排除Cat8000平台上的NAT故障

目录

简介

先决条件

- 要求
- 使用的组件

网络图

NAT耗尽池耗尽案例研究

- 可能的原因

NAT转换非Nat IP地址网守问题案例研究

- 确定症状
  - 正常结果
  - 如果结果不正常
- 建议

相关信息

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®

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

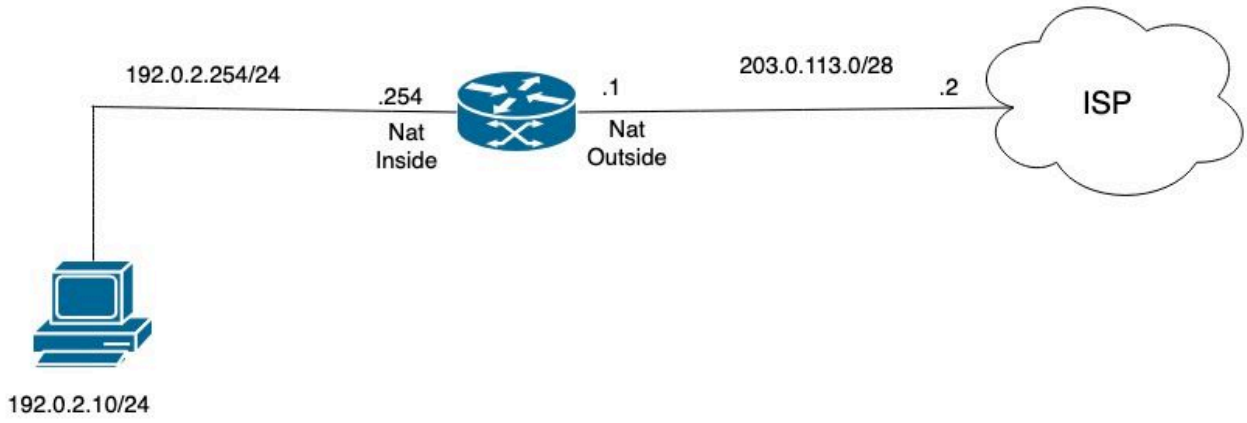
- 网络地址转换(NAT)常见问题
- 为IP地址保护配置NAT的限制

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

NAT耗尽池耗尽案例研究

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
```

步骤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
```

步骤2.检验NAT转换表并确定当前活动的转换数。

<#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
```

步骤3.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#
```

步骤4.从平台的角度，检查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**
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
```

- 会话数：指示QFP数据路径中当前存在的活动NAT会话的总数。在此输出中，值为3，该值确认三个NAT会话在收集时处于活动状态。
- icmp:显示ICMP流量的活动NAT会话数。值为3表示此输出中的所有活动NAT会话均为ICMP会话。
- 非扩展：指示平台分类为非扩展条目的NAT会话数量。在此输出中，值为3，与数据路径中显示的三个活动ICMP会话一致。
- entry_timeouts:指示超时并从数据路径中删除的NAT会话条目数。值为1可确认一个NAT条目已过期。
- 命中：命中表示数据包与NAT会话哈希表中的现有会话条目匹配。值为585149表示数据包已成功与现有NAT会话匹配。
- 未命中数：显示在数据路径中未找到匹配转换的NAT查找数。值为0表示此输出中未记录任何查找未命中。
- ipv4_nat_rx_pkt:显示此NAT数据路径记帐路径接收的IPv4数据包数。值154表示此内部接收计数器记录了154个数据包。
- ipv4_nat_tx_pkt:显示此NAT数据路径记帐路径传输的IPv4数据包数。值18791285989表示通过此内部传输计数器进行大量数据包转发活动。
- ipv4_nat_non_nat_in2out_pkts:指示在内部到外部方向观察到的、未由NAT转换的IPv4数据包的数量。值为144可确认144个数据包未应用NAT就通过此路径。
- ipv4_nat_non_nat_out2in_pkts:指示在外部到内部方向观察到的、未由NAT转换的IPv4数据包的数量。值为0表示此快照中未记录此类数据包。
- ipv4_nat_cfg_rcvd:显示数据路径接收的NAT相关配置消息的数量。值为8可确认已收到八条配置消息。
- ipv4_nat_cfg_rsp:显示数据路径发送的NAT相关配置响应数。值9确认已发送9个配置响应。
- 子代码#14 ADDR_ALLOC_FAIL:显示NAT数据路径地址分配失败的数量。值为5216959285表示数据路径在一段时间内记录了非常多的分配失败。此计数器与调查间歇NAT转换问题高度相关，需要与show ip nat statistics、show ip nat translations和其他QFP NAT数据路径输出关联。

步骤5.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
```

