



Firepower Threat Defense 用のネットワーク アドレス変換 (NAT)

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

- [NAT を使用する理由 \(1 ページ\)](#)
- [NAT の基本 \(2 ページ\)](#)
- [NAT のガイドライン \(11 ページ\)](#)
- [脅威に対する防御のための NAT の設定 \(17 ページ\)](#)
- [IPv6 ネットワークの変換 \(62 ページ\)](#)
- [NAT のモニタリング \(73 ページ\)](#)
- [NAT の例 \(73 ページ\)](#)

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 を設定できるからです。

NAT の他の機能は、次のとおりです。

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



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

NAT の基本

ここでは、NAT の基本について説明します。

NAT の用語

このマニュアルでは、次の用語を使用しています。

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



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

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

NAT タイプ

NAT は、次の方法を使用して実装できます。

- **ダイナミック NAT**：実際の IP アドレスのグループが、（通常は、より小さい）マッピング IP アドレスのグループに先着順でマッピングされます。実際のホストだけがトラフィックを開始できます。[ダイナミック NAT \(22 ページ\)](#) 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 \(29 ページ\)](#) 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 \(38 ページ\)](#) 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 \(49 ページ\)](#) を参照してください。

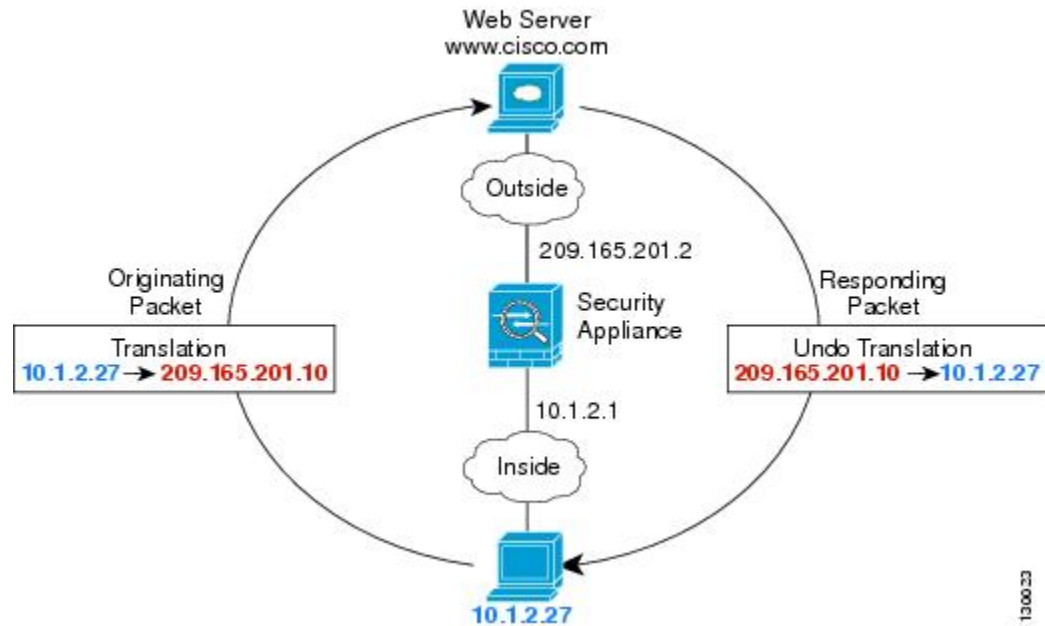
ルーテッドモードとトランスペアレントモードの NAT

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

ルーテッドモードの NAT

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

図 1: NAT の例 : ルーテッド モード



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

トランスペアレント モードまたはブリッジ グループ内の NAT

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

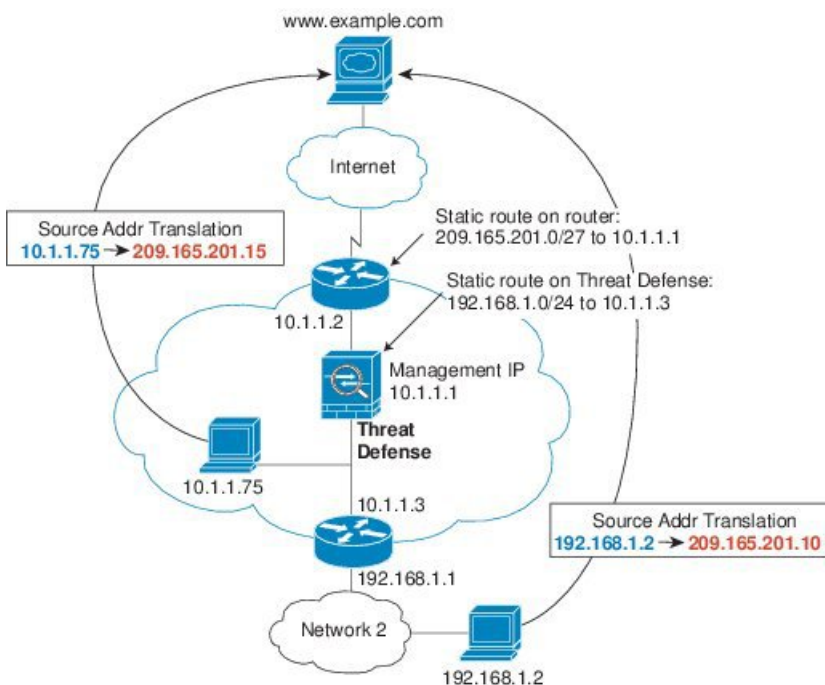
トランスペアレント モードまたは同じブリッジ グループのメンバー間のルーテッドモードの NAT には、以下の要件および制限があります。

- インターフェイスに接続されている IP アドレスがないため、マッピングされたアドレスがブリッジ グループ メンバーのインターフェイスである場合、インターフェイス PAT を設定することはできません。
- ARP インスペクションはサポートされていません。さらに、何らかの理由で /Firepower Threat Defense デバイスの片側にあるホストから /Firepower Threat Defense デバイスのもう片側にあるホストに ARP 要求が送信され、送信側ホストの実アドレスが同じサブネット上の別のアドレスにマップされている場合、その実アドレスは ARP 要求で表示されたままになります。

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

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

図 2: NAT の例: トランスペアレント モード



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

/自動 NAT および/手動 NAT

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

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

/自動 NAT

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

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

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

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

/手動 NAT

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



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

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

/自動 NAT と /手動 NAT の比較

自動 NAT と手動 NAT の主な違いは、次のとおりです。

- 実アドレスの定義方法。
 - 自動 NAT : NAT ルールがネットワーク オブジェクトのパラメータとなります。ネットワーク オブジェクトの IP アドレスは、元の (実) アドレスとして機能します。
 - /手動 NAT : 実アドレスおよびマッピングアドレスの両方に対し、ネットワーク オブジェクトまたはネットワーク オブジェクト グループを特定します。この場合、NAT はネットワーク オブジェクトのパラメータではありません。ネットワーク オブジェクトまたはグループが、NAT 設定のパラメータとなります。実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 : 個々のルールは、パケットの送信元または宛先のどちらかに適用されます。このため、送信元 IP アドレス、宛先 IP アドレスにそれぞれ 1 つずつ、計 2 つのルールが使用される場合もあります。このような 2 つのルールを 1 つに結合し、送信元/宛先ペアに対して特定の変換を強制することはできません。
 - /手動 NAT : 単一のルールが送信元と宛先の両方を変換します。1 つのパケットは 1 つのルールにしか一致せず、以降のルールはチェックされません。オプションの宛先アドレスを設定していない場合でも、パケットは 1 つの /手動 NAT ルールのみ的一致します。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 テーブル内で自動的に順序が決まります。
 - /手動 NAT : NAT テーブル内で手動で順序が決めます (/自動 NAT ルールの前または後)。

NAT ルールの順序

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

表 1: NAT ルール テーブル

テーブルのセクション	ルール タイプ	セクション内のルールの順序
セクション 1	/手動 NAT	設定に登場する順に、最初の一致ベースで適用されます。最初の一致が適用されるため、一般的なルールの前に固有のルールが来るようにする必要があります。そうしない場合、固有のルールを期待どおりに適用できない可能性があります。デフォルトでは、/手動 NAT ルールはセクション 1 に追加されます。
セクション 2	/自動 NAT	セクション 1 で一致が見つからない場合、セクション 2 のルールが次の順序で適用されます。 <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。
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。

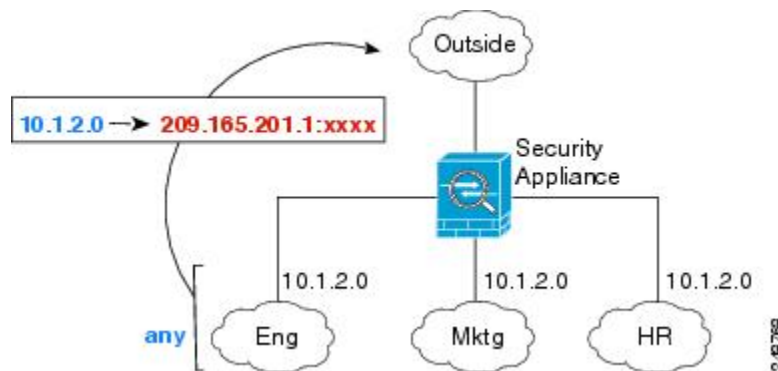
- 192.168.1.1/32 (スタティック)
- 10.1.1.0/24 (スタティック)
- 192.168.1.0/24 (スタティック)
- 172.16.1.0/24 (ダイナミック) (オブジェクト abc)
- 172.16.1.0/24 (ダイナミック) (オブジェクト def)
- 192.168.1.0/24 (ダイナミック)

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 3: 任意のインターフェイスの指定



ただし、「任意」のインターフェイスの概念は、ブリッジグループメンバーインターフェイスには適用されません。「任意」のインターフェイスを指定すると、すべてのブリッジグループ

ブ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。



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

NAT のルーティング設定

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

パケットを送信する際の出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 では、宛先インターフェイスを指定していてもルート ルックアップを使用するオプションがあります。

必要なルート設定のタイプは、次のトピックで説明するように、マッピングアドレスのタイプによって異なります。

マッピング インターフェイスと同じネットワーク上のアドレス

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



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

固有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、/Firepower Threat Defense デバイス を指しているマッピング アドレスのスタティック ルートが必要です。

また、ルーテッドモードの場合、宛先ネットワーク上の IP アドレスをゲートウェイとして使用して、マッピングアドレスの /Firepower Threat Defense デバイス にスタティック ルートを設定し、ルーティングプロトコルを使用してルートを再配布することができます。たとえば、内部ネットワーク (10.1.1.0/24) には NAT を使用して、マッピング IP アドレス 209.165.201.5 を使用する場合、209.165.201.5 255.255.255.255 (ホストアドレス) に対して、10.1.1.99 ゲートウェイへのスタティック ルートを設定し、これを再配布できます。

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

実際のアドレスと同じアドレス (アイデンティティ NAT)

アイデンティティ NAT のデフォルト動作で、プロキシ ARP は有効になっており、他のスタティック NAT ルールと一致します。必要に応じてプロキシ ARP を無効にすることができます。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。次に、/Firepower Threat Defense デバイスは、パケットが実際に /Firepower Threat Defense デバイス宛てでなくても、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)。/Firepower Threat Defense デバイスの ARP 応答が実際のホストの ARP 応答の前に受信された場合、トラフィックは誤って /Firepower Threat Defense デバイス に送信されます。

NAT のガイドライン

ここでは、NAT を実装するためのガイドラインについて詳細に説明します。

NAT のファイアウォール モードのガイドライン

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

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

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



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

IPv6 NAT のガイドライン

NAT では、IPv6 のサポートに次のガイドラインと制限が伴います。

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

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

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

IPv6 NAT の推奨事項

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

- NAT66 (IPv6-to-IPv6) : スタティック NAT を使用することを推奨します。ダイナミック NAT または PAT を使用できますが、IPv6 アドレスは大量にあるため、ダイナミック NAT を使用する必要がありません。リターントラフィックを許可しない場合は、スタティック NAT ルールを単一方向にできます (/手動 NAT のみ)。
- NAT46 (IPv4-to-IPv6) : スタティック NAT を使用することを推奨します。IPv6 アドレス空間は IPv4 アドレス空間よりもかなり大きいので、容易にスタティック変換に対応できます。リターントラフィックを許可しない場合は、スタティック NAT ルールを単一方向にできます (/手動 NAT のみ)。IPv6 サブネットに変換する場合 (/96 以下)、結果のマッピングアドレスはデフォルトで IPv4 埋め込み IPv6 アドレスとなります。このアドレスでは、IPv4 アドレスの 32 ビットが IPv6 プレフィックスの後に埋め込まれています。たとえば、IPv6 プレフィックスが /96 プレフィックスの場合、IPv4 アドレスは、アドレスの最後の 32 ビットに追加されます。たとえば、201b::0/96 に 192.168.1.0/24 をマッピングする場合、192.168.1.4 は 201b::0.192.168.1.4 にマッピングされます (混合表記で表示)。/64 など、より小さいプレフィックスの場合、IPv4 アドレスがプレフィックスの後に追加され、サフィックスの 0s が IPv4 アドレスの後に追加されます。また、任意で、ネット間のアドレスを変換できます。この場合、最初の IPv6 アドレスに最初の IPv4 アドレス、2 番目 IPv6 アドレスに 2 番目の IPv4 アドレス、のようにマッピングします。
- NAT64 (IPv6-to-IPv4) : IPv6 アドレスの数に対応できる十分な数の IPv4 アドレスがない場合があります。大量の IPv4 変換を提供するためにダイナミック PAT プールを使用することを推奨します。

インスペクション対象プロトコルに対する NAT サポート

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

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

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



- (注) NAT の書き換えは、リストされているポートでのみサポートされます。これらのプロトコルの一部では、ネットワーク解析ポリシーを使用してインスペクションを他のポートに拡張できますが、NAT の書き換えはこれらのポートに拡張されません。これには、DCERPC、DNS、FTP、および Sun RPC のインスペクションが含まれます。非標準ポートでこれらのプロトコルを使用する場合は、接続で NAT を使用しないでください。

表 2: NAT のサポート対象アプリケーションインスペクション

Application	インスペクション対象プロトコル、ポート	NAT に関する制限事項	作成済みのピンホール
DCERPC	TCP/135	NAT64 なし。	○
DNS over UDP	UDP/53	NAT サポートは、WINS 経由の名前解決では使用できません。	なし
ESMTP	TCP/25	NAT64 なし。	なし
FTP	TCP/21	制限なし。 (クラスタリング) スタティック PAT なし。	○
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	(クラスタリング) スタティック PAT なし。 拡張 PAT なし。 NAT64 なし。	○

Application	インスペクション対象 プロトコル、ポート	NAT に関する制限事項	作成済みのピンホール
ICMP ICMP エラー	ICMP (デバイス インター フェイスに送信される ICMP トラフィックの インスペクションは実 行されません。)	制限なし。	なし
IP オプション	RSVP	NAT64 なし。	なし
NetBIOS Name Server over IP	UDP/137、138 (送信元 ポート)	拡張 PAT なし。 NAT64 なし。	なし
RSH	TCP/514	PAT なし。 NAT64 なし。 (クラスタリング) スタティック PAT なし。	○
RTSP	TCP/554 (HTTP クローキング は処理しません。)	拡張 PAT なし。 NAT64 なし。 (クラスタリング) スタティック PAT なし。	○
SIP	TCP/5060 UDP/5060	拡張 PAT なし。 NAT64 または NAT46 なし。 (クラスタリング) スタティック PAT なし。	○
Skinny (SCCP)	TCP/2000	拡張 PAT なし。 NAT64、NAT46、または NAT66 なし。 (クラスタリング) スタティック PAT なし。	○
SQL*Net (バージョン 1、2)	TCP/1521	拡張 PAT なし。 NAT64 なし。 (クラスタリング) スタティック PAT なし。	○
Sun RPC	TCP/111 UDP/111	拡張 PAT なし。 NAT64 なし。	○
TFTP	UDP/69	NAT64 なし。 (クラスタリング) スタティック PAT なし。 ペイロード IP アドレスは変換されません。	○

Application	インスペクション対象 プロトコル、ポート	NAT に関する制限事項	作成済みのピンホール
XDMCP	UDP/177	拡張 PAT なし。 NAT64 なし。 (クラスタリング) スタティック PAT なし。	○

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。
- (/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 に適用されます。
- NAT 設定を変更したときに、既存の変換がタイムアウトするまで待たずに新しい NAT 設定が使用されるようにするには、デバイスの CLI で **clear xlate** コマンドを使用して変換テーブルを消去できます。ただし、変換テーブルを消去すると、変換を使用している現在の接続がすべて切断されます。



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

- 1 つのオブジェクトグループに IPv4 と IPv6 の両方のアドレスを含めることはできません。オブジェクトグループには、1 つのタイプのアドレスのみを含める必要があります。
- (/手動 NAT のみ) NAT ルールで送信元アドレスとして **any** を使用する場合、「any」トラフィックの定義 (IPv4 と IPv6) はルールによって異なります。/Firepower Threat Defense デバイスがパケットに対して NAT を実行する前に、パケットが IPv6-to-IPv6 または IPv4-to-IPv4 である必要があります。この前提条件では、/Firepower Threat Defense デバイ

スが、NAT ルールの **any** の値を決定できます。たとえば、「any」から IPv6 サーバへのルールを設定しており、このサーバが IPv4 アドレスからマップされている場合、**any** は「任意の IPv6 トラフィック」を意味します。「any」から「any」へのルールを設定しており、送信元をインターフェイス IPv4 アドレスにマッピングする場合、マッピングされたインターフェイスアドレスによって宛先も IPv4 であることが示されるため、**any** は「任意の IPv4 トラフィック」を意味します。

- 同じマッピング オブジェクトやグループを複数の NAT ルールで使用できます。
- マッピング IP アドレス プールに、次のアドレスを含めることはできません。
 - マッピング インターフェイスの IP アドレス。ルールに "any" インターフェイスを指定すると、すべてのインターフェイスの IP アドレスが拒否されます。インターフェイス PAT (ルーテッドモードのみ) の場合は、インターフェイスアドレスの代わりにインターフェイス名を指定します。
 - フェールオーバー インターフェイスの IP アドレス。
 - (トランスペアレント モード) 管理 IP アドレス。
 - (ダイナミック NAT) VPN が有効な場合は、スタンバイ インターフェイスの IP アドレス。
- スタティックおよびダイナミック NAT ポリシーでは重複アドレスを使用しないでください。たとえば、重複アドレスを使用すると、PPTP のセカンダリ接続がダイナミック xlate ではなくスタティックにヒットした場合、PPTP 接続の確立に失敗する可能性があります。
- 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カ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。

脅威に対する防御のための NAT の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin

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

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

割り当てられたデバイスにポリシーの特定のルールが適用されるかどうかは、ルールで 사용되는インターフェイスオブジェクト (セキュリティゾーンまたはインターフェイスグループ) によって決定されます。インターフェイスオブジェクトにデバイスのインターフェイスが1つ以上含まれている場合、ルールがデバイスに導入されます。したがって、注意深くインターフェイスオブジェクトを設計することで、単一の共有ポリシー内のデバイスのサブセットに適用されるルールを設定できます。「任意」のインターフェイスオブジェクトに適用されるルールは、すべてのデバイスに導入されます。

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

手順

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

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

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

- 既存の脅威防御 NAT ポリシーを編集するには、編集アイコン (✎) をクリックします。このページには、Firepower Threat Defense では使用されない Firepower NAT ポリシーも表示されます。

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 \(6 ページ\)](#) を参照してください。

ステップ 4 デバイスごとにカスタマイズするルールを決定します。

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

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

詳細については、[複数のデバイスの NAT ルールのカスタマイズ \(19 ページ\)](#) を参照してください。

ステップ 5 次の項で説明するルールを作成します。

- [ダイナミック NAT \(22 ページ\)](#)
- [ダイナミック PAT \(29 ページ\)](#)
- [スタティック NAT \(38 ページ\)](#)
- [アイデンティティ NAT \(49 ページ\)](#)

ステップ 6 NAT ポリシーとルールを管理します。

ポリシーとそのルールを管理するには、次のことを行います。

- ポリシーの名前または説明を編集するには、これらのフィールドをクリックし、変更を入力して、フィールドの外側をクリックします。
- 特定のデバイスに適用されるルールのみを表示するには、[デバイスによるフィルタ (Filter by Device)] をクリックし、目的のデバイスを選択します。ルールがデバイスのインターフェイスを含むインターフェイスオブジェクトを使用している場合、そのデバイスにルールが適用されます。
- ポリシーが割り当てられているデバイスを変更するには、[ポリシー割り当て (Policy Assignments)] リンクをクリックし、必要に応じて選択したデバイスリストを変更します。
- ルールが有効であるか、または無効であるかを変更するには、ルールを右クリックし、[状態 (State)] コマンドから目的のオプションを選択します。これらのコントロールを使用して、ルールを削除しないで一時的に無効にすることができます。
- ルールを編集するには、ルールの編集アイコン (✎) をクリックします。
- ルールを削除するには、ルールの削除アイコン (🗑️) をクリックします。

