Technology Tarena 达内科技

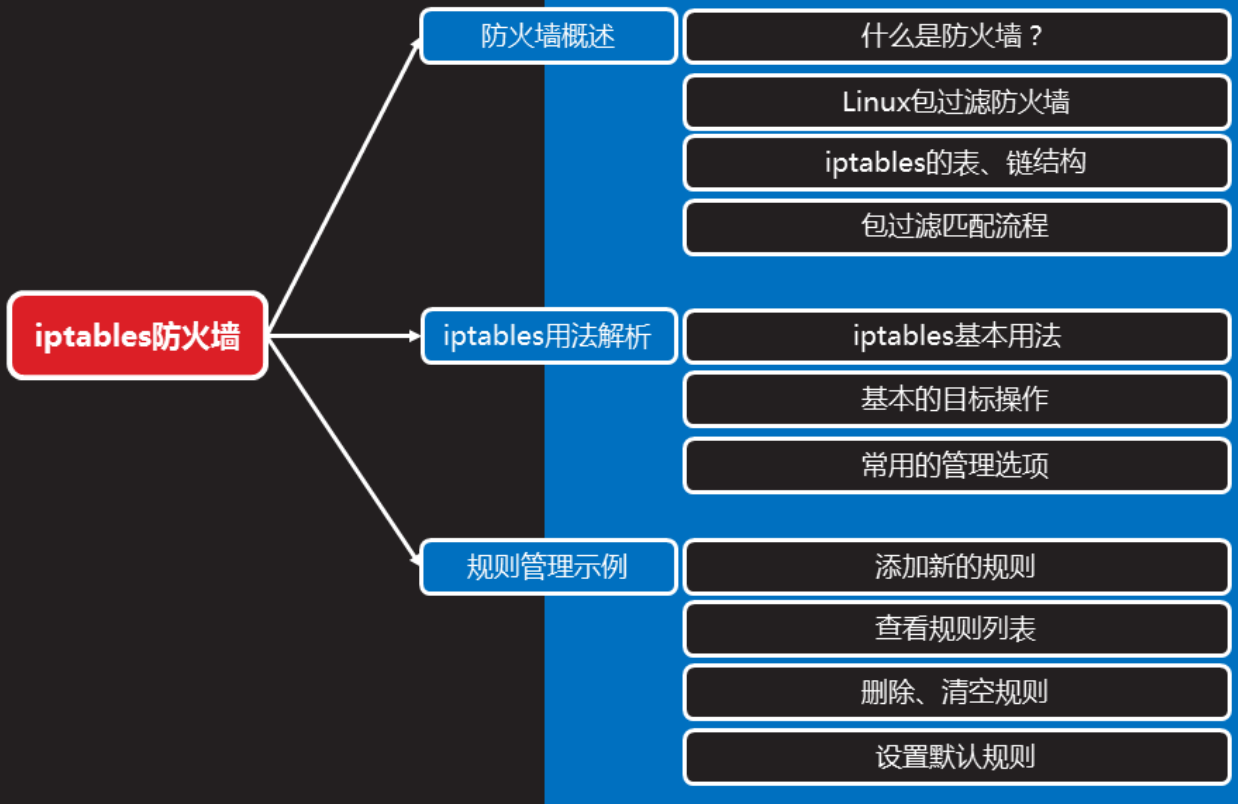
服务安全与监控

NSD 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



Technology Tarena 达内科技

防火墙概述

Technology Tarena 达内科技

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

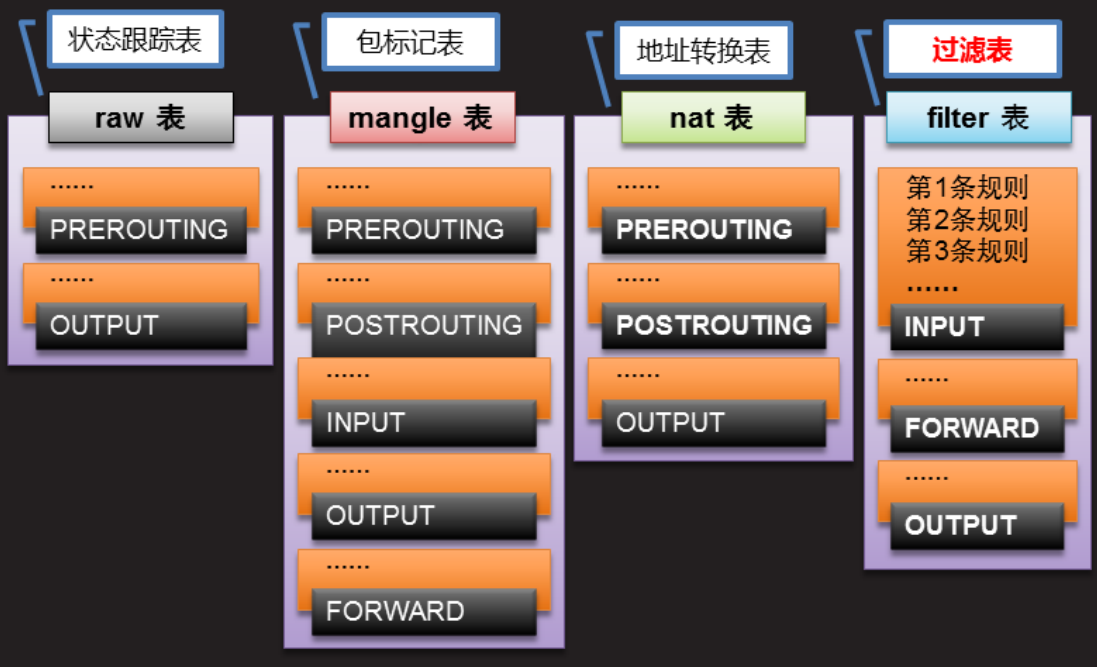
知识讲解

- 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



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用法解析

iptables基本用法

知识讲解

- 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/目标操作用大写字母，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

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

查看规则列表

知识讲解

- -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
```

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)
```

