スタティック NAT とダイナミック NAT 変換の設定

NAT の概要

ネットワークアドレス変換（NAT）は、登録されていないIPアドレスを使用してインターネットへ接続するプライベート IP インターネットワークをイネーブルにします。NAT はデバイス（通常は、2 つのネットワーク間の接続に使用される）で動作します。また、パケットを別のネットワークに転送する前に、社内ネットワークの（グローバルで固有のアドレスではなく）プライベート IP アドレスを正規の IP アドレスに変換します。NAT は、ネットワーク全体に対して1つのIPアドレスだけを外部にアドバタイズするように設定できます。この機能により、1つのIPアドレスの後ろに内部ネットワーク全体を効果的に隠すことで、セキュリティが強化されます。

NAT が設定されたデバイスには、内部ネットワークと外部ネットワークのそれぞれに接続するインターフェイスが少なくとも 1 つずつあります。標準的な環境では、NAT はスタブ ドメインとバックボーンの間の出口ルータに設定されます。パケットがドメインから出て行くと

き、NAT はローカルで意味のある送信元 アドレスをグローバルで一意の アドレスに変換します。パケットがドメインに入ってくる際は、NAT はグローバルに一意な宛先アドレスをローカル アドレスに変換します。出口点が複数存在する場合、個々の NAT は同じ変換テーブルを持っている必要があります。

NAT は RFC 1631 に記述されています。

スタティック NAT に関する情報

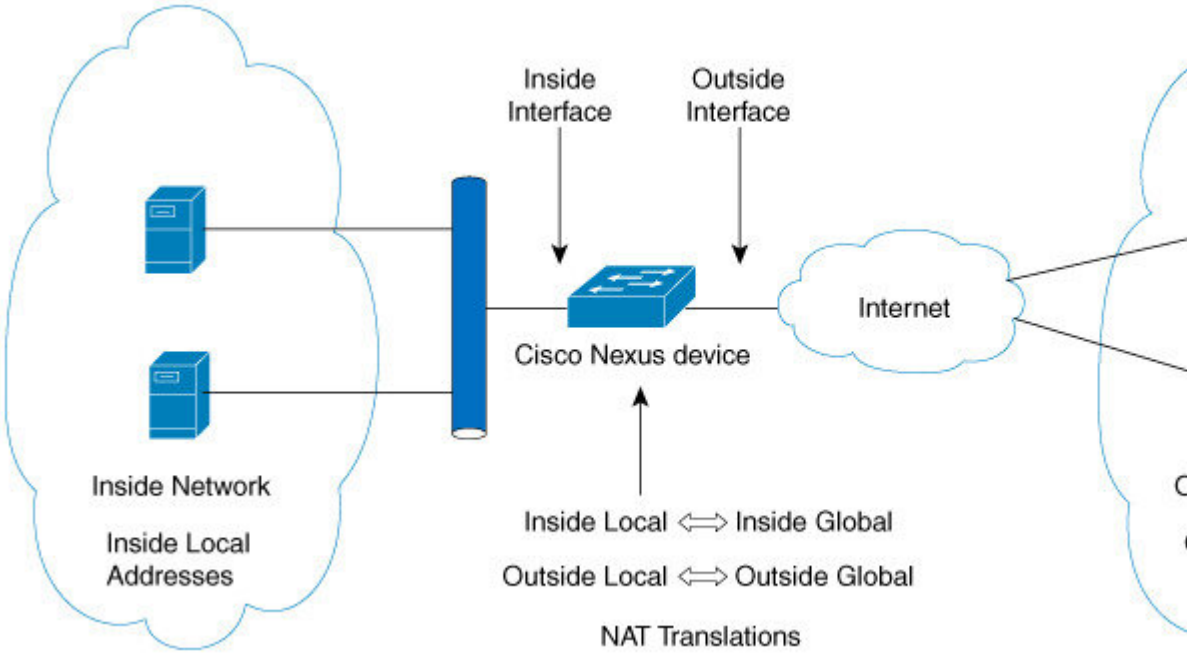
スタティック ネットワーク アドレス変換（NAT）を使用すると、ユーザは内部ローカル アドレスから外部グローバル アドレスへの 1 対 1 変換を設定することができます。これにより、内部から外部トラフィックおよび外部から内部トラフィックへの IP アドレスとポート番号の両方の変換が可能になります。Cisco Nexus デバイス はヒットレス NAT をサポートします。これは、既存の NAT トラフィック フローに影響を与えずに NAT 設定で NAT 変換を追加または削除できることを意味します。

スタティック NAT では、プライベート アドレスからパブリック アドレスへの固定変換が作成されます。スタティック NAT では 1 対 1 ベースでアドレスが割り当てられるため、プライベート アドレスと同じ数のパブリック アドレスが必要です。スタティック NAT では、パブリック 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 およびポート アドレス変換（PAT）では、各ホストは後続する変換ごとに異なるアドレスまたはポートを使用します。ダイナミック NAT とスタティック NAT 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。

次の図に、一般的なスタティック NAT のシナリオを示します。変換は常にアクティブであるため、変換対象ホストとリモート ホストの両方で接続を生成でき、マップ アドレスは **static** コマンドによって静的に割り当てられます。

図 *1* : スタティック *NAT*



次に、スタティック NAT を理解するのに役立つ主な用語を示します。

- NAT の内部インターフェイス：プライベート ネットワークに面するレイヤ 3 インターフェイス。
- NAT の外部インターフェイス：パブリック ネットワークに面するレイヤ 3 インターフェイス。
- ローカルアドレス：ネットワークの内部（プライベート）部分に表示される任意のアドレス。
- グローバルアドレス：ネットワークの外部（パブリック）部分に表示される任意のアドレス。
- 正規の IP アドレス：Network Information Center（NIC）やサービス プロバイダーにより割り当てられたアドレス。
- 内部ローカル アドレス：内部ネットワーク上のホストに割り当てられた IP アドレス。このアドレスは正規の IP アドレスである必要はありません。
- 外部ローカル アドレス：内部ネットワークから見た外部ホストの IP アドレス。これは、内部ネットワークのルーティング可能なアドレス空間から割り当てられるため、正規のアドレスである必要はありません。
- 内部グローバルアドレス：1 つ以上の内部ローカル IP アドレスを外部に対して表すために使用できる正規の IP アドレス。

- 外部グローバル アドレス：ホスト所有者が外部ネットワーク上のホストに割り当てる IP アドレス。このアドレスは、ルート可能なアドレスまたはネットワーク空間から割り当てられた正規のアドレスです。

ダイナミック NAT の概要

ダイナミック Network Address Translation (NAT) では、実際の IP 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 IP アドレスのプールに変換されます。ダイナミックNATは、未登録のIPアドレスと登録済みのIPアドレスの間に 1 対 1 のマッピングを確立します。ただし、マッピングは、通信時に使用可能な登録済み IP アドレスによって異なります。

ダイナミック NAT を設定すると、使用している内部ネットワークと外部ネットワークまたはインターネットとの間に、ファイウォールが自動的に構築されます。ダイナミック NAT は、スタブ ドメイン内で発信された接続のみを許可します。外部ネットワーク上のデバイスは、ネットワーク内のデバイス側で接続を開始していない限り、そのデバイスに接続できません。

ダイナミック NAT の場合、変換対象のトラフィックをデバイスが受信するまでは、NAT 変換テーブルには変換エントリが存在しません。ダイナミック変換では、新しいエントリ用のスペースが必要になると、使用されていないものが、クリアつまりタイムアウトされます。通常、NAT 変換エントリは、Ternary Content Addressable Memory（TCAM）エントリが制限されるとクリアされます。ダイナミック NAT 変換のデフォルトの最小タイムアウトは 30 分です。**ip nat translation sampling-timeout**コマンドのサンプリングタイムアウトの最小値は、30 分から 15 分に短縮されました。

