

# 目次

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定](#)

[ネットワーク図](#)

[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](#)

[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](#)

[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](#)

[スタティックアイデンティティ NAT](#)

[スタティックのポートリダイレクション \( フォワーディング \)](#)

[確認](#)

[接続](#)

[Syslog](#)

[パケットトレーサー](#)

[キャプチャ](#)

[トラブルシューティング](#)

[関連情報](#)

## 概要

この資料に CLI または適応性がある Security Device Manager ( ASDM ) の使用でポートリダイレクション ( フォワーディング ) および適応性があるセキュリティ アプライアンス モデル ( ASA ) ソフトウェア バージョン 9.x の外部 ネットワークアドレス 変換 ( NAT ) 機能を、設定する方法を説明されています。

その他の情報に関しては [Cisco ASA シリーズ ファイアウォール ASDM コンフィギュレーション ガイド](#)を参照して下さい。

## 前提条件

### 要件

[管理アクセスの](#)デバイスが ASDM によって設定されるように[設定](#)を参照して下さい。

### 使用するコンポーネント

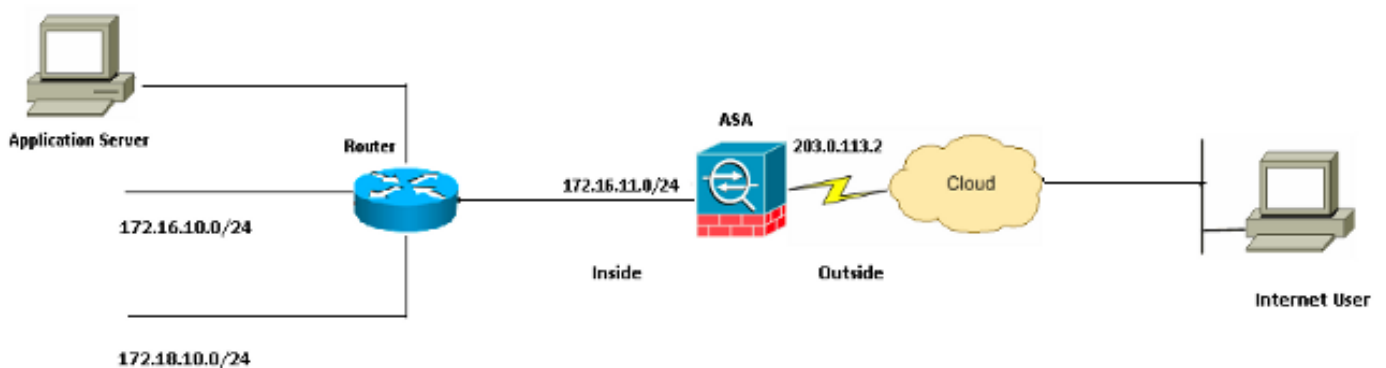
このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Cisco ASA 5525 シリーズ セキュリティ アプライアンス モデル ソフトウェア バージョン 9.x およびそれ以降
- ASDM バージョン 7.x および それ 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。

## 設定

### ネットワーク図



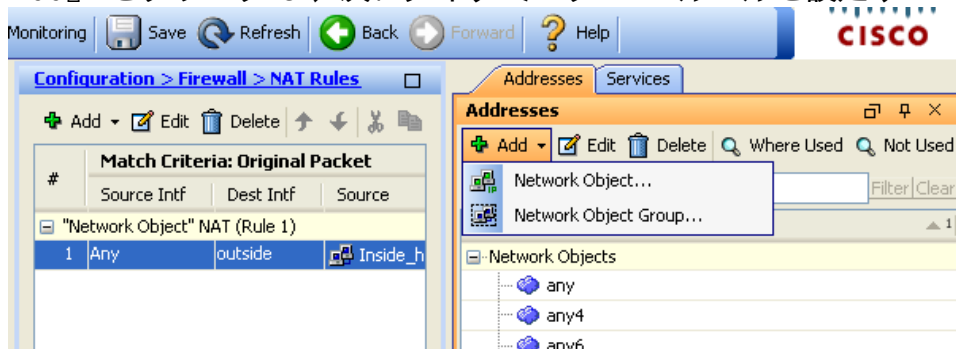
この設定で使用している IP アドレス スキームは、インターネット上で正式にルーティング可能なものではありません。これらはラボ環境で使用された RFC 1918 でのアドレスです。

### 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

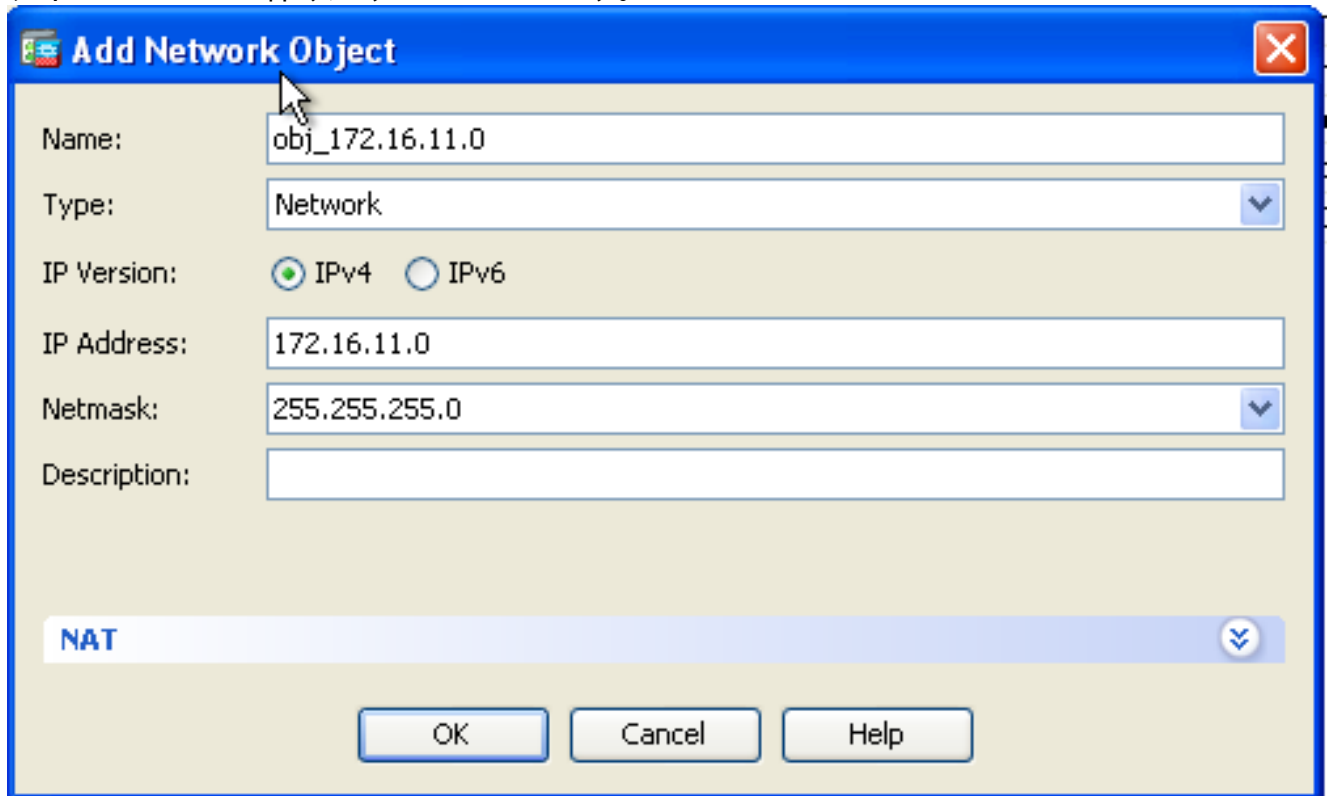
内部ホストに変換のための単一パブリックアドレスを共有してほしい場合ポートアドレス変換（PAT）を使用して下さい。最も簡単な PAT コンフィギュレーションの 1 つは outside インターフェイス IP アドレスのように見えるためにすべての内部ホストの変換を含みます。ISP から少数だけに利用可能なルーティング可能な IP アドレスの数が制限される、または多分ちょうど 1 使用されるときこれは典型的な PAT 設定です。

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。ネットワークオブジェクトを『Add』をクリックし、次にダイナミック NAT ルールを設定するために選択して下さい。



2. **ダイナミック PAT** が必要となるホスト/範囲を/ネットワーク設定して下さい。この例では、内部サブネットの1つは選択されました。このプロセスはこのように変換したい他のサブネットのために繰り返すことができます。



**Add Network Object**

Name: obj\_172.16.11.0

Type: Network

IP Version:  IPv4  IPv6

IP Address: 172.16.11.0

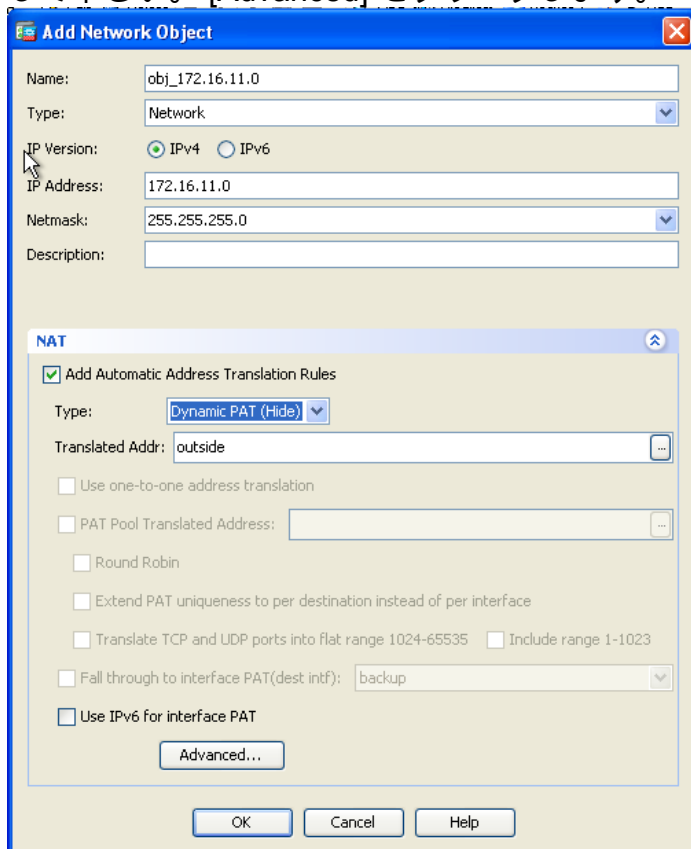
Netmask: 255.255.255.0

Description:

**NAT**

OK Cancel Help

3. NAT を拡張して下さい。追加自動アドレス変換規則チェックボックスをチェックして下さい。型ドロップダウンリストで、**ダイナミック PAT (非表示)** を選択して下さい。変換されたアドレス・フィールドで、outside インターフェイスを反映するオプションを選択して下さい。[Advanced] をクリックします。



**Add Network Object**

Name: obj\_172.16.11.0

Type: Network

IP Version:  IPv4  IPv6

IP Address: 172.16.11.0

Netmask: 255.255.255.0

Description:

**NAT**

Add Automatic Address Translation Rules

Type: Dynamic PAT (Hide)

Translated Addr: outside

Use one-to-one address translation

PAT Pool Translated Address:

Round Robin

Extend PAT uniqueness to per destination instead of per interface

Translate TCP and UDP ports into flat range 1024-65535  Include range 1-1023

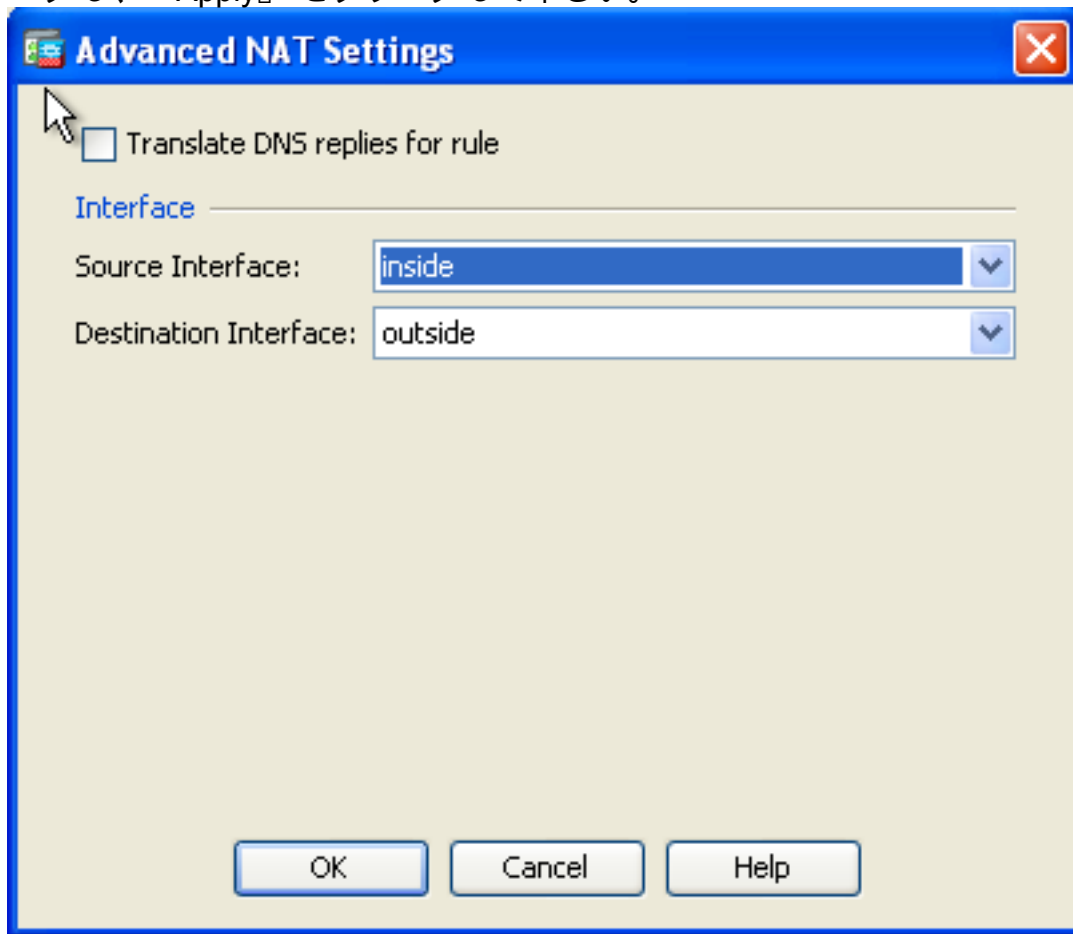
Fall through to interface PAT(dest intf): backup

Use IPv6 for interface PAT

Advanced...

OK Cancel Help

4. ソースインターフェイスおよびデスティネーションインターフェイス 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て下さい。変更を有効にするために『OK』をクリックし、『Apply』 をクリックして下さい。



この PAT 設定に対応する CLI 出力を以下に示します。

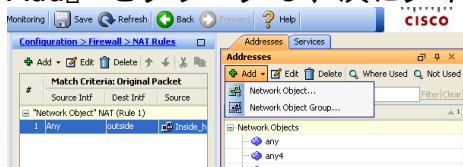
## NAT を使用した inside ホストから outside ネットワークへのアクセスの許可

内部ホスト/ネットワークのグループがダイナミック NAT ルールの設定の外界にアクセスするようになる可能性があります。PAT とは違って、ダイナミック NAT はアドレスのプールから変換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つのホストは同じ変換された IP アドレスを共有できません。

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。ネットワーク オブジェクトを『Add』 をクリックし、次にダイナミック NAT ルールを設定するために選択して下さい。



2. ダイナミック PAT が必要となるホスト/範囲を/ネットワーク設定して下さい。この例では *inside-network* 全体が選択されています。

**Add Network Object**

Name:

Type:

IP Version:  IPv4  IPv6

IP Address:

Netmask:

Description:

**NAT**

3. NAT を拡張して下さい。追加自動アドレス変換規則チェックボックスをチェックして下さい。型ドロップダウンリストで、ダイナミックを選択して下さい。変換されたアドレス・フィールドで、適切な選択を選択して下さい。[Advanced] をクリックします。

**Edit Network Object**

Name:

Type:

IP Version:  IPv4  IPv6

IP Address:

Netmask:

Description:

**NAT**

Add Automatic Address Translation Rules

Type:

Translated Addr:

Use one-to-one address translation

PAT Pool Translated Address:

Round Robin

Extend PAT uniqueness to per destination instead of per interface

Translate TCP and UDP ports into flat range 1024-65535  Include range 1-1023

Fall through to interface PAT(dest intf):

Use IPv6 for interface PAT

4. ネットワーク オブジェクトを追加するために『Add』をクリックして下さい。型ドロップダウンリストで、**範囲**を選択して下さい。開始アドレスおよび端 Address フィールドでは、開始し、終了 PAT IP アドレスを入力して下さい。[OK] をクリックします。

**Add Network Object**

Name: obj-my-range

Type: Range

IP Version:  IPv4  IPv6

Start Address: 203.0.113.10

End Address: 203.0.113.20

Description:

NAT

OK Cancel Help

5. 変換されたアドレス・フィールドで、アドレス オブジェクトを選択して下さい。送信元および宛先 インターフェイスを選択するために『Advanced』をクリックして下さい。

**Edit Network Object**

Name: obj\_172.16.11.0

Type: Network

IP Version:  IPv4  IPv6

IP Address: 172.16.11.0

Netmask: 255.255.255.0

Description:

**NAT**

Add Automatic Address Translation Rules

Type: Dynamic

Translated Addr: obj-my-range

Use one-to-one address translation

PAT Pool Translated Address:

Round Robin

Extend PAT uniqueness to per destination instead of per interface

Translate TCP and UDP ports into flat range 1024-65535  Include range 1-1023

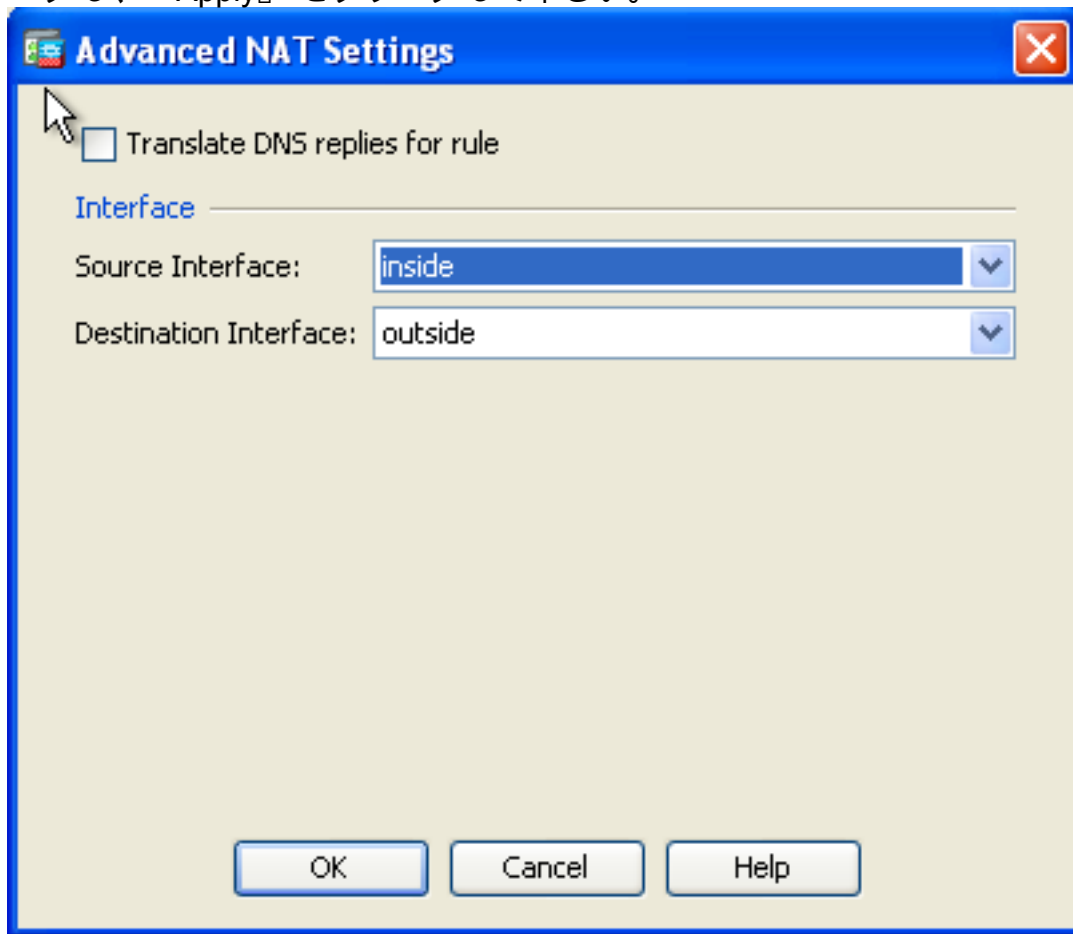
Fall through to interface PAT(dest intf): backup

