NATの処理順序

目次

概要

このドキュメントでは、ネットワーク アドレス変換（NAT）を使用してトランザクションが処理される順序について説明しています。この処理順序は、パケットが Inside のネットワークから Outside ネットワークへ送信されるのか、それとも Outside のネットワークから Inside のネットワークへ送信されるのかによって異なります。

前提条件

要件

このドキュメントの読者は次の項目に関する知識が必要です。

- ネットワーク アドレス変換（NAT）。 NAT の詳細は、『NAT の動作の仕組み』を参照してください。

使用するコンポーネント

このドキュメントは、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

注: このドキュメントの情報は、ソフトウェア バージョン、Cisco IOS® ソフトウェア リリース 12.2(27)T に基づくものです。

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 の概要

次の表に示すとおり、グローバルからローカルへの NAT 変換、またはローカルからグローバルへの NAT 変換がいつ実行されるかはそれぞれのフローにおいて異なります。

内部から外部へ	外部から内部へ
• IPSec の場合は入力アクセス リストをチェック • 復号化：CET（シスコ暗号化テクノロジー）または IPSec • 入力アクセス リストをチェック • 入力レート制限をチェック • 入力アカウンティング • Web キャッシュにリダイレクト • ポリシー ルーティング • ルーティング • **Inside から Outside への NAT（ローカルからグローバルへの変換）** • クリプト（暗号化用のマップのチェックとマーク） • 出力アクセス リストをチェック • 検査（コンテキストベース アクセス制御（CBAC）） • TCP インターセプト • 暗号化 • キューイング	• IPSec の場合は入力アクセス リストをチェック • 復号化： CET または IPSec • 入力アクセス リストをチェック • 入力レート制限をチェック • 入力アカウンティング • Web キャッシュにリダイレクト • **外部から内部への NAT（グローバルからローカルへの変換）** • ポリシー ルーティング • ルーティング • クリプト（暗号化用のマップのチェックとマーク） • 出力アクセス リストをチェック • CBAC 検査 • TCP インターセプト • 暗号化 • キューイング

NAT の設定および出力

次の例は、動作の順序が NAT にどのような影響を与えるかを示しています。 このケースでは、NAT とルーティングだけを示しています。

上の例では、次の設定に示すように、Router-A は Inside のローカル アドレス 171.68.200.48 を 172.16.47.150 に変換するように設定されています。

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

```
!
enable password ww
!
ip nat inside source static 171.68.200.48 172.16.47.150
!--- This command creates a static NAT translation !--- between 171.68.200.48 and 172.16.47.150
ip domain-name cisco.com ip name-server 171.69.2.132 ! interface Ethernet0 no ip address
shutdown ! interface Serial0 ip address 172.16.47.161 255.255.255.240 ip nat inside
!--- Configures Serial0 as the NAT inside interface 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
!--- Configures Serial1 as the NAT outside interface no ip mroute-cache no ip route-cache ! no
ip classless ip route 0.0.0.0 0.0.0.0 172.16.47.145
!--- Configures a default route to 172.16.47.145 ip route 171.68.200.0 255.255.255.0
172.16.47.162 ! ! line con 0 exec-timeout 0 0 line aux 0 line vty 0 4 password ww login ! end
```

変換テーブルには、意図した変換が存在することが示されます。

```
Router-A#show ip nat translation
Pro Inside global      Inside local       Outside local      Outside global
--- 172.16.47.150      171.68.200.48      ---                ---
```

次の出力は、debug ip packet detail および debug ip nat がイネーブルの状態の Router-A から得られたもので、デバイス 171.68.200.48 から 172.16.47.142 宛てに PING が発行されています。

注: debug コマンドからは、大量の出力が生成されます。 システムの他の動作に悪影響が及ばないように、IP ネットワーク上のトラフィック負荷が低い場合にだけ使用してください。 **debug** コマンドを発行する前に、『debug コマンドの重要な情報』を参照してください。

```
Router-A#show ip nat translation
Pro Inside global      Inside local       Outside local      Outside global
--- 172.16.47.150      171.68.200.48      ---                ---
```

上の出力に NAT のデバッグ メッセージがないため、既存のスタティック トランスレーションが使用されていないことと、ルータが宛先アドレス (172.16.47.142) へのルートを自身のルーティング テーブルに持っていないことがわかります。 パケットがルーティングできないため、ICMP 到達不能メッセージが生成され、内部デバイスに送信されます。

しかし、Router-A には、172.16.47.145 のデフォルト ルートがあります。なぜ、ルートがルーティング不能と認識されるのでしょうか。

ルータ A では **no ip classless** が設定されています。これは、パケットの宛先が「メジャー」ネットワーク アドレスの場合 (この場合は 172.16.0.0)、そのサブネットがルーティング テーブルに存在すると、ルータはデフォルト ルートに依存しないことを意味しています。 つまり、**no ip classless** コマンドを発行すると、ビットが最も長く一致するルートを検索するルータの機能をオフにしてしまいます。 この動作を変更するには、Router-A 上で ip classless を設定する必要があります。 ip classless コマンドは、Cisco IOS ソフトウェア リリース 11.3 移行の Cisco ルータでは、デフォルトでイネーブルになっています。

```
Router-A#configure terminal
Enter configuration commands, one per line.  End with CTRL/Z.
Router-A(config)#ip classless
Router-A(config)#end

Router-A#show ip nat translation
%SYS-5-CONFIG_I: Configured from console by console nat tr
Pro Inside global      Inside local       Outside local      Outside global
--- 172.16.47.150      171.68.200.48      ---                ---
```

