CentOs7 使用iptables防火墙开启关闭端口

# 0x01介绍

iptables命令是Linux上常用的防火墙软件，是netfilter项目的一部分

iptables文件设置路径：命令：vim /etc/sysconfig/iptables-config

# 0x02注意事项

如果说你以前使用的是contos7 那么默认使用的防火墙那么就是Firewall 这样的话，就要先把Firewall 给关闭在使用iptables

关闭Firewall 命令

命令：systemctl stop firewalld #关闭防火墙

命令：systemctl disable firewalld #禁止开机启动

# 0x03检查是否安装了iptables

命令：service iptables status

# 0x04安装iptables

命令：yum install -y iptables

# 0x05升级iptables

命令：yum update iptables

# 0x06安装iptables-services

命令：yum install iptables-services

# 0x07开启防火墙

命令：systemctl start iptables.service #启动防火墙

命令：systemctl enable iptables.service #设置开机自启动

# 0x08关闭防火墙

命令：systemctl stop iptables.service #关闭防火墙

命令：systemctl disable iptables.service #禁止开机启动

# 0x09查看iptables状态

命令：systemctl status iptables.service

# 0x10查看iptables现有规则

命令：iptables -L -n

# 0x11重点：清除默认的防火墙规则

## 11.1 安装完成基本配置-允许所有请求防止悲剧

#首先在清除前要将policy INPUT改成ACCEPT,表示接受一切请求。

#这个一定要先做，不然清空后可能会直接悲剧

#设置 INPUT 方向所有的请求都允许

命令：iptables -P INPUT ACCEPT

## 11.2 安装完成基本配置-清空所有默认规则

命令：iptables -F

## 11.3 安装完成基本配置-清空所有自定义规则

命令：iptables -X

## 11.4 安装完成基本配置-所有计数器归0

命令：iptables -Z

# 0x12重点：配置规则

## 12.1允许来自于lo接口的数据包

#如果没有此规则，你将不能通过127.0.0.1访问本地服务，例如ping 127.0.0.1

命令：iptables -A INPUT -i lo -j ACCEPT

## 12.2开启某个端口

iptables -A INPUT -p tcp --dport 端口 -j ACCEPT

### 12.2.1例子：开启80,22端口

命令：iptables -A INPUT -p tcp --dport 80 -j ACCEPT

命令：iptables -A INPUT -p tcp --dport 22 -j ACCEPT

## 12.3允许icmp包通过,也就是允许ping

命令：iptables -A INPUT -p icmp -m icmp --icmp-type 8 -j ACCEPT

## 12.4允许所有对外请求的返回包

#本机对外请求相当于OUTPUT,对于返回数据包必须要接收啊，这相当于INPUT了

命令：iptables -A INPUT -m state --state ESTABLISHED -j ACCEPT

## 12.5如果要添加内网ip信任（接受其所有TCP请求）

iptables -A INPUT -p tcp -s 192.168.1.50(改为允许的内网IP即可) -j ACCEPT

## 12.6过滤除iptables规则之外的所有请求

命令：iptables -P INPUT DROP

# 0x13 重点：保存规则

注意：设置完成以后先执行命令iptables -L -n看一下配置是否正确。

没问题后，先不要急着保存，因为没保存只是当前有效，重启后就不生效，这样万一有什么问题，可以后台强制重启服务器恢复设置。

另外开一个ssh连接，确保可以登陆。

确保没问题之后在进行保存

保存命令：service iptables save

# 0x14 重启防火墙

命令：systemctl restart iptables.service

# 0x15 杂项

## 15.1要封停一个IP，使用下面这条命令

命令：iptables -I INPUT -s \*\*\*.\*\*\*.\*\*\*.\*\*\* -j DROP

## 15.2 要解封一个IP，使用下面这条命令:

命令：iptables -D INPUT -s \*\*\*.\*\*\*.\*\*\*.\*\*\* -j DROP

# 0x16 删除某个已有规则

要删除规则那么我们就需要先将所有iptables规则以序号标记显示，执行：

命令：iptables -L -n --line-numbers

比如要删除INPUT里序号为8的规则，执行：

命令：iptables -D INPUT 8

# 0x17 例子：完整的设置脚本

1. #!/bin/sh
2. #查看iptables现有规则
3. iptables -L -n
4. #先允许所有,不然有可能会杯具
5. iptables -P INPUT ACCEPT
6. #清空所有默认规则
7. iptables -F
8. #清空所有自定义规则
9. iptables -X
10. #所有计数器归0
11. iptables -Z
12. #允许来自于lo接口的数据包(本地访问)
13. iptables -A INPUT -i lo -j ACCEPT
14. #开放22端口
15. iptables -A INPUT -p tcp --dport 22 -j ACCEPT
16. #开放21端口(FTP)
17. iptables -A INPUT -p tcp --dport 21 -j ACCEPT
18. #开放80端口(HTTP)
19. iptables -A INPUT -p tcp --dport 80 -j ACCEPT
20. #开放443端口(HTTPS)
21. iptables -A INPUT -p tcp --dport 443 -j ACCEPT
22. #允许ping
23. iptables -A INPUT -p icmp --icmp-type 8 -j ACCEPT
24. #允许接受本机请求之后的返回数据 RELATED,是为FTP设置的
25. iptables -A INPUT -m state --state  RELATED,ESTABLISHED -j ACCEPT
26. #其他入站一律丢弃
27. iptables -P INPUT DROP
28. #所有出站一律绿灯
29. iptables -P OUTPUT ACCEPT
30. #所有转发一律丢弃
31. iptables -P FORWARD DROP
32. #保存
33. service iptables save
34. #重启动
35. serv systemctl restart iptables.service