



Network Address Translation (NAT)

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

- [NAT を使用する理由 \(1 ページ\)](#)
- [NAT の基本 \(2 ページ\)](#)
- [NAT のガイドライン \(10 ページ\)](#)
- [NAT の設定 \(17 ページ\)](#)
- [IPv6 ネットワークの変換 \(51 ページ\)](#)
- [NAT のモニタリング \(67 ページ\)](#)
- [NAT の例 \(67 ページ\)](#)

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

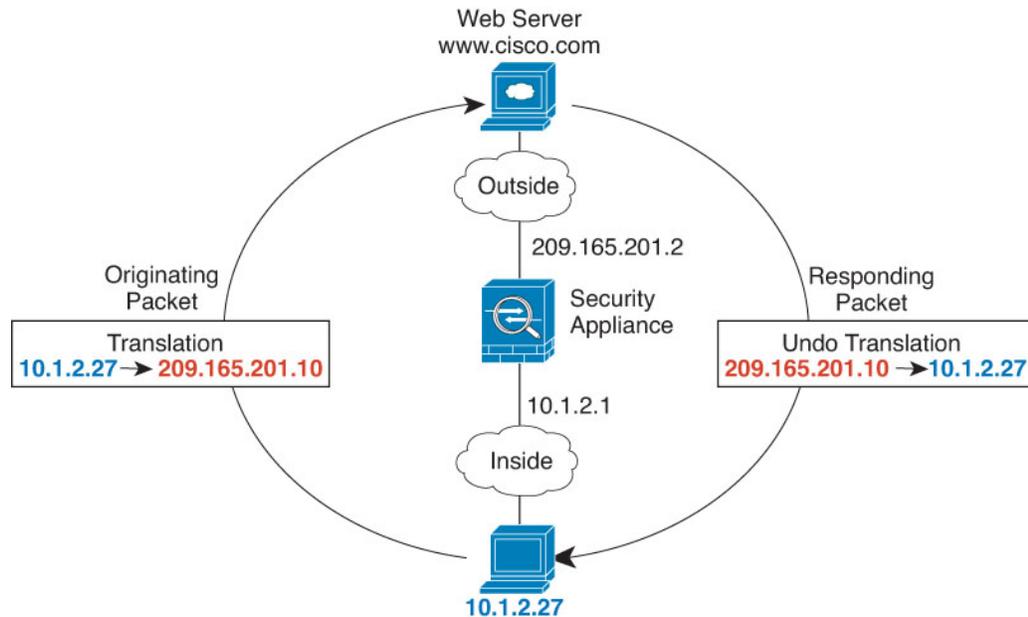
NAT は、次の方法を使用して実装できます。

- **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 \(18 ページ\)](#) を参照してください。
- **ダイナミック ポートアドレス変換 (PAT)** : 実際の IP アドレスのグループが、1 つの IP アドレスにマッピングされます。この IP アドレスの一意の送信元ポートが使用されます。[ダイナミック PAT \(24 ページ\)](#) を参照してください。
- **スタティック NAT** : 実際の IP アドレスとマッピング IP アドレスとの間での一貫したマッピング。双方向にトラフィックを開始できます。[スタティック NAT \(30 ページ\)](#) を参照してください。
- **アイデンティティ NAT** : 実際のアドレスが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 \(40 ページ\)](#) を参照してください。

ルーテッドモードの NAT

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

図 1: NAT の例 : ルーテッド モード



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

自動 NAT および 手動 NAT

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

手動 NAT の追加機能を必要としない場合は、自動 NAT を使用することをお勧めします。自動 NAT の設定が容易で、Voice over IP (VoIP) などのアプリケーションでは信頼性が高い場合があります (VoIP では、ルールで使用され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、最初的一致ベースで適用されます。最初的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"> • 静的ルールは動的ルールの前に配置する必要があります。 • 宛先変換を含むルールは、送信元変換のみのルールの前に配置する必要があります。 <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>
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"> 1. スタティック ルール 2. ダイナミック ルール <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"> 1. 実際の IP アドレスの数量：小から大の順。たとえば、アドレスが 1 個のオブジェクトは、アドレスが 10 個のオブジェクトよりも先に評価されます。 2. 数量が同じ場合には、IP アドレス番号（最小から最大まで）が使用されます。たとえば、10.1.1.0 は、11.1.1.0 よりも先に評価されます。 3. 同じ IP アドレスが使用される場合、ネットワークオブジェクトの名前がアルファベット順で使用されます。たとえば、abracadabra は catwoman よりも先に評価されます。

テーブルのセクション	ルールタイプ	セクション内のルールの順序
セクション 3	手動 NAT	まだ一致が見つからない場合、セクション 3 のルールがコンフィギュレーションに登場する順に、最初の一致ベースで適用されます。このセクションには、最も一般的なルールを含める必要があります。このセクションにおいても、一般的なルールの前に固有のルールが来るようにする必要があります。そうしない場合、一般的なルールが適用されます。

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

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

この結果、使用される順序は次のとおりです。

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

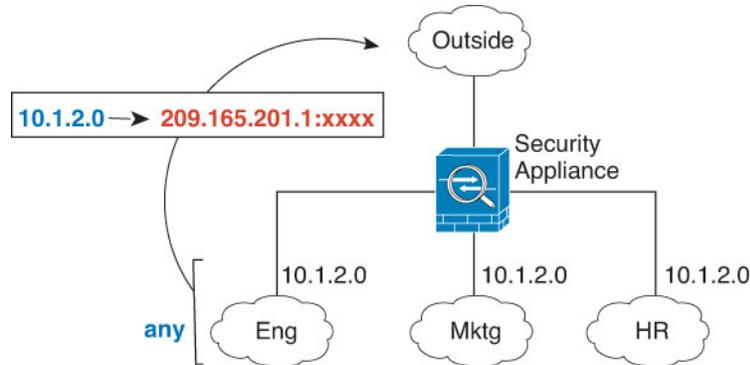
NAT インターフェイス

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

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

任意のインターフェイスを指定し、マッピングアドレスには `outside` インターフェイスを指定します。

図 2: 任意のインターフェイスの指定



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

パッシブインターフェイスでは NAT を設定できません。

NAT のルーティング設定

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

パケットを送信する際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。

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。

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 のガイドライン

ここでは、NAT を実装するためのガイドラインについて詳細に説明します。

インターフェイスのガイドライン

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

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

- ブリッジグループのメンバーに 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インターフェイス間で NAT を行う場合、送信元インターフェイスと宛先インターフェイスを指定する必要があります。インターフェイスとして「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、宛先インターフェイスがブリッジグループのメンバー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。

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、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、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、サブフィックスの 0s が IPv4 アドレスの後に追加されます。
- NAT64 (IPv6-to-IPv4) : IPv6 アドレスの数に対応できる十分な数の IPv4 アドレスがない場合があります。大量の IPv4 変換を提供するためにダイナミック PAT プールを使用することを推奨します。

インスペクション対象プロトコルに対する NAT サポート

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

- ピンホールの作成 : 一部のアプリケーションプロトコルは、標準ポートまたはネゴシエートされたポートでセカンダリ TCP または UDP 接続を開きます。インスペクションでは、これらのセカンダリポートのピンホールが開くため、ユーザ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する NAT 変換がある場合、インスペクションエンジンは、埋め込まれたアドレスおよびポートの NAT 変換を反映するようにパケットデータを書き換えます。セカンダリ接続は NAT の書き換えがないと動作しません。
- プロトコルの強制 : 一部のインスペクションでは、インスペクション対象プロトコルにある程度の RFC への準拠が強制されます。

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



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

表 2: NAT のサポート対象アプリケーションインスペクション

アプリケーション	インスペクション対象 プロトコル、ポート	NAT に関する制限事項	作成済みのピンホール
DCERPC	TCP/135	NAT64 なし。	対応
Diameter	TCP/3868 TCP/5868 (TCP/TLS 用) SCTP/3868	NAT/PAT 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	制限なし。	対応
GTP	UDP/3386 (GTPv0) UDP/2123 (GTPv1+)	拡張 PAT はサポートされません。 NAT は使用できません。	—
H.323 H.225 (コール シグナリング) H.323 RAS	TCP/1720 UDP/1718 RAS の場合、 UDP/1718 ~ 1719	NAT64 なし。	対応
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
M3UA	SCTP/2905	埋め込まれたアドレスに対する NAT または PAT はなし。	—
NetBIOS Name Server over IP	UDP/137、138 (送信元 ポート)	NAT64 なし。	非対応
RSH	TCP/514	PAT なし。 NAT64 なし。	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
RTSP	TCP/554 (HTTP クローキング は処理しません)	NAT64 なし。	対応
SIP	TCP/5060 UDP/5060	拡張 PAT なし NAT64 または NAT46 なし	対応
Skinny (SCCP)	TCP/2000	NAT64、NAT46、または NAT66 なし	対応
SQL*Net (バージョン 1、2)	TCP/1521	NAT64 なし。	対応
SCTP	SCTP	SCTP トラフィックでスタティック ネットワーク オブジェクト NAT を実行できますが (ダイナミック NAT/PAT なし)、インスペクション エンジン は NAT には使用されません。	非対応
Sun RPC	TCP/111 UDP/111	NAT64 なし。	対応
TFTP	UDP/69	NAT64 なし。 ペイロード IP アドレスは変換されません。	対応
XDMCP	UDP/177	NAT64 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。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、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」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。
 - (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。
- 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しないでください。
- Protocol Independent Multicast (PIM) レジスタの内部ペイロードで NAT を使用することはできません。
- (手動 NAT) デュアル ISP インターフェイス セットアップ (ルーティング設定でサービスレベルアグリーメントを使用するプライマリインターフェイスとバックアップインターフェイス) の NAT ルールを作成する場合は、ルールで宛先基準を指定しないでください。プライマリインターフェイスのルールがバックアップインターフェイスのルールよりも前にあることを確認してください。これにより、デバイスは、プライマリ ISP が利用できない場合に、現在のルーティング状態に基づいて正しい NAT 宛先インターフェイスを選択できます。宛先オブジェクトを指定すると、NAT ルールは、指定しない場合には重複するルールのプライマリインターフェイスを常に選択します。
- インターフェイスに定義された NAT ルールと一致しないトラフィックについて ASP ドロップ理由 `nat-no-xlate-to-pat-pool` が示される場合は、影響を受けるトラフィックのアイデンティティ NAT ルールを設定して、トラフィックが変換されずに通過できるようにします。
- GRE トンネルエンドポイントの NAT を設定する場合は、エンドポイントでキープアライブを無効にする必要があります。無効にしないと、トンネルを確立できません。エンドポイントは、キープアライブを元のアドレスに送信します。

NAT の設定

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

手順

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

ステップ 2 必要なルールを決定します。

ダイナミック NAT ルール、ダイナミック PAT ルール、スタティック NAT ルール、およびアイデンティティ NAT ルールを作成できます。概要については、「[NAT タイプ \(3 ページ\)](#)」を参照してください。

ステップ 3 手動 NAT または自動 NAT として実装するルールを決定します。

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

ステップ 4 次の項で説明するルールを作成します。

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

ステップ 5 NAT ポリシーとルールを管理します。

ポリシーとそのルールを管理するには、次のことを行います。

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

ダイナミック NAT

ここでは、ダイナミック NAT とその設定方法について説明します。

ダイナミック NAT について

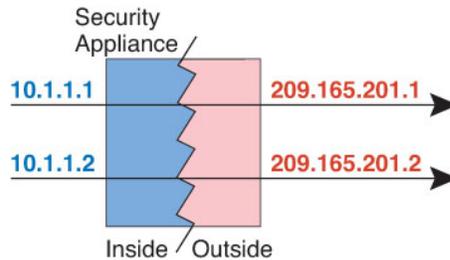
ダイナミック NAT では、実際のアドレスのグループは、宛先ネットワーク上でルーティング可能なマッピングアドレスのプールに変換されます。マッピングされたプールにあるアドレスは、通常、実際のグループより少なくなります。変換対象のホストが宛先ネットワークにアクセスすると、NAT は、マッピングされたプールから IP アドレスをそのホストに割り当てます。変換は、実際のホストが接続を開始したときにだけ作成されます。変換は接続が継続している間だけ有効であり、変換がタイムアウトすると、そのユーザは同じ IP アドレスを保持しません。したがって、アクセスルールでその接続が許可されている場合でも、宛先ネットワ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



- (注) 変換が継続している間、アクセスルールで許可されていれば、リモートホストは変換済みホストへの接続を開始できます。アドレスは予測不可能であるため、ホストへの接続は確立されません。ただし、この場合は、アクセスルールのセキュリティに依存できます。

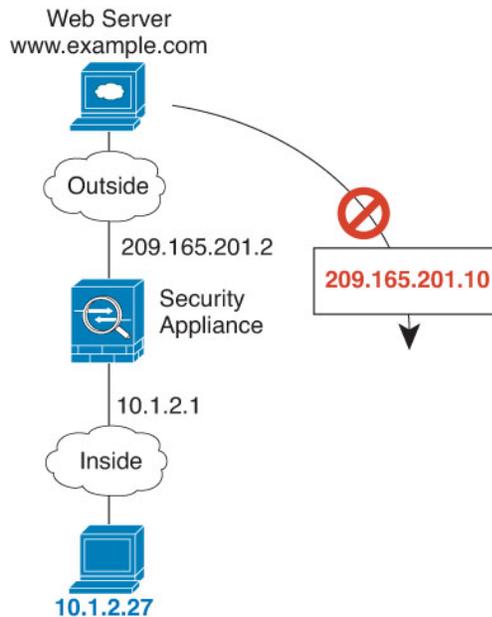
次の図に、一般的なダイナミック NAT のシナリオを示します。実際のホストだけが NAT セッションを作成でき、応答トラフィックが許可されます。

図 3: ダイナミック NAT



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

図 4: マッピングアドレスへの接続開始を試みているリモートホスト



ダイナミック NAT の欠点と利点

ダイナミック NAT には、次の欠点があります。

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

PAT では、1つのアドレスのポートを使用して 64,000 を超える変換を処理できるため、このイベントが頻繁に発生する場合は、PAT または PAT のフォールバック方式を使用します。

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

ダイナミック NAT の利点は、一部のプロトコルが PAT を使用できないということです。たとえば、PAT は次の場合は機能しません。

- GRE バージョン 0 などのように、オーバーロードするためのポートがない IP プロトコルでは機能しません。
- 一部のマルチメディアアプリケーションなどのように、1つのポート上にデータストリームを持ち、別のポート上に制御パスを持ち、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)] を選択し、ルールに必要なネットワーク オブジェクトまたはグループを作成します。または、NAT ルールを定義し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。

- [元のアドレス (Original Address)] : ネットワーク オブジェクト (グループではなく) する必要があります。ホスト、範囲、またはサブネットのいずれかを使用できます。
- [変換済みアドレス (Translated Address)] : ネットワーク オブジェクトまたはグループを指定できますが、サブネットを含めることはできません。グループに IPv4 アドレスと IPv6 アドレスの両方を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 [ポリシー (Policies)] > [NAT] を選択します。

