

知 U200-CX系列UTM 开启深度安全检测中的IPS和病毒库防护后，正常业务不通了怎么办？

IPS防攻击 张旭 2018-12-27 发表

问题描述

U200-CX系列UTM 开启深度安全检测中的IPS和病毒库防护后，正常业务不通了怎么办？

解决方法

- 1.访问一次业务，到IPS或病毒库日志中，根据访问业务时间和ip信息确认是否产生了对应的日志。
- 2.访问业务时，收集客户端侧和服务器侧抓包。
- 3.将日志、抓包及组网信息反馈给H3C工程师处理。
- 4.如果误识别只发生在个别终端的，可以考虑将这些终端ip地址添加到例外地址。