CHAPTER 6

ネットワーク オブジェクト NAT（ASA 8.3 以降）

ネットワーク オブジェクトのパラメータとして設定されているすべての NAT ルールは、*ネットワーク オブジェクト NAT* ルールと見なされます。ネットワーク オブジェクト NAT は、1 つの IP アドレス、アドレスの範囲、またはサブネットに対して NAT を設定するための迅速かつ容易な方法です。ネットワーク オブジェクトを設定したら、このオブジェクトのマッピング アドレスを識別できます。

この章では、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。この章は、次の項で構成されています。

（注） NAT の機能の詳細については、第 5 章「ネットワーク アドレス変換（NAT）（ASA 8.3 以降）」を参照してください。

ネットワーク オブジェクト NAT に関する情報

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

ルールがペアになることはありません。したがって、宛先 X に向かう場合は送信元アドレスが A と変換され、宛先 Y に向かう場合は B と変換さ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 を使用します（Twice NAT を使用すると、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 とネットワーク オブジェクト NAT の違いの詳細については、「NAT の実装方法」（P.5-15）を参照してください。

ネットワーク オブジェクト NAT ルールは、NAT ルール テーブルのセクション 2 に追加されます。NAT の順序付けの詳細については、「NAT ルールの順序」（P.5-20）を参照してください。

ネットワーク オブジェクト NAT のライセンス要件

次の表に、この機能のライセンス要件を示します。

モデル	ライセンス要件
ASAv	標準または Premium ライセンス
他のすべてのモデル	基本ライセンス

ネットワーク オブジェクト NAT の前提条件

コンフィギュレーションによっては、必要に応じてマッピング アドレスをインラインで設定したり、マッピング アドレスの別のネットワーク オブジェクトまたはネットワーク オブジェクト グループを作成したりできます。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。ネットワーク オブジェクトまたはグループを作成するには、『一般的な操作のコンフィギュレーション ガイド』を参照してください。

オブジェクトおよびグループに関する特定のガイドラインについては、設定する NAT タイプの設定の項を参照してください。「ガイドラインと制限事項」（P.6-2）も参照してください。

ガイドラインと制限事項

コンテキスト モードのガイドライン

シングル コンテキスト モードとマルチ コンテキスト モードでサポートされています。

ファイアウォール モードのガイドライン

- ルーテッド ファイアウォール 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。
- トランスペアレント モードでは、実際のインターフェイスおよびマッピング インターフェイスを指定する必要があります。--Any-- は使用できません。
- トランスペアレント モードでは、インターフェイス PAT を設定できません。トランスペアレント モードのインターフェイスには、IP アドレスが設定されていないためです。管理 IP アドレスもマッピング アドレスとして使用できません。
- トランスペアレント モードでは、IPv4 ネットワークと IPv6 ネットワークとの間の変換はサポートされていません。2 つの IPv6 ネットワーク間、または 2 つの IPv4 ネットワーク間の変換がサポートされます。

IPv6 のガイドライン

- IPv6 をサポートします。「NAT と IPv6」（P.5-15）も参照してください。
- ルーテッド モードの場合は、IPv4 と IPv6 との間の変換もできます。
- トランスペアレント モードの場合は、IPv4 ネットワークと IPv6 ネットワークとの間の変換はサポートされていません。2 つの IPv6 ネットワーク間、または 2 つの IPv4 ネットワーク間の変換がサポートされます。
- トランスペアレント モードの場合は、PAT プールは IPv6 に対してはサポートされません。
- 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。

その他のガイドライン

- 定義できる NAT ルールは 1 つのオブジェクトに対して 1 つだけです。1 つの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、複数のオブジェクトを作成する必要があります。それぞれに異なる名前を付け、IP アドレスは同じものを指定します。たとえば、**object network obj-10.10.10.1-01**、**object network obj-10.10.10.1-02** などとします。
- NAT コンフィギュレーションを変更したときに、既存の変換がタイムアウトするまで待たずに新しい NAT コンフィギュレーションが使用されるようにするには、**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。

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

- NAT で使用されるオブジェクトおよびオブジェクト グループを未定義にすることはできません。IP アドレスを含める必要があります。
- 1 つのオブジェクト グループに IPv4 と IPv6 の両方のアドレスを入れることはできません。オブジェクト グループには、1 つのタイプのアドレスだけが含まれている必要があります。
- 同じマッピング オブジェクトやグループを複数の NAT ルールで使用できます。
- マッピング IP アドレス プールは、次のアドレスを含むことができません。
  - マッピング インターフェイスの IP アドレス。ルールに --Any-- インターフェイスを指定すると、すべてのインターフェイスの IP アドレスが拒否されます。インターフェイス PAT（ルーテッド モードのみ）の場合、IP アドレスの代わりにインターフェイス名を使用します。
  - （トランスペアレント モード）管理 IP アドレス。
  - （ダイナミック NAT）VPN がイネーブルの場合は、スタンバイ インターフェイスの IP アドレス。
  - 既存の VPN プールのアドレス。

- スタティックおよびダイナミック NAT ポリシーでは重複アドレスを使用しないでください。たとえば、重複アドレスを使用すると、PPTP のセカンダリ接続がダイナミック xlate ではなくスタティックにヒットした場合、PPTP 接続の確立に失敗する可能性があります。
- NAT や PAT に伴うアプリケーション インスペクションの制限については、第 8 章「アプリケーション レイヤ プロトコル インスペクションの準備」の「デフォルト インスペクションと NAT に関する制限事項」（P.8-6）を参照してください。

デフォルト設定

- （ルーテッド モード）デフォルトの実際のインターフェイスおよびマッピング インターフェイスは Any で、すべてのインターフェイスにルールが適用されます。
- （8.3(1)、8.3(2)、8.4(1)）アイデンティティ NAT のデフォルト動作で、プロキシ ARP はディセーブルにされます。これは設定できません。（8.4(2) 以降）アイデンティティ NAT のデフォルト動作で、プロキシ ARP はイネーブルにされ、他のスタティック NAT ルールと一致します。必要に応じてプロキシ ARP をディセーブルにできます。詳細については、「NAT パケットのルーティング」（P.5-22）を参照してください。
- オプションのインターフェイスを指定する場合、ASA によって NAT コンフィギュレーションが使用されて、出力インターフェイスが決定されます。（8.3(1) ～ 8.4(1)）唯一の例外はアイデンティティ NAT です。アイデンティティ NAT では、NAT コンフィギュレーションに関係なく、常にルート ルックアップが使用されます。（8.4(2) 以降）アイデンティティ NAT の場合、デフォルト動作は NAT コンフィギュレーションの使用ですが、代わりにルート ルックアップを常に使用するオプションがあります。詳細については、「NAT パケットのルーティング」（P.5-22）を参照してください。

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 を設定する方法について説明します。

- 「ダイナミック NAT または PAT プールを使用したダイナミック PAT の設定」（P.6-4）
- 「ダイナミック PAT（隠蔽）の設定」（P.6-10）
- 「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 の設定」（P.6-13）
- 「アイデンティティ NAT の設定」（P.6-17）
- 「Per-Session PAT ルールの設定」（P.6-20）

ダイナミック NAT または PAT プールを使用したダイナミック PAT の設定

この項では、ダイナミック NAT または PAT プールを使用するダイナミック PAT のためのネットワーク オブジェクト NAT を設定する方法について説明します。詳細については、「ダイナミック NAT」（P.5-8）または「ダイナミック PAT」（P.5-10）を参照してください。

ガイドライン

PAT プールの場合：

- 使用できる場合、実際の送信元ポート番号がマッピング ポートに対して使用されます。ただし、実際のポートが使用 できない 場合は、デフォルトで、マッピング ポートは実際のポート番号と同じポート範囲（0 ～ 511、512 ～ 1023、および 1024 ～ 65535）から選択されます。したがって、1024 未満のポートに使用できるのは、小さな PAT プール 1 つだけです。（8.4(3) 以降、8.5(1) または 8.6(1) を除く）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 プールに対して、サイズが異なる 3 つの層の代わりにフラットなポート範囲を使用するように指定できます。1024 ～ 65535 または 1 ～ 65535 です。
- 同じ PAT プール オブジェクトを 2 つの異なるルールの中で使用する場合は、必ず同じオプションを各ルールに指定してください。たとえば、1 つのルールで拡張 PAT およびフラットな範囲が指定される場合は、もう一方のルールでも拡張 PAT およびフラットな範囲が指定される必要があります。

PAT プールに対する拡張 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、第 8 章「アプリケーション レイヤ プロトコル インスペクションの準備」の「デフォルト インスペクションと NAT に関する制限事項」（P.8-6）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は、PAT プール内のアドレスを、ポート変換ルールを設定した別のスタティック 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、ポート変換ルールを設定したスタティック NAT は作成できません。
- PAT プールを使用し、フォールバックのインターフェイスを指定する場合、拡張 PAT を使用できません。
- ICE または TURN を使用する VoIP 配置では、拡張 PAT を使用しないでください。ICE および TURN は、すべての宛先に対して同じであるために PAT バインディングに依存しています。

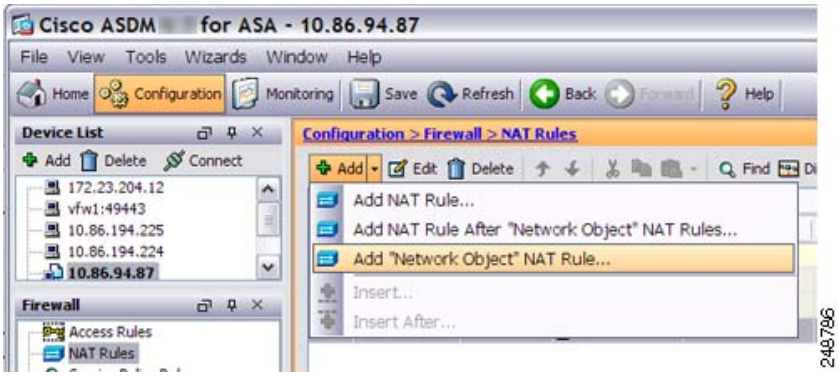
PAT プールのラウンドロビンの場合：

- 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）。**注**：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。ASA 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。
- 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。

手順の詳細

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 オブジェクトをダブルクリックします。

詳細については、『一般的な操作のコンフィギュレーション ガイド』を参照してください。

[Add/Edit Network Object] ダイアログボックスが表示されます。

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。

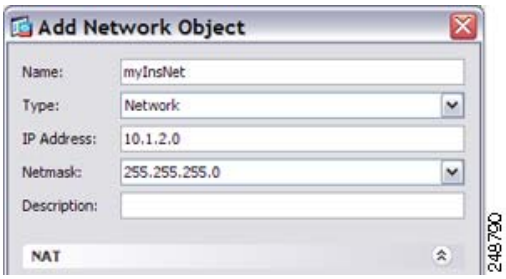
a. [Name]：オブジェクト名。a ～ z、A ～ Z、0 ～ 9、ピリオド、ハイフン、カンマ、またはアンダースコアの文字を使用してください。名前は 64 文字以下にする必要があります。

b. [Type]：ホスト、ネットワーク、または範囲。

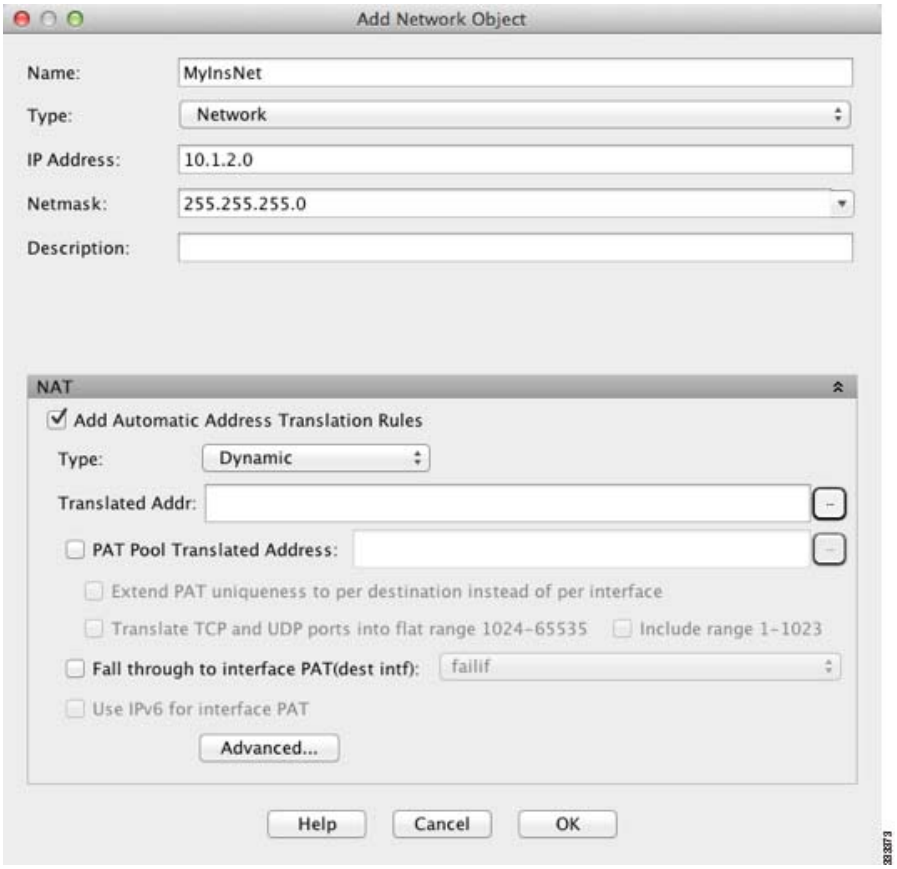
c. [IP Address] : IPv4 または IPv6 アドレス。オブジェクト タイプとして [Range] を選択した場合は、[IP Address] フィールドは、開始アドレスと終了アドレスを入力できるように変更されます。

d. [Netmask/Prefix Length]：サブネット マスクまたはプレフィックス長を入力します。

e. [Description]：（オプション）ネットワーク オブジェクトの説明（最大 200 文字）。



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。

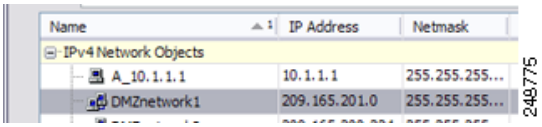


ステップ 4　[Add Automatic Translation Rules] チェックボックスをオンにします。

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。PAT プールを使用するダイナミック PAT を設定する場合であっても、[Dynamic] を選択してください。

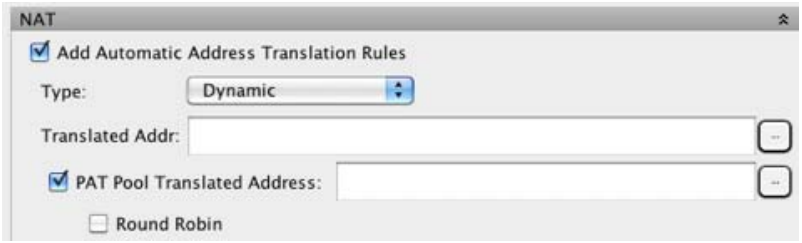
ステップ 6　ダイナミック NAT、または PAT プールを使用するダイナミック PAT を設定します。

- ダイナミック NAT：[Translated Addr] フィールドの右の参照ボタンをクリックし、[Browse Translated Addr] ダイアログボックスで、既存のネットワーク オブジェクトを選択するか新しいオブジェクトを作成します。



（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。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。

- PAT プールを使用したダイナミック PAT：フォールバックの PAT プールを有効にします。



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、[Browse Translated PAT Pool Address] ダイアログボックスで既存のネットワーク オブジェクトを選択するか新しいネットワーク オブジェクトを作成します。

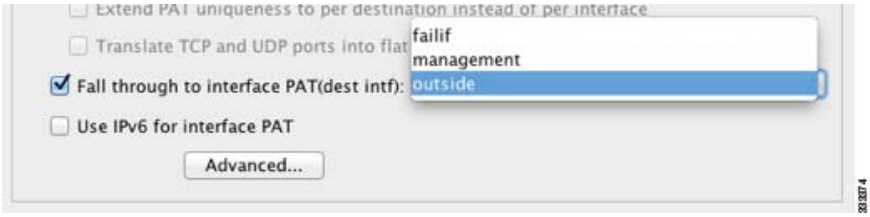
（注）　PAT プール オブジェクトまたはグループには、サブネットを含むことはできません。IPv4 アドレスと IPv6 アドレスの両方をグループに入れることはできません。1 つのタイプだけが含まれている必要があります。

c. （オプション）アドレス/ポートをラウンドロビン方式で割り当てるには、[Round Robin] チェックボックスをオンにします。デフォルトではラウンドロビンは使用されず、1 つの PAT アドレスのポートがすべて割り当てられると次の PAT アドレスが使用されます。ラウンドロビン方式では、プール内の各 PAT アドレスから 1 つずつアドレス/ポートが割り当てられると最初のアドレスに戻り、次に 2 番目のアドレスというように順に使用されます。

