IOS-XE NATの一部のパケットを変換する際の断続的な障害のトラブルシューティング

内容

はじめに

このドキュメントでは、Cisco IOS XEルータでNATをバイパスする未変換パケットについて説明します。このパケットにより、トラフィック障害が発生する可能性があります。

背景説明

ソフトウェアバージョン12.2(33)XNDでは、ネットワークアドレス変換(NAT)ゲートキーパーと呼ばれる機能が導入され、デフォルトで有効になっています。NATゲートキーパーは、非NAT対象フローが過剰なCPUを使用してNAT変換を作成することを防ぐために設計されました。これを実現するために、送信元アドレスに基づいて2つの小さなキャッシュ（in2out方向に1つとout2in方向に1つ）が作成されます。各キャッシュエントリは、送信元アドレス、Virtual Routing and Forwarding(VRF)ID、タイマー値（10秒後にエントリを無効にするために使用）、およびフレームカウンタで構成されます。キャッシュを構成するテーブルには256個のエントリがあります。NAT が必要なパケットと NAT が不要なパケットが混在する、同じ送信元アドレスからの複数のトラフィック フローが存在している場合は、パケットが NAT されず、無変換のままルータ経由で送信される可能性があります。シスコでは、可能な限り、NAT処理されたフローとNAT処理されていないフローを同じインターフェイス上に配置しないことを推奨しています。

注：これはH.323とは無関係です。

影響を受けるプラットフォーム

- ISR1K
- ISR4K
- C8200
- C8300
- C8500

バイパスされる NAT のデモ

このセクションでは、NATゲートキーパー機能が原因でNATをバイパスする方法について説明します。図の詳細を確認します。送信元ルータ、適応型セキュリティアプライアンス(ASA)ファイアウォール、ASR1K、および宛先ルータがあることがわかります。

非NAT対象宛先へのトラフィックフロー

1. 送信元：172.17.250.201宛先：198.51.100.11からpingが開始されます。
2. 送信元アドレス変換を実行する ASA の内部インターフェイスにパケットが到着します。パケットの送信元は203.0.113.231、宛先は198.51.100.11になります。
3. パケットはNAT外部から内部インターフェイスのASR1Kに到着します。NAT変換では宛先アドレスの変換が検出されないため、ゲートキーパー「out」キャッシュには送信元アドレス203.0.113.231が入力されます。
4. パケットが宛先に到着します。宛先はインターネット制御メッセージプロトコル(ICMP)パケットを受け入れ、ICMP ECHO応答を返します。この結果、pingは成功します。

同じ送信元からのトラフィックがNAT対象宛先を送信しようとする場合

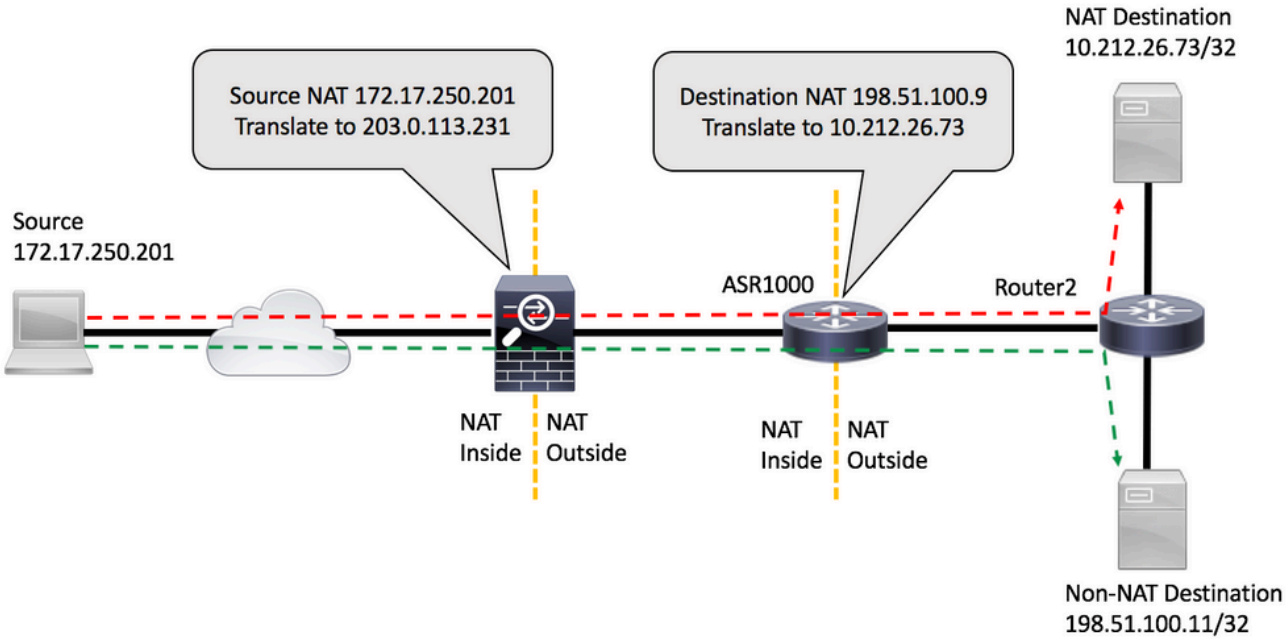
1. 送信元：172.17.250.201宛先：198.51.100.9から.pingが開始されます。
2. 送信元アドレス変換を実行する ASA の内部インターフェイスにパケットが到着します。パケットの送信元は203.0.113.231、宛先は198.51.100.9になります。
3. パケットはNAT外部から内部インターフェイスのASR1Kに到着します。NAT は、最初に送信元と宛先の変換を検索します。見つからないため、ゲートキーパーの「out」キャッシュをチェックして、送信元アドレス203.0.113.231を見つけます。パケット変換の必要なしと（誤って）想定し、宛先に向かうルートが存在する場合はパケットを転送し、そうでない場合はパケットをドロップします。どちらの方法でも、パケットは目的の宛先に到達しません。

