



# Network Address Translation (NAT)

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

- [NAT を使用する理由 \(1 ページ\)](#)
- [NAT の基本 \(2 ページ\)](#)
- [NAT のガイドライン \(8 ページ\)](#)
- [ダイナミック NAT \(15 ページ\)](#)
- [ダイナミック PAT \(24 ページ\)](#)
- [スタティック NAT \(37 ページ\)](#)
- [アイデンティティ NAT \(49 ページ\)](#)
- [NAT のモニタリング \(54 ページ\)](#)
- [NAT の履歴 \(54 ページ\)](#)

## 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 の他の機能には、次のとおりです。

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



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

## NAT の基本

ここでは、NAT の基本について説明します。

## NAT の用語

このマニュアルでは、次の用語を使用しています。

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



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

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

## NAT タイプ

NAT は、次の方法を使用して実装できます。

- **ダイナミック NAT**：実際の IP アドレスのグループが、（通常は、より小さい）マッピング IP アドレスのグループに先着順でマッピングされます。実際のホストだけがトラフィックを開始できます。[ダイナミック NAT \(15 ページ\)](#) を参照してください。
- **ダイナミック ポートアドレス変換 (PAT)**：実際の IP アドレスのグループが、1 つの IP アドレスにマッピングされます。この IP アドレスのポートが使用されます。[ダイナミック PAT \(24 ページ\)](#) を参照してください。
- **スタティック NAT**：実際の IP アドレスとマッピング IP アドレスとの間での一貫したマッピング。双方向にトラフィックを開始できます。[スタティック NAT \(37 ページ\)](#) 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。

## ネットワーク オブジェクト NAT および Twice NAT

ネットワーク オブジェクト NAT および Twice NAT という 2 種類の方法でアドレス変換を実装できます。

Twice NAT の追加機能を必要としない場合は、ネットワーク オブジェクト NAT を使用することをお勧めします。ネットワーク オブジェクト 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)。

### ネットワーク オブジェクト 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、ネットワーク オブジェクト 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。

ネットワーク オブジェクトを設定すると、このオブジェクトのマッピングアドレスをインラインアドレスとして、または別のネットワーク オブジェクトやネットワーク オブジェクトグループのいずれかとして識別できるようになります。

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 アドレスの両方がネットワーク オブジェクト NAT ルールと照合されます。個別の照合が行われる場合、パケット内の送信元 IP アドレスと宛先 IP アドレスは、個別のルールによって変換できます。これらのルールは、相互に結び付けられていません。トラフィックに応じて、異なる組み合わせのルールを使用できます。

ルールがペアになることはないので、sourceA/destinationA で sourceA/destinationB とは別の変換が行われるように指定することはできません。この種の機能には、Twice 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。

## Twice NAT

Twice NAT 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。

## ネットワーク オブジェクト NAT と Twice NAT の比較

これら 2 つの NAT タイプの主な違いは、次のとおりです。

- 実際のアドレスの定義方法
  - ネットワーク オブジェクト NAT : NAT をネットワーク オブジェクトのパラメータとして定義します。ネットワーク オブジェクトは、IP ホスト、範囲、またはサブネットの名前を指定するので、実際の IP アドレスではなく、NAT コンフィギュレーション内のオブジェクトを使用できます。ネットワーク オブジェクトの IP アドレスが実際のアドレスとして機能します。この方法では、ネットワーク オブジェクトがコンフィギュレーションの他の部分ですでに使用されていても、そのネットワーク オブジェクトに NAT を容易に追加できます。

- **Twice NAT** : 実際のアドレスとマッピングアドレスの両方のネットワーク オブジェクトまたはネットワーク オブジェクト グループを識別します。この場合、NAT はネットワーク オブジェクトのパラメータではありません。ネットワーク オブジェクトまたはグループが、NAT コンフィギュレーションのパラメータです。実際のアドレスのネットワーク オブジェクト グループを使用できることは、Twice 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
  - **ネットワーク オブジェクト NAT** : 各ルールは、パケットの送信元または宛先のいずれかに適用できます。つまり、送信元 IP アドレスに1つ、宛先 IP アドレスに1つと、2つのルールが使用されることがあります。これらの2つのルールを相互に結び付けて、送信先と宛先の組み合わせに特定の変換を適用することはできません。
  - **Twice NAT** : 1つのルールで送信元と宛先の両方を変換します。パケットは1つのルールにのみ一致し、それ以上のルールはチェックされません。オプションの宛先アドレスを設定しない場合でも、マッチングするパケットは1つの Twice NAT ルールだけに一致します。送信元および宛先は相互に結び付けられるので、送信元と宛先の組み合わせに応じて、異なる変換を適用できます。たとえば、sourceA/destinationA には、sourceA/destinationB とは異なる変換を設定できます。
- NAT ルールの順序
  - **ネットワーク オブジェクト NAT** : NAT テーブルで自動的に順序付けされます。
  - **Twice NAT** : NAT テーブルで手動で順序付けします (ネットワーク オブジェクト NAT ルールの前または後)。

## NAT ルールの順序

ネットワーク オブジェクト NAT および Twice NAT ルールは、3つのセクションに分かれた単一のテーブルに保存されます。最初にセクション1のルール、次にセクション2、最後にセクション3というように、一致が見つかるまで順番に適用されます。たとえば、セクション1で一致が見つかった場合、セクション2とセクション3は評価されません。次の表に、各セクション内のルールの順序を示します。

表 1: NAT ルール テーブル

テーブルのセクション	ルールタイプ	セクション内のルールの順序
セクション 1	Twice NAT	コンフィギュレーションに登場する順に、最初の一致ベースで適用されます。最初の一致が適用されるため、一般的なルールの前に固有のルールが来るようにする必要があります。そうしない場合、固有のルールを期待どおりに適用できない可能性があります。デフォルトでは、Twice NAT ルールはセクション 1 に追加されます。

テーブルのセクション	ルールタイプ	セクション内のルールの順序
セクション 2	ネットワーク オブジェクト NAT	<p>セクション 1 で一致が見つからない場合、セクション 2 のルールが次の順序で適用されます。</p> <ol style="list-style-type: none"> <li>1. スタティック ルール</li> <li>2. ダイナミック ルール</li> </ol> <p>各ルールタイプでは、次の順序ガイドラインが使用されます。</p> <ol style="list-style-type: none"> <li>1. 実際の IP アドレスの数量：小から大の順。たとえば、アドレスが 1 個のオブジェクトは、アドレスが 10 個のオブジェクトよりも先に評価されます。</li> <li>2. 数量が同じ場合には、アドレス番号（低から高の順）が使用されます。たとえば、10.1.1.0 は、11.1.1.0 よりも先に評価されます。</li> <li>3. 同じ IP アドレスが使用される場合、ネットワーク オブジェクトの名前がアルファベット順で使用されます。たとえば、abracadabra は catwoman よりも先に評価されます。</li> </ol>
セクション 3	Twice NAT	<p>まだ一致が見つからない場合、セクション 3 のルールがコンフィギュレーションに登場する順に、最初の一致ベースで適用されます。このセクションには、最も一般的なルールを含める必要があります。このセクションにおいても、一般的なルールの前に固有のルールが来るようにする必要があります。そうしない場合、一般的なルールが適用されます。</p>

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

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

この結果、使用される順序は次のとおりです。

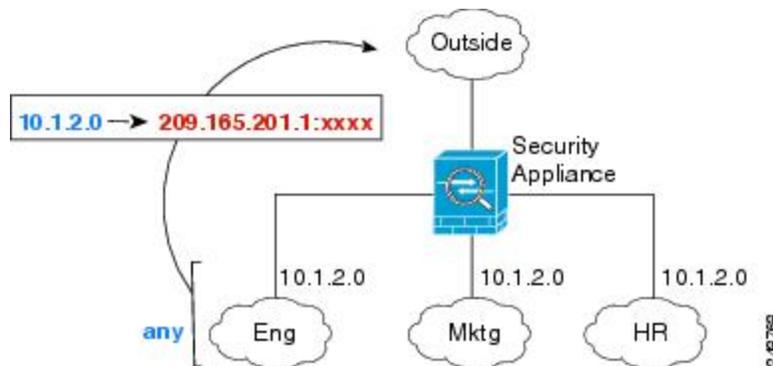
- 192.168.1.1/32 (ダイナミック)
- 10.1.1.0/24 (スタティック)
- 192.168.1.0/24 (スタティック)
- 172.16.1.0/24 (ダイナミック) (オブジェクト abc)
- 172.16.1.0/24 (ダイナミック) (オブジェクト def)
- 192.168.1.0/24 (ダイナミック)

## NAT インターフェイス

ブリッジグループメンバーのインターフェイスを除き、任意のインターフェイス（つまり、すべてのインターフェイス）に適用できるように NAT ルールを設定することも、特定の実際のインターフェイスおよびマッピングインターフェイスを識別することもできます。実際のアドレスには任意のインターフェイスを指定できます。マッピング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 1: 任意のインターフェイスの指定



ただし、「任意の」インターフェイスの概念は、ブリッジグループメンバーのインターフェイスには適用されません。「任意の」インターフェイスを指定すると、すべてのブリッジグループメンバーのインターフェイスは除外されます。したがって、ブリッジグループメンバーに NAT を適用するには、メンバーのインターフェイスを指定する必要があります。これでは、1つのインターフェイスのみが異なる多くの類似するルールが発生する可能性があります。ブリッジ仮想インターフェイス (BVI) 自体に NAT を設定することはできませんが、メンバーのインターフェイスのみに NAT を設定することはできます。

# 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の 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。ブリッジグループインターフェイス（BVI）の NAT 自体を設定することはできません。
- ブリッジグループメンバー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 と IPv6 ネットワーク間の変換はできません（NAT64/46）。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 だけが許可される方法であり、ダイナミック PAT66 はサポートされません。ただし、さまざまなブリッジグループのメンバー間、またはブリッジグループメンバー（送信元）と標準ルーテッドインターフェイス（宛先）間では NAT64/46 を実行できます。

## IPv6 NAT のガイドライン

NAT では、IPv6 のサポートに次のガイドラインと制約が伴います。

- ルーテッドモードインターフェイスの場合は、IPv4 と IPv6 との間の変換もできます。
- 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 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のインターフェイス間で変換するときは、IPv6 のダイナミック PAT（NAT66）を使用できません。この制限は、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 (Twice 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 (Twice 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。

## 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では、メンバーのインターフェイスに 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 NAT ルールを記述することはできません。
- (ネットワーク オブジェクト 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複数のオブジェクトを作成する必要があります。

たとえば、オブジェクト ネットワーク **obj-10.10.10.1-01**、オブジェクト ネットワーク **obj-10.10.10.1-02** などです。

- VPN がインターフェイスで定義されると、インターフェイスの着信 ESP トラフィックに NAT ルールは適用されません。システムでは確立された VPN トンネルの ESP トラフィックのみ許可され、既存のトンネルに関連付けられていないトラフィックは廃棄されます。この制約は ESP と UDP ポート 500 および 4500 に適用されます。
- ダイナミック PAT を適用するデバイスの背後のデバイス（VPN UDP ポート 500 と 4500 は実際に使用されるポートではない）でサイト間 VPN を定義した場合、PAT デバイスの背後にあるデバイスから接続を開始する必要があります。正しいポート番号がわからないため、レスポンドはセキュリティアソシエーション（SA）を開始できません。
- NAT コンフィギュレーションを変更したときに、既存の変換がタイムアウトするまで待たずに新しい NAT コンフィギュレーションが使用されるようにするには、デバイス CLI で **clear xlate** コマンドを使用して変換テーブルを消去できます。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できます。

- SCTP トラフィックを変換する際は、スタティック ネットワーク オブジェクト NAT のみを使用します。ダイナミック NAT/PAT は許可されません。スタティック Twice NAT を設定できますが、SCTP アソシエーションの宛先部分のトポロジが不明であるため、これは推奨されません。
- NAT で使用されるオブジェクトおよびオブジェクト グループを未定義にすることはできません。IP アドレスを含める必要があります。
- 1 つのオブジェクト グループに IPv4 と IPv6 の両方のアドレスを入れることはできません。オブジェクトグループには、1 つのタイプのアドレスだけが含まれている必要があります。
- (Twice NAT のみ)。発信元アドレスとして **any** を NAT ルールで使用する場合、「**any**」トラフィックの定義 (IPv4 と IPv6) はルールによって異なります。ASA 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、ASA は、NAT ルールの **any** の値を決定できます。たとえば、「**any**」から IPv6 サーバへのルールを設定しており、このサーバが IPv4 アドレスからマッピングされている場合、**any** は「任意の IPv6 トラフィック」を意味します。「**any**」から「**any**」へのルールを設定しており、送信元をインターフェイス IPv4 アドレスにマッピン

グする場合、マッピング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 プールは、次のアドレスを含むことができません。
  - 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 がイネーブルの場合は、スタンバイ インターフェイスの IP アドレス。
  - 既存の VPN プールのアドレス。
- スタティックおよびダイナミック NAT ポリシーでは重複アドレスを使用しないでください。たとえば、重複アドレスを使用すると、PPTP のセカンダリ接続がダイナミック xlate ではなくスタティックにヒットした場合、PPTP 接続の確立に失敗する可能性があります。
- NAT や PAT に伴うアプリケーション インспекションの制限については、[デフォルト インспекションと NAT に関する制限事項](#)を参照してください。
- アイデンティティ NAT のデフォルト動作で、プロキシ ARP はイネーブルにされ、他のスタティック NAT ルールと一致します。必要に応じてプロキシ ARP をディセーブルにできます。詳細については、「[NAT パケットのルーティング](#)」を参照してください。
- **arp permit-nonconnected** コマンドを有効にすると、マッピングされたアドレスが接続されているサブネットの一部ではなく、しかも、マッピングされているインターフェイスを NAT ルールに指定しなかった (つまり、「any」インターフェイスを指定した) 場合に、システムは ARP 要求に応答しません。この問題を解決するには、マッピングされたインターフェイスを指定します。
- ルールで宛先インターフェイスを指定すると、ルーティングテーブルでルートが検索されるのではなく、そのインターフェイスが出力インターフェイスとして使用されます。ただし、アイデンティティ NAT の場合は、代わりにルート ルックアップを使用するオプションがあります。
- NAT のトランザクション コミット モデルを使用すると、システムのパフォーマンスと信頼性を向上させることができます。詳細については、一般的な操作設定ガイドの基本設定の章を参照してください。 **asp rule-engine transactional-commit nat** コマンドを使用します。