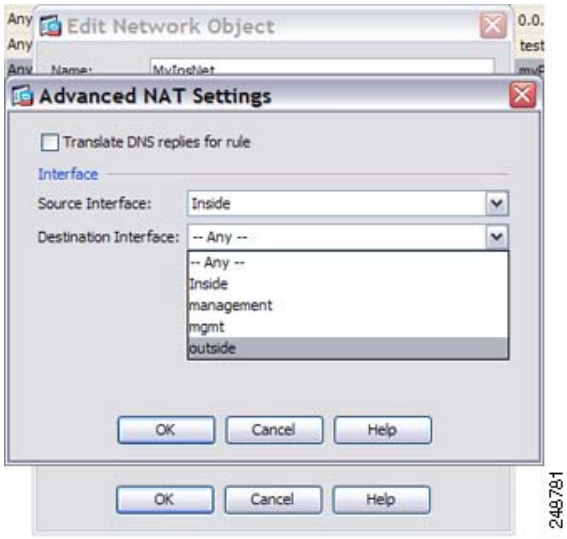
d. （任意、8.4(3) 以降、ただし 8.5(1) と 8.6(1) を除く）拡張 PAT を使用する場合は、[Extend PAT uniqueness to per destination instead of per interface] チェックボックスをオンにします。拡張 PAT では、変換情報の宛先アドレスとポートを含め、IP アドレスごとではなく、*サービス*ごとに 65535 個のポートが使用されます。通常は、PAT 変換を作成するときに宛先ポートとアドレスは考慮されないため、PAT アドレスごとに 65535 個のポートに制限されます。たとえば、拡張 PAT を使用して、192.168.1.7:23 に向かう場合の 10.1.1.1:1027 の変換、および 192.168.1.7:80 に向かう場合の 10.1.1.1:1027 の変換を作成できます。

e. （任意、8.4(3) 以降、ただし 8.5(1) と 8.6(1) を除く）ポートを割り当てるときに 1024 ～ 65535 のポート範囲を 1 つのフラット範囲として使用するには、[Translate TCP or UDP ports into flat range (1024-65535)] チェックボックスをオンにします。変換のマッピング ポート番号を選択するときに、ASA によって、使用可能な場合は実際の送信元ポート番号が使用されます。ただし、このオプションを設定しないと、実際のポートが使用 *できない* 場合は、デフォルトで、マッピング ポートは実際のポート番号と同じポート範囲（1 ～ 511、512 ～ 1023、および 1024 ～ 65535）から選択されます。下位範囲でポートが不足するのを回避するには、この設定を行います。1 ～ 65535 の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。

ステップ 7　（任意、ルーテッド モードのみ）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　（オプション）[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、「DNS および NAT」（P.5-32）を参照してください。
- （トランスペアレント ファイアウォール モードの場合に必須）[Source Interface]：この NAT ルールを適用する実際のインターフェイスを指定します。デフォルトでは、ルールは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 ファイアウォール モードの場合に必須）[Destination Interface]：この NAT ルールが適用されるマッピング インターフェイスを指定します。デフォルトでは、ルールはすべてのインターフェイスに適用されます。

入力が終わったら、[OK] をクリックします。[Add/Edit Network Object] ダイアログボックスに戻ります。

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

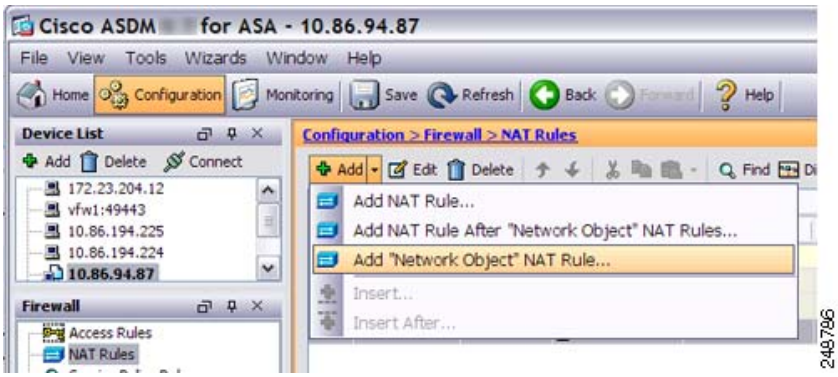
ダイナミック PAT（隠蔽）の設定

この項では、ダイナミック PAT（隠蔽）のためのネットワーク オブジェクト NAT の設定方法について説明します。PAT プールを使用するダイナミック PAT については、この項ではなく、「ダイナミック NAT または PAT プールを使用したダイナミック PAT の設定」（P.6-4）を参照してください。詳細については、「ダイナミック PAT」（P.5-10）を参照してください。

手順の詳細

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 オブジェクトをダブルクリックします。

詳細については、『一般的な操作のコンフィギュレーション ガイド』を参照してください。

[Add/Edit Network Object] ダイアログボックスが表示されます。

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。

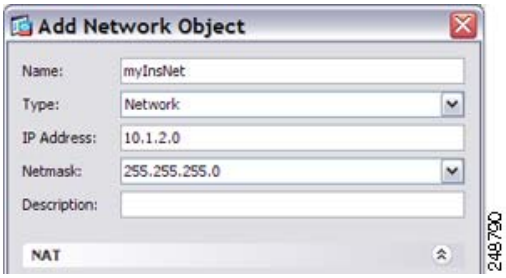
a. [Name]：オブジェクト名。a ～ z、A ～ Z、0 ～ 9、ピリオド、ハイフン、カンマ、またはアンダースコアの文字を使用してください。名前は 64 文字以下にする必要があります。

b. [Type]：ホスト、ネットワーク、または範囲。

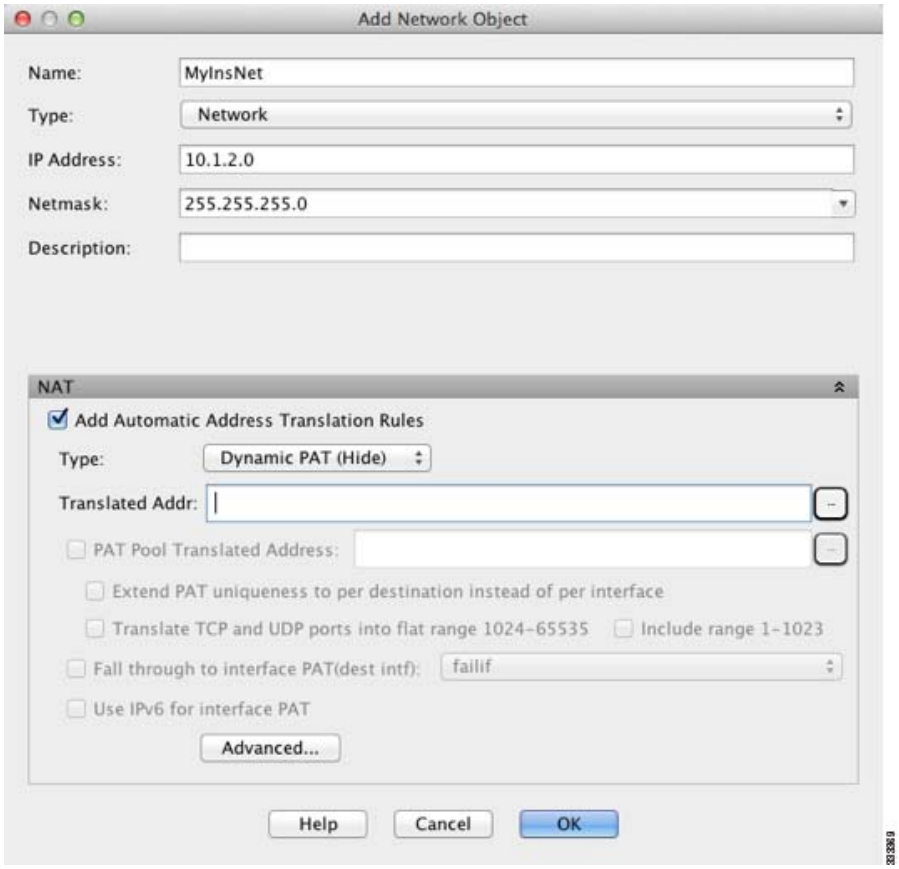
c. [IP Address] : IPv4 または IPv6 アドレス。オブジェクト タイプとして [Range] を選択した場合は、[IP Address] フィールドは、開始アドレスと終了アドレスを入力できるように変更されます。

d. [Netmask/Prefix Length]：サブネット マスクまたはプレフィックス長を入力します。

e. [Description]：（オプション）ネットワーク オブジェクトの説明（最大 200 文字）。



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。

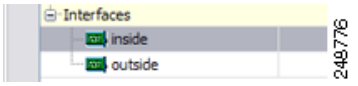
ステップ 5　[Type] ドロップダウン リストから、[Dynamic PAT (Hide)] を選択します。

（注）　1 つのアドレスの代わりに PAT プールを使用してダイナミック PAT を設定する方法については、「ダイナミック NAT または PAT プールを使用したダイナミック PAT の設定」（P.6-4）を参照してください。

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] フィールドには、次のいずれかの方法で、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。

- 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。

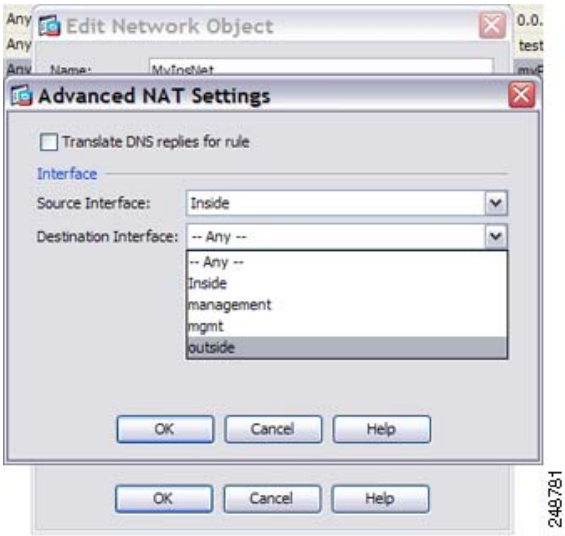


インターフェイス名を指定する場合は、*インターフェイス PAT* をイネーブルにしてください。このときに指定したインターフェイス IP アドレスがマッピング アドレスとして使用されます。IPv6 インターフェイス アドレスを使用するには、[Use IPv6 for interface PAT] もオンにする必要があります。インターフェイス PAT を使用する場合は、NAT ルールが適用されるのは指定したマッピング インターフェイスのみとなります（インターフェイス PAT を使用しない場合は、ルールはデフォルトですべてのインターフェイスに適用されます）。実際のインターフェイスも [--Any--] ではなく特定のインターフェイスとなるように設定する方法については、ステップ 7 を参照してください。

（注） 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。

- 参照ボタンをクリックし、[Browse Translated Addr] ダイアログボックスで既存のホスト アドレスを選択します。
- 参照ボタンをクリックし、[Browse Translated Addr] ダイアログボックスで新しい名前付きオブジェクトを作成します。

ステップ 7　（オプション）[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、「DNS および NAT」（P.5-32）を参照してください。
- （トランスペアレント ファイアウォール モードの場合に必須）[Source Interface]：この NAT ルールを適用する実際のインターフェイスを指定します。デフォルトでは、ルールは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 ファイアウォール モードの場合に必須）[Destination Interface]：この NAT ルールが適用されるマッピング インターフェイスを指定します。デフォルトでは、ルールはすべてのインターフェイスに適用されます。

入力が終わったら、[OK] をクリックします。[Add/Edit Network Object] ダイアログボックスに戻ります。

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

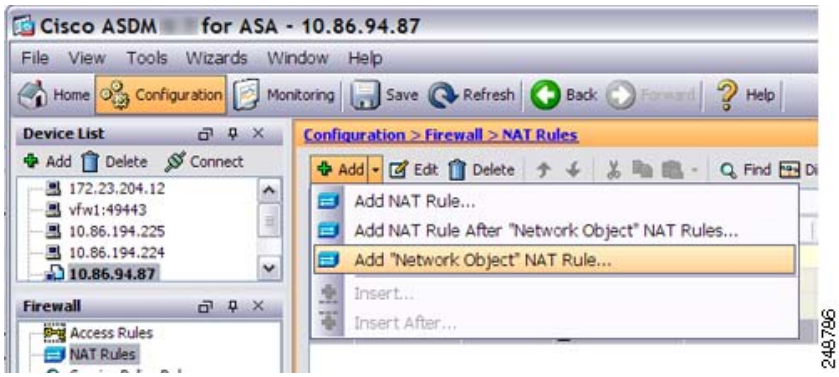
スタティック NAT またはポート変換を設定したスタティック NAT の設定

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。詳細については、「スタティック NAT」（P.5-3）を参照してください。

手順の詳細

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 オブジェクトをダブルクリックします。

詳細については、『一般的な操作のコンフィギュレーション ガイド』を参照してください。

[Add/Edit Network Object] ダイアログボックスが表示されます。

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。

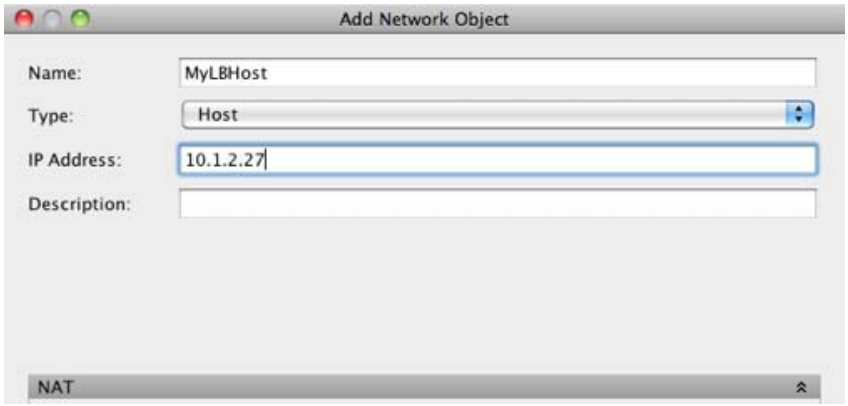
a. [Name]：オブジェクト名。a ～ z、A ～ Z、0 ～ 9、ピリオド、ハイフン、カンマ、またはアンダースコアの文字を使用してください。名前は 64 文字以下にする必要があります。

b. [Type]：ネットワーク、ホスト、または範囲。

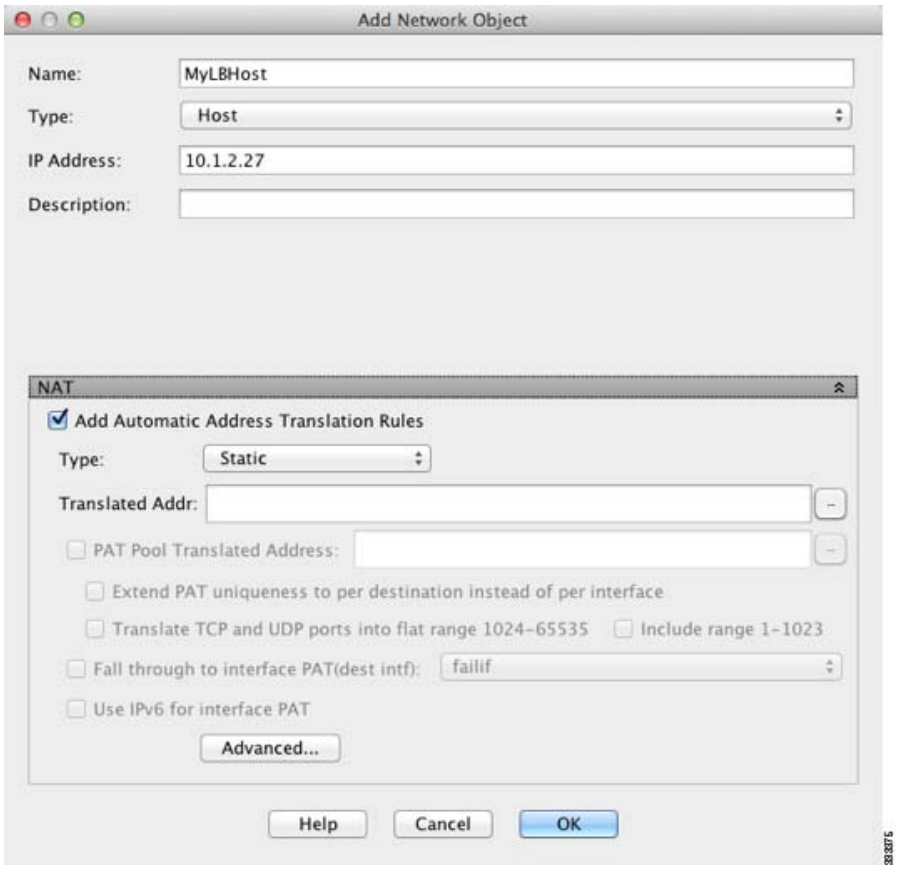
c. [IP Address] : IPv4 または IPv6 アドレス。オブジェクト タイプとして [Range] を選択した場合は、[IP Address] フィールドは、開始アドレスと終了アドレスを入力できるように変更されます。

d. [Netmask/Prefix Length]：サブネット マスクまたはプレフィックス長を入力します。

e. [Description]：（オプション）ネットワーク オブジェクトの説明（最大 200 文字）。



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。

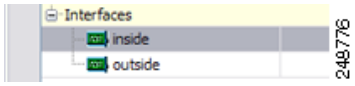
ステップ 5　[Type] ドロップダウン リストから、[Static] を選択します。

