ネットワーク アドレス変換（NAT）

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

NAT を使用する理由

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

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

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

NAT の他の機能は、次のとおりです。

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

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

NAT の基本

ここでは、NAT の基本について説明します。

NAT の用語

このマニュアルでは、次の用語を使用しています。

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

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

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

NAT タイプ

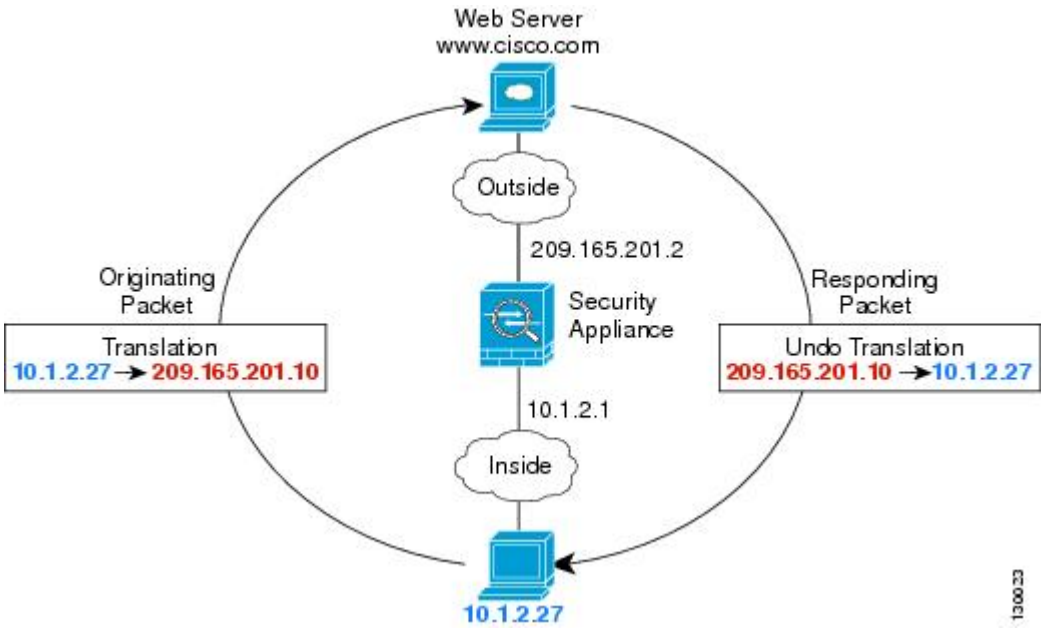
NAT は、次の方法を使用して実装できます。

- ダイナミック NAT：実際の IP アドレスのグループが、（通常は、より小さい）マッピング IP アドレスのグループに先着順でマッピングされます。実際のホストだけがトラフィックを開始できます。ダイナミック NAT, （15 ページ）を参照してください。
- ダイナミック ポート アドレス変換（PAT）：実際の IP アドレスのグループが、1 つの IP アドレスにマッピングされます。この IP アドレスの一意の送信元ポートが使用されます。ダイナミック PAT, （21 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, （27 ページ）を参照してください。
- アイデンティティ NAT：実際のアドレスが同一アドレスにスタティックに変換され、基本的に NAT をバイパスします。大規模なアドレスのグループを変換するものの、小さいアドレスのサブセットは免除する場合は、NAT をこの方法で設定できます。アイデンティティ NAT, （38 ページ）を参照してください。

ルーテッド モードの NAT

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

図 *1*：*NAT* の例：ルーテッド モード



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

/自動 NATと/手動 NAT

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

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

/自動 NAT

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

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

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

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

/手動 NAT

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

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

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

/自動 NAT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 ルールは、ネットワーク オブジェクトのパラメータとなります。ネットワーク オブジェクトの IP アドレスは元の（実際の）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 アドレスの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 つのルールが送信元と宛先の両方を変換します。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、一致するパケットは、1 つの /手動 NAT ルールのみに一致します。送信元および宛先は相互に結び付けられるため、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されます（/自動 NAT ルールの前または後）。

NAT ルールの順序

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

表 *1*：*NAT* ルール テーブル

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

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

- 192.168.1.0/24（スタティック）

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

この結果、使用される順序は次のとおりです。

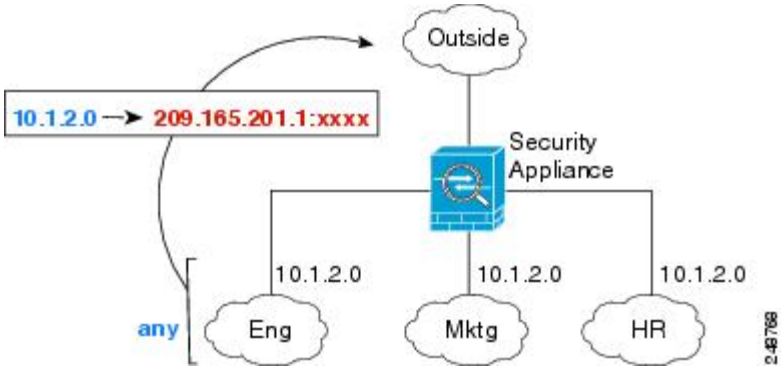
- 192.168.1.1/32（スタティック）
- 10.1.1.0/24（スタティック）
- 192.168.1.0/24（スタティック）
- 172.16.1.0/24（ダイナミック）（オブジェクト abc）
- 172.16.1.0/24（ダイナミック）（オブジェクト def）
- 192.168.1.0/24（ダイナミック）

NAT インターフェイス

ブリッジ グループ メンバー インターフェイスを除き、任意のインターフェイス（つまり、すべてのインターフェイス）に適用できるように NAT ルールを設定することも、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することもできます。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 アドレ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



NAT のルーティング設定

Firepower Threat Defense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の出力インターフェイスの決定に、指定した場合はその宛先インターフェイスが使用され、指定していない場合はルーティングテーブルルックアップが使用されます。アイデンティティ NAT では、宛先インターフェイスを指定していてもルート ルックアップを使用するオプションがあります。

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

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、Firepower Threat Defense デバイスをポイントするマッピング 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 は有効化され、他のスタティック NAT ルールと一致します。必要に応じてプロキシ ARP を無効にできます。必要に応じて標準スタティック NAT のプロキシ ARP を無効にできます。その場合は、アップストリーム ルータに適切なルートがあることを確認する必要があります。

アイデンティティ NAT の場合、通常はプロキシ ARP が不要で、場合によっては接続性に関する問題を引き起こす可能性があります。たとえば、「任意」の IP アドレスの広範なアイデンティティ NAT ルールを設定した場合、プロキシ ARP を有効のままにしておくと、マッピング インターフェイスに直接接続されたネットワーク上のホストの問題を引き起こすことがあります。この場合、マッピング ネットワークのホストが同じネットワークの他のホストと通信すると、ARP

要求内のアドレスは（「任意」のアドレスと一致する）NAT ルールと一致します。次に、実際には Firepower Threat Defense デバイス向けのパケットでない場合でも、Firepower Threat Defense デバイスはこのアドレスの ARP をプロキシします（この問題は、/手動 NATルールが設定されている場合にも発生します。NAT ルールは送信元と宛先のアドレス両方に一致する必要がありますが、プロキシ ARP 判定は「送信元」アドレスに対してのみ行われます）。実際のホストの ARP 応答の前に Firepower Threat Defense デバイスの ARP 応答を受信した場合、トラフィックは誤って Firepower Threat Defense デバイスに送信されます。

NAT のガイドライン

ここでは、NAT を実装するためのガイドラインについて詳細に説明します。

IPv6 NAT のガイドライン

NAT では、IPv6 のサポートに次のガイドラインと制限が伴います。

- 標準のルーテッド モードのインターフェイスの場合は、IPv4 と IPv6 との間でも変換できます。
- 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。

（注） 初期設定時に作成された Inside_Outside_Rule は、外部 IPv6 アドレスへの接続を阻止します。IPv6 を使用するときに PAT ルールをバイパスするには、それを編集して、内部 IPv4 ネットワークのネットワーク オブジェクトを送信元アドレスとして選択します。

IPv6 NAT の推奨事項

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

- NAT66（IPv6-to-IPv6）：スタティック NAT を使用することを推奨します。ダイナミック NAT または PAT を使用できますが、IPv6 アドレスは大量にあるため、ダイナミック NAT を使用する必要がありません。リターントラフィックを許可しない場合は、スタティック NAT ルールを単一方向にできます（/手動 NAT のみ）。
- NAT46（IPv4-to-IPv6）：スタティック NAT を使用することを推奨します。IPv6 アドレス空間は IPv4 アドレス空間よりもかなり大きいため、容易にスタティック変換に対応できます。

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

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

インスペクション対象プロトコルに対する NAT サポート

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

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

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

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

表 *2* : *NAT* のサポート対象アプリケーション インスペクション

アプリケーション	インスペクション対象プロトコル、ポート	NAT に関する制限事項	作成済みのピンホール
DCERPC	TCP/135	NAT64 なし。	あり
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。	なし
ESMTP	TCP/25	NAT64 なし。	なし
FTP	TCP/21	制限なし。	あり
H.323 H.225（コールシグナリング） H.323 RAS	TCP/1720 UDP/1718 RAS の場合、UDP/1718 ～ 1719	NAT64 なし。	あり
ICMP ICMP エラー	ICMP （デバイス インターフェイスに送信される ICMP トラフィックのインスペクションは実行されません。）	制限なし。	なし
IP オプション	RSVP	NAT64 なし。	なし
NetBIOS Name Server over IP	UDP/137、138（送信元ポート）	NAT64 なし。	なし
RSH	TCP/514	PAT なし。 NAT64 なし。	あり
RTSP	TCP/554 （HTTP クローキングは処理しません。）	NAT64 なし。	あり
SIP	TCP/5060 UDP/5060	拡張 PAT なし。 NAT64 または NAT46 なし。	あり
Skinny（SCCP）	TCP/2000	NAT64、NAT46、または NAT66 なし。	あり
SQL*Net （バージョン 1、2）	TCP/1521	NAT64 なし。	あり

アプリケーション	インスペクション対象プロトコル、ポート	NAT に関する制限事項	作成済みのピンホール
Sun RPC	UDP/111	NAT64 なし。	あり
TFTP	UDP/69	NAT64 なし。 ペイロード IP アドレスは変換されません。	あり
XDMCP	UDP/177	NAT64 なし。	あり

NAT のその他のガイドライン

- （/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。
- （/手動 NATのみ）送信元 IP アドレスがサブネットの場合は、FTP またはセカンダリ接続を使用する他のアプリケーションに対して宛先ポート変換を設定することはできません。FTP データ チャネルの確立は成功しません。
- NAT 設定を変更したときに、既存の変換がタイムアウトするまで待たずに新しい NAT 設定が使用されるようにするには、デバイスの CLI で **clear xlate** コマンドを使用して変換テーブルを消去できます。ただし、変換テーブルを消去すると、変換を使用している現在の接続がすべて切断されます。

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

- 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含め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のみを含める必要があります。
- （/手動NATのみ）NATルールで送信元アドレスとして **any** を使用する場合、"any" トラフィックの定義（IPv4 と IPv6）はルールによって異なります。Firepower Threat Defense デバイスがパケットに対して NAT を実行する前に、パケットが IPv6-to-IPv6 または IPv4-to-IPv4 である必要があります。この前提条件では、Firepower Threat Defense デバイスが、NAT ルールの **any** の値を決定できます。たとえば、"any" から IPv6 サーバへのルールを設定しており、このサーバが IPv4 アドレスからマッピングされている場合、**any** は「任意の IPv6 トラフィック」を意味します。"any" から "any" へのルールを設定しており、送信元をインターフェイス

IPv4 アドレスにマッピングする場合、マッピング インターフェイスのアドレスによって宛先も IPv4 であることが示されるため、**any** は「任意の IPv4 トラフィック」を意味します。

- 同じマッピング オブジェクトやグループを複数の NAT ルールで使用できます。
- マッピング IP アドレス プールに、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。
- スタティックおよびダイナミック NAT ポリシーでは重複アドレスを使用しないでください。たとえば、重複アドレスを使用すると、PPTP のセカンダリ接続がダイナミック xlate ではなくスタティックにヒットした場合、PPTP 接続の確立に失敗する可能性があります。
- ルールで宛先インターフェイスを指定すると、ルーティング テーブルでルートが検索されるのではなく、そのインターフェイスが出力インターフェイスとして使用されます。ただし、アイデンティティ NAT の場合は、代わりにルート ルックアップを使用するオプションがあります。

NAT の設定

ネットワーク アドレス変換は非常に複雑な場合があります。変換の問題やトラブルシューティングが困難な状況を避けるため、ルールはできるだけシンプルにすることを推奨します。NAT を実装する前に注意深く計画することが重要です。次の手順では、基本的なアプローチを示します。

手順

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

ステップ 2 必要なルールを決定します。
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 ルールを作成できます。概要については、「NAT タイプ, （3 ページ）」を参照してください。

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

ステップ 4 次のセクションで説明するルールを作成します。

- ダイナミック NAT, （15 ページ）
- ダイナミック PAT, （21 ページ）
- スタティック NAT, （27 ページ）

- アイデンティティ NAT, （38 ページ）

ステップ 5 NAT ポリシーとルールを管理します。
ポリシーとそのルールを管理するには、次のことを行います。

- ルールを編集するには、ルールの [編集（edit）] アイコン（）をクリックします。
- ルールを削除するには、ルールの [削除（delete）] 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。

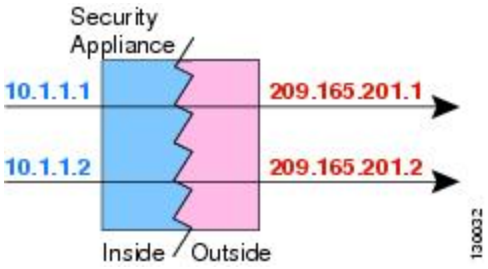
ダイナミック NAT について

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、NAT は、マッピングされたプールから IP アドレスをそのホストに割り当てます。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） 変換が継続している間、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。

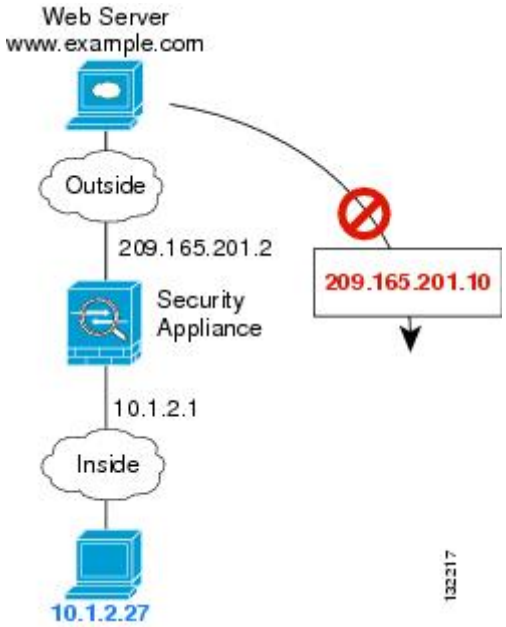
次の図に、一般的なダイナミック NAT のシナリオを示します。実際のホストだけが NAT セッションを作成でき、応答トラフィックが許可されます。

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。

  PAT では、1 つの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、このイベントが頻繁に発生する場合は、PAT または PAT のフォールバック方式を使用します。

- 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、一部のプロトコルが PAT を使用できないということです。たとえば、PAT は次の場合は機能しません。

- 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 プロトコルでは機能しません。
- 一部のマルチメディア アプリケーションなどのように、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ち、公開規格ではないアプリケーションでも機能しません。

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、宛先ネットワーク上でルーティング可能な別の IP アドレスにアドレスを変換します。

はじめる前に

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

- [元のアドレス（Original Address）]：グループではなくネットワーク オブジェクトである必要があり、ホストやサブネットを指定できます。
- [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 アドレスの両方を含めることはできません。1 つのタイプだけ含める必要があります。

手順

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

ステップ 2 次のいずれかを実行します。

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

（不要になったルールを削除するには、そ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 基本ルールのオプションを設定します。

- [タイトル（Title）]：ルールの名前を入力します。
- [ルールの作成対象（Create Rule For）]：[自動 NAT（Auto NAT）] を選択します。
- [タイプ（Type）]：[動的（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）]：この NAT ルールを適用するインターフェイス。[送信元（Source）]は、デバイスに入るトラフィックが通過する実際のインターフェイスです。[宛先（Destination）]は、デバイスから出るトラフィックが通過するマッピング インターフェイスです。デフォルトでは、ブリッジ グループ メンバー インターフェイスを除き、ルールはすべてのインターフェイスに適用されます（[すべて（Any）]）。
- [元のアドレス（Original 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。

- [変換済みアドレス（Translated Address）]：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。

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て、目的のオプションを選択します。

- [このルールと一致する DNS 応答を変換（Translate DNS replies that match this rule）]：DNS 応答の 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 インターフェイスに移動する 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状況で使用され、書き換えにより A レコードと AAAA レコード間でも変換が行われる NAT64/46 変換のために必要なことがあります。詳細については、NAT を使用した DNS クエリーのリライトと応答, （85 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））]：その他のマッピング アドレスがすでに割り当てられている場合に、宛先インターフェイスの IP アドレスをバックアップ方式として使用するかどうかを指定します（インターフェイス PAT フォールバック）。このオプションは、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

自動 NAT がお客様のニーズを満たしていない場合は、ダイナミック手動 NAT ルールを使用します。たとえば、宛先に基づいて別の変換を行いたい場合に使用します。ダイナミック NAT は、宛先ネットワーク上でルーティング可能な別の IP アドレスにアドレスを変換します。

はじめる前に

[オブジェクト（Objects）]を選択して、ルールに必要なネットワーク オブジェクトまたはグループを作成します。グループに IPv4 アドレスと IPv6 アドレスの両方を含めることはできません。1 つのタイプだけが含まれている必要があります。あるいは、NAT ルールを定義しているときにオブジェクトを作成することもできます。オブジェクトは次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、ホストやサブネットを含めることができます。元の送信元トラフィックをすべて変換する場合は、この手順をスキップして、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。

ルールにアドレスのスタティック変換を設定している場合、[元の宛先アドレス（Original Destination Address）]と [変換済み宛先アドレス（Translated Destination Address）] のネットワーク オブジェクトも作成できます。

ダイナミック NAT の場合、宛先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、[元の宛先ポート（Original Destination Port）]と [変換済み宛先ポート（Translated Destination Port）]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] を選択します。

ステップ 2 次のいずれかを実行します。

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

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

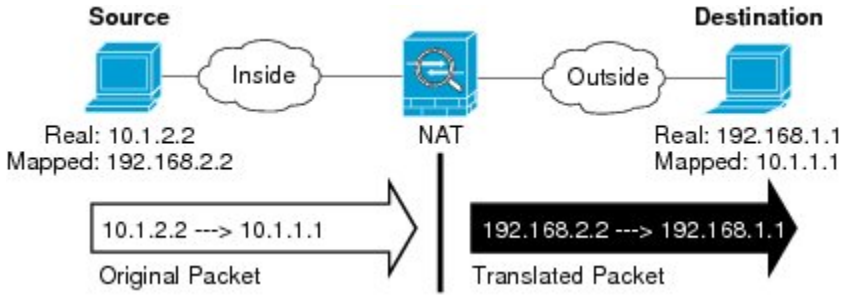
ステップ 3 基本ルールのオプションを設定します。

- [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を指定します。ルールはカテゴリ内（自動 NAT のルールの前後）、または選択するルールの上下に挿入できます。
- [タイプ（Type）] : [動的（Dynamic）]を選択します。この設定は、送信元アドレスにのみ適用されます。宛先アドレスの変換を定義している場合、変換は常に静的に行われます。

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）] : この NAT ルールを適用するインターフェイス。[送信元（Source）]は、デバイスに入るトラフィックが通過する実際のインターフェイスです。[宛先（Destination）]は、デバイスから出るトラフィックが通過するマッピング インターフェイスです。デフォルトでは、ブリッジ グループ メンバー インターフェイスを除き、ルールはすべてのインターフェイスに適用されます（[すべて（Any）]）。

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済みパケットの例については、次の図を参照してください。



- [元の送信元アドレス（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）]：（任意）。宛先のアドレスを含むネットワーク オブジェクト。空白のままにすると、宛先に関係なく、送信元アドレスの変換が適用されます。宛先アドレスを指定した場合、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 を使用することができます。

  [インターフェイス（Interface）][送信元インターフェイス IP（Source Interface IP）]を選択して、送信元インターフェイスの元の宛先（[すべて（Any）] は選択不可）をベースにすることができます。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。宛先アドレスに対して、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 を実装するには、このオプションを選択し、宛先ポートに適したポート オブジェクトも選択します。

ステップ 6 変換済みパケット アドレス（つまり、IPv4 または IPv6）を特定します。パケット アドレスは、宛先インターフェイス ネットワークに表示されます。必要に応じて、IPv4 と IPv6 の間で変換できます。

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

ステップ 7 （オプション）サービス変換の宛先サービス ポートを特定します。[元の宛先ポート（Original Destination Port）]、[変換済み宛先ポート（Translated Destination Port）]。
ダイナミック NAT はポート変換をサポートしていないため、[元の送信元ポート（Original Source Port）]フィールドと [変換済み送信元ポート（Translated Source Port）] フィールドは空白のままにする必要があります。ただし、宛先変換は常にスタティックであるため、宛先ポートに対してポート変換を実行できます。