ダイナミック NAT 変換のタイムアウトには、サンプリングタイムアウト値と TCP または UDP タイムアウト値の両方が含まれます。サンプリングタイムアウトは、デバイスが動的変換アクティビティをチェックするまでの時間を指定します。デフォルト値は 12 時間です。他のすべてのタイムアウトは、サンプリングタイムアウトが生じた後にのみ開始されます。サンプリングタイムアウト後、デバイスはこの変換にヒットしているパケットを検査します。このチェックは、TCP または UDP のタイムアウト期間に行われます。TCP または UDP タイムアウト期間にパケットがなかった場合、変換はクリアされます。変換でアクティビティが検出されると、チェックはすぐに停止され、サンプリングタイムアウト期間が開始されます。

この新しいサンプリングタイムアウト期間を待機した後、デバイスはダイナミック変換アクティビティを再度チェックします。アクティビティチェック中に、TCAM はダイナミック NAT 変換に一致するパケットのコピーを CPU に送信します。コントロール プレーン ポリシング（CoPP）が低しきい値に設定されている場合、TCP または UDP パケットがCPUに到達しないことがあり、CPU は NAT 変換が非アクティブであると見なします。

ダイナミック NATは、ポート アドレス変換（PAT）およびアクセス コントロール リスト（ACL）をサポートします。PAT はオーバーロードとも呼ばれ、複数の未登録 IP アドレスを、複数の異なるポートを使用して、1 つの登録済み IP アドレスにマップするダイナミック NAT の一形式です。NAT 設定には、同じまたは異なる ACL を持つ複数のダイナミック NAT 変換を含めることができます。ただし、特定の ACL に対して指定できるインターフェイスは1つだけです。

タイムアウト メカニズム

ダイナミック NAT 変換を作成した後は、特に TCAM エントリの数が制限されている場合、新しい変換を作成できるように、使用していないものをクリアする必要があります。Cisco NX-OS リリース 7.xは **syn-timeout** および **finrst-timeout** をサポートします。スイッチでは、次の NAT 変換タイムアウト タイマーがサポートされています。

- **syn-timeout**：TCP データのパケット タイムアウト値。SYN リクエストを送信後、SYN-ACK 応答を受信するまでの最大待ち時間です。

  タイムアウト値の範囲は、1 ～ 172800 秒です。デフォルト値は 60 秒です。

- **finrst-timeout**：RST または FIN パケットの受信によって接続が終了したときのフロー エントリのタイムアウト値。RST パケットと FIN パケットの両方の動作を設定するには、同じキーワードを使用します。

  - 接続が確立された後に RST パケットが受信されると（SYN-> SYN-ACK-> RST）、フローは設定されたタイムアウト値の後に期限切れになります。
  - 接続が確立された後に SYN パケット（SYN-> SYN-ACK-> FIN）が受信されると、finrst タイマーが開始されます。
  - 相手側から FIN-ACK を受信すると、変換エントリはすぐにクリアされます。それ以外の場合は、タイムアウト値の完了後にクリアされます。

  注　ダイナミック プールベースの設定が使用され、FIN-ACK が受信された場合、変換エントリはクリアされません。

  タイムアウト値の範囲は、1 ～ 172800 秒です。デフォルト値は 60 秒です。

- **tcp-timeout**：TCP 変換のタイムアウト値。3 ウェイ ハンドシェイク（SYN、SYN-ACK、ACK）の後に確立した接続の最大待ち時間です。接続が確立された後にアクティブ フローが発生しない場合、変換は設定されたタイムアウト値に従って期限切れになります。このタイムアウト値は、サンプリング タイムアウト値の完了後に開始されます。

  タイムアウト値の範囲は、1～172800秒です。これにはサンプリングタイムアウトも含まれます。

- **udp-timeout**：すべての NAT UDP パケットのタイムアウト値。

  タイムアウト値の範囲は、1～172800秒です。これにはサンプリングタイムアウトも含まれます。

- **timeout**：ダイナミック NAT 変換のタイムアウト値。

  タイムアウト値の範囲は、1～172800秒です。これにはサンプリングタイムアウトも含まれます。

- **sampling-timeout**：デバイスがダイナミック変換アクティビティをチェックするまでの時間。

  タイムアウト値の範囲は、1 ～ 172800 秒です。

tcp-timeout、**udp-timeout**、および **timeout** 値のタイマーは、**ip nat translation sampling-timeout** コマンドで設定されているタイムアウトの期限が切れた後にトリガーされます。

（注） 上記のタイマーはすべて、期限が切れるまでさらに時間がかかります（1ー30秒）。この追加時間は、パフォーマンスと最適化のためにタイマー期限切れイベントをランダム化するためのものです。

NAT の内部アドレスおよび外部アドレス

NAT 内部とは、変換を必要とする組織が所有するネットワークを指します。NAT が設定されている場合、このネットワーク内のホストは、別の空間（グローバルアドレス空間として知られている）にあるものとしてネットワークの外側に現れる 1 つ空間（ローカルアドレス空間として知られている）内のアドレスを持つことになります。

同様に、NAT 外部とは、スタブ ネットワークが接続するネットワークを指します。通常、組織の管理下にはありません。外部ネットワーク内のホストを変換の対象にすることもできるため、これらのホストもローカル アドレスとグローバル アドレスを持つことができます。

NAT では、次の定義が使用されます。

- ローカル アドレス：ネットワークの内側部分に表示されるローカルな IP アドレスです。
- グローバル アドレス：ネットワークの外側部分に表示されるグローバルな IP アドレスです。
- 内部ローカル アドレス：内部ネットワーク上のホストに割り当てられた IP アドレス。このアドレスは、多くの場合、インターネット ネットワーク情報センター（InterNIC）やサービス プロバイダーにより割り当てられた正規の IP アドレスではありません。
- 内部グローバル アドレス：外部に向けて、1 つ以上の内部ローカル IP アドレスを表現した正規の IP アドレス（InterNIC またはサービス プロバイダーにより割り当てられたもの）。
- 外部ローカル アドレス：内部ネットワークから見た外部ホストの IP アドレス。必ずしも正規のアドレスでありません。内部でルート可能なアドレス空間から割り当てられたものです。
- 外部グローバルアドレス：外部ネットワークに存在するホストに対して、ホストの所有者により割り当てられた IP アドレス。このアドレスは、グローバルにルート可能なアドレス、またはネットワーク空間から割り当てられたものです。

ダイナミック NAT のプール サポート

ダイナミック NAT を使用すると、グローバル アドレスのプールを設定して、新しい変換ごとにプールからグローバルアドレスを動的に割り当てることができます。アドレスは、セッションが期限切れになるか、閉じられた後にプールに返されます。これにより、要件に基づいてアドレスをより効率的に使用できます。

PAT のサポートには、グローバル アドレス プールの使用が含まれます。これにより、IP アドレスの使用率がさらに最適化されます。PAT は、ポート番号を使用して、一度に 1 つの IP アドレスを使い切ります。使用できるポート番号を該当ポート グループで見つけられなかった場合や、複数の外部 IP アドレスが設定されていると、PAT は次の IP アドレスに移動して最初の送信元ポートを再び割り当てようとします。このプロセスは、PAT で使用可能なポートと IP アドレスがなくなるまで続きます。

ダイナミック NAT および PAT では、各ホストは後続する変換ごとに異なるアドレスまたはポートを使用します。ダイナミック NAT とスタティック NAT 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。

スタティックおよびダイナミック双方向 NAT の概要

送信元 IP アドレスと宛先 IP アドレスの両方が、ネットワーク アドレス変換（NAT）デバイスを通過する単一のパケットとして変換される場合、双方向NATと呼ばれます。双方向NATは、スタティックおよびダイナミック変換でサポートされます。

