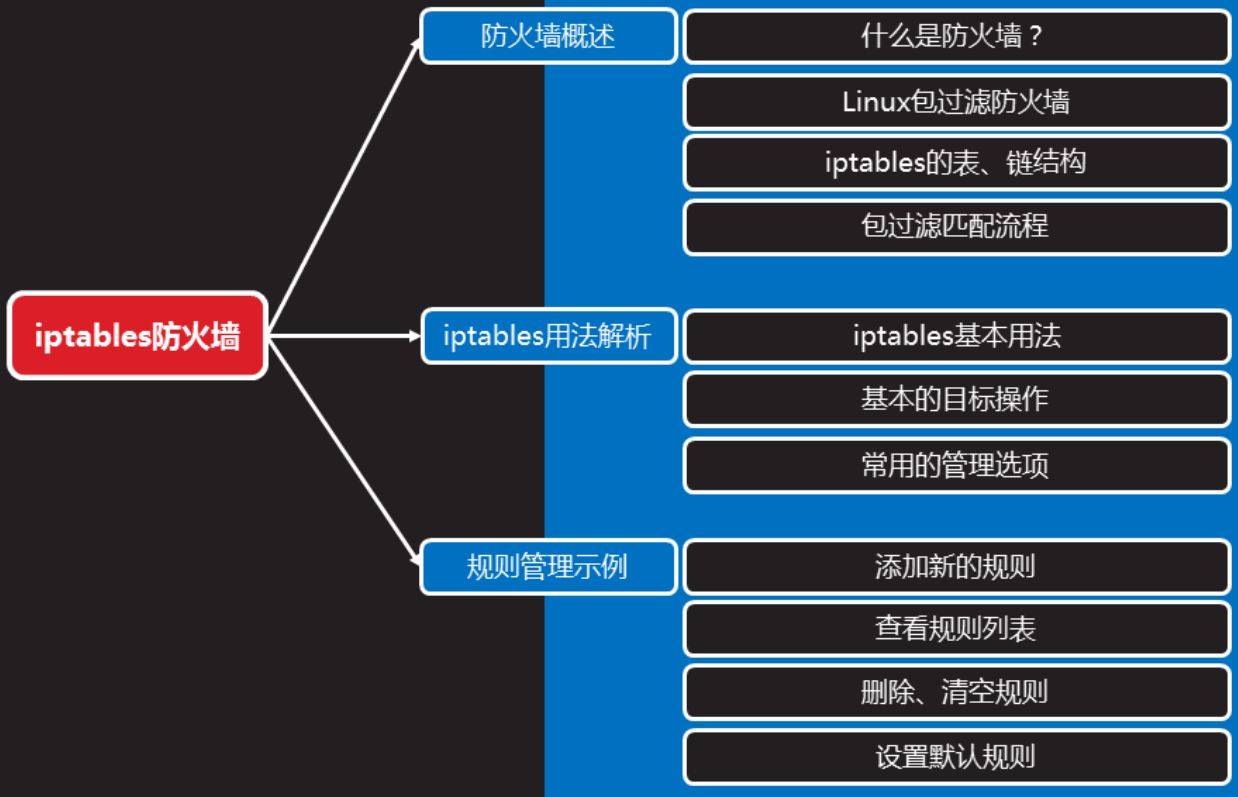
SECURITY DAY04

内容

上午	09:00 ~ 09:30	作业讲解和回顾
	09:30 ~ 10:20	iptables防火墙
	10:30 ~ 11:20	
	11:30 ~ 12:20	filter表控制
下午	14:00 ~ 14:50	扩展匹配
	15:00 ~ 15:50	nat表典型应用
	16:00 ~ 16:50	
	17:00 ~ 17:30	总结和答疑