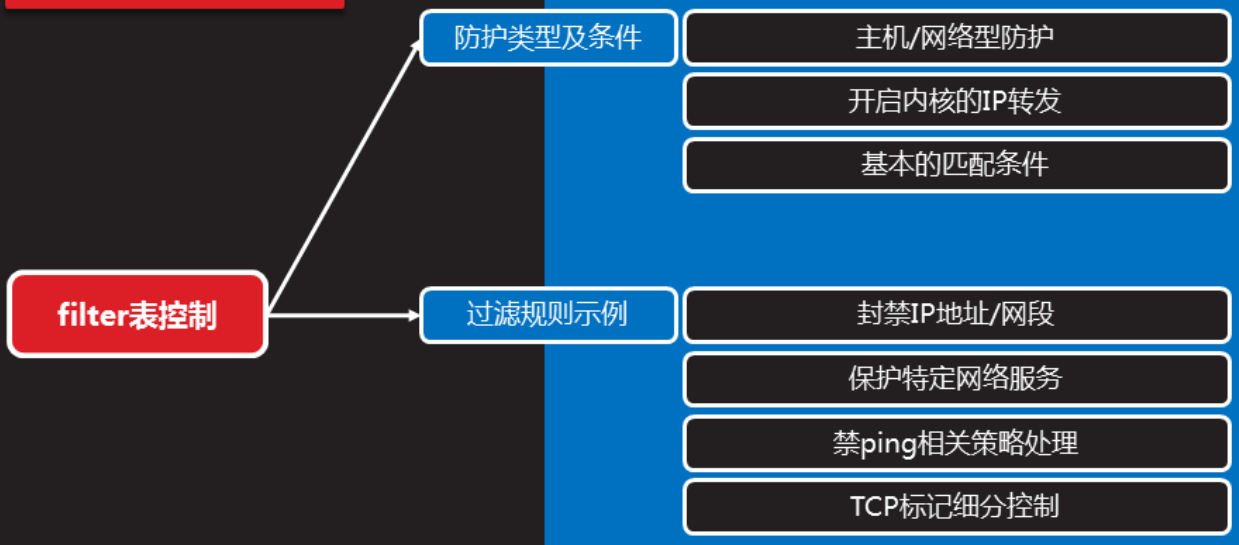
INPUT链的默认策略

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



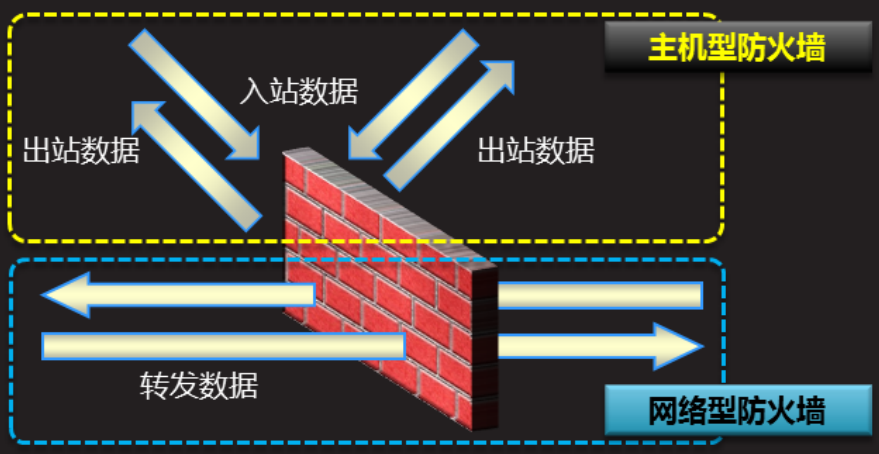
Technology Tarena 达内科技

防护类型及条件

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

- 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

知识讲解

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
.. ..
```

保护特定网络服务

知识讲解

- 限制对指定服务端口的访问

```
[root@svr7 ~]# iptables -A INPUT -s 192.168.168.0/24 \
 -p tcp --dport 22 -j ACCEPT

[root@svr7 ~]# iptables -A INPUT -s 220.181.78.0/24 -p tcp \
 --dport 22 -j ACCEPT

