TDXYBS

会会

昵称: TDXYBS
园龄: 5年7个月
粉丝: 0
关注: 0
+加关注

< 2024年11月 >

日	一	二	三	四	五	六
27	28	29	30	31	1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
1	2	3	4	5	6	7

搜索

找找看

常用链接

我的随笔
我的评论
我的参与
最新评论
我的标签

我的标签

Linux(4)
Julia(1)
Error(1)

随笔档案

2019年8月(1)
2019年7月(1)
2019年6月(3)
2019年5月(4)

阅读排行榜

1. 使用expect实现自动交互, shell命令行自动输入, 脚本自动化, 变量引用, expect spawn执行带引号命令, expect 变量为空, 不生效, 不能匹配通配符*, 函数, 数组(10599)
2. Ubuntu下Iptables的简单运用, 开放/关闭端口, 禁止/允许IP或IP段访问...(8064)
3. 编写expect程序报extra characters after close-brace错误或extra characters after close-quote, 解决(5666)
4. Linux中移动, 复制, 删除, 打包排除某个目录或文件(4477)
5. 解决Linux: Too many levels of symbolic links(2631)

推荐排行榜

1. 使用expect实现自动交互, shell命令行自动输入, 脚本自动化, 变量引用, expect spawn执行带引号命令, expect 变量为空, 不生效, 不能匹配通配符*, 函数, 数组(2)

Ubuntu下Iptables的简单运用, 开放/关闭端口, 禁止/允许IP或IP段访问...

首先添加规则有两个参数: -A和-I, 其中-A是添加到规则的末尾; -I可以插入到指定位置, 没有指定位置的话默认插入到规则的首部, 由于匹配规则是从上往下, 依次查找的, 可能出现配置的规则冲突导致后续的规则不起效

保存iptables规则

```
sudo iptables-save
```

保存ipv6 的iptables规则

```
sudo ip6tables-save
```

查看iptables规则

```
sudo iptables -L
```

查看iptables规则, 以数字形式

```
sudo iptables -L -n
```

查看iptables规则的序号, 用于删除规则参考

```
sudo iptables -L -n --line-numbers
```

清除所有iptables预设表filter里的所有规则

```
sudo iptabels -F
```

清除预设表filter中使用者自定链中的规则

```
sudo iptables -X
```

清除单条iptables规则

```
sudo iptables -D INPUT(链) 3(规则对应的序号)
```

修改单条iptables规则, 使用 -R, 修改INPUT链序号为3的规则为允许, 第4条规则为拒绝, 丢弃

```
sudo iptables -R INPUT 3 -j ACCEPT
sudo iptables -R INPUT 4 -j DROP
```

允许已经建立的连接发送和接收数据, 以免设置链为DROP时远程ssh断开

```
sudo iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
```

保证VPS可以进行的时候, 可以为loopback网卡添加进行规则, 规则第一行

```
sudo iptables -I INPUT 1 -i lo -j ACCEPT
```

允许某段IP访问本机的所有类型的所有端口

```
sudo iptables -I INPUT -s 192.168.2.0/24 -p all -j ACCEPT
sudo iptables -I INPUT -s 192.168.0.0/16 -p all -j ACCEPT
```

允许本机127.0.0.1访问自身所有端口

```
sudo iptables -I INPUT -s 127.0.0.1 -p all -j ACCEPT
```

允许某段IP访问本机的TCP 3306端口

```
sudo iptables -I INPUT -s 192.168.2.0/24 -p tcp --dport 3306 -j ACCEPT
```

允许某段IP访问本机的某段TCP端口

```
sudo iptables -I INPUT -s 192.168.2.0/24 -p tcp --dport 3306:65525 -j ACCEPT
```

向所有IP开放ssh的远程连接, 这里是已经更改了的19515端口, 默认为22端口

```
sudo iptables -A INPUT -p tcp --dport 19515 -j ACCEPT
```

默认INPUT OUTPUT FORWORD 链都是全部接受, 需要改为拒绝
将原ssh远程连接端口已经添加进 IPUNT 允许规则中, 否则执行以下命令将可能会断开远程

```
sudo iptables -A INPUT -p tcp --dport 19515 -j ACCEPT #这里ssh端口为19515
sudo iptables -P INPUT DROP
```

可选项,需保证SSH端口已经添加各链的允许规则, 否则会断开SSH连接并无法远程连接

```
sudo iptables -P OUTPUT DROP
sudo iptables -P FORWORD DROP
```

Iptables规则配置后, 无法访问外网, 无法接收返回的数据, 进行以下配置,并保证OUTPUT状态为ACCEPT, 会使Iptables允许由服务器本身请求的数据通过

```
sudo iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
sudo iptables -A OUTPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
```

Iptables 的持久化, 由于重启ubuntu会导致iptables规则丢失, 需要持久化
1.安装iptables-persistent工具帮助我们持久化

```
sudo apt-get update
sudo apt-get install iptables-persistent -y
```

执行命令持久化

```
sudo netfilter-persistent save
sudo netfilter-persistent reload
```

2.将iptables规则存入文件, 随网卡状态进行加载, 保存
将iptables保存的规则保存入当前用户的文件

```
sudo iptables-save > /home/user/iptables.rules
```

在/etc/network/interfaces 网卡配置文件里加入相应内容

```
vim /etc/network/interfaces
添加内容
pre-up iptables-restore < /home/user/iptables.rules
post-down iptables-save > /home/user/iptables.rules
```

用到的参数解释:
pre-up: 网卡启用前的动作
up: 启用时候的动作
post-up: 启用后的动作
pre-down: 关闭前的动作
down: 关闭时动作
post-down: 关闭后动作

Iptables的关闭, 使用清除规则来实现

```
sudo iptables-save > /home/user/iptables.rules
sudo iptables -X  清除默认filter表里的自定义规则
sudo iptables -t nat -F   清除nat表里的规则
sudo iptables -t nat -X
sudo iptables -t mangle -F  清除nat表里的规则
sudo iptables -t mangle -X
sudo iptables -P INPUT ACCEPT   将INPUT链默认更改为全部接受
sudo iptables -P OUTPUT ACCEPT
sudo iptables -P  FORWORD ACCEPT
```

如果想了解那入一些, 我个人觉得这个博主写的挺不错的朱双印的个人博客-Iptables详解

能力有限, 难免出错, 请多交流指出!!!

标签: Linux

好文要顶 关注我 收藏该文 微信分享

TDXYBS
粉丝 - 0 关注 - 0
+加关注

« 上一篇: Linux中移动, 复制, 删除, 打包排除某个目录或文件
» 下一篇: Linux生成ssh密钥免密登录, 允许/禁止密码登录, 允许/禁止root远程登录, 更改ssh端口

posted @ 2019-05-29 16:55 TDXYBS 阅读(8064) 评论(0) 编辑 收藏 举报

编辑推荐：

- 使用 C# 入门深度学习:线性代数
- .NET 9正式发布，亮点是.NET Aspire和AI
- 开发人员，千万不要去碰那该死的业务参数，无论什么时候！
- SQL Server 数据太多如何优化
- 带团队后的日常思考(十六)

阅读排行：

- .NET现在可以做什么，有哪些公司在用的？
- 使用 C# 入门深度学习:线性代数
- .NET 8 强大功能 IHostedService 与 BackgroundService 实战
- 在网页上调起本机C#程序
- .NET 创建动态方法方案及 Natasha V9