ステップ 2 次のいずれかを実行します。

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

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

ステップ 3 基本的なルール オプションを設定します。

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

ステップ 4 次のパケット変換オプションを設定します。

- [送信元インターフェイス (Source Interface)]、[宛先インターフェイス (Destination Interface)]: (ブリッジグループメンバーインターフェイスに必須) この NAT ルールが適用されるインターフェイス。[送信元 (Source)]は実際のインターフェイスで、このインターフェイスを経由してトラフィックはデバイスに入ります。[宛先 (Destination)]はマッピングされたインターフェイスで、このインターフェイスを経由してトラフィックはデバイスから出ます。デフォルトでは、ルールはブリッジグループメンバ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。
- [元のアドレス (Original Address)]: 変換するアドレスを含むネットワークオブジェクト。
- [変換済みアドレス (Translated Address)]: マッピングアドレスを含むネットワークオブジェクトまたはグループ。

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

- [このルールに一致する DNS 応答を変換 (Translate DNS replies that match this rule)]: DNS 応答の IP アドレスを変換するかどうかを指定します。マッピングインターフェイスから実際のインターフェイスに移動する DNS 応答の場合、アドレス (IPv4 A または IPv6 AAAA) レコードはマッピングされた値から実際の値に書き換えられます。反対に、実際のインターフェイスからマッピング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 \(88 ページ\)](#)」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。

ステップ 6 [OK] をクリックします。

ダイナミック手動 NAT の設定

自動 NAT では要件を満たせない場合は、ダイナミック手動 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)]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。

- [元の送信元アドレス (Original Source Address)]: ネットワーク オブジェクトまたはグループを指定できます。ホスト、範囲、またはサブネットを含めることができます。すべての元の送信元トラフィックを変換する場合、この手順をスキップし、ルールで [すべて (Any)] を指定します。
- [変換済み送信元アドレス (Translated Source Address)]: ネットワーク オブジェクトまたはグループを指定できますが、サブネットを含めることはできません。グループに IPv4 アドレスと IPv6 アドレスの両方を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。

ルールで各アドレスのスタティック変換を設定すると、[元の宛先アドレス (Original Destination Address)] および [変換済み宛先アドレス (Translated Destination Address)] のネットワーク オブジェクトを作成できます。

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

手順

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

ステップ 2 次のいずれかを実行します。

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

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

ステップ 3 基本的なルール オプションを設定します。

- [タイトル (Title)]: ルールの名前を入力します。
- [ルールの作成対象 (Create Rule For)]: [手動 NAT (Manual NAT)] を選択します。
- [ルールの配置 (Rule Placement)]: Where you want to add the rule. ルールはカテゴリ内 (自動 NAT のルールの前後)、または選択するルールの上下に挿入できます。
- [タイプ (Type)]: [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。

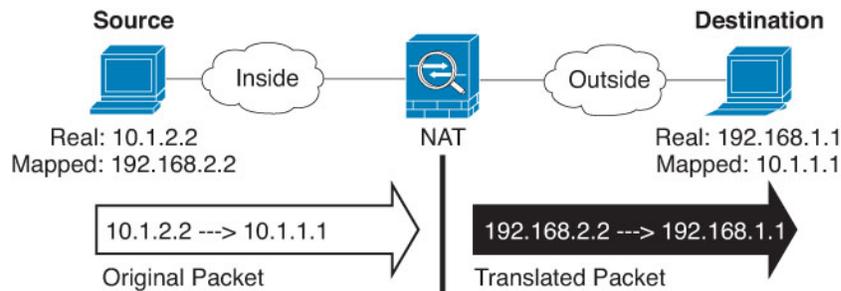
ステップ 4 次のインターフェイス オプションを設定します。

- [送信元インターフェイス (Source Interface)]、[宛先インターフェイス (Destination Interface)]: (ブリッジグループ メンバー インターフェイスに必須) この NAT ルールが

適用されるインターフェイス。[送信元 (Source)] は実際のインターフェイスで、このインターフェイスを経由してトラフィックはデバイスに入ります。[宛先 (Destination)] はマッピングされたインターフェイスで、このインターフェイスを経由してトラフィックはデバイスから出ます。デフォルトでは、ルールはブリッジグループメンバ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。



- [Original Source][Address] : 変換するアドレスを含むネットワークオブジェクト、またはネットワークグループ。
- [Original Destination][Address] : (オプション)。宛先アドレスを含むネットワークオブジェクト。空白のままにすると、宛先に関係なく、送信元アドレス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 (Interface)] を選択して、送信元インターフェイスの元の宛先 ([すべて (Any)] は選択不可) をベースにできます。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。

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

ステップ 7 (オプション) サービス変換の宛先サービスポートを特定します。[元の宛先ポート (Original Destination Port)]、[変換済み宛先ポート (Translated Destination Port)]。

ダイナミック NAT はポート変換をサポートしていないため、[元の送信元ポート (Original Source Port)] フィールドと [変換済み送信元ポート (Translated Source Port)] フィールドは空白のままにする必要があります。ただし、宛先変換は常にスタティックであるため、宛先ポートに対してポート変換を実行できます。

NAT では、TCP または UDP のみがサポートされます。ポートを変換する場合、実際のサービス オブジェクトのプロトコルとマッピング サービス オブジェクトのプロトコルの両方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) [詳細オプション (Advanced Options)] リンクをクリックし、目的のオプションを選択します。

- [このルールに一致する DNS 応答を変換 (Translate DNS replies that match this rule)] : DNS 応答の IP アドレスを変換するかどうかを指定します。マッピングインターフェイスから実際のインターフェイスに移動する DNS 応答の場合、アドレス (IPv4 A または IPv6 AAAA) レコードはマッピングされた値から実際の値に書き換えられます。反対に、実際のインターフェイスからマッピング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 \(88 ページ\)](#)」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。

ステップ 9 [OK] をクリックします。

ダイナミック PAT

次のトピックでは、ダイナミック PAT について説明します。

ダイナミック PAT について

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

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 5: ダイナミック PAT



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

接続の有効期限が切れると、ポート変換も有効期限切れになります。



- (注) インターフェイスごとに異なる PAT プールを使用することをお勧めします。複数のインターフェイス、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。ただし、インターフェイス上の IPv6 アドレスに対しインターフェイス PAT を使用することはできません。

同じブリッジグループ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、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 \(12 ページ\)](#) を参照してください。

ダイナミック PAT によって、単一の IP アドレスから送信されたように見える数多くの接続が作成されることがあります。この場合、このトラフィックはサーバーで DoS 攻撃として解釈される可能性があります。

ダイナミック自動 PAT の設定

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

始める前に

[オブジェクト (Objects)] を選択し、ルールに必要なネットワークオブジェクトまたはグループを作成します。または、NAT ルールを定義し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。

- [元のアドレス (Original Address)] : ネットワーク オブジェクト (グループではなく) にする必要があります。ホスト、範囲、またはサブネットのいずれかを使用できます。
- [変換済みアドレス (Translated Address)] : PAT アドレスを指定するオプションは次のとおりです。
 - [宛先インターフェイス (Destination Interface)] : 宛先インターフェイスの IPv4 アドレスを使用する場合、ネットワークオブジェクトは必要ありません。インターフェイス PAT は IPv6 には使用できません。
 - [単一の PAT アドレス (Single PAT address)] : 単一のホストを含むネットワーク オブジェクトを作成します。

手順

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

ステップ 2 次のいずれかを実行します。

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

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

ステップ 3 基本的なルール オプションを設定します。

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

ステップ 4 次のパケット変換オプションを設定します。

- [送信元インターフェイス (Source Interface)]、[宛先インターフェイス (Destination Interface)] : (ブリッジグループメンバーインターフェイスに必須) この NAT ルールが適用されるインターフェイス。[送信元 (Source)] は実際のインターフェイスで、このインターフェイスを経由してトラフィックはデバイスに入ります。[宛先 (Destination)] はマッピングされたインターフェイスで、このインターフェイスを経由してトラフィックはデバイスから出ます。デフォルトでは、ルールはブリッジグループメンバ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。
- [元のアドレス (Original Address)] : 変換するアドレスを含むネットワーク オブジェクト。
- [変換済みアドレス (Translated Address)] : 次のいずれかになります。

- (インターフェイス PAT) 宛先の IPv4 アドレスのインターフェイスを使用するには、[インターフェイス (Interface)] を選択します。また、ブリッジグループメンバーインターフェイスではない特定の宛先インターフェイスを選択する必要があります。IPv6 にインターフェイス PAT は使用できません。
- 宛先インターフェイスのアドレス以外の単一アドレスを使用する場合は、そのために作成したホスト ネットワーク オブジェクトを選択します。

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

- [インターフェイス PAT へのフォールスルー (Fallthrough to Interface PAT)] (宛先インターフェイス) : 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。すでにインターフェイス PAT を変換済みアドレスとして設定している場合には、このオプションは使用できません。このオプションは、IPv6 ネットワークで使用することもできません。

ステップ 6 [OK] をクリックします。

ダイナミック手動 PAT の設定

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。単一のアドレス (宛先インターフェイスのアドレスや別のアドレス) に変換できます。

始める前に

[オブジェクト (Objects)] を選択して、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。

- [元の送信元アドレス (Original Source Address)] : ネットワーク オブジェクトまたはグループを指定できます。ホスト、範囲、またはサブネットを含めることができます。すべての元の送信元トラフィックを変換する場合、この手順をスキップし、ルールで [すべて (Any)] を指定します。
- [変換済み送信元アドレス (Translated Source Address)] : PAT アドレスを指定するオプションは次のとおりです。

- [宛先インターフェイス (Destination Interface)] : 宛先インターフェイスの IPv4 アドレスを使用する場合、ネットワーク オブジェクトは必要ありません。インターフェイス PAT は IPv6 には使用できません。
- [単一の PAT アドレス (Single PAT address)] : 単一のホストを含むネットワーク オブジェクトを作成します。

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

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

手順

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

ステップ 2 次のいずれかを実行します。

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

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

ステップ 3 基本的なルール オプションを設定します。

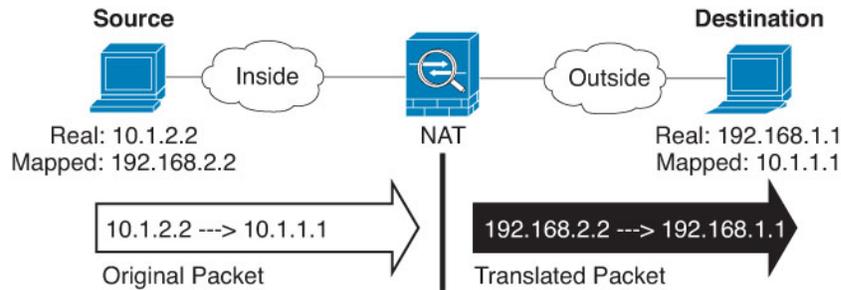
- [タイトル (Title)] : ルールの名前を入力します。
- [ルールの作成対象 (Create Rule For)] : [手動 NAT (Manual NAT)] を選択します。
- [ルールの配置 (Rule Placement)] : Where you want to add the rule. ルールはカテゴリ内 (自動 NAT のルールの前後) 、または選択するルールの上に挿入できます。
- [タイプ (Type)] : [ダイナミック (Dynamic)] を選択します。この設定は送信元アドレスにのみ適用されます。宛先アドレスの変換を定義している場合、変換は常に静的に行われます。

ステップ 4 次のインターフェイス オプションを設定します。

- [送信元インターフェイス (Source Interface)]、[宛先インターフェイス (Destination Interface)] : (ブリッジグループメンバーインターフェイスに必須) この NAT ルールが適用されるインターフェイス。[送信元 (Source)] は実際のインターフェイスで、このインターフェイスを経由してトラフィックはデバイスに入ります。[宛先 (Destination)] はマッピングされたインターフェイスで、このインターフェイスを経由してトラフィックはデバイスから出ます。デフォルトでは、ルールはブリッジグループメンバ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 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)。宛先アドレスを含むネットワークオブジェクト。空白のままにすると、宛先に関係なく、送信元アドレスの変換が適用されます。宛先アドレスを指定した場合、そのアドレスにスタティック変換を設定するか、単にアイデンティティ NAT を使用できます。

[**インターフェイス (Interface)**] を選択して、送信元インターフェイスの元の宛先 ([すべて (Any)] は選択不可) をベースにできます。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。

- [変換済み送信元アドレス (Translated Source Address)] : 次のいずれかになります。
 - (インターフェイス PAT) 宛先の IPv4 アドレスのインターフェイスを使用するには、[インターフェイス (Interface)] を選択します。また、ブリッジグループメンバーインターフェイスではない特定の宛先インターフェイスを選択する必要があります。IPv6 にインターフェイス PAT は使用できません。
 - 宛先インターフェイスのアドレス以外の単一アドレスを使用する場合は、そのために作成したホスト ネットワーク オブジェクトを選択します。
- [変換済み宛先アドレス (Translated Destination Address)] : (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) [詳細オプション (Advanced Options)] リンクをクリックし、目的のオプションを選択します。

- [インターフェイス PAT へのフォールスルー (Fallthrough to Interface PAT)] (宛先インターフェイス) : 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。すでにインターフェイス PAT を変換済みアドレスとして設定している場合には、このオプションは使用できません。このオプションは、IPv6 ネットワークで使用することもできません。

ステップ 9 [OK] をクリックします。

スタティック NAT

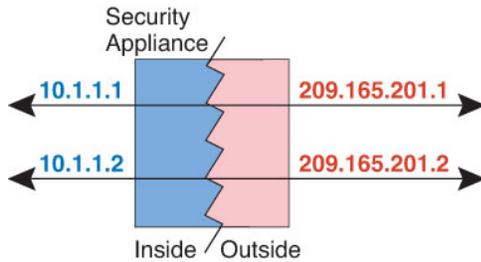
ここでは、スタティック NAT とその実装方法について説明します。

スタティック NAT について

スタティック NAT では、実際のアドレスからマッピング アドレスへの固定変換が作成されます。マッピング アドレスは連続する各接続で同じであるため、スタティック NAT では、双方向の接続 (ホストへの接続とホストから接続の両方) を開始できます (接続を許可するアクセスルールが存在する場合)。一方、ダイナミック NAT および PAT では、各ホストが以降の各変換に対して異なるアドレスまたはポートを使用するため、双方向の開始はサポートされません。

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

図 6:スタティック NAT



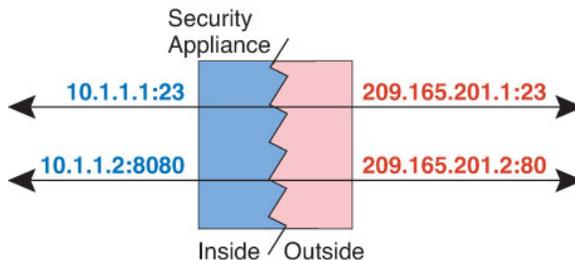
ポート変換を設定したスタティック NAT

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

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

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

図 7:ポート変換を設定したスタティック NAT の一般的なシナリオ



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、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

