

# NATを使用したASAバージョン9ポートフォワードイングの設定

## 内容

[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](#)

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

[確認](#)

[Connection](#)

[Syslog](#)

[パケットトレーサ](#)

[キャプチャ](#)

[トラブルシューティング](#)

[関連情報](#)

## 概要

このドキュメントでは、CLIまたはAdaptive Security Device Manager(ASDM)を使用して、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でポートリダイレクション (フォワーディング) と外部ネットワークアドレス変換(NAT)機能を設定する方法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

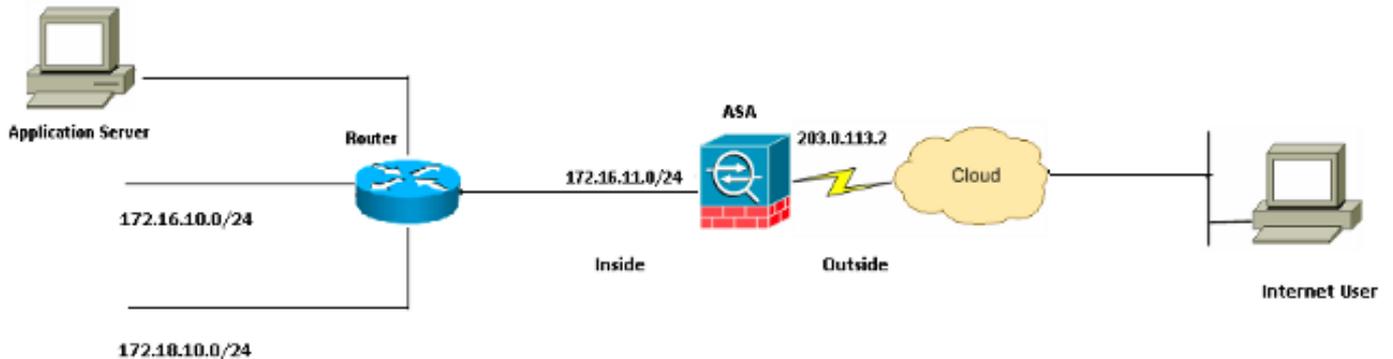
このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- 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

"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。ネットワークが稼働中の場合は、コマンド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"

## 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 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。

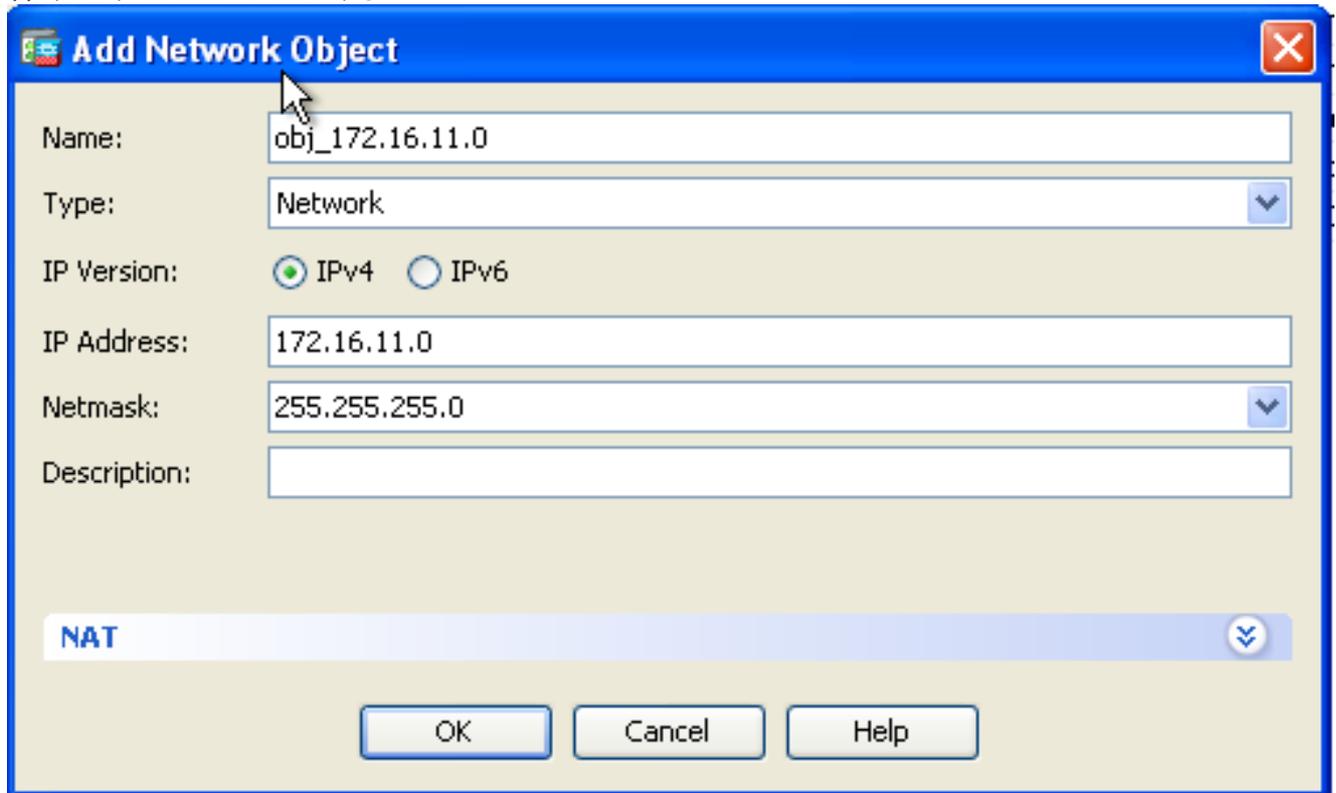
PAT を使用して inside ホストから outside ネットワークへのアクセスを許可するには、次の手順を実行します。

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。

The screenshot shows the Cisco ASDM interface. The main window displays the configuration for NAT Rules. The 'Match Criteria: Original Packet' table is visible, showing a rule with source 'Any' and destination 'outside'. The 'Addresses' window is also open, showing a list of network objects including 'any', 'any4', and 'any6'.

#	Source Intf	Dest Intf	Source
1	Any	outside	Inside_h

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。



**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。

**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

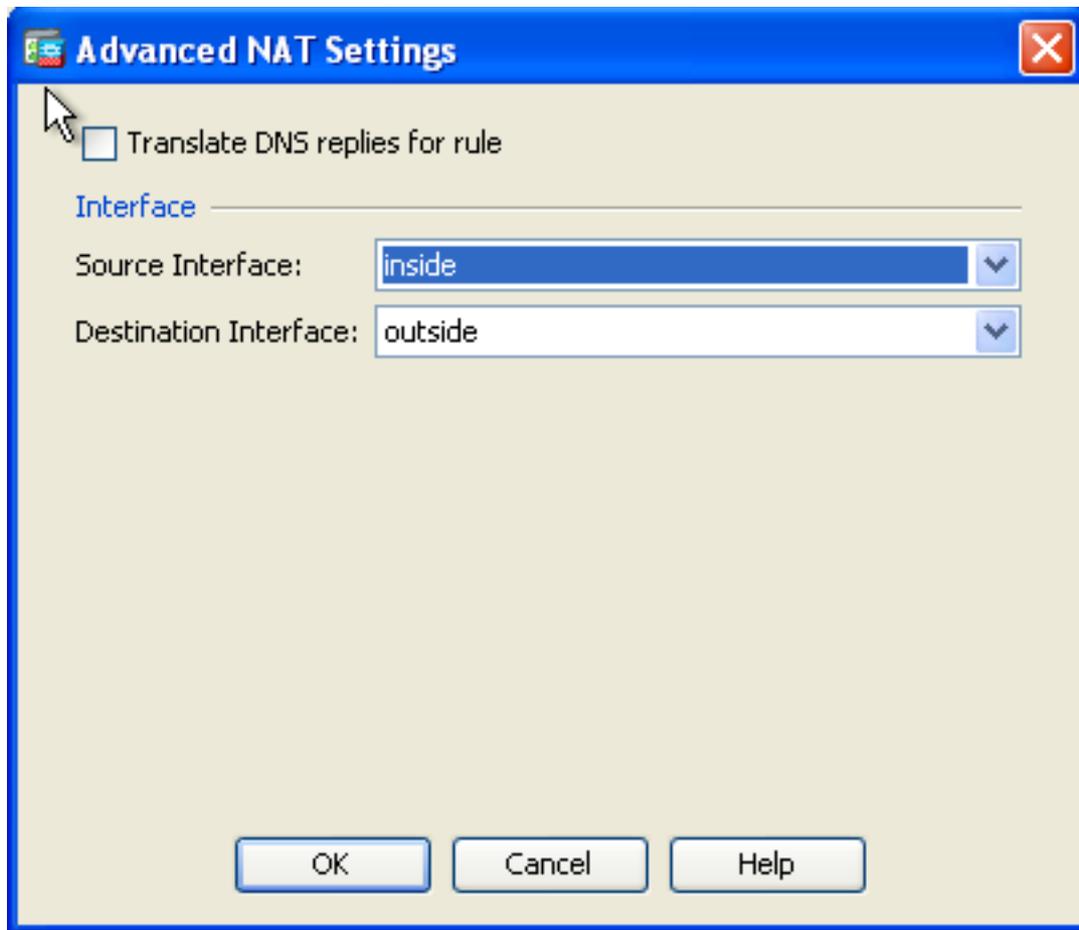
Fall through to interface PAT(dest intf): backup

Use IPv6 for interface PAT

Advanced...

