對IOS-XE NAT間歇性故障進行故障排除，以轉換某些資料包

目錄

簡介

本檔案將說明在Cisco IOS XE路由器上繞過NAT的未轉換封包，潛在導致流量失敗。

背景資訊

在軟體版本12.2(33)XND中，已加入網路位址轉譯(NAT)閘道管理員功能，並在預設情況下啟用。NAT網守旨在防止非NAT資料流使用過多的CPU來建立NAT轉換。為實現此目的，將根據來源位址建立兩個小型快取（一個用於in2out方向，一個用於out2in方向）。每個快取條目都包含源地址、虛擬路由和轉發(virtual routing and forwarding, VRF)ID、計時器值（用於在10秒後使條目失效）和幀計數器。表中有256個條目構成了快取。如果多個流量來自同一源地址，其中有些資料包需要NAT，有些則不需要，這會導致資料包無法進行NAT處理，並通過路由器傳送時無法轉換。Cisco建議客戶儘可能避免在同一介面上進行NAT和非NAT流。

註：這與H.323無關。

受影響的平台

- ISR1K
- ISR4K
- C8200

- C8300
- C8500

繞過NAT的演示

本節介紹如何由於NAT網守功能而繞過NAT。詳細檢視該圖。您可以看到存在源路由器、自適應安全裝置(ASA)防火牆、ASR1K和目的路由器。

流向非NAT目的地的流量

1. 從源裝置啟動Ping：源：172.17.250.201目的：198.51.100.11。
2. 資料包到達執行源地址轉換的ASA的內部介面。資料包現在具有源：203.0.113.231目的：198.51.100.11。
3. 資料包到達從NAT外部到內部介面的ASR1K。NAT轉換沒有發現目標地址的轉換，因此網守「外寄」快取會填充來源位址203.0.113.231。
4. 封包抵達目的地。目的地接受網際網路控制訊息通訊協定(ICMP)封包並傳回ICMP ECHO回覆，導致ping成功。

來自同一源的流量嘗試傳送NAT驅動的目標

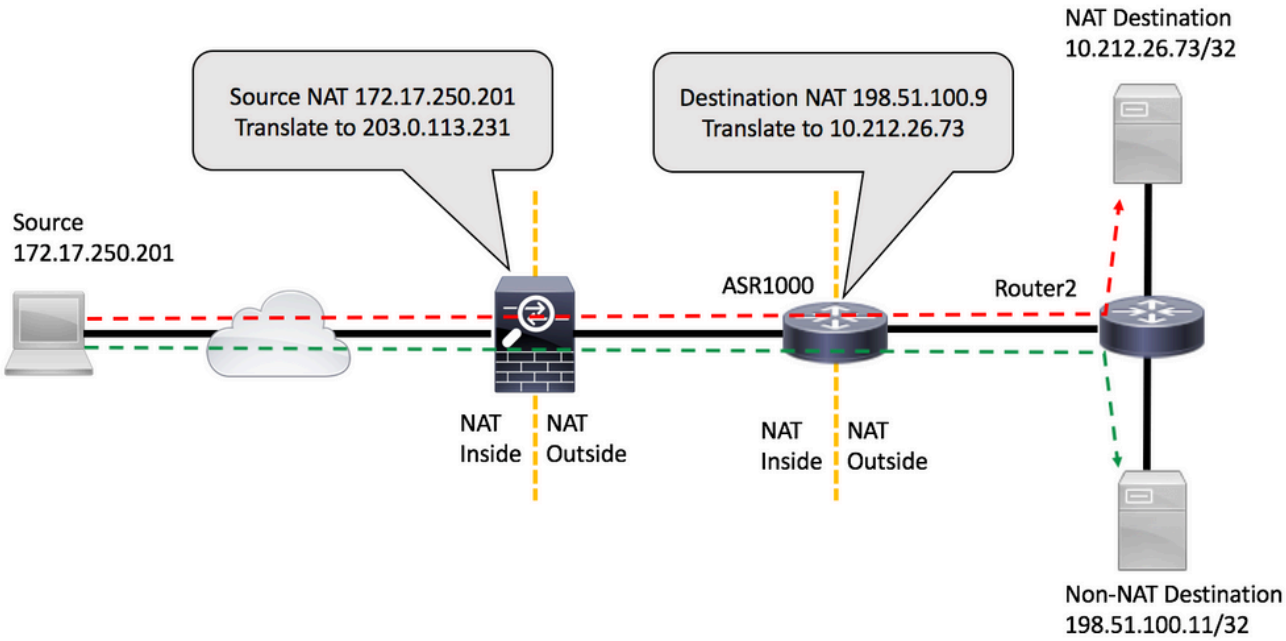
1. .Ping從源啟動：源：172.17.250.201目標：198.51.100.9。
2. 資料包到達執行源地址轉換的ASA的內部介面。資料包現在具有源：203.0.113.231目的：198.51.100.9。
3. 資料包到達從NAT外部到內部介面的ASR1K。NAT首先查詢源和目標的轉換。由於找不到該地址，因此它會檢查網守「out」快取並查詢源地址203.0.113.231。它（錯誤）假設資料包不需要轉換，如果存在目的地路由，它會轉發資料包或丟棄資料包。無論哪種方式，封包都無法到達預期目的地。

