



NAT の例と参照

次のトピックでは、NAT を設定する例を示し、さらに高度な設定およびトラブルシューティングに関する情報について説明します。

- [ネットワーク オブジェクト NAT の例 \(1 ページ\)](#)
- [Twice NAT の例 \(15 ページ\)](#)
- [ルーテッドモードとトランスペアレントモードの NAT \(28 ページ\)](#)
- [NAT パケットのルーティング \(31 ページ\)](#)
- [VPN の NAT \(35 ページ\)](#)
- [IPv6 ネットワークの変換 \(42 ページ\)](#)
- [NAT を使用した DNS クエリと応答の書き換え \(54 ページ\)](#)

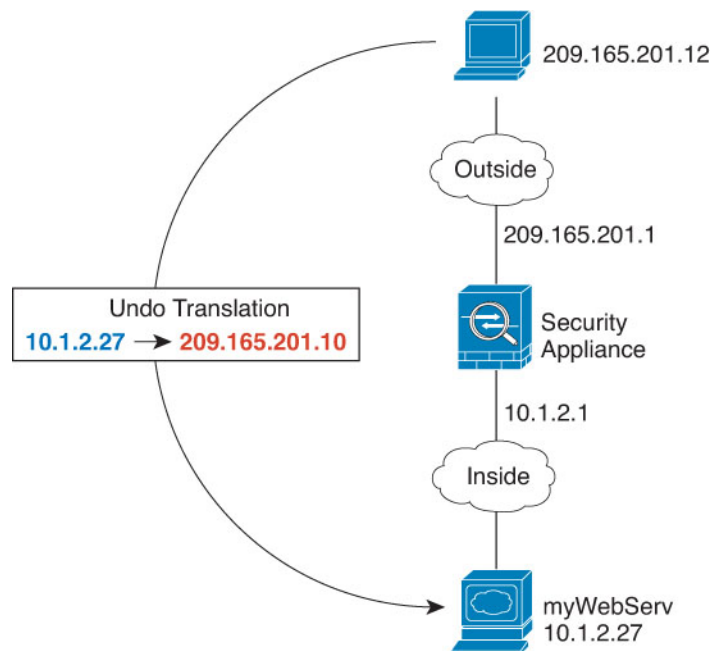
ネットワーク オブジェクト NAT の例

次に、ネットワーク オブジェクト NAT の設定例を示します。

内部 Web サーバーへのアクセスの提供 (スタティック NAT)

次の例では、内部 Web サーバに対してスタティック NAT を実行します。実際のアドレスはプライベート ネットワーク上にあるため、パブリックアドレスが必要です。スタティック NAT は、固定アドレスにある Web サーバーへのトラフィックをホストが開始できるようにするために必要です。

図 1: 内部 Web サーバーのスタティック NAT

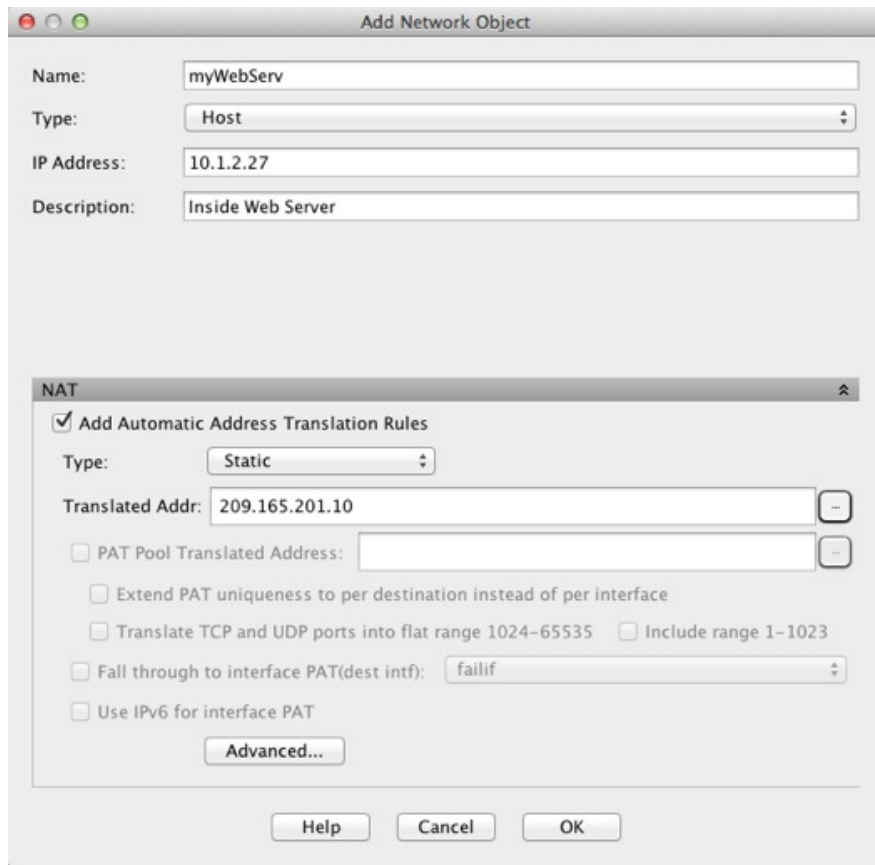


手順

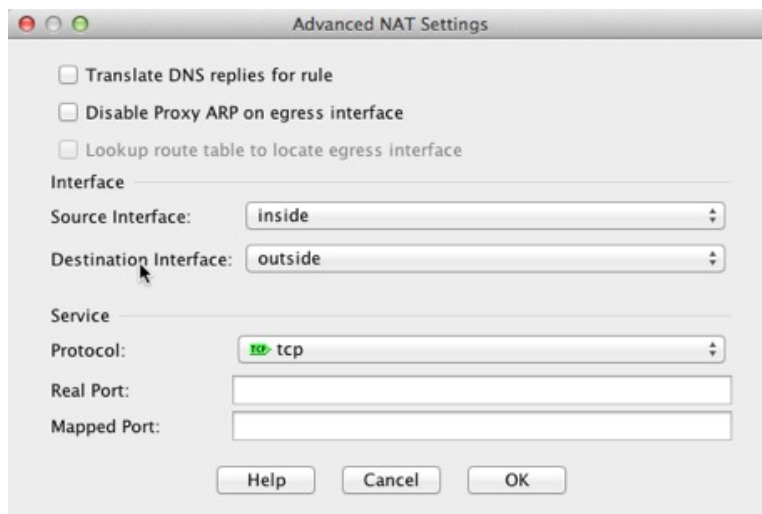
- ステップ 1 [Configuration] > [Firewall] > [NAT] を選択します。
- ステップ 2 [Add] > [Network Object NAT Rule] を選択し、新しいネットワーク オブジェクトに名前を付けて Web サーバーのホストアドレスを定義します。



- ステップ 3 オブジェクトのスタティック NAT を設定します。



ステップ 4 [Advanced] をクリックし、実際のインターフェイスとマッピングインターフェイスを設定します。

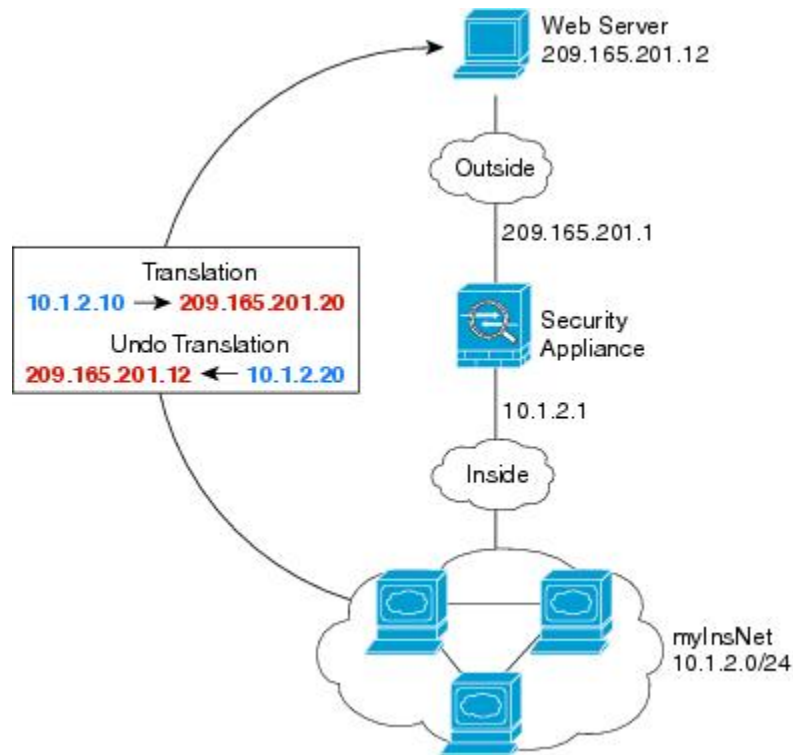


ステップ 5 [OK] をクリックして [ネットワーク オブジェクトの編集 (Edit Network Object)] ダイアログボックスに戻り、もう一度 [OK] をクリックし、[適用 (Apply)] をクリックします。

内部ホストの NAT (ダイナミック NAT) および外部 Web サーバーの NAT (スタティック NAT)

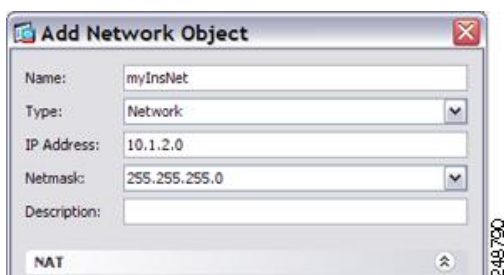
次の例では、プライベート ネットワーク上の内部ユーザーが外部にアクセスする場合、このユーザーにダイナミック NAT を設定します。また、内部ユーザーが外部 Web サーバーに接続する場合、この Web サーバーのアドレスが内部ネットワークに存在するよう見えるアドレスに変換されます。

図 2: 内部のダイナミック NAT、外部 Web サーバーのスタティック NAT

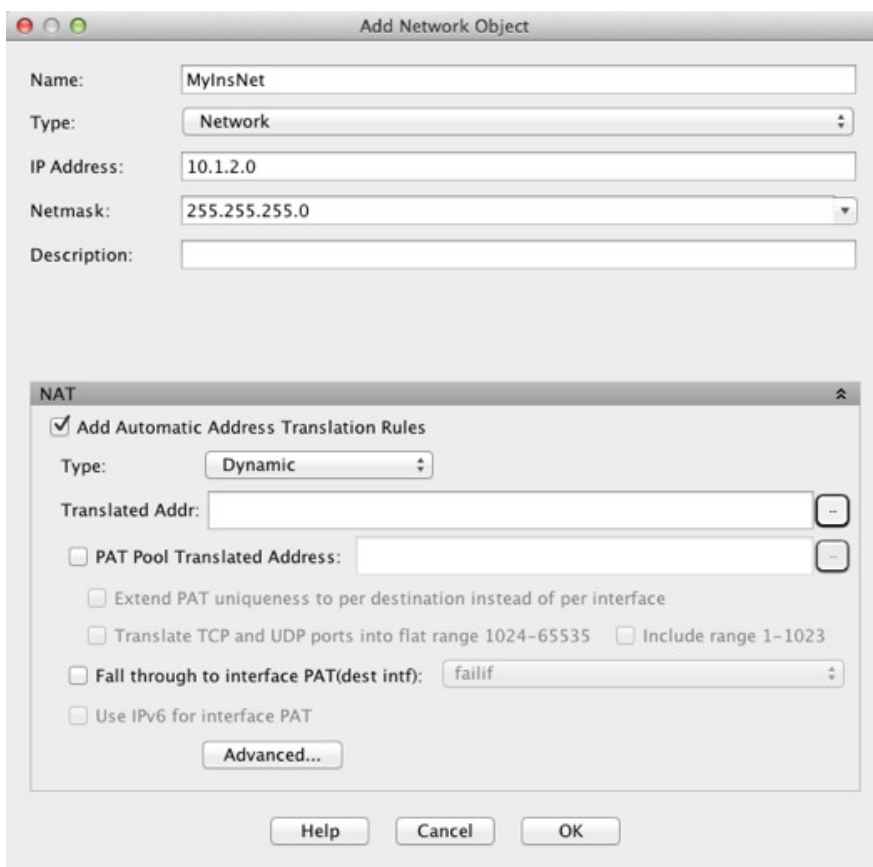


手順

- ステップ 1 [Configuration] > [Firewall] > [NAT] を選択します。
- ステップ 2 [Add] > [Network Object NAT Rule] を選択し、新しいネットワーク オブジェクトに名前を付けて内部ネットワークを定義します。

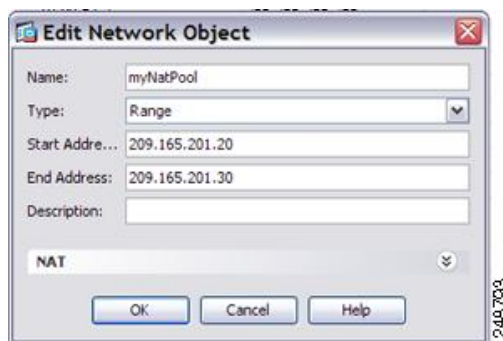


ステップ3 内部ネットワークのダイナミック NAT をイネーブルにします。



ステップ4 [Translated Addr] フィールドで、内部アドレスの変換先となるダイナミック NAT プールを表す新しいネットワーク オブジェクトを追加するには、参照ボタンをクリックします。

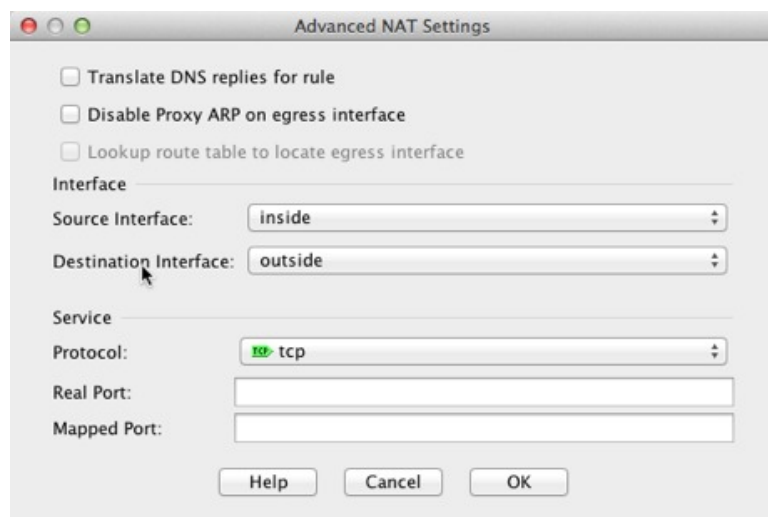
- a) [Add] > [Network Object] を選択し、新しいオブジェクトに名前を付けて NAT プールのアドレスの範囲を定義し、[OK] をクリックします。



- b) 新しいネットワークオブジェクトをダブルクリックで選択します。[OK]をクリックして、NAT コンフィギュレーションに戻ります。

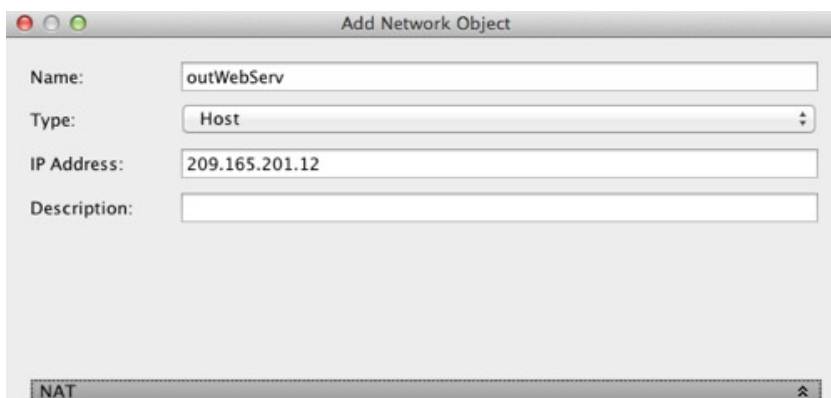


- ステップ 5** [Advanced] をクリックし、実際のインターフェイスとマッピングインターフェイスを設定します。



- ステップ 6** [OK] をクリックして [Edit Network Object] ダイアログボックスに戻り、もう一度 [OK] をクリックして [NAT Rules] テーブルに戻ります。

- ステップ 7** [Add] > [Network Object NAT Rule] を選択し、外部 Web サーバーのオブジェクトを作成します。



Add Network Object

Name: outWebServ

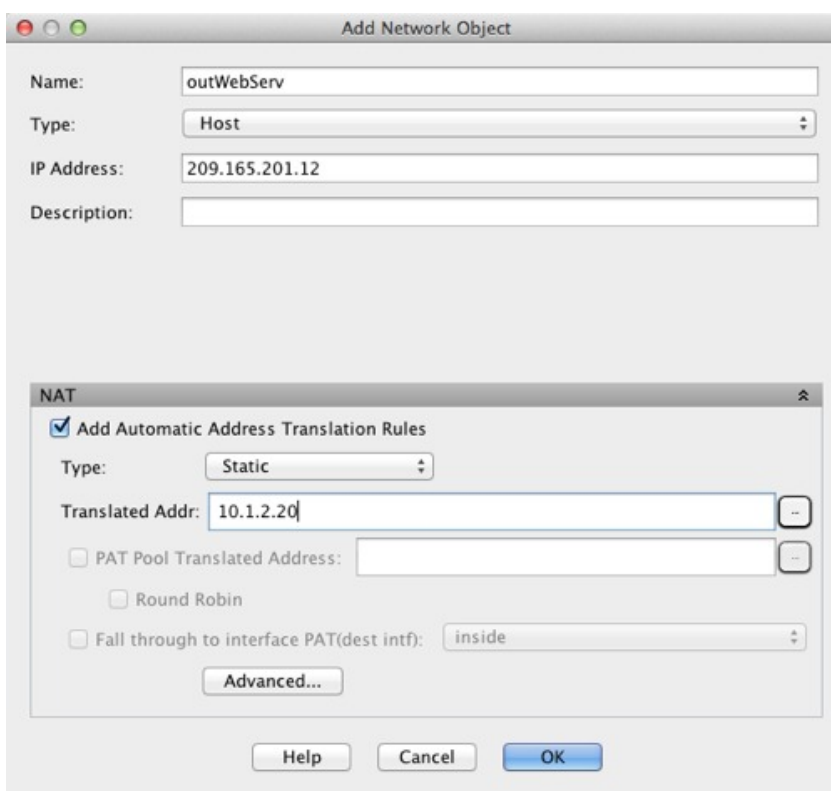
Type: Host

IP Address: 209.165.201.12

Description:

NAT

ステップ 8 Web サーバーのスタティック NAT を設定します。



Add Network Object

Name: outWebServ

Type: Host

IP Address: 209.165.201.12

Description:

NAT

Add Automatic Address Translation Rules

Type: Static

Translated Addr: 10.1.2.20

PAT Pool Translated Address:

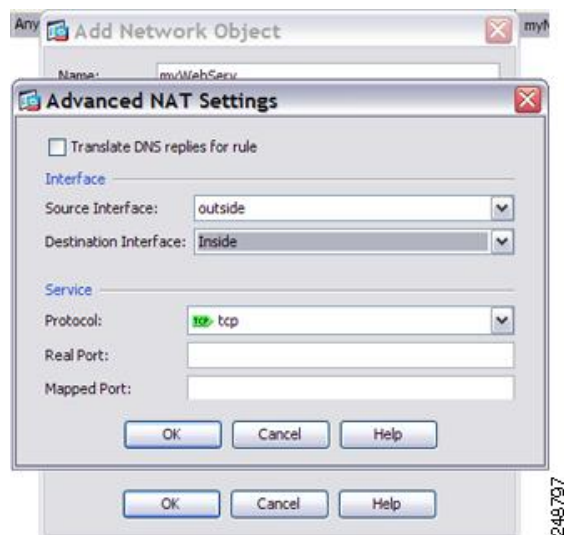
Round Robin

Fall through to interface PAT(dest intf): inside

Advanced...

