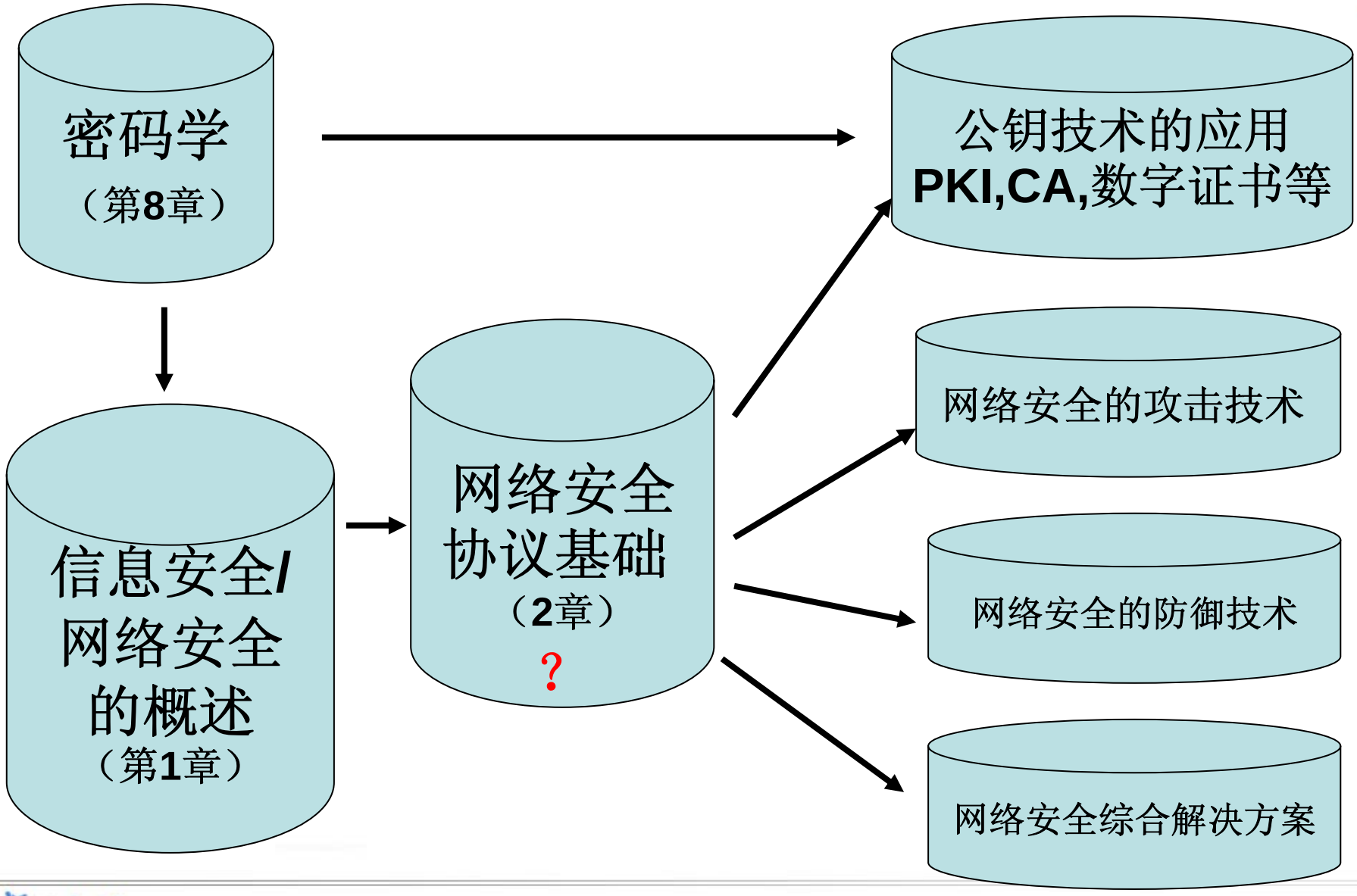
信息安全（）

防火墙

授课计划


密码学
（第8章）
公钥技术的应用
PKI,CA,数字证书等
信息安全/
网络安全
的概述
（第1章）
网络安全
协议基础
（2章）
?
网络安全的攻击技术
网络安全的防御技术
网络安全综合解决方案

