项目 4 配置与管理防火墙-实训任务指导书（4-1）

项目任务：配置动态防火墙 Firewalld

firewalld 提供了支持网络/防火墙区域（zone）定义网络链接以及接口安全等级的动态防火墙管理工具——Linux 系统的动态防火墙管理器（Dynamic Firewall Manager of Linux systems）。Linux 系统的动态防火墙管理器拥有基于 CLI（命令行界面）和基于 GUI（图形用户界面）的两种管理方式。

子任务 1：使用终端管理工具实现动态防火墙 Firewalld 配置

子任务 2：使用图形管理工具实现动态防火墙 Firewalld 配置

项目准备

两台虚拟主机，一台为服务器为方便使用主机名设为 server7-1，IP 地址配置为 192.168.10.1/24；另一台为客户端，设置主机名为 client7-2,，IP 地址配置为 192.168.10.20/24；网络模式均设置为桥接模式。

子任务 1. 打开客户机 client7-2，使用终端管理工具实现动态防火墙 Firewalld 配置，实现如下配置

```
[root@client7-2 ~]#  firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: ens33
  sources:
  services: dhcpv6-client http https ssh
  ports: 8088-8089/tcp
  protocols:
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
```

命令行终端是一种极富效率的工作方式，firewall-cmd 是 firewalld 防火墙配置管

理工具的 CLI（命令行界面）版本。

表3-6 firewall-cmd命令中使用的参数以及作用

参　数	作　用
--get-default-zone	查询默认的区域名称
--set-default-zone=<区域名称>	设置默认的区域，使其永久生效
--get-zones	显示可用的区域
--get-services	显示预先定义的服务
--get-active-zones	显示当前正在使用的区域与网卡名称
--add-source=	将源自此IP或子网的流量导向指定的区域
--remove-source=	不再将源自此IP或子网的流量导向某个指定区域
--add-interface=<网卡名称>	将源自该网卡的所有流量都导向某个指定区域
--change-interface=<网卡名称>	将某个网卡与区域关联
--list-all	显示当前区域的网卡配置参数、资源、端口以及服务等信息
--list-all-zones	显示所有区域的网卡配置参数、资源、端口以及服务等信息
--add-service=<服务名>	设置默认区域允许该服务的流量
--add-port=<端口号/协议>	设置默认区域允许该端口的流量
--remove-service=<服务名>	设置默认区域不再允许该服务的流量
--remove-port=<端口号/协议>	设置默认区域不再允许该端口的流量
--reload	让“永久生效”的配置规则立即生效，并覆盖当前的配置规则
--panic-on	开启应急状况模式
--panic-off	关闭应急状况模式

1．打开服务器，主机名设为 server7-1 使用终端管理工具

（1）查看 firewalld 服务当前使用的区域。

```
[root@192 ~]# systemctl start firewalld
[root@192 ~]# firewall-cmd --get-default-zone
public
```

（2）查询 ens33 网卡在 firewalld 服务中的区域。

```
[root@192 ~]# firewall-cmd --get-zone-of-interface=ens33
public
```

（3）把 firewalld 服务中 ens33 网卡的默认区域修改为 external，并在系统重启后生效。分别查看当前与永久模式下的区域名称。

```
[root@client7-3 ~]# systemctl start firewalld
[root@client7-3 ~]# firewall-cmd --permanent --zone=external --change-interface=
ens33
The interface is under control of NetworkManager, setting zone to 'external'.
success
[root@client7-3 ~]# firewall-cmd --get-zone-of-interface=ens33
external
[root@client7-3 ~]# firewall-cmd --permanent --get-zone-of-interface=ens33
external
[root@client7-3 ~]#
```

