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。

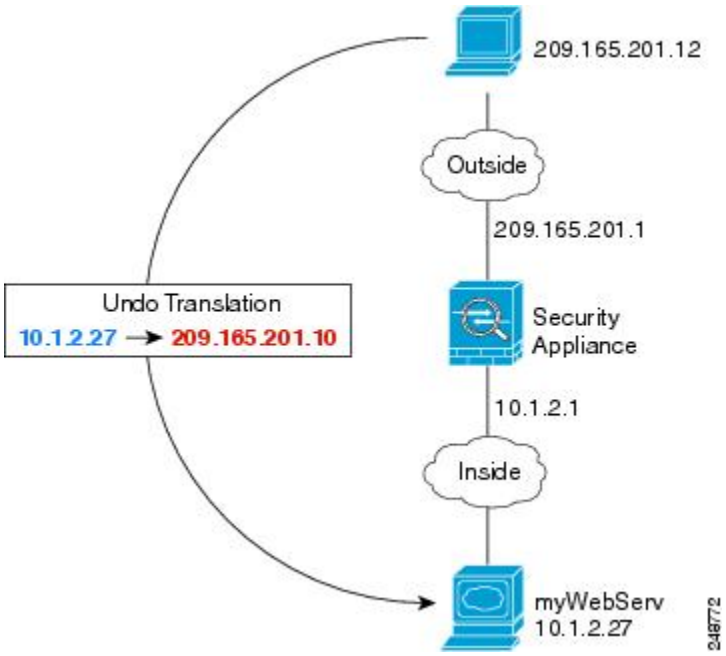
ネットワーク オブジェクト NAT の例

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ので、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

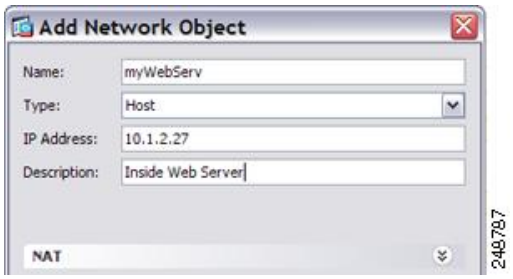
図 *1*: 内部 *Web* サーバのスタティック *NAT*



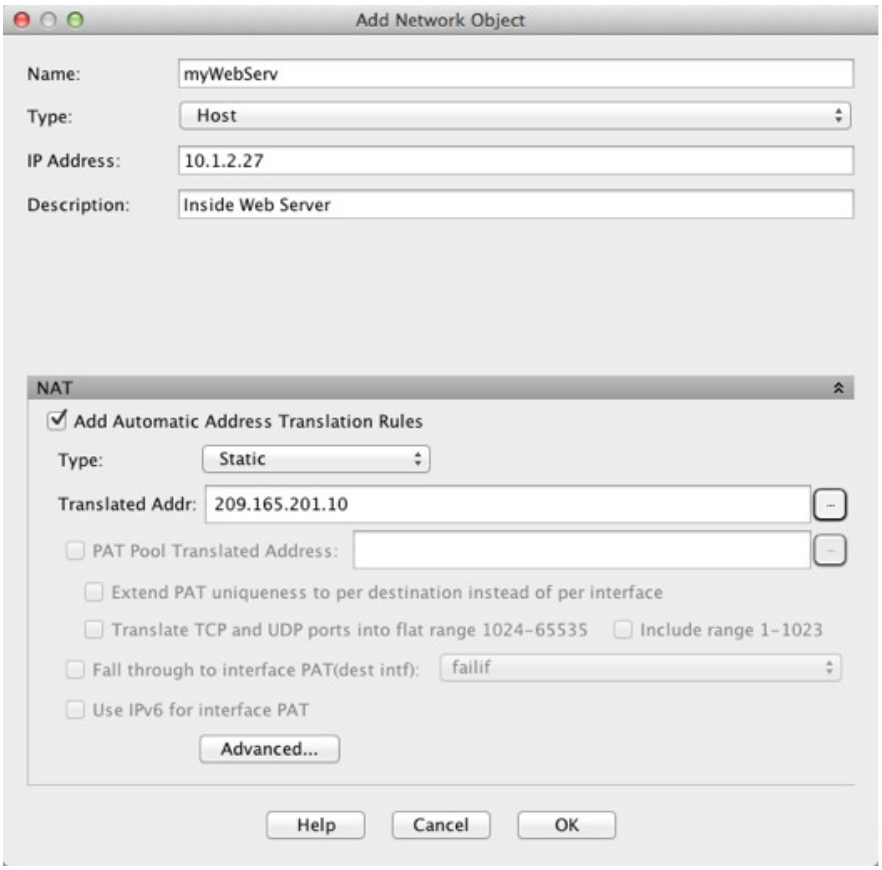
手順

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

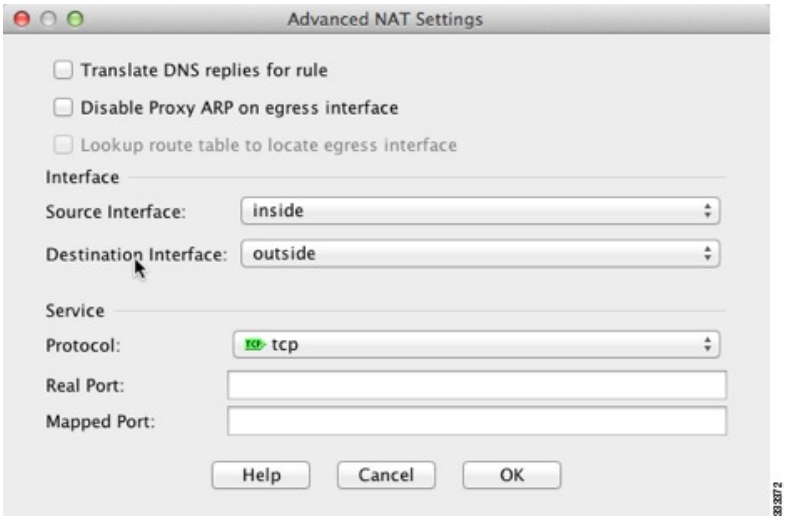
ステップ 2 **[Add]** > **[Network Object NAT Rule]** を選択し、新しいネットワーク オブジェクトに名前を付けて Web サーバのホスト アドレスを定義します。



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。

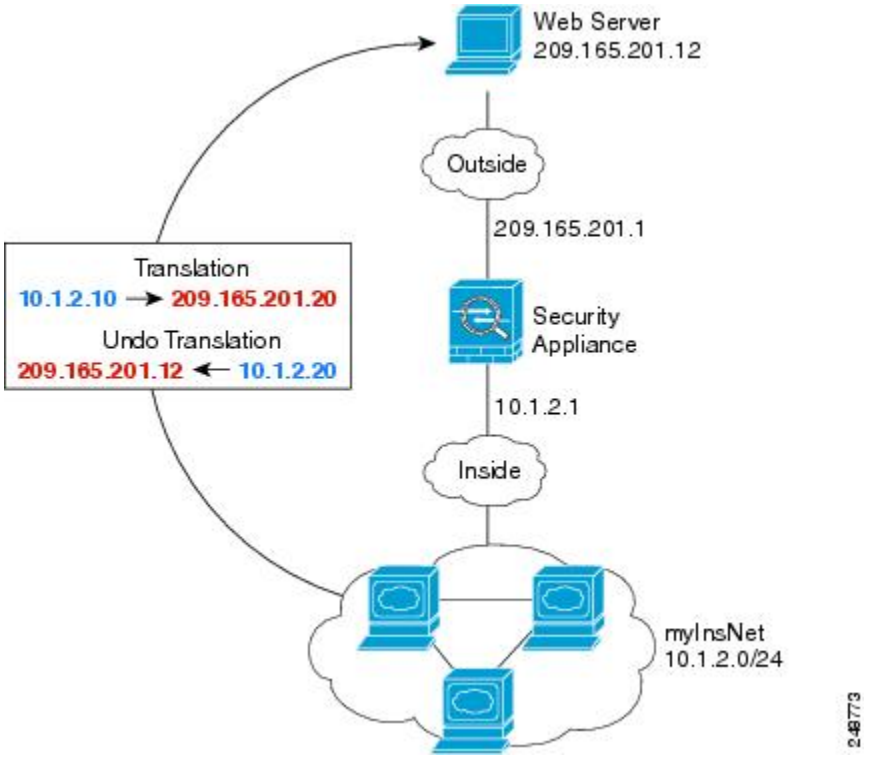


ステップ 5 [OK] をクリックして [Edit Network Object] ダイアログボックスに戻り、もう一度 [OK] をクリックし、[Apply] をクリックします。

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が外部にアクセスする場合、このユーザにダイナミック NAT を設定します。また、内部ユーザが外部 Web サーバに接続する場合、この Web サーバのアドレスが内部ネットワークに存在するように見えるアドレスに変換されます

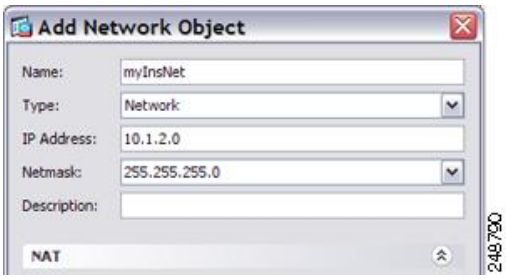
図 *2:* 内部のダイナミック *NAT*、外部 *Web* サーバのスタティック *NAT*



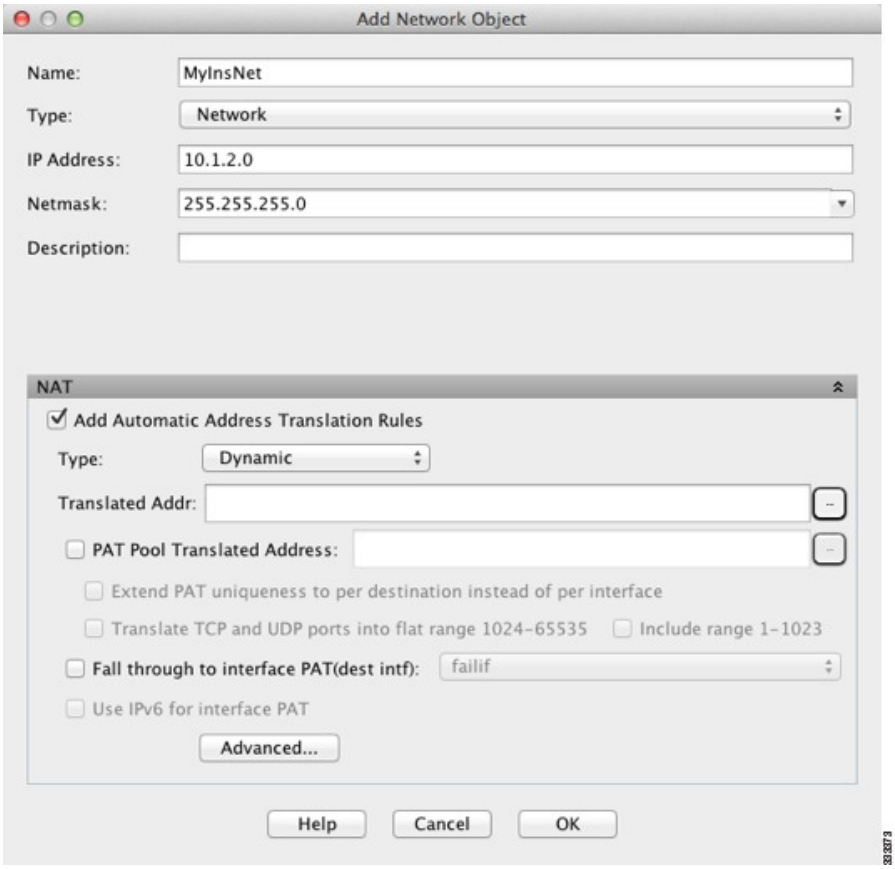
手順

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。

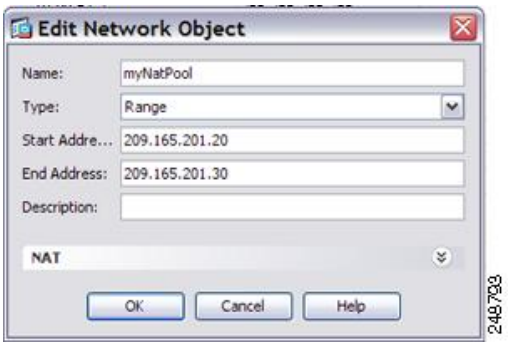


ステップ 3 内部ネットワークのダイナミック NAT をイネーブルにします。



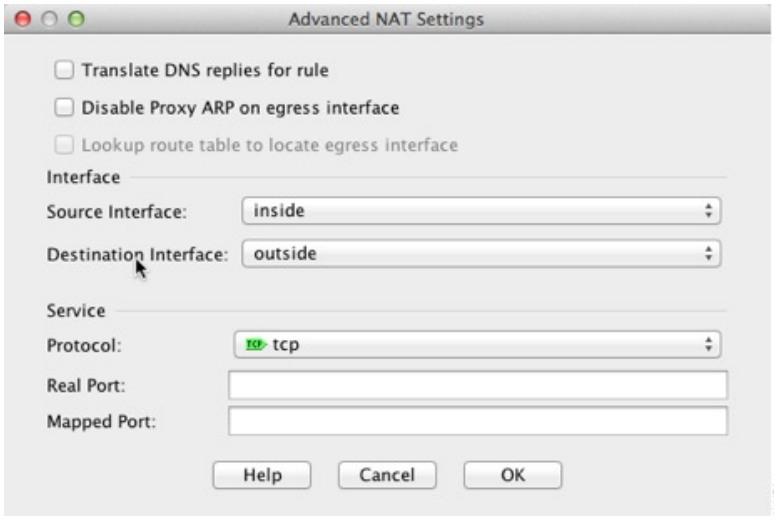
ステップ 4 [Translated Addr] フィールドで、内部アドレスの変換先となるダイナミック NAT プールを表す新しいネットワーク オブジェクトを追加するには、参照ボタンをクリックします。

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。



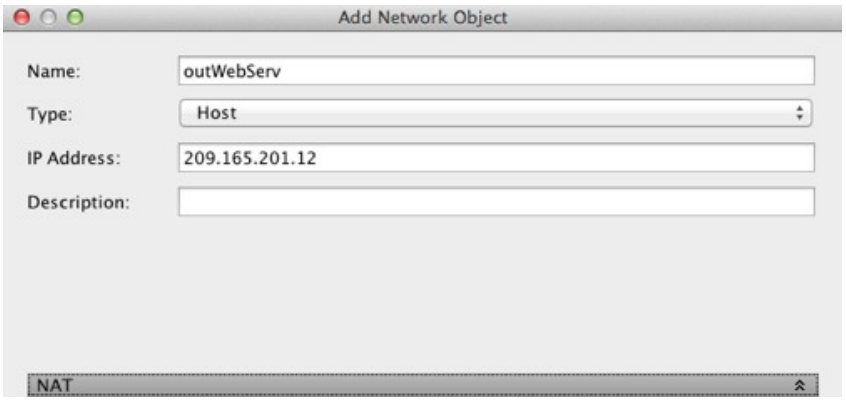
b) 新しいネットワーク オブジェクトをダブルクリックで選択します。[OK] をクリックして、NAT コンフィギュレーションに戻ります。

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。

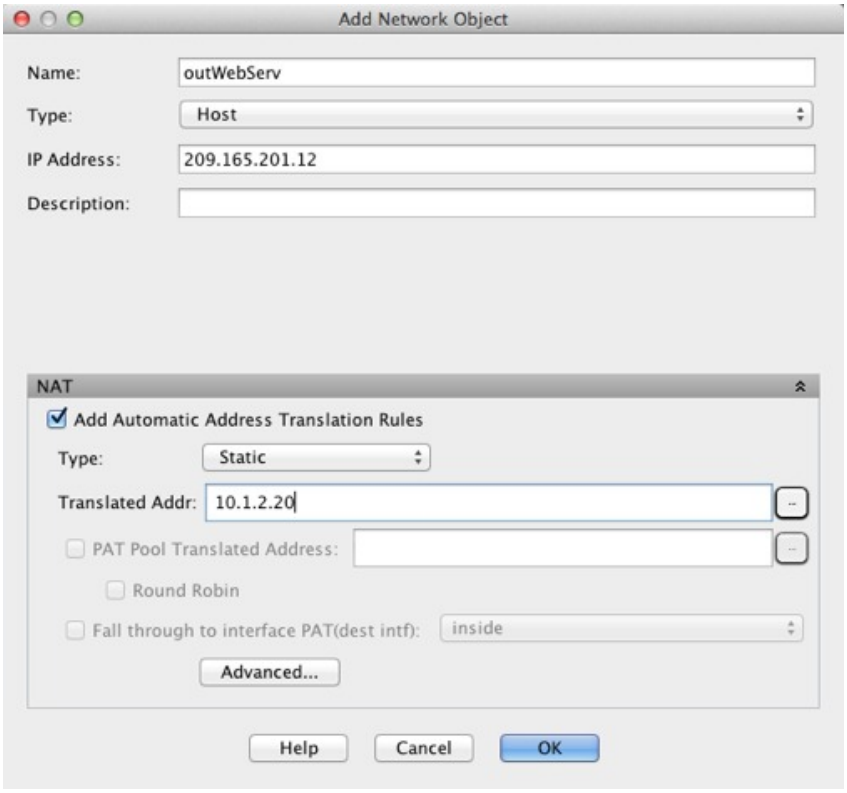


ステップ 6 [OK] をクリックして [Edit Network Object] ダイアログボックスに戻り、もう一度 [OK] をクリックして [NAT Rules] テーブルに戻ります。

