

网络安全 - 访问控制技术 (模型与应用)

曹越

国家网络安全学院

武汉大学

yue.cao@whu.edu.cn

上周回顾 - 1

1. 请简述DNS的工作原理，并指出在整个DNS解析过程中，可能存在的被欺骗攻击的地方。
2. Email欺骗攻击原理和过程
3. Web欺骗攻击有哪些具体形式？请简述其原理。

上周回顾 - 2

Web的三种安全问题

Web服务器常见漏洞

- 物理路径泄露，目录遍历，执行任意命令，缓冲区溢出，拒绝服务

什么是自主访问控制？方法有哪些？

基于访问者 (行)

- 权力表 (Capabilities List)
- 前缀表 (Profiles)
- 口令 (Password)

基于访问对象 (列)

- 保护位 (Protection Bits)
- 访问控制表 (Access Control List, ACL)

访问控制模式

物理隔离

访问控制模式

物理隔离

网络访问模式

网络的访问主要采用基于争用和定时两种方法

- 基于争用的方法意味着网上所有站点按先来先服务原则争用带宽
- 对网络的访问控制是为了防止非法用户进入系统和合法用户对系统的非法使用

功能

访问控制要对访问的申请、批准和撤消的全过程进行有效的控制

审计跟踪

- **对用户使用何种系统资源、使用的时间、执行的操作等问题进行完整的记录，以备非法事件发生后能进行有效的追查**

附加控制

- **除了对直接的访问进行控制外，还应对信息的流动和推理攻击施加控制**

口令

口令的选择原则

- 易记
- 难以被别人猜中或发现
- 抗分析能力强

需要考虑的方面

- 选择方法、使用期限、字符长度、分配和管理以及在计算机系统内的保护

口令等级

安全性要求	口令认证方案
无	无口令
低	合法用户公用口令
中	每个用户一个单独的口令
高	要求一次一密，或口令分散

系统中不存储口令的原文

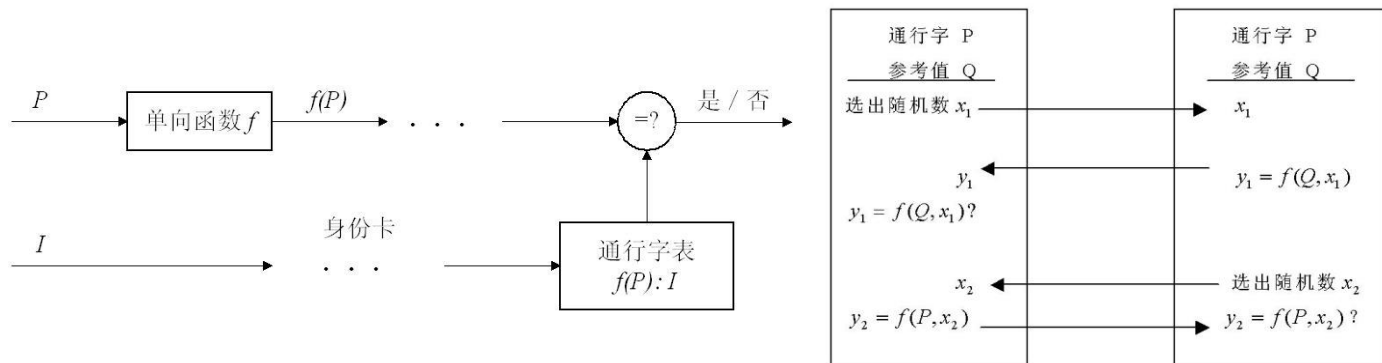
认证方式

单向认证

双向认证

询问认证

- 受理的用户可利用他所知道、而别人不太知道的一些信息向申请用户提问一系列不大相关的问题



访问控制模型 - 自主访问控制

自主访问控制

- Discretionary Access Control, 简称DAC
- 自主访问控制基于对主体或主体所属的主体组的识别来限制对客体的访问，这种控制是自主的