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

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

- [このルールと一致する DNS 応答を変換（Translate DNS replies that match this rule）]：DNS 応答の 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 インターフェイスに移動する 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状況で使用され、書き換えにより A レコードと AAAA レコード間でも変換が行われる NAT64/46 変換のために必要なことがあります。詳細については、NAT を使用した DNS クエリーのリライトと応答,（85 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））]：その他のマッピング アドレスがすでに割り当てられている場合に、宛先インターフェイスの IP アドレスをバックアップ方式として使用するかどうかを指定します（インターフェイス PAT フォールバック）。このオプションは、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

次のトピックでは、ダイナミック PAT について説明します。

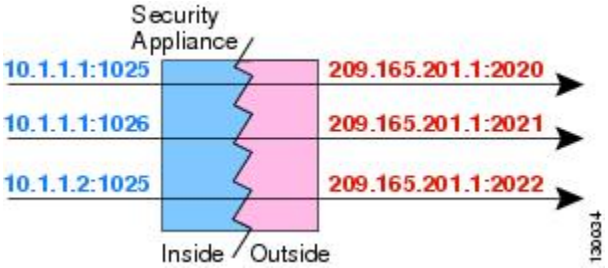
ダイナミック PAT について

ダイナミック PAT 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。使用できる場合、実際の送信元ポート番号がマッピング ポートに対して使用されます。ただし、実際のポートが使用できない場合は、デフォルトで、マッピング ポートは実際のポート番号と同じポート範囲（0 ～ 511、512 ～ 1023、および 1024 ～ 65535）から選択されます。そのため、1024 よりも下のポートでは、小さい PAT プールのみを使用できます。

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。

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、Firepower 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することもできます。ただし、インターフェイス PAT をインターフェイスの IPv6 アドレスのために使用することはできません。

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、インスペクション対象プロトコルに対する NAT サポート，（11 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、複数の IP アドレスのみに変換するのではなく、固有の IP アドレスとポートの組み合わせにアドレスを変換します。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。

はじめる前に

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

- [元のアドレス（Original Address）]：グループではなくネットワーク オブジェクトである必要があり、ホストやサブネットを指定できます。
- [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。
  - [宛先インターフェイス（Destination Interface）]：宛先インターフェイスの IPv4 アドレスを使用する場合、ネットワーク オブジェクトは必要ありません。インターフェイス PAT は IPv6 には使用できません。
  - [単一の PAT アドレス（Single PAT address）]：単一のホストを含むネットワーク オブジェクトを作成します。

手順

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

ステップ 2 次のいずれかを実行します。

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

（不要になったルールを削除するには、そ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 基本ルールのオプションを設定します。

- [タイトル（Title）]：ルールの名前を入力します。
- [ルールの作成対象（Create Rule For）]：[自動 NAT（Auto NAT）] を選択します。
- [タイプ（Type）]：[動的（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）]：この NAT ルールを適用するインターフェイス。[送信元（Source）]は、デバイスに入るトラフィックが通過する実際のインターフェイスです。[宛先（Destination）]は、デバイスから出るトラフィックが通過するマッピング インターフェイスです。デフォルトでは、ブリッジ グループ メンバー インターフェイスを除き、ルールはすべてのインターフェイスに適用されます（[すべて（Any）]）。
- [元のアドレス（Original 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。
- [変換済みアドレス（Translated Address）]：次のいずれかになります。
  - （インターフェイス PAT）。宛先インターフェイスの IPv4 アドレスを使用する場合は、[インターフェイス（Interface）]を選択します。特定の宛先インターフェイスを選択することもできます。。インターフェイス PAT は IPv6 には使用できません。

- 宛先インターフェイスのアドレス以外の単一アドレスを使用する場合は、そのために作成したホスト 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て、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（宛先インターフェイス）（Fallthrough to Interface PAT（Destination Interface））]：その他のマッピング アドレスがすでに割り当てられている場合に、宛先インターフェイスの IP アドレスをバックアップ方式として使用するかどうかを指定します（インターフェイス PAT フォールバック）。このオプションは、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。インターフェイス PAT を変換済みアドレスとしてすでに設定している場合、このオプションは選択できません。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

自動 PAT がお客様のニーズを満たしていない場合は、ダイナミック手動 PAT ルールを使用します。たとえば、宛先に基づいて別の変換を行いたい場合に使用します。ダイナミック PAT は、複数の IP アドレスのみに変換するのではなく、固有の IP アドレスとポートの組み合わせにアドレスを変換します。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。

はじめる前に

[オブジェクト（Objects）]を選択して、ルールに必要なネットワーク オブジェクトまたはグループを作成します。グループに IPv4 アドレスと IPv6 アドレスの両方を含めることはできません。1 つのタイプだけが含まれている必要があります。あるいは、NAT ルールを定義しているときにオブジェクトを作成することもできます。オブジェクトは次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、ホストやサブネットを含めることができます。元の送信元トラフィックをすべて変換する場合は、この手順をスキップして、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）：PAT アドレスを指定するオプションは次のとおりです。
  - [宛先インターフェイス（Destination Interface）]：宛先インターフェイスの IPv4 アドレスを使用する場合、ネットワーク オブジェクトは必要ありません。インターフェイス PAT は IPv6 には使用できません。
  - [単一の PAT アドレス（Single PAT address）]：単一のホストを含むネットワーク オブジェクトを作成します。

ルールにアドレスのスタティック変換を設定している場合、[元の宛先アドレス（Original Destination Address）]と [変換済み宛先アドレス（Translated Destination Address）] のネットワーク オブジェクトも作成できます。

ダイナミック PAT の場合、宛先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、[元の宛先ポート（Original Destination Port）]と [変換済み宛先ポート（Translated Destination Port）]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] を選択します。

ステップ 2 次のいずれかを実行します。

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

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

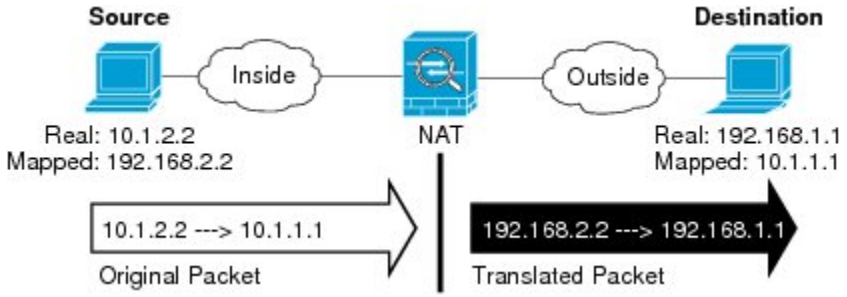
ステップ 3 基本ルールのオプションを設定します。

- [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を指定します。ルールはカテゴリ内（自動 NAT のルールの前後）、または選択するルールの上下に挿入できます。
- [タイプ（Type）] : [動的（Dynamic）]を選択します。この設定は、送信元アドレスにのみ適用されます。宛先アドレスの変換を定義している場合、変換は常に静的に行われます。

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）] : この NAT ルールを適用するインターフェイス。[送信元（Source）]は、デバイスに入るトラフィックが通過する実際のインターフェイスです。[宛先（Destination）]は、デバイスから出るトラフィックが通過するマッピング インターフェイスです。デフォルトでは、ブリッジ グループ メンバー インターフェイスを除き、ルールはすべてのインターフェイスに適用されます（[すべて（Any）]）。

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済みパケットの例については、次の図を参照してください。



- [元の送信元アドレス（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）]：（任意）。宛先のアドレスを含むネットワーク オブジェクト。空白のままにすると、宛先に関係なく、送信元アドレスの変換が適用されます。宛先アドレスを指定した場合、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 を使用することができます。

  [インターフェイス（Interface）][送信元インターフェイス IP（Source Interface IP）]を選択して、送信元インターフェイスの元の宛先（[すべて（Any）] は選択不可）をベースにすることができます。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。宛先アドレスに対して、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 を実装するには、このオプションを選択し、宛先ポートに適したポート オブジェクトも選択します。

ステップ 6 変換済みパケット アドレス（つまり、IPv4 または IPv6）を特定します。パケット アドレスは、宛先インターフェイス ネットワークに表示されます。必要に応じて、IPv4 と IPv6 の間で変換できます。

- [変換済み送信元アドレス（Translated Source Address）]：次のいずれかになります。
  - （インターフェイス PAT）。宛先インターフェイスの IPv4 アドレスを使用する場合は、[インターフェイス（Interface）]を選択します。特定の宛先インターフェイスを選択することもできます。。インターフェイス PAT は IPv6 には使用できません。
  - 宛先インターフェイスのアドレス以外の単一アドレスを使用する場合は、そのために作成したホスト ネットワーク オブジェクトを選択します。
- [変換済み宛先アドレス（Translated Destination Address）]：（任意）。変換済みパケットで使用されていた宛先アドレスを含むネットワーク オブジェクトまたはグループ。[元の宛先（Original Destination）]のオブジェクトを選択した場合、同じオブジェクトを選択してアイデンティティ NAT を設定できます（つまり、変換は不要です）。

ステップ 7 （オプション）サービス変換の宛先サービス ポートを特定します。[元の宛先ポート（Original Destination Port）]、[変換済み宛先ポート（Translated Destination Port）]。
ダイナミック NAT はポート変換をサポートしていないため、[元の送信元ポート（Original Source Port）]フィールドと [変換済み送信元ポート（Translated Source Port）] フィールドは空白のままに

する必要があります。ただし、宛先変換は常にスタティックであるため、宛先ポートに対してポート変換を実行できます。

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

ステップ 8 （オプション）[詳細オプション（Advanced Options）]リンクをクリックして、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（宛先インターフェイス）（Fallthrough to Interface PAT（Destination Interface））]：その他のマッピング アドレスがすでに割り当てられている場合に、宛先インターフェイスの IP アドレスをバックアップ方式として使用するかどうかを指定します（インターフェイス PAT フォールバック）。このオプションは、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。インターフェイス PAT を変換済みアドレスとしてすでに設定している場合、このオプションは選択できません。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

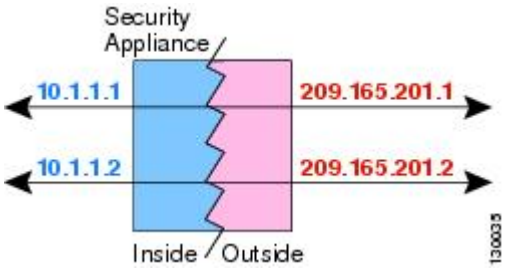
ここでは、スタティック NAT とその実装方法について説明します。

スタティック NAT について

スタティック NAT 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であるため、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、各ホストが以降の各変換に対して異なるアドレスまたはポートを使用するため、双方向の開始はサポートされません。

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であるため、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*



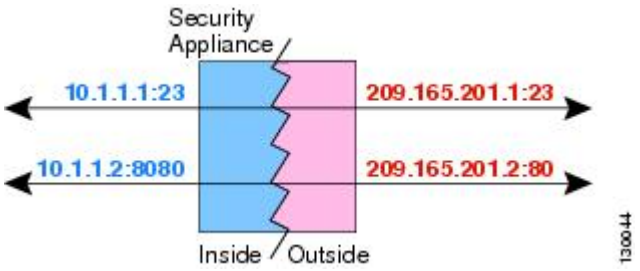
ポート変換を設定したスタティック NAT

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

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

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

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



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

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

アイデンティティ ポート変換を設定したスタティック NAT

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

標準以外のポートのポート変換を設定したスタティック NAT

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

ポート変換を設定したスタティック インターフェイス NAT

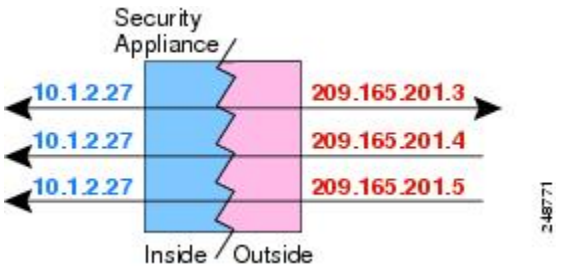
スタティックNATは、実際のアドレスをインターフェイス アドレスとポートの組み合わせにマッピングするように設定できます。たとえば、デバイスの外部インターフェイスへの Telnet アクセスを内部ホストにリダイレクトする場合、内部ホストの IP アドレス/ポート 23 を外部インターフェイス アドレス/ポート 23 にマッピングできます。

一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。

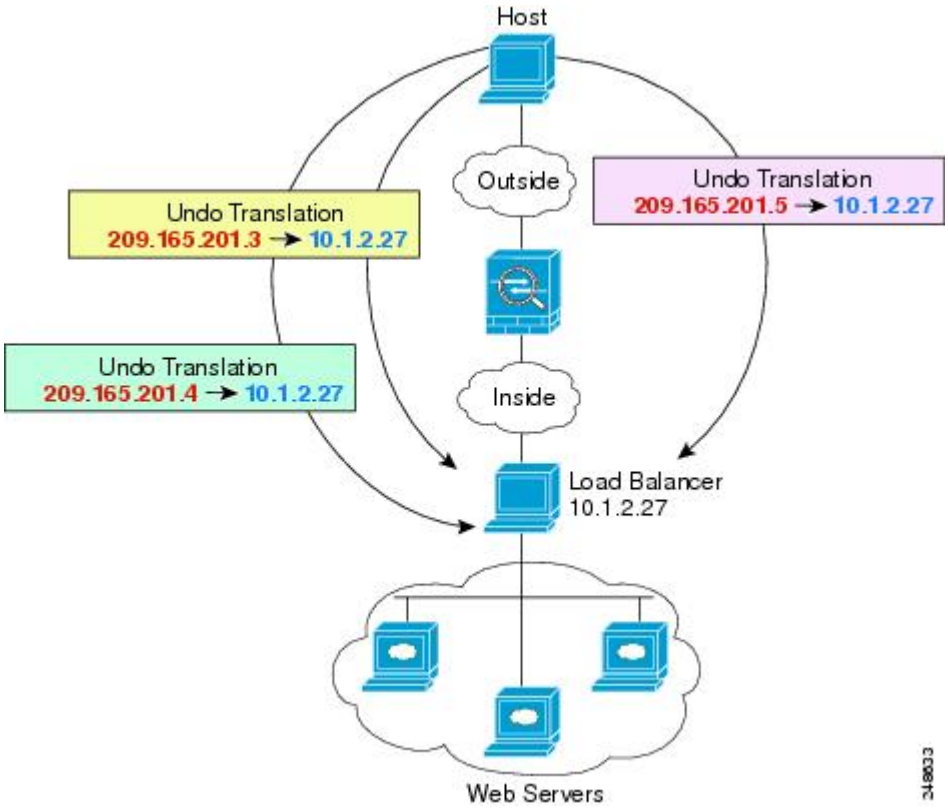
次の図に、一般的な一対多のスタティック NAT シナリオを示します。実際のホストが開始すると、常に最初のマッピング アドレスが使用されるため、実際のホスト IP/最初のマッピング IP の変換は、理論的には双方向変換のみが行われます。

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



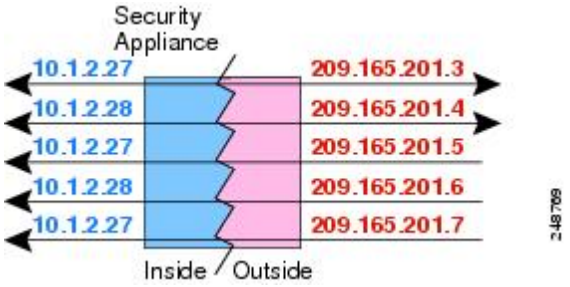
他のマッピング シナリオ（非推奨）

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。これらの他のマッピング オプションは、予期しない結果が発生する可能性があります。

機能的には、少対多は 1 対多と同じです。ただし、設定が複雑になり、実際のマッピングがひと目で明らかにならない可能性があるため、必要とする実際の各アドレスに対して 1 対多の設定を作成することをお勧めします。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、次のマッピング アドレスが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 対多の設定のように、最初のマッピングだけが双方向であり、以降のマッピングでは、実際のホストへのトラフィックを開始できますが、実際のホストからのすべてのトラフィックは、送信元の最初のマッピング アドレスだけを使用できます。

次の図に、一般的な少対多のスタティック NAT シナリオを示します。

図 *10*：少対多のスタティック *NAT*



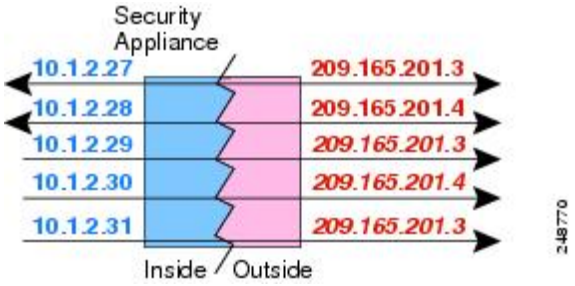
多対少または多対 1 の設定では、マッピング アドレスよりも多くの実際のアドレスが存在します。実際のアドレスが不足するよりも前に、マッピング アドレスが不足します。双方向の開始を実現できるのは、最下位の実際のIPアドレスとマッピング プールの間でマッピングを行ったときだけです。残りの上位の実際のアドレスはトラフィックを開始できますが、これらへのトラフィックを開始できません。接続のリターン トラフィックは、接続の固有の 5 つの要素（送信元 IP、宛先IP、送信元ポート、宛先ポート、プロトコル）によって適切な実際のアドレスに転送されます。

（注）

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

次の図に、一般的な多対少のスタティック NAT シナリオを示します。

図 *11*：多対少のスタティック *NAT*



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

スタティック自動 NAT の設定

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上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 ルールでポートの変換もできます。

はじめる前に

[オブジェクト（Objects）]を選択し、ルールに必要なネットワーク オブジェクトまたはグループを作成します。または、NAT ルールを定義しながらオブジェクトを作成することもできます。オブジェクトは次の要件を満たす必要があります。

- [元のアドレス（Original Address）]：これはネットワーク オブジェクト（グループではない）でなければならず、ホストまたはサブネットも可能です。
- [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。
  - [宛先インターフェイス（destination interface）]：宛先インターフェイスの IPv4 アドレスを使用するには、ネットワーク オブジェクトは必要ありません。これはポート変換と共に、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 は使用できません。
  - [アドレス（Address）]：ホストまたはサブネットを含むネットワーク オブジェクトまたはグループを作成します。IPv4 アドレスと IPv6 アドレスの両方をグループに入れることはできません。1 つのタイプだけが含まれている必要があります。通常、1 対 1 のマッピングでは、実際のアドレスと同じ数のマッピング アドレスを設定します。しかし、アドレスの数が一致しない場合もあります。

手順

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

ステップ 2 次のいずれかを実行します。

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

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

ステップ 3 基本的なルール オプションを設定します。

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

- [タイプ（Type）]：[スタティック（Static）] を選択します。

ステップ 4 次のパケット変換オプションを設定します。

- [送信元インターフェイス（Source Interface）]、[宛先インターフェイス（Destination Interface）]：この NAT ルールを適用するインターフェイス。[送信元（Source）]は、デバイスに入るトラフィックが通過する実際のインターフェイスです。[宛先（Destination）]は、デバイスから出るトラフィックが通過するマッピング インターフェイスです。デフォルトでは、ブリッジ グループ メンバー インターフェイスを除き、ルールはすべてのインターフェイスに適用されます（[すべて（Any）]）。
- [元のアドレス（Original Address）]：変換するアドレスを含むネットワーク オブジェクト。
- [変換済みアドレス（Translated Address）]：次のいずれかになります。
  - アドレスの設定グループを使用するには、マッピング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。通常、1 対 1 のマッピングでは、実際のアドレスと同じ数のマッピングアドレスを設定します。しかし、アドレスの数が一致しない場合もあります。
  - （ポート変換を設定したスタティック インターフェイス NAT）。宛先のアドレスのインターフェイスを使用するには、[インターフェイス（Interface）]を選択します。また、特定の宛先インターフェイスを選択する必要があります。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）]、[Translated Port（変換済みポート）]：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用でなければなりません。そのオブジェクトがまだ存在しない場合、[新規オブジェクトの作成（Create New Object）]をクリックします。たとえば、必要に応じて TCP/80 を TCP/8080 に変換できます。

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

- [このルールに一致する DNS 応答を変換する（Translate DNS replies that match this rule）]：DNS 応答の 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 インターフェイスに移動する 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状況で使用され、書き換えにより A レコードと AAAA レコード間でも変換が行われる NAT64/46 変換のために必要なことがあります。詳細については、NAT を使用した DNS クエリーのリライトと応答, （85 ページ）を参照してください。 ポート変換している場合、このオプションは使用できません。

- [宛先インターフェイスで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。この方法だと、デバイスがその他のネットワークのゲートウェイになる必要がないため、ルーティングが簡略化されます。プロキシARPは必要に応じて無効にできます。無効にする場合、上流に位置するルータに適切なルートが設定されている必要があります。アイデンティティ NAT の場合、通常はプロキシ ARP は不要です。場合によっては接続の問題が生じることがあります。

