校园网络安全分层防护策略的探讨

中国石油大学（华东）

田爱宝

主要内容

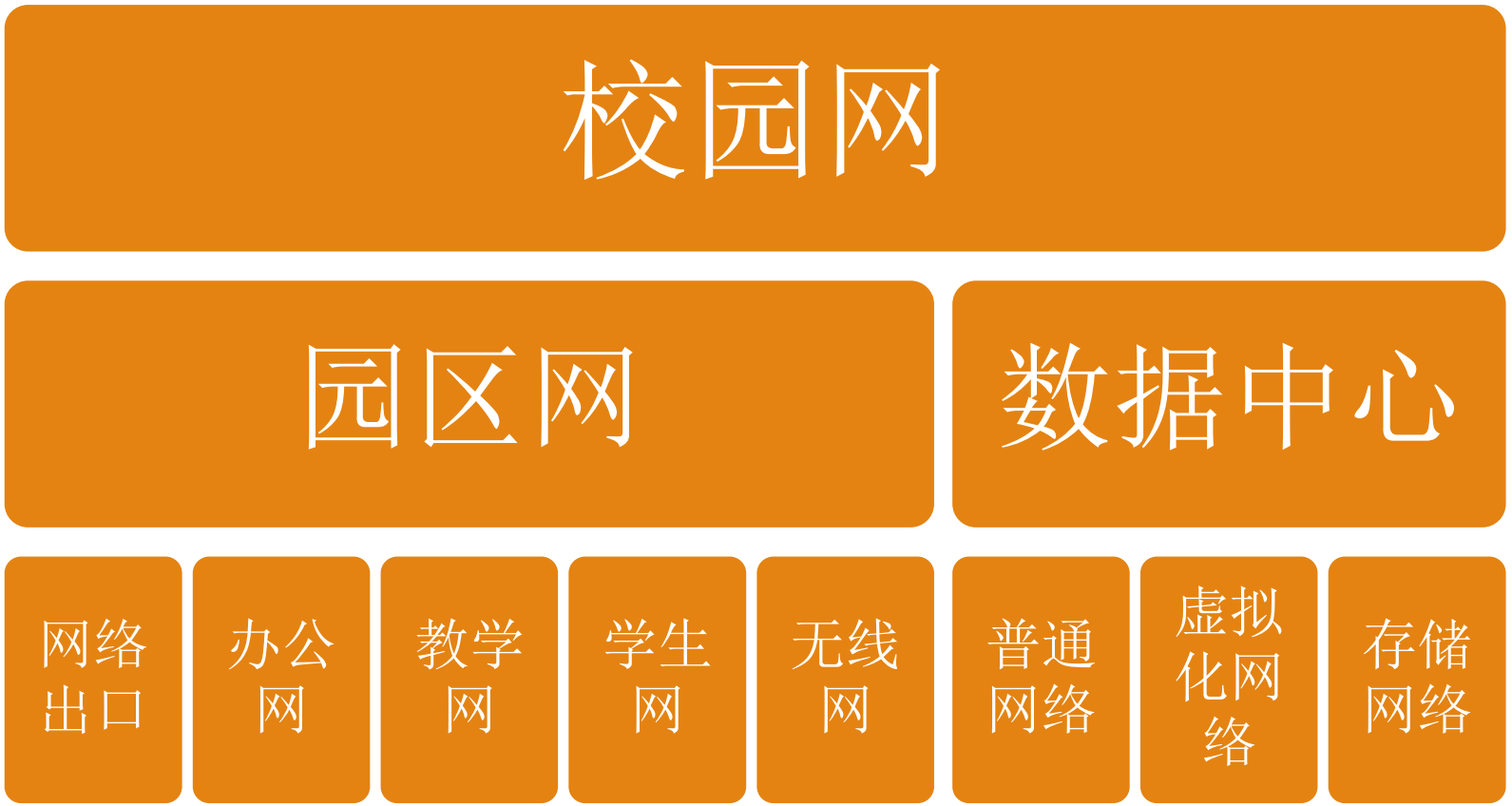
- 校园网络特点与安全分析
- 网络安全防护策略
- 网络安全管理策略

校园网络的特点与安全分析

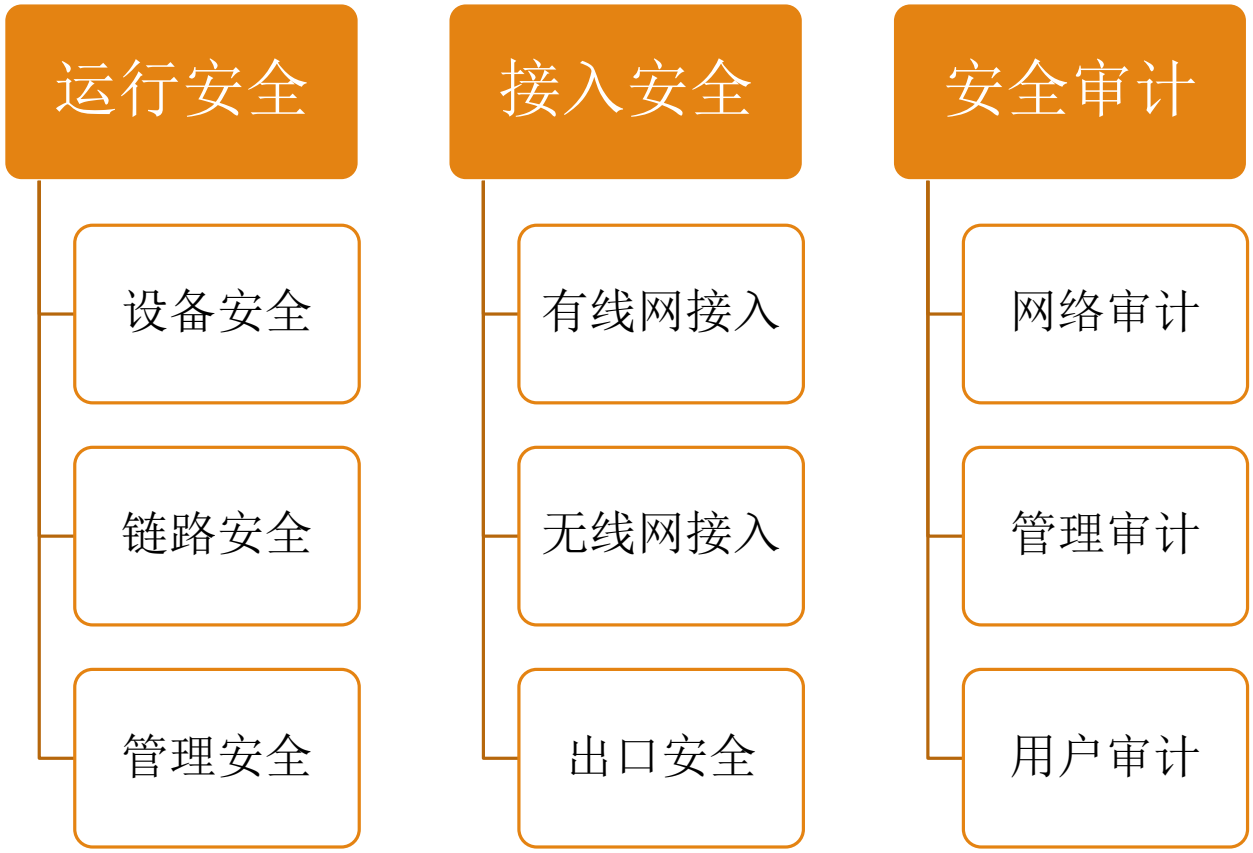
校园网络特点

- 规模大
- 用户多
- 需求多