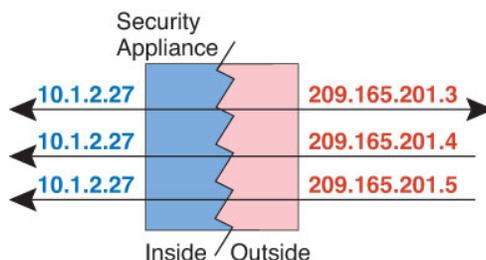
スタティック NAT は、実際のアドレスをインターフェイスアドレスとポートの組み合わせにマッピングするように設定できます。たとえば、デバイスの外部インターフェイスへの Telnet アクセスを内部ホストにリダイレクトする場合、内部ホストの IP アドレス/ポート 23 を外部インターフェイス アドレス/ポート 23 にマッピングできます。

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。

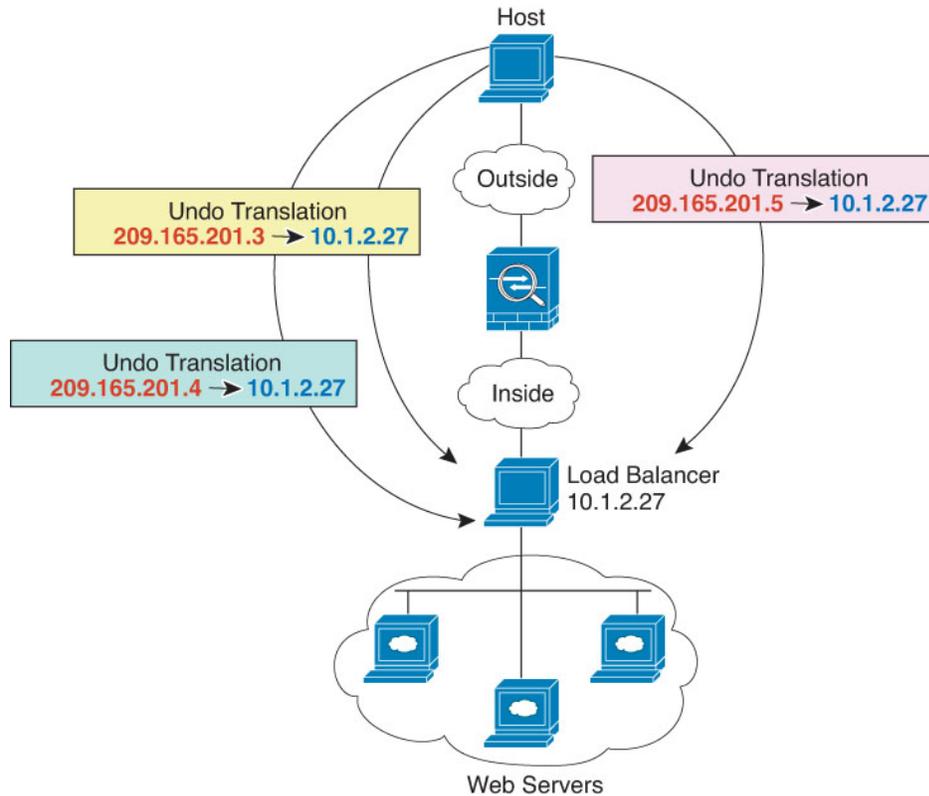
次の図に、一般的な 1 対多のスタティック NAT シナリオを示します。実際のホストが開始すると、常に最初のマッピングアドレスが使用されるため、実際のホスト IP/最初のマッピング IP の変換は、理論的には双方向変換のみが行われます。

図 8: 1 対多のスタティック NAT



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

図 9:1 対多のスタティック NAT の例



他のマッピングシナリオ (非推奨)

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

機能的には、少対多は1対多と同じです。ただし、設定が複雑になり、実際のマッピングがひと目で明らかにならない可能性があるため、必要とする実際の各アドレスに対して1対多の設定を作成することをお勧めします。たとえば、少対多のシナリオでは、少数の実際のアドレスが多数のマッピングアドレスに順番にマッピングされます (Aは1、Bは2、Cは3)。すべての実際のアドレスがマッピングされたら、次のマッピングアドレスが最初の実際のアドレスにマッピングされ、すべてのマッピングアドレスがマッピングされるまで続行されます (Aは4、Bは5、Cは6)。この結果、実際の各アドレスに対して複数のマッピングアドレスが存在することになります。1対多の設定のように、最初のマッピングだけが双方向であり、以降のマッピングでは、実際のホストへのトラフィックを開始できますが、実際のホストからのすべてのトラフィックは、送信元の最初のマッピングアドレスだけを使用できます。

次の図に、一般的な少対多のスタティック NAT シナリオを示します。

図 10: 少対多のスタティック NAT



多対少または多対1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中でマッピングを行ったときだけです。残りの上位の実際のアドレスはトラフィックを開始できますが、これらへのトラフィックを開始できません。接続のリターントラフィックは、接続の固有の5つの要素（送信元 IP、宛先 IP、送信元ポート、宛先ポート、プロトコル）によって適切な実際のアドレスに転送されます。



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

次の図に、一般的な多対少のスタティック NAT シナリオを示します。

図 11: 多対少のスタティック NAT



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

スタティック自動 NAT の設定

スタティック自動 NAT ルールを使用して、アドレスを宛先ネットワーク上でルーティング可能な別の IP アドレスに変換します。また、スタティック NAT ルールでポートの変換もできます。

始める前に

[オブジェクト (Objects)] を選択し、ルールに必要なネットワーク オブジェクトまたはグループを作成します。または、NAT ルールを定義し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。

- [元のアドレス (Original Address)] : ネットワーク オブジェクト (グループではなく) する必要があります。ホスト、範囲、またはサブネットのいずれかを使用できます。
- [変換済みアドレス (Translated Address)] : 変換済みアドレスを指定するには、次のオプションがあります。
 - [宛先インターフェイス (destination interface)] : 宛先インターフェイスの IPv4 アドレスを使用するには、ネットワーク オブジェクトは必要ありません。これはポート変換と共に、スタティック インターフェイス NAT を設定します。送信元アドレス/ポートは、インターフェイスのアドレス、および同じポート番号に変換されます。IPv6 にインターフェイス PAT は使用できません。
 - [アドレス (Address)] : ホスト、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 [ポリシー (Policies)] > [NAT] を選択します。

ステップ 2 次のいずれかを実行します。

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

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

ステップ 3 基本的なルール オプションを設定します。

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

ステップ 4 次のパケット変換オプションを設定します。

- [送信元インターフェイス (Source Interface)]、[宛先インターフェイス (Destination Interface)] : (ブリッジグループメンバーインターフェイスに必須) この NAT ルールが適用されるインターフェイス。[送信元 (Source)] は実際のインターフェイスで、このインターフェイスを経由してトラフィックはデバイスに入ります。[宛先 (Destination)] は

マッピングされたインターフェイスで、このインターフェイスを経由してトラフィックはデバイスから出ます。デフォルトでは、ルールはブリッジグループメンバ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。

- [元のアドレス (Original Address)] : 変換するアドレスを含むネットワーク オブジェクト。
- [変換済みアドレス (Translated Address)] : 次のいずれかになります。
 - アドレスの設定グループを使用するには、マッピングされたアドレスを含むネットワーク オブジェクトまたはグループを選択します。通常、1 対 1 のマッピングでは、実際のアドレスと同じ数のマッピングアドレスを設定します。しかし、アドレスの数が一致しない場合もあります。
 - (ポート変換を設定したスタティック インターフェイス NAT) 宛先インターフェイスの IP アドレスを使用するには、[インターフェイス (Interface)] を選択します。また、ブリッジグループ メンバー インターフェイスではない特定の宛先インターフェイスを選択する必要があります。IPv6 にインターフェイス PAT は使用できません。これはポート変換と共に、スタティック インターフェイス NAT を設定します。送信元アドレス/ポートは、インターフェイスのアドレス、および同じポート番号に変換されます。
- (オプション) [元のポート (Original Port)]、[Translated Port (変換済みポート)] : TCP または UDP ポートを変換する必要がある場合、元のポートと変換済みポートを定義するポート オブジェクトを選択します。オブジェクトは同じプロトコル用でなければなりません。そのオブジェクトがまだ存在しない場合、[新規オブジェクトの作成 (Create New Object)] をクリックします。たとえば、必要に応じて TCP/80 を TCP/8080 に変換できます。

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

- [このルールに一致する DNS 応答を変換 (Translate DNS replies that match this rule)] : DNS 応答の IP アドレスを変換するかどうかを指定します。マッピングインターフェイスから実際のインターフェイスに移動する DNS 応答の場合、アドレス (IPv4 A または IPv6 AAAA) レコードはマッピングされた値から実際の値に書き換えられます。反対に、実際のインターフェイスからマッピング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 \(88 ページ\)](#)」を参照してください。このオプションはポート変換を行う場合は使用できません。
- [宛先インターフェイスで ARP をプロキシしない (Do not proxy ARP on Destination Interface)] : マッピング IP アドレスへの着信パケットのプロキシ ARP を無効にします。マッピングインターフェイスと同じネットワーク上のアドレスを使用した場合、システムはプロキシ ARP を使用してマッピングアドレスのすべての ARP 要求に応答することで、マッピングアドレスを宛先とするトラフィックを代行受信します。この方法だと、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 6 [OK] をクリックします。

スタティック手動 NAT の設定

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

始める前に

[オブジェクト (Objects)] を選択して、ルールに必要なネットワーク オブジェクトまたはグループを作成します。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。

- [元の送信元アドレス (Original Source Address)] : ネットワーク オブジェクトまたはグループを指定できます。ホスト、範囲、またはサブネットを含めることができます。すべての元の送信元トラフィックを変換する場合、この手順をスキップし、ルールで [すべて (Any)] を指定します。
- [変換済み送信元アドレス (Translated Source Address)] : 変換済みアドレスを指定するには、次のオプションがあります。
 - [宛先インターフェイス (destination interface)] : 宛先インターフェイスの IPv4 アドレスを使用するには、ネットワーク オブジェクトは必要ありません。これはポート変換と共に、スタティック インターフェイス NAT を設定します。送信元アドレス/ポートは、インターフェイスのアドレス、および同じポート番号に変換されます。IPv6 にインターフェイス PAT は使用できません。
 - [アドレス (Address)] : ホスト、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。

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

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

手順

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

ステップ 2 次のいずれかを実行します。

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

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

ステップ 3 基本的なルール オプションを設定します。

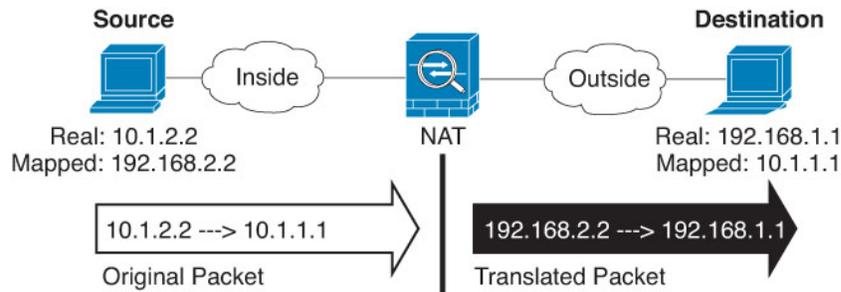
- [タイトル (Title)] : ルールの名前を入力します。
- [ルールの作成対象 (Create Rule For)] : [手動 NAT (Manual NAT)] を選択します。
- [ルールの配置 (Rule Placement)] : Where you want to add the rule. ルールはカテゴリ内 (自動 NAT のルールの前後)、または選択するルールの上に挿入できます。
- [タイプ (Type)] : [スタティック (Static)] を選択します。この設定は送信元アドレスにのみ適用されます。宛先アドレスの変換を定義している場合、変換は常に静的に行われます。

ステップ 4 次のインターフェイス オプションを設定します。

- [送信元インターフェイス (Source Interface)]、[宛先インターフェイス (Destination Interface)] : (ブリッジグループメンバーインターフェイスに必須) この NAT ルールが適用されるインターフェイス。[送信元 (Source)] は実際のインターフェイスで、このインターフェイスを経由してトラフィックはデバイスに入ります。[宛先 (Destination)] はマッピングされたインターフェイスで、このインターフェイスを経由してトラフィックはデバイスから出ます。デフォルトでは、ルールはブリッジグループメンバ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。



- [Original Source][Address] : 変換するアドレスを含むネットワークオブジェクト、またはネットワークグループ。
- [Original Destination][Address] : (オプション)。宛先アドレスを含むネットワークオブジェクト。空白のままにすると、宛先に関係なく、送信元アドレス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 (Interface)] を選択して、送信元インターフェイスの元の宛先 ([すべて (Any)] は選択不可) をベースにできます。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。

- [変換済み送信元アドレス (Translated Source Address)] : 次のいずれかになります。
 - アドレスの設定グループを使用するには、マッピングされたアドレスを含むネットワーク オブジェクトまたはグループを選択します。通常、1 対 1 のマッピングでは、実際のアドレスと同じ数のマッピングアドレスを設定します。しかし、アドレスの数が一致しない場合もあります。
 - (ポート変換を設定したスタティック インターフェイス NAT) 宛先の IPv4 アドレスのインターフェイスを使用するには、[インターフェイス (Interface)] を選択します。また、ブリッジグループメンバーインターフェイスではない特定の宛先インターフェイスを選択する必要があります。これはポート変換と共に、スタティック インターフェイス NAT を設定します。送信元アドレス/ポートは、インターフェイスのアドレス、および同じポート番号に変換されます。IPv6 にインターフェイス PAT は使用できません。
- [変換済み宛先アドレス (Translated Destination Address)] : (オプション) 変換されたパケットで使用される宛先アドレスを含むネットワーク オブジェクトまたはグループ。[元の宛先 (Original Destination)] を選択した場合、同じオブジェクトを選択することによって、アイデンティティ NAT (つまり変換なし) を設定できます。

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

ポート変換を設定したスタティック NAT を設定した場合、送信元、宛先、またはその両方のポートを変換できます。たとえば、TCP/80 と TCP/8080 間を変換できます。

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

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

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

- [このルールに一致する DNS 応答を変換 (Translate DNS replies that match this rule)] : DNS 応答の IP アドレスを変換するかどうかを指定します。マッピングインターフェイスから実際のインターフェイスに移動する DNS 応答の場合、アドレス (IPv4 A または IPv6 AAAA) レコードはマッピングされた値から実際の値に書き換えられます。反対に、実際のインターフェイスからマッピング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 \(88 ページ\)](#)」を参照してください。このオプションはポート変換を行う場合は使用できません。
- [宛先インターフェイスで ARP をプロキシしない (Do not proxy ARP on Destination Interface)] : マッピング IP アドレスへの着信パケットのプロキシ ARP を無効にします。マッピングインターフェイスと同じネットワーク上のアドレスを使用した場合、システムはプロキシ ARP を使用してマッピングアドレスのすべての ARP 要求に応答することで、マッピングアドレスを宛先とするトラフィックを代行受信します。この方法だと、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 9 [OK] をクリックします。

