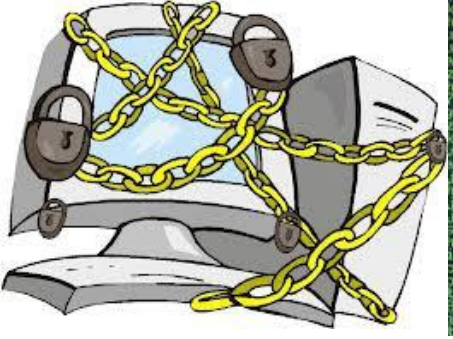


信息系统安全

网络安全

防火墙与入侵容忍系统

陈春华 博士
chunhuachen@scut.edu.cn

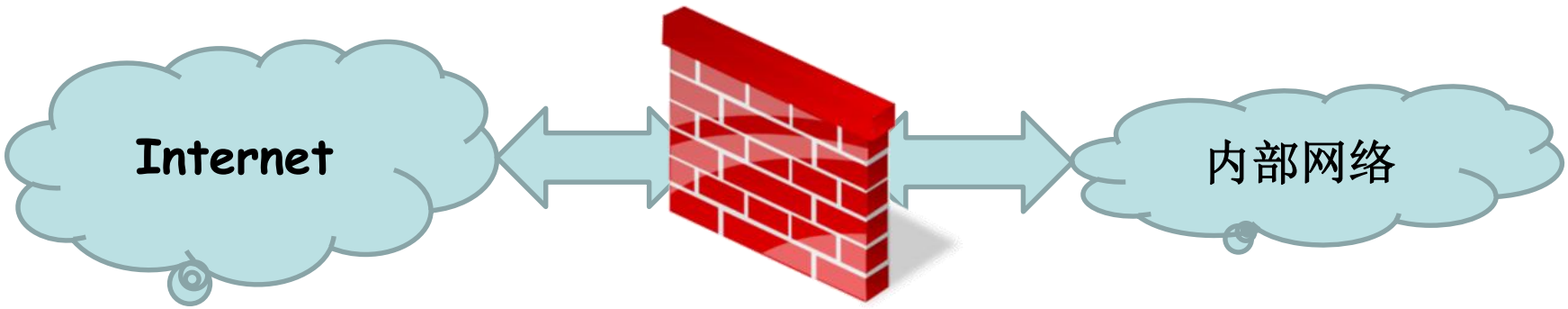
2018 春季
华南理工大学 软件学院

数据保护-可用性

- 保证数据能够被正常地使用
  - 数据有信息系统存储与处理，因此必须保证信息系统功能的可用性；
  - 从可用性方面，还需要考虑数据备份，容错和容灾等方面
- 保护信息系统功能：访问控制
  - 主机访问控制，通常有操作系统来实现
  - 网络访问控制，网络防火墙，入侵检测系统等
- 入侵检测系统可视为主动的信息系统保护机制

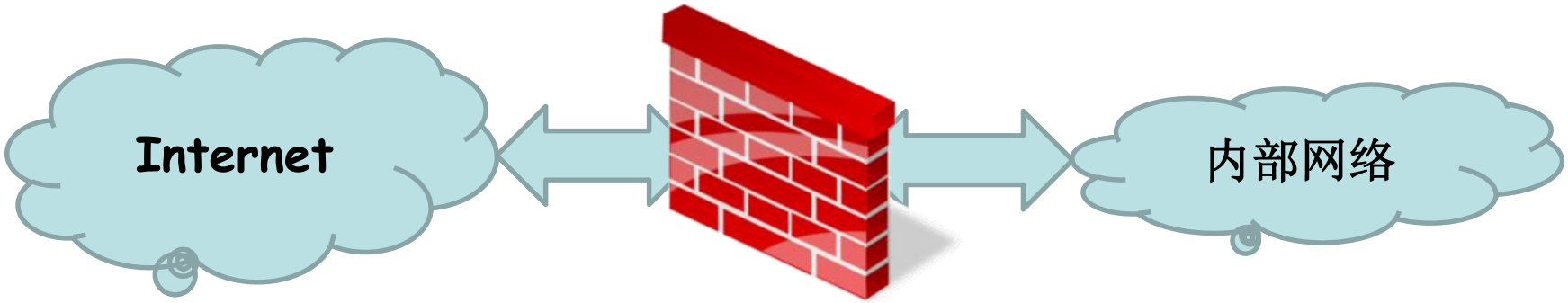
网络防火墙

- 在计算机网络中，防火墙是设置在可信任的内部网络与不可信任的外界之间的一道屏障，阻止不希望或者未授权的通信进出内部网络，通过强化边界控制来保障内部的安全，同时不妨碍正常访问行为。