自主

- 是指对其它具有授予某种访问权力的主体能够自主地（可能是间接的）将访问权的某个子集授予其它主体

访问控制模型 - 强制访问控制 1

强制访问控制

- **Mandatory Access Control, 简称MAC**
- **用户与文件都有一个固定的安全属性, 系统利用安全属性来决定一个用户是否可以访问某个文件**
- **安全属性是强制性的, 它是由安全管理员或操作系统根据限定的规则分配的, 用户或用户的程序不能修改安全属性**

访问控制模型 – 强制访问控制 2

强制访问控制

- 如果系统认为具有某一安全属性的用户不适于访问某个文件，那么任何人（包括文件的拥有者）都无法使该用户具有访问文件的能力
- 强制访问控制是比任意访问控制更强的一种访问控制机制，它可以通过无法回避的访问限制来防止某些对系统的非法入侵
- 强制访问控制可以防止一个进程生成共享文件，从而防止一个进程通过共享文件把信息从一个进程传送给另一个进程

DAC与MAC

DAC的优点

- 方便、实用
- 可由用户自由定制
- 可扩展性强

缺点

- 管理分散、用户关系不清
- 权限易被滥用

MAC一般与自主访问控制结合使用，并实施一些附加的、更强的访问限制

缺点

- 限制访问控制的灵活性
- 过程控制

如何结合？

DAC、MAC结合

自主访问控制防范其他用户对自己客体的攻击

强制访问控制防止其他用户偶然或者滥用自主访问控制权利

减少特洛伊木马攻击成功的可能性

- **限制访问控制的灵活性**
- **过程控制：警告用户不要运行系统目录以外的任何程序**

BLP与BIBA模型 - 1

Bell-La Padual模型 不足?

➤ 简单安全规则

- 仅当主体的敏感级**不低于**客体敏感级且**主体的类别集合包含客体时**，才允许该主体读该客体。
- 即主体只能读密级等于或低于它的客体，也就是说主体只能从下读，而不能从上读

➤ 星规则

- 仅当主体的敏感级**不高于**客体敏感级且**客体的类别集合包含主体的类别集合时**，才允许该主体写该客体。
- 即主体只能写密级等于或高于它的客体，也就是说主体只能向上写，而不能向下写

BLP与BIBA模型 - 2

BIBA模型

➤ 简单完整规则

- 仅当主体的完整级**大于等于**客体的完整级且**主体的类别集合包含客体的类别集时**，才允许该主体写该客体。
- 即主体只能向下写，而不能向上写，也就是说主体只能写（修改）完整性级别等于或低于它的客体

➤ 完整性制约规则（星规则）

- 仅当主体的完整级**不高于**客体完整级且**客体的类别集合包含主体的类别集合时**，才允许该主体读客体。
- 即主体只能从上读，而不能从下读

基于角色的访问控制技术 - 1

RBAC (Role-Based Access Control)

四种RBAC模型

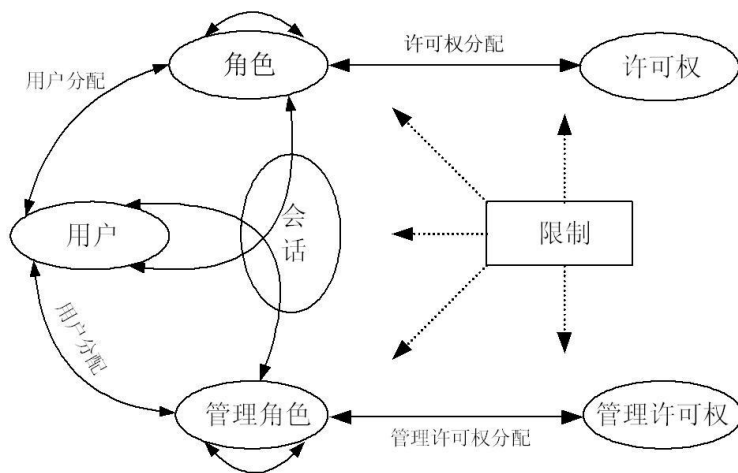
- 基本模型 $RBAC_0$
- 角色的层次结构 $RBAC_1$
- 约束模型 $RBAC_2$
- 混合模型 $RBAC_3$

