内容

使用 firewalld 构建 Linux 动态防火墙

曹 江华
2015 年 7 月 08 日发布

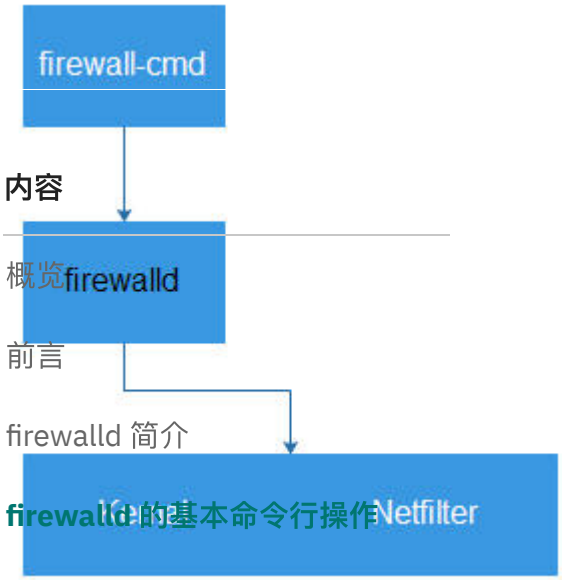
前言

防火墙是 Linux 系统的主要的安全工具，可以提供基本的安全防护，在 Linux 历史上已经使用过 ipchains、iptables。在 Firewalld 中新引入了区域（Zones）这个概念。本文介绍一下使用最新的方法和使用技巧，本文使用的 Linux 发行版本是 RHEL 7.0。

firewalld 简介

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设置以及以太网桥接，并且拥有运行时配置和永久配置选项。它也支持允许服务或者应用程序直的 iptables 防火墙是静态的，每次修改都要求防火墙完全重启。这个过程包括内核 netfilter 防的装载等。而模块的卸载将会破坏状态防火墙和确立的连接。现在 firewalld 可以动态管理防火功能于一身见图 1。

