T9000设备DPI检测不到攻击日志

IPS防攻击 杨凌轩 2020-02-28 发表

组网及说明

T9000----PC

问题描述

现场T9000直连电脑进行攻击测试，发现模拟攻击后在web界面没有威胁日志显示

过程分析

检查安全策略是全部放通，在里面也调用了IPS策略，模拟攻击时，安全策略有匹配增长
确认特征库是最新，license也在有效期内
dis session table 能看到相关会话
debug security-policy能看到报文是permit了的
但是在威胁日志里确实是空白

解决方法

检查相关接口配置发现，测试用的是加了VPN实例的management管理口
interface GigabitEthernet1/0/23
port link-mode route
ip binding vpn-instance management
ip address x.x.x.x 255.255.255.0
再次查看软件版本，发现有如下说明
DPI相关业务：
不支持跨VPN进行应用识别。
怀疑问题产生与该限制有关
重新测试另一个口，进行同实例里测试能够正常显示日志