OK Cancel Help

4. [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
```

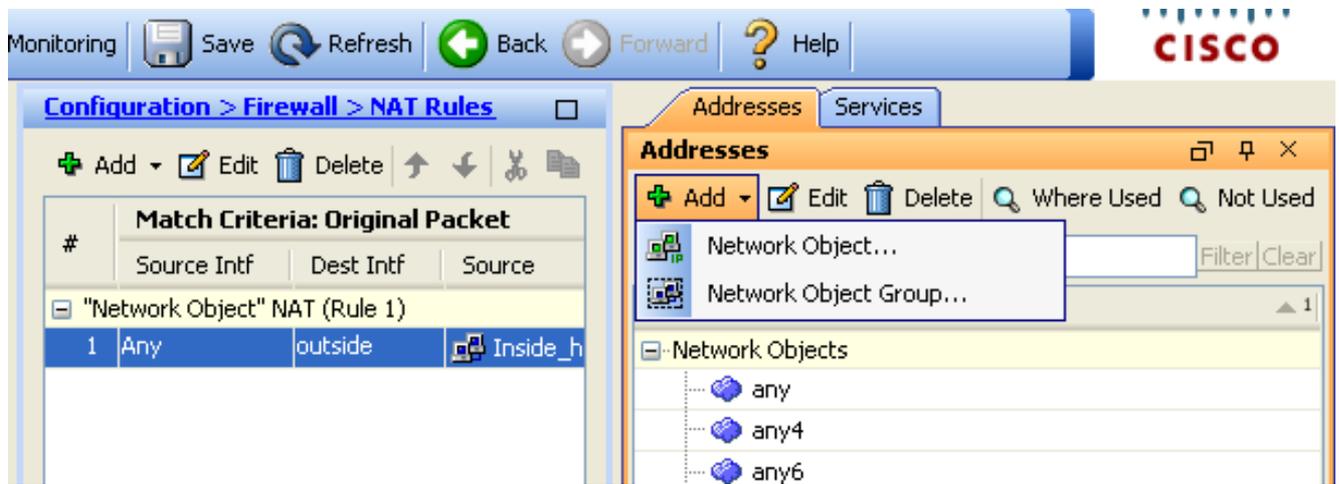
## NAT を使用した inside ホストから outside ネットワークへのアクセスの許可

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。

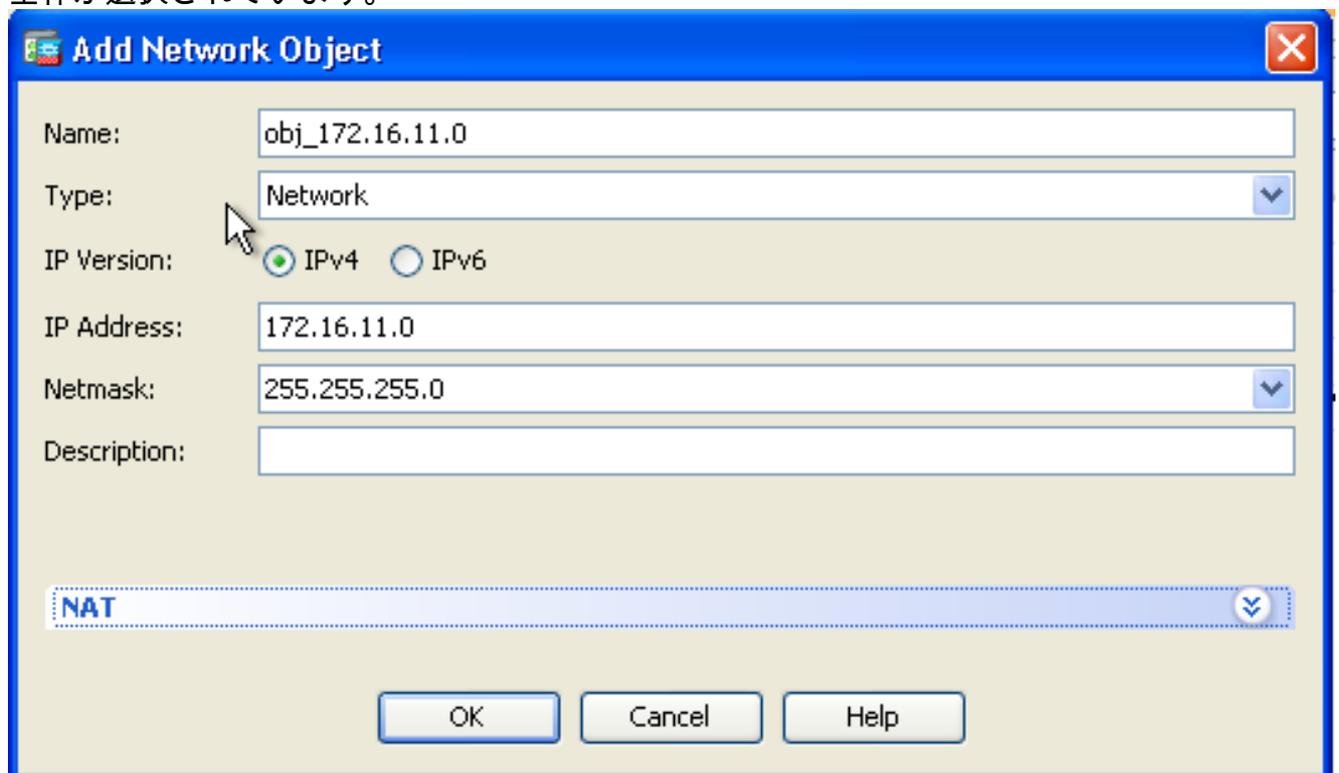
このためには、アクセスを許可するホスト/ネットワークの実アドレスを選択し、変換 IP アドレスのプールにマップする必要があります。

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。

**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: ...

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. [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。

**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. [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。

**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

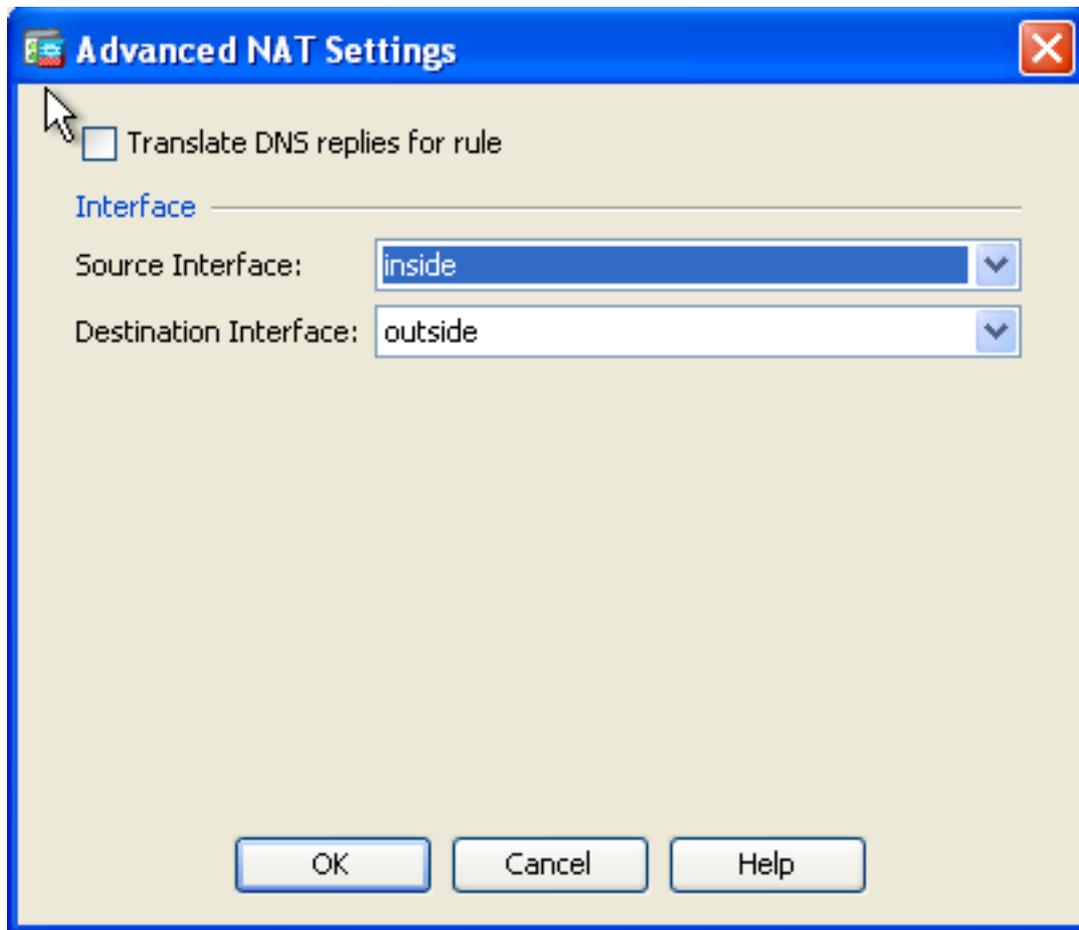
Fall through to interface PAT(dest intf): backup

Use IPv6 for interface PAT

Advanced...

OK Cancel Help

6. [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
```

