Troubleshoot NAT on Cat8000 Platforms

Contents

Introduction

This document describes how to troubleshoot NAT Issues on Cat8000 platforms.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Network Address Translations (NAT)
- Cisco IOS XE

For more information on these topics, see:

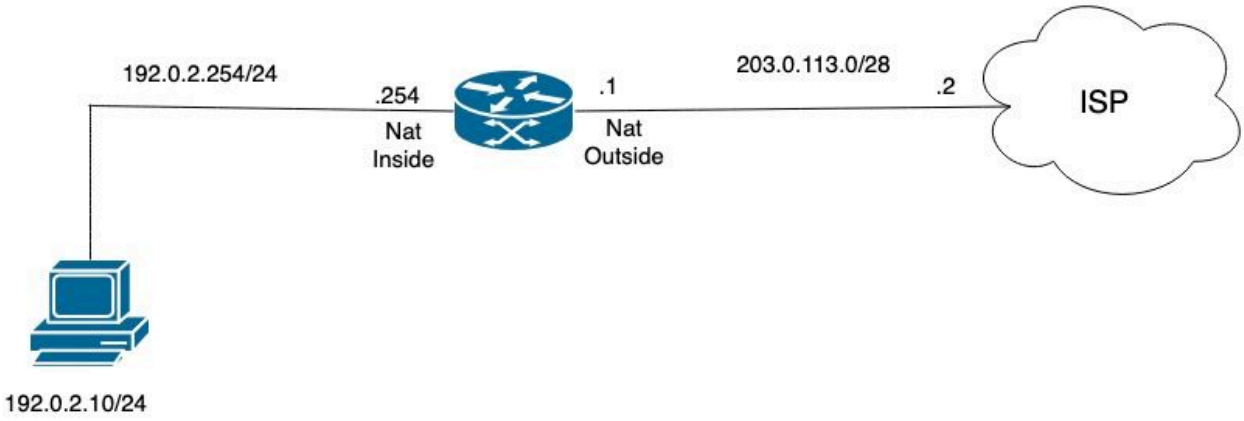
Configure Network Address Translation
Understand the NAT Order of Operation
Network Address Translation (NAT) Frequently Asked Questions
Restrictions for Configuring NAT for IP Address Conservation

Components Used

The information in this document is based on Cisco IOS XE software.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Network Diagram



NAT Topology

Case Study: NAT Exhaustion (Pool Exhausted)

This log message indicates that the device attempted to allocate an IP address for NAT, such as for a dynamic NAT or PAT translation, but the allocation was unsuccessful. This typically occurs when there are no available addresses or ports remaining in the configured NAT pool.

Common causes include:

• The NAT pool is exhausted (all available IP addresses or ports are in use).
• The NAT configuration does not have sufficient addresses or resources to accommodate the current translation requests.

```
%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
```

Verify the NAT pool to confirm the address translation range.

<#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

Verify the NAT translation table and determine the number of active translations currently present.

<#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

Verify whether drops appear in the NAT statistics. This result would indicate that incoming traffic requires translation but drops occur due to NAT allocation issues.

<#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#
```

From the platform perspective, review the QFP datapath NAT statistics to determine whether these drops correspond to the observed issue.

<#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
```

Verify the current number of entries and compare between the maxhost_count and maxhost_himark values :

- maxhost_count: shows the current entries on the router.
- maxhost_himark: shows 7, this indicates that the limit was reached at some point.

```
<#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
```

Possible Cause

The number of usable addresses in the NAT pool ranges from 3 to 5. Issues occur when inactive translations remain in the NAT table, which prevents other traffic from translation. This behavior is expected, as the default NAT translation timeout is 24 hours. To resolve this issue, configure the **ip nat translation timeout** command to clear inactive translations after this action the NAT table needs to be clear.

<#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
```

Case Study: NAT Translates Non Natted IP Addresses (Gatekeeper Issue)

The NAT Gatekeeper feature is designed to enhance router performance by protecting the NAT engine from processing non-NAT flows. When non-NAT packets traverse a NAT-enabled interface, they typically undergo extensive lookups before NAT determines that translation is not required. This process is CPU intensive on the Quantum Flow Processor (QFP). The Gatekeeper mitigates this by maintaining a small cache of non-NAT flows, allowing these packets to bypass the NAT engine once identified, thereby reducing CPU load. Entries in the Gatekeeper cache time out relatively quickly, allowing flows to be re-evaluated by the NAT engine in case network conditions change and the flow can now be subject to NAT.

This mechanism helps optimize resource utilization and improves overall system efficiency when handling mixed NAT and non-NAT traffic on the same interface. The cache size for the Gatekeeper can be configured to accommodate the volume of non-NAT traffic, with default values based on the platform. Adjusting the cache size is recommended when significant non-NAT traffic is present on a NAT interface.

In summary, the NAT Gatekeeper:

- Protects the NAT engine from unnecessary processing of non-NAT flows.
- Maintains a cache of non-NAT flows to allow them to bypass NAT processing.

• Uses timeouts on cache entries to allow re-evaluation of flows.
• Helps reduce CPU utilization on the QFP.
• Supports configurable cache size to optimize performance based on traffic patterns.