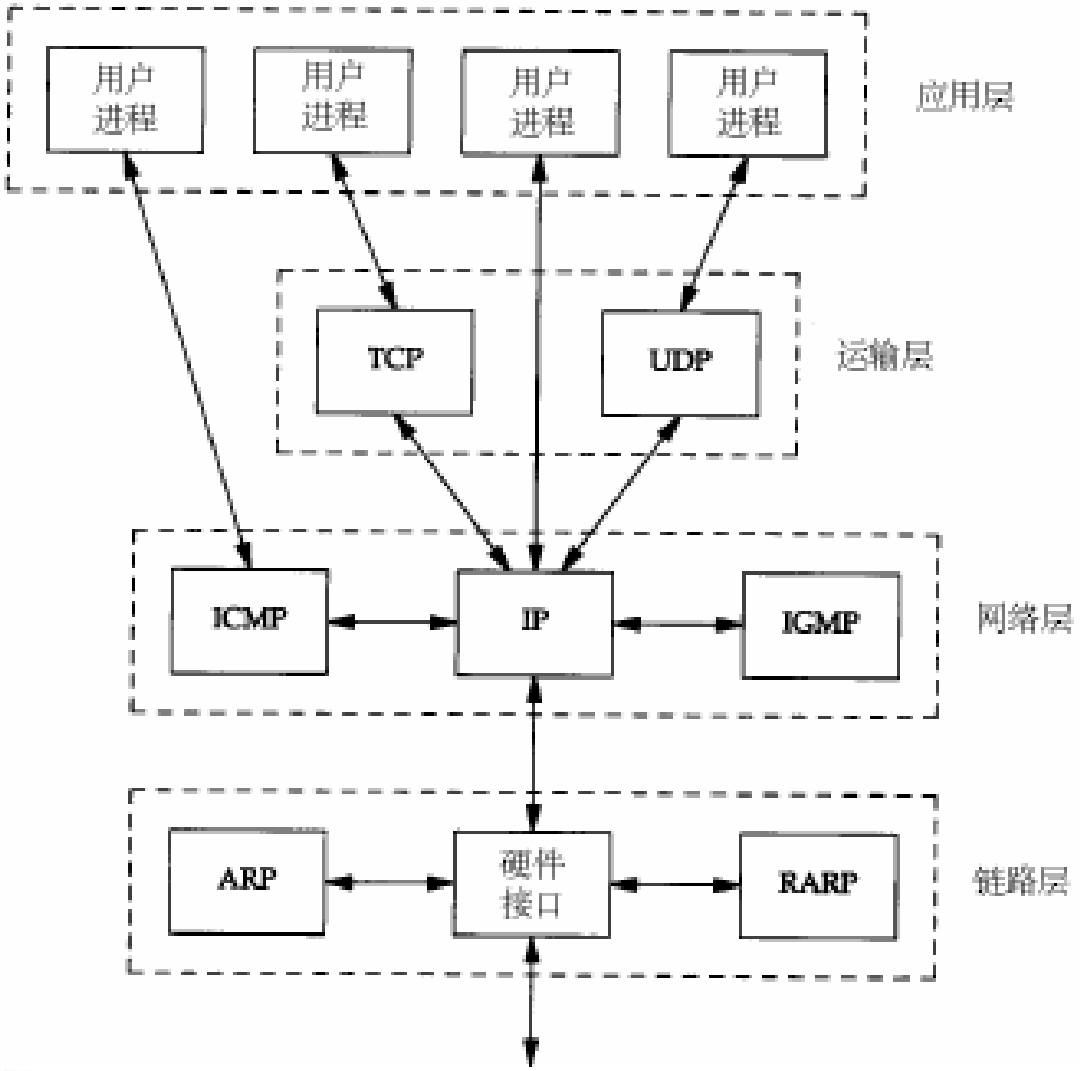
内容

- TCP/IP基础
- 防火墙
  - 防火墙的基本介绍
  - 几种防火墙的类型
  - 防火墙的配置
  - 防火墙技术的发展

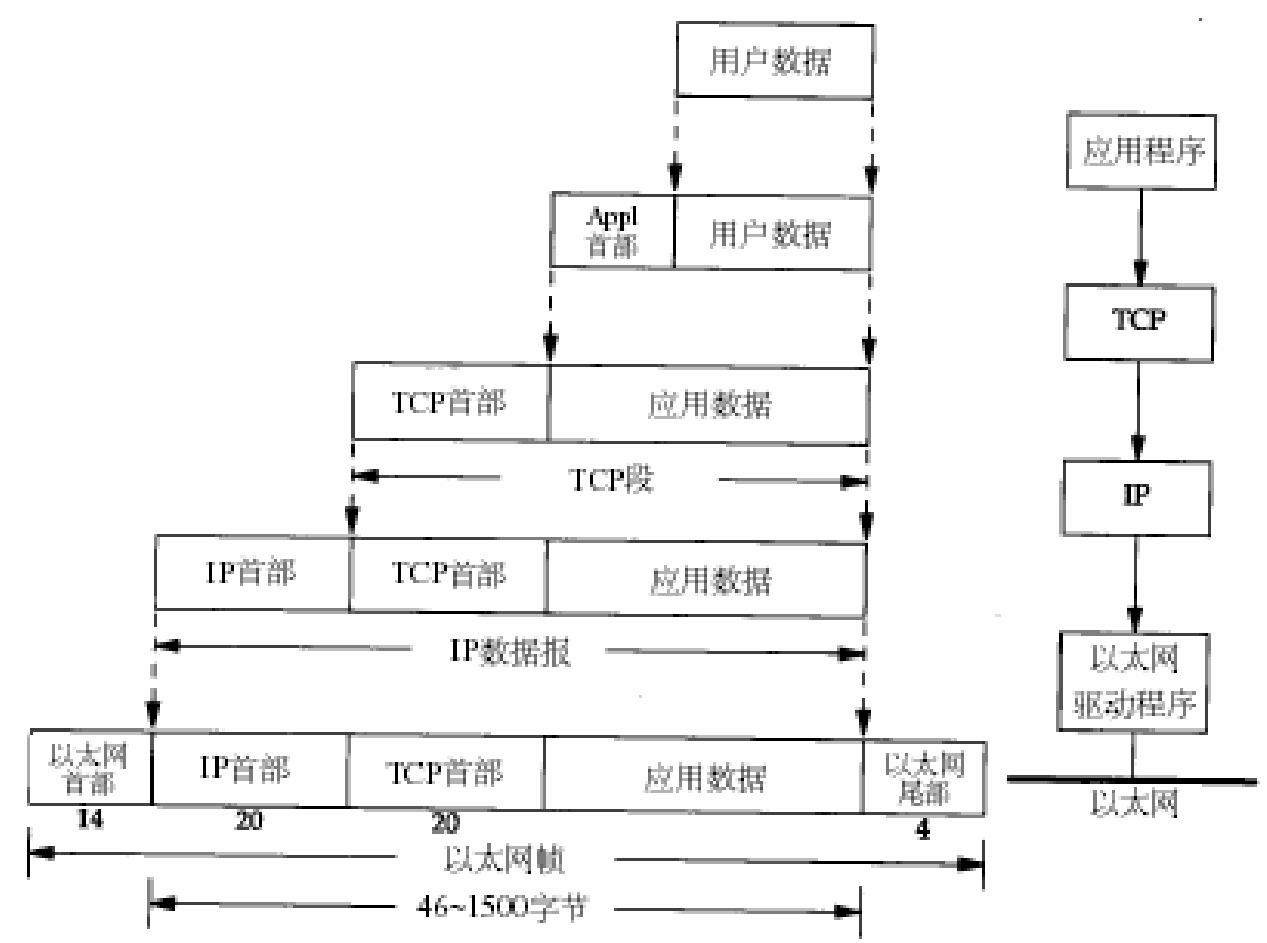
TCP/IP overview

- 协议栈
- 一些数据包的格式
  - IP数据包
  - TCP/UDP数据包
- 常用的上层协议
- 几个常用工具

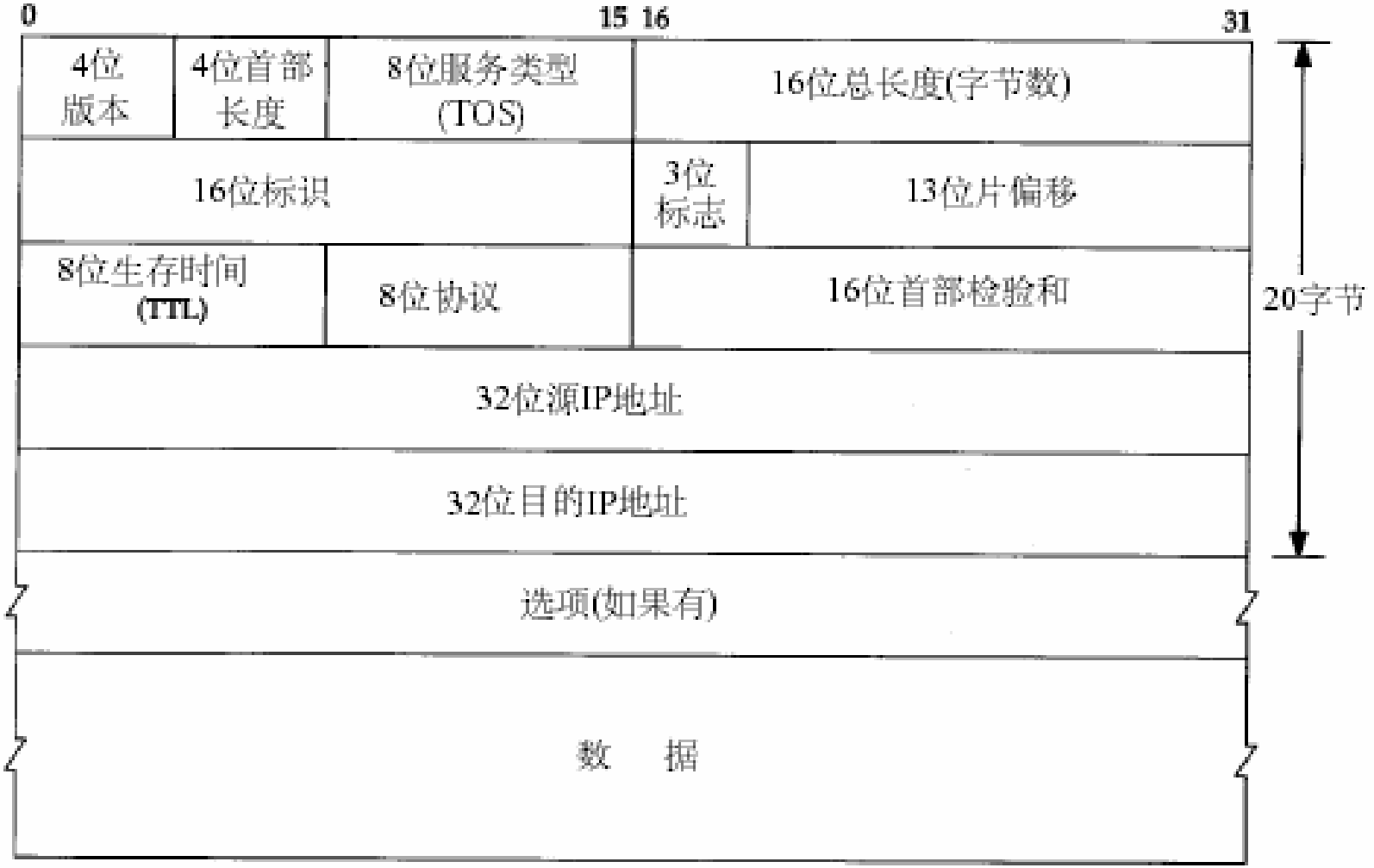
TCP/IP协议栈


用户进程
用户进程
用户进程
用户进程
应用层
TCP
UDP
运输层
ICMP
IP
IGMP
网络层
ARP
硬件接口
RARP
链路层

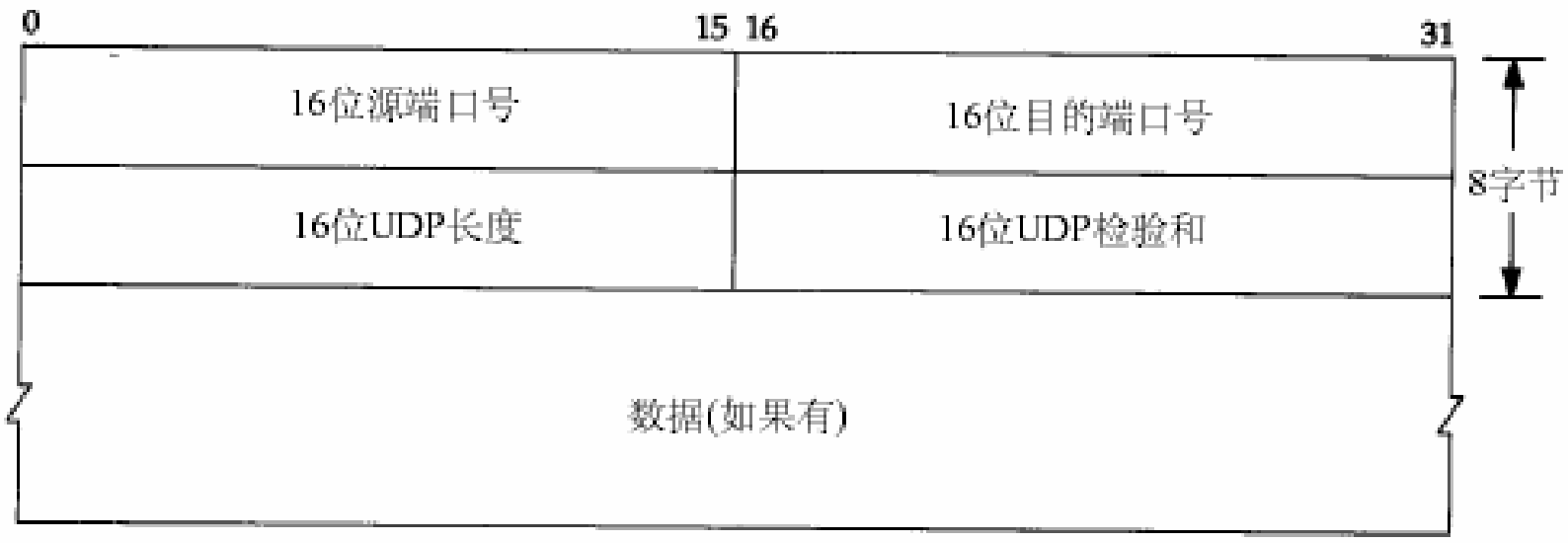
协议栈各层数据包的结构



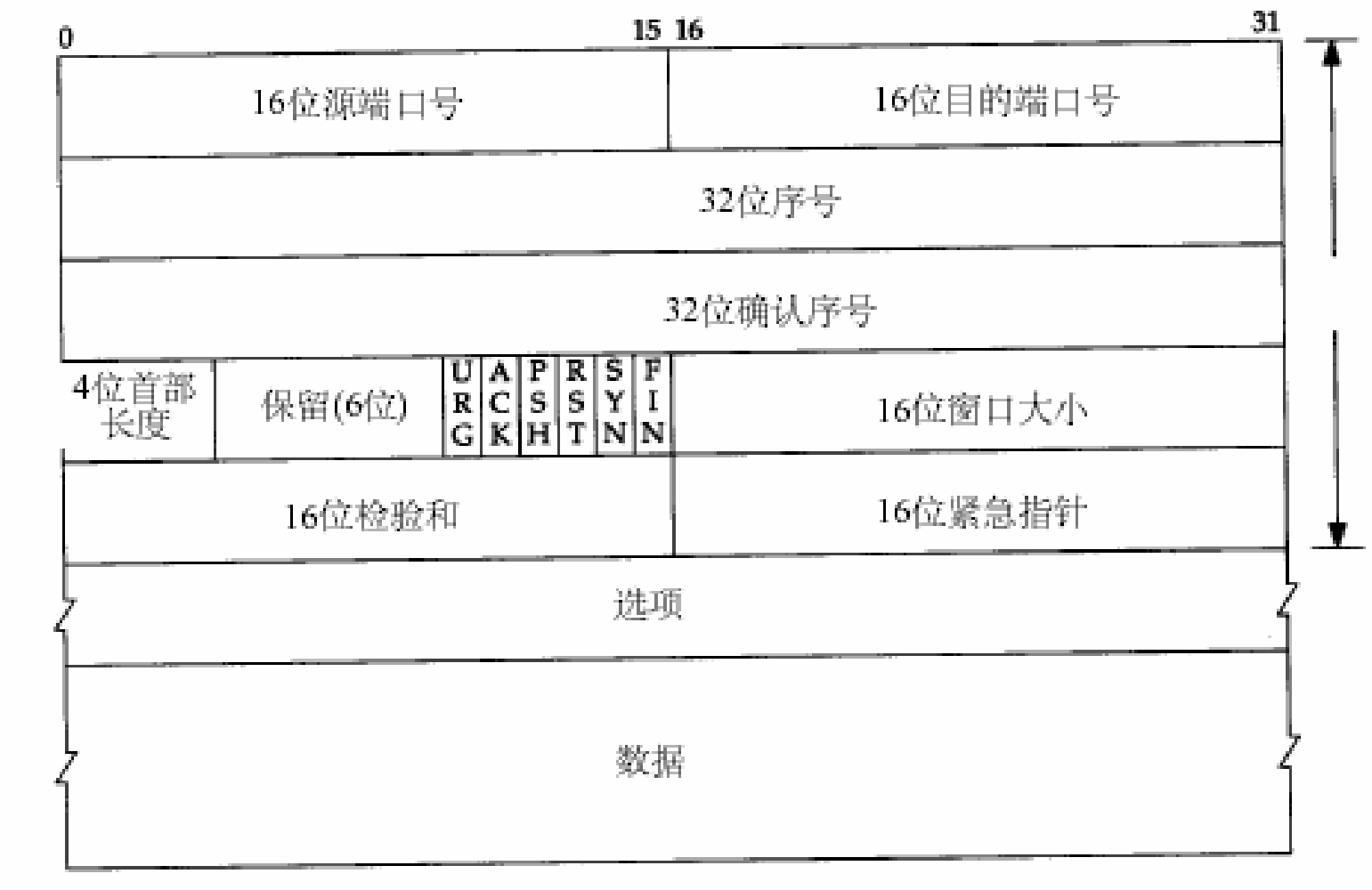
IP数据包格式


0
15 16
31
4位
版本