基于角色的访问控制技术 - 2

基本模型RBAC₀

➤ 四个基本要素

- 用户 (User)
- 角色 (Role)
- 会话 (Session)
- 授权 (Permission)



基于角色的访问控制技术 - 3

角色的层次结构RBAC₁

- RBAC₁的特征是为RBAC₀上引入了角色层次的概念

约束模型RBAC₂

- RBAC₂除了继承RBAC₀的原有特征外，还引入了约束 (Constraints) 的概念
- 互斥角色 (Mutually Exclusion Roles)
- 基数约束 (Cardinality Constraints)
- 先决条件角色
- 运行时约束

基于角色的访问控制技术 - 4

RBAC模型的优点

- 一种策略无关的访问控制技术
- 具有自我管理的能力
- 使得安全管理更贴近应用领域的机构或组织的实际情况

RBAC模型的不足

- 复杂、不成熟
- RBAC的策略无关性需要用户自己定义适合本领域的安全策略

其他访问控制技术 - 5

基于任务的访问控制技术

- TBAC (Task-Based Access Control)

基于组机制的访问控制技术

...

物理隔离

物理隔离

完全隔离

逻辑隔离

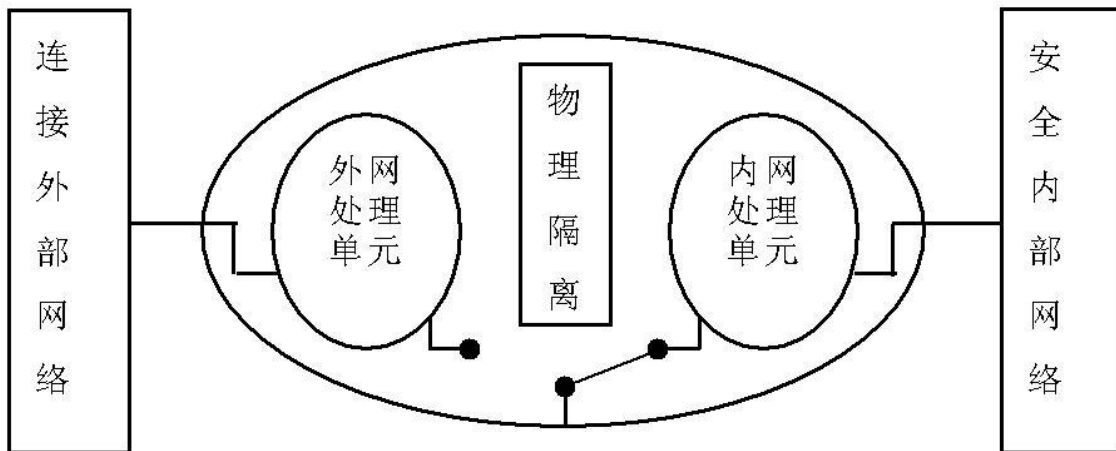
- 逻辑隔离技术是一种将内外网络从**物理上断开**，但保持逻辑连接的网络安全技术
- 任何时候内外网络都不存在连通的**物理连接**，同时原有的传输协议必须被中断
- 逻辑连接指能进行适度的数据交换

1999年12月29日国家保密局发布的《计算机信息系统国际联网保密管理规定》中第二章第六条规定：

- “涉及国家秘密的计算机信息系统，不得直接或间接地与国际互联网或其他公共信息网络相联接，必须进行物理隔离”