ステップ 6 [OK]をクリックします。

スタティック手動 NAT の設定

自動 NAT がニーズを満たさない場合、スタティック手動 NAT ルールを使用します。たとえば、宛先に応じて異なる変換をしたい場合などです。スタティック NAT は、アドレスを宛先ネットワーク上でルーティング可能な別の IP アドレスに変換します。また、スタティック NAT ルールでポートの変換もできます。

はじめる前に

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

- [送信元アドレス（Original Address）]：これはネットワーク オブジェクトまたはグループで、ホストまたはサブネットを含むことができます。すべての元の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）]：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。
  - [宛先インターフェイス（destination interface）]：宛先インターフェイスの IPv4 アドレスを使用するには、ネットワーク オブジェクトは必要ありません。これはポート変換と共に、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 は使用できません。
  - [アドレス（Address）]：ホストまたはサブネットを含むネットワーク オブジェクトまたはグループを作成します。IPv4 アドレスと IPv6 アドレスの両方をグループに入れることはできません。1 つのタイプだけが含まれている必要があります。通常、1 対 1 のマッピングでは、実際のアドレスと同じ数のマッピング アドレスを設定します。しかし、アドレスの数が一致しない場合もあります。

ルールで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。ポート変換を設定した宛先のスタティック インターフェイス NAT のみを設定する場合は、宛先のマッピング アドレスに対するオブジェクトの追加をスキップでき、ルールでインターフェイスを指定します。

また送信元、宛先、またはその両方のポート変換も実行できます。Object Managerでは、元のポートと変換されたポートで使用できるポート オブジェクトがあることを確認します。

手順

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

ステップ 2 次のいずれかを実行します。

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

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

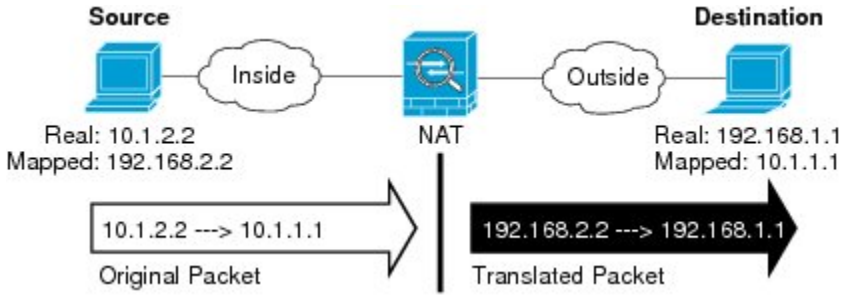
ステップ 3 基本的なルール オプションを設定します。

- [タイトル（Title）] ：ルールの名前を入力します。
- [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を指定します。ルールはカテゴリ内（自動 NAT のルールの前後）、または選択するルールの上下に挿入できます。
- [タイプ（Type）] : [スタティック（Static）] を選択します。この設定は送信元アドレスにのみ適用されます。宛先アドレスの変換を定義すると、変換は常にスタティックです。

ステップ 4 次のインターフェイス オプションを設定します。

- [送信元インターフェイス（Source Interface）]、[宛先インターフェイス（Destination Interface）] : この NAT ルールを適用するインターフェイス。[送信元（Source）]は、デバイスに入るトラフィックが通過する実際のインターフェイスです。[宛先（Destination）]は、デバイスから出るトラフィックが通過するマッピング インターフェイスです。デフォルトでは、ブリッジ グループ メンバー インターフェイスを除き、ルールはすべてのインターフェイスに適用されます（[すべて（Any）]）。

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済みパケットの例については、次の図を参照してください。



- [元の送信元アドレス（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）]：（任意）。宛先のアドレスを含むネットワーク オブジェクト。空白のままにすると、宛先に関係なく、送信元アドレスの変換が適用されます。宛先アドレスを指定した場合、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 を使用することができます。

  [インターフェイス（Interface）][送信元インターフェイス IP（Source Interface IP）]を選択して、送信元インターフェイスの元の宛先（[すべて（Any）] は選択不可）をベースにすることができます。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。宛先アドレスに対して、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 を実装するには、このオプションを選択し、宛先ポートに適したポート オブジェクトも選択します。

ステップ 6 変換されたパケット アドレス（IPv4 または IPv6）、すなわちそれが宛先インターフェイス ネットワーク上に現れるときのパケット アドレスを識別します。必要に応じて、IPv4 と IPv6 の間で変換できます。

- [変換済み送信元アドレス（Translated Source Address）]：次のいずれかになります。
  - アドレスの設定グループを使用するには、マッピング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。通常、1 対 1 のマッピングでは、実際のアドレスと同じ数のマッピング アドレスを設定します。しかし、アドレスの数が一致しない場合もあります。
  - （ポート変換を設定したスタティック インターフェイス NAT）。宛先の IPv4 アドレスのインターフェイスを使用するには、[インターフェイス（Interface）]を選択します。また、特定の宛先インターフェイスを選択する必要があります。これ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 は使用できません。
- [変換済み宛先アドレス（Translated Destination Address）]：（オプション）。変換されたパケットで使用される宛先アドレスを含むネットワーク オブジェクトまたはグループ。[元の

宛先（Original Destination）]を選択した場合、同じオブジェクトを選択することによって、アイデンティティ NAT（つまり変換なし）を設定できます。

ステップ 7 （オプション）サービス変換の送信元サービス ポートまたは宛先サービス ポートを識別します。ポート変換を設定したスタティック NAT を設定した場合、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 間を変換できます。

NAT では、TCP または UDP のみがサポートされますポートを変換する場合、実際のサービス オブジェクトのプロトコルとマッピング サービス オブジェクトのプロトコルの両方が同じになるようにします（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）]、[変換された送信元ポート（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）]、[変換された宛先ポート（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、希望するオプションを選択します。

- [このルールに一致する DNS 応答を変換する（Translate DNS replies that match this rule）]：DNS 応答の 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 インターフェイスに移動する 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状況で使用され、書き換えにより A レコードと AAAA レコード間でも変換が行われる NAT64/46 変換のために必要なことがあります。詳細については、NAT を使用した DNS クエリーのリライトと応答,（85 ページ）を参照してください。 ポート変換している場合、このオプションは使用できません。
- [宛先インターフェイスで 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。この方法だと、デバイスがその他のネットワークのゲートウェイになる必要がないため、ルーティングが簡略化されます。プロキシ ARP は必要に応じて無効にできます。無効にする場合、上流に位置するルータに適切なルートが設定されている必要があります。アイデンティティ NAT の場合、通常はプロキシ ARP は不要です。場合によっては接続の問題が生じることがあります。

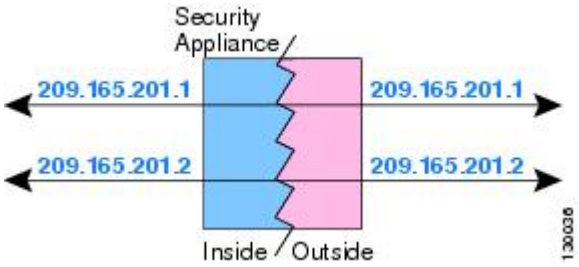
ステップ 9 [OK]をクリックします。

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、NAT を各ネットワークに適するものの、1 つのネットワークを NAT から除外するという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

スタティック アイデンティティ自動 NAT ルールを使用して、アドレスの変換を防止します。つまり、自身のアドレスに変換します。

はじめる前に

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

- [元のアドレス（Original Address）]：グループではなくネットワーク オブジェクトである必要があり、ホストやサブネットを指定できます。
- [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全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できます。

手順

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

ステップ 2 次のいずれかを実行します。

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

（不要になったルールを削除するには、そ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 基本ルールのオプションを設定します。

- [タイトル（Title）]：ルールの名前を入力します。
- [ルールの作成対象（Create Rule For）]：[自動 NAT（Auto NAT）] を選択します。
- [タイプ（Type）]：[静的（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）]：この NAT ルールを適用するインターフェイス。[送信元（Source）]は、デバイスに入るトラフィックが通過する実際のインターフェイスです。[宛先（Destination）]は、デバイスから出るトラフィックが通過するマッピング インターフェイスです。デフォルトでは、ブリッジ グループ メンバー インターフェイスを除き、ルールはすべてのインターフェイスに適用されます（[すべて（Any）]）。
- [元のアドレス（Original 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。
- [変換済みアドレス（Translated Address）]：元の送信元と同じオブジェクト。状況に応じて、コンテンツが全く同一の別のオブジェクトを選択できます。

アイデンティティ NAT には、[元のポート（Original Port）]オプションと [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）[詳細オプション（Advanced Options）]リンクをクリックして、目的の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プロキシ ARP を使用しない（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。この方法だと、デバイスがその他のネットワークのゲートウェイになる必要がないため、ルーティングが簡略化されます。プロキシARP は必要に応じて無効にできます。無効にする場合、上流に位置するルータに適切なルートが設定されている必要があります。アイデンティティ NAT の場合、通常はプロキシ ARP は不要です。場合によっては接続の問題が生じることがあります。
- [宛先インターフェイスのルート ルックアップを実行（Perform Route Lookup for Destination Interface）]：元の送信元アドレスと変換後の送信元アドレスに対して同じオブジェクトを選択している場合に、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して、NAT ルールに設定されている宛先インターフェイスを使用する代わ

りに、ルーティング テーブルに基づいて宛先インターフェイスを決めさせることができます。

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

自動 NAT がお客様のニーズを満たしていない場合は、スタティック アイデンティティ手動 NAT ルールを使用します。たとえば、宛先に基づいて別の変換を行いたい場合に使用します。スタティック アイデンティティ NAT ルールを使用して、アドレスの変換を防止します。つまり、自身のアドレスに変換します。

はじめる前に

[オブジェクト（Objects）]を選択して、ルールに必要なネットワーク オブジェクトまたはグループを作成します。グループに IPv4 アドレスと IPv6 アドレスの両方を含めることはできません。1 つのタイプだけが含まれている必要があります。あるいは、NAT ルールを定義しているときにオブジェクトを作成することもできます。オブジェクトは次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、ホストやサブネットを含めることができます。元の送信元トラフィックをすべて変換する場合は、この手順をスキップして、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）]：元の送信元と同じオブジェクト。状況に応じて、コンテンツが全く同一の別のオブジェクトを選択できます。

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

送信元、宛先、または両方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で使用できるポート 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 に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] を選択します。

ステップ 2 次のいずれかを実行します。

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

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

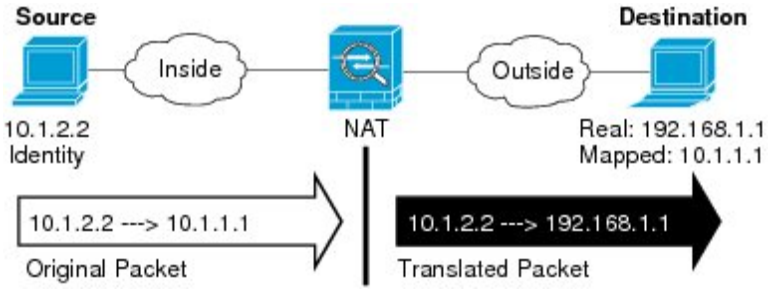
ステップ 3 基本ルールのオプションを設定します。

- [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を指定します。ルールはカテゴリ内（自動 NAT のルールの前後）、または選択するルールの上下に挿入できます。
- [タイプ（Type）]：[静的（Static）]を選択します。この設定は、送信元アドレスにのみ適用されます。宛先アドレスの変換を定義している場合、変換は常に静的に行われます。

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）]：この NAT ルールを適用するインターフェイス。[送信元（Source）]は、デバイスに入るトラフィックが通過する実際のインターフェイスです。[宛先（Destination）]は、デバイスから出るトラフィックが通過するマッピング インターフェイスです。デフォルトでは、ブリッジ グループ メンバー インターフェイスを除き、ルールはすべてのインターフェイスに適用されます（[すべて（Any）]）。

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済みパケットの例については、次の図を参照してください。ここでは、内部ホストでアイデンティティ NAT を実行しますが、外部ホストを変換します。



- [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）]：（任意）。宛先のアドレスを含むネットワーク オブジェクト。空白のままにすると、宛先に関係なく、送信元アドレスの変換が適用されます。宛先アドレスを指定した場合、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 を使用することができます。

  [インターフェイス（Interface）]を選択して、送信元インターフェイスの元の宛先（[すべて（Any）]は選択不可）をベースにすることができます。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。宛先アドレスに対して、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 を実装するには、このオプションを選択し、宛先ポートに適したポート オブジェクトも選択します。

ステップ 6 変換済みパケット アドレス（つまり、IPv4 または IPv6）を特定します。パケット アドレスは、宛先インターフェイス ネットワークに表示されます。必要に応じて、IPv4 と IPv6 の間で変換できます。

- [変換済み送信元アドレス（Translated Source Address）]：元の送信元と同じオブジェクト。状況に応じて、コンテンツが全く同一の別のオブジェクトを選択できます。
- [変換済み宛先アドレス（Translated Destination Address）]：（任意）。変換済みパケットで使用されていた宛先アドレスを含むネットワーク オブジェクトまたはグループ。[元の宛先アドレス（Original Destination Address）]のオブジェクトを選択した場合、同じオブジェクトを選択してアイデンティティ NAT を設定できます（つまり、変換は不要です）。

ステップ 7 （オプション）サービス変換の送信元サービス ポートまたは宛先サービス ポートを識別します。ポート変換を設定したスタティック NAT を設定している場合、送信元、宛先、または両方のポートを変換できます。たとえば、TCP/80 と TCP/8080 の間で変換できます。

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

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

ステップ 8 （オプション）[詳細オプション（Advanced Options）]リンクをクリックして、目的の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プロキシ ARP を使用しない（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。この方法だと、デバイスがその他のネットワークのゲートウェイになる必要がないため、ルーティングが簡略化されます。プロキシ ARP は必要に応じて無効にできます。無効にする場合、上流に位置するルータに適切なルートが設定されている必要があります。アイデンティティ NAT の場合、通常はプロキシ ARP は不要です。場合によっては接続の問題が生じることがあります。
- [宛先インターフェイスのルート ルックアップを実行（Perform Route Lookup for Destination Interface）]：元の送信元アドレスと変換後の送信元アドレスに対して同じオブジェクトを選

択している場合に、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して、NATルールに設定されている宛先インターフェイスを使用する代わりに、ルーティング テーブルに基づいて宛先インターフェイスを決めさせることができます。

ステップ 9 [OK]をクリックします。

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

ネットワークアドレス変換（NAT）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。通常は、NATルールを使用してプライベートアドレスをパブリックにルーティングできる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に変換するか、ポートアドレス変換（PAT）を使用して多数のアドレスを 1 つに変換し、ポート番号を使用して送信元アドレスを識別することができます。

NAT ルールの基本的なプロパティは、次のとおりです。プロパティは、指示されていることを除き、自動 NAT ルールと手動 NAT ルールで同じです。

役職（Title）

ルールの名前を入力します。名前にスペースを含めることはできません。

ルールの作成

変換ルールを [自動 NAT（Auto NAT）]にするか、[手動 NAT（Manual NAT）]にするか。自動 NAT は手動 NAT よりシンプルですが、手動 NAT を使用すると、宛先アドレスに基づいて送信元アドレスの個別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。

配置（Placement）（手動NAT のみ）

ルールを追加する場所を指定します。ルールはカテゴリ内（自動 NAT のルールの前後）、または選択するルールの上下に挿入できます。

タイプ（Type）

変換ルールを [ダイナミック（Dynamic）]にするか、[スタティック（Static）]にするか。ダイナミック変換では、アドレス プールからマッピング アドレスが自動的に選択されるか、または、PAT の実装時にはアドレス/ポートの組み合わせが自動的に選択されます。マッピングアドレス/ポートを明確に定義する必要がある場合は、スタティック変換を使用します。

次に、残りの NAT ルール プロパティを説明します。

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、送信元アドレスと変換済みマッピング 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（SourceInterface）、宛先インターフェイス（Destination Interface）

このNATルールを適用するインターフェイス。[送信元（Source）]は、デバイスに入るトラフィックが通過する実際のインターフェイスです。[宛先（Destination）]は、デバイスから出るトラフィックが通過するマッピング インターフェイスです。デフォルトでは、ブリッジ グループ メンバー インターフェイスを除き、ルールはすべてのインターフェイスに適用されます（[すべて（Any）]）。

元のアドレス（OriginalAddress）（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（TranslatedAddress）（通常は必須）

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

- ダイナミックNAT（Dynamic NAT）：マッピング アドレスを含むネットワーク オブジェクトまたはグループ。ネットワーク オブジェクトまたはグループ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。IPv4 アドレスと IPv6 アドレスの両方をグループに入れることはできません。1 つのタイプだけが含まれている必要があります。
- ダイナミックPAT（Dynamic PAT）：次のいずれかになります。
  - （インターフェイス PAT）宛先インターフェイスの IPv4 アドレスを使用するには、[インターフェイス（Interface）]を選択します。また、特定の宛先インターフェイスを選択する必要もあります。。IPv6 にインターフェイス PAT を使用することはできません。
  - 宛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、この目的のために作成したホスト 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）：次のいずれかになります。
  - アドレスのセット グループを使用するには、マッピング アドレスを含むネットワーク オブジェクトまたはグループを選択します。オブジェクトまたはグループに、ホストまたはサブネットを含めることができます。通常、1 対 1 のマッピングでは、実際のアドレスと同じ数のマッピング アドレスを設定します。しかし、アドレスの数が一致しない場合もあります。
  - （ポート変換を設定したスタティック インターフェイスNAT）宛先インターフェイスの IP アドレスを使用するには、[インターフェイス（Interface）]を選択します。また、特定の宛先インターフェイスを選択する必要もあります。。これによって、ポート変換を設定したスタティック インターフェイス NAT が設定されます。送信元アドレス/ポートは、インターフェイスのアドレスおよび同一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）：元の送信元と同じオブジェクト。オプションで、内容がまったく同じ別のオブジェクトを選択できます。

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

TCP または UDP ポートを変換する必要がある場合、元のポートおよび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向けにする必要があります。たとえば、必要に応じて TCP/80 を TCP/8080 に変換できます。

手動 NAT のパケット変換プロパティ

[パケット変換（Packet Translation）] オプションを使用して、送信元アドレスと変換済みマッピング 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。指示されている場合を除き、すべてオプションです。

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

このNATルールを適用するインターフェイス。[送信元（Source）]は、デバイスに入るトラフィックが通過する実際のインターフェイスです。[宛先（Destination）]は、デバイスから出るトラフィックが通過するマッピング インターフェイスです。デフォルトでは、ブリッジ グループ メンバー インターフェイスを除き、ルールはすべてのインターフェイスに適用されます（[すべて（Any）]）。

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

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

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

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

- ダイナミックNAT（Dynamic NAT）：マッピング アドレスを含むネットワーク オブジェクトまたはグループ。ネットワーク オブジェクトまたはグループ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。IPv4 アドレスと IPv6 アドレスの両方をグループに入れることはできません。1 つのタイプだけが含まれている必要があります。
- ダイナミックPAT（Dynamic PAT）：次のいずれかになります。
  - （インターフェイス PAT）宛先インターフェイスの IP アドレスを使用するには、[インターフェイス（Interface）]を選択します。また、特定の宛先インターフェイスを選択する必要もあります。。IPv6 にインターフェイス PAT を使用することはできません。
  - 宛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、この目的のために作成したホスト 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）：次のいずれかになります。
  - アドレスのセット グループを使用するには、マッピング アドレスを含むネットワーク オブジェクトまたはグループを選択します。通常、1 対 1 のマッピングでは、実際のアドレスと同じ数のマッピング アドレスを設定します。しかし、アドレスの数が一致しない場合もあります。
  - （ポート変換を設定したスタティック インターフェイスNAT）宛先インターフェイスの IP アドレスを使用するには、[インターフェイス（Interface）]を選択します。また、特定の宛先インターフェイスを選択する必要もあります。。これによって、ポート変換を設定したスタティック インターフェイスNAT が設定されます。送信元アドレス/ポートは、インターフェイスのアドレスおよび同一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）：元の送信元と同じオブジェクト。オプションで、内容がまったく同じ別のオブジェクトを選択できます。

元の宛先アドレス

宛先アドレスを含むネットワーク オブジェクト。これを空白のままにすると、送信元アドレスの変換が宛先に関係なく適用されます。宛先アドレスを指定した場合、このアドレスにスタティック変換を設定できるか、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、送信元インターフェイスを元の宛先のベースにすることができます（[すべて（Any）] をベースにすることはできません）。このオプションを使用するには、変換済み宛先オブジェクトも選択する必要があります。宛先アドレスに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 を実装するには、このオプションを選択し、宛先ポートに適したポート オブジェクトも選択します。

変換済み宛先アドレス

変換済みパケットで使用される宛先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。[元の宛先（Original Destination）] のオブジェクトを選択した場合、同じオブジェクトを選択することによってアイデンティティ NAT（変換されていない NAT）を設定できます。

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

元のパケットおよび変換済みパケットの送信元および宛先サービスを定義するポート オブジェクト。ポートを変換したり、ポートを変換せずに同じオブジェクトを選択してサービスに対するルールの感度を向上することができます。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）[元の送信元ポート（Original Source Port）]および [変換済み送信元ポート（Translated Source Port）]では変換できません。宛先ポートでのみ変換できます。
- NAT では、TCP または UDP のみがサポートされます。ポートを変換する場合、実際のサービス オブジェクトのプロトコルとマッピング サービス オブジェクトのプロトコルの両方を同じにします（両方とも TCP または両方とも UDP）。アイデンティティ NAT では、実際のポートとマッピング ポートの両方に同じオブジェクトを使用できます。