Help Cancel OK

ステップ 9 [Advanced] をクリックし、実際のインターフェイスとマッピングインターフェイスを設定します。

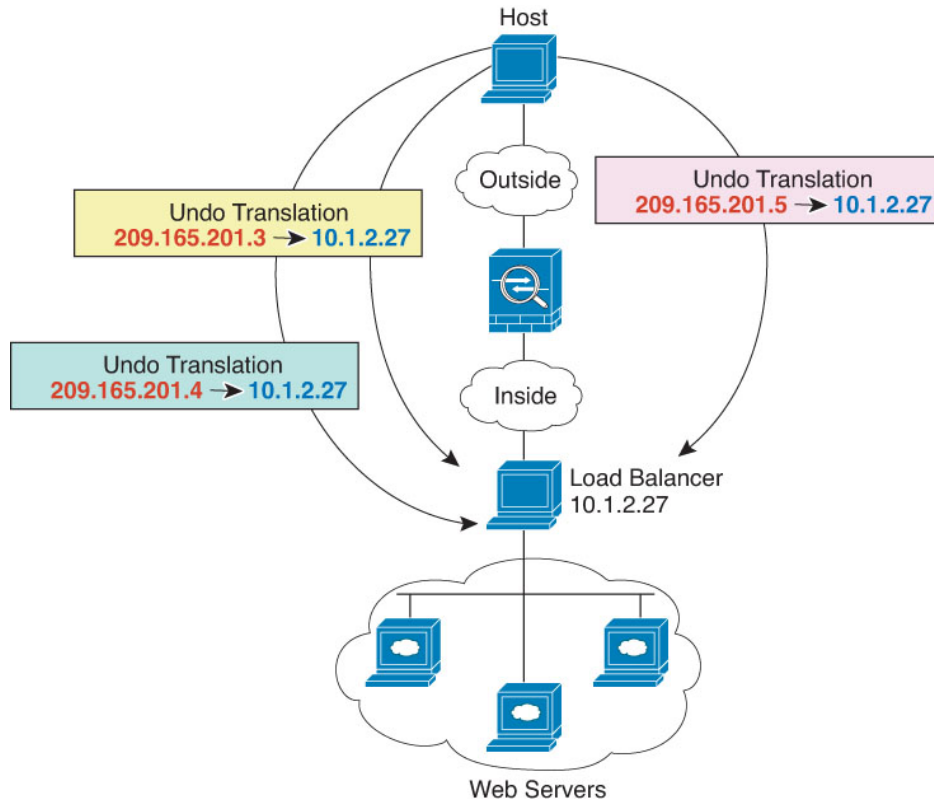


ステップ 10 [OK] をクリックして [ネットワーク オブジェクトの編集 (Edit Network Object)] ダイアログボックスに戻り、もう一度 [OK] をクリックし、[適用 (Apply)] をクリックします。

複数のマッピングアドレス（スタティック NAT、1 対多）を持つ内部ロード バランサ

次の例は、複数の IP アドレスに変換される内部ロード バランサを示します。外部ホストがいずれかのマッピング IP アドレスにアクセスすると、このアドレスは単一のロード バランサ アドレスに逆変換されます。要求される URL に応じて、トラフィックを正しい Web サーバにリダイレクトします。

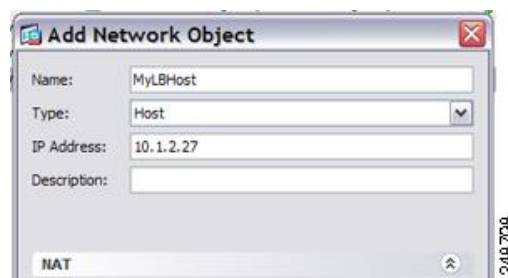
図 3: 内部ロードバランサに対する 1対多のスタティック NAT



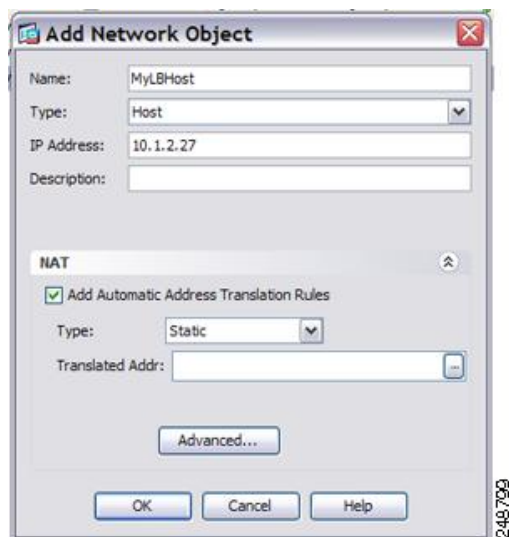
手順

ステップ 1 [設定 (Configuration)] > [ファイアウォール (Firewall)] > [NAT] を選択します。

ステップ 2 [追加 (Add)] > [ネットワーク オブジェクトの NAT ルール (Network Object NAT Rule)] を選択し、新しいネットワーク オブジェクトに名前を付けて、ロードバランサのアドレスを定義します。

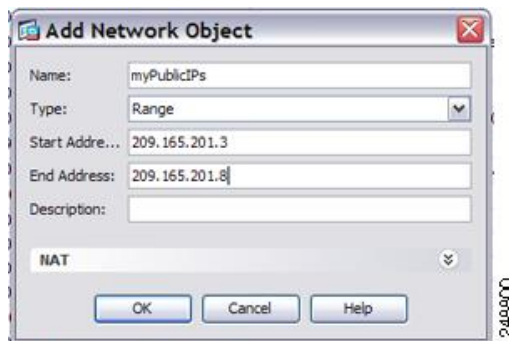


ステップ 3 ロードバランサのスタティック NAT をイネーブルにします。



ステップ 4 [Translated Addr] フィールドで、ロード バランサ アドレスの変換先となるスタティック NAT アドレス グループを表す新しいネットワーク オブジェクトを追加するには、参照ボタンをクリックします。

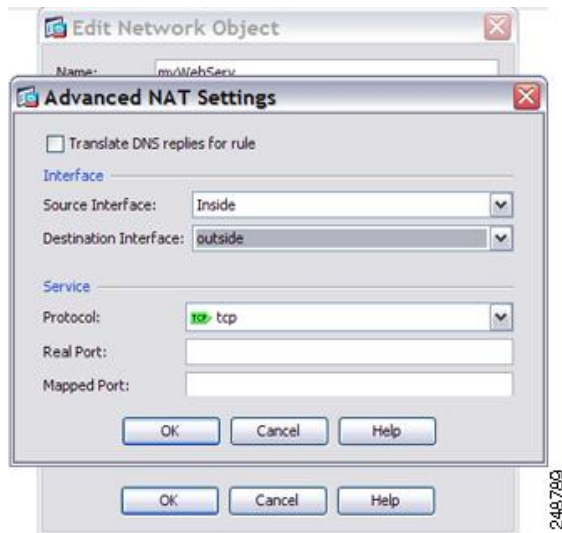
- a) [Add] > [Network Object] を選択し、を選択し、新しいオブジェクトに名前を付けてアドレスの範囲を定義し、[OK] をクリックします。



- b) 新しいネットワーク オブジェクトをダブルクリックで選択します。[OK] をクリックして、NAT コンフィギュレーションに戻ります。



ステップ 5 [Advanced] をクリックし、実際のインターフェイスとマッピングインターフェイスを設定します。

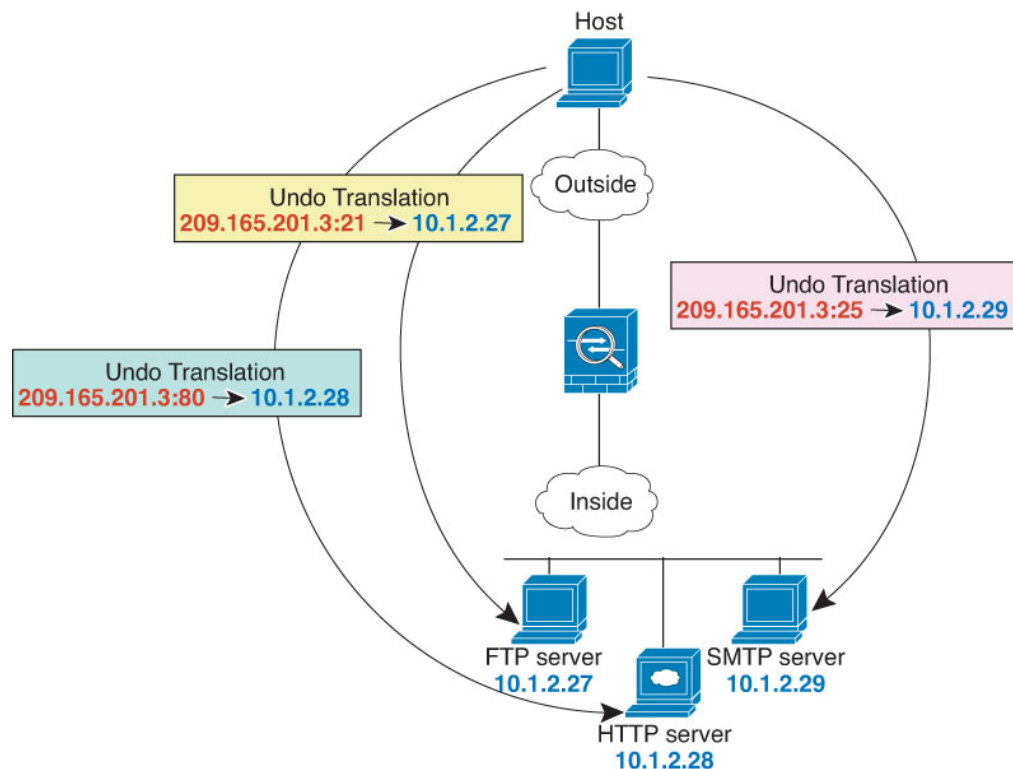


ステップ 6 [OK] をクリックして [ネットワーク オブジェクトの編集 (Edit Network Object)] ダイアログボックスに戻り、もう一度 [OK] をクリックし、[適用 (Apply)] をクリックします。

FTP、HTTP、および SMTP の単一アドレス（ポート変換を設定したスタティック NAT）

次のポート変換を設定したスタティック NAT の例では、リモートユーザーが FTP、HTTP、および SMTP にアクセスするための単一のアドレスを提供します。これらのサーバーは実際には、それぞれ異なるデバイスとして実際のネットワーク上に存在しますが、ポート変換を設定したスタティック NAT ルールを指定すると、使用するマッピング IP アドレスは同じで、それぞれ別のポートを使用できます。

図 4: ポート変換を設定したスタティック NAT

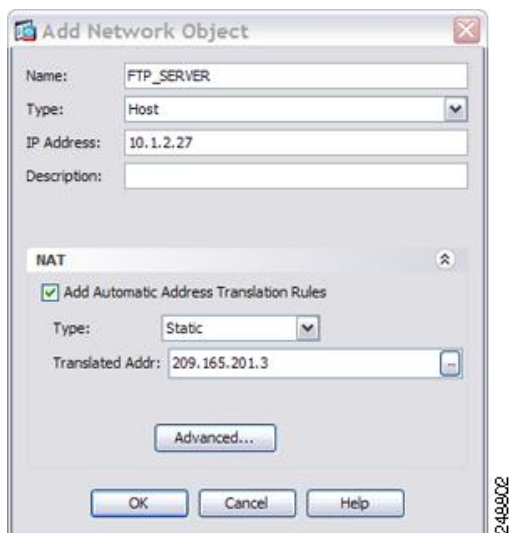


手順

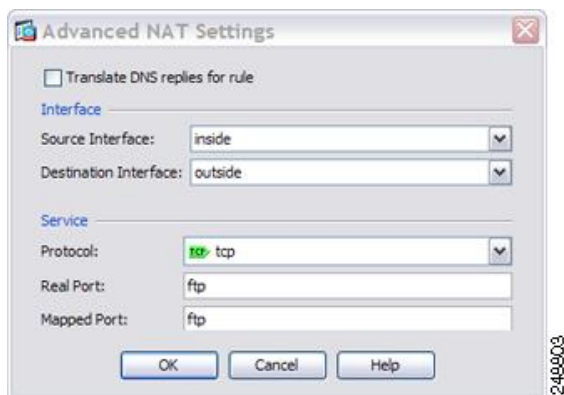
ステップ 1 [設定 (Configuration)] > [ファイアウォール (Firewall)] > [NAT] を選択します。

ステップ 2 FTP サーバーのポート変換ルールを設定したスタティック ネットワーク オブジェクト NAT を設定します。

- a) [追加 (Add)] > [ネットワーク オブジェクトの NAT ルール (Network Object NAT Rule)] を選択します。
- b) 新しいネットワーク オブジェクトに名前を付けて FTP サーバー アドレスを定義し、スタティック NAT をイネーブルにして変換されたアドレスを入力します。



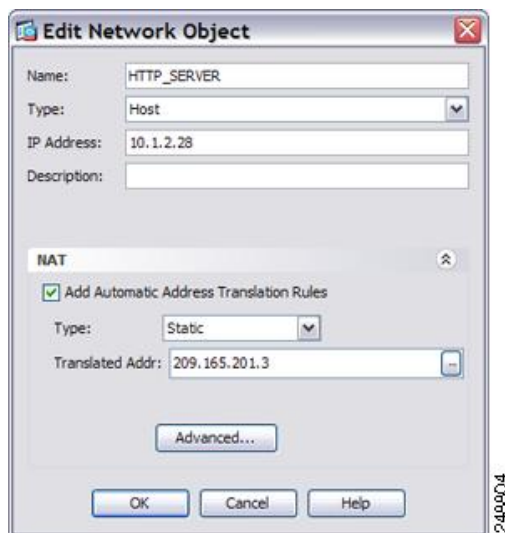
- c) [Advanced] をクリックして FTP の実際のインターフェイスおよびマッピングインターフェイスとポート変換を設定し、FTP ポートを自身にマッピングします。



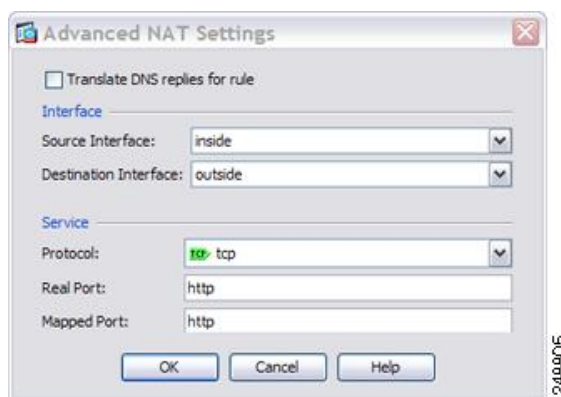
- d) [OK] をクリックしてもう一度 [OK] をクリックし、ルールを保存して [NAT] ページに戻ります。

ステップ 3 HTTP サーバのポート変換ルールを設定したスタティック ネットワーク オブジェクト NAT を設定します。

- [追加 (Add)] > [ネットワーク オブジェクトの NAT ルール (Network Object NAT Rule)] を選択します。
- 新しいネットワーク オブジェクトに名前を付けて HTTP サーバー アドレスを定義し、スタティック NAT をイネーブルにして変換されたアドレスを入力します。



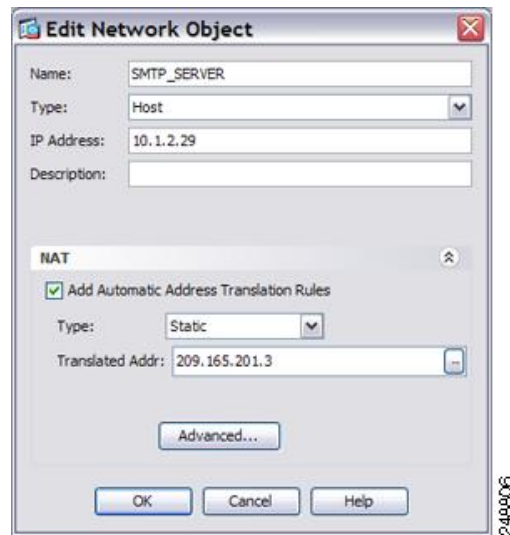
- c) [Advanced] をクリックして HTTP の実際のインターフェイスおよびマッピング インターフェイスとポート変換を設定し、HTTP ポートを自身にマッピングします。



- d) [OK] をクリックしてもう一度 [OK] をクリックし、ルールを保存して [NAT] ページに戻ります。

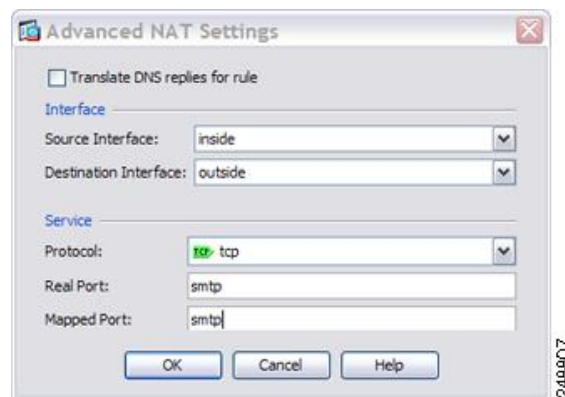
ステップ 4 SMTP サーバのポート変換ルールを設定したスタティック ネットワーク オブジェクト NAT を設定します。

- [追加 (Add)] > [ネットワーク オブジェクトの NAT ルール (Network Object NAT Rule)] を選択します。
- 新しいネットワーク オブジェクトに名前を付けて SMTP サーバー アドレスを定義し、スタティック NAT をイネーブルにして変換されたアドレスを入力します。



249806

- c) [Advanced] をクリックして SMTP の実際のインターフェイスおよびマッピング インターフェイスとポート変換を設定し、SMTP ポートを自身にマッピングします。



249807

- d) [OK] をクリックして [ネットワーク オブジェクトの編集 (Edit Network Object)] ダイアログボックスに戻り、もう一度 [OK] をクリックし、[適用 (Apply)] をクリックします。

Twice NAT の例

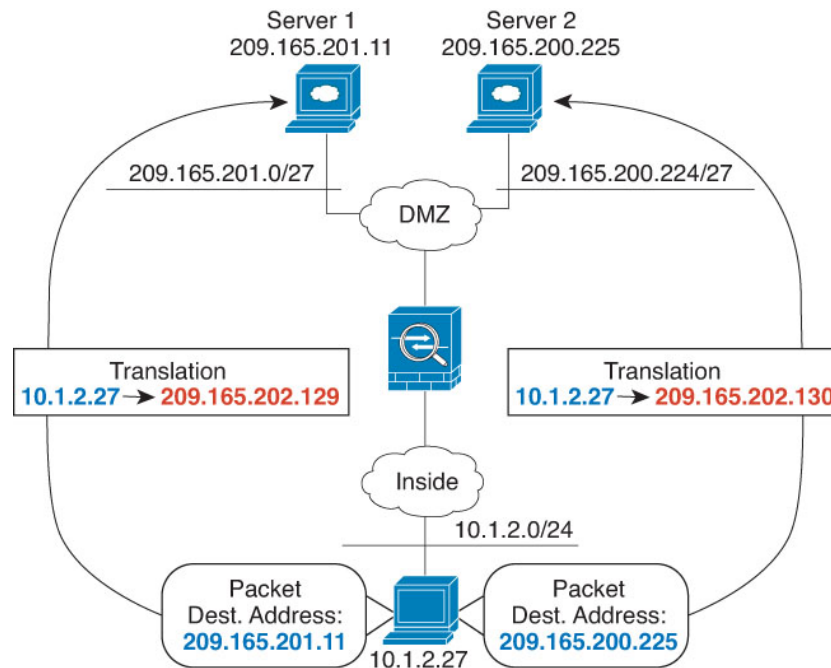
ここでは、次の設定例を示します。

宛先に応じて異なる変換 (ダイナミック Twice PAT)

次の図に、2 台の異なるサーバーにアクセスしている 10.1.2.0/24 ネットワークのホストを示します。ホストがサーバ 209.165.201.11 にアクセスすると、実際のアドレスは 209.165.202.129:

ポートに変換されます。ホストがサーバ 209.165.200.225 にアクセスすると、実際のアドレスは 209.165.202.130:ポートに変換されます。

図 5:異なる宛先アドレスを使用する **Twice NAT**

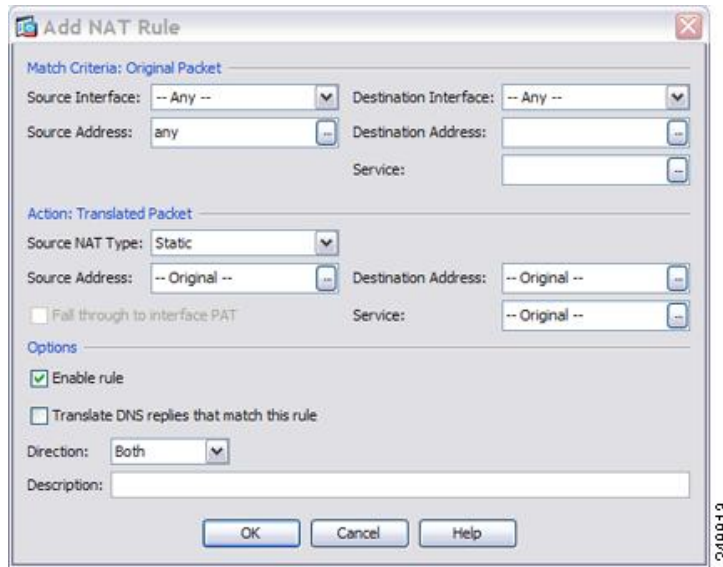


手順

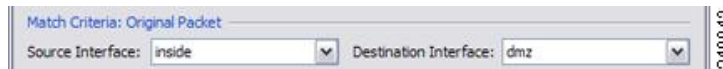
ステップ 1 [Configuration] > [Firewall] > [NAT Rules] ページで、[Add] > [Add NAT Rule Before Network Object NAT Rules] をクリックしてトラフィックの NAT ルールを内部ネットワークから DMZ ネットワーク 1 に追加します。