隔离方案 - 客户端的物理隔离 1

客户端的（物理硬盘空间）物理隔离

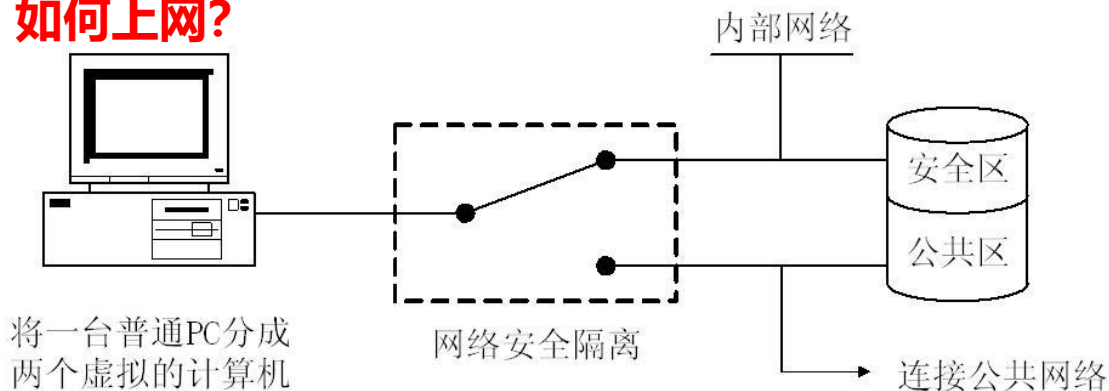


隔离方案 - 客户端的物理隔离 2

客户端的物理隔离 — 网络安全隔离卡



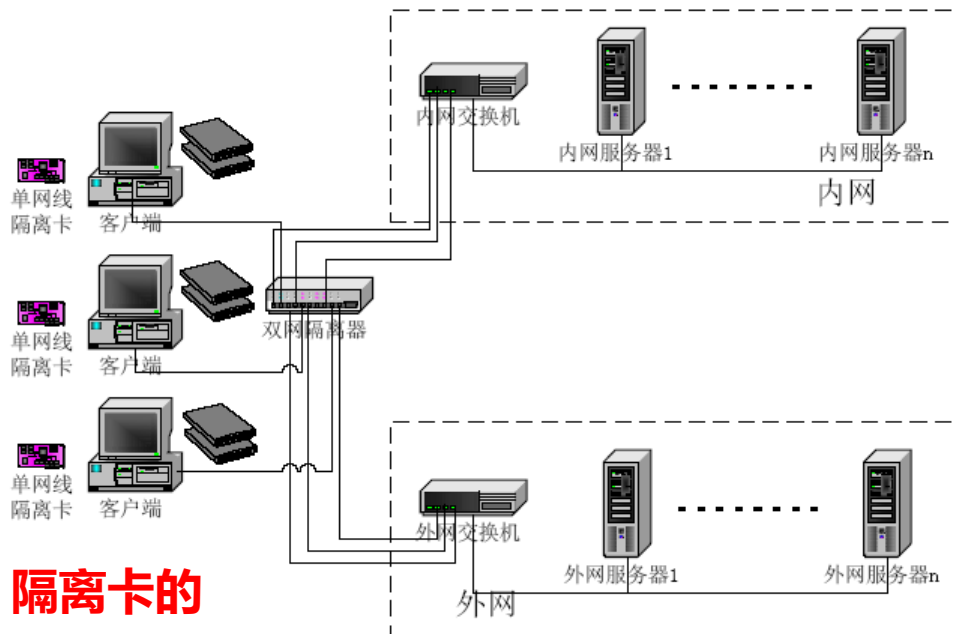
如何上网?



设置过渡区?

