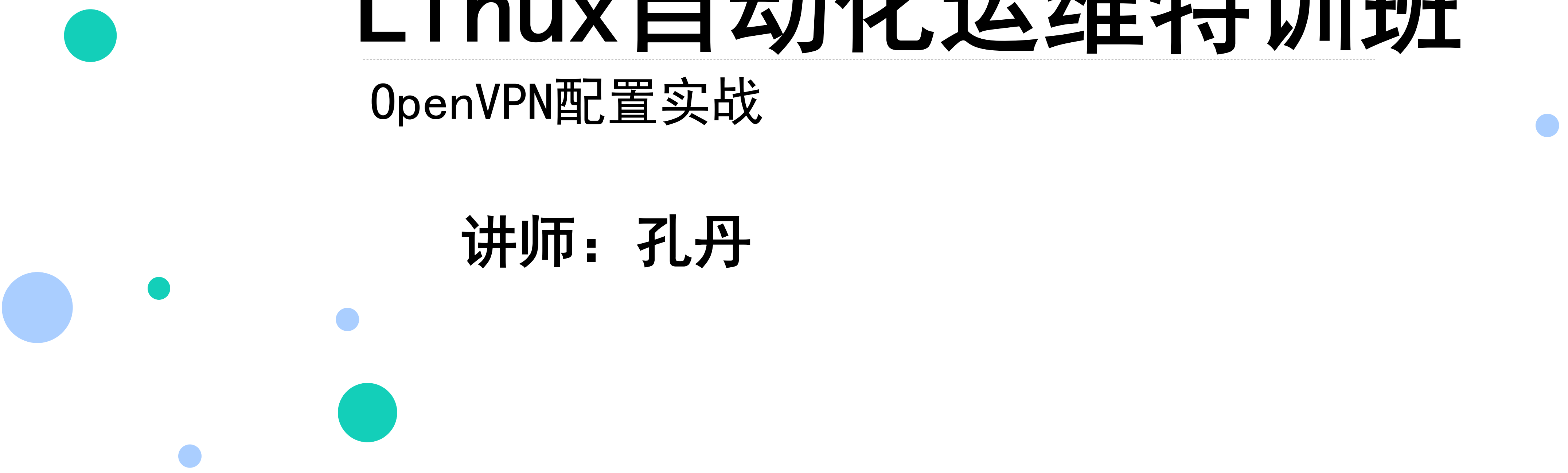


Linux自动化运维特训班

iptables企业级防火墙实战

讲师：孔丹



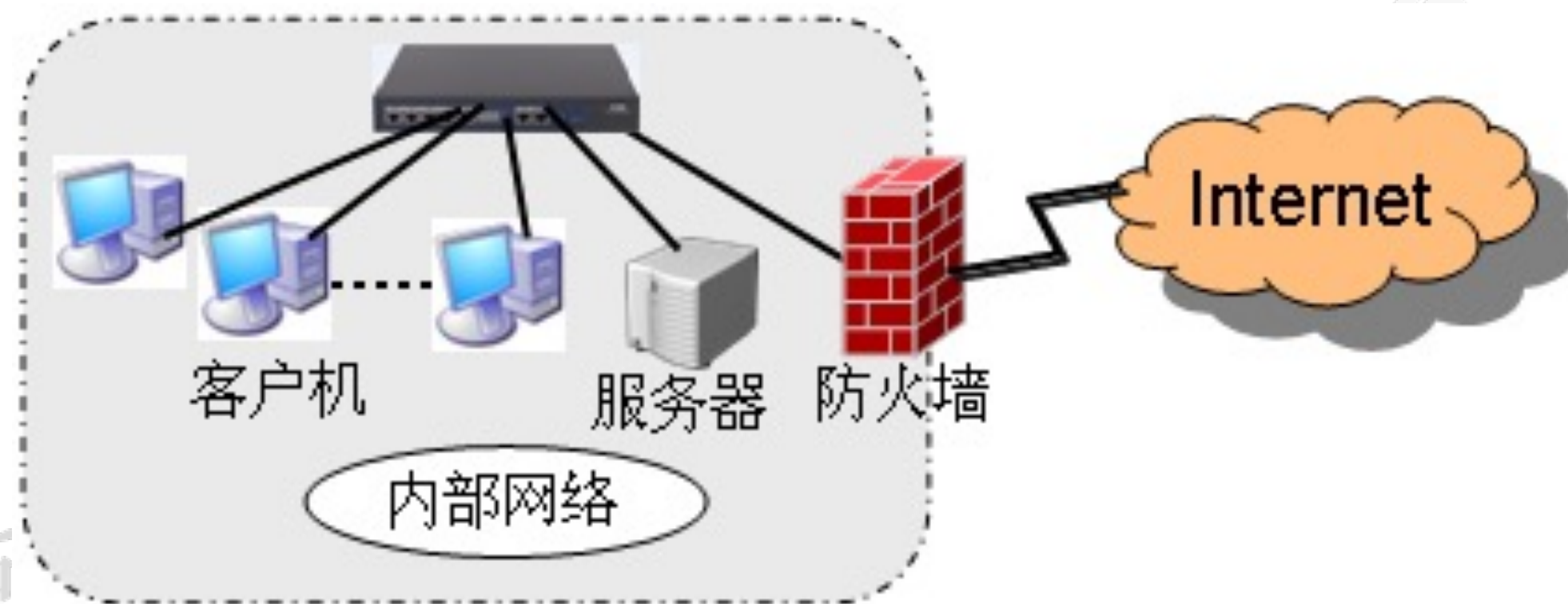
大纲

- 防火墙简介
- iptables简介
- iptables工作流程
- iptables表和链
- iptables命令规则
- 主机防火墙配置
- 配置SNAT和DNAT

版权所有，侵权必究

防火墙简介

- 什么是防火墙？
- 防火墙——是指设置在不同网络(如可信任的企业内部网和不可信的公网)或网络安全域之间的一系列部件的组合。
- 它是不同网络或网络安全域之间信息的唯一出入口,能根据企业的安全策略控制(允许、拒绝、监测)出入网络的信息流,且本身具有较强的抗攻击能力。
- 在逻辑上,防火墙是一个分离器、限制器和分析器,它能有效地监控内部网和Internet之间的任何活动,保证了内部网络的安全。



防火墙简介

- 防火墙的功能

- ①过滤进出网络的数据包, 封堵某些禁止的访问行为

- ②对进出网络的访问行为作出日志记录, 并提供网络使用情况的统计数据, 实现对网络存取和访问的监控审计。

- ③对网络攻击进行检测和告警。

防火墙可以保护网络免受基于路由的攻击, 如IP选项中的源路由攻击和ICMP重定向中的重定向路径, 并通知防火墙管理员。

- ④提供数据包的路由选择和网络地址转换(NAT), 从而解决局域网中主机使用内部IP地址也能够顺利访问外部网络的应用需求。

防火墙简介

□ 防火墙的分类

□ 按采用的技术划分

①包过滤型防火墙——在网络层或传输层对经过的数据包进行筛选。筛选的依据是系统内设置的过滤规则，通过检查数据流中每个数据包的IP源地址、IP目的地址、传输协议(TCP、UDP、ICMP等)、TCP/UDP端口号等因素，来决定是否允许该数据包通过。（包的大小1500字节）

②代理服务器型防火墙——是运行在防火墙之上的一种应用层服务器程序，它通过对每种应用服务编制专门的代理程序，实现监视和控制应用层数据流的作用。

防火墙简介

- 防火墙的分类

- 按实现的环境划分

- ① 软件防火墙：

- 普通计算机+通用的操作系统（如：linux）

- ② 硬件（芯片级）防火墙：基于专门的硬件平台和固化在ASIC芯片来执行防火墙的策略和数据加解密，具有速度快、处理能力强、性能高、价格比较昂贵的特点（如：NetScreen、FortiNet）

- 通常有三个以上网卡接口

- 外网接口：用于连接Internet网；

- 内网接口：用于连接代理服务器或内部网络；

- DMZ接口（非军事化区）：专用于连接提供服务的服务器群

Linux防火墙历史演进与架构

□ Linux防火墙的历史

□ 从1.1内核开始，Linux系统就已经具有包过滤功能了，随着Linux内核版本的不断升级，Linux下的包过滤系统经历了如下4个阶段：

- 在2.0内核中，包过滤的机制是ipfw，管理防火墙的命令工具是ipfwadm。
- 在2.2内核中，包过滤的机制是ipchain，管理防火墙的命令工具是ipchains。
- 在2.4之后的内核中，包过滤的机制是netfilter，防火墙的命令工具是iptables。
- 在3.10之后的内核中，包过滤机制是netfilter，管理防火墙的工具具有firewalld、iptables等。