4位首部
长度
8位服务类型
(TOS)
16位总长度(字节数)
16位标识
3位
标志
13位片偏移
8位生存时间
(TTL)
8位协议
16位首部检验和
20字节
32位源IP地址
32位目的IP地址
选项(如果有)
数　据

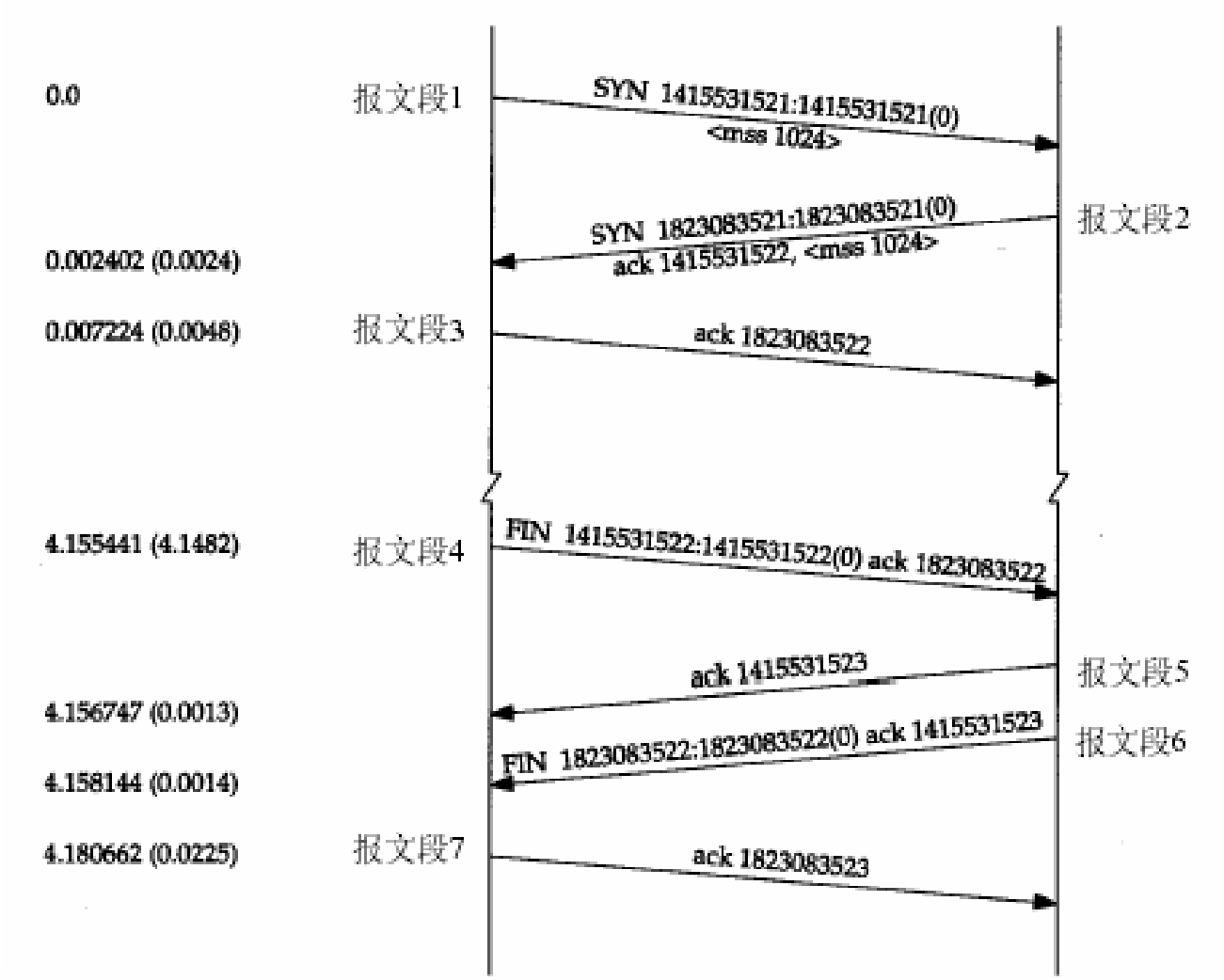
UDP数据包格式



TCP数据包格式


0
15 16
31
16位源端口号
16位目的端口号
32位序号
32位确认序号
4位首部长度
保留(6位)
URG
ACK
PSH
RST
SYN
FIN
16位窗口大小
16位检验和
16位紧急指针
选项
数据

TCP连接的建立和终止时序图



常用的上层协议

- DNS: 53/tcp,udp
- FTP: 20,21/tcp,udp
- telnet: 23/tcp,udp
- HTTP: 80/tcp,udp
- NNTP: 119/tcp,udp
- SMTP: 25/tcp,udp
- POP3: 110/tcp,udp
- 参考：IANA提供的port-numbers.txt

