DBAplus

大数据与安全-长沙站

人社业务系统安全防护实践

敬勇

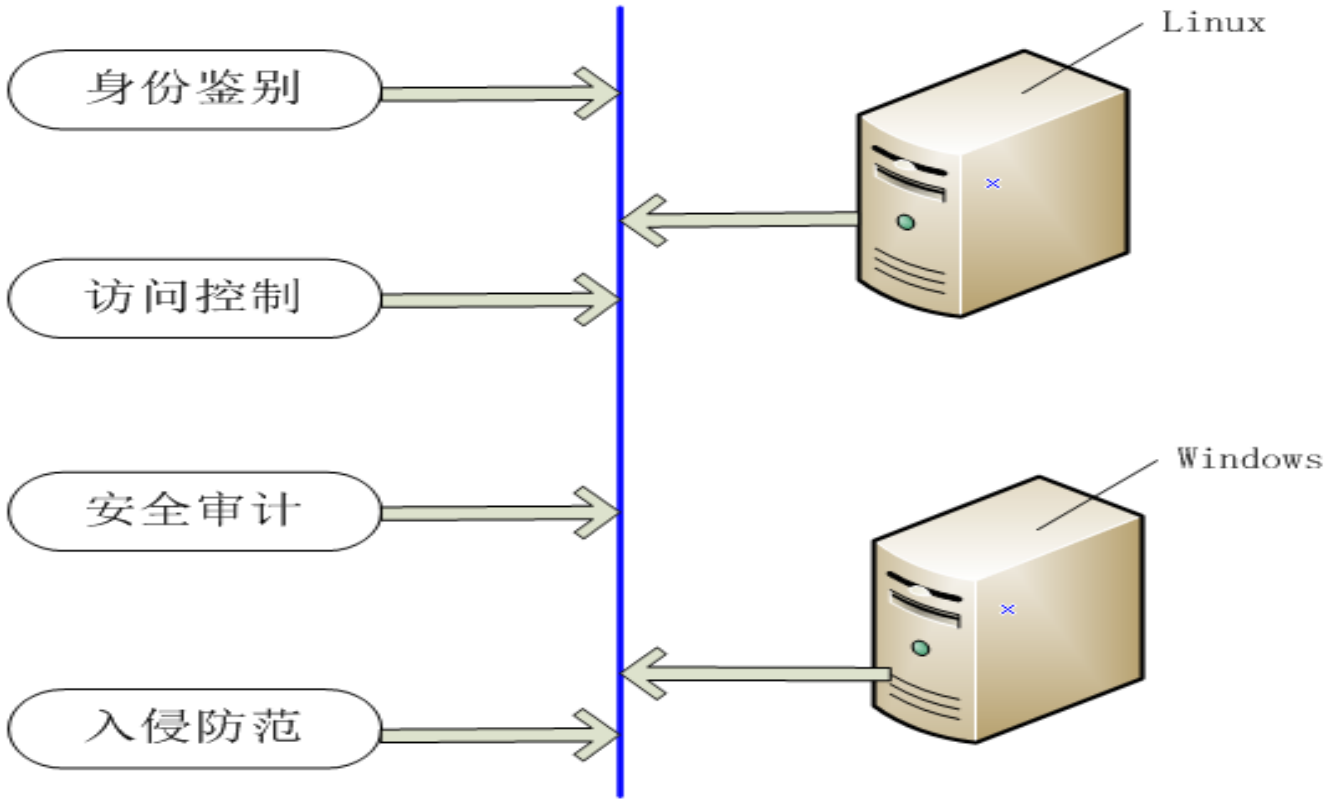
- Eric0435,个人网站 http://www.jydba.net/
- ACOUG核心会员
- Oracle Young Expert
- 系统架构师(高级工程师)
- DBA Plus社群联合发起人
- 湖南省政府采购评审专家
- 常德市信息化咨询委会员委员