詳細 NAT プロパティ

NAT を設定するとき、[詳細（Advanced）]オプションで特別なサービスを提供するプロパティを設定できます。これらすべてのプロパティはオプションであり、サービスを必要としている場合のみ設定します。

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 インターフェイスに移動する 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状況で使用され、書き換えにより A レコードと AAAA レコード間でも変換が行われる NAT64/46 変換のために必要なことがあります。詳細については、NAT を使用した DNS クエリーのリライトと応答，（85 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（宛先インターフェイス）へのフォールスルー（Fallthrough to Interface PAT (Destination Interface)）]（ダイナミック NAT のみ）

その他のマッピング アドレスがすでに割り当てられている場合に、宛先インターフェイスの IP アドレスをバックアップ方式として使用するかどうかを指定します（インターフェイス PAT フォールバック）。このオプションは、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。IPv6 ネットワークではこのオプションは使用できません。

宛先インターフェイスでプロキシ ARP 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。この方法だと、デバイスがその他のネットワークのゲートウェイになる必要がないため、ルーティングが簡略化されます。プロキシ ARP は必要に応じて無効にできます。無効にする場合、上流に位置するルータに適切なルートが設定されている必要があります。アイデンティティ NAT の場合、通常はプロキシ ARP は不要です。場合によっては接続の問題が生じることがあります。

宛先インターフェイスでルート ルックアップを実行します（スタティック ID NAT のみ。ルーテッド モードのみ）。

元の送信元アドレスと変換後の送信元アドレスに対して同じオブジェクトを選択している場合に、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して、NAT ルールに設定されている宛先インターフェイスを使用する代わりに、ルーティング テーブルに基づいて宛先インターフェイスを決めさせることができます。

IPv6 ネットワークの変換

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

IPv6 ネットワークとともに次の変換タイプを使用できます。

- NAT64、NAT46：IPv6 パケットを IPv4（およびその反対）に変換します。IPv6 から IPv4 への変換と IPv4 から IPv6 への変換に対する 2 つのポリシーを定義する必要があります。1 つの/手動 NAT ルールでこれを実現できますが、DNS サーバが外部ネットワークにある場合は、DNS 応答を書き換える必要がある可能性があります。宛先を指定するときに/手動 NAT ルールで DNS の書き換えを有効にすることはできないため、2 つの/自動 NATルールを作成する方法が適しています。

（注） NAT46 がサポートするのは、スタティック マッピングのみです。

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

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

NAT64/46：IPv6 アドレスから IPv4 への変換

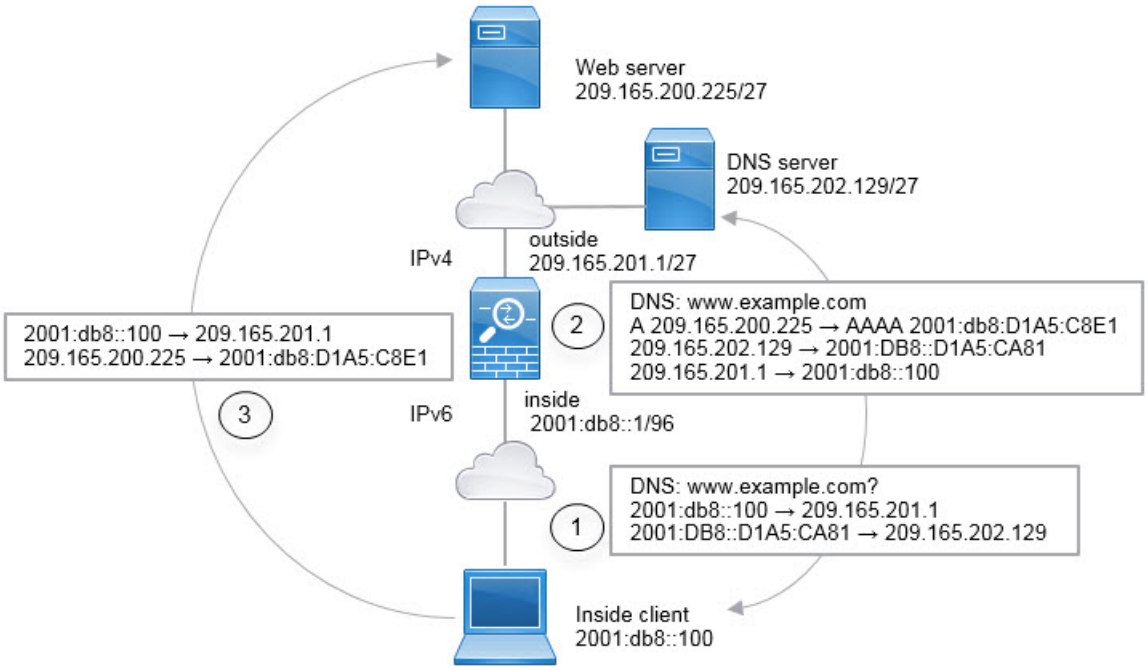
トラフィックが IPv6 ネットワークから IPv4 専用ネットワークに移動する場合、IPv6 アドレスを IPv4 に変換する必要があります。また、トラフィックを IPv4 から IPv6 に戻す必要があります。IPv4 ネットワークで IPv6 アドレスをバインドするための IPv4 アドレス プールと、IPv6 ネットワークで IPv4 アドレスをバインドするための IPv6 アドレス プールの 2 つを定義する必要があります。

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

送信元 IPv6 ネットワークと宛先 IPv4 ネットワークの 2 つのポリシーを定義する必要があります。1 つの/手動 NAT ルールでこれを実現できますが、DNS サーバが外部ネットワークにある場合は、DNS 応答を書き換える必要がある可能性があります。宛先を指定するときに /手動 NAT ルールで DNS の書き換えを有効にすることはできないため、2 つの/自動 NAT ルールを作成する方法が適しています。

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

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



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

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

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

3 これで、IPv6 クライアントが Web サーバの IP アドレスを取得し、www.example.com（2001:db8:D1A5:C8E1）に HTTP 要求を送信できます。（D1A5:C8E1 は IPv6 の 209.165.200.225 に相当します）。HTTP 要求の送信元と宛先が変換されます。

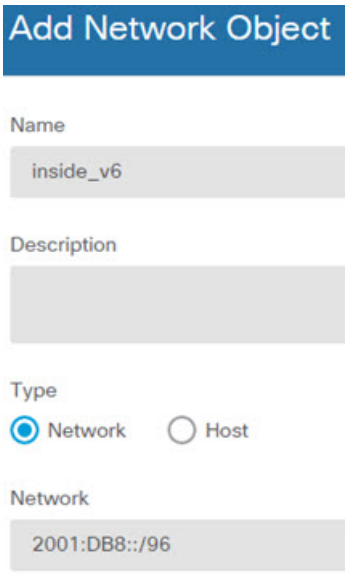
- 2001:DB8::100 を 209.156.101.54 上の一意のポートに変換（NAT64 インターフェイス PAT ルール）。
- 2001:db8:D1A5:C8E1 を 209.165.200.225 に変換（NAT46 ルール）。

次の手順では、この例の設定方法について説明します。

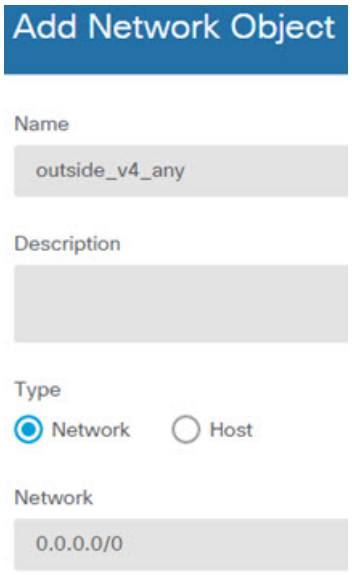
手順

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

a) [オブジェクト（Objects）]を選択します。
b) 目次から [ネットワーク（Network）]を選択して、[+] 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（inside_v6 など）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（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（outside_v4_any など）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（0.0.0.0/0）を入力します。



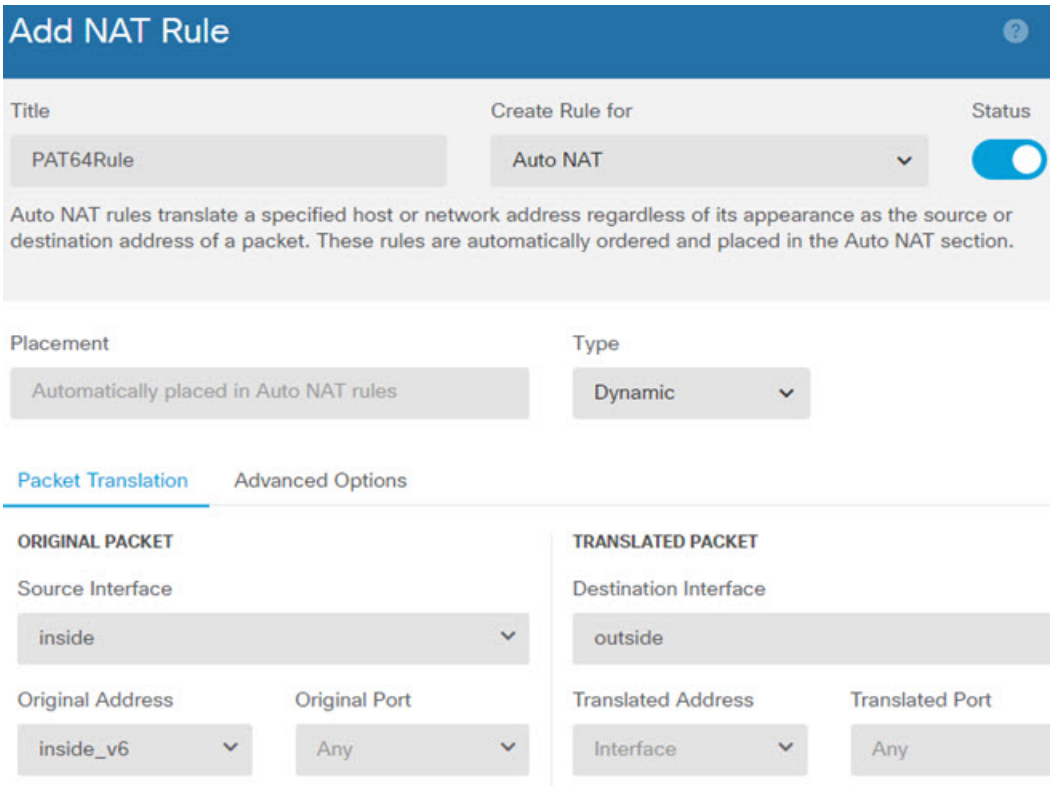
ステップ 2 内部 IPv6 ネットワークの NAT64 ダイナミック PAT ルールを設定します。

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）]。
- [タイプ（Type）]：[ダイナミック（Dynamic）]。
- [送信元インターフェイス（Source Interface）]：内部。
- [宛先インターフェイス（Destination Interface）]：外部。
- [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）]：[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。



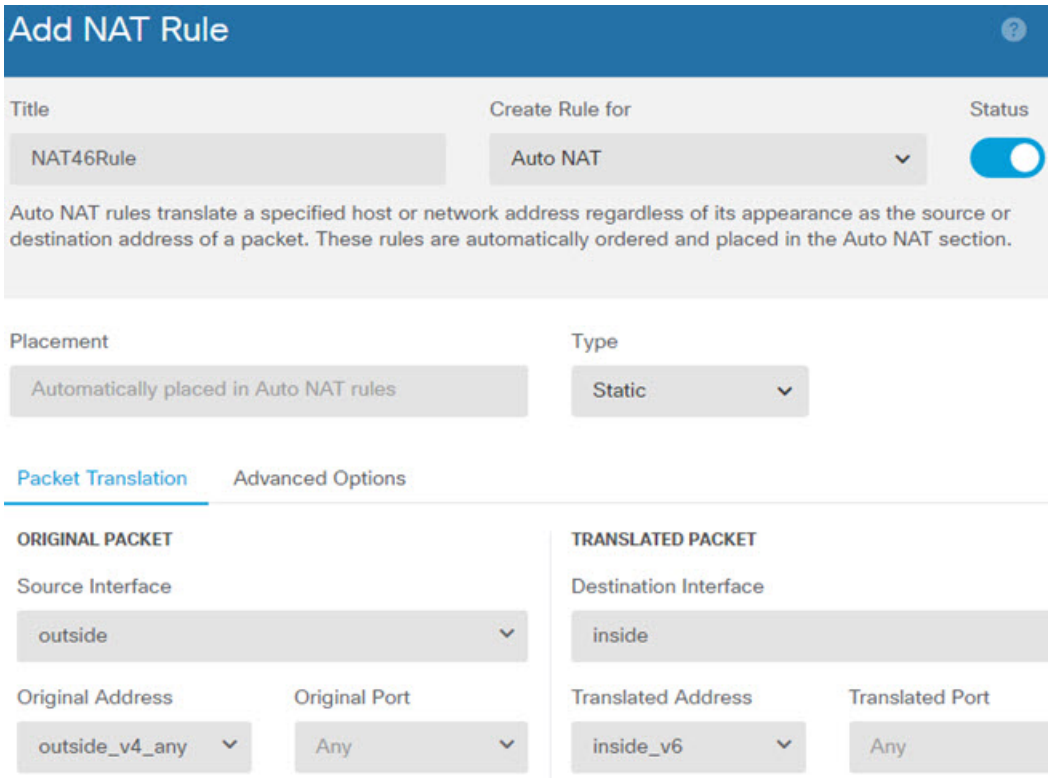
d) [OK]をクリックします。
このルールを使用すると、内部インターフェイスの2001:db8::/96サブネットから外部インターフェイスに移動するすべてのトラフィックが、外部インターフェイスの IPv4 アドレスを使用して NAT64 PAT 変換されます。

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

a) [+] 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）]。
- [タイプ（Type）]：[スタティック（Static）]。
- [送信元インターフェイス（Source Interface）]：外部。
- [宛先インターフェイス（Destination Interface）]：内部。
- [元のアドレス（Original Address）]：outside_v4_any ネットワーク オブジェクト。
- [変換済みアドレス（Translated Address）]：inside_v6 ネットワーク オブジェクト。
- [詳細オプション（Advanced Options）]タブで、[このルールと一致する DNS 応答を変換（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届く外部ネットワークのすべての IPv4 アドレスが、組み込みの IPv4 アドレス方式を使用して 2001:db8::/96 ネットワークのアドレスに変換されます。また、DNS 応答が A（IPv4）レコードから AAAA（IPv6）レコードに変換され、アドレスが IPv4 から IPv6 に変換されます。

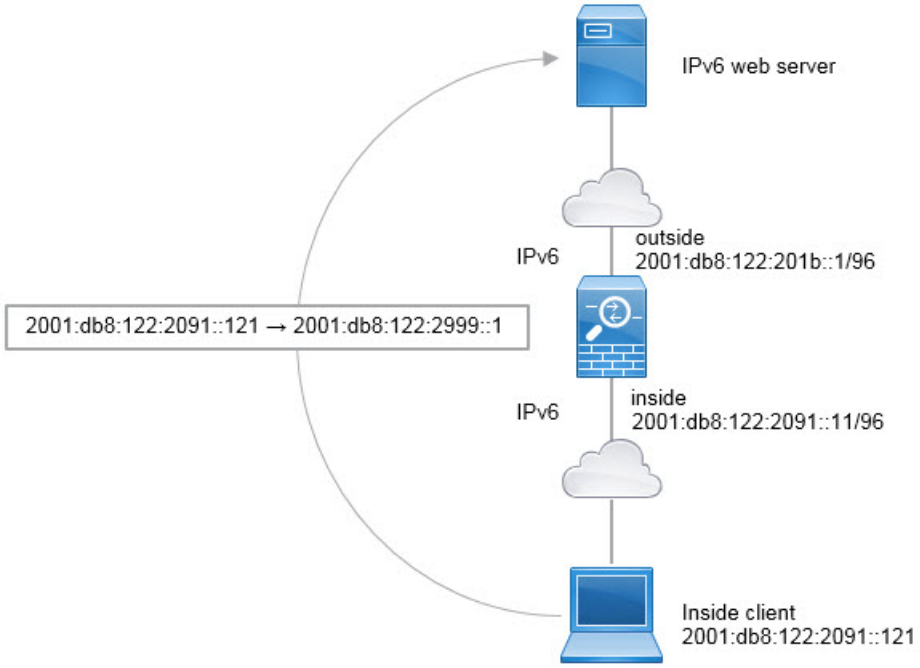
NAT66：IPv6 アドレスから別の IPv6 アドレスへの変換

IPv6 ネットワークから別の IPv6 ネットワークに移動する場合、アドレスを外部ネットワークの別の IPv6 アドレスに変換できます。スタティック NAT の使用をお勧めします。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 タイプ間での変換ではないため、NAT66 変換の単一のルールが必要です。/自動 NATを使用すると、これらのルールを容易にモデル化できます。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 ルールを単一方向にすることができます。

NAT66 の例、ネットワーク間のスタティック変換

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



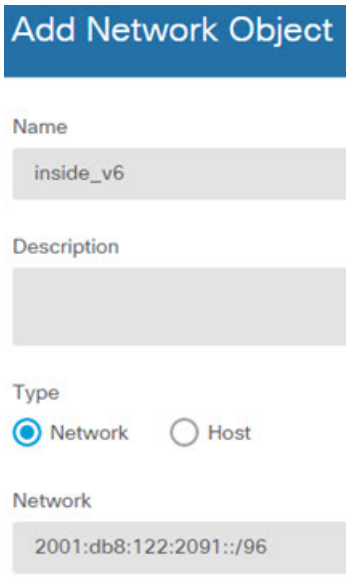
手順

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

a) [オブジェクト（Objects）]を選択します。

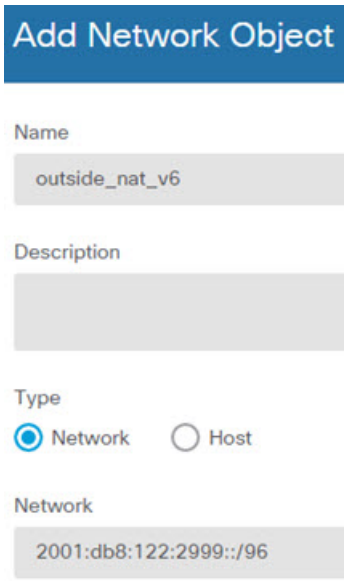
b) 目次から [ネットワーク（Network）]を選択して、[+] をクリックします。

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（inside_v6 など）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（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（outside_nat_v6 など）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（2001:db8:122:2999::/96）を入力します。



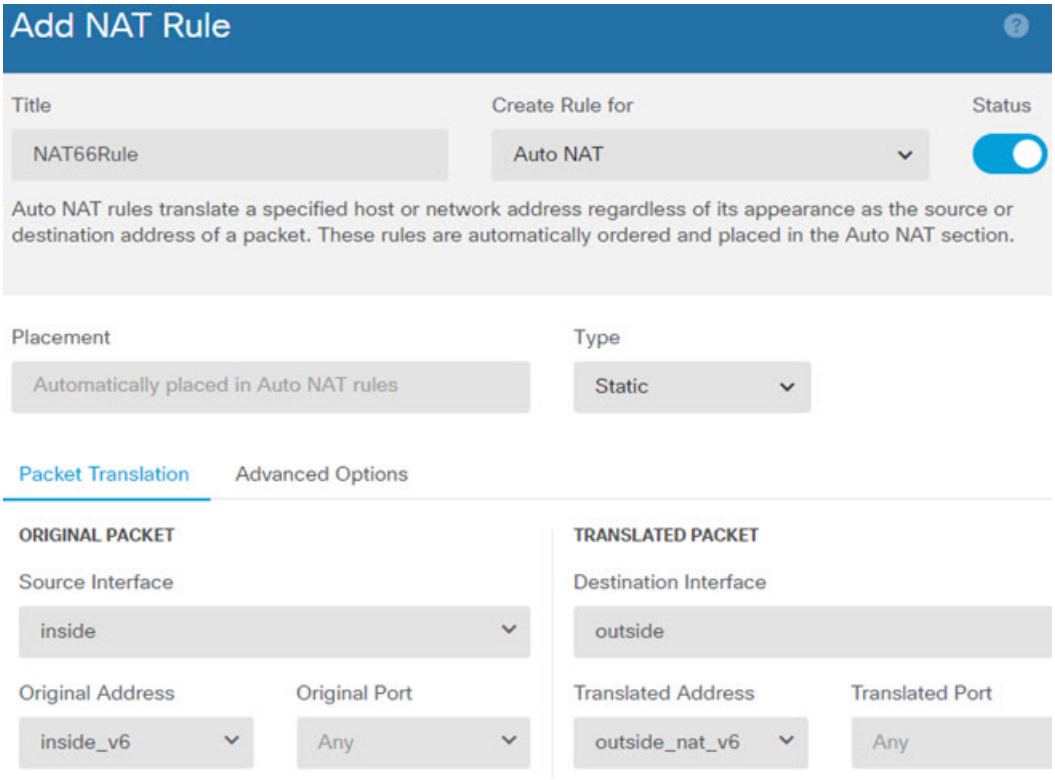
ステップ 2 内部 IPv6 ネットワークのスタティック NAT ルールを設定します。

