**招标项目采购需求**

说明：

1.本招标文件所称中小企业必须符合《政府采购促进中小企业发展暂行办法》第二条规定。

按照《财政部、司法部关于政府采购支持监狱企业发展有关问题的通知》（财库〔2014〕68号）之规定，监狱企业视同小型、微型企业。

按照财库〔2017〕141号三部门联合发布关于促进残疾人就业政府采购政策的通知，残疾人福利性单位，视同小型、微型企业。

2.小型和微型企业产品的价格给予6%-10%的扣除，用扣除后的价格参与评审，具体扣除比例请以第四章《评标办法及评标标准》的规定为准。

3.小型、微型企业提供中型企业制造的货物的，视同为中型企业。

4.小型、微型企业提供大型企业制造的货物的，视同为大型企业。

**5.根据财库〔2019〕9号及财库〔2019〕19号文件规定，台式计算机，便携式计算机、平板式微型计算机，激光打印机，针式打印机，液晶显示器，制冷压缩机（冷水机组、水源热泵机组、溴化锂吸收式冷水机组），空调机组[多联式空调（热泵）机组（制冷量＞14000W），单元式空气调节机（制冷量＞14000W）]，专用制冷、空调设备（机房空调），镇流器（管型荧光灯镇流器），空调机[房间空气调节器、多联式空调（热泵）机组（制冷量≤14000W）、单元式空气调节机（制冷量≤14000W）]，电热水器，普通照明用双端荧光灯，电视设备[普通电视设备（电视机）]，视频设备（视频监控设备、监视器），便器（坐便器、蹲便器、小便器），水嘴均为节能产品政府采购品目清单内标注“★”的品目，属于政府强制采购节能产品。若采购货物属于以上品目清单的产品时，投标人的投标货物必须使用政府强制采购的节能产品，投标人必须在投标文件中提供所投产品的节能产品认证证书复印件（加盖投标人公章），否则作无效投标处理。**

**6．本章采购需求表中，凡标注“▲”号的条款为关键指标或要求，不允许有负偏离，否则投标无效。**

**7.“项目需要及技术需求”中除已列明“如有请提供”外，其余未标注“▲”号的项目条款或技术要求有负偏离（或未作响应）达3项（含）数以上的投标无效。**

8.投标人必须自行为其投标产品侵犯其他投标人或专利人的专利成果承担相应法律责任；同时，具有产品专利的投标人应在其投标文件中提供与其自有产品专利相关的有效证明材料，否则，不能就其产品的专利在本项目投标过程中被侵权问题提出异议。

9.如本项目有硬件设备要求的，采购需求中参考品牌、型号及技术参数性能（配置）不明确或有误的，或投标人选用其他品牌型号替代的，请说明品牌型号和详细的技术参数性能（配置）同时填写“设备配置清单”和“技术偏离表”。

10.招标文件中所要求提供的证明材料，如为英文文本的请同时提供中文译本。

11.项目采购需求具有国家或其他强制性标准、规范等要求的，投标文件中必须提供相关强制性认证资料，否则投标无效。

12.本采购需求中技术要求所使用的标准或应用标准如与投标人所执行的标准不一致时，按最新标准或较高标准执行。

13.**评标委员会认为投标人的报价明显低于其他通过符合性审查投标人的报价，有可能影响产品质量或者不能诚信履约的，应当要求其在评标现场合理的时间内提供书面说明，必要时提交相关证明材料；投标人不能证明其报价合理性的，评标委员会应当将其作为无效投标处理**。

**14.投标人可选择其中一个分标参与投标也可选择所有分标参与投标，但只能成为一个分标的中标人。由评标委员会根据各投标人综合得分进行排名，按A分标→B分标的顺序推荐中标候选人。A分标第一中标候选人（如为联合体的，含联合体任意一方）不可同时作为B分标中标候选人。**