Use IPv6 for interface PAT

Advanced...

OK Cancel Help

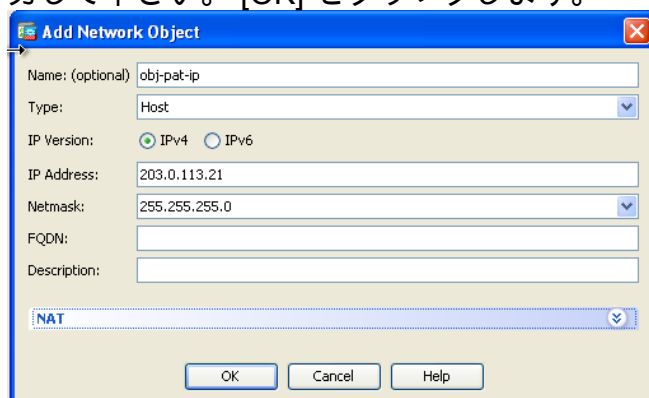
6. ソースインターフェイスおよびデスティネーションインターフェイス ドロップダウン リストで、適切なインターフェイスを選択して下さい。変更を有効にするために『OK』をクリックし、『Apply』 をクリックして下さい。



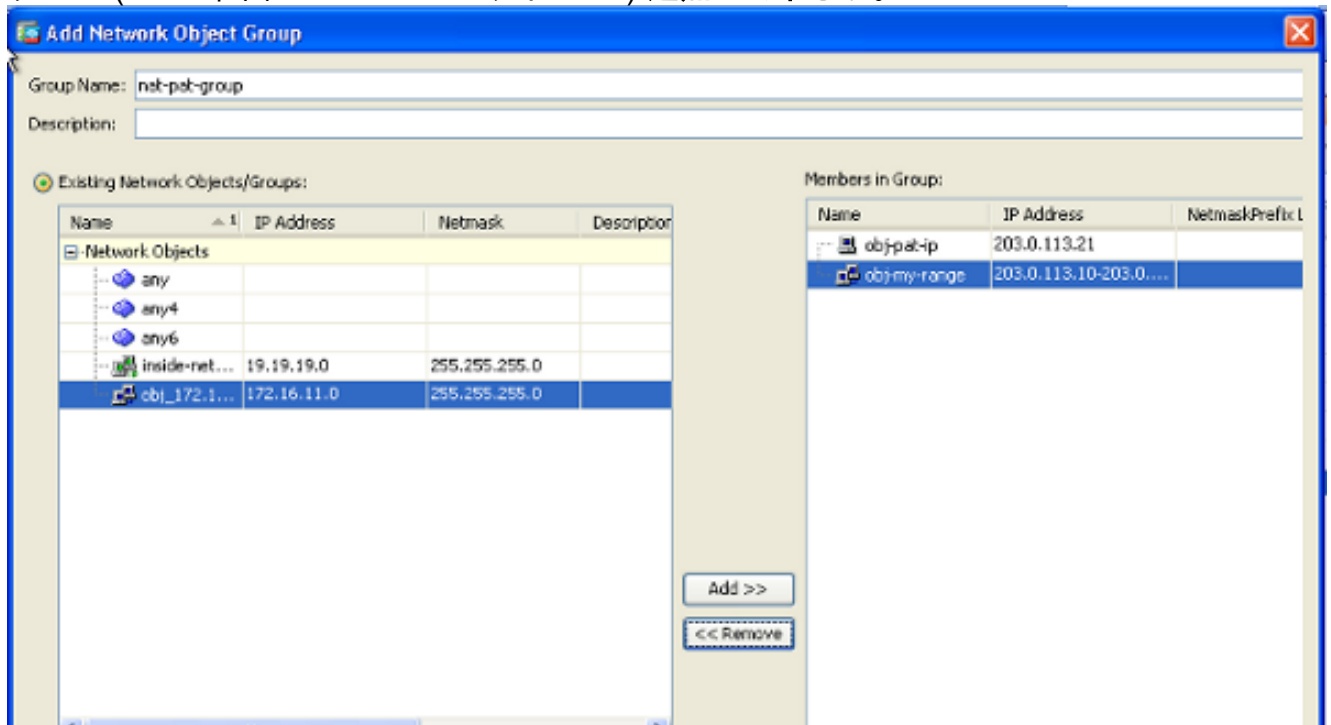
この ASDM 設定に対応する CLI 出力を以下に示します。

この設定によって、172.16.11.0 ネットワークのホストは NATプールからのあらゆる IP アドレスに、203.0.113.10 - 203.0.113.20 変換されます。マッピングされたプールに実質グループより少数のアドレスがある場合、アドレスを使い果たす可能性があります。その結果、ダイナミック PAT バックアップのダイナミック NAT を設定することを試みる可能性がありますまたは既存のプールを拡張することを試みる可能性があります。

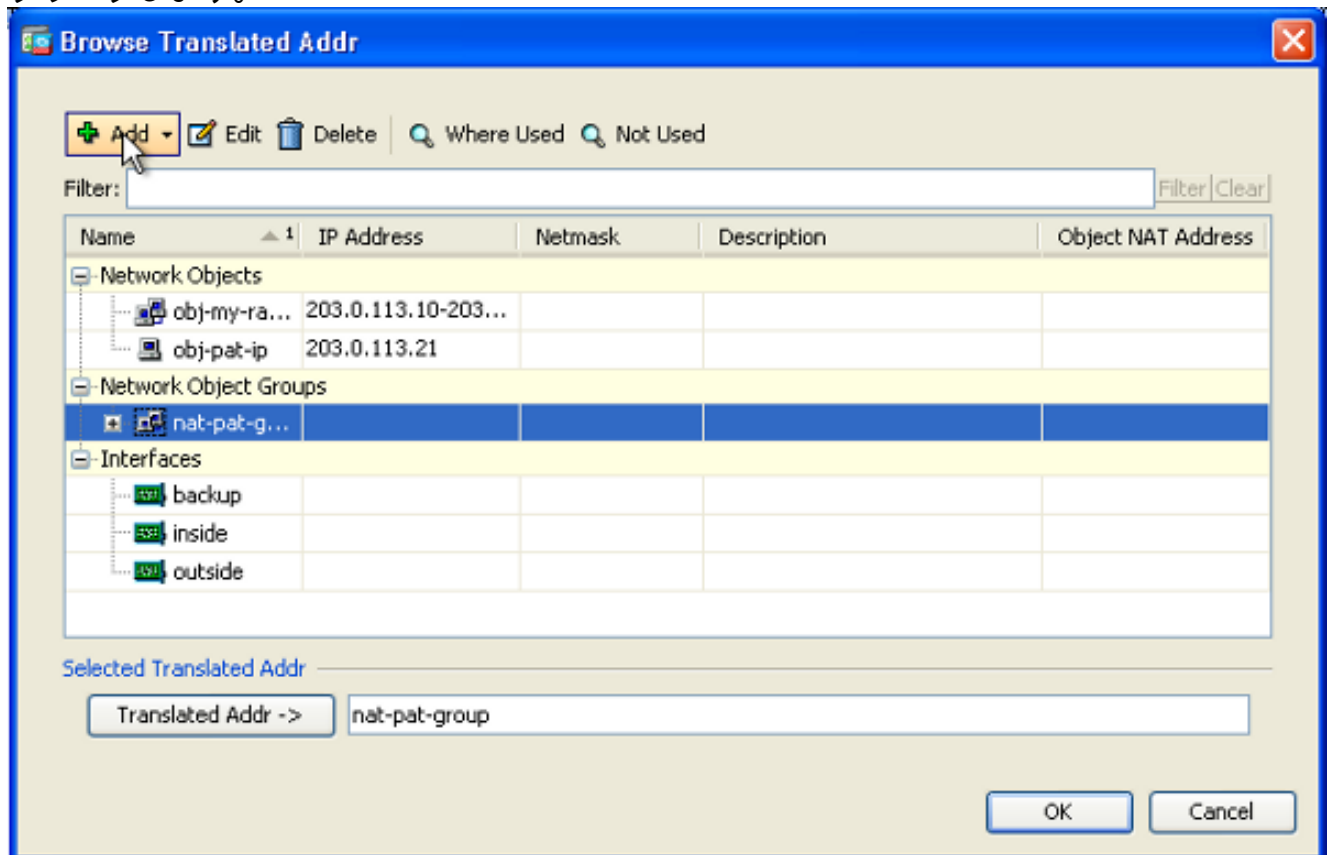
1. 以前のコンフィギュレーションのステップ 1 に 3 を繰り返し、ネットワーク オブジェクトを追加するためにもう一度『Add』 をクリックして下さい。型ドロップダウン リストで、**ホスト**を選択して下さい。IP Address フィールドでは、PAT バックアップ IP アドレスを入力して下さい。[OK] をクリックします。



2. ネットワーク オブジェクト グループを追加するために『Add』 をクリックして下さい。Group Name フィールドでは、グループ名を入力し、グループの両方のアドレス オブジェクトを ( NAT 範囲および PAT IP アドレス ) 追加して下さい。



3. 設定された NAT ルールを選択し、最近設定されたグループ「NAT 軽打グループ」であるために変換されたアドレスを変更して下さい ( 「obj 私範囲」は以前にありました )。[OK] をクリックします。



4. NAT ルールを追加するために『OK』 をクリックして下さい。送信元および宛先 インター



フェイスを選択するために『Advanced』 をクリックして下さい。

**Edit Network Object**

Name: obj\_172.16.11.0

Type: Network

IP Version:  IPv4  IPv6

IP Address: 172.16.11.0

Netmask: 255.255.255.0

Description:

**NAT**

Add Automatic Address Translation Rules

Type: Dynamic

Translated Addr: nat-pat-group

Use one-to-one address translation

PAT Pool Translated Address:

Round Robin

Extend PAT uniqueness to per destination instead of per interface

Translate TCP and UDP ports into flat range 1024-65535  Include range 1-1023

Fall through to interface PAT(dest intf): backup

Use IPv6 for interface PAT

Advanced...