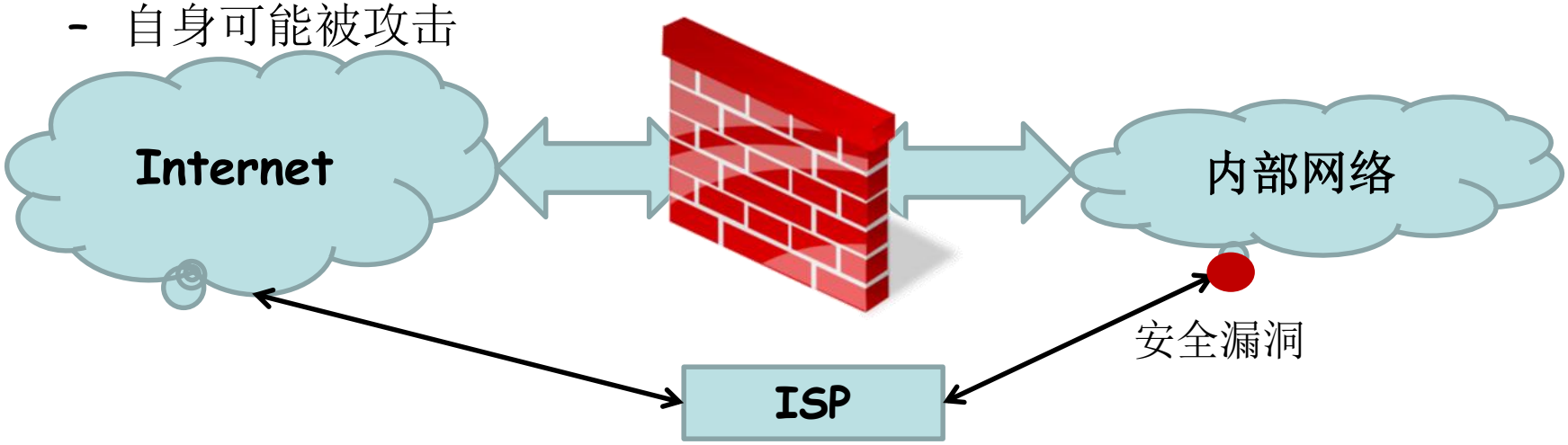
网络防火墙

- 防火墙的作用
  - 强化网络安全策略：过滤数据报，拒绝未经允许的访问
  - 防止故障蔓延：对网络进行隔离划分，防止安全问题对全局造成影响
  - 对网络访问进行监控审计和报警
  - 其他，比如流量控制等



网络防火墙

- 防火墙的局限
  - 防火墙可能被绕过：为了发挥防火墙的作用，**出入的信息必须都经过防火墙，仅允许合法信息通过**。
  - 对内部出卖性攻击或者内部误操作无效
  - 不能防止数据驱动攻击的攻击
  - 可以阻断攻击，但是无法消灭攻击源
  - 自身可能被攻击



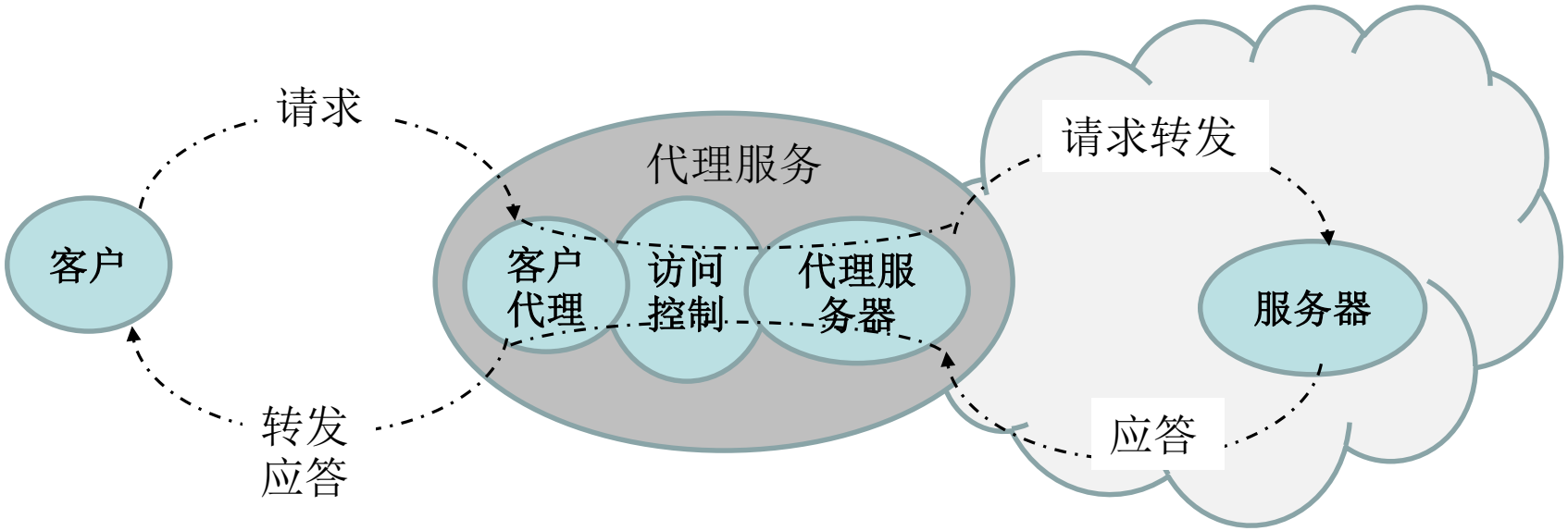
网络防火墙的基本技术

- 网络地址转换
  - 即Network Address Translation/NAT
  - 使用内部和外部两套IP地址，隐藏内部网络拓扑，使得外部主机无法直接发起与内部主机的连接
- 代理服务
- 包过滤
- 状态检测

防火墙技术：代理服务

- 代理服务器是用户计算机与Internet之间的中间代理机制，它采用客户/服务器工作模式。
- 即建立一个数据包的中转机制，并在数据的中转过程中加入一些安全机制-访问
- 代理技术主要实现在
  - 应用层，又称应用级代理
    - 针对每种应用独立开发与部署，如HTTP代理
  - 传输层，又称电路级代理
    - 对应用层透明

