Cat8000 플랫폼의 NAT 문제 해결

목차

소개

이 문서에서는 Cat8000 플랫폼에서 NAT 문제를 해결하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- 네트워크 주소 변환(NAT)
- Cisco IOS XE

이러한 항목에 대한 자세한 내용은 다음을 참조하십시오.

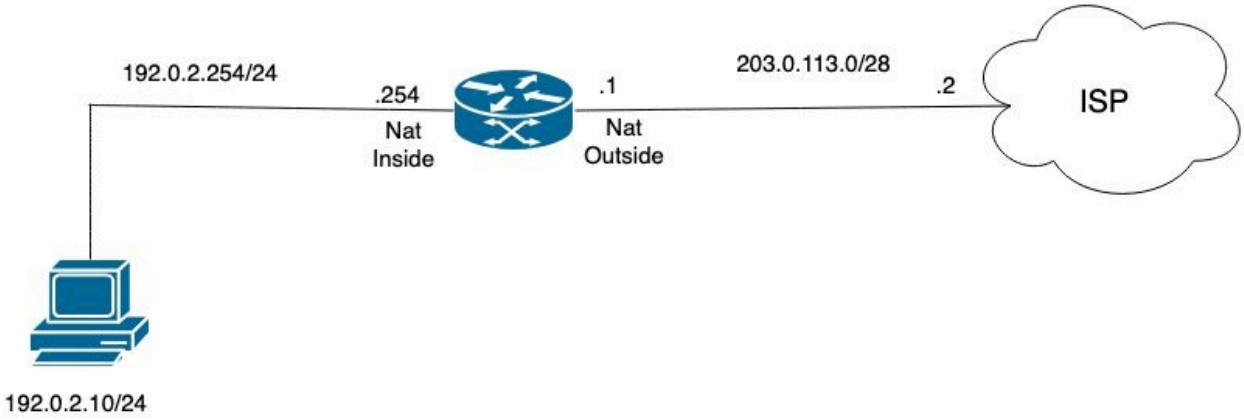
[네트워크 주소 변환 설정](#)
[NAT 작동 순서 이해](#)
[NAT(Network Address Translation) 자주 묻는 질문](#)
[IP 주소 보존을 위한 NAT 구성 제한 사항](#)

사용되는 구성 요소

이 문서의 정보는 Cisco IOS XE 소프트웨어를 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

네트워크 다이어그램



NAT 토폴로지

사례 연구: NAT 소모(풀 소진)

이 로그 메시지는 디바이스가 동적 NAT 또는 PAT 변환과 같은 NAT에 대해 IP 주소를 할당하려고 했지만 할당이 실패했음을 나타냅니다. 이는 일반적으로 구성된 NAT 풀에 남아 있는 사용 가능한 주소 또는 포트가 없을 때 발생합니다.

일반적인 원인은 다음과 같습니다.

· NAT 풀이 소진됩니다(사용 가능한 모든 IP 주소 또는 포트가 사용 중).
· NAT 컨피그레이션에 현재 변환 요청을 수용할 수 있는 충분한 주소 또는 리소스가 없습니다.

```
%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 풀을 확인하여 주소 변환 범위를 확인합니다.

<#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 변환 테이블을 확인하고 현재 존재하는 활성 변환의 수를 확인합니다.

<#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
```

NAT 통계에 드롭이 표시되는지 확인합니다. 이 결과는 수신 트래픽에 변환이 필요하지만 NAT 할당 문제로 인해 드랍이 발생함을 나타냅니다.

<#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#

플랫폼 관점에서 QFP 데이터 경로 NAT 통계를 검토하여 이러한 누락이 관찰된 문제와 일치하는지 확인합니다.

<#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
```

현재 항목 수를 확인하고 maxhost_count 값과 maxhost_himark 값을 비교합니다.

- maxhost_count: 라우터의 현재 항목을 표시합니다.
- maxhost_himark: 7을 표시합니다. 이는 특정 시점에 제한에 도달했음을 나타냅니다.

<#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
```

가능한 원인

NAT 풀에서 사용할 수 있는 주소의 수는 3개에서 5개까지 가능합니다. 비활성 변환이 NAT 테이블에 남아 있을 때 문제가 발생하여 다른 트래픽이 변환되지 않습니다. 기본 NAT 변환 시간 제한은 24시간이므로 이 동작이 필요합니다. 이 문제를 해결하려면 NAT 테이블을 지워야 하는 이 작업 이후에 비활성 변환을 지우도록 ip nat translation timeout 명령을 구성합니다.

```
<#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
```

사례 연구: NAT가 Nat가 아닌 IP 주소를 변환합니다(게이트키퍼 문제).

NAT 게이트키퍼 기능은 NAT 엔진이 비 NAT 플로우를 처리하지 않도록 보호하여 라우터 성능을 향상하도록 설계되었습니다. 비 NAT 패킷이 NAT 지원 인터페이스를 통과할 경우, NAT에서 변환이 필요하지 않다고 판단하기 전에 일반적으로 광범위한 조회를 거칩니다. 이 프로세스는 QFP(Quantum Flow Processor)에서 CPU를 많이 사용합니다. 게이트키퍼는 비 NAT 흐름의 작은 캐시를 유지 관리하여 이러한 패킷이 식별되면 NAT 엔진을 우회할 수 있도록 함으로써 CPU 부하를 줄여 줍니다. 게이트키퍼 캐시 항목의 시간이 비교적 빠르게 초과되므로, 네트워크 상태가 변경

되어 흐름이 NAT의 대상이 될 수 있는 경우 NAT 엔진에서 흐름을 다시 평가할 수 있습니다.

이 메커니즘은 동일한 인터페이스에서 혼합 NAT 및 비 NAT 트래픽을 처리할 때 리소스 사용률을 최적화하고 전반적인 시스템 효율성을 향상합니다. Gatekeeper의 캐시 크기는 플랫폼을 기반으로 하는 기본값과 함께 비 NAT 트래픽의 볼륨을 수용하도록 구성할 수 있습니다. NAT 인터페이스에 중요한 비 NAT 트래픽이 있는 경우 캐시 크기를 조정하는 것이 좋습니다.

요약하면, NAT 게이트키퍼는

· NAT 엔진을 불필요한 비 NAT 흐름 처리로부터 보호합니다.
· NAT 처리를 우회할 수 있도록 비 NAT 플로우의 캐시를 유지 관리합니다.
· 캐시 항목에 대한 시간 제한을 사용하여 흐름을 재평가할 수 있습니다.
· QFP의 CPU 사용률을 낮춥니다.
· 구성 가능한 캐시 크기를 지원하여 트래픽 패턴을 기반으로 성능을 최적화합니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.