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：IPv6 ネットワークを IPv4 ネットワークに 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 の基礎

ここでは、NAT の基礎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た任意のネットワークを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」ネットワークは、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） アドレスの変換時、デバイスのインターフェイス用に設定された 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、ルールは双方向です。このガイドでは、特定の接続が「宛先」アドレスから発生する場合でも、コマンドや説明に「送信元」および「宛先」が使用されるので注意してください。

NAT タイプ

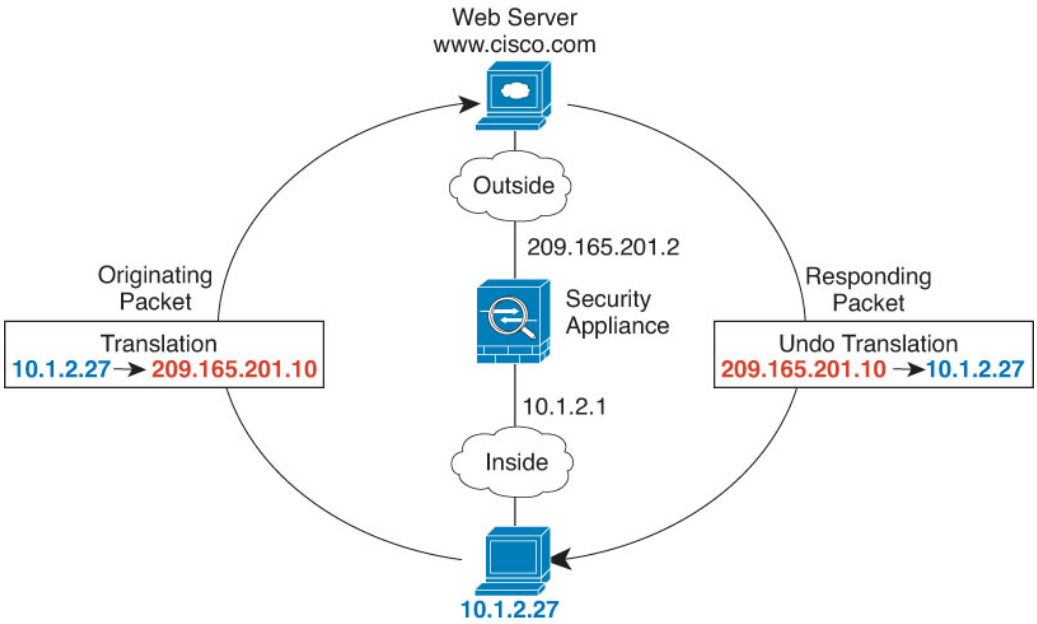
NAT は、次の方法を使用して実装できます。

- 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 （18 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。この時、この IP アドレスの一意の送信元ポートが使用されます。ダイナミック PAT （24 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 （30 ページ）を参照してください。
- アイデンティティ NAT：実際のアドレスがスタティックにそのアドレス自身に変換されます。基本的に NAT を回避します。大規模なアドレス グループは変換し、小さいアドレス グループは除外する場合、NAT をこの方法で設定します。「アイデンティティ NAT （40 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、Threat Defense デバイス がそのパケットを受信します。これは、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. 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 および 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* ルールとみなされます。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。ただし、これらのルールをグループ オブジェクトに対して作成できません。

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からオブジェクト定義内の NAT 設定は確認できません。

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ので、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と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、このガイド内で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 と 手動 NAT の比較

これら 2 つの NAT タイプの主な違いは、次のとおりです。

- 実際の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になります。ネットワーク オブジェクトの IP アドレスは元の（実際の）アドレスとして機能します。
  - 手動 NAT：実際のアドレスとマッピングアドレス両方の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 グループを識別します。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 コンフィギュレーションのパラメータです。実際のアドレスのネットワーク オブジェクト グループを使用できることは、手動 NAT がよりスケーラブルであることを意味します。
- 送信元および宛先 NAT の実装方法

- 自動 NAT：各ルールは、パケットの送信元または宛先のいずれかに適用できます。つまり、送信元 IP アドレスに 1 つ、宛先 IP アドレスに 1 つと、2 つのルールが使用されることがあります。これらの 2 つのルールを相互に結び付けて、送信先と宛先の組み合わせに特定の変換を適用することはできません。
- 手動 NAT：1 つのルールにより送信元と宛先の両方が変換されます。パケットは 1 つのルールにのみ一致し、それ以上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ない場合でも、マッチングするパケットは、1 つの 手動 NAT ルールだけに一致します。送信元および宛先は相互に結び付けられるので、送信元と宛先の組み合わせに応じて、異なる変換を適用できます。たとえば、sourceA/destinationA には、sourceA/destinationB とは異なる変換を設定できます。

- NAT ルールの順序
  - 自動 NAT：NAT テーブルで自動的に順序付けされます。
  - 手動 NAT：NAT テーブルで手動で順序付けします（自動 NAT ルールの前または後）。

NAT ルールの順序

自動 NAT 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。

（注） セクション 0 もあり、このセクションには、システムが使用するために作成される NAT ルールが含まれています。これらのルールは、他のすべてのルールよりも優先されます。これらのルールはシステムで自動的に作成され、必要に応じて xlate がクリアされます。セクション 0 では、ルールの追加、編集、または変更はできません。

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。 「固有のルールを前に」とは、次のことを意味します。 • 静的ルールは動的ルールの前に配置する必要があります。 • 宛先変換を含むルールは、送信元変換のみのルールの前に配置する必要があります。 送信元アドレスまたは宛先アドレスに基づいて複数のルールが適用される可能性がある重複するルールを排除できない場合は、これらの推奨事項に従うように特に注意してください。
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、次の順序の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、アドレス番号（低から高の順）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。

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 3	手動 NAT	まだ一致が見つからない場合、セクション3のルールは、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（ダイナミック）
- 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（ダイナミック）
- 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）

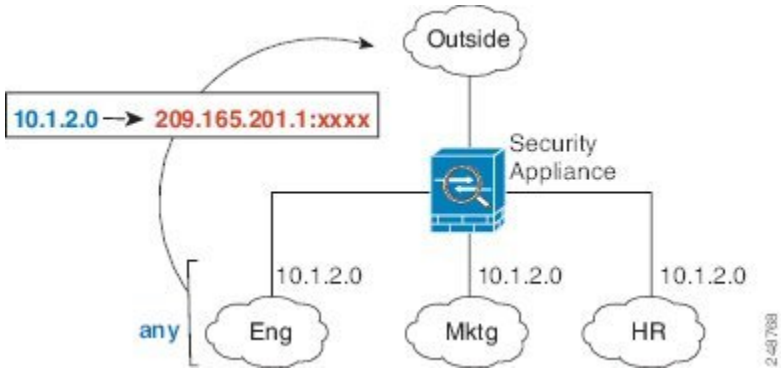
NAT インターフェイス

ブリッジ グループ メンバー インターフェイスを除き、NAT ルールを設定して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）に適用できます。または、特定の実際のインターフェイスおよびマッピング インターフェイスを識別できます。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外部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 メンバーの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場合、すべてのブリッジ グループ メンバー インターフェイスは除外されます。このため、NAT をブリッジ グループ メンバーに適用するには、メンバーインターフェイスを指定する必要があります。したがって、ただ 1 つのインターフェイスが異なるだけで多数の類似したルールができる可能性があります。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ませんが、メンバーのインターフェイスのみに NAT を設定することはできます。

パッシブ インターフェイスでは NAT を設定できません。

NAT 用のルーティングの設定

脅威に対する防御 デバイスは、変換された（マッピング）アドレスに送信されるパケットの宛先である必要があります。

パケットを送信する際、デバイスは宛先インターフェイスを使用するか（指定した場合）、またはルーティング テーブル ルックアップ（指定しない場合）を使用して、出力インターフェイスを決定します。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た場合でもルート ルックアップを使用することができます。

以下で説明するように、必要なルーティング設定はマッピングアドレスによって異なります。

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、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、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。このソリューションは、外部ネットワークに十分な数のフリーアドレスが含まれている場合に最も適しており、ダイナミック NAT またはスタティック NAT などの 1:1 変換を使用している場合は考慮が必要です。ダイナミック PAT ではアドレス数が少なくても使用できる変換の数が大幅に拡張されるので、外部ネットワークで使用できるアドレスが少ししかない場合

でも、この方法を使用できます。PAT では、マッピング インターフェイスの IP アドレスも使用できます。

固有のネットワーク上のアドレス

宛先（マッピングされた）インターフェイス ネットワークで使用可能なアドレスより多くのアドレスが必要な場合は、別のサブネット上のアドレスを識別できます。アップストリーム ルータには、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 は有効になっており、他の静的 NAT ルールと一致します。必要に応じてプロキシ ARP をディセーブルにできます。また、必要に応じて通常のスタティック NAT のプロキシ ARP をディセーブルにすることもできます。その場合には、アップストリーム ルータに適切なルートが確実に設定されていなくてはなりません。

アイデンティティ NAT の場合、通常はプロキシ ARP が不要で、場合によっては接続性に関する問題を引き起こす可能性があります。たとえば、「any」の IP アドレスに対して広範囲のアイデンティティ NAT ルールを設定した場合は、プロキシ ARP をイネーブルのままにしておくと、マッピング インターフェイスに直接接続されたネットワーク上のホストに問題が発生する可能性があります。この場合、マッピング ネットワークのホストが同じネットワークの他のホストと通信すると、ARP 要求内のアドレスは（任意のアドレスと一致する）NAT ルールと一致します。このとき、実際にはThreat Defense デバイス 向けのパケットでない場合でも、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 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 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 の実装に関する詳細なガイドラインについて説明します。

インターフェイス ガイドライン

NAT は標準の物理ルーテッド 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 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）の NAT の設定には次の制限があります。

- ブリッジ グループのメンバーの NAT を設定するときは、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 インターフェイス間で NAT を行う場合は、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」を指定することはできません。
- 宛先インターフェイスがブリッジグループ メンバーインターフェイスの場合は、インターフェイスにアタッチされている IP アドレスがないため、インターフェイス PAT を設定できません。
- 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、IPv4 と IPv6 ネットワーク（NAT64/46）の間での変換はできません。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 のみが使用可能な方式であり、ダイナミック PAT66 はサポートされていません。

IPv6 NAT ガイドライン

NAT では、次のガイドラインと制御事項に基づいて IPv6 をサポートしています。

- 標準ルーテッド モード インターフェイスの場合、IPv4 と IPv6 の間の変換も可能です。
- 同一ブリッジ グループのメンバーであるインターフェイスの IPv4 と IPv6 間の変換はできません。2 つの IPv6 または 2 つの IPv4 ネットワーク間でのみ変換できます。この制限は、ブリッジ グループのメンバーと標準的なルーテッド インターフェイスの間には該当しません。
- 同じブリッジ グループのインターフェイス間で変換するときは、IPv6 のダイナミック PAT（NAT66）を使用できません。この制限は、ブリッジ グループのメンバーと標準的なルーテッド インターフェイスの間には該当しません。
- 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 のベスト プラクティス

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ので、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 0 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。

検査対象プロトコルの NAT サポート

セカンダリ接続を開いたり、パケットに IP アドレスを埋め込んだりする、一部のアプリケーション層プロトコルは、次のサービスを提供するために検査されます。

- ピンホール作成：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 ポートのどちらかでセカンダリ TCP または UDP 接続を開きます。検査により、これらのセカンダリ ポートに対してピンホールが開かれるため、アクセス制御ルールを作成する必要はありません。
- NAT リライト：FTP などのプロトコルは、セカンダリ接続用の IP アドレスとポートをプロトコルの一部としてパケット データに埋め込みます。いずれかのエンドポイントに対して NAT 変換が含まれている場合、インスペクション エンジンはパケット データを書き換えて、埋め込まれたアドレスとポートの NAT 変換を反映させます。NAT リライトなしでは、セカンダリ接続は機能しません。
- プロトコル強制：一部の検査は、検査対象プロトコルの RFC に対して一定の準拠を強制します。

次の表は、NAT リライトが適用される検査対象プロトコルとそれらの NAT 制限を示します。これらのプロトコルを含む NAT ルールを作成する場合は、これらの制限に留意してください。ここに示されていない検査対象プロトコルには NAT リライトが適用されません。こうしたインスペクションには GTP、HTTP、IMAP、POP、SMTP、SSH および SSL があります。

（注） NAT リライトは示されているポートでのみサポートされます。これらのプロトコルを非標準ポートで使用する場合、接続で NAT を使用しないでください。

表 *2 : NAT* がサポートするアプリケーション インスペクション

アプリケーション	検査対象のプロトコル、ポート	NAT の制限	ピンホールの作成
DCERPC	TCP/135	NAT64 はサポートされません。	はい
直径	TCP/3868 TCP/5868（TCP/TLS の場合） SCTP/3868	NAT/PAT なし。	はい
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。	いいえ
ESMTP	TCP/25	NAT64 はサポートされません。	いいえ
FTP	TCP/21	制限なし。	○
GTP	UDP/3386 （GTPv0） UDP/2123（GTPv1+）	拡張 PAT はサポートされません。 NAT なし。	—
H.323 H.225（発呼信号） H.323 RAS	TCP/1720 UDP/1718 RAS の場合、UDP/1718 ～ 1719	NAT64 はサポートされません。	はい
ICMP ICMP Error	ICMP （デバイス インターフェイスに転送される ICMP トラフィックは検査されません）	制限なし。	いいえ
IP オプション	RSVP	NAT64 はサポートされません。	いいえ
M3UA	SCTP/2905	組み込みアドレス用の NAT または PAT なし。	—
NetBIOS Name Server over IP	UDP/137、138（送信元ポート）	NAT64 はサポートされません。	いいえ
RSH	TCP/514	PAT はサポートされません。 NAT64 はサポートされません。	○
RTSP	TCP/554 （HTTP クローキングは処理されません）	NAT64 はサポートされません。	○

アプリケーション	検査対象のプロトコル、ポート	NAT の制限	ピンホールの作成
SIP	TCP/5060 UDP/5060	拡張 PAT はサポートされません。 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 および 2）	TCP/1521	NAT64 はサポートされません。	○
SCTP	SCTP	SCTP トラフィックでスタティック ネットワーク オブジェクト NAT を実行できますが（ダイナミック NAT/PAT なし）、インスペクション エンジンは NAT には使用されません。	非対応
Sun RPC	TCP/111 UDP/111	NAT64 はサポートされません。	はい
TFTP	UDP/69	NAT64 はサポートされません。 ペイロード IP アドレスは変換されません。	はい
XDMCP	UDP/177	NAT64 はサポートされません。	対応

FQDN 宛先のガイドライン

IP アドレスの代わりに完全修飾ドメイン名（FQDN）ネットワークオブジェクトを使用して、手動 NAT ルールに変換済み（マッピング）宛先を指定できます。たとえば、www.example.com Web サーバを宛先とするトラフィックに基づいてルールを作成できます。

FQDN を使用すると、システムは DNS 解決を取得し、返されたアドレスに基づいて NAT ルールを書き込みます。DNS サーバから複数のアドレスを取得する場合、使用されるアドレスは次の情報に基づきます。

- 指定したインターフェイスと同じサブネット上にアドレスがある場合は、そのアドレスが使用されます。同じサブネットに存在しない場合は、最初に返されたアドレスが使用されます。
- 変換後の送信元と変換後の宛先の IP タイプは一致している必要があります。たとえば、変換後の送信元アドレスが IPv6 の場合、FQDN オブジェクトはアドレスタイプとして IPv6 を指定する必要があります。変換後の送信元が IPv4 の場合、FQDN オブジェクトはアドレスタイプとして IPv4 を指定する必要があります。変換後の送信元が IPv4 の場合、FQDN オブジェクトは IPv4 または IPv4 と IPv6 の両方を指定できます。この場合、IPv4 アドレスが選択されます。

手動 NAT 宛先に使用されるネットワークグループに FQDN オブジェクトを含めることはできません。NAT では、1 つの宛先ホストだけがこのタイプの NAT ルールに適しているため、FQDN オブジェクトは単独で使用する必要があります。

FQDN を IP アドレスに解決できない場合、DNS 解決が取得されるまでルールは機能しません。

NAT のガイドラインの補足

- ブリッジ グループ メンバーであるインターフェイスに対しては、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）自体には、 NAT ルールは作成できません
- サイト間 VPN で使用される仮想トンネルインターフェイス（VTI）の NAT ルールは作成できません。VTI の送信元インターフェイスのルールを作成すると、NAT は VPN トンネルに適用されません。VTI でトンネリングされた VPN トラフィックに適用される NAT ルールを作成するには、インターフェイスとして [任意（any）] を使用する必要があります。インターフェイス名を明示的に指定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。
- VPN がインターフェイスで定義されると、インターフェイスの着信 ESP トラフィックに NAT ルールは適用されません。システムでは、確立されている VPN トンネルの ESP トラフィックだけが許可され、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。この制約は ESP と UDP ポート 500 および 4500 に適用されます。
- ダイナミック PAT を適用しているデバイスの背後にあるデバイスでサイト間 VPN を定義する場合、UDP ポート 500 および 4500 は実際に使用されないため、PAT デバイス背後のデバイスから接続を開始する必要があります。正しいポート番号がわからないため、レスポンダはセキュリティ アソシエーション（SA）を開始できません。
- 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を使用できるようにするには、デバイス CLI で **clear xlate** コマンドを使用して変換テーブルを消去します。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。

  既存の接続（VPNトンネルなど）に適用する新しい NAT ルールを作成する場合は、**clear conn** を使用して接続を終了する必要があります。その後、接続を再確立しようとすると、NAT ルールが適用され、接続が正しく NAT 変換されます。

（注） ダイナミック NAT または PAT ルールを削除し、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、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** または **clear conn** コマンドを使用してクリアされるまで、新しいルールは使用されません。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。
- アドレスやサブネットの範囲内で明示的に指定するか暗黙的に指定するかにかかわらず、NAT で使用されるネットワークオブジェクトに 131,838 を超える IP アドレスを含めることはできません。アドレス空間をより狭い範囲に分割し、小さなオブジェクトに対して個別のルールを作成します。
- （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。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、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、送信元をインターフェイスの IPv4 アドレスにマッピングする場合、**any** は「任意の IPv4 トラフィック」を意味します。これは、マッピングされたインターフェイス アドレスが、宛先も IPv4 であることを暗示しているためです。
- 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 プールには、次のアドレスを含めることはできません。
  - 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 が有効な場合は、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 xlate 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。
- NAT ルールの送信元アドレスとリモートアクセス VPN アドレスプールの重複アドレスは使用できません。
- 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こともできます。
- NAT はトラフィックを介してのみ適用されます。システムによって生成されたトラフィックは、NAT の対象外です。

- ネットワークオブジェクトまたはグループの PAT プールには、大文字と小文字を組み合わせた名前を付けないでください。
- Protocol Independent Multicast（PIM）レジスタの内部ペイロードで NAT を使用することはできません。
- （手動 NAT）デュアル ISP インターフェイス セットアップ（ルーティング設定でサービス レベルアグリーメントを使用するプライマリインターフェイスとバックアップインターフェイス）の NAT ルールを作成する場合は、ルールで宛先基準を指定しないでください。プライマリインターフェイスのルールがバックアップインターフェイスのルールよりも前にあることを確認してください。これにより、デバイスは、プライマリ ISP が利用できない場合に、現在のルーティング状態に基づいて正しい NAT 宛先インターフェイスを選択できます。宛先オブジェクトを指定すると、NAT ルールは、指定しない場合には重複するルールのプライマリインターフェイスを常に選択します。
- インターフェイスに定義された NAT ルールと一致しないトラフィックについて ASP ドロップ理由 nat-no-xlate-to-pat-pool が示される場合は、影響を受けるトラフィックのアイデンティティ NAT ルールを設定して、トラフィックが変換されずに通過できるようにします。
- GRE トンネルエンドポイントの NAT を設定する場合は、エンドポイントでキープアライブを無効にする必要があります。無効にしないと、トンネルを確立できません。エンドポイントは、キープアライブを元のアドレスに送信します。
- DHCP と BOOTP はポート UDP/67 ～ 68 を共有します。BOOTP は廃止されているため、DHCP も実行している場合、BOOTP ポートの NAT ルールを作成するとポート割り当ての問題が発生する可能性があります。ネットワークセグメント間で DHCP 要求を送信する場合は、代わりに DHCP リレーを使用することを検討してください。

NAT の設定

ネットワーク アドレス変換は非常に複雑になることがあります。変換の問題が発生したり、トラブルシューティングが難しい状況にならないよう、ルールはできるだけ単純にすることを推奨します。NAT を実装する前に、慎重に計画を立てることが非常に重要です。以下の手順では、基本的なアプローチを説明します。

手順

ステップ 1 **[ポリシー（Policies）]** > **[NAT]** の順に選択します。

ステップ 2 必要となるルールのタイプを決定します。

作成できるルールには、ダイナミック NAT ルール、ダイナミック PAT ルール、スタティック NAT ルール、およびアイデンティティ NAT ルールがあります。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。

この 2 つの実装オプションの比較については、自動 NAT および 手動 NAT （4 ページ）を参照してください。

ステップ 4 以下の項で説明している手順に従ってルールを作成します。

- ダイナミック NAT （18 ページ）
- ダイナミック PAT （24 ページ）
- スタティック NAT （30 ページ）
- アイデンティティ NAT （40 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。

以下の操作によって、ポリシーとそのルールを管理できます。

- ルールを編集するには、対象の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、対象の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

ここでは、ダイナミック NAT とその設定方法について説明します。

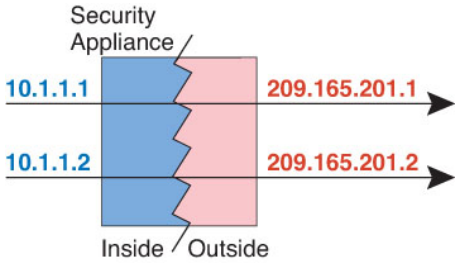
ダイナミック NAT について

ダイナミック NAT では、実際のアドレスのグループは、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変換されます。マッピングされたプールにあるアドレスは、通常、実際のグループより少なくなります。変換対象のホストが宛先ネットワークにアクセスすると、マッピングされたプールから IP アドレスが、NAT によって、そのホストに割り当てられます。変換は、実際のホストが接続を開始したときにだけ作成されます。変換は接続が継続している間だけ有効であり、変換がタイムアウトすると、そのユーザは同じ IP アドレスを保持しません。したがって、アクセス ルールでその接続が許可されている場合でも、宛先ネットワークのユーザは、ダイナミック NAT を使用するホストへの確実な接続を開始できません。

（注） 変換の実施中、アクセス ルールで許可されていれば、リモート ホストは変換済みホストへの接続を開始できます。アドレスは予測不可能であるため、ホストへの接続は確立されません。ただし、この場合は、アクセス ルールのセキュリティに依存できます。リモートホストからの接続が成功すると、接続のアイドルタイマーがリセットされます。

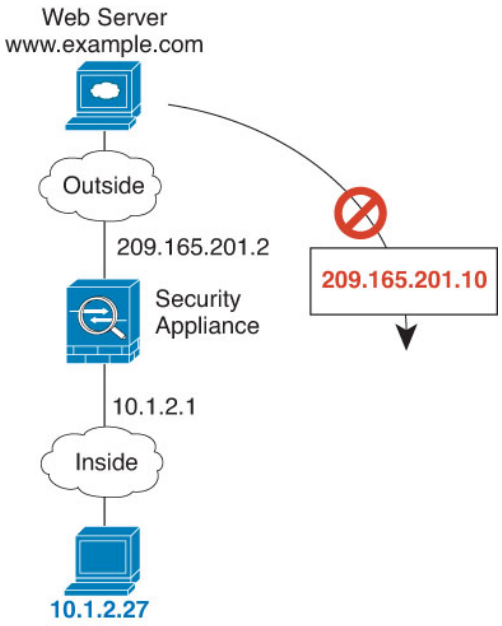
次の図に、一般的なダイナミック NAT のシナリオを示します。実際のホストだけが NAT セッションを作成でき、応答トラフィックが許可されます。

図 *3:* ダイナミック *NAT*



次の図に、マッピング アドレスへの接続開始を試みているリモート ホストを示します。このアドレスは、現時点では変換テーブルにないため、パケットはドロップされます。

図 *4:* マッピング アドレスへの接続開始を試みているリモート 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、次の欠点があります。