ステップ 6　[Translated Addr] フィールドで、次のいずれかを実行します。

- IP アドレスを入力します。

  IP アドレスを入力すると、マッピングされるネットワークのネットマスクや範囲は、実際のネットワークのものと同一になります。たとえば、実際のネットワークがホストの場合、このアドレスは、ホスト アドレスです。範囲の場合、マッピング アドレスには、実際の範囲と同じ数のアドレスが含まれます。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。

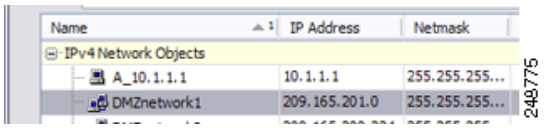
- （ポート変換を設定したスタティック NAT の場合のみ）インターフェイス名を入力するか、参照ボタンをクリックし、[Browse Translated Addr] ダイアログボックスでインターフェイス名を選択します。



  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] もオンにする必要があります。[Advanced NAT Settings] ダイアログボックスでのサービスの設定も必ず行ってください（ステップ 8 を参照）。（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）。

- 参照ボタンをクリックし、[Browse Translated Addr] ダイアログボックスで既存のアドレスを選択します。

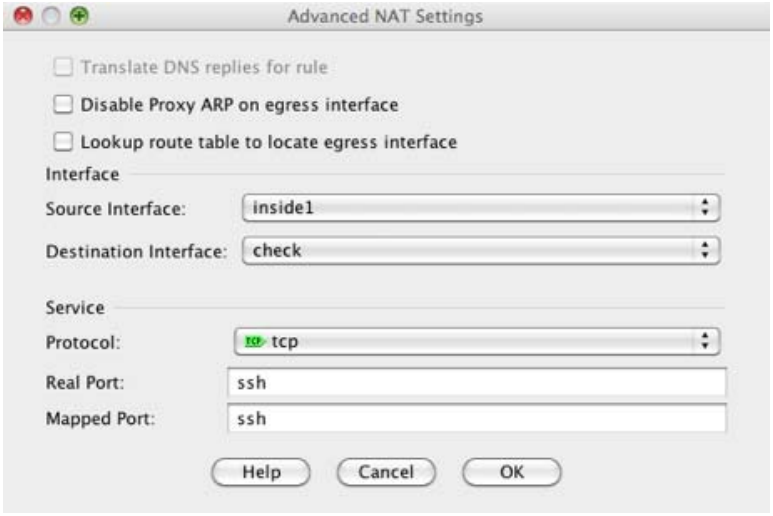
- 参照ボタンをクリックし、[Browse Translated Addr] ダイアログボックスで新しいアドレスを作成します。



通常、1 対 1 のマッピングでは、実際のアドレスと同じ数のマッピング アドレスを設定します。しかし、アドレスの数が一致しない場合もあります。詳細については、「スタティック NAT」（P.5-3）を参照してください。

ステップ 7　（オプション）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　（オプション）[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。

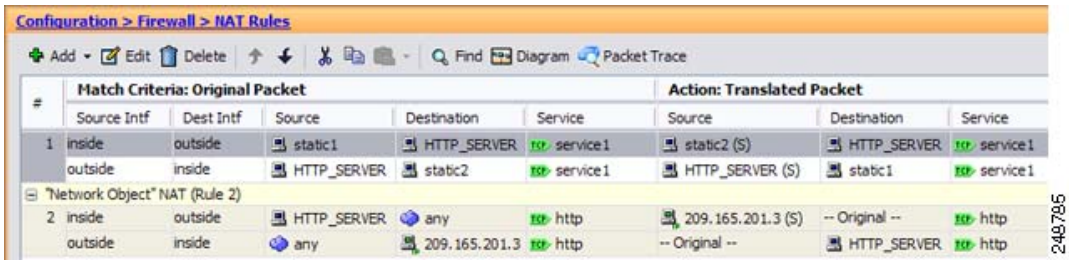


- [Translate DNS replies for rule]：DNS 応答内の IP アドレスを変換します。DNS インスペクションがイネーブルになっていることを確認してください（デフォルトではイネーブルです）。詳細については、「DNS および NAT」（P.5-32）を参照してください。
- [Disable Proxy ARP on egress interface]：マッピング IP アドレスへの着信パケットのプロキシ ARP をディセーブルにします。詳細については、「マッピング アドレスとルーティング」（P.5-22）を参照してください。
- （トランスペアレント ファイアウォール モードの場合に必須）[Interface]：
  - [Source Interface]：この NAT ルールを適用する実際のインターフェイスを指定します。デフォルトでは、ルールはすべてのインターフェイスに適用されます。
  - [Destination Interface]：この NAT ルールが適用されるマッピング インターフェイスを指定します。デフォルトでは、ルールはすべてのインターフェイスに適用されます。
- [Service]：
  - [Protocol]：ポート変換を設定したスタティック NAT を設定します。[tcp] または [udp] を選択します。
  - [Real Port]：ポート番号または予約済みポートの名前（たとえば「ftp」）のいずれかを入力できます。
  - [Mapped Port]：ポート番号または予約済みポートの名前（たとえば「ftp」）のいずれかを入力できます。

入力が終わったら、[OK] をクリックします。[Add/Edit Network Object] ダイアログボックスに戻ります。

ステップ 9　[OK] をクリックし、さらに [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。



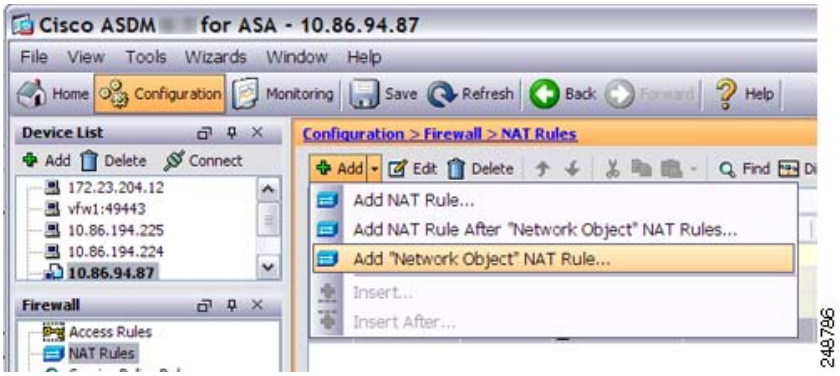
アイデンティティ NAT の設定

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。詳細については、「アイデンティティ NAT」（P.5-12）を参照してください。

手順の詳細

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 オブジェクトをダブルクリックします。

詳細については、『一般的な操作のコンフィギュレーション ガイド』を参照してください。

[Add/Edit Network Object] ダイアログボックスが表示されます。

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。

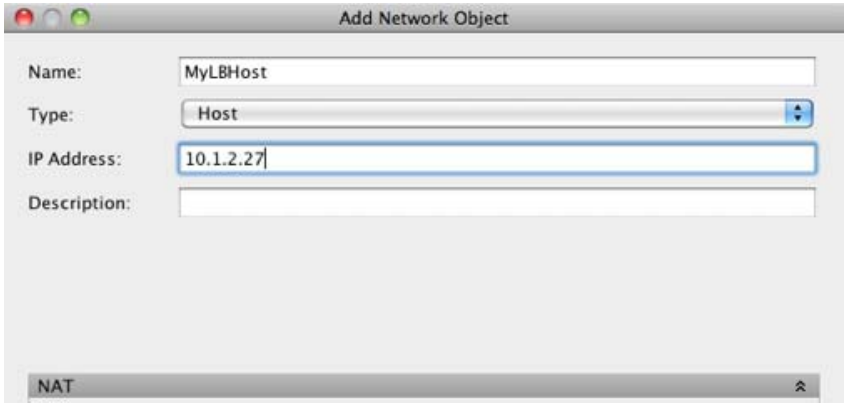
a. [Name]：オブジェクト名。a ～ z、A ～ Z、0 ～ 9、ピリオド、ハイフン、カンマ、またはアンダースコアの文字を使用してください。名前は 64 文字以下にする必要があります。

b. [Type]：ネットワーク、ホスト、または範囲。

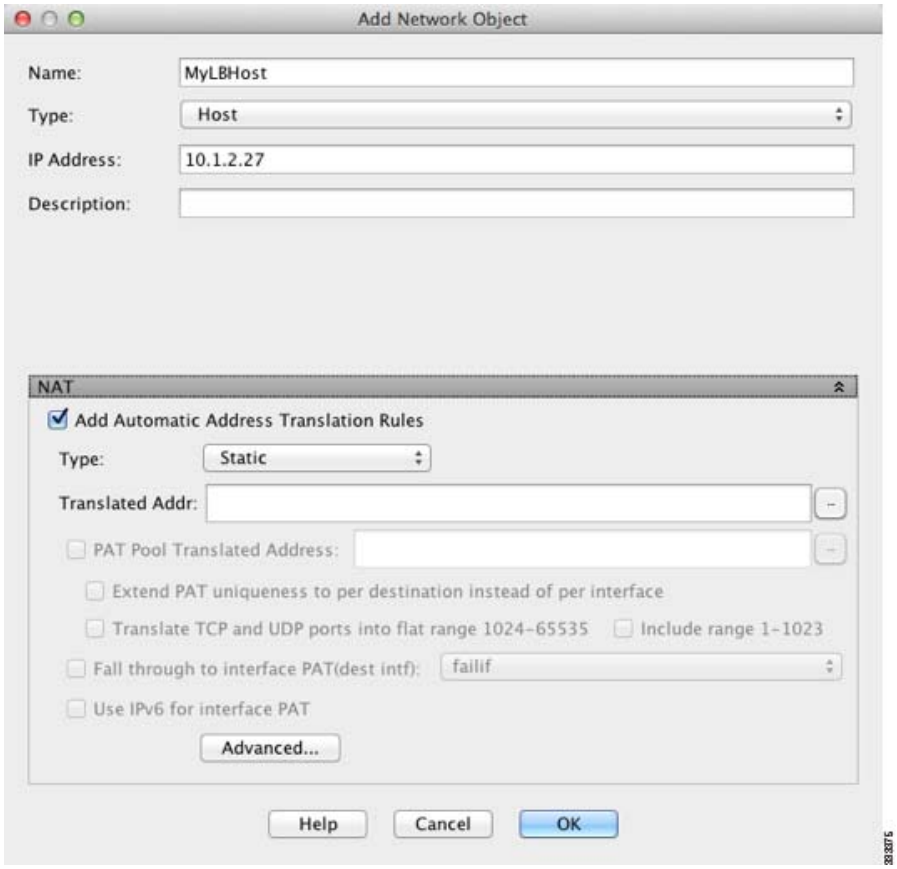
c. [IP Address] : IPv4 または IPv6 アドレス。オブジェクト タイプとして [Range] を選択した場合は、[IP Address] フィールドは、開始アドレスと終了アドレスを入力できるように変更されます。

d. [Netmask/Prefix Length]：サブネット マスクまたはプレフィックス長を入力します。

e. [Description]：（オプション）ネットワーク オブジェクトの説明（最大 200 文字）。



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。

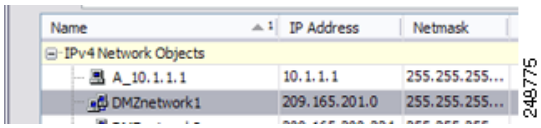


ステップ 4　[Add Automatic Translation Rules] チェックボックスをオンにします。

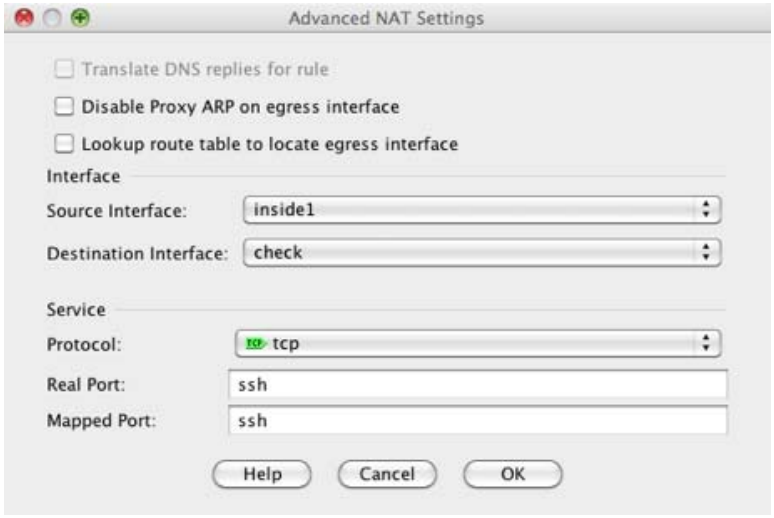
ステップ 5　[Type] ドロップダウン リストから、[Static] を選択します。

ステップ 6　[Translated Addr] フィールドで、次のいずれかを実行します。

- 実際のアドレスに使用したのと同じ IP アドレスを入力します。
- 参照ボタンをクリックし、[Browse Translated Addr] ダイアログボックスで、一致する IP アドレス定義を持つネットワーク オブジェクトを選択します。
- 参照ボタンをクリックし、[Browse Translated Addr] ダイアログボックスで、一致する IP アドレス定義を持つネットワーク オブジェクトを作成します。



ステップ 7　（オプション）[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ます。

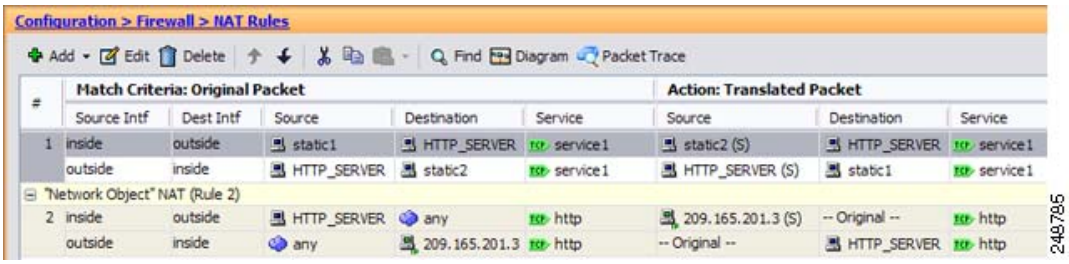


- [Disable Proxy ARP on egress interface]：マッピング IP アドレスへの着信パケットのプロキシ ARP をディセーブルにします。詳細については、「マッピング アドレスとルーティング」（P.5-22）を参照してください。
- （ルーテッド モード、インターフェイスを指定）[Lookup route table to locate egress interface]：NAT コマンドに指定したインターフェイスを使用する代わりに、ルート ルックアップを使用して出力インターフェイスを決定します。詳細については、「出力インターフェイスの決定」（P.5-25）を参照してください。
- （トランスペアレント ファイアウォール モードの場合に必須）[Interface]：
  - [Source Interface]：この NAT ルールを適用する実際のインターフェイスを指定します。デフォルトでは、ルールはすべてのインターフェイスに適用されます。
  - [Destination Interface]：この NAT ルールが適用されるマッピング インターフェイスを指定します。デフォルトでは、ルールはすべてのインターフェイスに適用されます。

