ネットワーク アドレス変換（NAT）

ここでは、ネットワーク アドレス変換（NAT）とその設定方法について説明します。

NAT を使用する理由

IP ネットワーク内の各コンピュータおよびデバイスには、ホストを識別する固有の IP アドレスが割り当てられています。パブリック IPv4 アドレスが不足しているため、これらの IP アドレスの大部分はプライベートであり、プライベートの企業ネットワークの外部にルーティングできません。RFC 1918 では、アドバタイズされない、内部で使用できるプライベート IP アドレスが次のように定義されています。

- 10.0.0.0 ～ 10.255.255.255
- 172.16.0.0 ～ 172.31.255.255
- 192.168.0.0 ～ 192.168.255.255

NAT の主な機能の 1 つは、プライベート IP ネットワークがインターネットに接続できるようにすることです。NAT は、プライベート IP アドレスをパブリック IP に置き換え、内部プライベートネットワーク内のプライベートアドレスをパブリックインターネットで使用可能な正式の、ルーティング可能なアドレスに変換します。このようにして、NAT はパブリック アドレスを節約します。これは、ネットワーク全体に対して 1 つのパブリック アドレスだけを外部に最小限にアドバタイズするように NAT を設定できるからです。

NAT の他の機能は、次のとおりです。

- セキュリティ：内部アドレスを隠蔽し、直接攻撃を防止します。
- IP ルーティング ソリューション：NAT を使用する際は、重複 IP アドレスが問題になりません。
- 柔軟性：外部で使用可能なパブリック アドレスに影響を与えずに、内部 IP アドレッシング スキームを変更できます。たとえば、インターネットにアクセス可能なサーバの場合、インターネット用に固定IPアドレスを維持できますが、内部的にはサーバのアドレスを変更できます。
- IPv4 と IPv6（ルーテッド モードのみ）の間の変換：IPv4 ネットワークに IPv6 ネットワークを接続する場合は、NAT を使用すると、2 つのタイプのアドレス間で変換を行うことができます。

（注） NAT は必須ではありません。特定のトラフィック セットに NAT を設定しない場合、そのトラフィックは変換されませんが、セキュリティ ポリシーはすべて通常どおりに適用されます。

NAT の基本

ここでは、NAT の基本について説明します。

NAT の用語

このマニュアルでは、次の用語を使用しています。

- 実際のアドレス/ホスト/ネットワーク/インターフェイス：実際のアドレスとは、ホストで定義されている、変換前のアドレスです。内部ネットワークが外部にアクセスするときに内部ネットワークを変換するという典型的な NAT のシナリオでは、内部ネットワークが「実際の」ネットワークになります。内部ネットワークだけでなく、デバイスに接続されている任意のネットワークに変換できることに注意してください。したがって、外部アドレスを変換するように NAT を設定した場合、「実際の」は、外部ネットワークが内部ネットワークにアクセスしたときの外部ネットワークを指します。
- マッピング アドレス/ホスト/ネットワーク/インターフェイス：マッピング アドレスとは、実際のアドレスが変換されるアドレスです。内部ネットワークが外部にアクセスするときに内部ネットワークを変換するという典型的なNATのシナリオでは、外部ネットワークが「マッピング」ネットワークになります。

（注） アドレスの変換中、デバイス インターフェイスに設定された IP アドレスは変換されません。

- 双方向の開始：スタティック NAT では、双方向に接続を開始できます。つまり、ホストへの接続とホストからの接続の両方を開始できます。
- 送信元および宛先の NAT：任意のパケットについて、送信元 IP アドレスと宛先 IP アドレスの両方を NAT ルールと比較し、1 つまたは両方を変換する、または変換しないことができます。スタティック NAT の場合、ルールは双方向であるため、たとえば、特定の接続が「宛先」アドレスから発生する場合でも、このガイドを通じてのコマンドおよび説明では「送信元」および「宛先」が使用されていることに注意してください。

NAT タイプ

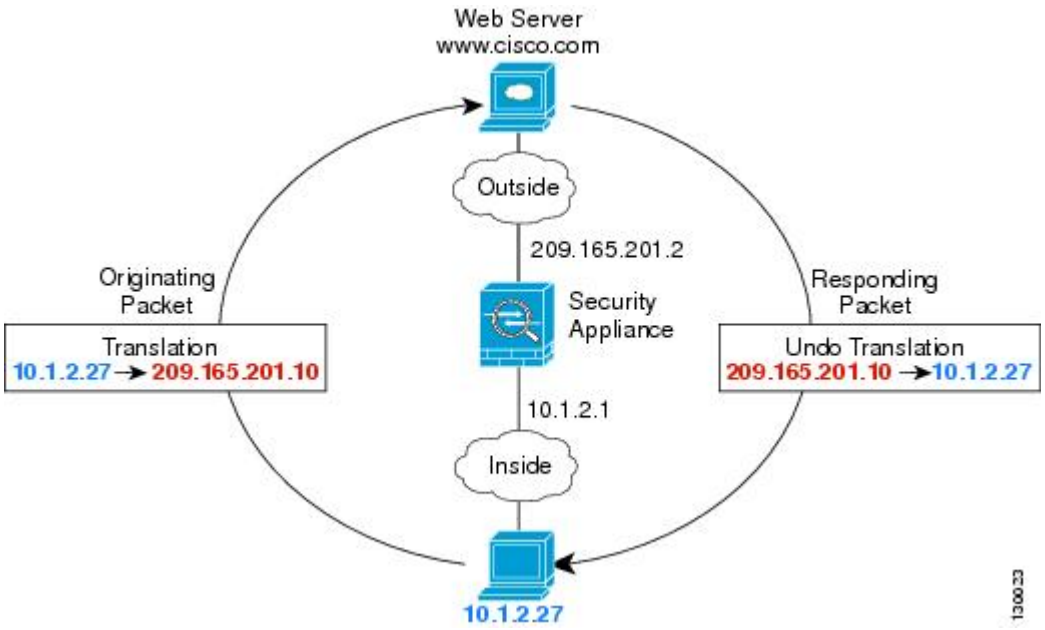
NAT は、次の方法を使用して実装できます。

- ダイナミック NAT：実際の IP アドレスのグループが、（通常は、より小さい）マッピング IP アドレスのグループに先着順でマッピングされます。実際のホストだけがトラフィックを開始できます。ダイナミック NAT, （16 ページ）を参照してください。
- ダイナミック ポート アドレス変換（PAT）：実際の IP アドレスのグループが、1 つの IP アドレスにマッピングされます。この IP アドレスのポートが使用されます。ダイナミック PAT, （22 ページ）を参照してください。
- スタティック NAT：実際の IP アドレスとマッピング IP アドレスとの間での一貫したマッピング。双方向にトラフィックを開始できます。スタティック NAT, （28 ページ）を参照してください。
- アイデンティティ NAT：実際のアドレスが同一アドレスにスタティックに変換され、基本的に NAT をバイパスします。大規模なアドレスのグループを変換するものの、小さいアドレスのサブセットは免除する場合は、NAT をこの方法で設定できます。アイデンティティ NAT, （39 ページ）を参照してください。

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 *1*：*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、Firepower Threat Defense デバイスがそのパケットを受信します。これは、Firepower Threat Defense デバイス 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. Firepower Threat Defense デバイスはその後、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。

自動 NATと 手動 NAT

自動 *NAT* および 手動 *NAT* という 2 種類の方法でアドレス変換を実装できます。

手動 NAT の追加機能を必要としない場合は、自動 NAT を使用することをお勧めします。自動 NATの設定が容易で、Voice over IP（VoIP）などのアプリケーションでは信頼性が高い場合があります（VoIP では、ルールで使用されているオブジェクトのいずれにも属さない間接アドレスの変換が失敗することがあります）。

自動 NAT

ネットワーク オブジェクトのパラメータとして設定されているすべてのNATルールは、自動*NAT*ルールと見なされます。これは、ネットワーク オブジェクトにNATを設定するための迅速かつ簡単な方法です。しかし、グループ オブジェクトに対してこれらのルールを作成することはできません。

これらのルールはオブジェクト自体の一部として設定されますが、オブジェクト マネージャを通してオブジェクト定義内の NAT 設定を確認することはできません。

パケットがインターフェイスに入ると、送信元 IP アドレスと宛先 IP アドレスの両方が自動 NAT ルールと照合されます。個別の照合が行われる場合、パケット内の送信元 IP アドレスと宛先 IP アドレスは、個別のルールによって変換できます。これらのルールは、相互に結び付けられていません。トラフィックに応じて、異なる組み合わせのルールを使用できます。

ルールがペアになることはないため、sourceA/destinationA で sourceA/destinationB とは別の変換が行われるように指定することはできません。この種の機能には、手動 NAT を使用することで、1 つのルールで送信元アドレスおよび宛先アドレスを識別できます。

手動 NAT

手動 NAT では、1 つのルールで送信元アドレスおよび宛先アドレスの両方を識別できます。送信元アドレスと宛先アドレスの両方を指定すると、sourceA/destinationA で sourceA/destinationB とは別の変換が行われるように指定できます。

（注） スタティック NAT の場合、ルールは双方向であるため、たとえば、特定の接続が「宛先」アドレスから発生する場合でも、このガイドを通じてのコマンドおよび説明では「送信元」および「宛先」が使用されていることに注意してください。たとえば、ポート アドレス変換を使用するスタティック NAT を設定し、送信元アドレスを Telnet サーバとして指定する場合に、Telnet サーバに向かうすべてのトラフィックのポートを 2323 から 23 に変換するには、変換する送信元ポート（実際：23、マッピング：2323）を指定する必要があります。Telnetサーバアドレスを送信元アドレスとして指定しているため、その送信元ポートを指定します。

宛先アドレスはオプションです。宛先アドレスを指定する場合、宛先アドレスを自身にマッピングするか（アイデンティティ NAT）、別のアドレスにマッピングできます。宛先マッピングは、常にスタティック マッピングです。

自動 NAT および手動 NAT の比較

自動 NAT と手動 NAT の主な違いは、次のとおりです。

- 実アドレスの定義方法。
  - 自動 NAT：NAT ルールがネットワーク オブジェクトのパラメータとなります。ネットワーク オブジェクトの IP アドレスは、元の（実）アドレスとして機能します。

- 手動 NAT：実アドレスおよびマッピング アドレスの両方に対し、ネットワーク オブジェクトまたはネットワーク オブジェクト グループを特定します。この場合、NAT はネットワーク オブジェクトのパラメータではありません。ネットワーク オブジェクトまたはグループが、NAT設定のパラメータとなります。実アドレスに対してネットワーク オブジェクト グループを使用できるため、手動 NAT はより高い拡張性を提供します。

- 送信元および宛先 NAT の実装方法。
  - 自動NAT：個々のルールは、パケットの送信元または宛先のどちらかに適用されます。このため、送信元 IP アドレス、宛先 IP アドレスにそれぞれ 1 つずつ、計 2 つのルールが使用される場合もあります。このような 2 つのルールを 1 つに結合し、送信元/宛先ペアに対して特定の変換を強制することはできません。
  - 手動 NAT：単一のルールが送信元と宛先の両方を変換します。1 つのパケットは 1 つのルールにしか一致せず、以降のルールはチェックされません。オプションの宛先アドレスを設定していない場合でも、パケットは 1 つの 手動 NAT ルールのみに一致します。送信元と宛先は 1 つに結合されるため、送信元/宛先ペアに応じて、異なる変換を適用できます。たとえば、送信元 A/宛先 A のペアには、送信元 A/宛先 B のペアとは異なる変換を適用できます。

- NAT ルールの順序。
  - 自動 NAT：NAT テーブル内で自動的に順序が決まります。
  - 手動 NAT：NAT テーブル内で手動で順序を決定します（自動 NAT ルールの前または後）。

NAT ルールの順序

自動 NAT ルールおよび 手動 NAT ルールは、3 つのセクションに分割される 1 つのテーブルに保存されます。最初にセクション 1 のルール、次にセクション 2、最後にセクション 3 というように、一致が見つかるまで順番に適用されます。たとえば、セクション 1 で一致が見つかった場合、セクション 2 とセクション 3 は評価されません。次の表に、各セクション内のルールの順序を示します。

表 *1*：*NAT* ルール テーブル

テーブルのセクション	ルール タイプ	セクション内のルールの順序
セクション 1	手動 NAT	コンフィギュレーションに登場する順に、最初の一致ベースで適用されます。最初の一致が適用されるため、一般的なルールの前に固有のルールが来るようにする必要があります。そうしない場合、固有のルールを期待どおりに適用できない可能性があります。デフォルトでは、手動 NAT ルールはセクション 1 に追加されます。
セクション 2	自動 NAT	セクション 1 で一致が見つからない場合、セクション 2 のルールが次の順序で適用されます。 **1** スタティック ルール。 **2** ダイナミック ルール。 **各ルール タイプでは、次の順序ガイドラインが使用されます。** **1** 実際の IP アドレスの数量：小から大の順。たとえば、アドレスが 1 個のオブジェクトは、アドレスが 10 個のオブジェクトよりも先に評価されます。 **2** 数量が同じ場合には、IP アドレス番号（最小から最大まで）が使用されます。たとえば、10.1.1.0 は、11.1.1.0 よりも先に評価されます。 **3** 同じ IP アドレスが使用される場合、ネットワーク オブジェクトの名前がアルファベット順で使用されます。たとえば、abracadabra は catwoman よりも先に評価されます。
セクション 3	手動 NAT	まだ一致が見つからない場合、セクション 3 のルールがコンフィギュレーションに登場する順に、最初の一致ベースで適用されます。このセクションには、最も一般的なルールを含める必要があります。このセクションにおいても、一般的なルールの前に固有のルールが来るようにする必要があります。そうしない場合、一般的なルールが適用されます。

たとえばセクション 2 のルールでは、ネットワーク オブジェクト内に定義されている次の IP アドレスがあるとします。

- 192.168.1.0/24（スタティック）

- 192.168.1.0/24（ダイナミック）
- 10.1.1.0/24（スタティック）
- 192.168.1.1/32（スタティック）
- 172.16.1.0/24（ダイナミック）（オブジェクト def）
- 172.16.1.0/24（ダイナミック）（オブジェクト abc）

この結果、使用される順序は次のとおりです。

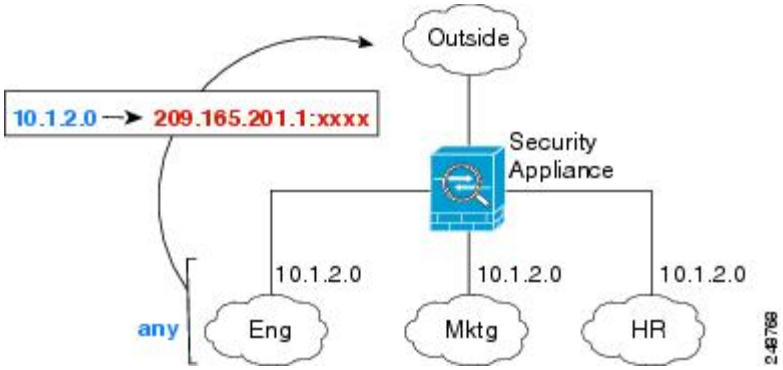
- 192.168.1.1/32（スタティック）
- 10.1.1.0/24（スタティック）
- 192.168.1.0/24（スタティック）
- 172.16.1.0/24（ダイナミック）（オブジェクト abc）
- 172.16.1.0/24（ダイナミック）（オブジェクト def）
- 192.168.1.0/24（ダイナミック）

NAT インターフェイス

ブリッジ グループ メンバー インターフェイスを除き、任意のインターフェイス（つまり、すべてのインターフェイス）に適用されるNATルールを設定したり、特定の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識別したりできます。実際のアドレスには任意のインターフェイスを指定できます。マッピング インターフェイスには特定のインターフェイスを指定できます。または、その逆も可能です。

たとえば、複数のインターフェイスで同じプライベート アドレスを使用し、外部へのアクセス時にはすべてのインターフェイスを同じグローバル プールに変換する場合、実際のアドレスに任意のインターフェイスを指定し、マッピング アドレスにはoutsideインターフェイスを指定します。

図 *2*：任意のインターフェイスの指定



ただし、「任意」のインターフェイスの概念は、ブリッジ グループ メンバー インターフェイスには適用されません。「任意」のインターフェイスを指定すると、すべてのブリッジグループメンバー インターフェイスが除外されます。そのため、ブリッジ グループ メンバーに NAT を適用するには、メンバーインターフェイスを指定する必要があります。この結果、1つのインターフェイスのみが異なる同様のルールが多数作成されることになります。ブリッジ仮想インターフェイス（BVI）自体に NAT を設定することはできず、メンバー インターフェイスにのみ NAT を設定できます。

NAT のルーティングの設定

Firepower Threat Defenseデバイスは、変換済み（マッピング）アドレスに送信されるすべてのパケットの宛先である必要があります。

パケットを送信する際の出力インターフェイスの決定に、指定した場合はその宛先インターフェイスが使用され、指定していない場合はルーティングテーブルルックアップが使用されます。アイデンティティ NAT の場合は、宛先インターフェイスを指定している場合でも、ルート ルックアップの使用を選択できます。

必要となるルーティング設定のタイプは、マッピング アドレスのタイプによって異なります。以下の各トピックでは、その詳細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、Firepower Threat Defense デバイスはプロキシ 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、Firepower Threat Defense デバイス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。外部ネットワークに十分な数の空きアドレスがあれば、このソリューションは最適です。ダイナミック NAT またはスタティック NAT など、1 対 1 の変換を使用する場合には使用を検討します。ダイナミック PAT を使用すると、少ない数のアドレスに対し、使用可能な変換アドレス数を大幅に増加できます。したがって、外部ネットワーク上で使用可能なアドレスが少ない場合でも、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。

一意のネットワーク上のアドレス

宛先（マッピング）インターフェイスのネットワーク上で使用可能な数より多くのアドレスが必要な場合は、別のサブネット上でアドレスを指定できます。上流に位置するルータには、Firepower Threat Defense デバイス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。

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。次に、実際には Firepower Threat Defense デバイス向けのパケットでない場合でも、Firepower Threat Defense デバイスはこのアドレスの ARP をプロキシします。（この問題は、手動 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 Firepower Threat Defense デバイスの ARP 応答を受信した場合、トラフィックは誤って Firepower Threat Defense デバイスに送信されます。

NAT のガイドライン

ここでは、NAT を実装するためのガイドラインについて詳細に説明します。

インターフェイスのガイドライン

NAT は、標準のルーテッド物理インターフェイスまたはサブインターフェイスでサポートされます。

ただし、ブリッジグループメンバーのインターフェイス（ブリッジ仮想インターフェイス（BVI）の一部であるインターフェイス）に NAT を設定する場合は、次の制限があります。

- ブリッジ グループのメンバーに NAT を設定するには、メンバー インターフェイスを指定します。ブリッジ グループ インターフェイス（BVI）自体に NAT を設定することはできません。
- ブリッジ グループ メンバーのインターフェイス間で NAT を実行する場合は、送信元と宛先のインターフェイスを指定する必要があります。インターフェイスとして "any" は指定できません。
- 宛先インターフェイスがブリッジグループ メンバーのインターフェイスの場合は、インターフェイスに接続された IP アドレスがないため、インターフェイス PAT は設定できません。
- 送信元と宛先のインターフェイスが同じブリッジ グループのメンバーである場合は、IPv4 ネットワークと IPv6 ネットワーク間の変換（NAT64/46）は実行できません。スタティック NAT/PAT 44/66、ダイナミック NAT44/66 およびダイナミック PAT44 のみが許可された方式です。ダイナミック PAT66 はサポートされていません。

IPv6 NAT のガイドライン

NAT では、IPv6 のサポートに次のガイドラインと制約が伴います。

- 標準のルーテッド モード インターフェイスの場合は、IPv4 と IPv6 の間の変換もできます。
- 同じブリッジ グループのメンバーであるインターフェイスの場合は、IPv4 と IPv6 の間の変換はできません。2 つの IPv6 ネットワークまたは 2 つの IPv4 ネットワークの間でのみ変換できます。この制約は、ブリッジ グループ メンバーと標準のルーティング インターフェイスの間には適用されません。
- 同じブリッジ グループに含まれるインターフェイス間で変換する場合、IPv6 のダイナミック PAT（NAT66）は使用できません。この制約は、ブリッジ グループ メンバーと標準のルーティング インターフェイスの間には適用されません。
- スタティック NAT の場合は、/64 までの IPv6 サブネットを指定できます。これよりも大きいサブネットはサポートされません。
- FTP を NAT46 とともに使用する場合は、IPv4 FTP クライアントが IPv6 FTP サーバに接続するときに、クライアントは拡張パッシブ モード（EPSV）または拡張ポート モード（EPRT）を使用する必要があります。PASV コマンドおよび PORT コマンドは IPv6 ではサポートされません。

IPv6 NAT の推奨事項

NAT を使用すると、IPv6 ネットワーク間、さらに IPv4 および IPv6 ネットワークの間で変換できます（ルーテッド モードのみ）。次のベスト プラクティスを推奨します。

- NAT66（IPv6-to-IPv6）：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。リターン トラフィックを許可しない場合は、スタティック NAT ルールを単一方向にできます（手動 NAT のみ）。
- NAT46（IPv4-to-IPv6）：スタティック NAT を使用することを推奨します。IPv6 アドレス空間は IPv4 アドレス空間よりもかなり大きいため、容易にスタティック変換に対応できます。リターン トラフィックを許可しない場合は、スタティック NAT ルールを単一方向にできます（手動 NAT のみ）。IPv6 サブネットに変換する場合（/96 以下）、結果のマッピング アドレスはデフォルトで IPv4 埋め込み IPv6 アドレスとなります。このアドレスでは、IPv4 アドレスの 32 ビットが IPv6 プレフィックスの後に埋め込まれています。たとえば、IPv6 プレフィックスが /96 プレフィックスの場合、IPv4 アドレスは、アドレスの最後の 32 ビットに追加されます。たとえば、201b::0/96 に 192.168.1.0/24 をマッピングする場合、192.168.1.4 は 201b::0.192.168.1.4 にマッピングされます（混合表記で表示）。/64 など、より小さいプレフィックスの場合、IPv4 アドレスがプレフィックスの後に追加され、サフィックスの 0s が IPv4 アドレスの後に追加されます。

- NAT64（IPv6-to-IPv4）：IPv6 アドレスの数に対応できる十分な数の IPv4 アドレスがない場合があります。大量の IPv4 変換を提供するためにダイナミック PAT プールを使用することを推奨します。

インスペクション対象プロトコルに対する NAT サポート

セカンダリ接続を開くアプリケーション層プロトコルの一部、またはパケットに IP アドレスを埋め込んだアプリケーション層プロトコルの一部は、次のサービスを提供するためにインスペクションが実行されます。

- ピンホールの作成：一部のアプリケーション プロトコルは、標準ポートまたはネゴシエートされたポートでセカンダリ TCP または UDP 接続を開きます。インスペクションでは、これらのセカンダリ ポートのピンホールが開くため、ユーザはそれらを許可するアクセス コントロール ルールを作成する必要はありません。
- NAT の書き換え：プロトコルの一部としてのパケット データ内のセカンダリ接続用の FTP 埋め込み型 IP アドレスおよびポートなどのプロトコル。エンドポイントのいずれかに関与する NAT 変換がある場合、インスペクション エンジンは、埋め込まれたアドレスおよびポートの NAT 変換を反映するようにパケット データを書き換えます。セカンダリ接続は NAT の書き換えがないと動作しません。
- プロトコルの強制：一部のインスペクションでは、インスペクション対象プロトコルにある程度の RFC への準拠が強制されます。

次の表に、NAT の書き換えと NAT の制限事項を適用するインスペクション対象プロトコルを示します。これらのプロトコルを含む NAT ルールの作成時は、これらの制限事項に留意してください。ここに記載されていないインスペクション対象プロトコルは NAT の書き換えを適用しません。これらのインスペクションには、GTP、HTTP、IMAP、POP、SMTP、SSH、および SSL が含まれます。

（注） NAT の書き換えは、リストされているポートでのみサポートされます。非標準ポートでこれらのプロトコルを使用する場合は、接続で NAT を使用しないでください。

表 *2*：*NAT* のサポート対象アプリケーション インスペクション

アプリケーション	インスペクション対象プロトコル、ポート	NAT に関する制限事項	作成済みのピンホール
DCERPC	TCP/135	NAT64 なし。	○
DNS over UDP	UDP/53	NAT サポートは、WINS 経由の名前解決では使用できません。	×
ESMTP	TCP/25	NAT64 なし。	×

アプリケーション	インスペクション対象プロトコル、ポート	NAT に関する制限事項	作成済みのピンホール
FTP	TCP/21	制限なし。	○
H.323 H.225（コールシグナリング） H.323 RAS	TCP/1720 UDP/1718 For RAS、UDP/1718-1719	NAT64 なし。	○
ICMP ICMP エラー	ICMP （デバイス インターフェイスに送信される ICMP トラフィックのインスペクションは実行されません。）	制限なし。	×
IP オプション	RSVP	NAT64 なし。	×
NetBIOS Name Server over IP	UDP/137、138（送信元ポート）	NAT64 なし。	×
RSH	TCP/514	PAT なし。 NAT64 なし。	○
RTSP	TCP/554 （HTTP クローキングは処理しません）。	NAT64 なし。	○
SIP	TCP/5060 UDP/5060	拡張 PAT なし。 NAT64 または NAT46 はなし。	○
Skinny（SCCP）	TCP/2000	NAT64、NAT46、または NAT66 はなし。	○
SQL*Net （バージョン 1、2）	TCP/1521	NAT64 なし。	○
Sun RPC	UDP/111	NAT64 なし。	○
TFTP	UDP/69	NAT64 なし。 ペイロード IP アドレスは変換されません。	○
XDMCP	UDP/177	NAT64 なし。	○

NAT のその他のガイドライン

- ブリッジ グループのメンバーになっているインターフェイス用に、メンバー インターフェイスの NAT ルールを作成します。ブリッジ仮想インターフェイス（BVI）自体の NAT ルールを作成することはできません。
- （自動 NAT のみ）特定のオブジェクトに対して 1 つの NAT ルールだけを定義できます。オブジェクトに対して複数の NAT ルールを設定する場合は、同じ IP アドレスを指定する異なる名前の複数のオブジェクトを作成する必要があります。
- インターフェイスで VPN が定義されている場合、インターフェイス上の着信 ESP トラフィックは NAT ルールの影響を受けません。確立された VPN トンネルについてのみ ESP トラフィックが許可され、既存のトンネルに関連付けられていないトラフィックはドロップされます。この制限は ESP および UDP ポートの 500 および 4500 に適用されます。
- （手動 NATのみ）送信元 IP アドレスがサブネットの場合は、FTP またはセカンダリ接続を使用する他のアプリケーションに対し宛先ポート変換を設定することはできません。FTP データ チャネルの確立は成功しません。
- NAT コンフィギュレーションを変更したときに、既存の変換がタイムアウトするまで待たずに新しい NAT コンフィギュレーションが使用されるようにするには、デバイスの CLI で clear xlate コマンドを使用して変換テーブルを消去できます。ただし、変換テーブルを消去すると、変換を使用している現在の接続がすべて切断されます。

（注） ダイナミック NAT または PAT ルールを削除し、次に削除したルールに含まれるアドレスと重複するマッピング アドレスを含む新しいルールを追加すると、新しいルールは、削除されたルールに関連付けられたすべての接続がタイムアウトするか、clear xlate コマンドを使用してクリアされるまで使用されません。この予防手段のおかげで、同じアドレスが複数のホストに割り当てられないようにできます。

- 1 つのオブジェクト グループに IPv4 と IPv6 の両方のアドレスを入れることはできません。オブジェクト グループには、1 つのタイプのアドレスだけが含まれている必要があります。
- （手動 NATのみ）発信元アドレスとして **any** を NAT ルールで使用する場合、「any」トラフィックの定義（IPv4 と IPv6）はルールによって異なります。Firepower Threat Defense デバイスがパケットに対して NAT を実行する前に、パケットが IPv6-to-IPv6 または IPv4-to-IPv4 である必要があります。この前提条件では、Firepower Threat Defense デバイスは、NAT ルールの **any** の値を決定できます。たとえば、「any」から IPv6 サーバへのルールを設定しており、このサーバが IPv4 アドレスからマッピングされている場合、**any** は「任意の IPv6 トラフィック」を意味します。「any」から「any」へのルールを設定しており、送信元をインターフェイス IPv4 アドレスにマッピングする場合、マッピングされたインターフェイス アドレスによって宛先も IPv4 であることが示されるため、**any** は「任意の IPv4 トラフィック」を意味します。
- 同じマッピング オブジェクトやグループを複数の NAT ルールで使用できます。

- マッピング IP アドレス プールは、次のアドレスを含むことができません。
  - マッピング インターフェイスの IP アドレス。ルールに「Any」インターフェイスを指定すると、すべてのインターフェイスの IP アドレスが拒否されます。インターフェイス PAT（ルーテッド モードのみ）の場合は、インターフェイス アドレスの代わりにインターフェイス名を指定します。
  - フェールオーバー インターフェイスの IP アドレス。
  - （ダイナミック NAT）VPN がイネーブルの場合は、スタンバイ インターフェイスの IP アドレス。
- スタティックおよびダイナミック NAT ポリシーでは重複アドレスを使用しないでください。たとえば、重複アドレスを使用すると、PPTP のセカンダリ接続がダイナミック xlate ではなくスタティックにヒットした場合、PPTP 接続の確立に失敗する可能性があります。
- ルールで宛先インターフェイスを指定すると、ルーティング テーブルでルートが検索されるのではなく、そのインターフェイスが出力インターフェイスとして使用されます。ただし、アイデンティティ NAT の場合は、代わりにルート ルックアップを使用するオプションがあります。

