iptables基础

规则（rules）其实就是网络管理员预定义的条件，规则一般的定义为"如果数据包头符合这样的条件，就这样处理这个数据包"。规则存储在内核空间的信息 包过滤表中，这些规则分别指定了源地址、目的地址、传输协议（如TCP、UDP、ICMP）和服务类型（如HTTP、FTP和SMTP）等。当数据包与规 则匹配时，iptables就根据规则所定义的方法来处理这些数据包，如放行（accept）、拒绝（reject）和丢弃（drop）等。配置防火墙的 主要工作就是添加、修改和删除这些规则。

规则链：

1.INPUT ——进来的数据包应用此规则链中的策略
2.OUTPUT ——外出的数据包应用此规则链中的策略
3.FORWARD ——转发数据包时应用此规则链中的策略
4.PREROUTING ——对数据包作路由选择前应用此链中的规则
（记住！所有的数据包进来的时侯都先由这个链处理）
5.POSTROUTING ——对数据包作路由选择后应用此链中的规则
（所有的数据包出来的时侯都先由这个链处理）

-A 在指定链的末尾添加（append）一条新的规则 -D 删除（delete）指定链中的某一条规则，可以按规则序号和内容删除 -I 在指定链中插入（insert）一条新的规则，默认在第一行添加 -R 修改、替换（replace）指定链中的某一条规则，可以按规则序号和内容替换 -L 列出（list）指定链中所有的规则进行查看 -E 重命名用户定义的链，不改变链本身 -F 清空（flush） -N 新建（new-chain）一条用户自己定义的规则链 -X 删除指定表中用户自定义的规则链（delete-chain） -P 设置指定链的默认策略（policy） -Z 将所有表的所有链的字节和数据包计数器清零 -n 使用数字形式（numeric）显示输出结果 -v 查看规则表详细信息（verbose）的信息 -V 查看版本(version) -h 获取帮助（help）

规则表之间的优先顺序：
Raw——mangle——nat——filter
规则链之间的优先顺序（分三种情况）：
第一种情况：入站数据流向
从外界到达防火墙的数据包，先被PREROUTING规则链处理（是否修改数据包地址等），之后会进行路由选择（判断该数据包应该发往何处），如果数据包 的目标主机是防火墙本机（比如说Internet用户访问防火墙主机中的web服务器的数据包），那么内核将其传给INPUT链进行处理（决定是否允许通 过等），通过以后再交给系统上层的应用程序（比如Apache服务器）进行响应。
第二冲情况：转发数据流向

来自外界的数据包到达防火墙后，首先被PREROUTING规则链处理，之后会进行路由选择，如果数据包的目标地址是其它外部地址（比如局域网用户通过网 关访问QQ站点的数据包），则内核将其传递给FORWARD链进行处理（是否转发或拦截），然后再交给POSTROUTING规则链（是否修改数据包的地 址等）进行处理。
第三种情况：出站数据流向
防火墙本机向外部地址发送的数据包（比如在防火墙主机中测试公网DNS服务器时），首先被OUTPUT规则链处理，之后进行路由选择，然后传递给POSTROUTING规则链（是否修改数据包的地址等）进行处理。

iptables 的安装与配置

由于centos7默认是使用firewall作为防火墙，下面介绍如何将系统的防火墙设置为iptables。

```
#停止firewall
systemctl stop firewall.service
#禁止firewall开机启动
systemctl disable firewall.service
```

#安装iptables

```
yum install iptables-services
```

#编辑防火墙文件 （建议都在配置文件配置，不要命令配置）

```
vi /etc/sysconfig/iptables
```

#添加80和3306端口 等等（自己配置）

```
-A INPUT -m state –state NEW -m tcp -p tcp –dport 80 -j ACCEPT          #80端口开放
-A INPUT -m state –state NEW -m tcp -p tcp –dport 3306 -j ACCEPT        #3306端口开放
-I INPUT -s 113.106.93.110 -p tcp --dport 8089 -j DROP                  #禁止指定IP访问 8089
-I INPUT -s 113.106.93.110 -p tcp --dport 8080 -j ACCEPT                #开放固定ipIP访问 8080
```

#重启防火墙使配置文件生效

```
systemctl restart iptables.service
```

#设置iptables防火墙为开机启动项

```
systemctl enable iptables.service
```

```
service iptables  start        #启动服务
service iptables  stop         #停止服务
service iptables  restart      #重启服务
```

关闭SELINUX

```
vi /etc/selinux/config
  #注释以下配置
  SELINUX=enforcing
  SELINUXTYPE=targeted

  #增加以下配置
  SELINUX=disabled

  #使配置立即生效
  setenforce 0
```