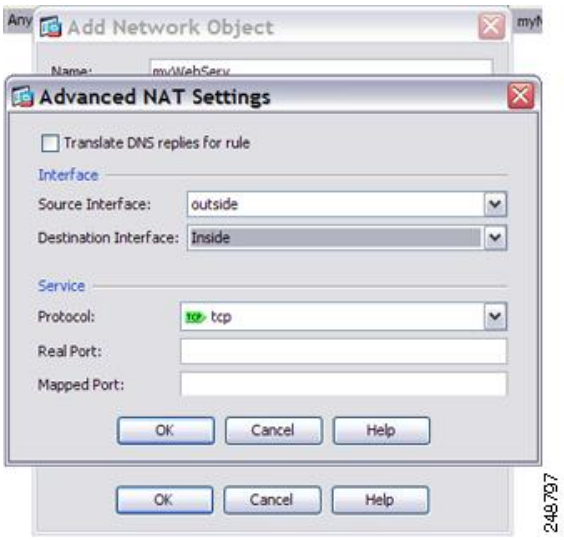
ステップ 7 **[Add]** > **[Network Object NAT Rule]** を選択し、外部 Web サーバのオブジェクトを作成します。



ステップ 8 Web サーバのスタティック NAT を設定します。



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。

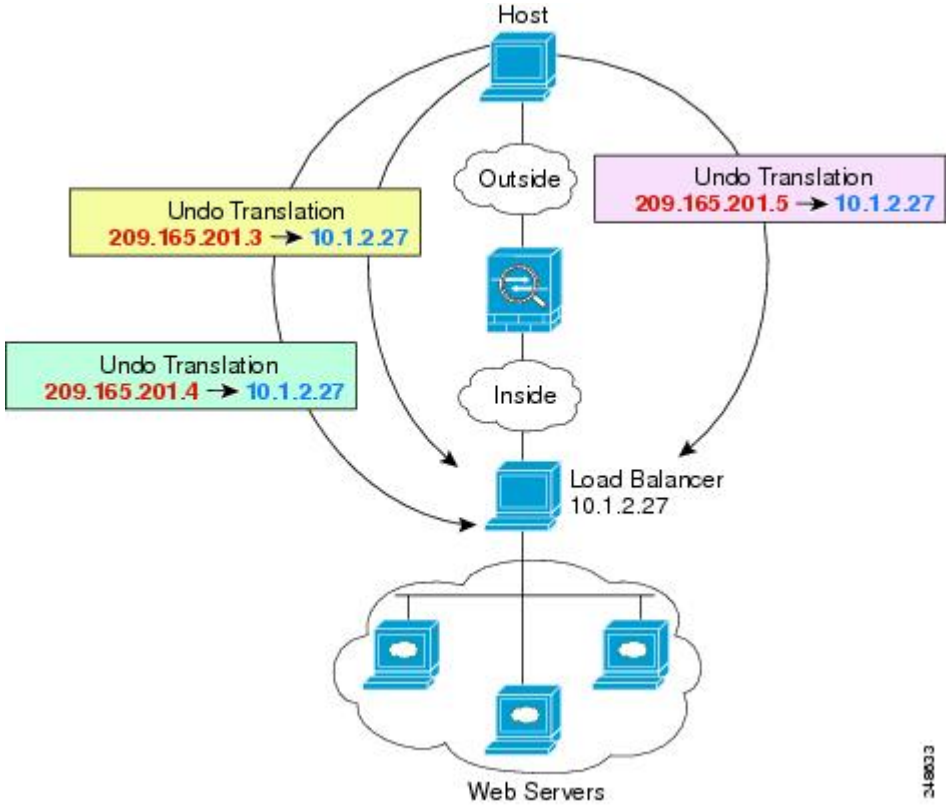


ステップ 10 [OK] をクリックして [Edit Network Object] ダイアログボックスに戻り、もう一度 [OK] をクリックし、[Apply] をクリックします。

複数のマッピングアドレス（スタティック NAT、一対多）を持つ内部ロード バランサ

次の例では、複数の IP アドレスに変換される内部ロード バランサを示しています。外部ホストがマッピング IP アドレスの 1 つにアクセスする場合、1 つのロード バランサのアドレスには変換されません。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 バランサのスタティック *NAT*（一対多）



手順

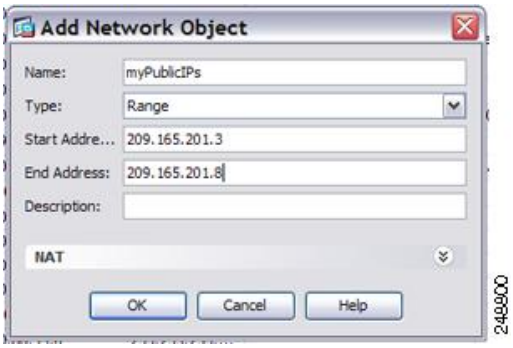
ステップ 1 **[Configuration]** > **[Firewall]** > **[NAT]** を選択します。

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。

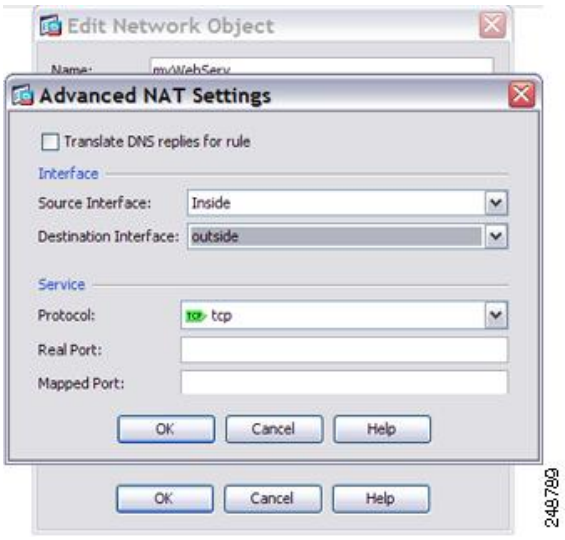
ステップ 4 [Translated Addr] フィールドで、ロード バランサ アドレスの変換先となるスタティック NAT アドレス グループを表す新しいネットワーク オブジェクトを追加するには、参照ボタンをクリックします。

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。

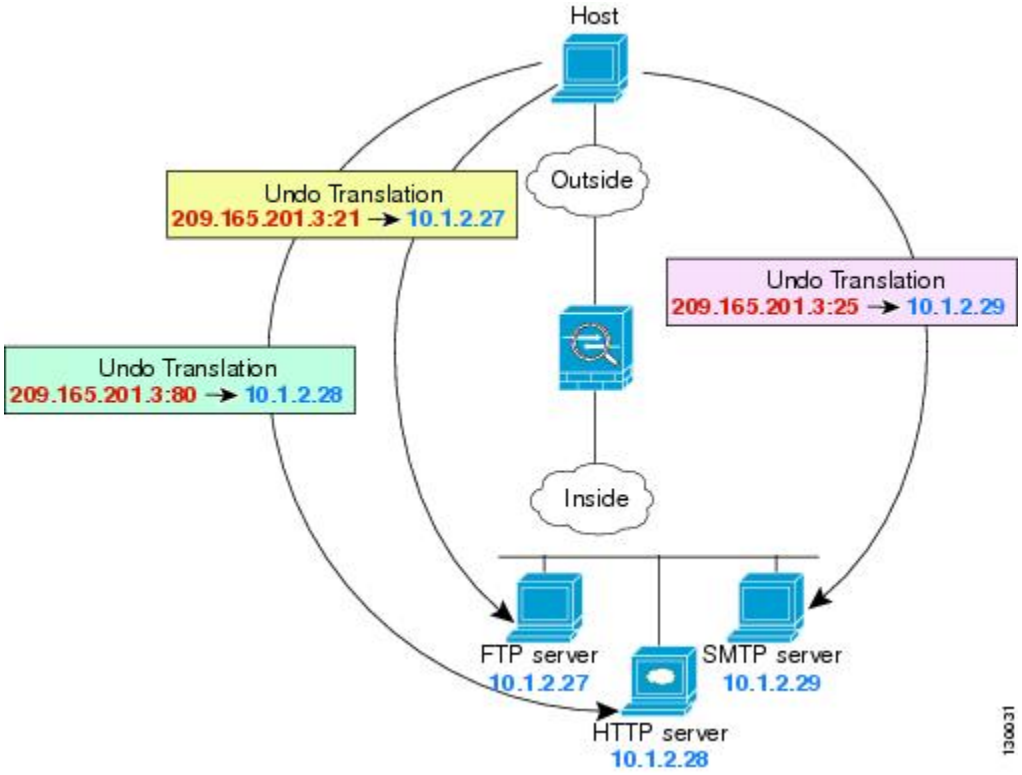


ステップ 6 [OK] をクリックして [Edit Network Object] ダイアログボックスに戻り、もう一度 [OK] をクリックし、[Apply] をクリックします。

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 ユーザは単一のアドレスで FTP、HTTP、および SMTP にアクセスできるようになります。これらのサーバは実際には、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することができます。

図 *4:* ポート変換を設定したスタティック *NAT*



手順

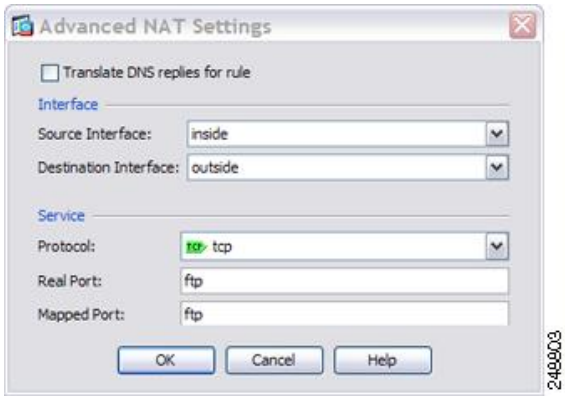
ステップ 1 **[Configuration]** > **[Firewall]** > **[NAT]** を選択します。

ステップ 2 FTP 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。

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 FTP サーバ 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。



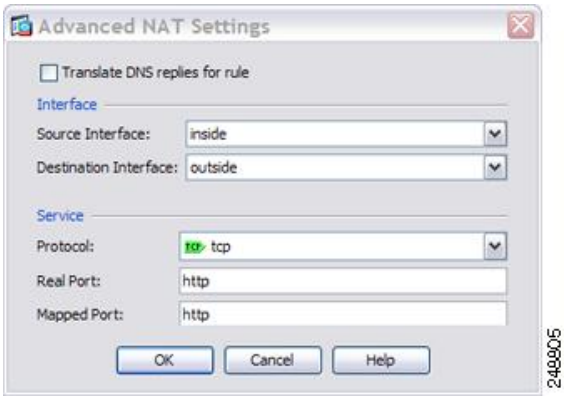
d) [OK] をクリックしてもう一度 [OK] をクリックし、ルールを保存して [NAT] ページに戻ります。

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。

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 HTTP サーバ 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。



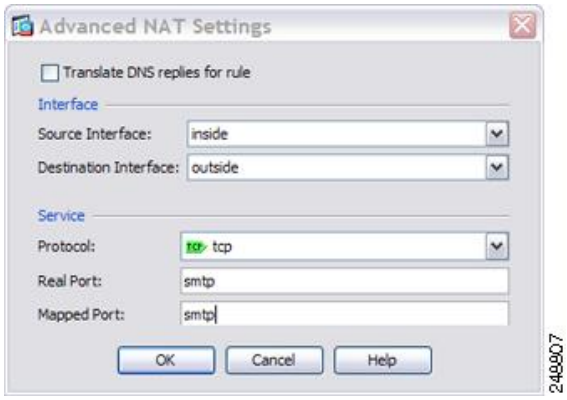
d) [OK] をクリックしてもう一度 [OK] をクリックし、ルールを保存して [NAT] ページに戻ります。

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。

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 SMTP サーバ 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 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。



d) [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、[Apply] をクリックします。

Twice NAT の例

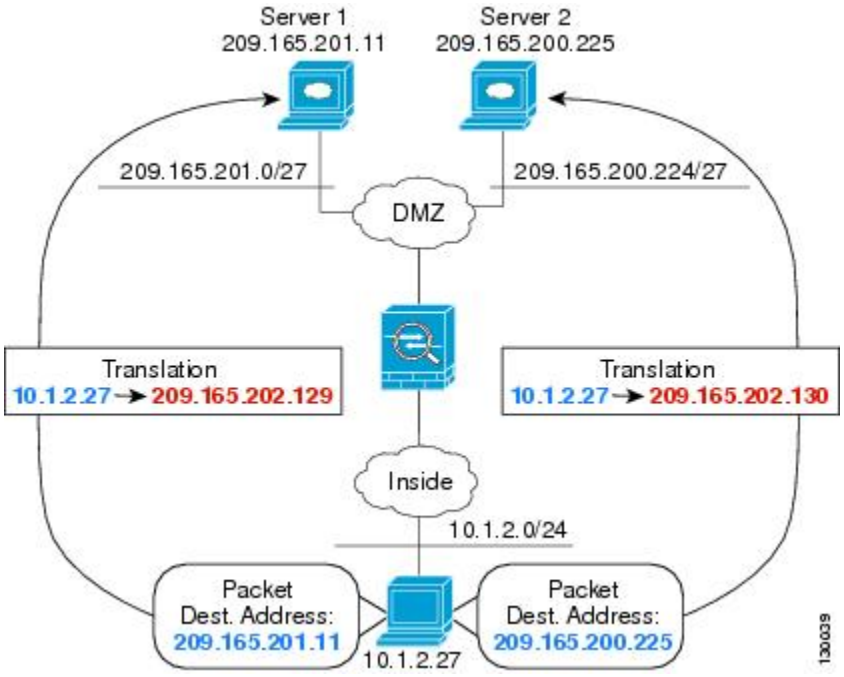
ここでは、次の設定例を示します。

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*

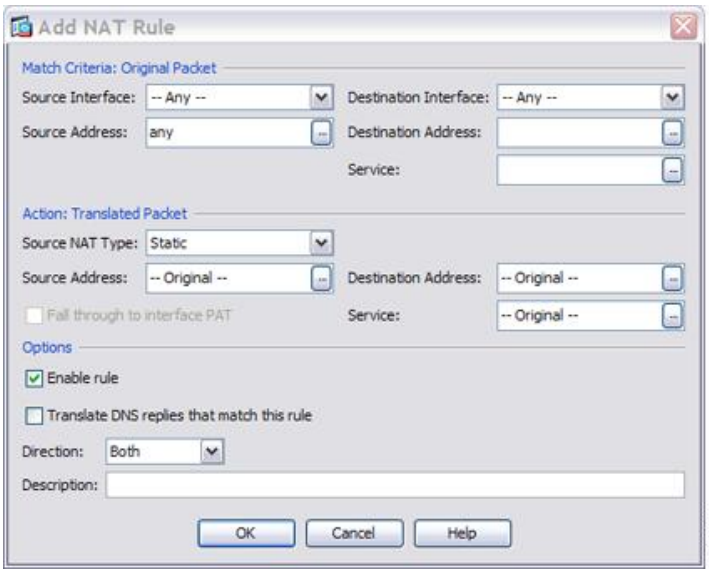


手順

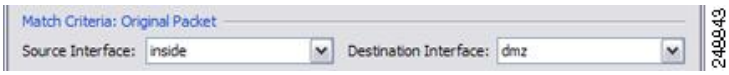
ステップ 1 **[Configuration]** > **[Firewall]** > **[NAT Rules]** ページで、**[Add]** > **[Add NAT Rule Before Network Object NAT Rules]** をクリックしてトラフィックの NAT ルールを内部ネットワークから DMZ ネットワーク 1 に追加します。

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。



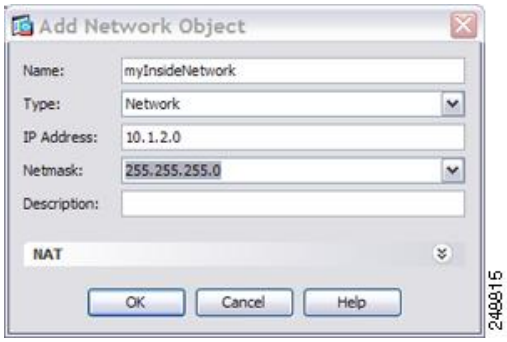
ステップ 2 送信元インターフェイスおよび宛先インターフェイスを設定します。



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。

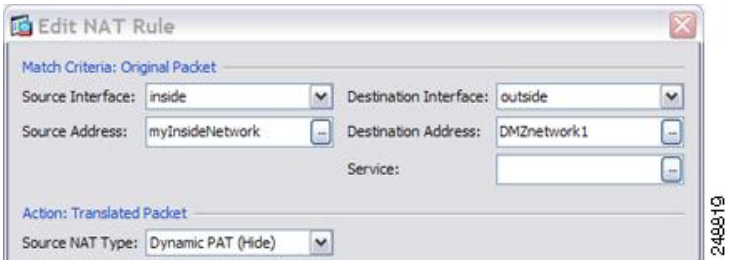
ステップ 4 [Original Destination Address] について、参照ボタンをクリックして、[Browse Original Destination Address] ダイアログボックスで DMZ ネットワーク 1 の新しいネットワーク オブジェクトを追加します。

