オーバーラッピング ネットワークで NAT を使用する場合

内容

概要

このドキュメントでは、重複するネットワークに対してネットワーク アドレス変換（NAT）を使用する方法を説明します。すでに合法的に所有されインターネットまたは外部ネットワーク上のデバイスに割り当てられている IP アドレスを、独自のネットワーク上の別のデバイスに割り当てると、ネットワークの重複が発生します。また、社内ネットワークで RFC 1918 の IP アドレスを使用している 2 つの会社が合併したときにも発生します。 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。

前提条件

要件

IP アドレッシング、IP ルーティング、およびドメイン ネーム システム（DNS）の基本的な知識は、このドキュメントの内容を理解するうえで役立ちます。

使用するコンポーネント

NATのサポートは、Cisco IOS®ソフトウェアバージョン11.2から開始されました。プラットフォームサポートの詳細については、『NATに関するFAQ』を参照してください。

表記法

ドキュメントの表記法の詳細は、「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。

設定

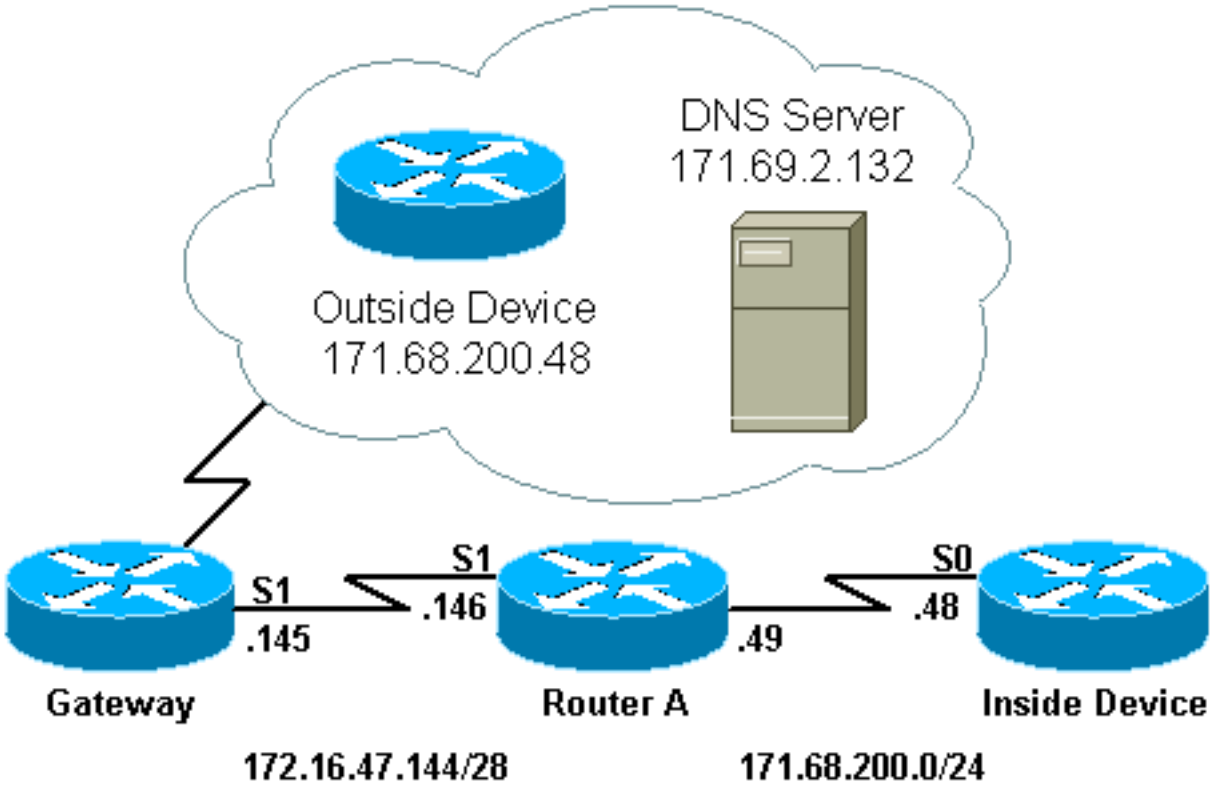
このセクションでは、このドキュメントで説明する機能を設定するために必要な情報を提供しています。

