CentOS 7.0防火墙Firewalld和服务相关配置

CentOS 7.0 版本之后相对于以前的版本更改行还是很大的，原先在 6.5 版本之前命令和配置文件大致都差不多，自 7.0 版本之后一些功能都有较大的改变，接下来会从防火墙和服务的相关配置来进行剖析。

（一）防火墙 firewall 的相关介绍及配置
CentOS 7 中防火墙是一个非常的强大的功能，在 CentOS 6.5 中在 iptables 防火墙中进行了升级了。(he dynamic firewall daemon firewalld provides a dynamically managed firewall with support for network "zones" to assign a level of trust to a network and its associated connections and interfaces. It has support for IPv4 and IPv6 firewall settings. It supports Ethernet bridges and has a separation of runtime and permanent configuration options. It also has an interface for services or applications to add firewall rules directly-----官方文档)

firewall--区域 zone

网络区域定义了网络连接的可信等级。这是一个 一对多的关系，这意味着一次连接可以仅仅是一个区域的一部分，而一个区域可以用于很多连接。那个区域是否可用室友 firewall 提供的区域按照从不信任到信任的顺序排序。

firewall 分类

Firewalls can be used to separate networks into different zones based on the level of trust the user has decided to place on the devices and traffic within that network. NetworkManager informs firewalld to which zone an interface belongs. An interface's assigned zone can be changed by NetworkManager or via the firewall-config tool which can open the relevant NetworkManager window for you.
The zone settings in /etc/firewalld/ are a range of preset settings which can be quickly applied to a network interface. They are listed here with a brief explanation:
drop
Any incoming network packets are dropped, there is no reply. Only outgoing network connections are possible.
block
Any incoming network connections are rejected with an icmp-host-prohibited message for IPv4 and icmp6-adm-prohibited for IPv6. Only network connections initiated from within the system are possible.
public
For use in public areas. You do not trust the other computers on the network to not harm your computer. Only selected incoming connections are accepted.
external
For use on external networks with masquerading enabled especially for routers. You do not trust the other computers on the network to not harm your computer. Only selected incoming connections are accepted.
dmz
For computers in your demilitarized zone that are publicly-accessible with limited access to your internal network. Only selected incoming connections are accepted.
work
For use in work areas. You mostly trust the other computers on networks to not harm your computer. Only selected incoming connections are accepted.
home
For use in home areas. You mostly trust the other computers on networks to not harm your computer. Only selected incoming connections are accepted.
internal
For use on internal networks. You mostly trust the other computers on the networks to not harm your computer. Only selected incoming connections are accepted.
trusted
All network connections are accepted.
It is possible to designate one of these zones to be the default zone. When interface connections are added to NetworkManager, they are assigned to the default zone. On installation, the default zone in firewalld is set to be the public zone.

firewall 相关的配置：

1，系统配置目录：/usr/lib/firewalld

```
[root@linuxidc firewalld]# cd /usr/lib/firewalld
[root@linuxidc firewalld]# ls
icmptypes  services  xmlschema  zones
[root@linuxidc firewalld]# cd services/
[root@linuxidc services]# ls
amanda-client.xml      high-availability.xml  ldap.xml        pmproxy.xml       samba.xml
bacula-client.xml      https.xml              libvirt-tls.xml pmwebapis.xml     smtp.xml
bacula.xml             http.xml               libvirt.xml     pmwebapi.xml      ssh.xml
dhcpv6-client.xml      imaps.xml              mdns.xml        pop3s.xml         telnet.xml
dhcpv6.xml             ipp-client.xml         mountd.xml      postgresql.xml    tftp-client.xml
dhcp.xml               ipp.xml                ms-wbt.xml      proxy-dhcp.xml    tftp.xml
dns.xml                ipsec.xml              mysql.xml       radius.xml        transmission-client.xml
freeipa-ldaps.xml      iscsi-target.xml       nfs.xml         RH-Satellite-6.xml  vdsm.xml
freeipa-ldap.xml       kerberos.xml           ntp.xml         rpc-bind.xml      vnc-server.xml
```

```
freeipa-replication.xml  kpasswd.xml          openvpn.xml      rsyncd.xml          wbem-https.xml
ftp.xml                  ldaps.xml            pmcd.xml         samba-client.xml
[root@linuxidc services]#
```

注意：目录中存放定义好的网络服务和端口参数，系统参数，不能修改。

2，用户配置目录：/etc/firewalld/

```
[root@linuxidc firewalld]# cd /etc/firewalld/
[root@linuxidc firewalld]# ls
firewalld.conf  icmptypes  lockdown-whitelist.xml  services  zones
```

