第二十章：Firewalld防火墙应用

**重点：**

**一、概述；**

**概述：**Filewalld（动态防火墙）作为redhat7系统中变更对于netfilter内核模块的管理工具；

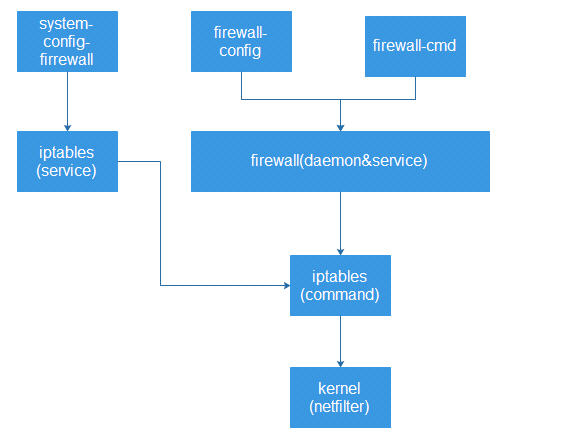
**差异点：**

**前者：iptables 防火墙：**

iptables service 管理防火墙规则的模式（静态）：用户将新的防火墙规则添加进 /etc/sysconfig/iptables 配置文件当中，再执行命令 /etc/init.d/iptables reload 使变更的规则生效。在这整个过程的背后，iptables service 首先对旧的防火墙规则进行了清空，然后重新完整地加载所有新的防火墙规则，如果加载了防火墙的模块，需要在重新加载后进行手动加载防火墙的模块；

**后者：firewalld防火墙：**

使用 python 语言开发，管理防火墙规则的模式（动态）:任何规则的变更都不需要对整个防火墙规则列表进行重新加载，只需要将变更部分保存并更新到运行中的 iptables 即可。还有命令行和图形界面配置工具，它仅仅是替代了 iptables service 部分，其底层还是使用 iptables 作为防火墙规则管理入口。



**二、Frewalld 的原理；**

**便于理解：**

firewalld支持动态更新技术并加入了区域（zone）的概念：

简单来说，区域就是firewalld预先准备了几套防火墙策略集合（策略模板），用户可以根据生产场景的不同而选择合适的策略集合，从而实现防火墙策略之间的快速切换。例如，我们有一台笔记本电脑，每天都要在办公室、咖啡厅和家里使用。按常理来讲，这三者的安全性按照由高到低的顺序来排列，应该是家庭、公司办公室、咖啡厅。

当前，我们希望为这台笔记本电脑指定如下防火墙策略规则：

在家中允许访问所有服务；

在办公室内仅允许访问文件共享服务；

在咖啡厅仅允许上网浏览。

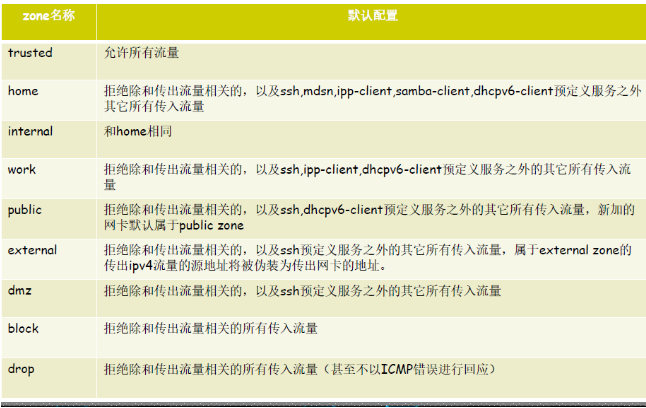
在以往，我们需要频繁地手动设置防火墙策略规则，而现在只需要预设好区域集合，

然后只需轻点鼠标就可以自动切换了，从而极大地提升了防火墙策略的应用效率。

**区域：**

zone 默认共有9个：block（拒绝）dmz（非军事化） drop（丢弃） external（外部） home（家庭） internal（内部） public（公开） trusted（信任） work（工作区）

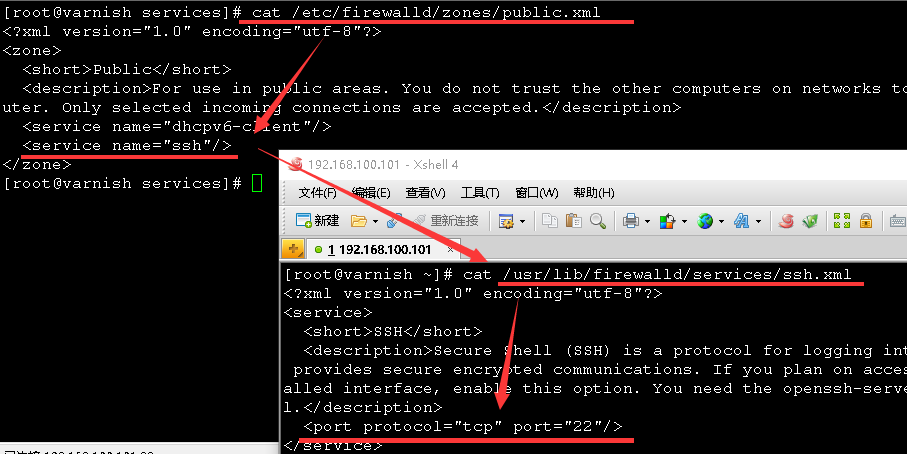
不同的区域之间的差异是其对待数据包的默认行为不同，firewalld的默认区域为public；



