ネットワーク アドレス変換の設定

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き Cisco Catalyst スイッチ、PIX、FWSM、および IPS をサポートしますが、拡張機能はサポートしていません。

ここでは、ネットワーク アドレス変換（NAT）に関する一般的な概念と、変換タイプおよびさまざまな実装について説明します。

ネットワーク アドレス変換について

アドレス変換は、パケット内の実際のアドレスを、宛先ネットワーク上でルーティング可能な、マッピングされたアドレスで置き換えます。また、プロセスの一環として、デバイスにより変換データベースにその置換が記録されます。これらのレコードは、「xlate」エントリと呼ばれます。適切な xlate エントリが存在して、戻りパケットでのアドレス変換（マッピングされたアドレスの元の実アドレスの置換）を許可する必要があります。この手順は、「非変換」と呼ばれることもあります。したがって、ネットワークアドレス変換（NAT）は、実際には次の 2 つのステップから成ります。実アドレスからマッピングされたアドレスへの変換、およびリターントラフィックの逆変換。

NAT の主な機能の 1 つは、プライベート IP ネットワークがインターネットに接続できるようにすることです。ネットワーク アドレス変換により、プライベート IP アドレスはパブリック IP アドレスに置き換えられます。つまり、内部ネットワーク内のプライベート アドレスが、パブリックなインターネットで使用できる合法的なルーティング可能アドレスに変換されます。このようにして、NAT はパブリック アドレスを保護します。たとえば、ネットワーク全体で 1 つのパブリック アドレスだけを外部との通信に使用するように NAT ルールを設定できます。

NAT の他の機能には、次のおりです。

- セキュリティ：内部 IP アドレスを隠蔽することで、直接攻撃を阻止します。

- IP ルーティング ソリューション：重複する IP アドレスの問題がなくなります。
- 柔軟性：外部で使用可能なパブリック アドレスに影響を与えずに、内部 IP アドレッシング方式を変更できます。たとえば、インターネットにアクセス可能なサーバでは、インターネット用に固定の IP アドレスを保持できますが、内部的には、サーバ アドレスを変更できます。

シスコ デバイスでは、NAT（アウトバウンドの各ホスト セッションに、グローバルに一意のアドレスを提供する）とポート アドレス変換（PAT）（一意のポート番号を組み合わせた単一の同じアドレスを提供する）の両方を、最大で 64,000 個のアウトバウンドまたはインバウンドの同時ホスト セッションに対してサポートしています。NAT で使用するグローバル アドレスは、アドレス変換用に特別に指定したアドレス プールから取得されます。PAT で使用する一意のグローバル アドレスには、1 つのグローバル アドレスまたは指定されたインターフェイスの IP アドレスのいずれかを指定できます。

デバイスは、既存の NAT ルールが特定のトラフィックと一致した場合にアドレスを変換します。NAT ルールが一致しなかった場合、パケットの処理が続行されます。ただし、NAT 制御をイネーブルにしている場合は例外です。NAT 制御では、よりセキュリティの高いインターフェイス（内部）からよりセキュリティの低いインターフェイス（外部）へのパケット通過は NAT ルールに一致している必要があります。一致していない場合、パケットの処理は停止します。

シスコ デバイスは、インバウンドとアウトバウンドの両方の接続で、NAT または PAT を実行できます。インバウンド アドレスを変換するこの機能は、外部の、つまりセキュリティの高くないインターフェイス上のアドレスが、使用可能な内部 IP アドレスに変換されるため、「外部 NAT」と呼ばれます。アウトバウンド トラフィックを変換する場合と同様に、ダイナミック NAT、スタティック NAT、ダイナミック PAT、またはスタティック PAT を選択できます。必要に応じて、内部 NAT とともに外部 NAT を使用して、パケットの送信元 IP アドレスおよび宛先 IP アドレスの両方を変換できます。

（注） このマニュアルでは、すべての変換タイプを一般的に NAT と呼びます。それぞれのタイプの詳細については、アドレス変換のタイプ （3 ページ）を参照してください。NAT を説明する場合、内部および外部という用語は 2 つのインターフェイス間のセキュリティ関係を表します。セキュリティ レベルの高い方が内部で、セキュリティ レベルの低い方が外部になります。

以前の ASA バージョンおよび他のデバイスと比較すると、ASA バージョン 8.3 のリリースでは、ネットワーク アドレス変換を設定する、インターフェイスに依存しない簡単なアプローチが提供されています。詳細については、ASA 8.3 以降のデバイスでの「簡易」NAT について （5 ページ）を参照してください。

Cisco IOS ルータ

- Cisco IOS ルータにおける NAT ポリシー （7 ページ）
  - [NAT] ページ - [Interface Specification] （7 ページ）

- [NAT] ページ - [Static Rules] （8 ページ）
- [NAT] ページ - [Dynamic Rules] （13 ページ）
- [NAT] ページ - [Timeouts] （17 ページ）

PIX、FWSM、および ASA セキュリティ デバイス

- セキュリティ デバイスの NAT ポリシー （20 ページ）
- トランスペアレント モードの NAT （20 ページ）
- [Translation Options] ページ （23 ページ）
- **PIX、FWSM、および 8.3 よりも前の ASA デバイス**
  - PIX、FWSM、および 8.3 よりも前の ASA デバイスでの NAT の設定 （25 ページ）
  - アドレス プール （25 ページ）
  - [Translation Rules]：PIX、FWSM、および 8.3 よりも前の ASA （27 ページ）
- **ASA 8.3+ デバイス**
  - ASA 8.3+ デバイスでの NAT の設定 （46 ページ）
  - [Translation Rules]：ASA 8.3+ （46 ページ）
  - [Add NAT Rule]/[Edit NAT Rule] ダイアログボックス （49 ページ）
  - [Add Network/Host]/[Edit Network/Host] ダイアログボックス - [NAT] タブ （60 ページ）
  - Per-Session NAT ルール: ASA 9.0（1）+ （65 ページ）
  - [セッションごとのNATルールの追加（Add Per Session NAT Rule）]/[セッションごとのNATルールの編集（Edit Per Session NAT Rule）] ダイアログボックス （68 ページ）

関連項目

- アドレス変換のタイプ （3 ページ）
- ASA 8.3 以降のデバイスでの「簡易」NAT について （5 ページ）

アドレス変換のタイプ

次の表に、アドレス変換のさまざまなタイプについての簡単な説明を示します。

表 *1:* アドレス変換のタイプ

スタティック NAT	実際の送信元アドレスから特定のマッピングされたアドレスへの固定変換。個々の送信元アドレスは、IPプロトコルおよびポート番号に関係なく、常にマッピングされた同じアドレスに変換されます。
スタティック PAT	特定の TCP または UDP ポート番号を含む実際の送信元アドレスから特定のマッピングされたアドレスおよびポートへの固定変換。つまり、個々の送信元アドレス/ポートは、常にマッピングされた同じアドレス/ポートに変換されます。
ポリシー スタティック NAT	実際の送信元アドレスから特定のマッピングされたアドレスへの固定変換。宛先ネットワーク/ホストも指定しますが、サービスは常に IP です。
ポリシー スタティック PAT	特定の TCP または UDP ポート番号を含む実際の送信元アドレスから特定のマッピングされたアドレスおよびポートへの固定変換。宛先ネットワーク/ホストおよびサービスも指定します。
ダイナミック NAT	実際の送信元アドレスから、共有アドレス プールから取得されるマッピングされたアドレスへのダイナミック変換。個々の送信元アドレスを、プール内の使用可能な任意のアドレスにマッピングできます。
ダイナミック PAT	実際の送信元アドレスから単一のマッピングされたアドレスへの変換。関連するポート番号のダイナミック変換によって、単一性が実現されます。つまり、個々の実際のアドレス/ポートの組み合わせは、マッピングされた同じアドレスに変換されますが、一意のポートに割り当てられます。これは、「オーバーロード」と呼ばれることがあります。
ポリシー ダイナミック NAT	共有アドレス プールを使用する、指定したインターフェイス上の特定の送信元アドレス/宛先アドレス/サービスの組み合わせのダイナミック変換。変換の方向（アウトバウンドまたはインバウンド）も指定します。
アイデンティティ NAT	指定したアドレスがそれ自身に変換されます。つまり、事実上、変換されません。アウトバウンド接続だけに適用されます。アイデンティティ NAT は、スタティック NAT の特別なタイプです。
NAT Exempt	指定した送信元/宛先アドレスの組み合わせに対して変換がバイパスされます。接続は、アウトバウンド方向とインバウンド方向の両方で開始できます。

（注） これらのタイプの一部は ASA 8.3 以降のデバイスに適用されませんが、ASA 8.3+ デバイスではダイナミック NAT と PAT のオプションが提供されます。これは、ダイナミック PAT のバックアップ機能を伴うダイナミック NAT です。

ASA 8.3 以降のデバイスでの「簡易」NAT について

以前の ASA バージョンおよび他のデバイスと比較すると、ASA バージョン 8.3 のリリースでは、ネットワーク アドレス変換（NAT）を設定する簡単なアプローチが提供されています。NAT の設定は、以前のフローベース方式を、「元のパケット」から「変換後のパケット」へのアプローチで置き換えることによって簡素化されています。

デバイス上のすべての NAT ルール（スタティック NAT、ダイナミック PAT、およびダイナミック NAT）が単一のテーブルに示され、基本的にすべての NAT ルールの設定に同じダイアログボックスが使用されます。NAT ルールはインターフェイスに依存せず（つまり、インターフェイスは任意）、このことは、セキュリティ レベルにも依存しないということを意味します。

NAT ルールは、セキュリティ レベルに依存しなくなりました。すべてのインターフェイスで構成されるグローバルアドレス空間が利用可能であり、キーワード「any」を使用して指定されます。すべてのインターフェイスフィールドはデフォルトで**any**に設定されるため、特定のインターフェイスが指定されない限り、ルールはすべてのインターフェイスに適用されます。

ネットワーク オブジェクト NAT

対応する NAT ルールが指定したセキュリティ デバイスに自動的に適用されるように、ホスト、アドレス範囲、およびネットワーク オブジェクトに NAT プロパティを定義することもできます。これらのオブジェクトを使用するということは、必要な IP アドレス、サービス、ポート、および任意のインターフェイスを 1 度だけ入力すればよいということを意味します。自動的に生成されるこれらのオブジェクトベースのルールは、「ネットワーク オブジェクト NAT」ルールと呼ばれます。これらのルールはルールテーブルからは編集または削除できません。Policy Object Manager で適切なオブジェクトを編集する必要があります。ただし、ネットワークオブジェクトに定義した後でルールテーブルから編集できます。詳細については、[Add Network/Host]/[Edit Network/Host] ダイアログボックス - [NAT] タブ （60 ページ）を参照してください。

（注） ネットワークオブジェクト NAT ルールはデバイス固有であるため、ポリシービューの [変換ルール（Translation Rules）] テーブルには表示されません。

NAT テーブル

前述のとおり、デバイス上の NAT ルールはすべて単一のテーブルに表示されます。このテーブルは、「手動」セクション、ネットワークオブジェクト NAT ルールセクション、およびもう 1 つの手動ルールセクションの 3 つのセクションに分かれています。両方の手動セクションでルールを追加、編集、および順序付けできます。ネットワーク オブジェクト NAT ルールは自動的に追加および順序付けされます。前述のとおり、これらのルールを編集するには、関連するオブジェクトを編集する必要があります。

テーブル内の NAT ルールはトップダウン方式で最初に一致したルールから順に適用されます。つまり、パケットは、NAT ルールに一致した場合にだけ変換され、一致するとすぐに、その位置またはセクションに関係なく、NAT ルールの処理が停止します。

このテーブルを使用して、手動ルールの整理および管理を行うことができます。つまり、任意の順序でルールを挿入したり、ルールを再順序付けしたりできます。手動ルールの2つのセクションにより、自動オブジェクト ルールの前と後の両方に手動ルールを配置できます。

ネットワーク オブジェクト NAT ルールは、スタティック ルールがダイナミック ルールの前にくるように、自動的に配置されます。これらの2つのタイプは、それぞれさらに次のように順序付けされます。

- IP アドレスの数が最も少ないルール：1 つの IP アドレスを持つオブジェクトのルールのあとに、2 つのアドレスを持つオブジェクトのルールが表示され、そのあとに 3 つのアドレスを持つオブジェクトのルールが表示されるというように続きます。
- IP アドレス番号：同じ数の IP アドレスを持つオブジェクトについては、IP アドレス自体が番号順（昇順）になるように整列されます。たとえば、10.1.1.1 のルールのあとに 11.1.1.1 のルールが表示されます。
- オブジェクト名：IPアドレスが等しい場合は、オブジェクト名のアルファベット順にルールが順序付けされます。

また、変換は最初に一致したルールに基づくことに注意してください。

Destination Translation

手動のスタティック ルールでは、送信元アドレス変換に加えて、宛先アドレス変換も設定できます。送信元変換と宛先変換は、同じダイアログボックスで同時に定義できます。さらに、送信元変換にはスタティックまたはダイナミックを指定できますが、宛先変換は常にスタティックであり、手動ルールでだけ使用できます。

双方向または Twice NAT

手動のスタティックルールを作成するときに、[双方向（Bi-directional）] オプションを選択できます。このオプションでは、実際には 2 つのスタティック NAT ルール（両方向の変換を含む）を示す 1 つのエントリがルールテーブル内に作成されます。つまり、指定した送信元/変換後のアドレスのペアに対してスタティック ルールが作成されるとともに、変換後のアドレス/送信元のペアに対して、逆のルールが作成されます。

たとえば、[Source] フィールドが [Host1] で [Translated] フィールドが [Host2] のスタティック ルールを作成するときに [Bi-directional] を選択した場合、ルール テーブルに 2 つの行が追加されます。1 つは Host1 を Host2 に変換する行、もう 1 つは Host2 を Host1 に変換する行です。

この変換は、実際には2つのルールを取得および処理するために必要なルックアップが 1 つで済むため、「Twice NAT」と呼ばれることもあります。

多対 1 のアドレッシング

一般に、スタティック NAT ルールは、1 対 1 のアドレス マッピングを使用して設定されますが、多数の IP アドレスを少数または 1 つの IP アドレスにマッピングするスタティック NAT ルールを定義できるようになりました。機能的には、多対少数のマッピングは多対1のマッピングと同じですが、設定がより複雑になるため、必要に応じてアドレスごとに多対1のルールを作成することを推奨します。

多対1のアドレッシングは、たとえば、要求を内部ネットワークにリダイレクトするロードバランサにアクセスするためにパブリック IP アドレスの範囲を使用する場合などに役立つことがあります。

関連項目

- [Add NAT Rule]/[Edit NAT Rule] ダイアログボックス （49 ページ）
- [Add Network/Host]/[Edit Network/Host] ダイアログボックス - [NAT] タブ （60 ページ）

Cisco IOS ルータにおける NAT ポリシー

[NAT] ポリシー ページの次のタブから Cisco IOS ルータ上の NAT ポリシーを設定できます。

- [NAT] ページ - [Interface Specification] （7 ページ）
- [Add NAT Static Rule]/[Edit NAT Static Rule] ダイアログボックス （10 ページ）
- [NAT] ページ - [Dynamic Rules] （13 ページ）
- [NAT] ページ - [Timeouts] （17 ページ）

ネットワーク アドレス変換（NAT）はプライベートな内部 LAN アドレスをグローバルにルーティング可能な IP アドレスに変換します。NAT を使用すると、少ない数のパブリック IP アドレスで多数のホストにグローバル接続を提供できます。

詳細については、 ネットワーク アドレス変換について （1 ページ）を参照してください。

ナビゲーション パス

- （デバイスビュー）ポリシーセレクタから [NAT] を選択します。
- （ポリシービュー）ポリシータイプセレクタから [NAT（ルータ）（NAT (Router)）] を選択します。共有ポリシー セレクタから既存のポリシーを選択するか、または新しいポリシーを作成します。

[NAT] ページ - [Interface Specification]

NAT ルールを作成する前に、内部および外部インターフェイスを指定して、変換されるトラフィックの「方向」を定義する必要があります。内部インターフェイスは、通常、ルータが提供する LAN に接続されます。外部インターフェイスは、通常、組織の WAN またはインターネットに接続されます。少なくとも内部インターフェイスおよび外部インターフェイスを1つずつ指定して、ルータがネットワーク アドレス変換を実行できるようにする必要があります。

内部および外部の指定は、変換ルールを解釈するときに使用されます。つまり、内部インターフェイスに接続されたアドレスが、外部インターフェイス上のアドレスに変換されます。これらのインターフェイスの定義が完了したあと、これらをすべてのスタティックおよびダイナミック NAT 変換ルールに使用します。

[NAT] ポリシー ページの [Interface Specification] タブを使用して、内部および外部インターフェイスを指定します。

ナビゲーション パス

- （デバイスビュー）ポリシーセレクタから [NAT] を選択し、次に [インターフェイスの仕様（Interface Specification）] タブをクリックします。
- （ポリシービュー）ポリシータイプセレクタから [NAT（ルータ）（NAT (Router)）] > [変換ルール（Translation Rules）] を選択します。既存のポリシーを選択するか新しいポリシーを作成し、[インターフェイスの仕様（Interface Specification）] タブをクリックします。