中国社会保险
CHINA SOCIAL INSURANCE

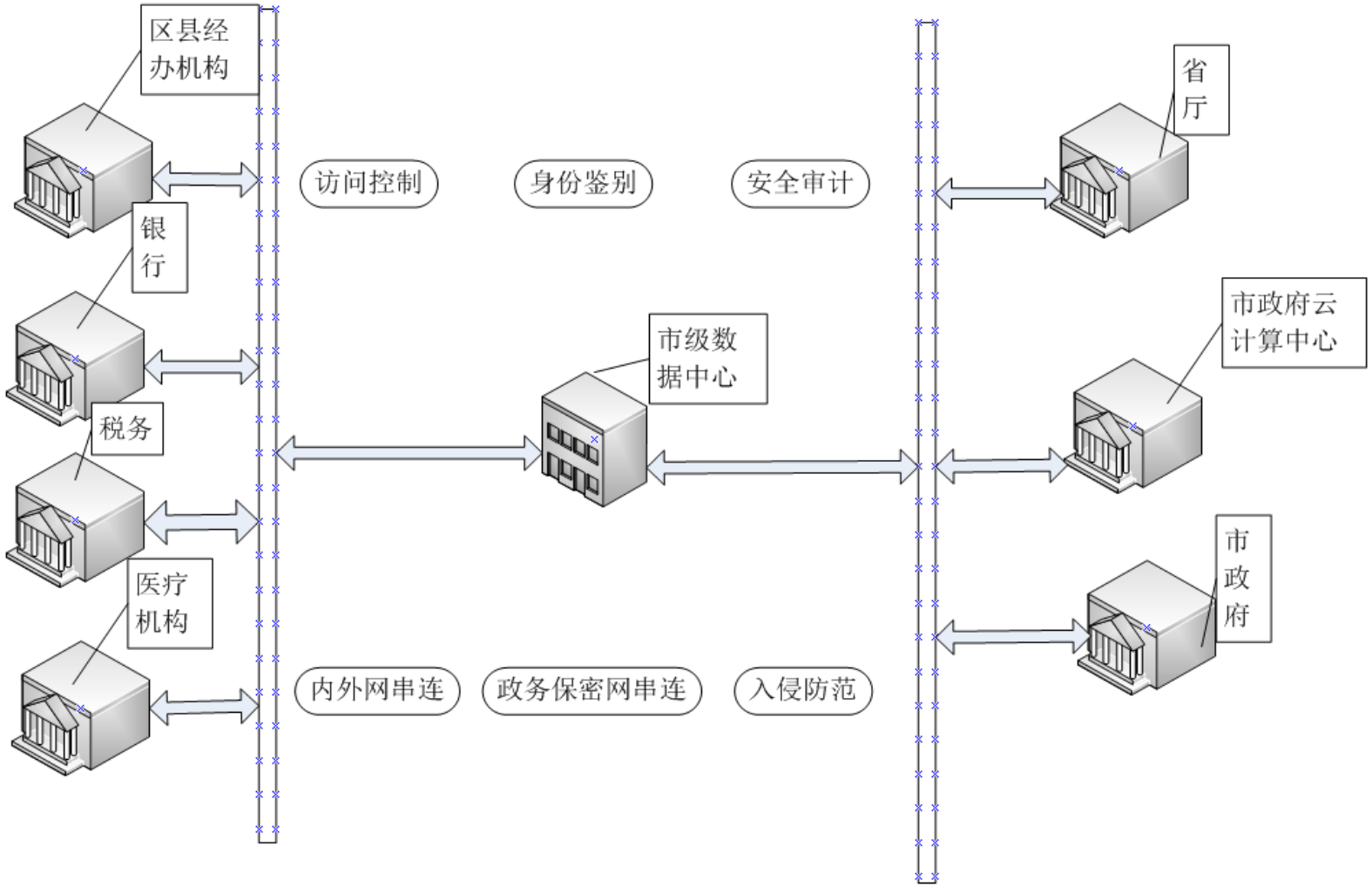
目录

- 面临的问题

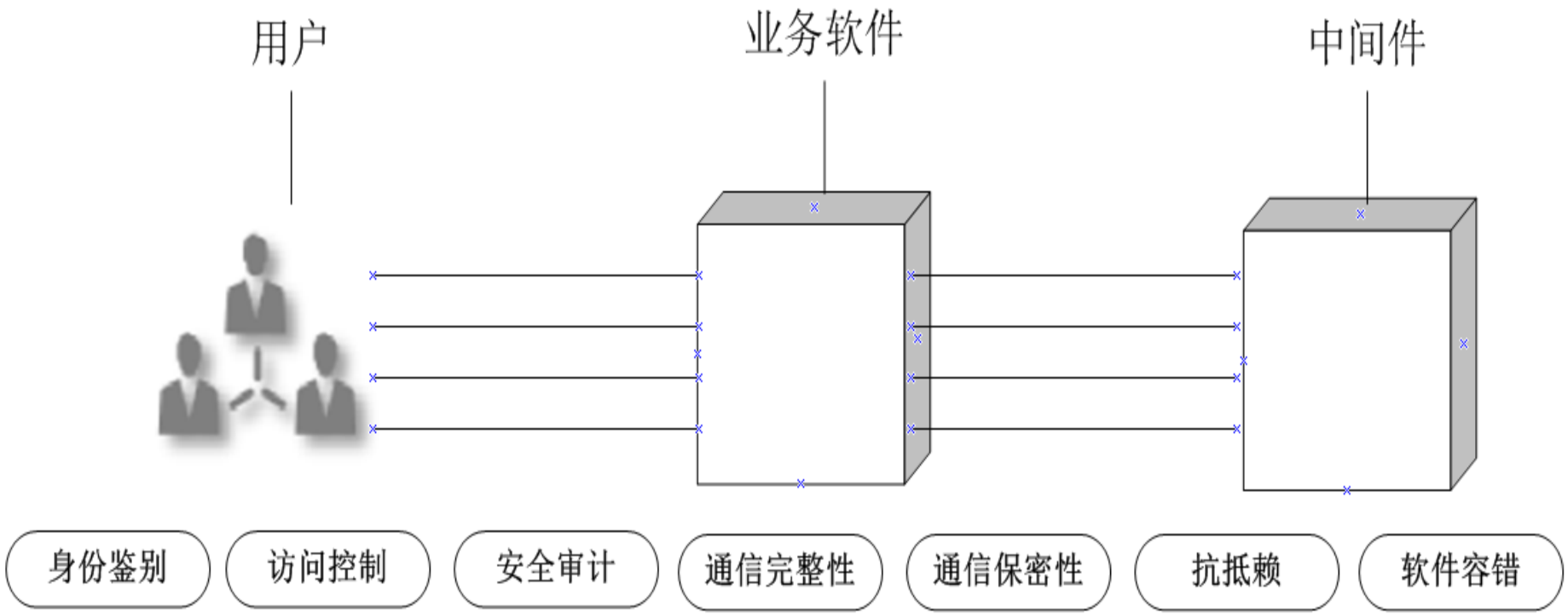
操作系统运行状况



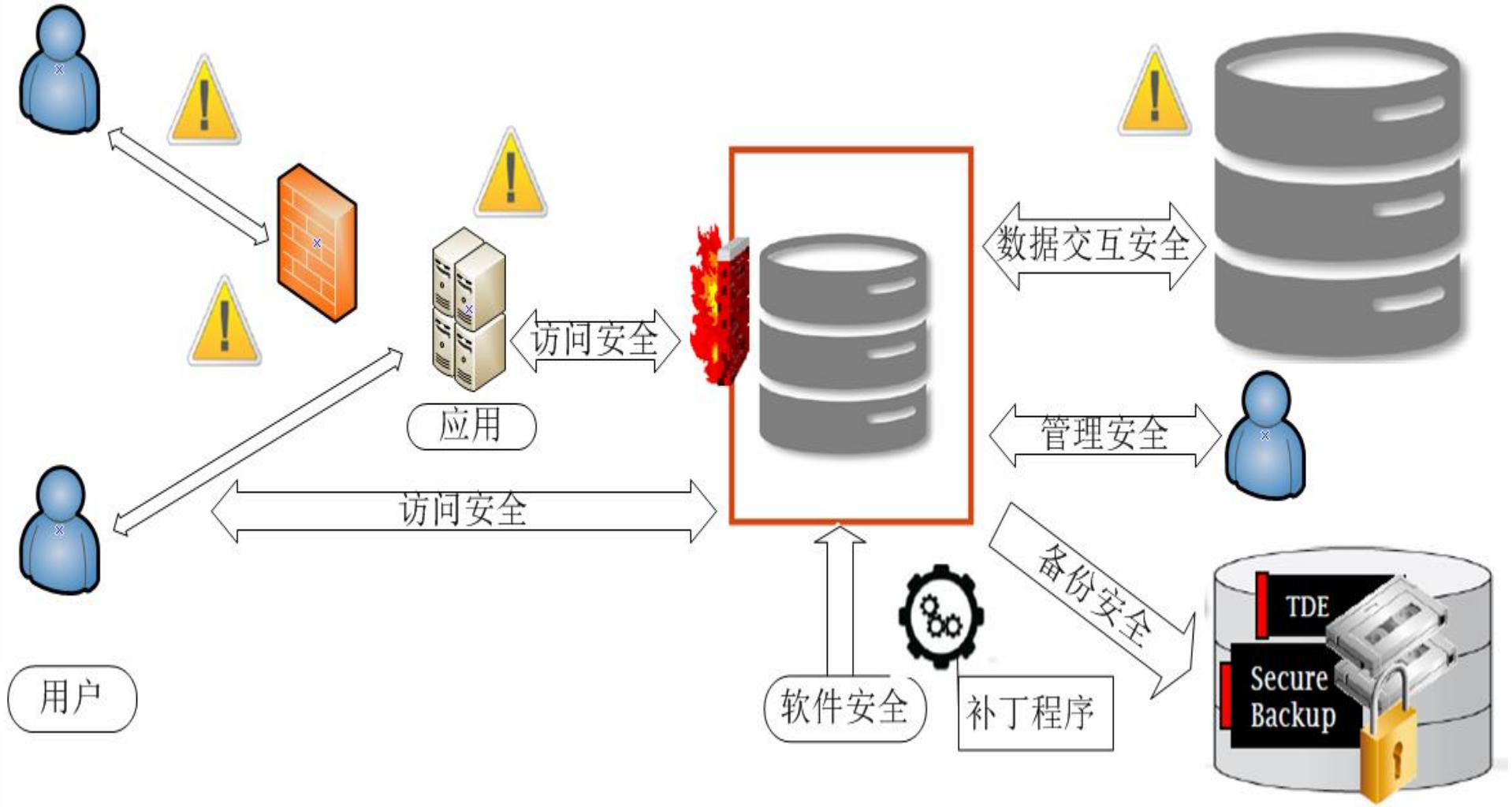
网络运行状况


区县经办机构
银行
税务
医疗机构
访问控制
身份鉴别
安全审计