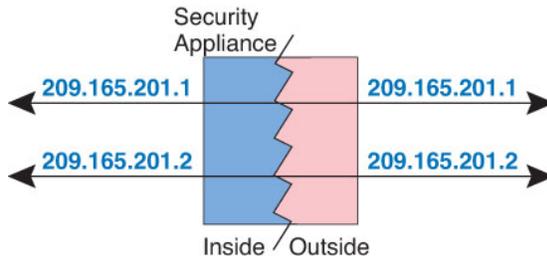
アイデンティティ NAT

IP アドレスを自身に変換する必要がある 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 12: アイデンティティ NAT



ここでは、アイデンティティ NAT の設定方法について説明します。

アイデンティティ自動 NAT の設定

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

始める前に

[オブジェクト (Objects)] を選択し、ルールに必要なネットワーク オブジェクトまたはグループを作成します。または、NAT ルールを定義し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。

- [元のアドレス (Original Address)] : ネットワーク オブジェクト (グループではなく) にする必要があります。ホスト、範囲、またはサブネットのいずれかを使用できます。
- [変換済みアドレス (Translated Address)] : 元の送信元オブジェクトとコンテンツがまったく同一のネットワーク オブジェクトまたはグループ。同じオブジェクトを使用できます。

手順

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

ステップ 2 次のいずれかを実行します。

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

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

ステップ 3 基本的なルール オプションを設定します。

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

ステップ 4 次のパケット変換オプションを設定します。

- [送信元インターフェイス (Source Interface)]、[宛先インターフェイス (Destination Interface)] : (ブリッジグループメンバーインターフェイスに必須) この NAT ルールが適用されるインターフェイス。[送信元 (Source)] は実際のインターフェイスで、このインターフェイスを経由してトラフィックはデバイスに入ります。[宛先 (Destination)] はマッピングされたインターフェイスで、このインターフェイスを経由してトラフィックはデバイスから出ます。デフォルトでは、ルールはブリッジグループメンバ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。
- [元のアドレス (Original Address)] : 変換するアドレスを含むネットワーク オブジェクト。
- [変換済みアドレス (Translated Address)] : 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 5 (オプション) [詳細オプション (Advanced Options)] リンクをクリックし、目的のオプションを選択します。

- [このルールと一致する DNS 応答を変換 (Translate DNS replies that match this rule)] : アイデンティティ NAT には、このオプションを設定しないでください。
- [宛先インターフェイスで ARP をプロキシしない (Do not proxy ARP on Destination Interface)] : マッピング IP アドレスへの着信パケットのプロキシ ARP を無効にします。マッピングインターフェイスと同じネットワーク上のアドレスを使用した場合、システムはプロキシ ARP を使用してマッピングアドレスのすべての ARP 要求に応答することで、マッピングアドレスを宛先とするトラフィックを代行受信します。この方法だと、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 6 [OK] をクリックします。

アイデンティティ手動 NAT の設定

自動 NAT がお客様のニーズを満たしていない場合は、スタティック アイデンティティ手動 NAT ルールを使用します。たとえば、宛先に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)] 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。

- [元の送信元アドレス (Original Source Address)] : ネットワーク オブジェクトまたはグループを指定できます。ホスト、範囲、またはサブネットを含めることができます。すべての元の送信元トラフィックを変換する場合、この手順をスキップし、ルールで [すべて (Any)] を指定します。
- [変換済み送信元アドレス (Translated Source Address)] : 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。

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

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

手順

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

ステップ 2 次のいずれかを実行します。

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

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

ステップ 3 基本的なルール オプションを設定します。

- [タイトル (Title)] : ルールの名前を入力します。

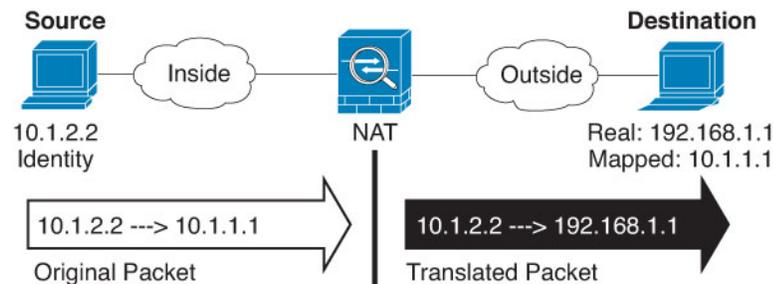
- [ルール作成対象 (Create Rule For)] : [手動 NAT (Manual NAT)] を選択します。
- [ルールの配置 (Rule Placement)] : Where you want to add the rule. ルールはカテゴリ内 (自動 NAT のルールの前後)、または選択するルールの上下に挿入できます。
- [タイプ (Type)] : [スタティック (Static)] を選択します。この設定は送信元アドレスにのみ適用されます。宛先アドレスの変換を定義している場合、変換は常に静的に行われます。

ステップ 4 次のインターフェイス オプションを設定します。

- [送信元インターフェイス (Source Interface)]、[宛先インターフェイス (Destination Interface)] : (ブリッジグループメンバーインターフェイスに必須) この NAT ルールが適用されるインターフェイス。[送信元 (Source)] は実際のインターフェイスで、このインターフェイスを経由してトラフィックはデバイスに入ります。[宛先 (Destination)] はマッピングされたインターフェイスで、このインターフェイスを経由してトラフィックはデバイスから出ます。デフォルトでは、ルールはブリッジグループメンバ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 と変換済みの 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。



- [元の送信元アドレス (Original Source Address)] : 変換しているアドレスを含むネットワーク オブジェクトまたはグループ。
- [元の宛先アドレス (Original Destination Address)] : (任意) 宛先アドレスを含むネットワーク オブジェクト。空白のままにすると、宛先に関係なく、送信元アドレスの変換が適用されます。宛先アドレスを指定した場合、そのアドレスにスタティック変換を設定するか、単にアイデンティティ NAT を使用できます。

[インターフェイス (Interface)] を選択して、送信元インターフェイスの元の宛先 ([すべて (Any)] は選択不可) をベースにできます。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。

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

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

ポート変換を設定したスタティック NAT を設定した場合、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) [詳細オプション (Advanced Options)] リンクをクリックし、目的のオプションを選択します。

- [このルールと一致する DNS 応答を変換 (Translate DNS replies that match this rule)]: アイデンティティ NAT には、このオプションを設定しないでください。
- [宛先インターフェイスで ARP をプロキシしない (Do not proxy ARP on Destination Interface)]: マッピング IP アドレスへの着信パケットのプロキシ ARP を無効にします。マッピングインターフェイスと同じネットワーク上のアドレスを使用した場合、システムはプロキシ ARP を使用してマッピングアドレスのすべての ARP 要求に回答することで、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 9 [OK] をクリックします。

Threat Defense の NAT ルールのプロパティ

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

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

[役職 (Title)]

ルールの名前を入力します。名前にスペースを含めることはできません。

[ルールの作成対象 (Create Rule For)]

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

[ステータス (Status)]

ルールをアクティブにするか無効にするか。

[配置 (Placement)] (手動 NAT のみ)

Where you want to add the rule. ルールはカテゴリ内 (自動 NAT のルールの前後) 、または選択するルールの上に挿入できます。

[タイプ (Type)]

変換ルールを [ダイナミック (Dynamic)]にするか、[スタティック (Static)]にするかを指定します。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。

次に、残りの NAT ルールプロパティを説明します。

自動 NAT のパケット変換プロパティ

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

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

(ブリッジグループメンバーインターフェイスに必須) この NAT ルールが適用されるインターフェイス。[送信元 (Source)]は実際のインターフェイスで、このインターフェイスを経由してトラフィックはデバイスに入ります。[宛先 (Destination)]はマッピングされたインターフェイスで、このインターフェイスを経由してトラフィックはデバイスから出ます。デフォルトでは、ルールはブリッジグループメンバ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。

[元のアドレス (Original Address)] (常に必須)

変換している送信元アドレスを含むネットワークオブジェクト。グループではなくネットワークオブジェクトにする必要があります、ホスト、範囲、またはサブネットを含めることができます。

[変換済みアドレス (Translated Address)] (通常は必須)

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

- **[ダイナミック NAT (Dynamic NAT)]** : マッピングアドレスを含むネットワークオブジェクトまたはグループ。ネットワークオブジェクトまたはグループにできますが、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) 宛先の IPv4 アドレスのインターフェイスを使用するには、[インターフェイス (Interface)]を選択します。また、ブリッジグループメンバーインターフェイスではない特定の宛先インターフェイスを選択する必要があります。IPv6 にインターフェイス PAT は使用できません。
 - 宛先インターフェイスのアドレス以外の単一アドレスを使用する場合は、そのために作成したホスト ネットワーク オブジェクトを選択します。
- **[スタティック NAT (Static NAT)]** : 次のいずれかになります。
 - アドレスの設定グループを使用するには、マッピングされたアドレスを含むネットワークオブジェクトまたはグループを選択します。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 IP アドレスを使用するには、[インターフェイス (Interface)]を選択します。また、ブリッジグループメンバーインターフェイスではない特定の宛先インターフェイスを選択する必要があります。これはポート変換と共に、スタティックインターフェイス NAT を設定します。送信元アドレス/ポートは、インター

フェイスのアドレス、および同じポート番号に変換されます。IPv6 にインターフェイス PAT は使用できません。

- [アイデンティティ 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、元のポートおよび変換済みポートを定義するポートオブジェクトを選択します。オブジェクトは同じプロトコル向けにする必要があります。たとえば、必要に応じて TCP/80 を TCP/8080 に変換できます。

手動 NAT のパケット変換プロパティ

[パケット変換 (Packet Translation)] オプションを使用して、送信元アドレスと変換済みマッピングアドレスを定義します。次のプロパティは、手動 NAT にのみ適用されます。指示されている場合を除き、すべてオプションです。

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

(ブリッジグループメンバーインターフェイスに必須) この NAT ルールが適用されるインターフェイス。[送信元 (Source)] は実際のインターフェイスで、このインターフェイスを経由してトラフィックはデバイスに入ります。[宛先 (Destination)] はマッピングされたインターフェイスで、このインターフェイスを経由してトラフィックはデバイスから出ます。デフォルトでは、ルールはブリッジグループメンバ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。

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

変換しているアドレスを含むネットワーク オブジェクトまたはグループ。ネットワークオブジェクトまたはグループにすることが可能で、ホスト、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。

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

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

- [ダイナミック NAT (Dynamic NAT)]: マッピングアドレスを含むネットワーク オブジェクトまたはグループ。ネットワークオブジェクトまたはグループにできますが、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 IP アドレスを使用するには、[インターフェイス (Interface)] を選択します。また、ブリッジグループメンバー

インターフェイスではない特定の宛先インターフェイスを選択する必要があります。IPv6 にインターフェイス PAT は使用できません。

- 宛先インターフェイスのアドレス以外の単一アドレスを使用する場合は、そのために作成したホスト ネットワーク オブジェクトを選択します。
- [スタティック NAT (Static NAT)] : 次のいずれかになります。
 - アドレスの設定グループを使用するには、マッピングされたアドレスを含むネットワーク オブジェクトまたはグループを選択します。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 IP アドレスを使用するには、[インターフェイス (Interface)] を選択します。また、ブリッジグループ メンバー インターフェイスではない特定の宛先インターフェイスを選択する必要があります。これはポート変換と共に、スタティック インターフェイス NAT を設定します。送信元アドレス/ポートは、インターフェイスのアドレス、および同じポート番号に変換されます。IPv6 にインターフェイス PAT は使用できません。
- [アイデンティティ 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。

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

宛先アドレスを含むネットワークオブジェクト。空白のままにすると、宛先に関係なく、送信元アドレス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 (Interface)] を選択して、送信元インターフェイスの元の宛先 ([すべて (Any)] は選択不可) をベースにできます。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。

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

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 \(14 ページ\)](#) 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オブジェクトを使用できます。

詳細 NAT プロパティ

NAT を設定するとき、[詳細 (Advanced)] オプションで特別なサービスを提供するプロパティを設定できます。これら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 \(88 ページ\)](#)」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。変換されたアドレスとしてすでにインターフェイス PAT を設定している場合、このオプションを選択できません。このオプションは、IPv6 ネットワークでは使用できません。

宛先インターフェイスでプロキシ ARP なし（スタティック NAT のみ）

マッピング IP アドレスへの着信パケットのプロキシ ARP を無効にします。マッピングインターフェイスと同じネットワーク上のアドレスを使用した場合、システムはプロキシ ARP を使用してマッピングアドレスのすべての ARP 要求に応答することで、マッピングアドレスを宛先とするトラフィックを代行受信します。この方法だと、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 IDNAT 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。

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

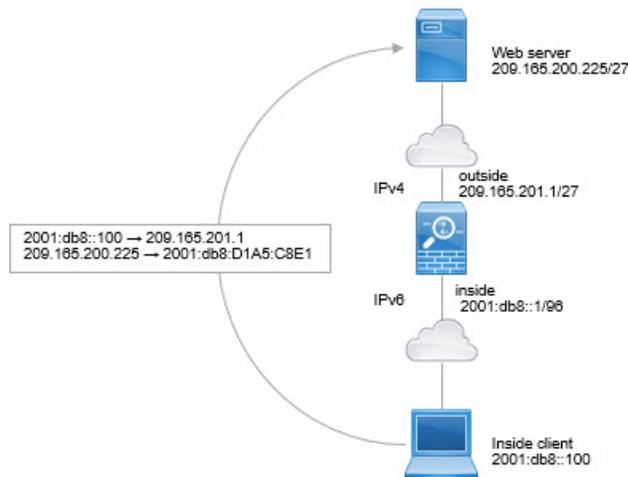
トラフィックが IPv6 ネットワークから IPv4 専用ネットワークに移動する場合、IPv6 アドレスを IPv4 に変換する必要があります。また、トラフィックを IPv4 から IPv6 に戻す必要があります。2つのアドレスプール (IPv4 ネットワークに IPv6 アドレスをバインドする IPv4 アドレスプールと、IPv6 ネットワークに IPv4 アドレスをバインドする IPv6 アドレスプール) を定義する必要があります。

- 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。

手順

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

- [オブジェクト (Objects)] を選択します。
- 目次から [ネットワーク (Network)] を選択し、[+] 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 (inside_v6 など) を付け、[ネットワーク (Network)] を選択して、ネットワーク アドレス (2001:db8::/96) を入力します。

Add Network Object

Name

inside_v6

Description

Type

Network Host

Network

2001:DB8::/96

d) **[OK]** をクリックします。

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

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

b) **[+]** ボタンをクリックします。

c) 次のプロパティを設定します。

- [タイトル (Title)] = PAT64Rule (またはユーザーが選択する別の名前)
- [ルールの作成対象 (Create Rule For)] = [手動 NAT (Manual NAT)]。
- [配置 (Placement)] = [自動 NAT ルールの前 (Before Auto NAT Rules)]
- [タイプ (Type)] = [ダイナミック (Dynamic)]
- [送信元インターフェイス (Source Interface)] = 内部 (inside)。
- [宛先インターフェイス (Destination Interface)] = [外部 (outside)]
- [元の packets 送信元アドレス (Original Packet Source Address)] = inside_v6 ネットワークオブジェクト
- [変換済み packets 送信元アドレス (Translated Packet Source Address)] : [インターフェイス (Interface)]。このオプションでは、宛先インターフェイスの IPv4 アドレスが PAT アドレスとして使用されます。
- [元の packets 宛先アドレス (Original Packet Destination Address)] = inside_v6 ネットワークオブジェクト
- [変換済み packets 宛先アドレス (Translated Packet Destination Address)] = any-ipv4 ネットワークオブジェクト