隔离方案 - 客户端的物理隔离 3

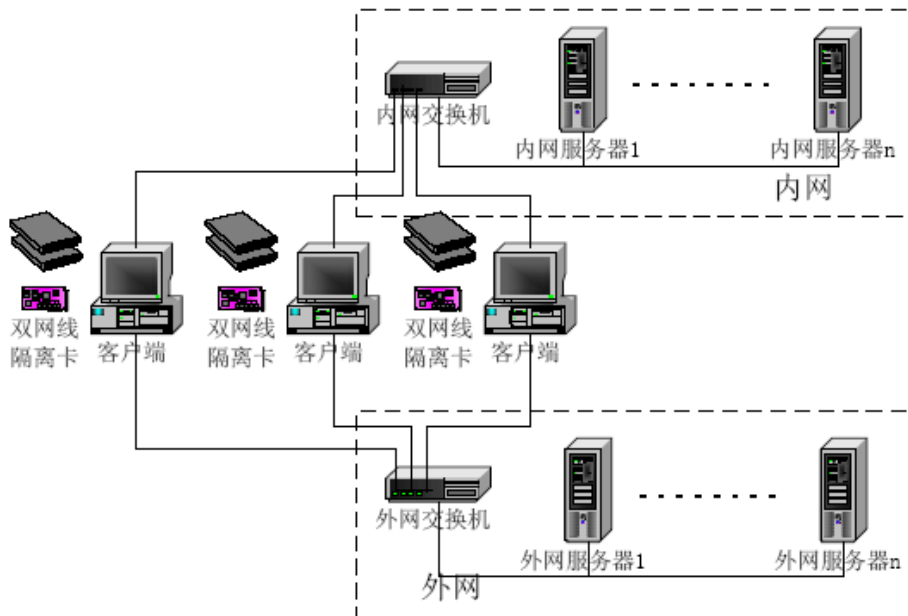
隔离网卡的应用方案 (一)



