CHAPTER 25

NAT の設定

この章では、ネットワーク アドレス変換について説明します。次の項目を取り上げます。

NAT の概要

ここでは、セキュリティ アプライアンス 上での NAT の機能について説明します。次の項目を取り上げます。

NAT の概要

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。NAT は 2 つのステップで構成されます。実際のアドレスをマッピング アドレスに変換するプロセスと、リターン トラフィック用に変換を元に戻すプロセスです。

セキュリティ アプライアンスは、NAT ルールがトラフィックに一致すると、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、セキュリティの高いインターフェイス（内部）からセキュリティの低いインターフェイス（外部）に移動するパケットが NAT 規則と一致することが要求されます。一致しない場合、パケットの処理は停止されます。セキュリティ レベルの詳細については、

「デフォルトのセキュリティ レベル」（P.5-4）を参照してください。NAT 制御の詳細については、「NAT コントロール」（P.25-5）を参照してください。

（注）　このマニュアルでは、すべてのタイプの変換を NAT と呼びます。NAT の説明では、*内部*および*外部*という用語は任意の 2 つのインターフェイス間のセキュリティ関係を表しています。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。たとえば、インターフェイス 1 が 60 でインターフェイス 2 が 50 の場合、インターフェイス 1 が「内部」、インターフェイス 2 が「外部」です。

NAT の利点の一部を紹介します。

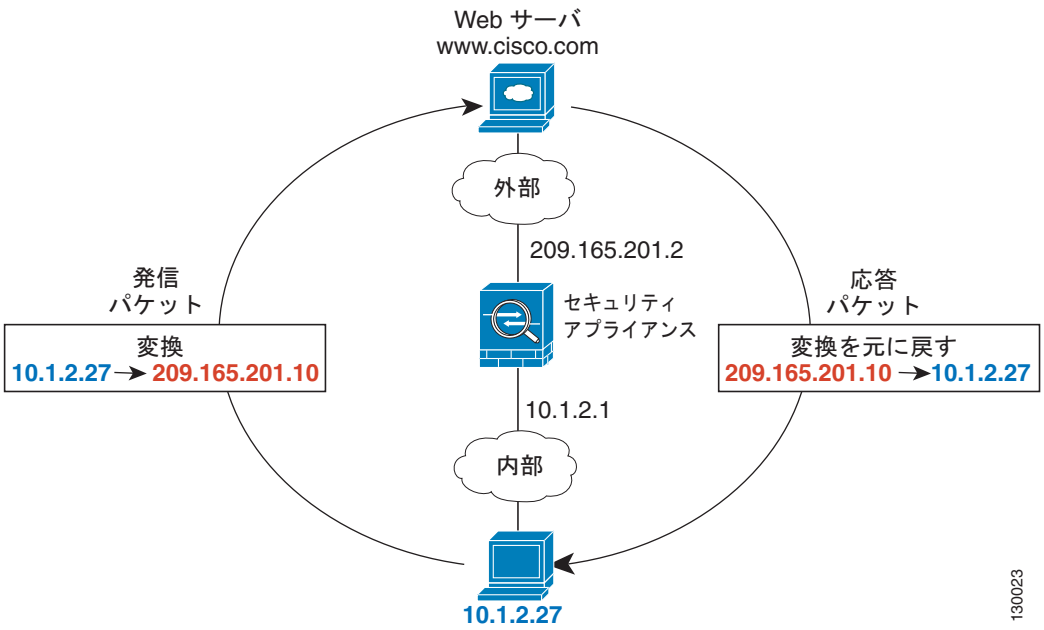
- 内部ネットワークでプライベート アドレスを使用できます。プライベート アドレスは、インターネットにルーティングできません。
- NAT は他のネットワークから実アドレスを隠すので、攻撃側はホストの実アドレスを突き止めることができません。
- 重複アドレスなど、IP ルーティングの問題を解決できます。

NAT でサポートされないプロトコルについては、表 24-1（P.24-3）を参照してください。

ルーテッド モードの NAT

図 25-1 は、内部にプライベート ネットワークを持つ、ルーテッド モードの一般的な NAT の例を示しています。10.1.1.27 にある内部ホストが Web サーバにパケットを送信すると、そのパケットの送信元実アドレス 10.1.1.27 がマップ アドレス 209.165.201.10 に変更されます。サーバが応答すると、応答がマッピング アドレス 209.165.201.10 に送信されます。そのパケットをセキュリティ アプライアンスが受信します。セキュリティ アプライアンスはその後、パケットをホストに送信する前に、変換したマッピング アドレス 209.165.201.10 を元の実際のアドレス 10.1.1.1.27 に戻します。

図 25-1　　NAT の例：ルーテッド モード



トランスペアレント モードの NAT

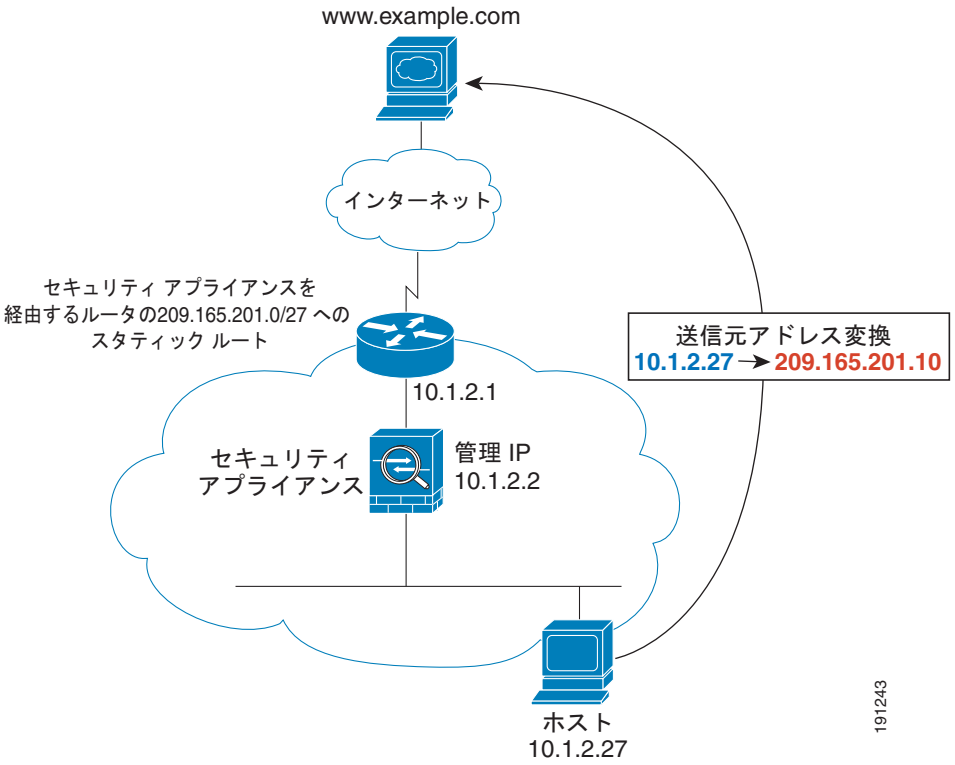
NAT をトランスペアレント モードで使用すると、ネットワークで NAT を実行するためのアップストリーム ルータまたはダウンストリーム ルータが必要なくなります。たとえば、トランスペアレント ファイアウォール セキュリティ アプライアンス は 2 つの VRF 間で役立ちます。つまり、VRF およびグローバル テーブル間で BGP ネイバー関係を確立できます。ただし、VRF ごとの NAT はサポートされない場合があります。この場合、トランスペアレント モードで NAT を使用することが必要不可欠です。

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 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上にない場合、アップストリーム ルータで、（セキュリティ アプライアンス から）ダウンストリーム ルータを指しているマッピング アドレスにスタティック ルートを追加する必要があります。
- 実際の宛先アドレスがセキュリティ アプライアンスに直接接続されていない場合、セキュリティ アプライアンスで、ダウンストリーム ルータを指している実際の宛先にもスタティック ルートを追加する必要があります。NAT を使用しない場合、アップストリーム ルータからダウンストリーム 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 アプライアンスでルートを何も必要としません。ただし、NAT を使用する場合、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、ダウンストリーム ルータへのスタティック ルートが必要になります。
- **alias** コマンドはサポートされていません。
- 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、何らかの理由でファイアウォール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。

図 25-2 に、インターフェイス内部と外部に同じネットワークを持つ、トランスペアレント モードの一般的な NAT のシナリオを示します。このシナリオのトランスペアレント ファイアウォールは NAT サービスを実行しているため、アップストリーム ルータは NAT を実行する必要がありません。内部ホスト 10.1.1.27 が Web サーバにパケットを送信すると、パケットの実際の送信元アドレス 10.1.1.27 はマッピング アドレス 209.165.201.10 に変更されます。サーバが応答すると、マッピング アドレス 209.165.201.10 に応答を送信し、セキュリティ アプライアンス がそのパケットを受信します。これは、アップストリーム ルータには、セキュリティ アプライアンス を経由するスタティック ルートのこのマッピング ネットワークが含まれるためです。その後、セキュリティ アプライアンス はマッピング アドレス 209.165.201.10 を変換して実際のアドレス 10.1.1.1.27 に戻します。実際のアドレスは直接接続されているため、セキュリティ アプライアンスはそのアドレスを直接ホストに送信します。

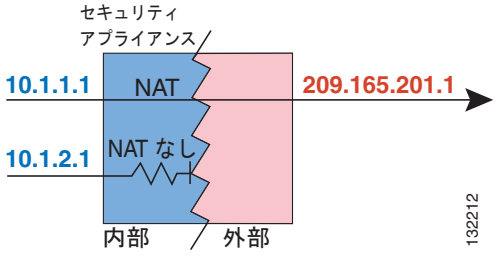
図 25-2　NAT の例：トランスペアレント モード



NAT コントロール

NAT 制御では、内部インターフェイスから外部インターフェイスに移動するパケットが NAT 規則と一致する必要があります。内部ネットワークの任意のホストが外部ネットワークのホストにアクセスできるようにするには、内部ホスト アドレスが変換されるように NAT を設定する必要があります（図 25-3 を参照）。

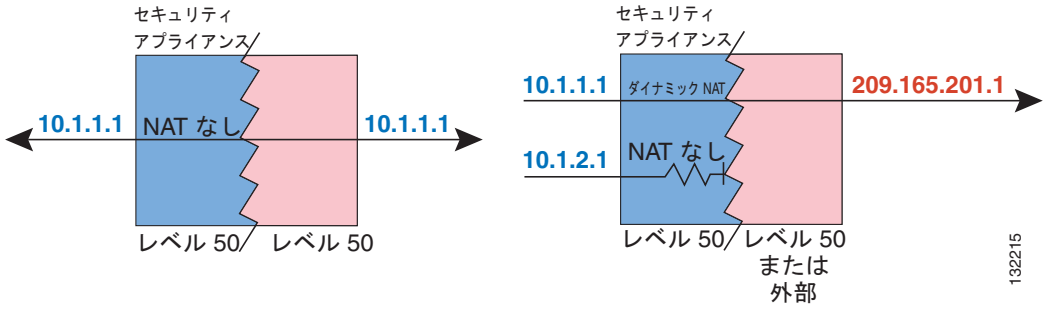
図 25-3　NAT 制御と発信トラフィック



セキュリティ レベルが同じインターフェイス同士で通信する場合には、NAT を使用する必要はありません。ただし、ダイナミック NAT または PAT を同じセキュリティ レベルのインターフェイス上に設定した場合は、そのインターフェイスから同じセキュリティ レベルのインターフェイス、または外部インターフェイスに向かうすべてのトラフィックは、NAT 規則と一致する必要があります（図 25-4 を

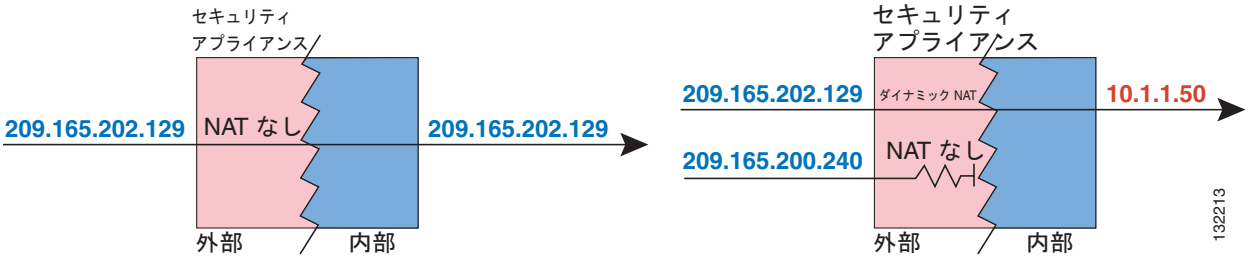
参照）。

図 25-4　NAT 制御と同一セキュリティ トラフィック



同様に、外部のダイナミック NAT または PAT をイネーブルにした場合、すべての外部トラフィックは、内部インターフェイスにアクセスするときに、NAT 規則と一致する必要があります（図 25-5 を参照）。

図 25-5　NAT 制御と着信トラフィック



スタティック NAT では、これらの制約は発生しません。

デフォルトでは、NAT 制御はディセーブルになっています。したがって、NAT を実行する場合以外、いずれのネットワークにおいても NAT を実行する必要はありません。ただし、新バージョンのソフトウェアにアップグレードした場合、NAT 制御がイネーブルになっていることがあります。NAT 制御がディセーブルになっている場合でも、ダイナミック NAT を設定するすべてのアドレスで NAT を実行する必要があります。ダイナミック NAT の適用方法については、「ダイナミック NAT の実装」（P.25-18）を参照してください。

NAT 制御によってセキュリティ レベルを上げる必要があるが、一部のケースで内部アドレスを変換しない場合、このようなアドレスに NAT 除外またはアイデンティティ NAT ルールを適用できます。（詳細については、「NAT 免除の使用」（P.25-32）を参照してください）。

NAT 制御を設定するには、「NAT 制御の設定」（P.25-17）を参照してください。

（注） マルチ コンテキスト モードでは、共有インターフェイスで固有の MAC アドレスをイネーブルにしない場合、パケット分類子が NAT コンフィギュレーションに依存してパケットをコンテキストに割り当てる場合があります。分類機能と NAT の関係の詳細については、「セキュリティ アプライアンスによるパケットの分類方法」（P.9-3）を参照してください。

NAT のタイプ

この項では、使用可能な NAT のタイプについて説明します。次の項目を取り上げます。

- 「ダイナミック NAT」（P.25-6）
- 「PAT」（P.25-9）
- 「スタティック NAT」（P.25-9）
- 「スタティック PAT」（P.25-9）
- 「NAT 制御がイネーブルな状態での NAT のバイパス」（P.25-10）

アドレス変換は、ダイナミック NAT、ポート アドレス変換（PAT）、スタティック NAT、スタティック PAT、またはこれらのタイプの組み合わせとして実装できます。NAT をバイパスする規則を設定することもできます。たとえば、NAT を実行しない場合に、NAT 制御をイネーブルにします。