NAT ルールをセクション 3 (ネットワーク オブジェクト NAT ルールの後) に追加する場合は、[Add NAT Rule After Network Object NAT Rules] を選択します。

[Add NAT Rule] ダイアログボックスが表示されます。

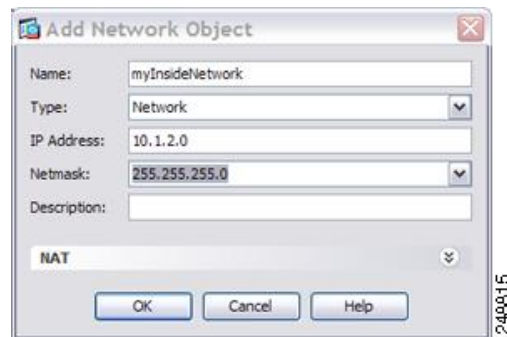


ステップ2 送信元インターフェイスおよび宛先インターフェイスを設定します。

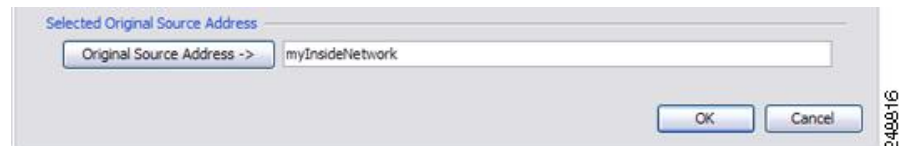


ステップ3 [Original Source Address] について、参照ボタンをクリックして、[Browse Original Source Address] ダイアログボックスで内部ネットワークの新しいネットワーク オブジェクトを追加します。

- a) [Add] > [Network Object] を選択します。
- b) 内部ネットワーク アドレスを定義し、[OK] をクリックします。



- c) 新しいネットワーク オブジェクトをダブルクリックで選択します。[OK] をクリックして、NAT コンフィギュレーションに戻ります。

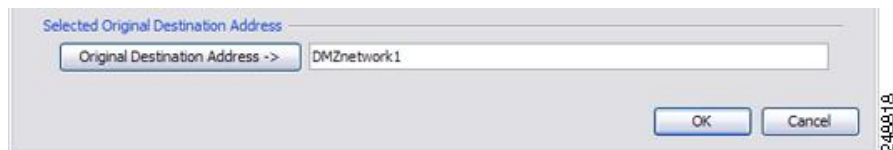


ステップ 4 [Original Destination Address] について、参照ボタンをクリックして、[Browse Original Destination Address] ダイアログボックスで DMZ ネットワーク 1 の新しいネットワーク オブジェクトを追加します。

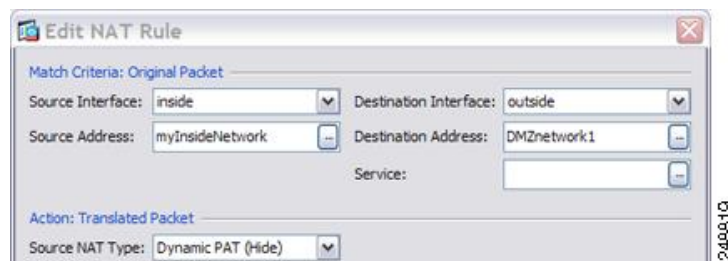
- a) [Add] > [Network Object] を選択します。
- b) DMZ ネットワーク 1 のアドレスを定義し、[OK] をクリックします。



- c) 新しいネットワーク オブジェクトをダブルクリックで選択します。[OK] をクリックして、NAT コンフィギュレーションに戻ります。



ステップ 5 NAT タイプを [Dynamic PAT (Hide)] に設定します。



ステップ 6 [Translated Source Address] について、参照ボタンをクリックして、[Browse Translated Source Address] ダイアログボックスで PAT アドレスの新しいネットワーク オブジェクトを追加します。

- a) [Add] > [Network Object] を選択します。
- b) PAT アドレスを定義し、[OK] をクリックします。

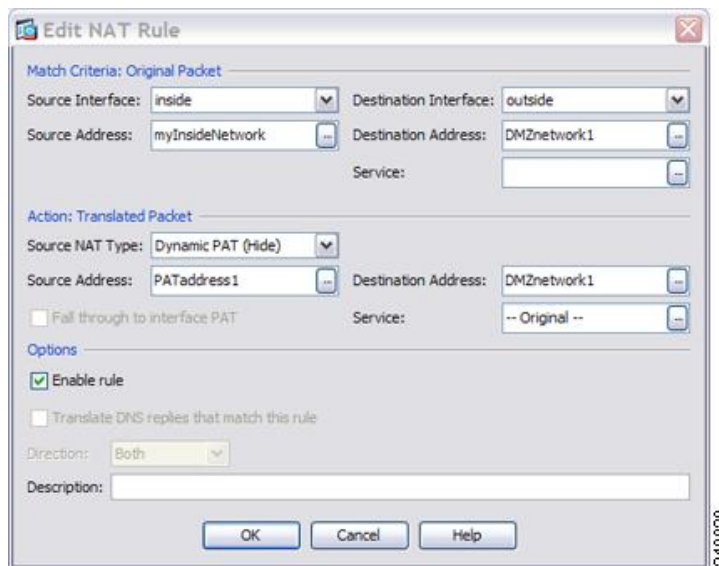


- c) 新しいネットワークオブジェクトをダブルクリックで選択します。[OK]をクリックして、NAT コンフィギュレーションに戻ります。



- ステップ 7** [Translated Destination Address] について、元の宛先アドレスの名前を入力するか (DMZnetwork1)、または参照ボタンをクリックして選択します。

宛先アドレスは変換しないため、元の宛先アドレスと変換された宛先アドレスに同じアドレスを指定することによって、アイデンティティ NAT を設定する必要があります。



- ステップ 8** [OK] をクリックして NAT テーブルにルールを追加します。

- ステップ 9** [Add] > [Add NAT Rule Before Network Object NAT Rules] または [Add NAT Rule After Network Object NAT Rules] をクリックしてトラフィックの NAT ルールを内部ネットワークから DMZ ネットワーク 2 に追加します。

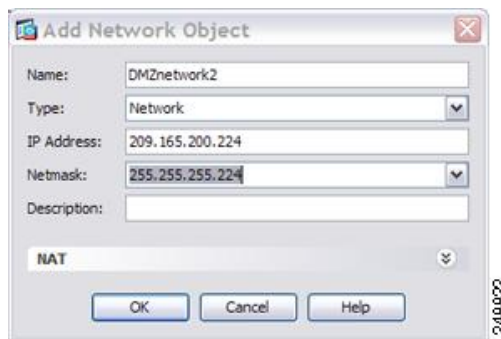
- ステップ 10** 送信元インターフェイスおよび宛先インターフェイスを設定します。



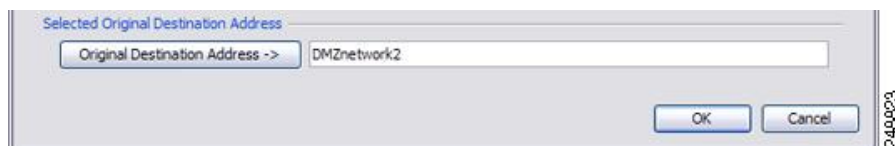
ステップ 11 [Original Source Address] について、内部ネットワーク オブジェクトの名前を入力するか (myInsideNetwork) 、または参照ボタンをクリックして選択します。

ステップ 12 [Original Destination Address] について、参照ボタンをクリックして、[Browse Original Destination Address] ダイアログボックスで DMZ ネットワーク 2 の新しいネットワーク オブジェクトを追加します。

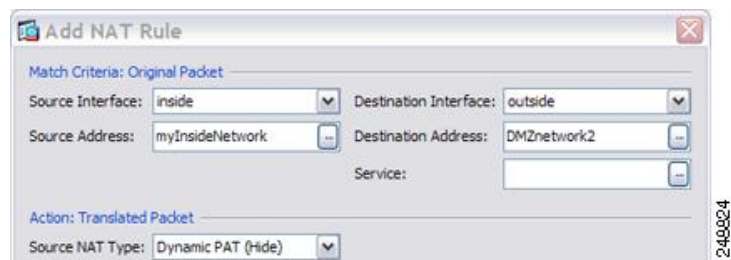
- a) [Add] > [Network Object] を選択します。
- b) DMZ ネットワーク 2 のアドレスを定義し、[OK] をクリックします。



- c) 新しいネットワーク オブジェクトをダブルクリックで選択します。[OK] をクリックして、NAT コンフィギュレーションに戻ります。

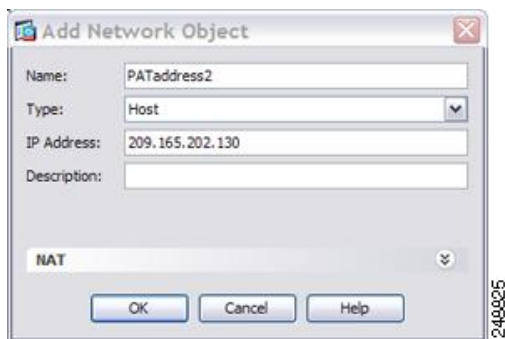


ステップ 13 NAT タイプを [Dynamic PAT (Hide)] に設定します。

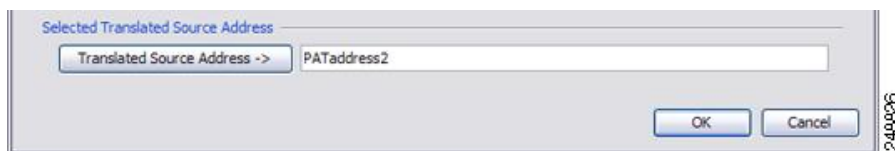


ステップ 14 [Translated Source Address] について、参照ボタンをクリックして、[Browse Translated Source Address] ダイアログボックスで PAT アドレスの新しいネットワーク オブジェクトを追加します。

- a) [Add] > [Network Object] を選択します。
- b) PAT アドレスを定義し、[OK] をクリックします。

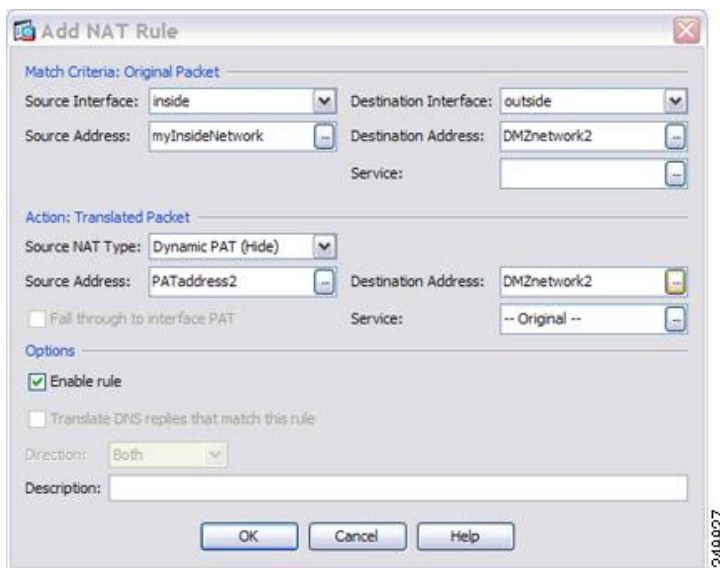


- c) 新しいネットワークオブジェクトをダブルクリックで選択します。[OK]をクリックして、NAT コンフィギュレーションに戻ります。



- ステップ 15** [Translated Destination Address] について、元の宛先アドレスの名前を入力するか (DMZnetwork2)、または参照ボタンをクリックして選択します。

宛先アドレスは変換しないため、元の宛先アドレスと変換された宛先アドレスに同じアドレスを指定することによって、アイデンティティ NAT を設定する必要があります。



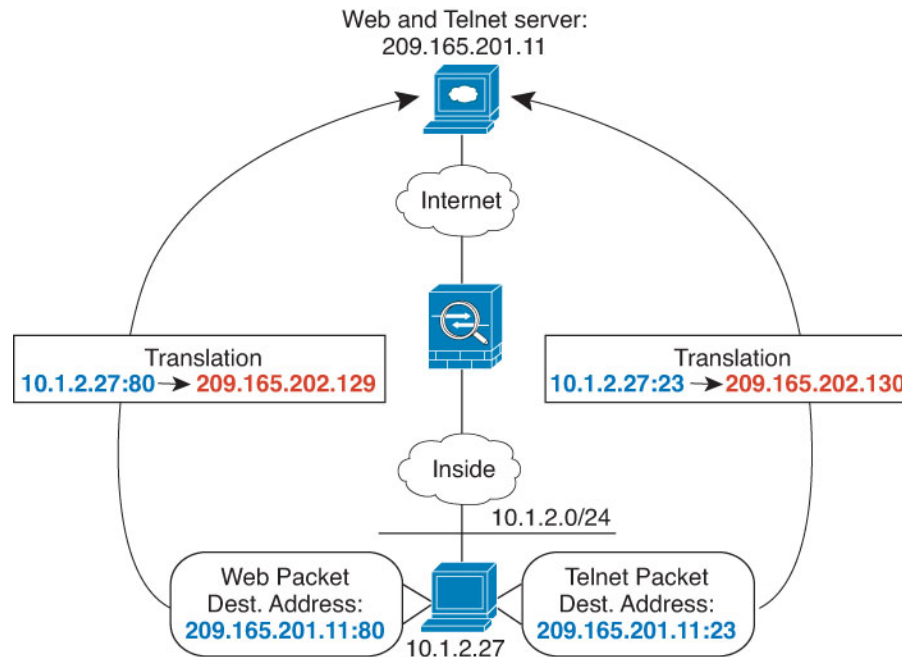
- ステップ 16** [OK] をクリックして NAT テーブルにルールを追加します。

- ステップ 17** [Apply] をクリックします。

宛先アドレスおよびポートに応じて異なる変換 (ダイナミック PAT)

次の図に、送信元ポートおよび宛先ポートの使用例を示します。10.1.2.0/24 ネットワークのホストは Web サービスと Telnet サービスの両方を提供する 1 つのホストにアクセスします。ホストが Telnet サービスを求めてサーバーにアクセスすると、実際のアドレスは 209.165.202.129:ポートに変換されます。ホストが Web サービスを求めて同じサーバーにアクセスすると、実際のアドレスは 209.165.202.130:ポートに変換されます。

図 6:異なる宛先ポートを使用する *Twice NAT*

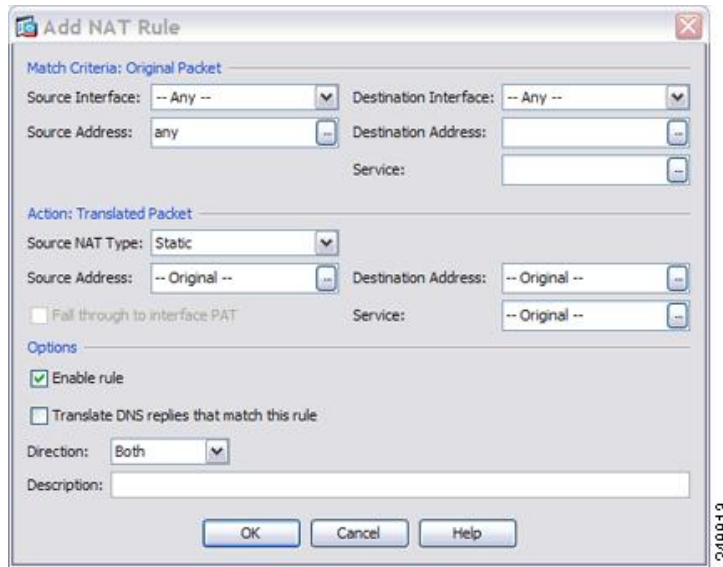


手順

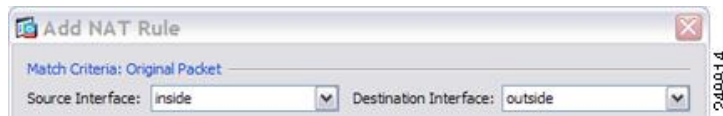
ステップ 1 [Configuration] > [Firewall] > [NAT Rules] ページで、[Add] > [Add NAT Rule Before Network Object NAT Rules] をクリックしてトラフィックの NAT ルールを内部ネットワークから Telnet サーバーに追加します。

NAT ルールをセクション 3 (ネットワーク オブジェクト NAT ルールの後) に追加する場合は、[Add NAT Rule After Network Object NAT Rules] を選択します。

[Add NAT Rule] ダイアログボックスが表示されます。

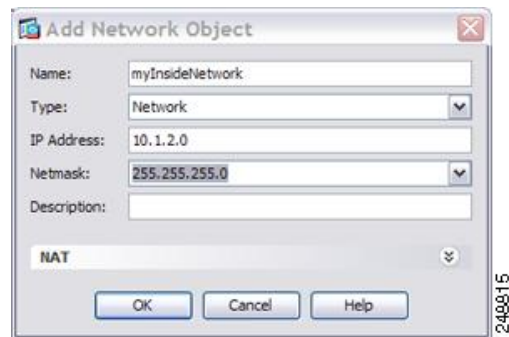


ステップ2 送信元インターフェイスおよび宛先インターフェイスを設定します。

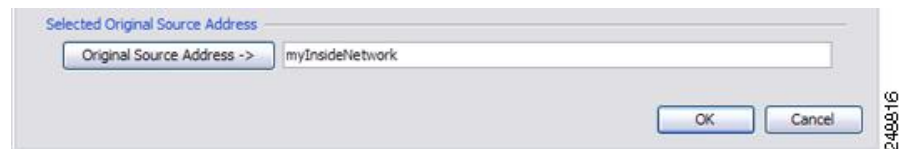


ステップ3 [Original Source Address] について、参照ボタンをクリックして、[Browse Original Source Address] ダイアログボックスで内部ネットワークの新しいネットワーク オブジェクトを追加します。

- a) [Add] > [Network Object] を選択します。
- b) 内部ネットワーク アドレスを定義し、[OK] をクリックします。



- c) 新しいネットワークオブジェクトをダブルクリックで選択します。[OK] をクリックして、NAT コンフィギュレーションに戻ります。

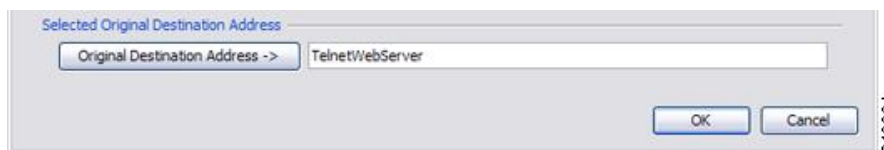


ステップ 4 [Original Destination Address] について、参照ボタンをクリックして、[Browse Original Destination Address] ダイアログボックスで Telnet/Web サーバーの新しいネットワーク オブジェクトを追加します。

- a) [Add] > [Network Object] を選択します。
- b) サーバー アドレスを定義し、[OK] をクリックします。



- c) 新しいネットワーク オブジェクトをダブルクリックで選択します。[OK] をクリックして、NAT コンフィギュレーションに戻ります。

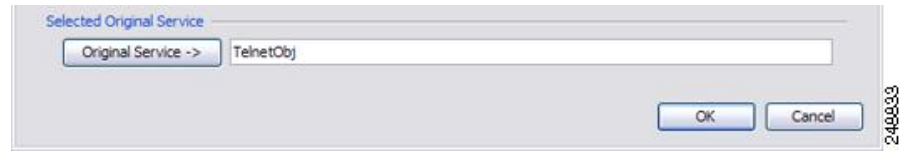


ステップ 5 [Original Service] について、参照ボタンをクリックして、[Browse Original Service] ダイアログボックスで Telnet の新しいサービス オブジェクトを追加します。

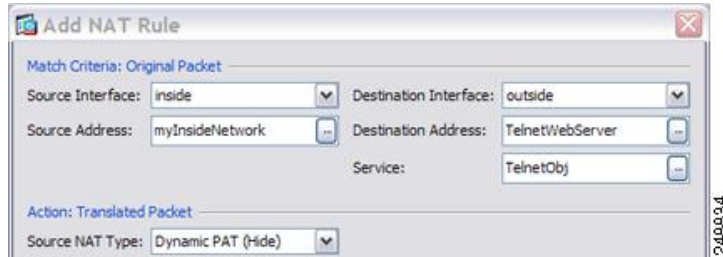
- a) [Add] > [Service Object] を選択します。
- b) プロトコルとポートを定義し、[OK] をクリックします。



