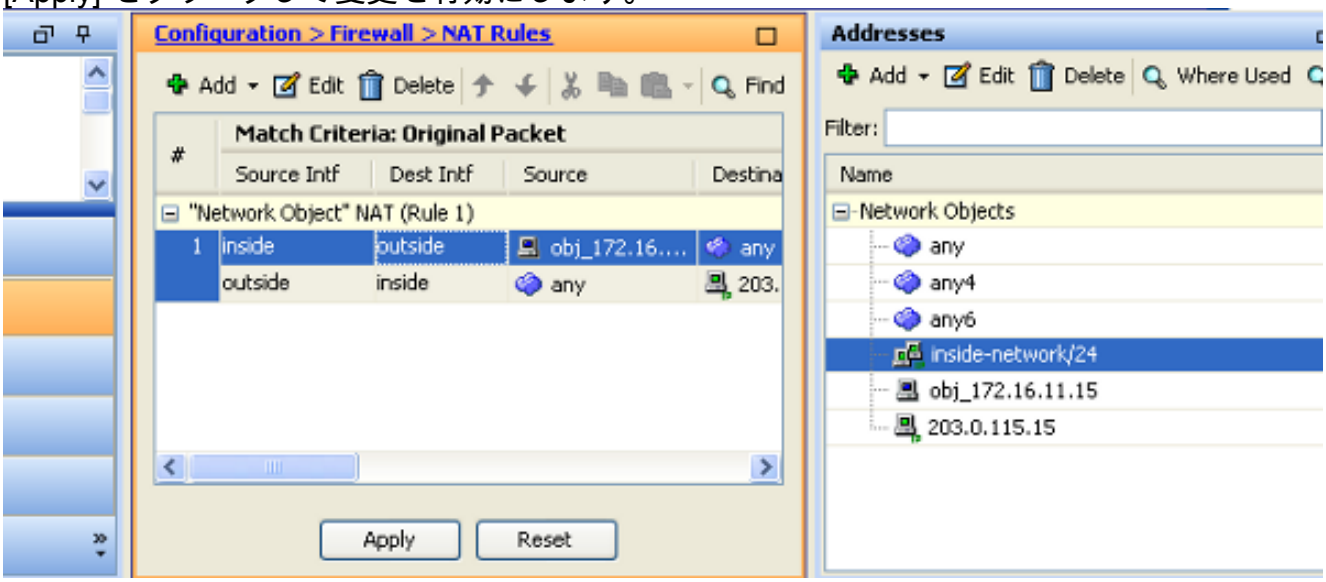
3. [NAT] を展開します。 [Add Automatic Address Translation Rules] チェックボックスをオンにします。 [Type] ドロップダウン リストから、[Static] を選択します。 [Translated Addr] フィールドに、IP アドレスを入力します。 サービスおよび送信元と宛先のインターフェイスを選択するには、[Advanced] をクリックします。



4. [Source Interface] および [Destination Interface] のドロップダウン リストで、適切なインターフェイスを選択します。 サービスを設定します。 [OK] をクリックします。



5. [Apply] をクリックして変更を有効にします。



この NAT 設定に対応する CLI 出力を以下に示します。

```
object network obj_172.16.11.15
host 172.16.11.15
nat (inside,outside) static 203.0.115.15 service tcp smtp smtp
```

確認

このセクションでは、設定が正常に機能していることを確認します。

Cisco CLI アナライザ（登録ユーザ専用）は、特定の **show** コマンドをサポートしています。

show コマンド出力の分析を表示するには、Cisco CLI アナライザを使用します。

Web ブラウザで HTTP を介して Web サイトにアクセスします。 この例では 198.51.100.100 でホストされているサイトを使用します。 接続が成功すると、次の出力が ASA CLI に表示されます。

接続

```
ASA(config)# show connection address 172.16.11.5
6 in use, 98 most used
TCP outside 198.51.100.100:80 inside 172.16.11.5:58799, idle 0:00:06, bytes 937,
flags UIO
```

ASA はステートフル ファイアウォールであり、Web サーバからのリターン トラフィックはファイアウォール接続テーブルの***接続***の 1 つと一致するため、ファイアウォールの通過を許可されます。 事前に存在する接続の 1 つと一致するトラフィックは、インターフェイス ACL によってブロックされないでファイアウォールの通過を許可されます。

上の出力では、内部インターフェイス上のクライアントが外部インターフェイスからの 198.51.100.100 ホストへの接続を確立しました。 この接続では TCP プロトコルが使用されており、6 秒間アイドル状態です。 接続のフラグは、この接続の現在の状態を示します。 接続のフラグの詳細については、「ASA の TCP 接続フラグ」を参照してください。

Syslog

```
ASA(config)# show log | in 172.16.11.5

Apr 27 2014 11:31:23: %ASA-6-305011: Built dynamic TCP translation from inside:
172.16.11.5/58799 to outside:203.0.113.2/58799

Apr 27 2014 11:31:23: %ASA-6-302013: Built outbound TCP connection 2921 for outside:
198.51.100.100/80 (198.51.100.100/80) to inside:172.16.11.5/58799 (203.0.113.2/58799)
```

ASA ファイアウォールは正常動作中に syslog を生成します。 syslog の冗長さはログ設定に基づいて変化します。 この出力はレベル 6、つまり「情報」レベルでの 2 種類の syslog を示します。