ステップ 7 [保存 (Save)] をクリックします。

これで、[展開 (Deploy)] をクリックし、割り当てたデバイスにポリシーを展開できます。変更は、実際に展開するまで有効化されません。

複数のデバイスの NAT ルールのカスタマイズ

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

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

次のような例が考えられます。

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

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

手順

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

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

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

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

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

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

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

- i) [保存 (Save)] をクリックします。

ステップ 4 NAT ルールを設定します。

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

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

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

e) [変換 (Translation)] タブで、次の項目を設定します。

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

f) [保存 (Save)] をクリックします。

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

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

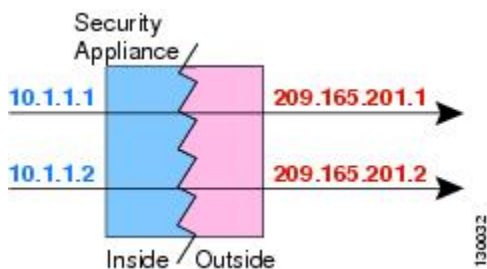
ダイナミック NAT では、実際のアドレスのグループは、宛先ネットワーク上でルーティング可能なマッピングアドレスのプールに変換されます。マッピングされたプールにあるアドレスは、通常、実際のグループより少なくなります。変換対象のホストが宛先ネットワークにアクセスすると、NATは、マッピングされたプールからIPアドレスをそのホストに割り当てます。変換は、実際のホストが接続を開始したときにだけ作成されます。変換は接続が継続している間だけ有効であり、変換がタイムアウトすると、そのユーザは同じIPアドレスを保持しません。したがって、アクセスルールでその接続が許可されている場合でも、宛先ネットワークのユー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

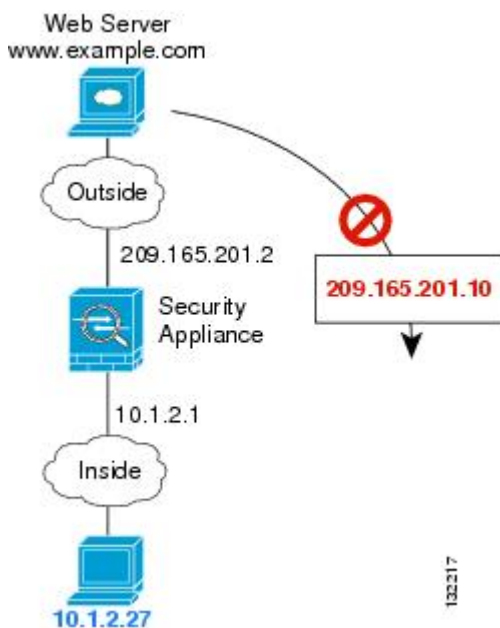
次の図に、一般的なダイナミック NAT のシナリオを示します。実際のホストだけが NAT セッションを作成でき、応答トラフィックが許可されます。

図 4: 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 5: マッピングアドレスへの接続開始を試みているリモートホスト



ダイナミック NAT の欠点と利点

ダイナミック NAT には、次の欠点があります。

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

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

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

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

- GRE バージョン 0 などのように、オーバーロードするためのポートがない IP プロトコルでは機能しません。
- 一部のマルチメディアアプリケーションなどのように、1つのポート上にデータストリームを持ち、別のポート上に制御パスを持ち、公開規格ではないアプリケーションでも機能しません。

ダイナミック自動 NAT の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin

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

始める前に

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

- [元の送信元 (Original Source)] : これはネットワーク オブジェクト (グループではない) でなければならず、ホスト、範囲、またはサブネットも可能です。
- [変換済み送信元 (Translated Source)] : ネットワーク オブジェクトまたはグループを指定できますが、サブネットを含めることはできません。グループに IPv4 アドレスと IPv6 アドレスの両方を含めることはできません。1つのタイプだけ含める必要があります。グループに範囲とホスト IP アドレスの両方が含まれている場合、範囲はダイナミック NAT に使用され、ホスト IP アドレスは PAT のフォールバックとして使用されます。

手順

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

ステップ 2 次のいずれかを実行します。

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

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

ステップ 3 基本ルールのオプションを設定します。

- [NAT ルール (NAT Rule)] : [自動 NAT ルール (Auto NAT Rule)] を選択します。
- [タイプ (Type)] : [動的 (Dynamic)] を選択します。

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

- [送信元インターフェイス オブジェクト (Source Interface Objects)]、[宛先インターフェイス オブジェクト (Destination Interface Objects)] : (ブリッジグループ メンバー インターフェイスの場合に必要な) **DestinationSource**

ステップ 5 [一般 (General)] [変換 (Translation)] タブで、次のオプションを設定します。

- [元の送信元 (Original Source)] : 変換するアドレスを含むネットワーク オブジェクト。
- [変換済み送信元 (Translated Source)] : マッピングアドレスを含むネットワーク オブジェクトまたはグループ。

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

- [このルールと一致する DNS 応答を変換 (Translate DNS replies that match this rule)] : 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 \(103 ページ\)](#) を参照してください。
- [インターフェイス PAT へのフォールスルー (宛先インターフェイス) (Fallthrough to Interface PAT (Destination Interface))] : その他のマッピング アドレスがすでに割り当てられている場合に、宛先インターフェイスの IP アドレスをバックアップ方式として使用するかどうかを指定します (インターフェイス PAT フォールバック)。このオプションは、ブリッジグループのメンバーではない宛先インターフェイスを選択した場合にのみ使用できます。インターフェイスの IPv6 アドレスを使用するには、[IPv6] オプションも選択します。
- [IPv6] : インターフェイス PAT に宛先インターフェイスの IPv6 アドレスを使用するかどうかを指定します。

ステップ 7 [保存 (Save)] をクリックしてルールを追加します。

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

ダイナミック手動 NAT の設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin

自動 NAT では要件を満たせない場合は、ダイナミック手動 NAT ルールを使用します。たとえば、宛先に応じて異なる変換をしたい場合などです。ダイナミック NAT は、宛先ネットワーク上でルーティング可能な別の IP アドレスにアドレスを変換します。

始める前に

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

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

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 (Original Destination)] および [変換済み宛先 (Translated Destination)] のネットワーク オブジェクトを作成できます。

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

手順

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

ステップ 2 次のいずれかを実行します。

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

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

ステップ 3 基本ルールのオプションを設定します。

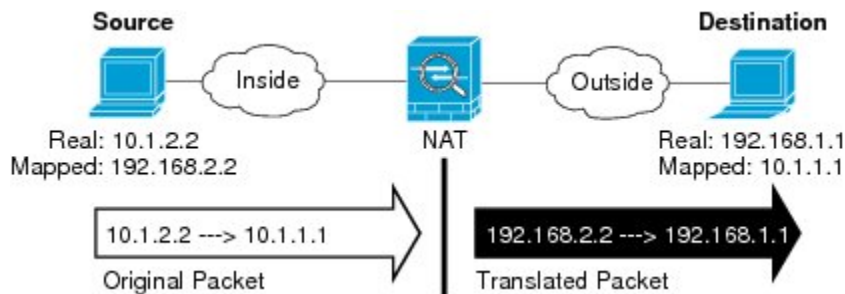
- [NAT ルール (NAT Rule)]: [手動 NAT ルール (Manual NAT Rule)] を選択します。
- [タイプ (Type)]: [ダイナミック (Dynamic)] を選択します。この設定は送信元アドレスにのみ適用されます。宛先アドレスの変換を定義している場合、変換は常に静的に行われます。
- [有効にする (Enable)]: ルールをアクティブにするかどうかを指定します。ルールページの右クリックメニューを使用して、後でルールをアクティブ化または非アクティブ化することができます。
- [挿入 (Insert)]: ルールを追加する場所を指定します。ルールは、カテゴリ (自動 NAT ルールの前か後) 、または指定したルール番号の上か下に挿入できます。

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

- [送信元インターフェイスオブジェクト (Source Interface Objects)]、[宛先インターフェイスオブジェクト (Destination Interface Objects)]: (共有ポリシーのみ) 。[送信元ゾーン (Source Zone)]、[宛先ゾーン (Destination Zone)]: (トランスペアレントファイアウォールモードの場合に必要) 。この NAT ルールが適用されるインターフェイスを識別するセキュリティゾーン。[送信元 (Source)] は、デバイスに入るトラフィックが通過する実際のインターフェイスを含むゾーン。[宛先 (Destination)] は、デバイスから出るトラフィックが通過するマッピングインターフェイスを含むゾーン。デフォルトでは、すべてのインターフェイスにルールが適用されます ([すべて (Any)]) 。(ブリッジグループメンバーインターフェイスの場合に必要) **Source Zone Destination Zone Source Destination Any**

ステップ 5 ([変換 (Translation)] タブで次を実行します。) 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。



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

[送信元インターフェイス IP (Source Interface IP)] を選択して、送信元インターフェイスの元の宛先 ([すべて (Any)]) は選択不可) をベースにすることができます。このオプションを選択する場合、変換済みの宛先オブジェクトも選択する必要があります。宛先ア

ドレスに対して、ポート変換を設定したスタティック インターフェイス NAT を実装するには、このオプションを選択し、宛先ポートに適したポートオブジェクトも選択します。

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

- [変換済み送信元 (Translated Source)]: マッピングアドレスを含むネットワーク オブジェクトまたはグループ。
- [変換済み宛先 (Translated Destination)]: (オプション)。変換された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) サービス変換の宛先サービスポートを特定します。[元の宛先ポート (Original Destination Port)]、[変換済み宛先ポート (Translated Destination Port)]。

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

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

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

- (送信元変換の場合のみ) [このルールと一致する DNS 応答を変換 (Translate DNS replies that match this rule)]: DNS 応答の IP アドレスを変換するかどうかを指定します。マッピング インターフェイスから実際のインターフェイスに移動する DNS 応答の場合、アドレス (IPv4 A または IPv6 AAAA) レコードはマッピングされた値から実際の値に書き換えられます。反対に、実際のインターフェイスからマッピング インターフェイスに移動する DNS 応答の場合、レコードは実際の値からマッピングされた値に書き換えられます。このオプションは特殊な状況で使用され、書き換えにより A レコードと AAAA レコード間でも変換が行われる NAT64/46 変換のために必要なことがあります。詳細については、[NAT を使用した DNS クエリと応答の書き換え \(103 ページ\)](#) を参照してください。
- [インターフェイス PAT へのフォールスルー (宛先インターフェイス) (Fallthrough to Interface PAT (Destination Interface))]: その他のマッピング アドレスがすでに割り当てられている場合に、宛先インターフェイスの IP アドレスをバックアップ方式として使用するかどうかを指定します (インターフェイス PAT フォールバック)。このオプションは、ブリッジグループのメンバーではない宛先インターフェイスを選択した場合にのみ使用できます。インターフェイスの IPv6 アドレスを使用するには、[IPv6] オプションも選択します。
- [IPv6] : [IPv6] : インターフェイス PAT に宛先インターフェイスの IPv6 アドレスを使用するかどうかを指定します。インターフェイス PAT に宛先インターフェイスの IPv6 アドレスを使用するかどうかを指定します。 **IPv6**

ステップ 9 [保存 (Save)] をクリックしてルールを追加します。

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

ダイナミック PAT

次のトピックでは、ダイナミック PAT について説明します。

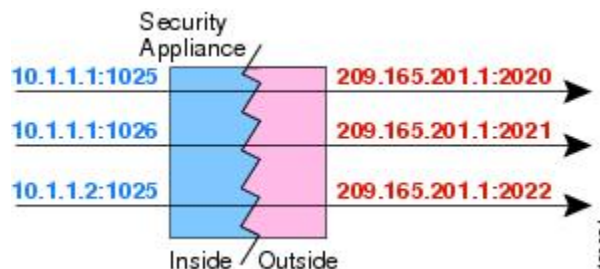
ダイナミック PAT について

ダイナミック PAT では、実際のアドレスおよび送信元ポートが 1 つのマッピング アドレスおよび固有のポートに変換されることによって、複数の実際のアドレスが 1 つのマッピング IP アドレスに変換されます。使用できる場合、実際の送信元ポート番号がマッピングポートに対して使用されます。ただし、実際のポートが使用できない場合は、デフォルトで、マッピングポートは実際のポート番号と同じポート範囲 (0 ~ 511、512 ~ 1023、および 1024 ~ 65535) から選択されます。そのため、1024 よりも下のポートでは、小さい PAT プールのみを使用できます。下位ポート範囲を使用するトラフィックが数多くある場合は、サイズが異なる 3 つの層の代わりにフラットなポート範囲を使用するように指定できます。

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

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

図 6: ダイナミック PAT



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

接続の有効期限が切れると、ポート変換も有効期限切れになります。

ダイナミック PAT の欠点と利点

ダイナミック PAT を使用すると、単一のマッピング アドレスを使用できるため、ルーティング可能なアドレスを節約できます。さらに、Firepower Threat Defense デバイス インターフェイスの IP アドレスを PAT アドレスとして使用できます。

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

ダイナミック PAT は、制御パスとは異なるデータ ストリームを持つ一部のマルチメディア アプリケーションでは機能しません。詳細については、[インスペクション対象プロトコルに対する NAT サポート \(13 ページ\)](#) を参照してください。

ダイナミック PAT によって、単一の IP アドレスから送信されたように見える数多くの接続が作成されることがあります。この場合、このトラフィックはサーバで DoS 攻撃として解釈される可能性があります。アドレスの PAT プールを設定し、PAT アドレスのラウンドロビン割り当てを使用することで、この状況を軽減することができます。

PAT プール オブジェクトのガイドライン

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

PAT プールの場合

- 使用できる場合、実際の送信元ポート番号がマッピングポートに対して使用されます。ただし、実際のポートが使用できない場合は、デフォルトで、マッピングポートは実際のポート番号と同じポート範囲 (0 ~ 511、512 ~ 1023、および 1024 ~ 65535) から選択されます。そのため、1024 よりも下のポートでは、小さい PAT プールのみを使用できます。下位ポート範囲を使用するトラフィックが数多くある場合は、サイズが異なる3つの層の代わりにフラットなポート範囲を使用するように指定できます。1024 ~ 65535 または 1 ~ 65535 です。
- 同じ PAT プール オブジェクトを2つの異なるルールの中で使用する場合は、必ず同じオプションを各ルールに指定してください。たとえば、1つのルールで拡張 PAT およびフラットな範囲が指定される場合は、もう一方のルールでも拡張 PAT およびフラットな範囲が指定される必要があります。

PAT プールの拡張 PAT の場合

- 多くのアプリケーション インスペクションでは、拡張 PAT はサポートされていません。
- ダイナミック PAT ルールに対して拡張 PAT をイネーブルにする場合、PAT プールのアドレスを、ポート トランスレーションルールを持つ別のスタティック NAT の PAT アドレスとしても使用することはできません。たとえば、PAT プールに 10.1.1.1 が含まれている場合、PAT アドレスとして 10.1.1.1 を使用する、ポート トランスレーションルールを持つスタティック NAT は作成できません。

- PAT プールを使用し、フォールバックのインターフェイスを指定する場合、拡張 PAT を使用できません。
- ICE または TURN を使用する VoIP 配置では、拡張 PAT を使用しないでください。ICE および TURN は、すべての宛先に対して同じであるために PAT バインディングに依存しています。

PAT プールのラウンドロビン方式の場合

- ホストに既存の接続がある場合は、そのホストからの以降の接続は同じ PAT IP アドレスを使用します (ポートが使用可能である場合)。ただし、この「粘着性」は、フェールオーバーが発生すると失われます。デバイスがフェールオーバーすると、ホストからの後の接続では最初の IP アドレスが使用されない場合があります。
- ラウンドロビンでは、特に拡張 PAT と組み合わせた場合に、大量のメモリが消費されます。NAT プールはマッピングされるプロトコル/IP アドレス/ポート範囲ごとに作成されるため、ラウンドロビンでは数多くの同時 NAT プールが作成され、メモリが使用されます。拡張 PAT では、さらに多くの同時 NAT プールが作成されます。

ダイナミック自動 PAT の設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin

ダイナミック自動 PAT ルールを使用して、複数の IP アドレスのみに変換するのではなく、固有の IP アドレスとポートの組み合わせにアドレスを変換します。1 つのアドレス (宛先インターフェイスまたは他のアドレスのいずれか) に変換するか、またはたくさんの有効な変換を提供するために、アドレスの PAT プールを使用します。

始める前に

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

- [元の送信元 (Original Source)] : これはネットワーク オブジェクト (グループではない) でなければならず、ホスト、範囲、またはサブネットも可能です。
- [変換済み送信元 (Translated Source)] : PAT アドレスを指定するオプションは次のとおりです。
 - [宛先インターフェイス (Destination Interface)] : 宛先インターフェイスのアドレスを使用するには、ネットワーク オブジェクトは必要ありません。

- [単一 PAT アドレス (Single PAT address)]: 単一のホストを含むネットワーク オブジェクトを作成します。
- [PAT プール (PAT pool)]: 範囲を含むネットワーク オブジェクトを作成するか、またはホスト、範囲あるいはその両方を含むネットワーク オブジェクト グループを作成します。サブネットを含めることはできません。グループに IPv4 アドレスと IPv6 アドレスの両方を含めることはできません。1つのタイプだけ含める必要があります。

手順

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

ステップ 2 次のいずれかを実行します。

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

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

ステップ 3 基本ルールのオプションを設定します。

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

ステップ 4 [インターフェイス オブジェクト (Interface Objects)] タブで、以下のオプションを設定します。

- [送信元インターフェイス オブジェクト (Source Interface Objects)]、[宛先インターフェイス オブジェクト (Destination Interface Objects)]: (ブリッジグループメンバー インターフェイスの場合に必要な) **DestinationSource**

ステップ 5 [一般 (General)] [変換 (Translation)] タブで、次のオプションを設定します。

- [元の送信元 (Original Source)]: 変換するアドレスを含むネットワーク オブジェクト。
- [変換済み送信元 (Translated Source)]: 以下のいずれかになります。
 - (インターフェイス PAT)。宛先のアドレスのインターフェイスを使用するには、[インターフェイス (Interface)] > [宛先インターフェイス IP (Destination Interface IP)] を選択します。また特定の宛先インターフェイス オブジェクトを選択する必要もあります。インターフェイスの IPv6 アドレスを使用するには、[詳細 (Advanced)] タブで [IPv6] オプションを選択する必要もあります。PAT プールの設定ステップを飛ばします。
 - 宛先インターフェイスのアドレス以外の単一アドレスを使用する場合は、そのために作成したホスト ネットワーク オブジェクトを選択します。PAT プールの設定ステップを飛ばします。

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

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

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

または、インターフェイス PAT を実装するもう 1 つの方法として、[インターフェイス (Interface)] [宛先インターフェイス IP (Destination Interface IP)] を選択します。

- c) (オプション) 必要に応じて、次のオプションを選択します。
 - [ラウンドロビン割り当てを使用 (Use Round Robin Allocation)] : アドレスとポートをラウンドロビン形式で割り当てます。デフォルトではラウンドロビンは使用されず、1 つの PAT アドレスのポートがすべて割り当てられてから次の PAT アドレスが使用されます。ラウンドロビン方式では、プール内の各 PAT アドレスから 1 つずつアドレスとポートが割り当てられると、また最初のアドレスに戻り、次に 2 番目のアドレスという順に使用されます。
 - [拡張 PAT テーブル (Extended PAT Table)] : 拡張 PAT を使用します。拡張 PAT では、変換情報に宛先アドレスとポートを含めることで、IP アドレスごとではなく、サービスごとに 65535 個のポートが使用されます。通常、PAT 変換の作成時に宛先ポートとアドレスは考慮されないため、PAT アドレスあたり 65535 個のポートに制限されます。たとえば、拡張 PAT を使用して、192.168.1.7:23 に向かう場合の 10.1.1.1:1027 の変換、および 192.168.1.7:80 に向かう場合の 10.1.1.1:1027 の変換を作成できます。このオプションは、インターフェイス PAT またはインターフェイス PAT フォールバックで使用することはできません。
 - [フラットなポート範囲 (Flat Port Range)]、[予約済みポートを含む (Include Reserved Ports)] : TCP/UDP ポートを割り当てる際に、ポート範囲 (1024 ~ 65535) を単一のフラットな範囲として使用します。変換用のマッピングポート番号を選択する場合、PAT によって、実際の送信元ポート番号が使用されます (使用可能な場合)。ただし、このオプションを設定しないと、実際のポートが使用できない場合、デフォルトでは、実際のポート番号と同じポート範囲 (1 ~ 511、512 ~ 1023、および 1024 ~ 65535) からマッピングポートが選択されます。下位の範囲でポートが不足するのを回避するには、この設定を行います。1 ~ 65535 の範囲全体を使用するには、[予約済みポートを含む (Include Reserved Ports)] オプションも選択します。

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

- [インターフェイス PAT へのフォールスルー (宛先インターフェイス) (Fallthrough to Interface PAT (Destination Interface))] : [インターフェイス PAT へのフォールスルー (宛先インターフェイス) (Fallthrough to Interface PAT (Destination Interface))] : (ルーテッドモードのみ)。その他のマッピングアドレスがすでに割り当てられている場合に、宛先インターフェイスの IP アドレスをバックアップ方式として使用するかどうかを指定します