- マッピングされたプールにあるアドレスが実際のグループより少ない場合、予想以上にトラフィックが多いと、アドレスが不足する可能性があります。

  この事象が発生した場合には、PAT または PAT フォールバック方式を使用します。PAT では、単一アドレスのポートを使用して 64,000 を超える変換を処理できるためです。

- マッピング プールではルーティング可能なアドレスを多数使用する必要があるのに、ルーティング可能なアドレスは多数用意できない場合があります。

ダイナミック NAT の利点は、一部のプロトコルで PAT を使用できないことです。たとえば、PAT は以下において機能しません。

- GRE バージョン 0 などのように、オーバーロードするためのポートがない IP プロトコル。
- 1 つのポート上にデータ ストリームを持ち、別のポート上に制御パスを持つオープンスタンダードではないアプリケーション。

ダイナミック自動 NAT の設定

ダイナミック自動 NAT ルールを使用して、アドレスを宛先ネットワークでルーティング可能な別の IP アドレスに変換します。

始める前に

[オブジェクト（Objects）] を選択し、ルールで必要となるネットワーク オブジェクトまたはグループを作成します。または、NAT ルールを定義する際にオブジェクトを作成することもできます。作成するオブジェクトは、以下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）にする必要があります。ホスト、範囲、またはサブネットのいずれかを使用できます。
- [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。グループに IPv4 アドレスと IPv6 アドレスの両方を混在させることはできません。グループに含まれるタイプは 1 つだけにする必要があります。 グループに範囲とホスト IP アドレスの両方が含まれている場合、範囲はダイナミック NAT に使用され、ホスト IP アドレスは PAT のフォールバックとして使用されます。

手順

ステップ 1 **[ポリシー（Policies）]** > **[NAT]** の順に選択します。

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場合は、[+] ボタンをクリックします。
- 既存のルールを編集する場合は、対象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場合は、対象のルールのゴミ箱アイコンをクリックします）。

ステップ 3 以下の基本ルール 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（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 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 メンバー インターフェイスの場合は必須）この NAT ルールを適用するインターフェイス。[Source] は実際のインターフェイスで、このインターフェイスを経由してトラフィックはデバイスに入ります。[Destination] はマッピングされたインターフェイスで、このインターフェイスを経由してトラフィックはデバイスから出ます。デフォルトでは、ルールはブリッジ グループ メンバ インターフェイスを除くすべてのインターフェイス（[Any]）に適用されます。
- [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。
- [変換後のアドレス（Translated Address）]：マッピング アドレスが含まれるネットワーク オブジェクトまたはグループを指定します。

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、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（Translate DNS replies that match this rule）]：DNS 応答の IP アドレスを変換するかどうかを指定します。マッピングインターフェイスから実際のインターフェイスに移動する DNS 応答の場合、アドレス（IPv4 A または IPv6 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、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殊なときに使用され、NAT64/46 の変換で必要になる場合もあります。この場合、書き換えによって A レコードと AAAA レコードの変換も実行されます。詳細については、「NAT を使用した DNS クエリと応答の書き換え （87 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）]：他のマッピングアドレスがすでに割り当てられている場合、バックアップ手段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）を指定します。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した場合にのみ使用できます。

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

ダイナミック手動 NAT ルールは、自動 NAT ではニーズを満たさない場合に使用します。たとえば、宛先に応じて異なる変換を適用する必要がある場合などです。ダイナミック NAT は、アドレスを宛先ネットワークでルーティング可能な別の IP アドレスに変換します。

始める前に

[オブジェクト（Objects）] を選択し、ルールで必要となるネットワーク オブジェクトまたはグループを作成します。グループに IPv4 アドレスと IPv6 アドレスの両方を混在させることはできません。グループに含まれるタイプは 1 つだけにする必要があります。または、NAT ルールを定義する際にオブジェクトを作成することもできます。作成するオブジェクトは、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を指定できます。ホスト、範囲、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、この手順をスキップし、ルールで [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。グループに IPv4 アドレスと IPv6 アドレスの両方を混在させることはできません。グループに含まれるタイプは 1 つだけにする必要があります。 グループに範囲とホスト IP アドレスの両方が含まれている場合、範囲はダイナミック NAT に使用され、ホスト IP アドレスは PAT のフォールバックとして使用されます。

ルールで各アドレスのスタティック変換を設定すると、[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できます。

ダイナミック NAT では、宛先でポート変換を行うこともできます。オブジェクト マネージャで、[元の宛先アドレス（Original Destination Address）] および [変換後の宛先アドレス（Translated Destination Address）] 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。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]** の順に選択します。

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場合は、[+] ボタンをクリックします。
- 既存のルールを編集する場合は、対象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場合は、対象のルールのゴミ箱アイコンをクリックします）。

ステップ 3 以下の基本ルール 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）]：ルールを追加する場所です。ルールは、カテゴリ（自動 NAT ルールの前か後）、または選択したルールの上か下に挿入できます。
- [タイプ（Type）]：[ダイナミック（Dynamic）] を選択します。この設定が適用されるのは、送信元アドレスだけです。宛先アドレスの変換を定義すると、変換は常にスタティックなものになります。

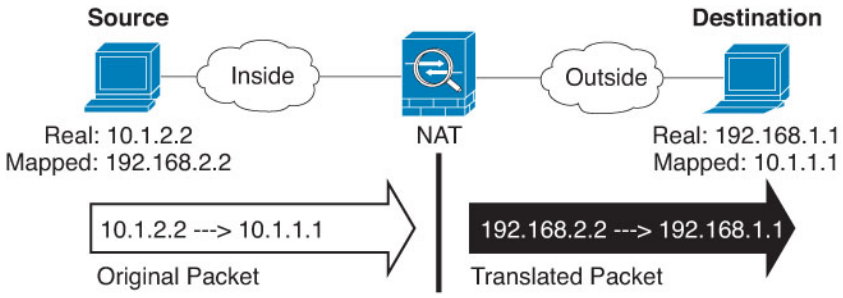
ステップ 4 次のインターフェイス オプションを設定します。

- [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 メンバー インターフェイスの場合は必須）この NAT ルールを適用するインターフェイス。[Source] は実際のインターフェイスで、このインターフェイスを経由してトラフィックはデバイスに入ります。[Destination] はマッピングされ

たインターフェイスで、このインターフェイスを経由してトラフィックはデバイスから出ます。デフォルトでは、ルールはブリッジ グループ メンバ インターフェイスを除くすべてのインターフェイス（[Any]）に適用されます。

ステップ 5 元のパケット アドレス（IPv4 または IPv6）、つまり、元のパケットに表示されるパケットアドレスを特定します。

元のパケットと変換されたパケットの例については、次の図を参照してください。



- [Original Source][Address]：変換するアドレスを含むネットワークオブジェクト、またはネットワークグループ。
- [Original Destination][Address]：（オプション）。宛先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、宛先に関係なく、送信元アドレス変換が適用されます。宛先アドレスを指定した場合、そ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 を使用できます。

  [インターフェイス（Interface）] の順に選択して、元の宛先を送信元インターフェイスに基づかせることもできます（この場合、[すべて（Any）]を指定することはできません）。このオプションを選択する場合、変換済みの宛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 に宛先アドレスのポート変換を実装するには、このオプションを選択し、さらにその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 変換後のパケットのアドレスが IPv4 または IPv6 のどちらであるかを識別します。つまり、宛先インターフェイス ネットワークで表されるパケット アドレスです。必要に応じて、IPv4 と IPv6 の間で変換できます。

- [変換後の送信元アドレス（Translated Source Address）]：マッピング アドレスが含まれるネットワーク オブジェクトまたはグループを指定します。
- [変換後の宛先アドレス（Translated Destination Address）]：（オプション）変換後の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を指定します。[元の宛先アドレス（Original Destination Address）] に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（つまり、変換なし）を設定します。

ステップ 7 （オプション）[元の宛先ポート（Original Destination Port）]、[変換後の宛先ポート（Translated Destination Port）] で、サービス変換の宛先サービス ポートを指定します。

ダイナミック NAT ではポート変換がサポートされないため、[元の送信元ポート（Original Source Port）] および [変換後の送信元ポート（Translated Source Port）] フィールドを空のまま

にします。ただし、宛先の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 だけ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、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（Translate DNS replies that match this rule）]：DNS 応答の IP アドレスを変換するかどうかを指定します。マッピングインターフェイスから実際のインターフェイスに移動する DNS 応答の場合、アドレス（IPv4 A または IPv6 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、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殊なときに使用され、NAT64/46 の変換で必要になる場合もあります。この場合、書き換えによって A レコードと AAAA レコードの変換も実行されます。詳細については、「NAT を使用した DNS クエリと応答の書き換え （87 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）]：他のマッピングアドレスがすでに割り当てられている場合、バックアップ手段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）を指定します。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した場合にのみ使用できます。

ステップ 9 **[OK]** をクリックします。

ダイナミック PAT

ここでは、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 では、実際のアドレスおよび送信元ポートが 1 つのマッピング アドレスおよび固有のポートに変換されることによって、複数の実際のアドレスが 1 つのマッピング IP アドレスに変換されます。

送信元ポートが接続ごとに異なるため、各接続には別の変換セッションが必要です。たとえば、10.1.1.1:1025 には、10.1.1.1:1026 とは別の変換が必要です。

次の図に、一般的なダイナミック PAT のシナリオを示します。実際のホストだけが NAT セッションを作成でき、応答トラフィックが許可されます。マッピングアドレスはどの変換でも同じですが、ポートがダイナミックに割り当てられます。

図 *5 :* ダイナミック *PAT*

変換が継続している間、アクセス ルールで許可されていれば、宛先ネットワーク上のリモート ホストは変換済みホストへの接続を開始できます。実際のポート アドレスおよびマッピング ポート アドレスはどちらも予測不可能であるため、ホストへの接続は確立されません。ただし、この場合は、アクセス ルールのセキュリティに依存できます。

接続の有効期限が切れると、ポート変換も有効期限切れになります。

（注） インターフェイスごとに異なる PAT プールを使用することをお勧めします。複数のインターフェイスに同じプールを使用する場合（特に「任意の」インターフェイスに使用する場合）は、プールが短時間で使い尽くされ、新しい変換に使用できるポートがなくなる可能性があります。

ダイナミック PAT の欠点と利点

ダイナミック PAT では、1 つのマッピング 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が節約されます。さらに、Threat Defense デバイス インターフェイスの IP アドレスを PAT アドレスとして使用できます。ただし、インターフェイス上の IPv6 アドレスに対しインターフェイス PAT を使用することはできません。

同じブリッジ グループのインターフェイス間で変換するときは、IPv6 のダイナミック PAT（NAT66）を使用できません。この制限は、ブリッジ グループのメンバーと標準的なルーテッド インターフェイスの間には該当しません。

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機能しません。詳細については、検査対象プロトコルの 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 によって、単一の IP アドレスから送信されたように見える数多くの接続が作成されることがあります。この場合、このトラフィックはサーバで DoS 攻撃として解釈される可能性があります。

ダイナミック自動 PAT の設定

ダイナミック自動 PAT ルールを使用して、アドレスを複数の IP アドレスだけに変換するのではなく、固有の IP アドレス/ポートの組み合わせに変換します。単一のアドレス（宛先インターフェイスのアドレスや別のアドレス）に変換できます。

始める前に

[オブジェクト（Objects）] を選択し、ルールで必要となるネットワーク オブジェクトまたはグループを作成します。または、NAT ルールを定義する際にオブジェクトを作成することもできます。作成するオブジェクトは、以下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）にする必要があります。ホスト、範囲、またはサブネットのいずれかを使用できます。
- [変換済みアドレス（Translated Address）]：PAT アドレスを指定するオプションは次のとおりです。
  - [接続先インターフェイス（Destination Interface）]：接続先インターフェイスの IPv4 アドレスを使用する場合、ネットワーク オブジェクトを作成する必要はありません。IPv6 にインターフェイス PAT を使用することはできません。
  - [単一 PAT アドレス（Single PAT address）]：単一のホストが含まれるネットワーク 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]** の順に選択します。

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場合は、[+] ボタンをクリックします。
- 既存のルールを編集する場合は、対象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場合は、対象のルールのゴミ箱アイコンをクリックします）。

ステップ 3 以下の基本ルール 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（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 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 メンバー インターフェイスの場合は必須）この NAT ルールを適用するインターフェイス。[Source] は実際のインターフェイスで、このインターフェイスを経由してトラフィックはデバイスに入ります。[Destination] はマッピングされたインターフェイスで、このインターフェイスを経由してトラフィックはデバイスから出ます。デフォルトでは、ルールはブリッジ グループ メンバ インターフェイスを除くすべてのインターフェイス（[Any]）に適用されます。
- [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。
- [変換後のアドレス（Translated Address）]：以下のいずれかを選択します。

- （インターフェイス PAT）。接続先インターフェイスの IPv4 アドレスを使用する場合は、[インターフェイス（Interface）] を選択します。この場合、特定の接続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。IPv6 にインターフェイス PAT を使用することはできません。
- 接続先インターフェイスアドレス以外の単一アドレスを使用するには、この目的で作成したホスト 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、目的の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（Fallthrough to Interface PAT）]（宛先インターフェイス）：他のマッピングアドレスがすでに割り当てられている場合、バックアップ手段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）を指定します。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した場合にのみ使用できます。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 ネットワークで使用することもできません。

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

ダイナミック手動 PAT ルールは、自動 PAT ではニーズを満たさない場合に使用します。たとえば、宛先に応じて異なる変換を適用する必要がある場合などです。ダイナミック PAT は、アドレスを複数の IP アドレスだけに変換するのではなく、固有の IP アドレス/ポートの組み合わせに変換します。単一のアドレス（宛先インターフェイスのアドレスや別のアドレス）に変換できます。

始める前に

[オブジェクト（Objects）] を選択し、ルールで必要となるネットワーク オブジェクトまたはグループを作成します。グループに IPv4 アドレスと IPv6 アドレスの両方を混在させることはできません。グループに含まれるタイプは 1 つだけにする必要があります。または、NAT ルールを定義する際にオブジェクトを作成することもできます。作成するオブジェクトは、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を指定できます。ホスト、範囲、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、この手順をスキップし、ルールで [すべて（Any）] を指定します。
- [変換後の送信元アドレス（Translated Source Address）]：PAT アドレスを指定する、以下のオプションがあります。

- [接続先インターフェイス（Destination Interface）]：接続先インターフェイスの IPv4 アドレスを使用する場合、ネットワーク オブジェクトを作成する必要はありません。IPv6 にインターフェイス PAT を使用することはできません。
- [単一 PAT アドレス（Single PAT address）]：単一のホストが含まれるネットワーク オブジェクトを作成します。

ルールで [元の宛先アドレス（Original Destination Address）] と [変換後の宛先アドレス（Translated Destination Address）] にスタティック変換を設定する場合は、これらのアドレスにおいてネットワーク 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 では、宛先でポート変換を行うこともできます。オブジェクト マネージャで、[元の宛先アドレス（Original Destination Address）] および [変換後の宛先アドレス（Translated Destination Address）] 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。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]** の順に選択します。

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場合は、[+] ボタンをクリックします。
- 既存のルールを編集する場合は、対象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場合は、対象のルールのゴミ箱アイコンをクリックします）。

ステップ 3 以下の基本ルール オプションを設定します。

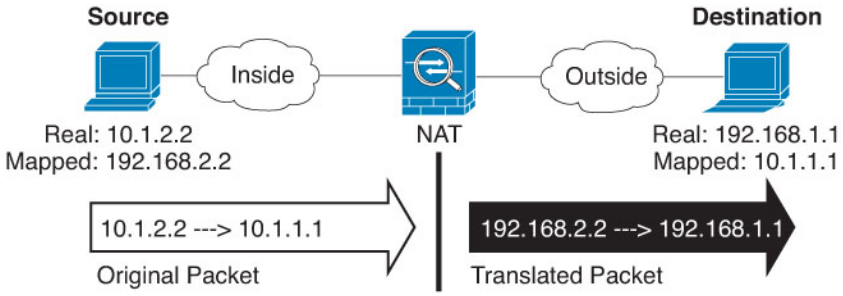
- [タイトル（Title）]：ルールの名前を入力します。
- [ルールの作成対象（Create Rule For）]：[手動 NAT（Manual NAT）] を選択します。
- [ルールの配置（Rule Placement）]：ルールを追加する場所です。ルールは、カテゴリ（自動 NAT ルールの前か後）、または選択したルールの上か下に挿入できます。
- [タイプ（Type）]：[ダイナミック（Dynamic）] を選択します。この設定が適用されるのは、送信元アドレスだけです。宛先アドレスの変換を定義すると、変換は常にスタティックなものになります。

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 メンバー インターフェイスの場合は必須）この NAT ルールを適用するインターフェイス。[Source] は実際のインターフェイスで、このインターフェイスを経由してトラフィックはデバイスに入ります。[Destination] はマッピングされたインターフェイスで、このインターフェイスを経由してトラフィックはデバイスから出ます。デフォルトでは、ルールはブリッジ グループ メンバ インターフェイスを除くすべてのインターフェイス（[Any]）に適用されます。

ステップ 5 元のパケット アドレス（IPv4 または IPv6）、つまり、元のパケットに表示されるパケットアドレスを特定します。

元のパケットと変換されたパケットの例については、次の図を参照してください。



- [Original Source][Address]：変換するアドレスを含むネットワークオブジェクト、またはネットワークグループ。
- [Original Destination][Address]：（オプション）。宛先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、宛先に関係なく、送信元アドレス変換が適用されます。宛先アドレスを指定した場合、そ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 を使用できます。

  [インターフェイス（Interface）] の順に選択して、元の宛先を送信元インターフェイスに基づかせることもできます（この場合、[すべて（Any）]を指定することはできません）。このオプションを選択する場合、変換済みの宛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 に宛先アドレスのポート変換を実装するには、このオプションを選択し、さらにその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 変換後のパケットのアドレスが IPv4 または IPv6 のどちらであるかを識別します。つまり、宛先インターフェイス ネットワークで表されるパケット アドレスです。必要に応じて、IPv4 と IPv6 の間で変換できます。

- **[変換後の送信元アドレス（Translated Source Address）]**：以下のいずれかを選択します。
  - （インターフェイス PAT）。接続先インターフェイスの IPv4 アドレスを使用する場合は、[インターフェイス（Interface）] を選択します。この場合、特定の接続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。IPv6 にインターフェイス PAT を使用することはできません。
  - 接続先インターフェイスアドレス以外の単一アドレスを使用するには、この目的で作成したホスト ネットワーク オブジェクトを選択します。
- [変換後の宛先アドレス（Translated Destination Address）]：（オプション）変換後の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を指定します。[変換前の宛先（Original Destination）] に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（つまり、変換なし）を設定します。

ステップ 7 （オプション）[元の宛先ポート（Original Destination Port）]、[変換後の宛先ポート（Translated Destination Port）] で、サービス変換の宛先サービス ポートを指定します。

ダイナミック NAT ではポート変換がサポートされないため、[元の送信元ポート（Original Source Port）] および [変換後の送信元ポート（Translated Source Port）] フィールドを空のままにします。ただし、宛先の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 だけ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、目的の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（Fallthrough to Interface PAT）]（宛先インターフェイス）：他のマッピングアドレスがすでに割り当てられている場合、バックアップ手段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）を指定します。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した場合にのみ使用できます。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 ネットワークで使用することもできません。

ステップ 9 **[OK]** をクリックします。

スタティック NAT

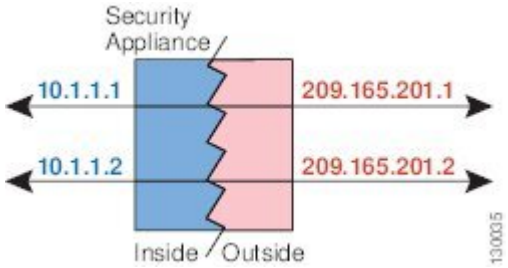
ここでは、スタティック NAT の概要およびその実装方法について説明します。

スタティック NAT について

スタティック NAT では、実際のアドレスからマッピング アドレスへの固定変換が作成されます。マッピング アドレスは連続する各接続で同じなので、スタティック NAT では、双方向の接続（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（接続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 では、各ホストが後続の変換に対して異なるアドレスまたはポートを使用するので、双方向の接続は開始できません。

次の図に、一般的なスタティック NAT のシナリオを示します。この変換は常にアクティブなので、実際のホストとリモート ホストの両方が接続を開始できます。

図 *6*：スタティック *NAT*



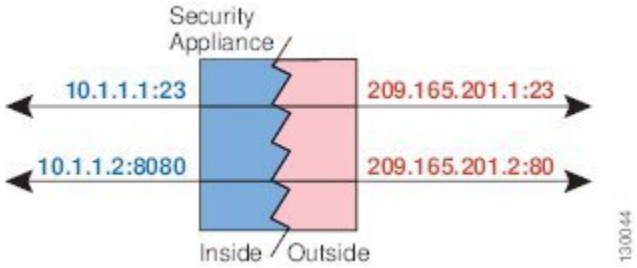
ポート変換を設定したスタティック NAT

ポート変換を設定したスタティック NAT では、実際のプロトコルとマッピング 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なので、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



ポート変換ルールを設定したスタティック NAT は、指定されたポートの宛先 IP アドレスのみにアクセスを制限します。NAT ルールの対象となっていない別のポートの宛先 IP アドレスにアクセスしようとすると、接続がブロックされます。さらに、手動 NAT の場合、NAT ルールの送信元 IP アドレスと一致しないトラフィックは、宛先ポートに関係なく、宛先 IP アドレスと一致するとドロップされます。そのため、宛先 IP アドレスに対して許可される他のすべてのトラフィックに関してルールを追加する必要があります。たとえば、ポートを指定しないで IP アドレスのスタティック NAT ルールを設定し、それをポート変換ルールの後に配置することができます。

（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。

次は、ポート変換を使用するスタティック NAT のその他の使用例です。

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（FTP、HTTP、および SMTP など）でサービスを提供する、3 つの独立したサーバがある場合、外部ユーザに単一の IP アドレスを付与してこれらのサービスにアクセスできるようにすることができます。次に、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 を設定して、単一の外部 IP アドレスを実際のサーバの正しい IP アドレスに、アクセスしようとしているポートに基づいてマッピングします。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

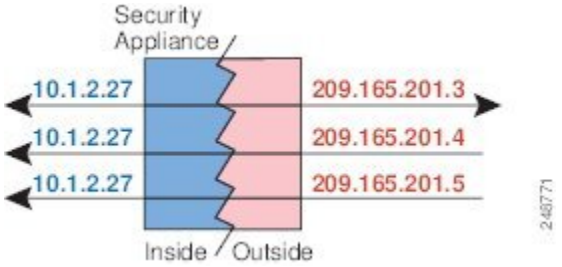
スタティック NAT は、実際のアドレスをインターフェイス アドレスとポートの組み合わせにマッピングするように設定できます。たとえば、デバイスの外部インターフェイスへの Telnet アクセスを内部ホストにリダイレクトする場合、内部ホストの IP アドレス/ポート 23 を外部インターフェイス アドレス/ポート 23 にマッピングできます。

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。

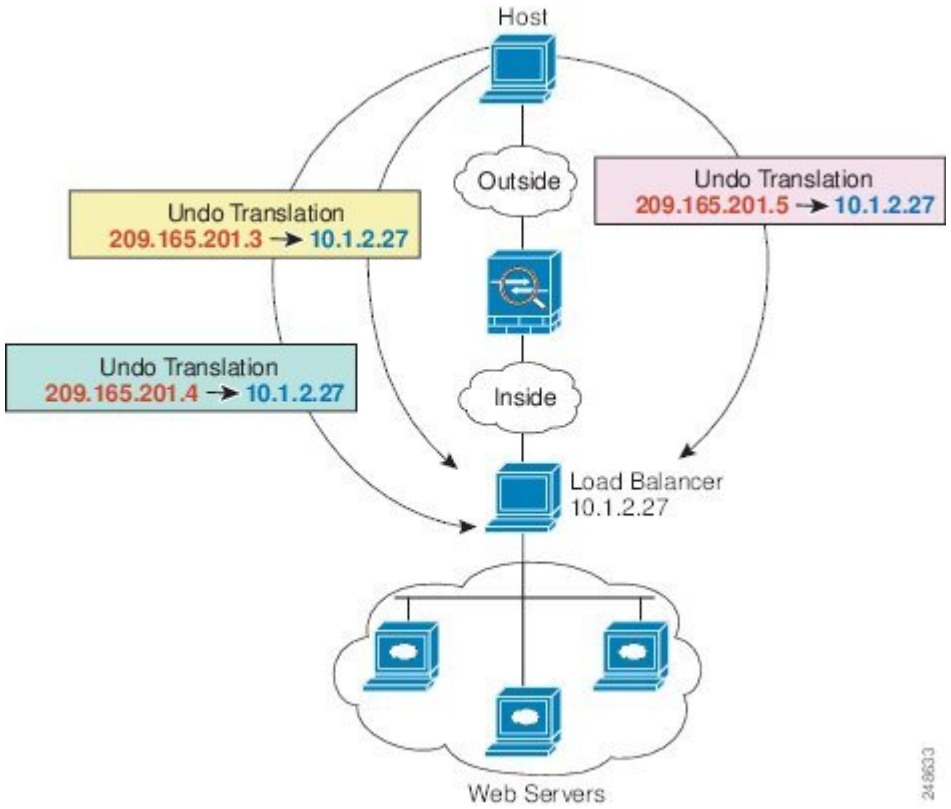
次の図に、一般的な 1 対多のスタティック NAT シナリオを示します。実際のホストが開始すると、常に最初のマッピング アドレスが使用されるため、実際のホスト IP/最初のマッピング IP の変換は、理論的には双方向変換のみが行われます。