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）]。
- [タイプ（Type）]：[スタティック（Static）]。
- [送信元インターフェイス（Source Interface）]：内部。
- [宛先インターフェイス（Destination Interface）]：外部。
- [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）]：outside_nat_v6 ネットワーク オブジェクト。

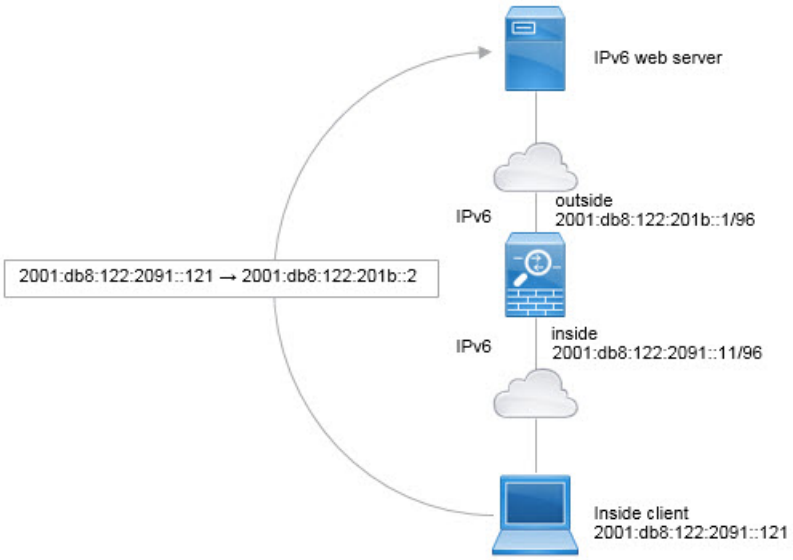


d) [OK]をクリックします。
このルールを使用すると、内部インターフェイスの 2001:db8:122:2091::/96 サブネットから外部インターフェイスに届くすべてのトラフィックが 2001:db8:122:2999::/96 ネットワークのアドレスにスタティック NAT66 変換されます。

NAT66 の例、シンプルな IPv6 インターフェイス PAT

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

ただし、Firepower 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、同じネットワーク上の 1 つの空きアドレスをダイナミック PAT プールとして使用します。



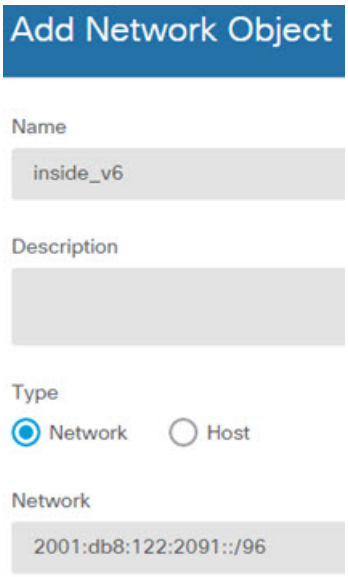
手順

ステップ 1 内部 IPv6 ネットワークと 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) 目次から [ネットワーク（Network）]を選択して、[+] 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（inside_v6 など）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（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（inside_v6 など）を付け、[ホスト（Host）]を選択して、ホスト アドレス（2001:db8:122:201b::2）を入力します。

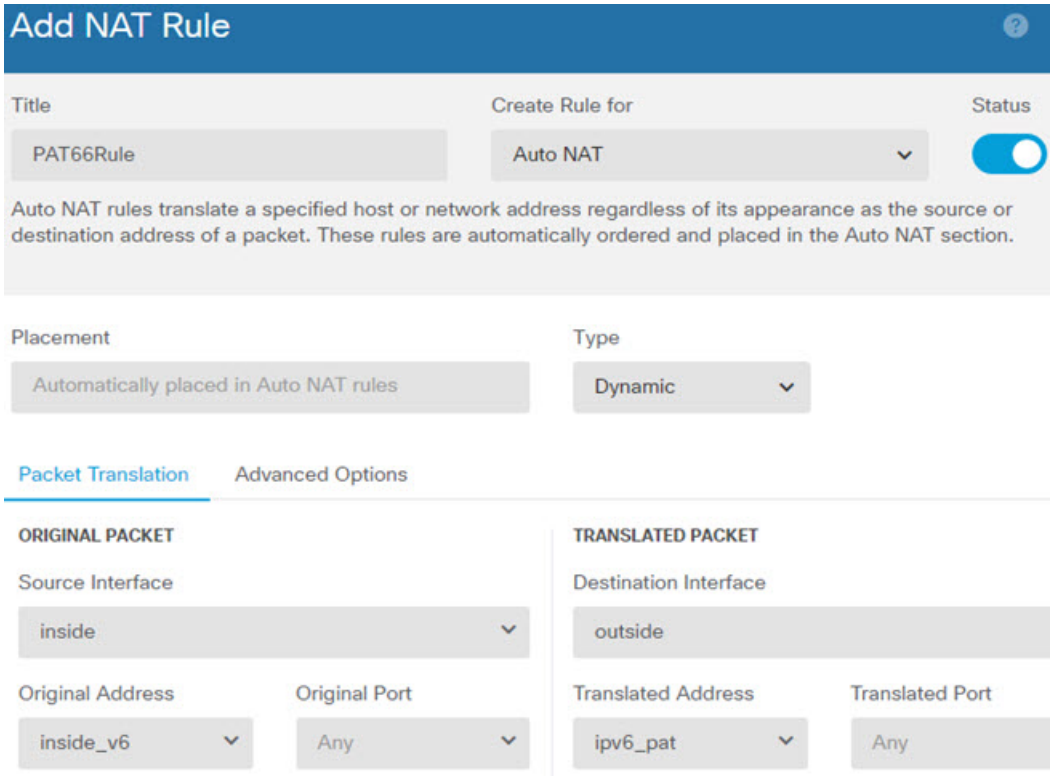
ステップ 2 内部 IPv6 ネットワークのダイナミック PAT ルールを設定します。

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）]。
- [タイプ（Type）]：[ダイナミック（Dynamic）]。
- [送信元インターフェイス（Source Interface）]：内部。
- [宛先インターフェイス（Destination Interface）]：外部。
- [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）]：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の 2001:db8:122:2091::/96 サブネットから外部インターフェイスに届くすべてのトラフィックが 2001:db8:122:201b::2 のポートにダイナミック PAT66 変換されます。

NAT のモニタリング

NAT 接続をモニタしてトラブルシューティングを実行するには、デバイス CLI にログインして次のコマンドを使用します。

- **show nat** は、NAT ルールとルールごとのヒット数を表示します。NAT の他の側面を表示するための追加キーワードがあります。
- **show xlate** は、現在アクティブな実際の NAT 変換を表示します。
- **clear xlate** を使用すると、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。変換をクリアすると、システムは、新しいルールに基づいたクライアントの次の接続試行でクライアントの新しい変換を作成できます。

NAT の例

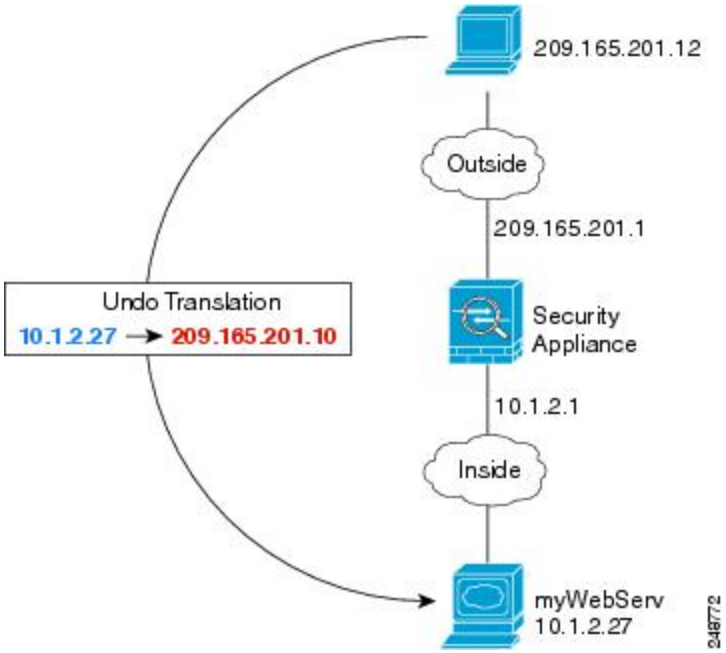
次に、脅威に対する防御デバイスでの NAT の設定例を示します。

内部 Web サーバへのアクセスの提供（スタティック自動 NAT）

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

固定アドレスにある Web サーバへのトラフィックをホストが開始できるようにするために必要です。

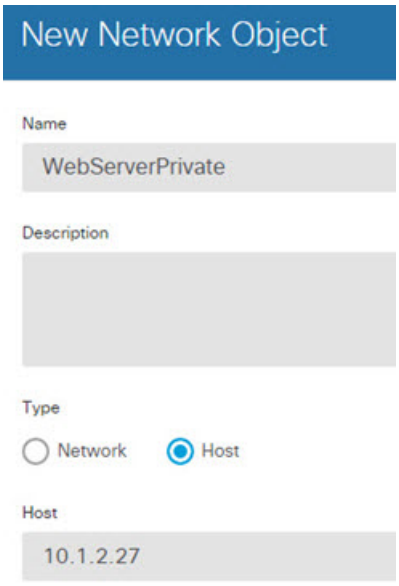
図 *13*：内部 *Web* サーバのスタティック *NAT*



手順

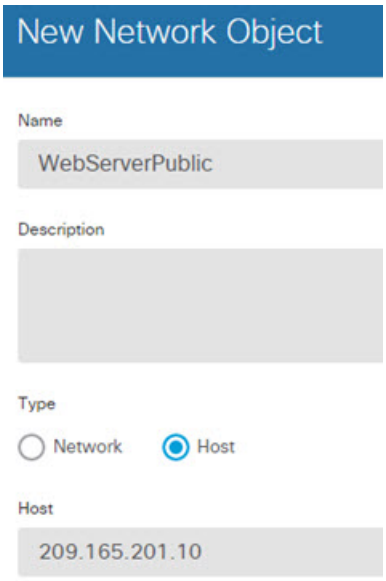
ステップ 1 サーバのプライベートおよびパブリック ホスト アドレスを定義するネットワーク オブジェクトを作成します。

a) [オブジェクト（Objects）]を選択します。
b) 目次から [ネットワーク（Network）]を選択して、[+] 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（WebServerPrivate など）を付け、[ホスト（Host）]を選択して、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]をクリックします。

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（WebServerPublic など）を付け、[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。



f) [追加（Add）]、[OK]をクリックします。

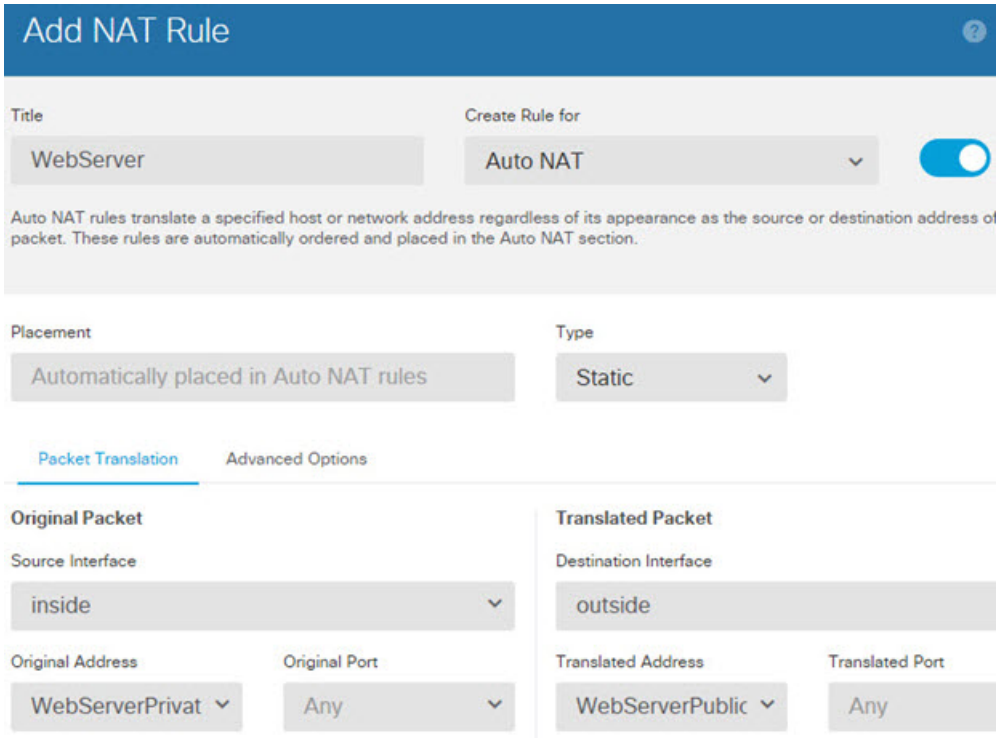
ステップ 2 オブジェクトのスタティック NAT を設定します。

a) [ポリシー（Policies）] > [NAT] を選択します。

b) [+] ボタンをクリックします。

c) 次のプロパティを設定します。

- [タイトル（Title）]：WebServer（またはユーザ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）]。
- [タイプ（Type）]：[スタティック（Static）]。
- [送信元インターフェイス（Source Interface）]：内部。
- [宛先インターフェイス（Destination Interface）]：外部。
- [元のアドレス（Original Address）]：WebServerPrivate ネットワーク オブジェクト。
- [変換済みアドレス（Translated Address）]：WebServerPublic ネットワーク オブジェクト。



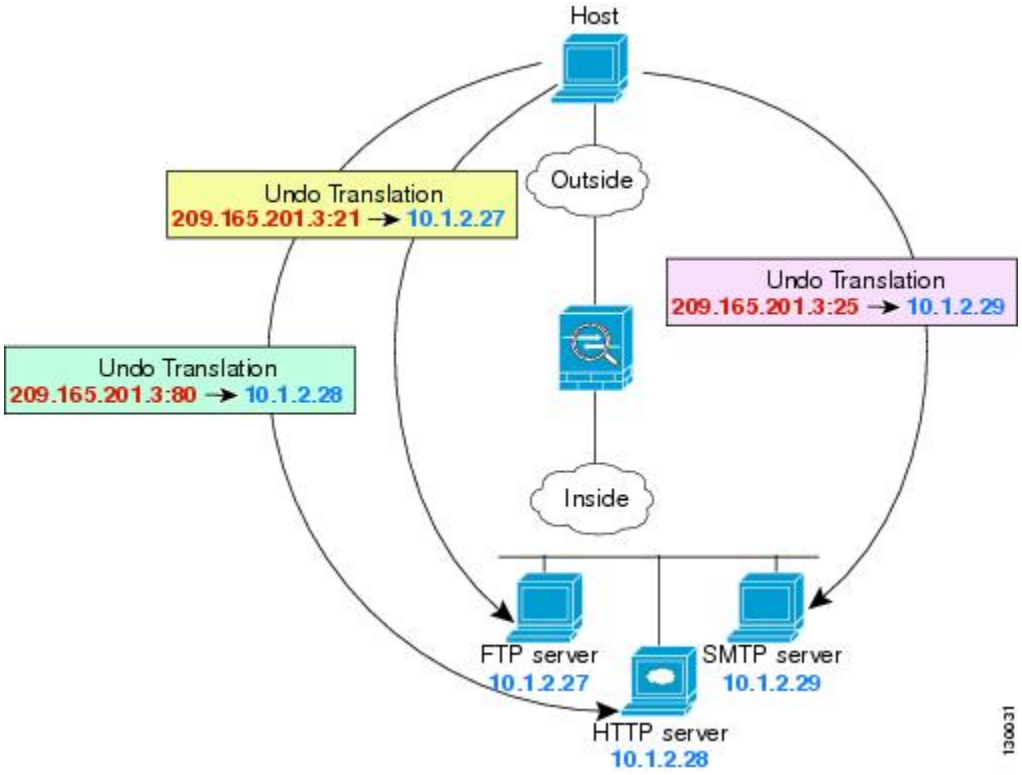
d) [OK]をクリックします。

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

次のポート変換を設定したスタティック NAT の例では、リモート ユーザが FTP、HTTP、および SMTP にアクセスするための単一のアドレスを提供します。これらのサーバは実際には、それぞ

れ異なるデバイスとして実際のネットワーク上に存在しますが、ポート変換を設定したスタティック NAT ルールを指定すると、使用するマッピング IP アドレスは同じで、それぞれ別のポートを使用することができます。

図 *14*：ポート変換を設定したスタティック *NAT*



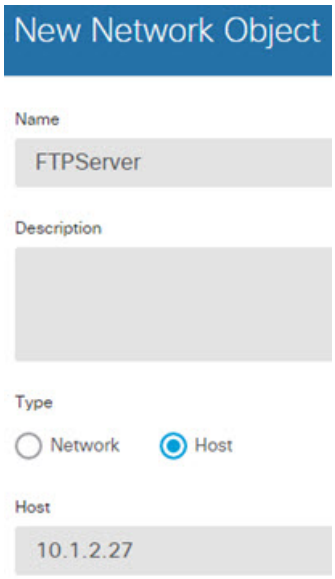
手順

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

c) ネットワーク オブジェクトに名前を付け（たとえば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。

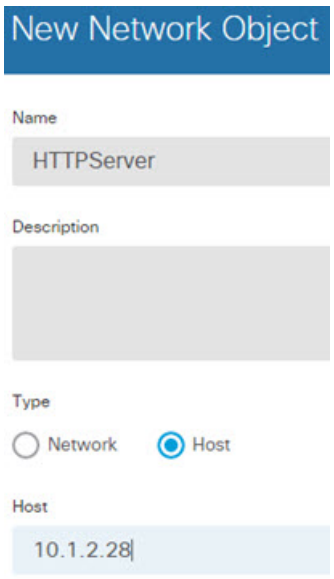


d) [追加（Add）] [OK] をクリックします。

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（たとえば 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。

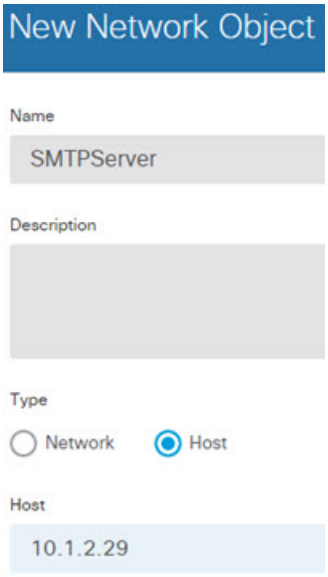


c) [追加（Add）] [OK] をクリックします。

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（たとえば 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。

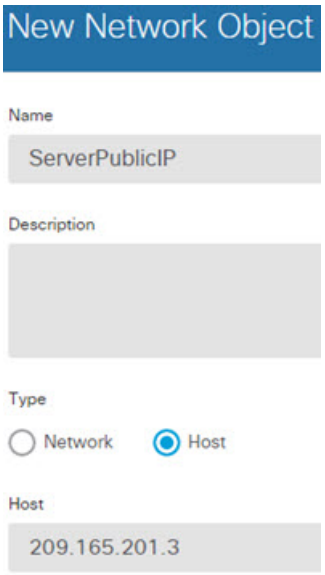


c) [追加（Add）] [OK] をクリックします。

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（たとえば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。

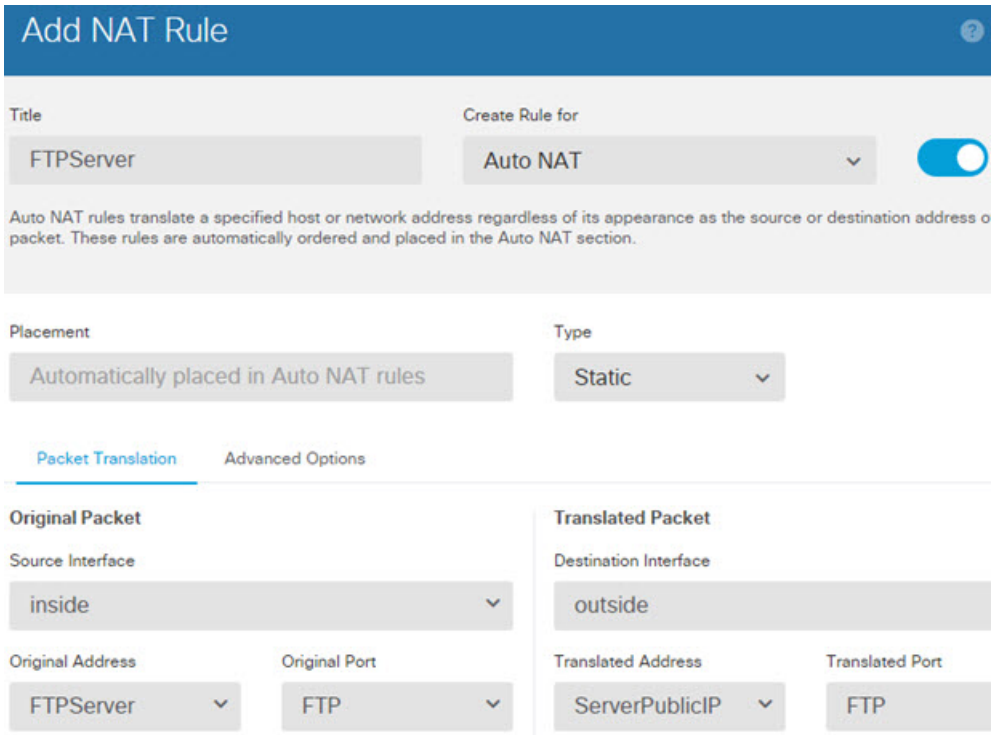


c) [追加（Add）] [OK] をクリックします。

ステップ 5 FTP サーバのポート変換を設定したスタティック NAT を設定し、FTP ポートを自身にマッピングします。

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）]。
- [タイプ（Type）]= [スタティック（Static）]。
- [送信元インターフェイス（Source Interface）]= [内部（inside）]。
- [宛先インターフェイス（Destination Interface）]= [外部（outside）]。
- [元のアドレス（Original Address）]= [FTPServer ネットワーク オブジェクト（FTPserver network object）]。
- [変換済みアドレス（Translated Address）]= [ServerPublicIP ネットワーク オブジェクト（ServerPublicIP network object）]。
- [元のポート（Original Port）]= [FTP ポート オブジェクト（FTP port object）]。
- [変換済みポート（Translated Port）]= [FTP ポート オブジェクト（FTP port object）]。