[root@svr7 ~]# iptables -A INPUT -p tcp --dport 22 -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

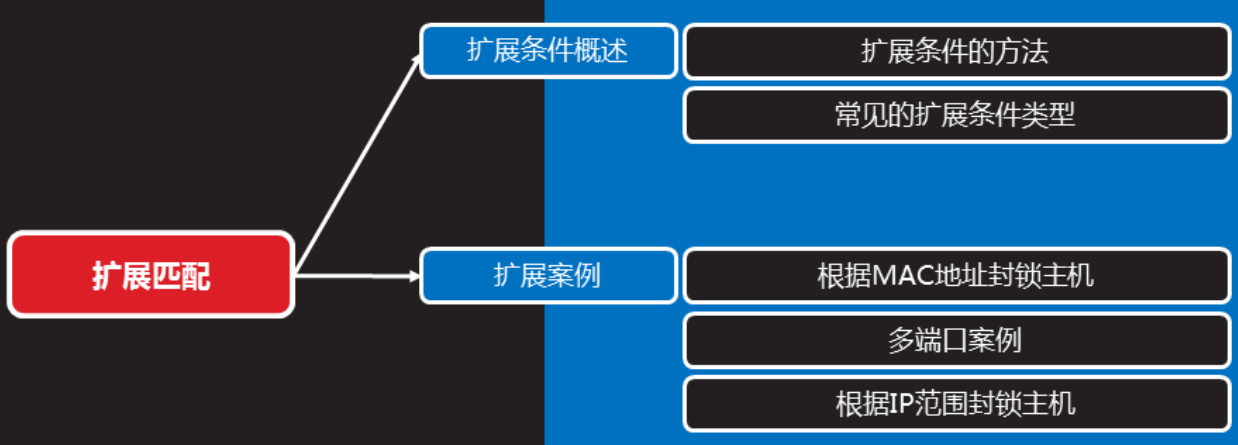
```
[root@svr5 ~]# iptables -A INPUT -p icmp --icmp-type \
  echo-request -j DROP
[root@svr5 ~]# iptables -A INPUT -p icmp ! --icmp-type \
  echo-request -j ACCEPT

[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

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

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

知识讲解

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

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
```

