

知 防火墙映射FT服务，外网访问不成功

ALG 张帅杰 2022-03-23 发表

组网及说明

防火墙是出口设备，服务器在内网，

问题描述

在防火墙上将FTP端口映射出去，外网客户端采用被动模式访问FTP不成功。

过程分析

1. ftp的alg默认开启
2. 查看配置无问题
3. 通过在终端的抓包信息看：终端发送的访问数据端口61325的报文被tcp重传，导致失败。

34 0.442778	TCP	153.17921 → 8954 [FIN, ACK] Seq=2756 Ack=604 Min=1104 Len=0 Tsvail=2104321278 TSecr=1116680810
35 0.443215	TCP	70.84481 → 61325 [SYN] Seq=0 Win=7800 Len=0 MSS=1460 SACK_PERM=1 Tsvail=116603040 TSecr=0 WS=128
36 0.442792	TCP	70.8960 → 37921 [ACK] Seq=681 Ack=2275 Win=1184 Len=0 Tsvail=1116683889 TSecr=2104321270
37 0.445256	TCP	70 [TCP Retransmission] 64461 → 61325 [SYN] Seq=0 Win=7800 Len=0 MSS=1460 SACK_PERM=1 Tsvail=1116680802 TSecr=0 WS=128
38 0.445793	TCP	70 [TCP Retransmission] 64461 → 61325 [SYN] Seq=0 Win=7800 Len=0 MSS=1460 SACK_PERM=1 Tsvail=1116680850 TSecr=0 WS=128
39 7.451973	TCP	111.8954 → 37921 [PSH, ACK] Seq=681 Ack=2275 Win=1184 Len=0 Tsvail=1116610864 TSecr=2104321270
40 7.452755	TCP	70.8954 → 37921 [FIN, ACK] Seq=735 Ack=2275 Min=1184 Len=0 Tsvail=1116610864 TSecr=2104321270
41 7.521741	TCP	70 [TCP Retransmission] 6254 → 37921 [FIN, ACK] Seq=735 Ack=2275 Win=1184 Len=0 Tsvail=1116610810 TSecr=2104321270
42 7.523227	TCP	70 [TCP Retransmission] 6254 → 37921 [FIN, ACK] Seq=735 Ack=2275 Win=1184 Len=0 Tsvail=1116610864 TSecr=2104321270
43 7.526119	TCP	86 [TCP Dup. ACK] 42811 → 8954 [ACK] Seq=2275 Ack=736 Min=1104 Len=0 Tsvail=2104321282 TSecr=1116610810 S1L=735 S1E=736
44 29.483812	TCP	70.8960 → 37921 [SYN] Seq=0 Win=7800 Len=0 MSS=1460 SACK_PERM=1 Tsvail=1116612090 TSecr=0 WS=128
45 29.515439	TCP	82 37921 → 8954 [SYN, ACK] Seq=0 Ack=0 Min=2008 Len=0 MSS=1460 SACK_PERM=1 Tsvail=2104350342 TSecr=1116632098 WS=128
46 29.515787	TCP	70.8960 → 37921 [ACK] Seq=1 Ack=1 Min=7424 Len=0 Tsvail=1116632122 TSecr=2104350342

4. 通过debug nat pack查看地址已经转化，通过debug ip pack查看终端发送的数据端口的报文提示命中黑洞路由给丢弃掉了，pktid跟抓包里边重传报文的pktid一致。说明是此原因导致tcp出现重传进而导致FTP访问不成功。

```
*Mar 16 16:36:52:978 2022 [Redacted] IPFW/7/IPFW_P1
Discarding, interface = [Redacted]
version = 4, headlen = 20, tos = 0
pktlen = 60, pktid = 56717, offset = 0, ttl = 60, protocol = 6
checksum = 38806, s = [Redacted], d = [Redacted]
channelID = 0, vpn-InstanceIn = 0, vpn-InstanceOut = 0.
prompt: FIB BLACKHOLE.
Payload: TCP
source port = 44481, destination port = 61325
```

5. 通过抓包看FTP终端跟服务器之间的交互是通过TLS加密的，而加密数据防火墙是识别不了里边的载荷报文，也无法识别到终端跟服务器之间协商的数据端口是多少，从而导致ALG功能不生效，终端发起的访问数据端口的报文被丢弃。

解决方法

明确了问题后，解决方法有如下两种：

1. 取消客户端到服务器之间的加密措施，让防火墙可以正常识别FTP里边的数据传输端口。（一般来说现场是取消不掉的）
2. 在防火墙上新增一条nat server，端口号是协商出来的数据端口号，一般来说服务器端是可以指定数据端口协商的范围，在防火墙上将此范围内的端口全部映射出去也可以解决。

