**达州技师学院校园网络升级改造和无线网络建设**

**说明书**

目 录

[第一章 本单位已建信息化项目建设现状 4](#_Toc146013304)

[第二章 本单位已建系统数据共享及迁移上云情况 6](#_Toc146013305)

[第三章 项目建设依据 7](#_Toc146013306)

[3.1 方案设计依据 7](#_Toc146013307)

[第四章 项目建设内容 9](#_Toc146013308)

[4.1 双域专网方案 9](#_Toc146013309)

[4.1.1 基于5G的远程办公需求 9](#_Toc146013310)

[4.1.2 解决方案优势 9](#_Toc146013311)

[4.1.3 网络建设设计方案（运营商侧） 11](#_Toc146013312)

[4.1.4 5G校园专网融合认证方案（学校侧） 24](#_Toc146013313)

[4.2 网络安全技术网络安全等级保护需求 35](#_Toc146013314)

[4.2.1 安全技术建设需求 36](#_Toc146013315)

[4.2.2 安全管理建设需求 42](#_Toc146013316)

[4.2.3 数据中心扩容建设需求 43](#_Toc146013317)

[4.2.4 方案设计原则 43](#_Toc146013318)

[4.2.5 方案设计思路 45](#_Toc146013319)

[4.2.6 整体建设框架 45](#_Toc146013320)

[4.2.7 安全技术差距分析 46](#_Toc146013321)

[4.2.8 安全计算环境 47](#_Toc146013322)

[4.2.9 安全区域边界 47](#_Toc146013323)

[4.2.10 安全网络通信 48](#_Toc146013324)

[4.2.11 安全管理中心 48](#_Toc146013325)

[4.3 技术方案及实施 48](#_Toc146013326)

[4.3.1 物理与环境安全保障 48](#_Toc146013327)

[4.3.2 计算环境安全设计 52](#_Toc146013328)

[**部署设备：备份一体机** 55](#_Toc146013329)

[4.3.3 区域边界安全保护设计 55](#_Toc146013330)

[4.3.4 通信网络安全保护设计 58](#_Toc146013331)

[4.3.5 安全管理中心设计 60](#_Toc146013332)

[4.4 安全管理方案设计 63](#_Toc146013333)

[4.4.1 安全策略与制度管理 63](#_Toc146013334)

[4.4.2 安全管理机构和人员 64](#_Toc146013335)

[4.4.3 安全建设管理 64](#_Toc146013336)

[4.4.4 安全运维管理 65](#_Toc146013337)

[4.4.5 安全管理制度汇总 66](#_Toc146013338)

[第五章 超融合数据中心扩容建设 67](#_Toc146013339)

[5.1.1 方案建设思路 67](#_Toc146013340)

[5.1.2 方案拓扑架构 70](#_Toc146013341)

[第六章 网络建设与运维运维技能赛项建设 71](#_Toc146013342)

[一、建设背景 71](#_Toc146013343)

[二、建设需求 71](#_Toc146013344)

[**（一）竞赛主要内容** 71](#_Toc146013345)

[**（二）重点考查技能** 71](#_Toc146013346)

# 本单位已建信息化项目建设现状

达州技师学院成立于2019年，是经四川省人民政府批准，在四川省达州市高级技工学校基础上，融合达州市水电学校、达州市经济贸易学校，三校合一的全日制技工教育和社会职业技能培训的工科类公办学校。学院实施以技师（预备技师）、高级技工、中级技工为主要培养方向的全日制技工教育和社会职业技能培训。

达州技师学院建设的智慧校园系列软硬件业务基本实现教育信息化的建设，但目前移动办公网络无法满足日常办公、教学系统运行，需建设双域专网移动网络，保障智慧校园系列软件无缝移动办公、教学，到达省级示范校建设要求。近年来，教育行业网络安全事故频频发生。

* 2016年，黑客入侵内蒙古十几所学校网站，大肆篡改了计算机及英语等级考试成绩数据，83名学生的考试成绩“被及格”，黑客还伪造等级证书，通过变卖的方式获取利益。
* 2018年高考成绩公布日，多省招生考试院官方网站遭到网络攻击，其中黑龙江省招生考试院长达2小时无法访问，致使数十万考生查不到自己高考成绩。
* 2018年，湖北、山东、黑龙江、河南等省份多所重点大学的官方网站被监测到木马，多为挖矿程序，严重影响运行速度，其中不乏985、211大学。
* 2018年8月，浙江省中小学生学籍信息管理类系统被黑客入侵，泄露学生学籍信息1000万条，除了文字数据，售卖的学籍数据里还提供有照片链接，在100G左右。

大量案例表明，黑客擅于利用恶意篡改、代码植入、DDoS大流量攻击、爬虫等方式，对高考查分网站、志愿填报网站、大学官网、在线教育网站等进行攻击，教育行业面临严峻安全挑战。

安全值发布的《2017年教育行业网络安全报告》显示，重点高校面对的威胁相对最严重，行业发现605个CVE安全漏洞，42%机构遭受到总计166,997次DDOS拒绝服务攻击，其中重点高校成为了黑客的主要目标。

在教育信息化发展的趋势下，云计算、大数据、物联网等技术在智慧校园建设中逐渐普及，也带访问、app使用量呈快速增长，同时产生更多的攻击。为此国家在2019年5月13号，发布等保2.0的三个关键标准GB/T22239-2019《信息安全技术 网络安全等级保护基本要求》，GB/T25070-2019《信息安全技术 网络安全等级保护安全设计要求》和GB/T28448-2019《信息安全技术 网络安全等级保护测评要求》发布并将于2019年12月1号实施，标志着我们正式进入等保2.0防护建设阶段，新的要准要求我们从新的技术体系，管理体系来审视过去的安全建设工作并将新技术、新体系应用到未来的网络安全建设中去。

# 本单位已建系统数据共享及迁移上云情况

目前达州技师学院的数字化校园建设具有一定规模，未来系统整合，数据共享是必然的趋势，本次项目建设将于现有平台系统的对接和级联，将融入达州技师学院内部系统整合对接，支持将可共享的数据，经领导批准在确保数据信息安全的前提下，支持提供给其他需要该信息数据的市级部门(单位)无偿使用，信息数据的共享交换，有效避免重复采集，重复建设。本项目建设软件及硬件设备将按照国家政策要求及技术规范保障数据共享开放，保障学院能共享的信息数据能对接达州市“城市大脑”、达州市城市公共信息服务平台。

# 项目建设依据

## 方案设计依据

自1994年《中华人民共和国计算机信息系统安全保护条例》第一次提出信息系统等级保护的概念以来，安全“等保”这一概念就备受国家关注，相关政策条文也不断更新，等级保护建设的目标、要求、设计框架、测评等整个流程逐渐完善，形成清晰、规范的体系架构。

2003年9月中办国办颁发《关于加强信息安全保障工作的意见》中办发[2003]27号，重点强调保护基础信息网络和关系国家安全、经济命脉、社会稳定等方面的重要信息系统，抓紧建立信息安全等级保护制度，制定信息安全等级保护的管理办法和技术指南。

2004年11月四部委会签《关于信息安全等级保护工作的实施意见》公通字[2004]66号强调信息安全等级保护制度是国家在国民经济和社会信息化的发展过程中，提高信息安全保障能力和水平，维护国家安全、社会稳定和公共利益，保障和促进信息化建设健康发展的一项基本制度。

2015年教育部在《教育行业信息系统安全等级保护定级工作指南》中也针对高校各业务系统的等级保护要求提出了明确的指导，要求各相关院校系统安全防护能力必须达到以上要求。

2016年11月十二届全国人大第二十一次三次审议表决通过了网络安全法，《中华人民共和国网络安全法》这部我国网络领域的基础性法律于2017年6月1日正式实施，正式的将网络等级保护的建设上升到法律的层面，其中第二十一条规定：国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改。

随着网络安全等级保护建设呼声越来越高，教育信息化安全建设也备受国家的关注。

2019年2月27日，教育部办公厅印发《2019年教育信息化和网络安全工作要点》，强调全面落实党中央国务院对教育领域网络安全和信息化的战略部署。

* 编写《网络空间安全研究生核心课程指南》。加强对有关“双一流”建设高校的指导，继续加强网络空间安全、人工智能相关学科建设。
* 根据落实网络安全等级保护制度的要求，进一步完善相关管理制度和标准规范。持续推进网络安全监测预警通报机制，建立常态化的通用软件安全评估机制；完善网络安全信息通报机制，加强与省级教育行政部门的信息共享，提高安全威胁信息的质量和针对性。
* 全面落实党中央国务院对教育领域网络安全和信息化的战略部署。加强教育部网络安全和信息化领导小组的统筹领导

2019年3月1日，教育部科技司印发《教育部科技司2019年工作要点》，强调加强教育系统网络安全保障能力,坚持教育部网络安全和信息化领导小组的统筹领导，全面落实党委（党组）网络安全责任制，建立覆盖教育系统的常态化监督考核机制。

网络安全等级保护建设备受国家关注，等级保护建设可谓势在必行，在教育行业尤其如此！

# 项目建设内容

## 双域专网方案

### 基于5G的远程办公需求

基于达州技师学院当前网络建设情况，学院提出了基于5G的远程办公需求，具体需求如下：

* 需求1：为达州技师学院建设5G精品网络，通过5G网络能够实现互联网及学院内网同时访问。
* 需求2：为全院近300名教职员工，开通5G双域专网，要求能实现省内外漫游访问学院内网，同时支持回落至4G访问内网。
* 需求3：为全院学生按需开通5G双域专网，要求能实现省内外漫游访问学院内网，同时支持回落至4G访问内网。

### 解决方案优势

依托5G精品网络，提供双域专网方案，解决远程办公VPN连接，内外网WIFI频繁切换，内网下载速度慢等困境，与传统传统WIFI、VPN等连接方式相比，存在如下优势：

**与传统WIFI+VPN方案对比：**

|  |  |  |  |
| --- | --- | --- | --- |
|  | **细项** | **WIFI+VPN方案** | **5G双域网方案** |
| 便捷性 | 网络覆盖 | 存在盲点 | 连续覆盖 |
| 业务质量 | 无QoS保障 | QoS保障 |
| 接入网络（WIFI） | 手动连接 | 无感接入 |
| 网络认证（VPN） | 手动认证 | 无感认证 |
| 维护主体 | 学院自身 | 运营商 |
| 安全性 | 安全性 | 使用公网，安全性相对难保障 | 专用切片，公私流量分流数据安全可靠 |

**① 传统WIFI访问内网**

**使用繁**：需要连接校园WiFI和登录portal手动认证，出校园之后无法访问。

**体验差**：覆盖有死角，高峰期间网络拥塞, AP间干扰严重，切换时延高，存在丢包风险。

**建设难**：WiFI光纤，网络都需要通道室内，穿线布线复杂。

**运维难**：需自建设备管理、连接管理系统，一般院校并无专业的网络运维人员。

**② 传统VPN访问内网**

**体验差：**校园VPN性能和带宽瓶颈，移动终端使用VPN不方便。

**成本高：**占用校园网出口带宽，学校带宽成本持续增加。

**安全低：**园区内访问需绕行Internet，无法确保接入的安全性、隐私性和可管理性。

**③5G双域专网**

**使用易**：原移动用户可不换卡、不换号，直接叠加相关功能套餐即可随时接入内部网络及互联网，无需手动进行操作。

**覆盖广**：拥有全球最大规模的4、5G网络，无线基站数量决定了移动网络覆盖更广更深。可以满足大部分广域网企业业务对无线信号的诉求。

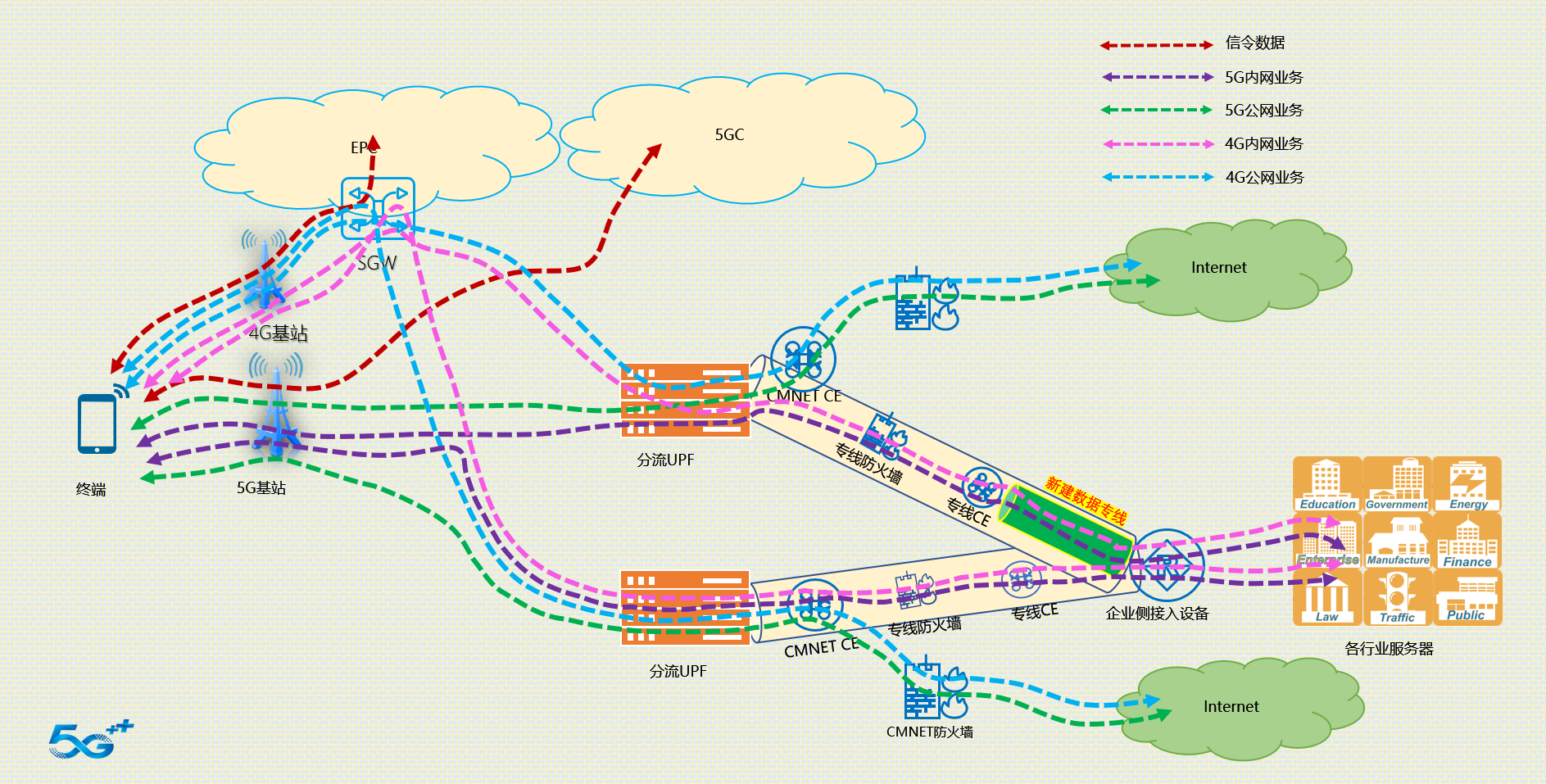
**网络优**：5G网络组网全部采用SA独立组网，无线部分使用独立的NR基站，与原有的LTE基站共址，保证了原4G信号覆盖区域的平稳升级，采用统一空口技术框架，满足多样化的5G场景和差异化的性能指标需求，新型的多址技术，满足高速率和海量物联网连接需求，并且部署大规模天线，满足高效率的需求，NR基站采用超密集组网技术，满足高流量密度需求，基站载波采用高频通信，满足高速率的需求。