## マッピングアドレスオブジェクトのネットワーク オブジェクト NAT のガイドライン

ダイナミック NAT の場合は、マッピングされたアドレスに対してオブジェクトまたはグループを使用する必要があります。他のタイプの NAT の場合は、オブジェクトまたはグループを作成することも、インラインアドレスを使用することもできます。ネットワーク オブジェクト グループは、非連続的な IP アドレスの範囲または複数のホストやサブネットで作成されるマッピングアドレスを作成する場合に特に便利です。**object network** コマンドと **object-group network** コマンドを使用してオブジェクトを作成します。

マッピングアドレスのオブジェクトを作成する場合は、次のガイドラインを考慮してください。

- 1つのネットワーク オブジェクト グループには、IPv4 アドレスと IPv6 アドレスのいずれか一方のオブジェクトやインラインアドレスを入れることができます。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。
- 拒否されるマッピング IP アドレスについては、[NAT のその他のガイドライン \(9 ページ\)](#) を参照してください。
- ダイナミック NAT :
  - インラインアドレスは使用できません。ネットワーク オブジェクトまたはグループを設定する必要があります。
  - オブジェクトまたはグループには、サブネットを含めることはできません。オブジェクトは、範囲を定義する必要があります。グループには、ホストと範囲を含めることができます。
  - マッピングされたネットワーク オブジェクトに範囲とホスト 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 (隠蔽) :
  - オブジェクトを使用する代わりに、任意でインラインホストアドレスを設定するか、またはインターフェイスアドレスを指定できます。
  - オブジェクトを使用する場合は、オブジェクトまたはグループにサブネットを含めることはできません。オブジェクトは、1つのホスト、または範囲 (PAT プールの場合) を定義する必要があります。グループ (PAT プールの場合) には、複数のホストと範囲を含めることができます。
- スタティック NAT またはポート変換を使用するスタティック NAT :
  - オブジェクトを使用する代わりに、インラインアドレスを設定するか、またはインターフェイスアドレスを指定できます (ポート変換を使用するスタティック NAT の場合)。

- オブジェクトを使用する場合は、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入れることができます。
- アイデンティティ NAT
  - オブジェクトを使用する代わりに、インライン アドレスを設定できます。
  - オブジェクトを使用する場合は、オブジェクトは、変換する実際のアドレスと一致する必要があります。

## 実際のアドレス オブジェクトおよびマッピング アドレス オブジェクトの Twice NAT のガイドライン

NAT ルールごとに、次にに関するネットワーク オブジェクトまたはグループを 4 つまで設定します。

- 送信元の実際のアドレス
- 送信元のマッピング アドレス
- 宛先の実際のアドレス
- 宛先のマッピング アドレス

すべてのトラフィックを表す **any** キーワードインライン、または一部のタイプの NAT の場合はインターフェイスアドレスを表す **interface** キーワードを指定しない場合は、オブジェクトが必要です。ネットワーク オブジェクト グループは、非連続的な IP アドレスの範囲または複数のホストやサブネットで構成されるマッピングアドレスを作成する場合に特に便利です。**object network** コマンドと **object-group network** コマンドを使用してオブジェクトを作成します。

Twice NAT のオブジェクトを作成する場合は、次のガイドラインを考慮してください。

- 1 つのネットワーク オブジェクト グループには、IPv4 アドレスと IPv6 アドレスのいずれか一方のオブジェクトやインラインアドレスを入れることができます。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。
- 拒否されるマッピング IP アドレスについては、[NAT のその他のガイドライン \(9 ページ\)](#) を参照してください。
- 送信元ダイナミック NAT :
  - 通常は、実際のアドレスの大きいグループが小さいグループにマッピングされるように設定します。
  - マッピングされたオブジェクトまたはグループには、サブネットを含めることはできません。オブジェクトは、範囲を定義する必要があります。グループには、ホストと範囲を含めることができます。

- マッピングされたネットワーク オブジェクトに範囲とホスト 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。
- 送信元ダイナミック PAT (隠蔽) :
  - オブジェクトを使用する場合は、オブジェクトまたはグループにサブネットを含めることはできません。オブジェクトは、1つのホスト、または範囲 (PAT プールの場合) を定義する必要があります。グループ (PAT プールの場合) には、複数のホストと範囲を含めることができます。
- 送信元スタティック NAT またはポート変換を設定したスタティック NAT :
  - マッピングされたオブジェクトまたはグループには、ホスト、範囲、またはサブネットを含めることができます。
  - スタティック マッピングは、通常1対1です。したがって、実際のアドレスとマッピングアドレスの数は同じです。ただし、必要に応じて異なる数にすることができます。
- 送信元アイデンティティ NAT
  - 実際のオブジェクトとマッピングされたオブジェクトが一致する必要があります。両方に同じオブジェクトを使用することも、同じ IP アドレスが含まれる個別のオブジェクトを作成することもできます。
- 宛先スタティック NAT またはポート変換を設定したスタティック NAT (宛先の変換は常にスタティックです) :
  - Twice NAT の主な機能は、宛先 IP アドレスを含めることですが、宛先アドレスはオプションです。宛先アドレスを指定した場合、このアドレスにスタティック変換を設定できるか、単にアイデンティティ NAT を使用できます。宛先アドレスを使用せずに Twice NAT を設定して、実際のアドレスに対するネットワーク オブジェクト グループの使用または手動でのルールの順序付けを含む、Twice NAT の他の特質の一部を活用することができます。詳細については、[ネットワーク オブジェクト NAT と Twice NAT の比較 \(4 ページ\)](#) を参照してください。
  - アイデンティティ NAT では、実際のオブジェクトとマッピングされたオブジェクトが一致する必要があります。両方に同じオブジェクトを使用することも、同じ IP アドレスが含まれる個別のオブジェクトを作成することもできます。
  - スタティック マッピングは、通常1対1です。したがって、実際のアドレスとマッピングアドレスの数は同じです。ただし、必要に応じて異なる数にすることができます。
  - ポート変換 (ルーテッドモードのみ) が設定されたスタティック インターフェイス NAT では、マッピングアドレスのネットワーク オブジェクト/グループではなく、interface キーワードを指定できます。

## 実際のポートおよびマッピングポートのサービスオブジェクトの Twice NAT のガイドライン

必要に応じて、次のサービスオブジェクトを設定できます。

- 送信元の実際のポート（スタティックのみ）または宛先の実際のポート
- 送信元のマッピングポート（スタティックのみ）または宛先のマッピングポート

object service コマンドを使用してオブジェクトを作成します。

Twice NAT のオブジェクトを作成する場合は、次のガイドラインを考慮してください。

- NAT は、TCP、UDP、および SCTP のみをサポートします。ポートを変換する場合、実際のサービスオブジェクトのプロトコルとマッピングサービスオブジェクトのプロトコルの両方を同じにします（たとえば両方とも TCP にします）。SCTP ポート仕様を含むスタティック Twice NAT ルールを設定できますが、SCTP アソシエーションの宛先部分のトポロジが不明であるため、これは推奨されません。SCTP に対して代わりにスタティックオブジェクト NAT を使用します。
- 「not equal（等しくない）」（**neq**）演算子はサポートされていません。
- アイデンティティポート変換では、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。
- 送信元ダイナミック NAT：送信元ダイナミック NAT では、ポート変換はサポートされません。
- 送信元ダイナミック PAT（隠蔽）：送信元ダイナミック PAT では、ポート変換はサポートされません。
- 送信元スタティック NAT、ポート変換を設定したスタティック NAT、またはアイデンティティ NAT：サービスオブジェクトには、送信元ポートと宛先ポートの両方を含めることができます。ただし、両方のサービスオブジェクトに、送信元ポートまたは宛先ポートのいずれかを指定する必要があります。ご使用のアプリケーションが固定の送信元ポートを使用する場合（一部の DNS サーバなど）に送信元ポートおよび宛先ポートの両方を指定する必要がありますが、固定の送信元ポートはめったに使用されません。たとえば、送信元ホストのポートを変換する場合は、送信元サービスを設定します。
- 宛先スタティック NAT またはポート変換を設定したスタティック NAT（宛先の変換は常にスタティックです）：非スタティックな送信元 NAT では、宛先でのみポート変換を実行できます。サービスオブジェクトには送信元ポートと宛先ポートの両方を含めることができますが、この場合は、宛先ポートだけが使用されます。送信元ポートを指定した場合、無視されます。

## ダイナミック NAT

ここでは、ダイナミック NAT とその設定方法について説明します。

## ダイナミック NAT について

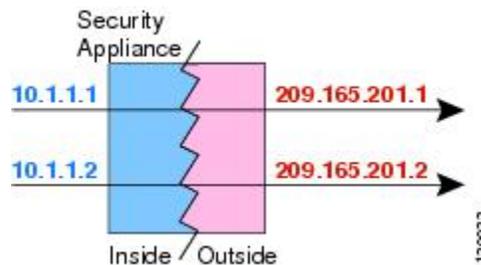
ダイナミック NAT では、実際のアドレスのグループは、宛先ネットワーク上でルーティング可能なマッピングアドレスのプールに変換されます。マッピングされたプールにあるアドレスは、通常、実際のグループより少なくなります。変換対象のホストが宛先ネットワークにアクセスすると、NAT は、マッピングされたプールから IP アドレスをそのホストに割り当てます。変換は、実際のホストが接続を開始したときにだけ作成されます。変換は接続が継続している間だけ有効であり、変換がタイムアウトすると、そのユーザは同じ IP アドレスを保持しません。したがって、アクセスルールでその接続が許可されている場合でも、宛先ネットワ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



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

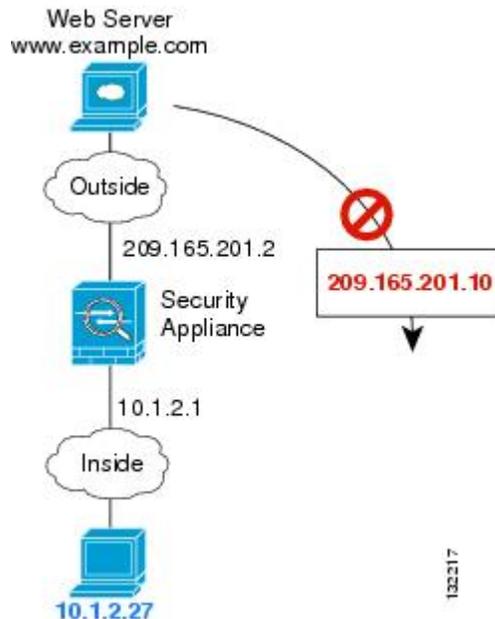
次の図に、一般的なダイナミック NAT のシナリオを示します。実際のホストだけが NAT セッションを作成でき、応答トラフィックが許可されます。

図 2: 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 3: 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。

NAT および PAT のサポートの詳細については、[デフォルト インспекションと NAT に関する制限事項](#)を参照してください。

## ダイナミック ネットワーク オブジェクト NAT の設定

この項では、ダイナミック NAT のネットワーク オブジェクト NAT を設定する方法について説明します。

### 手順

**ステップ 1** マッピングアドレスにホストまたは範囲のネットワーク オブジェクト (**object network** コマンド)、またはネットワーク オブジェクトグループ (**object-group network** コマンド) を作成します。

- オブジェクトまたはグループには、サブネットを含めることはできません。オブジェクトは、範囲を定義する必要があります。グループには、ホストと範囲を含めることができます。
- マッピングされたネットワーク オブジェクトに範囲とホスト 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。

**ステップ 2** NAT を設定するネットワーク オブジェクトを作成または編集します。 **object network obj\_name**  
例 :

```
hostname(config)# object network my-host-obj1
```

**ステップ 3** (正しいアドレスがあるオブジェクトを編集する場合はスキップする) 変換する実際の IPv4 または IPv6 アドレスを定義します。

- **host {IPv4\_address|IPv6\_address}** : 単一のホストの IPv4 または IPv6 アドレス。たとえば、10.1.1.1 または 2001:DB8::0DB8:800:200C:417A。
- **subnet {IPv4\_address IPv4\_mask|IPv6\_address/IPv6\_prefix}** : ネットワークのアドレス。IPv4 サブネットの場合、10.0.0.255.0.0.0 のように、スペースの後ろにマスクを含めます。IPv6 の場合、2001:DB8:0:CD30::/60 のように、アドレスとプレフィックスを単一のユニット (スペースなし) として含めます。
- **range start\_address end\_address** : アドレスの範囲。IPv4 または IPv6 の範囲を指定できます。マスクまたはプレフィックスを含めないでください。

例 :

```
hostname(config-network-object)# host 10.2.2.2
```

**ステップ 4** オブジェクト IP アドレスの **ダイナミック NAT** を設定します。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。

```
nat [(real_ifc,mapped_ifc)] dynamic mapped_obj [interface [ipv6]] [dns]
```

それぞれの説明は次のとおりです。

- インターフェイス：（ブリッジグループメンバーのインターフェイスに必要）実際のインターフェイス (*real\_ifc*) およびマッピングインターフェイス (*mapped\_ifc*) を指定します。丸カッコを含める必要があります。ルーテッドモードでは、実際のインターフェイスおよびマッピングインターフェイスを指定しない場合は、すべてのインターフェイスが使用されます。また、(any,outside) のようにインターフェイスのいずれかまたは両方にキーワード **any** を指定することもできます。ただし、**any** はブリッジグループのメンバインターフェイスには適用されません。
- マッピング IP アドレス：マッピング IP アドレスが含まれるネットワーク オブジェクトまたはネットワーク オブジェクト グループを指定します。
- インターフェイス PAT のフォールバック：（任意）**interface** キーワードは、インターフェイス PAT のフォールバックをイネーブルにします。マッピング IP アドレスを使い果たすと、マッピングインターフェイスの IP アドレスが使用されます。**ipv6** を指定すると、インターフェイスの IPv6 アドレスが使用されます。このオプションでは、*mapped\_ifc* に特定のインターフェイスを設定する必要があります。（マッピングされたインターフェイスがブリッジグループメンバーのときは、**interface** を指定できません）
- DNS：（任意）**dns** キーワードは、DNS 応答を変換します。DNS インспекションがイネーブルになっていることを確認してください（デフォルトではイネーブルです）。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](#)」を参照してください。

例：

```
hostname(config-network-object)# nat (inside,outside) dynamic MAPPED_IPS interface
```

例

次の例では、外部アドレス 10.2.2.1 ~ 10.2.2.10 の範囲の背後に 192.168.2.0 ネットワークを隠すダイナミック NAT を設定します。

```
hostname(config)# object network my-range-obj
hostname(config-network-object)# range 10.2.2.1 10.2.2.10
hostname(config)# object network my-inside-net
hostname(config-network-object)# subnet 192.168.2.0 255.255.255.0
hostname(config-network-object)# nat (inside,outside) dynamic my-range-obj
```