このダイアログボックスのその他の設定は変更しないでください。入力が終わったら、[OK] をクリックします。[Add/Edit Network Object] ダイアログボックスに戻ります。

ステップ 8　[OK] をクリックし、さらに [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。



Per-Session PAT ルールの設定

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 と Multi-Session PAT の詳細については、「Per-Session PAT と Multi-Session PAT（バージョン 9.0(1) 以降）」（P.5-11）を参照してください。

デフォルト

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、ルール テーブルに表示されません。

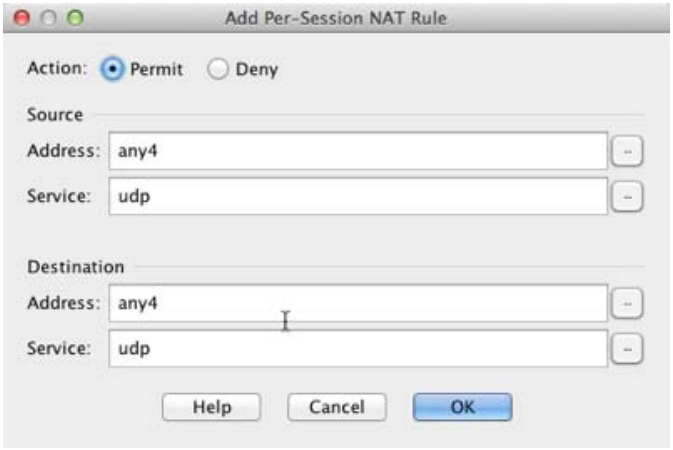
（注）　これらのルールは削除できません。これらのルールは常に、手動作成されたルールの後に存在します。ルールは順番に評価されるので、デフォルト ルールを無効にすることができます。たとえば、これらのルールを完全に反転させるには、次のものを追加します。

- 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

手順の詳細

ステップ 1　[Configuration] > [Firewall] > [Advanced] > [Per-Session NAT Rules] を選択し、[Add] > [Add Per-Session NAT Rule] をクリックします。

ステップ 2　[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。

ステップ 3　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。

ステップ 4　送信元サービスに UDP または TCP を指定します。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。

ステップ 5　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。

ステップ 6　宛先サービスに UDP または TCP を指定します。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。

ステップ 7　[OK] をクリックします。

ステップ 8　[Apply] をクリックします。

ネットワーク オブジェクト NAT のモニタリング

[Monitoring] > [Properties] > [Connection Graphs] > [Xlates] ペインでは、アクティブなネットワーク アドレス変換をグラフィック形式で表示できます。1 つのグラフ ウィンドウに表示する統計情報のタイプは 4 つまで選択できます。複数のグラフ ウィンドウを同時に開くことができます。

フィールド

- [Available Graphs]：グラフ化できるコンポーネントを一覧表示します。
  - [Xlate Utilization]：ASA の NAT の使用状況を表示します。
- [Graph Window Title]：グラフ タイプを追加するグラフ ウィンドウ名を表示します。既存のウィンドウ タイトルを使用するには、ドロップダウン リストからいずれかを選択します。新しいウィンドウにグラフを表示するには、新しいウィンドウ タイトルを入力します。
- [Add]：[Available Graphs] リストで選択したエントリを [Selected Graphs] リストに移動するには、このフィールドをクリックします。
- [Remove]：[Selected Graphs] リストから選択したエントリを削除するには、このフィールドをクリックします。

- [Show Graphs]：新しいグラフ ウィンドウ、または更新したグラフ ウィンドウを表示するには、このフィールドをクリックします。

[Monitoring] > [Properties] > [Connection Graphs] > [Perfmon] ペインでは、パフォーマンス情報をグラフィック形式で表示できます。1 つのグラフ ウィンドウに表示する統計情報のタイプは 4 つまで選択できます。複数のグラフ ウィンドウを同時に開くことができます。

フィールド

- [Available Graphs]：グラフ化できるコンポーネントを一覧表示します。
  - [AAA Perfmon]：ASA の AAA パフォーマンス情報を表示します。
  - [Inspection Perfmon]：ASA の検査パフォーマンス情報を表示します。
  - [Web Perfmon]：URL アクセスおよび URL サーバ要求などの ASA の Web パフォーマンス情報を表示します。
  - [Connections Perfmon]：ASA の接続パフォーマンス情報を表示します。
  - [Xlate Perfmon]：ASA の NAT パフォーマンス情報を表示します。
- [Graph Window Title]：グラフ タイプを追加するグラフ ウィンドウ名を表示します。既存のウィンドウ タイトルを使用するには、ドロップダウン リストからいずれかを選択します。新しいウィンドウにグラフを表示するには、新しいウィンドウ タイトルを入力します。
- [Add]：[Available Graphs] リストで選択したエントリを [Selected Graphs] リストに移動するには、このフィールドをクリックします。
- [Remove]：[Selected Graphs] リストから選択した統計タイプを削除するには、このフィールドをクリックします。
- [Show Graphs]：新しいグラフ ウィンドウ、または更新したグラフ ウィンドウを表示するには、このフィールドをクリックします。

ネットワーク オブジェクト NAT の設定例

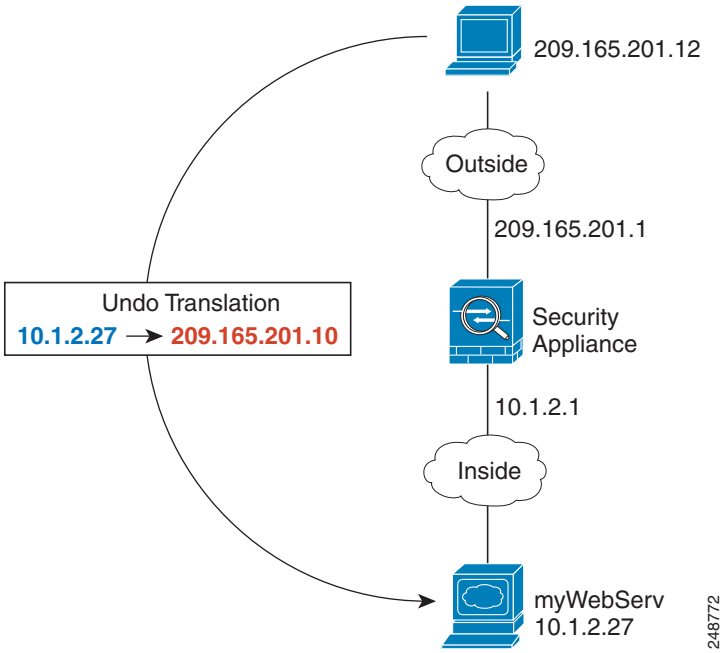
ここでは、次の設定例を示します。

- 「内部 Web サーバへのアクセスの提供（スタティック NAT）」（P.6-23）
- 「内部ホストの NAT（ダイナミック NAT）および外部 Web サーバの NAT（スタティック NAT）」（P.6-25）
- 「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」（P.6-30）
- 「FTP、HTTP、および SMTP のための単一アドレス（ポート変換を設定したスタティック NAT）」（P.6-34）
- 「マッピング インターフェイス上の DNS サーバ、実際のインターフェイス上の Web サーバ（DNS 修正を設定したスタティック NAT）」（P.6-37）
- 「マッピング インターフェイス上の DNS サーバおよび FTP サーバ、FTP サーバが変換される（DNS 修正を設定したスタティック NAT）」（P.6-40）
- 「マッピング インターフェイス上の IPv4 DNS サーバおよび FTP サーバ、実際のインターフェイス上の IPv6 ホスト（DNS64 修正を設定したスタティック NAT64）」（P.6-42）

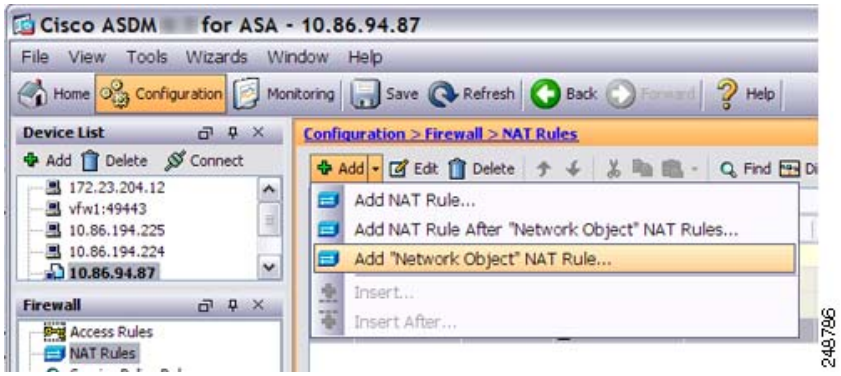
内部 Web サーバへのアクセスの提供（スタティック NAT）

次の例では、内部 Web サーバに対してスタティック NAT を実行します。実際のアドレスはプライベート ネットワーク上にあるので、パブリック アドレスが必要です。スタティック NAT は、固定アドレスにある Web サーバへのトラフィックをホストが開始できるようにするために必要です （図 6-1 を参照）。

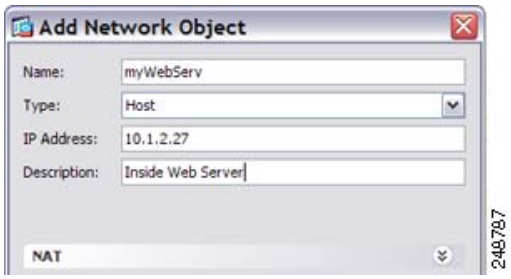
図 6-1　内部 Web サーバのスタティック NAT



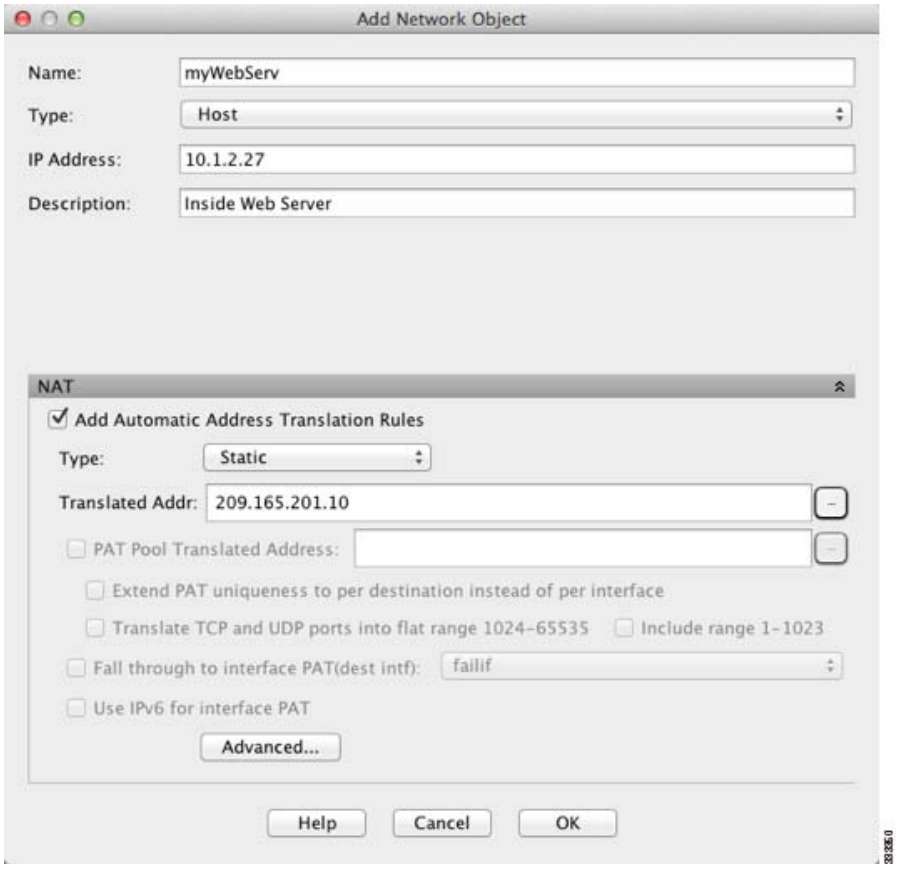
ステップ 1　内部 Web サーバのネットワーク オブジェクトを作成します。



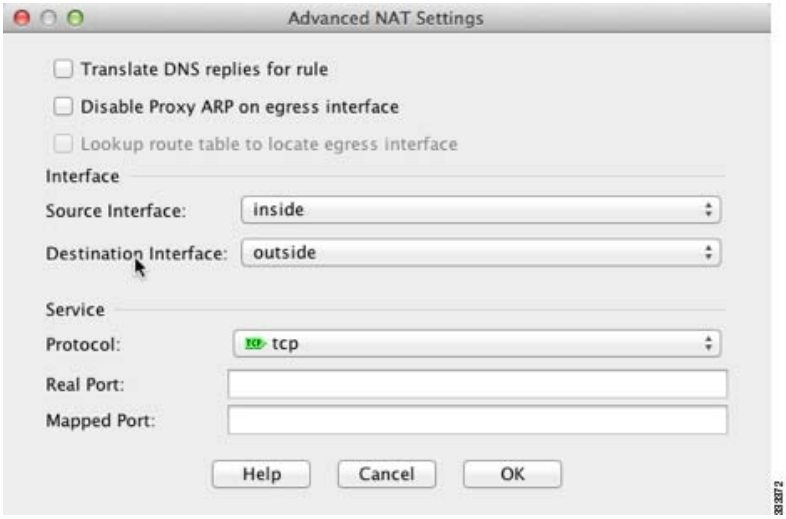
ステップ 2　Web サーバのアドレスを定義します。



ステップ 3　オブジェクトのスタティック NAT を設定します。



ステップ 4　[Advanced] をクリックして、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設定します。

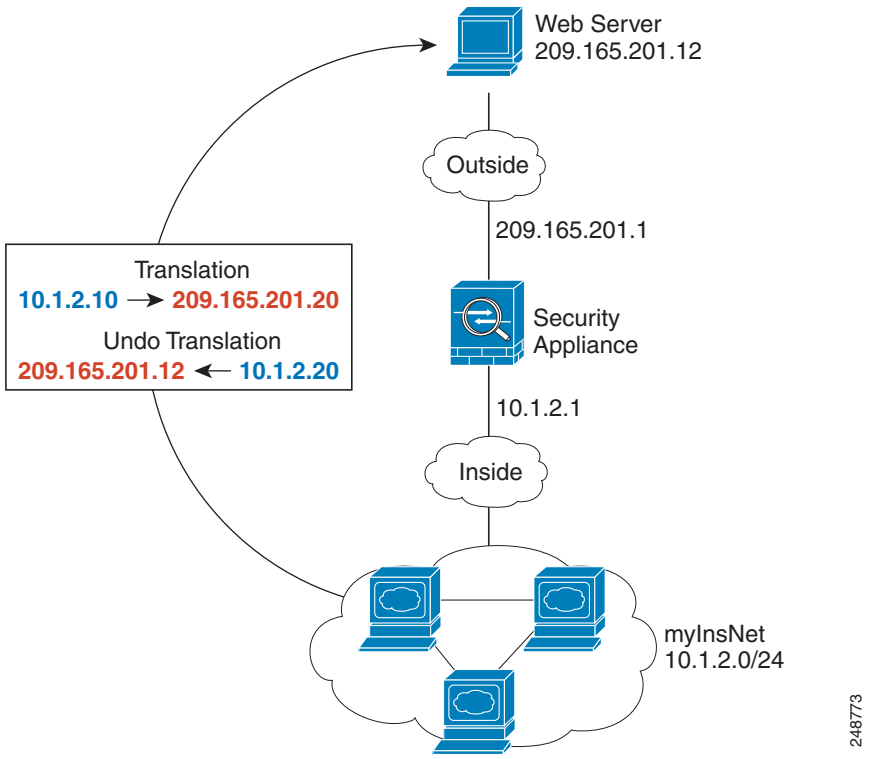


ステップ 5　[OK] をクリックして [Edit Network Object] ダイアログボックスに戻り、もう一度 [OK] をクリックし、[Apply] をクリックします。