市级数据中心
省厅
市政府云计算中心
市政府
内外网串连
政务保密网串连
入侵防范

软件安全现状



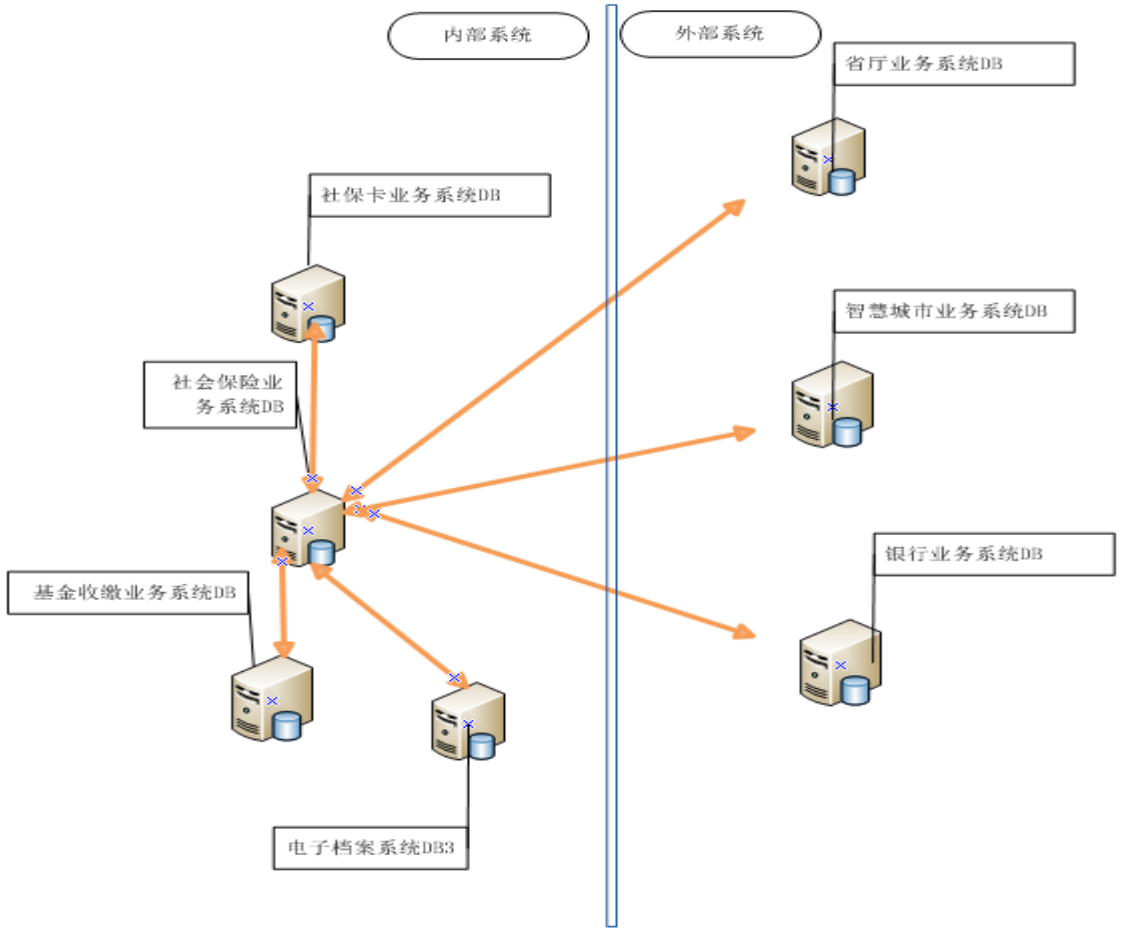
数据库安全状况



错综复杂的DB LINK

DBAplus

- 内部核心系统之间的DB Link
- 内部系统与外部系统之间的DB Link。



错综复杂的DB LINK

DBAplus

- 内部系统与外部系统之间的DB Link。

