

SECURITY DAY06



监控与服务安全

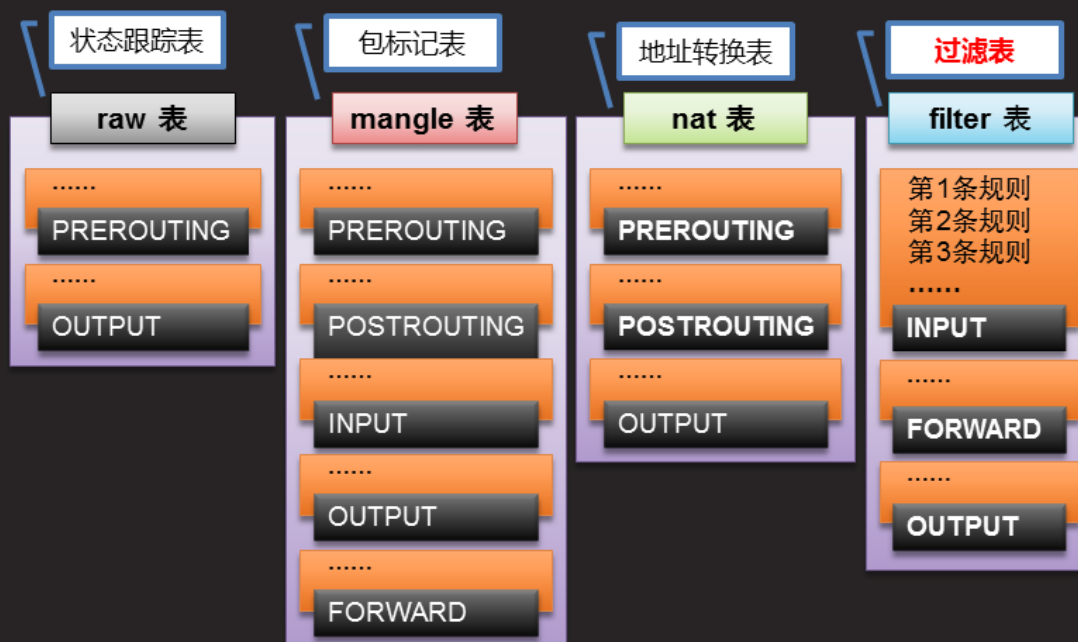
NSD SECURITY

DAY06



iptables的表、链结构

知识讲解



包过滤匹配流程

- 规则链内的匹配顺序
 - 顺序比对，匹配即停止（LOG除外）
 - 若无任何匹配，则按该链的默认策略处理

知识讲解



iptables基本用法

- 管理程序位置
 - /sbin/iptables
- 指令组成
 - iptables [-t 表名] 选项 [链名] [条件] [-j 目标操作]

```
[root@svr7 ~]# iptables -t filter -I INPUT -p icmp -j REJECT
```



```
[root@client ~]# ping 192.168.4.5
From 192.168.4.5 icmp_seq=1 Destination Port Unreachable
From 192.168.4.5 icmp_seq=2 Destination Port Unreachable
... ..
```

iptables基本用法（续1）

知识讲解

- 注意事项/整体规律
 - 可以不指定表，默认为filter表
 - 可以不指定链，默认为对应表的所有链
 - 如果没有匹配的规则，则使用防火墙默认规则
 - 选项/链名/目标操作大写字母，其余都小写



基本的目标操作

知识讲解

- 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

“匹配即停止”规律的唯一例外



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



规则管理示例

添加新的规则

- -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

知识讲解



查看规则列表

- -L查看

```
[root@svr7 ~]# iptables -nL INPUT
```

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
ACCEPT	tcp	--	0.0.0.0/0	0.0.0.0/0

```
[root@svr7 ~]# iptables -L INPUT --line-numbers
```

num	target	prot	opt	source	destination
1	ACCEPT	udp	--	anywhere	anywhere
2	ACCEPT	icmp	--	anywhere	anywhere
3	ACCEPT	tcp	--	anywhere	anywhere

知识讲解



删除、清空规则

- -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

知识讲解



设置默认规则

- 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

知识讲解



filter表控制

filter表控制

防护类型及条件

主机/网络型防护

开启内核的IP转发

基本的匹配条件

过滤规则示例

封禁IP地址/网段

保护特定网络服务

禁ping相关策略处理

防护类型及条件



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



基本的匹配条件（续1）

知识讲解

类别	选项	用法
通用匹配	协议匹配	-p 协议名
	地址匹配	-s 源地址、-d 目标地址
	接口匹配	-i 收数据的网卡、-o 发数据的网卡
隐含匹配	端口匹配	--sport 源端口、--dport 目标端口
	ICMP类型匹配	--icmp-type ICMP类型

需要取反条件时，用叹号！



过滤规则示例

封禁IP地址/网段

- 主机防护，针对入站访问的源地址
- 网络防护，针对转发访问的源地址

知识讲解

```
[root@svr7 ~]# iptables -A INPUT -s 192.168.4.120 -j DROP  
[root@svr7 ~]# iptables -A INPUT -s 10.0.10.0/24 -j DROP
```

```
[root@svr7 ~]# iptables -A FORWARD -s 192.168.0.0/16 -j DROP  
[root@svr7 ~]# iptables -A FORWARD -s 172.16.0.0/16 -j DROP  
... ..
```



禁ping相关策略处理

知识讲解

- 允许本机 ping 其他主机
- 但是，禁止其他主机 ping 本机

```
[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
```



