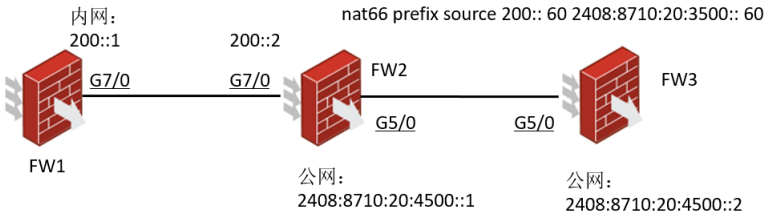
某局点comwareV7防火墙NAT66不成功

NAT 孔德飞 2021-10-15 发表

组网及说明

组网如下：

内网FW1通过NAT66来访问外网FW3



问题描述

现场配置了NAT66，发现内网FW1无法通过源地址200::1访问FW32408:8710:20:4500::2

```
interface GigabitEthernet5/0
 port link-mode route
 ip address 66.66.66.67 255.255.255.0
 nat66 prefix source 200:: 60 2408:8710:20:4500:: 60
 ipv6 address 2408:8710:20:4500::1/60
```

过程分析

查看配置手册，发现有如下说明：主要是我打中括号的说明，就是字面意思，NAT66前缀不能与外网口相同，也不能与内网访问的目的地址相同

1. 配置限制和指导

在同一个接口下，一个内网地址前缀和一个外网地址前缀必须是一对一的唯一映射关系。
不同接口下，同一个外网地址前缀不能映射为不同的内网地址前缀。
【内部服务器向外提供服务时对外公布的外网IPv6地址前缀不能与NAT66设备的外网地址前缀以及访问内部服务器的外网主机地址前缀相同。
不支持对 AH和ESP协议的报文进行NAT66目的地址转换。】

解决方法

因为如果NAT66前缀与接口地址在同一网段，NAT66前缀是不能响应对端发送的NS报文的，所以必须配置为不同网段

interface GigabitEthernet5/0

port link-mode route

ip address 66.66.66.67 255.255.255.0

nat66 prefix source 200:: 60 2408:8710:20:3500:: 60

ipv6 address 2408:8710:20:4500::1/60

此时FW1pingFW3,在FW2上可以看到NAT66的会话

```
:H3C>ping ipv6 -a 200::1  2408:8710:20:4500::2
'ing6(56 data bytes) 200::1 --> 2408:8710:20:4500::2, press CTRL+C to break
i6 bytes from 2408:8710:20:4500::2, icmp_seq=0 hlim=63 time=6.044 ms
i6 bytes from 2408:8710:20:4500::2, icmp_seq=1 hlim=63 time=2.045 ms
i6 bytes from 2408:8710:20:4500::2, icmp_seq=2 hlim=63 time=0.000 ms
i6 bytes from 2408:8710:20:4500::2, icmp_seq=3 hlim=63 time=0.000 ms
i6 bytes from 2408:8710:20:4500::2, icmp_seq=4 hlim=63 time=2.892 ms

-- Ping6 statistics for 2408:8710:20:4500::2 ---
 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
ound-trip min/avg/max/std-dev = 0.000/2.196/6.044/2.234 ms
:H3C>
```

FW2会话如下

```
[H3C]display  session  table ipv6 protocol icmpv6  verbose
Slot 0:
Total sessions found: 0
[H3C]display  session  table ipv6 protocol icmpv6  verbose
Slot 0:
Initiator:
  Source      IP/port: 200::1/42370
  Destination IP/port: 2408:8710:20:4500::2/32768
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: IPV6-ICMP(58)
  Inbound interface: GigabitEthernet7/0
  Source security zone: Trust
Responder:
  Source      IP/port: 2408:8710:20:4500::2/42370
  Destination IP/port: 2408:8710:20:3500:21C7::1/33024
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: IPV6-ICMP(58)
  Inbound interface: GigabitEthernet5/0
  Source security zone: Trust
State: ICMPV6_REPLY
Application: ICMP
Rule ID: 0
Rule name: 0
Start time: 2021-10-15 00:01:54  TTL: 28s
Initiator->Responder:            5 packets        520 bytes
Responder->Initiator:            5 packets        520 bytes

Total sessions found: 1
```