□ firewalld的官网：<http://www.firewalld.org/>

Linux防火墙历史演进与架构

□ Linux防火墙的架构

□ Linux防火墙系统由以下三层架构的三个子系统组成：

□ ①内核层的netfilter：

- netfilter是集成在内核中的一部分
- 作用是定义、保存相应的过滤规则。
- 提供了一系列的表，每个表由若干个链组成，而每条链可以由一条或若干条规则组成。
- netfilter是表的容器，表是链的容器，而链又是规则的容器。

表→链→规则的分层结构来组织规则

□ ②中间层服务程序：是连接内核和用户的与内核直接交互的监控防火墙规则的服务程序或守护进程，它将用户配置的规则交由内核中的netfilter来读取，从而调整防火墙规则。

□ ③用户层工具：是Linux系统为用户提供的用来定义和配置防火墙规则的工具软件。

企业中安全优化配置原则

- ❑ 尽可能不给服务器配置外网ip，可以通过代理转发或者通过防火墙映射。并发不是特别大情况有外网ip，可以开启防火墙服务。
- ❑ 大并发的情况，不能开iptables，影响性能，利用硬件防火墙提升架构安全
- ❑ 生产环境中iptables的实际应用

主要应用方向

- 1、主机防火墙（filter表的INPUT链）。
- 2、局域网共享上网（nat表的POSTROUTING链）。相当于路由器，NAT功能。
- 3、端口及IP映射（nat表的PREROUTING链），硬件防火墙的NAT功能。
- 4、IP一对一映射。

iptables简介

- Netfilter/Iptables（以下简称Iptables）unix/linux系统自带的一款优秀且完全免费的基于包过滤的防火墙工具，它的功能十分强大使用非常灵活，可以对流入、流出及流经服务器的数据包进行精细的控制。特别是它可以在一台非常低的硬件配置下运行非常好，提供几百台机器的办公上网环境毫不逊色数万RMB企业级专业的路由器防火墙。
- Iptables是linux2.4及2.6内核中集成的服务。其功能与安全性比其老一辈ipfwadm、ipchains强大，一般认为Iptables工作在OSI七层的二、三层、四层。

iptables的名词术语

□ 什么是容器？

容器本身就是指装东西的，如（箱、包、坛）。词典里面对容器解释，容器是用来包装或装载物品的储存器（如箱、坛、罐）或者成形或柔软不成形的包覆材料。在iptables中，就是用来描述这种包含或者说属于的关系。

□ 什么是Netfilter/Iptables？

Netfilter是表（tables）的容器。比如，如果把Netfilter比作某小区的一栋大楼，那么表（tables）就是楼里的其中一套房子。这套房子“表（tables）”属于这栋楼“Netfilter”。比如家里所在的小区的就是Netfilter。

□ 什么是表（tables）？

表（tables）是链的容器，即所有的链（chains）都属于表（tables）。如上，如果把Netfilter看成是某小区的一栋楼，那么表（tables）就是楼里的某一套房子。表可能不止一个。

iptables的名词术语

□ 什么是链（chains）？

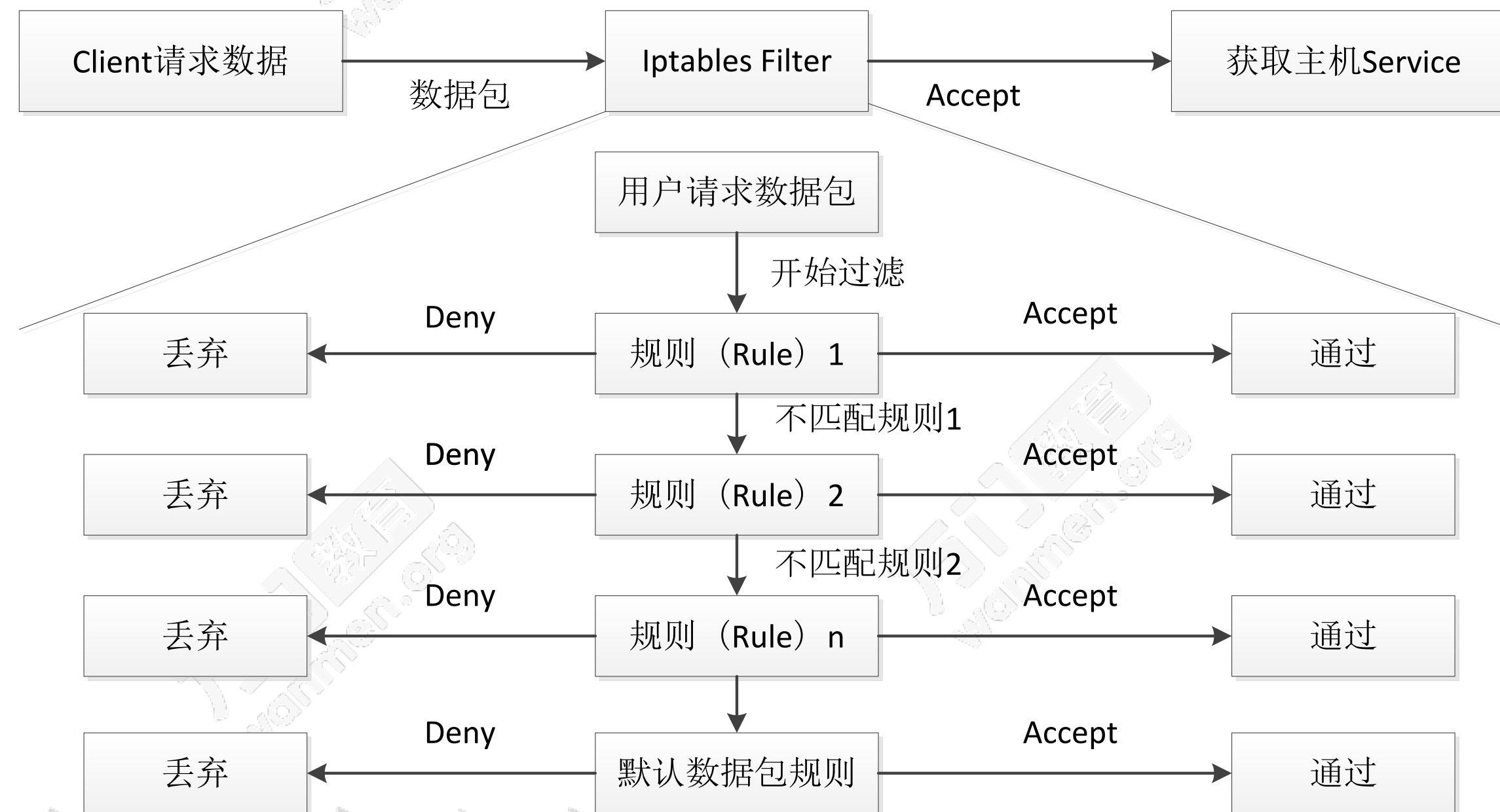
链（chains）是规则（Policies）的容器，链属于表。如果把表（tables）当作是一套房子，那么链（chains）就可以说是房子内的家具（桌子、柜子等），每一套房子内都可能会有桌子，柜子等。

□ 什么是规则（Policy）？

规则（Policy）属于链（chains），就是iptables一系列过滤信息规范和具体的操作方法。可以理解为为购买什么家具，并且如何摆放、设计的更符合需求等。

iptables的工作流程

- ❑ Iptables是采用数据包过滤机制工作的，所以它会对请求的数据包的包头数据进行分析并根据我们预先设定的规则进行匹配来决定是否可以进入、流出、流经主机。下面我们以iptables进入主机进行过滤的流程图为例进行讲解。