OK Cancel Help

5. ソースインターフェイスおよびデスティネーションインターフェイス 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て下さい。[OK] をクリックします。

**Advanced NAT Settings**

Translate DNS replies for rule

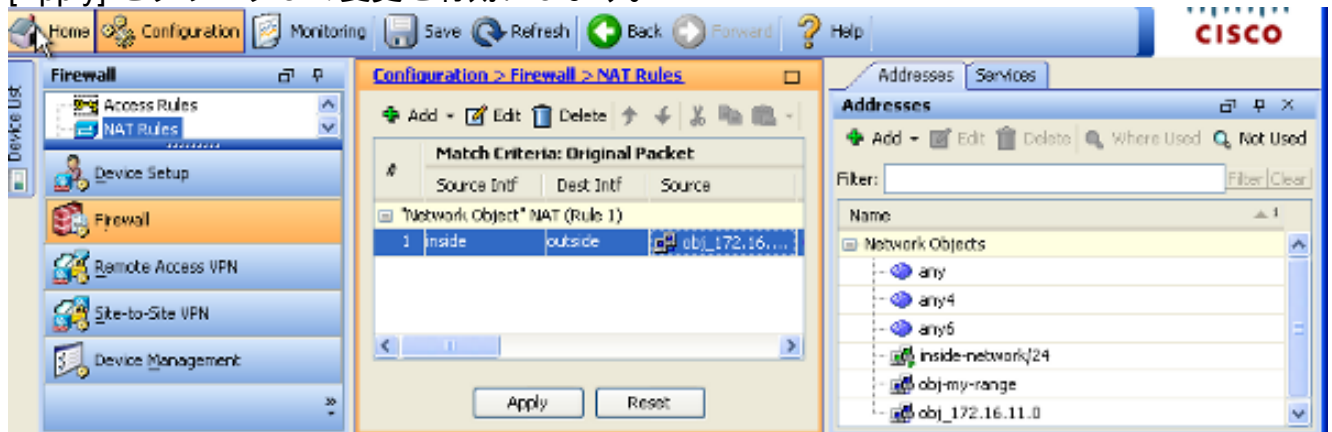
Interface

Source Interface: inside

Destination Interface: outside

OK Cancel Help

6. [Apply] をクリックして変更を有効にします。

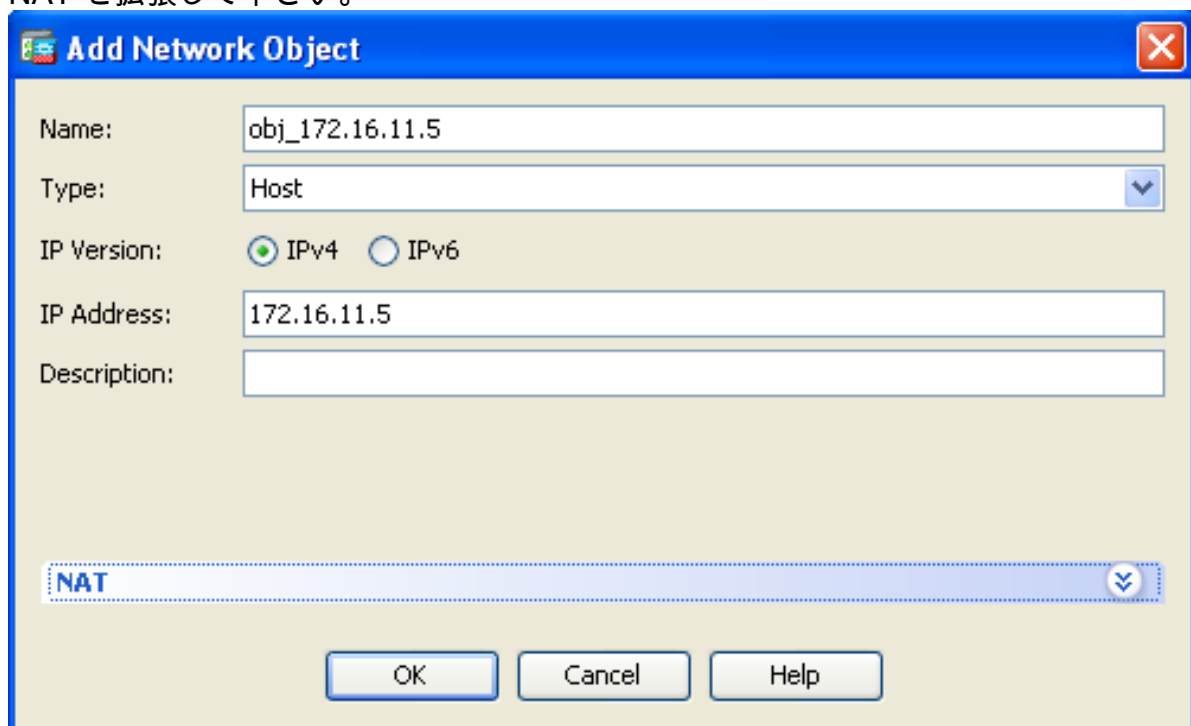


この ASDM 設定に対応する CLI 出力を以下に示します。

## 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

これを割り当てへの静的NAT交換およびアクセス規則のアプリケーションによってそれらのホスト達成することができます。内部ネットワークに坐らせる外部ユーザがサーバにアクセスすることを望む時はいつでもこれを設定するために必要となります。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。この作業を作るために、パブリックIPアドレスにこの私用サーバのIPアドレスを変換する必要があります。この例に 203.0.113.5 に 172.16.11.5 を変換するために双方向スタティック NAT を設定する方法を記述されています。

1. [Configuration] > [Firewall] > [NAT Rules] を選択します。ネットワークオブジェクトを『Add』をクリックし、次にスタティック NAT ルールを設定するために選択して下さい。NAT を拡張して下さい。



2. 追加自動アドレス変換規則 チェックボックスをチェックして下さい。型ドロップダウンリストで、**スタティック**を選択して下さい。変換されたアドレス・フィールドでは、IP アドレスを入力して下さい。送信元および宛先 インターフェイスを選択するために『Advanced』をクリックして下さい。

**Add Network Object**

Name: obj\_172.16.11.5

Type: Host

IP Version:  IPv4  IPv6

IP Address: 172.16.11.5

Description:

**NAT**

Add Automatic Address Translation Rules

Type: Static

Translated Addr: 203.0.113.5

Use one-to-one address translation

PAT Pool Translated Address:

Round Robin

Extend PAT uniqueness to per destination instead of per interface

Translate TCP and UDP ports into flat range 1024-65535  Include range 1-1023

Fall through to interface PAT(dest intf): backup

Use IPv6 for interface PAT

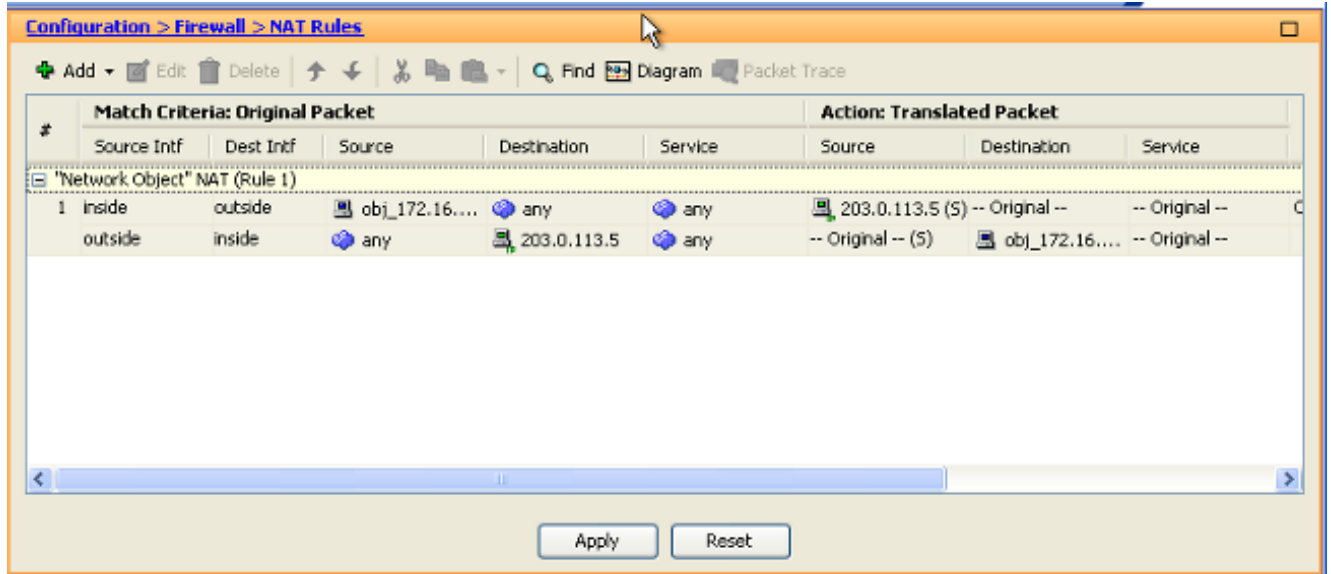
Advanced...

