ネットワークアドレス変換の設定

内容

はじめに

このドキュメントでは、Cisco ルータでネットワークアドレス変換（NAT）を設定する方法について説明します。

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。

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いています。

- 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ました。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。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

表記法

表記法の詳細については、『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の設定と導入

注：このドキュメントで「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、外部ネットワーク上のデバイスを意味します。

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。

1. 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？
    - インターネットに使用できるインターフェイスは複数ありますか。
2. NATを使用して何を実現するかを定義します。
    - 内部ユーザにインターネットへのアクセスを許可しますか？
    - 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アドレスを変更してすべてのクライアントを更新するまでは、更新されていないクライアントが元のIPアドレスでサーバにアクセスし、更新されたクライアントが新しいアドレスでサーバにアクセスできるようにしますか）？
    - を使用して、オーバーラップするネットワークが通信できるようにしますか？
3. 前に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で定義した内容に基づいて、次に使用する機能を決定する必要があります。
    - スタティック NAT
    - ダイナミック NAT
    - Overloading

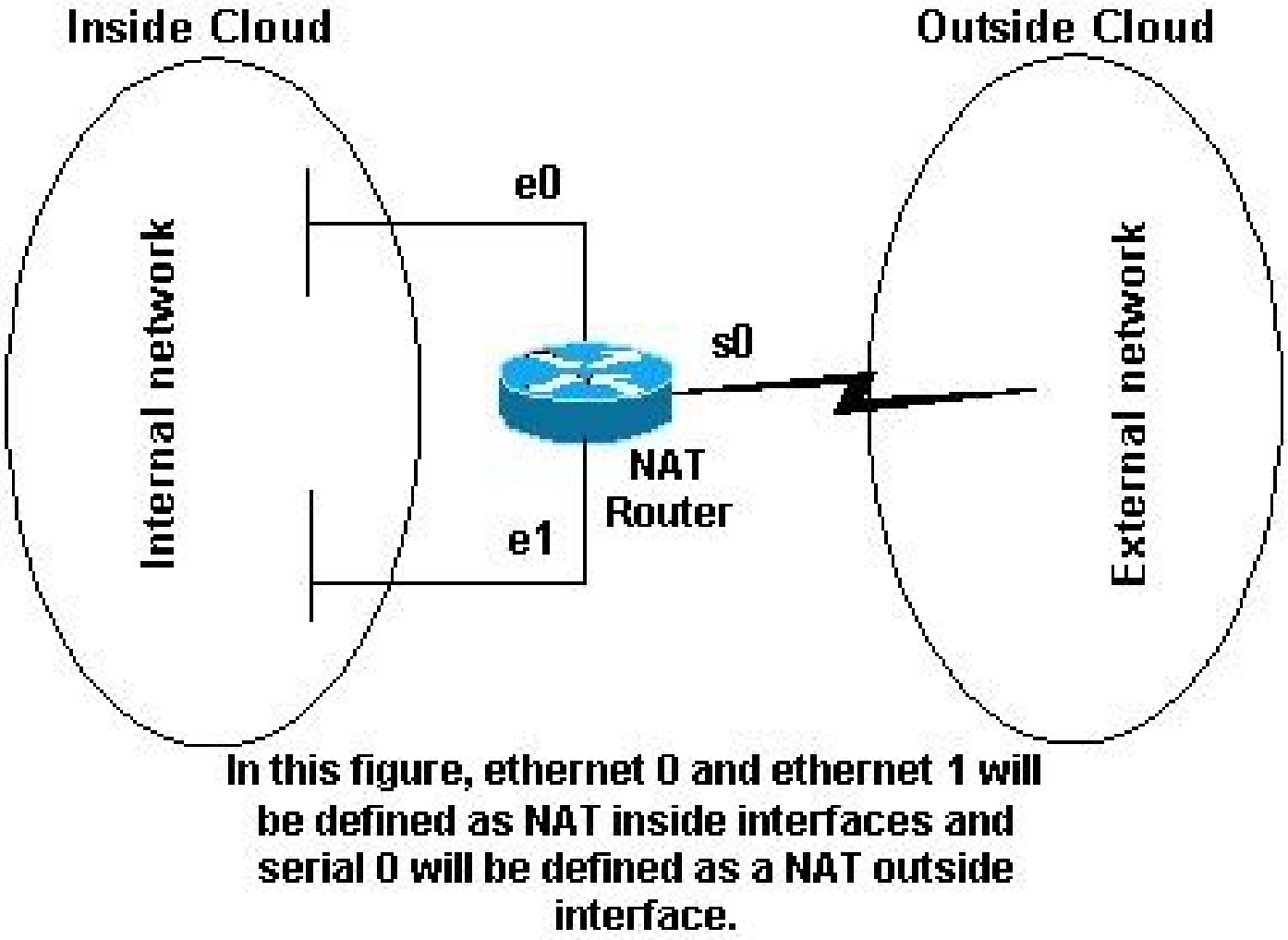
- これらの機能の任意の組み合わせ

4. NAT の動作を確認します。

これらのNATの例はそれぞれ、前の図のクイックスタートステップのステップ1 ~ 3を示しています。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として定義し、外部ネットワークを外部として定義するのが最も簡単です。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。



