

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 の機能 （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 （17 ページ）
- ダイナミック PAT （27 ページ）
- スタティック NAT （51 ページ）
- アイデンティティ NAT （65 ページ）
- NAT のモニタリング （72 ページ）
- NAT の履歴 （73 ページ）

NAT の機能

NAT では、プライベート IP アドレスをパブリック IP アドレスに置き換えることで、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なります。外部にアドバタイズするパブリックアドレスをネットワーク全体で最小で1つに抑えられるため、パブリックアドレスを節約できます。

プライベート IP アドレス範囲

IP ネットワーク内のほとんどのデバイスにはプライベート IP アドレスが割り当てられています。これは、パブリック IPv4 アドレスが不足しているために、企業ネットワーク外ではプライベート IP アドレスをルーティングできないからです。RFC 1918 では、外部にアドバタイズすべきでないプライベート IP アドレス範囲が次のように規定されています。

- 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 アドレスを有効でルーティング可能なパブリックアドレスに変換することによって、プライベート IP ネットワークがインターネットにアクセスできるようにすることです。この方法では、ネットワーク全体に対して単一のパブリックアドレスのみをアドバタイズするように NAT を設定できるため、パブリック IP アドレスを節約できます。

NAT のその他の機能として次のものがあります。

- セキュリティ：内部 IP アドレスを隠蔽し、直接攻撃を抑止します。
- IP ルーティングソリューション：重複する IP アドレスを競合なしで処理します。
- 柔軟性：外部から見えるパブリックアドレスに影響を与えずに、内部 IP アドレッシング方式を変更できます。
- IPv4 と IPv6 の間の変換（ルーテッドモードのみ）：IPv4 と IPv6 の間の変換をサポートし、異なるネットワークタイプ間の相互運用性を可能にします。

（注） NAT はオプション機能です。特定のトラフィックに対して NAT が設定されていない場合、そのトラフィックは変換されませんが、通常のセキュリティポリシーの対象になります。

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通信を開始できます。ダイナミック NAT （17 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 （27 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。双方向に通信を開始できます。スタティック NAT （51 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 （65 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

Network Object 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 が提供する追加機能を必要としない場合は、Network Object NAT を使用することをお勧めします。Network Object NAT は設定が容易で、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、*Network Object 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、そ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Network ObjectNAT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 では、1 つのルールで送信元アドレスと宛先アドレスの両方を識別できます。送信元アドレスと宛先アドレスの両方を指定すると、sourceA/destinationA で sourceA/destinationB とは別の変換が行われるように指定できます。

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

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

ネットワークオブジェクト NAT と twice 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。
  - 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 NATを定義します。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ため、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 アドレスは、実アドレスとして機能します。この方法では、設定の他の部分ですでに使用されているものであっても、ネットワーク オブジェクトに簡単に NAT を追加できます。

- 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 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、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。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。
  - twice NAT：1 つのルールにより送信元と宛先の両方が変換されます。1 つのパケットは 1 つのルールにしか一致せず、以降のルールはチェックされません。オプションの宛先アドレスを設定しない場合でも、マッチングするパケットは、1 つの 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。
  - 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（Network Object 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割される 1 つのテーブルに保存されます。最初にセクション 1 のルール、次にセクション 2、最後にセクション 3 というように、一致が見つかるまで順番に適用されます。たとえば、セクション 1 で一致が見つかった場合、セクション 2 とセクション 3 は評価されません。次の表に、各セクション内のルールの順序を示します。



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

表 *1 : NAT* ルール テーブル

テーブルのセクション	ルール タイプ	セクション内のルールの順序
セクション 1	twice 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、twice NAT ルールはセクション 1 に追加されます。 「固有のルールを前に」とは、次のことを意味します。 • 静的ルールは動的ルールの前に配置する必要があります。 • 宛先変換を含むルールは、送信元変換のみのルールの前に配置する必要があります。 送信元アドレスまたは宛先アドレスに基づいて複数のルールが適用される可能性がある重複するルールを排除できない場合は、これらの推奨事項に従うように特に注意してください。 上記の推奨事項に従わない場合は、マッピングされたアドレスに対して、正しい NAT ルールに一致する正確なルートが設定されるようにします。
セクション 2	ネットワークオブジェクト NAT	セクション 1 で一致が見つからない場合、セクション 2 のルールが次の順序で適用されます。 **1.** 静的ルール **2.** ダイナミックルール **各ルール タイプでは、次の順序ガイドラインが使用されます。** **1.** 実際の IP アドレスの数量：小から大の順。たとえば、アドレスが 1 個のオブジェクトは、アドレスが 10 個のオブジェクトよりも先に評価されます。 **2.** 数量が同じ場合には、IP アドレス番号（最小から最大まで）が使用されます。たとえば、10.1.1.0 は、11.1.1.0 よりも先に評価されます。 **3.** 同じ IP アドレスが使用される場合、ネットワーク オブジェクトの名前がアルファベット順で使用されます。たとえば、abracadabra は catwoman よりも先に評価されます。

テーブルのセクション	ルール タイプ	セクション内のルールの順序
セクション 3	twice 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。また、このセクションに固有のルールは、一般的なルールよりも前に来るようにする必要があります。そうでなければ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、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（静的）
- 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（静的）
- 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）

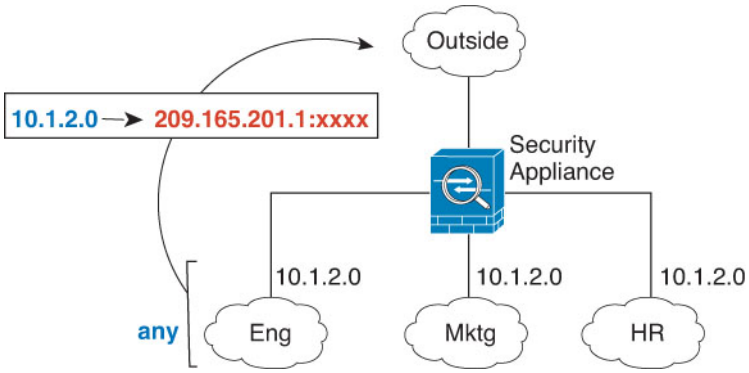
NAT インターフェイス

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。実際のアドレスに任意のインターフェイスを指定し、マッピングインターフェイスに特定のインターフェイスを指定することもでき、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 インターフェイスには適用されません。「任意」のインターフェイスを指定すると、すべてのブリッジ グループ メンバー インターフェイスが除外されます。そのため、ブリッジ グループ メンバーに NAT を適用するには、メンバー インターフェイスを指定する必要があります。この結果、1 つのインターフェイスのみが異なる同様のルールが多数作成されることになります。ブリッジ仮想インターフェイス（BVI）自体に NAT を設定することはできず、メンバー インターフェイスにのみ NAT を設定できます。

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。

IPv6 NAT のガイドライン

NAT では、IPv6 のサポートに次のガイドラインと制限が伴います。

- 標準のルーテッド モードのインターフェイスの場合は、IPv4 と IPv6 との間でも変換できます。
- 同じブリッジ グループのメンバーであるインターフェイスでは、IPv4 と IPv6 の間の変換はできません。2 つの IPv6 ネットワーク間または 2 つの IPv4 ネットワーク間でのみ変換できます。この制限は、インターフェイスが異なるブリッジグループのメンバーである場合、またはブリッジ グループのメンバーと標準的なルーテッド インターフェイスの間には該当しません。
- 同じブリッジグループ内のインターフェイス間で変換する場合は、IPv6 対応のダイナミック PAT（NAT66）は使用できません。この制限は、インターフェイスが異なるブリッジグループのメンバーである場合、またはブリッジグループのメンバーと標準的なルーテッド インターフェイスの間には該当しません。
- スタティック NAT の場合は、/64 までの IPv6 サブネットを指定できます。これよりも大きいサブネットはサポートされません。
- FTP を NAT46 とともに使用する場合は、IPv4 FTP クライアントが IPv6 FTP サーバに接続するときに、クライアントは拡張パッシブ モード（EPSV）または拡張ポート モード（EPRT）を使用する必要があります。PASV コマンドおよび PORT コマンドは IPv6 ではサポートされません。

IPv6 NAT のベストプラクティス

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

- NAT66（IPv6-to-IPv6）：スタティック NAT を使用することを推奨します。ダイナミック NAT または PAT を使用できますが、IPv6 アドレスは大量にあるため、ダイナミック NAT を使用する必要がありません。リターン トラフィックを許可しない場合は、スタティック NAT ルールを単一方向にできます （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

- NAT ルールは、デバイスを通過する通信にのみ適用され、RADIUS 認証など、デバイスによって開始される通信には適用されません。
- ブリッジ グループのメンバーであるインターフェイスの場合は、メンバー インターフェイス用の NAT ルールを記述します。ブリッジ仮想インターフェイス（BVI）自体に対する NAT ルールは記述できません。
- サイト間 VPN で使用される仮想トンネルインターフェイス（VTI）の NAT ルールは作成できません。VTI の送信元インターフェイスのルールを作成すると、NAT は VPN トンネルに適用されません。VTI でトンネリングされた VPN トラフィックに適用される NAT ルールを作成するには、インターフェイスとして [any] を使用する必要があります。インターフェイス名を明示的に指定することはできません。
- （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。
- 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、レスポンダはセキュリティ アソシエーション（SA）を開始できません。
- NAT コンフィギュレーションを変更したときに、既存の変換がタイムアウトするまで待たずに新しい NAT コンフィギュレーションを使用できるようにするには、デバイス CLI

で **clear xlate** コマンドを使用して変換テーブルを消去します。ただし、変換テーブルを消去すると、変換を使用している現在の接続がすべて切断されます。

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

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

- SCTP トラフィックを変換する場合は、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、そのような設定は推奨されません。
- 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。
- （twice 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」通信の定義（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 インターフェイスのアドレスによって宛先も IPv4 であることが示されるため、**any** は「任意の IPv4 トラフィック」を意味します。
- 同じマッピング オブジェクトやグループを複数の NAT ルールで使用できます。
- マッピング IP アドレス プールに、次のアドレスを含めることはできません。
  - マッピング インターフェイスの IP アドレス。ルールに「any」インターフェイスを指定すると、すべてのインターフェイスの IP アドレスが拒否されます。インターフェイス PAT（ルーテッドモードのみ）の場合は、インターフェイスアドレスの代わりにインターフェイス名を指定します。
  - フェイルオーバー 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。
- 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 ルールの送信元アドレスとリモートアクセス VPN アドレスプールの重複アドレスは使用できません。
- NAT や PAT に伴うアプリケーション検査の制限については、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。
- アイデンティティ NAT のデフォルト動作で、プロキシ ARP は有効になっており、他の静的 NAT ルールと一致します。必要に応じてプロキシ ARP を無効にできます。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。
- NFS サーバーへの接続に使用される Sun RPC トラフィックで PAT を使用する場合、PAT の対象となるポートが 1024 よりも大きいと、NFS サーバーが接続を拒否する可能性があることに注意してください。NFS サーバーのデフォルト設定では、1024 よりも大きいポートからの接続は拒否されます。エラーメッセージは、通常「Permission Denied（権限が拒否されました）」です。下位のポートが利用できない場合に「フラット範囲」オプションを使用して大きなポート番号を使用すると、1024 よりも大きいポートのマッピングが発生する可能性があります（特にフラット範囲に下位のポートを含めるオプションを選択していない場合）。PAT プールのポート範囲に予約済みポート（1 ー 1023）を含めるオプションを選択しない場合、1024 よりも大きいポートのマッピングが発生します。この問題を回避するには、すべてのポート番号を許可するように NFS サーバーの構成を変更します。
- NAT は、通過トラフィックにのみ適用されます。システムによって生成された通信は、NAT の対象外です。
- 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。このオプションは、[Configurations] > [Device Management] > [Advanced] > [Rule Engine] の下にあります。

- ネットワークオブジェクトまたはグループの PAT プールには、大文字と小文字を組み合わせた名前を付けないでください。
- 単方向オプションは主にテスト目的に有効であり、すべてのプロトコルで機能するとは限りません。たとえば、SIP では、NAT を使用して SIP ヘッダーを変換するためにプロトコルインスペクションが必要ですが、変換を単方向にするとこの処理は行われません。
- Protocol Independent Multicast（PIM）レジスタの内部ペイロードで NAT を使用することはできません。
- （twice NAT）デュアル ISP インターフェイス セットアップ（ルーティング設定でサービス レベルアグリーメントを使用するプライマリインターフェイスとバックアップインターフェイス）の NAT ルールを作成する場合は、ルールで宛先基準を指定しないでください。プライマリインターフェイスのルールがバックアップインターフェイスのルールよりも前にあることを確認してください。これにより、デバイスは、プライマリ ISP が利用できない場合に、現在のルーティング状態に基づいて正しい NAT 宛先インターフェイスを選択できます。宛先オブジェクトを指定すると、NAT ルールは、指定しない場合には重複するルールのプライマリインターフェイスを常に選択します。
- インターフェイスに定義された NAT ルールと一致しないトラフィックについて ASP ドロップ理由 nat-no-xlate-to-pat-pool が示される場合は、影響を受けるトラフィックのアイデンティティ NAT ルールを設定して、トラフィックが変換されずに通過できるようにします。
- GRE トンネルエンドポイントの NAT を設定する場合は、エンドポイントでキープアライブを無効にする必要があります。無効にしないと、トンネルを確立できません。エンドポイントは、キープアライブを元のアドレスに送信します。
- DHCP と BOOTP はポート UDP/67 ～ 68 を共有します。BOOTP は廃止されているため、DHCP も実行している場合、BOOTP ポートの NAT ルールを作成するとポート割り当ての問題が発生する可能性があります。ネットワークセグメント間で DHCP 要求を送信する場合は、代わりに DHCP リレーを使用することを検討してください。
- まれに、既存の変換（xlate）を使用した戻り通信（サーバからクライアント）が、[接続イベント（Connection Events）] に新しいフローとして記録されることがあります。これは、クライアントが接続をすでに終了しており、サーバーが別のパケットを送信すると、接続の終了と xlate の削除の間の短い間隔でデバイスに到達します（多くの場合、アプリケーションの動作または TCP スタックのクリーンアップが原因）。デバイスは接続を削除した後にのみ xlate を削除するため、xlate がまだ存在している間にサーバーパケットが届く可能性があります。有効な接続エントリが見つからない場合、デバイスは一致するアクセス コントロール ポリシーの規則に基づいて別の接続イベントをログに記録します。

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。

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 （10 ページ）を参照してください。
- ネットワークオブジェクトまたはグループの PAT プールには、大文字と小文字を組み合わせた名前を付けないでください。
- 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。オブジェクトにホストアドレスが1つしか含まれていない場合は、それが PAT に使用されます。
- 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。

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 （10 ページ）を参照してください。
- ネットワークオブジェクトまたはグループの PAT プールには、大文字と小文字を組み合わせた名前を付けないでください。
- 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。オブジェクトにホストアドレスが1つしか含まれていない場合は、それが PAT に使用されます。

- 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**

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 ポートの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 サーバーなど）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。

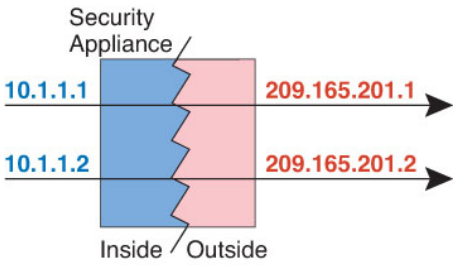
ダイナミック NAT について

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。リモートホストからの接続が成功すると、接続のアイドルタイマーがリセットされます。

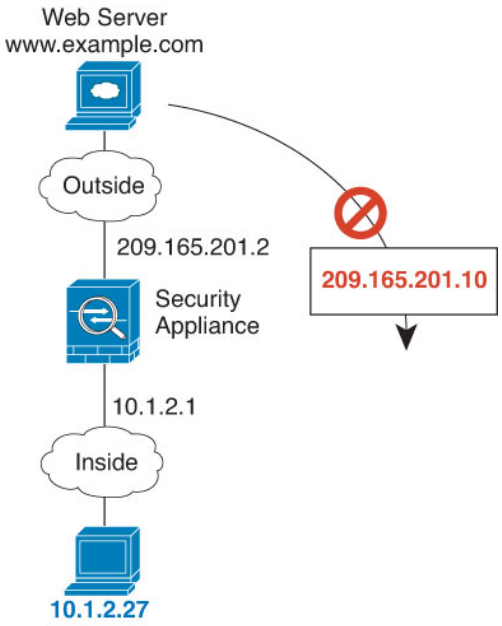
次の図に、一般的なダイナミック NAT のシナリオを示します。実際のホストだけが NAT セッションを作成でき、応答通信が許可されます。

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。

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

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

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

ダイナミック 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 新規または既存のネットワーク オブジェクトに NAT を追加します。

- 新しいネットワーク オブジェクトを追加するには、[Configuration] > [Firewall] > [NAT Rules] を選択し、[Add] > [Add Network Object NAT Rule] をクリックします。
- 既存のネットワーク オブジェクトに NAT を追加するには、[Configuration] > [Firewall] > [Objects] > [Network Objects/Groups] を選択し、ネットワーク オブジェクトを編集します。

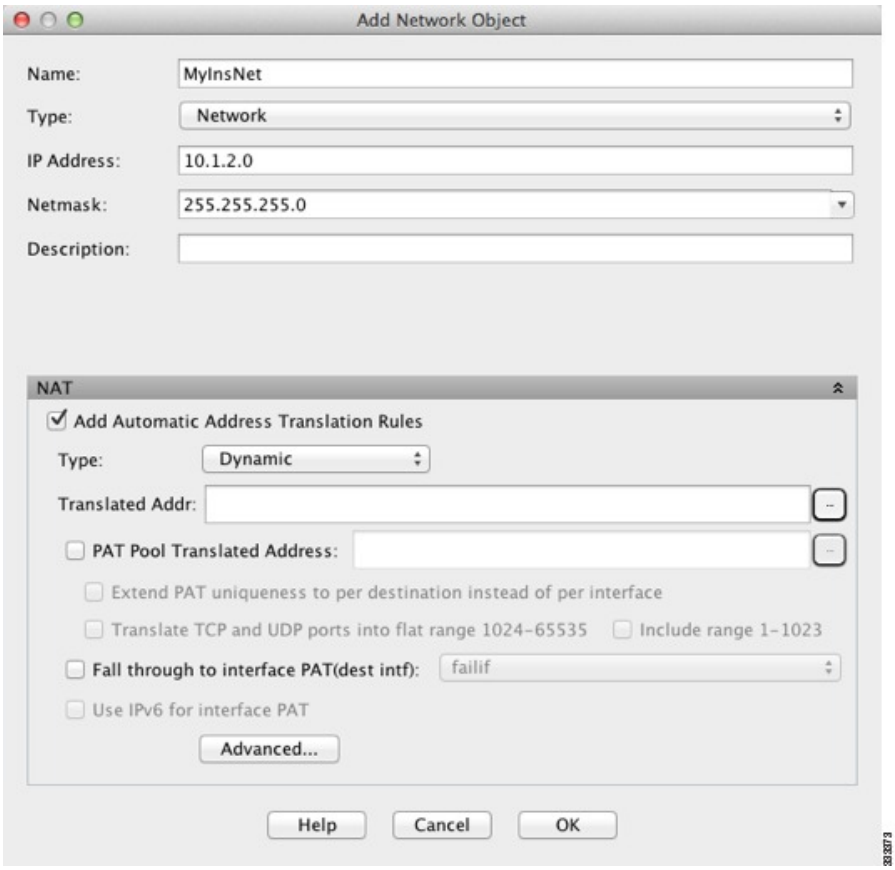
ステップ 2 新しいオブジェクトの場合は、次のフィールドに値を入力します。

a) [Name]：オブジェクト名。a ～ z、A ～ Z、0 ～ 9、ピリオド、ハイフン、カンマ、またはアンダースコアの文字を使用してください。名前は 64 文字以下にする必要があります。

b) [Type]：ホスト、ネットワーク、または範囲。

c) [IP Addresses]：IPv4 または IPv6 アドレス。ホストの場合は単一のアドレスを、範囲の場合は開始アドレスと終了アドレスを、サブネットの場合は IPv4 ネットワーク アドレスおよびマスク（たとえば、10.100.10.0 255.255.255.0）または IPv6 アドレスおよびプレフィックス長（たとえば、2001:DB8:0:CD30::/60）を入力します。