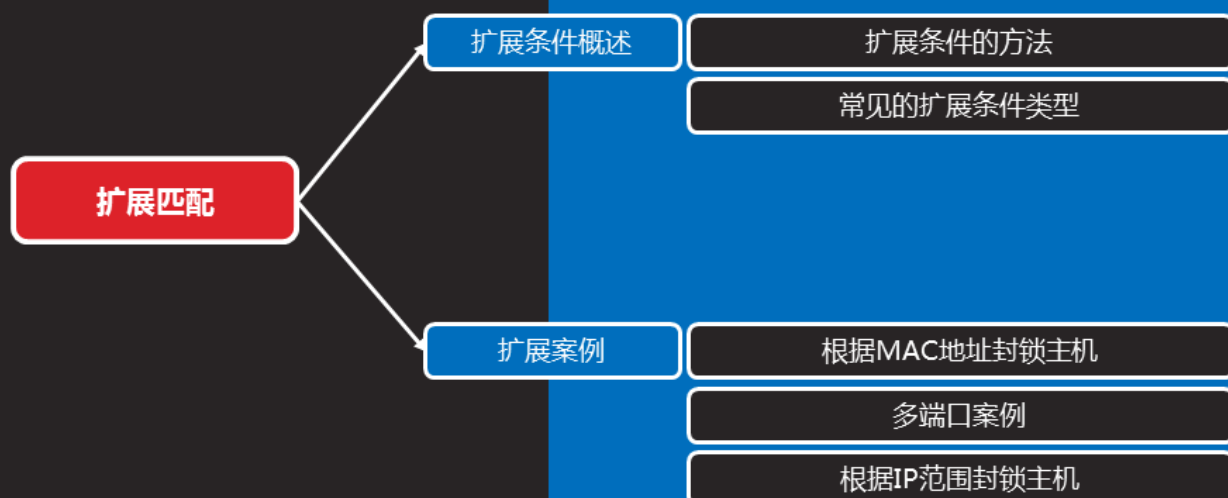
案例2：filter过滤和转发控制

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



扩展匹配



扩展条件的方法

Technology
Tarena
达内科技

- 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`

知识讲解



常见的扩展条件类型

知识讲解

类别	选项	用法
扩展匹配	MAC地址匹配	-m mac --mac-source MAC地址
	多端口匹配	-m multiport --sports 源端口列表
		-m multiport --dports 目标端口列表
	IP范围匹配	-m iprange --src-range IP1-IP2
		-m iprange --dst-range IP1-IP2



扩展案例

根据MAC地址封锁主机

- 适用于交换网络，针对源MAC地址
 - 不管其IP地址变成多少

```
[root@svr1 ~]# iptables -A INPUT -m mac \  
--mac-source 00:0C:29:74:BE:21 -j DROP
```

知识讲解



多端口案例

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

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

知识讲解



根据IP范围封锁主机

知识讲解

- SSH登录的IP范围控制
 - 允许从 192.168.4.10-192.168.4.20 登录
 - 禁止从 192.168.4.0/24 网段其他的主机登录
- ```
[root@svr1 ~]# iptables -A INPUT -p tcp --dport 22 -m iprange --src-range 192.168.4.10-192.168.4.20 -j ACCEPT
```
- ```
[root@svr1 ~]# iptables -A INPUT -p tcp --dport 22 \-s 192.168.4.0/24 -j DROP
```



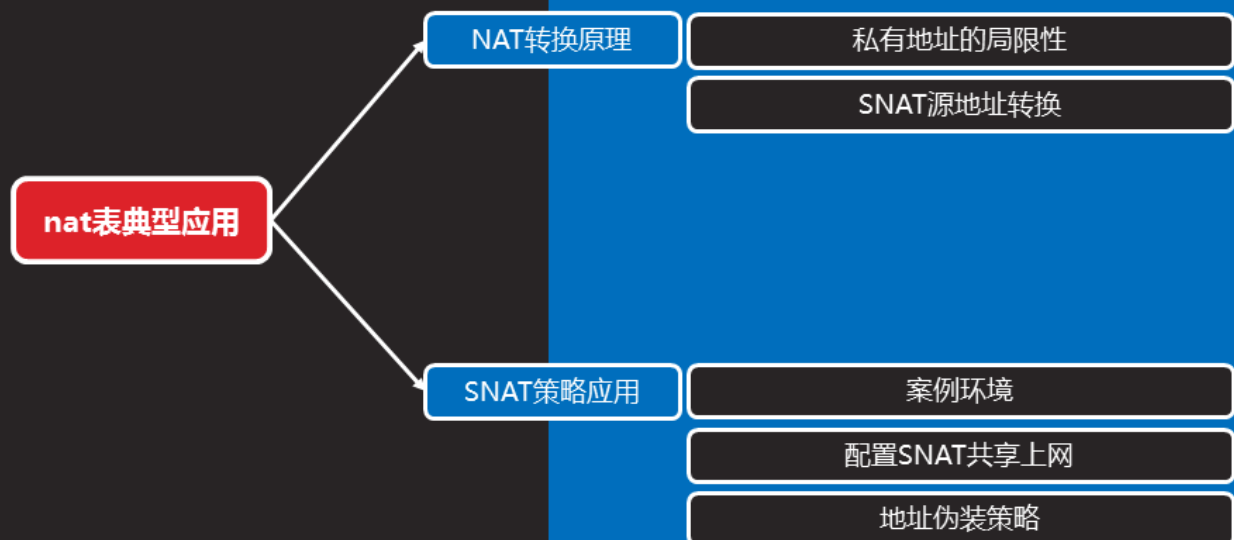
案例3：防火墙扩展规则

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

- 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？

知识讲解