|  |  |  |  |
| --- | --- | --- | --- |
| **一、项目要求及技术需求** | | | |
| 项号 | 采购标的 | 数量 | 项目需要及技术需求 |
| 1 | 广西教育网建设项目教育骨干网网络服务租用 | 1项 | **一、项目概况**  1.1项目建设目标、规模  1.1.1项目建设目标  广西教育网是万兆主干、千兆到学校、百兆到班级的，分层的教育信息网络系统，由教育骨干网、教育城域网和各级各类学校校园网组成。广西教育网的各级教育机构和各级各类学校都使用统一的数据标准进行信息传递，而且对外公开提供标准化的数据和功能接口，可以和遵守标准接口的第三方应用程序挂接。广西教育网将建成覆盖全区各级各类学校，支持各级各类教育教学信息化的，集数据、语音、视频服务于一体的，高带宽低延时的，支持IPv6部署和应用的，具有自主管理的，拥有统一管理公共IP地址的，拥有统一管理的全球域名的，满足“云、网、端”架构下开展各级各类教育教学的教育行业专用网络。  1.1.2项目建设规模  广西教育网由自治区教育厅统筹规划建设，连接自治区城乡各级各类学校和教育机构，是支撑培养造就德智体美劳全面发展的社会主义建设者和接班人的教育行业专用网络，是教育信息化基础设施的重要组成部分。具体建设规模如下：  1.1.2.1业务领域  搭建在满足“云、网、端”架构下开展各级各类教育教学的网络环境，实现各级各类教育应用互联互通，教育资源、教育数据全网共享。  1.1.2.3覆盖范围  纵向：包括广西教育数据中心、14个设区市、118个县（市、区）的各级各类学校和教育机构。  横向：涵盖学前教育、中小学教育、中等职业教育、高等教育、教育督导、教育科研、教育技术和信息化等业务部门。  1.1.2.4用户规模  本项目服务范围将覆盖广西全区1.96万所大中小院校、18.9万个班级、836万名在读学生和46万名任课教师，广西教育网与互联网、电子政务外网、中国教育网等外部系统实现互通。  **二、本次项目建设要求**  2.1广西教育网由教育骨干网、教育城域网和校园网三部分构成，将各级各类教育机构和学校连接起来，为将来统一教育管理平台、管理教育大数据、推广智慧教学应用等工作，构建网络基础条件。  2.2通过建设教育骨干网核心节点，组建教育骨干网核心环路，在各设区市建立市级汇聚节点（高校城市节点），连接至各核心节点，建成教育骨干网。在各设区市、县建立汇聚节点，各级学校建设校园网，连接至各设区市、县汇聚节点，形成设区市本级、县级教育城域网。各设区市、县级教育城域网连接教育骨干网市级汇聚节点，形成完整统一的教育基础网络。  本次项目招标教育骨干网，建设要求如下：  2.2.1.网络中心  （1）在教育骨干网的核心及汇聚节点设立网络中心，可以与目前各节点核心机房共用，各设区市本级、县级教育城域网、跨县域的教育城域网根据情况设立不同规模的网络中心。  （2）网络中心主要用于为教育网提供运行环境和运维保障，建设内容主要包括机房运行环境、网络设备及运维系统、网络安全设备和系统等。机房运行环境主要包括机房装修，以及电力、空调、消防、门禁、监控等子系统。网络设备及运维系统主要包括路由器、交换机、身份认证、缓存加速、机柜及配套设施、网络管理运维等子系统。网络安全设备和系统主要包括入侵防御检测、防DDOS攻击、防病毒、上网行为管理、实名审计、实名日志等子系统。  2.2.2.教育骨干网  （1）教育骨干网是指在广西行政区域范围内，利用计算机网络技术，以光纤为传输介质的，连接全区各教育城域网、高等院校校园网、区直中等职业学校校园网的，由核心节点、高校城市节点、主干光纤传输线路组成的网络。  （2）教育骨干网及各端纵向接入城域网，实现与线路两端的互通。鉴于教育骨干网的重要性，教育骨干网核心线路需具备自愈环保护功能，针对线路经过的骨干核心层，采取不同路径的物理链路在教育骨干网节点连接形成双路由保护，如其中一条线路阻断时，另一条线路仍能正常使用，以保证业务能够正常运行，不受单条线路故障影响。  2.2.3.安全系统  （1）本项目网络安全建设的最终目标是使教育骨干网符合网络安全等级保护第三级要求。  （2）本项目统筹规划教育骨干网和广西教育数据中心的网络安全设计和建设，统一实施网络安全的管理和运维。依据《信息安全技术网络安全等级保护基本要求》（GBT22239-2019）等标准规范要求，教育骨干网的网络安全保护等级定级第三级，按网络安全等级保护第三级的要求进行设计、建设、管理和运维。  （3）本项目根据等级保护的指导思想，以技术保障为基础、以管理运维为抓手、以监测预警为核心、以协同响应为目标规划网络安全防御体系并落地为具体的安全建设方案。整个技术防护体系采取的主要安全措施要求如下：  1）采用防火墙系统对区域边界进行访问控制，根据业务需求，设置访问控制策略，定期进行安全策略的优化和维护。  2）采用入侵防御系统，并开启防火墙的防病毒模块（或部署防病毒网关），对网络入侵行为和网络层病毒进行检测和阻断，并进行告警。  3）采用专业抗APT攻击系统实现对新型网络攻击行为的检测、发现，并结合专家服务进行分析处置。  4）采用一体化终端安全管理系统、虚拟机化安全管理平台实现对物理主机、虚拟主机的安全防护，并对终端进行集中安全管控、集中病毒管理、统一补丁管理和安全审计。  5）采用SSL VPN实现对远程通信传输、远程终端数据的安全防护，实现基于互联网的传输加密和数据安全，并进行远程接入用户身份认证和访问控制。  6）采用堡垒机实现对设备的集中管理和运维审计，并实现运维管理日志的集中存储和安全运维。  7）应用系统开发同步考虑相关安全功能的实现，对重要的业务数据和系统鉴权数据进行加密存储。  8）采用应用身份认证服务平台实现对应用的双因素认证，并通过集成SSL VPN实现应用数据的传输安全。  9）采用网络审计系统、数据库审计系统、上网行为审计系统、一体化终端安全管理系统的审计功能实现对用户行为审计的全覆盖，并满足远程访问和上网行为审计需求。  10）采用态势感知管理信息系统和抗APT攻击系统实现全网安全设备日志和安全事件的统一分析和告警，实现对高级威胁和未知威胁的发现、检测和告警，并提供安全事件报表。  11）采用防火墙集中管理，与态势感知管理信息系统联动，实现全网防火墙的自动化策略优化、下发、维护，实现策略可视化。  12）采用数字证书认证系统（教育CA、广西政务CA等）进行教育网用户的身份认证，实现多因素身份认证。  