访问控制技术

基本概念

自主访问控制方法

自主访问控制的类型

自主访问控制的优劣

访问控制模式

物理隔离

什么是“访问”

常规领域

- **Visit**

安全领域

- **Access**

美国国防部

…要讨论安全，…陈述安全。

…安全的系统会利用一些…安全特性来控制对信息的访问，…被授权的人…可以读、写、创建和删除这些信息。

访问控制技术

要保证计算机系统实体的安全，必须对计算机系统的访问进行控制

访问控制的基本任务

- **防止非法用户即未授权用户进入系统**
- **合法用户即授权用户对系统资源的非法使用**

3种安全控制技术：访问控制
信息流控制
推理控制

基本概念

主体：信息系统中用户或进程，系统所有的用户与进程形成主体集合

客体：系统中被处理、被控制或被访问的对象（如文件、程序、存储器等）

访问控制关系：根据制定的系统安全策略，形成了主体与客体、主体与主体、客体与客体相互间的关系。

访问控制的有效性

建立在两个前提上

l 用户鉴别与确证

l 信息受保护，不会被非法修改

基本概念

自主访问控制方法

自主访问控制的类型

自主访问控制的优劣

访问控制矩阵

	内容 1	内容 2	…	…	…	…
被授权者 1	A\B	A\B\C				
被授权者 2		A\B\C				
…						
…		…				
…					…	
…		…				

自主访问控制方法 - 1

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)**

自主访问控制方法 - 2

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)**

基于行 – 权利表

权利表决定用户是否可以对客体进行访问，以及以何种模式的访问（如读，写，执行）。

可以动态的发放和回收、删除或增加权利。

由于不能确定有权访问客体的所有主体，所以利用权利表不能实现完整的自主访问控制。

访问控制矩阵 - 权利表

	内容 1	内容 2	…	…	…	…
被授权者 1	A\B	A\B\C				
被授权者 2		A\B\C				
…						
…		…				
…					…	
…		…				

基于行－前缀表

前缀表中存放着主体可访问的每个客体的名字和访问权。

当主体要访问某个客体时，系统将检查该主体的前缀中是否具有它所请求的访问权。

基于行－前缀表存在的问题

主体的前缀表可能很大，增加了系统管理的困难。

只能由系统管理员进行修改。这种管理方法有些超出了DAC原则。

消与删除困难。

要系统回答“谁对某一客体具有访问权”这样的问题比较困难。但这个问题在安全系统中却是很重要的。

基于行－口令

每个客体相应地有一个口令，当主体请求访问一个客体时，必须向系统提供该客体的口令。

请注意，这里讲的口令与用户登录进入系统时回答的口令不是一回事。

为了安全性起见，一个客体至少要有两个口令，一个用于控制读，一个用于控制写。

利用口令机制对客体实施的访问控制是比较麻烦的和脆弱的

基于行－口令机制的缺陷

系统不知谁访问了客体：对客体访问的口令是手工分发的，不需要系统参与

安全性脆弱：需要把该客体的口令写在程序中，这样很容易造成口令的泄露。

使用不方便：每个用户需要记忆许多需要访问的客体的口令，很不友好。

管理麻烦：撤消某用户对某客体的访问权，只能改变该客体的口令，必须通知新口令给其他用户。

自主访问控制方法 - 3

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)**

基于列 – 保护位

保护位对所有主体、主体组以及该客体的拥有者指定了一个访问权限的集合，UNIX中利用了这种机制。

在保护位中包含了主体组的名字和拥有者的名字。保护位机制中不包含可访问该客体的各个主体的名字。

由于保护位的长度有限，用这种机制完全表示访问矩阵实际上是不可能的。

基于列 – 访问控制表

在这种机制中，每个客体附带了访问矩阵中可访问它自己的所有主体的访问权限信息表（即ACL表）。

该表中的每一项包括主体的身份和对该客体的访问权。

如果利用组或通配符的概念，可以使ACL表缩短。

ACL方式是实现DAC策略的最好方法。

客体i	id_1. RW	id_2. RE	id_3. R ……	id_n. E	

解决ACL表的长度问题

- 解决的办法是设法缩短ACL表的长度，采用分组与通配符的方法有助于达到该目的。一般而言，一个单位内部工作内容相同的人需要涉及的客体大部分是相同的，把他们分在一个组内作为一个主体对待，可以显著减少系统中主体的数目。再利用通配符手段加快匹配速度，同时也能简化ACL表的内容。通配符用“*”表示，可以代表任意组名或主体标识符。