ステップ 3 [NAT] セクションが表示されていない場合は、[NAT] をクリックしてセクションを展開します。



ステップ 4 [Add Automatic Translation Rules] チェックボックスをオンにします。

ステップ 5 [Type] ドロップダウン リストから、[Dynamic] を選択します。

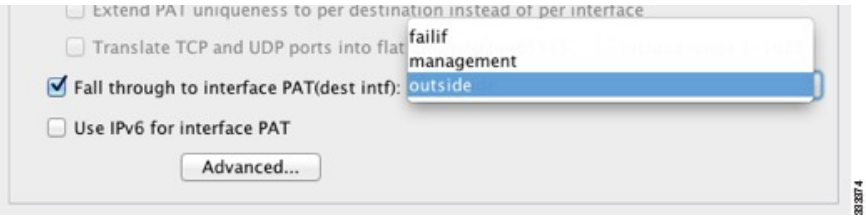
ステップ 6 [Translated Addr] フィールドの右の参照ボタンをクリックし、マッピング アドレスが含まれるネットワーク オブジェクトまたはネットワーク オブジェクト グループを選択します。

必要に応じて新しいオブジェクトを作成できます。

オブジェクトまたはグループは、サブネットを含むことはできません。IPv4 アドレスと IPv6 アドレスの両方をグループに入れることはできません。1 つのタイプだけが含まれている必要があります。

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。オブジェクトにホストアドレスが 1 つしか含まれていない場合は、それが PAT に使用されます。

ステップ 7 （任意、マッピングされたインターフェイスが非ブリッジ グループ メンバーのときのみ）他のマッピング アドレスがすべて割り当て済みの場合にインターフェイス IP アドレスをバックアップ方法として使用するには、[Fall through to interface PAT (dest intf)] チェック ボックスをオンにして、インターフェイスをドロップダウン リストから選択します。インターフェイスの IPv6 アドレスを使用するには、[Use IPv6 for interface PAT] チェック ボックスをオンにします。



ステップ 8 （任意）[Advanced] をクリックし、[Advanced NAT Settings] ダイアログボックスで次のオプションを設定して [OK] をクリックします。

- [Translate DNS replies for rule]：DNS 応答内の IP アドレスを変換します。DNS インスペク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。
- （ブリッジ グループ メンバーのインターフェイスに必要）[Interface]：この NAT ルールを適用する実際のインターフェイス（**送信元**）およびマッピング インターフェイス（**宛先**）を指定します。デフォルトでは、ルールはブリッジ グループ メンバーを除くすべてのインターフェイスに適用されます。

ステップ 9 [OK]、続いて [Apply] をクリックします。

ダイナミック Twice NAT の設定

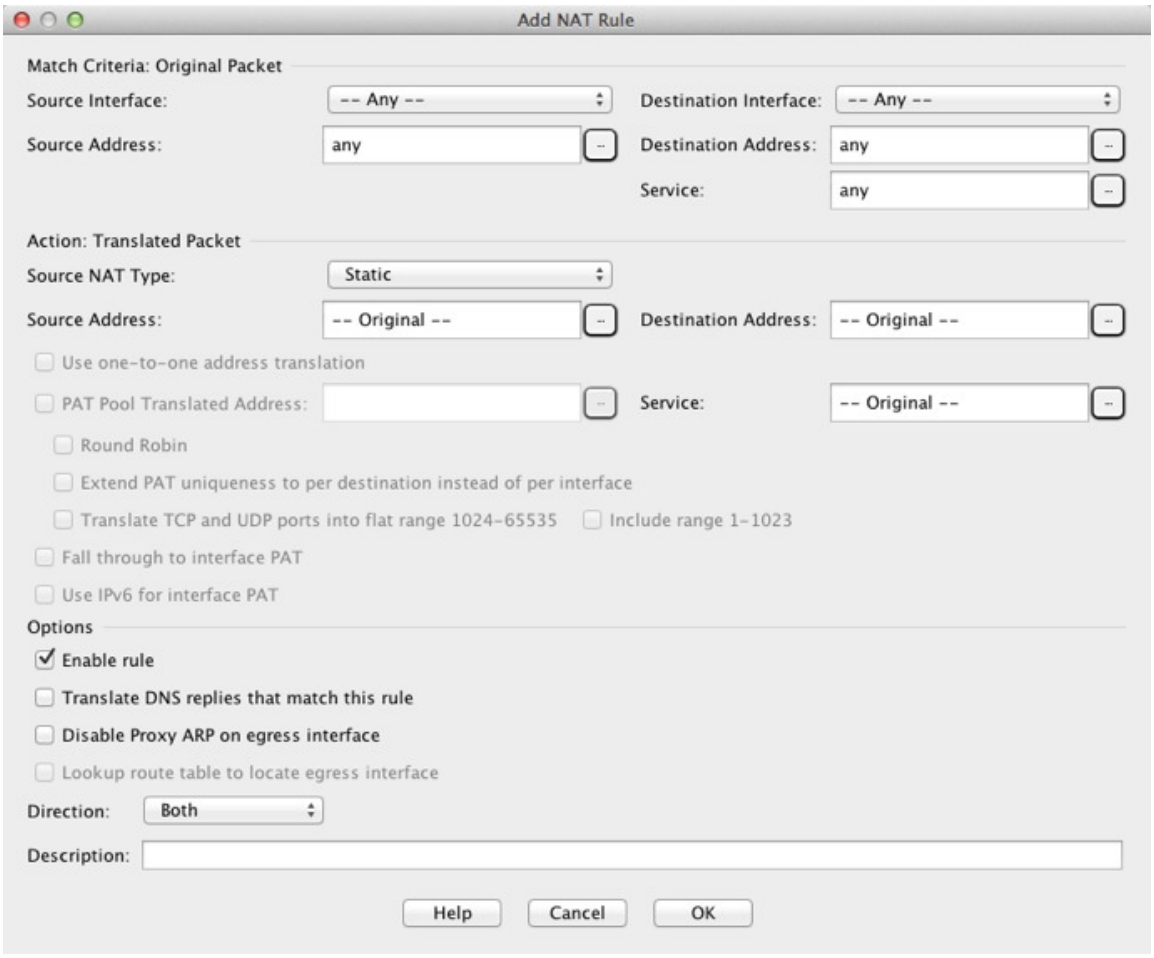
この項では、ダイナミック NAT の Twice NAT を設定する方法について説明します。

手順

ステップ 1 **[Configuration]** > **[Firewall]** > **[NAT Rules]** を選択して、次のいずれかを実行します。

- [Add] または [Add] > [Add NAT Rule Before Network Object NAT Rules] をクリックします。
- [Add] > [Add NAT Rule After Network Object NAT Rules] をクリックします。
- Twice NAT ルールを選択して [Edit] をクリックします。

[Add NAT Rule] ダイアログボックスが表示されます。

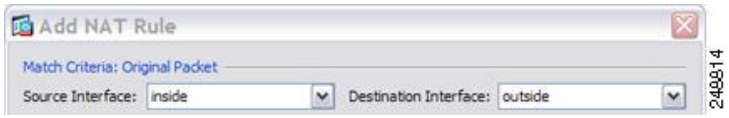


ステップ 2 （ブリッジ グループ メンバーのインターフェイスに必要）送信元インターフェイスおよび宛先インターフェイスを設定します。

ルーテッドモードでは、デフォルトは送信元と宛先の両方のインターフェイスです。いずれかまたは両方のオプションに、特定のインターフェイスを選択できます。ただし、ブリッジ グループ メンバーのインターフェイスにルールを記述するときに、インターフェイスを選択する必要があります。「any」にはこれらのインターフェイスが含まれていません。

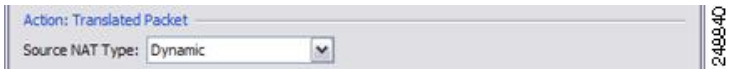
a) [Match Criteria: Original Packet] > [Source Interface] ドロップダウンリストから、送信元インターフェイスを選択します。

b) [Match Criteria: Original Packet] > [Destination Interface] ドロップダウンリストから、宛先インターフェイスを選択します。

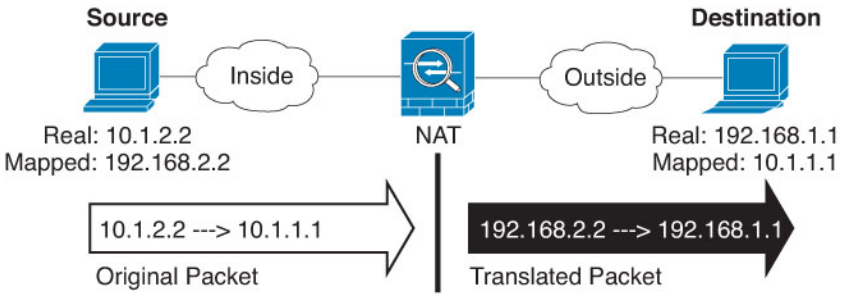


ステップ 3 **[Action: Translated Packet]** > **[Source NAT Type]** ドロップダウンリストから、[Dynamic] を選択します。

この設定は送信元アドレスにのみ適用されます。宛先の変換は常にスタティックになります。



ステップ 4 パケットの元の IPv4 または IPv6 のアドレス、つまり、送信元インターフェイス ネットワーク上に出現するときのパケットのアドレス（実際の送信元アドレスとマッピング宛先アドレス）を識別します。元のパケットと変換されたパケットの例については、次の図を参照してください。



a) [Match Criteria: Original Packet] > [Source Address] について、参照ボタンをクリックして既存のネットワーク オブジェクトまたはグループを選択するか、[Browse Original Source Address] ダイアログボックスから新しい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。デフォルトは **any** です。

b) （任意）[Match Criteria: Original Packet] > [Destination Address] について、参照ボタンをクリックして既存のネットワーク オブジェクト、グループ、またはインターフェイスを選択するか、[Browse Original Destination Address] ダイアログボックスから新しい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。

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。

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、[Browse] ダイアログボックスからインターフェイスを選択します。サービス変換も必ず設定します。このオプションでは、[Source Interface] 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 （51 ページ）」を参照してください。

ステップ 5 パケットの変換された IPv4 または IPv6 のアドレス、つまり、宛先インターフェイス ネットワーク上に出現するときのパケットのアドレス（マッピング送信元アドレスと実際の宛先アドレス）を識別します。必要に応じて、IPv4 と IPv6 の間で変換できます。

a) [Action: Translated Packet] > [Source Address] について、参照ボタンをクリックして既存のネットワーク オブジェクトまたはグループを選択するか、[Browse Translated Source Address] ダイアログボックスから新しいオブジェクトまたはグループを作成します。

ダイナミック NAT では、通常、大きい送信元アドレスのグループが小さいグループにマッピングされます。

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。オブジェクトにホストアドレスが 1 つしか含まれていない場合は、それが PAT に使用されます。

（注） オブジェクトまたはグループは、サブネットを含むことはできません。

b) [Action: Translated Packet] > [Destination Address] について、参照ボタンをクリックして既存のネットワーク オブジェクトまたはグループを選択するか、[Browse Translated Destination Address] ダイアログボックスから新しいオブジェクトまたはグループを作成します。

宛先アドレスのアイデンティティ 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。

宛先アドレスを変換する場合、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 （51 ページ）を参照してください。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（10 ページ）を参照してください。

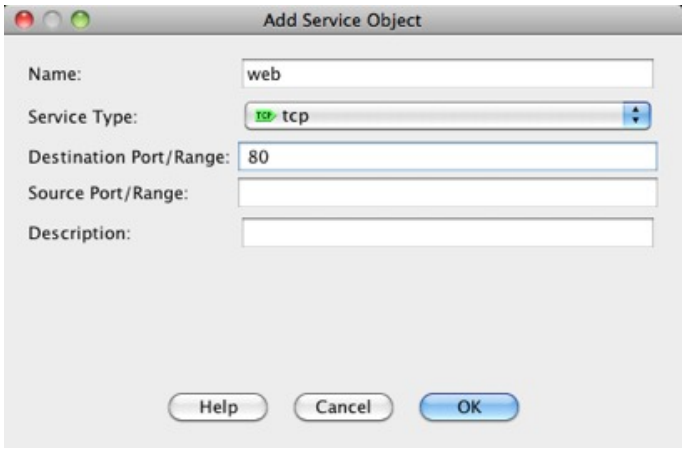
ステップ 6 （任意）サービス変換の宛先サービス ポートを識別します。

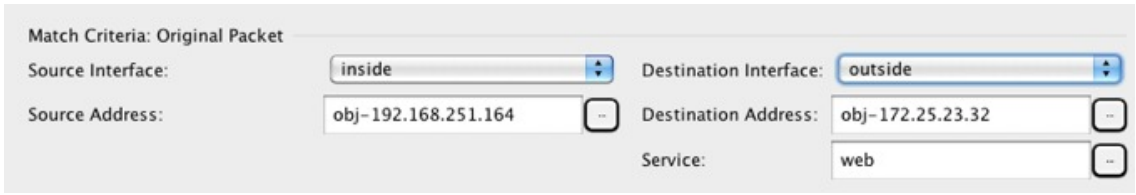
- 元のパケット ポート（マッピング宛先ポート）を識別します。[Match Criteria: Original Packet] > [Service] について、参照ボタンをクリックしてTCP ポートまたは UDP ポートを指定する既存のサービス オブジェクトを選択するか、[Browse Original Service] ダイアログボックスから新しいオブジェクトを作成します。
- 変換されたパケット ポート（実際の宛先ポート）を識別します。[Action: Original Packet] > [Service] について、参照ボタンをクリックしてTCP ポートまたは UDP ポートを指定する既存のサービス オブジェクトを選択するか、[Browse Translated Service] ダイアログボックスから新しいオブジェクトを作成します。

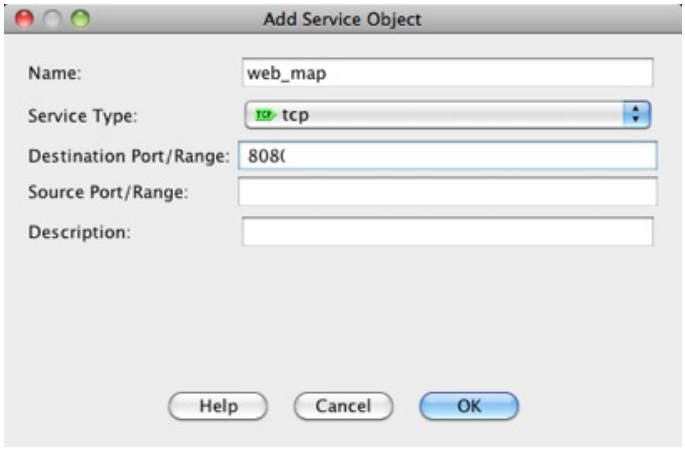
ダイナミック NAT では、ポート変換はサポートされません。しかし、宛先変換は常にスタティックなので、宛先ポートに対してポート変換を実行できます。サービス オブジェクトには送信元ポートと宛先ポートの両方を含めることができますが、この場合は、宛先ポートだけが使用されます。送信元ポートを指定した場合、無視されます。NAT では、TCP または UDP のみがサポートされます。ポートを変換する場合、実際のサービス オブジェクトのプロトコルとマッピング サービス オブジェクトのプロトコルの両方が同じになるようにします（両方とも TCP または両方とも UDP）。アイデンティティ NAT では、実際のポ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。「not equal（等しくない）」（**!=**）演算子はサポートされていません。

次に例を示します。





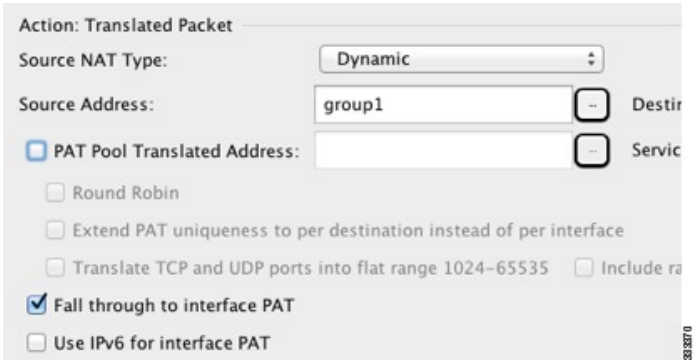




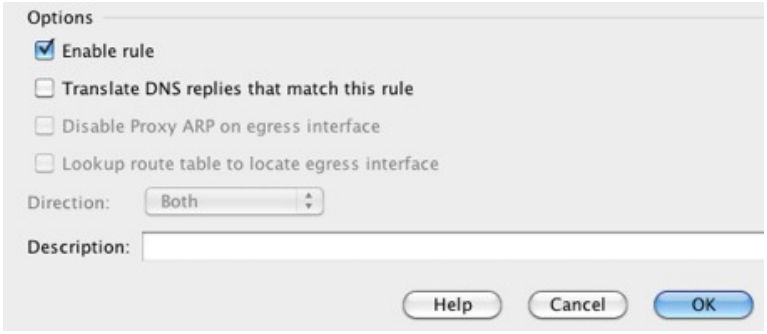
ステップ 7 （任意、マッピングされたインターフェイスが非ブリッジ グループ メンバーのときのみ）他のマッピングされた送信元アドレスがすでに割り当てられている場合に、インターフェイス IP アドレスをバックアップの手段として使用するには、[Fall through to interface PAT] チェック

ボックスをオンにします。IPv6 インターフェイス アドレスを使用するには、[Use IPv6 for interface PAT] チェックボックスもオンにします。

宛先インターフェイス IP アドレスが使用されます。このオプションは、特定の [Destination Interface] を設定する場合にだけ使用できます。



ステップ 8 （任意）[Options] 領域で NAT オプションを設定します。



- [Enable rule]：この NAT ルールをイネーブルにします。このルールはデフォルトでイネーブルになっています。
- （送信元専用ルールの場合）[Translate DNS replies that match this rule]：DNS 応答内の DNS A レコードを書き換えます。DNS インスペク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 修正は設定できません。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。
- [Description]：ルールに関する説明を 200 文字以内で追加します。

ステップ 9 [OK] をクリックし、続いて [Apply] をクリックします。

ダイナミック PAT

次のトピックでは、ダイナミック PAT について説明します。

ダイナミック PAT について

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

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

次の図は、ダイナミック PAT の一般的なシナリオを示します。実際のホストだけが NAT セッションを作成でき、応答通信が許可されます。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、ポート変換も期限切れになります。マルチセッション PAT では、PAT のタイムアウト（デフォルトでは 30 秒）が使用されます。セッションごとの PAT では、xlate がただちに削除されます。

（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。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、この通信はサーバで 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ガイドライン

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

PAT プールの場合

- ポートは、1024 ー 65535 の範囲の使用可能なポートにマッピングされます。必要に応じ、1024 番未満の予約ポートを含めて、ポート範囲全体を変換に使用することもできます。