内部インターフェイスと外部インターフェイスの定義

[NAT内部インターフェイス（NAT Inside Interfaces）] および [NAT外部インターフェイス（NAT Outside Interfaces）] フィールドに、内部および外部インターフェイスのインターフェイス名またはインターフェイスロールをそれぞれ入力するか、または選択します。複数の名前またはロールは、カンマで区切ります（Ethernet1/1, Ethernet1/2 など）。両方のフィールドに同じ名前は入力できないことに注意してください。

関連項目

- Cisco IOS ルータにおける NAT ポリシー （7 ページ）
- [NAT] ページ - [Static Rules] （8 ページ）
- [NAT] ページ - [Dynamic Rules] （13 ページ）
- [NAT] ページ - [Timeouts] （17 ページ）

[NAT] ページ - [Static Rules]

変換が必要なローカル アドレスと、そのローカル アドレスが変換されるグローバル アドレスを指定して、スタティック NAT ルールを定義します。これは、スタティックまたは固定のマッピングであり、ローカル アドレスは常に同じグローバル アドレスに変換されます。

単一ホストのアドレスを変換するスタティック NAT ルールと、サブネット内の複数のアドレスを変換するスタティック ルールを定義できます。複数のローカル アドレスで同じグローバル アドレスを使用する必要がある場合は、必要なポート リダイレクト情報を定義する必要があります。リダイレクト情報では、グローバル アドレスを使用して各ローカル アドレスにそれぞれ異なるポートを定義します。

（注） VPN を介して送信されるトラフィックに対しては NAT を実行しないことを強く推奨します。このトラフィックでアドレスを変換すると、暗号化された状態ではなく暗号化されていない状態で VPN を介して送信されます。

スタティック ルールの作成手順は、変換されるアドレスがポート、単一ホスト、またはサブネット全体のいずれを示しているかで決まります。

- 単一ホスト用のスタティック NAT ルールを定義するには、変換する元のアドレスと、そのアドレスが変換されるグローバルアドレスを入力します。グローバルアドレスは、デバイス上のインターフェイスから取得できます。
- サブネット用のスタティック NAT ルールを定義するには、元のアドレスとしてサブネット内（サブネットマスクを含む）のアドレスの 1 つを入力し、変換されたアドレスとして使用するグローバルアドレスの 1 つを入力します。ルータは、入力したサブネットマスクに基づいて残りのアドレスを設定します。
- ポート用のスタティック NAT ルールを定義するには、元の IP アドレスと、そのアドレスが変換されるグローバルアドレスを入力します。グローバルアドレスは、デバイス上のインターフェイスから取得できます。さらに、ポートが使用するプロトコルと、ローカル ポート番号およびグローバル ポート番号も選択する必要があります。

これらのルールを追加および編集するには、[Add Static NAT Rule] および [Edit Static NAT Rule] ダイアログボックスを使用します。このページのテーブルに表示されるフィールドについては、[Add NAT Static Rule]/[Edit NAT Static Rule] ダイアログボックス （10 ページ）を参照してください。

はじめる前に

- NAT に使用する内部インターフェイスと外部インターフェイスを定義します。[NAT] ページ - [Interface Specification] （7 ページ）を参照してください。

ナビゲーション パス

- （デバイスビュー）ポリシーセレクタから [NAT] を選択し、次に [スタティックルール（Static Rules）] タブをクリックします。
- （ポリシービュー）ポリシータイプセレクタから [NAT（ルータ）（NAT (Router)）] > [変換ルール（Translation Rules）] を選択します。既存のポリシーを選択するか新しいポリシーを作成し、[スタティックルール（Static Rules）] タブをクリックします。

関連項目

- Cisco IOS ルータにおける NAT ポリシー （7 ページ）
- [NAT] ページ - [Dynamic Rules] （13 ページ）
- [NAT] ページ - [Timeouts] （17 ページ）
- Security Manager の標準のルール テーブルに関する項：
  - ルール テーブルの使用
  - テーブルのフィルタリング

- テーブル カラムおよびカラム見出しの機能

[Add NAT Static Rule]/[Edit NAT Static Rule] ダイアログボックス

[Add NAT Static Rule]/[Edit NAT Static Rule] ダイアログボックスを使用して、スタティック アドレス変換ルールを追加または編集します。タイトルを除き、2 つのダイアログボックスは同じです。

ナビゲーション パス

[NAT] ページ - [Static Rules] （8 ページ）タブに移動します。テーブルの下にある [追加（Add）] ボタンをクリックして新しいルールを追加するか、テーブルでルールを選択し、[編集（Edit）] をクリックしてそのルールを更新します。

関連項目

- インターフェイス ロール オブジェクトについて

フィールド リファレンス

表 2 : [Add NAT Static Rule]/[Edit NAT Static Rule] ダイアログボックス

要素	説明
Static Rule Type	このスタティック ルールで変換されるローカル アドレスのタイプ。 • [Static Host]：単一ホストでスタティック アドレス変換が必要な場合。 • [Static Network]：サブネットでスタティック アドレス変換が必要な場合。 • [Static Port]：単一ポートでスタティック アドレス変換が必要な場合。このオプションを選択した場合は、[Port Redirection] パラメータを定義する必要があります。
元のアドレス	IP アドレス、または変換されるアドレスを示すネットワーク/ホスト オブジェクトの名前。オブジェクト名を入力するか、または選択できます。 ネットワーク/ホストオブジェクトは、ネットワーク、ホスト、またはこれらの両方を表す IP アドレスの論理集合です。詳細については、ネットワーク/ホストオブジェクトについてを参照してください。 （注） Security Manager の管理トラフィックを変換してしまう可能性があるため、このルータに属するローカル アドレスは入力しないでください。このトラフィックを変換すると、ルータと Security Manager 間の通信が失われます。

要素	説明
Translated Address	ダイアログボックスのこのセクションのオプションを使用して、元のアドレスが変換されるアドレスを指定します。 • [IPの指定（Specify IP）]：IP アドレス、または変換後のアドレスを提供するネットワーク/ホストオブジェクトの名前を指定するには、このオプションを選択します。IPアドレス、またはネットワーク/ホストオブジェクトの名前を[変換後のIP/ネットワーク（Translated IP/Network）]フィールドに追加します。オブジェクト名を入力するか、または選択できます。 • [インターフェイスIPの使用（Use Interface IP）]：特定のインターフェイスに割り当てられているIPアドレスを変換後のアドレスとして使用するように指定するには、このオプションを選択します。対象の[インターフェイス（Interface）]の名前を入力するか、選択します。（これは、通常、変換されたパケットがルータから発信される際の発信元のインターフェイスです）。 （注） このオプションは、ルールのタイプとして[Static Network]を選択している場合には使用できません。1 つのインターフェイスに 1 つのスタティック ルールしか定義できません。
Port Redirection	これらのパラメータは、アドレス変換のポート情報を指定します。ポートアドレス変換を使用すると、デバイスごとに異なるポートを指定しているかぎり、複数のデバイスに同じパブリック IP アドレスを使用できます。 （注） これらのポートは、ルールのタイプとして[Static Port]を選択している場合にだけ使用できます。 [リダイレクトポート（Redirect Port）]：ルールのタイプとして[スタティックポート（Static Port）]を選択した場合、このチェックボックスは自動的にオンになります。変更はできません。次のフィールドに、適切な情報を入力します。 • [プロトコル（Protocol）]：これらのポートで使用する通信プロトコル：TCP または UDP。 • [ローカルポート（Local Port）]：送信元ネットワーク上のポート番号。有効値の範囲は 1 ～ 65535 です。 • [グローバルポート（Global Port）]：ルータによってこの変換に使用される宛先ネットワーク上のポート番号。有効値の範囲は 1 ～ 65535 です。

要素	説明
詳細設定（Advanced）	このセクションには、任意の高度な変換オプションが含まれています。 （注） [Advanced] オプションは、変換されたアドレスの定義方法として [Specify IP] オプションを選択している場合にだけ使用できます。 • [No Alias]：選択すると、グローバル IP アドレス変換の自動エイリアス設定がディセーブルになります。 内部グローバル プールとして使用する NAT プールが、接続されているサブネット上のアドレスで構成されている場合、ルータでこれらのアドレスのアドレス解決プロトコル（ARP）要求に応答できるように、そのアドレスに対してエイリアスが生成されます。 選択を解除すると、グローバル アドレスのエイリアスが許可されます。 • [No Payload]：選択すると、ペイロード内の埋め込みアドレスまたはポートの変換が禁止されます。 ペイロード オプションは、同じ IP アドレスを共有している重複ネットワーク上のデバイス間で NAT を実行します。外部デバイスが DNS クエリーを送信して内部デバイスにアクセスした場合、DNS 応答のペイロード内のローカル アドレスは、関連する NAT ルールに応じて、グローバル アドレスに変換されます。 この機能は、[No Payload] オプションを選択することでディセーブルにできます。ディセーブルにしなかった場合、ペイロード内の埋め込みアドレスおよびポートが変換されることがあります。詳細については、重複するネットワークのペイロード オプションのディセーブル化 （12 ページ）を参照してください。 • [Create Extended Translation Entry]：オンにすると、変換テーブル内に拡張変換エントリ（アドレスおよびポート）が作成されます。これにより、複数のグローバル アドレスを単一のローカル アドレスに関連付けることができます。これがデフォルトです。 このオプションをオフにすると、簡単な変換エントリが作成され、単一のグローバル アドレスをローカル アドレスに関連付けできるようになります。 （注） このオプションは、ルールのタイプとして [Static Port] を選択している場合には使用できません。

重複するネットワークのペイロード オプションのディセーブル化

すでに合法的に所有されインターネットまたは外部ネットワーク上のデバイスに割り当てられている IP アドレスを、独自のネットワーク上の別のデバイスに割り当てると、ネットワークの重複が発生します。また、ネットワークの重複は、それぞれのネットワーク内で RFC 1918 IP アドレスを使用している 2 つの会社をマージした場合にも発生する可能性があります。これらの 2 つのネットワークは、可能であれば、すべてのデバイスのアドレスを再指定することなく、通信できる必要があります。

この通信は、次のように実現されます。内部デバイスの IP アドレスは外部デバイスに割り当てられているアドレスと同じであるため、外部デバイスは内部デバイスの IP アドレスを使用できません。代わりに、外部デバイスは内部デバイスのドメイン名を問い合わせるドメインネームシステム（DNS）クエリを送信します。このクエリーの送信元は外部デバイスの IP アドレスであり、この IP アドレスは指定したアドレス プールのアドレスに変換されます。内部ネットワーク上に配置されている DNS サーバーは、パケットのデータ部分に格納されている内部デバイスのドメイン名に関連付けられた IP アドレスを使用して応答します。応答パケットの宛先アドレスは外部デバイスのアドレスに変換され、応答パケットのデータ部分に格納されているアドレスは別のアドレスプールのアドレスに変換されます。このような方法で、外部デバイスは、内部デバイスの IP アドレスが 2 番めのアドレス プールのアドレスの 1 つであることを学習して、内部デバイスとの通信時にこのアドレスを使用します。NAT を実行しているルータは、この時点で変換を処理します。

ペイロード内のアドレスの変換をディセーブルにするには、グローバル IP 変換に基づいたスタティック NAT ルールを作成するときに、[ペイロードなし（No Payload）] オプションをオンにします。

[NAT] ページ - [Dynamic Rules]

ルータの [NAT] ページの [NATダイナミックルール（NAT Dynamic Rules）] タブを使用して、ダイナミックアドレス変換ルールを管理します。ダイナミック アドレス変換ルールは、特定のインターフェイスの IP アドレス（ダイナミック ポート変換を使用）、または宛先ネットワーク内でグローバルに一意であるアドレス プール内のアドレスを使用して、ホストをアドレスに動的にマッピングします。

ダイナミック NAT ルールの定義

ダイナミック NAT ルールを定義するには、最初に、変換が必要なトラフィックをルールで指定しているアクセス コントロール リスト（ACL）を選択します。

次に、変換後の IP アドレスを持つインターフェイスを選択するか、または使用されるアドレス プールを定義する必要があります。プールを定義するには、アドレスの範囲を指定して、その範囲に一意の名前を指定します。複数の範囲を指定できます。ルータは、インターネットまたは別の外部ネットワークとの接続に、プール内の使用可能なアドレス（スタティック変換にも、独自の WAN IP アドレスにも使用されていないアドレス）を使用します。アドレスは、不用になると、あとで別のデバイスに動的に割り当てられるようにアドレス プールに戻されます。

ネットワークのアドレッシング要求がダイナミック NAT プール内の使用可能なアドレスの数を超えた場合は、ポートアドレス変換（PAT）機能（オーバーロードとも呼ばれる）を使用して、多数のプライベート アドレスを 1 つまたは少数のパブリック IP アドレス グループに関連付け、ポート アドレッシングを使用して各変換を一意にすることができます。PAT をイネーブルにすると、ルータは各アウトバウンド変換スロットの IP アドレスに対して一意のポート番号を選択します。この機能は、アウトバウンド接続に割り当て可能な十分な数の一意の IP アドレスがない場合に役立ちます。ポート アドレス変換は、アドレス プールが枯渇するまでは行われません。

（注） デフォルトでは、Security Manager は VPN を介して送信されるトラフィックに対して NAT を実行しません。それ以外の場合、暗号化の前には常に NAT が実行されるため、インターフェイスに定義されている NAT ACL とクリプト ACL の両方に含まれるすべてのトラフィックが暗号化されずに送信されます。ただし、このデフォルト設定は変更できます。

ヒント [Global VPN Settings] ページから直接、VPN トポロジのスポーク上のスプリット トンネル トラフィックに対して PAT を実行できます。スポークごとにダイナミック NAT ルールを作成する必要はありません。個々のデバイスに定義した NAT ルールによって、VPN 設定は上書きされます。詳細については、VPN グローバル NAT 設定を参照してください。

これらのルールを追加および編集するには、[Add Dynamic NAT Rule] および [Edit Static NAT Rule] ダイアログボックスを使用します。このページのテーブルに表示されるフィールドについては、[Add NAT Dynamic Rule]/[Edit NAT Dynamic Rule] ダイアログボックス （15 ページ）を参照してください。

はじめる前に

- NAT に使用する内部インターフェイスと外部インターフェイスを定義します。[NAT] ページ - [Interface Specification] （7 ページ）を参照してください。

ナビゲーション パス

- （デバイスビュー）ポリシー セレクタから [NAT] を選択し、次に [ダイナミックルール（Dynamic Rules）] タブをクリックします。
- （ポリシービュー）ポリシータイプセレクタから [NAT（ルータ）（NAT (Router)）] > [変換ルール（Translation Rules）] を選択します。既存のポリシーを選択するか新しいポリシーを作成し、[ダイナミックルール（Dynamic Rules）] タブをクリックします。

関連項目

- Cisco IOS ルータにおける NAT ポリシー （7 ページ）
- [NAT] ページ - [Static Rules] （8 ページ）
- [NAT] ページ - [Timeouts] （17 ページ）
- Security Manager の標準のルール テーブルに関する項：
  - ルール テーブルの使用
  - テーブルのフィルタリング
  - テーブル カラムおよびカラム見出しの機能

[Add NAT Dynamic Rule]/[Edit NAT Dynamic Rule] ダイアログボックス

[Add NAT Dynamic Rule]/[Edit NAT Dynamic Rule] ダイアログボックスを使用して、ダイナミック アドレス変換ルールを追加または編集します。タイトルを除き、2つのダイアログボックスは同じです。

ナビゲーション パス

[NAT] ページ - [Dynamic Rules] （13 ページ）タブに移動します。テーブルの下にある [追加（Add）] ボタンをクリックして新しいルールを追加するか、テーブルでルールを選択し、[編集（Edit）] をクリックしてそのルールを更新します。

関連項目

- アクセス コントロール リスト オブジェクトの作成
- インターフェイス ロール オブジェクトについて

フィールド リファレンス

表 3 : [Add NAT Dynamic Rule]/[Edit NAT Dynamic Rule] ダイアログボックス

要素	説明
トラフィック フロー	[アクセスリスト（Access List）] フィールドで、ダイナミック変換が必要なアドレスをエントリで定義しているアクセス制御リスト（ACL）オブジェクトの名前を入力するか選択します。 （注） 指定した ACL で、このルータ上のデバイス アドレスを経由する Security Manager 管理トラフィックの変換が許可されていないことを確認してください。このトラフィックを変換すると、ルータと Security Manager 間の通信が失われます。

要素	説明
Translated Address	ダイアログボックスのこのセクションのオプションを使用して、ダイナミック変換に使用する方式およびアドレスを指定します。 • [ユーザーインターフェイスIP（Use Interface IP]：特定のインターフェイスに割り当てられているグローバルに登録された IP アドレスを変換後のアドレスとして使用するように指定するには、このオプションを選択します。ポートアドレッシングによって、各変換が一意であることが保証されます（[Enable Port Translation (Overload)] オプションは、[Use Interface IP] を選択すると自動的にオンになります）。 対象の [インターフェイス（Interface）] の名前を入力するか、選択します。これは、通常、変換されたパケットがルータから発信される際の発信元のインターフェイスです。つまり、インターフェイスまたはインターフェイス ロールは、ルータ上の外部インターフェイスを示している必要があります（[NAT] ページ - [Interface Specification] （7 ページ）を参照）。 • [アドレスプール（Address Pool）]：[ネットワーク範囲（Network Ranges）] プールで指定したアドレスに基づいてアドレス変換を実行させるには、このオプションを選択します。 プレフィックスを含めた 1 つまたは複数のアドレス範囲を入力します。書式は min1-max1/prefix（CIDR 表記）を使用します（「prefix」は有効なネットマスクを示します）。たとえば、172.16.0.0-172.31.0.223/12 のように入力します。 必要な数のアドレス範囲をアドレス プールに追加できますが、すべての範囲で同じプレフィックスを共有している必要があります。複数のエントリを指定する場合は、カンマで区切ります。

