CHAPTER 25

NAT の設定

この章では、Network Address Translation（NAT; 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

この項では、NAT がセキュリティ アプライアンスでどのように動作するかを説明します。次の項目を取り上げます。

NAT の概要

アドレス変換では、パケット内の実際のアドレスが、宛先ネットワークでルーティングできるマッピング アドレスに置き換えられます。NAT は、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の 2 つの手順で構成されます。

セキュリティ アプライアンスは、NAT ルールにトラフィックが一致するとアドレスを変換します。一致する NAT ルールがない場合、そのパケットの処理は続行されます。例外は、NAT 制御をイネーブルにした場合です。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 ルールに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、P.5-5 の「デフォルトのセキュリティ レベル」を参照してください。NAT 制御の詳細については、P.25-4 の「NAT 制御」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の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、セキュリティ レベルの低い方が外部です。たとえば、インターフェイス 1 のセキュリティ レベルが 60 で、インターフェイス 2 のセキュリティ レベルが 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」になります。

NAT の利点のいくつかを次に示します。

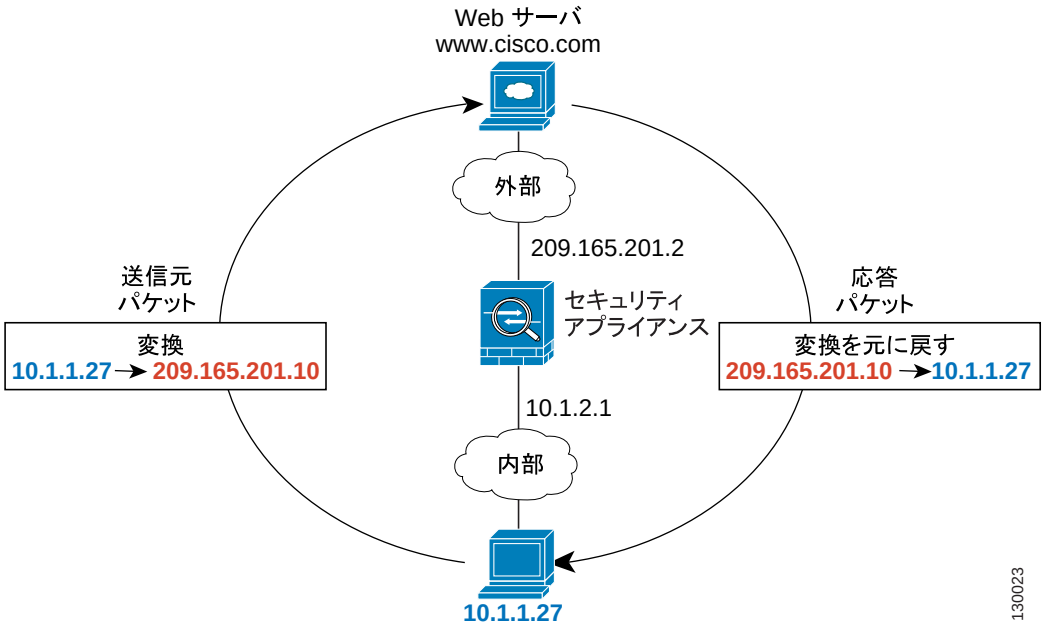
- 内部ネットワークでプライベート アドレスを使用できます。プライベート アドレスは、インターネットにルーティングできません。
- NAT は実際のアドレスを他のネットワークから隠蔽するため、攻撃者はホストの実際のアドレスを知ることができません。
- 重複アドレスなど、IP ルーティングの問題を解決できます。

NAT をサポートしていないプロトコルの詳細については、表 24-1 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、一般的なルーテッド モードの NAT の例を示しています。内部ホスト 10.1.2.27 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 10.1.2.27 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、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 10.1.2.27 に戻します。

図 25-1　NAT の例：ルーテッド モード



透過モードの NAT

透過モードで NAT を使用すると、ネットワークに対して NAT を実行するアップストリーム ルータとダウンストリーム ルータが不要になります。たとえば、2 つの VRF 間で透過ファイアウォールのセキュリティ アプライアンスを使用すると、VRF とグローバル テーブルの間に BGP ネイバー関係を確立できるので便利です。ただし、VRF 単位の NAT がサポートされない場合もあります。この場合は、必ず透過モードで NAT を使用します。

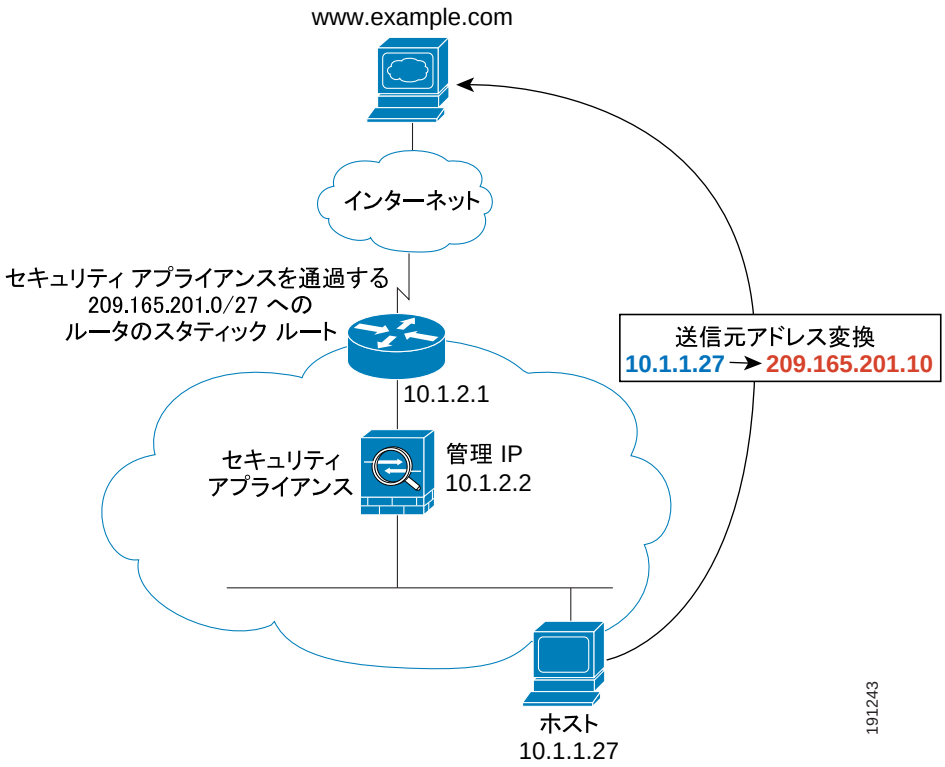
透過モードでの NAT には、次の要件と制約事項があります。

- マッピング アドレスが透過ファイアウォールと同じネットワークにない場合、アップストリーム ルータで、マッピング アドレス用に（セキュリティ アプライアンスを経由して）ダウンストリーム ルータをポイントするスタティック ルートを追加する必要があります。
- また、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は、実際の宛先アドレス用に、ダウンストリーム ルータをポイントするスタティック 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、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ので、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。一方、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 ルックアップではなくルート ルックアップを使用するので、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。
- 透過ファイアウォールにはインターフェイス IP アドレスがないので、インターフェイス PAT は使用できません。
- ARP 検査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のホストが ARP 要求を反対側のホストに送信した場合、発信側ホストの実際のアドレスが、同じサブネット上にある別のアドレスにマッピングされ、実際のアドレスは ARP 要求内で可視のままになります。

図 25-2 は、内部および外部インターフェイス上に同じネットワークを持つ、一般的な透過モードの NAT のシナリオを示しています。このシナリオでは、透過ファイアウォールが NAT サービスを実行するのでアップストリーム ルータは NAT を実行する必要はありません。内部ホスト 10.1.2.27 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 10.1.2.27 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、応答がマッピング アドレス 209.165.201.10 に送信され、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。これは、セキュリティ アプライアンス経由で誘導されるアップストリーム ルータ内のスタティック ルートにこのマッピング ネットワークが含まれているためです。続いて、セキュリティ アプライアンスは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 10.1.2.27 に戻します。実際のアドレスが直接接続されているので、セキュリティ アプライアンスはパケットをそのホストに直接送信します。

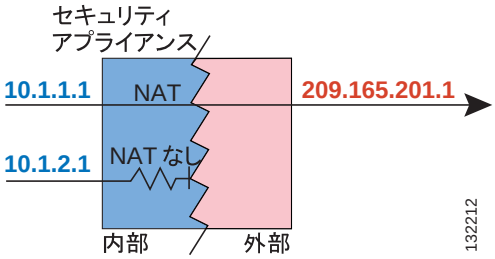
図 25-2　NAT の例：透過モード



NAT 制御

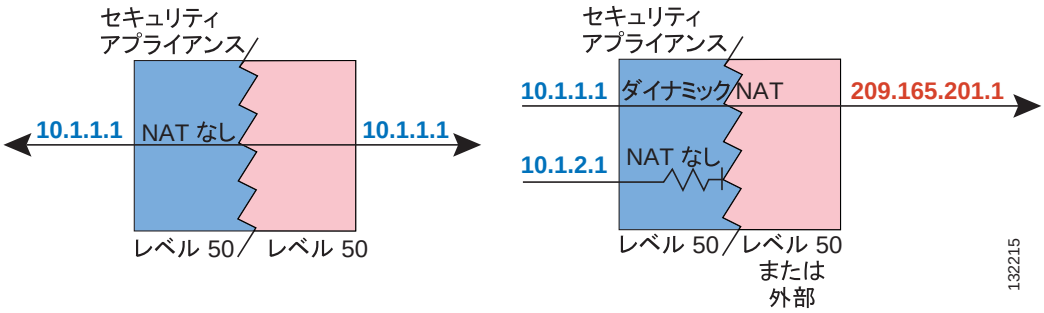
NAT 制御では、内部インターフェイスから外部インターフェイスに移動するパケットが NAT ルールと一致することが要求されます。内部ネットワークの任意のホストが外部ネットワークのホストにアクセスできるようにするには、内部ホストアドレスが変換されるように NAT を設定する必要があります（図 25-3）。