版权所有，侵权必究

iptables的工作流程

- 注意：
 - 防火墙规则的顺序默认为从前到后依次执行，遇到匹配的规则就不在继续向下查，如果遇到不匹配的规则则会继续向下进行。
 - 重点：匹配上了拒绝规则也是匹配。因此，不在继续向下进行。
 - 例如：同时执行以下规则
- ```
iptables -A INPUT -p tcp --dport 3306 -j DROP
```
- ```
# iptables -A INPUT -p tcp --dport 3306 -j ACCEPT
```
- 此时，第一条规则匹配，检查3306端口是不通的。

Iptables的表（tables）和链（chains）

- ❑ Iptables表（tables）和链（chains）的分类
- ❑ 默认情况下，Iptables根据功能和表的定义划分，最常用的有三个表，分别为filter、nat、mangle，其中，每个表又各自包含不同的操作链（chains）。
- ❑ 提示：用man iptables会发现还有一个表raw，平时几乎用不到。raw表：确定是否对该数据包进行状态跟踪
- ❑ 表和链的对应关系

表 (tables)	链 (chains)				
	INPUT	FORWARD	OUTPUT	PREROUTING	POSTROUTING
filter	✓	✓	✓	✗	✗
<u>nat</u>	✗	✗	✓	✓	✓
mangle	✓	✓	✓	✓	✓
注：✓ 表示有，✗ 表示无					

Iptables的表（tables）和链（chains）

表（tables）	链（chains）	
Filter	这是默认表，实现防火墙数据过滤功能。	
	INPUT	对于指定到本地套接字的包，即到达本地防火墙服务器的数据包。
	FORWARD	路由穿过的数据包，即经过本地防火墙服务器的数据包。
	OUTPUT	本地创建的数据包
NAT	当遇到新创建的数据包连接时将参考这个表	
	PREROUTING	一进来就对数据包进行改变
	OUTPUT	本地创建的数据包在路由前进行改变
	POSTROUTING	在数据包即将出去时改变数据包信息
Mangle	这个表专门用于改变数据包	
	INPUT	进入到设备本身的包
	FORWARD	对路由后的数据包信息进行修改
	PREROUTING	在路由之前更改传入的包

Iptables的表（tables）和链（chains）

□ Iptables的filter表介绍

filter表：	和主机自身有关，负责防火墙功能（过滤本机流入、流出数据包）。是iptables默认使用的表。这个表定义了三个链（chains），说明如下：	
	INPUT	负责过滤所有目标地址是本机（防火墙）地址的数据包。通俗的讲，就是过滤进入主机的数据包。
	FORWAED	负责转发流经主机但不进入本机的数据包。起转发的作用，和Nat表关系很大，后面详细介绍。
	OUTPUT	处理所有源地址是本机地址的数据包，通俗的讲就是处理从主机发出去的数据包。
附带英文解释：filter: This is the default table (if no -t option is passed). It contains the built-in chains INPUT (for packets destined to local sockets), FORWARD (for packets being routed through the box), and OUTPUT (for locally-generated packets).		

Iptables的表（tables）和链（chains）

▣ Iptables的nat表介绍

nat表：	英文全拼（Network Address Translation），是网络地址转换的意思，即负责来源与目的ip地址和port的转换。和主机本身无关。一般用于局域网多人共享上网或者内网ip映射外网ip及不同端口转换服务等功能，nat表的功能很重要。这个表定义了三个链（chains）说明如下：	
	OUTPUT	和主机发出去的数据包有关。在数据包路由之前改变主机产生的数据包的目标地址等。
	PREROUTING	在数据包刚到达防火墙时，进行路由判断之前执行的规则，改变包的目的地地址（DNAT功能）、端口等。把公网IP映射到局域网的机器上。此链多用于把外部Ip地址端口的服务，映射为内部IP地址及端口。
	POSTROUTING	在数据包离开防火墙时进行路由判断之后执行的规则，改变包的源地址（SNAT）、端口等。此链多用于局域网共享上网，把所有局域网的地址，转换为公网地址上。
附带英文解释：nat: This table is consulted when a packet that creates a new connection is encountered. It consists of three built-ins:PREROUTING (for altering packets as soon as they come in),OUTPUT (for altering locally-generated packets before routing), and POSTROUTING (for altering packets as they are about to go out).		

Iptables的表（tables）和链（chains）

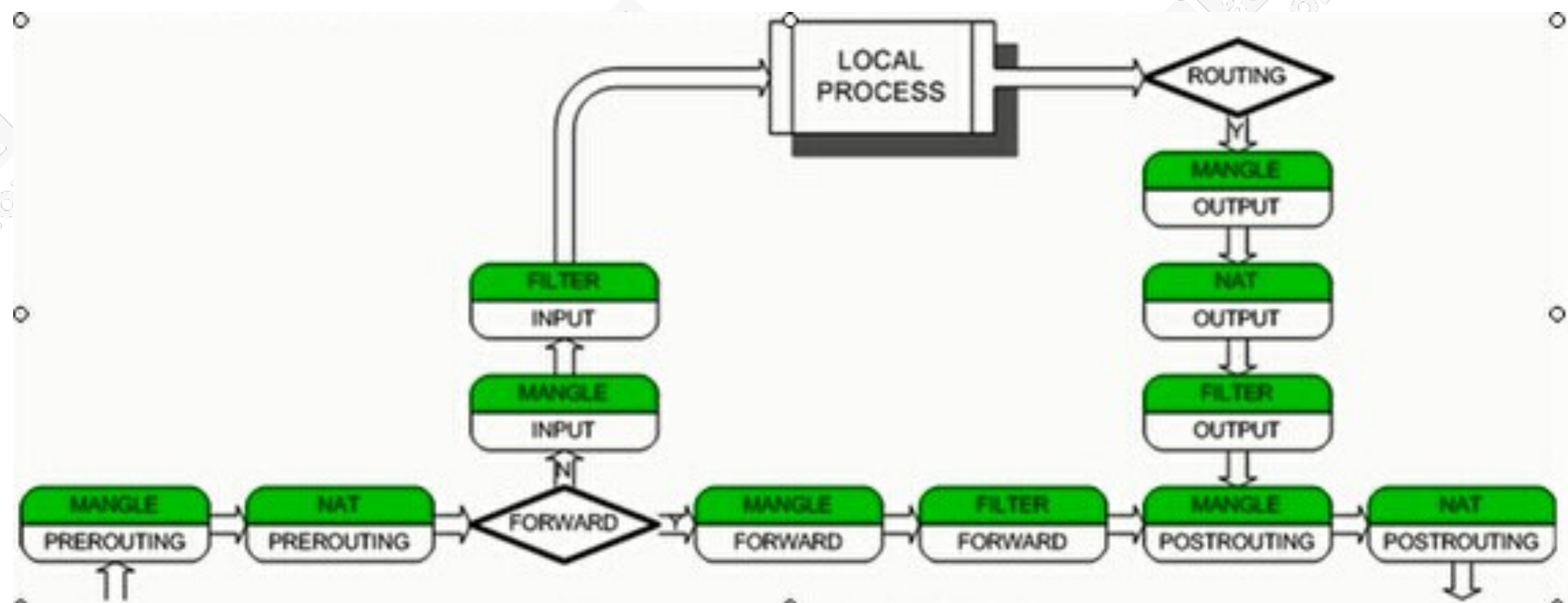
▣ Iptables的mangle表介绍

mangle表:	主要负责修改数据包中特殊的路由标记，如TTL，TOS，MARK 等，这个表定义了5个链（chains），说明如下：	
	INPUT	同filter表的INPUT
	FORWARD	同filter表的FORWARD
	OUTPUT	同filter表的OUTPUT
	PREROUTING	同nat表的PREROUTING
	POSTROUTING	同nat表的POSTROUTING
附带英文解释：mangle: This table is used for specialized packet alteration. Until kernel 2.4.17 it had two built-in chains: PREROUTING (for altering incoming packets before routing) and OUTPUT (for altering locally-generated packets before routing). Since kernel 2.4.18, three other built-in chains are also supported: INPUT (for packets coming into the box itself), FORWARD (for altering packets being routed through the box), and POSTROUTING (for altering packets as they are about to go out).		

