Linux自动化运维特训班

firewalld动态防火墙管理

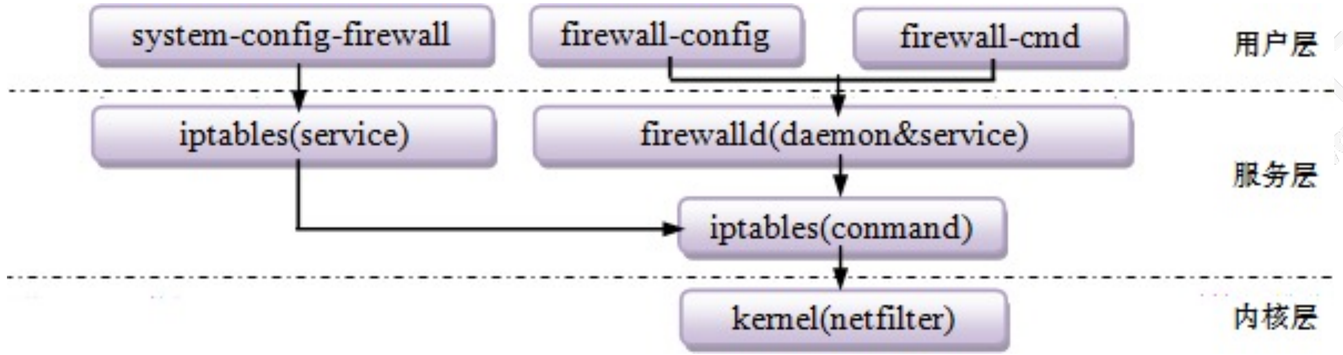
讲师：孔丹

大纲

- firewalld简介
- firewalld区域
- firewalld配置
- firewall-cmd配置防火墙
- firewall-config配置防火墙

firewalld简介

- Firewalld 服务是红帽 RHEL7 系统中默认的防火墙管理工具。
- RHEL 7中引入了一种与netfilter交互的新的中间层服务程序firewalld(旧版中的iptables、ip6tables和ebtables等仍保留)，firewalld是一个可以配置和监控系统防火墙规则的系统服务程序或守护进程,该守护进程具备了对IPv4、IPv6和ebtables等多种规则的监控功能,不过firewalld底层调用的命令仍然是iptables等。
  firewalld防火墙体系结构如图所示。



firewalld简介

- 在RHEL7中用户层的配置firewalld防火墙规则的工具有以下三种:
  - 图形工具firewall-config。
  - 命令行工具firewall-cmd。
  - 直接编辑/etc/firewalld/目录中扩展名为.xml的一系列配置文件。
- Firewalld和iptables 不同之处
  - iptables service 在 /etc/sysconfig/iptables 中储存配置,而 firewalld将配置储存在/usr/lib/firewalld/ 和 /etc/firewalld/ 中的各种XML文件里.
  - 使用 iptables service每一个单独更改意味着清除所有旧有的规则和从/etc/sysconfig/iptables里读取所有新的规则,然而使用 firewalld却不会再创建任何新的规则;仅仅运行规则中的不同之处。因此,firewalld可以在运行时间内,改变设置而不丢失现行连接。
  - iptables通过控制端口来控制服务，而firewalld则是通过控制协议来控制端口

firewalld区域

- 为了简化防火墙管理,firewalld将所有网络流量划分为多个区域。根据数据包源IP地址或传入网络接口等条件,流量将转入相应区域的防火墙规则,firewalld提供的几种预定义的区域及防火墙初始规则

trusted 允许所有的数据包

home 拒绝流入的流量,除非与流出的流量相关;而如果流量与 ssh、mdns、ipp-client、amba-client 与 dhcpv6-client 服务相关,则允许流量