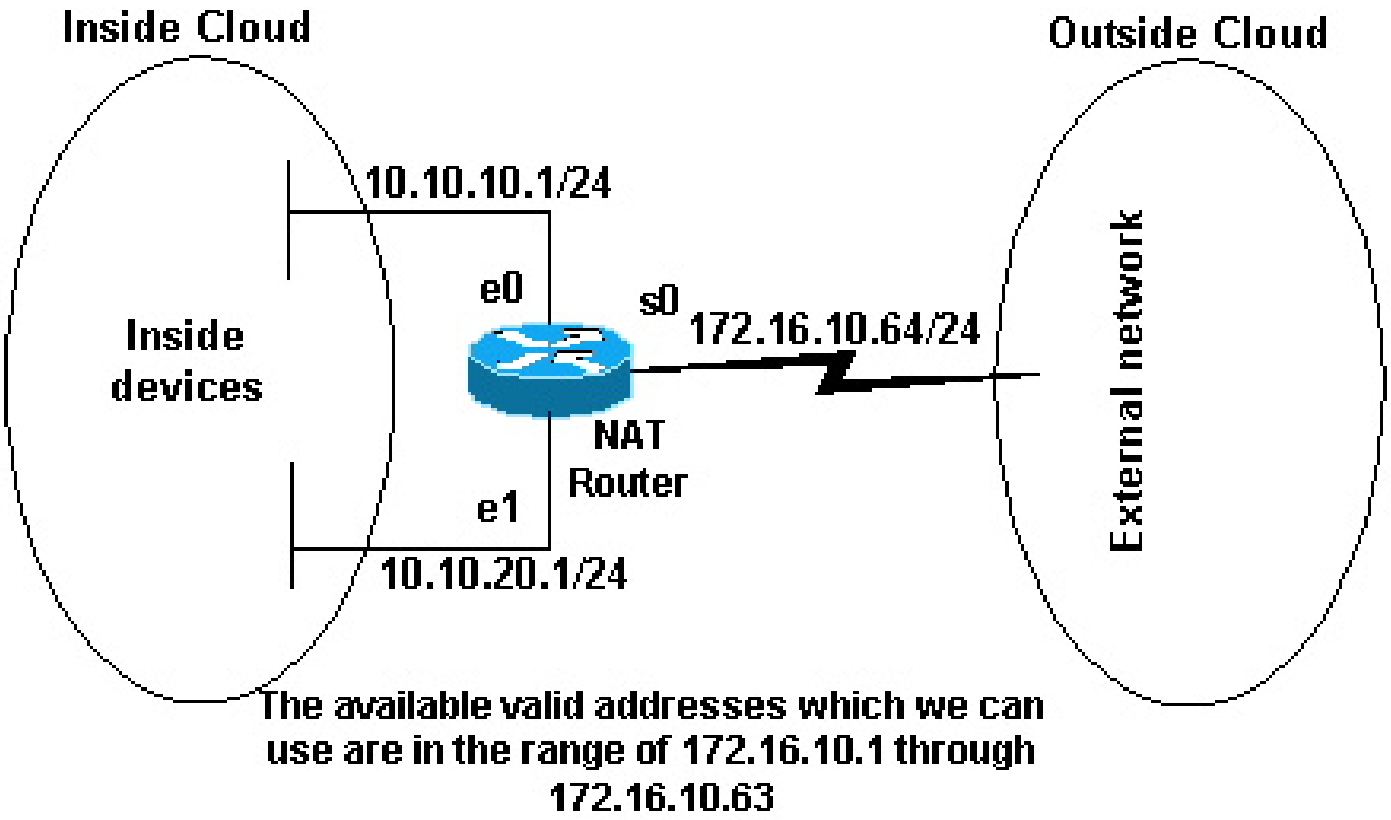
NAT トポロジ

例

1.内部ユーザのインターネットへのアクセスを許可する

内部ユーザにインターネットへのアクセスを許可する一方で、すべてのユーザに対応できる有効なアドレスが不足している可能性があります。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ダイアグラムです。



使用可能な有効なアドレス

この例では、Insideの特定のデバイス (各サブネットの最初の31) がOutsideのデバイスとの通信を開始できるようにし、それらの無効なアドレスを有効なアドレスまたはアドレスプールに変換します。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を設定できます。前の図で定義した内容を実現するには、ダイナミックNATを使用します。ダイナミックNATでは、ルータの変換テーブルは、最初は空で、ルータ変換されたパススルー必要があるトラフィックを一度設定されます。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。この2番目の方法は、と呼ばれま overloading 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NATを設定する

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を使用して設定しないことを強く推奨します。 NATでpermit anyを使用すると、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可能性があります。

上記の設定では、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。内部ネットワーク上に他のアドレスを持つ他のデバイスが存在する可能性がありますが、こ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。