図 25-3　NAT 制御と発信トラフィック



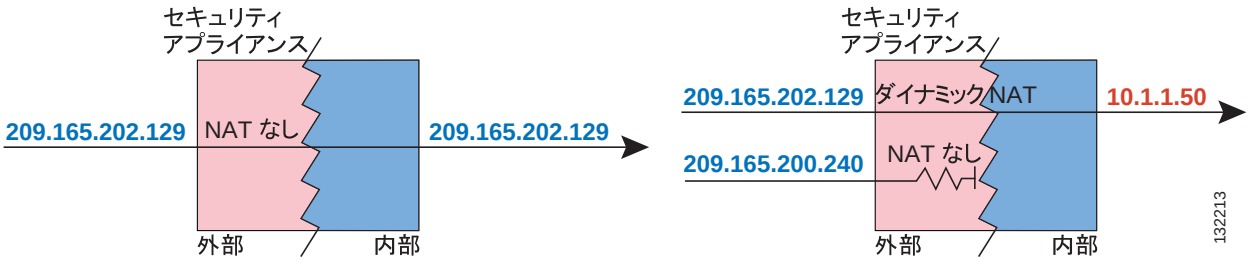
同じセキュリティ レベルのインターフェイスでは、通信するために NAT を使用する必要はありません。ただし、ダイナミック NAT または PAT を同じセキュリティのインターフェイス上に設定した場合、そのインターフェイスから同じセキュリティのインターフェイスまたは外部インターフェイスに向かうすべてのトラフィックは、NAT ルールに一致する必要があります（図 25-4 を参照）。

図 25-4　NAT 制御と同じセキュリティのトラフィック



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 ルール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るため、NAT の実行を選択しない限り、どのネットワークに対しても NAT を実行する必要はありません。ただし、以前のバージョンのソフトウェアからアップグレードした場合は、NAT 制御がシステムでイネーブルになっている可能性があります。NAT 制御をディセーブルにしても、ダイナミック NAT を設定したアドレスに対しては NAT を実行する必要があります。ダイナミック NAT を適用する方法の詳細については、P.25-17 の「ダイナミック NAT の実装」を参照してください。

NAT 制御によってセキュリティを強化し、同時に一部の内部アドレスを変換対象から外す場合、それらのアドレスに対して NAT 免除ルール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、P.25-33 の「NAT 免除の使用」を参照してください）。

NAT 制御を設定するには、P.25-16 の「NAT 制御の設定」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に対して固有の MAC アドレスをイネーブルにしないと、パケット分類子が NAT コンフィギュレーションを使用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。分類子と NAT の関係の詳細については、P.9-3 の「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」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。

アドレス変換は、ダイナミック NAT、Port Address Translation（PAT; ポート アドレス変換）、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せとして実装できます。NAT を実行する必要がない場合に NAT 制御をイネーブルにするなど、NAT をバイパスするルールを設定することもできます。

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 プールに含まれるアドレスは、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、そのホストにマッピング プールから IP アドレスを割り当てます。変換は、実際のホストが接続を開始したときにのみ追加されます。変換は接続が継続している間のみ有効であり、変換がタイムアウトすると、そのユーザは同じ IP アドレスは保持しません。したがって、宛先ネットワークのユーザは、アクセスリストで接続が許可されていても、ダイナミック NAT を使用しているホストへの接続を確実には開始できません。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方法の詳細については、「スタティック NAT」または「スタティック PAT」を参照してください。

（注）　場合によっては、変換が接続のために追加されてもセッションがセキュリティ アプライアンスに拒否されることがあります。この状況は、通常は変換がタイムアウトする、発信アクセスリスト、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 に、実際のアドレスへの接続を試みているリモート ホストを示します。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ます。

図 25-6　実際のアドレスへの接続を試みているリモートホスト

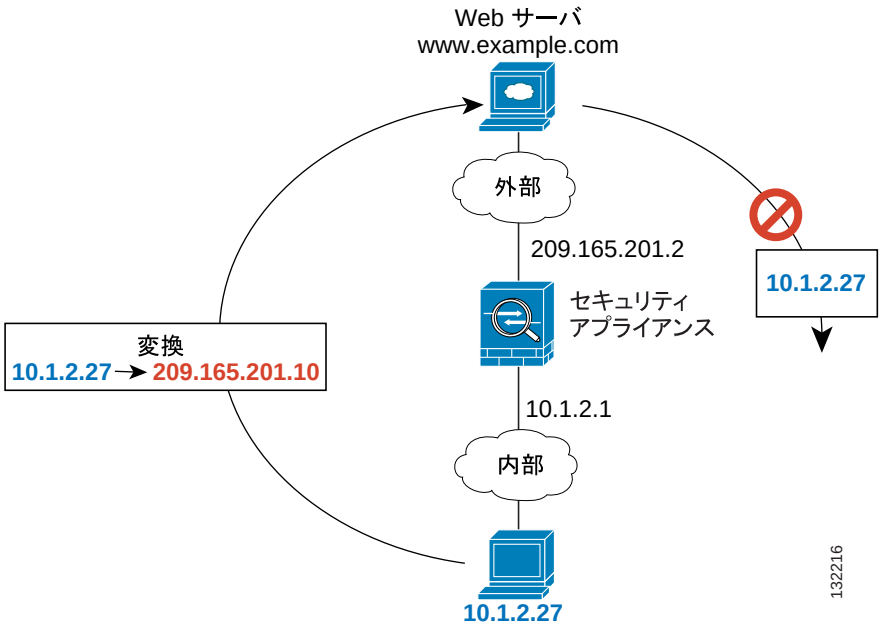
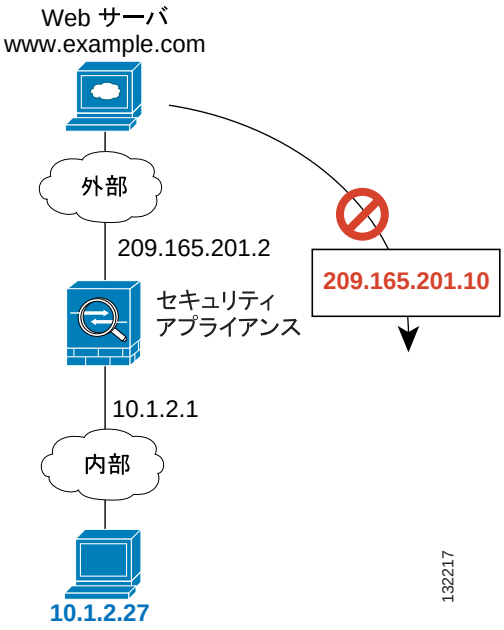


図 25-7 に、マッピング アドレスへの接続開始を試みているリモート ホストを示します。このアドレスは、現時点では変換テーブルにないため、セキュリティ アプライアンスはパケットをドロップします。

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）　変換が継続している間、アクセスリストで許可されていれば、リモート　ホストは変換済みのホストへの接続を開始できます。アドレスは予測不可能であるため、ホストへの接続は確立されません。ただし、この場合はアクセス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 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。

  この状態が頻繁に発生する場合は PAT を使用します。PAT では、1 つのアドレスの複数のポートを使用して 64,000 を超える変換が可能であるためです。
- マッピング プール内では多数のルーティング可能なアドレスを使用する必要があります。インターネットなど、宛先ネットワークが登録アドレスを要求する場合は、使用可能なアドレスが不足する可能性があります。

ダイナミック NAT の利点は、一部のプロトコルは PAT を使用できないということにあります。PAT は次のプロトコルでは機能しません。

- GRE バージョン 0 など、オーバーロードするためのポートがない IP プロトコル
- データ　ストリームと制御パスが別のポート上にあり、オープン規格ではない一部のマルチメディア アプリケーション

NAT および PAT のサポートの詳細については、P.24-3 の「アプリケーション プロトコル検査を使用するタイミング」を参照してください。

PAT

PAT では、複数の実際のアドレスが 1 つのマッピング IP アドレスに変換されます。具体的には、セキュリティ アプライアンスが、実際のアドレスと送信元ポート（実際のソケット）をマッピング アドレスと 1024 より大きい一意のポート（マッピング ソケット）に変換します。送信元ポートが接続ごとに異なるため、各接続には別の変換が必要です。たとえば、10.1.1.1:1025 には、10.1.1.1:1026 とは別の変換が必要です。