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。

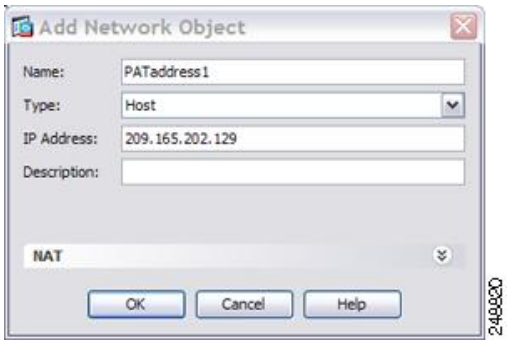
ステップ 5 NAT タイプを [Dynamic PAT (Hide)] に設定します。



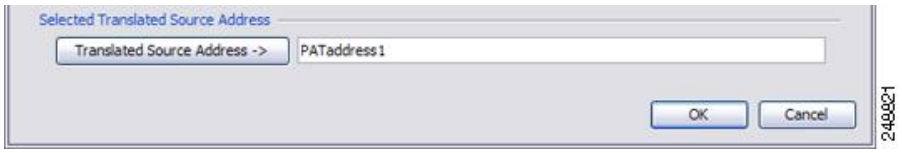
ステップ 6 [Translated Source Address] について、参照ボタンをクリックして、[Browse Translated Source Address] ダイアログボックスで PAT アドレスの新しいネットワーク オブジェクトを追加します。

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。

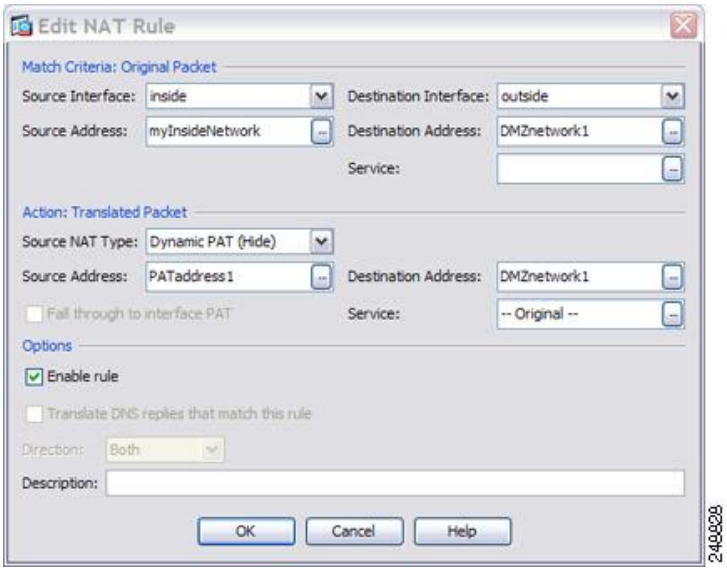


c) 新しいネットワーク オブジェクトをダブルクリックで選択します。[OK] をクリックして、NAT コンフィギュレーションに戻ります。



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。

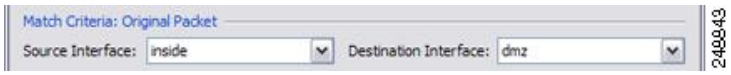
宛先アドレスは変換しないため、元の宛先アドレスと変換された宛先アドレスに同じアドレスを指定することによって、アイデンティティ NAT を設定する必要があります。



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。

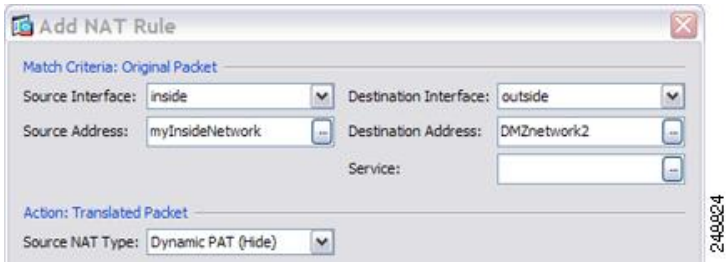
ステップ 12 [Original Destination Address] について、参照ボタンをクリックして、[Browse Original Destination Address] ダイアログボックスで DMZ ネットワーク 2 の新しいネットワーク オブジェクトを追加します。

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。

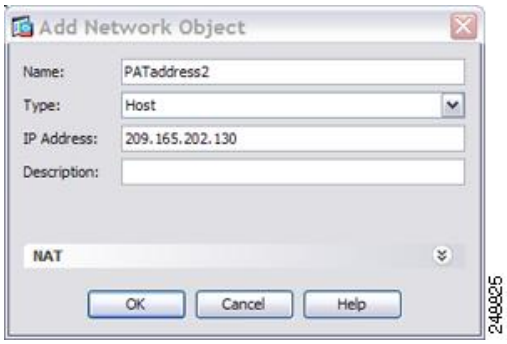
ステップ 13 NAT タイプを [Dynamic PAT (Hide)] に設定します。



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。

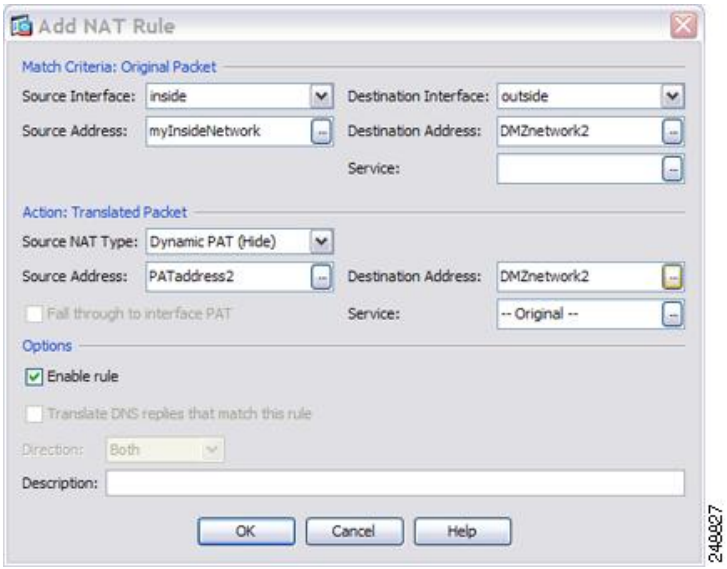
b) PAT アドレスを定義し、[OK] をクリックします。



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。



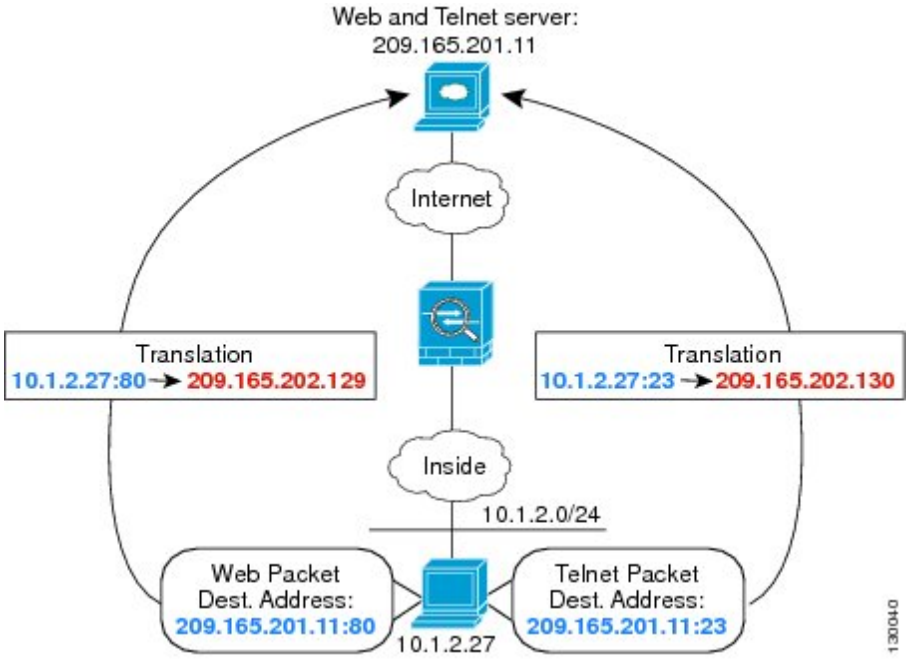
ステップ 16 [OK] をクリックして NAT テーブルにルールを追加します。

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にアクセスすると、実際のアドレスは 209.165.202.129:*port* 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にアクセスすると、実際のアドレスは 209.165.202.130:*port* に変換されます。

図 *6 :* 異なる宛先ポートを使用する *Twice NAT*

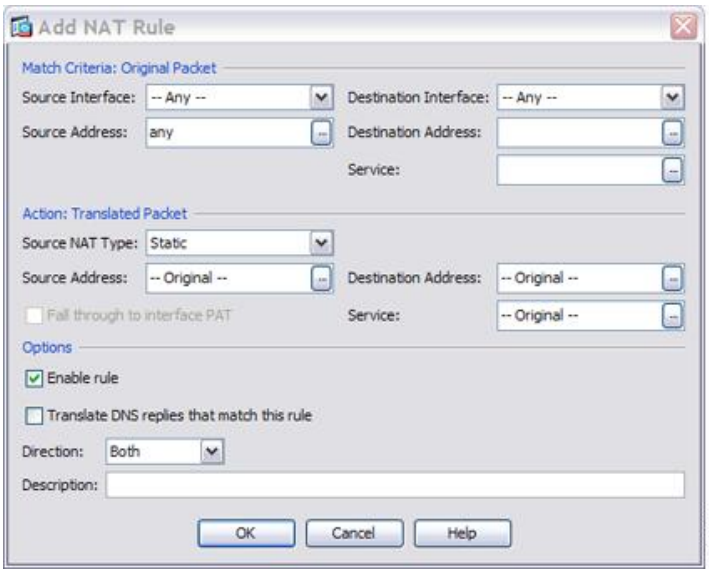


手順

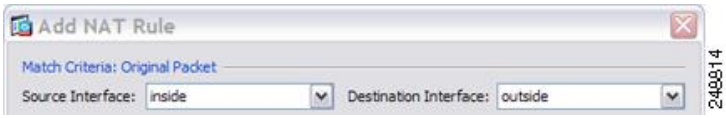
ステップ 1 **[Configuration]** > **[Firewall]** > **[NAT Rules]** ページで、**[Add]** > **[Add NAT Rule Before Network Object NAT Rules]** をクリックしてトラフィックの NAT ルールを内部ネットワークから Telnet サーバに追加します。

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。



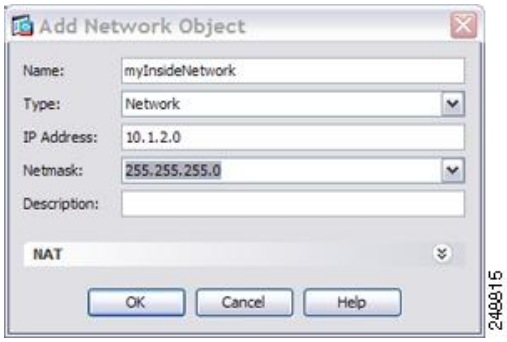
ステップ 2 送信元インターフェイスおよび宛先インターフェイスを設定します。



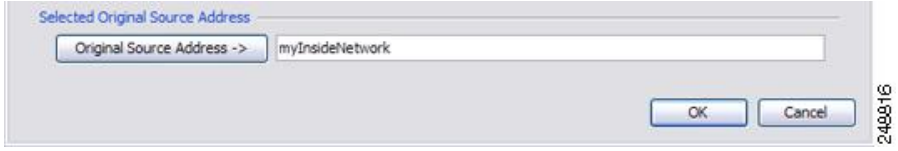
ステップ 3 [Original Source Address] について、参照ボタンをクリックして、[Browse Original Source Address] ダイアログボックスで内部ネットワークの新しいネットワーク オブジェクトを追加します。

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。

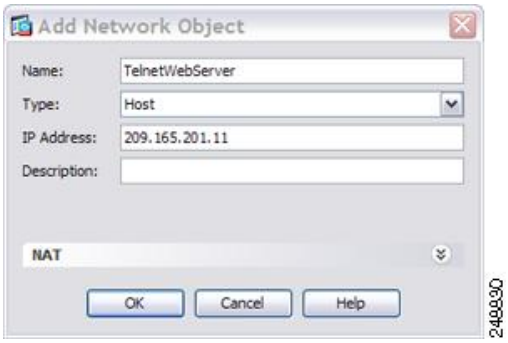


c) 新しいネットワーク オブジェクトをダブルクリックで選択します。[OK] をクリックして、NAT コンフィギュレーションに戻ります。



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。

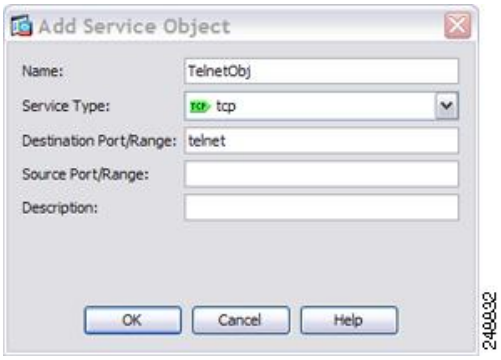
a) [Add] > [Network Object] を選択します。
b) サーバ アドレスを定義し、[OK] をクリックします。



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。

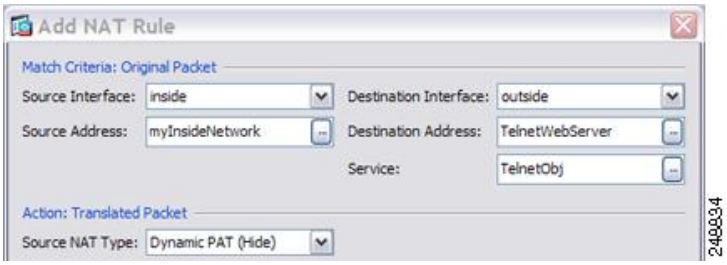
ステップ 5 [Original Service] について、参照ボタンをクリックして、[Browse Original Service] ダイアログボックスで Telnet の新しいサービス オブジェクトを追加します。

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。

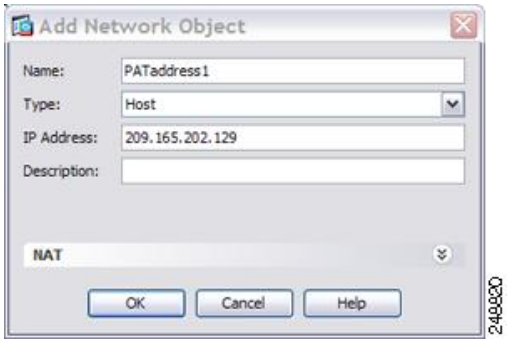
ステップ 6 NAT タイプを [Dynamic PAT (Hide)] に設定します。



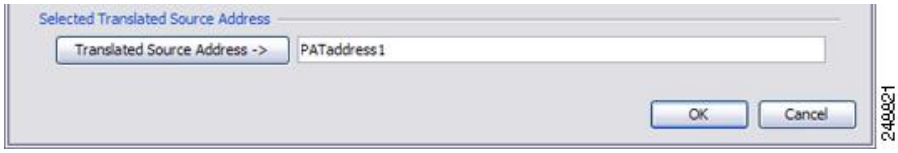
ステップ 7 [Translated Source Address] について、参照ボタンをクリックして、[Browse Translated Source Address] ダイアログボックスで PAT アドレスの新しいネットワーク オブジェクトを追加します。

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。

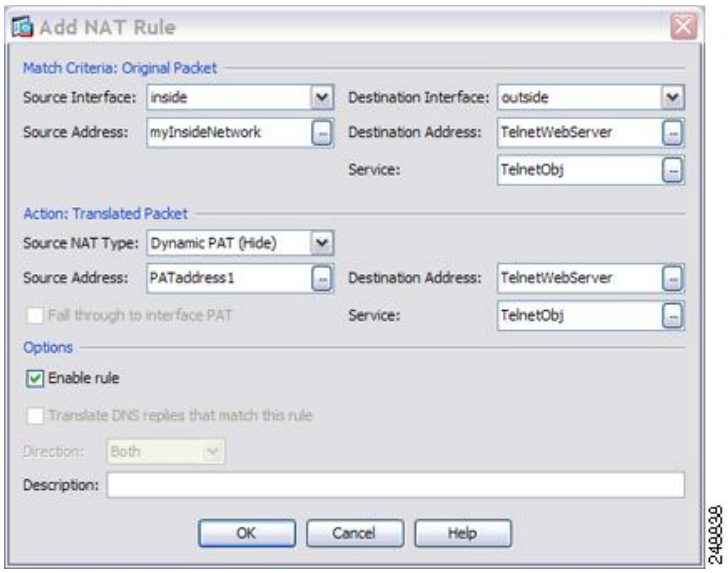


c) 新しいネットワーク オブジェクトをダブルクリックで選択します。[OK] をクリックして、NAT コンフィギュレーションに戻ります。



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。

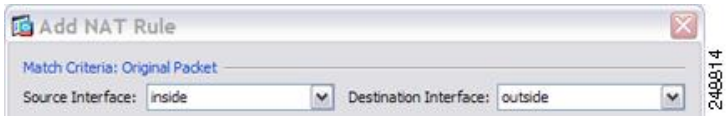
宛先アドレスは変換しないため、元の宛先アドレスと変換された宛先アドレスに同じアドレスを指定することによって、アイデンティティ NAT を設定する必要があります。



