

知 SecBlade LB ACL策略的匹配原则

域间策略/安全域 刘宏宇 2019-11-12 发表

问题描述

SecBlade LB ACL策略的匹配原则

解决方法

ACL策略优先级高于调度算法，当一个新的连接过来如果匹配了ACL策略，则根据策略对应的实服务转发而不再进行后续调度。

实服务组									
实服务									
虚服务									
统计信息									
实服务名 查询 高级查询									
☐	实服务名	实服务IP地址	端口号	状态	权值	最大连接数限制	实服务组	ACL	健康性检测方法
☐	Server1	192.168.1.1	80	●	110	0	Web_Servers	3000	与实服务组一致
☐	Server2	192.168.1.2	80	●	100	0	Web_Servers	3001	与实服务组一致

```
acl number 3000
rule 0 deny ip source 10.0.0.10 0
rule 5 permit ip source 10.0.0.0 0.0.0.255
acl number 3001
rule 0 deny ip source 10.0.0.10 0
rule 5 permit ip source 10.0.1.0 0.0.0.255
```

F3211之前的版本，ACL中的deny是跳出ACL策略匹配，继续后面的调度算法；从F3211版本开始，ACL中deny是跳出当前ACL，继续下一条ACL匹配。所以如果要排除某个IP，需要在所有ACL里面都排除。

如果会话表项已经生产，新添加到实服务的ACL策略可能暂时不生效，需要清除会话。