ダイナミック NAT

ダイナミック NAT では、実際のアドレスのグループは、宛先ネットワーク上でルーティング可能なマッピング アドレスのプールに変換されます。マッピングされたプールにあるアドレスは、実際のグループより少ないことがあります。変換対象のホストが宛先ネットワークにアクセスすると、セキュリティ アプライアンスは、マッピングされたプールから IP アドレスをそのホストに割り当てます。この変換は、実ホストが接続を開始するときにだけ追加されます。変換は接続が継続している間だけ有効であり、変換がタイムアウトすると、そのユーザは同じ IP アドレスを保持しません。したがって、アクセス リストでその接続が許可されている場合でも、宛先ネットワークのユーザは、ダイナミック NAT を使用しているホストへの確実な接続を開始できません。また、セキュリティ アプライアンスは、実際のホスト アドレスに直接接続しようとする試みを拒否します。ホストへの確実なアクセスについては、「スタティック NAT」の項または「スタティック PAT」の項を参照してください。

（注）　セキュリティ アプライアンスがセッションを拒否した場合でも、接続に変換が追加されることがあります。この状況は通常、変換がタイムアウトになる着信アクセス リスト、管理専用インターフェイス、またはバックアップ インターフェイスで発生します。

図 25-6 は、リモート ホストによる実アドレスへの接続試行を示しています。セキュリティ アプライアンスはマッピング アドレスへのリターン接続だけを許可するため、この接続は拒否されています。

図 25-6　リモート ホストによる実アドレスへの接続試行

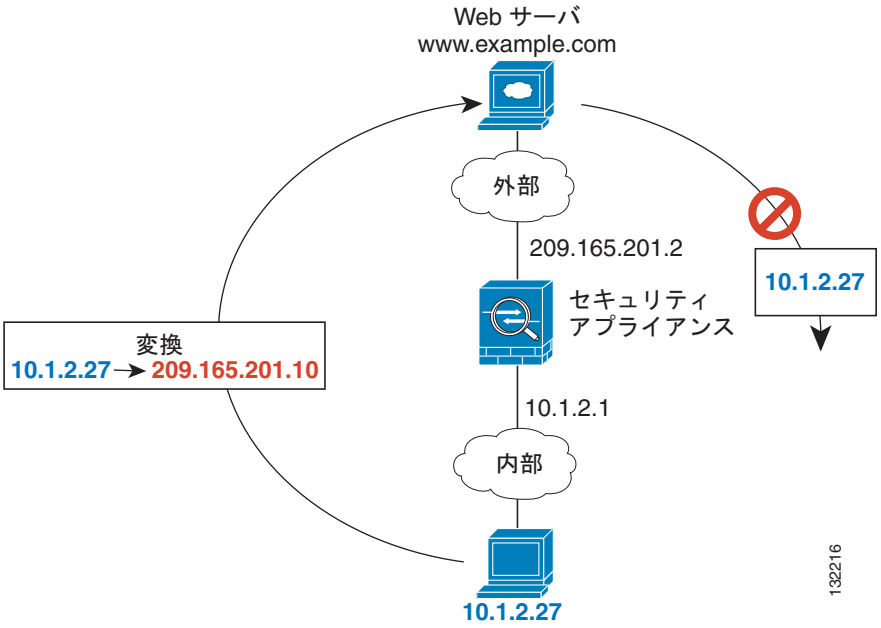
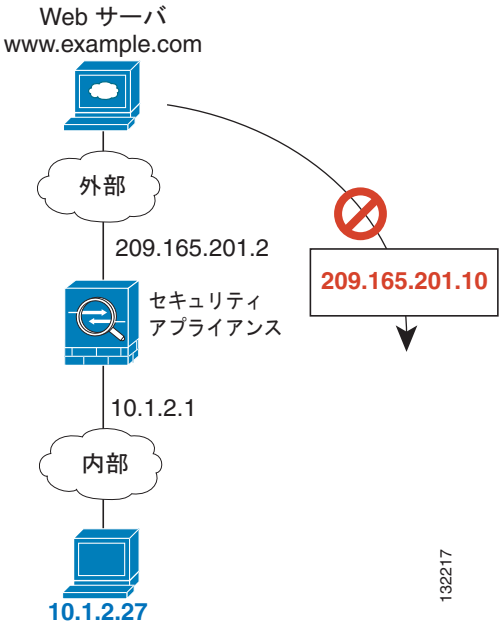


図 25-7 に、マッピング アドレスへの接続開始を試みているリモート ホストを示します。このアドレスは、現時点では変換テーブルにないため、セキュリティ アプライアンスはパケットをドロップしています。

図 25-7　マッピング アドレスへの接続開始を試みているリモート ホスト



（注） 変換の実施中、リモート ホストから、変換されたホストへの接続を開始できます（その接続がアクセス リストで許可されている場合）。アドレスは予測不可能であるため、ホストへの接続は確立されません。ただし、この場合は、アクセス リストのセキュリティに依存できます。

ダイナミック NAT には、次の欠点があります。

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

  この事象が発生した場合には、PAT を使用します。PAT では、単一アドレスのポートを使用して 64,000 を超える変換を処理できるためです。

- マッピング プールでは、ルーティング可能なアドレスを多数使用する必要があります。インターネットのように宛先ネットワークで登録済みアドレスが必要になる場合は、使用可能なアドレスが不足することがあります。

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

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

NAT および PAT のサポートの詳細については、「アプリケーション プロトコル インスペクションを使用するタイミング」（P.24-2）を参照してください。

PAT

PAT は、複数の実アドレスを単一のマッピング IP アドレスに変換します。具体的には、セキュリティ アプライアンスが複数の実際のアドレスおよび送信元ポート（実際のソケット）を 1 つのマッピング アドレスおよび 1024 より上の一意のポート（マッピング ソケット）に変換します。接続ごとに送信元ポートが異なるため、それぞれの接続で個別に変換を行う必要があります。たとえば、10.1.1.1:1025 には、10.1.1.1:1026 とは別の変換が必要です。

接続の有効期限が切れると、ポート変換も 30 秒間の非アクティブ状態の後に有効期限切れになります。このタイムアウトは変更できません。宛先ネットワーク上のユーザは、PAT を使用するホストに対して（アクセス リストによって接続が許可されていた場合でも）、接続を確実に開始することはできません。ホストの実またはマップ ポート番号を予測できないだけでなく、セキュリティ アプライアンス は変換対象ホストが接続を開始する側でない限り、変換を作成しません。ホストへの確実なアクセスについては、次の「スタティック NAT」または「スタティック PAT」の項を参照してください。

PAT では単一のマッピング先のアドレスを使用するため、ルーティング可能なアドレスの使用を抑えることができます。さらに、セキュリティ アプライアンス インターフェイスの IP アドレスを PAT アドレスとして使用できます。PAT は、データ ストリームが制御パスとは別のものであるマルチメディア アプリケーションでは機能しません。NAT および PAT のサポートの詳細については、「アプリケーション プロトコル インスペクションを使用するタイミング」（P.24-2）を参照してください。

（注） 変換の実施中、リモート ホストから、変換されたホストへの接続を開始できます（その接続がアクセス リストで許可されている場合）。実際のポート アドレスおよびマッピング ポート アドレスはどちらも予測不可能であるため、ホストへの接続は確立されません。ただし、この場合は、アクセス リストのセキュリティに依存できます。ただし、ポリシー PAT では時間ベースの ACL をサポートしていません。

スタティック NAT

スタティック NAT では、実アドレスからマッピング先のアドレスへの固定変換が作成されます。ダイナミック NAT および PAT では、各ホストは、後続の変換ごとに異なるアドレスまたはポートを使用します。スタティック NAT では、マッピング アドレスは連続する各接続で同じであり、永続的な変換規則が存在するため、宛先ネットワークのホストは変換済みのホストへのトラフィックを開始できます(そのトラフィックを許可するアクセス リストがある場合)。

ダイナミック NAT とスタティック NAT のアドレス範囲との主な違いは、スタティック NAT ではリモート ホストが変換済みのホストへの接続を開始でき（それを許可するアクセス リストがある場合)、ダイナミック NAT では開始できないという点です。また、スタティック NAT では、実アドレスと同じ数のマッピング先のアドレスが必要です。

スタティック PAT

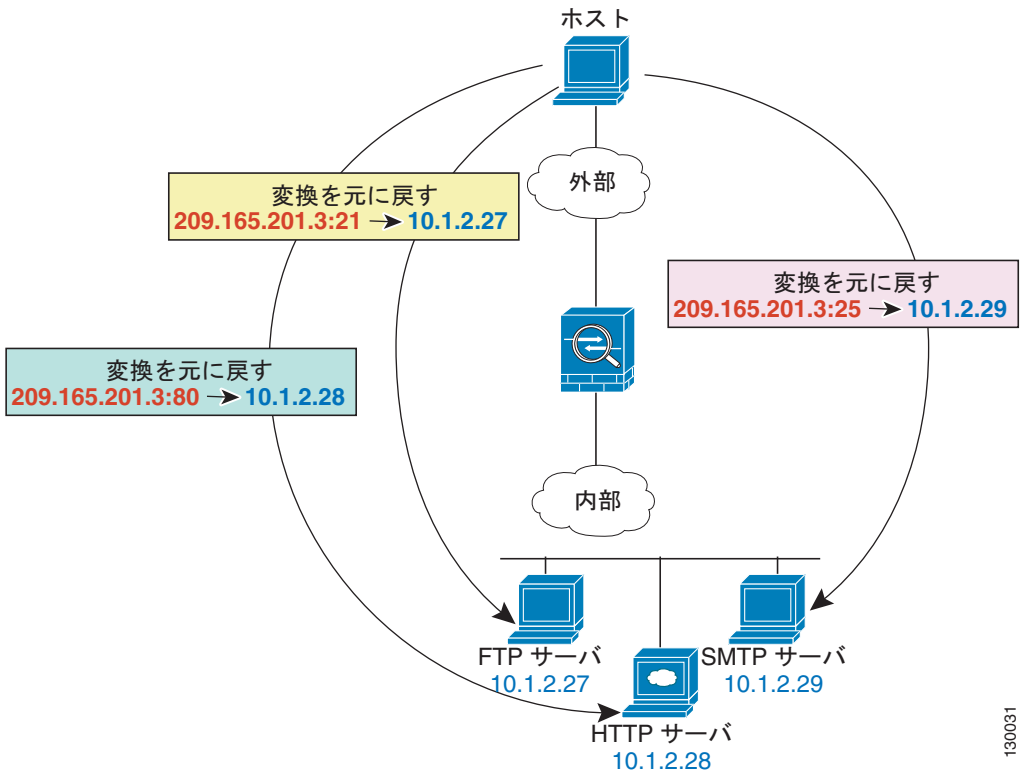
スタティック PAT は、プロトコル（TCP または UDP）および実際のアドレスとマッピング アドレスのポートを指定できる点を除いて、スタティック NAT と同じです。

この機能により、各文のポートが別個である限り、多数の異なるスタティック文にわたって同じマッピング アドレスを指定できます。複数のスタティック NAT 文に対しては、同じマッピング アドレスを使用できません。

セカンダリ チャネルの検査が必要なアプリケーション（FTP、VoIP など）を使用する場合は、セキュリティ アプライアンスが自動的にセカンダリ ポートを変換します。

たとえば、FTP、HTTP、および SMTP にアクセスする複数のリモート ユーザに単一アドレスを提供し、実際にはそれぞれが実ネットワーク上の別々のサーバである場合、マップ IP アドレスは同じでもポートが異なる各サーバに対し、スタティック PAT ステートメントを指定できます（図 25-8 を参照）。

図 25-8　スタティック PAT



スタティック PAT を使用して、well-known ポートを非標準ポートに、またはその逆に変換することもできます。たとえば、内部 Web サーバがポート 8080 を使用する場合、ポート 80 に接続することを外部ユーザに許可し、その後、変換を元のポート 8080 に戻すことができます。同様に、セキュリティをさらに高めるには、Web ユーザに標準以外のポート 6785 に接続するように指示し、その後、変換をポート 80 に戻すことができます。

NAT 制御がイネーブルな状態での NAT のバイパス

NAT コントロールをイネーブルにした場合、内部ホストは、外部ホストにアクセスするときに NAT ルールに一致する必要があります。一部のホストに対して NAT が実行されないようにするには、ホストに対する NAT をバイパスするか、NAT 制御をディセーブルにします。NAT をサポートしないアプリケーションを使用している場合などには、NAT をバイパスすることを推奨します。NAT をサポートしないインスペクション エンジンについては、「アプリケーション プロトコル インスペクションを使用するタイミング」（P.24-2）を参照してください。

3 通りの方法で、NAT をバイパスするようにトラフィックを設定できます。どの方法でも、インスペクション エンジンとの互換性が確保されます。ただし、機能は少しずつ異なります。

- アイデンティティ NAT：アイデンティティ NAT（ダイナミック NAT と類似）を設定するときは、変換を特定のインターフェイス上のホストに限定しません。つまり、アイデンティティ NAT は、すべてのインターフェイスを通過する接続に対して使用する必要があります。このため、インターフェイス A にアクセスするときには実アドレスに対して通常の変換の実行を選択できませんが、インターフェイス B にアクセスするときにはアイデンティティ NAT を使用できます。一方、通常

のダイナミック NAT では、アドレス変換を実施する特定のインターフェイスを指定できます。アイデンティティ NAT を使用する実アドレスが、アクセス リストに従って使用できるすべてのネットワークでルーティング可能であることを確認します。

アイデンティティ NAT の場合、マッピング先のアドレスは実アドレスと同じですが、外部から内部への接続を（インターフェイスのアクセス リストで許可されていても）開始できません。この機能には、スタティックなアイデンティティ NAT または NAT 免除を使用してください。

- スタティック アイデンティティ NAT：スタティック アイデンティティ NAT では、インターフェイスを指定して実際のアドレスを見えるようにするかどうかを許可できるため、インターフェイス A にアクセスするときにアイデンティティ NAT を使用し、インターフェイス B にアクセスするときに標準の変換を使用できます。スタティック アイデンティティ NAT では、ポリシー NAT も使用できます。この場合、変換する実アドレスを決定するときに、実アドレスと宛先アドレスを指定します（ポリシー NAT の詳細については、「ポリシー NAT」（P.25-11）を参照してください）。たとえば、内部アドレスから外部インターフェイスにアクセスし、宛先がサーバ A の場合に、内部アドレスにスタティック アイデンティティ NAT を使用し、外部サーバ B にアクセスするときには標準変換を使用するといったことが可能です。
- NAT 免除：NAT 免除では、変換済みのホストとリモート ホストの両方が接続を開始できます。アイデンティティ NAT と同様に、特定のインターフェイスでホストの変換を制限するのではなく、すべてのインターフェイスを経由する接続に NAT 免除を使用する必要があります。ただし、NAT 免除では、変換する実アドレスを判別するときに実アドレスおよび宛先アドレスを指定できるため（ポリシー NAT に似ています）、NAT 免除を使用する方が制御の柔軟性が増します。その反面、ポリシー NAT と異なり、NAT 免除ではアクセス リストのポートが考慮されません。NAT 免除では、最大 TCP 接続数など、接続制限の設定もできません。

ポリシー NAT

ポリシー NAT を使用すると、送信元アドレスおよび宛先アドレスを指定することにより、アドレス変換対象の実際のアドレスを指定できます。任意で送信元ポートおよび宛先ポートを指定することもできます。標準 NAT では送信元アドレスだけが考慮され、宛先は考慮されません。たとえば、ポリシー NAT を使用した場合、サーバ A にアクセスするときには実アドレスをマップ アドレス A に変換しますが、サーバ B にアクセスするときには実アドレスをマップ アドレス B に変換します。