图 1 内核中的防火墙 firewalld 守护进程



firewalld 主要功能

实现动态管理，对于规则的更改不再需要重新创建整个防火墙。

一个简单的系统托盘区图标来显示防火墙状态，方便开启和关闭防火墙。

提供 firewall-cmd 命令行界面进行管理及配置工作。

为 libvirt 提供接口及界面，会在必须的 PolicyKit 相关权限完成的情况下实现。

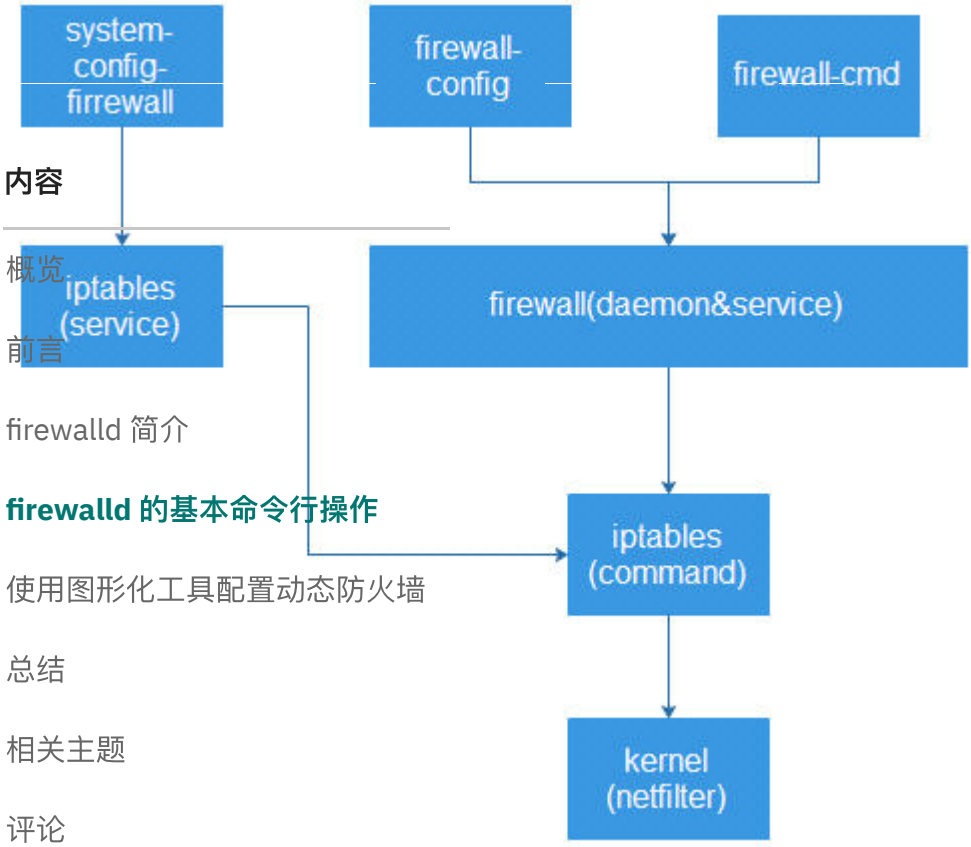
实现 firewall-config 图形化配置工具。

实现系统全局及用户进程的防火墙规则配置管理。

区域支持。

firewalld 防火墙堆栈示意图见图 2，iptables 服务在 /etc/sysconfig/iptables 中储存配置，而 f /usr/lib/firewalld/ 和 /etc/firewalld/ 中的各种 XML 文件里，使用 iptables 的时候每一个单独更 从 /etc/sysconfig/iptables 里读取所有新的规则，使用 firewalld 却不会再创建任何新的规则；firewalld 可以在运行时改变设置而不丢失现行配置。图 5 是 firewalld 防火墙堆栈示意图。

图 2 firewalld 防火墙堆栈示意图



firewalld 的基本命令行操作

安装软件包

```
1 # yum install firewalld firewall-config
```

启动服务

```
1 # systemctl enable firewalld.service
2  # systemctl start firewalld.service
```

查看防火墙状态

```
1 # systemctl status firewalld
2
```

区域管理

网络区域简介

通过将网络划分成不同的区域（通常情况下称为 zones），制定出不同区域之间的访问控制策略
数据流。例如互联网是不可信任的区域，而内部网络是高度信任的区域。以避免安全策略中禁
的任务在不同信任的区域。典型信任的区域包括互联网 (一个没有信任的区域) 和一个内部网络
是提供受控连通性在不同水平的信任区域通过安全政策的运行和连通性模型之间根据最少特权
应该不信任，而家庭有线网络连接就应该完全信任。网络安全模型可以在安装、初次启动和首
模型描述了主机所联的整个网络环境的可信级别，并定义了新连接的处理方式。在 /etc/firewa
连接行到网络接口的预设定。有几种不同的初始化区域：

drop（丢弃）

任何接收的网络数据包都被丢弃，没有任何回复。仅能有发送出去的网络连接。

block（限制）

任何接收的网络连接都被 IPv4 的 icmp-host-prohibited 信息和 IPv6 的 icmp6-adm-prohibite

public（公共）

在公共区域内使用，不能相信网络内的其他计算机不会对您的计算机造成危害，只能接收经过

external（外部）

特别是为路由器启用了伪装功能的外部网。您不能信任来自网络的其他计算，不能相信它们不
收经过选择的连接。

dmz（非军事区）

用于您的非军事区内的电脑，此区域内可公开访问，可以有限地进入您的内部网络，仅仅接收

work（工作）

用于工作区。您可以基本相信网络内的其他电脑不会危害您的电脑。仅仅接收经过选择的连接

home（家庭）

用于家庭网络。您可以基本信任网络内的其他计算机不会危害您的计算机。仅仅接收经过选择

internal（内部）

用于内部网络。您可以基本上信任网络内的其他计算机不会威胁您的计算机。仅仅接受经过选

内容

trusted（信任）

概览

可接受所有的网络连接。

前言

说明：firewalld 的缺省区域是 public。

firewalld 简介

显示支持的区域列表

firewalld 的基本命令行操作

```
1 # firewall-cmd --get-zones
2  block drop work internal external home dmz public trusted
```