(インターフェイス PAT フォールバック)。このオプションは、宛先インターフェイスを選択した場合にのみ使用できます。インターフェイスの IPv6 アドレスを使用するには、[IPv6] オプションを選択します。インターフェイス PAT を変換済みアドレスまたは PAT プールとしてすでに設定している場合、このオプションは選択できません。その他のマッピングアドレスがすでに割り当てられている場合に、宛先インターフェイスの IP アドレスをバックアップ方式として使用するかどうかを指定します (インターフェイス PAT フォールバック)。このオプションは、ブリッジグループのメンバーではない宛先インターフェイスを選択した場合にのみ使用できます。インターフェイスの IPv6 アドレスを使用するには、[IPv6] オプションも選択します。

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

ステップ 8 [保存 (Save)] をクリックしてルールを追加します。

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

ダイナミック手動 PAT の設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin

自動 PAT がお客様のニーズを満たしていない場合は、ダイナミック手動 PAT ルールを使用します。たとえば、宛先に基づいて別の変換を行いたい場合に使用します。ダイナミック PAT は、複数の IP アドレスのみに変換するのではなく、固有の IP アドレスとポートの組み合わせにアドレスを変換します。1 つのアドレス (宛先インターフェイスまたは他のアドレスのいずれか) に変換するか、またはたくさんの有効な変換を提供するために、アドレスの PAT プールを使用します。

始める前に

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

- [元の送信元 (Original Source)] : これはネットワーク オブジェクトまたはグループで、ホスト、範囲、またはサブネットを含むことができます。すべての元の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 (Translated Source)] : PAT アドレスを指定するオプションは次のとおりです。

- [宛先インターフェイス (Destination Interface)] : 宛先インターフェイスのアドレスを使用するには、ネットワーク オブジェクトは必要ありません。
- [単一 PAT アドレス (Single PAT address)] : 単一のホストを含むネットワーク オブジェクトを作成します。
- [PAT プール (PAT pool)] : 範囲を含むネットワーク オブジェクトを作成するか、またはホスト、範囲あるいはその両方を含むネットワーク オブジェクト グループを作成します。サブネットを含めることはできません。

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

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

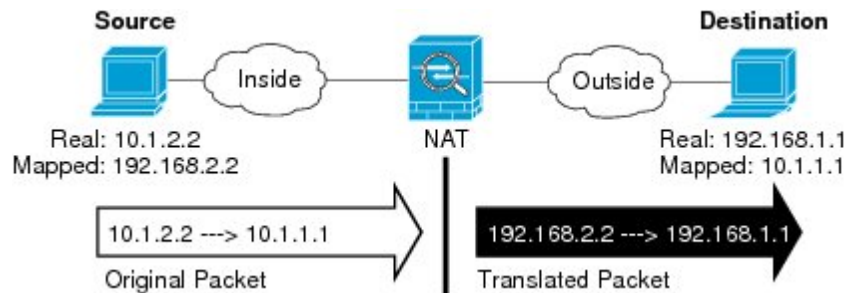
手順

-
- ステップ 1** [デバイス (Devices)] > [NAT] を選択し、Firepower Threat Defense NAT ポリシーを作成または編集します。
- ステップ 2** 次のいずれかを実行します。
- [ルールの追加 (Add Rule)] ボタンをクリックして、新しいルールを作成します。
 - 編集アイコン (✎) をクリックして、既存のルールを編集します。
- メニューを右クリックすると、ルールの切り取り、コピー、貼り付け、挿入、および削除オプションが表示されます。
- ステップ 3** 基本ルールのオプションを設定します。
- [NAT ルール (NAT Rule)] : [手動 NAT ルール (Manual NAT Rule)] を選択します。
 - [タイプ (Type)] : [ダイナミック (Dynamic)] を選択します。この設定は送信元アドレスにのみ適用されます。宛先アドレスの変換を定義している場合、変換は常に静的に行われます。
 - [有効にする (Enable)] : ルールをアクティブにするかどうかを指定します。ルール ページの右クリックメニューを使用して、後でルールをアクティブ化または非アクティブ化することができます。
 - [挿入 (Insert)] : ルールを追加する場所を指定します。ルールは、カテゴリ (自動 NAT ルールの前か後) 、または指定したルール番号の上か下に挿入できます。
- ステップ 4** [インターフェイス オブジェクト (Interface Objects)] タブで、以下のオプションを設定します。
- [送信元インターフェイス オブジェクト (Source Interface Objects)]、[宛先インターフェイス オブジェクト (Destination Interface Objects)] : (共有ポリシーのみ) 。[送信元ゾーン

[Source Zone]]、[宛先ゾーン (Destination Zone)]: (トランスペアレントファイアウォールモードの場合に必要)。この NAT ルールが適用されるインターフェイスを識別するセキュリティゾーン。[送信元 (Source)]は、デバイスに入るトラフィックが通過する実際のインターフェイスを含むゾーン。[宛先 (Destination)]は、デバイスから出るトラフィックが通過するマッピングインターフェイスを含むゾーン。デフォルトでは、すべてのインターフェイスにルールが適用されます ([すべて (Any)])。(ブリッジグループメンバーインターフェイスの場合に必要) **Source ZoneDestination ZoneSourceDestinationAny**

ステップ 5 ([変換 (Translation)]タブで次を実行します。) 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。



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

[送信元インターフェイス IP (Source Interface IP)]を選択して、送信元インターフェイスの元の宛先 ([すべて (Any)])は選択不可)をベースにすることができます。このオプションを選択する場合、変換済みの宛先オブジェクトも選択する必要があります。宛先アドレスに対して、ポート変換を設定したスタティック インターフェイス NAT を実装するには、このオプションを選択し、宛先ポートに適したポートオブジェクトも選択します。

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

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

- 宛先インターフェイスのアドレス以外の単一アドレスを使用する場合は、そのために作成したホスト ネットワーク オブジェクトを選択します。PAT プールの設定ステップを飛ばします。
- PAT プールを使用するには、[変換済み送信元 (Translated Source)] を空にしておきます。
- [変換済み宛先 (Translated Destination)]: (オプション)。変換されたパケットで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 PAT プールを使用している場合は、[PAT プール (PAT Pool)] タブを選択して、次の手順を実行します。

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

または、インターフェイス PAT を実装するもう 1 つの方法として、[インターフェイス (Interface)] [宛先インターフェイス IP (Destination Interface IP)] を選択します。

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

このオプションは、インターフェイス PAT またはインターフェイス PAT フォールバックで使用することはできません。

- [フラットなポート範囲 (Flat Port Range)]、[予約済みポートを含む (Include Reserved Ports)] : TCP/UDP ポートを割り当てる際に、ポート範囲 (1024 ~ 65535) を単一のフラットな範囲として使用します。変換用のマッピングポート番号を選択する場合、PAT によって、実際の送信元ポート番号が使用されます (使用可能な場合)。ただし、このオプションを設定しないと、実際のポートが使用できない場合、デフォルトでは、実際のポート番号と同じポート範囲 (1 ~ 511、512 ~ 1023、および 1024 ~ 65535) からマッピングポートが選択されます。下位の範囲でポートが不足するのを回避するには、この設定を行います。1 ~ 65535 の範囲全体を使用するには、[予約済みポートを含む (Include Reserved Ports)] オプションも選択します。

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

- [インターフェイス PAT へのフォールスルー (宛先インターフェイス) (Fallthrough to Interface PAT (Destination Interface))] : その他のマッピングアドレスがすでに割り当てられている場合に、宛先インターフェイスの IP アドレスをバックアップ方式として使用するかどうかを指定します (インターフェイス PAT フォールバック)。このオプションは、ブリッジグループのメンバーではない宛先インターフェイスを選択した場合にのみ使用できます。インターフェイスの IPv6 アドレスを使用するには、[IPv6] オプションも選択します。
- [IPv6] : [IPv6] : インターフェイス PAT に宛先インターフェイスの IPv6 アドレスを使用するかどうかを指定します。インターフェイス PAT に宛先インターフェイスの IPv6 アドレスを使用するかどうかを指定します。 **IPv6**

ステップ 10 [保存 (Save)] をクリックしてルールを追加します。

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

スタティック NAT

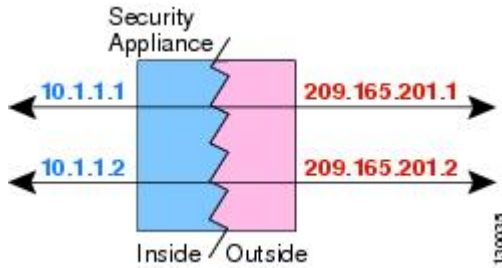
ここでは、スタティック NAT とその実装方法について説明します。

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。

次の図は、スタティック NAT の一般的な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 7:スタティック NAT



(注) 必要に応じて、双方向接続を無効にできます。

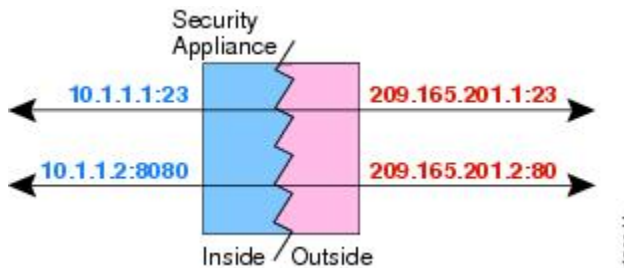
ポート変換を設定したスタティック NAT

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

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

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

図 8:ポート変換を設定したスタティック NAT の一般的なシナリオ



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

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

アイデンティティ ポート変換を設定したスタティック NAT

内部リソースへの外部アクセスを簡素化できます。たとえば、異なるポートでサービスを提供する3つの個別のサーバ (FTP、HTTP、SMTP など) がある場合は、それらのサービスにアクセスするための単一の IP アドレスを外部ユーザに提供できます。その後、アイ

デフォルトのポート変換を設定したスタティック NAT を設定し、アクセスしようとしているポートに基づいて、単一の外部 IP アドレスを実サーバの正しい IP アドレスにマッピングすることができます。サーバは標準のポート（それぞれ 21、80、および 25）を使用しているため、ポートを変更する必要はありません。

標準以外のポートのポート変換を設定したスタティック NAT

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

ポート変換を設定したスタティック インターフェイス NAT

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

一対多のスタティック NAT

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

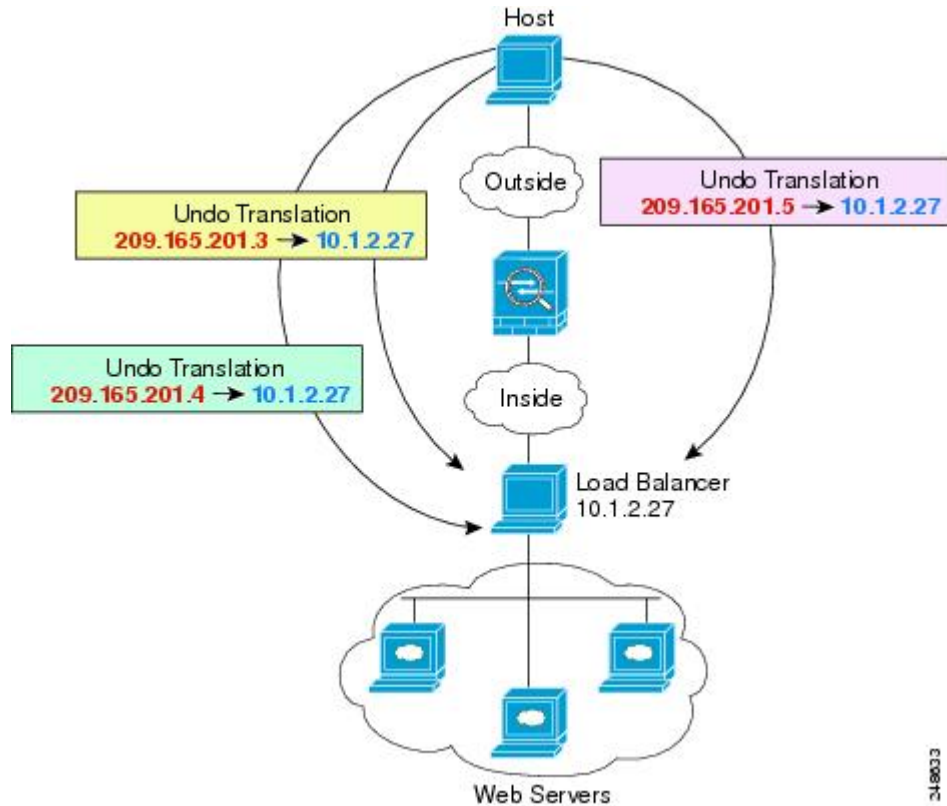
次の図に、一般的な一対多のスタティック NAT シナリオを示します。実際のホストが開始すると、常に最初のマッピングアドレスが使用されるため、実際のホスト IP/最初のマッピング IP の変換は、理論的には双方向変換のみが行われます。

図 9: 一対多のスタティック NAT



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

図 10: 一対多のスタティック NAT の例



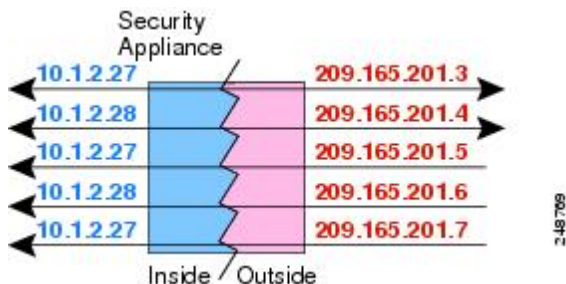
他のマッピング シナリオ (非推奨)

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

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

次の図に、一般的な少対多のスタティック NAT シナリオを示します。

図 11: 少対多のスタティック NAT



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



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

次の図に、一般的な多対少のスタティック NAT シナリオを示します。

図 12: 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

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin

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

始める前に

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

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

手順

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

ステップ 2 次のいずれかを実行します。

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

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

ステップ 3 基本ルールのオプションを設定します。

- [NAT ルール (NAT Rule)] : [自動 NAT ルール (Auto NAT Rule)] を選択します。
- [タイプ (Type)] : [スタティック (Static)] を選択します。

ステップ 4 [インターフェイス オブジェクト (Interface Objects)] タブで、以下のオプションを設定します。

- [送信元インターフェイス オブジェクト (Source Interface Objects)]、[宛先インターフェイス オブジェクト (Destination Interface Objects)] : (ブリッジグループ メンバー インターフェイスの場合に必要な) **DestinationSource**

ステップ 5 [一般 (General)] [変換 (Translation)] タブで、次のオプションを設定します。

- [元の送信元 (Original Source)] : 変換するアドレスを含むネットワーク オブジェクト。
- [変換済み送信元 (Translated Source)] : 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、[アドレス (Address)] およびマッピングされたアドレスを含むネットワーク オブジェクトまたはグループを選択します。通常、1 対 1 のマッピングでは、実際のアドレスと同じ数のマッピングアドレスを設定します。しかし、アドレスの数が一致しない場合もあります。
 - (ポート変換を設定したスタティック インターフェイス NAT) 。宛先のアドレスのインターフェイスを使用するには、[インターフェイス (Interface)] [宛先インターフェイス IP (Destination Interface IP)] を選択します。また特定の宛先インターフェイス オブジェクトを選択する必要もあります。インターフェイスの IPv6 アドレスを使用するには、[詳細 (Advanced)] タブで [IPv6] オプションを選択する必要もあります。これはポート変換と共に、スタティック インターフェイス NAT を設定します。送信元アドレス/ポートは、インターフェイスのアドレス、および同じポート番号に変換されます。
- (オプション) [元のポート (Original Port)]、[変換済みポート (Translated Port)] : TCP または UDP ポートを変換する必要がある場合は、[元のポート (Original Port)] でプロトコルを選択し、元のポート番号と変換済みポート番号を入力します。たとえば、必要に応じて TCP/80 を 8080 に変換できます。

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

- [このルールに一致する DNS 応答を変換する (Translate DNS replies that match this rule)] : DNS 応答の IP アドレスを変換するかどうかを指定します。マッピング インターフェイスから実際のインターフェイスに移動する DNS 応答の場合、アドレス (IPv4 A または IPv6 AAAA) レコードはマッピングされた値から実際の値に書き換えられます。反対に、実際のインターフェイスからマッピング インターフェイスに移動する DNS 応答の場合、レコードは実際の値からマッピングされた値に書き換えられます。このオプションは特殊な状況で使用され、書き換えにより A レコードと AAAA レコード間でも変換が行われる NAT64/46 変換のために必要なことがあります。詳細については、[NAT を使用した DNS クエリと応](#)

答の書き換え (103 ページ) を参照してください。ポート変換を実行する場合、このオプションは使用できません。

- [IPv6] : インターフェイス PAT に宛先インターフェイスの IPv6 アドレスを使用するかどうかを指定します。
- [ネット間マッピング (Net to Net Mapping)] : NAT 46 の場合、このオプションを選択して、最初の IPv4 アドレスを最初の IPv6 アドレスに変換し、2 番目を 2 番目に変換という順序で変換します。このオプションを選択しない場合、IPv4 埋め込み方式が使用されません。1 対 1 の変換の場合は、このオプションを使用する必要があります。
- [宛先インターフェイスで ARP をプロキシしない (Do not proxy ARP on Destination Interface)] : マッピング IP アドレスへの着信パケットのプロキシ ARP を無効にします。マッピングインターフェイスと同じネットワーク上のアドレスを使用した場合、システムはプロキシ ARP を使用してマッピングアドレスのすべての ARP 要求に応答することで、マッピングアドレスを宛先とするトラフィックを代行受信します。この方法だと、デバイスがその他のネットワークのゲートウェイになる必要がないため、ルーティングが簡略化されます。プロキシ ARP は必要に応じて無効にできます。無効にする場合、上流に位置するルータに適切なルートが設定されている必要があります。アイデンティティ NAT の場合、通常はプロキシ ARP は不要です。場合によっては接続の問題が生じることがあります。

ステップ 7 [保存 (Save)] をクリックしてルールを追加します。

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

スタティック手動 NAT の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin

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

始める前に

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

- [元の送信元 (Original Source)]: これはネットワーク オブジェクトまたはグループで、ホスト、範囲、またはサブネットを含むことができます。すべての元のトラフィックを変換する場合、この手順をスキップし、ルールで [すべて (Any)] を指定します。
- [変換済み送信元 (Translated Source)]: 変換済みアドレスを指定するには、次のオプションがあります。
 - [宛先インターフェイス (Destination Interface)]: 宛先インターフェイス アドレスを使用するには、ネットワーク オブジェクトは必要ありません。これはポート変換と共に、スタティック インターフェイス NAT を設定します。送信元アドレス/ポートは、インターフェイスのアドレス、および同じポート番号に変換されます。
 - [アドレス (Address)]: ホスト、範囲、またはサブネットを含むネットワーク オブジェクトまたはグループを作成します。通常、1 対 1 のマッピングでは、実際のアドレスと同じ数のマッピングアドレスを設定します。しかし、アドレスの数が一致しない場合もあります。

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

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

手順

-
- ステップ 1** [デバイス (Devices)] > [NAT] を選択し、Firepower Threat Defense NAT ポリシーを作成または編集します。
- ステップ 2** 次のいずれかを実行します。
- [ルールの追加 (Add Rule)] ボタンをクリックして、新しいルールを作成します。
 - 編集アイコン (✎) をクリックして、既存のルールを編集します。
- メニューを右クリックすると、ルールの切り取り、コピー、貼り付け、挿入、および削除オプションが表示されます。
- ステップ 3** 基本ルールのオプションを設定します。
- [NAT ルール (NAT Rule)]: [手動 NAT ルール (Manual NAT Rule)] を選択します。
 - [タイプ (Type)]: [スタティック (Static)] を選択します。この設定は送信元アドレスにのみ適用されます。宛先アドレスの変換を定義している場合、変換は常に静的に行われます。
 - [有効にする (Enable)]: ルールをアクティブにするかどうかを指定します。ルール ページの右クリックメニューを使用して、後でルールをアクティブ化または非アクティブ化することができます。

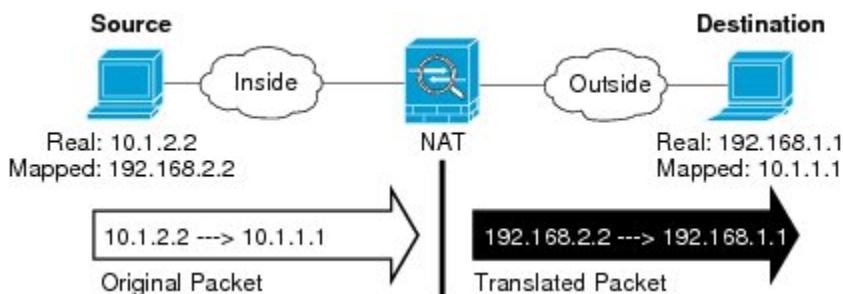
- [挿入 (Insert)]: ルールを追加する場所を指定します。ルールは、カテゴリ (自動 NAT ルールの前か後)、または指定したルール番号の上か下に挿入できます。

ステップ 4 [インターフェイス オブジェクト (Interface Objects)] タブで、以下のオプションを設定します。

- [送信元インターフェイス オブジェクト (Source Interface Objects)]、[宛先インターフェイス オブジェクト (Destination Interface Objects)]: (共有ポリシーのみ)。[送信元ゾーン (Source Zone)]、[宛先ゾーン (Destination Zone)]: (トランスペアレントファイアウォールモードの場合に必要)。この NAT ルールが適用されるインターフェイスを識別するセキュリティゾーン。[送信元 (Source)]は、デバイスに入るトラフィックが通過する実際のインターフェイスを含むゾーン。[宛先 (Destination)]は、デバイスから出るトラフィックが通過するマッピングインターフェイスを含むゾーン。デフォルトでは、すべてのインターフェイスにルールが適用されます ([すべて (Any)])。(ブリッジグループメンバー インターフェイスの場合に必要) **Source Zone Destination Zone Source Destination Any**