**相关文件：**

/usr/lib/firewalld/services/：firewalld服务默认在此目录下定义了70+种服务供我们使用；

/etc/firewalld/zones/：默认区域配置文件，配置文件中指定了编写完成的规则（规则中的服务名必须与上述文件名一致，调用关系）；



**三、规则编写：**

**语法：**firewall-cmd [选项]

**选项语法：**[--zone=zone] 动作 [--permanent]

注：如果不指定--zone选项，则为当前所在的默认区域；

--permanent选项为是否将改动写入到区域配置文件中，如果加此选项，需要重新加载firewalld服务方可生效；

**选项之状态：**

--state ##查看防火墙的状态

--reload ##重新加载防火墙，中断用户的连接，将临时配置清掉，加载配置文件中的永久配置

--complete-reload ##重新加载防火墙，不中断用户的连接（防火墙出严重故障时使用）

--panic-on ##紧急模式，强制关闭所有网络连接,--panic-off是关闭紧急模式

**选项之动作中查看操作：**

--get-icmptypes ##查看支持的所有ICMP类型

--get-zones ##查看所有区域

--get-default-zone ##查看当前的默认区域

--get-active-zones ##查看当前正在使用的区域

--get-services ##查看当前区域支持的服务

--list-services ##查看当前区域开放的服务列表

--list-all ##查看此区域内的所有配置，类似与iptables -L -n

**选项之更改区域操作：**

--set-default-zone=work ##更改默认的区域

**选项之新建--add或删除--remove规则：**

--add-interface=eth0 ##将网络接口添加到默认的区域内

--add-port=12222/tcp --permanent ##添加端口到区域开放列表中

--add-port=5000-10000/tcp --permanent ##将端口范围添加到开放列表中；

--add-service=ftp --permanent ##添加服务到区域开放列表中（注意服务的名称需要与此区域支持的服务列表中的名称一致）

--add-source=192.168.1.1 ##添加源地址的流量到指定区域

--remove-source=192.168.1.1 ##删除源地址的流量到指定区域

--change-interface=eth1 ##改变指定的接口到其他区域

--remove-service=http ##在home区域内将http服务删除在开放列表中删除

--add-masquerade ##开启SNAT（源地址转换）

--query-masquerade ##查询SNAT的状态

--remove-interface=eth0 ##将网络接口在默认的区域内删除

--query-interface=eth0 ##确定该网卡接口是否存在于此区域

**Rich规则：**

当基本firewalld语法规则不能满足要求时，可以使用以下更复杂的规则

.rich-rules 富规则，功能强,表达性语言,查看帮助：man 5 firewalld.richlanguage

.rich规则比基本的firewalld语法实现更强的功能，不仅实现允许/拒绝，还可以实现日志syslog和auditd，也可以实现端口转发，伪装和限制速率

rich规则实施顺序有以下四点

a.该区域的端口转发，伪造规则

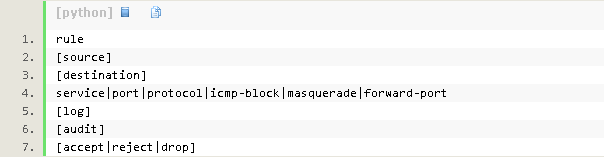
b.该区域的日志规则

c.该区域的允许规则

d.该区域的拒绝规则

每个匹配的规则都生效，所有规则都不匹配，该区域默认规则生效；

**Rich规则语法**：



**Rich规则选项：**

--add-rich-rule=’rule’ ##新建rich规则

--remove-rich-rule=’rule’ ##删除rich规则

--query-rich-rule=’rule’ ##查看单条rich规则

--list-rich-rules ##查看rich规则列表

**Rich规则示例：**

1.拒绝从192.168.100.0的ping流量；

firewall-cmd --zone=public --add-rich-rule='rule family=ipv4 source address=192.168.100.0/24 protocol value='icmp' reject

2.接受所有192.168.1.0/24子网端口范置7900-7905的TCP流量；

firewall-cmd  --permanent --zone=vnc  --add-rich-rule=‘rule family=ipv4 source address=192.168.1.0/24  port  port=7900-7905 protocol=tcp accept‘

3.开启SNAT；

firewall-cmd   --permanent --add-rich-rule=‘rule family=ipv4 source address=192.168.0.0/24 masquerade‘

4.拒绝192.168.100.100主机ping的流量（0代表优先级）；

firewall-cmd --direct --add-rule ipv4 filter INPUT 0 -s 192.168.100.100 -p icmp -j DROP

5.允许当前的数据包的状态；

firewall-cmd --direct --add-rule ipv4 filter INPUT 0 -m state --state RELATED,ESTABLISHED -j ACCEPT