

知 D032分支防火墙web界面命中策略分析无命中策略显示的原因

域间策略/安全域

刘宏宇

2019-10-29 发表

问题描述

web界面安全策略-命中策略分析仅显示未命中的策略，没有命中的显示

解决方法

该部分只显示未命中。

安全策略命中分析功能可以分析出指定时间段内的安全策略是否被命中过，并将未命中的安全策略按照从高到低的优先级顺序进行呈现，以帮助管理员对设备上的安全策略进行深度分析和处理。

只要符合如下两种情况中的任意一种，则认为策略未命中：

- 1、流量不符合安全策略的过滤条件。
- 2、安全策略之间存在深度冗余，例如IP地址和用户的冗余、应用和服务的冗余等。这样会由于高优先级的策略被命中，而导致低优先级的策略未命中。

不管是第一种还是第二种，都是实现未命中的，第一种是指流量和策略条件不符合，第二种是指虽然符合，但是命中了前面的rule，后面的也是没有命中，比如rule 1 和rule 2，1在前，2在后，他们都能匹配上流量，这时候因为流量已经命中了1，就不会再命中2

即策略rule优先级的问题。

此时就会用到冗余分析，通过冗余分析可以找到后面的优先级低的rule 2，然后进行优化。