internal 等同于 home 区域

work 拒绝流入的流量,除非与流出的流量数相关;而如果流量与ssh、ipp-client 与dhcpv6-client 服务相关,则允许流量

public 拒绝流入的流量,除非与流出的流量相关;而如果流量与 ssh、dhcpv6-client 服务相关,则允许流量

external 拒绝流入的流量,除非与流出的流量相关;而如果流量与 ssh 服务相关,则允许流量

dmz 拒绝流入的流量,除非与流出的流量相关;而如果流量与 ssh 服务相关,则允许流量

block 拒绝流入的流量,除非与流出的流量相关

drop 拒绝流入的流量,除非与流出的流量相关

firewalld配置模式

- 运行时模式：表示当前内存中运行的防火墙配置，在系统或firewalld服务重启、停止时将失效；

- 永久模式：表示重启防火墙或重新加载防火墙时的规则配置，是永久存储在配置文件中的。

- firewall-cmd命令工具与配置模式相关的选项有三个：

  - --reload：重新加载防火墙规则并保持状态信息，即将永久配置应用为运行时配置；
  - --permanent：带有此选项的命令用于设置永久性规则，这些规则只有在重新启动或重新加载防火墙规则时才会生效；若不带此项，表示用于设置运行时规则。
  - --runtime-to-permanent：将当前运行时的配置写入规则配置文件中，使当前内存中的规则称为永久性配置

firewalld安装与运行管理

- 安装firewalld软件包
  - # rpm -qa |grep firewall
  - # yum -y install firewalld firewall-config

- firewall服务的运行管理
  - firewalld防火墙的状态查看、启动、停止、重启、重载服务的命令格式为:
  - systemctl status | start| stop|restart|reload firewalld.service
  - 开机自动启动或停止firewalld服务的命令格式为:
  - systemctl enable |disable firewalld.service
  - 屏蔽iptables
  - systemctl mask iptables
  - systemctl umask iptables 停止屏蔽功能

注意:mask和disable的区别
mask将服务链接至/dev/null,禁止开机自启

firewalld配置

- 使用命令行接口配置firewall
  - 查看

1. firewall-cmd --state ##查看当前活动的区域,并附带一个目前分配给它们的接口列表
2. firewall-cmd --get-active-zones ##查看默认区域:
3. firewall-cmd --get-default-zone ##查看所有可用区域:
4. firewall-cmd --zone=public --list-all ##列出所有预设服务
5. firewall-cmd --get-services ##列出全部服务
6. firewall-cmd --list-all-zones ##列出所有区域的设置

firewalld配置

- 使用命令行接口配置firewall
  - 添加、改变、删除网络接口

1. firewall-cmd --permanent --zone=internal --add-interface=eth0
2. firewall-cmd --permanent --zone=internal --change-interface=eth0
3. firewall-cmd --permanent --zone=internal --remove-interface=eth0

如果没有添加区域，则为当前默认区域

firewalld配置

- 使用命令行接口配置firewall
  - 添加、删除服务

1. firewall-cmd --permanent --zone=public --add-service=smtp
2. firewall-cmd --permanent --zone=public --remove--service=smtp

  - 列出、添加、删除端口:

1. firewall-cmd --zone=public --list-ports
2. firewall-cmd --permanent --zone=public --add-port=8080/tcp
3. firewall-cmd --permanent --zone=public --remove-port=8080/tcp