図 *8 :* 一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:* 一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。その他のマッピング 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 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す。後続のマッピングでは、実際のホストへのトラフィックは開始できますが、実際のホストからのすべてのトラフィックは、送信元として最初にマッピングされたアドレスだけを使用します。

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は開始できません。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、アドレスの競合が起こるため（5 タプルが一意でない）、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

スタティック自動 NAT ルールを使用して、アドレスを宛先ネットワークでルーティング可能な別の IP アドレスに変換します。また、スタティック NAT ルールではポート変換を行うこともできます。

始める前に

[オブジェクト（Objects）] を選択し、ルールで必要となるネットワーク オブジェクトまたはグループを作成します。または、NAT ルールを定義する際にオブジェクトを作成することもできます。作成するオブジェクトは、以下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）にする必要があります。ホスト、範囲、またはサブネットのいずれかを使用できます。
- [変換済みアドレス（Translated Address）]：変換済みアドレスを指定するには、次のオプションがあります。
  - [接続先インターフェイス（Destination Interface）]：接続先インターフェイスの IPv4 アドレスを使用する場合、ネットワーク オブジェクトを作成する必要はありません。このオプションでは、ポート変換を適用するスタティック インターフェイス NAT を設定します。送信元アドレス/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 にインターフェイス PAT は使用できません。
  - [アドレス（Address）]：ホスト、範囲、またはサブネットが含まれるネットワーク オブジェクトまたはグループを作成します。グループに IPv4 アドレスと IPv6 アドレスの両方を混在させることはできません。グループに含まれるタイプは 1 つだけにする必要があります。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]** の順に選択します。

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場合は、[+] ボタンをクリックします。
- 既存のルールを編集する場合は、対象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場合は、対象のルールのゴミ箱アイコンをクリックします）。

ステップ 3 以下の基本ルール 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（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 メンバー インターフェイスの場合は必須）この NAT ルールを適用するインターフェイス。[Source] は実際のインターフェイスで、このインターフェイスを経由してトラフィックはデバイスに入ります。[Destination] はマッピングされたインターフェイスで、このインターフェイスを経由してトラフィックはデバイスから出ます。デフォルトでは、ルールはブリッジ グループ メンバ インターフェイスを除くすべてのインターフェイス（[Any]）に適用されます。
- [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。
- [変換後のアドレス（Translated Address）]：以下のいずれかを選択します。
  - 複数のアドレスが含まれるグループを使用するには、マッピング アドレスが含まれるネットワーク 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。
  - （ポート変換を適用するスタティック インターフェイス NAT の場合）接続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。この場合、特定の接続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。IPv6 にインターフェイス PAT は使用できません。これはポート変換と共に、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/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、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、同じプロトコルを対象としたものでなければなりません。オブジェクトが存在しない場合は、[新しいオブジェクトの作成（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 に変換することができます。

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（Translate DNS replies that match this rule）]：DNS 応答の IP アドレスを変換するかどうかを指定します。マッピング インターフェイスから実際のインターフェイスに移動する DNS 応答の場合、アドレス（IPv4 A または IPv6 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、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殊なときに使用され、NAT64/46 の変換で必要になる場合もあります。この場合、書き換えによって A レコードと AAAA レコードの変換も実行されます。詳細については、「NAT を使用した DNS クエリと応答の書き換え （87 ページ）」を参照してください。 このオプションはポート変換を行う場合は使用できません。
- [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）]：マッピング IP アドレスへの着信パケットのプロキシ ARP を無効にします。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で、

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 を無効にすることもできます。その場合、アップストリーム ルータに適切なルートが確実に設定されていなくてはなりません。アイデンティティ NAT の場合、通常はプロキシ ARP が不要で、場合によっては接続性に関する問題を引き起こす可能性があります。

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

スタティック手動 NAT ルールは、自動 NAT ではニーズを満たさない場合に使用します。たとえば、宛先に応じて異なる変換を適用する必要がある場合などです。スタティック NAT ルールを使用して、アドレスを宛先ネットワークでルーティング可能な別の IP アドレスに変換します。また、スタティック NAT ルールではポート変換を行うこともできます。

始める前に

[オブジェクト（Objects）] を選択し、ルールで必要となるネットワーク オブジェクトまたはグループを作成します。グループに IPv4 アドレスと IPv6 アドレスの両方を混在させることはできません。グループに含まれるタイプは 1 つだけにする必要があります。または、NAT ルールを定義する際にオブジェクトを作成することもできます。作成するオブジェクトは、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を指定できます。ホスト、範囲、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、この手順をスキップし、ルールで [すべて（Any）] を指定します。
- [変換後の送信元アドレス（Translated Source Address）]：変換後のアドレスを指定する、以下のオプションがあります。
  - [接続先インターフェイス（Destination Interface）]：接続先インターフェイスの IPv4 アドレスを使用する場合、ネットワーク オブジェクトを作成する必要はありません。このオプションでは、ポート変換を適用するスタティック インターフェイス NAT を設定します。送信元アドレス/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 にインターフェイス PAT は使用できません。
  - [アドレス（Address）]：ホスト、範囲、またはサブネットが含まれるネットワーク オブジェクトまたはグループを作成します。グループに IPv4 アドレスと IPv6 アドレスの両方を混在させることはできません。グループに含まれるタイプは 1 つだけにする必要があります。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。

スタティック変換をこれらのアドレスに対してルールで設定する場合は、[元の宛先アドレス（Original Destination Address）] と [変換後の宛先アドレス（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。ポート変換のみを適用する宛先スタ

ティック インターフェイス NAT を設定する場合は、宛先マッピング アドレスのオブジェクトを追加せずに、インターフェイスをルールに指定できます。

送信元、宛先、またはその両方でポート変換を実行することもできます。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]** の順に選択します。

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場合は、[+] ボタンをクリックします。
- 既存のルールを編集する場合は、対象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場合は、対象のルールのゴミ箱アイコンをクリックします）。

ステップ 3 以下の基本ルール オプションを設定します。

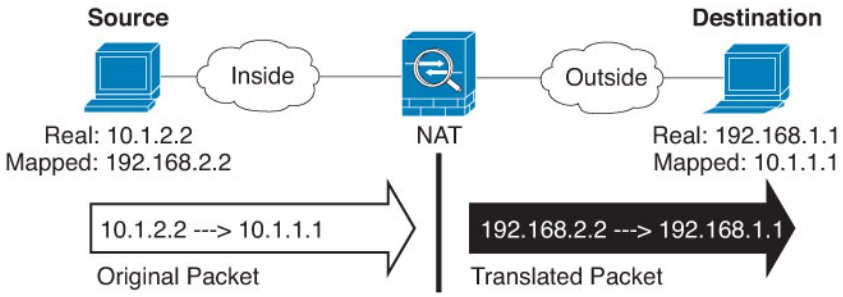
- [タイトル（Title）]：ルールの名前を入力します。
- [ルールの作成対象（Create Rule For）]：[手動 NAT（Manual NAT）] を選択します。
- [ルールの配置（Rule Placement）]：ルールを追加する場所です。ルールは、カテゴリ（自動 NAT ルールの前か後）、または選択したルールの上か下に挿入できます。
- [タイプ（Type）]：[スタティック（Static）]を選択します。この設定が適用されるのは、送信元アドレスだけです。宛先アドレスの変換を定義すると、変換は常にスタティックなものになります。

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 メンバー インターフェイスの場合は必須）この NAT ルールを適用するインターフェイス。[Source]は実際のインターフェイスで、このインターフェイスを経由してトラフィックはデバイスに入ります。[Destination] はマッピングされたインターフェイスで、このインターフェイスを経由してトラフィックはデバイスから出ます。デフォルトでは、ルールはブリッジ グループ メンバ インターフェイスを除くすべてのインターフェイス（[Any]）に適用されます。

ステップ 5 元のパケット アドレス（IPv4 または IPv6）、つまり、元のパケットに表示されるパケットアドレスを特定します。

元のパケットと変換されたパケットの例については、次の図を参照してください。



- [Original Source][Address]：変換するアドレスを含むネットワークオブジェクト、またはネットワークグループ。
- [Original Destination][Address]：（オプション）。宛先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、宛先に関係なく、送信元アドレス変換が適用されます。宛先アドレスを指定した場合、そ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 を使用できます。

  [インターフェイス（Interface）] の順に選択して、元の宛先を送信元インターフェイスに基づかせることもできます（この場合、[すべて（Any）]を指定することはできません）。このオプションを選択する場合、変換済みの宛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 に宛先アドレスのポート変換を実装するには、このオプションを選択し、さらにその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 変換後のパケットのアドレスが IPv4 または IPv6 のどちらであるかを識別します。つまり、宛先インターフェイス ネットワークで表されるパケット アドレスです。必要に応じて、IPv4 と IPv6 の間で変換できます。

- **[変換後の送信元アドレス（Translated Source Address）]**：以下のいずれかを選択します。
  - 複数のアドレスが含まれるグループを使用するには、マッピング アドレスが含まれるネットワーク 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。
  - （ポート変換を適用するスタティック インターフェイス NAT の場合）接続先インターフェイスの IPv4 アドレスを使用する場合は、[インターフェイス（Interface）] を選択します。この場合、特定の接続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。これはポート変換と共に、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/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 にインターフェイス PAT を使用することはできません。
- [変換後の宛先アドレス（Translated Destination Address）]：（オプション）変換後の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を指定します。[変換前の宛先（Original Destination）] に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（つまり、変換なし）を設定します。

ステップ 7 （任意）サービス変換の送信元または宛先サービスのポートを特定します。

ポート変換を適用するスタティック NAT を設定している場合、送信元、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 の間での変換が可能です。

NAT では、TCP または UDP だけ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（Translate DNS replies that match this rule）]：DNS 応答の IP アドレスを変換するかどうかを指定します。マッピングインターフェイスから実際のインターフェイスに移動する DNS 応答の場合、アドレス（IPv4 A または IPv6 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、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殊なときに使用され、NAT64/46 の変換で必要になる場合もあります。この場合、書き換えによって A レコードと AAAA レコードの変換も実行されます。詳細については、「NAT を使用した DNS クエリと応答の書き換え （87 ページ）」を参照してください。 このオプションはポート変換を行う場合は使用できません。
- [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）]：マッピング IP アドレスへの着信パケットのプロキシ ARP を無効にします。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で、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 を無効にすることもできます。その場合、アップストリーム ルータに適切なルートが確実に設定されていなくてはなりません。アイデンティティ NAT の場合、通常はプロキシ ARP が不要で、場合によっては接続性に関する問題を引き起こす可能性があります。

ステップ 9 **[OK]** をクリックします。

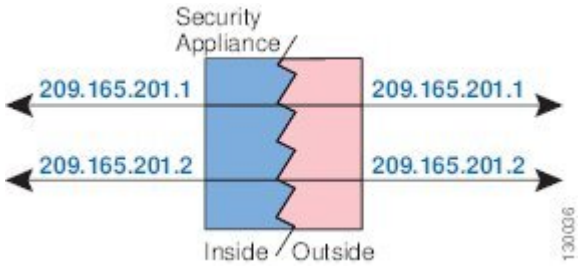
アイデンティティ NAT

IP アドレスを自身に変換する必要のある NAT コンフィギュレーションを設定できます。たとえば、1 つのネットワークを除いた、すべてのネットワークに NAT を適用するといった広範

なルールを作成する場合、スタティック NAT ルールを作成して、アドレスを自身に変換することができます。

次の図に、一般的なアイデンティティ NAT のシナリオを示します。

図 *12*：アイデンティティ *NAT*



ここでは、アイデンティティ NAT の設定方法について説明します。

アイデンティティ自動 NAT の設定

アドレスが変換されないようにするには、スタティック アイデンティティ自動 NAT ルールを使用します。つまり、アドレスをそのアドレス自体に変換するということです。

始める前に

[オブジェクト（Objects）] を選択し、ルールで必要となるネットワーク オブジェクトまたはグループを作成します。または、NAT ルールを定義する際にオブジェクトを作成することもできます。作成するオブジェクトは、以下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）にする必要があります。ホスト、範囲、またはサブネットのいずれかを使用できます。
- [変換済みアドレス（Translated Address）]：元の送信元オブジェクトとコンテンツがまったく同一のネットワーク オブジェクトまたはグループ。同じオブジェクトを使用することもできます。

手順

ステップ 1 **[ポリシー（Policies）]** > **[NAT]** の順に選択します。

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場合は、[+] ボタンをクリックします。
- 既存のルールを編集する場合は、対象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場合は、対象のルールのゴミ箱アイコンをクリックします）。

ステップ 3 以下の基本ルール 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（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 メンバー インターフェイスの場合は必須）この NAT ルールを適用するインターフェイス。[Source] は実際のインターフェイスで、このインターフェイスを経由してトラフィックはデバイスに入ります。[Destination] はマッピングされたインターフェイスで、このインターフェイスを経由してトラフィックはデバイスから出ます。デフォルトでは、ルールはブリッジ グループ メンバ インターフェイスを除くすべてのインターフェイス（[Any]）に適用されます。
- [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。
- [変換後のアドレス（Translated Address）]：元の送信元と同じオブジェクトを指定します。オプションで、内容が完全に同じ別のオブジェクトを選択することもできます。

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

ステップ 5 （オプション）[詳細（Advanced）] リンクをクリックし、適切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 を無効にします。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で、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 を無効にすることもできます。その場合、アップストリーム ルータに適切なルートが確実に設定されていなくてはなりません。アイデンティティ NAT の場合、通常はプロキシ ARP が不要で、場合によっては接続性に関する問題を引き起こす可能性があります。
- [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）]：元の発信元アドレスと変換された発信元アドレスに同一のオブジェクトを選択する際に送信元インターフェイスと宛先インターフェイスを選択する場合、このオプションを選択すると、NAT ルールで設定された宛先インターフェイスではなくルーティング テーブルに基づいてシステムが宛先インターフェイスを決定するようにできます。

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

スタティック アイデンティティ手動 NAT ルールは、自動 NAT ではニーズを満たさない場合に使用します。たとえば、宛先に応じて異なる変換を適用する必要がある場合などです。アド

レスが変換されないようにするには、スタティック アイデンティティ NAT ルールを使用します。つまり、アドレスをそのアドレス自体に変換するということです。

始める前に

[オブジェクト（Objects）] を選択し、ルールで必要となるネットワーク オブジェクトまたはグループを作成します。グループに IPv4 アドレスと IPv6 アドレスの両方を混在させることはできません。グループに含まれるタイプは 1 つだけにする必要があります。または、NAT ルールを定義する際にオブジェクトを作成することもできます。作成するオブジェクトは、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を指定できます。ホスト、範囲、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、この手順をスキップし、ルールで [すべて（Any）] を指定します。
- [変換後の送信元アドレス（Translated Source Address）]：元の送信元オブジェクトと同じオブジェクトを指定します。オプションで、内容が完全に同じ別のオブジェクトを選択することもできます。

スタティック変換をこれらのアドレスに対してルールで設定する場合は、[元の宛先アドレス（Original Destination Address）] と [変換後の宛先アドレス（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。ポート変換のみを適用する宛先スタティック インターフェイス NAT を設定する場合は、宛先マッピング アドレスのオブジェクトを追加せずに、インターフェイスをルールに指定できます。

送信元、宛先、またはその両方でポート変換を実行することもできます。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。アイデンティティ NAT では、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]** の順に選択します。

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場合は、[+] ボタンをクリックします。
- 既存のルールを編集する場合は、対象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場合は、対象のルールのゴミ箱アイコンをクリックします）。

ステップ 3 以下の基本ルール 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）]：ルールを追加する場所です。ルールは、カテゴリ（自動 NAT ルールの前か後）、または選択したルールの上か下に挿入できます。

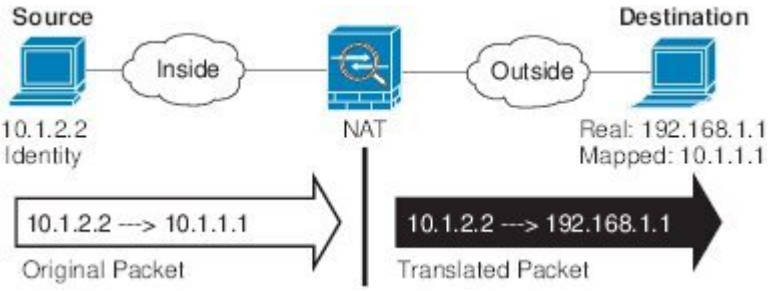
- [タイプ（Type）]：[スタティック（Static）]を選択します。この設定が適用されるのは、送信元アドレスだけです。宛先アドレスの変換を定義すると、変換は常にスタティックなものになります。

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 メンバー インターフェイスの場合は必須）この NAT ルールを適用するインターフェイス。[Source]は実際のインターフェイスで、このインターフェイスを経由してトラフィックはデバイスに入ります。[Destination] はマッピングされたインターフェイスで、このインターフェイスを経由してトラフィックはデバイスから出ます。デフォルトでは、ルールはブリッジ グループ メンバ インターフェイスを除くすべてのインターフェイス（[Any]）に適用されます。

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。つまり、元のパケットで表されているパケット アドレスです。

元のパケットと変換後のパケットを比較する例として、以下の図を参照してください。ここでは、内部ホストでアイデンティティ NAT を実行しますが、外部ホストは変換します。



- [元の送信元アドレス（Original Source Address）]：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。

- [元の宛先アドレス（Original Destination Address）]：（オプション）宛先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、宛先に関係なく、送信元アドレス変換が適用されます。宛先アドレスを指定した場合、そ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 を使用できます。

  [インターフェイス（Interface）] を選択して、元の宛先を送信元インターフェイスに基づかせることもできます（この場合、[すべて（Any）] を指定することはできません）。このオプションを選択する場合、変換済みの宛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 に宛先アドレスのポート変換を実装するには、このオプションを選択し、さらにその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 変換後のパケットのアドレスが IPv4 または IPv6 のどちらであるかを識別します。つまり、宛先インターフェイス ネットワークで表されるパケット アドレスです。必要に応じて、IPv4 と IPv6 の間で変換できます。

- [変換後の送信元アドレス（Translated Source Address）]：元の送信元オブジェクトと同じオブジェクトを指定します。オプションで、内容が完全に同じ別のオブジェクトを選択することもできます。
- [変換後の宛先アドレス（Translated Destination Address）]：（オプション）変換後の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を指定します。[元の宛先アドレス（Original Destination Address）] に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（つまり、変換なし）を設定します。

ステップ 7 （任意）サービス変換の送信元または宛先サービスのポートを特定します。

ポート変換を適用するスタティック NAT を設定している場合、送信元、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 の間での変換が可能です。

NAT では、TCP または UDP だけ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（Advanced）] リンクをクリックし、適切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 を無効にします。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で、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 を無効にすることもできます。その場合、アップストリーム ルータに適切なルートが確実に設定されていなくてはなりません。アイデンティティ NAT の場合、通常はプロキシ ARP が不要で、場合によっては接続性に関する問題を引き起こす可能性があります。
- [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）]：元の発信元アドレスと変換された発信元アドレスに同一のオブジェクトを選択する際に送信元インターフェイスと宛先インターフェイスを選択する場合、このオプションを選択すると、NAT ルールで設定された宛先インターフェイスではなくルーティング テーブルに基づいてシステムが宛先インターフェイスを決定するようにできます。

ステップ 9 **[OK]** をクリックします。

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）ルールを使用して、IP アドレスを他の IP アドレスに変換します。通常、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。1 つのアドレスから別のアドレスへ変換することも、また、ポートアドレス変換（PAT）を使用して、多数のアドレスを 1 つのアドレスへ変換することもできます（ポート番号を利用して送信元アドレスを区別します）。

NAT ルールには次の基本的なプロパティが含まれます。特に説明がない限り、自動 NAT ルールと手動 NAT ルールのプロパティは同じです。

立場

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（Create Role For）

変換ルールを [自動 NAT（Auto NAT）] にするか、[手動 NAT（Manual NAT）] にするかを指定します。自動 NAT は手動 NAT よりも簡単ですが、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別々の変換を作成できます。

[ステータス（Status）]

ルールをアクティブにするか、無効にするかを指定します。

配置（Placement）（手動 NAT のみ）

ルールを追加する場所です。ルールは、カテゴリ（自動 NAT ルールの前か後）、または選択したルールの上か下に挿入できます。

[タイプ（Type）]

変換ルールを [ダイナミック（Dynamic）] または [スタティック（Static）] で指定します。ダイナミック変換はマッピング アドレスをアドレスのプール（PAT 実装時にはアドレスとポートの組み合わせ）から自動的に選択します。マッピングアドレスおよびポートを独自に定義する場合はスタティック変換を使用します。

以降のトピックでは、その他の NAT ルール 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

[パケット変換（Packet Translation）] オプションを使用して、送信元アドレスとマッピング変換後アドレスを定義します。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 メンバー インターフェイスの場合は必須）この NAT ルールを適用するインターフェイス。[Source] は実際のインターフェイスで、このインターフェイスを経由してトラフィックはデバイスに入ります。[Destination] はマッピングされたインターフェイスで、このインターフェイスを経由してトラフィックはデバイスから出ます。デフォルトでは、ルールはブリッジ グループ メンバ インターフェイスを除くすべてのインターフェイス（[Any]）に適用されます。

[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。グループではなくネットワーク オブジェクトにする必要があり、ホスト、範囲、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）]（通常は必須）

変換先のマッピング アドレス。ここでの選択は定義する変換ルールのタイプに依存します。

- [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。これはネットワーク オブジェクトまたはグループにすることができますが、サブネットを含むことはできません。グループに IPv4 アドレスと IPv6 アドレスの両方を混在させることはできません。グループに含まれるタイプは 1 つだけにする必要があります。 グループに範囲とホスト IP アドレスの両方が含まれている場合、範囲はダイナミック NAT に使用され、ホスト IP アドレスは PAT のフォールバックとして使用されます。
- [ダイナミック PAT（Dynamic PAT）]：次のいずれかです。
  - （インターフェイス PAT）。接続先インターフェイスの IPv4 アドレスを使用する場合は、[インターフェイス（Interface）] を選択します。この場合、特定の接続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。IPv6 にインターフェイス PAT を使用することはできません。
  - 接続先インターフェイスアドレス以外の単一アドレスを使用するには、この目的で作成したホスト 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）]：次のいずれかです。
  - アドレスの設定グループを使用するには、マッピングされた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はホスト、範囲、またはサブネットを含むことができます。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。
  - （ポート変換を適用するスタティック インターフェイス NAT の場合）接続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。この場合、特定の接続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。これはポート変換と共に、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/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 にインターフェイス PAT を使用することはできません。
- [アイデンティティ NAT（Identity NAT）]：送信元と同じオブジェクト。オプションで、内容が完全に同じ別のオブジェクトを選択することもできます。

[変換前のポート（Original Port）]、[変換後のポート（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、変換前のポートと変換後の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、同じプロトコルを対象としたものでなければなりません。たとえば、必要に応じて TCP/80 を TCP/8080 に変換することができます。

手動 NAT のパケット変換プロパティ

[パケット変換（Packet Translation）] オプションを使用して、送信元アドレスとマッピング変換後アドレスを定義します。次のプロパティは手動 NAT にのみ適用されます。特に説明がない限り、すべてオプションです。

