排除Cat8000平台上的NAT故障

目錄

簡介

本文描述如何排除Cat8000平台上的NAT問題。

必要條件

需求

思科建議您瞭解以下主題：

- 網路位址轉譯(NAT)
- Cisco IOS XE

有關這些主題的詳細資訊，請參閱：

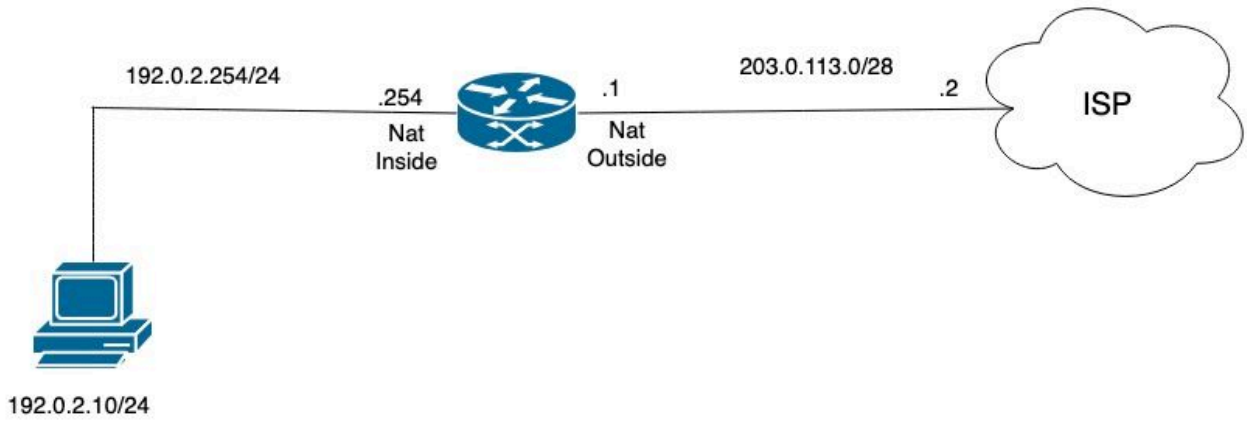
設定網路位址轉譯
瞭解NAT的運行順序
網路位址轉譯(NAT)常見問題
為IP地址保護配置NAT的限制

採用元件

本檔案中的資訊是根據Cisco IOS XE軟體。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

網路圖表



NAT 拓撲

案例研究：NAT耗盡（池耗盡）

此日誌消息表示裝置嘗試為NAT（例如為動態NAT或PAT轉換）分配IP地址，但分配失敗。當配置的NAT池中沒有剩餘可用地址或埠時，通常會發生這種情況。

常見原因包括：

· NAT池已用盡（所有可用IP地址或埠都在使用中）。
· NAT配置沒有足夠的地址或資源來滿足當前的轉換請求。

```
%NAT-6-ADDR_ALLOC_FAILURE: Address allocation failed; pool 2 may be exhausted [2] port range: NA, non-P
```

```
created by pkt: src_ip 192.0.2.13 dst_ip 192.x.x.40 src_port 0 dst_port 0 proto 1
```

檢驗NAT池以確認地址轉換範圍。

```
<#root>

NAT_R1#

show ip nat pool platform


Dump NAT pool config

ID: 2, Name: NAT_Pool, Type: Generic, Mask: 255.255.255.240
Flags: Unknown, Acct name:
Address range blocks: 1

Start: 203.0.113.3, End: 203.0.113.5


Last stats update: 07/31 13:08:43.708061785

Last refcount value: 3
```

檢驗NAT轉換表並確定當前存在的活動轉換數。

```
<#root>

NAT_R1#

show ip nat translations


Pro Inside global Inside local Outside local Outside global
--- 203.0.113.3 192.0.2.10 --- ---
--- 203.0.113.5 192.0.2.12 --- ---
--- 203.0.113.4 192.0.2.11 --- ---
icmp 203.0.113.5:0 192.0.2.12:0 198.51.100.30:0 198.51.100.30:0
icmp 203.0.113.3:0 192.0.2.10:0 198.51.100.10:0 198.51.100.10:0
icmp 203.0.113.4:0 192.0.2.11:0 198.51.100.20:0 198.51.100.20:0

Total number of translations: 6
```

檢驗NAT統計資訊中是否顯示丟棄資訊。此結果將指示傳入流量需要轉換，但由於NAT分配問題而發生丟棄。

```
<#root>

NAT_R1#

show ip nat statistics


Total active translations: 6 (0 static, 6 dynamic; 3 extended)
Outside interfaces:
GigabitEthernet0/0/4
Inside interfaces:
GigabitEthernet0/0/3
Hits: 11094661606 Misses: 10
Reserved port setting disabled provisioned no
Expired translations: 1412
Dynamic mappings:
-- Inside Source
[Id: 2] access-list 1 pool NAT_Pool

refcount 6


 <---- Translations count
pool NAT_Pool: id 2, netmask 255.255.255.240
start 203.0.113.3 end 203.0.113.5
type generic, total addresses 3, allocated 3 (100%), misses 3559386331
nat-limit statistics:
max entry: max allowed 0, used 0, missed 0

In-to-out drops: 3559337007


 Out-to-in drops: 0  <---- drops from in to out
Pool stats drop: 0 Mapping stats drop: 0
Port block alloc fail: 0
IP alias add fail: 0
Limit entry add fail: 0
NAT_R1#
```