要素	説明
設定	このセクションには 2 つのオプションが含まれています。 • [ポート変換（オーバーロード）の有効化（Enable Port Translation (Overload)）]：選択すると、アドレスプール内のグローバルアドレスの供給が枯渇した場合に、ルータはポートアドレッシング（PAT）を使用します。選択を解除すると、PAT は使用されません。 （注） [Translated Address] セクションで [Use Interface IP] を選択した場合、このチェックボックスは自動的にオンになります。変更はできません。 • [VPNトラフィックを変換しない（サイト間VPNのみ）（Do Not Translate VPN Traffic (Site-to-Site VPN only)）]：このオプションの選択を解除すると、サイト間 VPN 向けのトラフィックに対してアドレス変換が許可されます。 選択すると、VPN トラフィックに対してアドレス変換は実行されません。選択を解除した場合、ルータは、NAT ACL とクリプト ACL 間でアドレスが重複している場合に、VPN トラフィックに対してアドレス変換を実行します。 （注） このオプションの選択は解除しないことを強く推奨します。解除した場合、NAT ACL とクリプト ACL の両方に定義されているすべてのトラフィックが暗号化されずに送信されます。IPsec に対して NAT を実行する場合も、このオプションは選択したままにしておくことを推奨します。このオプションを選択しても、重複するネットワークから到着したアドレスの変換は実行されます。 この設定は、NAT ACL がサイト間 VPN で使用されるクリプト ACL と重複している状況でだけ適用されます。インターフェイスは最初に NAT を実行するため、この重複内のアドレスから到着したトラフィックはすべて変換され、その結果、トラフィックは暗号化されずに送信されます。このチェックボックスをオンのままにすると、このような問題は発生しなくなります。 （注） このオプションは、リモート アクセス VPN には適用されません。

[NAT] ページ - [Timeouts]

ルータの [NAT] ページの [NATタイムアウト（NAT Timeouts）] タブを使用して、ポートアドレス（オーバーロード）変換のタイムアウト値を管理します。これらのタイムアウトにより、指定した非アクティブ期間が経過したあと、ダイナミック変換は期限切れになります。また、このページのオプションを使用すると、ダイナミック NAT テーブルに格納できるエントリの数を制限したり、PAT 処理を含まないすべてのダイナミック変換に対してデフォルトのタイムアウトを変更したりできます。

ダイナミック NAT のタイムアウトについて

ダイナミック NAT 変換には不使用に対するタイムアウト時間があり、この時間が経過すると、ダイナミック NAT 変換は期限切れとなり、変換テーブルから削除されます。各変換エントリ

には、そのエントリを使用するトラフィックの状況に応じた追加情報が含まれているため、オーバーロード機能をイネーブルにして PAT を実行する場合は、これらのタイムアウトを詳細に制御できるさまざまな値を指定できます。

たとえば、非 DNS 変換は、デフォルトでは 5 分後にタイムアウトしますが、DNS 変換は 1 分後にタイムアウトします。さらに、TCP 変換は、RST または FIN がストリーム上で検出されないかぎり 24 時間後にタイムアウトし、検出された場合は、1 分後にタイムアウトします。これらのタイムアウト値はいずれも変更できます。

（注） すべてのダイナミック ルールに対してポート変換（オーバーロード）機能をディセーブルにしている場合は、PAT 関連のタイムアウト値を入力する必要はありません。ただし、PAT 以外のダイナミック変換のデフォルト タイムアウト値は変更できます（デフォルトでは、すべてのダイナミック変換は 24 時間後に期限切れになります）。オーバーロード機能の詳細については、[Add NAT Dynamic Rule]/[Edit NAT Dynamic Rule] ダイアログボックス （15 ページ）を参照してください。

ナビゲーション パス

- （デバイスビュー）ポリシーセレクタから [NAT] を選択し、次に [タイムアウト（Timeouts）] タブをクリックします。
- （ポリシービュー）ポリシータイプセレクタから [NAT（ルータ）（NAT (Router)）] > [変換ルール（Translation Rules）] を選択します。既存のポリシーを選択するか新しいポリシーを作成してから、[タイムアウト（Timeouts）] タブをクリックします。

関連項目

- [NAT] ページ - [Interface Specification] （7 ページ）
- [NAT] ページ - [Static Rules] （8 ページ）
- [NAT] ページ - [Dynamic Rules] （13 ページ）

フィールド リファレンス

表 4 : [NAT Timeouts] タブ

要素	説明
エントリの最大数（Max Entries）	ダイナミック NAT テーブルに格納できるエントリの最大数。1 ～ 2147483647 の値を入力できます。またはこのフィールドを空白（デフォルト）のままにできます。空白にすると、テーブル内のエントリの数は無制限になります。
Timeout (sec.)	ダイナミック変換が期限切れになるまでの秒数。PAT（オーバーロード）変換には適用されません。デフォルトは 86400 秒（24 時間）です。

要素	説明
UDP Timeout (sec.)	ユーザー データグラム プロトコル（UDP）ポートに適用されるタイムアウト値。デフォルトは 300 秒（5 分）です。 （注） この値が適用されるのは、ダイナミック NAT ルールでポート変換（オーバーロード）がイネーブルになっている場合だけです。[Add NAT Dynamic Rule]/[Edit NAT Dynamic Rule] ダイアログボックス （15 ページ）を参照してください。
DNS Timeout (sec.)	Domain Naming System（DNS; ドメイン ネーミング システム）サーバー接続に適用されるタイムアウト値。デフォルトは 60 秒です。 （注） この値が適用されるのは、ダイナミック NAT ルールでポート変換（オーバーロード）がイネーブルになっている場合だけです。[Add NAT Dynamic Rule]/[Edit NAT Dynamic Rule] ダイアログボックス （15 ページ）を参照してください。
TCP Timeout (sec.)	伝送制御プロトコル（TCP）ポートに適用されるタイムアウト値。デフォルトは 86400 秒（24 時間）です。 （注） この値が適用されるのは、ダイナミック NAT ルールでポート変換（オーバーロード）がイネーブルになっている場合だけです。[Add NAT Dynamic Rule]/[Edit NAT Dynamic Rule] ダイアログボックス （15 ページ）を参照してください。
FINRST Timeout (sec.)	終了（FIN）パケットまたはリセット（RST）パケット（どちらも接続を終了させる）が TCP ストリーム内で検出された場合に適用されるタイムアウト値。デフォルトは 60 秒です。 （注） この値が適用されるのは、ダイナミック NAT ルールでポート変換（オーバーロード）がイネーブルになっている場合だけです。[Add NAT Dynamic Rule]/[Edit NAT Dynamic Rule] ダイアログボックス （15 ページ）を参照してください。
ICMP Timeout (sec.)	インターネット制御メッセージ プロトコル（ICMP）フローに適用されるタイムアウト値。デフォルトは 60 秒です。 （注） この値が適用されるのは、ダイナミック NAT ルールでポート変換（オーバーロード）がイネーブルになっている場合だけです。[Add NAT Dynamic Rule]/[Edit NAT Dynamic Rule] ダイアログボックス （15 ページ）を参照してください。

要素	説明
PPTP Timeout (sec.)	NAT Point-to-Point Tunneling Protocol（PPTP; ポイントツーポイント トンネリング プロトコル）フローに適用されるタイムアウト値。デフォルトは 86400 秒（24 時間）です。 （注） この値が適用されるのは、ダイナミック NAT ルールでポート変換（オーバーロード）がイネーブルになっている場合だけです。[Add NAT Dynamic Rule]/[Edit NAT Dynamic Rule] ダイアログボックス （15 ページ）を参照してください。
SYN Timeout (sec.)	同期伝送（SYN）メッセージ（正確なクロッキングに使用）が検出されたあと、TCP フローに適用されるタイムアウト値。デフォルトは 60 秒です。 （注） この値が適用されるのは、ダイナミック NAT ルールでポート変換（オーバーロード）がイネーブルになっている場合だけです。[Add NAT Dynamic Rule]/[Edit NAT Dynamic Rule] ダイアログボックス （15 ページ）を参照してください。

セキュリティ デバイスの NAT ポリシー

ここでは、管理対象のセキュリティ アプライアンス（PIX ファイアウォール、Catalyst スイッチの Firewall Service Modules（FWSM; ファイアウォール サービス モジュール）、8.3 よりも前のバージョンの Adaptive Security Appliance（ASA; 適応型セキュリティ アプライアンス）、および ASA 8.3+ デバイス）でネットワーク アドレス変換（NAT）オプションを設定する方法について説明します。説明の順序は次のとおりです。

- トランスペアレント モードの NAT （20 ページ）
- [Translation Options] ページ （23 ページ）
- **PIX、FWSM、および 8.3 よりも前の ASA**
  - PIX、FWSM、および 8.3 よりも前の ASA デバイスでの NAT の設定 （25 ページ）
  - アドレス プール （25 ページ）
- **ASA 8.3+**
  - ASA 8.3+ デバイスでの NAT の設定 （46 ページ）
  - [Translation Rules]：ASA 8.3+ （46 ページ）

トランスペアレント モードの NAT

トランスペアレント モードで動作しているセキュリティ アプライアンスで NAT を使用すると、上流または下流のルータでそれらのネットワークに対して NAT を実行する必要性がなくなります。トランスペアレント モードの NAT には、次の要件および制限があります。

- マッピングされたアドレスがトランスペアレントファイアウォールと同じネットワークにない場合、マッピングされたアドレス用に、（セキュリティアプライアンス経由で）下流のルータを指し示すスタティック ルートを上流のルータに追加する必要があります。
- 実際の宛先アドレスが直接セキュリティアプライアンスに接続されていない場合は、実際の宛先アドレス用に、下流のルータを指し示すスタティック ルートをセキュリティ アプライアンスに追加する必要もあります。NAT を使用しない場合、上流のルータから下流のルータへのトラフィックは MAC アドレス テーブルを使用するため、セキュリティ アプライアンス上のルートを必要としません。ただし、NAT を使用すると、セキュリティ アプライアンスは MAC アドレス ルックアップの代わりにルート ルックアップを使用するため、下流のルータへのスタティック ルートが必要になります。
- トランスペアレント ファイアウォールにはインターフェイス IP アドレスがないため、インターフェイス PAT を使用できません。
- ARP インスペクションはサポートされていません。さらに、何らかの理由でセキュリティアプライアンスの片側にあるホストからもう片側にあるホストに ARP 要求が送信され、送信側ホストの実アドレスが同じサブネット上の別のアドレスにマップされている場合、その実アドレスは ARP 要求で表示されたままになります。

[CGNATマップ（CGNAT Map）] ページ

バージョン 4.20 以降、Cisco Security Manager は、シングル、マルチコンテキスト、およびルーテッドモードで動作する ASA 9.13(1) デバイスのアドレスおよびポート（CGNAT マップ）ドメインのキャリアグレード NAT マッピングをサポートしています。この機能は、デフォルトまたは基本的なマッピングルールを使用して MAP ドメインを構成するのに役立ちます。

（注） トランスペアレントモードでは CGNAT マップはサポートされていません。

ナビゲーション パス

- （デバイスビュー）デバイスポリシーセレクタから **[NAT] > [CGNATマップ（CGNAT MAP）]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから **[NAT（PIX/ASA/FWSM）] > [CGNAT マップ（CGNAT MAP）]** を選択します。共有ポリシーセレクタから既存のポリシーを選択するか、または [CGNATマップ（CGNAT MAP）] を右クリックして新しい CGNAT マップポリシーを作成します。

関連項目

- セキュリティ デバイスの NAT ポリシー （20 ページ）

フィールド リファレンス

表 *5:*

要素	説明
マップドメインの追加（Add Map Domain）	選択すると、基本またはデフォルトのマッピングルールを使用してマップドメインを追加できます。
マップドメイン名（Map Domain Name）	マッピングルールを適用する必要があるマップドメインの名前を入力します。
Basic Mapping Rule	[基本マッピングルール（Basic Mapping Rule）] チェックボックスをオンにして、IPv4 および IPv6プレフィックス、共有率、および開始ポート番号を指定します。
Default Mapping Rule	IPv6 プレフィックスを入力して、デフォルトのマッピングルールを適用します。

[グローバルオプション（Global Options）] ページ

Cisco Security Manager バージョン 4.9 は、ASA デバイス 9.5(1) 以降のポートブロック割り当てのブロックサイズとホストあたりの最大ブロック数を設定するキャリアグレードNATをサポートしています。グローバルオプションを設定するには、[グローバルオプション（Global Options）] ページを使用します。

ナビゲーション パス

- （デバイスビュー）デバイスポリシーセレクタから **[NAT]>[グローバルオプション（Global Options）]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから **[NAT（PIX/ASA/FWSM）]>[グローバルオプション（Global Options）]** を選択します。共有ポリシーセレクタから既存のポリシーを選択するか、または [グローバルオプション（Global Options）] を右クリックして新しいポリシーを作成します。

関連項目

- セキュリティ デバイスの NAT ポリシー （20 ページ）
- [Add NAT Rule]/[Edit NAT Rule] ダイアログボックス （49 ページ）

フィールド リファレンス

表 *6 : [*グローバルオプション（***Global Options***）*]* ページ

要素	説明
xlate block-allocation size	32 ～ 4096 の値を入力します。デフォルト値は 512 です。
xlate block-allocation maximum-per-host	1 ～ 8 の値を入力します。デフォルト値は 4 です。
xlate block-allocation interim logging	タイマー間隔を設定して、その時点で ASA 9.12(1) 以降のデバイスに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の syslog を生成します。43200 ～ 604800 の値を入力します。

[Translation Options] ページ

[Translation Options] ページを使用して、選択したセキュリティ アプライアンスのネットワークアドレス変換に影響するオプションを設定します。これらの設定は、デバイス上のすべてのインターフェイスに適用されます。

ナビゲーション パス

- （デバイスビュー）デバイスポリシーセレクタから **[NAT] > [変換オプション（Translation Options）]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから **[NAT (PIX/ASA/FWSM)] > [変換オプション（Translation Options）]** を選択します。共有ポリシーセレクタから既存のポリシーを選択するか、または [変換オプション（Translation Options）] を右クリックして新しいポリシーを作成します。

関連項目

- セキュリティ デバイスの NAT ポリシー （20 ページ）

フィールド リファレンス

表 *7 : [Translation Options]* ページ

要素	説明
アドレス変換なしでファイアウォール経由のトラフィックを有効にする（Enable traffic through the firewall without address translation）	選択すると、トラフィックはアドレス変換なしでセキュリティアプライアンスを通過できるようになります。このオプションを選択しなかった場合、変換ルールと一致しないトラフィックはすべてドロップされます。 （注） このオプションは、PIX 7.x、FWSM 3.x、および ASA デバイスのみで使用可能です。
Enable xlate bypass	選択すると、変換されないトラフィックに対する NAT セッションの確立がディセーブルになります（この機能は「xlate バイパス」と呼ばれます）。 （注） このオプションは、FWSM 3.2 以降のみで使用可能です。 デフォルトでは、FWSM は、NAT が使用されていなくても、すべての接続に対して NAT セッションを作成します。たとえば、NAT 制御がイネーブルになっていない場合、NAT 免除またはアイデンティティ NAT が使用されている場合、または同じセキュリティのインターフェイスを使用しており NAT を設定していない場合にも、セッションは変換対象でない接続ごとに作成されます。NAT セッションの数には最大限度があるため（266、同時には 144）、このような種類の NAT セッションで制限に達してしまう可能性があります。制限に達しないようにするには、xlate バイパスをイネーブルにします。 NAT 制御をディセーブルにして変換対象でないトラフィックを存在させるか NAT 免除を使用する場合、または NAT 制御をイネーブルにして NAT 免除を使用する場合には、xlate バイパスを使用すると、FWSM はこれらのタイプの変換対象でないトラフィックに対してセッションを作成しません。ただし、次の場合には、NAT セッションが作成されます。 • （NAT 制御の有無に関係なく）アイデンティティ NAT を設定する場合。アイデンティティ NAT は 1 つの変換と見なされます。 • NAT 制御で同じセキュリティのインターフェイスを使用する場合。同じセキュリティのインターフェイス間のトラフィックは、そのトラフィックに NAT を設定していなくても、NAT セッションを作成します。このような場合に NAT セッションを回避するには、NAT 制御をディセーブルにするか、または NAT 免除と xlate バイパスを使用します。
Do not translate VPN traffic	選択すると、VPN トラフィックはアドレス変換なしでセキュリティ アプライアンスを通過します。

要素	説明
Clear translates for existing connections	選択すると、ダイナミック変換に割り当てられた変換スロットおよび関連付けられた接続が、各セッションのあとにクリアされます。 セキュリティアプライアンスを介して接続し、なんらかの形式の NAT または PAT を受ける各セッションには、「xlate」と呼ばれる変換スロットが割り当てられます。これらの変換スロットは、セッションが完了した後も持続する可能性があり、変換スロットの枯渇、予期しないトラフィック動作、またはその両方につながる可能性があります。

