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。

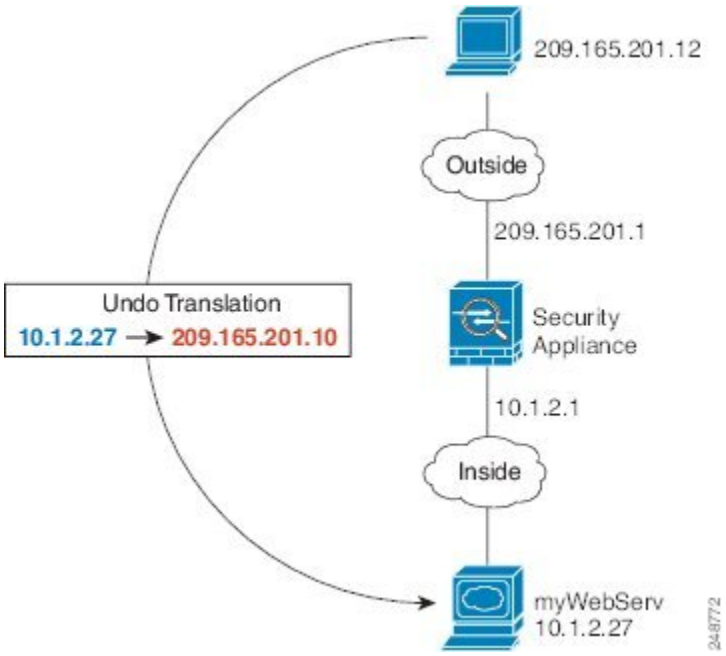
ネットワーク オブジェクト NAT の例

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* サーバーのスタティック *NAT*



手順

ステップ 1 内部 Web サーバーのネットワーク オブジェクトを作成します。

```
hostname(config)# object network myWebServ
hostname(config-network-object)# host 10.1.2.27
```

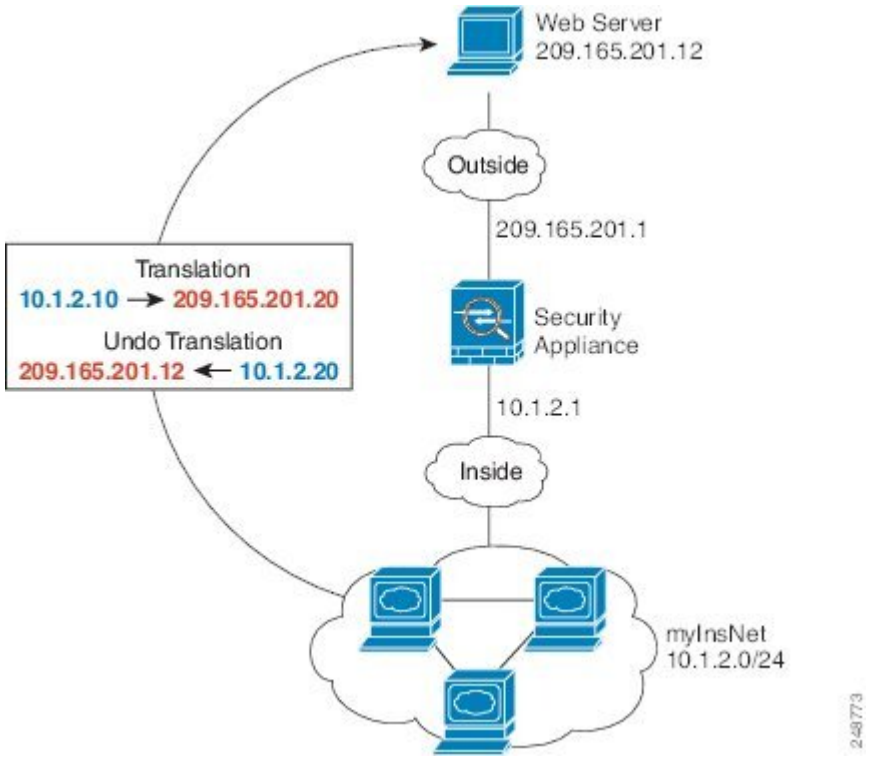
ステップ 2 オブジェクトのスタティック NAT を設定します。

```
hostname(config-network-object)# nat (inside,outside) static 209.165.201.10
```

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* サーバーのスタティック *NAT*



手順

ステップ 1 内部アドレスに変換するダイナミック NAT プールのネットワーク オブジェクトを作成します。

```
hostname(config)# object network myNatPool
hostname(config-network-object)# range 209.165.201.20 209.165.201.30
```

ステップ 2 内部ネットワークのネットワーク オブジェクトを作成します。

```
hostname(config)# object network myInsNet
hostname(config-network-object)# subnet 10.1.2.0 255.255.255.0
```

ステップ 3 ダイナミック NAT プール オブジェクトを使用して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。

```
hostname(config-network-object)# nat (inside,outside) dynamic myNatPool
```

ステップ 4 外部 Web サーバーのネットワーク オブジェクトを作成します。

```
hostname(config)# object network myWebServ
hostname(config-network-object)# host 209.165.201.12
```

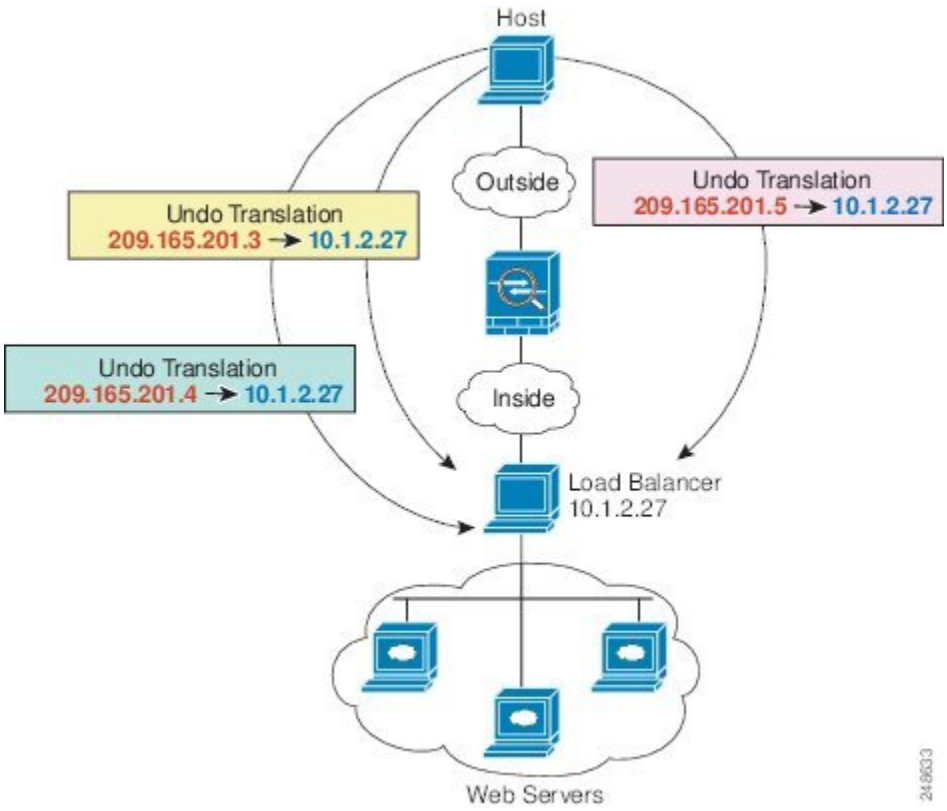
ステップ 5 Web サーバーのスタティック NAT を設定します。

```
hostname(config-network-object)# nat (outside,inside) static 10.1.2.20
```

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 つにアクセスする際、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 ロード バランサをマッピングするアドレスのネットワーク オブジェクトを作成します。

```
hostname(config)# object network myPublicIPs
hostname(config-network-object)# range 209.165.201.3 209.265.201.8
```

ステップ 2 ロード バランサのネットワーク オブジェクトを作成します。

```
hostname(config)# object network myLBHost
hostname(config-network-object)# host 10.1.2.27
```

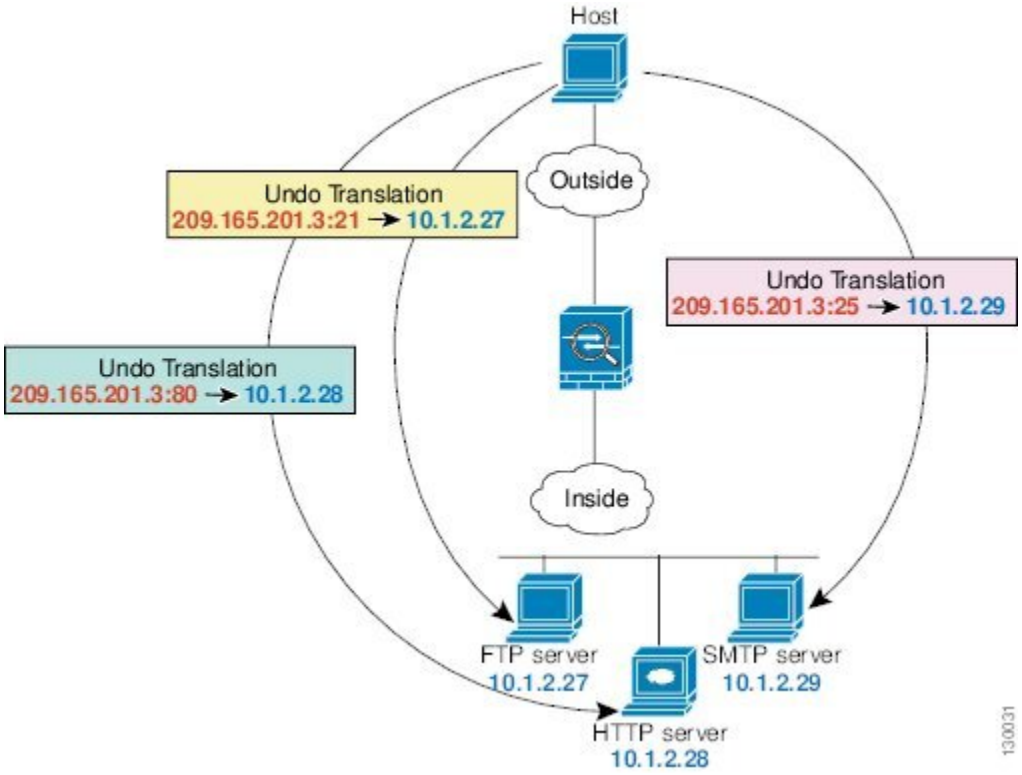
ステップ 3 範囲オブジェクトを適用するロード バランサのスタティック NAT を設定します。

```
hostname(config-network-object)# nat (inside,outside) static myPublicIPs
```