注：この文書で使用されているコマンドの詳細を調べるには、「Command Lookup ツール」を使用してください（登録ユーザのみ）。

ネットワーク図

このドキュメントでは次の図に示すネットワーク構成を使用しています。

内部デバイスは、通信しようとしている外部デバイスと IP アドレスが同じであることに注意してください。



設定

ルータ A では、内部デバイスをプール「test-loop」のアドレスに変換し、外部デバイスをプール「test-dns」のアドレスに変換するように、NAT を設定します。 この設定が重複でどのように役立つかの説明を、次の設定テーブルに示します。

ルータ A
`` ! version 11.2 no service udp-small-servers no service tcp-small-servers ! hostname Router-A ! ```

```
!
ip domain-name cisco.com
ip name-server 171.69.2.132
!
interface Loopback0
 ip address 1.1.1.1 255.0.0.0
!
interface Ethernet0
 ip address 135.135.1.2 255.255.255.0
 shutdown
!
interface Serial0
 ip address 171.68.200.49 255.255.255.0
 ip nat inside
 no ip mroute-cache
 no ip route-cache
 no fair-queue
!
interface Serial1
 ip address 172.16.47.146 255.255.255.240
 ip nat outside
 no ip mroute-cache
 no ip route-cache
!
ip nat pool test-loop 172.16.47.161 172.16.47.165
prefix-length 28
ip nat pool test-dns 172.16.47.177 172.16.47.180 prefix-
length 28
ip nat inside source list 7 pool test-loop
ip nat outside source list 7 pool test-dns
ip classless
ip route 0.0.0.0 0.0.0.0 172.16.47.145
access-list 7 permit 171.68.200.0 0.0.0.255
!
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 login
!
end
```

上記の設定が内部デバイスと外部デバイスの通信時に役立つためには、外部デバイスのドメイン ネームを使用する必要があります。

外部デバイスの IP アドレスは内部デバイスに割り当てられているアドレスと同じであるため、内部デバイスは外部デバイスの IP アドレスを使用できません。 したがって、内部デバイスが外部デバイスのドメイン ネームの DNS のクエリを送信します。内部デバイスの IP アドレスがこのクエリの送信元となりますが、そのアドレスが「test-loop」プールからのアドレスに変換されます。これは、**ip nat inside source list コマンドが設定されているためです。**

DNS サーバはパケットのペイロードで、外部デバイスのドメイン ネームに関連付けられた IP アドレスを使用して、プール「test-loop」からのアドレスに応答します。一方、**ip nat outside source list コマンドにより、応答パケットの宛先アドレスは内部デバイスのアドレスに再度変換され、応答パケットのペイロードのアドレスはプール「test-dns」のアドレスに変換されます。**したがって、内部デバイスは、外部デバイスの IP アドレスが「test-dns」プールからのアドレスの 1 つであることを学習し、外部デバイスと通信する場合にこのアドレスを使用します。NAT を実行しているルータは、この時点で変換を処理します。

このプロセスは、トラブルシューティングのセクションで詳細を確認できます。重複するアドレスを使用するデバイスは、DNS を使用せずに相互に通信できますが、その場合、スタティック NAT を設定する必要があります。この設定方法の例を示します。

ルータ A

```
!
version 11.2
no service udp-small-servers
no service tcp-small-servers
!
hostname Router-A
!
!

ip domain-name cisco.com
ip name-server 171.69.2.132
!
interface Loopback0
 ip address 1.1.1.1 255.0.0.0
!
interface Ethernet0
 ip address 135.135.1.2 255.255.255.0
 shutdown
!
interface Serial0
 ip address 171.68.200.49 255.255.255.0
 ip nat inside
 no ip mroute-cache
 no ip route-cache
 no fair-queue
!
interface Serial1
 ip address 172.16.47.146 255.255.255.240
 ip nat outside
 no ip mroute-cache
 no ip route-cache
!
ip nat pool test-loop 172.16.47.161 172.16.47.165
prefix-length 28
ip nat inside source list 7 pool test-loop
ip nat outside source static 171.68.200.48 172.16.47.177
ip classless
ip route 0.0.0.0 0.0.0.0 172.16.47.145
ip route 172.16.47.160 255.255.255.240 Serial0
!--- This line is necessary to make NAT work for return
traffic. !--- The router needs to have a route for the
pool to the inside !--- NAT interface so it knows that a
translation is needed. access-list 7 permit 171.68.200.0
0.0.0.255
!
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 login
!
end
```

上記の設定では、内部デバイスが外部デバイスと通信する場合に、IP アドレス 172.16.47.177 を

使用でき、不要な場合は DNS を使用できます。上で示すように、内部デバイスのアドレスの変換は動的に実行されるため、変換が作成される前にルータが内部デバイスからパケットを取得する必要があることを意味します。したがって、内部デバイスと外部デバイスが通信するためには、内部デバイスがすべての接続を開始する必要があります。外部デバイスが内部デバイスへの通信を開始する必要があった場合は、内部デバイスのアドレスも静的に設定する必要があります。