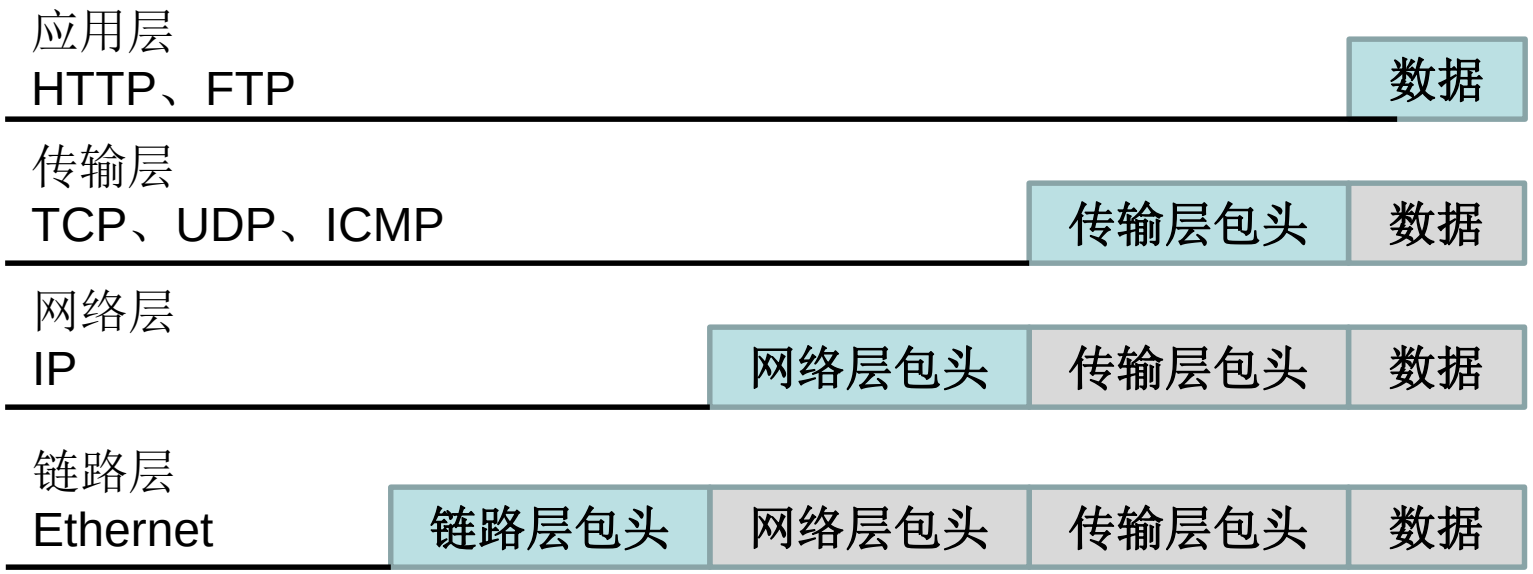
防火墙技术：代理服务



图：代理服务的结构及其数据控制和传输过程

防火墙技术：包过滤

- 网络数据包：



- 包过滤就是根据数据包的特征进行的，主要是根据数据包头的一些字段的特征进行过滤

防火墙：包过滤

- 数据包的主要特征
  - 源地址、目的地址
  - 源端口、目的端口
  - 协议：IP, TCP, UDP, ICMP等
  - 数据包内容中（某些关键字，即特征）
    - 病毒特征码等

防火墙：包过滤

- 包过滤安全策略的制定
  - 一条过滤规则规定了允许数据包流进或者流入内部网络的一个条件
  - 最小特权原则
  - 除明确禁止和允许的规则外，对没有明确规则的情况，可采取两种策略
    - 默认接受：凡未被禁止，即允许
    - 默认拒绝：凡未被允许，即禁止
  - 过滤效果与规则排列顺序有关
- 两种策略：基于地址和服务(端口)的包过滤

基于地址的数据包过滤策略

- 例子：某公司有一个B类网(123.45)。该网的子网(123.45.6.0/24)有若干合作网络(135.79)。管理员希望
  - 禁止一切来自Internet的对内网的访问
  - 允许来自合作网络的所有子网(135.79.0.0/16)访问内网(123.45.6.0/24)
  - 禁止对合作网络的子网(135.79.99.0/24)的访问权

规则	源地址	目的地址	过滤操作
A	135.79.0.0/16	123.45.6.0/24	允许
B	123.45.6.0/24	135.79.0.0/16	允许
C	123.45.0.0/16	135.79.99.0/24	拒绝
D	0.0.0.0/0	0.0.0.0/0	拒绝

防火墙技术：状态检测

- 又称为动态包过滤防火墙
- 在数据包的检测方面，对网络的各个层进行实时检测，跟踪每一个有效连接的状态，并根据这些信息决定对该连接是接受还是拒绝
- 静态数据包过滤，又称无状态数据包过滤：仅单独分析每一个数据包，不考虑包内高层的信息以及不同包之间的逻辑关系，也不关心数据传输的状态

