[面试题]防火墙相关

作者：

归档：学习笔记

2016/6/27

快捷键：

Ctrl + 1	标题 1
Ctrl + 2	标题 2
Ctrl + 3	标题 3
Ctrl + 4	实例
Ctrl + 5	程序代码
Ctrl + 6	正文

格式说明：

蓝色字体：注释

黄色背景：重要

绿色背景：注意

老男孩linux运维实战培训

老男孩教育教学核心思想 6 重：重目标、重思路、重方法、重实践、重习惯、重总结

学无止境，老男孩教育成就你人生的起点！

目 录

第1章 选择

1.1 rule permit ip source 210.78.1.1 0.0.255.255 destination202.38.5.2 0.0.0.0 的含义是（ D ）

A. 允许主机 210.78.1.1 访问主机 202.38.5.2
B. 允许 210.78.0.0 的网络访问 202.38.0.0 的网络
C. 允许主机 202.38.5.2 访问网络 210.78.0.0
D. 允许 210.78.0.0 的网络访问主机 202.38.5.2

1.2 在防火墙上允许 tcp 和 udp 端口 21、 23、 25 访问内网，下列那张协议包可以进来 （多选）

A C D

A. SMTP #25 简单邮件传输协议
B. STP #
C. FTP #21 20
D. Telnet #23
E. HTTP #80
F. POP3 #110

1.3 以下不属于防火墙能够实现的功能是(B)

A、网络地址转换

B、差错控制

C、数据包过滤

D、数据转发

1.4 哪个不属于 iptables 的表 D

A. filter
B. nat
C. mangle
D. INPUT

1.5 以下对防火墙的描述正确的是：（C）

A. 完全阻隔了网络
B. 能在物理层隔绝网络
C. 仅允许合法的通讯
D. 无法阻隔黑客的侵入

第2章 填空

2.1 （防火墙）是设置在被保护网络和外部网络之间的一道屏障，以防止破坏性侵入

2.2 在 CentOS7 下，我想关闭掉防火墙，应该用命令_systemctl stop firewalld_来关闭掉。如果以后开机都不想它启动起来，执行(systemctl disable firewalld)命令

2.3 在 CentOS7 配置 ip 转发需要在(/etc/sysctl.conf)里加入(net.ipv4.ip_forward=1)执行(sysctl -p)命令后生效

第3章 简答

3.1 防火期墙策略，开放服务器 80 端口，禁止来自 10.0.0.188 的地址访问服务器 80 端口的请求。

```
iptables -t filter -A INPUT -p tcp --dport 80 -j ACCEPT
iptables -t filter -I INPUT -p tcp --dport 80 -s 10.0.0.188 -j DROP
```

或

```
iptables -A INPUT -p tcp --dport 80  ! -s 10.0.0.188 -j ACCEPT
```

3.2 防火墙策略，实现把访问 10.0.0.3:80 的请求转到 172.16.1.17:8080 上。

```
iptables -t nat -A PREROUTING  -p tcp --dport 80 -j DNAT --to 172.16.1.17:8080
```

3.3 防火墙策略配置说明。阐述出 10.10.10.1 访问 192.168.1.1 所有端口策略需要的配置过程

```
iptables  -A INPUT  -p all -s 10.10.10.1  -d 192.168.1.1  --dport 1:65535  -j ACCEPT
```

iptables -t filter -I INPUT -p tcp --dport 1-65535 -s 10.10.10.1 -d 192.168.1.1 -j ACCPET

iptables 知识考察，根据要求写出防火墙规则

3.4 屏蔽 192.168.1.5 访问本机 dns 服务端口：

```
iptables -t filter -I INPUT -p udp --dport 53 -s 192.168.1.5 -j DROP
iptables -t filter -I INPUT -p tcp --dport 53 -s 192.168.1.5 -j DROP
```

3.5 允许 10.1.1.0/24 访问本机的 udp 8888 9999 端口

```
iptables -t filter -I INPUT -s 10.1.1.0/24  -p udp  -m multiport --dport 8888,9999 -j ACCEPT
```

3.6 iptables 禁止 10.10.10.1 访问本地 80 端口

```
iptables -t filter -I INPUT -p tcp -s 10.10.10.1 --dport 80 -j DROP
```

3.7 如何利用 iptables 屏蔽某个 IP 对 80 端口的访问

```
iptables -t filter -I INPUT -p tcp -s xx.xx.xx.xx --dport 80 -j DROP
```