根据IP范围封锁主机

- 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

知识讲解

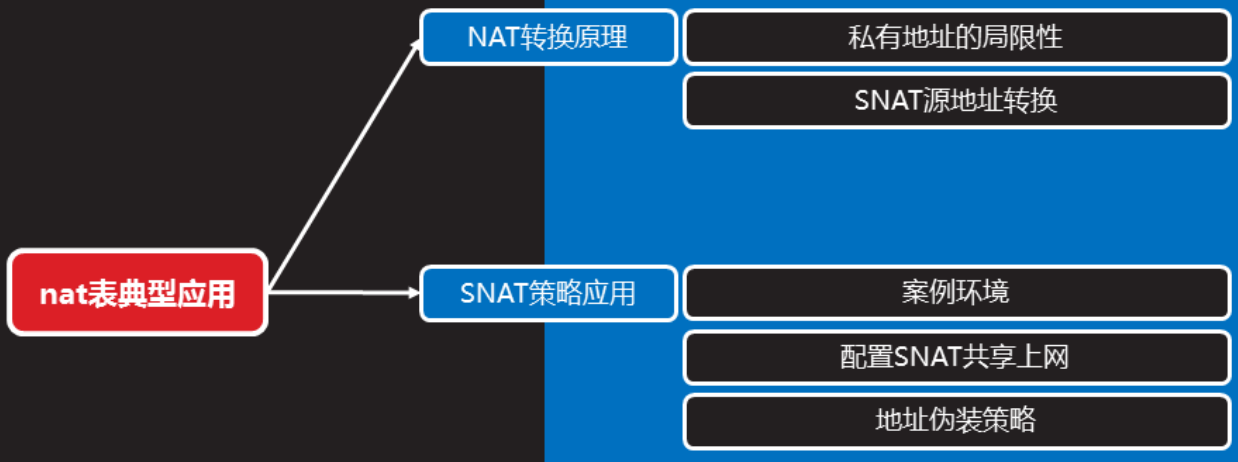
```
[root@svr1 ~]# iptables -A INPUT -p tcp --dport 22 -m\
iprange --src-range 192.168.4.10-192.168.4.20 -j ACCEPT

[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

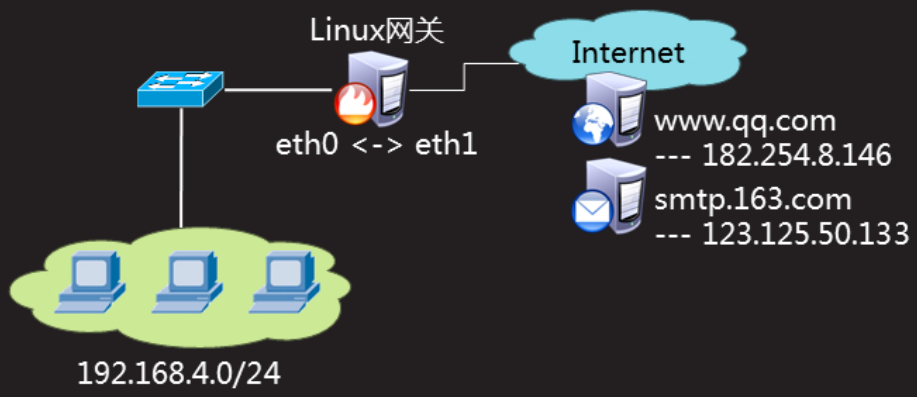


NAT转换原理

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



SNAT源地址转换

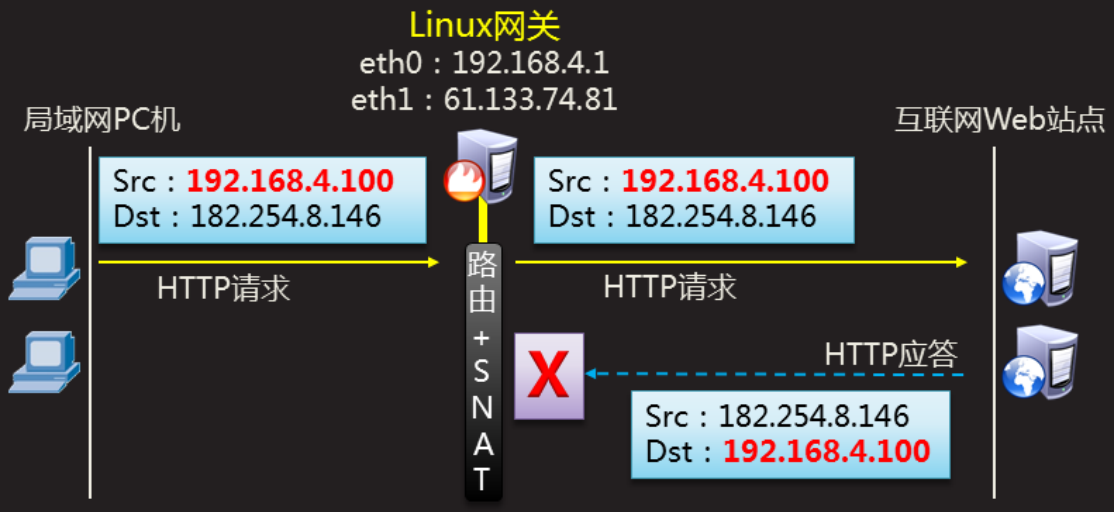
知识讲解