- 开放
- 业务复杂
- 流量大
- 功能全

校园网络结构



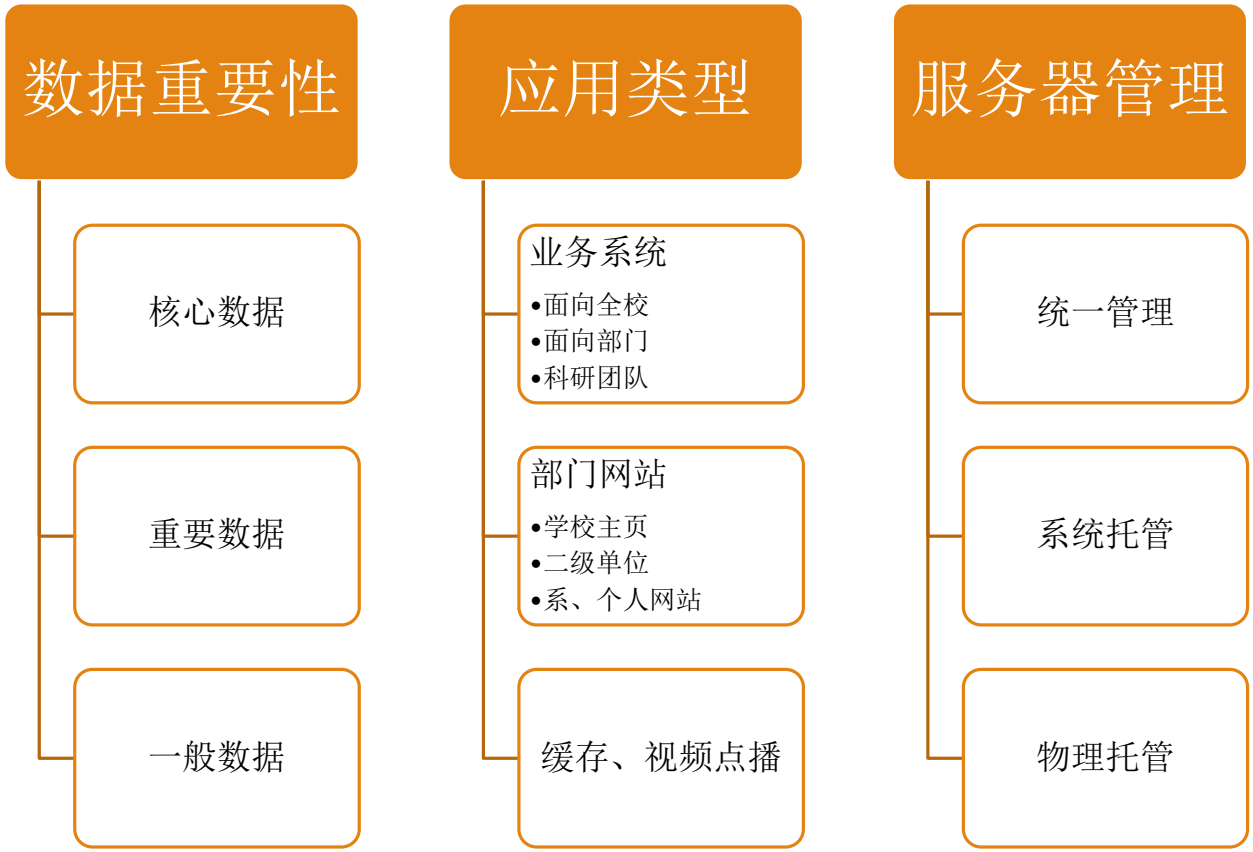
园区网络安全


运行安全
设备安全
链路安全
管理安全
接入安全
有线网接入
无线网接入
出口安全
安全审计
网络审计
管理审计
用户审计

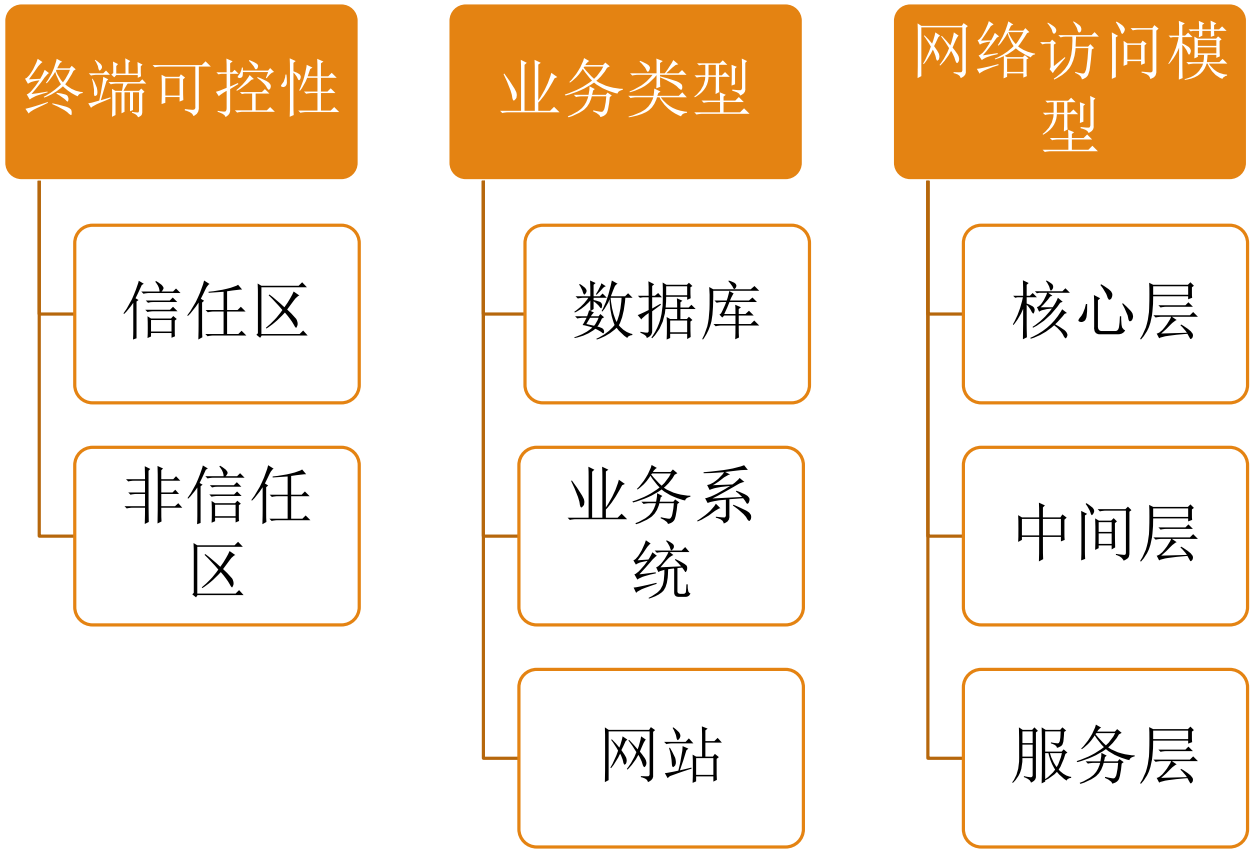
数据中心安全