- c) 新しいサービス オブジェクトをダブルクリックで選択します。[OK] をクリックして、NAT コンフィギュレーションに戻ります。

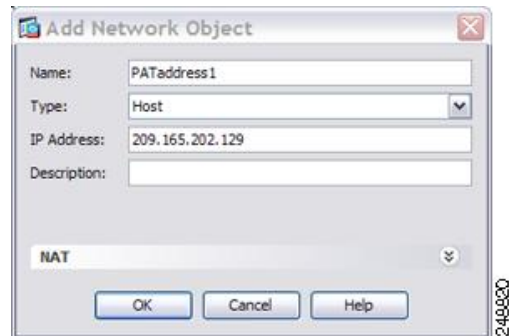


ステップ 6 NAT タイプを [Dynamic PAT (Hide)] に設定します。

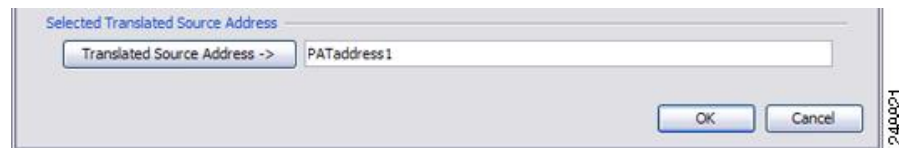


ステップ 7 [Translated Source Address] について、参照ボタンをクリックして、[Browse Translated Source Address] ダイアログボックスで PAT アドレスの新しいネットワーク オブジェクトを追加します。

- a) [Add] > [Network Object] を選択します。
- b) PAT アドレスを定義し、[OK] をクリックします。

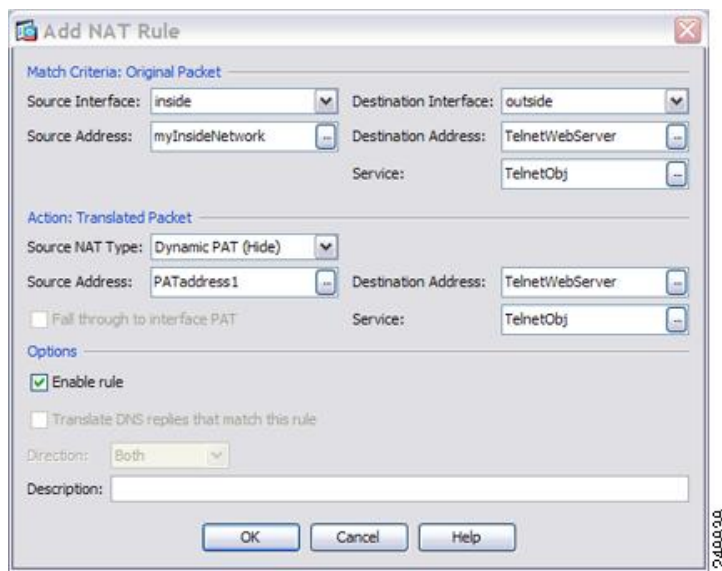


- c) 新しいネットワーク オブジェクトをダブルクリックで選択します。[OK] をクリックして、NAT コンフィギュレーションに戻ります。



ステップ 8 [Translated Destination Address] について、元の宛先アドレスの名前を入力するか (TelnetWebServer) 、または参照ボタンをクリックして選択します。

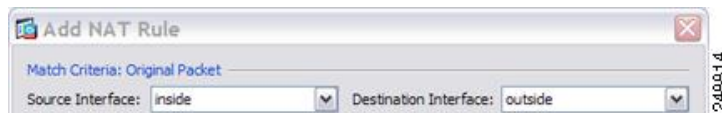
宛先アドレスは変換しないため、元の宛先アドレスと変換された宛先アドレスに同じアドレスを指定することによって、アイデンティティ NAT を設定する必要があります。



ステップ 9 [OK] をクリックして NAT テーブルにルールを追加します。

ステップ 10 [Add] > [Add NAT Rule Before Network Object NAT Rules] または [Add NAT Rule After Network Object NAT Rules] をクリックしてトラフィックの NAT ルールを内部ネットワークから Web サーバーに追加します。

ステップ 11 実際のインターフェイスおよびマッピング インターフェイスを設定します。

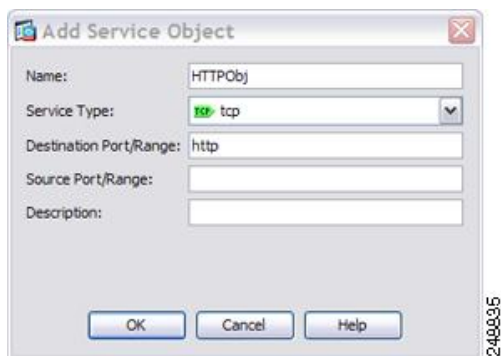


ステップ 12 [Original Source Address] について、内部ネットワーク オブジェクトの名前を入力するか (myInsideNetwork) 、または参照ボタンをクリックして選択します。

ステップ 13 [Original Destination Address] について、Telnet/Web サーバーのネットワーク オブジェクトの名前を入力するか (TelnetWebServer) 、または参照ボタンをクリックして選択します。

ステップ 14 [Original Service] について、参照ボタンをクリックして、[Browse Original Service] ダイアログボックスで HTTP の新しいサービス オブジェクトを追加します。

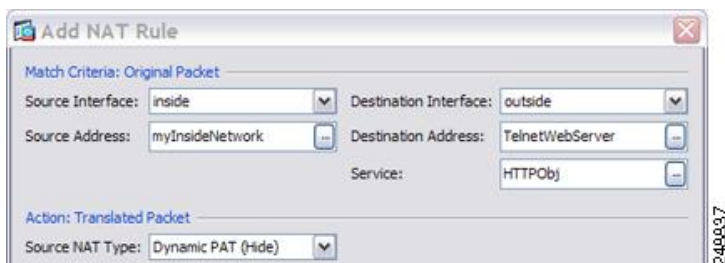
- a) [Add] > [Service Object] を選択します。
- b) プロトコルとポートを定義し、[OK] をクリックします。



- c) 新しいサービスオブジェクトをダブルクリックで選択します。[OK]をクリックして、NAT コンフィギュレーションに戻ります。

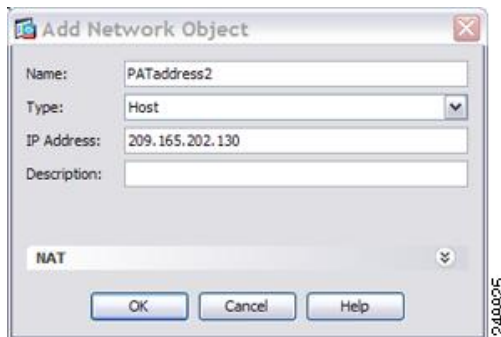


ステップ 15 NAT タイプを [Dynamic PAT (Hide)] に設定します。

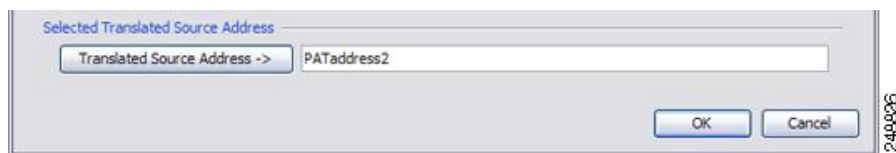


ステップ 16 [Translated Source Address] について、参照ボタンをクリックして、[Browse Translated Source Address] ダイアログボックスで PAT アドレスの新しいネットワーク オブジェクトを追加します。

- a) [Add] > [Network Object] を選択します。
b) PAT アドレスを定義し、[OK] をクリックします。

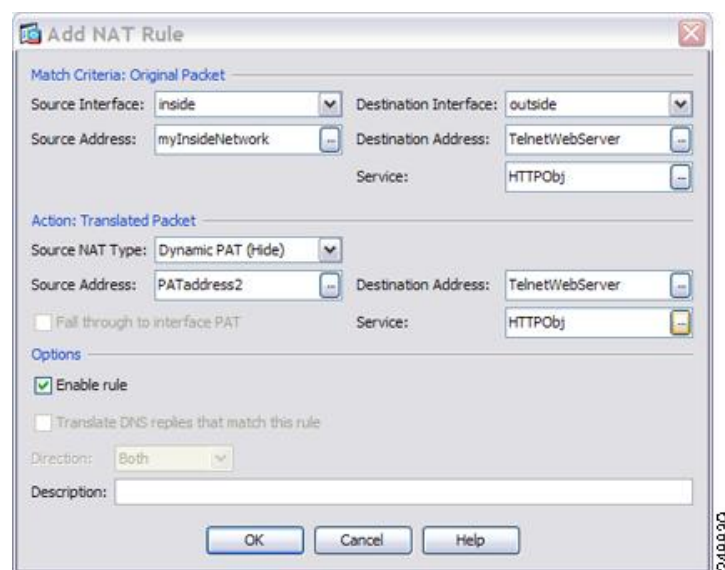


- c) 新しいネットワークオブジェクトをダブルクリックで選択します。[OK]をクリックして、NAT コンフィギュレーションに戻ります。



- ステップ 17** [Translated Destination Address] について、元の宛先アドレスの名前を入力するか (TelnetWebServer)、または参照ボタンをクリックして選択します。

宛先アドレスは変換しないため、元の宛先アドレスと変換された宛先アドレスに同じアドレスを指定することによって、アイデンティティ NAT を設定する必要があります。



- ステップ 18** [OK] をクリックして NAT テーブルにルールを追加します。

- ステップ 19** [Apply] をクリックします。

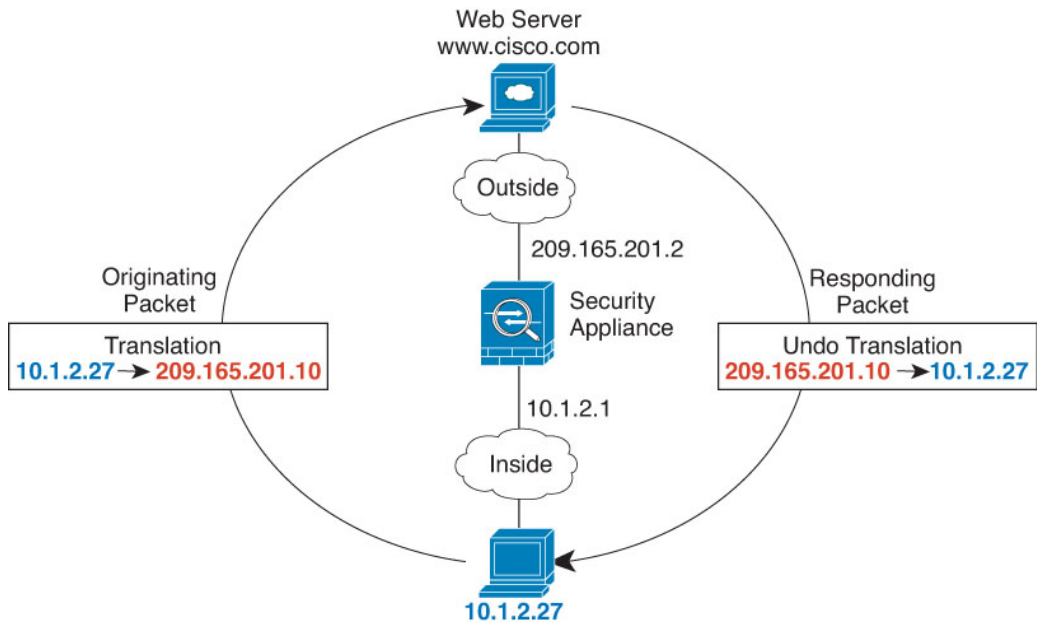
ルーテッドモードとトランスペアレントモードの NAT

NAT は、ルーテッドモードおよびトランスペアレントファイアウォールモードの両方に設定できます。次の項では、各ファイアウォールモードの一般的な使用方法について説明します。

ルーテッドモードの NAT

次の図は、内部にプライベートネットワークを持つ、ルーテッドモードの一般的な NAT の例を示しています。

図 7: NAT の例：ルーテッドモード



1. 内部ホスト 10.1.2.27 が Web サーバにパケットを送信すると、パケットの実際の送信元アドレス 10.1.2.27 はマッピングアドレス 209.165.201.10 に変換されます。
2. サーバが応答すると、マッピングアドレス 209.165.201.10 に応答を送信し、ASA がそのパケットを受信します。これは、ASA がプロキシ ARP を実行してパケットを要求するためです。
3. ASA はその後、パケットをホストに送信する前に、マッピングアドレス 209.165.201.10 を変換し、実際のアドレス 10.1.2.27 に戻します。

トランスペアレントモードまたはブリッジグループ内の NAT

NAT をトランスペアレントモードで使用すると、ネットワークで NAT を実行するためのアップストリームルータまたはダウンストリームルータがなくなります。これによりルーテッドモードでブリッジグループ内で同様の機能を実行できます。

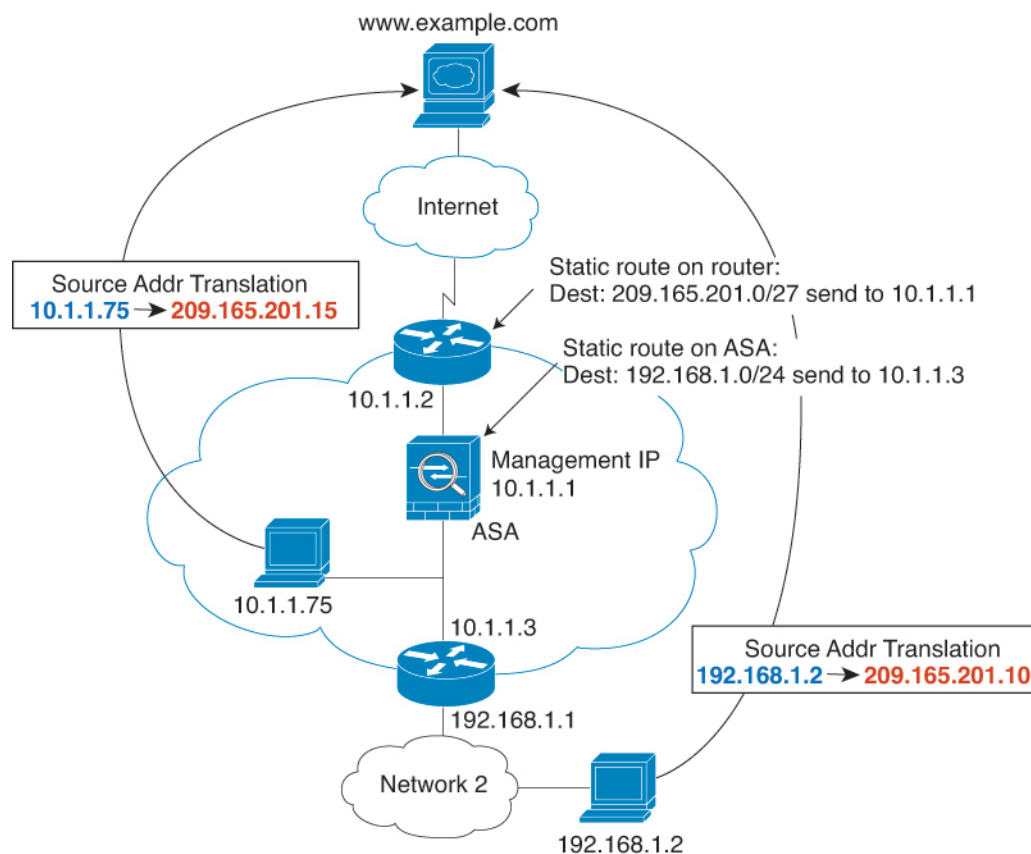
トランスペアレントモードまたは同じブリッジグループのメンバー間のルーテッドモードの NAT には、以下の要件および制限があります。

- インターフェイスに接続されている IP アドレスがないため、マッピングされたアドレスがブリッジグループメンバーのインターフェイスである場合、インターフェイス PAT を設定することはできません。
- ARP インスペクションはサポートされていません。また、何らかの理由で、一方の ASA のホストがもう一方の ASA のホストに ARP 要求を送信し、開始ホストの実際のアドレスが同じサブネットの別のアドレスにマッピングされる場合、実際のアドレスは ARP 要求で可視のままになります。

- IPv4 および IPv6 ネットワークの間の変換はサポートされていません。2つの IPv6 ネットワーク間、または2つの IPv4 ネットワーク間の変換がサポートされます。

次の図に、インターフェイス内部と外部に同じネットワークを持つ、トランスパアレントモードの一般的な NAT のシナリオを示します。このシナリオのトランスパアレントファイアウォールは NAT サービスを実行しているため、アップストリーム ルータは NAT を実行する必要がありません。

図 8: NAT の例 : トランスパアレントモード



1. 内部ホスト 10.1.1.75 が Web サーバーにパケットを送信すると、パケットの実際の送信元アドレス 10.1.1.75 はマッピングアドレス 209.165.201.15 に変更されます。
2. サーバが応答すると、マッピングアドレス 209.165.201.15 に応答を送信し、ASA がそのパケットを受信します。これは、アップストリーム ルータには、ASA の管理 IP アドレスに転送されるスタティックルートがこのマッピングネットワークが含まれるためです。
3. その後、ASA はマッピングアドレス 209.165.201.15 を変換して実際のアドレス 10.1.1.75 に戻します。実際のアドレスは直接接続されているため、ASA はそのアドレスを直接ホストに送信します。

4. ホスト 192.168.1.2 の場合も、リターントラフィックを除き、同じプロセスが発生します。ASA はルーティングテーブルでルートを検索し、192.168.1.0/24 の ASA スタティックルートに基づいてパケットを 10.1.1.3 にあるダウンストリーム ルータに送信します。

NAT パケットのルーティング

ASA は、マッピングアドレスに送信されるパケットの宛先である必要があります。ASA は、マッピングアドレス宛てに送信されるすべての受信パケットの出力インターフェイスを決定する必要があります。この項では、ASA が NAT を使用してパケットの受信および送信を処理する方法について説明します。

マッピングアドレスとルーティング

実際のアドレスをマッピングアドレスに変換する場合は、選択したマッピングアドレスによって、マッピングアドレスのルーティング（必要な場合）を設定する方法が決定されます。

マッピング IP アドレスに関するその他のガイドラインについては、[NAT のその他のガイドライン](#)を参照してください。

次のトピックでは、マッピングアドレスのタイプについて説明します。

マッピング インターフェイスと同じネットワーク上のアドレス

宛先（マッピング）インターフェイスと同じネットワーク上のアドレスを使用する場合、ASA はプロキシ ARP を使用してマッピングアドレスの ARP 要求に応答し、マッピングアドレス宛てのトラフィックを代行受信します。この方法では、ASA がその他のネットワークのゲートウェイである必要がないため、ルーティングが簡略化されます。このソリューションは、外部ネットワークに十分な数のフリーアドレスが含まれている場合に最も適しており、ダイナミック NAT またはスタティック NAT などの 1:1 変換を使用している場合は考慮が必要です。ダイナミック PAT ではアドレス数が少なくても使用できる変換の数が大幅に拡張されるため、外部ネットワークで使用できるアドレスが少ししかない場合でも、この方法を使用できます。PAT では、マッピングインターフェイスの IP アドレスも使用できます。



- (注) マッピング インターフェイスを任意のインターフェイスとして設定し、マッピング インターフェイスの1つとして同じネットワーク上のマッピングアドレスを指定すると、そのマッピングアドレスの ARP 要求を別のインターフェイスで受信する場合、入力インターフェイスでそのネットワークの ARP エントリを手動で設定し、その MAC アドレスを指定する必要があります。通常、マッピング インターフェイスに任意のインターフェイスを指定して、マッピングアドレスの固有のネットワークを使用すると、この状況は発生しません。[設定 (Configuration)] > [デバイス管理 (Device Management)] > [詳細 (Advanced)] > [ARP] > [ARP スタティックテーブル (ARP Static Table)] の順に選択し、ARP を設定します。

一意のネットワーク上のアドレス

宛先（マッピング）インターフェイスのネットワーク上で使用可能な数より多くのアドレスが必要な場合は、別のサブネット上でアドレスを指定できます。アップストリームルータには、ASA を指しているマッピングアドレスのスタティック ルートが必要です。

また、ルーテッドモードの場合、宛先ネットワーク上の IP アドレスをゲートウェイとして使用して、マッピングアドレスの ASA にスタティックルートを設定し、ルーティングプロトコルを使用してルートを再配布することができます。たとえば、内部ネットワーク（10.1.1.0/24）には NAT を使用して、マッピング IP アドレス 209.165.201.5 を使用する場合、209.165.201.5 255.255.255.255（ホストアドレス）に対して、10.1.1.99 ゲートウェイへのスタティックルートを設定し、これを再配布できます。

```
route inside 209.165.201.5 255.255.255.255 10.1.1.99
```