- Source Network Address Translation
  - 修改数据包的源地址
  - 仅用于 nat 表的 POSTROUTING 链

SNAT源地址转换（续1）

知识讲解

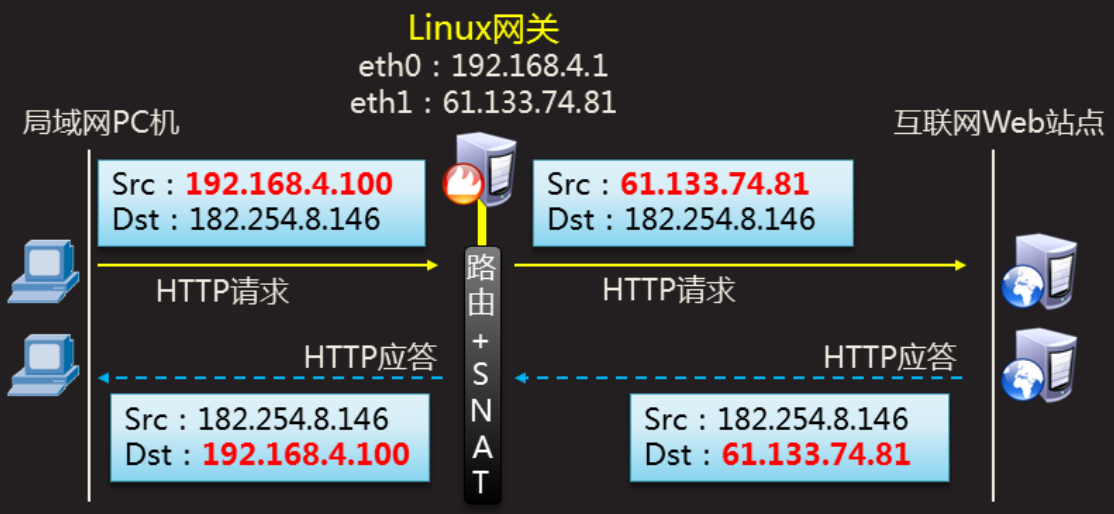
- 不修改源地址的情况



SNAT源地址转换（续2）

- 修改源地址的情况

知识讲解

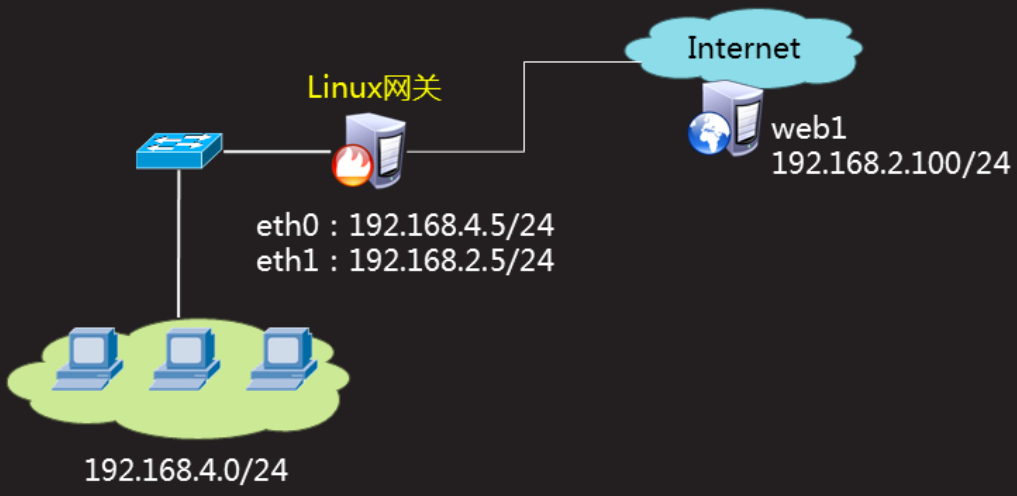


SNAT策略应用

案例环境

- 局域网共享公网IP上网

知识讲解



案例环境（续1）

- 前期准备
  - 局域网PC机正确设置IP地址/子网掩码
  - 局域网PC机正确设置默认网关
  - Linux网关服务器开启IP路由转发
  - 本实验中，不要为Web服务器设置默认网关

知识讲解

配置SNAT共享上网

知识讲解

- 配置的关键策略
  - 选择路由之后，针对来自局域网、即将从外网接口发出去的包，将源IP地址修改为网关的公网IP地址