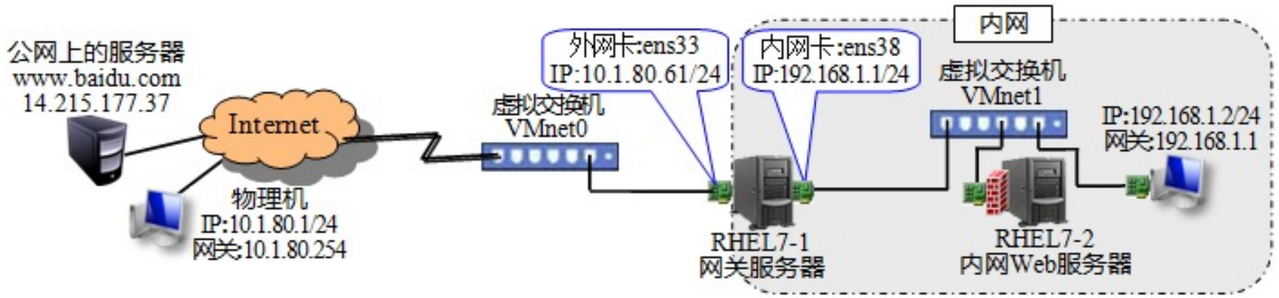
firewalld配置

- 使用命令行接口配置firewall
  - 端口转发和地址伪装

1. firewall-cmd --permanent --zone=< ZONE > --add-masquerade 在做伪装的时候，一定要先打开伪装选项（masquerade ）
2. firewall-cmd --permanent --zone=< ZONE > --add-rich-rule=’ rule family=ipv4 source addres=172.25.0.0/24 masquerade’
3. firewall-cmd --permanent --zone=< ZONE > --add-forward-port=port=80:proto=tcp:toport=8080:toaddr=172.25.0.10 端口转发

firewall-cmd配置防火墙

假设在内网架设了一台Web服务器，IP地址是192.168.1.2，端口是80，设置内网网段192.168.1.0/24中的主机均可以访问此Web服务器，如图所示。



firewall-cmd配置防火墙

- 配置步骤：

1、查看当前的默认区域→查询ens33网卡所属的区域→设置默认区域为dmz→将ens33网卡永久移至dmz区域→重新载入防火墙设置使上述设置立即生效

```
# firewall-cmd  --get-default-zone
public
# firewall-cmd  --get-zone-of-interface=ens33
public
# firewall-cmd  --set-default-zone=dmz
#   firewall-cmd      --permanent      --zone=dmz      --change-
   interface=ens33
# firewall-cmd  --reload
```

2、安装httpd服务软件包→启用httpd服务→创建网站的测试首页

```
# yum  -y  install  httpd
# systemctl  start  httpd.service
# echo  "防火墙配置测试"> /var/www/html/index.html
```

firewall-cmd配置防火墙

- 配置步骤：

3、测试:在本机可成功访问网站→在网段192.168.1.0/24中的其他主机上访问失败

4、在dmz区域允许http服务流量通过,要求立即生效且永久有效

```
# firewall-cmd  --permanent  --zone=dmz  --add-service=http
# firewall-cmd  --reload
```

firewall-cmd配置防火墙

- 为了安全起见,将【例7-14】中的Web服务器工作在8080端口,现要求通过端口转换,让用户能通过“http://192.168.1.2”的地址格式访问。

1、配置httpd服务,使其工作在8080端口→重启httpd服务。

```
# vim  /etc/httpd/conf/httpd.conf
……          //省略若干行
Listen  8080     //42行:将httpd监听端口修改为8080
# systemctl  restart  httpd.service
```

2、允许8080与8088端口流量通过dmz区域,立即生效且永久生效;查看对端口的操作是否成功

```
# firewall-cmd  --permanent  --zone=dmz  --add-port=8080-8088/tcp
# firewall-cmd  --reload
```

firewall-cmd配置防火墙

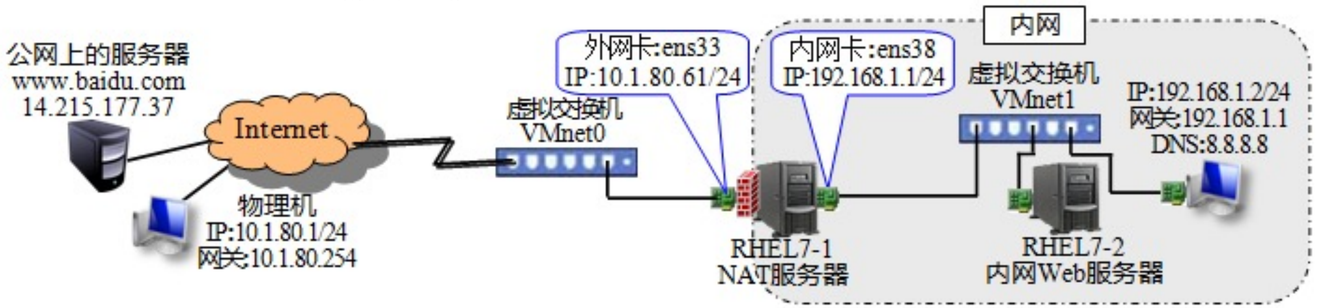
- 为了安全起见,将【例7-14】中的Web服务器工作在8080端口,现要求通过端口转换,让用户能通过“http://192.168.1.2”的地址格式访问。