NAT の設定

ネットワーク アドレス変換は、かなり複雑になる場合があります。変換問題や困難なトラブルシューティング状況を回避するため、ルールを可能なかぎりシンプルに保つことをお勧めします。NAT を実装する前に慎重に計画することが非常に重要です。次の手順は、基本的なアプローチを示しています。

手順

ステップ 1 [ポリシー（Policies）] > [NAT] を選択します。

ステップ 2 必要なルールの種類を決定します。
ダイナミック NAT、ダイナミック PAT、スタティック NAT およびアイデンティティ NAT のルールを作成できます。概要については、NAT タイプ, （3 ページ）を参照してください。

ステップ 3 手動 NAT または自動 NAT として実装するルールを決定します。
これらの 2 つの実装オプションの比較については、自動 NATと 手動 NAT, （4 ページ）を参照してください。

ステップ 4 以降で説明する手順に従って、ルールを作成します。

- ダイナミック NAT, （16 ページ）
- ダイナミック PAT, （22 ページ）
- スタティック NAT, （28 ページ）
- アイデンティティ NAT, （39 ページ）

ステップ 5 NAT ポリシーおよびルールを管理します。
ポリシーとルールを管理するには、次の手順を実行します。

- ルールを編集するには、ルールの編集アイコン（）をクリックします。
- ルールを削除するには、ルールの削除アイコン（）をクリックします。

ダイナミック NAT

以下の各トピックでは、ダイナミック NAT とその設定方法について説明します。

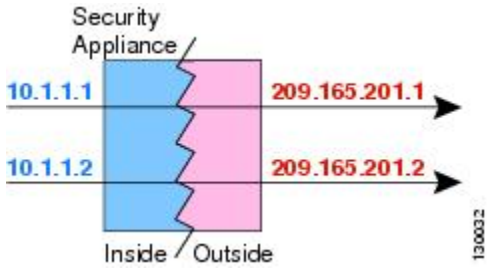
ダイナミック NAT について

ダイナミック NAT は、宛先ネットワーク上でルーティング可能なマッピング アドレスのプールに、実アドレスのグループを変換する機能です。マッピング プールには通常、実際のグループより少ない数のアドレスが含められます。変換しようとするホストが宛先ネットワークにアクセスすると、NAT はマッピング プール内の IP アドレスをこのホストに割り当てます。この変換は、実際のホストが接続を開始する時点のみに行われます。この接続が終了するまでの時間に限り、変換アドレスは有効であり、変換アドレスの有効時間が経過した後は、ユーザは同一の IP アドレスを維持することはありません。したがって、宛先ネットワーク上のユーザは、ダイナミック NAT を使用するホストへの安定した接続を開始することができません。これは、接続がアクセス ルールによって許可されている場合でも同様です。

（注） 変換の有効時間内であれば、アクセス ルールによって許可されている場合、リモート ホストは変換されたホストへの接続を開始できます。アドレスが予測できないため、ホストへの接続は成功しにくくなります。しかし、この場合でも、アクセス ルールのセキュリティは信頼できます。

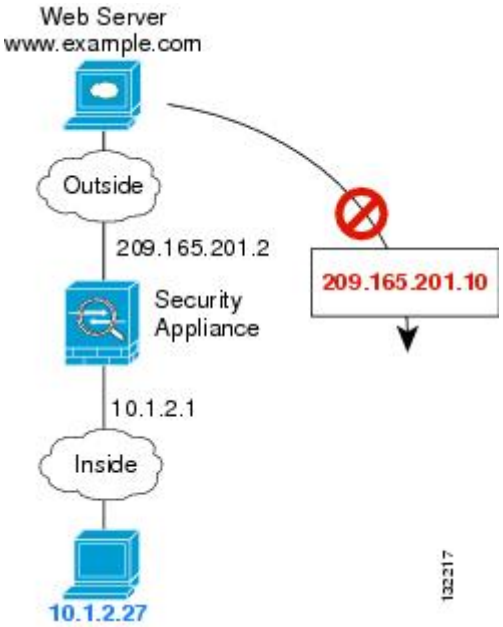
次の図は、ダイナミック NAT の一般的なシナリオを示します。実際のホストのみが NAT セッションを作成でき、応答トラフィックは送信元に戻ることを許可されます。

図 *3*：ダイナミック *NAT*



次の図は、マッピングアドレスに対して接続を開始しようとするリモートホストを示します。このアドレスは現時点で変換テーブルに存在しないため、パケットは破棄されます。

図 4：マッピング アドレスへの接続開始を試みるリモート ホスト



ダイナミック NAT の欠点と利点

ダイナミック NAT には、以下の欠点があります。

- マッピング プール内のアドレスの数が実際のグループより少ない場合は、トラフィック量が予想を上回るとアドレスが不足する可能性があります。

  この現象が頻繁に発生する場合は、PAT または PAT フォールバック方式を使用します。PAT を使用すると、単一アドレスのポートを使用して 64,000 以上の変換を実行できます。

- ルーティング可能なアドレスをマッピング プールで大量に使用する必要がありますが、大量のルーティング可能アドレスを使用できない場合があります。

ダイナミック NAT の利点は、PAT を使用できない一部のプロトコルにも対応可能であることです。PAT は、以下の状況では動作しません。

- オーバーロード ポートを持たない IP プロトコル（GRE バージョン 0 など）での使用
- データ ストリームと制御パスを異なるポートで送受信する、非オープン スタンダードの一部のマルチメディア アプリケーションでの使用

ダイナミック自動 NAT の設定

ダイナミック自動 NAT ルールは、宛先ネットワーク上でルーティング可能な、別の IP アドレスにアドレスを変換する機能です。

はじめる前に

[オブジェクト（Objects）]を選択し、ルールに必要なネットワーク オブジェクトまたはグループを作成します。または、NAT ルールを定義するときにオブジェクトを作成することもできます。オブジェクトは、以下の要件を満たしている必要があります。

- [元のアドレス（Original Address）]：ネットワーク オブジェクトである必要があります。（グループは不可）。ホストまたはサブネットを含めることができます。
- [変換済みアドレス（Translated Address）]：ネットワーク オブジェクトまたはグループ。サブネットを含めることはできません。IPv4 アドレスと IPv6 アドレスの両方をグループに入れることはできません。1 つのタイプだけが含まれている必要があります。

手順

ステップ 1 [ポリシー（Policies）] > [NAT] を選択します。

ステップ 2 次のいずれかを実行します。

- ルールを新規作成するには、[+]ボタンをクリックします。
- 既存のルールを編集するには、このルールの編集アイコン（）をクリックします

（不要になったルールを削除するには、このルールのごみ箱アイコンをクリック）。

ステップ 3 基本的なルール オプションを設定します。

- [タイトル（Title）]：ルールの名前を入力します。
- [作成するルールの適用対象（Create Rule For）]：[自動 NAT（Auto NAT）] を選択します。
- [タイプ（Type）]：[ダイナミック（Dynamic）] を選択します。

ステップ 4 以下のパケット変換オプションを設定します。

- [送信元インターフェイス（Source Interface）]、[宛先インターフェイス（Destination Interface）]：（ブリッジ グループのメンバー インターフェイスに必要）この NAT ルールを適用するインターフェイス。送信元は、トラフィックがデバイスに通過する入口となる、実際のインターフェイスです。宛先は、デバイスを通過したトラフィックの出口となる、マッピング インターフェイスです。デフォルトでは、ルールはすべてのインターフェイスに適用されますが（[すべて（Any）]）、ブリッジ グループのメンバー インターフェイスは例外です。
- [元のアドレス（Original Address）]：変換対象のアドレスを保持するネットワーク オブジェクト。

- [変換済みアドレス（Translated Address）]：マッピング アドレスを保持するネットワーク オブジェクトまたはグループ。

ステップ 5 （オプション）[詳細オプション（Advanced Options）]リンクをクリックし、必要なオプションを選択します。

- [このルールと一致する DNS 応答を変換（Translate DNS replies that match this rule）]：DNS 応答内の IP アドレスを変換するかどうか。マッピングされたインターフェイスから実際のインターフェイスへの DNS 応答の場合、Address レコード（IPv4 では A レコード、IPv6 では AAAA 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。反対に、実際のインターフェイスからマッピングされたインターフェイスへの DNS 応答の場合、このレコードは実際の値からマッピングされた値に書き換えられます。このオプションは特定の状況で使用します。また、NAT64/46 変換により、書き換えによって A レコードと AAAA レコードとが交換される場合にも必要となることがあります。詳細については、NAT による DNS クエリおよび応答のリライト，（86 ページ）を参照してください。
- [インターフェイス PAT へのフォールスルー（宛先インターフェイス）（Fallthrough to Interface PAT (Destination Interface)）]：相手のマッピング アドレスがすでに割り当て済みの場合、バックアップとして、宛先インターフェイスの IP アドレスを使用するかどうか（インターフェイス PAT フォールバック）。このオプションは、ブリッジ グループのメンバーではない宛先インターフェイスを選択する場合のみに使用できます。

ステップ 6 [OK]をクリックします。

ダイナミック手動 NAT の設定

自動 NAT では要件を満たせない場合は、ダイナミックな手動 NAT ルールを使用します。たとえば、宛先に応じて異なる変換を行いたいような場合です。ダイナミック NAT は、宛先ネットワーク上でルーティング可能な、別の IP アドレスにアドレスを変換する機能です。

はじめる前に

[オブジェクト（Objects）]を選択し、ルールに必要なネットワーク オブジェクトまたはグループを作成します。IPv4 アドレスと IPv6 アドレスの両方をグループに入れることはできません。1 つのタイプだけが含まれている必要があります。または、NAT ルールを定義するときにオブジェクトを作成することもできます。オブジェクトは、以下の要件も満たしている必要があります。

- [元の送信元アドレス（Original Source Address）]：ネットワーク オブジェクトまたはグループ。ここには、ホストまたはサブネットを含めることができます。元の送信元トラフィックをすべて変換するには、この手順を省略し、ルールに [すべて（Any）]を指定します。
- [変換済み送信元アドレス（Translated Source Address）]：ネットワーク オブジェクトまたはグループ。サブネットを含めることはできません。

宛先アドレスのスタティックな変換をルール内で設定する場合は、[元の宛先アドレス（Original Destination Address）]および [変換済み宛先アドレス（Translated Destination Address）] のネットワーク オブジェクトを作成することもできます。

ダイナミック NAT の場合、接続先でポート変換を実行することもできます。Object Manager で、[元の宛先ポート（Original Destination Port）]と [変換済み宛先ポート（Translated Destination Port）] のそれぞれに使用可能なポート オブジェクトがあることを確認します。送信元ポートを指定した場合、無視されます。

手順

ステップ 1 [ポリシー（Policies）] > [NAT] を選択します。

ステップ 2 次のいずれかを実行します。

- ルールを新規作成するには、[+]ボタンをクリックします。
- 既存のルールを編集するには、このルールの編集アイコン（  ）をクリックします

（不要になったルールを削除するには、このルールのごみ箱アイコンをクリック）。

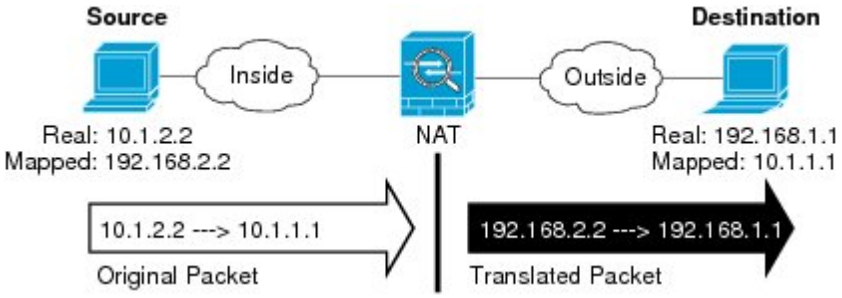
ステップ 3 基本的なルール オプションを設定します。

- [タイトル（Title）]：ルールの名前を入力します。
- [作成するルールの適用対象（Create Rule For）]：[手動 NAT（Manual NAT）] を選択します。
- [ルールの配置（Rule Placement）]：ルールを追加する位置。ルールはカテゴリ内に挿入することも（自動 NAT ルールの前または後）、選択したルールの前または後に挿入することもできます。
- [タイプ（Type）]：[ダイナミック（Dynamic）]を選択します。この設定は、送信元アドレスのみに適用されます。宛先アドレスに変換を定義する場合は、変換のタイプは常にスタティックとなります。

ステップ 4 以下のインターフェイス オプションを設定します。

- [送信元インターフェイス（Source Interface）]、[宛先インターフェイス（Destination Interface）]：（ブリッジ グループのメンバー インターフェイスに必要）この NAT ルールを適用するインターフェイス。送信元は、トラフィックがデバイスに通過する入口となる、実際のインターフェイスです。宛先は、デバイスを通過したトラフィックの出口となる、マッピング インターフェイスです。デフォルトでは、ルールはすべてのインターフェイスに適用されますが（[すべて（Any）]）、ブリッジ グループのメンバー インターフェイスは例外です。

ステップ 5 元のパケット アドレス（IPv4 または IPv6）を識別します。これは、元のパケットに表示されていた パケット アドレスです。
元のパケットと変換済みパケットの例については、次の図を参照してください。



- [元の発信元アドレス（Original Source Address）]：変換対象のアドレスを保持するネットワーク オブジェクトまたはグループ。
- [元の宛先アドレス（Original Destination Address）]：（オプション）宛先のアドレスを含むネットワーク オブジェクト。空白のままにすると、宛先にかかわらず、送信元アドレスの変換が適用されます。宛先アドレスを指定する場合は、このアドレスにスタティック変換を設定するか、単にアイデンティティ NAT を使用します。

  [インターフェイス（Interface）][送信元インターフェイス IP（Source Interface IP）] を選択すると、元の宛先を送信元インターフェイス（[すべて（Any)] 以外）に基づいて決定できます。このオプションを選択した場合は、変換済み接続先オブジェクトも選択する必要があります。スタティック インターフェイス NAT、および宛先アドレスへのポート変換を実装するには、このオプションを選択し、宛先ポートの適切なポート オブジェクトを選択します。

ステップ 6 変換済みパケット アドレス（IPv4 または IPv6）を識別します。これは、宛先インターフェイスのネットワークで表示されるパケット アドレスです。必要に応じて、IPv4 と IPv6 の間で変換できます。

- [変換済み送信元アドレス（Translated Source Address）]：マッピング アドレスを保持するネットワーク オブジェクトまたはグループ。
- [変換済み宛先アドレス（Translated Destination Address）]：（オプション）変換済みパケットに使用される宛先アドレスを保持するネットワーク オブジェクトまたはグループ。[元の宛先アドレス（Original Destination Address）]にオブジェクトを選択している場合は、同じオブジェクトを選択してアイデンティティ NAT（変換なし）を設定できます。

ステップ 7 （オプション）サービス変換の宛先サービス ポートを識別します（[元の宛先ポート（Original Destination Port）]、[変換済み宛先ポート（Translated Destination Port）]）。
ダイナミック NAT ではポート変換はサポートされません。したがって、[元の送信元ポート（Original Source Port）]および [変換済み送信元ポート（Translated Source Port）]フィールドは空白のままにしておきます。しかし、宛先変換は常にスタティックであるため、宛先ポートに対してポート変換を実行できます。

NAT では、TCP または UDP のみがサポートされますポートを変換する場合、実際のサービス オブジェクトのプロトコルとマッピング サービス オブジェクトのプロトコルの両方を同じにします（両方とも TCP または両方とも UDP）。アイデンティティ NAT では、実際のポートとマッピング ポートの両方に同じサービス オブジェクトを使用できます。

ステップ 8 （オプション）[詳細オプション（Advanced Options）]リンクをクリックし、必要なオプションを選択します。

- [このルールと一致する DNS 応答を変換（Translate DNS replies that match this rule）]：DNS 応答内の IP アドレスを変換するかどうか。マッピングされたインターフェイスから実際のインターフェイスへの DNS 応答の場合、Address レコード（IPv4 では A レコード、IPv6 では AAAA 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。反対に、実際のインターフェイスからマッピングされたインターフェイスへの DNS 応答の場合、このレコードは実際の値からマッピングされた値に書き換えられます。このオプションは特定の状況で使用します。また、NAT64/46 変換により、書き換えによって A レコードと AAAA レコードとが交換される場合にも必要となることがあります。詳細については、NAT による DNS クエリおよび応答のリライト，（86 ページ）を参照してください。
- [インターフェイス PAT へのフォールスルー（宛先インターフェイス）（Fallthrough to Interface PAT (Destination Interface)）]：相手のマッピング アドレスがすでに割り当て済みの場合、バックアップとして、宛先インターフェイスの IP アドレスを使用するかどうか（インターフェイス PAT フォールバック）。このオプションは、ブリッジ グループのメンバーではない宛先インターフェイスを選択する場合のみに使用できます。

ステップ 9 [OK]をクリックします。

ダイナミック PAT

以下の各トピックでは、ダイナミック PAT について説明します。

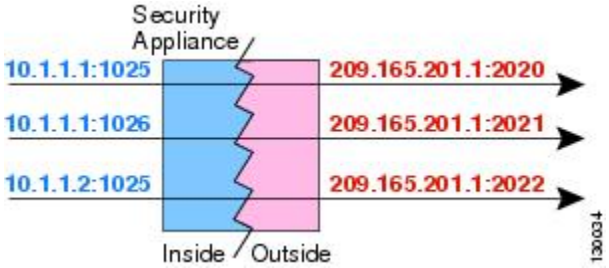
ダイナミック PAT について

ダイナミック PAT は、実アドレスと送信元ポートとを、マッピング アドレスおよび一意のポートに変換することで、複数の実アドレスを 1 つのマッピング IP アドレスに変換する機能です。使用可能である場合は、実際の送信元ポートの番号がマッピング ポートにも使用されます。ただし、実際のポートが使用できない場合は、デフォルトで、マッピング ポートは実際のポート番号と同じポート範囲（0 ～ 511、512 ～ 1023、および 1024 ～ 65535）から選択されます。したがって、1024 以下のポートは、使用可能な PAT プールがごく小さくなります。

送信元ポートは接続ごとに異なるため、個々の接続に個別の変換セッションが必要となります。たとえば、10.1.1.1:1025 には 10.1.1.1:1026 とは異なる変換が必要です。

次の図は、ダイナミック PAT の一般的なシナリオを示します。実際のホストのみが NAT セッションを作成でき、応答トラフィックは送信元に戻ることを許可されます。変換の都度、同じマッピング アドレスが使用されますが、ポートは動的に割り当てられます。

図 *5*：ダイナミック *PAT*



変換の有効時間内であれば、アクセス ルールによって許可されている場合、宛先ネットワーク上のリモート ホストは変換されたホストへの接続を開始できます。ポート アドレス（実際のアドレスおよびマッピング アドレス）が予測できないため、ホストへの接続は成功しにくくなります。しかし、この場合でも、アクセス ルールのセキュリティは信頼できます。

接続が有効期限切れになると、ポート変換も期限切れとなります。

ダイナミック PAT の欠点と利点

ダイナミック PAT を使用すると、単一のマッピング アドレスを使用できるため、ルーティング可能なアドレスを節約できます。Firepower Threat Defense デバイスのインターフェイス IP アドレスを PAT アドレスとして使用することもできます。ただし、インターフェイス上で、IPv6 アドレスに対するインターフェイス PAT を使用することはできません。

同じブリッジ グループに含まれるインターフェイス間で変換する場合、IPv6 のダイナミック PAT（NAT66）は使用できません。この制約は、ブリッジ グループ メンバーと標準のルーティング インターフェイスの間には適用されません。

ダイナミック PAT は、制御パスとは異なるデータ ストリームを持つ一部のマルチメディア アプリケーションでは無効になります。詳細については、インスペクション対象プロトコルに対する NAT サポート，（12 ページ） を参照してください。

ダイナミック PAT により、大量の接続が単一の IP アドレスから送信されているように見えることがあり、サーバがこのトラフィックを DoS 攻撃と解釈してしまう場合があります。

ダイナミック自動 PAT の設定

ダイナミック自動 PAT ルールは、アドレスを複数の IP アドレスのみに変換するのではなく、一意の IP アドレスおよびポートの組み合わせに変換する場合に使用します。アドレスは、単一のアドレス（宛先インターフェイスのアドレス、または別のアドレス）に変換できます。

はじめる前に

[オブジェクト（Objects）]を選択し、ルールに必要なネットワーク オブジェクトまたはグループを作成します。または、NAT ルールを定義するときにオブジェクトを作成することもできます。オブジェクトは、以下の要件を満たしている必要があります。

- [元のアドレス（Original Address）]：ネットワーク オブジェクトである必要があります。（グループは不可）。ホストまたはサブネットを含めることができます。
- [変換済みアドレス（Translated Address）]：以下のオプションを使用して PAT アドレスを指定できます。
  - [宛先インターフェイス（Destination Interface）]：宛先インターフェイスの IPv4 アドレスを使用する場合は、ネットワーク オブジェクトは不要です。IPv6 にインターフェイス PAT を使用することはできません。
  - [単一の PAT アドレス（Single PAT address）]：単一ホストを保持するネットワーク オブジェクトを作成します。

手順

ステップ 1 [ポリシー（Policies）] > [NAT] を選択します。

ステップ 2 次のいずれかを実行します。

- ルールを新規作成するには、[+]ボタンをクリックします。
- 既存のルールを編集するには、このルールの編集アイコン（  ）をクリックします

（不要になったルールを削除するには、このルールのごみ箱アイコンをクリック）。

ステップ 3 基本的なルール オプションを設定します。

- [タイトル（Title）]：ルールの名前を入力します。
- [作成するルールの適用対象（Create Rule For）]：[自動 NAT（Auto NAT）] を選択します。
- [タイプ（Type）]：[ダイナミック（Dynamic）] を選択します。

ステップ 4 以下のパケット変換オプションを設定します。

- [送信元インターフェイス（Source Interface）]、[宛先インターフェイス（Destination Interface）]：（ブリッジ グループのメンバー インターフェイスに必要）この NAT ルールを適用するインターフェイス。送信元は、トラフィックがデバイスに通過する入口となる、実際のインターフェイスです。宛先は、デバイスを通過したトラフィックの出口となる、マッピング インターフェイスです。デフォルトでは、ルールはすべてのインターフェイスに適用されますが（[すべて（Any）]）、ブリッジ グループのメンバー インターフェイスは例外です。

- [元のアドレス（Original Address）]：変換対象のアドレスを保持するネットワーク オブジェクト。
- [変換済みアドレス（Translated Address）]：以下のいずれかを設定します。
  - （インターフェイス PAT）宛先インターフェイスの IPv4 アドレスを使用するには、[インターフェイス（Interface）]を選択します。また、特定の宛先インターフェイスを選択する必要があります。これには、ブリッジ グループのメンバー インターフェイスは使用できません。IPv6 にインターフェイス PAT を使用することはできません。
  - 宛先インターフェイス以外の単一アドレスを使用するには、この用途で作成したホスト ネットワーク オブジェクトを選択します。

ステップ 5 （オプション）[詳細オプション（Advanced Options）]リンクをクリックし、必要なオプションを選択します。

- [インターフェイス PAT へのフォールスルー（宛先インターフェイス）（Fallthrough to Interface PAT (Destination Interface)）]：相手のマッピング アドレスがすでに割り当て済みの場合、バックアップとして、宛先インターフェイスの IP アドレスを使用するかどうか（インターフェイス PAT フォールバック）。このオプションは、ブリッジ グループのメンバーではない宛先インターフェイスを選択する場合のみに使用できます。すでにインターフェイス PAT を変換済みアドレスとして設定している場合には、このオプションは使用できません。また、IPv6 ネットワークでこのオプションを使用することはできません。

ステップ 6 [OK]をクリックします。

ダイナミック手動 PAT の設定

自動 PAT では要件を満たせない場合は、ダイナミックな手動 PAT ルールを使用します。たとえば、宛先に応じて異なる変換を行いたいような場合です。ダイナミック PAT では、アドレスを複数の IP アドレスのみに変換するのではなく、一意の IP アドレスおよびポートの組み合わせに変換します。アドレスは、単一のアドレス（宛先インターフェイスのアドレス、または別のアドレス）に変換できます。

はじめる前に

[オブジェクト（Objects）]を選択し、ルールに必要なネットワーク オブジェクトまたはグループを作成します。IPv4 アドレスと IPv6 アドレスの両方をグループに入れることはできません。1 つのタイプだけが含まれている必要があります。または、NAT ルールを定義するときにオブジェクトを作成することもできます。オブジェクトは、以下の要件も満たしている必要があります。

- [元の送信元アドレス（Original Source Address）]：ネットワーク オブジェクトまたはグループ。ここには、ホストまたはサブネットを含めることができます。元の送信元トラフィックをすべて変換するには、この手順を省略し、ルールに [すべて（Any）]を指定します。

- [変換済み送信元アドレス（Translated Source Address）]：以下のオプションを使用して PAT アドレスを指定できます。
  - [宛先インターフェイス（Destination Interface）]：宛先インターフェイスの IPv4 アドレスを使用する場合は、ネットワーク オブジェクトは不要です。IPv6 にインターフェイス PAT を使用することはできません。
  - [単一の PAT アドレス（Single PAT address）]：単一ホストを保持するネットワーク オブジェクトを作成します。

宛先アドレスのスタティックな変換をルール内で設定する場合は、[元の宛先アドレス（Original Destination Address）]および [変換済み宛先アドレス（Translated Destination Address）] のネットワーク オブジェクトを作成することもできます。

ダイナミック PAT の場合、接続先でポート変換を実行することもできます。Object Manager で、[元の宛先ポート（Original Destination Port）]と [変換済み宛先ポート（Translated Destination Port）] のそれぞれに使用可能なポート オブジェクトがあることを確認します。送信元ポートを指定した場合、無視されます。

手順

ステップ 1 [ポリシー（Policies）] > [NAT] を選択します。

ステップ 2 次のいずれかを実行します。

- ルールを新規作成するには、[+]ボタンをクリックします。
- 既存のルールを編集するには、このルールの編集アイコン（）をクリックします

（不要になったルールを削除するには、このルールのごみ箱アイコンをクリック）。

ステップ 3 基本的なルール オプションを設定します。

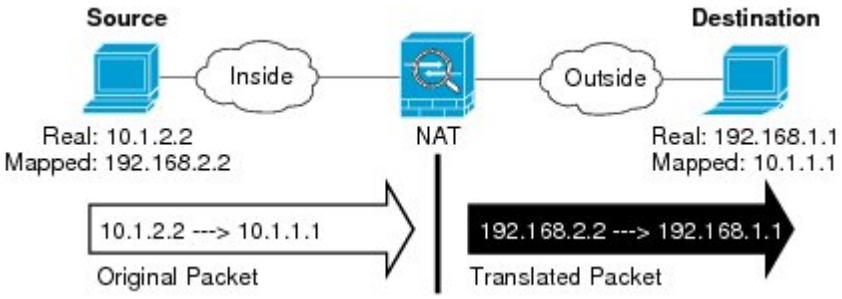
- [タイトル（Title）]：ルールの名前を入力します。
- [作成するルールの適用対象（Create Rule For）]：[手動 NAT（Manual NAT）] を選択します。
- [ルールの配置（Rule Placement）]：ルールを追加する位置。ルールはカテゴリ内に挿入することも（自動 NAT ルールの前または後）、選択したルールの前または後に挿入することもできます。
- [タイプ（Type）]：[ダイナミック（Dynamic）]を選択します。この設定は、送信元アドレスのみに適用されます。宛先アドレスに変換を定義する場合は、変換のタイプは常にスタティックとなります。

ステップ 4 以下のインターフェイス オプションを設定します。

- [送信元インターフェイス（Source Interface）]、[宛先インターフェイス（Destination Interface）]：（ブリッジ グループのメンバー インターフェイスに必要）この NAT ルールを適用するインターフェイス。送信元は、トラフィックがデバイスに通過する入口となる、実

際のインターフェイスです。宛先は、デバイスを通過したトラフィックの出口となる、マッピングインターフェイスです。デフォルトでは、ルールはすべてのインターフェイスに適用されますが（[すべて（Any）]）、ブリッジ グループのメンバー インターフェイスは例外です。

ステップ 5 元のパケットアドレス（IPv4またはIPv6）を識別します。これは、元のパケットに表示されていた パケット アドレスです。
元のパケットと変換済みパケットの例については、次の図を参照してください。



- [元の発信元アドレス（Original Source Address）]：変換対象のアドレスを保持するネットワーク オブジェクトまたはグループ。
- [元の宛先アドレス（Original Destination Address）]：（オプション）宛先のアドレスを含むネットワーク オブジェクト。空白のままにすると、宛先にかかわらず、送信元アドレスの変換が適用されます。宛先アドレスを指定する場合は、このアドレスにスタティック変換を設定するか、単にアイデンティティ NAT を使用します。

  [インターフェイス（Interface）][送信元インターフェイス IP（Source Interface IP）] を選択すると、元の宛先を送信元インターフェイス（[すべて（Any)] 以外）に基づいて決定できます。このオプションを選択した場合は、変換済み接続先オブジェクトも選択する必要があります。スタティック インターフェイス NAT、および宛先アドレスへのポート変換を実装するには、このオプションを選択し、宛先ポートの適切なポート オブジェクトを選択します。

ステップ 6 変換済みパケットアドレス（IPv4またはIPv6）を識別します。これは、宛先インターフェイスのネットワークで表示されるパケット アドレスです。必要に応じて、IPv4 と IPv6 の間で変換できます。

