スタティック NAT とダイナミック NAT の同時設定

内容

概要

状況によっては、Cisco ルータでスタティックおよびダイナミックのネットワーク アドレス変換（NAT）コマンドを設定することが必要になります。このドキュメントでは、これを実行する方法について説明し、サンプルのシナリオを示します。

前提条件

要件

NAT の基本的な概念と動作について理解していれば役立ちます。

- NAT の機能
- NATの処理順序

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 3600 シリーズ ルータ
- Cisco IOS® Software リリース 12.3（3）

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、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

表記法

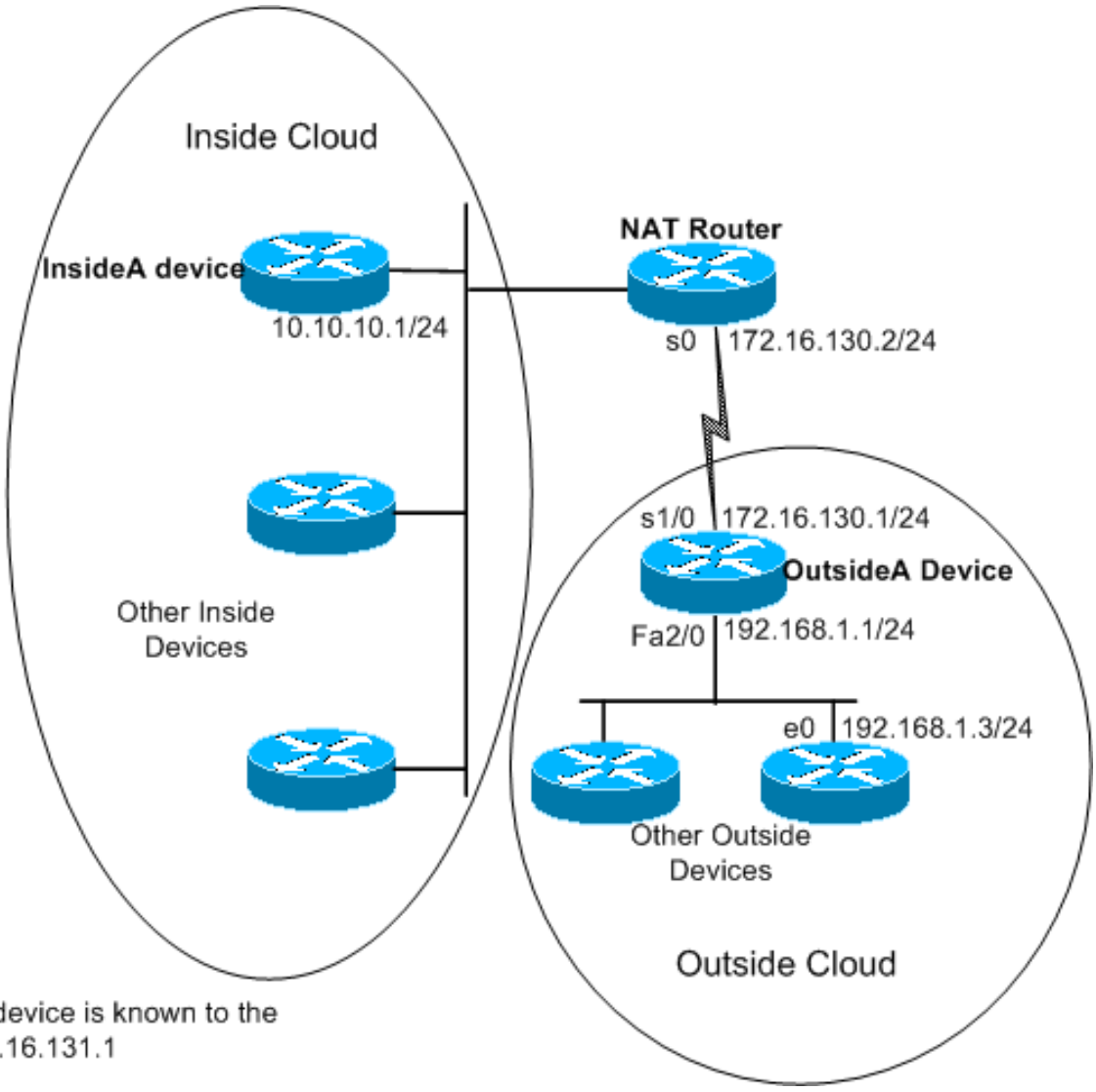
ドキュメント表記の詳細は、「シスコ テクニカル ティップスの表記法」を参照してください。