（4）把 firewalld 服务的当前默认区域设置为 public。

[root@RHEL7-1 ~]# firewall-cmd --set-default-zone=public

success

[root@RHEL7-1 ~]# firewall-cmd --get-default-zone

public

（5）启动/关闭 firewalld 防火墙服务的应急状况模式，阻断一切网络连接（当远程控制服务器时请慎用）。

[root@RHEL7-1 ~]# firewall-cmd --panic-on

success

[root@RHEL7-1 ~]# firewall-cmd --panic-off

Success

验证操作：关闭 firewalld 防火墙时，远程控制服务还能正常使用吗？

（6）查询 public 区域是否允许请求 SSH 和 HTTPS 协议的流量。

[root@RHEL7-1 ~]# firewall-cmd --zone=public --query-service=ssh

yes

[root@RHEL7-1 ~]# firewall-cmd --zone=public --query-service=https

No

（7）把 firewalld 服务中请求 HTTPS 和 http 以及 ftp 协议的流量设置为永久允许，并立即生效。

[root@RHEL7-1 ~]# firewall-cmd --zone=public --add-service=https

success

[root@RHEL7-1 ~]# firewall-cmd --permanent --zone=public --add-service=https

success

[root@RHEL7-1 ~]# firewall-cmd --zone=public --add-service=http

success

[root@RHEL7-1 ~]# firewall-cmd --permanent --zone=public --add-service=http

success

[root@RHEL7-1 ~]# firewall-cmd --zone=public --add-service=ftp

success

[root@RHEL7-1 ~]# firewall-cmd --permanent --zone=public --add-service=ftp

success

[root@RHEL7-1 ~]# firewall-cmd --reload

Success

（8）把 firewalld 服务中请求 HTTP 的流量设置为永久拒绝，并立即生效。

[root@RHEL7-1 ~]# firewall-cmd --permanent --zone=public --remove-service=https

success

[root@RHEL7-1 ~]# firewall-cmd --reload

Success

（9）把 firewalld 服务中请求 FTP 的流量设置为永久拒绝，并立即生效。

[root@RHEL7-1 ~]# firewall-cmd --permanent --zone=public --remove-service=ftp

success

[root@RHEL7-1 ~]# firewall-cmd --reload

success

（10）把在 firewalld 服务中访问 8088 和 8089 端口的流量策略设置为允许，但仅限当前生效。

[root@RHEL7-1 ~]# firewall-cmd --zone=public --add-port=8088-8089/tcp

Success

[root@RHEL7-1 ~]firewall-cmd --permanent --zone=public --add-port=8088-8089/tcp

[root@RHEL7-1 ~]# firewall-cmd --zone=public --list-ports

8088-8089/tcp

使用命令查看动态防火墙 firewalld 的配置结果

```
[root@client7-2 ~]#  firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: ens33
  sources:
  services: dhcpv6-client http https ssh
  ports: 8088-8089/tcp
  protocols:
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
```

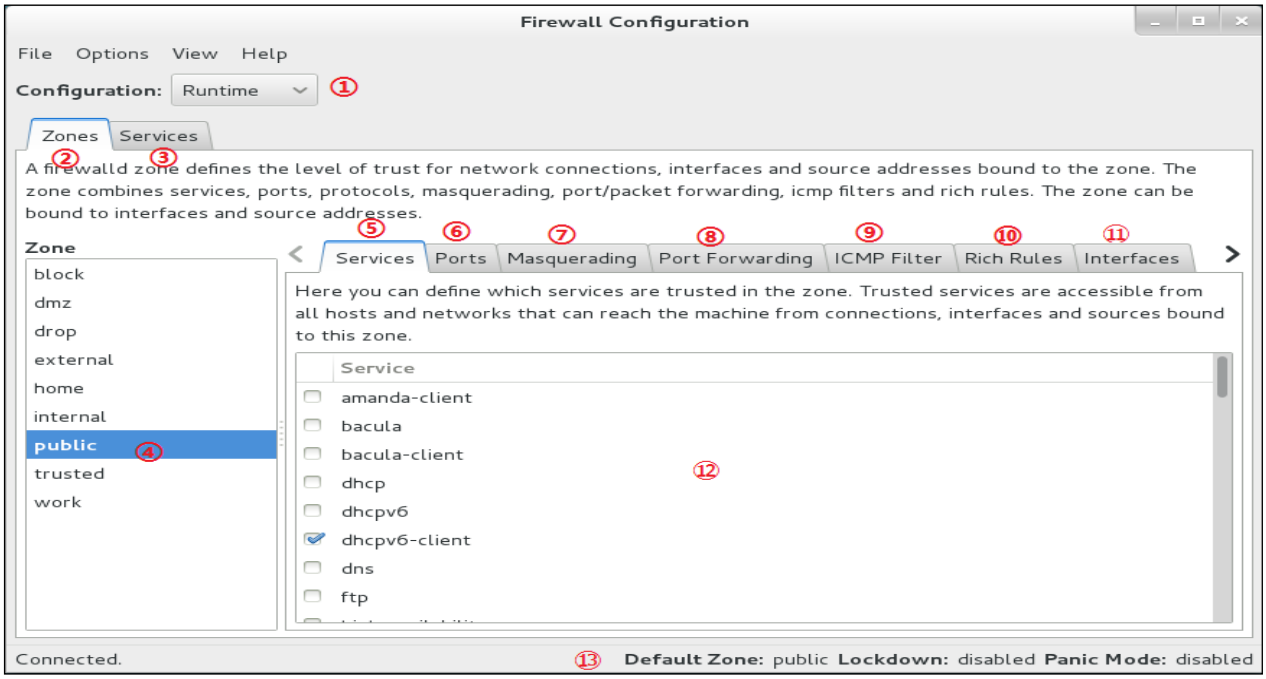
firewalld 中的富规则表示更细致、更详细的防火墙策略配置，它可以针对系统服务、端口号、源地址和目标地址等诸多信息进行更有针对性的策略配置。它的优先级在所有的防火墙策略中也是最高的。