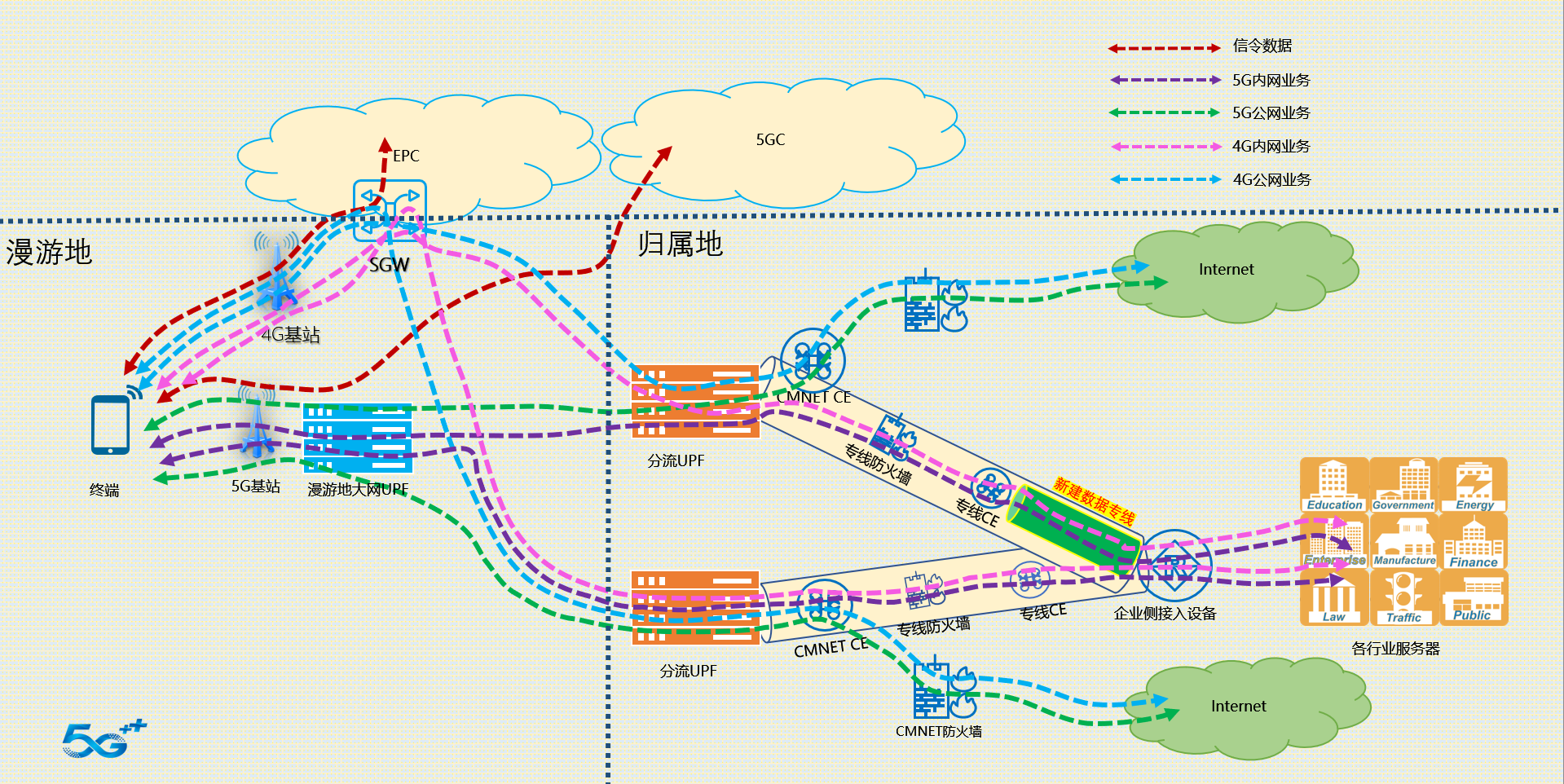
**更安全**：无需登录VPN，内网连接直接再核心网侧进行分流，减少暴露在互联网上的风险。

### 网络建设设计方案（运营商侧）

#### 方案概述

整体解决方案采用专用DNN+目的IP地址分流+数据专线+动态IP+GRE隧道，利用大网无线基站以及共享UPF资源，通过GRE隧道方式打通分流UPF与企业服务器间的数据通道，采用动态IP地址+负荷容灾模式建设。





**本地使用5G场景**

终端访问公网业务时数据通道：终端---5G基站---分流UPF---cmnet ce---cmnet防火墙---Internet公网。

终端访问内网业务时数据通道：终端---5G基站---分流UPF---cmnet ce---专线防火墙---专线CE---企业路由器---企业服务器。

**本地使用4G场景**

终端访问公网业务时数据通道：终端---4G基站---SGW---分流UPF---cmnet ce---cmnet防火墙---Internet公网。

终端访问内网业务时数据通道：终端---4G基站---SGW---分流UPF---cmnet ce---专线防火墙---专线CE---企业路由器---企业服务器。

**5G漫游场景**

终端访问公网业务时数据通道：终端---漫游地5G基站---漫游地大网UPF---归属地分流UPF---归属地cmnet ce---归属地cmnet防火墙---Internet公网。

终端访问内网业务时数据通道：终端---漫游地5G基站---漫游地大网UPF---归属地分流UPF---归属地cmnet ce---归属地专线防火墙---归属地专线CE---企业路由器---企业服务器。

**4G漫游场景**

终端访问公网业务时数据通道：终端---漫游地4G基站---漫游地SGW---归属地分流UPF---归属地cmnet ce---归属地cmnet防火墙---Internet公网。

终端访问内网业务时数据通道：终端---漫游地4G基站---漫游地SGW---归属地分流UPF---归属地cmnet ce---归属地专线防火墙---归属地专线CE---企业路由器---企业服务器。

【方案配置】

（1）两套分流UPF上分别与企业路由器建立一条GRE隧道。

（2）两套分流UPF配置配置园区路由策略，基于目的IP地址路由，将企业提供的收敛IP地址引入隧道。

（3）企业路由器上配置到UE静态路由分别入不同隧道，并针对分流UPF配置相同优先级。

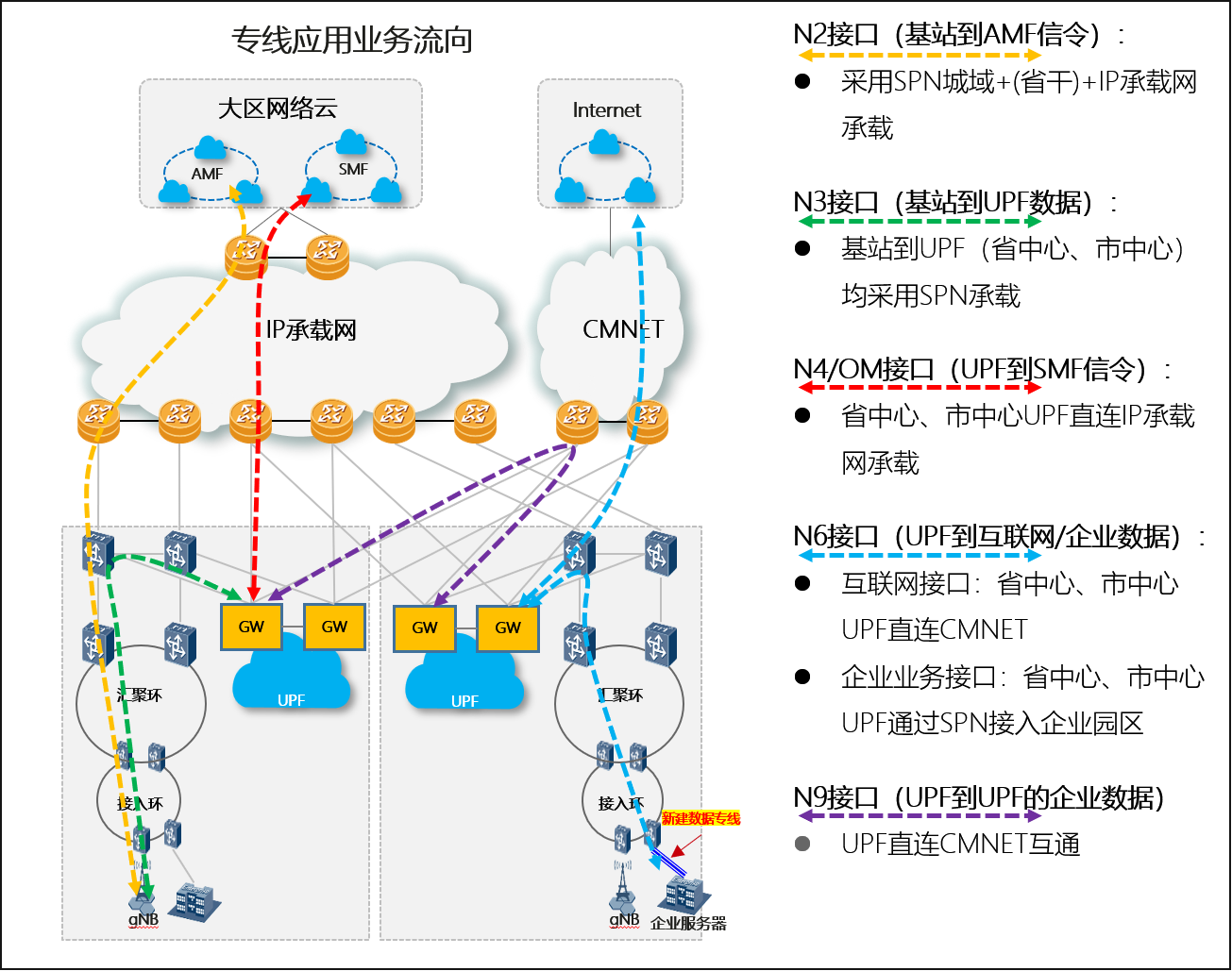
（4）UE IP地址由分流UPF动态分配，两套UPF上配置不同的地址池。

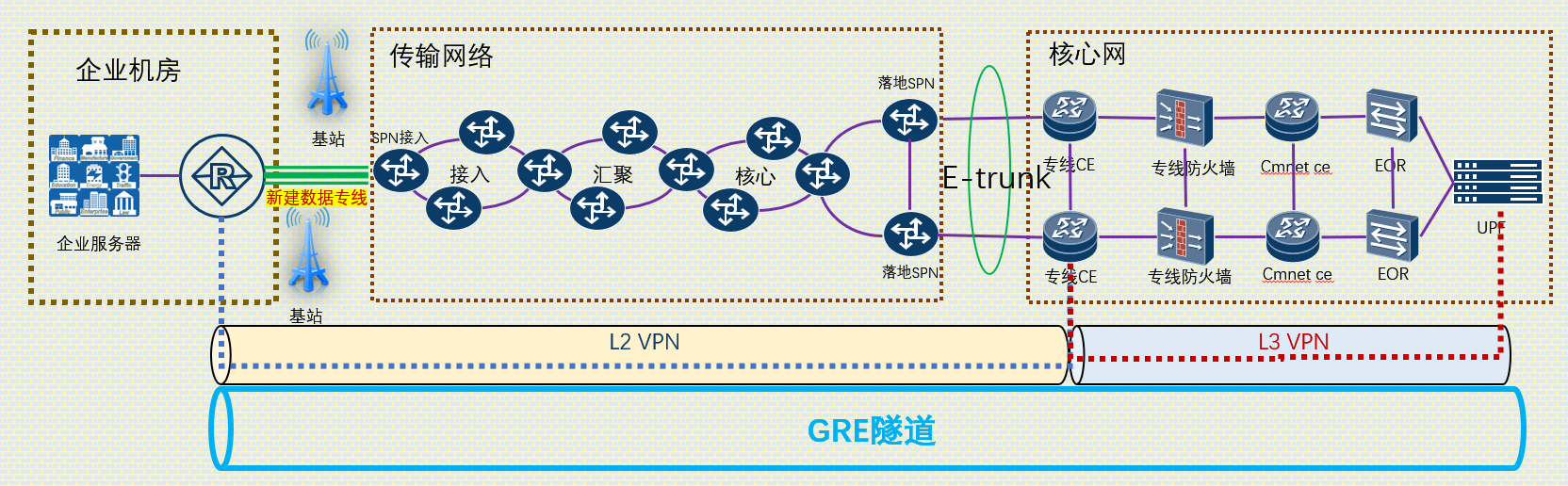
（5）AMF/MME需要开启APN纠错功能，以支持无法手动修改APN的终端注册，漫游场景下，漫游地的AMF/MME同样需要开启。

**传输建设方案（数据专线）**

传输组网如下，新建数据专线只打通接入环与服务器即可。如下图所示。

在企业服务器所在位置选取运营商机房的SPN侧新建一条光纤链路，连接到服务器机房的企业接入设备上，传输侧通过新建VLAN对于专线数据进行隔离。





* SPN上开通业务二层专线，打通用户路由器与落地SPN之间的L2 VPN通道；落地SPN与专网CE之间为100G端口链路，采用E-TRUNK双主对接。落地SPN汇聚所有的专网业务的L2专线，以每业务每VLAN的方式接入专网 CE；
* UPF---EOR(CE8861)---CMNET CE---专线防火墙---专线CE之间新建一个L3 VPN，使用OSPF VPN多实例发布UPF的GRE隧道地址至专线CE；
* 专线CE上创建二层接口与落地SPN对接vlan，vlanif绑定上一步新建的L3 VPN作为用户路由器的网关。vlanif采用双活网关的方式，两台CE配置相同的IP+MAC实现跨框的业务保护；
* 用户路由器根据实际情况配置明细或者缺省路由，建议配置目的IP为UPF 隧道地址，下一跳为专线CE vlanif接口IP；
* 专线CE的vlanif接口上配置入方向流量策略，仅允许行业服务器访问UPF的GRE隧道地址，拒绝访问所有其他UPF的地址。同时UPF可在本机做相关安全防护，确保设备安全；
* UPF和用户路由器之间用于创建GRE的地址路由打通后，在UPF与用户路由器之间创建GRE隧道，每个用户GRE隧道接口IP不能与用户网络内部使用的私网地址冲突，每个行业用户子接口IP也不能冲突，网段划分由UPF侧统一规划；
* 针对每个专网业务，手机地址池地址不能与客户内部使用的私网地址冲突。

传输带宽需要搜集终端的业务模型：进行业务时需要的上下行带宽，终端数量，计算方式为上下行带宽\*终端数量，单位为Mbps。

（例： 某业务终端使用时上下行带宽需要2Mbps，企业计划采购100台，则带宽为2Mbps\*100=200Mbps，数据专线带宽只要大于200Mbps即可满足）