基本概念

自主访问控制方法

3种控制访问权手段 **自主访问控制的类型**

自主访问控制的优劣

层次型

层次型的（hierarchical）文件的控制关系一般都呈树型的层次结构，系统管理员可修改所有文件的ACL表，文件主可以修改自己文件的ACL表。

层次型的优点是可以通过选择可信的人担任各级权限管理员，

缺点是一个客体可能会有多个主体对它具有控制权，发生问题后存在一个责任问题。

属主型

该类型的访问权控制方式是为每一个客体设置拥有者，一般情况下客体的创建者就是该客体的拥有者。

拥有者拥有对自己客体的全部控制权，但无权将该控制权转授给其他主体。

拥有者是唯一可以修改自己客体的ACL表的主体，也可以对其他主体授予或撤消对自己客体的访问操作权。

如果主体（用户）被调离他处或死亡，系统需要利用某种特权机制来删除该主体拥有的客体。

自由型的

客体的拥有者（创建者）可以把对自己客体的许可权转授给其他主体，并且也可以使其他主体拥有这种转授权，而且这种转授能力不受创建者自己的控制。

但由于这种许可权（修改权）可能会被转授给不可信的主体，因此这种对访问权修改的控制方式是很不安全的。

授权于谁

访问控制表

- **基于访问者**
- **基于访问对象**

基于角色的访问控制技术

- **RBAC (Role-Based Access Control)**

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 (基于偏序关系)

…

自主访问控制优缺点

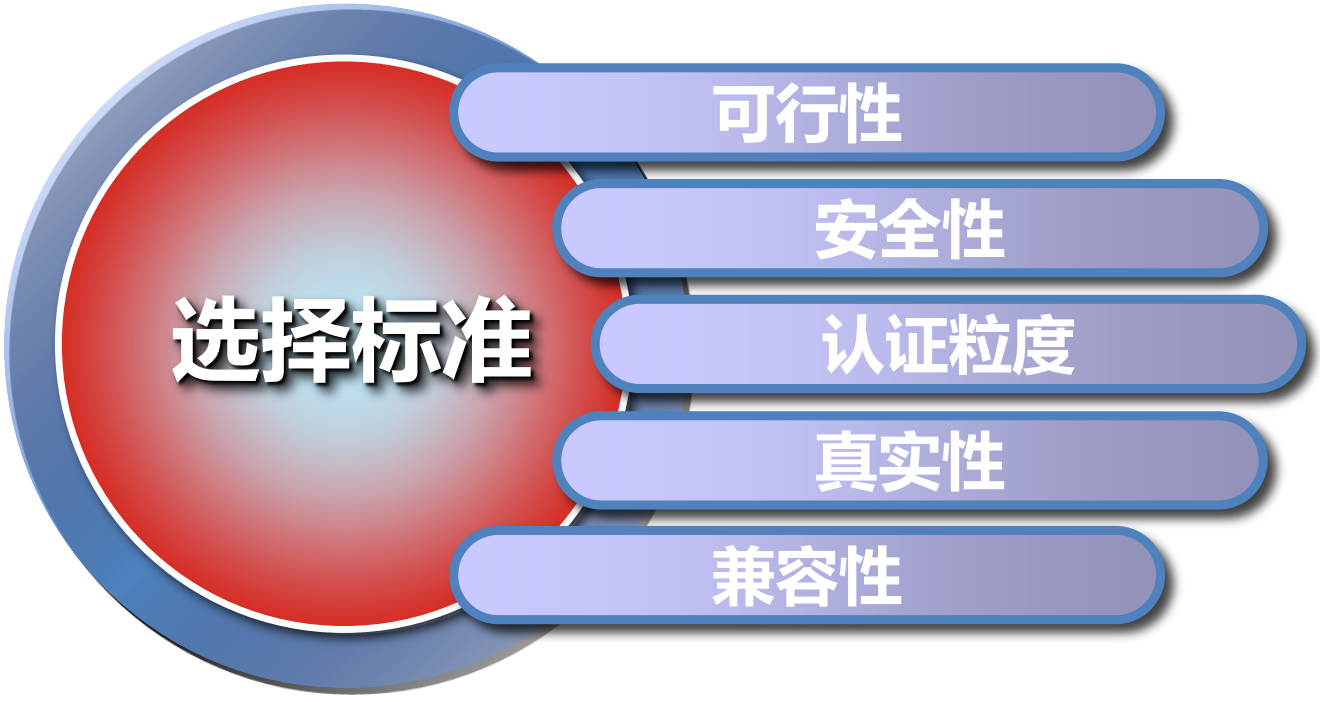
优点

- **方便、实用**
- **可由用户自由定制**
- **可扩展性强**

缺点

- **允许用户自主地转授访问权，这是系统不安全的隐患。**
- **系统无法区分是用户合法的修改还是木马程序的非法修改；**
- **无法解决因用户无意（如程序错误、某些误操作等）或不负责任的操作而造成的敏感信息的泄漏问题。**