接続の有効期限が切れた後、ポート変換は 30 秒間非アクティブ状態が続くと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。宛先ネットワークのユーザは、PAT を使用するホストへの接続を確実には開始できません（アクセスリストでその接続が許可されている場合も同じです）。ホストの実際のポート番号またはマッピング 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、変換済みのホストが発信側でなければ変換をまったく作成しません。ホストへの確実なアクセス方法については、「スタティック NAT」または「スタティック PAT」を参照してください。

PAT では 1 つのマッピング アドレスを使用できるため、ルーティング可能なアドレスが節約されます。さらに、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することもできます。PAT は、制御パスとは異なるデータ ストリームを持つ一部のマルチメディア アプリケーションでは機能しません。NAT および PAT のサポートの詳細については、P.24-3 の「アプリケーション プロトコル検査を使用するタイミング」を参照してください。

（注）　変換が継続している間、アクセスリストで許可されていれば、リモート　ホストは変換済みのホストへの接続を開始できます。実際のポート アドレスとマッピング 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 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、実際のアドレスからマッピング アドレスへの固定変換が作成されます。ダイナミック NAT および PAT を使用すると、それ以降、各ホストは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接続ごとに同じであり、永続的な変換ルールが存在するため、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。スタティック NAT では、実際のアドレスと同数のマッピング アドレスも必要になります。

スタティック PAT

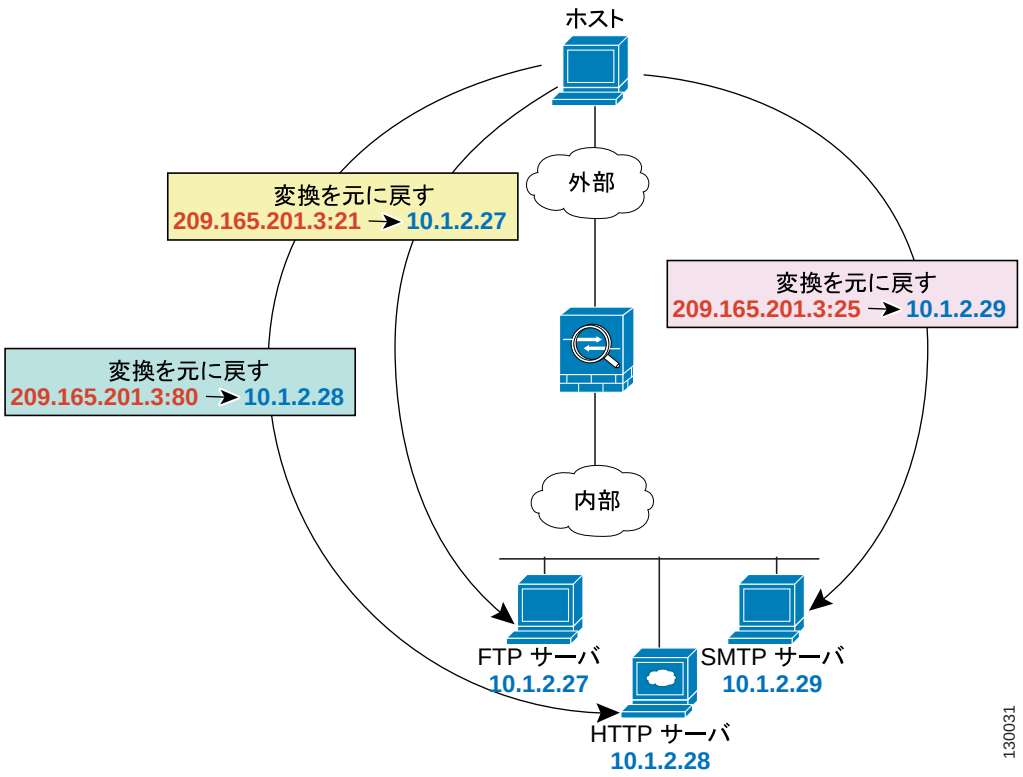
スタティック PAT は、プロトコル（TCP または UDP）および実際のアドレスとマッピング アドレスのポートを指定できる点を除いて、スタティック NAT と同じです。

この機能により、各文のポートが別である限り、複数の異なるスタティック文にまたが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）では、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、実際のネットワークでそれぞれ異なるサーバにある、FTP、HTTP、および SMTP にアクセスする複数のリモート ユーザにアドレスを 1 つだけ提供する場合、各サーバが使用するマッピング IP アドレスが同じでもポートが異なれば、サーバごとにスタティック PAT 文を指定できます（図 25-8 を参照）。

図 25-8　スタティック PAT



スタティック PAT を使用すると、ウェルノウン ポートから標準以外のポートへの変換や、その逆の変換も可能です。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、変換したポートを元のポート 8080 に戻すことができます。同様に、セキュリティを特に強化するには、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、変換したポートを元のポート 80 に戻すことができます。

NAT 制御がイネーブルな場合の NAT のバイパス

NAT 制御をイネーブルにすると、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。一部のホストを NAT の対象外とする場合、それらのホストについては NAT をバイパスできます。または、NAT 制御をディセーブルにすることもできます。たとえば、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は、NAT のバイパスが必要になることがあります（NAT をサポートしない検査エンジンの詳細については、P.24-3 の「アプリケーション プロトコル検査を使用するタイミング」を参照）。

次の 3 つの方法のいずれかを使用して、トラフィックが NAT をバイパスするように設定できます。どの方法も、検査エンジンとの互換性が実現されます。ただし、それぞれの方法で提供される機能は、次のようにわずかに異なります。

- 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。したがって、インターフェイス A にアクセスするときに実際のアドレスに対して標準の変換を実行し、インターフェイス B にアクセスするときにアイデンティティ NAT を使用するということは選択できません。一方、標準のダイナミック NAT では、アドレスを変換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 を適用する実際のアドレスは、アクセスリストで使用可能となっているすべてのネットワークでルーティング可能である必要があります。

  アイデンティティ NAT では、マッピング アドレスが実際のアドレスと同じであっても、外部から内部への接続を開始することはできません（インターフェイス アクセスリストで許可されている場合も同じです）。この機能が必要な場合は、スタティック アイデンティティ NAT または NAT 免除を使用します。
- 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。ポリシー NAT では、変換対象の実際のアドレスを決定するときに、実際のアドレスと宛先アドレスが指定されます（ポリシー NAT の詳細については、P.25-11 の「ポリシー NAT」を参照）。たとえば、内部アドレスが外部インターフェイスにアクセスするとき、宛先がサーバ A である場合は内部アドレスに対してスタティック アイデンティティ NAT を使用し、外部サーバ B にアクセスする場合は通常の変換を使用できます。
- 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、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。NAT 免除は、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。一方、NAT 免除では、変換対象の実際のアドレス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 免除を使用するとより詳細な制御が可能になります。ただし、ポリシー NAT とは異なり、NAT 免除では、アクセスリストのポートは考慮されません。NAT 免除では、最大 TCP 接続数など、接続制限を設定することもできません。

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。オプションで、送信元ポートと宛先ポートを指定することもできます。標準 NAT では、送信元アドレスのみが考慮され、宛先アドレスは考慮されません。たとえば、ポリシー NAT を使用すると、サーバ A にアクセスするときは実際のアドレスをマッピング アドレス A に変換し、サーバ B にアクセスするときは実際のアドレスをマッピング アドレス B に変換できます。

セカンダリ チャネルのアプリケーション検査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。ポートが予測できない場合は、ポリシーでセカンダリ チャネルの IP アドレスのみを指定する必要があります。このように設定すると、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。この結果、ホストはサーバと同じネットワークに存在するように見えるようになり、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

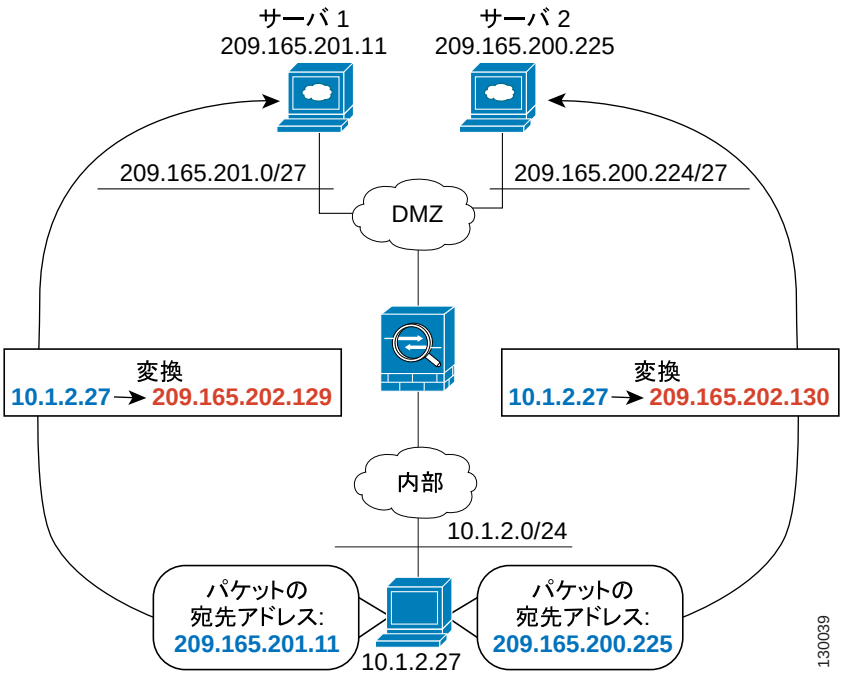
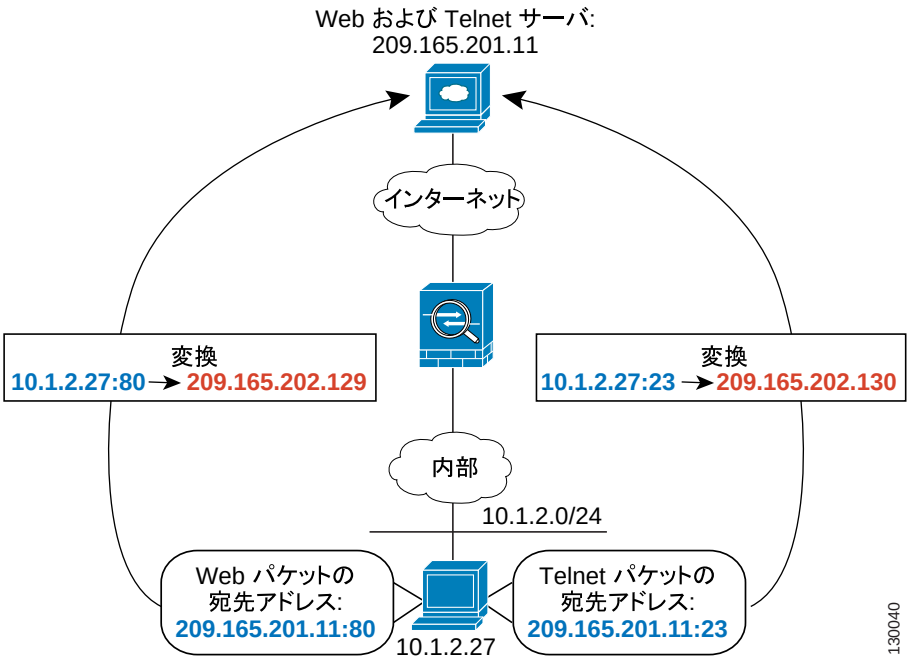