[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 メンバー インターフェイスの場合は必須）この NAT ルールを適用するインターフェイス。[Source] は実際のインターフェイスで、このインターフェイスを経由してトラフィックはデバイスに入ります。[Destination] はマッピングされたインターフェイスで、このインターフェイスを経由してトラフィックはデバイスから出ます。デフォルトでは、ルールはブリッジ グループ メンバ インターフェイスを除くすべてのインターフェイス（[Any]）に適用されます。

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

変換す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にすることが可能で、ホスト、範囲、またはサブネットを含むことができます。変換前のすべての送信元トラフィックを変換する場合、ルール内に [任意（Any）] を指定できます。

[変換後の送信元アドレス（Translated Source Address）]（通常は必須）

変換先のマッピング アドレス。ここでの選択は定義する変換ルールのタイプに依存します。

- [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。これはネットワーク オブジェクトまたはグループにすることができますが、サブネットを含むことはできません。グループに IPv4 アドレスと IPv6 アドレスの両方を混在させることはできません。グループに含まれるタイプは 1 つだけにする必要があります。 グループに範囲とホスト IP アドレスの両方が含まれている場合、範囲はダイナミック NAT に使用され、ホスト IP アドレスは PAT のフォールバックとして使用されます。
- [ダイナミック PAT（Dynamic PAT）] : 次のいずれかです。
  - （インターフェイス PAT）。接続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。この場合、特定の接続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。IPv6 にインターフェイス PAT を使用することはできません。

- 接続先インターフェイスアドレス以外の単一アドレスを使用するには、この目的で作成したホスト 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）]：次のいずれかです。
  - アドレスの設定グループを使用するには、マッピングされた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はホスト、範囲、またはサブネットを含むことができます。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。
  - （ポート変換を適用するスタティック インターフェイス NAT の場合）接続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。この場合、特定の接続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。これはポート変換と共に、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/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 にインターフェイス PAT を使用することはできません。

- [アイデンティティ NAT（Identity NAT）]：送信元と同じオブジェクト。オプションで、内容が完全に同じ別のオブジェクトを選択することもできます。

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

宛先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、宛先に関係なく、送信元アドレス変換が適用されます。宛先アドレスを指定した場合、そ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 を使用できます。

[インターフェイス（Interface）] を選択して、元の宛先を送信元インターフェイスに基づかせることもできます（この場合、[すべて（Any）] を指定することはできません）。このオプションを選択する場合、変換済みの宛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 に宛先アドレスのポート変換を実装するには、このオプションを選択し、さらにその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）]

変換後の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を指定します。[変換前の宛先（Original Destination）] に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（つまり、変換なし）を設定します。

変換後の宛先として完全修飾ドメイン名を指定するネットワークオブジェクトを使用できます。詳細については、FQDN 宛先のガイドライン （14 ページ）を参照してください。

[変換前の送信元ポート（Original Source Port）]、[変換後の送信元ポート（Translated Source Port）]、[変換前の宛先ポート（Original Destination Port）]、[変換後の宛先ポート（Translated Destination Port）]

変換前のパケットと変換後のパケットに対する送信元サービスと宛先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、もしくは、ポートを変換せずにルールをサービ

スに提供できるように同じオブジェクトを選択します。サービスを設定するときは、次のルールに注意してください。

- （ダイナミック NAT または PAT）。[変換前の送信元ポート（Original Source Port）] および [変換後の送信元ポート（Translated Source Port）] では変換できません。変換は宛先ポートでのみ実行できます。
- NAT では、TCP または UDP だけ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。

詳細 NAT プロパティ

NAT を設定する場合、**[詳細（Advanced）]** オプションで、専門サービスを提供する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す。サービスが必要な場合にのみ設定します。

このルールに一致する DNS 回答の変換

DNS 応答の IP アドレスを変換するかどうかを指定します。マッピングインターフェイスから実際のインターフェイスに移動する DNS 応答の場合、アドレス（IPv4 A または IPv6 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、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殊なときに使用され、NAT64/46 の変換で必要になる場合もあります。この場合、書き換えによって A レコードと AAAA レコードの変換も実行されます。詳細については、「NAT を使用した DNS クエリと応答の書き換え （87 ページ）」を参照してください。 このオプションは、スタティック NAT ルールでポート変換を行っているときは利用できません。

[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）

他のマッピングアドレスがすでに割り当てられている場合、バックアップ手段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）を指定します。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した場合にのみ使用できます。変換されたアドレスとしてすでにインターフェイス PAT を設定している場合、このオプションを選択できません。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プロキシ ARP なし（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 を無効にします。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で、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 を無効にすることもできます。その場合、アップストリーム

ルータに適切なルートが確実に設定されていなくてはなりません。アイデンティティ NAT の場合、通常はプロキシ ARP が不要で、場合によっては接続性に関する問題を引き起こす可能性があります。

[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）]（静的アイデンティティ NAT のみ、ルーテッド モードのみ）

元の発信元アドレスと変換された発信元アドレスに同一のオブジェクトを選択する際に送信元インターフェイスと宛先インターフェイスを選択する場合、このオプションを選択すると、NAT ルールで設定された宛先インターフェイスではなくルーティング テーブルに基づいてシステムが宛先インターフェイスを決定するようにできます。

IPv6 ネットワークの変換

トラフィックが IPv6 のみのネットワークと IPv4 のみのネットワークの間を通過するようにする必要がある場合、NAT を使用してアドレス タイプを変換する必要があります。2 つの IPv6 ネットワークの場合でも、外部ネットワークに対して内部アドレスを非表示にする必要がある場合があります。

IPv6 ネットワークでは次の変換タイプを使用できます。

- NAT64、NAT46—IPv6 パケットから IPv4 パケットへの変換とその逆変換2 つのポリシー、IPv6 から IPv4 への変換、および IPv4 から IPv6 への変換を定義する必要があります。これは、1 つの 手動 NAT ルールで実行できますが、DNS サーバが外部ネットワーク上にある場合、DNS 応答をリライトする必要があります。宛先を指定するときに 手動 NAT ルールで DNS リライトを有効にすることができないため、2 つの 自動 NAT ルールを作成することがより適切なソリューションです。

（注） NAT46 はスタティック マッピングのみをサポートします。

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

（注） NAT64 および NAT 46 は、標準のルーテッド インターフェイスのみで使用できます。NAT66 は、ルーテッドおよびブリッジ グループ メンバー インターフェイスの両方で使用できます。

NAT64/46：IPv6 から IPv4 へのアドレス変換

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

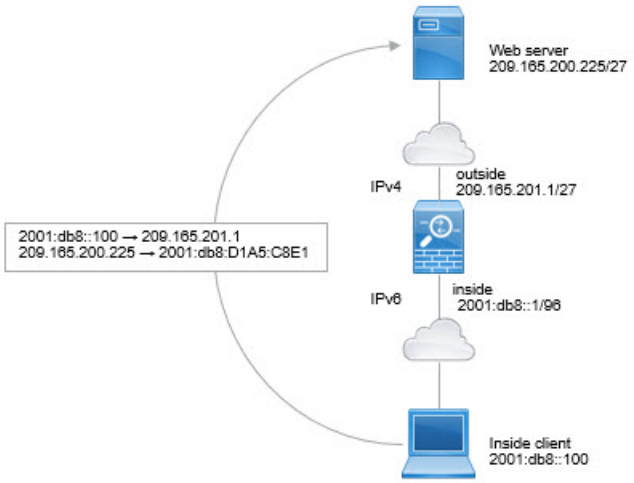
ンドする IPv6 アドレス プール（IPv6 内）という 2 つのアドレス プールを定義する必要があります。

- NAT64 ルール用の IPv4 アドレス プールは、一般に小さく、通常は IPv6 クライアント アドレスと 1 対 1 でマッピングするために十分なアドレスを持っていません。ダイナミック PAT は、ダイナミック NAT やスタティック NAT と比較して、多数の IPv6 クライアント アドレスに容易に適合します。
- NAT 46 ルール用の IPv6 アドレス プールは、マッピングされる IPv4 アドレスの数以上にすることができます。よって、各 IPv4 アドレスを異なる IPv6 アドレスにマッピングできます。NAT46 はスタティック マッピングのみをサポートするため、ダイナミック PAT は使用できません。

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

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

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



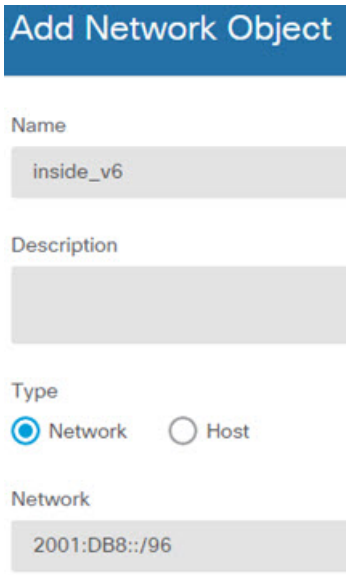
この例では、外部インターフェイスの IP アドレスとダイナミック PAT インターフェイスを使用して、内部 IPv6 ネットワークを IPv4 に変換します。外部 IPv4 トラフィックは 2001:db8::/96 ネットワークのアドレスに静的に変換され、内部ネットワークでの送信が許可されます。

手順

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

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（例：inside_v6）、[ネットワーク（Network）] を選択し、ネットワーク アドレス 2001:db8::/96 を入力します。



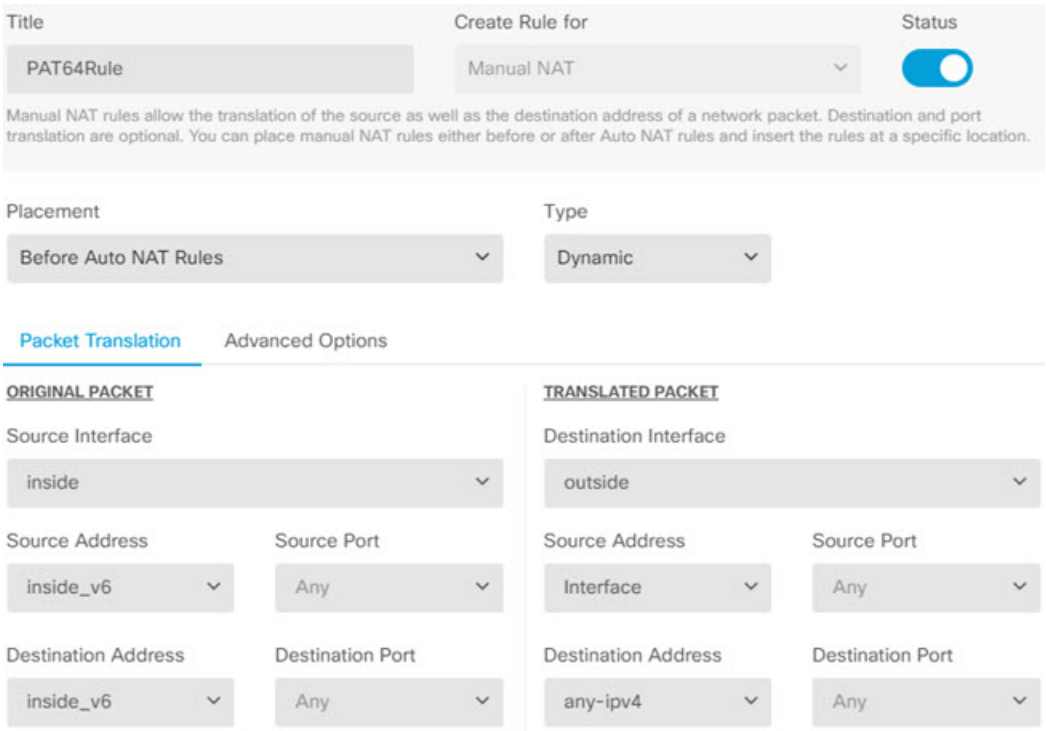
d) [追加（Add）]、[OK] をクリックします。

ステップ 2 IPv6ネットワークをIPv4に変換し、再度変換する手動NATルールを作成します。

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（またはユーザーが選択する別の名前）
- [ルールの作成対象（Create Rule For）] = [手動 NAT（Manual NAT）]。
- [配置（Placement）]：[自動NATルールの前（Before Auto NAT Rules）]。
- [タイプ（Type）] = [ダイナミック（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。
- [元のパケット発信元アドレス（Original Packet Source Address）]：inside_v6 ネットワークオブジェクト。
- [変換済みパケット発信元アドレス（Translated Packet Source Address）]：[インターフェイス（Interface）]。このオプションでは、宛先インターフェイスの IPv4 アドレスが PAT アドレスとして使用されます。

- [元のパケット宛先アドレス（Original Packet Destination Address）]：inside_v6 ネットワークオブジェクト。
- [変換済みパケット宛先アドレス（Translated Packet Destination Address）]：any-ipv4 ネットワークオブジェクト。

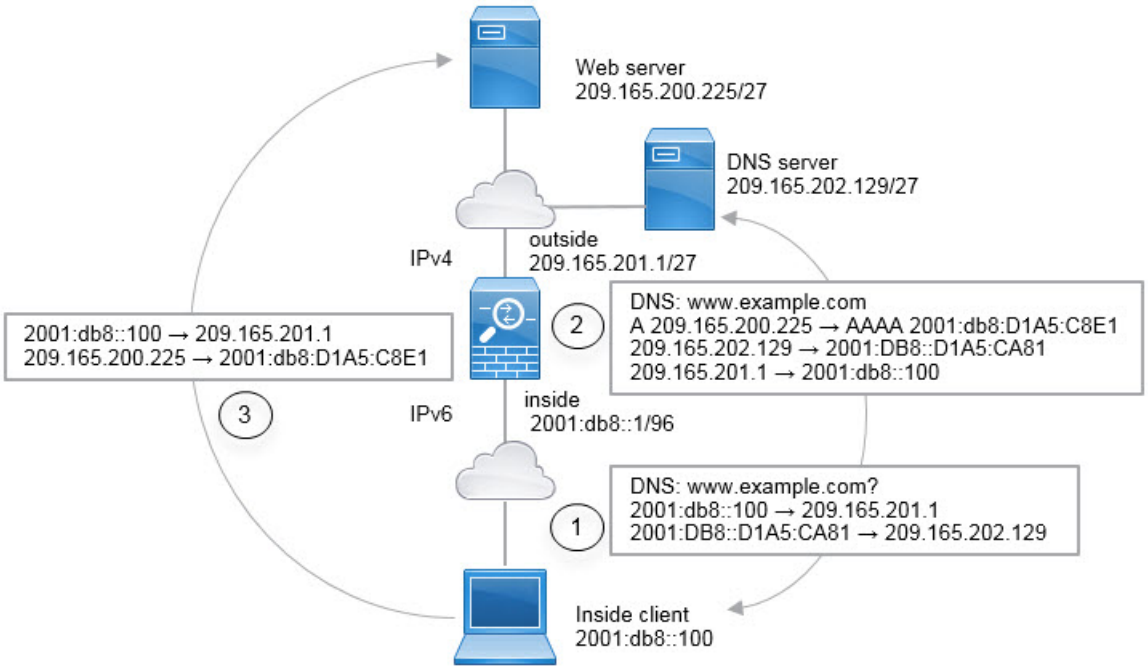


d) [OK] をクリックします。

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

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

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



この例では、外部インターフェイスの IP アドレスとダイナミック PAT インターフェイスを使用して、内部 IPv6 ネットワークを IPv4 に変換します。外部 IPv4 トラフィックは 2001:db8::/96 ネットワークのアドレスに静的に変換され、内部ネットワークでの送信が許可されます。NAT46 ルールでの DNS の書き換えを有効にし、外部 DNS サーバからの応答を A（IPv4）から AAAA（IPv6）レコードに変換したり、アドレスを IPv4 から IPv6 に変換したりできます。

内部 IPv6 ネットワーク上の 2001:DB8::100 にあるクライアントが www.example.com を開こうとする Web 要求の通常のシーケンスを次に示します。

1. クライアントのコンピュータは、2001:DB8::D1A5:CA81 で DNS サーバに DNS リクエストを送信します。NAT ルールは、DNS リクエストで送信元と宛先に以下の変換を実行します。
   - 2001:DB8::100 から 209.165.201.1 上の固有のポート（NAT64 インターフェイス PAT ルール）
   - 2001:DB8::D1A5:CA81 から 209.165.202.129（NAT46 ルール。D1A5:CA81 は IPv6 の 209.165.202.129 と同じです）
2. DNS サーバが応答で、www.example.com が 209.165.200.225 であるという A レコードを示します。DNS の書き換えが有効になっている NAT46 ルールは、A レコードを IPv6 版の AAAA レコードに変換し、AAAA レコードの 209.165.200.225 を 2001:db8:D1A5:C8E1 に変換します。さらに、DNS 応答の発信元アドレスと宛先アドレスは変換されません。
   - 209.165.202.129 から 2001:DB8::D1A5:CA81
   - 209.165.201.1 から 2001:db8::100

3. これで、IPv6 クライアントには Web サーバの IP アドレスが含まれるようになり、2001:db8:D1A5:C8E1 で www.example.com への HTTP リクエストを行います（D1A5:C8E1 は IPv6 の 209.165.200.225 と同じです）。HTTP リクエストの発信元アドレスと送信先アドレスは次のように変換されます。
   - 2001:DB8::100 から 209.156.101.54 上の固有のポート（NAT64 インターフェイス PAT ルール）
   - 2001:db8:D1A5:C8E1 から 209.165.200.225（NAT46 ルール）

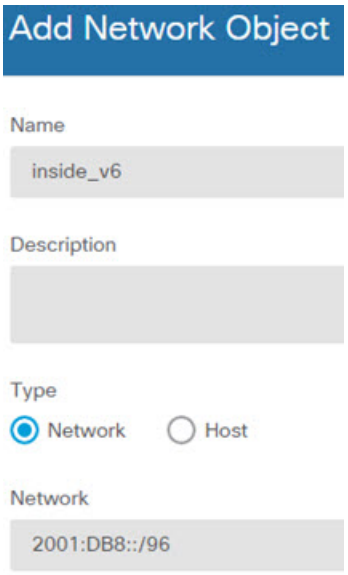
次の手順では、この例の指定方法について説明します。

手順

ステップ 1 内部 IPv6 ネットワークおよび外部 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。

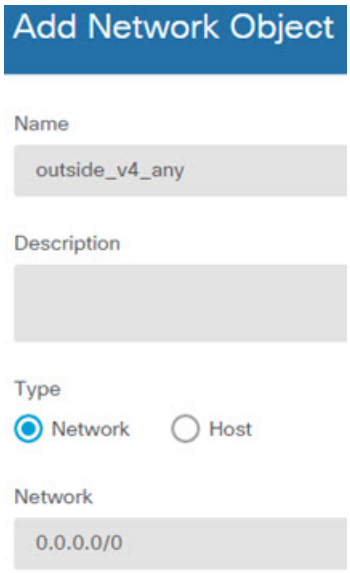
a) [オブジェクト（Objects）] を選択します。
b) コンテンツ テーブルから [ネットワーク（Network）] を選択し、[+] をクリックします。
c) 内部 IPv6 ネットワークを定義します。

ネットワーク オブジェクトに名前を付け（例：inside_v6）、[ネットワーク（Network）] を選択し、ネットワーク アドレス 2001:db8::/96 を入力します。



d) [追加（Add）]、[OK] をクリックします。
e) [+] をクリックして、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（例：outside_v4_any）、[ネットワーク（Network）] を選択し、ネットワーク アドレス 0.0.0.0/0 を入力します。



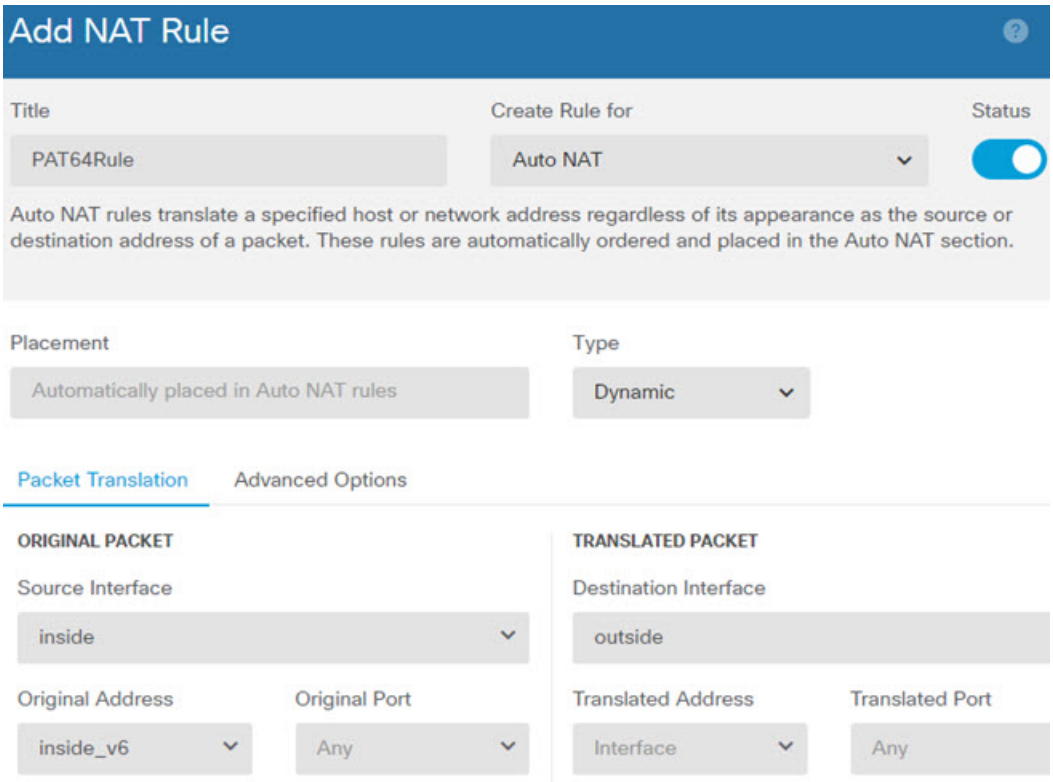
ステップ 2 内部 IPv6 ネットワークの NAT64 ダイナミック PAT ルールを設定します。

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（またはユーザーが選択する別の名前）
- [ルールの作成対象（Create Rule For）] = [自動 NAT（Auto NAT）]。
- [種類（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。
- [変換後のアドレス（Translated Address）] = [インターフェイス（Interface）]。このオプションは、PAT アドレスとしての宛先インターフェイスの IPv4 アドレスです。



d) [OK] をクリックします。

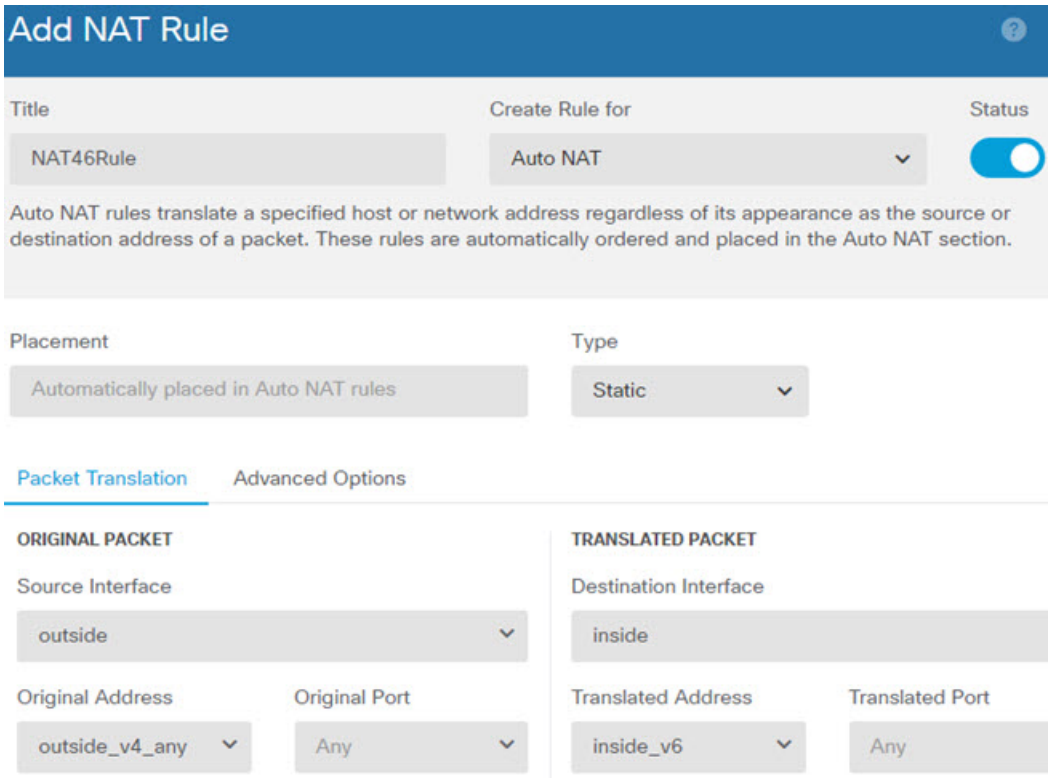
このルールを使用すると、内部インターフェイス上の 2001:db8::/96 サブネットから外部インターフェイスに入るすべてのトラフィックは、外部インターフェイスの IPv4 アドレスを使用して NAT64 PAT 変換を受けます。