iptables防火墙



防火墙概述

什么是防火墙？

- 一道保护性的安全屏障
  - 保护、隔离

知识讲解

Linux包过滤防火墙

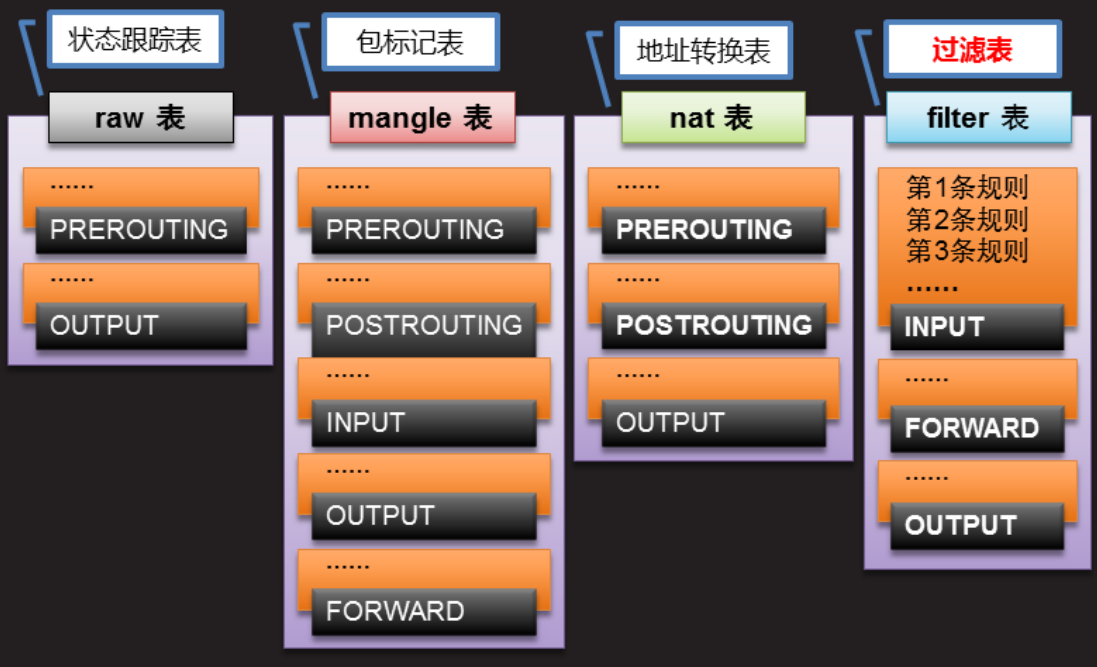
知识讲解

- RHEL7默认使用firewalld作为防火墙，
- 但firewalld底层还是调用包过滤防火墙iptables

```
[root@svr7 ~]# systemctl stop firewalld.service
[root@svr7 ~]# systemctl disable firewalld.service
[root@svr7 ~]# yum -y install iptables-services
[root@svr7 ~]# systemctl start iptables.service
```

iptables的表、链结构

知识讲解




Technology
Tarena
达内科技
iptables用法解析

基本的目标操作

- ACCEPT：允许通过/放行
- DROP：直接丢弃，不给出任何回应
- REJECT：拒绝通过，必要时会给出提示
- LOG：记录日志，然后传给下一条规则

知识讲解

“匹配即停止”规律的唯一例外

Technology Tarena 达内科技

常用的管理选项

知识讲解

类别	选项	用途
添加规则	-A	在链的末尾追加一条规则
	-I	在链的开头（或指定序号）插入一条规则
查看规则	-L	列出所有的规则条目
	-n	以数字形式显示地址、端口等信息
	--line-numbers	查看规则时，显示规则的序号
删除规则	-D	删除链内指定序号（或内容）的一条规则
	-F	清空所有的规则
默认策略	-P	为指定的链设置默认规则

Technology Tarena 达内科技

规则管理示例

添加新的规则

知识讲解

- -A追加、-I插入

```
[root@svr7 ~]# iptables -t filter -A INPUT -p tcp -j ACCEPT

[root@svr7 ~]# iptables -I INPUT -p udp -j ACCEPT

[root@svr7 ~]# iptables -I INPUT 2 -p icmp -j ACCEPT
```

-p 协议名或协议号

删除、清空规则

知识讲解

- -D删除、-F清空

```
[root@svr7 ~]# iptables -D INPUT 3
[root@svr7 ~]# iptables -nL INPUT
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     udp  --  0.0.0.0/0            0.0.0.0/0
ACCEPT     icmp --  0.0.0.0/0            0.0.0.0/0

[root@svr7 ~]# iptables -F
[root@svr7 ~]# iptables -t nat -F
[root@svr7 ~]# iptables -t mangle -F
[root@svr7 ~]# iptables -t raw -F
```

依次清空4个表的规则

设置默认规则

知识讲解

- 所有链的初始默认规则均为ACCEPT
- 通过 -P 选项可重置默认规则
  - ACCEPT 或者 DROP

```
[root@svr5 ~]# iptables -t filter -P INPUT DROP

[root@svr5 ~]# iptables -nL | head -1
Chain INPUT (policy DROP)
```

INPUT链的默认策略

案例1：iptables基本管理

课堂练习

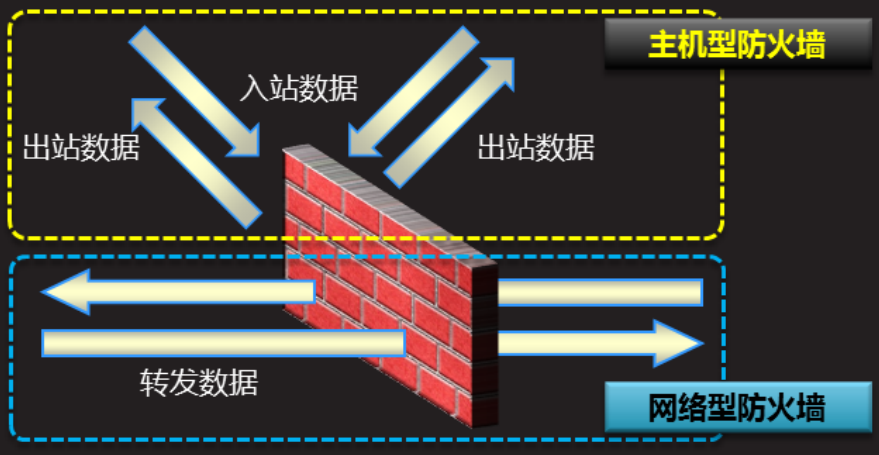
1.关闭firewalld，启动iptables服务
2. 查看防火墙规则
3. 追加、插入防火墙规则
4. 删除、清空防火墙规则