子任务 2．打开服务器 server7—1，使用图形管理工具配置防火墙，完成如下设置：http 服务的流量设置为允许；放行访问 8088～8089 端口（TCP）的流量，并将其设置为永久生效：

具体实训步骤：

在终端中输入命令：firewall-config 或者单击

“Applications”→“Sundry”→“Firewall”命令，打开图 3-4 所示的界面。



① 选择运行时（Runtime）模式或永久（Permanent）模式的配置。

② 可选的策略集合区域列表。

③ 常用的系统服务列表。

④ 当前正在使用的区域。

⑤ 管理当前被选中区域中的服务。

⑥ 管理当前被选中区域中的端口。

⑦ 开启或关闭 SNAT（源地址转换协议）技术。

⑧ 设置端口转发策略。

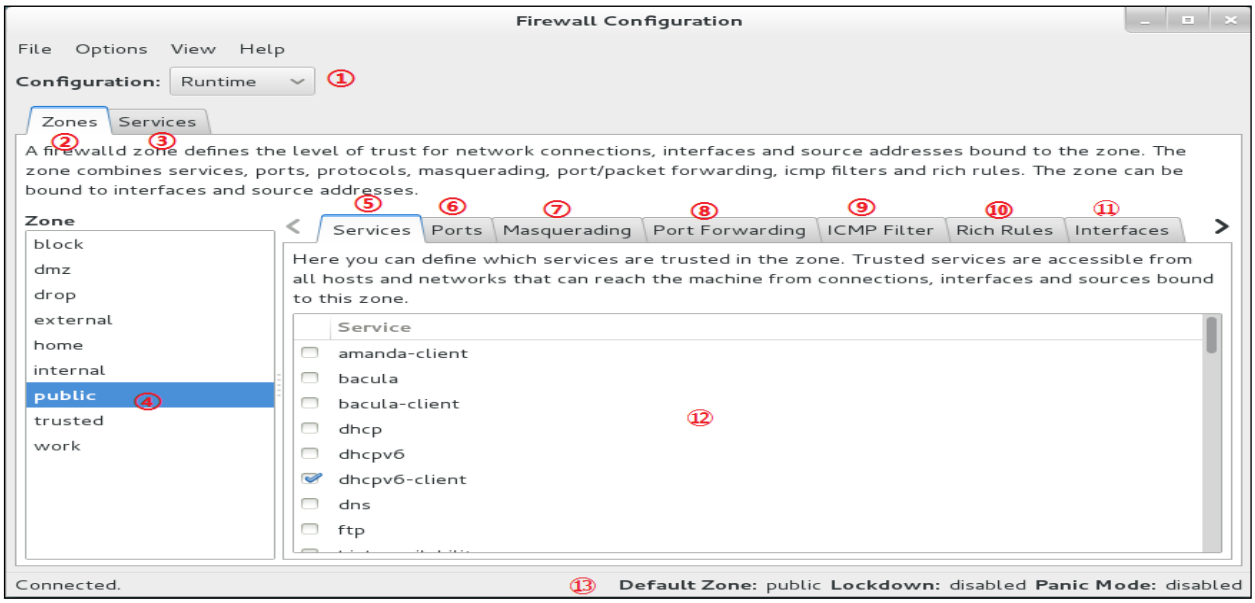
⑨ 控制请求 ICMP 服务的流量。

⑩ 管理防火墙的富规则。

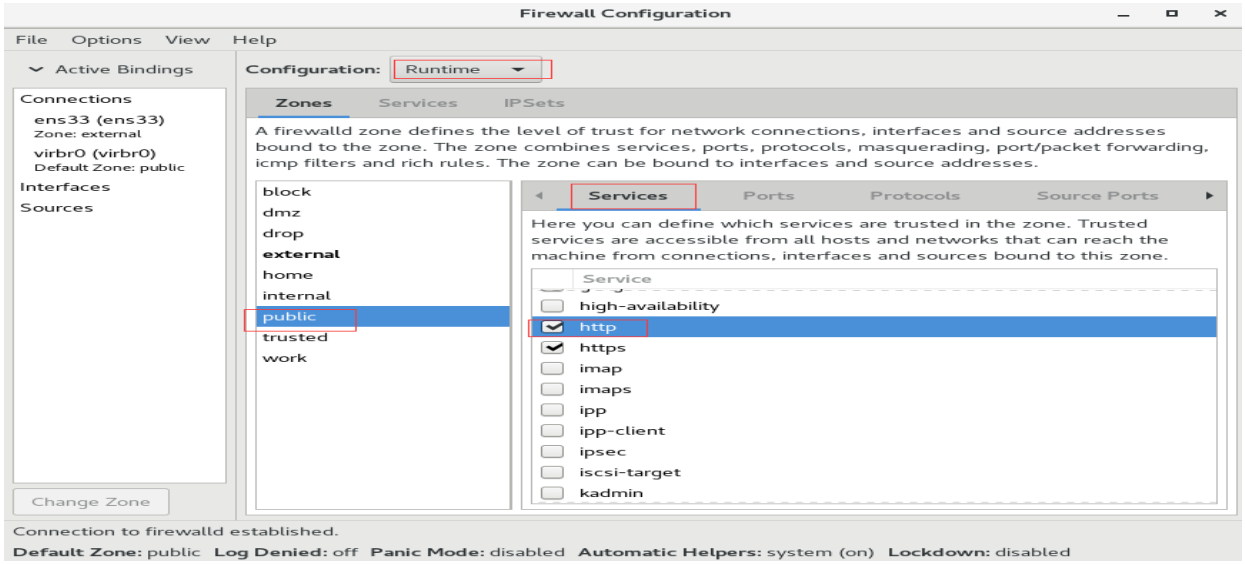
⑪ 管理网卡设备。

⑫被选中区域的服务，若勾选了相应服务前面的复选框，则表示允许与之相关的流量。

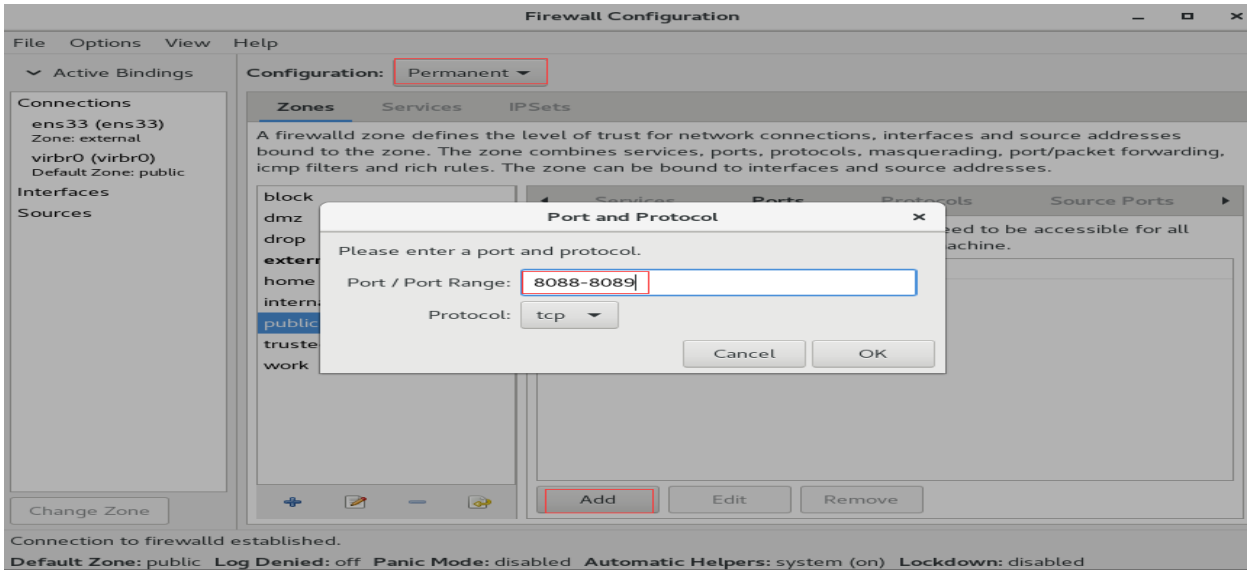
