

知 SecPath F1080(V7) 安全策略不生效问题案例分析

域间策略/安全域

刘宏宇 2019-10-29 发表

问题描述

现网中SecPath F1080(V7)透明模式部署在两套核心交换机网络（用户网络放在untrust和服务器网络在trust）之间进行安全策略控制，只对员工某些服务端口的访问，但是测试发现未放通对应445端口服务，但是可以访问。

解决方法

一、设备配置排查

二、怀疑访问的报文源端口正好是53端口被放通，但是查看会话以及debug ip packet acl以及debug security-policy packet ip acl信息

```
*Dec 3 15:10:30:477 2018 YDZC-YZ-O-S-PROD-FWL-1/2 FILTER/7/PACKET: -Context=1; The packet is permitted. Src-ZOne=Untrust, Dst-ZOne=Trust;If-In=Bridge-Aggregation1(135), If-Out=Bridge-Aggregation2(136), VLAN-In=2801, VLAN-Out=2801; Packet Info:Src-IP=172.17.19.131, Dst-IP=172.19.64.43, VPN-Instance=,Src-Port=64596, Dst-Port=445, Protocol=TCP(6), Application=microsoft-ds(85), SecurityPolicy=Untrust-Trust-1, Rule-ID=1.
```

测试源地址：172.17.19.131

目的地址：172.19.64.43 端口445

源端口不是53，但是debug显示就是被对应的rule1策略Untrust-Trust-1放行了。

三、

不管是自定义服务组还是预定义服务组，服务组的源和目的是与的关系，

如果存在服务对象组嵌套的情况，安全策略（默认加速）和对象策略开启加速的情况下，会将所有的源端口和目的端口进行或操作，现场是这个原因导致的；

如现场的ssh /telnet等都是目的端口固定，源端口是0到65535，而dns-1这个是源端口是53，目的端口是0到65535，开启加速之后会变成源目的端口都是0到65535，导致全通。

【解决方法】

规避方法：源端口变化的和目的端口变化的服务对象组不要放在同一个rule里面。后续合入版本解决