**5G专网优势**

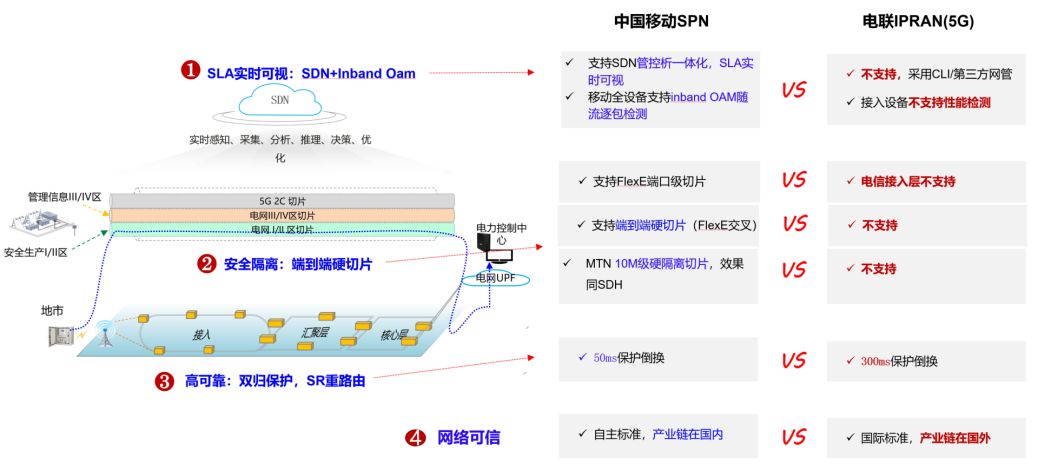
多DNN双域专网解决方案，是创新的双域专网解决方案，可以在用户不换卡不换号的情况下，实现同时访问公网/内网，免认证，无感切换，同时满足45G漫游的需求，是目前双域专网的最优解决方案。

**承载网优势**

提供传输网络具备端到端G.MTN交叉硬切片功能，保障业务的安全隔离、稳定低时延要求。在网络拥塞或流量突发情况下，可保障业务确定性的SLA（带宽、时延、抖动）指标要求。

提供对业务进行实时SLA可视，包括连通性、丢包率、时延、抖动等业务质量指标。在发生SLA性能劣化的情况下，网络能够自动优化及故障自动恢复。

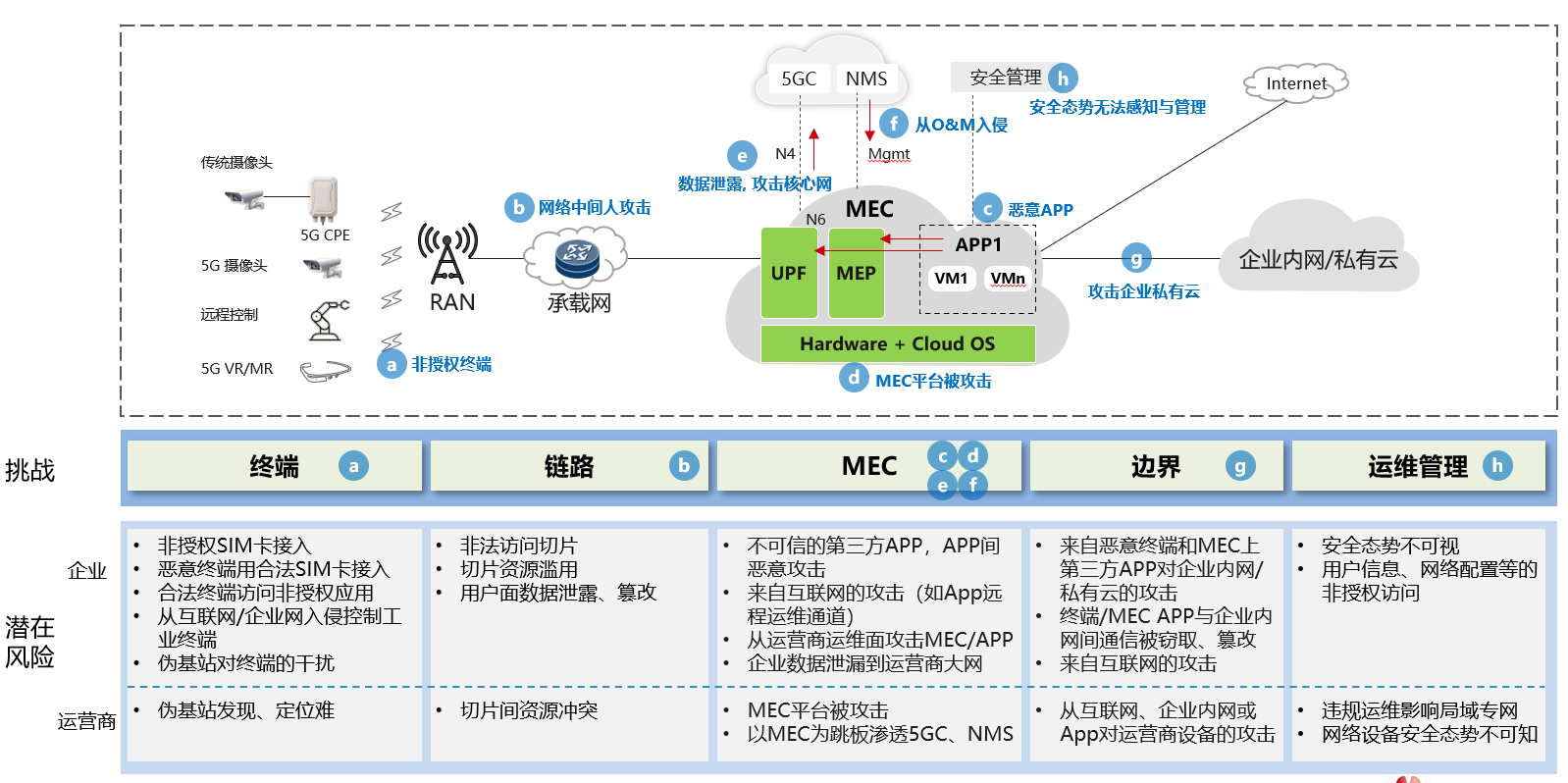
设备采用中国自主技术标准、设备国产化，保障业务安全可信。



* SPN（Slicing Packet Network，切片分组网）是向 5G 承载提出的创新技术体系，以切片以太网内核为基础的新一代融合承载网络架构，同时兼容以太网生态链，具有低成本易部署等特性。
* FlexE端口级切片：独立的端口调度队列，带宽硬隔离、低时延。FLexE端口级切片，解决了端口传统优先级报文调度机制存在的长包阻塞短包，导致短包时延变大（或丢包），业务之间相互影响的问题。通过时隙调度的方式，切片之间严格隔离，独占带宽，不同切片上业务之间不互相影响。在端口上实现了不同切片业务之间的物理硬隔离，保障了业务的安全隔离和低时延。
* 到端组网+随流检测新技术，实现专线质量可视，故障快速定位能力
* 独有零丢包技术，显著提升专线业务可靠性
* FlexE交叉硬切片：安全隔离、稳定低时延。端口转发时隙调度+设备转发时隙交叉，实现芯片级别的安全隔离保障。同时减少转发处理，避免报文调度阻塞，保证稳定时延转发。端到端FlexE1.5层比特块交换，免传统IP转发的成帧、组包、查表、缓存等
* 10M级小颗粒硬切片：FlexE切片的粒度可以支持10M级的粒度

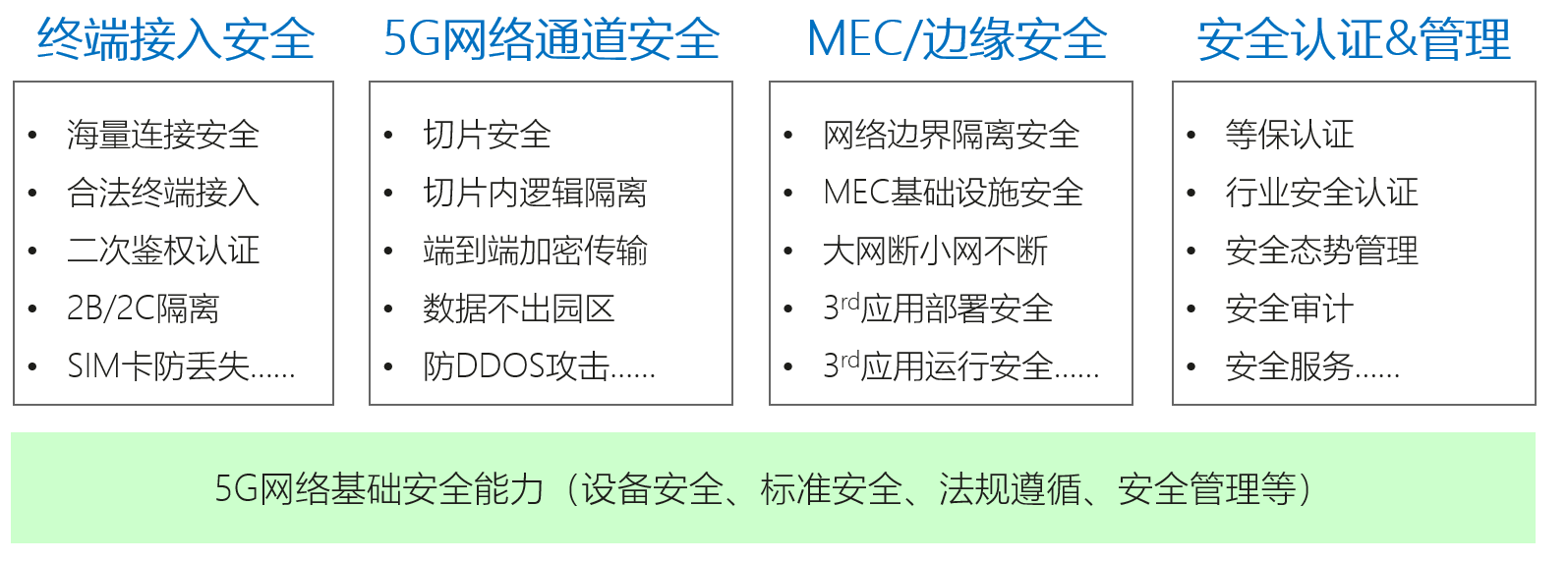
#### 网络建设安全保障

#### 专网安全现状

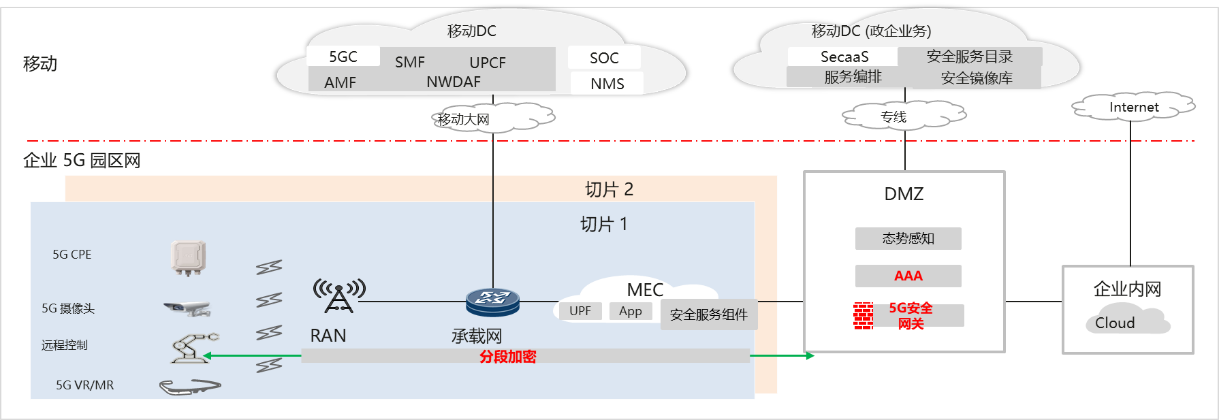


* 终端SIM卡被拔掉插入恶意终端上，造成业务滥用；
* 非法终端接入CPE，攻击其他合法终端，同时虚假终端可能发起网络攻击；
* 企业数据在专线中传输时存在被窥探、泄露风险；
* 对于网络直访企业主页的互联网专线场景，运营商面临来自互联网的攻击；
* 企业服务器面临来自互联网的攻击；

5G网络应用行业，安全需求如下：



5G行业专网支持为不同用户提供定制化的安全服务，从终端安全、网络安全、MEC安全、边界安全4个方面，为不同行业用户构建端到端的灵活安全策略。



#### 终端安全

①终端接入五重访问控制，先认证、再接入

* 主认证：5G终端（如5G CPE/5G 摄像头）与5G网络进行双向鉴权认证(5G AKA标准) 。
* 限制特定终端接入切片：在5GC配置IMSI与园区切片S-NSSAI对应关系，限制仅仅在园区IMSI清单内的终端才可以接入到切片。
* 二次认证：部署AAA服务器，采用IMSI（必选）、IMEI（必选）、 MSISDN (可选）、ULI (可选）组合检验的方式，对接入园区切片的终端进行二次认证，企业可自主实现机卡绑定功能、接入位置控制功能。
* 终端接入位置控制：借助5G网络能力限制终端可接入园区网络的位置。可基于不同控制者、位置控制精度的要求，选择TAI list、ULI或者两者组合方案。
* 企业资源访问控制：终端二次认证身份验证通过后，安全网关实现基于角色细颗粒度访问控制（RBAC）。

②传统终端通过5G CPE/AR接入安全

* 接入认证（依赖于CPE/AR等网关的能力）：

预共享密钥（PSK：pre-shared key ） ；

AAA服务器认证身份：传统终端接入CPE/AR需通过AAA认证；

* 加密：传统终端与CPE/AR之间无线可启用加密
* 开启CPE/AR防火墙的过滤功能：

MAC地址过滤

IP地址过滤

域名过滤：黑白名单

* CPE/AR具备：NAT, L2TP，IPsec等

运营商5G专网是透传管道，可提供分段传输加密，企业可自主实现应用层加密

* 运营商可在无线空口、承载网提供管道加密，以保护用户通信数据安全；
* RAN和UPF，在通信系统中定位于：透传管道，不解析用户数据，不存储用户数据；

#### 传输安全

①非3GPP终端接入

* WLAN接入安全：物理网线，或WLAN加密WEP/WPA /WPA2，保护数据安全传输；
* IPsec VPN：5G CPE到MEC APP边界防火墙FW2之间使用IPsec加密&完保。
* 应用层加密&完保

②5G终端接入

* 空口数据保护：5G基站开启空口PDCP加密&完保及用户隐私保护SUCI，保证空口数据安全。
* IPsec VPN：5G基站到MEC UPF边界防火墙FW1之间使用IPsec加密&完保。
* IPsec VPN：MEC UPF边界防火墙FW2到企业应用服务器之间使用IPsec加密&完保。
* IPsec VPN加密：5G终端到MEC APP边界防火墙FW2之间使用IPsec加密&完保。
* 应用层加密&完保

切片多层次安全措施协同，避免越权运维、数据泄露、资源抢占

避免越权运维

* 切片API接口TLS认证，基于Oauth授权的安全Portal防止切片越权运维
* 通过数字签名和证书，切片模板和实例防篡改

③杜绝数据泄露

* 5G-AKA基础上，提供切片认证；
* 二次认证，提供企业应用会话级鉴权
* 差异化key加密传输防止切片窃取数据、引发切片攻击等
* 空口NSSAI加密，保护敏感用户隐私
* 切片级的FW防护、端到端网络加密（IPSec）

④防止资源抢占

* 通过虚拟及物理隔离技术，确保不抢占周边切片资源

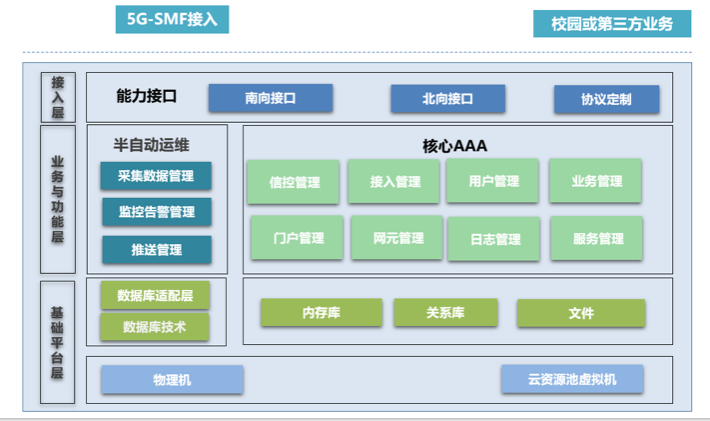
### 5G校园专网融合认证方案（学校侧）

#### 技术架构

采用专用DNN方式，校园内5G身份组件对接运营商SMF完成二次无感认证鉴权模式。设置达州技师学院专用DNN，用户使用互联网时走5G互联网，访问达州技师学院校园网与图书馆/数据库资源时，流量自动通过专线走达州技师学院校园网。支持实名审核、实名认证与审计，支持准入策略与准入权限统一灵活管控。