3.8 写出 iptables 四表五链，按照优先级排序

表的处理优先级：raw>mangle>nat>filter
进路由(PREROUTING)、进系统(INPUT) 、转发(FORWARD)、出系统(OUTPUT)、出路由(POSTROUTING)

3.9 如何通过 iptables 将本地 80 端口的请求转发到 8080 端口，当前主机 IP 为 192.168.2.1

```
iptables -t nat -A PREROUTING -p tcp --dport 80 -j DNAT --to-destination 192.168.2.1:8080
```

3.10 请写一条命令，只允许 80 端口，其他端口都拒绝，eth1 网卡 ip 为 192.168.1.12

一条命令的：

```
iptables -I INPUT -p tcp  ! --dport 80 -j DROP
或
iptables -I INPUT -p tcp -i eth1 -d 192.168.1.12 ! --dport 80 -j DROP
```

分为两步的:

```
iptables -t filter -I INPUT -p tcp -d 192.168.1.12 --dport 80 -j ACCEPT
iptables -P INPUT DROP
```

3.11 限制连接到 192.168.100.100:8080 后端服务最大 1000

```
iptables -I INPUT  -p tcp -d 192.168.100.100  --dport 8080  -m limit  --limit 10/min  --limit-burst 1000
```

3.12 请简述防火墙的基本功能和特点

基本功能：
包过滤
包的透明转发
阻挡外部攻击
记录攻击

特点：
数据必经之地
网络流量的合法性
抗攻击免疫力

3.13 内网环境中，A（10.0.0.1）机与 B（10.0.0.2）机互通，现在需要在 A 机上简单安全策略，禁止 B 机访问 A 机的 SSH 服务（22 端口）有几种方法？如何操作？

```
iptables -t filter -A INPUT -p tcp --dport 22 -j DROP
iptables -t filter -I INPUT -p tcp -s 10.0.0.2 -j DROP
iptables -t filter -I INPUT -p tcp -s 10.0.0.2 --dport 22 -j DROP
```

3.14 service iptables stop 与 iptables -F 有何区别？

systemctl stop iptables #关闭防火墙服务，如果规则没有保存 之前配置的规则丢失
前者是 iptables 服务的关闭，会清空当前规则。
后者是清空临时规则

3.15 iptables 封禁 eth0 网卡与 192.168.1.1 通讯的所有数据包

iptables -t filter -I INPUT -p all -i eth0 -s 192.168.1.1 -j DROP
iptables -t filter -I OUTPUT -p all -o eth0 -d 192.168.1.1 -j DROP

3.16 iptables 禁止所有到本机（eth0:10.10.10.200）22 端口的 TCP 访问

iptables -t filter -I INPUT -p tcp -d 10.10.10.200 --dport 22 -j DROP

3.17 如何禁止 192.168.500.2 访问本机 ssh 端口？

3.18 解释这条规则：/sbin/iptables -t nat -A PREROUTING -d 192.168.20.99/32 -p udp -m udp --dport 99 -j DNAT --to-destination 192.168.20.11

1. iptables -t filter -I INPUT -p tcp -s 192.168.500.2 --dport 22 -j DROP
2. 将请求 192.168.20.99 的 udp 99 端口的数据包转发到 192.168.20.11

3.19 有一台主机内网 IP：10.4.82.200，公网 IP：118.186.111.121，现欲使 10.4.82.0/24 网段,（该网段默认网关为 10.4.82.254），使用 10.4.82.200 作为跳板机出往，请给出配置方法

将默认网关改为 10.4.82.200

iptables -t nat -I POSTROUTING -p tcp -s 10.4.82.0/24 -j SNAT --to-source 118.186.111.121

3.20 配置跳板机主机的某个内核参数，并使其生效

3.21 配置跳板机的 iptables 防火墙规则

```
iptables -t filter -I INPUT -s xx.xx.xx.xx -p tcp --dport 2222 -j ACCEPT
```

3.22 把 10.10.0.0 网段流出的数据的原地址修改为 66.66.66.66

iptables -t nat -I POSTROUTING -p tcp -s 10.10.0.0/24 -j SNAT --to-source 66.66.66.66

3.23 本机有两张网卡，分别为 eth0 和 eth1，请写出仅允许从 eth0 访问本机 web（80）服务的 iptables 规则，允许 eth1 所有访问

```
iptables -t filter -I INPUT -p tcp --dport 80 -i eth0 -j ACCEPT
iptables -t filter -I INPUT -p all -i eth1 -j ACCEPT
```