版权所有，侵权必究

Iptables的表与链工作流程图

□ 下面图描绘了netfilter对数据包的整个处理流程：

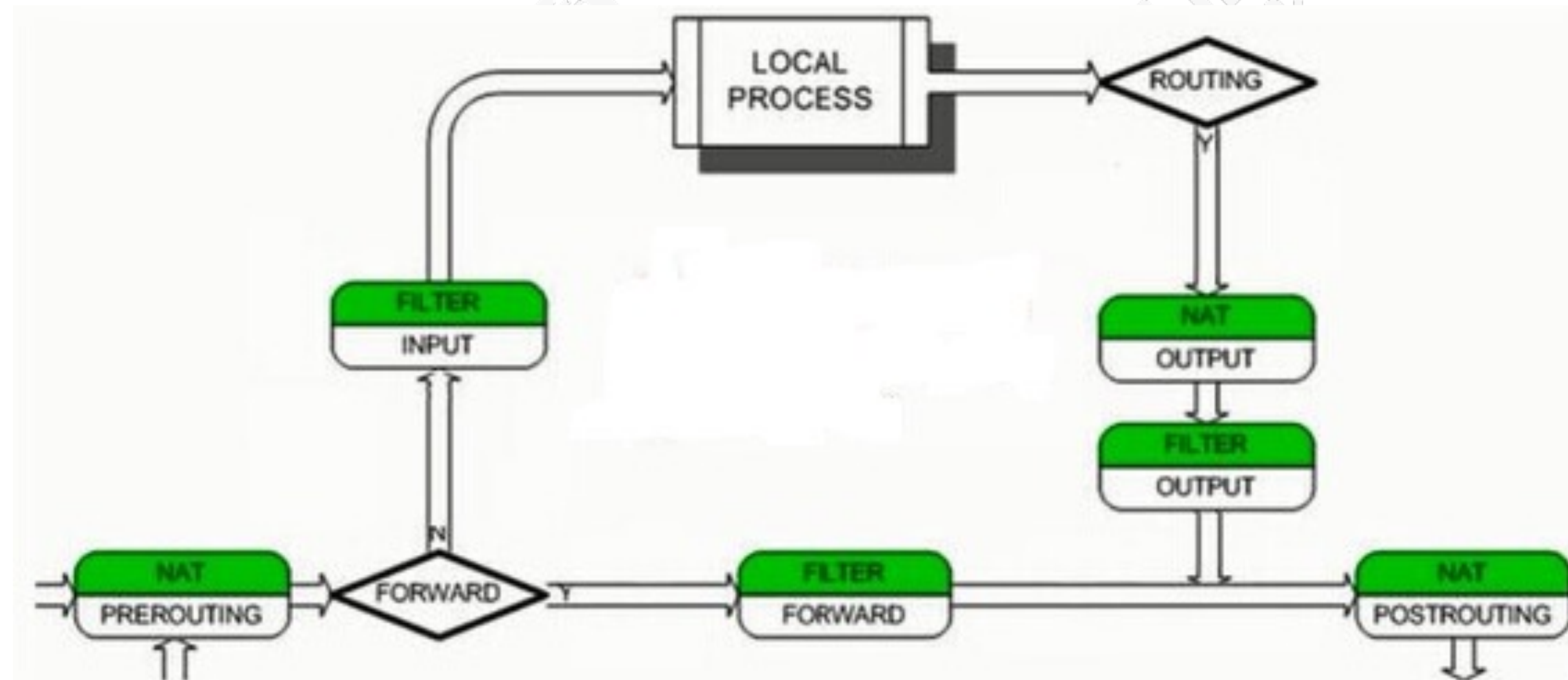


iptables是采用数据包过滤机制工作的，所以它会对请求的数据包的包头数据进行分析，并根据我们预先设定的规则进行匹配来决定是否可以进入主机。

数据包的流向是从左向右的。

Iptables的表与链工作流程图

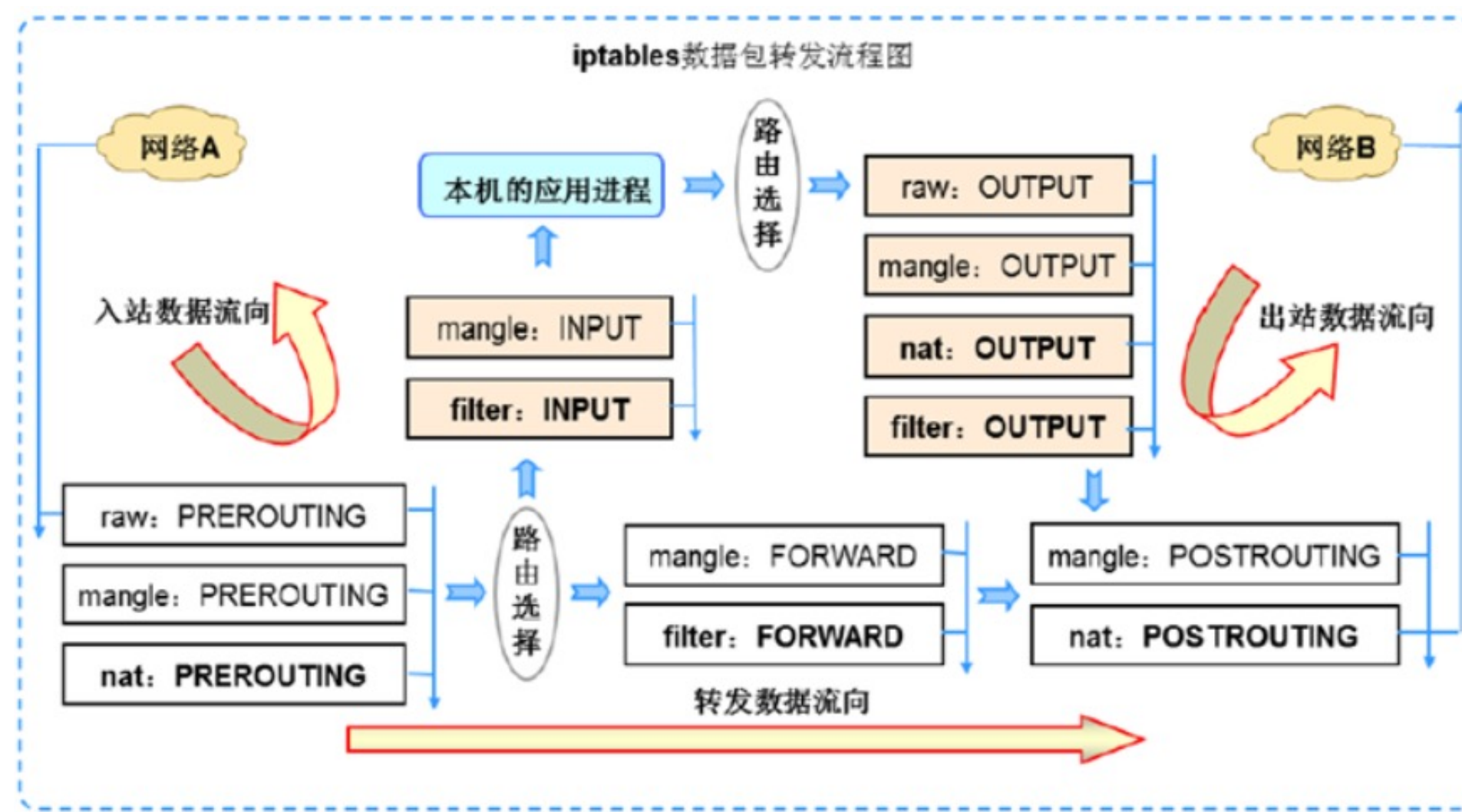
- 由于工作中，我们很少用到mangle表，因此，为了更好的理解掌握常用的iptables技术，把上图简化为如下



从上图我们可以看出，当数据包进入时，首先经过的是NAT表的PREROUTING的链，接着会分两条路走，如果是进入主机就通过FILTER表的INPUT链，然后到达主机内部（LOCAL PROCESS），最后通过NAT表与FILTER的OUTPUT返回；如果是流经主机则会通过FILTER表的FORWARD链，最后出站时通过NAT表的POSTROUTING链。

Iptables的表与链工作流程图

□ iptables数据包转发流程图



从上图我们可以看出，当数据包进入时，首先经过的是NAT表的PREROUTING的链，接着会分两条路走，如果是进入主机就通过FILTER表的INPUT链，然后到达主机内部（LOCAL PROCESS），最后通过NAT表与FILTER的OUTPUT返回；如果是流经主机则会通过FILTER表的FORWARD链，最后出站时通过NAT表的POSTROUTING链。

iptables命令规则

□ 显示相关参数

- n/--numeric 以数字的方式显示地址或端口信息
- L/ --list 列出一个链或所有链中的规则信息
- list-rules/-S Print the rules in a chain or all chains
- line-number 当列出规则信息时，打印规则行号
- v 显示详细信息，可以叠加
- h 显示帮助信息