身份认证



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

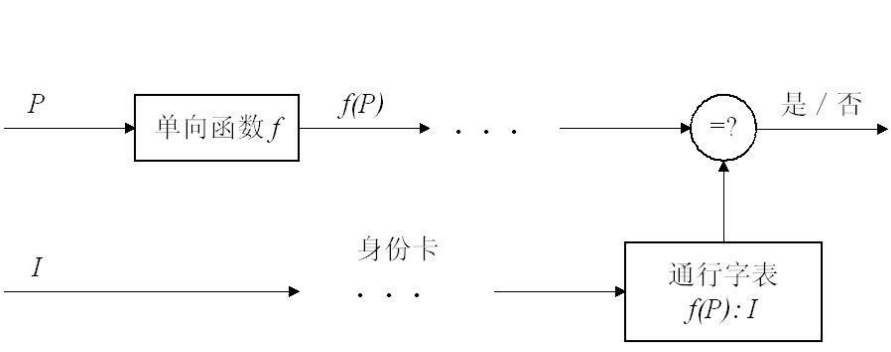
认证方式

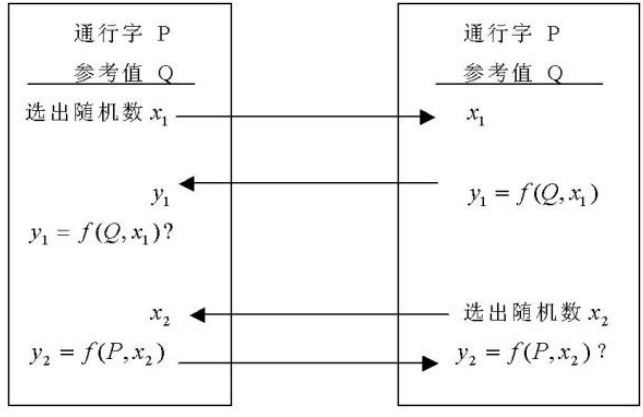
单向认证

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

一、 MAC机制的实现方法

- 最主要的是要做到两条：
- 第一是访问控制策略要符合MAC的原则，

把这些权利交给全系统权利最高和最受信任的安全管理员。

- 第二是对系统中的每一个主体与客体都要加安全标记，使它和主体或客体紧密相连而无法分开。

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

如何结合?

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

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)

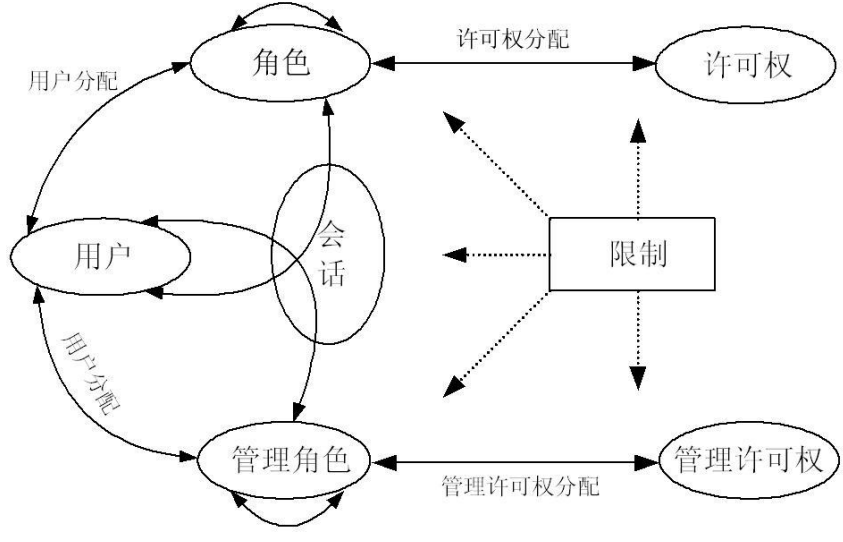
四种RBAC模型

- **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$RBAC_0$

- 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$RBAC_1$

- **$RBAC_1$的特征是为$RBAC_0$上引入了角色层次的概念**

约束模型$RBAC_2$

- **$RBAC_2$除了继承$RBAC_0$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

完全隔离

逻辑隔离

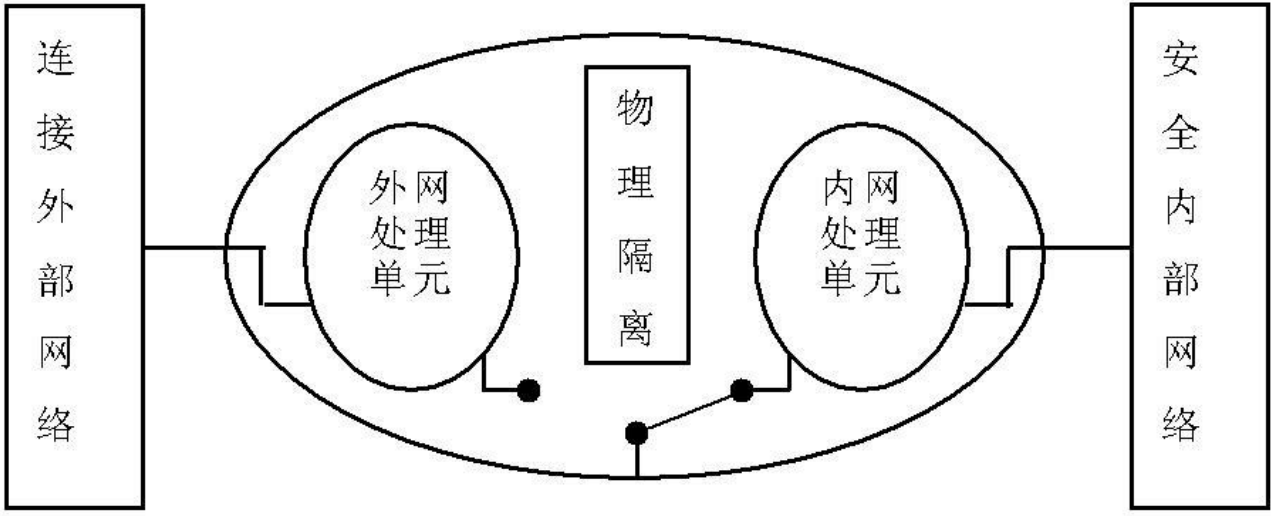
- **逻辑隔离技术是一种将内外网络从物理上断开，但保持逻辑连接的网络安全技术**
- **任何时候内外网络都不存在连通的物理连接，同时原有的传输协议必须被中断**
- **逻辑连接指能进行适度的数据交换**

