ネットワーク アドレス変換の設定： スタート ガイド

目次

概要

このドキュメントでは、一般的なネットワーク シナリオにおける、Cisco ルータでの Network Address Translation（NAT; ネットワーク アドレス変換）の設定について説明しています。 このドキュメントの対象読者は、NAT を初めて設定するユーザです。

注: このドキュメントで使用されている「インターネット」または「インターネット デバイス」という用語は、任意の外部ネットワークにあるデバイスを意味します。

前提条件

要件

このドキュメントを読むには、Network Address Translation（NAT; ネットワーク アドレス変換）との接続で使用される用語についての基本的な知識が必要です。 一部の用語の定義については、『NAT： ローカルおよびグローバルの定義』を参照してください。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

Cisco 2500 シリーズ ルータ

Cisco IOS® ソフトウェア リリース 12.2(10b)

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

クイック スタート手順：NAT の設定と展開

NAT を設定する場合、特に NAT の初心者にとっては、どこから手をつければよいかわからないことがよくあります。 NAT の機能の定義手順と設定方法は、次が参考になります。

NAT の内部インターフェイスと外部インターフェイスを定義します。

ユーザーが属するインターフェースは複数ありますか？

インターネットに出て行くインターフェースは複数ありますか。

NAT によって何を達成しようとしているのかを定義します。

内部ユーザがインターネットにアクセスできるようにしますか。

インターネットから内部デバイス（メール サーバや Web サーバなど）にアクセスできるようにしますか。

TCP トラフィックを別の TCP ポートまたはアドレスにリダイレクトしますか。

ネットワーク移行時に NAT を使用しますか（たとえば、サーバの IP アドレスを変更したときに、すべてのクライアントの更新が完了するまでの間、未更新クライアントは元の IP アドレスを使用してサーバにアクセスでき、更新済みクライアントは新しいアドレスを使用してサーバにアクセスできるようにする）。

NAT を使用して、オーバーラッピング ネットワーク同士が通信できるようにしますか。

前のステップで定義した目的を達成するために、NAT を設定します。 ステップ 2 で定義し

た目的に従って、次の機能の中からどれを使用するかを決定します。

スタティック NAT

ダイナミック NAT

オーバーロード

上記の組み合わせ

NAT の動作を確認します。

以降の NAT の例はそれぞれ、上記のクイック スタート手順のステップ 1 ~ 3 の内容を具体的に示しています。 これらの例で取り上げられているのはいずれも、NAT の展開が推奨される一般的なシナリオです。

NAT の内部インターフェイスと外部インターフェイスの定義

NAT を展開するための最初のステップは、NAT の内部インターフェイスと外部インターフェイスを定義することです。 内部ネットワークを内部、外部ネットワークを外部と定義するのが最も簡単であると思われるかもしれません。 ただし、「内部」と「外部」という用語はどちらも使用目的によって決まります。 次の図に、この例を示します。

例： 内部ユーザがインターネットにアクセスできるようにする場合

内部ユーザがインターネットにアクセスできるようにすることは可能であるものの、有効アドレスの数がすべてのユーザに対応できるほど十分にない場合があります。 インターネット上のデバイスとの通信がすべて内部デバイスから開始される場合は、1 つの有効アドレスか、または有効アドレスのプールが必要です。

次の図は、内部および外部として定義されたルータ インターフェイスを含む単純なネットワーク構成図です。

この例では、NAT の使用目的を「各デバイスの無効なアドレスを 1 つの有効アドレスまたはアドレス プールに変換して、内部にある特定のデバイス (サブネットごとに最初の 31 のデバイス) が外部デバイスとの通信を開始できるようにすること」と定義しました。 アドレス プールは、172.16.10.1 ~ 172.16.10.63 の範囲で定義されています。

これで NAT を設定する準備ができました。 上記の目的を達成するには、ダイナミック NAT を使用します。 ダイナミック NAT では、ルータ上の変換テーブルに最初は何も登録されておらず、変換が必要なトラフィックがルータを通過するたびにエントリが追加されます。 それに対してスタティック NAT では、変換があらかじめ静的に設定されており、変換が必要なトラフィックがなくても変換テーブル内にエントリが登録されています。

この例では、NAT を設定して、Inside デバイスをそれぞれ異なる有効アドレスに変換できます。また、Inside デバイスすべてを同じ有効アドレスに変換することも可能です。 後者の方法をオーバーロードと呼びます。 各方法の設定例を次に示します。