防火墙技术：状态检测

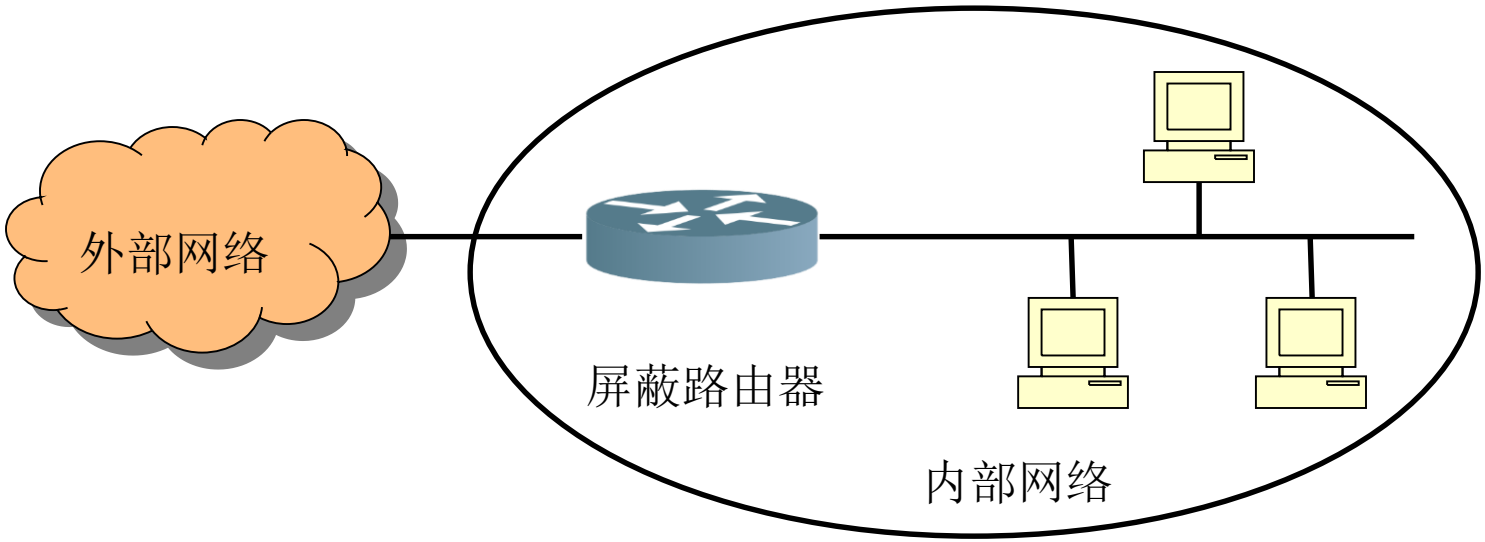
- 其检测引擎监视跟踪每一个有效连接的状态，动态地维护一个状态信息表，通过规则表与状态表的共同配合，对表中的各个连接状态因素加以识别。
- TCP包状态表
  - 是否为握手数据包，内部主机是否期待该握手包
  - 是否为数据传输报，状态表中是否存在相应的TCP连接

防火墙技术：状态检测

- 更好的扩展性
  - 在应用层之下工作，不需要为每一个应用开发与部署代理服务器程序
- 配置方便，应用范围广
  - 更好地支持基于面向无连接协议（UDP等）的应用
- 缺点：不能分析检测应用层数据（病毒，垃圾邮件等）

防火墙部署

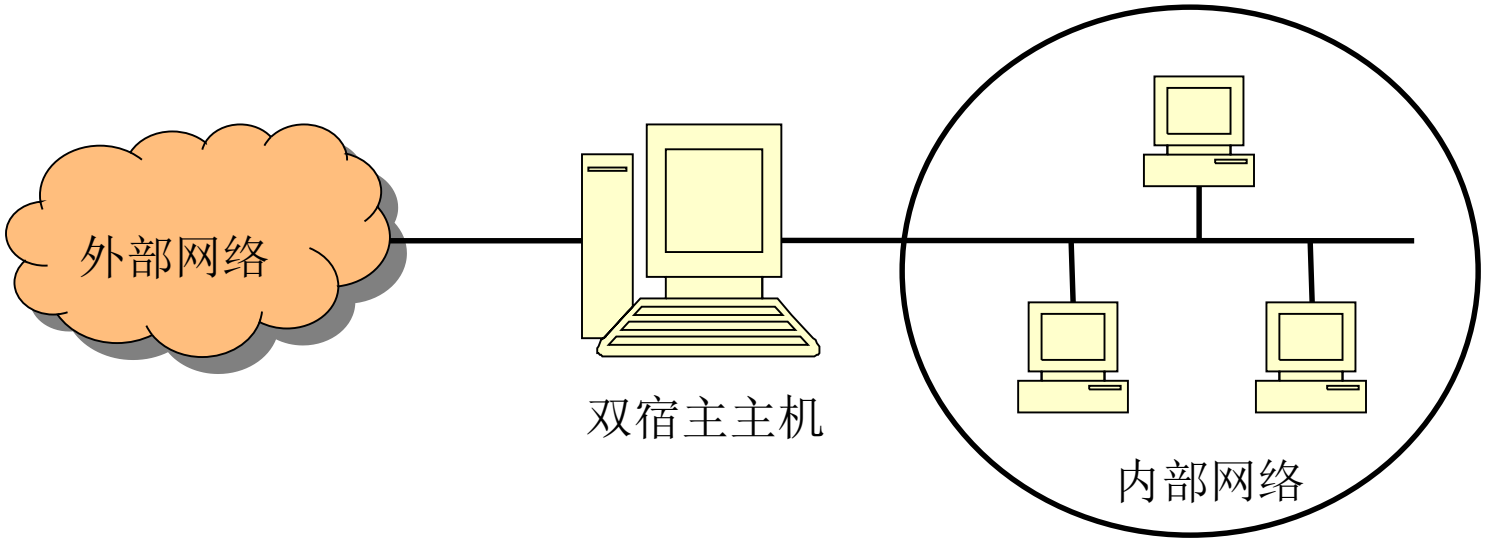
- 屏蔽路由器和屏蔽主机 (Screening Router&Host)
  - 在路由器/主机中配置数据包过滤功能



