NATの処理順序について

内容

概要

このドキュメントでは、NATで処理される順序トランザクションが、パケットがネットワークの内部または外部を移動する方向に基づいていることを説明します。

前提条件

要件

次の項目に関する専門知識があることが推奨されます。

- ネットワーク アドレス変換（NAT）。NAT の詳細については、「NAT の動作」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、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) に基づくものです。

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。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

ドキュメント表記の詳細については、『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。

背景説明

このドキュメントでは、Network Address Translation（NAT；ネットワークアドレス変換）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ます。この順序は、パケットが内部ネットワークから外部ネットワークへ送信されるのか、それとも外部ネットワークから内部ネットワークへ送信されるのかに基づきます。

NAT の概要

この表では、NAT のグローバルからローカルへのアドレス変換と、ローカルからグローバルへのアドレス変換は、フローごとに異なっています。

内部から外部へ

- IPSec なら入力アクセス リストを確認
- 復号：CET（Cisco Encryption Technology）または IPSec
- 入力アクセス リストを確認
- 入力レート制限を確認
- アカウンティングを入力
- Web キャッシュへリダイレクト
- ポリシー ルーティング（Policy routing）#ぽりしーるーてぃんぐ#
- ルーティング
- **内部から外部への NAT（ローカルからグローバルへの変換）**
- クリプト（マップの確認と暗号化のマークを設定）
- 出力アクセスリストを確認
- 検証（コンテキストベースのアクセス コントロール（CBAC））
- TCP 代行受信
- 暗号化
- キュー

外部から内部へ

- IPSec なら入力アクセス リストを確認
- 復号 - CET または IPSec の場合
- 入力アクセス リストを確認
- 入力レート制限を確認
- アカウンティングを入力
- Web キャッシュへリダイレクト
- **内部から外部への NAT（グローバルからロー**
  への変換）
- ポリシー ルーティング（Policy routing）#ほ
  ーるーてぃんぐ#
- ルーティング
- クリプト（マップの確認と暗号化のマークを
  ）
- 出力アクセスリストを確認
- CBAC 検証
- TCP 代行受信
- 暗号化
- キュー

NAT の設定と出力

この例では、処理の順番が NAT に影響することを説明します。この場合では、NAT とルーティングのみを表示します。

前の例では、ルータ A は内部ローカルアドレス 172.31.200.48 を 172.16.47.150 に変換するよう設定されています。

```
!
version 11.2
no service udp-small-servers
no service tcp-small-servers
!
hostname Router-A
!
enable password ww
!
ip nat inside source static 172.31.200.48 172.16.47.150
```

```
!--- This command creates a static NAT translation
!--- between 172.31.200.48 and 172.16.47.150 ip domain-name cisco.com ip name-server
172.31.2.132 ! 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 172.31.200.0 255.255.255.0
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ています。

```
Router-A#show ip nat translation
Pro Inside global      Inside local       Outside local      Outside global
--- 172.16.47.150      172.31.200.48      ---                ---
```

この出力は debug ip packet detail と debug ip nat を有効にしたルータ A から取得したものです。デバイス 172.31.200.48 からデバイス 172.16.47.142 に向けて ping を発行しました。

> **注：デバッグ コマンドではかなりの量の出力が生成されます。**IP ネットワーク上のトラフィックが少なく、システム上の他のアクティビティに悪影響がない場合にだけ、このコマンドを使用してください。**debug コマンドを使用する前に、『debug コマンドの重要な情報』を参照してください。**