この設定により、172.16.11.0ネットワーク内のホストは、NATプール203.0.113.10 ~ 203.0.113.20の任意のIPアドレスに変換されます。マッピングされたプールのアドレスが実際のグループよりも少ない場合、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バックアップを使用してダイナミックNATを実装したり、現在のプールを拡張したりすることができます。

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。

**Add Network Object**

Name: (optional)

Type:

IP Version:  IPv4  IPv6

IP Address:

Netmask:

FQDN:

Description:

**NAT**

OK Cancel Help

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。

**Add Network Object Group**

Group Name:

Description:

Existing Network Objects/Groups:

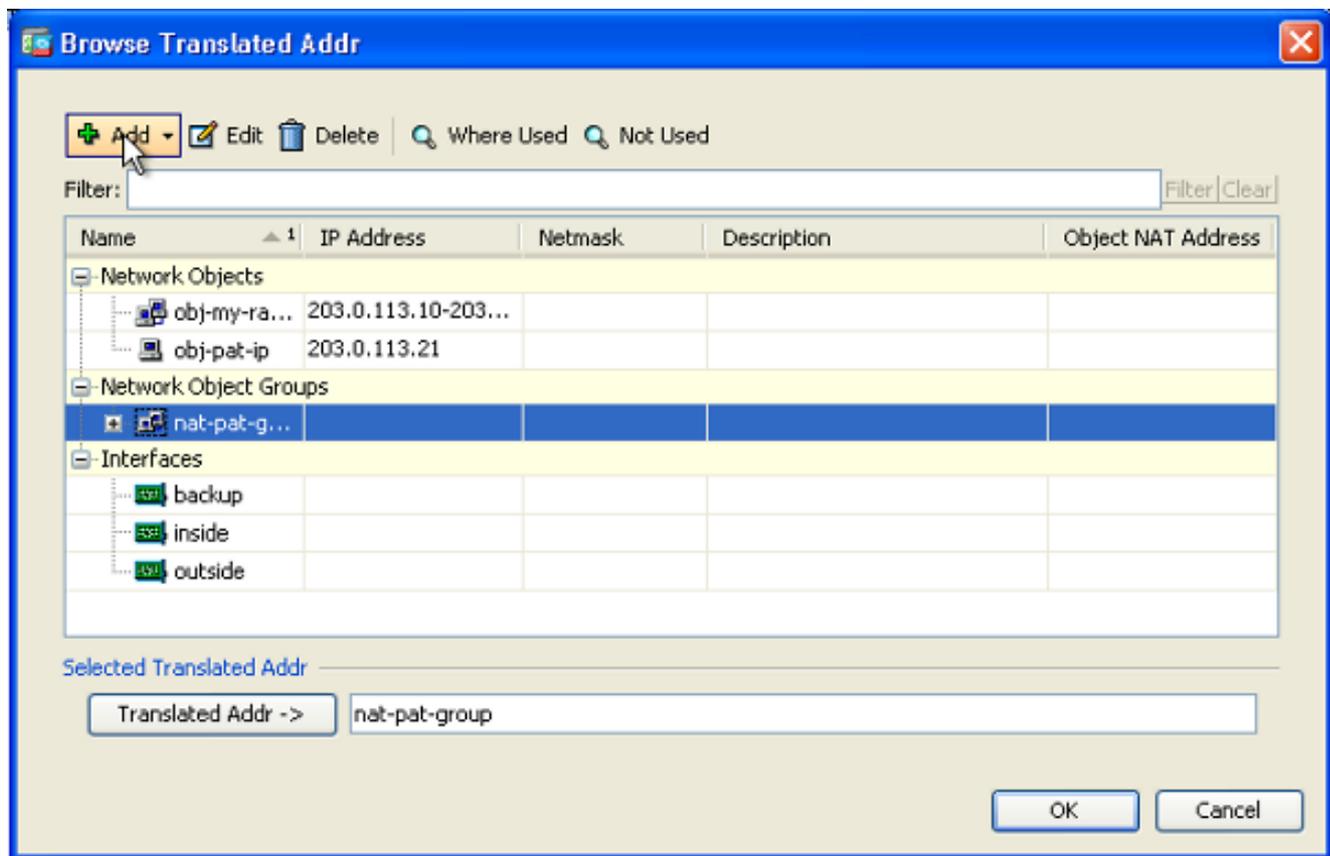
Name	IP Address	Netmask	Description
- Network Objects			
any			
any4			
any6			
inside-net...	19.19.19.0	255.255.255.0	
obj_172.1...	172.16.11.0	255.255.255.0	

Members in Group:

Name	IP Address	Netmask/Prefix L
obj-pat-ip	203.0.113.21	
obj-my-range	203.0.113.10-203.0.113.254	

Add >> << Remove

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。

**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

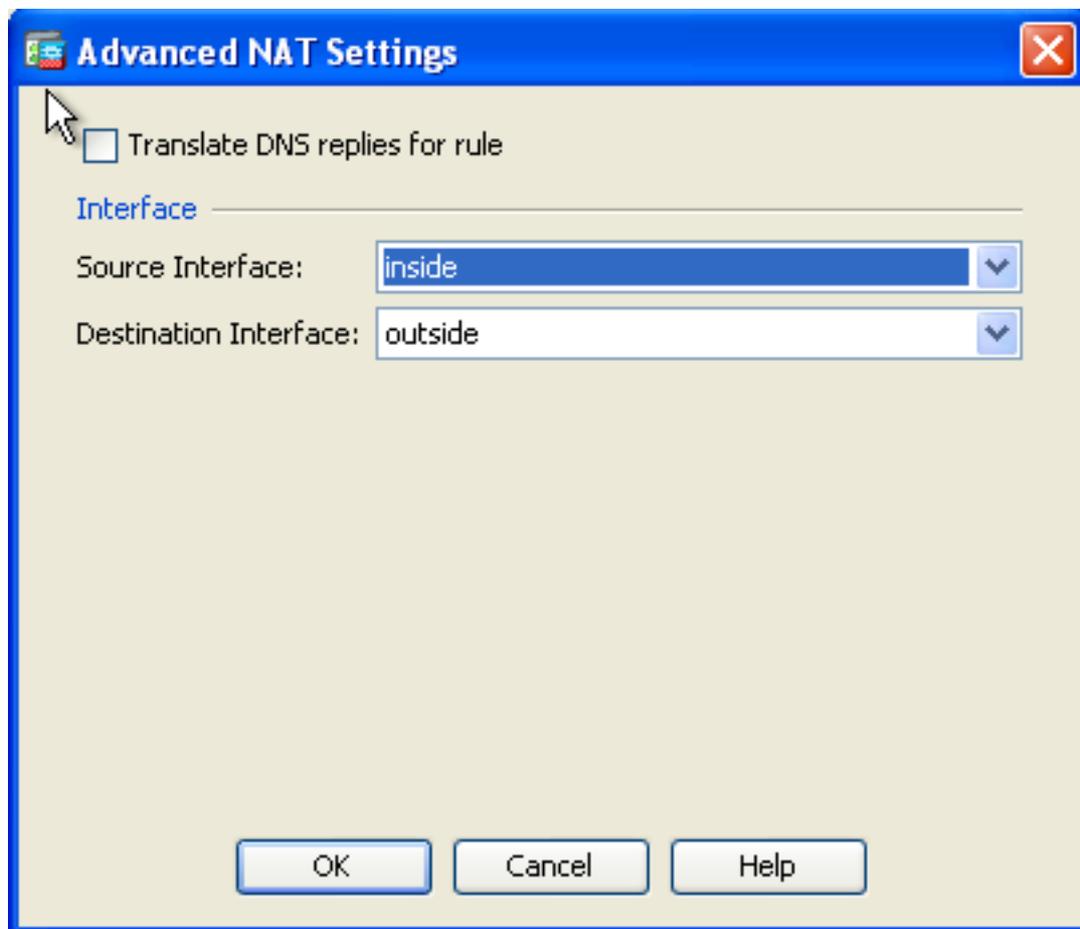
Fall through to interface PAT(dest intf): backup

