スタティック NAT とダイナミック NAT 変換の設定

この章の内容は、次のとおりです。

- ネットワーク アドレス変換の概要，1 ページ
- スタティック NAT に関する情報，2 ページ
- スタティック Twice NAT の概要，4 ページ
- ダイナミック NAT の概要，4 ページ
- NAT の内部アドレスおよび外部アドレス，5 ページ
- スタティック NAT のライセンス要件，6 ページ
- スタティック NAT の注意事項および制約事項，6 ページ
- ダイナミック NAT に関する制約事項，7 ページ
- スタティック NAT の設定，8 ページ
- ダイナミック NAT の設定，17 ページ

ネットワーク アドレス変換の概要

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、2 つのネットワークを接続するもの）で動作し、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（グローバルに一意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、少なくとも内部ネットワークに対して 1 つ、外部ネットワークに対して 1 つのインターフェイスがあります。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 IP アドレスをグローバルで一意の IP 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 はグローバルで一意の宛先 IP アドレスをローカル IP アドレスに変換します。出力点が複数存在する場合、個々の点で設定された NAT は、同一の変換テーブルを持っていなければなりません。

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

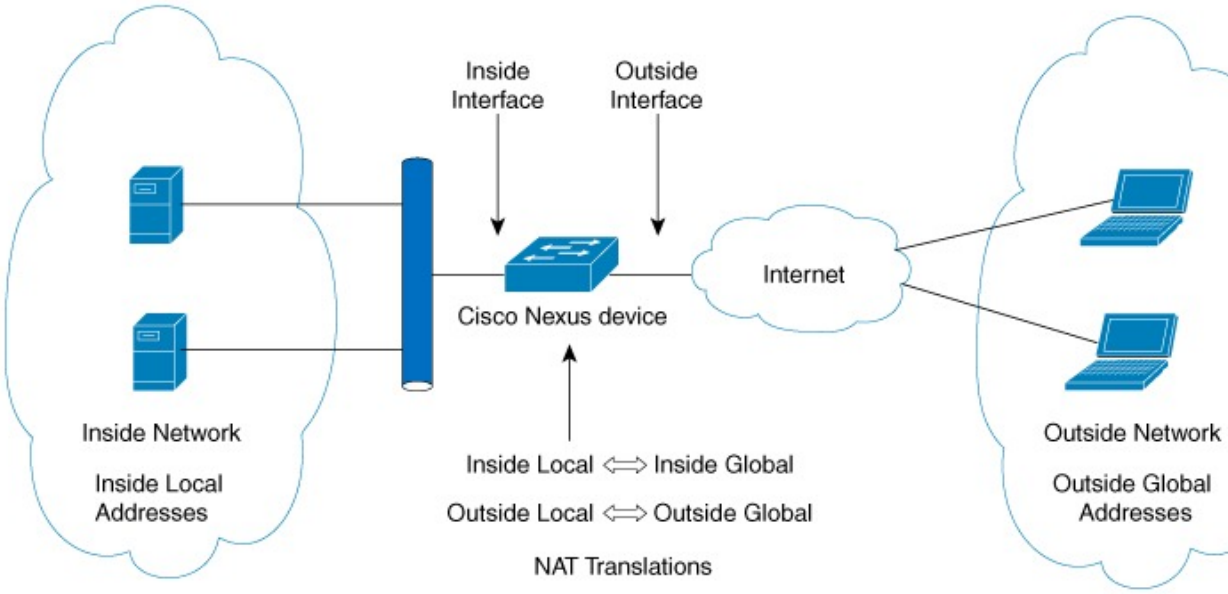
スタティック ネットワーク アドレス変換（NAT）を使用すると、ユーザは内部ローカル アドレスから外部グローバル アドレスへの 1 対 1 変換を設定することができます。これにより、内部から外部トラフィックおよび外部から内部トラフィックへの IP アドレスとポート番号の両方の変換が可能になります。Cisco Nexus デバイスはヒットレス NAT をサポートします。これは、既存の NAT トラフィック フローに影響を与えずに NAT 設定で NAT 変換を追加または削除できることを意味します。

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た 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。

スタティック Twice 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パケットとして変換されると、Twice NAT と呼ばれます。Twice NAT は、スタティック変換でのみサポートされます。