OK Cancel Help

3. ソースインターフェイスおよびデスティネーションインターフェイス 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て下さい。[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。



これはこの NAT 設定のために出力される同等の CLI です:

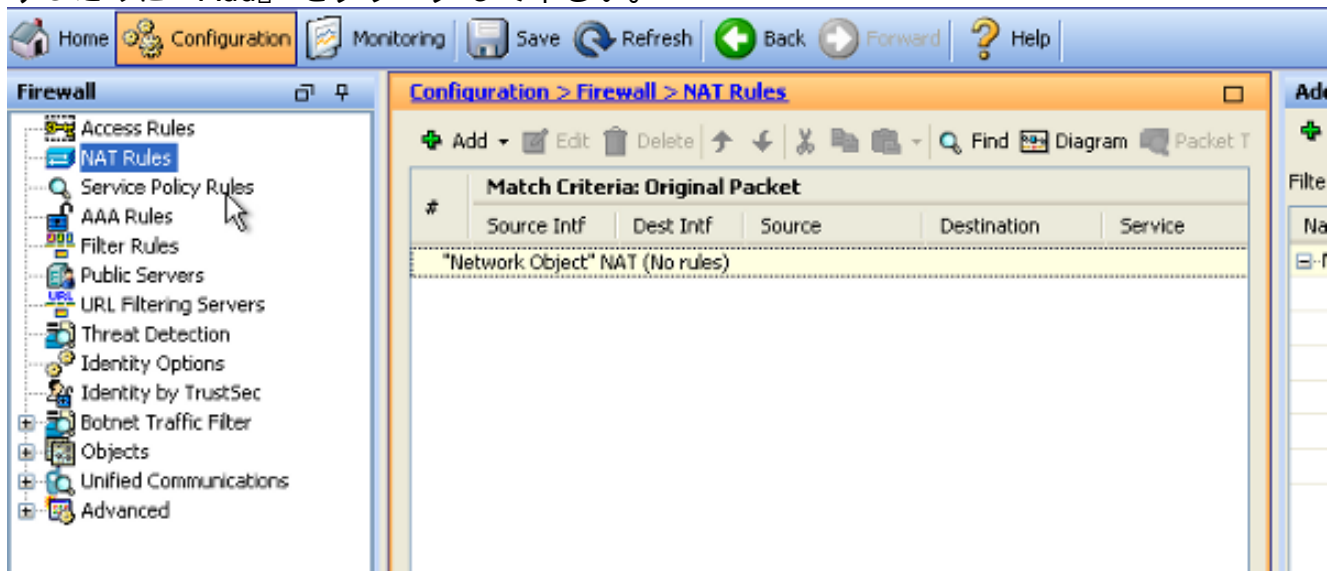
## スタティック アイデンティティ NAT

免除されている NAT は内部ユーザがリモート VPN ホスト/サーバが NAT の完了なしで ASA の他のどのインターフェイスの後ろでもホストされるホスト/サーバにアクセスを試みる有用な機能です。これを、プライベート IP アドレスがあるそれから NAT を行う宛先にアクセスすることができ、内部サーバは実現させるためにそれ自身に変換された識別です。

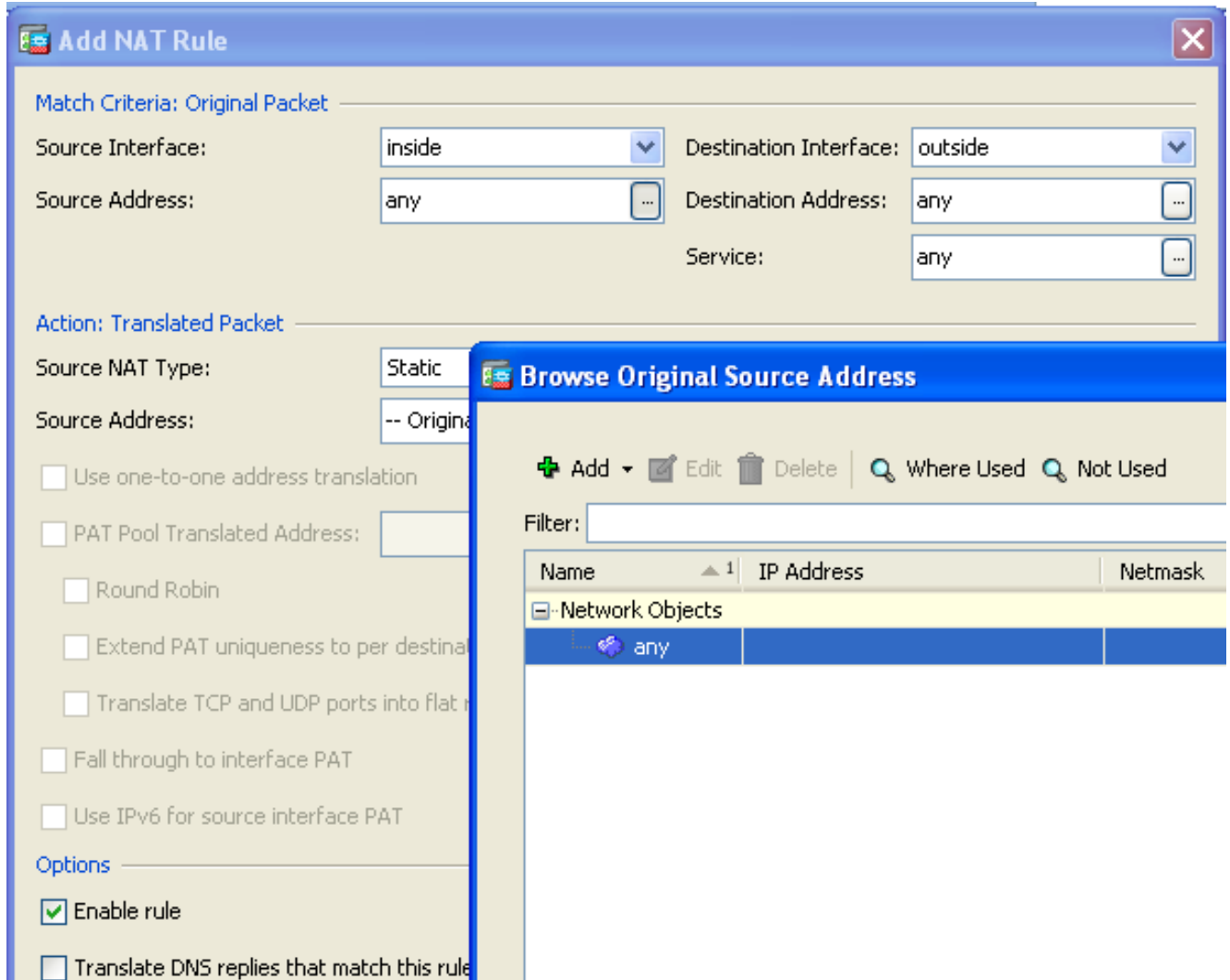
この例では、内部ホスト 172.16.11.15 はリモート VPN サーバ 172.20.21.15 にアクセスする必要があります。

NAT の完了を用いるリモート VPN ネットワークに内部ホスト アクセスを許可するためにこれらのステップを完了して下さい:

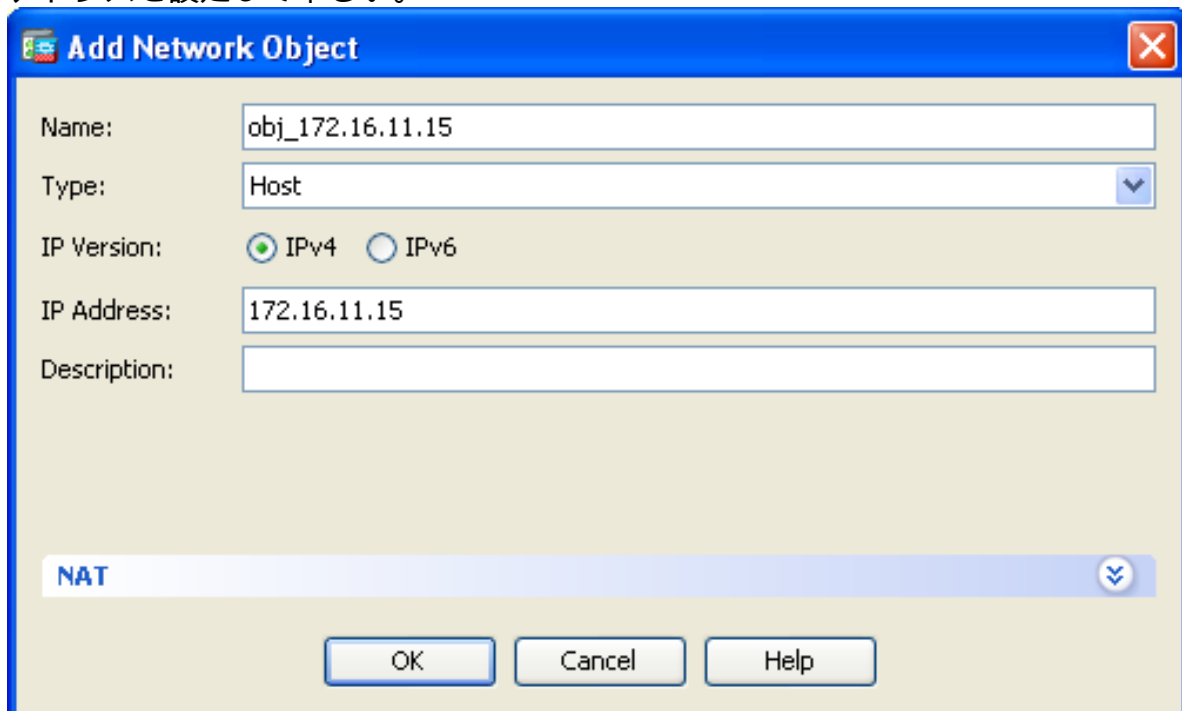
1. [Configuration] > [Firewall] > [NAT Rules] を選択します。 NAT 免除されているルールを設定するために『Add』 をクリックして下さい。