PIX、FWSM、および 8.3 よりも前の ASA デバイスでの NAT の設定

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き PIX および FWSM の機能をサポートしていますが、拡張機能はサポートしていません。

ここでは、PIX デバイスと FWSM デバイス、および 8.3 よりも前のバージョンの ASA でネットワーク アドレス変換を設定する方法について説明します（ASA 8.3+ デバイスでの NAT の設定については、ASA 8.3+ デバイスでの NAT の設定 （46 ページ）を参照してください）。

アドレス プール

[Address Pools] ページを使用して、ダイナミック NAT ルールで使用されるグローバル アドレス プールを表示および管理します。

これらのアドレス プールを追加および編集するには、[Address Pool] ダイアログボックスを使用します。このページの [Global Address Pools] テーブルに表示されるフィールドについては、[Address Pool] ダイアログボックス （26 ページ）を参照してください。

ナビゲーション パス

- （デバイスビュー）デバイスポリシーセレクタから **[NAT] > [アドレスプール（Address Pools）]** を選択します。

- （ポリシービュー）ポリシータイプセレクタから **[NAT（PIX/ASA/FWSM）] > [アドレスプール（Address Pools）]** を選択します。共有ポリシーセレクタから既存のポリシーを選択するか、または [アドレスプール（Address Pools）] を右クリックして新しいポリシーを作成します。

関連項目

- PIX、FWSM、および 8.3 よりも前の ASA デバイスでの NAT の設定 （25 ページ）

[Address Pool] ダイアログボックス

[Address Pool] ダイアログボックスを使用して、ダイナミック NAT ルールで使用するグローバル アドレス プールを追加または編集します。

ナビゲーション パス

[Address Pool] ダイアログボックスを開くには、アドレス プール （25 ページ）で [Add Row] または [Edit Row] ボタンをクリックします。

関連項目

- PIX、FWSM、および 8.3 よりも前の ASA デバイスでの NAT の設定 （25 ページ）

フィールド リファレンス

表 8 : [Address Pools] ダイアログボックス

要素	説明
Interface Name	マッピングされた IP アドレスが使用されるデバイス インターフェイスの名前を入力するか、または選択します。
Pool ID	このアドレス プールの一意の識別番号を 1 ～ 2147483647 の整数で入力します。ダイナミック NAT ルールを設定する場合は、[Pool ID] を選択して、変換に使用されるアドレス プールを指定します。

要素	説明
IP アドレス範囲	このアドレス プールに割り当てられるアドレスを入力するか、または選択します。これらのアドレスは次のように指定できます。 • ダイナミック NAT のアドレス範囲（192.168.1.1-192.168.1.15 など） • サブネットワーク（192.168.1.0/24 など） • カンマ区切りのアドレスのリスト（192.168.1.1, 192.168.1.2, 192.168.1.3 など） • PAT に使用する単一のアドレス（192.168.1.1 など） • 上記の組み合わせ（192.168.1.1-192.168.1.15, 192.168.1.25 など） • 接続されるネットワーク上のホストの名前。これらは IP アドレスに解決されます。
説明	アドレス プールの説明を入力します。
Enable Interface PAT	オンにすると、指定したインターフェイスでポートアドレス変換がイネーブルになります。

[Translation Rules]：PIX、FWSM、および 8.3 よりも前の ASA

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き PIX および FWSM の機能をサポートしていますが、拡張機能はサポートしていません。

[Translation Rules] ページを使用して、選択したデバイスのネットワーク アドレス変換（NAT）規則を定義します。[Translation Rules] ページは、次のタブで構成されています。

- [Translation Exemptions (NAT 0 ACL)] （28 ページ）：このタブを使用して、アドレス変換が免除されるトラフィックを指定するルールを設定します。

（注） 変換免除は、ルータ モードの PIX、ASA、および FWSM とトランスペアレント モードの FWSM 3.2 デバイスだけでサポートされます。トランスペアレント モードのその他のデバイスでは、スタティック変換ルールだけがサポートされます。

- [Dynamic Rules] タブ （31 ページ）：このタブを使用して、ダイナミック NAT ルールとダイナミック PAT ルールを設定します。

（注） ダイナミック変換ルールは、ルータ モードの PIX、ASA、および FWSM とトランスペアレント モードの FWSM 3.2 デバイスだけでサポートされます。トランスペアレント モードのその他のデバイスでは、スタティック変換ルールだけがサポートされます。

- [Policy Dynamic Rules] タブ （34 ページ）：このタブを使用して、送信元アドレスと宛先アドレスおよびサービスに基づいたダイナミック変換ルールを設定します。

（注） ポリシーのダイナミック ルールは、ルータ モードの PIX、ASA、および FWSM とトランスペアレント モードの FWSM 3.2 デバイスだけでサポートされます。トランスペアレント モードのその他のデバイスでは、スタティック変換ルールだけがサポートされます。

- [Static Rules] タブ （36 ページ）：このタブを使用して、セキュリティ アプライアンスまたは共有ポリシーのスタティック変換ルールを設定します。
- [General] タブ （43 ページ）：このタブを使用して、デバイス上で検証される順序で、現在あるすべての変換ルールを一覧表示します。

（注） [General] タブは、ルータ モードの PIX、ASA、および FWSM とトランスペアレント モードの FWSM 3.2 デバイスだけで表示されます。トランスペアレント モードのその他のデバイスでは、スタティック変換ルールだけがサポートされ、概要情報を表示する必要はありません。

ナビゲーション パス

[Translation Rules] ページにアクセスするには、次のいずれかを実行します。

- （デバイス ビュー）デバイス ポリシー セレクタから [NAT] > [変換ルール（Translation Rules）] を選択します。
- （ポリシー ビュー）ポリシー タイプ セレクタから [NAT (PIX/ASA/FWSM)] > [変換ルール（Translation Rules）] を選択します。共有ポリシー セレクタから既存のポリシーを選択するか、または [変換ルール（Translation Rules）] を右クリックして新しいポリシーを作成します。

[Translation Exemptions (NAT 0 ACL)]

[Translation Rules] ページの [Translation Exemptions (NAT 0 ACL)] タブを使用して、トラフィックにアドレス変換を免除するルールを表示および指定します。ルールは、リスト内の順序に従って評価されます。行番号は、リスト内の順序におけるルールの位置を示します。[Up Row] ボタンおよび [Down Row] ボタンを使用して、選択したルールの位置を変更できます。

[Add/Edit Translation Exemption (NAT-0 ACL) Rule] ダイアログボックスを使用して、これらのルールを追加および編集します。このページのテーブルに表示されるフィールドについては、[Add/Edit Translation Exemption (NAT-0 ACL) Rule] ダイアログボックス （29 ページ）を参照してください。

（注） 変換免除は、ルータ モードの PIX、ASA、および FWSM とトランスペアレント モードの FWSM 3.2 デバイスだけでサポートされます。トランスペアレント モードのその他のデバイスでは、スタティック変換ルールだけがサポートされます。

ナビゲーション パス

[Translation Exemptions (NAT 0 ACL)] タブには、[Translation Rules]：PIX、FWSM、および 8.3 よりも前の ASA （27 ページ）ページからアクセスできます。

関連項目

- PIX、FWSM、および 8.3 よりも前の ASA デバイスでの NAT の設定 （25 ページ）
- [Advanced NAT Options] ダイアログボックス （40 ページ）
- [General] タブ （43 ページ）
- Security Manager の標準のルール テーブルに関する項：
  - ルール テーブルの使用
  - テーブルのフィルタリング
  - テーブル カラムおよびカラム見出しの機能

[Add/Edit Translation Exemption (NAT-0 ACL) Rule] ダイアログボックス

[Add/Edit Translation Exemption (NAT-0 ACL) Rule] ダイアログボックスを使用して、ルータ モードの PIX、FWSM、および 8.3 よりも前の ASA デバイスと、トランスペアレント モードの FWSM 3.2 デバイスでの変換免除ルールを定義および編集します。

ナビゲーション パス

[Add/Edit Translation Exemption (NAT-0 ACL) Rule] ダイアログボックスには、[Translation Exemptions (NAT 0 ACL)] タブからアクセスできます。詳細については、[Translation Exemptions (NAT 0 ACL)] （28 ページ）を参照してください。

関連項目

- PIX、FWSM、および 8.3 よりも前の ASA デバイスでの NAT の設定 （25 ページ）
- [Translation Rules]：PIX、FWSM、および 8.3 よりも前の ASA （27 ページ）
- [Advanced NAT Options] ダイアログボックス （40 ページ）

フィールド リファレンス

表 *9 : [Add/Edit Translation Exemption (NAT-0 ACL) Rule]* ダイアログボックス

要素	説明
ルールの有効化（Enable Rule）	オンにすると、ルールがイネーブルになります。ルールを削除せずにディセーブルにするには、このオプションの選択を解除します。
操作	このルールのアクションを選択します。 • [exempt]：NAT が免除されるトラフィックをルールで指定します。 • [do not exempt]：NAT が免除されないトラフィックをルールで指定します。
Original: Interface	ルールを適用するデバイスインターフェイスの名前を入力するか、または選択します。
Original: Sources	ルールを適用する発信元ホストおよびネットワーク オブジェクトの IP アドレスを入力するか、または選択します。複数のエントリを指定する場合は、カンマで区切ります。 このパラメータは、[変換免除（NAT 0 ACL）（Translation Exemptions (NAT 0 ACL)）] テーブルの列見出し [元のアドレス（Original Address）] の下に表示されることに注意してください。
Translated: Direction	このオプションによる指定に従って、ルールをインバウンド トラフィックまたはアウトバウンド トラフィックに適用できます。
Traffic flow: Destinations	ルールを適用する宛先ホストおよびネットワーク オブジェクトの IP アドレスを入力するか、または選択します。複数のエントリを指定する場合は、カンマで区切ります。
カテゴリ	ルールをカテゴリに割り当てるには、このリストからカテゴリを選択します。カテゴリは、ラベルやカラーコーディングを使用したルールとオブジェクトの識別に役立ちます。詳細については、カテゴリ オブジェクトの使用を参照してください。 （注） カテゴリ属性のコマンドは生成されません。
説明	ルールの説明を入力します。
[詳細設定（Advanced）] ボタン（FWSM のみ）	クリックすると、[Advanced NAT Options] ダイアログボックス （40 ページ）が開き、このルールの高度な設定を行うことができます。

[Dynamic Rules] タブ

[Translation Rules] ページの [Dynamic Rules] タブを使用して、ダイナミック NAT ルールとダイナミック PAT ルールを表示および設定します。ルールは、リスト内の順序に従って評価されます。行番号は、リスト内の順序におけるルールの位置を示します。[Up Row] ボタンおよび [Down Row] ボタンを使用して、選択したルールの位置を変更できます。

ダイナミック NAT では、内部 IP アドレスは、グローバル アドレス プールの IP アドレスを使用して動的に変換されます。ダイナミック PAT では、内部 IP アドレスは、動的に割り当てられるポート番号とマッピングされたアドレスを併用して、単一のマッピングされたアドレスに変換されます。ダイナミック変換は、多くの場合、ローカルの RFC 1918 IP アドレスをインターネットでルーティング可能なアドレスにマッピングするために使用されます。

[Add/Edit Dynamic Translation Rule] ダイアログボックスを使用して、これらのルールを追加および編集します。このページのテーブルに表示されるフィールドについては、[Add/Edit Dynamic Translation Rule] ダイアログボックス （32 ページ）を参照してください。

（注） ダイナミック変換ルールは、ルータ モードの PIX、ASA、および FWSM とトランスペアレント モードの FWSM 3.2 デバイスだけでサポートされます。トランスペアレント モードのその他のデバイスでは、スタティック変換ルールだけがサポートされます。

ナビゲーション パス

[Dynamic Rules] タブには、[Translation Rules] ページからアクセスできます。[Translation Rules] ページの詳細については、[Translation Rules]：PIX、FWSM、および 8.3 よりも前の ASA （27 ページ）を参照してください。

（注） デフォルトでは、[Dynamic Rule] の標準要素だけがこのテーブルに表示されます。カラムの見出しを右クリックすると、[Advanced NAT Options] ダイアログボックスで定義されている要素の他のカラムを表示できます（[General] タブ （43 ページ）には、デフォルトですべてのカラムが表示されます）。

関連項目

- PIX、FWSM、および 8.3 よりも前の ASA デバイスでの NAT の設定 （25 ページ）
- [Advanced NAT Options] ダイアログボックス （40 ページ）
- [Select Address Pool] ダイアログボックス （33 ページ）
- [General] タブ （43 ページ）
- 標準のルール テーブルに関する内容：
  - ルール テーブルの使用

- テーブルのフィルタリング
- テーブル カラムおよびカラム見出しの機能

[Add/Edit Dynamic Translation Rule] ダイアログボックス

[Add/Edit Dynamic Translation Rule] ダイアログボックスを使用して、ダイナミック NAT ルールとダイナミック PAT ルールを定義および編集します。

ナビゲーション パス

[Add/Edit Dynamic Translation Rule] ダイアログボックスには、[Dynamic Rules] タブからアクセスできます。詳細については、[Dynamic Rules] タブ （31 ページ）を参照してください。

関連項目

- PIX、FWSM、および 8.3 よりも前の ASA デバイスでの NAT の設定 （25 ページ）
- [Translation Rules]：PIX、FWSM、および 8.3 よりも前の ASA （27 ページ）
- [Advanced NAT Options] ダイアログボックス （40 ページ）
- [Select Address Pool] ダイアログボックス （33 ページ）

フィールド リファレンス

表 10 : [Add/Edit Dynamic Translation Rule] ダイアログボックス

要素	説明
ルールの有効化（Enable Rule）	オンにすると、ルールがイネーブルになります。ルールを削除せずにディセーブルにするには、このオプションの選択を解除します。
Original: Interface	ルールを適用するデバイスインターフェイスの名前を入力するか、または選択します。
Original: Address	ルールを適用する発信元ホストおよびネットワーク オブジェクトの IP アドレスを入力するか、または選択します。複数のエントリを指定する場合は、カンマで区切ります。
Translated: Pool	変換に使用するアドレスのプールの ID 番号を入力するか、または選択します。[Select] をクリックすると [Select Address Pool] ダイアログボックス （33 ページ）が開きます。 これをアイデンティティ NAT ルールとして指定するには、値 0 を入力します。
Translated: Direction	このオプションによる指定に従って、ルールをインバウンド トラフィックまたはアウトバウンド トラフィックに適用できます。

要素	説明
[Advanced] ボタン	クリックすると、[Advanced NAT Options] ダイアログボックス （40 ページ）が開き、このルールの高度な設定を行うことができます。

[Select Address Pool] ダイアログボックス

[Select Address Pool] ダイアログボックスには、グローバル アドレス プールのリストが表示されます。これらのプールは、アドレス プール （25 ページ）を使用して定義および管理されます。このダイアログボックスを使用して、ダイナミック変換ルールまたはポリシー ダイナミック変換ルールで使用するアドレス プールを選択します。

ナビゲーション パス

ダイナミック変換ルールを追加または編集する場合は [Add/Edit Dynamic Translation Rule] ダイアログボックス （32 ページ）から、ポリシー ダイナミック変換ルールを追加または編集する場合は [Add/Edit Policy Dynamic Rules] ダイアログボックス （35 ページ）から [Select Address Pool] ダイアログボックスにアクセスできます。

関連項目

- PIX、FWSM、および 8.3 よりも前の ASA デバイスでの NAT の設定 （25 ページ）
- [Translation Rules]：PIX、FWSM、および 8.3 よりも前の ASA （27 ページ）
- アドレス プール （25 ページ）

フィールド リファレンス

表 *11 : [Select Address Pool]* ダイアログボックス

要素	説明
Pool ID	アドレス プールの識別番号。
インターフェイス	アドレス プールが適用されるデバイス インターフェイスの名前。
IP アドレス範囲（IP Address Ranges）	プールに割り当てられる IP アドレス。このリストの「インターフェイス」は、指定したインターフェイスで PAT が有効になっていることを示します。
説明	アドレス プールの説明。
Selected Row	このフィールドは、リスト内で現在選択されているプールを示します。[OK] をクリックするとダイアログボックスが閉じ、このプールが変換ルールに割り当てられます。

[Policy Dynamic Rules] タブ

[Translation Rules] ページの [Policy Dynamic Rules] タブを使用して、送信元アドレスと宛先アドレスおよびサービスに基づいたダイナミック変換ルールを表示および設定します。ルールは、リスト内の順序に従って評価されます。行番号は、リスト内の順序におけるルールの位置を示します。[Up Row] ボタンおよび [Down Row] ボタンを使用して、選択したルールの位置を変更できます。

[Add Policy Dynamic Rule]/[Edit Policy Dynamic Rule] ダイアログボックスを使用して、これらのルールを追加および編集します。このページのテーブルに表示されるフィールドについては、[Add/Edit Policy Dynamic Rules] ダイアログボックス （35 ページ）を参照してください。

（注） ポリシーのダイナミック ルールは、ルータ モードの PIX、ASA、および FWSM とトランスペアレント モードの FWSM 3.2 デバイスだけでサポートされます。トランスペアレント モードのその他のデバイスでは、スタティック変換ルールだけがサポートされます。