FTP、HTTP、および SMTP のための単一アドレス（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 FTP サーバのネットワーク オブジェクトを作成してポート変換を設定したスタティック NAT を設定し、FTP ポートを自身にマッピングします。

```
hostname(config)# object network FTP_SERVER
hostname(config-network-object)# host 10.1.2.27
hostname(config-network-object)# nat (inside,outside) static 209.165.201.3 service tcp
ftp ftp
```

ステップ 2 HTTP サーバのネットワーク オブジェクトを作成し、ポート変換を使用したスタティック NAT を設定し、HTTP ポートをマッピングします。

```
hostname(config)# object network HTTP_SERVER
hostname(config-network-object)# host 10.1.2.28
hostname(config-network-object)# nat (inside,outside) static 209.165.201.3 service tcp
http http
```

ステップ 3 SMTP サーバのネットワーク オブジェクトを作成してポート変換を設定したスタティック NAT を設定し、SMTP ポートを自身にマッピングします。

```
hostname(config)# object network SMTP_SERVER
hostname(config-network-object)# host 10.1.2.29
hostname(config-network-object)# nat (inside,outside) static 209.165.201.3 service tcp
smtp smtp
```

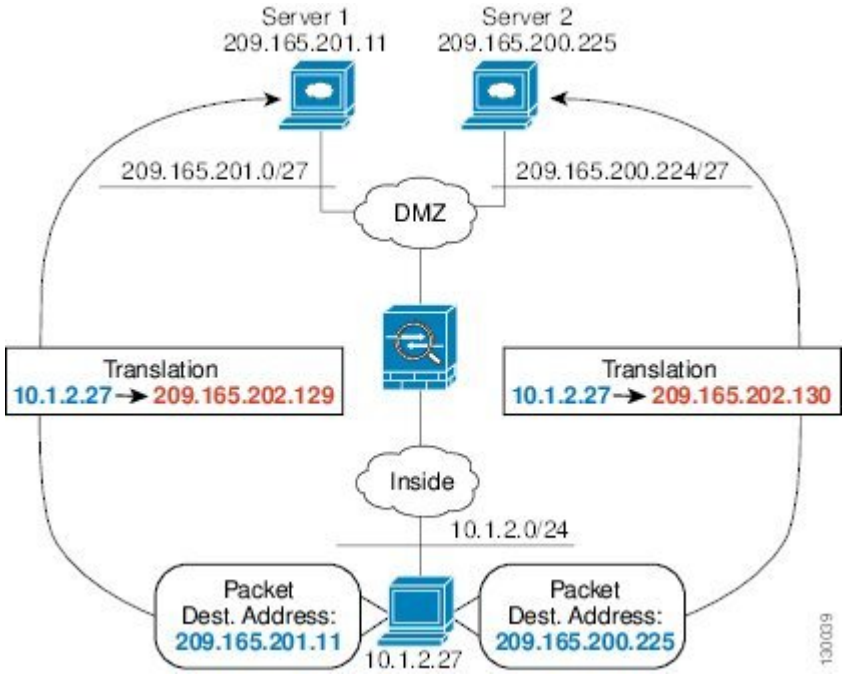
Twice NAT の例

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 つの異なるサーバにアクセスする、10.1.2.0/24 ネットワーク上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 内部ネットワークのネットワーク オブジェクトを追加します。

```
hostname(config)# object network myInsideNetwork
hostname(config-network-object)# subnet 10.1.2.0 255.255.255.0
```

ステップ 2 DMZ ネットワーク 1 のネットワーク オブジェクトを追加します。

```
hostname(config)# object network DMZnetwork1
hostname(config-network-object)# subnet 209.165.201.0 255.255.255.224
```

ステップ 3 PAT アドレスのネットワーク オブジェクトを追加します。

```
hostname(config)# object network PATaddress1
hostname(config-network-object)# host 209.165.202.129
```

ステップ 4 最初の Twice NAT ルールを設定します。

```
hostname(config)# nat (inside,dmz) source dynamic myInsideNetwork PATaddress1
destination static DMZnetwork1 DMZnetwork1
```

宛先アドレスは変換しないため、実際の宛先アドレスとマッピング宛先アドレスの両方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 5 DMZ ネットワーク 2 のネットワーク オブジェクトを追加します。

```
hostname(config)# object network DMZnetwork2
hostname(config-network-object)# subnet 209.165.200.224 255.255.255.224
```

ステップ 6 PAT アドレスのネットワーク オブジェクトを追加します。

```
hostname(config)# object network PATaddress2
hostname(config-network-object)# host 209.165.202.130
```

ステップ 7 2 つめの Twice NAT ルールを設定します。

例：

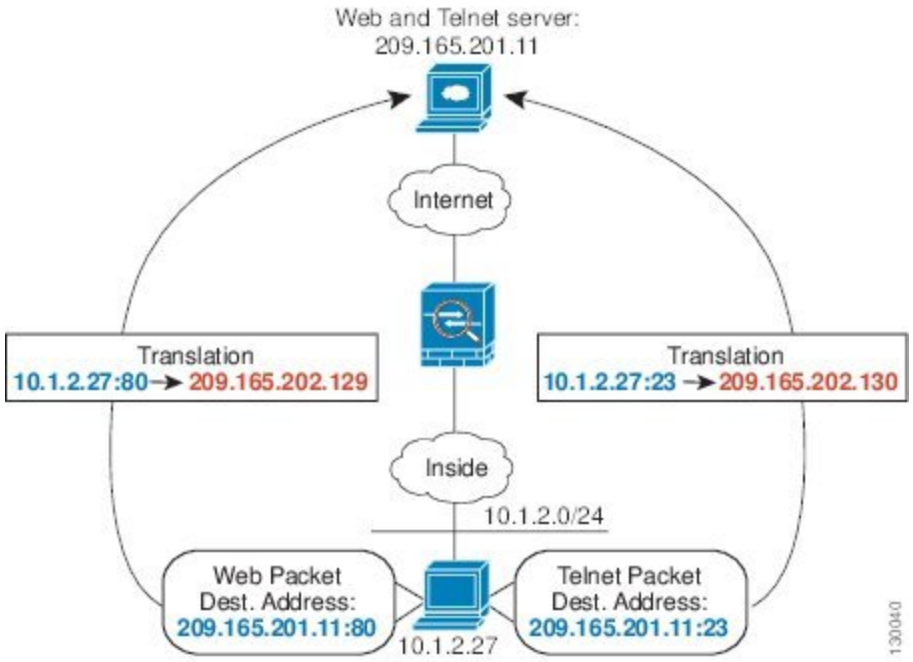
```
hostname(config)# nat (inside,dmz) source dynamic myInsideNetwork PATaddress2
destination static DMZnetwork2 DMZnetwork2
```

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 内部ネットワークのネットワーク オブジェクトを追加します。

```
hostname(config)# object network myInsideNetwork
hostname(config-network-object)# subnet 10.1.2.0 255.255.255.0
```

ステップ 2 Telnet/Web サーバーのネットワーク オブジェクトを追加します。

```
hostname(config)# object network TelnetWebServer
hostname(config-network-object)# host 209.165.201.11
```

ステップ 3 Telnet を使用するときは、PAT アドレスのネットワーク オブジェクトを追加します。

```
hostname(config)# object network PATaddress1
hostname(config-network-object)# host 209.165.202.129
```

ステップ 4 Telnet のサービス オブジェクトを追加します。

```
hostname(config)# object service TelnetObj
```

```
hostname(config-network-object)# service tcp destination eq telnet
```

ステップ 5 最初の Twice NAT ルールを設定します。

```
hostname(config)# nat (inside,outside) source dynamic myInsideNetwork PATaddress1
destination static TelnetWebServer TelnetWebServer service TelnetObj TelnetObj
```

宛先アドレスまたはポートを変換しないため、実際の宛先アドレスとマッピング宛先アドレスに同じアドレスを指定し、実際のサービスとマッピング サービスに同じポート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 6 HTTP を使用するときは、PAT アドレスのネットワーク オブジェクトを追加します。

```
hostname(config)# object network PATaddress2
hostname(config-network-object)# host 209.165.202.130
```