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。



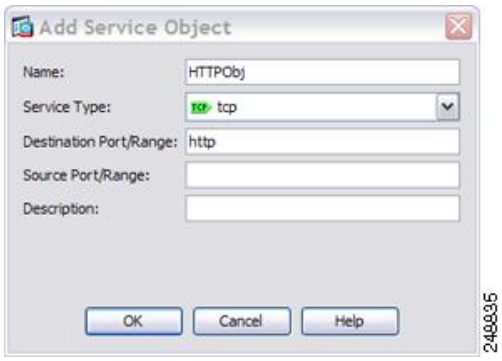
ステップ 12 [Original Source Address] について、内部ネットワーク オブジェクトの名前を入力するか（myInsideNetwork）、または参照ボタンをクリックして選択します。

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。

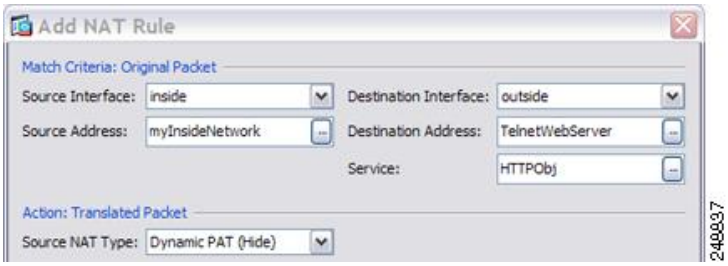
a) [Add] > [Service Object] を選択します。

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。

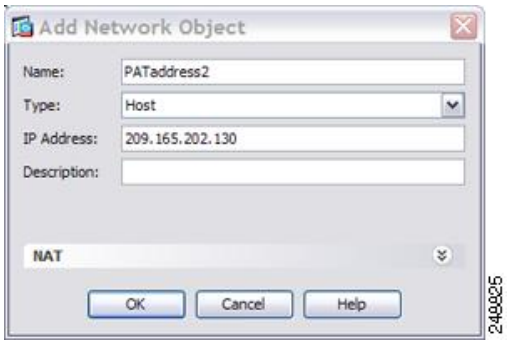
ステップ 15 NAT タイプを [Dynamic PAT (Hide)] に設定します。



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。

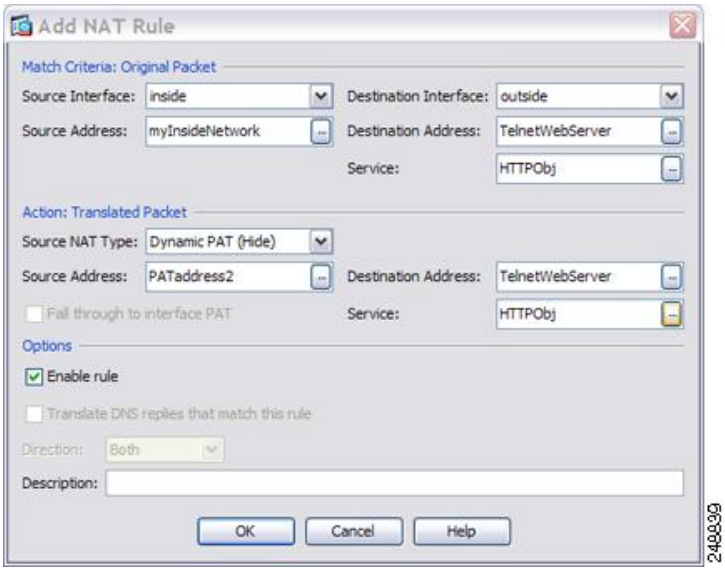
b) PAT アドレスを定義し、[OK] をクリックします。



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。



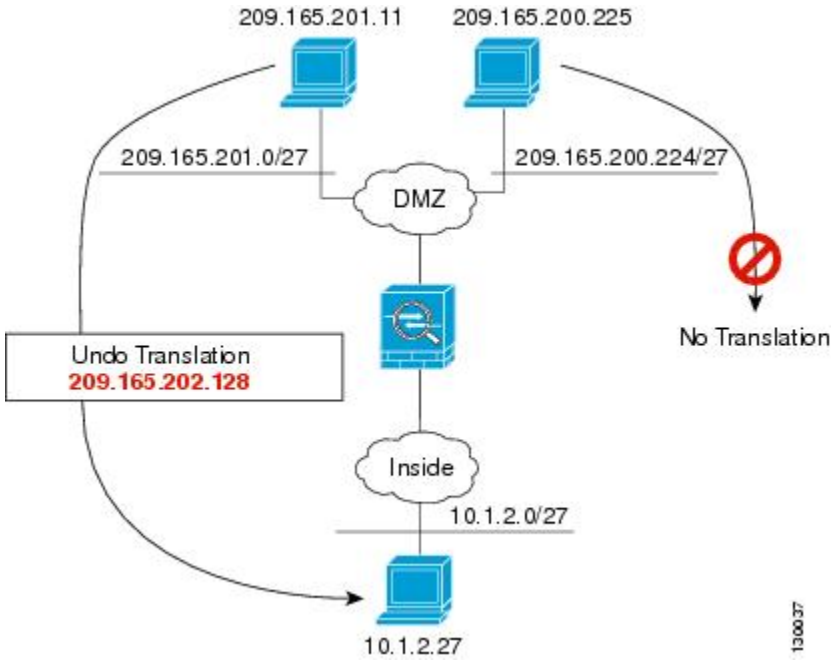
ステップ 18 [OK] をクリックして NAT テーブルにルールを追加します。

ステップ 19 [Apply] をクリックします。

例：宛先アドレス変換が設定された Twice NAT

次の図に、マッピングされるホストに接続するリモート ホストを示します。マッピングされるホストには、209.165.201.0/27 ネットワークが起点または終点となるトラフィックに限り実際のアドレスを変換するスタティック Twice NAT 変換が設定されています。209.165.200.224/27 ネットワーク用の変換は存在しません。したがって、変換済みのホストはそのネットワークに接続できず、そのネットワークのホストも変換済みのホストに接続できません。

図 *7:* 宛先アドレス変換が設定されたスタティック *Twice NAT*



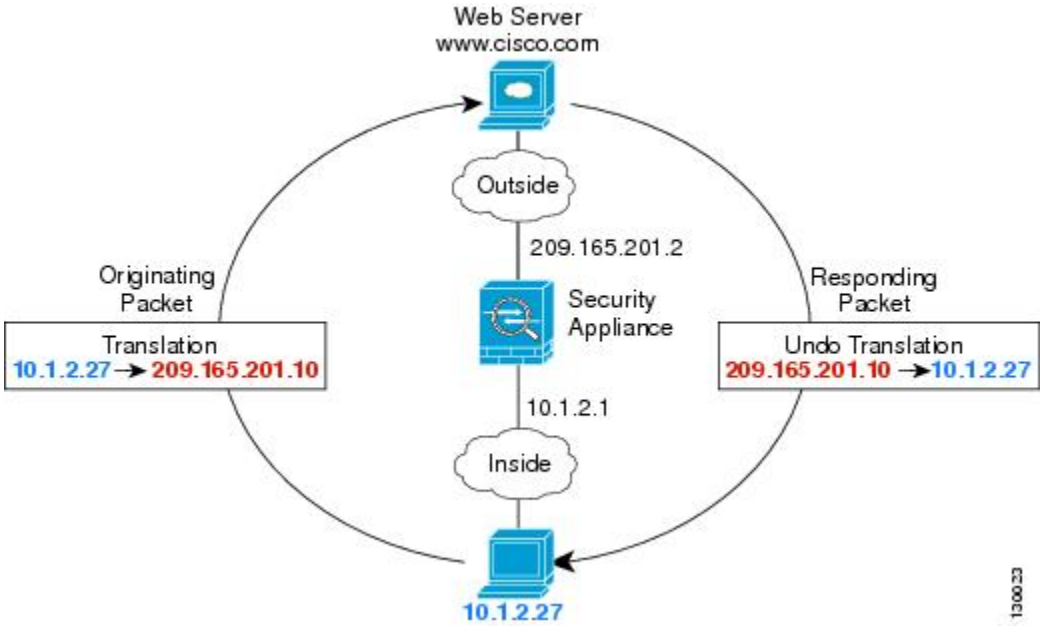
ルーテッド モードとトランスペアレント モードの NAT

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 *8 : 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 ルータが必要なくなります。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。

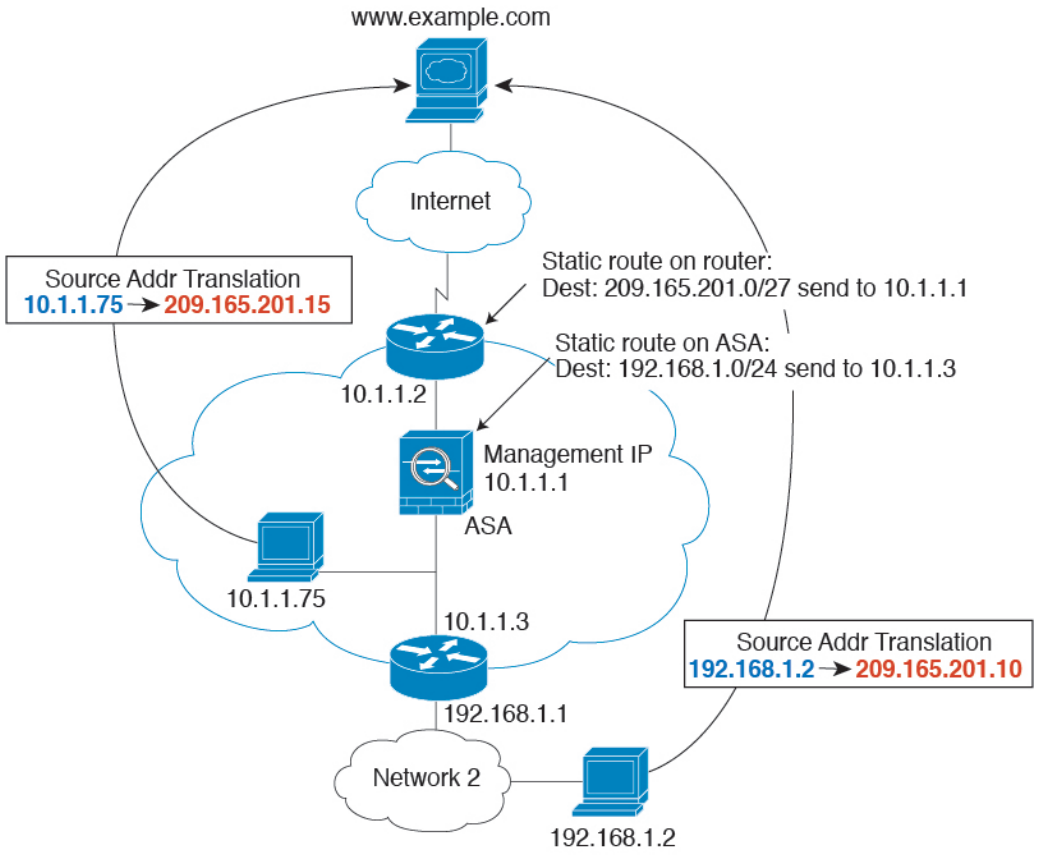
トランスペアレント モードまたは同じブリッジ グループのメンバー間のルーテッド モードの NAT には、以下の要件および制限があります。

- 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、トランスペアレント 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ペアレント 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 *9 : NAT* の例 : トランスペアレント モード



1. 内部ホスト 10.1.1.75 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 10.1.1.75 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 ルートのこのマッピング 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 10.1.1.1.75 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ので、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。**[Configuration]** > **[Device Management]** > **[Advanced]** > **[ARP]** > **[ARP Static Table]** の順に選択し、ARP を設定します。