网卡、隔离卡的区别？

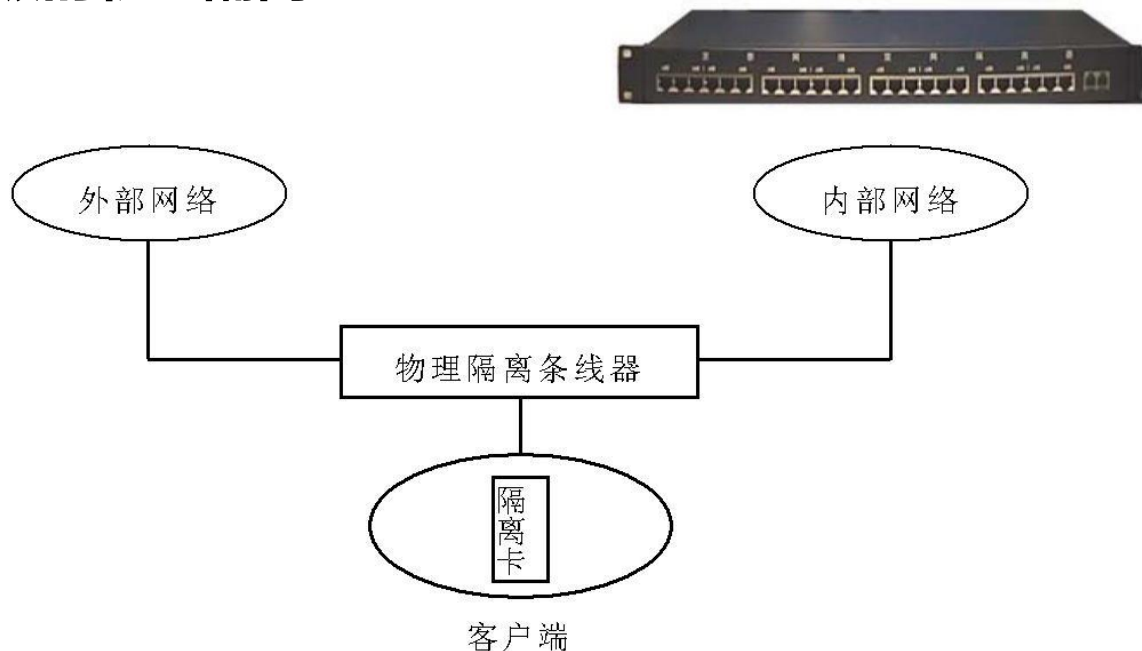
隔离方案 - 客户端的物理隔离 4

隔离网卡的应用方案（二）



隔离方案 - 集线器的物理隔离

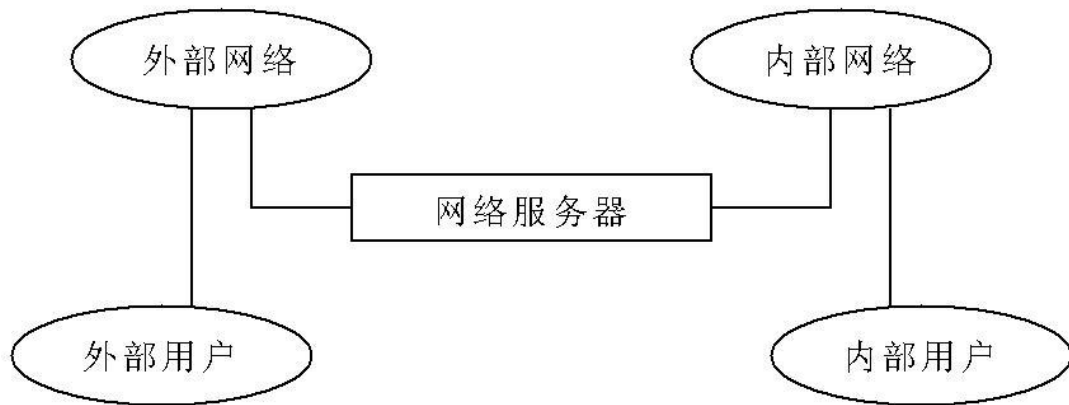
集线器级的物理隔离



在内外网线上，通过一条网络线来联通远端切换器

隔离方案

服务器端的物理隔离

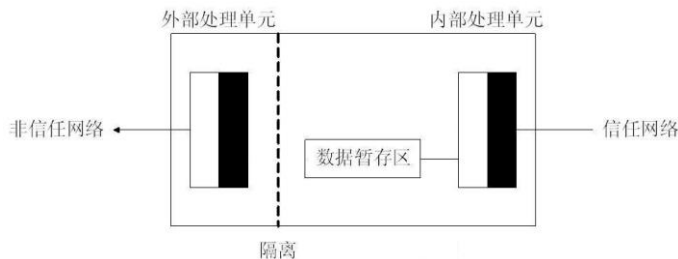
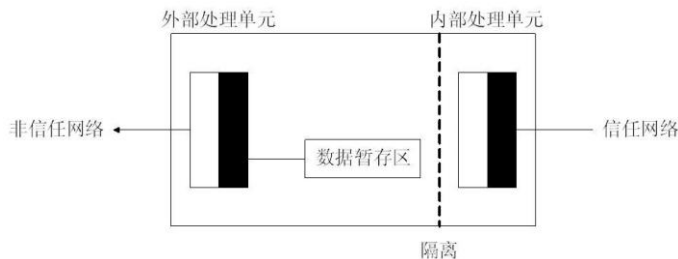


隔离方案

隔离网闸

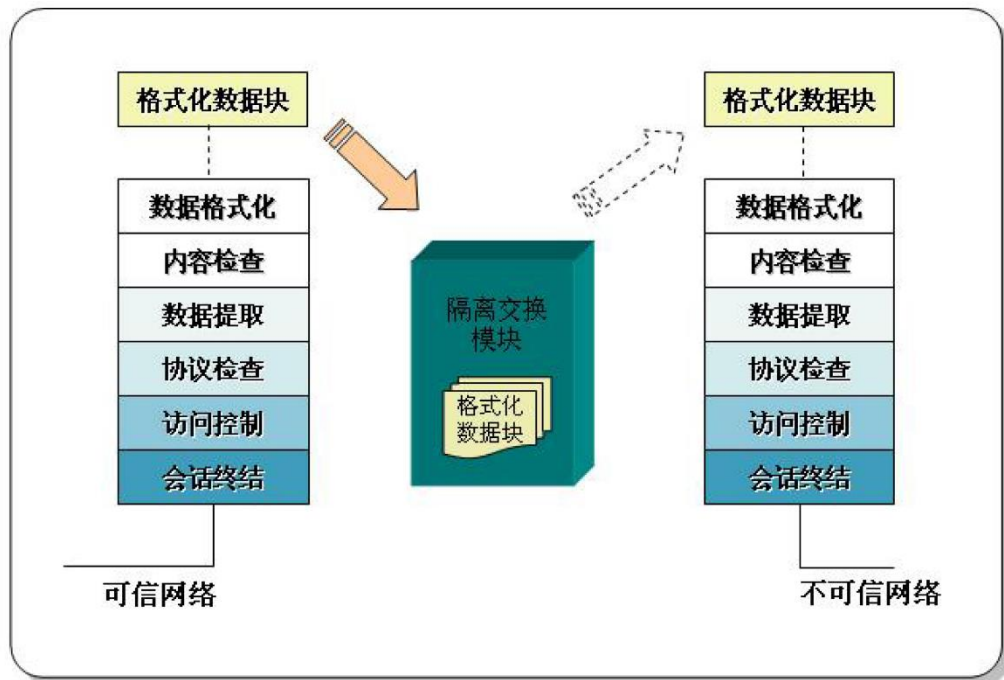
- 一套双主机系统
- 之间永远断开
- 拷贝、镜像等方式共享
- 与防火墙机理不同

