



# ネットワーク アドレス変換

ここでは、ネットワークアドレス変換（NAT）について、および Threat Defense デバイスでそれを設定する方法について説明します。

- [NAT を使用する理由](#)（1 ページ）
- [NAT の基本](#)（2 ページ）
- [NAT ポリシーの要件と前提条件](#)（13 ページ）
- [NAT のガイドライン](#)（13 ページ）
- [NAT ポリシーの管理](#)（21 ページ）
- [脅威に対する防御のための NAT の設定](#)（23 ページ）
- [IPv6 ネットワークの変換](#)（75 ページ）
- [NAT のモニタリング](#)（89 ページ）
- [NAT の例](#)（90 ページ）
- [Threat Defense NAT の履歴](#)（139 ページ）

## 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 を設定できるためです。

NAT の他の機能には、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に変換できることに注意してください。したがって、外部アドレスを変換するように NAT を設定した場合、「実際の」は、外部ネットワークが内部ネットワークにアクセスしたときの外部ネットワークを指します。
- マッピングアドレス/ホスト/ネットワーク/インターフェイス：マッピングアドレスとは、実際のアドレスが変換されるアドレスです。内部ネットワークが外部にアクセスするときに内部ネットワークを変換するという典型的な NAT のシナリオでは、外部ネットワークが「マッピング」ネットワークになります。



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

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

## NAT タイプ

NAT は、次の方法を使用して実装できます。

- ダイナミック NAT：実際の IP アドレスのグループが、（通常は、より小さい）マッピング IP アドレスのグループに先着順でマッピングされます。実際のホストだけがトラフィックを開始できます。[ダイナミック NAT \(31 ページ\)](#) 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 アドレスの一意的送信元ポートが使用されます。[ダイナミック PAT \(37 ページ\)](#) 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 \(50 ページ\)](#) 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 \(61 ページ\)](#) を参照してください。

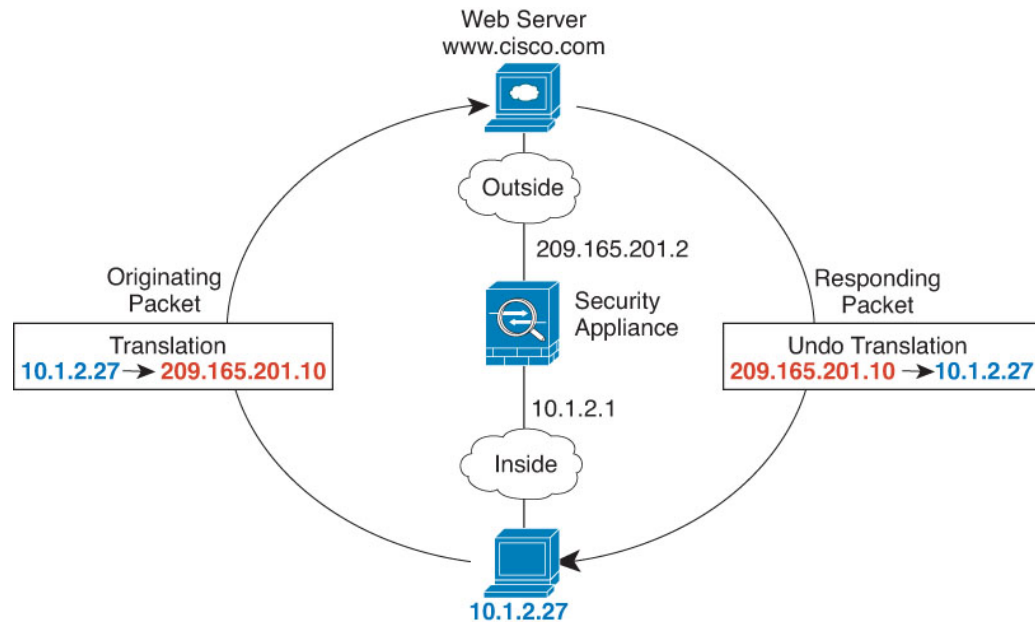
## ルーテッドモードとトランスペアレントモードの NAT

NAT は、ルーテッドモードおよびトランスペアレントファイアウォールモードの両方に設定できます。インライン、インライン タップ、またはパッシブモードで動作するインターフェイスに対しては NAT を設定できません。次の項では、各ファイアウォールモードの一般的な使用方法について説明します。

### ルーテッドモードの NAT

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

図 1: NAT の例 : ルーテッドモード



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

## トランスペアレントモードまたはブリッジグループ内の NAT

NAT をトランスペアレントモードで使用すると、ネットワークで NAT を実行するためのアップストリームルータまたはダウンストリームルータが必要なくなります。これによりルーテッドモードでブリッジグループ内で同様の機能を実行できます。

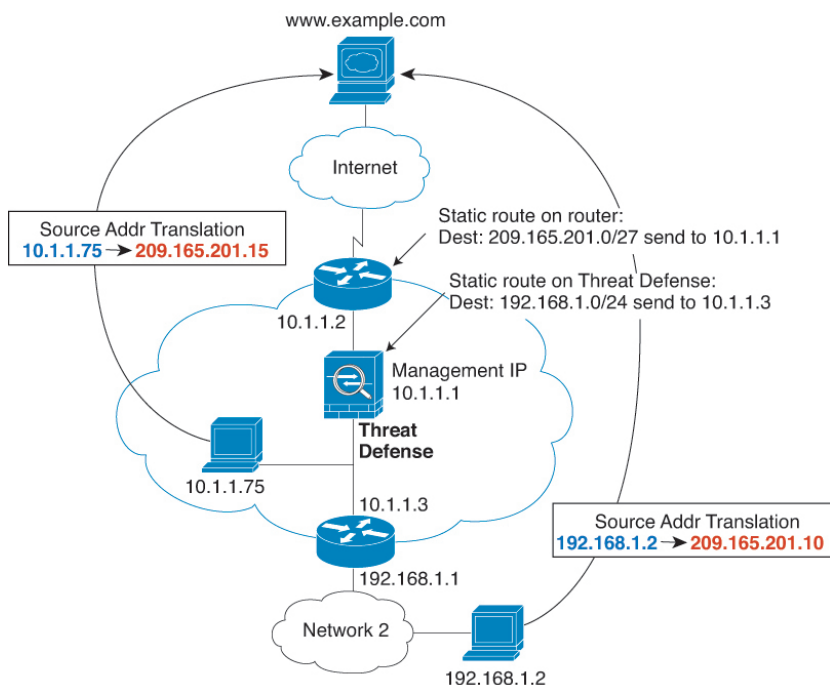
トランスペアレントモードまたは同じブリッジグループのメンバー間のルーテッドモードの NAT には、以下の要件および制限があります。

- インターフェイスに接続されている IP アドレスがないため、マッピングされたアドレスがブリッジグループメンバーのインターフェイスである場合、インターフェイス PAT を設定することはできません。
- ARP インスペクションはサポートされていません。また、何らかの理由で、一方のThreat Defenseのホストがもう一方のThreat Defenseのホストに ARP 要求を送信し、開始ホストの実際のアドレスが同じサブネットの別のアドレスにマッピングされる場合、実際のアドレスは ARP 要求で可視のままになります。

- IPv4 および IPv6 ネットワークの間の変換はサポートされていません。2つの IPv6 ネットワーク間、または2つの IPv4 ネットワーク間の変換がサポートされます。

次の図に、インターフェイス内部と外部に同じネットワークを持つ、トランスパレントモードの一般的な NAT のシナリオを示します。このシナリオのトランスパレントファイアウォールは NAT サービスを実行しているため、アップストリーム ルータは NAT を実行する必要がありません。

図 2: NAT の例: トランスパレントモード



1. 内部ホスト 10.1.1.75 が Web サーバーにパケットを送信すると、パケットの実際の送信元アドレス 10.1.1.75 はマッピングアドレス 209.165.201.15 に変更されます。
2. サーバが応答すると、マッピングアドレス 209.165.201.15 に応答を送信し、Threat Defense がそのパケットを受信します。これは、アップストリーム ルータには、Threat Defense の管理 IP アドレスに転送されるスタティック ルートのこのマッピング ネットワークが含まれるためです。
3. その後、Threat Defense はマッピングアドレス 209.165.201.15 を変換して実際のアドレス 10.1.1.1.75 に戻します。実際のアドレスは直接接続されているため、Threat Defense はそのアドレスを直接ホストに送信します。
4. ホスト 192.168.1.2 の場合も、リターントラフィックを除き、同じプロセスが発生します。Threat Defense はルーティング テーブルでルートを検索し、192.168.1.0/24 の Threat Defense スタティック ルートに基づいてパケットを 10.1.1.3 にあるダウンストリーム ルータに送信します。

## 自動 NAT および手動 NAT

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

手動 NAT の追加機能を必要としない場合は、自動 NAT を使用することをお勧めします。自動 NAT の設定が容易で、Voice over IP (VoIP) などのアプリケーションでは信頼性が高い場合があります (VoIP では、ルールで使用され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と宛先アドレスの両方を識別できます。送信元アドレスと宛先アドレスの両方を指定すると、sourceA/destinationA で sourceA/destinationB とは別の変換が行われるように指定できます。



- (注) スタティック NAT の場合、ルールは双方向であるため、たとえば、特定の接続が「宛先」アドレスから発生する場合でも、このガイド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

自動 NAT と手動 NAT の主な違いは、次のとおりです。

- 実アドレスの定義方法。
  - 自動 NAT : NAT ルールがネットワーク オブジェクトのパラメータとなります。ネットワーク オブジェクトの IP アドレスは、元の (実) アドレスとして機能します。
  - 手動 NAT : 実際のアドレスとマッピングアドレス両方のネットワークオブジェクトまたはネットワーク オブジェクト グループを識別します。この場合、NAT はネットワーク オブジェクトのパラメータではありません。ネットワーク オブジェクトまたはグループが、NAT 設定のパラメータとなります。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。このため、送信元 IP アドレス、宛先 IP アドレスにそれぞれ 1 つずつ、計 2 つのルールが使用される場合もあります。このような 2 つのルールを 1 つに結合し、送信元/宛先ペアに対して特定の変換を強制することはできません。
  - 手動 NAT : 1 つのルールにより送信元と宛先の両方が変換されます。1 つのパケットは 1 つのルールにしか一致せず、以降のルールはチェックされません。オプションの宛先アドレスを設定しない場合でも、マッチングするパケットは、1 つの手動 NAT ルールだけに一致します。送信元および宛先は相互に結び付けられるため、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、送信元 A/宛先 A のペアには、送信元 A/宛先 B のペアとは異なる変換を適用できます。
- NAT ルールの順序。
  - 自動 NAT : NAT テーブルで自動的に順序付けされます。
  - 手動 NAT : NAT テーブルで手動で順序付けします (自動 NAT ルールの前または後)。

## NAT ルールの順序

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



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

表 1: NAT ルール テーブル

テーブルのセクション	ルール タイプ	セクション内のルールの順序
セクション 1	手動 NAT	<p>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。</p> <p>「固有のルールを前に」とは、次のことを意味します。</p> <ul style="list-style-type: none"> <li>静的ルールは動的ルールの前に配置する必要があります。</li> <li>宛先変換を含むルールは、送信元変換のみのルールの前に配置する必要があります。</li> </ul> <p>送信元アドレスまたは宛先アドレスに基づいて複数のルールが適用される可能性がある重複するルールを排除できない場合は、これらの推奨事項に従うように特に注意してください。</p>



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 2	自動 NAT	<p>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。</p> <ol style="list-style-type: none"> <li>1. スタティック ルール</li> <li>2. ダイナミック ルール</li> </ol> <p>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。</p> <ol style="list-style-type: none"> <li>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。</li> <li>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。</li> <li>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。</li> </ol>
セクション 3	手動 NAT	<p>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。</p>

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

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

この結果、使用される順序は次のとおりです。

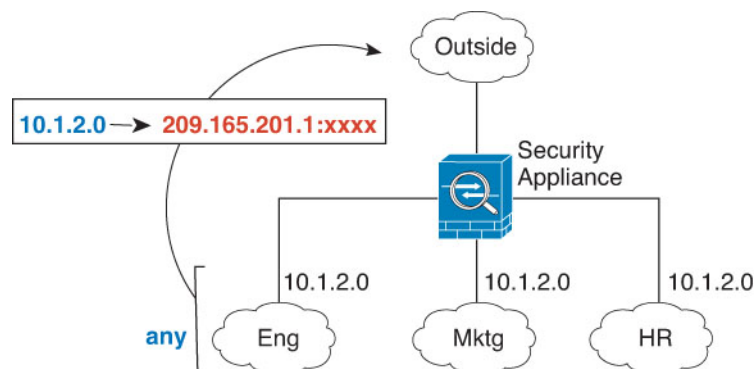
- 192.168.1.1/32 (スタティック)
- 10.1.1.0/24 (スタティック)
- 192.168.1.0/24 (スタティック)
- 172.16.1.0/24 (ダイナミック) (オブジェクト abc)
- 172.16.1.0/24 (ダイナミック) (オブジェクト def)
- 192.168.1.0/24 (ダイナミック)

## NAT インターフェイス

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

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

図 3: 任意のインターフェイスの指定



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



- (注) インライン、インライン タップ、またはパッシブ モードで動作するインターフェイスに対しては NAT を設定できません。インターフェイスの指定は、インターフェイスを含むインターフェイス オブジェクトを選択することによって間接的に行います。

## NAT 免除

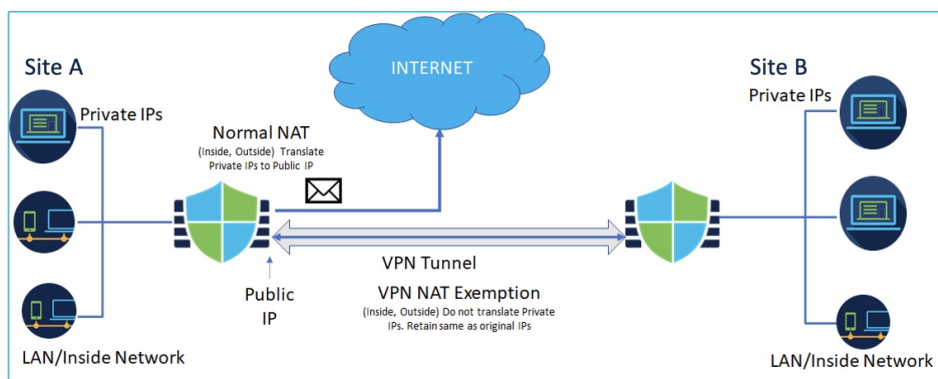
インターネットエッジデバイスのインターフェイスでサイト間 VPN が設定されていて、そのインターフェイス向けの NAT ルールがある場合、VPN トラフィックを NAT ルールの対象から除外する必要があります。NAT 変換の対象から VPN トラフィックを除外しない場合、トラフィックはドロップされるか、VPN トンネルを介してリモートピアにルーティングされません。

NAT 免除により、NAT ルールによる変換対象からトラフィックを除外できます。Management Center VPN ウィザードを使用してポリシーベースのサイト間 VPN を作成する場合、[NAT 免除 (NAT Exempt)] オプションを選択してルールを自動的に作成できます ([デバイス (Device)] > [サイト間 (Site To Site)])。デバイスの NAT 免除は、[NAT ポリシー (NAT policy)] ページ ([デバイス (Device)] > [NAT] > [NAT 免除 (NAT Exemptions)]) で確認できます。

Management Center では、すべてのポリシーベースのサイト間 VPN トポロジタイプについて、NAT 免除がサポートされています。詳細については、[ポリシーベースのサイト間 VPN の設定](#)を参照してください。

サイト A とサイト B を接続するサイト間 VPN トンネルを示す次の例を考えてみます。インターネットにアクセスする必要があるトラフィックの場合、インターネットにアクセスするために、NAT によってプライベート IP がパブリック IP アドレスに変換されます。VPN トンネルを通過する必要があるトラフィックについては、VPN ウィザードでデバイスの NAT 免除を設定する必要があります。

図 4: NAT 免除を使用したサイト間 VPN トポロジ



## NAT のルーティング設定

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

必要となるルーティング設定のタイプは、マッピングアドレスのタイプによって異なります。以下の各トピックでは、その詳細について説明します。

### マッピング インターフェイスと同じネットワーク上のアドレス

宛先（マッピング）インターフェイスと同じネットワーク上のアドレスを使用する場合、Threat Defense デバイスはプロキシ ARP を使用してマッピングアドレスの ARP 要求に応答し、マッピングアドレス宛てのトラフィックを代行受信します。この方法では、Threat Defense デバイスがその他のネットワークのゲートウェイである必要がないため、ルーティングが簡略化されます。このソリューションは、外部ネットワークに十分な数のフリーアドレスが含まれている場合に最も適しており、ダイナミック NAT またはスタティック NAT などの 1:1 変換を使用している場合は考慮が必要です。ダイナミック PAT ではアドレス数が少なくても使用できる変換の数が大幅に拡張されるため、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。



- (注) マッピングインターフェイスを任意のインターフェイスとして設定し、マッピングインターフェイスの1つとして同じネットワーク上のマッピングアドレスを指定すると、そのマッピングアドレスの ARP 要求を別のインターフェイスで受信する場合、入力インターフェイスでそのネットワークの ARP エントリを手動で設定し、その MAC アドレスを指定する必要があります。通常、マッピングインターフェイスに任意のインターフェイスを指定して、マッピングアドレスの固有のネットワークを使用すると、この状況は発生しません。入力インターフェイスの [Advanced] 設定で、ARP テーブルを設定します。

### 一意のネットワーク上のアドレス

宛先（マッピング）インターフェイスのネットワーク上で使用可能な数より多くのアドレスが必要な場合は、別のサブネット上でアドレスを指定できます。アップストリームルータには、Threat Defense デバイスを指しているマッピングアドレスのスタティックルートが必要です。

また、ルーテッドモードの場合、宛先ネットワーク上の IP アドレスをゲートウェイとして使用して、マッピングアドレスの Threat Defense デバイスにスタティックルートを設定し、ルーティングプロトコルを使用してルートを再配布することができます。たとえば、内部ネットワーク（10.1.1.0/24）には NAT を使用して、マッピング IP アドレス 209.165.201.5 を使用する

場合、209.165.201.5 255.255.255.255 (ホストアドレス) に対して、10.1.1.99 ゲートウェイへのスタティック ルートを設定し、これを再配布できます。

トランスペアレントモードの場合は、実際のホストが直接接続されている場合は、Threat Defense デバイスをポイントするようにアップストリームルータのスタティックルートを設定します。ブリッジグループの IP アドレスを指定します。トランスペアレントモードのリモートホストの場合は、上流に位置するルータのスタティック ルートで、代わりに下流ルータの IP アドレスを指定できます。

## 実際のアドレスと同じアドレス (アイデンティティ NAT)

アイデンティティ NAT のデフォルト動作で、プロキシ ARP は有効になっており、他の静的 NAT ルールと一致します。必要に応じてプロキシ ARP を無効にできます。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 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。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。このとき、実際には Threat Defense デバイス 向けのパケットでない場合でも、Threat Defense デバイスはこのアドレスの ARP をプロキシします（この問題は、手動 NAT ルールが設定されている場合にも発生します。NAT ルールは送信元と宛先のアドレス両方に一致する必要がありますが、プロキシ ARP 判定は「送信元」アドレスに対してのみ行われます）。実際のホストの ARP 応答の前に Threat Defense デバイスの ARP 応答を受信した場合、トラフィックは誤って Threat Defense デバイス に送信されます。

## NAT ポリシーの要件と前提条件

サポートされるドメイン

任意

ユーザの役割

管理者

アクセス管理者

ネットワーク管理者

## 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。

## NAT のファイアウォール モードのガイドライン

NAT は、ルーテッドモードとトランスペアレントファイアウォールモードでサポートされています。

ただし、ブリッジグループメンバーのインターフェイス（ブリッジグループ仮想インターフェイスの一部であるインターフェイス、BVI）での NAT 設定には次の制限があります。

- ブリッジグループのメンバーに NAT を設定するには、メンバーインターフェイスを指定します。NAT をブリッジグループインターフェイス（BVI）自体に設定することはできません。
- ブリッジグループメンバーのインターフェイス間で NAT を実行するときには、実際のおよびマッピングされたアドレスを指定する必要があります。インターフェイスとして「任意」を指定することはできません。
- インターフェイスに接続されている IP アドレスがないため、マッピングされたアドレスがブリッジグループメンバーのインターフェイスである場合、インターフェイス PAT を設定することはできません。
- 送信元インターフェイスと宛先インターフェイスが同じブリッジグループのメンバーである場合、IPv4 ネットワークと IPv6 ネットワーク（NAT64/46）同士を変換することはできません。スタティック NAT/PAT 44/66、ダイナミック NAT44/66、およびダイナミック PAT44 のみが許可されている方法であり、ダイナミック PAT66 はサポートされません。ただし、異なるブリッジグループのメンバー同士、またはブリッジグループのメンバー（送信元）と標準ルーテッドインターフェイス（宛先）の間では NAT64/46 を行うことができます。



(注) インライン、インライン タップ、またはパッシブ モードで動作するインターフェイスに対しては NAT を設定できません。

## IPv6 NAT のガイドライン

NAT では、IPv6 のサポートに次のガイドラインと制限が伴います。

- 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。
- 同じブリッジグループのメンバーであるインターフェイスでは、IPv4 と IPv6 の間の変換はできません。2つの IPv6 ネットワーク間または2つの IPv4 ネットワーク間でのみ変換できます。この制限は、インターフェイスが異なるブリッジグループのメンバーである場合、またはブリッジグループのメンバーと標準的なルーテッドインターフェイスの間には該当しません。
- 同じブリッジグループ内のインターフェイス間で変換する場合は、IPv6 対応のダイナミック PAT（NAT66）は使用できません。この制限は、インターフェイスが異なるブリッジ

グループのメンバーである場合、またはブリッジグループのメンバーと標準的なルーテッドインターフェイスの間には該当しません。

- スタティック NAT の場合は、/64 までの IPv6 サブネットを指定できます。これよりも大きいサブネットはサポートされません。
- FTP を NAT46 とともに使用する場合は、IPv4 FTP クライアントが IPv6 FTP サーバに接続するときに、クライアントは拡張パッシブモード (EPSV) または拡張ポートモード (EPRT) を使用する必要があります。PASV コマンドおよび PORT コマンドは IPv6 ではサポートされません。

## IPv6 NAT のベストプラクティス

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

- NAT66 (IPv6-to-IPv6) : スタティック NAT を使用することを推奨します。ダイナミック NAT または PAT を使用できますが、IPv6 アドレスは大量にあるため、ダイナミック NAT を使用する必要がありません。リターントラフィックを許可しない場合は、スタティック NAT ルールを単一方向にできます (手動 NAT のみ)。
- NAT46 (IPv4-to-IPv6) : スタティック NAT を使用することを推奨します。IPv6 アドレス空間は IPv4 アドレス空間よりもかなり大きいので、容易にスタティック変換に対応できます。リターントラフィックを許可しない場合は、スタティック NAT ルールを単一方向にできます (手動 NAT のみ)。IPv6 サブネットに変換する場合 (/96 以下)、結果のマッピングアドレスはデフォルトで IPv4 埋め込み IPv6 アドレスとなります。このアドレスでは、IPv4 アドレスの 32 ビットが IPv6 プレフィックスの後に埋め込まれています。たとえば、IPv6 プレフィックスが /96 プレフィックスの場合、IPv4 アドレスは、アドレスの最後の 32 ビットに追加されます。たとえば、201b::0/96 に 192.168.1.0/24 をマッピングする場合、192.168.1.4 は 201b::0.192.168.1.4 にマッピングされます (混合表記で表示)。/64 など、より小さいプレフィックスの場合、IPv4 アドレスがプレフィックスの後に追加され、サフィックスの 0s が IPv4 アドレスの後に追加されます。また、任意で、ネット間のアドレスを変換できます。この場合、最初の IPv6 アドレスに最初の IPv4 アドレス、2 番目 IPv6 アドレスに 2 番目の IPv4 アドレス、のようにマッピングします。
- 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、ユーザー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。これらのプロトコルの一部では、ネットワーク解析ポリシーを使用してインスペクションを他のポートに拡張できますが、NAT の書き換えはこれらのポートに拡張されません。これには、DCERPC、DNS、FTP、および Sun RPC のインスペクションが含まれます。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。	対応
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。	非対応
FTP	TCP/21	(クラスタリング) スタティック PAT なし。	対応
H.323 H.225 (コールシグナリング)	TCP/1720 UDP/1718	(クラスタリング) スタティック PAT はサポートされません。	対応
H.323 RAS	RAS の場合、 UDP/1718 ~ 1719	拡張 PAT なし NAT64 なし。	



アプリケーション	インスペクション対象 プロトコル、ポート	NAT に関する制限事項	作成済みのピンホール
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。	非対応
IP オプション	RSVP	NAT64 なし。	非対応
NetBIOS Name Server over IP	UDP/137、138 (送信元 ポート)	拡張 PAT なし NAT64 なし。	非対応
RSH	TCP/514	PAT なし。 NAT64 なし。 (クラスタリング) スタティック PAT なし。	対応
RTSP	TCP/554 (HTTP クローキング は処理しません)	拡張 PAT なし NAT64 なし。 (クラスタリング) スタティック PAT なし。	対応
SIP	TCP/5060 UDP/5060	拡張 PAT なし NAT64 または NAT46 なし (クラスタリング) スタティック PAT なし。	対応
Skinny (SCCP)	TCP/2000	拡張 PAT なし NAT64、NAT46、または NAT66 なし (クラスタリング) スタティック PAT なし。	対応
SQL*Net (バージョン 1、2)	TCP/1521	拡張 PAT なし NAT64 なし。 (クラスタリング) スタティック PAT なし。	対応
Sun RPC	TCP/111 UDP/111	拡張 PAT なし NAT64 なし。	対応
TFTP	UDP/69	NAT64 なし。 (クラスタリング) スタティック PAT なし。 ペイロード IP アドレスは変換されません。	対応

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
XDMCP	UDP/177	拡張 PAT なし NAT64 なし。 (クラスタリング) スタティック PAT なし。	対応

## FQDN 宛先のガイドライン

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

FQDN を使用すると、システムは DNS 解決を取得し、返されたアドレスに基づいて NAT ルールを書き込みます。複数の DNS サーバークラスを使用している場合は、フィルタドメインが優先され、フィルタに基づいて適切なグループからアドレスが要求されます。DNS サーバーから複数のアドレスを取得する場合、使用されるアドレスは次の情報に基づきます。

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

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

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

## NAT のその他のガイドライン

- ブリッジグループのメンバーであるインターフェイスの場合は、メンバー インターフェイス用の NAT ルールを記述します。ブリッジ仮想インターフェイス (BVI) 自体に対する NAT ルールは記述できません。
- サイト間 VPN で使用される仮想トンネルインターフェイス (VTI) の NAT ルールは作成できません。VTI の送信元インターフェイスのルールを作成すると、NAT は VPN トンネルに適用されません。VTI でトンネリングされた VPN トラフィックに適用される NAT ルールを作成するには、インターフェイスとして `[any]` を使用する必要があります。インターフェイス名を明示的に指定することはできません。

- (自動 NAT のみ)。特定のオブジェクトに対して 1 つの NAT ルールだけを定義できます。オブジェクトに対して複数の NAT ルールを設定する場合は、同じ IP アドレスを指定する異なる名前の複数のオブジェクトを作成する必要があります。
- インターフェイスで VPN が定義されている場合、そのインターフェイスの着信 ESP トラフィックには NAT ルールは適用されません。システムは、確立済みの VPN トンネルに対してのみ ESP トラフィックを許可し、既存のトンネルに関連付けられていないトラフィックはドロップされます。この制約は、ESP および UDP のポート 500 と 4500 に適用されません。
- ダイナミック PAT を適用するデバイスの背後のデバイス (VPN UDP ポート 500 と 4500 は実際に使用されるポートではない) でサイト間 VPN を定義した場合、PAT デバイスの背後にあるデバイスから接続を開始する必要があります。正しいポート番号がわからないため、レスポンドはセキュリティ アソシエーション (SA) を開始できません。
- NAT コンフィギュレーションを変更したときに、既存の変換がタイムアウトするまで待たずに新しい NAT コンフィギュレーションを使用できるようにするには、デバイス CLI で **clear xlate** コマンドを使用して変換テーブルを消去します。ただし、変換テーブルを消去すると、変換を使用している現在の接続がすべて切断されます。

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



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

- 1 つのオブジェクト グループに IPv4 と IPv6 の両方のアドレスを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。
- アドレスやサブネットの範囲内で明示的に指定するか暗黙的に指定するかにかかわらず、NAT で使用されるネットワークオブジェクトに 131,838 を超える IP アドレスを含めることはできません。アドレス空間をより狭い範囲に分割し、小さなオブジェクトに対して個別のルールを作成します。
- (手動 NAT のみ)。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。Threat Defense デバイスがパケットに対して NAT を実行する前に、パケットが IPv6-to-IPv6 または IPv4-to-IPv4 である必要があります。この前提条件では、Threat Defense デバイスは、NAT ルールの **any** の値を決定できます。たとえば、「any」から IPv6 サーバへのルールを設定しており、このサーバが IPv4 アドレスからマッピングされている場合、**any** は「任意の IPv6 トラフィック