図 25-10 に、送信元ポートと宛先ポートの使用例を示します。10.1.2.0/24 ネットワークのホストは Web サービスと Telnet サービスの両方を利用するために 1 つのホストにアクセスします。ホストが Web サービスを利用するためにサーバにアクセスすると、実際のアドレスは 209.165.202.129 に変換されます。ホストが Telnet サービスを利用するために同じサーバにアクセスすると、実際のアドレスは 209.165.202.130 に変換されます。

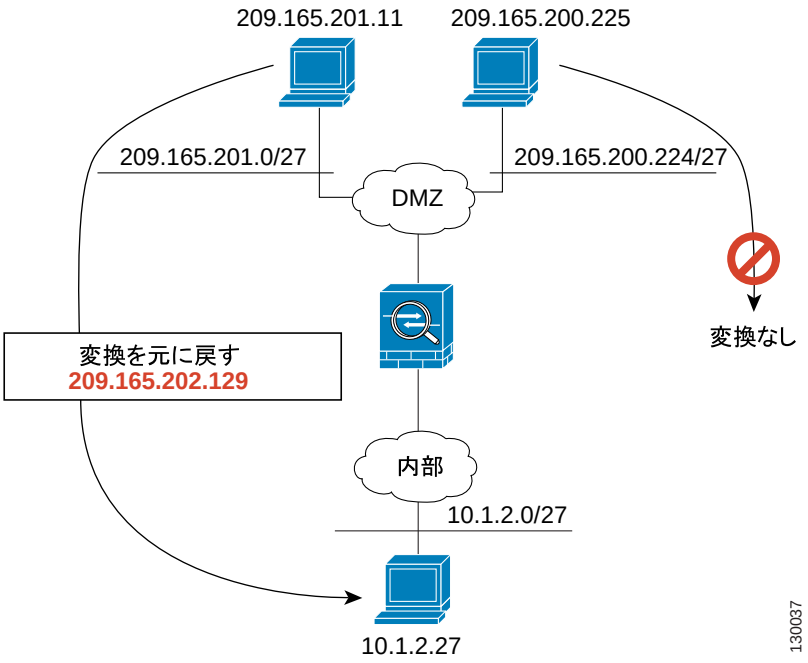
図 25-10　異なる宛先ポートを使用するポリシー NAT



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。変換済みのホストには、209.165.201.0/27 ネットワークを宛先または送信元とするトラフィックに限り実際のアドレスを変換するポリシー スタティック NAT 変換があります。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使用するポリシー 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 ではサポートされています。他のプロトコルへの NAT サポートの詳細については、P.24-3 の「アプリケーション プロトコル検査を使用するタイミング」を参照してください。

NAT と同じセキュリティ レベルのインターフェイス

同じセキュリティ レベルのインターフェイス間では、NAT 制御をイネーブルにしている場合であっても、NAT は必要ではありません。必要であれば、オプションで NAT を設定できます。ただし、NAT 制御がイネーブルの場合にダイナミック NAT を設定すると、NAT が必要になります。詳細については、P.25-4 の「NAT 制御」を参照してください。また、同じセキュリティのインターフェイス上でダイナミック NAT または PAT 対象として IP アドレスのグループを指定した場合、そのグループがセキュリティ レベルの低い（または同じ）インターフェイスにアクセスするときに、そのアドレス グループに対して NAT を実行する必要があります（NAT 制御がイネーブルになっていない場合も同じです）。スタティック NAT に指定されているトラフィックは影響を受けません。

（注）　同じセキュリティのインターフェイスに NAT を設定すると、セキュリティ アプライアンスで VoIP 検査エンジンがサポートされなくなります。このような検査エンジンには、Skinny、SIP、H.323 などがあります。サポートされる検査エンジンについては、P.24-3 の「アプリケーション プロトコル検査を使用するタイミング」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す。
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。アドレスの重複は許容されます。
4. 標準ダイナミック NAT : 最も適合するものを検出します。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 アドレスに関するガイドライン

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

  マッピング インターフェイス（トラフィックがセキュリティ アプライアンスから出るときに通過するインターフェイス）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 を使用してすべてのマッピング アドレス要求に応答することにより、実際のアドレスを宛先とする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。

- 一意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 を使用してすべてのマッピング アドレス要求に応答することにより、実際のアドレスを宛先とするトラフィックを代行受信します。OSPF を使用している場合、マッピング インターフェイス上のルートをアドバタイズすると、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場合）、またはスタティック ルーティングを使用する場合、マッピング アドレスを宛先とする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スタティック ルートをアップストリーム ルータに追加する必要があります。

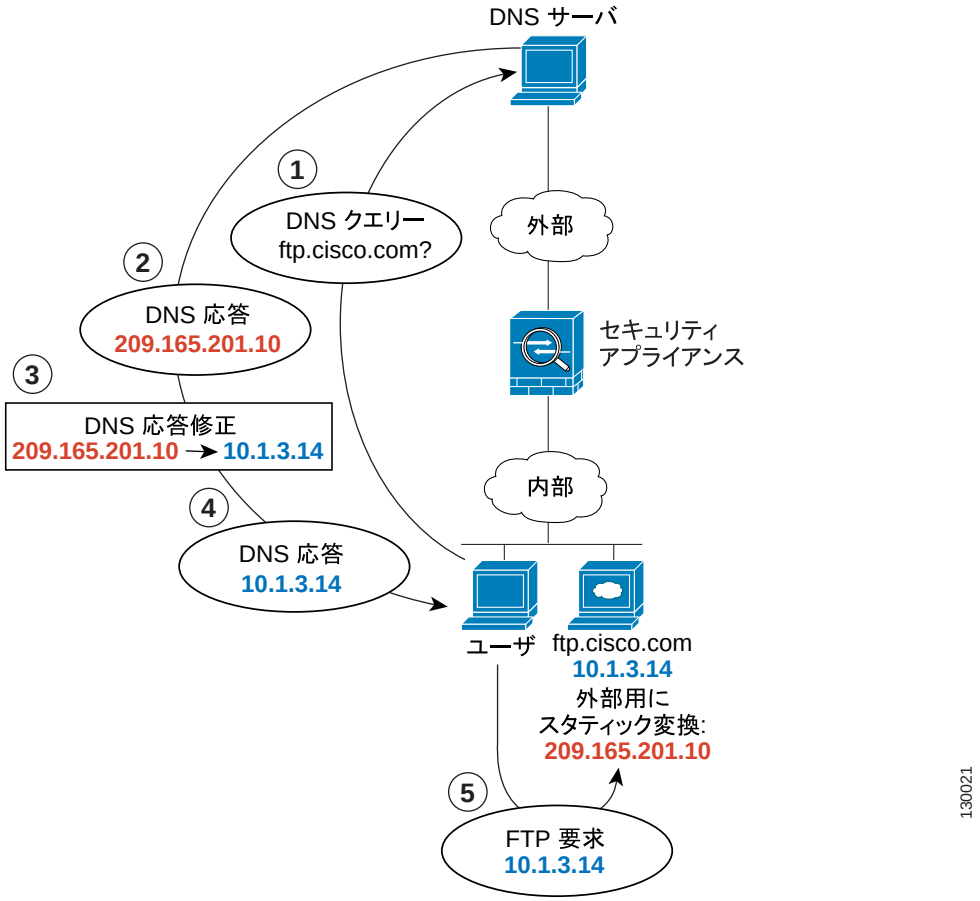
DNS と NAT

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。サーバ ftp.cisco.com は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 サーバから受信します。