ナビゲーション パス

[Policy Dynamic Rules] タブには、[Translation Rules] ページからアクセスできます。詳細については、[Translation Rules]：PIX、FWSM、および 8.3 よりも前の ASA （27 ページ）を参照してください。

（注） デフォルトでは、[Policy Dynamic Rule] の標準要素だけがこのテーブルに表示されます。カラムの見出しを右クリックすると、[Advanced NAT Options] ダイアログボックスで定義されている要素の他のカラムを表示できます（[General] タブ （43 ページ）には、デフォルトですべてのカラムが表示されます）。

関連項目

- PIX、FWSM、および 8.3 よりも前の ASA デバイスでの NAT の設定 （25 ページ）
- < [Add/Edit Policy Dynamic Rules] ダイアログボックス （35 ページ）
- [Advanced NAT Options] ダイアログボックス （40 ページ）
- [Select Address Pool] ダイアログボックス （33 ページ）
- [General] タブ （43 ページ）
- 標準のルール テーブルに関する内容：
  - ルール テーブルの使用
  - テーブルのフィルタリング
  - テーブル カラムおよびカラム見出しの機能

[Add/Edit Policy Dynamic Rules] ダイアログボックス

[Add/Edit Policy Dynamic Rules] ダイアログボックスを使用して、送信元アドレスと宛先アドレスおよびサービスに基づいたダイナミック変換ルールを定義および編集します。

ナビゲーション パス

[Add/Edit Policy Dynamic Rules] ダイアログボックスには、[Policy Dynamic Rules] タブからアクセスできます。詳細については、[Policy Dynamic Rules] タブ （34 ページ）を参照してください。

関連項目

- [Translation Rules]：PIX、FWSM、および 8.3 よりも前の ASA （27 ページ）
- PIX、FWSM、および 8.3 よりも前の ASA デバイスでの NAT の設定 （25 ページ）
- [Policy Dynamic Rules] タブ （34 ページ）
- [Advanced NAT Options] ダイアログボックス （40 ページ）
- [Select Address Pool] ダイアログボックス （33 ページ）

フィールド リファレンス

表 12 : [Add/Edit Policy Dynamic Rules] ダイアログボックス

要素	説明
ルールの有効化（Enable Rule）	オンにすると、ルールがイネーブルになります。ルールを削除せずにディセーブルにするには、このオプションの選択を解除します。
Original: Interface	ルールを適用するデバイスインターフェイスの名前を入力するか、または選択します。
Original: Sources	ルールを適用する発信元ホストおよびネットワーク オブジェクトの IP アドレスを入力するか、または選択します。複数のエントリを指定する場合は、カンマで区切ります。 このパラメータは、[ポリシーダイナミックルール（Policy Dynamic Rules）] テーブルのカラム見出し [元のアドレス（Original Address）] の下に表示されることに注意してください。
Translated: Pool	変換に使用するアドレスのプールの ID 番号を入力するか、または選択します。[Select] をクリックすると [Select Address Pool] ダイアログボックス （33 ページ）が開きます。 これをアイデンティティ NAT ルールとして指定するには、値 0 を入力します。

要素	説明
Translated: Direction	このオプションによる指定に従って、ルールをインバウンドトラフィックまたはアウトバウンド トラフィックに適用できます。
Traffic flow: Destinations	ルールを適用する宛先ホストおよびネットワーク オブジェクトの IP アドレスを入力するか、または選択します。複数のエントリを指定する場合は、カンマで区切ります。
Traffic flow: Services	ルールを適用するサービスを入力するか、または選択します。複数のエントリを指定する場合は、カンマで区切ります。
カテゴリ	ルールをカテゴリに割り当てるには、このリストからカテゴリを選択します。カテゴリは、ラベルやカラーコーディングを使用したルールとオブジェクトの識別に役立ちます。詳細については、カテゴリ オブジェクトの使用を参照してください。 （注） カテゴリ属性のコマンドは生成されません。
説明	ルールの説明を入力します。
[Advanced] ボタン	クリックすると、[Advanced NAT Options] ダイアログボックス （40 ページ）が開き、このルールの高度な設定を行うことができます。

[Static Rules] タブ

[Translation Rules] ページの [Static Rules] タブを使用して、セキュリティ アプライアンスまたは共有ポリシーのスタティック変換ルールを表示および設定します。ルールは、リスト内の順序に従って評価されます。行番号は、リスト内の順序におけるルールの位置を示します。[Up Row] ボタンおよび [Down Row] ボタンを使用して、選択したルールの位置を変更できます。

スタティック変換では、内部 IP アドレスは常にグローバル IP アドレスにマッピングされます。これらのルールは、セキュリティレベルの低いインターフェイス上のホストアドレスをセキュリティレベルの高いインターフェイス上のグローバルアドレスにマッピングします。たとえば、スタティックルールは、境界ネットワーク上の Web サーバーのローカルアドレスを、外部インターフェイス上のホストが Web サーバーへのアクセスに使用するグローバルアドレスにマッピングするために使用されます。

注意 セキュリティデバイス上のスタティック NAT ルールの順序は重要であり、Security Manager は展開時にこの順序を保持します。ただし、セキュリティ アプライアンスでは、スタティック NAT ルールのインライン編集はサポートしていません。つまり、リストの末尾よりも上の任意の場所でルールを移動、編集、または挿入すると、Security Manager は、新規または変更したルールの後に続くすべてのスタティック NAT ルールをデバイスから削除し、その時点から更新されたリストを再送信します。リストの長さによっては、この処理にかなりのオーバーヘッドがかかる可能性があり、結果としてトラフィックが中断されることがあります。可能なかぎり、新しいスタティック NAT ルールはリストの末尾に追加してください。

[Add/Edit Static Rule] ダイアログボックスを使用して、これらのルールを追加および編集します。このページのテーブルに表示されるフィールドについては、[Add/Edit Static Rule] ダイアログボックス （38 ページ）を参照してください。

[スタティックルール（Static Rules）] テーブルの「Nailed」カラム

[Add/Edit Static Rule] ダイアログボックス （38 ページ）で指定されたパラメータを表す列に加えて、[スタティックルール（Static Rules）] テーブルには、「Nailed」というラベルの付いた列が表示されます。この値はデバイス検出の製品です。Security Manager では変更できません。

「Nailed」カラムのエントリは、その接続に対して TCP ステートトラッキングおよびシーケンスチェックがスキップされるかどうかを「true」または「false」で示します。

ナビゲーション パス

[Static Rules] タブには、[Translation Rules] ページからアクセスできます。詳細については、[Translation Rules]：PIX、FWSM、および 8.3 よりも前の ASA （27 ページ）を参照してください。

（注） デフォルトでは、[Static Rules] の標準要素だけがこのテーブルに表示されます。カラムの見出しを右クリックすると、[Advanced NAT Options] ダイアログボックスで定義されている要素の他のカラムを表示できます（[General] タブ （43 ページ）には、デフォルトですべてのカラムが表示されます）。

関連項目

- PIX、FWSM、および 8.3 よりも前の ASA デバイスでの NAT の設定 （25 ページ）
- [Add/Edit Static Rule] ダイアログボックス （38 ページ）
- [Advanced NAT Options] ダイアログボックス （40 ページ）
- [General] タブ （43 ページ）
- 標準のルール テーブルに関する内容：

- ルール テーブルの使用
- テーブルのフィルタリング
- テーブル カラムおよびカラム見出しの機能

[Add/Edit Static Rule] ダイアログボックス

[Add/Edit Static Rule] ダイアログボックスを使用して、ファイアウォール デバイスまたは共有ポリシーのスタティック変換ルールを追加または編集します。

ナビゲーション パス

[Add/Edit Static Rule] ダイアログボックスには、[Static Rules] タブ （36 ページ）からアクセスできます。

関連項目

- PIX、FWSM、および 8.3 よりも前の ASA デバイスでの NAT の設定 （25 ページ）
- [Translation Rules]：PIX、FWSM、および 8.3 よりも前の ASA （27 ページ）
- [Advanced NAT Options] ダイアログボックス （40 ページ）

フィールド リファレンス

表 *13 : [Add/Edit Static Rule]* ダイアログボックス

要素	説明
ルールの有効化（Enable Rule）	オンにすると、ルールがイネーブルになります。ルールを削除せずにディセーブルにするには、このオプションの選択を解除します。
Translation Type	このルールの変換のタイプ（[NAT] または [PAT]）を選択します。
Original Interface	変換される元のアドレスを持つホストまたはネットワークに接続されているデバイス インターフェイスを入力するか、または選択します。
元のアドレス	変換される送信元アドレスを入力するか、または選択します。
Translated Interface	変換後のアドレスが使用されるインターフェイスを入力するか、または選択します。 このルールをアイデンティティ NAT ルールとして指定するには、このフィールドと [Original Interface] フィールドの両方に同じインターフェイスを入力します。

要素	説明
Use Interface IP/Use Selected Address	変換後のインターフェイスで使用するアドレスを指定します。[Use Interface IP]（アドレス）を選択するか、または [Use Selected Address] を選択してアドレスを入力するかネットワーク/ホスト オブジェクトを選択します。
Enable Policy NAT	この変換ルールに対してポリシー NAT をイネーブルにするには、このオプションを選択します。
宛先アドレス（Dest Address）	ポリシー NAT をイネーブルにした場合は、ルールが適用されるホストまたはネットワークの宛先アドレスを指定します。
サービス	ポリシー NAT をイネーブルにした場合は、ルールが適用されるサービスを入力するか、または選択します。 （注） スタティック ポリシー NAT の場合、指定できるサービスは IP だけです。 サービスおよびサービス オブジェクトを指定する構文は、次のとおりです。 {**tcp** | **udp** | **tcp&udp**}/{*source_port_number* | *port_list_object* }/{*destination_port_number* | *port_list_object* } 1 つのポートパラメータしか入力しなかった場合、このパラメータは宛先ポートとして解釈されることに注意してください（送信元ポートは「any」になります）。たとえば、**tcp/4443** は tcp、送信元ポート any、宛先ポート 4443 を意味し、**tcp/4443/Default Range** は tcp、送信元ポート 4443、宛先ポート Default Range（通常、1 ～ 65535）を意味します。 すべてのテキスト入力フィールドと同様に、Security Manager によってオートコンプリート オプションが表示されることがあります。たとえば、このフィールドに **tcp/** と入力すると、Security Manager に定義されているすべてのポートリストオブジェクトのオートコンプリートリストが表示されます。このリストには、DEFAULT RANGE、HTTPS、および WEBPORTS などのシステム生成オブジェクトが含まれています。 ポート リストの詳細についてはポート リスト オブジェクトの設定を、サービス定義の詳細についてはサービス オブジェクトの設定を参照してください。
プロトコル	[Translation Type] で [PAT] を選択した場合は、ルールが適用されるプロトコル（TCP または UDP）を選択します。
元のポート	[Translation Type] で [PAT] を選択した場合は、変換されるポート番号を入力します。 このパラメータは、[スタティックルール（Static Rules）] テーブルのカラム見出し [ローカルポート（Local Port）] の下に表示されることに注意してください。

要素	説明
[変換されたポート（Translated Port）]	[Translation Type] で [PAT] を選択した場合は、元のポート番号が変換されるポート番号を入力します。 このパラメータは、[スタティックルール（Static Rules）] テーブルのカラム見出し [グローバルポート（Global Port）] の下に表示されることに注意してください。
カテゴリ	ルールをカテゴリに割り当てるには、このリストからカテゴリを選択します。カテゴリは、ラベルやカラーコーディングを使用したルールとオブジェクトの識別に役立ちます。詳細については、カテゴリ オブジェクトの使用を参照してください。 （注）　カテゴリ属性のコマンドは生成されません。
説明	ルールの説明を入力します。
[Advanced] ボタン	クリックすると、[Advanced NAT Options] ダイアログボックス （40 ページ）が開き、このルールの高度な設定を行うことができます。

[Edit Translated Address] ダイアログボックス

スタティック変換ルールに割り当てられている変換後のアドレスだけを変更するには、[Edit Translated Address] ダイアログボックスを使用します。変換後のアドレスとは、元のアドレスが変更されるアドレスです。インターフェイスの IP アドレスを使用するか、特定の IP アドレスを入力できます。スタティック ルールおよび変換後のアドレスの詳細については、[Static Rules] タブ （36 ページ）を参照してください。

ファイアウォール ルールのセルの編集に関する詳細については、ルールの編集を参照してください。

ナビゲーション パス

（[NAT]>[変換ルール（Translation Rules）]ページにある）[スタティックルール（Static Rules）] テーブルの [変換済みアドレス（Translated Address）]セルを右クリックして、[変換済みアドレスの編集（Edit Translated Address）] を選択します。

[Advanced NAT Options] ダイアログボックス

[Advanced NAT Options] ダイアログボックスを使用して、NAT およびポリシー NAT の高度な接続設定（DNS 書き換え、最大 TCP および最大 UDP 接続数、初期接続制限、タイムアウト（PIX 6.x）、およびシーケンス番号のランダム化）を指定します。これらのオプションは、FWSM の変換免除（NAT 0 ACL）ルールでも設定できます。

ナビゲーション パス

変換ルールの追加または編集時に [詳細設定（Advanced）] ボタンをクリックすると、[NAT詳細オプション（Advanced NAT Options）] ダイアログボックスにアクセスできます。詳細については、次のトピックを参照してください。

- [Add/Edit Translation Exemption (NAT-0 ACL) Rule] ダイアログボックス （29 ページ）
- [Add/Edit Dynamic Translation Rule] ダイアログボックス （32 ページ）
- [Add/Edit Policy Dynamic Rules] ダイアログボックス （35 ページ）
- [Add/Edit Static Rule] ダイアログボックス （38 ページ）

関連項目

- PIX、FWSM、および 8.3 よりも前の ASA デバイスでの NAT の設定 （25 ページ）
- [Translation Rules]：PIX、FWSM、および 8.3 よりも前の ASA （27 ページ）

フィールド リファレンス

表 *14 : [Advanced NAT Options]* ダイアログボックス

要素	説明
Translate the DNS replies that match the translation rule	オンにすると、外部クライアントが内部 DNS サーバを使用して内部ホストの名前を解決できるように、またその逆ができるように、セキュリティ アプライアンスは DNS 応答を書き換えます。たとえば、NAT ルールに、DNS サーバ内にエントリを持つホストの実際のアドレスが含まれていて、DNS サーバがクライアントとは別のインターフェイス上にある場合、クライアントおよび DNS サーバにはそれぞれ異なるホスト用アドレスが必要です。つまり、片方にはマッピングされたアドレス、もう片方には実際のアドレスが必要です。このオプションは、クライアントに送信される DNS 応答内のアドレスを書き換えます。 例として、内部 Web サーバ www.example.com に IP アドレス 192.168.1.1 があり、このアドレスがアプライアンスの外部インターフェイス上の 10.1.1.1 に変換されるとします。外部クライアントは内部 DNS サーバに DNS 要求を送信し、これにより www.example.com は 192.168.1.1 に解決されます。DNS 書き換えをイネーブルにしたセキュリティ アプライアンスに応答が到着すると、外部クライアントが正しい IP アドレスを取得できるように、セキュリティ アプライアンスはペイロード内の IP アドレスを 10.1.1.1 に変換します。 マッピングされたホストがクライアントまたは DNS サーバと同じインターフェイス上に存在している必要があることに注意してください。通常、他のインターフェイスからのアクセスを許可する必要があるホストはスタティック変換を使用するため、このオプションはスタティック ルールで使用される可能性があります。

要素	説明
ルールあたりの最大TCP接続数（Max TCP Connections per Rule）	許容される TCP 接続の最大数を入力します。有効な値は 0 ～ 65,535 です。この値を 0 に設定すると、接続数は無制限になります。
Max UDP Connections per Rule	許容される UDP 接続の最大数を入力します。有効な値は 0 ～ 65,535 です。この値を 0 に設定すると、接続数は無制限になります。
Max Embryonic Connections	初期接続制限を超えると、クライアントからセキュリティ レベルのより高いサーバに送信される TCP SYN パケットが、TCP 代行受信機能によって代行受信されます。初期接続とは、送信元と宛先の間で必要になるハンドシェイクを完了していない接続要求のことです。この制限は、初期接続のフラッドによる攻撃を防ぐために設定します。有効な値は 0 ～ 65,535 です。この値を 0 に設定すると、接続数は無制限になります。 任意の正の値を入力すると、TCP 代行受信機能がイネーブルになります。TCP 代行受信は、TCP SYN パケットを使用してインターフェイスをフラッディングすることによる DoS 攻撃から内部システムを保護します。初期接続制限を超えると、クライアントからセキュリティ レベルのより高いサーバに送信される TCP SYN パケットが、TCP 代行受信機能によって代行受信されます。検証プロセス中に SYN クッキーが使用され、ドロップされる有効なトラフィックの数が最小限に抑えられます。したがって、到達不能なホストからの接続試行がサーバに到達することはありません。
タイムアウト（Timeout）	PIX 6.x デバイスの場合は、この変換ルールのタイムアウト値を hh:mm:ss の書式で入力します。この値は、00:00:00 を指定しないかぎり、[Platform] > [Security] > [Timeouts] で指定したデフォルトの変換タイムアウトを上書きします。00:00:00 を指定した場合、このルールに一致する変換では、（[Platform] > [Security] > [Timeouts] で指定した）デフォルトの変換タイムアウトが使用されます。