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（またはユーザーが選択する別の名前）。
- [ルールの作成対象（Create Rule For）] = [自動 NAT（Auto NAT）]。
- [種類（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。
- [変換後のアドレス（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。



c) [OK] をクリックします。

このルールを使用すると、内部インターフェイスに入る外部ネットワークの IPv4 アドレスはすべて、組み込み IPv4 アドレス方式を使用して 2001:db8::/96 ネットワーク上の 1 つのアドレスに変換されます。さらに、DNS 応答は、A（IPv4）から AAAA（IPv6）レコードに変換され、アドレスは IPv4 から IPv6 に変換されます。

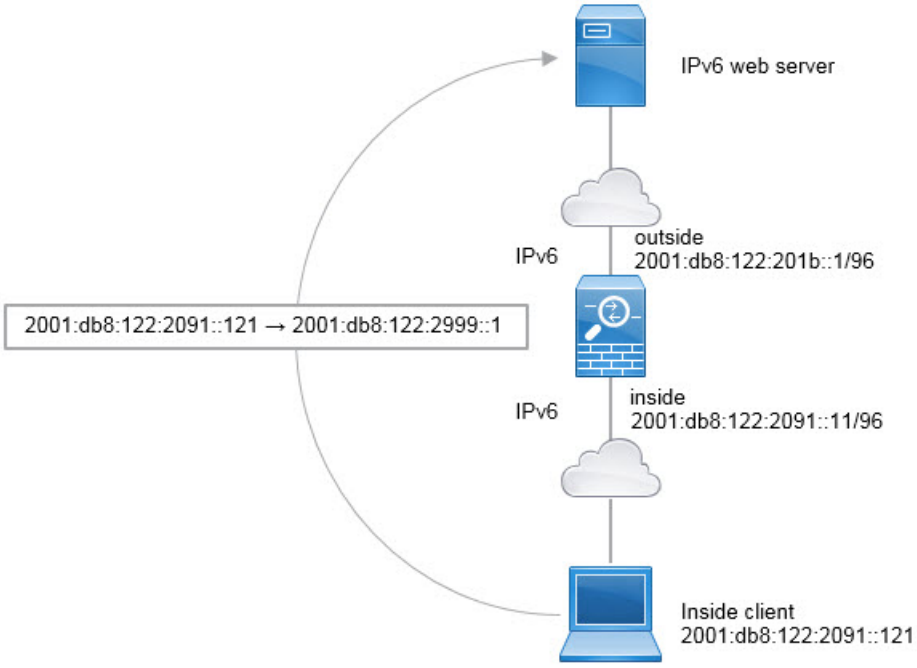
NAT66：IPv6 アドレスから別の IPv6 アドレスへの変換

IPv6 ネットワークから別の IPv6 ネットワークへと通過する場合、IPv6 アドレスを外部ネットワーク上の別の IPv6 アドレスに変換できます。スタティック NAT を使用することを推奨します。ダイナミック NAT または PAT を使用できますが、IPv6 アドレスは大量にあるため、ダイナミック NAT を使用する必要はありません。

異なるアドレス タイプの間で変換されていないため、NAT66 変換用の 1 つのルールが必要です。これらのルールは、自動 NATを使用して簡単にモデル化することができます。ただし、リターントラフィックを許可しない場合は、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変換を設定できます。次の例は、2001:db8:122:2091::/96 ネットワークの内部アドレスを、2001:db8:122:2999::/96 ネットワークの外部アドレスへ変換する方法について説明しています。



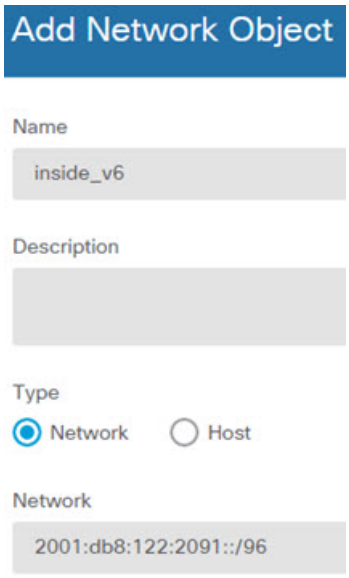
（注） この例では、内部インターフェイスがブリッジグループインターフェイス（BVI）ではなく、標準的なルーテッドインターフェイスであることを想定しています。内部インターフェイスがBVI の場合は、メンバー インターフェイスごとにルールを複製する必要があります。

手順

ステップ 1 内部 IPv6 ネットワークおよび外部 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。

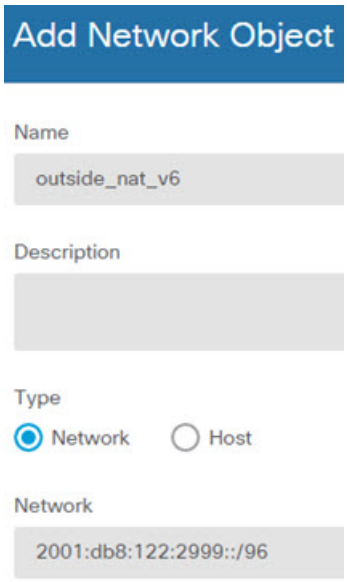
ネットワーク オブジェクトに名前を付け（例：inside_v6）、[ネットワーク（Network）] を選択し、ネットワーク アドレス 2001:db8:122:2091::/96 を入力します。



d) [追加（Add）]、[OK] をクリックします。

e) [+] をクリックして、外部 IPv6 PAT 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（例：outside_nat_v6）、[ネットワーク（Network）] を選択し、ネットワーク アドレス 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。

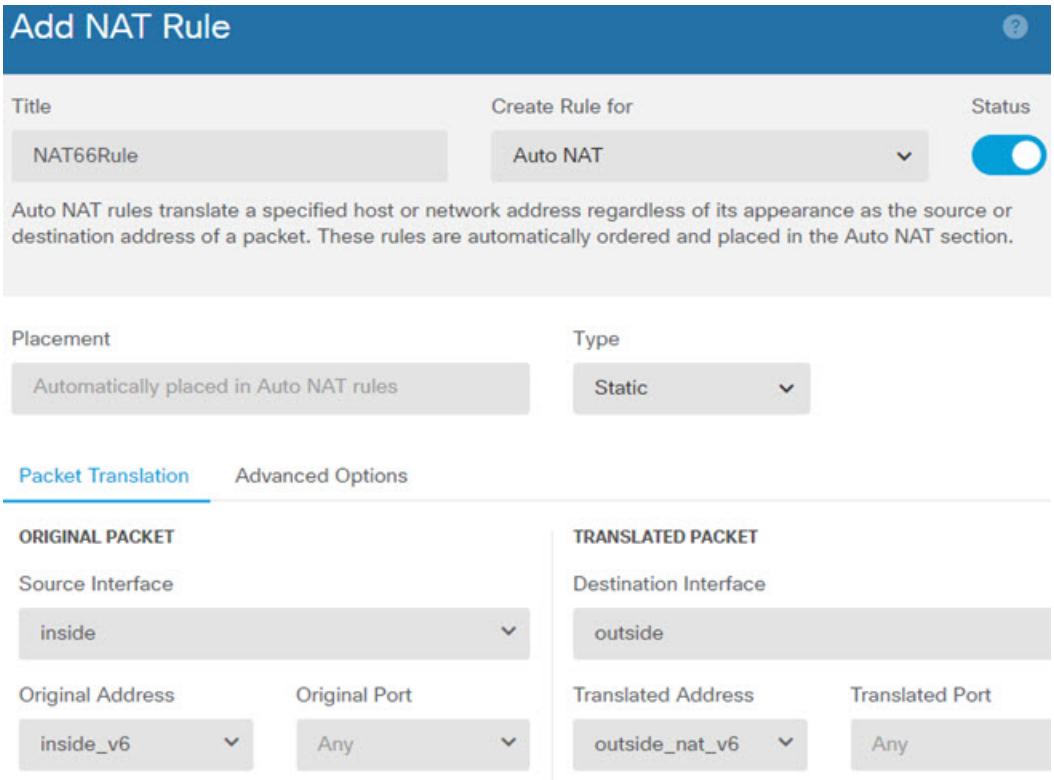
a) **[ポリシー（Policies）]** > **[NAT]** を選択します。

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（またはユーザーが選択する別の名前）

- [ルールの作成対象（Create Rule For）] = [自動 NAT（Auto NAT）]。
- [種類（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。
- [変換後のアドレス（Translated Address）] = [outside_nat_v6] ネットワーク オブジェクト。



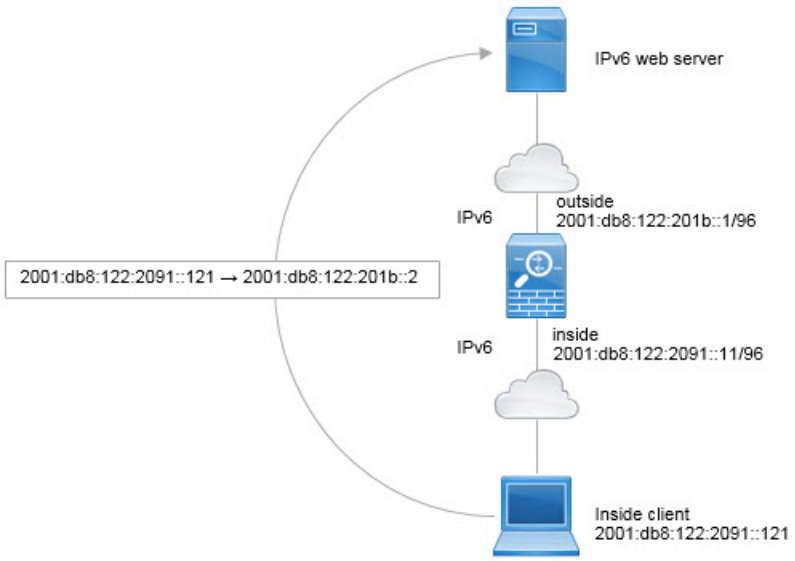
d) [OK] をクリックします。

このルールを使用すると、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入るすべてのトラフィックは、2001:db8:122:2999::/96 ネットワークのアドレスへのスタティック NAT66 変換を受けます。

NAT66 の例：シンプル IPv6 インターフェイス PAT

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

ただし、Device Manager を使用して、インターフェイスの IPv6 アドレスを使用するインターフェイス PAT は設定できません。代わりに、ダイナミック PAT プールと同じネットワークで単一のフリー アドレスを使用してください。



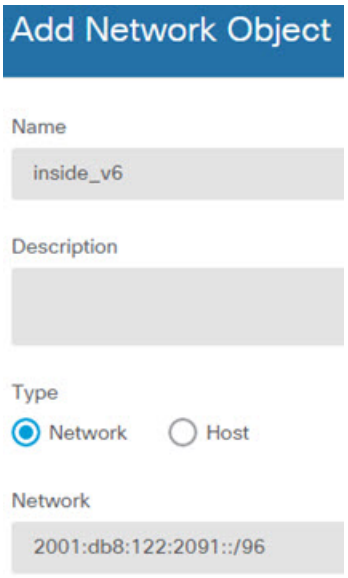
（注） この例では、内部インターフェイスがブリッジグループインターフェイス（BVI）ではなく、標準的なルーテッドインターフェイスであることを想定しています。内部インターフェイスが BVI の場合は、メンバー インターフェイスごとにルールを複製する必要があります。

手順

ステップ 1 内部 IPv6 ネットワークおよび IPv6 PAT 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) 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（例：inside_v6）、[ネットワーク（Network）] を選択し、ネットワーク アドレス 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) [+] をクリックして、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（例：ipv6_pat）、[ホスト（Host）] を選択し、ホスト アドレス 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。

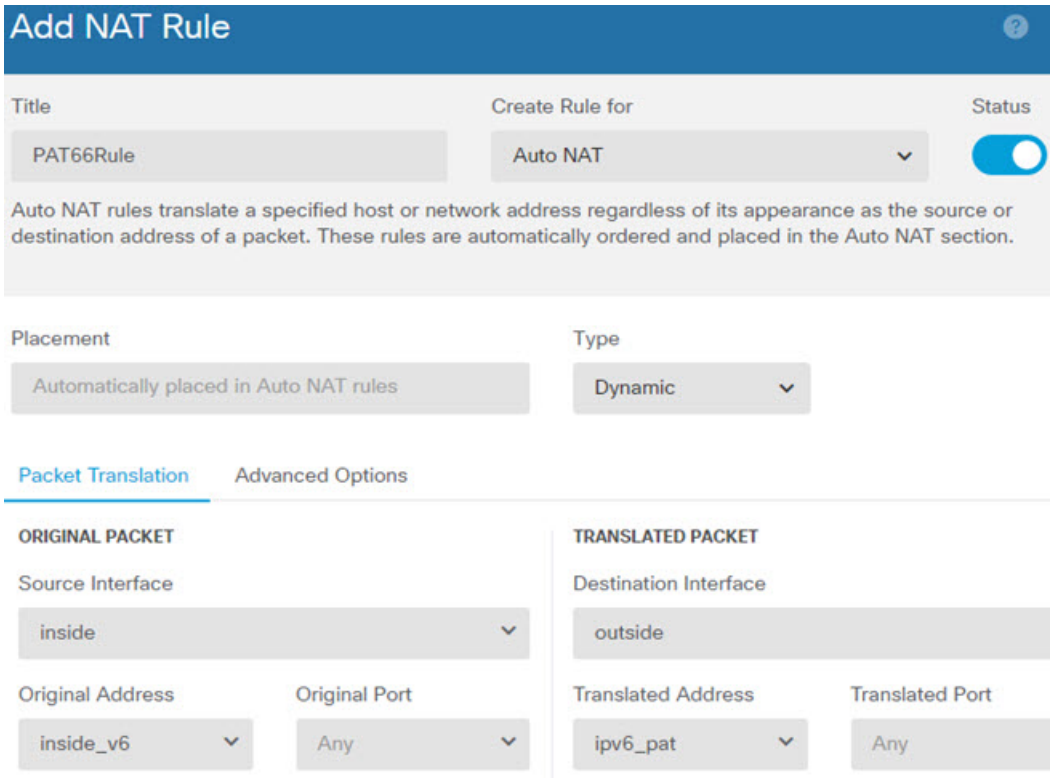
a) **[ポリシー（Policies）]** > **[NAT]** を選択します。

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（またはユーザーが選択する別の名前）。

- [ルールの作成対象（Create Rule For）] = [自動 NAT（Auto NAT）]。
- [種類（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。
- [変換後のアドレス（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。

このルールを使用すると、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入るすべてのトラフィックは、2001:db8:122:201b::2 のポートへのダイナミック PAT66 変換を受けます。

NAT のモニタリング

NAT接続をモニタし、トラブルシューティングを行うには、CLIコンソールを開くか、またはデバイスの 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数を表示します。NAT のその他の情報を表示する追加キーワードがあります。
- **show xlate** 現在アクティブな実際の NAT 変換を表示します。
- **clear xlate** アクティブな NAT 変換を削除できます。既存の接続は接続が終了するまで古い変換スロットを継続して使用するため、NAT ルールを変更する場合はアクティブな変換を削除しなければならないことがあります。変換を消去することで、クライアントの次回の接続時に、システムは新しいルールに基づいてクライアントの新しい変換を作成します。（このコマンドは CLI コンソールでは使用できません）

NAT の例

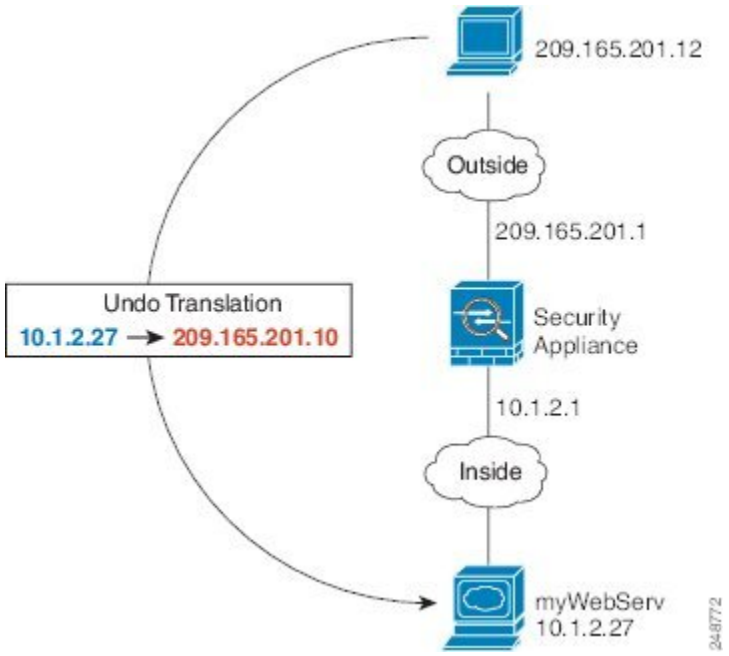
ここでは、Threat Defenceデバイス上で NAT を設定する例を紹介します。

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ので、パブリック アドレスが必要です。スタティック NAT は、固定アドレスにある Web サーバへのトラフィックをホストが開始できるようにするために必要です

（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、標準的なルーテッドインターフェイスであることを想定しています。内部インターフェイスが BVI である場合、Web サーバが接続された特定のブリッジ グループ メンバー インターフェイスを選択します（inside1_3 など）。

図 *13* : 内部 *Web* サーバーのスタティック *NAT*

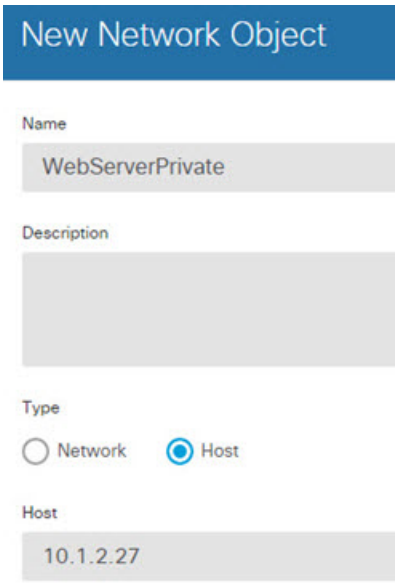


手順

ステップ 1 サーバのプライベートおよびパブリック 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。

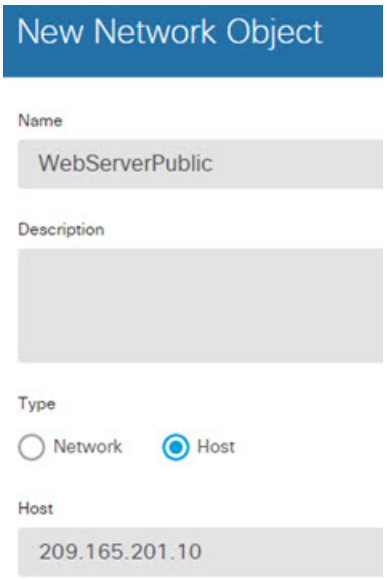
ネットワーク オブジェクトに名前を付け（例：WebServerPrivate）、[ホスト（Host）] を選択し、実際のホスト IP アドレス 10.1.2.27 を入力します。



d) [追加（Add）]、[OK] の順にクリックします。

e) [+] をクリックして、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（例：WebServerPublic）、[ホスト（Host）] を選択し、ホスト アドレス 209.165.201.10 を入力します。



f) [追加（Add）]、[OK] の順にクリックします。

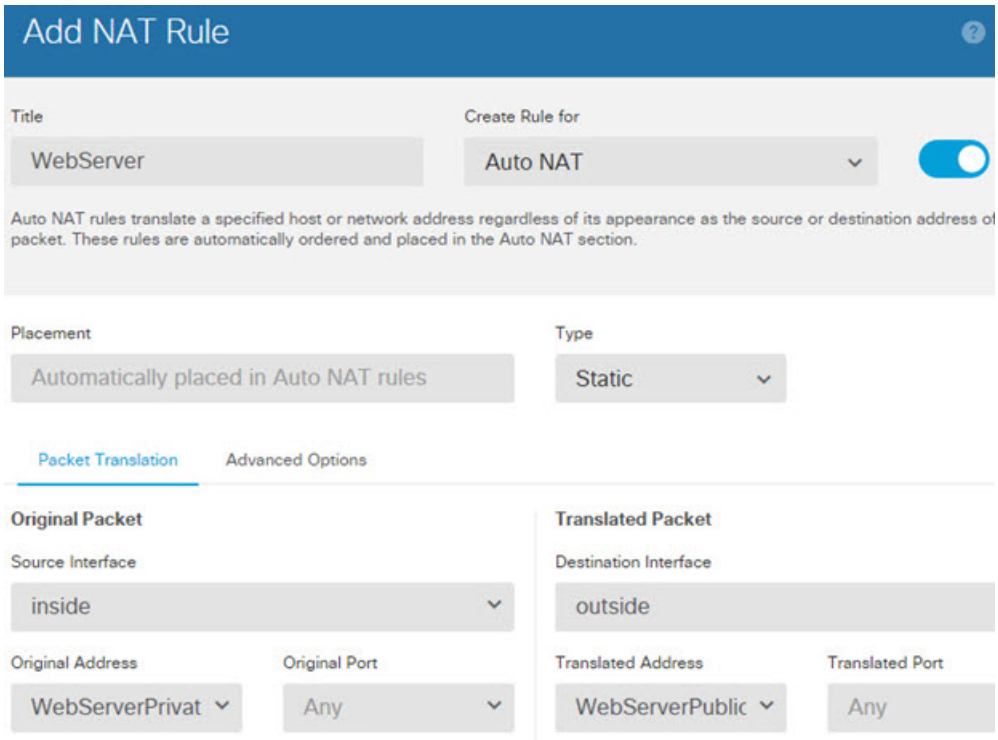
ステップ 2 オブジェクトのスタティック NAT を設定します。

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（またはユーザーが選択する別の名前）
- [ルールの作成対象（Create Rule For）] = [自動 NAT（Auto NAT）]。
- [種類（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。
- [変換後のアドレス（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。

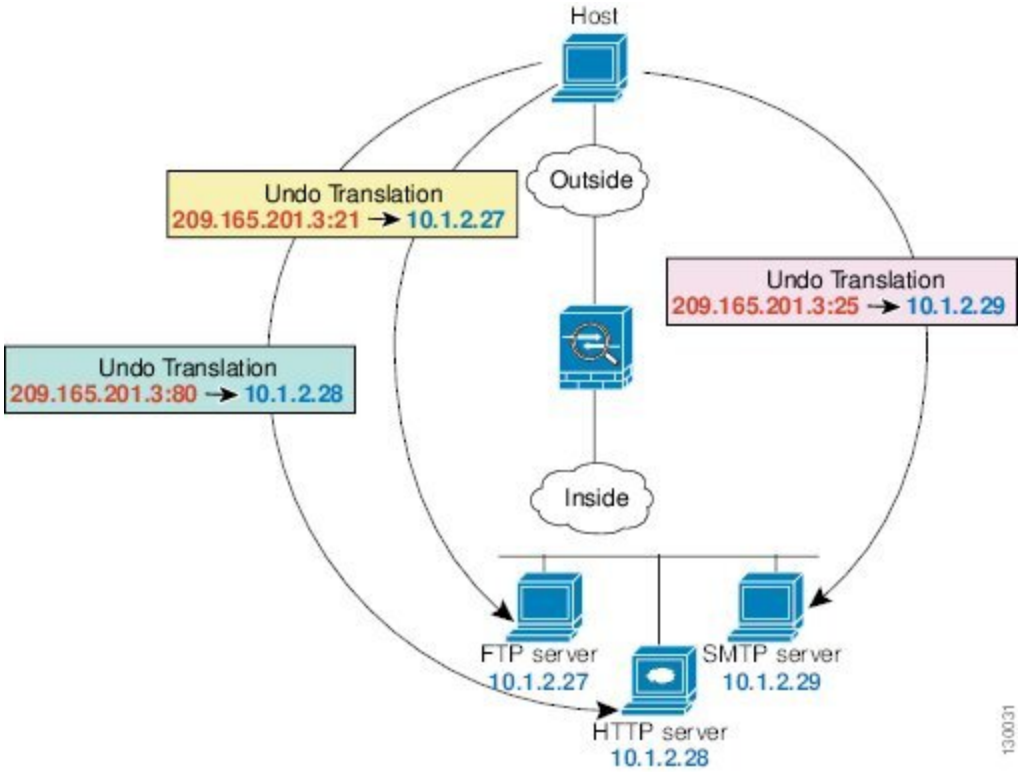
FTP、HTTP、および SMTP のための単一アドレス（ポート変換を設定したスタティック自動 NAT）