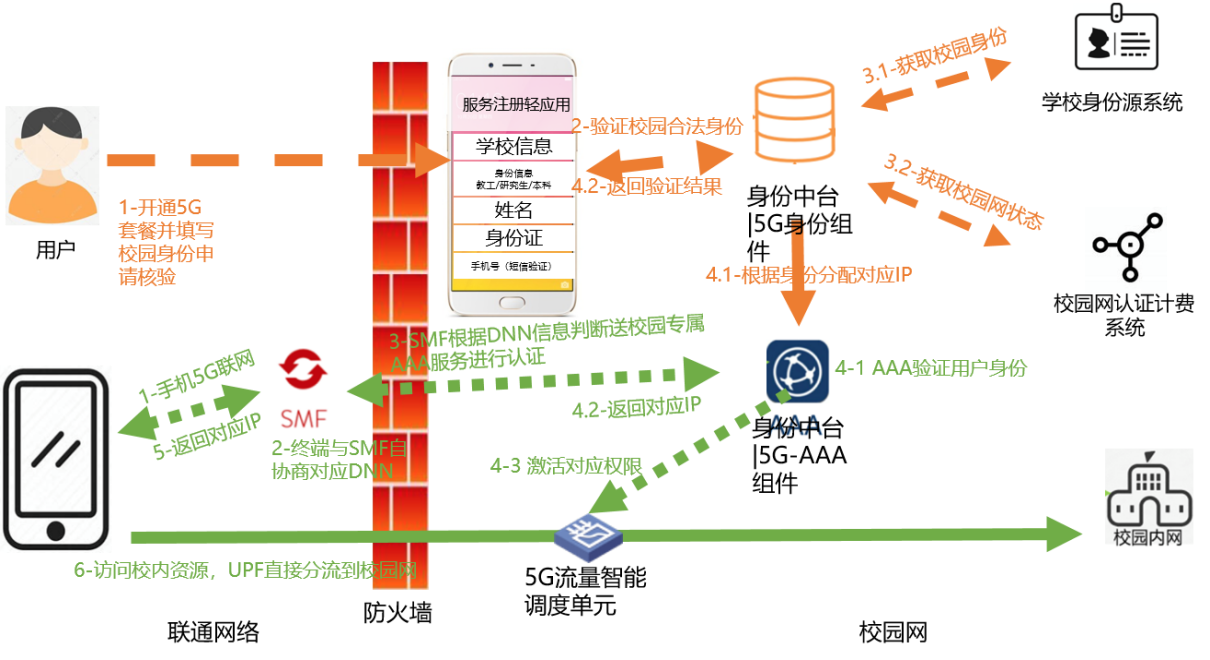
•支持校方二次审核、实名认证与审计、准入策略与准入权限统一灵活管控（通过静态IP或者动态ACL的方式），二次认证时由部署于校园网的5G-AAA认证并分配下发IP。

•访问公网走5G互联网，访问校园内网、图书馆与数据库资源通过专线走5G专网到校园内网。



身份平台|5G身份组件架构图

#### 系统流程图



系统总体流程

运营商提供部署于学校侧的“服务注册轻应用”、“身份中台|5G身份组件”与“身份中台|5G-AAA组件”，提供对应接口。

1. 服务注册轻应用负责为用户提供自助注册、查询与开通入口，用户通过轻应用提交证件号、姓名、手机号，进行短信验证码校验，校验通过后提交信息到5G身份组件核验并通告用户。
2. 5G身份组件负责实时与定时采集数据、核验、权限分配，配置审核与权限策略，以及常见的运营运维功能。5G身份组件从数据中心与校园网认证计费系统中采集数据，进行数据治理并依据规则对数据进行标签化处理，对服务注册轻应用与运营商应用提供“5G专网注册接口”与“查询/校验接口”，并提供定时全量校验接口，供服务注册轻应用与运营商应用调用。通过生涯事件将用户手机号与对应权限发送给5G-AAA组件。
3. 5G-AAA组件主要负责完成对于5G专网权限的授权，通过标准属性下发对应IP（整体策略是合法用户固定分配IP，非法用户轮询IP池中的IP）。实时动态调整与下发权限到5G流量智能调度单元中，以进行ACL、QoS、限速、选路等管控；对接学校实名审计系统与行为管理平台，以完成校园实名审计与行为管理。
4. 5G流量智能调度单元可以考虑利旧现有网关、防火墙，主要负责动态执行权限策略，对于5G校园专网流量进行ACL、QoS、限速、选路等权限执行与访问记录处理；支持高并发大带宽流量处理。

#### 5G校园专网用户注册流程

1. 用户在服务注册轻应用服务注册页面，阅读服务办理条款（其中明确标明注册通过后次日生效；主动或被动注销后次日生效；注明一个有效用户仅能开通运营商的一个专网服务功能，不能开通多个）并勾选同意后录入：姓名、证件类型、证件号、手机号等信息，服务注册轻应用核验输入的信息并通过短信验证码验证手机是否当前正常使用；
2. 正常情况下，此处需要进行用户实名校验，二期通过服务注册轻应用与5G身份中台对接学校数据中心的人脸1:1核验方式完成用户人脸核验，需要学校数据中心支持人脸1:1核验并与5G身份中台对接。
3. 服务注册轻应用将用户信息发送给身份中台|5G身份组件申请注册；
4. 身份中台|5G身份组件根据用户类型（学生/教职工/管理人员等）调用数据中心对应接口，传入证件号与姓名信息，查询姓名、学号与状态信息；
   1. 如果存在多条数据或者不存在数据，则直接业务注册失败并返回对应失败原因与编码。
   2. 身份信息合法，则进一步判断状态是否在允许注册的状态范围，如果不允许开通，则开通失败并返回对应失败原因与编码。
   3. 用户状态允许开通，则调用校园网认证计费系统数据，判断账号是否在校园网认证计费系统中存在，如果不存在或者状态为暂停、欠费或黑名单用户，则开通失败并返回对应失败原因与编码，否则开通成功并返回对应信息给服务注册轻应用。
5. 注册成功后，身份中台|5G身份组件根据用户类型（学生/老师）、状态、校园网状态、校园网黑名单状态等信息，对用户打标签，根据标签从对应地址池中选取未被分发出去的IP并与该手机号绑定；
6. 手机号反写到数据中心或5G身份组件中，用于留痕以便后续审计；
7. 运营商营业人员定时导出服务注册用户名单（手机号与IP地址），通过线上或线下的方式到运营商CBSS系统中开通服务。

#### 5G校园专网用户注销流程

1. 用户在服务注册轻应用服务注销页面，阅读业务办理条款并同意后录入：姓名、证件类型、证件号、手机号等信息，服务注册轻应用核验信息并通过短信验证码验证；
2. 服务注册轻应用将用户信息发送给5G身份组件申请注销；
3. 5G身份组件根据上述信息查询业务注册状态，如果已注册，则本地注销服务，用户绑定的IP释放到对应IP地址池中。如果未注册，则注销失败，并返回对应消息。其他原因导致的注销失败，也同步返回对应信息。
4. 运营商营业人员定时导出服务注销用户名单（手机号与IP地址），通过线上或线下的方式到运营商CBSS系统中注销服务；

#### 用户无感实名认证与审计流程

1. 5G校园专网用户使用5G网络时，终端与SMF自协商对应DNN（纠错）；终端向AMF与UPF发起数据通信请求；
2. SMF根据DNN信息判断是否送身份中台|5G-AAA组件进行认证，将手机号和签约DNN送身份中台|5G-AAA组件认证；
3. 身份中台|5G-AAA组件根据手机号和DNN信息进行认证与鉴权：
   * DNN信息不正确，拒绝，则用户不能使用5G专网与5G互联网；
   * 手机号和DNN信息正确，本地校验用户身份（是否校园合法用户）与校园网账号身份（校园网认证费系统中是否存在），如果校验失败，则认证成功但返回不允许接入的IP地址池中的动态IP；
   * 如果校验成功，则返下发该手机号绑定的IP（固定IP）；
4. 身份中台|5G-AAA组件将实名信息发送给审计系统与行为管理系统，以进行实名审计与行为管理；
5. 身份中台|5G-AAA组件根据用户身份激活对应校内网络权限（ACL、QoS、限速、选路等）。

#### 实时动态核验与权限变更流程

1. 身份中台|5G身份组件根据配置的策略，定时到数据中心与校园网认证计费系统中采集或核验用户信息，并基于配置的策略进行标签处理；
2. 身份中台|5G身份组件基于标签与策略，定期对用户的服务注册状态与权限进行动态更新，并同步给5G-AAA组件；
   1. 5G-AAA组件定期接收权限，并通过激活新权限、失效老权限的方式，进行权限更新。

#### 5G校园专网注册与实名审核功能

###### 功能需求

1.通过5G专网服务注册轻应用，用户只需填入身份信息（姓名、身份证号码或护照号码等），基于信息安全的考虑，不能填入与校园账号相关的任何信息，通过验证码验证用户手机号，用户在页面中阅读并同意业务办理条款，申请5G校园专网业务。

2. 服务注册轻应用将相关信息发往身份中台|5G身份组件受理接口，身份中台|5G身份组件受理接口对接学校数据中心进行身份核验（返回是/否成功，是的同时返回账号），对接校园网认证计费系统进行校园网账号存在性与状态合法性校验。身份中台|5G身份组件记录校园网账户名与注册手机关联信息，将注册成功/失败信息（仅手机号）返回服务注册轻应用。

3. 提供管理页面，以便学校进行5G校园专网用户查询和管理（由身份中台|5G身份组件提供），同时运营商人员可以导出注册数据（以表格的形式，包含手机号、状态、开通时间、IP等，但不包含用户个人信息）。

###### 实现方案

服务注册轻应用是运营商用户注册专网服务的门户，提供新用户注册、查询与注销功能，注册时实时和身份中台|5G身份组件对接，身份中台|5G身份组件从数据中心与校园网认证计费系统中采集核验信息，并根据本地采集的数据按照规则进行校验与注册，实现新开用户的受理和校园用户状态信息的更新功能，主要包括如下几个功能：

1. 增加业务注册模块功能用于支持新开用户信息的开通。
2. 增加业务注销接口模块功能用于支持业务注销。
3. 增加用户信息治理程序用于注册与注册成功用户信息定期自动治理并映射到对应状态与权限中。

通过标准ETL数据采集与数据治理，身份中台|5G身份组件定期采集并治理得到身份数据。通过部署注册实时接口，实现对服务注册轻应用的实时注册请求，根据核验结果进行本地认证平台用户受理过程，最后注册结果和映射返回码返回服务注册轻应用。

#### 5G校园专网注销与审核功能

###### 功能需求

1.通过5G专网服务注册轻应用，用户只需填入身份信息（姓名、身份证号码或护照号码等），基于信息安全的考虑，不能填入与校园账号相关的任何信息，通过验证码验证用户手机号，用户在页面中阅读并同意业务办理条款，注销5G校园专网业务。

2. 服务注册轻应用将相关信息发往身份中台|5G身份组件注销接口，5G身份组件完成注销，释放IP并记录日志。

3. 提供管理页面，以便运营商人员导出注销数据（以表格的形式，包含手机号、状态、状态变更原因、IP，注销时间等，但不包含用户个人信息）。

###### 实现方案

服务注册轻应用提供用户注销功能，实时和身份中台|5G身份组件对接完成注销：

1. 增加业务注销接口模块功能用于支持业务注销。
2. 注销后，用户逻辑删除，释放对应IP、实时取消网络权限，不能给记录生涯日志与事件日志。

#### 5G校园专网实名认证与审计对接功能

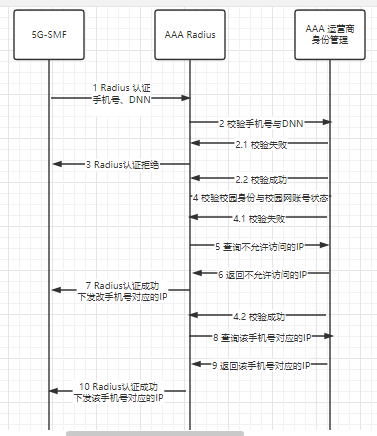
###### 功能需求

1. 5G校园专网用户发起5G移动网络数据连接时，5GC-SMF将用户手机号发往身份中台|5G-AAA进行认证（连接到5G网络、定时15分钟）。

2. 5G-AAA组件，根据手机号和DNN信息进行认证，并对手机号对应校园账号状态进行核验。

SMF发来的认证请求主要包括DNN和手机号；5G-AAA组件中，如果手机号与DNN不匹配，则认证拒绝，此时用户无法访问5G专网与5G互联网；手机号与DNN匹配，则校验5G专网服务状态，校验失败，则认证成功但下发不允许访问的IP地址（轮询）；校验成功，则下发该手机号绑定的IP地址。

###### 实现方案



认证流程：

1. 5G-AAA组件对接5GC-SMF接入Radius认证请求，实现接入报文的解析和关键用户接入属性的提取和二次封装.
2. 手机号与DNN不匹配，则认证拒绝；手机号与DNN匹配，则校验校园身份与校园网账号状态，校验失败，则认证成功但下发不允许访问的IP地址（轮询）；校验成功，则下发该手机号绑定的IP地址。
3. 对于认证成功或失败的请求，记录相关信息保存在日志中；
4. 对于实名认证成功的情况，5G-AAA激活对应IP的权限，并将实名数据实时同步到学校实名审计与行为管理系统中，以便学校进行统一实名审计与行为管理。

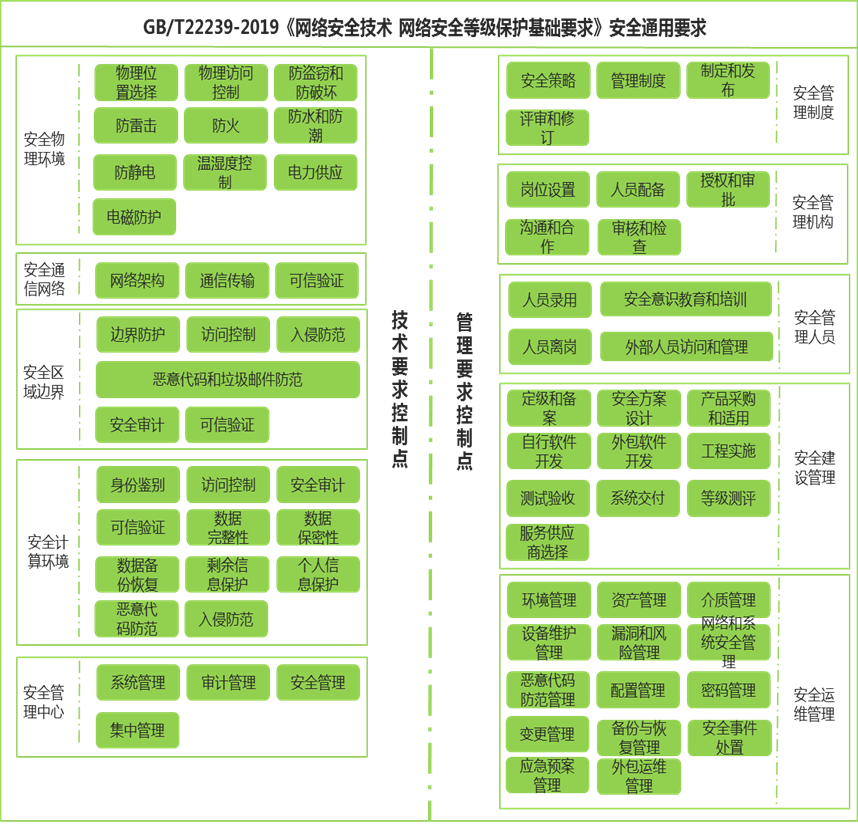
## 网络安全技术网络安全等级保护需求

根据GB/T 22239-2019《网络安全技术网络安全等级保护基本要求》，分为技术和管理两大类要求，具体如下图所示：

日程表

中度可信度描述已自动生成

根据技术与管理要求进行设计，首先应根据本级具体的基本要求设计本级系统的保护环境模型，根据GB/T22239-2019《网络安全等级保护基本要求》，结合技术要求和管理要求，把控以下控制要点：