Twice NAT は、変換グループの一部として、2 つの NAT 変換（1 つの内部および 1 つの外部）を設定することができます。これらの変換は、NAT デバイスを通して流れるように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、個々の変換と組み合わせ変換の両方が有効になります。

NAT の内部変換では、パケットが内部から外部へ流れる際に、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際に、宛先の IP アドレスとポート番号を変更します。NAT の外部変換では、パケットが外部から内部に流れる際に、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際に、宛先 IP アドレスとポート番号を変更します。

Twice NAT を使用しない場合、変換ルールのうちの 1 つだけがパケット、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、Twice NAT 設定と見なされます。スタティック設定が、設定されたグループ ID を持っていない場合は、Twice NAT 設定では動作しません。グループ ID によって識別される単一つのグループに属するすべての内部および外部 NAT 変換は、Twice NAT 変換を形成するように対になっています。

ダイナミック NAT の概要

ダイナミック ネットワーク アドレス変換（NAT）は、実 IP アドレスのグループを宛先ネットワーク上でルーティング可能なマッピングされた IP アドレスに変換します。ダイナミック NAT では、未登録および登録 IP アドレス間の 1 対 1 のマッピングを確立しますが、マッピングは通信時に利用可能な登録済みの IP アドレスに応じて変えることができます。

ダイナミック NAT の設定は、自動的に内部ネットワークと外部ネットワーク間またはインターネット間のファイアウォールを作成します。ダイナミック NAT は、スタブ ドメイン内で生じる接続だけを許可します。外部ネットワーク デバイスは、デバイスが通信を開始しない限り、ネットワークのデバイスに接続できません。

ダイナミック NAT 変換は、変換が必要なトラフィックをデバイスが受信するまで、NAT 変換テーブルには存在しません。ダイナミック変換は、新しいエントリのスペースを作成するために使用しないときに、クリアまたはタイムアウトされます。通常、NAT 変換エントリは、TCAM（Ternary

Content Addressable Memory）エントリが制限されてい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。

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。オーバーロードとしても知られている PAT は、異なるポートを使用することにより、単一の登録済み IP アドレスに複数の未登録の IP アドレスをマッピングするダイナミック NAT の一形態です。NAT 設定は、同一または異なる ACL を使用して複数のダイナミック NAT 変換することができます。ただし、特定の ACL では、1 つのインターフェイスだけしか指定することができません。

エージングでは、設定可能な次の 3 つの異なるオプションがあります。

- 1 タイムアウト：これは、フローのすべてのタイプ（TCP および UDP の両方）に適用されます
- 2 TCP タイムアウト：これは TCP フローにのみ適用されます
- 3 UDP タイムアウト：これは UDP フローにのみ適用されます

NAT の内部アドレスおよび外部アドレス

NAT の内部は、変換する必要があ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 の外側は、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。これらは一般に、組織の制御下にはありません。外部ネットワーク内のホストを変換の対象にすることができ、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：ネットワークの内部に表示されるローカル IP アドレス。
- グローバル アドレス：ネットワークの外部に表示されるグローバル IP 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、多くの場合、Internet Network Information Center（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。アドレスは必ずしも正規ではありません。アドレスは、内部でルート可能なアドレス空間から割り当てられます。
- 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ます。

スタティック NAT のライセンス要件

次の表に、スタティック NAT のライセンス要件を示します。

製品	ライセンス要件
Cisco NX-OS	

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 の変換に対応しています。
- 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
- NAT はデフォルトの仮想ルーティングおよびフォワーディング（VRF）テーブルのみでサポートされます。
- 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。
  - ソフトウェアの変換。すべての変換はハードウェアで行われます。
  - 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。
- HSRP および VRRP は NAT インターフェイ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。
- Twice NAT はサポートされていません。（Twice NAT は、データグラムがアドレスのドメインを（内部から外部または外部から内部に）通過するときに送信元アドレスと宛先アドレスの両方が NAT によって変更される NAT のバリエーションです）。
- 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。