常用的网络工具

- Netstat
- Ipconfig/ifconfig
- Ping
- Tracert
- ……

内容

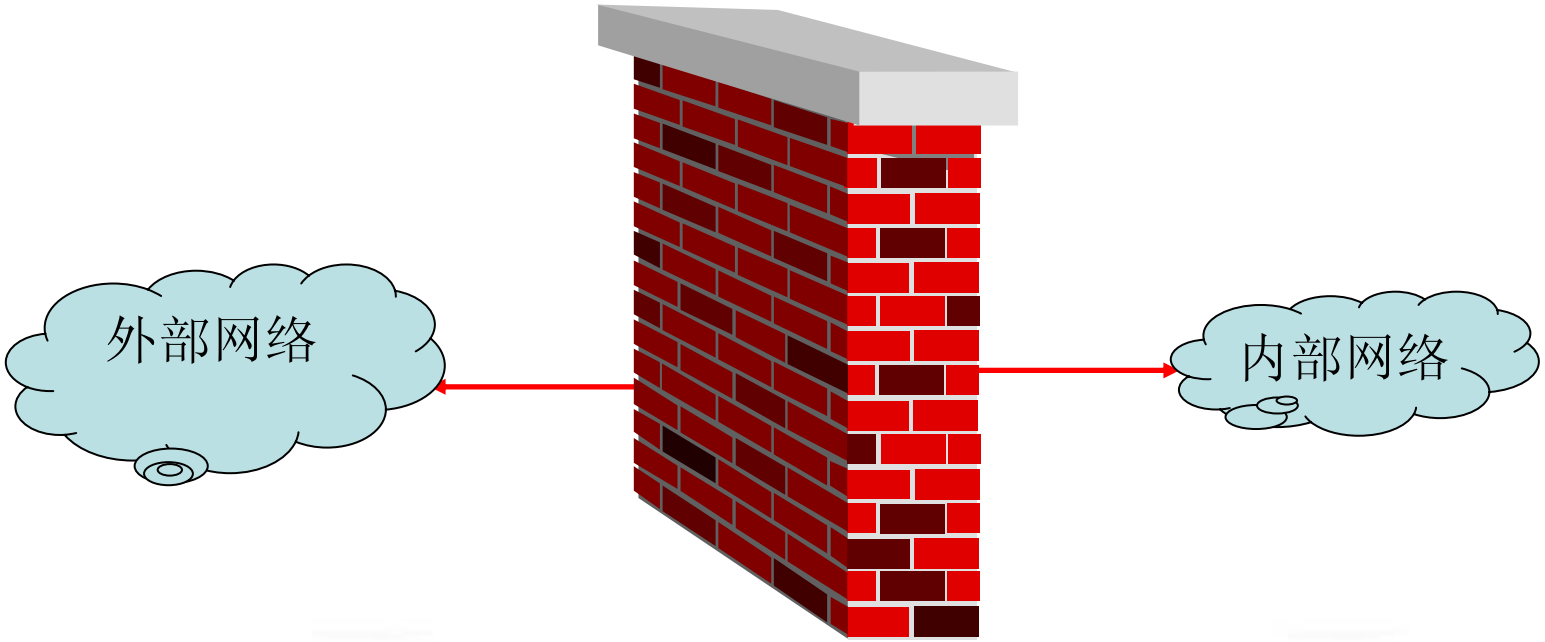
- TCP/IP基础
- 防火墙
  - 防火墙的基本介绍
  - 几种防火墙的类型
  - 防火墙的配置
  - 防火墙技术的发展

防火墙

防火墙：截断燃烧体或难燃烧体的屋顶结构，应高出燃烧体或难燃烧体的屋面不小于500mm

防火墙

- 互联网、内部网和外部网
- Internet ，intranet ，Extranet



互联网、内部网和外部网

- 内部网是应用于组织内部，使用Internet技术的专用网络。
  - 实现信息在组织内部及分支机构间的传播。
- 外部网是内部网的扩展，它将组织的内部网连入其业务伙伴、顾客或供应商的网络
  - 外部网是组织间主要的沟通方式
  - 类型
    - 公共网络
    - 安全（专用）网络
    - 虚拟专用网络（VPN）

防火墙(Firewall)

- 防火墙的基本设计目标
  - 对于一个网络来说，所有通过“内部”和“外部”的网络流量都要经过防火墙
  - 通过一些安全策略，来保证只有经过授权的流量才可以通过防火墙
  - 防火墙本身必须建立在安全操作系统的基础上
- 防火墙的控制能力
  - 服务控制，确定哪些服务可以被访问
  - 方向控制，对于特定的服务，可以确定允许哪个方向能够通过防火墙
  - 用户控制，根据用户来控制对服务的访问
  - 行为控制，控制一个特定的服务的行为

防火墙能为我们做什么

- 定义一个必经之点
  - 挡住未经授权的访问流量
  - 禁止具有脆弱性的服务带来危害
  - 实施保护，以避免各种IP欺骗和路由攻击
- 防火墙提供了一个监视各种安全事件的位置。因此对于有些Internet功能来说，防火墙也可以是一个理想的平台，比如：
  - 地址转换，日志、审计，甚至计费等功能
- 防火墙可以作为IPSec的实现平台

防火墙本身的一些局限性

- 对于绕过防火墙的攻击，它无能为力，例如，在防火墙内部通过拨号出去
- 防火墙不能防止内部的攻击，以及内部人员与外部人员的联合攻击(比如，通过tunnel进入)
- 防火墙不能防止被病毒感染的程序或者文件、邮件等
- 防火墙的性能要求

内容

- TCP/IP基础
- 防火墙
  - 防火墙的基本介绍
  - 几种防火墙的类型
  - 防火墙的配置
  - 防火墙技术的发展

防火墙的类型

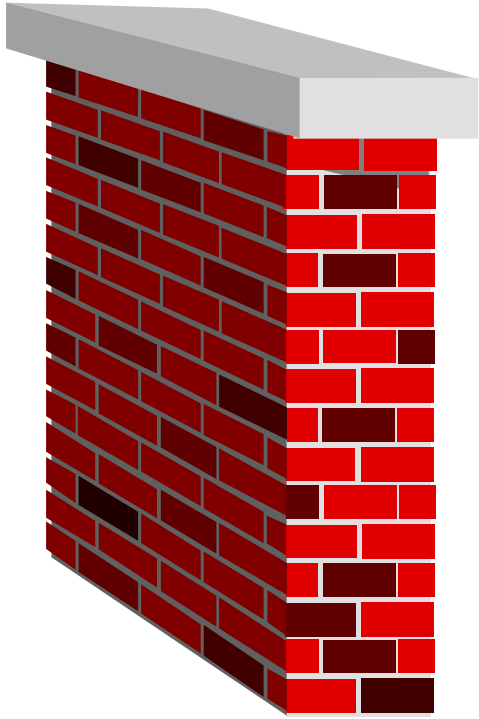
- 包过滤路由器
- 应用层网关

包过滤路由器

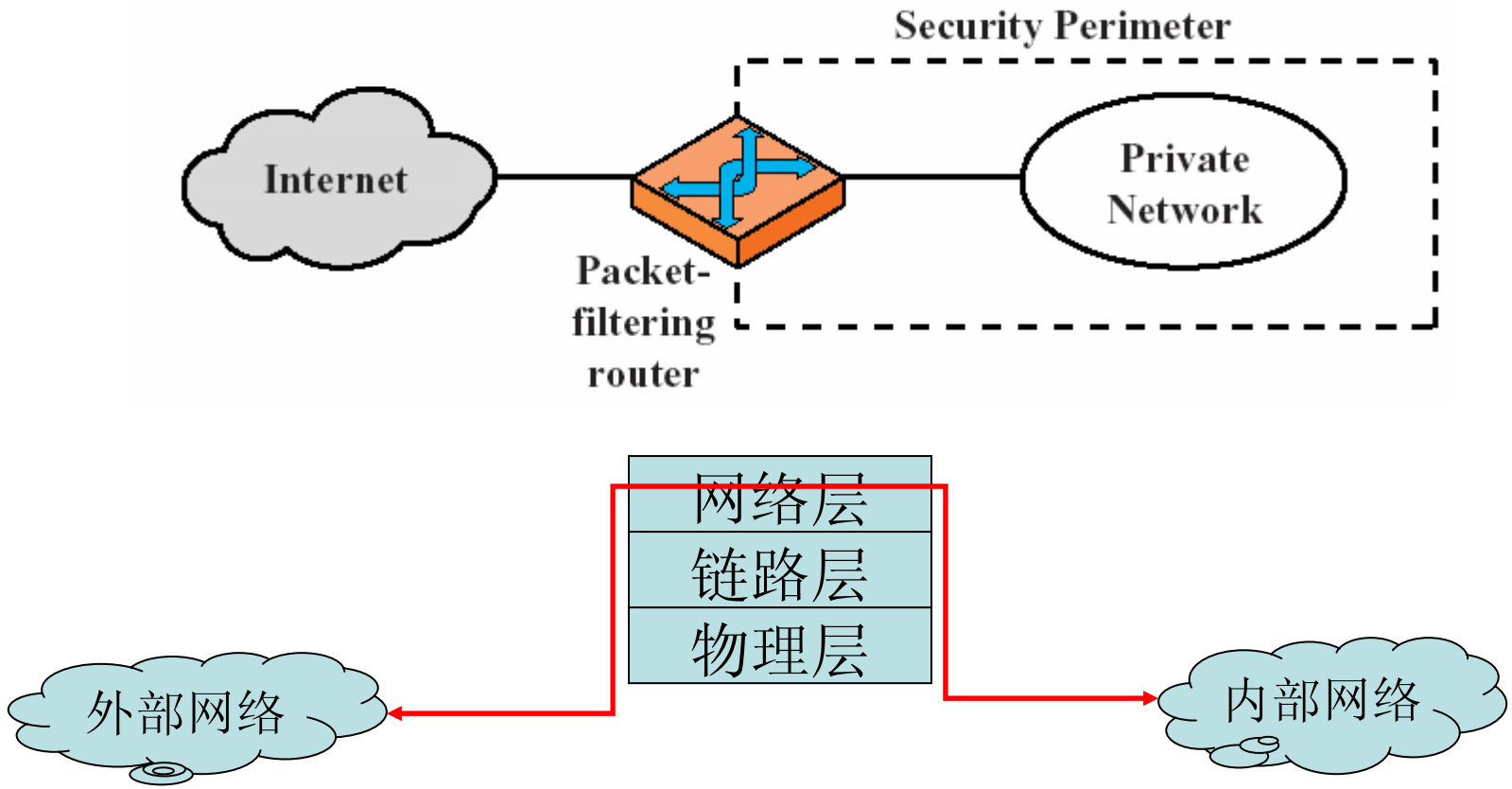
- 基本的思想很简单
  - 对于每个通过的包，匹配一组规则，然后决定转发或者丢弃该包
  - 往往配置成双向的
- 如何过滤
  - 过滤的规则以IP和传输层的头中的域(字段)为基础，
    - 包括源和目标IP地址、IP协议域、源和目标端口、标志位
  - 过滤器往往建立一组规则，根据IP包是否匹配规则中指定的条件来作出决定。
    - 如果匹配到一条规则，则根据此规则决定转发或者丢弃
    - 如果所有规则都不匹配，则根据缺省策略