设置为家庭区域

```
1 # firewall-cmd --set-default-zone=home
```

查看当前的区域

```
1 #firewall-cmd --get-active-zones
```

设置当前的区域的接口

```
1 #firewall-cmd --get-zone-of-interface=enp03s
```

显示所有公共区域（public）

```
1 # firewall-cmd --zone=public --list-all
```

临时修改网络接口 enp0s3 为 内部区域（internal）

```
1 # firewall-cmd --zone=internal --change-interface=enp03s
```

永久修改网络接口 enp0s3 为 内部区域（internal）

```
1 # firewall-cmd --permanent --zone=internal --change-interface=enp03s
```

服务管理

显示服务列表

内容

概览

amanda 、ftp 、samba 和 tftp 等最重要的服务已被 Firewalld 提供相应的服务，可以使用命令

```
# firewall-cmd --get-services
 cluster-suite pop3s bacula-client smtp ipp radius
 bacula ftp mdns samba dhcpv6-client https
 openvpn imaps samba-client http dns telnet libvirt
 ssh ipsec ipp-client amanda-client tftp-client nfs tftp libvirt-tls

```

使用图形化工具配置动态防火墙

总结

允许 ssh 服务通过

```
# firewall-cmd --enable service=ssh
```

评论

禁止 ssh 服务通过

```
# firewall-cmd --disable service=ssh
```

临时允许 samba 服务通过 600 秒

```
# firewall-cmd --enable service=samba --timeout=600
```

显示当前服务

```
# firewall-cmd --list-services
dhcpv6-client ssh
```

添加 http 服务到内部区域（internal）

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

将一个服务加入到分区

要把一个服务加入到分区，例如允许 SMTP 接入工作区：

```
# firewall-cmd --zone=work --add-service=smtp
```

```
 # firewall-cmd --reload
从一个分区移除服务
```

要从分区移除服务，比如从工作区移除 SMTP：

```
# firewall-cmd --zone=work --remove-service=smtp
 # firewall-cmd --reload
```


端口管理

打开端口

打开 443/tcp 端口在内部区域（internal）：

```
# firewall-cmd --zone=internal --add-port=443/tcp
 # firewall-cmd – reload
```

端口转发

```
# firewall-cmd --zone=external --add-masquerade
 # firewall-cmd --zone=external --add-forward-port=port=22:proto=tcp:toport=37
```

上面的两个命令的意思是，首先启用伪装（masquerade），然后把外部区域（external）的

直接接口设置 firewalld 有一个被称为“direct interface”（直接接口），它可以直接
和 ebtables 的规则。它适用于应用程序，而不是用户。firewalld 保持对所增加项目的
firewalld 和发现由使用直接端口模式的程序造成的更改。直接端口由增加 --direct 选
用。直接端口模式适用于服务或者程序，以便在运行时间内增加特定的防火墙规则。这些规则
过 D-BU S 从 firewalld 接到启动、重新启动和重新加载信息后运用。例如添加端口 tc
cmd --direct --add-rule ipv4 filter INPUT 0 -p tcp --dport 9000 -j AC

firewall-cmd – reload

给复杂防火墙规则配置富规则（Rich Language）

通过“rich language”语法，可以用比直接接口方式更易理解的方法建立复杂防火墙规则。
可以用来配置分区，也仍然支持现行的配置方式。所有命令都必须以 root 用户身份运行。增

```
#firewall-cmd [--zone=zone] --add-rich-rule='rule' [--timeout 9=seconds]
```

```
移除一项规则：
 firewall-cmd [--zone=zone] --remove-rich-rule='rule'
检查一项规则是否存在：
 firewall-cmd [--zone=zone] --query-rich-rule='rule'
```