NAT转换非Nat IP地址网守问题案例研究

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。

确定症状

典型症状包括：

- 间歇性流量丢弃
- 有些主机工作而另一些主机失败
- 存在NAT转换，但流量被丢弃
- 应用会话意外重置
- 影响大规模PAT部署
- 网守计数器增加

步骤1.在故障窗口期间检验NAT统计信息。
此步骤确认：

- nat是否正在接收匹配流量
- 是否正在创建转换
- 问题期间未命中数是否增加
- 地址池或过载状态是否正常

<#root>

NAT_R1#

show ip nat statistics

Total active translations: 29477 (736 static, 28741 dynamic; 28741 extended)

Outside interfaces:
GigabitEthernet1
Inside interfaces:
GigabitEthernet2, GigabitEthernet3

Hits: 32525856687 Misses: 293948584

Expired translations: 293549953

Dynamic mappings:
-- Inside Source
[Id: 1] route-map INTERNET_PAT interface GigabitEthernet1 refcount 25
nat-limit statistics:

max entry: max allowed 0, used 0, missed 0

In-to-out drops: 0 Out-to-in drops: 867

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#

show ip nat statistics | sec Misses

Hits: 32525856687

Misses: 293948584

NAT_R1#show ip nat statistics | sec Misses
Hits: 32527039444

Misses: 293952367

NAT_R1#show ip nat statistics | sec Misses
Hits: 32527308509

Misses: 293953221

NAT_R1#

一节对输出中的相关信息提供了详细说明。

- 活动转换总数：指示转换表中当前安装的NAT条目总数。在此输出中，有29,477个活动转换。
- 736静态：指定当前活动的静态NAT条目数。这些是手动配置的固定映射。
- 28741动态：指定当前活动的动态NAT条目数。这些条目是从流量中自动创建的。
- 28741扩展：表示所有动态条目都是扩展转换，这意味着它们包含第4层信息，例如协议和端口号。这通常适用于PAT流量。
- 命中数:显示与现有NAT转换条目匹配的数据包数量。值32,525,856,687表示NAT正在积极处理大量流量。
- 未命中数：显示查找时与现有NAT转换条目不匹配的数据包数量。在动态NAT/PAT中，这通常发生在创建转换之前新流量的第一个数据包上。值为293,948,584表示随时间推移大量新会话查找。
- In-to-out drops:显示NAT处理期间从内部到外部丢弃的数据包数量。值为0表示未发生出站NAT丢弃。
- 出站入站：显示NAT处理过程中从外部到内部方向丢弃的数据包数量。值867表示一些入站数据包到达时没有有效的匹配转换或有效的NAT状态。
- 池统计信息丢弃：显示与NAT池处理相关的丢弃数。值为0表示未发生与池相关的丢弃。
- 映射统计信息丢弃：显示与NAT映射问题相关的丢弃数。值为0表示未发生与映射相关的丢弃。
- 端口块分配失败：显示分配PAT端口块的失败次数。值为0表示未发生端口分配故障，并且没有PAT端口耗尽的迹象。
- IP别名添加失败：显示与NAT的IP别名创建相关的失败次数。值为0表示未发生与别名相关的故障。
- 限制条目添加失败：显示由于限制限制而添加NAT条目的失败次数。值0确认没有转换被NAT限制实施阻止。