上と同じ PING テストを繰り返すと、パケットが変換されて、PING が成功することがわかりま

す。

```
Ping Response on device 171.68.200.48

D:\>ping 172.16.47.142
Pinging 172.16.47.142 with 32 bytes of data:

Reply from 172.16.47.142: bytes=32 time=10ms TTL=255
Reply from 172.16.47.142: bytes=32 time<10ms TTL=255
Reply from 172.16.47.142: bytes=32 time<10ms TTL=255
Reply from 172.16.47.142: bytes=32 time<10ms TTL=255

Ping statistics for 172.16.47.142:
    Packets: Sent = 4, Received = 4, Lost = 0 (0%)
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum =  10ms, Average =  2ms

Debug messages on Router A indicating that the packets generated by device
171.68.200.48 are getting translated by NAT.

Router-A#
*Mar 28 03:34:28: IP: tableid=0, s=171.68.200.48 (Serial0), d=172.16.47.142
(Serial1), routed via RIB
*Mar 28 03:34:28: NAT: s=171.68.200.48->172.16.47.150, d=172.16.47.142 [160]
*Mar 28 03:34:28: IP: s=172.16.47.150 (Serial0), d=172.16.47.142 (Serial1),
 g=172.16.47.145, len 100, forward
*Mar 28 03:34:28: ICMP type=8, code=0
*Mar 28 03:34:28: NAT*: s=172.16.47.142, d=172.16.47.150->171.68.200.48 [160]
*Mar 28 03:34:28: IP: tableid=0, s=172.16.47.142 (Serial1), d=171.68.200.48
(Serial0), routed via RIB
*Mar 28 03:34:28: IP: s=172.16.47.142 (Serial1), d=171.68.200.48 (Serial0),
g=172.16.47.162, len 100, forward
*Mar 28 03:34:28: ICMP type=0, code=0
*Mar 28 03:34:28: NAT*: s=171.68.200.48->172.16.47.150, d=172.16.47.142 [161]
*Mar 28 03:34:28: NAT*: s=172.16.47.142, d=172.16.47.150->171.68.200.48 [161]
*Mar 28 03:34:28: IP: tableid=0, s=172.16.47.142 (Serial1), d=171.68.200.48
(Serial0), routed via RIB
*Mar 28 03:34:28: IP: s=172.16.47.142 (Serial1), d=171.68.200.48 (Serial0),
g=172.16.47.162, len 100, forward
*Mar 28 03:34:28: ICMP type=0, code=0
*Mar 28 03:34:28: NAT*: s=171.68.200.48->172.16.47.150, d=172.16.47.142 [162]
*Mar 28 03:34:28: NAT*: s=172.16.47.142, d=172.16.47.150->171.68.200.48 [162]
*Mar 28 03:34:28: IP: tableid=0, s=172.16.47.142 (Serial1), d=171.68.200.48
(Serial0), routed via RIB
*Mar 28 03:34:28: IP: s=172.16.47.142 (Serial1), d=171.68.200.48 (Serial0),
g=172.16.47.162, len 100, forward
*Mar 28 03:34:28: ICMP type=0, code=0
*Mar 28 03:34:28: NAT*: s=171.68.200.48->172.16.47.150, d=172.16.47.142 [163]
*Mar 28 03:34:28: NAT*: s=172.16.47.142, d=172.16.47.150->171.68.200.48 [163]
*Mar 28 03:34:28: IP: tableid=0, s=172.16.47.142 (Serial1), d=171.68.200.48
(Serial0), routed via RIB
*Mar 28 03:34:28: IP: s=172.16.47.142 (Serial1), d=171.68.200.48 (Serial0),
g=172.16.47.162, len 100, forward
*Mar 28 03:34:28: ICMP type=0, code=0
*Mar 28 03:34:28: NAT*: s=171.68.200.48->172.16.47.150, d=172.16.47.142 [164]
*Mar 28 03:34:28: NAT*: s=172.16.47.142, d=172.16.47.150->171.68.200.48 [164]
*Mar 28 03:34:28: IP: tableid=0, s=172.16.47.142 (Serial1), d=171.68.200.48
(Serial0), routed via RIB
*Mar 28 03:34:28: IP: s=172.16.47.142 (Serial1), d=171.68.200.48 (Serial0),
g=172.16.47.162, len 100, forward
```

```
*Mar 28 03:34:28: ICMP type=0, code=0

Router-A#undebug all
All possible debugging has been turned off
```

上の例は、パケットが Inside から Outside に通過する場合、NAT ルータは Outside アドレスへのルートを自身のルーティング テーブルでチェックし、それからパケットの変換を続けることを示しています。 したがって、NAT ルータに Outside ネットワークへの有効なルートがあることが重要です。 宛先ネットワークへのルートは、ルータの設定の中の NAT outside として定義されているインターフェイスを通じて判明します。

戻りパケットは経路選択される前に変換される点に注意してください。 したがって、NAT ルータは、Inside のローカル アドレスへの有効なルートも自身のルーティング テーブルに持っている必要があります。

関連情報

- ネットワーク アドレス変換の設定： スタートアップ ガイド
- NAT の動作確認と NAT の基本的なトラブルシューティング
- NAT： ローカルおよびグローバルの定義
- マルチキャスト NAT が Cisco ルータで機能するしくみ
- NAT に関するサポートページ
- テクニカル サポートとドキュメント – Cisco Systems