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）を返します。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文を参照し、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しようとします。

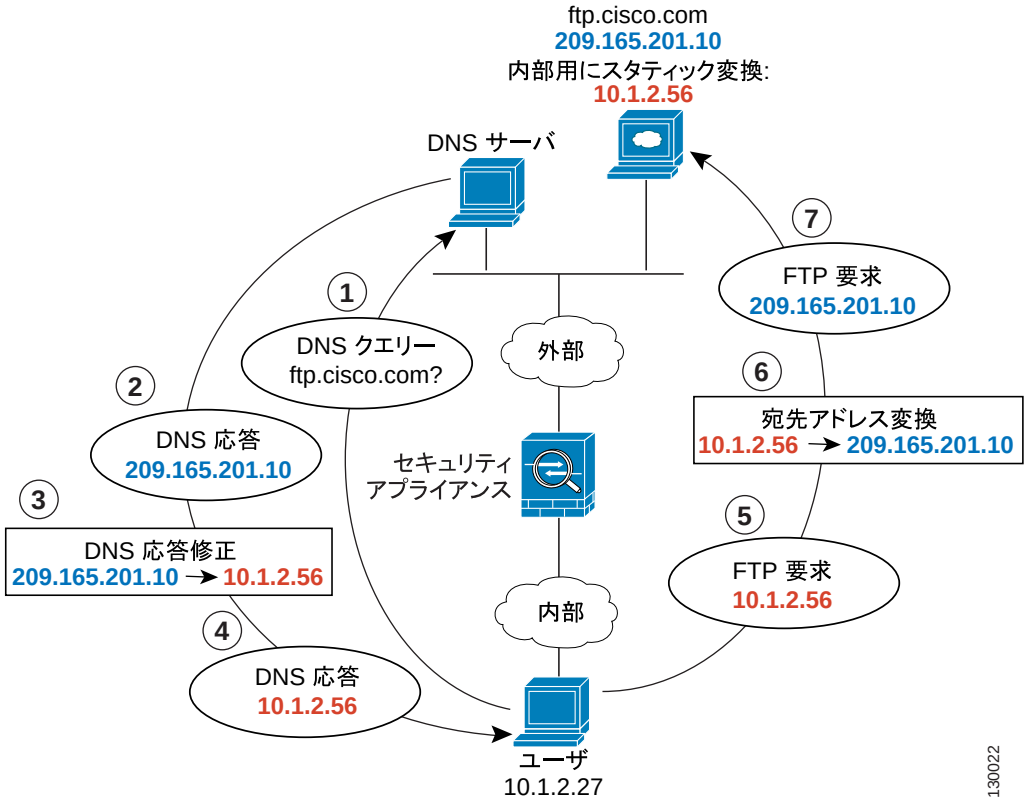
図 25-12　DNS 応答修正



（注）　別のネットワーク（DMZ など）上のユーザも外部 DNS サーバから ftp.cisco.com の IP アドレスを要求した場合、ユーザがスタティック ルールで参照される内部インターフェイス上にない場合でも、DNS 応答内の IP アドレスはこのユーザ用にも修正されます。

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、内部ユーザが ftp.cisco.com のアドレスを DNS サーバに要求すると、DNS サーバは応答で実際のアドレス 209.165.20.10 を返します。内部ユーザは ftp.cisco.com のマッピング アドレス（10.1.2.56）を使用する必要があるため、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に移動するパケットは NAT ルールに一致する必要があります。詳細については、P.25-4 の「NAT 制御」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。オプションで、送信元ポートと宛先ポートを指定することもできます。標準 NAT では、送信元アドレスのみが考慮され、宛先アドレスは考慮されません。詳細については、P.25-11 の「ポリシー NAT」を参照してください。

ここでは、次の項目について説明します。

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。次の項目を取り上げます。

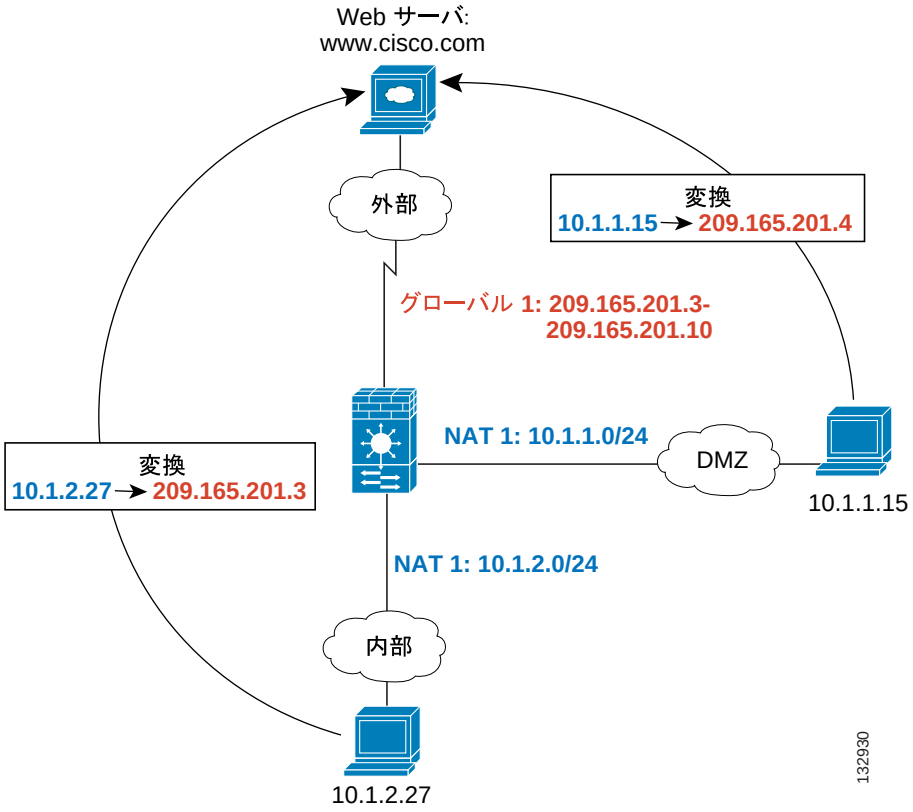
プール ID を使用した実際のアドレスとグローバル プールのペア

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および 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から出るときにマッピング プールまたは PAT アドレスを共有します（図 25-14 を参照）。

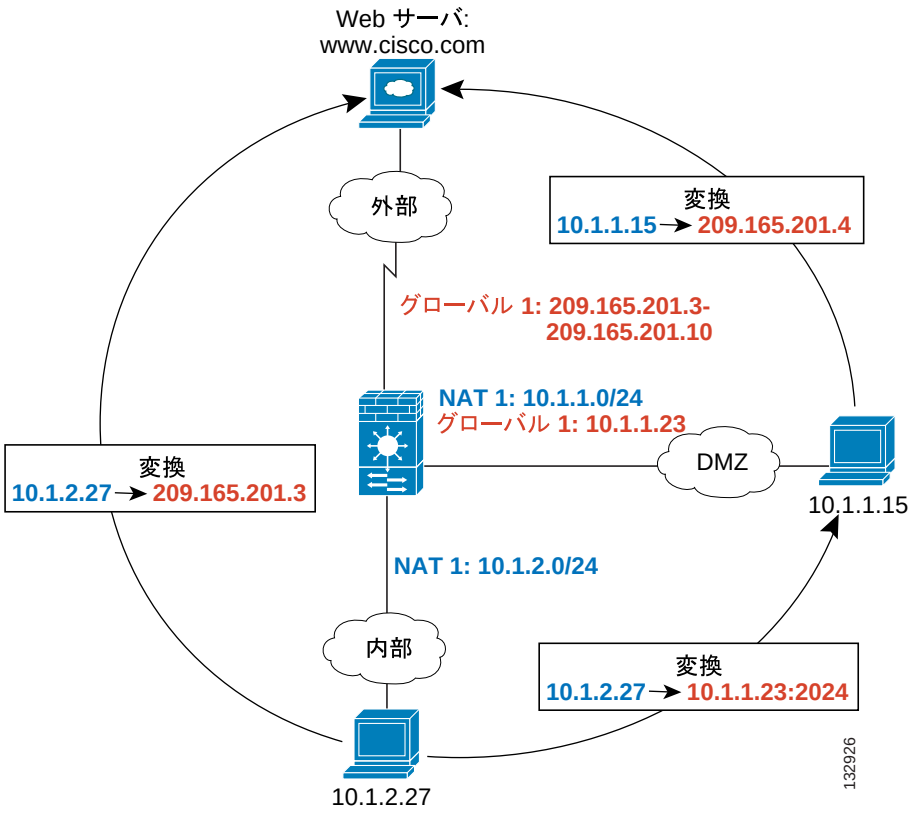
図 25-14　複数のインターフェイス上の同じグローバル プールを使用する NAT ルール