内容

一个具体例子，假设在一个 IP 地址（192.168.0.0）的服务器配置防火墙允许如下服务 h
PostgreSQL。

概览

前言

```
# firewall-cmd --add-rich-rule 'rule family="ipv4" source address="192.168.0.
 # firewall-cmd --add-rich-rule 'rule family="ipv4" source
  address="192.168.0.0/24" service name="http" accept'
  --permanent
 # firewall-cmd --add-rich-rule 'rule family="ipv4"
 source address="192.168.0.0/24" service name="https"
  accept'
 # firewall-cmd --add-rich-rule 'rule family="ipv4"
  source address="192.168.0.0/24" service name="https"
  accept' --permanent
 # firewall-cmd --add-rich-rule 'rule family="ipv4"
 source address="192.168.0.0/24" service name="vnc-server"
  accept'
 # firewall-cmd --add-rich-rule 'rule family="ipv4"
  source address="192.168.0.0/24" service name="vnc-server"
   accept' --permanent
 # firewall-cmd --add-rich-rule 'rule family="ipv4"
 source address="192.168.0.0/24" service name="postgresql"
 accept'
 # firewall-cmd --add-rich-rule 'rule family="ipv4"
 source address="192.168.0.0/24" service name="postgresql"
  accept' --permanent
 # firewall-cmd --reload
```

在防火墙配置文件中创建自己的服务

首先假设这里笔者需要建立的服务是 RTMP（RTMP 是 Real Time Messaging Protocol
写。该协议基于 TCP）端口号 1935。在 /etc/firewalld/services/ 目录中，利用现
板。

```
# cd /etc/firewalld/services/
```

说明：该目录中存放的是定义好的网络服务和端口参数，只用于参考，不能修改。这个目录中
该目录中没有定义的网络服务，也不必再增加相关 xml 定义，后续通过管理命令可以直接增

```
# cp /usr/lib/firewalld/services/nfs.xml /etc/firewalld/services/
```

说明：从上面目录中将需要使用的服务的 xml 文件拷至这个目录中，如果端口有变化则可以

```
# cd /etc/firewalld/services/

下面修改 nfs.xml 为 rtmp.xml
 #mv nfs.xml rtmp.xml
下面使用 vi 编辑器修改 rtmp.xml 文件为如下内容
```

清单 1. rtmp.xml 文件内容

```
<?xml version="1.0" encoding="utf-8"?>
 <service>
 <short>rtmp services</short>
 <description>RTMP Stream </description>
 <port protocol="tcp" port="1935"/>
 </service>
```

使用图形化工具配置动态防火墙

总结

每一个服务定义都需要一个简短的名字、描述和端口网络用于指定需要使用的协议、端口和模块则中。

相关主题

```
# firewall-cmd --add-service=rtmp
# firewall-cmd --add-service=rtmp --permanent
# firewall-cmd – reload
```

