排除Cat8000平台上的NAT故障

目录

简介

本文档介绍如何排除Cat8000平台上的NAT问题。

先决条件

要求

Cisco 建议您了解以下主题：

- 网络地址转换(NAT)
- 思科IOS XE

有关这些主题的详细信息，请参阅：

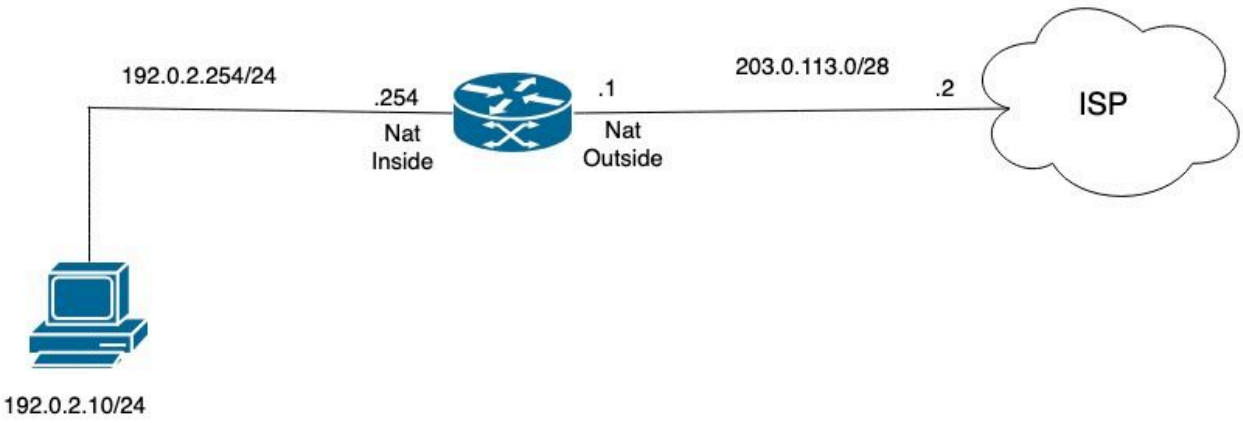
配置网络地址转换
了解NAT的运行顺序
网络地址转换(NAT)常见问题
为IP地址保护配置NAT的限制

使用的组件

本文档中的信息基于Cisco IOS XE软件。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

网络图



NAT 拓扑

案例分析：NAT耗尽（池耗尽）

此日志消息表示设备尝试为NAT分配IP地址，例如为动态NAT或PAT转换分配IP地址，但分配不成功。当配置的NAT池中没有剩余可用的地址或端口时，通常会发生这种情况。

常见原因包括：

· NAT池已用尽（所有可用IP地址或端口都在使用中）。
· NAT配置没有足够的地址或资源来满足当前的转换请求。

```
%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
```

检验NAT池以确认地址转换范围。

```
<#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
```

检验NAT转换表并确定当前存在的活动转换数。

```
<#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
```

检验NAT统计信息中是否出现丢弃。此结果将指示传入流量需要转换，但由于NAT分配问题而发生丢弃。

<#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#

从平台的角度，查看QFP数据路径NAT统计信息，以确定这些丢弃是否与观察到的问题相对应。

<#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
```

验证当前条目数并比较maxhost_count和maxhost_himark值：

- maxhost_count:显示路由器上的当前条目。
- maxhost_himark:显示7，这表示在某个点已达到限制。

<#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
```

此日志中的详细信息提供所记录事件和运行状态的全面说明：

- maxhost_limit:指定平台支持的NAT主机条目的最大数量。该值表示可处理的NAT会话或转换的上限。
- maxhost_count:指示当前使用中的活动NAT主机条目或会话的数量。
- maxhost_fail:显示由于达到最大限制而尝试分配NAT主机条目的失败计数。值为零表示未发生任何分配故障。
- maxhost_himark:表示自上次系统重置或重新启动以来使用的NAT主机条目的高水位线或峰值数。
- 总限制条目：显示已配置或已实施的NAT限制条目的总数。
- hash tbl 0x0:显示内存地址或指向用于NAT限制条目的哈希表的指针。值为0x0表示当前未分配哈希表。
- 最大条目数：指定NAT限制表中允许的最大条目数。零值表示未配置任何限制。
- limit_chunk 0x0:指示指向分配给NAT限制条目的内存块的指针。值0x0表示未分配内存块。
- allvrf限制：表示应用于所有VRF（虚拟路由和转发实例）的NAT限制。零值表示未设置全局限制。
- acl限制：指定访问控制列表(ACL)对NAT条目施加的限制。零值表示未配置基于ACL的限制。
- acl计数：显示与ACL关联的NAT条目的当前计数。
- acl失败：显示由于ACL限制而导致NAT条目失败的次数。

- acl_id 0x0:表示与ACL配置相关的标识符或指针。值0x0表示未分配ACL配置。

可能的原因

NAT池中的可用地址数量范围为3到5。当NAT表中保留非活动转换时，会出现一些问题，这会阻止其他流量进行转换。这是预期行为，因为默认NAT转换超时为24小时。要解决此问题，请配置ip nat translation timeout命令以在此操作后清除NAT表需要清除的非活动转换。

```
<#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
```

案例分析：NAT转换非nat的IP地址（网守问题）

NAT网守功能旨在通过保护NAT引擎不处理非NAT流量来增强路由器性能。当非NAT数据包通过启用NAT的接口时，它们通常会进行大量查找，然后NAT会确定不需要转换。此进程在量子流处理器(QFP)上占用了CPU资源。 网守通过维护非NAT流的小型缓存来缓解这种情况，这些数据包一旦被识别就可以绕过NAT引擎，从而减少CPU负载。网守缓存中的条目会相对较快地超时，因此NAT引擎会在网络条件发生变化时重新评估流量，并且流量现在可接受NAT。

当在同一接口上处理混合NAT和非NAT流量时，此机制有助于优化资源利用率并提高整体系统效率。网守的缓存大小可配置为容纳非NAT流量，默认值基于平台。当NAT接口上存在大量非NAT流量时，建议调整缓存大小。

总之，NAT网守：

·保护NAT引擎免于不必要的非NAT流处理。
·维护非NAT流的缓存以允许它们绕过NAT处理。
·对缓存条目使用超时以允许重新评估流。
·帮助降低QFP上的CPU使用率。
·支持可配置的缓存大小，以便根据流量模式优化性能。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。