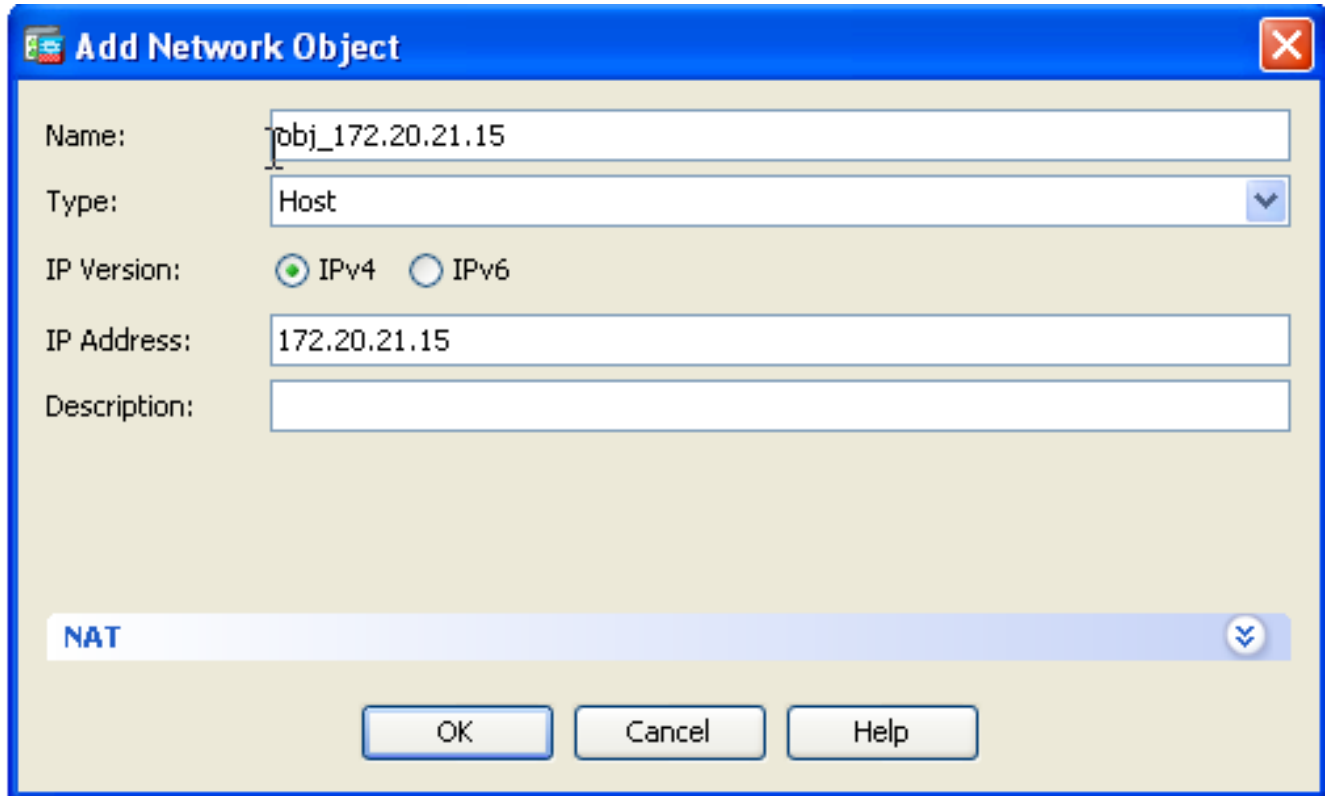
2. ソースインターフェイスおよびデスティネーションインターフェイス ドロップダウン リストで、適切なインターフェイスを選択して下さい。送信元アドレス フィールドで、適切なエントリを選択して下さい。



3. ネットワーク オブジェクトを追加するために『Add』 をクリックして下さい。ホスト IP アドレスを設定して下さい。



4. 同様に、宛先アドレスを参照して下さい。ネットワーク オブジェクトを追加するために『Add』をクリックして下さい。ホスト IP アドレスを設定して下さい。



**Add Network Object**

Name: obj\_172.20.21.15

Type: Host

IP Version:  IPv4  IPv6

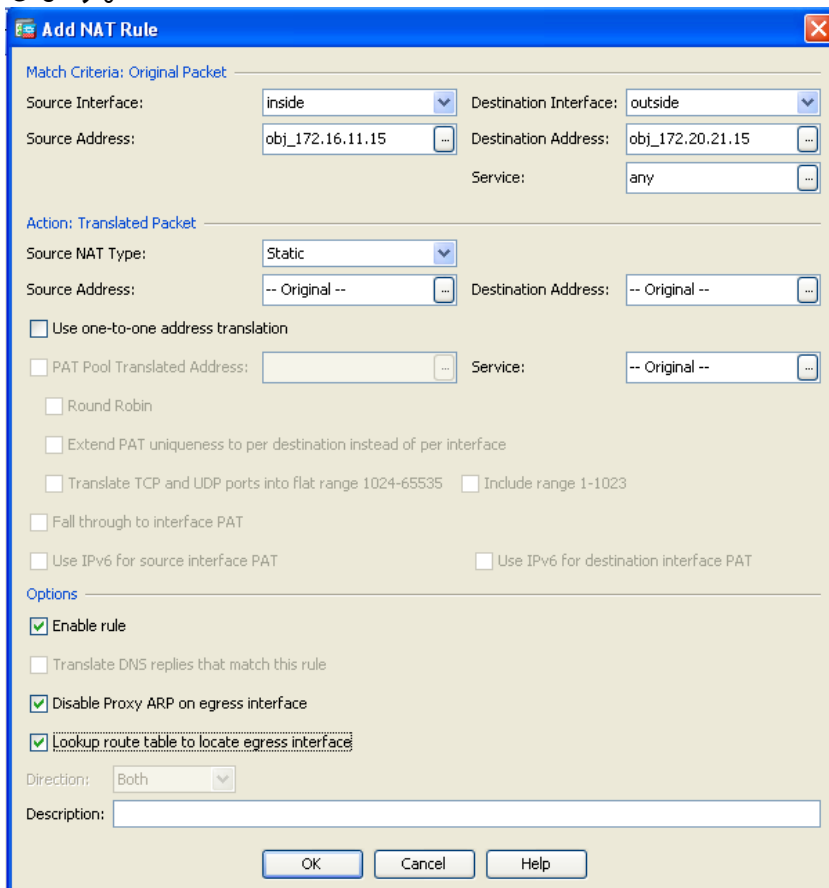
IP Address: 172.20.21.15

Description:

NAT

OK Cancel Help

5. 設定された送信元アドレスおよび宛先アドレス オブジェクトを選択して下さい。出力 インターフェイス チェックボックスを取付けるために出力 インターフェイスおよびルックアップ ルートテーブルのディセーブル プロキシARP をチェックして下さい。[OK] をクリック します。



**Add NAT Rule**

Match Criteria: Original Packet

Source Interface: inside Destination Interface: outside

Source Address: obj\_172.16.11.15 Destination Address: obj\_172.20.21.15

Service: any

Action: Translated Packet

Source NAT Type: Static

Source Address: -- Original -- Destination Address: -- Original --

Use one-to-one address translation

PAT Pool Translated Address: Service: -- Original --

Round Robin

Extend PAT uniqueness to per destination instead of per interface

Translate TCP and UDP ports into flat range 1024-65535  Include range 1-1023

Fall through to interface PAT

Use IPv6 for source interface PAT  Use IPv6 for destination interface PAT

Options

Enable rule

Translate DNS replies that match this rule

Disable Proxy ARP on egress interface

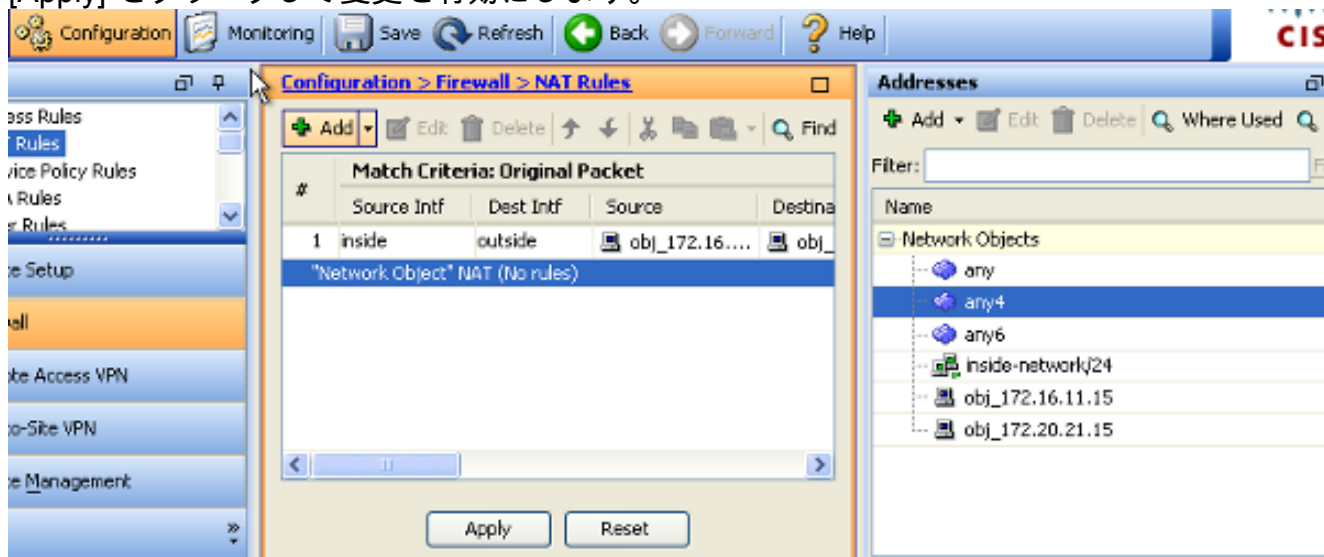
Lookup route table to locate egress interface