内部ユーザがオーバーロードでインターネットにアクセスできるようにNATを設定する

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.
```

上記の2番目の設定では、NATプール ovrld1つのアドレスの範囲だけが設定されています。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

数の内部デバイスがプール内の単一アドレスに変換されます。

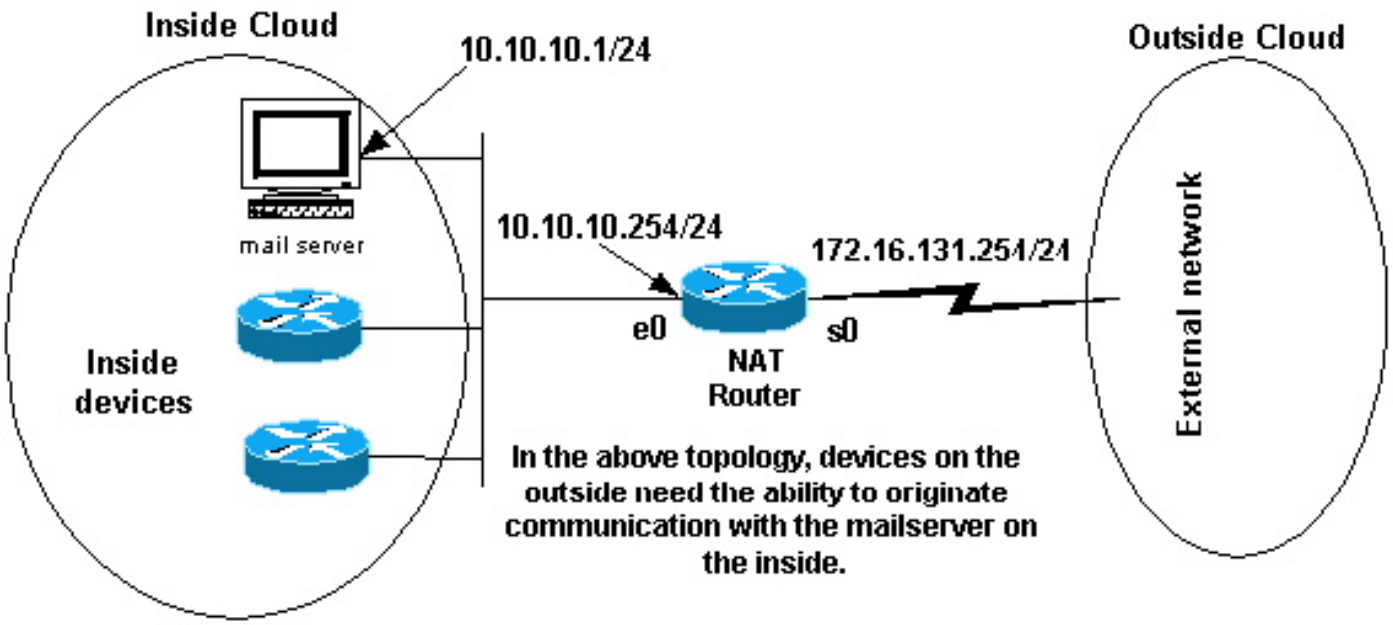
このコマンドのもう1つのバリエーションは、isip nat inside source list 7 interface serial 0 overloadです。このコマンドは、serial 0インターフェイスに割り当てられたアドレスにオーバーロードするようにNATを設定します。

が設定さoverloadingれている場合、ルータは上位レベルのプロトコル（TCPまたはUDPポート番号など）からの情報を保持して、グローバルアドレスを正しいローカルアドレスに逆変換します。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：ローカルおよびグローバルの定義』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。

2.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

インターネット上のデバイスと情報を交換するために内部デバイスが必要になる場合があります。インターネット上のデバイスでは、電子メールなどのインターネットデバイスから通信が開始されます。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。



通信の開始

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。

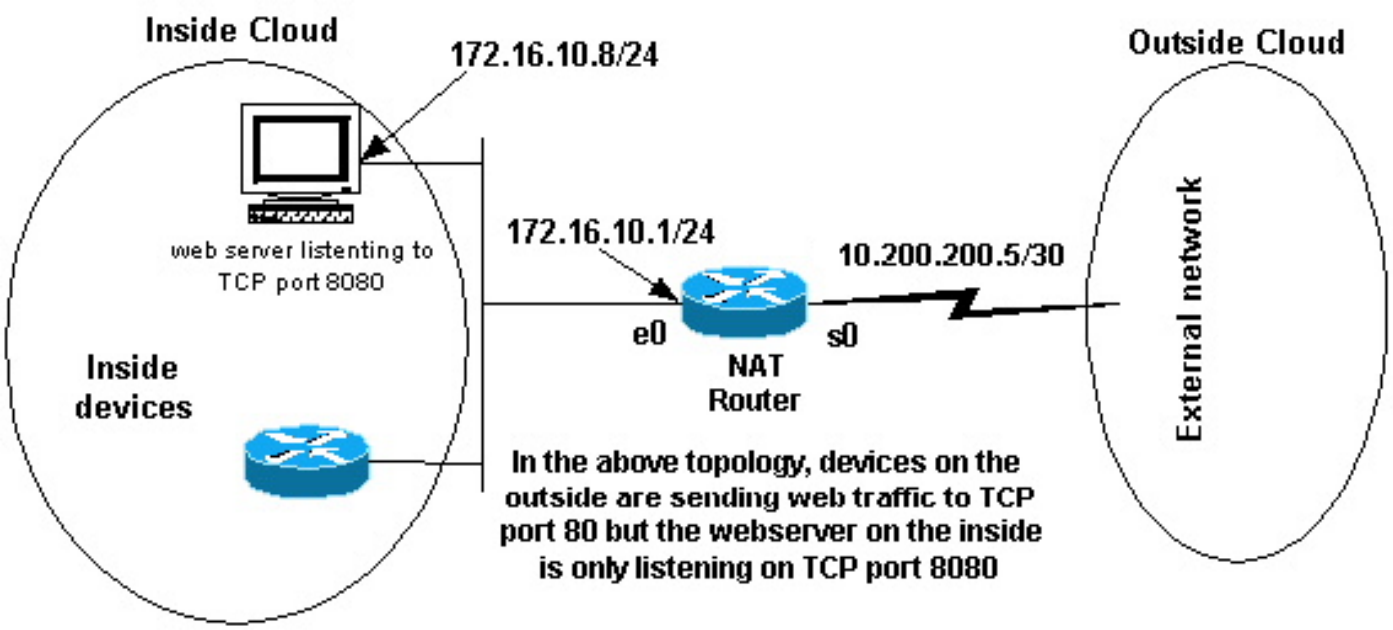
次に、内部ユーザが外部との通信を開始できるように定義します。Outsideのデバイスは、Insideのメールサーバのみとの通信を開始できる必要があります。

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の詳細は、『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することを確認することです。

3. 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

内部ネットワーク上のWebサーバは、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場合のもう1つの例です。場合によっては、内部Webサーバは、ポート80以外のTCPポートでWebトラフィックをリッスンするように設定できます。たとえば、TCPポート8080をリッスンするように内部Webサーバを設定できます。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。



Webトラフィックの TCPポート

前のネットワークダイアグラムに示すようにインターフェイスを定義した後、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」と決定できます。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ポートまたはアドレスにリダイレクトするためのNATの設定

NAT ルータ

`interface ethernet 0`
`ip address 172.16.10.1 255.255.255.0`
`ip nat inside`
 	
`!--- Defines Ethernet 0 with an IP address and as a NAT inside interface.`
 	
`interface serial 0`
`ip address 10.200.200.5 255.255.255.252`
`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.
```