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

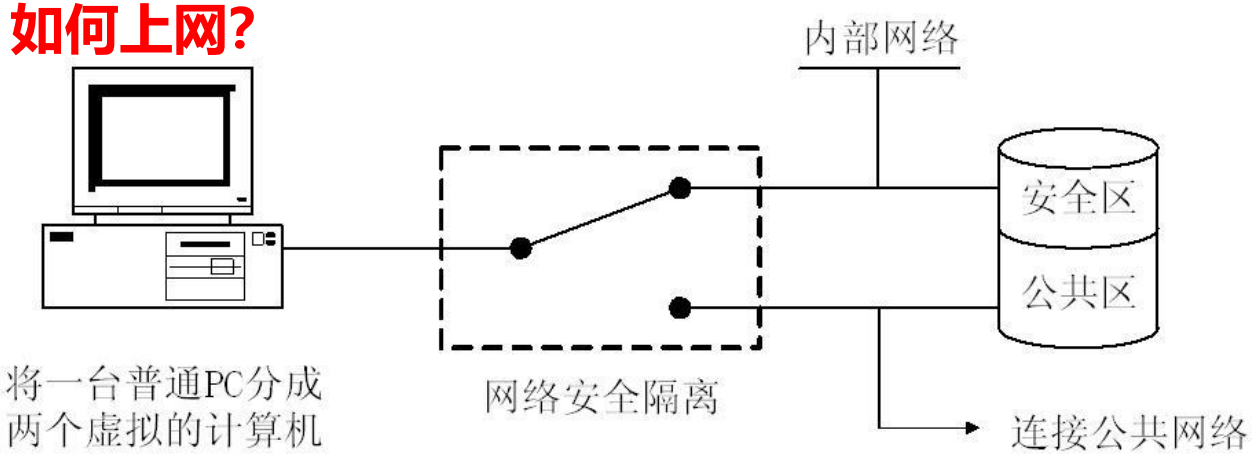


隔离方案 - 客户端的物理隔离 2

客户端的物理隔离

– 网络安全隔离卡

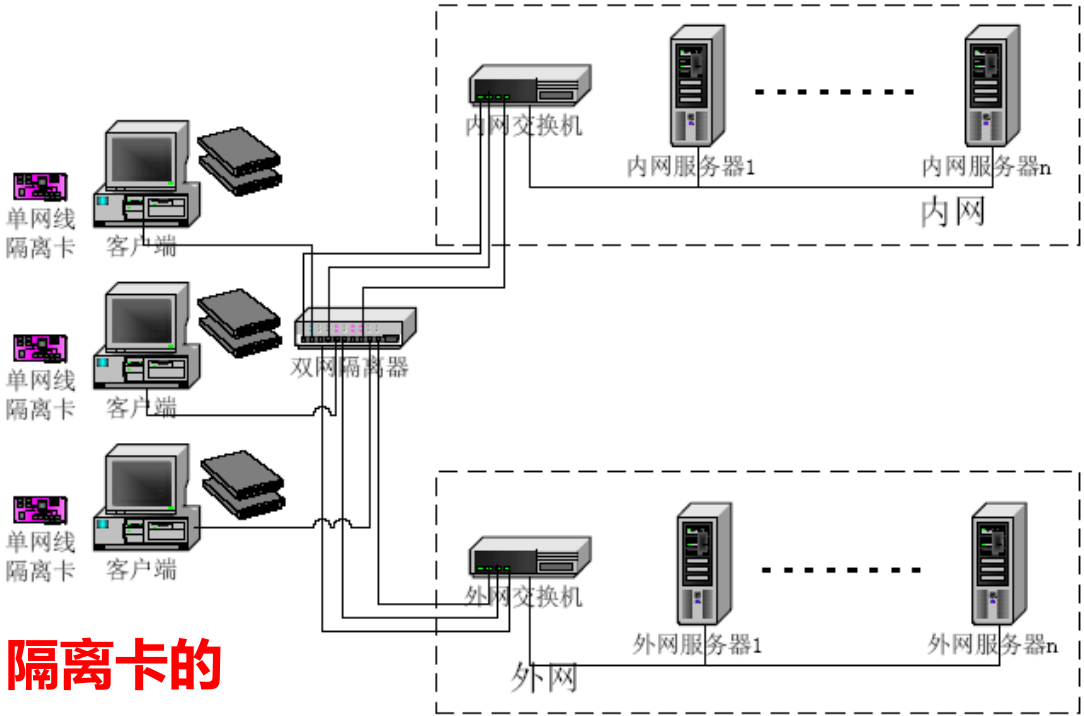
如何上网?