セカンダリ チャネルのアプリケーション インスペクションを必要とするアプリケーション（FTP、VoIP など）では、ポリシー NAT ルールで指定されたポリシーにセカンダリ ポートが含まれている必要があります。ポートを予測できない場合、ポリシーはセカンダリ チャネルの IP アドレスだけを指定する必要があります。このコンフィギュレーションを使用して、セキュリティ アプライアンスはセカンダリ ポートを変換します。

図 25-9 に、2 台の異なるサーバにアクセスしている 10.1.2.0/24 ネットワークのホストを示します。ホストがサーバ 209.165.201.11 にアクセスすると、実際のアドレスは 209.165.202.129 に変換されます。ホストがサーバ 209.165.200.225 にアクセスすると、実際のアドレスは 209.165.202.130 に変換されます。その結果、ホストはサーバと同じネットワークにあるように見え、ルーティングに役立ちます。

図 25-9　異なる宛先アドレスを使用するポリシー NAT

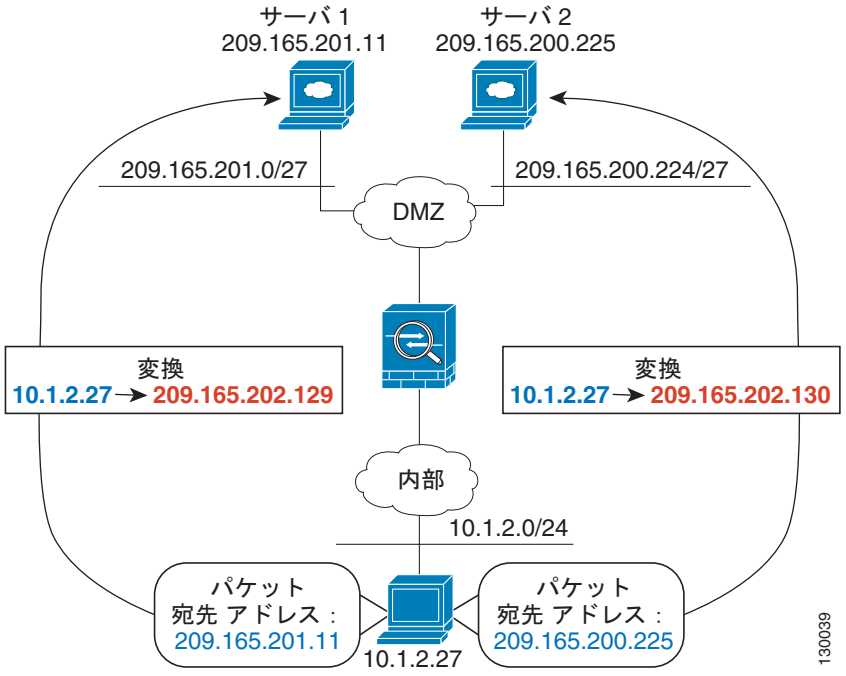
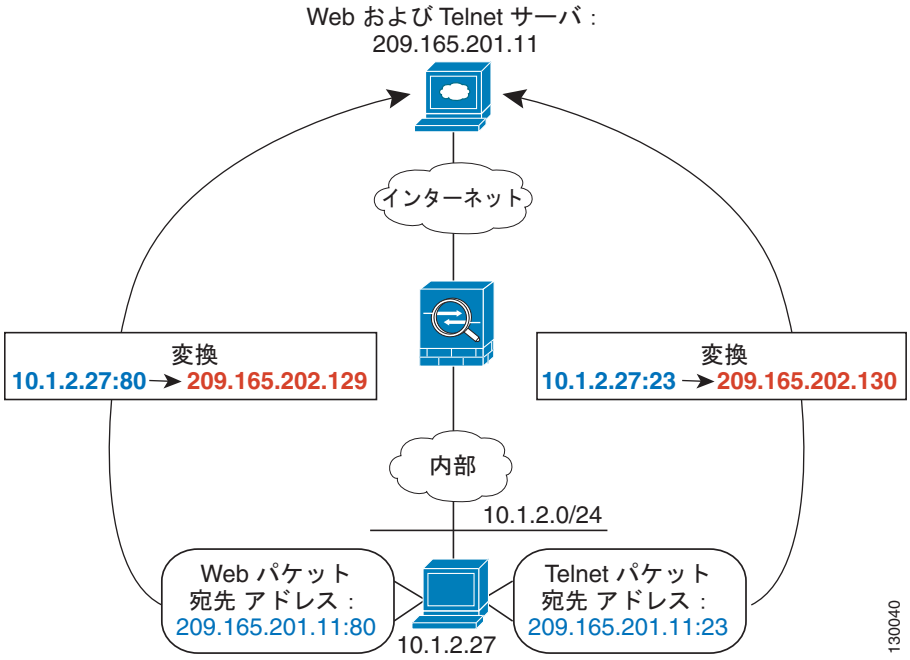


図 25-10 に、送信元ポートおよび宛先ポートの使用例を示します。10.1.2.0/24 ネットワークのホストは Web サービスと Telnet サービスの両方を提供する 1 つのホストにアクセスします。ホストが Web サービスを求めてサーバにアクセスすると、実際のアドレスは 209.165.202.129 に変換されます。ホストが Telnet サービスを求めて同じサーバにアクセスすると、実際のアドレスは 209.165.202.130 に変換されます。

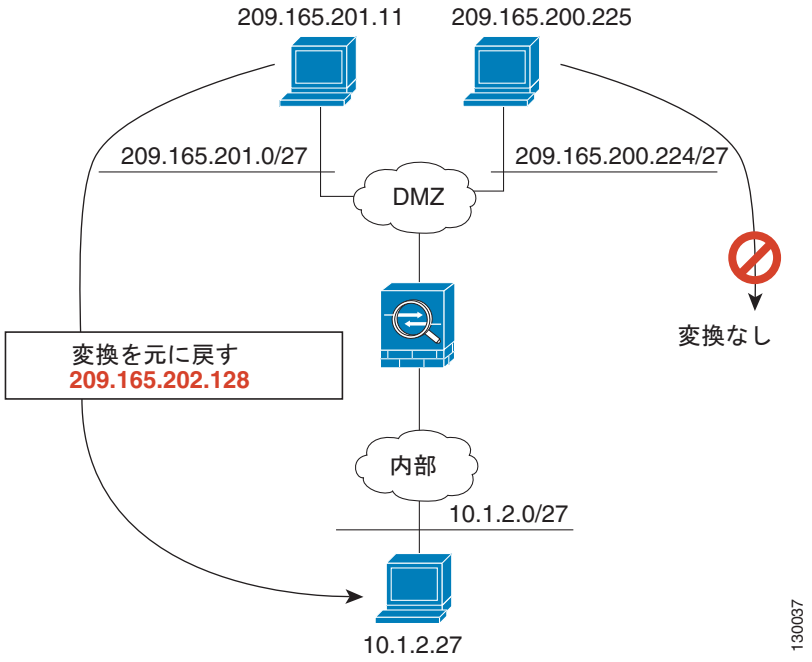
図 25-10　異なる宛先ポートを使用するポリシー NAT



ポリシー スタティック NAT では、変換済みのホストとリモート ホストの両方がトラフィックを発信できます。変換済みのネットワークで発信されたトラフィックについては、NAT ルールで実際のアドレスと*宛先*アドレスが指定されますが、リモート ネットワークで発信されたトラフィックについては、この変換を使用してホストに接続することを許可されているリモート ホストの実際のアドレスと*送信元*アドレスがルールで指定されます。

図 25-11 に、変換済みのホストに接続するリモート ホストを示します。変換対象ホストには、ネットワーク 209.165.201.0/27 との双方向のトラフィックだけに対し実アドレスを変換する、ポリシー スタティック NAT 変換が設定されています。209.165.200.224/27 ネットワーク用の変換は存在しません。したがって、変換済みのホストはそのネットワークに接続できず、そのネットワークのホストも変換済みのホストに接続できません。

図 25-11　宛先アドレス変換を行うポリシー スタティック NAT



（注）　ポリシー NAT は SQL*Net をサポートしませんが、標準 NAT は SQL*Net をサポートします。他のプロトコルの NAT サポートについては、「アプリケーション プロトコル インスペクションを使用するタイミング」（P.24-2）を参照してください。

NAT および同じセキュリティ レベルのインターフェイス

セキュリティ レベルが同じインターフェイス間では、NAT コントロールをイネーブルにした場合でも、NAT は必要ありません。必要に応じて任意で NAT を設定できます。ただし、NAT 制御がイネーブルになっている場合にダイナミック NAT を設定するときは、NAT が必要です。詳細については、「NAT コントロール」（P.25-5）を参照してください。また、同一セキュリティ レベルのインターフェイス上でダイナミック NAT または PAT に対して IP アドレス グループを指定する場合、そのアドレス グループが下位または同一セキュリティ レベルのインターフェイスにアクセスするときには、アドレス グループに対して NAT を実行する必要があります（NAT 制御がイネーブルでない場合でも）。スタティック NAT として識別されたトラフィックは影響を受けません。

（注）　同一セキュリティ レベルのインターフェイス上に NAT を設定した場合、セキュリティ アプライアンスは VoIP インスペクション エンジンをサポートしません。これらのインスペクション エンジンには、Skinny、SIP、および H.323 が含まれます。サポートされるインスペクション エンジンについては、「アプリケーション プロトコル インスペクションを使用するタイミング」（P.24-2）を参照してください。

実際のアドレスとの照合に使用される NAT ルールの順序

セキュリティ アプライアンスは、次の順序で実際のアドレスを NAT ルールと照合します。

1. NAT 免除：順序に従って、最初の一致が見つかるまで続行されます。
2. スタティック NAT とスタティック PAT（標準およびポリシー）：順序に従って、最初の一致が見つかるまで続行されます。スタティック アイデンティティ NAT はこのカテゴリに含まれません。
3. ポリシー ダイナミック NAT：順序に従って、最初の一致が見つかるまで続行されます。アドレスの重複は可能です。
4. 標準のダイナミック NAT：最も適合する一致を見つけます。標準アイデンティティ NAT はこのカテゴリに含まれます。NAT ルールの順序は関係なく、実際のアドレスと最も適合する NAT ルールが使用されます。たとえば、インターフェイス上のすべてのアドレス（0.0.0.0）を変換する汎用文を作成できます。ネットワークのサブネット（10.1.1.1）を別のアドレスに変換する場合は、10.1.1.1 だけを変換する文を作成できます。10.1.1.1 が接続を開始すると、10.1.1.1 用の特定のルールが使用されます。これは、それが実際のアドレスに最も適合するからです。重複するルールを使用することはお勧めしません。重複するルールにより、使用メモリが増え、セキュリティ アプライアンスのパフォーマンスが低下する可能性があります。

マッピング アドレスの注意事項

実際のアドレスをマッピング アドレスに変換するときは、次のマッピング アドレスを使用できます。

- マッピング インターフェイスと同じネットワーク上のアドレス

  （セキュリティ アプライアンス から出ていくトラフィックが通過する）マッピング インターフェイスと同じネットワーク上のアドレスを使用した場合、セキュリティ アプライアンス はプロキシ ARP を使用してマッピング アドレスの要求に応答することによって、実アドレス宛てのトラフィックを代行受信します。この方法では、セキュリティ アプライアンス がその他のネットワークのゲートウェイである必要がないため、ルーティングが簡略化されます。ただし、この方法では、変換に使用できるアドレス数に限度があります。

  PAT では、マッピング インターフェイスの IP アドレスも使用できます。

- 固有のネットワーク上のアドレス

  マッピング インターフェイスで使用可能なアドレスより多くのアドレスが必要な場合は、別のサブネット上のアドレスを指定できます。セキュリティ アプライアンス は、プロキシ ARP を使用してマッピング アドレス要求に応答することによって、実アドレス宛てのトラフィックを代行受信します。OSPF を使用し、マッピング インターフェイス上でルートをアドバタイズする場合、セキュリティ アプライアンス はマッピング アドレスをアドバタイズします。マッピング インターフェイスがパッシブの場合（ルートをアドバタイズしない）、またはスタティック ルーティングを使用する場合は、マッピング アドレス宛てのトラフィックを セキュリティ アプライアンス に送信するアップストリーム ルータ上でスタティック ルートを追加する必要があります。

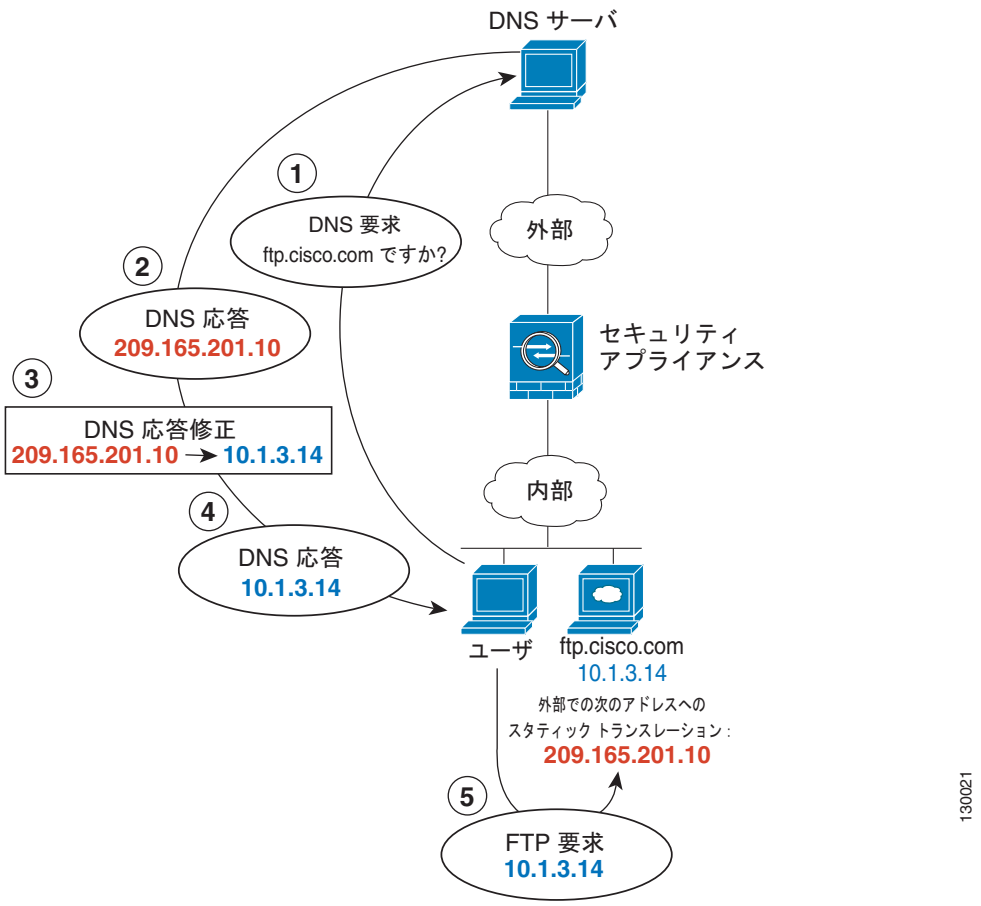
DNS および NAT

応答内のアドレスを NAT コンフィギュレーションと一致するアドレスに置き換えて、DNS 応答を修正するようにセキュリティ アプライアンスを設定することが必要になる場合があります。DNS 修正は、各変換を設定するときに設定できます。

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、セキュリティ アプライアンスを設定します（図 25-12 を参照）。この場合、このスタティック文で 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。セキュリティ アプライアンス は内部サーバのスタティック ステートメントを参照し、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。

