

知 关于IPS/ACG/UTM设备，我们在一个段上应用2个策略，并且这个2个策略的匹配范围完全一致，但是里面的规则完全不一样，那么第二条策略是否有可能生效？

域间策略/安全域 彭旭 2019-10-29 发表

#### 问题描述

关于IPS/ACG/UTM设备，我们在一个段上应用2个策略，并且这个2个策略的匹配范围完全一致，但是里面的规则完全不一样，那么第二条策略是否有可能生效？

#### 解决方法

不可能生效，一个流量过来会先匹配段，然后匹配策略，最后匹配规则，一个流只能匹配一个段一个策略一个规则。当一个流匹配了段，却没有匹配到策略时（比如说段上尚未新建任何策略），那么设备对这个流采用默认的动作permit；当一个流匹配了策略，却没有匹配到规则时（比如策略中没有任何规则，连默认的Default规则也是禁止的），那么设备对这个流采用默认的动作permit；

#### 举例：

ACG设备匹配策略的时，如果匹配的条件相同，则只会顺序匹配（从上到下），一个流只会匹配一条策略（这条策略中如果没有规则，则默认动作为permit），此时第二个策略是不会生效的。

一个段上多个策略匹配举例：

第一个策略只配Default规则permit+notify

第二个策略只配Default规则block+notify

可以ping通，有日志

第一个策略只配Default规则block+notify

第二个策略只配Default规则permit+notify

不可以ping通，有日志

第一个策略只配Default规则禁止

第二个策略只配Default规则Block+notify

可以ping通，没有日志