- 数据重要性
  - 核心数据
  - 重要数据
  - 一般数据
- 安全机制
  - 安全检测
  - 安全策略
  - 冗余备份
  - 日志审计

数据中心分类


数据重要性
核心数据
重要数据
一般数据
应用类型
业务系统
•面向全校
•面向部门
•科研团队
部门网站
•学校主页
•二级单位
•系、个人网站
缓存、视频点播
服务器管理
统一管理
系统托管
物理托管

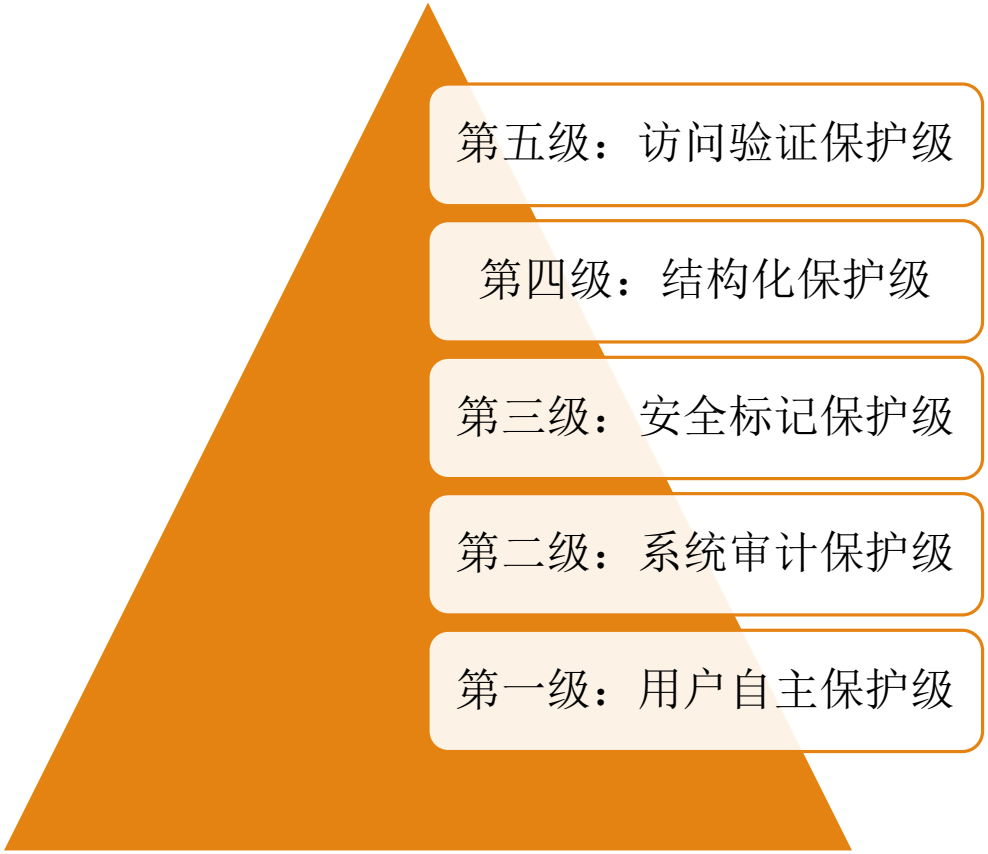
数据中心分类



安全分层

	数据中心		园区网
	信任区	非信任区	
重点防护	核心数据 全校性业务系统 学校主页	核心数据 全校性业务系统 学校主页	网络运行安全
重要防护	部门网站 部门业务系统 重点科研团队系统	部门网站 部门业务系统 重点科研团队系统	网络接入安全
一般防护	缓存、一般应用	个人系统、一般应用	用户网络终端