ステップ 5 ([変換 (Translation)] タブで次を実行します。) 元のパケットアドレス (IPv4 または IPv6)、つまり、元のパケットに表示されるパケットアドレスを特定します。

元のパケットと変換済みパケットの例については、次の図を参照してください。



- [元の送信元アドレス (Original Source Address)]: 変換しているアドレスを含むネットワーク オブジェクトまたはグループ。
- [元の宛先アドレス (Original Destination Address)]: (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 を使用することができます。

[送信元インターフェイス IP (Source Interface IP)] を選択して、送信元インターフェイスの元の宛先 ([すべて (Any)]) は選択不可) をベースにすることができます。このオプションを選択する場合、変換済みの宛先オブジェクトも選択する必要があります。宛先アドレスに対して、ポート変換を設定したスタティック インターフェイス NAT を実装するには、このオプションを選択し、宛先ポートに適したポートオブジェクトも選択します。

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

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

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

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

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

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

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

- [このルールに一致する DNS 応答を変換する (Translate DNS replies that match this rule)] : DNS 応答の IP アドレスを変換するかどうかを指定します。マッピング インターフェイスから実際のインターフェイスに移動する DNS 応答の場合、アドレス (IPv4 A または IPv6 AAAA) レコードはマッピングされた値から実際の値に書き換えられます。反対に、実際のインターフェイスからマッピング インターフェイスに移動する DNS 応答の場合、レコードは実際の値からマッピングされた値に書き換えられます。このオプションは特殊な状況で使用され、書き換えにより A レコードと AAAA レコード間でも変換が行われる NAT64/46 変換のために必要なことがあります。詳細については、[NAT を使用した DNS クエリと応答の書き換え \(103 ページ\)](#) を参照してください。ポート変換を実行する場合、このオプションは使用できません。

- [IPv6] : インターフェイス PAT に宛先インターフェイスの IPv6 アドレスを使用するかどうかを指定します。
- [ネット間マッピング (Net to Net Mapping)] : NAT 46 の場合、このオプションを選択して、最初の IPv4 アドレスを最初の IPv6 アドレスに変換し、2 番目を 2 番目に変換という順序で変換します。このオプションを選択しない場合、IPv4 埋め込み方式が使用されます。1 対 1 の変換の場合は、このオプションを使用する必要があります。
- [宛先インターフェイスで ARP をプロキシしない (Do not proxy ARP on Destination Interface)] : マッピング IP アドレスへの着信パケットのプロキシ ARP を無効にします。マッピングインターフェイスと同じネットワーク上のアドレスを使用した場合、システムはプロキシ ARP を使用してマッピングアドレスのすべての ARP 要求に応答することで、マッピングアドレスを宛先とするトラフィックを代行受信します。この方法だと、デバイスがその他のネットワークのゲートウェイになる必要がないため、ルーティングが簡略化されます。プロキシ ARP は必要に応じて無効にできます。無効にする場合、上流に位置するルータに適切なルートが設定されている必要があります。アイデンティティ NAT の場合、通常はプロキシ ARP 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。
- [単方向 (Unidirectional)] : 宛先アドレスから送信元アドレスへのトラフィックの送信開始を防ぐには、このオプションを選択します。

ステップ 9 [保存 (Save)] をクリックしてルールを追加します。

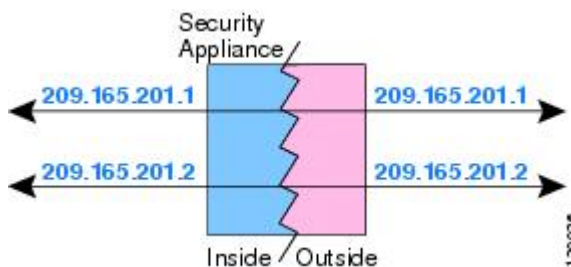
ステップ 10 NAT ページで [保存 (Save)] をクリックして変更を保存します。

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することができます。

次の図に、一般的なアイデンティティ NAT のシナリオを示します。

図 13: 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

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin

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

始める前に

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

- [元の送信元 (Original Source)] : これはネットワーク オブジェクト (グループではない) でなければならず、ホスト、範囲、またはサブネットも可能です。
- [変換済み送信元 (Translated Source)] : 元の送信元オブジェクトとコンテンツが全く同一のネットワーク オブジェクトまたはグループ。同じオブジェクトを使用できます。

手順

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

ステップ 2 次のいずれかを実行します。

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

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

ステップ 3 基本ルールのオプションを設定します。

- [NAT ルール (NAT Rule)] : [自動 NAT ルール (Auto NAT Rule)] を選択します。
- [タイプ (Type)] : [スタティック (Static)] を選択します。

ステップ 4 [インターフェイス オブジェクト (Interface Objects)] タブで、以下のオプションを設定します。

- [送信元インターフェイス オブジェクト (Source Interface Objects)]、[宛先インターフェイス オブジェクト (Destination Interface Objects)] : (ブリッジグループ メンバー インターフェイスの場合に必要) **DestinationSource**

ステップ 5 [一般 (General)] [変換 (Translation)] タブで、次のオプションを設定します。

- [元の送信元 (Original Source)] : 変換するアドレスを含むネットワーク オブジェクト。
- [変換済み送信元 (Translated Source)] : 元の送信元と同じオブジェクト。オプションで、内容がまったく同じ別のオブジェクトを選択できます。

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

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

- [このルールと一致する DNS 応答を変換 (Translate DNS replies that match this rule)] : アイデンティティ NAT には、このオプションを設定しないでください。
- [IPv6] : アイデンティティ NAT にこのオプションを設定しないでください。
- [ネット マッピングへのネット (Net to Net Mapping)] : アイデンティティ NAT にこのオプションを設定しないでください。
- [宛先インターフェイスで ARP をプロキシしない (Do not proxy ARP on Destination Interface)] : マッピング IP アドレスへの着信パケットのプロキシ ARP を無効にします。マッピングインターフェイスと同じネットワーク上のアドレスを使用した場合、システムはプロキシ ARP を使用してマッピングアドレスのすべての ARP 要求に応答することで、マッピングアドレスを宛先とするトラフィックを代行受信します。この方法だと、デバイスがその他のネットワークのゲートウェイになる必要がないため、ルーティングが簡略化されます。プロキシ ARP は必要に応じて無効にできます。無効にする場合、上流に位置するルータに適切なルートが設定されている必要があります。アイデンティティ NAT の場合、通常はプロキシ ARP は不要です。場合によっては接続の問題が生じることがあります。
- [宛先インターフェイスのルートルックアップを実行 (Perform Route Lookup for Destination Interface)] : 元の送信元アドレスと変換後の送信元アドレスに対して同じオブジェクトを選択していて、送信元インターフェイスと宛先インターフェイスを選択する場合、このオプションを選択して、NAT ルールに設定されている宛先インターフェイスを使用する代わりに、ルーティングテーブルに基づいて宛先インターフェイスを決めさせることができます。

ステップ 7 [保存 (Save)] をクリックしてルールを追加します。

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

アイデンティティ手動 NAT の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin

自動 NAT がお客様のニーズを満たしていない場合は、スタティック アイデンティティ手動 NAT ルールを使用します。たとえば、宛先に応じて異なる変換をしたい場合などです。スタティック アイデンティティ NAT ルールを使用して、アドレスの変換を防止します。つまり、自身のアドレスに変換します。

始める前に

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

- [元の送信元 (Original Source)]: これはネットワーク オブジェクトまたはグループで、ホスト、範囲、またはサブネットを含むことができます。すべての元の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 (Translated Source)]: 元の送信元と同じオブジェクト。オプションで、内容がまったく同じ別のオブジェクトを選択できます。

ルールで各アドレスの静的変換を設定すると、[元の宛先 (Original Destination)]および [変換済み宛先 (Translated Destination)]のネットワーク オブジェクトを作成できます。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。オブジェクトマネージャでは、元のポートと変換されたポートで使用できるポート オブジェクトがあることを確認します。アイデンティティ NAT には同じオブジェクトを使用できます。

手順

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

ステップ 2 次のいずれかを実行します。

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

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

ステップ 3 基本ルールのオプションを設定します。

- [NAT ルール (NAT Rule)]: [手動 NAT ルール (Manual NAT Rule)] を選択します。
- [タイプ (Type)]: [スタティック (Static)] を選択します。この設定は送信元アドレスのみ適用されます。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ず。

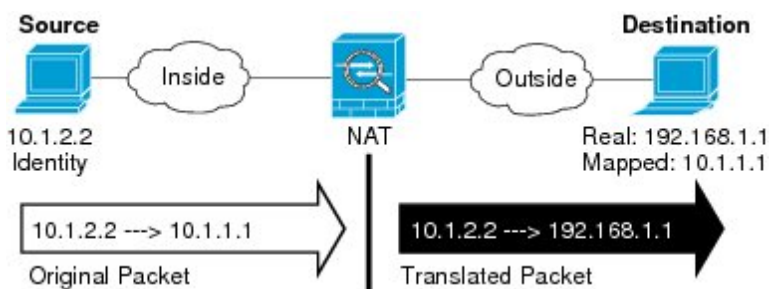
- [有効にする (Enable)]: ルールをアクティブにするかどうかを指定します。ルール ページの右クリックメニューを使用して、後でルールをアクティブ化または非アクティブ化することができます。
- [挿入 (Insert)]: ルールを追加する場所を指定します。ルールは、カテゴリ (自動 NAT ルールの前か後)、または指定したルール番号の上か下に挿入できます。

ステップ 4 [インターフェイス オブジェクト (Interface Objects)] タブで、以下のオプションを設定します。

- [送信元インターフェイス オブジェクト (Source Interface Objects)]、[宛先インターフェイス オブジェクト (Destination Interface Objects)]: (共有ポリシーのみ)。
- [送信元ゾーン (Source Zone)]、[宛先ゾーン (Destination Zone)]: (トランスペアレントファイアウォールモードの場合に必要)。
- NAT ルールが適用されるインターフェイスを識別するセキュリティゾーン。
- [送信元 (Source)]は、デバイスに入るトラフィックが通過する実際のインターフェイスを含むゾーン。
- [宛先 (Destination)]は、デバイスから出るトラフィックが通過するマッピング インターフェイスを含むゾーン。
- デフォルトでは、すべてのインターフェイスにルールが適用されます ([すべて (Any)])。
- (ブリッジグループメンバー インターフェイスの場合に必要)

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

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



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

[インターフェイス (Interface)] > [インターフェイス オブジェクト (Interface Object)] を選択し、送信元インターフェイスの元の宛先 ([Any] は選択不可) をベースにすることができます。このオプションを選択する場合、変換済みの宛先オブジェクトも選択する必要があります。宛先アドレスに対して、ポート変換を設定したスタティックインターフェイス NAT を実装するには、このオプションを選択し、宛先ポートに適したポート オブジェクトも選択します。

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

- [変換済み送信元 (Translated Source)]: 元の送信元と同じオブジェクト。オプションで、内容がまったく同じ別のオブジェクトを選択できます。
- [変換済み宛先 (Translated Destination)]: (オプション)。変換されたパケットで使用される宛先アドレスを含むネットワーク オブジェクトまたはグループ。[元の宛先 (Original Destination)]を選択した場合、同じオブジェクトを選択することによって、アイデンティティ NAT (つまり変換なし) を設定できます。

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

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

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

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

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

- [このルールと一致する DNS 応答を変換 (Translate DNS replies that match this rule)]: アイデンティティ NAT には、このオプションを設定しないでください。
- [IPv6] : [IPv6] : インターフェイス PAT に宛先インターフェイスの IPv6 アドレスを使用するかどうかを指定します。インターフェイス PAT に宛先インターフェイスの IPv6 アドレスを使用するかどうかを指定します。
- [宛先インターフェイスで ARP をプロキシしない (Do not proxy ARP on Destination Interface)]: マッピング IP アドレスへの着信パケットのプロキシ ARP を無効にします。マッピング インターフェイスと同じネットワーク上のアドレスを使用した場合、システムはプロキシ ARP を使用してマッピングアドレスのすべての ARP 要求に応答することで、マッピングアドレスを宛先とするトラフィックを代行受信します。この方法だと、デバイスがその他のネットワークのゲートウェイになる必要がないため、ルーティングが簡略化されます。プロキシ ARP は必要に応じて無効にできます。無効にする場合、上流に位置するルータに適切なルートが設定されている必要があります。アイデンティティ NAT の場合、通常はプロキシ ARP は不要です。場合によっては接続の問題が生じることがあります。
- [宛先インターフェイスのルートルックアップを実行 (Perform Route Lookup for Destination Interface)]: 元の送信元アドレスと変換後の送信元アドレスに対して同じオブジェクトを選択していて、送信元インターフェイスと宛先インターフェイスを選択する場合、このオプションを選択して、NAT ルールに設定されている宛先インターフェイスを使用する代

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

- [単方向 (Unidirectional)]: 宛先アドレスから送信元アドレスへのトラフィックの送信開始を防ぐには、このオプションを選択します。宛先アドレスから送信元アドレスへのトラフィックの送信開始を防ぐには、このオプションを選択します。

ステップ 9 [保存 (Save)] をクリックしてルールを追加します。

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

Firepower Threat Defense の NAT ルール プロパティ

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

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

NAT タイプ (NAT Type)

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

タイプ (Type)

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

有効化 (Enable) (手動 NAT のみ)

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

挿入 (Insert) (手動 NAT のみ)

ルールを追加する場所を指定します。ルールは、カテゴリ (自動 NAT ルールの前か後) 、または指定したルール番号の上か下に挿入できます。

説明 (任意、手動 NAT のみ)。

ルールの目的の説明。

以降のトピックで、NAT ルール プロパティのタブについて説明します。

インターフェイスオブジェクト : NAT のプロパティ

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



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

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

送信元インターフェイスオブジェクト、宛先インターフェイスオブジェクト

(ブリッジグループメンバーインターフェイスの場合に必要)

自動 NAT の [変換 (Translation)] プロパティ

[変換 (Translation)] タブのオプションを使って発信元アドレスやマッピングされた変換アドレスを定義します。次のプロパティは、自動 NAT にのみ適用されます。

[元の送信元 (Original Source)] (常に必須)。

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

[変換済み送信元 (Translated Source)] (通常は必須)。

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

- [ダイナミック NAT (Dynamic NAT)] : マッピングアドレスを含むネットワークオブジェクトまたはグループ。ネットワークオブジェクトまたはグループにすることができますが、サブネットを含むことはできません。グループに IPv4 アドレスと IPv6

アドレスの両方を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) 。宛先のアドレスのインターフェイスを使用するには、[インターフェイス (Interface)] > [宛先インターフェイス IP (Destination Interface IP)] を選択します。また特定の宛先インターフェイス オブジェクトを選択する必要もあります。インターフェイスの IPv6 アドレスを使用するには、[詳細 (Advanced)] タブで [IPv6] オプションを選択する必要があります。PAT プールは設定しないでください。
 - 宛先インターフェイスのアドレス以外の単一アドレスを使用する場合は、そのために作成したホスト ネットワーク オブジェクトを選択します。PAT プールは設定しないでください。
 - PAT プールを使用するには、[変換された送信元 (Translated Source)] を空のままにしておきます。[PAT プール (PAT Pool)] タブで PAT プール オブジェクトを選択します。
- [スタティック NAT (Static NAT)] : 次のいずれかを実行します。
 - アドレスの設定グループを使用するには、[アドレス (Address)] およびマッピングされたアドレスを含むネットワーク オブジェクトまたはグループを選択します。オブジェクトまたはグループに、ホスト、範囲、またはサブネットを含めることができます。通常、1対1のマッピングでは、実際のアドレスと同じ数のマッピングアドレスを設定します。しかし、アドレスの数が一致しない場合もあります。
 - (ポート変換を設定したスタティック インターフェイス NAT) 。宛先のアドレスのインターフェイスを使用するには、[インターフェイス (Interface)] [宛先インターフェイス IP (Destination Interface IP)] を選択します。また特定の宛先インターフェイス オブジェクトを選択する必要もあります。インターフェイスの IPv6 アドレスを使用するには、[詳細 (Advanced)] タブで [IPv6] オプションを選択する必要があります。これはポート変換と共に、スタティック インターフェイス NAT を設定します。送信元アドレス/ポートは、インターフェイスのアドレス、および同じポート番号に変換されます。
- [アイデンティティ NAT (Identity NAT)] : 元の送信元と同じオブジェクト。状況に応じて、コンテンツが全く同一の別のオブジェクトを選択できます。

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

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

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

手動 NAT の[一般 (General)] [変換 (Translation)] プロパティ

[変換 (Translation)] タブのオプションを使って発信元アドレスやマッピングされた変換アドレスを定義します。次のプロパティは、手動 NAT にのみ適用されます。指示されている場合を除き、すべてオプションです。

[元の送信元 (Original Source)] (常に必須)。

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

[変換済み送信元 (Translated Source)] (通常は必須)。

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

- **[ダイナミック NAT (Dynamic NAT)]**: マッピング アドレスを含むネットワーク オブジェクトまたはグループ。ネットワーク オブジェクトまたはグループにすることができますが、サブネットを含むことはできません。グループに IPv4 アドレスと IPv6 アドレスの両方を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)。宛先のアドレスのインターフェイスを使用するには、[インターフェイス (Interface)] > [宛先インターフェイス IP (Destination Interface IP)] を選択します。また特定の宛先インターフェイス オブジェクトを選択する必要もあります。インターフェイスの IPv6 アドレスを使用するには、[詳細 (Advanced)] タブで [IPv6] オプションを選択する必要があります。PAT プールは設定しないでください。
 - 宛先インターフェイスのアドレス以外の単一アドレスを使用する場合は、そのために作成したホスト ネットワーク オブジェクトを選択します。PAT プールは設定しないでください。
 - PAT プールを使用するには、[変換された送信元 (Translated Source)] を空のままにしておきます。[PAT プール (PAT Pool)] タブで PAT プール オブジェクトを選択します。
- **[スタティック NAT (Static NAT)]**: 次のいずれかを実行します。
 - アドレスの設定グループを使用するには、[アドレス (Address)] およびマッピングされたアドレスを含むネットワーク オブジェクトまたはグループを選択します。オブジェクトまたはグループに、ホスト、範囲、またはサブネットを含める

ことができます。通常、1対1のマッピングでは、実際のアドレスと同じ数のマッピングアドレスを設定します。しかし、アドレスの数が一致しない場合もあります。

- (ポート変換を設定したスタティック インターフェイス NAT)。宛先のアドレスのインターフェイスを使用するには、[インターフェイス (Interface)] [宛先インターフェイス IP (Destination Interface IP)] を選択します。また特定の宛先インターフェイスオブジェクトを選択する必要もあります。インターフェイスの IPv6 アドレスを使用するには、[詳細 (Advanced)] タブで [IPv6] オプションを選択する必要もあります。これはポート変換と共に、スタティック インターフェイス NAT を設定します。送信元アドレス/ポートは、インターフェイスのアドレス、および同じポート番号に変換されます。

- [アイデンティティ NAT (Identity NAT)] : 元の送信元と同じオブジェクト。状況に応じて、コンテンツが全く同一の別のオブジェクトを選択できます。

[元の宛先 (Original Destination)]

宛先アドレスを含むネットワークオブジェクト。空白のままにすると、宛先に関係なく、送信元アドレスの変換が適用されます。宛先アドレスを指定した場合、そのアドレスにスタティック変換を設定するか、単にアイデンティティ NAT を使用することができます。

[送信元インターフェイス IP (Source Interface IP)] を選択して、送信元インターフェイスの元の宛先 ([すべて (Any)] は選択不可) をベースにすることができます。このオプションを選択する場合、変換済みの宛先オブジェクトも選択する必要があります。宛先アドレスに対して、ポート変換を設定したスタティック インターフェイス NAT を実装するには、このオプションを選択し、宛先ポートに適したポートオブジェクトも選択します。

[変換済みの宛先 (Translated Destination)]

変換されたパケットで使用される宛先アドレスを含むネットワークオブジェクトまたはグループ。[元の宛先 (Original Destination)] を選択した場合、同じオブジェクトを選択することによって、アイデンティティ NAT (つまり変換なし) を設定できます。

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

元のパケットおよび変換済みパケットの送信元および宛先サービスを定義するポートオブジェクト。ポートを変換したり、ポートを変換せずに同じオブジェクトを選択してサービスに対するルールの感度を向上することができます。サービスを設定するときは、次のルールに注意してください。

- (ダイナミック NAT または PAT) [元の送信元ポート (Original Source Port)] および [変換済み送信元ポート (Translated Source Port)] では変換できません。宛先ポートでのみ変換できます。
- NAT では、TCP または UDP のみがサポートされます。ポートを変換する場合、実際のサービスオブジェクトのプロトコルとマッピングサービスオブジェクトのプロトコルの両方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

デスティティ NAT では、実際のポートとマッピング ポートの両方に同じサービス オブジェクトを使用できます。

PAT プールの NAT プロパティ

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

PAT プールの有効化 (Enable PAT Pool)