ステップ 7 HTTP のサービス オブジェクトを追加します。

```
hostname(config)# object service HTTPObj
hostname(config-network-object)# service tcp destination eq http
```

ステップ 8 2 つめの Twice NAT ルールを設定します。

```
hostname(config)# nat (inside,outside) source dynamic myInsideNetwork PATaddress2
destination static TelnetWebServer TelnetWebServer service HTTPObj HTTPObj
```

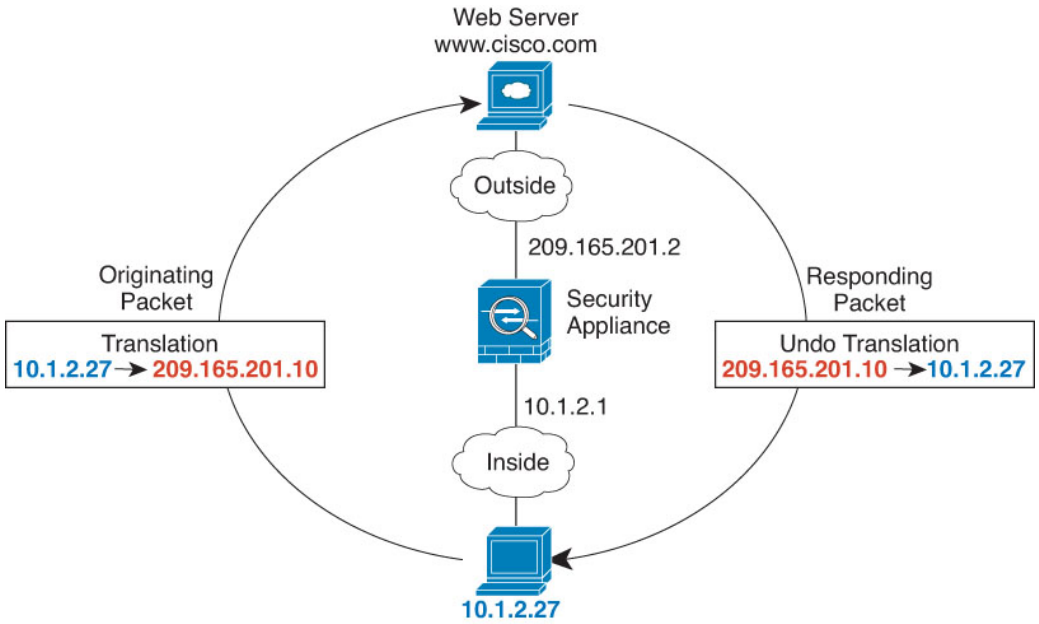
ルーテッド モードとトランスペアレント モードの NAT

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。

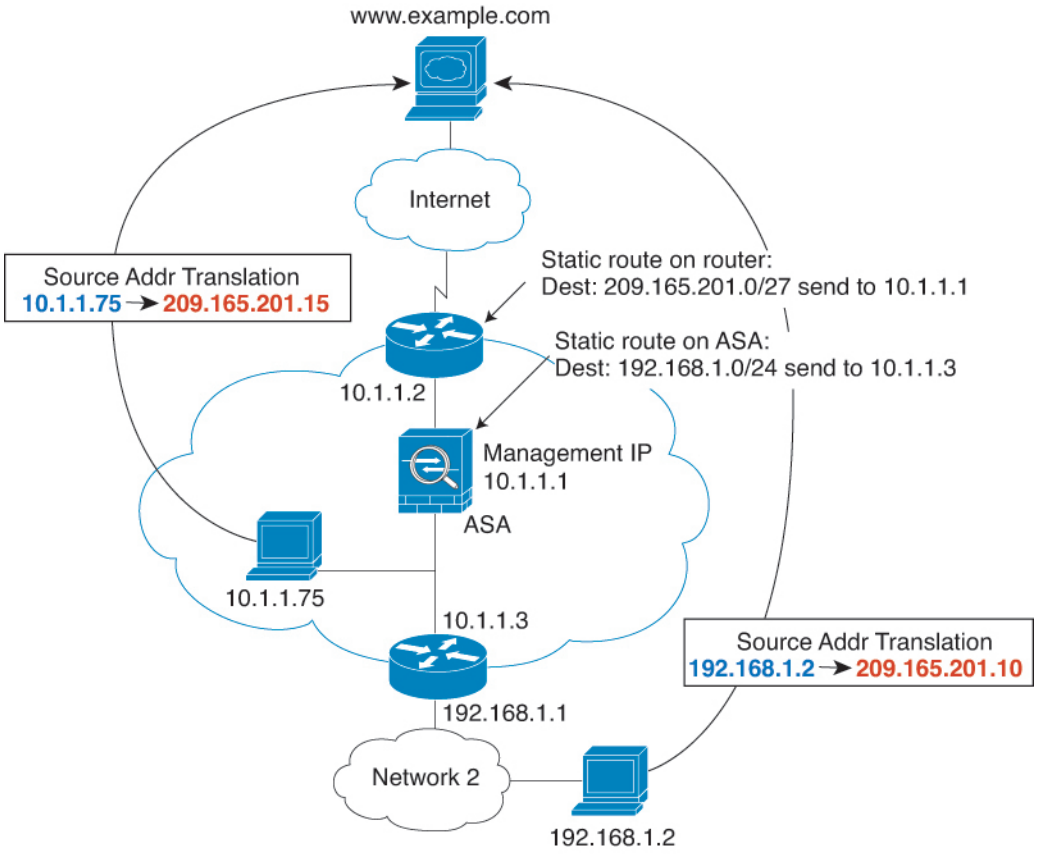
トランスペアレント モードまたは同じブリッジ グループのメンバー間のルーテッド モードの NAT には、以下の要件および制限があります。