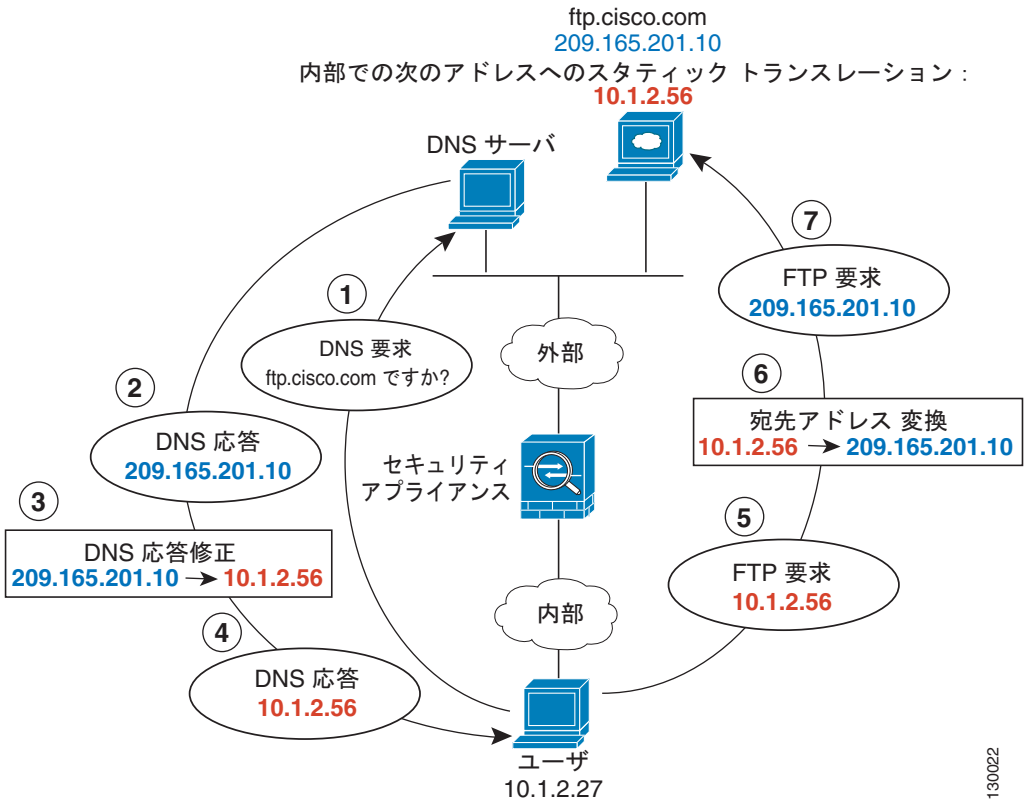
図 25-12　DNS 応答修正



（注）　他のネットワーク（DMZ など）のユーザも外部 DNS サーバから ftp.cisco.com の IP アドレスを要求している場合、そのユーザがスタティック規則で参照される内部インターフェイスに存在しない場合でも、そのユーザに対して DNS 応答の IP アドレスも修正されます。

図 25-13 に、外部の Web サーバと DNS サーバを示します。セキュリティ アプライアンスには、外部サーバ用のスタティック変換があります。この場合、ftp.cisco.com のアドレスを DNS サーバに要求すると、DNS サーバは応答で実際のアドレス 209.165.20.10 を示します。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 25-13　外部 NAT を使用する DNS 応答修正



NAT 制御の設定

NAT 制御では、内部インターフェイスから外部インターフェイスへのパケットは NAT ルールと一致する必要があります。詳細については、「NAT コントロール」（P.25-5）を参照してください。

NAT 制御をイネーブルにするには、[Configuration] > [Firewall] > [NAT Rules] ペインで、[Enable traffic through the firewall without address translation] をオンにします。

ダイナミック NAT の使用

この項では、ダイナミック NAT および PAT、ダイナミック ポリシー NAT および PAT、アイデンティティ NAT を含む、ダイナミック NAT の設定方法について説明します。

ポリシー NAT を使用すると、送信元アドレスおよび宛先アドレスを指定することにより、アドレス変換対象の実際のアドレスを指定できます。任意で送信元ポートおよび宛先ポートを指定することもできます。標準 NAT では送信元アドレスだけが考慮され、宛先は考慮されません。詳細については、「ポリシー NAT」（P.25-11）を参照してください。

この項では、次のトピックについて取り上げます。

ダイナミック NAT の実装

この項では、ダイナミック NAT の実装方法について説明します。説明する内容は次のとおりです。

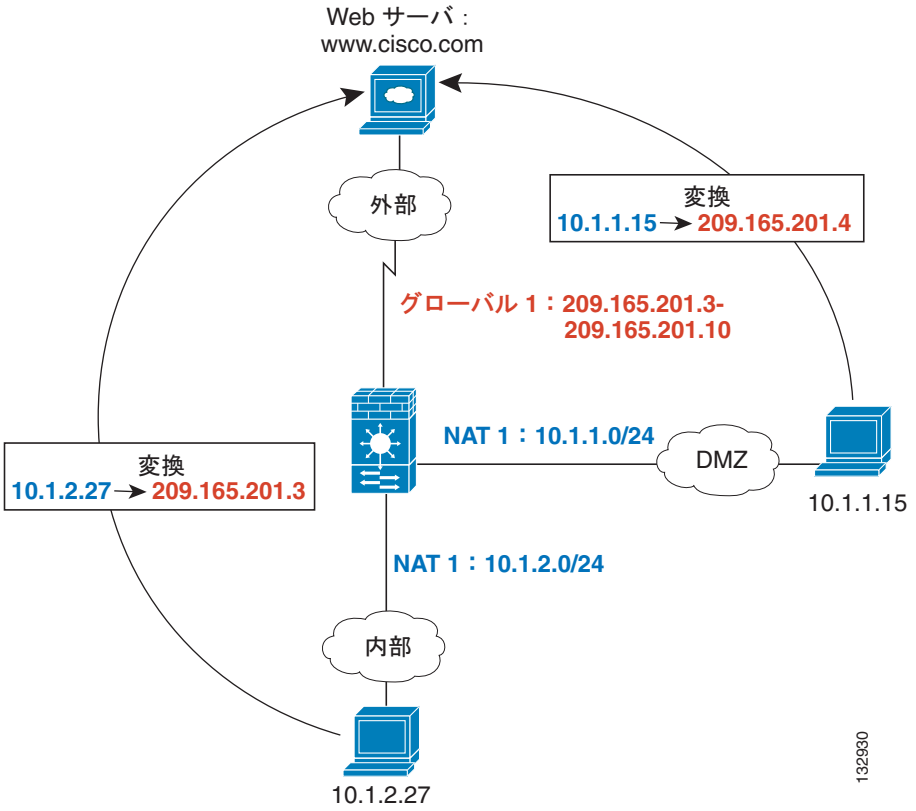
プール ID を使用した実際のアドレスとグローバル プールのペア

ダイナミック NAT ルールでは、実際のアドレスを指定し、それをアドレスのグローバル プールとペアにします。実際のアドレスは別のインターフェイスを出るときにこのグローバル プールにマッピングされます（PAT の場合、これは 1 つのアドレスになり、アイデンティティ NAT の場合は同じ実際のアドレスになります）。各グローバル プールにはプール ID が割り当てられます。

別のインターフェイス上の同じグローバル プールを使用する NAT ルール

同じグローバル アドレス プールを使用してインターフェイスごとに NAT ルールを作成できます。たとえば、内部インターフェイス用と DMZ インターフェイス用の両方に外部インターフェイス上のグローバル プール 1 を使用して NAT ルールを設定できます。内部インターフェイスと DMZ インターフェイスからのトラフィックは、外部インターフェイスを出るときに、マップ プールまたは PAT アドレスを共有します（図 25-14 を参照）。

図 25-14　複数のインターフェイス上の同じグローバル プールを使用する NAT ルール

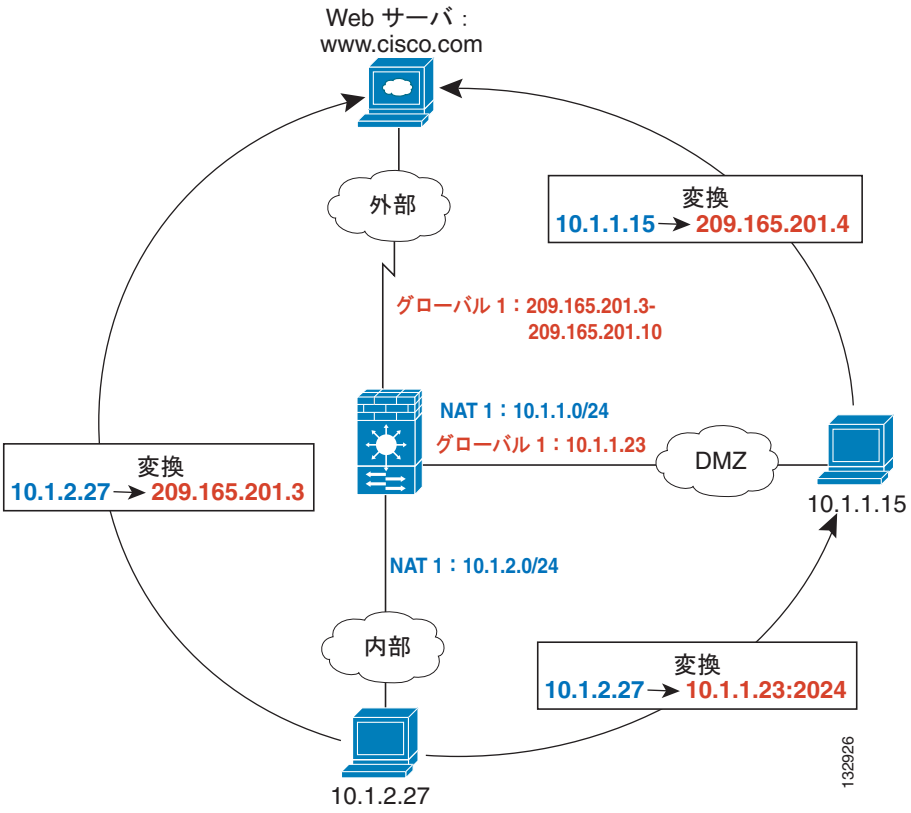


複数のインターフェイス上の同じプール ID を持つグローバル プール

同じプール ID を使用してインターフェイスごとにグローバル プールを作成できます。ID 1 で外部インターフェイスと DMZ インターフェイス用にグローバル プールを作成した場合、トラフィックが外部インターフェイスと DMZ インターフェイスの両方に向かうとき、ID 1 に関連付けられた 1 つの NAT ルールが変換対象のトラフィックを識別します。同様に、ID 1 で DMZ インターフェイス用の NAT ルールを作成した場合、ID 1 のすべてのグローバル プールもまた DMZ トラフィックに使用されます

（図 25-15 を参照）。

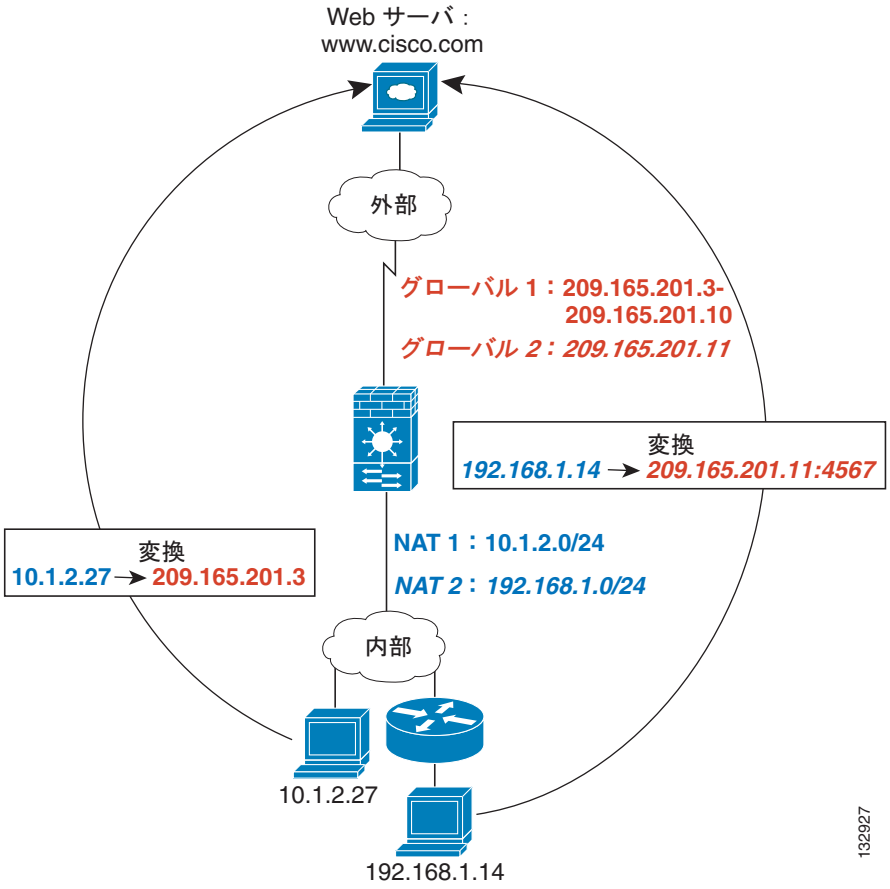
図 25-15　複数のインターフェイス上の同じ ID を使用する NAT ルールとグローバル プール



同じインターフェイス上の異なるグローバル プールを使用する複数の NAT ルール

異なる実際のアドレス セットが異なるマッピング アドレスを持つように指定できます。たとえば、内部インターフェイスに 2 つの異なるプール ID で 2 つの NAT ルールを設定できます。外部インターフェイスに、これらの 2 つの ID に対する 2 つのグローバル プールを設定します。設定後、内部ネットワーク A からのトラフィックが外部インターフェイスを出ると、IP アドレスはプール 1 のアドレスに変換され、内部ネットワーク B からのトラフィックはプール 2 のアドレスに変換されます（図 25-16 を参照）。ポリシー NAT を使用すると、宛先アドレスとポートが各アクセス リスト内で一意である限り、複数の NAT ルールに対して同じ実際のアドレスを指定できます。