從平台的角度，檢視QFP資料路徑NAT統計資訊，以確定這些丟棄是否與觀察到的問題相對應。

```
<#root>

NAT_R1#

show platform hardware qfp active feature nat datapath stats


Counter                                                         Value
--------------------------------------------------------------------------

number_of_session                                                 3 << The total number of active NAT se


udp                                                               0
```

```
tcp                                                    0

icmp                                                   3 << Counts of NAT sessions by protocc



non_extended                                           3 << Number of NAT sessions that are r


statics                                                0
static_net                                             0

entry_timeouts                                         1 << Number of NAT session entries tha



hits                                                585149 << Number of successful NAT lookups


misses                                                 0
cgn_dest_log_timeouts                                  0
ipv4_nat_alg_bind_pkts                                 0
ipv4_nat_alg_sd_not_found                              0
ipv4_nat_alg_sd_tail_not_found                         0

ipv4_nat_rx_pkt                                      154 << Number of IPv4 NAT packets receiv



ipv4_nat_tx_pkt                                 18791285989 << Number of IPv4 NAT packets transm


<snip>

ipv4_nat_non_natted_in2out_pkts                      144 << Number of IPv4 packets going from


ipv4_nat_non_nated_out2in_pkts                         0
<snip>

ipv4_nat_cfg_rcvd                                      8 << Number of NAT configuration messa



ipv4_nat_cfg_rsp                                       9



Subcode#14 ADDR_ALLOC_FAIL                      5216959285 << This counter indicates the number
```

驗證當前條目的數量，並比較maxhost_count和maxhost_himark值：

- maxhost_count:顯示路由器上的當前條目。
- maxhost_himark:顯示7，這表示在某個時間達到限制。

<#root>

NAT_R1#

show platform hardware qfp active feature nat datapath limit

maxhost_limit 131072

maxhost_count 5

maxhost_fail 0

maxhost_himark 7

total limit entries 0 hash tbl 0x0 max entries 0 limit_chunk 0x0 allvrf limit 0
acl limit 0 acl count 0 acl fail 0 acl_id 0x0

此日誌中的詳細資訊提供了所記錄事件和運行狀態的全面說明：

- maxhost_limit:指定平台支援的NAT主機條目的最大數量。該值表示可處理的NAT會話或轉換的上限。
- maxhost_count:指示當前使用的活動NAT主機條目或會話數。
- maxhost_fail:顯示由於達到最大限制而嘗試分配NAT主機條目的失敗次數。值為零表示未發生任何分配故障。
- maxhost_himark:表示自上次系統重置或重新啟動後使用的NAT主機條目的高水位線或峰值數。
- 總限制條目：顯示已配置或強制的NAT限制條目的總數。
- 雜湊表0x0:顯示記憶體地址或指向用於NAT限制條目的雜湊表的指標。值0x0表示當前未分配雜湊表。
- 最大條目數：指定NAT限製表中允許的最大條目數。零值表示未配置任何限制。
- limit_chunk 0x0:指示指向分配給NAT限制條目的記憶體塊的指標。值0x0表示未分配記憶體區塊。
- allvrf限制：表示應用於所有VRF（虛擬路由和轉發例項）的NAT限制。零值表示未設定全域性限制。
- acl限制：指定訪問控制清單(ACL)對NAT條目的限制。零值表示未配置任何基於ACL的限制。
- acl計數：顯示與ACL關聯的NAT條目的當前計數。

- acl fail:顯示由於ACL限制而導致NAT條目失敗的次數。
- acl_id 0x0:表示與ACL配置相關的識別符號或指標。值0x0表示未分配ACL配置。

可能起因

NAT池中的可用地址數量從3到5不等。當NAT表中保留非活動轉換時會出現問題，這會阻止其他流量進行轉換。這是預期行為，因為預設NAT轉換超時為24小時。要解決此問題，請配置ip nat translation timeout命令，以便在此操作後清除非活動轉換，NAT表需要清除。

<#root>

```
NAT_R1(config)#

ip nat translation timeout 10800


NAT_R1(config)#end
NAT_R1#

clear ip nat translation *


NAT_R1#

show ip nat translations


Pro Inside global Inside local Outside local Outside global
--- 203.0.113.5 192.0.2.11 --- ---
--- 203.0.113.4 192.0.2.10 --- ---
icmp 203.0.113.4:0 192.0.2.10:0 198.51.100.10:0 198.51.100.10:0
icmp 203.0.113.5:0 192.0.2.11:0 198.51.100.20:0 198.51.100.20:0
Total number of translations: 4
```

案例研究：NAT轉換非Nat的IP地址（網守問題）

NAT網守功能旨在通過保護NAT引擎不處理非NAT流來增強路由器效能。當非NAT資料包經過啟用了NAT的介面時，它們通常會進行大量查詢，然後NAT會確定不需要轉換。此進程在量子流處理器(QFP)上佔用CPU資源。 網守通過維護一個非NAT流的小型快取來緩解這一情況，在識別出這些資料包後，允許它們繞過NAT引擎，從而減少CPU負載。Gatekeeper快取中的條目會相對較快地超時，從而允許在網路條件發生變化且流現在可接受NAT的情況下由NAT引擎重新評估流。

當在同一介面上處理混合NAT和非NAT流量時，此機制有助於最佳化資源利用率並提高整體系統效率。可以將網守的快取大小配置為容納非NAT流量的大小，其預設值基於平台。當NAT介面上存在大量非NAT流量時，建議調整快取大小。

總而言之，NAT網守：

·保護NAT引擎避免對非NAT流進行不必要的處理。
·維護非NAT流的快取，以允許它們繞過NAT處理。
·對快取條目使用超時以允許重新評估流。
·幫助降低QFP上的CPU使用率。
·支援可配置的快取大小，以便根據流量模式最佳化效能。

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）。