等级保护



网络安全防护策略

园区网IP地址分配策略

区域	IP地址	分配类型
办公区	私网	动态+静态
教学区	私网	静态
学生宿舍区	公网	动态
无线网	私网	动态
数据中心	公网	静态

网络运行安全

设备冗余	链路冗余	路由冗余	远程管理控制
核心层	核心层	核心层	telnet
汇聚层	汇聚层	汇聚层	Consle
			密码

园区网用户接入安全


用户准入认证
• PPPoE
• IPoE
• 802.1x
用户二层隔离
• QinQ
• 端口隔离
• SuperVLAN
用户帐号管理
• 注册用户
• 访客
安全教育
• 用户安全意识
• 用户安全技术

网络出口

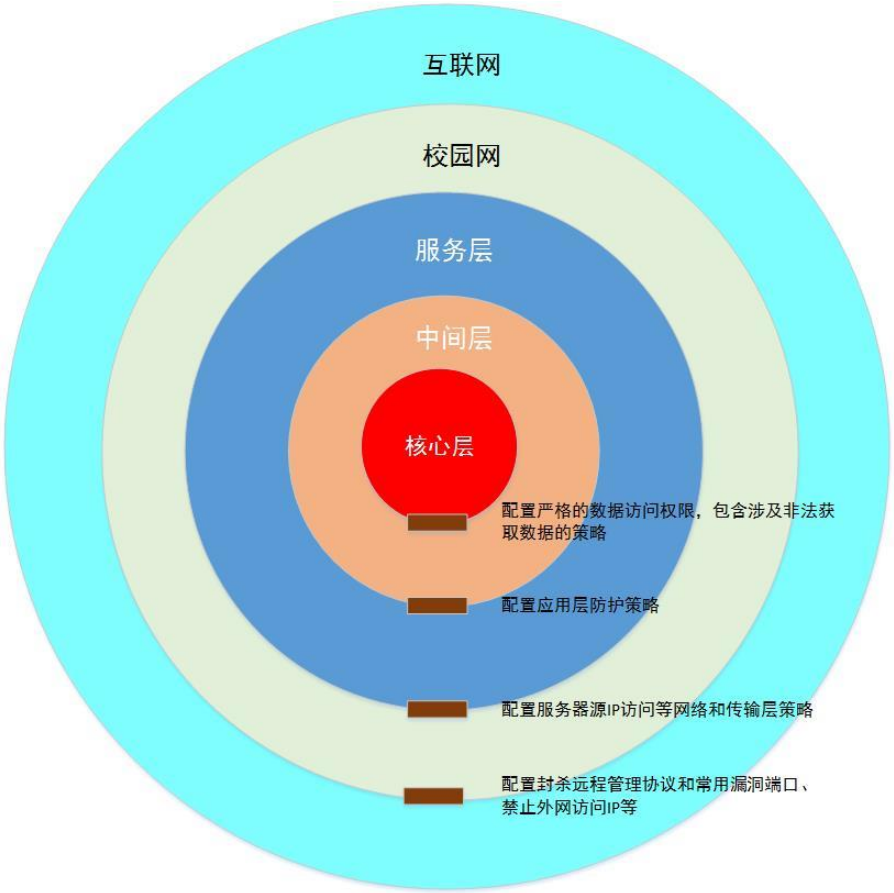
出入访问控制

- 禁止远程登录
- 禁止常见病毒端口
- 利用黑名单系统

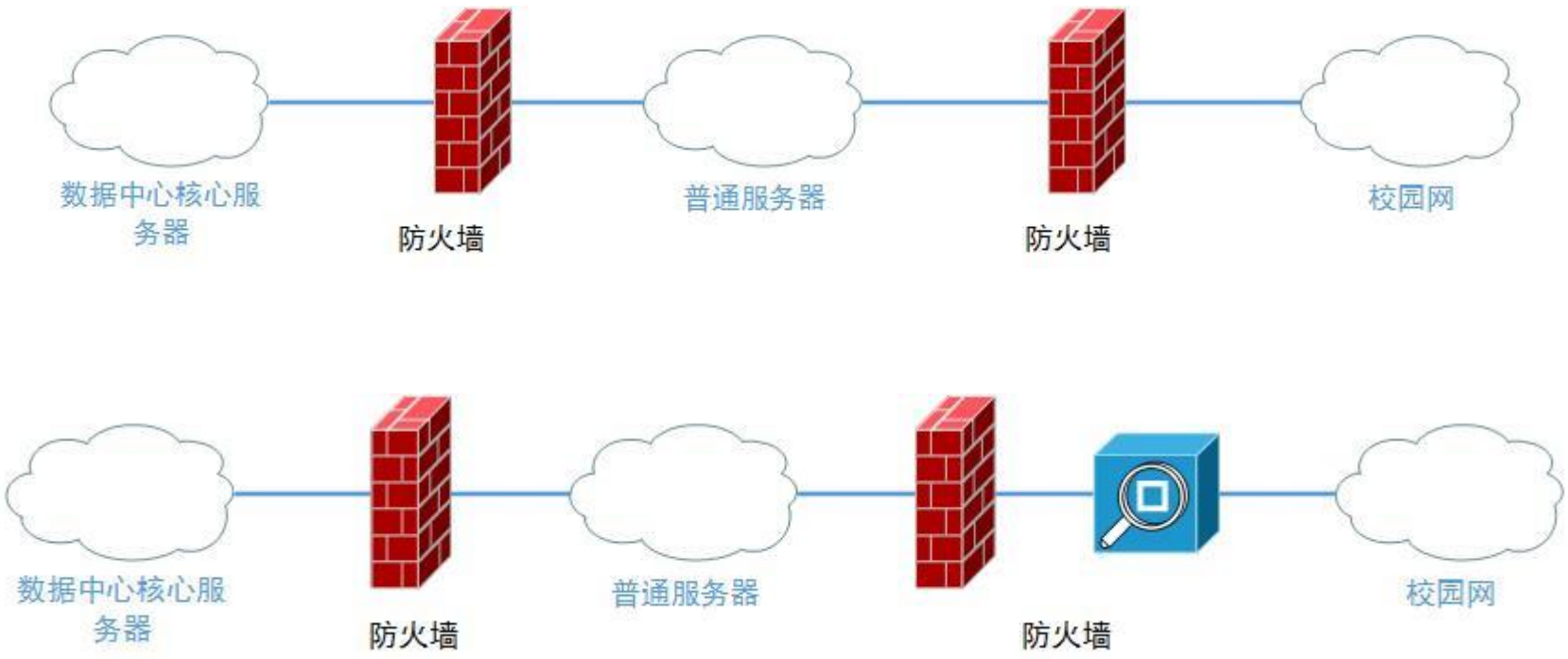
网络安全审计

- NAT日志
- 用户访问日志
- 舆情监控

数据中心分层防护

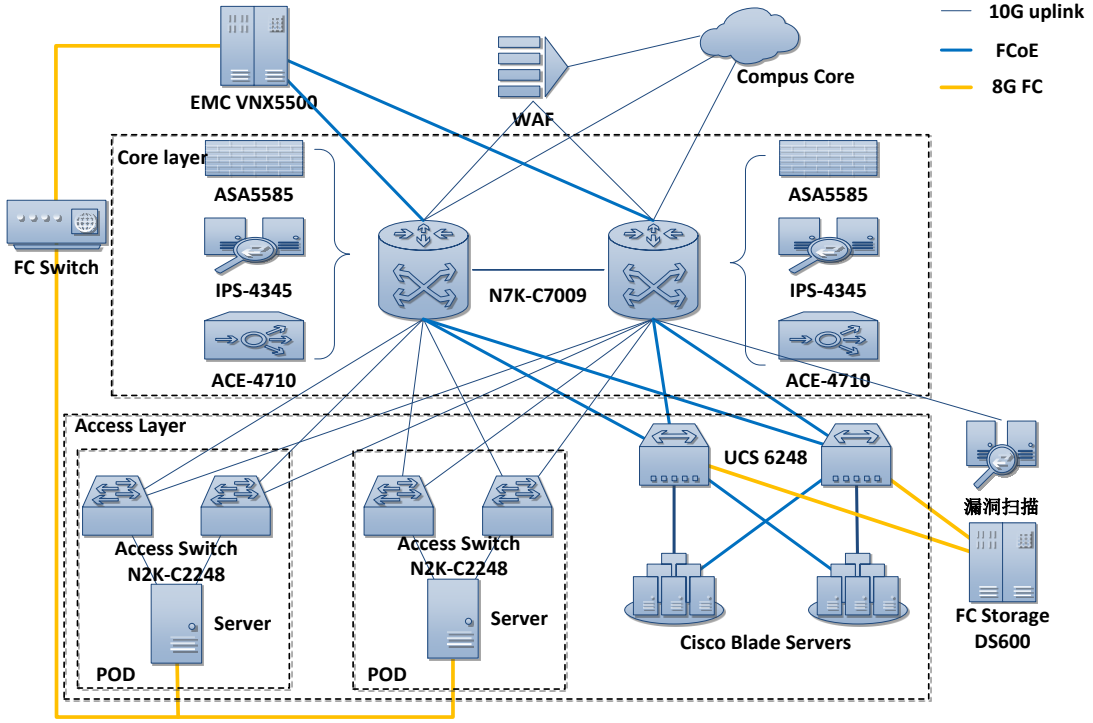

互联网
校园网
服务层
中间层
核心层
配置严格的数据访问权限，包含涉及非法获取数据的策略
配置应用层防护策略
配置服务器源IP访问等网络和传输层策略
配置封杀远程管理协议和常用漏洞端口、禁止外网访问IP等