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。
  - (トランスペアレント モード) 管理 IP アドレス。
  - (ダイナミック NAT) VPN が有効な場合は、スタンバイ インターフェイスの IP アドレス。
- スタティックおよびダイナミック NAT ポリシーでは重複アドレスを使用しないでください。たとえば、重複アドレスを使用すると、PPTP のセカンダリ接続がダイナミック xlate ではなくスタティックにヒットした場合、PPTP 接続の確立に失敗する可能性があります。
- NAT ルールの送信元アドレスとリモートアクセス VPN アドレスプールの重複アドレスは使用できません。
- ルールで宛先インターフェイスを指定すると、ルーティングテーブルでルートが検索されるのではなく、そのインターフェイスが出力インターフェイスとして使用されます。ただし、アイデンティティ NAT の場合は、代わりにルートルックアップを使用するオプションがあります。
- NFS サーバーへの接続に使用される Sun RPC トラフィックで PAT を使用する場合、PAT の対象となるポートが 1024 よりも大きいと、NFS サーバーが接続を拒否する可能性があることに注意してください。NFS サーバーのデフォルト設定では、1024 よりも大きいポートからの接続は拒否されます。エラーメッセージは、通常「Permission Denied (権限が拒否されました)」です。PAT プールのポート範囲に予約済みポート (1 ~ 1023) を含めるオプションを選択しない場合、1024 よりも大きいポートのマッピングが発生します。この問題を回避するには、すべてのポート番号を許可するように NFS サーバーの構成を変更します。
- NAT は、通過トラフィックにのみ適用されます。システムによって生成されたトラフィックは、NAT の対象外です。
- ネットワークオブジェクトまたはグループの PAT プールには、大文字と小文字を組み合わせた名前を付けないでください。
- 単方向オプションは主にテスト目的に有効であり、すべてのプロトコルで機能するとは限りません。たとえば、SIP では、NAT を使用して SIP ヘッダーを変換するためにプロトコルインスペクションが必要ですが、変換を単方向にするとこの処理は行われません。

- Protocol Independent Multicast (PIM) レジスタの内部ペイロードで NAT を使用することはできません。
- (手動 NAT) デュアル ISP インターフェイス セットアップ (ルーティング設定でサービス レベル アグリーメントを使用するプライマリ インターフェイスとバックアップ インターフェイス) の NAT ルールを作成する場合は、ルールで宛先基準を指定しないでください。プライマリ インターフェイスのルールがバックアップ インターフェイスのルールよりも前にあることを確認してください。これにより、デバイスは、プライマリ ISP が利用できない場合に、現在のルーティング状態に基づいて正しい NAT 宛先 インターフェイスを選択できます。宛先オブジェクトを指定すると、NAT ルールは、指定しない場合には重複するルールのプライマリ インターフェイスを常に選択します。
- インターフェイスに定義された NAT ルールと一致しないトラフィックについて ASP ドロップ理由 `nat-no-xlate-to-pat-pool` が示される場合は、影響を受けるトラフィックのアイデンティティ NAT ルールを設定して、トラフィックが変換されずに通過できるようにします。
- GRE トンネルエンドポイントの NAT を設定する場合は、エンドポイントでキープアライブを無効にする必要があります。無効にしないと、トンネルを確立できません。エンドポイントは、キープアライブを元のアドレスに送信します。


## NAT ポリシーの管理

ネットワークアドレス変換 (NAT) では、着信パケットの IP アドレスが発信パケットの別のアドレスに変換されます。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 では、プライベート IP アドレスがパブリック IP に置き換えられ、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がパブリックインターネットで使用可能でルーティング可能なアドレスに変換されます。NAT では、`xlate` と呼ばれる変換が追跡され、リターントラフィックが正しい未変換のホストアドレスに確実に送信されます。

### 手順

**ステップ 1** [デバイス (Devices)] > [NAT] を選択します。

**ステップ 2** NAT ポリシーを管理します。

- [作成 (Create)]: [新しいポリシー (New Policy)] をクリックして、[Threat Defense NAT] を選択します。[NAT ポリシーの作成 \(22 ページ\)](#) を参照してください。
- [コピー (Copy)]: コピーするポリシーの横にある [コピー (Copy)] () をクリックします。コピーに新しい一意の名前を付けるように求められます。コピーには、すべてのポリシールールと設定が含まれますが、デバイスの割り当ては含まれません。

- [レポート (Report)] : ポリシーの [レポート (Report)] (📄) をクリックします。ポリシー属性、デバイスの割り当て、ルール、およびオブジェクト使用情報を含むPDF レポートを保存するように求められます。
- [編集 (Edit)] : 編集するポリシーの横にある [編集 (Edit)] (✎) をクリックします。[脅威に対する防御のための NAT の設定 \(23 ページ\)](#) を参照してください。
- [削除 (Delete)] : 削除するポリシーの横にある [削除 (Delete)] (🗑️) をクリックして、[OK] をクリックします。続行するかどうかを尋ねるプロンプトで、ポリシー内に別のユーザーの未保存の変更が存在するかどうかも通知されます。

**注意** 管理対象デバイスに NAT ポリシーを展開した後は、デバイスからそのポリシーを削除できません。その代わりに、ルールを持たない NAT ポリシーを展開して、すでに管理対象デバイスに存在する NAT ルールを削除する必要があります。また、どのターゲットデバイスでも、最後に展開したポリシーは期限切れであっても削除できません。ポリシーを完全に削除する前に、それらのターゲットに異なるポリシーを展開する必要があります。

## NAT ポリシーの作成

新しい NAT ポリシーを作成する場合、少なくとも一意の名前を付ける必要があります。ポリシーの作成時にポリシー ターゲットを特定する必要はありませんが、ポリシーを展開する前に、この手順を実行する必要があります。ルールを持たない NAT ポリシーをデバイスに適用すると、そのデバイスからすべての NAT ルールが削除されます。

### 手順

**ステップ 1** [デバイス (Devices)] > [NAT] を選択します。

**ステップ 2** [新しいポリシー (New Policy)] をクリックし、ドロップダウンリストで、Threat Defense デバイスの [Threat Defense NAT] を選択します。

**Firepower NAT** は、このマニュアルで説明されていない古いデバイス用です。

**ステップ 3** [名前 (Name)] に一意の名前を入力します。

**ステップ 4** 必要に応じて、[説明 (Description)] を入力します。

**ステップ 5** ポリシーを展開するデバイスを選択します。

- [使用可能なデバイス (Available Devices)] リストでデバイスを選択し、[ポリシーに追加 (Add to Policy)] をクリックします。
- [使用可能なデバイス (Available Devices)] リストから [選択されたデバイス (Selected Devices)] リストに、デバイスをクリックしてドラッグします。
- デバイスの横にある [削除 (Delete)] (🗑️) をクリックして、[選択されたデバイス (Selected Devices)] リストからデバイスを削除します。

ステップ6 [保存 (Save)] をクリックします。

## NAT ポリシーの対象の設定

ポリシーを適用する管理対象デバイスは、ポリシーを作成または編集する際に特定できます。使用可能なデバイスおよび高可用性ペアのリストを検索して、選択したデバイスのリストに追加できます。

### 手順

ステップ1 [デバイス (Devices)] > [NAT] を選択します。

ステップ2 変更する NAT ポリシーの横にある [編集 (Edit)] (✎) をクリックします。

代わりに [表示 (View)] (👁) が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ3 [ポリシー割り当て (Policy Assignments)] をクリックします。

ステップ4 次のいずれかを実行します。

- デバイス、高可用性ペア、またはデバイスグループをポリシーに割り当てるには、[使用可能なデバイス (Available Devices)] リストで選択し、[ポリシーに追加 (Add to Policy)] をクリックします。ドラッグアンドドロップを使用することもできます。
- デバイスの割り当てを削除するには、[選択されたデバイス (Selected Devices)] リストのデバイス、高可用性ペア、またはデバイスグループの横にある [削除 (Delete)] (🗑) をクリックします。

ステップ5 [OK] をクリックします。

## 脅威に対する防御のための 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。

NAT ポリシーは、共有ポリシーです。同様の NAT ルールを持つべきデバイスに、ポリシーを割り当てます。

割り当てられたデバイスにポリシーの特定のルールが適用されるかどうかは、ルールで使用されるインターフェイスオブジェクト (セキュリティゾーンまたはインターフェイスグループ) によって決定されます。インターフェイスオブジェクトにデバイスのインターフェイスが1つ以上含まれている場合、ルールがデバイスに導入されます。したがって、注意深くインター

フェイスオブジェクトを設計することで、単一の共有ポリシー内のデバイスのサブセットに適用されるルールを設定できます。「任意」のインターフェイスオブジェクトに適用されるルールは、すべてのデバイスに導入されます。

インターフェイスのタイプを、そのインターフェイスがあるデバイスを対象とする NAT ポリシーでの使用が無効なタイプに変更した場合、ポリシーはそのインターフェイスに削除済みのラベルを付けます。NAT ポリシーの [保存 (Save)] をクリックすると、インターフェイスはポリシーから自動的に削除されます。

デバイスのグループにさまざまなルールが必要な場合は、複数の NAT ポリシーを設定できます。

## 手順

**ステップ 1** [デバイス (Devices)] > [NAT] を選択します。

- 新しいポリシーを作成するには、[新しいポリシー (New Policy)] > [Threat Defense NAT] をクリックします。ポリシーに名前を付け、オプションでデバイスを割り当て、[保存 (Save)] をクリックします。

デバイスの割り当てを後で変更するには、ポリシーを編集して、[ポリシー割り当て (Policy Assignments)] をクリックします。

- 既存の Threat Defense NAT ポリシーを編集するには、[編集 (Edit)] (✎) をクリックします。このページには、Threat Defense デバイスでは使用されない Firepower NAT ポリシーも表示されます。

代わりに [表示 (View)] (👁) が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

**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。

これらの 2 つの実装オプションの比較については、[自動 NAT および手動 NAT \(6 ページ\)](#) を参照してください。

**ステップ 4** デバイスごとにカスタマイズするルールを決定します。

複数のデバイスに 1 つの NAT ポリシーを割り当てることができるため、多くのデバイスに 1 つのルールを設定できます。ただし、各デバイスによって異なる解釈が必要なルールや、デバイスのサブセットにのみ適用すべきルールの場合もあります。

インターフェイスオブジェクトを使用して、ルールを設定するデバイスを制御します。次に、ネットワークオブジェクトでオブジェクトのオーバーライドを使用して、デバイスごとに使用されるアドレスをカスタマイズします。





詳細については、[複数のデバイスの NAT ルールのカスタマイズ \(26 ページ\)](#) を参照してください。

**ステップ 5** 次の項で説明するルールを作成します。

- [ダイナミック NAT \(31 ページ\)](#)
- [ダイナミック PAT \(37 ページ\)](#)
- [スタティック NAT \(50 ページ\)](#)
- [アイデンティティ NAT \(61 ページ\)](#)

**ステップ 6** 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。

- ポリシーの名前または説明を編集するには、これらのフィールドをクリックし、変更を入力して、フィールドの外側をクリックします。
- 特定のデバイスに適用されるルールのみを表示するには、[デバイスによるフィルタ (Filter by Device)] をクリックし、目的のデバイスを選択します。ルールがデバイスのインターフェイスを含むインターフェイスオブジェクトを使用している場合、そのデバイスにルールが適用されます。
- ポリシーの警告またはエラーを表示するには、[Show warnings] をクリックして、[Device] を選択します。警告とエラーによって、トラフィックフローに悪影響を及ぼしたり、ポリシーの展開を妨げたりする構成がマークされます。
- ポリシーが割り当てられているデバイスを変更するには、[ポリシー割り当て (Policy Assignments)] リンクをクリックし、必要に応じて選択したデバイス リストを変更します。
- ルールが有効であるか、または無効であるかを変更するには、ルールを右クリックし、[状態 (State)] コマンドから目的のオプションを選択します。これらのコントロールを使用して、ルールを削除しないで一時的に無効にすることができます。
- ルールを追加するには、[ルールの追加 (Add Rule)] ボタンをクリックします。
- ルールを編集するには、ルールの[編集 (Edit)] () 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)] () をクリックします。
- ページに表示するルールの数を変更するには、[Rows Per Page] ドロップダウンリストを使用します。
- 有効化、無効化、または削除する複数のルールを選択するには、各ルールのチェックボックスまたはヘッダーのチェックボックスをクリックしてから、アクションを実行します。

**ステップ 7** [Save (保存)] をクリックします。

これで、[展開 (Deploy)] > [展開 (Deployment)] をクリックし、割り当てたデバイスにポリシーを展開できるようになりました。変更はポリシーを展開するまで有効になりません。

## 複数のデバイスの NAT ルールのカスタマイズ

NAT ポリシーは共有されるため、複数のデバイスに特定のポリシーを割り当てることができません。ただし、指定したオブジェクトに設定できる自動 NAT ルールは 1 つまでです。そのため、変換を実行する特定のデバイスに基づいてオブジェクトにさまざまな変換を設定する場合は、インターフェイスオブジェクト（セキュリティゾーンまたはインターフェイスグループ）を注意深く設定し、変換済みアドレスのネットワークオブジェクトのオーバーライドを定義する必要があります。

インターフェイスオブジェクトでは、ルールを設定するデバイスを決定します。ネットワークオブジェクトのオーバーライドでは、そのオブジェクトの特定のデバイスで使用する IP アドレスを決定します。

次のような例が考えられます。

- FTD-A と FTD-B に、「inside」という名前のインターフェイスに接続される内部ネットワーク 192.168.1.0/24 があります。
- FTD-A では、「外部」インターフェイスに移動するときに、すべての 192.168.1.0/24 アドレスを 10.100.10.10 ~ 10.100.10.200 の範囲の NAT プールに変換する必要があります。
- FTD-B では、「外部」インターフェイスに移動するときに、すべての 192.168.1.0/24 アドレスを 10.200.10.10 ~ 10.200.10.200 の範囲の NAT プールに変換する必要があります。

このように変換するには、次の手順を実行します。この例のルールはダイナミック自動 NAT 用ですが、任意のタイプの NAT ルールにこのテクニックを一般化できます。

### 手順

**ステップ 1** 内部インターフェイスと外部インターフェイスのセキュリティゾーンを作成します。

- a) [オブジェクト (Objects)] > [オブジェクト管理 (Object Management)] を選択します。
- b) コンテンツのテーブルから [インターフェイス オブジェクト (Interface Objects)] を選択し、[追加 (Add)] > [セキュリティ ゾーン (Security Zone)] をクリックします。（ゾーンの代わりにインターフェイスグループを使用できます）。
- c) 内部ゾーンのプロパティを設定します。
  - [名前 (Name)] : **inside-zone** などの名前を入力します。
  - [タイプ (Type)] : ルーテッドモードのデバイスの場合は [ルーテッド (Routed)]、トランスペアレントモードの場合は [スイッチド (Switched)] を選択します。
  - [選択したインターフェイス (Selected Interfaces)] : 選択済みリストに FTD-A/内部および FTD-B/内部インターフェイスを追加します。

- d) [保存 (Save) ] をクリックします。
- e) [追加 (Add) ] > [セキュリティ ゾーン (Security Zone) ] をクリックし、外部ゾーンのプロパティを定義します。
  - [名前 (Name) ] : **outside-zone** などの名前を入力します。
  - [インターフェイスタイプ (Interface Type) ] : ルーテッドモードのデバイスの場合は [ルーテッド (Routed) ]、トランスペアレントモードの場合は [スイッチド (Switched) ] を選択します。
  - [選択したインターフェイス (Selected Interfaces) ] : 選択済みリストに FTD-A/外部および FTD-B/外部インターフェイスを追加します。
- f) [保存 (Save) ] をクリックします。

**ステップ 2** [オブジェクト管理 (Object Management) ] ページで、元の内部ネットワーク内のネットワーク オブジェクトを作成します。

- a) コンテンツのテーブルから [ネットワーク (Network) ] を選択し、[ネットワークの追加 (Add Network) ] > [Add Object (オブジェクトの追加) ] をクリックします。
- b) 内部ネットワークのプロパティを設定します。
  - [名前 (Name) ] : **inside-network** などの名前を入力します。
  - [ネットワーク (Network) ] : **192.168.1.0/24** などのネットワーク アドレスを入力します。
- c) [保存 (Save) ] をクリックします。

**ステップ 3** 変換済み NAT プールのネットワーク オブジェクトを作成し、オーバーライドを定義します。

- a) [ネットワークの追加 (Add Network) ] > [Add Object (オブジェクトの追加) ] をクリックします。
- b) FTD-A の NAT プールのプロパティを設定します。
  - [名前 (Name) ] : **NAT-pool** などの名前を入力します。
  - [ネットワーク (Network) ] : **10.100.10.10-10.100.10.200** などの FTD-A のプールに含めるアドレスの範囲を入力します。
- c) [オーバーライドを許可 (Allow Overrides) ] を選択します。
- d) [オーバーライド (Override) ] の見出しをクリックして、オブジェクト オーバーライドのリストを開きます。
- e) [追加 (Add) ] をクリックして、[オブジェクト オーバーライドの追加 (Add Object Override) ] ダイアログボックスを開きます。
- f) FTD-B を選択し、[選択されたデバイス (Selected Devices) ] リストに追加します。
- g) [オーバーライド (Override) ] をクリックし、[ネットワーク (Network) ] を [10.200.10.10-10.200.10.200] に変更します。
- h) [追加 (Add) ] をクリックして、オーバーライドをデバイスに追加します。

FTD-B のオーバーライドを定義すると、FTD-B のこのオブジェクトが設定されるたびに、元のオブジェクトに定義されている値の代わりにオーバーライド値が使用されます。

- i) [保存 (Save) ] をクリックします。

**ステップ 4** NAT ルールを設定します。

- a) [デバイス (Devices) ] > [NAT] を選択し、Threat Defense NAT ポリシーを作成または編集します。
- b) [ルールの追加 (Add Rule) ] をクリックします。
- c) 次のプロパティを設定します。

- [NAT ルール (NAT Rule) ] = 自動 NAT ルール。
- [タイプ (Type) ] = Dynamic。

- d) [インターフェイスオブジェクト (Interface Objects) ] で、次の項目を設定します。

- [送信元インターフェイス オブジェクト (Source Interface Objects) ] : inside-zone。
- [宛先インターフェイス オブジェクト (Destination Interface Objects) ] : outside-zone。

(注) インターフェイスオブジェクトはルールが設定されるデバイスを制御します。この例ではゾーンに FTD-A と FTD-B のインターフェイスのみが含まれているため、NAT ポリシーが追加のデバイスに割り当てられた場合でも、ルールはこれらの 2 つのデバイスにのみ展開されます。

- e) [変換 (Translation) ] で、次の項目を設定します。

- [元の送信元 (Original Source) ] : inside-network オブジェクト。
- [変換済み送信元 (Translated Source) ] > [アドレス (Address) ] : NAT-pool オブジェクト。

- f) [保存 (Save) ] をクリックします。

各ファイアウォールによって保護される内部ネットワークに固有の変換を指定して、1 つのルールを FTD-A と FTD-B で異なるように解釈できるようになりました。

## NAT ルールテーブルの検索とフィルタリング

NAT ルールテーブルを検索およびフィルタ処理して、変更または表示する必要があるルールを見つけることができます。テーブルをフィルタ処理すると、一致するルールのみが表示されます。ルール番号は 1、2、というように連続的に変化しますが、フィルタ処理によって、実際のルール番号や、非表示のルールに相対するテーブル内のルールの位置は変更されないことに注意してください。フィルタ処理では、関心のあるルールを見つけるのに役立つように、表示されるものを変更するだけです。

NAT ポリシーを編集するときは、テーブルの上にあるフィールドを使用して、次のタイプの検索/フィルタ処理を実行できます。

- **デバイスによるフィルタ**：[デバイスによるフィルタ (Filter by Device)] をクリックし、ルールを表示するデバイスを選択して、[OK] をクリックします。ルールがデバイスに適用されるかどうかは、ルールのインターフェイス制約によって決まります。送信元または宛先インターフェイスのいずれかにセキュリティゾーンまたはインターフェイスグループを指定した場合、デバイスの少なくとも1つのインターフェイスがゾーンまたはグループにあると、ルールがデバイスに適用されます。NAT ルールが任意の送信元および任意の宛先インターフェイスに適用される場合、すべてのデバイスに適用されます。

テキストまたは複数属性検索も実行すると、結果は選択したデバイスに限定されます。

このフィルタを削除するには、[デバイスによるフィルタ (Filter by Device)] をクリックしてデバイスの選択を解除するか、[すべて (All)] を選択して [OK] をクリックします。

- **単純なテキスト検索**：[フィルタ (Filter)] ボックスに文字列を入力し、Enter キーを押します。文字列は、ルール内のすべての値と比較されます。たとえば、ネットワークオブジェクトの名前である「network-object-1」を入力すると、送信元、宛先、および PAT プール属性でそのオブジェクトを使用するルールが取得されます。

ネットワークオブジェクトとポートオブジェクトの場合、文字列はルールで使用されるオブジェクトの内容とも比較されます。たとえば、PAT プールオブジェクトに 10.100.10.3 ~ 10.100.10.100 の範囲が含まれている場合、10.100.10.3 または 10.100.10.100 (または部分的に 10.100.10) で検索すると、その PAT プールオブジェクトを使用するルールが含まれます。ただし、完全に一致する必要があります。10.100.10.5 での検索は、この IP アドレスがオブジェクトの IP アドレス範囲内にある場合でも、この PAT プールオブジェクトと一致しません。

フィルタを削除するには、[フィルタ (Filter)] ボックスの右側にある [x] をクリックします。

- **複数属性検索**：単純なテキスト検索でヒット数が多すぎる場合は、検索に複数の値を設定できます。[フィルタ (Filter)] ボックスをクリックして属性のリストを開き、検索する属性の文字列を選択または入力して、[フィルタ (Filter)] ボタンをクリックします。これらの属性は、NAT ルール内で構成する属性と同じです。属性は AND 結合されているため、フィルタ処理された結果には、構成したすべての属性に一致するルールのみが含まれます。

- ルールの状態 (有効/無効)、PAT プールが構成されているか (有効/無効)、ルールの方向 (単方向/双方向)、ルールタイプ (静的/動的) などのバイナリ属性については、必要に応じてボックスをオンまたはオフにします。属性値を気にしない場合は、両方のボックスをオンにしてください。両方のボックスをオフにすると、どのルールもフィルタに一致しません。

- 文字列属性の場合、その属性に関連する文字列の全体または一部を入力します。これらは、セキュリティゾーン/インターフェイスグループ、ネットワークオブジェクト、またはポートオブジェクトのいずれかのオブジェクト名になります。また、ネットワークオブジェクトまたはポートオブジェクトのコンテンツである場合もあり、単純なテキスト検索の場合と同じ方法で照合されます。

フィルタを削除するには、[フィルタ (Filter) ] ボックスの右側にある [x] をクリックするか、[フィルタ (Filter) ] ボックスをクリックしてドロップダウンリストを開き、[クリア (Clear) ] ボタンをクリックします。

## 複数ルールの有効化、無効化、または削除

手動 NAT ルールを有効または無効にしたり、NAT ルールを 1 つずつ削除することができます。複数のルールを選択して、それらのすべてに一度に変更を適用することもできます。有効化/無効化は手動 NAT にのみ適用されるため、複数のルールタイプを組み合わせで選択した場合は、それらのみを削除できます。

ルールを有効または無効にする場合、すでに有効または無効になっているいくつかのルールを選択しても問題ないことに注意してください。たとえば、すでに有効になっているルールを有効にすると、そのルールは有効のままになります。

### 手順

**ステップ 1** [デバイス (Devices) ] > [NAT] を選択し、Threat Defense の NAT ポリシーを編集します。

**ステップ 2** (オプション) NAT ルールをフィルタ処理して、変更するものを見つけます。

フィルタ処理は、大規模な NAT ポリシーがある場合に特に役立ちます。たとえば、無効になっているルールを検索して、有効にする必要があるルールを見つけることができます。

**ステップ 3** 変更するルールを選択します。

- 個々のルールを選択 (または選択解除) するには、ルールの左側の列にあるチェックボックスをクリックします。
- 現在表示されているページのすべてのルールを選択するには、テーブルの見出しにあるチェックボックスをクリックします。

ページ間を移動しても、選択内容は保持されます。ただし、実際には、次のページに移動する前に、ページで選択したルールに対してアクションを実行することが最も合理的です。

**ステップ 4** 目的のアクションを実行します。複数のルールを選択する場合、アクションの確認を求められます。

これらのアクションは、右クリックメニューでも実行できることに注意してください。

- すべてのルールを有効にするには、[一括アクションの選択 (Select Bulk Action) ] > [有効化 (Enable) ] をクリックします。
- すべてのルールを無効にするには、[一括アクションの選択 (Select Bulk Action) ] > [無効化 (Disable) ] をクリックします。

- すべてのルールを削除するには、[一括アクションの選択 (Select Bulk Action)] > [削除 (Delete)] 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。リモートホストからの接続が成功すると、接続のアイドルタイマーがリセットされます。

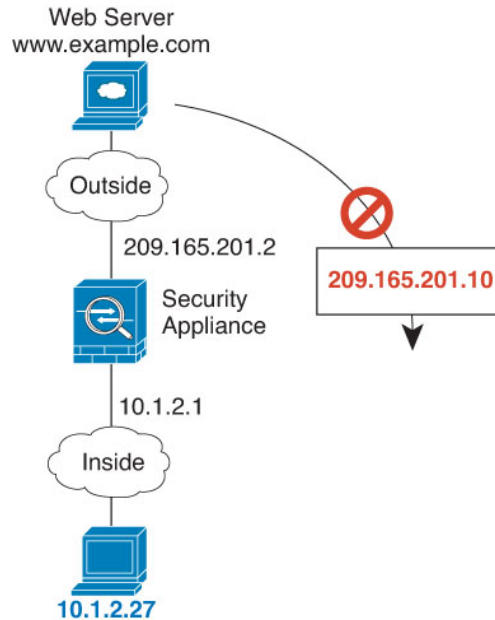
次の図に、一般的なダイナミック NAT のシナリオを示します。実際のホストだけが NAT セッションを作成でき、応答トラフィックが許可されます。

図 5: 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 6: 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、オープンスタンダード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。



## 始める前に

[オブジェクト (Objects)] > [オブジェクト管理 (Object Management)] 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。または、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す必要があります。

- [元の送信元 (Original Source)] : 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、範囲またはサブネットも可能です。
- [変換済み送信元 (Translated Source)] : 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。グループに範囲とホスト IP アドレスの両方が含まれている場合、範囲はダイナミック NAT に使用され、ホスト IP アドレスは PAT のフォールバックとして使用されます。

## 手順

**ステップ 1** [デバイス (Devices)] > [NAT] を選択し、Threat Defense NAT ポリシーを作成または編集します。

**ステップ 2** 次のいずれかを実行します。

- [ルールの追加 (Add Rule)] ボタンをクリックして、新しいルールを作成します。
- [編集 (Edit)] (✎) をクリックして、既存のルールを編集します。

メニューを右クリックすると、ルールの切り取り、コピー、貼り付け、挿入、および削除オプションが表示されます。

**ステップ 3** 基本ルールのオプションを設定します。

- [NAT ルール (NAT Rule)] : [自動 NAT ルール (Auto NAT Rule)] を選択します。
- [タイプ (Type)] : [ダイナミック (Dynamic)] を選択します。

**ステップ 4** [インターフェイスオブジェクト (Interface Objects)] で、次のフィールドを設定します。

- [送信元インターフェイスオブジェクト (Source Interface Objects)]、[宛先インターフェイスオブジェクト (Destination Interface Objects)] : (ブリッジグループメンバーインターフェイスの場合に必要)。この NAT ルールを適用するインターフェイスを特定するインターフェイス オブジェクト (セキュリティゾーンまたはインターフェイスグループ)。  
[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を含んでいるオブジェクトです。[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を含んでいるオブジェクトです。デフォルトでは、ルールはブリッジグループメンバー インターフェイスを除くすべてのインターフェイス ([Any]) に適用されます。

**ステップ 5** [変換 (Translation)] で、次のオプションを設定します。

- [元の送信元 (Original Source)] : 変換するアドレスを含むネットワーク オブジェクト。

- [変換済み送信元 (Translated Source) ] : 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 6** (オプション) [詳細 (Advanced) ] で、必要なオプションを選択します。

- [このルールに一致する DNS 応答を変換 (Translate DNS replies that match this rule) ] : DNS 応答の IP アドレスを変換するかどうかを指定します。マッピングインターフェイスから実際のインターフェイスに移動する DNS 応答の場合、アドレス (IPv4 A または IPv6 AAAA) レコードはマッピングされた値から実際の値に書き換えられます。反対に、実際のインターフェイスからマッピング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 クエリと応答の書き換え \(123 ページ\)](#) 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 (Fallthrough to Interface PAT) ] (宛先インターフェイス) : 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、ブリッジグループのメンバーではない宛先インターフェイスを選択した場合にのみ使用できます。インターフェイスの IPv6 アドレスを使用するには、[IPv6] オプションも選択します。
- [IPv6] : インターフェイス PAT に宛先インターフェイスの IPv6 アドレスを使用するかどうかを指定します。