图：屏蔽路由器防火墙

防火墙部署

- 双宿主主机 (Dual Homed Host)
  - 该类型主机具有至少两个网络接口，用于检查经过它的数据（从一个网络到另外一个网络）
  - 可在双宿主主机中配置NAT和代理两种安全机制



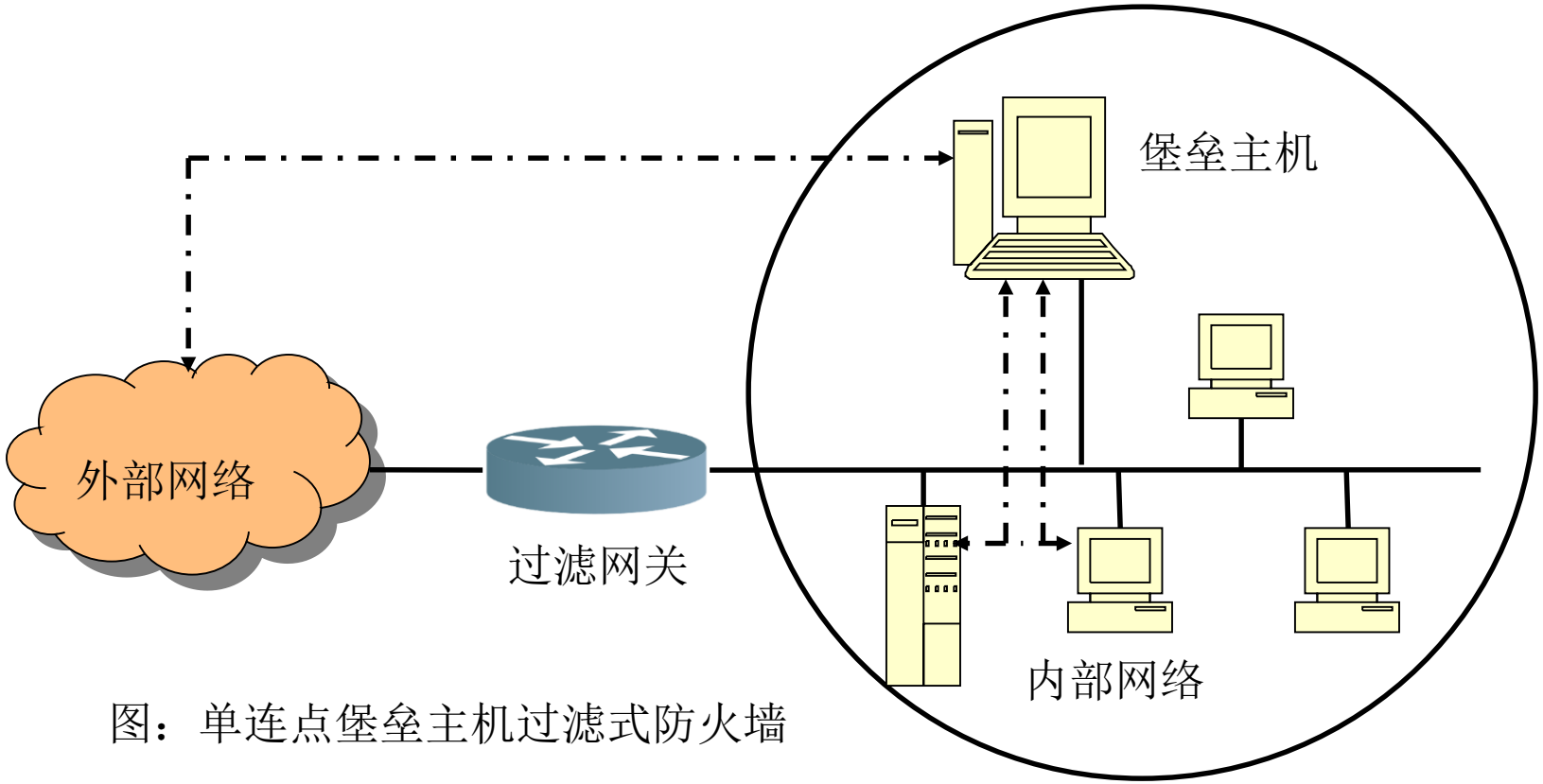
图：屏蔽路由器防火墙

防火墙部署

- 堡垒主机 (Bastion Host)
  - 一个被强化的、被暴露在被保护网络外部的、可预防进攻的计算机
  - 堡垒主机与内部网络是隔离的，并面对大量的恶意攻击
- 堡垒主机防火墙可以分为两种结构
  - 单连点结构
  - 双连点结构