  クラスタで動作する場合、アドレスごとに 512 個のポートのブロックがクラスタのメンバーに割り当てられ、これらのポートブロック内でマッピングが行われます。ブロック割り当ても有効にした場合は、ブロック割り当てサイズに従ってポートが分配されます。このデフォルトも 512 です。クラスターユニットの制限（クラスターのサイズ）を変更する場合は、xlate をクリアするか、デバイスを再起動して、PAT プールをクラスターユニットに適切に再割り当てできるようにしてください。

- PAT プールに対してブロック割り当てを有効にする場合、ポートブロックは 1024 ～ 65535 の範囲でのみ割り当てられます。そのため、アプリケーションが小さいポート番号（1 ～ 1023）を必要とするときは、機能しない可能性があります。たとえば、ポート 22（SSH）を要求するアプリケーションは、1024 ～ 65535 の範囲内で、ホストに割り当てられたブロック内の、マッピングされたポートを取得します。

- 同じ PAT プール オブジェクトを 2 つの異なるルールの中で使用する場合は、必ず同じオプションを各ルールに指定してください。たとえば、1 つのルールで拡張 PAT が指定される場合は、もう一方のルールでも拡張 PAT が指定される必要があります。

- ホストに既存の接続がある場合は、そのホストからの以降の接続は同じ PAT IP アドレスを使用します。使用可能なポートがない場合、接続が妨げられる可能性があります。この問題を回避するには、ラウンドロビンオプションを使用します。

- パフォーマンスを最大にするには、PAT プール内の IP アドレスの数を 10,000 に制限します。

PAT プールの拡張 PAT の場合

- 多くのアプリケーション インスペクションでは、拡張 PAT はサポートされていません。サポート対象外のインスペクションの完全な一覧については、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 ルールに対して拡張 PAT をイネーブルにする場合、PAT プールのアドレスを、ポート トランスレーション ルールを持つ別のスタティック NAT の PAT アドレスとしても使用することはできません。たとえば、PAT プールに 10.1.1.1 が含まれている場合、PAT アドレスとして 10.1.1.1 を使用する、ポート トランスレーション ルールを持つスタティック NAT は作成できません。
- PAT プールを使用し、フォールバックのインターフェイスを指定する場合、拡張 PAT を使用できません。
- ICE または TURN を使用する VoIP 配置では、拡張 PAT を使用しないでください。ICE および TURN は、すべての宛先に対して同じであるために PAT バインディングに依存しています。
- クラスタ内のユニットで拡張 PAT を使用することはできません。
- 拡張 PAT は、デバイスでのメモリ使用率が増加します。

PAT プールのラウンド ロビン方式の場合

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

ダイナミック ネットワーク オブジェクト PAT（隠蔽）の設定

この項では、PAT プールの代わりに変換のための単一のアドレスを使用するダイナミック PAT（隠蔽）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 新規または既存のネットワーク オブジェクトに NAT を追加します。

- 新しいネットワーク オブジェクトを追加するには、[Configuration] > [Firewall] > [NAT Rules] を選択し、[Add] > [Add Network Object NAT Rule] をクリックします。

- 既存のネットワーク オブジェクトに NAT を追加するには、[Configuration] > [Firewall] > [Objects] > [Network Objects/Groups] を選択し、ネットワーク オブジェクトを編集します。

ステップ 2 新しいオブジェクトの場合は、次のフィールドに値を入力します。

a) [Name]：オブジェクト名。a ～ z、A ～ Z、0 ～ 9、ピリオド、ハイフン、カンマ、またはアンダースコアの文字を使用してください。名前は 64 文字以下にする必要があります。

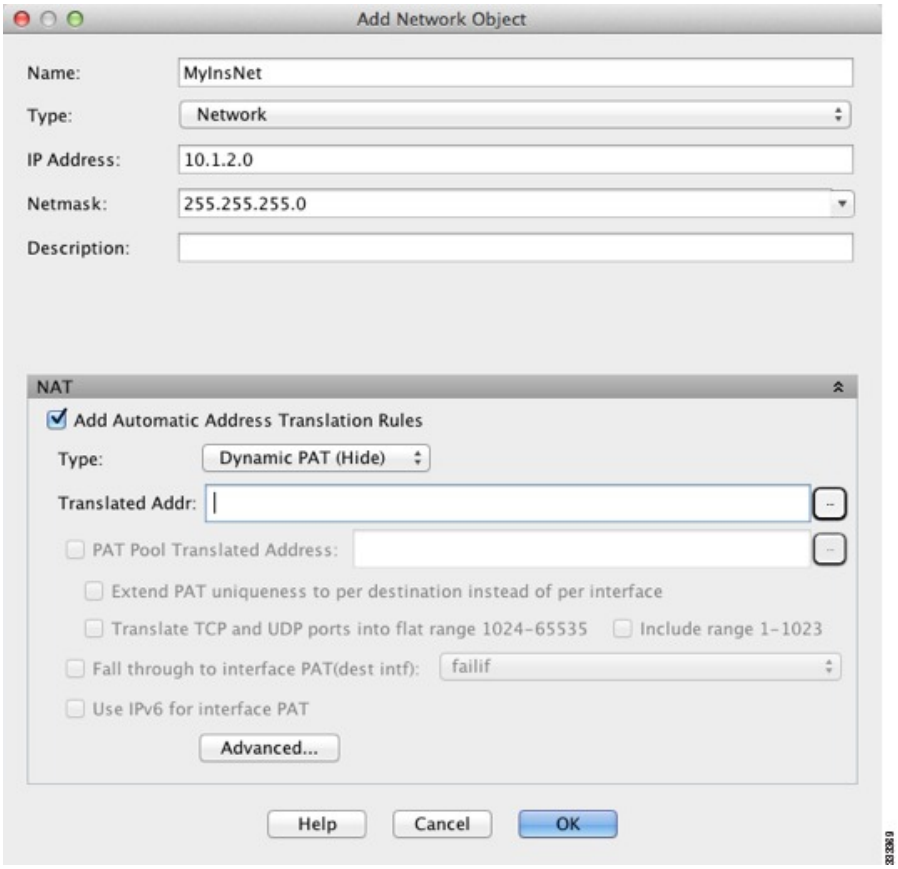
b) [Type]：ホスト、ネットワーク、または範囲。

c) [IP Addresses]：IPv4 または IPv6 アドレス。ホストの場合は単一のアドレスを、範囲の場合は開始アドレスと終了アドレスを、サブネットの場合は IPv4 ネットワーク アドレスおよびマスク（たとえば、10.100.10.0 255.255.255.0）または IPv6 アドレスおよびプレフィックス長（たとえば、2001:DB8:0:CD30::/60）を入力します。

ステップ 3 [NAT] セクションが表示されていない場合は、[NAT] をクリックしてセクションを展開します。

ステップ 4 [Add Automatic Translation Rules] チェックボックスをオンにします。

ステップ 5 [Type] ドロップダウン リストから、[Dynamic PAT (Hide)] を選択します。



ステップ 6 マッピング アドレスを 1 つだけ指定します。[Translated Addr] フィールドで、次のいずれかを行ってマッピング IP アドレスを指定します。

- ホスト IP アドレスを入力します。

- 参照ボタンをクリックし、ホスト ネットワーク オブジェクトを選択します（または新しいホスト ネットワーク オブジェクトを作成します）。
- （非ブリッジ グループ メンバーのインターフェイスのみ）インターフェイス名を入力するか、または参照ボタンをクリックし、[Browse Translated Addr] ダイアログボックスでインターフェイスを選択します。



インターフェイス名を指定する場合は、インターフェイス *PAT* をイネーブルにしてください。このときに指定したインターフェイス 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 インターフェイス アドレスを使用するには、[Use IPv6 for interface PAT] チェック ボックスもオンにする必要があります。インターフェイス PAT によって、NAT ルールはブリッジ グループのメンバーになることがない指定されたマッピング インターフェイスにのみ適用されます（インターフェイス PAT を使用しない場合、ルールはデフォルトですべてのインターフェイスに適用されます）。トランスペアレント モードでは、インターフェイスを指定することはできません。

ステップ 7 （任意）[Advanced] をクリックし、[Advanced NAT Settings] ダイアログボックスで次のオプションを設定して [OK] をクリックします。

- （ブリッジ グループ メンバーのインターフェイスに必要）[Interface]：この NAT ルールを適用する実際のインターフェイス（**送信元**）およびマッピング インターフェイス（**宛先**）を指定します。デフォルトでは、ルールはブリッジ グループ メンバーを除くすべてのインターフェイスに適用されます。

ステップ 8 [OK]、続いて [Apply] をクリックします。

PAT プールを使用するダイナミック ネットワーク オブジェクト PAT の設定

この項では、PAT プールを使用するダイナミック 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 新規または既存のネットワーク オブジェクトに NAT を追加します。

- 新しいネットワーク オブジェクト NAT ルールを追加するには、**[Configuration]** > **[Firewall]** > **[NAT Rules]** を選択し、**[Add]** > **[Add Network Object NAT Rule]** をクリックします。

- 既存のネットワーク オブジェクトに NAT を追加するには、**[Configuration]** > **[Firewall]** > **[Objects]** > **[Network Objects/Groups]** を選択し、ネットワーク オブジェクトを編集します。

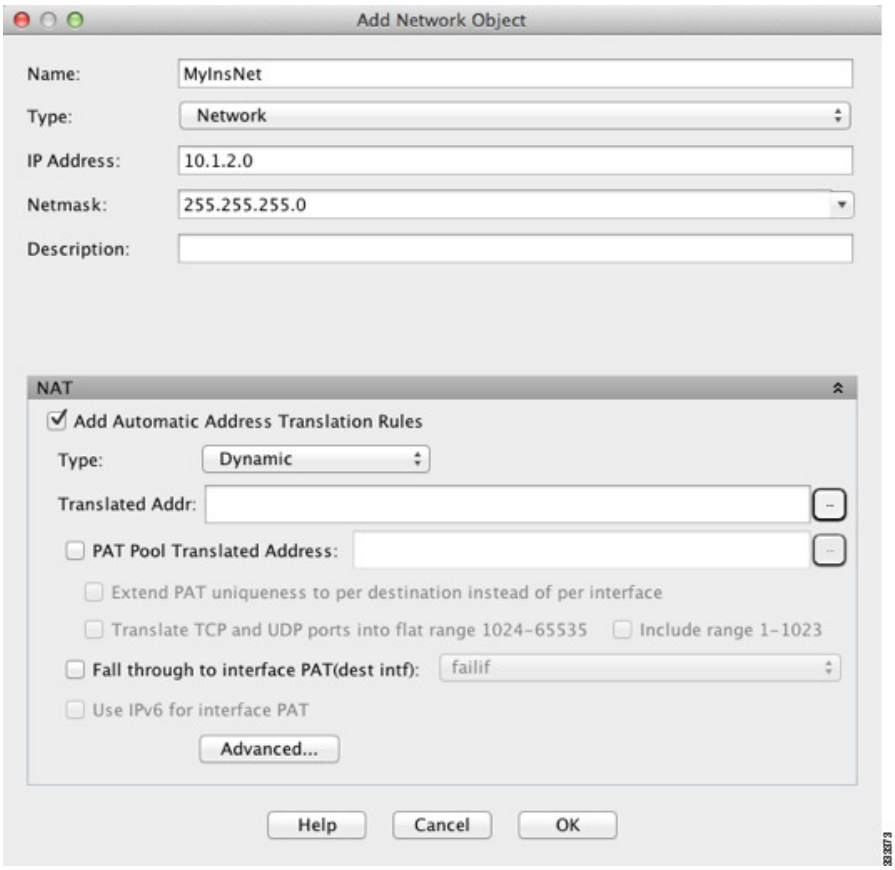
ステップ 2 新しいオブジェクトの場合は、次のフィールドに値を入力します。

a) [Name]：オブジェクト名。a ～ z、A ～ Z、0 ～ 9、ピリオド、ハイフン、カンマ、またはアンダースコアの文字を使用してください。名前は 64 文字以下にする必要があります。

b) [Type]：ホスト、ネットワーク、または範囲。

c) [IP Addresses]：IPv4 または IPv6 アドレス。ホストの場合は単一のアドレスを、範囲の場合は開始アドレスと終了アドレスを、サブネットの場合は IPv4 ネットワーク アドレスおよびマスク（たとえば、10.100.10.0 255.255.255.0）または IPv6 アドレスおよびプレフィックス長（たとえば、2001:DB8:0:CD30::/60）を入力します。

ステップ 3 [NAT] セクションが表示されていない場合は、[NAT] をクリックしてセクションを展開します。



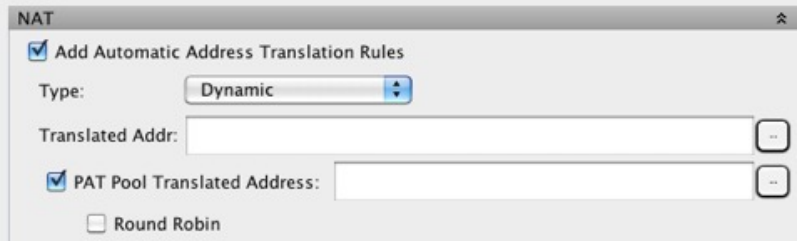
ステップ 4 [Add Automatic Translation Rules] チェックボックスをオンにします。

ステップ 5 PAT プールを使用するダイナミック PAT を設定している場合でも [Type] ドロップダウンリストから [Dynamic] を選択します。

ステップ 6 PAT プールを設定するには、次の手順を実行します。

a) [Translated Addr] フィールドには値を入力せず、空白のままにしてください。
b) [PAT Pool Translated Address] チェック ボックスをオンにしてから、参照ボタンをクリックして、PAT プール アドレスが含まれるネットワーク オブジェクトまたはグループを選択します。または、[Browse Translated PAT Pool Address] ダイアログボックスから新しいオブジェクトを作成します。

（注） PAT プール オブジェクトまたはグループにサブネットが含まれていてはなりません。IPv4 アドレスと IPv6 アドレスの両方をグループに入れることはできません。1 つのタイプだけが含まれている必要があります。

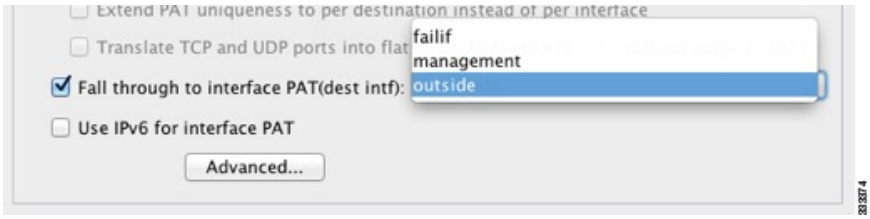


c) （オプション）必要に応じて、次のオプションを選択します。

- [Round Robin] ：アドレスおよびポートをラウンドロビン方式で割り当てる場合。デフォルトではラウンドロビンは使用されず、1 つの PAT アドレスのポートがすべて割り当てられると次の PAT アドレスが使用されます。ラウンドロビン方式では、プール内の各 PAT アドレスから 1 つずつアドレス/ポートが割り当てられると最初のアドレスに戻り、次に 2 番目のアドレスというように順に使用されます。
- [Extend PAT uniqueness to per destination instead of per interface] （8.4(3) 以降、ただし 8.5(1) または 8.6(1) は含まず）：拡張 PAT を使用する場合。拡張 PAT では、変換情報の宛先アドレスとポートを含め、IP アドレスごとではなく、サービスごとに 65535 個のポートが使用されます。通常、PAT 変換の作成時に宛先ポートとアドレスは考慮されないため、PAT アドレスあたり 65535 個のポートに制限されます。たとえば、拡張 PAT を使用して、192.168.1.7:23 に向かう場合の 10.1.1.1:1027 の変換、および 192.168.1.7:80 に向かう場合の 10.1.1.1:1027 の変換を作成できます。
- [Include Reserved Ports (1 to 1023)]：アドレス変換に使用できるポートの範囲に予約済みポート（1 ー 1023）を含めます。このオプションを指定しない場合、アドレスは 1024 ー 65535 の範囲内のポートのみに変換されます。
- [Enable Block Allocation]（9.5.1 以降）：ポートの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 では、NATに 1 度に 1 つのポート変換を割り当てさせるのではなく、各ホストにポートのブロックを割り当てることができます。ポートのブロックを割り当てると、ホストからのその後の接続では、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ラウンドロビンと互換性がありますが、拡張 PAT と

一緒に使用することはできません。また、インターフェイス PAT のフォールバックを使用することもできません。

ステップ 7 （任意、マッピングされたインターフェイスが非ブリッジ グループ メンバーのときのみ）他のマッピング アドレスがすべて割り当て済みの場合にインターフェイス IP アドレスをバックアップ方法として使用するには、[Fall through to interface PAT] チェック ボックスをオンにして、インターフェイスをドロップダウン リストから選択します。インターフェイスの IPv6 アドレスを使用するには、[Use IPv6 for interface PAT] チェック ボックスをオンにします。



ステップ 8 （任意）[Advanced] をクリックし、[Advanced NAT Settings] ダイアログボックスで次のオプションを設定して [OK] をクリックします。

- （ブリッジ グループ メンバーのインターフェイスに必要）[Interface]：この NAT ルールを適用する実際のインターフェイス（**送信元**）およびマッピング インターフェイス（**宛先**）を指定します。デフォルトでは、ルールはブリッジ グループ メンバーを除くすべてのインターフェイスに適用されます。

ステップ 9 [OK]、続いて [Apply] をクリックします。

ダイナミック Twice PAT（隠蔽）の設定

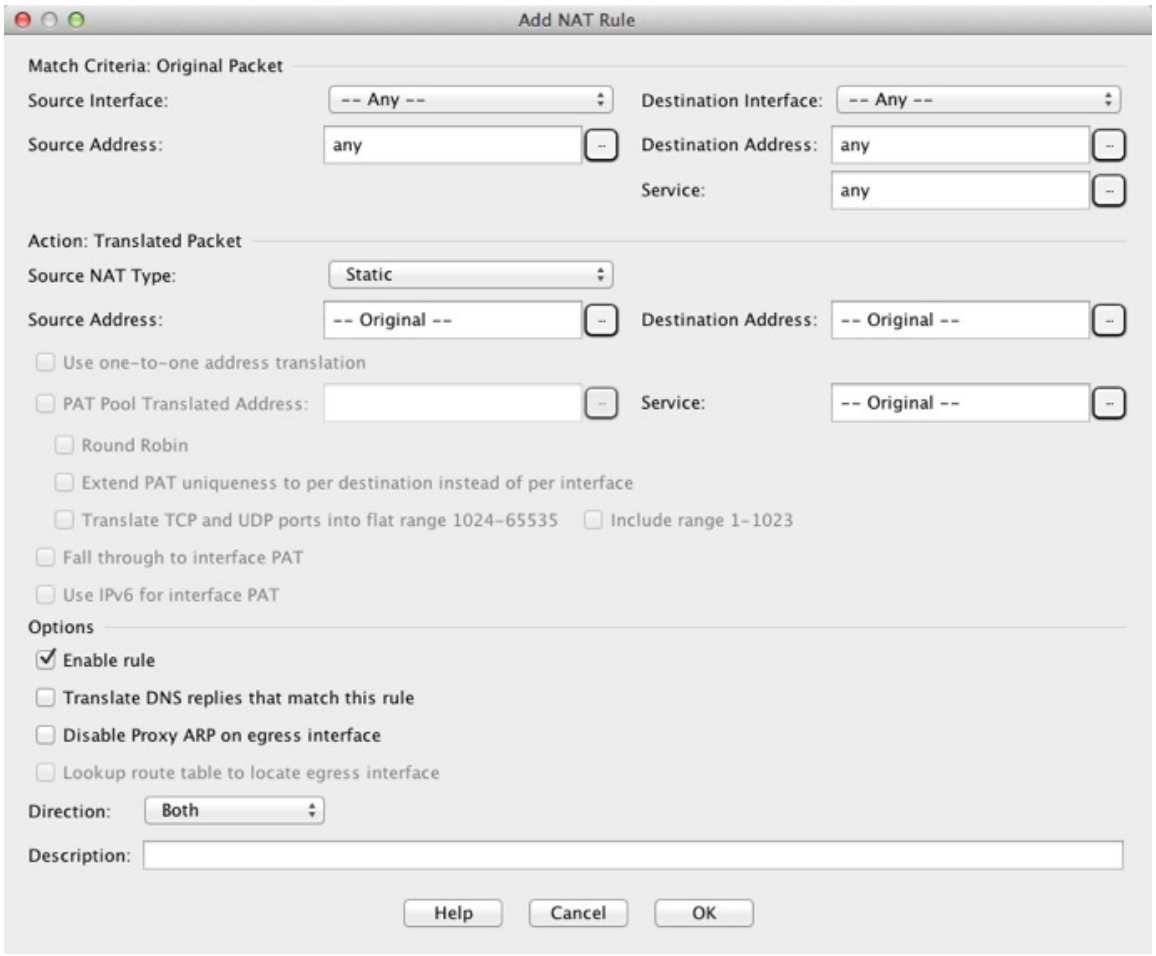
この項では、PAT プールの代わりに変換のための単一のアドレスを使用するダイナミック PAT（隠蔽）の Twice NAT を設定する方法について説明します。