Use IPv6 for interface PAT

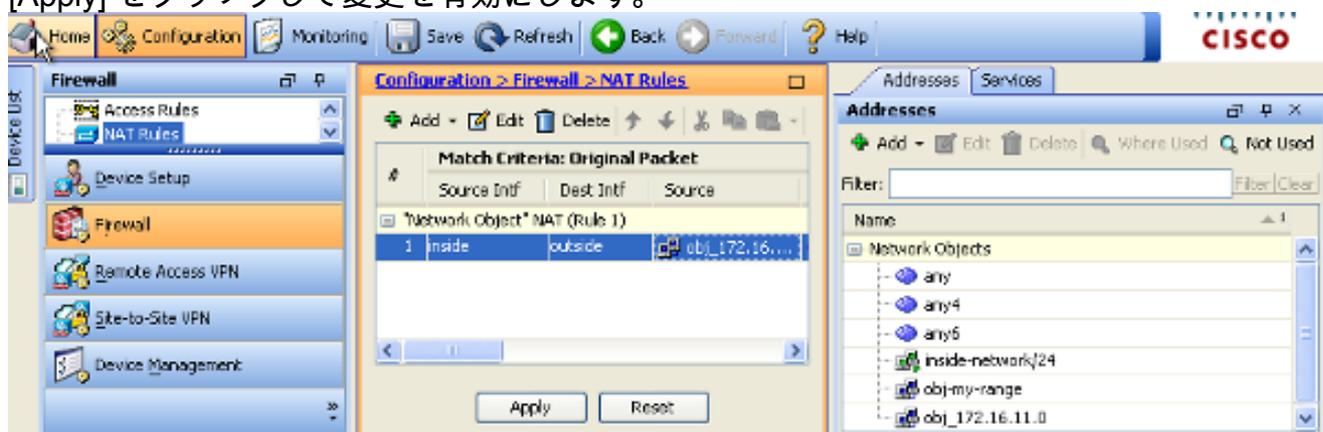
Advanced...

OK Cancel Help

5. [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
```

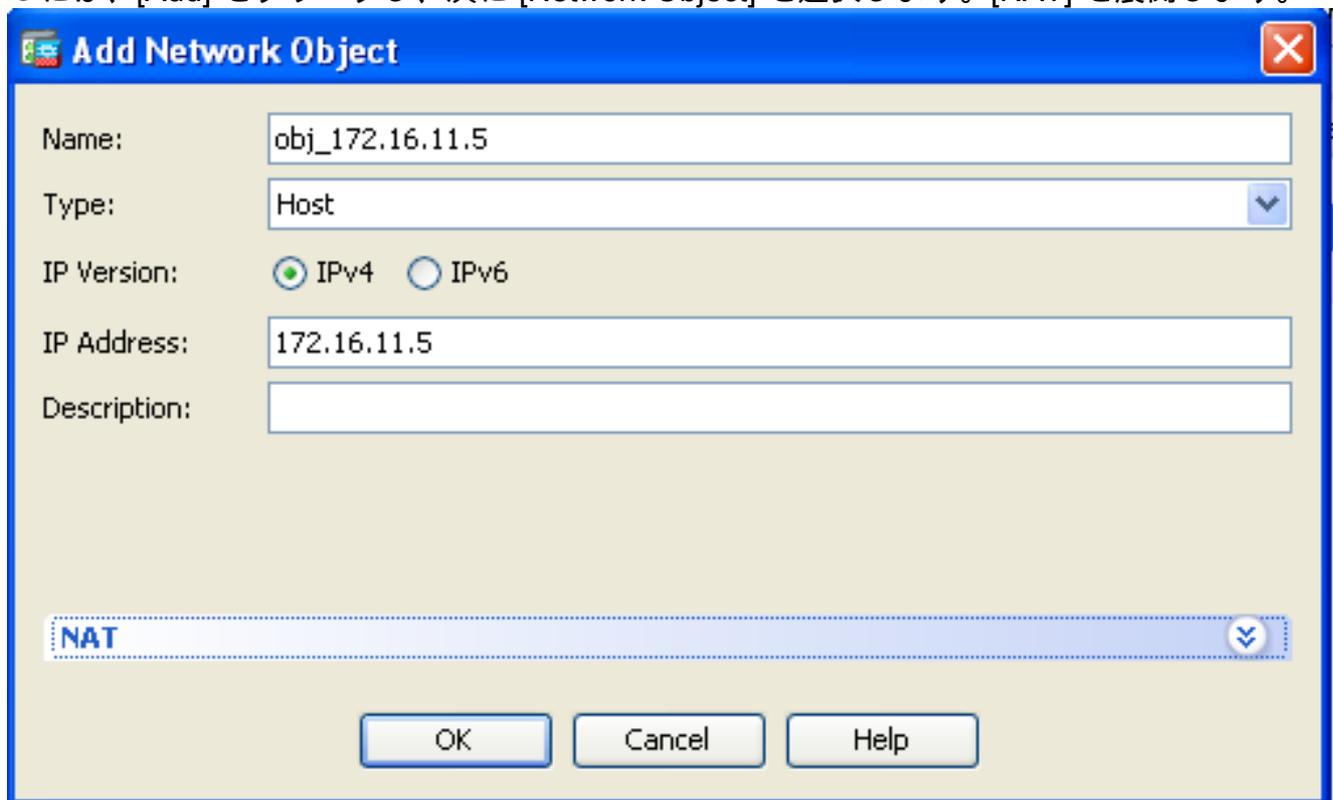
```
object-group network nat-pat-group
network-object object obj-my-range
network-object object obj-pat-ip
```