➢外部系统-> 内部系统(数据请求）= 性能、稳定

例如:SQL语句遗忘rollback或commit语句

➢DB Link -> 内部系统(合法性）= 数据泄露

例如:无法知晓访问者的身份

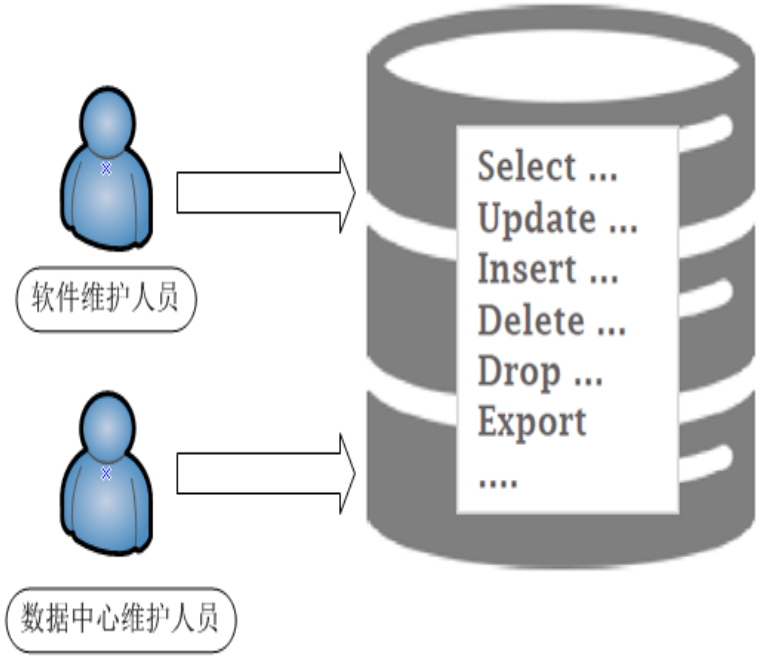
➢DB Link -> BUG= 稳定隐患

- 业务需求的变化，DB Link将变得越来越复杂，数据流向将很难梳理

高风险的数据维护操作

DBAplus

- 数据中心维护人员查询，修改权限
  - ➢查询，修改权限操作缺乏审计
  - ➢通过工具可以直接将查询到的数据导出
- 软件维护人员执行批量更新,DML，DDL等操作
  - ➢DML，DDL操作存在误操作的风险
  - ➢对误操作缺乏快速恢复的手段
  - ➢高风险的DML，DDL操作缺乏完整的审核流程
- 由于不同业务软件由不同软件厂家所维护，维护人员多不好管控
- 数据中心人员一人多职，权限难以分配



操作系统安全管控

DBAplus

- 身份鉴别
  - 关闭telnet,ftp等端口，使用ssh协议
  - 统一使用堡垒机登录

- 访问控制
  - 按用户职责分配相应服务器的使用权限

- 安全审计
  - 所有服务器启用安全日志审计服务

- 入侵防护
  - 启用操作系统软件防火墙与硬件防火墙设置访问控制列表
  - 使用正版防病毒软件并定期更新病毒库
  - 使用入侵检查设备
  - 使用复杂口令并每个季度更改一次