设置过渡区?

隔离方案 - 客户端的物理隔离 3

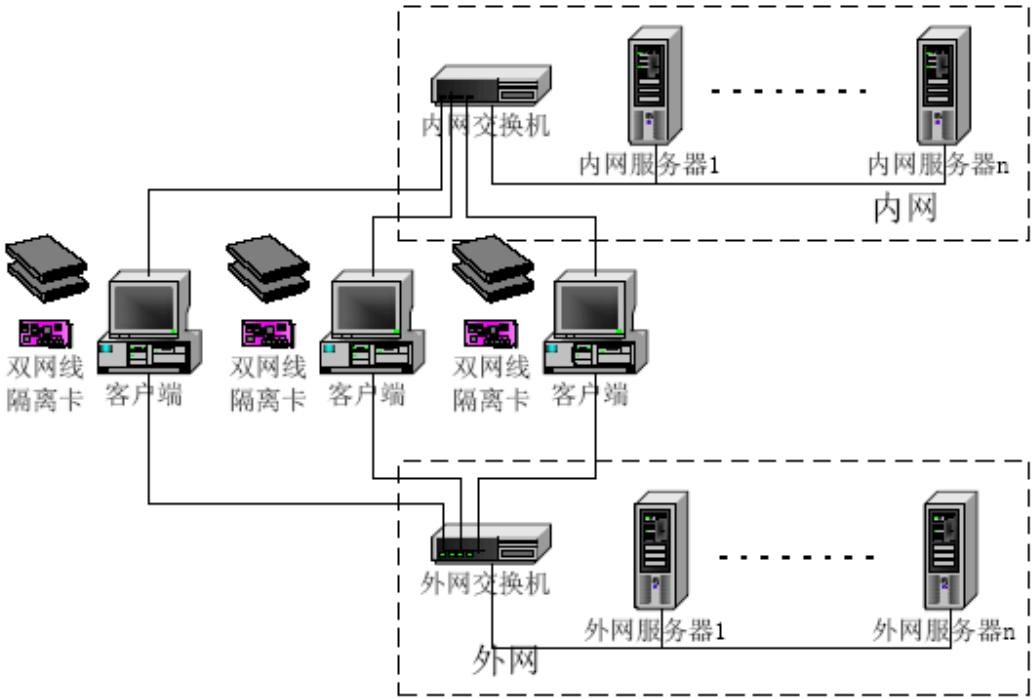
隔离网卡的应用方案（一）



网卡、隔离卡的区别?