ダイナミック NAT に関する制約事項

次の制限はダイナミック ネットワーク アドレス変換（NAT）に適用されます。

- 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 レイヤ ゲートウェイ（ALG）変換はサポートされません。アプリケーション レベル ゲートウェイとしても知られている ALG は、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 と仮想アクセス コントロール リスト（ACL）は、インターフェイスで同時にサポートされていません。インターフェイスで NAT または仮想 ACL のいずれかを設定することができます。
- 出力 ACL は、変換されたパケットには適用されません。
- デフォルト以外の Virtual Routing and Forwarding（VRF）インスタンスはサポートされません。
- MIB はサポートされていません。
- Cisco Data Center Network Manager（DCNM）はサポートされません。
- 複数のグローバル仮想デバイス コンテキスト（VDC）は、Cisco Nexus デバイスではサポートされていません。
- 外部ドメインから着信したトラフィックのダイナミック NAT 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 はサポートされません。ただし、NAT と Hot Standby Router Protocol（HSRP）は共存できます。
- レイヤ3インターフェイスでダイナミックNATを設定する場合、リロードした後またはNAT変換をクリアした後、既存の NAT 変換は学習されません。このため、NAT 設定に一致するアクセス コントロール リスト（ACL）のトラフィックのドロップがあります。これを回避

するには、NAT 設定を削除し、NAT 変換が学習できるように、同じインターフェイスで再設定します。

- タイムアウト値は、設定されているタイムアウト + 119 秒になります。

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

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

	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。

	コマンドまたはアクション	目的
		（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	switch(config)# **copy running-config startup-config**	（任意） 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。

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 デバイスは内部宛先 IP アドレス（newDst: ip1）への外部宛先 IP アドレス（Dst: ip2）の変換を暗黙的に追加します。

手順

	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*	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	switch(config)# **copy running-config startup-config**	（任意） 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。

次に、内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

	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-addresslocal-ip-address* [**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。ポートなしで内部変換が設定されると、暗黙的な追加ルートが実行されます。外部変換の設定中、最初の追加ルート機能はオプションです。
ステップ 3	switch(config)# **copy running-config startup-config**	（任意） 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。

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

	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*}}	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	switch(config)# **copy running-config startup-config**	（任意） 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。

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、サービスを特定の外部ホストにマッピングできます。

手順

	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*}}	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	switch(config)# **copy running-config startup-config**	（任意） 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

	コマンドまたはアクション	目的
		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。

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 Twice 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 Twice ネットワーク アドレス 変換（NAT）ルールを作成する際に考慮されます。

手順

	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 モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Switch# configure terminal`	特権 EXEC モードを開始します。
ステップ 3	**ip nat inside source static** *inside-local-ip-address outside-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、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 Twice 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** *inside-local-ip-address outside-global-ip-address* [**group** *group-id*] [**add-route**]	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、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 Twice NAT を設定します。

	コマンドまたはアクション	目的
	例： `Switch(config)# ip nat outside source static 209.165.201.1 10.3.2.42 group 4 add-route`	• **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** | **outside**} 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	**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。

外部送信元アドレスのスタティック Twice 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 Twice ネットワーク アドレス 変換（NAT）ルールを作成する際に考慮されます。内部および外部 NAT 変換のあらゆる組み合わせを Twice NAT ルールとして使用できます。

手順

	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 モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `switch# configure terminal`	特権 EXEC 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 nat outside source static** *local-ip-address global-ip-address* [**group** *group-id*] 例： `switch(config)# ip nat outside source static 10.1.1.1 192.168.34.4 group 4`	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 Twice 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	**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 5	**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 6	**ip nat** {**inside** | **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 7	**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。

NAT 制限の設定

NAT 制限を特定の値に設定する場合、すべての ASIC の TCAM の VACL リージョンで VACL をその値より小さくすることはできません。たとえば、NAT 制限を 400 に設定する場合、すべての ASIC の TCAM の VACL リージョンにオフセット 400 を下回る VACL を設定できません。NAT 制限を下回る VACL がある場合、このコマンドは、現在のすべての VACL がスイッチのリロード時に NAT 制限を満たすことができるかどうかを確認します。コマンドが完了すると、スイッチをリロードするように求められます。

手順

	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)# **hardware profile tcam feature nat limit** *tcam-size*	NAT TCAM 制限を設定します。*tcam-size* の有効範囲は 2 ～ 2048 です。
ステップ 3	switch(config)# **show hardware profile tcam feature nat limit** *tcam-size*	NAT 制限を表示します。
ステップ 4	switch(config)# **copy running-config startup-config**	（任意） 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。

次に、NAT 制限を 400 に設定する例を示します。

```
switch# configure terminal
switch(config)# hardware profile tcam feature nat limit 400
switch(config)# show hardware profile tcam feature nat limit 400
switch(config)# copy running-config startup-config
```