双方向 NATでは、2 つの NAT 変換（ 1 つは内部、もう 1 つは外部）を変換グループの一部として設定できます。これらの変換は、NAT デバイスを通過する単一のパケットに適用できます。グループの一部として2つの変換を追加すると、個々の変換と結合された変換の両方が有効になります。

NAT 内部変換は、パケットが内部から外部に流れるときに送信元 IP アドレスとポート番号を変更します。パケットが外部から内部に戻るときに、宛先 IP アドレスとポート番号を変更します。NAT外部変換は、パケットが外部から内部に流れるときに送信元 IP アドレスとポート番号を変更し、パケットが内部から外部に戻るときに宛先 IP アドレスとポート番号を変更します。

双方向 NATを使用しない場合、送信元 IP アドレスとポート番号、または宛先 IP アドレスとポート番号のいずれか 1 つの変換ルールのみがパケットに適用されます。

同じグループに属するスタティック NAT 変換は、双方向 NAT 設定の対象と見なされます。スタティック設定にグループ ID が設定されていない場合、双方向 NAT 設定は機能しません。グループ ID で識別される単一のグループに属するすべての内部および外部 NAT 変換は、ペアになって 双方向 NAT 変換を形成します。

ダイナミック双方向 NAT 変換は、事前定義された **ip nat pool** または **インターフェイス オーバーロード** 設定から、送信元 IP アドレスとポート番号の情報を動的に選択します。パケット

フィルタリングは ACL の設定によって行われ、トラフィックはダイナミック NAT 変換ルールの向きを基にして発信される必要があります。送信元変換をダイナミック NAT ルールを使用して行うためです。

ダイナミック双方向 NAT では、2 つの NAT 変換（内部と外部）を変換グループの一部として設定できます。1つの変換はダイナミックで、他の変換はスタティックである必要があります。これらの2つの変換が変換のグループの一部である場合、内部から外部または外部から内部のいずれかで NAT デバイスを通過するときに、両方の変換を 1 つのパケットに適用できます。

スタティック NAT の注意事項および制約事項

スタティック NAT 設定時の注意事項および制約事項は、次のとおりです。

- NAT は、スタティック NAT とダイナミック NAT の両方を含む最大 1024 の変換をサポートします。
- Cisco Nexus 3500 シリーズ スイッチは、vPC トポロジでの NAT をサポートしていません。
- Cisco Nexus デバイスは、次のインターフェイス タイプ上の NAT をサポートします。
  - スイッチ仮想インターフェイス（SVI）
  - ルーテッド ポート
  - レイヤ 3 ポート チャネル
- NAT は、IPv4 ユニキャストだけでサポートされています。
- Cisco Nexus デバイスは、次をサポートしません。
  - アプリケーション層の変換。レイヤ 4 およびその他の組み込み IP は変換されません（FTP、ICMP の障害、IPSec、HTTPS など）。
  - インターフェイス上で同時に設定された NAT および VLAN アクセス コントロール リスト（VACL）。
  - フラグメント化された IP パケットの PAT 変換。
  - ソフトウェア転送パケットの NAT 変換。たとえば、IP オプションを持つパケットは NAT 変換されません。
- 出力 ACL は元のパケットに適用され、NAT 変換済みパケットには適用されません。
- デフォルトでは、NAT は 256 TCAM エントリで最大 127 の変換まで実行できます。より多くの NAT 変換が必要な場合は、他のエリア内の TCAM リージョン割り当てを減らしてから、**hardware profile tcam region nat** コマンドを使用して、NAT TCAM リージョンを増やします。
- HSRP および VRRP は NAT 内部アドレスではサポートされますが、NAT 外部アドレスではサポートされません。

- ワープ モード遅延パフォーマンスは、外部から内部ドメインに着信するパケットではサポートされません。
- IP アドレスがスタティック NAT 変換または PAT 変換に使用される場合、他の目的には使用できません。たとえば、インターフェイスに割り当てることはできません。
- スタティック NAT の場合は、外部グローバル IP アドレスが外部インターフェイス IP アドレスと異なる必要があります。
- 変換された IP が、外部インターフェイス サブネットの一部である場合、NAT の外部インターフェイスで **ip local-proxy-arp** コマンドを使用します。
- NAT 統計情報は利用できません。
- （100 を超える）多数の変換を設定する場合、変換を設定してから NAT インターフェイスを設定する方が迅速に設定できます。
- インターフェイスで一度に有効にできるのは、次の機能のいずれか1つだけです。これらの機能の1つ以上がインターフェイスで有効になっている場合、最後に有効になっている機能のみが機能します。
  - NAT
  - DHCP リレー
  - VACL
- 127 を超える PD NAT スタティック エントリは、一貫性のない CoPP ハードウェア カウンタの増分を行うハードウェアの制限によりサポートされません。

ダイナミック NAT の制約事項

ダイナミック ネットワーク アドレス変換（NAT）には、次の制約事項が適用されます。

- フラグメント化されたパケットはサポートされません。
- アプリケーション層ゲートウェイ（ALG）変換はサポートされていません。ALGはまた、アプリケーション レベル ゲートウェイとも呼ばれるもので、アプリケーション パケットのペイロード内の IP アドレス情報を変換するアプリケーションです。
- NAT および VLAN アクセス コントロール リスト（VACL）は、インターフェイスで一緒にサポートされません。インターフェイスで NAT または VACL を設定できます。
- 出力 ACL は、変換されたパケットには適用されません。
- サポート対象 MIB
- Cisco Data Center Network Manager（DCNM）はサポートされません。
- ダイナミック NAT 変換は、アクティブ デバイスおよびスタンバイ デバイスと同期されません。

- ステートフル NAT はサポートされていません。ただし、NAT と Hot Standby Router Protocol（HSRP）は共存できます。
- 通常、ICMP NAT フローは、設定されたサンプリングタイムアウトおよび変換タイムアウトの満了後にタイムアウトします。ただし、スイッチに存在する ICMP NAT フローがアイドル状態になると、設定されたサンプリングタイムアウトの期限が切れた直後にタイムアウトします。
- 変換された IP が、外部インターフェイス サブネットの一部である場合、NAT の外部インターフェイスで **ip local-proxy-arp** コマンドを使用します。
- Cisco Nexus 3548 シリーズ スイッチで新しい変換を作成する場合、変換がハードウェアでプログラムされるまでフローがソフトウェア転送されます。これには数秒かかることがあります。この期間中、内部グローバル アドレスの変換エントリはありません。したがって、リターン トラフィックはドロップされます。この制限を克服するには、ループバック インターフェイスを作成し、NAT プールに属する IP アドレスを割り当てます。

ダイナミック NAT の注意事項および制約事項

ダイナミック双方向 NAT の設定については、次の注意事項を参照してください。

- ダイナミック双方向 NATでは、スタティック NAT フローを作成する前にダイナミック NAT フローを作成しないと、ダイナミック双方向 NAT フローが正しく作成されません。
- 空の ACL が作成されると、**permit ip any any** のデフォルト ルールが設定されます。最初の ACL が空白の場合、NAT-ACL はそれ以上の ACL エントリに一致しません。
- TCAM スペースを最適に使用するためにサポートされる ICMP 変換またはフローエントリの最大数は 176 です。
- NAT は ECMP 対応であり、最大 24 の ECMP パスをサポートします。
- Cisco NX-OS リリース 9.x は、Cisco Nexus 3548 スイッチのネットワーク アドレス変換 (NAT) 統計情報をサポートします。
- traceroute は、スタティックおよびダイナミック NAT ではサポートされていません。

スタティック NAT の設定

スタティック NAT のイネーブル化

手順の概要

1. switch# **configure terminal**
2. switch(config)# **feature nat**

3. （任意） switch(config)# **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **feature nat**	デバイス上でスタティック NAT 機能をイネーブルにします。
ステップ 3	（任意） switch(config)# **copy running-config startup-config**	リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

