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

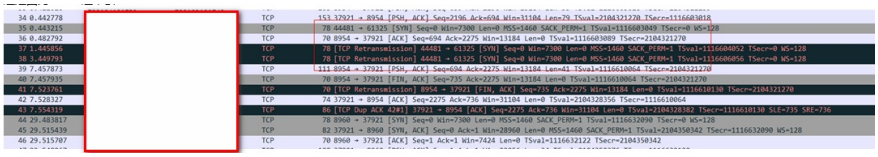
在防火墙上将FTP端口映射出去，外网客户端采用被动模式访问FTP不成功。

过程分析

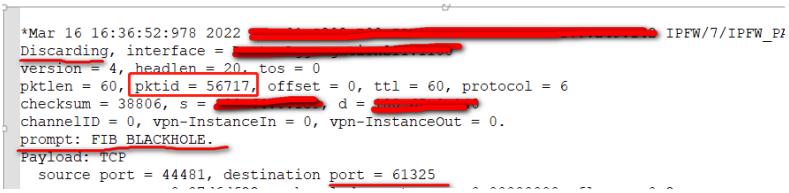
1. ftp的alg默认开启

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。



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。



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。