iptables详解（14）：iptables小结之常用套路

朱双印
2年前更新

不知不觉，已经总结了13篇IPTABLES文章，这些文章中有一些需要注意的地方。

此处，我们对前文中的一些注意点进行总结，我们可以理解为对”常用套路”的总结。

记住这些套路，能让我们事半功倍。

阅读这篇文章之前，请确定你已经阅读了之前的文章，否则你有可能会不理解为什么要这样做。

1、规则的顺序非常重要。

如果报文已经被前面的规则匹配到，IPTABLES则会对报文执行对应的动作，通常是ACCEPT或者REJECT，报文被放行或拒绝以后，即使后面的规则也能匹配到刚才放行或拒绝的报文，也没有机会再对报文执行相应的动作了（前面规则的动作为LOG时除外），所以，针对相同服务的规则，更严格的规则应该放在前面。

2、当规则中有多个匹配条件时，条件之间默认存在”与”的关系。

如果一条规则中包含了多个匹配条件，那么报文必须同时满足这个规则中的所有匹配条件，报文才能被这条规则匹配到。

3、在不考虑1的情况下，应该将更容易被匹配到的规则放置在前面。

比如，你写了两条规则，一条针对sshd服务，一条针对web服务。

假设，一天之内，有20000个请求访问web服务，有200个请求访问sshd服务，

那么，应该将针对web服务的规则放在前面，针对sshd的规则放在后面，因为访问web服务的请求频率更高。

如果将sshd的规则放在前面，当报文是访问web服务时，sshd的规则也要白白的验证一遍，由于访问web服务的频率更高，白白耗费的资源就更多。

如果web服务的规则放在前面，由于访问web服务的频率更高，所以无用功会比较少。

换句话说就是，在没有顺序要求的情况下，不同类别的规则，被匹配次数多的、匹配频率高的规则应该放在前面。

4、当IPTABLES所在主机作为网络防火 墙时，在配置规则时，应着重考虑方向性，双向都要考虑，从外到内，从内到外。

5、在配置IPTABLES白名单时，往往会将链的默认策略设置为ACCEPT，通过在链的最后设置REJECT规则实现白名单机制，而不是将链的默认策略设置为DROP，如果将链的默认策略设置为DROP，当链中的规则被清空时，管理员的请求也将会被DROP掉。

好了，套路就总结到这里，希望能够对你有所帮助。

THE END