2.2.4.建设原则  （1）可靠性：网络整体设计要求能可靠稳定承受业务信息的正常运行，在出现意外故障时尽可能保证业务可用，整体网络设计必须始终遵循可靠性第一的原则。  （2）安全性：具有多种有效手段，防范各种形式对网络的非法入侵和内部攻击，以保证网络的实体安全、网络安全、系统安全和信息安全，有效地保障正常的业务活动和防止内部信息数据不被非法窃取、篡改或泄漏。  （3）先进性：方案设计要采用先进的概念、技术和方法，整个系统的生命周期应有比较长的时间，保证在系统建成以后比较长的一段时间内能满足教学业务不断发展的需要。  （4）扩展性：系统必须具有良好的可扩充性，在结构、性能容量等方面必须具有升级换代的冗余性，整体网络设备应当采用模块化的结构，符合网络的发展趋势并具有充分的扩展性。  （5）高性能：网络链路和设备具备足够高的数据转发能力，保证各种信息的高质量传输；交换系统具有较高的交换容量与多业务服务支撑的能力，保证网络服务的质量。  （6）可管理性：整体网络必须具有较强的易于管理和维护的特性。  （7）开放性和标准化：网络方案设计必须遵循国际标准化组织提出的开放系统互联的标准，设备和系统能对第三方进行标准兼容，整体网络具有良好的可扩展性、可移植性和互操作性。  **三、设计方案要求（见本章附件“项目设计方案需求及要求”）** |
| **二、涉及项目的其他要求** | | | |
| ▲采购预算金额 | | A分标：439万元/年，B分标：461万元/年。 | |
| 采购标的需实现的功能或者目标 | | 见本表“项目需要及技术需求”。 | |
| 为落实政府采购政策需满足的要求 | | 具体见本招标文件“投标人须知”及“评标办法及评分标准”。 | |
| 规范标准 | | 采购标的需执行的国家标准、行业标准、地方标准或者其他标准、规范。多项标准的，按最新标准或较高标准执行。 | |
| 采购标的需满足的质量、安全、技术规格、物理特性等 | | 见本表“项目需要及技术需求”。 | |
| 采购标的需满足的服务标准、期限、效率等要求 | | 见本表“项目需要及技术需求”及“商务条款”。 | |
| 采购标的验收标准及要求 | | 符合国家标准、行业标准、地方标准，以及项目技术要求。 | |
| 其他技术、服务要求 | | 投标人结合自身能力，并根据项目要求于投标文件中提供详细的项目技术及实施方案（至少包括但不限于：技术方案、骨干网建设带宽性能和管理运维保障、出口带宽承诺、管理运维备品备件、实施团队、合理化建议、售后服务等）。 | |
| **三、投标人的资信要求** | | | |
| 政策性加分条件 | | 符合节能环保等国家政策要求。 | |
| 质量管理、企业信用要求 | | 见本招标文件第四章“评标办法及评分标准”。 | |
| 能力或业绩要求 | | 见本招标文件第四章“评标办法及评分标准”。 | |
| 原厂商授权 | | “项目需要及技术需求”中有特殊要求的，按其要求执行；未作要求的，如有请于投标文件中提供。 | |
| 产品资料及说明文件 | | 无 | |
| ▲**四、商务条款** | | | |
| 售后技术服务要求 | | 1.中标供应商负责网络设备、线路及机房租赁等服务的实施；负责相关设备的到货、安装、调试；负责线路的施工、调试；负责所提供设备、线路的监控及维护服务。  2.培训要求  （1）中标供应商及设备厂家在网络服务租用期间提供免费知识培训，选派优秀的培训讲师组建高素质的培训队伍，培训教员应具有丰富的理论知识和至少具有三年的教学经验，主要负责网络、平台的功能、性能、操作、维护及日常管理等方面的培训，以及系统原理、架构、设备的性能、操作使用、日常维护与故障排查等方面的培训。培训结束必须要进行考试。  （2）培训方式：集中面授、现场培训、网络培训等方式。  （3）通过培训达到如下几个目标：  1）熟悉现代常用通信网络技术。  2）了解各种网络业务产品。  3）熟练使用本项目网络应用设备，具有一定的系统维护、判断故障的能力和综合处理能力。  4）具备独立操作能力，能够进行日常维护，解决常见故障。  ①高校城市节点网络中心：要求培训达到具备联合判断故障和处理故障的能力，包括故障定位，业务配置等。  ②示范性高中和教育集团：如南宁二中、南宁三中、柳州高中等，除了具备基本的故障判断能力外，还要有业务配置和网络故障的运维处理能力。  ③城市、乡镇所在地学校：掌握交换机上的告警灯所示信息，能识别网络通断状态和表征，基本了解交换机使用说明。  ④农村学校（含教学点）：受训人员达到识别设备外观，判断网线、电源是否正常连接。  通过对采购单位的维修、操作和项目设计人员的培训，使受训人员在本项目的管理运维中能有效地操作、修理和检查各系统，确保整个项目的正常运行及工作开展。  3.投标文件中提供售后服务承诺书，在网络覆盖地（至少到县级）有专人实施网络服务的售后服务，提供售后服务机构及联系人名单，列明详细地址及联系方式；  4.提供7×24小时热线电话服务，并提供故障申告途径及绿色通道，做到全方位响应，并指定专人负责上门受理调试日常维护及平时协助采购人维护检测等工作；提供365×24小时的售后服务响应；  5.保证网络的畅通，供应商负责线路运营商到用户单位主干光缆所有设备的免费运行维护，如光端机、转换器等设备，如果主干网络出现问题，必须在接到报告后2个小时内到达现场，负责排除故障，直到网络恢复正常，如设备故障在4小时内无法解决的应免费提供备用设备及备件，确保网络正常运行；  6.每个季度对网络进行一次巡检，检查网络设备和主干光缆的运行情况，提交巡检报告；  7.当采购方网络需要扩展、迁移或升级时，供应商负责免费提供相应解决方案等技术支持；因供应商施工、网络割接等原因影响网络运行的，应当提前一天通知采购方，并且尽快消除故障、恢复网络通信线路。  8.投标人须另行书面承诺（格式自拟）并附在投标文件中，承诺合同执行期间，如遇国家新政策、标准、规范或规定更新的，中标人无条件根据新规要求负责对项目进行调整或优化。  9.中标供应商须按其投标文件提供的技术及实施方案、售后服务承诺的人员为采购人提供服务。在合同履行过程中，原则上不得更换项目服务人员，如确有需要更换的需经采购人同意，且所更换人员必须为同等条件人员。 | |