内部ユーザがインターネットにアクセスできるようにする NAT の設定

NAT ルータ
interface ethernet 0 ip address 10.10.10.1 255.255.255.0 ip nat inside *!--- Defines Ethernet 0 with an IP address and as a NAT inside interface.* interface ethernet 1 ip address 10.10.20.1 255.255.255.0 ip nat inside *!--- Defines Ethernet 1 with an IP address and as a NAT inside interface.* interface serial 0 ip address 172.16.10.64 255.255.255.0 ip nat outside *!--- Defines serial 0 with an IP address and as a NAT outside interface.* ip nat pool no-overload 172.16.10.1 172.16.10.63 prefix 24 ! *!-- Defines a NAT pool named no-overload with a range of addresses !--- 172.16.10.1 - 172.16.10.63.* ip nat inside source list 7 pool no-overload ! ! *!--- Indicates that any packets received on the inside interface that !--- are permitted by access-list 7 has !--- the source address translated to an address out of the !--- NAT pool "no-overload".* access-list 7 permit 10.10.10.0 0.0.0.31 access-list 7 permit 10.10.20.0 0.0.0.31 *!--- Access-list 7 permits packets with source addresses ranging from !--- 10.10.10.0 through 10.10.10.31 and 10.10.20.0 through 10.10.20.31.*

注: NAT コマンドで参照されるアクセス リストを **permit any** 付きで設定しないでください。 **permit any** を使用すると NAT によって大量のルータ リソースが消費され、ネットワークの問題を引き起こすおそれがあります。

前述の設定では、サブネット 10.10.10.0 から最初の 32 アドレスと、サブネット 10.10.20.0 から最初の 32 アドレスのみが **access-list 7** によって許可されています。 したがって、これらの送信元アドレスのみが変換されます。 内部ネットワークには、これ以外のアドレスを持つデバイスがある可能性がありますが、それらは変換されません。

最後のステップは、NAT が意図したとおりに動作していることを確認することです。

オーバーロードにより内部ユーザがインターネットにアクセスできるようにする NAT の設定

NAT ルータ
interface ethernet 0 ip address 10.10.10.1 255.255.255.0 ip nat inside *!--- Defines Ethernet 0 with an IP address and as a NAT inside interface.* interface ethernet 1 ip address 10.10.20.1 255.255.255.0 ip nat inside *!--- Defines Ethernet 1 with an IP address and as a NAT inside interface.* interface serial 0 ip address 172.16.10.64 255.255.255.0 ip nat outside *!--- Defines serial 0 with an IP address and as a NAT outside interface.* ip nat pool ovrld 172.16.10.1 172.16.10.1 prefix 24 ! *!--- Defines a NAT pool named ovrld with a range of a single IP !--- address, 172.16.10.1.* ip nat inside source list 7 pool ovrld overload ! ! ! ! *!--- Indicates that any packets received on the inside interface that !--- are permitted by access-list 7 has the source address !--- translated to an address out of the NAT pool named ovrld. !--- Translations are overloaded, which allows*

```
multiple inside !--- devices to be translated to the
same valid IP address. access-list 7 permit 10.10.10.0
0.0.0.31 access-list 7 permit 10.10.20.0 0.0.0.31 !---
Access-list 7 permits packets with source addresses
ranging from !--- 10.10.10.0 through 10.10.10.31 and
10.10.20.0 through 10.10.20.31.
```

前述の 2 番目の設定では、NAT プール ovrld の範囲に 1 つのアドレスしか含まれていません。 **ip nat inside source list 7 pool ovrld overload** コマンドのようにキーワード **overload** を使用すると、複数の Inside デバイスがプール内の単一アドレスに変換されます。

このコマンドのもう 1 つの形が **ip nat inside source list 7 interface serial 0 overload** です。このように設定すると、serial 0 インターフェイスに割り当てられたアドレスにオーバーロードされます。

オーバーロードを設定すると、ルータではグローバル アドレスを適切なローカル アドレスに逆変換するために、高レベル プロトコルからの情報（TCP ポート番号や UDP ポート番号など）が保持されます。 グローバル アドレスとローカル アドレスの定義については、『NAT： グローバルおよびローカルの定義』を参照してください。

最後のステップは、NAT が意図したとおりに動作していることを確認することです。

例： インターネットから内部デバイスにアクセスできるようにする場合

インターネットにあるデバイスと情報を交換する内部デバイスが必要となる場合があります。この場合、通信はインターネット デバイスから開始されます。 典型的な例として、インターネット上のデバイスが内部ネットワークにあるメール サーバに電子メールを送信するケースが挙げられます。

インターネットから内部デバイスにアクセスできるようにする NAT の設定

この例では、まず NAT の内部インターフェイスと外部インターフェイスを上記のネットワーク構成図のように定義します。

次に、内部ユーザが外部との通信を開始できるように定義します。 Outside のデバイスは、Inside のメール サーバとの通信のみを開始できるようにする必要があります。