□ 基本语法

iptables [-t 表名] 命令选项 [链名] [条件匹配] [-j 目标动作或跳转]

iptables命令规则

❑ 查看默认规则: `iptables -L -n`

❑ 清除默认规则

`iptables -F` 清除所有规则

`iptables -X` 删除用户自定义的链

`iptables -Z` 链的计数器清零

iptables命令规则

□ 配置常用参数

- t 表名称 指定配置哪个表，指定配置表名称。
- append/-A 链名称 附加或追加相应规则策略，到指定链(链名称必须大写)，默认将配置的规则插入到最后一条。
- check/-C Check for the existence of a rule
- insert/-I 链名称 插入相应规则策略，到指定链上，默认将配置的规则插入到第一条（可以根据规则序号插入到指定位置）
- 封IP地址使用。
- delete/-D 链名称 删除指定的规则(可以根据规则序号进行删除)
- replace/-R Replace rule rulenum (1 = first) in chain
- P(大写)链名称 改变链上的最终默认规则策略
- new/-N 创建新的用户定义链
- p 协议名称 指定规则的协议名称 all tcp udp icmp
- dport 指定匹配的目标端口信息
- sport 指定匹配的源端口信息

版权所有，侵权必究

iptables命令规则

□ 配置常用参数

-j 动作 匹配数据包后的动作

ACCEPT 允许

DROP 丢弃(没有响应)

REJECT 拒绝(回应请求者明确的拒绝)

MASQUERADE 伪装上网时使用

SNAT 共享地址上网

DNAT 目的地址改写

-i 在INPUT链配置规则中，指定从哪一个网卡接口进入的流量
(只能配置在INPUT链上)

-o 在OUTPUT链配置规则中，指定从哪一个网接口出去的流量
(只能配置在OUTPUT链上)

-s 指定源IP地址或源网段信息

-d 指定目标IP地址或目标网段信息

iptables命令规则

□ 配置扩展参数

-m 模块 表示增加扩展，匹配功能扩展匹配（可以加载扩展参数）

multiport 实现不连续多端口扩展匹配

icmp 使用icmp的扩展

state 状态模块扩展

--icmp-type 只有类型8是真正会影响ping，或者也可以采用any；了解很多icmp类型iptables -p icmp -h

--limit n/{second/minute/hour} 指定时间内的请求速率”n”为速率，后面为时间分别为：秒 分 时

--limit-burst [n] 在同一时间内允许通过的请求”n”为数字，不指定默认为5

--exact/-x 扩展数字（显示精确数值）

注意：在iptables中所有链名必须大写，表明必须小写，动作必须大写，匹配必须小写

版权所有，侵权必究

iptables命令规则

□ iptables防火墙规则的保存与恢复

使用命令iptables-save来保存规则。一般用
iptables-save > /etc/sysconfig/iptables
生成保存规则的文件 /etc/sysconfig/iptables,

也可以用

```
service iptables save
```

它能把规则自动保存在/etc/sysconfig/iptables中。

iptables命令规则

□ iptables 规则

1、禁止 ssh 默认的 22 端口。

```
# iptables -A INPUT -p tcp --dport 22 -j DROP
```

#iptables默认用的表示filter表

提示：执行此命令后，终端无法ssh连接，需要先放行本地的ssh连接，先添加下面命令

```
iptables -A INPUT -p tcp -m state --state  
ESTABLISHED,RELATED -j ACCEPT
```

2、禁止192.168.150.0/24网段连入

```
# iptables -A INPUT -i ens33 -s 192.168.150.0/24 -j DROP
```

3、测试[!(非)]

```
iptables -I INPUT -p icmp --icmp-type 8 -s ! 192.168.1.101  
-j DROP
```

只允许合法地址192.168.1.101这个地址ping防火墙。

iptables命令规则

□ iptables 规则实践

4、匹配指定的协议

```
iptables -A INPUT -p tcp
```

```
iptables -A INPUT -p udp
```

5、匹配主机

```
iptables -A INPUT -s 192.168.1.101
```

6、匹配网络

```
iptables -A INPUT -s 192.168.1.0/24
```

7、匹配单一端口

```
iptables -A INPUT -p tcp -s --sport 53
```

```
iptables -A INPUT -p udp -s --dport 53
```

iptables命令规则

□ iptables 规则实践

8、匹配端口范围

```
iptables -A INPUT -p tcp --sport 22:80
```

```
iptables -I INPUT -p tcp -m multiport --dport 21, 22, 23, 24 -  
j ACCEPT
```

```
iptables -I INPUT -p tcp --dport 3306:8809 -j ACCEPT
```

9、匹配ICMP端口和ICMP类型

```
iptables -A INPUT -p icmp --icmp-type 8
```

```
iptables -A INPUT -p icmp -m icmp --icmp-type any -j ACCEPT
```

```
iptables -A FORWARD -s 192.168.1.0/24 -p icmp -m icmp --  
icmp-type any -j ACCEPT
```

10) 匹配指定的网络接口

```
iptables -A INPUT -i eth0
```

```
iptables -A FORWARD -o eth0
```

版权所有，侵权必究

iptables命令规则

□ iptables 常用规则实践

1、仅允许内部合法的IP地址访问服务器

```
iptables -A INPUT -s 203.24.12.0/24 -p all -j ACCEPT
```

```
iptables -A INPUT -s 123.42.61.96/27 -p all -j ACCEPT
```

```
iptables -A INPUT -s 192.168.1.0/24 -p all -j ACCEPT
```

```
iptables -A INPUT -s 172.16.0.0/24 -p all -j ACCEPT
```

提示：合法的IP段为，办公IP，IDC的内外网IP段及公司机房的IP段。

2、仅运行内部合法的IP段访问监控服务nagios

```
iptables -A INPUT -s 192.168.1.0/24 -p tcp --dport 5666 -j  
ACCEPT
```

```
iptables -A INPUT -s 203.24.12.0/24 -p tcp --dport 5666 -j  
ACCEPT
```

iptables命令规则

□ iptables 常用规则实践

3、仅允许内部合法的IP段访问MySQL数据库和oracle数据库。

```
iptables -A INPUT -s 192.168.1.0/24 -p tcp --dport 3306 -j  
ACCEPT
```

```
iptables -A INPUT -s 192.168.1.0/24 -p tcp --dport 1521 -j  
ACCEPT
```

4、仅允许内部合法的IP段访问SSH远程连接服务

```
iptables -A INPUT -s 192.168.1.0/24 -p tcp --dport 52112 -j  
ACCEPT
```

```
iptables -A INPUT -s 203.24.12.0/24 -p tcp --dport 52112 -j  
ACCEPT
```

提示：处于安全考虑，不使用默认22端口，修改为52112。

iptables命令规则

□ iptables 常用规则实践

5、对HTTP服务的不同限制

A、对外提供http服务的业务，要允许http服务通过，并且不限制IP。

```
iptables -A INPUT -p tcp --dport 80 -j ACCEPT
```

B、对内提供http服务的业务，一般用特殊端口，并且限制合法IP连接或VPN连接。

```
iptables -A INPUT -s 192.168.1.0/24 -p tcp -m multiport --  
dport 8080,8081,8082,8888 -j ACCEPT
```

```
iptables -A INPUT -s 203.24.12.0/24 -p tcp -m multiport --  
dport 8080,8081,8082,8888 -j ACCEPT
```

6、snmp的限制

```
iptables -A INPUT -s 192.168.1.0/24 -p udp --dport 161 -j  
ACCEPT
```

```
iptables -A INPUT -s 203.24.12.0/24 -p udp --dport 161 -j  
ACCEPT
```


iptables命令规则

□ iptables 常用规则实践

7、rsync服务的限制

```
iptables -A INPUT -s 192.168.1.0/24 -p tcp -m tcp --dport  
873 -j ACCEPT
```

```
iptables -A INPUT -s 203.24.12.0/24 -p tcp -m tcp --dport  
873 -j ACCEPT
```