NAT统计信息显示未命中计数器的计数增加，但增加的模式与正常的动态NAT/PAT会话创建模式相同。

在所观察到的间隔内：

点击量从32,525,856,687增加到32,527,308,509
    增量：1,451,822
未命中数从293 948 584增加到293 953 221
    增量：4,637

这反映了同期每多出1次未命中，大约增加313次命中。在动态NAT/PAT环境中，当数据包在表中已存在匹配转换之前到达时，会发生未命中。一旦创建了转换，该流的后续数据包将计为命中数。根据此行为，所观察到的丢失事件增加与正在进行的会话创建和正常的转换变动一致。

步骤2.检验NAT表中是否存在转换。过滤准确受影响流量的输出（如果适用）。
此步骤确认路由处理器(RP)NAT表是否包含受影响流的转换条目。

正常结果

该折算存在并反映：
正确的内部本地
更正内部全局
正确的外部地址
正确的协议和端口映射

如果结果不正常

解释：
不存在转换条目
重点关注NAT匹配、ACL、路由映射或资源分配。
转换存在，但流量仍然失败
转到QFP验证步骤。

这是工作流中最重要的分支之一。

<#root>

```
NAT_R1#

show ip nat translations verbose


Pro Inside global Inside local Outside local Outside global
icmp 203.0.113.2:3157 192.0.2.2:3157 x.x.x.x:3157 x.x.x.x:3157
  create: 06/19/26 05:36:53, use: 06/19/26 05:36:53, timeout: 00:00:45
  RuleID : X
  Flags: unknown
  ALG Application Type: NA
  WLAN-Flags: unknown
  Mac-Address: 0000.0000.0000 Input-IDB: GigabitEthernet2
  entry-id: 0xe8a48090, use_count:1
  In_pkts: X In_bytes: 44, Out_pkts: X Out_bytes: X
  Output-IDB: GigabitEthernet1
```

- 协议 | icmp |转换条目用于ICMP流量：在ICMP条目中，冒号后面的值代表ICMP标识符，而不

是TCP或UDP端口。

- 内部全局 |203.0.113.2:3157 |在外部网络上看到的转换后的源地址。203.0.113.2是用于此流量的公有NAT地址。
- 内部本地 |192.0.2.2:3157 |转换前内部主机的原始源地址。
- 外部本地 | x.x.x.x:3157 |从内部网络看到的目标地址。
- 外部全局 | x.x.x.x:3157 |外部网络上的实际目标地址。此字段与外部本地值匹配，因为没有应用外部转换。
- 规则ID | X |创建此转换条目的NAT规则。
- 标志 | unknown |与条目关联的内部NAT标志。CLI不会解码显示的输出中的此值。
- ALG应用类型 | NA |没有应用层网关与此ICMP转换关联。
- WLAN标志 | unknown |平台特定的WLAN相关标志。此字段与此条目在操作上无关。
- Mac 地址 |0000.0000.0000 |此转换条目未填充MAC地址字段。
- Input-IDB | GigabitEthernet2 |原始数据包进入路由器的入口接口。这将确认源自GigabitEthernet2内部的数据流。
- 条目ID | 0xe8a48090 |内存中NAT转换条目的内部标识符。
- 使用计数 |转换条目的内部引用计数。
- 在数据包中 |此转换在一个方向上计数的数据包数。
- 以字节为单位 |在与In数据包相同的方向上计数的字节数。
- 传出数据包 |与此转换反向计数的数据包数。
- 输出字节 |与Out数据包具有相同方向的字节数。
- Output-IDB | GigabitEthernet1 |已转换流量使用的出口接口。这确认转换后的数据包通过GigabitEthernet1退出。