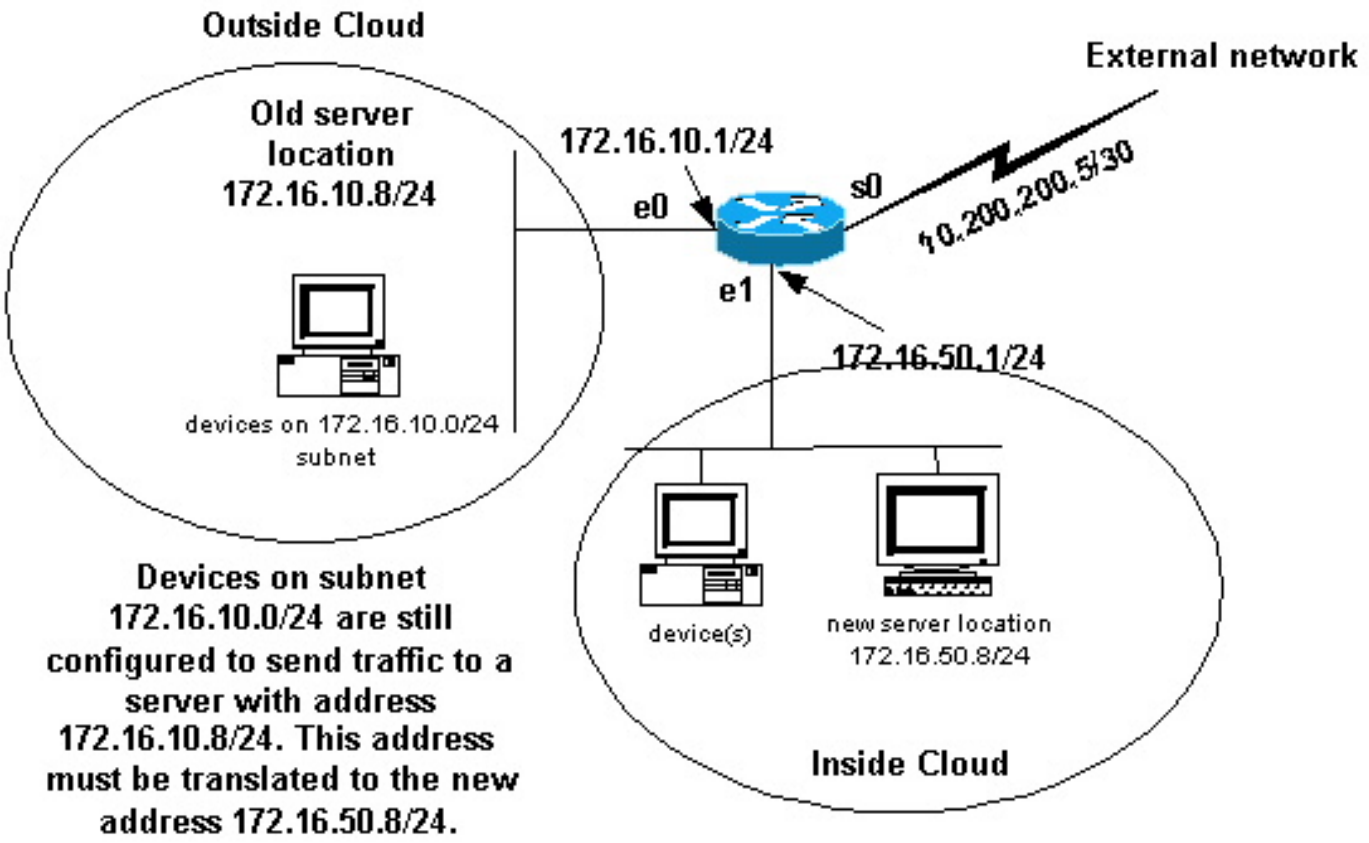
注：スタティックNATコマンドの設定は、内部インターフェイスで受信された、送信元アドレスが172.16.10.8:8080であるパケットがすべて172.16.10.8:80に変換されることを示しています。これはまた、内部インターフェイスで受信された、宛先アドレスが 172.16.10.8:80 であるパケットがすべて 172.16.10.8:8080 の宛先に変換されることも意味します。