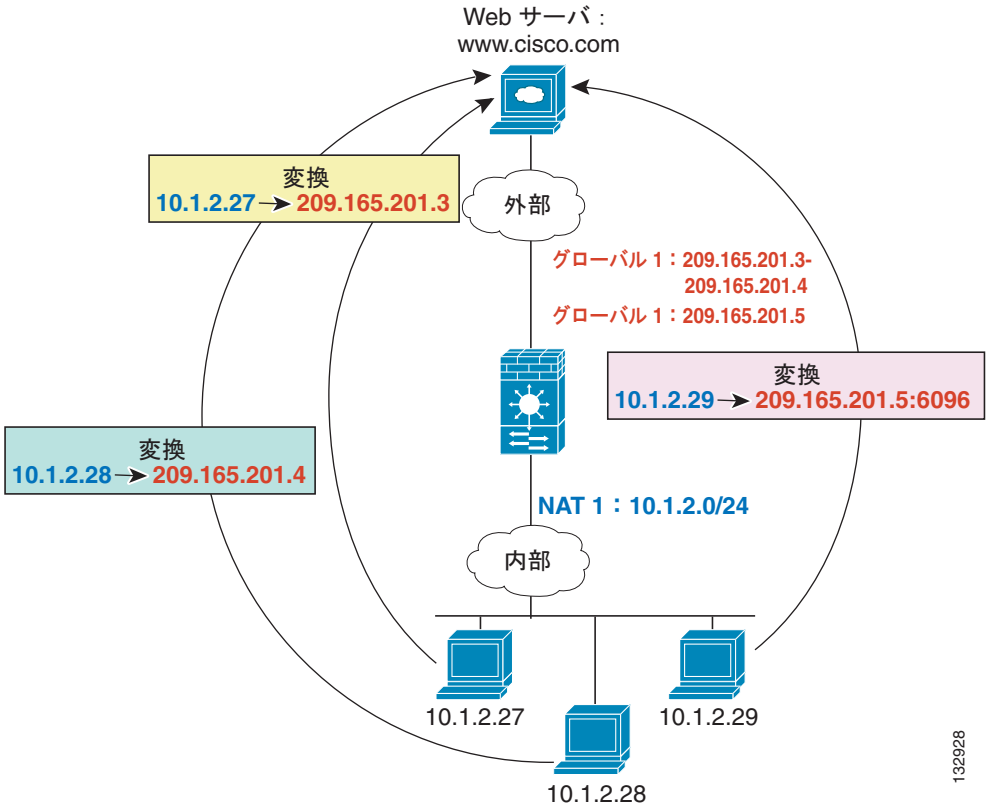
図 25-16　異なる NAT ID



同じグローバル プール内の複数のアドレス

同じグローバル プール内に複数のアドレスを持てます。セキュリティ アプライアンスは最初にダイナミック NAT のアドレス範囲をコンフィギュレーション内の順序に従って使用し、次に PAT の 1 つのアドレスを順序に従って使用します。さらに、特定のアプリケーションにはダイナミック NAT を使用し、ダイナミック NAT のアドレスをすべて使い切ったときに備えて予備の PAT ルールを用意する必要がある場合、アドレス範囲と PAT アドレスの両方を追加できます。同様に、1 つの PAT マッピング アドレスがサポートするおよそ 64,000 より多くの PAT セッションが必要な場合、プールに 2 つの PAT アドレスを持てます（図 25-17 を参照）。

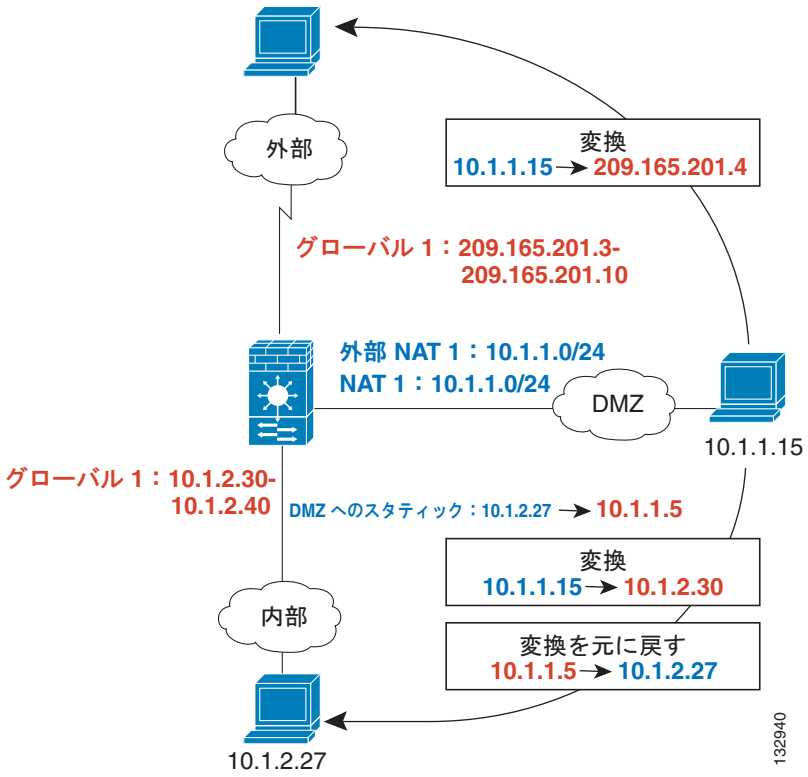
図 25-17　NAT および PAT の併用



外部 NAT

アドレスを外部インターフェイスから内部インターフェイスに変換する NAT ルールは外部 NAT ルールです。外部 NAT ルールが着信トラフィックを変換することを指定する必要があります。同じトラフィックがセキュリティの低いインターフェイスにアクセスするときも変換が必要な場合（たとえば、DMZ のトラフィックを内部および外部インターフェイスにアクセスするときに変換する場合など）、同じ NAT ID を使用して、発信を指定する 2 つ目の NAT ルールを作成できます（図 25-18 を参照）。外部 NAT（DMZ インターフェイスから内部インターフェイス）の場合、内部ホストはスタティック ルールを使用して外部アクセスを許可するので、送信元アドレスと宛先アドレスの両方が変換されます。

図 25-18　外部 NAT および内部 NAT の組み合わせ



NAT ルール内の実際のアドレスは同位または低位のセキュリティ レベルのインターフェイスすべてで変換が必要

IP アドレス グループに対する NAT ルールを作成した場合、そのグループが同位か低位のセキュリティ レベルのインターフェイスにアクセスするときに NAT を実行する必要があります。また、各インターフェイスに同じプール ID を持つグローバル プールを作成するか、スタティック ルールを使用する必要があります。グループが高位のセキュリティ インターフェイスにアクセスするときには、NAT は必要ありません。外部 NAT ルールを作成した場合、上記の NAT 要件は、そのアドレス グループが高位のセキュリティ インターフェイスにアクセスするときは常に適用されます。スタティック ルールで指定されたトラフィックは影響を受けません。

グローバル プールの管理

ダイナミック NAT は変換にグローバル プールを使用します。グローバル プールの動作については、「ダイナミック NAT の実装」（P.25-18）を参照してください。

グローバル プールを管理するには、次の手順を実行します。

ステップ 1　[Configuration] > [Firewall] > [Objects] > [Global Pools] ペインで、[Add] をクリックして新しいプールを追加するか、プールを選択して [Edit] をクリックします。

[Add/Edit Dynamic NAT Rule] ダイアログボックスで [Manage] ボタンをクリックしてもグローバル プールを管理できます。

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

ステップ 2　新しいプールの場合、[Interface] ドロップダウン リストから、マッピング IP アドレスを使用するインターフェイスを選択します。

ステップ 3　新しいプールの場合、[Pool ID] フィールドに 1 ～ 2147483647 の範囲の数値を入力します。すでに使用されているプール ID は入力しないでください。すでに使用されている場合、設定は拒否されます。

ステップ 4　[IP Addresses to Add] 領域で、[Range]、[Port Address Translation (PAT)]、または [PAT Address Translation (PAT) Using IP Address of the interface] をクリックします。

アドレスの範囲を指定すると、セキュリティ アプライアンスはダイナミック NAT を実行します。[Netmask] フィールドにサブネット マスクを指定すると、その値がマッピング アドレスがホストに割り当てられるときに使用されるサブネット マスクになります。マスクを指定しない場合は、アドレス クラスのデフォルト マスクが使用されます。

ステップ 5　[Addresses Pool] ウィンドウにアドレスを追加するには、[Add] をクリックします。

ステップ 6　（任意）グローバル プールには複数のアドレスを追加できます。たとえば、ダイナミック範囲を設定した後に PAT アドレスを追加する場合、PAT アドレスの値を入力して再度 [Add] をクリックします。1 つのインターフェイスに同じプール ID で複数のアドレスを使用する方法については、「同じグローバル プール内の複数のアドレス」（P.25-21）を参照してください。

ステップ 7　[OK] をクリックします。

ダイナミック NAT、ダイナミック PAT、またはダイナミック アイデンティティ NAT の設定

ダイナミック NAT、ダイナミック PAT、またはダイナミック アイデンティティ NAT のルールを設定するには、次の手順を実行します。

ステップ 1　[Configuration] > [Firewall] > [NAT Rules] ペインで、[Add] > [Add Dynamic NAT Rule] を選択します。

[Add Dynamic NAT Rule] ダイアログボックスが表示されます。

ステップ 2　[Original] 領域で、[Interface] ドロップダウン リストから、変換対象の実際のアドレスを持つホストに接続するインターフェイスを選択します。

ステップ 3　[Source] フィールドに実際のアドレスを入力します。または [...] ボタンをクリックして、ASDM ですでに定義されている IP アドレスを選択します。

プレフィックス / 長さ表記（10.1.1.0/24 など）を使用してアドレスとサブネット マスクを指定します。マスクを使用せずに IP アドレスを入力すると、そのアドレスは最後が 0 であってもホスト アドレスと見なされます。

ステップ 4　グローバル プールを選択するには、次のいずれかのオプションを使用します。

- すでに定義されているグローバル プールを選択する。

  プールにアドレス範囲が含まれている場合、セキュリティ アプライアンスはダイナミック NAT を実行します。プールに含まれるアドレスが 1 つだけの場合、セキュリティ アプライアンスはダイナミック PAT を実行します。プールにアドレス範囲と単一アドレスの両方が含まれている場合、範囲が順序に従って使用され、続いて PAT アドレスが順序に従って使用されます。詳細については、「同じグローバル プール内の複数のアドレス」（P.25-21）を参照してください。

プールはプール ID で識別されます。異なるインターフェイスにある複数のグローバル プールが同じプール ID を共有する場合、それらのプールはグループとなります。複数のインターフェイスを持つプール ID を選択すると、トラフィックはプールのいずれかのインターフェイスにアクセスしたときに指定どおりに変換されます。プール ID の詳細については、「ダイナミック NAT の実装」（P.25-18）を参照してください。

- [Manage] をクリックして新しいグローバル プールを作成するか既存のプールを編集する。「グローバル プールの管理」（P.25-23）を参照してください。
- [global pool 0] を選択してアイデンティティ NAT を選択する。

ステップ 5　（任意）DNS 応答内部のアドレスの変換をイネーブルにするには、[Connection Settings] 領域をクリックして開き、[Translate the DNS replies that match the translation rule] をオンにします。

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おり、その DNS サーバがクライアントと異なるインターフェイス上にある場合、クライアントと DNS サーバではホストのアドレスが異なっている必要があります。一方にはマッピング アドレスが、もう一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。マッピングされるホストは、クライアントまたは DNS サーバのいずれかと同じインターフェイス上にある必要があります。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。詳細については、「DNS および NAT」（P.25-16）を参照してください。

ステップ 6　（任意）接続設定をイネーブルにするには、[Connection Settings] 領域をクリックして開き、次のオプションを 1 つ以上設定します。

（注）　これらの値は、セキュリティ ポリシー ルールを使用しても設定できます（「接続の設定」（P.27-6）を参照）。これらのオプションを両方に設定した場合、セキュリティ アプライアンスは低い方の制限値を使用します。TCP シーケンスのランダム化がいずれかの方法を使用してディセーブルになっている場合、セキュリティ アプライアンスは TCP シーケンスのランダム化をディセーブルにします。

- [Randomize sequence number]：このチェックボックスをオンにすると（デフォルト）、セキュリティ アプライアンスは TCP パケットのシーケンス番号をランダム化します。それぞれの TCP 接続には 2 つの ISN が割り当てられており、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、着信と発信の両方向で通過する TCP SNY の ISN をランダム化します。

  保護されたホストの ISN をランダム化することにより、攻撃者が新しい接続で次の ISN を予測できないようにして、新規セッションが乗っ取られるのを防ぎます。

  TCP 初期シーケンス番号のランダム化は、必要に応じてディセーブルにできます。次に例を示します。

  - 別の直列接続されたファイアウォールでも初期シーケンス番号がランダム化され、トラフィックに影響することはないものの、両方のファイアウォールでこの動作を実行する必要がない場合。
  - セキュリティ アプライアンスで eBGP マルチホップを使用しており、eBGP ピアで 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 アプライアンスで接続のシーケンスをランダム化しないようにする必要がある WAAS デバイスを使用する場合。
- [Maximum TCP Connections]：TCP の最大接続数を 0 ～ 65,535 の範囲で指定します。この値を 0 に設定すると、接続数は無制限になります。
- [Maximum UDP Connections]：UDP の最大接続数を 0 ～ 65,535 の範囲で指定します。この値を 0 に設定すると、接続数は無制限になります。

- [Maximum Embryonic Connections]：初期接続の最大数を 65,536 までの範囲で指定します。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。この制限により、TCP 代行受信機能がイネーブルになります。デフォルトは **0** で、最大初期接続数であることを示します。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。

ステップ 7　[OK] をクリックします。

ダイナミック ポリシー NAT またはダイナミック ポリシー PAT の設定

ダイナミック ポリシー NAT またはダイナミック ポリシー PAT を設定するには、次の手順を実行します。

ステップ 1　[Configuration] > [Firewall] > [NAT Rules] ペインで、[Add] > [Advanced] > [Add Dynamic Policy NAT Rule] を選択します。

[Add Dynamic Policy NAT Rule] ダイアログボックスが開きます。

ステップ 2　[Original] 領域で、[Interface] ドロップダウン リストから、変換対象の実際のアドレスを持つホストに接続するインターフェイスを選択します。

ステップ 3　[Source] フィールドに実際のアドレスを入力します。または [...] ボタンをクリックして、ASDM ですでに定義されている IP アドレスを選択します。

プレフィックス / 長さ表記（10.1.1.0/24 など）を使用してアドレスとサブネット マスクを指定します。マスクを使用せずに IP アドレスを入力すると、そのアドレスは最後が 0 であってもホスト アドレスと見なされます。

実際のアドレスが複数ある場合はカンマで区切ります。

ステップ 4　[Destination] フィールドに宛先アドレスを入力します。または [...] ボタンをクリックして、ASDM ですでに定義されている IP アドレスを選択します。

プレフィックス / 長さ表記（10.1.1.0/24 など）を使用してアドレスとサブネット マスクを指定します。マスクを使用せずに IP アドレスを入力すると、そのアドレスは最後が 0 であってもホスト アドレスと見なされます。

宛先アドレスが複数ある場合はカンマで区切ります。

デフォルトでは、フィールドには任意の宛先アドレスを許可する **any** が表示されています。

ステップ 5　グローバル プールを選択するには、次のいずれかのオプションを使用します。

- すでに定義されているグローバル プールを選択する。

  プールにアドレス範囲が含まれている場合、セキュリティ アプライアンスはダイナミック NAT を実行します。プールに含まれるアドレスが 1 つだけの場合、セキュリティ アプライアンスはダイナミック PAT を実行します。プールにアドレス範囲と単一アドレスの両方が含まれている場合、範囲が順序に従って使用され、続いて PAT アドレスが順序に従って使用されます。詳細については、「同じグローバル プール内の複数のアドレス」（P.25-21）を参照してください。

  プールはプール ID で識別されます。異なるインターフェイスにある複数のグローバル プールが同じプール ID を共有する場合、それらのプールはグループとなります。複数のインターフェイスを持つプール ID を選択すると、トラフィックはプールのいずれかのインターフェイスにアクセスし

たときに指定どおりに変換されます。プール ID の詳細については、「ダイナミック NAT の実装」（P.25-18）を参照してください。

- [Manage] をクリックして新しいグローバル プールを作成するか既存のプールを編集する。「グローバル プールの管理」（P.25-23）を参照してください。
- [global pool 0] を選択してアイデンティティ NAT を選択する。

