## 系统安全

**一、Security -Enhanced Linux**

1、美国国家安全局主导开发，一套增强Linux系统安全的强制体系

集成到Linux内核（2.6及以上）中运行

针对用户、进程、目录和文件提供保护策略，以及管理工具

SELinux运行模式

Enforcing（强制）、permissive（宽松）、disabled（彻底禁用）

2、切换模式

任何模式变成disabled都要需重启才生效

固定配置：/etc/selinux/config

临时切换：setenforce 1|0 #本次开机临时切换状态1：enforcing、0：permissive

获取当前运行模式：getenforce

1. selinux的安全内容

布尔值

getsebool -a | grep samba#获取samba相关的布尔值列表

setsebool samba\_export\_all\_rw on #打开samba开关

安全上下文

chcon --reference=/var/www /xiao

#把/xiao的selinux的安全上下文值设置成与/var/www的一样设置

针对服务开放端口

semanage -a -t http\_export\_t -p tcp 8909

#打开http协议的8909端口

Semanage -l | grep http

#查看selinux端口开放情况

1. **防火墙策略管理**

严格过滤入站，允许出站

防火墙策略管理：隔离

1. Firewalld

管理工具fireewall-cmd（命令） 、fireewall-config（图形）

2.欲设安全区域

public：仅允许访问本机的sshd、dhcp、ping等服务

trusted：允许任何访问

block：阻塞任何来访请求，明确拒绝（返回拒绝）

drop：丢弃任何来访的数据包，直接丢弃

防火墙默认区域：public

1. 防火墙进入区域的判断： 匹配即停止
2. 查看访问请求中的源ip地址，查询所有的区域中，哪个区域于该源ip地址的策略，则进入该区域
3. 若其他区域没有设置该ip的策略，则进入默认区域（public）

不同区域不能有统一ip

1. 默认区域的查看和设置

firewall-cmd --get-default-zone #查看

firewall-cmd --set-default-zone=drop #设置

firewall-cmd --zone=public --list-all

默认区域添加服务：

firewall-cmd --zone=public --add-service=http

firewall-cmd --zone=public --add-service=ftp

firewall-cmd --zone=public --list-all 查看默区域的服务

重启之后上述添加服务就会失效，配置永久生效 --permanent #写入配置文件

firewall-cmd --permanent --zone=public --add-service=http

firewall-cmd --reload #加载配置文件

允许服务通过防火墙策略：

firewall-cmd --add-service=http

firewall-cmd --add-service=ftp

## 端口转发

将访问5423端口的消息转发给80端口

防火墙进行端口转发将5423变成80

firewall-cmd --zone=public --add-service=http

firewall-cmd --permanent --zone=public

--add-forward-port=port=5423:proto=tcp:toport=80

firewall-cmd --permanent --zone=public

--add-forward-port= port=源端口 ：proto=协议 ：toport= 目标端口