NAT 対象トラフィックの復元

1. 10 秒後に、送信元アドレス 203.0.113.231 のエントリがゲートキーパー アウト キャッシュ内でタイムアウトになります

> 注：エントリはキャッシュ内に物理的に存在しますが、期限切れになったため使用されません。

2. ここで、同じ送信元172.17.250.201がNAT対象宛先198.51.100.9に送信する場合、パケットがASR1Kのout2inインターフェイスに到着しても、変換は見つかりません。ゲートキーパーアウトキャッシュを確認すると、アクティブエントリが見つからないため、宛先の変換を作成し、パケットが期待どおりに流れます。
3. このフローのトラフィックは、非アクティブ状態が原因で変換がタイムアウトにならない限り継続します。その間に、送信元が再び非NAT対象宛先にトラフィックを送信し、それが原因でキャッシュからゲートキーパーに別のエントリが生成される場合、確立されたセッションには影響しませんが、同じ送信元からNAT対象宛先への新しいセッションが失敗する10秒間があります。



問題の例

1. 送信元ルータ：送信元：172.17.250.201宛先：198.51.100.9からpingが開始されます。繰り返し回数2回のpingが繰り返し発行されます[FLOW1]。
2. 次に、ASR1KによってNAT変換されていない別の宛先にpingを実行します。送信元：172.17.250.201宛先：198.51.100.11 [FLOW2]。
3. その後、198.51.100.9 にさらにパケットを送信します [FLOW1]。このフローの最初のいくつかのパケットは、宛先ルータのアクセスリスト照合によって確認されるようにNATをバイパスします。

```
<#root>

source#

ping 198.51.100.9 source lo1 rep 2



Type escape sequence to abort.
Sending 2, 100-byte ICMP Echos to 198.51.100.9, timeout is 2 seconds:
Packet sent with a source address of 172.17.250.201
!!
```

```
Success rate is 100 percent (2/2), round-trip min/avg/max = 1/1/1 ms
source#ping 198.51.100.9 source lo1 rep 2

Type escape sequence to abort.
Sending 2, 100-byte ICMP Echos to 198.51.100.9, timeout is 2 seconds:
Packet sent with a source address of 172.17.250.201
!!
Success rate is 100 percent (2/2), round-trip min/avg/max = 1/1/1 ms
source#ping 198.51.100.11 source lo1 rep 200000

Type escape sequence to abort.
Sending 200000, 100-byte ICMP Echos to 198.51.100.11, timeout is 2 seconds:
Packet sent with a source address of 172.17.250.201
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!.
Success rate is 99 percent (3007/3008), round-trip min/avg/max = 1/1/16 ms
source#
```

ping 198.51.100.9 source lo1 rep 10

```
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 198.51.100.9, timeout is 2 seconds:
Packet sent with a source address of 172.17.250.201
...!!!!!!!
Success rate is 70 percent (7/10), round-trip min/avg/max = 1/1/1 ms
source#
```

宛先ルータでのACLの一致は、失敗した3つのパケットが変換されなかったことを示しています。

<#root>

```
Router2#
```

show access-list 199

```
Extended IP access list 199
    10 permit udp host 172.17.250.201 host 198.51.100.9
    20 permit udp host 172.17.250.201 host 10.212.26.73
    30 permit udp host 203.0.113.231 host 198.51.100.9
    40 permit udp host 203.0.113.231 host 10.212.26.73 (4 matches)
    50 permit icmp host 172.17.250.201 host 198.51.100.9
    60 permit icmp host 172.17.250.201 host 10.212.26.73
```