⑬firewall-config 工具的运行状态。

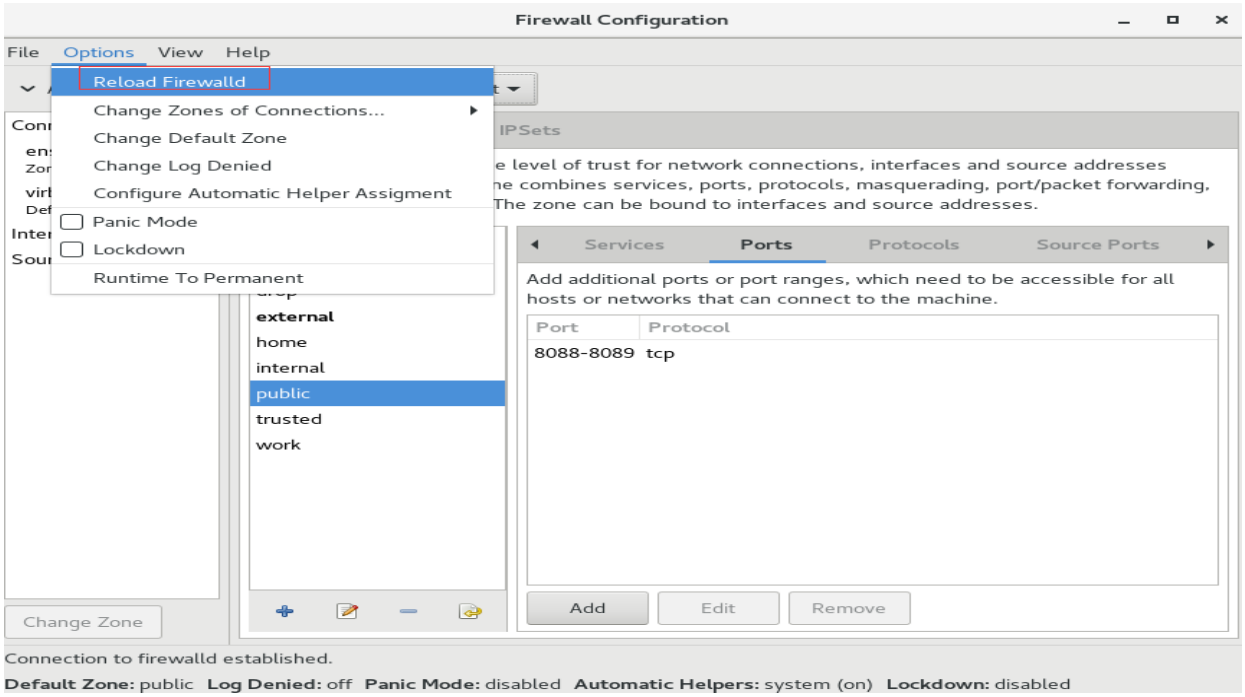


（1）将当前区域中请求 http 服务的流量设置为允许，但仅限当前生效。具体配置如图 3-5 所示。



（2）尝试添加一条防火墙策略规则，使其放行访问 8088～8089 端口（TCP）的流量，并将其设置为永久生效，以达到系统重启后防火墙策略依然生效的目的。按照图 3-6 所示配置完毕，还需要在 Options 菜单中单击 Reload Firewalld 命令，让配置的防火墙策略立即生效，如图 3-7 所示。这与在命令行中执行--reload 参数的效果一样。




Firewall Configuration
File
Options
View
Help
Reload Firewalld
Change Zones of Connections...
Change Default Zone
Change Log Denied
Configure Automatic Helper Assigment
Panic Mode
Lockdown
Runtime To Permanent
IPSets
level of trust for network connections, interfaces and source addresses
combines services, ports, protocols, masquerading, port/packet forwarding,
The zone can be bound to interfaces and source addresses.
external
home
internal
public
trusted
work
Services
Ports
Protocols
Source Ports
Add additional ports or port ranges, which need to be accessible for all hosts or networks that can connect to the machine.
Port
Protocol
8088-8089
tcp
Add
Edit
Remove
Change Zone
Connection to firewalld established.
Default Zone: public
Log Denied: off
Panic Mode: disabled
Automatic Helpers: system (on)
Lockdown: disabled