次の例では、ダイナミック PAT バックアップを設定したダイナミック NAT を設定します。ネットワーク 10.76.11.0 内のホストは、まず **nat-range1** プール（10.10.10.10 ~ 10.10.10.20）にマッピングされます。**nat-range1** プール内のすべてのアドレスが割り当てられたら、**pat-ip1** アドレス（10.10.10.21）を使用してダイナミック PAT が実行されます。万一、PAT 変換もすべて使用されてしまった場合は、外部インターフェイスアドレスを使用してダイナミック PAT が実行されます。

```

hostname(config)# object network nat-rangel
hostname(config-network-object)# range 10.10.10.10 10.10.10.20

hostname(config-network-object)# object network pat-ip1
hostname(config-network-object)# host 10.10.10.21

hostname(config-network-object)# object-group network nat-pat-grp
hostname(config-network-object)# network-object object nat-rangel
hostname(config-network-object)# network-object object pat-ip1

hostname(config-network-object)# object network my_net_obj5
hostname(config-network-object)# subnet 10.76.11.0 255.255.255.0
hostname(config-network-object)# nat (inside,outside) dynamic nat-pat-grp interface

```

次の例では、ダイナミック NAT とダイナミック PAT バックアップを使用して IPv6 ホストを IPv4 に変換するように設定します。内部ネットワーク 2001:DB8::/96 上のホストは最初に、IPv4\_NAT\_RANGE プール (209.165.201.30 ~ 209.165.201.1) にマッピングされます。IPv4\_NAT\_RANGE プール内のすべてのアドレスが割り当てられた後は、IPv4\_PAT アドレス (209.165.201.31) を使用してダイナミック PAT が実行されます。PAT 変換もすべて使用されてしまった場合は、外部インターフェイスアドレスを使用してダイナミック PAT が実行されます。

```

hostname(config)# object network IPv4_NAT_RANGE
hostname(config-network-object)# range 209.165.201.1 209.165.201.30

hostname(config-network-object)# object network IPv4_PAT
hostname(config-network-object)# host 209.165.201.31

hostname(config-network-object)# object-group network IPv4_GROUP
hostname(config-network-object)# network-object object IPv4_NAT_RANGE
hostname(config-network-object)# network-object object IPv4_PAT

hostname(config-network-object)# object network my_net_obj5
hostname(config-network-object)# subnet 2001:DB8::/96
hostname(config-network-object)# nat (inside,outside) dynamic IPv4_GROUP interface

```

## ダイナミック Twice NAT の設定

この項では、ダイナミック NAT の Twice NAT を設定する方法について説明します。

### 手順

**ステップ 1** 送信元の実際のアドレス、送信元のマッピングアドレス、宛先の実際のアドレス、および宛先のマッピングアドレスに、ホストまたは範囲のネットワークオブジェクト (**object network** コマンド)、またはネットワークオブジェクトグループ (**object-group network** コマンド) を作成します。

- すべての送信元トラフィックを変換する場合、送信元の実際のアドレスに対するオブジェクトの追加をスキップして、代わりに、**nat** コマンドに **any** キーワードを指定できます。

- ポート変換を設定した宛先のスタティック インターフェイス NAT のみを設定する場合は、宛先のマッピングアドレスに対するオブジェクトの追加をスキップして、代わりに、**nat** コマンドに **interface** キーワードを指定できます。

オブジェクトを作成する場合は、次のガイドラインを考慮してください。

- 通常は、実際のアドレスの大きいグループが小さいグループにマッピングされるように設定します。
- オブジェクトまたはグループには、サブネットを含めることはできません。オブジェクトは、範囲を定義する必要があります。グループには、ホストと範囲を含めることができます。
- マッピングされたネットワーク オブジェクトに範囲とホスト 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 のフォーラバックとして使用されます。

**ステップ 2** (任意) 宛先の実際のポートおよび宛先のマッピング ポートにサービス オブジェクトを作成します。

ダイナミック NAT の場合、宛先でポート変換のみを実行できます。サービス オブジェクトには送信元ポートと宛先ポートの両方を含めることができますが、この場合は、宛先ポートだけが使用されます。送信元ポートを指定した場合、無視されます。

**ステップ 3** ダイナミック NAT を設定します。

```
nat [(real_ifc,mapped_ifc)] [line | {after-auto [line]}] source dynamic {real_obj | any} {mapped_obj
[interface [ipv6]]} [destination static {mapped_obj | interface [ipv6]} real_obj] [service
mapped_dest_svc_obj real_dest_svc_obj] [dns] [unidirectional] [inactive] [description desc]
```

それぞれの説明は次のとおりです。

- インターフェイス：(ブリッジグループ メンバーのインターフェイスに必要) 実際のインターフェイス (*real\_ifc*) およびマッピングインターフェイス (*mapped\_ifc*) を指定します。丸カッコを含める必要があります。ルーテッドモードでは、実際のインターフェイスおよびマッピングインターフェイスを指定しない場合は、すべてのインターフェイスが使用されます。また、(*any,outside*) のようにインターフェイスのいずれかまたは両方にキーワード **any** を指定することもできます。ただし、**any** はブリッジグループのメンバインターフェイスには適用されません。
- セクションおよび行：(任意) デフォルトでは、NAT 規則は、NAT テーブルのセクション 1 の末尾に追加されます (NAT ルールの順序 (5 ページ) を参照)。セクション 1 ではなく、セクション 3 (ネットワーク オブジェクト NAT ルールの後ろ) にルールを追加する場合、**after-auto** キーワードを使用します。ルールは、*line* 引数を使用して、適切なセクションの任意の場所に挿入できます。
- 送信元アドレス：
  - 実際のアドレス：ネットワーク オブジェクト、グループ、または **any** キーワードを指定します。

- マッピングアドレス：異なるネットワーク オブジェクトまたはグループを指定します。必要に応じて、次のフォールバック方式を設定できます。
  - インターフェイス PAT のフォールバック：（任意） **interface** キーワードは、インターフェイス PAT のフォールバックをイネーブルにします。マッピング IP アドレスを使い果たすと、マッピング インターフェイスの IP アドレスが使用されます。 **ipv6** を指定すると、インターフェイスの IPv6 アドレスが使用されます。このオプションでは、 *mapped\_ifc* に特定のインターフェイスを設定する必要があります。（マッピングされたインターフェイスがブリッジグループ メンバーになっているときは、 **interface** を指定できません）
- 宛先アドレス（任意）：
  - マッピングアドレス：ネットワーク オブジェクトまたはグループを指定します。ポート変換が設定されたスタティック インターフェイス NAT に限り、 **interface** キーワードを指定します。 **ipv6** を指定すると、インターフェイスの IPv6 アドレスが使用されます。 **interface** を指定する場合は、必ず **service** キーワードも設定します。このオプションでは、 *real\_ifc* に特定のインターフェイスを設定する必要があります。詳細については、「[ポート変換を設定したスタティック NAT（38 ページ）](#)」を参照してください。
  - 実際のアドレス：ネットワーク オブジェクトまたはグループを指定します。アイデンティティ NAT では、実際のアドレスとマッピング アドレスの両方に単に同じオブジェクトまたはグループを使用します。
- 宛先ポート：（任意） マッピングされたサービス オブジェクトおよび実際のサービス オブジェクトとともに、 **service** キーワードを指定します。アイデンティティ ポート変換では、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します。
- DNS：（任意、送信元のみ適用されるルール） **dns** キーワードは、DNS 応答を変換します。DNS インспекションがイネーブルになっていることを確認してください（デフォルトではイネーブルです）。宛先アドレスを設定する場合、 **dns** キーワードは設定できません。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](#)」を参照してください。
- 単方向：（任意）宛先アドレスが送信元アドレスへのトラフィックを開始できないようにするには、 **unidirectional** を指定します。
- 非アクティブ：（任意）コマンドを削除する必要なくこの規則を非アクティブにするには、 **inactive** キーワードを使用します。再度アクティブ化するには、 **inactive** キーワードを除いてコマンド全体を再入力します。
- 説明：（任意） **description** キーワードを使用して、最大 200 文字の説明を入力します。

例：

```
hostname(config)# nat (inside,outside) source dynamic MyInsNet NAT_POOL
```

```
destination static Server1_mapped Server1 service MAPPED_SVC REAL_SVC
```

---

## 例

次に、209.165.201.1/27 ネットワークのサーバおよび203.0.113.0/24 ネットワークのサーバにアクセスする場合の内部ネットワーク 10.1.1.0/24 のダイナミック NAT を設定する例を示します。

```
hostname(config)# object network INSIDE_NW
hostname(config-network-object)# subnet 10.1.1.0 255.255.255.0

hostname(config)# object network MAPPED_1
hostname(config-network-object)# range 209.165.200.225 209.165.200.254

hostname(config)# object network MAPPED_2
hostname(config-network-object)# range 209.165.202.129 209.165.200.158

hostname(config)# object network SERVERS_1
hostname(config-network-object)# subnet 209.165.201.0 255.255.255.224

hostname(config)# object network SERVERS_2
hostname(config-network-object)# subnet 203.0.113.0 255.255.255.0

hostname(config)# nat (inside,outside) source dynamic INSIDE_NW MAPPED_1
destination static SERVERS_1 SERVERS_1
hostname(config)# nat (inside,outside) source dynamic INSIDE_NW MAPPED_2
destination static SERVERS_2 SERVERS_2
```

次に、IPv4 209.165.201.1/27 ネットワークのサーバおよび203.0.113.0/24 ネットワークのサーバにアクセスする場合の IPv6 内部ネットワーク 2001:DB8:AAAA::/96 のダイナミック NAT を設定する例を示します。

```
hostname(config)# object network INSIDE_NW
hostname(config-network-object)# subnet 2001:DB8:AAAA::/96

hostname(config)# object network MAPPED_1
hostname(config-network-object)# range 209.165.200.225 209.165.200.254

hostname(config)# object network MAPPED_2
hostname(config-network-object)# range 209.165.202.129 209.165.200.158

hostname(config)# object network SERVERS_1
hostname(config-network-object)# subnet 209.165.201.0 255.255.255.224

hostname(config)# object network SERVERS_2
hostname(config-network-object)# subnet 203.0.113.0 255.255.255.0

hostname(config)# nat (inside,outside) source dynamic INSIDE_NW MAPPED_1
destination static SERVERS_1 SERVERS_1
hostname(config)# nat (inside,outside) source dynamic INSIDE_NW MAPPED_2
destination static SERVERS_2 SERVERS_2
```

# 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。

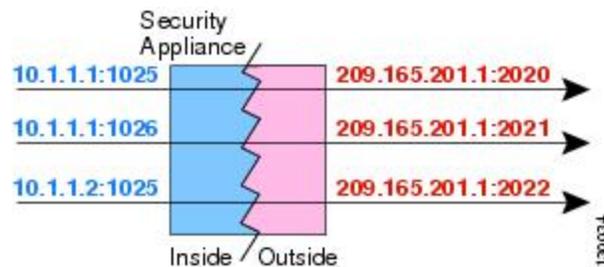
## ダイナミック PAT について

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 4: 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。Multi-Session PAT では、デフォルトで 30 秒の PAT タイムアウトが使用されます。Per-Session PAT の場合、xlate が即座に削除されます。



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

## ダイナミック PAT の欠点と利点

ダイナミック PAT では、1つのマッピングアドレスを使用できるため、ルーティング可能なアドレスが節約されます。さらに、ASA 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のインターフェイス間で変換するときは、IPv6 のダイナミック PAT (NAT66) を使用できません。この制限は、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。NAT および PAT のサポートの詳細については、[デフォルト インスペクションと NAT に関する制限事項](#)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 プールを設定して、PAT アドレスのラウンドロビン割り当てを使用すると、この状況を緩和できます。

## PAT プール オブジェクトの注意事項

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。
- PAT プールに対してブロック割り当てを有効にする場合、ポートブロックは1024 ~ 65535 の範囲でのみ割り当てられます。そのため、アプリケーションが小さいポート番号 (1 ~ 1023) を必要とするときは、機能しない可能性があります。たとえば、ポート 22 (SSH) を要求するアプリケーションは、1024 ~ 65535 の範囲内のホストに割り当てられたブロック内でマッピングされたポートを取得します。
- 同じ PAT プール オブジェクトを2つの異なるルールの中で使用する場合は、必ず同じオプションを各ルールに指定してください。たとえば、1つのルールで拡張 PAT 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спекションでは、拡張 PAT はサポートされていません。サポート対象外のインспекションの完全なリストについては、[デフォルト インспекション](#)と [NAT に関する制限事項](#)を参照してください。
- 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、ホストからの後続の接続では最初の IP アドレスが使用されない場合があります。
- PAT プールルール/ラウンドロビンルールとインターフェイス PAT ルールが同じインターフェイス上で混在していると、IP アドレスの「スティッキ性」も影響を受けます。指定したインターフェイスで PAT プールまたはインターフェイス PAT のいずれかを選択します。競合する PAT ルールは作成しないでください。
- ラウンドロビンでは、特に拡張 PAT と組み合わせた場合に、大量のメモリが消費されます。NAT プールはマッピングされるプロトコル/IP アドレス/ポート範囲ごとに作成されるため、ラウンドロビンでは数多くの同時 NAT プールが作成され、メモリが使用されます。拡張 PAT では、さらに多くの同時 NAT プールが作成されます。

## ダイナミック ネットワーク オブジェクト PAT の設定

この項では、ダイナミック PAT のネットワーク オブジェクト NAT を設定する方法について説明します。

### 手順

- ステップ 1** (任意) マッピングアドレスにホストまたは範囲のネットワーク オブジェクト (**object network** コマンド)、またはネットワーク オブジェクト グループ (**object-group network** コマンド) を作成します。

- オブジェクトを使用する代わりに、任意でインライン ホスト アドレスを設定するか、またはインターフェイス アドレスを指定できます。
- オブジェクトを使用する場合は、オブジェクトまたはグループにサブネットを入れることはできません。オブジェクトは、1つのホスト、または範囲 (PAT プールの場合) を定義する必要があります。グループ (PAT プールの場合) には、複数のホストと範囲を入れることができます。

**ステップ 2** NAT を設定するネットワーク オブジェクトを作成または編集します。 **object network *obj\_name***  
例 :

```
hostname(config)# object network my-host-obj1
```