filter表控制

主机/网络型防护

- 根据保护对象（本机、其他主机）区分

知识讲解



开启内核的IP转发

知识讲解

- 作为网关、路由的必要条件
  - echo 'net.ipv4.ip_forward=1' >> /etc/sysctl.conf

  或者
  - echo 1 > /proc/sys/net/ipv4/ip_forward

基本的匹配条件

知识讲解

- 通用匹配
  - 可直接使用，不依赖于其他条件或扩展
  - 包括网络协议、IP地址、网络接口等条件
- 隐含匹配
  - 要求以特定的协议匹配作为前提
  - 包括端口、TCP标记、ICMP类型等条件

禁ping相关策略处理

- 允许本机 ping 其他主机
- 但是，禁止其他主机 ping 本机

知识讲解

```
[root@svr5 ~]# iptables  -A  INPUT  -p icmp  --icmp-type \
  echo-request  -j  DROP
[root@svr5 ~]# iptables  -A  INPUT  -p icmp  !  --icmp-type \
  echo-request  -j  ACCEPT

[root@svr5 ~]# iptables  -A  OUTPUT  -p icmp  --icmp-type \
  echo-request  -j  ACCEPT
[root@svr5 ~]# iptables -A OUTPUT -p icmp ! --icmp-type \
  echo-request  -j  DROP
```

案例2：filter过滤和转发控制

课堂练习

1. 利用ip_forward机制实现Linux路由/网关功能
2. 针对Linux主机进行出站、入站控制
3. 在Linux网关上实现数据包转发访问控制

扩展条件的方法

知识讲解

- 前提条件
  - 有对应的防火墙模块支持
- 基本用法
  - -m 扩展模块 --扩展条件 条件值
  - 示例： -m mac --mac-source 00:0C:29:74:BE:21

扩展案例

多端口案例

- 一条规则开放多个端口
  - 比如 Web、FTP、Mail、SSH 等等

知识讲解

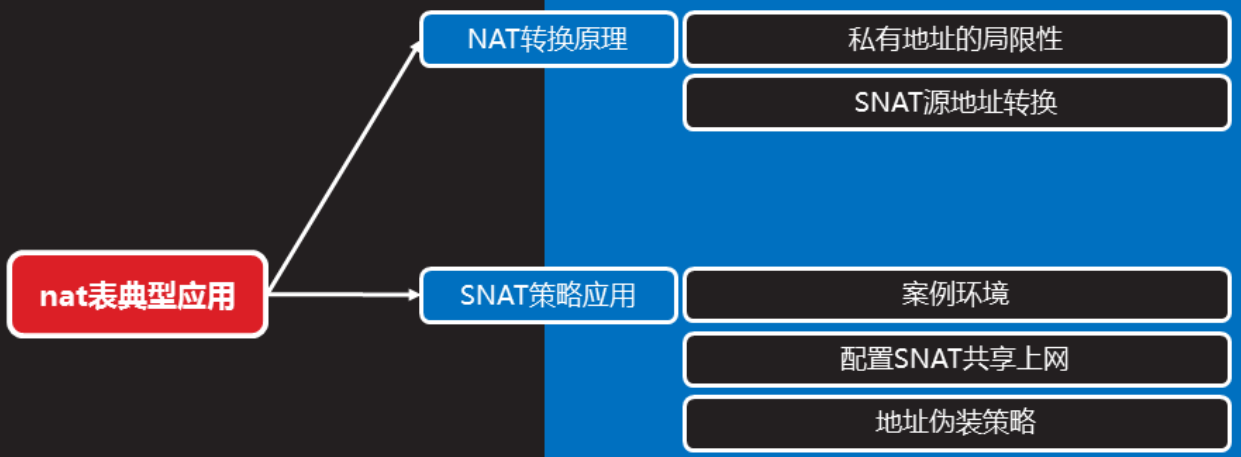
```
[root@svr1 ~]# iptables  -A  INPUT  -p tcp   -m  multiport \
 --dports  20:22,25,80,110,143,16501:16800 -j  ACCEPT
```

案例3：防火墙扩展规则

课堂练习

1. 根据MAC地址封锁主机
2. 在一条规则中开放多个TCP服务
3. 根据IP范围设置封锁规则

nat表典型应用



NAT转换原理

私有地址的局限性

知识讲解

- 从局域网访问互联网的时候
  - 比如看网页、收邮件、……
  - 源地址为私有地址，服务器如何正确给出回应？