



链滴

iptables

作者: [zengxiaoyun](#)

原文链接: <https://ld246.com/article/1480409502924>

来源网站: [链滴](#)

许可协议: [署名-相同方式共享 4.0 国际 \(CC BY-SA 4.0\)](#)

<h5 data-source-line="1">一. 服务启停</h5>

```
<pre data-source-line="2"><code class="hljs">service iptables <span class="hljs-built_in">start</span>
<span class="hljs-comment">#启动</span>
service iptables <span class="hljs-built_in">stop</span>    <span class="hljs-comment">#
止</span>
service iptables restart <span class="hljs-comment">#重启</span>
chkconfig iptables <span class="hljs-command"><span class="hljs-keyword">on</span></span>
服务自动启动</span>
chkconfig iptables off    <span class="hljs-comment">#服务永久关闭</span></code></pre>
```

<h5 data-source-line="9">二. 规则配置</h5>

```
<pre data-source-line="10"><code class="hljs"><span class="hljs-preprocessor">#!/bin/ba
h</span>
<span class="hljs-preprocessor">#iptables rule</span>
<span class="hljs-preprocessor">#清除</span>
iptables -F
<span class="hljs-preprocessor">#保持已连接的?</span>
iptables -A INPUT -m state --state ESTABLISHED,RELATED,UNTRACKED -j ACCEPT
<span class="hljs-preprocessor">#回环?</span>
iptables -A INPUT -i lo -j ACCEPT
<span class="hljs-preprocessor">#本机访问本机</span>
iptables -A INPUT -s <span class="hljs-number">127.0</span><span class="hljs-number">.</span>
</span><span class="hljs-number">.1</span> -d <span class="hljs-number">127.0</span><span class="hljs-number">.</span>
<span class="hljs-number">.0</span><span class="hljs-number">.1</span> -j ACCEPT
<span class="hljs-preprocessor">#icmp (ping包) </span>
iptables -A INPUT -p icmp -j ACCEPT
<span class="hljs-preprocessor">#开放<span class="hljs-number">22</span>/<span class="hljs-number">.</span><span class="hljs-number">80</span>/<span class="hljs-number">3306</span>端口</span>
iptables -A INPUT -p tcp --dport <span class="hljs-number">22</span> -j ACCEPT
iptables -A INPUT -p tcp --dport <span class="hljs-number">80</span> -j ACCEPT
iptables -A INPUT -p tcp --dport <span class="hljs-number">22122</span> -j ACCEPT
<span class="hljs-preprocessor">#拒绝其他端口</span>
iptables -P INPUT DROP
<span class="hljs-preprocessor">#开放全部output出去的端口</span>
iptables -P OUTPUT ACCEPT</code></pre>
```

<h5 data-source-line="32">三. 其他操作</h5>

<h6 data-source-line="33">1. 编辑防火墙配置文件</h6>

```
<pre data-source-line="34"><code class="hljs">vim <span class="hljs-regexp">/etc/</span>
sysconfig<span class="hljs-regexp">/iptables</span></code></pre>
```

<h6 data-source-line="37">2. 查看防火墙状态</h6>

```
<pre data-source-line="38"><code class="hljs">iptables -nvL
<span class="hljs-preprocessor">#或者</span>
service iptables status
<span class="hljs-preprocessor">#或者</span>
cat /etc/sysconfig/iptables</code></pre>
```