互联>安全 or 安全>互联





网闸工作逻辑图

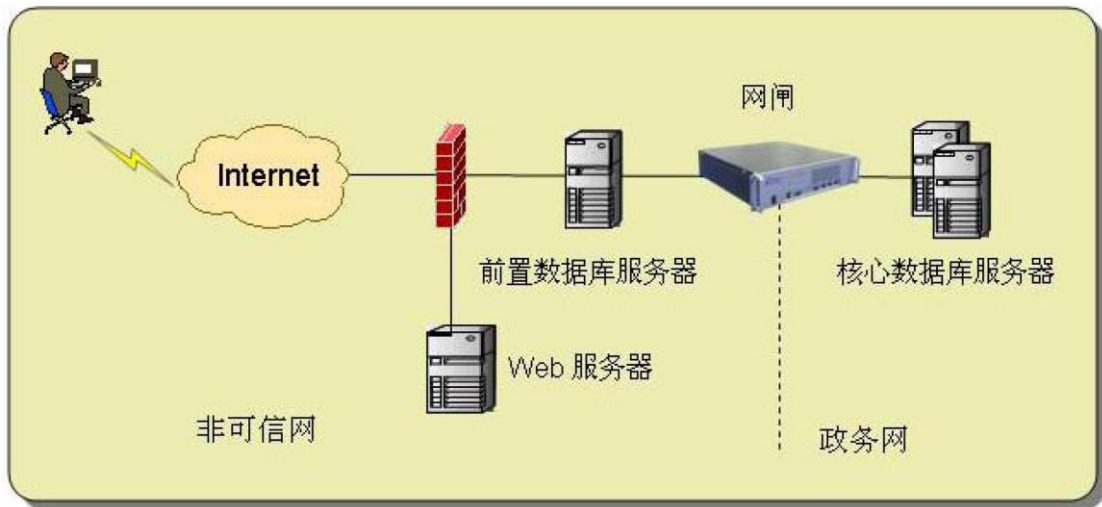


网闸能够交换的数据类型

- **文件交换模块：**实现不同安全等级网络间文件的安全交换
- **数据库同步模块：**通过灵活的同步机制，保证安全等级不同的网络中的数据库系统实现数据同步更新
- **邮件交换模块：**保证在内外网隔离的环境下实现安全的邮件收发
- **安全浏览模块：**保证在内外网隔离的环境下，内网用户安全浏览外网资源
- **通用模块：**保证内外网隔离的同时实现FTP、DNS、TNS 等协议及其他
- **通用TCP/IP 协议的定制交换。**
- **其它定制用户专有应用模块。**