安全缺省策略

- 两种基本策略，或缺省策略
  - 没有被拒绝的流量都可以通过
    - 管理员必须针对每一种新出现的攻击，制定新的规则
  - 没有被允许的流量都要拒绝
    - 比较保守
    - 根据需要，逐渐开放

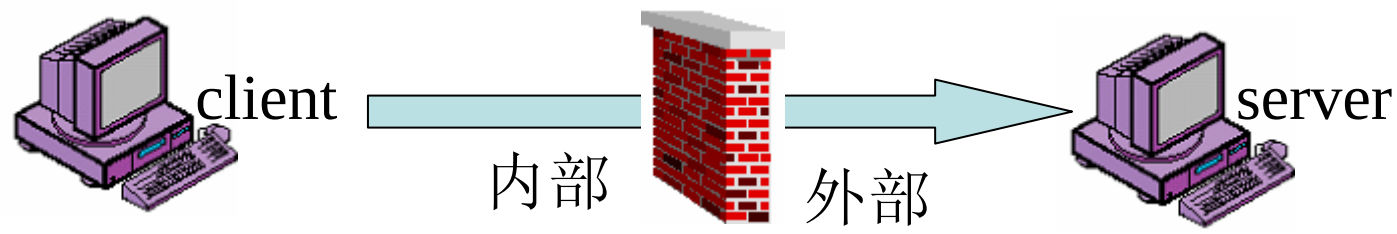


包过滤路由器示意图


Security Perimeter
Internet
Private Network
Packet-filtering router
网络层
链路层
物理层
外部网络
内部网络

例子：包过滤防火墙的设置(1)

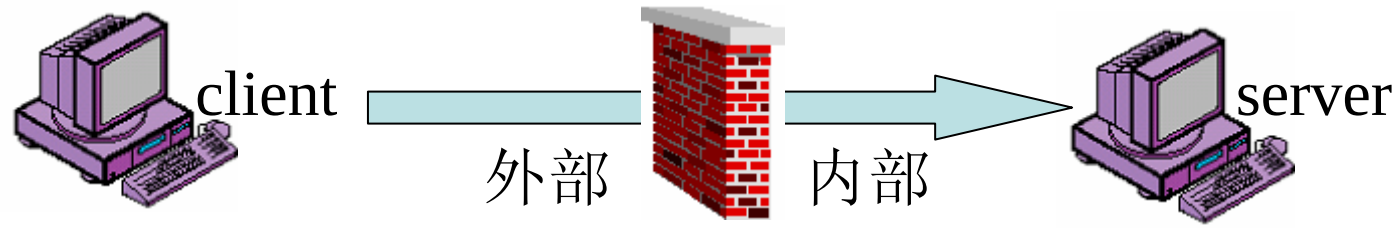
- 从内往外访问telnet服务



- 往外包的特性(用户操作信息)
  - IP源是内部地址
  - 目标地址为server
  - TCP协议，目标端口23
  - 源端口>1023
  - 连接的第一个包ACK=0，其他包ACK=1
- 往内包的特性(显示信息)
  - IP源是server
  - 目标地址为内部地址
  - TCP协议，源端口23
  - 目标端口>1023
  - 所有往内的包都是ACK=1

包过滤防火墙的设置(2)

- 从外往内访问telnet服务



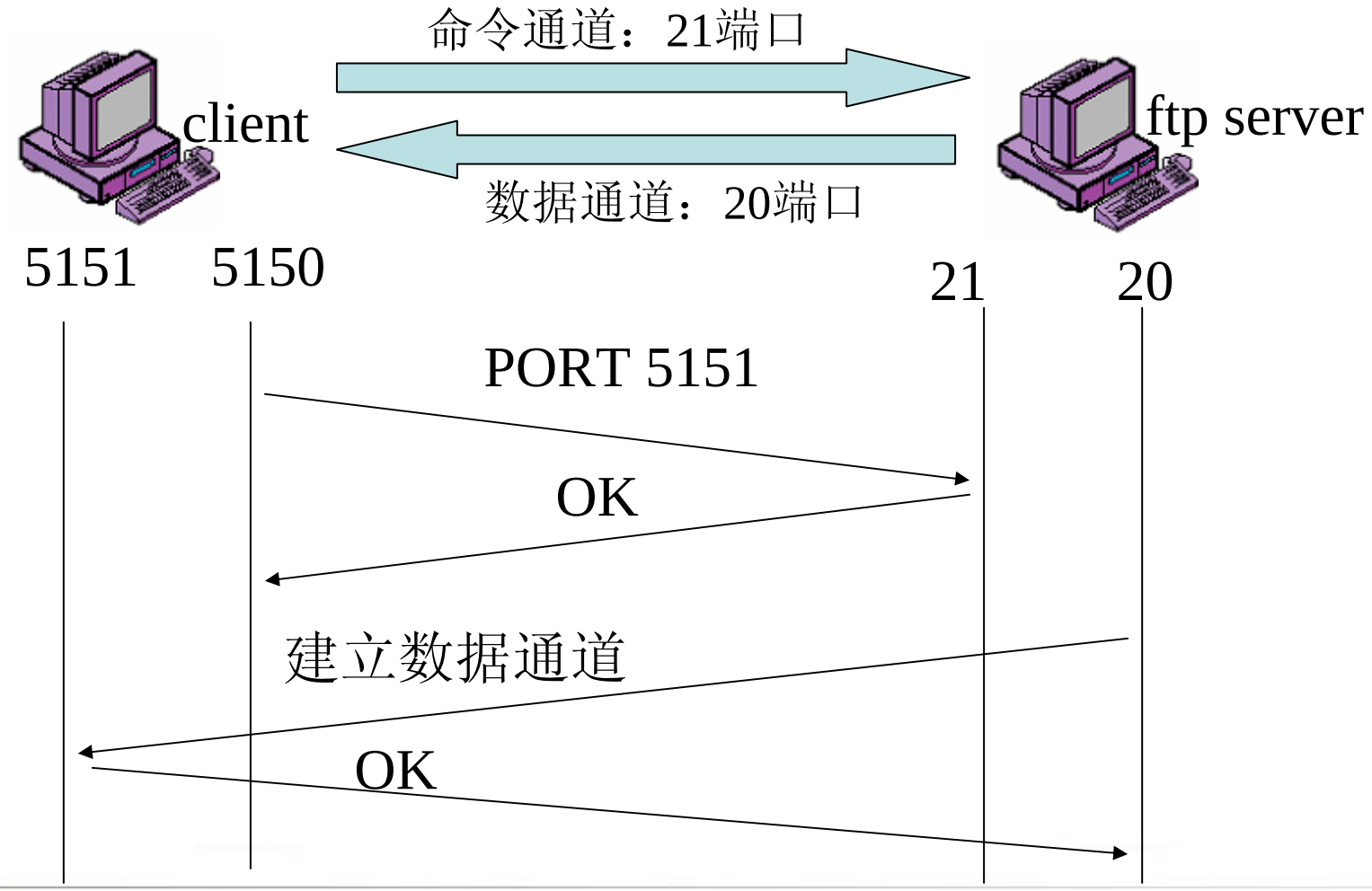
- 往内包的特性(用户操作信息)
  - IP源是外部地址
  - 目标地址为本地server
  - TCP协议，目标端口23
  - 源端口>1023
  - 连接的第一个包ACK=0，其他包ACK=1
- 往外包的特性(显示信息)
  - IP源是本地server
  - 目标地址为外部地址
  - TCP协议，源端口23
  - 目标端口>1023
  - 所有往内的包都是ACK=1