8、nfs服务的限制

```
iptables -A INPUT -s 192.168.1.0/24 -p tcp -m multiport --  
dport 111,892,2049 -j ACCEPT
```

```
iptables -A INPUT -s 192.168.1.0/24 -p udp -m multiport --  
dport 111,892,2049 -j ACCEPT
```

iptables命令规则

□ iptables 常用规则实践

9、ftp服务的限制

```
iptables -A INPUT -p tcp --dport 21 -j ACCEPT
```

```
iptables -A INPUT -m state --state ESTABLISHED,RELATED -j  
ACCEPT
```

```
iptables -A OUTPUT -m state --state ESTABLISHED,RELATED -j  
ACCEPT
```

提示：上面内容表示对已经建立连接的数据包，或者发出去的数据包允许通过。

10、icmp协议的限制

```
iptables -A INPUT -p icmp --icmp-type 8 -j ACCEPT
```

```
iptables -A INPUT -p icmp -m icmp --icmp-type any -j ACCEPT
```

```
iptables -A FORWARD -s 192.168.1.0/24 -p icmp -m icmp --  
icmp-type any -j ACCEPT
```

版权所有，侵权必究

主机防火墙配置

□ 手工配置

一种模型是，有明确的许可才可。

另一种是把明确的不合法的请求禁止。

1、清除所有的规则

```
iptables -F
```

```
iptables -Z
```

```
iptables -X
```

2、配置运行SSH登录端口进入

```
iptables -A INPUT -p tcp --dport 22 -s 192.168.79.0/24 -j  
ACCEPT
```

3、配置运行lo接口的进入和流出

```
iptables -A INPUT -i lo -j ACCEPT
```

```
iptables -A OUTPUT -o lo -j ACCEPT
```

主机防火墙配置

□ 手工配置

4、设置默认的防火墙禁止和允许规则

```
iptables -P INPUT DROP
```

```
iptables -P FORWARD DROP
```

```
iptables -P OUTPUT ACCEPT
```

5、开启信任的IP段

```
iptables -A INPUT -s 192.168.79.0/24 -p all -j ACCEPT
```

```
iptables -A INPUT -s 172.16.0.0/24 -p all -j ACCEPT
```

```
iptables -A INPUT -s 203.24.12.0/24 -p all -j ACCEPT
```

提示：运行IDC、公司内网段和VPN地址段访问。

6、允许http服务无条件通过

```
iptables -A INPUT -p tcp --dport 80 -j ACCEPT
```

主机防火墙配置

□ 手工配置

7、允许icmp类型协议通过

```
iptables -A INPUT -p icmp -m icmp --icmp-type any -j ACCEPT
iptables -A INPUT -p icmp -s 192.168.79.0/24 -m icmp --
    icmp-type any -j ACCEPT
iptables -A INPUT -p icmp --icmp-type 8 -j ACCEPT
```

8、允许关联的状态包通过

```
iptables -A INPUT -m state --state ESTABLISHED,RELATED -j
    ACCEPT
iptables -A OUTPUT -m state --state ESTABLISHED,RELATED -j
    ACCEPT
```

注意：配置完毕要保存配置。

配置SNAT和DNAT

▣ nat表相关名词

SNAT

源地址转换（Source Network Address Translation）是Linux防火墙的一种地址转换操作，也是iptables命令中的一种数据包控制类型，并根据指定条件修改数据包的源IP地址。

SNAT策略的典型应用环境：局域网主机共享单个公网IP地址接入Internet

DNAT

目标地址转换，Destination Network Address Translation，是Linux防火墙的另一种地址转换操作，也是iptables命令中的一种数据包控制类型，其作用是根据指定条件修改数据包的目标IP地址、目标端口。

DNAT是一种改变数据包目的IP地址等功能的技术，它可以使多台服务器共享一个IP地址连如internet，并且继续对外提供服务。通过对同一个外部ip地址分配不同端口，映射到不同的内部服务器的ip和端口，从而实现各种服务的目的。