Direction: Both

Description:

OK Cancel Help

6. [Apply] をクリックして変更を有効にします。



これは NAT のために出力される同等の CLI 免除されているまたはアイデンティティ NAT 設定です:

## スタティックのポートリダイレクション (フォワーディング)

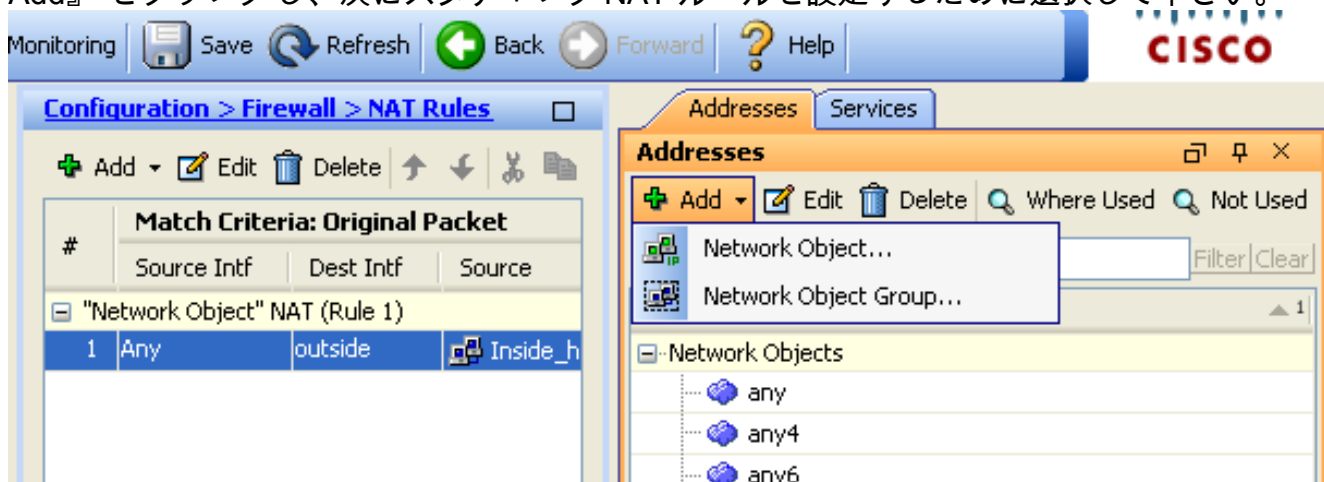
ポート フォワーディング (ポート リダイレクション) は、外部ユーザが特定ポートから内部サーバにアクセスする場合に便利な機能です。このためには、内部サーバに設定されているプライベート IP アドレスをパブリック IP アドレスに変換し、特定のポートでのアクセスを許可します。

この例では、外部ユーザはポート 25 で SMTP サーバに、203.0.115.15 アクセスしたいと思います。このためには次の 2 つの手順を実行します。

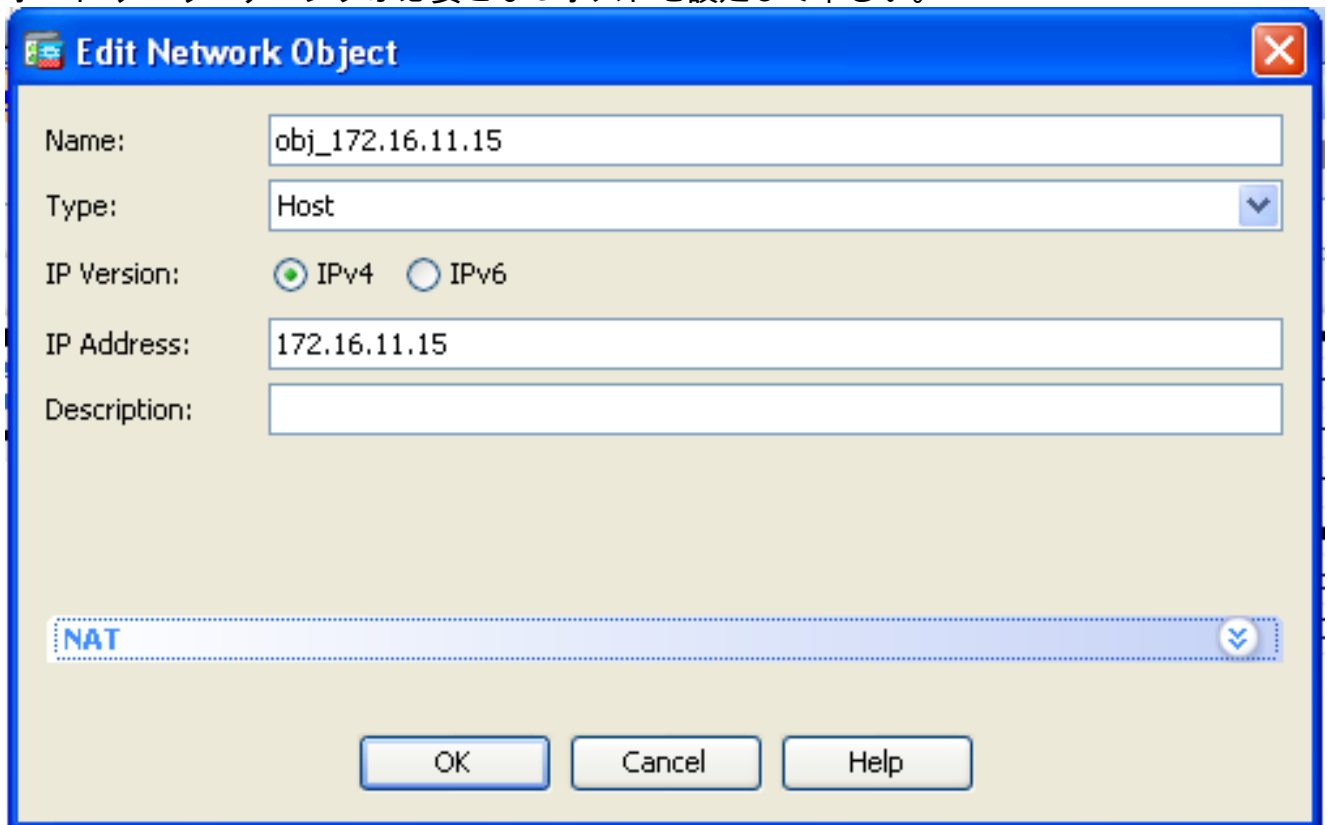
1. ポート 25 で、パブリック IP アドレスに、内部メールサーバを、ポート 25 の 172.16.11.15 203.0.115.15 変換して下さい。
2. ポート 25 で公共メールサーバにアクセスを、203.0.115.15 許可して下さい。

外部ユーザがサーバにアクセスを試みるときポート 25 の 203.0.115.15 は内部メールサーバに、このトラフィック、ポート 25 の 172.16.11.15 リダイレクトされます。

1. [Configuration] > [Firewall] > [NAT Rules] を選択します。ネットワーク オブジェクトを『Add』をクリックし、次にスタティック NAT ルールを設定するために選択して下さい。



2. ポート フォワーディングが必要となるホストを設定して下さい。



**Edit Network Object**

Name: obj\_172.16.11.15

Type: Host

IP Version:  IPv4  IPv6

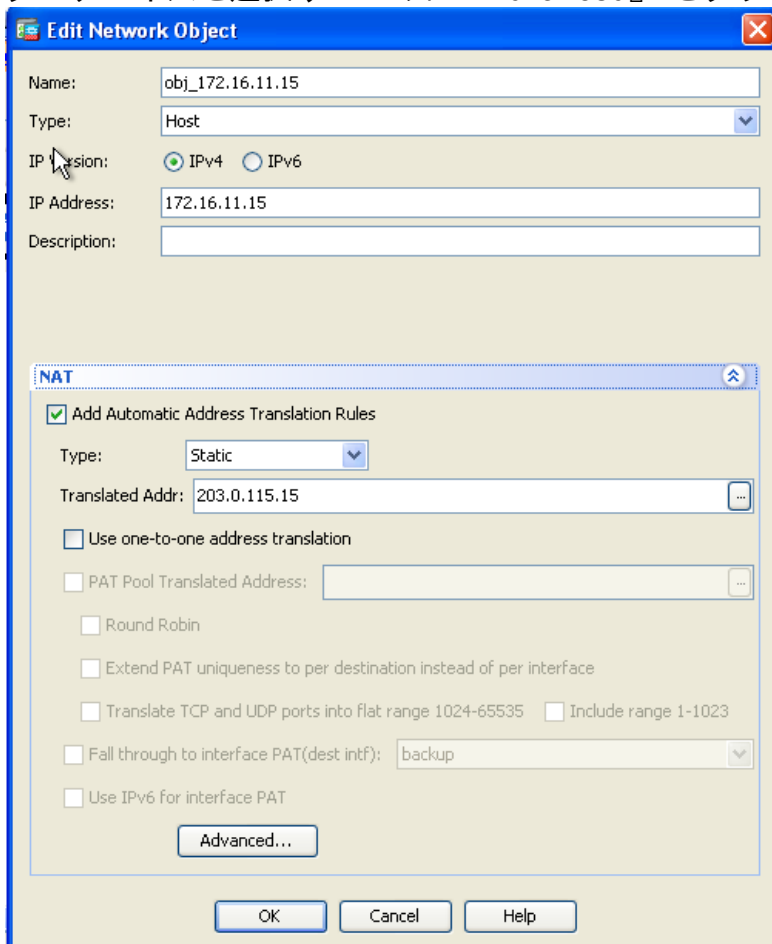
IP Address: 172.16.11.15

Description:

NAT

OK Cancel Help

3. NAT を拡張して下さい。追加自動アドレス変換規則 チェックボックスをチェックして下さい。型ドロップダウンリストで、スタティックを選択して下さい。変換されたアドレス・フィールドでは、IP アドレスを入力して下さい。サービスおよび送信元および宛先 インターフェイスを選択するために『Advanced』 をクリックして下さい。



**Edit Network Object**

Name: obj\_172.16.11.15

Type: Host

IP Version:  IPv4  IPv6

IP Address: 172.16.11.15

Description:

NAT

Add Automatic Address Translation Rules

Type: Static

Translated Addr: 203.0.115.15

Use one-to-one address translation

PAT Pool Translated Address:

Round Robin

Extend PAT uniqueness to per destination instead of per interface

Translate TCP and UDP ports into flat range 1024-65535  Include range 1-1023

Fall through to interface PAT(dest intf): backup

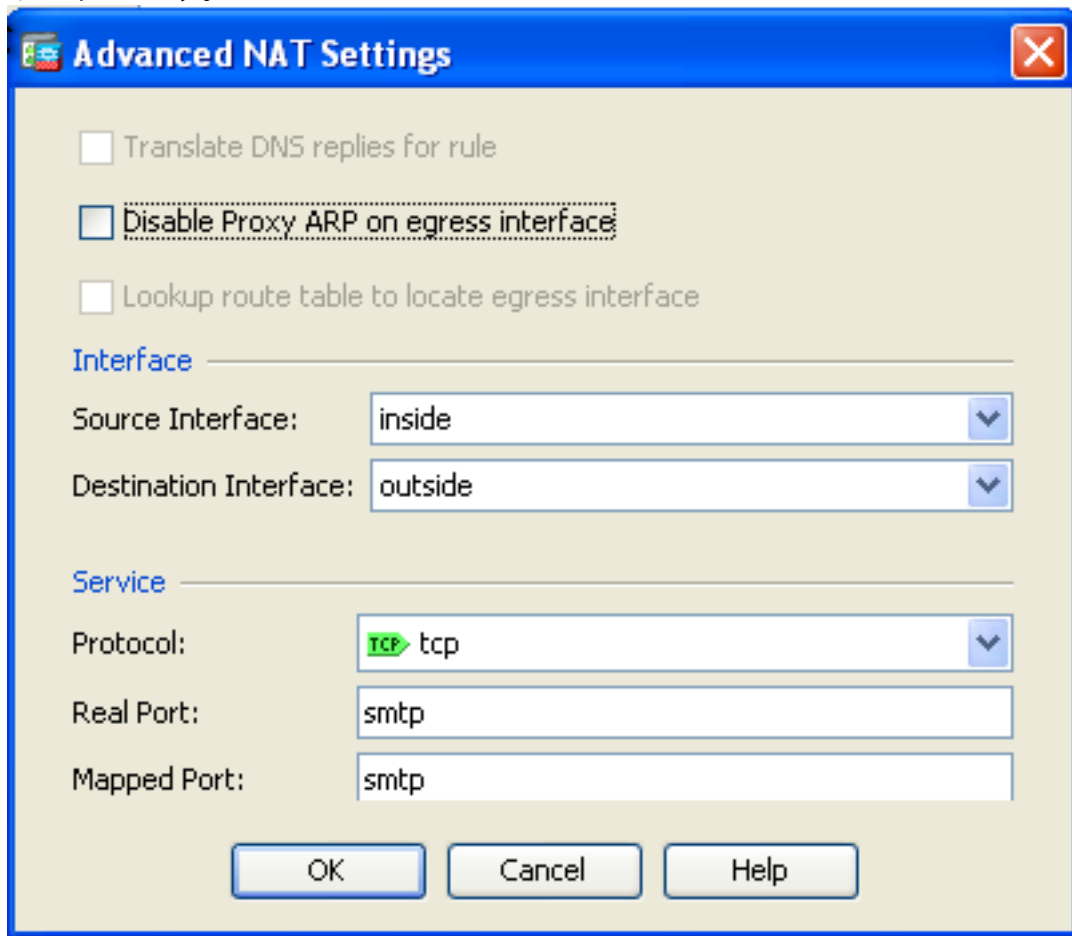
Use IPv6 for interface PAT

Advanced...

OK Cancel Help



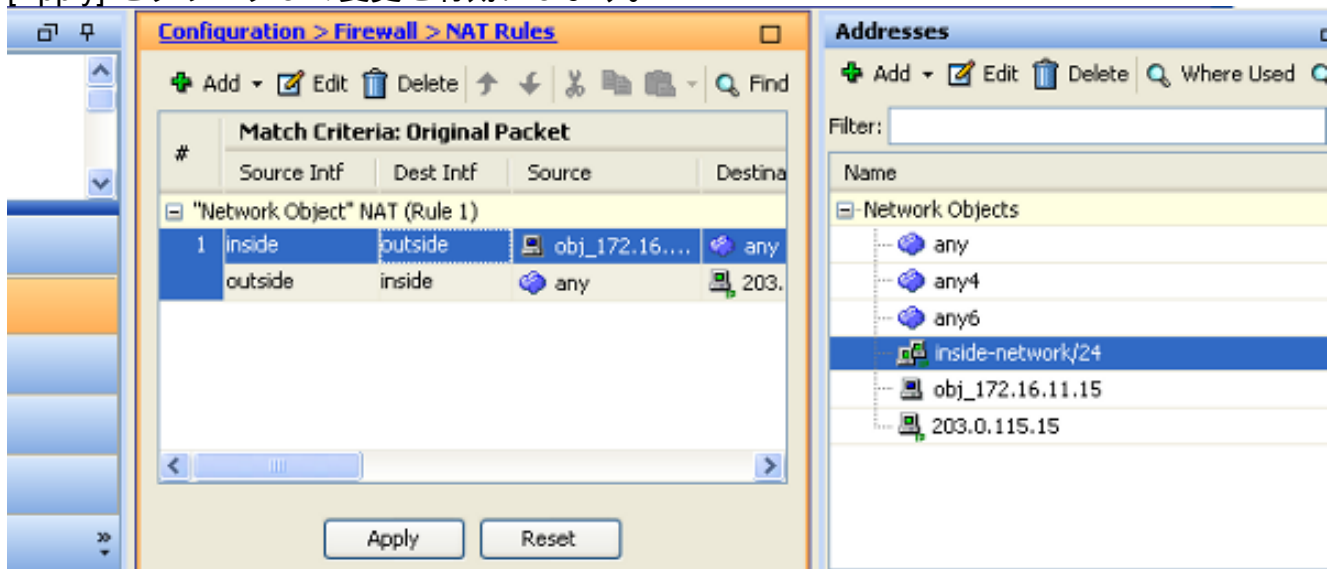
4. ソースインターフェイスおよびデスティネーションインターフェイス ドロップダウン リストで、適切なインターフェイスを選択して下さい。サービスを設定して下さい。[OK] をクリックします。



The image shows the 'Advanced NAT Settings' dialog box. It has a blue title bar with a close button. The main area is light beige and contains several sections:

- Options:** Three unchecked checkboxes: 'Translate DNS replies for rule', 'Disable Proxy ARP on egress interface', and 'Lookup route table to locate egress interface'.
- Interface:** A section with two dropdown menus: 'Source Interface' set to 'inside' and 'Destination Interface' set to 'outside'.
- Service:** A section with three input fields: 'Protocol' set to 'tcp', 'Real Port' set to 'smtp', and 'Mapped Port' set to 'smtp'.
- Buttons:** Three buttons at the bottom: 'OK', 'Cancel', and 'Help'.

5. [Apply] をクリックして変更を有効にします。



The image shows a network configuration interface with two main windows:

- Configuration > Firewall > NAT Rules:** A table showing NAT rules. The table has columns for '#', 'Source Intf', 'Dest Intf', 'Source', and 'Destina'. There are two rows for rule 1: one for traffic from 'inside' to 'outside' and another for traffic from 'outside' to 'inside'. The source and destination are set to network objects.
- Addresses:** A list of network objects. The object 'inside-network/24' is selected and highlighted in blue.

これはこの NAT 設定のために出力される同等の CLI です:

## 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。

特定の show コマンドが[アウトプット インタープリタ ツール \( 登録ユーザ専用 \)](#) でサポートされています。 show コマンド出力の分析を表示するには、アウトプット インタープリタ ツールを使用します。

Webブラウザの HTTP によって Webサイトにアクセスして下さい。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。接続が正常である場合、この出力は ASA CLI で見られる場合があります。

## 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。出力はレベル 6 で見られる、または「情報」レベルを示したものです 2 syslog。

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な TCP の変換 ( 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。

## パケットトレーサー

```
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は内部に到達します。
- 使用されているプロトコルが TCP である。
- 模倣されたクライアントIPアドレスは 172.16.11.5 です。
- 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 のサーバに向かいます。
- トラフィックはポート 80 宛てです。

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

### キャプチャを加えて下さい

```
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 198.51.100.100ASA#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 32768ASA#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 に関しては、( 入力か出力 ) その内部インターフェイスで見られて一致する TCP ホスト 172.16.11.5 ホスト 198.51.100.100 とトラフィックを一致するたいと思ったことを示しました。すなわち、198.51.100.100 をホストするためにホスト 172.16.11.5 からまたは逆に送信される TCP トラフィックをキャプチャしたいと思います。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後、それから接続を再度確立するように試み提示キャプチャ `<capture_name>` コマンドでキャプチャを表示することを続行します。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 設定例の ASA パケットキャプチャ](#)
- [テクニカルサポートとドキュメント - Cisco Systems](#)