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

PAT

PAT プールに使用するアドレスとして、以下のいずれかを指定します。

- [アドレス (Address)] : PAT プールアドレスを定義するオブジェクト。アドレスの範囲を含むネットワーク オブジェクト、またはホスト、範囲、あるいはその両方を含むネットワーク オブジェクト グループのいずれかです。サブネットを含めることはできません。グループに IPv4 アドレスと IPv6 アドレスの両方を含めることはできません。1 つのタイプだけ含める必要があります。
- [宛先インターフェイス IP (Destination Interface IP)] : PAT アドレスとして使用する宛先インターフェイスを指定します。このオプションを使用する場合、特定の [宛先インターフェイス オブジェクト (Destination Interface Object)] を選択する必要があります。[すべて (Any)] を宛先インターフェイスとして使用することはできません。これは、インターフェイス PAT を実装するもう 1 つの方法です。

ラウンドロビン (Round Robin)

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

拡張 PAT テーブル (Extended PAT Table)

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

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

TCP/UDP ポートを割り当てる際に、ポート範囲 (1024 ~ 65535) を単一のフラットな範囲として使用します。変換用のマッピング ポート番号を選択する場合、PAT によって、実際の送信元ポート番号が使用されます (使用可能な場合) 。ただし、このオプションを

設定しないと、実際のポートが使用できない場合、デフォルトでは、実際のポート番号と同じポート範囲 (1 ~ 511、512 ~ 1023、および 1024 ~ 65535) からマッピングポートが選択されます。下位の範囲でポートが不足するのを回避するには、この設定を行います。1 ~ 65535 の範囲全体を使用するには、[予約済みポートを含む (Include Reserved Ports)] オプションも選択します。

詳細 NAT プロパティ

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

このルールに一致する DNS 回答の変換

DNS 応答の IP アドレスを変換するかどうかを指定します。マッピングインターフェイスから実際のインターフェイスに移動する DNS 応答の場合、アドレス (IPv4 A または IPv6 AAAA) レコードはマッピングされた値から実際の値に書き換えられます。反対に、実際のインターフェイスからマッピングインターフェイスに移動する DNS 応答の場合、レコードは実際の値からマッピングされた値に書き換えられます。このオプションは特殊な状況で使用され、書き換えにより A レコードと AAAA レコード間でも変換が行われる NAT64/46 変換のために必要なことがあります。詳細については、[NAT を使用した DNS クエリと応答の書き換え \(103 ページ\)](#) を参照してください。スタティック NAT ルールでポート変換を行っている場合には、このオプションは使用できません。

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

その他のマッピングアドレスがすでに割り当てられている場合に、宛先インターフェイスの IP アドレスをバックアップ方式として使用するかどうかを指定します (インターフェイス PAT フォールバック)。このオプションは、ブリッジグループのメンバーではない宛先インターフェイスを選択した場合にのみ使用できます。インターフェイスの IPv6 アドレスを使用するには、[IPv6] オプションも選択します。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。PAT プールを構成する場合も、このオプションを選択することはできません。

IPv6

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

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

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

宛先インターフェイスでプロキシ ARP なし (スタティック NAT のみ)

マッピング IP アドレスへの着信パケットのプロキシ ARP を無効にします。マッピングインターフェイスと同じネットワーク上のアドレスを使用した場合、システムはプロキシ

ARP を使用してマッピング アドレスのすべての ARP 要求に応答することで、マッピング アドレスを宛先とするトラフィックを代行受信します。この方法だと、デバイスがその他のネットワークのゲートウェイになる必要がないため、ルーティングが簡略化されます。プロキシ ARP は必要に応じて無効にできます。無効にする場合、上流に位置するルータに適切なルートが設定されている必要があります。アイデンティティ NAT の場合、通常はプロキシ ARP は不要です。場合によっては接続の問題が生じることがあります。

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

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

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

宛先アドレスから送信元アドレスへのトラフィックの送信開始を防ぐには、このオプションを選択します。

IPv6 ネットワークの変換

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

IPv6 ネットワークとともに次の変換タイプを使用できます。

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



(注) NAT46 がサポートするのは、スタティック マッピングのみです。

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



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

NAT64/46 : IPv6 アドレスの 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 アドレスに変換して、IPv4 から IPv6 にトラフィックを戻す必要があります。IPv4 ネットワークで IPv6 アドレスをバインドするための IPv4 アドレスプールと、IPv6 ネットワークで IPv4 アドレスをバインドするための IPv6 アドレスプールの 2 つを定義する必要があります。

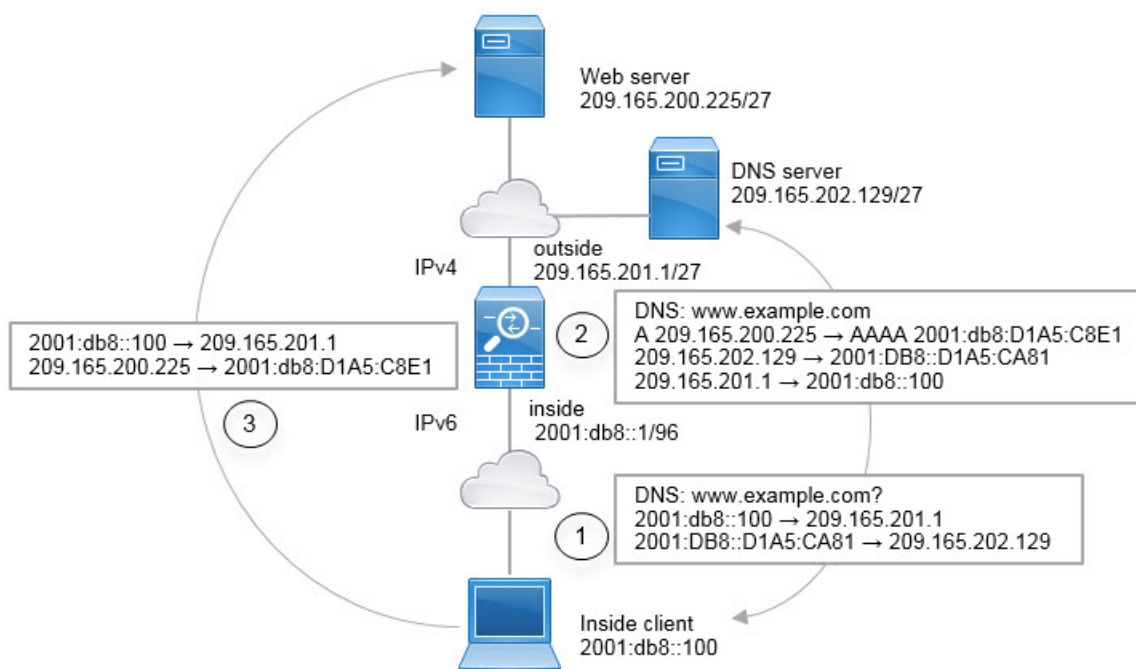
- NAT64 ルール用の IPv4 アドレスプールは通常は小さく、一般的に IPv6 クライアントアドレスを使用して 1 対 1 のマッピングを設定するにはアドレスが足りない場合があります。ダイナミック PAT は、ダイナミック NAT またはスタティック NAT と比較して、できる限り多数の IPv6 クライアントアドレスにより容易に対応します。
- NAT 46 ルールの IPv6 アドレスプールは、マッピングされる IPv4 アドレスの数と等しいか、それより多くなります。これによって、各 IPv4 アドレスを別の IPv6 アドレスにマッピングできます。NAT 46 はスタティック マ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

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

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

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin

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



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

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

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

3. これで、IPv6 クライアントが Web サーバの IP アドレスを取得し、www.example.com (2001:db8:D1A5:C8E1) に HTTP 要求を送信できます。(D1A5:C8E1 は IPv6 の 209.165.200.225 に相当します)。HTTP 要求の送信元と宛先が変換されます。
 - 2001:DB8::100 を 209.156.101.54 上の一意のポートに変換 (NAT64 インターフェイス PAT ルール)。
 - 2001:db8:D1A5:C8E1 を 209.165.200.225 に変換 (NAT46 ルール)。

次の手順では、この例の設定方法について説明します。

始める前に

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

手順

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

- a) **[オブジェクト (Objects)] > [オブジェクト管理 (Object Management)]** を選択します。
- b) コンテンツのテーブルから **[ネットワーク (Network)]** を選択し、**[ネットワークを追加 (Add Network)] > [オブジェクトの追加 (Add Object)]** をクリックします。
- c) 内部 IPv6 ネットワークを定義します。

ネットワークオブジェクトに名前 (inside_v6 など) を付け、ネットワークアドレス 2001:DB8::/96 を入力します。

New Network Objects ? ×

Name:

Description:

Network:

Format: ipaddr or ipaddr/len or range (ipaddr-ipaddr)

Allow Overrides:

- d) **[保存 (Save)]** をクリックします。
- e) **[ネットワークの追加 (Add Network)] > [オブジェクトの追加 (Add Object)]** をクリックして、外部 IPv4 ネットワークを定義します。

ネットワーク オブジェクトに名前 (たとえば、outside_v4_any) を付けて、ネットワーク アドレス 0.0.0.0/0 を入力します。

f) [保存 (Save)] をクリックします。

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

- a) [デバイス (Devices)] > [NAT] を選択し、Firepower Threat Defense NAT ポリシーを作成または編集します。
- b) [ルールの追加 (Add Rule)] をクリックします。
- c) 次のプロパティを設定します。
 - [NAT ルール (NAT Rule)] = 自動 NAT ルール。
 - [タイプ (Type)] = Dynamic。
- d) [インターフェイス オブジェクト (Interface Objects)] タブで、以下の設定を行います。
 - [送信元インターフェイス オブジェクト (Source Interface Objects)] = inside。
 - [宛先インターフェイス オブジェクト (Destination Interface Objects)] = outside。
- e) [変換 (Translation)] タブで、次の項目を設定します。
 - [元の送信元 (Original Source)] = inside_v6 ネットワーク オブジェクト。
 - [変換済みの送信元 (Translated Source)] = 宛先インターフェイス IP (Destination Interface IP) 。

- f) [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) [ルール の追加 (Add Rule)] をクリックします。
- b) 次のプロパティを設定します。
 - [NAT ルール (NAT Rule)] = 自動 NAT ルール (Auto NAT Rule)。
 - [タイプ (Type)] = スタティック (Static)。
- c) [インターフェイス オブジェクト (Interface Objects)] タブで、以下の設定を行います。
 - [送信元インターフェイス オブジェクト (Source Interface Objects)] = outside。
 - [宛先インターフェイス オブジェクト (Destination Interface Objects)] = inside。
- d) [変換 (Translation)] タブで、次の項目を設定します。
 - [元の送信元 (Original Source)] = outside_v4_any ネットワーク オブジェクト。
 - [変換済みの送信元 (Translated Source)] > [アドレス (Address)] = inside_v6 ネットワーク オブジェクト。
- e) [詳細 (Advanced)] 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。

The screenshot shows the 'Add NAT Rule' configuration interface. At the top, 'NAT Rule' is set to 'Auto NAT Rule' and 'Type' is 'Static'. Below this, there are tabs for 'Interface Objects', 'Translation', 'PAT Pool', and 'Advanced'. The 'Translation' tab is selected, showing two main sections: 'Original Packet' and 'Translated Packet'. In the 'Original Packet' section, 'Original Source' is set to 'outside_v4_any' and 'Original Port' is set to 'TCP'. In the 'Translated Packet' section, 'Translated Source' is set to 'Address' and 'inside_v6'.

- f) [OK] をクリックします。

このルールにより、内部インターフェイスに向かう外部ネットワーク上のすべての IPv4 アドレスが、組み込み IPv4 アドレス方式を使用して 2001:db8::/96 ネットワーク上のアドレスに変換されます。また、DNS 応答が A (IPv4) レコードから AAAA (IPv6) レコードに変換され、アドレスが IPv4 から IPv6 に変換されます。

NAT66 : IPv6 アドレスの異なる IPv6 アドレスへの変換

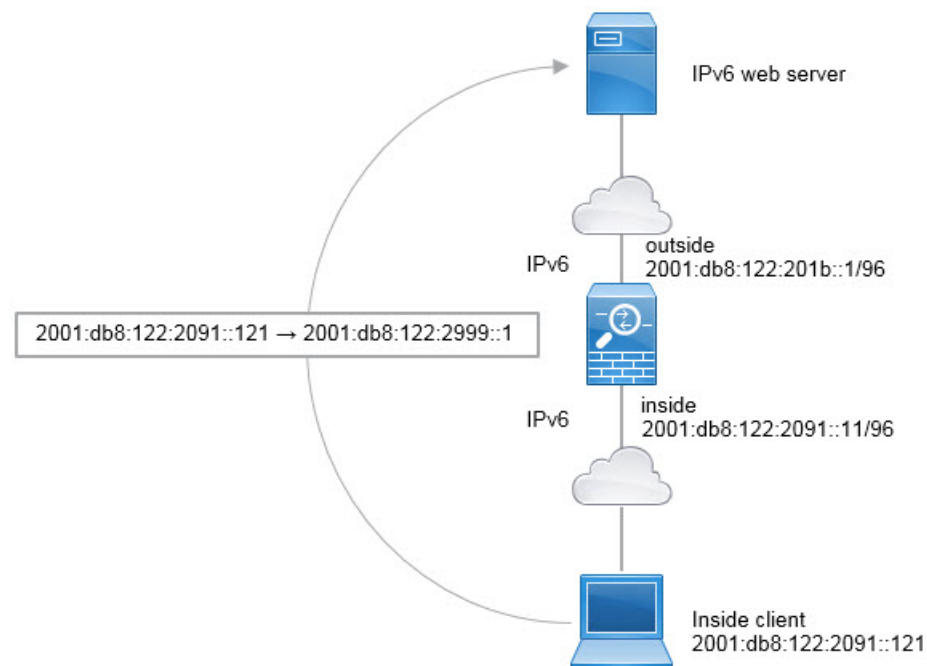
IPv6 ネットワークから別の IPv6 ネットワークに移動する場合、アドレスを外部ネットワークの別の IPv6 アドレスに変換できます。スタティック NAT の使用をお勧めします。ダイナミック NAT または PAT を使用できますが、IPv6 アドレスは大量にあるため、ダイナミック NAT を使用する必要はありません。

異なるアドレス タイプ間での変換ではないため、NAT66 変換の単一のルールが必要です。/自動 NAT を使用して、これらのルールを簡単にモデル化できます。ただし、リターントラフィックを許可しない場合は、/手動 NAT のみを使用してスタティック NAT ルールを単一方向にすることができます。

NAT66 の例 : ネットワーク間のスタティック変換

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin

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



始める前に

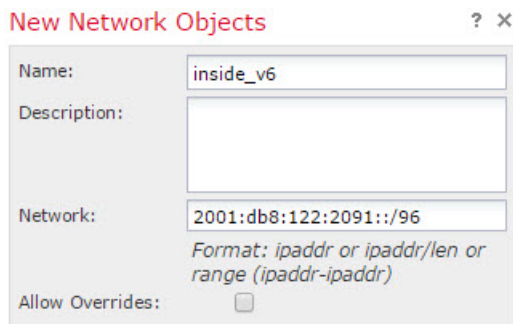
デバイスに対応するインターフェイスが含まれているインターフェイスオブジェクト (セキュリティゾーンまたはインターフェイスグループ) があることを確認します。この例では、インターフェイスオブジェクトは **inside** および **outside** という名前のセキュリティゾーンであると仮定します。インターフェイスオブジェクトを設定するには、**[オブジェクト (Objects)] > [オブジェクト管理 (Object Management)]** を選択してから、**[インターフェイス (Interface)]** を選択します。

手順

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

- [オブジェクト (Objects)] > [オブジェクト管理 (Object Management)]** を選択します。
- コンテンツのテーブルから **[ネットワーク (Network)]** を選択し、**[ネットワークを追加 (Add Network)] > [オブジェクトの追加 (Add Object)]** をクリックします。
- 内部 IPv6 ネットワークを定義します。

ネットワークオブジェクトに名前 (たとえば、inside_v6) を付けて、ネットワークアドレス 2001:db8:122:2091::/96 を入力します。



New Network Objects ? x

Name: inside_v6

Description:

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

Format: ipaddr or ipaddr/len or range (ipaddr-ipaddr)

Allow Overrides:

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

ネットワークオブジェクトに名前 (たとえば、outside_nat_v6) を付けて、ネットワークアドレス 2001:db8:122:2999::/96 を入力します。

New Network Objects ? x

Name: outside_nat_v6

Description:

Network: 2001:db8:122:2999::/96
Format: ipaddr or ipaddr/len or range (ipaddr-ipaddr)

Allow Overrides:

f) [保存 (Save)] をクリックします。

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

- a) [デバイス (Devices)] > [NAT] を選択し、Firepower Threat Defense NAT ポリシーを作成または編集します。
- b) [ルールの追加 (Add Rule)] をクリックします。
- c) 次のプロパティを設定します。
 - [NAT ルール (NAT Rule)] = 自動 NAT ルール (Auto NAT Rule)。
 - [タイプ (Type)] = スタティック (Static)。
- d) [インターフェイス オブジェクト (Interface Objects)] タブで、次の項目を設定します。
 - [送信元インターフェイス オブジェクト (Source Interface Objects)] = inside。
 - [宛先インターフェイス オブジェクト (Destination Interface Objects)] = outside。
- e) [変換 (Translation)] タブで、次の項目を設定します。
 - [元の送信元 (Original Source)] = inside_v6 ネットワーク オブジェクト。
 - [変換済みの送信元 (Translated Source)] > [アドレス (Address)] = outside_nat_v6 ネットワーク オブジェクト。

Add NAT Rule

NAT Rule: Auto NAT Rule

Type: Static Enable

Interface Objects Translation PAT Pool Advanced

Original Packet

Original Source:* inside_v6

Translated Packet

Translated Source: Address
outside_nat_v6

f) [OK] をクリックします。

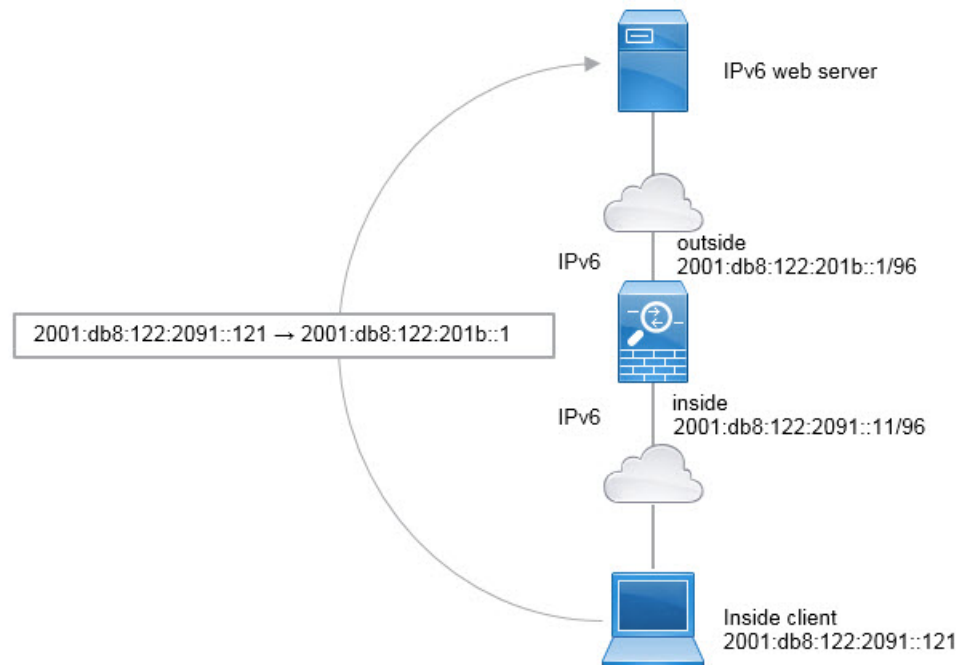
このルールにより、内部インターフェイス上の 2001:db8:122:2091::/96 サブネットから外部インターフェイスに向かうすべてのトラフィックが、2001:db8:122:2999::/96 ネットワーク上のアドレスにスタティック NAT66 変換されます。

NAT66 の例 : シンプルな IPv6 インターフェイス PAT

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin

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

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



始める前に

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

[**オブジェクト管理 (Object Management)**] を選択してから、[**インターフェイス (Interface)**] を選択します。

手順

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

- a) [**オブジェクト (Objects)**] > [**オブジェクト管理 (Object Management)**] を選択します。
- b) コンテンツのテーブルから [ネットワーク (Network)] を選択し、[**ネットワークを追加 (Add Network)**] > [**オブジェクトの追加 (Add Object)**] をクリックします。
- 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 (たとえば、inside_v6) を付けて、ネットワーク アドレス 2001:db8:122:2091::/96 を入力します。

The screenshot shows a dialog box titled "New Network Objects" with a close button (X) and a help button (?). It contains the following fields and options:

- Name:** inside_v6
- Description:** (empty text area)
- Network:** 2001:db8:122:2091::/96
- Format: ipaddr or ipaddr/len or range (ipaddr-ipaddr)*
- Allow Overrides:**