```
object network obj_172.16.11.0
subnet 172.16.11.0 255.255.255.0
```

## 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、インターネット上でルーティングできないプライベート IP アドレスを設定できます。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。

**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

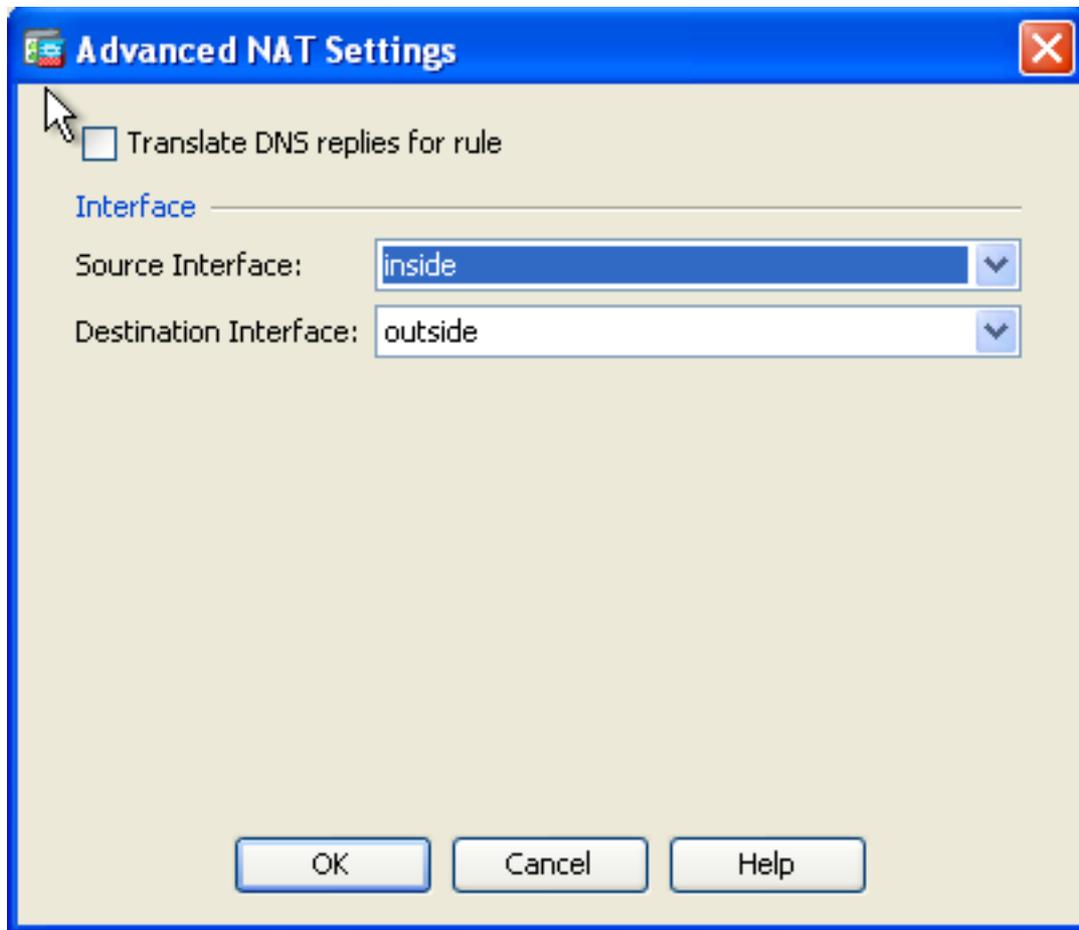
Fall through to interface PAT(dest intf): backup

Use IPv6 for interface PAT

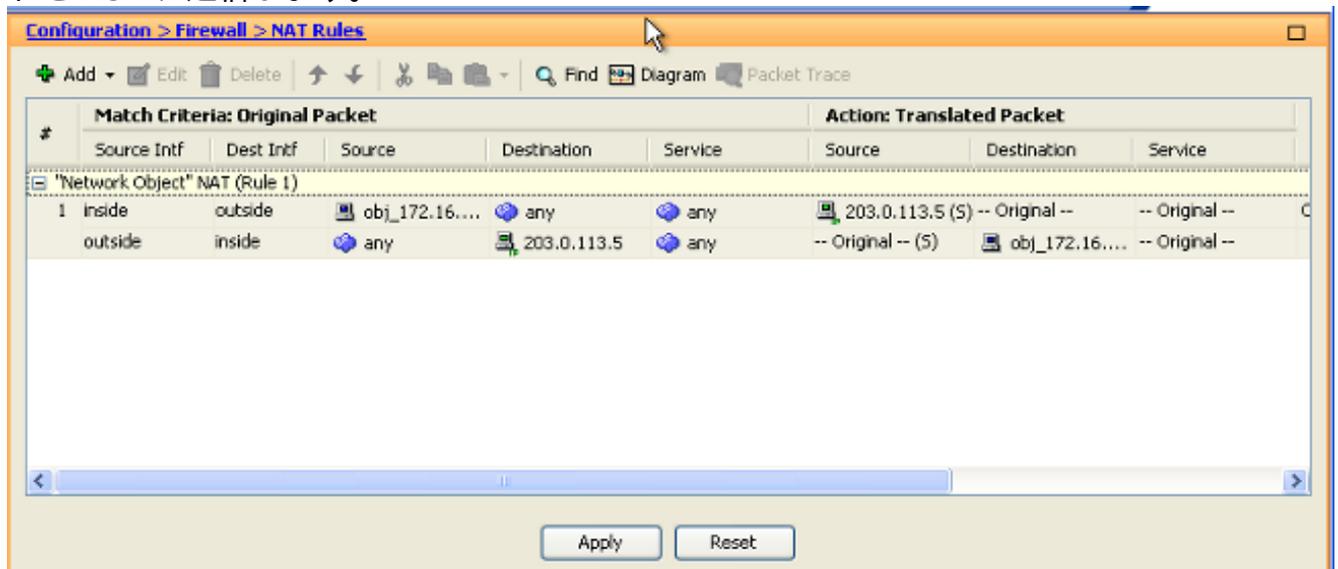
Advanced...

OK Cancel Help

3. [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

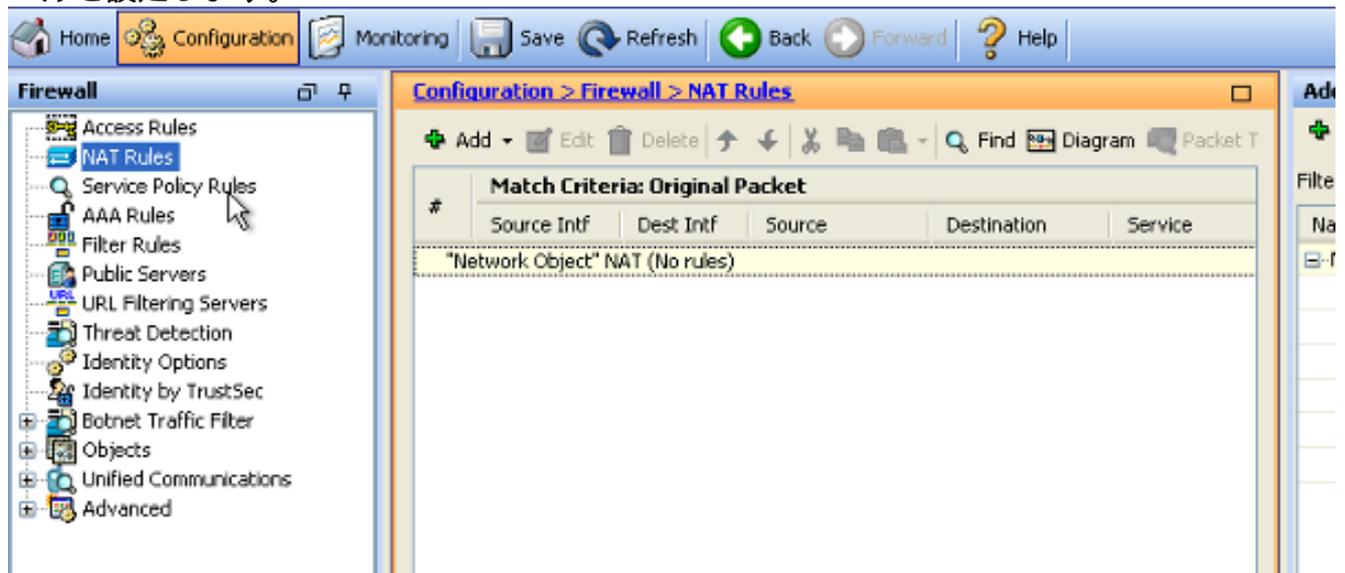
NAT 免除は、内部のユーザが NAT の完了なしに、リモート VPN ホスト/サーバ、または ASA の他のインターフェイスの背後にあるホスト/サーバにアクセスしようとする場合に便利な機能です

。これを実現するために、プライベートIPアドレスを持つ内部サーバは、それ自体にID変換でき、次にNATを実行する宛先へのアクセスを許可されます。

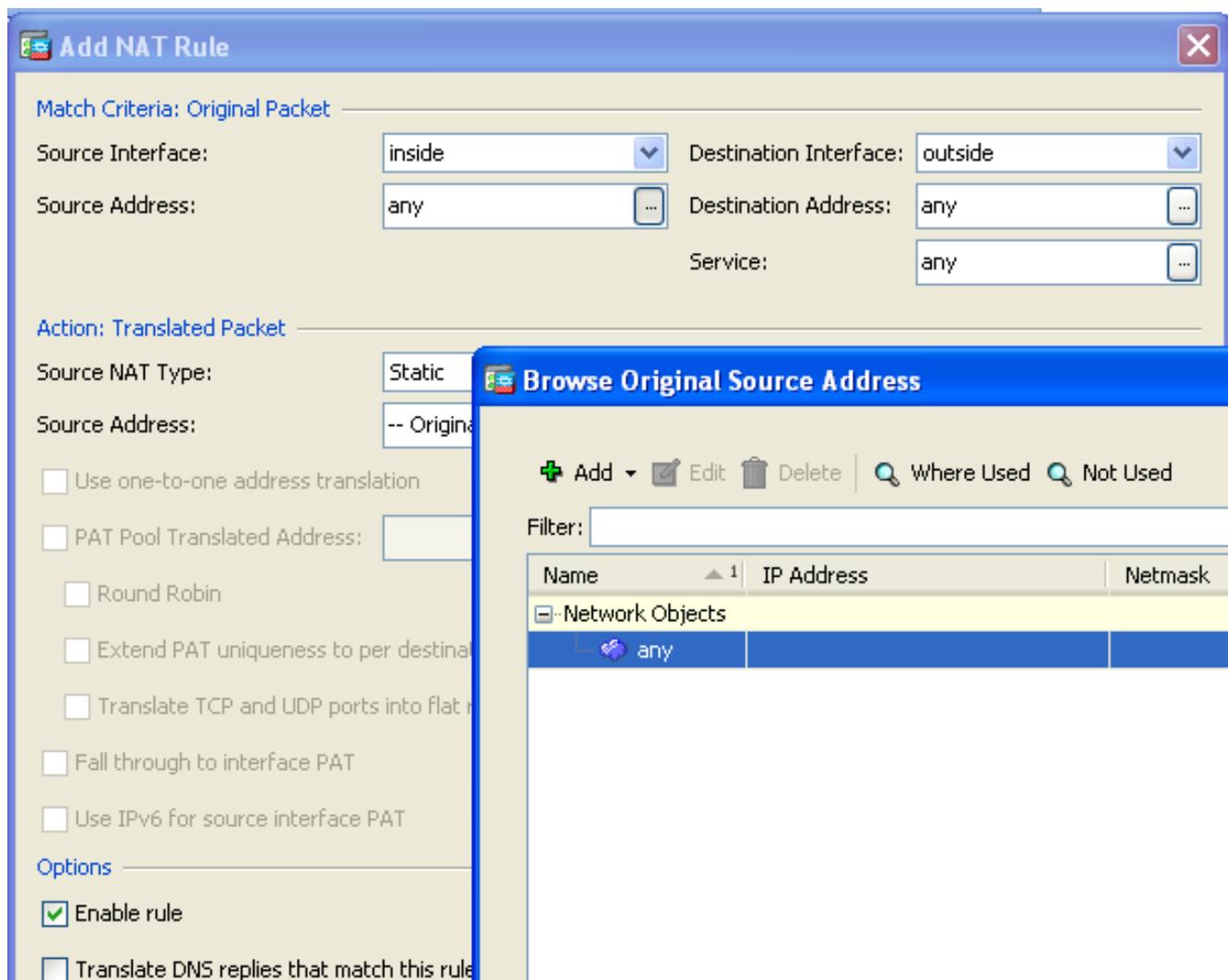
この例では、内部ホスト 172.16.11.15 は、リモート VPN サーバの 172.20.21.15 にアクセスする必要があります。

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。

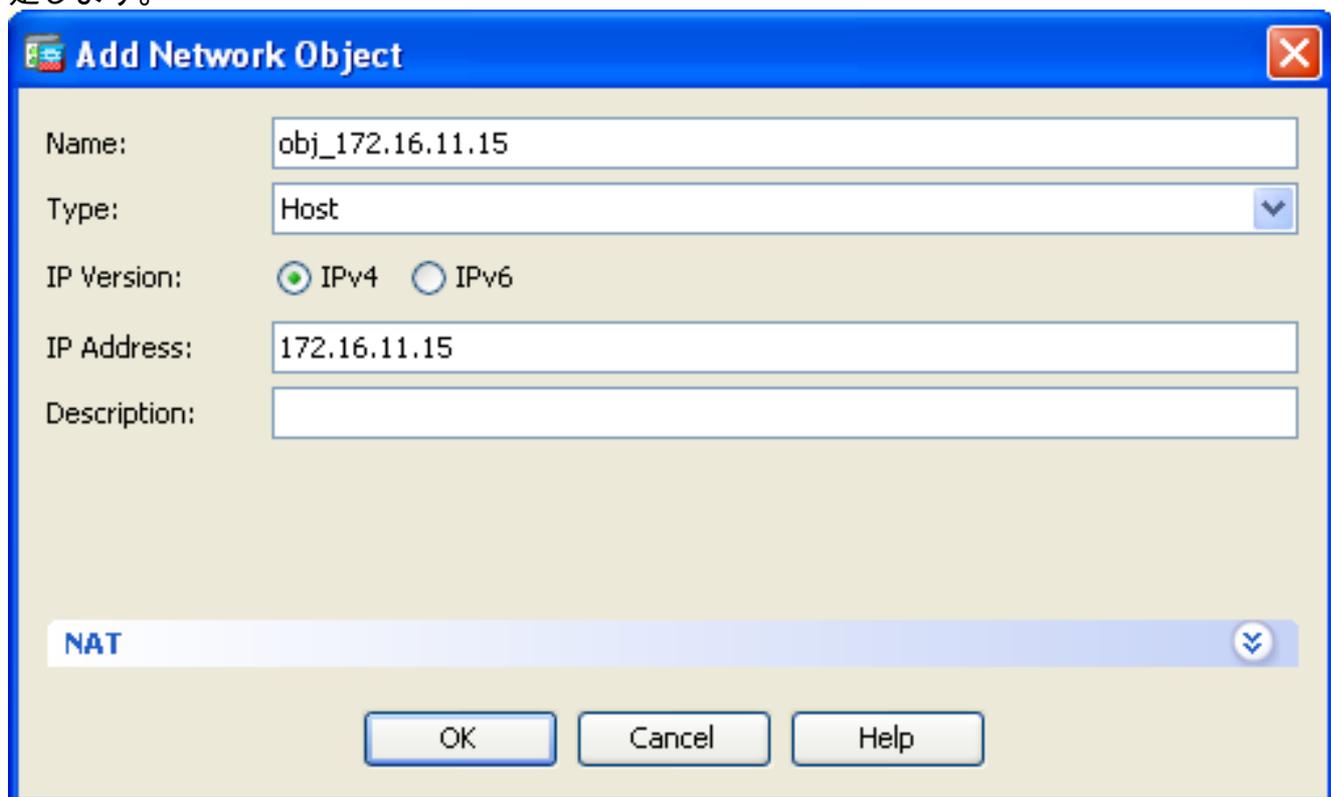
1. [Configuration] > [Firewall] > [NAT Rules] を選択します。[Add] をクリックして、NAT 免除ルールを設定します。