### 安全技术建设需求

#### 物理环境安全建设需求

物理安全风险主要是指网络周边的环境和物理特性引起的网络设备和线路的不可使用，从而会造成网络系统的不可使用，甚至导致整个网络的瘫痪。它是整个网络系统安全的前提和基础，只有保证了物理层的可用性，才能使得整个网络的可用性，进而提高整个网络的抗破坏力，例如：

1) 机房缺乏控制，人员随意出入带来的风险；

2) 网络设备被盗、被毁坏；

3) 线路老化或是有意、无意的破坏线路；

4) 设备在非预测情况下发生故障、停电等；

5) 自然灾害如地震、水灾、火灾、雷击等；

6) 电磁干扰等。

因此，在通盘考虑安全风险时，应优先考虑物理安全风险。保证网络正常运行的前提是将物理层安全风险降到最低或是尽量考虑在非正常情况下物理层出现风险问题时的应对方案。

#### 通信网络安全建设需求

通信网络的安全主要包括：网络结构安全、网络安全审计、网络设备防护、通信完整性与保密性等方面。

* 网络结构

网络结构是否合理直接影响着是否能够有效的承载业务需要。因此网络结构需要具备一定的冗余性；带宽能够满足业务高峰时期数据交换需求；并合理的划分网段和VLAN。

* 网络安全审计

由于用户的计算机相关的知识水平参差不齐，一旦某些安全意识薄弱的管理用户误操作，将给信息系统带来致命的破坏。没有相应的审计记录将给事后追查带来困难。有必要进行基于网络行为的审计。从而威慑那些心存侥幸、有恶意企图的少部分用户，以利于规范正常的网络应用行为。

* 网络设备防护

由于高校在建网络系统将会使用大量的网络设备和安全设备，如交换机、防火墙、入侵检测设备等。这些设备的自身安全性也会直接关系到涉密网和各种网络应用的正常运行。如果发生网络设备被不法分子攻击，将导致设备不能正常运行。更加严重情况是设备设置被篡改，不法分子轻松获得网络设备的控制权，通过网络设备作为跳板攻击服务器，将会造成无法想象的后果。例如，交换机口令泄漏、防火墙规则被篡改、入侵检测设备失灵等都将成为威胁网络系统正常运行的风险因素。

* 通信完整性与保密性

由于网络协议及文件格式均具有标准、开发、公开的特征，因此数据在网上存储和传输过程中，不仅仅面临信息丢失、信息重复或信息传送的自身错误，而且会遭遇信息攻击或欺诈行为，导致最终信息收发的差异性。因此，在信息传输和存储过程中，必须要确保信息内容在发送、接收及保存的一致性；并在信息遭受篡改攻击的情况下，应提供有效的察觉与发现机制，实现通信的完整性。

而数据在传输过程中，为能够抵御不良企图者采取的各种攻击，防止遭到窃取，应采用加密措施保证数据的机密性。

*  网络可信接入

对于一个不断发展的网络而言，为方便办公，在网络设计时保留大量的接入端口，这对于随时随地快速接入到校园网业务网络进行办公是非常便捷的，但同时也引入了安全风险，一旦外来用户不加阻拦的接入到网络中来，就有可能破坏网络的安全边界，使得外来用户具备对网络进行破坏的条件，由此而引入诸如蠕虫扩散、文件泄密等安全问题。因此需要对非法客户端实现禁入，能监控网络，对于没有合法认证的外来机器，能够阻断其网络访问，保护好已经建立起来的安全环境。

#### 区域边界安全建设需求

区域边界的安全主要包括：边界访问控制、边界完整性检测、边界入侵防范以及边界安全审计等方面。

* 边界访问控制

对于各类边界最基本的安全需求就是访问控制，对进出安全区域边界的数据信息进行控制，阻止非授权及越权访问。

* 边界完整性检测

边界的完整性如被破坏则所有控制规则将失去效力，因此需要对内部网络中出现的内部用户未通过准许私自联到外部网络的行为进行检查，维护边界完整性。

* 边界入侵防范

各类网络攻击行为既可能来自于大家公认的互联网等外部网络，在内部也同样存在。通过安全措施，要实现主动阻断针对信息系统的各种攻击，如病毒、木马、间谍软件、可疑代码、端口扫描、DoS/DDoS等，实现对网络层以及业务系统的安全防护，保护核心信息资产的免受攻击危害。

* 边界安全审计

在安全区域边界需要建立必要的审计机制，对进出边界的各类网络行为进行记录与审计分析，可以和主机审计、应用审计以及网络审计形成多层次的审计系统。并可通过安全管理中心集中管理。

* 边界恶意代码防范

现今，病毒的发展呈现出以下趋势:病毒与黑客程序相结合、蠕虫病毒更加泛滥，目前计算机病毒的传播途径与过去相比已经发生了很大的变化，更多的以网络（包括 Internet、广域网、局域网）形态进行传播，因此为了安全的防护手段也需以变应变。迫切需要网关型产品在网络层面对病毒予以查杀。

#### 计算环境安全建设需求

计算环境的安全主要指主机以及应用层面的安全风险与需求分析，包括：身份鉴别、访问控制、系统审计、入侵防范、恶意代码防范、软件容错、数据完整性与保密性、备份与恢复、资源合理控制、剩余信息保护、抗抵赖等方面。

* 身份鉴别

身份鉴别包括主机和应用两个方面。

主机操作系统登录、数据库登陆以及应用系统登录均必须进行身份验证。过于简单的标识符和口令容易被穷举攻击破解。同时非法用户可以通过网络进行窃听，从而获得管理员权限，可以对任何资源非法访问及越权操作。因此必须提高用户名/口令的复杂度，且防止被网络窃听；同时应考虑失败处理机制。

* 访问控制

访问控制包括主机和应用两个方面。访问控制主要为了保证用户对主机资源和应用系统资源的合法使用。非法用户可能企图假冒合法用户的身份进入系统，低权限的合法用户也可能企图执行高权限用户的操作，这些行为将给主机系统和应用系统带来了很大的安全风险。用户必须拥有合法的用户标识符，在制定好的访问控制策略下进行操作，杜绝越权非法操作。

* 系统审计

系统审计包括主机审计和应用审计两个方面。

对于登陆主机后的操作行为则需要进行主机审计。对于服务器和重要主机需要进行严格的行为控制，对用户的行为、使用的命令等进行必要的记录审计，便于日后的分析、调查、取证，规范主机使用行为。而对于应用系统同样提出了应用审计的要求，即对应用系统的使用行为进行审计。重点审计应用层信息，和业务系统的运转流程息息相关。能够为安全事件提供足够的信息，与身份认证与访问控制联系紧密，为相关事件提供审计记录。

* 入侵防范

主机操作系统面临着各类具有针对性的入侵威胁，常见操作系统存在着各种安全漏洞，并且现在漏洞被发现与漏洞被利用之间的时间差变得越来越短，这就使得操作系统本身的安全性给整个系统带来巨大的安全风险，因此对于主机操作系统的安装，使用、维护等提出了需求，防范针对系统的入侵行为。

* 恶意代码防范

病毒、蠕虫等恶意代码是对计算环境造成危害最大的隐患，当前病毒威胁非常严峻，特别是蠕虫病毒的爆发，会立刻向其他子网迅速蔓延，发动网络攻击和数据窃密。大量占据正常业务十分有限的带宽，造成网络性能严重下降、服务器崩溃甚至网络通信中断，信息损坏或泄漏。严重影响正常业务开展。因此必须部署恶意代码防范软件进行防御。同时保持恶意代码库的及时更新。

* 软件容错

软件容错的主要目的是提供足够的冗余信息和算法程序,使系统在实际运行时能够及时发现程序设计错误,采取补救措施,以提高软件可靠性,保证整个计算机系统的正常运行。

* 数据安全

主要指数据的完整性与保密性。数据是信息资产的直接体现。所有的措施最终无不是为了业务数据的安全。因此数据的备份十分重要，是必须考虑的问题。应采取措施保证数据在传输过程中的完整性以及保密性。

* 备份与恢复

数据是信息资产的直接体现。所有的措施最终无不是为了业务数据的安全。因此数据的备份十分重要，是必须考虑的问题。对于关键数据应建立数据的备份机制，而对于网络的关键设备、线路均需进行冗余配置，备份与恢复是应对突发事件的必要措施。

* 资源合理控制

资源合理控制包括主机和应用两个方面。

主机系统以及应用系统的资源是有限的，不能无限滥用。系统资源必须能够为正常用户提供资源保障。否则会出现资源耗尽、服务质量下降甚至服务中断等后果。因此对于系统资源进行控制，制定包括：登陆条件限制、超时锁定、用户可用资源阈值设置等资源控制策略。

* 剩余信息保护

对于正常使用中的主机操作系统和数据库系统等，经常需要对用户的鉴别信息、文件、目录、数据库记录等进行临时或长期存储，在这些存储资源重新分配前，如果不对其原使用者的信息进行清除，将会引起用户信息泄漏的安全风险，因此，需要确保系统内的用户鉴别信息文件、目录和数据库记录等资源所在的存储空间，被释放或重新分配给其他用户前得到完全清除。

对于动态管理和使用的客体资源，应在这些客体资源重新分配前，对其原使用者的信息进行清除，以确保信息不被泄漏。

* 抗抵赖

对于数据安全，不仅面临着机密性和完整性的问题，同样还面临着抗抵赖性（不可否认性）的问题，应采用技术手段防止用户否认其数据发送和接收行为，为数据收发双方提供证据。

#### 管理中心安全建设需求

“安全管理中心”是纵深防御体系的“大脑”，通过“安全管理中心”实现技术层面的系统管理、审计管理和安全管理，同时通过“安全管理中心”实现整改云计算环境的集中管控。“安全管理中心”并非一个机构，也并非一个产品，是一个技术管控枢纽，通过一个技术工具或多个技术工具实现一定程度上的集中管理，便于云计算资源进行调度、管理以及监控，同时能够对统一身份、认证、授权及密钥进行管理。

### 安全管理建设需求

#### 管理制度安全建设需求

根据安全管理制度的基本要求制定各类管理规定、管理办法和暂行规定。从安全策略主文档中规定的安全各个方面所应遵守的原则方法和指导性策略引出的具体管理规定、管理办法和实施办法，是具有可操作性，且必须得到有效推行和实施的制度。

制定严格的制定与发布流程，方式，范围等，制度需要统一格式并进行有效版本控制；发布方式需要正式、有效并注明发布范围，对收发文进行登记。

信息安全领导小组负责定期组织相关部门和相关人员对安全管理制度体系的合理性和适用性进行审定，定期或不定期对安全管理制度进行评审和修订，修订不足及进行改进。

#### 管理机构安全建设需求

根据基本要求设置安全管理机构的组织形式和运作方式，明确岗位职责；

设置安全管理岗位，设立系统管理员、网络管理员、安全管理员等岗位，根据要求进行人员配备，配备专职安全员；成立指导和管理信息安全工作的委员会或领导小组，其最高领导由监所主管领导委任或授权；制定文件明确安全管理机构各个部门和岗位的职责、分工和技能要求。

建立授权与审批制度；

建立内外部沟通合作渠道；

定期进行全面安全检查，特别是系统日常运行、系统漏洞和数据备份等。

#### 管理人员安全建设需求

根据基本要求制定人员录用，离岗、考核、培训几个方面的规定，并严格执行；规定外部人员访问流程，并严格执行。

#### 建设管理安全建设需求

根据基本要求制定系统建设管理制度，包括：系统定级、安全方案设计、产品采购和使用、自行软件开发、外包软件开发、工程实施、测试验收、系统交付、系统备案、等级评测、安全服务商选择等方面。从工程实施的前、中、后三个方面，从初始定级设计到验收评测完整的工程周期角度进行系统建设管理。

#### 运维管理安全建设需求

校园业务系统的安全性及其保护机制，在校园网整体安全防护中一直处于极为重要的地位，为了避免应用系统出现漏洞，应建立有效的访问控制机制。

### 数据中心扩容建设需求

学校原有超融合数据中心配置有3套超融合节点，承载学校的所有业务系统。超融合系统通过融合计算、存储与网络于一体，通过软件定义的方式，在提供存储的同时，也提供计算能力，这不但大量减少了硬件投入和电力成本，也将计算放在离存储更近的地方，达到最优的性能。超融合架构通常采用了全分布式的组件，横向可扩展，不存在单点失效，数据能够自动恢复和备份，性能优势非常明显，是目前国际上主流科技公司普遍采用的IT基础架构，也是未来IT基础架构的方向。

但是随着学校应用系统的快速建设，原有超融合硬件性能已经无法满足应用系统的需求，急需扩容，同时扩容也需要兼容原超融合系统，实现融合一体化管理。

### 方案设计原则

校园网安全防御体系设计以安全合规要求为基础，以实际业务安全需求为主导，构建信息安全等级保护深度防御体系。在建设过程中，遵循统一规划、统一标准、统一管理、适度保护、重点保护、强化管理的原则。除此之外，作为国家等级保护重点防护的信息系统，在信息系统设计环节重点把握如下原则：

1、统一性、整体性原则

达州技师学院的信息系统是一个有机的整体，为适应目前以及未来业务发展的需要，为业务系统提供可靠的安全保障，需要有一个完整、可靠的整体安全体系。

对整个校园网安全防御体系实行统一规划，统一标准，并进行一体化安全建设、安全管理和安全运营；按照总体规划、部署和要求，做好各层面的统一建设和管理工作。

2、一致性原则

“木桶的最大容积取决于最短的一块木板”。网络信息系统是一个复杂的计算机系统，它本身在物理上、操作上和管理上不同层次不同位置上的种种漏洞构成了系统的安全脆弱性，尤其是多用户网络系统自身的复杂性、资源共享性使单纯的技术保护防不胜防。攻击者使用的是“最易渗透原则”，必然在系统中最薄弱的地方进行攻击。因此，充分、全面、完整地对系统的安全威胁和安全风险进行分析、评估和检测，是设计信息安全系统的必要前提条件。安全机制和安全服务设计的首要目的是防止最常用的攻击手段，重要目标是提高整个系统的“安全最低点”的安全性能。

3、多重保护原则

任何单一层次的安全措施都不是绝对安全的，都可能被攻破。必须建立系统性的安全防护措施，从多层次，多维度进行多重保护，各个层次的保护相互补充，形成统一协调的安全策略，避免防护短板，层层防护，即使某一层保护被攻破时，其它层保护仍可保护信息系统的安全。