**ステップ 3** (正しいアドレスがあるオブジェクトを編集する場合はスキップする) 変換する実際の IPv4 または IPv6 アドレスを定義します。

- **host**{*IPv4\_address* | *IPv6\_address*} : 単一のホストの IPv4 または IPv6 アドレス。たとえば、10.1.1.1 または 2001:DB8::0DB8:800:200C:417A。
- **subnet** {*IPv4\_address IPv4\_mask* | *IPv6\_address/IPv6\_prefix*} : ネットワークのアドレス。IPv4 サブネットの場合、10.0.0.0 255.0.0.0 のように、スペースの後ろにマスクを含めます。IPv6 の場合、2001:DB8:0:CD30::/60 のように、アドレスとプレフィックスを単一のユニット (スペースなし) として含めます。
- **range start\_address end\_address** : アドレスの範囲。IPv4 または IPv6 の範囲を指定できます。マスクまたはプレフィックスを含めないでください。

例 :

```
hostname(config-network-object)# range 10.1.1.1 10.1.1.90
```

**ステップ 4** オブジェクト IP アドレスの **ダイナミック PAT** を設定します。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。

```
nat [(real_ifc,mapped_ifc)] dynamic {mapped_inline_host_ip | mapped_obj | pat-pool mapped-obj [round-robin] [extended] [flat [include-reserve]] [block-allocation] | interface [ipv6]} [interface [ipv6]]
```

それぞれの説明は次のとおりです。

- **インターフェイス** : (ブリッジグループメンバーのインターフェイスに必要) 実際のインターフェイス (*real\_ifc*) およびマッピングインターフェイス (*mapped\_ifc*) を指定します。丸カッコを含める必要があります。ルーテッドモードでは、実際のインターフェイスおよびマッピングインターフェイスを指定しない場合は、すべてのインターフェイスが使用されます。また、(any,outside) のようにインターフェイスのいずれかまたは両方にキーワード **any** を指定することもできます。ただし、**any** はブリッジグループのメンバーインターフェイスには適用されません。
- **マッピング IP アドレス** : マッピング IP アドレスを次のものとして指定できます。

- *mapped\_inline\_host\_ip* : インライン ホスト アドレス。
  - *mapped\_obj* : ホスト アドレスとして定義されるネットワーク オブジェクト。
  - *pat-pool mapped-obj* : 複数の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。
  - **interface [ipv6]** : マッピングされたインターフェイスの IP アドレスがマッピングアドレスとして使用されます。 **ipv6** を指定した場合、インターフェイスの IPv6 アドレスが使用されます。このオプションでは、 *mapped\_ifc* に特定のインターフェイスを設定する必要があります。(マッピングされたインターフェイスがブリッジグループメンバーのときは、 **interface** を指定できません) このキーワードは、インターフェイスの IP アドレスを使用するときに使用する必要があります。インラインで、またはオブジェクトとして入力することはできません。
- PAT プールについて、次のオプションの 1 つ以上を指定できます。
- **round-robin** : PAT プールのラウンドロビンアドレス割り当てをイネーブルにします。ラウンドロビンを指定しなければ、デフォルトで PAT アドレスのすべてのポートは次の PAT アドレスが使用される前に割り当てられます。ラウンドロビン方式では、最初のアドレスに戻って再び使用される前に、2 番目のアドレス、またその次と、プール内の各 PAT アドレスからアドレス/ポートが割り当てられます。
  - **extended** : 拡張 PAT をイネーブルにします。拡張 PAT では、変換情報の宛先アドレスとポートを含め、IP アドレスごとではなく、サービスごとに 65535 個のポートが使用されます。通常は、PAT 変換を作成するときに宛先ポートとアドレスは考慮されないため、PAT アドレスごとに 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。
  - **flat [include-reserve]** : (フラット範囲) ポートを割り当てるときに 1024 ~ 65535 のポート範囲全体を使用できるようにします。変換のマッピングポート番号を選択するときに、ASA によって、使用可能な場合は実際の送信元ポート番号が使用されます。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 (1 ~ 511、512 ~ 1023、および 1024 ~ 65535) から選択されます。下位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、 **include-reserve** キーワードも指定します。
  - **block-allocation** : ポートブロック割り当てをイネーブルにします。キャリアグレードまたは大規模 PAT の場合は、NAT に一度に 1 つずつポート変換を割り当てさせる代わりに、各ホストのポートのブロックを割り当てることができます。ポートのブロックを割り当てると、ホストからのその後の接続では、ブロック内のランダムに選択される新しいポートが使用されます。必要に応じて、ホストが元のブロック内のすべてのポートに関してアクティブな接続を持つ場合は追加のブロックが割り当てられます。ポートブロックは、1024 ~ 65535 の範囲でのみ割り当てられます。ポートのブロック割り当ては **round-robin** と互換性がありますが、 **extended** または **flat**

**[include-reserve]** オプションを使用することはできません。また、インターフェイス PAT のフォールバックを使用することもできません。

- インターフェイス PAT のフォールバック：（任意）**interface [ipv6]** キーワードは、プライマリ PAT アドレスの後に入力されたときにインターフェイス PAT のフォールバックをイネーブルにします。プライマリ PAT アドレスを使い果たすと、マッピングインターフェイスの IP アドレスが使用されます。**ipv6** を指定した場合、インターフェイスの IPv6 アドレスが使用されます。このオプションでは、*mapped\_ifc* に特定のインターフェイスを設定する必要があります。（マッピングされたインターフェイスがブリッジグループメンバーのときは、**interface** を指定できません）

例：

```
hostname(config-network-object)# nat (any,outside) dynamic interface
```

例

次の例では、アドレス 10.2.2.2 の背後に 192.168.2.0 ネットワークを隠すダイナミック PAT を設定します。

```
hostname(config)# object network my-inside-net
hostname(config-network-object)# subnet 192.168.2.0 255.255.255.0
hostname(config-network-object)# nat (inside,outside) dynamic 10.2.2.2
```

次の例では、外部インターフェイスアドレスの背後に 192.168.2.0 ネットワークを隠蔽するダイナミック PAT を設定します。

```
hostname(config)# object network my-inside-net
hostname(config-network-object)# subnet 192.168.2.0 255.255.255.0
hostname(config-network-object)# nat (inside,outside) dynamic interface
```

次の例では、ダイナミック PAT と PAT プールを使用して内部 IPv6 ネットワークを外側 IPv4 ネットワークに変換するように設定します。

```
hostname(config)# object network IPv4_POOL
hostname(config-network-object)# range 203.0.113.1 203.0.113.254
hostname(config)# object network IPv6_INSIDE
hostname(config-network-object)# subnet 2001:DB8::/96
hostname(config-network-object)# nat (inside,outside) dynamic pat-pool IPv4_POOL
```

## ダイナミック Twice PAT の設定

この項では、ダイナミック PAT の Twice NAT を設定する方法について説明します。

## 手順

**ステップ 1** 送信元の実際アドレス、送信元のマッピングアドレス、宛先の実際アドレス、および宛先のマッピングアドレスに、ホストまたは範囲のネットワーク オブジェクト (**object network** コマンド)、またはネットワーク オブジェクト グループ (**object-group network** コマンド) を作成します。

- すべての送信元トラフィックを変換する場合、送信元の実際アドレスに対するオブジェクトの追加をスキップして、代わりに、**nat** コマンドに **any** キーワードを指定できます。
- インターフェイス アドレスをマッピング アドレスとして使用する場合は、送信元のマッピングアドレスに対するオブジェクトの追加をスキップして、代わりに、**nat** コマンドに **interface** キーワードを指定できます。
- ポート変換を設定した宛先のスタティック インターフェイス NAT のみを設定する場合は、宛先のマッピングアドレスに対するオブジェクトの追加をスキップして、代わりに、**nat** コマンドに **interface** キーワードを指定できます。

オブジェクトを使用する場合は、オブジェクトまたはグループにサブネットを含めることはできません。オブジェクトは、1つのホスト、または範囲 (PAT プールの場合) を定義する必要があります。グループ (PAT プールの場合) には、複数のホストと範囲を含めることができます。

**ステップ 2** (任意) 宛先の実際のポートおよび宛先のマッピング ポートにサービス オブジェクトを作成します。

ダイナミック NAT の場合、宛先でポート変換のみを実行できます。サービス オブジェクトには送信元ポートと宛先ポートの両方を含めることができますが、この場合は、宛先ポートだけが使用されます。送信元ポートを指定した場合、無視されます。

**ステップ 3** ダイナミック PAT を設定します。

```
nat[(real_ifc,mapped_ifc)][line | after-auto [line]] source dynamic {real_obj | any} {mapped_obj
[interface [ipv6]] | pat-pool mapped_obj [round-robin] [extended] [flat [include-reserve]]
[block-allocation] [interface [ipv6]] | interface [ipv6]} [destination static {mapped_obj | interface
[ipv6]} real_obj] [ service mapped_dest_svc_obj real_dest_svc_obj] [unidirectional] [inactive] [
description description]
```

それぞれの説明は次のとおりです。

- インターフェイス：(ブリッジグループメンバーのインターフェイスに必要) 実際のインターフェイス (*real\_ifc*) およびマッピング インターフェイス (*mapped\_ifc*) を指定します。丸カッコを含める必要があります。ルーテッドモードでは、実際のインターフェイス およびマッピング インターフェイスを指定しない場合は、すべてのインターフェイスが使用されます。また、(any,outside) のようにインターフェイスのいずれかまたは両方にキーワード **any** を指定することもできます。ただし、**any** はブリッジグループのメンバ インターフェイスには適用されません。
- セクションおよび行：(任意) デフォルトでは、NAT 規則は、NAT テーブルのセクション 1 の末尾に追加されます (NAT ルールの順序 (5 ページ) を参照)。セクション 1 で

はなく、セクション 3 (ネットワーク オブジェクト NAT ルールの後ろ) にルールを追加する場合、**after-auto** キーワードを使用します。ルールは、*line* 引数を使用して、適切なセクションの任意の場所に挿入できます。

• 送信元アドレス :

- 実際のアドレス : ネットワーク オブジェクト、グループ、または **any** キーワードを指定します。実際のインターフェイスからマッピングされたインターフェイスへのすべてのトラフィックを変換する場合、**any** キーワードを使用します。
- マッピングアドレス : 次のいずれかを設定します。
  - ネットワークオブジェクト : ホストアドレスを含むネットワークオブジェクト。
  - **pat-pool mapped-obj** : 複数の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。
  - **interface [ipv6]** : (ルーテッドモードのみ。) マッピングインターフェイスの IP アドレスがマッピングアドレス (インターフェイス PAT) として使用されます。**ipv6** を指定した場合、インターフェイスの IPv6 アドレスが使用されます。このオプションでは、*mapped\_ifc* に特定のインターフェイスを設定する必要があります。(マッピングされたインターフェイスがブリッジグループメンバーのときは、**interface** を指定できません) PAT プールまたはネットワーク オブジェクトでこのキーワードを指定すると、インターフェイス PAT のフォールバックが有効になります。PAT IP アドレスを使い果たすと、マッピングインターフェイスの IP アドレスが使用されます。

PAT プールについて、次のオプションの 1 つ以上を指定できます。

- **round-robin** : PAT プールのラウンドロビンアドレス割り当てをイネーブルにします。ラウンドロビンを指定しなければ、デフォルトで PAT アドレスのすべてのポートは次の PAT アドレスが使用される前に割り当てられます。ラウンドロビン方式では、最初のアドレスに戻って再び使用される前に、2 番目のアドレス、またその次と、プール内の各 PAT アドレスからアドレス/ポートが割り当てられます。
- **extended** : 拡張 PAT をイネーブルにします。拡張 PAT では、変換情報の宛先アドレスとポートを含め、IP アドレスごとではなく、サービスごとに 65535 個のポートが使用されます。通常は、PAT 変換を作成するときに宛先ポートとアドレスは考慮されないため、PAT アドレスごとに 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。
- **flat [include-reserve]** : (フラット範囲) ポートを割り当てるときに 1024 ~ 65535 のポート範囲全体を使用できるようにします。変換のマッピングポート番号を選択するとき、ASA によって、使用可能な場合は実際の送信元ポート番号が使用されます。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 (1 ~ 511、512 ~ 1023、および 1024 ~ 65535) から選択されます。下位範囲

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、**include-reserve** キーワードも指定します。

- **block-allocation** : ポートブロック割り当てをイネーブルにします。キャリアグレードまたは大規模 PAT の場合は、NAT に一度に1つずつポート変換を割り当てさせる代わりに、各ホストのポートのブロックを割り当てることができます。ポートのブロックを割り当てると、ホストからのその後の接続では、ブロック内のランダムに選択される新しいポートが使用されます。必要に応じて、ホストが元のブロック内のすべてのポートに関してアクティブな接続を持つ場合は追加のブロックが割り当てられます。ポートブロックは、1024 ~ 65535 の範囲でのみ割り当てられます。ポートのブロック割り当ては **round-robin** と互換性がありますが、**extended** または **flat [include-reserve]** オプションを使用することはできません。また、インターフェイス PAT のフォールバックを使用することもできません。
- 宛先アドレス (任意) :
  - マッピングアドレス : ネットワーク オブジェクトまたはグループを指定します。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 に限り (非ブリッジグループのメンバインターフェイスのみ)、**interface** キーワードを指定します。**ipv6** を指定した場合、インターフェイスの IPv6 アドレスが使用されます。**interface** を指定する場合は、必ず **service** キーワードも設定します。このオプションでは、*real\_ifc* に特定のインターフェイスを設定する必要があります。詳細については、「[ポート変換を設定したスタティック NAT \(38 ページ\)](#)」を参照してください。
  - 実際のアドレス : ネットワーク オブジェクトまたはグループを指定します。アイデンティティ NAT では、実際のアドレスとマッピングアドレスの両方に単に同じオブジェクトまたはグループを使用します。
- 宛先ポート : (任意) マッピングされたサービス オブジェクトおよび実際のサービス オブジェクトとともに、**service** キーワードを指定します。アイデンティティ ポート変換では、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します。
- 単方向 : (任意) 宛先アドレスが送信元アドレスへのトラフィックを開始できないようにするには、**unidirectional** を指定します。
- 非アクティブ : (任意) コマンドを削除する必要なくこのルールを非アクティブにするには、**inactive** キーワードを使用します。再度アクティブ化するには、**inactive** キーワードを除いてコマンド全体を再入力します。
- 説明 : (任意) **description** キーワードを使用して、最大 200 文字の説明を入力します。

例 :

```
hostname(config)# nat (inside,outside) source dynamic MyInsNet interface
destination static Server1 Server1
```

```
description Interface PAT for inside addresses when going to server 1
```