手順

ステップ 1 **[Configuration]** > **[Firewall]** > **[NAT Rules]** を選択して、次のいずれかを実行します。

- [Add] または [Add] > [Add NAT Rule Before Network Object NAT Rules] をクリックします。
- [Add] > [Add NAT Rule After Network Object NAT Rules] をクリックします。
- Twice NAT ルールを選択して [Edit] をクリックします。

[Add NAT Rule] ダイアログボックスが表示されます。

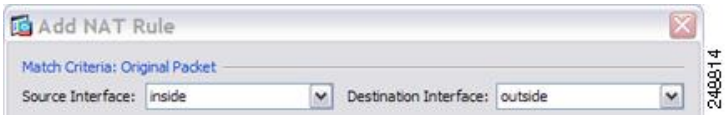


ステップ 2 （ブリッジ グループ メンバーのインターフェイスに必要）送信元インターフェイスおよび宛先インターフェイスを設定します。

ルーテッドモードでは、デフォルトは送信元と宛先の両方のインターフェイスです。いずれかまたは両方のオプションに、特定のインターフェイスを選択できます。ただし、ブリッジ グループ メンバーのインターフェイスにルールを記述するときに、インターフェイスを選択する必要があります。「any」にはこれらのインターフェイスが含まれていません。

a) [Match Criteria: Original Packet] > [Source Interface] ドロップダウンリストから、送信元インターフェイスを選択します。

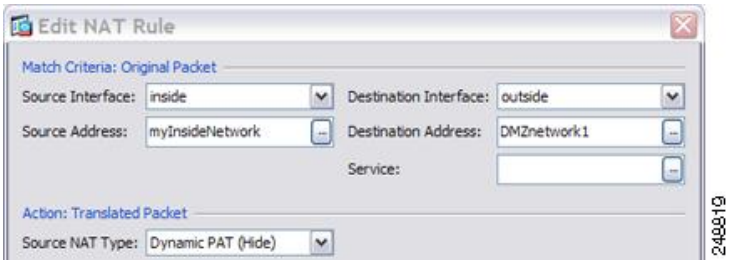
b) [Match Criteria: Original Packet] > [Destination Interface] ドロップダウンリストから、宛先インターフェイスを選択します。



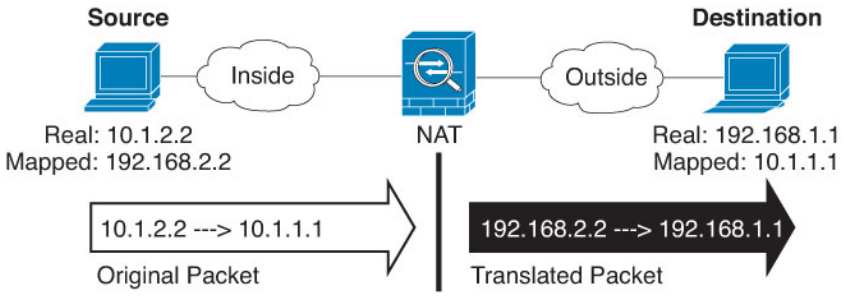
ステップ 3 **[Action: Translated Packet]** > **[Source NAT Type]** ドロップダウンリストから、[Dynamic PAT (Hide)] を選択します。

この設定は送信元アドレスにのみ適用されます。宛先の変換は常にスタティックになります。

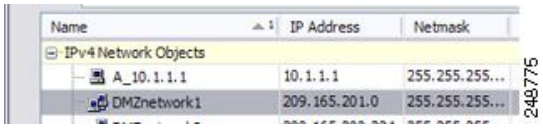
（注） PAT プールを使用するダイナミック PAT を設定するには、[Dynamic PAT (Hide)] の代わりに [Dynamic] を選択します。PAT プールを使用するダイナミック Twice PAT の設定 （40 ページ）を参照してください。



ステップ 4 パケットの元の IPv4 または IPv6 のアドレス、つまり、送信元インターフェイス ネットワーク上に出現するときのパケットのアドレス（実際の送信元アドレスとマッピング宛先アドレス）を識別します。元のパケットと変換されたパケットの例については、次の図を参照してください。



a) [Match Criteria: Original Packet] > [Source Address] について、参照ボタンをクリックして既存のネットワーク オブジェクトまたはグループを選択するか、[Browse Original Source Address] ダイアログボックスから新しい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。デフォルトは **any** です。



b) （任意）[Match Criteria: Original Packet] > [Destination Address] の場合、参照ボタンをクリックして既存のネットワーク オブジェクト、グループ、またはインターフェイス（非ブリッジ グループ メンバーのインターフェイスのみ）を選択するか、[Browse Original Destination Address] ダイアログボックスから新しい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。

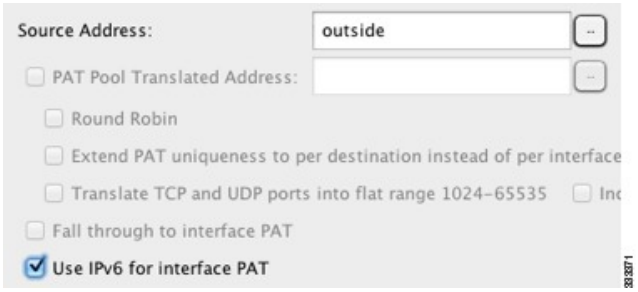
Twice NAT の主な機能は、宛先 IP アドレスを含めることですが、宛先アドレスはオプションです。宛先アドレスを指定した場合、このアドレスにスタティック変換を設定できるか、単にアイデンティティ NAT を使用できます。宛先アドレスを使用せずに Twice NAT を設定して、実際のアドレスに対するネットワーク オブジェクト グループの使用または手動でのルールの順序付けを含む、Twice NAT の他の特質の一部を活用することができます。詳細については、ネットワークオブジェクト NAT と twice NAT の比較 （4 ページ）を参照してください。

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、[Browse] ダイアログボックスからインターフェイスを選択します。サービス変換も必ず設定します。このオプションでは、[Source Interface] 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 （51 ページ）」を参照してください。

ステップ 5 パケットの変換された IPv4 または IPv6 のアドレス、つまり、宛先インターフェイス ネットワーク上に出現するときのパケットのアドレス（マッピング送信元アドレスと実際の宛先アドレス）を識別します。必要に応じて、IPv4 と IPv6 の間で変換できます。

a) [Action: Translated Packet] > [Source Address] について、参照ボタンをクリックしてホストアドレスまたはインターフェイスを定義する既存のネットワーク オブジェクトを選択するか、[Browse Translated Source Address] ダイアログボックスから新しいオブジェクトを作成します。インターフェイスはブリッジ グループ メンバーになることはできません。

インターフェイスの IPv6 アドレスを使用するには、[Use IPv6 for interface PAT] チェックボックスをオンにします。



b) （任意）[Action: Translated Packet] > [Destination Address] について、参照ボタンをクリックして既存のネットワーク オブジェクトまたはグループを選択するか、[Browse Translated Destination Address] ダイアログボックスから新しい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。

宛先アドレスのアイデンティティ 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。

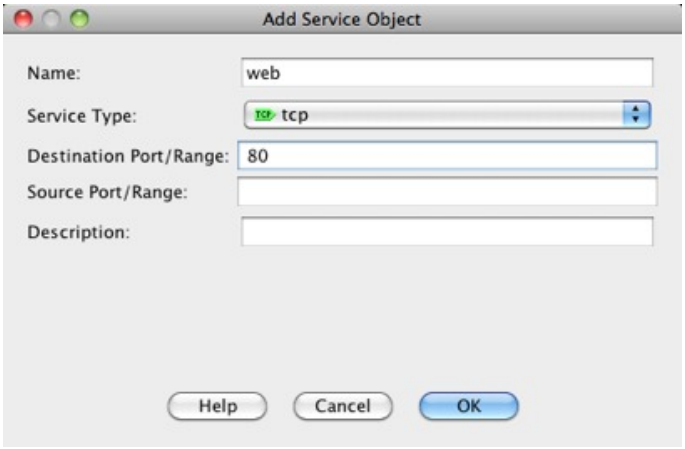
宛先アドレスを変換する場合、スタティック マッピングは、通常 1 対 1 です。したがって、実際のアドレスとマッピングアドレスの数は同じです。ただし、必要に応じて異なる数にすることができます。詳細については、スタティック NAT （51 ページ）を参照してください。拒否されるマッピング IP アドレスについては、NAT のガイドライン （8 ページ）を参照してください。

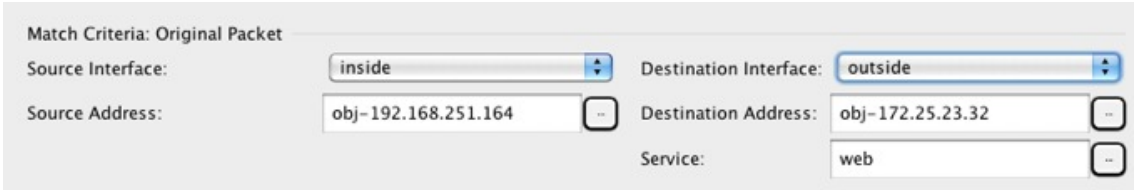
ステップ 6 （任意）サービス変換の宛先サービス ポートを識別します。

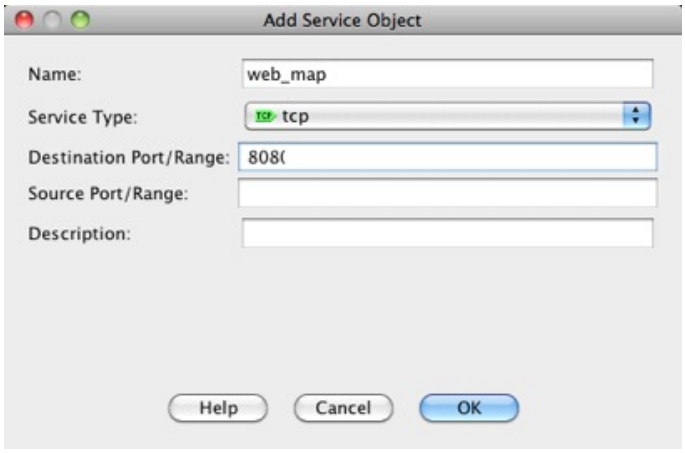
- 元のパケット ポート（マッピング宛先ポート）を識別します。[Match Criteria: Original Packet] > [Service] について、参照ボタンをクリックしてTCP ポートまたは UDP ポートを指定する既存のサービス オブジェクトを選択するか、[Browse Original Service] ダイアログボックスから新しいオブジェクトを作成します。
- 変換されたパケット ポート（実際の宛先ポート）を識別します。[Action: Original Packet] > [Service] について、参照ボタンをクリックしてTCP ポートまたは UDP ポートを指定する既存のサービス オブジェクトを選択するか、[Browse Translated Service] ダイアログボックスから新しいオブジェクトを作成します。

ダイナミック NAT では、ポート変換はサポートされません。しかし、宛先変換は常にスタティックなので、宛先ポートに対して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。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。「not equal（等しくない）」（**!=**）演算子はサポートされていません。

次に例を示します。

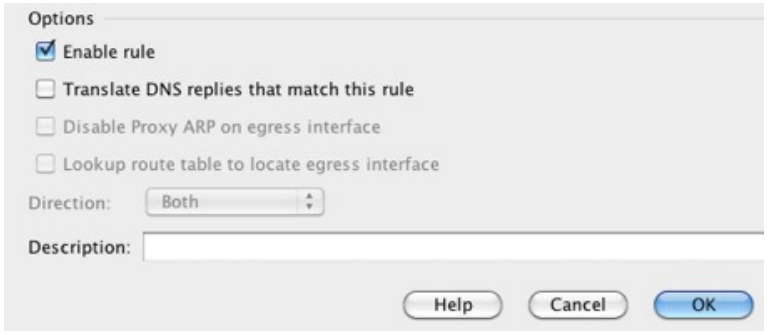








ステップ 7 （任意）[Options] 領域で NAT オプションを設定します。



- [Enable rule]：この NAT ルールをイネーブルにします。このルールはデフォルトでイネーブルになっています。
- [Description]：ルールに関する説明を 200 文字以内で追加します。

ステップ 8 [OK] をクリックし、続いて [Apply] をクリックします。

PAT プールを使用するダイナミック Twice PAT の設定

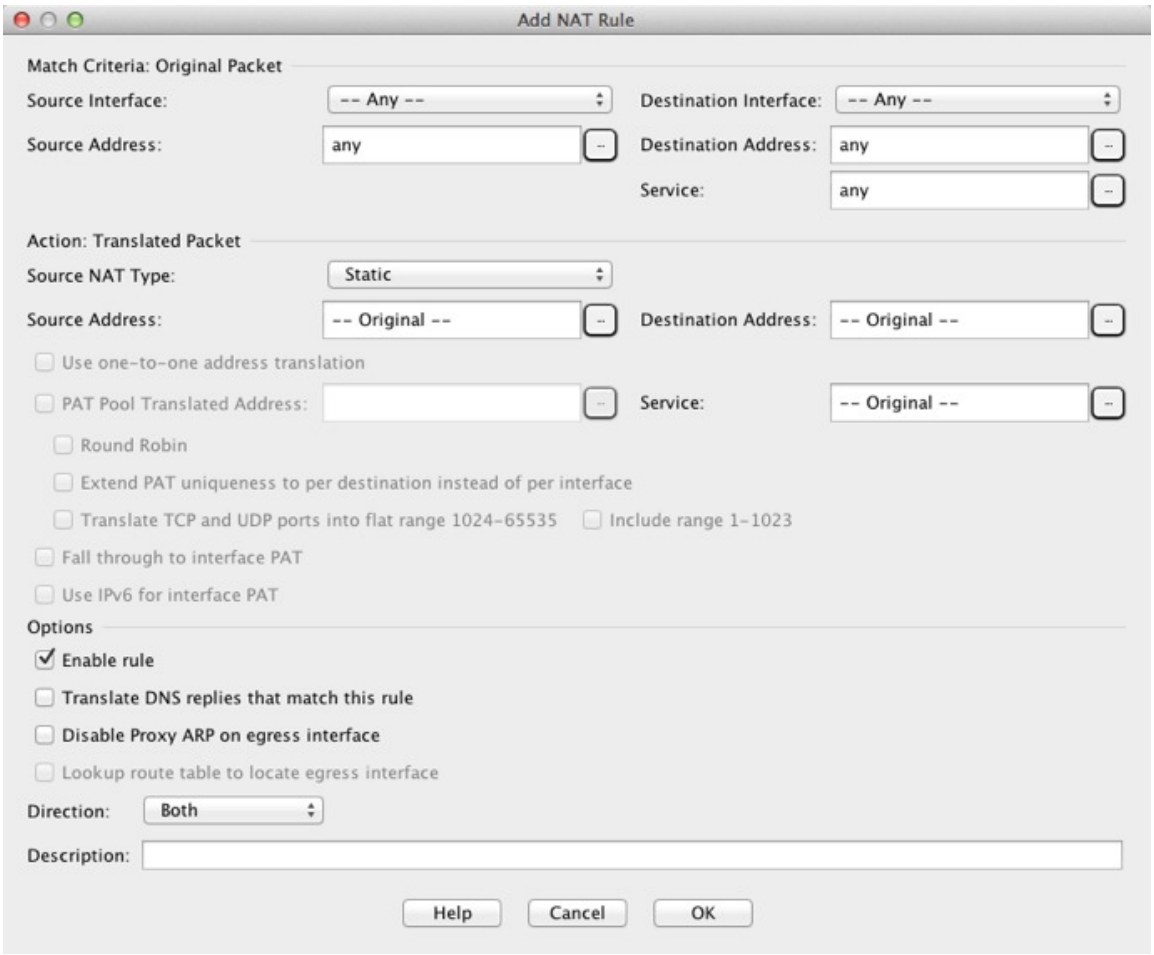
この項では、PAT プールを使用するダイナミック PAT の Twice NAT を設定する方法について説明します。

手順

ステップ 1 **[Configuration]** > **[Firewall]** > **[NAT Rules]** を選択して、次のいずれかを実行します。

- [Add] または **[Add]** > **[Add NAT Rule Before Network Object NAT Rules]** をクリックします。
- **[Add]** > **[Add NAT Rule After Network Object NAT Rules]** をクリックします。
- Twice NAT ルールを選択して [Edit] をクリックします。

[Add NAT Rule] ダイアログボックスが表示されます。



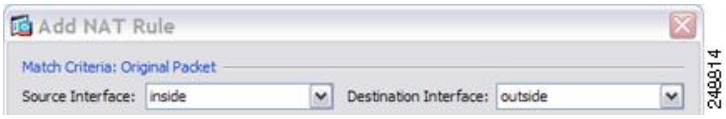
ステップ 2 （ブリッジ グループ メンバーのインターフェイスに必要）送信元インターフェイスおよび宛先インターフェイスを設定します。

ルーテッドモードでは、デフォルトは送信元と宛先の両方のインターフェイスです。いずれかまたは両方のオプションに、特定のインターフェイスを選択できます。ただし、ブリッジ グ

ループ メンバーのインターフェイスにルールを記述するときに、インターフェイスを選択する必要があります。「any」にはこれらのインターフェイスが含まれていません。

a) **[Match Criteria: Original Packet]** > **[Source Interface]** ドロップダウンリストから、送信元インターフェイスを選択します。

b) **[Match Criteria: Original Packet]** > **[Destination Interface]** ドロップダウンリストから、宛先インターフェイスを選択します。

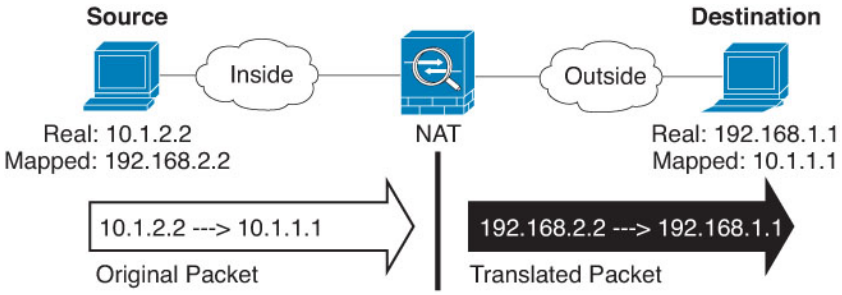


ステップ 3 **[Action: Translated Packet]** > **[Source NAT Type]** ドロップダウンリストから、[Dynamic] を選択します。