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がスイッチに接続された標準的なルーテッドインターフェイスであること、サーバがそのスイッチに接続されていることを想定しています。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、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、該当するルールにおいて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ます。たとえば、内部ではなく、送信元インターフェイスにルール inside1_2、inside1_3、inside1_4 が指定されるなどです。

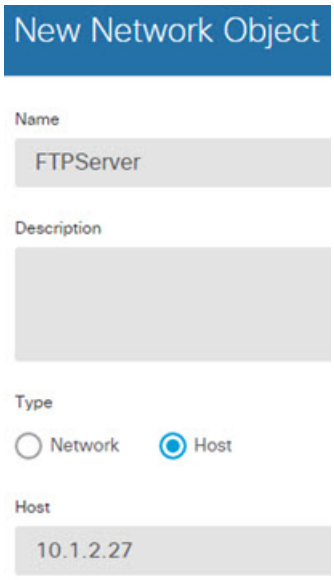
図 *14 :* ポート変換を設定したスタティック *NAT*



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 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 オブジェクトに名前を付け（例：FTPServer）、[ホスト（Host）] 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。

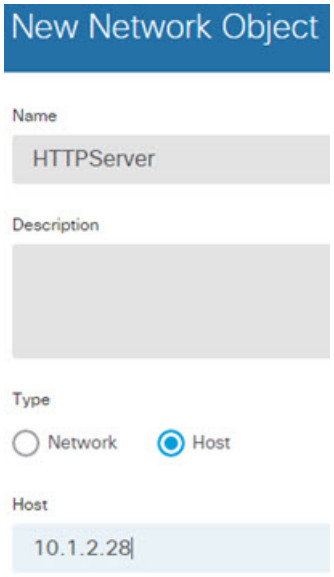


d) [追加（Add）]、[OK] の順にクリックします。

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 オブジェクトに名前を付け（例：HTTPServer）、[ホスト（Host）] を選択し、ホスト アドレス 10.1.2.28 を入力します。

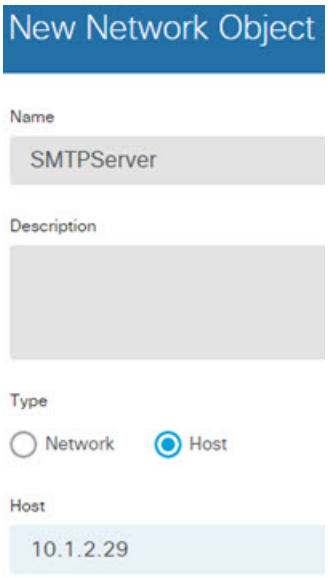


c) [追加（Add）]、[OK] の順にクリックします。

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 オブジェクトに名前を付け（例：SMTPServer）、[ホスト（Host）] を選択し、ホスト アドレス 10.1.2.29 を入力します。

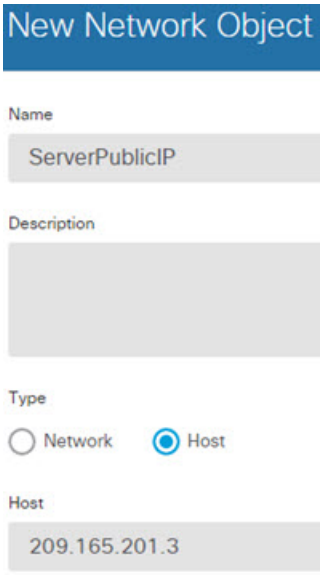


c) [追加（Add）]、[OK] の順にクリックします。

ステップ 4 3つのサーバに使用されるパブリック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 オブジェクトに名前を付け（例：ServerPublicIP）、[ホスト（Host）] を選択し、ホスト 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。

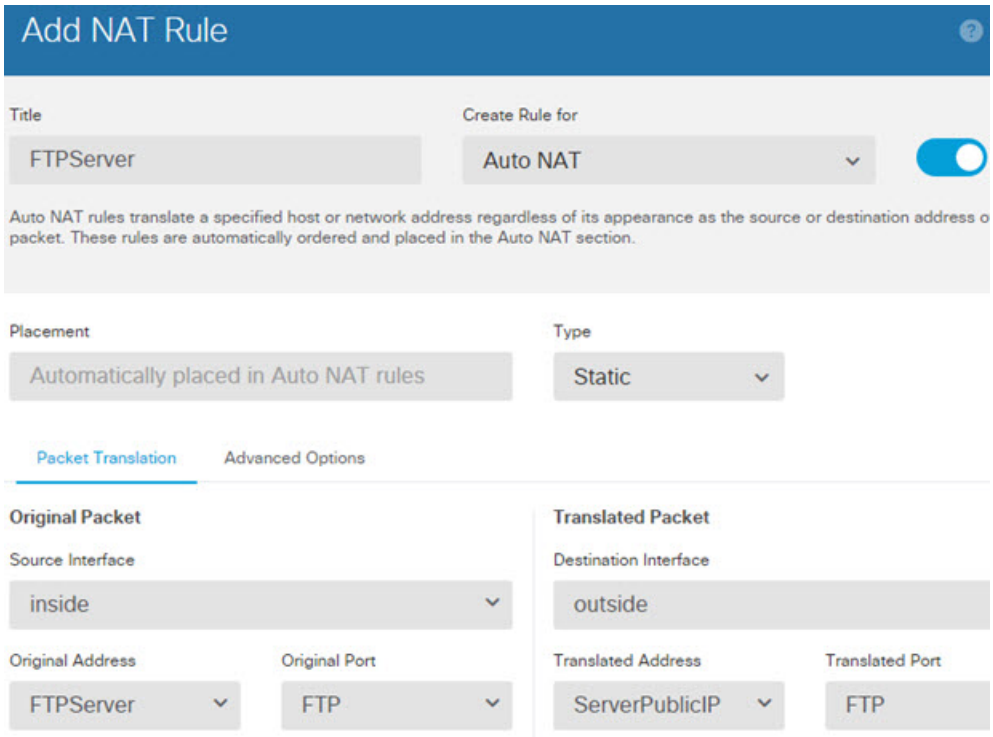
ステップ 5 FTP サーバに対するポート変換を設定したスタティック NAT を設定し、FTP ポートをマッピングします。

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）
- [ルールの作成対象（Create Rule For）] = [自動 NAT（Auto NAT）]。
- [種類（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。
- [変換後のアドレス（Translated Address）] = [ServerPublicIP] ネットワーク オブジェクト。
- [元のアドレス（Original Address）] = [FTP] ポート オブジェクト。
- [変換後のアドレス（Translated Address）] = [FTP] ポート オブジェクト。



d) [OK] をクリックします。

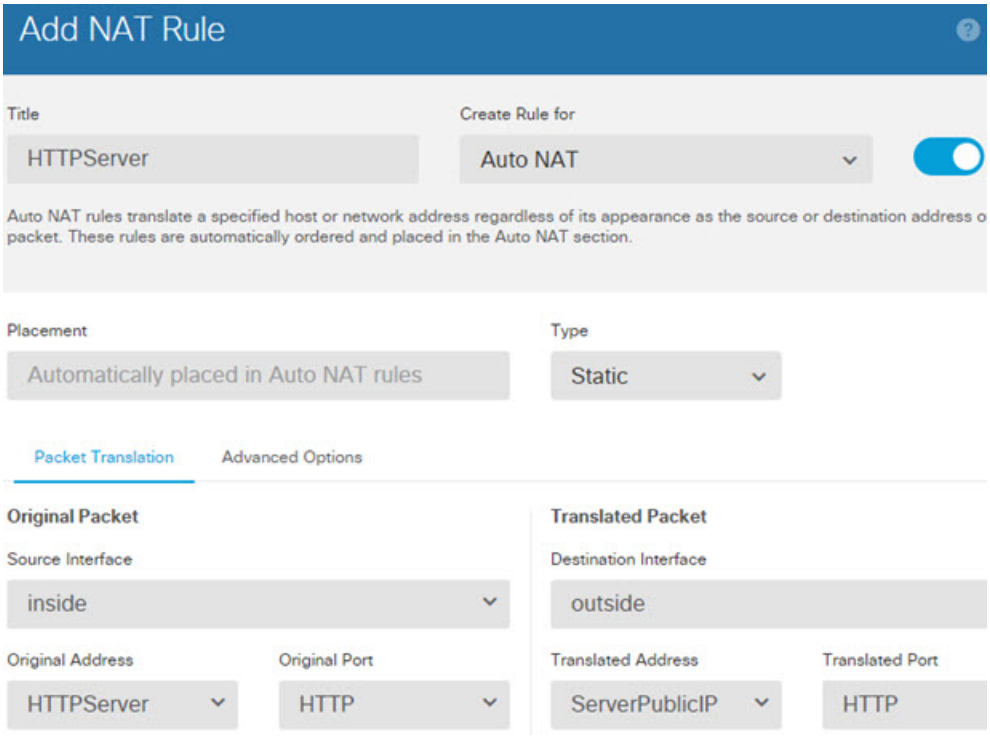
ステップ 6 HTTP サーバに対するポート変換を設定したスタティック NAT を設定し、HTTP ポートをマッピングします。

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（または任意の別の名前）。

- [ルールの作成対象（Create Rule For）] = [自動 NAT（Auto NAT）]。
- [種類（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。
- [変換後のアドレス（Translated Address）] = [ServerPublicIP] ネットワーク オブジェクト。
- [元のアドレス（Original Address）] = [HTTP] ポート オブジェクト。
- [変換後のアドレス（Translated Address）] = [HTTP] ポート オブジェクト。



c) [OK] をクリックします。

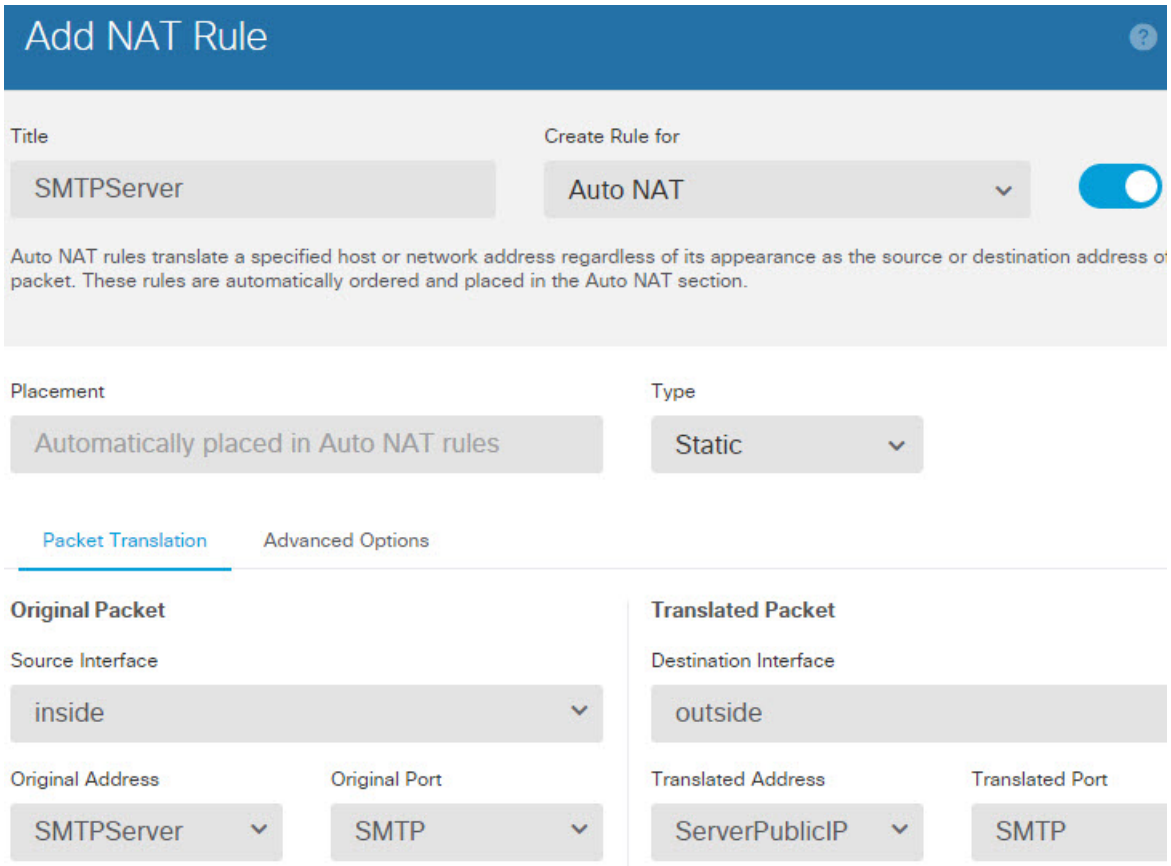
ステップ 7 SMTP サーバに対するポート変換を設定したスタティック NAT を設定し、SMTP ポートをマッピングします。

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（または任意の別の名前）。
- [ルールの作成対象（Create Rule For）] = [自動 NAT（Auto NAT）]。
- [種類（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。
- [変換後のアドレス（Translated Address）] = [ServerPublicIP] ネットワーク オブジェクト。
- [元のアドレス（Original Address）] = [SMTP] ポート オブジェクト。
- [変換後のアドレス（Translated Address）] = [SMTP] ポート オブジェクト。



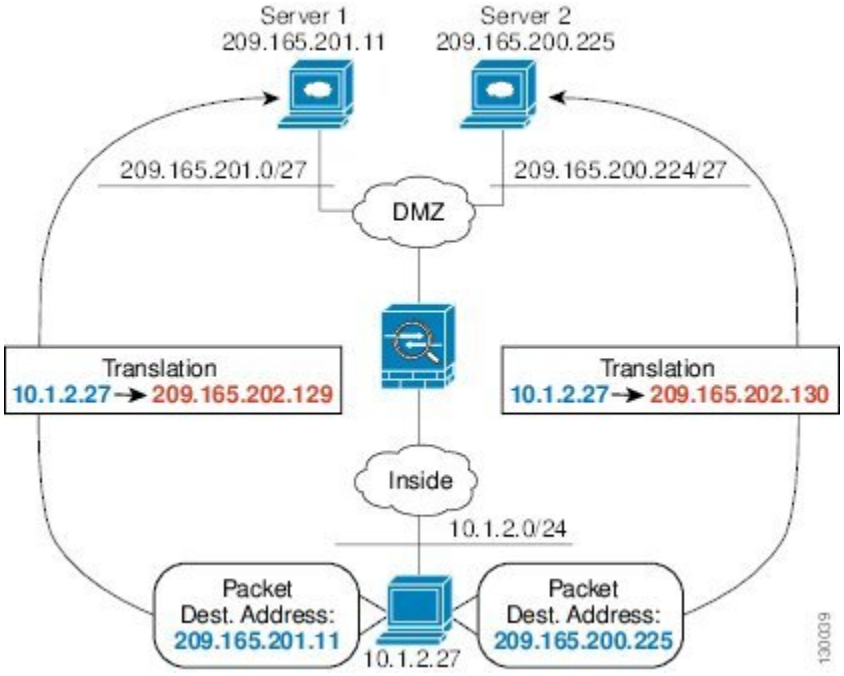
c) **[OK]** をクリックします。

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 つの異なるサーバにアクセスする、10.1.2.0/24 ネットワーク上のホストを示します。ホストがサーバ 209.165.201.11 にアクセスすると、実際のアドレスは 209.165.202.129:ポートに変換されます。ホストがサーバ 209.165.200.225 にアクセスすると、実際のアドレスは 209.165.202.130:ポートに変換されます。

（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た標準的なルーテッドインターフェイスであること、サーバがそのスイッチに接続されていることを想定しています。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、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、該当するルールにおいて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ます。たとえば、ルールで、内部ではなく送信元インターフェイスに inside1_2 と inside1_3 が指定されるなどです。

図 *15 :* 異なる宛先アドレスを使用する手動*NAT*



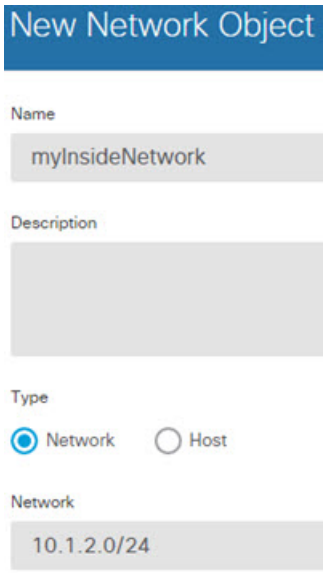
手順

ステップ 1 内部ネットワーク用のネットワーク 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 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。

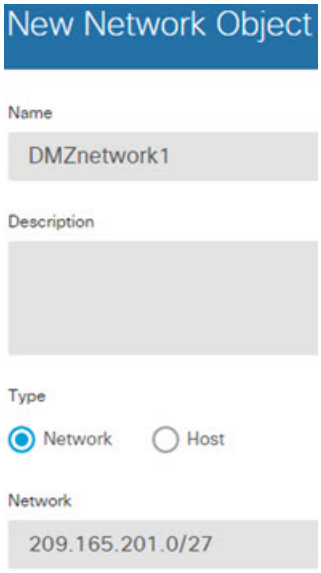


d) **[OK]** をクリックします。

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（例：DMZnetwork1）を付け、[ネットワーク（Network）] を選択して、ネットワーク アドレス「209.165.201.0/27」（サブネットマスク「255.255.255.224」）を入力します。

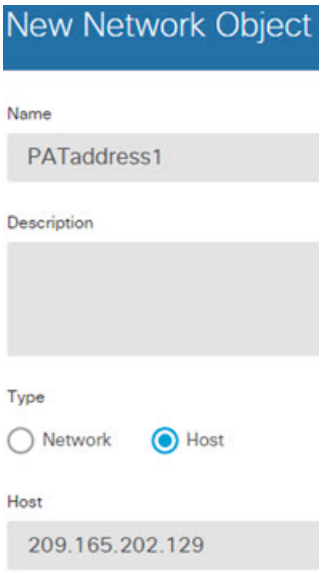


c) [追加（Add）]、[OK] をクリックします。

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（例：PATaddress1）を付け、[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。

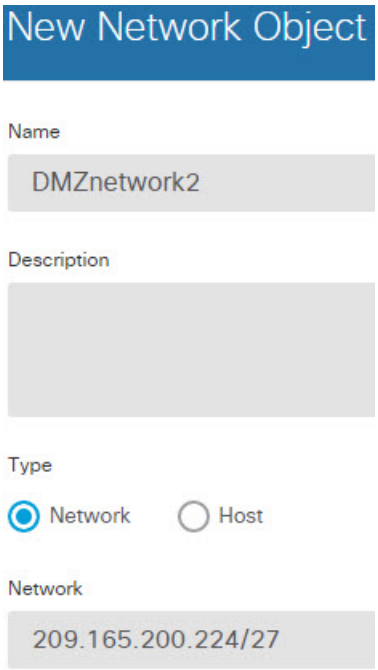


c) [追加（Add）]、[OK] をクリックします。

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（例：DMZnetwork2）を付け、[ネットワーク（Network）]を選択して、ネットワーク アドレス「209.165.200.224/27」（サブネットマスク「255.255.255.224」）を入力します。

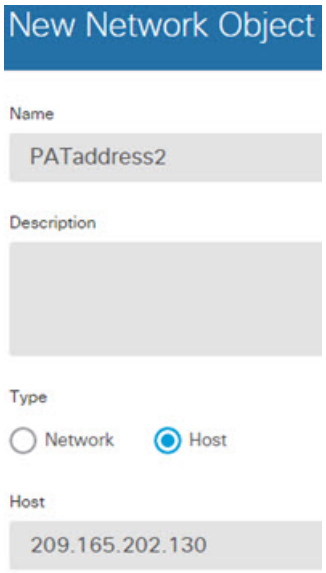


c) [追加（Add）]、[OK] をクリックします。

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（例：PATaddress2）を付け、[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。

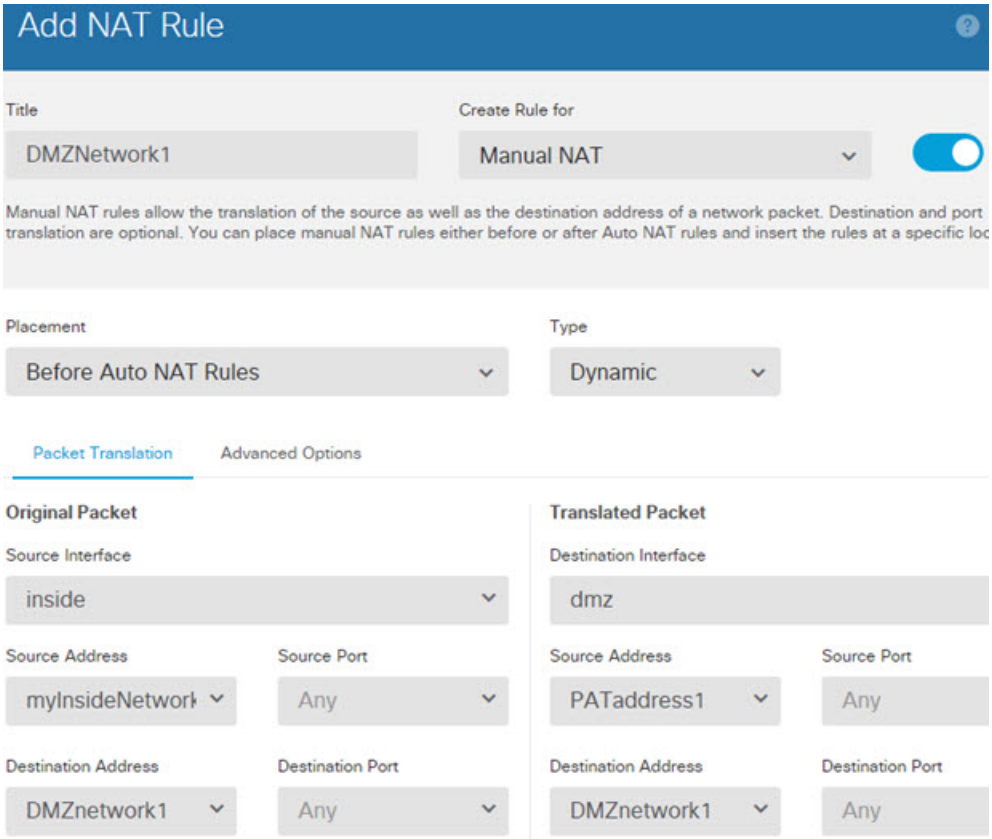
b) [+] ボタンをクリックします。

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）。
- [ルールの作成対象（Create Rule For）] = [手動NAT（Manual NAT）]。
- [種類（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 ネットワーク オブジェクト。
- [変換済み発信元アドレス（Translated Source Address）]：PATaddress1 ネットワーク オブジェクト。
- [元の宛先アドレス（Original Destination Address）]：DMZnetwork1 ネットワーク オブジェクト。