**ステップ 7** [保存 (Save) ] をクリックしてルールを追加します。

**ステップ 8** NAT ページで [保存 (Save) ] をクリックして変更を保存します。

## ダイナミック手動 NAT の設定

自動 NAT では要件を満たせない場合は、ダイナミック手動 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。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。

### 始める前に

[オブジェクト (Objects) ] > [オブジェクト管理 (Object Management) ] 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。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 ルールを定義しているときに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。

- [元の送信元 (Original Source) ] : ネットワークオブジェクトまたはグループを指定できます。ホスト、範囲、またはサブネットを含めることができます。すべての元の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 (Translated Source) ] : 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。グループに範囲とホスト IP アドレ

スの両方が含まれている場合、範囲はダイナミック NAT に使用され、ホスト IP アドレスは PAT のフォールバックとして使用されます。

ルールで各アドレスの静的変換を設定すると、[元の宛先 (Original Destination)] および [変換済み宛先 (Translated Destination)] のネットワークオブジェクトまたはグループを作成できません。

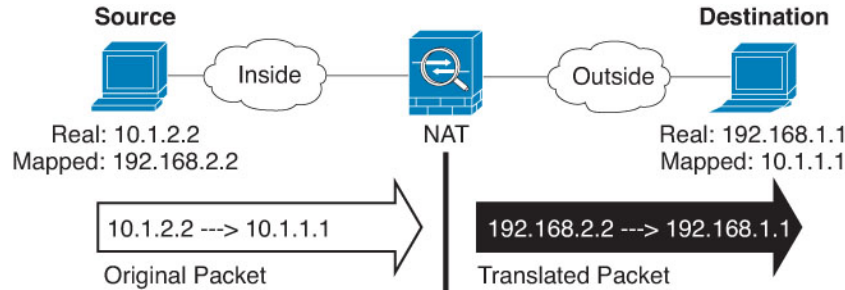
ダイナミック NAT の場合、宛先でポート変換を実行することもできます。オブジェクトマネージャで、[元の宛先ポート (Original Destination Port)] と [変換済み宛先ポート (Translated Destination Port)] に使用できるポートオブジェクトがあることを確認します。送信元ポートを指定した場合、無視されます。

## 手順

- 
- ステップ 1** [デバイス (Devices)] > [NAT] を選択し、Threat Defense NAT ポリシーを作成または編集します。
- ステップ 2** 次のいずれかを実行します。
- [ルールの追加 (Add Rule)] ボタンをクリックして、新しいルールを作成します。
  - [編集 (Edit)] (✎) をクリックして、既存のルールを編集します。
- メニューを右クリックすると、ルールの切り取り、コピー、貼り付け、挿入、および削除オプションが表示されます。
- ステップ 3** 基本ルールのオプションを設定します。
- [NAT ルール (NAT Rule)] : [手動 NAT ルール (Manual NAT Rule)] を選択します。
  - [タイプ (Type)] : [ダイナミック (Dynamic)] を選択します。この設定は送信元アドレス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。
  - [有効化 (Enable)] : ルールをアクティブにするかどうかを指定します。ルールページの右クリックメニューを使用して、後でルールをアクティブ化または非アクティブ化することができます。
  - [挿入 (Insert)] : 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)、または指定するルール番号の上下に挿入できます。
- ステップ 4** [インターフェイスオブジェクト (Interface Objects)] で、次のフィールドを設定します。
- [送信元インターフェイスオブジェクト (Source Interface Objects)]、[宛先インターフェイスオブジェクト (Destination Interface Objects)] : (ブリッジグループメンバーインターフェイスの場合に必要)。この NAT ルールを適用するインターフェイスを特定するインターフェイスオブジェクト (セキュリティゾーンまたはインターフェイスグループ)。  
[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を含んでいるオブジェクトです。[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を含んでいるオブジェクトです。デフォルトでは、ルールはブリッジグループメンバーインターフェイスを除くすべてのインターフェイス ([Any]) に適用されます。

**ステップ5** ([変換 (Translation)] ページ上。) 元の packet アドレス (IPv4 または IPv6)、つまり、元の packet に表示される packet アドレスを特定します。

元の packet と変換済み packet の例については、次の図を参照してください。



- [Original Source][Address] : 変換するアドレスを含むネットワークオブジェクト、またはネットワークグループ。
- [Original Destination][Address] : (オプション)。宛先のアドレスを含むネットワークオブジェクト、またはネットワークグループ。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 を使用できます。

[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 packet アドレス (つまり、IPv4 または IPv6) を特定します。packet 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 (Translated Source)] : 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 (Translated Destination)] : (オプション)。変換された packet 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。

**ステップ 8** (オプション) [詳細 (Advanced)] で、必要なオプションを選択します。

- (送信元変換の場合のみ) [このルールに一致する DNS 応答を変換 (Translate DNS replies that match this rule)] : DNS 応答の IP アドレスを変換するかどうかを指定します。マッピングインターフェイスから実際のインターフェイスに移動する DNS 応答の場合、アドレス (IPv4 A または IPv6 AAAA) レコードはマッピングされた値から実際の値に書き換えられます。反対に、実際のインターフェイスからマッピング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 クエリと応答の書き換え \(123 ページ\)](#) 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 (Fallthrough to Interface PAT)] (宛先インターフェイス) : 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、ブリッジグループのメンバーではない宛先インターフェイスを選択した場合にのみ使用できます。インターフェイスの IPv6 アドレスを使用するには、[IPv6] オプションも選択します。
- [IPv6] : インターフェイス PAT に宛先インターフェイスの IPv6 アドレスを使用するかどうかを指定します。

**ステップ 9** [保存 (Save)] をクリックしてルールを追加します。

**ステップ 10** NAT ページで [保存 (Save)] をクリックして変更を保存します。

## 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。

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。

次の図は、ダイナミック PAT の一般的なシナリオを示します。実際のホストだけが 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 7: ダイナミック PAT



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

接続の有効期限が切れると、ポート変換も有効期限切れになります。



- (注) インターフェイスごとに異なる PAT プールを使用することをお勧めします。複数のインターフェイス、特に「any」インターフェイスに同じプールを使用すると、プールがすぐに枯渇し、新しい変換に使用できるポートがなくなります。

## 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、Threat Defense デバイスインターフェイスの IP アドレスを PAT アドレスとして使用できます。

同じブリッジグループ内のインターフェイス間で変換する場合は、IPv6 対応のダイナミック PAT (NAT66) は使用できません。この制限は、インターフェイスが異なるブリッジグループのメンバーである場合、またはブリッジグループのメンバーと標準的なルーテッドインターフェイスの間には該当しません。

ダイナミック PAT は、制御パスとは異なるデータストリームを持つ一部のマルチメディアアプリケーションでは機能しません。詳細については、[インスペクション対象プロトコルに対する NAT サポート \(15 ページ\)](#) 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ーで DoS 攻撃として解釈される可能性があります。アドレスの PAT プールを設定して、PAT アドレスのラウンドロビン割り当てを使用すると、この状況を緩和できます。

## PAT プール オブジェクトのガイドライン

PAT プールのネットワーク オブジェクトを作成する場合は、次のガイドラインに従ってください。

### PAT プールの場合

- ポートは、1024～65535の範囲の使用可能なポートにマッピングされます。必要に応じ、1024番未満の予約ポートを含めて、ポート範囲全体を変換に使用することもできます。  
クラスタで動作する場合、アドレスごとに512個のポートのブロックがクラスタのメンバーに割り当てられ、これらのポートブロック内でマッピングが行われます。ブロック割り当てでも有効にした場合は、ブロック割り当てサイズに従ってポートが分配されます。このデフォルトも512です。
- PATプールに対してブロック割り当てを有効にする場合、ポートブロックは1024～65535の範囲でのみ割り当てられます。そのため、アプリケーションが小さいポート番号（1～1023）を必要とするときは、機能しない可能性があります。たとえば、ポート22（SSH）を要求するアプリケーションは、1024～65535の範囲内で、ホストに割り当てられたブロック内の、マッピングされたポートを取得します。
- 同じPATプールオブジェクトを2つの異なるルールの中で使用する場合は、必ず同じオプションを各ルールに指定してください。たとえば、1つのルールで拡張PATが指定される場合は、もう一方のルールでも拡張PATが指定される必要があります。
- ホストに既存の接続がある場合は、そのホストからの以降の接続は同じPAT IPアドレスを使用します。使用可能なポートがない場合、接続が妨げられる可能性があります。この問題を回避するには、ラウンドロビンオプションを使用します。
- パフォーマンスを最大にするには、PATプール内のIPアドレスの数を10,000に制限します。

### PAT プールの拡張PATの場合

- 多くのアプリケーションインスペクションでは、拡張PATはサポートされていません。
- ダイナミックPATルールに対して拡張PATをイネーブルにする場合、PATプールのアドレスを、ポートトランスレーションルールを持つ別のスタティックNATのPATアドレスとしても使用することはできません。たとえば、PATプールに10.1.1.1が含まれている場合、PATアドレスとして10.1.1.1を使用する、ポートトランスレーションルールを持つスタティックNATは作成できません。
- PATプールを使用し、フォールバックのインターフェイスを指定する場合、拡張PATを使用できません。
- ICEまたはTURNを使用するVoIP配置では、拡張PATを使用しないでください。ICEおよびTURNは、すべての宛先に対して同じであるためにPATバインディングに依存しています。
- クラスタ内のユニットで拡張PATを使用することはできません。
- 拡張PATは、デバイスでのメモリ使用率が増加します。

### PAT プールのラウンドロビン方式の場合

- ホストに既存の接続がある場合は、そのホストからの以降の接続は同じ PAT IP アドレスを使用します（ポートが使用可能である場合）。ただし、この「粘着性」は、フェールオーバーが発生すると失われます。デバイスがフェールオーバーすると、ホストからの後続の接続では最初の IP アドレスが使用されない場合があります。
- PAT プールルール/ラウンドロビンルールとインターフェイス PAT ルールが同じインターフェイス上で混在していると、IP アドレスの「粘着性」も影響を受けます。指定したインターフェイスで PAT プールまたはインターフェイス PAT のいずれかを選択します。競合する PAT ルールは作成しないでください。
- ラウンドロビンでは、特に拡張 PAT と組み合わせた場合に、大量のメモリが消費されます。NAT プールはマッピングされるプロトコル/IP アドレス/ポート範囲ごとに作成されるため、ラウンドロビンでは数多くの同時 NAT プールが作成され、メモリが使用されます。拡張 PAT では、さらに多くの同時 NAT プールが作成されます。

## 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。1つのアドレス（宛先インターフェイスまたは他のアドレスのいずれか）に変換するか、またはたくさんの有効な変換を提供するために、アドレスの PAT プールを使用します。

### 始める前に

[オブジェクト (Objects)] > [オブジェクト管理 (Object Management)] 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。または、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す必要があります。

- [元の送信元 (Original Source)] : 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、範囲またはサブネットも可能です。
- [変換済み送信元 (Translated Source)] : 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。
  - [単一 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。
  - [PAT プール (PAT pool)] : 範囲を含むネットワーク オブジェクトを作成するか、またはホスト、範囲あるいはその両方を含むネットワーク オブジェクトグループを作成します。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** [デバイス (Devices) ] > [NAT] を選択し、Threat Defense NAT ポリシーを作成または編集します。

**ステップ 2** 次のいずれかを実行します。

- [ルール の追加 (Add Rule) ] ボタンをクリックして、新しいルールを作成します。
- [編集 (Edit) ] (✎) をクリックして、既存のルールを編集します。

メニューを右クリックすると、ルールの切り取り、コピー、貼り付け、挿入、および削除オプションが表示されます。

**ステップ 3** 基本ルールのオプションを設定します。

- [NAT ルール (NAT Rule) ] : [自動 NAT ルール (Auto NAT Rule) ] を選択します。
- [タイプ (Type) ] : [ダイナミック (Dynamic) ] を選択します。

**ステップ 4** [インターフェイスオブジェクト (Interface Objects) ] で、次のフィールドを設定します。

- [送信元インターフェイスオブジェクト (Source Interface Objects) ]、[宛先インターフェイスオブジェクト (Destination Interface Objects) ] : (ブリッジグループメンバーインターフェイスの場合に必要)。この NAT ルールを適用するインターフェイスを特定するインターフェイスオブジェクト (セキュリティゾーンまたはインターフェイスグループ)。  
[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を含んでいるオブジェクトです。[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を含んでいるオブジェクトです。デフォルトでは、ルールはブリッジグループメンバーインターフェイスを除くすべてのインターフェイス ([Any]) に適用されます。

**ステップ 5** 変換 (Translation) ] で、次のオプションを設定します。

- [元の送信元 (Original Source) ] : 変換するアドレスを含むネットワーク オブジェクト。
- [変換済み送信元 (Translated Source) ] : 以下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アドレスを使用するには、[宛先インターフェイス IP (Destination Interface IP) ] を選択します。また、特定の宛先インターフェイス オブジェクトを選択する必要があります。インターフェイスの IPv6 アドレスを使用するには、[詳細 (Advanced) ] で [IPv6] オプションを選択する必要があります。PAT プールの設定ステップを飛ばします。
  - 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。PAT プールの設定ステップを飛ばします。
  - PAT プールを使用するには、[変換済み送信元 (Translated Source) ] を空にしておきます。

**ステップ 6** PAT プールを使用している場合は、[PATプール (PAT Pool) ] ページを選択して、次の手順を実行します。

- a) [PATプールの有効化 (Enable PAT pool) ] を選択します。
- b) [PAT] > [アドレス (Address) ] フィールドで、プールのアドレスを保持するネットワークオブジェクトグループを選択します。

または、インターフェイス PAT を実装するための別の方法として、[宛先インターフェイス IP (Destination Interface IP) ] を選択できます。

- c) (任意) 必要に応じて、次のオプションを選択します。
  - [ラウンドロビン割り当てを使用 (Use Round Robin Allocation) ] : アドレスとポートをラウンドロビン形式で割り当てます。デフォルトではラウンドロビンは使用されず、1 つの PAT アドレスのポートがすべて割り当てられると次の PAT アドレスが使用されます。ラウンドロビン方式では、プール内の各 PAT アドレスから 1 つずつアドレス/ポートが割り当てられると最初のアドレスに戻り、次に 2 番目のアドレスというように順に使用されます。
  - [拡張 PAT テーブル (Extended PAT Table) ] : 拡張 PAT を使用します。拡張 PAT では、変換情報の宛先アドレスとポートを含め、IP アドレスごとではなく、サービスごとに 65535 個のポートが使用されます。通常、PAT 変換の作成時に宛先ポートとアドレスは考慮されないため、PAT アドレスあたり 65535 個のポートに制限されます。たとえば、拡張 PAT を使用して、192.168.1.7:23 に向かう場合の 10.1.1.1:1027 の変換、および 192.168.1.7:80 に向かう場合の 10.1.1.1:1027 の変換を作成できます。このオプションは、インターフェイス PAT またはインターフェイス PAT フォールバックで使用することはできません。
  - [フラットなポート範囲 (Flat Port Range) ]、[予約済みポートを含む (Include Reserved Ports) ] : TCP/UDP ポートを割り当てる際に、ポート範囲 (1024 ~ 65535) を単一のフラットな範囲として使用します。(6.7 より前) 変換のマッピングポート番号を選択すると、PAT は実際の送信元ポート番号を使用できます (使用可能な場合)。ただし、このオプションを設定しないと、実際のポートが使用できない場合、デフォルトでは、実際のポート番号と同じポート範囲 (1 ~ 511、512 ~ 1023、および 1024 ~ 65535) からマッピングポートが選択されます。下位の範囲でポートが不足するのを回避するには、この設定を行います。1 ~ 65535 の範囲全体を使用するには、[予約済みポートを含む (Include Reserved Ports) ] オプションも選択します。バージョン 6.7 以降を実行している Threat Defense デバイスの場合、オプションを選択するかどうかにかかわらず、フラットなポート範囲が常に設定されます。これらのシステムには、[予約済みポートを含む (Include Reserved Ports) ] オプションを選択しても、その設定が適用されます。
  - [ブロック割り当て (Block Allocation) ] : ポートのブロック割り当てを有効にする場合。キャリアグレードまたは大規模 PAT では、NAT に 1 度に 1 つのポート変換を割り当てさせるのではなく、各ホストにポートのブロックを割り当てることができます。ポートのブロックを割り当てる場合、ホストからの後続の接続はブロック内の新しい任意選択されたポートを使用します。必要に応じて、ホストが元のブロック内のすべてのポートに関してアクティブな接続を持つ場合は追加のブロックが割り当てられます。ポートブロックは、1024 ~ 65535 の範囲でのみ割り当てられます。ポートのブ

ロック割り当てはラウンドロビンと互換性がありますが、拡張 PAT またはフラットなポート範囲のオプションと一緒に使用することはできません。また、インターフェイス PAT フォールバックも使用できません。

**ステップ 7** (オプション) [詳細 (Advanced)] で、必要なオプションを選択します。

- [インターフェイス PAT へのフォールスルー (Fallthrough to Interface PAT)] (宛先インターフェイス) : 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、ブリッジグループのメンバーではない宛先インターフェイスを選択した場合にのみ使用できます。インターフェイスの IPv6 アドレスを使用するには、[IPv6] オプションも選択します。すでにインターフェイス PAT を変換済みアドレスとして設定している場合には、このオプションは使用できません。
- [IPv6] : インターフェイス PAT に宛先インターフェイスの IPv6 アドレスを使用するかどうかを指定します。

**ステップ 8** [保存 (Save)] をクリックしてルールを追加します。

**ステップ 9** NAT ページで [保存 (Save)] をクリックして変更を保存します。

## 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、宛先に応じて異なる変換をしたい場合などです。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。1つのアドレス (宛先インターフェイスまたは他のアドレスのいずれか) に変換するか、またはたくさんの有効な変換を提供するために、アドレスの PAT プールを使用します。

### 始める前に

[オブジェクト (Objects)] > [オブジェクト管理 (Object Management)] 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。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 ルールを定義しているときに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。

- [元の送信元 (Original Source)] : ネットワークオブジェクトまたはグループを指定できます。ホスト、範囲、またはサブネットを含めることができます。すべての元の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 (Translated Source)] : 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。

- [単一 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。
- [PAT プール (PAT pool)] : 範囲を含むネットワーク オブジェクトを作成するか、またはホスト、範囲あるいはその両方を含むネットワーク オブジェクト グループを作成します。サブネットを含めることはできません。

ルールで各アドレスの静的変換を設定すると、[元の宛先 (Original Destination)] および [変換済み宛先 (Translated Destination)] のネットワークオブジェクトまたはグループを作成できます。

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。

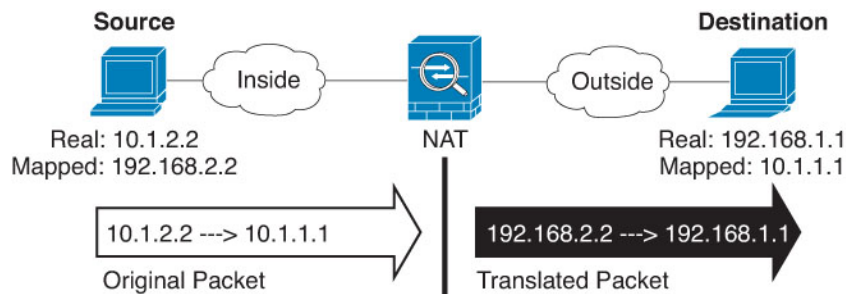
## 手順

- 
- ステップ 1** [デバイス (Devices)] > [NAT] を選択し、Threat Defense NAT ポリシーを作成または編集します。
- ステップ 2** 次のいずれかを実行します。
- [ルールの追加 (Add Rule)] ボタンをクリックして、新しいルールを作成します。
  - [編集 (Edit)] (✎) をクリックして、既存のルールを編集します。
- メニューを右クリックすると、ルールの切り取り、コピー、貼り付け、挿入、および削除オプションが表示されます。
- ステップ 3** 基本ルールのオプションを設定します。
- [NAT ルール (NAT Rule)] : [手動 NAT ルール (Manual NAT Rule)] を選択します。
  - [タイプ (Type)] : [ダイナミック (Dynamic)] を選択します。この設定は送信元アドレス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。
  - [有効化 (Enable)] : ルールをアクティブにするかどうかを指定します。ルールページの右クリックメニューを使用して、後でルールをアクティブ化または非アクティブ化することができます。
  - [挿入 (Insert)] : 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)、または指定するルール番号の上下に挿入できます。
- ステップ 4** [インターフェイスオブジェクト (Interface Objects)] で、次のフィールドを設定します。
- [送信元インターフェイスオブジェクト (Source Interface Objects)]、[宛先インターフェイスオブジェクト (Destination Interface Objects)] : (ブリッジグループメンバーインターフェイスの場合に必要)。この NAT ルールを適用するインターフェイスを特定するインターフェイスオブジェクト (セキュリティゾーンまたはインターフェイスグループ)。  
[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

を含んでいるオブジェクトです。[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を含んでいるオブジェクトです。デフォルトでは、ルールはブリッジグループメンバー インターフェイスを除くすべてのインターフェイス ([Any]) に適用されます。

**ステップ 5** ([変換 (Translation)] ページ上。) 元の packets アドレス (IPv4 または IPv6)、つまり、元の packets に表示される packets アドレスを特定します。

元の packets と変換済み packets の例については、次の図を参照してください。



- [Original Source][Address] : 変換するアドレスを含むネットワークオブジェクト、またはネットワークグループ。
- [Original Destination][Address] : (オプション)。宛先のアドレスを含むネットワークオブジェクト、またはネットワークグループ。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 を使用できます。

[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 packets アドレス (つまり、IPv4 または IPv6) を特定します。packets 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 (Translated Source)] : 以下のいずれかになります。
  - (インターフェイス PAT)。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)] > [宛先インターフェイス IP (Destination Interface IP)] を選択します。また、特定の宛先インターフェイスオブジェクトを選択する必要があります。インターフェイスの IPv6 アドレスを使用するには、[詳細 (Advanced)] で [IPv6] オプションを選択する必要があります。PAT プールの設定ステップを飛ばします。
  - 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。PAT プールの設定ステップを飛ばします。

- PAT プールを使用するには、[変換済み送信元 (Translated Source) ] を空にしておきます。

- [変換済み宛先 (Translated Destination) ]: (オプション)。変換されたパケットで 사용되는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。

**ステップ 8** PAT プールを使用している場合は、[PAT プール (PAT Pool) ] ページを選択して、次の手順を実行します。

- [PAT プールの有効化 (Enable PAT pool) ] を選択します。
- [PAT] > [アドレス (Address) ] フィールドで、プールのアドレスを保持するネットワーク オブジェクト グループを選択します。

または、インターフェイス PAT を実装するための別の方法として、[宛先インターフェイス IP (Destination Interface IP) ] を選択できます。

- (任意) 必要に応じて、次のオプションを選択します。
  - [ラウンドロビン割り当てを使用 (Use Round Robin Allocation) ]: アドレスとポートをラウンドロビン形式で割り当てます。デフォルトではラウンドロビンを使用されず、1 つの PAT アドレスのポートがすべて割り当てられると次の PAT アドレスが使用されます。ラウンドロビン方式では、プール内の各 PAT アドレスから 1 つずつアドレス/ポートが割り当てられると最初のアドレスに戻り、次に 2 番目のアドレスというように順に使用されます。
  - [拡張 PAT テーブル (Extended PAT Table) ]: 拡張 PAT を使用します。拡張 PAT では、変換情報の宛先アドレスとポートを含め、IP アドレスごとではなく、サービスごとに 65535 個のポートが使用されます。通常、PAT 変換の作成時に宛先ポートとアドレスは考慮されないため、PAT アドレスあたり 65535 個のポートに制限されます。たとえば、拡張 PAT を使用して、192.168.1.7:23 に向かう場合の 10.1.1.1:1027 の変換、および 192.168.1.7:80 に向かう場合の 10.1.1.1:1027 の変換を作成できます。このオプションは、インターフェイス PAT またはインターフェイス PAT フォールバックで使用することはできません。

- [フラットなポート範囲 (Flat Port Range) ]、[予約済みポートを含む (Include Reserved Ports) ]: TCP/UDP ポートを割り当てる際に、ポート範囲 (1024 ~ 65535) を単一のフラットな範囲として使用します。(6.7 より前) 変換のマッピングポート番号を選択すると、PAT は実際の送信元ポート番号を使用できます (使用可能な場合)。ただし、このオプションを設定しないと、実際のポートが使用できない場合、デフォルトでは、実際のポート番号と同じポート範囲 (1 ~ 511、512 ~ 1023、および 1024 ~ 65535) からマッピング ポートが選択されます。下位の範囲でポートが不足するのを回避するには、この設定を行います。1 ~ 65535 の範囲全体を使用するには、[予約済みポートを含む (Include Reserved Ports) ] オプションも選択します。バージョン 6.7 以降を実行している Threat Defense デバイスの場合、オプションを選択するかどうかにかかわらず、フラットなポート範囲が常に設定されます。これらのシステムには、**[予約済みポートを含む (Include Reserved Ports) ]** オプションを選択しても、その設定が適用されます。
- [ブロック割り当て (Block Allocation) ]: ポートのブロック割り当てを有効にする場合。キャリアグレードまたは大規模 PAT では、NAT に 1 度に 1 つのポート変換を割り当てさせるのではなく、各ホストにポートのブロックを割り当てることができます。ポートのブロックを割り当てる場合、ホストからの後続の接続はブロック内の新しい任意選択されたポートを使用します。必要に応じて、ホストが元のブロック内のすべてのポートに関してアクティブな接続を持つ場合は追加のブロックが割り当てられます。ポートブロックは、1024 ~ 65535 の範囲でのみ割り当てられます。ポートのブロック割り当てはラウンドロビンと互換性がありますが、拡張 PAT またはフラットなポート範囲のオプションと一緒に使用することはできません。また、インターフェイス PAT フォールバックも使用できません。

**ステップ 9** (オプション) [詳細 (Advanced) ] で、必要なオプションを選択します。

- [インターフェイス PAT へのフォールスルー (Fallthrough to Interface PAT) ] (宛先インターフェイス) : 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、ブリッジグループのメンバーではない宛先インターフェイスを選択した場合にのみ使用できます。インターフェイスの IPv6 アドレスを使用するには、[IPv6] オプションも選択します。
- [IPv6] : インターフェイス PAT に宛先インターフェイスの IPv6 アドレスを使用するかどうかを指定します。

**ステップ 10** [保存 (Save) ] をクリックしてルールを追加します。

**ステップ 11** NAT ページで [保存 (Save) ] をクリックして変更を保存します。

## ポート ブロック割り当てによる PAT の設定

キャリアグレードまたは大規模 PAT では、NAT に 1 度に 1 つのポート変換を割り当てさせるのではなく、各ホストにポートのブロックを割り当てることができます (RFC 6888 を参照してください)。ポートのブロックを割り当てると、ホストからのその後の接続では、ブロック内のランダムに選択される新しいポートが使用されます。必要に応じて、ホストが元のブロッ

ク内のすべてのポートに関してアクティブな接続を持つ場合は追加のブロックが割り当てられます。ブロックのポートを使用する最後の `xlate` が削除されると、ブロックが解放されます。

ポート ブロックを割り当てる主な理由は、ロギングの縮小です。ポート ブロックの割り当てが記録され、接続が記録されますが、ポートブロック内で作成された `xlate` は記録されません。一方、ログ分析はより困難になります。

ポートのブロックは 1024 ~ 65535 の範囲でのみ割り当てられます。そのため、アプリケーションが小さいポート番号 (1 ~ 1023) を必要とするときは、機能しない可能性があります。たとえば、ポート 22 (SSH) を要求するアプリケーションは、1024 ~ 65535 の範囲内で、ホストに割り当てられたブロック内の、マッピングされたポートを取得します。低いポート番号を使用するアプリケーションに対してブロック割り当てを使用しない個別の NAT ルールを作成できます。Twice NAT の場合は、ルールが確実にブロック割り当てルールの前に来るようにします。

### 始める前に

NAT ルールの使用上の注意：

- [ラウンドロビン割り当ての使用 (Use Round Robin Allocation) ] オプションは含めることができますが、PAT 一意性の拡張、フラットな範囲の使用、予約済みポートを含めること、またはインターフェイス PAT へのフォールスルーに関するオプションは含めることができません。その他の送信元/宛先のアドレスとポート情報も許可されます。
- 既存のルールを置き換える場合は、NAT を変更するすべてのケースと同様、置き換えるルールに関連する `xlate` をクリアする必要があります。これは、新しいルールを有効にするために必要です。それらを明示的にクリアするか、または単にタイムアウトになるまで待ちます。クラスタでの動作の場合、クラスタ全体で `xlate` をグローバルにクリアする必要があります。



