WAF中怎么样只拒绝一个URL

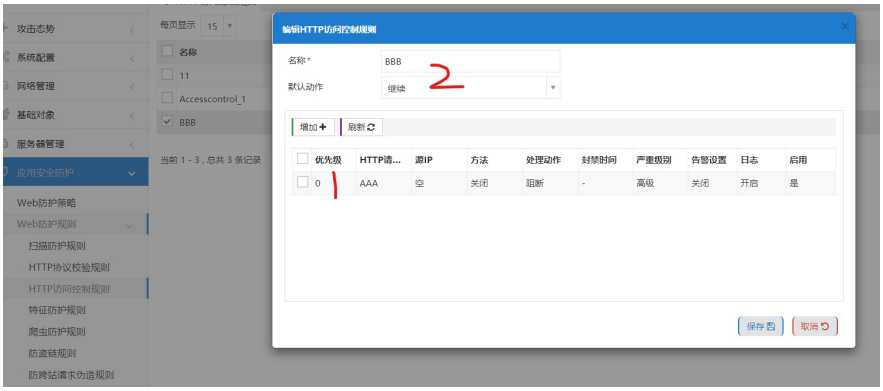
WAF 孔梦龙 2021-03-19 发表

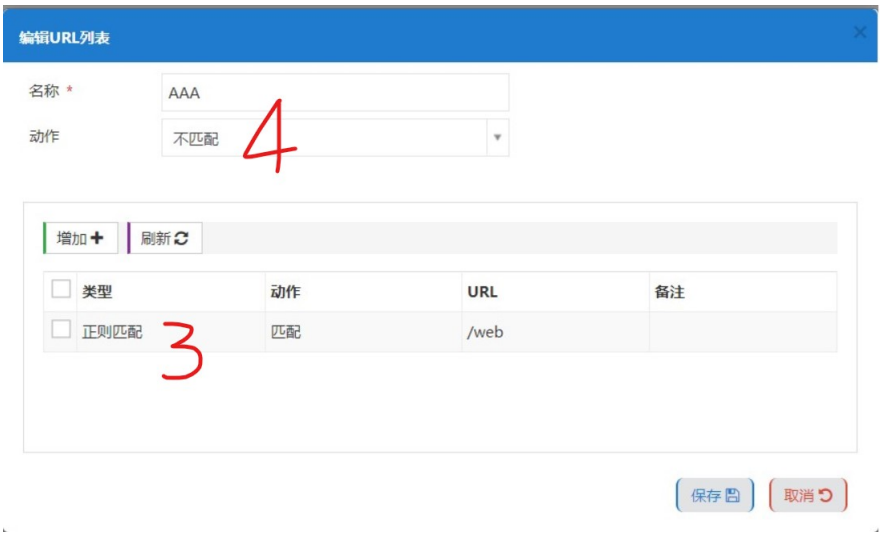
问题描述

现场想只拒绝一个URL或者一类正则表达式的URL

解决方法

配置：





然后这个http的规则被某一个服务器调用

解释：

例如1.1.1.1/web，此时可以分两层看

第一层：

URL到了WAF上以后，先被HTTP的访问控制规则检查，假设名字是AAA，此时的AAA中分为内层1和外层2；

此时1.1.1.1/web去匹配AAA，如果要是匹配上，因为AAA的动作是阻断，此时就是阻断了，如果匹配不上AAA，就会匹配外层2，外层2的动作是继续，此时流量就放行了，如果此时外层2的动作也是阻断，那就是没有匹配AAA，此时外层2也会阻断了。

第二层：

接上面，如何判定流量有没有匹配AAA，此时看图2也分为内层3和外层4，流量1.1.1.1/web也是先匹配内层；

内层的规则是：正则匹配+匹配+/web，此时1.1.1.1/web可以匹配上内层3，也就相当于匹配上了AAA，也就不再检查外层4了

如果1.1.1.1/web没有匹配上内层3，此时就会去匹外层4，如果匹配上外层4，也算是匹配上了AAA（1.1.1.1/web不管是匹配3还是4，就算匹配上），

因为上面举的例子，可以匹配3，就不会匹配4。所以整个流量就算匹配上了AAA。

上面的例子就相当于rule中的规则，rule有规则，但是rule也有默认规则，匹配不上rule内容的，默认的动作是放过还是阻断。

按上面的例子，此时流量1.1.1.1/portal上WAF

第一步：匹配3，明显不能匹配

第二步：外层4的动作是不匹配（默认动作），此时1.1.1.1/portal发现4是不匹配，那就直接放过

第三步：3和4都没匹配上，就匹配不上AAA

第四步：显然也就匹配不上1

第五步：外层2的动作是继续，所以WAF直接放过该流量

按以上的逻辑设计，可以在3和4上实现匹配和不匹配的多种组合，实现不同的功能。