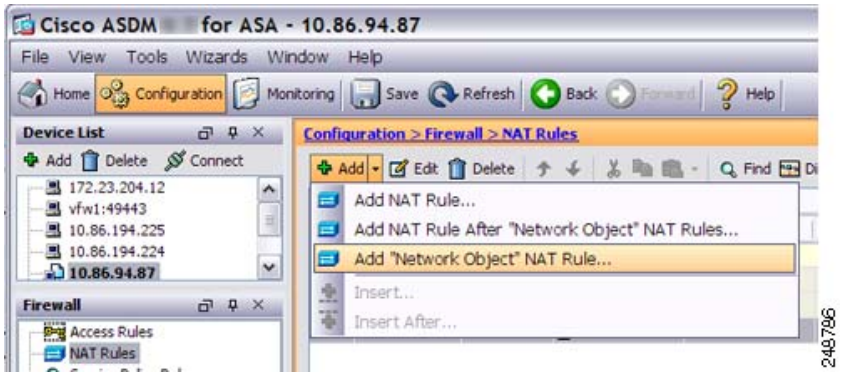
内部ホストの NAT（ダイナミック NAT）および外部 Web サーバの NAT（スタティック NAT）

次の例では、プライベート ネットワーク上の内部ユーザが外部にアクセスする場合、このユーザにダイナミック NAT を設定します。また、内部ユーザが外部 Web サーバに接続する場合、この Web サーバのアドレスが内部ネットワークに存在するように見えるアドレスに変換されます（図 6-2 を参照）。

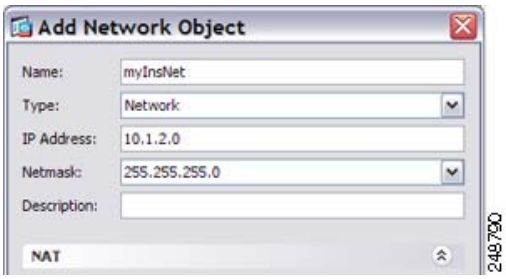
図 6-2　内部のダイナミック NAT、外部 Web サーバのスタティック NAT



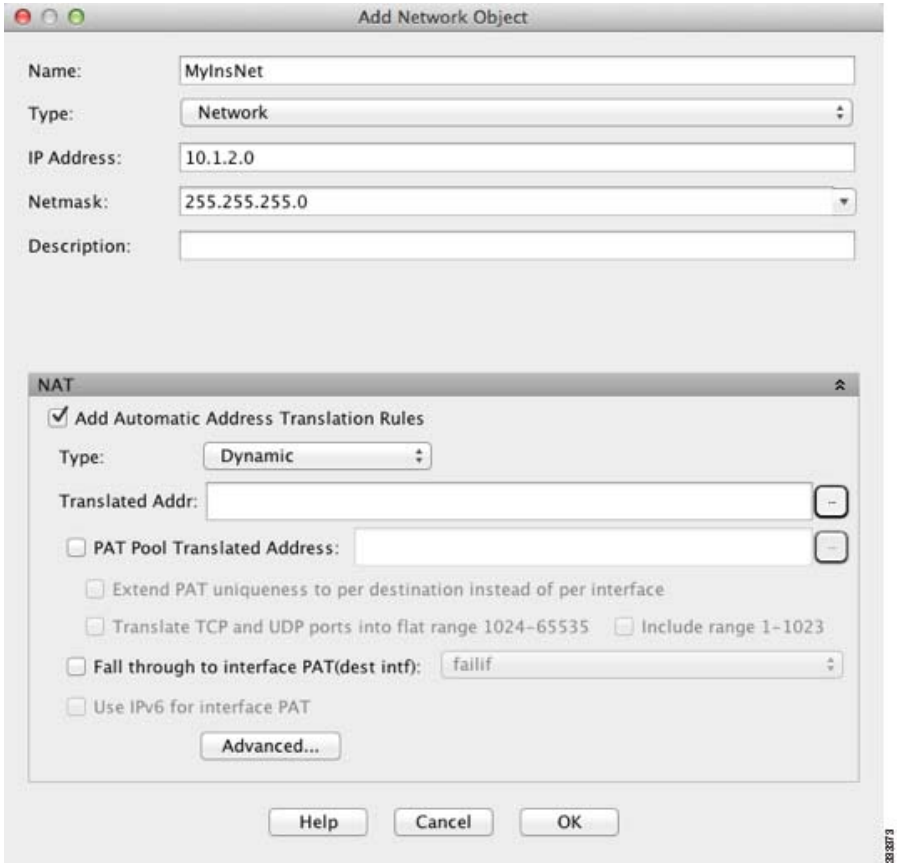
ステップ 1　内部ネットワークのネットワーク オブジェクトを作成します。



ステップ 2　内部ネットワークのアドレスを定義します。

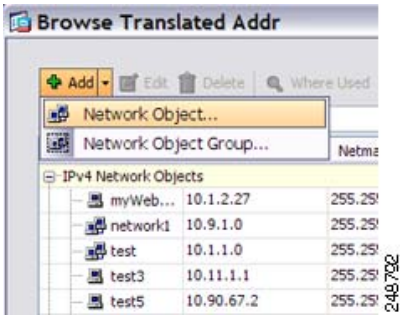


ステップ 3　内部ネットワークのダイナミック NAT をイネーブルにします。



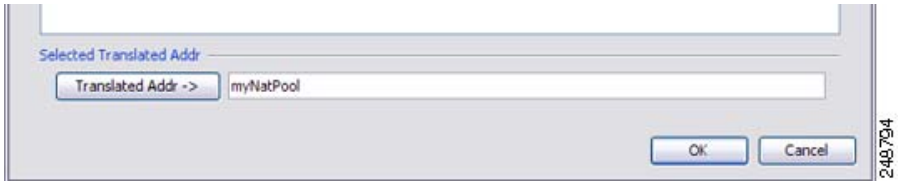
ステップ 4　[Translated Addr] フィールドで、内部アドレスの変換先となるダイナミック NAT プールを表す新しいネットワーク オブジェクトを追加するには、参照ボタンをクリックします。

a.　新しいネットワーク オブジェクトを追加します。

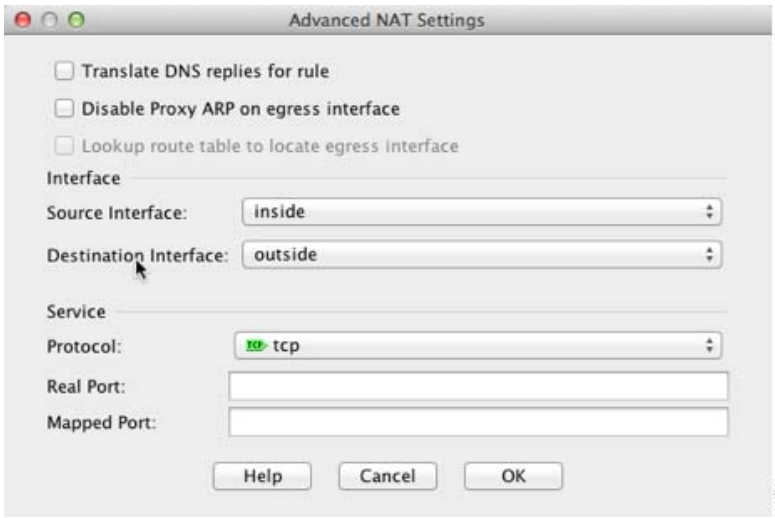


b. NAT プールのアドレスを定義して、[OK] をクリックします。

c. 新しいネットワーク オブジェクトをダブルクリックで選択します。[OK] をクリックして、NAT コンフィギュレーションに戻ります。

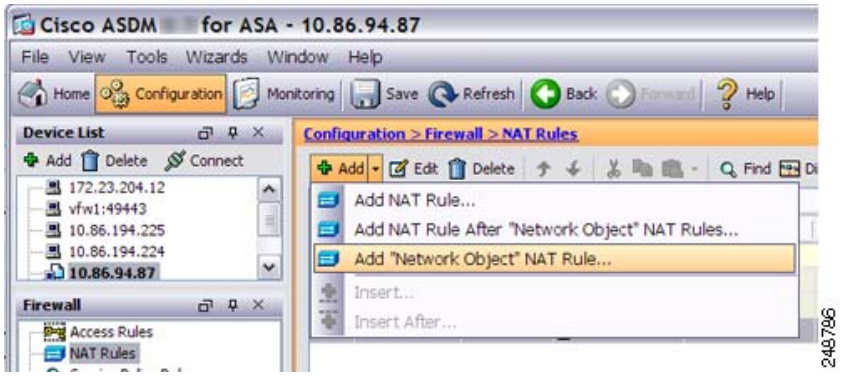


ステップ 5　[Advanced] をクリックして、実際のインターフェイスとマッピング インターフェイスを設定します。

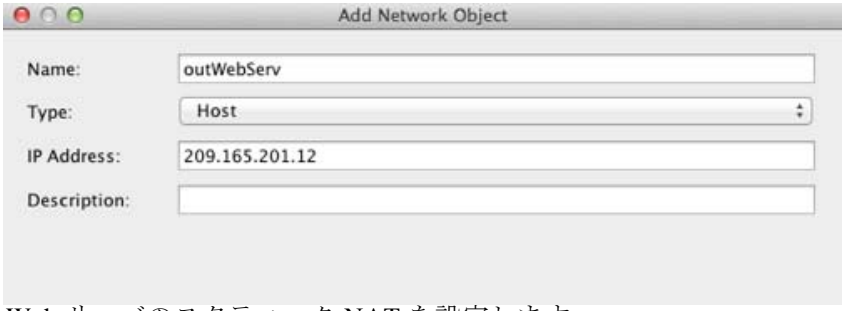


ステップ 6　[OK] をクリックして [Edit Network Object] ダイアログボックスに戻り、もう一度 [OK] をクリックして [NAT Rules] テーブルに戻ります。

ステップ 7　外部 Web サーバのネットワーク オブジェクトを作成します。

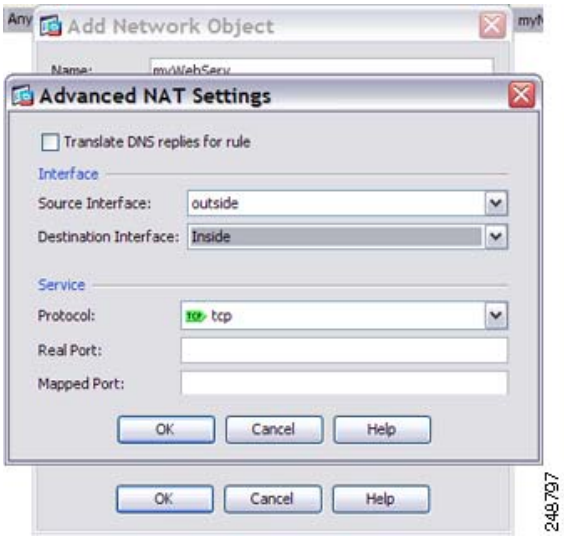


ステップ 8　Web サーバのアドレスを定義します。



ステップ 9　Web サーバのスタティック NAT を設定します。

ステップ 10　[Advanced] をクリックして、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設定します。

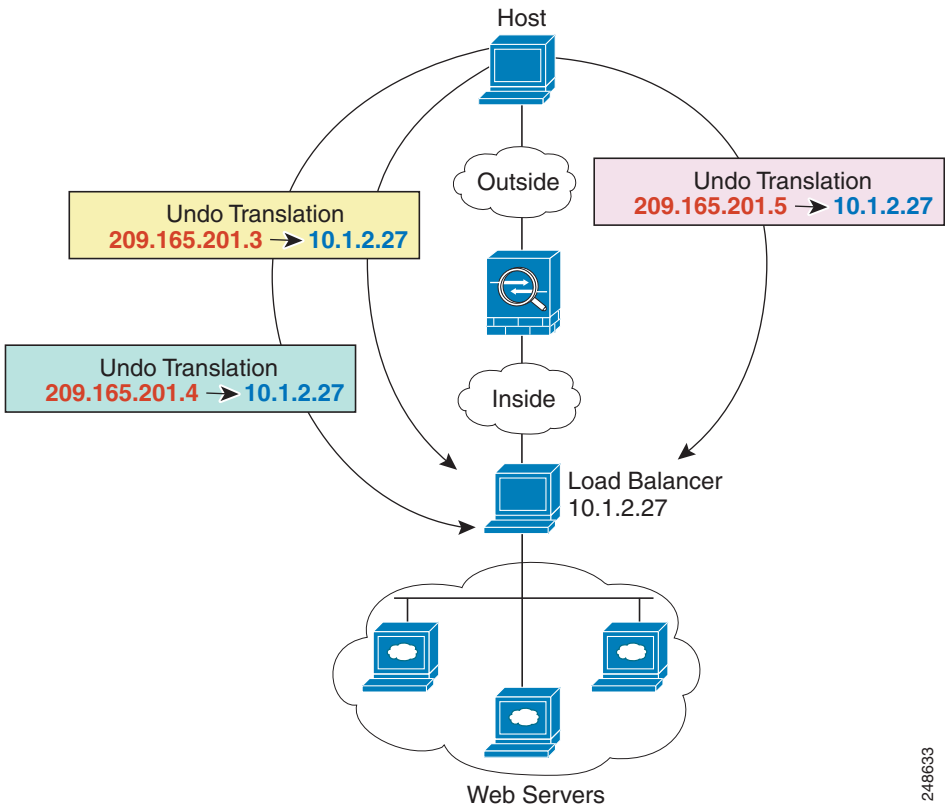


ステップ 11　[OK] をクリックして [Edit Network Object] ダイアログボックスに戻り、もう一度 [OK] をクリックし、[Apply] をクリックします。

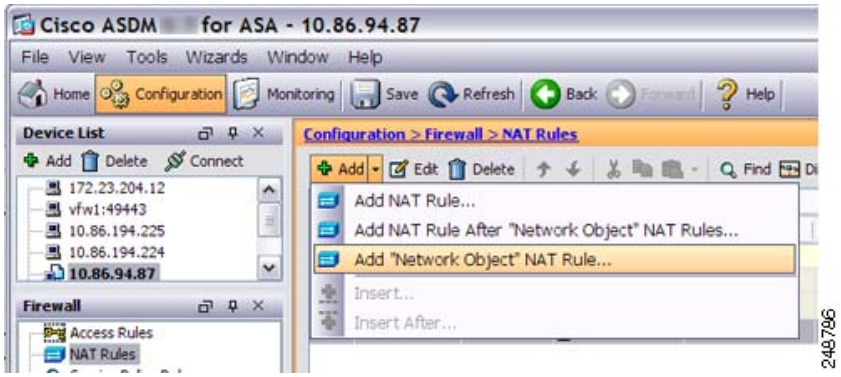
複数のマッピング アドレス（スタティック NAT、1 対多）を持つ内部ロード バランサ

次の例では、複数の IP アドレスに変換される内部ロード バランサを示しています。外部ホストがマッピング IP アドレスの 1 つにアクセスする場合、1 つのロード バランサのアドレスには変換されません。要求される URL に応じて、トラフィックを正しい Web サーバにリダイレクトします（図 6-3 を参照）。

