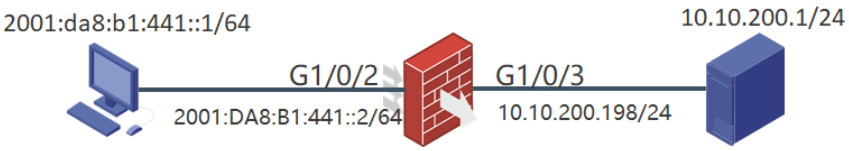
某局点IPv6客户端访问IPv4服务器业务不通

AFT 刘诚 2021-07-29 发表

组网及说明



IPv6网络客户端通过防火墙去访问Internet IPv4服务器，防火墙互联接口、客户端及服务器地址如图所示。

问题描述

这是典型的IPv6网络访问Internet IPv4的场景，按照官网配置，发现IPv6客户端ping不通Internet IPv4服务器

C:\Users\PC>ping 2012::10.10.200.1

正在 Ping 2012::10.10.200.1 具有 32 字节的数据:
请求超时。
请求超时。
请求超时。
请求超时。

2012::10.10.200.1 的 Ping 统计信息:

数据包: 已发送 = 4，已接收 = 0，丢失 = 4 (100% 丢失)
且看不到AFT IPv6和IPv4的会话：
[H3C]display aft session ipv6 verbose
Slot 1:
Total sessions found: 0
[H3C]display aft session ipv4 verbose
Slot 1:
Total sessions found: 0

过程分析

首先检查配置

（1）接口是否加入安全域，安全域是否放通 //IPv4和IPv6安全策略全放通，没问题

```
#
security-zone name Trust
 import interface GigabitEthernet1/0/3
#
security-zone name Untrust
 import interface GigabitEthernet1/0/2
#
#
security-policy ip
 rule 0 name Any→Any_0_IPv4
  action pass
  counting enable
#
security-policy ipv6
 rule 0 name Any→Any_0_IPv6
  action pass
  logging enable
  counting enable
#
```

（2）AFT功能是否配置

i） 地址组是否配置

```
#
aft address-group 0
 address 10.10.200.199 10.10.200.200
#
```

ii） IPv6 ACL是否匹配终端所属网段

```
#
acl ipv6 basic 2000
 rule 0 permit source 2001:DA8:B1:441::/64 logging counting
#
```

Iii） IPv6到IPv4的源地址动态转换策略是否配置

```
#
aft v6tov4 source acl ipv6 number 2000 address-group 0
#
```

iiii） IPv6地址前缀如何配置

```
#
 aft prefix-nat64 2012:: 96  //问题就出在此
#
```

iiiii）接口下是否开启aft

```
#
interface GigabitEthernet1/0/2
 port link-mode route
 aft enable
 ipv6 address 2001:DA8:B1:441::2/64
#
interface GigabitEthernet1/0/3
```

port link-mode route

ip address 10.10.200.198 255.255.255.0

解决方法

undo portswitch 客户端只能是64位，那相应的设备上接口地址和AFT 地址前缀都得改成64位

#

interface GigabitEthernet1/0/2

port link-mode route

undo portswitch

ipv6 address 2001:DA8:B1:441::2/64 //本来就是64位不用改

#

aft enable

#

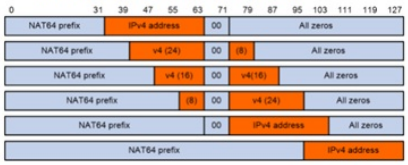
我们发现客户端、防火墙与客户端互联接口IPv6前缀都是64位，但设备配置的IPv6地址前缀是96位（标红处），于是我们把客户端、防火墙与客户端互联接口IPv6前缀都改为96位，这时候从客户端ping服务器能通，但是客户端由于运营商分配的地址限制，只能是64位，无法改为96位。

1. NAT64前缀转换

NAT64前缀是长度为32、40、48、56、64或96位的IPv6地址前缀，用来构造IPv4节点在IPv6网络中的地址，以便IPv4主机与IPv6主机通信。网络中并不存在带有NAT64前缀的IPv6地址的主机。

如图1-2所示，NAT64前缀长度不同时，地址转换方法有所不同。其中，NAT64前缀长度为32、64和96位时，IPv4地址作为一个整体添加到IPv6地址中；NAT64前缀长度为40、48和56位时，IPv4地址被拆分成两部分，分别添加到64～71位的前后。

图1-2 对应IPv4地址带有NAT64前缀的IPv6地址格式



IPv4侧发起访问时，AFT利用NAT64前缀将报文的源IPv4地址转换为IPv6地址；IPv6侧发起访问时，AFT利用NAT64前缀将报文的目的IPv6地址转换为IPv4地址。

根据nat64地址前缀转换规则：

64位前缀+0x00 + ipv4 + 0

例如填充10.10.200.1这个地址，使用64位前缀2012::/64，按上面的规则对应的v6地址为2012:0000:0000:0000:000a:0ac8:0100:0000

简写为2012::a:ac8:100: 0

使用64位前缀相对麻烦，需要自己计算对应的v6地址，无法直接填充到末尾。

测试业务的时候直接ping 2012::a:ac8:100: 0