- [変換済み宛先アドレス（Translated Destination Address）]：DMZnetwork1 ネットワーク オブジェクト。

（注）
宛先アドレスを変換する必要はないため、元の宛先アドレスと変換後の宛先アドレスに同じアドレスを指定することにより、アイデンティティ NAT を設定する必要があります。ポート フィールドはすべて空欄のままにしておきます。



d) [OK] をクリックします。

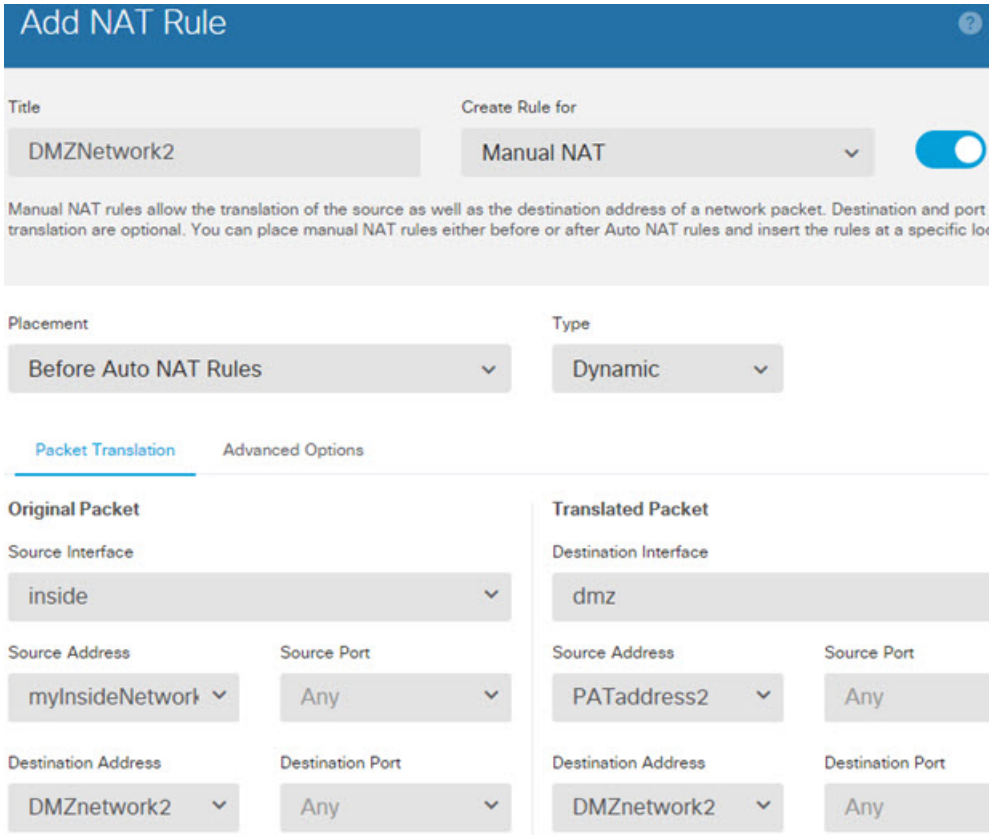
ステップ 7 DMZ ネットワーク 2 用のダイナミック手動 PAT を設定します。

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）。
- [ルールの作成対象（Create Rule For）] = [手動NAT（Manual NAT）]。
- [種類（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 ネットワーク オブジェクト。
- [変換済み発信元アドレス（Translated Source Address）]：PATaddress2 ネットワーク オブジェクト。
- [元の宛先アドレス（Original Destination Address）]：DMZnetwork2 ネットワーク オブジェクト。
- [変換済み宛先アドレス（Translated Destination Address）]：DMZnetwork2 ネットワーク オブジェクト。



c) **[OK]** をクリックします。

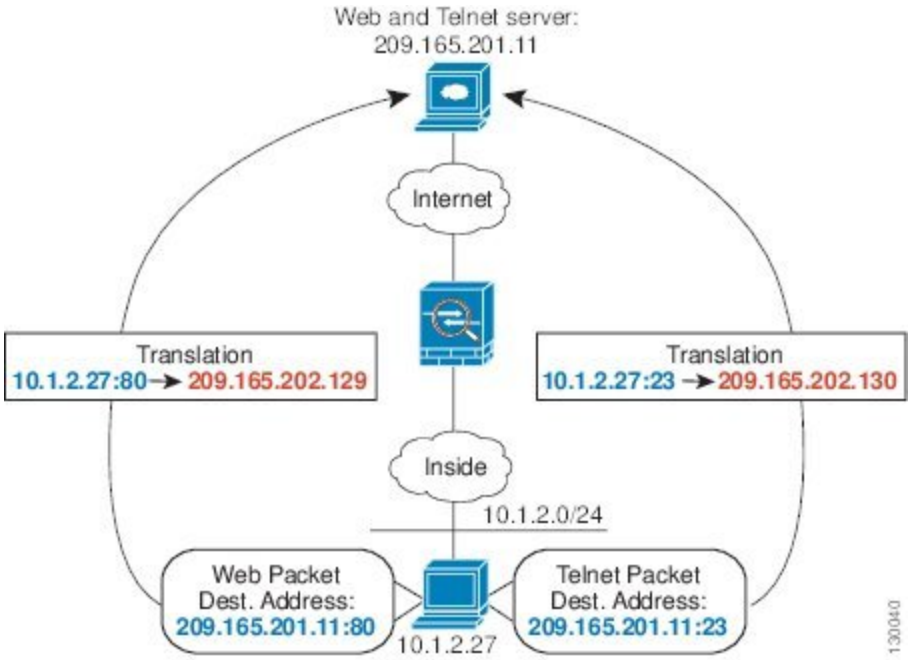
宛先アドレスおよびポートに応じて異なる変換（ダイナミック手動 PAT）

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:*port*

に変換されます。ホストが Web サービスを求めて同じサーバにアクセスすると、実際のアドレスは 209.165.202.130:*port* に変換されます。

（注） この例は、内部インターフェイスがスイッチに接続された標準的なルーテッドインターフェイスで、サーバがそのスイッチに接続されていることを想定しています。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、□ブリッジ グループ メンバー インターフェイスにサーバが接続されている場合は、サーバの接続先である特定のメンバー インターフェイスを選択します。たとえば、ルールでは内部ではなく送信元インターフェイスに inside1_2 が指定されるなどです。

図 *16 :* 異なる宛先ポートを使用する手動*NAT*



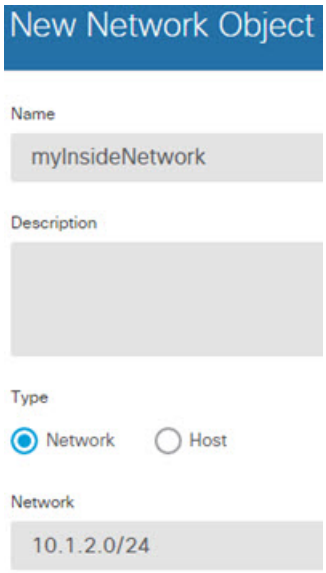
手順

ステップ 1 内部ネットワーク用のネットワーク 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 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。

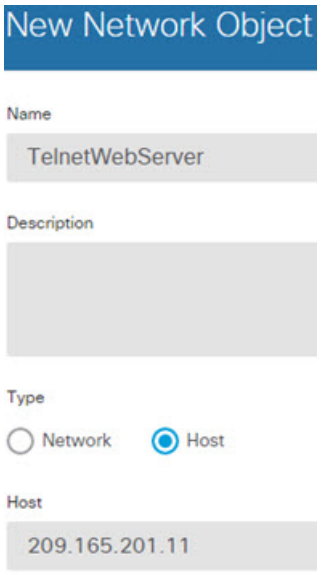


d) **[OK]** をクリックします。

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（例：TelnetWebServer）、[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。

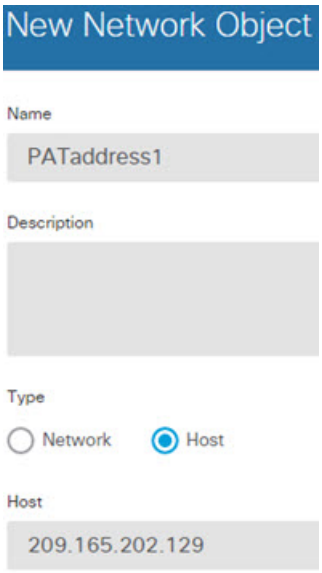


c) [追加（Add）]、[OK] をクリックします。

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（例：PATaddress1）を付け、[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。

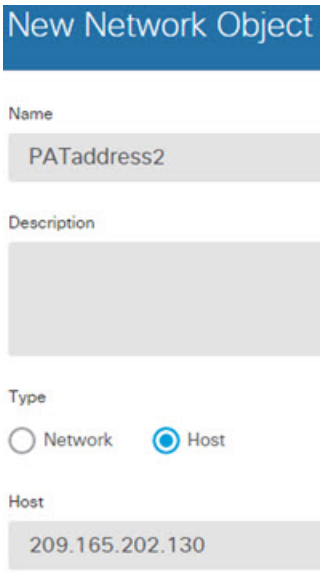


c) [追加（Add）]、[OK] をクリックします。

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（例：PATaddress2）を付け、[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。

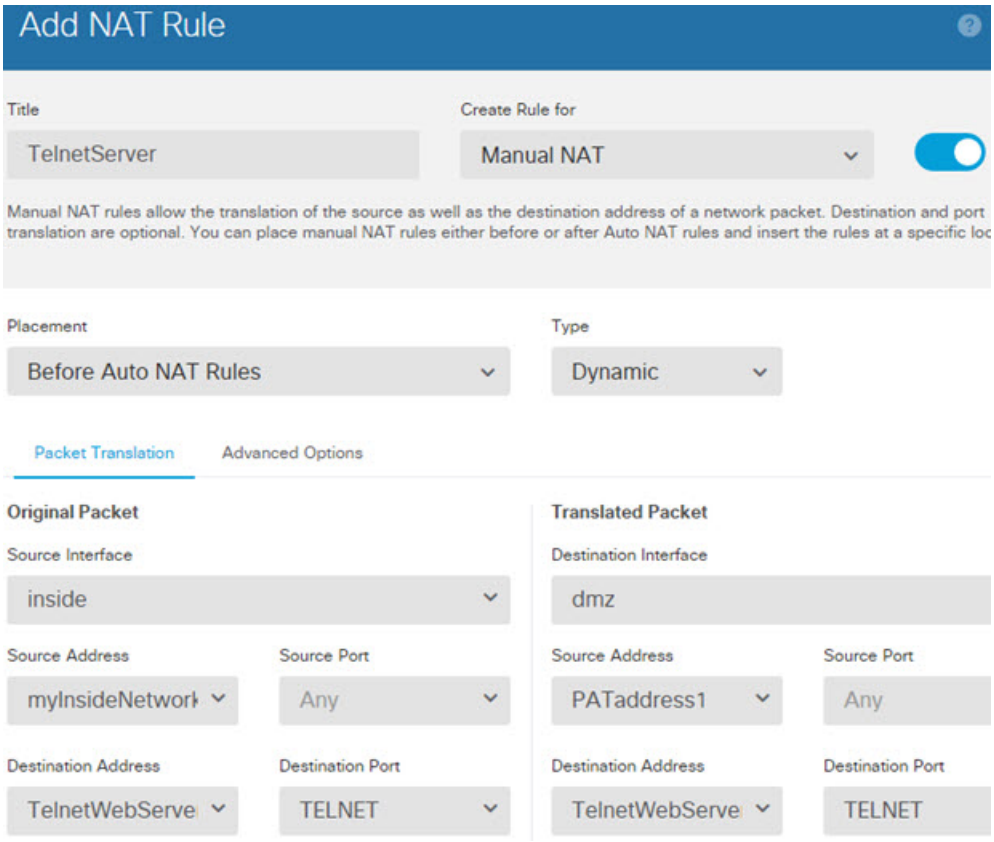
a) **[ポリシー（Policies）]** > **[NAT]** を選択します。

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）。
- [ルールの作成対象（Create Rule For）] = [手動NAT（Manual NAT）]。
- [種類（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 ネットワーク オブジェクト。
- [変換済み発信元アドレス（Translated Source Address）]：PATaddress1 ネットワーク オブジェクト。
- [元の宛先アドレス（Original Destination Address）]：TelnetWebServer ネットワーク オブジェクト。
- [変換済み宛先アドレス（Translated Destination Address）]：TelnetWebServer 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）
宛先アドレスやポートを変換する必要はないため、元の宛先アドレスと変換後の宛先アドレスに同じアドレスを指定し、元のポートと変換後のポートに同じポートを指定することにより、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。

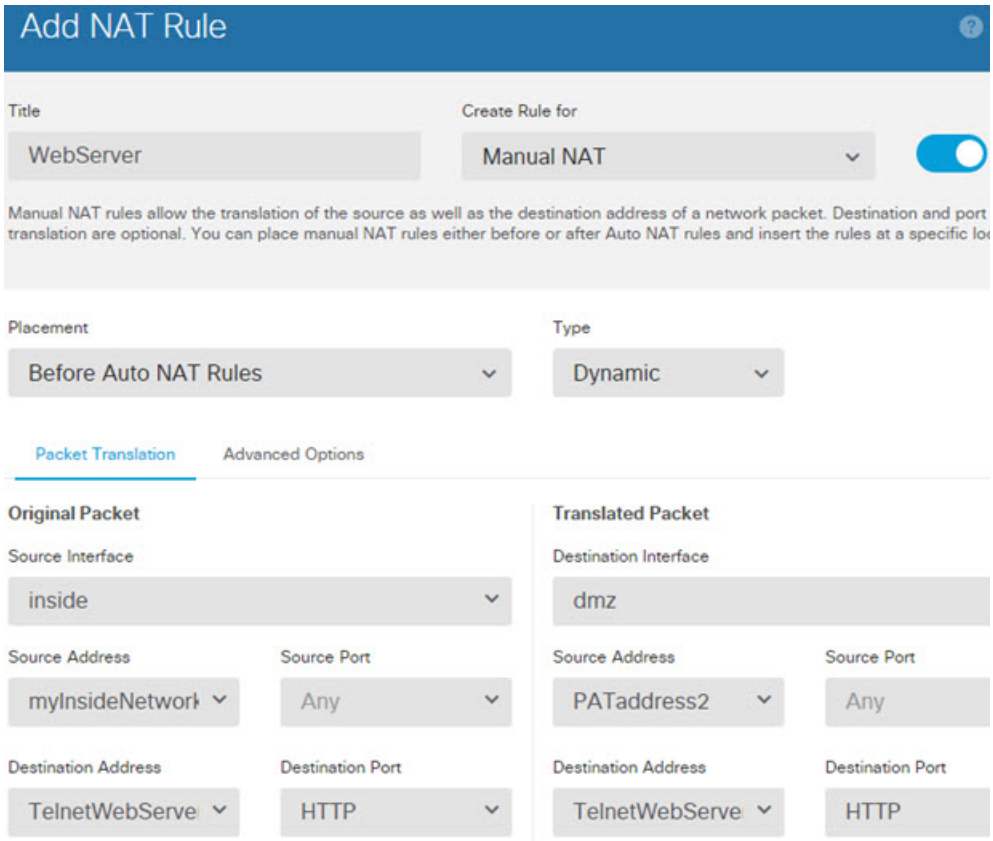
ステップ 6 Web アクセス用のダイナミック手動 PAT を設定します。

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（またはユーザーが選択する別の名前）
- [ルールの作成対象（Create Rule For）] = [手動NAT（Manual NAT）]。
- [種類（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 ネットワーク オブジェクト。
- [変換済み発信元アドレス（Translated Source Address）]：PATaddress2 ネットワーク オブジェクト。
- [元の宛先アドレス（Original Destination Address）]：TelnetWebServer ネットワーク オブジェクト。

- [変換済み宛先アドレス（Translated Destination Address）]：TelnetWebServer 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 を使用した DNS クエリと応答の書き換え

応答内のアドレスを NAT コンフィギュレーションと一致するアドレスに置き換えて、DNS 応答を修正するようにThreat Defenseデバイスを設定することが必要になる場合があります。DNS 修正は、各変換ルールの設定時に設定できます。DNS 修正は、DNS Doctoring とも呼ばれます。

この機能は、NAT ルールに一致する DNS クエリーと応答のアドレスをリライトします（たとえば、IPv4 の A レコード、IPv6 の AAAA レコード、または逆引き DNS クエリーの PTR レコード）。マッピング インターフェイスから他のインターフェイスに移動する DNS 応答の場合、レコードはマッピングされた値から実際の値に書き換えられます。逆に、任意のインターフェイスからマッピング インターフェイスに移動する DNS 応答では、A レコードは実際の値から

マップされた値へ書き換えられます。この機能は、NAT44、NAT66、 NAT46、および NAT64 と連動します。

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

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

DNS 書き換えに関する制限事項

DNS 書き換えに伴う制限事項を以下に示します。

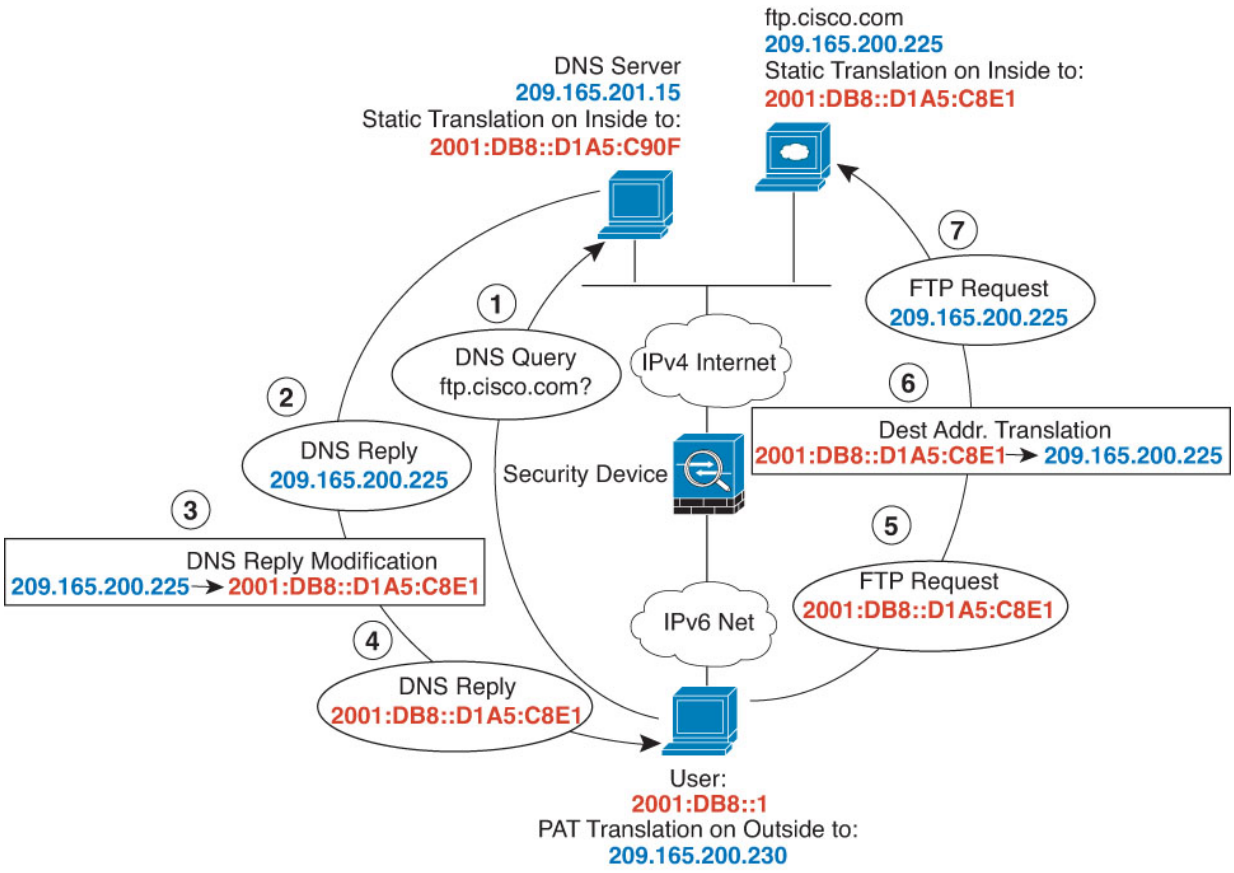
- DNS 書き換えは PAT に適用できません。これは、個々の A または AAAA レコードに複数の PAT ルールを適用できるので、使用する PAT ルールが不明確になるためです。
- 手動 NAT ルールを設定する場合、宛先アドレスおよび送信元アドレスを指定すると、DNS 修正を設定できません。これらの種類のルールでは、A と B に向かった場合に 1 つのアドレスに対して異なる変換が行われる可能性があります。したがって、DNS 応答内の IP アドレスを適切な Twice NAT ルールに一致させることができません。DNS 応答には、DNS 要求を求めたパケット内の送信元アドレスと宛先アドレスの組み合わせに関する情報が含まれません。
- 実際には、DNS 書き換えは NAT ルールではなく xlate エントリで実行されます。そのため、動的ルール用の xlate が存在しない場合は、書き換えを正しく実行できません。スタティック NAT では、同じ問題が発生しません。
- DNS 書き換えでは、DNS 動的更新メッセージ（opcode 5）が書き換えられません。

次のセクションでは、NAT ルール内の DNS 書き換えの例を示します。

DNS 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、内部 IPv6 ユーザが ftp.cisco.com のアドレスを DNS サーバに要求すると、DNS サーバは応答で実際のアドレス 209.165.200.225 を示します。

内部ユーザが ftp.cisco.com のマッピング アドレス（2001:DB8::D1A5:C8E1。D1A5:C8E1 は 209.165.200.225 と同等の IPv6 アドレス）を使用するようにするには、スタティック変換に対して DNS 応答修正を設定する必要があります。この例には、DNS サーバのスタティック NAT 変換、および内部 IPv6 ホストの PAT ルールも含まれています。



（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、標準的なルーテッドインターフェイスであることを想定しています。内部インターフェイスがBVI の場合は、メンバー インターフェイスごとにルールを複製する必要があります。

手順

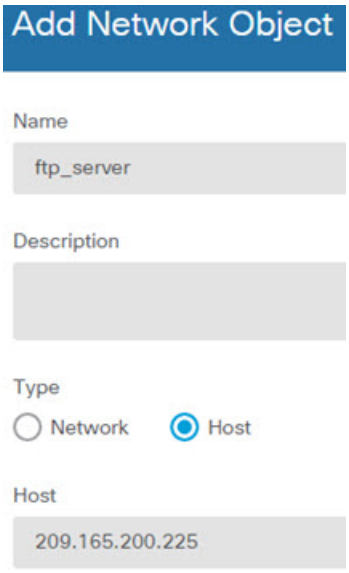
ステップ 1 FTP サーバ、DNS サーバ、内部ネットワーク、および PAT プール用のネットワーク オブジェクトを作成します。

a) [オブジェクト（Objects）] を選択します。

b) コンテンツ 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) 実際の FTP サーバ アドレスを定義します。

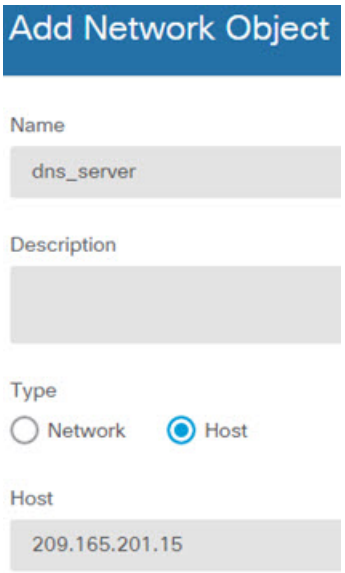
ネットワーク オブジェクトに名前を付け（例：ftp_server）、[ホスト（Host）] を選択して、実際の IP アドレス「209.165.200.225」を入力します。



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。

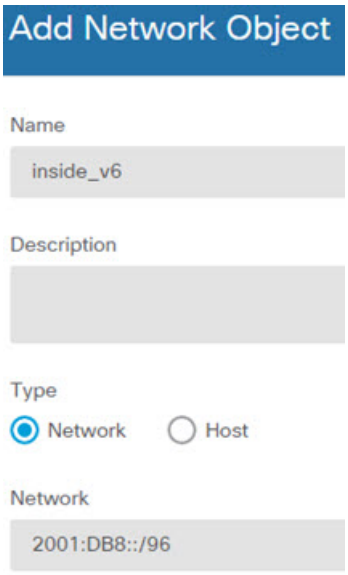
ネットワーク オブジェクトに名前を付け（例：dns_server）、[ホスト（Host）] を選択して、ホスト アドレス「209.165.201.15」を入力します。



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。

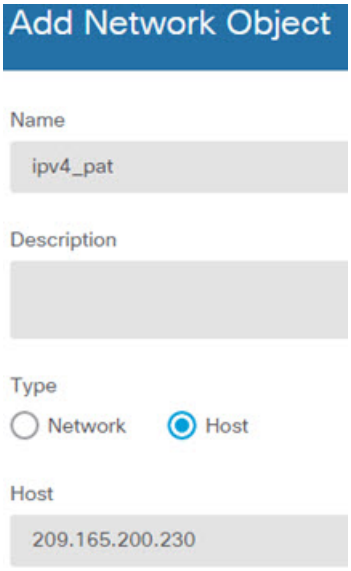
ネットワーク オブジェクトに名前を付け（例：inside_v6）、[ネットワーク（Network）] を選択し、ネットワーク アドレス 2001:db8::/96 を入力します。