図 6-3　内部ロード バランサのスタティック NAT（1 対多）



ステップ 1　ロード バランサのネットワーク オブジェクトを作成します。

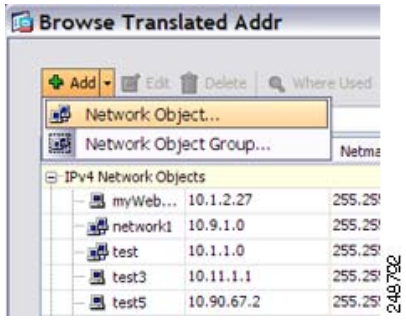


ステップ 2　ロード バランサのアドレスを定義します。

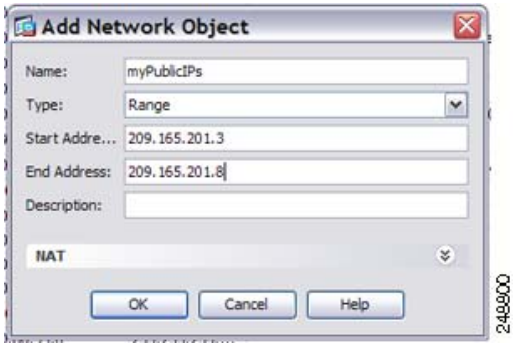
ステップ 3　ロード バランサのスタティック NAT を設定します。

ステップ 4　[Translated Addr] フィールドで、ロード バランサ アドレスの変換先となるスタティック NAT アドレス グループを表す新しいネットワーク オブジェクトを追加するには、参照ボタンをクリックします。

a.　新しいネットワーク オブジェクトを追加します。

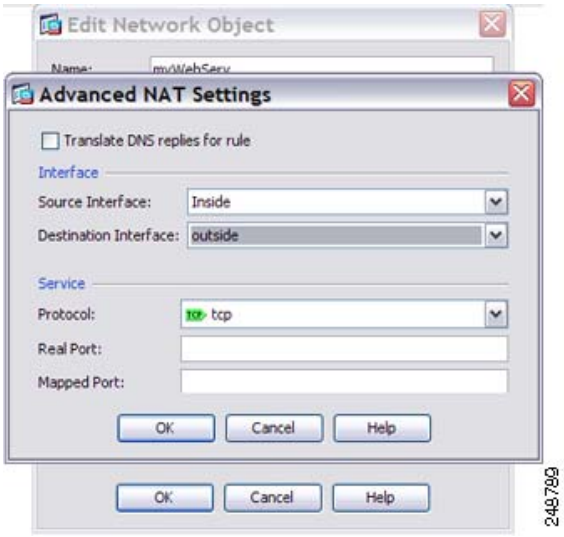


b.　スタティック NAT アドレス グループを定義し、[OK] をクリックします。



c. 新しいネットワーク オブジェクトをダブルクリックで選択します。[OK] をクリックして、NAT コンフィギュレーションに戻ります。

ステップ 5　[Advanced] をクリックして、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設定します。

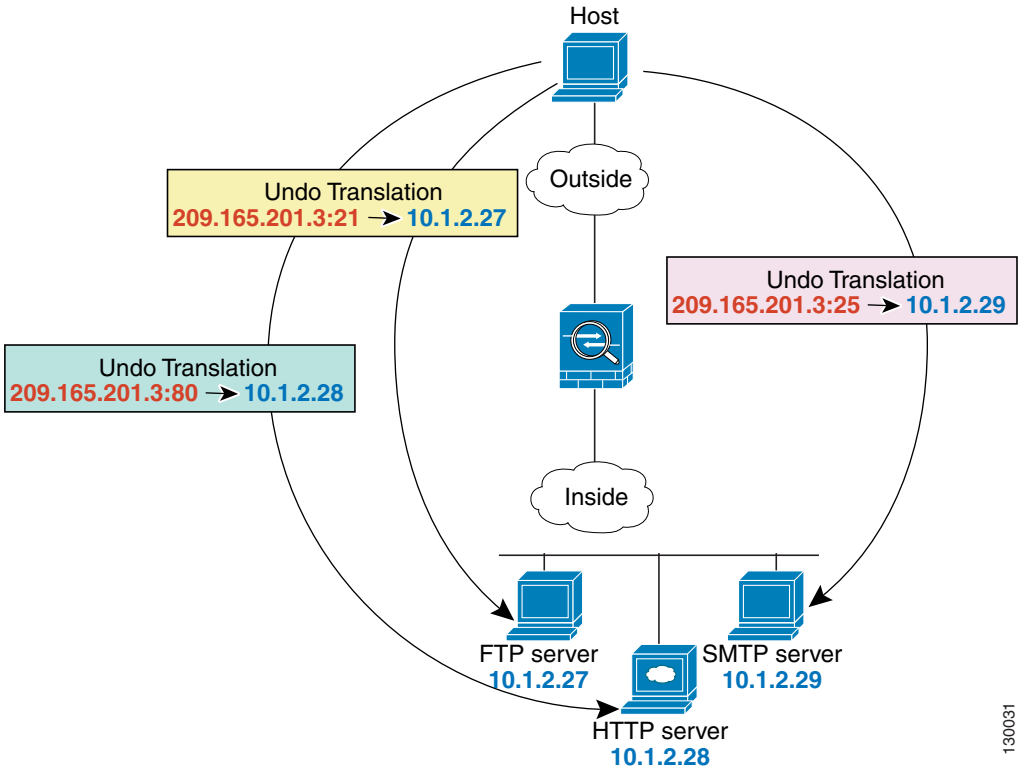


ステップ 6　[OK] をクリックして [Edit Network Object] ダイアログボックスに戻り、もう一度 [OK] をクリックし、[Apply] をクリックします。

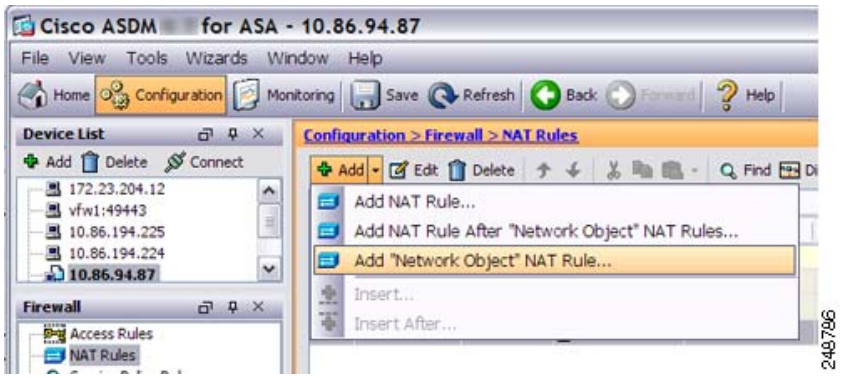
FTP、HTTP、および SMTP のための単一アドレス（ポート変換を設定したスタティック NAT）

次のポート変換を設定したスタティック NAT の例では、リモート ユーザは単一のアドレスで FTP、HTTP、および SMTP にアクセスできるようになります。これらのサーバは実際には、それぞれ異なるデバイスとして実際のネットワーク上に存在しますが、ポート変換を設定したスタティック NAT ルールを指定すると、使用するマッピング IP アドレスは同じで、それぞれ別のポートを使用することができます。（図 6-4 を参照）。

図 6-4　　ポート変換を設定したスタティック NAT

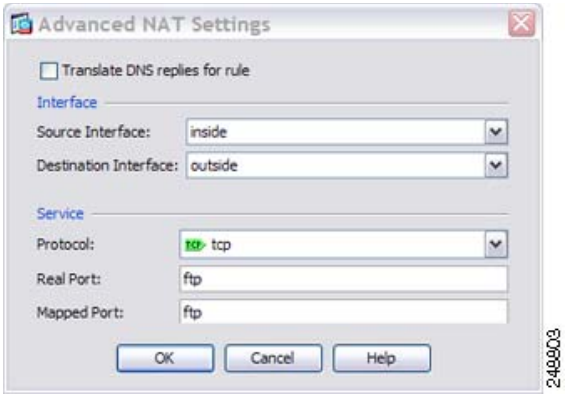


ステップ 1　FTP サーバ アドレスのネットワーク オブジェクトを作成します。

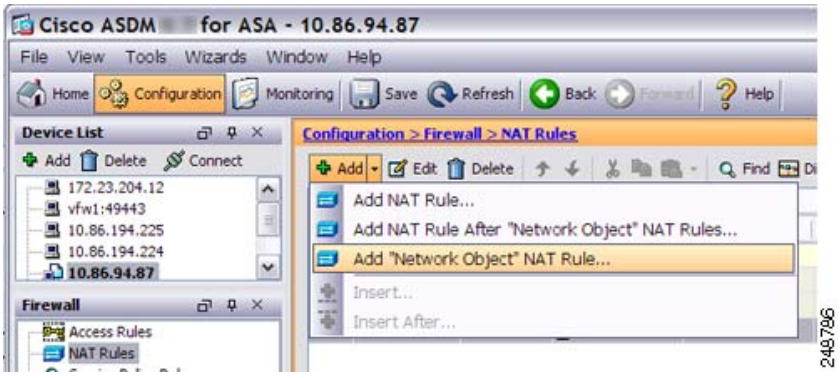


ステップ 2　FTP サーバのアドレスを定義し、アイデンティティ ポート変換を設定したスタティック NAT を FTP サーバに設定します。

ステップ 3　[Advanced] をクリックし、FTP の実際のインターフェイスおよびマッピング インターフェイスとポート変換を設定します。

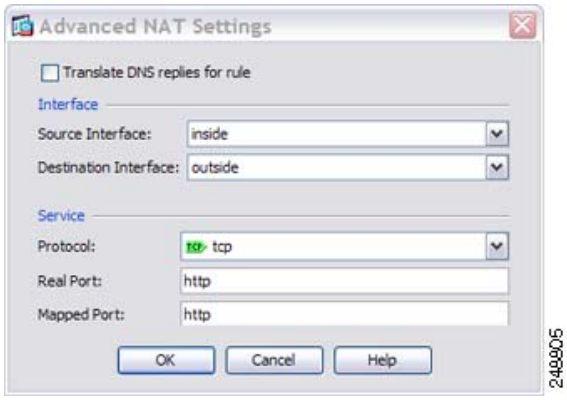


ステップ 4　HTTP サーバ アドレスのネットワーク オブジェクトを作成します。

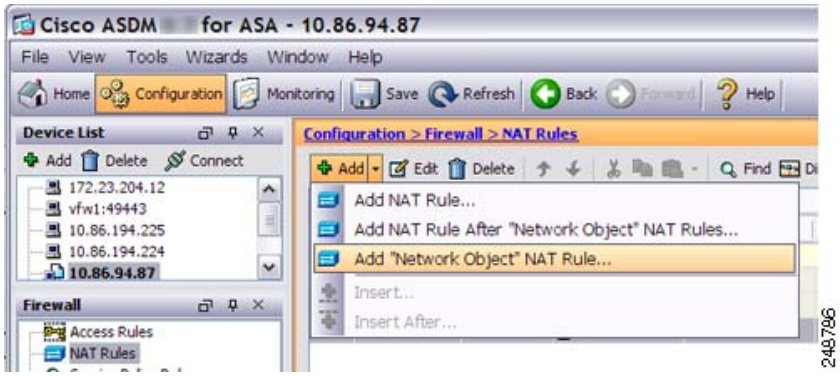


ステップ 5　HTTP サーバのアドレスを定義し、アイデンティティ ポート変換を設定したスタティック NAT を HTTP サーバに設定します。

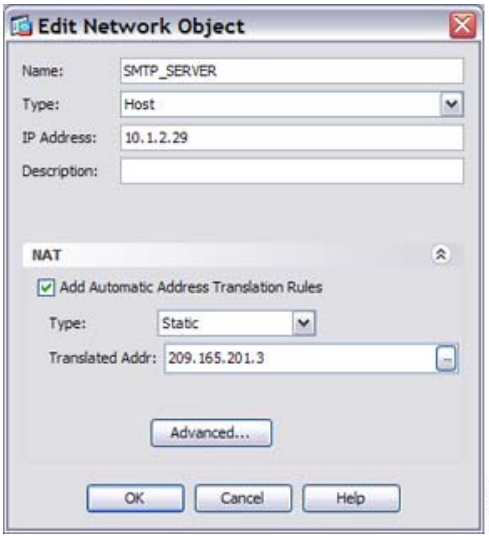
ステップ 6　[Advanced] をクリックし、HTTP の実際のインターフェイスおよびマッピング インターフェイスとポート変換を設定します。



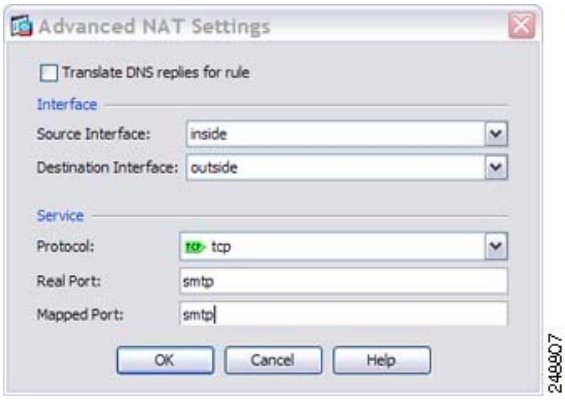
ステップ 7　SMTP サーバ アドレスのネットワーク オブジェクトを作成します。



ステップ 8　SMTP サーバのアドレスを定義し、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 SMTP サーバに設定します。



ステップ 9　[Advanced] をクリックし、SMTP の実際のインターフェイスおよびマッピング インターフェイスとポート変換を設定します。



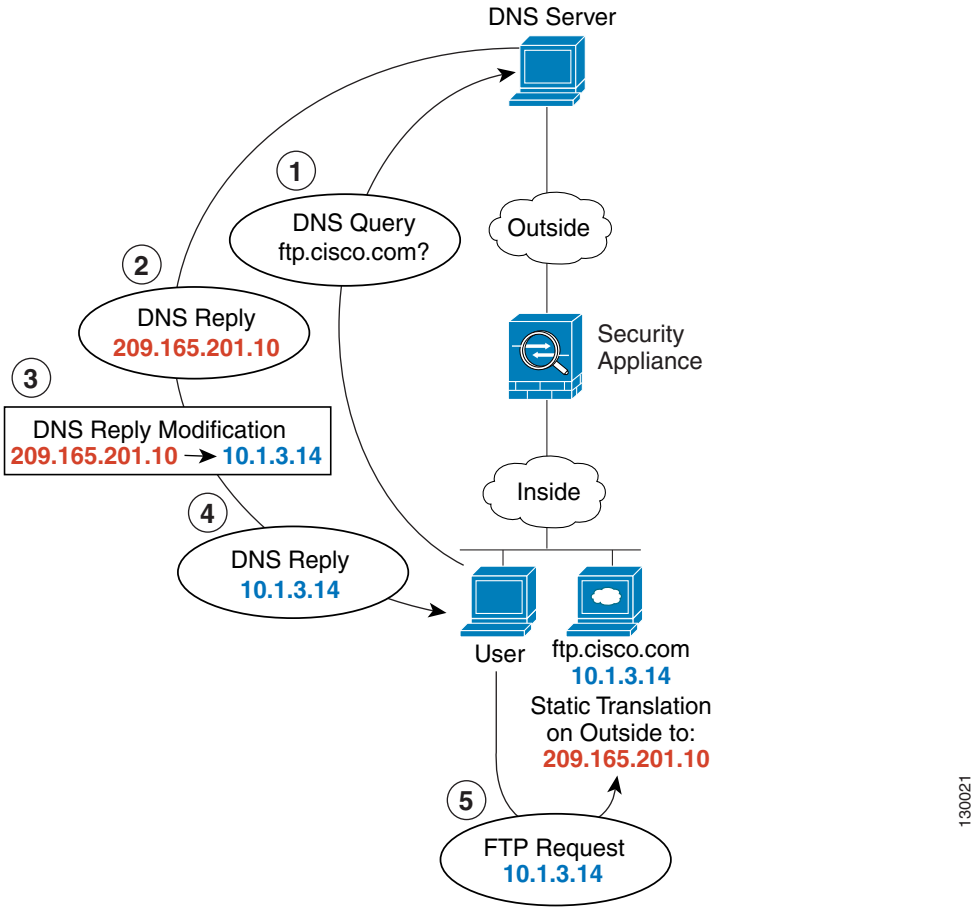
ステップ 10　[OK] をクリックして [Edit Network Object] ダイアログボックスに戻り、もう一度 [OK] をクリックし、[Apply] をクリックします。

マッピング インターフェイス上の DNS サーバ、実際のインターフェイス上の Web サーバ（DNS 修正を設定したスタティック NAT）

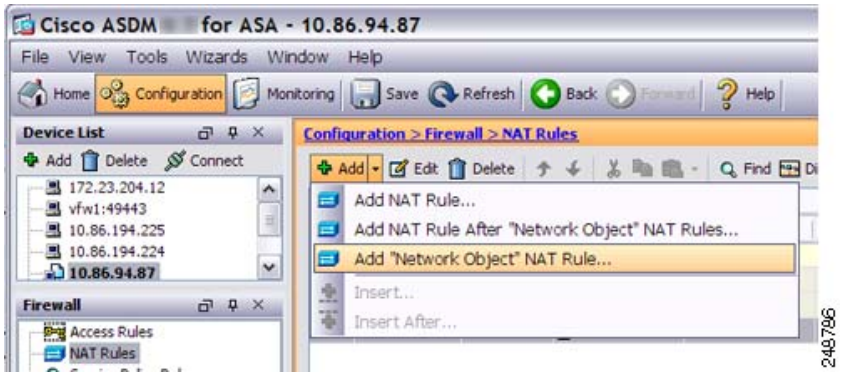
たとえば、DNS サーバが外部インターフェイスからアクセス可能であるとします。ftp.cisco.com というサーバが内部インターフェイス上にあります。ftp.cisco.com の実際のアドレス（10.1.3.14）を、外部ネットワーク上で可視のマッピング アドレス（209.165.201.10）にスタティックに変換するように、ASA を設定します（図 6-5 を参照）。この場合、このスタティック ルールで DNS 応答修正をイネーブルにする必要があります。これにより、実際のアドレスを使用して ftp.cisco.com にアクセスすることを許可されている内部ユーザは、マッピング アドレスではなく実際のアドレスを DNS サーバから受信できるようになります。