---

## 例

次に、外部 Telnet サーバ 209.165.201.23 へのアクセス時に内部ネットワーク 192.168.1.0/24 のインターフェイス PAT を設定し、203.0.113.0/24 ネットワーク上のサーバへのアクセス時に PAT プールを使用してダイナミック PAT を設定する例を示します。

```
hostname(config)# object network INSIDE_NW
hostname(config-network-object)# subnet 192.168.1.0 255.255.255.0

hostname(config)# object network PAT_POOL
hostname(config-network-object)# range 209.165.200.225 209.165.200.254

hostname(config)# object network TELNET_SVR
hostname(config-network-object)# host 209.165.201.23

hostname(config)# object service TELNET
hostname(config-service-object)# service tcp destination eq 23

hostname(config)# object network SERVERS
hostname(config-network-object)# subnet 203.0.113.0 255.255.255.0

hostname(config)# nat (inside,outside) source dynamic INSIDE_NW interface
destination static TELNET_SVR TELNET_SVR service TELNET TELNET
hostname(config)# nat (inside,outside) source dynamic INSIDE_NW pat-pool PAT_POOL
destination static SERVERS SERVERS
```

次に、外部 IPv6 Telnet サーバ 2001:DB8::23 へのアクセス時に内部ネットワーク 192.168.1.0/24 のインターフェイス PAT を設定し、2001:DB8:AAAA::/96 ネットワーク上のサーバへのアクセス時に PAT プールを使用してダイナミック PAT を設定する例を示します。

```
hostname(config)# object network INSIDE_NW
hostname(config-network-object)# subnet 192.168.1.0 255.255.255.0

hostname(config)# object network PAT_POOL
hostname(config-network-object)# range 2001:DB8:AAAA::1 2001:DB8:AAAA::200

hostname(config)# object network TELNET_SVR
hostname(config-network-object)# host 2001:DB8::23

hostname(config)# object service TELNET
hostname(config-service-object)# service tcp destination eq 23

hostname(config)# object network SERVERS
hostname(config-network-object)# subnet 2001:DB8:AAAA::/96

hostname(config)# nat (inside,outside) source dynamic INSIDE_NW interface ipv6
destination static TELNET_SVR TELNET_SVR service TELNET TELNET
hostname(config)# nat (inside,outside) source dynamic INSIDE_NW pat-pool PAT_POOL
destination static SERVERS SERVERS
```

## ポート ブロック割り当てによる PAT の設定

キャリア グレードまたは大規模 PAT では、NAT に 1 度に 1 つのポート変換を割り当てさせるのではなく、各ホストにポートのブロックを割り当てることができます (RFC 6888 を参照してください)。ポートのブロックを割り当てる場合、ホストからの後続の接続はブロック内の新しい任意選択されたポートを使用します。必要に応じて、元のブロックにすべてのポートに対するアクティブな接続がホストにある場合は、追加のブロックが割り当てられます。ブロック内のポートを使用する最後の `xlate` が削除されると、ブロックは解放されます。

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

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

### 始める前に

NAT ルールの使用上の注意：

- **round-robin** キーワードは含めることはできますが、**extended**、**flat**、**include-reserve**、または **interface** (インターフェイス PAT フォールバック用) を含めることはできません。その他の送信元/宛先のアドレスとポート情報も許可されます。
- 既存のルールを置き換える場合は、NAT を変更するすべてのケースと同様、置き換えるルールに関連する `xlate` をクリアする必要があります。これは、新しいルールを有効にするために必要です。それらを明示的にクリアするか、または単にタイムアウトになるまで待ちます。
- 特定の PAT プールに対し、そのプールを使用するすべてのルールに対してブロック割り当てを指定する (または指定しない) 必要があります。1 つのルールにブロックを割り当てることはできず、別のルールに割り当てることもできません。重複する PAT プールもまたブロック割り当て設定を混在させることはできません。また、ポート変換ルールを含むスタティック NAT とプールを重複させることはできません。

### 手順

**ステップ 1** (任意) ブロック割り当てサイズを設定します。これは各ブロックのポート数です。

**`xlate block-allocation size value`**

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

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

**ステップ 2** (任意) ホストごとに割り当てることができる最大ブロック数を設定します。

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

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

**ステップ 3** PAT プールのブロック割り当てを使用する NAT ルールを追加します。

- オブジェクト PAT。

**nat [(*real\_ifc*,*mapped\_ifc*)] dynamic pat-pool *mapped-obj* block-allocation**

例 :

```
object network mapped-pat-pool
  range 10.100.10.1 10.100.10.2
object network src_host
  host 10.111.10.15
object network src_host
  nat (inside,outside) dynamic
pat-pool mapped-pat-pool block-allocation
```

- Twice PAT。

**nat [(*real\_ifc*,*mapped\_ifc*)] [*line* | after-auto [*line*]] source dynamic *real\_obj* pat-pool*mapped-obj* block-allocation**

例 :

```
object network mapped-pat-pool
  range 10.100.10.1 10.100.10.2
object network src_network
  subnet 10.100.10.0 255.255.255.0
nat (inside,outside) 1 source dynamic src_network
pat-pool mapped-pat-pool block-allocation
```

## Per-Session PAT または Multi-Session PAT の設定

デフォルトでは、すべての TCP PAT トラフィックおよびすべての UDP DNS トラフィックが Per-Session PAT を使用します。トラフィックに Multi-Session PAT を使用するには、Per-Session PAT ルールを設定します。許可ルールで Per-Session PAT を使用し、拒否ルールで Multi-Session PAT を使用します。

Per-Session PAT によって PAT のスケーラビリティが向上し、クラスタリングの場合に各メンバーユニットに独自の PAT 接続を使用できるようになります。Multi-Session PAT 接続は、マスターユニットに転送してマスターユニットを所有者とする必要があります。Per-Session PAT セッションの終了時に、ASA からリセットが送信され、即座に xlate が削除されます。このリセットによって、エンドノードは即座に接続を解放し、TIME\_WAIT 状態を回避します。対照的に、Multi-Session PAT では、PAT タイムアウトが使用されます（デフォルトでは 30 秒）。

HTTP や HTTPS などの「ヒットエンドラン」トラフィックの場合、Per-Session PAT は、1 つのアドレスによってサポートされる接続率を大幅に増やすことができます。Per-Session PAT を使用しない場合は、特定の IP プロトコルに対する 1 アドレスの最大接続率は約 2000/秒です。Per-Session PAT を使用する場合は、特定の IP プロトコルに対する 1 アドレスの接続率は 65535/平均ライフタイムです。

Multi-Session PAT のメリットを活用できるトラフィック、たとえば H.323、SIP、Skinny に対して Per-session PAT をディセーブルにするには、Per-session 拒否ルールを作成します。ただし、これらのプロトコルで使用する UDP ポートにセッション単位の PAT も使用する場合は、それらに許可ルールを作成する必要があります。

### 始める前に

デフォルトでは、次のルールがインストールされます。

```
xlate per-session permit tcp any4 any4
xlate per-session permit tcp any4 any6
xlate per-session permit tcp any6 any4
xlate per-session permit tcp any6 any6
xlate per-session permit udp any4 any4 eq domain
xlate per-session permit udp any4 any6 eq domain
xlate per-session permit udp any6 any4 eq domain
xlate per-session permit udp any6 any6 eq domain
```

これらのルールは削除できません。これらのルールは常に、手動作成されたルールの後に存在します。ルールは順番に評価されるので、デフォルトルールを無効にすることができます。たとえば、これらのルールを完全に反転させるには、次のものを追加します。

```
xlate per-session deny tcp any4 any4
xlate per-session deny tcp any4 any6
xlate per-session deny tcp any6 any4
xlate per-session deny tcp any6 any6
xlate per-session deny udp any4 any4 eq domain
xlate per-session deny udp any4 any6 eq domain
xlate per-session deny udp any6 any4 eq domain
xlate per-session deny udp any6 any6 eq domain
```

### 手順

Per-session PAT の許可または拒否ルールを作成します。このルールはデフォルトルールの上に置かれますが、他の手動作成されたルールよりは下です。ルールは必ず、適用する順序で作成してください。

```
xlate per-session {permit | deny} {tcp | udp} source_ip [operator src_port] destination_ip [operator dest_port]
```

変換元と変換先の IP アドレスについては、次のように設定できます。

- **host ip\_address** : IPv4 または IPv6 ホスト アドレスを指定します。
- **ip\_address mask** : IPv4 ネットワーク アドレスおよびサブネット マスクを指定します。
- **ipv6-address/prefix-length** : IPv6 ネットワーク アドレスとプレフィックスを指定します。
- **any4** および **any6** : **any4** は IPv4 トラフィックだけを指定します。**any6** は any6 トラフィックを指定します。

*operator* では、変換元または変換先で使用されるポート番号の条件を指定します。デフォルトでは、すべてのポートです。使用できる演算子は、次のとおりです。

- **lt** : より小さい
- **gt** : より大きい
- **eq** : 等しい
- **neq** : 等しくない
- **range** : 値の包括的な範囲。この演算子を使用する場合は、2つのポート番号を指定します (例 : **range 100 200**) 。

## 例

次の例では、H.323 トラフィックのための拒否ルールを作成します。このトラフィックには Multi-Session PAT が使用されるようにするためです。

```
hostname(config)# xlate per-session deny tcp any4 209.165.201.7 eq 1720
hostname(config)# xlate per-session deny udp any4 209.165.201.7 range 1718 1719
```

次に、SIP UDP ポートにセッション単位の PAT を許可することで、クラスタのメンバー間での SIP の分散を有効にする例を示します。SIP TCP ポートではセッション単位の PAT がデフォルトであるため、デフォルトのルールを変更した場合を除き、TCP にルールは必要ありません。

```
hostname(config)# xlate per-session permit udp any4 any4 eq sip
```

# スタティック NAT

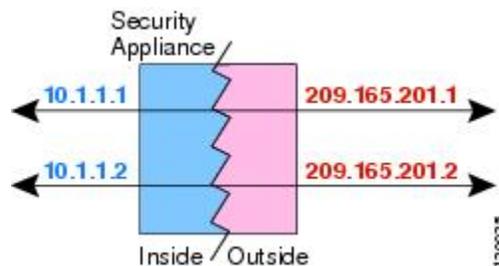
ここでは、スタティック NAT とその実装方法について説明します。

## 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なので、スタティック NAT では、双方向の接続（ホストへの接続とホストから接続の両方）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ので、双方向の開始はサポートされません。

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

図 5: スタティック NAT



(注) 必要に応じて、双方向をディセーブルにできます。

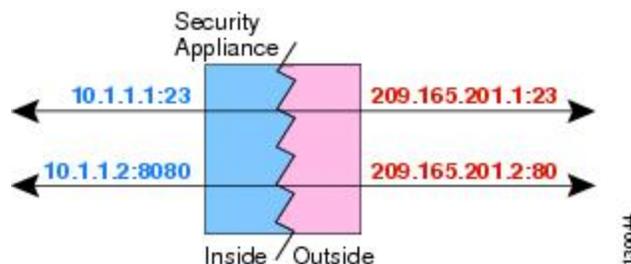
## ポート変換を設定したスタティック NAT

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なので、変換されたホストとリモートホストの両方が接続を開始できます。

図 6: ポート変換を設定したスタティック NAT の一般的なシナリオ



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



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

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

#### アイデンティティ ポート変換を設定したスタティック NAT

内部リソースへの外部アクセスを簡素化できます。たとえば、異なるポートでサービスを提供する3つの個別のサーバ (FTP、HTTP、SMTP など) がある場合は、それらのサービスにアクセスするための単一の IP アドレスを外部ユーザに提供できます。その後、アイデンティティ ポート変換を設定したスタティック NAT を設定し、アクセスしようとしているポートに基づいて、単一の外部 IP アドレスを実サーバの正しい IP アドレスにマッピング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。この例の設定方法については、[FTP、HTTP、および SMTP の単一アドレス \(ポート変換を設定したスタティック NAT\)](#) を参照してください。

#### 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。

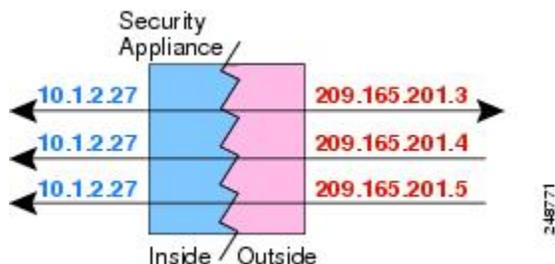
## 一対多のスタティック NAT

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。

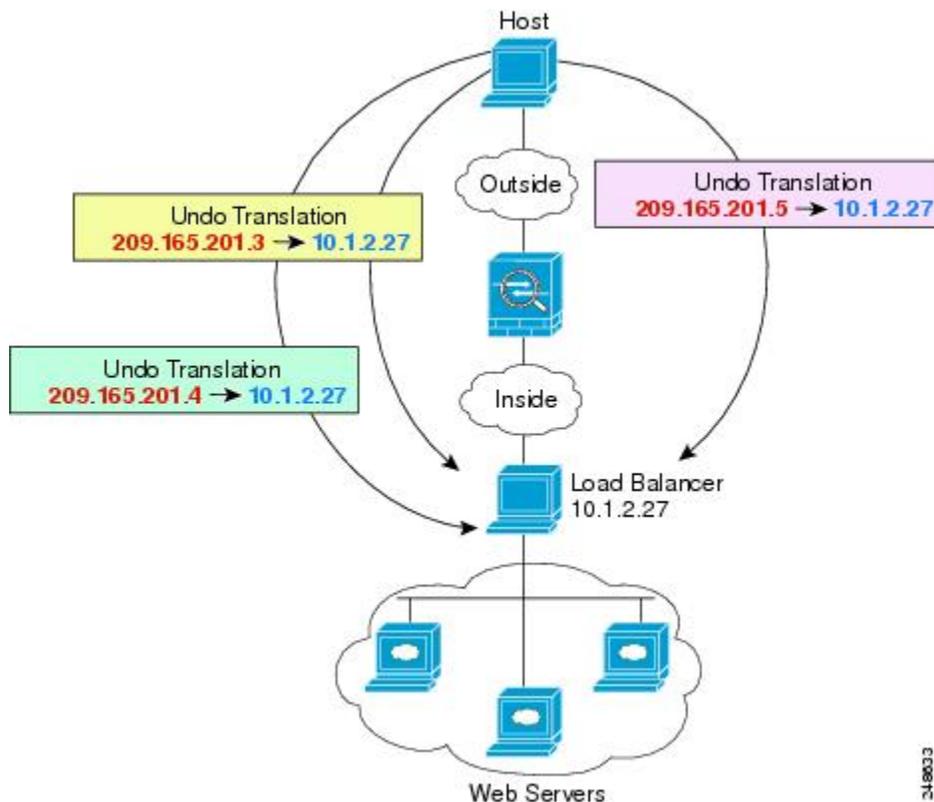
次の図に、一般的な1対多のスタティック NAT シナリオを示します。実際のホストが開始すると、常に最初のマッピングアドレスが使用されるため、実際のホスト IP/最初のマッピング IP の変換は、理論的には双方向変換のみが行われます。