4、适应性及灵活性原则

针对达州技师学院的安全体系设计上必须具备一定的冗余和前瞻性，能随着网络性能及安全需求的变化而变化，要在整个系统内尽可能引入更多的灵活自适应的因素，并具有良好的扩展性。要能够为将来业务扩展提供足够的安全扩展能力。

### 方案设计思路

结合达州技师学院现网的实际情况，按照《网络安全等级保护安全设计技术要求》和《网络安全等级保护基本要求》等相关标准要求，以“一个中心、三重防护”为核心指导思想，从安全计算环境、安全区域边界、安全通信网络以及安全管理中心四个方面构建安全建设方案，以满足等级保护三级系统的相关要求。

本方案充分结合系统业务应用流程、网络现状、等级保护要求及实际的安全需求进行设计，在设计过程中将采取如下原则：

* 1. **综合防范、整体安全**

坚持管理与技术并重，从人员、管理、安全技术手段等多方面着手，建立综合防范机制，实现整体安全；

* 1. **分域保护、务求实效**

将信息资源划分为计算环境、区域边界、通信网络三个方面进行安全防护设计，以体现层层递进，逐级深入的安全防护理念；

* 1. **同步建设**

安全保障体系规划与系统建设同步，协调发展，将安全保障体系建设融入到信息化建设的规划、建设、运行和维护的全过程中；

* 1. **纵深防御，集中管理**

可构建一个从外到内、功能互补的纵深防御体系，对资产、安全事件、风险、访问行为等进行集中统一分析与监管；

* 1. **等级保护策略**

安全保障体系设计以实现等级保护为基本出发点进行安全防护体系建设，并遵照《信息安全技术 网络安全等级保护基本要求》进行安全防护措施设计。

### 整体建设框架

本方案将严格根据技术与管理要求同时进行设计，同时根据本级具体的设计技术要求设计本级系统安全保护环境建设模型，按照物理安全、通信网络安全、计算环境安全、区域边界安全、运维管理安全以及管理要求，形成如下模型框架：



### 安全技术差距分析

《信息安全技术 网络安全等级保护安全设计技术要求》技术标准中将等保建设的环境分为：

1. 安全计算环境：对定级系统的信息进行存储、处理及实施安全策略的相关部件
2. 安全区域边界：对定级系统的安全计算环境边界，以及安全计算环境与安全通信网络之间实现连接并实施安全策略的相关部件。
3. 安全通信网络：对定级系统安全计算环境之间进行信息传输及实施安全策略的相关部件。
4. 安全管理中心：对定级系统的安全策略及安全计算环境、安全区域边界和安全通信网络上的安全机制实施统一管理的平台。

依据等保建设环境的划分，从以下四个方面展开建设需求分析：

### 安全计算环境

根据《信息安全技术 网络安全等级保护基本要求》与《信息安全技术 网络安全等级保护安全设计技术要求》，达州技师学院如果想达到等级保护三级的要求，安全计算环境存在如下差距：

1. 主机防病毒：该信息系统缺少主机防病毒的相关安全策略，需要配置网络版主机防病毒系统，从而实现对全网主机的恶意代码防范。
2. 数据库审计：该信息系统缺少针对数据的审计设备，不能很好的满足主机安全审计的要求，需要部署专业的数据库审计设备。
3. 运维堡垒主机：该信息系统无法实现管理员对网络设备和服务器进行管理时的双因素认证，需要部署堡垒机来实现。
4. 备份与恢复：该信息系统没有完善的数据备份与恢复方案，需要制定相关策略。同时，该信息系统没有实现对关键网络设备的冗余，建议部署双链路确保设备冗余。

### 安全区域边界

1. 边界访问控制：该信息系统无法实现对边界的访问控制，需要部署防火墙等安全设备来实现。
2. 边界入侵防范：该信息系统无法实现对边界的访问控制，需要部署防火墙等安全设备来实现。
3. 边界恶意代码过滤：该信息系统无法实现对边界的访问控制，需要部署防火墙等安全设备来实现。
4. 防web攻击：该信息系统无法实现对边界的访问控制，需要部署WEB防火墙等安全设备来实现。
5. 安全域边界安全审计：该信息系统无法实现对边界的访问控制，需要部署署网络安全审计等安全设备来实现。
6. 互联网出口安全审计：该信息系统无法实现对边界的访问控制，需要部署行为管理等设备来实现。

### 安全网络通信

1. 通信完整性和保密性：该信息系统无法实现对边界的访问控制，需要部署SSL VPN等安全设备来实现。
2. 流量管理：该信息系统无法实现对边界的访问控制，需要部署流量管理系统等安全设备来实现。

### 安全管理中心

1. 统一日志平台：该信息系统无法实现对相关网络及安全设备的日志审计功能，需要部署日志审计系统来实现。
2. 统一监控平台：该信息系统无法统一展示边界的安全威胁情况，需要部署安全感知平台等来实现。
3. 统一管理平台：该信息系统无法实现对边界的访问控制，需要部署运维堡垒主机来实现。

## 技术方案及实施

### 物理与环境安全保障

#### 机房出入控制

设置门禁系统，进入机房的人员进行身份鉴别并登记在案；设置视频监控系统，监控并限制进入机房人员的活动；应对机房划分区域进行管理，区域和区域之间设置物理隔离装置，在重要区域前设置交付或安装等过度区域；应对重要区域配置电子门禁系统，鉴别和记录进入的人员身份并监控其活动。

相应采取的技术措施有：监控设备；门禁系统。

1.监控设备

* 多路监控：能够同时对多路的视频同时进行监控，用户可以任意选择区域内的视频通道。
* 视频录像：应采用硬盘实时记录多路监控信号，免除用普通录像带录制带来的一些不便。硬盘存满前有相应操作提示。
* 视频检索与回放：可以根据用户的查询请求查询录制在硬盘上的数据，并显示回放，供事后调查取证使用。回放时可以进行快进、快倒、慢进、慢倒、单帧步进等控制，图像可整图放大、局部放大。还可根据需要对录制的数据进行锁定（防止误删除）、删除、复制等操作，对图像可以进行编辑、打印等操作。
* 报警接入与报警联动：通过网络视频服务器，用户能够接入多种报警信号，包括烟感、红外探测和其他各种报警，并且能够外接多路继电器输出。
* 云台及镜头控制：一般情况下，摄像机采用定焦距、定方向的固定方式，在光照度变化大的场所应选用自动光圈镜头并配备防护罩，大范围监控区域宜选用带有转动云台和变焦镜头的摄像机。

2.门禁系统

* 脱机运行功能：控制器有存贮功能，保存有用户资料，用户刷卡开门时将记录保存。不需要电脑控制二十四小时运行；
* 设定进出门的权限：对每个门禁进行设置，确定哪些卡可以进出；
* 设定每张卡进出门的时段：设置每个门禁上每张卡在什么时间范围内可以进出；
* 主动上传功能：监控时计算机不需要扫描，而控制器主动上传信号，异常情况时同时报警；
* 实时监控功能：系统管理人员可以通过监控计算机实时查看每个门人员的进出情况、每个门的状态（包括门的开关，各种非正常状态报警等）。紧急情况发生时会打开某一个门或所有的门；
* 出入记录查询功能：系统可储存所有的进出记录、状态记录，可按不同的查询条件查询。
* 异常报警功能：当门打开时间过长，非法闯入、门锁被破坏等情况出现时，可以实现计算机报警
* 网络管理监控功能：门禁系统通常由一台计算机管理。本系统则可以在网络上任何一台有网络管理门禁软件的计算机上对整个系统进行设置、监控、查询、管理。

#### 防盗窃和防破坏

主要设备存放位置物理受限；主要设备和部件固定，并加上不易拆除标记；通信线路隐藏铺设；存储介质分类标记和存储；安装防盗报警设备。

相应采取的技术措施有：防盗报警器。

#### 防雷击

购置防雷设备，进行防雷击措施的保护；设置交流电接地线；防雷保安器，防止感应雷。对于计算机网络防雷保护，由最外层到最内层必须实行多级保护：

1、最外层是直接雷击区域，危险性最高，采用AR限流避雷针保护可减少雷害。

2、电源系统采用DSOP多级保护，可将雷电过电压降到设备承受的水平。

3、网络设备间可根据其接口形式和敏感度来选择不同的电涌保护器。DLP、CSP

4、电源线应尽可能远离信号线，并避免并排敷设。否则，应采取屏蔽措施。

5、工作、保护、直流和防雷四种接地以共用同一组接地装置，接地电组值不应大于4欧姆。

相应采取的技术措施有：防雷击设备、防雷保安器等。

#### 防火

设置火灾自动消防系统，自动检测火情、自动报警，并自动灭火；机房、工作场所建筑材料应当采用耐火材料；机房采取防火隔离设施，将重要设备和其他设备隔离开。

相应采取的技术措施有：烟感器，自动灭火器；耐火材料，防火隔离设施。

#### 防水防潮

在水管安装时，不要使得水管穿过屋顶和活动地板下，以免水管破裂或者爆裂造成水灾；对穿过墙壁和楼板的水管增加必要的保护措施，如设置套管；采取必要的措施防止雨水通过屋顶和墙壁渗透，造成水灾；采取措施防止室内水蒸气结露和地下积水的转移与渗透。

相应采取的技术措施有：套管，除湿装备。

#### 防静电

在机房和办公场所设置必要的接地等防静电措施；可以采用防静电地板或地毯。

相应采取的技术措施有：机房湿度控制设备，防静电地板。

#### 温湿度控制

购置恒温恒湿设备，保持机房的温湿度，保证设备运行在允许温湿度环境下，防止设备在非正常的情况下运行造成的安全隐患。

相应采取的技术措施有：恒湿空调设备。

#### 电力供应

计算机系统供电应与其他供电分开；设置稳压和过压防护设备；提供短期电力供应系统，如UPS系统；电力供应系统配置冗余或者并行的电力电缆；必要时，配置备用电力系统。

相应采取的技术措施有：稳压、过压器；UPS；备用发电机。

#### 电磁防护

交流电一定要接地线，防止外界电磁干扰和寄生设备耦合；电力电缆与通信线缆要实行分离部署，防止产生电磁干扰；重要设备和磁介质实行电子屏蔽。

相应采取的技术措施有：绝缘地板、防电磁干扰设备、电子屏蔽设备。

### 计算环境安全设计

#### 用户身份鉴别

身份鉴别可分为主机身份鉴别和应用身份鉴别两个方面：

1.主机身份鉴别：

为提高主机系统安全性，保障各种应用的正常运行，对主机系统需要进行一系列的加固措施，包括：

* 对登录操作系统和数据库系统的用户进行身份标识和鉴别，且保证用户名的唯一性。
* 根据基本要求配置用户名/口令；口令必须具备采用3种以上字符、长度不少于8位并定期更换；
* 启用登陆失败处理功能，登陆失败后采取结束会话、限制非法登录次数和自动退出等措施。
* 远程管理时应启用SSH等管理方式，加密管理数据，防止被网络窃听。
* 对主机管理员登录进行双因素认证方式，采用USBkey+密码进行身份鉴别。

2.应用身份鉴别：

为提高应用系统系统安全性，应用系统需要进行一系列的加固措施，包括：

* 对登录用户进行身份标识和鉴别，且保证用户名的唯一性。
* 根据基本要求配置用户名/口令，必须具备一定的复杂度；口令必须具备采用3种以上字符、长度不少于8位并定期更换；
* 启用登陆失败处理功能，登陆失败后采取结束会话、限制非法登录次数和自动退出等措施。
* 应用系统如具备上述功能则需要开启使用，若不具备，则需进行相应的功能开发，且使用效果要达到以上要求。
* 对于三级系统，要求对用户进行两种或两种以上组合的鉴别技术，因此可采用双因素认证（USBkey+密码）或者构建PKI体系，采用CA证书的方式进行身份鉴别。

#### 终端安全

通过部署1套终端健康检查和修复系统实现终端安全的集中统一管理，包括终端补丁的集中下载与分发、应用软件的集中分发、禁止非工作软件或有害软件的安装和运行等，强化终端安全策略，终端安全管理软件还可满足接入和外联的可管理要求。对终端进行安全检查，确保终端符合安全规范，对不合规终端进行隔离修复。对系统自身安全问题及终端安检问题进行报警统计，具体功能包括：

**1.限制非法外联**

应设定只有与终端管理系统通讯的网卡才能发送和接收数据除，禁止其他任何网卡发送和接收数据，包括多网卡、拨号连接，VPN连接等。

**2.终端安全基线自动检测与强制修复**

能够监控计算机终端的操作系统补丁、防病毒软件、软件进程、登录口令、注册表等方面的运行情况。如果计算机终端没有安装规定的操作系统补丁、防病毒软件的运行状态和病毒库更新状态不符合要求、没有运行指定的软件或运行了禁止运行的软件，或者有其它的安全基线不能满足要求的情况，该计算机终端的网络访问将被禁止。

**3.移动存储管理**

可以实现移动存储设备的认证和设备使用授权，只有认证的移动存储存储设备和具有使用权限的用户才能使用。对于认证过的移动存储设备，可以根据防泄密控制要求的高低，可以选择多种数据保存和共享授权方式。可以只认证设备，不对其中保存数据进行加密共享；也可以对认证的设备选择专用目录或全盘加密共享，并可以对移动设备使用全过程进行审计，方便在发生意外时进行查证。

**4.终端审计**

包括“文件操作审计与控制”，“打印审计与控制”，“网站访问审计与控制”，“异常路由审计”和“终端Windows登录审计”。所审计的内容尽量只与内网安全合规相关的信息，不对涉及终端用户的个人隐私信息，保证在达到合规管理的审计要求的前提下，保护终端用户个人私隐。

**部署设备：终端安全管理系统**

#### 漏洞发现

漏洞扫描就是对重要计算机信息系统进行检查，发现其中可被黑客利用的漏洞，通过合规性检测对系统中不合适的设置（如不应开放的端口）、脆弱的口令以及其他同安全规则相抵触的对象进行检查；另外基于网络的检测(Network Scanner)，通过执行一些脚本文件对系统进行攻击，并记录它的反应，从而发现其中的漏洞。

**部署设备：漏洞扫描系统**

#### 数据库安全审计

计划部署数据库审计系统对用户行为、用户事件及系统状态加以审计，范围覆盖到每个用户，从而把握数据库系统的整体安全。

数据库审计系统适用于等级保护标准和规范。数据库审计系统支持所有主流关系型数据库的安全审计，采用多核、多线程并行处理及CPU绑定技术及镜像流量零拷贝技术，采用黑盒逆向协议分析技术，严格按照数据库协议规律，对所有数据库的操作行为进行还原，支持请求和返回的全审计，保证100%还原原始操作的真实情况，实现细粒度审计、精准化行为回溯、全方位风险控制，为学校的核心数据库提供全方位、细粒度的保护功能。数据库审计系统可以帮助我们解决目前所面临的数据库安全审计缺失问题，避免数据被内部人员及外部黑客恶意窃取泄露，极大的保护系统的核心敏感数据的安全，带来以下安全价值：

* 全面记录数据库访问行为，识别越权操作等违规行为，并完成追踪溯源
* 跟踪敏感数据访问行为轨迹，建立访问行为模型，及时发现敏感数据泄漏
* 检测数据库配置弱点、发现SQL注入等漏洞、提供解决建议
* 为数据库安全管理与性能优化提供决策依据
* 提供符合法律法规的报告，满足等级保护审计要求。