3、添加一条永久生效的富规则,把从192.168.1.0/24网段进入的数据流的目标80端口转换为8080端口→让以上配置立即生效→查看dmz区域的配置结果

```
# firewall-cmd --permanent --zone=dmz --add-rich-rule="rule family=ipv4 source address=192.168.1.0/24 forward-port port=80 protocol=tcp to-port=8080"
# firewall-cmd --reload
```

firewalld防火墙部署NAT服务

- 部署SNAT和DNAT服务，使得内部网络的计算机均能访问互联网且互联网中的用户能访问内部网络中的Web服务器，网络结构及配置参数如图所示



firewalld防火墙部署NAT服务

- 使用SNAT技术实现共享上网
- SNAT主要通过在连接互联网的外部网卡上配置“伪装”来实现,其步骤如下:

1、在NAT服务器上,开启防火墙→将网络接口ens33移至外部区域(external)→将网络接口ens38移至内部区域(internal),并确保设置永久生效和立即生效。

```
#systemctl  start  firewalld
#firewall-cmd --change-interface=ens38 --
  zone=external --permanent
#firewall-cmd  --change-interface=ens38  --
  zone=external
#firewall-cmd --change-interface=ens33 --
  zone=internal  --permanent
#firewall-cmd  --change-interface=ens33  --
  zone=internal
```

firewalld防火墙部署NAT服务

- 使用SNAT技术实现共享上网

2、查看在外网卡所属的外部区域(external)上是否添加伪装(masquerading)功能(默认已添加),若未添加,则执行添加命令。

```
# firewall-cmd  --list-all  --zone=external
# firewall-cmd  --zone=external  --add-masquerade  --permanent
```

3、在NAT服务器上开启IP转发服务

```
# vim  /usr/lib/sysctl.d/00-system.conf
net.ipv4.ip_forward = 1
# sysctl  -p  /usr/lib/sysctl.d/00-system.conf
```

firewalld防火墙部署NAT服务

- 使用SNAT技术实现共享上网

4、将NAT服务器内部区域(internal)设置为默认区域➡重载防火墙规则,将以上设置的永久状态信息在当前运行下生效。

```
# firewall-cmd  --set-default-zone=internal
# firewall-cmd  --reload
```

5、测试。将内网中的服务器或客户机的默认网关设置为NAT服务器的内网卡的IP地址,若以下ping命令能ping通,表明SNAT服务搭建成功。

```
# ping  -c  2  www.baidu.com
```

firewalld防火墙部署NAT服务

◘ 使用DNAT技术向互联网发布服务器

DNAT服务主要通过不同主机间的“端口转发”(或端口映射)来实现,其配置步骤如下:

1、在内网的RHEL7-2主机(192.168.1.2/24)上搭建好要发布的Web服务器(8080端口)并准备好测试页面➡开启http服务和8080端口,并使其立即生效和永久生效。

```
# firewall-cmd  --permanent  --zone= dmz  --add-
  service=http
# firewall-cmd  --permanent  --zone=dmz  --add-
  port=8080/tcp
# firewall-cmd  --reload
# echo  "DNAT测试"> /var/www/html/index.html
```

firewalld防火墙部署NAT服务

- 使用DNAT技术向互联网发布服务器

2、将流入NAT服务器外网卡ens33(10.1.80.61)的80端口的数据包转发给Web服务器(192.168.1.2)的8080端口。

```
# firewall-cmd --permanent --zone=external --add-
  forward-
  port=port=80:proto=tcp:toport=8080:toaddr=192.168.
  1.2
# firewall-cmd  --reload
```