要素	説明
Randomize Sequence Number	オンにすると、セキュリティ アプライアンスによって TCP パケットのシーケンス番号がランダム化されます。個々の TCP 接続には 2 つの Initial Sequence Number（ISN; 初期シーケンス番号）があり、そのうちの 1 つはクライアントで生成され、もう 1 つはサーバで生成されます。セキュリティ アプライアンスは、インバウンド方向とアウトバウンド方向の両方で、TCP SYN の ISN をランダム化します。保護対象のホストの ISN をランダム化することにより、攻撃者が新しい接続に使用される次の ISN を予測して新しいセッションをハイジャックするのを阻止します。 この機能は、次の場合にかぎりディセーブルにします。 • 別のインライン セキュリティ アプライアンスでも初期シーケンス番号をランダム化しており、データがスクランブル化されている場合。 • セキュリティアプライアンスを介して eBGP マルチホップを使用しており、eBGP ピアが MD5 を使用している場合。ランダム化により、MD5 チェックサムは分解されます。 • セキュリティ アプライアンスによって接続のシーケンス番号がランダム化されないことを必要とする WAAS デバイスを使用している場合。 このオプションをディセーブルにすると、セキュリティ アプライアンスにセキュリティ ホールが開きます。

[General] タブ

[Translation Rules] ページの [General] タブを使用して、現在のデバイスまたは共有ポリシーに定義されているすべての変換ルールの概要を表示します。変換ルールは、デバイス上で検証される順序で一覧表示されます。

（注） [General] タブは、ルータ モードの PIX、ASA、および FWSM デバイスとトランスペアレント モードの FWSM 3.2 デバイスだけで表示されます。トランスペアレント モードのその他のデバイスでは、スタティック変換ルールだけがサポートされ、概要情報を表示する必要はありません。

ナビゲーション パス

[General] タブには、[Translation Rules] ページからアクセスできます。詳細については、を参照してください。

関連項目

- PIX、FWSM、および 8.3 よりも前の ASA デバイスでの NAT の設定 （25 ページ）
- [Translation Exemptions (NAT 0 ACL)] （28 ページ）

- [Dynamic Rules] タブ （31 ページ）
- [Policy Dynamic Rules] タブ （34 ページ）
- [Static Rules] タブ （36 ページ）
- 標準のルール テーブルに関する内容：
  - ルール テーブルの使用
  - テーブルのフィルタリング
  - テーブル カラムおよびカラム見出しの機能

フィールド リファレンス

表 *15 : [*全般（*General***）*]* タブ：変換ルール概要テーブル**

要素	説明
（注） テーブル内のエントリに斜線の網掛けが適用されている場合は、ルールが現在ディセーブルになっていることを示します（これらのルールのイネーブル化およびディセーブル化の詳細については、[Add/Edit Dynamic Translation Rule] ダイアログボックス （32 ページ）の [Enable Rule] を参照してください）。	
番号	ルールは、リスト内の順序に従って評価されます。この番号は、リストの順序におけるルールの位置を示します。
タイプ（Type）	トランスレーション ルールのタイプ。[Static]、[Dynamic]、[Exemption] など。
操作	ルールが NAT から免除される場合は、「exempt」と表示されます。
Original Interface	ルールが適用されるデバイス インターフェイスの ID。
元のアドレス	ルールが適用される送信元ホストおよびネットワークのオブジェクト名または IP アドレス。
ローカル ポート（Local Port）	ホストまたはネットワークによって提供されるポート番号（スタティック PAT 用）。
Translated Pool	変換に使用されるアドレス プールの ID 番号。
Translated Interface	変換後のアドレスが使用されるインターフェイス。
Translated Address	変換後のアドレス。
Global Port	元のポート番号が変換されるポート番号（スタティック PAT 用）。

要素	説明
[接続先（Destination）]	ルールが適用される宛先ホストまたはネットワークのオブジェクト名および IP アドレス。
プロトコル	ルールが適用されるプロトコル。
サービス	ルールが適用されるサービス。
方向	ルールが適用されるトラフィックの方向（[Inbound] または [Outbound]）。
DNS Rewrite	DNS 書き換えオプションがイネーブルかどうか（このオプションは [Advanced NAT Options] ダイアログボックス （40 ページ）で設定される）。
Maximum TCP Connections	静的に変換された IP アドレスに接続できる TCP 接続の最大数。0 の場合、接続数は無制限です。このオプションは、[Advanced NAT Options] ダイアログボックス （40 ページ）で設定します。
Embryonic Limit	セキュリティアプライアンスが初期接続を拒否し始めるまでに確立が許可される初期接続の数。0 の場合、接続数は無制限です。正の数を入力すると、TCP 代行受信機能がイネーブルになります。 このオプションは、[Advanced NAT Options] ダイアログボックス （40 ページ）で設定します。
Maximum UDP Connections	静的に変換された IP アドレスに接続できる UDP 接続の最大数。0 の場合、接続数は無制限です。このオプションは、[Advanced NAT Options] ダイアログボックス （40 ページ）で設定します。
タイムアウト（Timeout）	PIX 6.x デバイスの場合、これはスタティック変換ルールのタイムアウト値です。この値は、[Platform] > [Security] > [Timeouts] で指定したデフォルトの変換タイムアウトを上書きします。ここで 00:00:00 のタイムアウト値を指定すると、このルールと一致する変換では、[Platform] > [Security] > [Timeouts] で指定したデフォルトの変換タイムアウトが使用されます。
Randomize Sequence Number	セキュリティアプライアンスが TCP パケットのシーケンス番号をランダム化するかどうか：「Yes」または「No」。このオプションは [Advanced NAT Options] ダイアログボックス （40 ページ）で設定され、デフォルトはイネーブル）。

要素	説明
カテゴリ	ルールが割り当てられるカテゴリ。カテゴリはラベルやカラーコーディングを使用して、ルールおよびオブジェクトを識別しやすくします。詳細については、カテゴリ オブジェクトの使用を参照してください。 （注）　カテゴリ属性のコマンドは生成されません。
説明	ルールの説明（指定してある場合）。
最後のチケット	ルールの最終変更に関連付けられたチケットを表示します。[最後のチケット（Last Ticket(s)）] 列のチケット ID をクリックして、チケットの詳細を表示し、そのチケットに移動できます。外部チケット管理システムへのリンクが設定されている場合は、チケットの詳細からそのシステムに移動することもできます（[チケット管理（Ticket Management）] ページを参照）。

ASA 8.3+ デバイスでの NAT の設定

ここでは、バージョン 8.3 以降の ASA デバイスでネットワーク アドレス変換を設定する方法について説明します。

- [Translation Rules]：ASA 8.3+ （46 ページ）
  - [Add NAT Rule]/[Edit NAT Rule] ダイアログボックス （49 ページ）
  - [Add Network/Host]/[Edit Network/Host] ダイアログボックス - [NAT] タブ （60 ページ）
- Per-Session NAT ルール: ASA 9.0（1）+ （65 ページ）

他のセキュリティ アプライアンスでの NAT の設定については、 PIX、FWSM、および 8.3 よりも前の ASA デバイスでの NAT の設定 （25 ページ）を参照してください。NAT ルールの一般的な情報、および ASA 8.3 で実装された NAT 設定の変更点については、 ASA 8.3 以降のデバイスでの「簡易」NAT について （5 ページ）を参照してください。

（注）　ロールにマップされた変更権限を持っている場合にのみ、NAT オブジェクトを作成できます。Cisco Security Manager は認証のエラーメッセージを表示します。

[Translation Rules]：ASA 8.3+

[Translation Rules] ページを使用して、選択した ASA 8.3+ デバイスのネットワーク アドレス変換（NAT）規則を管理します。他のセキュリティデバイスでの変換ルールの設定については、セキュリティ デバイスの NAT ポリシー （20 ページ）を参照してください。

このテーブルには 2 つのタイプの NAT ルールが表示されます。該当ユーザや別のユーザが追加した「手動」ルールと、NAT プロパティを持つオブジェクトがデバイスに割り当てられている場合に Security Manager によって生成および適用される「自動」ルールです。これらはそれぞれ「NAT ルール」および「ネットワークオブジェクト NAT ルール」と呼ばれます。

[Translation Rules] テーブルの一部の機能

この [Translation Rules] テーブルは、ルール テーブルの使用で示すような標準的な Security Managerのルールテーブルです。たとえば、カラムを移動、表示、または非表示にしたり、手動ルールを再順序付けしたり、特定のテーブルセルを右クリックしてそのパラメータを編集したりできます。また、次の機能はこの [Translation Rules] テーブルに固有です。

- すべてのルールが、テーブル内にある事前定義済みの 3 つのセクションのいずれかに割り当てられます。
  - [NAT Rules Before]：これらは、該当ユーザまたは別のユーザがそのデバイスに「手動で」定義したルールです。ルールを追加する前にセクション見出しをクリックすることで、このセクションにルールが追加されることを指定できますが、セクションを指定しなかった場合にも、新しいルールはデフォルトでこのセクションに追加されます。
  - [Network Object NAT Rules]：これらは、NAT プロパティを含むネットワークオブジェクトがデバイスに割り当てられている場合に、Security Manager によって自動的に生成され、順序付けされるルールです。NAT プロパティをオブジェクトに割り当てる方法については、[Add Network/Host]/[Edit Network/Host] ダイアログボックス - [NAT] タブ （60 ページ）を参照してください。これらのルールを順序付けする方法については、ASA 8.3 以降のデバイスでの「簡易」NAT について （5 ページ）のセクション「NAT テーブル」を参照してください。

（注） これらのルールはデバイス固有であるため、このセクションはポリシー ビューの [Translation Rules] テーブルには表示されません。

  - [NAT Rules After]：これらもまた、該当ユーザまたは別のユーザがそのデバイスに手動で定義したルールです。ルールを追加する前にセクション見出しをクリックすることで、このセクションにルールが追加されることを指定できます。

このテーブルに一覧表示されているNATルールは最初に一致したものから順に処理されます。そのため、順序は重要です。ルールはそのセクション内でしか再順序付けできないため、自動ルールの前と後の両方で手動セクションを指定することによって、すべてのルールが適切な順序になるように設定できます。各セクションのルールは、そのあとのセクションのルールに優先します。たとえば、一番上の「前」セクションのルールは、ネットワークオブジェクトNATセクションのルールに優先するというように続きます。

- 各ルールのタイプ（スタティック、ダイナミック PAT、またはダイナミック NAT と PAT）は、[変換済み（Translated）] カラムの [送信元（Source）] パラメータの次に青色で **(S)**、**(DP)**、または**(DNP)** を表示することによって、テーブル内で視覚的に示されます。
- 双方向ルールは、実際にはペアになった 2 つのルール（指定した送信元の値と宛先の値の間で実行される発信変換と着信変換のそれぞれに 1 つずつ）で構成されるスタティック ルールです。ルール テーブルには、各双方向ルール エントリが 2 行で表示されます。

たとえば、[Source] フィールドが [Host1] で [Translated] フィールドが [Host2] のスタティック ルールを作成するときに [Bi-directional] を選択した場合、ルール テーブルに 2 つの行が追加されます。1 つは Host1 を Host2 に変換する行、もう 1 つは Host2 を Host1 に変換する行です。

関連項目

- セキュリティ デバイスの NAT ポリシー （20 ページ）
- ASA 8.3 以降のデバイスでの「簡易」NAT について （5 ページ）
- 標準のルール テーブルに関する内容：
  - ルール テーブルの使用
  - テーブルのフィルタリング
  - テーブル カラムおよびカラム見出しの機能

ナビゲーション パス

- （デバイスビュー）デバイスポリシーセレクタから [NAT] > [変換ルール（Translation Rules）] を選択します。
- （ポリシービュー）ポリシータイプセレクタから [NAT (PIX/ASA/FWSM)] > [変換ルール（Translation Rules）] を選択します。共有ポリシーセレクタから既存のポリシーを選択するか、または [変換ルール（Translation Rules）] を右クリックして新しいポリシーを作成します。

[Translation Rules] ページが表示されます。ネットワーク オブジェクト NAT ルールはデバイス固有であるため、ポリシー ビューでは [Network Object NAT Rules] セクションが表示されないことに注意してください。

ルールの追加、編集、および削除

NAT ルールを**追加**するには、次の手順を実行します。

1. ルールを追加するセクションの見出しを選択します。見出しを選択しなかった場合、ルールはデフォルトで [NAT Rules Before] に追加されます。
2. [Add NAT Rule] ダイアログボックスを開きます。テーブルの下部にある [Add Row] ボタンをクリックするか、またはテーブル内の任意の場所（既存のルールエントリの上以外）を右クリックしてポップアップ メニューから [Add Row] を選択します。

3. ルールを定義してから [OK] をクリックしてダイアログボックスを閉じると、ルールがテーブルに追加されます。

NAT ルールを**編集**するには、次の手順を実行します。

1. 目的のルールの [Edit NAT Rule] ダイアログボックスを開きます。NAT ルール テーブルでルールを選択してテーブルの下部にある [Edit Row] ボタンをクリックするか、または単に目的のルール エントリを右クリックしてポップアップ メニューから [Edit Row] を選択します。
2. ルールを編集してから [OK] をクリックしてダイアログボックスを閉じます。

[Add NAT Rule] ダイアログボックスの詳細な説明については、[Add NAT Rule]/[Edit NAT Rule] ダイアログボックス （49 ページ）を参照してください。

NAT ルールを**削除**するには、テーブルでルールを選択してテーブルの下部にある [行の削除（Delete Row）] ボタンをクリックするか、または単に目的のルールエントリを右クリックしてポップアップメニューから [行の削除（Delete Row）] を選択します。

（注） このテーブルからネットワーク オブジェクト NAT ルールを削除するには、関連する [Edit Network Host] ダイアログボックスで [Add Automatic Address Translation NAT Rule] オプションをオフにするか、またはルールの割り当て先のデバイスを変更します。詳細については、[Add Network/Host]/[Edit Network/Host] ダイアログボックス - [NAT] タブ （60 ページ）を参照してください。

ルールの有効化と無効化

次のように、1 つ以上の連続するルールをテーブルから削除せずにディセーブルにできます。

1. ディセーブルにするルールを選択します。連続したルールのブロックを選択する場合は、ブロックの最初のルールをクリックしてから、ブロックの最後のルールを Shift を押した状態でクリックします。
2. 選択したルールを右クリックして、ポップアップメニューから [無効化（Disable）] を選択します。

無効になっているルールは、テーブルでグレー表示されます。

無効になっている 1 つ以上の連続するルールを再度有効にするには、このプロセスを繰り返して、ポップアップメニューから [有効化（Enable）] を選択します。

[Add NAT Rule]/[Edit NAT Rule] ダイアログボックス

[Add NAT Rule] ダイアログボックスを使用して、選択した ASA 8.3+ デバイスに NAT ルールを追加します。このダイアログボックスは、以前のバージョンの ASA でも、PIX または FWSM デバイスでも使用できません。これらのデバイスで NAT ルールを追加および編集する方法については、PIX、FWSM、および 8.3 よりも前の ASA デバイスでの NAT の設定 （25 ページ）を参照してください。

（注） タイトルを除いて、[Add NAT Rule] ダイアログボックスと [Edit NAT Rule] ダイアログボックスは同一であり、次の説明は両方に適用されます。

ナビゲーション パス

ルールを追加するには、ルールを追加するセクション（[NATルールを前に（NAT Rules Before）] または [NATルールを後に（NAT Rules After）]）を選択してから、ルールテーブルの下にある [行の追加（Add Row）] ボタンをクリックするか、またはテーブル内の任意の場所を右クリックし、[行の追加（Add Row）] を選択して [NATルールの追加（Add NAT Rule）] ダイアログボックスを開きます。セクションを選択しなかった場合、新しいルールは [NAT Rules Before] セクションに追加されることに注意してください。

ルールを編集するには、ルールを選択して [Edit Row] ボタンをクリックするか、単にルールを右クリックし [Edit Row] コマンドを選択して、そのルールの [Edit NAT Rule] ダイアログボックスを開きます。

関連項目

- ネットワーク アドレス変換の設定 （1 ページ）
- [Translation Rules]：ASA 8.3+ （46 ページ）
- [Add Network/Host]/[Edit Network/Host] ダイアログボックス - [NAT] タブ （60 ページ）

フィールド リファレンス

表 16 : [Add NAT Rule]/[Edit NAT Rule] ダイアログボックス

要素	説明
送信元インターフェイス（Source Interface）	パケットが発信されるインターフェイスの名前。これは「実際の」インターフェイスです。デフォルトは、すべてのインターフェイスを表す [任意（Any）] です。目的のインターフェイスを入力するか、または選択します。 （注） トランスペアレント ファイアウォール モードでは、特定のインターフェイスを設定する必要があります。
Destination Interface	[宛先インターフェイス（Destination Interface）]：パケットが到着するインターフェイスの名前。これは「マッピングされた」インターフェイスです。デフォルトは、すべてのインターフェイスを表す [任意（Any）] です。目的のインターフェイスを入力するか、または選択します。 （注） トランスペアレント ファイアウォール モードでは、特定のインターフェイスを設定する必要があります。