この例では、2 種類の syslog が生成されています。 1 番目は、ファイアウォールが変換を作成したこと、具体的にはダイナミック TCP 変換（PAT）を行ったことを示すログ メッセージです。 これは、トラフィックが内部インターフェイスから外部インターフェイスに渡るときの、送信元 IP アドレスとポート、および変換後の IP アドレスとポートを示します。

2 番目の syslog は、ファイアウォールがクライアントとサーバ間のこの特定のトラフィック用に接続テーブルで接続を作成したことを示します。 この接続試行をブロックするようにファイアウォールが設定された場合や、その他の要因（リソース制約または設定ミスの可能性）によってこの接続の作成が妨げられる場合は、ファイアウォールは接続が確立されたことを示すログを生成しません。 通常は、代わりに、接続が拒否される理由や、接続の作成を妨げた要因に関する兆候を記録します。

Packet Tracer

```
ASA(config)# packet-tracer input inside tcp 172.16.11.5 1234 198.51.100.100 80
```

```
--Omitted--

Result:
input-interface: inside
input-status: up
input-line-status: up
output-interface: outside
output-status: up
output-line-status: up
Action: allow
```

ASA のパケット トレーサ機能を使用すると、*シミュレート*されたパケットを指定して、ファイアウォールでトラフィックを処理するときに通るさまざまなステップ、チェック、機能をすべて確認できます。 このツールを使用すると、ファイアウォールをパス スルーすることが許可されるはずのトラフィックの例を識別するために役立ち、その 5 タプルを使用してトラフィックをシミュレートできます。 前記の例では、以下の条件を満たす接続試行をシミュレートするために、パケット トレーサを使用します。

- シミュレートされたパケットが内部に到達する。
- 使用されているプロトコルが TCP である。
- シミュレートされたクライアントの IP アドレスが 172.16.11.5 である。
- クライアントは送信元がポート 1234 であるトラフィックを送信している。
- トラフィックは、IP アドレス 198.51.100.100 のサーバ宛てに送信される。
- トラフィックはポート 80 宛てである。

コマンドにインターフェイス outside に関する言及がないことに注意してください。 これはパケット トレーサの設計による動作です。 このツールは、このタイプの接続試行をファイアウォールでどのように処理するのかを示し、ルーティングの方法や、どのインターフェイスから送信するのかが含まれます。 パケット トレーサの詳細については、パケット トレースを使用したパケットのトレースを参照してください。

キャプチャ

キャプチャの適用

```
ASA# capture capin interface inside match tcp host 172.16.11.5 host 198.51.100.100
ASA# capture capout interface outside match tcp any host 198.51.100.100

ASA#show capture capin

3 packets captured

1: 11:31:23.432655 172.16.11.5.58799 > 198.51.100.100.80: S 780523448:
780523448(0) win 8192 <mss 1460,nop,wscale 2,nop,nop,sackOK>
2: 11:31:23.712518 198.51.100.100.80 > 172.16.11.5.58799: S 2123396067:
2123396067(0) ack 780523449 win 8192 <mss 1024,nop,nop,sackOK,nop,wscale 8>
3: 11:31:23.712884 172.16.11.5.58799 > 198.51.100.100.80: . ack 2123396068
win 32768

ASA#show capture capout

3 packets captured

1: 11:31:23.432869 203.0.113.2.58799 > 198.51.100.100.80: S 1633080465:
1633080465(0) win 8192 <mss 1380,nop,wscale 2,nop,nop,sackOK>
2: 11:31:23.712472 198.51.100.100.80 > 203.0.113.2.58799: S 95714629:
```

```
95714629(0) ack 1633080466 win 8192 <mss 1024,nop,nop,sackOK,nop,wscale 8>
3: 11:31:23.712914 203.0.113.2.58799 > 198.51.100.100.80: . ack 95714630
win 32768/pre>
```

ASA ファイアウォールでは、インターフェイスに着信または発信するトラフィックをキャプチャできます。 このキャプチャ機能は、トラフィックがファイアウォールに着信したかやファイアウォールから送信したかを確実に保証できるため便利です。 前の例は、内部インターフェイスの capin と外部インターフェイスの capout という 2 個のキャプチャの設定を示しています。 capture コマンドは、match キーワードを使用します。キャプチャするトラフィックを具体的に指定できます。

キャプチャ **capin** に対しては、TCP host 172.16.11.5 host 198.51.100.100 と一致する内部インターフェイス (入力または出力) 上のトラフィックを照合することを示しています。 つまり、host 172.16.11.5 から host 198.51.100.100 に送信されたか、この逆の TCP トラフィックをすべてキャプチャする必要があります。 match キーワードを使用すると、ファイアウォールでトラフィックを双方向でキャプチャできるようになります。 外部インターフェイスに定義された capture コマンドは、ファイアウォールがそのクライアントの IP アドレスに PAT を実行するため、内部クライアントの IP アドレスを参照しません。 したがって、そのクライアントの IP アドレスと照合できません。 代わりに、この例では、可能性のあるすべての IP アドレスがその基準と一致することを示すために any を使用します。

キャプチャを設定したら、次に接続の確立を再試行してから、**show capture *<capture_name>*** コマンドによるキャプチャの表示に進みます。 この例では、キャプチャにある TCP の 3 ウェイ ハンドシェイクによって明らかなようにクライアントがサーバに接続できたことを確認できます。

トラブルシューティング

現在のところ、この設定に関する特定のトラブルシューティング情報はありません。

関連情報

- ASA Syslog 設定例
- CLI および ASDM を使用したパケットのキャプチャの設定例
- テクニカル サポートとドキュメント – Cisco Systems