DNAT策略的典型应用环境：在Internet中发布位于企业局域网内的服务器

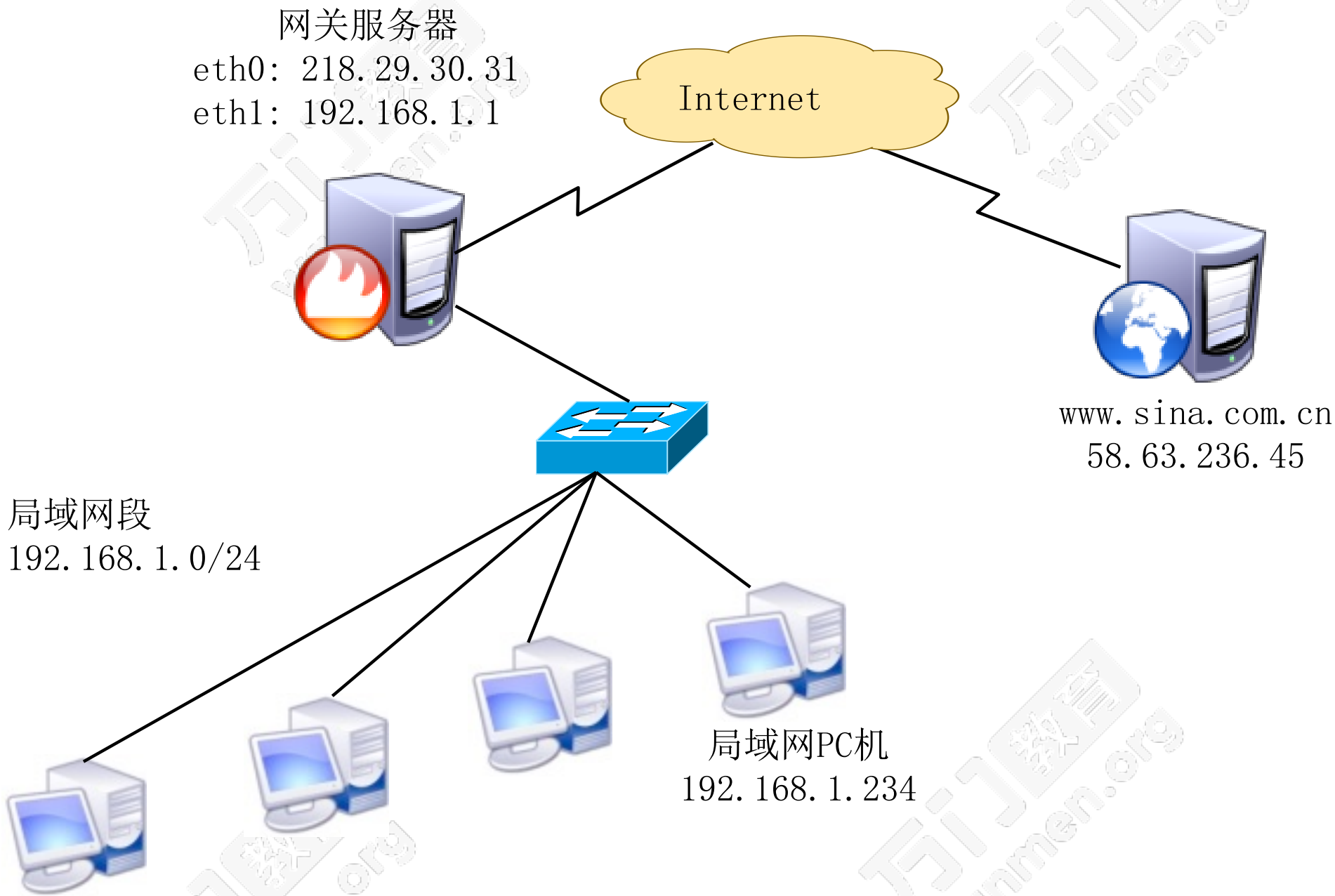
MASQUERADE

地址伪装，算是snat中的一种特例，可以实现自动化的snat。

典型应用：共享动态IP地址上网

配置SNAT和DNAT

生产实战案例
办公室局域网共享上网--配置SNAT实现。



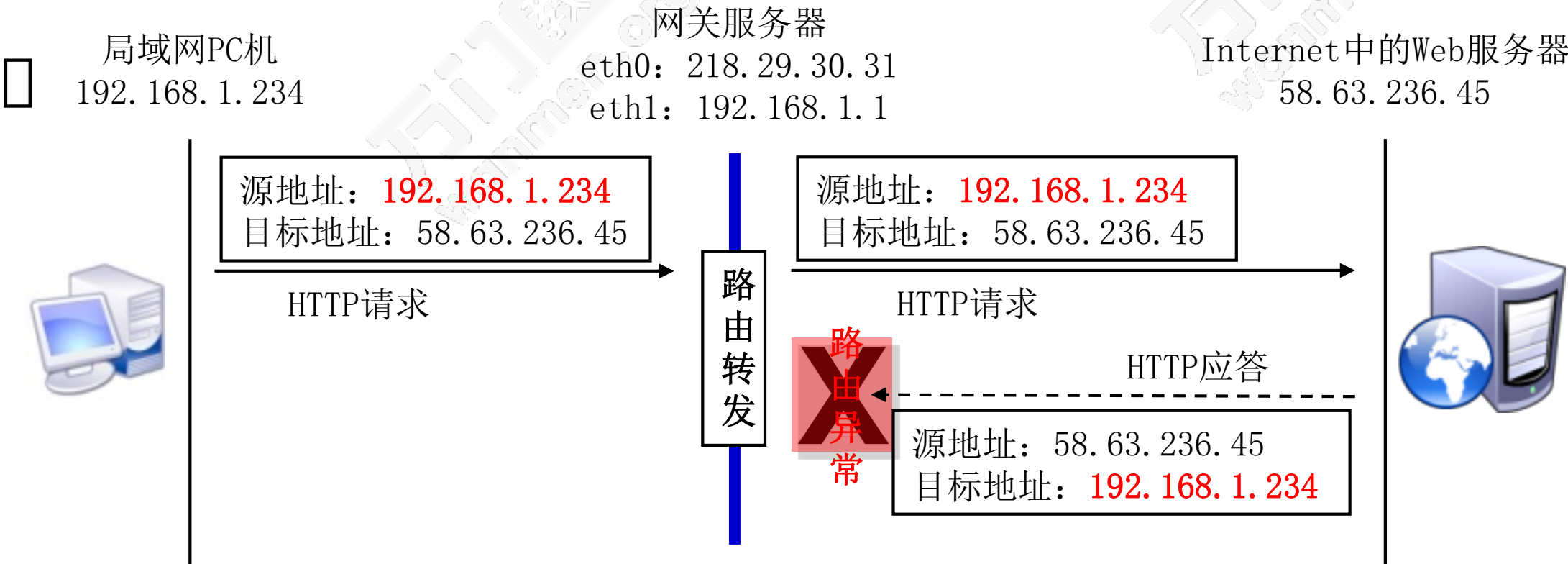
版权所有，侵权必究

配置SNAT和DNAT

生产实战案例

办公室局域网共享上网--配置SNAT实现。

1) 只开启路由转发功能，未做地址转换的情况；



从局域网PC机访问Internet的数据包经过网关转发后其源IP地址保持不变；

当Internet中的主机收到这样的请求数据包后，响应数据包将无法正确返回，从而导致访问失败。

配置SNAT和DNAT

□ 生产实战案例

办公室局域网共享上网--配置SNAT实现。

1) 只开启路由转发功能，未做地址转换的情况；

开启路由转发方法：

临时开启

方法1：# echo 1 > /proc/sys/net/ipv4/ip_forward

方法2：# sysctl -w net.ipv4.ip_forward=1

永久开启：

修改配置文件/etc/sysctl.conf

net.ipv4.ip_forward=1

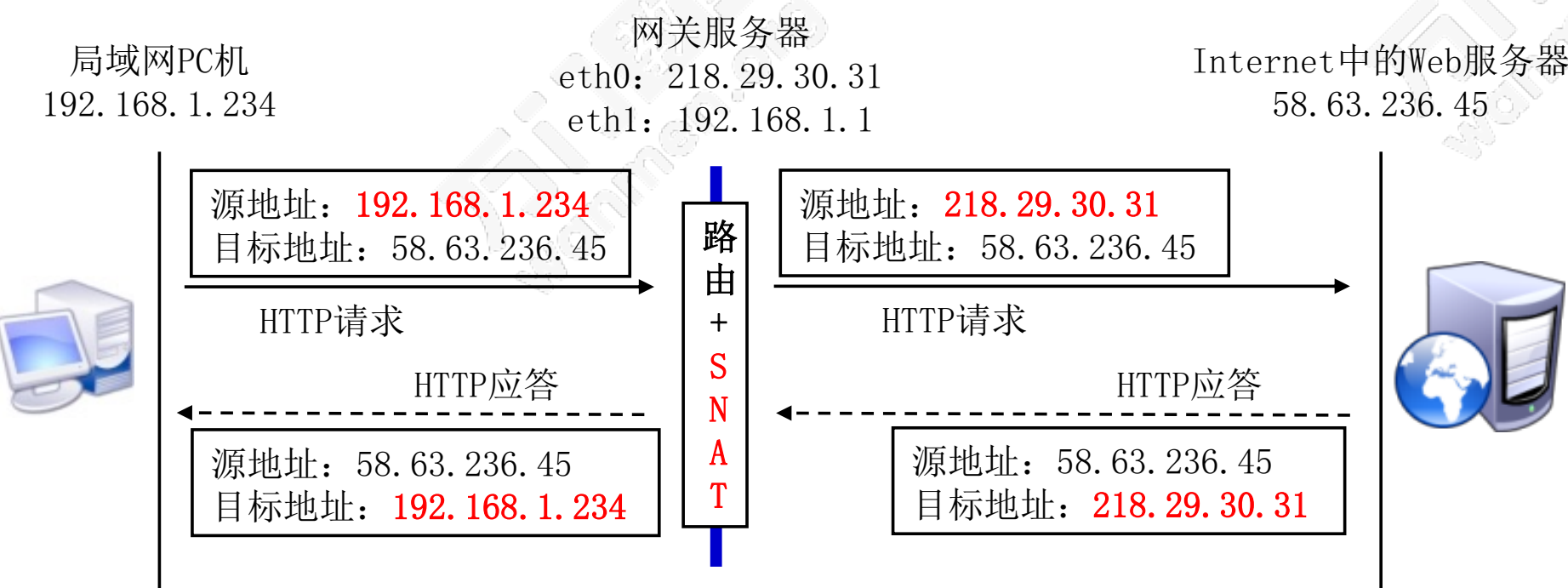
修改完毕执行 sysctl -p

配置SNAT和DNAT

生产实战案例

办公室局域网共享上网--配置SNAT实现。

2) 开启路由转发，并设置SNAT转换的情况：



局域网PC机访问Internet的数据包到达网关服务器时，会先进行路由选择；

如果该数据包需要从外网接口eth0向外转发，则将其源IP地址192.168.1.234修改为网关的外网接口地址218.29.30.31，然后发送给目标主机。

这种访问方式的优点：

Internet中的服务器并不知道局域网PC机的实际IP地址，中间的转换完全由网关主机完成，起到了保护内部网络的作用。

配置SNAT和DNAT

□ 生产实战案例

办公室局域网共享上网--配置SNAT实现。

配置步骤：

前提：

- 局域网各主机正确设置IP地址/子网掩码
- 局域网各主机正确设置默认网关地址
- Linux网关支持IP路由转发

1) 开启路由转发；

2) 设置SNAT规则；

```
iptables -t nat -A POSTROUTING -s 192.168.1.0/24 -o eth0 -j
```

```
SNAT --to-source 218.29.30.31
```