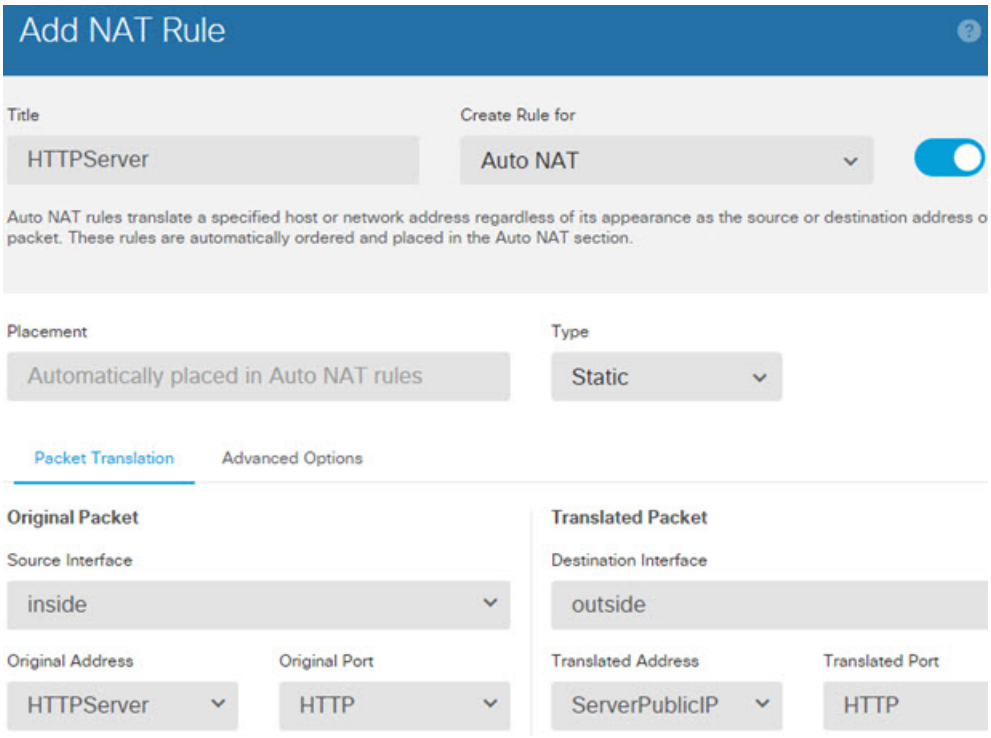
d) [OK]をクリックします。

ステップ 6 HTTP サーバのポート変換を設定したスタティック NAT を設定し、HTTP ポートを自身にマッピングします。

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）]。
- [タイプ（Type）]= [スタティック（Static）]。
- [送信元インターフェイス（Source Interface）]= [内部（inside）]。
- [宛先インターフェイス（Destination Interface）]= [外部（outside）]。
- [元のアドレス（Original Address）]= [HTTPserver ネットワーク オブジェクト（HTTPserver network object）]。
- [変換済みアドレス（Translated Address）]= [ServerPublicIP ネットワーク オブジェクト（ServerPublicIP network object）]。
- [元のポート（Original Port）]= [HTTP ポート オブジェクト（FTP port object）]。
- [変換済みポート（Translated Port）]= [HTTP ポート オブジェクト（HTTP port object）]。



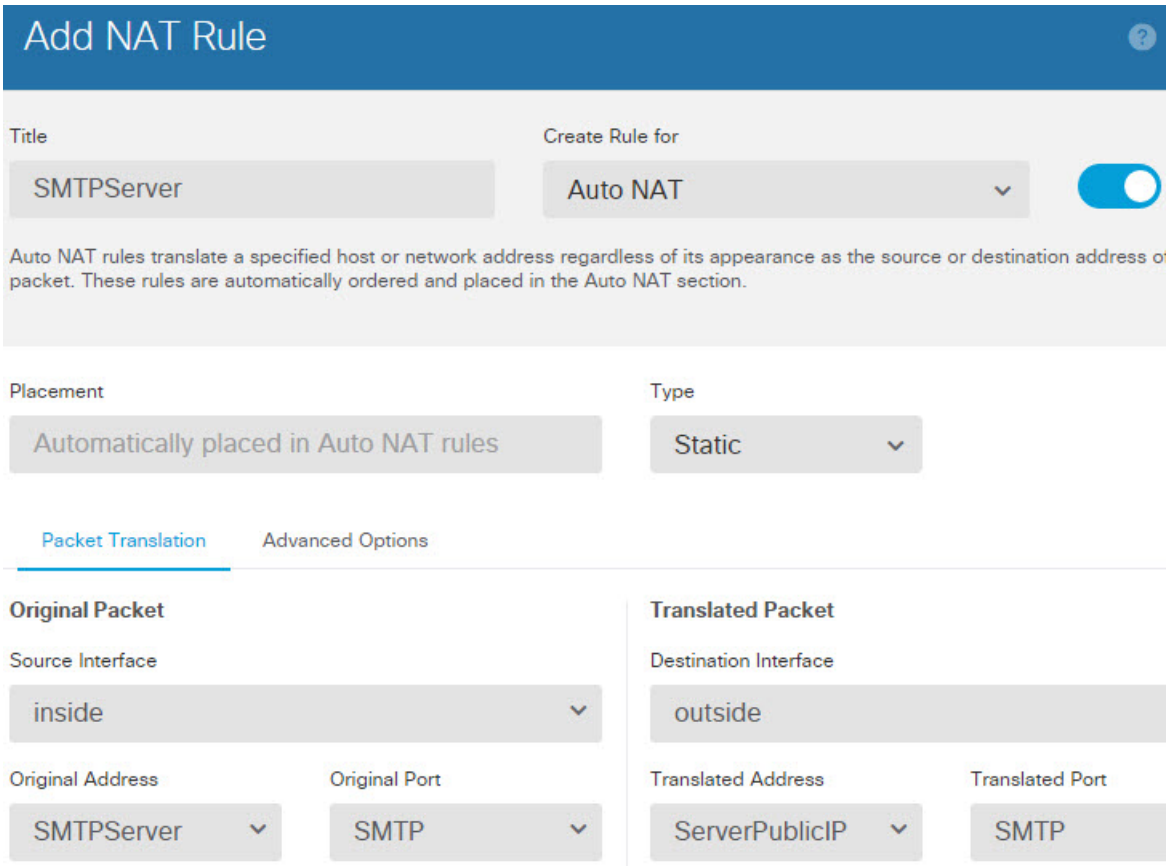
c) [OK]をクリックします。

ステップ 7 SMTP サーバのポート変換を設定したスタティック NAT を設定し、SMTP ポートを自身にマッピングします。

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）] 。
- [タイプ（Type）]= [スタティック（Static）]。
- [送信元インターフェイス（Source Interface）]= [内部（inside）]。
- [宛先インターフェイス（Destination Interface）]= [外部（outside）]。
- [元のアドレス（Original Address）]= [SMTPserver ネットワーク オブジェクト（SMTPserver network object）]。
- [変換済みアドレス（Translated Address）]= [ServerPublicIP ネットワーク オブジェクト（ServerPublicIP network object）]。
- [元のポート（Original Port）]= [SMTP ポート オブジェクト（SMTP port object）]。
- [変換済みポート（Translated Port）]= [SMTP ポート オブジェクト（SMTP port object）]。



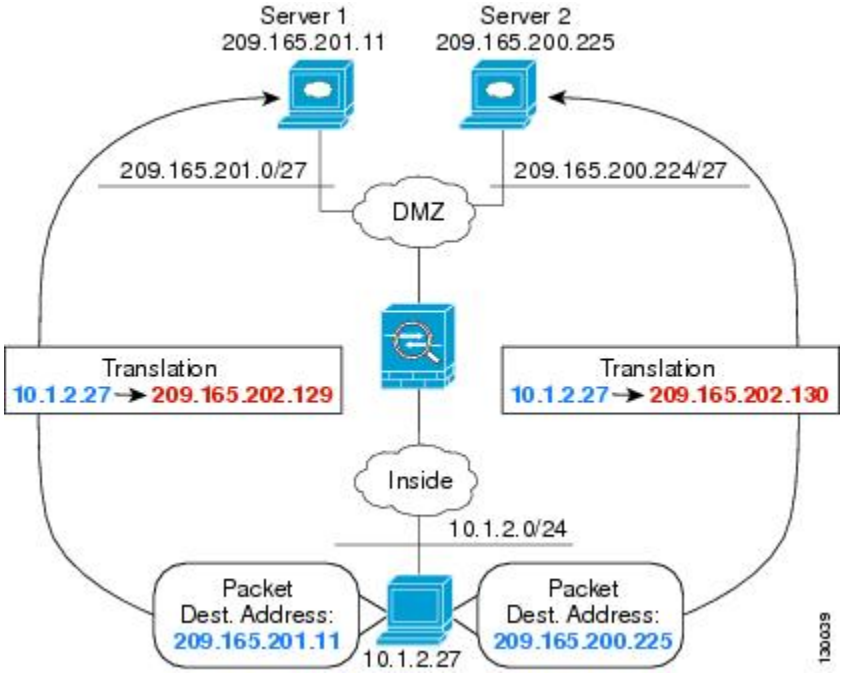
c) [OK]をクリックします。

宛先に応じて異なる変換（ダイナミック手動 PAT）

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

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

図 *15*：異なる宛先アドレスを使用する手動 *NAT*



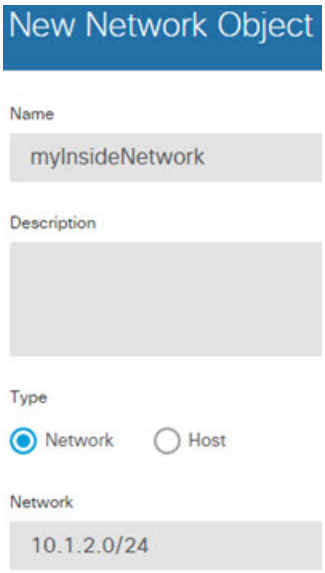
手順

ステップ 1 内部ネットワークのネットワーク オブジェクトを作成します。

a) [オブジェクト（Objects）]を選択します。

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

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

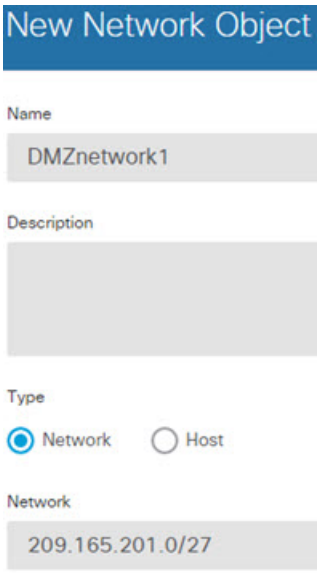


d) [追加（Add）][OK]をクリックします。

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

a) [+]をクリックします。

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

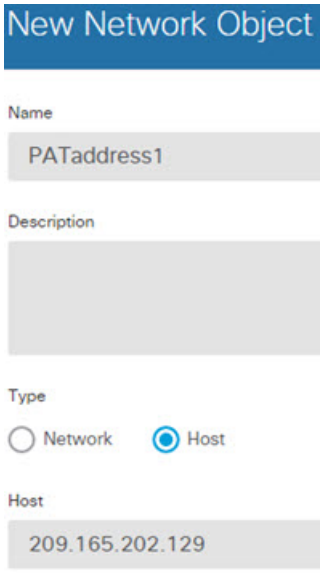


c) [追加（Add）][OK]をクリックします。

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

a) [+]をクリックします。

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

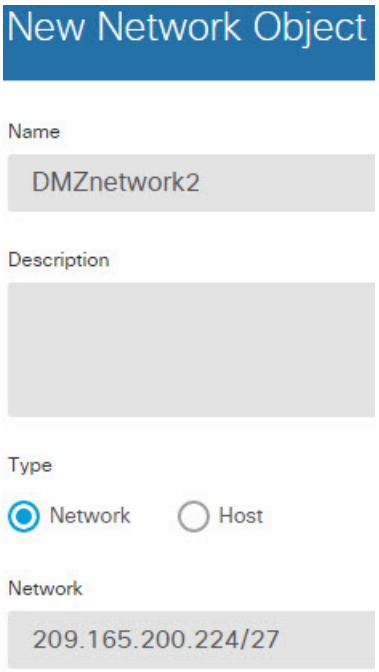


c) [追加（Add）][OK]をクリックします。

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

a) [+]をクリックします。

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

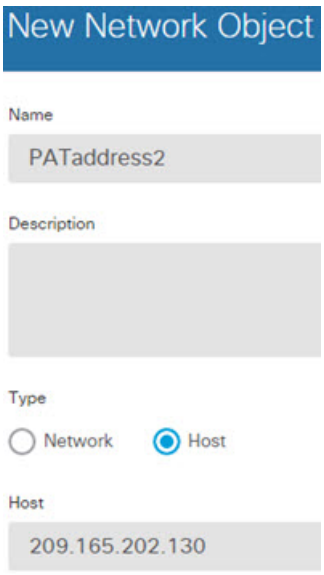


c) [追加（Add）][OK]をクリックします。

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

a) [+]をクリックします。

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



c) [追加（Add）][OK]をクリックします。

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

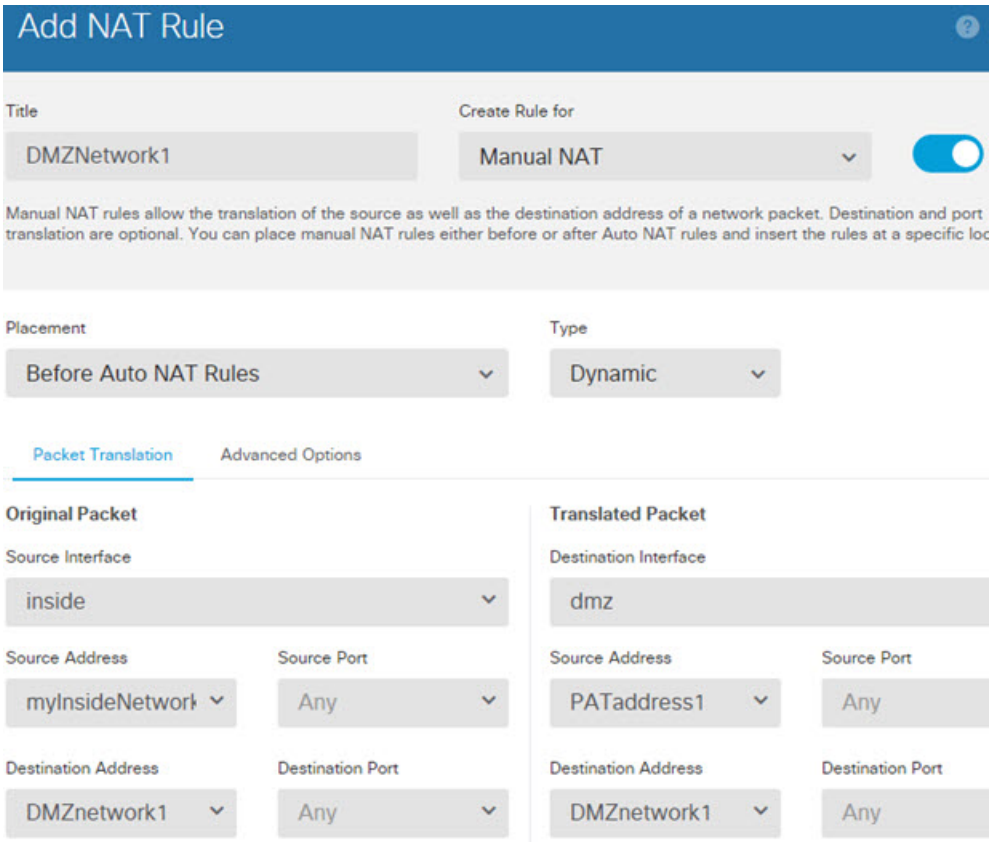
a) [ポリシー（Policies）] > [NAT] を選択します。

b) [+]ボタンをクリックします。

c) 次のプロパティを設定します。

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

（注） 宛先アドレスは変換しないため、元の宛先アドレスと変換された宛先アドレスに同じアドレスを指定することによって、アイデンティティ NAT を設定する必要があります。[ポート（Port）] フィールドはすべて空白のままにします。



d) [OK]をクリックします。

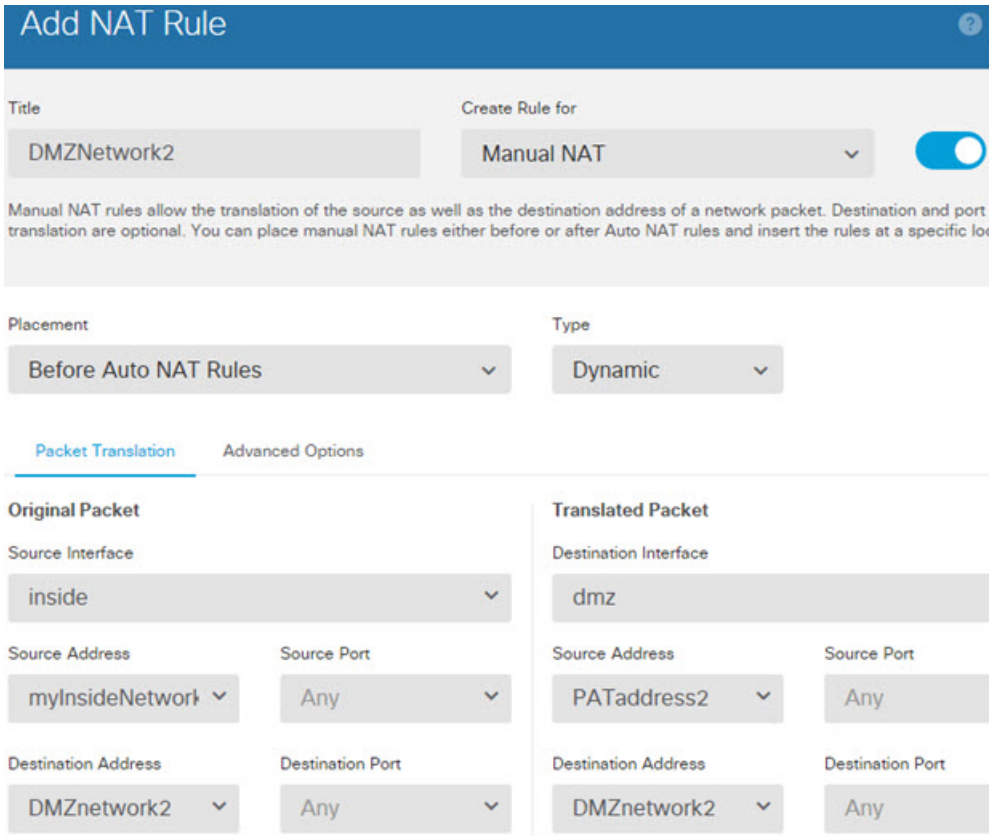
ステップ 7 DMZ ネットワーク 2 のダイナミック手動 PAT を設定します。