固有のネットワーク上のアドレス

宛先（マッピングされた）インターフェイス ネットワークで使用可能なアドレスより多くのアドレスが必要な場合は、別のサブネット上のアドレスを識別できます。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 NAT を使用し、マッピング IP アドレス 209.165.201.5 を使用する場合は、209.165.201.5 255.255.255.255（ホスト アドレス）のスタティック ルートを再配布可能な 10.1.1.99 ゲートウェイに設定できます。

```
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、アップストリーム ルータのスタティック ルートで代わりにダウンストリーム ルータの IP アドレスを指定できます。

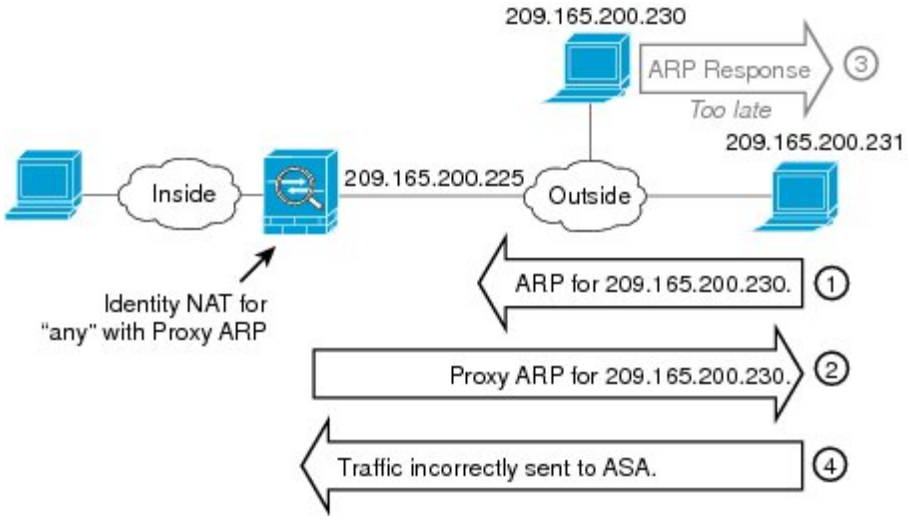
実際のアドレスと同じアドレス（アイデンティティ NAT）

（8.3(1)、8.3(2)、8.4(1)）アイデンティティ NAT のデフォルト動作で、プロキシ ARP はディセーブルにされます。これは設定できません。

（8.4(2) 以降）アイデンティティ NAT のデフォルト動作で、プロキシ ARP はイネーブルにされ、他のスタティック NAT ルールと一致します。必要に応じてプロキシ ARP をディセーブルにできます。必要に応じて標準スタティック NAT のプロキシ ARP をディセーブルにできます。その場合は、アップストリーム ルータの適切なルートがあることを確認する必要があります。

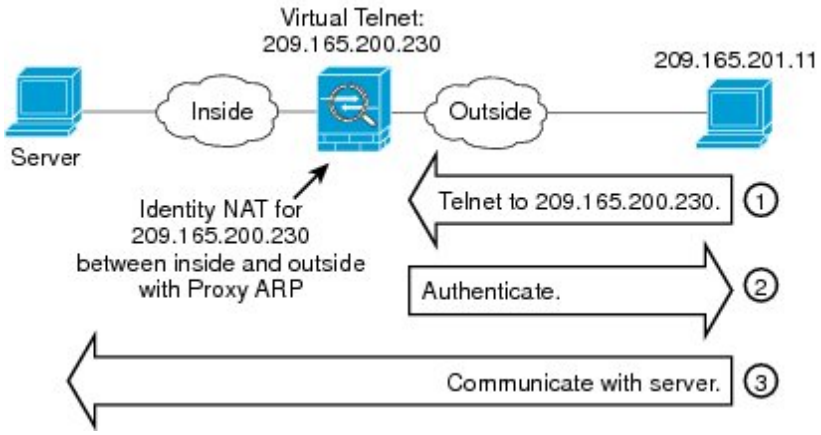
アイデンティティ NAT の場合、通常はプロキシ ARP が不要で、場合によっては接続性に関する問題を引き起こす可能性があります。たとえば、任意の IP アドレスの広範なアイデンティティ NAT ルールを設定した場合、プロキシ ARP をイネーブルのままにしておくと、マッピング インターフェイスに直接接続されたネットワーク上のホストの問題を引き起こすことがあります。この場合、マッピング ネットワークのホストが同じネットワークの他のホストと通信すると、ARP 要求内のアドレスは（任意のアドレスと一致する）NAT ルールと一致します。このとき、実際には ASA 向けのパケットでない場合でも、ASA 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 *10 :* 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 *11 :* 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。

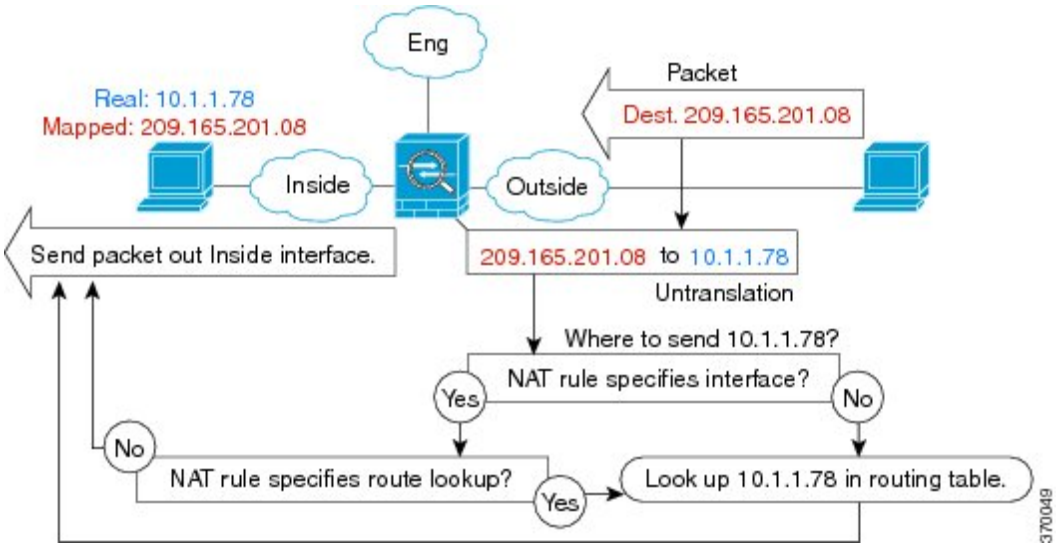
出力インターフェイスの決定

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力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力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力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力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 コンフィギュレーション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力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力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 *12 : NAT* によるルーテッド モードでの出力インターフェイスの選択



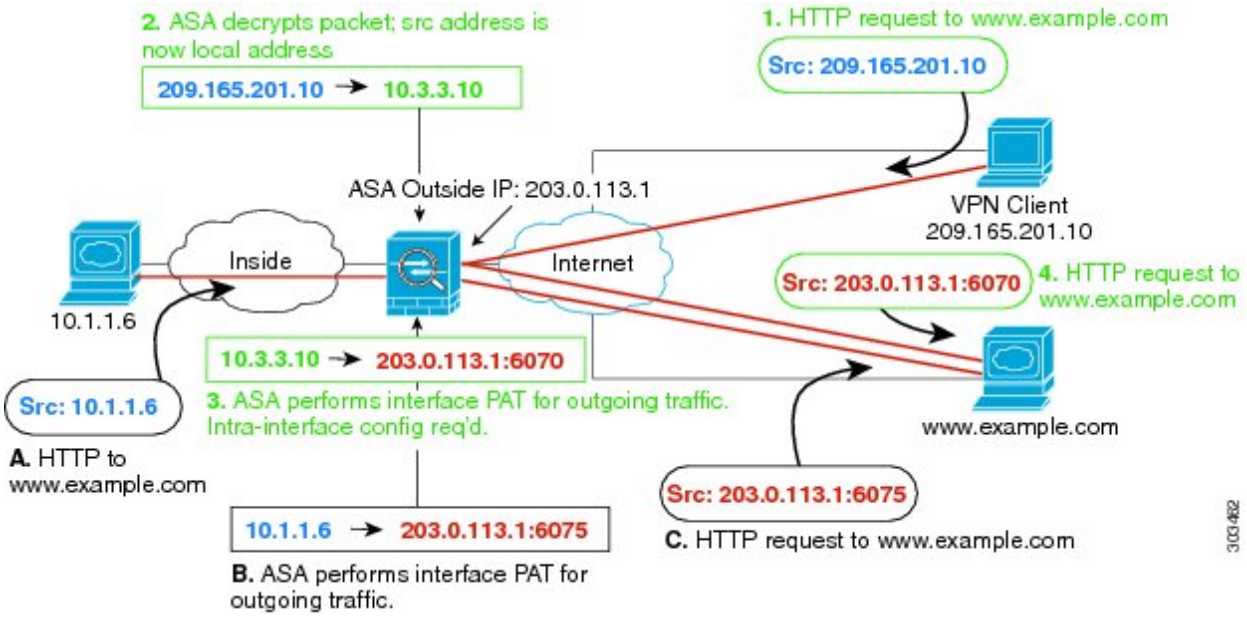
VPN の NAT

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

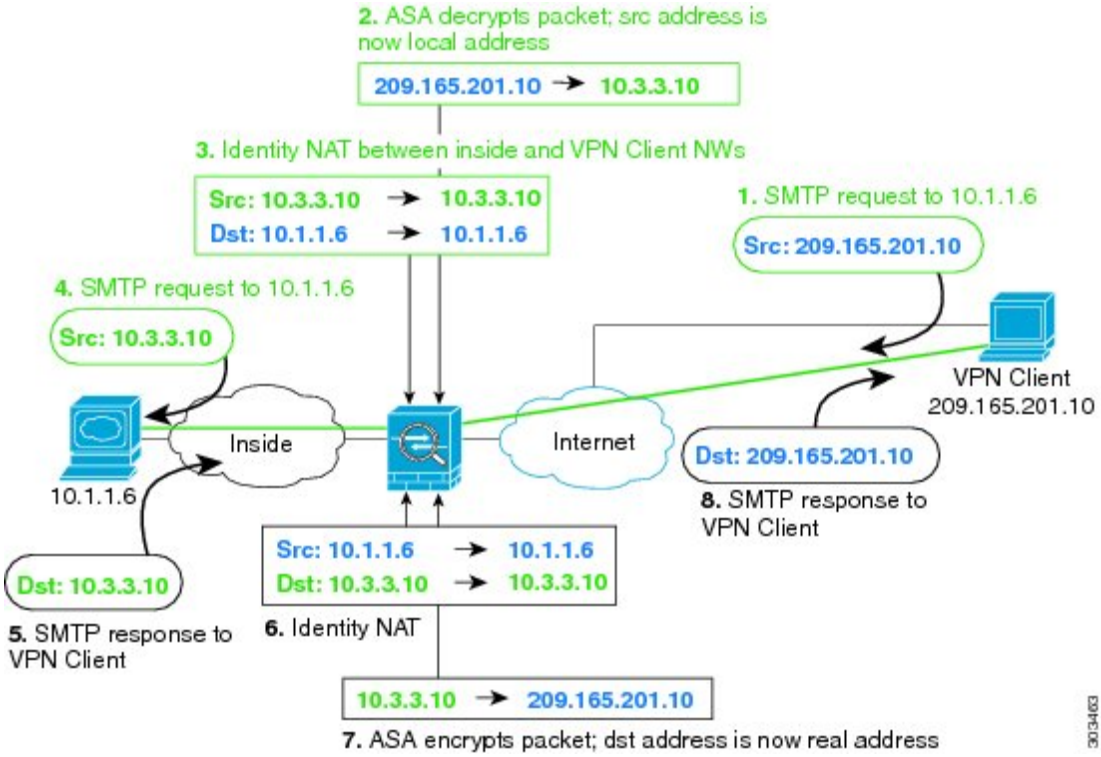
次の図に、内部サーバ（10.1.1.6）とインターネットにアクセスする VPN クライアント（209.165.201.10）の両方を示します。VPN クライアント用のスプリット トンネリング（指定したトラフィックのみがVPNトンネル上でやりとりされる）を設定しない限り、インターネット バインドされた VPN トラフィックも ASA を経由する必要があります。VPN トラフィックが ASA に渡されると、ASA はパケットを復号化し、得られたパケットには送信元として VPN クライアント ローカル アドレス（10.3.3.10）が含まれています。内部ネットワークと VPN クライアント ローカル 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 ネットワーキング」）をイネーブルにする必要があります。

図 *13 :* 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（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 は同じアドレスにアドレスを変換します。

図 *14 : VPN* クライアントのアイデンティティ *NAT*



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。

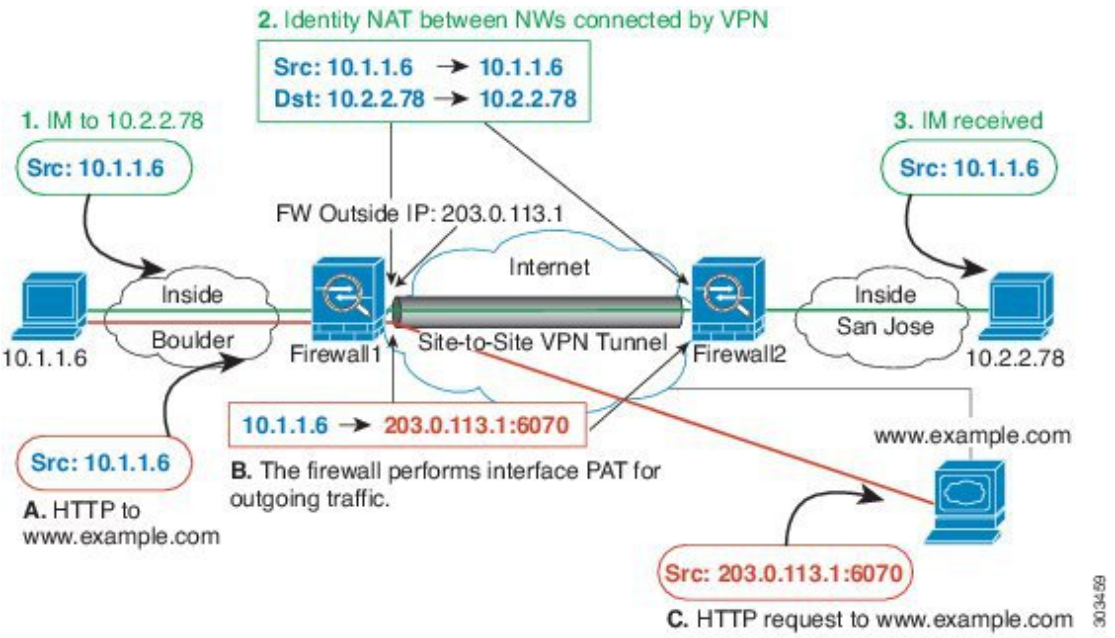
```
! Enable hairpin for non-split-tunneled VPN client traffic:
same-security-traffic permit intra-interface

! 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 およびサイトツーサイト 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

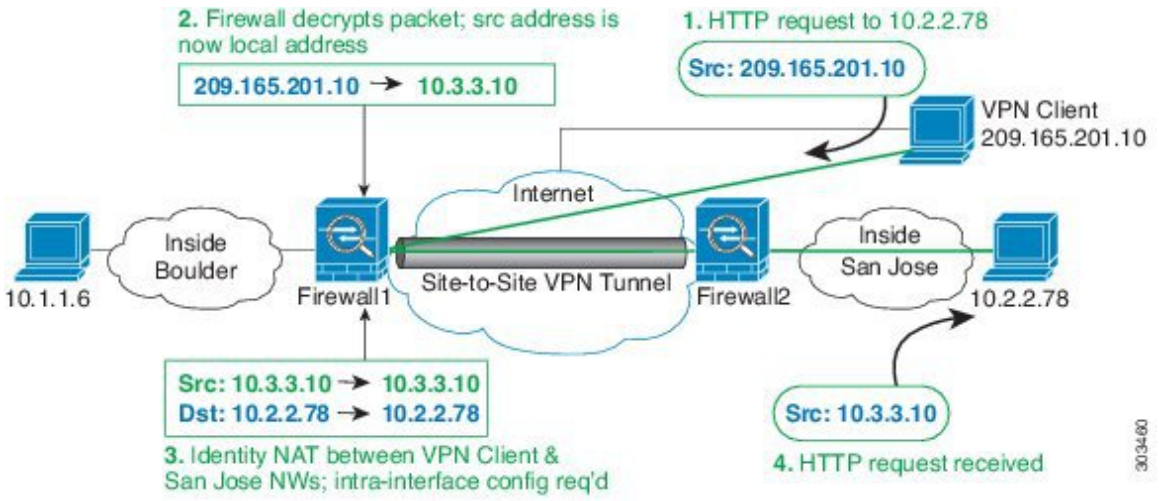
す。ただし、VPN トンネルを経由するトラフィックについては（たとえば、ボールダーの 10.1.1.6 からサンノゼの 10.2.2.78 へ）、NAT を実行しません。そのため、アイデンティティ NAT ルールを作成して、そのトラフィックを除外する必要があります。アイデンティティ NAT は同じアドレスにアドレスを変換します。

図 *15*：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（ボールダー）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（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ダ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 を設定する必要もあります。

図 *16 :* 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
```

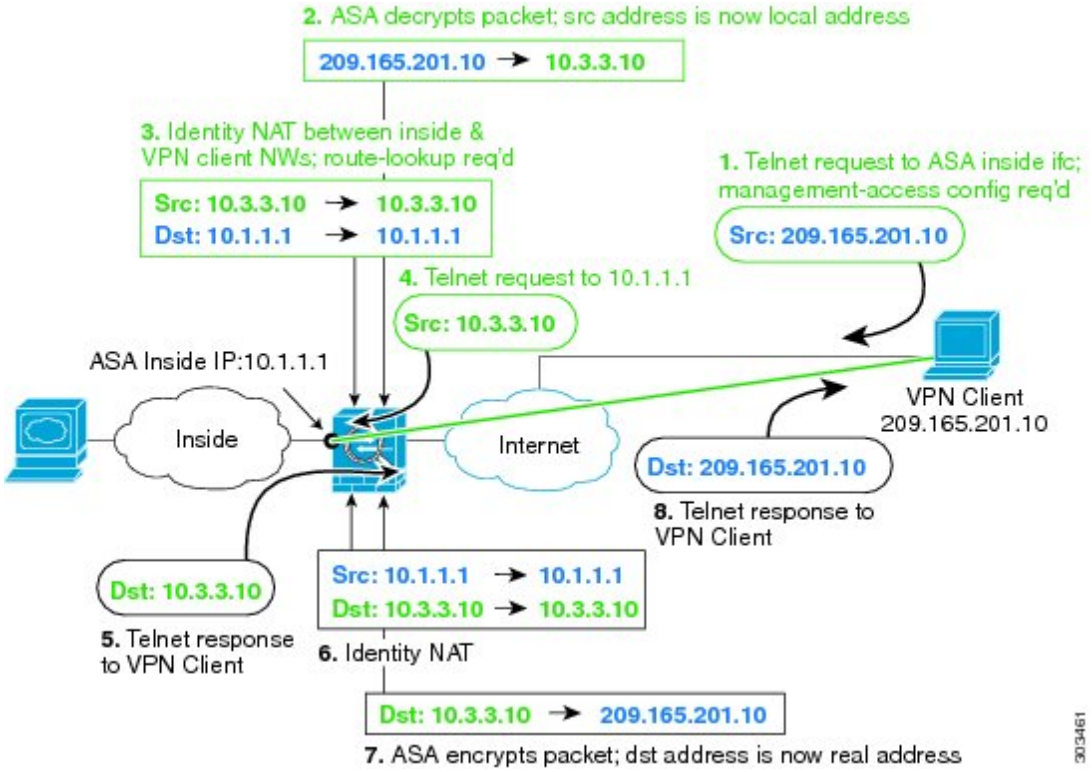
```
subnet 10.2.2.0 255.255.255.0
nat (inside,outside) dynamic interface

! 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 （36 ページ）またはNAT およびサイトツーサイト VPN （38 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 （35 ページ）を参照してください。

図 *17 : VPN* 管理アクセス



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 のみと IPv4 のみのネットワーク間でトラフィックを通過させる必要がある場合、アドレス タイプの変換に NAT を使用する必要があります。2 つの IPv6 ネットワークでも、外部ネットワークから内部アドレスを非表示にする必要がある場合もあります。

IPv6 ネットワークで次の変換タイプを使用できます。

- NAT64、NAT46：IPv6 パケットを IPv4 パケットに（またはその逆に）変換します。2 つのポリシー、IPv6 から IPv4 への変換、および IPv4 から IPv6 への変換を定義する必要があります。これは 1 つの twice NAT ルールで実現できますが、DNS サーバが外部ネットワークにある場合は、おそらく 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 はスタティック マッピングのみをサポートします。

- 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 を使用することを推奨します。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。

（注） NAT64 および NAT 46 は標準ルーテッド インターフェイスでのみ有効です。NAT66 はルーテッドおよびブリッジ グループ メンバーのインターフェイスの両方で有効です。

NAT64/46：IPv6 アドレスの IPv4 への変換

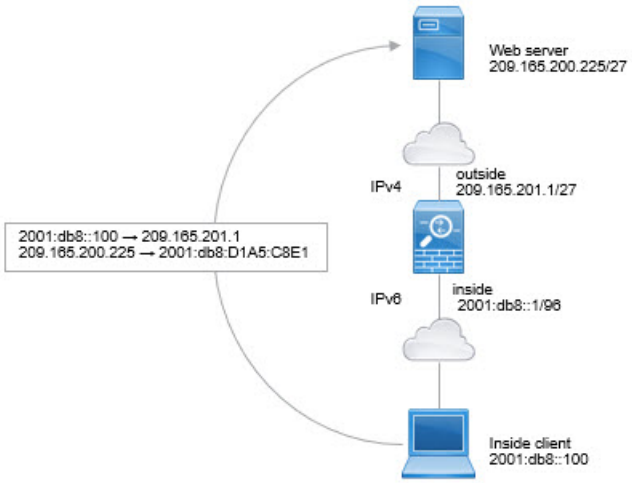
トラフィックが IPv6 ネットワークから IPv4 のみのネットワークにアクセスするときは、IPv6 アドレスを IPv4 アドレスに変換し、IPv4 から IPv6 へトラフィックが返される必要があります。2 つのアドレス プールを定義する必要があります。IPv4 ネットワークでの IPv6 アドレスをバインドする IPv4 アドレス プールと、IPv6 ネットワークの IPv4 アドレスをバインドする IPv6 アドレス プールです。