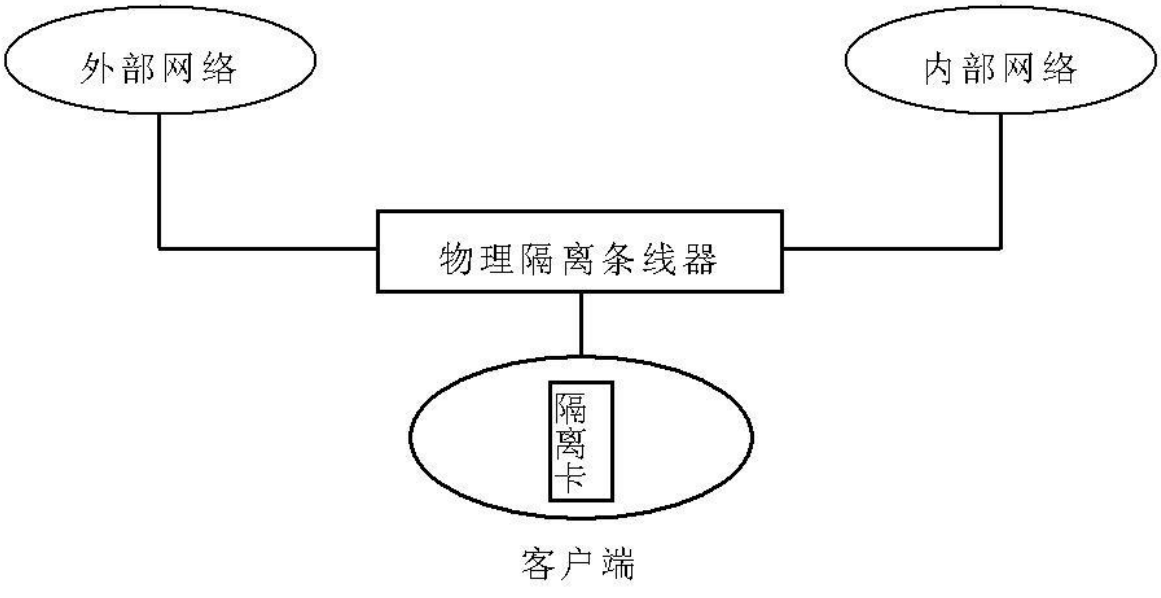
隔离方案 - 客户端的物理隔离 4

隔离网卡的应用方案（二）



隔离方案 - 集线器的物理隔离

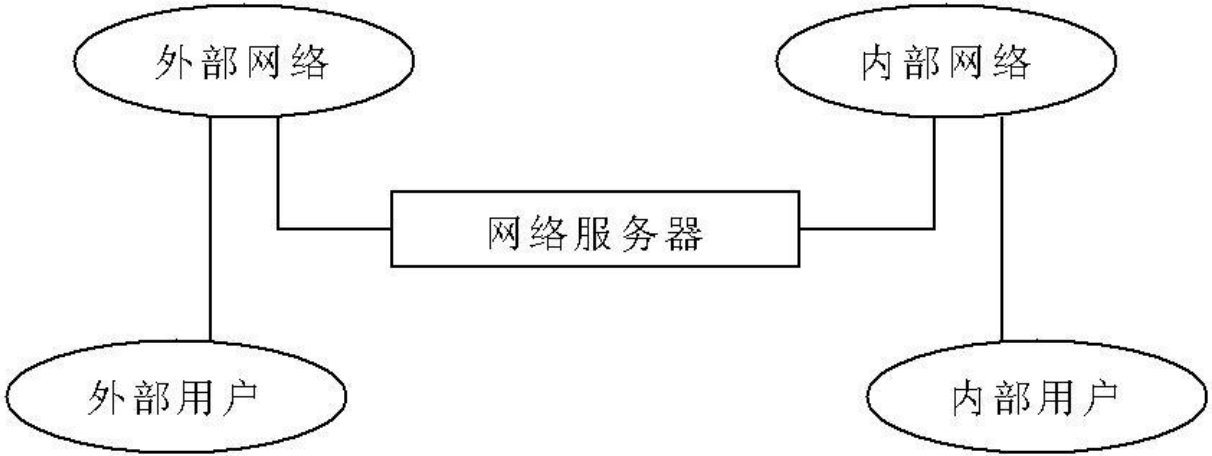
集线器级的物理隔离



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

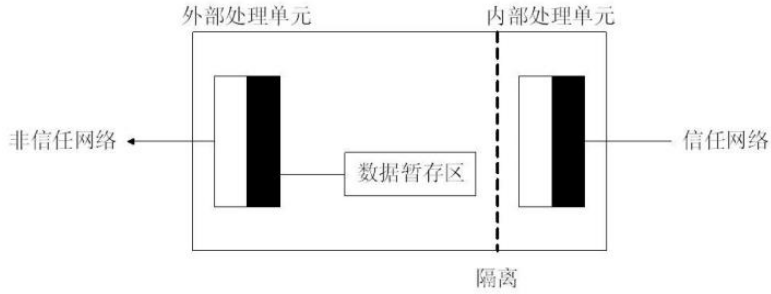


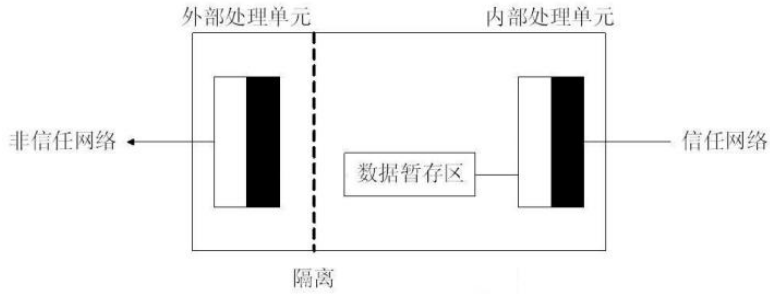
