# Linux 防火墙firewall

**1.systemctl是CentOS7的服务管理工具中主要的工具，它融合之前service和chkconfig的功能于一体。**

**启动一个服务：systemctl start firewalld.service**

**关闭一个服务：systemctl stop firewalld.service**

**重启一个服务：systemctl restart firewalld.service**

**显示一个服务的状态：systemctl status firewalld.service**

**在开机时启用一个服务：systemctl enable firewalld.service**

**在开机时禁用一个服务：systemctl disable firewalld.service**

**查看服务是否开机启动：systemctl is-enabled firewalld.service**

**查看已启动的服务列表：systemctl list-unit-files|grep enabled**

**查看启动失败的服务列表：systemctl –failed**

**2.配置firewalld-cmd**

**查看版本： firewall-cmd –version**

**查看帮助： firewall-cmd –help**

**显示状态： firewall-cmd --state**

**查看所有打开的端口： firewall-cmd --zone=public --list-ports**

**更新防火墙规则： firewall-cmd --reload**

**查看区域信息:  firewall-cmd --get-active-zones**

**查看指定接口所属区域： firewall-cmd --get-zone-of-interface=eth0**

**拒绝所有包：firewall-cmd --panic-on**

**取消拒绝状态： firewall-cmd --panic-off**

**查看是否拒绝： firewall-cmd --query-panic**

**3.常见端口**

**http:80**

**ssh:22**

**redis:6379 7000 7001 7002**

**mysql:3306**

**mongdb: 27017 mongod 和 mongos 实例的默认端口。你可以通过 port 或 --port 改变该端口。**

**27018 设置 --shardsvr 运行变量或在配置文件里设置 clusterRole 为 shardsvr 时的默认端口。**

**27019 设置 --configsvr 运行变量或在配置文件中将 clusterRole 设置为 configsvr 时的默认端口。**

**28017 系统状态网页的默认端口。系统状态网络页面永远可以在比 port 大 1000 的端口反问。**

**es:9300**

**rebbitmq:5672**

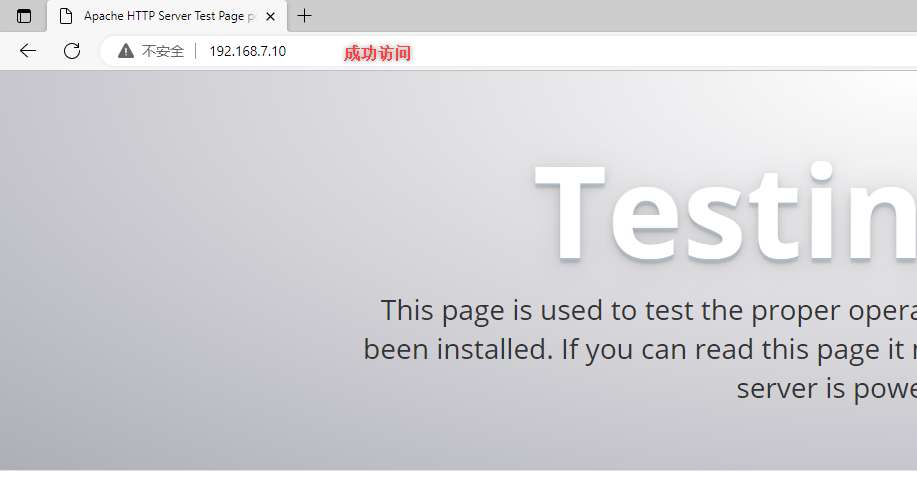
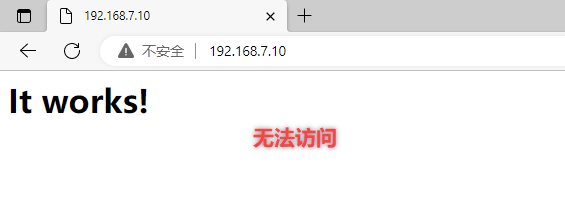
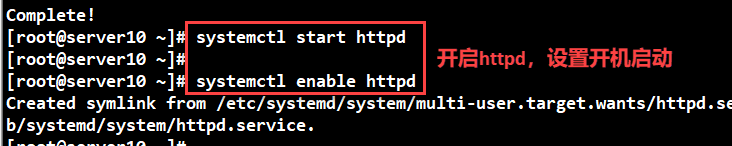
**consul:8500**