インターフェイスでのスタティック NAT の設定

手順の概要

1. switch# **configure terminal**
2. switch(config)# **interface** *type slot*/*port*
3. switch(config-if)# **ip nat** {**inside** | **outside**}
4. （任意） switch(config)# **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **interface** *type slot*/*port*	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	switch(config-if)# **ip nat** {**inside**	**outside**}	内部または外部としてインターフェイスを指定します。 （注） マーク付きインターフェイスに到着したパケットだけが変換できます。
ステップ 4	（任意） switch(config)# **copy running-config startup-config**	リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

例

次に、スタティック NAT を使用して内部のインターフェイスを設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/4
switch(config-if)# ip nat inside
```

内部送信元アドレスのスタティック NAT のイネーブル化

内部送信元変換の場合、トラフィックは内部インターフェイスから外部インターフェイスに流れます。NAT は、内部ローカル IP アドレスを内部グローバル IP アドレスに変換します。リターン トラフィックでは、宛先の内部グローバル IP アドレスが内部ローカル IP アドレスに変換されて戻されます。

（注） Cisco Nexus デバイス が、内部送信元 IP アドレス（Src:ip1）を外部送信元 IP アドレス（newSrc:ip2）に変換するように設定されている場合、Cisco Nexus デバイス は外部宛先 IP アドレス（Dst: ip2）の内部宛先 IP アドレス（newDst: ip1）への変換を暗黙的に追加します。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **ip nat inside source static** *local-ip-address global-ip-address* [**group** *group-id*]
3. （任意） switch(config)# **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **ip nat inside source static** *local-ip-address global-ip-address* [**group** *group-id*]	内部グローバル アドレスを内部ローカル アドレスに、またはその逆に（内部ローカル トラフィックを内部グローバル トラフィックに）変換するようにスタティック NAT を設定します。
ステップ 3	（任意） switch(config)# **copy running-config startup-config**	リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

例

次に、外部送信元アドレスのスタティック NAT を設定する例を示します。

```
switch# configure terminal
switch(config)# ip nat inside source static 1.1.1.1 5.5.5.5
switch(config)# copy running-config startup-config
```

外部送信元アドレスのスタティック NAT のイネーブル化

外部送信元変換の場合、トラフィックは外部インターフェイスから内部インターフェイスに流れます。NAT は、外部グローバル IP アドレスを外部ローカル IP アドレスに変換します。リターン トラフィックでは、宛先の外部ローカル IP アドレスが外部グローバル IP アドレスに変換されて戻されます。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **ip nat outside source static** *global-ip-address local-ip-address* [**group** *group-id*] [**add-route**]
3. （任意） switch(config)# **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **ip nat outside source static** *global-ip-address local-ip-address* [**group** *group-id*] [**add-route**]	外部グローバル アドレスを外部ローカル アドレスに、またはその逆に外部ローカル トラフィックを外部グローバル トラフィックに変換するようにスタティック NAT を設定します。
ステップ 3	（任意） switch(config)# **copy running-config startup-config**	リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

例

次に、外部送信元アドレスのスタティック NAT を設定する例を示します。

```
switch# configure terminal
switch(config)# ip nat outside source static 2.2.2.2 6.6.6.6
switch(config)# copy running-config startup-config
```

内部送信元アドレスのスタティック PAT の設定

ポート アドレス変換（PAT）を使用して、特定の内部ホストにサービスをマッピングできます。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **ip nat inside source static** {*inside-local-address outside-local-address* | {**tcp**| **udp**} *inside-local-address* {*local-tcp-port* | *local-udp-port*} *inside-global-address* {*global-tcp-port* | *global-udp-port*}} **group** *group-id*
3. （任意） switch(config)# **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **ip nat inside source static** {*inside-local-address outside-local-address* | {**tcp**| **udp**} *inside-local-address* {*local-tcp-port* | *local-udp-port*} *inside-global-address* {*global-tcp-port* | *global-udp-port*}} **group** *group-id*	スタティック NAT を内部ローカル ポート、内部グローバル ポートにマッピングします。
ステップ 3	（任意） switch(config)# **copy running-config startup-config**	リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

例

次に、UDP サービスを特定の内部送信元アドレスおよび UDP ポートにマッピングする例を示します。

```
switch# configure terminal
switch(config)#  ip nat inside source static udp 20.1.9.2 63 35.48.35.48 130
switch(config)# copy running-config startup-config
```

外部送信元アドレスのスタティック PAT の設定

ポート アドレス変換（PAT）を使用して、特定の外部ホストにサービスをマッピングできます。

手順の概要

1. switch# **configure terminal**

2. switch(config)# **ip nat outside source static** {*outside-global-address outside-local-address* | {**tcp** | **udp**} *outside-global-address* {*global-tcp-port* | *global-udp-port*} *outside-local-address* {*global-tcp-port* | *global-udp-port*}}**group** *group-id* **add-route**
3. （任意） switch(config)# **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **ip nat outside source static** {*outside-global-address outside-local-address* | {**tcp** | **udp**} *outside-global-address* {*global-tcp-port* | *global-udp-port*} *outside-local-address* {*global-tcp-port* | *global-udp-port*}}**group** *group-id* **add-route**	スタティック NAT を、外部グローバル ポート、外部ローカル ポートにマッピングします。
ステップ 3	（任意） switch(config)# **copy running-config startup-config**	リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

例

次に、TCP サービスを特定の外部送信元アドレスおよび TCP ポートにマッピングする例を示します。

```
switch# configure terminal
switch(config)#  ip nat outside source static tcp 20.1.9.2 63 35.48.35.48 130
switch(config)# copy running-config startup-config
```

スタティック双方向 NAT の設定

同じグループ内のすべての変換は、スタティック双方向 Network Address Translation（NAT）ルールの作成のために考慮されます。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip nat inside source static** *inside-local-ip-address inside-global-ip-address* [**group** *group-id*]
4. **ip nat outside source static** *outside-global-ip-address outside-local-ip-address* [**group** *group-id*] [**add-route**]
5. **interface** *type number*
6. **ip address** *ip-address mask*
7. **ip nat inside**
8. **exit**
9. **interface** *type number*

10. **ip address** *ip-address mask*
11. **ip nat outside**
12. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `switch> enable`	特権 EXEC モードを有効にします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `switch# configure terminal`	特権 EXEC モードに切り替えます。
ステップ 3	**ip nat inside source static** *inside-local-ip-address inside-global-ip-address* [**group** *group-id*] 例： `switch(config)# ip nat inside source static 10.1.1.1 192.168.34.4 group 4`	内部ローカル IP アドレスを対応する内部グローバル IP アドレスに変換するようにスタティック双方向 NAT を設定します。 • **group** キーワードは、変換が属するグループを決定します。
ステップ 4	**ip nat outside source static** *outside-global-ip-address outside-local-ip-address* [**group** *group-id*] [**add-route**] 例： `switch(config)# ip nat outside source static 209.165.201.1 10.3.2.42 group 4 add-route`	外部グローバル IP アドレスを対応する外部ローカル IP アドレスに変換するようにスタティック双方向 NAT を設定します。 • **group** キーワードは、変換が属するグループを決定します。
ステップ 5	**interface** *type number* 例： `switch(config)# interface ethernet 1/2`	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 6	**ip address** *ip-address mask* 例： `switch(config-if)# ip address 10.2.4.1 255.255.255.0`	インターフェイスのプライマリ IP アドレスを設定します。
ステップ 7	**ip nat inside** 例： `switch(config-if)# ip nat inside`	NATの対象である内部ネットワークにインターフェイスを接続します。
ステップ 8	**exit** 例： `switch(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、グローバルコンフィギュレーションモードに戻ります。

	コマンドまたはアクション	目的
ステップ 9	**interface** *type number* 例： `switch(config)# interface ethernet 1/1`	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 10	**ip address** *ip-address mask* 例： `switch(config-if)# ip address 10.5.7.9 255.255.255.0`	インターフェイスのプライマリ IP アドレスを設定します。
ステップ 11	**ip nat outside** 例： `switch(config-if)# ip nat outside`	NATの対象である内部ネットワークにインターフェイスを接続します。
ステップ 12	**end** 例： `switch(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

スタティック NAT および PAT の設定例

次に、スタティック NAT の設定例を示します。