- d) [保存 (Save)] をクリックします。

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

- a) [**デバイス (Devices)**] > [**NAT**] を選択し、Firepower Threat Defense NAT ポリシーを作成または編集します。
- b) [ルール の追加 (Add Rule)] をクリックします。
- c) 次のプロパティを設定します。
 - [NAT ルール (NAT Rule)] = 自動 NAT ルール。
 - [タイプ (Type)] = Dynamic。
- d) [インターフェイス オブジェクト (Interface Objects)] タブで、以下の設定を行います。
 - [送信元インターフェイス オブジェクト (Source Interface Objects)] = inside。
 - [宛先インターフェイス オブジェクト (Destination Interface Objects)] = outside。
- e) [変換 (Translation)] タブで、次の項目を設定します。
 - [元の送信元 (Original Source)] = inside_v6 ネットワーク オブジェクト。
 - [変換済みの送信元 (Translated Source)] = 宛先インターフェイス IP (Destination Interface IP)。

- f) [詳細 (Advanced)] タブで、[IPv6] を選択します。これは、宛先インターフェイスの IPv6 が使用されることを意味します。

Add NAT Rule

NAT Rule: Auto NAT Rule

Type: Dynamic Enable

Interface Objects Translation PAT Pool Advanced

Original Packet

Original Source:* inside_v6

Original Port: TCP

Translated Packet

Translated Source: Destination Interface IP

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

- g) [OK] をクリックします。

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

NAT のモニタリング

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

- **show nat** NAT ルールとルールごとのヒット数を表示します。NAT の他の側面を表示するための追加キーワードがあります。
- **show xlate** 現在アクティブな実際の NAT 変換を表示します。
- **clear xlate** アクティブな NAT 変換を削除できます。既存の接続は接続が終了するまで古い変換スロットを継続して使用するため、NAT ルールを変更する場合はアクティブな変換を削除しなければならないことがあります。変換をクリアすると、システムは、新しいルールに基づいたクライアントの次の接続試行でクライアントの新しい変換を作成できません。

NAT の例

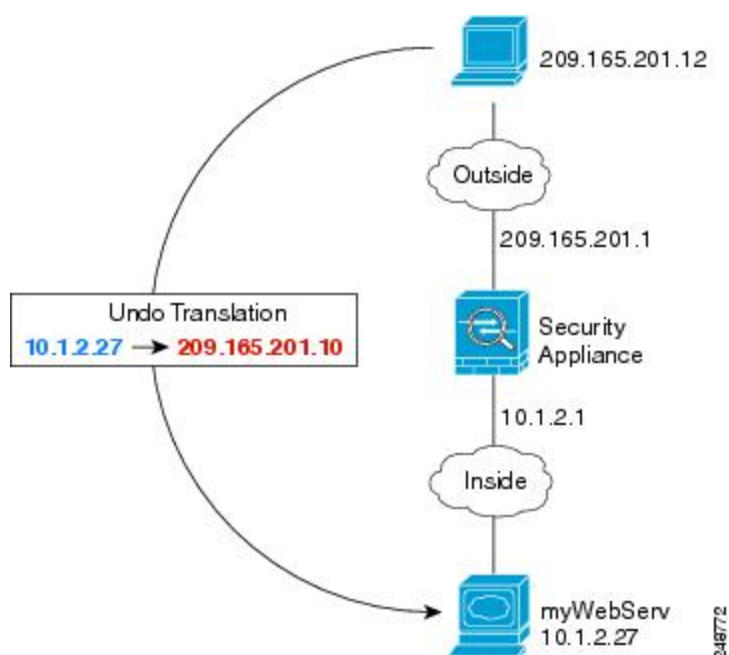
以下の各トピックでは、Threat Defense デバイスでの NAT の設定例を紹介します。

内部 Web サーバへのアクセスの提供 (スタティック自動 NAT)

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin

次の例では、内部 Web サーバに対してスタティック NAT を実行します。実際のアドレスはプライベート ネットワーク上にあるため、パブリック アドレスが必要です。スタティック NAT は、固定アドレスにある Web サーバへのトラフィックをホストが開始できるようにするために必要です

図 14: 内部 Web サーバのスタティック NAT



始める前に

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

手順

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

- [**オブジェクト (Objects)**] > [**オブジェクト管理 (Object Management)**] を選択します。
- 目次から [**ネットワーク (Network)**] を選択して、[**ネットワークの追加 (Add Network)**] > [**オブジェクトの追加 (Add Object)**] をクリックします。
- Web サーバのプライベート アドレスを定義します。

ネットワーク オブジェクトに名前 (たとえば、WebServerPrivate) を付けて、実際のホスト IP アドレス 10.1.2.27 を入力します。



- [**保存 (Save)**] をクリックします。
- [**ネットワークの追加 (Add Network)**] > [**オブジェクトの追加 (Add Object)**] をクリックして、パブリック アドレスを定義します。

ネットワーク オブジェクトに名前 (たとえば、WebServerPublic) を付けて、ホストアドレス 209.165.201.10 を入力します。



- [**保存 (Save)**] をクリックします。

ステップ 2 オブジェクトのスタティック NAT を設定します。

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

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

Add NAT Rule

- f) [保存 (Save)] をクリックします。

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

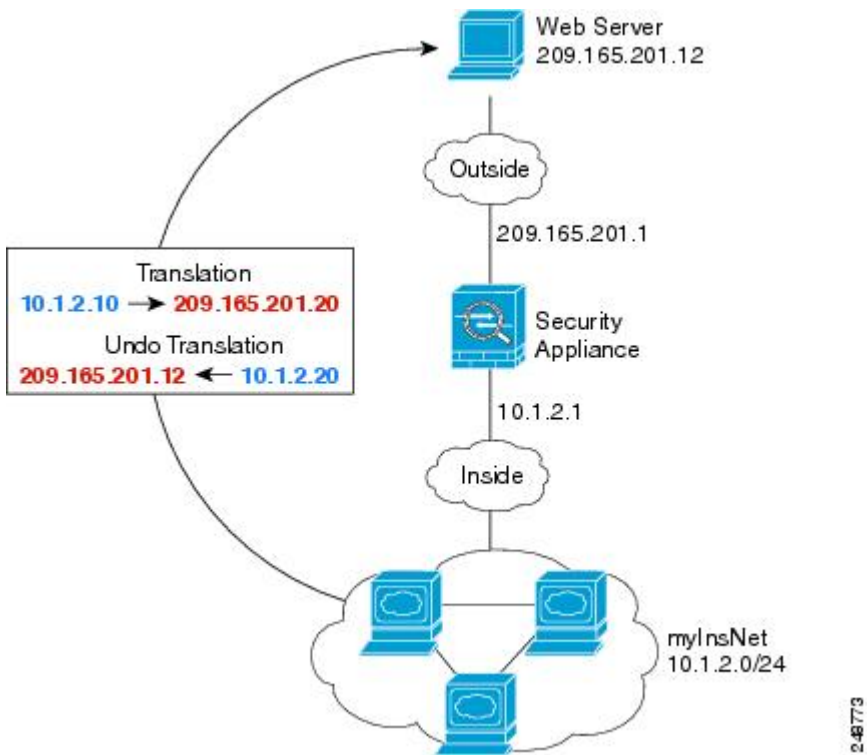
内部ホストのダイナミック自動 NAT および外部 Web サーバのスタティック NAT

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin

次の例では、プライベートネットワーク上の内部ユーザが外部にアクセスする場合、このユーザにダイナミック NAT を設定します。また、内部ユーザが外部 Web サーバに接続する場合、

この Web サーバのアドレスが内部ネットワークに存在するように見えるアドレスに変換されます。

図 15: 内部の動的 NAT、外部 Web サーバの静的 NAT



始める前に

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

手順

- ステップ 1** 内部アドレスを変換する動的 NAT プールのネットワーク オブジェクトを作成します。
- [オブジェクト (Objects)] > [オブジェクト管理 (Object Management)] を選択します。
 - コンテンツのテーブルから [ネットワーク (Network)] を選択し、[ネットワークを追加 (Add Network)] > [オブジェクトの追加 (Add Object)] をクリックします。
 - 動的 NAT プールを定義します。

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

New Network Objects ? X

Name: myNATpool

Description:

Network: 209.165.201.20-209.165.201.30
Format: ipaddr or ipaddr/len or range (2.2.2.10-2.2.2.20)

Allow Overrides:

d) [保存 (Save)]をクリックします。

ステップ2 内部ネットワークのネットワーク オブジェクトを作成します。

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

New Network Objects

Name: MyInsNet

Description:

Network: 10.1.2.0/24

Allow Overrides:

c) [保存 (Save)]をクリックします。

ステップ3 外部 Web サーバのネットワーク オブジェクトを作成します。

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

New Network Objects

Name: myWebServer

Description:

Network: 209.165.201.12

Allow Overrides:

c) [保存 (Save)]をクリックします。

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

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

Name:	TransWebServer
Description:	
Network:	10.1.2.20
Allow Overrides:	<input checked="" type="checkbox"/>

- c) [保存 (Save)] をクリックします。

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

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

Add NAT Rule

f) [保存 (Save)]をクリックします。

ステップ 6 Web サーバのスタティック NAT を設定します。

a) [ルール追加 (Add Rule)]をクリックします。

b) 次のプロパティを設定します。

- [NAT ルール (NAT Rule)] = 自動 NAT ルール (Auto NAT Rule) 。
- [タイプ (Type)] = スタティック (Static) 。

c) [インターフェイス オブジェクト (Interface Objects)] タブで、以下の設定を行います。

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

d) [変換 (Translation)] タブで、次の項目を設定します。

- [元の発信元 (Original Source)] = myWebServer ネットワーク オブジェクト。
- [変換済みの発信元アドレス (Translated Source Address)] = TransWebServer ネットワーク オブジェクト。 >

Add NAT Rule

e) [保存 (Save)]をクリックします。

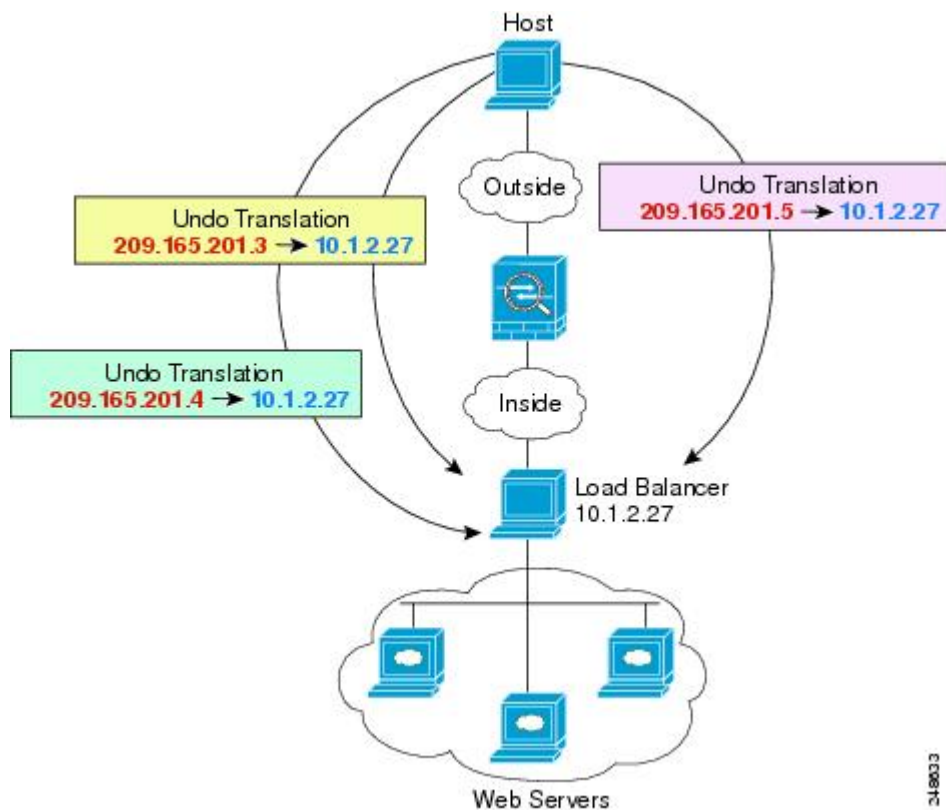
ステップ7 [NAT ルール (NAT rule)] ページで [保存 (Save)] をクリックします。

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

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin

次の例は、複数の IP アドレスに変換される内部ロード バランサを示しています。外部ホストがマッピング IP アドレスの 1 つにアクセスする場合、1 つのロード バランサのアドレスには変換されません。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 16: 内部ロード バランサのスタティック NAT (1 対多)



始める前に

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

手順

ステップ 1 ロードバランサをマッピングするアドレスに対し、ネットワーク オブジェクトを作成します。

- [オブジェクト (Objects)] > [オブジェクト管理 (Object Management)] を選択します。
- コンテンツのテーブルから [ネットワーク (Network)] を選択し、[ネットワークを追加 (Add Network)] > [オブジェクトの追加 (Add Object)] をクリックします。
- アドレスを定義します。

ネットワーク オブジェクトに名前 (たとえば、myPublicIPs) を付けて、ネットワーク範囲 209.165.201.3-209.165.201.5 を入力します。

- [保存 (Save)] をクリックします。

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

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

c) [保存 (Save)] をクリックします。

ステップ 3 ロードバランサのスタティック NAT を設定します。

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

Add NAT Rule

The screenshot shows the 'Add NAT Rule' configuration interface. At the top, 'NAT Rule' is set to 'Auto NAT Rule' and 'Type' is 'Static'. An 'Enable' checkbox is checked. Below this are tabs for 'Interface Objects', 'Translation', 'PAT Pool', and 'Advanced'. The 'Translation' tab is selected, showing two columns: 'Original Packet' and 'Translated Packet'. In the 'Original Packet' column, 'Original Source:*' is set to 'myLBHost' and 'Original Port' is set to 'TCP'. In the 'Translated Packet' column, 'Translated Source' is set to 'Address' and 'Translated Port' is empty.

f) [保存 (Save)] をクリックします。

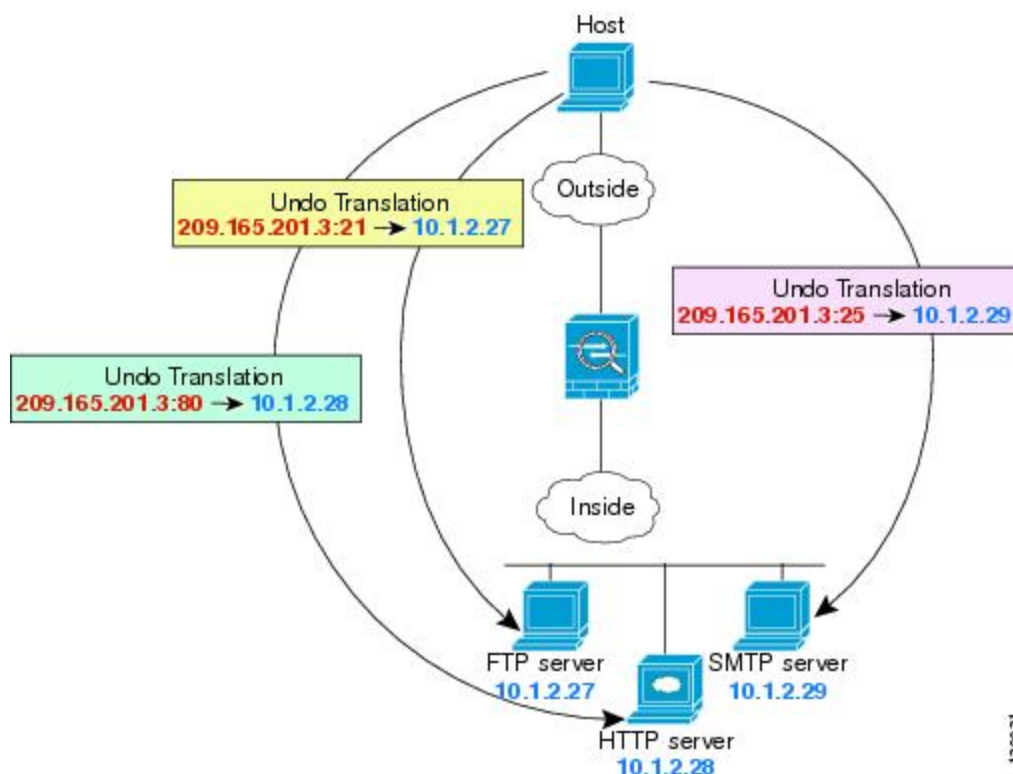
ステップ 4 [NAT ルール (NAT rule)] ページで [保存 (Save)] をクリックします。

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

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin

次のポート変換を設定したスタティック NAT の例では、リモートユーザが FTP、HTTP、および SMTP にアクセスするための単一のアドレスを提供します。これらのサーバは実際には、それぞれ異なるデバイスとして実際のネットワーク上に存在しますが、ポート変換を設定したスタティック NAT ルールを指定すると、使用するマッピング IP アドレスは同じで、それぞれ別のポートを使用することができます。

図 17: ポート変換を設定したスタティック NAT



始める前に

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

(Objects)]> [オブジェクト管理 (Object Management)] を選択し、[インターフェイス (Interface)] を選択します。

手順

ステップ 1 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)]> [オブジェクト管理 (Object Management)] を選択します。
- コンテンツのテーブルから [ネットワーク (Network)] を選択し、[ネットワークの追加 (Add Network)]> [オブジェクトの追加 (Add Object)] をクリックします。
- ネットワーク オブジェクトに名前を付け (たとえば「FTPserver」)、FTP サーバの実際の IP アドレス (10.1.2.27) を入力します。

New Network Objects

Name:	FTPserver
Description:	
Network:	10.1.2.27
Allow Overrides:	<input checked="" type="checkbox"/>

- [保存 (Save)] 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。

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

New Network Objects

Name:	HTTPserver
Description:	
Network:	10.1.2.28
Allow Overrides:	<input checked="" type="checkbox"/>

- [保存 (Save)] 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。

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

Edit Network Objects

Name:	SMTPserver
Description:	
Network:	10.1.2.29
Allow Overrides:	<input checked="" type="checkbox"/>

- c) [保存 (Save)]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) [ネットワークの追加 (Add Network)]>[オブジェクトの追加 (Add Object)]をクリックします。
- b) ネットワーク オブジェクトに名前を付け (たとえば「ServerPublicIP」) 、ホストアドレス (209.165.201.3) を入力します。

New Network Objects

Name:	ServerPublicIP
Description:	
Network:	209.165.201.3
Allow Overrides:	<input checked="" type="checkbox"/>

- c) [保存 (Save)]をクリックします。

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

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

- [元のポート (Original Port)] > [TCP] = 21。
- [変換済みポート (Translated Port)] = 21。

Add NAT Rule

f) [保存 (Save)] をクリックします。

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

- [ルール の追加 (Add Rule)] をクリックします。
- 次のプロパティを設定します。
 - [NAT ルール (NAT Rule)] = 自動 NAT ルール (Auto NAT Rule) 。
 - [タイプ (Type)] = スタティック (Static) 。
- [インターフェイス オブジェクト (Interface Objects)] タブで、次の項目を設定します。
 - [送信元インターフェイス オブジェクト (Source Interface Objects)] = inside。
 - [宛先インターフェイス オブジェクト (Destination Interface Objects)] = outside。
- [変換 (Translation)] タブで、次の項目を設定します。
 - [元の発信元 (Original Source)] = HTTPserver ネットワーク オブジェクト。
 - [変換済みの発信元 (Translated Source)] > [アドレス (Address)] = ServerPublicIP ネットワーク オブジェクト。
 - [元のポート (Original Port)] > [TCP] = 80。
 - [変換済みポート (Translated Port)] = 80。

Add NAT Rule

The screenshot shows the 'Add NAT Rule' configuration interface. At the top, 'NAT Rule' is set to 'Auto NAT Rule' and 'Type' is 'Static'. There is an 'Enable' checkbox. Below this are tabs for 'Interface Objects', 'Translation', 'PAT Pool', and 'Advanced'. The 'Translation' tab is selected. It is divided into two sections: 'Original Packet' and 'Translated Packet'. In the 'Original Packet' section, 'Original Source' is 'HTTPserver' and 'Original Port' is 'TCP' with a value of '80'. In the 'Translated Packet' section, 'Translated Source' is 'Address' with a value of 'ServerPublicIP' and 'Translated Port' is '80'.

e) [保存 (Save)]をクリックします。

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

a) [ルール の追加 (Add Rule)]をクリックします。

b) 次のプロパティを設定します。

- [NAT ルール (NAT Rule)] = 自動 NAT ルール (Auto NAT Rule) 。
- [タイプ (Type)] = スタティック (Static) 。