| 租用期及地点 | | 1.租用期：租用期3年，自完成教育骨干网建设，并验收合格之日起计算。  2.项目工期：2021年5月31日前完成教育骨干网建设并验收合格。  3.建设地点：广西区内采购人指定地点。[详见教育骨干网核心及汇聚节点规划；项目实施建设前，采购人可以调整承担高校城市节点网络中心的建设学校（在设区市内变更建设学校，或按本项目贵港市高校城市节点网络中心的处置方式由教育网核心节点临时托管），并确认具体建设地点，中标人须无条件配合]。 | |
| 付款条件 | | 1.合同签订之日起10日内，中标人应以支票、汇票、本票或者金融机构、担保机构出具的保函等非现金方式向采购人提供中标金额的2%履约保证金。待服务期满后，由中标人向履约保证金收取单位提供《广西壮族自治区政府采购项目合同验收书》及《采购项目履约保证金退付意见书》，履约保证金收取单位在收到合格材料后5个工作日内以银行转帐方式如数退还（不计利息）。涉及违约的违约金和损失赔偿从履约保证金中扣减。  2.合同总价包括中标人完成本项目采购要求所产生的全部费用（含税），采购人不再另行向中标人支付其他任何费用。  3.按中标金额分3年，逐年支付。合同签订后支付预付款145.2万元，其中A分标72.6万元，B分标72.6万元；之后按实际尾款分3年等额，逐年支付，于每年度结束后20个工作日内支付上年度服务费用。  4.中标人在每次收到合同款项后10个工作日内向采购人开具正式等额发票。  5.采购人可根据每年财政拨款情况提前支付或延后支付，若因采购人财政拨款问题导致采购人付款迟延的，采购人不承担责任。 | |
| 报价及其他要求 | | 1.要求为实现广西教育网服务能力建设，由投标人负责投入必要的设备设施，基本配置应达到采购单位提出的技术参数要求（见本章附件2“软硬件配置参考清单”），并符合国家有关质量安全标准。3年服务期满后，所投入本项目的信息资产（含软硬件系统设备，租用光纤线路除外）无偿归采购人所有。  2.本项目实行总承包报价；投标报价包含设备设施的投入、系统实施(含咨询）、软件开发、集成安装、运抵指定地点运输及装卸、现场安装调试、网络建设、第三方履约验收代理服务费用、各项保险、附加培训、售后服务、税金、利润及其他所有可能发生的一切费用及所有的不定因素的风险，合同履行过程中，采购人不再另行向中标人支付其他任何费用。 | |
| 项目验收要求 | | 1.在项目验收过程中，采购人将同时按照政府采购合同约定、招标文件及中标单位其投标文件承诺的条款进行逐项验收，如项目验收不合格，由中标供应商返工直至合格，有关返工、再行验收，以及给采购单位造成的损失等费用由中标供应商承担。连续两次项目验收不合格的，或发现成交供应商在投标文件中有弄虚作假的行为，或在投标文件中有针对技术商务条款有虚假响应情况的，采购单位将不予验收，并追究成交供应商的责任，由此带来的一切损失由中标供应商自行承担。  2.主要参考验收依据：  （1）《关于印发广西壮族自治区政府采购项目履约验收管理办法的通知》（桂财采〔2015〕22号）  （2）《关于印发广西壮族自治区电子政务工程建设项目管理暂行办法的通知》（桂发改高技〔2017〕732号）  （3）《国家政务信息化项目建设管理办法》（国办发〔2019〕57号）  3.履约验收：  （1）**验收过程中所产生的一切费用均由中标供应商承担。报价时应考虑相关费用**。  （2）本项目验收委托云之龙招标集团有限公司（以下简称“代理机构”）组织实施，由验收小组对照采购文件、采购合同（含补充协议）的要求全面核对检验，对所有要求出具的证明文件的原件进行核查，如不符合要求以及提供虚假承诺的，按相关规定做退货处理及违约处理，中标/成交供应商承担所有责任和费用，采购人保留进一步追究责任的权利。  （3）**每分标项目验收代理服务费，按每分标预算金额的0.3392%收取，由中标供应商一次性向代理机构付清**。  1）验收活动开始前，中标供应商应对所有服务工作及服务内容作出全面检查和对验收文件进行整理，并列出清单，作为采购人收货验收和使用的技术条件依据。  2）中标供应商一次性通过验收的，由验收小组出具结论报告，自验收合格之日起五个工作日内由中标供应商向代理机构一次性付清验收代理服务费。  3）采购委托采购代理机构组织的验收项目，其验收时间以该项目验收方案确定的验收时间为准，验收结果以该项目验收报告结论为准。在验收过程中发现中标供应商有违约问题，可暂缓资金结算，待违约问题解决后，方可办理资金结算事宜。  4）**中标供应商验收不合格的，再次验收的验收代理服务费每次均按首次收费标准收取，由中标供应商承担**；多次验收不合格导致退货（或不能继续履约）的，在收到采购人书面处理意见之日起，中标供应商须于五个工作日内向代理机构一次性付清验收代理服务费。  （4）本项目服务中，投标人承诺作为服务基础的在本项目投入的相关设备运送抵达指定现场后，中标供应商必须提供加盖单位公章的设备清单（包括货物名称、品牌、产地、规格型号、数量及产品附件等内容），采购单位或采购单位委托的第三方机构等多方组成验收小组，将同时对中标供应商承诺配备的所有货物进行检验和核实，若为进口产品的还需提供海关报关证明资料。  **（5）项目验收过程中，需质量监督检测机构介入的（如有），费用由中标供应商另行承担**。  （6）多次验收后，最终验收达不到要求的不予验收，视为验收不合格，采购单位可解除双方的合同。  （7）中标供应商最终服务前应按招标文件要求提供各类产品或服务检验合格的检测报告（如有）。  （8）本项目涉及范围广、金额大，在履约验收过程中存在多处材料对接，人员对接的情况，投标人、监理单位、履约验收代理等需要多方配合，投标人可根据自身的情况，对履约验收的相关内容提出相关建议及意见，以及合理实施化意见。  4.根据《国家政务信息化项目建设管理办法》（国办发〔2019〕57号）、《关于印发广西壮族自治区电子政务工程建设项目管理暂行办法的通知》（桂发改高技〔2017〕732号）有关要求，本项目执行工程监理制度，监理单位根据《信息技术服务监理》（GB/T 19668）、合同和招投标等文件要求对项目建设的各个阶段和各个层面进行全方位的监督管理，中标单位必须无条件接受本项目监理单位的监督管理。 | |
| **五、采购人对项目的特殊要求及说明** | | | |
| 说明 | | 本项目为服务类项目，无进口产品，无核心产品要求。 | |
| 其他说明 | | 为配合采购人进行政府采购项目执行和备案，未在政采云注册的供应商可在获取招标文件后登录政采云进行注册，如在操作过程中遇到问题或者需要技术支持，请致电政采云客服热线：400-881-7190。 | |