关闭 firewalld 服务

您也可以关闭目前还不熟悉的 Firewalld 防火墙，使用老的 iptables，步骤如下：

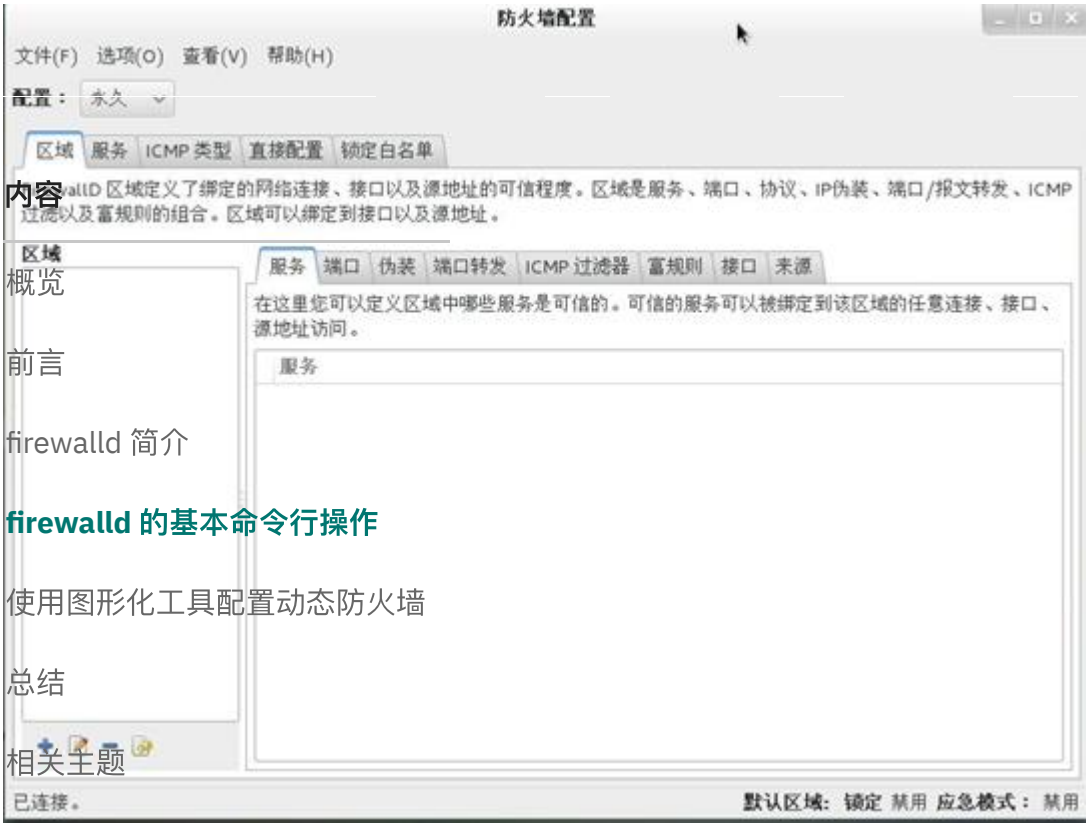
```
# systemctl stop firewalld
 # systemctl disable firewalld
 # yum install iptables-services
 # systemctl start iptables
 # systemctl enable iptables
```

使用图形化工具配置动态防火墙

firewall-config 简介

firewall-config 支持防火墙的所有特性。管理员可以用它来改变系统或用户策略。通过置防火墙允许通过的服务、端口 、伪装 、端口转发 、和 ICMP 过滤器和调整 zone（区域的自由、安全和强健。firewall-config 工作界面见图 3。

图 3. firewall-config 工作界面



firewall-config 工作界面分成三个部分：上面是主菜单，中间是配置选项卡。下面是区域设置选项卡。最底部是状态栏（状态栏显示四个信息：从左到右以此是连接状态、默认区域、左下方角落寻找“已连接”字符，这标志着 **firewall-config**工具已经连接到用户区后台程序**型**、直接配置 **（Direct Configuration）**和锁定白名单 **（Lockdown Whitlist）**标签才能看见。