NAT の設定

ダイナミック NAT では、変換を必要とするトラフィックをルータが受信するまでは NAT 変換テーブルにトランスレーションが存在しません。ダイナミック トランスレーションにはタイムアウト時間があり、この時間を経過すると変換テーブルからトランスレーションが削除されます。

スタティック NAT では、スタティック NAT コマンドを設定したときからトランスレーションが NAT 変換テーブルに存在します。このトランスレーションは、スタティック NAT コマンドを削除するまで変換テーブルに存在し続けます。

例として、次のネットワーク ダイアグラムを取り上げます。



Using NAT, InsideA device is known to the outside cloud as 172.16.131.1

上記の NAT ルータでは、次のコマンドが設定されています。

NAT ルータ
version 12.3 ip nat pool test 172.16.131.2 172.16.131.10 netmask 255.255.255.0 *!--- Refer to* **ip nat pool** for more details on the command.

```
.

ip nat inside source list 7 pool test

!--- Refer to ip nat inside source  for more details on
the command.


ip nat inside source static 10.10.10.1 172.16.131.1

 interface e 0

 ip address 10.10.10.254 255.255.255.0

 ip nat inside

 interface s 0

 ip address 172.16.130.2 255.255.255.0

 ip nat outside

ip route 192.168.1.0 255.255.255.0 172.16.130.1

 access-list 7 permit 10.10.10.0 0.0.0.255
```

OutsideA というデバイスの設定は次のとおりです。

OutsideA ルータ

```
version 12.3
hostname outsideA

!
!
!
interface Serial1/0

ip address 172.16.130.1 255.255.255.0

serial restart-delay 0

clockrate 64000

!

interface FastEthernet2/0

ip address 192.168.1.1 255.255.255.0

speed auto

half-duplex

ip route 172.16.131.0 255.255.255.0 172.16.130.2
```

InsideA というデバイスの設定は次のとおりです。

InsideA ルータ

```
version 12.3

!
interface Ethernet1/0
 ip address 10.10.10.1 255.255.255.0
 half-duplex
!
ip route 0.0.0.0 0.0.0.0 10.10.10.254
!
!
```

show ip nat translations コマンドを使用すると、変換テーブルの内容が次のように表示されます。

```
NATrouter#show ip nat translations
Pro Inside global    Inside local    Outside local    Outside global
--- 172.16.131.1     10.10.10.1      ---              ---
```

変換テーブルにはスタティック トランスレーションのみがリストされている点に注意してください。このエントリは、内部グローバル アドレスを内部ローカル アドレスに戻します。これは、外部クラウドのデバイスがグローバル アドレス 172.16.131.1 宛てに送信したパケットが、ローカル アドレスが 10.10.10.1 である内部クラウドのデバイスに到達できることを意味します。

同じことが次のように表示されます。

```
outsideA#ping 172.16.131.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.131.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/32/32 ms



NATrouter#debug ip nat

18:12:06: NAT*: s=172.16.130.1, d=172.16.131.1->10.10.10.1 [1005]
18:12:06: NAT: s=10.10.10.1->172.16.131.1, d=172.16.130.1 [1005]
18:12:06: NAT*: s=172.16.130.1, d=172.16.131.1->10.10.10.1 [1006]
18:12:06: NAT*: s=10.10.10.1->172.16.131.1, d=172.16.130.1 [1006]
18:12:06: NAT*: s=172.16.130.1, d=172.16.131.1->10.10.10.1 [1007]
18:12:06: NAT*: s=10.10.10.1->172.16.131.1, d=172.16.130.1 [1007]
18:12:06: NAT*: s=172.16.130.1, d=172.16.131.1->10.10.10.1 [1008]
18:12:06: NAT*: s=10.10.10.1->172.16.131.1, d=172.16.130.1 [1008]
18:12:06: NAT*: s=172.16.130.1, d=172.16.131.1->10.10.10.1 [1009]
18:12:06: NAT*: s=10.10.10.1->172.16.131.1, d=172.16.130.1 [1009]
```

access-list 7 によって許可された送信元アドレスのパケットが、ルータの内部インターフェイスによって受信されない限り、それ以外のトランスレーションは変換テーブルに生成も入力もされません。