この設定は送信元アドレスにのみ適用されます。宛先の変換は常にスタティックになります。



ステップ 4 パケットの元の IPv4 または IPv6 のアドレス、つまり、送信元インターフェイス ネットワーク上に出現するときのパケットのアドレス（実際の送信元アドレスとマッピング宛先アドレス）を識別します。元のパケットと変換されたパケットの例については、次の図を参照してください。



a) **[Match Criteria: Original Packet]** > **[Source Address]** について、参照ボタンをクリックして既存のネットワーク オブジェクトまたはグループを選択するか、[Browse Original Source Address] ダイアログボックスから新しい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。デフォルトは **any** です。

b) （任意）**[Match Criteria: Original Packet]** > **[Destination Address]** の場合、参照ボタンをクリックして既存のネットワーク オブジェクト、グループ、またはインターフェイス（非ブリッジ グループ メンバーのインターフェイスのみ）を選択するか、[Browse Original Destination Address] ダイアログボックスから新しい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。

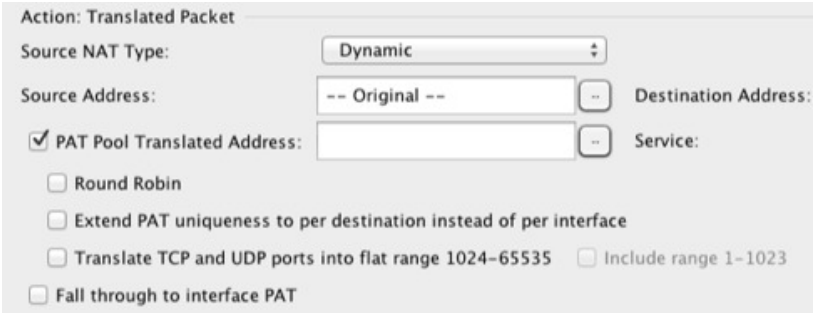
Twice NAT の主な機能は、宛先 IP アドレスを含めることですが、宛先アドレスはオプションです。宛先アドレスを指定した場合、このアドレスにスタティック変換を設定できる

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。

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、[Browse] ダイアログボックスからインターフェイスを選択します。サービス変換も必ず設定します。このオプションでは、[Source Interface] 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 （51 ページ）」を参照してください。

ステップ 5 パケットの変換された IPv4 または IPv6 のアドレス、つまり、宛先インターフェイス ネットワーク上に出現するときのパケットのアドレス（マッピング送信元アドレスと実際の宛先アドレス）を識別します。必要に応じて、IPv4 と IPv6 の間で変換できます。

a) [PAT Pool Translated Address] チェック ボックスをオンにしてから、参照ボタンをクリックして既存のネットワーク オブジェクトまたはグループを選択するか、[Browse Translated PAT Pool Address] ダイアログボックスから新しいオブジェクトまたはグループを作成します。**注**：[Source Address] フィールドは空のままにしておきます。



（注） オブジェクトまたはグループは、サブネットを含むことはできません。

b) （任意）**[Action: Translated Packet]** > **[Destination Address]** について、参照ボタンをクリックして既存のネットワーク オブジェクトまたはグループを選択するか、[Browse Translated Destination Address] ダイアログボックスから新しいオブジェクトまたはグループを作成します。

宛先アドレスのアイデンティティ 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。

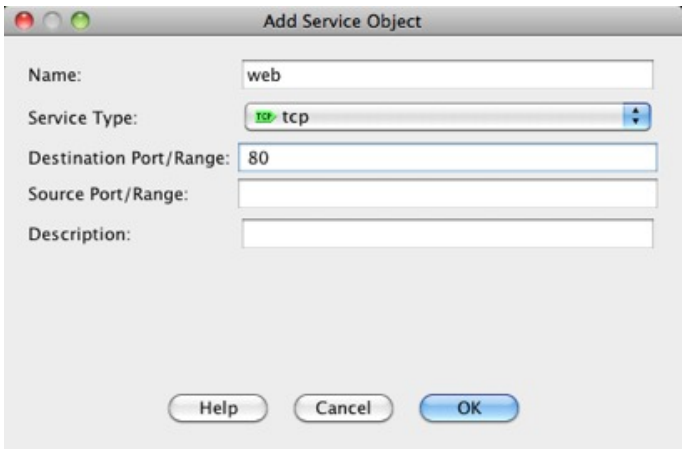
宛先アドレスを変換する場合、スタティック マッピングは、通常 1 対 1 です。したがって、実際のアドレスとマッピング アドレスの数は同じです。ただし、必要に応じて異なる数にすることができます。詳細については、スタティック NAT （51 ページ）を参照してください。拒否されるマッピング IP アドレスについては、NAT のガイドライン （8 ページ）を参照してください。

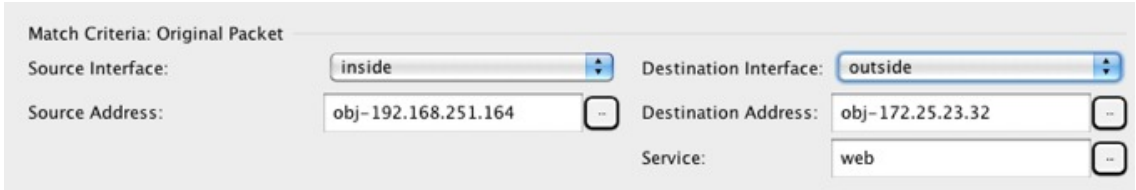
ステップ 6　（任意）サービス変換の宛先サービス ポートを識別します。

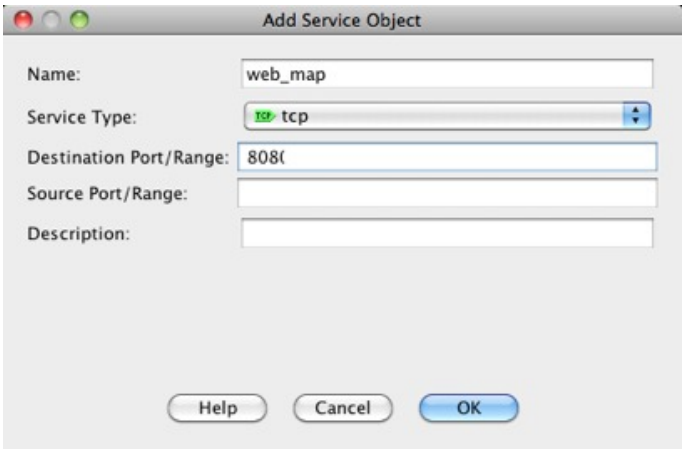
- 元のパケット ポート（マッピング宛先ポート）を識別します。**[Match Criteria: Original Packet]** > **[Service]** について、参照ボタンをクリックして TCP ポートまたは UDP ポートを指定する既存のサービス オブジェクトを選択するか、[Browse Original Service] ダイアログボックスから新しいオブジェクトを作成します。
- 変換されたパケット ポート（実際の宛先ポート）を識別します。**[Action: Translated Packet]** > **[Service]** について、参照ボタンをクリックして TCP ポートまたは UDP ポートを指定する既存のサービス オブジェクトを選択するか、[Browse Translated Service] ダイアログボックスから新しいオブジェクトを作成します。

ダイナミック NAT では、ポート変換はサポートされません。しかし、宛先変換は常にスタティックなので、宛先ポートに対して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。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。「not equal（等しくない）」（**!=**）演算子はサポートされていません。

次に例を示します。









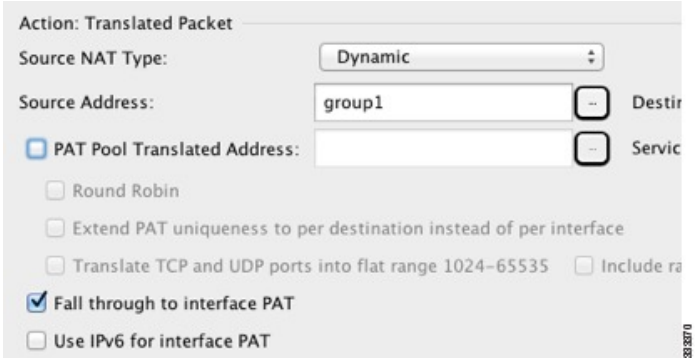
ステップ 7 （任意）PAT プールの場合は、必要に応じて次のオプションを設定します。

- [Round Robin]：アドレス/ポートをラウンドロビン方式で割り当てる場合。デフォルトではラウンドロビンは使用されず、1 つの PAT アドレスのポートがすべて割り当てられると次の PAT アドレスが使用されます。ラウンドロビン方式では、プール内の各 PAT アドレスから 1 つずつアドレス/ポートが割り当てられると最初のアドレスに戻り、次に 2 番目のアドレスというように順に使用されます。
- [Extend PAT uniqueness to per destination instead of per interface] （8.4(3) 以降、ただし 8.5(1) または 8.6(1) は含まず）：拡張 PAT を使用する場合。拡張 PAT では、変換情報の宛先アドレスとポートを含め、IP アドレスごとではなく、サービスごとに 65535 個のポートが使用されます。通常、PAT 変換の作成時に宛先ポートとアドレスは考慮されないため、PAT アドレスあたり 65535 個のポートに制限されます。たとえば、拡張 PAT を使用して、192.168.1.7:23 に向かう場合の 10.1.1.1:1027 の変換、および 192.168.1.7:80 に向かう場合の 10.1.1.1:1027 の変換を作成できます。
- [Translate TCP or UDP ports into flat range (1024-65535)] （8.4(3) 以降、ただし 8.5(1) または 8.6(1) は含まず）：ポートの割り当て時に 1 つのフラットな範囲として 1024 ～ 65535 のポート範囲を使用する場合。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、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 の全範囲を使用するには、[Include range 1 to 1023] チェックボックスもオンにします。

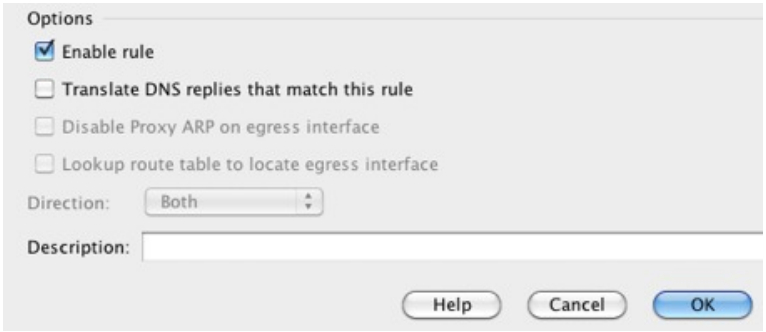
- [Include Reserved Ports (1 to 1023)]：アドレス変換に使用できるポートの範囲に予約済みポート（1 ー 1023）を含めます。このオプションを指定しない場合、アドレスは 1024 ー 65535 の範囲内のポートのみに変換されます。
- [Enable Block Allocation]（9.5.1 以降）：ポートのブロック割り当てをイネーブルにします。キャリアグレードまたは大規模 PAT では、NATに 1 度に 1 つのポート変換を割り当てさせるのではなく、各ホストにポートのブロックを割り当てることができます。ポートのブロックを割り当てると、ホストからのその後の接続では、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ラウンドロビンと互換性がありますが、拡張 PAT と一緒に使用することはできません。また、インターフェイス PAT のフォールバックを使用することもできません。

ステップ 8 （任意、マッピングされたインターフェイスが非ブリッジ グループ メンバーのときのみ）他のマッピングされた送信元アドレスがすでに割り当てられている場合に、インターフェイス IP アドレスをバックアップの手段として使用するには、[Fall through to interface PAT] チェックボックスをオンにします。IPv6 インターフェイス アドレスを使用するには、[Use IPv6 for interface PAT] チェックボックスもオンにします。

宛先インターフェイス IP アドレスが使用されます。このオプションは、特定の [Destination Interface] を設定する場合にだけ使用できます。



ステップ 9 （任意）[Options] 領域で NAT オプションを設定します。



- [Enable rule]：この NAT ルールをイネーブルにします。このルールはデフォルトでイネーブルになっています。
- [Description]：ルールに関する説明を 200 文字以内で追加します。

ステップ 10 [OK] をクリックし、続いて [Apply] をクリックします。

ポート ブロック割り当てによる PAT の設定

キャリア グレードまたは大規模 PAT では、NAT に 1 度に 1 つのポート変換を割り当てさせるのではなく、各ホストにポートのブロックを割り当てることができます（RFC 6888 を参照してください）。ポートのブロックを割り当てると、ホストからのその後の接続では、ブロック内のランダムに選択される新しいポートが使用されます。必要に応じて、ホストが元のブロック内のすべてのポートに関してアクティブな接続を持つ場合は追加のブロックが割り当てられます。ブロックのポートを使用する最後の xlate が削除されると、ブロックが解放されます。

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

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

始める前に

NAT ルールの使用上の注意：

- [Round Robin] オプションは含めることができますが、PAT 一意性の拡張、またはインターフェイス PAT へのフォールスルーに関するオプションは含めることができません。その他の送信元/宛先のアドレスとポート情報も許可されます。
- 既存のルールを置き換える場合は、NAT を変更するすべてのケースと同様、置き換えるルールに関連する xlate をクリアする必要があります。これは、新しいルールを有効にするために必要です。それらを明示的にクリアするか、または単にタイムアウトになるまで待ちます。ただし、クラスターで動作する場合、ユニットがブロックを正しく配布できるようにクラスターをリロードする必要があります。

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

- 制御ノードになるデバイスに PAT プールを使用している既存の NAT ポリシーがある間にクラスターを形成すると、PAT ポートブロック分配が正しく初期化されないことがあります。制御ノードがポートブロックを所有または分配せず、**show nat pool cluster summary** コマンドでは、すべてのクラスターノードですべてのポートブロックが *RESERVED* と表示されることがあります。
  - クラスターを形成する前に、制御ノードになるデバイスから、PAT プールを使用している既存の NAT ポリシーを削除します。クラスターの形成が完了したら、NAT ポリシーを再設定して展開します。
  - クラスターが形成済みであり、すべてのポートブロックが *RESERVED* と表示されている場合は、影響を受ける NAT ポリシーを削除してから変更を展開します。その後に、ポリシーを再作成して展開します。**show nat pool cluster summary** コマンドを使用して、ポートブロックがクラスターノード間で正しく分散されていることを確認します。
- 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 **[Configuration]** > **[Firewall]** > **[Advanced]** > **[PAT Port Block Allocation]** を選択し、次の設定を行います。

- [Size of the block]：各ブロックのポート数。範囲は 32 ～ 4096 です。デフォルトは 512 です。

  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。
- [Maximum block allocation per host]：ホストごとに割り当てることができるブロックの最大数。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。

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

  %ASA-6-305017: Pba-interim-logging: Active *protocol* block of ports for translation from *real_interface*:*real_host_ip* to *mapped_interface*:*mapped_ip_address*/*start_port_num-end_port_num*

ステップ 2 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。

a) **[Configuration]** > **[Firewall]** > **[NAT Rules]** を選択します。
b) オブジェクト NAT または Twice NAT ルールを追加または編集します。
c) 少なくとも次のオプションは設定してください。
   - （Twice NAT。）**[Original Packet]** > **[Source Address]** で発信元アドレスを定義するオブジェクトを選択します。
   - [Type] = [Dynamic]
   - [Pat Pool Translated Address] PAT プール ネットワークを定義するネットワーク オブジェクトを選択します。
   - [Enable Block Allocation]
d) [OK] をクリックします。

Per-Session PAT または Multi-Session PAT（バージョン 9.0(1) 以降）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 の拡張性が向上し、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、制御ユニットに転送して制御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。

- any（IPv4 および IPv6）から any（IPv4 および IPv6）への TCP を許可する。
- any（IPv4 および IPv6）からドメインへの UDP を許可する。

これらのルールは、テーブルに表示されません。

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。

- any（IPv4 および IPv6）から any（IPv4 および IPv6）への TCP を拒否する。
- any（IPv4 および IPv6）からドメインへの UDP を拒否する。

手順

ステップ 1 **[Configuration]** > **[Firewall]** > **[Advanced]** > **[Per-Session NAT Rules]** を選択します。

ステップ 2 次のいずれかを実行します。

- [Add] > [Add Per-Session NAT Rule] を選択します。
- ルールを選択して [Edit] をクリックします。

ステップ 3 ルールを設定します。

- [Action]：[Permit] または [Deny] をクリックします。許可ルールは、per-session PAT を使用し、拒否ルールは multi-session PAT を使用します。
- [Source]：アドレスを入力するか、または [...] ボタンをクリックし、オブジェクトを選択して、送信元アドレスを指定します。サービスの場合、UDP または TCP を選択します。通常は宛先ポートだけを指定しますが、任意で送信元ポートを指定できます。[UDP/port] または [TCP/port] に入力するか、[...] ボタンをクリックして、共通の値またはオブジェクトを選択します。
- [Destination]：アドレスを入力するか、または [...] ボタンをクリックし、オブジェクトを選択して、宛先アドレスを指定します。サービスの場合、UDP または TCP を選択します。これは送信元サービスと一致する必要があります。任意で宛先ポートを指定できます。

[UDP/port] または [TCP/port] に入力するか、[...] ボタンをクリックして、共通の値またはオブジェクトを選択します。演算子（!=（等しくない)、>（より大きい）、<（より小さい））を使用することも、ハイフン（たとえば、100-200）を指定することもできます。

ステップ 4 [OK] をクリックし、続いて [Apply] をクリックします。

スタティック NAT

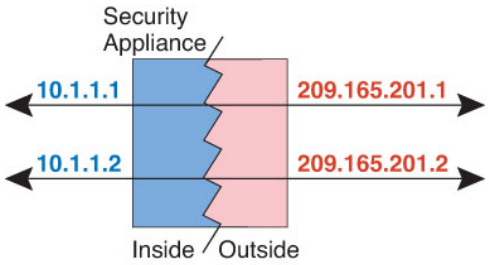
ここでは、スタティック NAT とその実装方法について説明します。

スタティック NAT について

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

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

図 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。

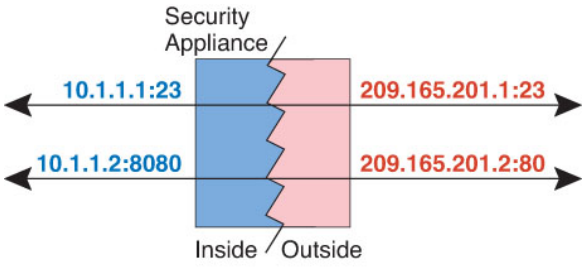
ポート変換を設定したスタティック NAT

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 *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と、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）については、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ーの正しい IP アドレスにマッピングできます。サーバーは標準のポート（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、ウェルノウン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

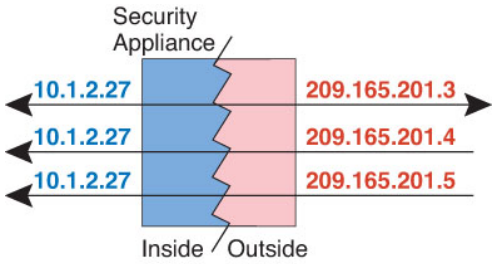
スタティック NAT は、実際のアドレスをインターフェイスアドレスとポートの組み合わせにマッピングするように設定できます。たとえば、デバイスの外部インターフェイスへの Telnet アクセスを内部ホストにリダイレクトする場合、内部ホストの IP アドレス/ポート 23 を外部インターフェイス アドレス/ポート 23 にマッピングできます。