步骤3.检验转换是否已在QFP中编程

此步骤确认RP中可见的转换是否也在转发硬件路径中编程。

<#root>

```
NAT_R1#

show platform hardware qfp active feature nat datapath gateout


Gatekeeper on
<snip>
sip 192.0.2.35 dip x.x.x.x vrf 0 ts 0xcdd07450 idx 10268
sip 192.0.2.67 dip x.x.x.x vrf 0 ts 0xcdd072de idx 44104
sip 198.51.100.12 vrf 0 cnt 225 ts 0x1b393b5 idx 56738

sip 198.51.100.89 dip x.x.x.x vrf 0 ts 0xcdd071b2 idx 59429 <---------------- Affected Host
```

| 0xcdd07450 |内部QFP时间戳/年龄值（十六进制）。
| idx | 10268 |内部入口表索引。

| cnt | 225 |该入口对象的内部活动/引用计数。在某些条目类型上可见。

|条目1 | sip 192.0.2.35 dip x.x.x.x vrf 0 ts 0xcdd07450 idx 10268 |源192.0.2.35的元组特定网关条目指向VRF 0中的目标x.x.x.x。
|条目2 | sip 192.0.2.67 dip x.x.x.x vrf 0 ts 0xcdd072de idx 44104 |源192.0.2.67的元组特定网关条目，指向VRF 0中的组播目标x.x.x.x。
|条目3 | sip 198.51.100.12 vrf 0 cnt 225 ts 0x1b393b5 idx 56738 | VRF 0中源主机导向的网关条目198.51.100.12，内部活动/参考计数为225。
|条目4 | sip 198.51.100.89 dip x.x.x.x vrf 0 ts 0xcdd071b2 idx 59429 |源198.51.100.89的元组特定网关条目，指向VRF 0中的目标x.x.x.x。

输出确认设备上启用了NAT数据路径网守功能。它还显示，受影响的源地址198.51.100.89在QFP NAT网关表中作为与VRF 0中的目标流关联的一个元组特定条目存在。

这表示源自198.51.100.89的流量到达QFP数据路径中的NAT转换创建路径，并由网守进程进行内部跟踪。ts和idx值是该网关条目的内部QFP引用。

此输出不确认是否已为受影响的流成功安装完全NAT转换。它仅确认该源/目标元组存在内部网守状态。

对于报告的间歇性行为，相关观察是198.51.100.89在问题窗口期间在网闸中可见，该窗口将故障域与NAT数据路径网守或转换安装阶段对齐，而不是完全没有来自受影响主机的流量。

步骤4.检查NAT网守统计信息。

缓存未命中率快速增加表示未将非NAT转换流添加到缓存。这种情况会提高量子流处理器(QFP)的利用率。

<#root>

```
NAT_R1#
```

show platform hardware qfp active feature nat datapath gateout activity

```
Gatekeeper on
def mode Size 8192, Hits 448492109001,
```

Miss 53295038401

```
, Aged 149941327 Added 603614728 Active 1899
```

<#root>

NAT_R1#

show platform hardware qfp active feature nat datapath gateout activity

Gatekeeper on
def mode Size 8192, Hits 191540578459,

Miss 3196566091

, Aged 1365537 Added 9 Active 7

步骤5.在QFP级别验证丢弃。

检查与NAT相关的丢弃计数器

<#root>

NAT_R1#

show platform hardware qfp active statistics drop

Last clearing of QFP drops statistics : never

Global Drop Stats	Packets	Octets
NatIn2out	1701	174437
NatOut2in	4838	267167

NAT_R1#

show platform hardware qfp active statistics drop

Last clearing of QFP drops statistics : never

Global Drop Stats	Packets	Octets
NatIn2out	8039	823998
NatOut2in	26427	1461299

NAT_R1#

show platform hardware qfp active statistics drop

```
Last clearing of QFP drops statistics : never

-------------------------------------------------------------------------
Global Drop Stats                                  Packets         Octets
-------------------------------------------------------------------------
NatIn2out                                            12498        1281045
NatOut2in                                            41211        2278842
```