```
ip nat inside source static 103.1.1.1 11.3.1.1
ip nat inside source static 139.1.1.1 11.39.1.1
ip nat inside source static 141.1.1.1 11.41.1.1
ip nat inside source static 149.1.1.1 95.1.1.1
ip nat inside source static 149.2.1.1 96.1.1.1
ip nat outside source static 95.3.1.1 95.4.1.1
ip nat outside source static 96.3.1.1 96.4.1.1
ip nat outside source static 102.1.2.1 51.1.2.1
ip nat outside source static 104.1.1.1 51.3.1.1
ip nat outside source static 140.1.1.1 51.40.1.1
```

次に、スタティック PAT の設定例を示します。

```
ip nat inside source static tcp 10.11.1.1 1 210.11.1.1 101
ip nat inside source static tcp 10.11.1.1 2 210.11.1.1 201
ip nat inside source static tcp 10.11.1.1 3 210.11.1.1 301
ip nat inside source static tcp 10.11.1.1 4 210.11.1.1 401
ip nat inside source static tcp 10.11.1.1 5 210.11.1.1 501
ip nat inside source static tcp 10.11.1.1 6 210.11.1.1 601
ip nat inside source static tcp 10.11.1.1 7 210.11.1.1 701
ip nat inside source static tcp 10.11.1.1 8 210.11.1.1 801
ip nat inside source static tcp 10.11.1.1 9 210.11.1.1 901
ip nat inside source static tcp 10.11.1.1 10 210.11.1.1 1001
ip nat inside source static tcp 10.11.1.1 11 210.11.1.1 1101
ip nat inside source static tcp 10.11.1.1 12 210.11.1.1 1201
```

例：スタティック双方向 NATの設定

次に、内部送信元および外部送信元のスタティック双方向NATを設定する例を示します。

```
Switch> enable
Switch# configure terminal
Switch(config)# ip nat inside source static 10.1.1.1 192.168.34.4 group 4
Switch(config)# ip nat outside source static 209.165.201.1 10.3.2.42 group 4
Switch(config)# interface ethernet 1/2
Switch(config-if)# ip address 10.2.4.1 255.255.255.0
Switch(config-if)# ip nat inside
switch(config-if)# exit
switch(config)# interface ethernet 1/1
switch(config-if)# ip address 10.5.7.9 255.255.255.0
switch(config-if)# ip nat outside
Switch(config-if)# end
```

スタティック NAT の設定の確認

スタティック NAT の設定を表示するには、次の作業を行います。

手順の概要

1. switch# **show ip nat translations**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **show ip nat translations**	内部グローバル、内部ローカル、外部ローカル、および外部グローバルの各 IP アドレスを示します。

例

次に、スタティック NAT の設定を表示する例を示します。

```
switch# show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
any ---                ---                20.4.4.40          220.2.2.20
tcp ---                ---                23.1.1.133:333     210.3.3.33:555
any 160.200.1.140      10.1.1.40          ---                ---
any 160.200.1.140      10.1.1.40          20.4.4.40          220.2.2.20
tcp 172.9.9.142:777    12.2.2.42:444      ---                ---
tcp 172.9.9.142:777    12.2.2.42:444      23.1.1.133:333     210.3.3.33:555
```

ダイナミック NAT の設定

ダイナミック変換および変換タイムアウトの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **ip access-list** *access-list-name*
4. **permit** *protocol source source-wildcard* **any**
5. **deny** *protocol source source-wildcard* **any**
6. **exit**
7. **ip nat inside source list** *access-list-name* **interface** *type number* **overload**
8. **interface** *type number*
9. **ip address** *ip-address mask*
10. **ip nat inside**
11. **exit**
12. **interface** *type number*
13. **ip address** *ip-address mask*
14. **ip nat outside**
15. **exit**
16. **ip nat translation tcp-timeout** *seconds*
17. **ip nat translation max-entries [all-host]** *number-of-entries*
18. **ip nat translation udp-timeout** *seconds*
19. **ip nat translation timeout** *seconds*
20. **ip nat translation syn-timeout** {*seconds* | **never**}
21. **ip nat translation finrst-timeout** {*seconds* | **never**}
22. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードを有効にします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**ip access-list** *access-list-name* 例： `Switch(config)# ip access-list acl1`	アクセス リストを定義し、アクセス リスト コンフィギュレーション モードを開始します。
ステップ 4	**permit** *protocol source source-wildcard* **any** 例： `Switch(config-acl)# permit ip 10.111.11.0/24 any`	条件に一致するトラフィックを許可する条件を IP アクセス リストに設定します。
ステップ 5	**deny** *protocol source source-wildcard* **any** 例： `Switch(config-acl)# deny udp 10.111.11.100/32 any`	ネットワークにパケットが入るのを拒否する IP アクセス リストの条件を設定します。 **deny** ルールは **permit** として扱われ、拒否ルールに記載された条件に一致するパケットは NAT 変換されずに転送されます。
ステップ 6	**exit** 例： `Switch(config-acl)# exit`	アクセスリスト コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 7	**ip nat inside source list** *access-list-name* **interface** *type number* **overload** 例： `Switch(config)# ip nat inside source list acl1 interface ethernet 1/1 overload`	ステップ 3 で定義したアクセス リストを指定して、ダイナミック送信元変換を設定します。
ステップ 8	**interface** *type number* 例： `Switch(config)# interface ethernet 1/4`	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 9	**ip address** *ip-address mask* 例： `Switch(config-if)# ip address 10.111.11.39 255.255.255.0`	インターフェイスのプライマリ IP アドレスを設定します。
ステップ 10	**ip nat inside** 例： `Switch(config-if)# ip nat inside`	NAT の対象である内部ネットワークにインターフェイスを接続します。
ステップ 11	**exit** 例： `Switch(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、グローバルコンフィギュレーションモードに戻ります。
ステップ 12	**interface** *type number* 例： `Switch(config)# interface ethernet 1/1`	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 13	**ip address** *ip-address mask* 例： `Switch(config-if)# ip address 172.16.232.182 255.255.255.240`	インターフェイスのプライマリ IP アドレスを設定します。
ステップ 14	**ip nat outside** 例： `Switch(config-if)# ip nat outside`	インターフェイスを外部ネットワークに接続します。
ステップ 15	**exit** 例： `Switch(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、グローバルコンフィギュレーションモードに戻ります。
ステップ 16	**ip nat translation tcp-timeout** *seconds* 例： `Switch(config)# ip nat translation tcp-timeout 50000`	TCP ベースのダイナミック NAT エントリのタイムアウト値を指定します。 • ダイナミックに作成された NAT 変換は、設定されたタイムアウト制限に達するとクリアされます。すべての設定されたタイムアウトは、**ip nat translation sampling-timeout** コマンドのために設定されたタイムアウトが終了すると、トリガされます。
ステップ 17	**ip nat translation max-entries [all-host]** *number-of-entries* 例： `Switch(config)# ip nat translation max-entries 300`	ダイナミック NAT 変換の最大数を指定します。エントリの数は 1 ー 1023 です。 **all-host** キーワードは、この変換制限をすべてのホストに適用します。ホストあたりのエントリ数は1 ー 1023 です。
ステップ 18	**ip nat translation udp-timeout** *seconds* 例： `Switch(config)# ip nat translation udp-timeout 45000`	UDP ベースのダイナミック NAT エントリのタイムアウト値を指定します。 • ダイナミックに作成された NAT 変換は、設定されたタイムアウト制限に達するとクリアされます。すべての設定されたタイムアウトは、**ip nat translation sampling-timeout** コマンドのために設定されたタイムアウトが終了すると、トリガされます。
ステップ 19	**ip nat translation timeout** *seconds* 例： `switch(config)# ip nat translation timeout 13000`	ダイナミック NAT 変換のタイムアウト値を指定します。

	コマンドまたはアクション	目的
ステップ 20	**ip nat translation syn-timeout** {*seconds* | **never**} 例： `switch(config)# ip nat translation syn-timeout 20`	SYN 要求を送信するが SYN-ACK 応答を受信しない TCP データのパケット タイムアウト値を指定します。 タイムアウト値の範囲は、1 ～ 172800 秒です。デフォルト値は 60 秒です。 **never** キーワードは、SYN タイマーが実行されないことを指定します。
ステップ 21	**ip nat translation finrst-timeout** {*seconds* | **never**} 例： `switch(config)# ip nat translation finrst-timeout 30`	終了（FIN）パケットまたはリセット（RST）パケットを受信して接続が終了するときのフローエントリのタイムアウト値を指定します。RST パケットと FIN パケットの両方の動作を設定するには、同じキーワードを使用します。 タイムアウト値の範囲は、1 ～ 172800 秒です。デフォルト値は 60 秒です。 **never** キーワードは、FIN または RST タイマーが実行されないことを指定します。
ステップ 22	**end** 例： `Switch(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

ダイナミック NAT プールの設定

NAT プールは、単一の **ip nat pool** コマンドか、または **ip nat pool** と **address** コマンドを使用して、IP アドレスの範囲を定義することで作成できます。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **feature nat**
3. switch(config)# **ip nat pool** *pool-name* [*startip endip*] {**prefix** *prefix-length* | **netmask** *network-mask*}
4. （任意） switch(config-ipnat-pool)# **address** *startip endip*
5. （任意） switch(config)# **no ip nat pool** *pool-name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	switch(config)# **feature nat**	デバイスの NAT 機能をイネーブルにします。
ステップ 3	switch(config)# **ip nat pool** *pool-name* [*startip endip*] {**prefix** *prefix-length* | **netmask** *network-mask*}	グローバル IP アドレスの範囲で NAT プールを作成します。IP アドレスは、プレフィックス長またはネットワークマスクを使用してフィルタリングされます。
ステップ 4	（任意） switch(config-ipnat-pool)# **address** *startip endip*	グローバル IP アドレスの範囲を指定します（プールの作成時に指定していなかった場合）。
ステップ 5	（任意） switch(config)# **no ip nat pool** *pool-name*	指定した NAT プールを削除します。

例

次に、プレフィックス長を使用して NAT プールを作成する例を示します。

