某局点M9000设备NAT业务异常的经验案例

NAT 叶靖 2022-01-29 发表

组网及说明

某局点购买了两台我司的M9000系列防火墙设备，设备型号为H3C SecPath M9000-AI-E16，版本为Version 7.1.064, Release 9001P3002。两台M9000配置堆叠irf，并将M9000设备作为出口防火墙，在外网口配置了NAT，但是配置完成以后经测试发现，内网用户无法正常通过NAT访问外网。

问题描述

现场的外网口为二层聚合口1，成员接口是T1/0/2/23以及T2/0/2/23，配置简要如下：

```
#
interface Bridge-Aggregation1
 port access vlan 4094
#
#
interface Ten-GigabitEthernet1/0/2/23
 port link-mode bridge
 port access vlan 4094
 port link-aggregation group 1
#
interface Ten-GigabitEthernet2/0/2/23
 port link-mode bridge
 port access vlan 4094
port link-aggregation group 1
#
interface LoopBack0
 ip address 10.10.10.10 255.255.255.255（作为测试地址）
#
interface Vlan-interface4094
 ip address 1.1.1.190 255.255.255.192
 nat outbound 2000 address-group 1
#
[FW-Vlan-interface4094]dis nat ad
[FW-Vlan-interface4094]dis nat address-group 1
 Address group ID: 1
 Port range: 1-65535
 Blade-load-sharing-group: Blade5fw1
 Address information:
  Start address  End address
  1.1.1.136 1.1.1.143
 Exclude address information:
  Start address  End address
  ---   --
```

现场测试结果如下：

在设备上直接ping公网下一跳1.1.1.129，可以直接ping通ping 1.1.1.129------直接ping能ping通

```
Ping  1.1.1.129 ( 1.1.1.129): 56 data bytes, press CTRL+C to break
56 bytes from  1.1.1.129: icmp_seq=0 ttl=254 time=1.368 ms
56 bytes from  1.1.1.129: icmp_seq=1 ttl=254 time=1.114 ms
56 bytes from  1.1.1.129: icmp_seq=2 ttl=254 time=1.023 ms
56 bytes from  1.1.1.129: icmp_seq=3 ttl=254 time=1.078 ms
56 bytes from  1.1.1.129: icmp_seq=4 ttl=254 time=1.150 ms

--- Ping statistics for  1.1.1.129 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 1.023/1.147/1.368/0.118 ms
```

带loopback接口地址ping外网下一跳，无法ping通

ping -a 10.10.10.10 1.1.1.129--------带设备上loopback接口地址ping外网不通

```
Ping  1.1.1.129 ( 1.1.1.129) from 10.10.10.10: 56 data bytes, press CTRL+C to break
Request time out
Request time out

--- Ping statistics for  1.1.1.129 ---
3 packet(s) transmitted, 0 packet(s) received, 100.0% packet loss
```

过程分析

1、我们知道M9000系列设备对于NAT是有很多限制的，主要如下：

- 接口板引流表项有限，需要配置时保证引流表项有余量，当引流表项满时会导致流量异常。QACL资源不足的时候下发大量NAT相关配置会导致串口长时间等待无响应。由于接口卡支持引流表项有限，NAT地址池包含地址建议配置成掩码网段。例如10.0.0.16~10.0.0.31。
- NAT地址池中的地址数必须大于或者等于备份组个数*2。这里的备份组特指自动备份组和手动备份组，且整机环境中所有业务板使用的备份组类型必须一致，要么都是自动备份组，要么都是手动备份组，不允许自动备份组和手动备份组混用。

但是现场针对以上限制都是满足的，地址池里的地址数是足够的，另外地址也配置成了掩码网段（1.1.1.136-1.1.1.143）。

2、由于现场配置了堆叠irf，所以需要开启会话同步功能，但是现场确认也是正常开启了会话同步功能的。

session synchronization enable
session synchronization dns
session synchronization http

3、接下来我们查看会话，通过以下命令进行查看，具体如下：

dis session table ipv4 source-ip 10.10.10.10 destination-ip 1.1.1.129 verbose
CPU 1 on slot 2 in chassis 1:
Total sessions found: 0

CPU 2 on slot 2 in chassis 1:
Total sessions found: 0

CPU 1 on slot 3 in chassis 1:
Total sessions found: 0

CPU 2 on slot 3 in chassis 1:
Initiator:
  Source   IP/port: 10.10.10.10/12537
  Destination IP/port: 1.1.1.129/2048
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: ICMP(1)
  Inbound interface: InLoopBack0
  Source security zone: Local
Responder:
  Source   IP/port: 1.1.1.129/4
  Destination IP/port: 1.1.1.136/0
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: ICMP(1)
  Inbound interface: Vlan-interface4094
  Source security zone: Untrust
State: ICMP_REQUEST
Application: ICMP
Rule ID: 21
Rule name: Local-Untrust
Start time: 2022-01-16 00:42:14 TTL: 22s
Initiator->Responder: 5 packets   420 bytes
Responder->Initiator: 0 packets   0 bytes----------看会话是对端没回。

Total sessions found: 1

Slot 8 in chassis 1:
Total sessions found: 0

Slot 9 in chassis 1:
Total sessions found: 0

CPU 1 on slot 2 in chassis 2:
Total sessions found: 0

CPU 2 on slot 2 in chassis 2:
Total sessions found: 0

CPU 1 on slot 3 in chassis 2:
Total sessions found: 0

CPU 2 on slot 3 in chassis 2:
Total sessions found: 0

Slot 8 in chassis 2:
Total sessions found: 0

Slot 9 in chassis 2:
Total sessions found: 0
[FW]

根据会话来看，Initiator->Responder方向是发送了5个报文，但是Responder->Initiator方向没有看到任何回应，另外能看到，源地址已经正常的进行了转换，转换为了NAT地址池中的地址1.1.1.136，说明NAT也是正常生效的。因此我们怀疑是否是外网线路的问题，但是经现场测试，将外网口配置地址为1.1.1.136，是能正常ping通1.1.1.129的。网络线路问题也被排除。

4、最后查阅M9000系列防火墙的版本说明书发现，设备有以下限制：
·　　不支持携带两层VLAN Tag的QinQ报文。启用三层VLAN虚接口，对应二层口需为Trunk/Hybrid类型，且接收报文须携带VLAN Tag。不支持在三层VLAN虚接口上配置BFD MAD检测。
现场的M9000防火墙上启用了三层vlan虚接口之后，正是将对于二层聚合口interface Bridge-Aggregation1配置为了access接口，port access vlan 4094，接口收到的报文也是不携带vlan tag的。现场正是匹配上了设备限制，导致设备流表下发异常，最终造成现场该问题。

解决方法

将外网口由之前的二层聚合口修改为三层聚合口，将NAT的配置配置在该三层接口上，修改后，测试NAT等业务均正常。