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）。

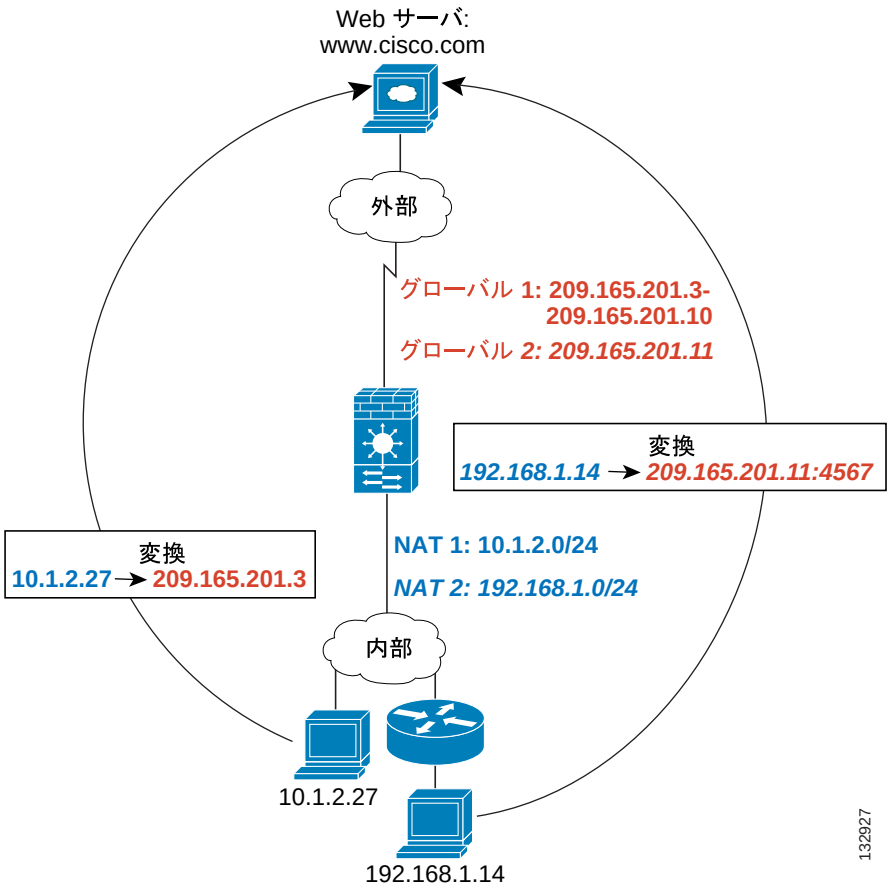
図 25-15　複数のインターフェイス上の同じ ID を使用する NAT ルールとグローバル プール



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。

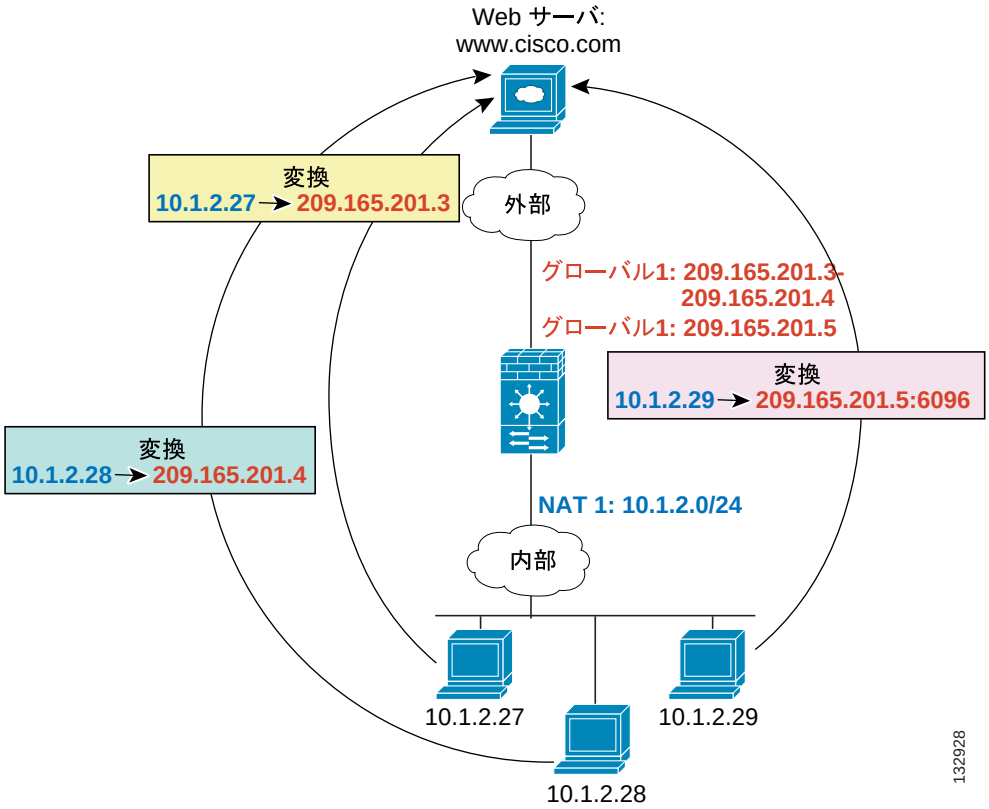
図 25-16　異なる NAT ID



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つことができます。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。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することもできます。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 アドレスを持つこともできます（図 25-17 を参照）。

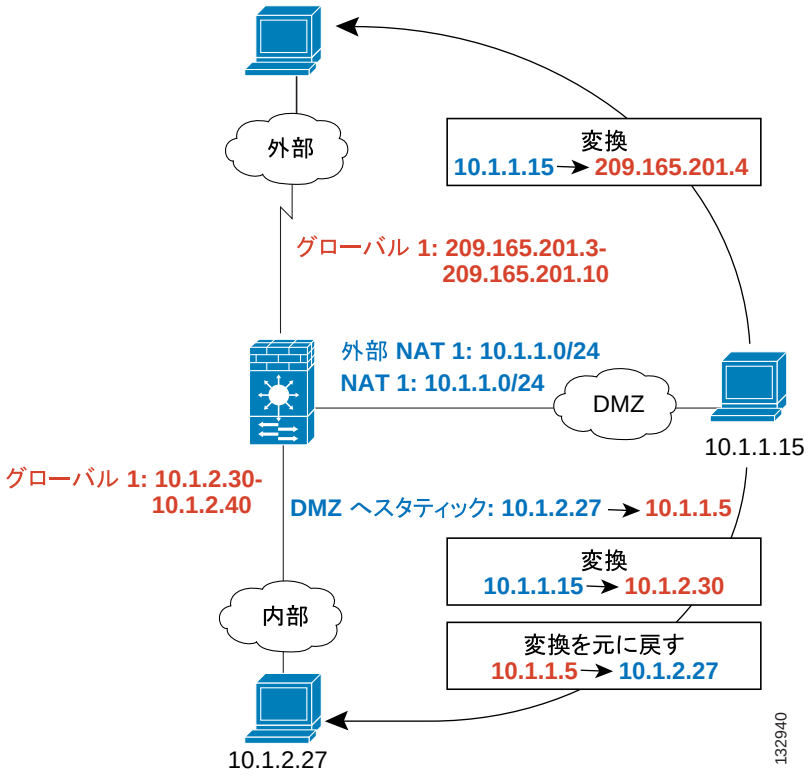
図 25-17　NAT と PAT を一緒に使用する場合



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 と内部 NAT の組み合せ



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 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、P.25-17 の「ダイナミック NAT の実装」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作成するか、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と、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　（オプション）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、P.25-20 の「同じグローバル プール内の複数のアドレス」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 ペインから、**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、P.25-20 の「同じグローバル プール内の複数のアドレス」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 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、P.25-17 の「ダイナミック NAT の実装」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。P.25-22 の「グローバル プールの管理」を参照してください。
- グローバル プール 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　（オプション）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。このオプションにより、クライアントに対する DNS 応答内のアドレスが書き換えられます。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。一般に、他のインターフェイスからのアクセスを許可する必要のあるホストはスタティック変換を使用するため、このオプションは多くの場合スタティック ルールで使用されます。詳細については、P.25-15 の「DNS と NAT」を参照してください。

ステップ 6　（オプション）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 ルールを使用して設定することもできます（P.27-7 の「接続の設定」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でディセーブルにされている場合、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。各 TCP 接続には、2 つの Initial Sequence Number（ISN; 初期シーケンス番号）があります。1 つはクライアントが生成し、もう 1 つはサーバが生成します。セキュリティ アプライアンスは、着信および発信の両方向で通過する TCP SYN の ISN をランダム化します。

  保護されているホストの初期シーケンス番号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 を予想してセッションを乗っ取ることができないようにします。

  TCP の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。次の例を参考にしてください。

  - 別のインライン ファイアウォールも初期シーケンス番号をランダム化している場合。両方のファイアウォールでランダム化を実行する必要はありません。ただし、ランダム化によってトラフィックに影響が出ることはありません。
  - セキュリティ アプライアンスを経由する eBGP マルチホップを使用し、さらに eBGP ピアが MD5 を使用する場合。ランダム化によって MD5 チェックサムが破損します。
  - WAAS デバイスを使用する場合。WAAS デバイスでは、セキュリティ アプライアンスが接続のシーケンス番号をランダム化しないことが要求されます。

- **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 UDP Connections** : UDP 接続の最大数を 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** : ホストごとの初期接続の最大数を 65,536 までの範囲で指定します。初期接続は、送信元と宛先の間で必要なハンドシェイクを終了していない接続要求です。この制限により、TCP 代行受信機能をイネーブルにします。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 代行受信により、TCP SYN パケットによってインターフェイスをフラッディングさせる DoS 攻撃から内部システムを保護します。初期接続の制限値を超えると、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へ送信される 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。SYN クッキーは、検証プロセス中に使用され、ドロップされる有効なトラフィックの量を最小限に抑えるのに役立ちます。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、P.25-20 の「同じグローバル プール内の複数のアドレス」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 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、P.25-17 の「ダイナミック NAT の実装」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。P.25-22 の「グローバル プールの管理」を参照してください。
- グローバル プール 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　（オプション）Description フィールドに説明を入力します。

