nat address-group地址和nat server地址配置冲突

NAT NAT444 AFT **曾招维** 2022-01-30 发表

组网及说明

本案例适用于盒式防火墙和LB设备。

现场反馈在SecPath L5030(V7)上nat group地址和nat server地址同时配置xxx.7.197.248提示冲突，但是可以成功配置上，而且现场反馈配置可正常运行，想确认配置报地址冲突是否有影响。 用实验室防火墙测试，也有相同报错，而且nat outbound和nat server同时生效。

现象：

[H3C-address-group-4]address XXX.7.197.248 221.7.197.248

[H3C-GigabitEthernet2/0/1]nat server protocol tcp global XXX .7.197.248 81 inside 10.6.53.138 81

IP address XXX.7.197.248 conflicts with the existing nat address group, please exclude it from the address group.

[H3C -GigabitEthernet2/0/1]dis th

#

 interface GigabitEthernet2/0/1

port link-mode route

nat outbound address-group 4

nat server protocol tcp global xxx.7.197.248 81 inside 10.6.53.138 81 rule ServerRule_14

#

问题描述

实验室模拟，已放通安全策略、打通路由。

模拟终端：

[PC-GigabitEthernet1/0/10]dis th

#

interface GigabitEthernet1/0/10

port link-mode route

ip address xxx.7.190.177 255.255.255.252

#

防火墙模拟LB：

[F1030-NEW-LoopBack1]DIS TH

#

interface LoopBack1

ip address 1.1.1.1 255.255.255.0

#

[F1030-NEW-address-group-4]dis th

#

nat address-group 4

address xxx.7.197.248 xxx.7.197.248

#

[F1030-NEW-GigabitEthernet2/0/10]dis th

#

interface GigabitEthernet2/0/10

port link-mode route

ip address xxx.7.190.178 255.255.255.252

nat outbound address-group 4

nat server global xxx.7.197.248 inside 1.1.1.1 rule ServerRule_15

#

防火墙 ping 终端：

ping -a 1.1.1.1 xxx.7.190.177

Ping xxx.7.190.177 (xxx.7.190.177) from 1.1.1.1: 56 data bytes, press CTRL+C to break

56 bytes from xxx.7.190.177: icmp_seq=0 ttl=255 time=0.868 ms

56 bytes from xxx.7.190.177: icmp_seq=1 ttl=255 time=0.333 ms

56 bytes from xxx.7.190.177: icmp_seq=2 ttl=255 time=0.337 ms

56 bytes from xxx.7.190.177: icmp_seq=3 ttl=255 time=0.304 ms

56 bytes from xxx.7.190.177: icmp_seq=4 ttl=255 time=0.324 ms

--- Ping statistics for xxx.7.190.177 ---

5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss

round-trip min/avg/max/std-dev = 0.304/0.433/0.868/0.218 ms

display session table ipv4 destination-ip xxx.7.190.177 verbose

Initiator:

Source IP/port: 1.1.1.1/36775

Destination IP/port: xxx.7.190.177/2048

DS-Lite tunnel peer: -

VPN instance/VLAN ID/Inline ID: -/-/-

Protocol: ICMP(1)

Inbound interface: InLoopBack0

Source security zone: Local

Responder:

Source IP/port: xxx.7.190.177/1

Destination IP/port: **xxx.7.197.248/0//nat outbound有生效**

DS-Lite tunnel peer: -

VPN instance/VLAN ID/Inline ID: -/-/-

Protocol: ICMP(1)

Inbound interface: GigabitEthernet2/0/10

Source security zone: Trust

State: ICMP_REPLY
Application: ICMP
Rule ID: 4
Rule name: any_93160
Start time: 2022-01-19 00:37:04 TTL: 29986s
Initiator->Responder: 5 packets 420 bytes
Responder->Initiator: 5 packets 420 bytes

过程分析

可以看出虽然配置地址存在冲突时候会报错，但测试效果是没有受到影响的。
那什么时候会触发异常呢?
1.端口outbound先于nat server建立会话，因为nat outbound先建立会话，nat server就不会取用这个端口了。
2.nat outbound使用端口后，端口没有释放的时候，nat server有触发访问。
3.nat outbound长时间不释放，才会导致nat server长时间无法建立。
所以这个冲突的触发条件其实比较苛刻，但是一旦触发也很难排查，因此是不推荐配置冲突，但多数情况可以正常使用。

终端ping global地址:
[H3C-M-2(D045)]ping xxx.7.197.248
Ping xxx.7.197.248 (xxx.7.197.248): 56 data bytes, press CTRL+C to break
56 bytes from xxx.7.197.248: icmp_seq=0 ttl=255 time=0.228 ms
56 bytes from xxx.7.197.248: icmp_seq=1 ttl=255 time=0.288 ms
56 bytes from xxx.7.197.248: icmp_seq=2 ttl=255 time=0.237 ms
56 bytes from xxx.7.197.248: icmp_seq=3 ttl=255 time=0.250 ms
56 bytes from xxx.7.197.248: icmp_seq=4 ttl=255 time=0.228 ms

--- Ping statistics for xxx.7.197.248 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 0.228/0.324/0.623/0.151 ms

[F1030-NEW]display session table ipv4 destination-ip xxx.7.197.248 verbose
Slot 2:
Initiator:
  Source   IP/port: xxx.7.190.177/11940
  Destination IP/port: xxx.7.197.248/2048
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: ICMP(1)
  Inbound interface: GigabitEthernet2/0/10
  Source security zone: Trust
Responder:
  Source   IP/port: **1.1.1.1/11940//nat server目的地址转变成功**
  Destination IP/port: xxx.7.190.177/0
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: ICMP(1)
  Inbound interface: InLoopBack0
  Source security zone: Local
State: ICMP_REPLY
Application: ICMP
Rule ID: 4
Rule name: any_93160
Start time: 2022-01-19 00:14:55 TTL: 29996s
Initiator->Responder: 5 packets 420 bytes
Responder->Initiator: 5 packets 420 bytes

解决方法

中低端安全产品出现这条报错可以正常使用，但对于高端安全产品涉及到流表信息不可以有冲突。

IP address XXX.7.197.248 conflicts with the existing nat address group, please exclude it from the address group.