ステップ 6　（任意）[Description] フィールドに説明を入力します。

ステップ 7　（任意）DNS 応答内部のアドレスの変換をイネーブルにするには、[Connection Settings] 領域をクリックして開き、[Translate the DNS replies that match the translation rule] をオンにします。

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おり、その DNS サーバがクライアントと異なるインターフェイス上にある場合、クライアントと DNS サーバではホストのアドレスが異なっている必要があります。一方にはマッピング アドレスが、もう一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。マッピングされるホストは、クライアントまたは DNS サーバのいずれかと同じインターフェイス上にある必要があります。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。詳細については、「DNS および NAT」（P.25-16）を参照してください。

ステップ 8　（任意）接続設定をイネーブルにするには、[Connection Settings] 領域をクリックして開き、次のオプションを 1 つ以上設定します。

（注）　これらの値は、セキュリティ ポリシー ルールを使用しても設定できます（「接続の設定」（P.27-6）を参照）。これらのオプションを両方に設定した場合、セキュリティ アプライアンスは低い方の制限値を使用します。TCP シーケンスのランダム化がいずれかの方法を使用してディセーブルになっている場合、セキュリティ アプライアンスは TCP シーケンスのランダム化をディセーブルにします。

- [Randomize sequence number]：このチェックボックスをオンにすると（デフォルト）、セキュリティ アプライアンスは TCP パケットのシーケンス番号をランダム化します。それぞれの TCP 接続には 2 つの ISN が割り当てられており、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、着信と発信の両方向で通過する TCP SNY の ISN をランダム化します。

  保護されたホストの ISN をランダム化することにより、攻撃者が新しい接続で次の ISN を予測できないようにして、新規セッションが乗っ取られるのを防ぎます。

  TCP 初期シーケンス番号のランダム化は、必要に応じてディセーブルにできます。次に例を示します。

  - 別の直列接続されたファイアウォールでも初期シーケンス番号がランダム化され、トラフィックに影響することはないものの、両方のファイアウォールでこの動作を実行する必要がない場合。
  - セキュリティ アプライアンスで eBGP マルチホップを使用しており、eBGP ピアで 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 アプライアンスで接続のシーケンスをランダム化しないようにする必要がある WAAS デバイスを使用する場合。
- [Maximum TCP Connections]：TCP の最大接続数を 0 ～ 65,535 の範囲で指定します。この値を 0 に設定すると、接続数は無制限になります。
- [Maximum UDP Connections]：UDP の最大接続数を 0 ～ 65,535 の範囲で指定します。この値を 0 に設定すると、接続数は無制限になります。

- [Maximum Embryonic Connections]：初期接続の最大数を 65,536 までの範囲で指定します。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。この制限により、TCP 代行受信機能がイネーブルになります。デフォルトは **0** で、最大初期接続数であることを示します。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。

ステップ 9　[OK] をクリックします。

スタティック NAT の使用

この項では、標準またはポリシー スタティック NAT、PAT、またはアイデンティティ NAT を使用してスタティック変換を設定する方法について説明します。

スタティック NAT の詳細については、「スタティック NAT」（P.25-9）を参照してください。

ポリシー NAT を使用すると、送信元アドレスおよび宛先アドレスを指定することにより、アドレス変換対象の実際のアドレスを指定できます。任意で送信元ポートおよび宛先ポートを指定することもできます。標準 NAT では送信元アドレスだけが考慮され、宛先は考慮されません。詳細については、「ポリシー NAT」（P.25-11）を参照してください。

スタティック PAT を使用すると、実 IP アドレスをマップ IP アドレスに変換し、さらに実ポートをマップ ポートに変換できます。同じポートを変換する場合は、特定のトラフィック タイプを変換できます。または、別のポートに変換することによってさらに細かく制御することもできます。セカンダリ チャネルのアプリケーション インスペクションが必要なアプリケーション（FTP、VoIP など）を使用する場合は、セキュリティ アプライアンスが自動的にセカンダリ ポートを変換します。スタティック PAT の詳細については、「スタティック PAT」（P.25-9）を参照してください。

同じ 2 つのインターフェイス間で複数のスタティック ルールに同じ実際のアドレスまたはマッピング アドレスを使用するには、スタティック PAT を使用する必要があります。同じマッピング インターフェイスのグローバル プールにも定義されているマッピング アドレスをスタティック ルールに使用しないでください。

スタティック アイデンティティ NAT では、実際の IP アドレスが同じ IP アドレスに変換されます。

この項では、次のトピックについて取り上げます。

- 「スタティック NAT、スタティック PAT、またはスタティック アイデンティティ NAT の設定」（P.25-28）
- 「スタティック ポリシー NAT、スタティック ポリシー PAT、またはスタティック ポリシー アイデンティティ NAT の設定」（P.25-30）

スタティック NAT、スタティック PAT、またはスタティック アイデンティティ NAT の設定

スタティック NAT、スタティック PAT、またはスタティック アイデンティティ NAT を設定するには、次の手順を実行します。

ステップ 1　[Configuration] > [Firewall] > [NAT Rules] ペインで、[Add] > [Add Static NAT Rule] を選択します。

[Add Static NAT Rule] ダイアログボックスが表示されます。

ステップ 2　[Original] 領域で、[Interface] ドロップダウン リストから、変換対象の実際のアドレスを持つホストに接続するインターフェイスを選択します。

ステップ 3　[Source] フィールドに実際のアドレスを入力します。または [...] ボタンをクリックして、ASDM ですでに定義されている IP アドレスを選択します。

プレフィックス / 長さ表記（10.1.1.0/24 など）を使用してアドレスとサブネット マスクを指定します。マスクを使用せずに IP アドレスを入力すると、そのアドレスは最後が 0 であってもホスト アドレスと見なされます。

ステップ 4　[Translated] 領域で、[Interface] ドロップダウン リストから、マッピング アドレスを使用するインターフェイスを選択します。

ステップ 5　マッピング IP アドレスを指定するには、次のいずれかをクリックします。

- **Use IP Address**

  IP アドレスを入力するか、[...] ボタンをクリックして ASDM ですでに定義されている IP アドレスを選択します。

  プレフィックス / 長さ表記（10.1.1.0/24 など）を使用してアドレスとサブネット マスクを指定します。マスクを使用せずに IP アドレスを入力すると、そのアドレスは最後が 0 であってもホスト アドレスと見なされます。

- **Use Interface IP Address**

実際のアドレスとマッピング アドレスのサブネット マスクは同じである必要があります。

（注）　アイデンティティ NAT の場合、[Original] フィールドと [Translated] フィールドに同じ IP アドレスを入力します。

ステップ 6　（任意）スタティック PAT を使用するには、[Enable Port Address Translation (PAT)] をオンにします。

a.　[Protocol] では、[TCP] または [UDP] をクリックします。

b.　[Original Port] フィールドで、実際のポート番号を入力します。

c.　[Translated Port] フィールドで、マッピング ポート番号を入力します。

ステップ 7　（任意）DNS 応答内部のアドレスの変換をイネーブルにするには、[Connection Settings] 領域をクリックして開き、[Translate the DNS replies that match the translation rule] をオンにします。

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おり、その DNS サーバがクライアントと異なるインターフェイス上にある場合、クライアントと DNS サーバではホストのアドレスが異なっている必要があります。一方にはマッピング アドレスが、もう一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。マッピングされるホストは、クライアントまたは DNS サーバのいずれかと同じインターフェイス上にある必要があります。詳細については、「DNS および NAT」（P.25-16）を参照してください。

ステップ 8　（任意）接続設定をイネーブルにするには、[Connection Settings] 領域をクリックして開き、次のオプションを 1 つ以上設定します。

（注）　これらの値は、セキュリティ ポリシー ルールを使用しても設定できます（「接続の設定」（P.27-6）を参照）。これらのオプションを両方に設定した場合、セキュリティ アプライアンスは低い方の制限値を使用します。TCP シーケンスのランダム化がいずれかの方法を使用してディセーブルになっている場合、セキュリティ アプライアンスは TCP シーケンスのランダム化をディセーブルにします。

- [Randomize sequence number]：このチェックボックスをオンにすると（デフォルト）、セキュリティ アプライアンスは TCP パケットのシーケンス番号をランダム化します。それぞれの TCP 接続には 2 つの ISN が割り当てられており、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、着信と発信の両方向で通過する TCP SNY の ISN をランダム化します。

  保護されたホストの ISN をランダム化することにより、攻撃者が新しい接続で次の ISN を予測できないようにして、新規セッションが乗っ取られるのを防ぎます。

  TCP 初期シーケンス番号のランダム化は、必要に応じてディセーブルにできます。次に例を示します。

  - 別の直列接続されたファイアウォールでも初期シーケンス番号がランダム化され、トラフィックに影響することはないものの、両方のファイアウォールでこの動作を実行する必要がない場合。
  - セキュリティ アプライアンスで eBGP マルチホップを使用しており、eBGP ピアで 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 アプライアンスで接続のシーケンスをランダム化しないようにする必要がある WAAS デバイスを使用する場合。
- [Maximum TCP Connections] : TCP の最大接続数を 0 ～ 65,535 の範囲で指定します。この値を 0 に設定すると、接続数は無制限になります。
- [Maximum UDP Connections] : UDP の最大接続数を 0 ～ 65,535 の範囲で指定します。この値を 0 に設定すると、接続数は無制限になります。
- [Maximum Embryonic Connections] : 初期接続の最大数を 65,536 までの範囲で指定します。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。この制限により、TCP 代行受信機能がイネーブルになります。デフォルトは **0** で、最大初期接続数であることを示します。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。

ステップ 9　[OK] をクリックします。

スタティック ポリシー NAT、スタティック ポリシー PAT、またはスタティック ポリシー アイデンティティ NAT の設定

スタティック ポリシー NAT、スタティック ポリシー PAT、またはスタティック ポリシー アイデンティティ NAT を設定するには、次の手順を実行します。

ステップ 1　[Configuration] > [Firewall] > [NAT Rules] ペインで、[Add] > [Advanced] > [Add Static Policy NAT Rule] を選択します。

[Add Static Policy NAT Rule] ダイアログボックスが表示されます。

ステップ 2　[Original] 領域で、[Interface] ドロップダウン リストから、変換対象の実際のアドレスを持つホストに接続するインターフェイスを選択します。

ステップ 3　[Source] フィールドに実際のアドレスを入力します。または [...] ボタンをクリックして、ASDM ですでに定義されている IP アドレスを選択します。

プレフィックス / 長さ表記（10.1.1.0/24 など）を使用してアドレスとサブネット マスクを指定します。マスクを使用せずに IP アドレスを入力すると、そのアドレスは最後が 0 であってもホスト アドレスと見なされます。

ステップ 4　[Destination] フィールドに宛先アドレスを入力します。または [...] ボタンをクリックして、ASDM ですでに定義されている IP アドレスを選択します。

プレフィックス / 長さ表記（10.1.1.0/24 など）を使用してアドレスとサブネット マスクを指定します。マスクを使用せずに IP アドレスを入力すると、そのアドレスは最後が 0 であってもホスト アドレスと見なされます。

宛先アドレスが複数ある場合はカンマで区切ります。

デフォルトでは、フィールドには任意の宛先アドレスを許可する **any** が表示されています。

ステップ 5　[Translated] 領域で、[Interface] ドロップダウン リストから、マッピング アドレスを使用するインターフェイスを選択します。

ステップ 6　マッピング IP アドレスを指定するには、次のいずれかをクリックします。

- Use IP Address

  IP アドレスを入力するか、[...] ボタンをクリックして ASDM ですでに定義されている IP アドレスを選択します。

  プレフィックス / 長さ表記（10.1.1.0/24 など）を使用してアドレスとサブネット マスクを指定します。マスクを使用せずに IP アドレスを入力すると、そのアドレスは最後が 0 であってもホスト アドレスと見なされます。
- Use Interface IP Address

実際のアドレスとマッピング アドレスのサブネット マスクは同じである必要があります。

ステップ 7　（任意）スタティック PAT を使用するには、[Enable Port Address Translation (PAT)] をオンにします。

a.　[Protocol] では、[TCP] または [UDP] をクリックします。

b.　[Original Port] フィールドで、実際のポート番号を入力します。

c.　[Translated Port] フィールドで、マッピング ポート番号を入力します。

ステップ 8　（任意）[Description] フィールドに説明を入力します。

ステップ 9　（任意）DNS 応答内部のアドレスの変換をイネーブルにするには、[Connection Settings] 領域をクリックして開き、[Translate the DNS replies that match the translation rule] をオンにします。

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おり、その DNS サーバがクライアントと異なるインターフェイス上にある場合、クライアントと DNS サーバではホストのアドレスが異なっている必要があります。一方にはマッピング アドレスが、もう一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。マッピングされるホストは、クライアントまたは DNS サーバのいずれかと同じインターフェイス上にある必要があります。詳細については、「DNS および NAT」（P.25-16）を参照してください。

ステップ 10　（任意）接続設定をイネーブルにするには、[Connection Settings] 領域をクリックして開き、次のオプションを 1 つ以上設定します。

（注）　これらの値は、セキュリティ ポリシー ルールを使用しても設定できます（「接続の設定」（P.27-6）を参照）。これらのオプションを両方に設定した場合、セキュリティ アプライアンスは低い方の制限値を使用します。TCP シーケンスのランダム化がいずれかの方法を使用してディセーブルになっている場合、セキュリティ アプライアンスは TCP シーケンスのランダム化をディセーブルにします。

- [Randomize sequence number]：このチェックボックスをオンにすると（デフォルト）、セキュリティ アプライアンスは TCP パケットのシーケンス番号をランダム化します。それぞれの TCP 接続には 2 つの ISN が割り当てられており、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、着信と発信の両方向で通過する TCP SNY の ISN をランダム化します。

  保護されたホストの ISN をランダム化することにより、攻撃者が新しい接続で次の ISN を予測できないようにして、新規セッションが乗っ取られるのを防ぎます。

  TCP 初期シーケンス番号のランダム化は、必要に応じてディセーブルにできます。次に例を示します。

  - 別の直列接続されたファイアウォールでも初期シーケンス番号がランダム化され、トラフィックに影響することはないものの、両方のファイアウォールでこの動作を実行する必要がない場合。
  - セキュリティ アプライアンスで eBGP マルチホップを使用しており、eBGP ピアで 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 アプライアンスで接続のシーケンスをランダム化しないようにする必要がある WAAS デバイスを使用する場合。
- [Maximum TCP Connections] : TCP の最大接続数を 0 ～ 65,535 の範囲で指定します。この値を 0 に設定すると、接続数は無制限になります。
- [Maximum UDP Connections] : UDP の最大接続数を 0 ～ 65,535 の範囲で指定します。この値を 0 に設定すると、接続数は無制限になります。
- [Maximum Embryonic Connections] : 初期接続の最大数を 65,536 までの範囲で指定します。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。この制限により、TCP 代行受信機能がイネーブルになります。デフォルトは **0** で、最大初期接続数であることを示します。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。

ステップ 11　[OK] をクリックします。

NAT 免除の使用

NAT 除外ではアドレスを変換処理から除外して、実ホストとリモート ホストの両方で接続を開始できるようにします。NAT 免除では、免除対象の実際のトラフィックを決定するときに実際のアドレスと宛先アドレスを指定できるので（ポリシー NAT と同様）、NAT 免除を使用するとダイナミック アイデンティティ NAT よりも詳細に制御が可能です。ただし、ポリシー NAT とは異なり、NAT 免除ではポートは考慮されません。ポートを考慮するには、スタティック ポリシー アイデンティティ NAT を使用してください。