- [変換済み送信元アドレス（Translated Source Address）]：以下のいずれかを設定します。
  - （インターフェイス PAT）宛先インターフェイスの IPv4 アドレスを使用するには、[インターフェイス（Interface）]を選択します。また、特定の宛先インターフェイスを選択する必要があります。これには、ブリッジ グループのメンバー インターフェイスは使用できません。IPv6 にインターフェイス PAT を使用することはできません。
  - 宛先インターフェイス以外の単一アドレスを使用するには、この用途で作成したホスト ネットワーク オブジェクトを選択します。

- [変換済み宛先アドレス（Translated Destination Address）]：（オプション）変換済みパケットに使用される宛先アドレスを保持するネットワーク オブジェクトまたはグループ。[元の宛先（Original Destination）]にオブジェクトを選択している場合は、同じオブジェクトを選択してアイデンティティ NAT（変換なし）を設定できます。

ステップ 7 （オプション）サービス変換の宛先サービス ポートを識別します（[元の宛先ポート（Original Destination Port）]、[変換済み宛先ポート（Translated Destination Port）]）。
ダイナミック NAT ではポート変換はサポートされません。したがって、[元の送信元ポート（Original Source Port）]および [変換済み送信元ポート（Translated Source Port）]フィールドは空白のままにしておきます。しかし、宛先変換は常にスタティックであるため、宛先ポートに対してポート変換を実行できます。

NAT では、TCP または UDP のみがサポートされますポートを変換する場合、実際のサービス オブジェクトのプロトコルとマッピング サービス オブジェクトのプロトコルの両方を同じにします（両方とも TCP または両方とも UDP）。アイデンティティ NAT では、実際のポートとマッピング ポートの両方に同じサービス オブジェクトを使用できます。

ステップ 8 （オプション）[詳細オプション（Advanced Options）]リンクをクリックし、必要なオプションを選択します。

- [インターフェイス PAT へのフォールスルー（宛先インターフェイス）（Fallthrough to Interface PAT (Destination Interface)）]：相手のマッピング アドレスがすでに割り当て済みの場合、バックアップとして、宛先インターフェイスの IP アドレスを使用するかどうか（インターフェイス PAT フォールバック）。このオプションは、ブリッジ グループのメンバーではない宛先インターフェイスを選択する場合のみに使用できます。すでにインターフェイス PAT を変換済みアドレスとして設定している場合には、このオプションは使用できません。また、IPv6 ネットワークでこのオプションを使用することはできません。

ステップ 9 [OK]をクリックします。

スタティック NAT

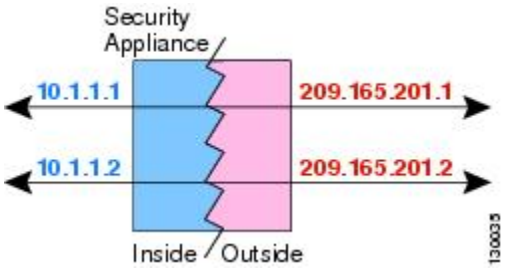
ここでは、スタティック NAT とその実装方法について説明します。

スタティック NAT について

スタティック NAT は、実際のアドレスをマッピング アドレスに固定的に変換します。スタティック NAT を使用する場合、以降のどの接続でもマッピング アドレスが同じであるため、ホスト宛て、またはホストからの双方向接続を開始できます（これを許可するアクセス ルールが存在する場合）。一方、ダイナミック NAT および PAT の場合は、変換の都度、ホストは異なるアドレスまたはポートを使用するため、双方向接続の開始はサポートされません。

次の図は、スタティックNATの一般的なシナリオを示します。変換は常にアクティブなため、実際のホスト、リモート ホストのいずれも接続を開始できます。

図 *6*：スタティック *NAT*



ポート変換を設定したスタティック NAT

ポート変換を設定したスタティックNATでは、実際のプロトコルおよびポートとマッピングされたプロトコルおよびポートを指定できます。

スタティック NAT を使用してポートを指定する場合、ポートまたは IP アドレスを同じ値にマッピングするか、別の値にマッピングするかを選択できます。

次の図に、ポート変換が設定された一般的なスタティック NAT のシナリオを示します。自身にマッピングしたポートと、別の値にマッピングしたポートの両方を示しています。いずれのケースでも、IPアドレスは別の値にマッピングされています。この変換は常にアクティブであるため、変換されたホストとリモート ホストの両方が接続を開始できます。

図 *7*：ポート変換を設定したスタティック *NAT* の一般的なシナリオ

（注） セカンダリ チャネルのアプリケーションインスペクションが必要なアプリケーション（FTP、VoIP など）を使用する場合は、NAT が自動的にセカンダリ ポートを変換します。

次に、ポート変換を設定したスタティック NAT のその他の使用例の一部を示します。

アイデンティティ ポート変換を設定したスタティック NAT

内部リソースへの外部アクセスを簡素化できます。たとえば、異なるポートでサービスを提供する3つの個別のサーバ（FTP、HTTP、SMTPなど）がある場合は、それらのサービスにアクセスするための単一のIPアドレスを外部ユーザに提供できます。その後、アイデンティティ ポート変換を設定したスタティック NAT を設定し、アクセスしようとしているポートに基づいて、単一の外部 IP アドレスを実サーバの正しい IP アドレスにマッピングすることができます。サーバは標準のポート（それぞれ 21、80、および 25）を使用しているため、ポートを変更する必要はありません。

標準以外のポートのポート変換を設定したスタティック NAT

ポート変換を設定したスタティックNATを使用すると、予約済みポートから標準以外のポートへの変換や、その逆の変換も実行できます。たとえば、内部 Web サーバがポート 8080 を使用する場合、ポート 80 に接続することを外部ユーザに許可し、その後、変換を元のポート 8080 に戻すことができます。同様に、セキュリティをさらに高めるには、Web ユーザに標準以外のポート 6785 に接続するように指示し、その後、変換をポート 80 に戻すことができます。

ポート変換を設定したスタティック インターフェイス NAT

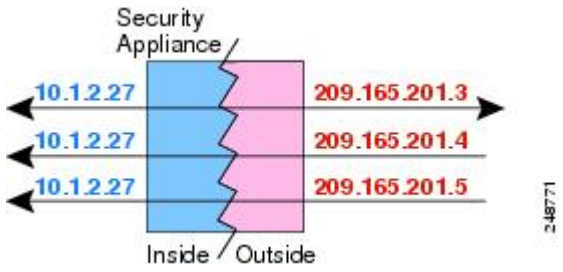
スタティック NAT は、実際のアドレスをインターフェイス アドレスとポートの組み合わせにマッピングするように設定できます。たとえば、デバイスの外部インターフェイスへの Telnet アクセスを内部ホストにリダイレクトする場合、内部ホストの IP アドレス/ポート 23 を外部インターフェイス アドレス/ポート 23 にマッピングできます。

1 対多のスタティック NAT

通常、スタティック NAT は 1 対 1 のマッピングで設定します。しかし場合によっては、1 つの実際のアドレスを複数のマッピング アドレスに設定することがあります（1 対多）。1 対多のスタティックNATを設定する場合、実際のホストがトラフィックを開始すると、常に最初のマッピング アドレスが使用されます。しかし、ホストに向けて開始されたトラフィックの場合、任意のマッピング アドレスへのトラフィックを開始でき、1 つの実際のアドレスには変換されません。

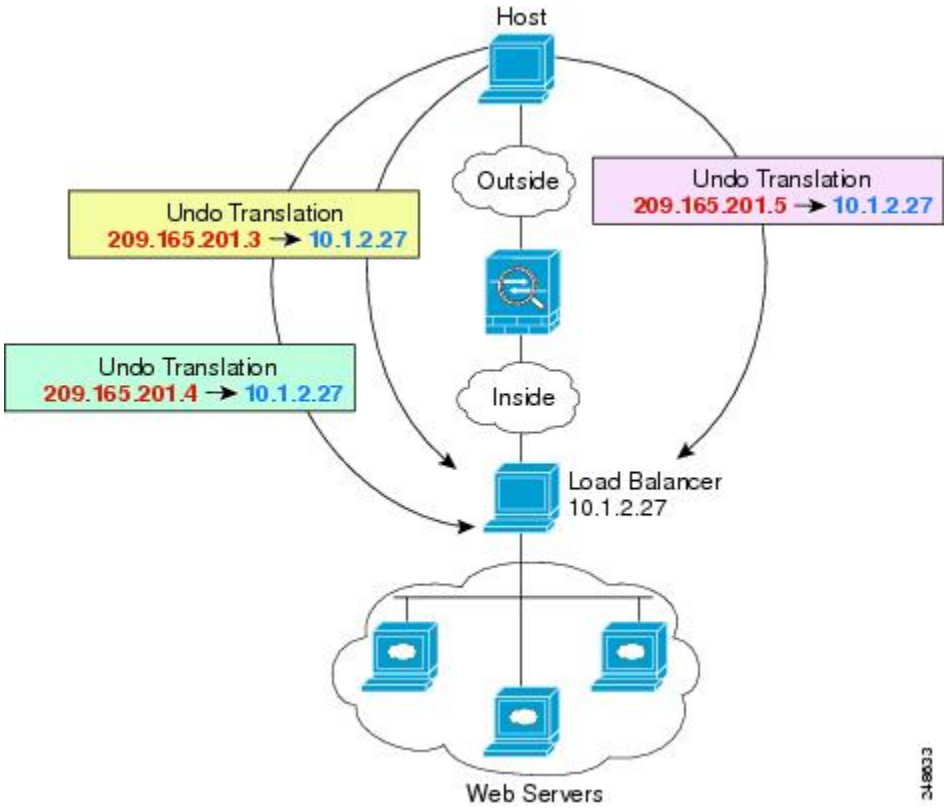
次の図に、一般的な 1 対多のスタティック NAT シナリオを示します。実際のホストが開始すると、常に最初のマッピング アドレスが使用されるため、実際のホスト IP/最初のマッピング IP の変換は、理論的には双方向変換のみが行われます。

図 *8*：*1* 対多のスタティック *NAT*



たとえば、10.1.2.27 にロード バランサが存在するとします。要求される URL に応じて、トラフィックを正しい Web サーバにリダイレクトします。

図 *9*：*1* 対多のスタティック *NAT* の例



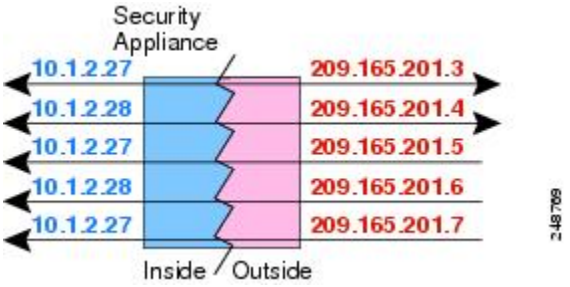
他のマッピング シナリオ（非推奨）

NAT には、1 対 1、1 対多だけではなく、少対多、多対少、多対 1 など任意の種類のスタティック マッピング シナリオを使用できるという柔軟性があります。1 対 1 マッピングまたは 1 対多マッピングだけを使用することをお勧めします。これらの他のマッピング オプションは、予期しない結果が発生する可能性があります。

機能的には、少対多は、1 対多と同じです。しかし、コンフィギュレーションが複雑化して、実際のマッピングが一目では明らかでない場合があるため、必要とする実際の各アドレスに対して 1 対多のコンフィギュレーションを作成することを推奨します。たとえば、少対多のシナリオでは、少数の実際のアドレスが多数のマッピング アドレスに順番にマッピングされます（A は 1、B は 2、C は 3）。すべての実際のアドレスがマッピングされたら、次にマッピングされるアドレスは、最初の実際のアドレスにマッピングされ、すべてのマッピング アドレスがマッピングされるまで続行されます（A は 4、B は 5、C は 6）。この結果、実際の各アドレスに対して複数のマッピング アドレスが存在することになります。1 対多のコンフィギュレーションのように、最初のマッピングだけが双方向であり、以降のマッピングでは、実際のホストへのトラフィックを開始できますが、実際のホストからのすべてのトラフィックは、送信元の最初のマッピング アドレスだけを使用できます。

次の図に、一般的な少対多のスタティック NAT シナリオを示します。

図 *10*：少対多のスタティック *NAT*



多対少または多対 1 コンフィギュレーションでは、マッピング アドレスよりも多くの実際のアドレスが存在します。実際のアドレスが不足するよりも前に、マッピング アドレスが不足します。双方向の開始を実現できるのは、最下位の実際の IP アドレスとマッピングされたプールの間でマッピングを行ったときだけです。残りの上位の実際のアドレスはトラフィックを開始できますが、これらへのトラフィックを開始できません。接続のリターン トラフィックは、接続の固有の 5 つの要素（送信元 IP、宛先 IP、送信元ポート、宛先ポート、プロトコル）によって適切な実際のアドレスに転送されます。

（注） 多対少または多対 1 の NAT は PAT ではありません。2 つの実際のホストが同じ送信元ポート番号を使用して同じ外部サーバおよび同じ TCP 宛先ポートにアクセスする場合は、両方のホストが同じIPアドレスに変換されると、アドレスの競合がある（5つのタプルが一意でない）ため、両方の接続がリセットされます。

次の図に、一般的な多対少のスタティック NAT シナリオを示します。

図 *11*：多対少のスタティック *NAT*

このようにスタティック ルールを使用するのではなく、双方向の開始を必要とするトラフィックに 1 対 1 のルールを作成し、残りのアドレスにダイナミック ルールを作成することをお勧めします。

スタティック自動 NAT の設定

アドレスを宛先ネットワーク上でルーティング可能な異なるIPアドレスに変換するには、スタティック自動 NAT ルールを使用します。また、スタティック NAT ルールを使用してポート変換を実行することもできます。

はじめる前に

[オブジェクト（Objects）]を選択して、ルールで必要なネットワーク オブジェクトまたはグループを作成します。代わりに、NAT ルールを定義する一方で、オブジェクトを作成することもできます。オブジェクトは次の要件を満たす必要があります。

- 元のアドレス（Original Address）：ネットワーク オブジェクト（グループではなく）を指定する必要があります。ホストまたはサブネットを指定できます。
- 変換済みアドレス（Translated Address）：変換済みアドレスを指定するための次のオプションがあります。
  - 宛先インターフェイス（Destination Interface）：宛先インターフェイスの IPv4 アドレスを使用するために、ネットワーク オブジェクトは必要ありません。これはポート変換でのスタティック インターフェイス NAT を設定します。送信元アドレスとポートはインターフェイスのアドレスおよび同じポート番号に変換されます。IPv6の場合、インターフェイス PAT は使用できません。
  - アドレス（Address）：ホストまたはサブネットを含むネットワーク オブジェクトまたはグループを作成します。IPv4 アドレスと IPv6 アドレスの両方をグループに入れることはできません。1つのタイプだけが含まれている必要があります。通常、1対1のマッピングでは、実際のアドレスと同じ数のマッピングアドレスを設定します。しかし、アドレスの数が一致しない場合もあります。

手順

ステップ 1 [ポリシー（Policies）] > [NAT] を選択します。

ステップ 2 次のいずれかを実行します。

- 新しいルールを作成するには、[+]ボタンをクリックします。
- 既存のルールを編集するには、ルールの編集アイコン（  ）をクリックします。

（不要になったルールを削除するには、ルールのごみ箱アイコンをクリックします。）

ステップ 3 基本ルール オプションを設定します。

- タイトル（Title）：ルールの名前を入力します。
- ルールの作成対象（Create Rule For）：[自動 NAT（Auto NAT）] を選択します。

- タイプ（Type）：[スタティック（Static）] を選択します。

ステップ 4 次のパケット変換オプションを設定します。

- 送信元インターフェイス（Source Interface）、宛先インターフェイス（Destination Interface）：（ブリッジ グループのメンバー インターフェイスに必要）この NAT ルールを適用するインターフェイス。送信元は、トラフィックがデバイスに通過する入口となる、実際のインターフェイスです。宛先は、デバイスを通過したトラフィックの出口となる、マッピング インターフェイスです。デフォルトでは、ルールはすべてのインターフェイスに適用されますが（[すべて（Any）]）、ブリッジ グループのメンバー インターフェイスは例外です。
- 元のアドレス（Original Address）：変換するアドレスを含むネットワーク オブジェクト。
- 変換済みアドレス（Translated Address）：次のいずれかを指定します。
  - アドレスの設定グループを使用するには、マッピング アドレスを含むネットワーク オブジェクトまたはグループを選択します。通常、1 対 1 のマッピングでは、実際のアドレスと同じ数のマッピング アドレスを設定します。しかし、アドレスの数が一致しない場合もあります。
  - （ポート変換でのスタティック インターフェイス NAT）宛先インターフェイスのアドレスを使用するには、[インターフェイス（Interface）]を選択します。また、ブリッジ グループ メンバー インターフェイスにすることができない特定の宛先インターフェイスを選択する必要があります。IPv6 の場合はインターフェイス PAT を使用できません。これは、ポート変換でのスタティック インターフェイス NAT を設定します。送信元アドレスとポートはインターフェイスのアドレスおよび同じポート番号に変換されます。
- （オプション）元のポート（Original Port）、変換済みポート（Translated Port）：TCP または UDP ポートを変換する必要がある場合は、元のポートと変換済みポートを定義するポート オブジェクトを選択します。オブジェクトは同じプロトコルに対応している必要があります。オブジェクトが存在しない場合は、[オブジェクトの新規作成（Create New Object）]リンクをクリックします。たとえば、必要に応じて TCP/80 を TCP/8080 に変換できます。

ステップ 5 （オプション）[詳細オプション（Advanced Options）]リンクをクリックし、目的のオプションを選択します。

- このルールに一致する DNS 応答を変換する（Translate DNS replies that match this rule）：DNS 応答内の IP アドレスを変換するかどうか。マッピングされたインターフェイスから実際のインターフェイスへの DNS 応答の場合、Address レコード（IPv4 では A レコード、IPv6 では AAAA 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。反対に、実際のインターフェイスからマッピングされたインターフェイスへの DNS 応答の場合、このレコードは実際の値からマッピングされた値に書き換えられます。このオプションは特定の状況で使用します。また、NAT64/46 変換により、書き換えによって A レコードと AAAA レコードとが交換される場合にも必要となることがあります。詳細については、NAT による DNS クエリおよび応答のリライト，（86 ページ）を参照してください。ポート変換を実行する場合、このオプションは使用できません。

- 宛先インターフェイスでプロキシ ARP を実行しない（Do not proxy ARP on Destination Interface）：マッピング IP アドレスへの着信パケットのプロキシ ARP をディセーブルにします。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を使用した場合、システムはプロキシ ARP を使用してマッピング アドレスのすべての ARP 要求に応答することによって、マッピングアドレスを宛先とするトラフィックを代行受信します。この方法では、デバイス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。必要に応じて、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。

ステップ 6 [OK]をクリックします。

スタティック手動 NAT の設定

自動 NAT ではニーズが満たされない場合は、スタティック手動 NAT ルールを使用します。たとえば、宛先に基づいて異なる変換を実行する場合などです。スタティック NAT は、アドレスを宛先ネットワーク上でルーティング可能な異なるIPアドレスに変換します。また、スタティック NAT ルールを使用してポート変換を実行することもできます。

はじめる前に

[オブジェクト（Objects）]を選択して、ルールで必要なネットワーク オブジェクトまたはグループを作成します。IPv4 アドレスと IPv6 アドレスの両方をグループに入れることはできません。1 つのタイプのみを含める必要があります。代わりに、NAT ルールを定義する一方で、オブジェクトを作成することもできます。オブジェクトは次の要件も満たす必要があります。

- 元の送信元アドレス（Original Source Address）：ネットワーク オブジェクトまたはグループを指定できます。ホストまたはサブネットを含めることができます。すべての元の送信元トラフィックを変換する場合は、この手順をスキップして、ルールで [すべて（Any）]を指定できます。
- 変換済み送信元アドレス（Translated Source Address）：変換済みアドレスを指定するための次のオプションがあります。
  - 宛先インターフェイス（Destination Interface）：宛先インターフェイスの IPv4 アドレスを使用するために、ネットワーク オブジェクトは必要ありません。これはポート変換でのスタティック インターフェイス NAT を設定します。送信元アドレスとポートはインターフェイスのアドレスおよび同じポート番号に変換されます。IPv6 の場合、インターフェイス PAT は使用できません。
  - アドレス（Address）：ホストまたはサブネットを含むネットワーク オブジェクトまたはグループを作成します。IPv4 アドレスと IPv6 アドレスの両方をグループに入れることはできません。1 つのタイプだけが含まれている必要があります。通常、1 対 1 のマッ

ピングでは、実際のアドレスと同じ数のマッピングアドレスを設定します。しかし、アドレスの数が一致しない場合もあります。

ルールで [元の宛先アドレス（Original Destination Address）]および [変換済み宛先アドレス（Translated Destination Address）] のスタティック変換を設定している場合は、それらのアドレスのネットワーク オブジェクトを作成することもできます。ポート変換を設定した宛先のスタティック インターフェイス NAT のみを設定する場合は、宛先のマッピング アドレスに対するオブジェクトの追加をスキップして、ルールでインターフェイスを指定できます。

送信元、宛先または両方のポート変換を実行できます。オブジェクト マネージャで、元のポートと変換済みポートに使用できるポート オブジェクトがあることを確認します。

手順

ステップ 1 [ポリシー（Policies）] > [NAT] を選択します。

ステップ 2 次のいずれかを実行します。

- 新しいルールを作成するには、[+]ボタンをクリックします。
- 既存のルールを編集するには、ルールの編集アイコン（）をクリックします。

（不要になったルールを削除するには、ルールのごみ箱アイコンをクリックします。）

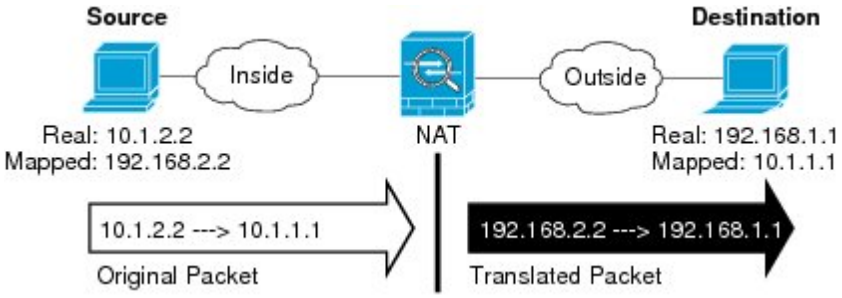
ステップ 3 基本ルール オプションを設定します。

- タイトル（Title）：ルールの名前を入力します。
- ルールの作成対象（Create Rule For）：[手動 NAT（Manual NAT）] を選択します。
- ルールの配置（Rule Placement）：ルールを追加する位置。ルールはカテゴリ内に挿入することも（自動 NAT ルールの前または後）、選択したルールの前または後に挿入することもできます。
- タイプ（Type）：[スタティック（Static）] を選択します。この設定は、送信元アドレスにのみ適用されます。宛先アドレスの変換を定義する場合は、変換は常にスタティックです。

ステップ 4 次のインターフェイス オプションを設定します。

- 送信元インターフェイス（Source Interface）、宛先インターフェイス（Destination Interface）：（ブリッジ グループのメンバー インターフェイスに必要）この NAT ルールを適用するインターフェイス。送信元は、トラフィックがデバイスに通過する入口となる、実際のインターフェイスです。宛先は、デバイスを通過したトラフィックの出口となる、マッピング インターフェイスです。デフォルトでは、ルールはすべてのインターフェイスに適用されますが（[すべて（Any）]）、ブリッジ グループのメンバー インターフェイスは例外です。

ステップ 5 元のパケット アドレス（IPv4 または IPv6）を識別します。これは、元のパケットに表示されていた パケット アドレスです。
元のパケットと変換済みパケットの例については、次の図を参照してください。



- [元の発信元アドレス（Original Source Address）]：変換対象のアドレスを保持するネットワーク オブジェクトまたはグループ。
- [元の宛先アドレス（Original Destination Address）]：（オプション）宛先のアドレスを含むネットワーク オブジェクト。空白のままにすると、宛先にかかわらず、送信元アドレスの変換が適用されます。宛先アドレスを指定する場合は、このアドレスにスタティック変換を設定するか、単にアイデンティティ NAT を使用します。

  [インターフェイス（Interface）][送信元インターフェイス IP（Source Interface IP）] を選択すると、元の宛先を送信元インターフェイス（[すべて（Any)] 以外）に基づいて決定できます。このオプションを選択した場合は、変換済み接続先オブジェクトも選択する必要があります。スタティック インターフェイス NAT、および宛先アドレスへのポート変換を実装するには、このオプションを選択し、宛先ポートの適切なポート オブジェクトを選択します。

ステップ 6 変換済みパケット アドレスが、IPv4 または IPv6 のいずれであるか、つまり、宛先ネットワーク インターフェイス上に現れたときのパケット アドレスを特定します。必要に応じて、IPv4 と IPv6 の間で変換できます。

- 変換済み送信元アドレス（Translated Source Address）：次のいずれかを指定します。
  - アドレスの設定グループを使用するには、マッピング アドレスを含むネットワーク オブジェクトまたはグループを選択します。通常、1 対 1 のマッピングでは、実際のアドレスと同じ数のマッピング アドレスを設定します。しかし、アドレスの数が一致しない場合もあります。
  - （ポート変換でのスタティック インターフェイス NAT）宛先インターフェイスの IPv4 アドレスを使用するには、[インターフェイス（Interface）]を選択します。また、ブリッジ グループ メンバー インターフェイスにすることができない特定の宛先インターフェイスを選択する必要があります。これはポート変換でのスタティック インターフェイス NAT を設定します。送信元アドレスとポートはインターフェイスのアドレスおよび同じポート番号に変換されます。IPv6 の場合、インターフェイス PAT は使用できません。
- 変換済み宛先アドレス（Translated Destination Address）：（任意）変換済みパケットで使用される宛先アドレスを含むネットワーク オブジェクトまたはグループです。[元の宛先（Original Destination）]のオブジェクトを選択した場合は、同じオブジェクトを選択することでアイデンティティ NAT（つまり、変換なし）を設定できます。

ステップ 7 （オプション）サービス変換の送信元サービス ポートまたは宛先サービス ポートを識別します。

ポート変換でのスタティック NAT を設定する場合は、送信元、宛先または両方のポートを変換できます。たとえば、TCP/80 と TCP/8080 の間で変換できます。

NAT では、TCP または UDP のみがサポートされますポートを変換する場合、実際のサービス オブジェクトのプロトコルとマッピング サービス オブジェクトのプロトコルの両方を同じにします（両方とも TCP または両方とも UDP）。アイデンティティ NAT では、実際のポートとマッピング ポートの両方に同じサービス オブジェクトを使用できます。

- 元の送信元ポート（Original Source Port）、変換済み送信元ポート（Translated Source Port）：送信元アドレスのポート変換を定義します。
- 元の宛先ポート（Original Destination Port）、変換済み宛先ポート（Translated Destination Port）：宛先アドレスのポート変換を定義します。

ステップ 8 （オプション）[詳細オプション（Advanced Options）]リンクをクリックし、目的のオプションを選択します。

- このルールに一致する DNS 応答を変換する（Translate DNS replies that match this rule）：DNS 応答内の IP アドレスを変換するかどうか。マッピングされたインターフェイスから実際のインターフェイスへの DNS 応答の場合、Address レコード（IPv4 では A レコード、IPv6 では AAAA 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。反対に、実際のインターフェイスからマッピングされたインターフェイスへの DNS 応答の場合、このレコードは実際の値からマッピングされた値に書き換えられます。このオプションは特定の状況で使用します。また、NAT64/46 変換により、書き換えによって A レコードと AAAA レコードとが交換される場合にも必要となることがあります。詳細については、NAT による DNS クエリおよび応答のリライト，（86 ページ）を参照してください。ポート変換を実行する場合、このオプションは使用できません。
- 宛先インターフェイスでプロキシ ARP を実行しない（Do not proxy ARP on Destination Interface）：マッピング IP アドレスへの着信パケットのプロキシ ARP をディセーブルにします。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を使用した場合、システムはプロキシ ARP を使用してマッピング アドレスのすべての ARP 要求に応答することによって、マッピング アドレスを宛先とするトラフィックを代行受信します。この方法では、デバイス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。必要に応じて、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。

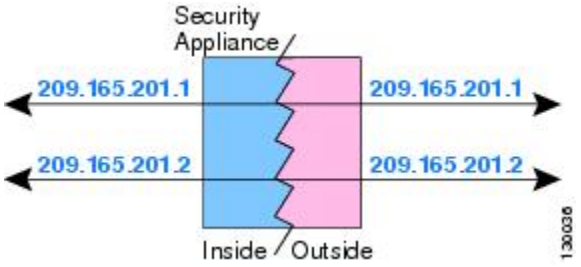
ステップ 9 [OK]をクリックします。

アイデンティティ NAT

IP アドレスをそれ自体に変換する必要がある NAT 設定が存在する場合があります。たとえば、NAT をすべてのネットワークに適用する広範なルールを作成するが、1 つのネットワークを NAT から除外する場合は、アドレスをそれ自体に変換するスタティック NAT ルールを作成できます。

次の図は、典型的なアイデンティティ NAT のシナリオを示しています。

図 *12*：アイデンティティ *NAT*



以降のトピックでは、アイデンティティ NAT の設定方法を説明します。

アイデンティティ自動 NAT の設定

スタティックなアイデンティティ自動NATルールは、アドレスを変換させたくない場合に使用します。つまり、アドレスを自分自身に変換します。

はじめる前に

[オブジェクト（Objects）]を選択し、ルールに必要なネットワーク オブジェクトまたはグループを作成します。または、NAT ルールを定義するときにオブジェクトを作成することもできます。オブジェクトは、以下の要件を満たしている必要があります。