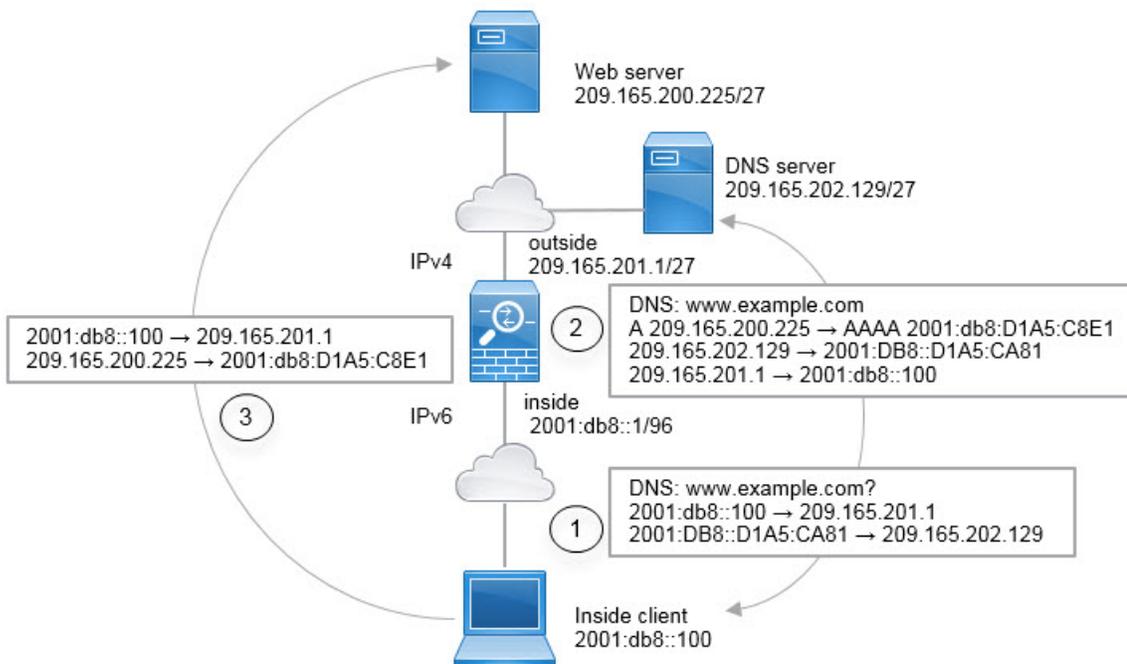
Title		Create Rule for		Status
PAT64Rule		Manual NAT		<input checked="" type="checkbox"/>
Manual NAT rules allow the translation of the source as well as the destination address of a network packet. Destination and port translation are optional. You can place manual NAT rules either before or after Auto NAT rules and insert the rules at a specific location.				
Placement		Type		
Before Auto NAT Rules		Dynamic		
Packet Translation		Advanced Options		
ORIGINAL PACKET		TRANSLATED PACKET		
Source Interface		Destination Interface		
inside		outside		
Source Address	Source Port	Source Address	Source Port	
inside_v6	Any	Interface	Any	
Destination Address	Destination Port	Destination Address	Destination Port	
inside_v6	Any	any-ipv4	Any	

d) [OK] をクリックします。

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

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

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 アドレスを持つダイナミック インターフェイス PAT を使用して、内部の IPv6 ネットワークを IPv4 に変換します。外部 IPv4 トラフィックは、2001:db8::/96 ネットワークのアドレスにスタティックに変換され、内部ネットワークでの送信が可能になります。NAT46 ルールで DNS の書き換えを有効にすると、外部 DNS サーバーからの応答を 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 レコードに応答します。DNS の書き換えが有効になっている NAT46 ルールにより、A レコードが IPv6 の同等の AAAA レコードに変換されて、AAAA レコードの 209.165.200.225 が 2001:db8:D1A5:C8E1 に変換されます。なお、DNS 応答の送信元アドレスと宛先アドレスは変換されません。
 - 209.165.202.129 を 2001:DB8::D1A5:CA81 に変換
 - 209.165.201.1 を 2001:db8::100 に変換

3. これで、IPv6 クライアントが Web サーバーの 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。

手順

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

- a) [オブジェクト (Objects)] を選択します。
- b) 目次から [ネットワーク (Network)] を選択し、[+] をクリックします。
- c) 内部 IPv6 ネットワークを定義します。

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

Add Network Object

Name
inside_v6

Description

Type
 Network Host

Network
2001:DB8::/96

- d) [OK] をクリックします。
- e) [+] をクリックして、外部 IPv4 ネットワークを定義します。

ネットワーク オブジェクトに名前 (outside_v4_any など) を付け、[ネットワーク (Network)] を選択して、ネットワーク アドレス (0.0.0.0/0) を入力します。

Add Network Object

Name
outside_v4_any

Description

Type
 Network Host

Network
0.0.0.0/0

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

- a) [ポリシー (Policies)] > [NAT] を選択します。
- b) [+] ボタンをクリックします。
- c) 次のプロパティを設定します。
 - [タイトル (Title)] = PAT64Rule (またはユーザーが選択する別の名前)
 - [ルールの作成対象 (Create Rule For)] = [自動 NAT (Auto NAT)]
 - [タイプ (Type)] = [ダイナミック (Dynamic)]
 - [送信元インターフェイス (Source Interface)] = 内部 (inside)。
 - [宛先インターフェイス (Destination Interface)] = [外部 (outside)]
 - [元のアドレス (Original Address)] : inside_v6 ネットワーク オブジェクト (inside_v6 network object)
 - [変換済みアドレス (Translated Address)] = [インターフェイス (Interface)]。このオプションでは、宛先インターフェイスの IPv4 アドレスが PAT アドレスとして使用されます。

Add NAT Rule

Title: PAT64Rule Create Rule for: Auto NAT Status:

Auto NAT rules translate a specified host or network address regardless of its appearance as the source or destination address of a packet. These rules are automatically ordered and placed in the Auto NAT section.

Placement: Automatically placed in Auto NAT rules Type: Dynamic

Packet Translation Advanced Options

ORIGINAL PACKET		TRANSLATED PACKET	
Source Interface	inside	Destination Interface	outside
Original Address	inside_v6	Translated Address	Interface
Original Port	Any	Translated Port	Any

d) [OK] をクリックします。

このルールにより、内部インターフェイスの 2001:db8::/96 サブネットから外部インターフェイスに向かうすべてのトラフィックが、外部インターフェイスの IPv4 アドレスを使用して NAT64 PAT 変換されます。

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

- a) [+] ボタンをクリックします。
- b) 次のプロパティを設定します。
 - [タイトル (Title)] = NAT46Rule (またはユーザーが選択する別の名前)。
 - [ルールの作成対象 (Create Rule For)] = [自動 NAT (Auto NAT)]
 - [タイプ (Type)] = [スタティック (Static)]
 - [送信元インターフェイス (Source Interface)] = [外部 (outside)]
 - [宛先インターフェイス (Destination Interface)] = [内部 (inside)]
 - [元のアドレス (Original Address)] = outside_v4_any ネットワーク オブジェクト (outside_v4_any network object)。
 - [変換済みアドレス (Translated Address)] = inside_v6 ネットワーク オブジェクト (inside_v6 network object)

- [詳細オプション (Advanced Options)] タブで、[このルールと一致するDNS応答を変換 (Translate DNS replies that match this rule)] を選択します。

Add NAT Rule ?

Title	Create Rule for	Status
NAT46Rule	Auto NAT ▼	<input checked="" type="checkbox"/>

Auto NAT rules translate a specified host or network address regardless of its appearance as the source or destination address of a packet. These rules are automatically ordered and placed in the Auto NAT section.

Placement	Type
Automatically placed in Auto NAT rules	Static ▼

Packet Translation

Advanced Options

ORIGINAL PACKET		TRANSLATED PACKET	
Source Interface	Destination Interface		
outside ▼	inside		
Original Address	Original Port	Translated Address	Translated Port
outside_v4_any ▼	Any ▼	inside_v6 ▼	Any

- c) [OK] をクリックします。

このルールを使用すると、内部インターフェイスに届く外部ネットワークのすべての IPv4 アドレスが、組み込みの IPv4 アドレス方式を使用して 2001:db8::/96 ネットワークのアドレスに変換されます。また、DNS 応答が A (IPv4) レコードから AAAA (IPv6) レコードに変換され、アドレスが IPv4 から IPv6 に変換されます。

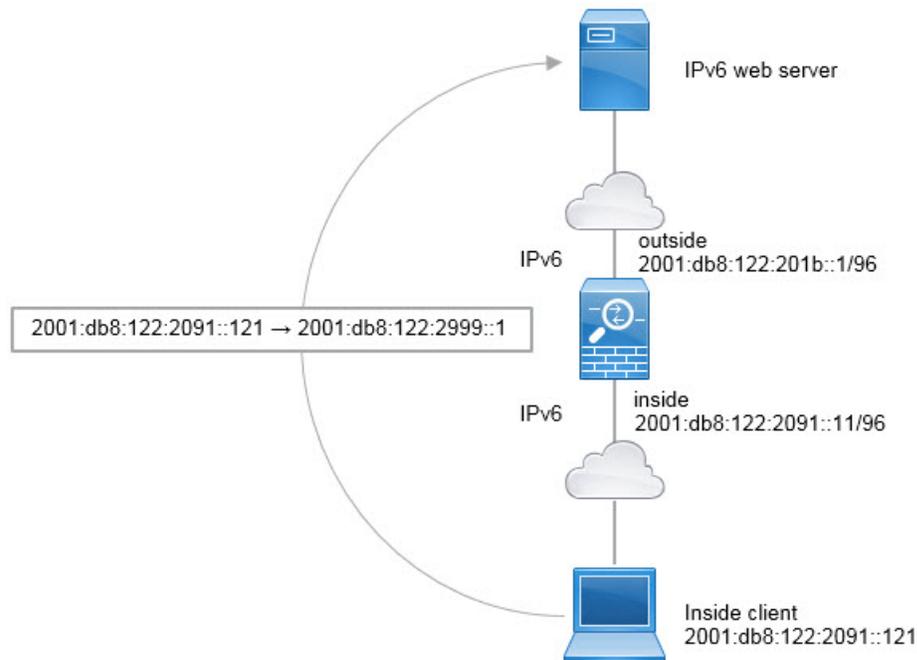
NAT66 : IPv6 アドレスの異なる IPv6 アドレスへの変換

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。



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

手順

ステップ 1 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)] を選択します。
- 目次から [ネットワーク (Network)] を選択し、[+] 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 (inside_v6 など) を付け、[ネットワーク (Network)] を選択して、ネットワーク アドレス (2001:db8:122:2091::/96) を入力します。

Add Network Object

Name
inside_v6

Description

Type
 Network Host

Network
2001:db8:122:2091::/96

- d) **[OK]** をクリックします。
- e) **[+]** をクリックして、外部 IPv6 PAT ネットワークを定義します。

ネットワークオブジェクトに名前（outside_nat_v6など）を付け、[ネットワーク（Network）] を選択して、ネットワークアドレス（2001:db8:122:2999::/96）を入力します。

Add Network Object

Name
outside_nat_v6

Description

Type
 Network Host

Network
2001:db8:122:2999::/96

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

- a) **[ポリシー（Policies）]** > **[NAT]** を選択します。
- b) **[+]** ボタンをクリックします。
- c) 次のプロパティを設定します。
- [タイトル（Title）] = NAT66Rule（またはユーザーが選択する別の名前）

- [ルールの作成対象 (Create Rule For)] = [自動 NAT (Auto NAT)]
- [タイプ (Type)] = [スタティック (Static)]
- [送信元インターフェイス (Source Interface)] = 内部 (inside) 。
- [宛先インターフェイス (Destination Interface)] = [外部 (outside)]
- [元のアドレス (Original Address)] : inside_v6 ネットワーク オブジェクト (inside_v6 network object)
- [変換済みアドレス (Translated Address)] = outside_nat_v6 ネットワーク オブジェクト (outside_nat_v6 network object) 。

Add NAT Rule ?

Title	Create Rule for	Status
NAT66Rule	Auto NAT ▼	<input checked="" type="checkbox"/>

Auto NAT rules translate a specified host or network address regardless of its appearance as the source or destination address of a packet. These rules are automatically ordered and placed in the Auto NAT section.

Placement	Type
Automatically placed in Auto NAT rules	Static ▼

Packet Translation

Advanced Options

ORIGINAL PACKET		TRANSLATED PACKET	
Source Interface	Destination Interface		
inside ▼	outside		
Original Address	Original Port	Translated Address	Translated Port
inside_v6 ▼	Any ▼	outside_nat_v6 ▼	Any

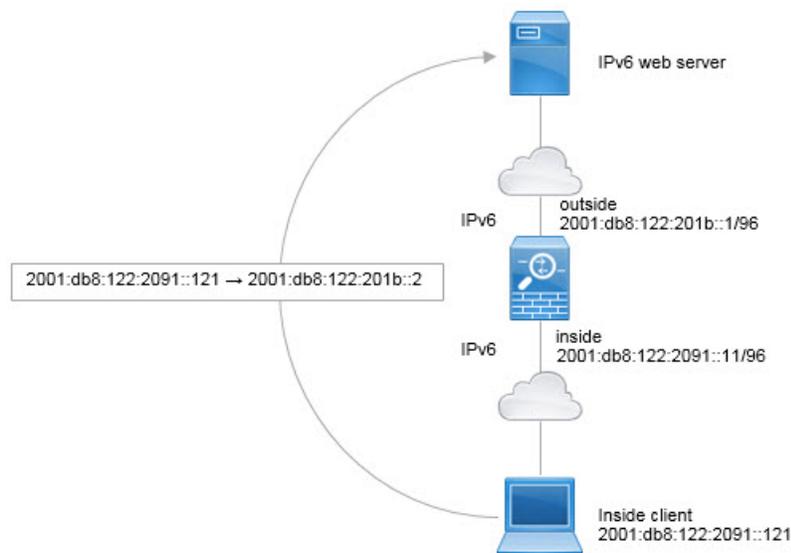
d) [OK] をクリックします。

このルールにより、内部インターフェイス上の 2001:db8:122:2091::/96 サブネットワーク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。

ただし、Device Manager を使用して、インターフェイスの IPv6 アドレスを使用するインターフェイス PAT は設定できません。代わりに、同じネットワーク上の 1 つの空きアドレスを動的 PAT プールとして使用します。



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

手順

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

- [オブジェクト (Objects)] を選択します。
- 目次から [ネットワーク (Network)] を選択し、[+] 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 (inside_v6 など) を付け、[ネットワーク (Network)] を選択して、ネットワーク アドレス (2001:db8:122:2091::/96) を入力します。

Add Network Object

Name
inside_v6

Description

Type
 Network Host

Network
2001:db8:122:2091::/96

- d) **[OK]** をクリックします。
- e) **[+]** をクリックして、外部 IPv6 PAT アドレスを定義します。
ネットワーク オブジェクトに名前 (`inside_v6` など) を付け、**[ホスト (Host)]** を選択して、ホストアドレス (`2001:db8:122:201b::2`) を入力します。

Add Network Object

Name
ipv6_pat

Description

Type
 Network Host

Host
2001:db8:122:201b::2

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

- a) **[ポリシー (Policies)]** > **[NAT]** を選択します。
- b) **[+]** ボタンをクリックします。
- c) 次のプロパティを設定します。
- **[タイトル (Title)]** = PAT66Rule (またはユーザーが選択する別の名前)。

- [ルールの作成対象 (Create Rule For)] = [自動 NAT (Auto NAT)]
- [タイプ (Type)] = [ダイナミック (Dynamic)]
- [送信元インターフェイス (Source Interface)] = 内部 (inside) 。
- [宛先インターフェイス (Destination Interface)] = [外部 (outside)]
- [元のアドレス (Original Address)] : inside_v6 ネットワーク オブジェクト (inside_v6 network object)
- [変換済みアドレス (Translated Address)] = ipv6_pat ネットワーク オブジェクト (ipv6_pat network object)。

Add NAT Rule ?