```
switch# configure terminal
switch(config)# ip nat pool pool1 30.1.1.1 30.1.1.2 prefix-length 24
switch(config)#
```

次に、ネットワークマスクを使用して NAT プールを作成する例を示します。

```
switch# configure terminal
switch(config)# ip nat pool pool5 20.1.1.1 20.1.1.5 netmask 255.0.255.0
switch(config)#
```

この例では **ip nat pool** と **address** コマンドを使用してNAT プールを作成し、グローバル IP アドレスの範囲を定義します。

```
switch# configure terminal
switch(config)# ip nat pool pool7 netmask 255.255.0.0
switch(config-ipnat-pool)# address 40.1.1.1 40.1.1.5
switch(config-ipnat-pool)#
```

次の例は、NAT プールの削除方法を示します。

```
switch# configure terminal
switch(config)# no ip nat pool pool4
switch(config)#
```

送信元リストの設定

内部インターフェイスと外部インターフェイスのIPアドレスの送信元リストを設定できます。

始める前に

プールの送信元リストを設定する前に、必ずプールを設定してください。

手順の概要

1. switch# **configure terminal**
2. （任意） switch# **ip nat inside source list** *list-name* **pool** *pool-name* [**overload**]
3. （任意） switch# **ip nat outside source list** *list-name* **pool** *pool-name* [**add-route**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	（任意） switch# **ip nat inside source list** *list-name* **pool** *pool-name* [**overload**]	オーバーロードの有無にかかわらず、プールを使用して NAT 内部送信元リストを作成します。
ステップ 3	（任意） switch# **ip nat outside source list** *list-name* **pool** *pool-name* [**add-route**]	オーバーロードなしでプールを使用して NAT 外部送信元リストを作成します。

例

次に、オーバーロードのないプールを使用してNAT内部送信元リストを作成する例を示します。

```
switch# configure terminal
switch(config)# ip nat inside source list list1 pool pool1
switch(config)#
```

次に、オーバーロードのあるプールを使用してNAT内部送信元リストを作成する例を示します。

```
switch# configure terminal
switch(config)# ip nat inside source list list2 pool pool2 overload
switch(config)#
```

次に、オーバーロードのないプールを使用してNAT外部送信元リストを作成する例を示します。

```
switch# configure terminal
switch(config)# ip nat outside source list list3 pool pool3
switch(config)#
```

内部送信元アドレスのダイナミック双方向 NAT の設定

内部送信元変換の場合、トラフィックは内部インターフェイスから外部インターフェイスに流れます。内部送信元アドレスにはダイナミック双方向 NAT を設定できます。

始める前に

スイッチで NAT がイネーブルになっていることを確認します。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **ip nat outside source static** *outside-global-ip-address outside-local-ip-address* | [**tcp** | **udp**] *outside-global-ip-address outside-global-port outside-local-ip-address outside-local-port* [**group** *group-id*] [**add-route**] [**dynamic**]
3. switch(config)# **ip nat inside source list** *access-list-name* [**interface** *type slot/port* **overload** | **pool** *pool-name*] [**group** *group-id*] [**dynamic**]]
4. switch(config)# **ip nat pool** *pool-name* [*startip endip*] {**prefix** *prefix-length* | **netmask** *network-mask*}
5. switch(config)# **interface** *type slot/port*
6. switch(config-if)# **ip nat outside**
7. switch(config-if)# **exit**
8. switch(config)# **interface** *type slot/port*
9. switch(config-if)# **ip nat inside**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **ip nat outside source static** *outside-global-ip-address outside-local-ip-address*	[**tcp**	**udp**] *outside-global-ip-address outside-global-port outside-local-ip-address outside-local-port* [**group** *group-id*] [**add-route**] [**dynamic**]	外部グローバル アドレスを内部ローカル アドレスに変換するか、または内部ローカル トラフィックを内部グローバル トラフィックに変換するようにスタティック NAT を設定します。 **group** キーワードは、変換が属するグループを決定します。
ステップ 3	switch(config)# **ip nat inside source list** *access-list-name* [**interface** *type slot/port* **overload**	**pool** *pool-name*] [**group** *group-id*] [**dynamic**]]	オーバーロードの有無にかかわらず、プールを使用して NAT 内部ソースリストを作成することによって、ダイナミック ソース変換を確立します。 **group** キーワードは、変換が属するグループを決定します。
ステップ 4	switch(config)# **ip nat pool** *pool-name* [*startip endip*] {**prefix** *prefix-length*	**netmask** *network-mask*}	グローバル IP アドレスの範囲で NAT プールを作成します。IP アドレスは、プレフィックス長または

	コマンドまたはアクション	目的
		ネットワーク マスクを使用してフィルタリングされます。
ステップ 5	switch(config)# **interface** *type slot/port*	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 6	switch(config-if)# **ip nat outside**	インターフェイスを外部ネットワークに接続します。
ステップ 7	switch(config-if)# **exit**	インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 8	switch(config)# **interface** *type slot/port*	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 9	switch(config-if)# **ip nat inside**	NAT の対象である内部ネットワークにインターフェイスを接続します。

例

次に、内部送信元アドレスのダイナミック双方向 NAT を設定する例を示します。