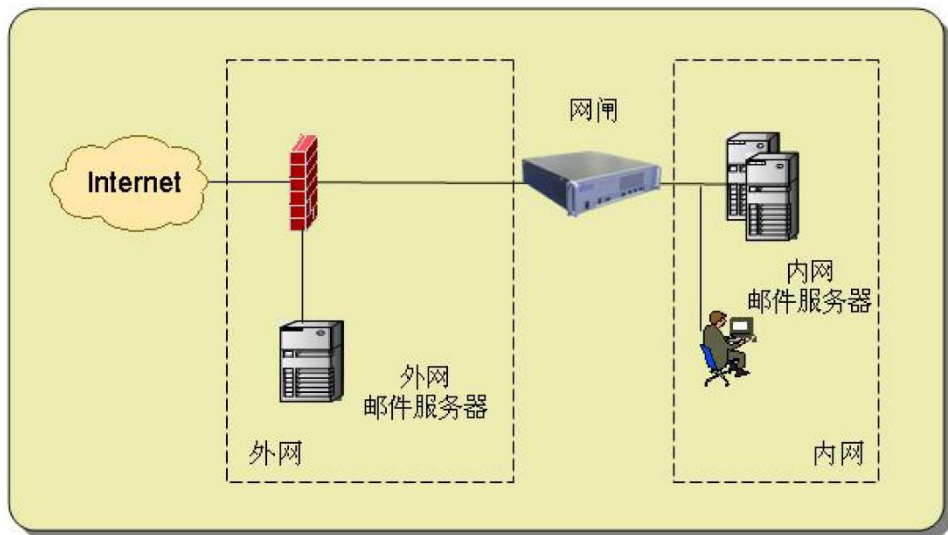
网闸应用例

数据库同步



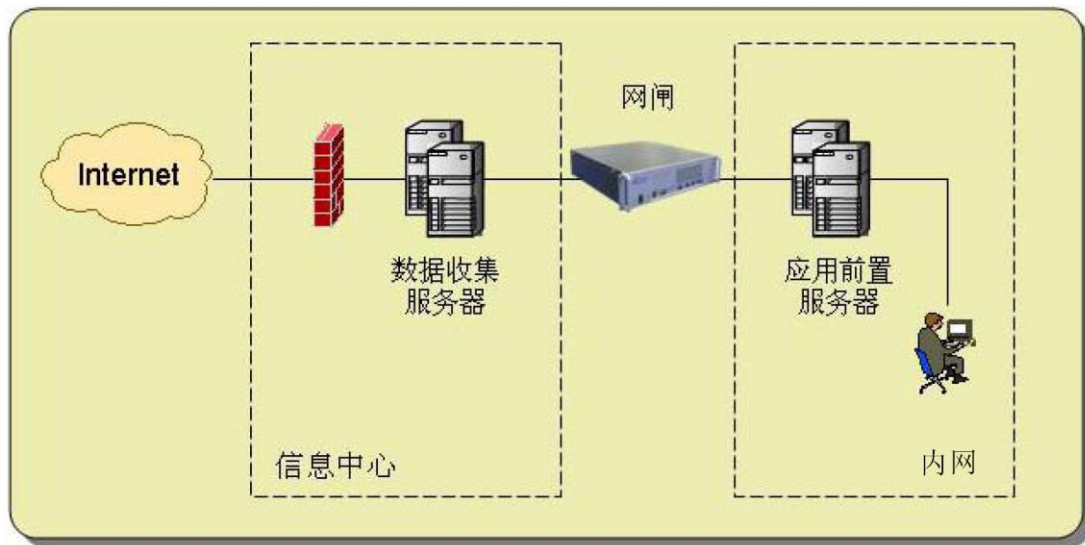
网闸应用例

邮件同步



网闸应用例

文件同步



对比

网闸

- 交换模块的安全不依赖于任何操作系统
- 分析应用层数据

防火墙

- 软件的运行依赖于操作系统的安全
- 一般只关心地址和端口

网闸

物理隔离的优点

- 安全级别高，保障强
- 易于在现有涉密网上安装

物理隔离的未尽之处

- 资源消耗大
- 没有实时功能
- 缺乏管理
 - 认证、访问控制、审计、取证
- 妨碍应用

思考题

1. 简述口令认证技术的认证方法。用哪些方法可以提高口令认证技术的安全性？
2. 网络的物理隔离技术包含哪几方面？它们各自采用了什么样的技术？
3. 什么是基于角色的访问控制技术？它与传统的访问控制技术有什么不同？
4. 简述RBAC模型技术。它们各有什么特点？

谢谢!