Title	Create Rule for	Status
PAT66Rule	Auto NAT ▼	<input checked="" type="checkbox"/>

Auto NAT rules translate a specified host or network address regardless of its appearance as the source or destination address of a packet. These rules are automatically ordered and placed in the Auto NAT section.

Placement	Type
Automatically placed in Auto NAT rules	Dynamic ▼

Packet Translation Advanced Options

ORIGINAL PACKET				TRANSLATED PACKET			
Source Interface				Destination Interface			
inside ▼				outside			
Original Address		Original Port		Translated Address		Translated Port	
inside_v6 ▼		Any ▼		ipv6_pat ▼		Any	

d) [OK] をクリックします。

このルールを使用すると、内部インターフェイスの 2001:db8:122:2091::/96 サブネットから外部インターフェイスに届くすべてのトラフィックが 2001:db8:122:201b::2 のポートにダイナミック PAT66 変換されます。

NAT のモニタリング

NAT 接続をモニターしてトラブルシューティングを実行するには、CLI コンソールを開くかデバイス 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。（このコマンドは CLI コンソールでは使用できません。）

NAT の例

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。

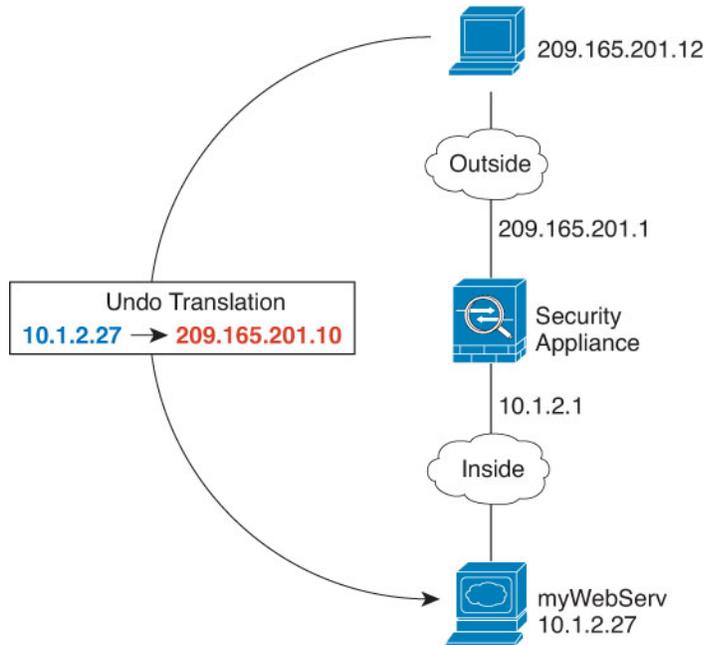
内部 Web サーバーへのアクセスの提供（スタティック自動 NAT）

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。



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

図 13: 内部 Web サーバーのスタティック NAT



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)] を選択します。
- 目次から [ネットワーク (Network)] を選択し、[+] をクリックします。
- Web サーバのプライベートアドレスを定義します。

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

New Network Object

Name
WebServerPrivate

Description

Type
 Network Host

Host
10.1.2.27

- d) **[OK]** をクリックします。
- e) **[+]** をクリックして、パブリック アドレスを定義します。

ネットワークオブジェクトに名前 (WebServerPublic など) を付け、[ホスト (Host)] を選択して、ホストアドレス (209.165.201.10) を入力します。

New Network Object

Name
WebServerPublic

Description

Type
 Network Host

Host
209.165.201.10

- f) **[OK]** をクリックします。

ステップ 2 オブジェクトのスタティック NAT を設定します。

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

- [タイトル (Title)] = WebServer（またはユーザーが選択する別の名前）
- [ルールの作成対象 (Create Rule For)] = [自動 NAT (Auto NAT)]
- [タイプ (Type)] = [スタティック (Static)]
- [送信元インターフェイス (Source Interface)] = 内部 (inside) 。
- [宛先インターフェイス (Destination Interface)] = [外部 (outside)]
- [元のアドレス (Original Address)] = WebServerPrivate ネットワーク オブジェクト (WebServerPrivate network object)
- [変換済みアドレス (Translated Address)] = WebServerPublic ネットワーク オブジェクト (WebServerPublic network object)

d) [OK] をクリックします。

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

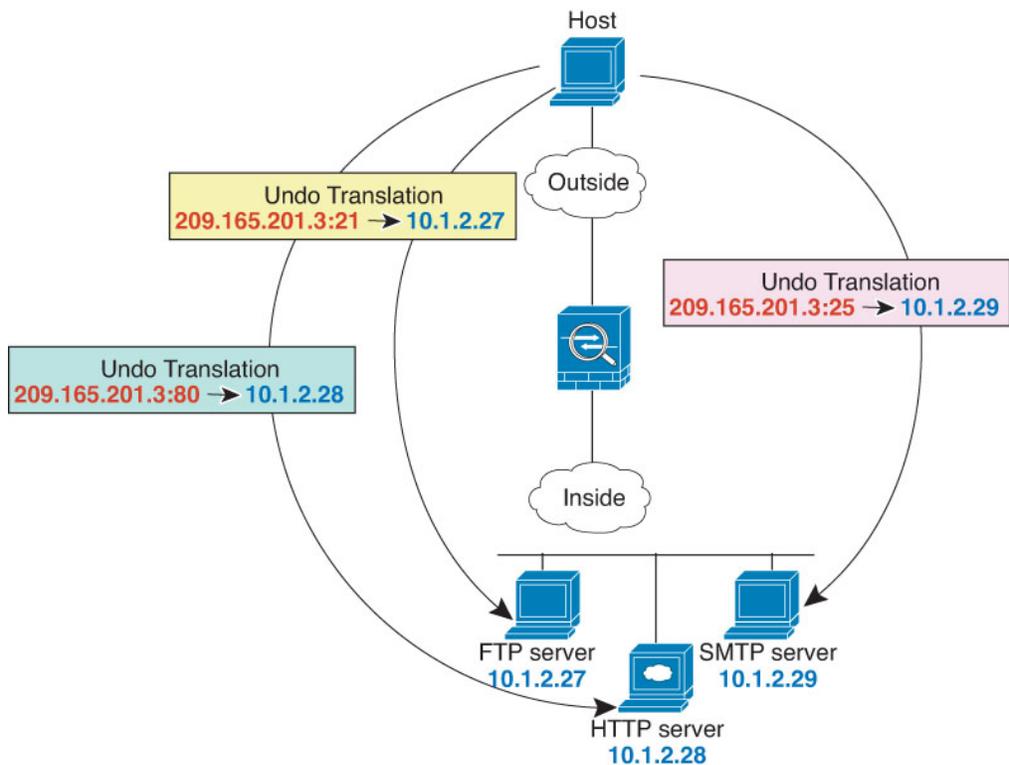
次のポート変換を設定したスタティック NAT の例では、リモートユーザーが FTP、HTTP、および SMTP にアクセスするための単一のアドレスを提供します。これらのサーバーは実際には、それぞれ異なるデバイスとして実際のネットワーク上に存在しますが、ポート変換を設定

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。



- (注) この例では、内部インターフェイスはスイッチに接続された標準ルーテッドインターフェイスで、スイッチにサーバーが接続されていると仮定します。内部インターフェイスがブリッジグループインターフェイス (BVI) であり、サーバーが別のブリッジグループメンバーインターフェイスに接続されている場合、各サーバーが対応するルールで接続する特定のメンバーインターフェイスを選択します。たとえば、ルールは「inside」ではなく、送信元インターフェイスの「inside1_2」、「inside1_3」、および「inside1_4」の可能性がります。

図 14: ポート変換を設定したスタティック NAT



手順

ステップ 1 FTP サーバーのネットワーク オブジェクトを作成します。

- [オブジェクト (Objects)] を選択します。
- 目次から [ネットワーク (Network)] を選択し、[+] 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)、[ホスト (Host)] を選択し、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

Type
 Network Host

Host
10.1.2.27

d) **[OK]** をクリックします。

ステップ2 HTTP サーバのネットワーク オブジェクトを作成します。

- a) **[+]** をクリックします。
- b) ネットワーク オブジェクトに名前を付け（たとえばHTTPserver）、[ホスト (Host)]を選択し、ホストアドレス（10.1.2.28）を入力します。

New Network Object

Name
HTTPServer

Description

Type
 Network Host

Host
10.1.2.28

c) **[OK]** をクリックします。

ステップ3 SMTP サーバのネットワーク オブジェクトを作成します。

- a) **[+]** をクリックします。
- b) ネットワーク オブジェクトに名前を付け（たとえばSMTPserver）、[ホスト (Host)]を選択し、ホストアドレス（10.1.2.29）を入力します。

New Network Object

Name
SMTPServer

Description

Type
 Network Host

Host
10.1.2.29

- c) **[OK]** をクリックします。

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

- a) **[+]** をクリックします。
b) ネットワーク オブジェクトに名前を付け（たとえば **ServerPublicIP**）、**[ホスト (Host)]** を選択し、ホストアドレス（**209.165.201.3**）を入力します。

New Network Object

Name
ServerPublicIP

Description

Type
 Network Host

Host
209.165.201.3

- c) **[OK]** 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) **[ポリシー (Policies)]** > **[NAT]** を選択します。
b) **[+]** ボタンをクリックします。

c) 次のプロパティを設定します。

- [タイトル (Title)] = FTPServer (または任意の別の名前)
- [ルールの作成対象 (Create Rule For)] = [自動 NAT (Auto NAT)]
- [タイプ (Type)] = [スタティック (Static)]
- [送信元インターフェイス (Source Interface)] = 内部 (inside) 。
- [宛先インターフェイス (Destination Interface)] = [外部 (outside)]
- [元のアドレス (Original Address)] = FTPServer ネットワーク オブジェクト (FTPserver network object)
- [変換済みアドレス (Translated Address)] = ServerPublicIP ネットワーク オブジェクト (ServerPublicIP network object) 。
- [元のポート (Original Port)] = FTP ポート オブジェクト (FTP port object) 。
- [変換済みポート (Translated Port)] = FTP ポート オブジェクト (FTP port object) 。

d) [OK] をクリックします。

ステップ 6 HTTP サーバー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。

- [+] ボタンをクリックします。
- 次のプロパティを設定します。

- [タイトル (Title)]= HTTPServer（または任意の別の名前）。
- [ルールの作成対象 (Create Rule For)]=[自動 NAT (Auto NAT)]
- [タイプ (Type)]=[スタティック (Static)]
- [送信元インターフェイス (Source Interface)]= 内部 (inside) 。
- [宛先インターフェイス (Destination Interface)]=[外部 (outside)]
- [元のアドレス (Original Address)]= HTTPserver ネットワーク オブジェクト (HTTPserver network object) 。
- [変換済みアドレス (Translated Address)]= ServerPublicIP ネットワーク オブジェクト (ServerPublicIP network object) 。
- [元のポート (Original Port)]= HTTP ポート オブジェクト (FTP port object) 。
- [変換済みポート (Translated Port)]= HTTP ポート オブジェクト (HTTP port object) 。

Add NAT Rule

Title: HTTPServer

Create Rule for: Auto NAT

Auto NAT rules translate a specified host or network address regardless of its appearance as the source or destination address of a packet. These rules are automatically ordered and placed in the Auto NAT section.

Placement: Automatically placed in Auto NAT rules

Type: Static

Packet Translation | Advanced Options

Original Packet		Translated Packet	
Source Interface	inside	Destination Interface	outside
Original Address	HTTPServer	Translated Address	ServerPublicIP
Original Port	HTTP	Translated Port	HTTP

c) [OK] をクリックします。

ステップ7 SMTP 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、SMTP ポートを自身にマッピングします。

- [+] ボタンをクリックします。
- 次のプロパティを設定します。

- [タイトル (Title)]= SMTPServer（または任意の別の名前）。

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

Add NAT Rule

Title: SMTPServer Create Rule for: Auto NAT

Auto NAT rules translate a specified host or network address regardless of its appearance as the source or destination address of packet. These rules are automatically ordered and placed in the Auto NAT section.