在观察到的行为期间，NatIn2out和NatOut2in QFP丢弃计数器持续增加，表示内部到外部和外到内部NAT转换路径中的数据包持续丢弃。

步骤6.使用数据包验证捕获受到影响的数据包。

此问题中的数据包捕获提供了对通过设备的数据包流和处理的详细可视性，从而能够识别数据包是被NAT转换还是绕过，并帮助隔离NAT网守相关问题的根本原因。这有助于有针对性地排除故障和验证配置更改。

<#root>

ip access-list extended TAC

```
permit ip host 198.51.100.89 <destination IP >
permit ip <destination IP > host 198.51.100.89
```

```
debug platform condition ipv4 access-list TAC both
debug platform packet packet 128 fia-trace circular
debug platform packet-trace copy packet both
debug platform condition start
debug platform condition stop
```

注意：本文档不深入介绍数据包捕获。有关数据包捕获的详细信息，请参阅本文档：数据路径[数据包跟踪功能 — 数据包捕获]

根据数据包捕获分析，发现NAT进程丢弃了受影响的主机流量。具体而言，捕获的数据包与任何现有NAT转换条目或访问控制列表(ACL)中定义的子网都不匹配。 这表示数据包不受NAT转换的约束，也不受已配置的ACL的允许，这可能是导致连接问题的原因。进一步调查可以侧重于检验NAT转换规则和ACL配置，以确保正确处理受影响的流量。

<#root>

NAT_R1#

show platform packet-trace packet 122 decode

Packet: 122 CBUG ID: 650
Summary
Input   : GigabitEthernet1
Output   : GigabitEthernet2
State   : FWD
Timestamp
Start   : 6725512391055 ns (07/01/2026 16:56:32.593082 UTC)
Stop   : 6725512441820 ns (07/01/2026 16:56:32.593133 UTC)
Path Trace
Feature : IPV4(Input)
Input   : GigabitEthernet1
Output   : GigabitEthernet2
Source   : 198.51.100.89
Destination   : <remote Host>
Protocol   : 6 (TCP)
SrcPort   : 16130
DstPort   : 1560
<snip>

Feature : NAT

Direction   : OUT to IN
Action   : FWD

FWD-POINT   : GATEKEEPER_BLOCKED

VRF   : 2
Feature: IPV4_NAT_INPUT_FIA
Entry   : Input - 0x700140f0
Input   : GigabitEthernet1
Output   : <unknown>
Lapsed time   : 8970 ns
<snip>
Packet Copy In
<snip>
ARPA
Destination MAC   : aaaa.bbbb.cccc
Source MAC   : bbbb.bbbb.aaaa
<snip>
Packet Copy Out
<snip>>

Found the issue to be gatekeeper:

Feature: NAT
Direction   : IN to OUT
Action   : FWD

FWD-POINT   : GATEKEEPER_BLOCKED

建议

Cisco建议将NATed和非NATed流量分离到不同的接口或设备，以防止与NAT网守功能相关的问题。这种分离有助于避免同一接口上混合流量类型导致的过度处理。

此外，Cisco建议升级到包含NAT网守功能增强功能的Cisco版本。这些增强功能可同时缓存源和目标IP地址，并允许配置缓存大小。可以在全局配置模式下使用命令调整缓存大小：

```
ip nat settings gatekeeper-size <value>
```

值必须是2的幂，建议以接近默认设置的大小开头。调整缓存大小后，监控缓存命中与未命中以确保最佳性能和资源利用率。

增加缓存大小可以减少缓存未命中次数并提高NAT处理效率，但它也会消耗量子流处理器(QFP)上的额外内存。 因此，在仔细监测下可逐渐进行调整。

这些建议旨在优化NAT网守性能，并减少由NAT和非NAT流量混合产生的潜在问题。

相关信息

- 由于NAT网守默认配置导致高QFP利用率故障排除
- 排除IOS NAT间歇性故障以转换数据包

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）。