- 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 *8 : 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たすべてのパケットの宛先となる必要があります。ASA は、マッピング アドレスの送信先を受信するすべての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 のガイドラインの補足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。**arp** コマンドを使用して、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
```

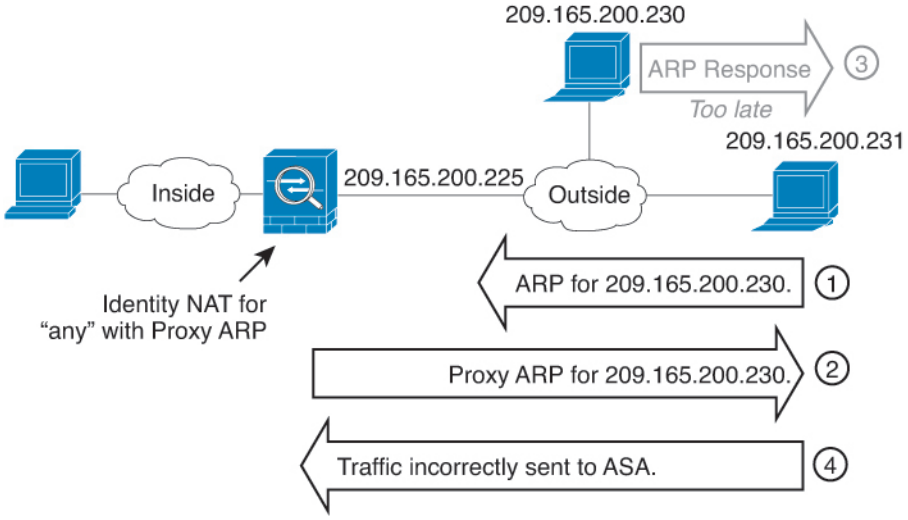
トランスペアレント モードの場合は、実際のホストが直接接続されてる場合は、ASA をポイントするようにアップストリーム ルータのスタティック ルートを設定します。ブリッジ グループの IP アドレスを指定します。トランスペアレント モードのリモート ホストの場合は、アップストリーム ルータのスタティック ルートで、代わりにダウンストリーム ルータの IP アドレスを指定できます。

実際のアドレスと同じアドレス（アイデンティティ NAT）

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 をディセーブルにできます。また、必要に応じて通常のスタティック NAT のプロキシ ARP をディセーブルにすることもできます。その場合には、アップストリーム ルータに適切なルートが確実に設定されていなくてはなりません。

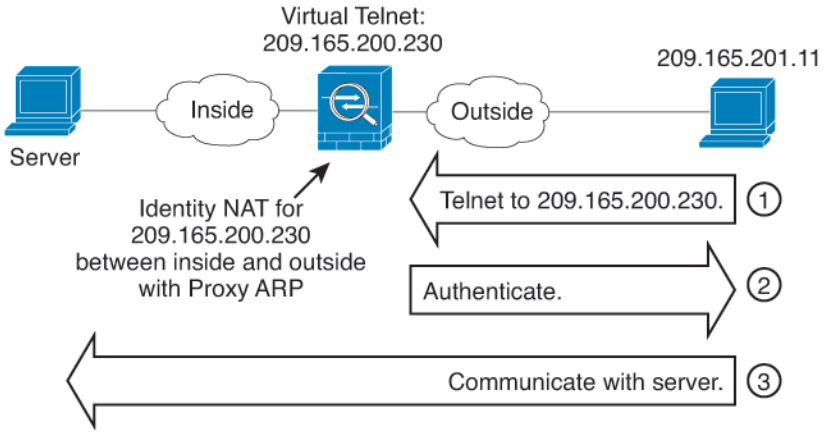
アイデンティティ NAT の場合、通常はプロキシ ARP が不要で、場合によっては接続性に関する問題を引き起こす可能性があります。たとえば、「any」の IP アドレスに対して広範囲のアイデンティティ NAT ルールを設定した場合は、プロキシ ARP をイネーブルのままにしておくと、マッピング インターフェイスに直接接続されたネットワーク上のホストに問題が発生する可能性があります。この場合、マッピング ネットワークのホストが同じネットワークの他のホストと通信すると、ARP 要求内のアドレスは（任意のアドレスと一致する）NAT ルールと一致します。このとき、実際にはASA 向けのパケットでない場合でも、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）。ネットワーク アクセスに AAA を使用する場合、ホストは他のトラフィックが通過する前に Telnet のようなサービスを使用して ASA で認証を受ける必要があります。ASA に仮想 Telnet サーバを設定すると、必要なログインを提供できます。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 を使用すると ASA が NAT ルールに従って送信元インターフェイスからトラフィックを送信せず、トラフィックを仮想 Telnet アドレス宛のままにすることができます（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。

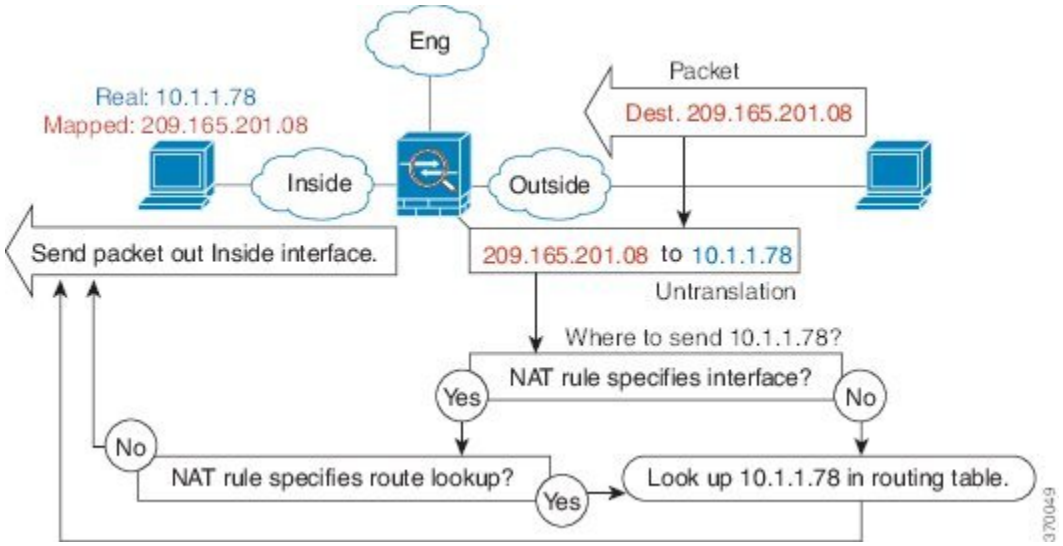
出力インターフェイスの決定

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。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 *11 : 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



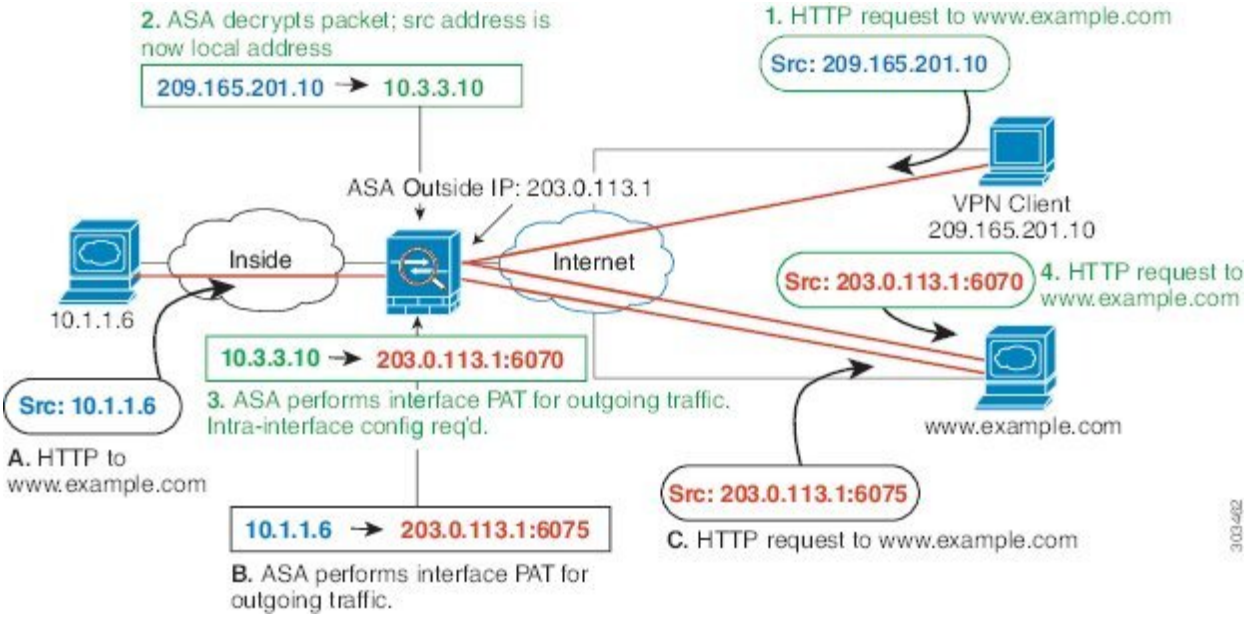
VPN の NAT

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

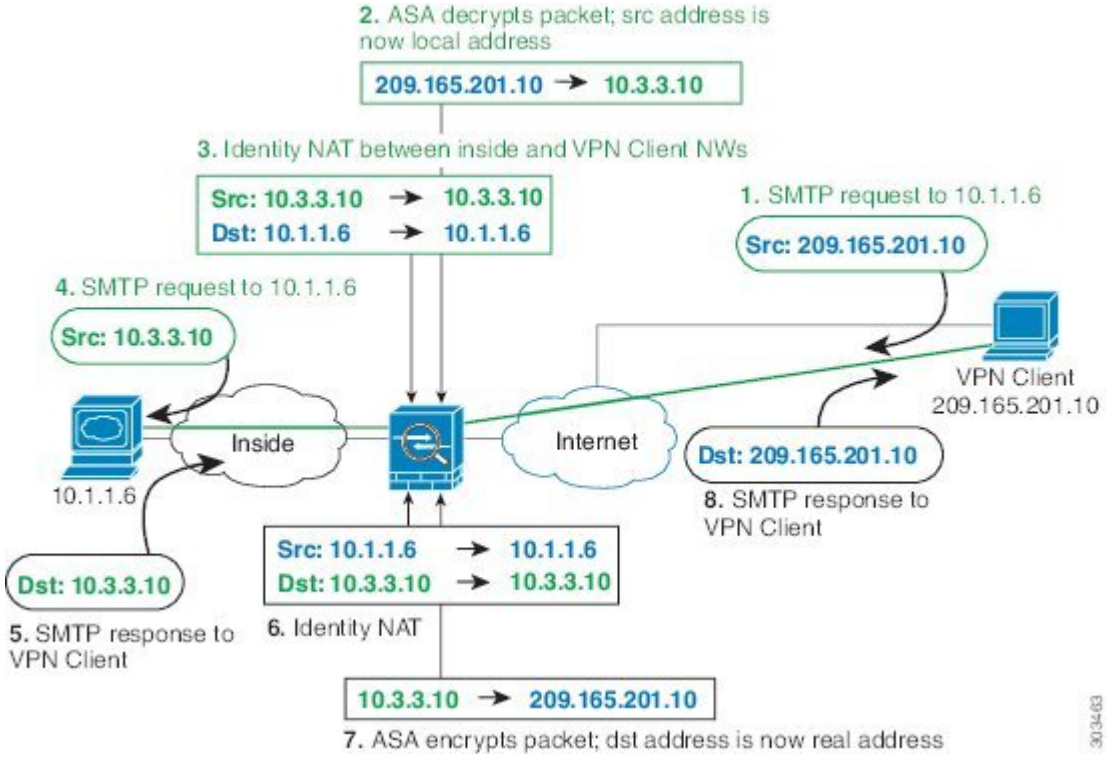
次の図に、内部サーバー（10.1.1.6）とインターネットにアクセスする VPN クライアント（209.165.201.10）の両方を示します。VPN クライアント用のスプリット トンネリング（指定したトラフィックのみが VPN トンネル上でやりとりされる）を設定しない限り、インターネット バインドされた VPN トラフィックも ASA を経由する必要があります。VPN トラフィックが ASA に渡されると、ASA はパケットを復号化し、得られたパケットには送信元として VPN クライアント ローカル アドレス（10.3.3.10）が含まれています。内部ネットワークと VPN クライアント ロ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

図 *13 : 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。

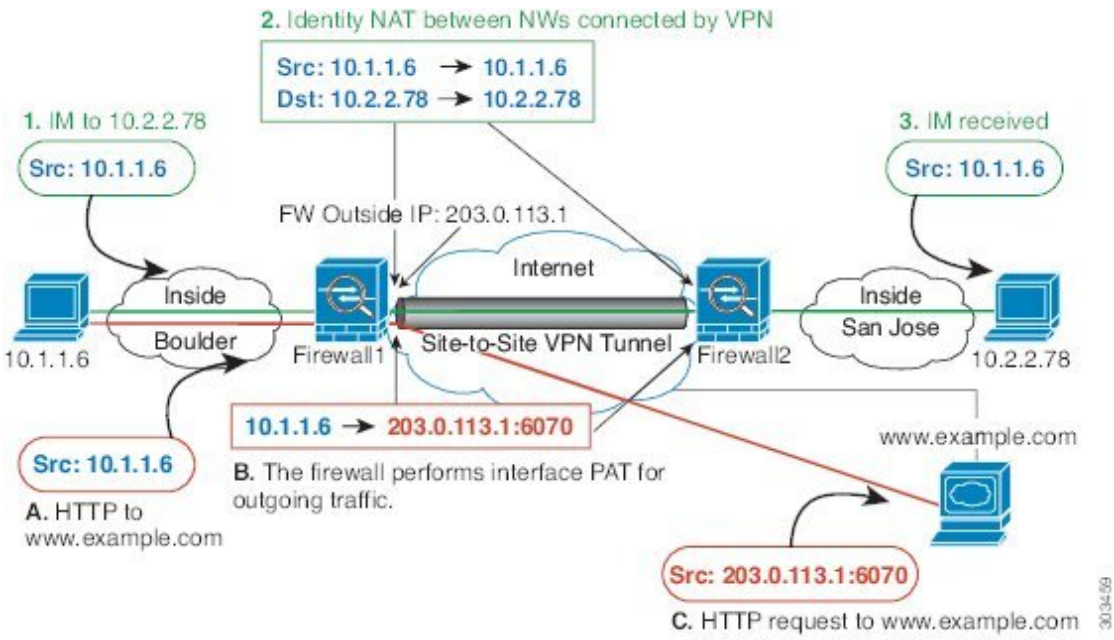
```
! Enable hairpin for non-split-tunneled VPN client traffic:
same-security-traffic permit intra-interface