3,用户如何自定义添加端口，分为使用命令行添加和修改相关的配置文件。

3.1，使用命令的方式添加

```
[root@linuxidc services]# firewall-cmd --zone=public --permanent --add-port=8080/tcp
success
[root@linuxidc services]# firewall-cmd --reload
```

CentOS 7 防火墙服务 FirewallD 指南 http://www.linuxidc.com/Linux/2016-10/136431.htm

firewalld 和 iptables 详解 http://www.linuxidc.com/Linux/2017-03/141434.htm

CentOS7 下 Firewalld 防火墙使用实例 http://www.linuxidc.com/Linux/2017-01/139637.htm

CentOS 7 下 FirewallD 使用简介 http://www.linuxidc.com/Linux/2016-11/137093.htm

参数介绍：

1、firewall-cmd：是 Linux 提供的操作 firewall 的一个工具；

2、--permanent：表示设置为持久；

3、--add-port：标识添加的端口

4、--zone:指定某个区域

5、firewall-cmd --reload ：重启生效

3.2 修改配置文件方式添加端口

```
[root@linuxidc zones]# vim /usr/lib/firewalld/zones/public.xml
<?xml version="1.0" encoding="utf-8"?>
<zone>
  <short>Public</short>
  <description>For use in public areas. You do not trust the other computers on networks to not harm your
computer. O
nly selected incoming connections are accepted.</description>
  <service name="ssh"/>
  <service name="dhcpv6-client"/>
  <rule family="ipv4">
    <source address="127.0.0.1"/>
    <port protocol="tcp" port="10050-10051"/>
    <accept/>
  </rule>
</zone>
```

firewall 常用命令：

1，重启，关闭开启 firewall.service 服务

```
[root@linuxidc zones]# service firewalld restart
Redirecting to /bin/systemctl restart  firewalld.service
[root@linuxidc zones]# service firewalld stop
Redirecting to /bin/systemctl stop  firewalld.service
[root@linuxidc zones]# service firewalld start
Redirecting to /bin/systemctl start  firewalld.service
```

2，查看 firewalld 服务状态：

```
[root@linuxidc zones]# systemctl status firewalld
● firewalld.service - firewalld - dynamic firewall daemon
   Loaded: loaded (/usr/lib/systemd/system/firewalld.service; disabled; vendor preset: enabled)
   Active: active (running) since Wed 2017-04-19 11:10:50 CST; 43s ago
 Main PID: 4290 (firewalld)
   CGroup: /system.slice/firewalld.service
```

```
           └─4290 /usr/bin/python -Es /usr/sbin/firewalld --nofork --nopid
Apr 19 11:10:50 linuxidc systemd[1]: Starting firewalld - dynamic firewall daemon...
Apr 19 11:10:50 linuxidc systemd[1]: Started firewalld - dynamic firewall daemon.
```

3，查看 firewall 的状态

```
[root@linuxidc zones]# firewall-cmd --state
running
```

4,查看防火墙 firewall 规则

```
[root@linuxidc ~]# firewall-cmd --list-all
public (default)
  interfaces:
  sources:
  services: dhcpv6-client ssh
  ports: 10050/tcp 8080/tcp 10051/tcp
  masquerade: no
  forward-ports:
  icmp-blocks:
  rich rules:
```

后注：如果感觉 firewall 防火墙玩不好，可以关闭 firewall 而安装 iptables,具体步骤如下

```
[root@linuxidc ~]# service firewalld stop                    ####停止 firewalld 服务
Redirecting to /bin/systemctl stop  firewalld.service
[root@linuxidc ~]# systemctl disable firewalld.service   ####禁止 firewalld 开机启动
[root@linuxidc ~]# yum install iptables-services     #####安装 iptables
Loaded plugins: fastestmirror
Repodata is over 2 weeks old. Install yum-cron? Or run: yum makecache fast
base                                                                          | 3.6 kB  00:00:00
epel                                                                          | 4.3 kB  00:00:00
extras                                                                        | 3.4 kB  00:00:00
updates                                                                       | 3.4 kB  00:00:00
[root@linuxidc ~]# vim /etc/sysconfig/iptables        ########编辑 iptables 配置文件
[root@linuxidc ~]#service iptables start              #开启
[root@linuxidc ~]#systemctl enable iptables.service       #设置防火墙开机启动
```

备注：centos7.Xfireward 防火墙基本使用：

1、firewalld 的基本使用

启动： systemctl start firewalld
查看状态： systemctl status firewalld
停止： systemctl disable firewalld
禁用： systemctl stop firewalld