ステップ 7　（オプション）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。このオプションにより、クライアントに対する DNS 応答内のアドレスが書き換えられます。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。一般に、他のインターフェイスからのアクセスを許可する必要のあるホストはスタティック変換を使用するため、このオプションは多くの場合スタティック ルールで使用されます。詳細については、P.25-15 の「DNS と NAT」を参照してください。

ステップ 8　（オプション）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 ルールを使用して設定することもできます（P.27-7 の「接続の設定」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でディセーブルにされている場合、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。各 TCP 接続には、2 つの Initial Sequence Number（ISN; 初期シーケンス番号）があります。1 つはクライアントが生成し、もう 1 つはサーバが生成します。セキュリティ アプライアンスは、着信および発信の両方向で通過する TCP SYN の ISN をランダム化します。

  保護されているホストの初期シーケンス番号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 を予想してセッションを乗っ取ることができないようにします。

TCP の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。次の例を参考にしてください。

- 別のインライン ファイアウォールも初期シーケンス番号をランダム化している場合。両方のファイアウォールでランダム化を実行する必要はありません。ただし、ランダム化によってトラフィックに影響が出ることはありません。
- セキュリティ アプライアンスを経由する eBGP マルチホップを使用し、さらに eBGP ピアが MD5 を使用する場合。ランダム化によって MD5 チェックサムが破損します。
- WAAS デバイスを使用する場合。WAAS デバイスでは、セキュリティ アプライアンスが接続のシーケンス番号をランダム化しないことが要求されます。

- **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 UDP Connections** : UDP 接続の最大数を 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** : ホストごとの初期接続の最大数を 65,536 までの範囲で指定します。初期接続は、送信元と宛先の間で必要なハンドシェイクを終了していない接続要求です。この制限により、TCP 代行受信機能をイネーブルにします。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 代行受信により、TCP SYN パケットによってインターフェイスをフラッディングさせる DoS 攻撃から内部システムを保護します。初期接続の制限値を超えると、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へ送信される 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。SYN クッキーは、検証プロセス中に使用され、ドロップされる有効なトラフィックの量を最小限に抑えるのに役立ちます。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、スタティック、ポリシーの NAT、PAT、またはアイデンティティ NAT を使用した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、P.25-9 の「スタティック NAT」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。オプションで、送信元ポートと宛先ポートを指定することもできます。標準 NAT では、送信元アドレスのみが考慮され、宛先アドレスは考慮されません。詳細については、P.25-11 の「ポリシー NAT」を参照してください。

スタティック NAT を使用すると、実際のアドレスをマッピング IP アドレスに、また実際のポートをマッピング ポートに変換できます。実際のポートを同じポートに変換することを選択して、特定のタイプのトラフィックだけを変換することができます。または、別のポートに変換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検査を必要とするアプリケーションの場合（FTP や VoIP など）、セキュリティ アプライアンスは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、P.25-9 の「スタティック PAT」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 は、実際の IP アドレスを同じ IP アドレスに変換します。

ここでは、次の項目について説明します。

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

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 ペインから、**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　（オプション）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　（オプション）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。このオプションにより、クライアントに対する DNS 応答内のアドレスが書き換えられます。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、P.25-15 の「DNS と NAT」を参照してください。

ステップ 8　（オプション）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 ルールを使用して設定することもできます（P.27-7 の「接続の設定」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でディセーブルにされている場合、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。各 TCP 接続には、2 つの Initial Sequence Number（ISN; 初期シーケンス番号）があります。1 つはクライアントが生成し、もう 1 つはサーバが生成します。セキュリティ アプライアンスは、着信および発信の両方向で通過する TCP SYN の ISN をランダム化します。

  保護されているホストの初期シーケンス番号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 を予想してセッションを乗っ取ることができないようにします。

  TCP の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。次の例を参考にしてください。

  - 別のインライン ファイアウォールも初期シーケンス番号をランダム化している場合。両方のファイアウォールでランダム化を実行する必要はありません。ただし、ランダム化によってトラフィックに影響が出ることはありません。
  - セキュリティ アプライアンスを経由する eBGP マルチホップを使用し、さらに eBGP ピアが MD5 を使用する場合。ランダム化によって MD5 チェックサムが破損します。
  - WAAS デバイスを使用する場合。WAAS デバイスでは、セキュリティ アプライアンスが接続のシーケンス番号をランダム化しないことが要求されます。
- **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 UDP Connections**：UDP 接続の最大数を 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** : ホストごとの初期接続の最大数を 65,536 までの範囲で指定します。初期接続は、送信元と宛先の間で必要なハンドシェイクを終了していない接続要求です。この制限により、TCP 代行受信機能をイネーブルにします。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 代行受信により、TCP SYN パケットによってインターフェイスをフラッディングさせる DoS 攻撃から内部システムを保護します。初期接続の制限値を超えると、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へ送信される 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。SYN クッキーは、検証プロセス中に使用され、ドロップされる有効なトラフィックの量を最小限に抑えるのに役立ちます。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　（オプション）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　（オプション）Description フィールドに説明を入力します。

ステップ 9　（オプション）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。このオプションにより、クライアントに対する DNS 応答内のアドレスが書き換えられます。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、P.25-15 の「DNS と NAT」を参照してください。

ステップ 10（オプション）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 ルールを使用して設定することもできます（P.27-7 の「接続の設定」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でディセーブルにされている場合、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。各 TCP 接続には、2 つの Initial Sequence Number（ISN; 初期シーケンス番号）があります。1 つはクライアントが生成し、もう 1 つはサーバが生成します。セキュリティ アプライアンスは、着信および発信の両方向で通過する TCP SYN の ISN をランダム化します。

  保護されているホストの初期シーケンス番号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 を予想してセッションを乗っ取ることができないようにします。

  TCP の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。次の例を参考にしてください。

  - 別のインライン ファイアウォールも初期シーケンス番号をランダム化している場合。両方のファイアウォールでランダム化を実行する必要はありません。ただし、ランダム化によってトラフィックに影響が出ることはありません。
  - セキュリティ アプライアンスを経由する eBGP マルチホップを使用し、さらに eBGP ピアが MD5 を使用する場合。ランダム化によって MD5 チェックサムが破損します。
  - WAAS デバイスを使用する場合。WAAS デバイスでは、セキュリティ アプライアンスが接続のシーケンス番号をランダム化しないことが要求されます。
- **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 UDP Connections**：UDP 接続の最大数を 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**：ホストごとの初期接続の最大数を 65,536 までの範囲で指定します。初期接続は、送信元と宛先の間で必要なハンドシェイクを終了していない接続要求です。この制限により、TCP 代行受信機能をイネーブルにします。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 代行受信により、TCP SYN パケットによってインターフェイスをフラッディングさせる DoS 攻撃から内部システムを保護します。初期接続の制限値を超えると、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へ送信される 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。SYN クッキーは、検証プロセス中に使用され、ドロップされる有効なトラフィックの量を最小限に抑えるのに役立ちます。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 免除は、アドレスの変換を免除し、実際のホストとリモート ホストの両方が接続を開始できるようにします。NAT 免除では、免除対象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、P.25-10 の「NAT 制御がイネーブルな場合の NAT のバイパス」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 ペインで、**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　（オプション）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　（オプション）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一致すると、それ以降のルールはチェックされません。

NAT のフィールドの説明

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

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。追加するルールのタイプをドロップダウン リストから選択します。
  - 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、重複するルールがあると順序によって評価が異なります。
- 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、新しいルールを同じパラメータで開始できます。
- Paste: コピーまたは切り取ったルールのパラメータがあらかじめ入力された Add/Edit Rule ダイアログボックスが開きます。そこでルールを変更し、テーブルに追加します。Paste ボタンをクリックすると、選択したルールの上に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、選択したルールの後に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。Filter フィールドを非表示にするには、もう一度 **Find** をクリックします。

  - 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、複数の基準の集合で、保存して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。それ以外の基準はすべて **is** 条件を使用します。
  - Filter フィールド : Interface タイプの場合、このフィールドはドロップダウン リストになり、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、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。アドレスを手動で入力するか、または **...** ボタンをクリックして Browse Address ダイアログボックスを開いてアドレスを参照します。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。プロトコル タイプを手動で入力するか、または **...** ボタンをクリックして Browse Translated Service ダイアログボックスを開き、プロトコル タイプを参照します。
  - Filter : フィルタリングを実行します。
  - 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を開き、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 領域を表示します。この図では、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、およびアクションを示しています。
- 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 Packet Tracer ツールを開きます。

NAT Rules テーブル

テーブル セルをダブルクリックすると、カラムの内容を編集できます。カラム ヘッダーをダブルクリックすると、選択したカラムが並び替えキーとして使用され、テーブルが英数字の昇順に並び替わります。ルールを右クリックすると、Insert および Insert After 項目と共に、ボタンで表されているオプションがすべて上に表示されます。これらの項目では、選択したルールの前に新しいルールが挿入されるか（Insert）、選択したルールの後ろに新しいルールが挿入されます（Insert After）。