firewall-config 主菜单

firewall-config 主菜单包括四个选项：文件，选项，查看，帮助。其中选项子菜单是最主

重载防火墙：重载防火墙规则。例如所有现在运行的配置规则如果没有在永久配置中操作，那

更改连接区域：更改网络连接的默认区域。

改变默认区域：更改网络连接的所属区域和接口。

应急模式：应急模式意味着丢弃所有的数据包。

锁定：锁定可以对防火墙配置就行加锁，只允许白名单上的应用程序进行改动。锁定特性为 f或者服务配置的简单配置方式。它是一种轻量级的应用程序策略。

配置选项卡

firewall-config 配置选项卡包括：运行时和永久。

运行时：运行时配置为当前使用的配置规则。运行时配置并非永久有效，在重新加载时可以被
时，这些选项将会丢失。

内容

永久：永久配置规则在系统或者服务重启的时候使用。永久配置存储在配置文件种，每次机器
自动恢复。

概览

前言

firewalld 简介

区域选项卡

firewalld 的基本命令行操作

区域选项卡是一个主要设置界面：

使用图形化工具配置动态防火墙

总结

网络或者防火墙区域定义了连接的可信程度。firewalld 提供了几种预定义的区域。区域配
firewall.zone(5) 的手册里查到。这里的区域是服务、端口、协议、伪装、ICMP 过滤等
和源地址。服务子选项卡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

