S7506E 设备报syn-flood攻击日志问题说明

攻击防范及检测 秦婷婷 2018-02-25 发表

客户一台S7506E日志中频繁报syn-flood攻击，但设备并未配置攻击检测与防御功能，咨询报日志的原因，及如何解决：

%Feb 20 19:12:11:006 2018 H3C SOCKET/6/TCP_SYNFLOOD: -Chassis=2-Slot=4; atckType(1016)=(05)SYN-flood; srcIPAddr(1017)=10.11.66.65; destIPAddr(1019)=10.11.66.4; atckSpeed(1047)=300; atckTime_cn(1048)=2018022122542

1、TCP攻击检测在设备上分两个模块，安全业务模块和TCP模块，两者独立；攻击检测与防御做在安全业务模块，现场未配置；TCP模块同时也会对报文进行检测，只要每秒超过300个就会打印TCP_SYNFLOOD，只做检测打印日志，不做其它动作，默认开启不能关闭或调整；

2、通过日志找到攻击源，避免终端发送大量TCP SYN报文解决。