某局点SecPath F5000(V7) AFT功能不通

AFT 关萌 2022-09-30 发表

组网及说明

用户使用我司F5060防火墙作为用户出口网关设备。该用户内网使用纯IPv6网络，用户需要访问互联网IPv4网络，需要用到防火墙AFT功能。

问题描述

客户在使用我司F5060防火墙时配置了AFT功能，需要把内网IPv6网段2002::/64网段转换成IPv4网段，设备关键配置如下

```
#
aft address-group 1
 address 2.2.2.1 2.2.2.100
#
 aft prefix-nat64 2002:: 64
 aft v6tov4 source acl ipv6 number 2000 address-group 1 no-pat
#
```

配置完成后，用户通过2001::10/64地址访问2002::114.114.114.114，发现无法访问，不能ping通。

过程分析

收集会话信息确认转换状态，收集会话发现，无法收集到会话。收集结果显示信息如下。

dis session table ipv6 source-ip 2001::10 destination-ip 2002::114.114.114.114 ver

Slot 1 in chassis 1:

Total sessions found: 0

Slot 2 in chassis 1:

Total sessions found: 0

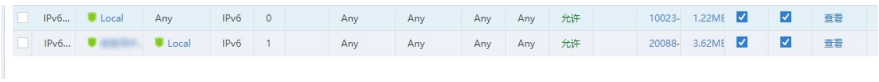
Slot 1 in chassis 2:

Total sessions found: 0

Slot 2 in chassis 2:

Total sessions found: 0

没有会话怀疑是安全策略没有放通，检查安全策略发现用户只配置了local彰的安全策略，对于防火墙本地转换的流量也需要放通源安全域到目的安全域的流量，不是放通到local的流量。



进一步检查配置，发现场前缀配的64位，但是ping 2012::114.114.114.114，导致地址匹配错误，所以需要修改为96位。

解决方法

配置如下命令后解决。

aft prefix-nat64 2002:: 96

对于NAT64功能可以配置多种IPv6地址格式，如果将IPv4地址放在末尾，需要将前缀修改成96位的，如下是相关格式具体匹配方式。