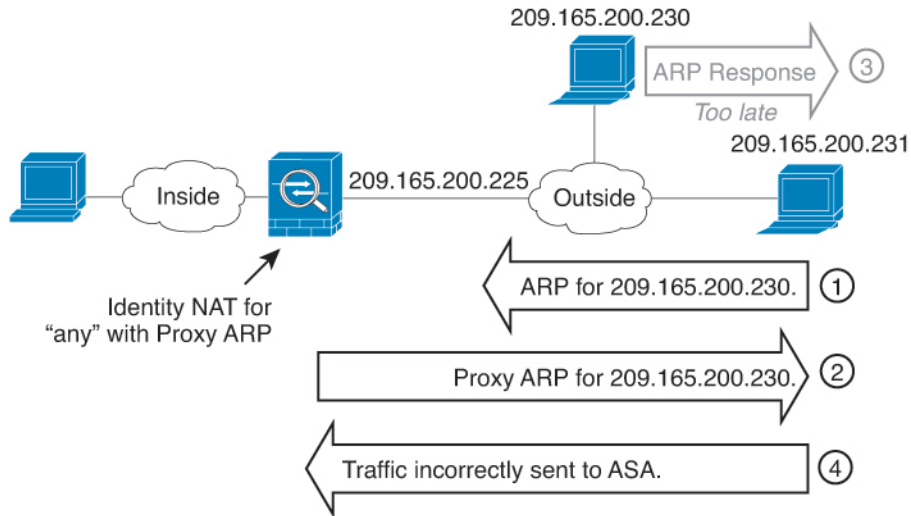
トランスペアレントモードの場合は、実際のホストが直接接続されている場合は、ASA をポイントするようにアップストリームルータのスタティックルートを設定します。8.3 では、グローバルな管理 IP アドレスを指定します。8.4(1) 以降では、ブリッジグループの IP アドレスを指定します。トランスペアレントモードのリモートホストの場合は、上流に位置するルータのスタティックルートで、代わりに下流ルータの IP アドレスを指定できます。

実際のアドレスと同じアドレス（アイデンティティ NAT）

アイデンティティ NAT のデフォルト動作で、プロキシ ARP は有効になっており、他の静的 NAT ルールと一致します。必要に応じてプロキシ ARP を無効にできます。必要に応じて標準スタティック NAT のプロキシ ARP を無効にできます。その場合は、アップストリームルータに適切なルートがあることを確認する必要があります。

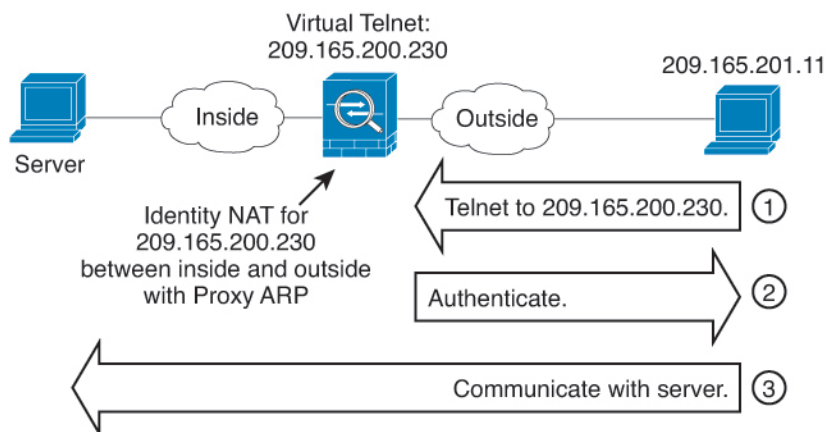
アイデンティティ NAT の場合、通常はプロキシ ARP は不要です。場合によっては接続の問題が生じることがあります。たとえば、「任意」の IP アドレスの広範なアイデンティティ NAT ルールを設定した場合、プロキシ ARP を有効のままにしておくと、マッピングインターフェイスに直接接続されたネットワーク上のホストの問題を引き起こすことがあります。この場合、マッピングネットワークのホストが同じネットワークの他のホストと通信すると、ARP 要求内のアドレスは（「任意」のアドレスと一致する）NAT ルールと一致します。このとき、実際には ASA 向けのパケットでない場合でも、ASA はこのアドレスの ARP をプロキシします（この問題は、twice NAT ルールが設定されている場合にも発生します。NAT ルールは送信元と宛先のアドレス両方に一致する必要がありますが、プロキシ ARP 判定は「送信元」アドレスに対してのみ行われます）。実際のホストの ARP 応答の前に ASA の ARP 応答を受信した場合、トラフィックは誤って ASA に送信されます。

図 9: アイデンティティ NAT に関するプロキシ ARP の問題



まれに、アイデンティティ NAT に対してプロキシ ARP が必要になります (仮想 Telnet など)。AAA をネットワーク アクセスに使用すると、ホストは、その他のトラフィックが通過する前に、Telnet などのサービスを使用して ASA に対して認証する必要があります。必要なログインを提供するために、ASA に仮想 Telnet サーバを設定できます。外部から仮想 Telnet アドレスにアクセスする場合は、プロキシ ARP 機能専用アドレスのアイデンティティ NAT ルールを設定する必要があります。仮想 Telnet の内部プロセスにより、プロキシ ARP では ASA は NAT ルールに応じて送信元インターフェイスからトラフィックを送信するのではなく、仮想 Telnet アドレス宛てのトラフィックを保持できます (次の図を参照してください)。

図 10: プロキシ ARP と仮想 Telnet



リモート ネットワークのトランスペアレント モードのルーティング要件

トランスペアレント モードで NAT を使用する場合、一部のタイプのトラフィックには、スタティックルートが必要になります。詳細については、一般的な操作の設定ガイドを参照してください。

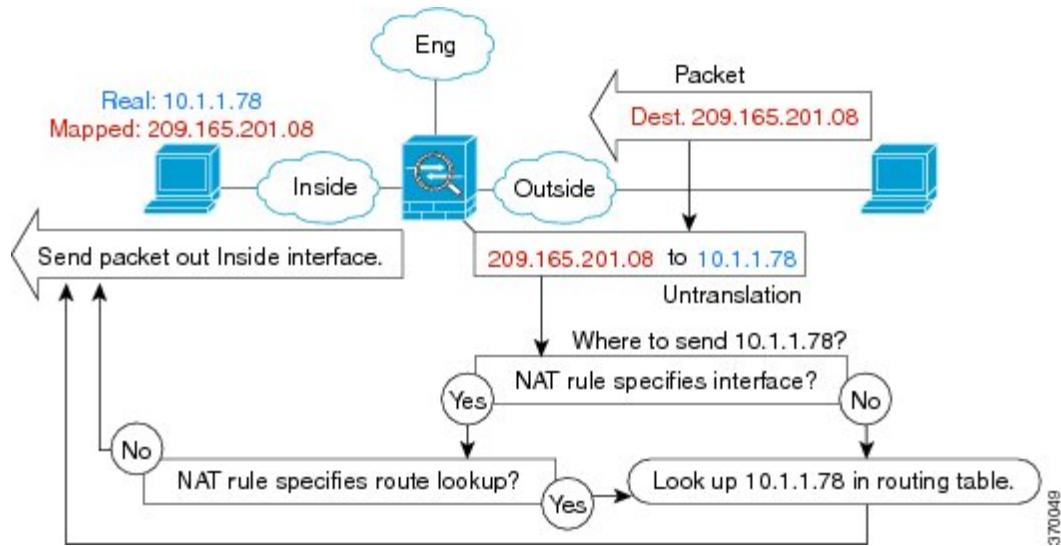
出インターフェイスの決定

NAT を使用していて、ASA がマッピング アドレスのトラフィックを受信する場合、ASA は NAT ルールに従って宛先アドレスを逆変換し、実際のアドレスにパケットを送信します。ASA は、次の方法でパケットの出インターフェイスを決定します。

- トランスペアレント モードまたはルーテッドモードのブリッジグループ インターフェイス：ASA は NAT ルールを使用して実際のアドレスの出インターフェイスを決定します。NAT ルールの一部として送信元、宛先のブリッジグループ メンバー インターフェイスを指定する必要があります。
- ルーテッドモードの通常インターフェイス：ASA は、次のいずれかの方法で出インターフェイスを決定します。
 - NAT ルールでインターフェイスを設定する：ASA は NAT ルールを使用して出インターフェイスを決定します。(8.3(1) ~ 8.4(1)) 唯一の例外はアイデンティティ NAT です。アイデンティティ NAT では、NAT コンフィギュレーションに関係なく、常にルート ルックアップが使用されます。(8.4 (2) 以降) アイデンティティ NAT の場合、デフォルト動作は NAT の設定を使用することです。ただし、代わりにオプションとして常にルート ルックアップを使用することもできます。一部のシナリオでは、ルート ルックアップの上書きが必要になる場合があります。
 - NAT ルールでインターフェイスを設定しない：ASA はルート ルックアップを使用して出インターフェイスを決定します。

次の図に、ルーテッドモードでの出インターフェイスの選択方法を示します。ほとんどの場合、ルート ルックアップは NAT ルールのインターフェイスと同じです。ただし、一部の構成では、2つの方法が異なる場合があります。

図 11: NATによるルーテッドモードでの出インターフェイスの選択



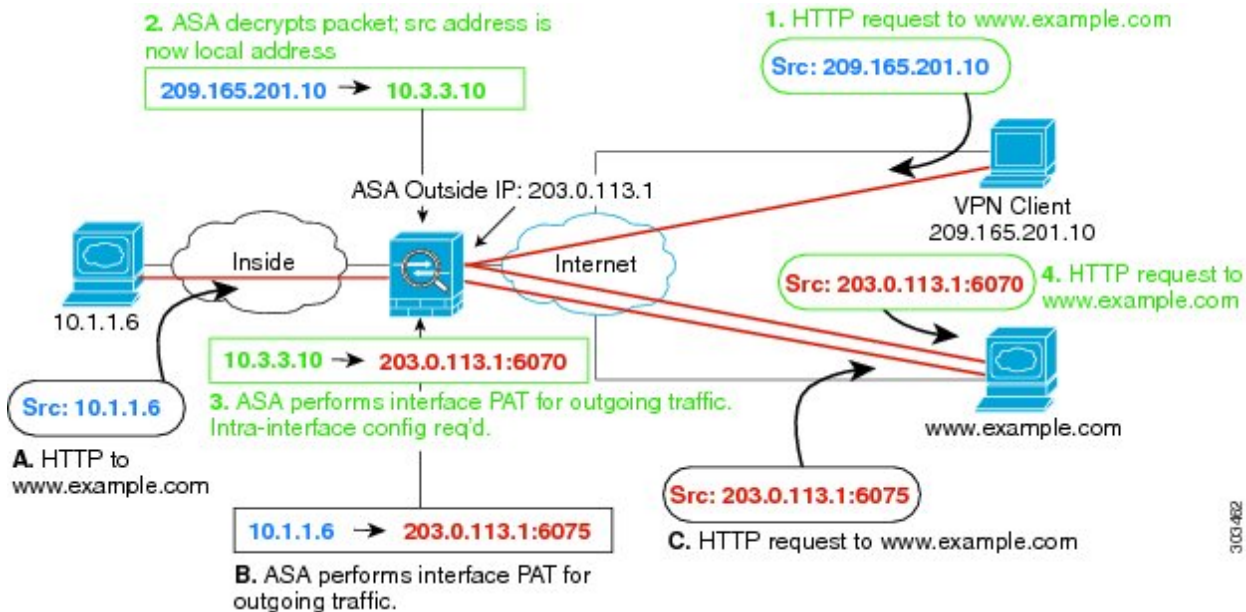
VPN の NAT

次のトピックでは、さまざまなタイプの VPN を用いた NAT の使用例について説明します。

NAT とリモート アクセス VPN

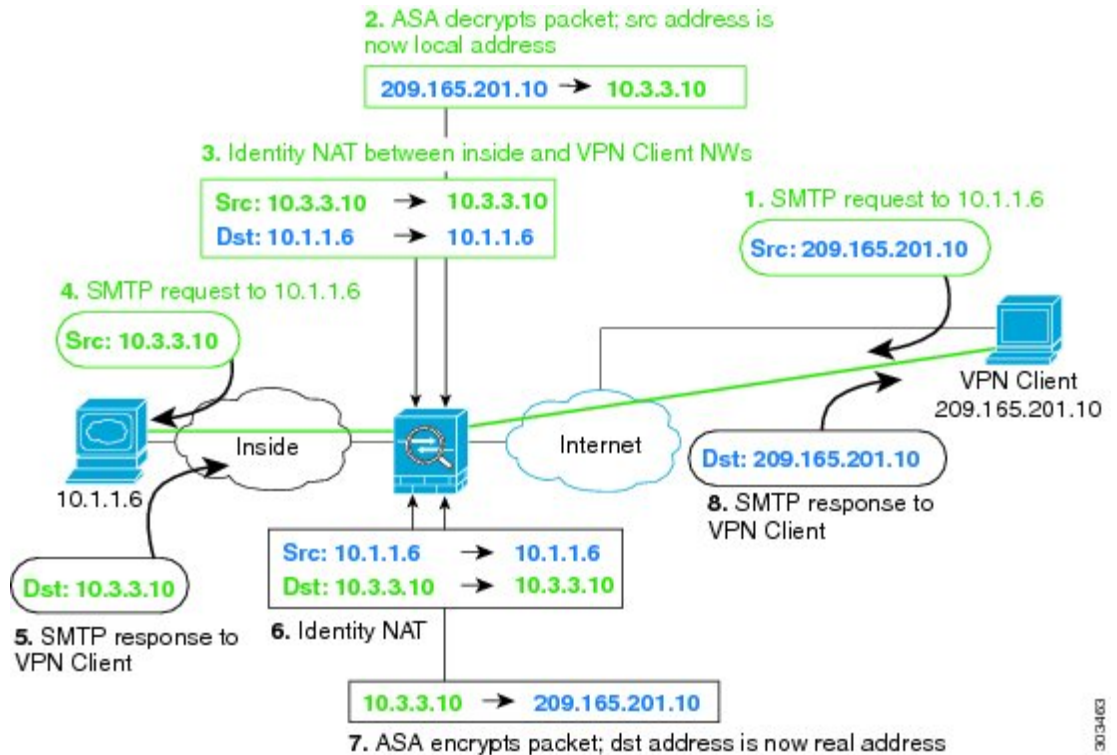
次の図に、内部サーバー（10.1.1.6）とインターネットにアクセスする VPN クライアント（209.165.201.10）の両方を示します。VPN クライアント用のスプリットトンネリング（指定したトラフィックのみが VPN トンネル上でやりとりされる）を設定しない限り、インターネットバインドされた VPN トラフィックも ASA を経由する必要があります。VPN トラフィックが ASA に渡されると、ASA はパケットを復号化し、得られたパケットには送信元として VPN クライアントローカルアドレス（10.3.3.10）が含まれています。内部ネットワークと VPN クライアントローカルネットワークの両方で、インターネットにアクセスするために NAT によって提供されるパブリック IP アドレスが必要です。次の例では、インターフェイス PAT ルールを使用しています。VPN トラフィックが、入ってきたインターフェイスと同じインターフェイスから出て行けるようにするには、インターフェイス内通信（別名「ヘアピンネットワーク」）をイネーブルにする必要があります。

図 12: インターネット宛 VPN トラフィックのインターフェイス PAT (インターフェイス内)



次の図に、内部のメールサーバーにアクセスする VPN クライアントを示します。ASA は、内部ネットワークと外部ネットワークの間のトラフィックが、インターネットアクセス用に設定したインターフェイス PAT ルールに一致することを期待するので、VPN クライアント (10.3.3.10) から SMTP サーバー (10.1.1.6) へのトラフィックは、リバースパス障害が原因で廃棄されます。10.3.3.10 から 10.1.1.6 へのトラフィックは、NAT ルールに一致しませんが、10.1.1.6 から 10.3.3.10 へのリターントラフィックは、送信トラフィックのインターフェイス PAT ルールに一致する必要があります。順方向および逆方向のフローが一致しないため、ASA は受信時にパケットをドロップします。この障害を回避するには、それらのネットワーク間のアイデンティティ NAT ルールを使用して、インターフェイス PAT ルールから VPN クライアント内部のトラフィックを除外する必要があります。アイデンティティ NAT は同じアドレスに変換します。

図 13: VPN クライアントのアイデンティティ NAT



303463

上記のネットワークのための次のサンプル NAT の設定を参照してください。

```
! Enable hairpin for non-split-tunneled VPN client traffic:
same-security-traffic permit intra-interface
```

```
! Identify local VPN network, & perform object interface PAT when going to Internet:
object network vpn_local
subnet 10.3.3.0 255.255.255.0
nat (outside,outside) dynamic interface
```

```
! Identify inside network, & perform object interface PAT when going to Internet:
object network inside_nw
subnet 10.1.1.0 255.255.255.0
nat (inside,outside) dynamic interface
```

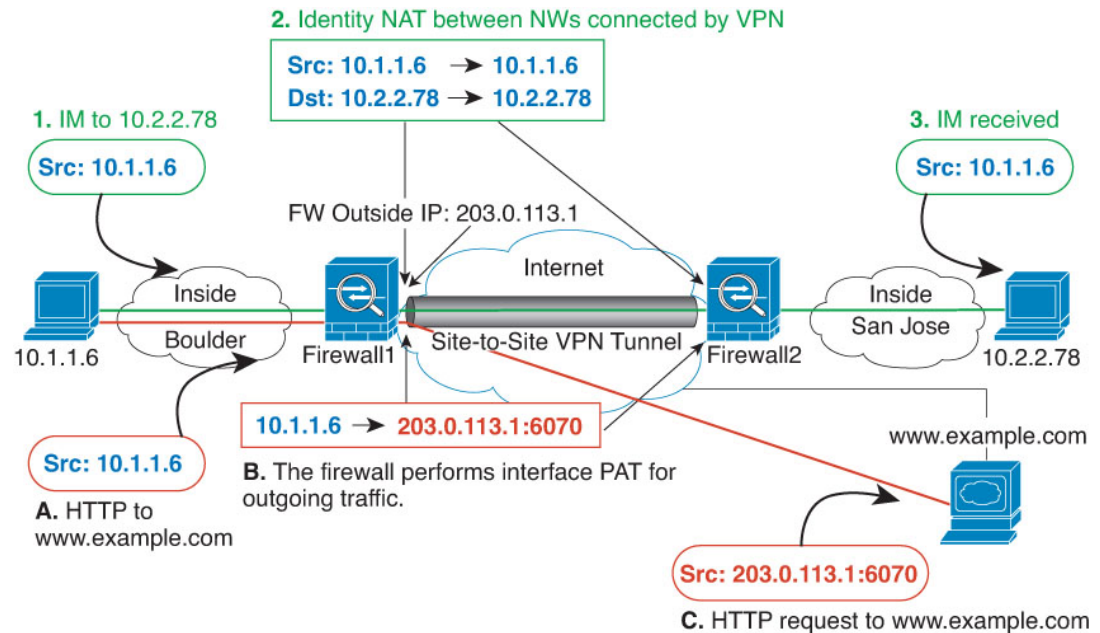
```
! Use twice NAT to pass traffic between the inside network and the VPN client without
! address translation (identity NAT):
nat (inside,outside) source static inside_nw inside_nw destination static vpn_local
vpn_local
```

NAT およびサイト間 VPN

次の図に、ボールダーとサンノゼのオフィスを接続するサイトツーサイト トンネルを示します。インターネットに渡すトラフィックについて（たとえばボールダーの 10.1.1.6 から www.example.com へ）、インターネットへのアクセスのために NAT によって提供されるパブリック IP アドレスが必要です。次の例では、インターフェイス PAT ルールを使用しています。

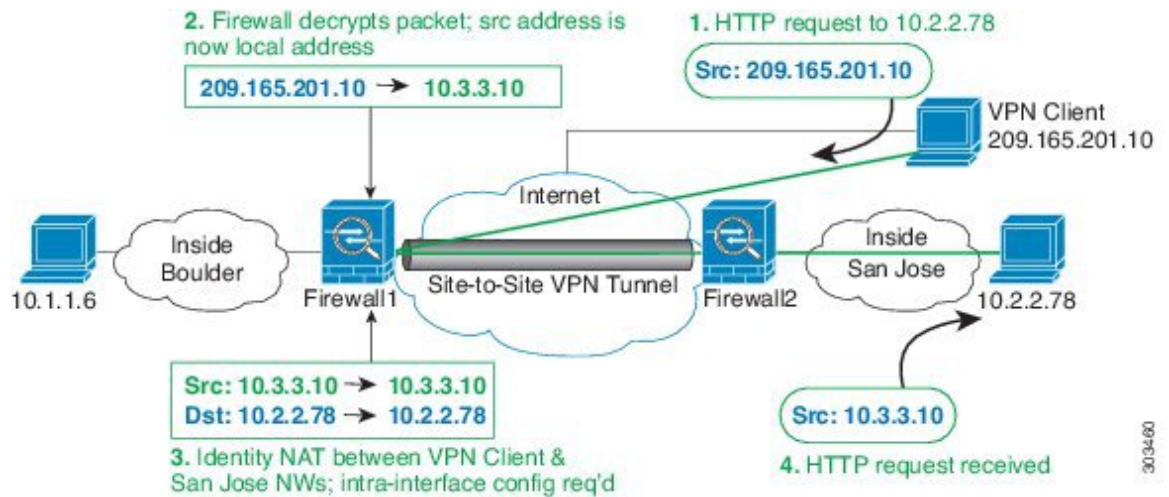
す。ただし、VPN トンネルを経由するトラフィックについては（たとえば、ボールドーの 10.1.1.6 からサンノゼの 10.2.2.78 へ）、NAT を実行しません。そのため、アイデンティティ NAT ルールを作成して、そのトラフィックを除外する必要があります。アイデンティティ NAT は同じアドレスにアドレスを変換します。

