Contents

目录

1. 环境准备：

1.1 构建 Web 服务（在虚拟机 A 上操作）

1.1.1 安装 httpd 软件包

```
[root@A ~]# yum -y install httpd    #注：安装失败检测yum源是否可用
[root@A ~]# rpm -q httpd
```

1.1.2 启动 httpd 服务

```
[root@A ~]#  systemctl  start  httpd
```

1.1.3 书写页面文件，测试

默认存放网页文件的路径：/var/www/html

默认网页文件的名称：index.html

```
[root@A ~]# vim  /var/www/html/index.html
I am king.
测试
[root@A ~]# curl http://192.168.4.7
```

1.2 搭建 FTP 服务（在虚拟机 A 上操作）

1.2.1 安装 vsftpd 软件包

```
[root@A~]# yum -y install vsftpd    #注：安装失败检测yum源是否可用
[root@A ~]# rpm -q vsftpd
```

1.2.2 启动 httpd 服务

```
[root@A ~]#  systemctl  start  vsftpd
```

1.2.3 测试

默认共享数据目录：/var/ftp

```
[root@A ~]#  touch /var/ftp/a.txt                    #创建测试文件
[root@A ~]# curl ftp://192.168.4.7
```

2. 防火墙简介：

2.1 防火墙简介

防火墙分为硬件防火墙，软件防火墙

作用：隔离，进行过滤所有入站请求

2.2 firewalld 服务基础

• 管理工具:firewall-cmd、firewall-config（图形工具）

预设安全区域

• 根据所在的网络场所区分,预设保护规则集

– public：仅允许访问本机的 sshd、ping、dhcp 服务

– trusted：允许任何访问

– block：阻塞任何来访请求（明确拒绝，有回应客户端）

– drop：丢弃任何来访的数据包（直接丢弃，没有回应客户端），节省服务器资源

防火墙判定规则：（进入哪一个区域）

1.首先查看，客户端数据包中源 IP 地址，然后查看自己所有区域规则，那个区域有该源 IP 地址的规则，则进入该区域

2.进入默认区域（public）

2.3 防火墙默认区域的修改

虚拟机 A 操作：

```
[root@A ~]# firewall-cmd --get-default-zone      #查看默认区域
```

虚拟机 B（svr7）测试：

```
[root@svr7 ~]# ping 192.168.4.10          #可以通信
[root@svr7 ~]# curl 192.168.4.10          #拒绝访问
[root@svr7 ~]# curl ftp://192.168.4.10    #拒绝访问
```

虚拟机 A 操作：

```
[root@A ~]# firewall-cmd --set-default-zone=trusted #修改默认区域为trusted
[root@A ~]# firewall-cmd --get-default-zone
```

虚拟机 B（svr7）测试：

```
[root@svr7 ~]# curl ftp://192.168.4.10          #可以访问
[root@svr7 ~]# ping 192.168.4.10                #可以通信
```

虚拟机 A 操作：

```
[root@A ~]# firewall-cmd --set-default-zone=block #修改默认区域为block
[root@A ~]# firewall-cmd --get-default-zone
```

虚拟机 B（svr7）测试：

```
[root@svr7 ~]# ping 192.168.4.10      #不可以通信，有回应
```

虚拟机 A 操作：

```
[root@A ~]# firewall-cmd --set-default-zone=drop #修改默认区域为drop
[root@A ~]# firewall-cmd --get-default-zone
```

虚拟机 B（svr7）测试：

```
[root@svr7 ~]# ping 192.168.4.10          #不可以通信，没有回应
```

2.4 防火墙的策略管理

2.4.1 互联网常见的协议

http：超文本传输协议　　默认端口：80

https：安全的超文本传输协议　　默认端口：443

ftp：文件传输协议　　默认端口：21

tftp：简单文件传输协议　　默认端口：69

DNS：域名解析协议　　默认端口：53

telnet：远程管理协议　　默认端口：23

smtp：邮件协议（发邮件）　　默认端口：25

pop3：邮件协议（收邮件）　　默认端口：110

snmp：简单的网络管理协议　　默认端口：161

2.4.2 封网段，开服务

虚拟机 A 查看区域为 public 区域

```
[root@A ~]# firewall-cmd --get-default-zone
public
```

虚拟机 B（svr7）主机测试访问 http 和 ftp，访问失败

```
[root@svr7 ~]# curl ftp://192.168.4.10
[root@svr7 ~]#  curl 192.168.4.10
```

设置允许 http 协议通过 public 区域

```
[root@A ~]#firewall-cmd --zone=public --add-service=http
查看区域策略
[root@A ~]#firewall-cmd --zone=public --list-all
```

虚拟机 B（svr7）主机测试访问

```
[root@svr7 ~]#  curl http://192.168.4.10    #成功
[root@svr7 ~]#  curl ftp://192.168.4.10     #失败
```

设置允许 ftp 协议通过 public 区域

```
[root@A ~]#firewall-cmd --zone=public --add-service=ftp
[root@A ~]# firewall-cmd --zone=public --list-all
```

虚拟机 B（svr7）主机测试访问

```
[root@svr7 ~]#  curl ftp://192.168.4.10
```

测试若是重启机器或者重新加载防火墙，配置会失效

```
[root@A ~]# reboot
```

需要永久性配置：

永久(--permanent)

```
[root@A ~]# firewall-cmd --permanent --zone=public --add-ervice=http
[root@A ~]# firewall-cmd --permanent --zone=public --add-service=ftp
[root@A ~]# firewall-cmd --reload          #重新加载配置文件
[root@A ~]# firewall-cmd --zone=public --list-all
```

单独拒绝虚拟机 pc207（192.168.4.207）进行访问本机所有服务

虚拟机 A 配置拒绝策略

```
[root@A ~]# firewall-cmd --zone=block --add-source=192.168.4.7
```

虚拟机 B（svr7）主机测试访问

```
[root@svr7 ~]#  curl ftp://192.168.4.10 #失败
[root@svr7 ~]# curl 192.168.4.10 #失败
```

其他主机可以访问成功

虚拟机 A 删除规则

```
[root@A ~]# firewall-cmd --zone=block --remove-source=192.168.4.7
```