NAT 免除の詳細については、「NAT 制御がイネーブルな状態での NAT のバイパス」（P.25-10）を参照してください。

NAT 免除を設定するには、次の手順を実行します。

ステップ 1　[Configuration] > [Firewall] > [NAT Rules] ペインから、[Add] > [Add NAT Exempt Rule] を選択します。

[Add NAT Exempt Rule] ダイアログボックスが表示されます。

ステップ 2　[Action: Exempt] をクリックします。

ステップ 3　[Original] 領域で、[Interface] ドロップダウン リストから、免除対象の実際のアドレスを持つホストに接続するインターフェイスを選択します。

ステップ 4　[Source] フィールドに実際のアドレスを入力します。または [...] ボタンをクリックして、ASDM ですでに定義されている IP アドレスを選択します。

プレフィックス / 長さ表記（10.1.1.0/24 など）を使用してアドレスとサブネット マスクを指定します。マスクを使用せずに IP アドレスを入力すると、そのアドレスは最後が 0 であってもホスト アドレスと見なされます。

（注）　免除対象外のアドレスは後で指定できます。たとえば、免除対象のサブネット（10.1.1.0/24 など）を指定できますが、10.1.1.50 を変換する必要がある場合は、そのアドレスについて免除を除外する別のルールを作成できます。

実際のアドレスが複数ある場合はカンマで区切ります。

ステップ 5　[Destination] フィールドに宛先アドレスを入力します。または [...] ボタンをクリックして、ASDM ですでに定義されている IP アドレスを選択します。

プレフィックス / 長さ表記（10.1.1.0/24 など）を使用してアドレスとサブネット マスクを指定します。マスクを使用せずに IP アドレスを入力すると、そのアドレスは最後が 0 であってもホスト アドレスと見なされます。

宛先アドレスが複数ある場合はカンマで区切ります。

デフォルトでは、フィールドには任意の宛先アドレスを許可する **any** が表示されています。

ステップ 6　[NAT Exempt Direction] 領域で、低位のセキュリティ インターフェイス（デフォルト）と高位のセキュリティ インターフェイスのどちらに向かうトラフィックを免除対象とするかを、該当するオプション ボタンをクリックして選択します。

ステップ 7　（任意）[Description] フィールドに説明を入力します。

ステップ 8　[OK] をクリックします。

ステップ 9　（任意）NAT 免除ルールに含まれていた一部のアドレスを免除対象外とする場合、免除を削除する別のルールを作成します。既存の NAT Exempt ルールを右クリックし、[Insert] を選択します。

[Add NAT Exempt Rule] ダイアログボックスが表示されます。

a.　[Action: Do not exempt] をクリックします。

b.　ステップ 3 ～ 8 を実行してルールを完成させます。

No Exempt ルールが Exempt ルールの前に追加されます。Exempt ルールと No Exempt ルールの順序は重要です。セキュリティ アプライアンスがパケットを免除するかどうか判断するとき、セキュリティ アプライアンスは、ルールが並んでいる順序に従い、パケットをそれぞれの NAT Exempt ルールと No Exempt ルールについて検証します。いずれかのルールに合致した場合、それ以降のルールはチェックされません。

[NAT] フィールドの説明

この項では、[NAT] 画面のフィールドについて説明します。次の項目を取り上げます。

- 「NAT Rules」（P.25-34）

- 「Add/Edit Static NAT Rule」（P.25-37）
- 「Add/Edit Dynamic NAT Rule」（P.25-39）
- 「Manage Global Pool」（P.25-40）
- 「Add/Edit Global Address Pool」（P.25-41）
- 「Add/Edit Static Policy NAT Rule」（P.25-41）
- 「Add/Edit Dynamic Policy NAT Rule」（P.25-43）
- 「Add/Edit NAT Exempt Rule」（P.25-45）

NAT Rules

フィールド

メニュー項目：

- [Add]：新しい NAT ルールを追加します。ドロップダウン リストから追加するルールのタイプを選択します。
  - [Add Static NAT Rule]：スタティック NAT ルール、スタティック PAT ルール、またはスタティック アイデンティティ NAT ルールを追加します。
  - [Add Dynamic NAT Rule]：ダイナミック NAT ルール、ダイナミック PAT ルール、またはアイデンティティ NAT ルールを追加します。
  - [Add NAT Exempt Rule]：NAT 免除ルールを追加します。
  - [Advanced]：ポリシー NAT ルールを追加します。

    [Add Static Policy NAT Rule]：スタティック ポリシー NAT ルール、スタティック ポリシー PAT ルール、またはスタティック ポリシー アイデンティティ NAT ルールを追加します。

    [Add Dynamic Policy NAT Rule]：ダイナミック ポリシー NAT ルールまたはダイナミック ポリシー PAT ルールを追加します。
  - [Insert]：テーブルで選択したルールの上に同じタイプの新しいルールを挿入します。
  - [Insert After]：テーブルで選択したルールの下に同じタイプの新しいルールを挿入します。
- [Edit]：NAT ルールを編集します。
- [Delete]：NAT ルールを削除します。
- [Move Up]：ルールを上に移動します。ルールは、このテーブルに表示される順序で評価されるため、重複したルールがある場合は、それらを表示する順序に注意が必要です。
- [Move Down]：ルールを下に移動します。
- [Cut]：ルールを切り取ります。
- [Copy]：ルールのパラメータをコピーします。[Paste] ボタンを使用すれば、それと同じパラメータを持つルールを新たに作成できます。
- [Paste]：ルールからコピーしたパラメータまたは切り取ったパラメータがあらかじめ入力された状態の [Add/Edit Rule] ダイアログボックスが表示されます。このダイアログボックスでは、それらのパラメータを修正して新しいルールを作成し、それをテーブルに追加できます。[Paste] ボタンをクリックすると、選択したルールのすぐ前にそのルールが追加されます。[Paste] ドロップダウン リストから [Paste After] 項目を選択すると、選択したルールのすぐ後にそのルールが追加されます。

- [Find] : 一致するルールだけを表示するように、表示内容をフィルタリングします。[Find] をクリックすると、[Filter] フィールドが開きます。もう一度 [Find] をクリックすると、[Filter] フィールドは非表示になります。
  - [Filter] ドロップダウン リスト : [Interface]、[Original Source]、[Original Service]、[Translated Interface]、[Translated Address]、[Translated Service]、[Rule Type]、[Query] の中からフィルタ基準を選択します。ルール クエリーとは、複数の基準を 1 つにまとめたもので、保存しておけば繰り返し使用できます。
  - [Condition] ドロップダウン リスト : 基準が [Original Source] または [Translate Address] の場合、条件を [is] または [contains] から選択します。他のすべての基準では、[is] 条件を使用します。
  - [Filter] フィールド : [Interface] タイプが選択された場合、このフィールドはドロップダウン リストになり、そこからインターフェイス名を選択できます。[Rule] タイプの場合、ドロップダウン リストには [Exempt]、[Static]、および [Dynamic] が含まれます。[Query] タイプの場合、このドロップダウン リストには、すべての定義済みルール クエリーが含まれます。[Original Source] タイプおよび [Translated Address] タイプには、IP アドレスを指定できます。手動で入力できるほか、[...] ボタンをクリックし、[Browse Address] ダイアログボックスを開いて参照することもできます。[Translated Service] タイプには、複数のプロトコル タイプを指定できます。手動で入力できるほか、[...] ボタンをクリックし、[Browse Translated Service] ダイアログボックスを開いて参照することもできます。
  - [Filter] : フィルタを実行します。
  - [Clear] : [Filter] フィールドをクリアします。
  - [Define Query] : [Define Query] ダイアログボックスが表示されます。このダイアログボックスでは、名前付きルール クエリーを管理できます。
- [Diagram] : ルール テーブルの下に [Rule Flow Diagram] 領域が表示されます。この図には、ネットワーク、トラフィックのタイプ、インターフェイス名、フローの方向、およびアクションが表示されます。
- [Packet Trace] : 選択したルールの特性とともにパラメータがあらかじめ入力されたパケット トレーサ ツールを開きます。

[NAT Rules] テーブル :

カラムの内容を編集する場合は、テーブル セルをダブルクリックします。カラム ヘッダーをダブルクリックすると、選択されたカラムをソート キーとして、テーブルが英数字の昇順でソートされます。ルールを右クリックすると、上記のボタンで選択できるすべてオプションのほか、[Insert] 項目および [Insert After] 項目が表示されます。[Insert] 項目を指定すると、選択したルールのすぐ前に新しいルールが挿入され、[Insert After] 項目を指定すると、選択したルールのすぐ後に新しいルールが挿入されます。

- [Real Interface Name] : NAT ルールは送信元インターフェイスごとにまとめられ、送信元インターフェイスは、変換対象となる実際のホストに接続されます。+ または - ボタンをクリックして、インターフェイスの NAT ルールを表示または非表示にできます。
- [#] : ルールの評価順序を示します。
- [Type] : 変換ルール タイプを表示します。
- [Original] : 実際のアドレスを表示します。
  - [Source] : 変換する実際のアドレスを示します。
  - [Destination] : ポリシー NAT と NAT 免除の場合は、実際のアドレスの宛先ネットワークを示します。標準 NAT の場合、表示は空白になります。
  - [Service] : スタティック PAT の場合、変換元のサービスを示します。
- [Translated] : マッピング アドレスとそれに関連付けられたインターフェイスを表示します。

  - [Interface]：マッピング インターフェイスを示します。
  - [Address]：マッピング アドレスを示します。
  - [Service]：スタティック PAT の場合、変換先のサービスを示します。
- [Options]：次の項目があります。
  - [DNS Rewrite]：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おり、その DNS サーバがクライアントと異なるインターフェイス上にある場合、クライアントと DNS サーバではホストのアドレスが異なっている必要があります。一方にはマッピング アドレスが、もう一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。マッピングされるホストは、クライアントまたは DNS サーバのいずれかと同じインターフェイス上にある必要があります。詳細については、「DNS および NAT」（P.25-16）を参照してください。このオプションはテーブルで直接オンまたはオフにできます。
  - [Maximum TCP Connections]：TCP の最大接続数を 0 ～ 65,535 の範囲で指定します。この値を 0 に設定すると、接続数は無制限になります。
  - [Maximum Embryonic Connections]：初期接続の最大数を 65,536 までの範囲で指定します。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。この制限により、TCP 代行受信機能がイネーブルになります。デフォルトは 0 で、最大初期接続数であることを示します。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。
  - [Maximum UDP Connections]：UDP の最大接続数を 0 ～ 65,535 の範囲で指定します。この値を 0 に設定すると、接続数は無制限になります。
  - [Randomize sequence number]：このチェックボックスをオンにすると（デフォルト）、セキュリティ アプライアンスは TCP パケットのシーケンス番号をランダム化します。それぞれの TCP 接続には 2 つの ISN が割り当てられており、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、着信と発信の両方向で通過する TCP SNY の ISN をランダム化します。

    保護されたホストの ISN をランダム化することにより、攻撃者が新しい接続で次の ISN を予測できないようにして、新規セッションが乗っ取られるのを防ぎます。

    TCP 初期シーケンス番号のランダム化は、必要に応じてディセーブルにできます。次に例を示します。

    別の直列接続されたファイアウォールでも初期シーケンス番号がランダム化され、トラフィックに影響することはないものの、両方のファイアウォールでこの動作を実行する必要がない場合。

    セキュリティ アプライアンスで eBGP マルチホップを使用しており、eBGP ピアで 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 アプライアンスで接続のシーケンスをランダム化しないようにする必要がある WAAS デバイスを使用する場合。

    このオプションはテーブルで直接オンまたはオフにできます。
- [Description]（Policy NAT の場合のみ）：ルールの説明がある場合は、このカラムに表示されます。

その他の領域：

- [Enable traffic through the firewall without address translation]：NAT 制御をイネーブルまたはディセーブルにします。詳細については、「NAT コントロール」（P.25-5）を参照してください。
- [Addresses]：このタブでは、IP アドレス オブジェクトまたはネットワーク オブジェクト グループを追加、編集、削除、または検索できます。
- [Services]：このタブでは、サービスを追加、編集、削除、または検索できます。
- [Global Pools]：このタブでは、ダイナミック NAT コンフィギュレーションで使用されるグローバル アドレスの NAT プールを管理できます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit Static NAT Rule

フィールド

- [Original]：ネットワーク変換が適用される前の実際のアドレスとそれに関連付けられているインターフェイス。
  - [Interface]：実際のホストまたはネットワークがある、セキュリティ アプライアンスのネットワーク インターフェイスを選択します。
  - [Source]：ルールを適用するホストまたはネットワークの IP アドレスを指定します。

    プレフィックス/長さ表記（10.1.1.0/24 など）を使用してアドレスとサブネット マスクを指定します。マスクを使用せずに IP アドレスを入力すると、そのアドレスは最後が 0 であってもホスト アドレスと見なされます。
  - [...]：ASDM ですでに定義されている IP アドレスを選択できます。
- [Translated]：マッピング インターフェイスと IP アドレスを指定できます。実際のアドレスとマッピング アドレスのサブネット マスクは同じである必要があります。
  - [Interface]：マッピング アドレスを使用するインターフェイスを設定します。
  - [IP address]：マッピング IP アドレスを設定します。
  - [...]：ASDM ですでに定義されている IP アドレスを選択できます。
  - [Use Interface IP address]：[Interface] ドロップダウン リストで選択したインターフェイスのインターフェイス IP アドレスとなるマッピング IP アドレスを設定します。
- [Port Address Translation (PAT)]：PAT パラメータを設定します。
  - [Enable Port Address Translation (PAT)]：スタティック PAT をイネーブルにします。
  - [Protocol]：TCP または UDP。
  - [Original Port]：ポート番号または名前を入力します。
  - [Translated Port]：ポート番号または名前を入力します。

- [Connection Settings] : [DNS Rewrite]、[Maximum Connections]、[Embryonic Limit]、および [Randomize Sequence Number] を設定できます。
  - [DNS Rewrite] : 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おり、その DNS サーバがクライアントと異なるインターフェイス上にある場合、クライアントと DNS サーバではホストのアドレスが異なっている必要があります。一方にはマッピング アドレスが、もう一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。マッピングされるホストは、クライアントまたは DNS サーバのいずれかと同じインターフェイス上にある必要があります。詳細については、「DNS および NAT」（P.25-16）を参照してください。このオプションはテーブルで直接オンまたはオフにできます。
  - [Maximum TCP Connections] : TCP の最大接続数を 0 ～ 65,535 の範囲で指定します。この値を 0 に設定すると、接続数は無制限になります。
  - [Maximum Embryonic Connections] : 初期接続の最大数を 65,536 までの範囲で指定します。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。この制限により、TCP 代行受信機能がイネーブルになります。デフォルトは **0** で、最大初期接続数であることを示します。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。
  - [Maximum UDP Connections] : UDP の最大接続数を 0 ～ 65,535 の範囲で指定します。この値を 0 に設定すると、接続数は無制限になります。
  - [Randomize sequence number] : このチェックボックスをオンにすると（デフォルト）、セキュリティ アプライアンスは TCP パケットのシーケンス番号をランダム化します。それぞれの TCP 接続には 2 つの ISN が割り当てられており、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、着信と発信の両方向で通過する TCP SNY の ISN をランダム化します。