! 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。インターネットに向かうトラフィック（たとえばボールダーの 10.1.1.6 から www.example.com へ）については、インターネット アクセス用に 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

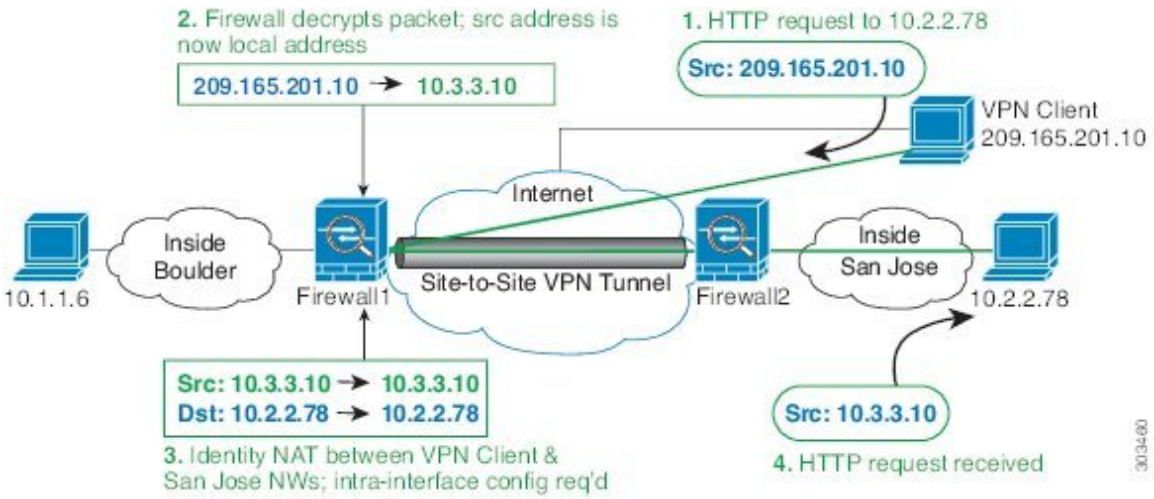
トンネルを経由するトラフィック（たとえば、ボールダーの 10.1.1.6 からサンノゼの 10.2.2.78 へ）については NAT を実行しません。したがって、アイデンティティ NAT ルールを作成して、そのトラフィックを除外する必要があります。アイデンティティ NAT は、あるアドレスを同じアドレスに変換するだけです。

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 *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
```

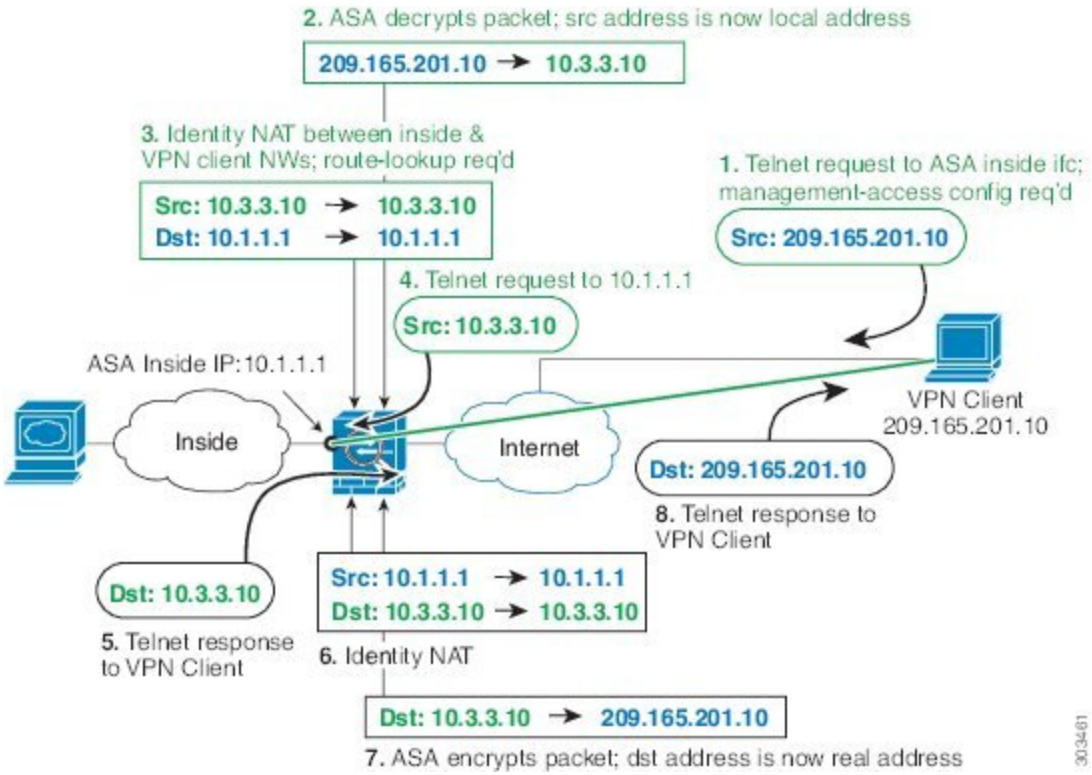
```
subnet 10.2.2.0 255.255.255.0
nat (inside,outside) dynamic interface

! 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（**management-access** コマンドを参照）。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 （17 ページ）またはNAT およびサイトツーサイト VPN （19 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 （16 ページ）を参照してください。

図 *16 : 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

トラフィックが IPv6 のみのネットワークと IPv4 のみのネットワークの間を通過するようにする必要がある場合、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、外部ネットワークに対して内部アドレスを非表示にする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 パケットから IPv4 パケットへの変換とその逆変換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 ルールで実行できますが、DNS サーバ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 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 を使用する必要はありません。

（注） NAT64 および NAT 46 は、標準のルーテッド インターフェイスのみで使用できます。NAT66 は、ルーテッドおよびブリッジ 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 から IPv4 へのアドレス変換

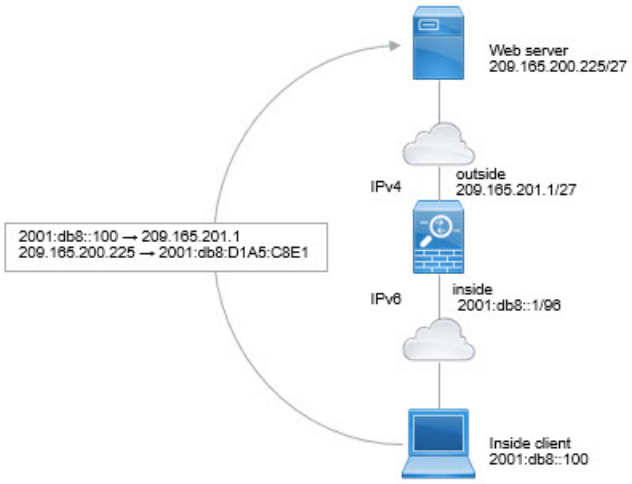
トラフィックが IPv6 ネットワークから IPv4 専用のネットワークへ通過する際には IPv6 アドレスを IPv4 に変換し、リターン トラフィックに対しては IPv4 から IPv6 に変換する必要があります。IPv6 アドレスをバインドする IPv4 アドレス プール（IPv4 内）と IPv4 アドレスをバインドする IPv6 アドレス プール（IPv6 内）という 2 つのアドレス プールを定義する必要があります。

- NAT64 ルール用の IPv4 アドレス プールは、一般に小さく、通常は IPv6 クライアント アドレスと 1 対 1 でマッピングするために十分なアドレスを持っていません。ダイナミック PAT は、ダイナミック NAT やスタティック NAT と比較して、多数の IPv6 クライアント アドレスに容易に適合します。
- NAT 46 ルール用の IPv6 アドレス プールは、マッピングされる IPv4 アドレスの数以上にすることができます。よって、各 IPv4 アドレスを異なる IPv6 アドレスにマッピングできます。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 は使用できません。