図 14: サイトツーサイト VPN のためのインターフェイス PAT およびアイデンティティ NAT



次の図に、Firewall1（ボールドー）に接続する VPN クライアントと、Firewall1 と Firewall2（サンノゼ）間のサイトツーサイト トンネル上でアクセス可能なサーバー（10.2.2.78）に対する Telnet 要求を示します。これはヘアピン接続であるため、VPN クライアントからの非スプリットトンネルのインターネット宛トラフィックにも必要な、インターフェイス内通信を有効化する必要があります。発信 NAT ルールからこのトラフィックを除外するため、VPN に接続された各ネットワーク間で行うのと同様に、VPN クライアントとボールドーおよびサンノゼのネットワーク間でアイデンティティ NAT を設定する必要があります。

図 15: サイトツーサイト VPN への VPN クライアント アクセス



2 番目の例の Firewall1 (ボールダー) については、次の NAT の設定例を参照してください。

```
! Enable hairpin for VPN client traffic:
same-security-traffic permit intra-interface

! Identify local VPN network, & perform object interface PAT when going to Internet:
object network vpn_local
subnet 10.3.3.0 255.255.255.0
nat (outside,outside) dynamic interface

! Identify inside Boulder network, & perform object interface PAT when going to Internet:
object network boulder_inside
subnet 10.1.1.0 255.255.255.0
nat (inside,outside) dynamic interface

! Identify inside San Jose network for use in twice NAT rule:
object network sanjose_inside
subnet 10.2.2.0 255.255.255.0

! Use twice NAT to pass traffic between the Boulder network and the VPN client without
! address translation (identity NAT):
nat (inside,outside) source static boulder_inside boulder_inside
destination static vpn_local vpn_local

! Use twice NAT to pass traffic between the Boulder network and San Jose without
! address translation (identity NAT):
nat (inside,outside) source static boulder_inside boulder_inside
destination static sanjose_inside sanjose_inside

! Use twice NAT to pass traffic between the VPN client and San Jose without
! address translation (identity NAT):
nat (outside,outside) source static vpn_local vpn_local
destination static sanjose_inside sanjose_inside
```

Firewall2 (サンノゼ) については、次の NAT の設定例を参照してください。

```
! Identify inside San Jose network, & perform object interface PAT when going to Internet:
object network sanjose_inside
```

```
subnet 10.2.2.0 255.255.255.0
nat (inside,outside) dynamic interface

! Identify inside Boulder network for use in twice NAT rule:
object network boulder_inside
subnet 10.1.1.0 255.255.255.0

! Identify local VPN network for use in twice NAT rule:
object network vpn_local
subnet 10.3.3.0 255.255.255.0

! Use twice NAT to pass traffic between the San Jose network and Boulder without
! address translation (identity NAT):
nat (inside,outside) source static sanjose_inside sanjose_inside
destination static boulder_inside boulder_inside

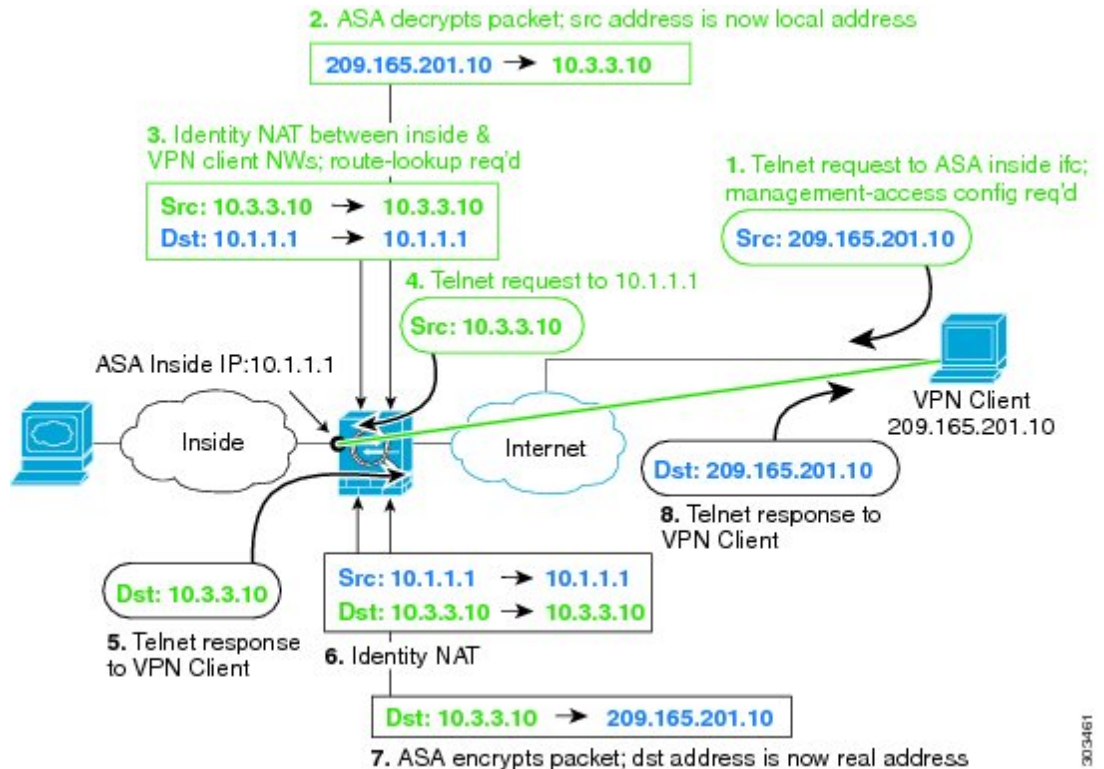
! Use twice NAT to pass traffic between the San Jose network and the VPN client without
! address translation (identity NAT):
nat (inside,outside) source static sanjose_inside sanjose_inside
destination static vpn_local vpn_local
```

NAT および VPN 管理アクセス

VPN を使用する場合、ASA を開始したインターフェイス以外のインターフェイスへの管理アクセスを許可することができます。たとえば、外部インターフェイスから ASA を開始する場合、管理アクセス機能では、ASDM、SSH、Telnet、または SNMP を使用して内部インターフェイスに接続することが可能です。または、内部インターフェイスに ping を実行できます。

次の図に、ASA の内部インターフェイスに Telnet 接続する VPN クライアントを示します。管理アクセスインターフェイスを使用し、[NAT とリモートアクセス VPN \(35 ページ\)](#) または [NAT およびサイト間 VPN \(37 ページ\)](#) に従ってアイデンティティ NAT を設定する場合、ルートルックアップ オプションを使用して NAT を設定する必要があります。ルートルックアップがない場合、ASA は、ルーティングテーブルの内容に関係なく、NAT コマンドで指定されたインターフェイスからトラフィックを送信します。次の例では、出力インターフェイスは内部インターフェイスです。ASA で、内部ネットワークに管理トラフィックを送信しません。これは、内部インターフェイスの IP アドレスには戻りません。ルートルックアップ オプションを使用すると、ASA は、内部ネットワークの代わりに内部インターフェイスの IP アドレスに直接トラフィックを送信できます。VPN クライアントから内部ネットワーク上のホストへのトラフィックの場合、ルートルックアップ オプションがあっても正しい出力インターフェイス (内部) になるため、通常のトラフィックフローは影響を受けません。ルートルックアップ オプションの詳細については、[出力インターフェイスの決定 \(34 ページ\)](#) を参照してください。

図 16: VPN 管理アクセス



303461

上記のネットワークのための次のサンプル NAT の設定を参照してください。

```
! Enable hairpin for non-split-tunneled VPN client traffic:
same-security-traffic permit intra-interface
```

```
! Enable management access on inside ifc:
management-access inside
```

```
! Identify local VPN network, & perform object interface PAT when going to Internet:
object network vpn_local
subnet 10.3.3.0 255.255.255.0
nat (outside,outside) dynamic interface
```

```
! Identify inside network, & perform object interface PAT when going to Internet:
object network inside_nw
subnet 10.1.1.0 255.255.255.0
nat (inside,outside) dynamic interface
```

```
! Use twice NAT to pass traffic between the inside network and the VPN client without
! address translation (identity NAT), w/route-lookup:
nat (outside,inside) source static vpn_local vpn_local
destination static inside_nw inside_nw route-lookup
```

NAT と VPN のトラブルシューティング

VPN を使用した NAT の問題をトラブルシューティングするためには、次の監視ツールを参照してください。

- パケット トレーサ：正しく使用した場合、パケット トレーサは、パケットが該当している NAT ルールを表示します。
- **show nat detail**：特定の NAT ルールのヒットカウントおよび変換解除されたトラフィックを表示します。
- **show conn all**：ボックストラフィックとの間の接続を含むアクティブ接続を表示します。

動作に関係のない設定と動作するための設定をよく理解するには、次の手順を実行します。

1. アイデンティティ NAT を使用しない VPN を設定します。
2. **show nat detail** と **show conn all** を入力します。
3. アイデンティティ NAT の設定を追加します。
4. **show nat detail** と **show conn all** を繰り返します。

IPv6 ネットワークの変換

IPv6 専用ネットワークと IPv4 専用ネットワークの間でトラフィックを通過させる必要がある場合、NAT を使用してアドレス タイプを変換する必要があります。2つの IPv6 ネットワークの場合でも、外部ネットワークから内部アドレスを隠す必要がある場合があります。

IPv6 ネットワークでは次の変換タイプを使用できます。

- NAT64、NAT46：IPv6 パケットを IPv4（およびその反対）に変換します。2つのポリシーを定義する必要があります。1つは IPv6 から IPv4 への変換用、もう1つは IPv4 から IPv6 への変換用です。これは、1つの twice NAT ルールで実行できますが、DNS サーバーが外部ネットワーク上にある場合、DNS 応答をリライトする必要があります。宛先を指定するときに twice NAT ルールで DNS リライトを有効にすることができないため、2つの Network Object NAT ルールを作成することがより適切なソリューションです。



(注) NAT46がサポートするのは、スタティックマッピングのみです。

- NAT66：IPv6 パケットを別の IPv6 アドレスに変換します。スタティック NAT の使用を推奨します。ダイナミック NAT または PAT を使用できますが、IPv6 アドレスは大量にあるため、ダイナミック NAT を使用する必要はありません。



(注) NAT64 および NAT 46 は、標準的なルーテッドインターフェイスでのみ使用できます。NAT66 は、ルーテッドインターフェイスとブリッジグループメンバーインターフェイスの両方で使用できます。

NAT64/46 : IPv6 アドレスの IPv4 への変換

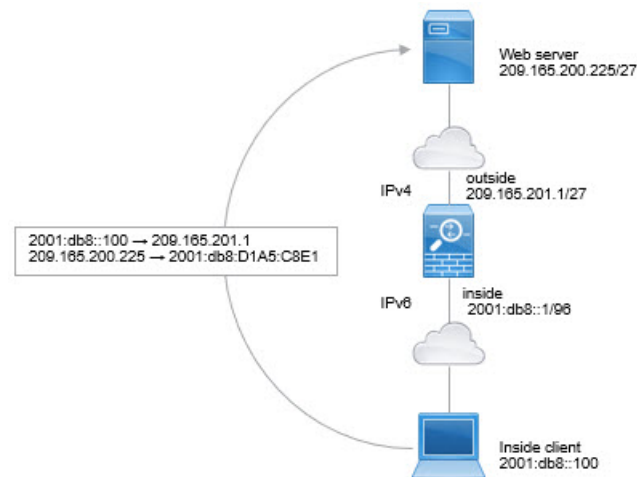
トラフィックが IPv6 ネットワークから IPv4 専用ネットワークに移動する場合、IPv6 アドレスを IPv4 に変換する必要があります。また、トラフィックを IPv4 から IPv6 に戻す必要があります。2つのアドレスプール（IPv4 ネットワークに IPv6 アドレスをバインドする IPv4 アドレスプールと、IPv6 ネットワークに IPv4 アドレスをバインドする IPv6 アドレスプール）を定義する必要があります。

- NAT64 ルール用の IPv4 アドレスプールは通常は小さく、一般的に IPv6 クライアントアドレスを使用して 1 対 1 のマッピングを設定するにはアドレスが足りない場合があります。ダイナミック PAT は、ダイナミック NAT やスタティック NAT と比べると、多数の IPv6 クライアントアドレスがある場合でも、比較的簡単に対応できます。
- NAT 46 ルールの IPv6 アドレスプールは、マッピングされる IPv4 アドレスの数と等しいか、それより多くなります。これによって、各 IPv4 アドレスを別の IPv6 アドレスにマッピングできます。NAT 46 はスタティックマッピングのみをサポートするため、ダイナミック PAT を使用することはできません。

送信元 IPv6 ネットワークと宛先 IPv4 ネットワークの 2 つのポリシーを定義する必要があります。これは、1 つの twice NAT ルールで実行できますが、DNS サーバーが外部ネットワーク上にある場合、DNS 応答をリライトする必要があります。宛先を指定するときに twice NAT ルールで DNS リライトを有効にすることができないため、2 つの Network Object NAT ルールを作成することがより適切なソリューションです。

NAT64/46 の例 : 内部 IPv6 ネットワークと外部 IPv4 インターネット

次に、内部 IPv6 専用ネットワークがある場合に、インターネットに送信されるトラフィックを IPv4 に変換する簡単な例を示します。この例の想定では DNS 変換が不要なため、1 つの twice NAT ルールで NAT64 と NAT46 の両方の変換を実行できます。



この例では、外部インターフェイスの IP アドレスを持つダイナミック インターフェイス PAT を使用して、内部の IPv6 ネットワークを IPv4 に変換します。外部 IPv4 トラフィックは、

2001:db8::/96 ネットワークのアドレスにスタティックに変換され、内部ネットワークでの送信が可能になります。

手順

ステップ 1 内部 IPv6 ネットワークのためのネットワーク オブジェクトを作成します。

- a) **[Configuration]** > **[Firewall]** > **[Objects]** > **[Network Objects/Groups]** を選択します。
- b) **[Add]** > **[Network Object]** をクリックします。
- c) 次のプロパティを使用してオブジェクトを設定します。
 - Name : たとえば、[inside_v6] です。
 - Type : [Network] を選択します。
 - IP Version : [IPv6] を選択します。
 - IP Address : 2001:db8:: と入力します。
 - Prefix Length : 96 と入力します。

- d) **[OK]** をクリックします。

ステップ 2 IPv6 ネットワークを IPv4 に変換して再び戻すための Twice NAT ルールを作成します。

- a) **[Configuration]** > **[Firewall]** > **[NAT Rules]** の順に選択します。
- b) **[Add]** > **[Add NAT Rule Before "Network Object" NAT Rules]** をクリックします。
- c) 次の **[Match Criteria: Original Packet]** オプションを設定します。
 - Source Interface : [inside] を選択します。
 - Destination Interface : [outside] を選択します。
 - Source Address : inside_v6 ネットワークオブジェクトを選択します。

- Destination Address : inside_v6 ネットワークオブジェクトを選択します。
 - Service : デフォルトの [any] を維持します。
- d) 次の [Match Criteria: Translated Packet] オプションを設定します。
- Source NAT Type : [Dynamic PAT (Hide)]を選択します。
 - Source Address : 外部インターフェイスを選択します。
 - Destination Address : [any] を選択します。

その他のオプションはデフォルト値のままにします。

ダイアログボックスは次のようになります。

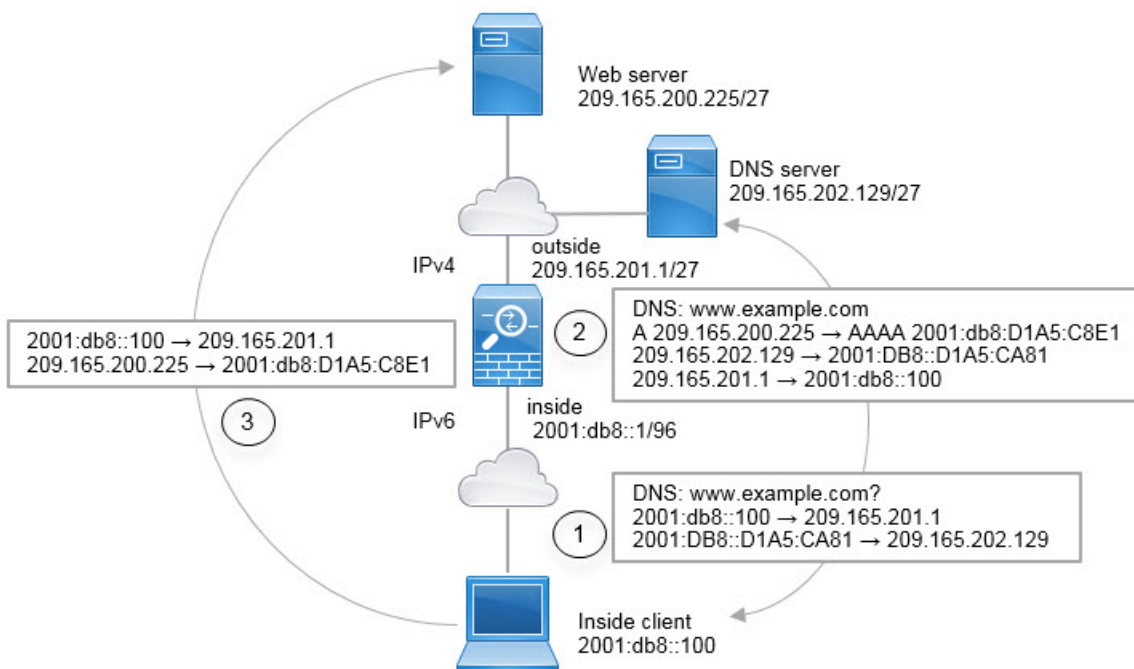
Match Criteria: Original Packet			
Source Interface:	inside	Destination Interface:	outside
Source Address:	inside_v6	Destination Address:	inside_v6
		Service:	any
Action: Translated Packet			
Source NAT Type:	Dynamic PAT (Hide)		
Source Address:	outside	Destination Address:	any

- e) [OK] をクリックします。

このルールにより、内部インターフェイスの 2001:db8::/96 サブネットから外部インターフェイスに向かうすべてのトラフィックが、外部インターフェイスの IPv4 アドレスを使用して NAT64 PAT 変換されます。逆に、内部インターフェイスに入る外部ネットワークの IPv4 アドレスはすべて、組み込み IPv4 アドレス方式を使用して 2001:db8::/96 ネットワーク上の 1 つのアドレスに変換されます。

NAT64/46 の例 : 外部 IPv4 インターネットと DNS 変換を使用した内部 IPv6 ネットワーク

次の図は、内部の IPv6 専用ネットワークが存在し、内部ユーザーが必要とするいくつかの IPv4 専用サービスが外部のインターネット上に存在する一般的な例です。



この例では、外部インターフェイスの IP アドレスを持つダイナミック インターフェイス PAT を使用して、内部の IPv6 ネットワークを IPv4 に変換します。外部 IPv4 トラフィックは、2001:db8::/96 ネットワークのアドレスにスタティックに変換され、内部ネットワークでの送信が可能になります。NAT46 ルールで DNS の書き換えを有効にすると、外部 DNS サーバーからの応答を A (IPv4) レコードから AAAA (IPv6) レコードに変換でき、アドレスが IPv4 から IPv6 に変換されます。

次は、内部 IPv6 ネットワーク上の 2001:DB8::100 にあるクライアントが www.example.com を開こうとしている場合の Web 要求の一般的なシーケンスです。

1. クライアントのコンピュータが 2001:DB8::D1A5:CA81 にある DNS サーバーに DNS 要求を送信します。NAT ルールにより、DNS 要求の送信元と宛先が次のように変換されます。
 - 2001:DB8::100 を 209.165.201.1 上の一意のポートに変換 (NAT64 インターフェイス PAT ルール)。
 - 2001:DB8::D1A5:CA81 を 209.165.202.129 に変換 (NAT46 ルール。D1A5:CA81 は IPv6 の 209.165.202.129 に相当します)。
2. DNS サーバーが、www.example.com が 209.165.200.225 であることを示す A レコードに応答します。DNS の書き換えが有効になっている NAT46 ルールにより、A レコードが IPv6 の同等の AAAA レコードに変換されて、AAAA レコードの 209.165.200.225 が 2001:db8:D1A5:C8E1 に変換されます。なお、DNS 応答の送信元アドレスと宛先アドレスは変換されません。
 - 209.165.202.129 を 2001:DB8::D1A5:CA81 に変換
 - 209.165.201.1 を 2001:db8::100 に変換