```
switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# ip nat outside source static 2.2.2.2 4.4.4.4 group 20 dynamic
switch(config)# ip nat inside source list acl_1 pool pool_1 overload group 20 dynamic
switch(config)# ip nat pool pool_1 3.3.3.3 3.3.3.10 prefix-length 24
switch(config)# interface Ethernet1/8
switch(config-if)# ip nat outside
switch(config-if)# exit
switch(config)# interface Ethernet1/15
switch(config-if)# ip nat inside
```

外部送信元アドレスのダイナミック双方向 NATの設定

内部送信元変換の場合、トラフィックは外部インターフェイスから内部インターフェイスに流れます。外部送信元アドレスにダイナミック双方向 NATを設定できます。

始める前に

スイッチで NAT がイネーブルになっていることを確認します。

手順の概要

1. switch# **configure terminal**

2. switch(config)# **ip nat inside source static** *inside-local-ip-address inside-global-ip-address* | [**tcp** | **udp**] *inside-local-ip-address local-port inside-global-ip-address global-port* [**group** *group-id*] [**dynamic**]
3. switch(config)# **ip nat outside source list** *access-list-name* [**interface** *type slot/port* **pool** *pool-name*] [**group** *group-id*] [**add-route**] [**dynamic**]
4. switch(config)# **ip nat pool** *pool-name* [*startip endip*] {**prefix** *prefix-length* | **netmask** *network-mask*}
5. switch(config)# **interface** *type slot/port*
6. switch(config-if)# **ip nat outside**
7. switch(config-if)# **exit**
8. switch(config)# **interface** *type slot/port*
9. switch(config-if)# **ip nat inside**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **ip nat inside source static** *inside-local-ip-address inside-global-ip-address*	[**tcp**	**udp**] *inside-local-ip-address local-port inside-global-ip-address global-port* [**group** *group-id*] [**dynamic**]	内部グローバル アドレスを内部ローカル アドレスに変換するか、または内部ローカル トラフィックを内部グローバル トラフィックに変換するようにスタティック NAT を設定します。 **group** キーワードは、変換が属するグループを決定します。
ステップ 3	switch(config)# **ip nat outside source list** *access-list-name* [**interface** *type slot/port* **pool** *pool-name*] [**group** *group-id*] [**add-route**] [**dynamic**]	プールを使用して NAT 外部送信元リストを作成することによって、ダイナミック送信元変換を確立します。
ステップ 4	switch(config)# **ip nat pool** *pool-name* [*startip endip*] {**prefix** *prefix-length*	**netmask** *network-mask*}	グローバル IP アドレスの範囲で NAT プールを作成します。IP アドレスは、プレフィックス長またはネットワーク マスクを使用してフィルタリングされます。
ステップ 5	switch(config)# **interface** *type slot/port*	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 6	switch(config-if)# **ip nat outside**	インターフェイスを外部ネットワークに接続します。
ステップ 7	switch(config-if)# **exit**	インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 8	switch(config)# **interface** *type slot/port*	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 9	switch(config-if)# **ip nat inside**	NAT の対象である内部ネットワークにインターフェイスを接続します。

例

次に、外部送信元アドレスにダイナミック双方向 NATを設定する例を示します。

```
switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# ip nat inside source static 7.7.7.7 5.5.5.5 group 30 dynamic
switch(config)# ip nat outside source list acl_2 pool pool_2 group 30 dynamic
switch(config)# ip nat pool pool_2 4.4.4.4 4.4.4.10 prefix-length 24
switch(config)# interface Ethernet1/6
switch(config-if)# ip nat outside
switch(config-if)# exit
switch(config)# interface Ethernet1/11
switch(config-if)# ip nat inside
```

ダイナミック NAT 変換のクリア

ダイナミック変換をクリアするには、次の作業を実行します。

コマンド	目的
clear ip nat translation [**all** | **inside** *global-ip-address local-ip-address* [**outside** *local-ip-address global-ip-address*] | **outside** *local-ip-address global-ip-address*]	すべてまたは特定のダイナミック NAT 変換を削除します。

例

次に、すべてのダイナミック変換をクリアする例を示します。

```
switch# clear ip nat translation all
```

次に、内部アドレスと外部アドレスのダイナミック変換をクリアする例を示します。

```
switch# clear ip nat translation inside 2.2.2.2 4.4.4.4 outside 5.5.5.5 7.7.7.7
```

ダイナミック NAT の設定の確認

ダイナミック NAT の設定を表示するには、次の作業を行います。

コマンド	目的
show ip nat translations	ダイナミック変換を含むアクティブなネットワーク アドレス変換（NAT）変換を表示します。 エントリが作成および使用された日時など、各変換テーブル エントリの追加情報を表示します。
show ip nat translations verbose	ダイナミック変換を含むアクティブなネットワークアドレス変換（NAT）変換を読みやすい形式で表示します。
show run nat	NAT の設定を表示します。

例

次に、NAT の実行コンフィギュレーションを表示する例を示します。

```
switch# show run nat

!Command: show running-config nat
!Time: Wed Apr 23 11:17:43 2014

version 6.0(2)A3(1)
feature nat

ip nat inside source list list1 pool pool1
ip nat inside source list list2 pool pool2 overload
ip nat inside source list list7 pool pool7 overload
ip nat outside source list list3 pool pool3
ip nat pool pool1 30.1.1.1 30.1.1.2 prefix-length 24
ip nat pool pool2 10.1.1.1 10.1.1.2 netmask 255.0.255.0
ip nat pool pool3 30.1.1.1 30.1.1.8 prefix-length 24
ip nat pool pool5 20.1.1.1 20.1.1.5 netmask 255.0.255.0
ip nat pool pool7 netmask 255.255.0.0
  address 40.1.1.1 40.1.1.5
```

次に、アクティブな NAT 変換を表示する例を示します。

オーバーロードのある内部プール

```
switch# show ip nat translation
Pro  Inside global      Inside local       Outside local      Outside global
icmp 20.1.1.3:64762     10.1.1.2:133       20.1.1.1:0         20.1.1.1:0
icmp 20.1.1.3:64763     10.1.1.2:134       20.1.1.1:0         20.1.1.1:0



switch# sh ip nat translations verbose
Pro Inside global      Inside local       Outside local      Outside global
any 1.1.1.1            10.1.1.2           ---                ---
    Flags:0x1  Entry-id:0  State:0x0  Group_id:0 Format(H:M:S) Time-left:0:0:-1
icmp 101.1.0.1:65351   101.0.0.1:0        102.1.0.1:231      102.1.0.1:231
   Flags:0x82  Entry-id:101  State:0x3  Group_id:0 VRF: red Format(H:M:S) Time-left:12:0:9
udp 101.1.0.1:65383    101.0.0.1:63       102.1.0.1:63       102.1.0.1:63
```