堡垒主机：单连点结构

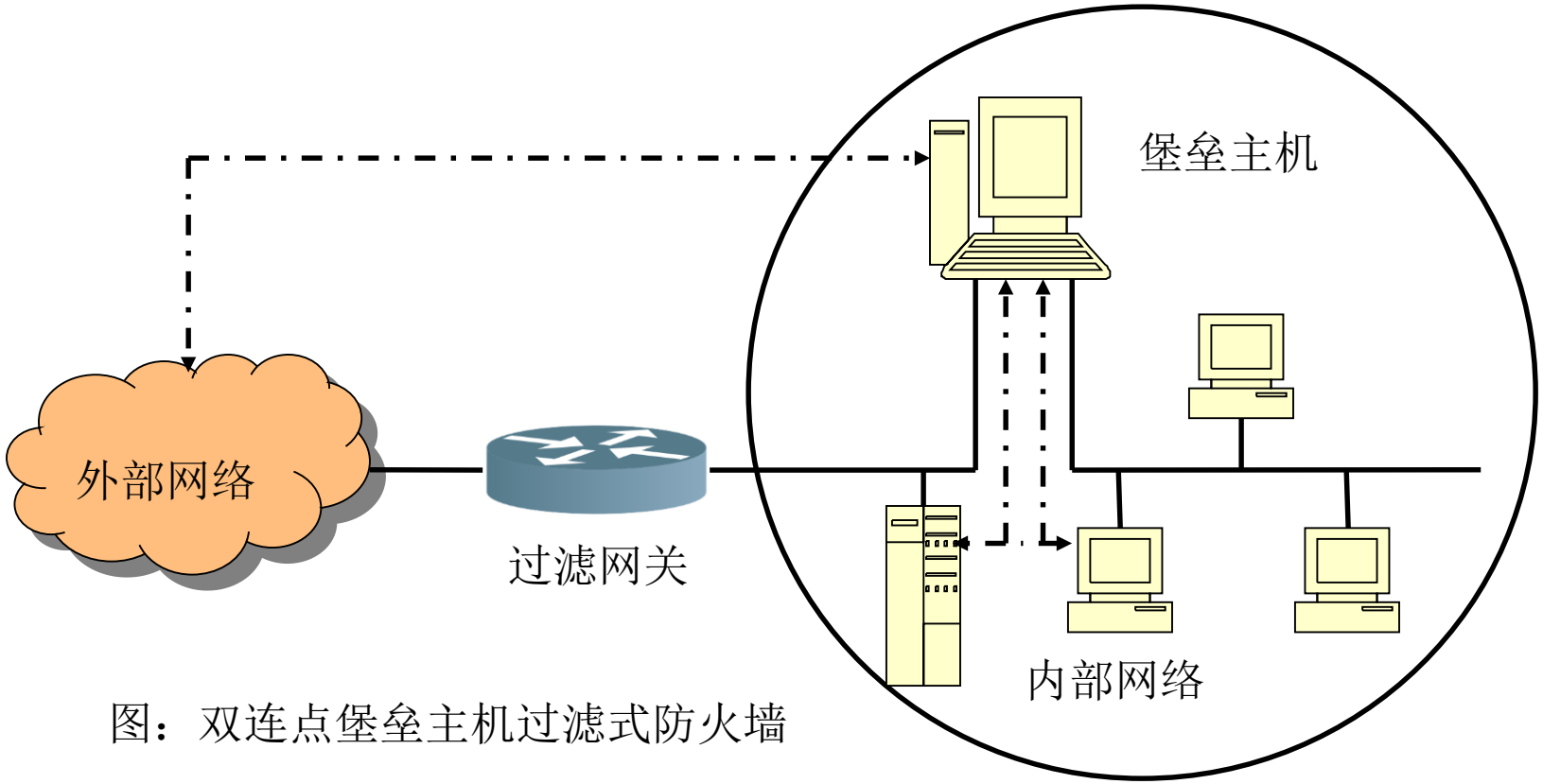
- 堡垒主机部署在过滤路由器之后，实现网络层安全(包过滤)和应用层安全(代理)，具有比单纯包过滤更高的安全等级