- [元のアドレス（Original Address）]：ネットワーク オブジェクトである必要があります。（グループは不可）。ホストまたはサブネットを含めることができます。
- {変換済みアドレス（Translated Address）]：元の送信元オブジェクトとまったく同じ内容のネットワーク オブジェクトまたはグループ。同じオブジェクトを使用できます。

手順

ステップ 1 [ポリシー（Policies）] > [NAT] を選択します。

ステップ 2 次のいずれかを実行します。

- ルールを新規作成するには、[+]ボタンをクリックします。
- 既存のルールを編集するには、このルールの編集アイコン（）をクリックします

（不要になったルールを削除するには、このルールのごみ箱アイコンをクリック）。

ステップ 3 基本的なルール オプションを設定します。

- [タイトル（Title）]：ルールの名前を入力します。
- [作成するルールの適用対象（Create Rule For）]：[自動 NAT（Auto NAT）] を選択します。
- [タイプ（Type）]：[スタティック（Static）] を選択します。

ステップ 4 以下のパケット変換オプションを設定します。

- [送信元インターフェイス（Source Interface）]、[宛先インターフェイス（Destination Interface）]：（ブリッジ グループのメンバー インターフェイスに必要）この NAT ルールを適用するインターフェイス。送信元は、トラフィックがデバイスに通過する入口となる、実際のインターフェイスです。宛先は、デバイスを通過したトラフィックの出口となる、マッピング インターフェイスです。デフォルトでは、ルールはすべてのインターフェイスに適用されますが（[すべて（Any）]）、ブリッジ グループのメンバー インターフェイスは例外です。
- [元のアドレス（Original Address）]：変換対象のアドレスを保持するネットワーク オブジェクト。
- [変換済みアドレス（Translated Address）]：元の送信元と同じオブジェクト。オプションとして、まったく同じ内容を持つ、別のオブジェクトを選択できます。

アイデンティティ NAT に [元のポート（Original Port）]および [変換済みポート（Translated Port）] オプションは設定しないでください。

ステップ 5 （オプション）[詳細オプション（Advanced Options）]リンクをクリックし、必要なオプションを選択します。

- [このルールと一致する DNS 応答を変換（Translate DNS replies that match this rule）]：アイデンティティ NAT には、このオプションを設定しないでください。
- [宛先インターフェイスで ARP をプロキシしない（Do not proxy ARP on Destination Interface）]：マッピング IP アドレスへの着信パケットのプロキシ ARP をディセーブルにします。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を使用した場合、システムはプロキシ ARP を使用してマッピング アドレスのすべての ARP 要求に応答することによって、マッピング アドレスを宛先とするトラフィックを代行受信します。この方法では、デバイス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。必要に応じて、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。
- [宛先インターフェイスのルート ルックアップの実行（Perform Route Lookup for Destination Interface）]：元の送信元アドレス、変換後の送信元アドレスとに同じオブジェクトを選択する場合に、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選択するとき、このオプションを選択すると、NAT ルールに設定された宛先インターフェイスを使用するのではな

く、ルーティング テーブルに基づく宛先インターフェイスがシステムによって決定されます。

ステップ 6 [OK]をクリックします。

アイデンティティ手動 NAT の設定

自動 NAT では要件を満たせない場合は、スタティックなアイデンティティ手動 NAT ルールを使用します。たとえば、宛先に応じて異なる変換を行いたいような場合です。スタティックなアイデンティティ NAT ルールは、アドレスを変換させたくない場合に使用します。つまり、アドレスを自分自身に変換します。

はじめる前に

[オブジェクト（Objects）]を選択し、ルールに必要なネットワーク オブジェクトまたはグループを作成します。IPv4 アドレスと IPv6 アドレスの両方をグループに入れることはできません。1 つのタイプだけが含まれている必要があります。または、NAT ルールを定義するときにオブジェクトを作成することもできます。オブジェクトは、以下の要件も満たしている必要があります。

- [元の送信元アドレス（Original Source Address）]：ネットワーク オブジェクトまたはグループ。ここには、ホストまたはサブネットを含めることができます。元の送信元トラフィックをすべて変換するには、この手順を省略し、ルールに [すべて（Any）]を指定します。
- [変換済み送信元アドレス（Translated Source Address）]：元の送信元と同じオブジェクト。オプションとして、まったく同じ内容を持つ、別のオブジェクトを選択できます。

宛先アドレスのスタティックな変換をルール内で設定する場合は、[元の宛先アドレス（Original Destination Address）]および[変換済み宛先アドレス（Translated Destination Address）]のネットワーク オブジェクトを作成することもできます。ポート変換のみを使用するスタティックな宛先インターフェイスを設定する場合は、宛先をマッピングしたアドレスに対するオブジェクトの追加を省略して、ルール内でインターフェイスを指定できます。

送信元または宛先、またはその両方に対してポート変換を実行できます。Object Manager で、元のポートと変換済みポートのそれぞれに使用可能なポート オブジェクトがあることを確認します。アイデンティティ NAT には、同一オブジェクトを使用できます。

手順

ステップ 1 [ポリシー（Policies）] > [NAT] を選択します。

ステップ 2 次のいずれかを実行します。

- ルールを新規作成するには、[+] ボタンをクリックします。
- 既存のルールを編集するには、このルールの編集アイコン（）をクリックします

（不要になったルールを削除するには、このルールのごみ箱アイコンをクリック）。

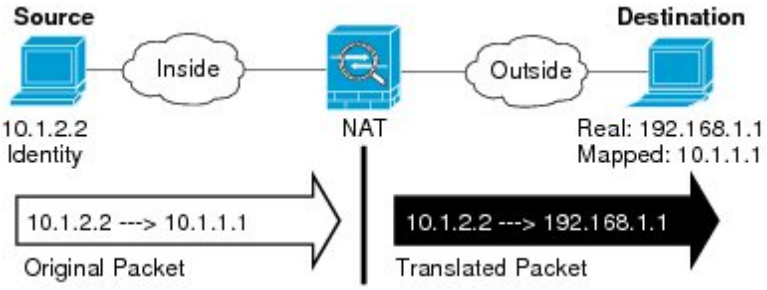
ステップ 3 基本的なルール オプションを設定します。

- [タイトル（Title）]：ルールの名前を入力します。
- [作成するルールの適用対象（Create Rule For）]：[手動 NAT（Manual NAT）] を選択します。
- [ルールの配置（Rule Placement）]：ルールを追加する位置。ルールはカテゴリ内に挿入することも（自動 NAT ルールの前または後）、選択したルールの前または後に挿入することもできます。
- [タイプ（Type）]：[スタティック（Static）]を選択します。この設定は、送信元アドレスのみに適用されます。宛先アドレスに変換を定義する場合は、変換のタイプは常にスタティックとなります。

ステップ 4 以下のインターフェイス オプションを設定します。

- [送信元インターフェイス（Source Interface）]、[宛先インターフェイス（Destination Interface）]：（ブリッジ グループのメンバー インターフェイスに必要）この NAT ルールを適用するインターフェイス。送信元は、トラフィックがデバイスに通過する入口となる、実際のインターフェイスです。宛先は、デバイスを通過したトラフィックの出口となる、マッピングインターフェイスです。デフォルトでは、ルールはすべてのインターフェイスに適用されますが（[すべて（Any）]）、ブリッジ グループのメンバー インターフェイスは例外です。

ステップ 5 元のパケット アドレス（IPv4 または IPv6）を識別します。これは、元のパケットに表示されていた パケット アドレスです。
元のパケットと変換済みパケットの例については、次の図を参照してください。ここでは、内部ホストにはアイデンティティ NAT を実行しますが、外部ホストは変換します。



- [元の発信元アドレス（Original Source Address）]：変換対象のアドレスを保持するネットワーク オブジェクトまたはグループ。
- [元の宛先アドレス（Original Destination Address）]：（オプション）宛先のアドレスを含むネットワーク オブジェクト。空白のままにすると、宛先にかかわらず、送信元アドレスの変換が適用されます。宛先アドレスを指定する場合は、このアドレスにスタティック変換を設定するか、単にアイデンティティ NAT を使用します。

[インターフェイス（Interface）]を選択すると、元の接続先を送信元インターフェイス（[すべて（Any)] 以外）に基づいて決定できます。このオプションを選択した場合は、変換済み接続先オブジェクトも選択する必要があります。スタティック インターフェイス NAT、および宛先アドレスへのポート変換を実装するには、このオプションを選択し、宛先ポートの適切なポート オブジェクトを選択します。

ステップ 6 変換済みパケット アドレス（IPv4 または IPv6）を識別します。これは、宛先インターフェイスのネットワークで表示されるパケット アドレスです。必要に応じて、IPv4 と IPv6 の間で変換できます。

- [変換済み送信元アドレス（Translated Source Address）]：元の送信元と同じオブジェクト。オプションとして、まったく同じ内容を持つ、別のオブジェクトを選択できます。
- [変換済み宛先アドレス（Translated Destination Address）]：（オプション）変換済みパケットに使用される宛先アドレスを保持するネットワーク オブジェクトまたはグループ。[元の宛先アドレス（Original Destination Address）]にオブジェクトを選択している場合は、同じオブジェクトを選択してアイデンティティ NAT（変換なし）を設定できます。

ステップ 7 （オプション）サービス変換の送信元サービス ポートまたは宛先サービス ポートを識別します。ポート変換を行うスタティック NAT を設定する場合は、送信元または宛先、またはその両方のポートを変換できます。たとえば、TCP/80 と TCP/8080 間で変換できます。

NAT では、TCP または UDP のみがサポートされますポートを変換する場合、実際のサービス オブジェクトのプロトコルとマッピング サービス オブジェクトのプロトコルの両方を同じにします（両方とも TCP または両方とも UDP）。アイデンティティ NAT では、実際のポートとマッピング ポートの両方に同じサービス オブジェクトを使用できます。

- [元の送信元ポート（Original Source Port）、[変換済み送信元ポート（Translated Source Port）]：送信元アドレスのポート変換を定義します。
- [元の宛先ポート（Original Destination Port）]、[変換済み宛先ポート（Translated Destination Port）]：宛先アドレスのポート変換を定義します。

ステップ 8 （オプション）[詳細オプション（Advanced Options）]リンクをクリックし、必要なオプションを選択します。

- [このルールと一致する DNS 応答を変換（Translate DNS replies that match this rule）]：アイデンティティ NAT には、このオプションを設定しないでください。
- [宛先インターフェイスで ARP をプロキシしない（Do not proxy ARP on Destination Interface）]：マッピング IP アドレスへの着信パケットのプロキシ ARP をディセーブルにします。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を使用した場合、システムはプロキシ ARP を使用してマッピング アドレスのすべての ARP 要求に応答することによって、マッピング アドレスを宛先とするトラフィックを代行受信します。この方法では、デバイス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。必要に応じて、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。

- [宛先インターフェイスのルート ルックアップの実行（Perform Route Lookup for Destination Interface）]：元の送信元アドレス、変換後の送信元アドレスとに同じオブジェクトを選択する場合に、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選択するとき、このオプションを選択すると、NAT ルールに設定された宛先インターフェイスを使用するのではなく、ルーティング テーブルに基づく宛先インターフェイスがシステムによって決定されます。

ステップ 9 [OK]をクリックします。

Firepower Threat Defense の NAT ルールのプロパティ

ネットワーク アドレス変換（NAT）のルールを使用して、IP アドレスを別の IP アドレスに変換します。通常は、NAT ルールを使用して、プライベート アドレスをパブリックにルーティング可能なアドレスに変換します。変換は 1 つのアドレスから別のアドレスに行うことができ、ポート アドレス変換（PAT）を使用して、複数のアドレスを 1 つのアドレスに変換することもできます。送信元アドレス間で区別するためにはポート番号を使用します。

NAT ルールには、次の基本プロパティが含まれます。別途示されている場合を除き、自動 NAT ルールと手動 NAT ルールのプロパティは同じです。

[役職（Title）]

ルールの名前を入力します。名前にスペースを含めることはできません。

[ルールの作成対象（Create Rule For）]

変換ルールが [自動 NAT（Auto NAT）] か、[手動 NAT（Manual NAT）]であるかを指定します。自動 NAT は手動 NAT よりシンプルですが、手動 NAT では、宛先アドレスに基づいて送信元アドレス用に異なる変換を作成することができます。

[ステータス（Status）]

ルールをアクティブするか、無効にするかを指定します。

[配置（Placement）]（手動 NAT のみ）

ルールを追加する位置。ルールはカテゴリ内に挿入することも（自動 NAT ルールの前または後）、選択したルールの前または後に挿入することもできます。

[タイプ（Type）]

変換ルールが [ダイナミック（Dynamic）]か、[スタティック（Static）]であるかを指定します。ダイナミック変換では、アドレスのプールからマッピング アドレス、またはアドレスとポートの組み合わせ（PAT を実装している場合）が自動的に選択されます。マッピング アドレスとポートを正確に定義したい場合は、スタティック変換を使用します。

次のトピックでは、NAT ルールの残りのプロパティについて説明します。

自動 NAT のパケット変換プロパティ

送信元アドレスと変換されたマッピング アドレスを定義するには、[パケット変換（Packet Translation）]オプションを使用します。次のプロパティは、自動 NAT にのみ適用されます。

[送信元インターフェイス（Source Interface）]、[宛先インターフェイス（Destination Interface）]

（ブリッジ グループのメンバー インターフェイスに必要）この NAT ルールを適用するインターフェイス。送信元は、トラフィックがデバイスに通過する入口となる、実際のインターフェイスです。宛先は、デバイスを通過したトラフィックの出口となる、マッピング インターフェイスです。デフォルトでは、ルールはすべてのインターフェイスに適用されますが（[すべて（Any）]）、ブリッジ グループのメンバー インターフェイスは例外です。

[元のアドレス（Original Address）]（常に必須）

変換している送信元アドレスを含むネットワーク オブジェクト。これは（グループではなく）ネットワーク オブジェクトである必要があり、ホストまたはサブネットを指定できます。

[変換済みアドレス（Translated Address）]（通常は必須）

変換先のマッピング アドレス。ここで選択する内容は、定義している変換ルールのタイプによって異なります。

- [ダイナミック NAT（Dynamic NAT）]：マッピング アドレスを含むネットワーク オブジェクトまたはグループ。ネットワーク オブジェクトまたはグループを指定できますが、サブネットを含めることはできません。IPv4 アドレスと IPv6 アドレスの両方をグループに入れることはできません。1 つのタイプだけが含まれている必要があります。
- [ダイナミック PAT（Dynamic PAT）]：次のいずれかを実行します。
  - （インターフェイス PAT）。宛先インターフェイスの IPv4 アドレスを使用するには、[インターフェイス（Interface）]を選択します。特定の宛先インターフェイスも選択する必要があります。ブリッジ グループ メンバー インターフェイスは選択できません。インターフェイス PAT は IPv6 には使用できません。
  - 宛先インターフェイス以外の単一アドレスを使用するには、この用途で作成したホスト ネットワーク オブジェクトを選択します。
- [スタティック NAT（Static NAT）]：次のいずれかを実行します。
  - 一連のアドレスのグループを使用するには、マッピング アドレスを含むネットワーク オブジェクトまたはグループを選択します。オブジェクトまたはグループには、ホストやサブネットを含めることができます。通常、1 対 1 のマッピングでは、実際のアドレスと同じ数のマッピング アドレスを設定します。しかし、アドレスの数が一致しない場合もあります。
  - （ポート変換を設定したスタティック インターフェイス NAT）。宛先インターフェイスのアドレスを使用するには、[インターフェイス（Interface）]を選択します。特定の宛先インターフェイスも選択する必要があります。ブリッジ グループ メンバー インターフェイスは選択できません。これで、ポート変換を設定したスタティック インターフェイス NAT が設定されます。送信元アドレスとポートは、インターフェイスのアドレスおよび同じポート番号に変換されます。インターフェイス PAT は IPv6 には使用できません。
- [アイデンティティ NAT（Identity NAT）]：元の送信元と同じオブジェクト。オプションとして、まったく同じ内容を持つ、別のオブジェクトを選択できます。

[元のポート（Original Port）]、[変換済みポート（Translated Port）]（スタティック NAT のみ）

TCP または UDP ポートを変換する必要がある場合は、元のポートと変換済みポートを定義するポート オブジェクトを選択します。オブジェクトは同じプロトコルのものである必要があります。たとえば、必要に応じて、TCP/80 を TCP/8080 に変換できます。

手動 NAT のパケット変換プロパティ

送信元アドレスと変換されたマッピング アドレスを定義するには、[パケット変換（Packet Translation）]オプションを使用します。次のプロパティは、手動 NAT にのみ適用されます。指定されている場合を除き、すべて任意選択です。

[送信元インターフェイス（Source Interface）]、[宛先インターフェイス（Destination Interface）]

（ブリッジ グループのメンバー インターフェイスに必要）この NAT ルールを適用するインターフェイス。送信元は、トラフィックがデバイスに通過する入口となる、実際のインターフェイスです。宛先は、デバイスを通過したトラフィックの出口となる、マッピング インターフェイスです。デフォルトでは、ルールはすべてのインターフェイスに適用されますが（[すべて（Any）]）、ブリッジ グループのメンバー インターフェイスは例外です。

[元の送信元アドレス（Original Source Address）]（常に必須）

変換しているアドレスを含むネットワーク オブジェクトまたはグループ。これは、ネットワーク オブジェクトまたはグループを指定でき、ホストまたはサブネットを含めることができます。元の送信元トラフィックをすべて変換する場合は、ルールで [すべて（Any）]を指定できます。

[変換済み送信元アドレス（Translated Source Address）]（通常は必須）

変換先のマッピング アドレス。ここで選択する内容は、定義している変換ルールのタイプによって異なります。

- [ダイナミック NAT（Dynamic NAT）]：マッピング アドレスを含むネットワーク オブジェクトまたはグループ。ネットワーク オブジェクトまたはグループを指定できますが、サブネットを含めることはできません。IPv4 アドレスと IPv6 アドレスの両方をグループに入れることはできません。1 つのタイプだけが含まれている必要があります。
- [ダイナミック PAT（Dynamic PAT）]：次のいずれかを実行します。
  - （インターフェイス PAT）。宛先インターフェイスのアドレスを使用するには、[インターフェイス（Interface）]を選択します。特定の宛先インターフェイスも選択する必要があります。ブリッジ グループ メンバー インターフェイスは選択できません。インターフェイス PAT は IPv6 には使用できません。
  - 宛先インターフェイス以外の単一アドレスを使用するには、この用途で作成したホスト ネットワーク オブジェクトを選択します。
- [スタティック NAT（Static NAT）]：次のいずれかを実行します。
  - 一連のアドレスのグループを使用するには、マッピング アドレスを含むネットワーク オブジェクトまたはグループを選択します。通常、1 対 1 のマッピングでは、実際のアドレスと同じ数のマッピング アドレスを設定します。しかし、アドレスの数が一致しない場合もあります。
  - （ポート変換を設定したスタティック インターフェイス NAT）。宛先インターフェイスのアドレスを使用するには、[インターフェイス（Interface）]を選択します。特定の宛先インターフェイスも選択する必要があります。ブリッジ グループ メンバー インターフェイスは選択できません。これで、ポート変換を設定したスタティック インターフェイス NAT が設定されます。送信元アドレスとポートは、インターフェイスのアドレスおよび同じポート番号に変換されます。インターフェイス PAT は IPv6 には使用できません。
- [アイデンティティ NAT（Identity NAT）]：元の送信元と同じオブジェクト。オプションとして、まったく同じ内容を持つ、別のオブジェクトを選択できます。

[元の宛先アドレス（Original Destination Address）]

宛先のアドレスを含むネットワーク オブジェクト。空白のままにすると、宛先にかかわらず、送信元アドレスの変換が適用されます。宛先アドレスを指定する場合は、このアドレスにスタティック変換を設定するか、単にアイデンティティ NAT を使用します。

[インターフェイス（Interface）]を選択すると、元の接続先を送信元インターフェイス（[すべて（Any）] 以外）に基づいて決定できます。このオプションを選択した場合は、変換済み接続先オブジェクトも選択する必要があります。スタティック インターフェイス NAT、および宛先アドレスへのポート変換を実装するには、このオプションを選択し、宛先ポートの適切なポート オブジェクトを選択します。

[変換済み宛先アドレス（Translated Destination Address）]

変換済みパケットで使用される宛先アドレスを含むネットワーク オブジェクトまたはグループ。[元の宛先（Original Destination）]のオブジェクトを選択した場合、同じオブジェクトを選択してアイデンティティ NAT を設定できます（つまり、変換は不要です）。

[元の送信元ポート（Original Source Port）]、[変換済み送信元ポート（Translated Source Port）]、[元の宛先ポート（Original Destination Port）]、[変換済み宛先ポート（Translated Destination Port）]

元のパケットと変換済みパケットの送信元と宛先のサービスを定義するポート オブジェクト。ポートを変換するか、または同じオブジェクトを選択して、ポートを変換せずにルールをサービスに依存させることができます。サービスを設定するときは、次の点に注意してください。

- （ダイナミック NAT または PAT）。[元の送信元ポート（Original Source Port）]と [変換済み送信元ポート（Translated Source Port）]で変換を実行することはできません。宛先ポートでのみ変換を実行できます。
- NAT では、TCP または UDP のみがサポートされますポートを変換する場合、実際のサービス オブジェクトのプロトコルとマッピング サービス オブジェクトのプロトコルの両方を同じにします（両方とも TCP または両方とも UDP）。アイデンティティ NAT では、実際のポートとマッピング ポートの両方に同じオブジェクトを使用できます。

高度な NAT のプロパティ

NAT を設定する際、[詳細（Advanced）] オプションを使用すると、特殊なサービスを実現する各種プロパティを設定できます。これらのプロパティはすべてオプションであり、該当サービスが必要な場合だけに設定します。

[このルールに一致する DNS 応答を変換（Translate DNS replies that match this rule）]

DNS 応答内の IP アドレスを変換するかどうか。マッピングされたインターフェイスから実際のインターフェイスへの DNS 応答の場合、Address レコード（IPv4 では A レコード、IPv6 では AAAA 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。反対に、実際のインターフェイスからマッピングされたインターフェイスへの DNS 応答の場合、このレコードは実際の値からマッピングされた値に書き換えられます。このオプションは特定の状況で使用します。また、NAT64/46 変換により、書き換えによって A レコードと AAAA レコードとが交換される場合にも必要となることがあります。詳細については、NAT による DNS クエリおよび応答のリライト，（86 ページ）を参照してください。スタティック NAT ルールでポート変換を行っている場合には、このオプションは使用できません。

[インターフェイス PAT へのフォールスルー（宛先インターフェイス）（Fallthrough to Interface PAT (Destination Interface)）]（**ダイナミック NAT のみ**）

相手のマッピング アドレスがすでに割り当て済みの場合、バックアップとして、宛先インターフェイスのIPアドレスを使用するかどうか（インターフェイスPATフォールバック）。このオプションは、ブリッジ グループのメンバーではない宛先インターフェイスを選択する場合のみに使用できます。すでにインターフェイス PAT を変換済みアドレスとして設定している場合には、このオプションは使用できません。このオプションは、IPv6ネットワークでは使用できません。

[宛先インターフェイスでARPをプロキシしない（Do not proxy ARP on Destination Interface）]（スタティック NAT のみ）

マッピングIPアドレスへの着信パケットのプロキシARPをディセーブルにします。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を使用した場合、システムはプロキシ ARP を使用してマッピング アドレスのすべての ARP 要求に応答することによって、マッピング アドレスを宛先とするトラフィックを代行受信します。この方法では、デバイス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。必要に応じて、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。

宛先インターフェイスに対し、ルートルックアップを実行します（スタティックなアイデンティティ NAT のみ、ルーテッド モードのみ）。

元の送信元アドレス、変換後の送信元アドレスとに同じオブジェクトを選択する場合に、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選択するとき、このオプションを選択すると、NAT ルールに設定された宛先インターフェイスを使用するのではなく、ルーティング テーブルに基づく宛先インターフェイスがシステムによって決定されます。

IPv6 ネットワークの変換

IPv6 のみ、および IPv4 のみのネットワーク間でトラフィックを渡す必要がある場合、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 ネットワークであっても、外部ネットワークから内部アドレスを隠したい場合もあります。

IPv6 ネットワークでは次の変換タイプを使用できます。

- NAT64、NAT46：IPv6 パケットを IPv4 パケットに（またはその逆に）変換します。2 つのポリシーを定義する必要があります。1 つは IPv6 から IPv4 への変換用、もう 1 つは IPv4 から IPv6 への変換用です。DNS サーバが外部ネットワーク上にあり、DNS 応答を書き換える必要がある場合、1 つの 手動 NAT ルールで同じことを実現できます。宛先を指定している場合、手動 NAT ルールでは DNS の書き換えを有効にできないため、2 つの自動 NAT ルールを作成することを推奨します。

（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 の使用を推奨します。ダイナミック NAT または PAT を使用できますが、IPv6 アドレスは大量にあるため、ダイナミック NAT を使用する必要がありません。

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

NAT64/46：IPv6 アドレスから IPv4 への変換

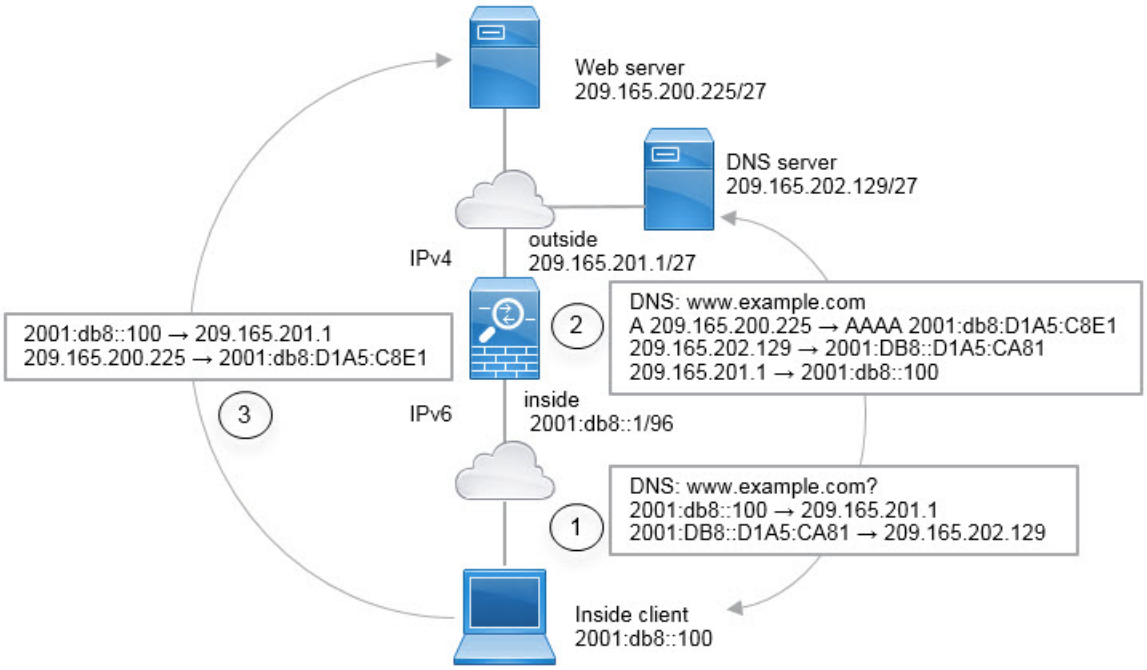
トラフィックが IPv6 ネットワークから IPv4 専用ネットワークに移動する場合、IPv6 アドレスを IPv4 アドレスに変換して、IPv4 から IPv6 にトラフィックを戻す必要があります。2 つのアドレス プール（IPv4 ネットワークに IPv6 アドレスをバインドする IPv4 アドレス プールと、IPv6 ネットワークに IPv4 アドレスをバインドする IPv6 アドレス プール）を定義する必要があります。

- NAT64 ルールの IPv4 アドレス プールは一般的に小さく、通常、IPv6 クライアント アドレスと 1 対 1 でマッピングするだけの十分なアドレスが含まれていません。ダイナミック PAT は、ダイナミックまたはスタティック NAT と比較すると、想定される大量の IPv6 クライアント アドレスをより簡単に満たすことができます。
- NAT46 ルールの IPv6 アドレス プールは、マッピングする IPv4 アドレスの数以上のサイズにできます。そのため、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 マッピングのみサポートしているため、ダイナミック PAT は使用できません。

2 つのポリシー（1 つは送信元 IPv6 ネットワーク用、もう 1 つは宛先 IPv4 ネットワーク用）を定義する必要があります。DNS サーバが外部ネットワーク上にあり、DNS 応答を書き換える必要がある場合、1 つの 手動 NAT ルールで同じことを実現できます。宛先を指定している場合、手動 NAT ルールでは DNS の書き換えを有効にできないため、2 つの自動 NAT ルールを作成することを推奨します。

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

以下に、IPv6 専用の内部ネットワークを使用しているにもかかわらず内部ユーザが外部インターネット上のいくつかの IPv4 専用サービスを必要とする一般的な例を示します。



この例では、ダイナミック インターフェイス PAT と外部インターフェイスの IP アドレスを使用して、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 ネットワーク上のアドレスにスタティックに変換され、内部ネットワークでの送信が可能になります。外部 DNS サーバからの応答を A（IPv4）レコードから AAAA（IPv6）レコードに変換し、アドレスを IPv4 から IPv6 に変換できるように、NAT46 ルールで DNS リライトを有効にします。