Placement: Automatically placed in Auto NAT rules Type: Static

Packet Translation Advanced Options

Original Packet		Translated Packet	
Source Interface	inside	Destination Interface	outside
Original Address	SMTPServer	Translated Address	ServerPublicIP
Original Port	SMTP	Translated Port	SMTP

c) [OK] をクリックします。

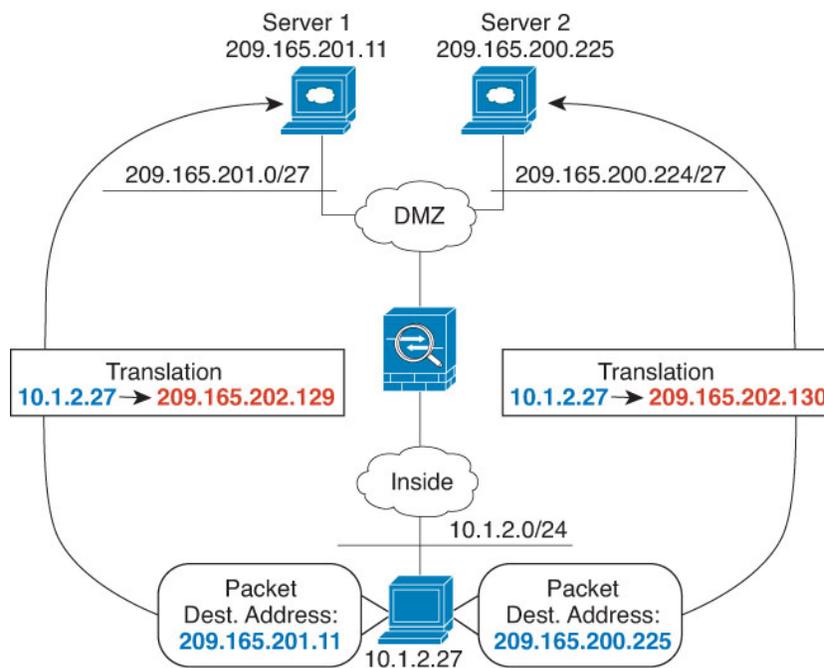
宛先に応じて異なる変換 (ダイナミック手動 PAT)

次の図に、2 台の異なるサーバ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。



- (注) この例では、内部インターフェイスはスイッチに接続された標準ルーテッドインターフェイスで、スイッチにサーバーが接続されていると仮定します。内部インターフェイスがブリッジグループインターフェイス (BVI) であり、サーバーが別のブリッジグループメンバーインターフェイスに接続されている場合、各サーバーが対応するルールで接続する特定のメンバーインターフェイスを選択します。たとえば、ルールは、内部インターフェイスではなく、送信元インターフェイスの `inside1_2` および `inside1_3` を持つ場合があります。

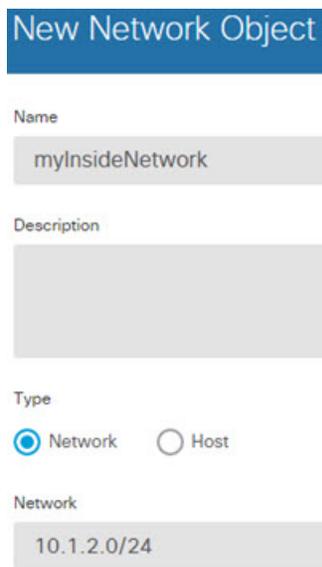
図 15:異なる宛先アドレスを使用する手動 NAT



手順

ステップ 1 内部ネットワークのネットワーク オブジェクトを作成します。

- [オブジェクト (Objects)] を選択します。
- 目次から [ネットワーク (Network)] を選択し、[+] 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)、[ネットワーク (Network)] を選択して、実際のネットワーク アドレス 10.1.2.0/24 を入力します。



New Network Object

Name
myInsideNetwork

Description

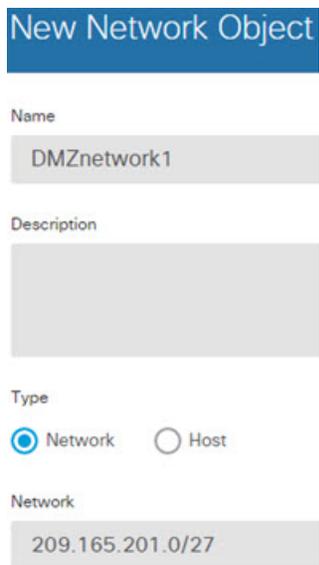
Type
 Network Host

Network
10.1.2.0/24

d) **[OK]** をクリックします。

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

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



New Network Object

Name
DMZnetwork1

Description

Type
 Network Host

Network
209.165.201.0/27

c) **[OK]** をクリックします。

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

- a) **[+]** をクリックします。

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

New Network Object

Name
PATaddress1

Description

Type
 Network Host

Host
209.165.202.129

- c) [OK] をクリックします。

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

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

New Network Object

Name
DMZnetwork2

Description

Type
 Network Host

Network
209.165.200.224/27

- c) **[OK]** をクリックします。

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

- a) **[+]** をクリックします。
 b) ネットワーク オブジェクトに名前を付け (PATAddress2 など)、**[ホスト (Host)]** を選択して、ホストアドレス 209.165.202.130 を入力します。

New Network Object

Name
 PATAddress2

Description

Type
 Network Host

Host
 209.165.202.130

- c) **[OK]** をクリックします。

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

- a) **[ポリシー (Policies)]** > **[NAT]** を選択します。
 b) **[+]** ボタンをクリックします。
 c) 次のプロパティを設定します。
- **[タイトル (Title)]** = DMZNetwork1 (または任意の別の名前)。
 - **[ルールの作成対象 (Create Rule For)]** = 手動 NAT (Manual NAT)。
 - **[タイプ (Type)]** = **[ダイナミック (Dynamic)]**
 - **[送信元インターフェイス (Source Interface)]** = 内部 (inside)。
 - **[宛先インターフェイス (Destination Interface)]** = dmz。
 - **[元の発信元アドレス (Original Source Address)]** = myInsideNetwork のネットワーク オブジェクト (myInsideNetwork network object)。
 - **[変換済みの発信元アドレス (Translated Source Address)]** = PATAddress1 のネットワーク オブジェクト (PATAddress1 network object)。
 - **[元の宛先アドレス (Original Destination Address)]** = DMZnetwork1 のネットワーク オブジェクト (DMZnetwork1 network object)。

- [変換済みの宛先アドレス (Translated Destination Address)] = DMZnetwork1 のネットワーク オブジェクト (DMZnetwork1 network object) 。

(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。

Add NAT Rule

Title: DMZNetwork1

Create Rule for: Manual NAT

Manual NAT rules allow the translation of the source as well as the destination address of a network packet. Destination and port translation are optional. You can place manual NAT rules either before or after Auto NAT rules and insert the rules at a specific location.

Placement: Before Auto NAT Rules

Type: Dynamic

Packet Translation

Original Packet		Translated Packet	
Source Interface	inside	Destination Interface	dmz
Source Address	myInsideNetwork	Source Address	PATaddress1
Source Port	Any	Source Port	Any
Destination Address	DMZnetwork1	Destination Address	DMZnetwork1
Destination Port	Any	Destination Port	Any

d) [OK] をクリックします。

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

- [+] ボタンをクリックします。
- 次のプロパティを設定します。
 - タイトル (Title) = DMZNetwork2 (または任意の別の名前) 。
 - [ルール of の作成対象 (Create Rule For)] = 手動 NAT (Manual NAT) 。
 - [タイプ (Type)] = [ダイナミック (Dynamic)]
 - [送信元インターフェイス (Source Interface)] = 内部 (inside) 。
 - [宛先インターフェイス (Destination Interface)] = dmz。

- [元の発信元アドレス（Original Source Address）] = myInsideNetwork のネットワーク オブジェクト（myInsideNetwork network object）。
- [変換済みの発信元アドレス（Translated Source Address）] = PATaddress2 のネットワーク オブジェクト（PATaddress2 network object）。
- [元の宛先アドレス（Original Destination Address）] = DMZnetwork2 のネットワーク オブジェクト（DMZnetwork2 network object）。
- [変換済みの宛先アドレス（Translated Destination Address）] = DMZnetwork2 のネットワーク オブジェクト（DMZnetwork2 network object）。

Add NAT Rule

Title: DMZNetwork2 Create Rule for: Manual NAT

Manual NAT rules allow the translation of the source as well as the destination address of a network packet. Destination and port translation are optional. You can place manual NAT rules either before or after Auto NAT rules and insert the rules at a specific location.

Placement: Before Auto NAT Rules Type: Dynamic

Packet Translation Advanced Options

Original Packet		Translated Packet	
Source Interface	inside	Destination Interface	dmz
Source Address	myInsideNetwork	Source Address	PATaddress2
Source Port	Any	Source Port	Any
Destination Address	DMZnetwork2	Destination Address	DMZnetwork2
Destination Port	Any	Destination Port	Any

c) [OK] をクリックします。

宛先アドレスおよびポートに応じて異なる変換（ダイナミック手動 PAT）

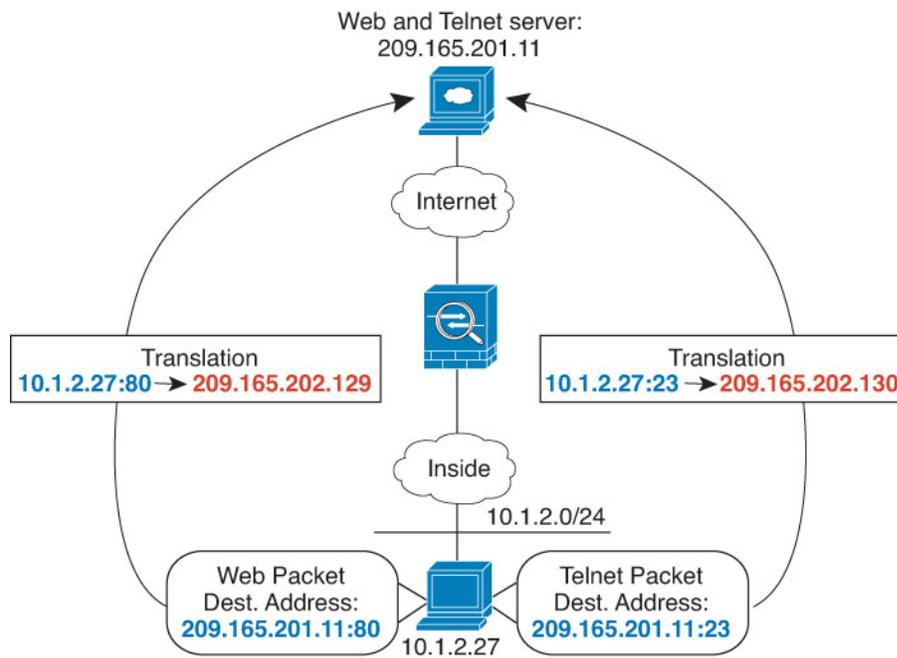
次の図に、送信元ポートおよび宛先ポートの使用例を示します。10.1.2.0/24 ネットワークのホストは Web サービスと Telnet サービスの両方を提供する 1 つのホストにアクセスします。ホストが Telnet サービスを求めてサーバーにアクセスすると、実際のアドレスは 209.165.202.129:

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。



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

図 16:異なる宛先ポートを使用する手動 NAT



手順

ステップ 1 内部ネットワークのネットワーク オブジェクトを作成します。

- [オブジェクト (Objects)] を選択します。
- 目次から [ネットワーク (Network)] を選択し、[+] 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)、[ネットワーク (Network)] を選択して、実際のネットワーク アドレス 10.1.2.0/24 を入力します。

New Network Object

Name
myInsideNetwork

Description

Type
 Network Host

Network
10.1.2.0/24

d) **[OK]** をクリックします。

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

- [+] 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 (TelnetWebServer など)、[ホスト (Host)] を選択して、ホスト アドレス 209.165.201.11 を入力します。

New Network Object

Name
TelnetWebServer

Description

Type
 Network Host

Host
209.165.201.11

c) **[OK]** 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。

- [+] 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 (PATAddress1 など)、[ホスト (Host)] を選択して、ホスト アドレス 209.165.202.129 を入力します。

New Network Object

Name
PATaddress1

Description

Type
 Network Host

Host
209.165.202.129

c) **[OK]** をクリックします。

ステップ 4 HTTP 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。

- [+] 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 (PATaddress2 など)、[ホスト (Host)] を選択して、ホストアドレス 209.165.202.130 を入力します。

New Network Object

Name
PATaddress2

Description

Type
 Network Host

Host
209.165.202.130

c) **[OK]** をクリックします。

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

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

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

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

d) [OK] をクリックします。

ステップ 6 Web アクセスのダイナミック手動 PAT を設定します。

a) [+] ボタンをクリックします。

b) 次のプロパティを設定します。

- [タイトル (Title)] = WebServer (またはユーザーが選択する別の名前)
- [ルールの実行対象 (Create Rule For)] = 手動 NAT (Manual NAT) 。
- [タイプ (Type)] = [ダイナミック (Dynamic)]
- [送信元インターフェイス (Source Interface)] = 内部 (inside) 。
- [宛先インターフェイス (Destination Interface)] = dmz。
- [元の発信元アドレス (Original Source Address)] = myInsideNetwork のネットワーク オブジェクト (myInsideNetwork network object) 。
- [変換済みの発信元アドレス (Translated Source Address)] = PATAddress2 のネットワーク オブジェクト (PATAddress2 network object) 。
- [元の宛先アドレス (Original Destination Address)] = TelnetWebServer のネットワーク オブジェクト (TelnetWebServer network object) 。

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

Add NAT Rule

Title: WebServer Create Rule for: Manual NAT

Manual NAT rules allow the translation of the source as well as the destination address of a network packet. Destination and port translation are optional. You can place manual NAT rules either before or after Auto NAT rules and insert the rules at a specific location.

Placement: Before Auto NAT Rules Type: Dynamic

Packet Translation Advanced Options

Original Packet		Translated Packet	
Source Interface	inside	Destination Interface	dmz
Source Address	myInsideNetwork	Source Address	PATaddress2
Source Port	Any	Source Port	Any
Destination Address	TelnetWebServe	Destination Address	TelnetWebServe
Destination Port	HTTP	Destination Port	HTTP

c) [OK] をクリックします。

NAT を使用した DNS クエリと応答の書き換え

応答内のアドレスを NAT 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になる場合があります。DNS 修正は、各トランスレーションルールを設定するときに設定できます。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。
- 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。

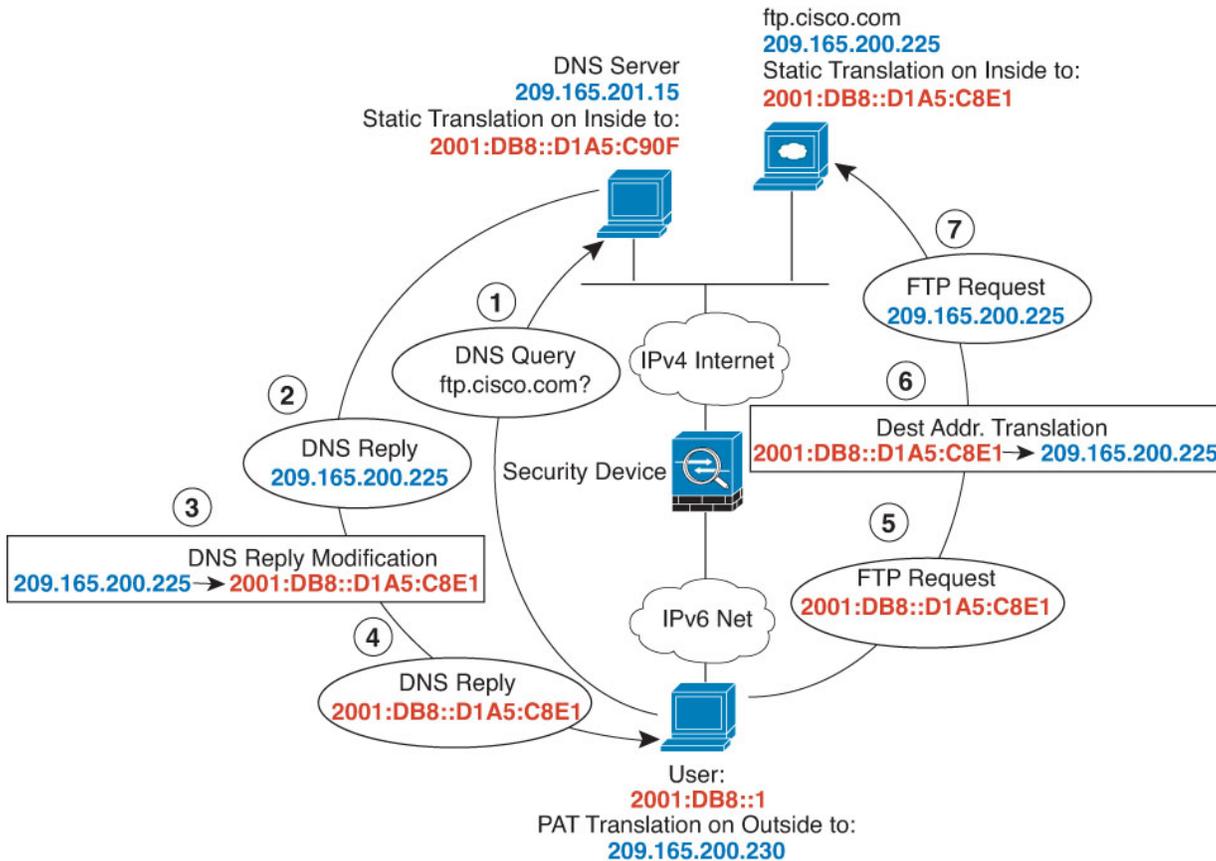
次のトピックで、NAT ルールでの DNS の書き換えの例を示します。

DNS 64 応答修正

次の図に、外部の IPv4 ネットワーク上の FTP サーバと DNS サーバを示します。システムには、外部サーバ用のスタティック変換があります。この場合、内部 IPv6 ユーザーが `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 (209.165.200.225) 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 サーバーのスタティック NAT 変換、および内部 IPv6 ホストの PAT ルールも含まれています。