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、実際のホストが通信を開始すると、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通信の場合、任意のマッピングアドレスへの通信を開始でき、1 つの実際のアドレスには変換されません。

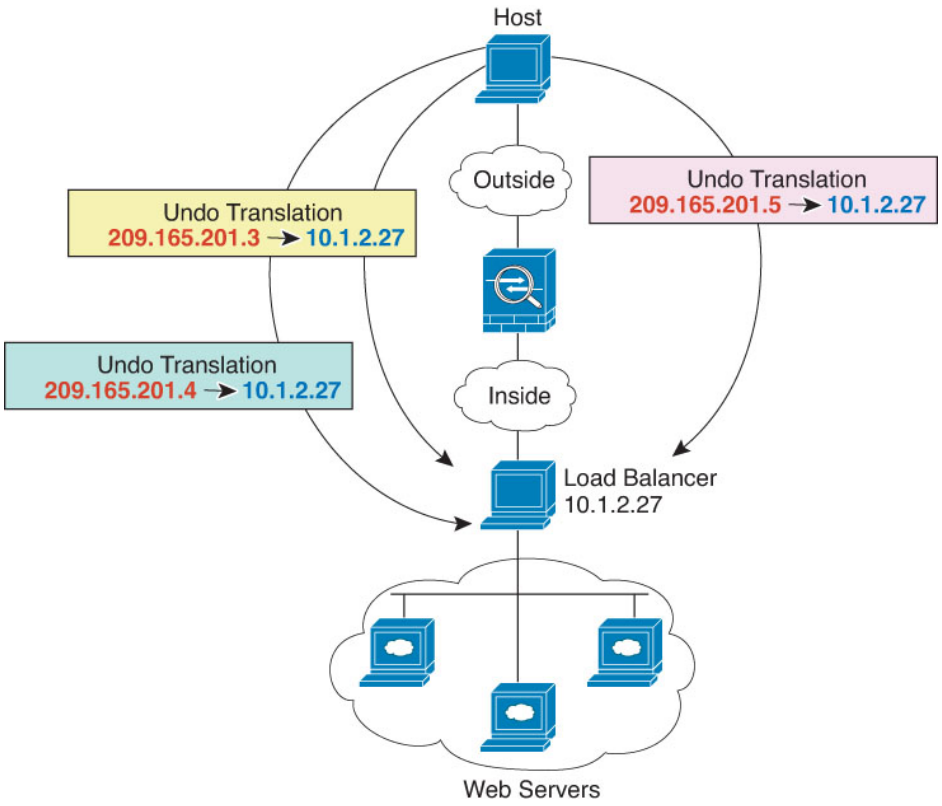
次の図に、一般的な 1 対多のスタティック NAT シナリオを示します。実際のホストが開始すると、常に最初のマッピングアドレスが使用されるため、実際のホスト IP/最初のマッピング IP の変換は、理論的には双方向変換のみが行われます。

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、1 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 : 1* 対多のスタティック *NAT* の例



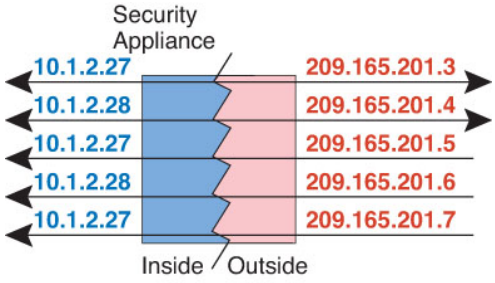
他のマッピングシナリオ（非推奨）

NAT には、1 対 1、1 対多だけではなく、少対多、多対少、多対 1 など任意の種類のスタティック 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 *9*：少対多のスタティック *NAT*

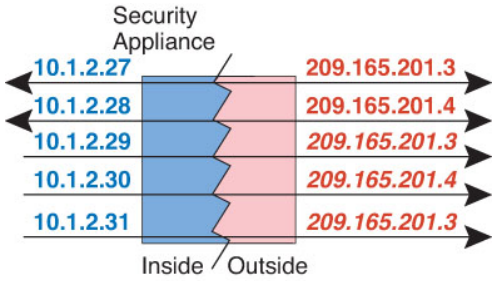


多対少または多対1の設定では、マッピングアドレスよりも多くの実際のアドレスが存在します。実際のアドレスが不足する前に、マッピングアドレスが不足します。双方向の開始を実現できるのは、最下位の実際の IP アドレスとマッピング プールの間でマッピングを行ったときだけです。残りの上位の実際のアドレスはトラフィックを開始できますが、これらへのトラフィックを開始できません。接続のリターントラフィックは、接続の固有の5つの要素（送信元 IP、宛先 IP、送信元ポート、宛先ポート、プロトコル）によって適切な実際のアドレスに転送されます。

（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 *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 新規または既存のネットワーク オブジェクトに NAT を追加します。

- 新しいネットワーク オブジェクトを追加するには、[Configuration] > [Firewall] > [NAT Rules] を選択し、[Add] > [Add Network Object NAT Rule] をクリックします。
- 既存のネットワーク オブジェクトに NAT を追加するには、[Configuration] > [Firewall] > [Objects] > [Network Objects/Groups] を選択し、ネットワーク オブジェクトを編集します。

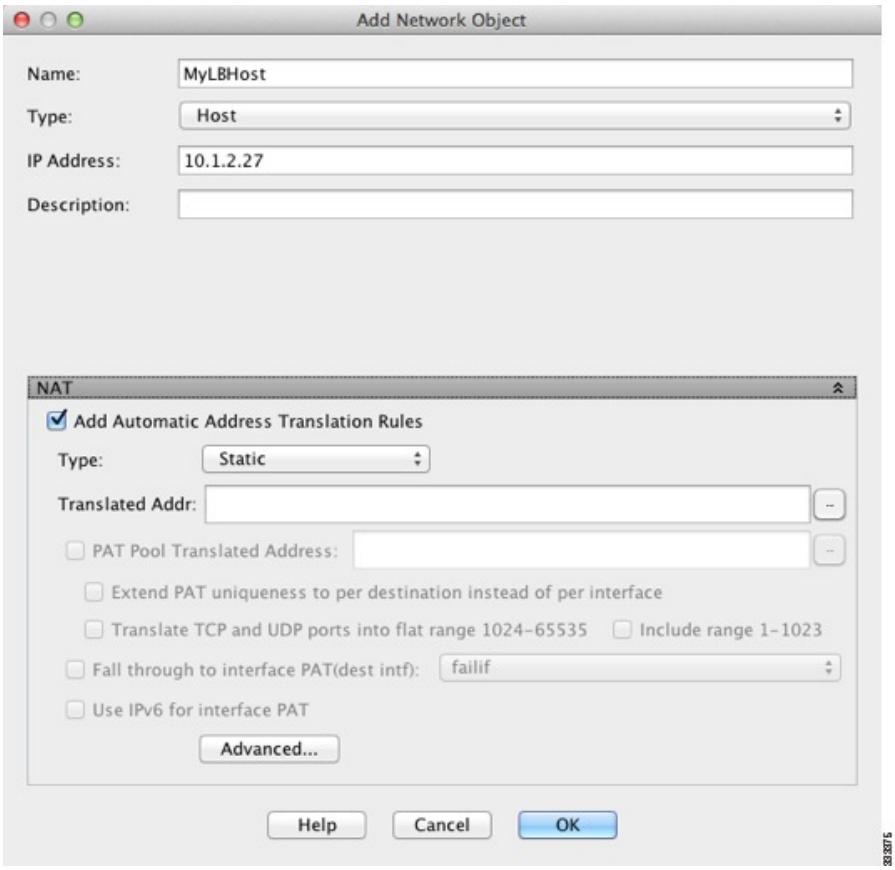
ステップ 2 新しいオブジェクトの場合は、次のフィールドに値を入力します。

- [Name]：オブジェクト名。a ～ z、A ～ Z、0 ～ 9、ピリオド、ハイフン、カンマ、またはアンダースコアの文字を使用してください。名前は 64 文字以下にする必要があります。
- [Type]：ホスト、ネットワーク、または範囲。
- [IP Addresses]：IPv4 または IPv6 アドレス。ホストの場合は単一のアドレスを、範囲の場合は開始アドレスと終了アドレスを、サブネットの場合は IPv4 ネットワーク アドレスおよびマスク（たとえば、10.100.10.0 255.255.255.0）または IPv6 アドレスおよびプレフィックス長（たとえば、2001:DB8:0:CD30::/60）を入力します。

ステップ 3 [NAT] セクションが表示されていない場合は、[NAT] をクリックしてセクションを展開します。

ステップ 4 [Add Automatic Translation Rules] チェックボックスをオンにします。

ステップ 5 [Type] ドロップダウン リストから、[Static] を選択します。



ステップ 6 [Translated Addr] フィールドで、マッピング IP アドレスを次のいずれかとして指定します。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。詳細については、スタティック NAT（51 ページ）を参照してください。

- ホスト IP アドレスを入力します。これにより、ホストオブジェクトに 1 対 1 のマッピングが提供されます。サブネットオブジェクトの場合は、インラインホストアドレスに対して同じネットマスクが使用され、マッピングされたインラインホストのサブネット内のアドレスに対して 1 対 1 の変換が行われます。範囲オブジェクトの場合は、マッピングされたアドレスには、範囲オブジェクトにある同じ数のホストが含まれ、それらはマッピングされたホストアドレスから始まります。たとえば、実際のアドレスが 10.1.1.1 ～ 10.1.1.6 の範囲として定義され、172.20.1.1 をマッピング アドレスとして指定する場合、マッピング範囲には、172.20.1.1 ～ 172.20.1.6 が含まれます。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。
- 参照ボタンをクリックし、ネットワーク オブジェクトを選択します（または新しいネットワーク オブジェクトを作成します）。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。
- （ポート変換を設定したスタティック NAT の場合のみ）インターフェイス名を入力するか、または参照ボタンをクリックし、[Browse Translated Addr] ダイアログボックスでイン

ターフェイスを選択します。ブリッジ グループ メンバーのインターフェイスを選択することはできません。



IPv6 インターフェイス アドレスを使用するには、[Use IPv6 for interface PAT] チェック ボックスもオンにする必要があります。[Advanced] をクリックしてサービス ポート変換も必ず設定します（トランスペアレント モードでは、インターフェイスを指定することはできません）。

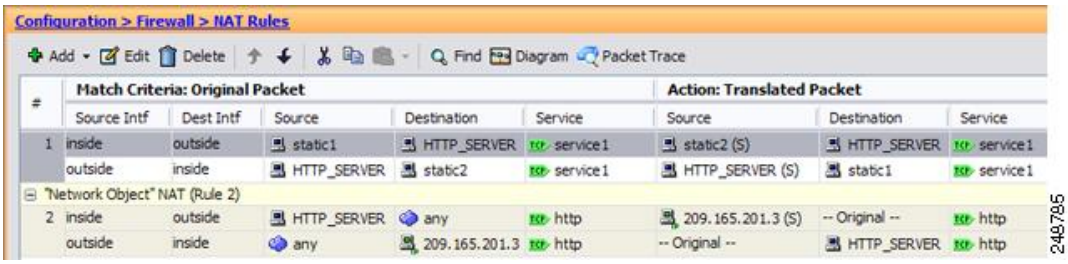
ステップ 7 （任意）NAT46 の場合、[Use one-to-one address translation] をオンにします。NAT 46 の場合、最初の IPv4 アドレスを最初の IPv6 アドレス、2 番目の IPv4 アドレスを 2 番目の IPv6 アドレス、以下同様に 1 対 1 で順に変換するように指定します。このオプションを指定しない場合は、IPv4 埋め込み方式が使用されます。1 対 1 変換の場合は、このキーワードを使用する必要があります。

ステップ 8 （任意）[Advanced] をクリックし、[Advanced NAT Settings] ダイアログボックスで次のオプションを設定して [OK] をクリックします。

- [Translate DNS replies for rule]：DNS 応答内の IP アドレスを変換します。DNS インスペク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。
- [Disable Proxy ARP on egress 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 をディセーブルにします。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。
- （ブリッジ グループ メンバーのインターフェイスに必要）[Interface]：この NAT ルールを適用する実際のインターフェイス（**送信元**）およびマッピング インターフェイス（**宛先**）を指定します。デフォルトでは、ルールはブリッジ グループ メンバーを除くすべてのインターフェイスに適用されます。
- [Service]：ポート変換を設定したスタティック NAT を設定します。プロトコルを選択してから、実際のポートとマッピング ポートを入力します。ポート番号または既知のポート名（http など）を使用できます。

ステップ 9 [OK]、続いて [Apply] をクリックします。

スタティック ルールが二方向である（開始を実際のホストの間で許可する）ため、NAT ルール テーブルは各スタティック ルールに対して、各方向に 1 つずつ 2 つの行を表示します。



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

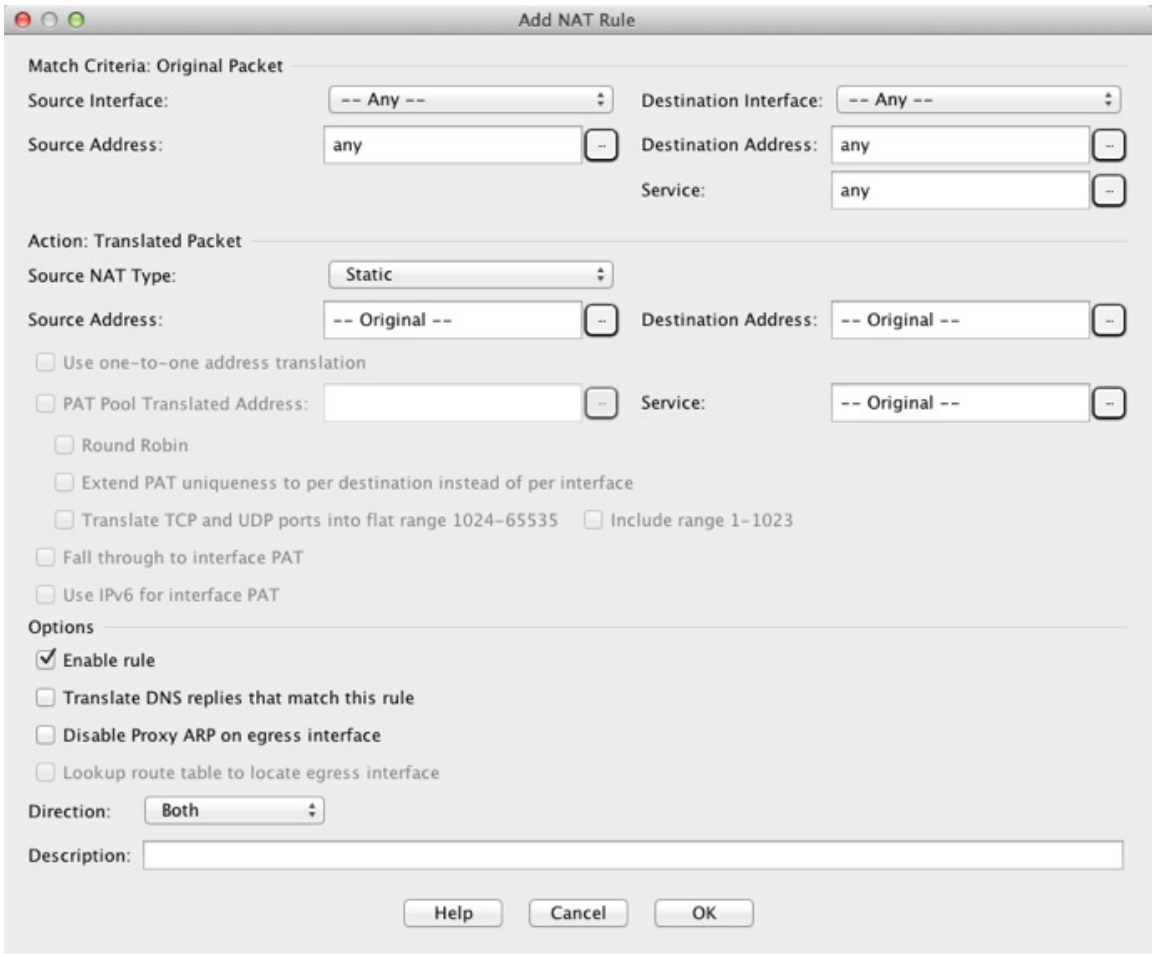
この項では、Twice NAT を使用してスタティック NAT ルールを設定する方法について説明します。

手順

ステップ 1 **[Configuration]** > **[Firewall]** > **[NAT Rules]** を選択して、次のいずれかを実行します。

- [Add] または [Add] > [Add NAT Rule Before Network Object NAT Rules] をクリックします。
- [Add] > [Add NAT Rule After Network Object NAT Rules] をクリックします。
- Twice NAT ルールを選択して [Edit] をクリックします。

[Add NAT Rule] ダイアログボックスが表示されます。

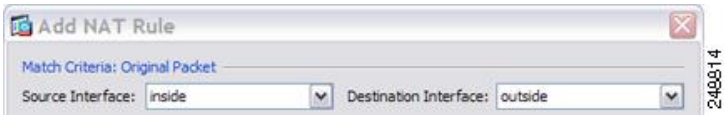


ステップ 2 （ブリッジ グループ メンバーのインターフェイスに必要）送信元インターフェイスおよび宛先インターフェイスを設定します。

ルーテッドモードでは、デフォルトは送信元と宛先の両方のインターフェイスです。いずれかまたは両方のオプションに、特定のインターフェイスを選択できます。ただし、ブリッジ グループ メンバーのインターフェイスにルールを記述するときに、インターフェイスを選択する必要があります。「any」にはこれらのインターフェイスが含まれていません。

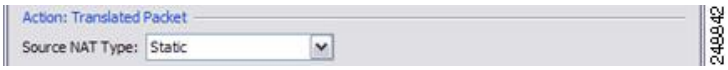
a) [Match Criteria: Original Packet] > [Source Interface] ドロップダウンリストから、送信元インターフェイスを選択します。

b) [Match Criteria: Original Packet] > [Destination Interface] ドロップダウンリストから、宛先インターフェイスを選択します。

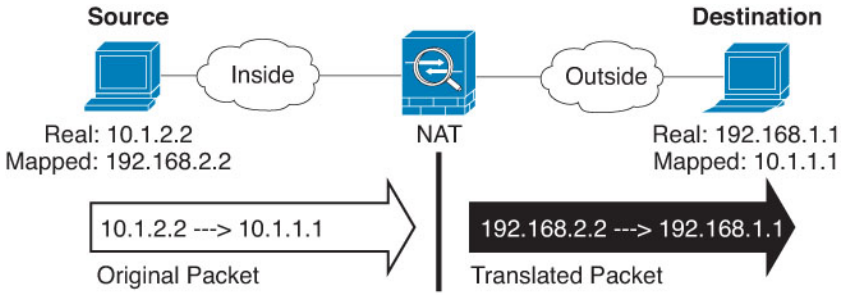


ステップ 3 **[Action: Translated Packet]** > **[Source NAT Type]** ドロップダウンリストから、[Static] を選択します。[Static] がデフォルトの設定です。

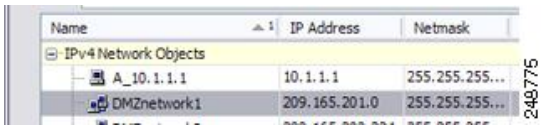
この設定は送信元アドレスにのみ適用されます。宛先の変換は常にスタティックになります。