```
   Flags:0x82  Entry-id:103  State:0x3  Group_id:0 VRF: red Format(H:M:S) Time-left:12:0:9
tcp 101.1.0.1:64549    101.0.0.1:8809     102.1.0.1:9087     102.1.0.1:9087
   Flags:0x82  Entry-id:102  State:0x1  Group_id:0 VRF: red Format(H:M:S) Time-left:12:0:9

    syn:0:1:9  fin-rst:12:0:9
```

オーバーロードのない外部プール

```
switch# show ip nat translation
Pro  Inside global      Inside local       Outside local      Outside global
any  ---                ---                177.7.1.1:0        77.7.1.64:0
any  ---                ---                40.146.1.1:0       40.46.1.64:0
any  ---                ---                10.4.146.1:0       10.4.46.64:0


switch# show ip nat translations verbose
Pro Inside global      Inside local       Outside local      Outside global
any 1.1.1.1            10.1.1.2           ---                ---
    Flags:0x1  Entry-id:0  State:0x0  Group_id:0 Format(H:M:S) Time-left:0:0:-1
any 101.1.0.1          101.0.0.1          ---                ---
   Flags:0x0  Entry-id:92  State:0x3  Group_id:0 VRF: red Format(H:M:S) Time-left:12:0:11
```

NAT 統計情報の確認

ネットワーク アドレス変換（NAT）統計情報を表示するには、次の作業を実行します。

コマンド	目的
show ip nat statistics	ネットワーク アドレス変換（NAT）統計を表示します。

例

次に、**show ip nat statistics** コマンドのサンプル出力例を示します。

NAT 統計情報のクリア

ネットワーク アドレス変換（NAT）統計情報をクリアするには、次のタスクを実行します。

コマンド	目的
clear ip nat Statistics	ネットワーク アドレス変換（NAT）統計情報エントリをクリアします。

例

clear ip nat statistics コマンドは、ネットワーク アドレス変換（NAT）統計エントリをクリアします。

```
switch# clear ip nat statistics

-----------------------------------------------------
Total expired Translations: 0
SYN timer expired:
FIN-RST timer expired:
Inactive timer expired:
-----------------------------------------------------
Total Hits: 0
In-Out Hits: 0
Out-In Hits: 0
-----------------------------------------------------
Total Misses: 0
In-Out Misses: 0
Out-In Misses: 0
-----------------------------------------------------
Total SW Translated Packets: 0
In-Out SW Translated: 0
Out-In SW Translated: 0
-----------------------------------------------------
Total SW Dropped Packets: 0
In-Out SW Dropped: 0
-----------------------------------------------------
Address alloc. failure drop: 0
Port alloc. failure drop: 0
Dyn. Translation max limit drop: 0
ICMP max limit drop: 0
Allhost max limit drop: 0
-----------------------------------------------------
Inside / Outside source list:
Missed: 0
-----------------------------------------------------
```

例：ダイナミック変換および変換タイムアウトの設定

次に、アクセス リストを指定してダイナミック オーバーロードのネットワーク アドレス変換（NAT）を設定する例を示します。

```
Switch> enable
Switch# configure terminal
Switch(config)# ip access-list acl1
Switch(config-acl)# permit ip 10.111.11.0/24 any
Switch(config-acl)# deny udp 10.111.11.100/32 any
Switch(config-acl)# exit
Switch(config)# ip nat inside source list acl1 interface ethernet 1/1 overload
Switch(config)# interface ethernet 1/4
Switch(config-if)# ip address 10.111.11.39 255.255.255.0
Switch(config-if)# ip nat inside
Switch(config-if)# exit
Switch(config)# interface ethernet 1/1
```

```
Switch(config-if)# ip address 172.16.232.182 255.255.255.240
Switch(config-if)# ip nat outside
Switch(config-if)# exit
Switch(config)# ip nat translation tcp-timeout 50000
Switch(config)# ip nat translation max-entries 300
Switch(config)# ip nat translation udp-timeout 45000
Switch(config)# ip nat translation timeout 13000
Switch(config)# end
```

VRF 対応 NAT に関する情報

VRF 対応 NAT は、スタティックおよびダイナミック NAT 設定でサポートされます。トラフィックが、デフォルト以外の VRF（内部）から同じデフォルト以外の VRF（外部）に流れるように設定されている場合、IP NAT コマンドの match-in-vrf オプションを指定する必要があります。

トラフィックが、デフォルト以外の VRF（内部）からデフォルトの VRF（外部）に流れるように設定されている場合、IP NAT コマンドの match-in-vrf オプションを指定することはできません。NAT の内部設定がデフォルトの VRF インターフェイスで設定されている場合、NAT の外部設定はデフォルト以外の VRF インターフェイスではサポートされません。

NAT 内部インターフェイスの異なる VRF 間で重複したアドレスが設定されている場合、NAT 外部インターフェイスをデフォルトの VRF インターフェイスにすることはできませんたとえば、vrfA と vrfB が同じ送信元サブネットを持つ NAT 内部インターフェイスとして設定され、NAT 外部インターフェイスはデフォルト VRF として設定されていたとします。このような設定では、NAT 外部インターフェイスから NAT 内部インターフェイスへのパケットのルーティングがあいまいであるため、NAT はサポートされません。

VRF 対応 NAT の設定

始める前に

スイッチで NAT がイネーブルになっていることを確認します。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **[no] ip nat** *inside* | *outside* **source list** *ACL_NAME* [*interface INTERFACE NAME* **overload**][*pool POOL NAME* **overload**] [**group** *group-id*] [**dynamic**] [**vrf** *<vrf-name>* [**match-in-vrf**]]
3. switch(config)# **[no] ip nat** *inside* | *outside* **source static** *LOCAL IP GLOBAL IP* | [*tcp* | *udp LOCAL IP LOCAL PORT GLOBAL IP GLOBAL PORT*] [**group** *group-id*] [**dynamic**] [**vrf** *<vrf-name>* [**match-in-vrf**]]
4. switch(config)# **interface** *type slot/port* [**vrf** *<vrf-name* **ip nat** *inside* | *outside*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **[no] ip nat** *inside* | *outside* **source list** *ACL_NAME* [*interface INTERFACE NAME* **overload**][*pool POOL NAME* **overload**] [**group** *group-id*] [**dynamic**] [**vrf** <*vrf-name*> [**match-in-vrf**]]	VRF 固有のダイナミック NAT を作成または削除します。 **group** キーワードは、変換が属するグループを決定します。
ステップ 3	switch(config)# **[no] ip nat** *inside* | *outside* **source static** *LOCAL IP GLOBAL IP* | [*tcp* | *udp LOCAL IP LOCAL PORT GLOBAL IP GLOBAL PORT*] [**group** *group-id*] [**dynamic**] [**vrf** <*vrf-name*> [**match-in-vrf**]]	VRF 固有のスタティック NAT を作成または削除します。 **group** キーワードは、変換が属するグループを決定します。
ステップ 4	switch(config)# **interface** *type slot/port* [**vrf** <*vrf-name* **ip nat** *inside* | *outside*	VRF 対応インターフェイスで NAT をイネーブルにします。

show run nat コマンドの出力を参照してください。

```
#show run nat
….
feature nat
ip nat inside source static 1.1.1.1 1.1.1.100 vrf red match-in-vrf
ip nat outside source static 2.2.2.200 2.2.2.2 vrf red match-in-vrf add-route
ip nat inside source list nat-acl-in1 pool pool-in1 vrf red match-in-vrf overload
ip nat outside source list nat-acl-out1 pool pool-out1 vrf red match-in-vrf add-route
interface Ethernet1/3
  ip nat outside
interface Ethernet1/5
  ip nat inside

N3548#show ip nat translation verbose
Pro Inside global      Inside local       Outside local      Outside global
any 1.1.1.1            10.1.1.2           ---                ---
    Flags:0x1  Entry-id:0  State:0x0  Group_id:0 Format(H:M:S) Time-left:0:0:-1
icmp 101.1.0.1:65351   101.0.0.1:0        102.1.0.1:231      102.1.0.1:231
    Flags:0x82  Entry-id:101  State:0x3  Group_id:0 VRF: red Format(H:M:S) Time-left:12:0:9
udp 101.1.0.1:65383    101.0.0.1:63       102.1.0.1:63       102.1.0.1:63
    Flags:0x82  Entry-id:103  State:0x3  Group_id:0 VRF: red Format(H:M:S) Time-left:12:0:9
tcp 101.1.0.1:64549    101.0.0.1:8809     102.1.0.1:9087     102.1.0.1:9087
    Flags:0x82  Entry-id:102  State:0x1  Group_id:0 VRF: red Format(H:M:S) Time-left:12:0:9

    syn:0:1:9  fin-rst:12:0:9
```