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

手順

ステップ 1 FTP サーバー、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)] を選択します。
- 目次から [ネットワーク (Network)] を選択し、[+] をクリックします。
- 実際の FTP サーバアドレスを定義します。

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

Add Network Object

Name
ftp_server

Description

Type
 Network Host

Host
209.165.200.225

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

Add Network Object

Name
dns_server

Description

Type
 Network Host

Host
209.165.201.15

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

Add Network Object

Name
inside_v6

Description

Type
 Network Host

Network
2001:DB8::/96

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

Add Network Object

Name
ipv4_pat

Description

Type
 Network Host

Host
209.165.200.230

- j) **[OK]** 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) **[ポリシー (Policies)]** > **[NAT]** を選択します。
- b) **[+]** ボタンをクリックします。
- c) 次のプロパティを設定します。
- **[タイトル (Title)]** = FTPServer (または任意の別の名前)

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

Add NAT Rule

Title: FTPServer Create Rule for: Auto NAT Status:

Auto NAT rules translate a specified host or network address regardless of its appearance as the source or destination address of a packet. These rules are automatically ordered and placed in the Auto NAT section.

Placement: Automatically placed in Auto NAT rules Type: Static

Packet Translation Advanced Options

ORIGINAL PACKET		TRANSLATED PACKET	
Source Interface	outside	Destination Interface	inside
Original Address	ftp_server	Translated Address	inside_v6
Original Port	Any	Translated Port	Any

d) [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。

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

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

Add NAT Rule ?

Title	Create Rule for	Status
DNSServer	Auto NAT ▼	<input checked="" type="checkbox"/>

Auto NAT rules translate a specified host or network address regardless of its appearance as the source or destination address of a packet. These rules are automatically ordered and placed in the Auto NAT section.

Placement	Type
Automatically placed in Auto NAT rules	Static ▼

Packet Translation Advanced Options

ORIGINAL PACKET		TRANSLATED PACKET	
Source Interface	outside ▼	Destination Interface	inside
Original Address	dns_server ▼	Translated Address	inside_v6 ▼
Original Port	Any ▼	Translated Port	Any

d) [OK] をクリックします。

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

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

- [タイトル (Title)] = PAT64Rule (またはユーザーが選択する別の名前)
- [ルールの作成対象 (Create Rule For)] = [自動 NAT (Auto NAT)]
- [タイプ (Type)] = [ダイナミック (Dynamic)]
- [送信元インターフェイス (Source Interface)] = 内部 (inside) 。
- [宛先インターフェイス (Destination Interface)] = [外部 (outside)]
- [元のアドレス (Original Address)] : inside_v6 ネットワーク オブジェクト (inside_v6 network object)
- [変換済みのアドレス (Translated Address)] = ipv4_pat のネットワーク オブジェクト (ipv4_pat network object) 。

Add NAT Rule

Title: PAT64Rule Create Rule for: Auto NAT Status:

Auto NAT rules translate a specified host or network address regardless of its appearance as the source or destination address of a packet. These rules are automatically ordered and placed in the Auto NAT section.

Placement: Automatically placed in Auto NAT rules Type: Dynamic

Packet Translation Advanced Options

ORIGINAL PACKET		TRANSLATED PACKET	
Source Interface	inside	Destination Interface	outside
Original Address	inside_v6	Translated Address	ipv4_pat
Original Port	Any	Translated Port	Any

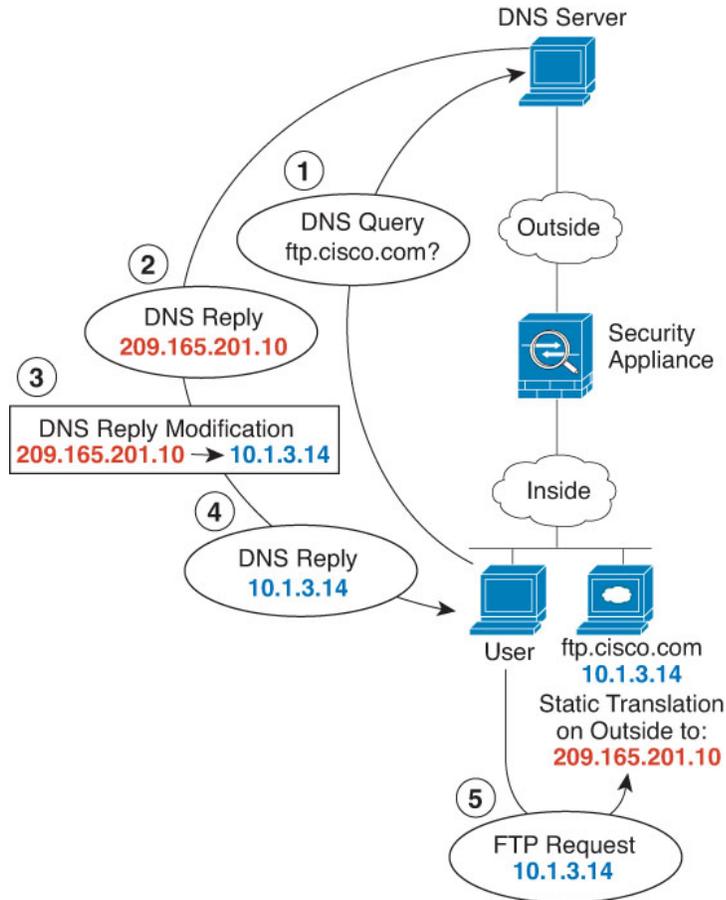
d) [OK] をクリックします。

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。



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

手順

ステップ 1 FTP サーバのネットワーク オブジェクトを作成します。

- a) [オブジェクト (Objects)] を選択します。
- b) 目次から [ネットワーク (Network)] を選択し、[+] をクリックします。
- c) 実際の FTP サーバアドレスを定義します。

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

Add Network Object

Name
ftp_server

Description

Type
 Network Host

Host
10.1.3.14

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

Add Network Object

Name
ftp_server_outside

Description

Type
 Network Host

Host
209.165.201.10

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) [ポリシー (Policies)] > [NAT] を選択します。
- b) [+] ボタンをクリックします。
- c) 次のプロパティを設定します。
 - [タイトル (Title)] = FTPServer (または任意の別の名前)
 - [ルールの作成対象 (Create Rule For)] = [自動 NAT (Auto NAT)]
 - [タイプ (Type)] = [スタティック (Static)]
 - [送信元インターフェイス (Source Interface)] = 内部 (inside)。
 - [宛先インターフェイス (Destination Interface)] = [外部 (outside)]
 - [元のアドレス (Original Address)] = ftp_server のネットワーク オブジェクト (ftp_server network object)。
 - [変換済みアドレス (Translated Address)] = ftp_server_outside のネットワーク オブジェクト (ftp_server_outside network object)。
 - [詳細オプション (Advanced Options)] タブで、[このルールに一致する DNS 応答を変換する (Translate DNS replies that match this rule)] を選択します。

Add NAT Rule ?

Title

Create Rule for

Auto NAT
▼

Status

Auto NAT rules translate a specified host or network address regardless of its appearance as the source or destination address of a packet. These rules are automatically ordered and placed in the Auto NAT section.

Placement

Automatically placed in Auto NAT rules

Type

Static
▼

Packet Translation

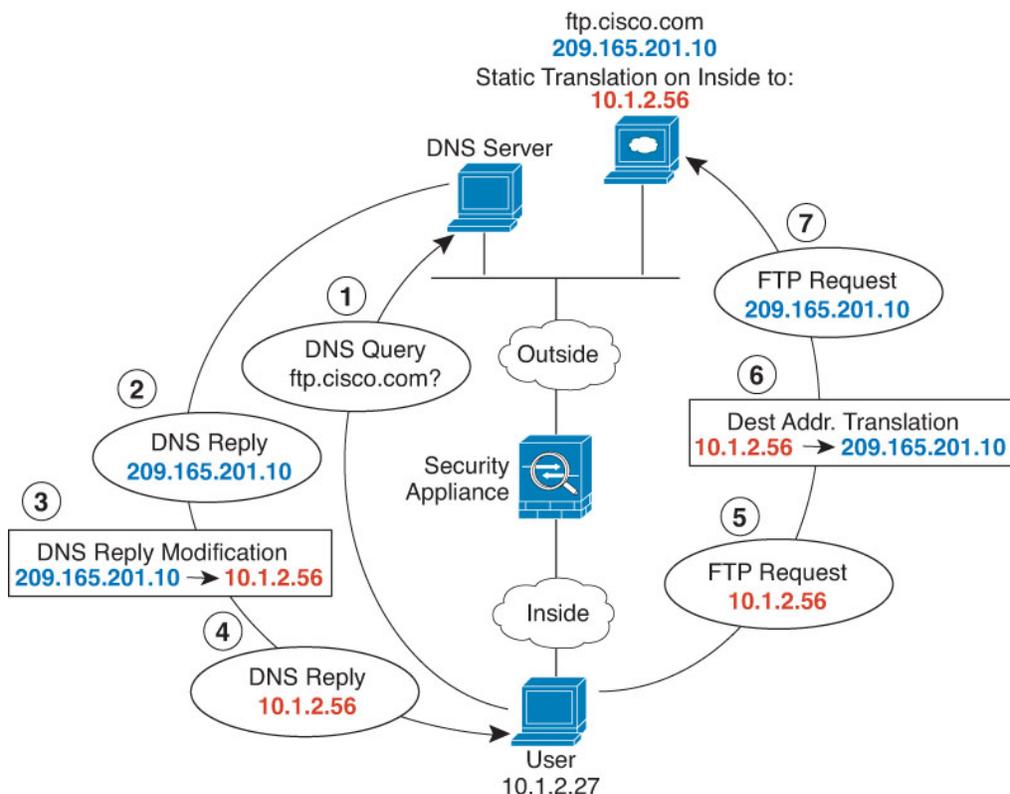
Advanced Options

ORIGINAL PACKET		TRANSLATED PACKET	
<p>Source Interface</p> <div style="border: 1px solid #ccc; padding: 2px; display: flex; align-items: center;"> inside ▼ </div>	<p>Destination Interface</p> <div style="border: 1px solid #ccc; padding: 2px; display: flex; align-items: center;"> outside </div>		
<p>Original Address</p> <div style="border: 1px solid #ccc; padding: 2px; display: flex; align-items: center;"> ftp_server ▼ </div>	<p>Translated Address</p> <div style="border: 1px solid #ccc; padding: 2px; display: flex; align-items: center;"> ftp_server_outside ▼ </div>		
<p>Original Port</p> <div style="border: 1px solid #ccc; padding: 2px; display: flex; align-items: center;"> Any ▼ </div>	<p>Translated Port</p> <div style="border: 1px solid #ccc; padding: 2px; display: flex; align-items: center;"> Any </div>		

- d) [OK] をクリックします。

DNS 応答修正：ホスト ネットワーク上の DNS サーバー

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 (209.165.201.10) 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。



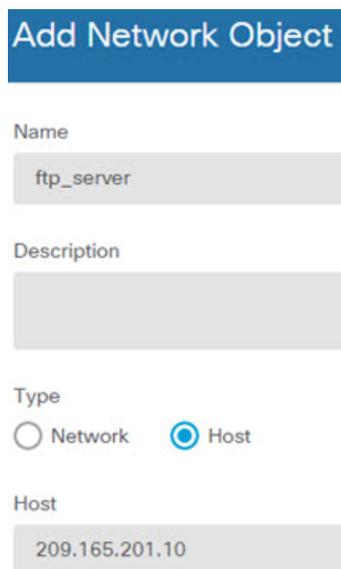
(注) この例は、内部インターフェイスがブリッジグループインターフェイス (BVI) ではなく、標準のルーテッドインターフェイスであることを前提としています。内部インターフェイスが BVI の場合、各メンバーインターフェイスのルールを複製する必要があります。

手順

ステップ 1 FTP サーバのネットワーク オブジェクトを作成します。

- [オブジェクト (Objects)] を選択します。
- 目次から [ネットワーク (Network)] を選択し、[+] をクリックします。
- 実際の FTP サーバアドレスを定義します。

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



Add Network Object

Name
ftp_server

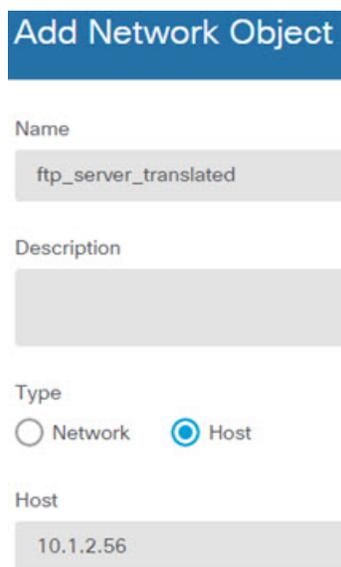
Description

Type
 Network Host

Host
209.165.201.10

- d) **[OK]** をクリックします。
- e) **[+]** 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 (Host)] を選択して、ホストアドレス 10.1.2.56 を入力します。



Add Network Object

Name
ftp_server_translated

Description

Type
 Network Host

Host
10.1.2.56

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) **[ポリシー (Policies)] > [NAT]** を選択します。
- b) **[+]** ボタンをクリックします。

c) 次のプロパティを設定します。

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

Add NAT Rule

Title: FTPServer Create Rule for: Auto NAT Status:

Auto NAT rules translate a specified host or network address regardless of its appearance as the source or destination address of a packet. These rules are automatically ordered and placed in the Auto NAT section.

Placement: Automatically placed in Auto NAT rules Type: Static

Packet Translation Advanced Options

ORIGINAL PACKET		TRANSLATED PACKET	
Source Interface	outside	Destination Interface	inside
Original Address	ftp_server	Translated Address	ftp_server_transla
Original Port	Any	Translated Port	Any

d) [OK] をクリックします。

DNS 応答修正 : ホスト ネットワーク上の DNS サーバー

翻訳について

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