(注) 通常の PAT ルールとブロック割り当て PAT ルールを切り替える場合、オブジェクト NAT では、まずルールを削除してから `xlate` をクリアする必要があります。その後、新しいオブジェクト NAT ルールを作成できます。そうしないと、`show asp drop` 出力に `pat-port-block-state-mismatch` ドロップが表示されます。

- 特定の PAT プールに対し、そのプールを使用するすべてのルールに対してブロック割り当てを指定する (または指定しない) 必要があります。1 つのルールにブロックを割り当てることはできず、別のルールに割り当てることもできません。重複する PAT プールもまたブロック割り当て設定を混在させることはできません。また、ポート変換ルールを含むスタティック NAT とプールを重複させることはできません。

### 手順

**ステップ 1** (オプション) グローバル PAT ポート ブロック割り当ての設定を行います。



ポートブロック割り当てを制御するグローバル設定がいくつかあります。これらのオプションのデフォルトを変更する場合は、FlexConfig オブジェクトを設定し、それを FlexConfig ポリシーに追加する必要があります。

- a) [オブジェクト (Objects) ]>[オブジェクト管理 (Object Management) ]>[FlexConfig] > [FlexConfig オブジェクト (FlexConfig Object) ] を選択します。

- b) ブロック割り当てサイズを設定します。これは各ブロックのポート数です。

**xlate block-allocation size value**

範囲は 32 ~ 4096 です。デフォルトは 512 です。デフォルト値に戻すには、no 形式を使用します。

デフォルトを使用しない場合は、選択したサイズが 64,512 に均等に分割していることを確認します (1024 ~ 65535 の範囲のポート数)。確認を怠ると、使用できないポートが混入します。たとえば、100 を指定すると、12 個の未使用ポートがあります。

- c) ホストごとに割り当てることができる最大ブロック数を設定します。

**xlate block-allocation maximum-per-host number**

制限はプロトコルごとに設定されるので、制限「4」は、ホストごとの上限が 4 つの UDP ブロック、4 つの TCP ブロック、および 4 つの ICMP ブロックであることを意味します。指定できる値の範囲は 1 ~ 8 で、デフォルトは 4 です。デフォルト値に戻すには、no 形式を使用します。

- d) (オプション) 暫定 syslog の生成をイネーブルにします。

**xlate block-allocation pba-interim-logging seconds**

デフォルトでは、ポートブロックの作成および削除中にシステムで syslog メッセージが生成されます。暫定ロギングをイネーブルにすると、指定した間隔で次のメッセージが生成されます。メッセージは、その時点で割り当てられているすべてのアクティブ ポート ブロックをレポートします (プロトコル (ICMP、TCP、UDP)、送信元および宛先インターフェイス、IP アドレス、ポートブロックを含む)。間隔は 21600 ~ 604800 秒 (6 時間から 7 日間) を指定することができます。

%ASA-6-305017: Pba-interim-logging: Active protocol block of ports for translation from real\_interface:real\_host\_ip to mapped\_interface:mapped\_ip\_address/start\_port\_num-end\_port\_num

例 :

次に、ブロック割り当てサイズを 64 (ホストごとの最大サイズは 8) に設定し、暫定ロギングを 6 時間おきに有効にする例を示します。

```
xlate block-allocation size 64
xlate block-allocation maximum-per-host 8
xlate block-allocation pba-interim-logging 21600
```

- e) FlexConfig オブジェクトで、次のオプションを選択します。

- [展開 (Deployment) ]=[毎回 (Everytime) ]
- [タイプ (Type) ]=[後ろに付加 (Append) ]

- f) [保存 (保存)] をクリックして FlexConfig オブジェクトを作成します。
- g) [デバイス (Devices)] > [FlexConfig] を選択し、これらの設定を調整する必要があるデバイスに割り当てられている FlexConfig ポリシーを作成または編集します。
- h) 使用可能なオブジェクトリスト内のオブジェクトを選択し、> をクリックしてそのオブジェクトを選択したオブジェクトリストに移動します。
- i) [保存 (Save)] をクリックします。  
[設定のプレビュー (Preview Config)] をクリックしてターゲット デバイスのいずれかを選択し、xlate コマンドが正しく表示されていることを確認します。

**ステップ 2** PAT プール ポートのブロック割り当てを使用する NAT ルールを追加します。

- a) [デバイス (Devices)] > [NAT] を選択し、Threat Defense の NAT ポリシーを追加または編集します。
- b) NAT ルールを追加または編集し、少なくとも次のオプションを設定します。
  - [タイプ (Type)] = [ダイナミック (Dynamic)]
  - [変換 (Translation)] > [元の送信元 (Original Source)] で、送信元アドレスを定義するオブジェクトを選択します。
  - [PAT プール (PAT Pool)] で、次のオプションを設定します。
    - [PAT プールの有効化 (Enable PAT Pool)] を選択します。
    - [PAT] > [アドレス (Address)] で、PAT プールを定義するネットワークオブジェクトを選択します。
    - [ブロック割り当て (Block Allocation)] オプションを選択します。
- c) ルールと NAT ポリシーに変更を保存します。

## スタティック NAT

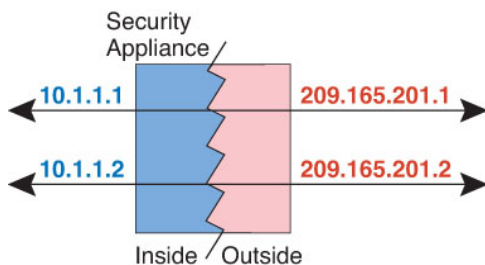
ここでは、スタティック NAT とその実装方法について説明します。

### 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 8:スタティック NAT



(注) 必要に応じて、双方向を無効化できます。

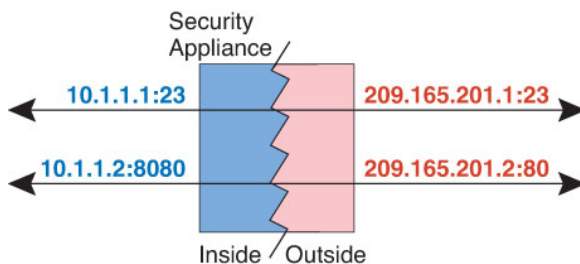
### ポート変換を設定したスタティック NAT

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 9:ポート変換を設定したスタティック NAT の一般的なシナリオ



ポート変換ルールを設定したスタティック NAT は、指定されたポートの宛先 IP アドレスのみにアクセスを制限します。NAT ルール対象外の別のポートで宛先 IP アドレスにアクセスしようとすると、接続がブロックされます。さらに、手動 NAT の場合、NAT ルールの送信元 IP アドレスと一致しないトラフィックが宛先 IP アドレスと一致する場合、宛先ポートに関係なくドロップされます。したがって、宛先 IP アドレスに対して許可される他のすべてのトラフィックに追加ルールを追加する必要があります。たとえば、ポートを指定せずに IP アドレスにスタティック NAT ルールを設定し、ポート変換ルールの後ろにそれを配置できます。



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

次に、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できます。サーバは標準のポート (それぞれ 21、80、および 25) を使用しているため、ポートを変更する必要はありません。

#### 標準以外のポートのポート変換を設定したスタティック NAT

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

#### ポート変換を設定したスタティック インターフェイス NAT

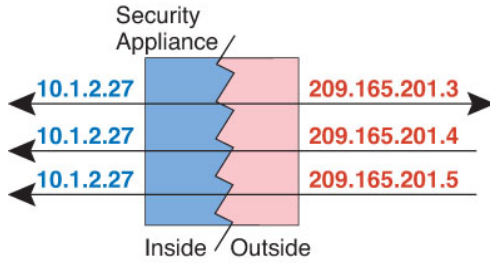
スタティック NAT は、実際のアドレスをインターフェイス アドレスとポートの組み合わせにマッピングするように設定できます。たとえば、デバイスの外部インターフェイスへの Telnet アクセスを内部ホストにリダイレクトする場合、内部ホストの IP アドレス/ポート 23 を外部インターフェイス アドレス/ポート 23 にマッピングできます。

## 1 対多のスタティック NAT

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

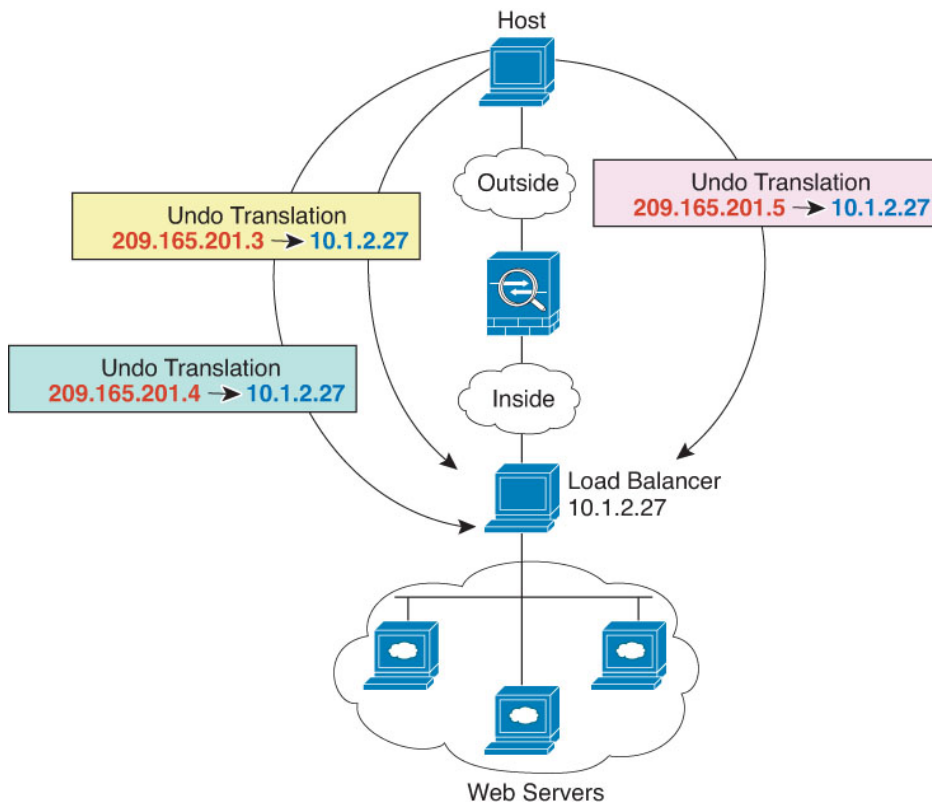
次の図に、一般的な 1 対多のスタティック NAT シナリオを示します。実際のホストが開始すると、常に最初のマッピング アドレスが使用されるため、実際のホスト IP/最初のマッピング IP の変換は、理論的には双方向変換のみが行われます。

図 10: 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 11: 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 12: 少対多のスタティック NAT



多対少または多対1コンフィギュレーションでは、マッピングアドレスよりも多くの実際のアドレスが存在します。実際のアドレスが不足するよりも前に、マッピングアドレスが不足します。双方向の開始を実現できるのは、最下位の実際のIPアドレスとマッピング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 13: 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。

### 始める前に

[オブジェクト (Objects)] > [オブジェクト管理 (Object Management)] 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。または、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す必要があります。

- [元の送信元 (Original Source)] : 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、範囲またはサブネットも可能です。
- [変換済み送信元 (Translated Source)] : 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 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。
  - [アドレス (Address)] : ホスト、範囲、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** [デバイス (Devices)] > [NAT] を選択し、Threat Defense NAT ポリシーを作成または編集します。

**ステップ 2** 次のいずれかを実行します。

- [ルールの追加 (Add Rule)] ボタンをクリックして、新しいルールを作成します。
- [編集 (Edit)] (✎) をクリックして、既存のルールを編集します。

メニューを右クリックすると、ルールの切り取り、コピー、貼り付け、挿入、および削除オプションが表示されます。

**ステップ 3** 基本ルールのオプションを設定します。

- [NAT ルール (NAT Rule) ] : [自動 NAT ルール (Auto NAT Rule) ] 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** [インターフェイスオブジェクト (Interface Objects) ] で、次のフィールドを設定します。

- [送信元インターフェイスオブジェクト (Source Interface Objects) ]、[宛先インターフェイスオブジェクト (Destination Interface Objects) ] : (ブリッジグループメンバーインターフェイスの場合に必要)。この NAT ルールを適用するインターフェイスを特定するインターフェイスオブジェクト (セキュリティゾーンまたはインターフェイスグループ)。  
[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を含んでいるオブジェクトです。[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を含んでいるオブジェクトです。デフォルトでは、ルールはブリッジグループメンバーインターフェイスを除くすべてのインターフェイス ([Any]) に適用されます。

**ステップ 5** [変換 (Translation) ] で、次のオプションを設定します。

- [元の送信元 (Original Source) ] : 変換するアドレスを含むネットワークオブジェクト。
- [変換済み送信元 (Translated Source) ] : 以下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、[アドレス (Address) ] および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) 宛先インターフェイスのアドレスを使用するには、[宛先インターフェイス IP (Destination Interface IP) ] を選択します。また、特定の宛先インターフェイスオブジェクトを選択する必要があります。インターフェイスの IPv6 アドレスを使用するには、[詳細 (Advanced) ] で [IPv6] オプション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。
- (オプション) [元のポート (Original Port) ]、[変換済みポート (Translated Port) ] : TCP または UDP ポートを変換する必要がある場合は、[元のポート (Original Port) ] でプロトコルを選択し、元のポート番号と変換済みポート番号を入力します。たとえば、必要に応じて TCP/80 を 8080 に変換できます。

**ステップ 6** (オプション) [詳細 (Advanced) ] で、必要なオプションを選択します。

- [このルールに一致する DNS 応答を変換 (Translate DNS replies that match this rule) ] : DNS 応答の IP アドレスを変換するかどうかを指定します。マッピングインターフェイスから実際のインターフェイスに移動する DNS 応答の場合、アドレス (IPv4 A または IPv6 AAAA) レコードはマッピングされた値から実際の値に書き換えられます。反対に、実際のインターフェイスからマッピング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 クエリと応](#)



答の書き換え (123 ページ) を参照してください。このオプションはポート変換を行う場合は使用できません。

- [IPv6] : インターフェイス PAT に宛先インターフェイスの IPv6 アドレスを使用するかどうかを指定します。
- [ネット間マッピング (Net to Net Mapping) ] : NAT 46 の場合、このオプションを選択して、最初の IPv4 アドレスを最初の IPv6 アドレスに変換し、2 番目を 2 番目に変換という順序で変換します。このオプションを選択しない場合、IPv4 埋め込み方式が使用されません。1 対 1 変換の場合は、このオプションを使用する必要があります。
- [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 が不要で、場合によっては接続性に関する問題を引き起こす可能性があります。

ステップ 7 [保存 (Save) ] をクリックしてルールを追加します。

ステップ 8 NAT ページで [保存 (Save) ] をクリックして変更を保存します。

## 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。

### 始める前に

[オブジェクト (Objects) ] > [オブジェクト管理 (Object Management) ] 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。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 ルールを定義しているときに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。

- [元の送信元 (Original Source) ] : 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せん。ホスト、範囲、またはサブネットを含めることができます。すべての元の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 (Translated Source) ] : 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。

- [アドレス (Address) ]: ホスト、範囲、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。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静的変換を設定すると、[元の宛先 (Original Destination) ] および [変換済み宛先 (Translated Destination) ] のネットワークオブジェクトまたはグループを作成できます。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** [デバイス (Devices) ] > [NAT] を選択し、Threat Defense NAT ポリシーを作成または編集します。

**ステップ 2** 次のいずれかを実行します。

- [ルール の追加 (Add Rule) ] ボタンをクリックして、新しいルールを作成します。
- [編集 (Edit) ] (✎) をクリックして、既存のルールを編集します。

メニューを右クリックすると、ルールの切り取り、コピー、貼り付け、挿入、および削除オプションが表示されます。

**ステップ 3** 基本ルールのオプションを設定します。

- [NAT ルール (NAT Rule) ]: [手動 NAT ルール (Manual NAT Rule) ] を選択します。
- [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している場合、変換は常に静的に行われます。
- [有効化 (Enable) ]: ルールをアクティブにするかどうかを指定します。ルールページの右クリックメニューを使用して、後でルールをアクティブ化または非アクティブ化することができます。
- [挿入 (Insert) ]: 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) 、または指定するルール番号の上下に挿入できます。

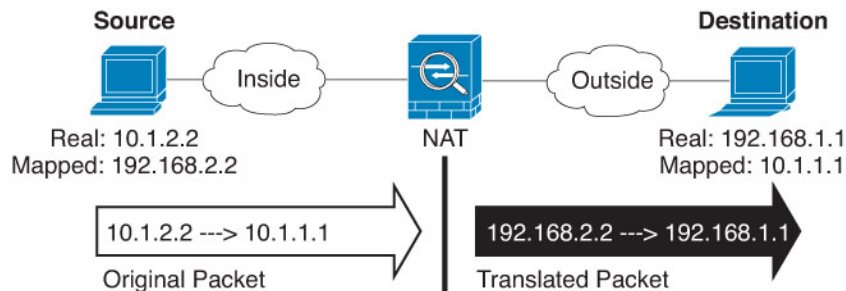
**ステップ 4** [インターフェイスオブジェクト (Interface Objects) ] で、次のフィールドを設定します。

- [送信元インターフェイスオブジェクト (Source Interface Objects) ]、[宛先インターフェイスオブジェクト (Destination Interface Objects) ]: (ブリッジグループメンバーインターフェイスの場合に必要)。この NAT ルールを適用するインターフェイスを特定するインターフェイスオブジェクト (セキュリティゾーンまたはインターフェイスグループ) 。

[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を含んでいるオブジェクトです。[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を含んでいるオブジェクトです。デフォルトでは、ルールはブリッジグループメンバー インターフェイスを除くすべてのインターフェイス ([Any]) に適用されます。

**ステップ 5** ([変換 (Translation)] ページ上。) 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。



- [Original Source][Address] : 変換するアドレスを含むネットワークオブジェクト、またはネットワークグループ。
- [Original Destination][Address] : (オプション)。宛先のアドレスを含むネットワークオブジェクト、またはネットワークグループ。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 を使用できます。

[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 (Translated Source)] : 以下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、[アドレス (Address)] および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、実際アドレスと同じ数のマッピングアドレスを設定します。しかし、アドレスの数が一致しない場合もあります。
  - (ポート変換を設定したスタティック インターフェイス NAT) 宛先インターフェイスのアドレスを使用するには、[宛先インターフェイス IP (Destination Interface IP)] を選択します。また、特定の宛先インターフェイスオブジェクトを選択する必要があります。インターフェイスの IPv6 アドレスを使用するには、[詳細 (Advanced)] で

[IPv6] オプション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。

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

**ステップ 8** (オプション) [詳細 (Advanced) ] で、必要なオプションを選択します。

- [このルールに一致する DNS 応答を変換 (Translate DNS replies that match this rule) ]: DNS 応答の IP アドレスを変換するかどうかを指定します。マッピングインターフェイスから実際のインターフェイスに移動する DNS 応答の場合、アドレス (IPv4 A または IPv6 AAAA) レコードはマッピングされた値から実際の値に書き換えられます。反対に、実際のインターフェイスからマッピング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 クエリと応答の書き換え \(123 ページ\)](#) を参照してください。このオプションはポート変換を行う場合は使用できません。
- [IPv6]: インターフェイス PAT に宛先インターフェイスの IPv6 アドレスを使用するかどうかを指定します。
- [ネット間マッピング (Net to Net Mapping) ]: NAT 46 の場合、このオプションを選択して、最初の IPv4 アドレスを最初の IPv6 アドレスに変換し、2 番目を 2 番目に変換という順序で変換します。このオプションを選択しない場合、IPv4 埋め込み方式が使用されます。1 対 1 変換の場合は、このオプションを使用する必要があります。
- [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 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。

- [単一方向 (Unidirectional) ]: このオプションを選択すると、宛先アドレスが発信元アドレスにトラフィックを開始しないようにできます。単方向オプションは主にテスト目的に有効であり、すべてのプロトコルで機能するとは限りません。たとえば、SIP では、NAT を使用して SIP ヘッダーを変換するためにプロトコルインスペクションが必要ですが、変換を単方向にするとこの処理は行われません。

**ステップ 9** [保存 (Save) ]をクリックしてルールを追加します。

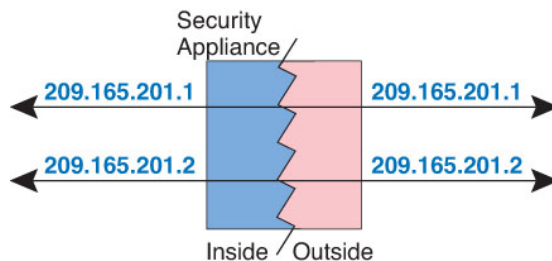
**ステップ 10** NAT ページで [保存 (Save) ]をクリックして変更を保存します。

## アイデンティティ NAT

IP アドレスを自身に変換する必要がある 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 14: 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。

始める前に

[オブジェクト (Objects) ] > [オブジェクト管理 (Object Management) ] を選択して、ルールで必要なネットワーク オブジェクトまたはグループを作成します。または、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す必要があります。

- [元の送信元 (Original Source)] : 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、範囲、またはサブネットも可能です。
- [変換済み送信元 (Translated Source)] : 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** [デバイス (Devices)] > [NAT] を選択し、Threat Defense NAT ポリシーを作成または編集します。

**ステップ 2** 次のいずれかを実行します。

- [ルール の追加 (Add Rule)] ボタンをクリックして、新しいルールを作成します。
- [編集 (Edit)] (✎) をクリックして、既存のルールを編集します。

メニューを右クリックすると、ルールの切り取り、コピー、貼り付け、挿入、および削除オプションが表示されます。

**ステップ 3** 基本ルールのオプションを設定します。

- [NAT ルール (NAT Rule)] : [自動 NAT ルール (Auto NAT Rule)] 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** [インターフェイスオブジェクト (Interface Objects)] で、次のフィールドを設定します。

- [送信元インターフェイスオブジェクト (Source Interface Objects)]、[宛先インターフェイスオブジェクト (Destination Interface Objects)] : (ブリッジグループメンバーインターフェイスの場合に必要)。この NAT ルールを適用するインターフェイスを特定するインターフェイス オブジェクト (セキュリティゾーンまたはインターフェイスグループ)。  
[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を含んでいるオブジェクトです。[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を含んでいるオブジェクトです。デフォルトでは、ルールはブリッジグループメンバー インターフェイスを除くすべてのインターフェイス ([Any]) に適用されます。

**ステップ 5** [変換 (Translation)] で、次のオプションを設定します。

- [元の送信元 (Original Source)] : 変換するアドレスを含むネットワーク オブジェクト。
- [変換済み送信元 (Translated Source)] : 元の送信元と同じオブジェクト。状況に応じて、コンテンツがまった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 6** (オプション) [詳細 (Advanced)] で、必要なオプションを選択します。

- [このルールと一致する DNS 応答を変換 (Translate DNS replies that match this rule) ] : アイデンティティ NAT には、このオプションを設定しないでください。
- [IPv6] : アイデンティティ NAT にこのオプションを設定しないでください。
- [ネット マッピングへのネット (Net to Net Mapping) ] : アイデンティティ NAT にこのオプションを設定しないでください。
- [宛先インターフェイスで ARP をプロキシしない (Do not proxy ARP on Destination Interface) ] : マッピング IP アドレスへの着信パケットのプロキシ ARP を無効にします。マッピングインターフェイスと同じネットワーク上のアドレスを使用した場合、システムはプロキシ ARP を使用してマッピングアドレスのすべての ARP 要求に回答することで、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 が不要で、場合によっては接続性に関する問題を引き起こす可能性があります。
- [宛先インターフェイスのルートルックアップの実行 (Perform Route Lookup for Destination Interface) ] : 元の送信元アドレス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て、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 7** [保存 (Save) ] をクリックしてルールを追加します。

**ステップ 8** NAT ページで [保存 (Save) ] をクリックして変更を保存します。

## 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、宛先に応じて異なる変換をしたい場合などです。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。

### 始める前に

[オブジェクト (Objects) ] > [オブジェクト管理 (Object Management) ] 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。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 ルールを定義しているときに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。

- [元の送信元 (Original Source) ] : 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、範囲、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 (Translated Source)] : 元の送信元と同じオブジェクトまたはグループ。状況に応じて、コンテンツがまったく同一の別のオブジェクトを選択できます。

ルールで各アドレスの静的変換を設定すると、[元の宛先 (Original Destination)] および [変換済み宛先 (Translated Destination)] のネットワークオブジェクトまたはグループを作成できます。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。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** [デバイス (Devices)] > [NAT] を選択し、Threat Defense NAT ポリシーを作成または編集します。

**ステップ 2** 次のいずれかを実行します。

- [ルールの追加 (Add Rule)] ボタンをクリックして、新しいルールを作成します。
- [編集 (Edit)] (✎) をクリックして、既存のルールを編集します。

メニューを右クリックすると、ルールの切り取り、コピー、貼り付け、挿入、および削除オプションが表示されます。

**ステップ 3** 基本ルールのオプションを設定します。

- [NAT ルール (NAT Rule)] : [手動 NAT ルール (Manual NAT Rule)] を選択します。
- [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している場合、変換は常に静的に行われます。
- [有効化 (Enable)] : ルールをアクティブにするかどうかを指定します。ルールページの右クリックメニューを使用して、後でルールをアクティブ化または非アクティブ化することができます。
- [挿入 (Insert)] : 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)、または指定するルール番号の上下に挿入できます。

**ステップ 4** [インターフェイスオブジェクト (Interface Objects)] で、次のフィールドを設定します。

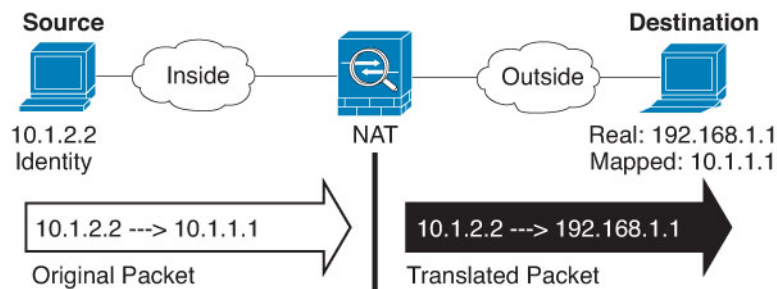
- [送信元インターフェイスオブジェクト (Source Interface Objects)]、[宛先インターフェイスオブジェクト (Destination Interface Objects)] : (ブリッジグループメンバーインターフェイスの場合に必要)。この NAT ルールを適用するインターフェイスを特定するインターフェイスオブジェクト (セキュリティゾーンまたはインターフェイスグループ)。  
[送信元 (Source)] は、デバイスに入るトラフィックが通過する実際のインターフェイスを含んでいるオブジェクトです。[宛先 (Destination)] は、デバイスから出るトラフィックが通過するマッピングインターフェイスを含んでいるオブジェクトです。デフォルトで



は、ルールはブリッジグループメンバー インターフェイスを除くすべてのインターフェイス ([Any]) に適用されます。

**ステップ 5** 元の packets アドレス (IPv4 または IPv6) 、つまり、元の packets に表示される packets アドレスを特定します。

元の packets と変換済み packets 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 (Original Source) ]: 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 (Original Destination) ]: (オプション)。宛先のアドレスを含むネットワーク オブジェクト、またはネットワークグループ。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 を使用できます。

[インターフェイス オブジェクト (Interface Object) ] を選択し、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 packets アドレス (つまり、IPv4 または IPv6) を特定します。 packets 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 (Translated Source) ]: 元の送信元と同じオブジェクトまたはグループ。状況に応じて、コンテンツがまった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 (Translated Destination) ]: (オプション)。変換された packets 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) ]、[変換済み送信元ポート (Translated Source Port) ] : 送信元アドレスのポート変換を定義します。
- [元の宛先ポート (Original Destination Port) ]、[変換済み宛先ポート (Translated Destination Port) ] : 宛先アドレスのポート変換を定義します。

**ステップ 8** (オプション) [詳細 (Advanced) ] で、必要なオプションを選択します。

- [このルールと一致する DNS 応答を変換 (Translate DNS replies that match this rule) ] : アイデンティティ NAT には、このオプションを設定しないでください。
- [IPv6] : インターフェイス PAT に宛先インターフェイスの IPv6 アドレスを使用するかどうかを指定します。
- [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 が不要で、場合によっては接続性に関する問題を引き起こす可能性があります。
- [宛先インターフェイスのルートルックアップの実行 (Perform Route Lookup for Destination Interface) ] : 元の送信元アドレス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て、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。
- [単一方向 (Unidirectional) ] : このオプションを選択すると、宛先アドレスが発信元アドレスにトラフィックを開始しないようにできます。単方向オプションは主にテスト目的に有効であり、すべてのプロトコルで機能するとは限りません。たとえば、SIP では、NAT を使用して SIP ヘッダーを変換するためにプロトコルインスペクションが必要ですが、変換を単方向にするとこの処理は行われません。