図 7:一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。この例の設定方法については、[複数のマッピングアドレス \(スタティック NAT、一対多\) を持つ内部ロードバランサ](#)を参照してください。

図 8:一対多のスタティック NAT の例



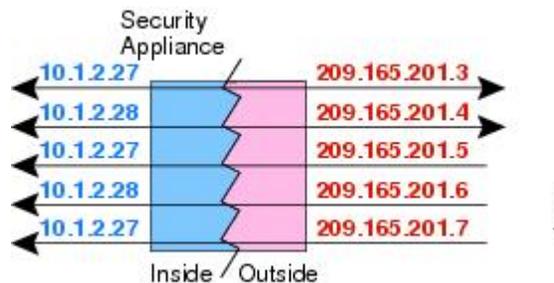
## 他のマッピングシナリオ (非推奨)

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。しかし、コンフィギュレーションが複雑化して、実際のマッピングが一目では明らかでない場合があるため、必要とする実際の各アドレスに対して1対多のコンフィギュレーションを作成することを推奨します。たとえば、少対多のシナリオでは、少数の実際のアドレスが多数のマッピングアドレスに順番にマッピングされます (Aは1、Bは2、Cは3)。すべての実際のアドレスがマッピングされたら、次にマッピングされるアドレスは、最初の実際のアドレスにマッピングされ、すべてのマッピングアドレスがマッピングされるまで続行されます (Aは4、Bは5、Cは6)。この結果、実際の各アドレスに対して複数のマッピングアドレスが存在することになります。1対多のコンフィギュレーションのように、最初のマッピングだけが双方向であり、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 9: 少対多のスタティック NAT



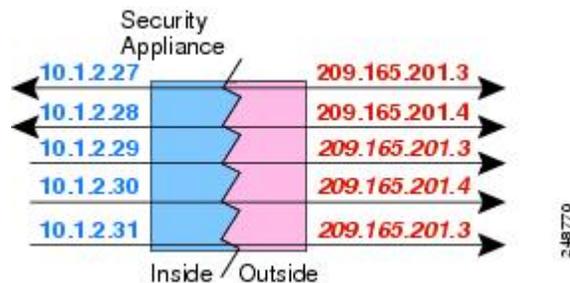
多対少または多対1コンフィギュレーションでは、マッピングアドレスよりも多くの実際のアドレスが存在します。実際のアドレスが不足するよりも前に、マッピングアドレスが不足します。双方向の開始を実現できるのは、最下位の実際の IP アドレスとマッピングされたプールの中でマッピングを行ったときだけです。残りの上位の実際のアドレスはトラフィックを開始できますが、これらへのトラフィックを開始できません。接続のリターントラフィックは、接続の固有の5つの要素 (送信元 IP、宛先 IP、送信元ポート、宛先ポート、プロトコル) によって適切な実際のアドレスに転送されます。



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

次の図に、一般的な多対少のスタティック NAT シナリオを示します。

図 10: 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 ネットワーク オブジェクト NAT またはポート変換を設定したスタティック NAT の設定

この項では、ネットワーク オブジェクト NAT を使用してスタティック NAT ルールを設定する方法について説明します。

### 手順

**ステップ 1** (任意) マッピングアドレスにネットワーク オブジェクト (**object network** コマンド) またはネットワーク オブジェクト グループ (**object-group network** コマンド) を作成します。

- オブジェクトを使用する代わりに、インラインアドレスを設定するか、またはインターフェイスアドレスを指定できます (ポート変換を使用するスタティック NAT の場合)。
- オブジェクトを使用する場合は、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入れることができます。

**ステップ 2** NAT を設定するネットワーク オブジェクトを作成または編集します。 **object network obj\_name**  
例 :

```
hostname(config)# object network my-host-obj1
```

**ステップ 3** (正しいアドレスがあるオブジェクトを編集する場合はスキップする) 変換する実際の IPv4 または IPv6 アドレスを定義します。

- **host {IPv4\_address|IPv6\_address}** : 単一のホストの IPv4 または IPv6 アドレス。たとえば、10.1.1.1 または 2001:DB8::0DB8:800:200C:417A。
- **subnet {IPv4\_address IPv4\_mask|IPv6\_address|IPv6\_prefix}** : ネットワークのアドレス。IPv4 サブネットの場合、10.0.0.0 255.0.0.0 のように、スペースの後ろにマスクを含めます。IPv6

の場合、2001:DB8:0:CD30::/60 のように、アドレスとプレフィックスを単一のユニット（スペースなし）として含めます。

- **range start address end address** : アドレスの範囲。IPv4 または IPv6 の範囲を指定できます。マスクまたはプレフィックスを含めないでください。

例 :

```
hostname(config-network-object)# subnet 10.2.1.0 255.255.255.0
```

**ステップ 4** オブジェクト IP アドレスのスタティック NAT を設定します。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。

```
nat(real_ifc,mapped_ifc) static {mapped_inline_host_ip | mapped_obj [interface [ipv6]] [net-to-net] [dns | service {tcp | udp | sctp} real_port mapped_port] [no-proxy-arp]
```

それぞれの説明は次のとおりです。

- **インターフェイス** : (ブリッジグループメンバーのインターフェイスに必要) 実際のインターフェイス (*real\_ifc*) およびマッピングインターフェイス (*mapped\_ifc*) を指定します。丸カッコを含める必要があります。ルーテッドモードでは、実際のインターフェイスおよびマッピングインターフェイスを指定しない場合は、すべてのインターフェイスが使用されます。また、(*any,outside*) のようにインターフェイスのいずれかまたは両方にキーワード **any** を指定することもできます。ただし、**any** はブリッジグループのメンバインターフェイスには適用されません。
- **マッピング IP アドレス** : マッピング IP アドレスを次のいずれかとして指定できます。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。[スタティック NAT \(37 ページ\)](#) を参照してください。
  - **mapped\_inline\_host\_ip** : インラインホスト IP アドレス。これにより、ホストオブジェクトだけに 1 対 1 のマッピングが提供されます。それ以外の場合は、多対 1 のマッピングを取得します。NAT46 または NAT66 変換では、IPv6 ネットワークアドレスを指定できます。
  - **mapped\_obj** : 既存のネットワーク オブジェクトまたはグループ。IP アドレスの範囲に 1 対 1 のマッピングを行うには、同じ数のアドレスを含む範囲を含むオブジェクトを選択します。
  - **interface** : (ポート変換を設定したスタティック NAT のみ) マッピングインターフェイスの IP アドレスがマッピングアドレスとして使用されます。**ipv6** を指定すると、インターフェイスの IPv6 アドレスが使用されます。このオプションでは、*mapped\_ifc* に特定のインターフェイスを設定する必要があります。(マッピングされたインターフェイスがブリッジグループメンバーのときは、**interface** を指定できません) このキーワードは、インターフェイスの IP アドレスを使用するときに使用する必要があります。インラインで、またはオブジェクトとして入力することはできません。**service** キーワードも必ず設定します

- ネットツーネット：（任意）NAT 46 の場合、**net-to-net** を指定すると、最初の IPv4 アドレスが最初の IPv6 アドレスに、2 番目が 2 番目に、というように変換されます。このオプションを指定しない場合は、IPv4 埋め込み方式が使用されます。1 対 1 変換の場合は、このキーワードを使用する必要があります。
- DNS：（任意）**dns** キーワードは、DNS 応答を変換します。DNS インспекションがイネーブルになっていることを確認してください（デフォルトではイネーブルです）。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](#)」を参照してください。
- ポート変換：（ポート変換を設定したスタティック NAT のみ）希望するプロトコルキーワードと実際のポートおよびマッピングポートとともに **service** を指定します。ポート番号または予約済みポートの名前（**http** など）のいずれかを入力できます。
- プロキシ ARP なし：（任意）マッピング IP アドレスに着信したパケットのプロキシ ARP をディセーブルにするには、**no-proxy-arp** を指定します。プロキシ ARP のディセーブル化が必要となる可能性がある状況については、[マッピングアドレスとルーティング](#)を参照してください。

例：

```
hostname(config-network-object)#
nat (inside,outside) static MAPPED_IPS service tcp 80 8080
```

例

次の例では、内部にある実際のホスト 10.1.1.1 の、DNS リライトがイネーブルに設定された外部にある 10.2.2.2 へのスタティック NAT を設定します。

```
hostname(config)# object network my-host-obj1
hostname(config-network-object)# host 10.1.1.1
hostname(config-network-object)# nat (inside,outside) static 10.2.2.2 dns
```

次の例では、内部にある実際のホスト 10.1.1.1 の、マッピングされたオブジェクトを使用する外部にある 10.2.2.2 へのスタティック NAT を設定します。

```
hostname(config)# object network my-mapped-obj
hostname(config-network-object)# host 10.2.2.2

hostname(config-network-object)# object network my-host-obj1
hostname(config-network-object)# host 10.1.1.1
hostname(config-network-object)# nat (inside,outside) static my-mapped-obj
```

次の例では、10.1.1.1 の TCP ポート 21 の、外部インターフェイスのポート 2121 への、ポート変換を設定したスタティック NAT を設定します。

```
hostname(config)# object network my-ftp-server
hostname(config-network-object)# host 10.1.1.1
```

```
hostname(config-network-object)# nat (inside,outside) static interface service tcp 21 2121
```

次の例では、内部 IPv4 ネットワークを外部 IPv6 ネットワークにマッピングします。

```
hostname(config)# object network inside_v4_v6
hostname(config-network-object)# subnet 10.1.1.0 255.255.255.0
hostname(config-network-object)# nat (inside,outside) static 2001:DB8::/96
```

次の例では、内部 IPv6 ネットワークを外部 IPv6 ネットワークにマッピングします。

```
hostname(config)# object network inside_v6
hostname(config-network-object)# subnet 2001:DB8:AAAA::/96
hostname(config-network-object)# nat (inside,outside) static 2001:DB8:BBBB::/96
```

## スタティック **Twice NAT** またはポート変換を設定したスタティック **NAT** の設定

この項では、Twice NAT を使用してスタティック NAT ルールを設定する方法について説明します。

### 手順

**ステップ 1** 送信元の実際のアドレス、送信元のマッピングアドレス、宛先の実際のアドレス、および宛先のマッピングアドレスに、ホストまたは範囲のネットワーク オブジェクト (**object network** コマンド)、またはネットワーク オブジェクトグループ (**object-group network** コマンド) を作成します。

- ポート変換を設定した送信元のスタティック インターフェイス NAT のみを設定する場合は、送信元のマッピングアドレスに対するオブジェクトの追加をスキップして、代わりに、**nat** コマンドに **interface** キーワードを指定できます。
- ポート変換を設定した宛先のスタティック インターフェイス NAT のみを設定する場合は、宛先のマッピングアドレスに対するオブジェクトの追加をスキップして、代わりに、**nat** コマンドに **interface** キーワードを指定できます。

オブジェクトを作成する場合は、次のガイドラインを考慮してください。

- マッピングされたオブジェクトまたはグループには、ホスト、範囲、またはサブネットを含めることができます。
- スタティック マッピングは、通常 1 対 1 です。したがって、実際のアドレスとマッピングアドレスの数は同じです。ただし、必要に応じて異なる数にすることができます。詳細については、[スタティック NAT \(37 ページ\)](#) を参照してください。

**ステップ 2** (任意) 次のサービス オブジェクトを作成します。

- 送信元または宛先の実際のポート
- 送信元または宛先のマッピング ポート

サービスオブジェクトには、送信元ポートと宛先ポートの両方を含めることができますが、両方のサービスオブジェクトに送信元ポートまたは宛先ポートのいずれかを指定する必要があります。ご使用のアプリケーションが固定の送信元ポートを使用する場合（一部の DNS サーバなど）に送信元ポートおよび宛先ポートの両方を指定する必要がありますが、固定の送信元ポートはめったに使用されません。たとえば、送信元ホストのポートを変換する場合は、送信元サービスを設定します。

### ステップ3 スタティック NAT を設定します。

```
nat [(real_ifc,mapped_ifc)] [line | {after-object [line]}] source static real_ob [mapped_obj | interface [ipv6]] [destination static {mapped_obj | interface [ipv6]} real_obj] [service real_src_mapped_dest_svc_obj mapped_src_real_dest_svc_obj] [net-to-net] [dns] [unidirectional | no-proxy-arp] [inactive] [description desc]
```

それぞれの説明は次のとおりです。

- インターフェイス：（ブリッジグループメンバーのインターフェイスに必要）実際のインターフェイス (*real\_ifc*) およびマッピングインターフェイス (*mapped\_ifc*) を指定します。丸カッコを含める必要があります。ルーテッドモードでは、実際のインターフェイスおよびマッピングインターフェイスを指定しない場合は、すべてのインターフェイスが使用されます。また、(*any,outside*) のようにインターフェイスのいずれかまたは両方にキーワード **any** を指定することもできます。ただし、**any** はブリッジグループのメンバインターフェイスには適用されません。
- セクションおよび行：（任意）デフォルトでは、NAT 規則は、NAT テーブルのセクション1の末尾に追加されます（[NAT ルールの順序（5 ページ）](#) を参照）。セクション1ではなく、セクション3（ネットワーク オブジェクト NAT ルールの後ろ）にルールを追加する場合、**after-auto** キーワードを使用します。ルールは、*line* 引数を使用して、適切なセクションの任意の場所に挿入できます。
- 送信元アドレス：
  - 実際のアドレス：ネットワーク オブジェクトまたはグループを指定します。アイデンティティ NAT に使用される **any** キーワードを使用しないでください。
  - マッピングアドレス：異なるネットワーク オブジェクトまたはグループを指定します。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 に限り、**interface** キーワードを指定できます。**ipv6** を指定すると、インターフェイスの IPv6 アドレスが使用されます。**interface** を指定する場合、**service** キーワードも設定します（この場合、サービス オブジェクトは送信元ポートだけを含む必要があります）。このオプションでは、*mapped\_ifc* に特定のインターフェイスを設定する必要があります。（マッピングされたインターフェイスがブリッジグループメンバーのときは、**interface** を指定できません）詳細については、「[ポート変換を設定したスタティック NAT（38 ページ）](#)」を参照してください。
- 宛先アドレス（任意）：

