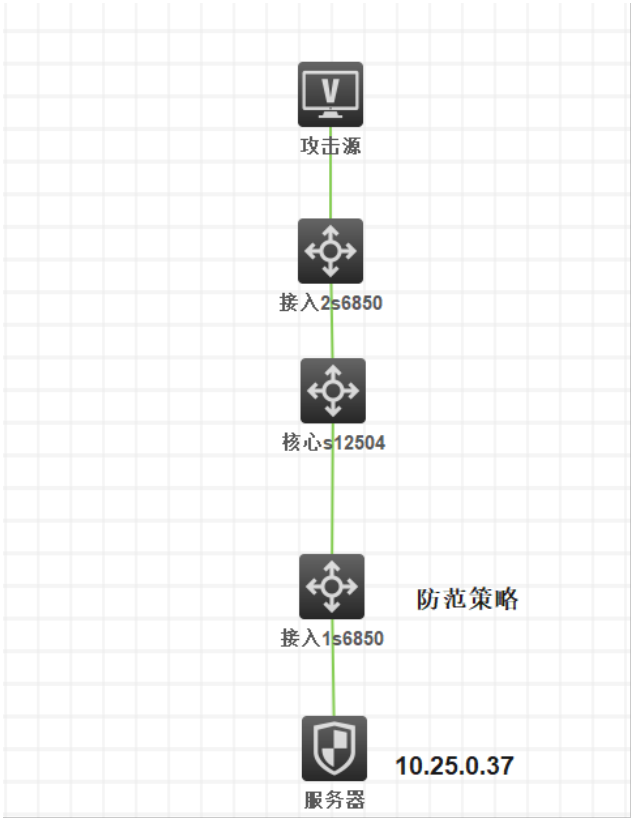
S6850攻击防范功能不生效问题

攻击检测与防范 倪民 2022-12-09 发表

组网及说明



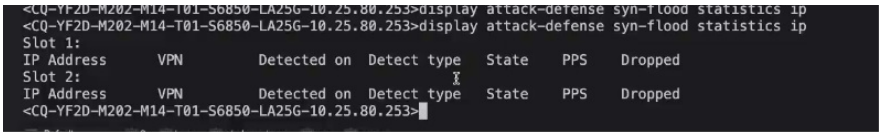
问题描述

组网如上，客户在中间的接入S6850上配置了如下攻击防范策略，检测sys flood攻击。

```
#
attack-defense policy ceping
 syn-flood action logging
 syn-flood threshold 100
 syn-flood detect ip 10.25.0.37 threshold 100 action logging
 syn-flood detect ip 10.25.80.253 threshold 100 action logging
 signature detect tcp-all-flags action logging
 signature detect tcp-syn-fin action logging
#
```

过程分析

从攻击源发起sys攻击，在S6850上查看发现，该防范策略没有任何信息，未生效。



解决方法

对于attack-defense这个功能，只能对攻击交换机自身的报文有效，对于转发的流量无法生效。
一般来说这个功能主要是为了防止攻击本机的流量。