针对telnet服务的防火墙规则

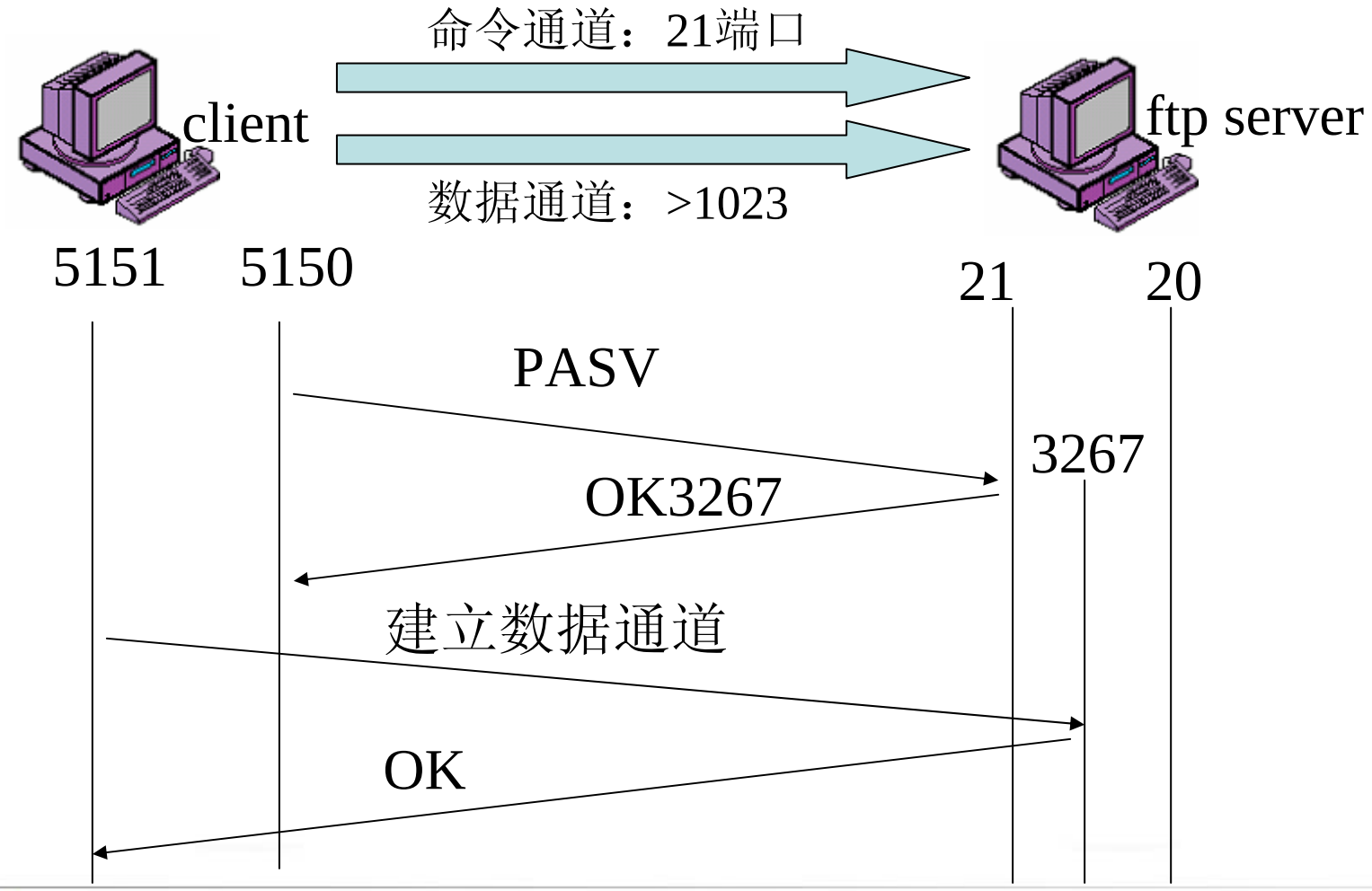
服务方向	包方向	源地址	目标地址	包类型	源端口	目标端口	ACK
往外	外	内部	外部	TCP	>1023	23	*
往外	内	外部	内部	TCP	23	>1023	1
往内	外	外部	内部	TCP	>1023	23	*
往内	内	内部	外部	TCP	23	>1023	1

*: 第一个ACK=0, 其他=1

Ftp文件传输协议


命令通道：21端口
client
ftp server
数据通道：20端口
5151
5150
21
20
PORT 5151
OK
建立数据通道
OK

Ftp文件传输协议(续)


命令通道：21端口
client
ftp server
数据通道：>1023
5151
5150
21
20
PASV
3267
OK3267
建立数据通道
OK

- 建立一组复杂的规则集
  - 是否允许正常模式的ftp数据通道？
  - 有些ftp client不支持pasv模式
- 动态监视ftp通道发出的port命令
  - 有一些动态包过滤防火墙可以做到
    - 动态包过滤（动态地在过滤规则中增加或更新条目）
- 启示
  - 包过滤防火墙比较适合于单连接的服务(比如smtp, pop3)，不适合于多连接的服务(比如ftp)

针对包过滤防火墙的攻击

- IP地址欺骗，例如，假冒内部的IP地址
  - 对策：在外部接口上禁止内部地址
- 源路由攻击，即由源指定路由
  - 对策：禁止这样的选项
- 小碎片攻击，利用IP分片功能把TCP头部切分到不同的分片中
  - 对策：丢弃分片太小的分片
- 利用复杂协议和管理员的配置失误进入防火墙
  - 例如，利用ftp协议对内部进行探查
    - TCP FTPPROXY扫描

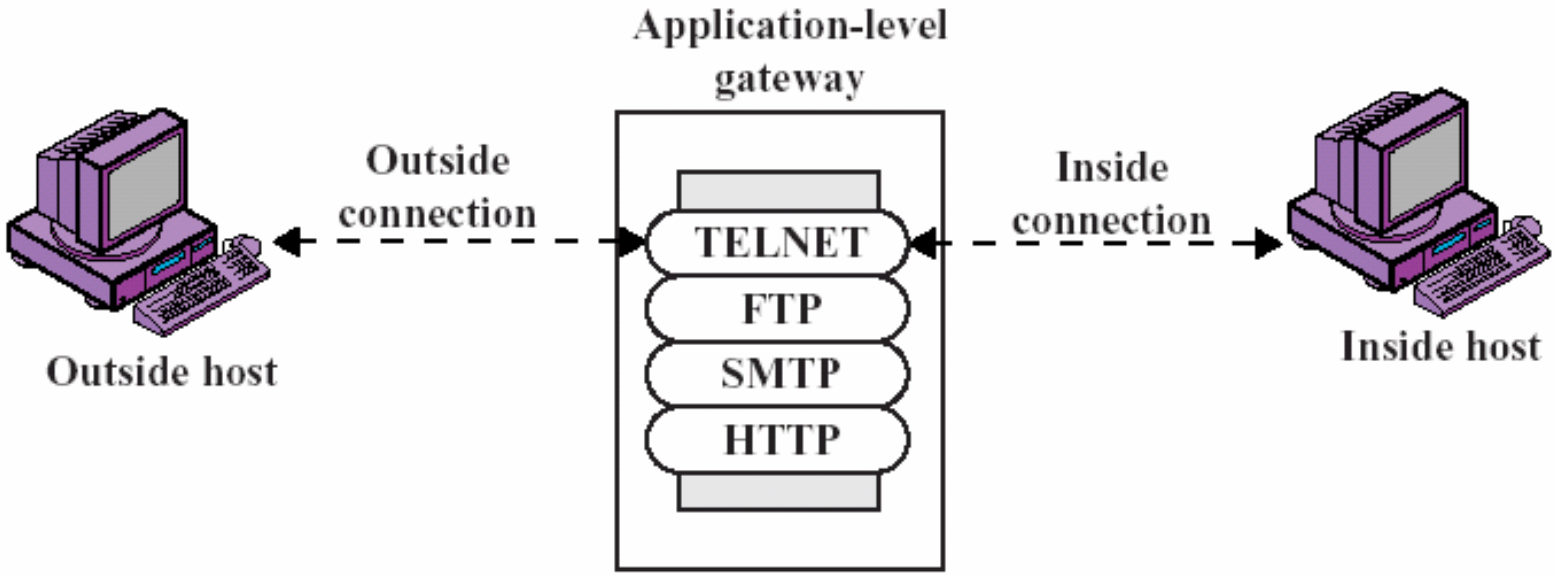
包过滤防火墙

- 在网络层上进行监测
  - 并没有考虑连接状态信息
- 通常在路由器上实现
  - 实际上是一种网络的访问控制机制
- 优点：
  - 实现简单
  - 对用户透明
  - 效率高
- 缺点：
  - 正确制定规则并不容易
  - 不可能引入认证机制