**DHCP用的端号是UDP67和UDP68**

**Samba服务所使用的端口和协议：**

1. **Port 137 (UDP) - NetBIOS 名字服务 ； nmbd**
2. **Port 138 (UDP) - NetBIOS 数据报服务**
3. **Port 139 (TCP) - 文件和打印共享 ； smbd**
4. **Port 389 (TCP) - 用于 LDAP (Active Directory Mode)**
5. **Port 445 (TCP) - NetBIOS服务在windos 2000及以后版本使用此端口, (Common Internet File System，CIFS，它是SMB协议扩展到Internet后，实现Internet文件共享)**
6. **Port 901 (TCP) - 用于 SWAT，用于网页管理Samba**

**4.防火墙设置http规则**



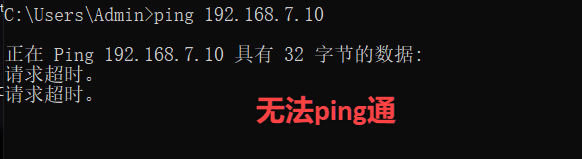
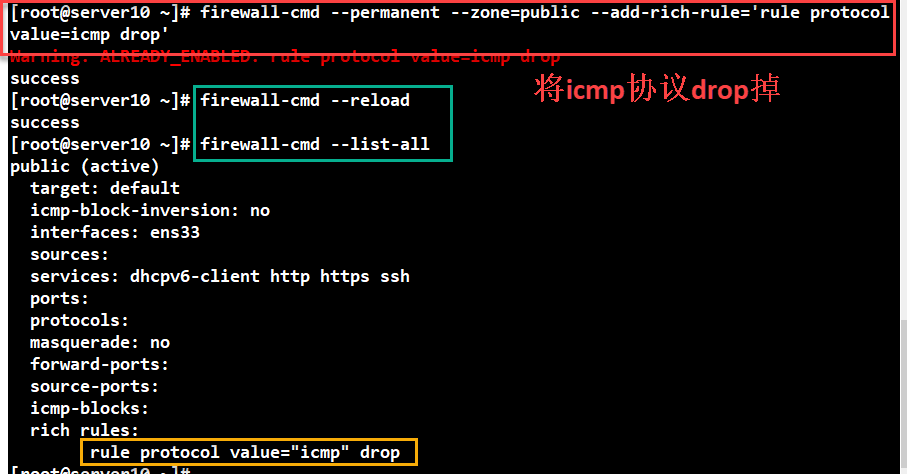
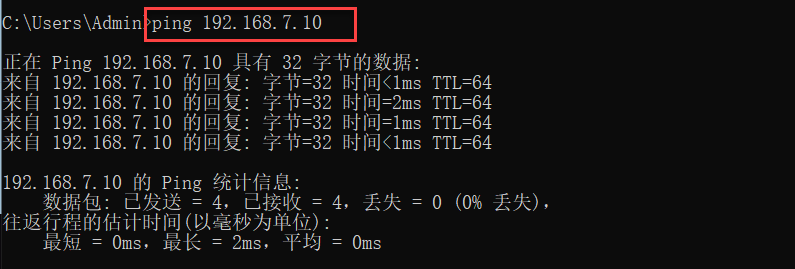
**防火墙移除http规则**

[root@localhost ~]# **firewall-cmd --zone=public --remove-service=http --permanent**