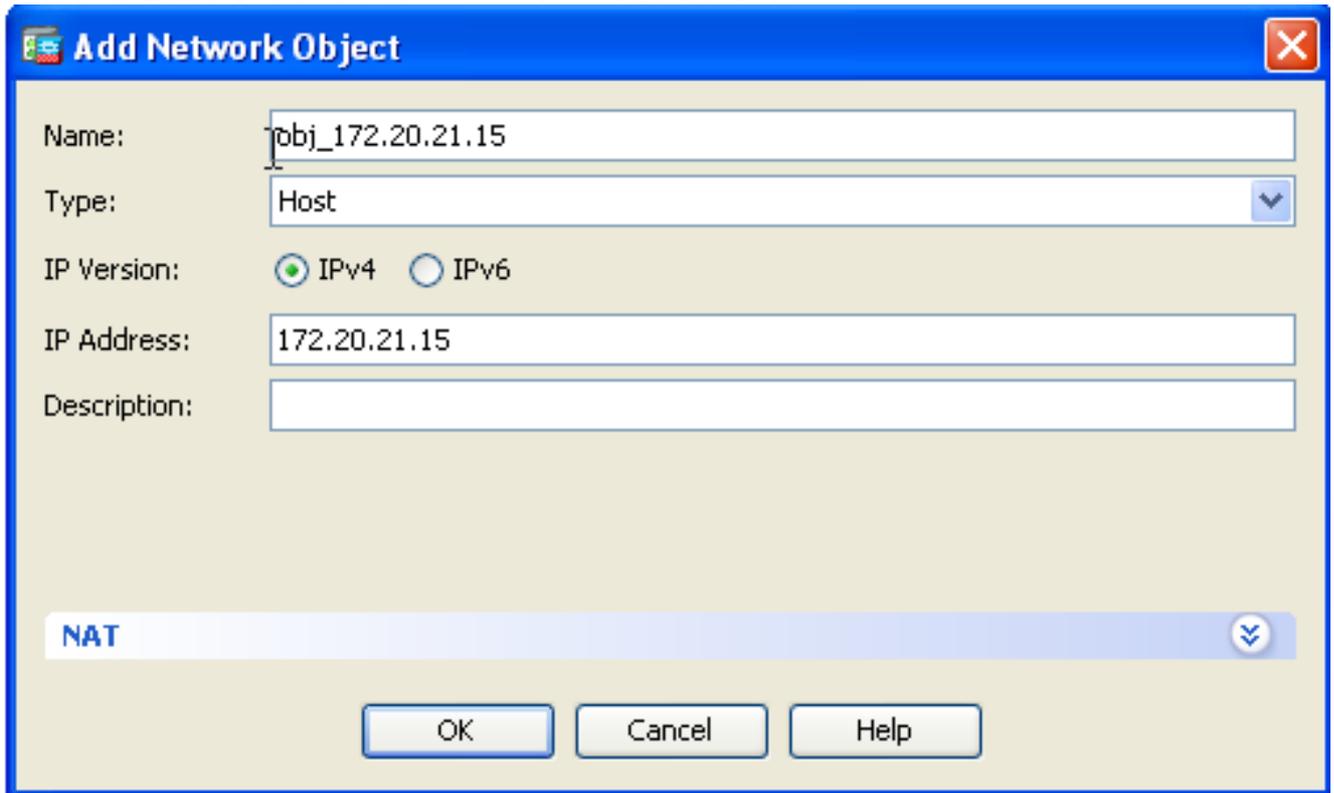
2. [Source Interface] および [Destination Interface] のドロップダウン リストで、適切なインターフェイスを選択します。[Source Address] フィールドで、適切なエントリを選択します。



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。



**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 [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。

**Add NAT Rule**

Match Criteria: Original Packet

Source Interface:  Destination Interface:

Source Address:  Destination Address:

Service:

Action: Translated Packet

Source NAT Type:

Source Address:  Destination Address:

Use one-to-one address translation

PAT Pool Translated Address:  Service:

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

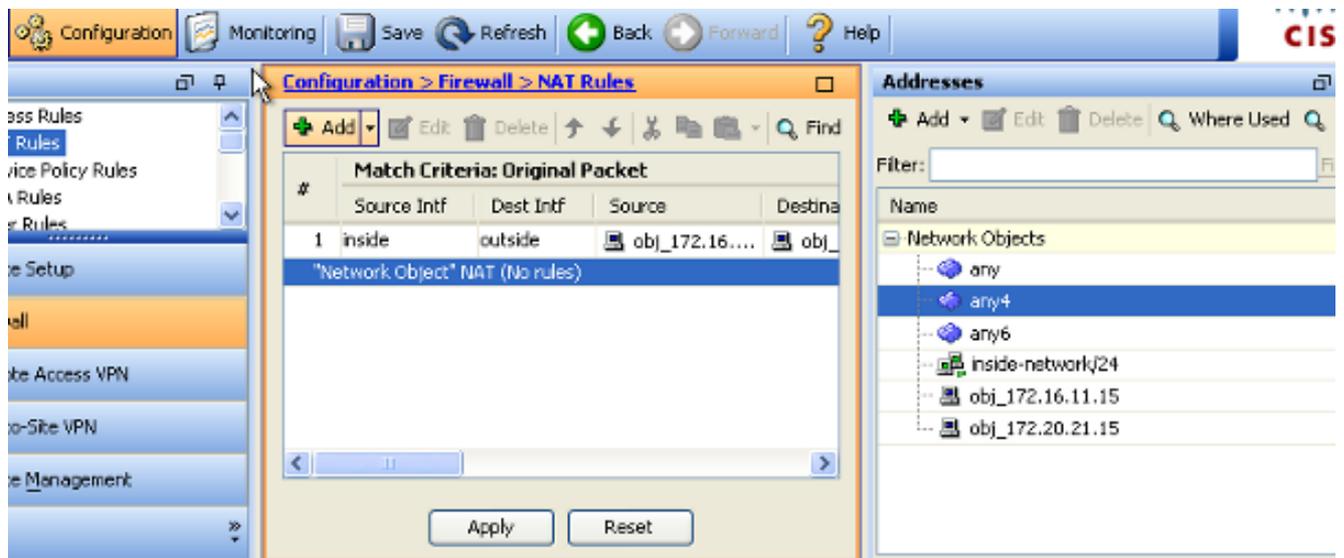
Disable Proxy ARP on egress interface

Lookup route table to locate egress interface

Direction:

Description:

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 )

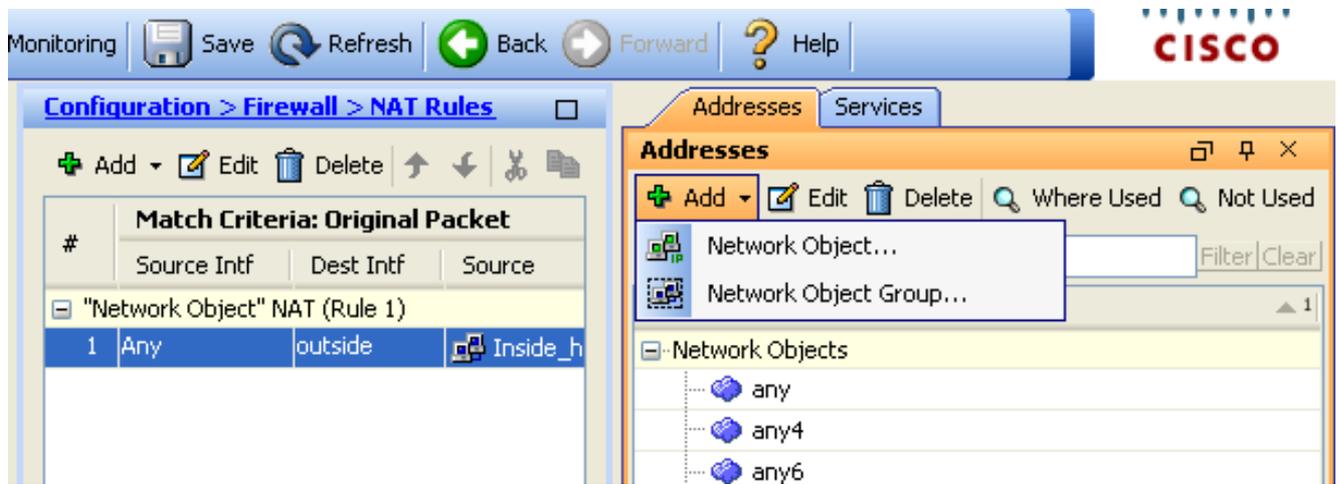