3. これで、IPv6 クライアントが Web サーバーの IP アドレスを取得し、www.example.com (2001:db8:D1A5:C8E1) に HTTP 要求を送信できます。(D1A5:C8E1 は IPv6 の 209.165.200.225 に相当します)。HTTP 要求の送信元と宛先が変換されます。
 - 2001:DB8::100 を 209.156.101.54 上の一意のポートに変換 (NAT64 インターフェイス PAT ルール)。
 - 2001:db8:D1A5:C8E1 を 209.165.200.225 に変換 (NAT46 ルール)。

次の手順では、この例の設定方法について説明します。

手順

ステップ 1 [Configuration] > [Firewall] > [NAT Rules] の順に選択します。

ステップ 2 内部 IPv6 ネットワークの NAT64 ダイナミック PAT ルールを設定します。

- a) [Add] > [Network Object NAT Rule] の順に選択します。
- b) 基本的なオブジェクトプロパティを設定します。
 - Name : たとえば、[inside_v6] です。
 - Type : [Network] を選択します。
 - IP Version : [IPv6] を選択します。
 - IP Address : 「2001:db8::」と入力します。
 - Prefix Length : 「96」と入力します。
- c) NAT のタイプに応じて [Dynamic] または [Dynamic PAT (Hide)] を選択します。
- d) [Translated Address] では、参照ボタンをクリックし、「外部」インターフェイスを選択します。

Add Network Object

Name: inside_v6

Type: Network

IP Version: IPv4 IPv6

IP Address: 2001:db8::

Prefix Length: 96

Description:

NAT

Add Automatic Address Translation Rules

Type: Dynamic PAT (Hide)

Translated Addr: outside

- e) [Advanced] ボタンをクリックし、次のオプションを設定します。
- Source Interface : [inside] を選択します。
 - Destination Interface : 「外部」 インターフェイスがすでに選択されています。
- f) [OK] をクリックして詳細設定を保存します。
- g) [OK] をクリックして NAT ルールを追加します。

このルールにより、内部インターフェイスの 2001:db8::/96 サブネットから外部インターフェイスに向かうすべてのトラフィックが、外部インターフェイスの IPv4 アドレスを使用して NAT64 PAT 変換されます。

ステップ 3 外部 IPv4 ネットワークのスタティック NAT46 ルールを設定します。

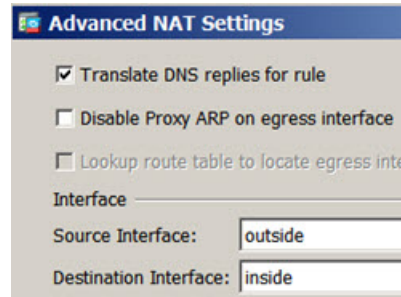
- a) [Add] > [Network Object NAT Rule] の順に選択します。
- b) 基本的なオブジェクトプロパティを設定します。
- Name : たとえば、[outside_v4_any] です。
 - Type : [Network] を選択します。
 - IP Version : [IPv4] を選択します。
 - IP Address : 「0.0.0.0」と入力します。
 - Netmask : 「0.0.0.0」と入力します。
- c) 基本的な NAT プロパティを設定します。
- NAT Type : [Static] を選択します。
 - Translated Address : 「2001:db8::/96」と入力します。

The screenshot shows the 'Add Network Object' dialog box with the following configuration:

- Name: outside_v4_any
- Type: Network
- IP Version: IPv4 (selected)
- IP Address: 0.0.0.0
- Netmask: 0.0.0.0
- Description: (empty)
- NAT Section:
 - Add Automatic Address Translation Rules
 - Type: Static
 - Translated Addr: 2001:db8::/96
 - Use one-to-one address translation

- d) [Advanced] ボタンをクリックし、次のオプションを設定します。

- Translate DNS Replies for Rule : このオプションを選択します。
- Source Interface : [outside] を選択します。
- Destination Interface : [inside] を選択します。



- [OK] をクリックして詳細設定を保存します。
- [OK] をクリックして NAT ルールを追加します。

このルールを使用すると、内部インターフェイスに届く外部ネットワークのすべての IPv4 アドレスが、組み込みの IPv4 アドレス方式を使用して 2001:db8::/96 ネットワークのアドレスに変換されます。また、DNS 応答が A (IPv4) レコードから AAAA (IPv6) レコードに変換され、アドレスが IPv4 から IPv6 に変換されます。

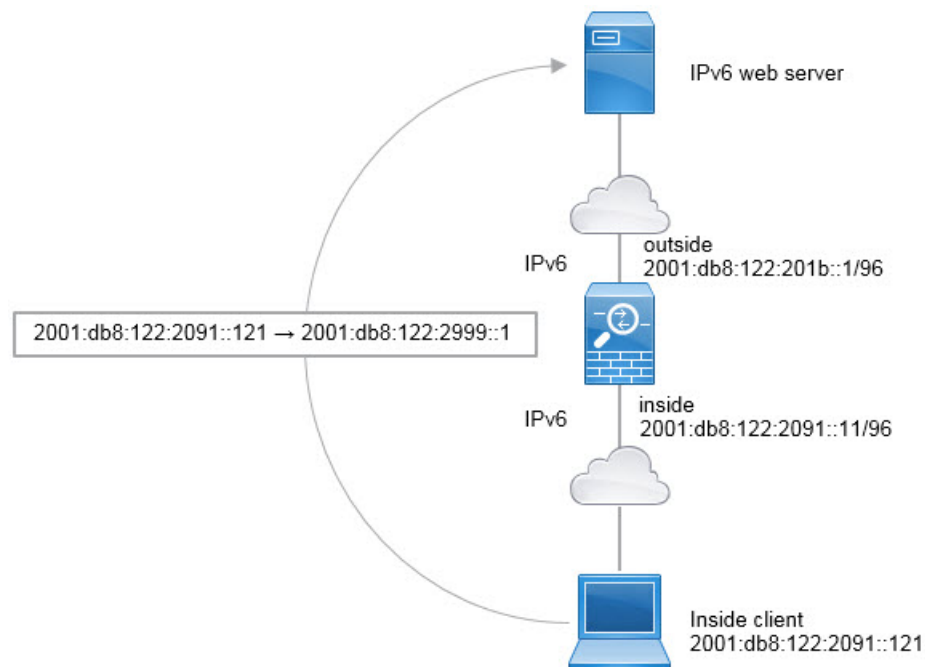
NAT66 : IPv6 アドレスの異なる IPv6 アドレスへの変換

IPv6 ネットワークから別の IPv6 ネットワークに移動する場合、アドレスを外部ネットワークの別の IPv6 アドレスに変換できます。スタティック NAT の使用を推奨します。ダイナミック NAT または PAT を使用できますが、IPv6 アドレスは大量にあるため、ダイナミック NAT を使用する必要がありません。

異なるアドレス タイプ間での変換ではないため、NAT66 変換の単一のルールが必要です。これらのルールは、Network Object NAT を使用して簡単にモデル化することができます。ただし、リターントラフィックを許可しない場合は、twice NAT のみを使用してスタティック NAT ルールを単方向にできます。

NAT66 の例 : ネットワーク間のスタティック変換

Network Object NAT を使用して、IPv6 アドレスプール間のスタティック変換を設定できます。次の例では、2001:db8:122:2091::/96 ネットワークの内部アドレスを 2001:db8:122:2999::/96 ネットワークの外部アドレスに変換する方法について説明します。



手順

ステップ1 [Configuration] > [Firewall] > [NAT Rules] の順に選択します。

ステップ2 内部 IPv6 ネットワークのスタティック NAT ルールを設定します。

a) [Add] > [Network Object NAT Rule] の順に選択します。

b) 基本的なオブジェクトプロパティを設定します。

- Name : たとえば、[inside_v6] です。
- Type : [Network] を選択します。
- IP Version : [IPv6] を選択します。
- IP Address : 「2001:db8:122:2091::」と入力します。
- Prefix Length : 「96」と入力します。

c) [NAT Type] に [Static] を選択します。

d) [Translated Address] に 「2001:db8:122:2999::/96」と入力します。

The screenshot shows the 'Add Network Object' dialog box. The 'Name' field contains 'inside_v6', 'Type' is 'Network', 'IP Version' has 'IPv6' selected, 'IP Address' is '2001:db8:122:2091::', and 'Prefix Length' is '96'. Below this, the 'NAT' section is expanded, showing a checked box for 'Add Automatic Address Translation Rules', a dropdown menu for 'Type' set to 'Static', and a text field for 'Translated Addr' containing '2001:db8:122:2999::/96'.

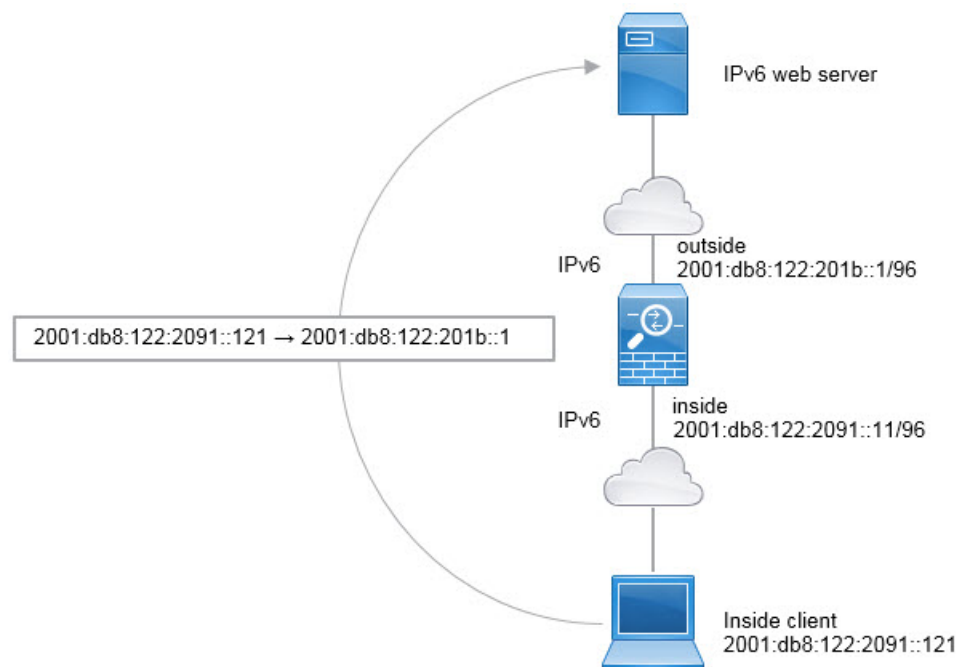
- e) [Advanced] ボタンをクリックし、次のオプションを設定します。
- Source Interface : [inside] を選択します。
 - Destination Interface : [outside] を選択します。
- f) [OK] をクリックして詳細設定を保存します。
- g) [OK] をクリックして NAT ルールを追加します。

このルールにより、内部インターフェイス上の 2001:db8:122:2091::/96 サブネットから外部インターフェイスに向かうすべてのトラフィックが、2001:db8:122:2999::/96 ネットワーク上のアドレスにスタティック NAT66 変換されます。

NAT66 の例 : シンプルな IPv6 インターフェイス PAT

NAT66 を実装するための簡単なアプローチは、外部インターフェイスの IPv6 アドレス上の異なるポートに内部アドレスを動的に割り当てる方法です。

NAT66 のインターフェイス PAT ルールを設定すると、そのインターフェイスに設定されているすべてのグローバルアドレスが PAT のマッピングに使用されます。インターフェイスのリンクローカルアドレスまたはサイトローカルアドレスは、PAT には使用されません。



手順

ステップ 1 [Configuration] > [Firewall] > [NAT Rules] の順に選択します。

ステップ 2 内部 IPv6 ネットワーク用のダイナミック PAT ルールを設定します。

- a) [Add] > [Network Object NAT Rule] の順に選択します。
- b) 基本的なオブジェクトプロパティを設定します。
 - Name : たとえば、[inside_v6] です。
 - Type : [Network] を選択します。
 - IP Version : [IPv6] を選択します。
 - IP Address : 「2001:db8:122:2091::」と入力します。
 - Prefix Length : 「96」と入力します。
- c) NAT のタイプに応じて [Dynamic] または [Dynamic PAT (Hide)] を選択します。
- d) [Translated Address] では、参照ボタンをクリックし、「外部」インターフェイスを選択します。
- e) [Use IPv6 for Interface PAT] オプションを選択します。

Add Network Object

Name: inside_v6
Type: Network
IP Version: IPv4 IPv6
IP Address: 2001:db8:122:2091::
Prefix Length: 96
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

Enable Block Allocation

Block size of 512 and maximum block allocation per host 4 has been configured.
To change click [here](#)

Fall through to interface PAT(dest intf): dmz

Use IPv6 for interface PAT

Advanced...

OK Cancel Help

f) [Advanced] ボタンをクリックし、次のオプションを設定します。

- Source Interface : [inside] を選択します。
- Destination Interface : 「外部」 インターフェイスがすでに選択されています。

g) [OK] をクリックして詳細設定を保存します。

h) [OK] をクリックして NAT ルールを追加します。

このルールでは、内部インターフェイスの 2001:db8:122:2091::/96 サブネットから外部インターフェイスへのトラフィックは、外部インターフェイス用に設定された IPv6 グローバルアドレスのいずれかに NAT66 PAT 変換されます。

NAT を使用した DNS クエリと応答の書き換え

応答内のアドレスを NAT 設定と一致するアドレスに置き換えて、DNS 応答を修正するように ASA を設定することが必要になる場合があります。DNS 修正は、各トランスレーションルールを設定するときに設定できます。DNS 修正は DNS 改ざんとも呼ばれます。

この機能は、NAT ルールに一致する DNS クエリと応答のアドレスを書き換えます（たとえば、IPv4 の A レコード、IPv6 の AAAA レコード、または逆引き DNS クエリの PTR レコード）。マッピングインターフェイスから他のインターフェイスに移動する DNS 応答では、A レコードはマップされた値から実際の値へ書き換えられます。逆に、任意のインターフェイスからマッピングインターフェイスに移動する DNS 応答では、A レコードは実際の値からマップされた値へ書き換えられます。この機能は、NAT44、NAT66、NAT46、および NAT64 と連動します。

以下に、NAT ルールで DNS の書き換えを設定する必要がある主な状況を示します。

- ルールは NAT64 または NAT46 であり、DNS サーバは外部ネットワークにあります。DNS A レコード (IPv4 用) と AAAA レコード (IPv6 用) を変換するために DNS の書き換えが必要です。
- DNS サーバは外部にあり、クライアントは内部にあります。クライアントが使用する一部の完全修飾ドメイン名が他の内部ホストに解決されます。
- DNS サーバは内部にあり、プライベート IP アドレスを使用して応答します。クライアントは外部にあり、クライアントは内部でホストされているサーバを指定する完全修飾ドメイン名にアクセスします。

DNS の書き換えの制限事項

次に DNS の書き換えの制限事項を示します。

- 個々の A または AAAA レコードに複数の PAT ルールを適用できることで、使用する PAT ルールが不明確になるため、DNS の書き換えは PAT には適用されません。
- twice NAT ルールを設定する場合、送信元アドレスおよび宛先アドレスを指定すると、DNS 修正を設定できません。これらの種類のルールでは、A と B に向かった場合に 1 つのアドレスに対して異なる変換が行われる可能性があります。したがって、DNS 応答内の IP アドレスを適切な Twice NAT ルールに一致させることができません。DNS 応答には、DNS 要求を求めたパケット内の送信元アドレスと宛先アドレスの組み合わせに関する情報が含まれません。
- DNS クエリと応答を書き換えるには、NAT ルールに対して有効な DNS NAT の書き換えを用いた DNS アプリケーションインスペクションを有効にする必要があります。デフォルトでは、有効にされた DNS NAT の書き換えによる DNS インスペクションはグローバルに適用されるため、インスペクション設定を変更する必要はありません。

- 実際には、DNS の書き換えは NAT ルールではなく `xlate` エントリで実行されます。したがって、ダイナミック ルールに `xlate` がない場合、書き換えが正しく実行されません。スタティック NAT の場合は、同じような問題が発生しません。
- DNS の書き換えによって、DNS ダイナミック アップデートのメッセージ（オペレーションコード 5）は書き換えられません。

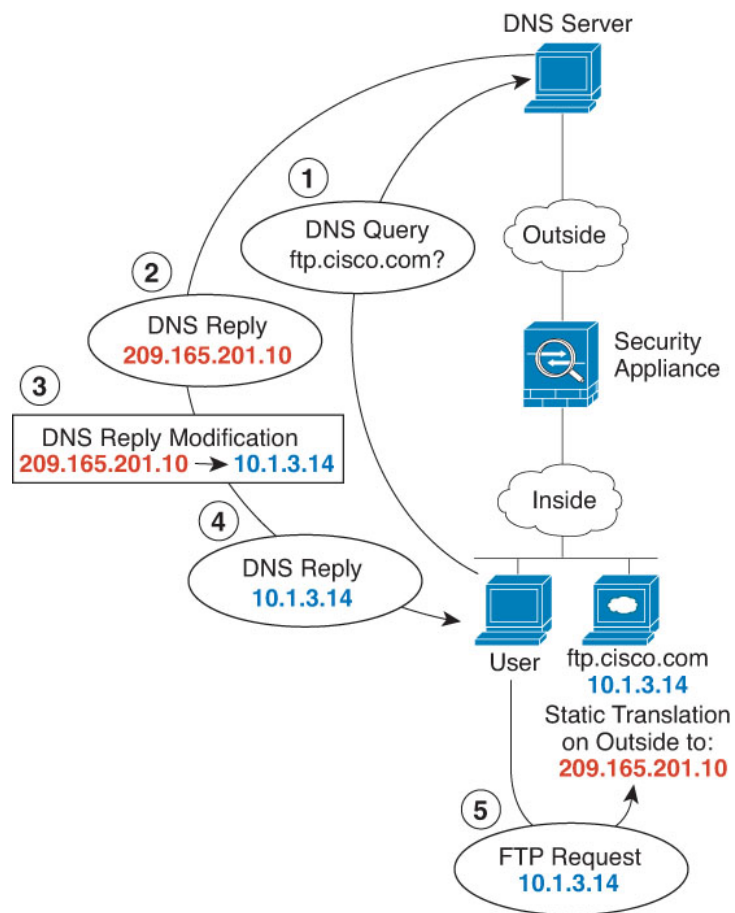
次のトピックで、NAT ルールでの DNS の書き換えの例を示します。

DNS 応答修正：外部の DNS サーバー

次の図に、外部インターフェイスからアクセス可能な DNS サーバを示します。 `ftp.cisco.com` というサーバが内部インターフェイス上にあります。 `ftp.cisco.com` の実際のアドレス（`10.1.3.14`）を、外部ネットワーク上で確認できるマッピングアドレス（`209.165.201.10`）にスタティックに変換するように NAT を設定します。

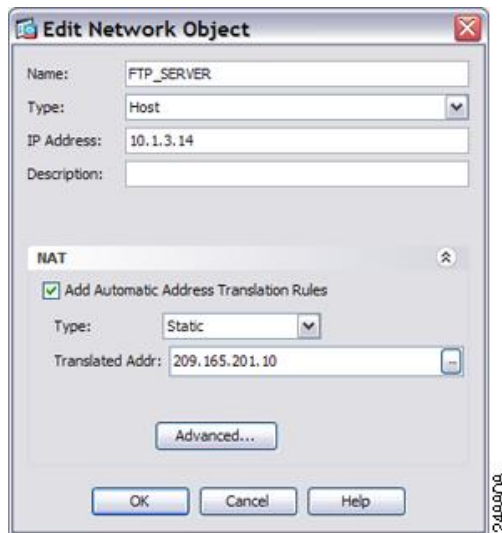
この場合、このスタティック ルールで DNS 応答修正を有効にする必要があります。有効にすると、実際のアドレスを使用して `ftp.cisco.com` にアクセスできる内部ユーザーは、マッピングアドレスではなく実際のアドレスを DNS サーバーから受信できるようになります。

内部ホストが `ftp.cisco.com` のアドレスを求める DNS 要求を送信すると、DNS サーバーはマッピングアドレス（`209.165.201.10`）を応答します。システムは、内部サーバのスタティックルールを参照し、DNS 応答内のアドレスを `10.1.3.14` に変換します。DNS 応答修正を有効にしない場合、内部ホストは `ftp.cisco.com` に直接アクセスする代わりに、`209.165.201.10` にトラフィックの送信を試みます。