图：单连点堡垒主机过滤式防火墙

堡垒主机：双连点结构

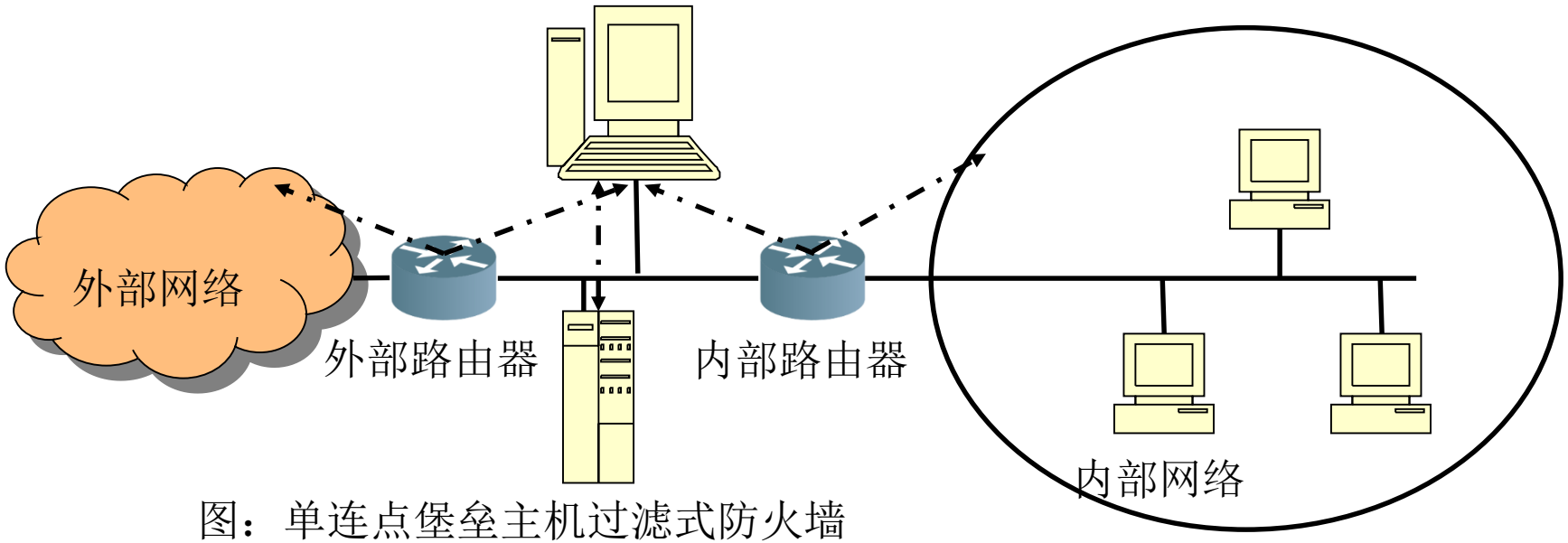
- 具有比单连点结构更高的安全等级



图：双连点堡垒主机过滤式防火墙

防火墙部署

- 屏蔽子网 (Screened subnet)
  - 在被保护网络和Internet之间设置一个独立的子网作为防火墙，即为非军事区



图：单连点堡垒主机过滤式防火墙

入侵检测系统

- 1980, James P. Anderson在《计算机安全威胁监控与监视》提出：应该针对计算机系统风险与威胁分类，并对系统非法行为进行跟踪与审计，以便监视入侵活动的思想。
  - 威胁可分为：外部渗透，内部渗透和不法行为
- 入侵(Intrusion)是一个广义的概念，包括
  - 收集系统漏洞
  - （分布式）拒绝服务攻击(DDOS)
  - 通过攻击获取系统合法权限
  - 等其他造成系统危害的行为

入侵检测系统

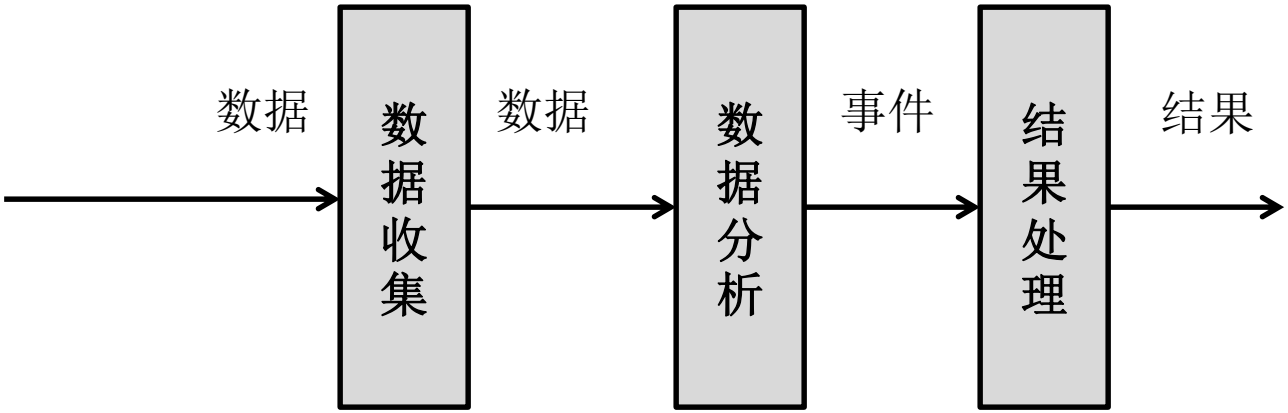
- 入侵检测系统(Intrusion Detection System, IDS)是对计算机和网络系统资源上的恶意使用行为进行识别和响应的处理系统
- IDS作为一种主动的安全防护技术，提供了对内部攻击，外部攻击和误操作的实时保护，被认为是防火墙后面的第二道安全防线
- IDS依赖于入侵特征(Signature)数据库进行入侵行为检测
  - 特征：指用于判别通信信息种类的样板数据，如僵尸网络特征等
- IDS除了包含检测模块外，通常还提供响应与警报功能
  - 主动响应：系统将自动阻断攻击工程
  - 被动响应：系统仅报告与记录发生的事件

入侵检测系统

- 具体功能
  - 监视并分析用户和系统的行为
  - 审计系统配置和漏洞
  - 评估敏感系统和数据的完整性
  - 识别攻击行为，对异常行为进行统计
  - 等等
- 实时与事后检测
  - 在系统使时进行审计还是针对用户操作的历史进行审计

入侵检测系统

- 入侵检测系统的通用模型
  - 粗略模型、反应入侵检测系统的最基本部件



信息收集与数据分析

- 数据收集的内容
  - 主机与网络日志文件
    - 登录记录，用户与用户访问权限变化等
  - 目录与文件的不期望改变
    - 黑客可能对正常情况下限制访问的文件进行改变（修改，创建和删除等）
  - 程序执行中的不期望行为
    - 改变进程的行为，使其失败或者越权
  - 物理形式的入侵信息

信息收集与数据分析

- 数据收集机制：要求准确性、可靠性和效率
  - 基于主机和基于网络的数据收集机制
    - 主机：在主机后台运行一个监控程序，检测各种可疑行径
    - 网络：在网络恰当位置部署网络引擎执行监控任务，检测特定网络数据流
    - 两种方式具有互补性，可结合使用，构造优化的主动防御体系
  - 分布式与集中式数据收集机制

