**官网地址**

http://www.firewalld.org/

开始试验：准备干净的虚拟机

# yum install firewalld firewall-config -y

# systemctl restart firewalld --启动服务

# systemctl status firewalld --确认状态

# systemctl enable firewalld --设为开机自动启动(可选)

# systemctl disable firewalld --禁止开机自动启动(可选)

**概念一 ZONE:**

Zone 简单来说就是防火墙方案,就是一套规则集，你可以切换使用哪一个zone

# firewall-cmd --get-zones --查看现在有哪些zone

work drop internal external trusted home dmz public block

drop：拒绝所有外部连接请求。

block：拒绝所有外部连接(with an icmp-host-prohibited message for IPv4 and icmp6-adm-prohibited for IPv6)，允许内部发起的连接

public：适用公共环境，拒绝所有外部连接请求，但指定外部连接可以进入

external：特别适用路由器启用了伪装功能的外部网。拒绝所有外部连接请求，只能接收经过选择的连接。

dmz：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，仅仅接收经过选择的连接。（受限制的公共连接可以进入）

work：适用于工作网络环境，概念和workgoup一样，也是指定的外部连接允许用于工作区。

home：类似家庭组,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。仅仅接收经过选择的连接

internal：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。仅仅接受经过选择的连接

trusted：可接受所有的网络连接。（最不安全）

# firewall-cmd --get-default-zone 　--查看当前使用的zone

public

# firewall-cmd --set-default-zone=work

# firewall-cmd --set-default-zone=public --修改当前使用的zone

# firewall-cmd --list-all　--查看当前使用的zone的规则集

# firewall-cmd --zone=work --list-all --指定查看work这个zone的规则集

# vim /etc/firewalld/zones/public.xml"。firewall的默认模式"public"的配置文件，如下图所示，可以看到添加的服务都在里面，如果在其中按照格式添加"ftp"，重新加载后就添加了这个服务了。

#cd /usr/lib/firewalld/services/

进入这个目录后，如下图所示，输入"ls"，就可以看到可以添加哪些服务，并且可以看到这些服务的名称了。

**概念二:网卡接口**

# firewall-cmd --zone=public --add-interface=ens33 --指定网卡加入到哪个zone

# firewall-cmd --get-zone-of-interface=ens33 --查看网卡加入到哪个zone

-------------------

常用命令：

firewall‐cmd ‐‐reload //重新载入防火墙策略，未设置为永久策略的规则会丢失。

firewall‐cmd ‐‐permanent //永久策略属性

firewall‐cmd ‐‐add‐ //添加一条策略

‐‐add‐source=source[/mask]

‐‐add‐service=http

firewall‐cmd ‐‐remove‐ //删除一条策略

firewall-cmd --list-all 查询已有防火墙规则

**概念三:服务于端口**

port,service 分别表示端口和服务

# firewall-cmd --add-port=80/tcp　　--允许tcp的80端口进来的通迅（类似iptables的INPUT)

# firewall-cmd --remove-port=80/tcp --删除上面的规则

# firewall-cmd --add-service=http --允许http服务进来的通迅（不用管它是什么端口，只记住服务就好了)

# firewall-cmd --remove-service=http

# firewall-cmd --add-service=ftp --允许ftp服务进来的通迅（无论主动还是被动都可以，这样就把iptables的写法简单化了)

# firewall-cmd --remove-service=ftp

**概念四:富规则**

rich-rule复杂规则（富规则）

富规则中可以包含很多网络元素，比如:IP地址、端口、以及处

理动作、记录日志等操作。我们可以使用富规则来精确控制我们

的访问流量，而不是粗放的。

# firewall-cmd --add-rich-rule="rule family='ipv4' source address=192.168.224.11 service name='ssh' accept"

下面两条合起来实现允许所有人访问我的http,但drop掉192.168.224.11的访问我的http的包

# firewall-cmd --add-service=http

# firewall-cmd --add-rich-rule="rule family="ipv4" source address=192.168.224.11 service name="http" drop"

# firewall-cmd --list-rich-rule （查询现有的富规则）

**概念五:关于立即生效与永久生效**

立即生效：上面的练习都是立刻生效，但是无法永久保存，重新防火墙服务，重启机器，以及执行--realod参数都会导致规则被覆盖。

永久生效： 在命令行中加入参数 --permanent 为永久保存，但是运行时不会立即生效，需要执行 firewall --reload命令才会让规则立刻生效。

# firewall-cmd --permanent --add-service=ftp　　--加了一个--permanent参数后，立即不生效，需要reload后才能生效

实际写规则时，建议直接写（不加--permanent参数)，所有规则写完，测试完成后，再使用

# firewall-cmd --runtime-to-permanent 全部转成permanent规则

**概念六:**

panic模式,在遭受攻击的时候进入紧急模式，以保护服务器。

# firewall-cmd --panic-on

# firewall-cmd --panic-off

**概念七:**

图形配置

# firewall-config