隔离方案

隔离网闸

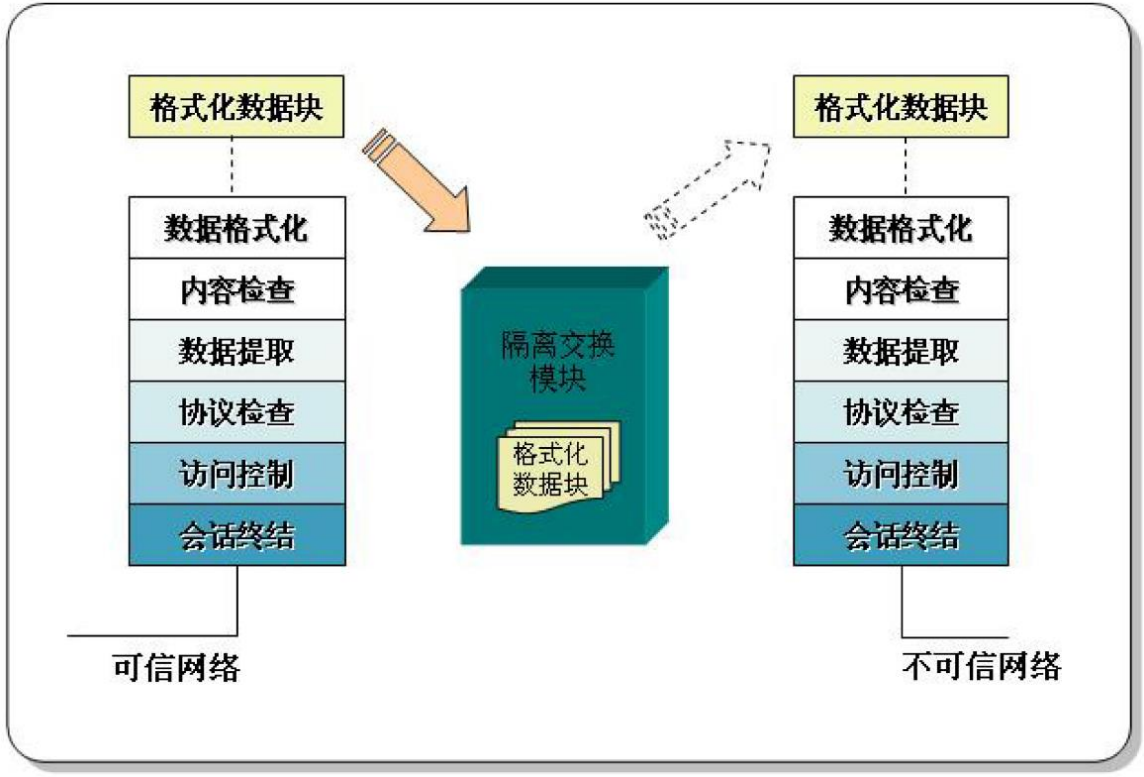
- 一套双主机系统
- 之间永远断开
- 拷贝、镜像等方式共享
- 与防火墙机理不同

互联>安全 or 安全>互联





网闸工作逻辑图

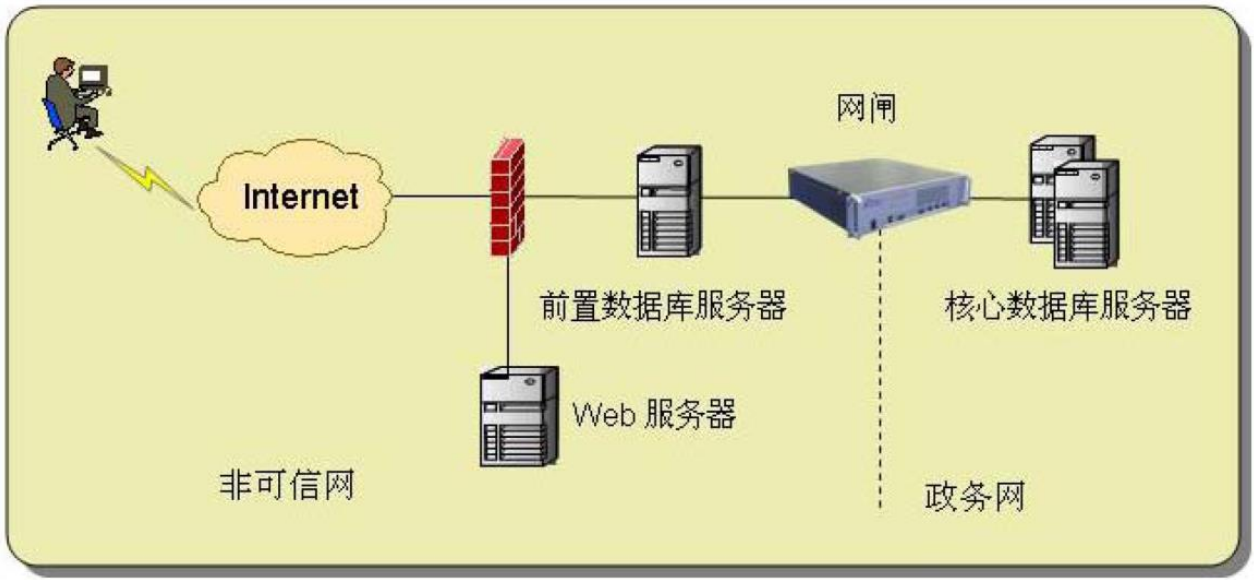

格式化数据块
数据格式化
内容检查
数据提取
协议检查
访问控制
会话终结
可信网络
隔离交换模块
格式化数据块
格式化数据块
数据格式化
内容检查
数据提取
协议检查
访问控制
会话终结
不可信网络