**ステップ 9** [保存 (Save) ] をクリックしてルールを追加します。

**ステップ 10** NAT ページで [保存 (Save) ] をクリックして変更を保存します。

## Threat Defense の NAT ルールのプロパティ

ネットワークアドレス変換 (NAT) ルールを使用して、IP アドレスを他の IP アドレスに変換します。通常は、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つのアドレスを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つまたは少数のアドレスに変換し、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。

### NAT タイプ (NAT Type)

[手動 NAT ルール (Manual NAT Rule)] または [自動 NAT ルール (Auto NAT Rule)] のどちらを設定するのかを指定します。自動 NAT は、送信元アドレスのみを変換します。宛先アドレスに基づいた他の変換方法作成することはできません。自動 NAT のほうが設定するのが簡単なので、手動 NAT の機能を追加する必要がない限り、自動 NAT を使用してください。この2つの間の違いについては、[自動 NAT および手動 NAT \(6 ページ\)](#) を参照してください。

### [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)] にするかを指定します。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。

### 有効化 (Enable) (手動 NAT のみ)

ルールをアクティブにするかどうかを指定します。ルールページの右クリックメニューを使用して、後でルールをアクティブ化または非アクティブ化することができます。自動 NAT ルールを無効化することはできません。

### 挿入 (Insert) (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)、または指定するルール番号の上下に挿入できます。

### 説明 (任意、手動 NAT のみ)。

ルールの目的の説明。

以降のトピックで、NAT ルールプロパティのタブについて説明します。

## インターフェイスオブジェクト : NAT のプロパティ

インターフェイスオブジェクト (セキュリティゾーンまたはインターフェイスグループ) は、NAT ルールが適用されるインターフェイスを定義します。ルーテッドモードでは、送信元と宛先の両方にデフォルトの「任意 (Any)」を使用すれば、割り当てられたすべてのデバイスのすべてのインターフェイスに適用できます。ただし、通常は特定の送信元と宛先インターフェイスを選択します。

## 注記

- 「任意」のインターフェイスの概念は、ブリッジグループメンバーインターフェイスには適用されません。「任意」のインターフェイスを指定すると、すべてのブリッジグループメンバーインターフェイスが除外されます。そのため、ブリッジグループメンバーに NAT を適用するには、メンバーインターフェイスを指定する必要があります。ブリッジ仮想インターフェイス (BVI) 自体に NAT を設定することはできず、メンバーインターフェイスにのみ NAT を設定できます。

インターフェイス オブジェクトを選択すると、NAT ルールはデバイスのインターフェイスが選択されたすべてのオブジェクトに含まれているときにのみ設定されます。たとえば、送信元と宛先の両方のセキュリティゾーンを選択すると、特定のデバイスに対して 1 つ以上のインターフェイスが両方のゾーンに含まれている必要があります。

- 特定のデバイスにインターフェイスオブジェクト内の複数のインターフェイスが存在する場合は、インターフェイスごとに同一のルールが作成されます。これは、宛先変換を含む静的 NAT ルールで問題になる可能性があります。NAT ルールは最初に一致したルールに基づいて適用されるため、オブジェクトに設定された最初のインターフェイス用に作成されたルールのみがトラフィックと一致します。宛先変換を使用して静的 NAT を設定する場合は、NAT ポリシーに割り当てられたデバイスごとに最大 1 つのインターフェイスを含むインターフェイス オブジェクトを使用して、目的の結果が得られるようにします。

## 送信元インターフェイス オブジェクト、宛先インターフェイス オブジェクト

(ブリッジグループメンバーインターフェイスの場合に必要)。この NAT ルールを適用するインターフェイスを特定するインターフェイスオブジェクト (セキュリティゾーンまたはインターフェイスグループ)。**[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を含んでいるオブジェクトです。**[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を含んでいるオブジェクトです。デフォルトでは、ルールはブリッジグループメンバーインターフェイスを除くすべてのインターフェイス (**[Any]**) に適用されます。

## 自動 NAT の変換プロパティ

**[変換 (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。

**[元の送信元 (Original Source)]** (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。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ます、ホスト、範囲、またはサブネットを含めることができます。

システム定義の **any-ipv4** または **any-ipv6** オブジェクトには自動 NAT ルールを作成できません。

**[変換済み送信元 (Translated Source)]** (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できますが、サブネットを含むことはできません。グループに IPv4 アドレスと IPv6 アドレスの両方を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。グループに範囲とホスト IP アドレスの両方が含まれている場合、範囲はダイナミック NAT に使用され、ホスト IP アドレスは PAT のフォールバックとして使用されます。
- [ダイナミック PAT (Dynamic PAT) ] : 次のいずれかを実行します。
  - (インターフェイス PAT) 宛先インターフェイスのアドレスを使用するには、[宛先インターフェイス IP (Destination Interface IP) ] を選択します。また、特定の宛先インターフェイス オブジェクトを選択する必要があります。インターフェイスの IPv6 アドレスを使用するには、[詳細 (Advanced) ] で [IPv6] オプションを選択する必要があります。PAT プールは設定しないでください。
  - 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。PAT プールは設定しないでください。
  - PAT プールを使用するには、[変換された送信元 (Translated Source) ] を空のままにしておきます。[PAT プール (PAT Pool) ] で PAT プール オブジェクトを選択します。
- [スタティック NAT (Static NAT) ] : 次のいずれかを実行します。
  - アドレスの設定グループを使用するには、[アドレス (Address) ] およびマッピングされたアドレスを含むネットワーク オブジェクトまたはグループを選択します。オブジェクトまたはグループに、ホスト、範囲、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アドレスを使用するには、[宛先インターフェイス IP (Destination Interface IP) ] を選択します。また、特定の宛先インターフェイス オブジェクトを選択する必要があります。インターフェイスの IPv6 アドレスを使用するには、[詳細 (Advanced) ] タブで [IPv6] オプション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。
- [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。状況に応じて、コンテンツがまったく同一の別のオブジェクトを選択できます。

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

TCP または UDP ポートを変換する必要がある場合、[元のポート (Original Port) ] でプロトコルを選択し、元のポートおよび変換済みポートの番号を入力します。たとえば、必要

に応じて TCP/80 を 8080 に変換できます。アイデンティティ NAT にこれらのオプションを設定しないでください。

## 手動 NAT の変換プロパティ

[変換 (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。

[元の送信元 (Original Source) ] (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、範囲、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 (Translated Source) ] (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できますが、サブネットを含むことはできません。グループに IPv4 アドレスと IPv6 アドレスの両方を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。グループに範囲とホスト IP アドレスの両方が含まれている場合、範囲はダイナミック NAT に使用され、ホスト IP アドレスは PAT のフォールバックとして使用されます。
- [ダイナミック PAT (Dynamic PAT) ]: 次のいずれかを実行します。
  - (インターフェイス PAT) 宛先インターフェイスのアドレスを使用するには、[宛先インターフェイス IP (Destination Interface IP) ] を選択します。また、特定の宛先インターフェイス オブジェクトを選択する必要があります。インターフェイスの IPv6 アドレスを使用するには、[詳細 (Advanced) ] で [IPv6] オプションを選択する必要があります。PAT プールは設定しないでください。
  - 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。PAT プールは設定しないでください。
  - PAT プールを使用するには、[変換された送信元 (Translated Source) ] を空のままにしておきます。[PAT プール (PAT Pool) ] で PAT プール オブジェクトを選択します。
- [スタティック NAT (Static NAT) ]: 次のいずれかを実行します。
  - アドレスの設定グループを使用するには、[アドレス (Address) ] およびマッピングされたアドレスを含むネットワーク オブジェクトまたはグループを選択します。オブジェクトまたはグループに、ホスト、範囲、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アドレスを使用するには、[宛先インターフェイス IP (Destination Interface IP)] を選択します。また、特定の宛先インターフェイス オブジェクトを選択する必要があります。インターフェイスの IPv6 アドレスを使用するには、[詳細 (Advanced)] タブで [IPv6] オプション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。

- [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。状況に応じて、コンテンツがまったく同一の別のオブジェクトを選択できます。

#### [元の宛先 (Original Destination)]

宛先のアドレスを含むネットワークオブジェクト、またはネットワークグループ。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 を使用できます。

[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。

#### [変換済みの宛先 (Translated Destination)]

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。

変換後の宛先として完全修飾ドメイン名を指定するネットワークオブジェクトを使用できます。詳細については、[FQDN 宛先のガイドライン \(18 ページ\)](#) を参照してください。

#### [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。

## PAT プールの NAT プロパティ

ダイナミック NAT を設定する際に、[PAT プール (PAT Pool)] タブのプロパティを使用して、ポート アドレス変換に使用するアドレスのプールを定義できます。

### PAT プールの有効化 (Enable PAT Pool)

PAT に使用するアドレスのプールを設定する場合は、このオプションを選択します。

### PAT

PAT プールに使用するアドレスとして、以下のいずれかを指定します。

- [アドレス (Address)] : PAT プールアドレスを定義するオブジェクト。アドレスの範囲を含むネットワーク オブジェクト、またはホスト、範囲、あるいはその両方を含むネットワーク オブジェクト グループのいずれかです。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。
- [宛先インターフェイス IP (Destination Interface IP)] : PAT アドレスとして使用する宛先インターフェイスを指定します。このオプションを使用する場合、特定の [宛先インターフェイス オブジェクト (Destination Interface Object)] を選択する必要があります。[すべて (Any)] を宛先インターフェイスとして使用することはできません。これは、インターフェイス PAT を実装するもう 1つの方法です。

### ラウンドロビン (Round Robin)

アドレスとポートをラウンドロビン形式で割り当てます。デフォルトではラウンドロビンは使用されず、1つの PAT アドレスのポートがすべて割り当てられると次の PAT アドレスが使用されます。ラウンドロビン方式では、プール内の各 PAT アドレスから 1つずつアドレス/ポートが割り当てられると最初のアドレスに戻り、次に 2 番目のアドレスというように順に使用されます。

### 拡張 PAT テーブル (Extended PAT Table)

拡張 PAT を使用します。拡張 PAT では、変換情報の宛先アドレスとポートを含め、IP アドレスごとではなく、サービスごとに 65535 個のポートが使用されます。通常、PAT 変換の作成時に宛先ポートとアドレスは考慮されないため、PAT アドレスあたり 65535 個のポートに制限されます。たとえば、拡張 PAT を使用して、192.168.1.7:23 に向かう場合の 10.1.1.1:1027 の変換、および 192.168.1.7:80 に向かう場合の 10.1.1.1:1027 の変換を作成できます。このオプションは、インターフェイス PAT またはインターフェイス PAT フォールバックで使用することはできません。



### フラットポート範囲 (Flat Port Range)、予約済みポートを含める (Include Reserved Ports)

TCP/UDP ポートを割り当てる際に、ポート範囲 (1024 ~ 65535) を単一のフラットな範囲として使用します。(6.7より前) 変換のマッピングポート番号を選択すると、PAT は実際の送信元ポート番号を使用できます (使用可能な場合)。ただし、このオプションを設定しないと、実際のポートが使用できない場合、デフォルトでは、実際のポート番号と同じポート範囲 (1 ~ 511、512 ~ 1023、および 1024 ~ 65535) からマッピングポートが選択されます。下位の範囲でポートが不足するのを回避するには、この設定を行います。1 ~ 65535 の範囲全体を使用するには、[予約済みポートを含む (Include Reserved Ports)] オプションも選択します。バージョン 6.7以降を実行している Threat Defense デバイスの場合、オプションを選択するかどうかにかかわらず、フラットなポート範囲が常に設定されます。これらのシステムには、[予約済みポートを含む (Include Reserved Ports)] オプションを選択しても、その設定が適用されます。

### ブロック割り当て

ポートのブロック割り当てを有効にする場合。キャリアグレードまたは大規模 PAT では、NAT に 1 度に 1 つのポート変換を割り当てさせるのではなく、各ホストにポートのブロックを割り当てることができます。ポートのブロックを割り当てると、ホストからの後続の接続はブロック内の新しい任意選択されたポートを使用します。必要に応じて、ホストが元のブロック内のすべてのポートに関してアクティブな接続を持つ場合は追加のブロックが割り当てられます。ポートブロックは、1024 ~ 65535 の範囲でのみ割り当てられます。ポートのブロック割り当てはラウンドロビンと互換性がありますが、拡張 PAT またはフラットなポート範囲のオプションと一緒に使用することはできません。また、インターフェイス PAT フォールバックも使用できません。

## 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。これらのプロパティはすべてオプションであり、該当サービスが必要な場合だけに設定します。

### このルールに一致する DNS 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 クエリと応答の書き換え \(123 ページ\)](#) 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、ブリッジグループのメンバーではない宛先インターフェイスを選択した場合にのみ使用できます。インターフェイスの IPv6 アドレスを使用するには、[IPv6] オプションも選択します。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。PAT プールを構成する場合も、このオプションを選択することはできません。

## IPv6

インターフェイス PAT に宛先インターフェイスの IPv6 アドレスを使用するかどうかを指定します。

### [ ネット間マッピング (Net to Net Mapping) ] (スタティック NAT のみ)

NAT 46 の場合、このオプションを選択して、最初の IPv4 アドレスを最初の IPv6 アドレスに変換し、2 番目を 2 番目に変換という順序で変換します。このオプションを選択しない場合、IPv4 埋め込み方式が使用されます。1 対 1 変換の場合は、このオプションを使用する必要があります。

### 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 が不要で、場合によっては接続性に関する問題を引き起こす可能性があります。

### 宛先インターフェイス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て、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。

### [ 単方向 (Unidirectional) ] (手動 NAT のみ、スタティック NAT のみ)。

このオプションを選択すると、宛先アドレスが発信元アドレスにトラフィックを開始しないようにできます。単方向オプションは主にテスト目的に有効であり、すべてのプロトコルで機能するとは限りません。たとえば、SIP では、NAT を使用して SIP ヘッダーを変換するためにプロトコルインスペクションが必要ですが、変換を単方向にするとこの処理は行われません。

## 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 ネットワークでは次の変換タイプを使用できます。

- NAT64、NAT46 : IPv6 パケットを IPv4 (およびその反対) に変換します。2 つのポリシーを定義する必要があります。1 つは IPv6 から IPv4 への変換用、もう 1 つは IPv4 から IPv6 への変換用です。これは、1 つの手動 NAT ルールで実行できますが、DNS サーバーが外部ネットワーク上にある場合、DNS 応答をリライトする必要があります。宛先を指定するときに手動 NAT ルールで DNS リライトを有効にすることができないため、2 つの自動 NAT ルールを作成することがより適切なソリューションです。



(注) NAT46 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 の使用を推奨します。ダイナミック NAT または PAT を使用できますが、IPv6 アドレスは大量にあるため、ダイナミック NAT を使用する必要はありません。



(注) NAT64 および NAT 46 は、標準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 アドレスの IPv4 への変換

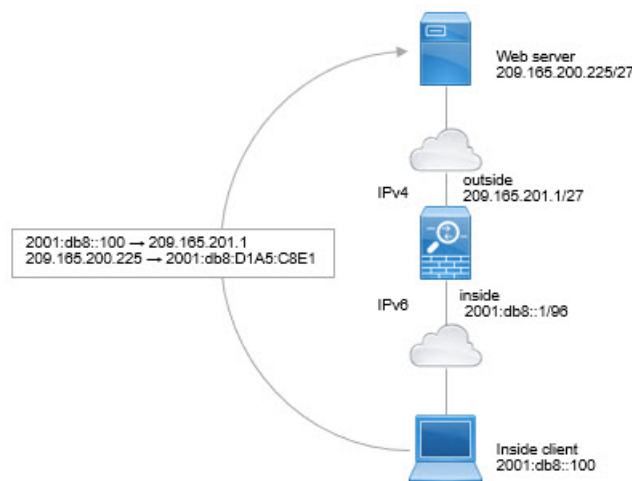
トラフィックが IPv6 ネットワークから IPv4 専用ネットワークに移動する場合、IPv6 アドレスを IPv4 に変換する必要があります。また、トラフィックを IPv4 から IPv6 に戻す必要があります。2 つのアドレス プール (IPv4 ネットワークに IPv6 アドレスをバインドする IPv4 アドレス プールと、IPv6 ネットワークに IPv4 アドレスをバインドする IPv6 アドレス プール) を定義する必要があります。

- NAT64 ルール用の 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 やスタティック NAT と比べると、多数の IPv6 クライアント アドレスがある場合でも、比較的簡単に対応できます。
- 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。これは、1 つの手動 NAT ルールで実行できますが、DNS サーバーが外部ネットワーク上にある場合、DNS 応答をリライトする必要があります。宛先を指定するときに手動 NAT ルールで DNS リライトを有効にすることができないため、2 つの自動 NAT ルールを作成することがより適切なソリューションです。

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

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



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。

### 手順

**ステップ 1** 内部 IPv6 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)] > [オブジェクト管理 (Object Management)] を選択します。
- b) 目次から [ネットワーク (Network)] を選択して、[ネットワークの追加 (Add Network)] > [オブジェクトの追加 (Add Object)] 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 アドレス 2001:DB8::/96 を入力します。

## New Network Object

Name

inside\_v6

Description

Network

 Host  Range  Network  FQDN

2001:db8::/96

 Allow Overrides

d) [保存 (Save) ]をクリックします。

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

- a) [デバイス (Devices) ]> [NAT] を選択し、Threat Defense NAT ポリシーを作成または編集します。
- b) [ルールの追加 (Add Rule) ]をクリックします。
- c) 次のプロパティを設定します。
  - [NAT ルール (NAT Rule) ] = 手動 NAT ルール (Manual NAT Rule) 。
  - [タイプ (Type) ] = Dynamic。
- d) [インターフェイスオブジェクト (Interface Objects) ] で、次の項目を設定します。
  - [送信元インターフェイス オブジェクト (Source Interface Objects) ] = inside。
  - [宛先インターフェイス オブジェクト (Destination Interface Objects) ] = outside。
- e) [変換 (Translation) ] で、次の項目を設定します。
  - [元の送信元 (Original Source) ] = inside\_v6 ネットワーク オブジェクト。
  - [変換済みの送信元 (Translated Source) ] = 宛先インターフェイス IP (Destination Interface IP) 。
  - [元の宛先 (Original Destination) ] : inside\_v6 ネットワーク オブジェクト。
  - [変換済みの宛先 (Translated Destination) ] = any-ipv4 ネットワーク オブジェクト。

## Add NAT Rule

Insert:  
 In Category:

Type:

Enable

Description:

Interface Objects   Translation   PAT Pool   Advanced

Original Packet	Translated Packet
Original Source:* <input type="text" value="inside_v6"/> +	Translated Source: <input type="text" value="Destination Interface IP"/> <small>The values selected for Destination Interface Objects in 'Interface Objects' tab will be used</small>
Original Destination: <input type="text" value="Address"/> <input type="text" value="inside_v6"/> +	Translated Destination: <input type="text" value="any-ipv4"/> +

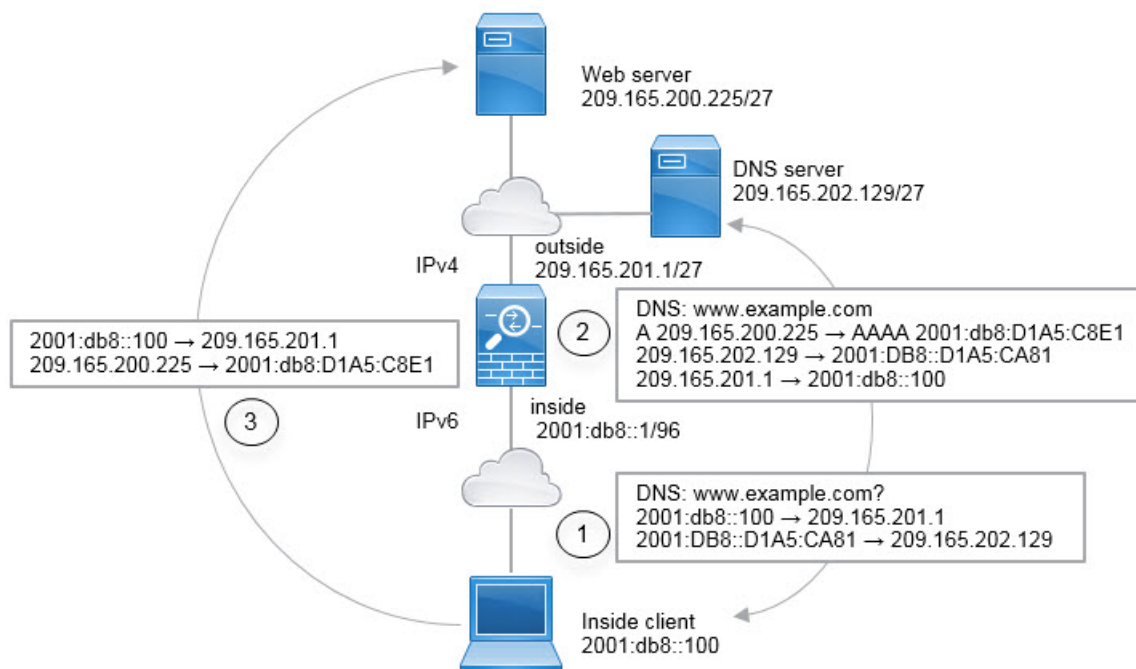
f) [OK] をクリックします。

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

g) [NATルール (NAT rule) ] ページで [保存 (Save) ] をクリックします。

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

次の図は、内部の IPv6 専用ネットワークが存在し、内部ユーザー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 アドレスを持つ動的インターフェイス 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 サーバーからの応答を 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 サーバーに 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 サーバーが、www.example.com が 209.165.200.225 であることを示す A レコードに回答します。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 サーバーの 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。

### 始める前に

デバイスに対応するインターフェイスが含まれているインターフェイスオブジェクト (セキュリティゾーンまたはインターフェイスグループ) があることを確認します。この例では、インターフェイスオブジェクトは **inside** および **outside** という名前のセキュリティゾーンであると仮定します。インターフェイスオブジェクトを設定するには、[オブジェクト (Objects)] > [オブジェクト管理 (Object Management)] を選択し、[インターフェイス (Interface)] を選択します。

### 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)] > [オブジェクト管理 (Object Management)] を選択します。
- b) 目次から [ネットワーク (Network)] を選択して、[ネットワークの追加 (Add Network)] > [オブジェクトの追加 (Add Object)] 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、ネットワークアドレス 2001:DB8::/96 を入力します。



## New Network Object

Name

inside\_v6

Description

Network

 Host  Range  Network  FQDN

2001:db8::/96

 Allow Overrides

- d) [保存 (Save) ] をクリックします。
- e) [ネットワークの追加 (Add Network) ] > [オブジェクトの追加 (Add Object) ] 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 (たとえば、outside\_v4\_any) を付けて、ネットワーク アドレス 0.0.0.0/0 を入力します。

## New Network Object

Name

outside\_v4\_any

Description

Network

 Host  Range  Network  FQDN

0.0.0.0/0

 Allow Overrides

- f) [保存 (Save) ] をクリックします。

**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。

**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) [ルール of の追加 (Add Rule) ] をクリックします。
- b) 次のプロパティを設定します。

- [NAT ルール (NAT Rule) ] = 自動 NAT ルール。
  - [タイプ (Type) ] = Static。
- c) [インターフェイスオブジェクト (Interface Objects) ] で、次の項目を設定します。
- [送信元インターフェイス オブジェクト (Source Interface Objects) ] = outside。
  - [宛先インターフェイス オブジェクト (Destination Interface Objects) ] = inside。
- d) [変換 (Translation) ] で、次の項目を設定します。
- [元の送信元 (Original Source) ] = outside\_v4\_any ネットワーク オブジェクト。
  - [変換済みの送信元 (Translated Source) ] > [アドレス (Address) ] = inside\_v6 ネットワークオブジェクト。
- e) [詳細 (Advanced) ] 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。

## Add NAT Rule

NAT Rule:

Type:

Enable

Interface Objects   Translation   PAT Pool   Advanced

Original Packet	Translated Packet
Original Source:* <input type="text" value="outside_v4_any"/> +	Translated Source: <input type="text" value="Address"/> +
Original Port: <input type="text" value="TCP"/>	Translated Port: <input type="text"/>

- f) [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。

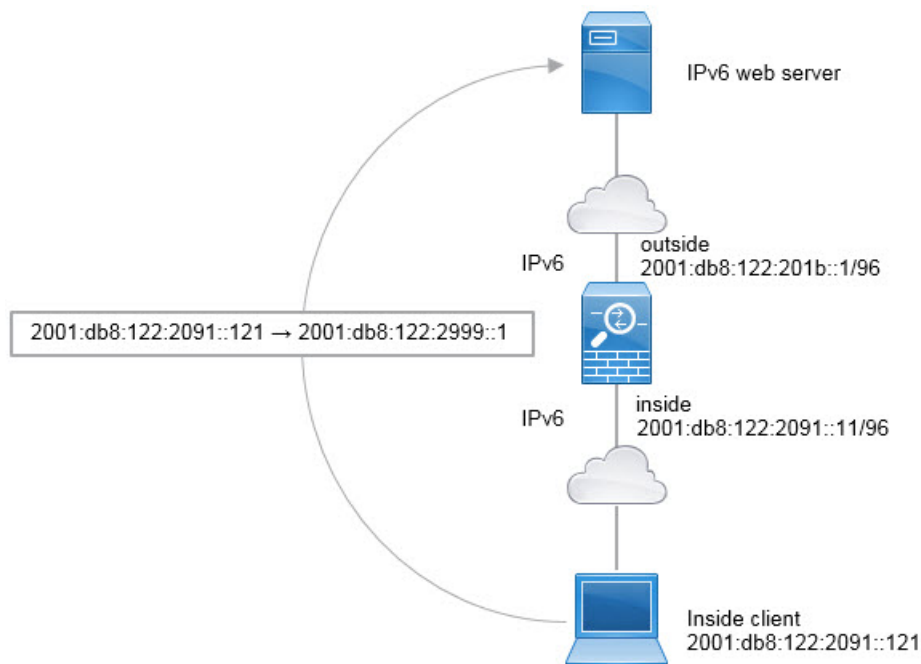
## NAT66 : IPv6 アドレスの異なる IPv6 アドレスへの変換

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

異なるアドレス タイプ間での変換ではないため、NAT66 変換の単一のルールが必要です。これらのルールは、自動 NAT を使用して簡単にモデル化することができます。ただし、リターントラフィックを許可しない場合は、手動 NAT のみを使用してスタティック NAT ルールを単方向にできます。

### NAT66 の例 : ネットワーク間のスタティック変換

自動 NAT を使用して、IPv6 アドレスプール間のスタティック変換を設定できます。次の例では、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。



#### 始める前に

デバイスに対応するインターフェイスが含まれているインターフェイスオブジェクト（セキュリティゾーンまたはインターフェイスグループ）があることを確認します。この例では、インターフェイスオブジェクトは **inside** および **outside** という名前のセキュリティゾーンであると仮定します。インターフェイスオブジェクトを設定するには、[オブジェクト (Objects)] > [オブジェクト管理 (Object Management)] を選択し、[インターフェイス (Interface)] を選択します。

## 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。

- [オブジェクト (Objects)] > [オブジェクト管理 (Object Management)] を選択します。
- 目次から [ネットワーク (Network)] を選択して、[ネットワークの追加 (Add Network)] > [オブジェクトの追加 (Add Object)] をクリックします。
- 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 (たとえば、inside\_v6) を付けて、ネットワークアドレス 2001:db8:122:2091::/96 を入力します。

## New Network Object

Name

inside\_v6

Description

Network

 Host  Range  Network  FQDN

2001:db8:122:2091::/96

 Allow Overrides

- [保存 (Save)] をクリックします。
- [ネットワークの追加 (Add Network)] > [オブジェクトの追加 (Add Object)] をクリックして、外部 IPv6 NAT ネットワークを定義します。

ネットワーク オブジェクトに名前 (たとえば、outside\_nat\_v6) を付けて、ネットワークアドレス 2001:db8:122:2999::/96 を入力します。

## New Network Object

Name

outside\_nat\_v6

Description

Network

 Host  Range  Network  FQDN

2001:db8:122:2999::/96

 Allow Overrides

f) [保存 (Save) ]をクリックします。

**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) [デバイス (Devices) ]> [NAT] を選択し、Threat Defense NAT ポリシーを作成または編集します。
- b) [ルール追加 (Add Rule) ]をクリックします。
- c) 次のプロパティを設定します。
  - [NAT ルール (NAT Rule) ] = 自動 NAT ルール。
  - [タイプ (Type) ] = Static。
- d) [インターフェイスオブジェクト (Interface Objects) ]で、次の項目を設定します。
  - [送信元インターフェイス オブジェクト (Source Interface Objects) ] = inside。
  - [宛先インターフェイス オブジェクト (Destination Interface Objects) ] = outside。
- e) [変換 (Translation) ]で、次の項目を設定します。
  - [元の送信元 (Original Source) ] = inside\_v6 ネットワーク オブジェクト。
  - [変換済みの送信元 (Translated Source) ]> [アドレス (Address) ] = outside\_nat\_v6 ネットワークオブジェクト。

## Add NAT Rule

NAT Rule:

Type:

Enable

Interface Objects   Translation   PAT Pool   Advanced

Original Packet	Translated Packet
Original Source:*	Translated Source:
<input type="text" value="inside_v6"/> +	<input type="text" value="Address"/>
Original Port:	Translated Port:
<input type="text" value="TCP"/>	<input type="text" value="outside_nat_v6"/> +
<input type="text"/>	<input type="text"/>

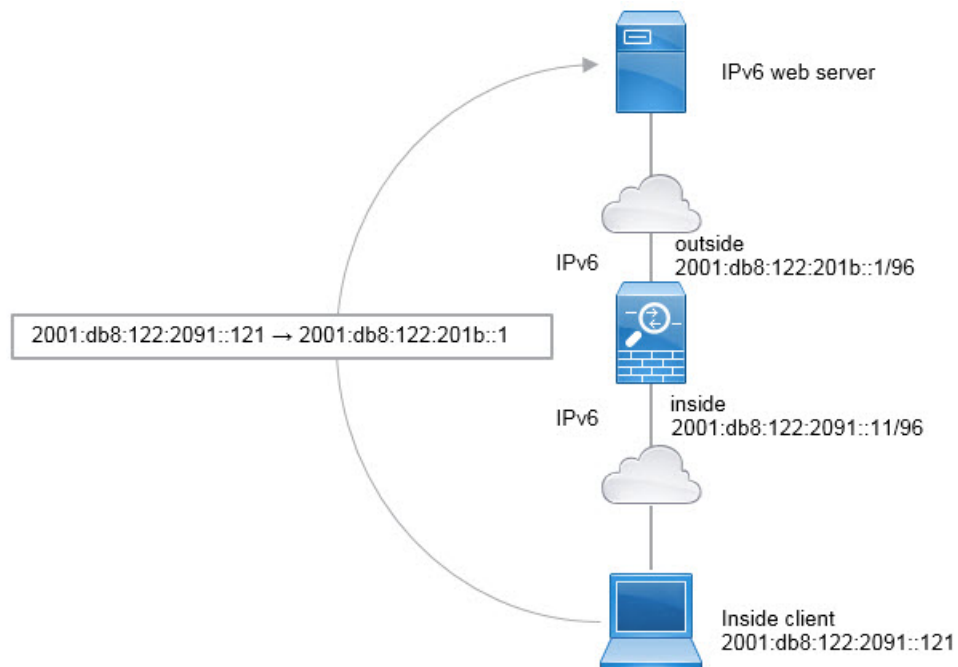
f) [OK] をクリックします。

このルールにより、内部インターフェイス上の 2001:db8:122:2091::/96 サブネットから外部インターフェイスに向かうすべてのトラフィックが、2001:db8:122:2999::/96 ネットワーク上のアドレスにスタティック 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。

NAT66 のインターフェイス PAT ルールを設定すると、そのインターフェイスに設定されているすべてのグローバルアドレスが PAT のマッピングに使用されます。インターフェイスのリンクローカルアドレスまたはサイトローカルアドレスは、PAT には使用されません。



### 始める前に

デバイスに対応するインターフェイスが含まれているインターフェイスオブジェクト（セキュリティゾーンまたはインターフェイスグループ）があることを確認します。この例では、インターフェイスオブジェクトは **inside** および **outside** という名前のセキュリティゾーンであると仮定します。インターフェイスオブジェクトを設定するには、**[オブジェクト (Objects)] > [オブジェクト管理 (Object Management)]** を選択し、**[インターフェイス (Interface)]** を選択します。

### 手順

**ステップ 1** 内部 IPv6 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。

- [オブジェクト (Objects)] > [オブジェクト管理 (Object Management)]** を選択します。
- 目次から **[ネットワーク (Network)]** を選択して、**[ネットワークの追加 (Add Network)] > [オブジェクトの追加 (Add Object)]** をクリックします。
- 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（たとえば、`inside_v6`）を付けて、ネットワークアドレス `2001:db8:122:2091::/96` を入力します。

## New Network Object

Name

Description

Network

Host     Range     Network     FQDN

Allow Overrides

d) [保存 (Save) ]をクリックします。

**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) [デバイス (Devices) ]>[NAT] を選択し、Threat Defense NAT ポリシーを作成または編集します。
- b) [ルールの追加 (Add Rule) ]をクリックします。
- c) 次のプロパティを設定します。
  - [NAT ルール (NAT Rule) ] = 自動 NAT ルール。
  - [タイプ (Type) ] = Dynamic。
- d) [インターフェイスオブジェクト (Interface Objects) ] で、次の項目を設定します。
  - [送信元インターフェイス オブジェクト (Source Interface Objects) ] = inside。



- [宛先インターフェイス オブジェクト (Destination Interface Objects) ] = outside。
- e) [変換 (Translation) ] で、次の項目を設定します。
- [元の送信元 (Original Source) ] = inside\_v6 ネットワーク オブジェクト。
  - [変換済みの送信元 (Translated Source) ] = 宛先インターフェイス IP (Destination Interface IP) 。
- f) [詳細 (Advanced) ] で、[IPv6] を選択します。これは、宛先インターフェイスの IPv6 が使用されることを意味します。

## Add NAT Rule

NAT Rule:  
Auto NAT Rule ▼

Type:  
Dynamic ▼

Enable

Interface Objects   Translation   PAT Pool   Advanced

Original Packet	Translated Packet
Original Source:* inside_v6 ▼ +	Translated Source: Destination Interface IP ▼ <small>i The values selected for Destination Interface Objects in 'Interface Objects' tab will be used</small>
Original Port: TCP ▼	Translated Port: [ ]

- g) [OK] をクリックします。

このルールでは、内部インターフェイスの 2001:db8:122:2091::/96 サブネットから外部インターフェイスへのトラフィックは、外部インターフェイス用に設定された IPv6 グローバルアドレスのいずれかに NAT66 PAT 変換されます。

## NAT のモニタリング

NAT 接続をモニター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** 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** 現在アクティブな実際の NAT 変換を表示します。
- **clear xlate** アクティブな NAT 変換を削除できます。既存の接続は接続が終了するまで古い変換スロットを継続して使用するため、NAT ルールを変更する場合はアクティブな変換を削除しなければならないことがあります。変換を消去することで、クライアントの次の接続時に、システムは新しいルールに基づいてクライアントの新しい変換を作成します。

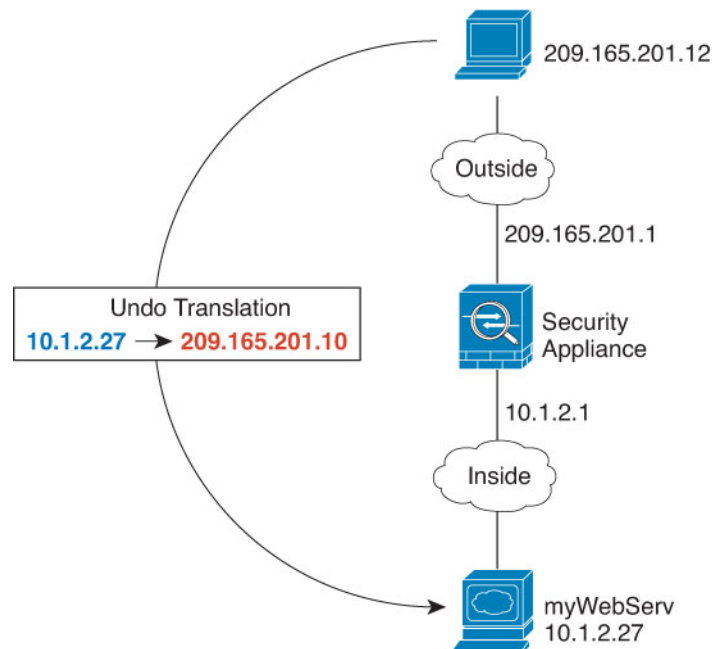
## NAT の例

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

### 内部 Web サーバー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 サーバー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 15: 内部 Web サーバーのスタティック NAT



### 始める前に

Web サーバを保護するデバイスのインターフェイスが含まれているインターフェイス オブジェクト (セキュリティ ゾーンまたはインターフェイス グループ) があることを確認します。この例では、インターフェイス オブジェクトは **inside** および **outside** という名前のセキュリティ ゾーンであると仮定します。インターフェイス オブジェクトを設定するには、[オブジェクト (Objects)] > [オブジェクト管理 (Object Management)] を選択し、[インターフェイス (Interface)] を選択します。

### 手順

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

- [オブジェクト (Objects)] > [オブジェクト管理 (Object Management)] を選択します。
- 目次から [ネットワーク (Network)] を選択して、[ネットワークの追加 (Add Network)] > [オブジェクトの追加 (Add Object)] をクリックします。
- Web サーバーのプライベート 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 (たとえば、WebServerPrivate) を付けて、実際のホスト IP アドレス 10.1.2.27 を入力します。

#### New Network Object

Name

Description

Network

Host  Range  Network  FQDN

Allow Overrides

▶ Override (0)

- [保存 (Save)] をクリックします。
- [ネットワークの追加 (Add Network)] > [オブジェクトの追加 (Add Object)] 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 (たとえば、WebServerPublic) を付けて、ホスト アドレス 209.165.201.10 を入力します。

### New Network Object

Name  
WebServerPublic

Description

Network  
 Host  Range  Network  FQDN

209.165.201.10

Allow Overrides

► Override (0)

f) [保存 (Save) ]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) [デバイス (Devices) ]>[NAT] を選択し、Threat Defense NAT ポリシーを作成または編集します。
- b) [ルールの追加 (Add Rule) ]をクリックします。
- c) 次のプロパティを設定します。
  - [NAT ルール (NAT Rule) ] = 自動 NAT ルール。
  - [タイプ (Type) ] = Static。
- d) [インターフェイスオブジェクト (Interface Objects) ] で、次の項目を設定します。
  - [送信元インターフェイス オブジェクト (Source Interface Objects) ] = inside。
  - [宛先インターフェイス オブジェクト (Destination Interface Objects) ] = outside。
- e) [変換 (Translation) ] で、次の項目を設定します。
  - [元の送信元 (Original Source) ] = WebServerPrivate ネットワーク オブジェクト。
  - [変換済みの送信元 (Translated Source) ]>[アドレス (Address) ] = WebServerPublic ネットワークオブジェクト。

## Add NAT Rule

NAT Rule:  
Auto NAT Rule

Type:  
Static

Enable

Interface Objects Translation PAT Pool Advanced

Original Packet Translated Packet

Original Source:\*  
WebServerPrivate +

Original Port:  
TCP

Translated Source:  
Address

Translated Port:  
WebServerPublic +

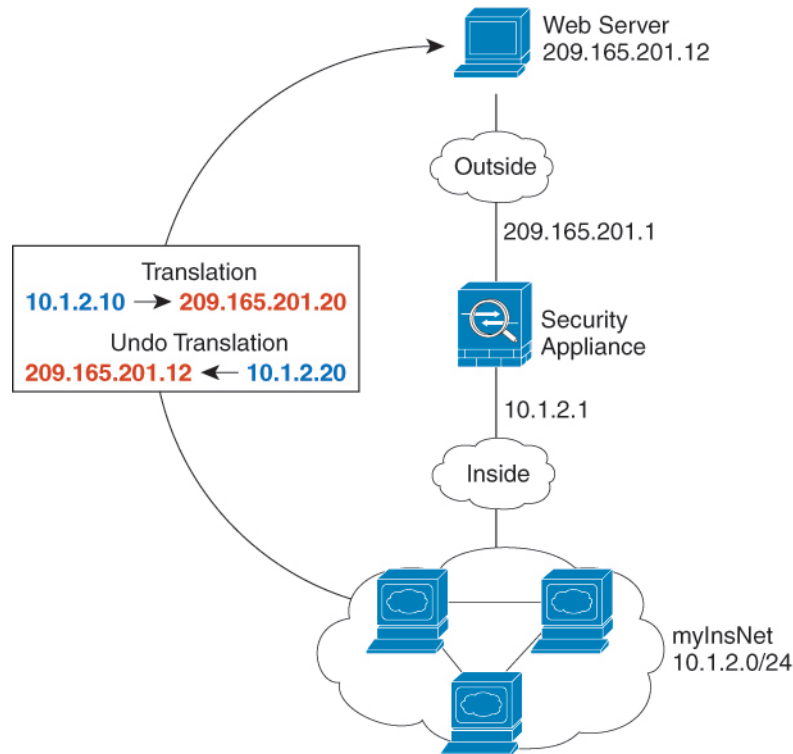
f) [保存 (Save)] をクリックします。

ステップ3 [NAT ルール (NAT rule)] ページで [保存 (Save)] をクリックします。

## 内部ホストのダイナミック自動 NAT および外部 Web サーバーのスタティック NAT

次の例では、プライベート ネットワーク上の内部ユーザーが外部にアクセスする場合、このユーザーにダイナミック NAT を設定します。また、内部ユーザーが外部 Web サーバーに接続する場合、この Web サーバーのアドレスが内部ネットワークに存在するように見えるアドレスに変換されます。

図 16: 内部の動的 NAT、外部 Web サーバーの静的 NAT



### 始める前に

Web サーバを保護するデバイスのインターフェイスが含まれているインターフェイス オブジェクト (セキュリティゾーンまたはインターフェイス グループ) があることを確認します。この例では、インターフェイス オブジェクトは **inside** および **outside** という名前のセキュリティゾーンであると仮定します。インターフェイス オブジェクトを設定するには、[オブジェクト (Objects)] > [オブジェクト管理 (Object Management)] を選択し、[インターフェイス (Interface)] を選択します。

### 手順

**ステップ 1** 内部アドレスを変換する動的 NAT プールのネットワーク オブジェクトを作成します。

- [オブジェクト (Objects)] > [オブジェクト管理 (Object Management)] を選択します。
- 目次から [ネットワーク (Network)] を選択して、[ネットワークの追加 (Add Network)] > [オブジェクトの追加 (Add Object)] をクリックします。
- 動的 NAT プールを定義します。

ネットワーク オブジェクトに名前を付け (myNATpool など)、ネットワーク範囲 209.165.201.20 ~ 209.165.201.30 を入力します。

New Network Object

Name  
myNATpool

Description

Network  
 Host  Range  Network  FQDN  
209.165.201.20-209.165.201.30

Allow Overrides

d) [保存 (Save) ] をクリックします。

**ステップ 2** 内部ネットワークのネットワーク オブジェクトを作成します。

- [ネットワークを追加 (Add Network) ] > [オブジェクトの追加 (Add Object) ] をクリックします。
- ネットワーク オブジェクトに名前を付け (MyInsNet など) 、ネットワーク アドレス 10.1.2.0/24 を入力します。

New Network Object

Name  
MyInsNet

Description

Network  
 Host  Range  Network  FQDN  
10.1.2.0/24

Allow Overrides

c) [保存 (Save) ] をクリックします。

**ステップ 3** 外部 Web サーバーのネットワーク オブジェクトを作成します。

- [ネットワークを追加 (Add Network) ] > [オブジェクトの追加 (Add Object) ] をクリックします。
- ネットワーク オブジェクトに名前を付け (MyWebServer など) 、ホストアドレス 209.165.201.12 を入力します。

### New Network Object

Name

Description

Network

Host  Range  Network  FQDN

Allow Overrides

c) [保存 (Save) ]をクリックします。

**ステップ 4** 変換済み Web サーバー アドレスのネットワーク オブジェクトを作成します。

- [ネットワークを追加 (Add Network) ]>[オブジェクトの追加 (Add Object) ]をクリックします。
- ネットワーク オブジェクトに名前を付け (TransWebServer など) 、ホストアドレス 10.1.2.20 を入力します。

### New Network Object

Name

Description

Network

Host  Range  Network  FQDN

Allow Overrides

c) [保存 (Save) ]をクリックします。

**ステップ 5** ダイナミック NAT プール オブジェクトを使用して内部ネットワークのダイナミック NAT を設定します。



- a) [デバイス (Devices) ]> [NAT] を選択し、Threat Defense NAT ポリシーを作成または編集します。
- b) [ルール の追加 (Add Rule) ] をクリックします。
- c) 次のプロパティを設定します。
  - [NAT ルール (NAT Rule) ] = 自動 NAT ルール。
  - [タイプ (Type) ] = Dynamic。
- d) [インターフェイスオブジェクト (Interface Objects) ] で、次の項目を設定します。
  - [送信元インターフェイス オブジェクト (Source Interface Objects) ] = inside。
  - [宛先インターフェイス オブジェクト (Destination Interface Objects) ] = outside。
- e) [変換 (Translation) ] で、次の項目を設定します。
  - [元の発信元 (Original Source) ] = myInsNet ネットワーク オブジェクト。
  - [変換済みの送信元 (Translated Source) ]> [アドレス (Address) ] = myNATpool ネットワークオブジェクト。

### Add NAT Rule

NAT Rule:  
Auto NAT Rule

Type:  
Dynamic

Enable

Interface Objects   Translation   PAT Pool   Advanced

Original Packet	Translated Packet
Original Source:* MyInsNet	Translated Source: Address
Original Port: TCP	Translated Port: 

- f) [保存 (Save) ] をクリックします。

### ステップ 6 Web サーバのスタティック NAT を設定します。

- a) [ルール の追加 (Add Rule) ] をクリックします。
- b) 次のプロパティを設定します。

- [NAT ルール (NAT Rule) ] = 自動 NAT ルール。
  - [タイプ (Type) ] = Static。
- c) [インターフェイスオブジェクト (Interface Objects) ] で、次の項目を設定します。
- [送信元インターフェイス オブジェクト (Source Interface Objects) ] = outside。
  - [宛先インターフェイス オブジェクト (Destination Interface Objects) ] = inside。
- d) [変換 (Translation) ] で、次の項目を設定します。
- [元の発信元 (Original Source) ] = myWebServer ネットワーク オブジェクト。
  - [変換済みの送信元 (Translated Source) ] > [アドレス (Address) ] = TransWebServer ネットワークオブジェクト。

## Add NAT Rule

NAT Rule:

Type:

Enable

Interface Objects   **Translation**   PAT Pool   Advanced

Original Packet	Translated Packet
Original Source:* <input type="text" value="MyWebServer"/> +	Translated Source: <input type="text" value="Address"/> +
Original Port: <input type="text" value="TCP"/>	Translated Port: <input type="text" value=""/>
<input type="text" value=""/>	<input type="text" value=""/>

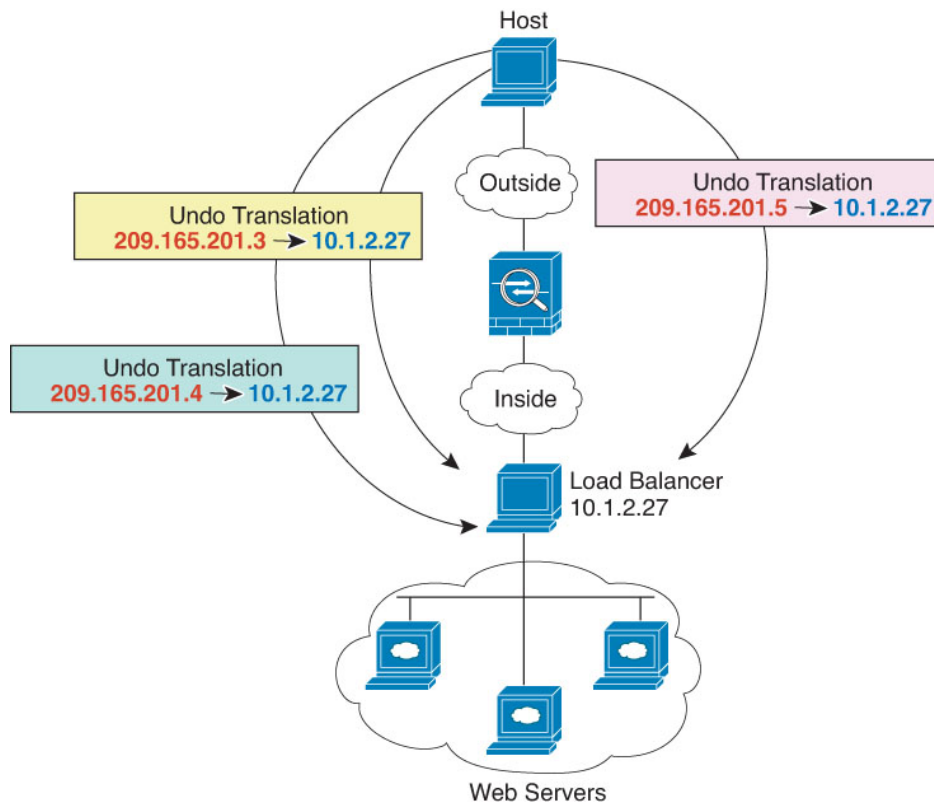
- e) [保存 (Save) ] をクリックします。

**ステップ 7** [NAT ルール (NAT rule) ] ページで [保存 (Save) ] をクリックします。

## 複数のマッピングアドレス（スタティック自動 NAT、1 対多）を持つ内部ロードバランサ

次の例は、複数の IP アドレスに変換される内部ロードバランサを示します。外部ホストがいずれかのマッピング IP アドレスにアクセスすると、このアドレスは単一のロードバランサアドレスに逆変換されます。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 17: 内部ロードバランサに対する 1 対多のスタティック NAT



### 始める前に

Web サーバを保護するデバイスのインターフェイスが含まれているインターフェイス オブジェクト（セキュリティ ゾーンまたはインターフェイス グループ）があることを確認します。この例では、インターフェイス オブジェクトは **inside** および **outside** という名前のセキュリティ ゾーンであると仮定します。インターフェイス オブジェクトを設定するには、[オブジェクト (Objects)] > [オブジェクト管理 (Object Management)] を選択し、[インターフェイス (Interface)] を選択します。

### 手順

**ステップ 1** ロードバランサをマッピングするアドレスに対し、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)] > [オブジェクト管理 (Object Management)] を選択します。
- b) 目次から [ネットワーク (Network)] を選択して、[ネットワークの追加 (Add Network)] > [オブジェクトの追加 (Add Object)] をクリックします。
- c) 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（たとえば、myPublicIPs）を付けて、ネットワーク範囲 209.165.201.3-209.165.201.5 を入力します。

New Network Object

Name  
myPublicIPs

Description

Network  
 Host  Range  Network  FQDN  
 209.165.201.3-209.165.201.5  
 Allow Overrides

- d) [保存 (Save)] をクリックします。

**ステップ 2** ロードバランサに対するネットワーク オブジェクトを作成します。

- a) [ネットワークの追加 (Add Network)] > [オブジェクトの追加 (Add Object)] をクリックします。
- b) ネットワーク オブジェクトに名前（たとえば、myLBHost）を付けて、ホストアドレス 10.1.2.27 を入力します。

New Network Object

Name  
myLBHost

Description

Network  
 Host  Range  Network  FQDN  
 10.1.2.27  
 Allow Overrides

- c) [保存 (Save)] をクリックします。

**ステップ 3** ロードバランサのスタティック NAT を設定します。

- a) [デバイス (Devices)] > [NAT] を選択し、Threat Defense NAT ポリシーを作成または編集します。
- b) [ルールの追加 (Add Rule)] をクリックします。

- c) 次のプロパティを設定します。
- [NAT ルール (NAT Rule) ] = 自動 NAT ルール。
  - [タイプ (Type) ] = Static。
- d) [インターフェイスオブジェクト (Interface Objects) ] で、次の項目を設定します。
- [送信元インターフェイス オブジェクト (Source Interface Objects) ] = inside。
  - [宛先インターフェイス オブジェクト (Destination Interface Objects) ] = outside。
- e) [変換 (Translation) ] で、次の項目を設定します。
- [元の送信元 (Original Source) ] = myLBHost ネットワーク オブジェクト。
  - [変換済みの送信元 (Translated Source) ] > [アドレス (Address) ] = myPublicIPs ネットワークグループ。

## Add NAT Rule

NAT Rule:  
Auto NAT Rule

Type:  
Static

Enable

Interface Objects   Translation   PAT Pool   Advanced

Original Packet	Translated Packet
Original Source:* myLBHost	Translated Source: Address
Original Port: TCP	Translated Port: myPublicIPs

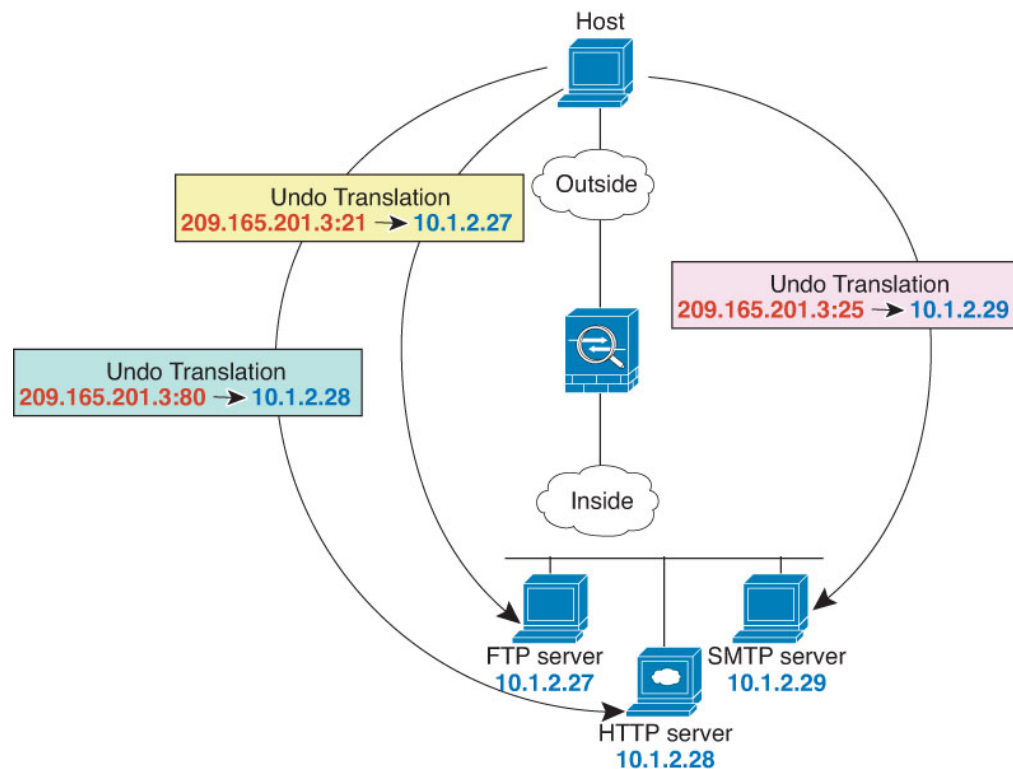
- f) [保存 (Save) ] をクリックします。

**ステップ 4** [NAT ルール (NAT rule) ] ページで [保存 (Save) ] 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、リモートユーザーが 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。これらのサーバーは実際には、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できます。

図 18: ポート変換を設定したスタティック NAT



### 始める前に

サーバを保護するデバイスのインターフェイスが含まれるインターフェイスオブジェクト（セキュリティゾーンまたはインターフェイスグループ）があることを確認します。この例では、インターフェイスオブジェクトは **inside** および **outside** という名前のセキュリティゾーンであると仮定します。インターフェイスオブジェクトを設定するには、[オブジェクト (Objects)] > [オブジェクト管理 (Object Management)] を選択し、[インターフェイス (Interface)] を選択します。

## 手順

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

- [オブジェクト (Objects)] > [オブジェクト管理 (Object Management)] を選択します。
- 目次から [ネットワーク (Network)] を選択して、[ネットワークの追加 (Add Network)] > [オブジェクトの追加 (Add Object)] をクリックします。
- ネットワーク オブジェクトに名前を付け（たとえば「FTPserver」）、FTP サーバーの実際の IP アドレス（10.1.2.27）を入力します。

New Network Object

Name  
FTPserver

Description

Network  
 Host  Range  Network  FQDN  
10.1.2.27

Allow Overrides

- [保存 (Save)] をクリックします。

**ステップ 2** HTTP サーバーのネットワーク オブジェクトを作成します。

- [ネットワークの追加 (Add Network)] > [オブジェクトの追加 (Add Object)] をクリックします。
- ネットワーク オブジェクトに名前を付け（たとえば「HTTPserver」）、ホストアドレス（10.1.2.28）を入力します。

New Network Object

Name  
HTTPserver

Description

Network  
 Host  Range  Network  FQDN  
10.1.2.28

Allow Overrides

- [保存 (Save)] をクリックします。

**ステップ 3** SMTP サーバーのネットワーク オブジェクトを作成します。

- [ネットワークの追加 (Add Network)] > [オブジェクトの追加 (Add Object)] をクリックします。
- ネットワーク オブジェクトに名前を付け（たとえば「SMTPserver」）、ホストアドレス（10.1.2.29）を入力します。

New Network Object

Name

Description

Network  
 Host  Range  Network  FQDN

Allow Overrides

c) [保存 (Save) ]をクリックします。

**ステップ 4** 3つのサーバー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) [ネットワークの追加 (Add Network) ]>[オブジェクトの追加 (Add Object) ]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」）、ホストアドレス（209.165.201.3）を入力します。

New Network Object

Name

Description

Network  
 Host  Range  Network  FQDN

Allow Overrides

c) [保存 (Save) ]をクリックします。

**ステップ 5** FTP サーバー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) [デバイス (Devices) ]>[NAT] を選択し、Threat Defense NAT ポリシーを作成または編集します。
- b) [ルール of 追加 (Add Rule) ]をクリックします。
- c) 次のプロパティを設定します。
  - [NAT ルール (NAT Rule) ] = 自動 NAT ルール。
  - [タイプ (Type) ] = Static。
- d) [インターフェイスオブジェクト (Interface Objects) ]で、次の項目を設定します。
  - [送信元インターフェイス オブジェクト (Source Interface Objects) ] = inside。
  - [宛先インターフェイス オブジェクト (Destination Interface Objects) ] = outside。
- e) [変換 (Translation) ]で、次の項目を設定します。
  - [元の発信元 (Original Source) ] = FTPserver ネットワーク オブジェクト。



- [変換済みの発信元（Translated Source）] > [アドレス（Address）] = ServerPublicIP ネットワークオブジェクト。
- [元のポート（Original Port）] > [TCP] = 21。
- [変換済みポート（Translated Port）] = 21。

## Add NAT Rule



NAT Rule:  
Auto NAT Rule

Type:  
Static

Enable

Interface Objects Translation PAT Pool Advanced

Original Packet	Translated Packet
Original Source:* FTPserver	Translated Source: Address
Original Port: TCP	Translated Port: 21

Cancel OK

f) [保存（Save）] 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) [ルール の追加（Add Rule）] をクリックします。
- b) 次のプロパティを設定します。
  - [NAT ルール（NAT Rule）] = 自動 NAT ルール。
  - [タイプ（Type）] = Static。
- c) [インターフェイスオブジェクト（Interface Objects）] で、次の項目を設定します。
  - [送信元インターフェイス オブジェクト（Source Interface Objects）] = inside。
  - [宛先インターフェイス オブジェクト（Destination Interface Objects）] = outside。
- d) [変換（Translation）] で、次の項目を設定します。

- [元の発信元（Original Source）] = HTTPserver ネットワーク オブジェクト。
- [変換済みの発信元（Translated Source）] > [アドレス（Address）] = ServerPublicIP ネットワーク オブジェクト。
- [元のポート（Original Port）] > [TCP] = 80。
- [変換済みポート（Translated Port）] = 80。

Add NAT Rule ?