70 permit icmp host 203.0.113.231 host 198.51.100.9 (3 matches) <<<<<<<

```
    80 permit icmp host 203.0.113.231 host 10.212.26.73 (42 matches)
    90 permit udp any any log (2 matches)
    100 permit icmp any any log (4193 matches)
    110 permit ip any any (5 matches)
Router2#
```

ASR1Kでは、ゲートキーパーキャッシュエントリを確認できます。

```
<#root>

PRIMARY#

show platform hardware qfp active feature nat datapath gatein


Gatekeeper on
sip 203.0.113.231 vrf 0 cnt 1 ts 0x17ba3f idx 74
sip 10.203.249.226 vrf 0 cnt 0 ts 0x36bab6 idx 218
sip 10.203.249.221 vrf 0 cnt 1 ts 0x367ab4 idx 229

PRIMARY#

show platform hardware qfp active feature nat datapath gateout


Gatekeeper on
sip 198.51.100.11 vrf 0 cnt 1 ts 0x36db07 idx 60
sip 10.203.249.225 vrf 0 cnt 0 ts 0x36bb7a idx 217
sip 10.203.249.222 vrf 0 cnt 1 ts 0x367b7c idx 230
```

回避策と修正

ほとんどの環境では、NAT ゲートキーパー機能は正常に動作し、問題は発生しません。ただし、この問題が発生した場合は、いくつかの解決方法があります。

解決策 1

推奨されるオプションは、Cisco IOS® XEをゲートキーパー機能拡張を含むバージョンにアップグレードすることです。

Cisco Bug ID CSCun06260 XE3.13ゲートキーパーの強化

この機能拡張により、NATゲートキーパーは送信元アドレスと宛先アドレスをキャッシュできるようになり、キャッシュサイズを設定可能になります。拡張モードをオンにするには、次のコマンドを使用してキャッシュサイズを増やす必要があります。また、キャッシュをモニタして、サイズを増やす必要があるかどうかを確認することもできます。

```
<#root>

PRIMARY(config)#

ip nat settings gatekeeper-size 1024


PRIMARY(config)#

end
```

拡張モードは、次のコマンドをチェックすることで確認できます。

<#root>

PRIMARY#

show platform hardware qfp active feature nat datapath gatein

Gatekeeper on

sip 10.203.249.221 dip 10.203.249.222 vrf 0 ts 0x5c437 idx 631

PRIMARY#

show platform hardware qfp active feature nat datapath gateout

Gatekeeper on

sip 10.203.249.225 dip 10.203.249.226 vrf 0 ts 0x5eddf idx 631

PRIMARY#

show platform hardware qfp active feature nat datapath gatein active

Gatekeeper on

ext mode Size 1024

, Hits 2, Miss 4, Aged 0 Added 4 Active 1

PRIMARY#

show platform hardware qfp active feature nat datapath gateout active

Gatekeeper on

ext mode Size 1024

, Hits 0, Miss 1, Aged 1 Added 2 Active 0

解決策 2

Cisco Bug ID CSCun06260に対する修正がないリリースでは、ゲートキーパー機能をオフにするのが唯一のオプションです。唯一の悪影響は、非NAT対象トラフィックのパフォーマンスがわずかに低下し、Quantum Flow Processor(QFP)のCPU使用率が高くなることです。

<#root>

PRIMARY(config)#

no ip nat service gatekeeper

PRIMARY(config)#

end

PRIMARY#PRIMARY#

Sh platform hardware qfp active feature nat datapath gatein

Gatekeeper off

PRIMARY#

QFP使用率は、次のコマンドを使用して監視できます。

<#root>

show platform hardware qfp active data utilization summary

show platform hardware qfp active data utilization qfp 0

解決策 3

NAT パケットと非 NAT パケットが同じインターフェイスに到着しないようにトラフィック フローを分離します。

要約

NAT Gatekeeperコマンドは、非NAT対象フローに対するルータのパフォーマンスを向上させるために導入されました。状況によっては、同じ送信元からNATパケットと非NATパケットが混在して到着した場合に、この機能によって問題が発生する可能性があります。解決策は、強化されたゲートキーパー機能を使用するか、それが不可能な場合はゲートキーパー機能を無効にすることです。

参考資料

ゲートキーパーをオフにできるソフトウェア変更：
Cisco Bug ID CSCty67184 ASR1k NAT CLI – ゲートキーパーのオン/オフ
Cisco Bug ID CSCth23984 NATゲートキーパー機能をオン/オフにするためのCLI機能の追加

NAT ゲートキーパーの強化
Cisco Bug ID CSCun06260 XE3.13ゲートキーパーの強化

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。