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。

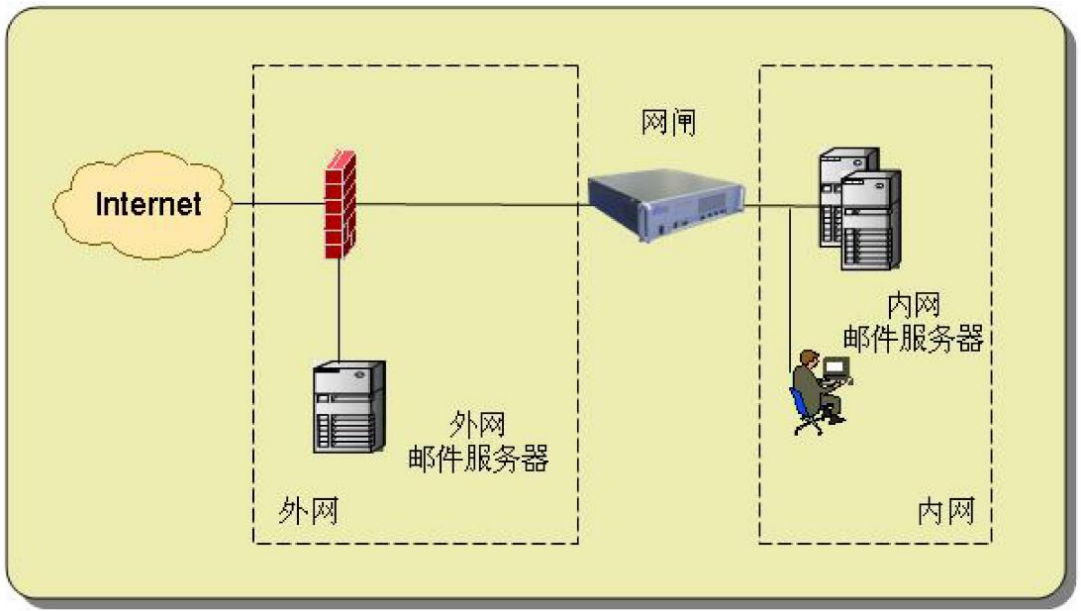
网闸应用例

数据库同步



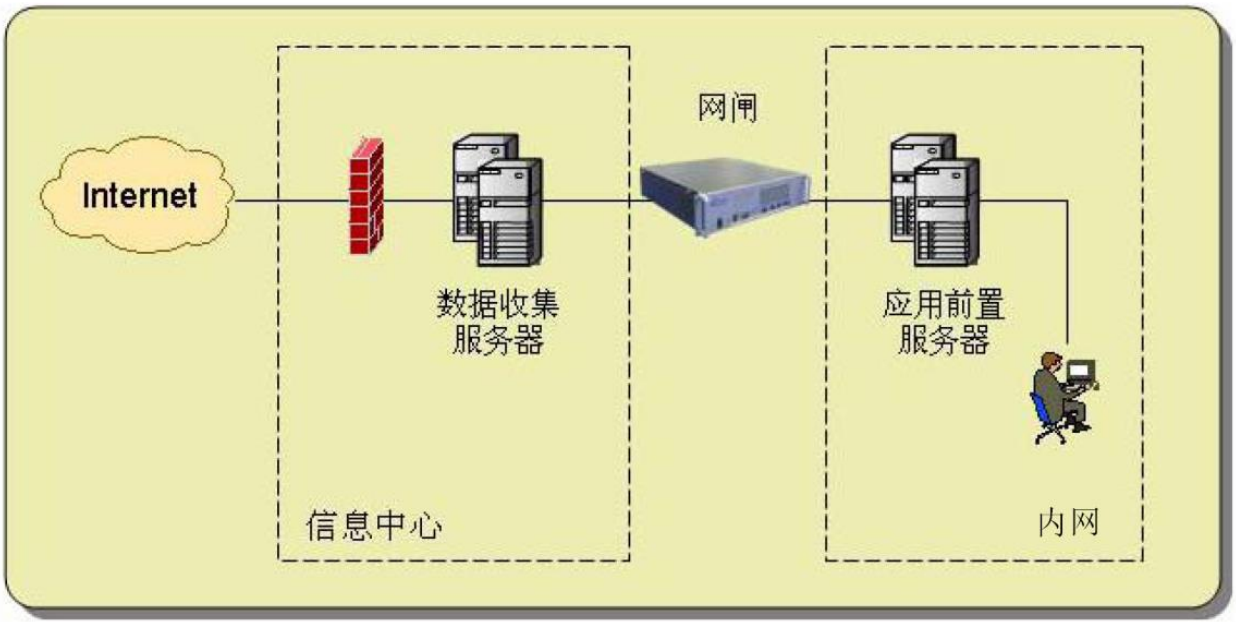
网闸应用例

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
  - 口 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?