NAT Rule:

Type:

Enable

Interface Objects   Translation   PAT Pool   Advanced

Original Packet	Translated Packet
Original Source:*	Translated Source:
<input type="text" value="HTTPserver"/> +	<input type="text" value="Address"/>
Original Port:	<input type="text" value="ServerPublicIP"/> +
<input type="text" value="TCP"/>	Translated Port:
<input type="text" value="80"/>	<input type="text" value="80"/>

e) [保存（Save）] 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。

- [ルール の追加（Add Rule）] をクリックします。
- 次のプロパティを設定します。
  - [NAT ルール（NAT Rule）] = 自動 NAT ルール。
  - [タイプ（Type）] = Static。
- [インターフェイスオブジェクト（Interface Objects）] で、次の項目を設定します。
  - [送信元インターフェイス オブジェクト（Source Interface Objects）] = inside。
  - [宛先インターフェイス オブジェクト（Destination Interface Objects）] = outside。
- [変換（Translation）] で、次の項目を設定します。

- [元の発信元（Original Source）] = SMTPserver ネットワーク オブジェクト。
- [変換済みの発信元（Translated Source）] > [アドレス（Address）] = ServerPublicIP ネットワークオブジェクト。
- [元のポート（Original Port）] > [TCP] = 25。
- [変換済みポート（Translated Port）] = 25。

Add NAT Rule

NAT Rule:  
Auto NAT Rule

Type:  
Static

Enable

Interface Objects Translation PAT Pool Advanced

Original Packet	Translated Packet
Original Source:* SMTPserver	Translated Source: Address
Original Port: TCP	Translated Source: ServerPublicIP
25	Translated Port: 25

Cancel OK

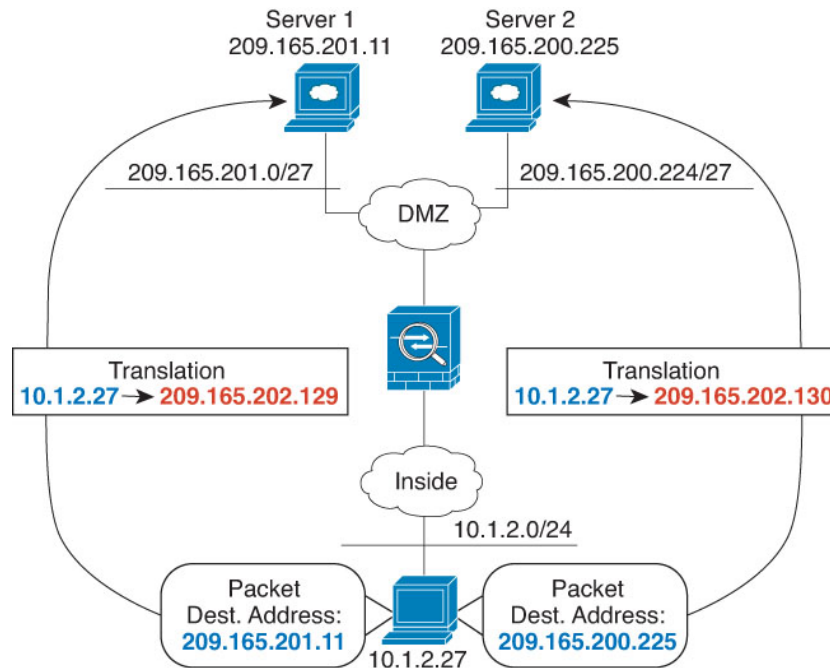
e) [保存（Save）] をクリックします。

**ステップ 8** [NAT ルール（NAT rule）] ページで [保存（Save）] 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 台の異なるサーバー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 19:異なる宛先アドレスを使用する手動 NAT



### 始める前に

サーバを保護するデバイスのインターフェイスが含まれるインターフェイスオブジェクト (セキュリティゾーンまたはインターフェイスグループ) があることを確認します。この例では、インターフェイス オブジェクトは「inside」および「dmz」という名前のセキュリティゾーンであると仮定しています。インターフェイス オブジェクトを設定するには、**[オブジェクト (Objects)] > [オブジェクト管理 (Object Management)]** を選択し、**[インターフェイス (Interface)]** を選択します。

### 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。
- [オブジェクト (Objects)] > [オブジェクト管理 (Object Management)]** を選択します。
  - 目次から **[ネットワーク (Network)]** を選択して、**[ネットワークの追加 (Add Network)] > [オブジェクトの追加 (Add Object)]** をクリックします。
  - ネットワーク オブジェクトに名前を付け (myInsideNetwork など)、実際のネットワーク アドレス 10.1.2.0/24 を入力します。

New Network Object

Name  
myInsideNetwork

Description

Network  
 Host  Range  Network  FQDN  
 10.1.2.0/24

Allow Overrides

d) [保存 (Save)] 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) [ネットワークを追加 (Add Network)] > [オブジェクトの追加 (Add Object)] 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 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)。

New Network Object

Name  
DMZnetwork1

Description

Network  
 Host  Range  Network  FQDN  
 209.165.201.0/27

Allow Overrides

c) [保存 (Save)] 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) [ネットワークを追加 (Add Network)] > [オブジェクトの追加 (Add Object)] 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)、ホストアドレス 209.165.202.129 を入力します。

New Network Object

Name  
PATaddress1

Description

Network  
 Host  Range  Network  FQDN  
 209.165.202.129

Allow Overrides

- c) [保存 (Save) ] 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) [ネットワークを追加 (Add Network) ] > [オブジェクトの追加 (Add Object) ] 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 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)。

New Network Object

Name

Description

Network  
 Host  Range  Network  FQDN

Allow Overrides

- c) [保存 (Save) ] 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) [ネットワークを追加 (Add Network) ] > [オブジェクトの追加 (Add Object) ] 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 アドレス 209.165.202.130 を入力します。

New Network Object

Name

Description

Network  
 Host  Range  Network  FQDN

Allow Overrides

- c) [保存 (Save) ] 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) [デバイス (Devices) ] > [NAT] を選択し、Threat Defense NAT ポリシーを作成または編集します。
- b) [ルール の追加 (Add Rule) ] をクリックします。
- c) 次のプロパティを設定します。
- [NAT ルール (NAT Rule) ] = 手動 NAT ルール (Manual NAT Rule) 。
  - [タイプ (Type) ] = Dynamic。
- d) [インターフェイスオブジェクト (Interface Objects) ] で、次の項目を設定します。
- [送信元インターフェイス オブジェクト (Source Interface Objects) ] = inside。

- [宛先インターフェイス オブジェクト (Destination Interface Objects) ] = dmz。
- e) [変換 (Translation) ] で、次の項目を設定します。
- [元の発信元 (Original Source) ] = myInsideNetwork ネットワーク オブジェクト。
  - [変換された送信元 (Translated Source) ] > [アドレス (Address) ] = PATaddress1 ネットワークオブジェクト。
  - [元の宛先 (Original Destination) ] > [アドレス (Address) ] = DMZnetwork1 ネットワークオブジェクト。
  - [変換済みの宛先 (Translated Destination) ] = DMZnetwork1 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。

The screenshot shows the 'Add NAT Rule' dialog box with the following configuration:

- Manual NAT Rule (selected)
- Insert: In Category (dropdown), NAT Rules Before (dropdown)
- Type: Dynamic (dropdown)
- Enable:
- Description: (empty text box)
- Interface Objects: Translation (selected), PAT Pool, Advanced
- Original Packet:
  - Original Source: myInsideNetwork
  - Original Destination: Address
  - Translated Destination: DMZnetwork1
- Translated Packet:
  - Translated Source: Address
  - Translated Destination: DMZnetwork1
- Buttons: Cancel, OK

- f) [保存 (Save) ] 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) [ルールの追加 (Add Rule) ] をクリックします。
- b) 次のプロパティを設定します。
- [NAT ルール (NAT Rule) ] = 手動 NAT ルール (Manual NAT Rule) 。

- [タイプ (Type) ] = Dynamic。
- c) [インターフェイスオブジェクト (Interface Objects) ] で、次の項目を設定します。
- [送信元インターフェイス オブジェクト (Source Interface Objects) ] = inside。
  - [宛先インターフェイス オブジェクト (Destination Interface Objects) ] = dmz。
- d) [変換 (Translation) ] で、次の項目を設定します。
- [元の発信元 (Original Source) ] = myInsideNetwork ネットワーク オブジェクト。
  - [変換された送信元 (Translated Source) ] > [アドレス (Address) ] = PATaddress2 ネットワークオブジェクト。
  - [元の宛先 (Original Destination) ] > [アドレス (Address) ] = DMZnetwork2 ネットワークオブジェクト。
  - [変換済みの宛先 (Translated Destination) ] = DMZnetwork2 ネットワーク オブジェクト。

The screenshot shows the 'Add NAT Rule' dialog box with the 'Translation' tab selected. The configuration is as follows:

Original Packet	Translated Packet
Original Source*: myInsideNetwork	Translated Source: Address
Original Destination: DMZnetwork2	Translated Destination: DMZnetwork2

Additional settings: Type: Dynamic, Enable: checked, Description: (empty). Buttons: Cancel, OK.

- e) [保存 (Save) ] をクリックします。

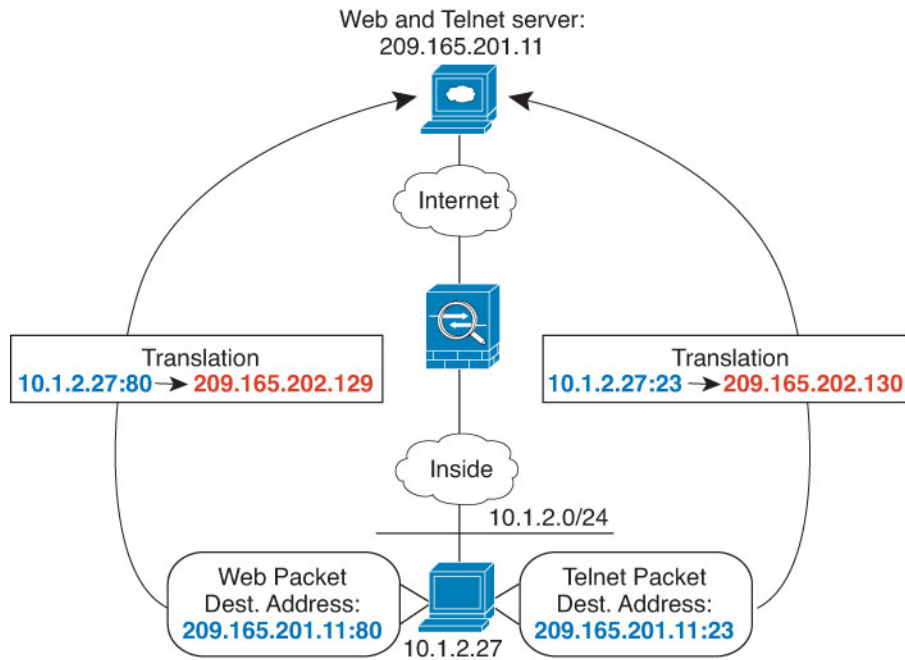
**ステップ 8** [NAT ルール (NAT rule) ] ページで [保存 (Save) ] をクリックします。



## 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ーにアクセスすると、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ーにアクセスすると、実際のアドレスは 209.165.202.130:ポートに変換されます。

図 20:異なる宛先ポートを使用する手動 NAT



### 始める前に

サーバを保護するデバイスのインターフェイスが含まれるインターフェイスオブジェクト（セキュリティゾーンまたはインターフェイスグループ）があることを確認します。この例では、インターフェイスオブジェクトは「inside」および「dmz」という名前のセキュリティゾーンであると仮定しています。インターフェイスオブジェクトを設定するには、[オブジェクト (Objects)] > [オブジェクト管理 (Object Management)] を選択し、[インターフェイス (Interface)] を選択します。

### 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)] > [オブジェクト管理 (Object Management)] を選択します。

- b) 目次から [ネットワーク (Network)] を選択して、[ネットワークの追加 (Add Network)] > [オブジェクトの追加 (Add Object)] 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)、実際のネットワーク アドレス 10.1.2.0/24 を入力します。

New Network Object

---

Name

Description

Network  
 Host  Range  Network  FQDN

Allow Overrides

- d) [保存 (Save)] をクリックします。

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

- a) [ネットワークを追加 (Add Network)] > [オブジェクトの追加 (Add Object)] 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 アドレス 209.165.201.11 を入力します。

New Network Object

---

Name

Description

Network  
 Host  Range  Network  FQDN

Allow Overrides

- c) [保存 (Save)] をクリックします。

**ステップ 3** Telnet を使用するときには、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) [ネットワークを追加 (Add Network)] > [オブジェクトの追加 (Add Object)] 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 アドレス 209.165.202.129 を入力します。

New Network Object

---

Name

Description

Network  
 Host  Range  Network  FQDN

Allow Overrides

- c) [保存 (Save) ] をクリックします。

**ステップ 4** HTTP を使用するとき、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) [ネットワークを追加 (Add Network) ] > [オブジェクトの追加 (Add Object) ] 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)、ホストアドレス 209.165.202.130 を入力します。

New Network Object

Name

Description

Network  
 Host  Range  Network  FQDN

Allow Overrides

- c) [保存 (Save) ] 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) [デバイス (Devices) ] > [NAT] を選択し、Threat Defense NAT ポリシーを作成または編集します。
- b) [ルール of 追加 (Add Rule) ] をクリックします。
- c) 次のプロパティを設定します。
  - [NAT ルール (NAT Rule) ] = 手動 NAT ルール (Manual NAT Rule) 。
  - [タイプ (Type) ] = Dynamic。
- d) [インターフェイスオブジェクト (Interface Objects) ] で、次の項目を設定します。
  - [送信元インターフェイス オブジェクト (Source Interface Objects) ] = inside。
  - [宛先インターフェイス オブジェクト (Destination Interface Objects) ] = dmz。
- e) [変換 (Translation) ] で、次の項目を設定します。
  - [元の発信元 (Original Source) ] = myInsideNetwork ネットワーク オブジェクト。
  - [変換された送信元 (Translated Source) ] > [アドレス (Address) ] = PATaddress1 ネットワークオブジェクト。
  - [元の宛先 (Original Destination) ] > [アドレス (Address) ] = TelnetWebServer ネットワークオブジェクト。
  - [変換済みの宛先 (Translated Destination) ] = TelnetWebServer ネットワーク オブジェクト。
  - [元の宛先ポート (Original Destination Port) ] = TELNET ポート オブジェクト (システム定義) 。

- [変換済みの宛先ポート（Translated Destination Port）] = TELNET ポート オブジェクト（システム定義）。

（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。

Add NAT Rule

Enable  
Description:

Interface Objects Translation PAT Pool Advanced

Original Packet	Translated Packet
Original Source:* myInsideNetwork +	Translated Source: Address +
Original Destination: Address +	Translated Destination: PATaddress1 +
TelnetWebServer +	TelnetWebServer +
Original Source Port: +	Translated Source Port: +
Original Destination Port: TELNET +	Translated Destination Port: TELNET +

Cancel OK

f) [保存（Save）] 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。

- [ルール の追加（Add Rule）] をクリックします。
- 次のプロパティを設定します。
  - [NAT ルール（NAT Rule）] = 手動 NAT ルール（Manual NAT Rule）。
  - [タイプ（Type）] = Dynamic。
- [インターフェイスオブジェクト（Interface Objects）] で、次の項目を設定します。
  - [送信元インターフェイス オブジェクト（Source Interface Objects）] = inside。
  - [宛先インターフェイス オブジェクト（Destination Interface Objects）] = dmz。
- [変換（Translation）] で、次の項目を設定します。

- [元の発信元 (Original Source) ] = myInsideNetwork ネットワーク オブジェクト。
- [変換された送信元 (Translated Source) ] > [アドレス (Address) ] = PATAddress2 ネットワークオブジェクト。
- [元の宛先 (Original Destination) ] > [アドレス (Address) ] = TelnetWebServer ネットワークオブジェクト。
- [変換済みの宛先 (Translated Destination) ] = TelnetWebServer ネットワーク オブジェクト。
- [元の宛先ポート (Original Destination Port) ] = HTTP ポート オブジェクト (システム定義)。
- [変換済みの宛先ポート (Translated Destination Port) ] = HTTP ポート オブジェクト (システム定義)。

Add NAT Rule

Enable  
Description:

Interface Objects Translation PAT Pool Advanced

Original Packet	Translated Packet
Original Source:* myInsideNetwork +	Translated Source: Address +
Original Destination: Address +	Translated Destination: PATAddress2 +
TelnetWebServer +	TelnetWebServer +
Original Source Port: +	Translated Source Port: +
Original Destination Port: HTTP +	Translated Destination Port: HTTP +

Cancel OK

e) [保存 (Save) ] をクリックします。

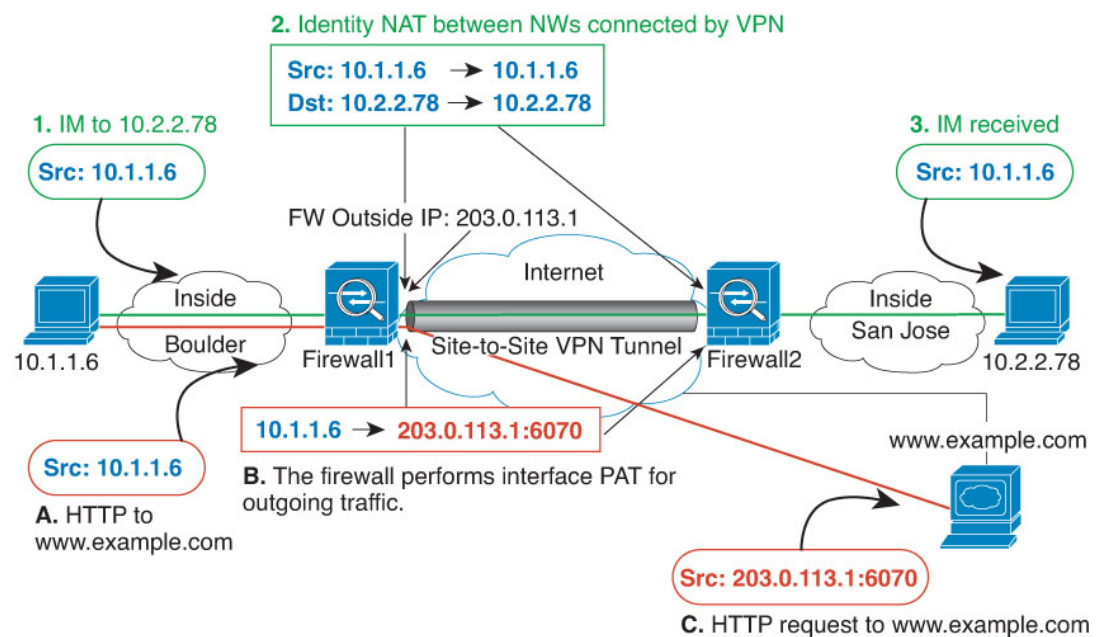
**ステップ 7** [NAT ルール (NAT rule) ] ページで [保存 (Save) ] をクリックします。

## NAT およびサイト間 VPN

Management Center の VPN ウィザードを使用してポリシーベースのサイト間 VPN を作成する場合 ([デバイス (Device)] > [サイト間 (Site To Site)]、[NAT免除 (NAT Exempt)] オプションを選択してルールを自動的に作成できます。NAT ポリシーページ ([デバイス (Device)] > [NAT] > [NAT免除 (NAT Exemptions)]) でデバイスの NAT 免除を表示できます。VPN ウィザードで NAT 免除を設定しない場合は、次の手順で NAT 免除を使用できます。

次の図に、ボールドーとサンノゼのオフィスを接続するサイトツーサイトトンネルを示します。インターネットに渡すトラフィックについて（たとえばボールドーの 10.1.1.6 から www.example.com へ）、インターネットへのアクセスのために NAT によって提供されるパブリック IP アドレスが必要です。次の例では、インターフェイス PAT ルールを使用しています。ただし、VPN トンネルを経由するトラフィックについては（たとえば、ボールドーの 10.1.1.6 からサンノゼの 10.2.2.78 へ）、NAT を実行しません。そのため、アイデンティティ NAT ルールを作成して、そのトラフィックを除外する必要があります。アイデンティティ NAT は同じアドレスにアドレスを変換します。

図 21: サイトツーサイト VPN のためのインターフェイス PAT およびアイデンティティ NAT



次の例は、Firewall1（ボールドー）の設定を示します。

### 始める前に

VPN 内のデバイスに対応するインターフェイスが含まれているインターフェイス オブジェクト（セキュリティゾーンまたはインターフェイスグループ）があることを確認します。この例では、インターフェイスオブジェクトは、Firewall1（ボールドー）インターフェイスに対応する **inside-boulder** および **outside-boulder** という名前のセキュリティゾーンであると仮定します。インターフェイスオブジェクトを設定するには、[オブジェクト (Objects)] > [オブジェ

クト管理 (Object Management) ]を選択してから、[インターフェイス (Interfaces) ]を選択します。

#### 手順

**ステップ 1** さまざまなネットワークを定義するには、オブジェクトを作成します。

- [オブジェクト (Objects) ]>[オブジェクト管理 (Object Management) ]を選択します。
- 目次から[ネットワーク (Network) ]を選択して、[ネットワークの追加 (Add Network) ]>[オブジェクトの追加 (Add Object) ]をクリックします。
- ボールドー内部ネットワークを特定します。

ネットワーク オブジェクトに名前 (たとえば、boulder-network) を付けて、ネットワーク アドレス 10.1.1.0/24 を入力します。

#### New Network Object

Name

Description

Network

Host  Range  Network  FQDN

Allow Overrides

- [保存 (Save) ]をクリックします。
- [ネットワークの追加 (Add Network) ]>[オブジェクトの追加 (Add Object) ]をクリックして、内部サンノゼ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 (たとえば、sanjose-network) を付けて、ネットワーク アドレス 10.2.2.0/24 を入力します。

## New Network Object

Name

Description

Network  
 Host  Range  Network  FQDN

Allow Overrides

f) [保存 (Save) ]をクリックします。

**ステップ 2** Firewall1 (ボールドー) 上で VPN 経由でサンノゼに向かう場合、ボールドー ネットワークの手動アイデンティティ NAT を設定します。

- a) [デバイス (Devices) ]>[NAT] を選択し、Threat Defense NAT ポリシーを作成または編集します。
- b) [ルールの追加 (Add Rule) ]をクリックします。
- c) 次のプロパティを設定します。
  - [NAT ルール (NAT Rule) ] = 手動 NAT ルール (Manual NAT Rule) 。
  - [タイプ (Type) ] = Static。
- d) [インターフェイスオブジェクト (Interface Objects) ] で、次の項目を設定します。
  - [送信元インターフェイス オブジェクト (Source Interface Objects) ] = inside-boulder。
  - [宛先インターフェイス オブジェクト (Destination Interface Objects) ] = outside-boulder。
- e) [変換 (Translation) ] で、次の項目を設定します。
  - [元の送信元 (Original Source) ] = boulder-network オブジェクト。
  - [変換済みの送信元 (Translated Source) ]>[アドレス (Address) ] = boulder-network オブジェクト。
  - [元の宛先 (Original Destination) ]>[アドレス (Address) ] = sanjose-network オブジェクト。
  - [変換済みの宛先] = sanjose-network 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。このルールは、送信元と宛先の両方のアイデンティティ NAT を設定します。

- f) [詳細 (Advanced) ] で [宛先インターフェイスでプロキシARPなし (Do not proxy ARP on Destination interface) ] を選択します。

### Add NAT Rule

Manual NAT Rule

Insert:

In Category: NAT Rules Before

Type: Static

Enable

Description:

Interface Objects Translation PAT Pool Advanced

Original Packet	Translated Packet
Original Source:* boulder-network +	Translated Source: Address
Original Destination: Address	boulder-network +
sanjose-network +	Translated Destination: sanjose-network +

- g) [保存 (Save) ] をクリックします。

**ステップ 3** Firewall1 (ボールドー) 上で内部ボールドーネットワークのインターネットに入る場合、手動ダイナミック インターフェイス PAT を設定します。

- a) [ルールの追加 (Add Rule) ] をクリックします。
- b) 次のプロパティを設定します。
- [NAT ルール (NAT Rule) ] = 手動 NAT ルール (Manual NAT Rule) 。
  - [タイプ (Type) ] = Dynamic。
  - [挿入ルール (Insert Rule) ] = 最初のルールの後の任意の位置。このルールは任意の宛先アドレスに適用されるため、sanjose-network を宛先として使用するルールはこのルールの前に来る必要があります。そうでなければ、sanjose-network ルールは永遠に一致

することがありません。デフォルトでは、新しい手動 NAT ルールは [自動 NAT の前に NAT ルール (NAT Rules Before Auto NAT) ] セクションの最後に配置されます。

- c) [インターフェイスオブジェクト (Interface Objects) ] で、次の項目を設定します。
- [送信元インターフェイス オブジェクト (Source Interface Objects) ] = inside-boulder。
  - [宛先インターフェイス オブジェクト (Destination Interface Objects) ] = outside-boulder。
- d) [変換 (Translation) ] で、次の項目を設定します。
- [元の送信元 (Original Source) ] = boulder-network オブジェクト。
  - [変換済みの送信元 (Translated Source) ] = 宛先インターフェイス IP (Destination Interface IP) 。このオプションでは、宛先インターフェイスオブジェクトに含まれているインターフェイスを使用して、インターフェイス PAT を設定します。
  - [元の宛先 (Original Destination) ] > [アドレス (Address) ] = 任意 (空白のまま) 。
  - [変換済みの宛先 (Translated Destination) ] = 任意 (空白のまま) 。

## Add NAT Rule

NAT Rule:  
Manual NAT Rule

Insert:  
In Category NAT Rules Before

Type:  
Dynamic

Enable

Description:  
[Empty text box]

Interface Objects Translation PAT Pool Advanced

Original Packet Translated Packet

Original Source:\*  
boulder-network +

Original Destination:  
Address

Translated Source:  
Destination Interface IP

**i** The values selected for Destination Interface Objects in 'Interface Objects' tab will be used

- e) [保存 (Save) ] をクリックします。

**ステップ 4** Firewall2 (サンノゼ) の管理を行っている場合、そのデバイスに同様のルールを設定できません。

- 手動アイデンティティ NAT ルールは、宛先が `boulder-network` の場合は `sanjose-network` 向けになります。Firewall2 の内部および外部ネットワーク向けに新しいインターフェイスオブジェクトを作成します。
- 手動ダイナミックインターフェイス PAT ルールは、宛先が「任意」の場合は `sanjose-network` 向けになります。