- マッピングアドレス：ネットワークオブジェクトまたはグループを指定します。ポート変換が設定されたスタティック インターフェイス NAT に限り、**interface** キーワードを指定します。**ipv6** を指定すると、インターフェイスの IPv6 アドレスが使用されます。**interface** を指定する場合、必ず **service** キーワードも設定します（この場合、サービスオブジェクトは宛先ポートだけを含む必要があります）。このオプションでは、**real\_ifc** に特定のインターフェイスを設定する必要があります。（マッピングされたインターフェイスがブリッジグループメンバーのときは、**interface** を指定できません）
- 実際のアドレス：ネットワークオブジェクトまたはグループを指定します。アイデンティティ NAT では、実際のアドレスとマッピングアドレスの両方に単に同じオブジェクトまたはグループを使用します。
- ポート：（任意）実際のサービスオブジェクトおよびマッピングされたサービスオブジェクトとともに、**service** キーワードを指定します。送信元ポート変換の場合、オブジェクトは送信元サービスを指定する必要があります。送信元ポート変換のコマンド内のサービスオブジェクトの順序は、**service real\_obj mapped\_obj** です。宛先ポート変換の場合、オブジェクトは宛先サービスを指定する必要があります。宛先ポート変換のサービスオブジェクトの順序は、**service mapped\_obj real\_obj** です。オブジェクトで送信元ポートと宛先ポートの両方を指定することはほとんどありませんが、この場合には、最初のサービスオブジェクトに実際の送信元ポート/マッピングされた宛先ポートが含まれます。2つめのサービスオブジェクトには、マッピングされた送信元ポート/実際の宛先ポートが含まれます。アイデンティティ ポート変換の場合は、実際のポートとマッピングポートの両方（コンフィギュレーションに応じて、送信元ポート、宛先ポート、またはその両方）に同じサービスオブジェクトを使用するだけです。
- ネットツーネット：（任意）NAT 46 の場合、**net-to-net** を指定すると、最初の IPv4 アドレスが最初の IPv6 アドレスに、2 番目が 2 番目に、というように変換されます。このオプションを指定しない場合は、IPv4 埋め込み方式が使用されます。1 対 1 変換の場合は、このキーワードを使用する必要があります。
- DNS：（任意、送信元にのみ適用されるルール）**dns** キーワードは、DNS 応答を変換しません。DNS インспекションがイネーブルになっていることを確認してください（デフォルトではイネーブルです）。宛先アドレスを設定する場合、**dns** キーワードは設定できません。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](#)」を参照してください。
- 単方向：（任意）宛先アドレスが送信元アドレスへのトラフィックを開始できないようにするには、**unidirectional** を指定します。
- プロキシ ARP なし：（任意）マッピング IP アドレスに着信したパケットのプロキシ ARP をディセーブルにするには、**no-proxy-arp** を指定します。詳細については、「[マッピングアドレスとルーティング](#)」を参照してください。
- 非アクティブ：（任意）コマンドを削除する必要なくこの規則を非アクティブにするには、**inactive** キーワードを使用します。再度アクティブ化するには、**inactive** キーワードを除いてコマンド全体を再入力します。

- 説明：（任意）**description** キーワードを使用して、最大 200 文字の説明を入力します。

例：

```
hostname(config)# nat (inside,dmz) source static MyInsNet MyInsNet_mapped
destination static Server1 Server1 service REAL_SRC_SVC MAPPED_SRC_SVC
```

例

次に、ポート変換を使用するスタティック インターフェイス NAT の使用例を示します。外部にあるホストが、宛先ポート 65000 ~ 65004 を指定して外部インターフェイス IP アドレスに接続することにより、内部にある FTP サーバにアクセスします。トラフィックは、192.168.10.100:6500 ~ 65004 の内部 FTP サーバに変換されません。コマンドで指定した送信元アドレスとポートを変換するため、サービスオブジェクトには送信元ポート範囲（宛先ポートではなく）を指定することに注意してください。宛先ポートは「any」です。スタティック NAT は双方向であるため、「送信元」および「宛先」を使用して一次的にコマンドキーワードを扱うものであり、パケット内の実際の送信元および実際の宛先のアドレスとポートは、パケットを送信するホストによって異なります。この例では、外部から内部への接続が発生しているため、FTP サーバの「送信元」アドレスとポートは、実際には発信元パケット内では宛先アドレスとポートになります。

```
hostname(config)# object service FTP_PASV_PORT_RANGE
hostname(config-service-object)# service tcp source range 65000 65004

hostname(config)# object network HOST_FTP_SERVER
hostname(config-network-object)# host 192.168.10.100

hostname(config)# nat (inside,outside) source static HOST_FTP_SERVER interface
service FTP_PASV_PORT_RANGE FTP_PASV_PORT_RANGE
```

次に、IPv6 ネットワークへのアクセス時のある IPv6 から別の IPv6 へのスタティック変換、および IPv4 ネットワークへのアクセス時の IPv4 PAT プールへのダイナミック PAT 変換の例を示します。

```
hostname(config)# object network INSIDE_NW
hostname(config-network-object)# subnet 2001:DB8:AAAA::/96

hostname(config)# object network MAPPED_IPv6_NW
hostname(config-network-object)# subnet 2001:DB8:BBBB::/96

hostname(config)# object network OUTSIDE_IPv6_NW
hostname(config-network-object)# subnet 2001:DB8:CCCC::/96

hostname(config)# object network OUTSIDE_IPv4_NW
hostname(config-network-object)# subnet 10.1.1.0 255.255.255.0

hostname(config)# object network MAPPED_IPv4_POOL
hostname(config-network-object)# range 10.1.2.1 10.1.2.254
```

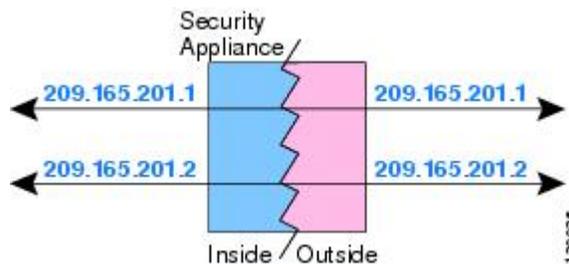
```
hostname(config)# nat (inside,outside) source static INSIDE_NW MAPPED_IPv6_NW
destination static OUTSIDE_IPv6_NW OUTSIDE_IPv6_NW
hostname(config)# nat (inside,outside) source dynamic INSIDE_NW pat-pool MAPPED_IPv4_POOL
destination static OUTSIDE_IPv4_NW OUTSIDE_IPv4_NW
```

## 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。アイデンティティ NAT は、NAT からクライアントトラフィックを除外する必要がある、リモートアクセス VPN で必要です。

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 11: 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 ネットワーク オブジェクト NAT の設定

この項では、ネットワーク オブジェクト NAT を使用してアイデンティティ NAT ルールを設定する方法について説明します。

### 手順

- ステップ 1 (任意) マッピングアドレスにネットワーク オブジェクト (**object network** コマンド) またはネットワーク オブジェクト グループ (**object-group network** コマンド) を作成します。
  - オブジェクトを使用する代わりに、インライン アドレスを設定できます。
  - オブジェクトを使用する場合は、オブジェクトは、変換する実際のアドレスと一致する必要があります。
- ステップ 2 NAT を設定するネットワーク オブジェクトを作成または編集します。 **object network obj\_name** 各オブジェクトのコンテンツが同一である必要がある場合でも、オブジェクトはマッピングアドレスに使用する内容とは異なるオブジェクトにする必要があります。

例：

```
hostname (config)# object network my-host-obj1
```

**ステップ 3** (正しいアドレスがあるオブジェクトを編集する場合はスキップする) 変換する実際の IPv4 または IPv6 アドレスを定義します。

- **host** {*IPv4\_address* | *IPv6\_address*} : 単一のホストの IPv4 または IPv6 アドレス。たとえば、10.1.1.1 または 2001:DB8::0DB8:800:200C:417A。
- **subnet** {*IPv4\_address IPv4\_mask* | *IPv6\_address/IPv6\_prefix*} : ネットワークのアドレス。IPv4 サブネットの場合、10.0.0.0 255.0.0.0 のように、スペースの後ろにマスクを含めます。IPv6 の場合、2001:DB8:0:CD30::/60 のように、アドレスとプレフィックスを単一のユニット (スペースなし) として含めます。
- **range** *start\_address end\_address* : アドレスの範囲。IPv4 または IPv6 の範囲を指定できます。マスクまたはプレフィックスを含めないでください。

例：

```
hostname (config-network-object)# subnet 10.2.1.0 255.255.255.0
```

**ステップ 4** オブジェクト IP アドレスの **アイデンティティ NAT** を設定します。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。

```
nat [(real_ifc,mapped_ifc)] static {mapped_inline_host_ip | mapped_obj} [no-proxy-arp] [route-lookup]
```

それぞれの説明は次のとおりです。

- **インターフェイス** : (ブリッジ グループ メンバーのインターフェイスに必要) 実際のインターフェイス (*real\_ifc*) およびマッピングインターフェイス (*mapped\_ifc*) を指定します。丸カッコを含める必要があります。ルーテッドモードでは、実際のインターフェイス およびマッピングインターフェイスを指定しない場合は、すべてのインターフェイスが使用されます。また、(*any,outside*) のようにインターフェイスのいずれかまたは両方にキーワード **any** を指定することもできます。ただし、**any** はブリッジ グループのメンバインターフェイスには適用されません。
- **マッピング IP アドレス** : マッピングアドレスと実際のアドレスの両方に同じ IP アドレスを設定するようにしてください。次のいずれかを使用します。
  - *mapped\_inline\_host\_ip* : インラインホスト IP アドレス。これにより、ホストオブジェクトだけにアイデンティティ NAT が提供されます。
  - *mapped\_obj* : 実際のオブジェクトと同じ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。
- **プロキシ ARP なし** : (任意) マッピング IP アドレスに着信したパケットのプロキシ ARP をディセーブルにするには、**no-proxy-arp** を指定します。プロキシ ARP のディセーブル化が必要となる可能性がある状況については、[マッピングアドレスとルーティング](#)を参照してください。

- ルートルックアップ：（ルーテッドモードのみ、インターフェイスを指定）NAT コマンドに指定したインターフェイスを使用する代わりに、ルートルックアップを使用して出力インターフェイスを決定するには、**route-lookup** を指定します。詳細については、「[出力インターフェイスの決定](#)」を参照してください。

例：

```
hostname(config-network-object)# nat (inside,outside) static MAPPED_IPS
```

例

次の例では、インラインのマッピングアドレスを使用して、ホストアドレスを自身にマッピングします。

```
hostname(config)# object network my-host-obj1
hostname(config-network-object)# host 10.1.1.1
hostname(config-network-object)# nat (inside,outside) static 10.1.1.1
```

次の例では、ネットワーク オブジェクトを使用して、ホストアドレスを自身にマッピングします。

```
hostname(config)# object network my-host-obj1-identity
hostname(config-network-object)# host 10.1.1.1

hostname(config-network-object)# object network my-host-obj1
hostname(config-network-object)# host 10.1.1.1
hostname(config-network-object)# nat (inside,outside) static my-host-obj1-identity
```

## アイデンティティ Twice NAT の設定

この項では、Twice NAT を使用してアイデンティティ NAT ルールを設定する方法について説明します。

手順

- ステップ 1** 送信元の実際アドレス（通常、送信元のマッピングアドレスと同じオブジェクトを使用）、宛先の実際アドレス、および宛先のマッピングアドレスに、ホストまたは範囲のネットワーク オブジェクト（**object network** コマンド）、またはネットワーク オブジェクトグループ（**object-group network** コマンド）を作成します。

- すべてのアドレスに対してアイデンティティ NAT を実行する場合、送信元の実際アドレスのオブジェクトの作成をスキップして、代わりに、**nat** コマンドで **any any** キーワードを使用できます。

- ポート変換を設定した宛先のスタティック インターフェイス NAT のみを設定する場合は、宛先のマッピングアドレスに対するオブジェクトの追加をスキップして、代わりに、**nat** コマンドに **interface** キーワードを指定できます。

オブジェクトを作成する場合は、次のガイドラインを考慮してください。

- マッピングされたオブジェクトまたはグループには、ホスト、範囲、またはサブネットを含めることができます。
- 実際のオブジェクトとマッピングされた送信元オブジェクトが一致する必要があります。両方に同じオブジェクトを使用することも、同じ IP アドレスが含まれる個別のオブジェクトを作成することもできます。

**ステップ 2** (任意) 次のサービス オブジェクトを作成します。

- 送信元または宛先の実際のポート
- 送信元または宛先のマッピング ポート

サービスオブジェクトには、送信元ポートと宛先ポートの両方を含めることができますが、両方のサービスオブジェクトに送信元ポートまたは宛先ポートのいずれかを指定する必要があります。ご使用のアプリケーションが固定の送信元ポートを使用する場合（一部の DNS サーバなど）に送信元ポートおよび宛先ポートの両方を指定する必要がありますが、固定の送信元ポートはめったに使用されません。たとえば、送信元ホストのポートを変換する場合は、送信元サービスを設定します。

**ステップ 3** アイデンティティ NAT を設定します。

```
nat [(real_ifc,mapped_ifc)] [line | {after-object [line]}] source static {nw_obj nw_obj | any any}
[destination static {mapped_obj | interface [ipv6]} real_obj] [service real_src_mapped_dest_svc_obj
mapped_src_real_dest_svc_obj] [no-proxy-arp] [route-lookup] [inactive] [description desc]
```

それぞれの説明は次のとおりです。

- インターフェイス：（ブリッジグループメンバーのインターフェイスに必要）実際のインターフェイス (*real\_ifc*) およびマッピングインターフェイス (*mapped\_ifc*) を指定します。丸カッコを含める必要があります。ルーテッドモードでは、実際のインターフェイスおよびマッピングインターフェイスを指定しない場合は、すべてのインターフェイスが使用されます。また、(any,outside) のようにインターフェイスのいずれかまたは両方にキーワード **any** を指定することもできます。ただし、**any** はブリッジグループのメンバインターフェイスには適用されません。
- セクションおよび行：（任意）デフォルトでは、NAT 規則は、NAT テーブルのセクション 1 の末尾に追加されます（[NAT ルールの順序 \(5 ページ\)](#) を参照）。セクション 1 ではなく、セクション 3（ネットワーク オブジェクト NAT ルールの後ろ）にルールを追加する場合、**after-auto** キーワードを使用します。ルールは、*line* 引数を使用して、適切なセクションの任意の場所に挿入できます。
- 送信元アドレス：実際のアドレスとマッピングアドレスの両方にネットワーク オブジェクト、グループ、または **any** キーワードを指定します。

