

[首页](#) [归档](#) [分类](#) [标签](#) [搜索](#) [订阅](#) [关于](#) [帮助](#) [广告](#) [赞助](#) [打赏](#) [留言](#) [反馈](#) [退出](#) [登录](#)[博客专区](#) > [yearnfar的博客](#) > [博客详情](#)

## 实战Linux下防火墙iptables设置

[yearnfar](#) 发表于 2年前 阅读 1523 收藏 141 点赞 5 评论 2[收藏](#)**腾讯云·云上实验室：开发者零门槛，免费使用真机在线实验！>>>****HOT**

通过本教程操作，请确认您能使用linux本机。如果您使用的是ssh远程，而又不能直接操作本机，那么先加上下面的代码。。。当然最坏的结果是所有的端口都不能访问，甚至无法登陆ssh，但5分钟之后，定时器会帮你关掉防火墙。

```
[root@localhost ~]# crontab -u root -e

*/5 * * * * /etc/init.d/iptables stop    ##定时5分钟关闭防火墙，防止设置错误，导致无法进行ssh登陆
```

首先介绍几个简单命令：

```
/etc/init.d/iptables save    ##保存防火墙规则，如果不进行保存的话 重启iptables之后规则将消失

iptables -L -n               ##查看当前防火墙规则
```

**PS：**在添加规则之前先用iptables -L -n查看一下当前规则，如果显示没有规则，可能是你的iptables没有开启。如果这个时候添加规则，保存之后将覆盖之前的规则。如果要继续使用之前的规则，先开启iptables服务，这时候就能看到之前的规则，然后再在之前的基础上添加。

我们先添加两条规则

```
iptables -A INPUT -p tcp --dport 22 -j ACCEPT    ##添加一个开放端口22的输入流的规则

iptables -A OUTPUT -p tcp --sport 22 -j ACCEPT    ##添加一个开放端口22的输出流的规则
```

添加以上两条规则之后，就不用担心登陆不了SSH了，想了解命令详情使用iptables --help

**这里重点讲一下iptables 里面的 dport 和 sport的区别：**

dport：目的端口

sport：来源端口

通过两个INPUT的例子，大家区分下INPUT里面的dport和sport

例子1：

```
iptables -A INPUT -p tcp --dport 22 -j ACCEPT
```

这条INPUT规则可以这么描述：

- 1.这是一条从外部进入内部本地服务器的数据。
- 2.数据包的目的（dport）地址是22，就是要访问我本地的22端口。
- 3.允许以上的数据行为通过。

例子2：

```
iptables -A INPUT -p tcp --sport 22 -j ACCEPT
```

这条INPUT规则可以这么描述：

- 1.这是一条从外部进入内部本地服务器的数据。
- 2.数据包的来源端口是（sport）22，就是对方的数据包是22端口发送过来的。

3.允许以上数据行为。

通过两个OUTPUT的例子，大家区分下OUTPUT里面的dport 和sport

例子1：

```
iptables -A OUTPUT -p tcp --dport 22 -j ACCEPT
```

这条OUTPUT规则可以这么描述：

- 1.这是一条从内部出去的数据。
- 2.出去的目的（ dport ）端口是22。
- 3.允许以上数据行为。

例子2：

```
iptables -A OUTPUT -p tcp --sport 22 -j ACCEPT
```

这条OUTPUT规则可以这么描述：

- 1.这是一条从内部出去的数据。
- 2.数据包的来源端口是（ sport ）22，从本服务器的22端口发出数据。
- 3.允许以上数据行为。

### 默认INPUT、OUTPUT、FORWARD都是ACCEPT的

不添加规则，则对所有端口的数据来者不拒~

```
iptables -P INPUT DROP #如果没有添加端口22的accept规则，切勿运行此命令
```

如果运行上述命令的话，则是除了添加的规则之外的INPUT数据包都DROP掉。。。

同理还有这些命令：

```
iptables -P OUTPUT DROP
iptables -P FORWARD DROP
```

一般把INPUT设置为DROP。那么我们需要添加一些规则针对INPUT的ACCEPT的规则：

```
iptables -A INPUT -p tcp --dport 22 -j ACCEPT #开放ssh端口
iptables -A INPUT -p tcp --dport 80 -j ACCEPT #开放web服务端口
iptables -A INPUT -p tcp --dport 21 -j ACCEPT #开放ftp服务端口

iptables -A INPUT -p icmp -j ACCEPT #允许icmp包通过,也就是允许ping
iptables -A INPUT -i lo -p all -j ACCEPT #允许loopback
```

#####如果你还做了其他的服务器,需要开启哪个端口,照写就行了。

一般把OUTPUT设置为ACCEPT。那么我们需要添加一些规则针对OUTPUT的DROP规则：

```
关闭一些端口
iptables -A OUTPUT -p tcp --sport 27444 -j DROP
iptables -A OUTPUT -p tcp --sport 27665 -j DROP
iptables -A OUTPUT -p tcp --sport 31337 -j DROP
```

© 著作权归作者所有

分类：Linux 字数：1020

打赏

点赞

收藏

分享



yearnfar

程序员

+ 关注

粉丝 45 | 博文 84 | 码字总数 24369



### 相关博客

 面码

初识linux防火墙

4320

 cas\_

Linux 防火墙配置

190

 yzbt23

Linux下查看、关闭及开启防火墙命令

290

### 评论 (2)

Ctrl+Enter 发表评论



graysign

1楼 2015/06/23 09:35

mark



韩庚庚

2楼 2015/07/11 12:08

没看懂

#### 社区

开源项目  
技术问答  
动弹  
博客

开源资讯  
技术翻译  
专题  
招聘

#### 众包

项目大厅  
软件与服务  
接活赚钱

#### 码云

Git代码托管  
Team  
PaaS  
在线工具

#### 活动

线下活动  
发起活动  
源创会

#### 关注微信公众号



#### 下载手机客户端



©开源中国(OSChina.NET) 关于我们 广告联系 @新浪微博 合作单位

开源中国社区是工信部 开源软件推进联盟 指定的官方社区  
粤ICP备12009483号-3 深圳市奥思网络科技有限公司版权所有