- NAT64 ルールの IPv4 アドレス プールは通常小さく、IPv6 クライアント アドレスとの 1 対 1 のマッピングを行うのに十分なアドレスがない可能性があります。ダイナミック PAT はダイナミックまたはスタティック NAT と比較して、より簡単に多数の IPv6 クライアント アドレスに対応できます。
- NAT46 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、またはそれを超える数が可能です。これにより、各 IPv4 アドレスを異なる IPv6 アドレスにマッピングできるようになります。NAT46 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 ネットワーク用と、宛先 IPv4 ネットワーク用の 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 ルールで実現できますが、DNS サーバが外部ネットワークにある場合は、おそらく 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

次に示すのは単純な例で、IPv6 のみの内部ネットワークがあり、インターネットに送信するトラフィックについて IPv4 に変換する必要があります。この例では DNS 変換の必要がないことを前提としています。そのため、単一の 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 アドレスとダイナミック PAT インターフェイスを使用して、内部 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静的に変換され、内部ネットワークでの送信が許可されます。

手順

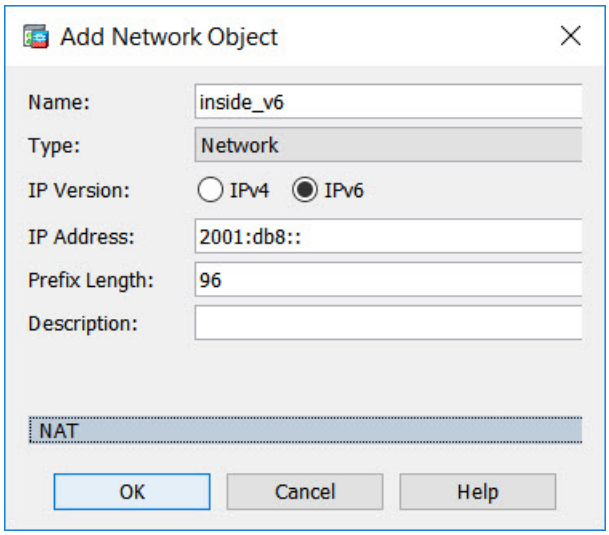
ステップ 1 内部 IPv6 ネットワークのためのネットワーク オブジェクトを作成します。

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。

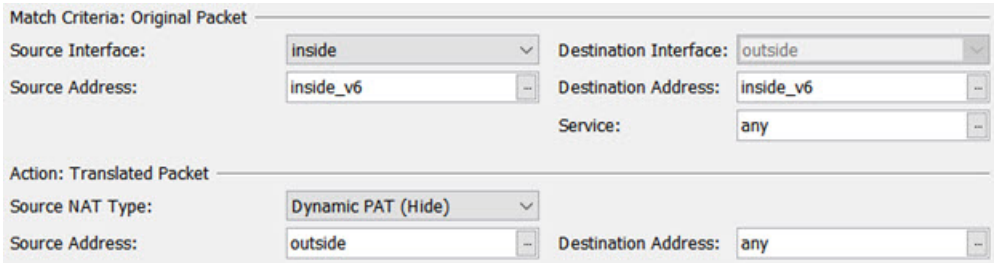
- Destination Address：inside_v6 ネットワークオブジェクトを選択します。
- Service：デフォルトの [any] を維持します。

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。

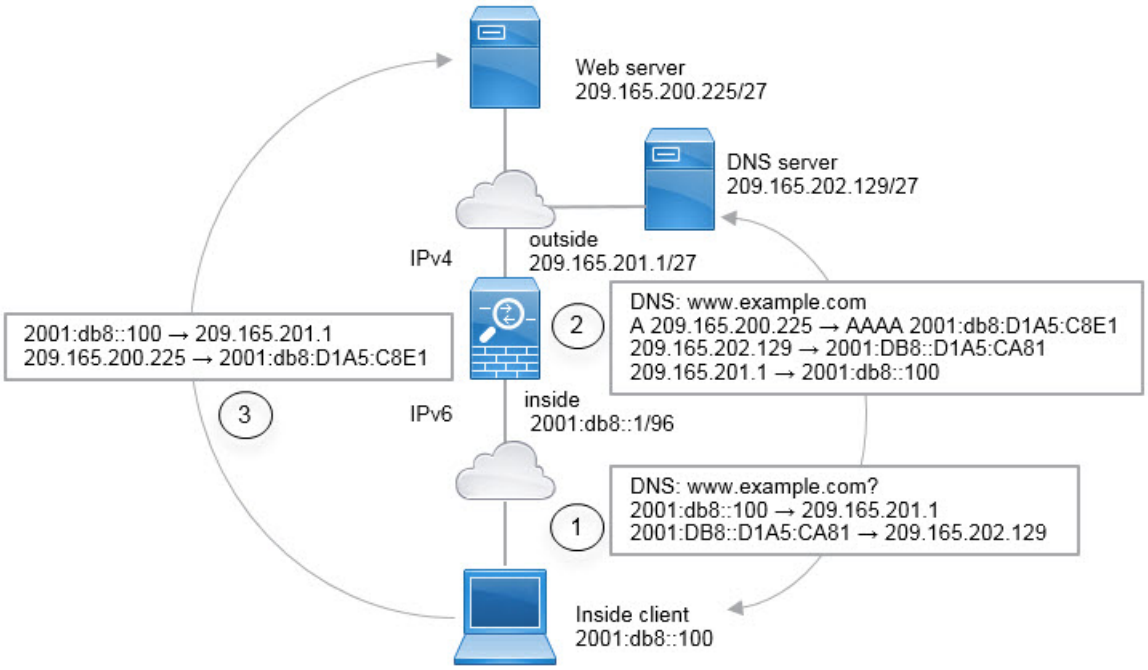


e) [OK] をクリックします。

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

以下は、IPv6 のみの内部ネットワークがあり、外部のインターネットに内部ユーザが必要とする IPv4 のみのサービスがある場合の代表的な例です。



この例では、外部インターフェイスの IP アドレスとダイナミック PAT インターフェイスを使用して、内部 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静的に変換され、内部ネットワークでの送信が許可されます。外部 DNS サーバからの応答が A（IPv4）から AAAA（IPv6）レコードに変換され、アドレスが IPv4 から IPv6 に変換されるように、NAT46 ルールの DNS リライトを有効にします。

以下は、内部 IPv6 ネットワークの 2001:DB8::100 のクライアントが 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 コンピュータは 2001:DB8::D1A5:CA81 の DNS サーバに DNS 要求を送信します。NAT ルールが DNS 要求の送信元と宛先に対して次の変換を行います。
   - 2001:DB8::100 から 209.165.201.1 の一意のポートへ（NAT64 インターフェイス PAT ルール）
   - 2001:DB8::D1A5:CA81 から 209.165.202.129 へ（NAT46 ルール。D1A5:CA81 は 209.165.202.129 に相当する IPv6 です）
2. DNS サーバは、www.example.com が 209.165.200.225 であることを示す A レコードを使用して応答します。DNS リライトが有効な NAT46 ルールは、A レコードを IPv6 相当の AAAA レコードに変換し、AAAA レコードで 209.165.200.225 を 2001:db8:D1A5:C8E1 に変換します。また、DNS 応答の送信元と宛先アドレスは、変換されません。
   - 209.165.202.129 から 2001:DB8::D1A5:CA81 へ
   - 209.165.201.1 から 2001:db8::100 へ

3. IPv6 クライアントは、Web サーバの IP アドレスを持つことになり、2001:db8:D1A5:C8E1 の www.example.com への HTTP 要求を作成します。（D1A5:C8E1 は 209.165.200.225 に相当する IPv6 です）HTTP 要求の送信元と宛先が次のように変換されます。
   - 2001:DB8::100 から 209.156.101.54 の一意のポートへ（NAT64 インターフェイス PAT ルール）
   - 2001:db8:D1A5:C8E1 から 209.165.200.225 へ（NAT46 ルール）

次の手順では、この例の指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。

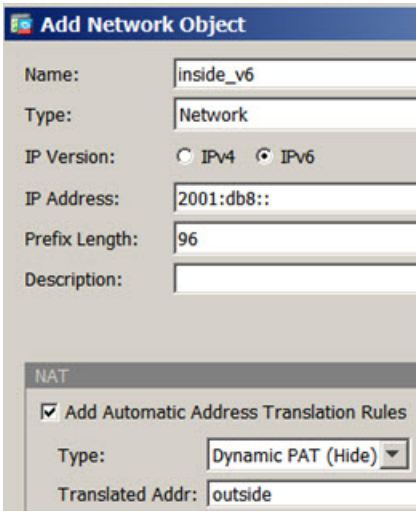
ステップ 2 内部 IPv6 ネットワークの NAT64 ダイナミック PAT ルールを設定します。

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。



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へのトラフィックは、外部インターフェイスの IPv4 アドレスを使用した NAT64 PAT 変換を取得します。

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。

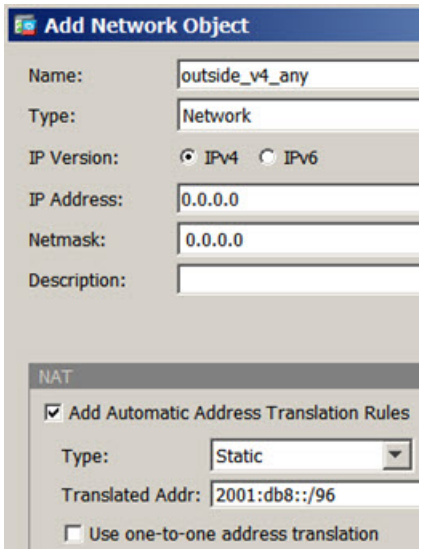
a) **[Add]** > **[Network Object NAT Rule]** の順に選択します。

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。

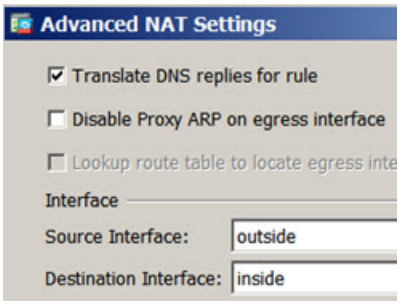
c) 基本的な NAT プロパティを設定します。

- NAT Type：[Static] を選択します。
- Translated Address：「2001:db8::/96」と入力します。



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。



e) [OK] をクリックして詳細設定を保存します。

f) [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に向かう外部ネットワークのすべての IPv4 アドレスは、組み込み IPv4 アドレス方式を使用して 2001:db8::/96 ネットワークのアドレスに変換されます。また、DNS 応答は A（IPv4）から AAAA（IPv6）レコードに変換され、アドレスは IPv4 から IPv6 に変換されます。

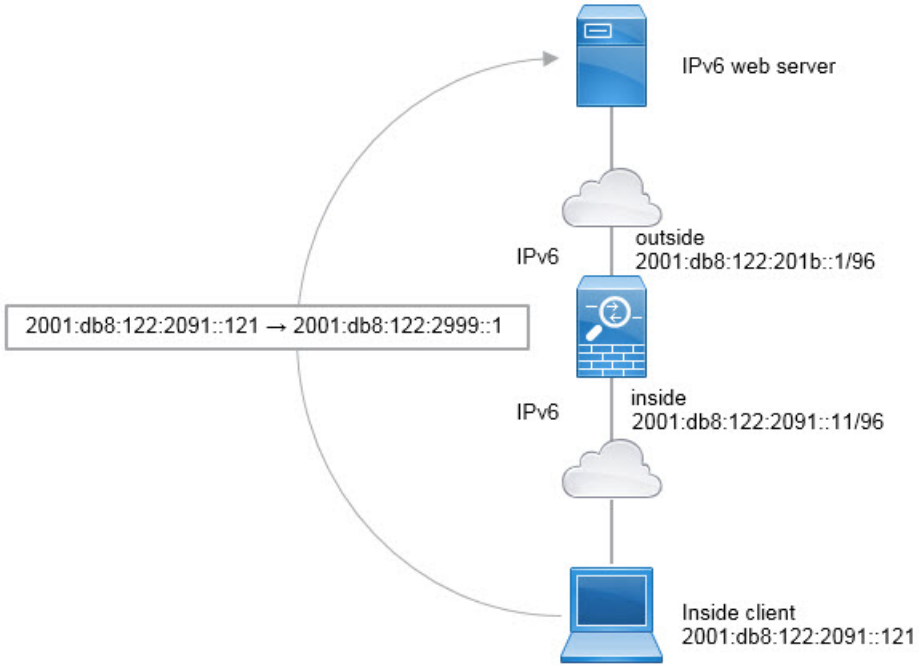
NAT66：IPv6 アドレスから別の IPv6 アドレスへの変換

IPv6 ネットワークから別の IPv6 ネットワークへ移動するとき、その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 を使用することを推奨します。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 タイプの間で変換されていないため、NAT66 変換用の 1 つ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へ変換する方法について説明しています。



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。

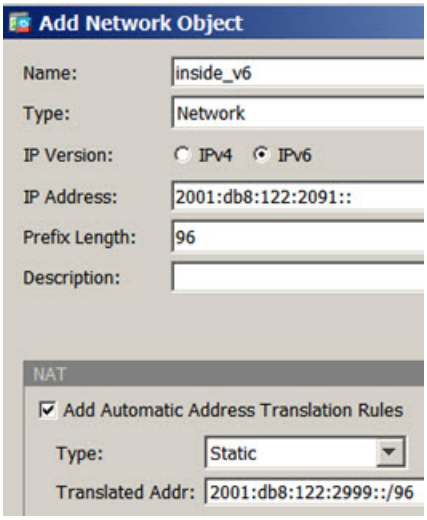
a) **[Add]** > **[Network Object NAT Rule]** の順に選択します。

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。



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。

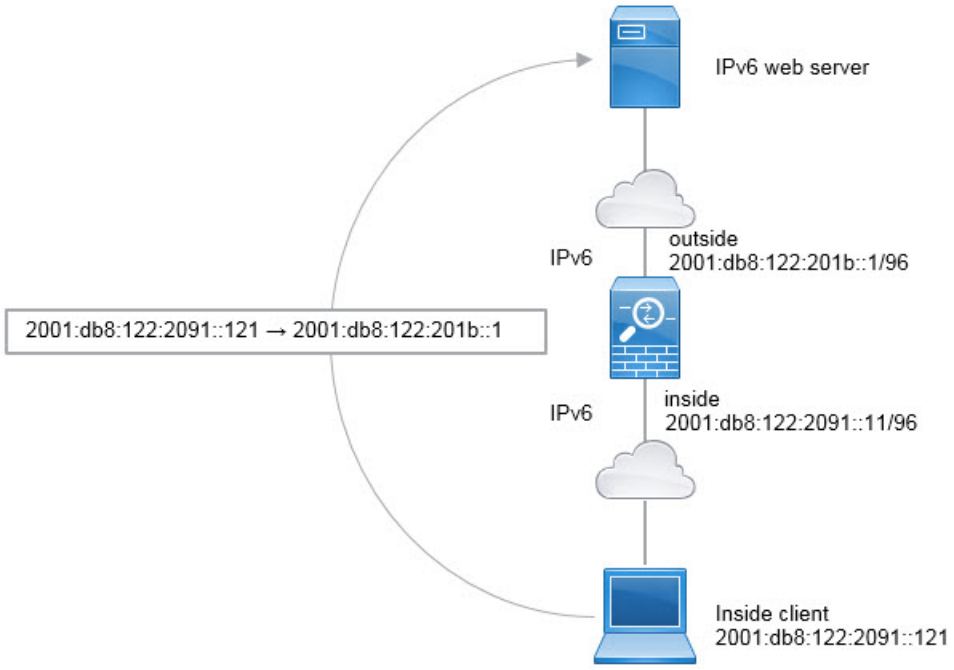
g) [OK] をクリックして NAT ルールを追加します。

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すべてのトラフィックは、2001:db8:122:2999::/96 ネットワークのアドレスへのスタティック NAT66 変換を取得します。

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 IPv6 アドレスの別のポートに内部アドレスを動的に割り当てることです。

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 アドレスは、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またはサイトローカル アドレスは、PAT に使用されません。