確認

現在、この設定に使用できる確認手順はありません。

トラブルシュート

ここでは、設定のトラブルシューティングに使用できる情報を示します。

前述のように、内部デバイスが DNS を使用して外部デバイスと通信した方法は、次のトラブルシューティング手順を使用して確認できます。

現在、show ip nat translations コマンドで表示できる変換テーブルに変換アドレスはありません。次の例では、代わりに **debug ip packet および debug ip nat コマンドを使用しています。**

注：デバッグ コマンドは、大量の出力を生成します。IP ネットワークのトラフィックが少なく、システムのその他の処理が悪影響を受けない場合にだけ使用してください。

```
Router-A# show ip nat translations
Router-A# show debug
Generic IP:
  IP packet debugging is on (detailed)
  IP NAT debugging is on
```

内部デバイスが DNS クエリーを NAT ドメイン外にある DNS サーバに送信した場合、DNS クエリーの送信元アドレス (内部デバイスのアドレス) は、ip nat inside コマンドによって変換されます。これは次のデバッグ出力で確認できます。

```
NAT: s=171.68.200.48->172.16.47.161, d=171.69.2.132 [0]
IP: s=172.16.47.161 (Serial0), d=171.69.2.132 (Serial1), g=172.16.47.145, len 66, forward
    UDP src=6988, dst=53
```

DNS サーバが DNS 応答を送信する場合、DNS 応答のペイロードは、ip nat outside コマンドによって変換されます。

注：NATは、応答パケットのIPヘッダーで変換が発生しない限り、DNS応答のペイロードを参照しません。上のルータ構成の ip nat outside source list 7 pool コマンドを参照してください。

次のデバッグ出力の最初のNATメッセージは、ルータがDNS応答を認識し、ペイロード内のIPアドレスを172.16.47.177に変換することを示しています。2番目のNATメッセージは、ルータがDNS応答の宛先を変換して、初期DNSクエリを実行する。ヘッダーの宛先の部分 (内部グローバル アドレス) は、内部ローカル アドレスに変換されます。

DNS 応答のペイロードが変換されます。

```
NAT: DNS resource record 171.68.200.48 -> 172.16.47.177
```
DNS 応答の IP ヘッダーの宛先部分が変換されます。

```
NAT: s=171.69.2.132, d=172.16.47.161->171.68.200.48 [65371]
IP: s=171.69.2.132 (Serial1), d=171.68.200.48 (Serial0), g=171.68.200.48, len 315, forward
    UDP src=53, dst=6988
```
ここで、別の DNS のクエリーおよび応答を見てみます。

```
NAT: s=171.68.200.48->172.16.47.161, d=171.69.2.132 [0]
IP: s=172.16.47.161 (Serial0), d=171.69.2.132 (Serial1), g=172.16.47.145, len 66, forward
    UDP src=7419, dst=53
NAT: DNS resource record 171.68.200.48 -> 172.16.47.177
NAT: s=171.69.2.132, d=172.16.47.161->171.68.200.48 [65388]
IP: s=171.69.2.132 (Serial1), d=171.68.200.48 (Serial0), g=171.68.200.48, len 315, forward
    UDP src=53, dst=7419
```
DNS のペイロードが変換されたため、変換テーブルには、外部デバイスの外部ローカルおよびグローバル アドレスを示すエントリがあります。テーブル内のこれらのエントリを使用して、内部デバイスと外部デバイス間で交換された ICMP パケットのヘッダー全体を変換できます。次のデバッグ出力でこの交換を確認してください。