以下に、内部 IPv6 ネットワーク上の 2001:DB8::100 のクライアントが www.example.com を開こうとする Web 要求の一般的なシーケンスを示します。

1. クライアントのコンピュータが、2001:DB8::D1A5:CA81 の DNS サーバに DNS 要求を送信します。NAT ルールにより、DNS 要求の送信元と宛先に対して次の変換が実行されます。
   - 2001:DB8::100 から 209.165.201.1 上の一意のポート（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 209.165.202.129 の IPv6 の相当物）
2. DNS サーバは、www.example.com が 209.165.200.225 にあることを示す A レコードで応答します。NAT46 ルールは、DNS リライトが有効になっている場合、A レコードを IPv6 の相当物の 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 この時点で、IPv6 クライアントは Web サーバの IP アドレスを取得しており、2001:db8:D1A5:C8E1 の www.example.com に HTTP 要求を送信します（D1A5:C8E1 は 209.165.200.225 の IPv6 の相当物）。HTTP 要求の送信元と宛先が変換されます。

- 2001:DB8::100 から 209.156.101.54 上の一意のポート（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）

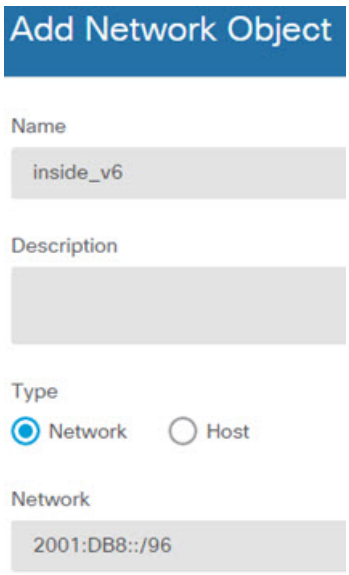
次の手順では、この例を設定する方法について説明します。

（注） この例は、内部インターフェイスがブリッジ グループ インターフェイス（BVI）ではなく標準ルーテッドインターフェイスであることを前提としています。内部インターフェイスが BVI の場合は、各メンバー インターフェイスにルールを複製する必要があります。

手順

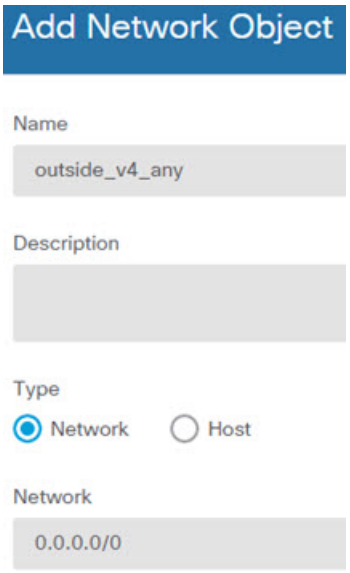
ステップ 1 内部 IPv6 ネットワークと外部 IPv4 ネットワークを定義するネットワーク オブジェクトを作成します。

a) [オブジェクト（Objects）] を選択します。
b) コンテンツ テーブルから [ネットワーク（Network）] を選択し、[+] をクリックします。
c) 内部 IPv6 ネットワークを定義します。
ネットワーク オブジェクトに名前を付け（inside_v6 など）、[ネットワーク（Network）] を選択して、ネットワーク アドレスとして 2001:db8::/96 を入力します。



d) [OK] をクリックします。

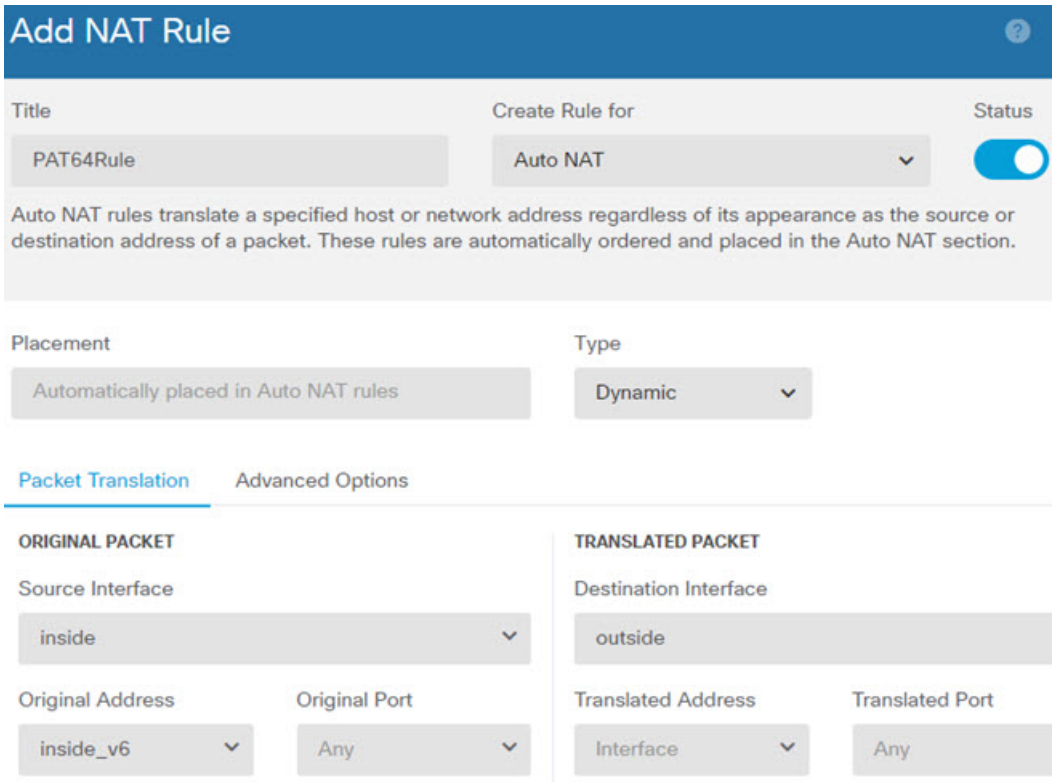
e) [+]をクリックし、外部 IPv4 ネットワークを定義します。
ネットワーク オブジェクトに名前を付け（outside_v4_any など）、[ネットワーク（Network）] を選択して、ネットワーク アドレスとして 0.0.0.0/0 を入力します。



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) [ポリシー（Policies）] > [NAT] を選択します。
b) [+]ボタンをクリックします。
c) 次のプロパティを設定します。

- [タイトル（Title）] = PAT64Rule（または任意の別の名前）。
- [ルール作成目的（Create Rule For）] = Auto NAT。
- [タイプ（Type）] = Dynamic。
- [送信元インターフェイス（Source Interface）] = inside。
- [宛先インターフェイス（Destination Interface）] = outside。
- [元のアドレス（Original Address）] = inside_v6 ネットワーク オブジェクト。
- [変換されたアドレス（Translated Address）] = Interface。このオプションは、宛先インターフェイスの IPv4 アドレスを PAT アドレスとして使用します。



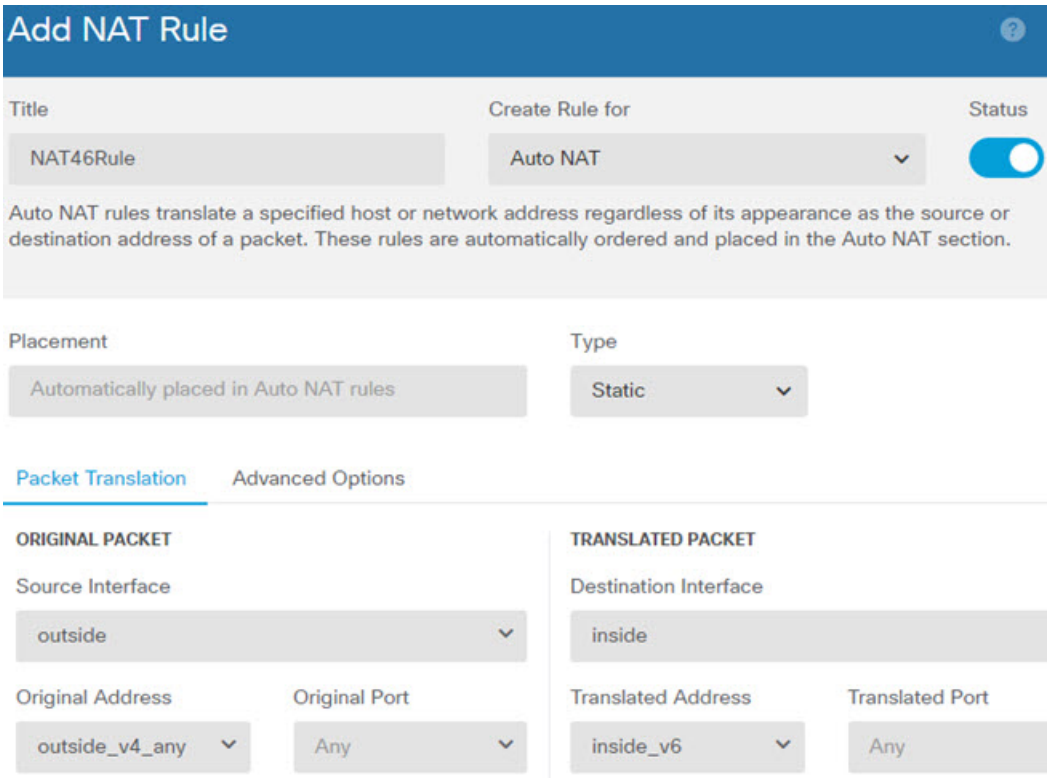
d) [OK]をクリックします。
このルールにより、内部インターフェイス上の 2001:db8::/96 サブネットから外部インターフェイスに向かうすべてのトラフィックが、外部インターフェイスの IPv4 アドレスを使用して NAT64 PAT 変換を取得します。

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) [+]ボタンをクリックします。

b) 次のプロパティを設定します。

- [タイトル（Title）] = NAT46Rule（または任意の別の名前）。
- [ルール作成目的（Create Rule For）]= Auto NAT。
- [タイプ（Type）] = Static。
- [送信元インターフェイス（Source Interface）] = outside。
- [宛先インターフェイス（Destination Interface）] = inside。
- [元のアドレス（Original Address）] = outside_v4_any ネットワーク オブジェクト。
- [変換されたアドレス（Translated Address）] = inside_v6 ネットワーク オブジェクト。
- [詳細オプション（Advanced Options）] タブで、[このルールと一致する DNS 応答を変換する（Translate DNS replies that match this rule）] をオンにします。



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

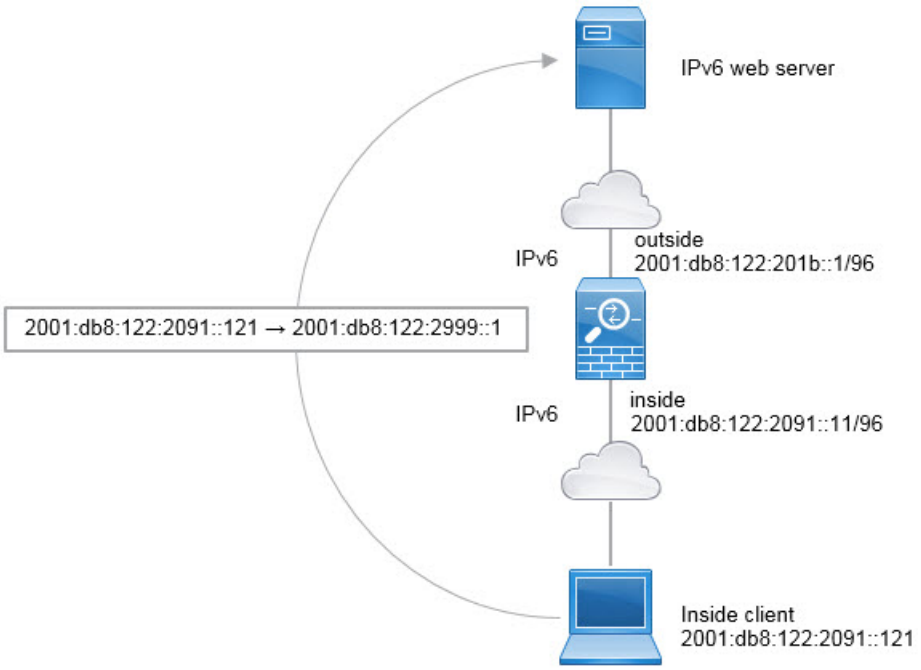
NAT66：IPv6 アドレスを別の IPv6 アドレスに変換

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

異なるアドレス タイプ間で変換しているわけではないため、NAT66 変換用の単一のルールが必要です。これらのルールは、自動 NAT を使用して簡単にモデリングできます。ただし、リターン トラフィックを許可しない場合は、手動 NAT のみを使用して、スタティック NAT ルールを単方向にすることができます。

NAT66 の例：ネットワーク間のスタティック変換

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

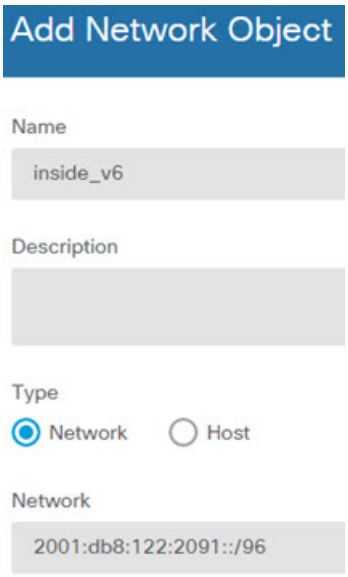


（注） この例は、内部インターフェイスがブリッジ グループ インターフェイス（BVI）ではなく標準ルーテッドインターフェイスであることを前提としています。内部インターフェイスがBVIの場合は、各メンバー インターフェイスにルールを複製する必要があります。

手順

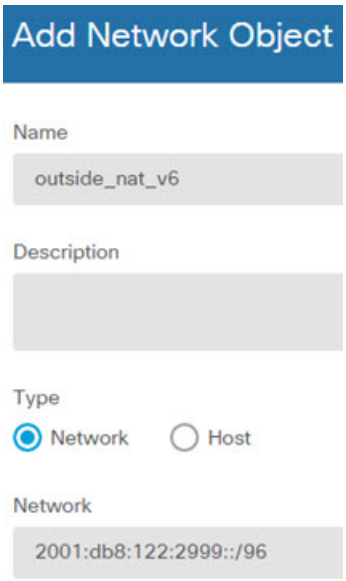
ステップ 1 内部 IPv6 ネットワークと外部 IPv6 NAT ネットワークを定義するネットワーク オブジェクトを作成します。

a) [オブジェクト（Objects）] を選択します。
b) コンテンツ テーブルから [ネットワーク（Network）] を選択し、[+] をクリックします。
c) 内部 IPv6 ネットワークを定義します。
ネットワーク オブジェクトに名前を付け（inside_v6 など）、[ネットワーク（Network）] を選択して、ネットワーク アドレスとして 2001:db8:122:2091::/96 を入力します。



d) [追加（Add）][OK] をクリックします。

e) [+]をクリックし、外部 IPv6 NAT ネットワークを定義します。
ネットワーク オブジェクトに名前を付け（outside_nat_v6 など）、[ネットワーク（Network）] を選択して、ネットワーク アドレスとして 2001:db8:122:2999::/96 を入力します。



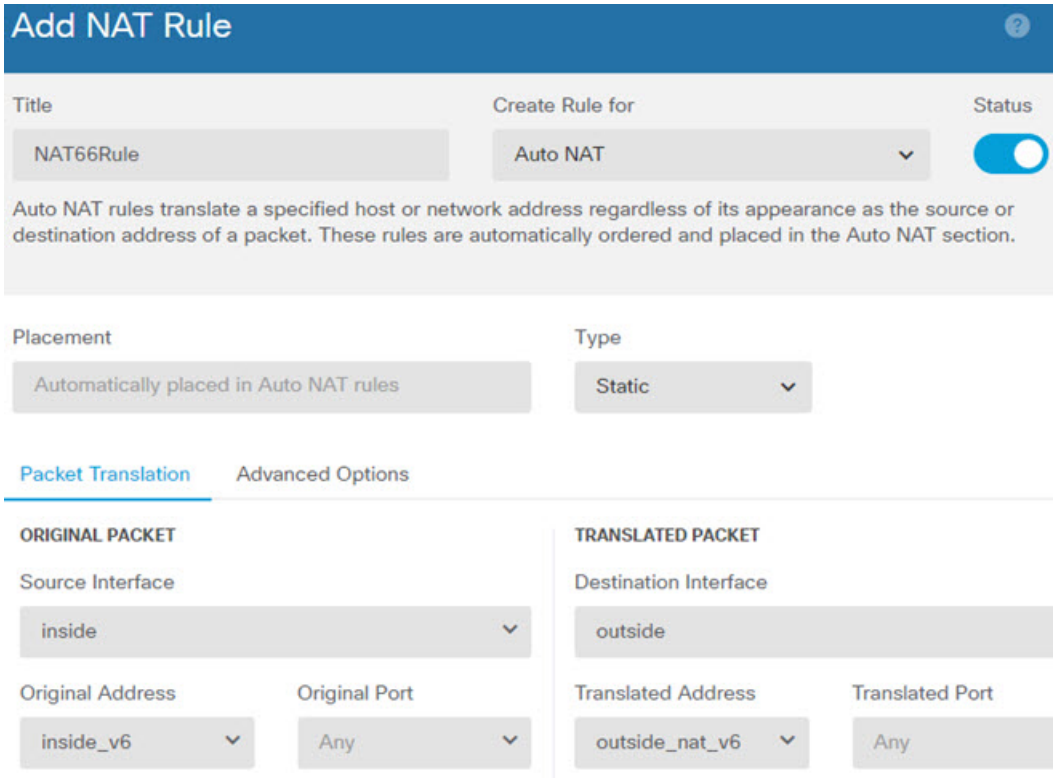
ステップ 2 内部 IPv6 ネットワークのスタティック NAT ルールを設定します。

a) [ポリシー（Policies）] > [NAT] を選択します。

b) [+]ボタンをクリックします。

c) 次のプロパティを設定します。

- [タイトル（Title）] = NAT66Rule（または任意の別の名前）。
- [ルール作成目的（Create Rule For）]= Auto NAT。
- [タイプ（Type）] = Static。
- [送信元インターフェイス（Source Interface）] = inside。
- [宛先インターフェイス（Destination Interface）] = outside。
- [元のアドレス（Original Address）] = inside_v6 ネットワーク オブジェクト。
- [変換されたアドレス（Translated Address）] = outside_nat_v6 ネットワーク オブジェクト。

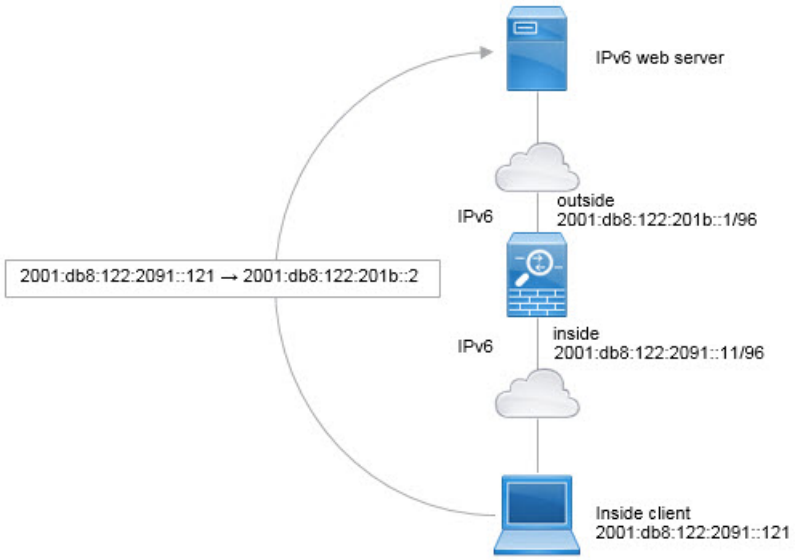


d) [OK]をクリックします。
このルールにより、内部インターフェイス上の 2001:db8:122:2091::/96 サブネットから外部インターフェイスに向かうすべてのトラフィックが、2001:db8:122:2999::/96 ネットワーク上のアドレスへのスタティック NAT66 変換を取得します。

NAT66 の例：簡単な 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 アドレスの異なるポートに内部アドレスをダイナミックに割り当てることです。

ただし、Firepower Device Manager によりインターフェイスの IPv6 アドレスを使用してインターフェイス PAT を設定することはできません。代わりに、ダイナミック PAT プールと同じネットワーク上の 1 つの空きアドレスを使用します。

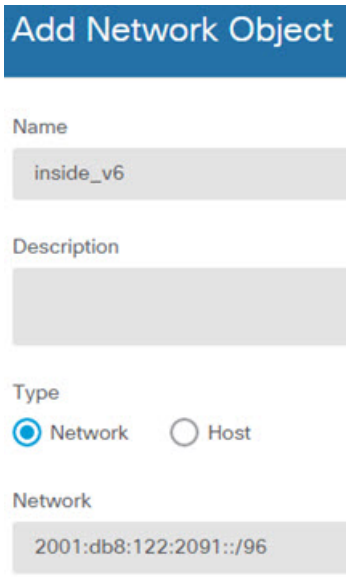


（注） この例は、内部インターフェイスがブリッジ グループ インターフェイス（BVI）ではなく標準ルーテッドインターフェイスであることを前提としています。内部インターフェイスが BVI の場合は、各メンバー インターフェイスにルールを複製する必要があります。

手順

ステップ 1 内部 IPv6 ネットワークと IPv6 PAT ネットワークを定義するネットワーク オブジェクトを作成します。

a) [オブジェクト（Objects）] を選択します。
b) コンテンツ テーブルから [ネットワーク（Network）] を選択し、[+] をクリックします。
c) 内部 IPv6 ネットワークを定義します。
ネットワーク オブジェクトに名前を付け（inside_v6 など）、[ネットワーク（Network）] を選択して、ネットワーク アドレスとして 2001:db8:122:2091::/96 を入力します。



d) [OK] をクリックします。

e) [+]をクリックし、外部 IPv6 PAT アドレスを定義します。
ネットワーク オブジェクトに名前を付け（ipv6_pat など）、[ホスト（Host）] を選択して、ホスト アドレスとして 2001:db8:122:201b::2 を入力します。

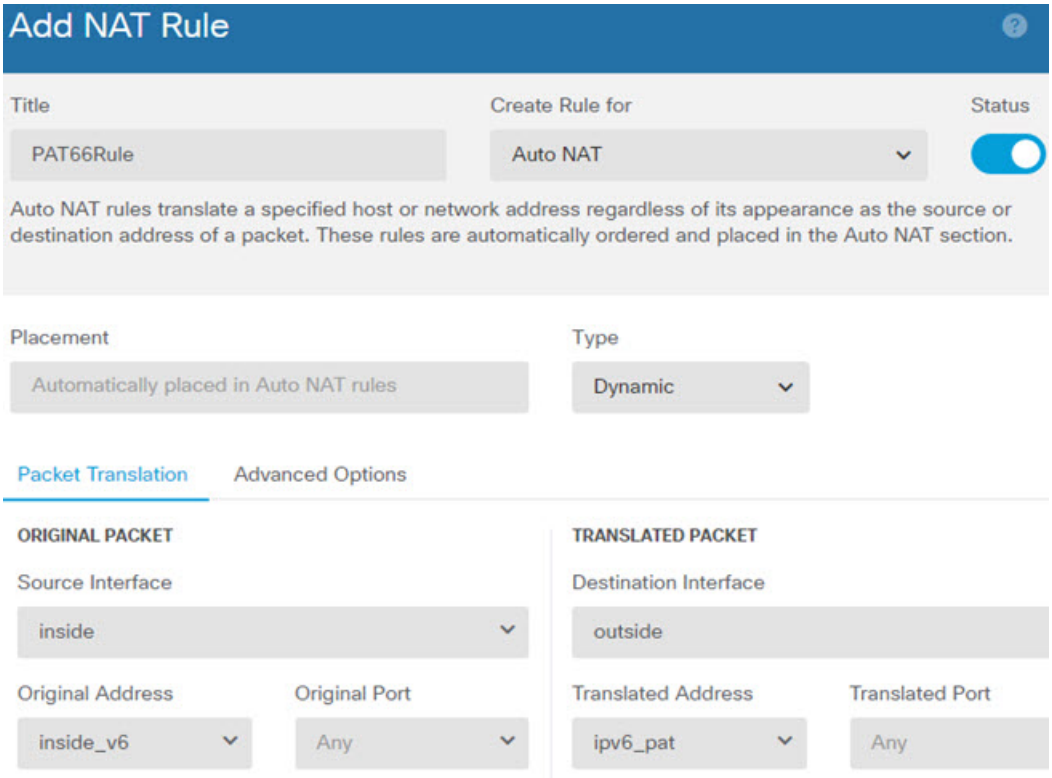
ステップ 2 内部 IPv6 ネットワークのダイナミック PAT ルールを設定します。

a) [ポリシー（Policies）] > [NAT] を選択します。

b) [+]ボタンをクリックします。

c) 次のプロパティを設定します。

- [タイトル（Title）] = PAT66Rule（または任意の別の名前）。
- [ルール作成目的（Create Rule For）]= Auto NAT。
- [タイプ（Type）] = Dynamic。
- [送信元インターフェイス（Source Interface）] = inside。
- [宛先インターフェイス（Destination Interface）] = outside。
- [元のアドレス（Original Address）] = inside_v6 ネットワーク オブジェクト。
- [変換されたアドレス（Translated Address）] = ipv6_pat ネットワーク オブジェクト。



d) [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上の 2001:db8:122:2091::/96 サブネットから外部インターフェイスに向かうすべてのトラフィックが、2001:db8:122:201b::2 上のポートへのダイナミック PAT66 変換を取得します。

NAT のモニタリング

NAT 接続をモニタしてトラブルシュートするには、デバイスの CLI にログインして次のコマンドを使用します。

- **show nat**：NAT ルールとルールごとのヒット カウントが表示されます。NAT のその他のアスペクトを表示するための追加キーワードがあります。
- **show xlate**：現在アクティブになっている実際の NAT 変換が表示されます。
- **clear xlate**：アクティブな NAT 変換を削除できます。既存の接続ではその接続が終了するまで古い変換スロットが使用されるため、NAT ルールを変更すると、アクティブな変換の削除が必要になることがあります。変換を削除することで、システムは新しいルールに基づき、次にクライアントの接続が試行されるときにそのクライアントに対する新しい変換を作成できます。

NAT の例

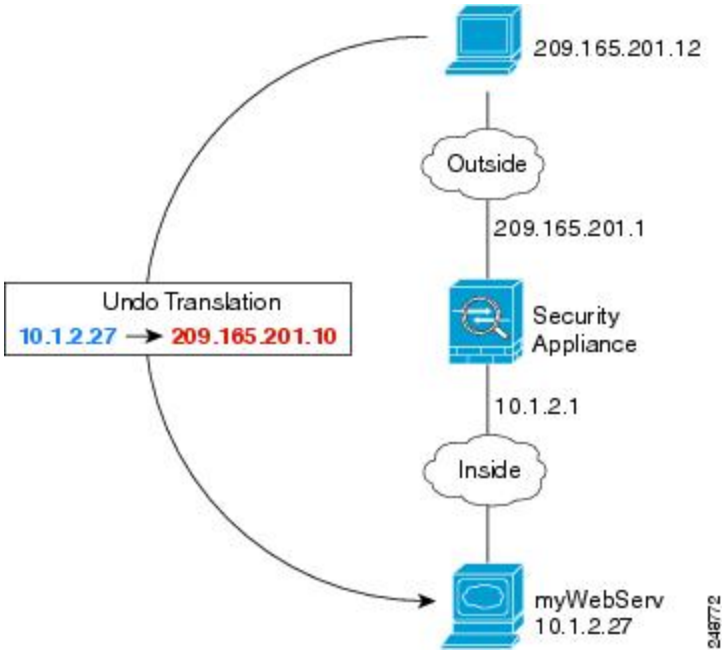
以下の各トピックでは、Threat Defense デバイスでの NAT の設定例を紹介します。

内部 Web サーバへのアクセスの提供（スタティック自動 NAT）

次の例では、内部 Web サーバに対してスタティック NAT を実行します。実際のアドレスはプライベート ネットワーク上にあるため、パブリック アドレスが必要です。スタティック NAT は、固定アドレスにある Web サーバ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。

（注） この例は、内部インターフェイスがブリッジ グループ インターフェイス（BVI）ではなく標準ルーテッドインターフェイスであることを前提としています。内部インターフェイスがBVIの場合は、Web サーバが接続されている特定のブリッジグループ メンバー インターフェイス（inside1_3 など）を選択します。