相关主题

4

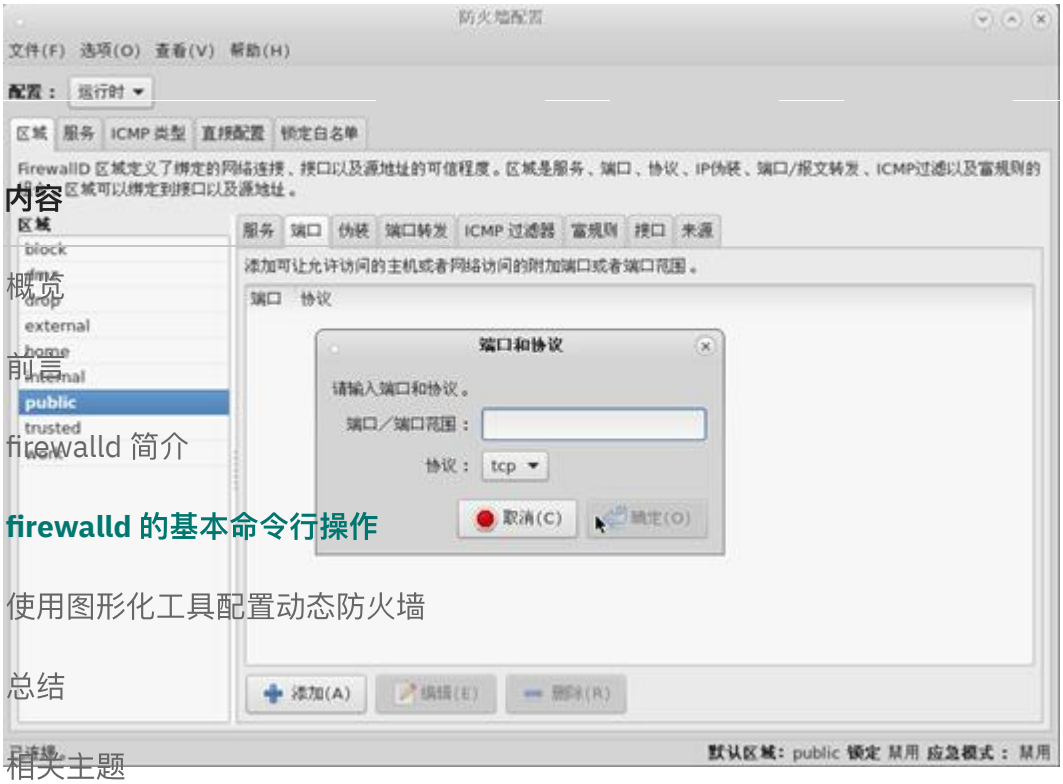
评论

图 4. 服务选项卡

端口子选项卡

端口子选项卡用来设置允许主机或者网络访问的端口范围，配置界面见图 5。

图 5. 端口子选项卡



内容

概览

前言

firewalld 简介

firewalld 的基本命令行操作

使用图形化工具配置动态防火墙

总结

相关主题

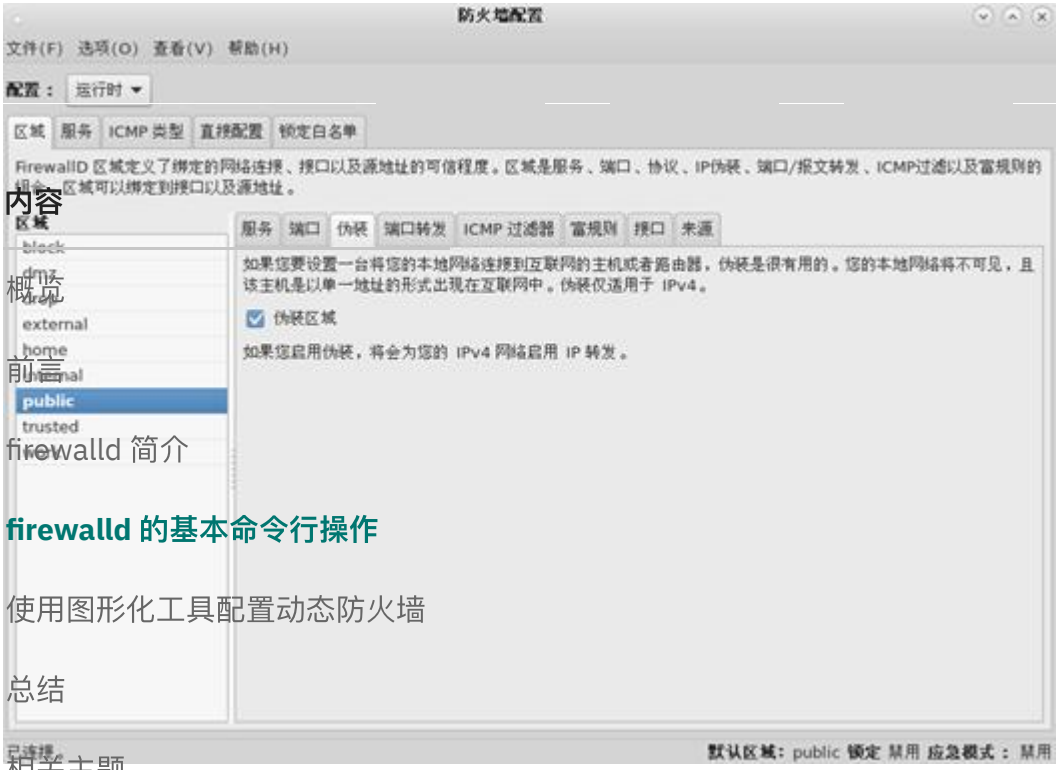
要允许流量通过防火墙到达某个端口，则启动 firewall-config 并选择您想更改设定的网络连接的 添加 按钮，Port and Protocol 就打开了。