次の出力は、変換される送信元アドレス (内部デバイスのアドレス) を示しています。

```
NAT: s=171.68.200.48->172.16.47.161, d=172.16.47.177 [406]
```
ここで、宛先アドレス (外部デバイスの外部ローカル アドレス) が変換されます。

```
NAT: s=172.16.47.161, d=172.16.47.177->171.68.200.48 [406]
```
変換の後に、IP パケットは次のようになります。

```
IP: s=172.16.47.161 (Serial0), d=171.68.200.48 (Serial1), g=172.16.47.145, len 100, forward
    ICMP type=8, code=0
```
次の出力は、応答パケットで変換される送信元アドレス (外部デバイスのアドレス) を示しています。

```
NAT*: s=171.68.200.48->172.16.47.177, d=172.16.47.161 [16259]
```
次に、応答パケットの宛先アドレス (内部デバイスのグローバル アドレス) が変換されます。

```
NAT*: s=172.16.47.177, d=172.16.47.161->171.68.200.48 [16259]
```
変換の後に、応答パケットは次のようになります。

```
IP: s=172.16.47.177 (Serial1), d=171.68.200.48 (Serial0), g=171.68.200.48, len 100, forward
    ICMP type=0, code=0
```
内部デバイスと外部デバイス間で、パケットの交換が続きます。

```
NAT: s=171.68.200.48->172.16.47.161, d=172.16.47.177 [407]
NAT: s=172.16.47.161, d=172.16.47.177->171.68.200.48 [407]
IP: s=172.16.47.161 (Serial0), d=171.68.200.48 (Serial1), g=172.16.47.145, len 100, forward
    ICMP type=8, code=0
```

```
NAT*: s=171.68.200.48->172.16.47.177, d=172.16.47.161 [16262]
NAT*: s=172.16.47.177, d=172.16.47.161->171.68.200.48 [16262]
IP: s=172.16.47.177 (Serial1), d=171.68.200.48 (Serial0), g=171.68.200.48, len 100, forward
    ICMP type=0, code=0
NAT: s=171.68.200.48->172.16.47.161, d=172.16.47.177 [408]
NAT: s=172.16.47.161, d=172.16.47.177->171.68.200.48 [408]
IP: s=172.16.47.161 (Serial0), d=171.68.200.48 (Serial1), g=172.16.47.145, len 100, forward
    ICMP type=8, code=0
NAT*: s=171.68.200.48->172.16.47.177, d=172.16.47.161 [16267]
NAT*: s=172.16.47.177, d=172.16.47.161->171.68.200.48 [16267]
IP: s=172.16.47.177 (Serial1), d=171.68.200.48 (Serial0), g=171.68.200.48, len 100, forward
    ICMP type=0, code=0
NAT: s=171.68.200.48->172.16.47.161, d=172.16.47.177 [409]
NAT: s=172.16.47.161, d=172.16.47.177->171.68.200.48 [409]
IP: s=172.16.47.161 (Serial0), d=171.68.200.48 (Serial1), g=172.16.47.145, len 100, forward
    ICMP type=8, code=0
NAT*: s=171.68.200.48->172.16.47.177, d=172.16.47.161 [16273]
NAT*: s=172.16.47.177, d=172.16.47.161->171.68.200.48 [16273]
IP: s=172.16.47.177 (Serial1), d=171.68.200.48 (Serial0), g=171.68.200.48, len 100, forward
    ICMP type=0, code=0
NAT: s=171.68.200.48->172.16.47.161, d=172.16.47.177 [410]
NAT: s=172.16.47.161, d=172.16.47.177->171.68.200.48 [410]
IP: s=172.16.47.161 (Serial0), d=171.68.200.48 (Serial1), g=172.16.47.145, len 100, forward
    ICMP type=8, code=0
NAT*: s=171.68.200.48->172.16.47.177, d=172.16.47.161 [16277]
NAT*: s=172.16.47.177, d=172.16.47.161->171.68.200.48 [16277]
IP: s=172.16.47.177 (Serial1), d=171.68.200.48 (Serial0), g=171.68.200.48, len 100, forward
    ICMP type=0, code=0
```

外部デバイスと内部デバイス間でパケットの交換が終了した後で変換テーブルを表示すると、3 つのエントリがあります。最初のエントリは、内部デバイスが DNS クエリーを送信したときに作成されました。2 番目のエントリは、DNS 応答のペイロードの変換時に作成されました。3 番目のエントリは、内部デバイスと外部デバイス間での PING の交換時に作成されました。3 番目のエントリは、先頭の 2 つのエントリのサマリーで、より効率的な変換のために使用されます。

```
Router-A# show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
--- 172.16.47.161      171.68.200.48      ---                ---
--- ---                ---                172.16.47.177      171.68.200.48
--- 172.16.47.161      171.68.200.48      172.16.47.177      171.68.200.48
```

1 台のシスコ ルータでダイナミック NAT を実行することにより、2 つの重複ネットワーク間に接続を確立しようとする場合は、DNS を使用して、外部ローカル アドレスから外部グローバル アドレスへの変換を行う必要があります。DNS を使用しない場合は、スタティック NAT で接続を確立できますが、管理がより困難になります。

関連情報

- NAT に関するサポート ページ
- テクニカルサポート - Cisco Systems