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（例：ipv4_pat）、[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 サーバ用の DNS 修正を設定したスタティック NAT ルールを設定します。

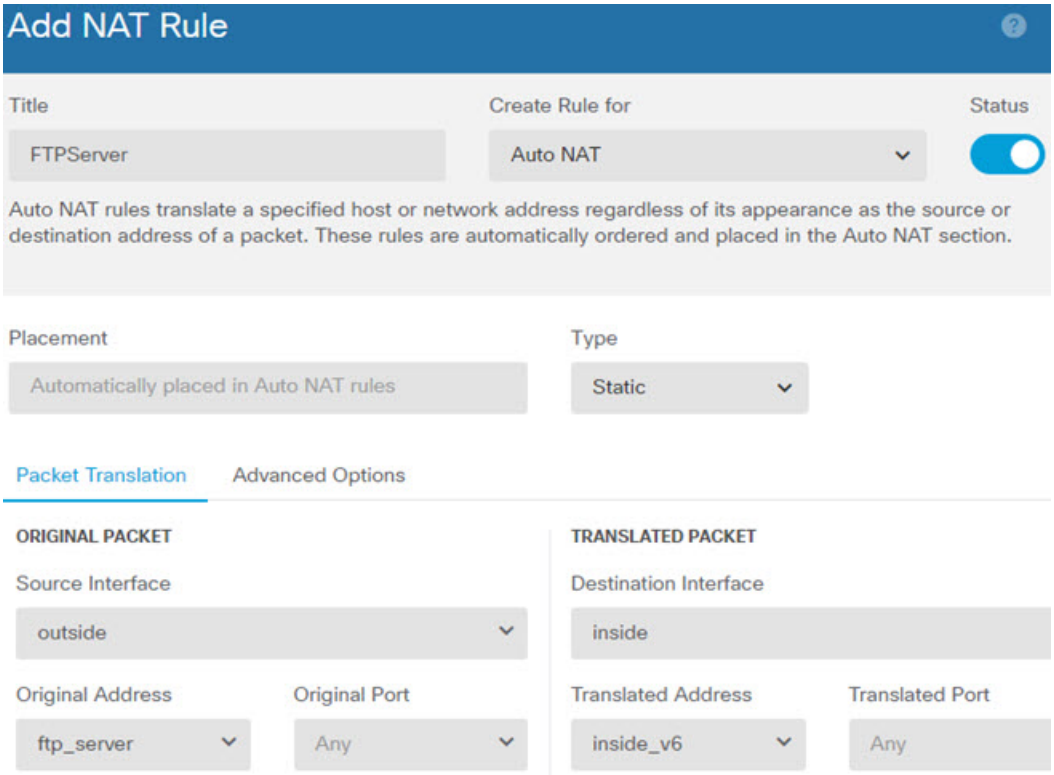
a) **[ポリシー（Policies）]** > **[NAT]** を選択します。

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）

- [ルールの作成対象（Create Rule For）] = [自動 NAT（Auto NAT）]。
- [種類（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 ネットワーク オブジェクト。
- [変換済みアドレス（Translated Address）]：inside_v6 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際に IPv4 埋め込みアドレス方式が使用されているため、209.165.200.225 は IPv6 でこれに相当する 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 になります。
- [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。



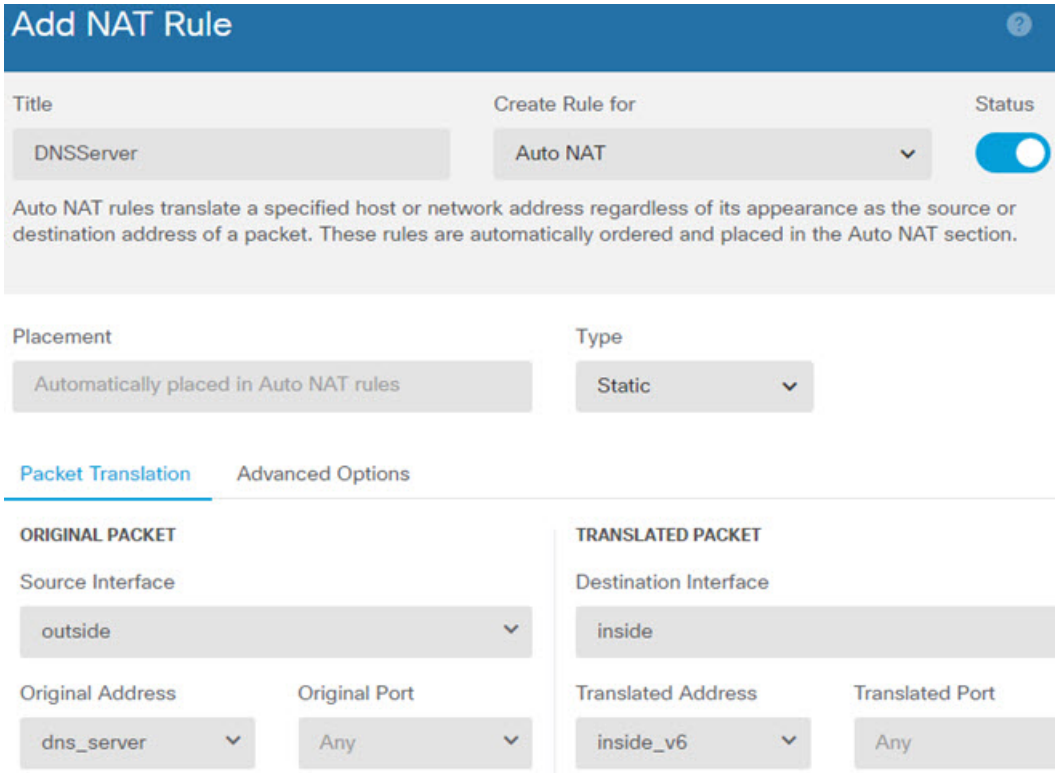
d) [OK] をクリックします。

ステップ 3 DNS サーバ用のスタティック 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）。

- [ルールの作成対象（Create Rule For）] = [自動 NAT（Auto NAT）]。
- [種類（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 ネットワーク オブジェクト。
- [変換済みアドレス（Translated Address）]：inside_v6 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際に IPv4 埋め込みアドレス方式が使用されているため、209.165.201.15 は IPv6 でこれに相当する 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 になります。



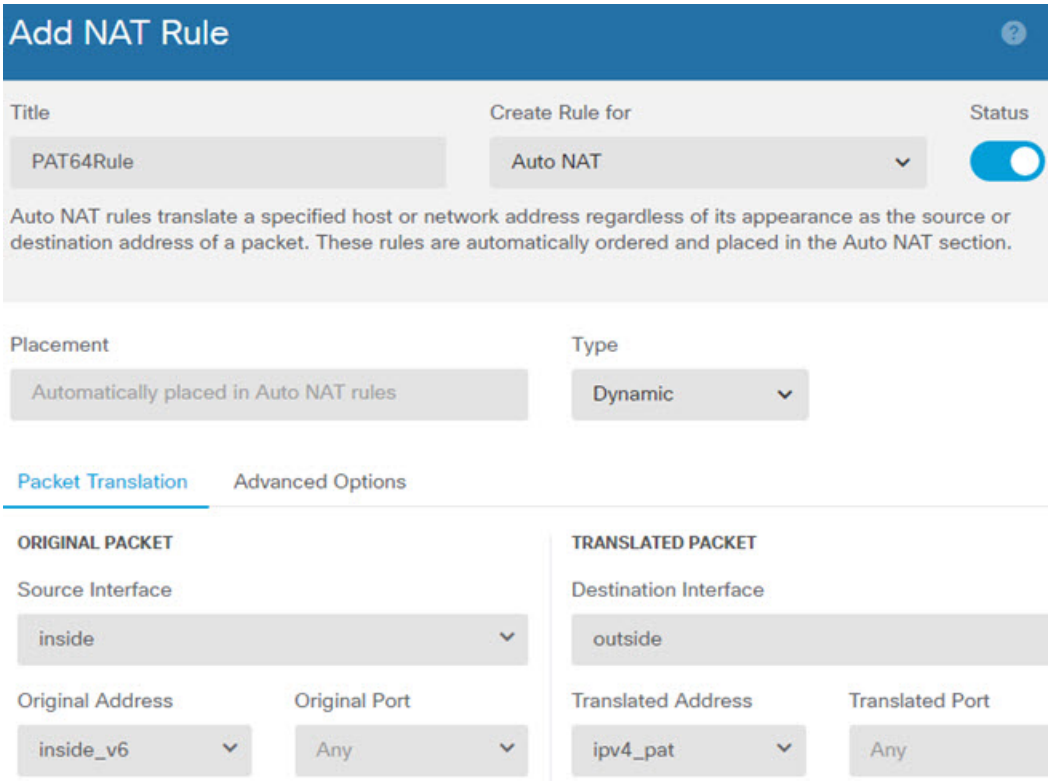
d) [OK] をクリックします。

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（またはユーザーが選択する別の名前）
- [ルールの作成対象（Create Rule For）] = [自動 NAT（Auto NAT）]。
- [種類（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。
- [変換済みアドレス（Translated Address）]：[ipv4_pat] ネットワーク オブジェクト。



d) **[OK]** をクリックします。

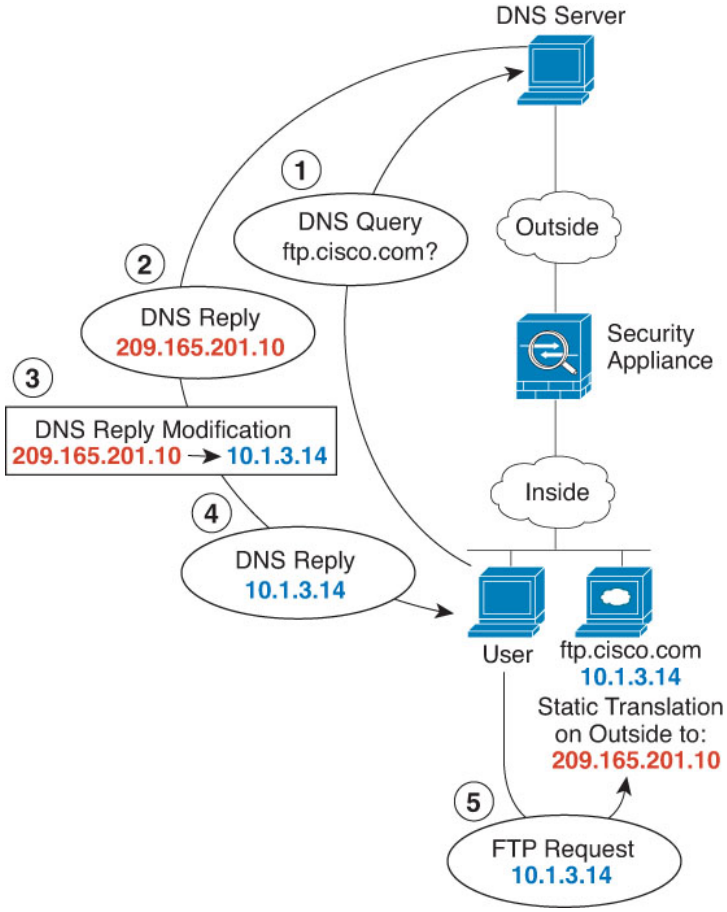
DNS 応答修正、外部の DNS サーバ

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

この場合、このスタティック ルールで DNS 応答修正をイネーブルにする必要があります。これにより、実際のアドレスを使用して ftp.cisco.com にアクセスすることを許可されている内部ユーザは、マッピング アドレスではなく実際のアドレスを DNS サーバから受信できるようになります。

内部ホストが ftp.cisco.com のアドレスを求める DNS 要求を送信すると、DNS サーバは応答でマッピング アドレス（209.165.201.10）を示します。システムは、内部サーバのスタティック

ルールを参照し、DNS 応答内のアドレスを 10.1.3.14 に変換します。DNS 応答修正をイネーブルにしない場合、内部ホストは ftp.cisco.com に直接アクセスする代わりに、209.165.201.10 にトラフィックを送信することを試みます。



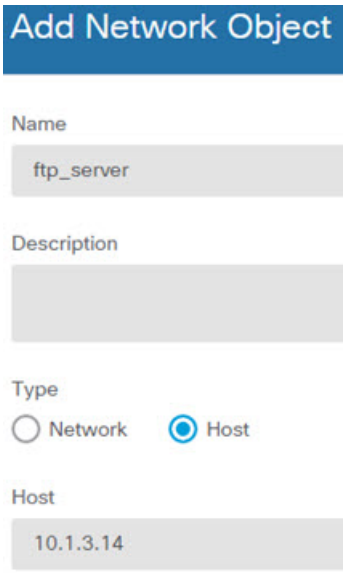
（注） この例では、内部インターフェイスがブリッジグループインターフェイス（BVI）ではなく、標準的なルーテッドインターフェイスであることを想定しています。内部インターフェイスが BVI の場合は、メンバー インターフェイスごとにルールを複製する必要があります。

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。

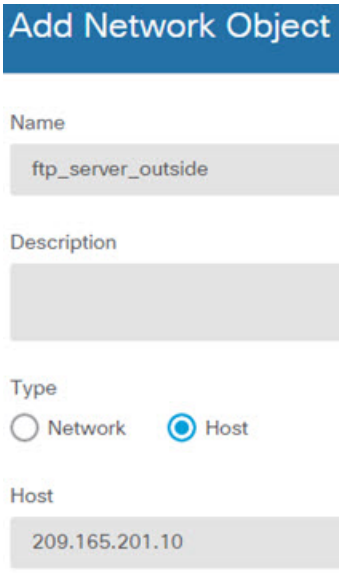
a) [オブジェクト（Objects）] を選択します。
b) コンテンツ テーブルから [ネットワーク（Network）] を選択し、[+] をクリックします。
c) 実際の FTP サーバ アドレスを定義します。

ネットワーク オブジェクトに名前を付け（例：ftp_server ）、[ホスト（Host）] を選択して、実際の 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。

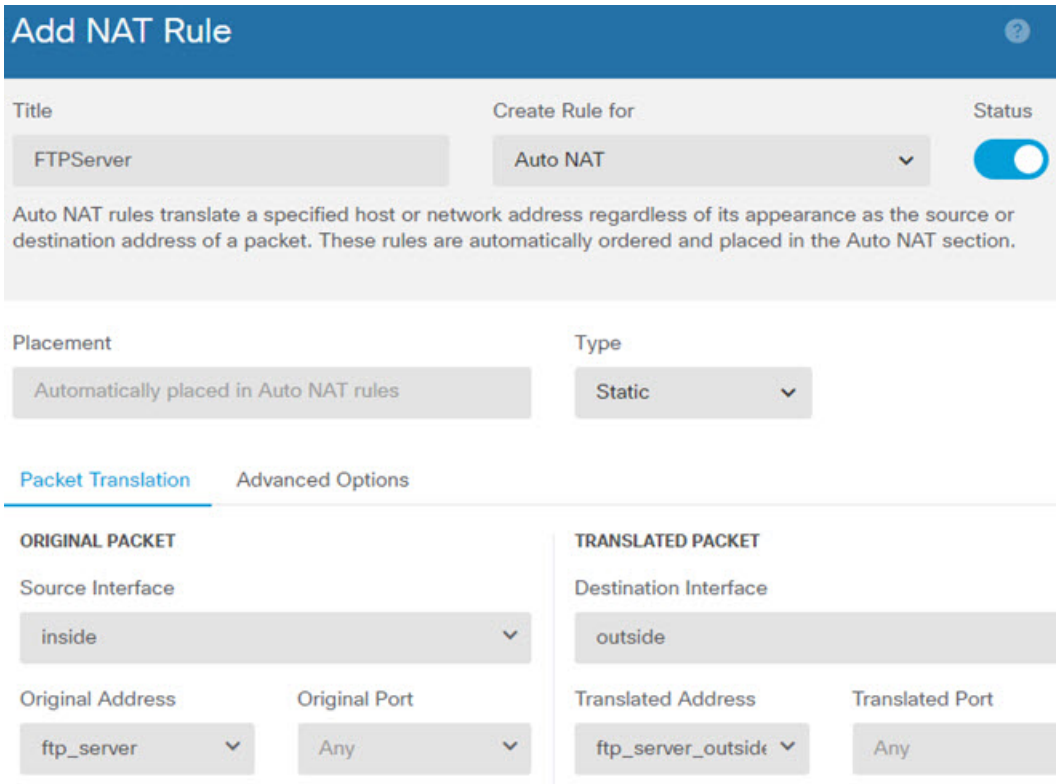
ネットワーク オブジェクトに名前を付け（例：ftp_server_outside）、[ホスト（Host）] を選択して、ホスト アドレス「209.165.201.10」を入力します。



ステップ 2 FTP サーバ用の 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）
- [ルールの作成対象（Create Rule For）] = [自動 NAT（Auto NAT）]。
- [種類（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 ネットワーク オブジェクト。
- [変換済みアドレス（Translated Address）]：ftp_server_outside 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。

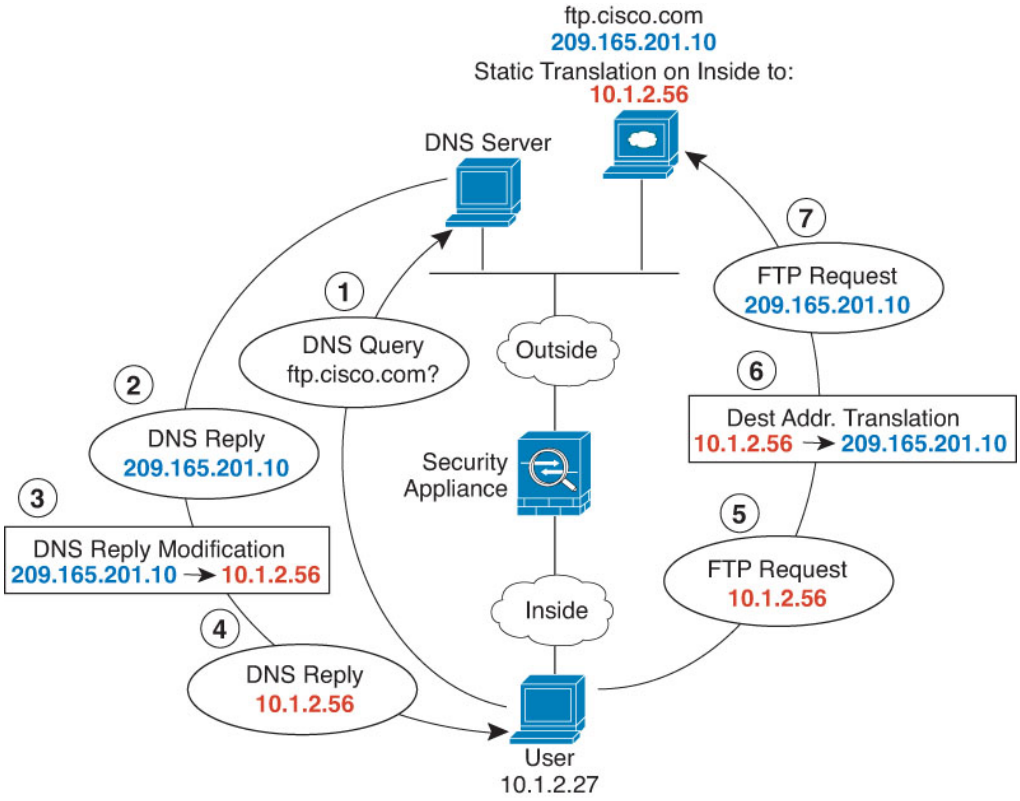


d) **[OK]** をクリックします。

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、標準的なルーテッドインターフェイスであることを想定しています。内部インターフェイスが BVI の場合は、メンバー インターフェイスごとにルールを複製する必要があります。

手順

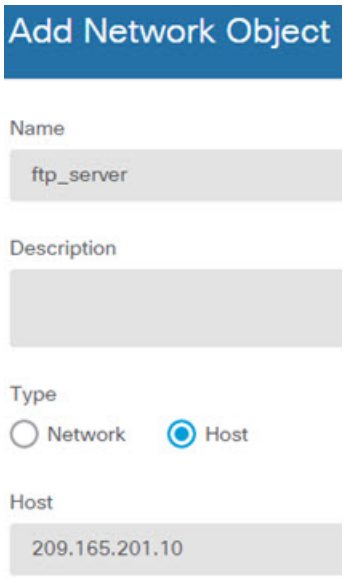
ステップ 1 FTP サーバのネットワーク オブジェクトを作成します。

a) [オブジェクト（Objects）] を選択します。

b) 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) 実際の FTP サーバ アドレスを定義します。

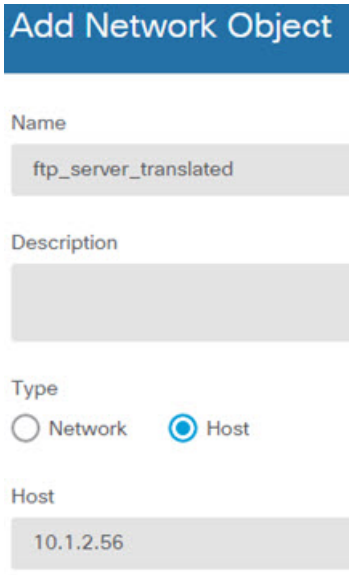
ネットワーク オブジェクトに名前を付け（例：ftp_server）、[ホスト（Host）] を選択して、実際の IP アドレス「209.165.201.10」を入力します。



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（例：ftp_server_translated）、[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 サーバ用の DNS 修正を設定したスタティック NAT ルールを設定します。

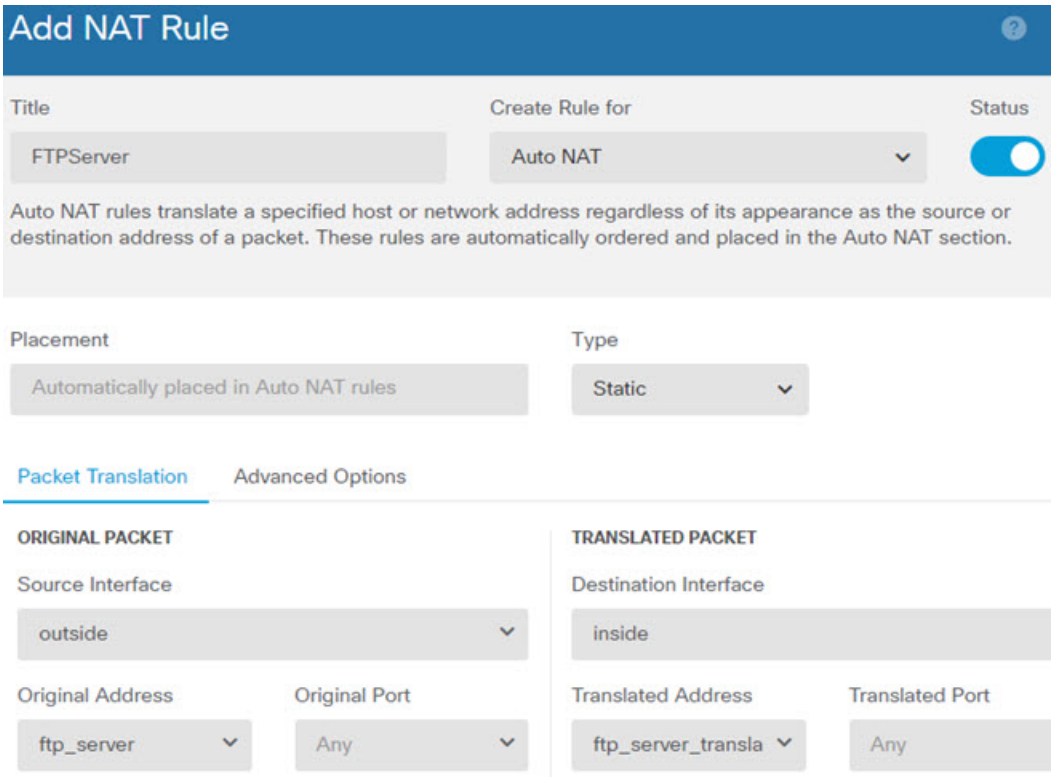
a) **[ポリシー（Policies）]** > **[NAT]** を選択します。

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）

- [ルールの作成対象（Create Rule For）] = [自動 NAT（Auto NAT）]。
- [種類（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 ネットワーク オブジェクト。
- [変換済みアドレス（Translated Address）]：ftp_server_translated 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。

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