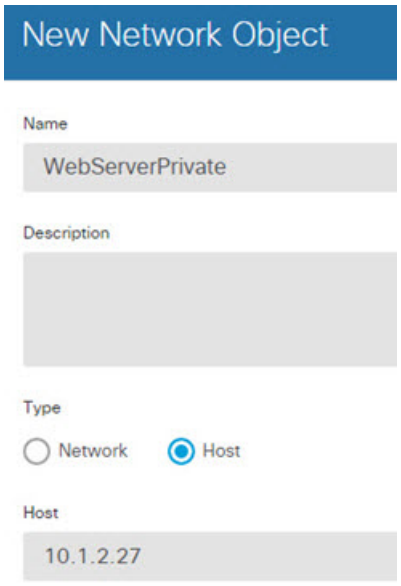
図 *13*：内部 *Web* サーバのスタティック *NAT*



手順

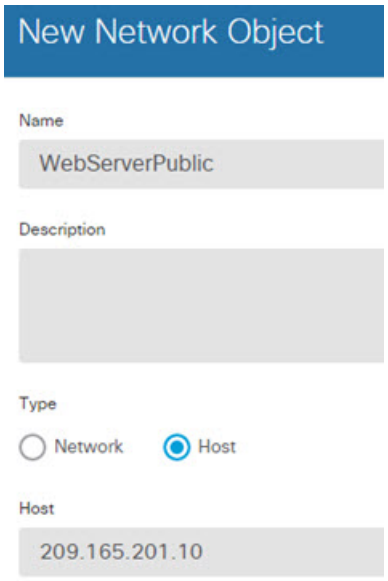
ステップ 1 サーバのプライベート ホスト アドレスとパブリック ホスト アドレスを定義するネットワーク オブジェクトを作成します。

a) [オブジェクト（Objects）] を選択します。
b) コンテンツ テーブルから [ネットワーク（Network）] を選択し、[+] をクリックします。
c) Web サーバのプライベート アドレスを定義します。
ネットワーク オブジェクトに名前を付け（WebServerPrivate など）、[ホスト（Host）] を選択して、実際のホスト IP アドレスとして 10.1.2.27 を入力します。



d) [追加（Add）][OK] をクリックします。

e) [+]をクリックし、パブリック アドレスを定義します。
ネットワーク オブジェクトに名前を付け（WebServerPublic など）、[ホスト（Host）] を選択して、ホスト アドレスとして 209.165.201.10 を入力します。



f) [追加（Add）][OK] をクリックします。

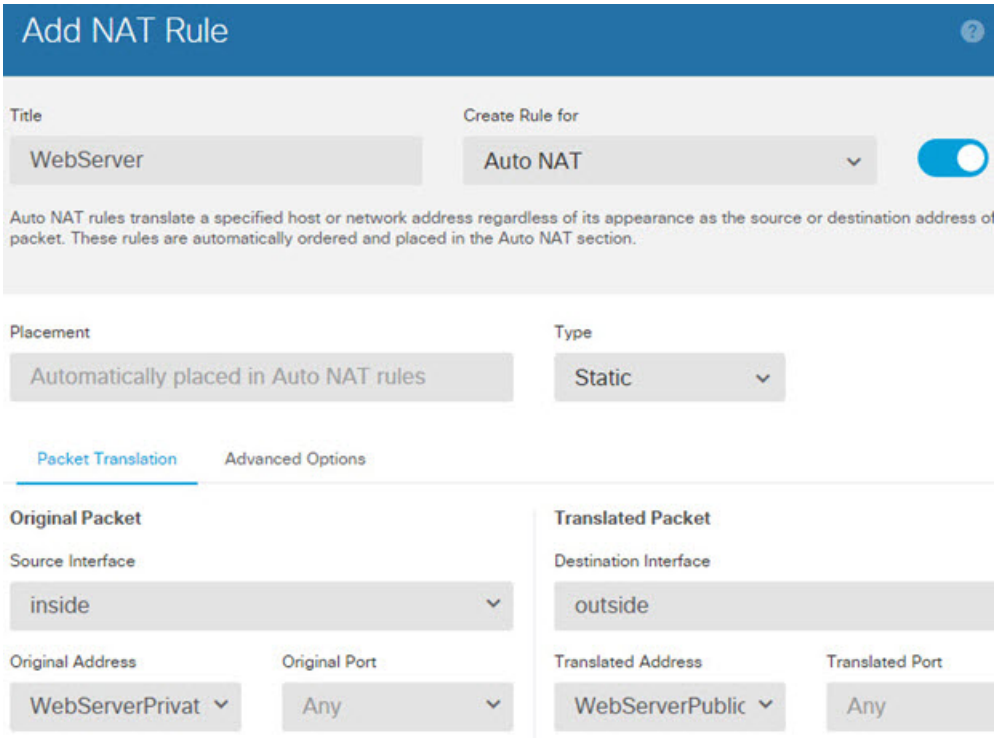
ステップ 2 オブジェクトのスタティック NAT を設定します。

a) [ポリシー（Policies）] > [NAT] を選択します。

b) [+]ボタンをクリックします。

c) 次のプロパティを設定します。

- [タイトル（Title）] = WebServer（または任意の別の名前）。
- [ルール作成目的（Create Rule For）]= Auto NAT。
- [タイプ（Type）] = Static。
- [送信元インターフェイス（Source Interface）] = inside。
- [宛先インターフェイス（Destination Interface）] = outside。
- [元のアドレス（Original Address）] = WebServerPrivate ネットワーク オブジェクト。
- [変換されたアドレス（Translated Address）] = WebServerPublic ネットワーク オブジェクト。



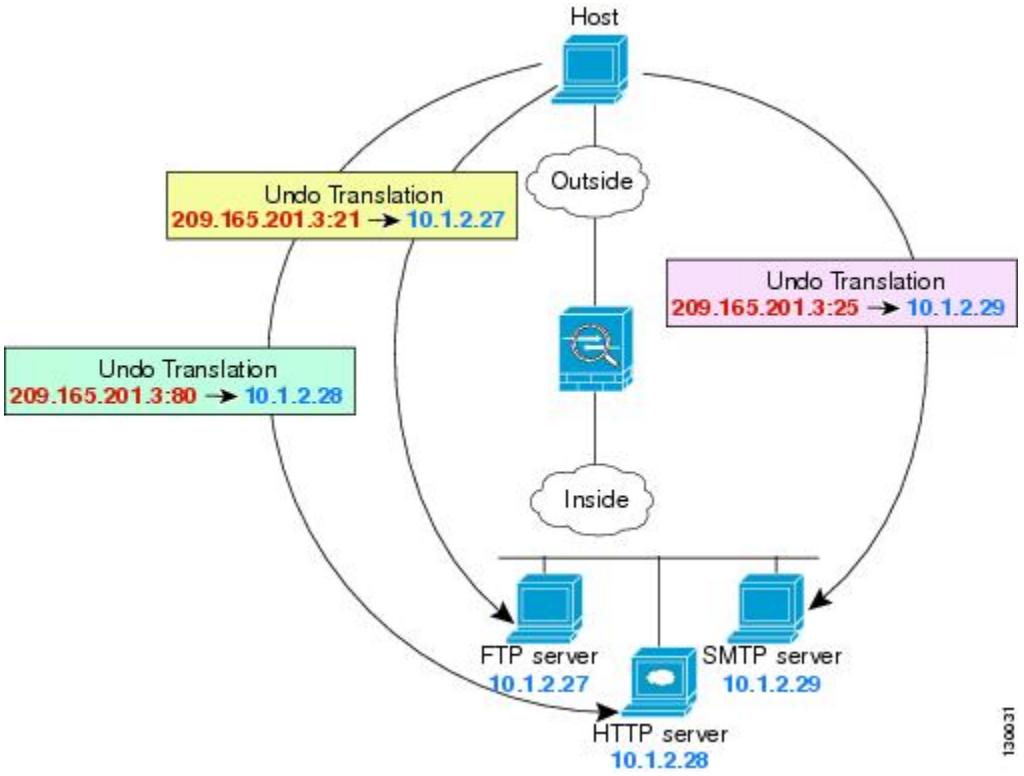
d) [OK]をクリックします。

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自動 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。

（注） この例では、内部インターフェイスはスイッチに接続されている標準のルーテッド インターフェイスであり、サーバはそのスイッチに接続されていると仮定します。内部インターフェイスがブリッジ グループ インターフェイス（BVI）であり、各サーバが別個のブリッジ グループ メンバー インターフェイスに接続されている場合は、各サーバが接続されている特定のメンバー インターフェイスを選択して対応するルールを設定します。たとえば、ルールでは送信元インターフェイスとして inside ではなく inside1_2、inside1_3、および inside1_4 を設定します。

図 *14*：ポート変換を設定したスタティック *NAT*



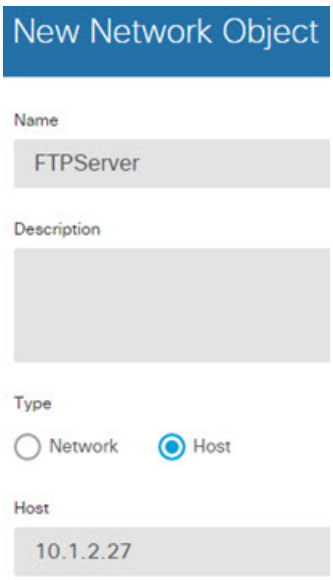
手順

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ます。

a) [オブジェクト（Objects）]を選択します。

b) コンテンツのテーブルから [ネットワーク（Network）]を選択し、[+] をクリックします。

c) ネットワーク オブジェクトの名前（たとえば FTPserver）を入力し、[ホスト（Holst）]を選択し、FTP サーバの実際の IP アドレス（10.1.2.27）を入力します。

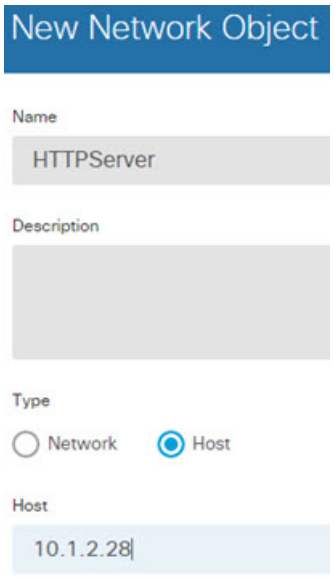


d) [追加（Add）]、[OK] の順にクリックします。

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ます。

a) [+]をクリックします。

b) ネットワーク オブジェクトの名前（たとえばHTTPserver）を入力し、[ホスト（Holst）]を選択し、ホストのアドレス（10.1.2.28）を入力します。

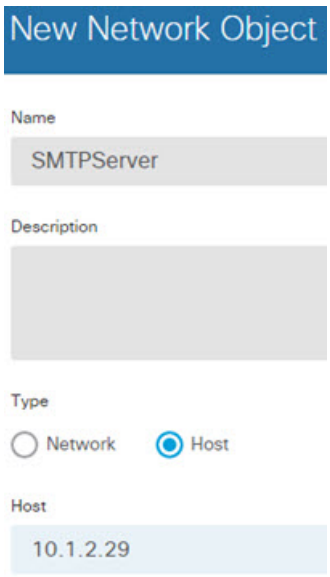


c) [追加（Add）]、[OK] の順にクリックします。

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ます。

a) [+]をクリックします。

b) ネットワーク オブジェクトの名前（たとえば SMTPserver）を入力し、[ホスト（Holst）]を選択し、ホストのアドレス（10.1.2.29）を入力します。

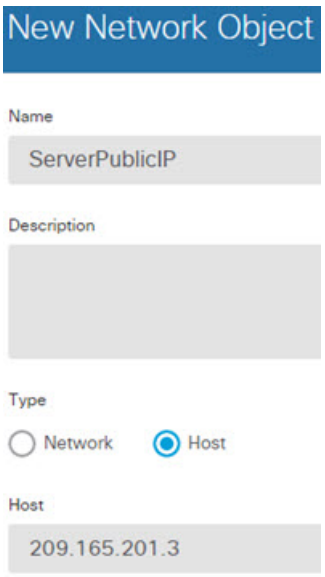


c) [追加（Add）]、[OK] の順にクリックします。

ステップ 4 3 つのサーバに使用するパブリック IP アドレスのネットワーク オブジェクトを作成します。

a) [+]をクリックします。

b) ネットワーク オブジェクトの名前（たとえば ServerPublicIP）を入力し、[ホスト（Holst）]を選択し、ホストのアドレス（209.165.201.3）を入力します。

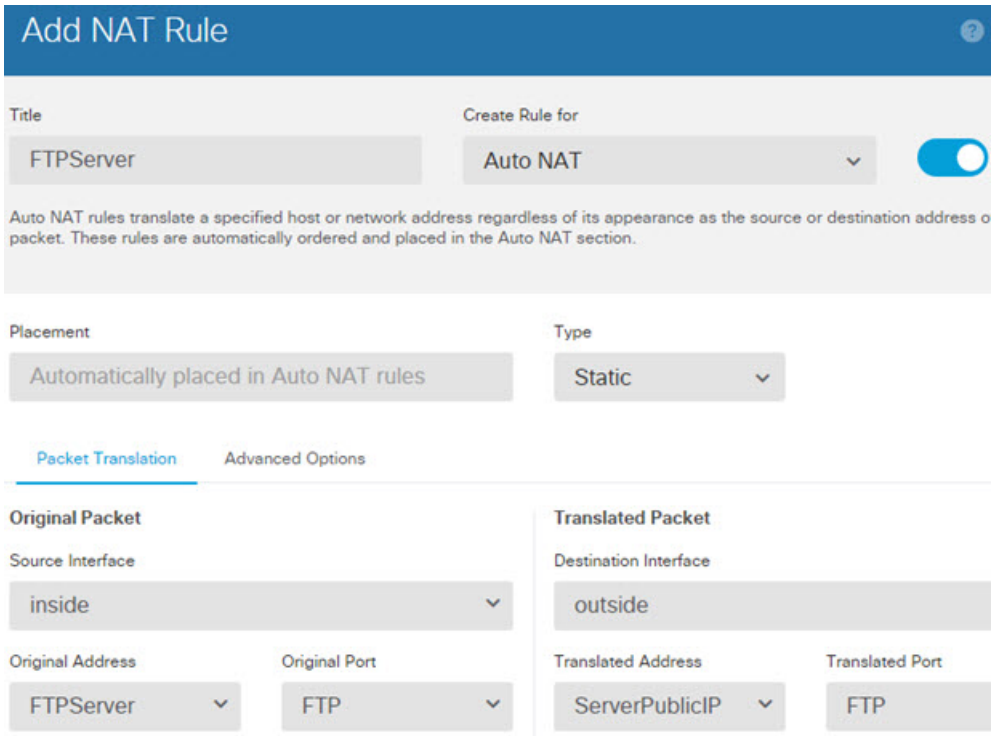


c) [追加（Add）]、[OK] の順にクリックします。

ステップ 5 FTP サーバ用に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プします。

a) [ポリシー（Policies）] > [NAT] を選択します。
b) [+]ボタンをクリックします。
c) 次のプロパティを設定します。

- [タイトル（Title）]：FTPServer（または選択した別の名前）。
- [作成するルールの対象（Create Rule For）]：Auto NAT。
- [タイプ（Type）]：Static。
- [送信元インターフェイス（Source Interface）]：inside。
- [宛先インターフェイス：（Destination Interface）]：outside。
- [元のアドレス（Original Address）]：FTPserver ネットワーク オブジェクト。
- [変換されたアドレス（Translated Address）]：ServerPublicIP ネットワーク オブジェクト。
- [元のポート（Original Port）]：FTP ポート オブジェクト。
- [変換されたポート（Translated Port）]：FTP ポート オブジェクト。



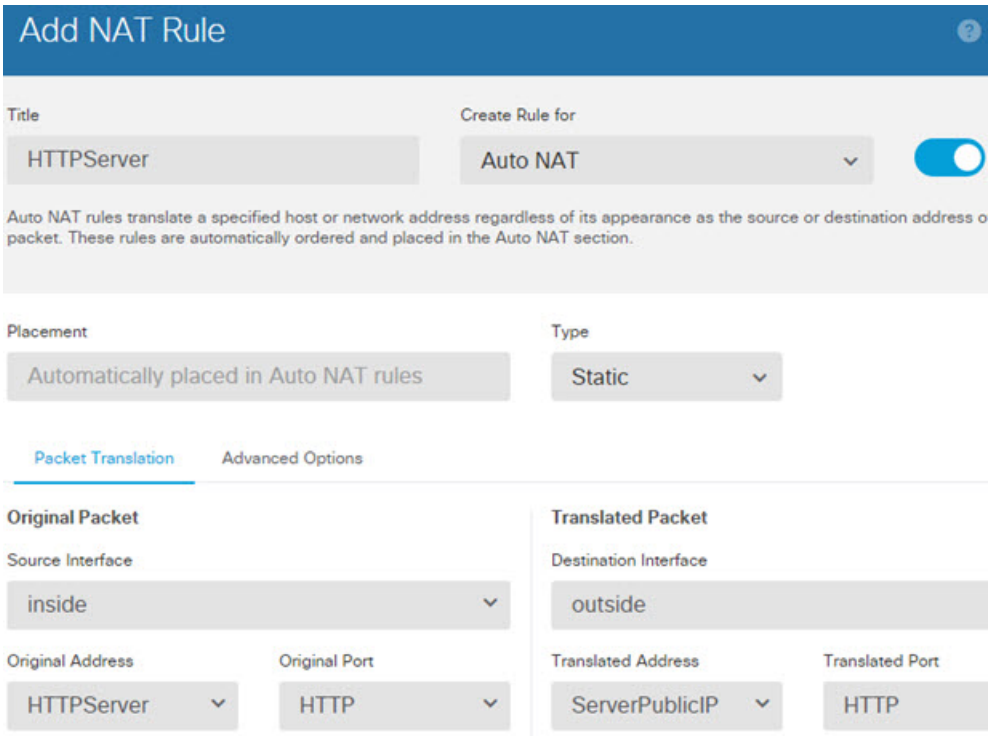
d) [OK]をクリックします。

ステップ 6 HTTP サーバ用にポート変換を設定したスタティック NAT を設定し、HTTP ポートを自身にマップします。

a) [+]ボタンをクリックします。

b) 次のプロパティを設定します。

- [タイトル（Title）]：HTTPServer（または選択した別の名前）。
- [作成するルールの対象（Create Rule For）]：Auto NAT。
- [タイプ（Type）]：Static。
- [送信元インターフェイス（Source Interface）]：inside。
- [宛先インターフェイス：（Destination Interface）]：outside。
- [元のアドレス（Original Address）]：HTTPserver ネットワーク オブジェクト。
- [変換されたアドレス（Translated Address）]：ServerPublicIP ネットワーク オブジェクト。
- [元のポート（Original Port）]：HTTP ポート オブジェクト。
- [変換されたポート（Translated Port）]：HTTP ポート オブジェクト。



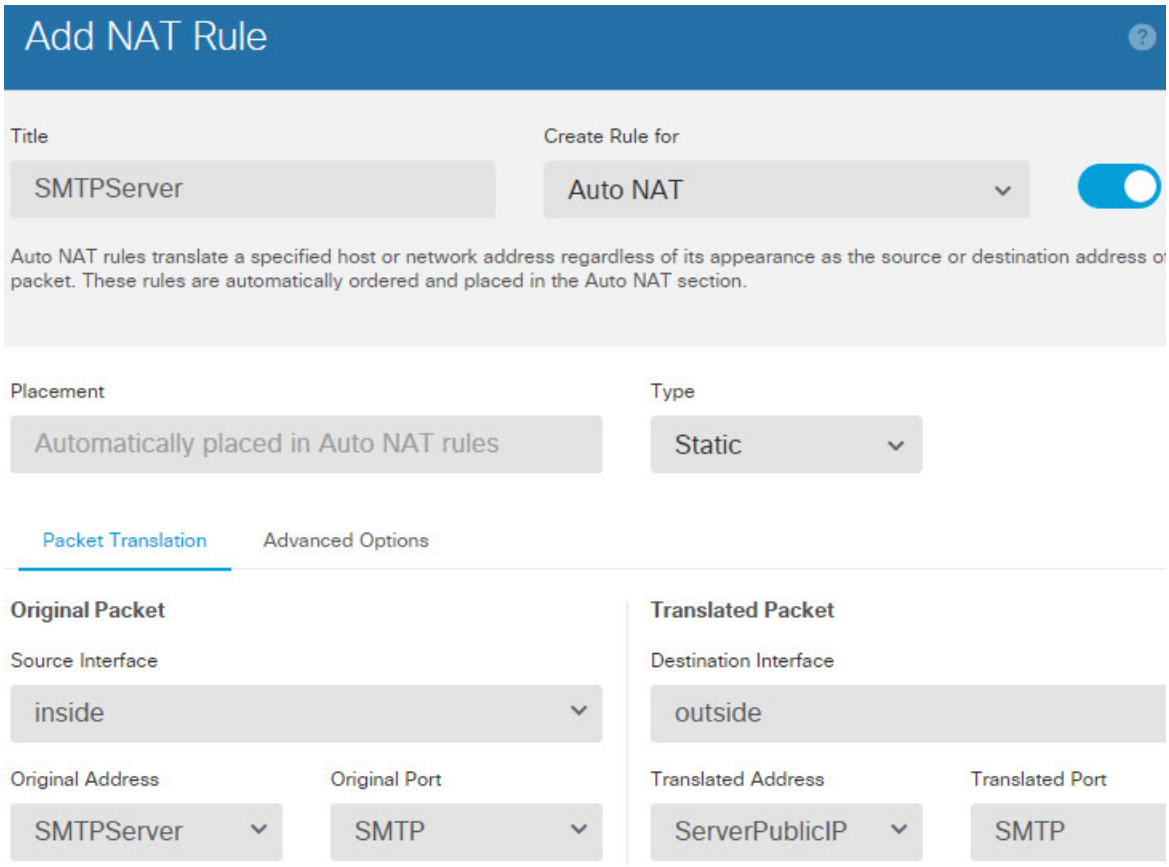
c) [OK]をクリックします。

ステップ 7 SMTP サーバ用に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プします。

a) [+]ボタンをクリックします。

b) 次のプロパティを設定します。

- [タイトル（Title）]：SMTPServer（または選択した別の名前）。
- [作成するルールの対象（Create Rule For）]：Auto NAT。
- [タイプ（Type）]：Static。
- [送信元インターフェイス（Source Interface）]：inside。
- [宛先インターフェイス：（Destination Interface）]：outside。
- [元のアドレス（Original Address）]：SMTPServer ネットワーク オブジェクト。
- [変換されたアドレス（Translated Address）]：ServerPublicIP ネットワーク オブジェクト。
- [元のポート（Original Port）]：SMTP ポート オブジェクト。
- [変換されたポート（Translated Port）]：SMTP ポート オブジェクト。



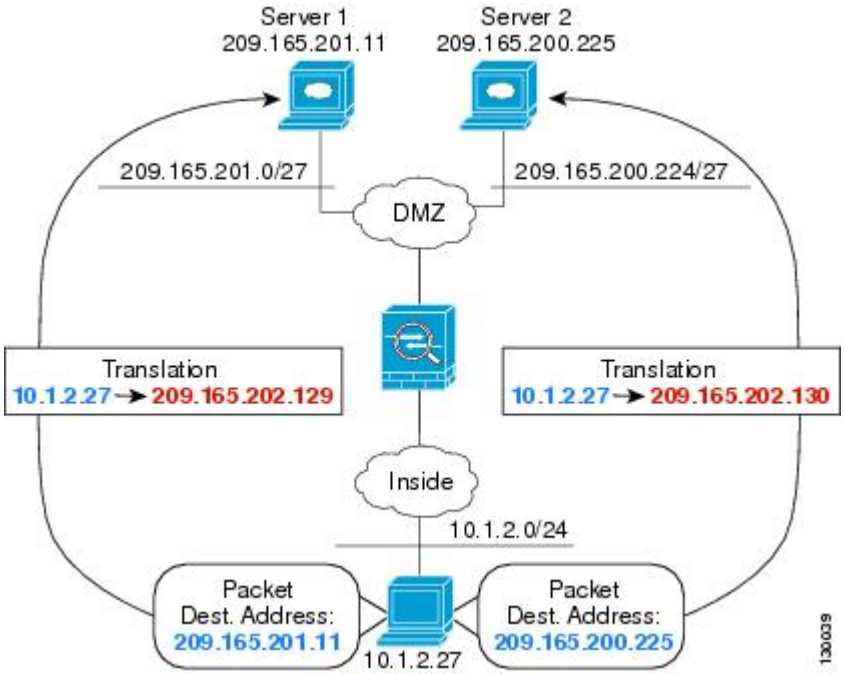
c) [OK]をクリックします。

宛先に応じて異なる変換（ダイナミック手動 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。

（注） この例では、内部インターフェイスがスイッチに接続され、サーバがスイッチに接続されている標準ルーテッド インターフェイスであると仮定します。内部インターフェイスがブリッジ グループ インターフェイス（BVI）であり、サーバが別のブリッジ グループ メンバー インターフェイスに接続されている場合、対応するルールに対してサーバが接続されている特定のメンバー インターフェイスを選択します。たとえば、ルールは、内部インターフェイスではなく、送信元インターフェイスの inside1_2 および inside1_3 を持つ場合があります。

図 *15*：異なる宛先アドレスを使用する手動 *NAT*



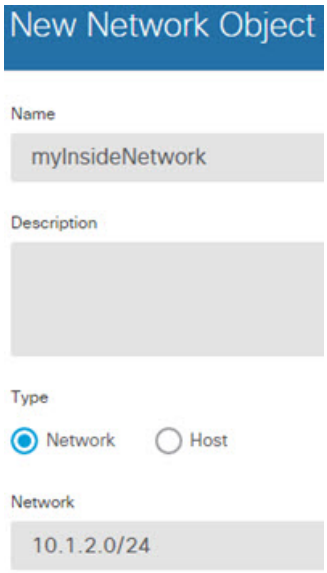
手順

ステップ 1 内部ネットワークのネットワーク オブジェクトを作成します。

a) [オブジェクト（Objects）]を選択します。

b) 目次から [ネットワーク（Network）]を選択し、[+] をクリックします。

c) ネットワーク オブジェクトに名前を付け（myInsideNetwork など）、[ネットワーク（Network）] を選択して、実際のネットワーク アドレス 10.1.2.0/24 を入力します。

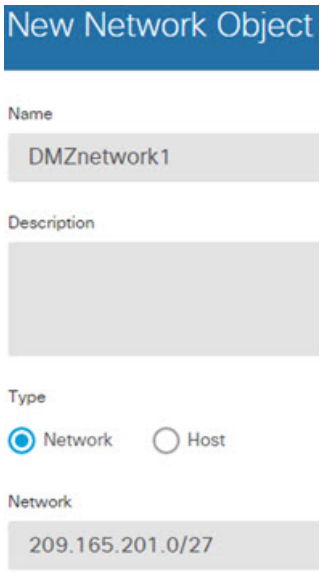


d) [追加（Add）][OK] をクリックします。

ステップ 2 DMZ ネットワーク 1 のネットワーク オブジェクトを作成します。

a) [+]をクリックします。

b) ネットワーク オブジェクトに名前を付け（DMZnetwork1 など）、[ネットワーク（Network）] を選択し、ネットワーク アドレス 209.165.201.0/27 を入力します（255.255.255.224 のサブネット マスク）。

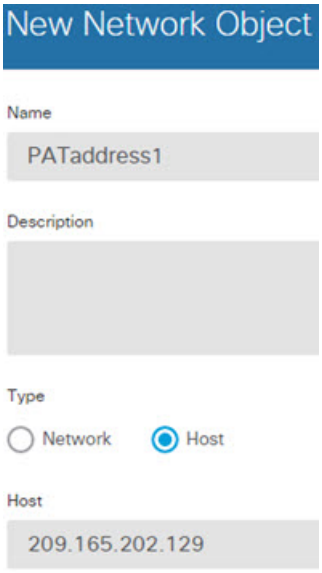


c) [追加（Add）][OK] をクリックします。

ステップ 3 DMZ ネットワーク 1 の PAT アドレスのネットワーク オブジェクトを作成します。

a) [+]をクリックします。

b) ネットワーク オブジェクトに名前を付け（PATaddress1 など）、[ホスト（Host）]を選択して、ホスト アドレス 209.165.202.129 を入力します。

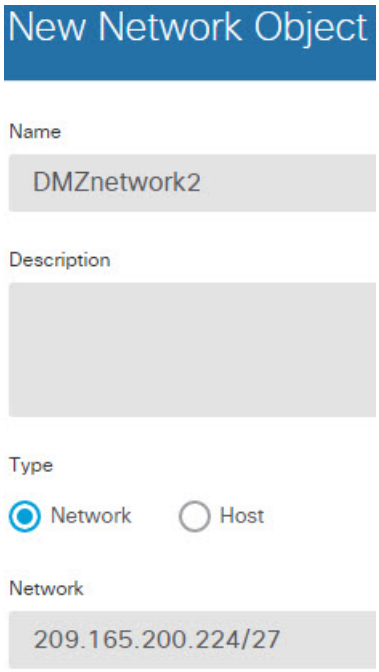


c) [追加（Add）][OK] をクリックします。

ステップ 4 DMZ ネットワーク 2 のネットワーク オブジェクトを作成します。

a) [+]をクリックします。

b) ネットワーク オブジェクトに名前を付け（DMZnetwork2 など）、[ネットワーク（Network）]を選択し、ネットワーク アドレス 209.165.200.224/27 を入力します（255.255.255.224 のサブネット マスク）。

