



IPS板卡规则动作分级和全阻断的差别

IPS防攻击

毫先生

2017-11-20 发表

组网及说明

设备是S75E+IPS板卡，一台机框，5块板卡。

问题描述

IPS板卡应用默认IPS策略，规则动作中默认是分级的。

同一台设备中，有的板卡的规则动作是分级的，有的板卡的动作是全阻断。

这种配置也没有影响到业。

怎么衡量分级的好，还是全阻断的好，全阻断只可能影响到业务的点一般有哪些？

曾经遇到http弱口令检测（特征库中分级动作是允许+记录日志），好像改成阻断会拦截弱口令登录的报文，实践没做过。

求分享

解决方法

建议用默认IPS策略，里面推荐的动作都是经验值

答案来自于 悠哈悠哈