3) 测试

配置SNAT和DNAT

□ 生产实战案例

办公室局域网共享上网--配置SNAT实现。

配置步骤：

共享动态IP地址上网：

MASQUERADE —— 地址伪装

适用于外网IP地址不固定的情况

对于ADSL拨号连接，接口通常为ppp0、ppp1

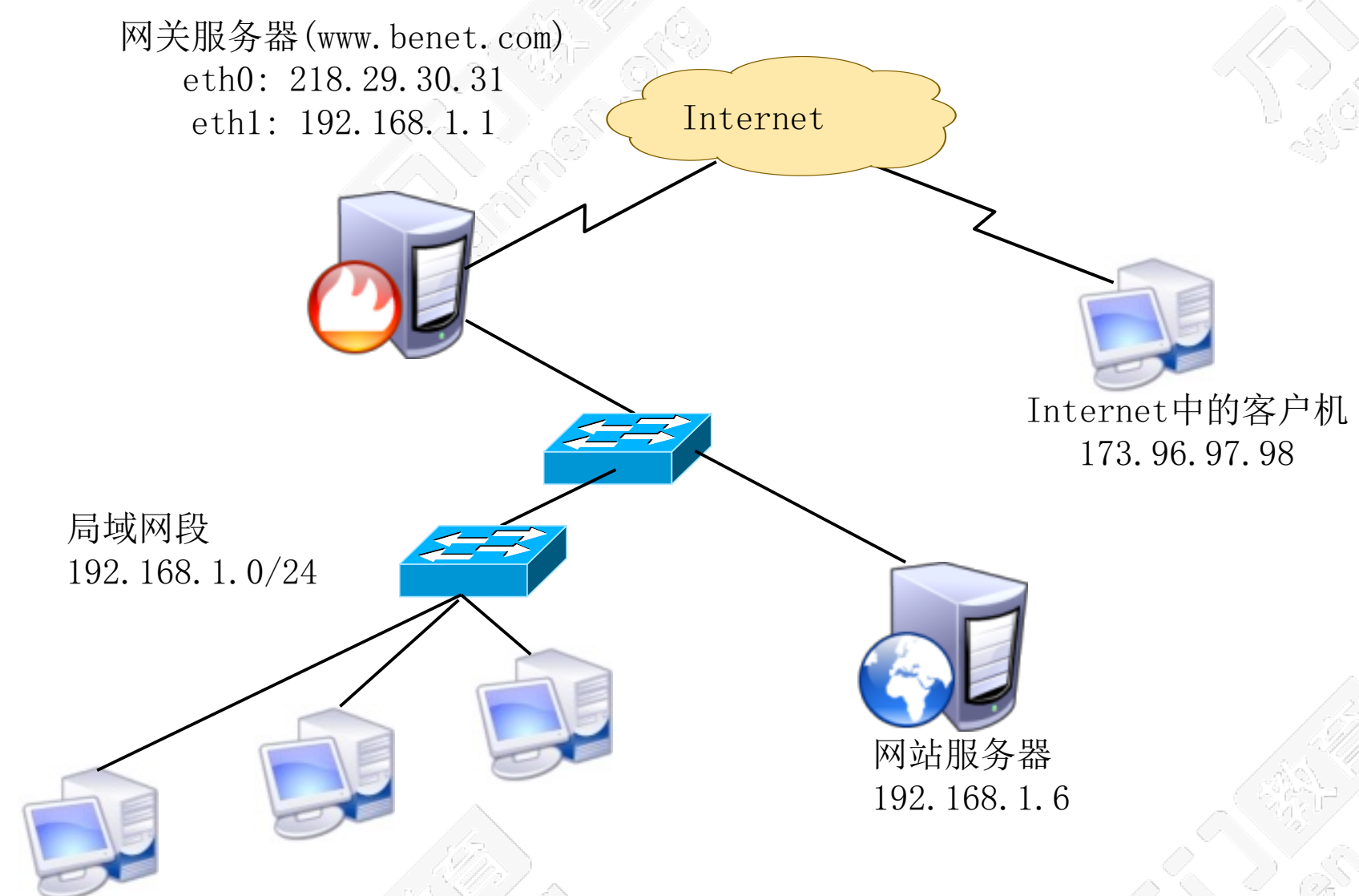
将SNAT规则改为MASQUERADE即可

```
[root@localhost ~]# iptables -t nat -A POSTROUTING -s  
192.168.1.0/24 -o ppp0 -j MASQUERADE
```

版权所有，侵权必究

配置SNAT和DNAT

□ 生产实战案例
发布内网服务器--配置DNAT实现。



版权所有，侵权必究

配置SNAT和DNAT

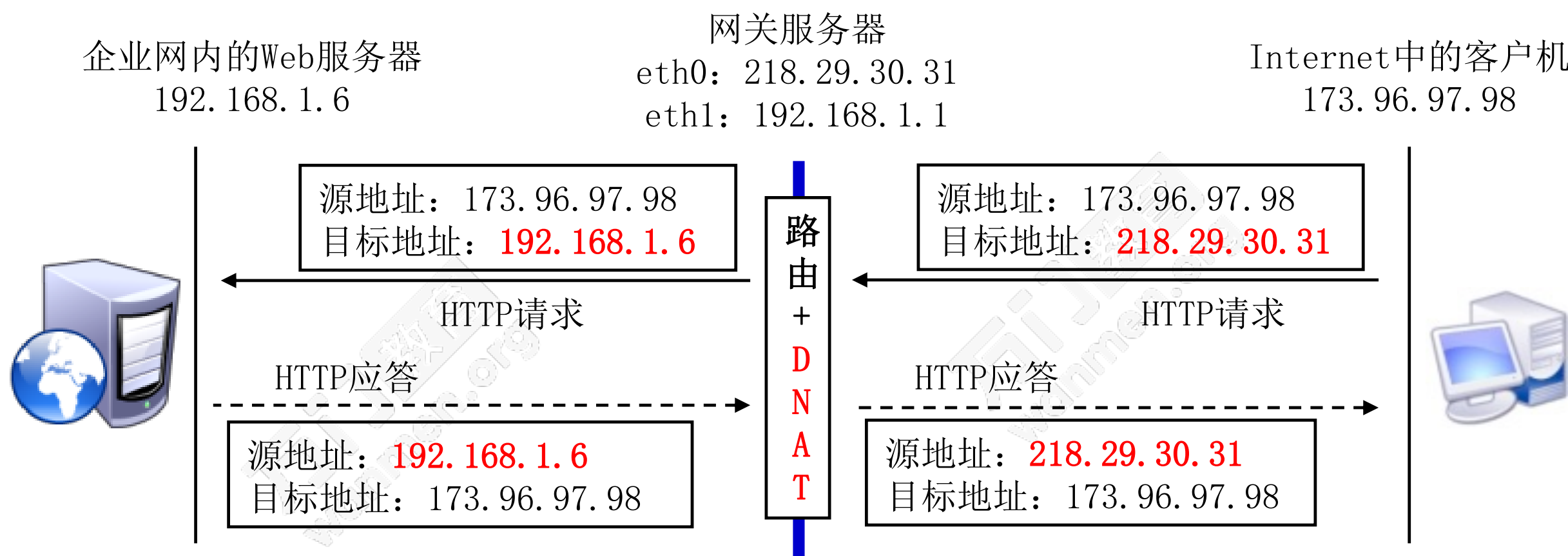
生产实战案例

发布内网服务器--配置DNAT实现。

提示：

SNAT用来修改源IP地址，而DNAT用来修改目标IP地址、目标端口；
SNAT只能用在nat表的POSTROUTING链，而DNAT只能用在nat表的PREROUTING链和OUTPUT链（或被其调用的链）中。

进行DNAT转换后的情况：



配置SNAT和DNAT

□ 生产实战案例

发布内网服务器--配置DNAT实现。

配置示例：

前提条件：

- 局域网的Web服务器能够访问Internet
- 网关的外网IP地址有正确的DNS解析记录
- Linux网关支持IP路由转发

配置步骤：

- 1) 开启路由转发；
- 2) 设置DNAT规则；

```
iptables -t nat -A PREROUTING -i eth0 -d 218.29.30.31 -p  
tcp -dport 80 -j DNAT --to-destination 192.168.1.6
```

- 3) 测试

版权所有，侵权必究

防火墙规则备份恢复

❑ 导出规则

导出即备份规则，使用iptables-save结合输出重定向实现。

```
iptables-save > /opt/iprules_all.txt
```

❑ 导入规则

导入即还原规则，使用iptables-restore工具结合输入重定向实现。

```
iptables-restore < /opt/iprules_all.txt
```

❑ 批量规则

方法1：编写规则导出使用iptables服务

方法2：编写防火墙脚本开机时自动执行脚本

总结

- 防火墙简介
- iptables简介
- iptables工作流程
- iptables表和链
- iptables命令规则
- 主机防火墙配置
- 配置SNAT和DNAT

版权所有，侵权必究



谢谢观看

更多好课，请关注万门大学APP

