Cat8000プラットフォームでのNAT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、Cat8000プラットフォームでのNATの問題をトラブルシューティングする方法について説明します。

前提条件

要件

次の項目に関する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)
- Cisco IOS XE

これらのトピックの詳細は、次の項を参照してください。

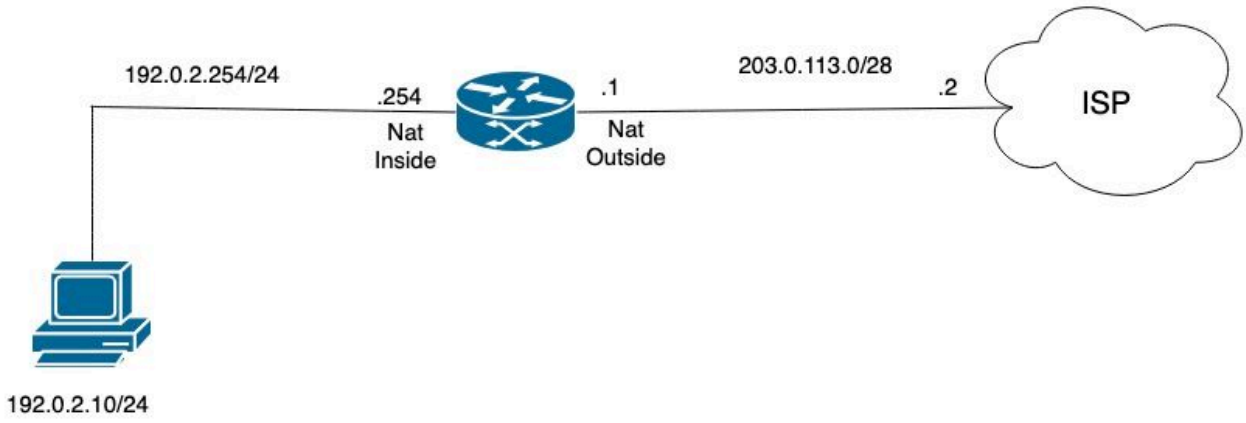
ネットワークアドレス変換の設定
NATの処理順序の理解
ネットワークアドレス変換(NAT)に関するFAQ
IPアドレス節約のためにNATを設定する場合の制約事項

使用するコンポーネント

このドキュメントの情報は、Cisco IOS XEソフトウェアに基づくものです。

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たものです。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。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。

ネットワーク図



NAT トポロジ

ケーススタディ：NAT枯渇（プール枯渇）

このログメッセージは、デバイスがダイナミックNATやPAT変換などのNATにIPアドレスを割り当てようとしたが、割り当てが失敗したことを示しています。これは通常、設定されたNATプールに使用可能なアドレスまたはポートが残っていない場合に発生します。

一般的な原因には次のものがあります。

・ NATプールが枯渇している（使用可能なすべてのIPアドレスまたはポートが使用中である）。
・ NAT構成には、現在の変換要求に対応するのに十分なアドレスまたはリソースがありません。

```
%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
```

NATプールを確認して、アドレス変換範囲を確認します。

<#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
```

NAT変換テーブルを確認し、現在存在するアクティブな変換の数を判別します。

<#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
```

ドロップがNAT統計情報に表示されるかどうかを確認します。この結果は、着信トラフィックは変換を必要とするが、NAT割り当ての問題によりドロップが発生することを示します。

```
<#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#
```

プラットフォームの観点から、QFPデータパスNAT統計情報を確認して、これらのドロップが確認された問題に対応しているかどうかを判断します。

```
<#root>

NAT_R1#

show platform hardware qfp active feature nat datapath stats
```

```
Counter                                                                    Value
-------------------------------------------------------------------------------
number_of_session                                                              3
udp                                                                            0
tcp                                                                            0
icmp                                                                           3
non_extended                                                                   3
statics                                                                        0
static_net                                                                     0
entry_timeouts                                                                 1
hits                                                                      585149
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
ipv4_nat_tx_pkt                                                     18791285989
<snip>

ipv4_nat_non_natted_in2out_pkts                                              144


ipv4_nat_non_nated_out2in_pkts                                                 0
<snip>
ipv4_nat_cfg_rcvd                                                              8
ipv4_nat_cfg_rsp                                                               9

Subcode#14 ADDR_ALLOC_FAIL                                          5216959285
```

現在のエントリ数を確認し、maxhost_countとmaxhost_himarkの値を比較します（次の例を参照）。

- maxhost_count：ルータの現在のエントリを表示します。
- maxhost_himark: 7が表示されます。これは、ある時点で制限に達したことを示します。

<#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
```

考えられる原因

NATプールで使用可能なアドレスの数は3 ~ 5です。非アクティブな変換がNATテーブルに残っている場合に問題が発生し、他のトラフィックが変換できなくなります。デフォルトのNAT変換タイムアウトは24時間であるため、この動作は予想どおりです。この問題を解決するには、このアクションの後で、非アクティブな変換をクリアするようにip nat translation timeoutコマンドを設定します。NATテーブルはクリアされている必要があります。

```
<#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
```

ケーススタディ：NATによる非NAT済みIPアドレスの変換（ゲートキーパー問題）

NATゲートキーパー機能は、NATエンジンが非NATフローを処理しないようにすることによって、ルータのパフォーマンスを向上させるように設計されています。非NATパケットがNAT対応のインターフェイスを通過する場合、通常は、変換が不要であるとNATが判断する前に広範なルックアップが実行されます。このプロセスは、Quantum Flow Processor(QFP)でCPUに負荷がかかります。 ゲートキーパーは、非NATフローの小さいキャッシュを維持し、これらのパケットが特定された後にNATエンジンをバイパスできるようにすることで、CPUの負荷を軽減することで、この問題を軽減します。ゲートキーパーキャッシュのエントリは比較的短時間でタイムアウトするため、ネットワークの状態が変化し、フローがNATの対象となる場合に、NATエンジンによってフローを再評価できます。

このメカニズムは、同じインターフェイス上でNATと非NATの混在トラフィックを処理する際に、リソース使用率を最適化し、システム全体の効率を向上させるのに役立ちます。Gatekeeperのキャッシュサイズは、プラットフォームに基づくデフォルト値を使用して、非NATトラフィックのボリュームに対応するように設定できます。NATインターフェイスに重要な非NATトラフィックが存在する場合は、キャッシュサイズを調整することをお勧めします。

要約すると、NATゲートキーパーでは次のことが行われます。

・ 非NATフローの不要な処理からNATエンジンを保護します。
・ 非NATフローのキャッシュを維持し、非NATフローがNAT処理をバイパスできるようにします。
・ キャッシュエントリのタイムアウトを使用して、フローの再評価が可能になります。
・ QFP上のCPU使用率の削減に役立ちます。
・ 設定可能なキャッシュサイズをサポートし、トラフィックパターンに基づいてパフォーマンスを最適化

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。