3、在NAT服务器上开启IP包转发功能。

```
# vim  /usr/lib/sysctl.d/00-system.conf
net.ipv4.ip_forward = 1
# sysctl  -p  /usr/lib/sysctl.d/00-system.conf
```

firewalld防火墙部署NAT服务

- 使用DNAT技术向互联网发布服务器

4、在外网的主机(10.1.80.1),添加一条经过外网卡(10.1.80.61)到内网段192.168.1.0/24的路由。

若是RHEL7主机,则执行以下命令添加路由:

```
# ip route add 192.168.1.0/24 via 10.1.80.61
```

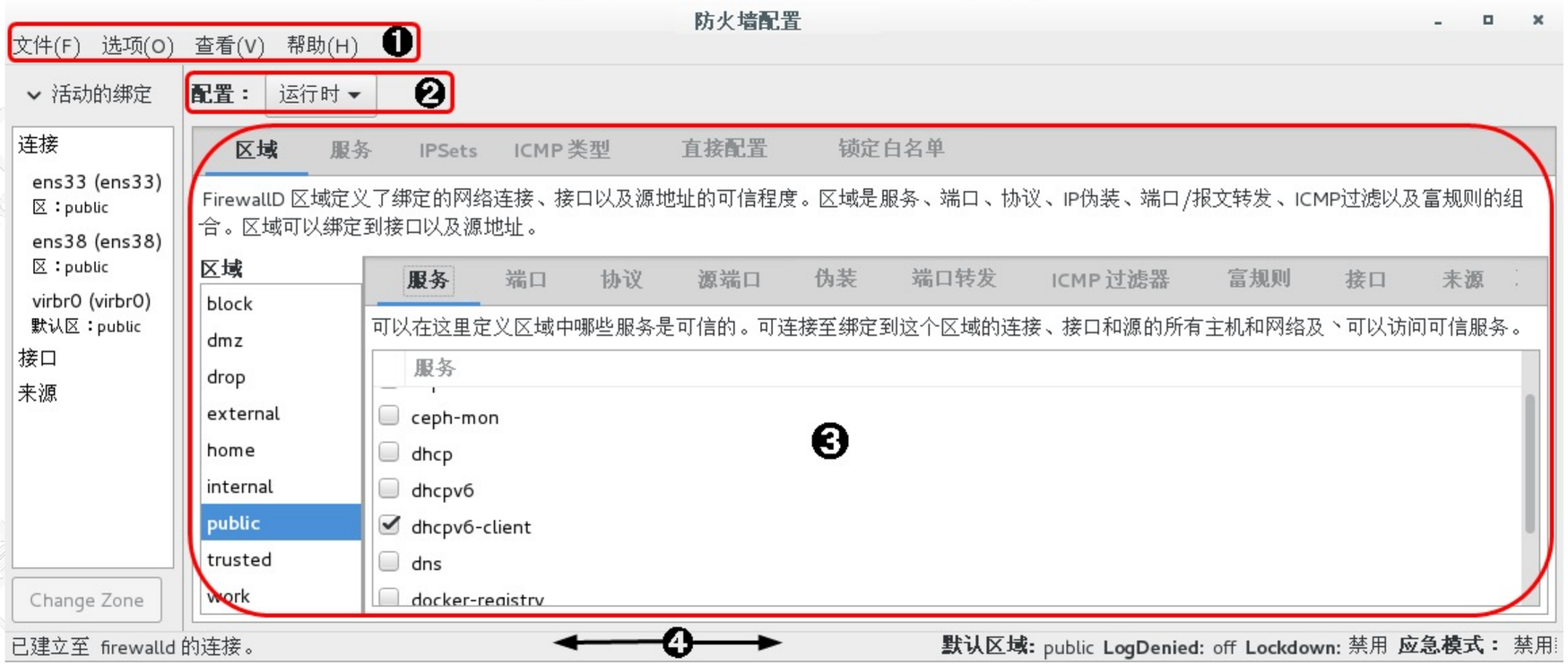
若是Windows主机,则执行以下命令添加永久生效的路由记录:

```
route add -p 192.168.1.0 mask 255.255.255.0 10.1.80.61 metric 1
```