次のステップは NAT の設定です。 上記の目的を達成するには、スタティック NAT とダイナミック NAT をどちらも設定します。 この例の設定方法については、『スタティック NAT とダイナミック NAT の同時設定』を参照してください。

最後のステップは、NAT が意図したとおりに動作していることを確認することです。

例： TCP トラフィックを別の TCP ポートまたはアドレスにリダイレクトする場合

インターネット上のデバイスが内部デバイスとの通信を開始する必要があるもう 1 つの例が、内部ネットワークに Web サーバがある場合です。 内部 Web サーバでは、TCP ポート 80 以外のポートで Web トラフィックをリスニングするように設定することがあります。 たとえば 内部 Web サーバを、TCP ポート 8080 をリッスンするように設定することがあります。 この場合は、NAT を使用して、TCP ポート 80 宛てのトラフィックを TCP ポート 8080 にリダイレクトできます。

インターフェイスを上記のネットワーク構成図のように定義した後、NAT の使用目的を「Outside から到達した 172.16.10.8:80 宛てのパケットを 172.16.10.8:8080 にリダイレクトすること」と決定します。 この目的を達成するには、**static nat コマンド**を使用して TCP ポート番号を変換します。 設定例を次に示します。

TCP トラフィックを別の TCP ポートやアドレスにリダイレクトする NAT の設定

NAT ルータ

```
interface ethernet 0
 ip address 172.16.10.1 255.255.255.0
 ip nat inside
!--- Defines Ethernet 0 with an IP address and as a NAT
inside interface. interface serial 0 ip address
200.200.200.5 255.255.255.252 ip nat outside !---
Defines serial 0 with an IP address and as a NAT outside
interface. ip nat inside source static tcp 172.16.10.8
8080 172.16.10.8 80 !--- Static NAT command that states
any packet received in the inside !--- interface with a
source IP address of 172.16.10.8:8080 is !--- translated
to 172.16.10.8:80.
```

上記のスタティック NAT コマンドの設定は、内部インターフェイスで受信された、送信元アドレスが 172.16.10.8:8080 であるパケットがすべて 172.16.10.8:80 に変換されることを示しています。 これはまた、内部インターフェイスで受信された、宛先アドレスが 172.16.10.8:80 であるパケットがすべて 172.16.10.8:8080 の宛先に変換されることも意味します。

最後のステップは、NAT が意図したとおりに動作していることを確認することです。

```
show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
tcp 172.16.10.8:80     172.16.10.8:8080   ---                ---
```

例： ネットワーク移行時に NAT を使用する場合

ネットワーク上のデバイスのアドレスを変更する場合や、あるデバイスを別のデバイスに置き換える場合は、NAT を使用すると便利です。 たとえば、ネットワーク内のすべてのデバイスが使用している特定のサーバを、新しい IP アドレスを持つ新しいデバイスに置き換える場合、すべてのネットワーク デバイスの設定を新しいサーバ アドレスに変更するには相当時間がかかります。 その間に、古いアドレスを使用しているデバイスのパケットを変換するよう NAT を設定すれば、それらのデバイスと新しいサーバが通信可能になります。

NAT インターフェイスを上記のように定義した後、NAT の使用目的を「外部から到達した、古いサーバ アドレス (172.16.10.8) 宛てのパケットを変換し、新しいサーバ アドレスに送信すること」と決定しました。 新しいサーバは別の LAN にあるため、この LAN 上のデバイス、またはこの LAN を経由して到達可能なデバイス (ネットワークの Inside 側にあるデバイス) は、可能であれば新しいサーバの IP アドレスを使用できるように設定します。

上記の目的を達成するには、スタティック NAT を使用します。 次に設定例を示します。

ネットワーク移行時に使用するための NAT の設定

NAT ルータ

```
interface ethernet 0
 ip address 172.16.10.1 255.255.255.0
 ip nat outside
!--- Defines Ethernet 0 with an IP address and as a NAT
```

```
outside interface. interface ethernet 1 ip address
172.16.50.1 255.255.255.0 ip nat inside !--- Defines
Ethernet 1 with an IP address and as a NAT inside
interface. interface serial 0 ip address 200.200.200.5
255.255.255.252 !--- Defines serial 0 with an IP
address. This interface is not !--- participating in
NAT. ip nat inside source static 172.16.50.8 172.16.10.8
!--- States that any packet received on the inside
interface with a !--- source IP address of 172.16.50.8
is translated to 172.16.10.8.
```