```
[root@proxy ~]# iptables  -t  nat  -A POSTROUTING \
 -s  192.168.4.0/24  -p tcp --dport 80 -j SNAT  --to-source  192.168.2.5
```

局域网网段地址　　外网接口　　外网接口的IP地址

配置SNAT共享上网（续1）

知识讲解

- 验证SNAT访问结果
  - 客户机上：PC机192.168.4.100能够访问外网的Web服务器 174.16.16.120
  - 服务器上：查看Web主机192.168.2.100的访问日志，来访者应是Linux网关的外网IP地址192.168.2.5

```
[root@www ~]# tail  /var/log/httpd/access_log
.. ..
192.168.2.5 - - [12/Aug/2018:17:57:10 +0800] "GET / HTTP/1.1" 200
27 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)"
```

地址伪装策略

知识讲解

- 共享动态公网IP地址实现上网
  - 主要针对外网接口的IP地址不固定的情况
  - 将SNAT改为MASQUERADE即可
  - 对于ADSL宽带拨号连接，网络接口可写为 ppp+

```
[root@gw1 ~]# iptables -t nat -A POSTROUTING \
 -s  192.168.4.0/24  -o eth1  -j SNAT  --to-source  174.16.16.1
```

```
-j MASQUERADE
```

案例4：配置SNAT实现共享上网

课堂练习

1. 搭建内外网案例环境
2. 配置SNAT策略实现共享上网访问

总结和答疑

Technology Tarena 达内科技

表链结构及流程

默认的表、链构成

知识讲解

- 四个表：raw、mangle、nat、filter
- 五种规则链：
  - INPUT、OUTPUT、FORWARD、PREROUTING、POSTROUTING

数据流向及匹配

知识讲解

- 规则链之间的顺序
  - 入站：PREROUTING → INPUT
  - 出站：OUTPUT → POSTROUTING
  - 转发：PREROUTING → FORWARD → POSTROUTING

iptables命令格式

基本用法

知识讲解

- 指令组成
  - iptablls [-t 表名] 选项 [链名] [条件] [-j 目标操作]
- 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
  - 除非设置默认策略，否则必须指定匹配条件
  - 选项/链名/目标操作用大写字母，其余都小写