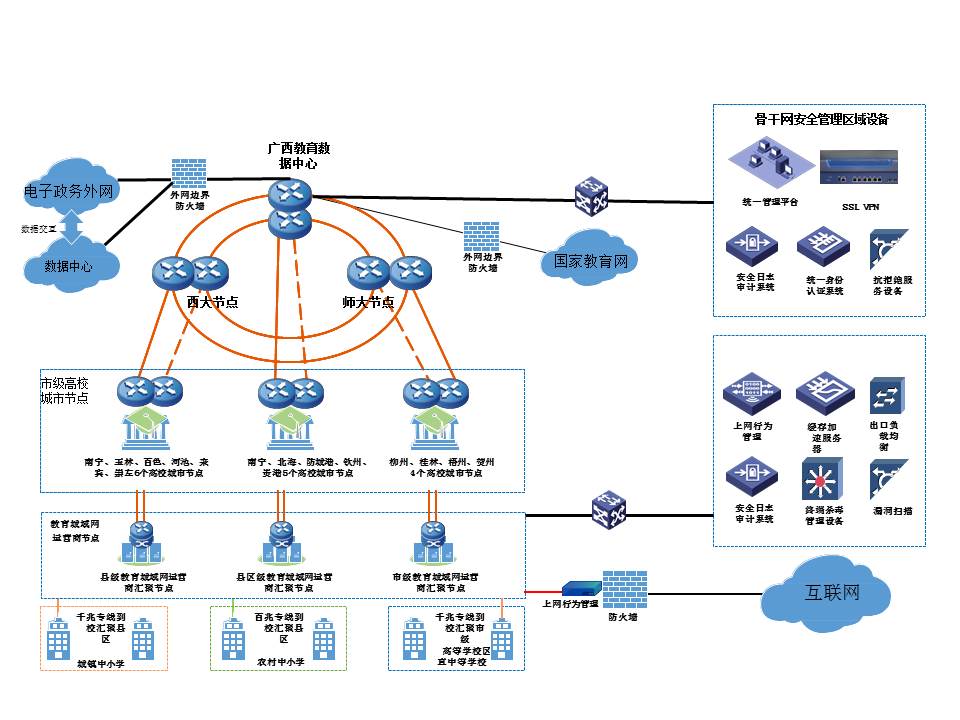
**附件1：**

**项目设计方案需求及要求**

广西教育网主要由教育骨干网、教育城域网、校园网三个主要部分组成。广西教育网的建设主要包括网络中心、传输网络、IP地址规划、网络安全等级保护。

**一、总体网络架构**

广西教育网将各级各类学校（教学点）连接起来，为将来统一教育管理平台、管理教育大数据、推广智慧教学应用等工作，搭建网络基础。整体架构如下图：



教育网拓扑图

通过建设教育骨干网核心节点，组建教育骨干网核心环路，在各设区市建立市级汇聚节点（高校城市节点），连接至各核心节点，建成教育骨干网。在各设区市、县（市、区）建立汇聚节点，各级学校（教学点）建设校园网，连接至各设区市、县（市、区）汇聚节点，形成教育城域网。各教育城域网连接教育骨干网市级汇聚节点，形成完整统一的教育基础网络。

**二、网络中心**

在教育骨干网的核心及汇聚节点设立网络中心，可以与目前各节点核心机房共用，各设区市级、县级教育城域网、跨县域的教育城域网根据情况设立不同规模的网络中心。

网络中心主要用于教育网提供运行环境和运维保障，建设内容主要包括机房运行环境、网络设备及运维系统、网络安全设备和系统等。机房运行环境主要包括机房装修，以及电力、空调、消防、门禁、监控等子系统。网络设备及运维系统主要包括路由、交换机、身份认证、缓存加速、机柜及配套设施、网络管理运维等子系统。网络安全设备和系统主要包括入侵防御检测、防DDOS攻击、防病毒、上网行为管理、实名审计、实名日志等子系统。

**三、教育骨干网**

教育骨干网是指在广西行政区域范围内，利用计算机网络技术，以光纤为传输介质的，连接全区各教育城域网、高等学校和区直中等职业学校校园网的，由核心节点、高校城市节点、主干光纤传输线路组成的网络。

教育骨干网及各端纵向接入城域网，实现线路两端的互通。鉴于教育骨干网的重要性，教育骨干网核心线路需具备自愈环保护功能，针对线路经过的骨干核心层，采取不同路径的物理链路在教育骨干网节点连接形成双路由保护，如其中一条线路阻断时，另一条线路仍能正常使用，以保证业务能够正常运行，不受单条线路故障影响。

3.1架构设计

根据国家IPv6发展战略，本期设计要求在原有高校互联网络基础上实施升级改造，以IPv6为网络基础协议。考虑到IPv6不可能立刻替代IPv4，在相当一段时间内IPv4和IPv6会共存在一个环境中，因此教育网需要支持IPv6和IPv4双栈协议。本期设计要求以MPLS技术为基础搭建教育骨干网，同时全面支持SRv6。在具备条件的环境下，近期内，用SRv6技术实现VPN业务的互联互通，用SRv6 Policy技术实现业务的精细化管理和流量调度，用SRv6 policy流量统计实现隧道流量可视化。未来通过IPv6技术实现教育骨干网多业务承载及运维，加大主干带宽，提升网络互联互通能力，并扩展连接范围，持续支撑中小学学校信息化应用的需要。