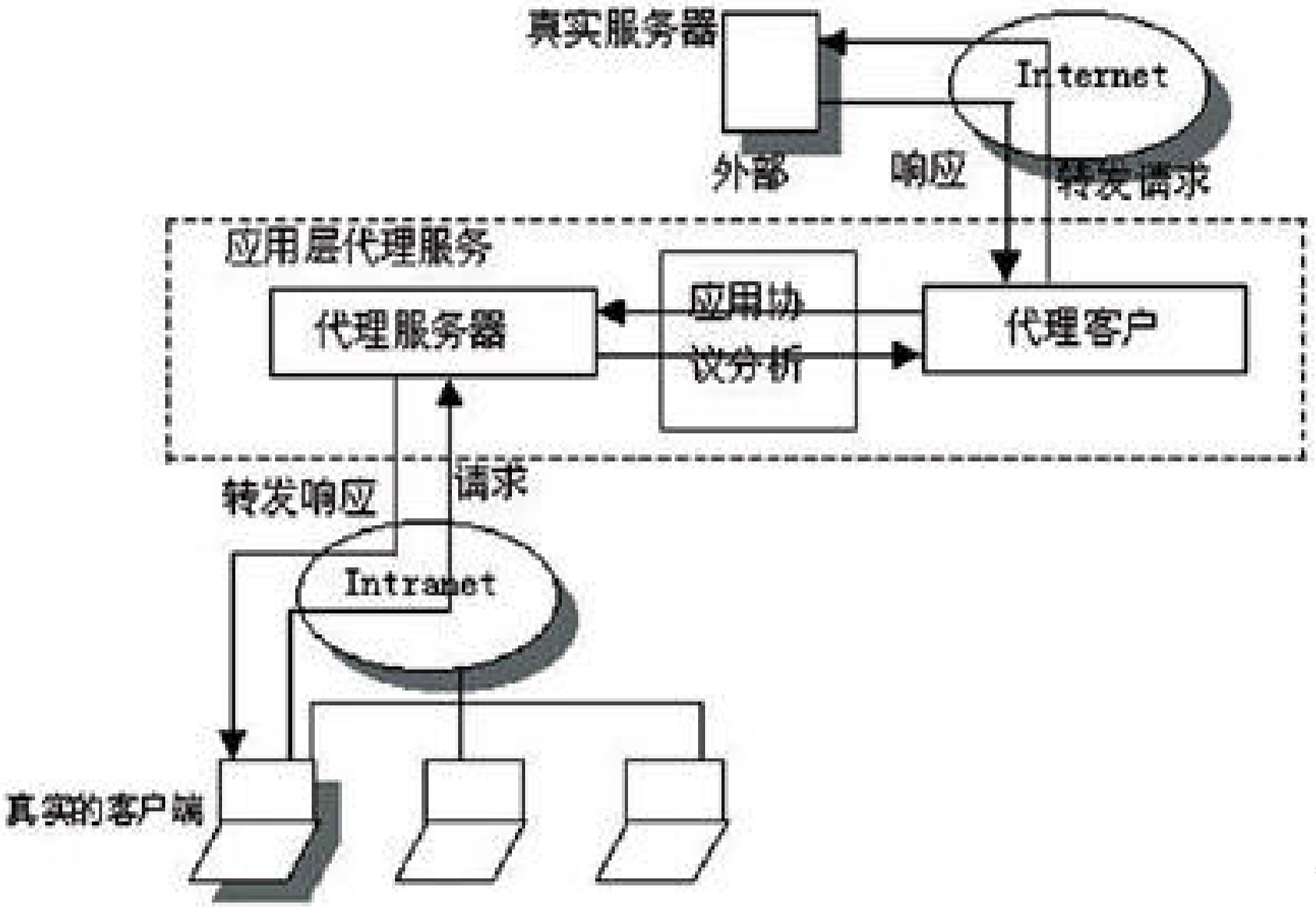
应用层网关

- 也称为代理服务器
- 特点
  - 所有的连接都通过防火墙，防火墙作为网关
  - 在应用层上实现
  - 可以监视包的内容
  - 可以实现基于用户的认证
  - 所有的应用需要单独实现
  - 可以提供理想的日志功能
  - 非常安全，但是开销比较大

应用层网关的结构示意图



应用层网关结构示意图


真实服务器
Internet
外部
响应
转发请求
应用层代理服务
代理服务器
应用协
议分析
代理客户
转发响应
请求
Intranet
真实的客户端

应用层网关的优缺点

- 优点
  - 允许用户“直接”访问Internet
  - 易于记录日志
- 缺点
  - 新的服务不能及时地被代理
  - 每个被代理的服务都要求专门的代理软件
  - 客户软件需要修改，重新编译或者配置
  - 有些服务要求建立直接连接，无法使用代理
  - 代理服务不能避免协议本身的缺陷或者限制

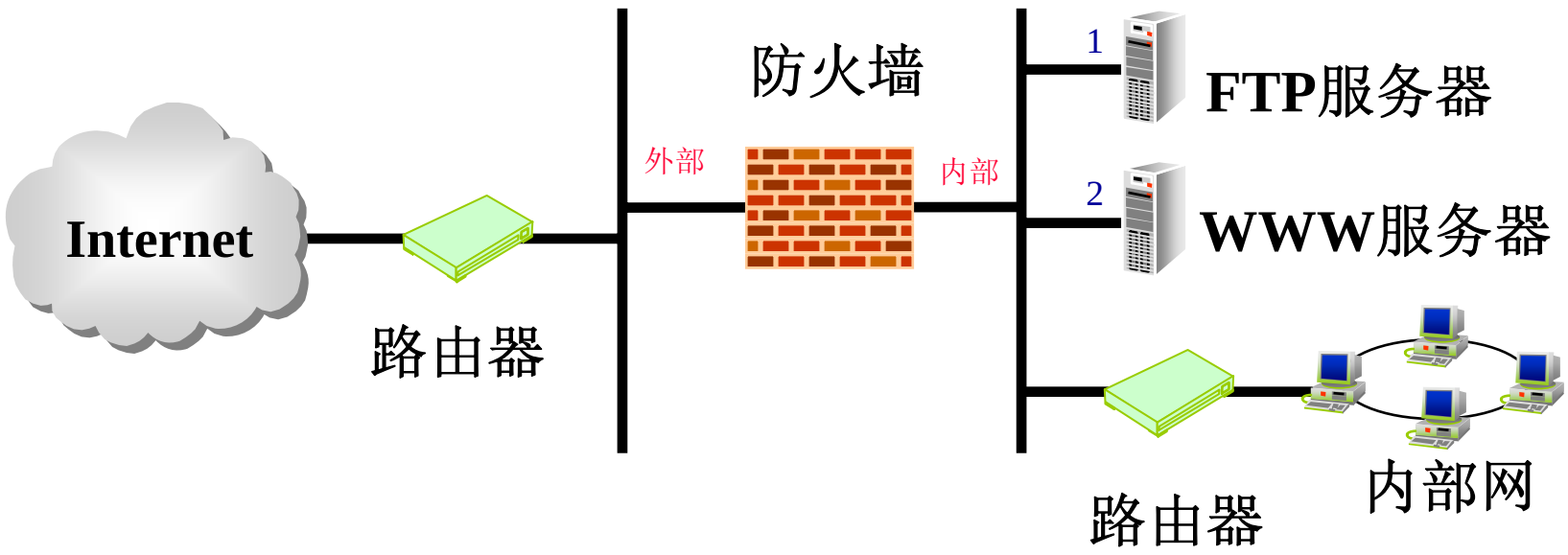
应用层网关实现

- 编写代理软件
  - 代理软件一方面是服务器软件
    - 但是它所提供的服务可以是简单的转发功能
  - 另一方面也是客户软件
    - 对于外面真正的服务器来说，是客户软件
  - 针对每一个服务都需要编写模块或者单独的程序
  - 实现一个标准的框架，以容纳各种不同类型的服务
    - 软件实现的可扩展性和可重用性
- 客户软件
  - 软件需要定制或者改写
  - 对于最终用户的透明性？
- 协议对于应用层网关的处理
  - 协议设计时考虑到中间代理的存在，特别是在考虑安全性，比如数据完整性的时候

内容

- TCP/IP基础
- 防火墙
  - 防火墙的基本介绍
  - 几种防火墙的类型
  - 防火墙的配置
  - 防火墙技术的发展

问题：现实环境下防火墙配置？



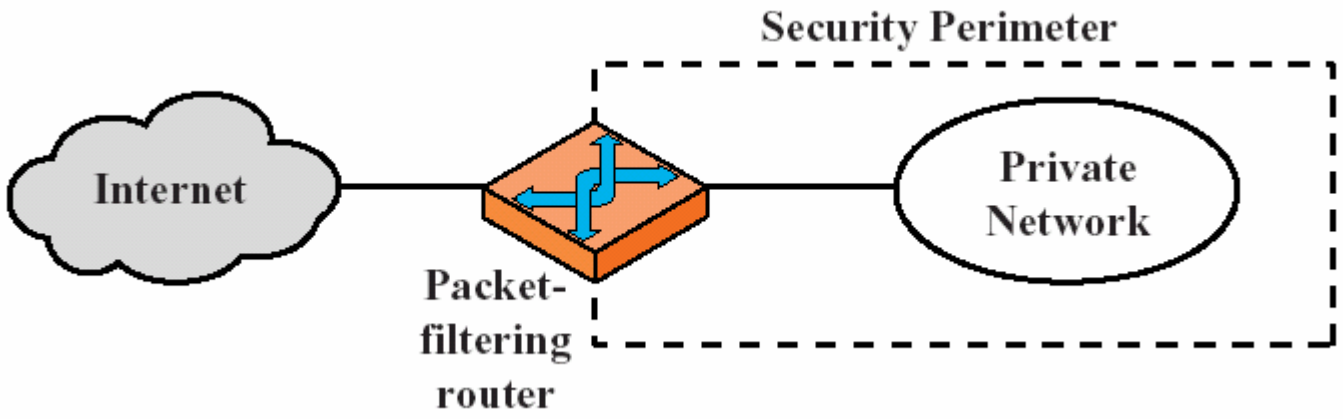
防火墙的配置

- 几个概念
  - 堡垒主机(Bastion Host)：对外部网络暴露，同时也是内部网络用户的主要连接点
  - 双宿主主机(dual-homed host)：至少有两个网络接口的通用计算机系统
  - DMZ(Demilitarized Zone，非军事区或者停火区)：在内部网络和外部网络之间增加的一个子网