最後のステップは、NATが意図したとおりに動作す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   ---                ---
```

4.ネットワークの移行にNATを使用する

NATは、ネットワーク上のデバイスのアドレスを変更する必要がある場合や、あるデバイスを別のデバイスに置き換える場合に便利です。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ネットワークの移行

前の図に示すようにNATインターフェイスを定義した後で、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て、新しいサーバアドレスに送信すること」と決定できます。新しいサーバは別のLAN上にあり、このLAN上のデバイス、またはこのLAN経由で到達可能なデバイス（ネットワークの内部側にあるデバイス）は、可能であれば新しいサーバIPアドレスを使用するように設定する必要があることに注意してください。

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 10.200.200.5 255.255.255.252

!--- 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.
```

注：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、宛先アドレスが172.16.50.8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することを確認することです。

5.オーバーラップするネットワークにNATを使用する

重複するネットワークは、インターネット内の他のデバイスによってすでに使用されている内部デバイスにIPアドレスを割り当てたときに発生します。これらのネットワークは、ネットワーク内でRFC 1918の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発生します。これら2つのネットワークは、すべてのデバイスが再び装備されていなくても、通信する必要があります。

1対1マッピングと多対多マッピングの違い

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。例：

<#root>

```
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、詳細設定で次の手順を実行します。

1. アドレスのプールを作成します。

```
<#root>

Router(config)#

ip nat pool MYPOOLEXAMPLE 10.41.10.1 10.41.10.41 netmask 255.255.255.0
```

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

```
<#root>

Router(config)#

access-list 100 permit ip 10.3.2.0 0.0.0.255 any
```

3. NAT対象の内部ネットワーク10.3.2.0 0.0.0.255を選択するアクセスリスト100をプールMYPOOLEXAMPLEに関連付け、アドレスをオーバーロードします。

```
<#root>

Router(config)#

ip nat inside source list 100 pool MYPOOLEXAMPLE overload
```

NATの動作の確認

NATを設定したら、期待どおりに動作することを確認します。これには、ネットワークアナライザ、showコマンド、またはdebugコマンドを使用する方法があります。NATの動作確認例についての詳細は、『NATの動作の確認と基本的なNAT』を参照してください。

結論

このドキュメントの例では、NATの設定と導入に役立つクイックスタート手順を示します。

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。

1. 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。
2. NATを使用して何を実現したいですか。
3. 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。
4. 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 insidecommandが使用されています。ip nat outsidecommandコマンドを使用して同じ目的を達成することもできますが、NATの動作の順序に注意してください。ip nat outside decommandsを使用する設定例については、『IP NAT Outside Source Listコマンドを使用する設定例』を参照してください。

前の例では、これらのアクションを提供:

コマンド	アクション
ip nat inside source	• 内部から外部へ移動する IP パケットの発信元を変換します。 • 外部から内部へ移動する IP パケットの宛先を変換します。
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。 • 内部から外部へ移動する IP パケットの宛先を変換します。

関連情報

- NAT：ローカルおよびグローバルの定義を参照。
- 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
- IP アドレッシング サービス
- 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

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。