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 ルールで実行できますが、DNS サーバ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る、と想定しています。



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。

```
hostname(config)# object network inside_v6
hostname(config-network-object)# subnet 2001:db8::/96
```

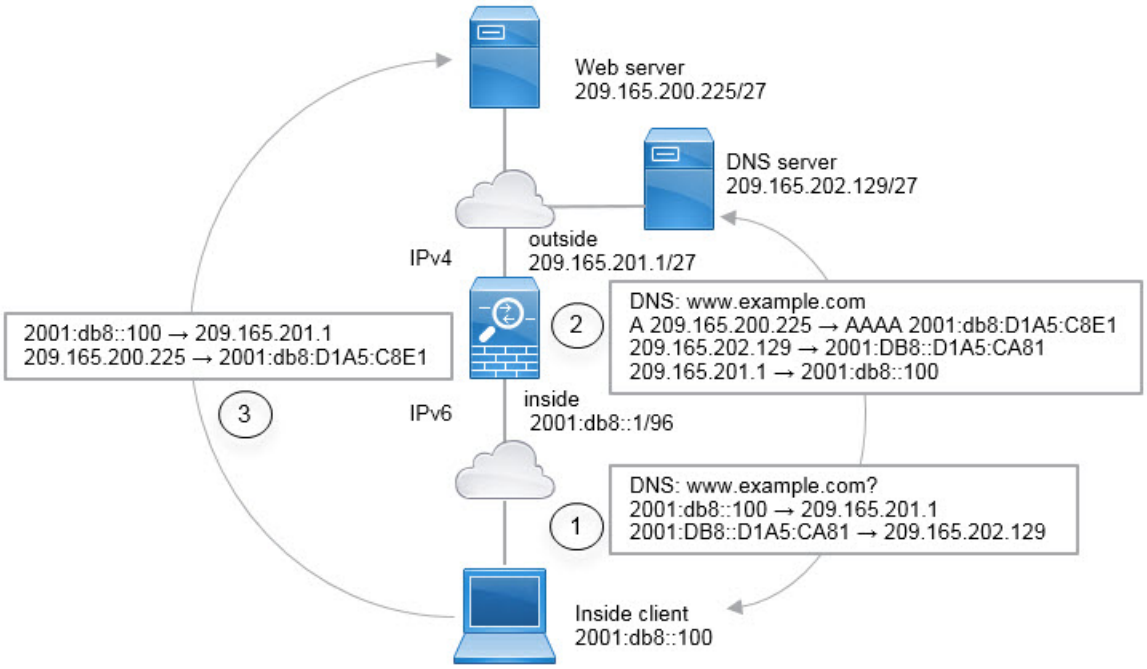
ステップ 2 IPv6 ネットワークを IPv4 に変換して再び戻すための Twice NAT ルールを作成します。

```
hostname(config)# nat (inside,outside) source dynamic inside_v6 interface
destination static inside_v6 any
```

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

内部の IPv6 専用ネットワークが存在するものの、内部ユーザが必要とする一部の IPv4 専用サービスがインターネット外部に存在する例を次に示します。



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。NAT46 ルールでの DNS の書き換えを有効にし、外部 DNS サーバからの応答を A（IPv4）から AAAA（IPv6）レコードに変換したり、アドレスを IPv4 から IPv6 に変換したりできます。

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 を開こうとする Web 要求の通常のシーケンスを次に示します。

1. クライアントのコンピュータは、2001:DB8::D1A5:CA81 で DNS サーバに DNS リクエストを送信します。NAT ルールは、DNS リクエストで送信元と宛先に以下の変換を実行します。
   - 2001:DB8::100 から 209.165.201.1 上の固有のポート（NAT64 インターフェイス PAT ルール）
   - 2001:DB8::D1A5:CA81 から 209.165.202.129（NAT46 ルール。D1A5:CA81 は IPv6 の 209.165.202.129 と同じです）
2. DNS サーバが応答で、www.example.com が 209.165.200.225 であるという A レコードを示します。DNS の書き換えが有効になっている NAT46 ルールは、A レコードを IPv6 版の AAAA レコードに変換し、AAAA レコードの 209.165.200.225 を 2001:db8:D1A5:C8E1 に変換します。さらに、DNS 応答の発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 から 2001:DB8::D1A5:CA81
   - 209.165.201.1 から 2001:db8::100
3. これで、IPv6 クライアントには Web サーバの IP アドレスが含まれるようになり、2001:db8:D1A5:C8E1 で www.example.com への HTTP リクエストを行います（D1A5:C8E1 は IPv6 の 209.165.200.225 と同じです）。HTTP リクエストの発信元アドレスと送信先アドレスは次のように変換されます。
   - 2001:DB8::100 から 209.156.101.54 上の固有のポート（NAT64 インターフェイス PAT ルール）
   - 2001:db8:D1A5:C8E1 から 209.165.200.225（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 内部 IPv6 ネットワーク用のネットワーク オブジェクトを作成し、NAT64 ルールを追加します。

```
hostname(config)# object network inside_v6
hostname(config-network-object)# subnet 2001:db8::/96
hostname(config-network-object)# nat(inside,outside) dynamic interface
```

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 2 外部 IPv4 ネットワーク用に変換された IPv6 ネットワークのネットワーク オブジェクトを作成し、NAT46 ルールを追加します。

```
hostname(config)# object network outside_v4_any
hostname(config-network-object)# subnet 0.0.0.0 0.0.0.0
hostname(config-network-object)# nat(outside,inside) static 2001:db8::/96 dns
```

このルールを使用すると、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。さらに、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。

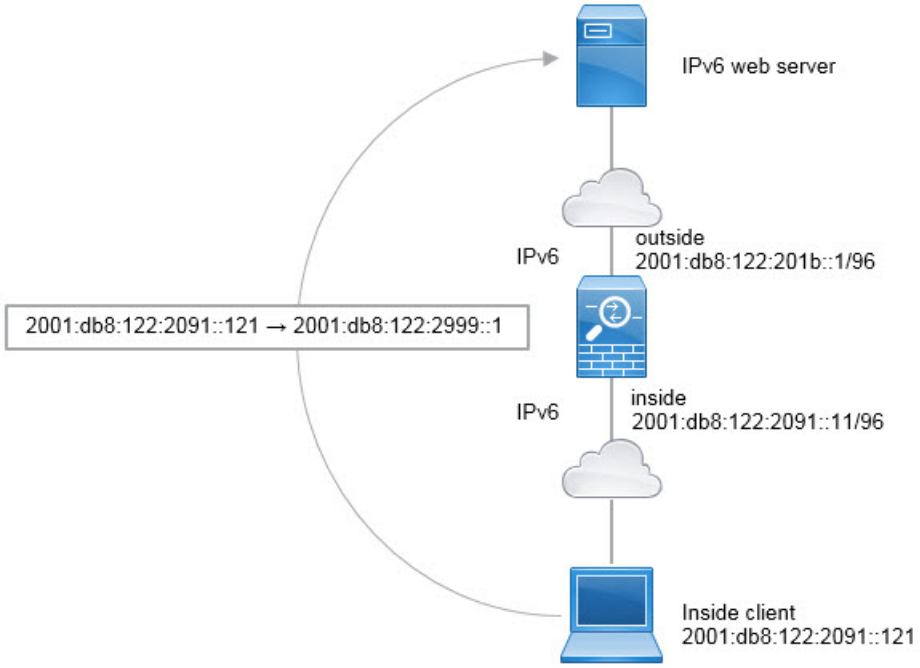
NAT66：IPv6 アドレスから別の IPv6 アドレスへの変換

IPv6 ネットワークから別の IPv6 ネットワークへと通過する場合、IPv6 アドレスを外部ネットワーク上の別の 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 を使用する必要はありません。

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

内部 IPv6 ネットワークのネットワーク オブジェクトを作成し、スタティック NAT のルールを追加します。

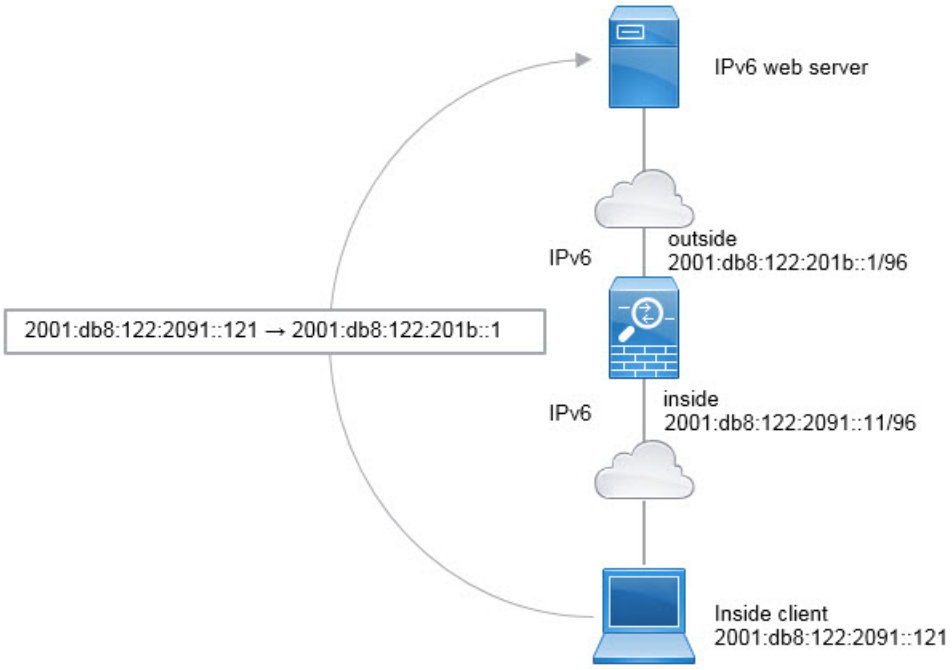
```
hostname(config)# object network inside_v6
hostname(config-network-object)# subnet 2001:db8:122:2091::/96
hostname(config-network-object)# nat(inside,outside) static 2001:db8:122:2999::/96
```