ステップ 4 パケットの元の IPv4 または IPv6 のアドレス、つまり、送信元インターフェイス ネットワーク上に出現するときのパケットのアドレス（実際の送信元アドレスとマッピング宛先アドレス）を識別します。元のパケットと変換されたパケットの例については、次の図を参照してください。



a) [Match Criteria: Original Packet] > [Source Address] について、参照ボタンをクリックして既存のネットワーク オブジェクトまたはグループを選択するか、[Browse Original Source Address] ダイアログボックスから新しい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。デフォルトは **any** ですが、アイデンティティ NAT を除いてはこのオプションを使用しないでください。



b) （任意）[Match Criteria: Original Packet] > [Destination Address] について、参照ボタンをクリックして既存のネットワーク オブジェクト、グループ、またはインターフェイスを選択するか、[Browse Original Destination Address] ダイアログボックスから新しいオブジェクトまたはグループを作成します。

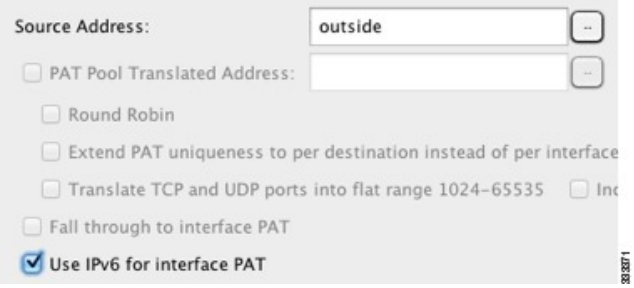
Twice NAT の主な機能は、宛先 IP アドレスを含めることですが、宛先アドレスはオプションです。宛先アドレスを指定した場合、このアドレスにスタティック変換を設定できるか、単にアイデンティティ NAT を使用できます。宛先アドレスを使用せずに Twice NAT を設定して、実際のアドレスに対するネットワーク オブジェクト グループの使用または手動でのルールの順序付けを含む、Twice NAT の他の特質の一部を活用することができます。詳細については、ネットワークオブジェクト NAT と twice NAT の比較 （4 ページ）を参照してください。

ステップ 5 パケットの変換された IPv4 または IPv6 のアドレス、つまり、宛先インターフェイス ネットワーク上に出現するときのパケットのアドレス（マッピング送信元アドレスと実際の宛先アドレス）を識別します。必要に応じて、IPv4 と IPv6 の間で変換できます。

a) [Action: Translated Packet] > [Source Address] について、参照ボタンをクリックして既存のネットワーク オブジェクトまたはグループを選択するか、[Browse Translated Source Address] ダイアログボックスから新しいオブジェクトまたはグループを作成します。

スタティック NAT のマッピングは、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、インターフェイスを指定できます。インターフェイスの IPv6 アドレスを使用するには、[Use IPv6 for interface PAT] チェックボックスをオンにします。ブリッジ グループ メンバーのインターフェイスを選択することはできません。



詳細については、ポート変換を設定したスタティック NAT （51 ページ）を参照してください。拒否されるマッピング IP アドレスについては、NAT のガイドライン （8 ページ）を参照してください。

b) （任意）[Action: Translated Packet] > [Destination Address] について、参照ボタンをクリックして既存のネットワーク オブジェクトまたはグループを選択するか、[Browse Translated Destination Address] ダイアログボックスから新しいオブジェクトまたはグループを作成します。

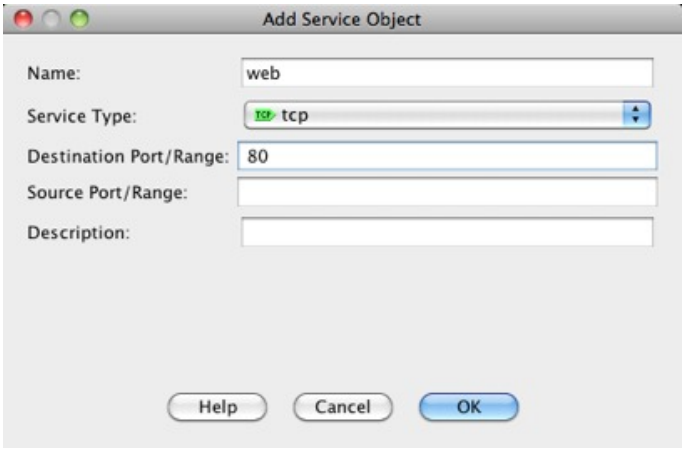
ステップ 6 （オプション）サービス変換の送信元サービス ポートまたは宛先サービス ポートを識別します。

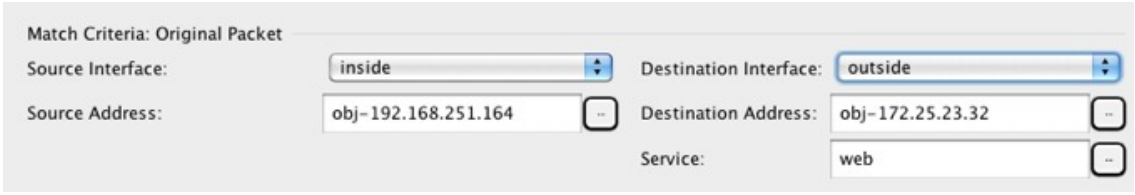
- 元のパケットの送信元ポートまたは宛先ポート（実際の送信元ポート**または**マッピング宛先ポート）を識別します。[Match Criteria: Original Packet] > [Service] について、参照ボタンをクリックしてポートを指定する既存のサービス オブジェクトを選択するか、[Browse Original Service] ダイアログボックスから新しいオブジェクトを作成します。
- 変換されたパケットの送信元ポートまたは宛先ポート（マッピング送信元ポート**または**実際の宛先ポート）を識別します。[Action: Original Packet] > [Service] について、参照ボタンをクリックしてポートを指定する既存のサービス オブジェクトを選択するか、[Browse Translated Service] ダイアログボックスから新しいオブジェクトを作成します。

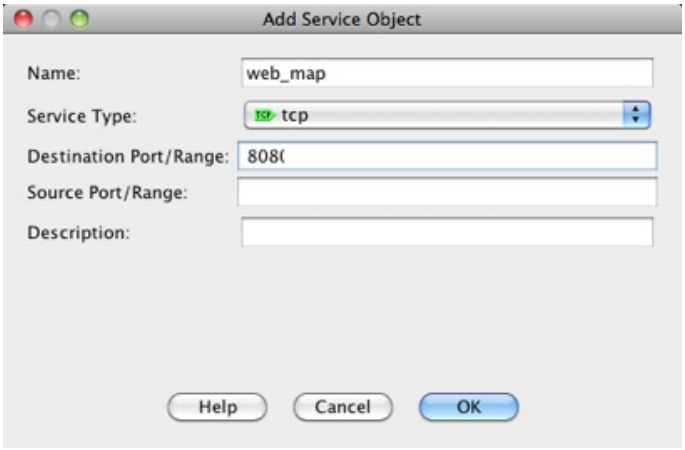
サービス オブジェクトは、送信元ポートと宛先ポートの両方を含むことができます。実際のサービス オブジェクトとマッピング サービス オブジェクトの両方に、送信元ポートまたは宛先ポートのいずれかを指定する必要があります。ご使用のアプリケーションが固定の送信元ポートを使用する場合（一部の DNS サーバーなど）に送信元ポートおよび宛先ポートの両方を指定する必要がありますが、固定の送信元ポートはめったに使用されません。オブジェクト

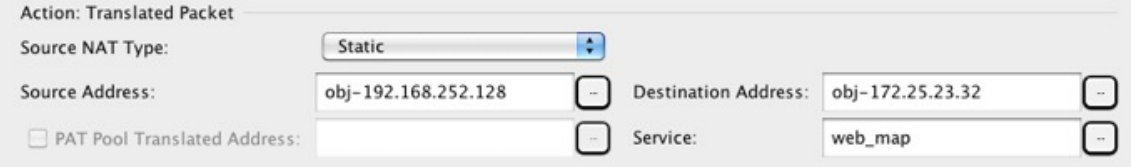
で送信元ポートと宛先ポートの両方を指定することはほとんどありませんが、この場合には、元のパケットのサービス オブジェクトに実際の送信元ポート/マッピングされた宛先ポートが含まれます。変換されたパケットのサービス オブジェクトには、マッピングされた送信元ポート/実際の宛先ポートが含まれます。ポートを変換する場合、実際のサービス オブジェクトのプロトコルとマッピング サービス オブジェクトのプロトコルの両方を同じにします（たとえば両方とも TCP にします）。アイデンティティ NAT では、実際のポートとマッピングポートの両方に同じサービスオブジェクトを使用できます。「not equal（等しくない）」（**!=**）演算子はサポートされていません。

次に例を示します。



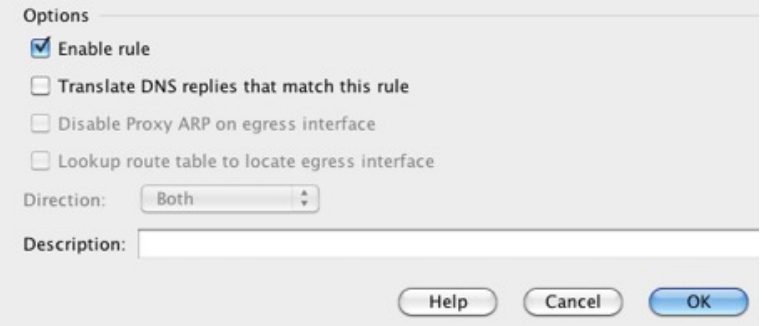






ステップ 7 （任意）NAT46 の場合、[Use one-to-one address translation] チェック ボックスをオンにします。NAT 46 の場合、最初の IPv4 アドレスを最初の IPv6 アドレス、2 番目の IPv4 アドレスを 2 番目の IPv6 アドレス、以下同様に 1 対 1 で順に変換するように指定します。このオプションを指定しない場合は、IPv4 埋め込み方式が使用されます。1 対 1 変換の場合は、このキーワードを使用する必要があります。

ステップ 8 （任意）[Options] 領域で NAT オプションを設定します。



- [Enable rule]：この NAT ルールをイネーブルにします。このルールはデフォルトでイネーブルになっています。
- （送信元専用ルールの場合）[Translate DNS replies that match this rule]：DNS 応答内の DNS A レコードを書き換えます。DNS インスペク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 修正は設定できません。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。
- [Disable Proxy ARP on egress 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 をディセーブルにします。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。
- [Direction]：ルールを単方向にするには、[Unidirectional] を選択します。デフォルトは [Both] です。ルールを単方向にすると、宛先アドレスが実際のアドレスへの接続を開始するのを回避できます。
- [Description]：ルールに関する説明を 200 文字以内で追加します。

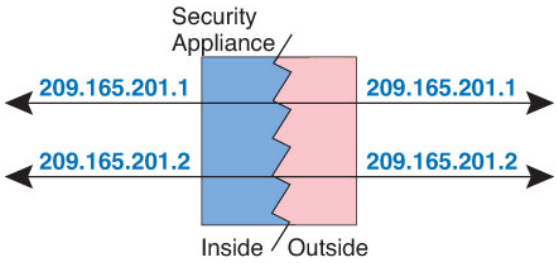
ステップ 9 [OK] をクリックし、続いて [Apply] をクリックします。

アイデンティティ NAT

NAT 設定では、IP アドレスを自身に変換する必要がある場合があります。たとえば、すべてのネットワークに NAT を適用する広範なルールを作成し、1 つのネットワークを NAT から除外したい場合、スタティック NAT ルールを作成してそのネットワーク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、クライアント トラフィックを NAT から除外する必要のあるリモート アクセス VPN の場合に必須です。

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 新規または既存のネットワーク オブジェクトに NAT を追加します。

- 新しいネットワーク オブジェクトを追加するには、[Configuration] > [Firewall] > [NAT Rules] を選択し、[Add] > [Add Network Object NAT Rule] をクリックします。
- 既存のネットワーク オブジェクトに NAT を追加するには、[Configuration] > [Firewall] > [Objects] > [Network Objects/Groups] を選択し、ネットワーク オブジェクトを編集します。

ステップ 2 新しいオブジェクトの場合は、次のフィールドに値を入力します。

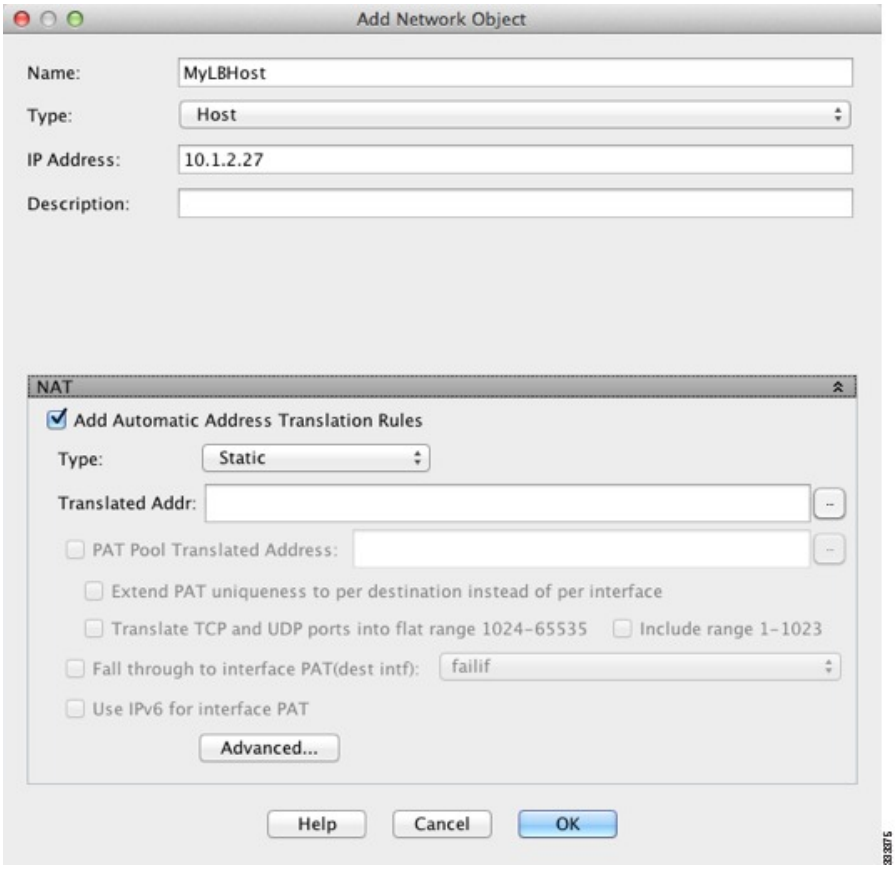
- [Name]：オブジェクト名。a ～ z、A ～ Z、0 ～ 9、ピリオド、ハイフン、カンマ、またはアンダースコアの文字を使用してください。名前は 64 文字以下にする必要があります。
- [Type]：ホスト、ネットワーク、または範囲。
- [IP Addresses]：IPv4 または IPv6 アドレス。ホストの場合は単一のアドレスを、範囲の場合は開始アドレスと終了アドレスを、サブネットの場合は IPv4 ネットワーク アドレスお

よびマスク（たとえば、10.100.10.0 255.255.255.0）または IPv6 アドレスおよびプレフィックス長（たとえば、2001:DB8:0:CD30::/60）を入力します。

ステップ 3 [NAT] セクションが表示されていない場合は、[NAT] をクリックしてセクションを展開します。

ステップ 4 [Add Automatic Translation Rules] チェックボックスをオンにします。

ステップ 5 [Type] ドロップダウン リストから、[Static] を選択します。



ステップ 6 [Translated Addr] フィールドで、次のいずれかの操作を行います。

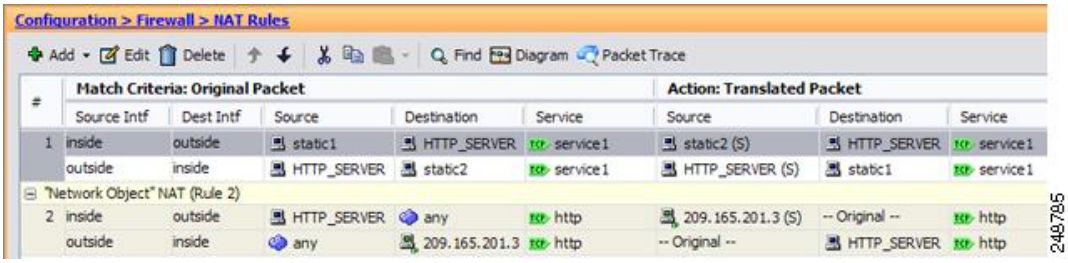
- ホストオブジェクトの場合は、同じアドレスを入力します。範囲オブジェクトの場合は、実際の範囲における最初のアドレスを入力します（範囲内の同じ数のアドレスが使用されます）。サブネットオブジェクトの場合は、実際のサブネット内にある任意のアドレスを入力します（サブネット内のすべてのアドレスが使用されます）。
- 参照ボタンをクリックし、ネットワーク オブジェクトを選択します（または新しいネットワーク オブジェクトを作成します）。アドレスの範囲にアイデンティティ NAT を設定するときは、このオプションを使用します。

ステップ 7 （任意）[Advanced] をクリックし、[Advanced NAT Settings] ダイアログボックスで次のオプションを設定して [OK] をクリックします。

- [Translate DNS replies for rule]：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。
- [Disable Proxy ARP on egress 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 をディセーブルにします。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。
- （ルーテッドモード、インターフェイスを指定）[Lookup route table to locate egress interface]：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。
- （ブリッジ グループ メンバーのインターフェイスに必要）[Interface]：この NAT ルールを適用する実際のインターフェイス（**送信元**）およびマッピング インターフェイス（**宛先**）を指定します。デフォルトでは、ルールはブリッジ グループ メンバーを除くすべてのインターフェイスに適用されます。
- [Service]：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。

ステップ 8 [OK]、続いて [Apply] をクリックします。

スタティック ルールが二方向である（開始を実際のホストの間で許可する）ため、ルート ルックアップ オプションを選択しない限り、NAT ルール テーブルは各スタティック ルールに対して、各方向に 1 つずつ 2 つの行を表示します。



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。

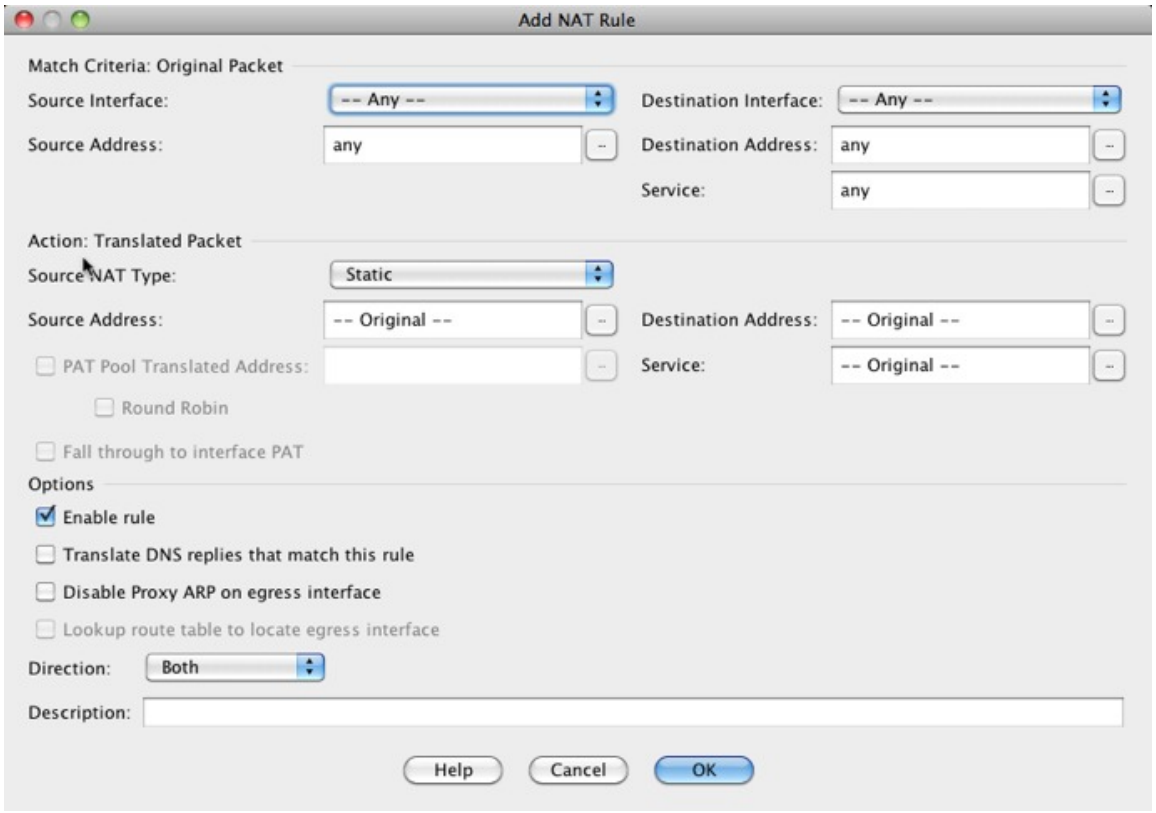
手順

ステップ 1 **[Configuration]** > **[Firewall]** > **[NAT Rules]** を選択して、次のいずれかを実行します。