    保護されたホストの ISN をランダム化することにより、攻撃者が新しい接続で次の ISN を予測できないようにして、新規セッションが乗っ取られるのを防ぎます。

    TCP 初期シーケンス番号のランダム化は、必要に応じてディセーブルにできます。次に例を示します。

    別の直列接続されたファイアウォールでも初期シーケンス番号がランダム化され、トラフィックに影響することはないものの、両方のファイアウォールでこの動作を実行する必要がない場合。

    セキュリティ アプライアンスで eBGP マルチホップを使用しており、eBGP ピアで 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 アプライアンスで接続のシーケンスをランダム化しないようにする必要がある WAAS デバイスを使用する場合。

    このオプションはテーブルで直接オンまたはオフにできます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit Dynamic NAT Rule

フィールド

- [Original]：ネットワーク変換が適用される前の実際のアドレスとそれに関連付けられているインターフェイス。
  - [Interface]：実際のホストまたはネットワークがある、セキュリティ アプライアンスのネットワーク インターフェイスを選択します。
  - [Source]：ルールを適用するホストまたはネットワークの IP アドレスを指定します。

    プレフィックス/長さ表記（10.1.1.0/24 など）を使用してアドレスとサブネット マスクを指定します。マスクを使用せずに IP アドレスを入力すると、そのアドレスは最後が 0 であってもホスト アドレスと見なされます。
  - [...]：ASDM ですでに定義されている IP アドレスを選択できます。
- [Translated]：ダイナミック インターフェイスとグローバル アドレス プールを指定できます。
  - [Pool ID]：グローバル プールのプール ID を示します。
  - [Interface]：プール ID に関連付けられたインターフェイスを示します。
  - [Addresses Pool]：インターフェイスごとにプール内のアドレスを示します。
  - [Manage]：グローバル プールを管理します。
- [Connection Settings]：[DNS Rewrite]、[Maximum Connections]、[Embryonic Limit]、および [Randomize Sequence Number] を設定できます。
  - [DNS Rewrite]：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おり、その DNS サーバがクライアントと異なるインターフェイス上にある場合、クライアントと DNS サーバではホストのアドレスが異なっている必要があります。一方にはマッピング アドレスが、もう一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。マッピングされるホストは、クライアントまたは DNS サーバのいずれかと同じインターフェイス上にある必要があります。詳細については、「DNS および NAT」（P.25-16）を参照してください。このオプションはテーブルで直接オンまたはオフにできます。
  - [Maximum TCP Connections]：TCP の最大接続数を 0 ～ 65,535 の範囲で指定します。この値を 0 に設定すると、接続数は無制限になります。
  - [Maximum Embryonic Connections]：初期接続の最大数を 65,536 までの範囲で指定します。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。この制限により、TCP 代行受信機能がイネーブルになります。デフォルトは 0 で、最大初期接続数であることを示します。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。

- [Maximum UDP Connections]：UDP の最大接続数を 0 ～ 65,535 の範囲で指定します。この値を 0 に設定すると、接続数は無制限になります。
- [Randomize sequence number]：このチェックボックスをオンにすると（デフォルト）、セキュリティ アプライアンスは TCP パケットのシーケンス番号をランダム化します。それぞれの TCP 接続には 2 つの ISN が割り当てられており、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、着信と発信の両方向で通過する TCP SNY の ISN をランダム化します。

  保護されたホストの ISN をランダム化することにより、攻撃者が新しい接続で次の ISN を予測できないようにして、新規セッションが乗っ取られるのを防ぎます。

  TCP 初期シーケンス番号のランダム化は、必要に応じてディセーブルにできます。次に例を示します。

  別の直列接続されたファイアウォールでも初期シーケンス番号がランダム化され、トラフィックに影響することはないものの、両方のファイアウォールでこの動作を実行する必要がない場合。

  セキュリティ アプライアンスで eBGP マルチホップを使用しており、eBGP ピアで 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 アプライアンスで接続のシーケンスをランダム化しないようにする必要がある WAAS デバイスを使用する場合。

  このオプションはテーブルで直接オンまたはオフにできます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Manage Global Pool

フィールド

- [Add]：新しいグローバル プールを追加します。
- [Edit]：選択したグローバル プールを編集します。
- [Delete]：選択したグローバル プールを削除します。
- [Pool ID]：プール ID を示します。
- [Interface]：アドレス プールに関連付けられているインターフェイス名を表示します。
- [Addresses Pool]：プール内のアドレスを指定します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit Global Address Pool

フィールド

- [Interface]：新しいアドレス プールに関連付けるインターフェイス名を指定します。[Interface] ドロップダウン リストで名前を選択します。
- [Pool ID]：このアドレス プールを参照するためにダイナミック NAT ルールが使用する ID 番号を指定します。[Pool ID] フィールドに番号を入力します。
- [Range]：IP アドレスの範囲を新しいアドレス プールで使用することを指定するには、このオプションを選択します。このオプションを選択する場合は、次の値を指定します。
  - [Starting IP address]：範囲の開始 IP アドレスを指定します。
  - [Ending IP Address]：範囲の終了 IP アドレスを指定します。
  - [Netmask]（任意）：この値により、変換後の IP アドレスがメンバーになるネットワークのマスクを指定します。
- [Port Address Translation (PAT)]：IP アドレスが PAT で使用されることを指定するには、このオプションを選択します。このオプションを選択する場合は、次の値を指定します。
  - [IP Address]：PAT アドレスを指定します。
  - [Netmask]（任意）：この値により、変換後の IP アドレスがメンバーになるネットワークのマスクを指定します。
- [Port Address Translation (PAT) using IP address of the interface]：[Interface] ドロップダウン リストで選択したインターフェイスに割り当てられている IP アドレスを、PAT の変換後のアドレスとして使用することを指定するには、このオプションを選択します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit Static Policy NAT Rule

- [Original]：ネットワーク変換が適用される前の実際のアドレスとそれに関連付けられているインターフェイス。

  - [Interface]：実際のホストまたはネットワークがある、セキュリティ アプライアンスのネットワーク インターフェイスを選択します。
  - [Source]：ルールを適用するホストまたはネットワークの IP アドレスを指定します。

    プレフィックス/長さ表記（10.1.1.0/24 など）を使用してアドレスとサブネット マスクを指定します。マスクを使用せずに IP アドレスを入力すると、そのアドレスは最後が 0 であってもホスト アドレスと見なされます。
  - [...]：ASDM ですでに定義されている IP アドレスを選択できます。
  - [Destination]：宛先アドレスを指定します。

    プレフィックス/長さ表記（10.1.1.0/24 など）を使用してアドレスとサブネット マスクを指定します。マスクを使用せずに IP アドレスを入力すると、そのアドレスは最後が 0 であってもホスト アドレスと見なされます。

    宛先アドレスが複数ある場合はカンマで区切ります。

    デフォルトでは、フィールドには任意の宛先アドレスを許可する **any** が表示されています。
  - [...]：ASDM ですでに定義されている IP アドレスを選択できます。
- [Translated]：マッピング インターフェイスと IP アドレスを指定できます。実際のアドレスとマッピング アドレスのサブネット マスクは同じである必要があります。
  - [Interface]：マッピング アドレスを使用するインターフェイスを設定します。
  - [Use IP address]：マッピング IP アドレスを設定します。
  - [...]：ASDM ですでに定義されている IP アドレスを選択できます。
  - [Use Interface IP address]：[Interface] ドロップダウン リストで選択したインターフェイスのインターフェイス IP アドレスとなるマッピング IP アドレスを設定します。
- [Port Address Translation (PAT)]：PAT パラメータを設定します。
  - [Enable Port Address Translation (PAT)]：スタティック PAT をイネーブルにします。
  - [Protocol]：TCP または UDP。
  - [Original Port]：ポート番号または名前を入力します。
  - [Translated Port]：ポート番号または名前を入力します。
- [Description]：このルールの説明を設定します。
- [Connection Settings]：[DNS Rewrite]、[Maximum Connections]、[Embryonic Limit]、および [Randomize Sequence Number] を設定できます。
  - [DNS Rewrite]：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おり、その DNS サーバがクライアントと異なるインターフェイス上にある場合、クライアントと DNS サーバではホストのアドレスが異なっている必要があります。一方にはマッピング アドレスが、もう一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。マッピングされるホストは、クライアントまたは DNS サーバのいずれかと同じインターフェイス上にある必要があります。詳細については、「DNS および NAT」（P.25-16）を参照してください。このオプションはテーブルで直接オンまたはオフにできます。
  - [Maximum TCP Connections]：TCP の最大接続数を 0 ～ 65,535 の範囲で指定します。この値を 0 に設定すると、接続数は無制限になります。
  - [Maximum Embryonic Connections]：初期接続の最大数を 65,536 までの範囲で指定します。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。この制限により、TCP 代行受信機能がイネーブルになります。デフォルトは 0 で、最大初期接続数であることを示します。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。

- [Maximum UDP Connections]：UDP の最大接続数を 0 ～ 65,535 の範囲で指定します。この値を 0 に設定すると、接続数は無制限になります。
- [Randomize sequence number]：このチェックボックスをオンにすると（デフォルト）、セキュリティ アプライアンスは TCP パケットのシーケンス番号をランダム化します。それぞれの TCP 接続には 2 つの ISN が割り当てられており、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、着信と発信の両方向で通過する TCP SNY の ISN をランダム化します。

  保護されたホストの ISN をランダム化することにより、攻撃者が新しい接続で次の ISN を予測できないようにして、新規セッションが乗っ取られるのを防ぎます。

  TCP 初期シーケンス番号のランダム化は、必要に応じてディセーブルにできます。次に例を示します。

  別の直列接続されたファイアウォールでも初期シーケンス番号がランダム化され、トラフィックに影響することはないものの、両方のファイアウォールでこの動作を実行する必要がない場合。

  セキュリティ アプライアンスで eBGP マルチホップを使用しており、eBGP ピアで 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 アプライアンスで接続のシーケンスをランダム化しないようにする必要がある WAAS デバイスを使用する場合。

  このオプションはテーブルで直接オンまたはオフにできます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit Dynamic Policy NAT Rule

- [Original]：ネットワーク変換が適用される前の実際のアドレスとそれに関連付けられているインターフェイス。
  - [Interface]：実際のホストまたはネットワークがある、セキュリティ アプライアンスのネットワーク インターフェイスを選択します。
  - [Source]：ルールを適用するホストまたはネットワークの IP アドレスを指定します。

    プレフィックス/長さ表記（10.1.1.0/24 など）を使用してアドレスとサブネット マスクを指定します。マスクを使用せずに IP アドレスを入力すると、そのアドレスは最後が 0 であってもホスト アドレスと見なされます。

    実際のアドレスが複数ある場合はカンマで区切ります。

  - [...]：ASDM ですでに定義されている IP アドレスを選択できます。
  - [Destination]：宛先アドレスを指定します。

    プレフィックス/長さ表記（10.1.1.0/24 など）を使用してアドレスとサブネット マスクを指定します。マスクを使用せずに IP アドレスを入力すると、そのアドレスは最後が 0 であってもホスト アドレスと見なされます。

    宛先アドレスが複数ある場合はカンマで区切ります。

    デフォルトでは、フィールドには任意の宛先アドレスを許可する any が表示されています。
  - [...]：ASDM ですでに定義されている IP アドレスを選択できます。
- [Translated]：ダイナミック インターフェイスとグローバル アドレス プールを指定できます。
  - [Pool ID]：グローバル プールのプール ID を示します。
  - [Interface]：プール ID に関連付けられたインターフェイスを示します。
  - [Addresses Pool]：インターフェイスごとにプール内のアドレスを示します。
  - [Manage]：グローバル プールを管理します。
- [Description]：このルールの説明を設定します。
- [Connection Settings]：[DNS Rewrite]、[Maximum Connections]、[Embryonic Limit]、および [Randomize Sequence Number] を設定できます。
  - [DNS Rewrite]：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おり、その DNS サーバがクライアントと異なるインターフェイス上にある場合、クライアントと DNS サーバではホストのアドレスが異なっている必要があります。一方にはマッピング アドレスが、もう一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。マッピングされるホストは、クライアントまたは DNS サーバのいずれかと同じインターフェイス上にある必要があります。詳細については、「DNS および NAT」（P.25-16）を参照してください。このオプションはテーブルで直接オンまたはオフにできます。
  - [Maximum TCP Connections]：TCP の最大接続数を 0 ～ 65,535 の範囲で指定します。この値を 0 に設定すると、接続数は無制限になります。
  - [Maximum Embryonic Connections]：初期接続の最大数を 65,536 までの範囲で指定します。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。この制限により、TCP 代行受信機能がイネーブルになります。デフォルトは **0** で、最大初期接続数であることを示します。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。
  - [Maximum UDP Connections]：UDP の最大接続数を 0 ～ 65,535 の範囲で指定します。この値を 0 に設定すると、接続数は無制限になります。
  - [Randomize sequence number]：このチェックボックスをオンにすると（デフォルト）、セキュリティ アプライアンスは TCP パケットのシーケンス番号をランダム化します。それぞれの TCP 接続には 2 つの ISN が割り当てられており、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、着信と発信の両方向で通過する TCP SNY の ISN をランダム化します。

    保護されたホストの ISN をランダム化することにより、攻撃者が新しい接続で次の ISN を予測できないようにして、新規セッションが乗っ取られるのを防ぎます。

TCP 初期シーケンス番号のランダム化は、必要に応じてディセーブルにできます。次に例を示します。

別の直列接続されたファイアウォールでも初期シーケンス番号がランダム化され、トラフィックに影響することはないものの、両方のファイアウォールでこの動作を実行する必要がない場合。

セキュリティ アプライアンスで eBGP マルチホップを使用しており、eBGP ピアで 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 アプライアンスで接続のシーケンスをランダム化しないようにする必要がある WAAS デバイスを使用する場合。

このオプションはテーブルで直接オンまたはオフにできます。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit NAT Exempt Rule

フィールド

- [Action]：アドレスを免除するかどうかを設定します。
  - [Exempt]：アドレスの NAT を免除します。
  - [Do not exempt]：アドレスに対する免除を削除します。
- [Original]：NAT 免除ルール対象のアドレスを指定します。
  - [Interface]：実際のホストまたはネットワークがある、セキュリティ アプライアンスのネットワーク インターフェイスを選択します。
  - [Source]：ホストまたはネットワークの実際の IP アドレスを指定します。

    プレフィックス/長さ表記（10.1.1.0/24 など）を使用してアドレスとサブネット マスクを指定します。マスクを使用せずに IP アドレスを入力すると、そのアドレスは最後が 0 であってもホスト アドレスと見なされます。

    実際のアドレスが複数ある場合はカンマで区切ります。
  - [...]：ASDM ですでに定義されている IP アドレスを選択できます。
  - [Destination]：宛先アドレスを指定します。

    プレフィックス/長さ表記（10.1.1.0/24 など）を使用してアドレスとサブネット マスクを指定します。マスクを使用せずに IP アドレスを入力すると、そのアドレスは最後が 0 であってもホスト アドレスと見なされます。

    宛先アドレスが複数ある場合はカンマで区切ります。

    デフォルトでは、フィールドには任意の宛先アドレスを許可する **any** が表示されています。
  - [...]：ASDM ですでに定義されている IP アドレスを選択できます。

- [NAT Exempt Direction]：着信または発信トラフィックの NAT ルールを設定します。
  - [NAT Exempt outbound traffic from interface "*real interface*" to lower security interfaces (default)]：発信トラフィック用の NAT ルールを設定します。
  - [NAT Exempt inbound traffic from interface "*real interface*" to higher security interfaces]：着信トラフィック用の NAT ルールを設定します。
- [Description]：このルールの説明を設定します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—