IPS用自带的packet-trace抓包方法

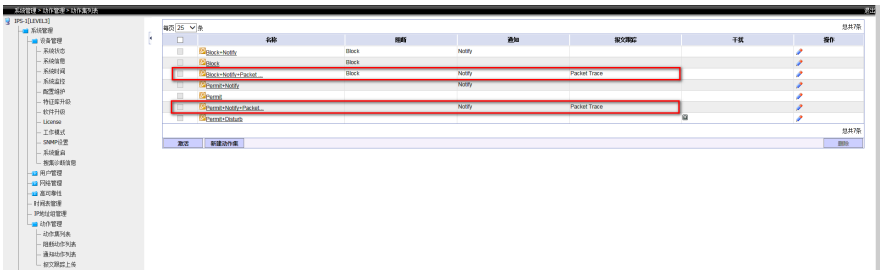
IPS防攻击　易予晴　2016-01-27 发表

IPS里自带抓包功能，如果怀疑IPS误识别，可以通过packet-trace抓个包跟研发确认。

不涉及。

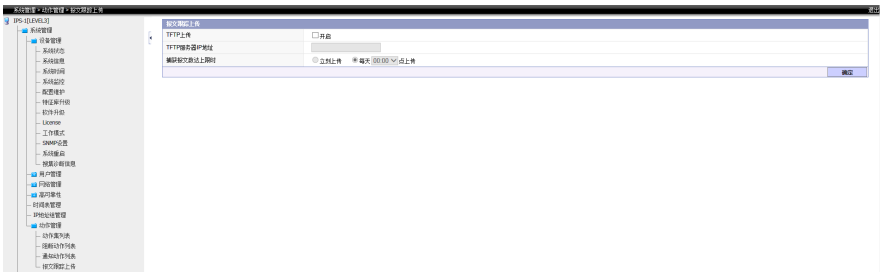
无。

在动作集里查看带Packet Trace的动作集名称，Block和Permit对应都有一个。



然后在规则管理里把规则的动作改成带Packet Trace的，并在策略管理里激活策略。

开一个TFTP服务器，开启报文跟踪上传，选择立刻上传。抓包会自动上传到服务器上。



不设置报文跟踪上传就使用手动下载Packet Trace抓包。此时日志里Packet Trace列表里会出现抓包链接，可直接点击下载。

规则里修改动作后一定要对策略进行激活。