2.systemctl 是 CentOS7 的服务管理工具中主要的工具，它融合之前 service 和 chkconfig 的功能于一体。
启动一个服务：systemctl start firewalld.service 关闭一个服务：systemctl stop firewalld.service 重启一个服务：systemctl restart firewalld.service 显示一个服务的状态：systemctl status firewalld.service 在开机时启用一个服务：systemctl enable firewalld.service 在开机时禁用一个服务：systemctl disable firewalld.service 查看服务是否开机启动：systemctl is-enabled firewalld.service 查看已启动的服务列表：systemctl list-unit-files|grep enabled 查看启动失败的服务列表：systemctl --failed

3.配置 firewalld-cmd

查看版本： firewall-cmd --version
查看帮助： firewall-cmd --help
显示状态： firewall-cmd --state
查看所有打开的端口： firewall-cmd --zone=public --list-ports
更新防火墙规则： firewall-cmd --reload
查看区域信息: firewall-cmd --get-active-zones
查看指定接口所属区域： firewall-cmd --get-zone-of-interface=eth0
拒绝所有包：firewall-cmd --panic-on
取消拒绝状态： firewall-cmd --panic-off
查看是否拒绝： firewall-cmd --query-panic

那怎么开启一个端口呢

添加

```
firewall-cmd --zone=public --add-port=80/tcp --permanent    （--permanent 永久生效，没有此参数重启后失效）
```

重新载入

```
firewall-cmd --reload
```

查看

```
firewall-cmd --zone= public --query-port=80/tcp
```

删除

```
firewall-cmd --zone= public --remove-port=80/tcp --permanent
```

（二）CentOS 7.x 添加自定义服务

CentOS 系统服务脚本目录：

/usr/lib/systemd/

有系统（system）和用户（user）之分，
如需要开机没有登陆情况下就能运行的程序，存在系统服务（system）里，即：
/lib/systemd/system/

反之，用户登录后才能运行的程序，存在用户（user）里
服务以.service 结尾。
这边以 nginx 开机运行为例

1,建立服务文件

```
[root@linuxidc system]# vim nginx.service
[Unit]
Description=nginx
After=network.target
[Service]
Type=forking
ExecStart=/usr/local/nginx/sbin/nginx
ExecReload=/usr/local/nginx/sbin/nginx -s reload
ExecStop=/usr/local/nginx/sbin/nginx -s quit
PrivateTmp=true
[Install]
WantedBy=multi-user.target
```

说明：
Unit]:服务的说明
Description:描述服务
After:描述服务类别
[Service]服务运行参数的设置
Type=forking 是后台运行的形式
ExecStart 为服务的具体运行命令
ExecReload 为重启命令
ExecStop 为停止命令
PrivateTmp=True 表示给服务分配独立的临时空间
注意：[Service]的启动、重启、停止命令全部要求使用绝对路径
[Install]服务安装的相关设置，可设置为多用户

2，保存该文件，并赋予 754 权限

```
[root@linuxidc system]# chmod 754 nginx.service
[root@linuxidc system]# ll nginx.service
-rwxr-xr-- 1 root root 258 Apr 19 14:39 nginx.service
```

3，设置开机自启动

```
[root@linuxidc system]# systemctl enable nginx.service
[root@linuxidc system]# systemctl list-unit-files|grep enabled|grep nginx.service
nginx.service                                  enabled
```

其他相关的命令

systemctl 是系统服务管理器命令，它实际上将 service 和 chkconfig 这两个命令组合到一起。

任务	旧指令	新指令
使某服务自动启动	chkconfig –level 3 httpd on	systemctl enable httpd.service
使某服务不自动启动	chkconfig –level 3 httpd off	systemctl disable httpd.service

检查服务状态	service httpd status	systemctl status httpd.service （服务详细信息） systemctl is-active httpd.service （仅显示是否 Active)
显示所有已启动的服务	chkconfig –list	systemctl list-units |grep enabled
启动某服务	service httpd start	systemctl start httpd.service
停止某服务	service httpd stop	systemctl stop httpd.service
重启某服务	service httpd restart	systemctl restart httpd.service

启动 nginx 服务

```
systemctl start nginx.service
```

设置开机自启动

```
systemctl enable nginx.service
```

停止开机自启动

```
systemctl disable nginx.service
```

查看服务当前状态

```
systemctl status nginx.service
```

重新启动服务

```
systemctl restart nginx.service
```

查看所有已启动的服务

```
systemctl list-units --type=service
```

分类: 网络

列出所有服务的层级和依赖关系，可以指定某个服务

```
systemctl list-dependencies [服务名称]
```

更多 CentOS 相关信息见 CentOS 专题页面 http://www.linuxidc.com/topicnews.aspx?tid=14

本文永久更新链接地址：http://www.linuxidc.com/Linux/2017-04/142993.htm