- 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。このオプションにより、クライアントに対する DNS 応答内のアドレスが書き換えられます。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、P.25-15 の「DNS と NAT」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：ホストごとの初期接続の最大数を 65,536 までの範囲で指定します。初期接続は、送信元と宛先の間で必要なハンドシェイクを終了していない接続要求です。この制限により、TCP 代行受信機能をイネーブルにします。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 代行受信により、TCP SYN パケットによってインターフェイスをフラッディングさせる DoS 攻撃から内部システムを保護します。初期接続の制限値を超えると、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へ送信される 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。SYN クッキーは、検証プロセス中に使用され、ドロップされる有効なトラフィックの量を最小限に抑えるのに役立ちます。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 接続の最大数を 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。各 TCP 接続には、2 つの Initial Sequence Number（ISN; 初期シーケンス番号）があります。1 つはクライアントが生成し、もう 1 つはサーバが生成します。セキュリティ アプライアンスは、着信および発信の両方向で通過する TCP SYN の ISN をランダム化します。

    保護されているホストの初期シーケンス番号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 を予想してセッションを乗っ取ることができないようにします。

    TCP の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。次の例を参考にしてください。

    別のインライン ファイアウォールも初期シーケンス番号をランダム化している場合。両方のファイアウォールでランダム化を実行する必要はありません。ただし、ランダム化によってトラフィックに影響が出ることはありません。

    セキュリティ アプライアンスを経由する eBGP マルチホップを使用し、さらに eBGP ピアが MD5 を使用する場合。ランダム化によって MD5 チェックサムが破損します。

    WAAS デバイスを使用する場合。WAAS デバイスでは、セキュリティ アプライアンスが接続のシーケンス番号をランダム化しないことが要求されます。

    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、P.25-4 の「NAT 制御」を参照してください。
- Addresses：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、または検索できるタブです。
- 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：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 プールを管理するためのタブです。

モード

次の表に、この機能を使用できるモードを示します。

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 インターフェイスおよび 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。このオプションにより、クライアントに対する DNS 応答内のアドレスが書き換えられます。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、P.25-15 の「DNS と NAT」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 : ホストごとの初期接続の最大数を 65,536 までの範囲で指定します。初期接続は、送信元と宛先の間で必要なハンドシェイクを終了していない接続要求です。この制限により、TCP 代行受信機能をイネーブルにします。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 代行受信により、TCP SYN パケットによってインターフェイスをフラッディングさせる DoS 攻撃から内部システムを保護します。初期接続の制限値を超えると、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へ送信される 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。SYN クッキーは、検証プロセス中に使用され、ドロップされる有効なトラフィックの量を最小限に抑えるのに役立ちます。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 接続の最大数を 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。各 TCP 接続には、2 つの Initial Sequence Number（ISN; 初期シーケンス番号）があります。1 つはクライアントが生成し、もう 1 つはサーバが生成します。セキュリティ アプライアンスは、着信および発信の両方向で通過する TCP SYN の ISN をランダム化します。

  保護されているホストの初期シーケンス番号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 を予想してセッションを乗っ取ることができないようにします。

  TCP の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。次の例を参考にしてください。

  別のインライン ファイアウォールも初期シーケンス番号をランダム化している場合。両方のファイアウォールでランダム化を実行する必要はありません。ただし、ランダム化によってトラフィックに影響が出ることはありません。

  セキュリティ アプライアンスを経由する eBGP マルチホップを使用し、さらに eBGP ピアが MD5 を使用する場合。ランダム化によって MD5 チェックサムが破損します。

  WAAS デバイスを使用する場合。WAAS デバイスでは、セキュリティ アプライアンスが接続のシーケンス番号をランダム化しないことが要求されます。

  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

次の表に、この機能を使用できるモードを示します。

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：グループ 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。このオプションにより、クライアントに対する DNS 応答内のアドレスが書き換えられます。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、P.25-15 の「DNS と NAT」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：ホストごとの初期接続の最大数を 65,536 までの範囲で指定します。初期接続は、送信元と宛先の間で必要なハンドシェイクを終了していない接続要求です。この制限により、TCP 代行受信機能をイネーブルにします。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 代行受信により、TCP SYN パケットによってインターフェイスをフラッディングさせる DoS 攻撃から内部システムを保護します。初期接続の制限値を超えると、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へ送信される 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。SYN クッキーは、検証プロセス中に使用され、ドロップされる有効なトラフィックの量を最小限に抑えるのに役立ちます。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 接続の最大数を 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。各 TCP 接続には、2 つの Initial Sequence Number（ISN; 初期シーケンス番号）があります。1 つはクライアントが生成し、もう 1 つはサーバが生成します。セキュリティ アプライアンスは、着信および発信の両方向で通過する TCP SYN の ISN をランダム化します。

    保護されているホストの初期シーケンス番号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 を予想してセッションを乗っ取ることができないようにします。

    TCP の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。次の例を参考にしてください。

    別のインライン ファイアウォールも初期シーケンス番号をランダム化している場合。両方のファイアウォールでランダム化を実行する必要はありません。ただし、ランダム化によってトラフィックに影響が出ることはありません。

    セキュリティ アプライアンスを経由する eBGP マルチホップを使用し、さらに eBGP ピアが MD5 を使用する場合。ランダム化によって MD5 チェックサムが破損します。

    WAAS デバイスを使用する場合。WAAS デバイスでは、セキュリティ アプライアンスが接続のシーケンス番号をランダム化しないことが要求されます。

    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

次の表に、この機能を使用できるモードを示します。

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

次の表に、この機能を使用できるモードを示します。

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（オプション）：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（オプション）：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

次の表に、この機能を使用できるモードを示します。

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 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。

    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 インターフェイスおよび 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。このオプションにより、クライアントに対する DNS 応答内のアドレスが書き換えられます。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、P.25-15 の「DNS と NAT」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：ホストごとの初期接続の最大数を 65,536 までの範囲で指定します。初期接続は、送信元と宛先の間で必要なハンドシェイクを終了していない接続要求です。この制限により、TCP 代行受信機能をイネーブルにします。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 代行受信により、TCP SYN パケットによってインターフェイスをフラッディングさせる DoS 攻撃から内部システムを保護します。初期接続の制限値を超えると、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へ送信される 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。SYN クッキーは、検証プロセス中に使用され、ドロップされる有効なトラフィックの量を最小限に抑えるのに役立ちます。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 接続の最大数を 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。各 TCP 接続には、2 つの Initial Sequence Number（ISN; 初期シーケンス番号）があります。1 つはクライアントが生成し、もう 1 つはサーバが生成します。セキュリティ アプライアンスは、着信および発信の両方向で通過する TCP SYN の ISN をランダム化します。

    保護されているホストの初期シーケンス番号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 を予想してセッションを乗っ取ることができないようにします。

    TCP の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。次の例を参考にしてください。

    別のインライン ファイアウォールも初期シーケンス番号をランダム化している場合。両方のファイアウォールでランダム化を実行する必要はありません。ただし、ランダム化によってトラフィックに影響が出ることはありません。

    セキュリティ アプライアンスを経由する eBGP マルチホップを使用し、さらに eBGP ピアが MD5 を使用する場合。ランダム化によって MD5 チェックサムが破損します。

    WAAS デバイスを使用する場合。WAAS デバイスでは、セキュリティ アプライアンスが接続のシーケンス番号をランダム化しないことが要求されます。

    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

次の表に、この機能を使用できるモードを示します。

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 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。

    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：グループ 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。このオプションにより、クライアントに対する DNS 応答内のアドレスが書き換えられます。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、P.25-15 の「DNS と NAT」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 : ホストごとの初期接続の最大数を 65,536 までの範囲で指定します。初期接続は、送信元と宛先の間で必要なハンドシェイクを終了していない接続要求です。この制限により、TCP 代行受信機能をイネーブルにします。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 代行受信により、TCP SYN パケットによってインターフェイスをフラッディングさせる DoS 攻撃から内部システムを保護します。初期接続の制限値を超えると、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へ送信される 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。SYN クッキーは、検証プロセス中に使用され、ドロップされる有効なトラフィックの量を最小限に抑えるのに役立ちます。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 接続の最大数を 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。各 TCP 接続には、2 つの Initial Sequence Number（ISN; 初期シーケンス番号）があります。1 つはクライアントが生成し、もう 1 つはサーバが生成します。セキュリティ アプライアンスは、着信および発信の両方向で通過する TCP SYN の ISN をランダム化します。

  保護されているホストの初期シーケンス番号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 を予想してセッションを乗っ取ることができないようにします。

  TCP の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。次の例を参考にしてください。

  別のインライン ファイアウォールも初期シーケンス番号をランダム化している場合。両方のファイアウォールでランダム化を実行する必要はありません。ただし、ランダム化によってトラフィックに影響が出ることはありません。

  セキュリティ アプライアンスを経由する eBGP マルチホップを使用し、さらに eBGP ピアが MD5 を使用する場合。ランダム化によって MD5 チェックサムが破損します。

  WAAS デバイスを使用する場合。WAAS デバイスでは、セキュリティ アプライアンスが接続のシーケンス番号をランダム化しないことが要求されます。

  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

次の表に、この機能を使用できるモードを示します。

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 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。

    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

次の表に、この機能を使用できるモードを示します。

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
•	•	•	•	—