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

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

d) [変換 (Translation)] タブで、次の項目を設定します。

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

Add NAT Rule

NAT Rule: Auto NAT Rule

Type: Static Enable

Interface Objects Translation PAT Pool Advanced

Original Packet

Original Source:* SMTPserver

Original Port: TCP 25

Translated Packet

Translated Source: Address

ServerPublicIP

Translated Port: 25

e) [保存 (Save)] をクリックします。

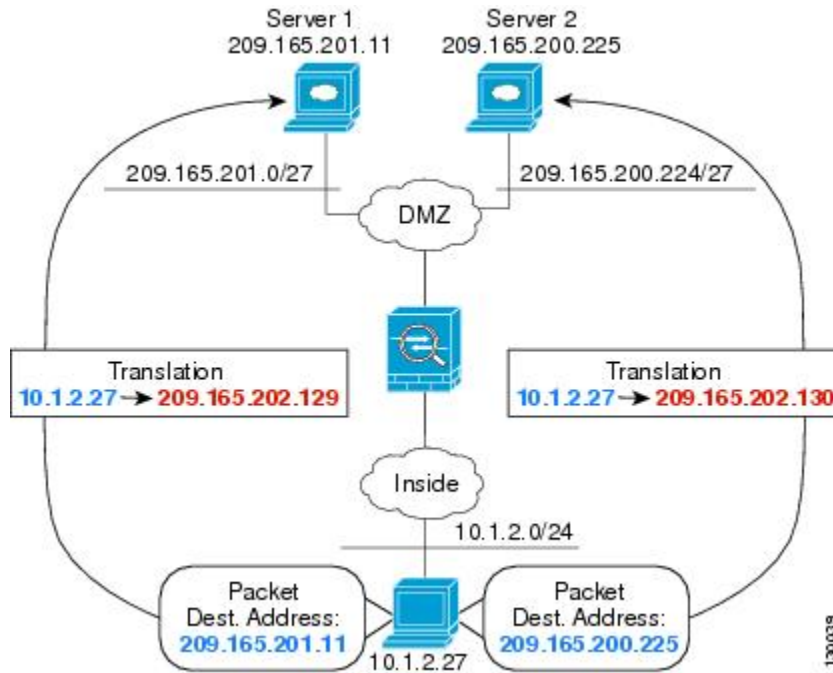
ステップ 8 [NAT ルール (NAT rule)] ページで [保存 (Save)] をクリックします。

宛先に応じて異なる変換 (ダイナミック手動 PAT)

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin

次の図に、2 台の異なるサーバにアクセスしている 10.1.2.0/24 ネットワークのホストを示します。ホストがサーバ 209.165.201.11 にアクセスすると、実際のアドレスは 209.165.202.129:ポートに変換されます。ホストがサーバ 209.165.200.225 にアクセスすると、実際のアドレスは 209.165.202.130:ポートに変換されます。

図 18:異なる宛先アドレスを使用する手動 NAT



始める前に

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

手順

- ステップ 1** 内部ネットワークのネットワーク オブジェクトを作成します。
- [オブジェクト (Objects)] > [オブジェクト管理 (Object Management)] を選択します。
 - コンテンツのテーブルから [ネットワーク (Network)] を選択し、[ネットワークを追加 (Add Network)] > [オブジェクトの追加 (Add Object)] をクリックします。
 - ネットワーク オブジェクトに名前を付け (myInsideNetwork など)、実際のネットワーク アドレス 10.1.2.0/24 を入力します。

New Network Objects

Name:	myInsideNetwork
Description:	
Network:	10.1.2.0/24
Allow Overrides:	<input checked="" type="checkbox"/>

d) [保存 (Save)] をクリックします。

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

- [ネットワークを追加 (Add Network)] > [オブジェクトの追加 (Add Object)] をクリックします。
- ネットワーク オブジェクトに名前を付け (DMZnetwork1 など)、ネットワーク アドレス 209.165.201.0/27 を入力します (255.255.255.224 のサブネット マスク)。

New Network Objects

Name:	DMZnetwork1
Description:	
Network:	209.165.201.0/27
Allow Overrides:	<input checked="" type="checkbox"/>

c) [保存 (Save)] をクリックします。

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

- [ネットワークを追加 (Add Network)] > [オブジェクトの追加 (Add Object)] をクリックします。
- ネットワーク オブジェクトに名前を付け (PATaddress1 など)、ホスト アドレス 209.165.202.129 を入力します。

New Network Objects

Name:	PATaddress1
Description:	
Network:	209.165.202.129
Allow Overrides:	<input checked="" type="checkbox"/>

c) [保存 (Save)] をクリックします。

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

- [ネットワークを追加 (Add Network)] > [オブジェクトの追加 (Add Object)] をクリックします。

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

New Network Objects

Name:	DMZnetwork2
Description:	
Network:	209.165.200.224/27
Allow Overrides:	<input checked="" type="checkbox"/>

- c) [保存 (Save)] をクリックします。

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

- a) [ネットワークを追加 (Add Network)] > [オブジェクトの追加 (Add Object)] をクリックします。
- b) ネットワーク オブジェクトに名前を付け (PATaddress2 など)、ホスト アドレス 209.165.202.130 を入力します。

New Network Objects

Name:	PATaddress2
Description:	
Network:	209.165.202.130
Allow Overrides:	<input checked="" type="checkbox"/>

- c) [保存 (Save)] をクリックします。

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

- a) [デバイス (Devices)] > [NAT] を選択し、Firepower Threat Defense NAT ポリシーを作成または編集します。
- b) [ルール of の追加 (Add Rule)] をクリックします。
- c) 次のプロパティを設定します。
- [NAT ルール (NAT Rule)] = 手動 NAT ルール。
 - [タイプ (Type)] = Dynamic。
- d) [インターフェイス オブジェクト (Interface Objects)] タブで、以下の設定を行います。
- [送信元インターフェイス オブジェクト (Source Interface Objects)] = inside。
 - [宛先インターフェイス オブジェクト (Destination Interface Objects)] = dmz。
- e) [変換 (Translation)] タブで、次の項目を設定します。
- [元の発信元 (Original Source)] = myInsideNetwork ネットワーク オブジェクト。

- [変換済みの発信元アドレス (Translated Source Address)] = PATAddress1 ネットワーク オブジェクト。
- [元の宛先アドレス (Original Destination Address)] = DMZnetwork1 ネットワーク オブジェクト。 >
- [変換済みの宛先 (Translated Destination)] = DMZnetwork1 ネットワーク オブジェクト。

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

Add NAT Rule

The screenshot shows the 'Add NAT Rule' configuration interface. At the top, 'NAT Rule' is set to 'Manual NAT Rule' and 'Type' is 'Dynamic'. The 'Enable' checkbox is checked. Below this, there are tabs for 'Interface Objects', 'Translation', 'PAT Pool', and 'Advanced'. The 'Translation' tab is active, showing two columns: 'Original Packet' and 'Translated Packet'. Under 'Original Packet', 'Original Source' is 'myInsideNetwork', 'Original Destination' is 'Address', and 'Translated Destination' is 'DMZNetwork1'. Under 'Translated Packet', 'Translated Source' is 'Address' and 'PATAddress1'.

f) [保存 (Save)] をクリックします。

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

- [ルール の追加 (Add Rule)] をクリックします。
- 次のプロパティを設定します。
 - [NAT ルール (NAT Rule)] = 手動 NAT ルール。
 - [タイプ (Type)] = Dynamic。
- [インターフェイス オブジェクト (Interface Objects)] タブで、以下の設定を行います。
 - [送信元インターフェイス オブジェクト (Source Interface Objects)] = inside。
 - [宛先インターフェイス オブジェクト (Destination Interface Objects)] = dmz。
- [変換 (Translation)] タブで、次の項目を設定します。
 - [元の発信元 (Original Source)] = myInsideNetwork ネットワーク オブジェクト。
 - [変換済みの発信元アドレス (Translated Source Address)] = PATAddress2 ネットワーク オブジェクト。 >

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)

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

Add NAT Rule

NAT Rule: Manual NAT Rule Insert: In Category NAT Rules Before

Type: Dynamic Enable

Description:

Interface Objects **Translation** PAT Pool Advanced

Original Packet

Original Source:* myInsideNetwork

Original Destination: Address

DMZNetwork2

Translated Packet

Translated Source: Address

PATaddress2

Translated Destination: DMZNetwork2

e) [保存 (Save)] をクリックします。

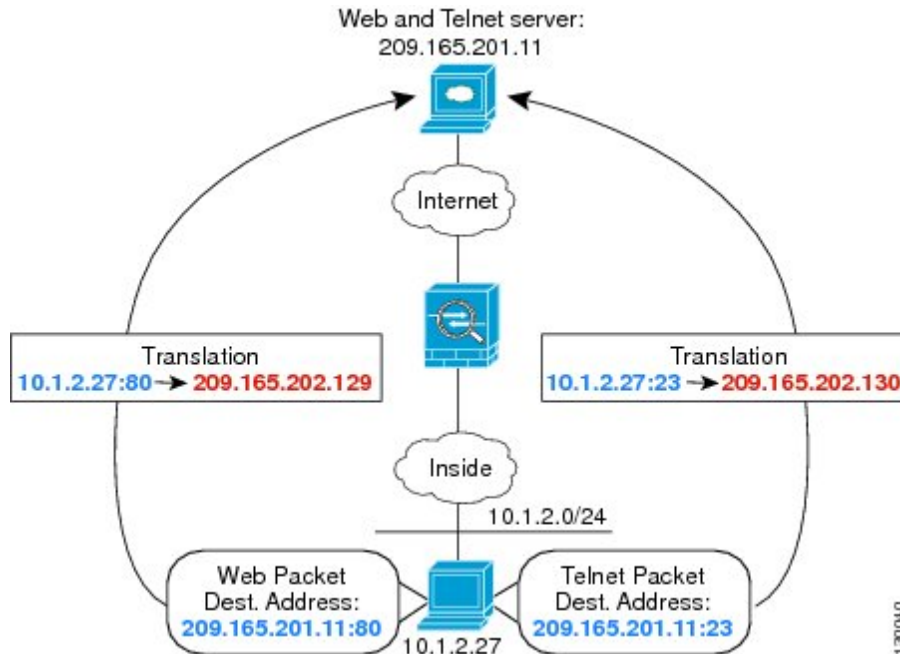
ステップ 8 [NAT ルール (NAT rule)] ページで [保存 (Save)] をクリックします。

宛先アドレスおよびポートに応じて異なる変換 (ダイナミック手動 PAT)

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin

次の図に、送信元ポートおよび宛先ポートの使用例を示します。10.1.2.0/24 ネットワークのホストは Web サービスと Telnet サービスの両方を提供する 1 つのホストにアクセスします。ホストが Telnet サービスを求めてサーバにアクセスすると、実際のアドレスは 209.165.202.129:ポートに変換されます。ホストが Web サービスを求めて同じサーバにアクセスすると、実際のアドレスは 209.165.202.130:ポートに変換されます。

図 19:異なる宛先ポートを使用する手動 NAT



始める前に

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

手順

ステップ 1 内部ネットワークのネットワーク オブジェクトを作成します。

- [オブジェクト (Objects)] > [オブジェクト管理 (Object Management)] を選択します。
- コンテンツのテーブルから [ネットワーク (Network)] を選択し、[ネットワークを追加 (Add Network)] > [オブジェクトの追加 (Add Object)] をクリックします。
- ネットワーク オブジェクトに名前を付け (myInsideNetwork など)、実際のネットワーク アドレス 10.1.2.0/24 を入力します。

New Network Objects

Name:	myInsideNetwork
Description:	
Network:	10.1.2.0/24
Allow Overrides:	<input checked="" type="checkbox"/>

d) [保存 (Save)]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。

- [ネットワークを追加 (Add Network)]>[オブジェクトの追加 (Add Object)]をクリックします。
- ネットワーク オブジェクトに名前を付け (TelnetWebServer など)、ホスト アドレス 209.165.201.11 を入力します。

New Network Objects

Name:	TelnetWebServer
Description:	
Network:	209.165.201.11
Allow Overrides:	<input checked="" type="checkbox"/>

c) [保存 (Save)]をクリックします。

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

- [ネットワークを追加 (Add Network)]>[オブジェクトの追加 (Add Object)]をクリックします。
- ネットワーク オブジェクトに名前を付け (PATAddress1 など)、ホスト アドレス 209.165.202.129 を入力します。

New Network Objects

Name:	PATAddress1
Description:	
Network:	209.165.202.129
Allow Overrides:	<input checked="" type="checkbox"/>

c) [保存 (Save)]をクリックします。

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

- [ネットワークを追加 (Add Network)]>[オブジェクトの追加 (Add Object)]をクリックします。

- b) ネットワーク オブジェクトに名前を付け (PATaddress2 など)、ホストアドレス 209.165.202.130 を入力します。

New Network Objects

Name:	PATaddress2
Description:	
Network:	209.165.202.130
Allow Overrides:	<input checked="" type="checkbox"/>

- c) [保存 (Save)] をクリックします。

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

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

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

Add NAT Rule

NAT Rule:	Manual NAT Rule	Insert:	In Category	NAT Rules Before
Type:	Dynamic	<input checked="" type="checkbox"/> Enable		
Description:				
Interface Objects Translation PAT Pool Advanced				
Original Packet			Translated Packet	
Original Source:*	myInsideNetwork	Translated Source:	Address	
Original Destination:	Address		PATAddress1	
	TelnetWebServer	Translated Destination:	TelnetWebServer	
Original Source Port:		Translated Source Port:		
Original Destination Port:	TELNET	Translated Destination Port:	TELNET	

- f) [保存 (Save)] をクリックします。

ステップ 6 Web アクセスのダイナミック手動 PAT を設定します。

- [ルール の追加 (Add Rule)] をクリックします。
- 次のプロパティを設定します。
 - [NAT ルール (NAT Rule)] = 手動 NAT ルール。
 - [タイプ (Type)] = Dynamic。
- [インターフェイス オブジェクト (Interface Objects)] タブで、以下の設定を行います。
 - [送信元インターフェイス オブジェクト (Source Interface Objects)] = inside。
 - [宛先インターフェイス オブジェクト (Destination Interface Objects)] = dmz。
- [変換 (Translation)] タブで、次の項目を設定します。
 - [元の発信元 (Original Source)] = myInsideNetwork ネットワーク オブジェクト。
 - [変換済みの発信元アドレス (Translated Source Address)] = PATAddress2 ネットワーク オブジェクト。 >
 - [元の宛先アドレス (Original Destination Address)] = TelnetWebServer ネットワーク オブジェクト。 >
 - [変換済みの宛先 (Translated Destination)] = TelnetWebServer ネットワーク オブジェクト。

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

Add NAT Rule

NAT Rule: Insert:

Type: Enable

Description:

Interface Objects **Translation** PAT Pool Advanced

Original Packet	Translated Packet
Original Source:* <input type="text" value="myInsideNetwork"/>	Translated Source: <input type="text" value="Address"/>
Original Destination: <input type="text" value="Address"/> <input type="text" value="TelnetWebServer"/>	Translated Destination: <input type="text" value="TelnetWebServer"/>
Original Source Port: <input type="text"/>	Translated Source Port: <input type="text"/>
Original Destination Port: <input type="text" value="HTTP"/>	Translated Destination Port: <input type="text" value="HTTP"/>

e) [保存 (Save)] をクリックします。

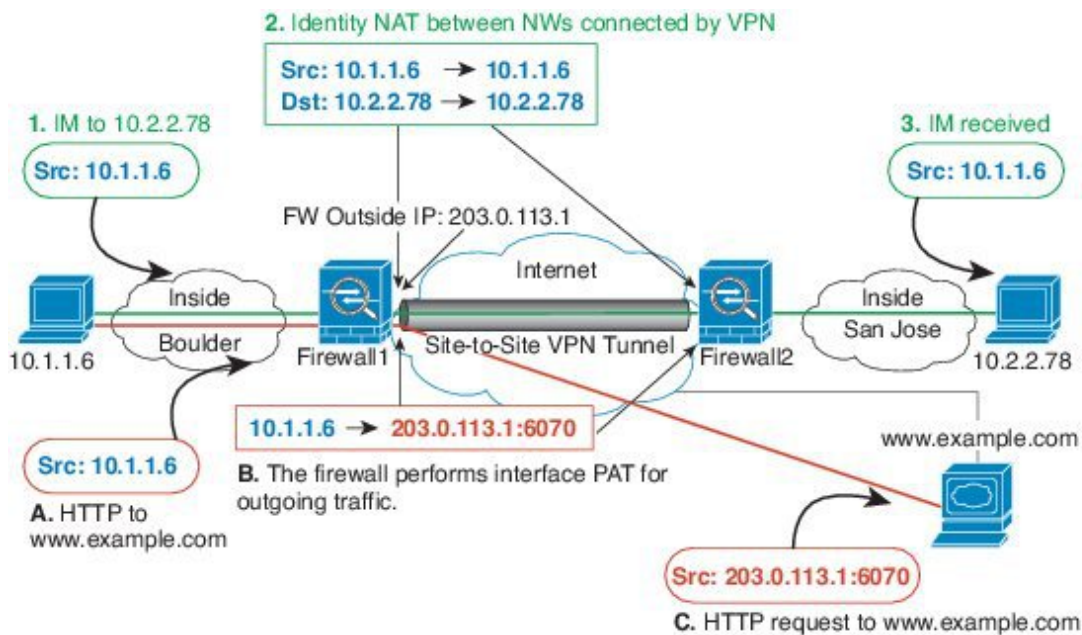
ステップ 7 [NAT ルール (NAT rule)] ページで [保存 (Save)] をクリックします。

NAT およびサイト間 VPN

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin

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

図 20: サイトツーサイト VPN のためのインターフェイス PAT およびアイデンティティ NAT



次の例は、Firewall1（ボールドー）の設定を示します。

始める前に

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

手順

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

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

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

New Network Objects ? X

Name:

Description:

Network:
 Format: ipaddr or ipaddr/len
 or range (2.2.2.10-2.2.2.20)

Allow Overrides:

- d) [保存 (Save)] をクリックします。
- e) [ネットワークの追加 (Add Network)] > [オブジェクトの追加 (Add Object)] をクリックして、内部サンノゼ ネットワークを定義します。

ネットワーク オブジェクトに名前 (たとえば、sanjose-network) を付けて、ネットワーク アドレス 10.2.2.0/24 を入力します。

New Network Objects ? X

Name:

Description:

Network:
 Format: ipaddr or ipaddr/len
 or range (2.2.2.10-2.2.2.20)

Allow Overrides:

- f) [保存 (Save)] をクリックします。

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

- a) [デバイス (Devices)] > [NAT] を選択し、Firepower Threat Defense NAT ポリシーを作成または編集します。
- b) [ルールの追加 (Add Rule)] をクリックします。
- c) 次のプロパティを設定します。
- [NAT ルール (NAT Rule)] = 手動 NAT ルール (Manual NAT Rule) 。
 - [タイプ (Type)] = スタティック (Static) 。
- d) [インターフェイス オブジェクト (Interface Objects)] タブで、次の項目を設定します。
- [送信元インターフェイス オブジェクト (Source Interface Objects)] = inside-boulder。
 - [宛先インターフェイス オブジェクト (Destination Interface Objects)] = outside-boulder。
- e) [変換 (Translation)] タブで、次の項目を設定します。
- [元の送信元 (Original Source)] = boulder-network オブジェクト。

- [変換済みの送信元 (Translated Source)] > [アドレス (Address)] = boulder-network オブジェクト。
- [元の宛先 (Original Destination)] > [アドレス (Address)] = sanjose-network オブジェクト。
- [変換済みの宛先] = sanjose-network オブジェクト。

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

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

Add NAT Rule

The screenshot shows the 'Add NAT Rule' configuration interface. At the top, 'NAT Rule' is set to 'Manual NAT Rule' and 'Type' is 'Static'. The 'Insert' dropdown is set to 'In Category' and 'NAT Rules Before'. The 'Description' field is empty. Below this are tabs for 'Interface Objects', 'Translation', 'PAT Pool', and 'Advanced'. The 'Translation' tab is active, showing 'Original Packet' and 'Translated Packet' sections. In 'Original Packet', 'Original Source' is 'boulder-network', and 'Original Destination' is 'Address' and 'sanjose-network'. In 'Translated Packet', 'Translated Source' is 'Address' and 'Translated Destination' is 'sanjose-network'.