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 Twice NAT の設定

次の例は、内部送信元および外部送信元のスタティック Twice NAT 設定を設定する方法を示しています。

```
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)# end
```

例：外部送信元アドレスのスタティック Twice NAT の設定

次に、外部ローカル IP アドレス 10.1.1.2 と外部グローバル IP アドレス 192.168.34.4 に対してスタティック Twice NAT を設定する例を示します。

```
switch> enable
switch# configure terminal
switch(config)# ip nat outside source static 10.1.1.2 192.168.34.4 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 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

	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。

次に、スタティック NAT の設定を表示する例を示します。

```
switch# sh ip nat translations
Pro Inside global      Inside local       Outside local      Outside global

--- ---                ---                51.3.1.1           104.1.1.1
--- ---                ---                95.4.1.1           95.3.1.1
--- ---                ---                96.4.1.1           96.3.1.1
--- ---                ---                51.40.1.1          140.1.1.1
--- ---                ---                51.42.1.1          142.1.2.1
--- ---                ---                51.1.2.1           102.1.2.1
--- 11.1.1.1           101.1.1.1          ---                ---
--- 11.3.1.1           103.1.1.1          ---                ---
--- 11.39.1.1          139.1.1.1          ---                ---
```

```
--- 11.41.1.1          141.1.1.1          ---                ---
--- 95.1.1.1           149.1.1.1          ---                ---
--- 96.1.1.1           149.2.1.1          ---                ---
    130.1.1.1:590      30.1.1.100:5000    ---                ---
    130.2.1.1:590      30.2.1.100:5000    ---                ---
    130.3.1.1:590      30.3.1.100:5000    ---                ---
    130.4.1.1:590      30.4.1.100:5000    ---                ---
    130.1.1.1:591      30.1.1.101:5000    ---                ---
```

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

	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 モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
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。
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`	条件に一致したトラフィックを許可する IP アクセス リストの条件を設定する。
ステップ 5	**deny** *protocol source source-wildcard***any** 例： `Switch(config-acl)# deny udp 10.111.11.100/32 any`	ネットワークの入力からのパケットを拒否する IP アクセス リストの条件を設定する。
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。

	コマンドまたはアクション	目的
ステップ 7	**ip nat inside source list** *access-list-name***interface** *typenumber***overload** 例： `Switch(config)# ip nat inside source list acl1 interface ethernet 1/1 overload`	手順 3 で定義されたアクセス 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** *typenumber* 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-addressmask* 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** *typenumber* 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 13	**ip address** *ip-addressmask* 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`	外部ネットワークにインターフェイスを接続します。

	コマンドまたはアクション	目的
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。 • 設定されたタイムアウトの上限に達すると、動的に作成された NAT 変換がクリアされます。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。
ステップ 17	**ip nat translation max-entries** *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 ～ 1023 を指定できます。
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。 • 設定されたタイムアウトの上限に達すると、動的に作成された NAT 変換がクリアされます。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。
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。 • NAT は、**tcp-timeout** または **udp-timeout** キーワードが設定されていない場合のみ、このタイムアウト値を使用します。
ステップ 20	**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。

ダイナミックおよびスタティック Twice NAT 設定の確認

手順

ステップ 1 **enable**

例：
```
Switch> enable
```
特権 EXEC モードをイネーブルにします。

- パスワードを入力します（要求された場合）。

ステップ 2 **show ip nat translations**

例：
```
Switch# show ip nat translations
```
ネットワーク アドレス変換（NAT）のアクティブな変換を表示します。

- エントリがいつ生成され、いつ使用されたかを含む各変換テーブルエントリの追加情報が表示されます。

例

次に、**show ip nat translations** コマンドの出力例を示します。
```
switch# show ip nat translations

Pro Inside global      Inside local       Outside local      Outside global
any ---                ---                10.4.4.40          203.2.133.20
tcp ---                ---                10.24.1.133:333    198.5.133:555
any 192.168.1.140      10.1.1.40          ---                ---
any 192.168.1.140      10.1.1.40          10.4.4.40          203.2.133.20
tcp 172.16.9.142:777   10.2.2.42:444      ---                ---
tcp 172.16.9.142:777   10.2.2.42:444      10.24.1.133:333    198.5.133:555
```

例：ダイナミック変換および変換タイムアウトの設定

次の例では、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 ネットワーク アドレス変換（NAT）を設定する方法を示します。
```
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
```