内部ホストが ftp.cisco.com のアドレスを求める DNS 要求を送信すると、DNS サーバは応答でマッピング アドレス（209.165.201.10）を示します。ASA は、内部サーバのスタティック ルールを参照し、DNS 応答内のアドレスを 10.1.3.14 に変換します。DNS 応答修正をイネーブルにしない場合、内部ホストは ftp.cisco.com に直接アクセスする代わりに、209.165.201.10 にトラフィックを送信することを試みます。

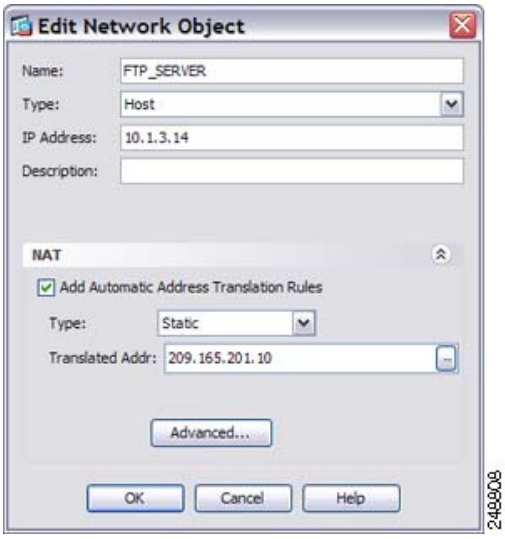
図 6-5　DNS 応答修正



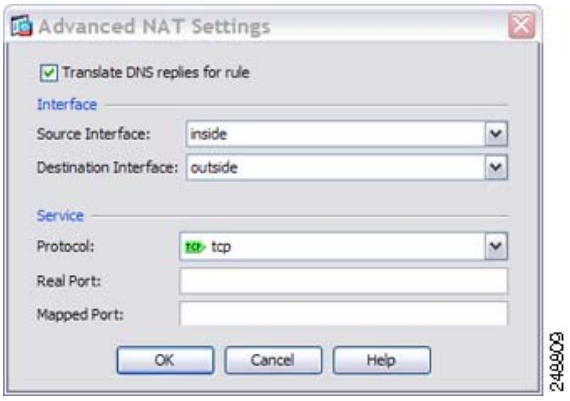
ステップ 1　FTP サーバ アドレスのネットワーク オブジェクトを作成します。



ステップ 2　FTP サーバのアドレスを定義し、DNS 修正を設定したスタティック NAT を設定します。



ステップ 3　実際のインターフェイスとマッピング インターフェイスおよび DNS 修正を設定するには、[Advanced] をクリックします。

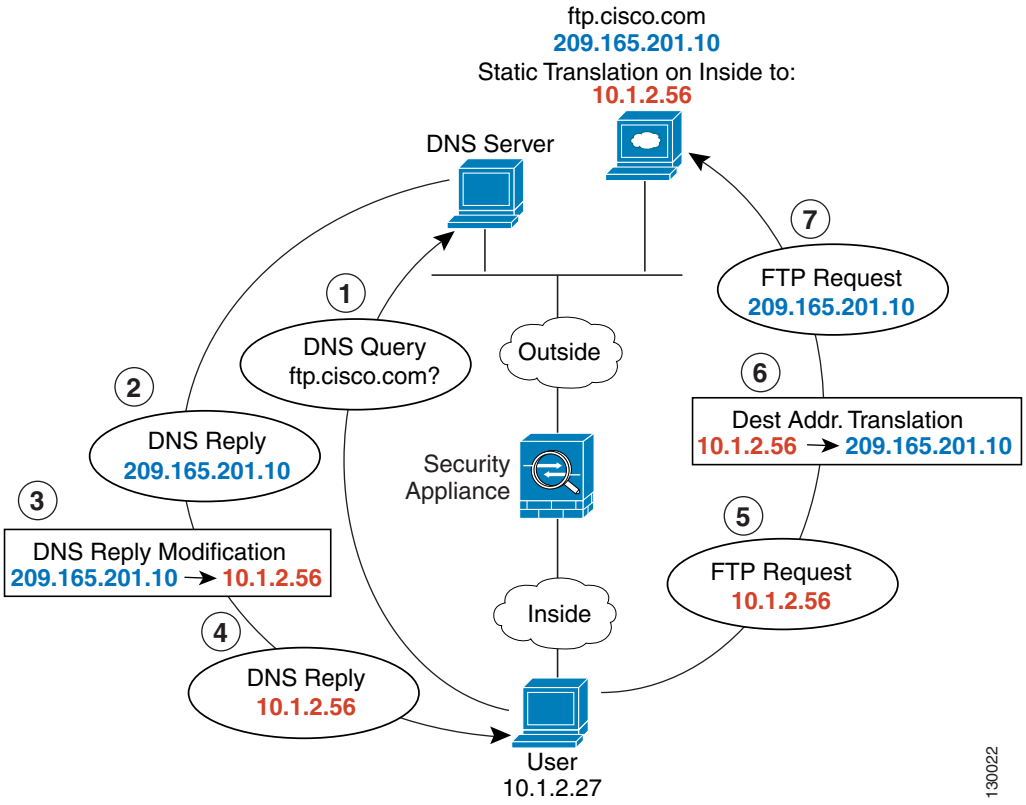


ステップ 4　[OK] をクリックして [Edit Network Object] ダイアログボックスに戻り、もう一度 [OK] をクリックし、[Apply] をクリックします。

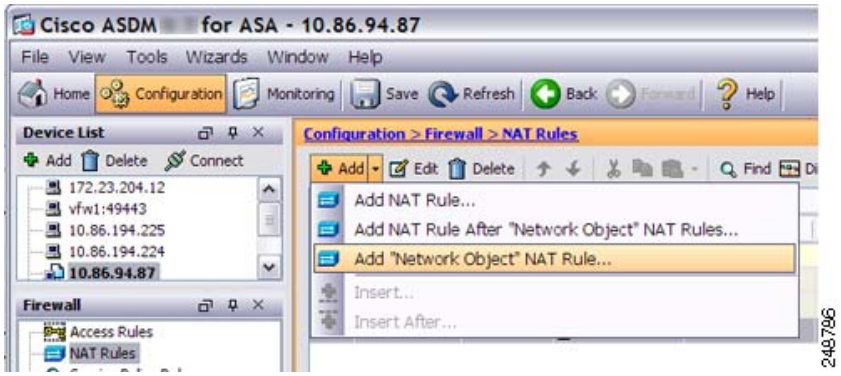
マッピング インターフェイス上の DNS サーバおよび FTP サーバ、FTP サーバが変換される（DNS 修正を設定したスタティック NAT）

図 6-6 に、外部の FTP サーバと DNS サーバを示します。ASA には、外部サーバ用のスタティック変換があります。この場合に、内部ユーザが ftp.cisco.com のアドレスを DNS サーバに要求すると、DNS サーバは応答として実際のアドレス 209.165.201.10 を返します。ftp.cisco.com のマッピング アドレス（10.1.2.56）が内部ユーザによって使用されるようにするには、スタティック変換に対して DNS 応答修正を設定する必要があります。

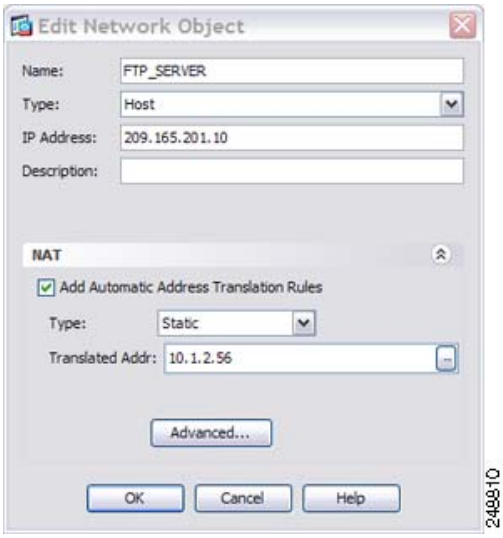
図 6-6　外部 NAT を使用する DNS 応答修正



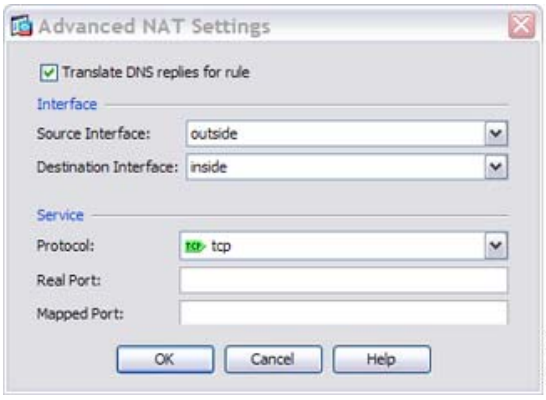
ステップ 1　FTP サーバ アドレスのネットワーク オブジェクトを作成します。



ステップ 2　FTP サーバのアドレスを定義し、DNS 修正を設定したスタティック NAT を設定します。



ステップ 3　実際のインターフェイスとマッピング インターフェイスおよび DNS 修正を設定するには、[Advanced] をクリックします。

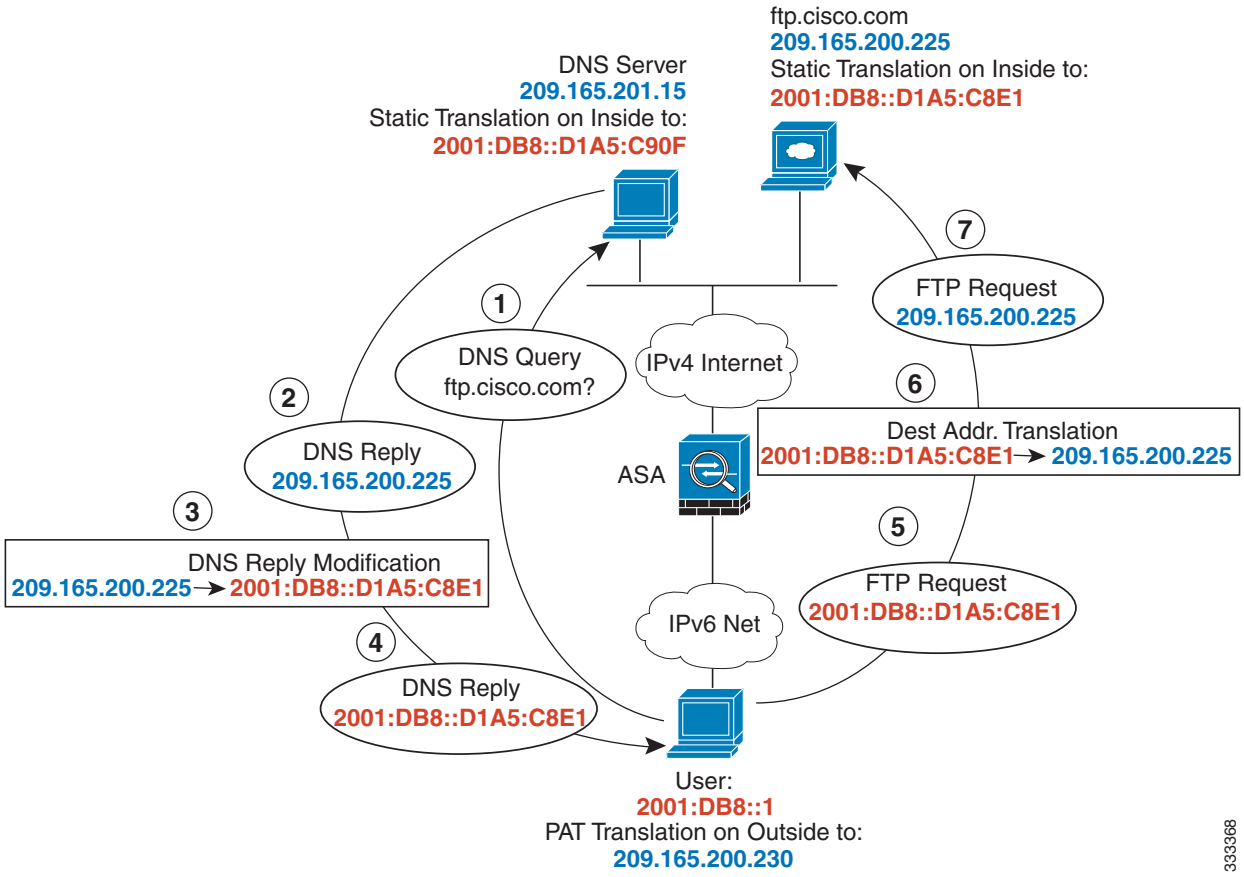


ステップ 4　[OK] をクリックして [Edit Network Object] ダイアログボックスに戻り、もう一度 [OK] をクリックし、[Apply] をクリックします。

マッピング インターフェイス上の IPv4 DNS サーバおよび FTP サーバ、実際のインターフェイス上の IPv6 ホスト（DNS64 修正を設定したスタティック NAT64）

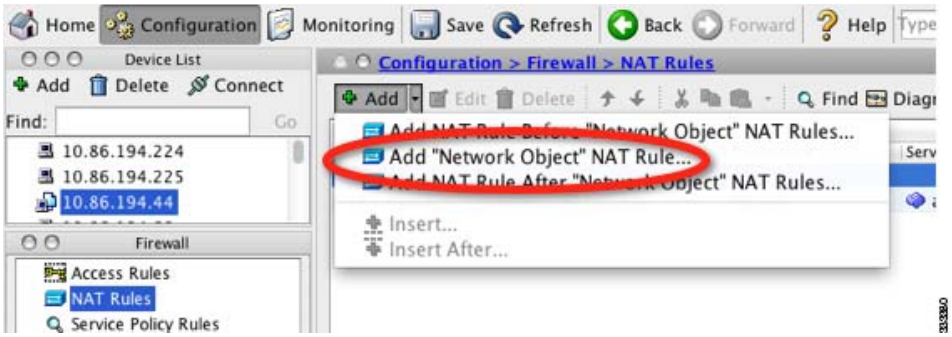
図 6-6 に、外部の IPv4 ネットワーク上の FTP サーバと DNS サーバを示します。ASA には、外部サーバ用のスタティック変換があります。この場合に、内部 IPv6 ユーザが ftp.cisco.com のアドレスを DNS サーバに要求すると、DNS サーバは応答として実際のアドレス 209.165.200.225 を返します。ftp.cisco.com のマッピング アドレス（2001:DB8::D1A5:C8E1）が内部ユーザによって使用されるようにするには、スタティック変換に対して DNS 応答修正を設定する必要があります。この例には、DNS サーバのスタティック NAT 変換、および内部 IPv6 ホストの PAT ルールも含まれています。