网络安全管控

DBAplus

- 身份鉴别
  - 启用准入系统，入网计算机唯一标识

- 访问控制
  - 使用准入系统进行访问控制
  - 使用准入系统与网闸将内外网，政务网与保密网进行隔离

- 安全审计
  - 所有网络服务器启用安全日志审计服务

- 入侵防护
  - 启用操作系统软件防火墙与硬件防火墙设置访问控制列表
  - 使用入侵检查设备
  - 使用复杂口令并每个季度更改一次

软件安全管控

DBAplus

- 身份鉴别
  - 使用CA证书与口令进行登录认证

- 访问控制
  - 使用准入系统与硬件防火墙进行访问控制

- 安全审计
  - 所有应用服务器启用安全日志审计服务

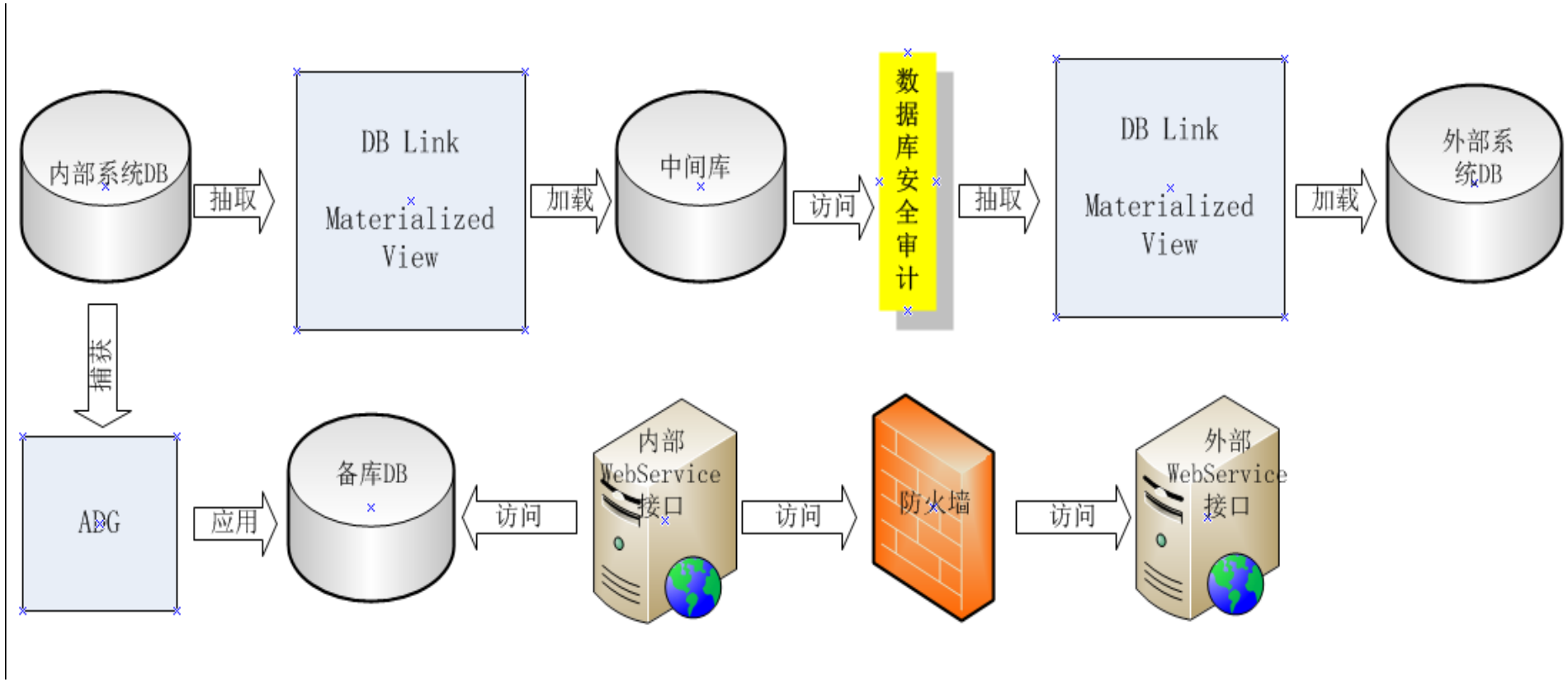
- 通信保密与完整性
  - 使用SSL协议

- 安全检测
  - 定期进行渗透测试

- 抗抵赖
  - CA证书

- 核心数据交互管控

数据交互使用DB Link与WebService



DB Link隔离策略

- 内部系统与外部系统隔离
- 根据数据范围，抽取时间，用途，统一制定抽取任务计划
- 按需抽取，定期清理，数据容量与数据副本最小化
- 使用中间库有效保存数据安全

WebService数据交互

- 跨平台的可操作性,可以让异构的程序相互访问
- 功能复用
- 安全的通信

- 数据运维管控

数据运维管控

DBAplus

- 使用统一的数据运维管理平台
- 最小化数据操作权限
- 执行数据变更审核流程
- 启用数据库操作日志审计平台
- 使用双副本备库dataguard，一份使用active dataguard实时同步，一份使用实时传输日志，延时一周同步。

DBAplus

www.dbaplus.cn

THANK YOU !