ポート フォワーディング ( ポート リダイレクション ) は、外部ユーザが特定ポートから内部サーバにアクセスする場合に便利な機能です。これを実現するには、プライベートIPアドレスを持つ内部サーバをパブリックIPアドレスに変換し、次に特定のポートに対するアクセスを許可します。

この例では、外部ユーザがSMTPサーバ203.0.113.15にポート25でアクセスしようとしています。これは、次の2つの手順で実現します。

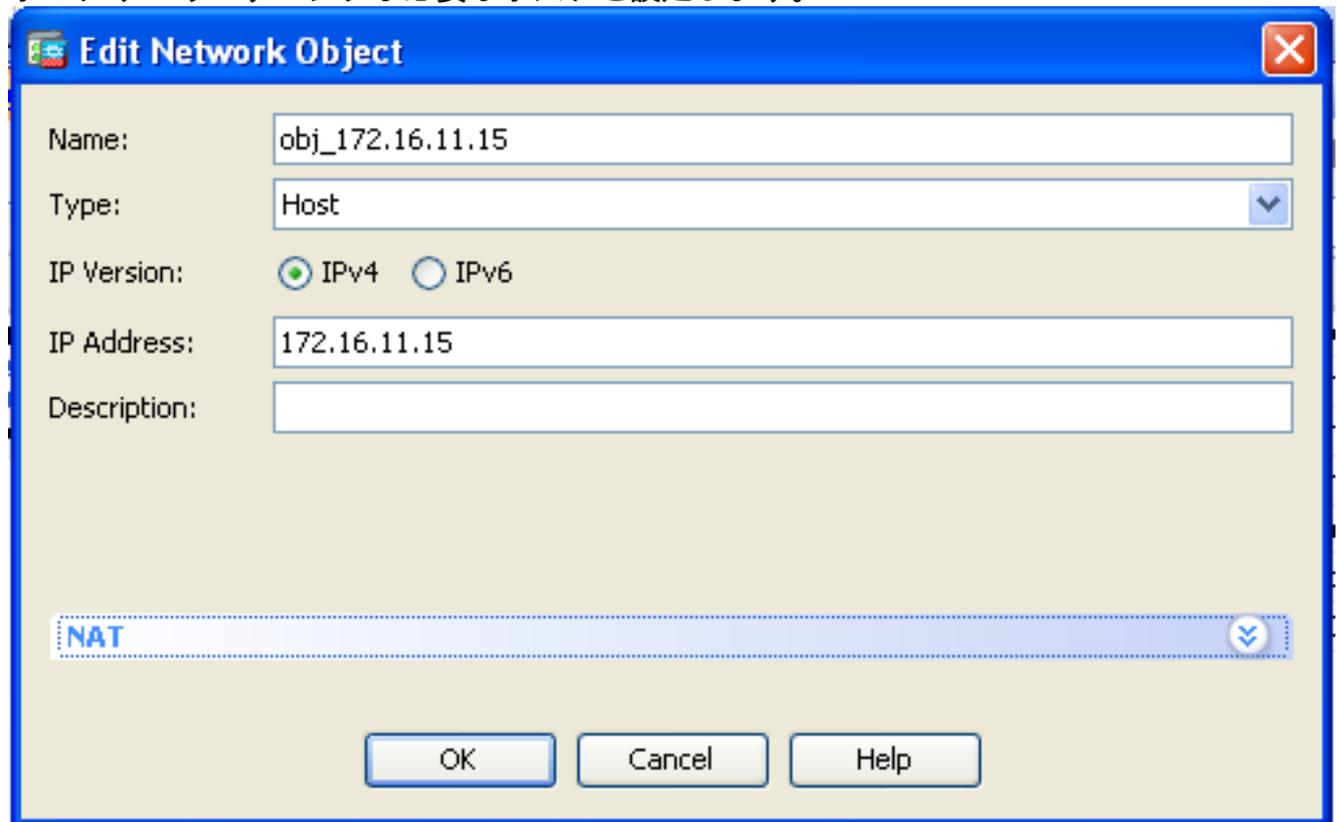
1. 内部メールサーバ ( ポート25の172.16.11.15 ) をパブリックIPアドレス ( ポート25の203.0.113.15 ) に変換します。
2. パブリック メール サーバ 203.0.113.15 へのポート 25 でのアクセスを許可します。

外部ユーザがサーバ203.0.113.15 ( ポート25 ) にアクセスしようとする、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。

**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

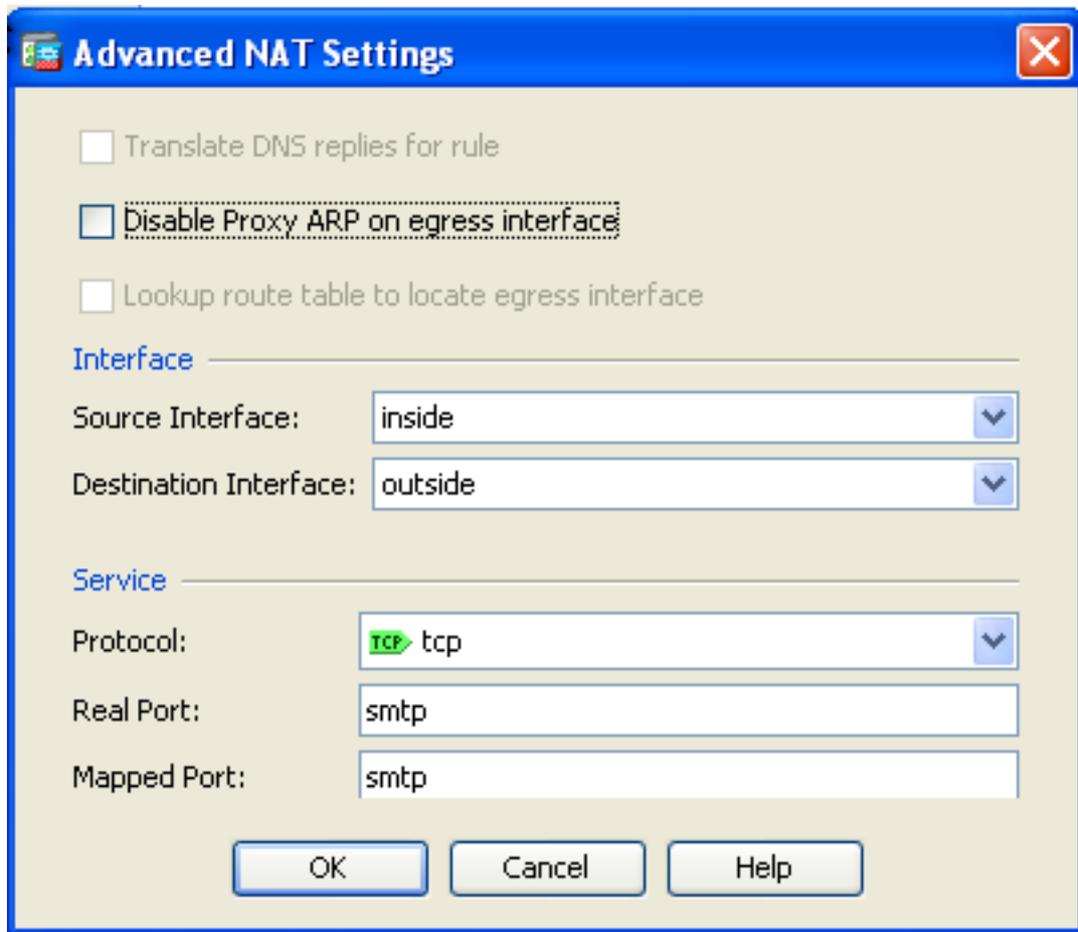
Fall through to interface PAT(dest intf): backup

Use IPv6 for interface PAT

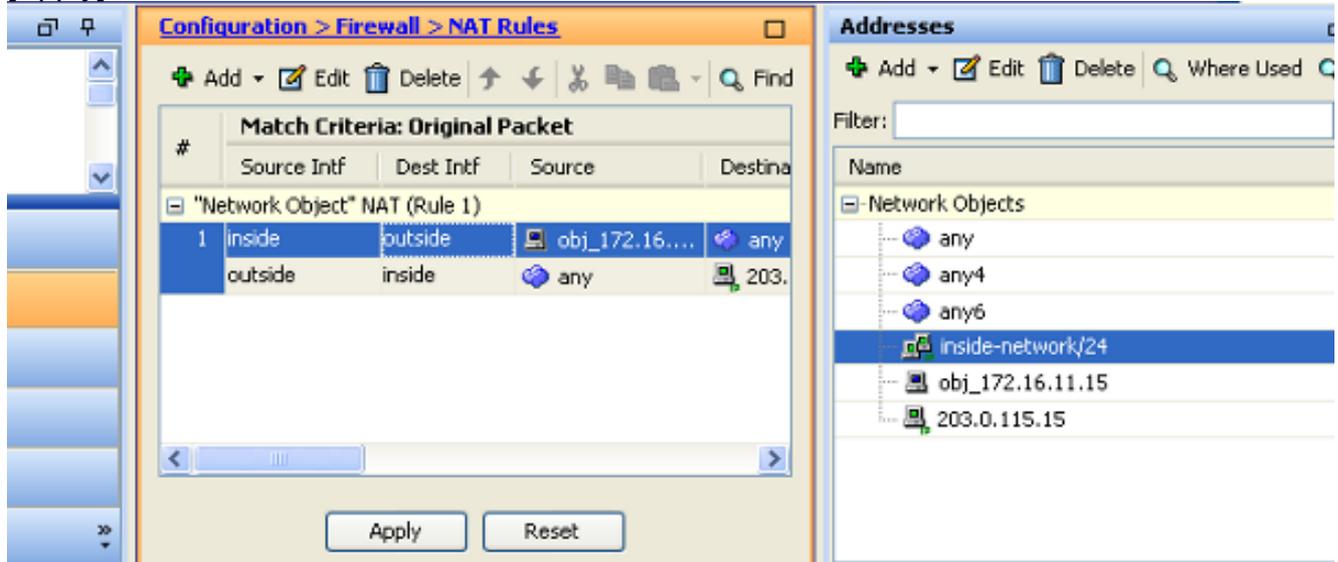
Advanced...

OK Cancel Help

4. [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 203.0.113.15 service tcp smtp smtp
```

## 確認

ここでは、設定が正常に機能しているかどうかを確認します。

[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ています。接続に成功した場合、この出力は ASA CLI に表示されます。

## Connection

```
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 の詳細レベルはログ設定に基づきます。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 つの 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ています。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

```
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せん。このツールを使用すると、ファイアウォールの通過を許可できると考えられるトラフィックの例を特定し、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ます。
- トラフィックの宛先はポート 80 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、『[パケットトレーサ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 で、TCP ホスト 172.16.11.5 から ホスト 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指定しました。つまり、ホスト 172.16.11.5 から ホスト 198.51.100.100 に送信されるすべての TCP トラフィックをキャプチャします。match キーワードを使用することで、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 アドレスとは照合できません。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の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、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 の設定例](#)
- [CLI および ASDM を使用した ASA パケット 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](#)

## 翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。