- g) [保存 (Save)] をクリックします。

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

- a) [ルールの追加 (Add Rule)] をクリックします。
- b) 次のプロパティを設定します。
- [NAT ルール (NAT Rule)] = 手動 NAT ルール。
 - [タイプ (Type)] = ダイナミック (Dynamic) 。
 - [挿入ルール (Insert Rule)] = 最初のルールの後の任意の位置。このルールは任意の宛先アドレスに適用されるため、sanjose-network を宛先として使用するルールはこのルールの前に来る必要があります。そうでなければ、sanjose-network ルールは永遠に一致することがありません。デフォルトでは、新しい手動 NAT ルールは [自動 NAT の前に NAT ルール (NAT Rules Before Auto NAT)] セクションの最後に配置されます。
- c) [インターフェイス オブジェクト (Interface Objects)] タブで、次の項目を設定します。

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

d) [変換 (Translation)] タブで、次の項目を設定します。

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

Add NAT Rule

The screenshot shows the 'Add NAT Rule' configuration interface. At the top, 'NAT Rule' is set to 'Manual NAT Rule' and 'Type' is 'Dynamic'. The 'Translation' tab is selected, showing 'Original Packet' and 'Translated Packet' sections. In the 'Original Packet' section, 'Original Source' is 'boulder-network' and 'Original Destination' is 'Address'. In the 'Translated Packet' section, 'Translated Source' is 'Destination Interface IP' and 'Translated Destination' is blank. A note indicates that values for 'Destination Interface Objects' in the 'Interface Objects' tab will be used.

e) [保存 (Save)] をクリックします。

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

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

NAT を使用した DNS クエリと応答の書き換え

応答内のアドレスを NAT コンフィギュレーションと一致するアドレスに置き換えて、DNS 応答を修正するように Firepower Threat Defense デバイスを設定することが必要になる場合があります。DNS 修正は、各トランスレーションルールを設定するときに設定できます。

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

以下に、NAT ルールで DNS のリライトを設定する必要が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 のリライトが必要です。
- DNS サーバは外部にあり、クライアントは内部にあります。クライアントが使用する一部の完全修飾ドメイン名が他の内部ホストに解決されます。
- DNS サーバは内部にあり、プライベート IP アドレスを使用して応答します。クライアントは外部にあり、クライアントは内部でホストされているサーバを指定する完全修飾ドメイン名にアクセスします。

DNS リライトに関する制限事項

次に DNS リライトの制限事項を示します。

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

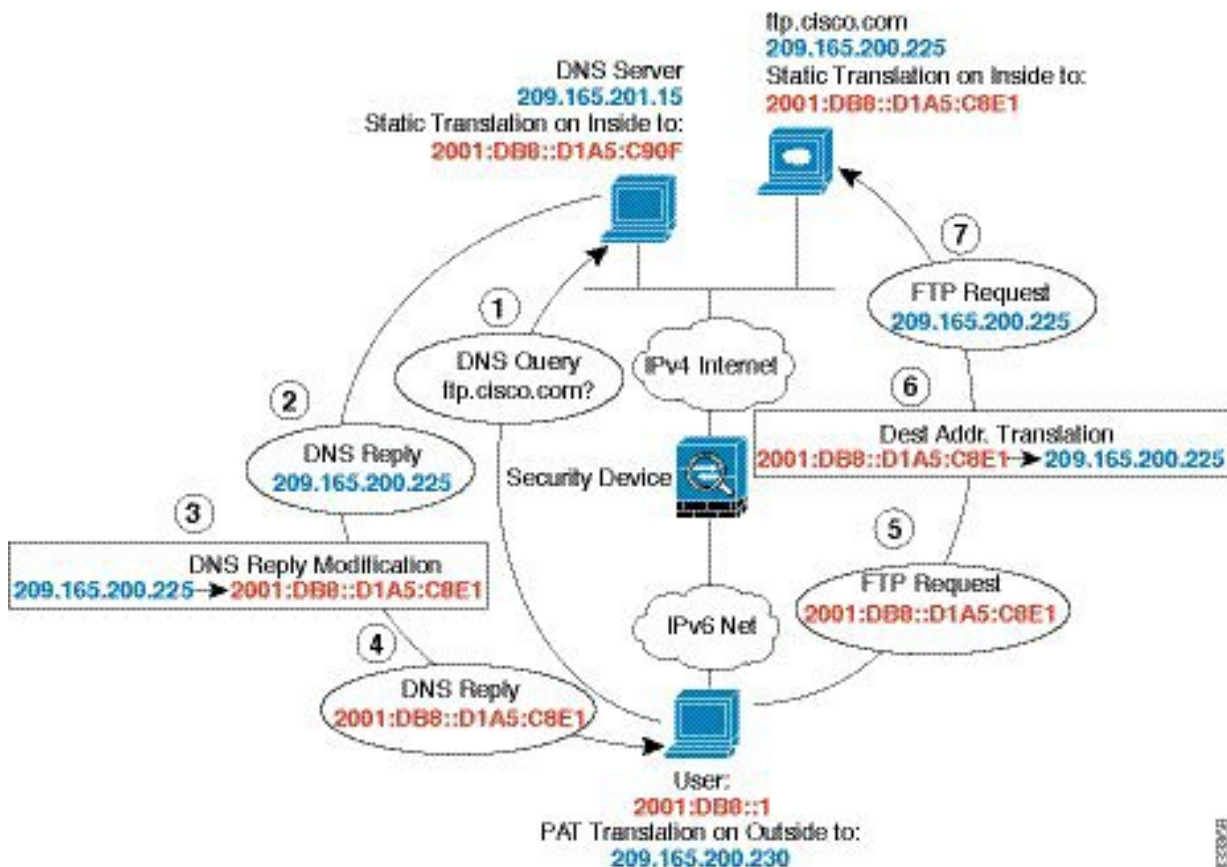
次のトピックで、NAT ルールでの DNS リライトの例を示します。

DNS64 応答修正

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin

次の図に、外部の IPv4 ネットワーク上の FTP サーバと DNS サーバを示します。システムには、外部サーバ用のスタティック変換があります。この場合、内部 IPv6 ユーザが ftp.cisco.com のアドレスを DNS サーバに要求すると、DNS サーバは実際のアドレス (209.165.200.225) を応答します。

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



始める前に

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

手順

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

- a) **[オブジェクト (Objects)] > [オブジェクト管理 (Object Management)]** を選択します。
- b) コンテンツのテーブルから **[ネットワーク (Network)]** を選択し、**[ネットワークを追加 (Add Network)] > [オブジェクトの追加 (Add Object)]** をクリックします。
- 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)、ホストアドレス 209.165.200.225 を入力します。

The screenshot shows a dialog box titled "New Network Objects" with a close button (X) and a help button (?). It contains the following fields and options:

- Name:** ftp_server
- Description:** (empty text area)
- Network:** 209.165.200.225
- Format:** ipaddr or ipaddr/len or range (ipaddr-ipaddr)
- Allow Overrides:**

- d) **[保存 (Save)]** をクリックします。
- e) **[ネットワークを追加 (Add Network)] > [オブジェクトの追加 (Add Object)]** をクリックして、FTP サーバの変換済み IPv6 アドレスを定義します。

ネットワーク オブジェクトに名前を付け (ftp_server_v6 など)、ホストアドレス 2001:DB8::D1A5:C8E1 を入力します。

New Network Objects ? x

Name: ftp_server_v6

Description:

Network: 2001:DB8::D1A5:C8E1
Format: ipaddr or ipaddr/len or range (ipaddr-ipaddr)

Allow Overrides:

- f) [保存 (Save)] をクリックします。
- g) [ネットワークを追加 (Add Network)] > [オブジェクトの追加 (Add Object)] をクリックして、DNS サーバの実際のアドレスを定義します。

ネットワーク オブジェクトに名前を付け (dns_server など)、ホストアドレス 209.165.201.15 を入力します。

New Network Objects ? x

Name: dns_server

Description:

Network: 209.165.201.15
Format: ipaddr or ipaddr/len or range (ipaddr-ipaddr)

Allow Overrides:

- h) [保存 (Save)] をクリックします。
- i) [ネットワークを追加 (Add Network)] > [オブジェクトの追加 (Add Object)] をクリックして、DNS サーバの変換済み IPv6 アドレスを定義します。

ネットワーク オブジェクトに名前を付け (dns_server_v6 など)、ホストアドレス 2001:DB8::D1A5:C90F を入力します (ここで、D1A5:C90F は IPv6 の場合の 209.165.201.15 です)。

New Network Objects ? x

Name: dns_server_v6

Description:

Network: 2001:DB8::D1A5:C90F
Format: ipaddr or ipaddr/len or range (ipaddr-ipaddr)

Allow Overrides:

- j) [保存 (Save)] をクリックします。

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

ネットワーク オブジェクトに名前 (inside_v6 など) を付け、ネットワーク アドレス 2001:DB8::/96 を入力します。

New Network Objects ? x

Name:

Description:

Network:
 Format: ipaddr or ipaddr/len or range (ipaddr-ipaddr)

Allow Overrides:

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

ネットワーク オブジェクトに名前を付け (ipv4_pool など)、範囲 209.165.200.230 ~ 209.165.200.235 を入力します。

New Network Objects ? x

Name:

Description:

Network:
 Format: ipaddr or ipaddr/len or range (ipaddr-ipaddr)

Allow Overrides:

- n) [保存 (Save)] をクリックします。

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

- a) [デバイス (Devices)] > [NAT] を選択し、Firepower Threat Defense NAT ポリシーを作成または編集します。
- b) [ルールの追加 (Add Rule)] をクリックします。
- c) 次のプロパティを設定します。
- [NAT ルール (NAT Rule)] = 自動 NAT ルール (Auto NAT Rule)。
 - [タイプ (Type)] = スタティック (Static)。
- d) [インターフェイス オブジェクト (Interface Objects)] タブで、以下の設定を行います。
- [送信元インターフェイス オブジェクト (Source Interface Objects)] = outside。

- [宛先インターフェイス オブジェクト (Destination Interface Objects)] = inside。
- e) [変換 (Translation)] タブで、次の項目を設定します。
- [元の発信元 (Original Source)] = ftp_server ネットワーク オブジェクト。
 - [変換済みの発信元アドレス (Translated Source Address)] = ftp_server_v6 ネットワーク オブジェクト。 >

Add NAT Rule

The screenshot shows the 'Add NAT Rule' configuration interface. At the top, 'NAT Rule' is set to 'Auto NAT Rule' and 'Type' is 'Static'. Below this, there are tabs for 'Interface Objects', 'Translation', 'PAT Pool', and 'Advanced'. The 'Translation' tab is selected, showing two sections: 'Original Packet' and 'Translated Packet'. In the 'Original Packet' section, 'Original Source' is set to 'ftp_server' and 'Original Port' is set to 'TCP'. In the 'Translated Packet' section, 'Translated Source' is set to 'Address' and 'ftp_server_v6'.

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

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

- a) [ルール追加 (Add Rule)] をクリックします。
- b) 次のプロパティを設定します。
- [NAT ルール (NAT Rule)] = 自動 NAT ルール (Auto NAT Rule) 。
 - [タイプ (Type)] = スタティック (Static) 。
- c) [インターフェイス オブジェクト (Interface Objects)] タブで、以下の設定を行います。
- [送信元インターフェイス オブジェクト (Source Interface Objects)] = outside。
 - [宛先インターフェイス オブジェクト (Destination Interface Objects)] = inside。
- d) [変換 (Translation)] タブで、次の項目を設定します。
- [元の発信元 (Original Source)] = dns_server ネットワーク オブジェクト。
 - [変換済みの発信元アドレス (Translated Source Address)] = dns_server_v6 ネットワーク オブジェクト。 >
- e) これは 1 対 1 の NAT46 変換であるため、[詳細 (Advanced)] タブで、[ネット間マッピング (Net to Net Mapping)] を選択します。

Add NAT Rule

f) [OK] をクリックします。

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

a) [ルールの追加 (Add Rule)] をクリックします。

b) 次のプロパティを設定します。

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

c) [インターフェイス オブジェクト (Interface Objects)] タブで、以下の設定を行います。

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

d) [変換 (Translation)] タブで、次の項目を設定します。

- [元の発信元 (Original Source)] = inside_v6 ネットワーク オブジェクト。
- [変換済みの発信元アドレス (Translated Source Address)] > = このフィールドは空のままにします。

Add NAT Rule

e) [PAT プール (PAT Pool)] タブで、以下の設定を行います。

- [PAT プールの有効化 (Enable PAT Pool)] = このオプションを選択します。
- [変換済みの発信元アドレス (Translated Source Address)] = ipv4_pool ネットワーク オブジェクト。 >

Add NAT Rule

NAT Rule:

Type: Enable

Interface Objects Translation **PAT Pool** Advanced

Enable PAT Pool

PAT:

Use Round Robin Allocation

Extended PAT Table

Flat Port Range

Include Reserve Ports

f) [OK] をクリックします。

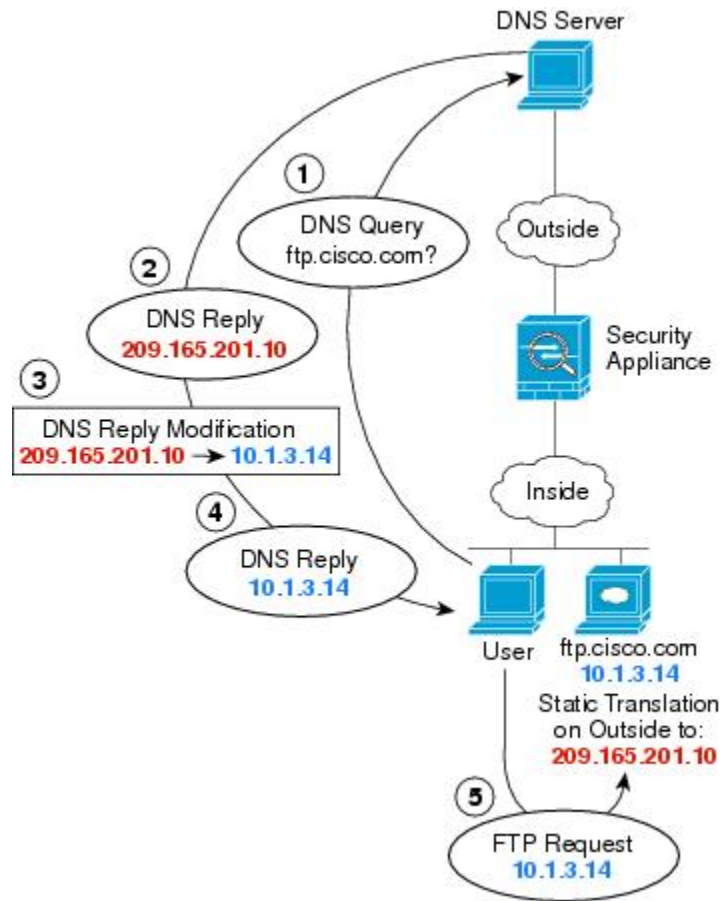
DNS 応答修正 : 外部の DNS サーバ

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin

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

この場合、このスタティック ルールで DNS 応答修正を有効にする必要があります。有効にすると、実際のアドレスを使用して ftp.cisco.com にアクセスできる内部ユーザは、マッピングアドレスではなく実際のアドレスを DNS サーバから受信できるようになります。

内部ホストが ftp.cisco.com のアドレスを求める DNS 要求を送信すると、DNS サーバはマッピングアドレス (209.165.201.10) を応答します。システムは、内部サーバのスタティック ルールを参照し、DNS 応答内のアドレスを 10.1.3.14 に変換します。DNS 応答修正を有効にしない場合、内部ホストは ftp.cisco.com に直接アクセスする代わりに、209.165.201.10 にトラフィックの送信を試みます。



始める前に

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

手順

ステップ 1 FTP サーバのネットワーク オブジェクトを作成します。

- [オブジェクト (Objects)] > [オブジェクト管理 (Object Management)]** を選択します。
- コンテンツのテーブルから **[ネットワーク (Network)]** を選択し、**[ネットワークを追加 (Add Network)] > [オブジェクトの追加 (Add Object)]** をクリックします。
- 実際の FTP サーバアドレスを定義します。

ネットワーク オブジェクトに名前を付け (ftp_server など)、ホストアドレス 10.1.3.14 を入力します。

New Network Objects ? x

Name:

Description:

Network:
 Format: ipaddr or ipaddr/len or range (ipaddr-ipaddr)

Allow Overrides:

- d) [保存 (Save)] をクリックします。
- e) [ネットワークを追加 (Add Network)] > [オブジェクトの追加 (Add Object)] をクリックして、FTP サーバの変換済みアドレスを定義します。

ネットワーク オブジェクトに名前を付け (ftp_server_outside など)、ホストアドレス 209.165.201.10 を入力します。

New Network Objects ? x

Name:

Description:

Network:
 Format: ipaddr or ipaddr/len or range (ipaddr-ipaddr)

Allow Overrides:

- f) [保存 (Save)] をクリックします。

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

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

DNS 応答修正 : ホスト ネットワーク上の DNS サーバ

- [変換済みの発信元アドレス (Translated Source Address)] = ftp_server_outside ネットワーク オブジェクト。 >

- f) [詳細 (Advanced)] 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

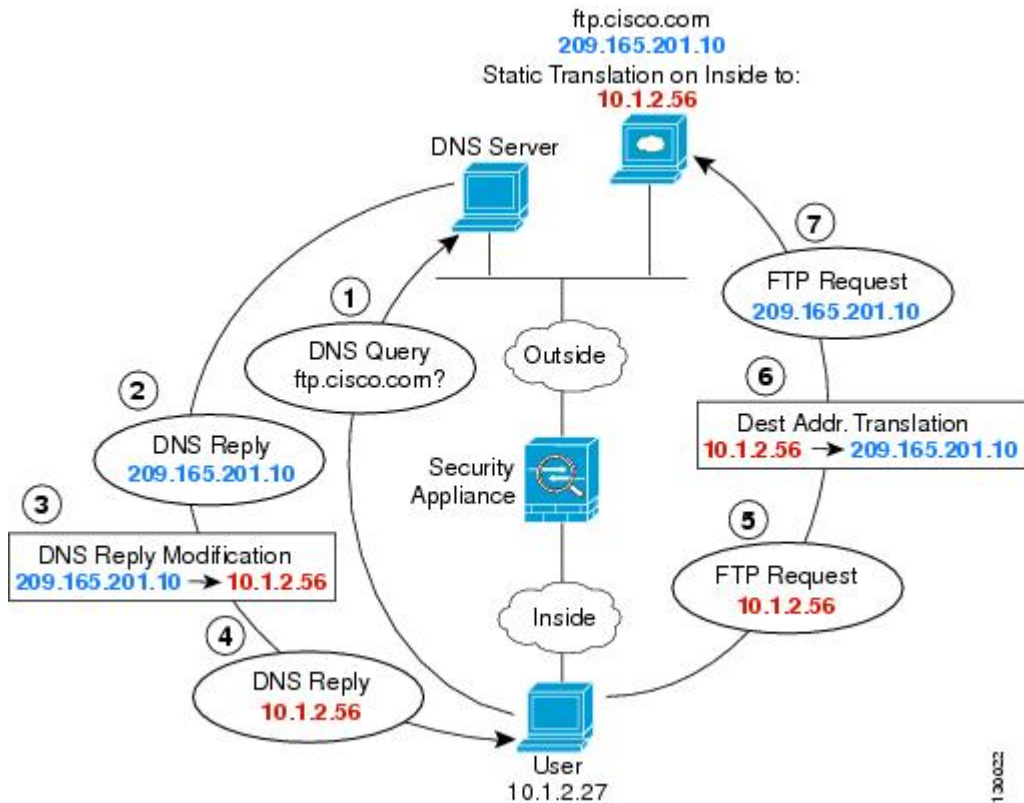
The screenshot shows the 'Add NAT Rule' configuration interface. The 'NAT Rule' is set to 'Auto NAT Rule' and the 'Type' is 'Static'. The 'Translation' tab is active. In the 'Original Packet' section, 'Original Source' is 'ftp_server' and 'Original Port' is 'TCP'. In the 'Translated Packet' section, 'Translated Source' is 'ftp_server_outside'.

- g) [OK] をクリックします。

DNS 応答修正 : ホスト ネットワーク上の DNS サーバ

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin

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



始める前に

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

手順

ステップ 1 FTP サーバのネットワーク オブジェクトを作成します。

- [オブジェクト (Objects)] > [オブジェクト管理 (Object Management)]** を選択します。
- コンテンツのテーブルから **[ネットワーク (Network)]** を選択し、**[ネットワークを追加 (Add Network)] > [オブジェクトの追加 (Add Object)]** をクリックします。
- 実際の FTP サーバアドレスを定義します。

ネットワーク オブジェクトに名前を付け (ftp_server など)、ホストアドレス 209.165.201.10 を入力します。

New Network Objects ? x

Name:

Description:

Network:
 Format: ipaddr or ipaddr/len or range (ipaddr-ipaddr)

Allow Overrides:

- d) [保存 (Save)]をクリックします。
- e) [ネットワークを追加 (Add Network)]>[オブジェクトの追加 (Add Object)]をクリックして、FTP サーバの変換済みアドレスを定義します。

ネットワーク オブジェクトに名前を付け (ftp_server_translated など)、ホストアドレス 10.1.2.56 を入力します。

New Network Objects ? x

Name:

Description:

Network:
 Format: ipaddr or ipaddr/len or range (ipaddr-ipaddr)

Allow Overrides:

- f) [保存 (Save)]をクリックします。

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

- a) [デバイス (Devices)]>[NAT] を選択し、Firepower Threat Defense NAT ポリシーを作成または編集します。
- b) [ルールの追加 (Add Rule)]をクリックします。
- c) 次のプロパティを設定します。
- [NAT ルール (NAT Rule)] = 自動 NAT ルール (Auto NAT Rule) 。
 - [タイプ (Type)] = スタティック (Static) 。
- d) [インターフェイス オブジェクト (Interface Objects)] タブで、以下の設定を行います。
- [送信元インターフェイス オブジェクト (Source Interface Objects)] = outside。
 - [宛先インターフェイス オブジェクト (Destination Interface Objects)] = inside。
- e) [変換 (Translation)] タブで、次の項目を設定します。
- [元の発信元 (Original Source)] = ftp_server ネットワーク オブジェクト。

- [変換済みの発信元アドレス (Translated Source Address)] = ftp_server_translated ネットワーク オブジェクト。 >

f) [詳細 (Advanced)]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。

The screenshot shows the 'Add NAT Rule' configuration interface. At the top, 'NAT Rule' is set to 'Auto NAT Rule' and 'Type' is 'Static'. The 'Enable' checkbox is checked. Below this are tabs for 'Interface Objects', 'Translation', 'PAT Pool', and 'Advanced'. The 'Translation' tab is active. It is divided into two sections: 'Original Packet' and 'Translated Packet'. In the 'Original Packet' section, 'Original Source:*' is a dropdown menu with 'ftp_server' selected, and 'Original Port' is a dropdown menu with 'TCP' selected. In the 'Translated Packet' section, 'Translated Source' is a text input field containing 'ftp_server_translated'.

g) [OK] をクリックします。

DNS 応答修正 : ホスト ネットワーク上の DNS サーバ