

# 知 SecPath F1090(V7) 策略匹配异常，同时匹配两条rule

域间策略/安全域 陈美静 2024-09-27 发表

## 问题描述

会话方向：10.x.x.122访问10.x.x.57从Yidong安全域进防火墙，在JiaXing安全域内G1/0/29口nat出去。

同源目IP地址的会话存在同时匹配rule 22和rule 3两条安全策略的情况。

## 过程分析

1、查看会话，发现除端口外其余全部一致：

```
<DX_SYB_JX_FW01_F1090>display session table ipv4 source-ip 10. .122 destination-ip 10. .57 verbose
Slot 1:
Initiator:
Source IP/port: 10. .122/42303
Destination IP/port: 10.2 .57/53
DS-Lite tunnel peer: -
VPN instance/VLAN ID/Inline ID: -/-/
Protocol: UDP(17)
Inbound interface: Route-Aggregation1
Source security zone: Yidong
Responder:
Source IP/port: 10. .57/53
Destination IP/port: 10. .15/6743
DS-Lite tunnel peer: -
VPN instance/VLAN ID/Inline ID: -/-/
Protocol: UDP(17)
Inbound interface: GigabitEthernet1/0/29
Source security zone: JiaXing
State: UDP_OPEN
Application: DNS
Rule ID: 22
Rule name: ??-20240821
Start time: 2024-08-22 10:52:09 TTL: 15s
Initiator->Responder: 1 packets 59 bytes
Responder->Initiator: 0 packets 0 bytes

Initiator:
Source IP/port: 10. .122/47350
Destination IP/port: 10.2 .57/53
DS-Lite tunnel peer: -
VPN instance/VLAN ID/Inline ID: -/-/
Protocol: UDP(17)
Inbound interface: Route-Aggregation1
Source security zone: Yidong
Responder:
Source IP/port: 10. .57/53
Destination IP/port: 10. .15/7859
DS-Lite tunnel peer: -
VPN instance/VLAN ID/Inline ID: -/-/
Protocol: UDP(17)
Inbound interface: GigabitEthernet1/0/29
Source security zone: JiaXing
State: UDP_READY
Application: DNS
Rule ID: 3
Rule name: Local
```

2、无特殊配置，策略未指定匹配端口；

3、一般从上往下匹配，一旦匹配其余规则不再继续进行，但现场在两个规则中不断匹配：

发起方VPN/...	接收安全域	发起方地址...	发起方协议	应用	响应方源IP	响应方目的IP	发送安全域	响应方到...	主备状态	状态	安全策略
VPN:公网		1	UDP	DNS	10.2...	2...	...	1	主	正常	Local
VPN:公网		1	UDP	DNS	...	...	...	0	主	正常	??-20240821

local-any	Local	Any	IPv4	15	Any	Any	Any	Any	Any	Any	Any	77605	6.52MB
any-local	Any	Local	IPv4	14	Any	Any	Any	Any	Any	Any	Any	99635	10.19MB
20240821	Any	Any	IPv4	22	Any	Any	Any	Any	Any	Any	Any	5.69*10	10.09GB
20240821	Any	Any	IPv4	23	Any	Any	Any	Any	Any	Any	Any	65069	8.14MB
f-1	Any	Any	IPv4	21	Any	Any	Any	Any	Any	Any	Any	779	23.70KB
20240821	Any	Any	IPv4	9	Any	Any	Any	Any	Any	Any	Any	0	0.00B
20240821	Any	Any	IPv4	8	Any	Any	Any	Any	Any	Any	Any	0	0.00B
20240821	Any	Any	IPv4	0	Any	Any	Any	Any	Any	Any	Any	0	0.00B
20240821	Any	Any	IPv4	1	Any	Any	Any	Any	Any	Any	Any	0	0.00B
Local	Local	Local	IPv4	3	Any	Any	Any	Any	Any	Any	Any	8897	757.23KB
20240821	Any	Any	IPv4	4	Any	Any	Any	Any	Any	Any	Any	0	0.00B

4、怀疑之前匹配rule3的会话没老化的情况下，改了防火墙的策略配置，在前面添加了rule22，这样即使有新的策略，就还会走rule3。把匹配rule3的这条会话清一下。dis session table看设备上确认没有这个会话了，再重新触发下流量尝试故障依旧。

#### 解决方法

从抓包的信息也能看到，有一些icmp差错报文，这种报文因为版本bug所以匹配错了，正常报文的匹配则没有问题。因为差错报文本就不属于正常业务报文，所以即使没有匹配到正确的安全策略，也不影响业务。

目前已经确认是有个版本已知问题导致的，匹配顺序错误，60P24及之后版本解决。可以直接升级ftp的最新版。