3.1.1核心环路

广西教育骨干网在广西教育数据中心（南宁）、教科网广西节点广西大学（南宁）和广西师范大学（桂林）分别设置三个核心节点，各新建两台核心路由器，通过租用2家运营商线路组成双环网，教育骨干网核心环总带宽不小于80G（首次开通带宽不小于20G）。

3.1.2市级节点部分

本项目在14个设区市设置共计13个汇聚节点（其中，南宁市设置2个汇聚点，钦州市、北海市、防城港市共用1个汇聚节点），各新建2台汇聚路由器，通过2家运营商就近接入核心节点，每个汇聚节点总带宽不小于20G（首次开通带宽不小于2G）。

鉴于北海市、防城港市的中小学整体规模较小，目前教育应用的整体流量需求较低，且其属地高等院校支撑高校城市节点建设、管理、运维的条件较弱，在钦州市（北部湾大学）设置汇聚节点，北海市和防城港市所辖的教育城域网全部接入钦州市（北部湾大学）汇聚节点。将来，北海市和防城港市的中小学整体规模上升后，再考虑单独设置汇聚节点。

另外，贵港市虽然中小学整体规模较大，但是考虑到目前暂时没有具备支撑高校城市节点建设、管理、运维的条件的高等院校，从保证系统运维安全、可靠性等的角度出发，把贵港汇聚节点设备暂时放置到广西教育数据中心，未来待贵港市建设有具备相应保障能力的高等院校后，再搬迁汇聚节点设备，并同步割接下辖的教育城域网和业务至新的贵港汇聚节点。

3.2汇聚节点规划

教育骨干网核心及汇聚节点选取要求：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 核心节点 | | 汇聚节点 | | | |
| 序号 | 汇聚节点 | 序号 | 地市 | 设区市节点 | 备注 |
| 1 | 广西教育数据中心  （植物路） | 1 | 南宁 | 广西教育数据中心 | 南宁市本级、兴宁区、江南区、青秀区、西乡塘区、良庆区、邕宁区、武鸣区 |
| 2 | 钦州 | 北部湾大学 | 钦州、北海、防城港市本级，以及所辖的各县（市、区） |
| 3 | 贵港 | 广西教育数据中心  （托管） | 市本级，以及所辖的各县（市、区） |
| 2 | 广西大学  （南宁） | 4 | 南宁 | 广西大学 | 南宁市高新技术产业开发区、南宁市华侨投资区、南宁市经济技术开发区、横县、宾阳县、上林县、马山县、隆安县 |
| 5 | 玉林 | 玉林师范学院 | 市本级，以及所辖的各县（市、区） |
| 6 | 百色 | 百色学院 | 市本级，以及所辖的各县（市、区） |
| 7 | 河池 | 河池学院 | 市本级，以及所辖的各县（市、区） |
| 8 | 来宾 | 广西科技师范学院 | 市本级，以及所辖的各县（市、区） |
| 9 | 崇左 | 广西民族师范学院 | 市本级，以及所辖的各县（市、区） |
| 3 | 广西师范大学 （桂林） | 10 | 柳州 | 广西科技大学 | 市本级，以及所辖的各县（市、区） |
| 11 | 桂林 | 广西师范大学 | 市本级，以及所辖的各县（市、区） |
| 12 | 梧州 | 梧州学院 | 市本级，以及所辖的各县（市、区） |
| 13 | 贺州 | 贺州学院 | 市本级，以及所辖的各县（市、区） |

在南宁设置两个汇聚节点，按照各设区市、县（市、区）学校规模以及区域，就近接入两个汇聚节点。

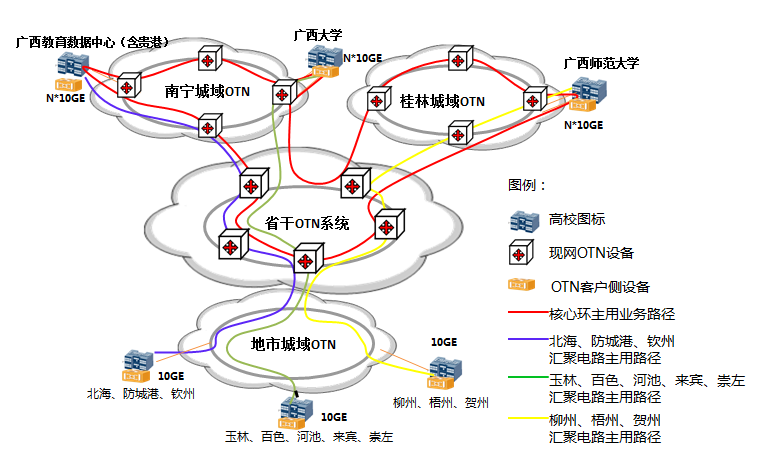
3.3传输设计

3.3.1核心层

通过南宁、桂林本地OTN系统及省干OTN系统承载和调度，配置10G/100G波道，开通1个10G子波道，后续带宽可以平滑扩容。

3.3.2汇聚层

南宁、桂林以外的节点，通过裸纤或城域OTN系统（优先）承载至省干OTN系统，再通过省干OTN系统调度至归属城市的城域OTN系统，最后通过南宁或桂林城域OTN系统接入教育骨干网核心节点。北海、钦州、防城港、贵港城市节点汇聚至广西教育数据中心，玉林、百色、河池、来宾、崇左城市节点汇聚至广西大学，柳州、梧州、贺州业务汇聚至广西师范大学。南宁、桂林两个地市以及托管于广西教育数据中心的贵港等汇聚节点与教育骨干网核心节点共用机房，可通过光纤直连。



教育骨干网线路图

3.4带宽要求

教育骨干网核心节点间互联设计带宽不小于80G，首次开通带宽不小于20G；核心节点与高校城市节点间互联设计带宽不小于20G，首次开通带宽不小于2G。当带宽占用率达到70%时进行扩容，教育骨干网与电子政务外网互联带宽按自治区本级电子政务外网接入点的技术要求执行。