5、测试。在外网(模拟外网)客户机的浏览器地址栏中输入内网Web服务器的地址

firewall-config配置防火墙

- 认识firewall-config的工作界面



firewall-config配置防火墙

认识firewall-config的工作界面

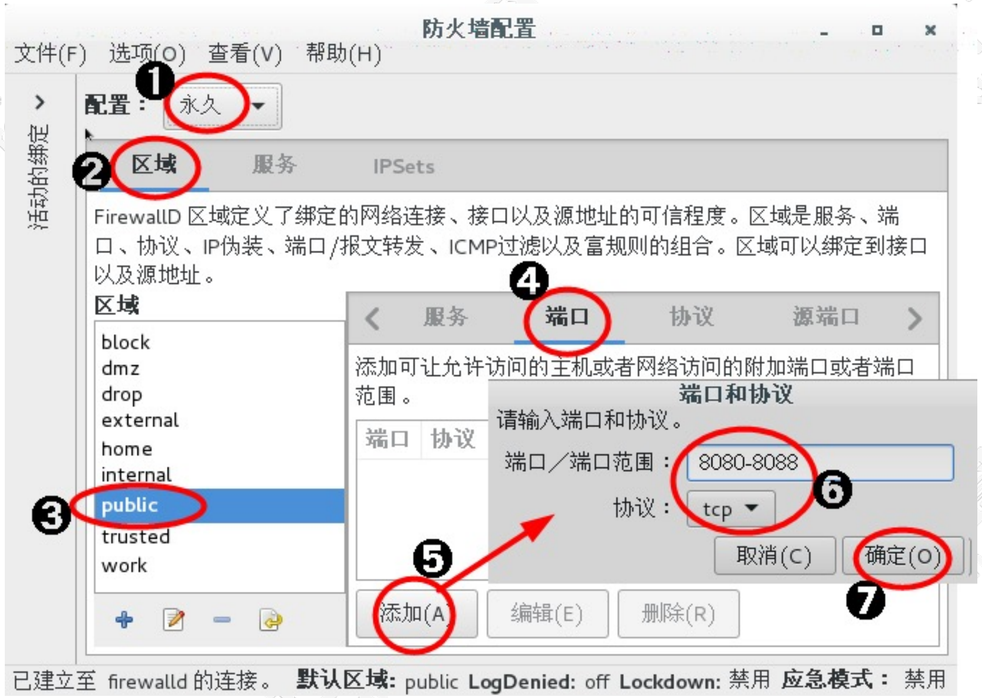
标签名称	标签的设置功能
服务	定义哪些区域的服务是可信的。可信的服务可以绑定该区的任意连接、接口和源地址。
端口	用于添加并设置允许访问的主机或者网络的附加端口或端口范围。
协议	用于添加所有主机或网络均可访问的协议
源端口	添加额外的源端口或范围，它们对于所有可连接至这台主机的所有主机或网络都需要是可以访问的。
伪装	将本地的私有网络的多个IP地址进行隐藏并映射到一个公网IP，伪装功能目前只能适用于 ipv4。
端口转发	将本地系统的(源)端口映射为本地系统或其他系统的另一个(目标)端口，此功能只适应于IPv4
ICMP过滤器	可以选择Internet 控制报文协议的报文。这些报文可以是信息请求亦可是对信息请求或错误条件创建的响应
富规则	用于同时基于服务、主机地址、端口号等多种因素，进行更详细、更复杂的规则设置，优先级最高。
接口	用于为所选区域绑定相应的网络接口(即网卡)