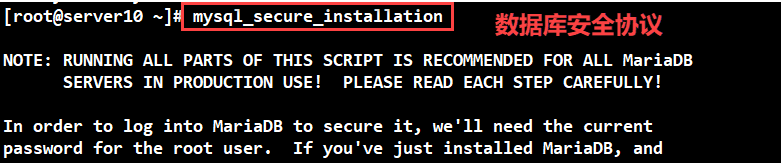
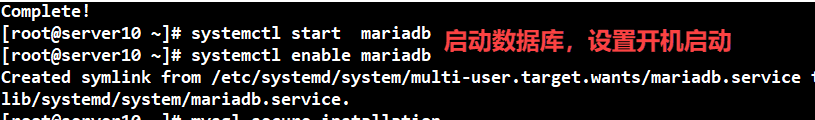
[root@localhost ~]# **firewall-cmd --reload**

success

**5防火墙设置拒绝被ping**



**6防火墙设置mariadbs数据库规则**





**只允许192.168.7.12主机远程登录数据库**

[root@localhost ~]# **firewall-cmd --permanent --add-rich-rule='rule family=ipv4 source address=192.168.7.12 service name=mysql accept'**

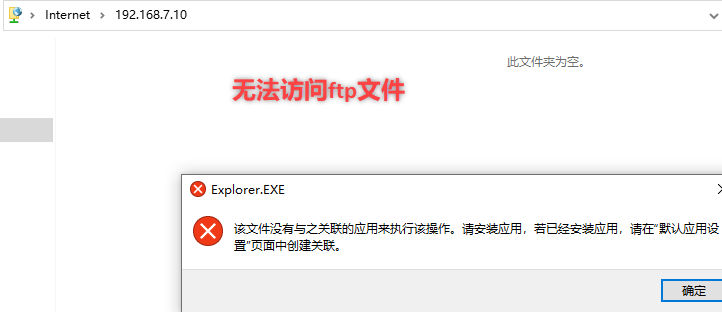
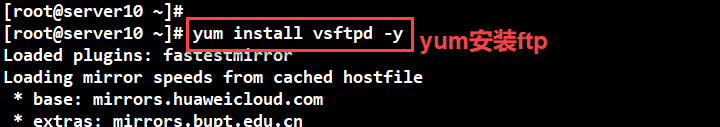
[root@localhost ~]# **firewall-cmd --permanent --add-rich-rule='rule family=ipv4 source address=192.168.7.12 service name=mysql accept'**

[root@localhost ~]# **firewall-cmd --list-all**

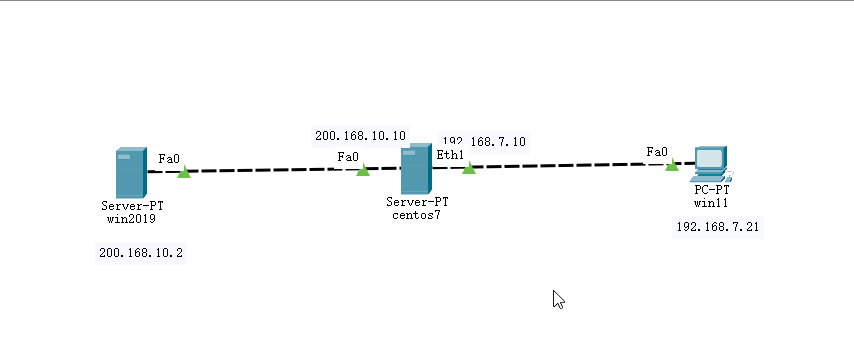
rich rules:

rule family="ipv4" source address="192.168.7.12" service name="mysql" accept

**8在防火墙中设置ftp规则**



# 实验1：Linux防火墙nat

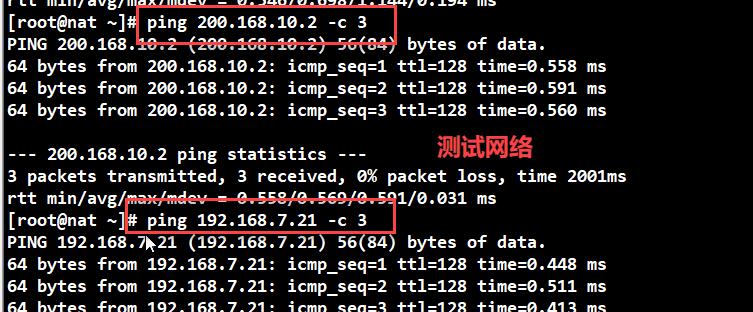
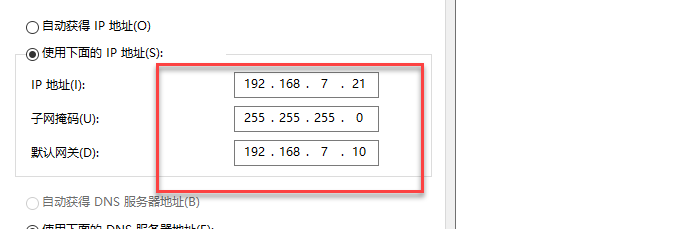
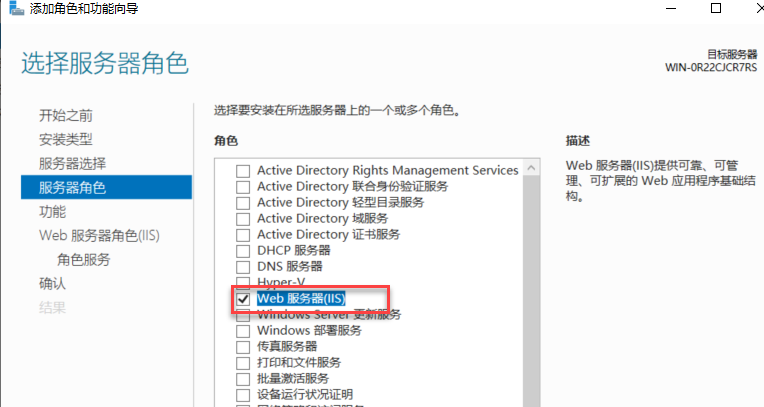
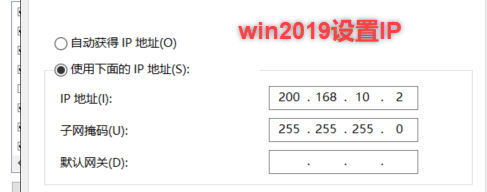
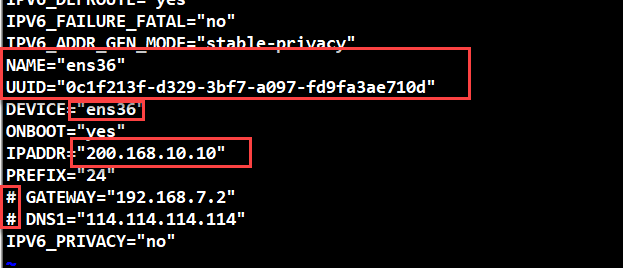
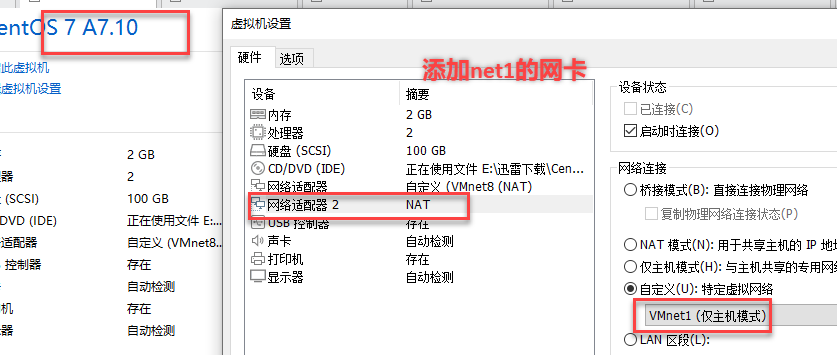