a) [+]ボタンをクリックします。

b) 次のプロパティを設定します。

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

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



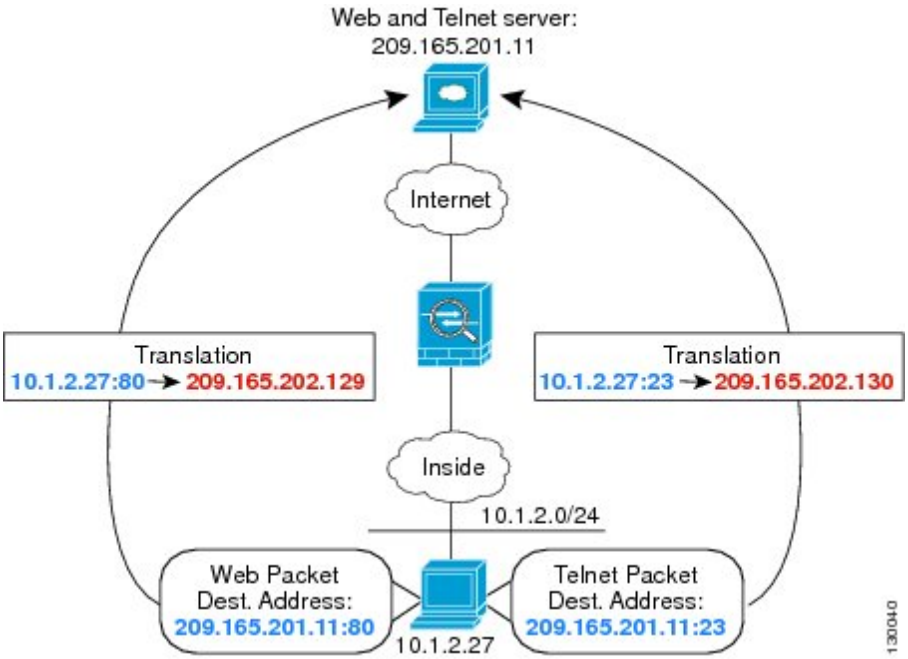
c) [OK]をクリックします。

宛先アドレスおよびポートに応じて異なる変換（ダイナミック手動 PAT）

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

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

図 *16*：異なる宛先ポートを使用する手動 *NAT*



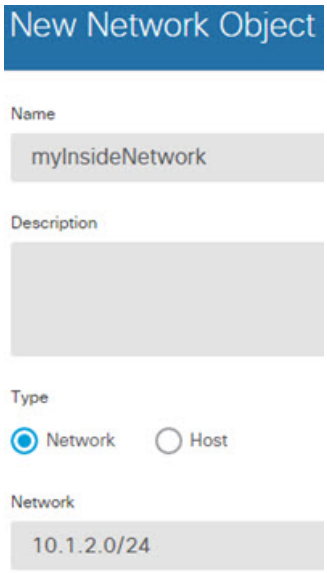
手順

ステップ 1 内部ネットワークのネットワーク オブジェクトを作成します。

a) [オブジェクト（Objects）]を選択します。

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

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

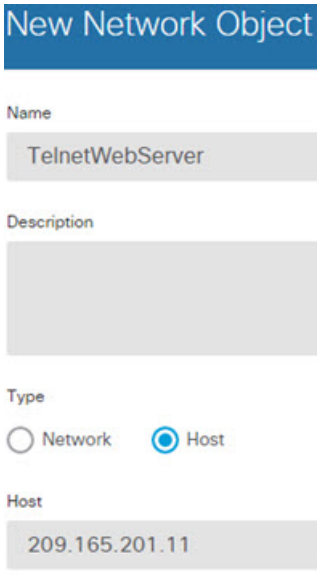


d) [追加（Add）][OK]をクリックします。

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

a) [+]をクリックします。

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

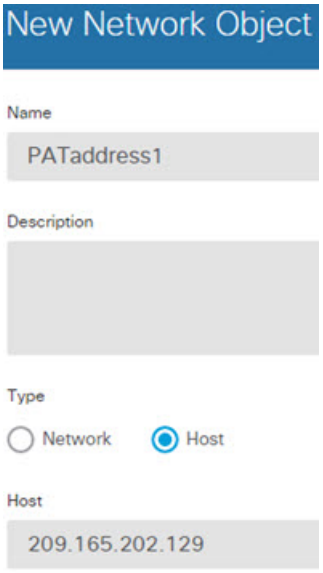


c) [追加（Add）][OK]をクリックします。

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

a) [+]をクリックします。

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

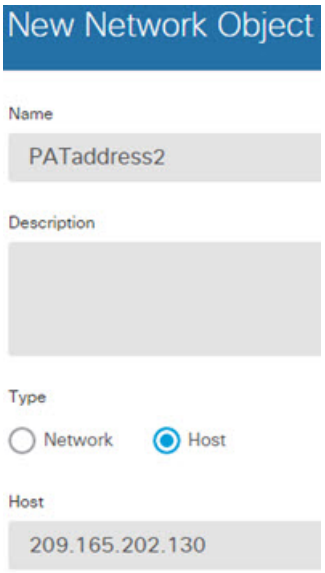


c) [追加（Add）][OK]をクリックします。

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

a) [+]をクリックします。

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



c) [追加（Add）][OK]をクリックします。

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

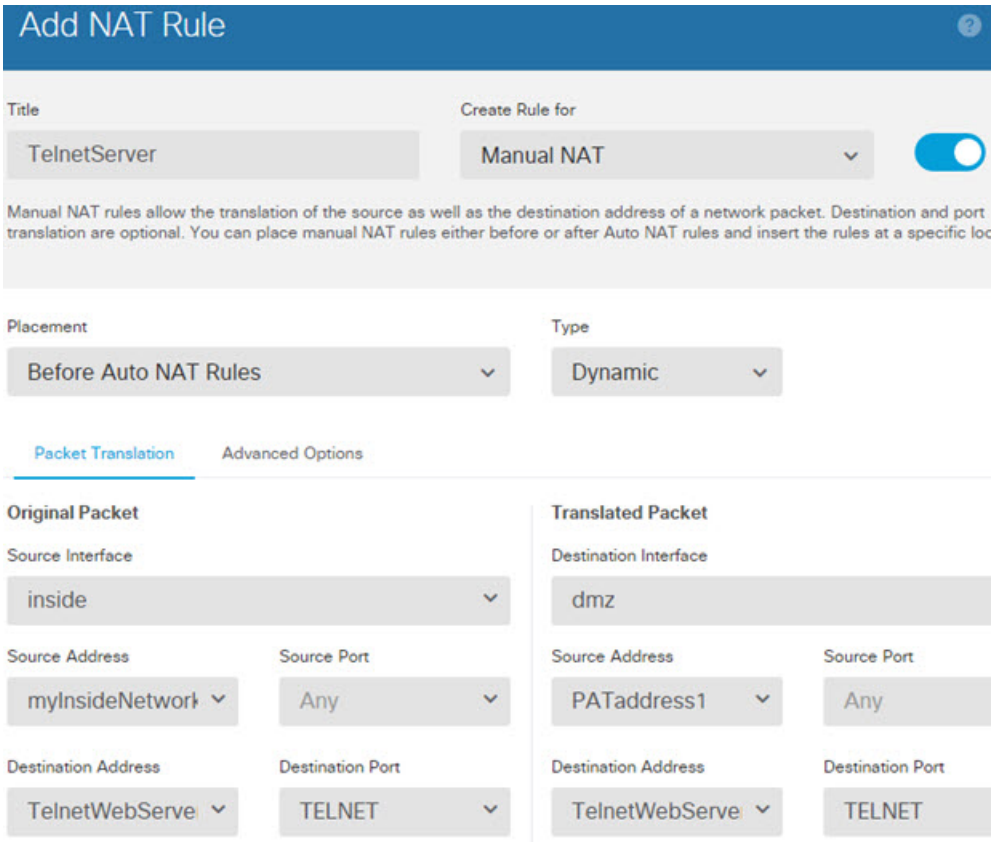
a) [ポリシー（Policies）] > [NAT] を選択します。

b) [+]ボタンをクリックします。

c) 次のプロパティを設定します。

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

（注） 宛先アドレスまたはポートを変換しないため、元のアドレスと変換済みの宛先アドレスに同じアドレスを指定し、元のポートと変換済みのポートに同じポートを指定することによって、アイデンティティ NAT を設定する必要があります。



d) [OK]をクリックします。

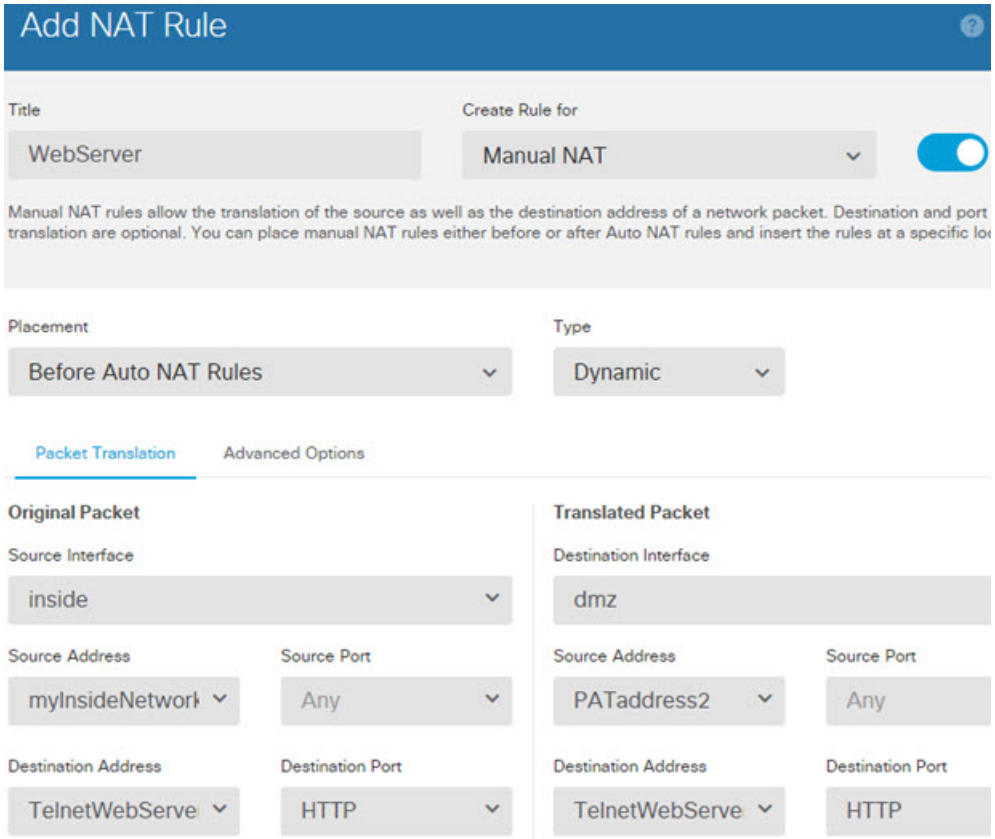
ステップ 6 Web アクセスのダイナミック手動 PAT を設定します。

a) [+]ボタンをクリックします。

b) 次のプロパティを設定します。

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

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



c) [OK]をクリックします。

NAT を使用した DNS クエリーのリライトと応答

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Firepower 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、各トランスレーション ルールを設定するときに設定できます。

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 応答では、A レコードはマップされた値から実際の値へリライトされます。逆に、任意のインターフェイスから

マッピング インターフェイスに移動する DNS 応答では、A レコードは実際の値からマップされた値へリライトされます。

以下に、NAT ルールで DNS のリライトを設定する必要が生じる主な状況を示します。

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

DNS リライトに関する制限事項

次に DNS リライトの制限事項を示します。

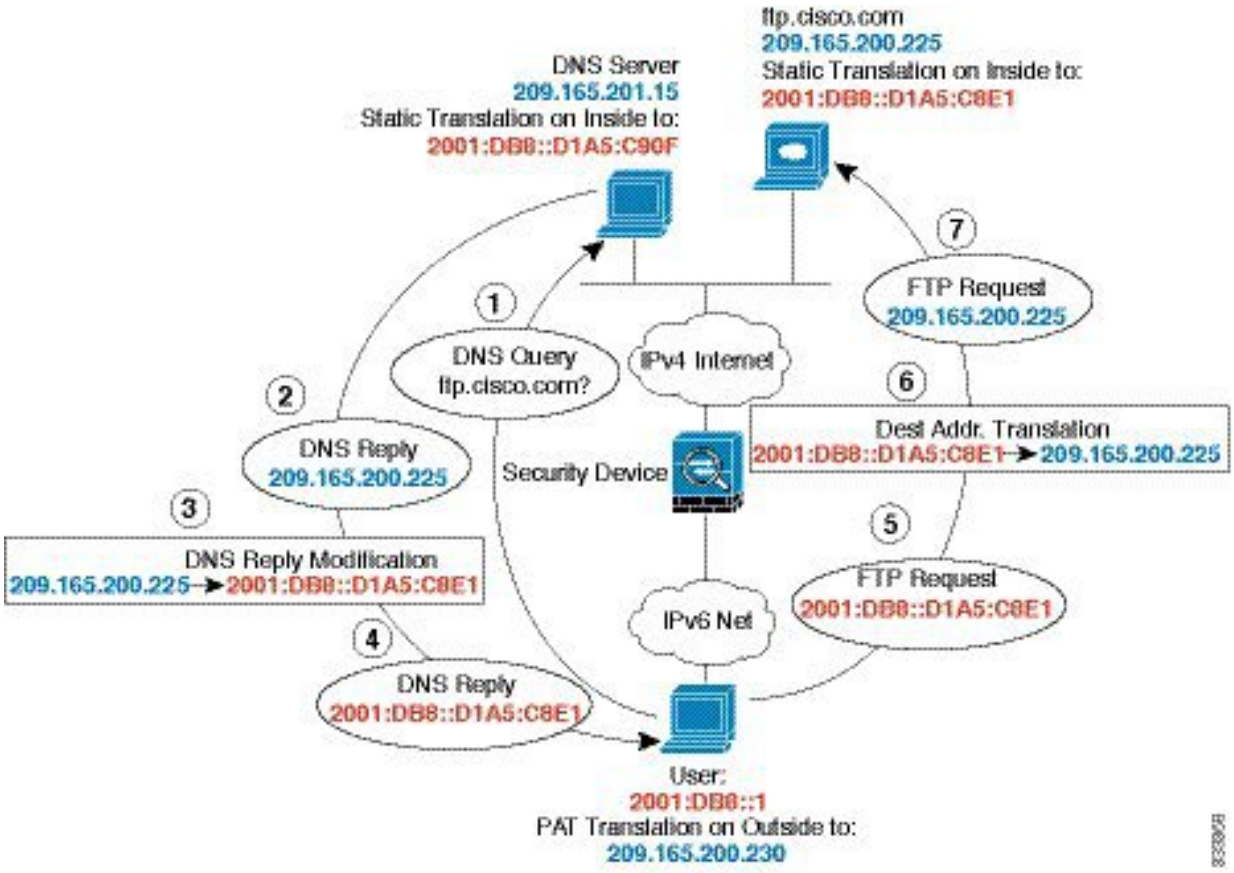
- 個々の A または AAAA レコードに複数の PAT ルールを適用できることで、使用する PAT ルールが不明確になるため、DNS リライトは PAT には適用されません。
- /手動 NATルールを設定する場合、送信元アドレスおよび宛先アドレスを指定すると、DNS 修正を設定できません。これらの種類のルールでは、A と B に向かった場合に 1 つのアドレスに対して異なる変換が行われる可能性があります。したがって、Firepower Threat Defense デバイスは、DNS 応答内の IP アドレスを適切な Twice NAT ルールに一致させることができません。DNS 応答には、DNS 要求を求めたパケット内の送信元アドレスと宛先アドレスの組み合わせに関する情報が含まれません。
- 実際には、DNS リライトは NAT ルールではなく xlate エントリで実行されます。したがって、ダイナミック ルールに xlate がない場合、リライトが正しく実行されません。スタティック NAT の場合は、同じような問題が発生しません。
- DNS のリライトによって、DNS ダイナミック アップデートのメッセージ（オペレーション コード 5）は書き換えられません。

次のトピックで、NAT ルールでの DNS リライトの例を示します。

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 サーバは実際のアドレス（209.165.200.225）を応答します。

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



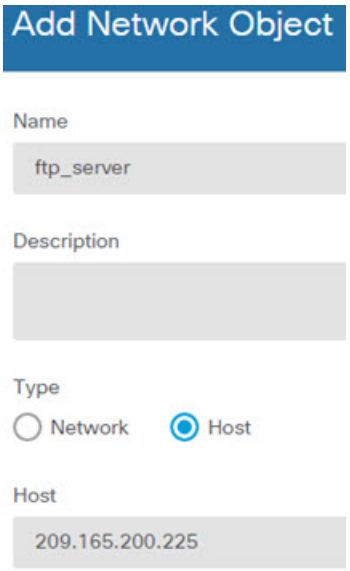
手順

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

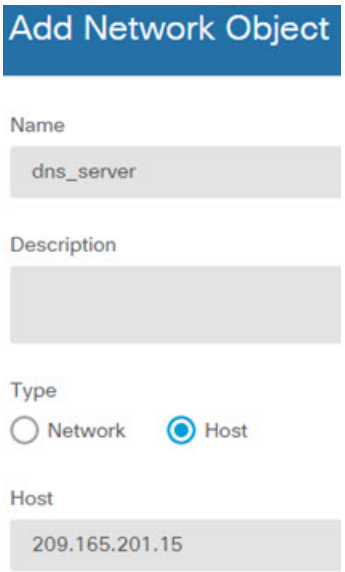
a) [オブジェクト（Objects）]を選択します。

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

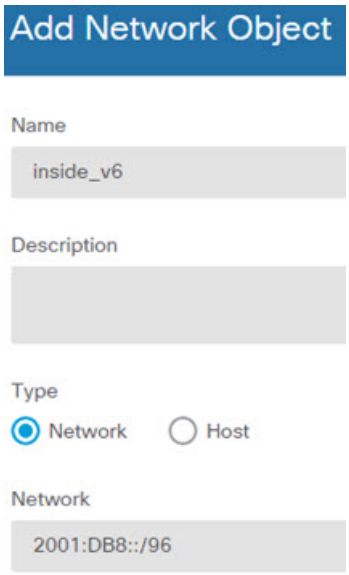
c) 実際の FTP サーバ アドレスを定義します。
ネットワーク オブジェクトに名前を付け（ftp_server など）、[ホスト（Host）]を選択して、実際のホストの IP アドレス 209.165.200.225 を入力します。



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

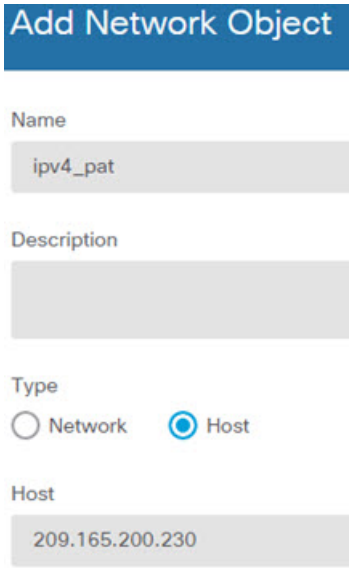


f) [追加（Add）][OK]をクリックします。
g) [+]をクリックして内部 IPv6 ネットワークを定義します。
ネットワーク オブジェクトに名前を付け（inside_v6 など）、[ネットワーク（Network）]を選択して、ネットワーク アドレス 2001:DB8::/96 を入力します。



h) [追加（Add）][OK]をクリックします。

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



j) [追加（Add）][OK]をクリックします。

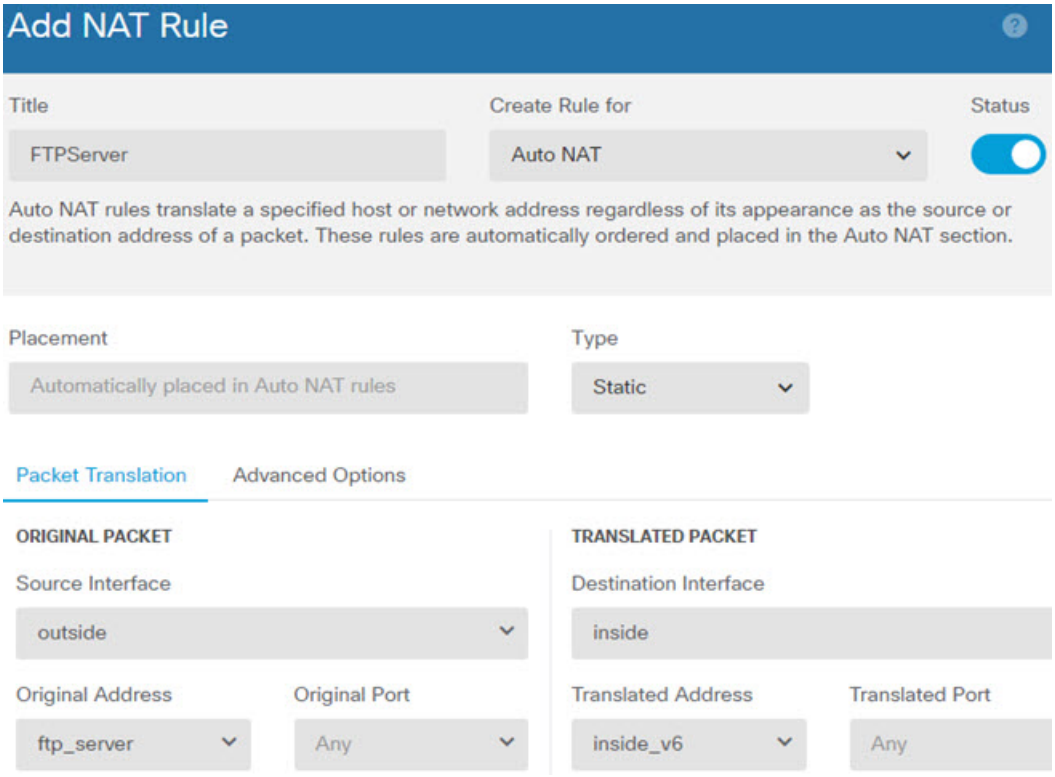
ステップ 2 FTP サーバのための、DNS 修正を設定したスタティック NAT ルールを設定します。