firewall-config配置防火墙

- firewall-config的使用
- 案例：允许其他主机访问本机的http服务，仅当前生效

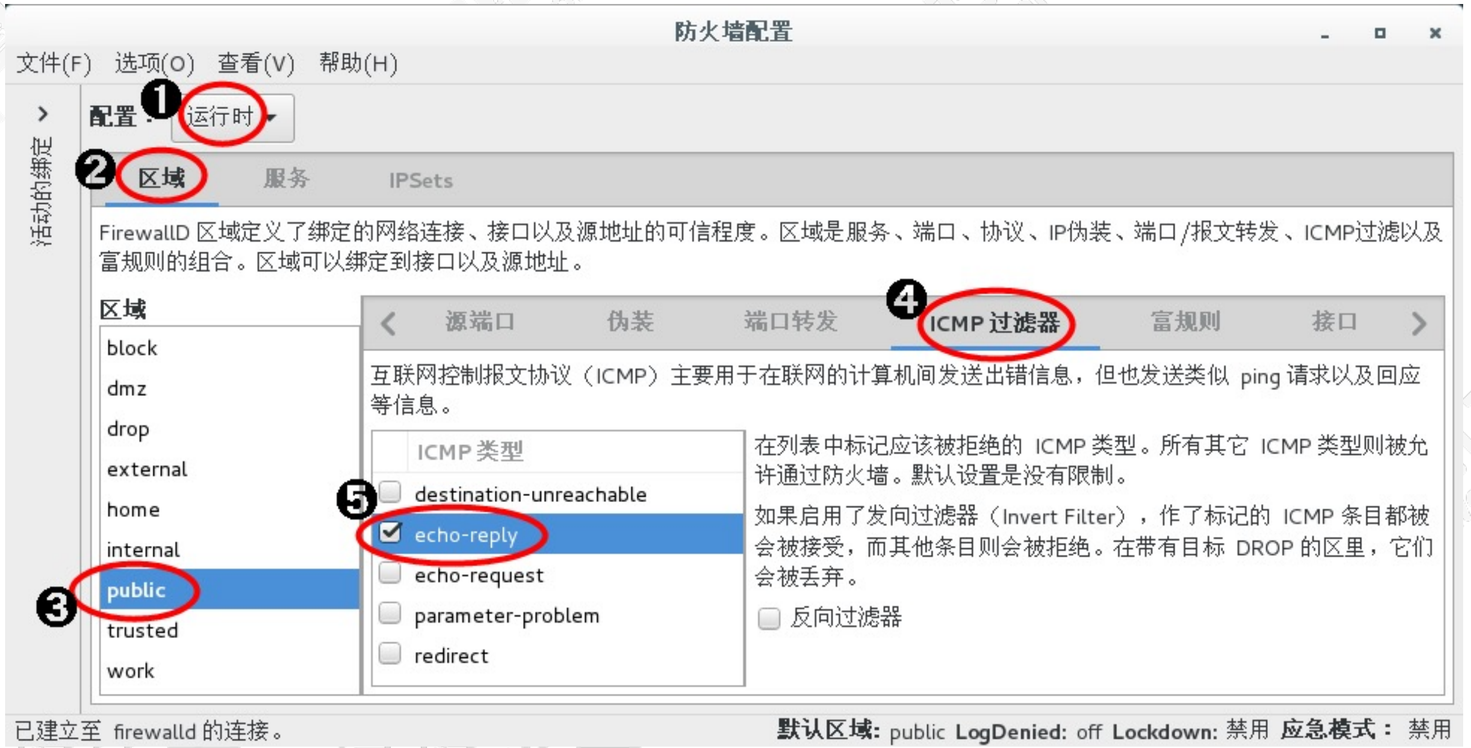
firewall-config配置防火墙

- firewall-config的使用
- 案例：开放本机的8080-8088端口且重启后依然生效。



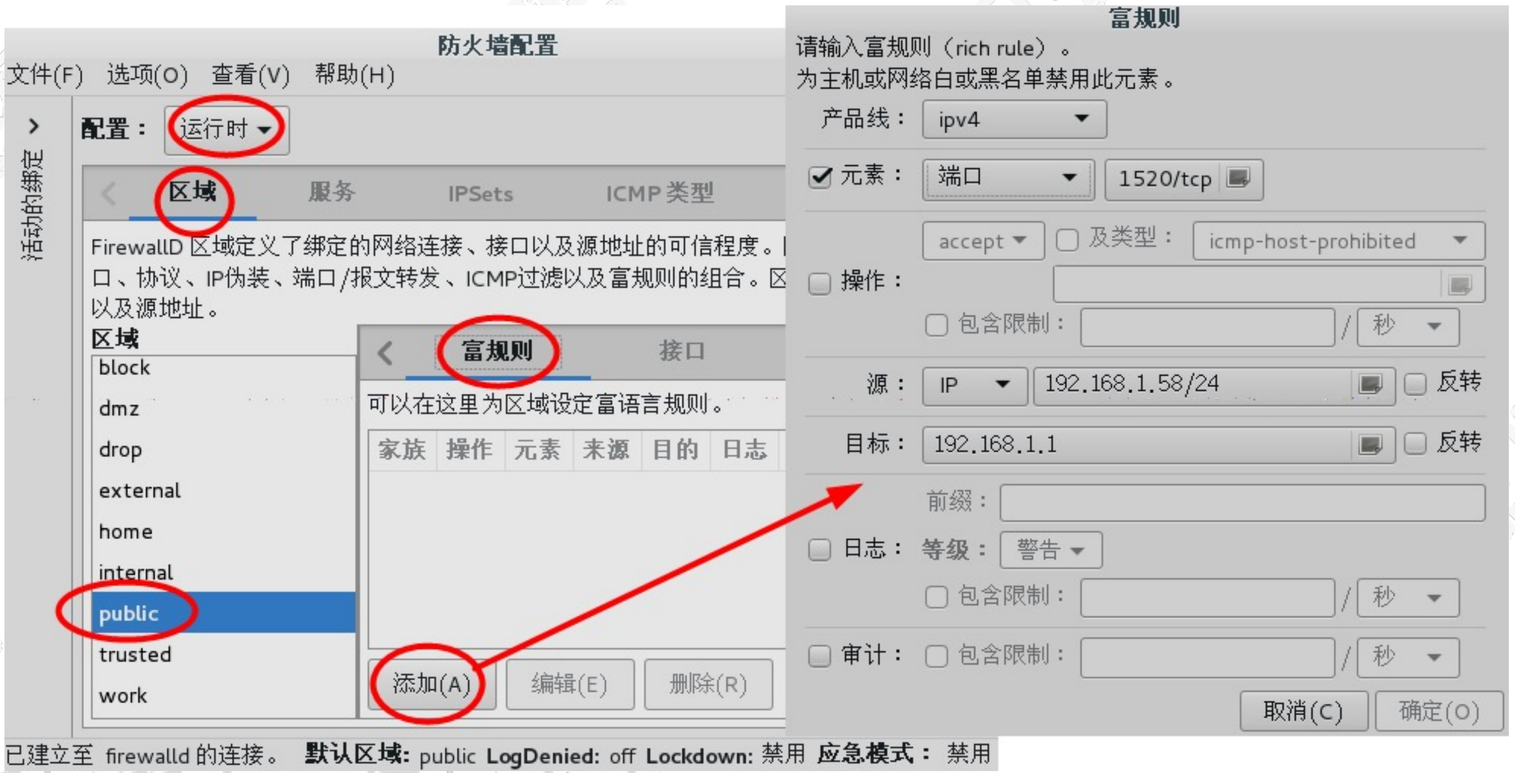
firewall-config配置防火墙

- firewall-config的使用
- 案例：过滤 “echo-reply”的ICMP协议报文数据包，仅当前生效。



firewall-config配置防火墙

- firewall-config的使用
- 案例：仅允许192.168.1.58主机访问本机(192.168.1.1)的1520端口，当前生效。



firewall-config配置防火墙

- firewall-config的使用
- 案例：将本机的网络接口ens38添加到dmz区域，仅运行时生效。

总结

- firewalld简介
- firewalld区域
- firewalld配置
- firewall-cmd配置防火墙
- firewall-config配置防火墙

谢谢观看

更多好课，请关注万门大学APP