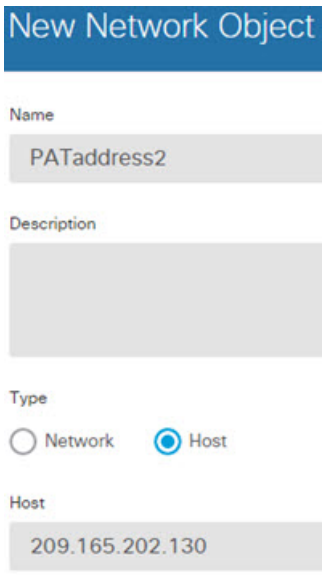


c) [追加（Add）][OK] をクリックします。

ステップ 5 DMZ ネットワーク 2 の PAT アドレスのネットワーク オブジェクトを作成します。

a) [+]をクリックします。

b) ネットワーク オブジェクトに名前を付け（PATaddress2 など）、[ホスト（Host）]を選択して、ホスト アドレス 209.165.202.130 を入力します。



c) [追加（Add）][OK] をクリックします。

ステップ 6 DMZ ネットワーク 1 のダイナミック手動 PAT を設定します。

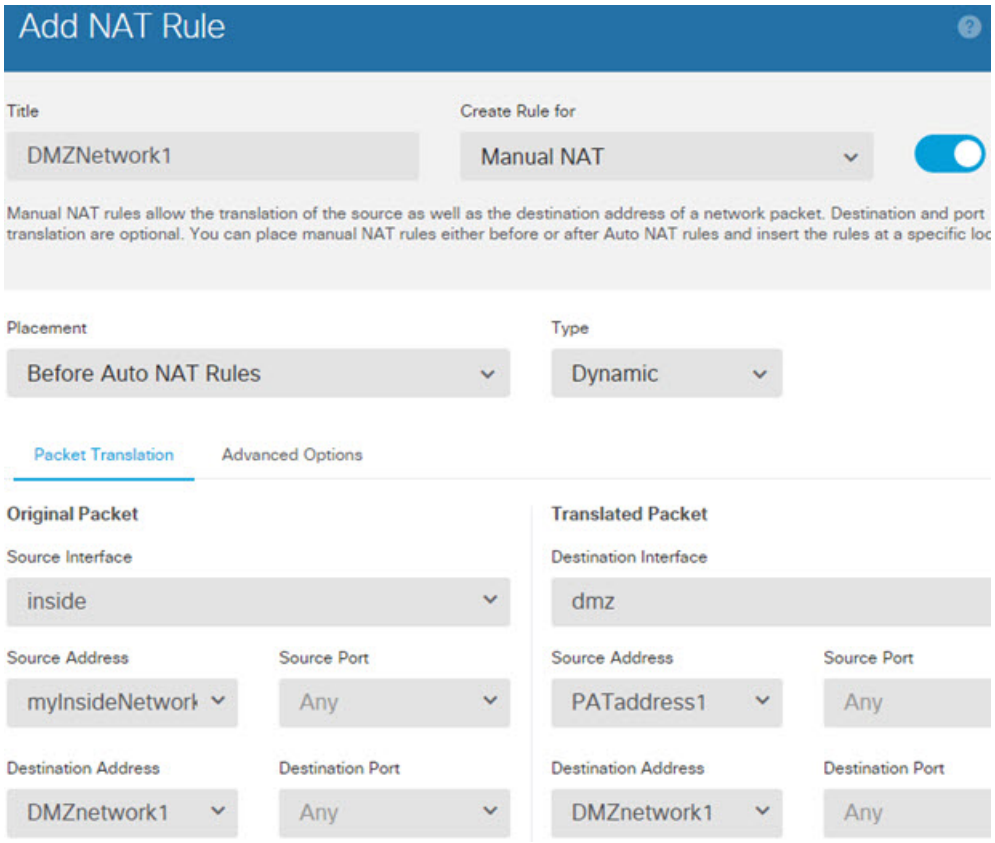
a) [ポリシー（Policies）] > [NAT] を選択します。

b) [+]ボタンをクリックします。

c) 次のプロパティを設定します。

- タイトル（Title）= DMZNetwork1（または任意の別の名前）。
- ルールの作成先（Create Rule For）= Manual NAT。
- タイプ（Type）= Dynamic。
- 送信元インターフェイス（Source Interface）= inside。
- 宛先インターフェイス（Destination Interface）= dmz。
- 元の発信元アドレス（Original Source Address）= myInsideNetwork のネットワーク オブジェクト。
- 変換済みの発信元アドレス（Translated Source Address）= PATaddress1 のネットワーク オブジェクト。
- 元の宛先アドレス（Original Destination Address）= DMZnetwork1 のネットワーク オブジェクト。
- 変換済みの宛先アドレス（Translated Destination Address）= DMZnetwork1 のネットワーク オブジェクト。

（注） 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。[ポート（Port）] フィールドはすべて空白のままにします。



d) [OK]をクリックします。

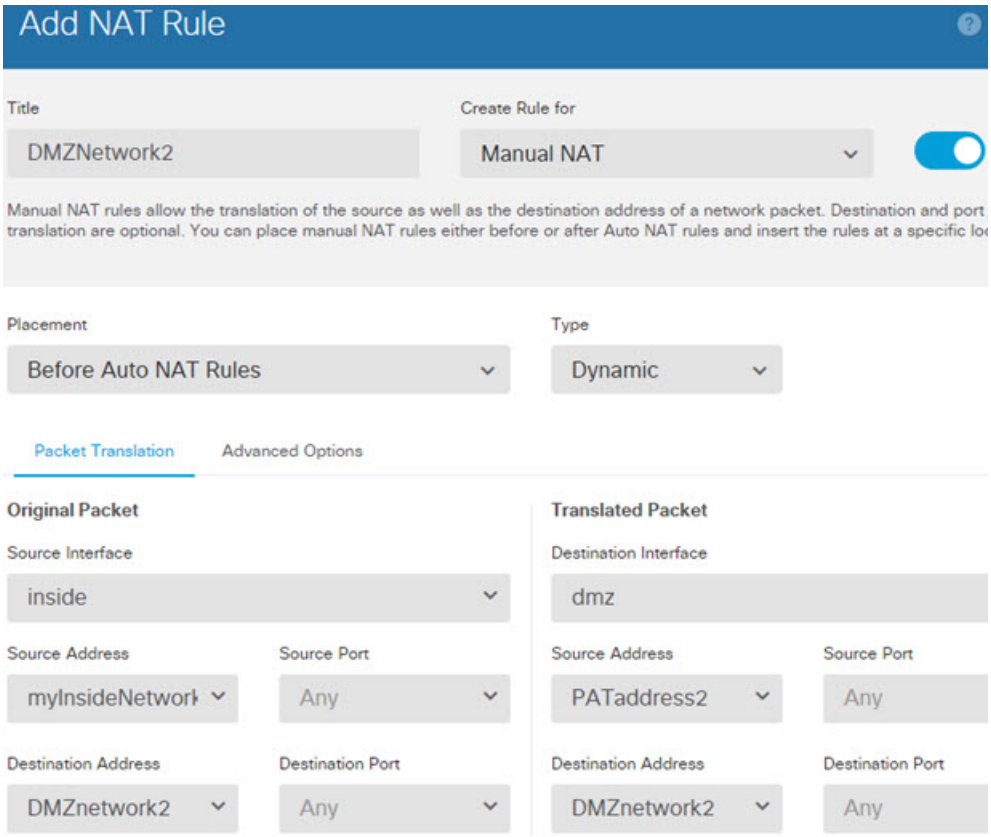
ステップ 7 DMZ ネットワーク 2 のダイナミック手動 PAT を設定します。

a) [+]ボタンをクリックします。

b) 次のプロパティを設定します。

- タイトル（Title）= DMZNetwork2（または任意の別の名前）。
- ルールの作成先（Create Rule For）= Manual NAT。
- タイプ（Type）= Dynamic。
- 送信元インターフェイス（Source Interface）= inside。
- 宛先インターフェイス（Destination Interface）= dmz。
- 元の発信元アドレス（Original Source Address）=myInsideNetwork のネットワーク オブジェクト。
- 変換済みの発信元アドレス（Translated Source Address）= PATaddress2 のネットワーク オブジェクト。
- 元の宛先アドレス（Original Destination Address）=DMZnetwork2 のネットワーク オブジェクト。

- 変換済みの宛先アドレス（Translated Destination Address）= DMZnetwork2 のネットワークオブジェクト。



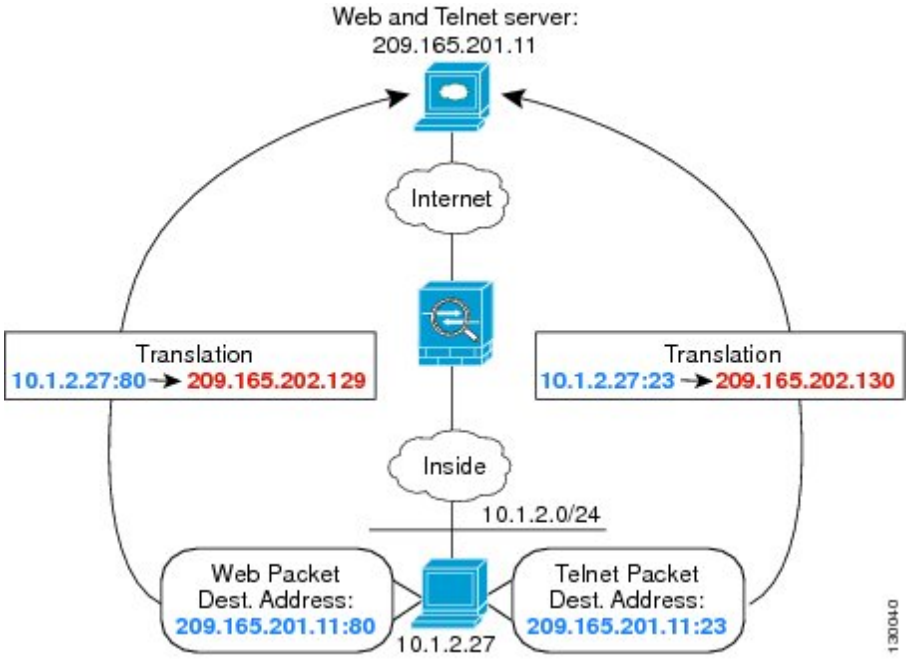
c) [OK]をクリックします。

宛先アドレスおよびポートに応じて異なる変換（ダイナミック手動 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:ポートに変換されます。ホストが Web サービスを求めて同じサーバにアクセスすると、実際のアドレスは 209.165.202.130:ポートに変換されます。

（注） この例では、内部インターフェイスがスイッチに接続され、サーバがスイッチに接続されている標準ルーテッド インターフェイスであると仮定します。内部インターフェイスがブリッジ グループ インターフェイス（BVI）であり、サーバがブリッジ グループ メンバー インターフェイスに接続されている場合、サーバが接続されている特定のメンバー インターフェイスを選択します。たとえば、ルールは、内部インターフェイスではなく、送信元インターフェイスの inside1_2 を持つ場合があります。

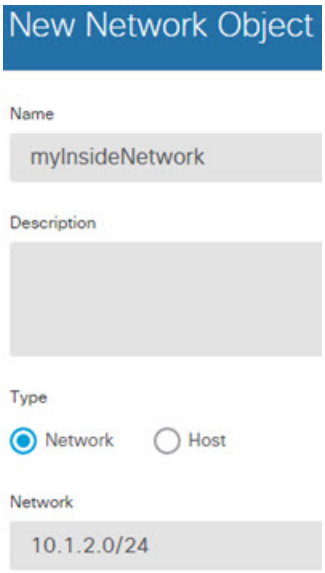
図 *16*：異なる宛先ポートを使用する手動 *NAT*



手順

ステップ 1 内部ネットワークのネットワーク オブジェクトを作成します。

a) [オブジェクト（Objects）]を選択します。
b) 目次から [ネットワーク（Network）]を選択し、[+] をクリックします。
c) ネットワーク オブジェクトに名前を付け（myInsideNetwork など）、[ネットワーク（Network）] を選択して、実際のネットワーク アドレス 10.1.2.0/24 を入力します。

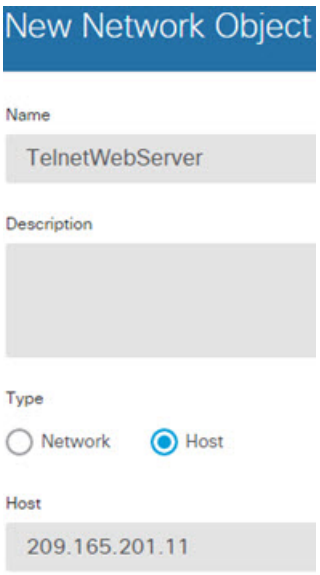


d) [追加（Add）][OK] をクリックします。

ステップ 2 Telnet/Web サーバのネットワーク オブジェクトを作成します。

a) [+]をクリックします。

b) ネットワーク オブジェクトに名前を付け（TelnetWebServer など）、[ホスト（Host）]を選択して、ホスト アドレス 209.165.201.11 を入力します。

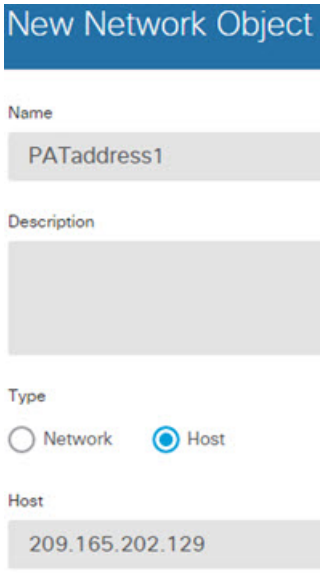


c) [追加（Add）][OK] をクリックします。

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 オブジェクトを作成します。

a) [+]をクリックします。

b) ネットワーク オブジェクトに名前を付け（PATaddress1 など）、[ホスト（Host）]を選択して、ホスト アドレス 209.165.202.129 を入力します。

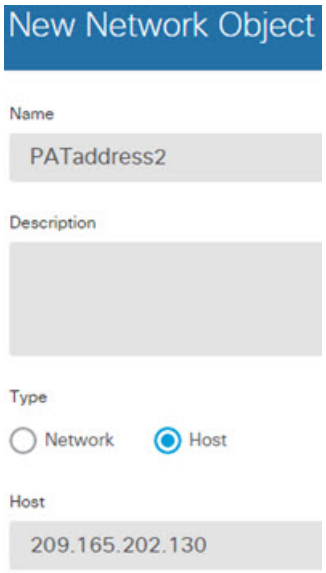


c) [追加（Add）][OK] をクリックします。

ステップ 4 HTTP を使用するときは、PAT アドレスのネットワーク オブジェクトを作成します。

a) [+]をクリックします。

b) ネットワーク オブジェクトに名前を付け（PATaddress2 など）、[ホスト（Host）]を選択して、ホスト アドレス 209.165.202.130 を入力します。



c) [追加（Add）][OK] をクリックします。

ステップ 5 Telnet アクセスのダイナミック手動 PAT を設定します。

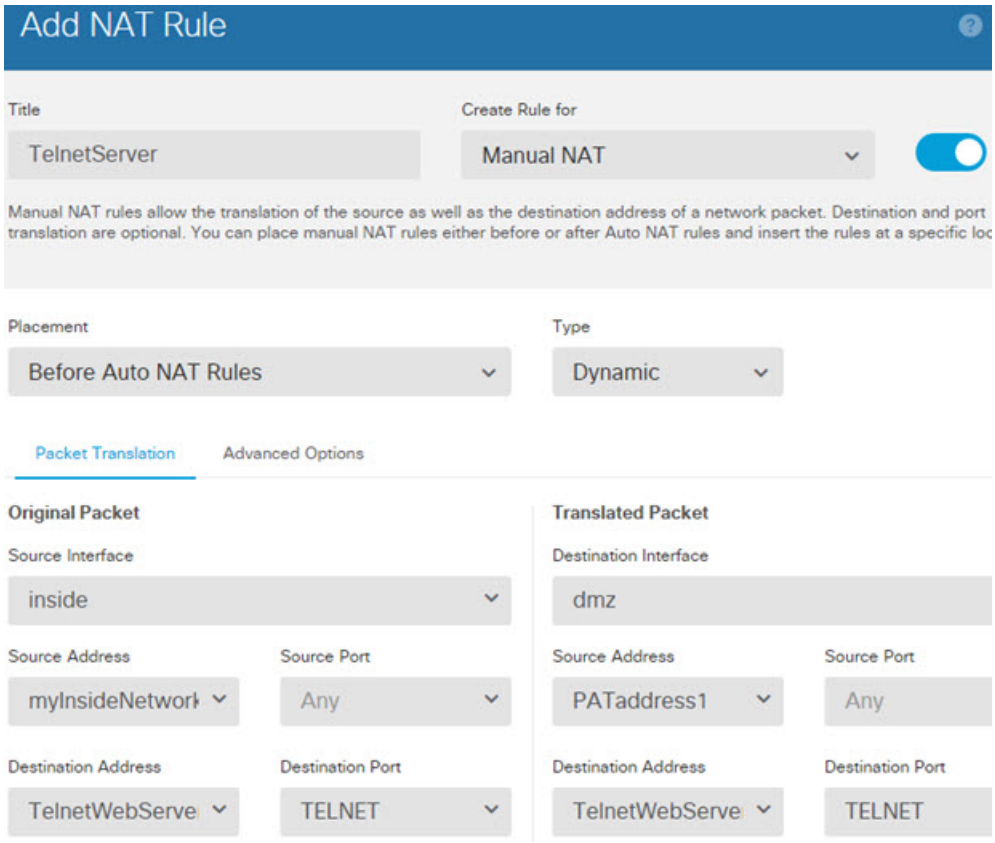
a) [ポリシー（Policies）] > [NAT] を選択します。

b) [+]ボタンをクリックします。

c) 次のプロパティを設定します。

- タイトル（Title）= TelnetServer（または任意の別の名前）。
- ルールの作成先（Create Rule For）= Manual NAT。
- タイプ（Type）= Dynamic。
- 送信元インターフェイス（Source Interface）= inside。
- 宛先インターフェイス（Destination Interface）= dmz。
- 元の発信元アドレス（Original Source Address）= myInsideNetwork のネットワーク オブジェクト。
- 変換済みの発信元アドレス（Translated Source Address）= PATaddress1 のネットワーク オブジェクト。
- 元の宛先アドレス（Original Destination Address）= TelnetWebServer のネットワーク オブジェクト。
- 変換済みの宛先アドレス（Translated Destination Address）= TelnetWebServer のネットワーク オブジェクト。
- 元の宛先ポート（Original Destination Port）= TELNET ポート オブジェクト。
- 変換済みの宛先ポート（Translated Destination Port）= TELNET ポート オブジェクト。

（注） 宛先アドレスまたはポートを変換しないため、元のアドレスと変換済みの宛先アドレスに同じアドレスを指定し、元のポートと変換済みのポート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。



d) [OK]をクリックします。

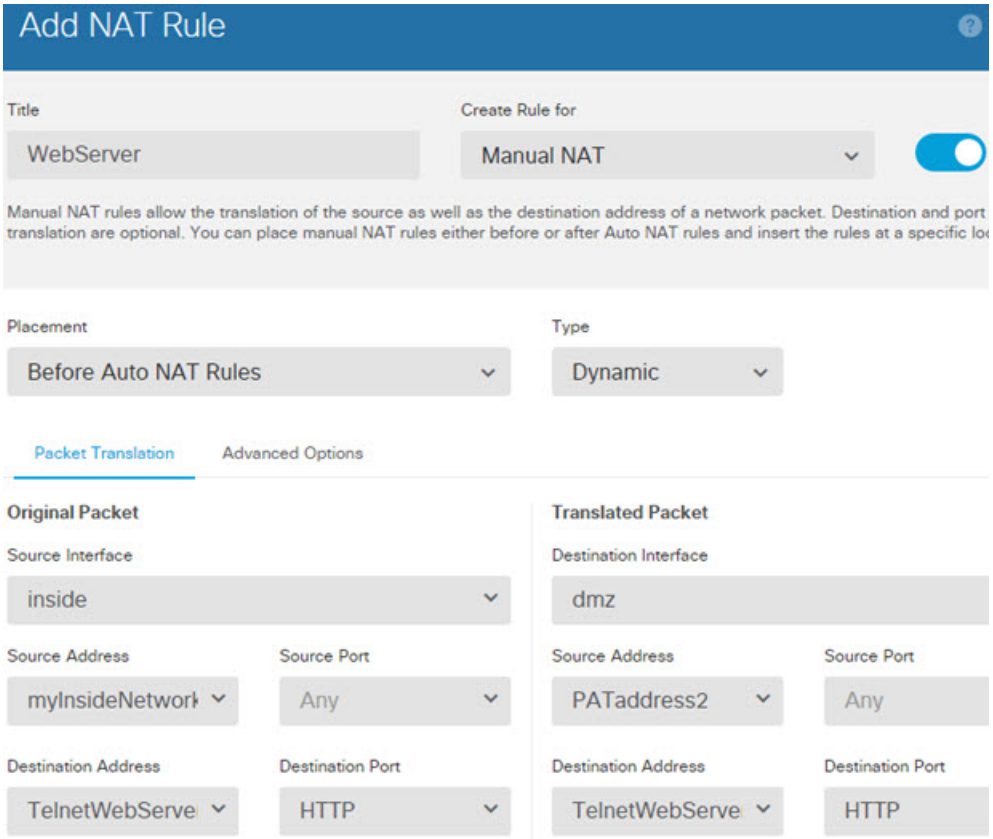
ステップ 6 Web アクセスのダイナミック手動 PAT を設定します。

a) [+]ボタンをクリックします。

b) 次のプロパティを設定します。

- タイトル（Title）= WebServer（または任意の別の名前）。
- ルールの作成先（Create Rule For）= Manual NAT。
- タイプ（Type）= Dynamic。
- 送信元インターフェイス（Source Interface）= inside。
- 宛先インターフェイス（Destination Interface）= dmz。
- 元の発信元アドレス（Original Source Address）=myInsideNetwork のネットワーク オブジェクト。
- 変換済みの発信元アドレス（Translated Source Address）= PATaddress2 のネットワーク オブジェクト。
- 元の宛先アドレス（Original Destination Address）= TelnetWebServer のネットワーク オブジェクト。

- 変換済みの宛先アドレス（Translated Destination Address）= TelnetWebServer のネットワーク オブジェクト。
- 元の宛先ポート（Original Destination Port）= HTTP ポート オブジェクト。
- 変換済みの宛先ポート（Translated Destination Port）= HTTP ポート オブジェクト。



c) [OK]をクリックします。

NAT による DNS クエリおよび応答のリライト

DNS 応答を修正して、応答内のアドレスを、NAT 設定に適合するアドレスに置換できるように、Firepower Threat Defense デバイスを設定しなければならない場合があります。DNS 修正は、各トランスレーション ルールの設定時に設定できます。

これは、NAT ルールに一致する DNS クエリおよび応答内のアドレスをリライトする機能です（たとえば、IPv4 の場合は A レコード、IPv6 の場合は AAAA、逆引き DNS クエリの場合は 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リライトされます。

NAT ルールに対して DNS リライトを設定しなければならなくなるのは、次のような状況です。

- ルールが NAT64 または NAT46 であり、DNS サーバが外部ネットワーク上にある場合。DNS A レコード（IPv4 用）と AAAA レコード（IPv6）とを変換するため、DNS リライトが必要になります。
- DNS サーバは外部に、クライアントは内部にあり、クライアントが使用する完全修飾ドメイン名の一部が、他の内部ホストとして解決される場合。
- DNS サーバは内部にあり、プライベート IP アドレスを使用して応答しているのに対し、クライアントが外部にあり、これらのクライアントが、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場合。

DNS リライトの制限事項

DNS リライトには、次のようないくつかの制限事項があります。

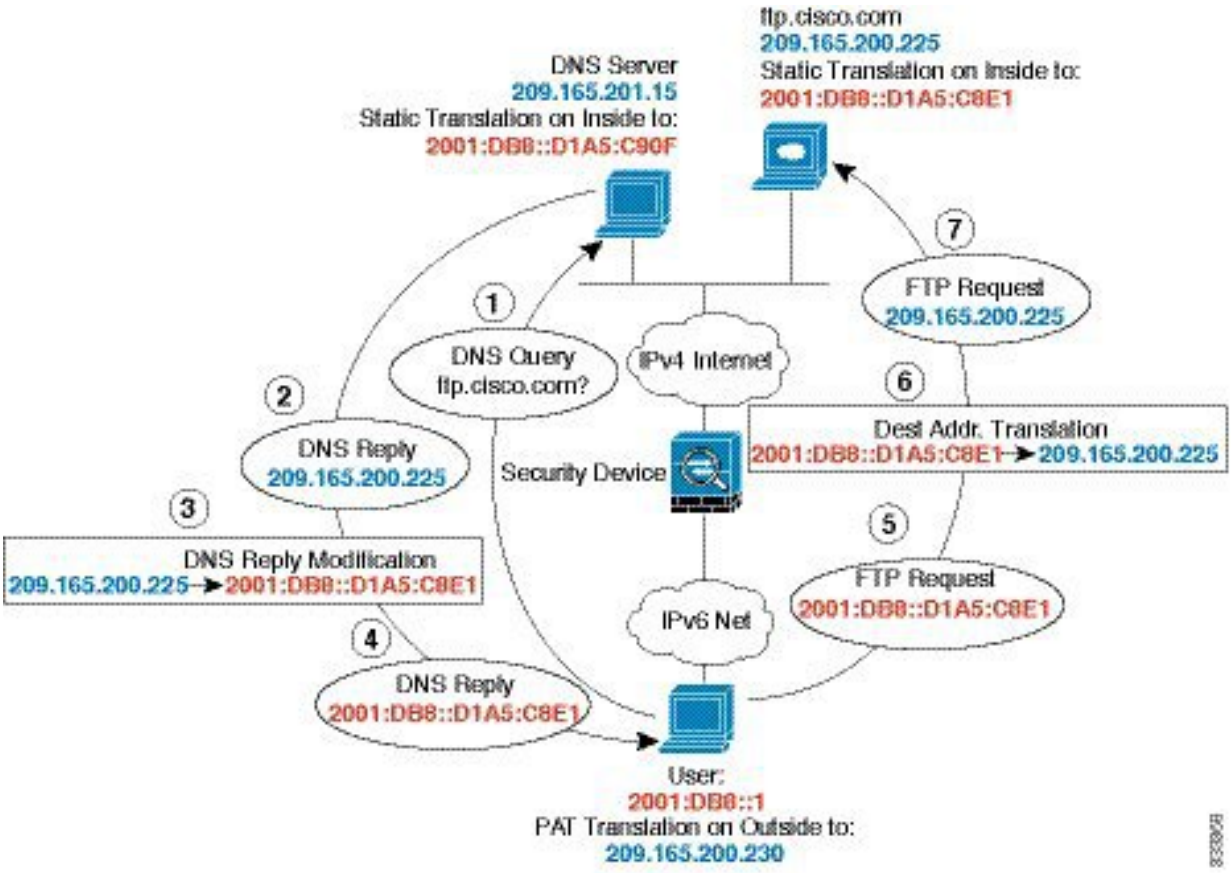
- DNS リライトは PAT には適用されません。個々の A レコードまたは AAAA レコードには複数の PAT ルールが適用可能であり、どの PAT ルールが使用されるかはあいまいであるためです。
- 手動 NATルールを設定し、宛先アドレスと発信元アドレスの両方を指定する場合は、DNS 修正を設定することはできません。このようなルールでは、A に送信する場合、B に送信する場合とで、単一アドレスが異なるアドレスに変換される可能性があります。この場合、Firepower Threat Defense デバイスでは、DNS 応答内の IP アドレスを適切な Twice NAT ルールに正確に適合させることができません。DNS 応答には、DNS 要求を促すパケット内に、どのような送信元/宛先アドレスの組み合わせが含まれていたかを示す情報は含まれません。
- DNS リライトは実際には、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 が存在しない場合は、リライトは正しく実行されません。スタティック NAT の場合は、この問題が生じることはありません。
- DNS リライトでは、DNS 動的更新メッセージはリライトされません（opcode 5）。

以下の各トピックでは、NAT ルールにおける DNS リライトのさまざまな例を示します。

DNS 64 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 の IPv6 の相当物）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。

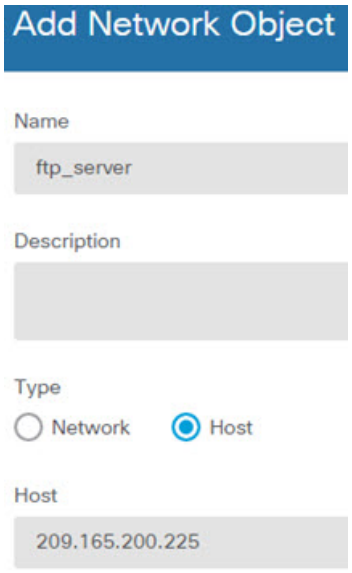


（注） この例では、内部インターフェイスがブリッジグループインターフェイス（BVI）ではなく、標準ルーテッド インターフェイスであると仮定します。内部インターフェイスが BVI である場合、各メンバー インターフェイスのルールを複製する必要があります。

手順

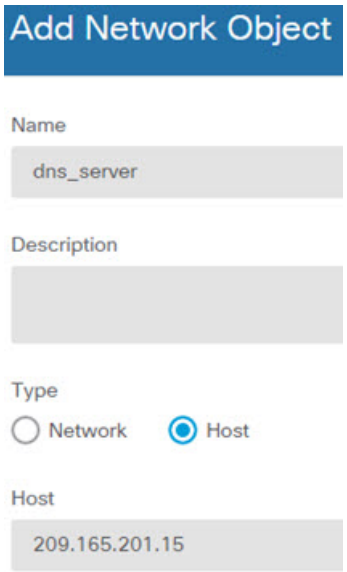
ステップ 1 FTP サーバ、DNS サーバ、内部ネットワーク、および PAT プールのネットワーク オブジェクトを作成します。

a) [オブジェクト（Objects）]を選択します。
b) 目次から [ネットワーク（Network）]を選択し、[+] をクリックします。
c) 実際の FTP サーバ アドレスを定義します。
ネットワーク オブジェクトに名前を付け（ftp_server など）、[ホスト（Host）]を選択して、実際のホストの IP アドレス 209.165.200.225 を入力します。