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。

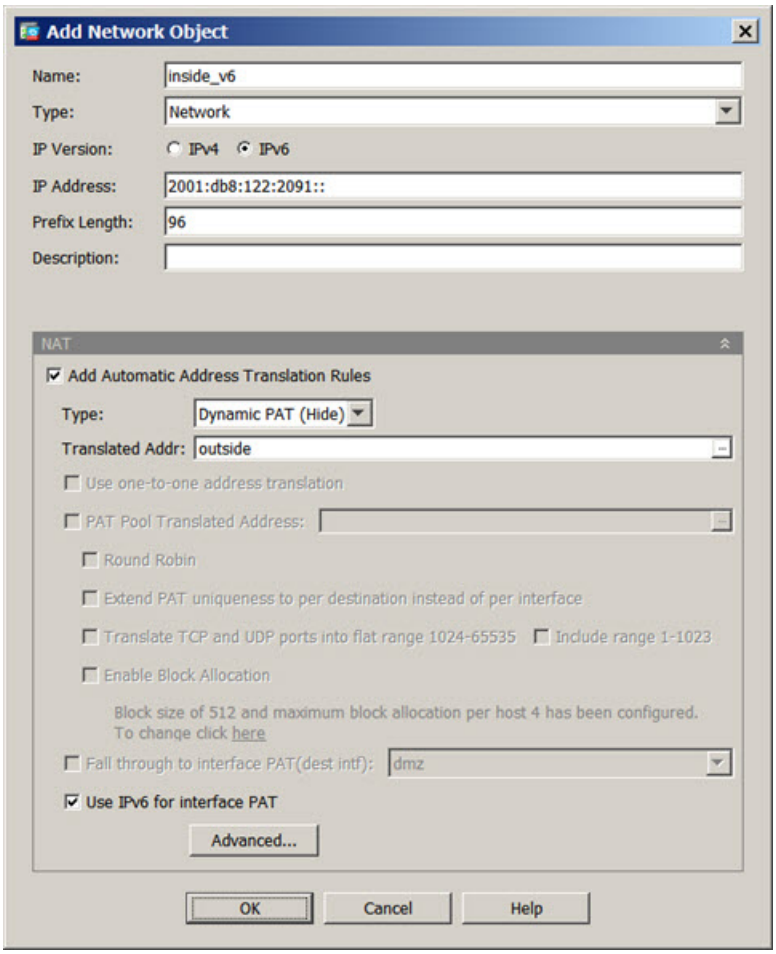
b) 基本的なオブジェクト プロパティを設定します。

- 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。



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への NAT66 PAT 変換を取得します。

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 コンフィギュレーション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リライトされます。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。

NAT ルールに DNS の書き換えを設定する必要が生じる主な状況を次に示します。

- ルールが NAT64 または NAT46 で、DNS サーバが外部ネットワークにある場合。DNS A レコード（IPv4 向け）と AAAA レコード（IPv6 向け）間の変換のために DNS を書き換える場合。
- DNS サーバが外部に、クライアントが内部にあり、クライアントが使用する完全修飾ドメイン名を解決すると他の内部ホストになる場合。
- DNS サーバが内部にあり、プライベート IP アドレスを使用して応答し、クライアントが外部にあり、クライアントが完全修飾ドメイン名を指定して内部にホストされているサーバをアクセスする場合。

DNS の書き換えの制限

次に DNS リライトの制限事項を示します。

- 個々の A レコードまたは 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 リライトは PAT には適用されません。
- twice NAT ルールを設定する場合、宛先アドレスおよび送信元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、ASA は、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 のルールに対して DNS NAT リライトを有効にした 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。DNS NAT のリライトを有効にした DNS アプリケーション インスペクションはデフォルトでグローバルに適用されるため、インスペクションの設定を変更する必要は通常ありません。
- 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、リライト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。

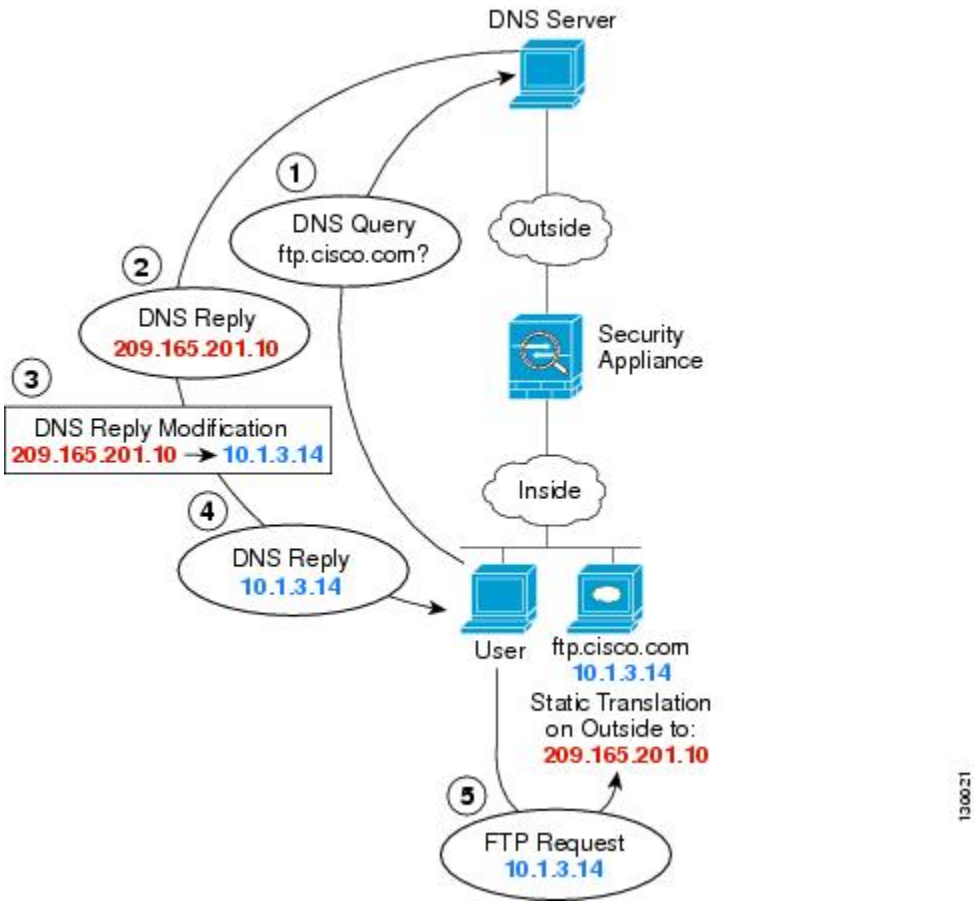
次のトピックで、NAT ルールの DNS リライトの例を示します。

DNS 応答修正：Outside 上の DNS サーバ

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可視のマッピング 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応答修正をイネーブルにする必要があります。これにより、実際のアドレスを使用してftp.cisco.comにアクセスすることを許可されている内部ユーザは、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サーバは応答でマッピング アドレス（209.165.201.10）を示します。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。

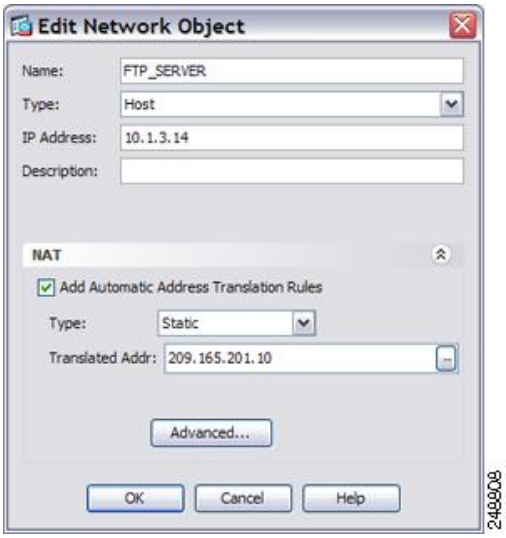


手順

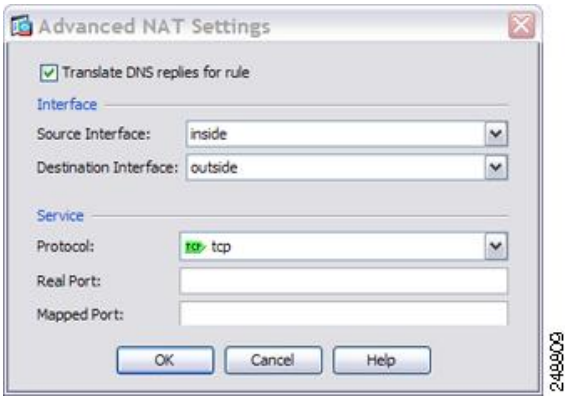
ステップ 1 **[Configuration]** > **[Firewall]** > **[NAT]** を選択します。

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 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。



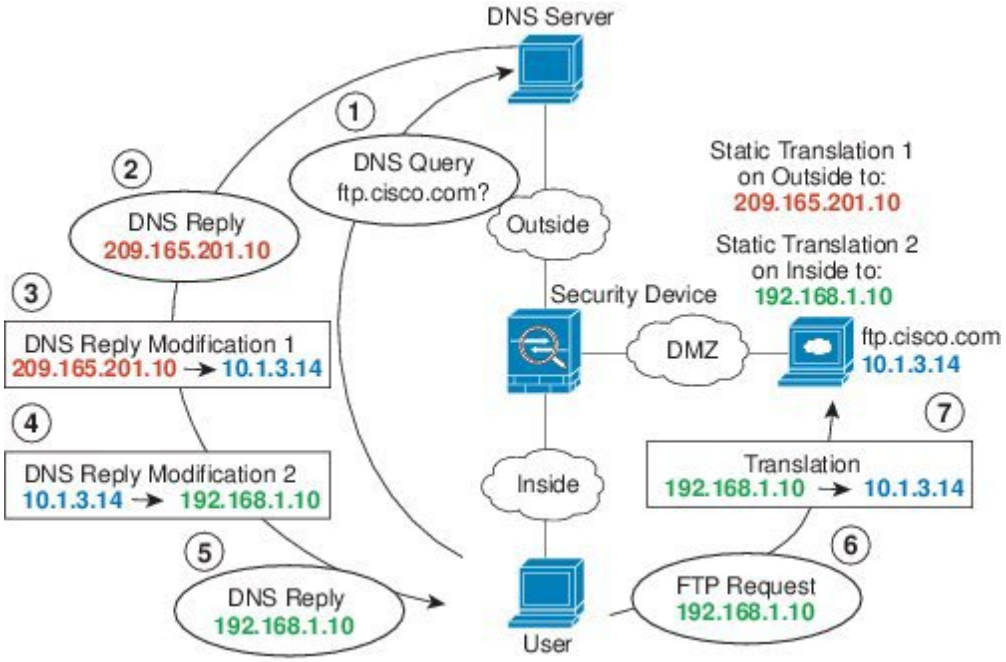
ステップ 5 [OK] をクリックして [Edit Network Object] ダイアログボックスに戻り、もう一度 [OK] をクリックし、[Apply] をクリックします。

DNS応答修正：別々のネットワーク上のDNSサーバ、ホスト、およびサーバ

次の図に、外部 DNS サーバから 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を示します。DNS サーバは、ユーザが 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。

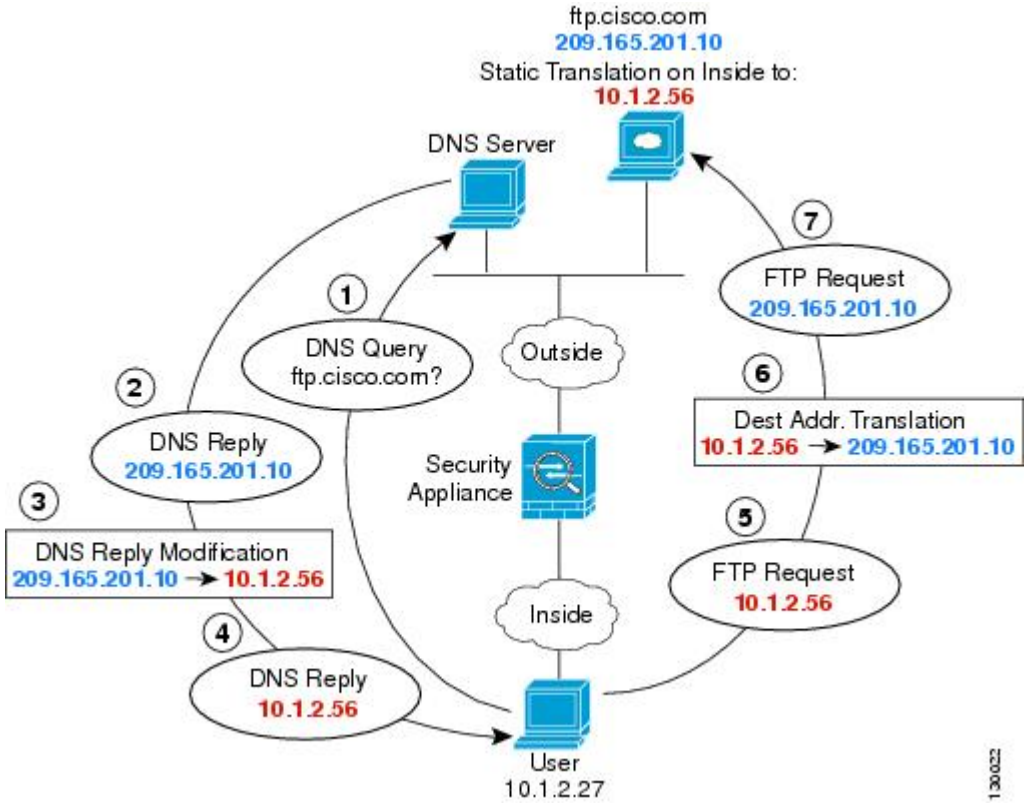
ユーザが実際のアドレスを使用して ftp.cisco.com にアクセスする必要がある場合、これ以上の設定は必要ありません。内部と DMZ 間にもスタティック ルールがある場合は、このルールに対して DNS 応答修正もイネーブルにする必要があります。DNS 応答は、2 回変更されます。この場合、ASA は内部と DMZ 間のスタティック ルールに従ってもう一度 DNS 応答内のアドレスを 192.168.1.10 に変換します。

図 *18 : DNS* 応答修正：別々のネットワーク上の *DNS* サーバ、ホスト、およびサーバ



DNS 応答修正：ホスト ネットワーク上の DNS サーバ

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、ftp.cisco.com のアドレスを DNS サーバに要求すると、DNS サーバは応答で実際のアドレス 209.165.20.10 を示します。内部ユーザに 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。

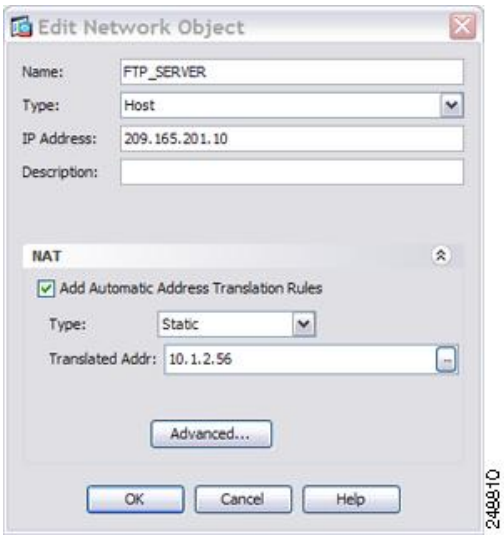


手順

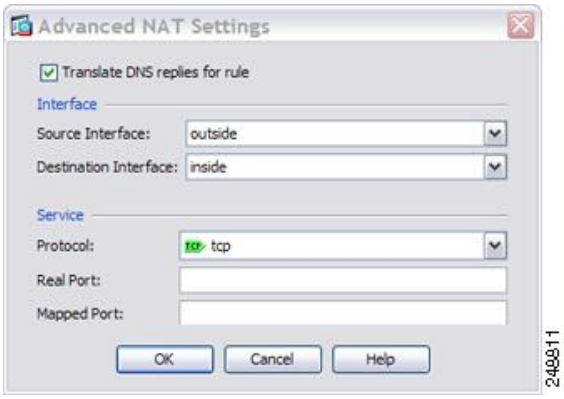
ステップ 1 **[Configuration]** > **[Firewall]** > **[NAT]** を選択します。

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 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。