数据中心防护逻辑

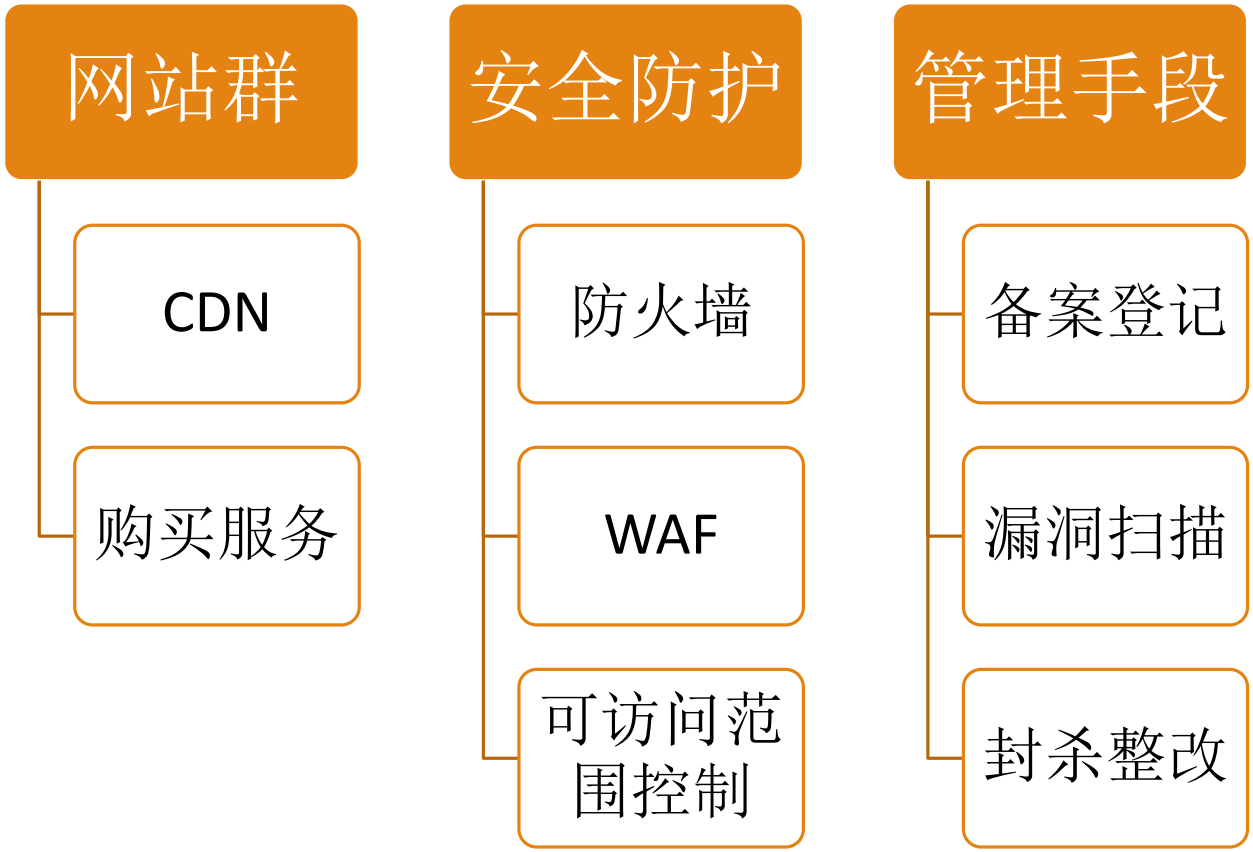


数据中心网络拓扑


防火墙
入侵检测
WAF
Web漏洞扫描


10G uplink
FCoE
8G FC
EMC VNX5500
WAF
Compus Core
Core layer
ASA5585
ASA5585
FC Switch
IPS-4345
IPS-4345
N7K-C7009
ACE-4710
ACE-4710
Access Layer
UCS 6248
漏洞扫描
Access Switch
N2K-C2248
Access Switch
N2K-C2248
Server
Server
POD
POD
Cisco Blade Servers
FC Storage
DS600