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 IPv6 インターフェイス PAT

NAT66 を実装する簡単な方法は、内部アドレスを外部インターフェイス IPv6 アドレスのさまざまなポートに動的に割り当てることです。

NAT66 に対してインターフェイス PAT ルールを設定する場合、そのインターフェイスで設定されたすべてのグローバル アドレスは PAT 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

内部 IPv6 ネットワークのネットワーク オブジェクトを作成し、ダイナミック PAT ルールを追加します。

```
hostname(config)# object network inside_v6
hostname(config-network-object)# subnet 2001:db8:122:2091::/96
hostname(config-network-object)# nat(inside,outside) dynamic interface ipv6
```

このルールでは、内部インターフェイスの 2001:db8:122:2091::/96 subnet 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、各変換ルールの設定時に設定できます。DNS 修正は、DNS Doctoring とも呼ばれます。

この機能は、NAT ルールに一致する DNS クエリーと応答のアドレスをリライトします（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 クエリーの 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 応答の場合、

レコードはマッピングされた値から実際の値に書き換えられます。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生じる主な状況を示します。

- ルールが NAT64 または NAT46 で、DNS サーバが外部ネットワーク上に存在する。DNS A レコード（IPv4 ）と AAAA レコード（IPv6）間で変換するために DNS 書き換えが必要です。
- DNS サーバが外部に存在し、クライアントが内部に存在し、クライアントが使用する完全修飾ドメイン名の一部が、他の内部ホストに解決される。
- DNS サーバが内部に存在してプライベート IP アドレスで応答し、クライアントが外部に存在する。そして、クライアントが、内部でホストされているサーバを指す完全修飾ドメイン名にアクセスする。

DNS 書き換えに関する制限事項

DNS 書き換えに伴う制限事項を以下に示します。

- DNS 書き換えは PAT に適用できません。これは、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ので、使用する PAT ルールが不明確になるためです。
- 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、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 DNS NAT 書き換えを有効にした 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。デフォルトで、DNS NAT 書き換えを有効にした DNS インスペクションが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 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。そのため、動的ルール用の xlate が存在しない場合は、書き換えを正しく実行できません。スタティック NAT では、同じ問題が発生しません。
- DNS 書き換えでは、DNS 動的更新メッセージ（opcode 5）が書き換えられません。

次のセクションでは、NAT ルール内の DNS 書き換えの例を示します。

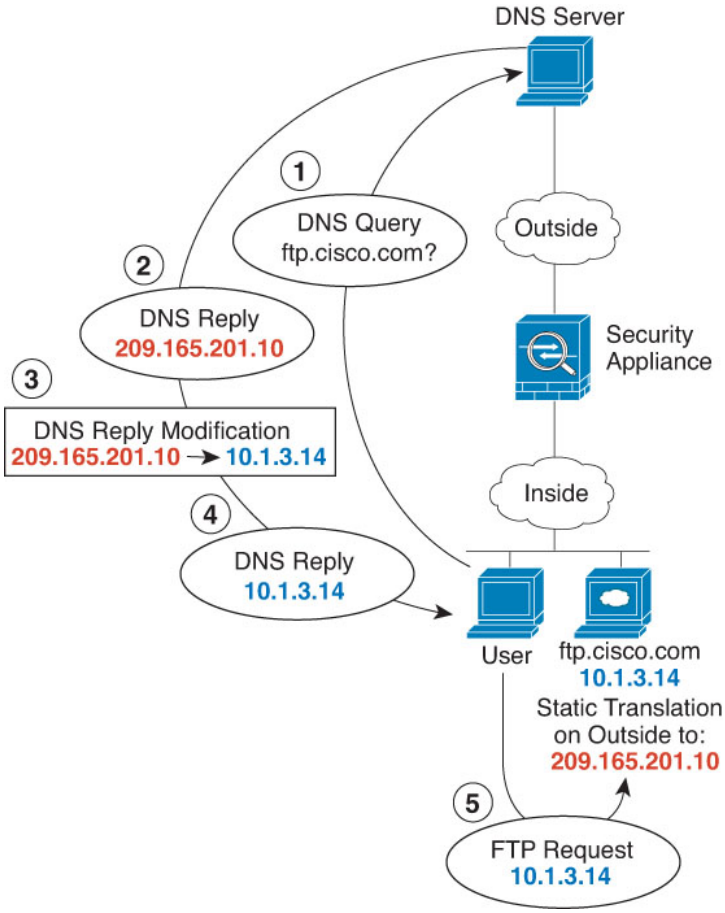
DNS 応答修正、外部の DNS サーバ

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 応答修正をイネーブルにしない場合、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 にトラフィックを送信することを試みます。



手順

ステップ 1 FTP サーバーのネットワーク オブジェクトを作成します。

```
hostname(config)# object network FTP_SERVER
```

```
hostname(config-network-object)# host 10.1.3.14
```

ステップ 2 DNS 修正を設定したスタティック NAT を設定します。

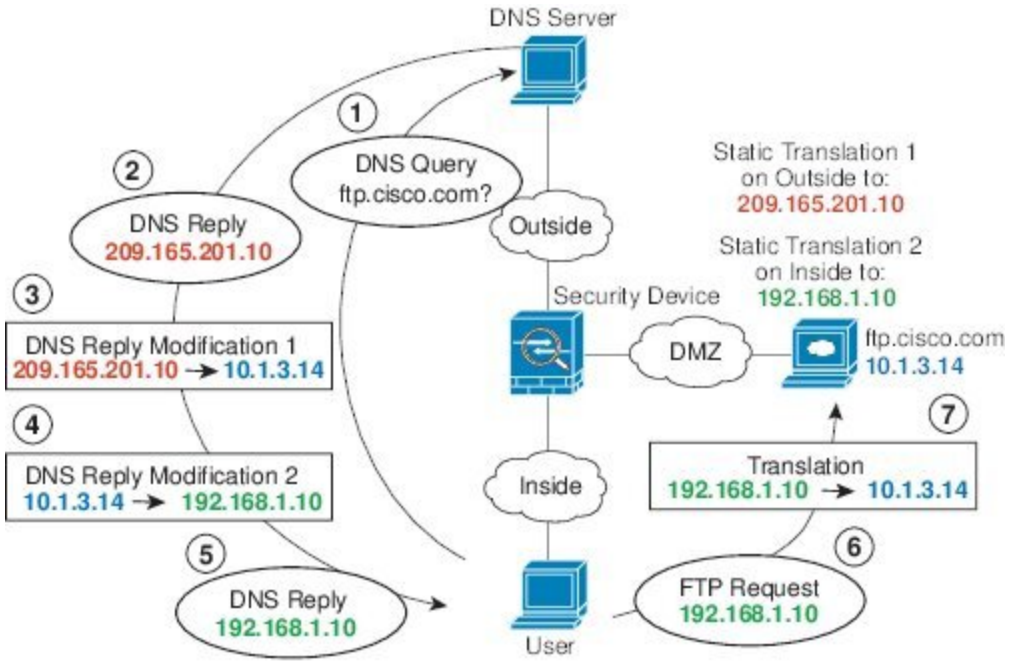
```
hostname(config-network-object)# nat (inside,outside) static 209.165.201.10 dns
```

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。

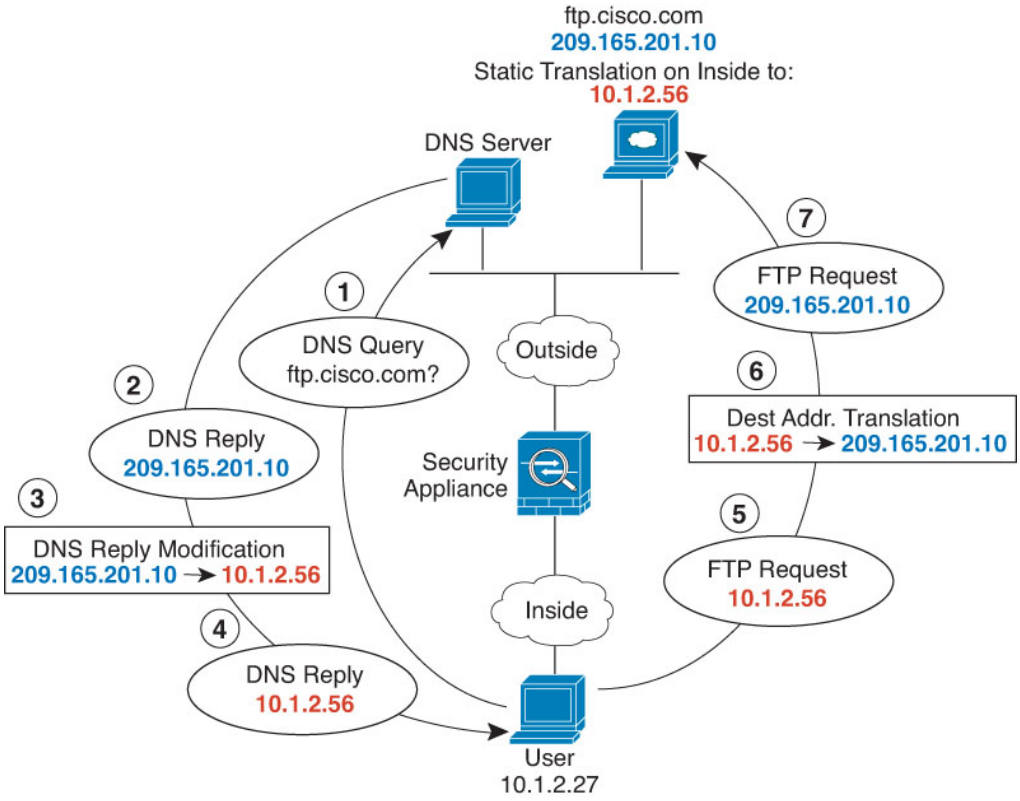
ユーザーが実際のアドレスを使用して ftp.cisco.com にアクセスする必要がある場合、これ以上の設定は必要ありません。内部と DMZ 間にもスタティック ルールがある場合は、このルールに対して DNS 応答修正もイネーブルにする必要があります。DNS 応答は、2 回変更されます。この場合、ASA は内部と DMZ 間のスタティック ルールに従ってもう一度 DNS 応答内のアドレスを 192.168.1.10 に変換します。