- 宛先アドレス（任意）：
  - マッピングアドレス：ネットワークオブジェクトまたはグループを指定します。ポート変換が設定されたスタティック インターフェイス NAT に限り、**interface** キーワードを指定します。**ipv6** を指定すると、インターフェイスの IPv6 アドレスが使用されます。**interface** を指定する場合、必ず **service** キーワードも設定します（この場合、サービスオブジェクトは宛先ポートだけを含む必要があります）。このオプションでは、**real\_ifc** に特定のインターフェイスを設定する必要があります。（実際のインターフェイスがブリッジグループメンバーである場合、**interface** を指定することはできません）
  - 実際のアドレス：ネットワークオブジェクトまたはグループを指定します。アイデンティティ NAT では、実際のアドレスとマッピングアドレスの両方に単に同じオブジェクトまたはグループを使用します。
- ポート：（任意）実際のサービスオブジェクトおよびマッピングされたサービスオブジェクトとともに、**service** キーワードを指定します。送信元ポート変換の場合、オブジェクトは送信元サービスを指定する必要があります。送信元ポート変換のコマンド内のサービスオブジェクトの順序は、**service real\_obj mapped\_obj** です。宛先ポート変換の場合、オブジェクトは宛先サービスを指定する必要があります。宛先ポート変換のサービスオブジェクトの順序は、**service mapped\_obj real\_obj** です。オブジェクトで送信元ポートと宛先ポートの両方を指定することはほとんどありませんが、この場合には、最初のサービスオブジェクトに実際の送信元ポート/マッピングされた宛先ポートが含まれます。2つめのサービスオブジェクトには、マッピングされた送信元ポート/実際の宛先ポートが含まれます。アイデンティティ ポート変換の場合、実際のポートとマッピング ポートの両方（コンフィギュレーションに応じて、送信元ポート、宛先ポート、またはその両方）に同じサービスオブジェクトを使用するだけです。
- プロキシ ARP なし：（任意）マッピング IP アドレスに着信したパケットのプロキシ ARP をディセーブルにするには、**no-proxy-arp** を指定します。詳細については、「[マッピングアドレスとルーティング](#)」を参照してください。
- ルートルックアップ：（任意、ルーテッドモードのみ、インターフェイスを指定）NAT コマンドに指定したインターフェイスを使用する代わりに、ルートルックアップを使用して出力インターフェイスを決定するには、**route-lookup** を指定します。詳細については、「[出力インターフェイスの決定](#)」を参照してください。
- 非アクティブ：（任意）コマンドを削除する必要なくこの規則を非アクティブにするには、**inactive** キーワードを使用します。再度アクティブ化するには、**inactive** キーワードを除いてコマンド全体を再入力します。
- 説明：（オプション）**description** キーワードを使用して、最大 200 文字の説明を入力します。

例：

```
hostname(config)# nat (inside,outside) source static MyInsNet MyInsNet
```

```
destination static Server1 Server1
```

## NAT のモニタリング

NAT をモニタするには、次のコマンドを使用します。

- **show nat**

各 NAT ルールのヒットを含む NAT の統計情報を表示します。

- **show nat pool**

割り当てられたアドレスとホスト、および割り当て回数を含む、NAT プールの統計情報を表示します。

- **show running-config nat**

NAT コンフィギュレーションを表示します。**show running-config object** を使用してオブジェクト NAT ルールを表示することはできません。修飾子を指定せずに **show running-config** コマンドを使用すると、NAT ルールが含まれるオブジェクトが 2 回表示されます。最初に基本アドレス設定とともに、その後、設定で NAT ルールとともにオブジェクトが表示されます。完全なオブジェクトは、アドレスと NAT ルールとともにユニットとして表示されません。

- **show xlate**

現在の NAT セッション情報を表示します。

## NAT の履歴

機能名	プラットフォームリリース	説明
ネットワーク オブジェクト NAT	8.3(1)	ネットワーク オブジェクトの IP アドレスの NAT を設定します。 <b>nat</b> (オブジェクトネットワークコンフィギュレーションモード)、 <b>show nat</b> 、 <b>show xlate</b> 、 <b>show nat pool</b> コマンドが導入または変更されました。
Twice NAT	8.3(1)	Twice 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。 <b>nat</b> 、 <b>show nat</b> 、 <b>show xlate</b> 、 <b>show nat pool</b> コマンドが変更または導入されました。

機能名	プラットフォームリリース	説明
アイデンティティ NAT の設定が可能なプロキシ ARP およびルート ルックアップ	8.4(2)/8.5(1)	<p>アイデンティティ NAT の以前のリリースでは、プロキシ ARP はディセーブルにされ、出力インターフェイスの決定には常にルート ルックアップが使用されていました。これらを設定することはできませんでした。8.4(2)以降、アイデンティティ NAT のデフォルト動作は他のスタティック NAT コンフィギュレーションの動作に一致するように変更されました。これにより、デフォルトでプロキシ ARP はイネーブルにされ、NAT コンフィギュレーションにより出力インターフェイスが決定されるようになりました（指定されている場合）。これらの設定をそのまま残すこともできますし、個別にイネーブルまたはディセーブルにすることもできます。通常のスタティック NAT のプロキシ ARP をディセーブルにすることもできるようになっています。</p> <p>8.3 よりも前の設定の場合、8.4(2) 以降への NAT 免除ルール（<code>nat 0 access-list</code> コマンド）の移行には、プロキシ ARP をディセーブルにするキーワード <b>no-proxy-arp</b> およびルート ルックアップを使用するキーワード <b>route-lookup</b> があります。8.3(2) および 8.4(1) への移行に使用された <b>unidirectional</b> キーワードは、移行に使用されなくなりました。8.3(1)、8.3(2)、8.4(1) から 8.4(2) にアップグレードすると、既存機能を保持するため、すべてのアイデンティティ NAT コンフィギュレーションに <b>no-proxy-arp</b> キーワードと <b>route-lookup</b> キーワードが含まれるようになっています。<b>unidirectional</b> キーワードは削除されました。</p> <p><code>nat static [no-proxy-arp] [route-lookup]</code> コマンドが変更されました。</p>

機能名	プラットフォームリリース	説明
PAT プールおよびラウンドロビンアドレス割り当て	8.4(2)/8.5(1)	<p>1つのアドレスの代わりに、PAT アドレスのプールを指定できるようになりました。また、オプションで、PAT アドレスのすべてのポートを使用してからプール内の次のアドレスを使用するのではなく、PAT アドレスのラウンドロビン割り当てをイネーブルにすることもできます。これらの機能は、1つの PAT アドレスで多数の接続を行っている場合にそれが DoS 攻撃の対象となることを防止するのに役立ちます。またこの機能により、多数の PAT アドレスを簡単に設定できます。</p> <p><b>nat dynamic [pat-pool mapped_object [round-robin]]</b> コマンドおよび <b>nat source dynamic [pat-pool mapped_object [round-robin]]</b> コマンドが変更されました。</p>
ラウンドロビン PAT プール割り当てで、既存のホストの同じ IP アドレスを使用する	8.4(3)	<p>ラウンドロビン割り当てで PAT プールを使用するときに、ホストに既存の接続がある場合、そのホストからの後続の接続では、ポートが使用可能であれば同じ PAT IP アドレスが使用されます。</p> <p>変更されたコマンドはありません。</p> <p>この機能は、8.5(1) または 8.6(1) では使用できません。</p>
PAT プールの PAT ポートのフラットな範囲	8.4(3)	<p>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 よりも下のポートには、小さい PAT プールのみがあります。</p> <p>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、PAT プールを使用するときに、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。</p> <p><b>nat dynamic [pat-pool mapped_object [flat [include-reserve]]]</b> コマンドおよび <b>nat source dynamic [pat-pool mapped_object [flat [include-reserve]]]</b> コマンドが変更されました。</p> <p>この機能は、8.5(1) または 8.6(1) では使用できません。</p>

機能名	プラットフォームリリース	説明
PAT プールの拡張 PAT	8.4(3)	<p>各 PAT IP アドレスでは、最大 65535 個のポートを使用できます。65535 個のポートで変換が不十分な場合は、PAT プールに対して拡張 PAT をイネーブルにすることができます。拡張 PAT では、変換情報の宛先アドレスとポートを含め、IP アドレスごとではなく、サービスごとに 65535 個のポートが使用されます。</p> <p><b>nat dynamic [pat-pool mapped_object [extended]]</b> コマンドおよび <b>nat source dynamic [pat-pool mapped_object [extended]]</b> コマンドが変更されました。</p> <p>この機能は、8.5(1) または 8.6(1) では使用できません。</p>

機能名	プラットフォームリリース	説明
VPN ピアのローカル IP アドレスを変換してピアの実際の IP アドレスに戻す自動 NAT ルール	8.4(3)	<p>まれに、内部ネットワークで、割り当てられたローカル IP アドレスではなく、VPN ピアの実際の IP アドレスを使用する場合があります。VPN では通常、内部ネットワークにアクセスするために、割り当てられたローカル IP アドレスがピアに指定されます。ただし、内部サーバおよびネットワーク セキュリティがピアの実際の IP アドレスに基づく場合などに、ローカル IP アドレスを変換してピアの実際のパブリック IP アドレスに戻す場合があります。</p> <p>この機能は、トンネルグループごとに 1 つのインターフェイスでイネーブルにすることができます。VPN セッションが確立または切断されると、オブジェクト NAT ルールが動的に追加および削除されます。ルールは <b>show nat</b> コマンドを使用して表示できます。</p> <p>ルーティングの問題のため、この機能が必要でない場合は、この機能の使用は推奨しません。ご使用のネットワークとの機能の互換性を確認するには、Cisco TAC にお問い合わせください。次の制限事項を確認してください。</p> <ul style="list-style-type: none"> <li>• Cisco IPsec および AnyConnect クライアントのみがサポートされます。</li> <li>• NAT ポリシーおよび VPN ポリシーが適用されるように、パブリック IP アドレスへのリターントラフィックは ASA にルーティングされる必要があります。</li> <li>• ロードバランシングはサポートされません（ルーティングの問題のため）。</li> <li>• ローミング（パブリック IP 変更）はサポートされません。</li> </ul> <p><b>nat-assigned-to-public-ip interface</b> コマンド（トンネルグループ一般属性コンフィギュレーションモード）が導入されました。</p>

機能名	プラットフォームリリース	説明
IPv6 用の NAT のサポート	9.0(1)	<p>NAT が IPv6 トラフィックをサポートするようになり、IPv4 と IPv6 の間の変換もサポートされます。IPv4 と IPv6 の間の変換は、トランスペアレント モードではサポートされません。</p> <p><b>nat</b> (global and object network configuration modes)、<b>show nat</b>、<b>show nat pool</b>、<b>show xlate</b> の各コマンドが変更されました。</p>
逆引き DNS ルックアップ用の NAT のサポート	9.0(1)	<p>NAT ルールがイネーブルにされた DNS インспекションを使用する IPv4 NAT、IPv6 NAT、および NAT64 を使用する場合、NAT は逆引き DNS ルックアップ用の DNS PTR レコードの変換をサポートするようになりました。</p>
Per-Session PAT	9.0(1)	<p>Per-session PAT 機能によって PAT のスケーラビリティが向上し、クラスタリングの場合に各メンバーユニットに独自の PAT 接続を使用できるようになります。</p> <p>Multi-Session PAT 接続は、マスターユニットに転送してマスターユニットを所有者とする必要があります。</p> <p>Per-Session PAT セッションの終了時に、ASA からリセットが送信され、即座に xlate が削除されます。このリセットによって、エンドノードは即座に接続を解放し、TIME_WAIT 状態を回避します。対照的に、Multi-Session PAT では、PAT タイムアウトが使用されます (デフォルトでは 30 秒)。「ヒットエンドラン」トラフィック、たとえば HTTP や HTTPS の場合は、Per-session 機能によって、1 アドレスでサポートされる接続率が大幅に増加することがあります。Per-session 機能を使用しない場合は、特定の IP プロトコルに対する 1 アドレスの最大接続率は約 2000/秒です。Per-session 機能を使用する場合は、特定の IP プロトコルに対する 1 アドレスの接続率は 65535/平均ライフタイムです。</p> <p>デフォルトでは、すべての TCP トラフィックおよび UDP DNS トラフィックが、Per-session PAT xlate を使用します。Multi-Session PAT を必要とするトラフィック、たとえば H.323、SIP、Skinny に対して Per-session PAT をディセーブルにするには、Per-session 拒否ルールを作成します。</p> <p><b>xlate per-session</b>、<b>show nat pool</b> の各コマンドが導入されました。</p>

機能名	プラットフォームリリース	説明
NAT ルールエンジンのトランザクションコミットモデル	9.3(1)	<p>イネーブルの場合、NAT ルールの更新はルールコンパイルの完了後に適用され、ルール照合のパフォーマンスに影響を及ぼすことはありません。</p> <p><b>asp rule-engine transactional-commit</b>、<b>show running-config asp rule-engine transactional-commit</b>、<b>clear configure asp rule-engine transactional-commit</b> の各コマンドに <b>nat</b> キーワードが追加されました。</p> <p>[Configuration] &gt; [Device Management] &gt; [Advanced] &gt; [Rule Engine] 画面に NAT が追加されました。</p>
キャリアグレード NAT の拡張	9.5(1)	<p>キャリアグレードまたは大規模 PAT では、NAT で 1 度に 1 つのポート変換を割り当てるのではなく、各ホストにポートのブロックを割り当てることができます (RFC 6888 を参照してください)。</p> <p><b>xlate block-allocation size</b> および <b>xlate block-allocation maximum-per-host</b> コマンドが追加されました。 <b>block-allocation</b> キーワードが <b>nat</b> コマンドに追加されました。</p>
SCTP に対する NAT サポート	9.5(2)	<p>スタティック ネットワーク オブジェクト NAT ルールに SCTP ポートを指定できるようになりました。スタティック Twice NAT での SCTP の使用は推奨されません。ダイナミック NAT/PAT は SCTP をサポートしていません。</p> <p><b>nat static</b> コマンドが変更されました (オブジェクト)。</p>