図 6-7　外部 NAT を使用する DNS 応答修正

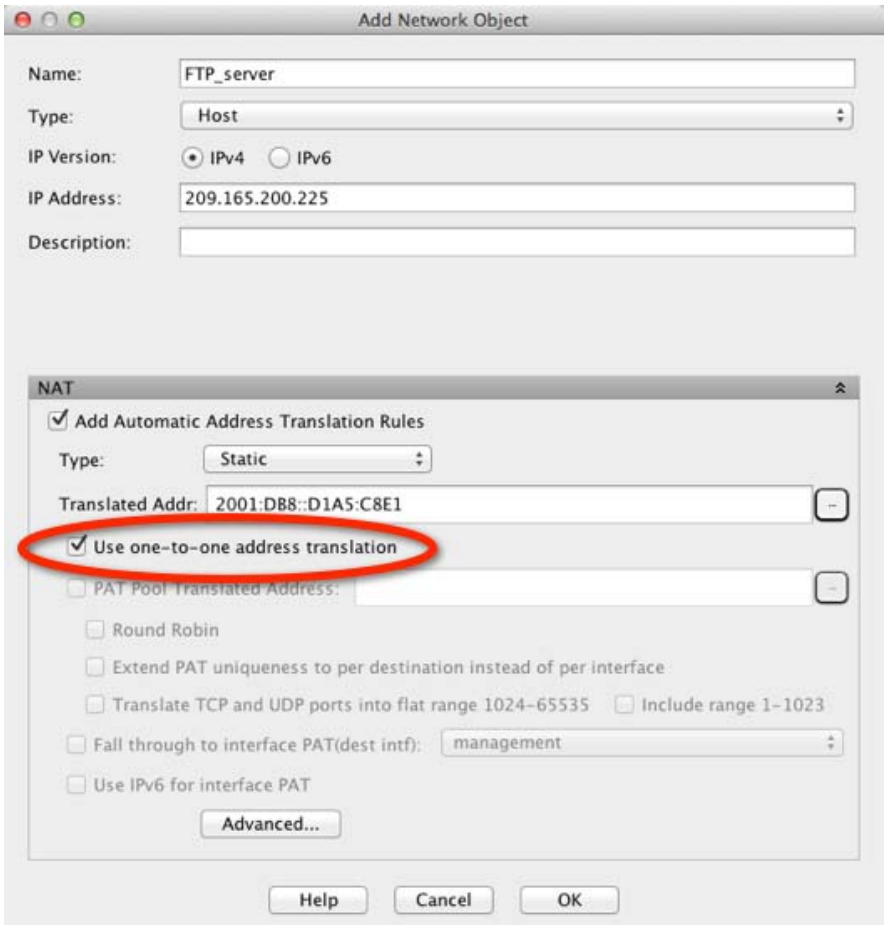


ステップ 1　FTP サーバのための、DNS 修正を設定したスタティック NAT を設定します。

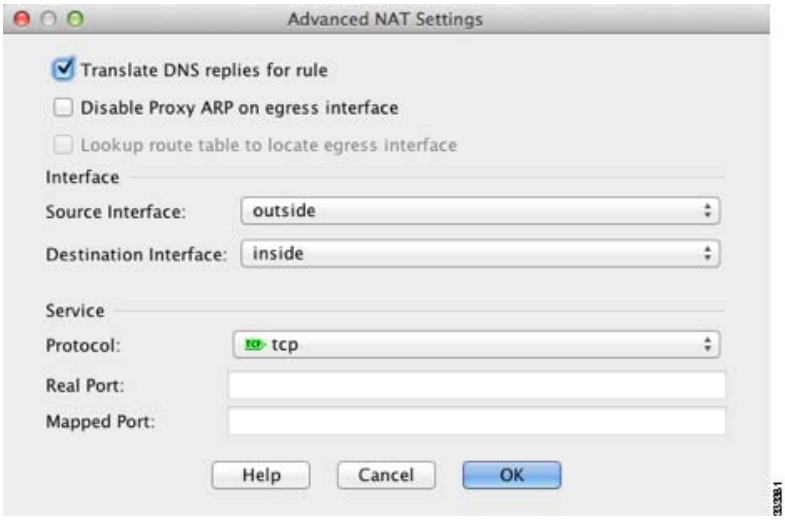
a. FTP サーバ アドレスのためのネットワーク オブジェクトを作成します。



b. FTP サーバのアドレスを定義し、DNS 修正を設定したスタティック NAT を設定します。これは 1 対 1 変換であるため、NAT46 に対して one-to-one 方式を設定します。



c. 実際のインターフェイスとマッピング インターフェイスおよび DNS 修正を設定するには、[Advanced] をクリックします。

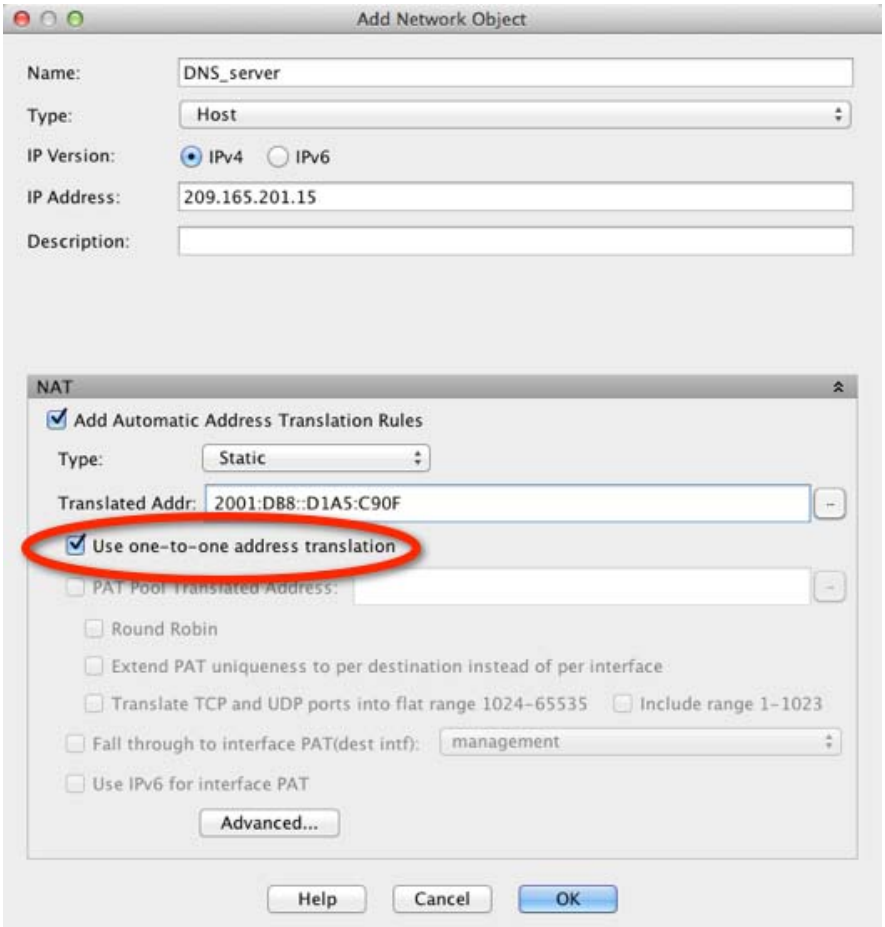


d. [OK] をクリックして [Edit Network Object] ダイアログボックスに戻ります。

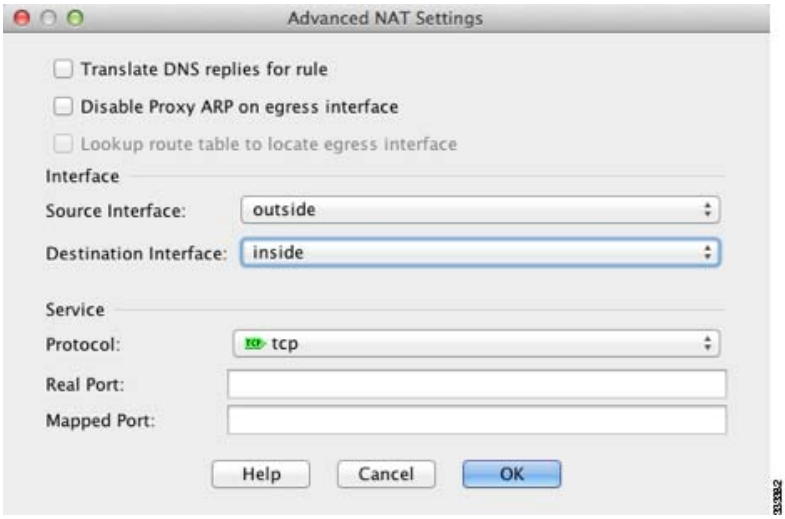
ステップ 2　DNS サーバの NAT を設定します。

a. DNS サーバ アドレスのためのネットワーク オブジェクトを作成します。

b. DNS サーバのアドレスを定義し、one-to-one 方式を使用してスタティック NAT を設定します。

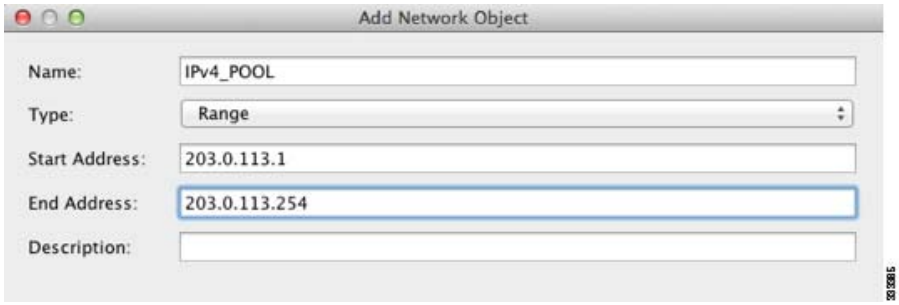


c. 実際のインターフェイスとマッピング インターフェイスを設定するには、[Advanced] をクリックします。



d. [OK] をクリックして [Edit Network Object] ダイアログボックスに戻ります。

ステップ 3　内部 IPv6 ネットワークを変換するための IPv4 PAT プールを設定します。

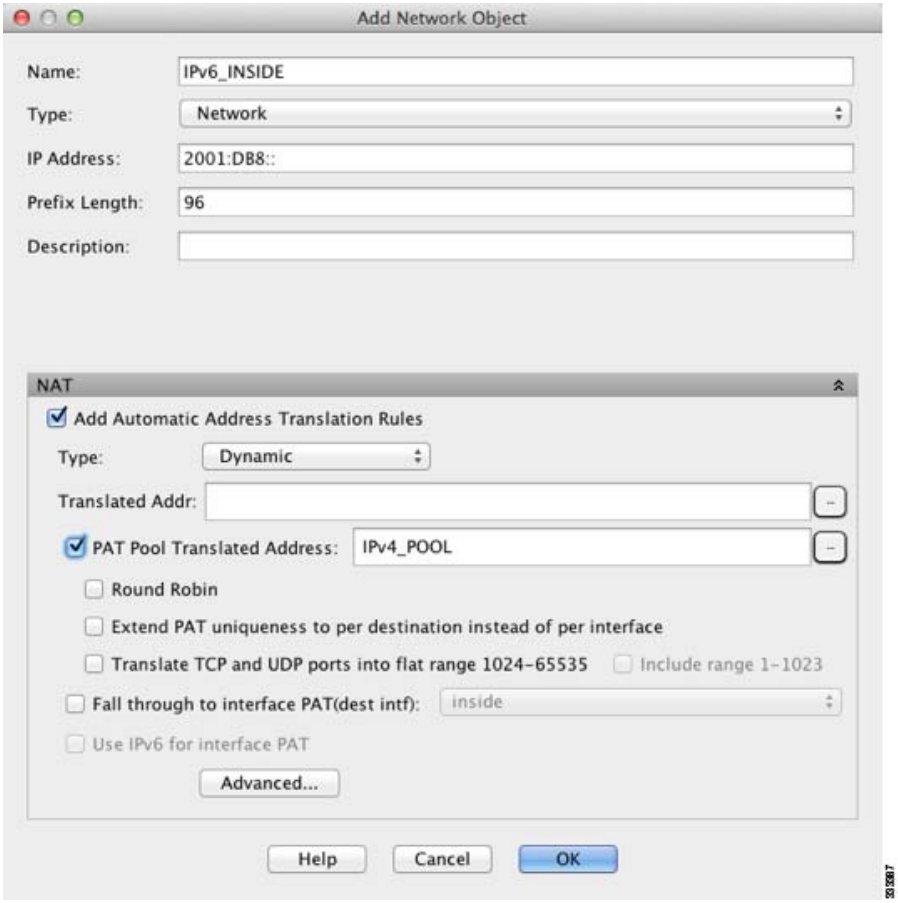


[NAT] で、[Add Automatic Address Translation Rules] チェックボックスをオフにします。

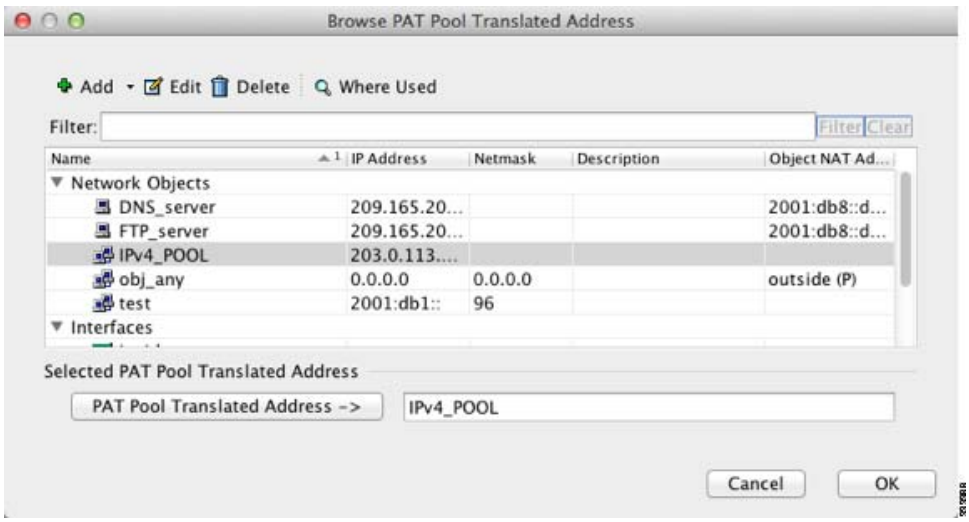
ステップ 4　内部 IPv6 ネットワークのための PAT を設定します。

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

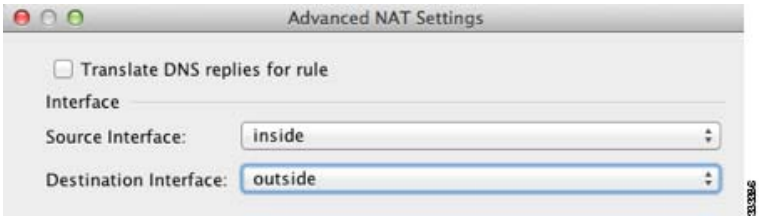
b. IPv6 ネットワーク アドレスを定義し、PAT プールを使用するダイナミック NAT を設定します。



c. [PAT Pool Translated Address] フィールドの横にある、[...] ボタンをクリックし、以前に作成した PAT プールを選択して、[OK] をクリックします。



d. 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設定するには、[Advanced] をクリックします。



e. [OK] をクリックして [Edit Network Object] ダイアログボックスに戻ります。

ステップ 5　[OK] をクリックし、さらに [Apply] をクリックします。

ネットワーク オブジェクト NAT の機能履歴

表 6-1 に、各機能変更と、それが実装されたプラットフォーム リリースを示します。ASDM は、複数のプラットフォーム リリースとの下位互換性があるため、サポートが追加された特定の ASDM リリースは一覧には含まれていません。

表 6-1　ネットワーク オブジェクト NAT の機能履歴

機能名	プラットフォーム リリース	機能情報
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]
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(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。 次の画面が変更されました。[Configuration] > [Firewall] > [NAT Rules] > [Add/Edit Network Object] > [Advanced NAT Settings]。

表 6-1　ネットワーク オブジェクト NAT の機能履歴（続き）

機能名	プラットフォーム リリース	機能情報
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。 次の画面が変更されました。[Configuration] > [Firewall] > [NAT Rules] > [Add/Edit Network Object]。
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。 次の画面が変更されました。[Configuration] > [Firewall] > [NAT Rules] > [Add/Edit Network Object]。 *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。 次の画面が変更されました。[Configuration] > [Firewall] > [NAT Rules] > [Add/Edit Network Object]。 *この機能は、8.5(1) または 8.6(1) では使用できません。*

表 6-1　ネットワーク オブジェクト NAT の機能履歴（続き）

機能名	プラットフォーム リリース	機能情報
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。 (注)　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。
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]。
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。

表 6-1　ネットワーク オブジェクト NAT の機能履歴 （続き）

機能名	プラットフォーム リリース	機能情報
Per-Session PAT	9.0(1)	Per-session PAT 機能によって PAT のスケーラビリティが向上し、クラスタリングの場合に各メンバ ユニットに独自の PAT 接続を使用できるようになります。Multi-Session PAT 接続は、マスター ユニットに転送してマスター ユニットを所有者とする必要があります。Per-Session PAT セッションの終了時に、ASA からリセットが送信され、即座に xlate が削除されます。このリセットによって、エンド ノードは即座に接続を解放し、TIME_WAIT 状態を回避します。対照的に、Multi-Session PAT では、PAT タイムアウトが使用されます（デフォルトでは 30 秒）。「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。 次の画面が導入されました。[Configuration] > [Firewall] > [Advanced] > [Per-Session NAT Rules]。