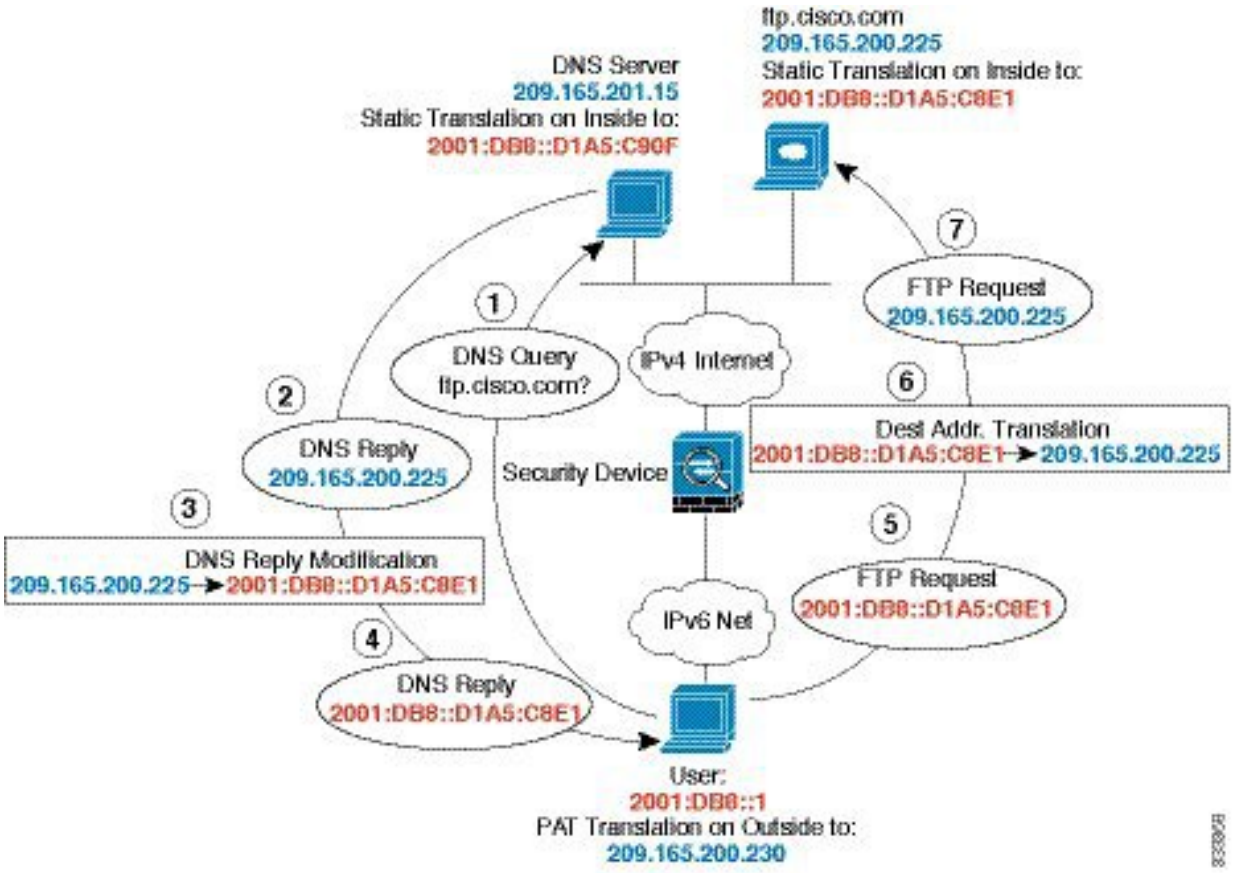


ステップ 5 [OK] をクリックして [Edit Network Object] ダイアログボックスに戻り、もう一度 [OK] をクリックし、[Apply] をクリックします。

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。この場合に、内部 IPv6 ユーザが ftp.cisco.com のアドレスを DNS サーバに要求すると、DNS サーバは応答として実際のアドレス 209.165.200.225 を返します。

ftp.cisco.com のマッピング アドレス（2001:DB8::D1A5:C8E1、ここで D1A5:C8E1 は 209.165.200.225 に相当する IPv6）が内部ユーザによって使用されるようにするには、スタティック変換に対して 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。



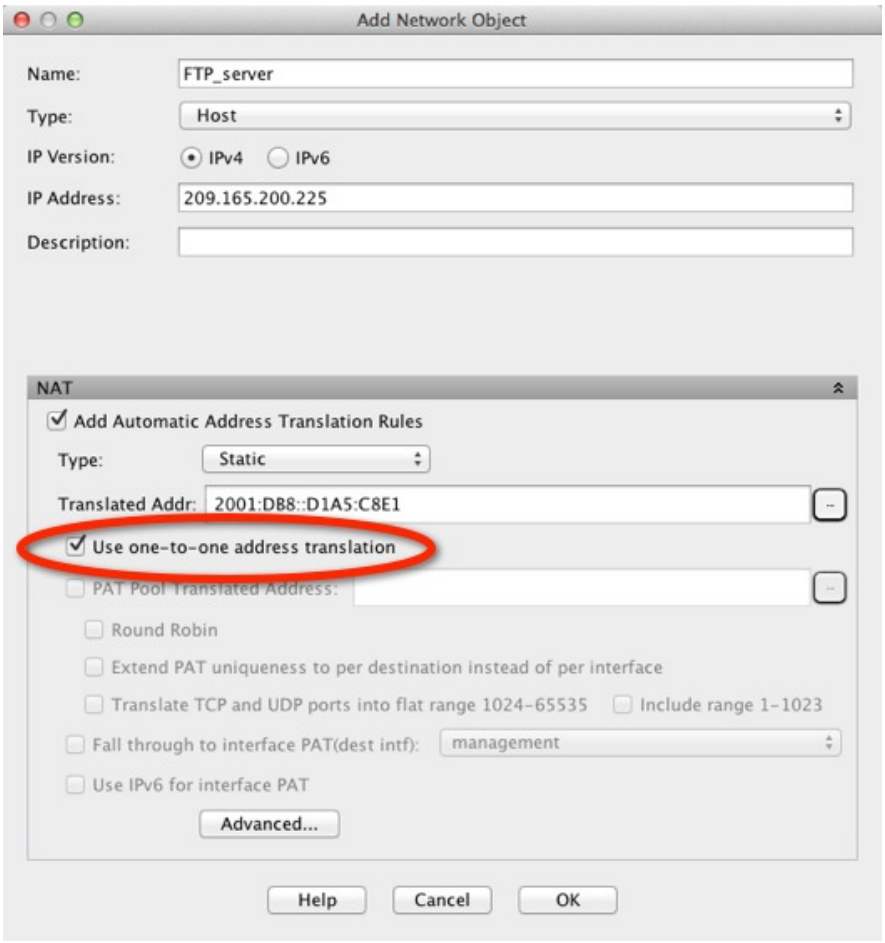
手順

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

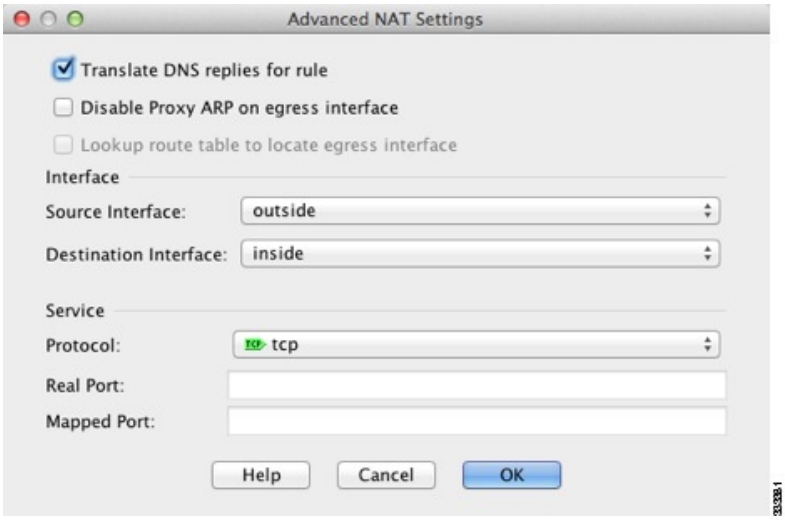
ステップ 2 FTP サーバの DNS 修正を設定したスタティック ネットワーク オブジェクト NAT を設定します。

a) [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 FTP サーバ 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。

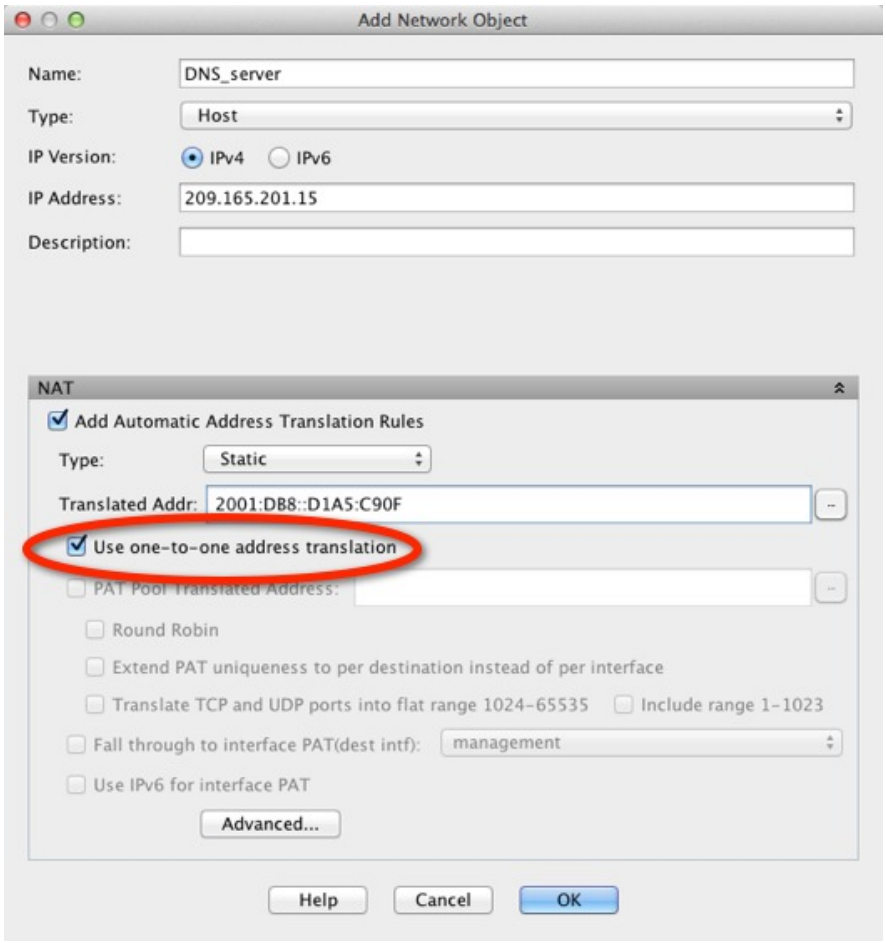


d) [OK] をクリックして [Network Object] ダイアログボックスに戻り、もう一度 [OK] をクリックしてルールを保存します。

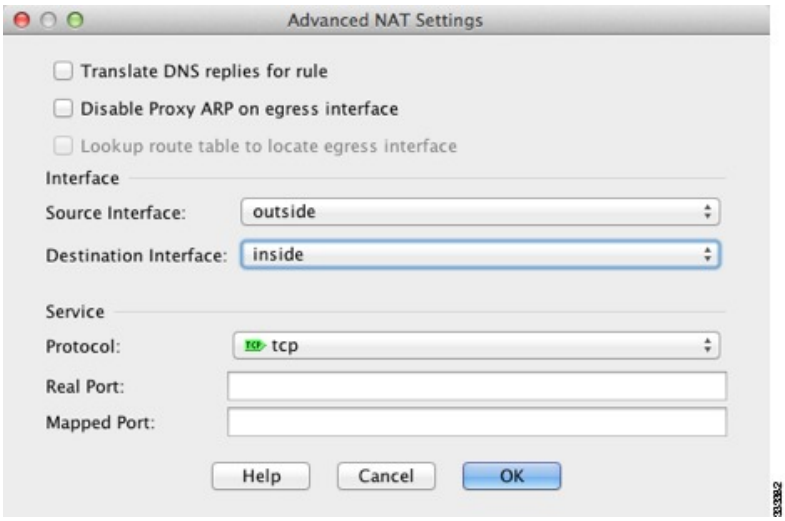
ステップ 3 DNS サーバのスタティック ネットワーク オブジェクト NAT を設定します。

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 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。

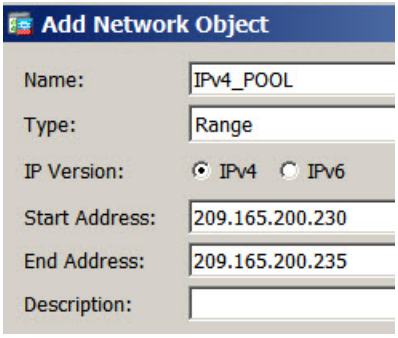
ステップ 4 内部 IPv6 ネットワークのための PAT を設定します。

a) [Add] > [Network Object NAT Rule] を選択します。

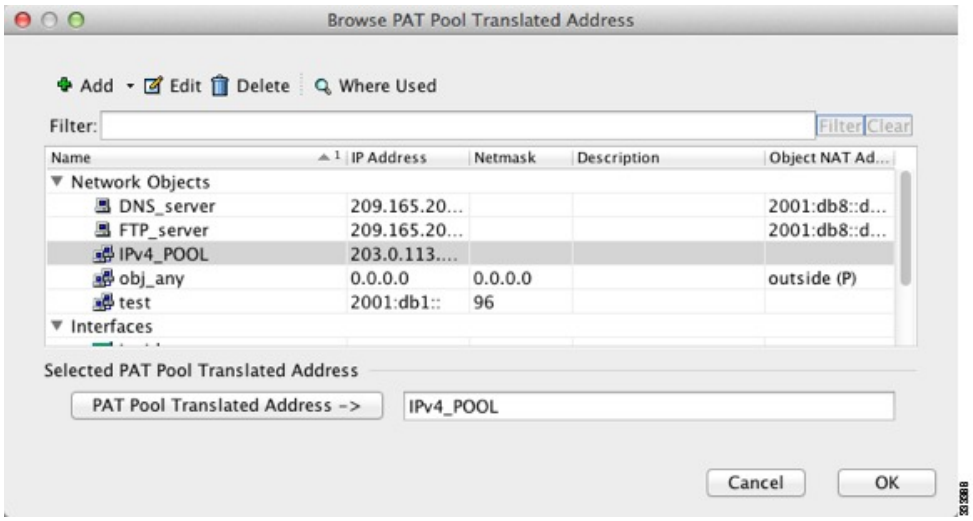
b) 新しいネットワーク オブジェクトに名前を付けて IPv6 ネットワーク アドレスを定義し、ダイナミック NAT を選択します。

c) [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。

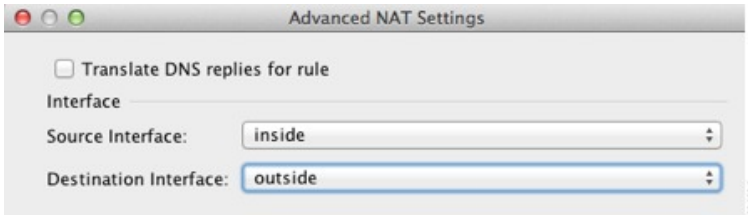
d) [Browse PAT Pool Translated Address] ダイアログボックスで、[Add] > [Network Object] を選択します。新しいオブジェクトに名前を付けて PAT プールのアドレス範囲を入力し、[OK] をクリックします。



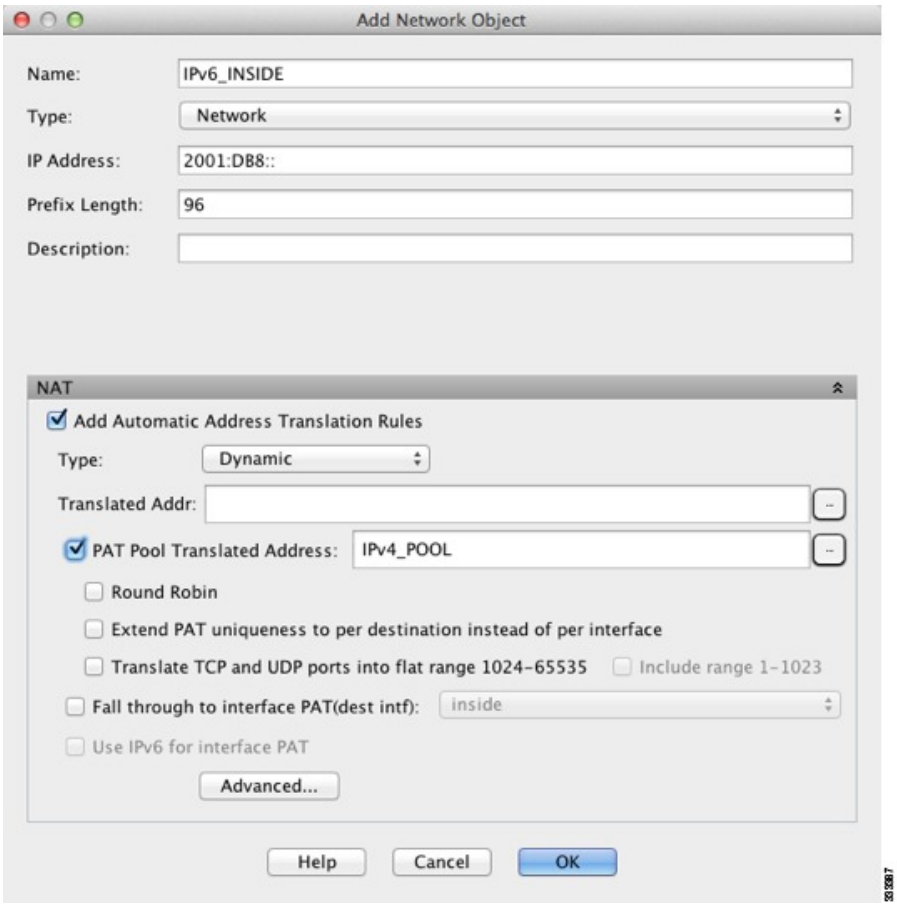
e) [Browse PAT Pool Translated Address] ダイアログボックスで、作成した PAT プール オブジェクトをダブルクリックして選択し、[OK] をクリックします。



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

次の図に、外部の FTP サーバと DNS サーバを示します。ASA 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、内部のユーザが 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 サーバはサーバ名、ftp.cisco.com を使用して応答します。

図 *19 : PTR* の変更、ホスト ネットワークの *DNS* サーバ