3.5 VPN规划

3.5.1 VRF命名

为保证VPN数据的独立性和安全性，PE上每个VPN实例都有相对独立的路由表。为了区分不同的VPN实例，使用不同的VRF名称来进行区分。

3.5.2 RD（Route Distinguisher，路由标示符）规划原则

传统BGP无法正确处理地址空间重叠的VPN的路由。假设VPN1和VPN2都使用了10.110.10.0/24网段的地址，并各自发布了一条去往此网段的路由，BGP将只会选择其中一条路由，从而导致去往另一个VPN的路由丢失。PE路由器之间使用MP-BGP来发布VPN路由，并使用VPN-IPv4、VPN-IPv6地址族来解决上述问题。PE从CE接收到普通路由后，需要将这些私网VPN路由发布给对端PE。私网路由的独立性是通过为这些路由附加RD实现的。

在进行RD规划时，必须保证RD的全局唯一性。这样，即使VPN使用了同样的地址空间，PE路由器也可以向各个VPN发布不同的路由。RD的作用是添加了一个特定的前缀，使之成为全局唯一的VPN 路由前缀。教育骨干网RD采用以下格式：16位自治系统号：32位用户自定义数字。

3.5.3 RT（router target，路由目标）规划原则

L3VPN使用BGP扩展团体属性—Route Target来控制VPN路由信息的发布。PE路由器上的VPN实例有两类RT属性：

Export Target属性：在本地PE将从与自己直接相连的Site学到的VPN路由发布给其他PE之前，为这些路由设置Export Target属性；

Import Target属性：PE在接收到其他PE路由器发布的VPN路由时，检查其Import Target属性，只有当此属性与PE上VPN实例的Export Target属性匹配时，才把路由加入到相应的VPN路由表中。

也就是说，RT属性定义了一条VPN路由可以为哪些Site所接收，PE路由器可以接收哪些Site发送来的路由。RT也必须全局进行规划。采用RT值的格式为：16位自治系统号：32位用户自定义数字。在RT规划时，既要能够保证各教育系统VPN能够各自形成，还要能够通过RT控制，使各教育系统VPN能够相互引入各自的路由，从而实现VPN之间的横向互访。

3.5.4 VPN规划的原则

为适应现全区教育系统的信息资源共享的需求，教育网将在加强网络边界防护的基础上，规划设置公共域，在公共域内不设置任何访问限制，可实现各个教学单位间服务器与终端的互访。对有特殊隔离需求的网站应用，视频教学、远程教学等业务系统可单独设置VPN形成相互独立的虚拟专网。这些虚拟专网可根据业务需要，与公共域实现完全隔离或在采取安全措施满足相应安全防护要求的前提下进行双向互访。

3.6 MPLS路由设计

3.6.1路由规划原则

承载网是一个大型并且相对复杂的网络系统，它覆盖多家单位，上联网络中心，承载多种网络业务，并需要具备可运营、可管理、高可用等特点。从路由设计的维度看，承载网需要重点考虑路由的收敛性、网络的可扩展性、网络的安全性和网络的可控性四个方面。基于以上这些因素，承载网路由设计原则如下：

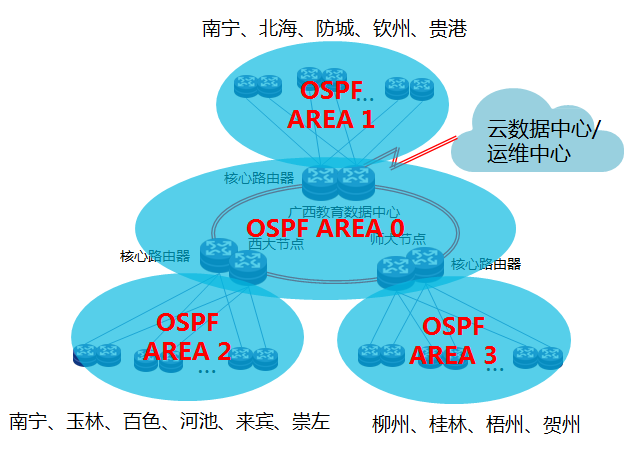
稳定性：必须考虑避免小范围（区域）的用户路由振荡引起对整个承载网大范围的路由振荡；

可控性：必须考虑能对承载网的IGP 路由、业务路由能够进行区分、控制；

可靠性：必须考虑网络故障时路由的快速收敛、恢复，可以通过运行动态路由协议、多链路的冗余保护等手段减少对用户业务的影响。

3.6.2路由总体设计

承载网路由总体模型如下：



整网路由协议规划

公网路由：公网路由用于所有承载网设备之间的互连地址和设备的Loopback地址的传递，并指导公网侧隧道的建立承载业务流量在承载网范围内的转发。

私网路由：各个不同业务各自的路由在各个PE之间互相传递，并指导流量传递方向。

承载路由协议（IGP）选择OSPF协议，该协议主要用于宣告各设备的loopback 地址、设备间的互联地址。私网网络路由通过MPBGP协议承载，以保证承载网络路由与用户网络路由的隔离，确保用户网络路由的波动不会影响承载网络路由的稳定性。

3.6.3教育骨干网OSPF规划

OSPF作为公网路由协议，负责所有PE和P设备的互联接口和loopback口路由发布。指导流量在教育骨干网转发，并为BGP邻居关系建立提供路由可达条件。

在本项目承载网中，所有PE和P设备接口都在骨干域：即Area 0，负责全网进行高速、稳定的数据包转发。承载网各P、PE节点设备之间的互联链路以及这些设备的Loopback接口地址划分到Area 0。

3.6.4 BGP路由规划

BGP 路由设计包括自治域设计、路由反射器，IPV4 全局路由设计以及VPN路由设计。

自治域设计：从网络业务拓展和维护管理等各方面综合考虑，为承载网分配独立的自治域AS号。

路由反射器RR（route-reflect）：

为了教育网IBGP 的方便部署和维护，减少BGP对等体的数量，需要采用路由反射器RR（route-reflect）技术。路由反射器RR同时为全局路由IPv4、MPLS VPN 路由VPNv4 提供服务。P设备作为路由反射器，网络中心出口设备以及各单位所在PE设备作为client。