**部署设备：数据库审计系统**

#### 运维能力

计划部署运维堡垒主机，堡垒机可提供全面的运维管理体系和运维能力，支持资产管理、用户管理、双因子认证、命令阻断、访问控制、自动改密、审计等功能，能够有效的保障运维过程的安全。在协议方面，堡垒机全面支持SSH/TELNET/RDP（远程桌面）/FTP/SFTP/VNC，并可通过应用中心技术扩展支持VMware/XEN等虚拟机管理、oracle等数据库管理、HTTP/HTTPS、小型机管理**等。**

**部署设备：运维堡垒主机**

#### 容灾备份

虽然通过大量的安全设备对攻击入侵进行了安全防护，但是任然无法避免人为误删除、系统逻辑故障造成的系统停机以及数据丢失，一旦出现故障或者数据的丢失，将会造成严重的安全事故，因此在建设各种安全防护及分析的同时，还需要建设本地的容灾备份机制，提供数据的最后保护能力。

**部署设备：备份一体机**

### 区域边界安全保护设计

通过深入了解达州技师学院业务系统特点和系统功能要求，并在充分利用现有网络设施的基础上，结合国家等级保护政策和标准要求，对信息系统的安全区域保护目标进行如下设计。

#### 边界隔离与访问控制

在本方案中，达州技师学院系统分布在网络出口边界、数据中心区边界、网络管理区，所以每个边界也部署防火墙，并且通过配置防火墙的安全策略，实现各区域边界的隔离与细粒度的访问控制。防火墙是部署在不同网络安全域之间的一系列部件的组合。它是信息的唯一出入口，能根据安全策略控制（允许、拒绝、监测）出入网络的信息流，且本身具有较强的抗攻击能力。它是提供信息安全服务，实现网络和信息安全的基础设施。防火墙实现网与网之间的访问隔离，以保护整个校园网络抵御来自其它网络的入侵者。

通过对全网网络拓扑结构进行分析，确定需要进行访问控制的网络边界位置，并使用防火墙等边界访问控制系统，解决边界安全问题、实现各个安全域间的网络访问控制。

**部署设备：防火墙**

#### 网络入侵检测系统

入侵检测产品是一种对网络深层威胁行为（尤其是那些防火墙所不能防御的威胁行为）进行抵御的安全产品，通常以串行方式透明接入网络。和其他安全产品不同的是，入侵防御产品的主要防御对象是网络上TCP/IP的四层以上的实时恶意数据流（四层以下的攻击可以由其他安全产品如防火墙等防御）。在本方案中入侵防御系统主要保护对外提供服务的业务系统的安全。在现有网络中部署入侵检测与防御系统可以对访问达州技师学院信息系统进行实时监测，并进行入侵行为跟踪分析。

**部署设备：入侵检测系统**

#### 网络恶意代码防范

浏览器都能解释和执行来自 Web 服务器的嵌入到 Web 页面下载部分的脚本（用 JavaScript、JScript、VBScript 等脚本语言创建）。当攻击者向用户提交的动态表单输入恶意代码时，就会产生跨站点脚本 (XSS) 攻击或是SQL注入。Web应用防火墙主要针对Web服务器进行第7层流量分析，防护以Web应用程序漏洞为目标的攻击，并针对Web应用访问进行各方面优化，以提高Web或网络协议应用的可用性、性能和安全性，确保业务应用能够快速、安全、可靠地交付。同时，校园网内部师生也会通过互联网对外进行访问，Internet网络区域的安全风险级别最高，所以对于对外访问和信息获取等操作都应进行实时的恶意代码检测和事后的清除修复工作。

对于恶意代码的防范应达到如下要求：

* 应在网络边界及核心业务网段处对恶意代码进行检测和清除；
* 应维护恶意代码库的升级和检测系统的更新；
* 应支持恶意代码防范的统一管理。

**部署设备：web应用防火墙**

#### 边界完整性保护

边界完整性检查核心是要对内部网络中出现的内部用户未通过准许私自联到外部网络的行为进行检查，维护网络边界完整性。通过部署终端准入控制系统可应对此类问题。

终端准入控制系统其中一个重要功能模块就是非法外联控制，探测内部网中非法上互联网的计算机。非法外联控制功能模块可发现用户非法自行建立通路连接非授权网络的行为，通过其对应的非法外联管理功能，可以防止用户访问非信任网络资源及由于访问非信任网络资源而引入安全风险或者导致信息泄密。

#### 边界安全审计

各安全区域边界已经部署了相应的安全设备负责进行区域边界的安全隔离。对于流经各主要边界（数据中心区域、校园网互联网边界区域）需要设置必要的审计机制，进行数据监视并记录各类操作，通过审计分析能够发现跨区域的安全威胁，实时地综合分析出校园网中发生的安全事件。本项目中开启边界安全设备的审计功能模块，根据审计策略进行数据的日志记录与审计。同时将所有审计信息通过安全管理中心进行统一集中管理，为安全管理中心提供必要的边界安全审计数据，利于管理中心进行全局管控。并部署网络审计系统，实现对于所有访问业务系统的行为的审计，并能够记录该行为的源IP、目的IP等，并可以方便的生成报表等。网络审计系统通过网络旁路侦听的方式对网络数据流进行采集、分析和识别，并对应用层协议进行完整还原，根据制定的安全审计策略进行审计响应。将边界安全审计、主机审计、应用审计和网络审计等一起构成完整的、多层次的审计系统。

### 通信网络安全保护设计

根据达州技师学院网络现状，应从链路冗余设计、通信网络安全审计及网络可信接入方面进行展开设计。

#### 网络结构安全

网络结构的安全是网络安全的前提和基础，对于数据中心网络，选用主要网络设备时会充分考虑业务处理能力的高峰数据流量，考虑冗余空间满足业务高峰期需要；网络各个部分的带宽需要保证接入网络和核心网络满足业务高峰期需要。

按照校园业务系统服务的重要次序定义带宽分配的优先级，在网络拥堵时优先保障重要主机；合理规划路由，在业务终端与业务服务器之间建立安全路径；绘制与当前运行情况相符的网络拓扑结构图；根据各子系统的业务属性以及系统需求，划分不同的网段或VLAN。保存有重要业务系统及数据的重要网段不能直接与外部系统连接，需要和其他网段隔离，单独划分区域。

#### 网络行为安全审计

为满足等级保护要求中对三级系统通信网络安全审计要求，需在网络中建立基于网络的安全审计措施，以实现通信网络安全审计的防护要求。

在网络中应部署数据库审计系统，可以通过网络端口镜像的方式抓取进、出区域边界数据包，基于数据包的源地址、目的地址、传输层协议、请求的服务等应用访问行为，确定行为符合安全策略，并以收集的记录信息作为追踪违规事件、界定安全责任的主要依据。

#### 网络实名准入系统

对于三级系统需建立网络接入认证机制，可采用由密码技术支持的可信网络连接机制，通过对连接到网络的设备进行可信检验，确保接入网络的设备真实可信，防止设备的非法接入。

为保证达州技师学院信息系统对接入用户实行全生命周期的数字身份管理，有效管理校内师生用户的访问凭证和接入权限，记录用户的网络访问行为，在发生信息安全事件时，能将责任追溯到人，本项目将沿用终端准入EAD系统，从而实现网络可信接入和用户的身份级别，需求功能包括：

**终端准入功能**

利用终端管理系统与交换机配合，如采用802.1x共同完成网络准入控制。

**限制非法外联。**

应设定只有与终端管理系统通讯的网卡才能发送和接收数据除，禁止其他任何网卡发送和接收数据，包括多网卡、拨号连接，VPN连接等。

**终端审计**

包括“文件操作审计与控制”，“打印审计与控制”，“网站访问审计与控制”，“异常路由审计”和“终端Windows登录审计”。所审计的内容尽量只与内网安全合规相关的信息，不对涉及终端用户的个人隐私信息，保证在达到合规管理的审计要求的前提下，保护终端用户个人私隐。

#### 网络设备保护

对于网络中的基础设施资产的管理，包括：网络设备、安全设备、服务器和数据库等，均需要通过堡垒机实现对重要业务资产操作的认证、授权和操作记录审计的要求，同时降低运维人员的管理成本，提高运维效率，通过运维堡垒主机的方式进行集中管理、协议代理和身份授权分离的安全操作。

**资源集中管理：**集中的资源访问入口、集中帐号管理、集中授权管理、集中认证管理、集中审计管理等等。

**协议代理：**为了对字符终端、图形终端操作行为进行审计和监控，对各种字符终端和图形终端使用的协议进行代理，实现多平台的操作支持和审计，例如Telnet、SSH、FTP、Windows平台的RDP远程桌面协议，Linux/Unix平台的X Window图形终端访问协议等。

当运维机通过堡垒主机访问服务器时，首先由堡垒主机模拟成远程访问的服务端，接受运维机的连接和通讯，并对其进行协议的还原、解析、记录，最终获得运维机的操作行为，之后堡垒主机模拟运维机与真正的目标服务器建立通讯并转发运维机发送的指令信息，从而实现对各种维护协议的代理转发过程。在通讯过程中，堡垒主机会记录各种指令信息，并根据策略对通信过程进行控制，如发现违规操作，则不进行代理转发，并由堡垒主机反馈禁止执行的回显提示。

**身份授权分离：**在堡垒主机上建立主帐号体系，用于身份认证，原各IT系统上的系统帐号仅用于系统授权，这样可以有效增强身份认证和系统授权的可靠性，从本质上解决帐号管理混乱问题，为认证、授权、审计提供可靠的保障。

#### 通信完整性

信息的完整性设计包括信息传输的完整性校验以及信息存储的完整性校验。

对于信息传输和存储的完整性校验可以采用的技术包括校验码技术、消息鉴别码、密码校验函数、散列函数、数字签名等。

#### 通信保密性

应用层的通信保密性主要由应用系统完成。在通信双方建立连接之前，应用系统应利用密码技术进行会话初始化验证；并对通信过程中的敏感信息字段进行加密。

### 安全管理中心设计

建立安全管理中心，形成具备基本功能的安全监控信息汇总枢纽和信息安全事件协调处理中心，提高对校园网和重要业务系统信息安全事件的预警、响应和安全管理能力。具体来说应该实现以下功能：

1. 安全信息采集

采集校园网内所有的网络设备（交换机、路由器等）、安全设备（防火墙、入侵检测、安全审计设备等）和重要业务系统（操作系统、数据库、中间件等）的安全事件信息。

2. 安全信息分析

对汇集的安全事件信息进行综合的关联分析，从海量的信息中挖掘、发现可能的安全事件并且提前预警。

3. 信息安全管理

实现统一的安全事件、安全策略、安全风险和信息安全支撑系统的管理，实现安全运维流程的自动化管理，满足校园安全管理中心对安全事件及时响应处置的需求。

4. 可视化展示

实现整体安全态势的多维度、多视角的展示，实现系统运行和安全监测的全景化和在线化。

#### 建设目标

安全管理中心的建设目标是为了支撑安全运行体系的建设和流转，从而提升安全防护能力、隐患发现能力、监控预警能力以及响应恢复能力，以保障达州技师学院信息系统的安全可靠，实现安全运行工作的“可感知”、“可管理”、“可测量”、“可展示”。

1.“可感知”目标：安全管理中心具备对校园网内各类安全资产的脆弱性和海量安全事件的采集、分析、处理报告能力，可以按需展现全网安全资产的脆弱性分布状况和高危风险事件分布状况，可集中管理各类安全资产的配置基线，能够智能化分析安全事件对业务系统可能产生的实际影响和潜在危害，实现化被动防御为主动安全的目标。

2.“可管理”目标：初步实现集中化的安全风险、安全事件、安全预警和安全策略、安全合规性和绩效考核管理，实现安全运维流程的自动化管理，满足达州技师学院对安全事件及时有效响应处置的需求。

3.“可测量”目标：安全管理中心具备针对各类信息安全管理标准或要求的符合性测量检查能力，提供针对诸如信息安全管理体系标准要求、等级保护要求、信息安全专项工作要求的符合性检查功能，支持通过技术手段实现符合性检查工作的自动调度、自动执行、自动核查、自动报告功能。

4.“可展示”目标：实现校园网整体安全态势的多维度、多视角的展示，实现系统运行和安全监测的全景化和在线化。针对达州技师学院决策层、管理层和执行层等不同角色提供不同展现视图，可以向PC、移动终端上推送当前各业务系统风险管理状态和趋势。

#### 总体结构

综合管理平台门户作为整个安全管理中心统一人机界面接口，采用Web应用架构，支持各功能模块的信息展示和系统配置管理。针对不同用户角色的特点，提供不同视角（决策层、管理层、执行层）的展现内容。安全态势感知系统是安全管理中心的大脑，负责安全管理中心核心功能的承载。其技术架构图如下：

图形用户界面, 应用程序

描述已自动生成

该架构可划分为四个层次，数据采集层、计算存储层、业务能力层和系统服务层。

（1）数据采集层

主要采集网络入口处防火墙日志、入侵检测日志，网络中关键主机日志以及主机漏洞信息，接入威胁情报。由于不同数据源对网络安全事件的定义通常具有不同的格式，还需要通过范式处理将数据归一化为统一格式，然后进行去除冗余及噪声数据。

（2）计算存储层

采用Hadoop MapReduce和Spark构建大数据计算、存储平台。大数据存储支撑态势感知的海量日志存储与处理；大数据的快速处理为高速网络流量的深度安全分析提供了技术支持，为高智能模型算法提供计算资源。

（3）业务能力层

通过云沙箱引擎、Web安全引擎、安全分析引擎、云化运维引擎和智能学习引擎协同工作，通过融合、归并和关联底层多个检测设备提供的安全事件信息，从整体上动态反映网络安全情况，并对网络安全的发展趋势进行预测和预警。采用数据级（基础数据驱动）、特征级（安全事件驱动）、决策级（初级态势信息驱动）的分层数据处理融合分析模型，能够为不同目的的应用提供不同级别的信息，增强了分析模型的可用性和分析的全面性和准确性。

（4）系统服务层

通过安全态势感知和情报中心感知网络状态、受攻击情况、攻击来源，掌握校园网安全状况和发展趋势，制定有预见性的应急预案，做好相应的防范准备。通过安全云服务中心构建关键信息基础设施安全体系，增强校园网安全防御能力和威慑能力。在安全告警事件的基础上提供统一的网络安全高层视图，能够快速准确地把握网络当前的安全状态，从而支持对安全态势的全局理解和及时做出正确的响应。

## 安全管理方案设计

安全管理体系的作用是通过建立健全组织机构、规章制度，以及通过人员安全管理、安全教育与培训和各项管理制度的有效执行，来落实人员职责，确定行为规范，保证技术措施真正发挥效用，与技术体系共同保障安全策略的有效贯彻和落实。信息安全管理体系主要包括组织机构、规章制度、人员安全、安全教育和培训等四个方面内容。

### 安全策略与制度管理

根据安全管理制度的基本要求制定各类管理规定、管理办法和暂行规定。从安全策略主文档中规定的安全各个方面所应遵守的原则方法和指导性策略引出的具体管理规定、管理办法和实施办法，是具有可操作性，且必须得到有效推行和实施的制度。

制定严格的制定与发布流程，方式，范围等，制度需要统一格式并进行有效版本控制；发布方式需要正式、有效并注明发布范围，对收发文进行登记。

信息安全领导小组负责定期组织相关部门和相关人员对安全管理制度体系的合理性和适用性进行审定，定期或不定期对安全管理制度进行评审和修订，修订不足及进行改进。

### 安全管理机构和人员

1. 根据基本要求设置安全管理机构的组织形式和运作方式，明确岗位职责；
2. 设置安全管理岗位，设立系统管理员、网络管理员、安全管理员等岗位，根据要求进行人员配备，配备专职安全员；
3. 成立指导和管理信息安全工作的委员会或领导小组，其最高领导由学校单位主管领导委任或授权；
4. 制定文件明确安全管理机构各个部门和岗位的职责、分工和技能要求。
5. 建立授权与审批制度；
6. 建立内外部沟通合作渠道；