- [Add] または [Add] > [Add NAT Rule Before Network Object NAT Rules] をクリックします。
- [Add] > [Add NAT Rule After Network Object NAT Rules] をクリックします。

- Twice NAT ルールを選択して [Edit] をクリックします。

[Add NAT Rule] ダイアログボックスが表示されます。

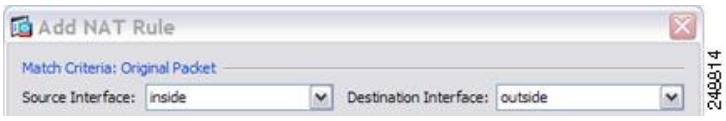


ステップ 2 （ブリッジ グループ メンバーのインターフェイスに必要）送信元インターフェイスおよび宛先インターフェイスを設定します。

ルーテッドモードでは、デフォルトは送信元と宛先の両方のインターフェイスです。いずれかまたは両方のオプションに、特定のインターフェイスを選択できます。ただし、ブリッジ グループ メンバーのインターフェイスにルールを記述するときに、インターフェイスを選択する必要があります。「any」にはこれらのインターフェイスが含まれていません。

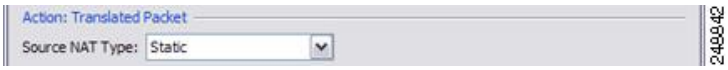
a) [Match Criteria: Original Packet] > [Source Interface] ドロップダウンリストから、送信元インターフェイスを選択します。

b) [Match Criteria: Original Packet] > [Destination Interface] ドロップダウンリストから、宛先インターフェイスを選択します。

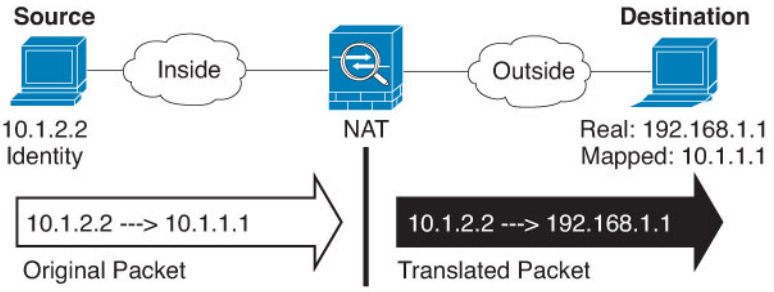


ステップ 3 **[Action: Translated Packet]** > **[Source NAT Type]** ドロップダウンリストから、[Static] を選択します。[Static] がデフォルトの設定です。

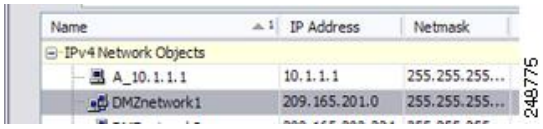
この設定は送信元アドレスにのみ適用されます。宛先の変換は常にスタティックになります。



ステップ 4 パケットの元の IPv4 または IPv6 のアドレス、つまり、送信元インターフェイス ネットワーク上に出現するときのパケットのアドレス（実際の送信元アドレスとマッピング宛先アドレス）を識別します。元のパケットと変換されたパケットの例については、次の図を参照してください。ここでは、内部ホストでアイデンティティ NAT を実行しますが、外部ホストを変換します。



a) [Match Criteria: Original Packet] > [Source Address] について、参照ボタンをクリックして既存のネットワーク オブジェクトまたはグループを選択するか、[Browse Original Source Address] ダイアログボックスから新しい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。デフォルトは **any** です。このオプションは、マッピング アドレスも **any** に設定する場合にのみ使用します。



b) （任意）[Match Criteria: Original Packet] > [Destination Address] について、参照ボタンをクリックして既存のネットワーク オブジェクト、グループ、またはインターフェイスを選択するか、[Browse Original Destination Address] ダイアログボックスから新しいオブジェクトまたはグループを作成します。

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。

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、インターフェイスを選択します。インターフェイスを指定する場合は、必ずサービス変換も設定します。詳細については、ポート変換を設定したスタティック NAT （51 ページ）を参照してください。

ステップ 5 変換されたパケット アドレスを識別します。つまり、宛先インターフェイス ネットワークに表示されるパケット アドレス（マッピング送信元アドレスと実際の宛先アドレス）です。

a) [Action: Translated Packet] > [Source Address] について、参照ボタンをクリックして [Browse Translated Source Address] ダイアログボックスから実際の送信元アドレスに選択したものと同じネットワーク オブジェクトまたはグループを選択します。実際のアドレスに **any** を指定した場合は **any** を使用します。

b) [Match Criteria: Translated Packet] > [Destination Address] について、参照ボタンをクリックして既存のネットワーク オブジェクトまたはグループを選択するか、[Browse Translated Destination Address] ダイアログボックスから新しいオブジェクトまたはグループを作成します。

宛先アドレスのアイデンティティ 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。

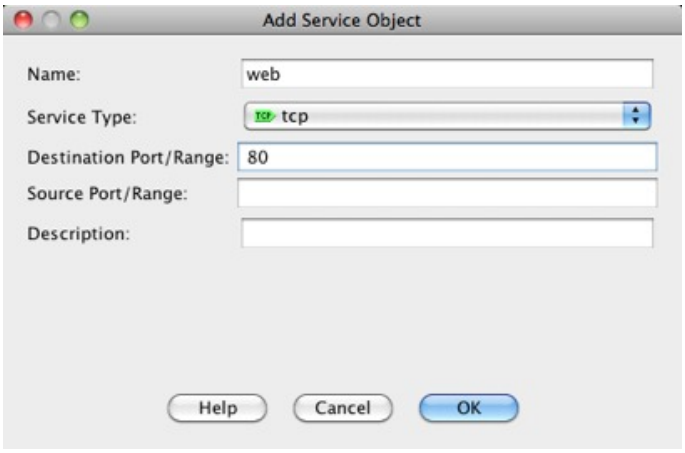
宛先アドレスを変換する場合、スタティック マッピングは、通常 1 対 1 です。したがって、実際のアドレスとマッピング アドレスの数は同じです。ただし、必要に応じて異なる数にすることができます。詳細については、スタティック NAT （51 ページ）を参照してください。拒否されるマッピング IP アドレスについては、NAT のガイドライン （8 ページ）を参照してください。

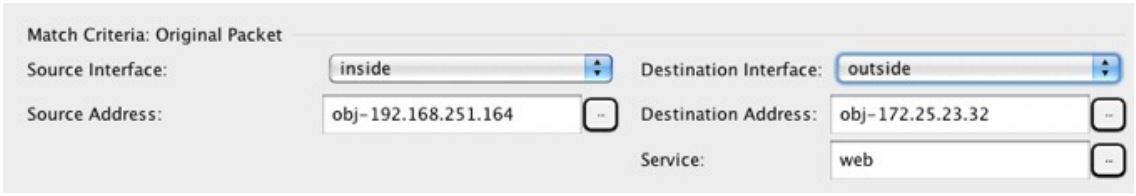
ステップ 6 （オプション）サービス変換の送信元サービス ポートまたは宛先サービス ポートを識別します。

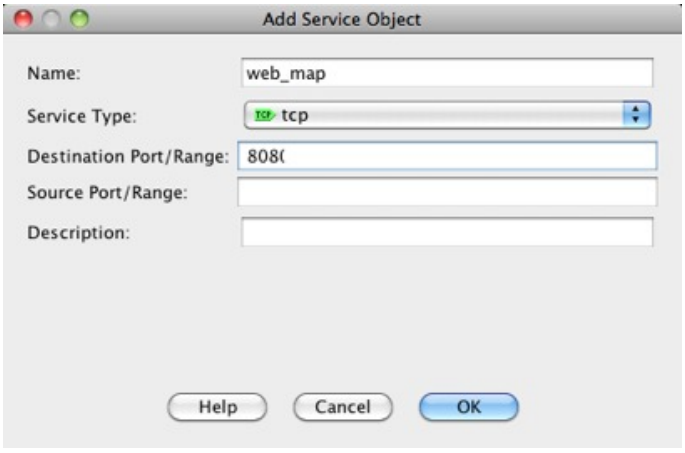
- 元のパケットの送信元ポートまたは宛先ポート（実際の送信元ポート**または**マッピング宛先ポート）を識別します。[Match Criteria: Original Packet] > [Service] について、参照ボタンをクリックしてポートを指定する既存のサービス オブジェクトを選択するか、[Browse Original Service] ダイアログボックスから新しいオブジェクトを作成します。
- 変換されたパケットの送信元ポートまたは宛先ポート（マッピング送信元ポート**または**実際の宛先ポート）を識別します。[Action: Original Packet] > [Service] について、参照ボタンをクリックしてポートを指定する既存のサービス オブジェクトを選択するか、[Browse Translated Service] ダイアログボックスから新しいオブジェクトを作成します。

サービス オブジェクトは、送信元ポートと宛先ポートの両方を含むことができます。実際のサービス オブジェクトとマッピング サービス オブジェクトの両方に、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 サーバーなど）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。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、元のパケットのサービス 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。変換されたパケットのサービス 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。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）。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。「not equal（等しくない）」（**!=**）演算子はサポートされていません。

次に例を示します。

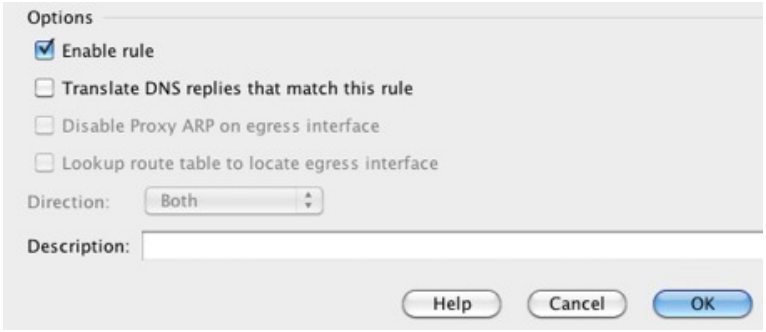








ステップ 7 （任意）[Options] 領域で NAT オプションを設定します。



- [Enable rule]：この NAT ルールをイネーブルにします。このルールはデフォルトでイネーブルになっています。
- （送信元専用ルールの場合）[Translate DNS replies that match this rule]：宛先アドレスを設定しない場合でもこのオプションを使用できますが、アドレスをそれ自身に変換しているので DNS 応答に修正が必要ないため、このオプションはアイデンティティ NAT には適用されません。
- [Disable Proxy ARP on egress 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 をディセーブルにします。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。
- （ルーテッドモード、インターフェイスを指定）[Lookup route table to locate egress interface]：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。
- [Direction]：ルールを単方向にするには、[Unidirectional] を選択します。デフォルトは [Both] です。ルールを単方向にすると、トラフィックが実際のアドレスへの接続を開始するのを回避できます。この設定は、テストのために使用する場合があります。
- [Description]：ルールに関する説明を 200 文字以内で追加します。

ステップ 8 [OK] をクリックし、続いて [Apply] をクリックします。

NAT のモニタリング

次のページから NAT に関するグラフを表示できます。

- [Monitoring] > [Properties] > [Connection Graphs] > [Xlates]：使用中の xlate および最も使用されている xlate を表示するには、[Xlate Utilization] グラフを選択します。これは、show xlate コマンドと同等です。
- [Monitoring] > [Properties] > [Connection Graphs] > [Perfmon]：NAT のパフォーマンス情報を表示するには、[Xlate Perfmon] グラフを選択します。これは、show perfmon コマンドからの xlate 情報と同等です。

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。 次の画面が導入または変更されました。 [Configuration] > [Firewall] > [NAT Rules] [Configuration] > [Firewall] > [Objects] > [Network Objects/Groups]
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。 次の画面が変更されました。[Configuration] > [Firewall] > [NAT Rules]。

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)	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。 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（**nat 0 access-list** 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 **no-proxy-arp** およびルート ルックアップを使用するキーワード **route-lookup** があります。8.3(2) および 8.4(1) への移行に使用された **unidirectional** 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 **no-proxy-arp** キーワードと **route-lookup** キーワードが含まれるようになっています。**unidirectional** キーワードは削除されました。 その次の画面が変更されました。[Configuration] > Firewall] > [NAT Rules] > [Add/Edit Network Object] > [Advanced NAT Settings]、[Configuration] > [Firewall] > [NAT Rules] > [Add/Edit NAT Rule]。

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)	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。 その次の画面が変更されました。[Configuration] > Firewall] > [NAT Rules] > [Add/Edit Network Object]、[Configuration] > [Firewall] > [NAT Rules] > [Add/Edit NAT Rule]。
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)	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。 変更された画面はありません。 この機能は、*8.5(1)* または *8.6(1)* では使用できません。
PAT プールの PAT ポートのフラットな範囲	8.4(3)	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。 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。 その次の画面が変更されました。[Configuration] > Firewall] > [NAT Rules] > [Add/Edit Network Object]、[Configuration] > [Firewall] > [NAT Rules] > [Add/Edit NAT Rule]。 この機能は、*8.5(1)* または *8.6(1)* では使用できません。

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)	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。 その次の画面が変更されました。[Configuration] > Firewall] > [NAT Rules] > [Add/Edit Network Object]、[Configuration] > [Firewall] > [NAT Rules] > [Add/Edit NAT Rule]。 この機能は、*8.5(1)* または *8.6(1)* では使用できません。

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)	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、内部サーバー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。 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**show nat** コマンドを使用して表示できます。 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。 • Cisco IPsec および AnyConnect クライアント のみがサポートされます。 • 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。 • 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）。 • ローミング（パブリック IP 変更）はサポートされません。 ASDM ではこのコマンドはサポートされません。コマンドライン ツールを使用してコマンドを入力してください。

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)	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。 次の画面が変更されました。[Configuration] > [Firewall] > [Objects] > [Network Objects/Group]、[Configuration] > [Firewall] > [NAT Rules]。
逆引き DNS ルックアップ用の NAT のサポート	9.0(1)	NAT ルールがイネーブルにされた DNS インスペクションを使用する 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。
Per-Session PAT	9.0(1)	Per-session PAT 機能によって PAT の拡張性が向上し、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、制御ユニットに転送して制御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）。「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。 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。 次の画面が変更されました。[Configuration] > [Firewall] > [Advanced] > [Per-Session NAT Rules]。

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)	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。 [Configuration] > [Device Management] > [Advanced] > [Rule Engine] 画面に NAT が追加されました。
キャリア グレード NAT の拡張	9.5(1)	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）。 **[Configuration] > [Firewall] > [Advanced] > [PAT Port Block Allocation]** コマンドが追加されました。[Enable Block Allocation] オブジェクト NAT および Twice NAT ダイアログボックスが追加されました。
SCTP に対する NAT サポート	9.5(2)	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。 次の画面が変更されました：**[Configuration] > [Firewall] > [NAT]** 追加/編集スタティック ネットワーク オブジェクト NAT ルール、[Advanced NAT Settings] ダイアログボックス。
NAT のポート ブロック割り当てに対する暫定ログ	9.12(1)	NAT のポートブロックの割り当てを有効にすると、ポートブロックの作成および削除中にシステムで syslog メッセージが生成されます。暫定ログの記録を有効にすると、指定した間隔でメッセージ 305017 が生成されます。メッセージは、その時点で割り当てられているすべてのアクティブ ポート ブロックをレポートします（プロトコル（ICMP、TCP、UDP）、送信元および宛先インターフェイス、IP アドレス、ポート ブロックを含む）。 次の画面が変更されました。**[構成（Configuration）] > [ファイアウォール（Firewall）] > [詳細設定（Advanced）] > [PATのポート ブロック割り当て（PAT Port Block Allocation）]**。

機能名	プラットフォームリリース	説明
クラスタリングでの PAT アドレス割り当ての変更。PAT プールの **flat** オプションがデフォルトで有効になり、設定できなくなりました。	9.15(1)	PAT アドレスがクラスタのメンバーに配布される方法が変更されます。以前は、アドレスはクラスタのメンバーに配布されていたため、PAT プールにはクラスタメンバーごとに少なくとも 1 つのアドレスが必要でした。制御ユニットは各 PAT プールアドレスを等しいサイズのポートブロックに分割し、それらをクラスタメンバーに配布するようになりました。各メンバーには、同じPATアドレスのポートブロックがあります。したがって、通常 PAT に必要な接続量に応じて、PAT プールのサイズを 1 つの IP アドレスにまで減らすことができます。ポートブロックは、1024 ～ 65535 の範囲で 512 ポートのブロック単位で割り当てられます。オプションで、PAT プールルールを設定するときに、このブロック割り当てに予約ポート 1 ー 1023 を含めることができます。たとえば、単一ノードでは PAT プール IP アドレスあたり 65535 個の接続すべてを処理するのに対し、4 ノードクラスタでは、各ノードは 32 個のブロックを取得し、PAT プール IP アドレスあたり 16384 個の接続を処理できます。 この変更の一環として、スタンドアロンまたはクラスタ内での動作に関わりなく、すべてのシステムの PAT プールは、フラットなポート範囲 1023 ー 65535 を使用できるようになりました。以前は、**flat** オプションを PAT プールルールに含めることで、フラットな範囲をオプションで使用できました。**flat** キーワードはサポートされなくなりました。PAT プールは常にフラットになります。**include-reserve** キーワードは、以前は **flat** のサブキーワードでしたが、PAT プール構成内の独立したキーワードになりました。このオプションを使用すると、PAT プール内に 1 ー 1023 のポート範囲を含めることができます。 ポートブロック割り当てを設定する（**block-allocation** PAT プールオプション）と、デフォルトの 512 ポートブロックではなく、独自のブロック割り当てサイズが使用されます。また、クラスタ内のシステムの PAT プールに拡張 PAT を設定することはできません。 新規/変更された画面：[NAT PAT Pool configuration]

機能名	プラットフォームリリース	説明
システム定義の NAT ルールの新しいセクション 0。	9.16(1)	新しいセクション 0 が NAT ルールテーブルに追加されました。このセクションは、システムの使用に限定されます。システムが正常に機能するために必要なすべての NAT ルールがこのセクションに追加され、これらのルールは作成したルールよりも優先されます。以前は、システム定義のルールがセクション 1 に追加され、ユーザー定義のルールがシステムの適切な機能を妨げる可能性がありました。セクション 0 のルールを追加、編集、または削除することはできませんが、**show nat detail** コマンド出力に表示されます。

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