防火墙几种典型配置方案

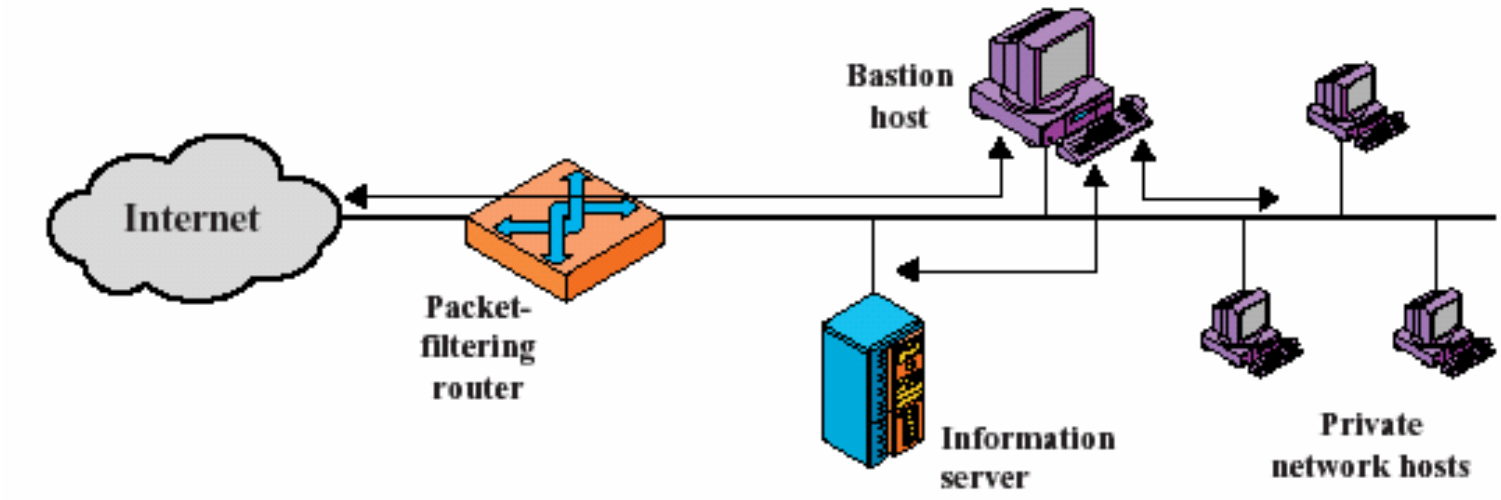
- 包过滤
- 屏蔽主机方案
  - 单宿主堡垒主机
  - 双宿主堡垒主机
- 屏蔽子网方案

配置方案一



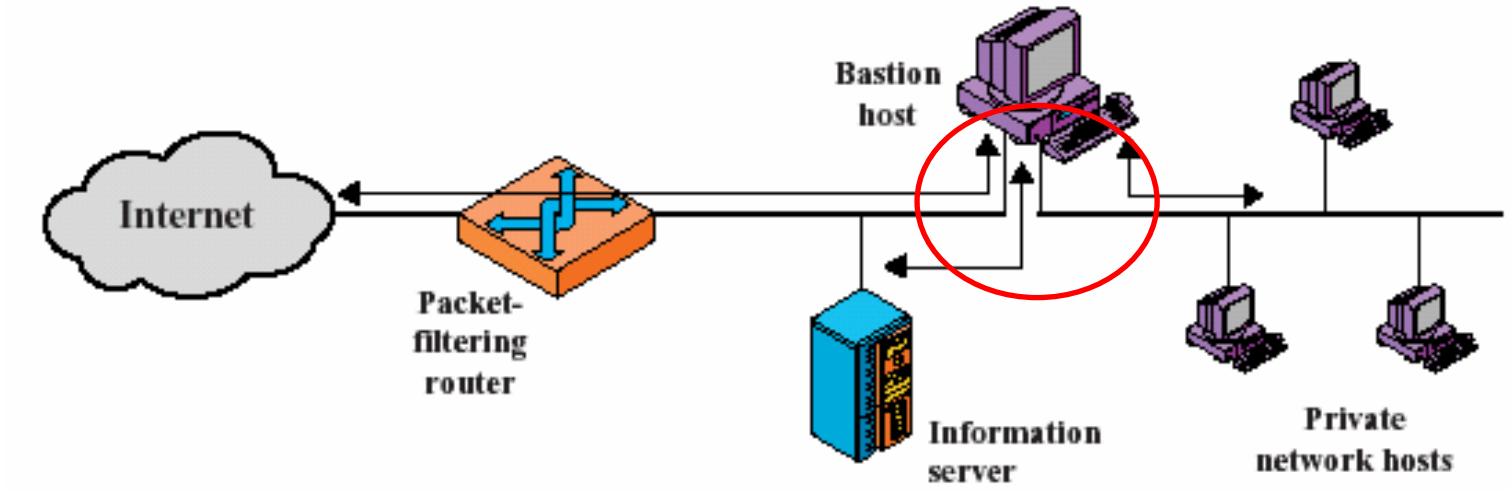
- 包过滤方案
- 所有的流量都通过堡垒（包过滤路由器）
- 优点：简单

配置方案二



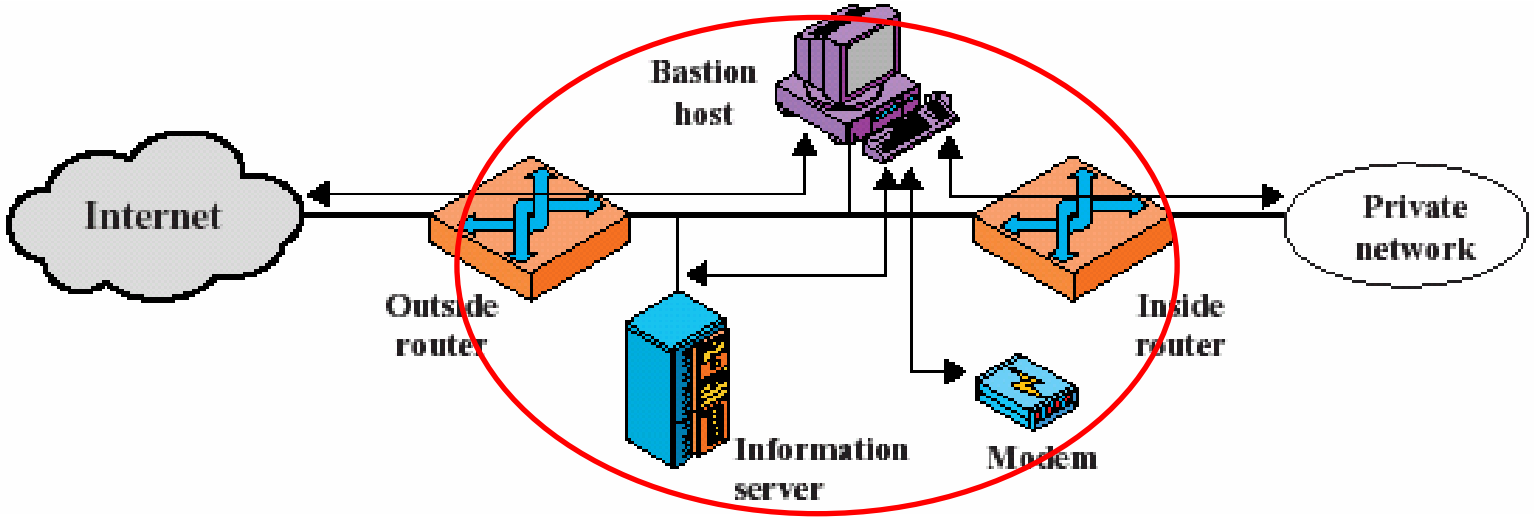
- 屏蔽主机方案：单宿主堡垒主机
- 只允许堡垒主机可以与外界直接通讯
- 优点：两层保护：包过滤+应用层网关；灵活配置
- 缺点：一旦包过滤路由器被攻破，则内部网络被暴露

配置方案三



- 屏蔽主机方案：双宿主堡垒主机
- 从物理上把内部网络和Internet隔开，必须通过两层屏障
- 优点：两层保护：包过滤+应用层网关；配置灵活

配置方案四



- 屏蔽子网防火墙
- 优点：
  - 三层防护，用来阻止入侵者
  - 外面的router只向Internet暴露屏蔽子网中的主机
  - 内部的router只向内部私有网暴露屏蔽子网中的主机

防火墙的发展

- 分布式防火墙
- 应用层网关的进一步发展
  - 认证机制
  - 智能代理
- 与其他技术的集成
  - 比如NAT、VPN(IPSec)、IDS，以及一些认证和访问控制技术
  - 防火墙自身的安全性和稳定性