しかし、ダイナミック トランスレーションがまだ 1 つも入力されていないため、外部デバイスは、たとえパケットをグローバル アドレス（172.16.131.2 ~ 172.16.131.10）に送信しても、どの内部デバイスにも到達できません。 これらのグローバル アドレスの 1 つに宛てたパケットをルータが受信すると、ルータは変換テーブルから既存のトランスレーションを探します。既存のトランスレーションがない場合は、ルータはパケットのルーティングを試みます（このケースでは、シリアル インターフェイスに戻すことを意味します）。この NAT の動作については、「ip nat outside source list コマンドを使用した設定例」と「Sample Configuration Using the ip nat

outside source static Command」の 2 つのテック ノートを参照してください。

上記のトポロジでは、ネットワークの内部デバイスと外部デバイスの間の通信が内部デバイスによってのみ開始される場合は、ダイナミック トランスレーションがうまく機能します。しかし、外部から送信されたパケットを受信する必要がある電子メール サーバを、内部ネットワークに追加するとどうなるでしょうか。この場合は、外部の電子メール サーバが内部の電子メール サーバとの通信を開始できるように、スタティック NAT エントリを設定する必要があります。上記の例で、電子メール サーバが 10.10.10.1 のローカル アドレスを持つデバイスであれば、すでにスタティック トランスレーションは存在します。

しかし、多くの場合は予備のグローバル アドレスが少ないため、NAT 用に単一のデバイスを静的に設定する必要がある場合は、次のような設定を使用します。

NAT ルータ

```
ip nat inside source list 7 interface serial 0 overload


ip nat inside source static tcp 10.10.10.1 25
172.16.130.2 25
!--- Refer to ip nat inside source  for more details on
the command.


 interface e 0

 ip address 10.10.10.254 255.255.255.0

 ip nat inside
!--- For more details the ip nat inside|outside command,
!--- please refer to ip nat inside .


 interface s 0

ip address 172.16.130.2 255.255.255.0

ip nat outside

 access-list 7 permit 10.10.10.0 0.0.0.255

 ip route 0.0.0.0 0.0.0.0 172.16.130.1
```

上記の例では、NAT が serial 0 の IP アドレスをオーバーロードするように設定されています。これは、複数の内部ローカルアドレスを同じグローバルアドレス (この場合はSerial 0に割り当てられたアドレス) に動的に変換できることを意味します。また、TCPポート25(SMTP)を持つローカルアドレス10.10.10.1からのパケットをSerial 0のIPアドレスTCPポート225 SMTP (TCPポート25) パケットをグローバルアドレス172.16.131.254に送信します。

注：ダイナミックNATとスタティックNATの両方に同じグローバルアドレスを使用することは可能ですが、可能な限り異なるグローバルアドレスを使用することをお勧めします。

NAT 変換テーブルには次のエントリがあります。

```
NATRouter#show ip nat translations
```

```
   Pro Inside global    Inside local   Outside local Outside global

   tcp 172.16.130.2:25  10.10.10.1:25      ---           ---
```

debug ip nat の出力には、OutsideA デバイスが InsideA デバイスにアクセスするときの NAT 変換が次のように表示されます。

```
04:21:16: NAT: s=192.168.1.3, d=172.16.130.2->10.10.10.1    [9919]

   04:21:16: NAT: s=10.10.10.1->172.16.130.2, d=192.168.1.3 [0]

   04:21:16: NAT*: s=192.168.1.3, d=172.16.130.2->10.10.10.1 [9922]

   04:21:16: NAT*: s=192.168.1.3, d=172.16.130.2->10.10.10.1 [9923]

   04:21:16: NAT*: s=10.10.10.1->172.16.130.2, d=192.168.1.3 [1]

   04:21:16: NAT*: s=10.10.10.1->172.16.130.2, d=192.168.1.3 [2]

   04:21:16: NAT*: s=10.10.10.1->172.16.130.2, d=192.168.1.3 [3]

   04:21:16: NAT*: s=192.168.1.3, d=172.16.130.2->10.10.10.1 [9927]

   04:21:16: NAT*: s=10.10.10.1->172.16.130.2, d=192.168.1.3 [4]

   04:21:16: NAT: s=10.10.10.1->172.16.130.2, d=192.168.1.3 [5]

   04:21:16: NAT*: s=192.168.1.3, d=172.16.130.2->10.10.10.1 [9931]

   04:21:17: NAT*: s=192.168.1.3, d=172.16.130.2->10.10.10.1 [9934]

   04:21:17: NAT: s=192.168.1.3, d=172.16.130.2->10.10.10.1 [9935]

   04:21:17: NAT*: s=10.10.10.1->172.16.130.2, d=192.168.1.3 [6]
```

要約すると、ダイナミック NAT では変換テーブルに NAT トランスレーションを作成するには、パケットが NAT ルータでスイッチングされる必要があります。ip nat inside コマンドを使用する場合は、これらのパケットは内部から送信される必要があります。ip nat outside コマンドを使用する場合は、これらのパケットは外部から送信される必要があります。

スタティック NAT ではパケットがルータでスイッチングされる必要はなく、トランスレーションは変換テーブルに静的(スタティック)に入力されます。

関連情報

- NAT に関する FAQ
- テクニカルサポート - Cisco Systems