## NAT を使用した DNS クエリと応答の書き換え

応答内のアドレスを NAT 設定と一致するアドレスに置き換えて、DNS 応答を修正するように Threat Defense デバイスを設定することが必要な場合があります。DNS 修正は、各トランスレーションルールを設定するときに設定できます。DNS 修正は DNS 改ざんとも呼ばれます。

この機能は、NAT ルールに一致する DNS クエリと応答のアドレスを書き換えます (たとえば、IPv4 の A レコード、IPv6 の AAAA レコード、または逆引き DNS クエリの PTR レコード)。マッピングインターフェイスから他のインターフェイスに移動する DNS 応答では、A レコードはマップされた値から実際の値へ書き換えられます。逆に、任意のインターフェイスからマッピングインターフェイスに移動する DNS 応答では、A レコードは実際の値からマップされた値へ書き換えられます。この機能は、NAT44、NAT66、NAT46、および NAT64 と連動します。

以下に、NAT ルールで DNS の書き換えを設定する必要があ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 の書き換えが必要です。
- 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 の書き換えの制限事項

次に DNS の書き換え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 の書き換えは 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、DNS 応答内の IP アドレスを適切な Twice NAT ルールに一致させることができません。DNS 応答には、DNS 要求を求めたパケット内の送信元アドレスと宛先アドレスの組み合わせに関する情報が含まれません。

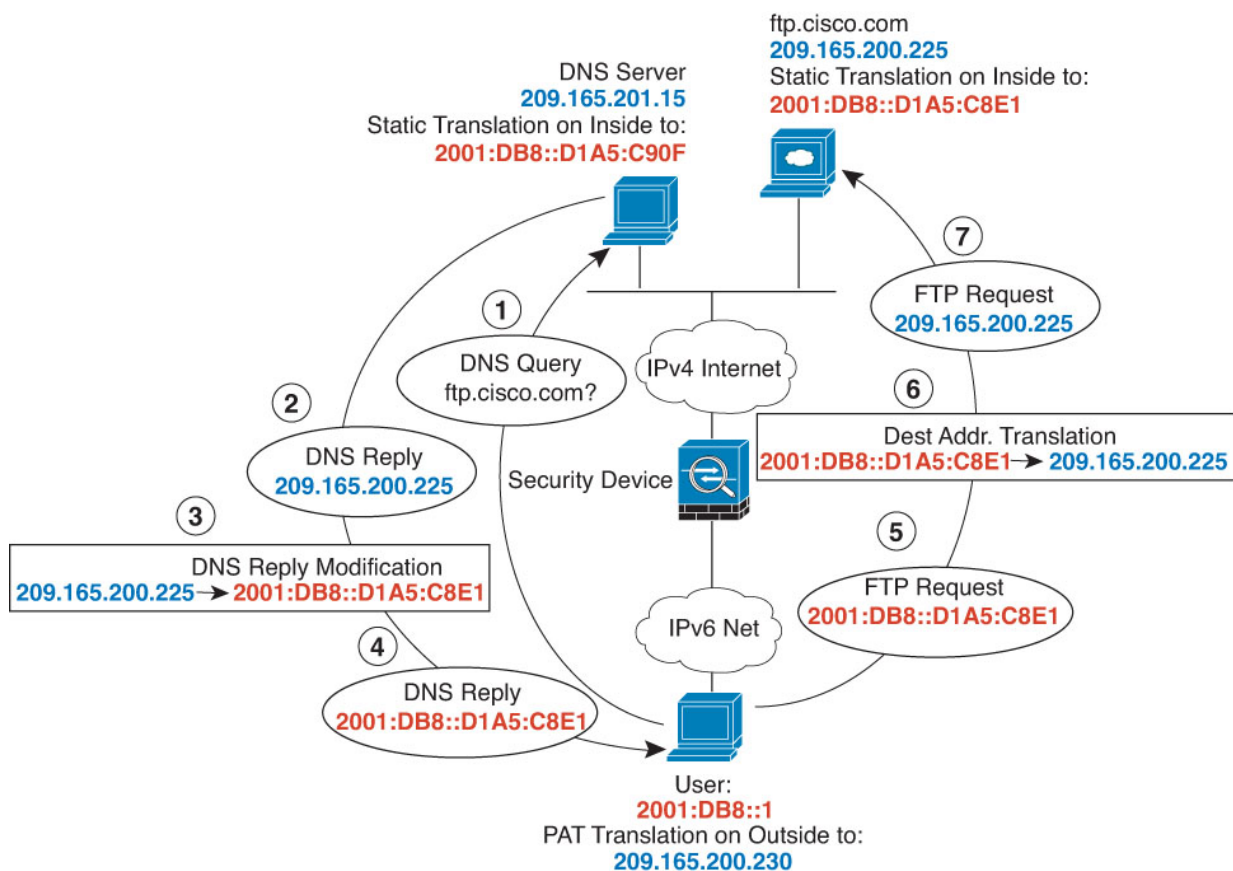
- DNS クエリと応答を書き換えるには、NAT ルールに対して有効な DNS NAT の書き換えを用いた DNS アプリケーション インспекションを有効にする必要があります。デフォルトでは、有効にされた DNS NAT の書き換えによる DNS インспекションはグローバルに適用されるため、インспекション設定を変更する必要はありません。
- 実際には、DNS の書き換えは NAT ルールではなく xlate エントリで実行されます。したがって、ダイナミック ルールに xlate がいない場合、書き換えが正しく実行されません。スタティック NAT の場合は、同じような問題が発生しません。
- DNS の書き換えによって、DNS ダイナミック アップデートのメッセージ（オペレーションコード 5）は書き換えられません。

次のトピックで、NAT ルールでの DNS の書き換えの例を示します。

## DNS64 応答修正

次の図に、外部の IPv4 ネットワーク上の FTP サーバと DNS サーバを示します。システムには、外部サーバ用のスタティック変換があります。この場合、内部 IPv6 ユーザーが 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。

内部ユーザーに 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。



### 始める前に

デバイスに対応するインターフェイスが含まれているインターフェイスオブジェクト（セキュリティゾーンまたはインターフェイスグループ）があることを確認します。この例では、インターフェイスオブジェクトは **inside** および **outside** という名前のセキュリティゾーンであると仮定します。インターフェイスオブジェクトを設定するには、**[オブジェクト (Objects)] > [オブジェクト管理 (Object Management)]** を選択し、**[インターフェイス (Interface)]** を選択します。

### 手順

- ステップ 1** FTP サーバー、DNS サーバー、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。
- [オブジェクト (Objects)] > [オブジェクト管理 (Object Management)]** を選択します。
  - 目次から **[ネットワーク (Network)]** を選択して、**[ネットワークの追加 (Add Network)] > [オブジェクトの追加 (Add Object)]** をクリックします。
  - 実際の FTP サーバー 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)、ホストアドレス 209.165.200.225 を入力します。

## New Network Object

Name

ftp\_server

Description

Network

 Host    Range    Network    FQDN

209.165.200.225

 Allow Overrides

- d) [保存 (Save) ]をクリックします。
- e) [ネットワークを追加 (Add Network) ]>[オブジェクトの追加 (Add Object) ]をクリックして、FTP サーバの変換済み IPv6 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\_v6 など) 、ホストアドレス 2001:DB8::D1A5:C8E1 を入力します。

## New Network Object

Name

ftp\_server\_v6

Description

Network

 Host    Range    Network    FQDN

2001:DB8::D1A5:C8E1

 Allow Overrides

- f) [保存 (Save) ]をクリックします。
- g) [ネットワークを追加 (Add Network) ]>[オブジェクトの追加 (Add Object) ]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) 、ホストアドレス 209.165.201.15 を入力します。

## New Network Object

Name

dns\_server

Description

Network

 Host  Range  Network  FQDN

209.165.201.15

 Allow Overrides

- h) [保存 (Save) ] をクリックします。
- i) [ネットワークを追加 (Add Network) ] > [オブジェクトの追加 (Add Object) ] をクリックして、DNS サーバの変換済み IPv6 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\_v6 など)、ホストアドレス 2001:DB8::D1A5:C90F を入力します (ここで、D1A5:C90F は IPv6 の場合の 209.165.201.15 です)。

## New Network Object

Name

dns\_server\_v6

Description

Network

 Host  Range  Network  FQDN

2001:DB8::D1A5:C90F

 Allow Overrides

- j) [保存 (Save) ] をクリックします。
- k) [ネットワークを追加 (Add Network) ] > [オブジェクトの追加 (Add Object) ] 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 (inside\_v6 など) を付け、ネットワーク アドレス 2001:DB8::/96 を入力します。

New Network Object

---

Name

Description

Network  
 Host  Range  Network  FQDN

Allow Overrides

- l) [保存 (Save) ] をクリックします。
- m) [ネットワークを追加 (Add Network) ] > [オブジェクトの追加 (Add Object) ] をクリックし、内部 IPv6 ネットワークの IPv4 PAT プールを定義します。

ネットワーク オブジェクトに名前を付け (ipv4\_pool など)、範囲 209.165.200.230 ~ 209.165.200.235 を入力します。

New Network Object

---

Name

Description

Network  
 Host  Range  Network  FQDN

Allow Overrides

- n) [保存 (Save) ] をクリックします。

**ステップ 2** FTP サーバーのための、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) [デバイス (Devices) ] > [NAT] を選択し、Threat Defense NAT ポリシーを作成または編集します。
- b) [ルールの追加 (Add Rule) ] をクリックします。
- c) 次のプロパティを設定します。
- [NAT ルール (NAT Rule) ] = 自動 NAT ルール。
  - [タイプ (Type) ] = Static。
- d) [インターフェイスオブジェクト (Interface Objects) ] で、次の項目を設定します。
- [送信元インターフェイス オブジェクト (Source Interface Objects) ] = outside。
  - [宛先インターフェイス オブジェクト (Destination Interface Objects) ] = inside。
- e) [変換 (Translation) ] で、次の項目を設定します。
- [元の発信元 (Original Source) ] = ftp\_server ネットワーク オブジェクト。



- [変換された送信元 (Translated Source)] > [アドレス (Address)] = ftp\_server\_v6 ネットワークオブジェクト。

Add NAT Rule

NAT Rule:  
Auto NAT Rule

Type:  
Static

Enable

Interface Objects Translation PAT Pool Advanced

Original Packet	Translated Packet
Original Source:* ftp_server +	Translated Source: Address
Original Port: TCP	Translated Port: ftp_server_v6 +

- f) [詳細 (Advanced)] で、以下のオプションを選択します。
- [このルールに一致する DNS 応答を変換 (Translate DNS replies that match this rule)]。
  - [ネット間マッピング (Net to Net Mapping)]。1 対 1 の NAT46 変換であるためです。
- g) [OK] をクリックします。

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

- a) [ルールの追加 (Add Rule)] をクリックします。
- b) 次のプロパティを設定します。
- [NAT ルール (NAT Rule)] = 自動 NAT ルール。
  - [タイプ (Type)] = Static。
- c) [インターフェイスオブジェクト (Interface Objects)] で、次の項目を設定します。
- [送信元インターフェイス オブジェクト (Source Interface Objects)] = outside。
  - [宛先インターフェイス オブジェクト (Destination Interface Objects)] = inside。
- d) [変換 (Translation)] で、次の項目を設定します。
- [元の発信元 (Original Source)] = dns\_server ネットワーク オブジェクト。
  - [変換された送信元 (Translated Source)] > [アドレス (Address)] = dns\_server\_v6 ネットワークオブジェクト。

- e) これは1対1のNAT46変換であるため、[詳細 (Advanced)] で、[ネット間マッピング (Net to Net Mapping)] を選択します。

## Add NAT Rule

NAT Rule:

Type:

Enable

Interface Objects   Translation   PAT Pool   Advanced

Original Packet	Translated Packet
Original Source:*	Translated Source:
<input type="text" value="dns_server"/> +	<input type="text" value="Address"/>
Original Port:	Translated Port:
<input type="text" value="TCP"/>	<input type="text" value="dns_server_v6"/> +
<input type="text"/>	<input type="text"/>

- f) [OK] をクリックします。

**ステップ4** 内部IPv6ネットワークに対し、PATプールルールを持つダイナミックNATを設定します。

- [ルールの追加 (Add Rule)] をクリックします。
- 次のプロパティを設定します。
  - [NATルール (NAT Rule)] = 自動NATルール。
  - [タイプ (Type)] = Dynamic。
- [インターフェイスオブジェクト (Interface Objects)] で、次の項目を設定します。
  - [送信元インターフェイスオブジェクト (Source Interface Objects)] = inside。
  - [宛先インターフェイスオブジェクト (Destination Interface Objects)] = outside。
- [変換 (Translation)] で、次の項目を設定します。
  - [元の送信元 (Original Source)] = inside\_v6 ネットワーク オブジェクト。
  - [変換された送信元 (Translated Source)] > [アドレス (Address)] = このフィールドは空のままにします。

## Add NAT Rule

NAT Rule:  
Auto NAT Rule

Type:  
Dynamic

Enable

Interface Objects Translation PAT Pool Advanced

Original Packet

Original Source:\*  
inside\_v6 +

Original Port:  
TCP

Translated Packet

Translated Source:  
Address

Translated Port:

e) [PAT プール (PAT Pool)] で、以下の設定を行います。

- [PAT プールの有効化 (Enable PAT Pool)] = このオプションを選択します。
- [変換された送信元 (Translated Source)] > [アドレス (Address)] = ipv4\_pool ネットワークオブジェクト。

Add NAT Rule

NAT Rule:  
Auto NAT Rule

Type:  
Dynamic

Enable

Interface Objects Translation PAT Pool Advanced

Enable PAT Pool

PAT:  
Address + ipv4\_pool +

Use Round Robin Allocation

Extended PAT Table

Flat Port Range

Include Reserve Ports

Block Allocation

f) [OK] をクリックします。

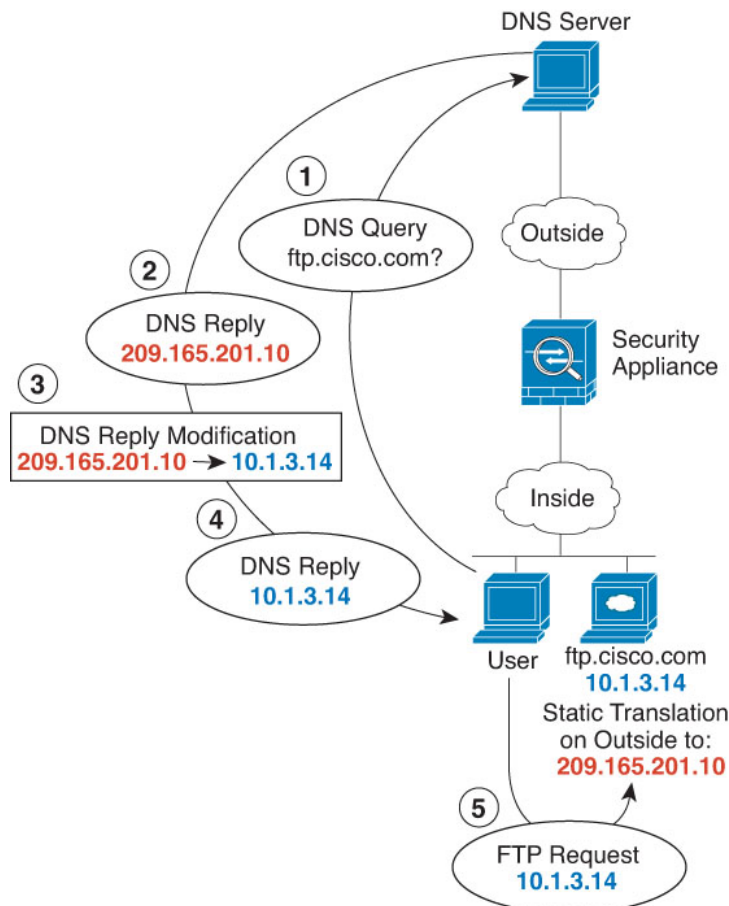
## DNS 応答修正：外部の DNS サーバー

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ーは、マッピングアドレスではなく実際のアドレスを DNS サーバー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 サーバー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。



### 始める前に

デバイスに対応するインターフェイスが含まれているインターフェイスオブジェクト (セキュリティゾーンまたはインターフェイスグループ) があることを確認します。この例では、インターフェイスオブジェクトは **inside** および **outside** という名前のセキュリティゾーンであると仮定します。インターフェイスオブジェクトを設定するには、[オブジェクト (Objects)] > [オブジェクト管理 (Object Management)] を選択し、[インターフェイス (Interface)] を選択します。

## 手順

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

- a) [オブジェクト (Objects)] > [オブジェクト管理 (Object Management)] を選択します。
- b) 目次から [ネットワーク (Network)] を選択して、[ネットワークの追加 (Add Network)] > [オブジェクトの追加 (Add Object)] をクリックします。
- c) 実際の FTP サーバー 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)、ホストアドレス 10.1.3.14 を入力します。

### New Network Object

Name

Description

Network

Host  Range  Network  FQDN

Allow Overrides

- d) [保存 (Save)] をクリックします。
- e) [ネットワークを追加 (Add Network)] > [オブジェクトの追加 (Add Object)] をクリックして、FTP サーバー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)、ホストアドレス 209.165.201.10 を入力します。

## New Network Object

Name

ftp\_server\_outside

Description

Network

 Host  Range  Network  FQDN

209.165.201.10

 Allow Overrides

f) [保存 (Save) ]をクリックします。

**ステップ2** FTP サーバーのための、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) [デバイス (Devices) ]>[NAT] を選択し、Threat Defense NAT ポリシーを作成または編集します。
- b) [ルールの追加 (Add Rule) ]をクリックします。
- c) 次のプロパティを設定します。
  - [NAT ルール (NAT Rule) ] = 自動 NAT ルール。
  - [タイプ (Type) ] = Static。
- d) [インターフェイスオブジェクト (Interface Objects) ] で、次の項目を設定します。
  - [送信元インターフェイス オブジェクト (Source Interface Objects) ] = inside。
  - [宛先インターフェイス オブジェクト (Destination Interface Objects) ] = outside。
- e) [変換 (Translation) ] で、次の項目を設定します。
  - [元の発信元 (Original Source) ] = ftp\_server ネットワーク オブジェクト。
  - [変換済み送信元 (Translated Source) ]>[アドレス (Address) ] = ftp\_server\_outside ネットワークオブジェクト。
- f) [詳細 (Advanced) ] 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。

## Add NAT Rule

NAT Rule:  
Auto NAT Rule

Type:  
Static

Enable

Interface Objects   Translation   PAT Pool   Advanced

Original Packet

Original Source:\*  
ftp\_server +

Original Port:  
TCP

Translated Packet

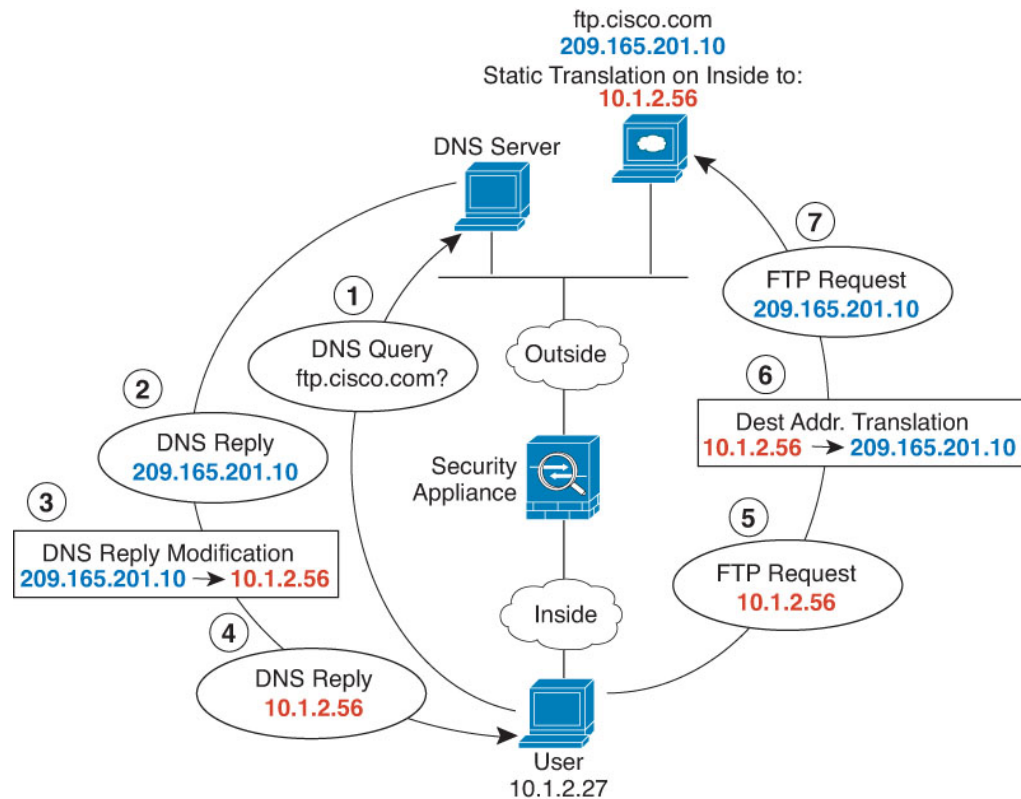
Translated Source:  
Address +

Translated Port:

g) [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 サーバー

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、内部ユーザーが `ftp.cisco.com` のアドレスを DNS サーバーに要求すると、DNS サーバーは実際のアドレス (209.165.20.10) を応答します。内部ユーザーに `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。



### 始める前に

デバイスに対応するインターフェイスが含まれているインターフェイスオブジェクト（セキュリティゾーンまたはインターフェイス グループ）があることを確認します。この例では、インターフェイス オブジェクトは **inside** および **outside** という名前のセキュリティゾーンであると仮定します。インターフェイスオブジェクトを設定するには、**[オブジェクト (Objects)]** > **[オブジェクト管理 (Object Management)]** を選択し、**[インターフェイス (Interface)]** を選択します。

### 手順

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

- [オブジェクト (Objects)]** > **[オブジェクト管理 (Object Management)]** を選択します。
- 目次から **[ネットワーク (Network)]** を選択して、**[ネットワークの追加 (Add Network)]** > **[オブジェクトの追加 (Add Object)]** をクリックします。
- 実際の FTP サーバー 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)、ホストアドレス 209.165.201.10 を入力します。



## New Network Object

Name

ftp\_server

Description

Network

 Host  Range  Network  FQDN

209.165.201.10

 Allow Overrides

- d) [保存 (Save)] をクリックします。
- e) [ネットワークを追加 (Add Network)] > [オブジェクトの追加 (Add Object)] をクリックして、FTP サーバー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 アドレス 10.1.2.56 を入力します。

## New Network Object

Name

ftp\_server\_translated

Description

Network

 Host  Range  Network  FQDN

10.1.2.56

 Allow Overrides

- f) [保存 (Save)] をクリックします。

**ステップ 2** FTP サーバーのための、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) [デバイス (Devices)] > [NAT] を選択し、Threat Defense NAT ポリシーを作成または編集します。
- b) [ルールの追加 (Add Rule)] をクリックします。
- c) 次のプロパティを設定します。

- [NAT ルール (NAT Rule) ] = 自動 NAT ルール。
  - [タイプ (Type) ] = Static。
- d) [インターフェイスオブジェクト (Interface Objects) ] で、次の項目を設定します。
- [送信元インターフェイス オブジェクト (Source Interface Objects) ] = outside。
  - [宛先インターフェイス オブジェクト (Destination Interface Objects) ] = inside。
- e) [変換 (Translation) ] で、次の項目を設定します。
- [元の発信元 (Original Source) ] = ftp\_server ネットワーク オブジェクト。
  - [変換された送信元 (Translated Source) ] > [アドレス (Address) ] = ftp\_server\_translated ネットワークオブジェクト。
- f) [詳細 (Advanced) ] 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。

## Add NAT Rule

NAT Rule:

Type:

Enable

Interface Objects   **Translation**   PAT Pool   Advanced

Original Packet	Translated Packet
Original Source:*	Translated Source:
<input type="text" value="ftp_server"/> +	<input type="text" value="Address"/> +
Original Port:	Translated Port:
<input type="text" value="TCP"/>	<input type="text" value="ftp_server_translated"/>
<input type="text"/>	<input type="text"/>

- g) [OK] をクリックします。

## Threat Defense NAT の履歴

機能	最小 Management Center	最小 Threat Defense	詳細
NAT ルールの編集時にネットワークグループを作成します。	7.4.1	任意 (Any)	NAT ルールの編集時に、ネットワークオブジェクトに加えてネットワークグループを作成できます。 この機能は、バージョン 7.3.x または 7.4.0 ではサポートされていません。
一度に複数の NAT ルールの有効化、無効化、削除が可能。	7.2	いずれか	複数の NAT ルールを選択して、すべてを同時に有効化、無効化、または削除できます。有効化および無効化の対象は手動 NAT ルールのみです。削除はすべての NAT ルールが対象になります。
変換後の宛先としての完全修飾ドメイン名 (FQDN) オブジェクトの手動 NAT サポート。	7.1	任意 (Any)	www.example.com を指定する FQDN ネットワークオブジェクトを、手動 NAT ルールの変換後の宛先アドレスとして使用できます。システムでは、DNS サーバーから返された IP アドレスに基づいてルールが設定されます。

機能	最小 Management Center	最小 Threat Defense	詳細
<p>クラスタリングでの PAT アドレス割り当ての変更。PAT プールの [フラットなポート範囲 (Flat Port Range) ] オプションがデフォルトで有効になり、設定できなくなりました。</p>	6.7	任意 (Any)	<p>PAT アドレスがクラスタのメンバーに配布される方法が変更されま す。以前は、アドレスはクラスタのメンバーに配布されていたため、 PAT プールにはクラスタメンバーごとに少なくとも 1 つのアドレスが 必要でした。制御ユニットは各 PAT プールアドレスを等しいサイズの ポートブロックに分割し、それらをクラスタメンバーに配布するよう になりました。各メンバーには、同じ PAT アドレスのポートブロック があります。したがって、通常 PAT に必要な接続量に応じて、PAT プールのサイズを 1 つの IP アドレスにまで減らすことができます。 ポートブロックは、1024 ～ 65535 の範囲で 512 ポートのブロック単位 で割り当てられます。オプションで、PAT プールルールを設定する ときに、このブロック割り当てに予約ポート 1 ～ 1023 を含めること ができます。たとえば、単一ノードでは PAT プール IP アドレスあたり 65535 個の接続すべてを処理するのに対し、4 ノードクラスタでは、 各ノードは 32 個のブロックを取得し、PAT プール IP アドレスあたり 16384 個の接続を処理できます。</p> <p>この変更の一環として、スタンドアロンまたはクラスタ内での動作に 関わりなく、すべてのシステムの PAT プールは、フラットなポート範 囲 1023 ～ 65535 を使用できるようになりました。以前は、[フラット なポート範囲 (Flat Port Range) ] オプションを PAT プールルールに含 めることで、フラットな範囲をオプションで使用できました。[フラット なポート範囲 (Flat Port Range) ] オプションは無視され、PAT プール は常にフラットになります。必要に応じて [予約済みポートを含める (Include Reserved Ports) ] オプションを選択して、PAT プールに 1 ～ 1023 のポート範囲を含めることができます。</p> <p>ポートブロック割り当てを設定する ([ブロック割り当て (Block Allocation) ] PAT プールオプション) と、デフォルトの 512 ポートブ ロックではなく、独自のブロック割り当てサイズが使用されます。ま た、クラスタ内のシステムの PAT プールに拡張 PAT を設定すること はできません。</p>
<p>Threat Defense NAT ルールテーブルを検索 およびフィルタリング する機能。</p>	6.7	任意 (Any)	<p>Threat Defense NAT ポリシーでルールを検索して、IP アドレス、ポー ト、オブジェクト名などに基づいてルールを検索できるようになりま した。検索結果には部分一致が含まれます。条件で検索すると、ルー ルテーブルがフィルタリングされ、一致するルールのみが表示されま す。</p> <p>Threat Defense NAT ポリシーを編集するときに、ルールテーブルの上 に検索フィールドが追加されました。</p>

機能	最小 Management Center	最小 Threat Defense	詳細
キャリアグレード NAT の拡張機能。	6.5	任意 (Any)	<p>キャリア グレードまたは大規模 PAT では、NAT に 1 度に 1 つのポート変換を割り当てさせるのではなく、各ホストにポートのブロックを割り当てることができます (RFC 6888 を参照してください)。</p> <p>新規/変更された画面 : [ブロック割り当て (Block Allocation) ] オプションを Threat Defense の NAT ルールの [NAT PAT プール (NAT PAT Pool) ] タブに追加しました。</p>
Threat Defense の NAT のネットワーク範囲のオブジェクトのサポート。	6.1.0	いずれか	Threat Defense NAT ルール内のネットワーク範囲のオブジェクトを必要に応じて使用できるようになりました。
Threat Defense のネットワークアドレス変換 (NAT) 。	6.0.1	いずれか	<p>Threat Defense の NAT ポリシーが追加されました。</p> <p>新規/変更された画面 : Threat Defense が NAT ポリシーのタイプとして [デバイス (Devices) ] &gt; [NAT] ページに追加されました。</p>



## 翻訳について

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