链滴

CentOS下iptables配置 - 只开放特定端口供访问，填坑

作者：wangsch

原文链接：https://ld246.com/article/1458735864061

来源网站：链滴

<h1 style="text-align: center;">CentOS下iptables配置 - 只开放特定端口供访问</h1>
<h2>iptables介绍</h2>
iptables是Linux中，尤其是红帽系列（RHEL、CentOS、Fedora）中常用的防火墙软件，工作TCP/IP网络模型的网络层之上，可以基于IP、端口等做到网络通信的控制，如：防止某些ip访问本服器，禁止本机某些端口被访问等。iptables工作在内核中，全称是netfilter/iptables，其实不光是为火墙使用，还有另外的nat和mangle功能，分别作为代理nat代理服务和网络整流工具。这两个功能包括iptables基本原理不在这篇文章的讨论范围。

<h2>一、需求</h2>
机器在外网，为了机器安全性和规范性，不希望暴露太多的端口（比如：nginx和tomcat在同台器上，不希望tomcat的8080端口被直接暴露，而是希望请求都先通过nginx再转发给tomcat）。所，只开放特定的几个端口，如最重要的22和80端口，其他的端口访问都拒绝。

<h2>二、问题</h2>
我的配置是这样的

首先，开启80、22和21端口（分别为：nginx、ssh、ftp）
iptables -A INPUT -p tcp -m tcp --dport 80 -j ACCEPT
iptables -A INPUT -p tcp -m cp --dport 22 -j ACCEPT
iptables-A INPUT -p tcp -m tcp --dport 21 -j ACCEPT
其他的都丢弃
iptables -P INPUT DROP
然后，我的nginx和ftp就不能访问了

<h2>三、解决</h2>
加上下面这两条就可以了
iptables -I INPUT -i lo -j ACCEPT
iptables -I INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
第一句代表，所有本地接口（lo）的数据包都接收，因为系统内部经常会使用lo接口通讯，所以开起。
第二句代表，-m state代表根据状态来匹配数据包，--state RELATED,ESTABLISHED，RELATE代表“相关的”，意思就是说与请求相关的的响应数据，那么就允许，这样就省去在OUPUT链中另外配置一条对于响应数据的规则了。ESTABLISHED为已链接，状态为已链接，那么就允。