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

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。ftp.cisco.com のマッピング アドレス（10.1.2.56）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。



手順

ステップ 1 FTP サーバーのネットワーク オブジェクトを作成します。

```
hostname(config)# object network FTP_SERVER
hostname(config-network-object)# host 209.165.201.10
```

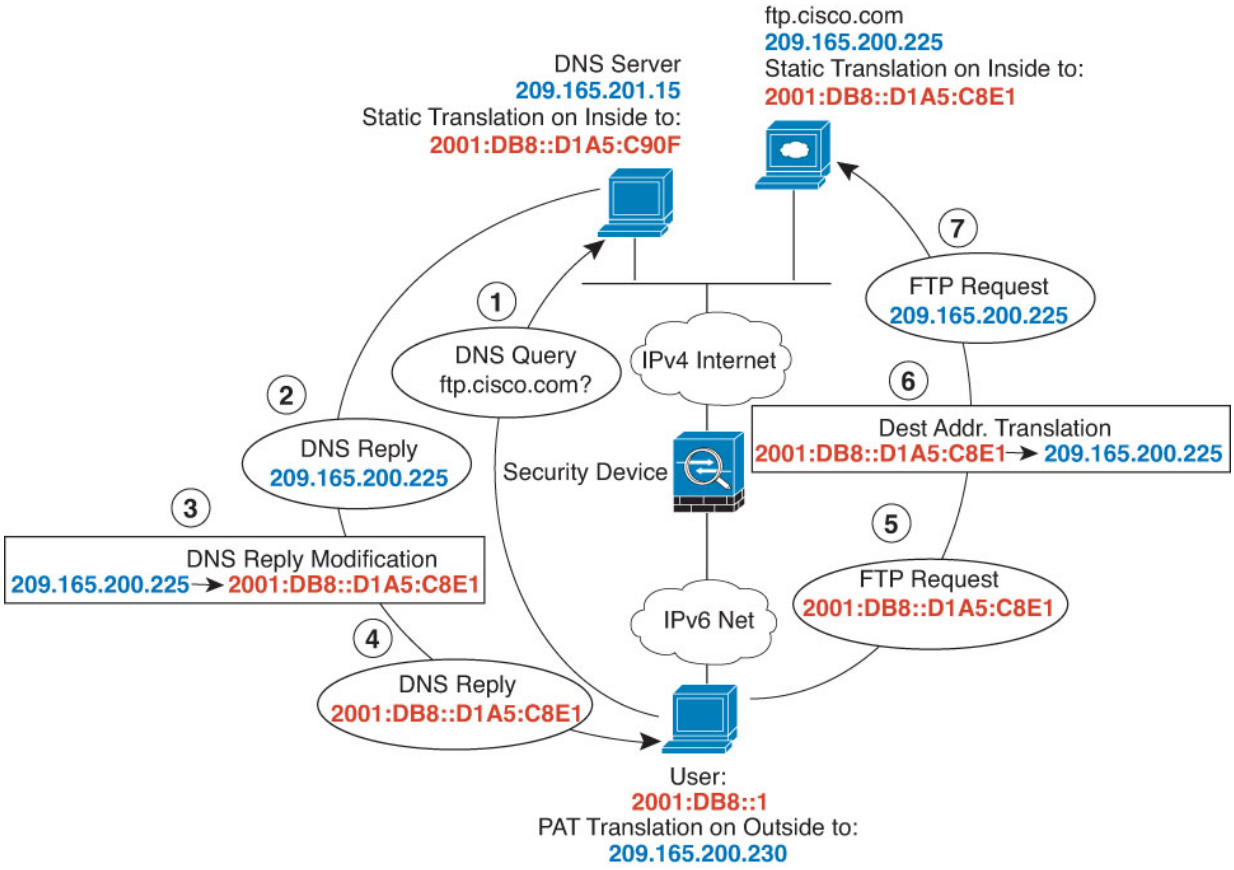
ステップ 2 DNS 修正を設定したスタティック NAT を設定します。

```
hostname(config-network-object)# nat (outside,inside) static 10.1.2.56 dns
```

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 サーバは応答で実際のアドレス 209.165.200.225 を示します。

内部ユーザが ftp.cisco.com のマッピング アドレス（2001:DB8::D1A5:C8E1。D1A5:C8E1 は 209.165.200.225 と同等の IPv6 アドレス）を使用するようにするには、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 FTP サーバーのネットワーク オブジェクトを作成して DNS 修正を設定したスタティック NAT を設定します。これは 1 対 1 変換であるため、NAT 46 の **net-to-net** オプションを含めます。

```
hostname(config)# object network FTP_SERVER
hostname(config-network-object)# host 209.165.200.225
hostname(config-network-object)# nat (outside,inside) static 2001:DB8::D1A5:C8E1/128
```

```
net-to-net dns
```

ステップ 2 DNS サーバーのネットワーク オブジェクトを作成して、スタティック NAT を設定します。NAT 46 の **net-to-net** オプションを含めます。

```
hostname(config)# object network DNS_SERVER
hostname(config-network-object)# host 209.165.201.15
hostname(config-network-object)# nat (outside,inside) static 2001:DB8::D1A5:C90F/128
net-to-net
```

ステップ 3 内部 IPv6 ネットワークを変換するための IPv4 PAT プールを設定します。

例：

```
hostname(config)# object network IPv4_POOL
hostname(config-network-object)# range 209.165.200.230 209.165.200.235
```

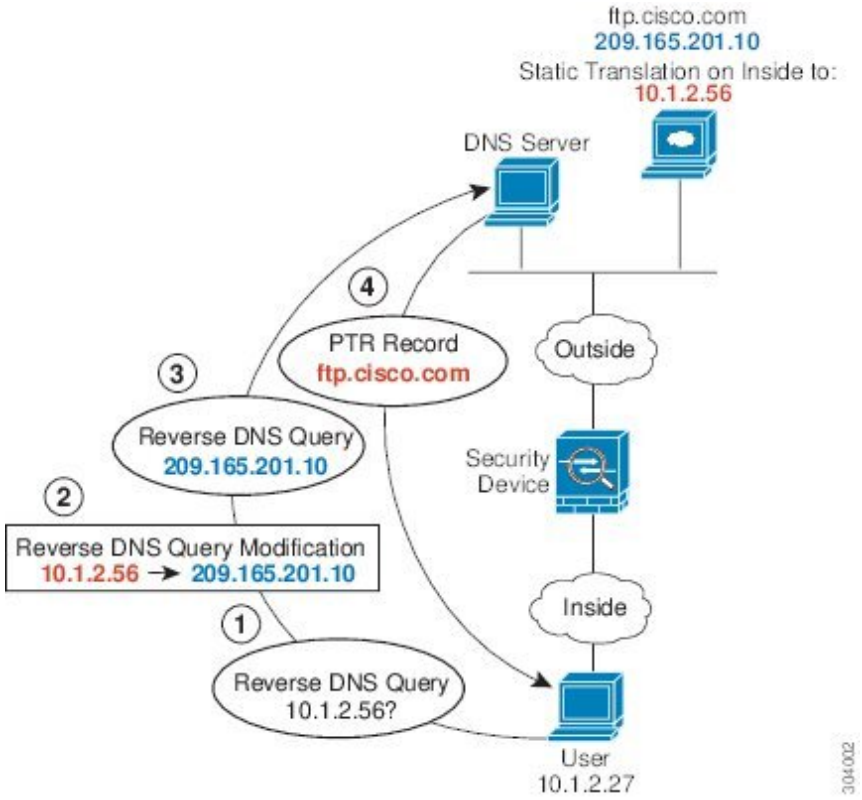
ステップ 4 内部 IPv6 ネットワークのネットワーク オブジェクトを作成して、PAT プールを設定したダイナミック NAT を設定します。

```
hostname(config)# object network IPv6_INSIDE
hostname(config-network-object)# subnet 2001:DB8::/96
hostname(config-network-object)# nat (inside,outside) dynamic pat-pool IPv4_POOL
```

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



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。