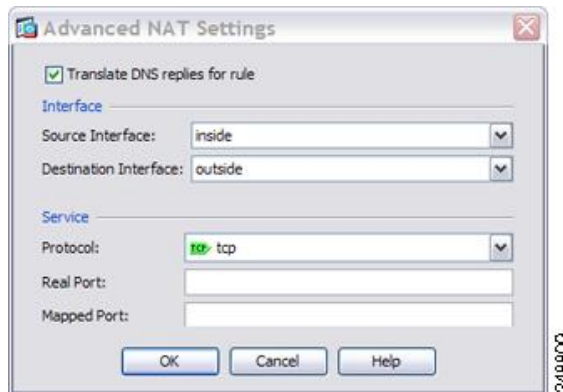


手順

- ステップ 1** [Configuration] > [Firewall] > [NAT] を選択します。
- ステップ 2** [Add] > [Network Object NAT Rule] の順に選択します。
- ステップ 3** 新しいネットワークオブジェクトに名前を付けてFTPサーバーアドレスを定義し、スタティック NAT をイネーブルにして変換されたアドレスを入力します。



ステップ 4 [Advanced] をクリックし、実際のインターフェイスおよびマッピングインターフェイスと DNS 修正を設定します。



ステップ 5 [OK] をクリックして [ネットワーク オブジェクトの編集 (Edit Network Object)] ダイアログボックスに戻り、もう一度 [OK] をクリックし、[適用 (Apply)] をクリックします。

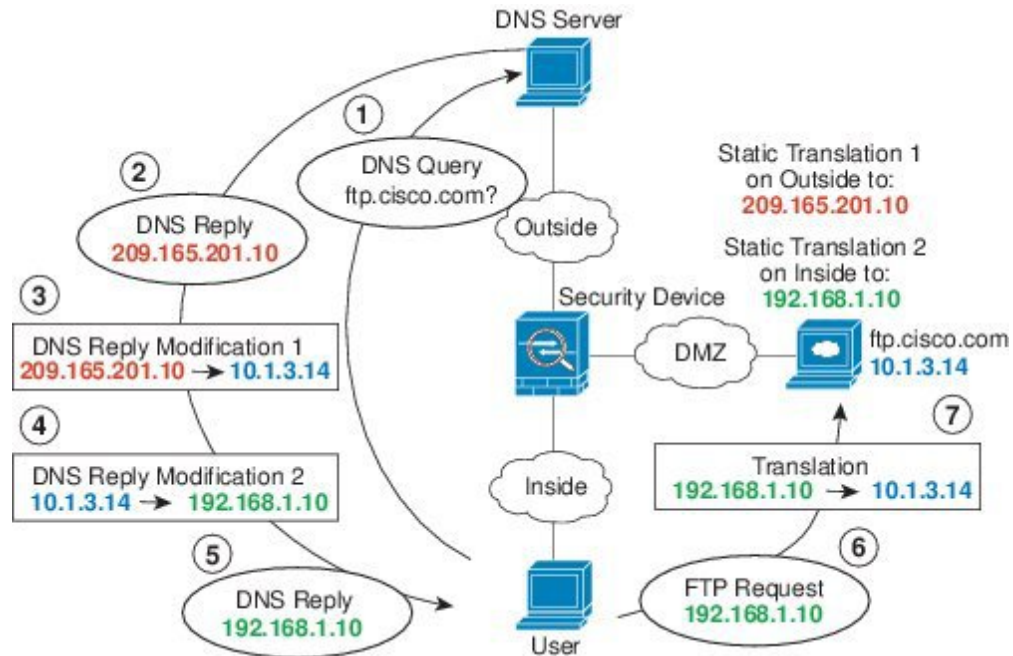
DNS 応答修正 : 別々のネットワーク上の DNS サーバー、ホスト、およびサーバー

次の図に、外部 DNS サーバーから DMZ ネットワークにある ftp.cisco.com の IP アドレスを要求する内部ネットワークのユーザーを示します。DNS サーバーは、ユーザーが DMZ ネットワーク上に存在しない場合でも、外部と DMZ 間のスタティック ルールに従って応答でマッピングアドレス (209.165.201.10) を示します。ASA は、DNS 応答内のアドレスを 10.1.3.14 に変換します。

ユーザーが実際のアドレスを使用して ftp.cisco.com にアクセスする必要がある場合、これ以上の設定は必要ありません。内部と DMZ 間にもスタティック ルールがある場合は、このルール

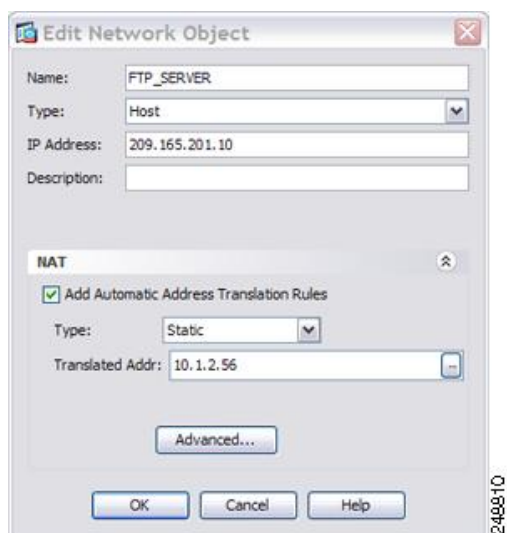
に対して DNS 応答修正もイネーブルにする必要があります。DNS 応答は、2回変更されます。この場合、ASA は内部と DMZ 間のスタティックルールに従ってもう一度 DNS 応答内のアドレスを 192.168.1.10 に変換します。

図 17: DNS 応答修正 : 別々のネットワーク上の DNS サーバー、ホスト、およびサーバー

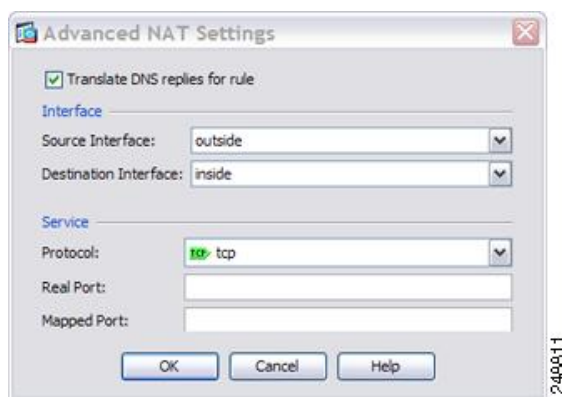


DNS 応答修正 : ホスト ネットワーク上の DNS サーバー

次の図に、外部の FTP サーバと DNS サーバを示します。システムには、外部サーバ用のスタティック変換があります。この場合、内部ユーザーが ftp.cisco.com のアドレスを DNS サーバーに要求すると、DNS サーバーは実際のアドレス (209.165.20.10) を応答します。内部ユーザーに ftp.cisco.com のマッピングアドレス (10.1.2.56) を使用させるには、スタティック変換用の DNS 応答修正を設定する必要があります。



ステップ4 [Advanced]をクリックし、実際のインターフェイスおよびマッピングインターフェイスとDNS修正を設定します。

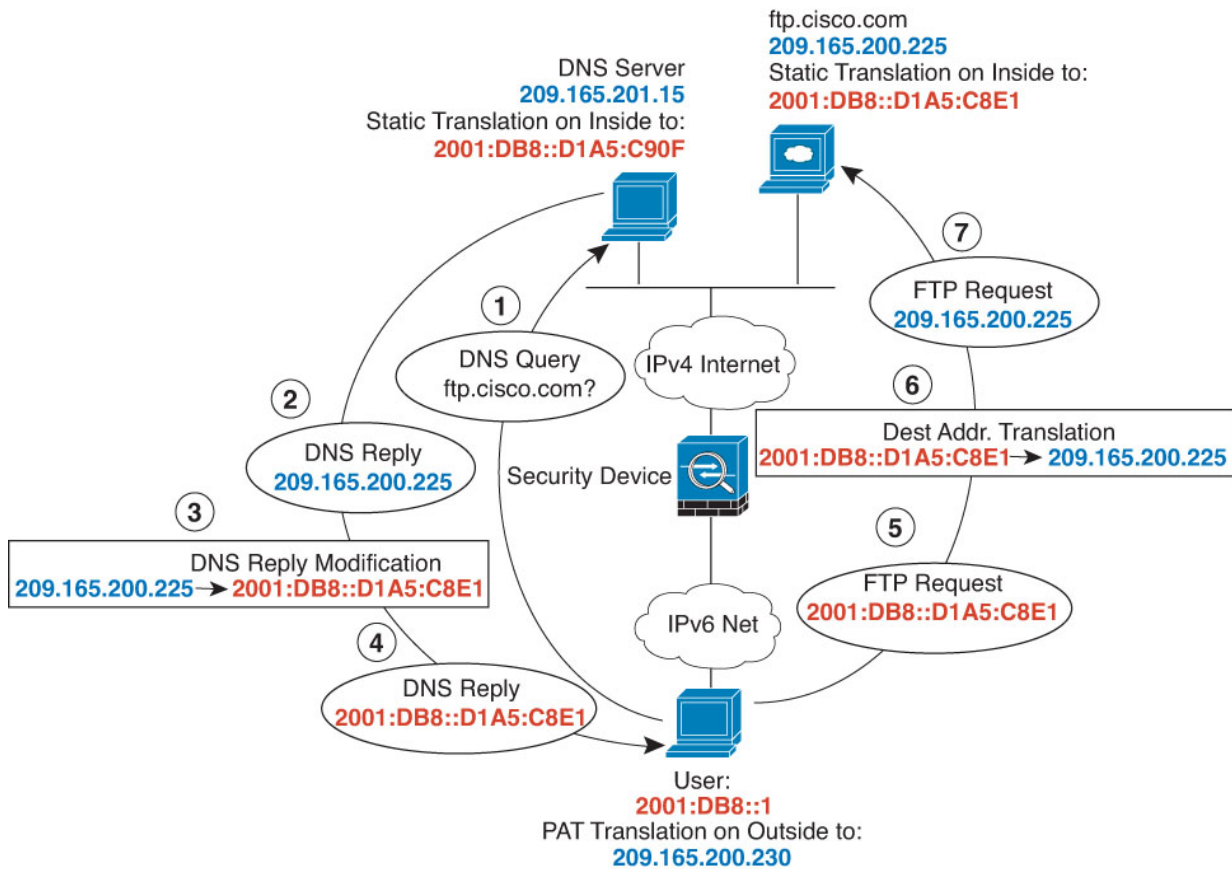


ステップ5 [OK]をクリックして[ネットワーク オブジェクトの編集 (Edit Network Object)]ダイアログボックスに戻り、もう一度 [OK]をクリックし、[適用 (Apply)]をクリックします。

DNS64 応答修正

次の図に、外部のIPv4ネットワーク上のFTPサーバとDNSサーバを示します。システムには、外部サーバ用のスタティック変換があります。この場合、内部IPv6ユーザーがftp.cisco.comのアドレスをDNSサーバに要求すると、DNSサーバは実際のアドレス(209.165.200.225)を応答します。

内部ユーザーにftp.cisco.comのマッピングアドレス(2001:DB8::D1A5:C8E1 : D1A5:C8E1はIPv6の209.165.200.225に相当)を使用させるには、スタティック変換用のDNS応答修正を設定する必要があります。この例には、DNSサーバのスタティックNAT変換、および内部IPv6ホストのPATルールも含まれています。



手順

ステップ 1 [Configuration] > [Firewall] > [NAT] を選択します。

ステップ 2 FTP サーバーの DNS 修正を設定したスタティック ネットワーク オブジェクト NAT を設定します。

- a) [追加 (Add)] > [ネットワーク オブジェクトの NAT ルール (Network Object NAT Rule)] を選択します。
- b) 新しいネットワーク オブジェクトに名前を付けて FTP サーバー アドレスを定義し、スタティック NAT をイネーブルにして変換されたアドレスを入力します。これは NAT46 の 1 対 1 変換であるため、[Use one-to-one address translation] を選択します。

- c) 実際のインターフェイスとマッピングインターフェイスおよびDNS修正を設定するには、[Advanced] をクリックします。

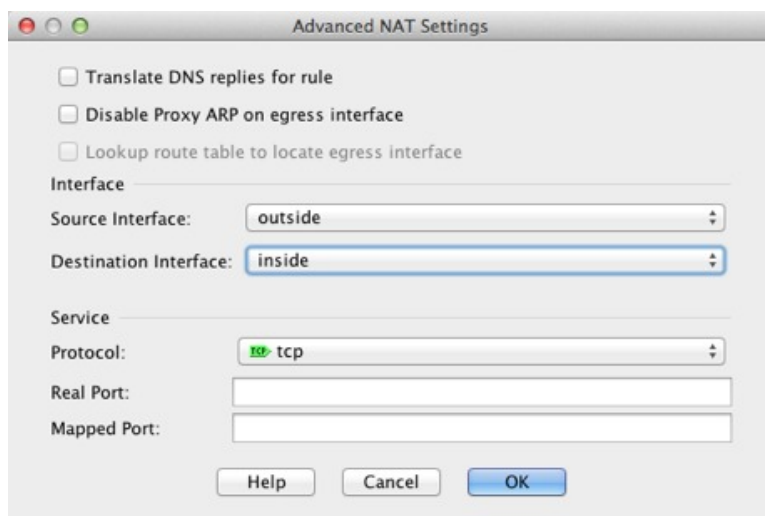
- d) [OK] をクリックして [Network Object] ダイアログボックスに戻り、もう一度 [OK] をクリックしてルールを保存します。

ステップ 3 DNS サーバーのスタティック ネットワーク オブジェクト NAT を設定します。

- a) [Add] > [Network Object NAT Rule] を選択します。
- b) 新しいネットワーク オブジェクトに名前を付けて DNS サーバー アドレスを定義し、スタティック NAT をイネーブルにして変換されたアドレスを入力します。これは NAT46 の 1 対 1 変換であるため、[Use one-to-one address translation] を選択します。

The screenshot shows the 'Add Network Object' dialog box. The 'Name' field is 'DNS_server', 'Type' is 'Host', 'IP Version' is 'IPv4', and 'IP Address' is '209.165.201.15'. The 'NAT' section is expanded, showing 'Add Automatic Address Translation Rules' checked, 'Type' set to 'Static', and 'Translated Addr' set to '2001:DB8::D1A5:C90F'. The checkbox 'Use one-to-one address translation' is checked and circled in red. Other options are unchecked. The 'Advanced...' button is visible at the bottom of the NAT section. The main dialog has 'Help', 'Cancel', and 'OK' buttons at the bottom.

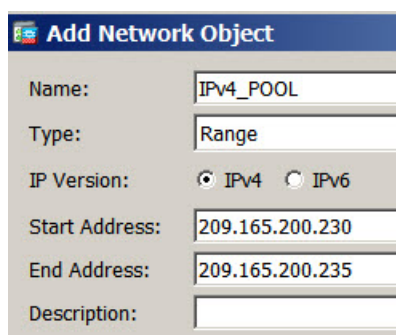
- c) 実際のインターフェイスとマッピングインターフェイスを設定するには、[Advanced] をクリックします。



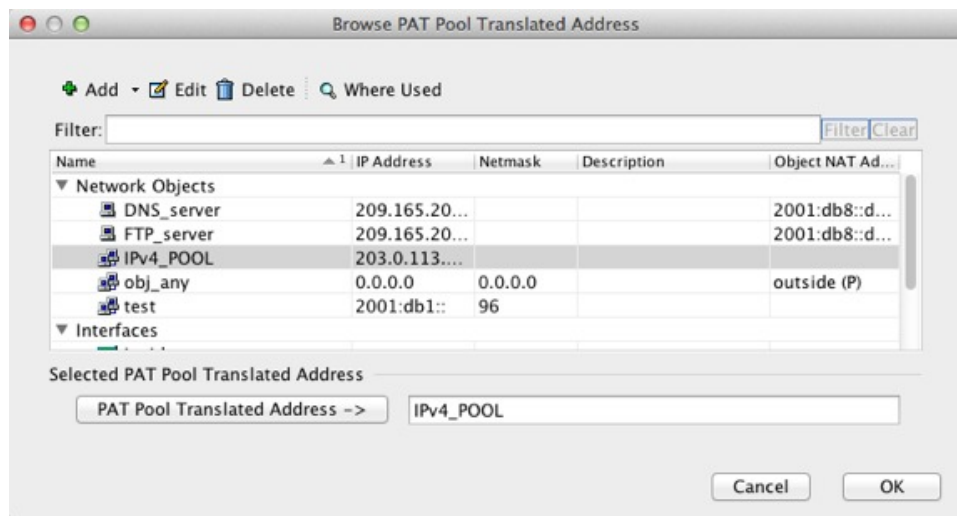
- d) [OK] をクリックして [Network Object] ダイアログボックスに戻り、もう一度 [OK] をクリックしてルールを保存します。

ステップ 4 内部 IPv6 ネットワークのための PAT を設定します。

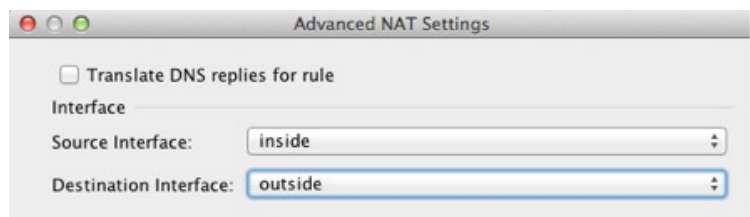
- [Add] > [Network Object NAT Rule] を選択します。
- 新しいネットワーク オブジェクトに名前を付けて IPv6 ネットワーク アドレスを定義し、ダイナミック NAT を選択します。
- [PAT Pool Translated Address] を選択し、[...] (参照) ボタンをクリックして PAT プール オブジェクトを作成します。
- [Browse PAT Pool Translated Address] ダイアログボックスで、[Add] > [Network Object] を選択します。新しいオブジェクトに名前を付けて PAT プールのアドレス範囲を入力し、[OK] をクリックします。



- e) [Browse PAT Pool Translated Address] ダイアログボックスで、作成した PAT プール オブジェクトをダブルクリックして選択し、[OK] をクリックします。



- f) 実際のインターフェイスとマッピングインターフェイスを設定するには、[Advanced] をクリックします。



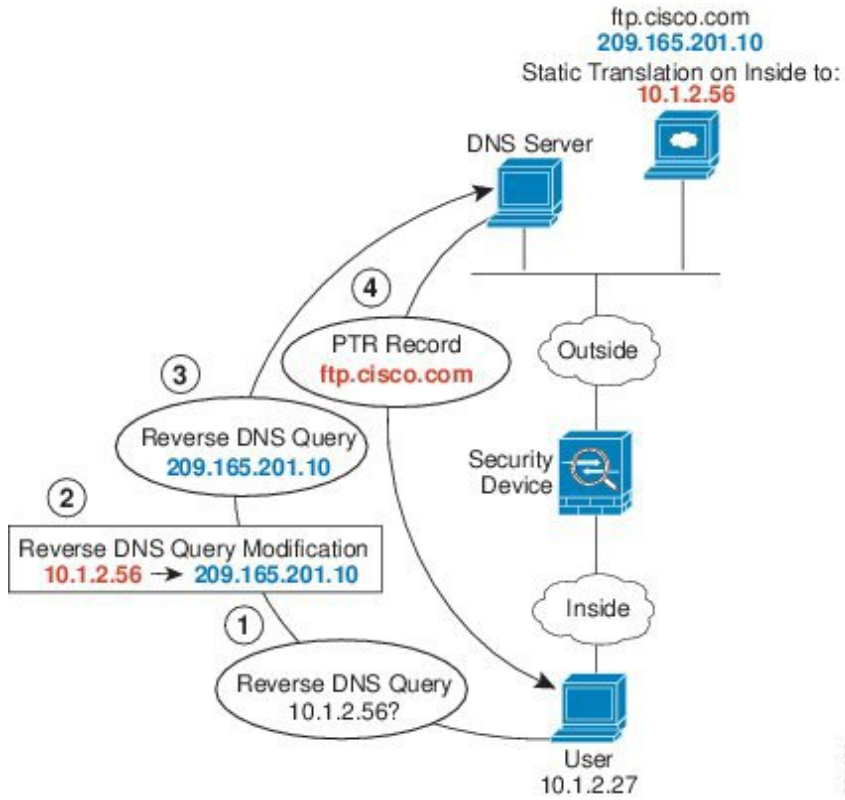
- g) [OK] をクリックして [Network Object] ダイアログボックスに戻ります。

ステップ5 [OK] をクリックし、さらに [Apply] をクリックします。

PTR の変更、ホスト ネットワークの DNS サーバー

次の図に、外部の FTP サーバーと DNS サーバーを示します。ASA には、外部サーバー用のスタティック変換があります。この場合、内部のユーザーが 10.1.2.56 の逆引き DNS ルックアップを実行する場合、ASA は実際のアドレスを使用して逆引き DNS クエリーを変更し、DNS サーバーはサーバー名、ftp.cisco.com を使用して応答します。

図 18: PTR の変更、ホストネットワークの DNS サーバー



304-002

翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。