恢復NAT流量

1. 10秒後，網守輸出快取中源地址203.0.113.231的條目超時。

   注意：該項在快取中仍然實際存在，但由於其已過期，因此未使用它。

2. 現在，如果同一個來源172.17.250.201傳送到NAT目的地198.51.100.9。當資料包到達ASR1K的out2in介面時，未找到轉換。當檢查網守輸出快取時，您找不到活動條目，因此您可以按照預期為目標和資料包流建立轉換。
3. 只要轉換未因不活動而超時，此流中的流量將繼續。同時，如果源再次向非NAT目標傳送流量（這會導致將另一個條目填充到快取之外的網守中），則不會影響已建立的會話，但有10秒的時間段內，從同一源到NAT目標的新會話會失敗。



問題示例

1. 從源路由器發起Ping：源：172.17.250.201目標：198.51.100.9。發出ping時，重複計數為2，且反複於[FLOW1]。
2. 然後ping另一個未被ASR1KNAT控制的目的地：來源：172.17.250.201目的地：198.51.100.11 [FLOW2]。
3. 然後將更多資料包傳送到198.51.100.9 [FLOW1]。此流的前幾個資料包會繞過NAT，如目標路由器上的訪問清單匹配所見。

<#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#
```

目的地路由器上的ACL匹配項顯示未轉換失敗的三個封包：

<#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#
```

在ASR1K上，您可以檢查網守快取條目：

<#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
```

解決方法/修復

在大多數環境中，NAT gatekeeper功能可以正常工作並且不會引起問題。但是，如果確實遇到此問題，則有幾種方法可以解決此問題。

解決方案1

首選選項是將Cisco IOS® XE升級到包含網守增強功能的版本：

思科錯誤ID CSCun06260 XE3.13網守強化

此增強功能允許NAT網守快取源和目標地址，並使快取大小可配置。若要啟用擴展模式，您需要使用這些命令增大快取記憶體大小。您還可以監控快取記憶體以檢視是否需要增加大小。

```
<#root>

PRIMARY(config)#
ip nat settings gatekeeper-size 1024


PRIMARY(config)#
end
```

可通過檢查以下命令來驗證擴展模式：

```
<#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
```

解決方案2

對於沒有修正思科錯誤ID CSCun06260的版本，唯一的選項是關閉閘道管理員功能。唯一的負面影響是非NAT流量的效能略有降低，以及量子流處理器(QFP)上的CPU利用率較高。

```
<#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#
```

可以使用以下命令監控QFP利用率：

<#root>

```
show platform hardware qfp active data utilization summary
```

```
show platform hardware qfp active data utilization qfp 0
```

解決方案3

流量分開，使NAT和非NAT資料包不會到達同一介面。

摘要

引入了NAT Gatekeeper命令來增強路由器對非NAT流量的效能。在某些情況下，當NAT和非NAT資料包混合從同一源到達時，此功能可能會出現問題。解決方法是使用增強型閘道管理員功能，如果無法使用，請停用閘道管理員功能。

參考資料

允許關閉網守的軟體更改：
思科漏洞ID CSCty67184 ASR1k NAT CLI — 閘道管理員開啟/關閉
思科漏洞ID CSCth23984新增cli功能以開啟/關閉nat網守功能

NAT閘道管理員增強功能
思科錯誤ID CSCun06260 XE3.13網守強化

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。