要素	説明
[送信元NATタイプ（Source NAT Type）]	作成する変換ルールのタイプ。 • [Static]：実際のアドレスからマッピングされたアドレスへのスタティックな割り当てを提供します。 • [ダイナミックPAT（非表示）（Dynamic Dynamic PAT (Hide)）]：複数のローカルアドレスから単一のグローバル IP アドレスおよび一意のポート番号へのダイナミックな割り当てを提供し、実質的に、ローカルアドレスを 1 つのグローバルアドレスの背後に「隠します」。 • [ダイナミックNATおよびPAT（Dynamic NAT and PAT）]：実際のアドレスからマッピングされたアドレス、および実際のポートからマッピングされたポートへのダイナミックな割り当てを提供します。 このオプションを選択すると、[PATプールアドレス変換（PAT Pool Address Translation）]オプションがダイアログボックスに追加されます。ルーテッドモードで稼働しているデバイスでは、このオプションによって次で説明するフォールスルーオプションも提供されます。 （注） このセクションは指定した送信元の変換にだけ適用されます。宛先の変換は常にスタティックになります。
[送信元の変換（Source Translation）]	
Original Source	NAT ルールで変換される送信元アドレス。アドレス範囲またはネットワークの場合は、範囲またはネットワーク内のすべてのアドレスが変換されます。

要素	説明
Translated Source アドレス（Address） インターフェイス	変換がデバイス上のアドレスまたはインターフェイスのどちらに基づくかを示します。次のいずれかを選択します。 • [アドレス（Address）] : [変換済み送信元（Translated Source）] フィールドで指定したネットワーク/ホストオブジェクトを使用して、元のアドレスを変換します。このエントリは変換アドレスのプールを示します。目的のネットワーク/ホストを入力するか、選択します。デフォルトは元の送信元アドレスです（アイデンティティ NAT ルールが作成されます）。 • [インターフェイス（Interface）] : [変換済み送信元（Translated Source）] フィールドで指定したインターフェイスに基づいて、元のアドレスを変換します。 このインターフェイスに基づくポート アドレス変換については、必ず（このダイアログボックスの [Advanced] パネルにある）[Service Translation] セクションでオプションを設定してください。 [宛先インターフェイス（Destination Interface）] フィールドを定義しなかった場合、[アドレス（Address）] と [インターフェイス（Interface）] の選択は [アドレス（Address）] に戻り、元の送信元アドレスが [アドレス（Address）] フィールドに挿入されます。これにより、アイデンティティ NAT ルールが作成されます。つまり、指定したアドレスはそれ自身に変換されます（事実上、変換されません）。アイデンティティ NAT はアウトバウンド接続だけに適用されます。 （注） これらのオプションは、選択されたタイプがダイナミック NAT および PAT である場合には使用できません。また、トランスペアレントモードで動作しているデバイスでは使用できません。

要素	説明
PAT Pool Address Translation	

要素	説明
	このオプションは、タイプとして [Dynamic NAT and PAT] を選択している場合に使用できます。関連パラメータを使用すると、PATマッピングに使用されるアルゴリズムを変更できるだけでなく、特にポートアドレス変換に使用するIPアドレスの「プール」を指定することができます。これらの機能の詳細については、PAT プールおよびラウンド ロビン割り当て （58 ページ）を参照してください。 [PAT Pool Address Translation] チェックボックスをオンにして、次のオプションをイネーブルにします。 • [アドレス（Address）] または [インターフェイス（Interface）]：[PATプールアドレス（PAT Pool Address）] フィールドに含まれているのが、PATプールとして使用するネットワーク/ホスト（またはネットワーク/ホストオブジェクト）であることを示すには、[アドレス（Address）] を選択します。インターフェイスを選択して、フォールスルー インターフェイスを指定します。 • [アドレス（Address）]：上記のアドレスまたはインターフェイスの選択に従って、目的のネットワーク/ホストまたはインターフェイスを入力するか、選択します。 • [ラウンドロビン割り当てを使用（Use Round Robin Allocation）]：「ラウンドロビン」アプローチを使用してアドレス/ポートをマッピングするには、このボックスをオンにします。このオプションの詳細については、PAT プールおよびラウンド ロビン割り当て （58 ページ）を参照してください。 • [拡張PATテーブル（Extended PAT Table）]（ASA 8.4(3) 以降で使用可能、8.5(1) または 8.6(1) を除く）：拡張 PAT を有効にするには、この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、PAT 変換の作成時に宛先ポートとアドレスは考慮されないため、PAT アドレスあたり 65535 個のポートに制限されます。たとえば、拡張 PAT を使用して、192.168.1.7:23 に向かう場合の 10.1.1.1:1027 の変換、および 192.168.1.7:80 に向かう場合の 10.1.1.1:1027 の変換を作成できます。このオプションは、ASA 8.4(3) 以降（8.5(1) または 8.6(1) を除く）で使用できます。 • [フラットなポート範囲（Flat Port Range）]（ASA 8.4(3) 以降で使用可能、8.5(1) または 8.6(1) を除く）：ポートの割り当て時に 1024 ～ 65535 のポート範囲全体の使用を有効にするには、この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

要素	説明
	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。下位の範囲でポートが不足するのを回避するには、この設定を行います。1 ～ 65535 の範囲全体を使用するには、[予約済みポートを含める（Include Reserved Ports）] もオンにします。 • [予約済みポートを含める（Include Reserved Ports）]（ASA 8.4(3) 以降で使用可能、8.5(1) または 8.6(1) を除く）：PAT 範囲に予約ポート 1 ～ 1023 を含めるには、このボックスをオンにします。 • [ブロック割り当て（Block Allocation）]（ASA 9.5(1) 以降で使用可能）：ホストごとにポートのブロックを割り当てるには、このボックスをオンにします。この機能は、ASA デバイス 9.5(1) 以降の Security Manager バージョン 4.9 以降でサポートされています。
Destination Translation 宛先アドレスの任意のスタティック変換を設定するには、このセクションのオプションを使用します。 （注） 定義すると、ルールのタイプに関係なく、宛先変換は常にスタティックになります。 （注） これらのオプションは、トランスペアレント モードで動作しているデバイスでは使用できません。	
[元の宛先（Original Destination）] アドレス（Address） インターフェイス	変換がデバイス上のアドレスまたはインターフェイスのどちらに基づくかを示します。次のいずれかを選択します。 • [アドレス（Address）] : [変換済み宛先（Translated Destination）] フィールドで指定したネットワーク/ホストオブジェクトを使用して、元の宛先を変換します。 [アドレス（Address）] を選択した場合、[元の宛先（Original Destination）] エントリフィールドで、元の宛先アドレスを変換するネットワーク/ホストオブジェクトを指定します。 • [インターフェイス（Interface）] : [変換済み宛先（Translated Destination）] フィールドで指定したネットワーク/ホストオブジェクトを使用して、元の宛先を変換します。 [インターフェイス（Interface）] を選択した場合は、[宛先インターフェイス（Destination Interface）] フィールドで目的のインターフェイスを入力または選択します。インターフェイス セレクタ リストには、デバイスに現在定義されているすべてのインターフェイスが含まれています。

要素	説明
[変換済みの宛先（Translated Destination）]	このエントリは、変換に使用する宛先アドレスのプールを示します。目的のネットワーク/ホストオブジェクトを入力するか、選択します。 （注） FPR-2000、FPR-4000、および FPR-9000 シリーズ プラットフォームの ASA 9.17(1) 以降のデバイスで使用する FQDN シングルトンオブジェクトを入力または選択できるようになりました。
Service Translation ポートアドレス変換を設定するには、このセクションのオプションを使用します。 これらのサービス オブジェクトは、サービス プロトコル（TCP または UDP）と 1 つ以上のポートを示します。元のポートから変換後のポートへのマッピングは循環されます。つまり、最初の元の値が最初の変換後の値にマッピングされ、2 番めの元の値が 2 番めの変換後の値にマッピングされるというように、元の値がすべて変換されるまで続きます。その時点までに変換後のポートのプールが枯渇してしまった場合、マッピングは、最初の変換後の値を再使用して続行されます。サービス オブジェクトの設定の詳細については、サービスとサービス オブジェクトおよびポート リスト オブジェクトの理解と指定を参照してください。 （注） [サービス変換（Service Translation）] と次の [このルールに一致するDNS応答を変換（Translate DNS replies that match this rule）] オプションは、同時には使用できません。	
[元のサービス（Original Service）]	変換対象のサービスが定義されているサービスオブジェクトを入力するか、選択します。任意のサービスから、指定した変換後のサービスへの変換を設定するには、[Original Service] フィールドを空白のままにします。 （注） 両方のサービス オブジェクトに指定されているプロトコルが同じである必要があります。
[変換対象サービス（Translated Service）]	変換に使用されるサービスを示すサービスオブジェクトを入力するか、選択します。
[オプション（Options）]	
このルールに一致する DNS 回答の変換	オンにすると、このルールに一致する DNS 応答に埋め込まれたアドレスが書き換えられます。 マッピングされたインターフェイスから実際のインターフェイスへの DNS 応答の場合、Address（または「A」）レコードはマッピングされた値から実際の値に書き換えられます。反対に、実際のインターフェイスからマッピングされたインターフェイスへの DNS 応答の場合、A レコードは実際の値からマッピングされた値に書き換えられます。この機能をサポートするには、DNS インスペクションをイネーブルにする必要があります。

要素	説明
[インターフェイスPATへのフォールスルー(宛先インターフェイス)（Fallthrough to Interface PAT (Destination Interface)）]	オンにすると、ダイナミック PAT のバックアップが有効になります。ダイナミック NAT アドレスのプールが枯渇すると、[Use Address] フィールドで指定されたアドレス プールを使用して、ポート アドレス変換が実行されます。このオプションは、ルーテッド モードで稼働しているデバイスで、タイプとして [Dynamic NAT and PAT] を選択している場合にだけ使用できます。
IPv6	選択すると、インターフェイスの IPv6 アドレスが使用されます。
[IPv4からIPv6へのネット間マッピング（Net to net mapping of IPv4 to IPv6）]	オンにすると、最初の IPv4 アドレスが最初の IPv6 アドレスに、2 番目が 2 番目に変換されます（以降も同様）。このオプションを指定しない場合、32 ビットの IPv4 アドレスが IPv6 プレフィックスの後に埋め込まれる IPv4 埋め込み方式が使用されます。1 対 1 変換の場合は、このオプションを選択する必要があります。
[宛先インターフェイスでARPをプロキシしない（Do not proxy ARP on Destination Interface）]	指定した宛先インターフェイスでプロキシ ARP を無効にするには、このボックスをオンにします。このオプションは、ルールのタイプとして [スタティック（Static）] を選択している場合には使用できません。 （注） このオプションは、方向として [Bidirectional] を選択している場合に、ASA 8.4.2+ デバイスだけで使用できます。 デフォルトでは、すべての NAT ルールは、出力インターフェイスでプロキシ ARP が含まれます。NAT 免除ルールは出力インターフェイスを検出するときにルートの概要に依存する入力トラフィックと出力トラフィックの両方に対して NAT をバイパスするために使用されます。したがって、プロキシ ARP は、NAT 免除ルールを無効にする必要があります。（NAT 免除ルールが常に優先し、[Translation Rules] テーブルの他のすべての NAT ルールの上に表示されます。） （注） [No Proxy ARP] の設定の説明に従って、個々のインターフェイスでプロキシ ARP を無効にすることもできます。
[宛先インターフェイスのルートルックアップの実行（Perform route lookup for Destination Interface）]	このオプションを選択すると、出力インターフェイスは、指定した宛先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決定されます。NAT 免除ルールでは、このチェックボックスをオンにしてください。このオプションは、スタティック アイデンティティ NAT でだけサポートされています。 （注） このオプションは、方向として [Bidirectional] を選択している場合に、ASA 8.4.2+ デバイスだけで使用できます。このオプションは、トランスペアレント モードで動作しているデバイスでは使用できません。

要素	説明
単一方向（Unidirectional）	この機能を使用すると、単一方向のみのスタティック NAT ルールか、両方向（順方向と逆方向）に 1 つずつの 2 つのルールを設定できます。 選択すると、このダイアログボックスに含まれる他のオプションの指定に従って、単一のスタティック NAT が作成されます。ダイナミック ルールは、デフォルトでは単一方向です。 選択を解除すると、このダイアログボックスに含まれる他のオプションの指定に従って、両方向の変換を含む 2 つのリンクされたスタティック NAT ルールが作成されます。ルール テーブルでは、各双方向ルール エントリが 2 行で構成されることに注意してください。
説明	（任意）ルールの説明を入力します。
カテゴリ	（任意）ルールに割り当てるカテゴリを選択します。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。詳細については、カテゴリ オブジェクトの使用を参照してください。 （注） このオプションは、ルールのタイプとして [Dynamic NAT and PAT] を選択している場合には使用できません。

PAT プールおよびラウンド ロビン割り当て

適応型セキュリティ アプライアンス バージョン 8.4.2 以降には、ポートアドレス変換（PAT）が行われる方法を変更できる 2 つの機能が含まれています。特に PAT の IP アドレスプールを明示的に定義でき、PAT 時のポート割り当てに「ラウンド ロビン」アルゴリズムを選択できます。

これらの機能によって、大量の PAT アドレスの設定を単純化でき、DoS 攻撃の一部として利用されることがある、単一の PAT アドレスからの大量の接続を防ぐことができます。

明示的な PAT プールの定義

バージョン 8.4.2 以前では、ダイナミック NAT および PAT ルールを定義するときに、変換に使用する IP アドレスのプールを指定します（ [NATルールの追加/編集（Add/Edit NAT rule）] ダイアログボックスの [変換済みソース（Translated Source）] フィールド）。このプールは、個別のIPアドレス、アドレスの範囲、ネットワーク/ホストオブジェクトまたはネットワーク/ホスト グループ オブジェクト、およびこれらの組み合わせで構成できました。

複数の IP アドレスを含む範囲とオブジェクトが「NAT プール」にあると見なされましたが、個々の IP アドレス、および 1 つ以上の個々の IP アドレスで構成されるグループ オブジェクトが「PAT プール」の一部と見なされました。

デバイスでのアドレス変換は、使用可能なすべてのアドレスを使い果たすまで NAT プールを通じて進行します。その後、PAT プールを使用してポート アドレス変換が起動します。PAT プールの最初の IP アドレスにポートを割り当て、すべてのポート（約 64,000 個）を割り当て終えると、プールの次のアドレスにポートを割り当てます。その後も同様に動作します。プー

ル内のすべての IP アドレスですべてのポートが完全に登録されると、これ以上の変換は行われません。

バージョン 8.4.2 以降の ASA デバイスでは、ダイナミックな NAT の個別の PAT プールと PAT ルールを明示的に定義できます。このように定義する場合、アドレスの最初の集合（[変換済みソース（Translated Source）] フィールドで定義される）は NAT プールと見なされますが、PAT プールアドレスは、[PATプールアドレス変換（PAT Pool Address Translation）] フィールドで指定されます。

（注） 明示的に PAT プールを指定しない場合、アドレス変換は 8.4.2 以前のデバイスの説明に従って実行されます。

トランスレーション ルールの定義の詳細については、[Add NAT Rule]/[Edit NAT Rule] ダイアログボックス （49 ページ） を参照してください。

ラウンド ロビン ポート割り当て

バージョン 8.4.2 以降の ASA デバイスでは、PAT 処理でのポート割り当てに別の方法を指定することもできます。すでに説明したように、PAT ポート番号は、最後のポート番号が割り当てられるまで単一の IP アドレスに連続して割り当てられ、その後、プールで次に使用できる IP アドレスを使用して、プロセスが再開します。

ただし、8.4.2 以降のデバイスの新しいパラメータである [PATプールにラウンドロビン割り当てを使用（Use Round Robin Allocation for PAT Pool）] を使用すると、使用可能な IP アドレスとポート番号を使用した「ラウンド ロビン」サイクルを指定できます。 この方法では、プールでそれぞれ連続するアドレスを使用して、アドレス/ポートの組み合わせを割り当てます。その後、最初のアドレスを異なるポートで再度使用し、次に2番目のアドレスを使用し、以後、同様に動作します。

さらに、ラウンドロビン アルゴリズムは、PAT 処理でアドレスとポートの組み合わせを割り当てるときに準拠を試行する 2 つの追加の原則を組み込みます。

- 送信元から宛先への特定のマッピングがすでに存在する場合は、アルゴリズムは新しい接続に対して既存の変換を使用しようとします。これが不可能な場合（たとえば、その IP アドレスのすべてのポートが使い果たされたとき）、アルゴリズムは標準のラウンドロビン サイクルを続行します。
- 可能な場合、元の送信元ポート番号がマッピング ポート番号として使用されます。つまり、たとえば、変換するアドレスとポートの組み合わせのポート番号が 4904 で、4904 が PAT プールの次の IP アドレスで使用可能な場合、変換後のアドレスは *PAT_address* /4904 になります。これが不可能な場合（そのポートが次の PAT アドレスで使用できない）、アルゴリズムは標準のラウンドロビンサイクルを続行することに注意してください。

（注） 明示的にラウンド ロビン割り当てを指定しない場合、ポート割り当て循環は 8.4.2 以前のデバイスの説明に従って実行されます。

[Add Network/Host]/[Edit Network/Host] ダイアログボックス - [NAT] タブ

ホスト、ネットワーク、またはアドレス範囲オブジェクトの追加または編集に使用するダイアログボックスのいずれかの [NAT] タブを使用して、オブジェクト NAT ルールを作成または更新します。この NAT 設定は、ASA 8.3+ デバイスでだけ使用されます。他のタイプのデバイスでこのオブジェクトを使用した場合、NAT 設定は無視されます。