a) [ポリシー（Policies）] > [NAT] を選択します。

b) [+]ボタンをクリックします。

c) 次のプロパティを設定します。

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

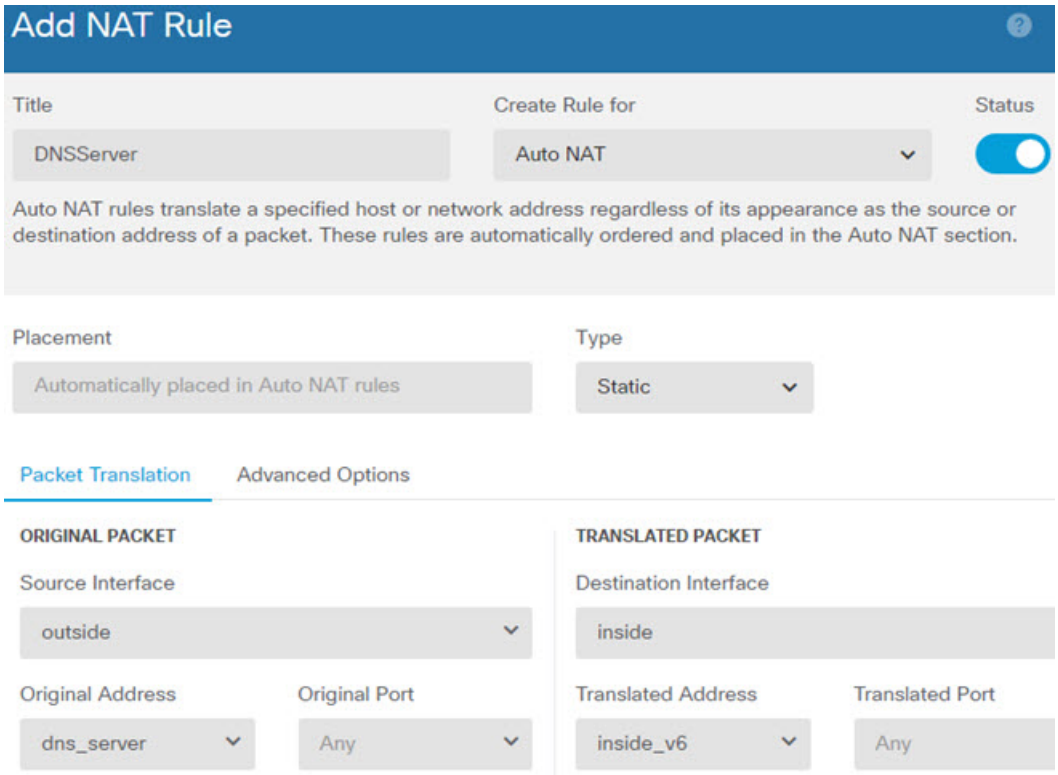


d) [OK]をクリックします。

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

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

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



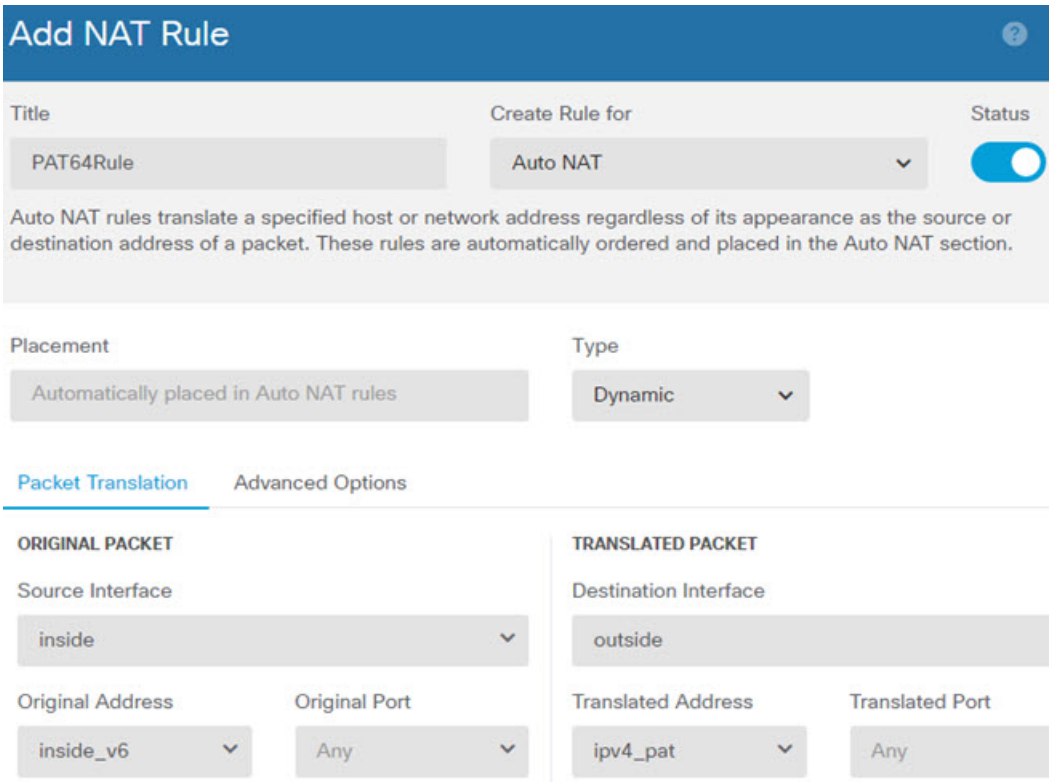
d) [OK]をクリックします。

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

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

- タイトル（Title）= PAT64Rule（または任意の別の名前）。

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



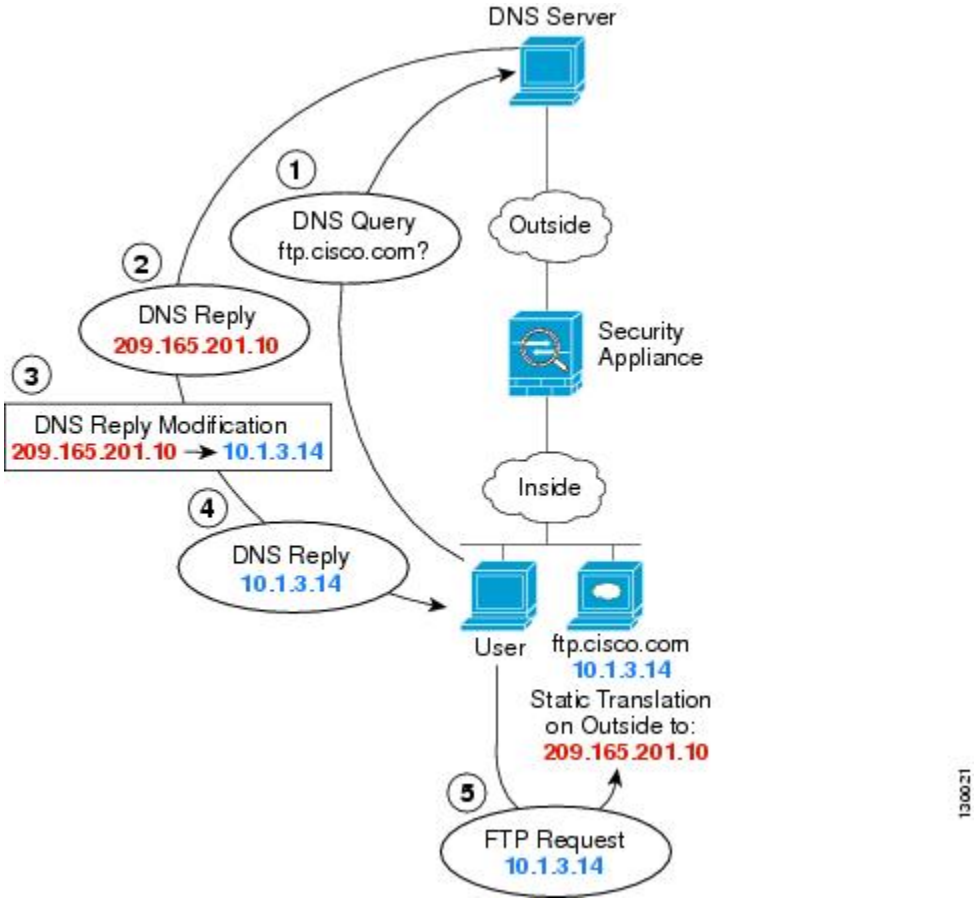
d) [OK]をクリックします。

DNS 応答修正：Outside 上の DNS サーバ

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

この場合、このスタティック ルールで DNS 応答修正を有効にする必要があります。有効にすると、実際のアドレスを使用して ftp.cisco.com にアクセスできる内部ユーザは、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 サーバはマッピング アドレス（209.165.201.10）を応答します。システムは、内部サーバのスタティック ルールを参照し、DNS 応答内のアドレスを 10.1.3.14 に変換します。DNS 応答修正を有効にしない場合、内部ホストは ftp.cisco.com に直接アクセスする代わりに、209.165.201.10 にトラフィックの送信を試みます。



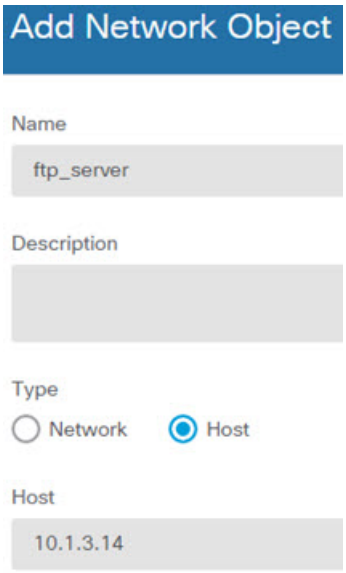
手順

ステップ 1 FTP サーバのネットワーク オブジェクトを作成します。

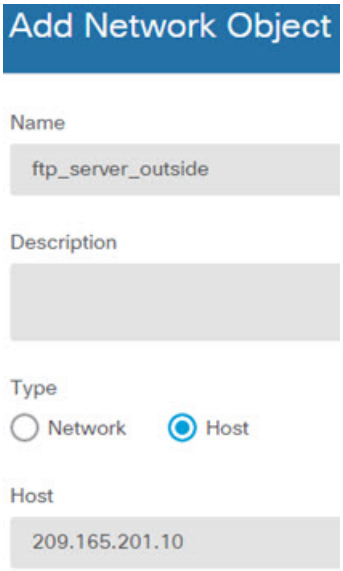
a) [オブジェクト（Objects）]を選択します。

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

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

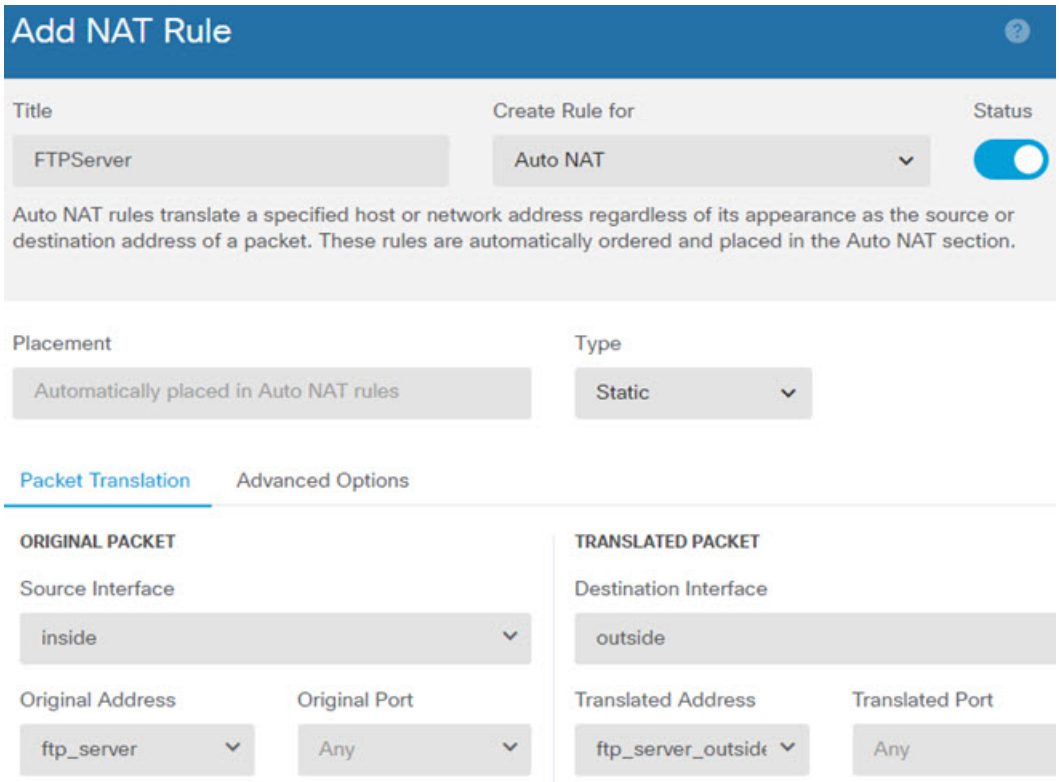


d) [追加（Add）][OK]をクリックします。
e) [+]をクリックして FTP サーバの変換済みアドレスを定義します。
ネットワーク オブジェクトに名前を付け（ftp_server_outside など）、[ホスト（Host）]を選択して、ホスト アドレス 209.165.201.10 を入力します。



ステップ 2 FTP サーバのための、DNS 修正を設定したスタティック NAT ルールを設定します。
a) [ポリシー（Policies）] > [NAT] を選択します。
b) [+]ボタンをクリックします。
c) 次のプロパティを設定します。

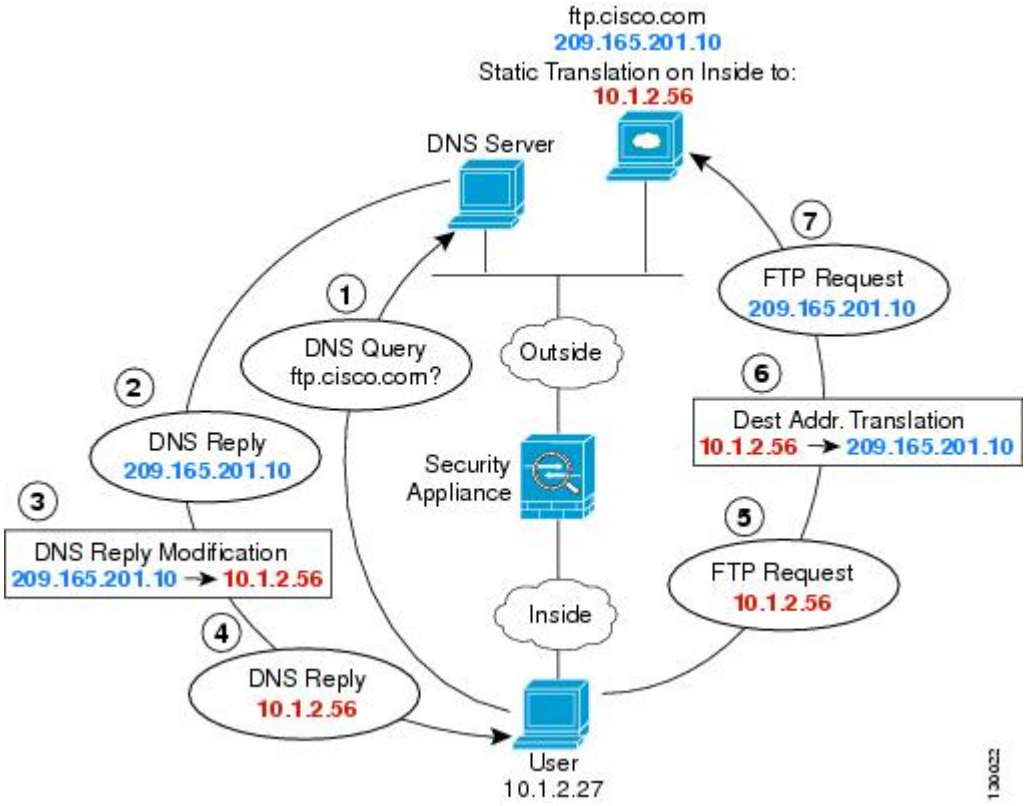
- タイトル（Title）= FTPServer（または任意の別の名前）。
- ルールの作成先（Create Rule For）= Auto NAT。
- タイプ（Type）= Static。
- 送信元インターフェイス（Source Interface）= inside。
- 宛先インターフェイス（Destination Interface）= outside。
- 元のアドレス（Original Address）= ftp_server のネットワーク オブジェクト。
- 変換済みのアドレス（Translated Address）= ftp_server_outside のネットワーク オ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



d) [OK]をクリックします。

DNS 応答修正：ホスト ネットワーク上の DNS サーバ

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



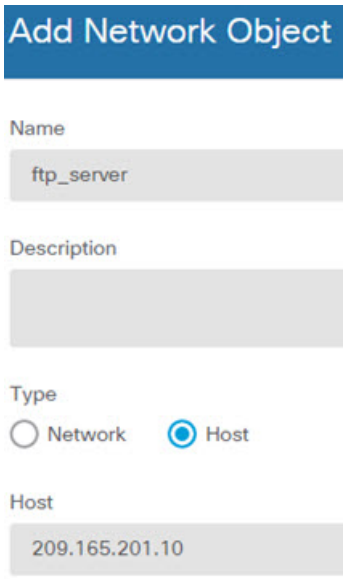
手順

ステップ 1 FTP サーバのネットワーク オブジェクトを作成します。

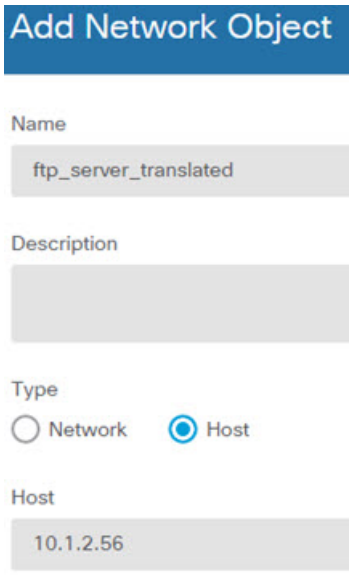
a) [オブジェクト（Objects）]を選択します。

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

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

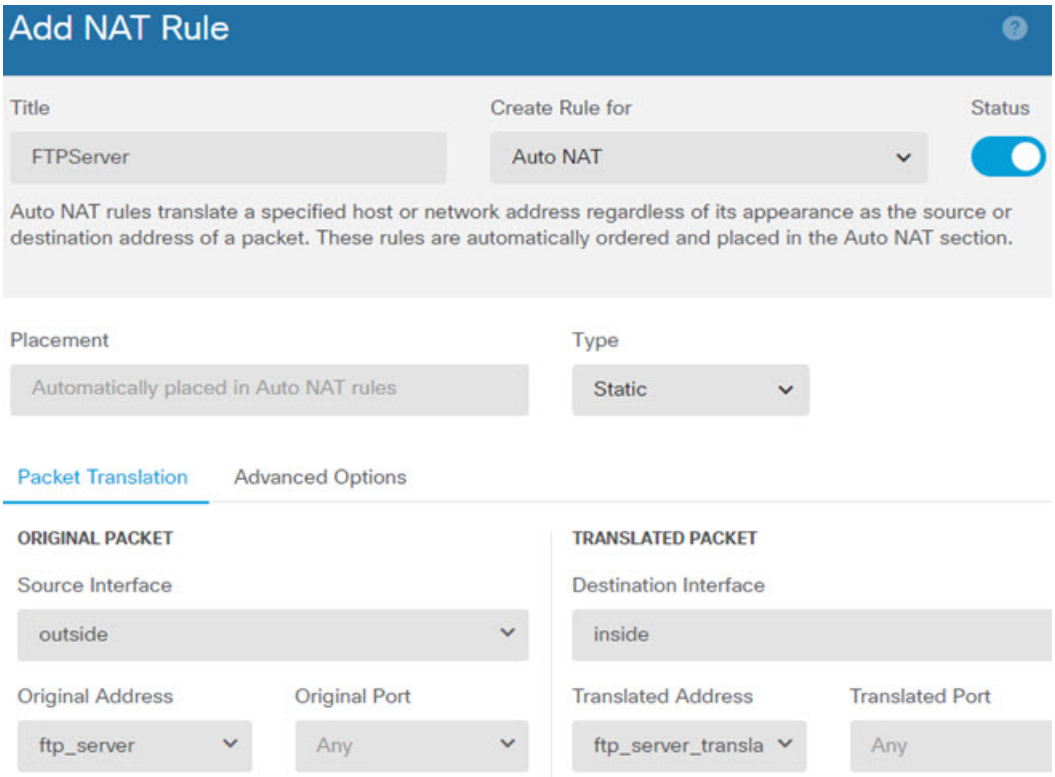


d) [追加（Add）][OK]をクリックします。
e) [+]をクリックして FTP サーバの変換済みアドレスを定義します。
ネットワーク オブジェクトに名前を付け（ftp_server_translated など）、[ホスト（Host）]を選択して、ホスト アドレス 10.1.2.56 を入力します。



ステップ 2 FTP サーバのための、DNS 修正を設定したスタティック NAT ルールを設定します。
a) [ポリシー（Policies）] > [NAT] を選択します。
b) [+]ボタンをクリックします。
c) 次のプロパティを設定します。

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



d) [OK]をクリックします。