输入端口数量或者端口号范围，获得许可。从下拉菜单中选择 tcp 或者 udp。

伪装子选项卡

伪装子选项卡用来把私有网络地址可以被映射到公开的 IP 地址。目前只能适用于 Ipv4，配

图 6. 伪装子选项卡

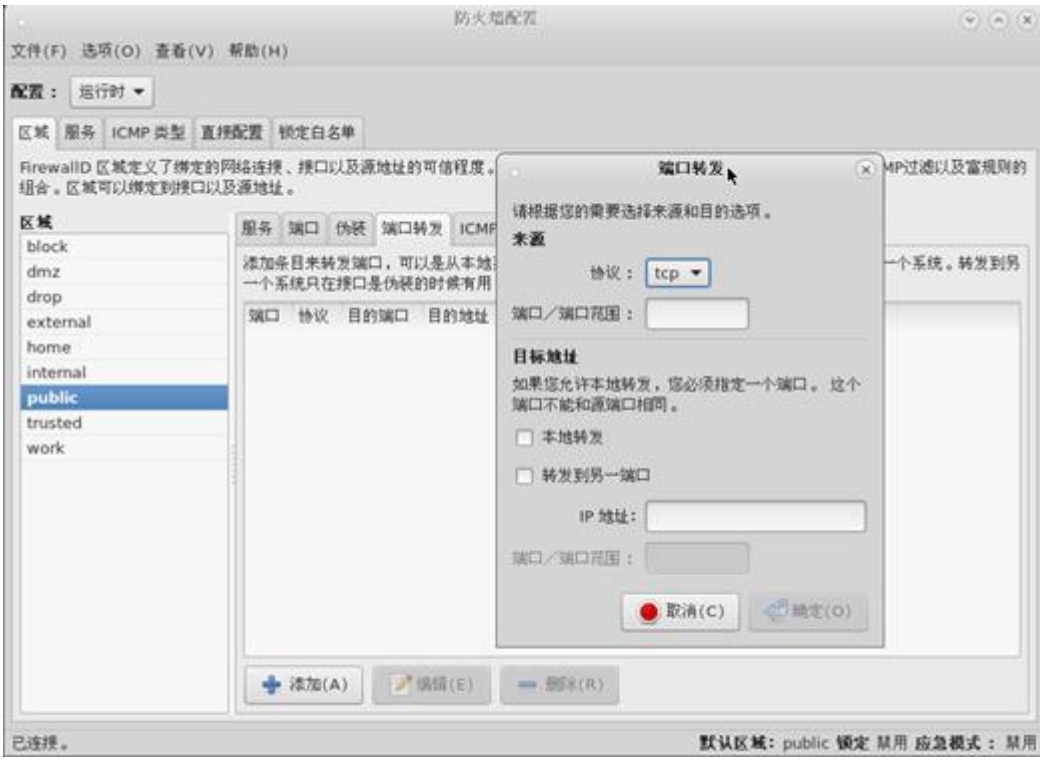


要将 IPv4 地址转换为一个单一的外部地址，则启动 **firewall-config**工具并选择需要转签和复选框以便把 IPv4 地址转换成一个单一的地址。

端口转发子选项卡

端口转发可以映射到另一个端口以及 / 或者其他主机，配置界面见图 7。

图 7 . 端口转发子选项卡



为一个特定端口转发入站网络流量或“packets”到一个内部地址或者替代端口，首先激活伪装
签。在窗口靠上部分选择入站流量协议和端口或者端口范围。靠下部分是用于设置目的端口细

要转发流量到一个本地端口即同一系统上的端口，需选择本地转发复选框，输入要转发的流量
发流量到其他的 IPv4 地址，则选择转发到另一个端口复选框，输入目的地 IP 地址和端口
则默认发送到同一个端口。点击 确定按钮执行更改。

ICMP 过滤器子选项卡

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
配置界面见图 8。

图 8. ICMP 过滤器子选项卡

要使用或者禁用一个 ICMP 过滤，则启动 firewall-config 工具并选择要过滤其信息的网
图标并选择每种您需要过滤的 ICMP 信息类型的复选框。清除复选框以禁用过滤。这种设定是

直接配置选项卡

直接配置选项卡包括三个子选项卡：链、规则和穿通见图 9。说明一下这个选项卡主要用于服
规则。这些规则并非永久有效，并且在收到 firewalld 通过 D-Bus 传递的启动、重启、重

图 9. 直接配置选项卡

内容

改变防火墙设置

要立刻改变现在的防火墙设置，须确定当前视图设定在 运行时。或者，从下拉菜单中选择永久
下次启动系统或者防火墙重新加载时执行的设定。

在运行时（**Runtime**）模式下更改防火墙的设定时，一旦您启动或者清除连接服务器的复选框
模式下更改防火墙的设定，仅仅在重新加载防火墙或者系统重启之后生效。可以使用 **文件**菜单
项菜单，选择 **重新加载防火墙**。

图 10. 从下拉菜单中选择永久（Permanent）

修改默认分区

要设定一个将要被分配新接口的分区作为默认值，则启动 **firewall-config**，从菜单栏选择
默认区域，出现默认区域窗口见图 11。从给出的列表中选择您需要用的分区作为默认分区，点

图 11．修改默认分区