NAT 設定は、デバイスのオーバーライドとして作成され、グローバル オブジェクトには保持されません。そのため、これらの NAT オプションを設定する場合は、[デバイスごとに値のオーバーライドを許可（Allow Value Override per Device）] オプションを選択する必要があります（このオプションはダイアログボックスを閉じたときに、自動的に選択されます）。

この項では、[NAT] タブのフィールドについて説明します。[General] タブのフィールドの詳細については、[Add Network/Host]/[Edit Network/Host] ダイアログボックスを参照してください。

ナビゲーション パス

ホスト、ネットワーク、またはアドレス範囲オブジェクトの作成時か編集時に、[Add Network/Host]/[Edit Network/Host] ダイアログボックスの [NAT] タブを選択します。

フィールド リファレンス

表 17 : [Add Network/Host]/[Edit Network/Host] ダイアログボックスの [NAT] タブ

要素	説明
Add Automatic Address Translation NAT Rule	オンにすると、ネットワーク アドレス変換（NAT）規則が、ここでの定義に従って、[Translated By] フィールドで指定したデバイスに適用されます。ルールは、そのデバイスの [Translation Rules] テーブルの [Network Object NAT Rule] セクションに表示されます（[Translation Rules]：ASA 8.3+ （46 ページ）を参照）。
Translated By	NAT ルールを設定するデバイス。[Select] をクリックして、リストからデバイスを選択します。リストは、ASA 8.3+ デバイスだけを表示するようにフィルタリングされています。
送信元インターフェイス（Source Interface）	パケットが発信されるインターフェイスの名前。これは「実際の」インターフェイスです。デフォルトは、すべてのインターフェイスを表す [任意（Any）] です。
Destination Interface	パケットが到着するインターフェイスの名前。これは「マッピングされた」インターフェイスです。デフォルトは、すべてのインターフェイスを表す [任意（Any）] です。

要素	説明
タイプ（Type）	作成する変換ルールのタイプ。 • [静的（Static）]：実際のアドレスからマッピングされたアドレスへのスタティックな割り当てを提供します。 • [PAT（非表示）（PAT (Hide)）]：複数のローカルアドレスから単一のグローバル IP アドレスおよび一意のポート番号へのダイナミックな割り当てをイネーブルにします。 • [ダイナミックNATおよびPAT（Dynamic NAT and PAT）]：実際のアドレスからマッピングされたアドレス、および実際のポートからマッピングされたポートへのダイナミックな割り当てを提供します。
送信元の変換	
Original value	このダイアログボックスの [General] タブで設定したアドレスが表示されます。これは、NAT ルールで変換する送信元アドレスです。アドレス範囲またはネットワークの場合は、範囲またはネットワーク内のすべてのアドレスが変換されます。
Translated Source Use Address Use Interface（スタティックおよびPAT にかぎり有効）	変換がデバイス上のアドレスまたはインターフェイスのどちらに基づくかを示します。 • [アドレスを使用（Use Address）]：指定したアドレスまたはネットワーク/ホストオブジェクトを使用して、元のアドレスを変換します。[アドレス（Address）] フィールドにアドレスまたはオブジェクト名を入力するか、または [選択（Select）] をクリックしてリストからオブジェクトを選択します。 • [インターフェイスを使用（Use Interface）]：[変換済み送信元（Translated Source）] フィールドで指定したインターフェイスに基づいて、元のアドレスを変換します。 （注） [Use Interface] オプションは、タイプとして [Static] または [PAT (Hide)] を選択している場合にだけ使用できます。

要素	説明
PAT Pool Address Translation	

要素	説明
	このオプションは、タイプとして [Dynamic NAT and PAT] を選択している場合に使用できます。関連パラメータを使用すると、PAT マッピングに使用されるアルゴリズムを変更できるだけでなく、特にポート アドレス変換に使用する IP アドレスの「プール」を指定することができます。これらの機能の詳細については、PAT プールおよびラウンド ロビン割り当て （58 ページ）を参照してください。 [PAT Pool Address Translation] チェックボックスをオンにして、次のオプションをイネーブルにします。 • [アドレスを使用（Use Address）] または [インターフェイスを使用（Use Interface）] : [PATプールアドレス（PAT Pool Address）] フィールドに含まれているのが、PATプールとして使用するネットワーク/ホスト（またはネットワーク/ホストオブジェクト）であることを示すには、[アドレスを使用（Use Address）] を選択します。フォールスルー インターフェイスを提供するには、[インターフェイスを使用（Use Interface）] を選択します。 • [PATプールアドレス（PAT Pool Address）] : 上記のアドレスまたはインターフェイスの選択に従って、目的のネットワーク/ホストまたはインターフェイスを入力するか、選択します。 • [PATプールにラウンドロビン割り当てを使用（Use Round Robin Allocation for PAT Pool）] : 「ラウンドロビン」アプローチを使用してアドレス/ポートをマッピングするには、このボックスをオンにします。このオプションの詳細については、PAT プールおよびラウンド ロビン割り当て （58 ページ）を参照してください。 • [拡張PATテーブル（Extended PAT Table）]（ASA 8.4(3) 以降で使用可能、8.5(1) または 8.6(1) を除く） : 拡張 PAT を有効にするには、この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、PAT 変換の作成時に宛先ポートとアドレスは考慮されないため、PAT アドレスあたり 65535 個のポートに制限されます。たとえば、拡張 PAT を使用して、192.168.1.7:23 に向かう場合の 10.1.1.1:1027 の変換、および 192.168.1.7:80 に向かう場合の 10.1.1.1:1027 の変換を作成できます。このオプションは、ASA 8.4(3) 以降（8.5(1) または 8.6(1) を除く）で使用できます。 • [フラットなポート範囲（Flat Port Range）]（ASA 8.4(3) 以降で使用可能、8.5(1) または 8.6(1) を除く） : ポートの割り当て時に 1024 ～ 65535 のポート範囲全体の使用を有効にするには、この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

要素	説明
	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。下位の範囲でポートが不足するのを回避するには、この設定を行います。1 ～ 65535 の範囲全体を使用するには、[予約済みポートを含める（Include Reserved Ports）] もオンにします。 • [予約済みポートを含める（Include Reserved Ports）]（ASA 8.4(3) 以降で使用可能、8.5(1) または 8.6(1) を除く）：PAT 範囲に予約ポート 1 ～ 1023 を含めるには、このボックスをオンにします。
Service Translation スタティック ポート アドレス変換を設定するには、[Advanced] パネルのこのセクションのオプションを使用します。 （スタティック ルールにかぎり有効） （注） [サービス変換（Service Translation）] と [このルールに一致するDNS応答を変換（Translate DNS replies that match this rule）] オプションは、同時には使用できません。	
プロトコル	TCP ポートか UDP ポートか。
元のポート	トラフィックがデバイスに着信するポート。
[変換されたポート（Translated Port）]	元のポート番号を交換するポート番号。
[オプション（Options）]	
このルールに一致する DNS 回答の変換	オンにすると、このルールに一致する DNS 応答に埋め込まれたアドレスが書き換えられます。 マッピングされたインターフェイスから実際のインターフェイスへの DNS 応答の場合、Address（または「A」）レコードはマッピングされた値から実際の値に書き換えられます。反対に、実際のインターフェイスからマッピングされたインターフェイスへの DNS 応答の場合、A レコードは実際の値からマッピングされた値に書き換えられます。この機能をサポートするには、DNS インスペクションをイネーブルにする必要があります。 （注） このオプションと [サービス変換（Service Translation）] は、同時には使用できません。

要素	説明
[インターフェイスPATへのフォールスルー(宛先インターフェイス)（Fallthrough to Interface PAT (Destination Interface)）]	オンにすると、ダイナミック PAT のバックアップが有効になります。ダイナミック NAT アドレスのプールが枯渇すると、[Use Address] フィールドで指定されたアドレス プールを使用して、ポート アドレス変換が実行されます。このオプションは、ルーテッド モードで稼働しているデバイスで、タイプとして [Dynamic NAT and PAT] を選択している場合にだけ使用できます。
IPv6	選択すると、インターフェイスの IPv6 アドレスが使用されます。
[IPv4からIPv6へのネット間マッピング（Net to net mapping of IPv4 to IPv6）]	オンにすると、最初の IPv4 アドレスが最初の IPv6 アドレスに、2 番目が 2 番目に変換されます（以降も同様）。このオプションを指定しない場合、32 ビットの IPv4 アドレスが IPv6 プレフィックスの後に埋め込まれる IPv4 埋め込み方式が使用されます。1 対 1 変換の場合は、このオプションを選択する必要があります。
[宛先インターフェイスでARPをプロキシしない（Do not proxy ARP on Destination Interface）]	指定した宛先インターフェイスでプロキシ ARP を無効にするには、このボックスをオンにします。このオプションは、ルールのタイプとして [スタティック（Static）] を選択している場合には使用できません。 デフォルトでは、すべての NAT ルールは、出力インターフェイスでプロキシ ARP が含まれます。NAT 免除ルールは出力インターフェイスを検出するときにルートの概要に依存する入力トラフィックと出力トラフィックの両方に対して NAT をバイパスするために使用されます。したがって、プロキシ ARP は、NAT 免除ルールを無効にする必要があります。（NAT 免除ルールが常に優先し、[Translation Rules] テーブルの他のすべての NAT ルールの上に表示されます。） （注） [No Proxy ARP] の設定の説明に従って、個々のインターフェイスでプロキシ ARP を無効にすることもできます。
[宛先インターフェイスのルートルックアップの実行（Perform route lookup for Destination Interface）]	このオプションを選択すると、出力インターフェイスは、指定した宛先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決定されます。NAT 免除ルールでは、このチェックボックスをオンにしてください。このオプションは、スタティック アイデンティティ NAT でだけサポートされています。 （注） このオプションは、トランスペアレント モードで動作しているデバイスでは使用できません。

Per-Session NAT ルール: ASA 9.0（1）+

[Per-Session NATルール（Per-Session NAT Rules）] ページを使用して、選択した ASA 9.0(1)+ デバイスで Per-Session PAT ルールを設定します。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。特定のトラフィックに Multi-session PAT を使用するように、Per-session ルールを設定できます。

Per-Session PAT と Multi-Session PAT の比較（バージョン 9.0(1) 以降）

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 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。

[Per-Session NATルール（Per-Session NAT Rules）] テーブルの一部の機能

この [Translation Rules] テーブルは、ルール テーブルの使用で示すような標準的な Security Managerのルールテーブルです。たとえば、カラムを移動、表示または非表示にしたり、ルールの順序を変更したり、特定のテーブルセルを右クリックしてそのパラメータを編集したりできます。

このテーブルに一覧表示されているNATルールは最初に一致したものから順に処理されます。そのため、順序は重要です。

関連項目

- [セッションごとのNATルールの追加（Add Per Session NAT Rule）]/[セッションごとのNATルールの編集（Edit Per Session NAT Rule）] ダイアログボックス （68 ページ）
- セキュリティ デバイスの NAT ポリシー （20 ページ）
- ASA 8.3 以降のデバイスでの「簡易」NAT について （5 ページ）
- 標準のルール テーブルに関する内容：
  - ルール テーブルの使用
  - テーブルのフィルタリング
  - テーブル カラムおよびカラム見出しの機能

ナビゲーション パス

- （デバイスビュー）デバイスポリシーセレクタから [NAT] > [Per-Session NATルール（Per-Session NAT Rules）] を選択します。

- （ポリシービュー）ポリシータイプセレクタから [NAT（PIX/ASA/FWSM）] > [Per-Session NATルール（Per-Session NAT Rules）] を選択します。共有ポリシーセレクタから既存のポリシーを選択するか、または [変換ルール（Translation Rules）] を右クリックして新しいポリシーを作成します。

[Per-Session NATルール（Per-Session NAT Rules）] ページが表示されます。

ルールの追加、編集、および削除

Per-Session NAT ルールを**追加**するには：

1. ルールを追加するルールを選択します。見出しを選択しなかった場合、ルールはデフォルトでテーブルの末尾に追加されます。
2. [Per-Session NATルールの追加（Add Per-Session NAT Rule）] ダイアログボックスを開きます。テーブルの下部にある [行の追加（Add Row）] ボタンをクリックするか、またはテーブル内の任意の場所を右クリックしてポップアップメニューから [行の追加（Add Row）] を選択します。
3. ルールを定義してから [OK] をクリックしてダイアログボックスを閉じると、ルールがテーブルに追加されます。

[Per-Session NATルールの追加（Add Per-Session NAT Rule）] ダイアログボックスの詳細な説明については、[セッションごとのNATルールの追加（Add Per Session NAT Rule）]/[セッションごとのNATルールの編集（Edit Per Session NAT Rule）] ダイアログボックス （68 ページ）を参照してください。

Per-Session NAT ルールを**編集**するには：

1. 目的のルールの [Per-Session NATルールの編集（Edit Per-Session NAT Rule）] ダイアログボックスを開きます。[Per-Session NATルール（Per-Session NAT Rule）] テーブルでルールを選択してテーブルの下部にある [行の編集（Edit Row）] ボタンをクリックするか、または単に目的のルールエントリを右クリックしてポップアップメニューから [行の編集（Edit Row）] を選択します。
2. ルールを編集してから [OK] をクリックしてダイアログボックスを閉じます。

[Per-Session NATルールの編集（Edit Per-Session NAT Rule）] ダイアログボックスの詳細な説明については、[セッションごとのNATルールの追加（Add Per Session NAT Rule）]/[セッションごとのNATルールの編集（Edit Per Session NAT Rule）] ダイアログボックス （68 ページ）を参照してください。

NAT ルールを**削除**するには、テーブルでルールを選択してテーブルの下部にある [行の削除（Delete Row）] ボタンをクリックするか、または単に目的のルールエントリを右クリックしてポップアップメニューから [行の削除（Delete Row）] を選択します。

ルールの有効化と無効化

次のように、1 つ以上の連続するルールをテーブルから削除せずにディセーブルにできます。

1. ディセーブルにするルールを選択します。連続したルールのブロックを選択する場合は、ブロックの最初のルールをクリックしてから、ブロックの最後のルールを Shift を押した状態でクリックします。
2. 選択したルールを右クリックして、ポップアップメニューから [無効化（Disable）] を選択します。

無効になっているルールは、テーブルでグレー表示されます。

無効になっている 1 つ以上の連続するルールを再度有効にするには、このプロセスを繰り返して、ポップアップメニューから [有効化（Enable）] を選択します。

[セッションごとのNATルールの追加（Add Per Session NAT Rule）]/[セッションごとのNATルールの編集（Edit Per Session NAT Rule）] ダイアログボックス

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 の違いの詳細については、Per-Session NAT ルール: ASA 9.0（1）+ （65 ページ）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無効にするには、次を追加できます。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

ナビゲーション パス

Per-Session NAT ルール: ASA 9.0（1）+ （65 ページ）ページから、次のいずれかを実行します。

- ルールを追加するには、ルールを追加するルールを選択してから、ルールテーブルの下にある [行の追加（Add Row）] ボタンをクリックするか、またはテーブル内の任意の場所を右クリックし、[行の追加（Add Row）] を選択して [Per-Session NATルールの追加（Add Per-Session NAT Rule）] ダイアログボックスを開きます。

- ルールを編集するには、ルールを選択して [行の編集（Edit Row）] ボタンをクリックするか、単にルールを右クリックし [行の編集（Edit Row）] を選択して、そのルールの [NAT ルールの編集（Edit NAT Rule）] ダイアログボックスを開きます。

関連項目

- Per-Session NAT ルール: ASA 9.0（1）+ （65 ページ）
- [Translation Rules]：ASA 8.3+ （46 ページ）
- [Add Network/Host]/[Edit Network/Host] ダイアログボックス - [NAT] タブ （60 ページ）

フィールド リファレンス

表 *18 : [Add NAT Rule]/[Edit NAT Rule]* ダイアログボックス

要素	説明
操作	このルールのアクション。許可または拒否します。 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。
[元のネットワーク（Original Network）]	送信元アドレス、またはルールが適用されるアドレス（またはネットワーク/ホストオブジェクト）。アドレス範囲またはネットワークの場合は、範囲またはネットワーク内のすべてのアドレスが変換されます。
宛先ネットワーク	宛先アドレス、またはルールが適用されるアドレス（またはネットワーク/ホストオブジェクト）。
[サービス（TCP/UDP のみ）（Service (tcp/udp Only)）]	変換対象のサービスが定義されているサービスオブジェクトを入力するか、選択します。 これらのサービス オブジェクトは、サービス プロトコル（TCP または UDP）と 1 つ以上のポートを示します。サービス オブジェクトの設定の詳細については、サービスとサービス オブジェクトおよびポート リスト オブジェクトの理解と指定を参照してください。
カテゴリ	（任意）ルールに割り当てるカテゴリを選択します。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。詳細については、カテゴリ オブジェクトの使用を参照してください。 （注） このオプションは、ルールのタイプとして [Dynamic NAT and PAT] を選択している場合には使用できません。
説明	（任意）ルールの説明を入力します。

[セッションごとのNATルールの追加（**Add Per Session NAT Rule**）]/[セッションごとのNATルールの編集（**Edit Per Session NAT Rule**）] ダイアログ ボックス

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。