**win2019 vmnet1 IP:200.168.10.2**

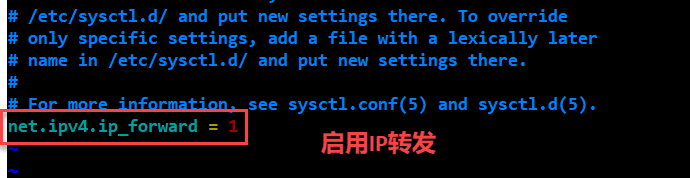
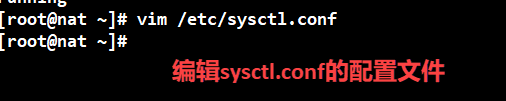
**Centos7 vmnet1 IP:200.168.10.10**

**vmnet8 IP:192.168.7.10**

**win11 vmnet8 IP:192.168.7.21**



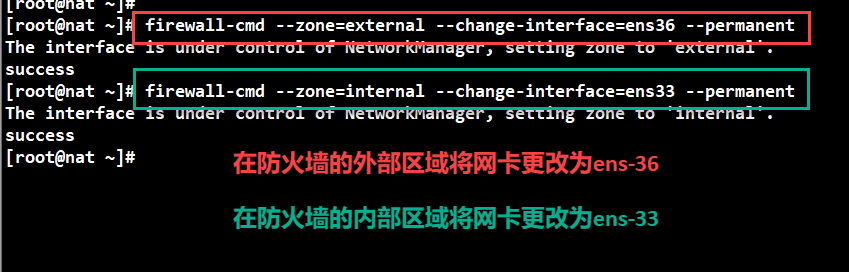
**1.启用IP转发**



**2.修改接口区域**

**ens33设置internal(内部区域)**

**ens36设置external(外部区域)**



**3.设置IP地址伪装**

**firewall-cmd --zone=external --add-masquerade --permanent**

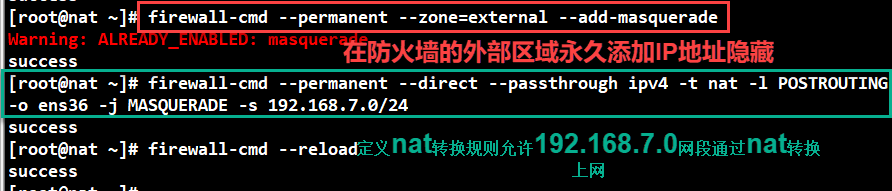
**移除地址伪装**

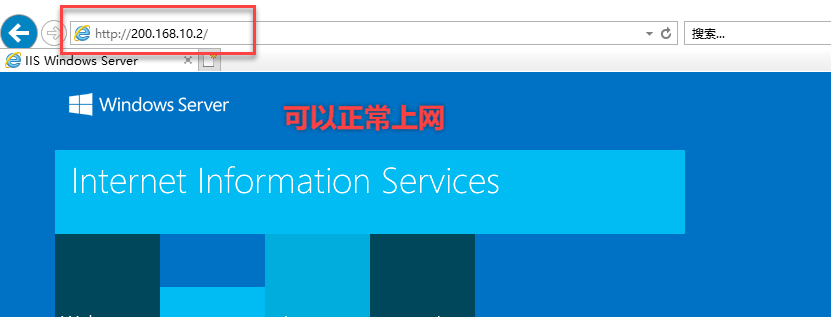
**firewall-cmd --zone=external --remove-masquerade –permanent**

**4.设置NAT规则**

**firewall-cmd --permanent --direct --passthrough ipv4 -t nat -I POSTROUTING -o ens36 -j MASQUERADE -s 192.168.7.0/24**

**firewall-cmd --reload**





**5.配置端口映射**