定期进行全面安全检查，特别是系统日常运行、系统漏洞和数据备份等。

人员安全管理主要包括人员录用、离岗、考核、教育培训等内容。

一般学校都有统一的人事管理部门负责人员管理，这里的人员安全管理主要指对关键岗位人员进行的以安全为核心的管理，例如对关键岗位的人员采取在录用或上岗前进行全面、严格的安全审查和技能考核，与关键岗位人员签署保密协议，对离岗人员撤销系统帐户和相关权限等措施。

只有注重对安全管理人员的培养，提高其安全防范意识，才能做到安全有效的防范，因此需要对各类人员进行安全意识教育、岗位技能培训和相关安全技术培训。培训的内容包括单位的信息安全方针、信息安全方面的基础知识、安全技术、安全标准、岗位操作规程、最新的工作流程、相关的安全责任要求、法律责任和惩戒措施等。

### 安全建设管理

系统建设管理的重点是与系统建设活动相关的过程管理，由于主要的建设活动是由服务方，如集成方、开发方、测评方、安全服务方等完成，学校的主要工作是对之进行管理，应制定系统建设相关的管理制度，明确系统定级备案、方案设计、产品采购使用、软件开发、工程实施、验收交付、等级测评、安全服务等活动的管理责任部门、具体的管理内容和控制方法，并按照管理制度落实各项管理措施，完整保存相关的管理记录和过程文档。

### 安全运维管理

（1）环境和资产安全管理制度

环境包括计算机、网络机房环境以及设置有网络终端的办公环境，明确环境安全管理的责任部门或责任人，加强对人员出入、来访人员的控制，对有关物理访问、物品进出和环境安全等方面作出规定。对重要区域设置门禁控制手段，或使用视频监控等措施。

资产包括介质、设备、设施、数据、软件、文档等，资产管理不等同于设备物资管理，而是从安全和信息系统角度对资产进行管理，将资产作为信息系统的组成部分，按其在信息系统中的作用进行管理。应明确资产安全管理的责任部门或责任人，对资产进行分类、标识，编制与信息系统相关的软件资产、硬件资产等资产清单。

（2）设备和介质安全管理制度

明确配套设施、软硬件设备管理、维护的责任部门或责任人，对信息系统的各种软硬件设备采购、发放、领用、维护和维修等过程进行控制，对介质的存放、使用、维护和销毁等方面作出规定，加强对涉外维修、敏感数据销毁等过程的监督控制。

（3）日常运行维护制度

明确网络、系统日常运行维护的责任部门或责任人，对运行管理中的日常操作、账号管理、安全配置、日志管理、补丁升级、口令更新等过程进行控制和管理；制订设备操作管理、业务应用操作管理、变更控制和重用管理、信息交换管理相应的管理制度；制定与信息系统安全管理相配套的规范和操作规程并落实执行；正确实施为信息系统可靠运行而采取的各种检测、监控、审计、分析、备份及容错等方法和措施，对运行安全进行监督检查。

（4）集中安全管理制度

第三级以上信息系统应按照统一的安全策略、安全管理要求，统一管理信息系统的安全运行，进行安全机制的配置与管理，对设备安全配置、恶意代码、补丁升级、安全审计等进行管理，对与安全有关的信息进行汇集与分析，对安全机制进行集中管理。

（5）事件处置与应急响应制度

按照国家有关标准规定，确定信息安全事件的等级。结合信息系统安全保护等级，制定信息安全事件分级应急处置预案，明确应急处置策略，落实应急指挥部门、执行部门和技术支撑部门，建立应急协调机制。落实安全事件报告制度，第三级以上信息系统发生较大、重大、特别重大安全事件时，学校应按照相应预案开展应急处置，并及时向受理备案的公安机关报告。组织应急技术支撑力量和专家队伍，按照应急预案定期组织开展应急演练。

（6）灾难备份制度

要对第三级以上信息系统采取灾难备份措施，防止重大事故、事件发生。识别需要定期备份的重要业务信息、系统数据及软件系统等，制定数据的备份策略和恢复策略，建立备份与恢复管理相关的安全管理制度。

（7）安全监测制度

开展信息系统实时安全监测，实现对物理环境、通信线路、主机、网络设备、用户行为和业务应用等的监测和报警，及时发现设备故障、病毒入侵、黑客攻击、误用和误操作等安全事件，以便及时对安全事件进行响应与处置。

（8）其他制度

对系统运行维护过程中的其它活动，如系统变更、密码使用等进行控制和管理。按国家密码管理部门的规定，对信息系统中密码算法和密钥的使用进行分级管理。

### 安全管理制度汇总

制定安全检查制度，明确检查的内容、方式、要求等，检查各项制度、措施的落实情况，并不断完善。定期对信息系统安全状况进行自查，第三级信息系统每年自查一次，第四级信息系统每半年自查一次。经自查，信息系统安全状况未达到安全保护等级要求的，应当进一步开展整改。

最终提交安全制度包括但不限于以下内容：

* 总体安全策略（组织、流程、策略、技术）
* 岗位安全责任制度
* 第三方安全管理制度
* 系统日常安全管理工作制度
* 系统安全评估管理办法
* 机房建设运行标准
* 安全区域划分及管理规定
* 管理信息区域网管制度
* 系统建设管理制度
* 设备入网安全管理制度
* 系统软件和补丁管理制度
* 备份与恢复管理制度
* 账号和口令及权限管理制度
* 介质管理
* 加密技术使用管理办法
* 应急预案管理制度
* 安全事件报告和处置管理制度
* 安全审计管理

# 超融合数据中心扩容建设

### 方案建设思路

IT基础设施是由上层应用的发展决定，现在云计算以及虚拟化技术已经深刻的改变了IT基础架构，必须能够优化计算、网络和存储资源之间的关系，实现真正的灵活部署以及弹性扩展，才能支撑起IT瞬息变化的需求。从近些年IT基础设施的发展可以得出如下结论：硬件平台单一化，越来越多的IT设备均由X86服务器承载；专用设备软件化，即通过软件定义技术实现灵活的业务部署。

基于此发展趋势，超融合设备成为基础设施领域最热门的产品。图表, 瀑布图

描述已自动生成

HCI超融合是实现“软件定义数据中心”的终极技术途径。HCI类似Google、Facebook等互联网数据中心的大规模基础架构模式，可以为数据中心带来最优的效率、灵活性、规模、成本和数据保护。使用计算存储超融合的一体化平台，替代了传统的服务器加集中存储的架构，使得整个架构更清晰简单。

相比分离式的计算存储虚拟化，超融合在提供存储的同时，也提供计算能力，这不但大量减少了硬件投入和电力成本，也将计算放在离存储更近的地方，达到最优的性能。超融合架构通常采用了全分布式的组件，横向可扩展，不存在单点失效，数据能够自动恢复和备份，性能优势非常明显，是目前国际上主流科技公司普遍采用的IT基础架构，也是未来IT基础架构的方向。

下表列举了使用超融合架构（计算+存储）和传统数据中心三层架构（服务器+光纤交换机+存储）的对比：

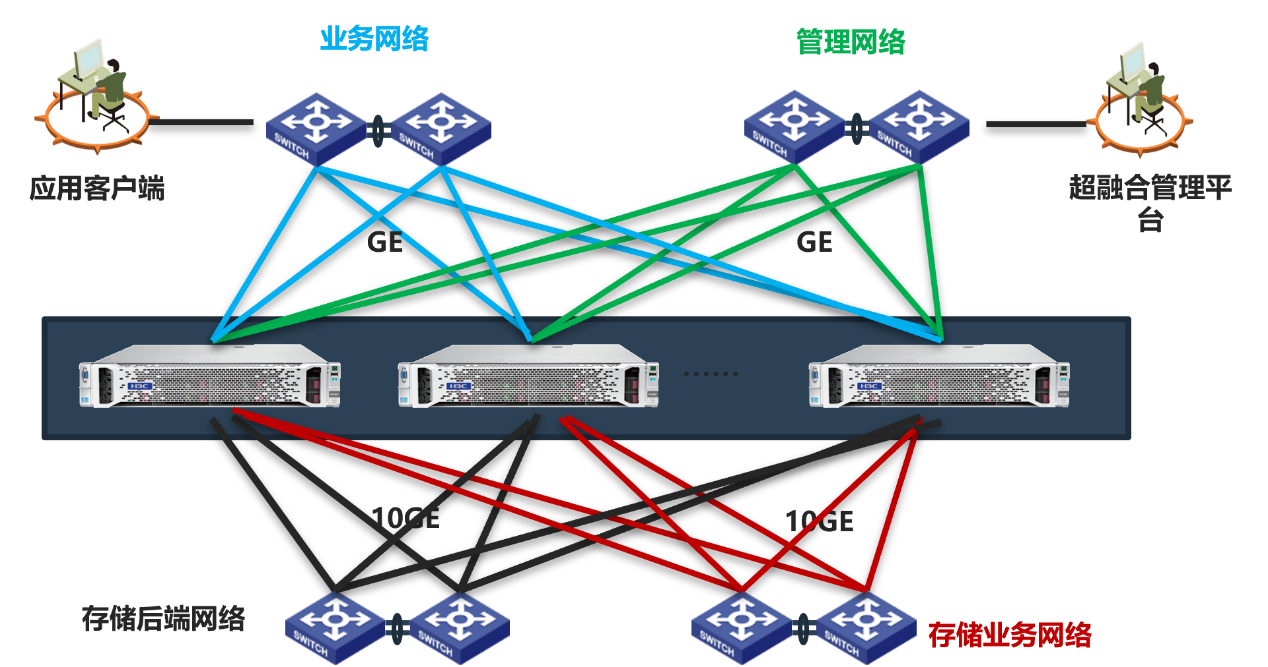
|  | 超融合架构 | 传统数据中心基础架构 |
| --- | --- | --- |
| 性能 | 尽可能提供本地吞吐，并使用SSD保证应用IO需求。不存在性能瓶颈 | 随着访问集中存储的服务器越来越多，性能瓶颈将日益凸显 |
| 横向扩展 | 可以简单的在集群中增加节点以扩展集群规模和性能 | 由于架构限制，无法实现横向扩展 |
| 高可用性 | 可以通过三副本的方式容忍最多两个节点同时故障，并且硬件故障时数据重建速度快，性能几乎不受影响 | 通过raid技术实现高可用性，但面对硬件故障时，性能下降严重。 |
| 整合比 | 虚拟机密度高，是传统2倍以上 | 虚拟机密度低 |
| 安装配置 | 开箱即用的部署方式，只需30分钟即可完成安装配置 | 需要准备大量安装实施前的信息收集和整理工作，并且由专人进行安装部署，最少需要2天时间 |
| 管理维护 | 统一WEB界面管理，维护方便  无需配置LUN、卷、Raid组 | 需要专门存储管理软件，配置复杂。需要厂商支持。 |
| 空间占用 | 使用超融合架构：2台4U高，总共包含8个节点（包含服务器和存储）  总共占用空间4U | 使用传统架构：8台2路服务器至少占用8U，存储至少需要3U  总共占用空间11U |
| 耗电 | 使用超融合架构：2台8节点，共耗电 2000W  运行三年电费支出约：5.5万元 | 使用传统架构：8台服务器平均每台服务器耗电600W计算，存储耗电1500w，总共耗电6300W  运行三年电费支出约为：16.8万元 |

基于以上项目背景及建设思路，本次建设在原有超融合基础上，扩容7个节点的超融合，无缝接入原数据中心系统，融合了计算、网络、存储和安全四大模块，通过全虚拟化的方式构建IT架构资源池。所有的模块资源均可以按需部署，灵活调度，动态扩展。通过超融合一体机或者超融合操作系统能够在最短的时间内，将业务系统安全、稳定、高效的迁移到超融合平台中，并且为后期迈向私有云平台奠定基础，从而能够实现云服务目录、多租户的管理及计费审计等功能。

超融合架构解决方案软件架构主要包含服务器虚拟化、存储虚拟化、网络虚拟化超融合管理平台等。

### 方案拓扑架构

本次新增7台服务器部署了所有业务系统，采用全实体机的方式，每个服务器运行1-2个业务系统。总体拓扑设计如下：



|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 网络规划 | 端口类型 | 组网 | 建议端口数量 | 承载数据 |
| 存储业务网 | 万兆 | 独立组网，建议双链路 | 2 | 计算虚拟化与分布式存储数据交互、ONEStor MON管理集群、OSD前端心跳报文 |
| 存储后端网络 | 万兆 | 独立组网，建议双链路 | 2 | 数据副本复制、硬盘或节点故障时数据重构、ONEStor OSD后端心跳 |
| 业务网 | 至少千兆 | 独立组网，建议双链路 | 2 | 业务访问数据 |
| 管理网 | 至少千兆 | 独立组网，建议双链路 | 2 | 主机及虚拟机软件管理报文（包括HA、集群心跳等报文）、迁移数据 |

# 网络建设与运维运技能赛项建设

一、建设背景

本竞赛旨在贯彻党中央、国务院对职业教育工作的决策部署，响应党的二十大提出的“加快建设网络强国、数字中国”的国家战略，适应国产自主且安全可控的新诉求和信息技术应用创新产业的发展，通过产教协同发展，培养中职网络建设与运维方向高素质网络技术人才，促进数字化转型升级，服务信息基础建设和国家战略。以立德树人为根本任务，推进“三全育人”、深化“三教改革”，发挥树旗、导航、定标、催化作用，培养德智体美劳全面发展网络技术相关专业的高素质劳动者和技术技能人才。

二、建设需求

**（一）竞赛主要内容**

本赛项设置网络理论测试、网络建设与调试、服务搭建与运维三个模块，竞赛内容包括：职业规范与素养、网络布线与施工、网络设备配置与调试、安全策略配置、网络安全防护和应急响应、云平台网络连接、X86与ARM架构计算机操作系统安装与管理、Windows与Linux服务配置、网络运维等内容。各模块有机结合，比赛过程中，要求两名参赛选手按照题目独立完成理论测试，合理分工，安排工作流程、合作完成模块二和模块三等有关网络建设与运维职业典型工作任务，检验选手专业核心能力与职业综合能力。

**（二）重点考查技能**

重点考查参赛选手的网络理论的掌握以及灵活运用的实战能力，具体包括：

1．能够全面正确理解网络基本知识理论，考查选手的专业可持续发展能力。

2．能够根据提供的竞赛要求，读懂文档需求，理解业务架构，实现项目应用，检验网络实施规划统筹的综合规划能力。

3．能够完成线缆制作、合理划分网络地址，配置路由器、交换机、无线控制器、无线AP和防火墙等网络设备，实现网络的正常运行，考核综合布线和设备安装调试专业实践能力。

4．能够根据业务需求和应用环境，安装部署各类服务器、数据库、存储等相关服务；并根据网络业务需求配置各种策略，以达到网络互联互通，实现云平台和网络资源适应业务需求，考核多样化环境下系统部署和数据库应用的专业实践能力。

5．能够预判网络运行中所面临的安全威胁，防范并解决网络恶意攻击行为；考查选手防御不良信息及病毒、构建和维护绿色网络的专业实战能力。

6．能够通过竞赛前发布的竞赛设备列表、配套技术文档、赛项规程和公开赛题等信息，分析网络架构、查找技术资料；能够根据临场30%竞赛要求变化，结合技术原理，参考设备技术文档进行现场任务解决，检验了参赛团队整体的文档理解、项目执行、故障解决、网络运维等各项综合专业能力。