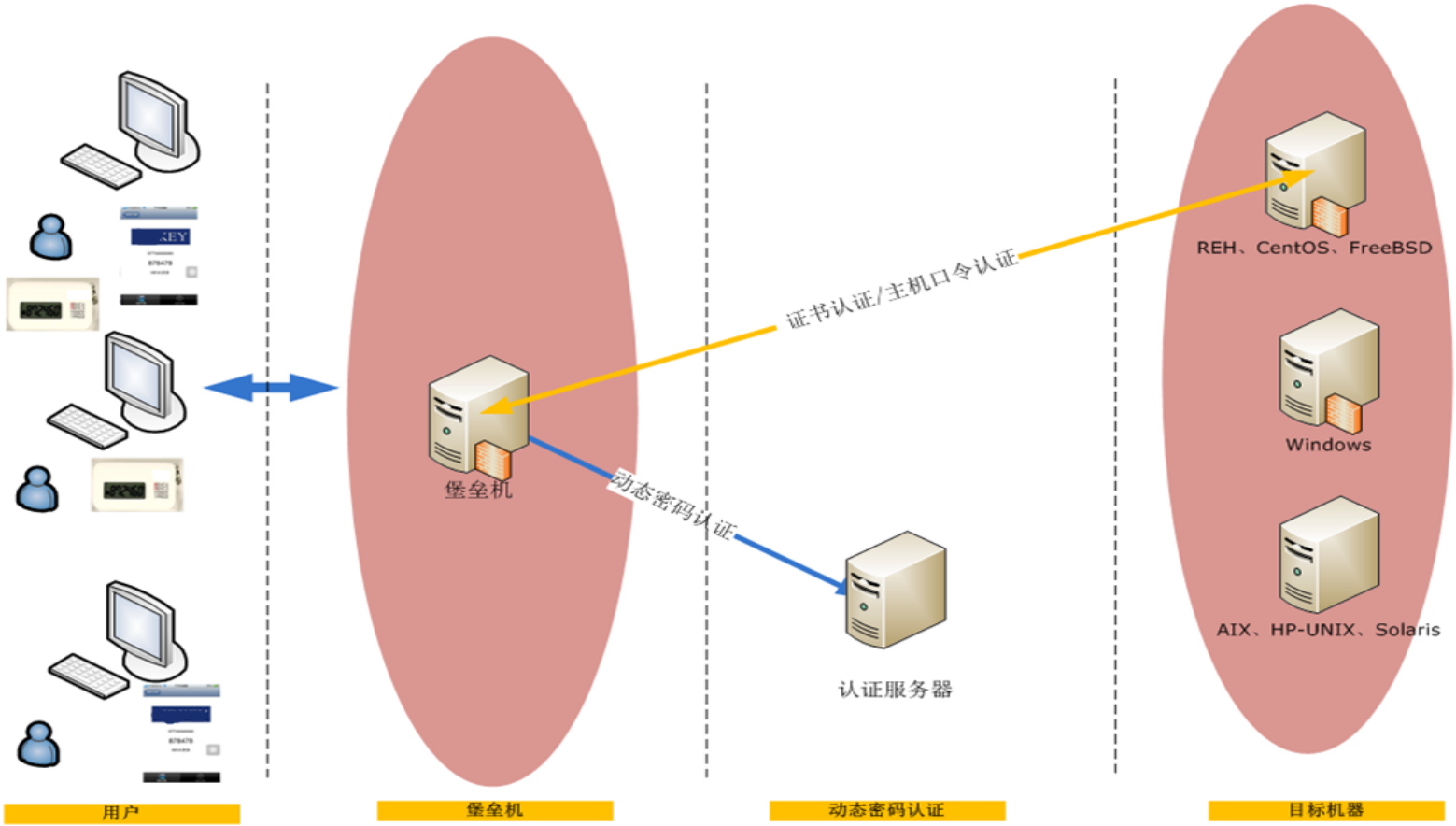
网站防护



应用系统防护

- 做好防火墙安全策略
- 严格控制访问范围
- 安全责任落实到人
- 加强远程访问管理

远程管理策略


证书认证/主机口令认证
动态密码认证
堡垒机
认证服务器
REH、CentOS、FreeBSD
Windows
AIX、HP-UNIX、Solaris
用户
堡垒机
动态密码认证
目标机器

网络安全管理策略

安全三“心”

改变传统安全认识

- 管理与技术同等重要
- 不同类型的应用需要不同的安全设备与策略
- 网络端永远解决不了终端的安全问题
- 需要让网络使用者知道安全的重要性
- 有了安全设备并不代表就安全

谢谢！