この例の inside source NAT コマンドは、外部インターフェイスで受信された、宛先アドレスが 172.16.10.8 であるパケットがすべて 172.16.50.8 の宛先アドレスに変換されることも意味します。

最後のステップは、NAT が意図したとおりに動作していることを確認することです。

例： 重複ネットワークでの NAT の使用

オーバーラッピング ネットワークは、インターネット内の他のデバイスですでに使用されている IP アドレスを内部デバイスに割り当てたときに起こります。 また、社内ネットワークでいずれも RFC 1918 IP アドレスを使用している 2 つの企業が合併した場合にも、重複ネットワークが生じます。 これら 2 つのネットワークは、できればすべてのデバイスのアドレスを再設定せずに通信できる必要があります。 この目的で NAT を設定する場合についての詳細は、『重複ネットワークでの NAT の使用』を参照してください。

1 対 1 のマッピングと多対多のマッピングの違い

スタティック NAT 設定では、1 対 1 のマッピングが作成され、特定のアドレスが別のアドレスに変換されます。 このタイプの設定では、設定が存在する限り、NAT テーブルに恒久的なエントリが作成され、内部ホストと外部ホストの両方から接続を開始できます。 これは、主にメール、Web、FTP などのアプリケーション サービスを提供するホストで便利な設定です。 次に、例を示します。

```
Router(config)#ip nat inside source static 10.3.2.11 10.41.10.12 Router(config)#ip nat inside
source static 10.3.2.12 10.41.10.13
```

ダイナミック NAT は、変換されるホストの実際の数より使用できるアドレスが少ない場合に便利です。 ホストが接続を開始すると NAT テーブルにエントリが作成され、アドレス間に 1 対 1 のマッピングが確立されます。 ただし、マッピングは変化する場合があり、通信の時点でのプール内の使用可能な登録済みアドレスに依存します。 ダイナミック NAT では、NAT が設定されている Inside または Outside のネットワークからのみ、セッションを開始できます。 一定の時間ホストが通信を行わないと、ダイナミック NAT のエントリは変換テーブルから削除されます。この時間は設定可能です。 次に、アドレスはプールに戻されて、別のホストが使用できるようになります。

たとえば、詳細設定の次の手順を実行します。

アドレスのプールを作成します。

```
Router(config)#ip nat pool MYPOOLEXAMPLE 10.41.10.1 10.41.10.41 netmask 255.255.255.0
```

マッピングする必要のある内部ネットワークの access-list を作成します。

```
Router(config)#access-list 100 permit ip 10.3.2.0 0.0.0.255 any
```

NAT 対象の内部ネットワーク 10.3.2.0 0.0.0.255 を選択する access-list 100 をプール MYPOOLEXAMPLE と関連付けた後、アドレスをオーバーロードします。

```
Router(config)#ip nat inside source list 100 pool MYPOOLEXAMPLE overload
```

NAT の動作確認

NAT の設定が完了したら、それが期待通りに動作するかを確認します。 これには次に記載するようないくつかの方法があります。 ネットワーク アナライザの使用や、**show コマンド**、**debug コマンド**の使用など。 NAT の動作確認例についての詳細は、『NAT オペレーションの検証と NAT の基本的なトラブルシューティング』を参照してください。

結論

このドキュメントの例は、クイック スタート手順が NAT の設定と展開に役立つことを具体的に示しています。 クイック スタート手順は、次のステップから構成されています。

NAT の内部インターフェイスと外部インターフェイスを定義します。

NAT によって何を達成しようとしているのかを定義します。

ステップ 2 で定義した目的を達成するために、NAT を設定します。

NAT の動作を確認します。

前述のそれぞれの例では、さまざまな形式の **ip nat inside コマンド**が使用されています。 NAT の動作の順序に留意すれば、**ipnat outside コマンド**を使用しても同じ目的を達成できます。 **ip nat outside コマンド**を使用した設定例については、『ip nat outside source list コマンドを使用した設定例』および『ip nat outside source static コマンドを使用した設定例』を参照してください。

前述の例では次のアクションも示されています。

コマンド	Action
ip nat inside source	• 内部から外部へ送られる IP パケットの送信元が変換されます。 • 外部から内部へ送られる IP パケットの宛先が変換される。
ip nat outside source	• 外部から内部へ移動する IP パケットの発信元を変換します。 • 内部から外部へ送られる IP パケットの宛先が変換される。

関連情報

- NAT に関するサポートページ
- IP ルーティング プロトコルに関するサポート ページ

- IP ルーティングに関するサポート ページ
- NAT の機能
- NAT の処理順序
- Cisco IOS NAT についての FAQ
- テクニカルサポートとドキュメント - Cisco Systems