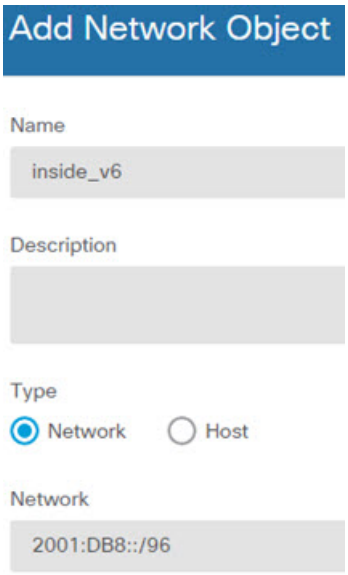
d) [追加（Add）][OK] をクリックします。

e) [+]をクリックして DNS サーバの実際のアドレスを定義します。
ネットワーク オブジェクトに名前を付け（dns_server など）、[ホスト（Host）]を選択して、ホスト アドレス 209.165.201.15 を入力します。



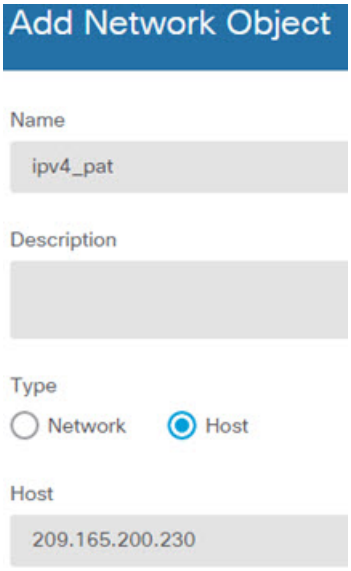
f) [追加（Add）][OK] をクリックします。

g) [+]をクリックして内部 IPv6 ネットワークを定義します。
ネットワーク オブジェクトに名前を付け（inside_v6 など）、[ネットワーク（Network）]を選択して、ネットワーク アドレス 2001:DB8::/96 を入力します。



h) [追加（Add）][OK] をクリックします。

i) [+]をクリックして内部 IPv6 ネットワークの IPv4 PAT アドレスを定義します。
ネットワーク オブジェクトに名前を付け（ipv4_pat など）、[ホスト（Host）]を選択して、ホスト アドレス 209.165.200.230 を入力します。



j) [追加（Add）][OK] をクリックします。

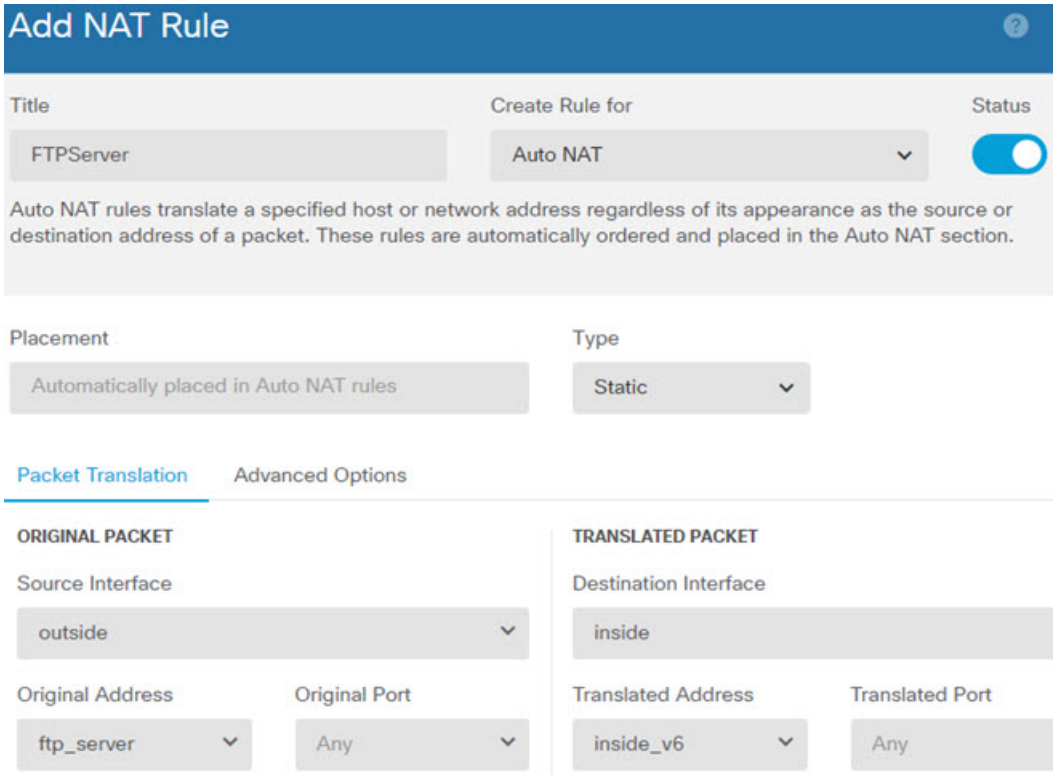
ステップ 2 FTP サーバのための、DNS 修正を設定したスタティック NAT ルールを設定します。

a) [ポリシー（Policies）] > [NAT] を選択します。

b) [+]ボタンをクリックします。

c) 次のプロパティを設定します。

- タイトル（Title）= FTPServer（または任意の別の名前）。
- ルールの作成先（Create Rule For）= Auto NAT。
- タイプ（Type）= Static。
- 送信元インターフェイス（Source Interface）= outside。
- 宛先インターフェイス（Destination Interface）= inside。
- 元のアドレス（Original Address）= ftp_server のネットワーク オブジェクト。
- 変換済みのアドレス（Translated Address）= inside_v6 のネットワーク オブジェクト。IPv4 アドレスを IPv6 アドレスに変換する場合、IPv4 組み込みアドレス方式が使用されているため、209.165.200.225 は IPv6 で対応する D1A5:C8E1 に変換され、ネットワーク プレフィックスが追加されて完全なアドレス 2001:DB8::D1A5:C8E1 となります。
- [詳細オプション（Advanced Options）]タブで、[このルールに一致する DNS 応答を変換する（Translate DNS replies that match this rule）] を選択します。

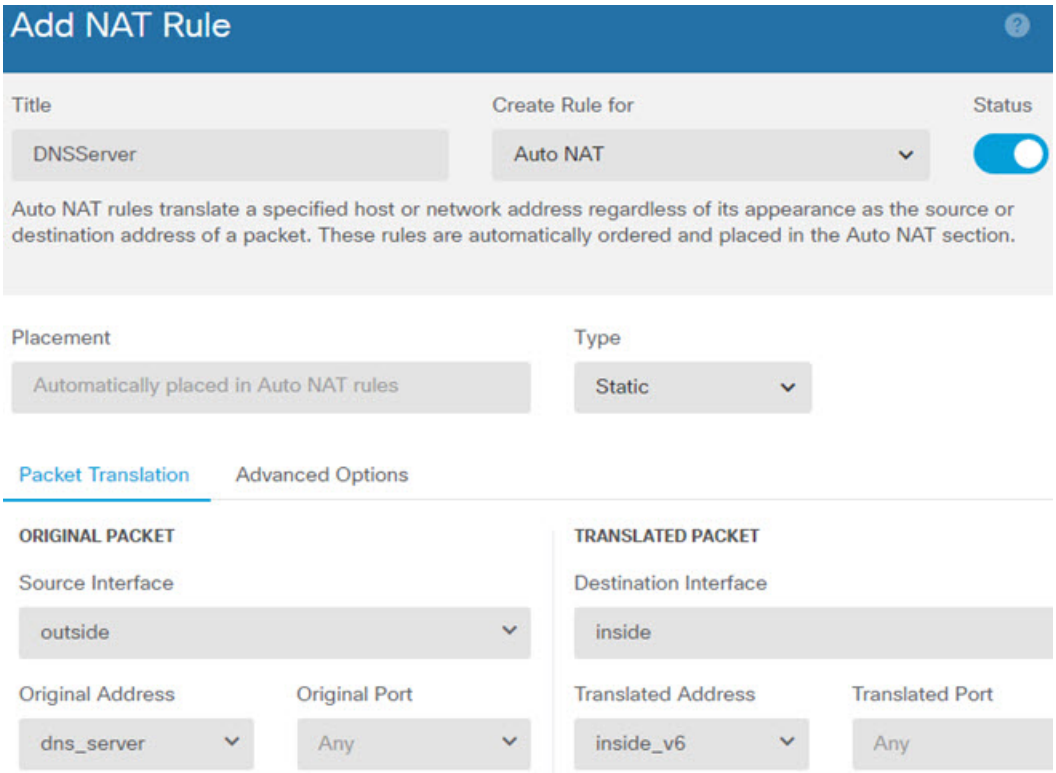


d) [OK]をクリックします。

ステップ 3 DNS サーバのためのスタティック NAT ルールを設定します。

a) [ポリシー（Policies）] > [NAT] を選択します。
b) [+]ボタンをクリックします。
c) 次のプロパティを設定します。

- タイトル（Title）= DNSServer（または任意の別の名前）。
- ルールの作成先（Create Rule For）= Auto NAT。
- タイプ（Type）= Static。
- 送信元インターフェイス（Source Interface）= outside。
- 宛先インターフェイス（Destination Interface）= inside。
- 元のアドレス（Original Address）= dns_server のネットワーク オブジェクト。
- 変換済みのアドレス（Translated Address）= inside_v6 のネットワーク オブジェクト。IPv4 アドレスを IPv6 アドレスに変換する場合、IPv4 組み込みアドレス方式が使用されているため、209.165.201.15 は IPv6 で対応する D1A5:C90F に変換され、ネットワーク プレフィックスが追加されて完全なアドレス 2001:DB8::D1A5:C90F となります。



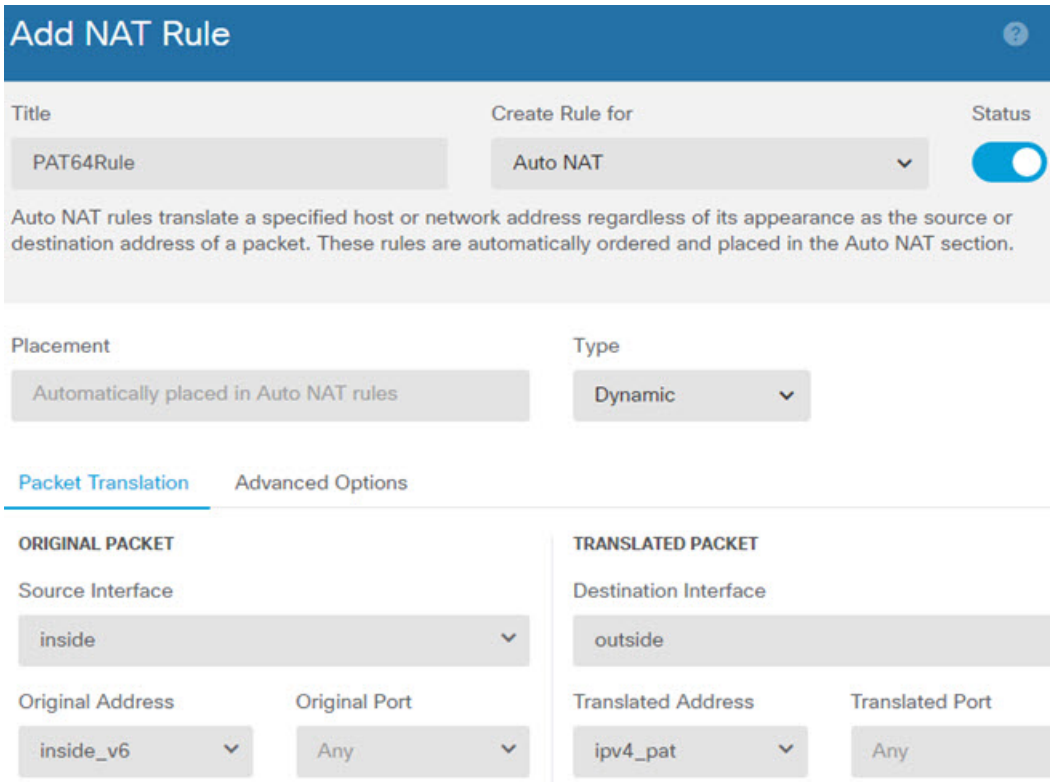
d) [OK]をクリックします。

ステップ 4 内部 IPv6 ネットワークのダイナミック PAT ルールを設定します。

a) [ポリシー（Policies）] > [NAT] を選択します。
b) [+]ボタンをクリックします。
c) 次のプロパティを設定します。

- タイトル（Title）= PAT64Rule（または任意の別の名前）。

- ルールの作成先（Create Rule For）= Auto NAT。
- タイプ（Type）= Dynamic。
- 送信元インターフェイス（Source Interface）= inside。
- 宛先インターフェイス（Destination Interface）= outside。
- 元のアドレス（Original Address）= inside_v6 のネットワーク オブジェクト。
- 変換済みのアドレス（Translated Address）= ipv4_pat のネットワーク オブジェクト。



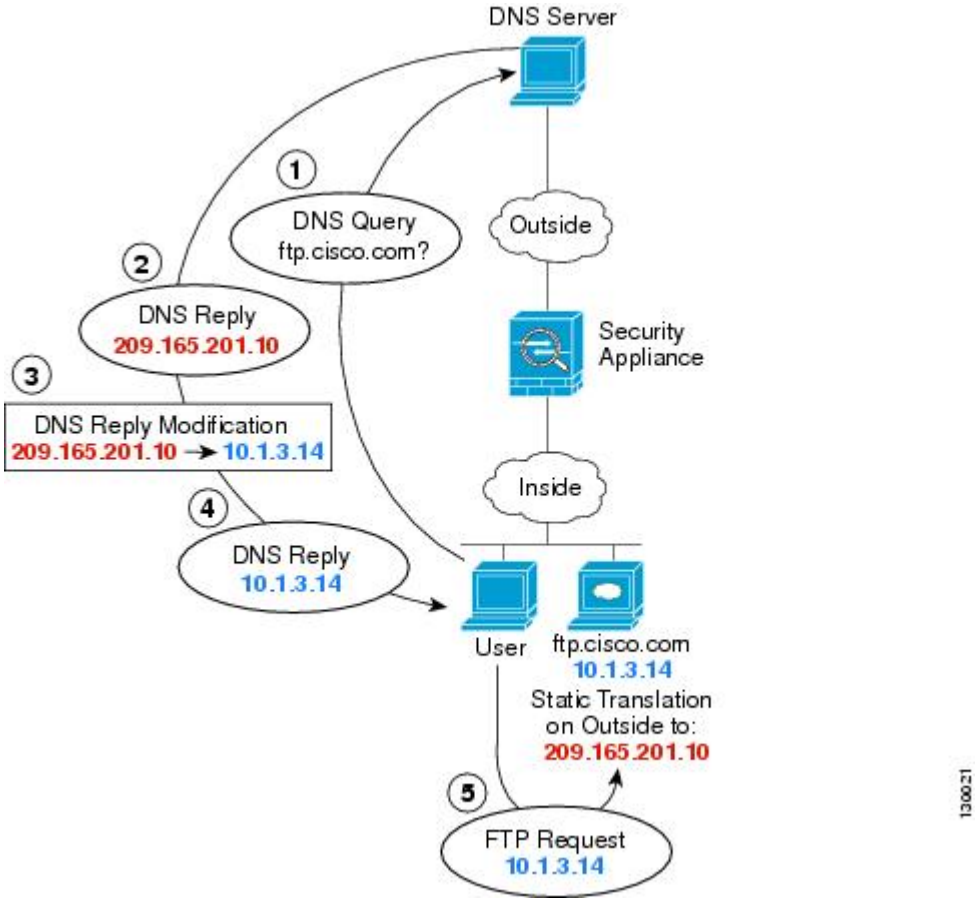
d) [OK]をクリックします。

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 応答修正を有効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 にトラフィックを送信することを試みます。

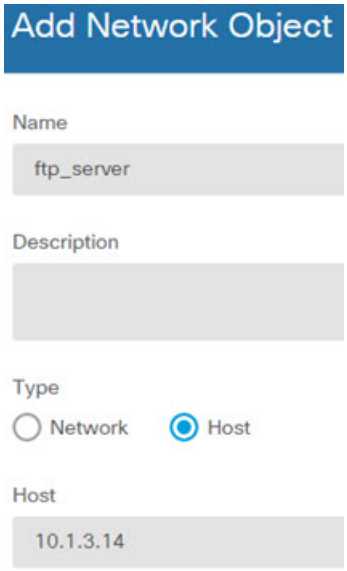


（注） この例では、内部インターフェイスがブリッジグループインターフェイス（BVI）ではなく、標準ルーテッド インターフェイスであると仮定します。内部インターフェイスが BVI である場合、各メンバー インターフェイスのルールを複製する必要があります。

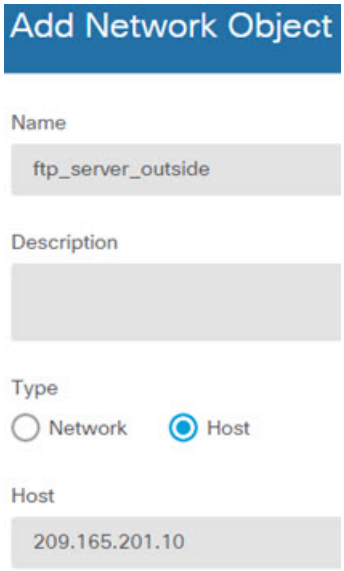
手順

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ます。

a) [オブジェクト（Objects）]を選択します。
b) 目次から [ネットワーク（Network）]を選択し、[+] をクリックします。
c) 実際の FTP サーバ アドレスを定義します。
ネットワーク オブジェクトに名前を付け（ftp_server など）、[ホスト（Host）]を選択して、実際のホストの IP アドレス 10.1.3.14 を入力します。



d) [追加（Add）][OK] をクリックします。
e) [+]をクリックして FTP サーバの変換済みアドレスを定義します。
ネットワーク オブジェクトに名前を付け（ftp_server_outside など）、[ホスト（Host）]を選択して、ホスト アドレス 209.165.201.10 を入力します。



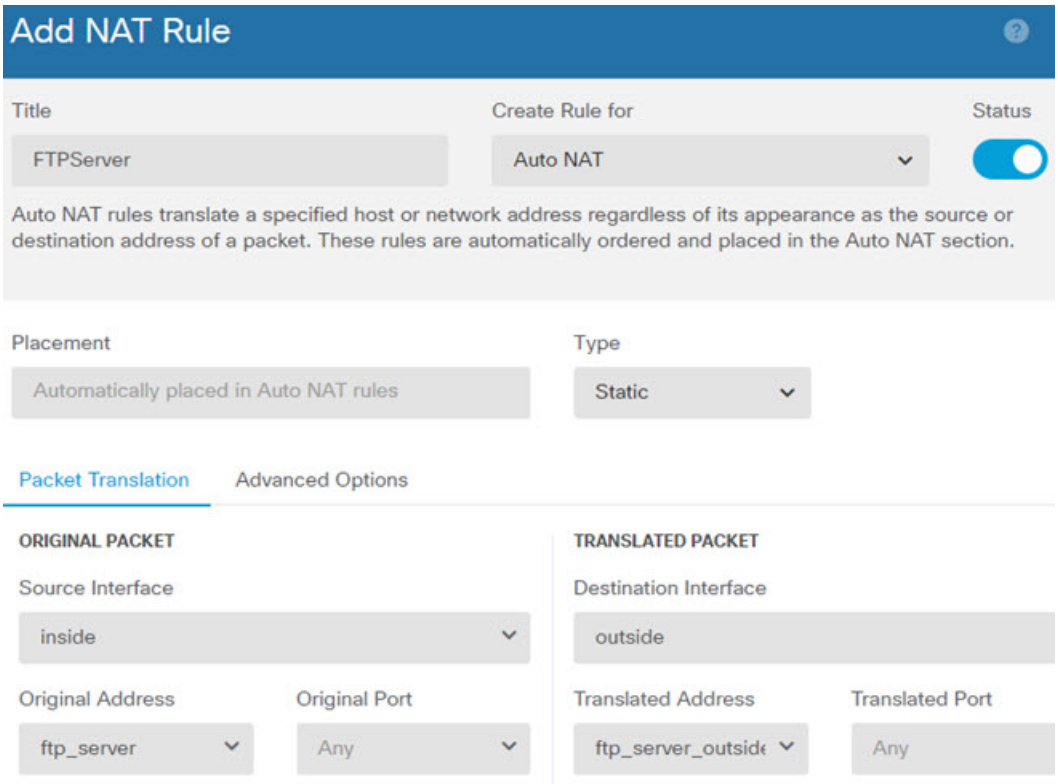
ステップ 2 FTP サーバのための、DNS 修正を設定したスタティック NAT ルールを設定します。

a) [ポリシー（Policies）] > [NAT] を選択します。

b) [+]ボタンをクリックします。

c) 次のプロパティを設定します。

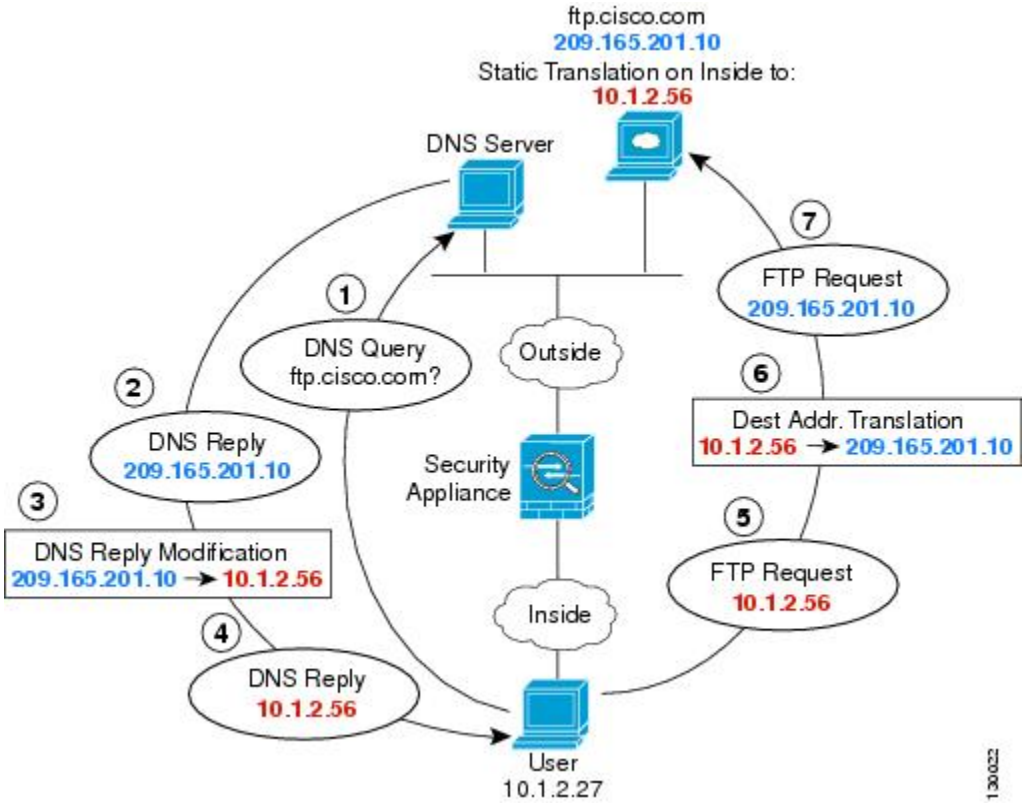
- タイトル（Title）= FTPServer（または任意の別の名前）。
- ルールの作成先（Create Rule For）= Auto NAT。
- タイプ（Type）= Static。
- 送信元インターフェイス（Source Interface）= inside。
- 宛先インターフェイス（Destination Interface）= outside。
- 元のアドレス（Original Address）= ftp_server のネットワーク オブジェクト。
- 変換済みのアドレス（Translated Address）= ftp_server_outside のネットワーク オブジェクト。
- [詳細オプション（Advanced Options）]タブで、[このルールに一致する DNS 応答を変換する（Translate DNS replies that match this rule）] を選択します。



d) [OK]をクリックします。

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。



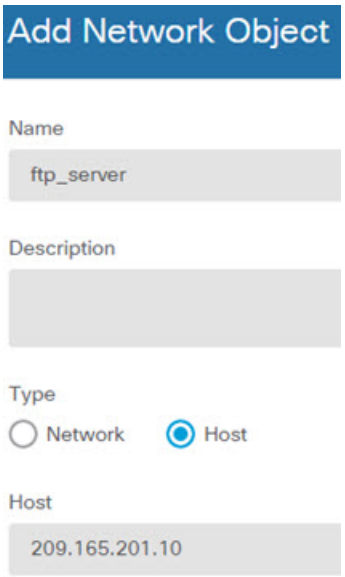
（注） この例では、内部インターフェイスがブリッジグループインターフェイス（BVI）ではなく、標準ルーテッド インターフェイスであると仮定します。内部インターフェイスが BVI である場合、各メンバー インターフェイスのルールを複製する必要があります。

手順

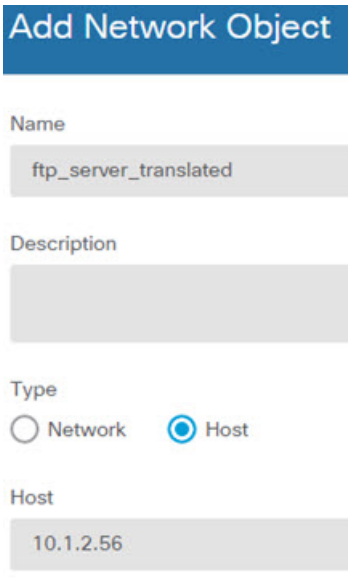
ステップ 1 FTP サーバのネットワーク オブジェクトを作成します。

a) [オブジェクト（Objects）]を選択します。

b) 目次から [ネットワーク（Network）]を選択し、[+] をクリックします。
c) 実際の FTP サーバ アドレスを定義します。
ネットワーク オブジェクトに名前を付け（ftp_server など）、[ホスト（Host）]を選択して、実際のホストの IP アドレス 209.165.201.10 を入力します。



d) [追加（Add）][OK] をクリックします。
e) [+]をクリックして FTP サーバの変換済みアドレスを定義します。
ネットワーク オブジェクトに名前を付け（ftp_server_translated など）、[ホスト（Host）]を選択して、ホスト アドレス 10.1.2.56 を入力します。



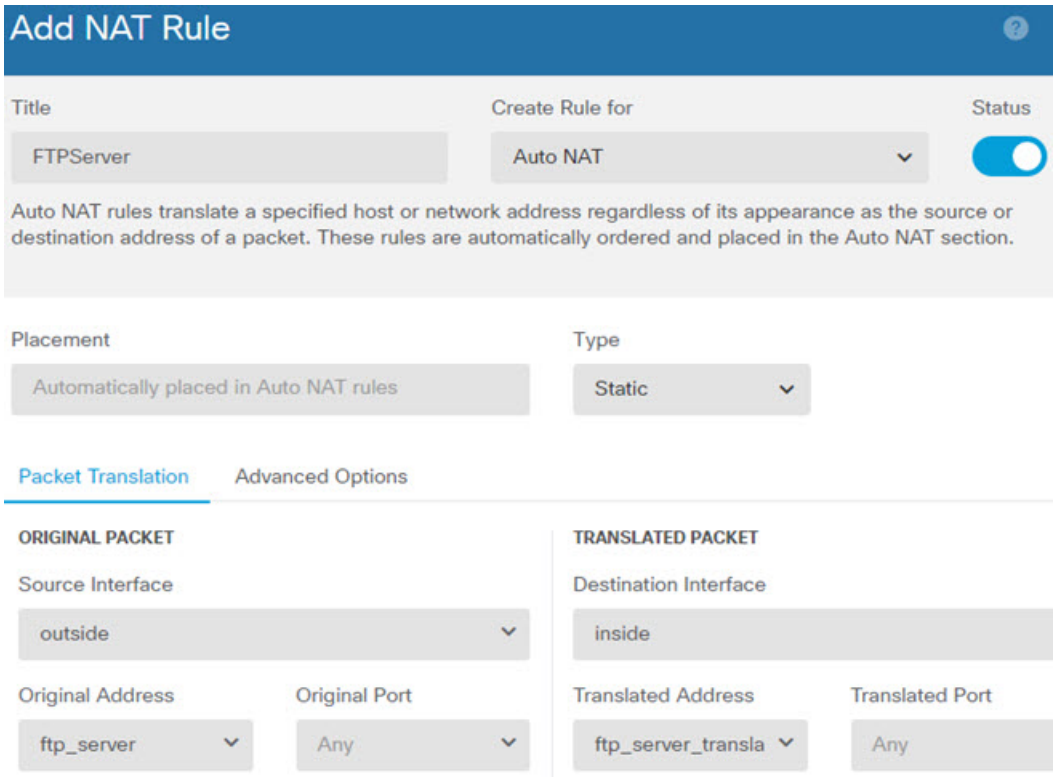
ステップ 2 FTP サーバのための、DNS 修正を設定したスタティック NAT ルールを設定します。

a) [ポリシー（Policies）] > [NAT] を選択します。

b) [+]ボタンをクリックします。

c) 次のプロパティを設定します。

- タイトル（Title）= FTPServer（または任意の別の名前）。
- ルールの作成先（Create Rule For）= Auto NAT。
- タイプ（Type）= Static。
- 送信元インターフェイス（Source Interface）= outside。
- 宛先インターフェイス（Destination Interface）= inside。
- 元のアドレス（Original Address）= ftp_server のネットワーク オブジェクト。
- 変換済みのアドレス（Translated Address）= ftp_server_translated のネットワーク オブジェクト。
- [詳細オプション（Advanced Options）]タブで、[このルールに一致する DNS 応答を変換する（Translate DNS replies that match this rule）] を選択します。



d) [OK]をクリックします。