```
IP: s=172.31.200.48 (Serial0), d=172.16.47.142, len 100, unroutable
    ICMP type=8, code=0
IP: s=172.16.47.161 (local), d=172.31.200.48 (Serial0), len 56, sending
    ICMP type=3, code=1
IP: s=172.31.200.48 (Serial0), d=172.16.47.142, len 100, unroutable
    ICMP type=8, code=0
IP: s=172.31.200.48 (Serial0), d=172.16.47.142, len 100, unroutable
    ICMP type=8, code=0
IP: s=172.16.47.161 (local), d=172.31.200.48 (Serial0), len 56, sending
    ICMP type=3, code=1
IP: s=172.31.200.48 (Serial0), d=172.16.47.142, len 100, unroutable
    ICMP type=8, code=0
IP: s=172.31.200.48 (Serial0), d=172.16.47.142, len 100, unroutable
    ICMP type=8, code=0
IP: s=172.16.47.161 (local), d=172.31.200.48 (Serial0), len 56, sending
    ICMP type=3, code=1
```

上記の出力にはNATデバッグメッセージが含まれていないため、現在のスタティック変換は使用されず、ルータのルーティングテーブルには宛先アドレス(172.16.47.142)へのルートが含まれていません。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、ルータ A には 172.16.47.145 のデフォルト ルートがあります。なぜルーティング不能と認識されるのでしょうか。

ルータ A には no ip classless が設定されています。これにより、ルーティング テーブルにサブネットの指定がある「上位」のネットワークアドレス (この場合、172.16.0.0) を宛先とするパケットについてはデフォルトルートは適用されません。言い換えると、no ip classless コマンドを発行することでビット列が最も長く合致するルートを探す機能がオフになります。この動作を変

更するには、ルータ A に ip classless を設定します。ip classless コマンドは Cisco IOS Software Releases 11.3 以降を実行している Cisco ルータではデフォルトで有効になっています。

```
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      172.31.200.48      ---                ---
```

前述と同様の ping を実行すると、今度はパケットのアドレスが変換され、ping が成功することを確認できます。

```
Ping Response on device 172.31.200.48

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
172.31.200.48 are getting translated by NAT.

Router-A#
*Mar 28 03:34:28: IP: tableid=0, s=172.31.200.48 (Serial0), d=172.16.47.142
(Serial1), routed via RIB
*Mar 28 03:34:28: NAT: s=172.31.200.48->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->172.31.200.48 [160]
*Mar 28 03:34:28: IP: tableid=0, s=172.16.47.142 (Serial1), d=172.31.200.48
(Serial0), routed via RIB
*Mar 28 03:34:28: IP: s=172.16.47.142 (Serial1), d=172.31.200.48 (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=172.31.200.48->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->172.31.200.48 [161]
*Mar 28 03:34:28: IP: tableid=0, s=172.16.47.142 (Serial1), d=172.31.200.48
(Serial0), routed via RIB
*Mar 28 03:34:28: IP: s=172.16.47.142 (Serial1), d=172.31.200.48 (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=172.31.200.48->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->172.31.200.48 [162]
*Mar 28 03:34:28: IP: tableid=0, s=172.16.47.142 (Serial1), d=172.31.200.48
(Serial0), routed via RIB
*Mar 28 03:34:28: IP: s=172.16.47.142 (Serial1), d=172.31.200.48 (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=172.31.200.48->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->172.31.200.48 [163]
*Mar 28 03:34:28: IP: tableid=0, s=172.16.47.142 (Serial1), d=172.31.200.48
(Serial0), routed via RIB
*Mar 28 03:34:28: IP: s=172.16.47.142 (Serial1), d=172.31.200.48 (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=172.31.200.48->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->172.31.200.48 [164]
*Mar 28 03:34:28: IP: tableid=0, s=172.16.47.142 (Serial1), d=172.31.200.48
(Serial0), routed via RIB
*Mar 28 03:34:28: IP: s=172.16.47.142 (Serial1), d=172.31.200.48 (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
```

上の例では、パケットが内部から外部へ移動するとき、パケット変換を続ける前に NAT ルータはルーティング テーブルで外部アドレスへのルートを確認します。したがって、NAT ルータに外部ネットワークへの有効なルートが指定されていることが重要です。宛先のネットワークへのルートは、ルータの設定で NAT outside と指定されたインターフェイスを介して既知である必要があります。

返信パケットは、そのルーティングの前にアドレス変換が行われることに注意してください。そのため、NAT ルータのルーティング テーブルには有効な内部ローカル アドレスの指定が必要です。

関連情報

- ネットワーク アドレス変換の設定
- 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 ルータで機能する仕組み
- NAT に関するサポート ページ
- シスコテクニカルサポートおよびダウンロード

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。