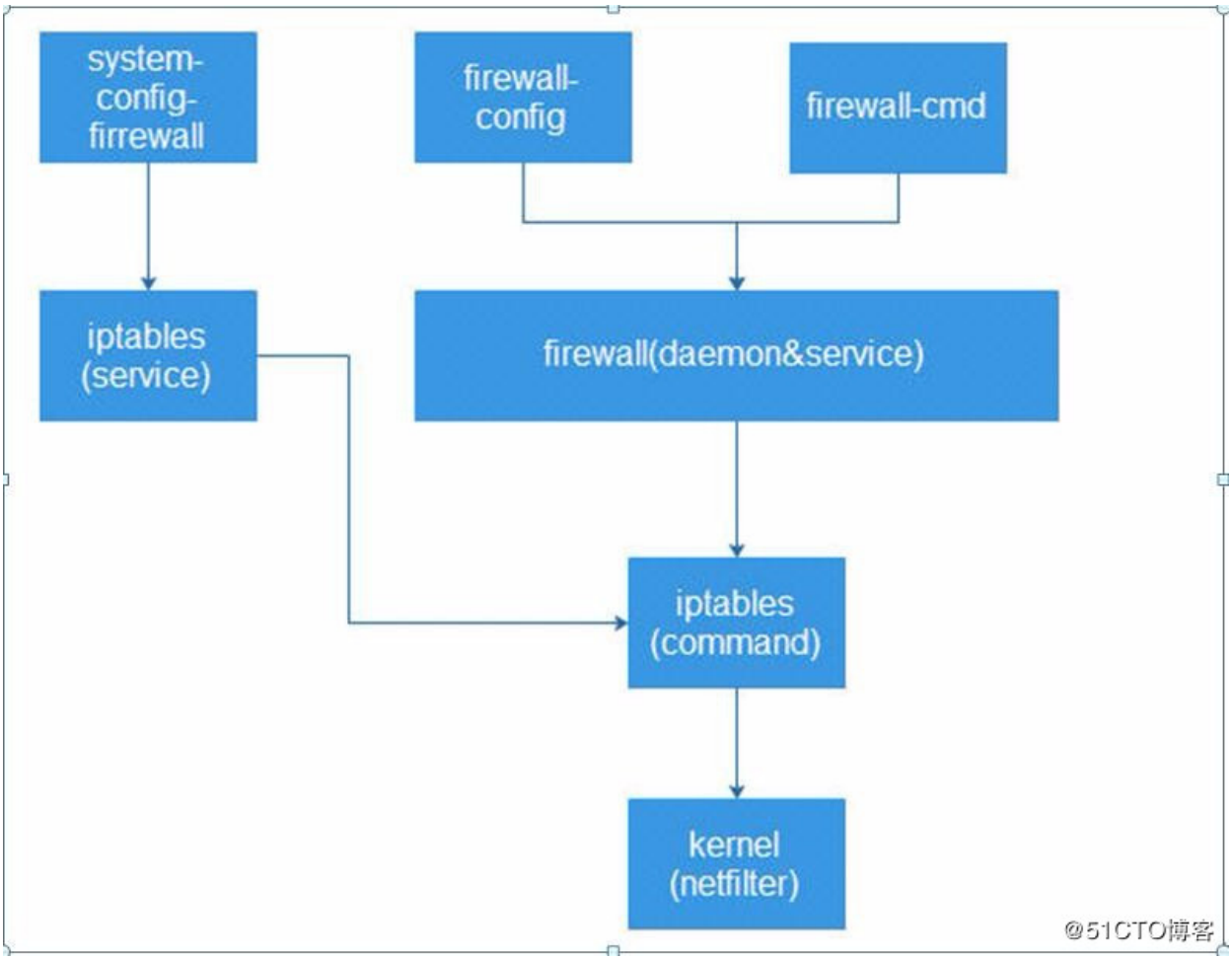
Centos7-----firewalld详解

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;

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；
firewalld 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。
firewalld 使用 python 语言开发，在新版本中已经计划使用 c++ 重写 daemon 部分。



便于理解：
相较于传统的防火墙管理配置工具，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。
firewalld中常见的区域名称（默认为public）；
区域：
firewalld将网卡对应到不同的区域（zone），zone 默认共有9个：block（拒绝）
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；
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，格式：服务名.xml；
/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）；
分为多个文件的优点 :
第一，通过服务名字来管理规则更加人性化，
第二，通过服务来组织端口分组的模式更加高效，如果一个服务使用了若干个网络端口，则服务的配置文件就相当于提供了到这些端口的规则管理的批量操作快捷方式；
命令语法：firewall-cmd [--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
firewall的状态：
--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
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

更改区域操作：

--set-default-zone=work ##更改默认的区域

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

--add-forward-port=port=513:proto=tcp:toport=22:toaddr=192.168.100.101 ##端口转发

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：

#拒绝从192.168.0.11的所有流量

firewall-cmd --permanent --zone=cla***oom --add-rich-rule= ‘rule family=ipv4 source address=192.168.0.11/32 reject ‘

#限制每分钟只有两个连接到ftp服务

firewall-cmd --add-rich-rule=‘ rule service name=ftp limitvalue=2/m accept’

#抛弃esp协议的所有数据包

firewall-cmd --permanent --add-rich-rule= ‘rule protocol value=esp drop ‘

#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 ‘

##开启SNAT

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

##使用rule规则实现端口转发，to-addr选项如果不指定默认转发到本机

firewall-cmd --permanent --add-rich-rule='rule family=ipv4 source address=192.168.100.0/24 forward-port port=80 protocol=tcp to-port=8080 to-addr=192.168.100.100