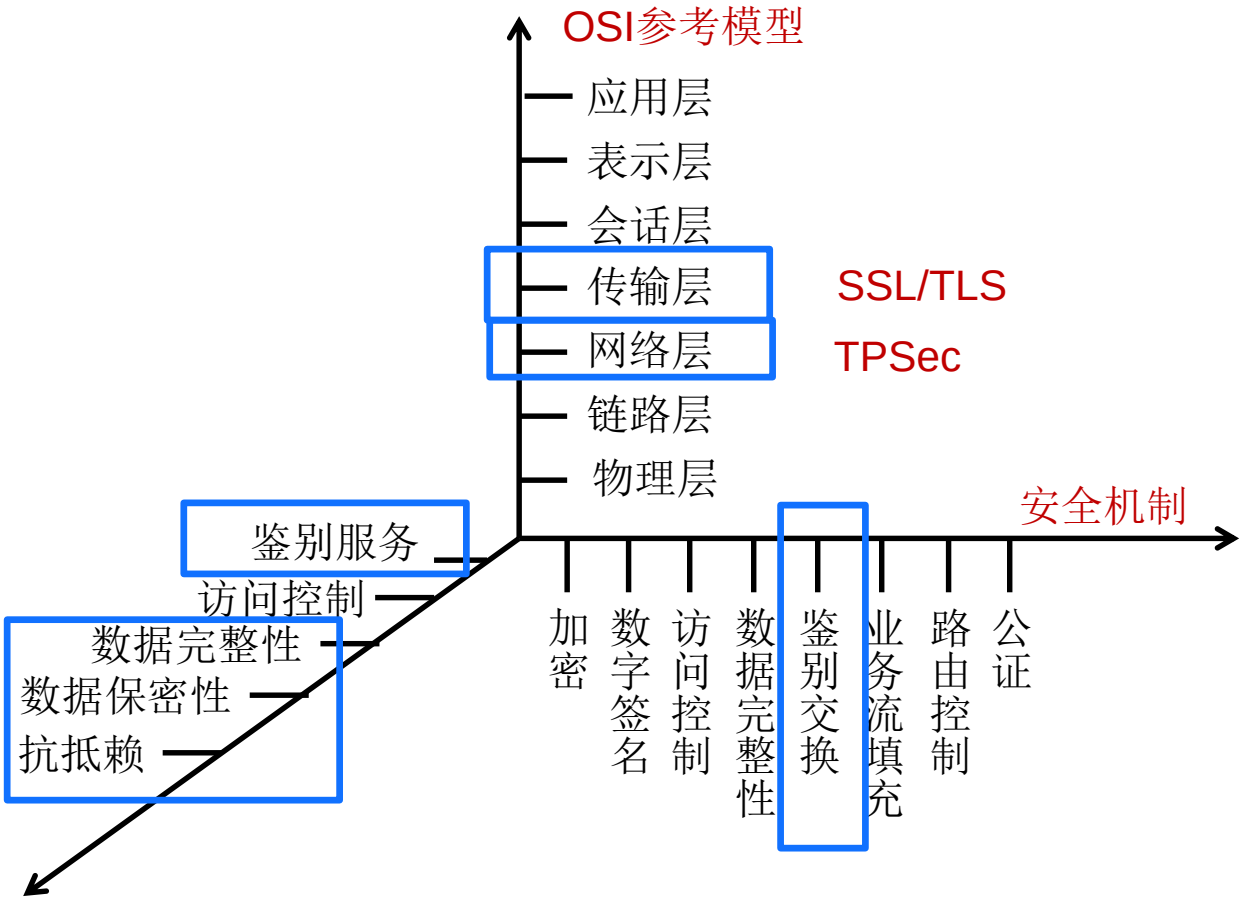
信息收集与数据分析

- 数据收集机制：要求准确性、可靠性和效率
  - 直接监控和间接监控
    - 直接：从它所监控的对象处获得数据
    - 间接：由一个单独的进程或工具获得数据
    - 直接方式更优，但是更复杂，不容易实现
  - 外部探测器和内部探测器

信息收集与数据分析

- 数据分析：对数据源提供的系统运行状态和活动记录进行同步、整理、组织、分类以及各种类型的细致分析，提取其中包含的系统活动特征或者模式，用于对正常和异常行为的判断
- 依据检测目标和数据属性，可分为两大类
  - 异常发现技术
    - 建立系统正常行为轨迹，则与正常行为轨迹不同的系统状态可视为可以异常
  - 模式发现技术，又称为特征检测或者滥用检测
    - 基于已知系统缺陷和入侵模式，需要事先定义出非法行为

网络安全体系结构


OSI参考模型
应用层
表示层
会话层
传输层
网络层
链路层
物理层
SSL/TLS
TPSec
安全机制
鉴别服务
访问控制
数据完整性
数据保密性
抗抵赖
加密
数字签名
访问控制
数据完整性
鉴别交换
业务流填充
路由控制
公证
安全服务

Internet各协议层次安全要素

<table>
<tr><td colspan="6">HTTPS、SET、PGP等</td><td colspan="2">应用层</td></tr>
<tr><td colspan="6">有状态检测、信息流管制、SSL/TLS等</td><td colspan="2">传输层</td></tr>
<tr><td colspan="6">安全路由协议、分组过滤、NAT、IPSec等</td><td colspan="2">网络层</td></tr>
<tr><td rowspan="2">以太网</td><td>安全端口、接入认证</td><td rowspan="2">无线局域网</td><td>WEP、WAP、WAP2</td><td rowspan="2">接入网络</td><td>接入认证、VPN、L2TP等</td><td>链路层</td><td rowspan="2">网络接口层</td></tr>
<tr><td>电缆、光缆保护、电磁屏蔽</td><td>信号能量控制</td><td>电缆、光缆保护、电磁屏蔽</td><td>物理层</td></tr>
<tr><td colspan="6">加密、消息认证、哈希函数、数字签名、实体认证等技术</td><td colspan="2">网络安全基础</td></tr>
</table>

实验（待安排）

- 最后一个实验（VPN，暂定）
  - 第11周星期4（5月14号）下午
- 实验报告：
  - 第一次：9周星期4之前
  - 第二次：10周星期4之前
  - 第三次：11周星期4之前
  - 第四次：12周星期4之前
- 评价系统+邮件
  - 主题:学号_姓名_infosec_report_X

Further Reading: