某局点F1000防火墙nat server映射pptp vpn服务器异常的经验处理案例

NAT 孙轶宁 2020-05-31 发表

组网及说明

F1000防火墙作为出口，有两条出口链路，通过等价路由负载均衡，在某一出口做了nat server，将内网的pptp vpn服务器映射到公网。

问题描述

发现能够正常发起vpn拨号，但是ppp无法协商成功。配置如下（只放了nat server相关配置，安全域等配置省略）

```
 nat alg h323
 nat alg ils
 nat alg mgcp
 nat alg nbt
 nat alg rsh
 nat alg sccp
 nat alg sip
 nat alg sqlnet
 nat alg tftp
 nat alg xdmcp
#
interface GigabitEthernet1/0/1
 port link-mode route
 description VPN
 combo enable copper
 ip address 116.X.X.X 255.255.255.248
 ip last-hop hold
 nat outbound
 nat server protocol tcp global 116.X.X.X
1723 inside 192.168.1.252 1723 rule ServerRule_1 counting
 nat server protocol tcp global 116.X.X.X 8090 inside 192.168.1.198 80 rule ServerRule_3 counting
 nat server protocol udp global 116.X.X.X
1723 inside 192.168.1.252 1723 rule ServerRule_4 counting
 undo dhcp select server
 gateway 116.X.X.X
```

过程分析

1、检查出接口的配置，确认有配置ip last-hop hold，作用是保证来回路径一致，使回包不从另一出接口发出去。

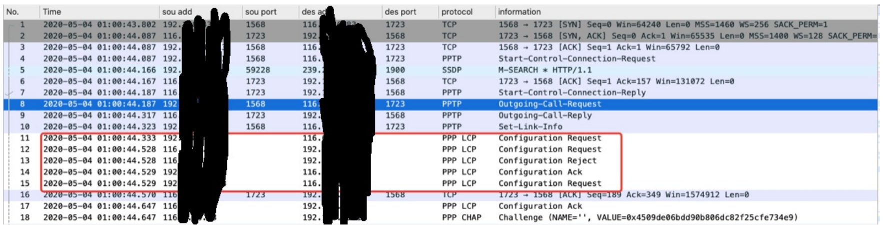
2、检查nat alg，确认nat alg pptp处于开启状态。

```
[F1000]dis nat alg
NAT ALG:
 DNS : Enabled
 FTP : Enabled
 H323 : Enabled
 ICMP-ERROR : Enabled
 ILS : Enabled
 MGCP : Enabled
 NBT : Enabled
 PPTP : Enabled
 RTSP : Enabled
 RSH : Enabled
 SCCP : Enabled
 SIP : Enabled
 SQLNET : Enabled
 TFTP : Enabled
 XDMCP : Enabled
```

3、尝试配置port-mapping application pptp port 1723，问题依旧。

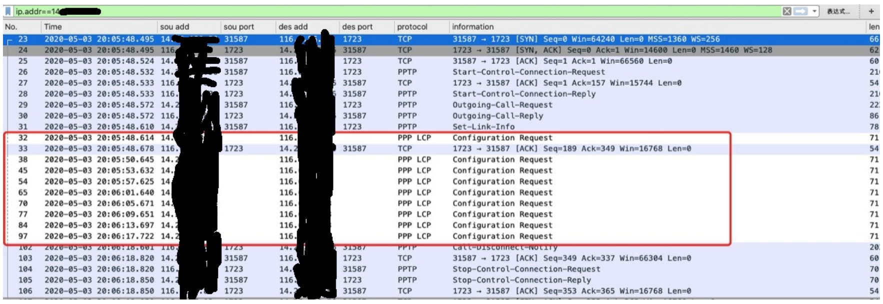
4、对比正常和非正常的抓包文件，发现正常报文交互能够看到ppp报文来回协商，但是异常报文只能看到客户端发给服务器的ppp报文，没有看到服务器发给客户端的ppp报文

正常



No.	Time	sou add	sou port	des add	des port	protocol	information
1	2020-05-04 01:00:43.802	192.[redacted]	1568	116.[redacted]	1723	TCP	1568 → 1723 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
2	2020-05-04 01:00:44.087	116.[redacted]	1723	192.[redacted]	1568	TCP	1723 → 1568 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1400 WS=128 SACK_PERM=
3	2020-05-04 01:00:44.087	192.[redacted]	1568	116.[redacted]	1723	TCP	1568 → 1723 [ACK] Seq=1 Ack=1 Win=65792 Len=0
4	2020-05-04 01:00:44.087	192.[redacted]	1568	116.[redacted]	1723	PPTP	Start-Control-Connection-Request
5	2020-05-04 01:00:44.166	192.[redacted]	59228	239.[redacted]	1900	SSDP	M-SEARCH * HTTP/1.1
6	2020-05-04 01:00:44.167	116[redacted]	1723	192.[redacted]	1568	TCP	1723 → 1568 [ACK] Seq=1 Ack=157 Win=131072 Len=0
7	2020-05-04 01:00:44.187	116[redacted]	1723	192.[redacted]	1568	PPTP	Start-Control-Connection-Reply
8	2020-05-04 01:00:44.187	192[redacted]	1568	116.[redacted]	1723	PPTP	Outgoing-Call-Request
9	2020-05-04 01:00:44.317	116[redacted]	1723	192.[redacted]	1568	PPTP	Outgoing-Call-Reply
10	2020-05-04 01:00:44.323	192[redacted]	1568	116.[redacted]	1723	PPTP	Set-Link-Info
11	2020-05-04 01:00:44.333	192[redacted]		116.[redacted]		PPP LCP	Configuration Request
12	2020-05-04 01:00:44.528	116[redacted]		192.[redacted]		PPP LCP	Configuration Request
13	2020-05-04 01:00:44.528	116[redacted]		192.[redacted]		PPP LCP	Configuration Reject
14	2020-05-04 01:00:44.529	192[redacted]		116.[redacted]		PPP LCP	Configuration Ack
15	2020-05-04 01:00:44.529	192[redacted]		116.[redacted]		PPP LCP	Configuration Request
16	2020-05-04 01:00:44.570	116[redacted]	1723	192.[redacted]	1568	TCP	1723 → 1568 [ACK] Seq=189 Ack=349 Win=1574912 Len=0
17	2020-05-04 01:00:44.647	116[redacted]		192.[redacted]		PPP LCP	Configuration Ack
18	2020-05-04 01:00:44.647	116[redacted]		192.[redacted]		PPP CHAP	Challenge (NAME='', VALUE=0x4509de06bdd90b806dc82f25cfe734e9)

异常



ip.addr==14[redacted]

No.	Time	sou add	sou port	des add	des port	protocol	information	len
23	2020-05-03 20:05:48.495	14.[redacted]	31587	116.[redacted]	1723	TCP	31587 → 1723 [SYN] Seq=0 Win=64240 Len=0 MSS=1360 WS=256	66
24	2020-05-03 20:05:48.495	116.[redacted]	1723	14.[redacted]	31587	TCP	1723 → 31587 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 WS=128	62
25	2020-05-03 20:05:48.524	14.[redacted]	31587	116.[redacted]	1723	TCP	31587 → 1723 [ACK] Seq=1 Ack=1 Win=66560 Len=0	60
26	2020-05-03 20:05:48.532	14.[redacted]	31587	116.[redacted]	1723	PPTP	Start-Control-Connection-Request	21
27	2020-05-03 20:05:48.533	116.[redacted]	1723	14.[redacted]	31587	TCP	1723 → 31587 [ACK] Seq=1 Ack=157 Win=15744 Len=0	54
28	2020-05-03 20:05:48.533	116.[redacted]	1723	14.[redacted]	31587	PPTP	Start-Control-Connection-Reply	21
29	2020-05-03 20:05:48.572	14.2[redacted]	31587	116.[redacted]	1723	PPTP	Outgoing-Call-Request	22
30	2020-05-03 20:05:48.572	116.[redacted]	1723	14.[redacted]	31587	PPTP	Outgoing-Call-Reply	86
31	2020-05-03 20:05:48.610	14.[redacted]	31587	116.[redacted]	1723	PPTP	Set-Link-Info	78
32	2020-05-03 20:05:48.614	14.[redacted]		116.[redacted]		PPP LCP	Configuration Request	71
33	2020-05-03 20:05:48.678	116.[redacted]	1723	14.2[redacted]	31587	TCP	1723 → 31587 [ACK] Seq=189 Ack=349 Win=16768 Len=0	54
38	2020-05-03 20:05:50.645	14.2[redacted]		116.[redacted]		PPP LCP	Configuration Request	71
45	2020-05-03 20:05:53.632	14.[redacted]		116.[redacted]		PPP LCP	Configuration Request	71
54	2020-05-03 20:05:57.625	14[redacted]		116.[redacted]		PPP LCP	Configuration Request	71
65	2020-05-03 20:06:01.640	14[redacted]		116.[redacted]		PPP LCP	Configuration Request	71
70	2020-05-03 20:06:05.671	14.[redacted]		116.[redacted]		PPP LCP	Configuration Request	71
77	2020-05-03 20:06:09.651	14.[redacted]		116.[redacted]		PPP LCP	Configuration Request	71
84	2020-05-03 20:06:13.697	14.2[redacted]		116.[redacted]		PPP LCP	Configuration Request	71
97	2020-05-03 20:06:17.722	14.2[redacted]		116.[redacted]		PPP LCP	Configuration Request	71
102	2020-05-03 20:06:18.601	116.[redacted]	1723	14.2[redacted]	31587	PPTP	Call-Disconnect-Notify	20
103	2020-05-03 20:06:18.820	14.2[redacted]	31587	116.[redacted]	1723	TCP	31587 → 1723 [ACK] Seq=349 Ack=337 Win=66304 Len=0	60
104	2020-05-03 20:06:18.820	116.[redacted]	1723	14.[redacted]	31587	PPTP	Stop-Control-Connection-Request	70
105	2020-05-03 20:06:18.850	14.2[redacted]	31587	116.[redacted]	1723	PPTP	Stop-Control-Connection-Reply	70
106	2020-05-03 20:06:18.850	116.[redacted]	1723	14.2[redacted]	31587	TCP	1723 → 31587 [ACK] Seq=353 Ack=365 Win=16768 Len=0	54

5、在防火墙上开启debug后，发现服务器端发送的configuration request，是从Dialer0口出去，不是从外网口（GigabitEthernet1/0/1） 发出去

```
*May 5 20:24:23:236 2020 fw IPFW/7/IPFW_PACKET:
 Sending, interface = Dialer0
```

6、通过上述现象判断，报文在交互过程中数据五元组应该发生过改变，导致回包的时候匹配不到ip last-hop hold生成的表项，从错误的接口发了出去。

解决方法

配置策略路由，使服务器的报文固定从公网口出去。