如下图方式建立MP-IBGP邻居关系，P节点兼做反射器（所有PE都和P建立邻居关系，包括骨干层和接入层PE）。

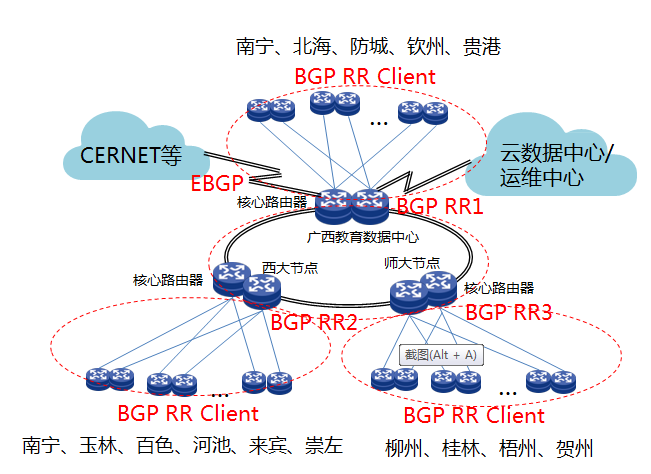
私网路由引入方式：

私网路由通过PE上配置私网侧的静态路由，并引入MP-BGP私网侧。

私网路由根据下联的加密方式有两种不同的方式：

方式一，加密方式为隧道方式，则只发布加密设备的隧道地址。需要在加密时将业务的DSCP值复制到外层隧道的DSCP，用以识别不同业务。

方式二，加密方式为传输模式，只加密报文的负载，报文头不做加密。私网路由发布时，发布内网业务的明细地址。使用VPN+地址区分不同业务。



BGP邻居关系

3.6.5路由策略设计

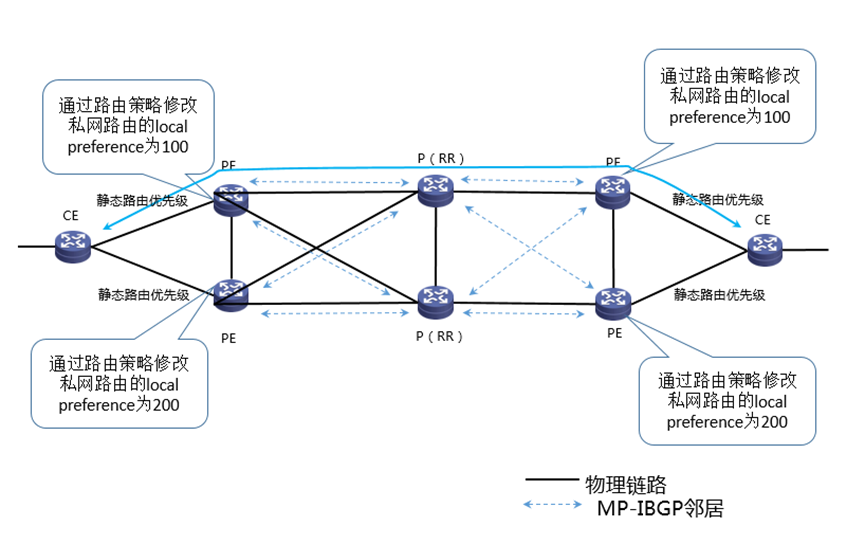
在骨干层PE为双节点时，直接接入骨干层PE的业务需要使用路由策略来区分主备PE，以确保不同流量在PE上的负载分担。其他业务接入时都是单节点接入不存在此问题，无需配置策略。

MP-IBGP 路由策略

PE侧引入私网路由通过策略修改Local-preference值，区分PE节点主备。不同私网业务使用不同策略确保业务在两台PE节点上负载分担。

全局路由以汇总方式进行通告，通过静态路由指向全局路由网段、以Network 方式引入IBGP，减少IBGP 路由数量。根据用户接入需求，通过BGP 丰富的路由属性、选路规则，进行路由过滤、路由策略制定。（途中以一端举例，两端策略对称。同一私网其他节点主备设备保持一致。）

接入侧通过静态路由优先级区分PE主备，需要与BGP策略一致。



策略说明

3.7 SRv6路由设计

3.7.1 IGP路由协议

教育骨干网内部采用IGP实现路由发布，常见的动态IGP协议有OSPF和IS-IS（Intermediate System-to-Intermediate System，中间系统到中间系统），相比较OSPF，ISIS具有更好的开放性、扩展性和兼容性，同时ISISv6对IPv6的可扩展性更好，新技术标准进展更加成熟和全面，因此在教育骨干网部署ISISv6协议。

教育骨干网规划为ISISv6的Level-2，有核心路由器和汇聚路由器都运行在ISISv6 Level-2进程内，对路由进行发布，从而学习到教育骨干网的拓扑信息和路由信息。

教育骨干网设备的Loopback接口/链路互联接口/SRv6 Locator的IPv6地址都发布到ISISv6进程中，实现教育骨干网的路由互通。

3.7.2 MP-BGP路由协议

教育骨干网采用SRv6技术进行VPN业务承载，作为一张SRv6 VPN专网，VPN的路由需要通过MP-IBGP协议来进行通告学习。教育骨干网的MP-IBGP路由设计可以采用和IBGP路由相同的方式，在自治系统（AS）域内，需要在核心路由器P和汇聚路由器PE上部署MP-IBGP协议，同时为了保证MP-IBGP对等体之间的连通性，需要在IBGP对等体之间建立全连接关系。同时，在教育骨干网内部署RR反射器来解决这一问题。

3.7.3 RR反射器设计：

RR作为MP-BGP路由的反射器。核心P设备一般为高端设备，性能较强，所以直接由核心P设备兼任RR。RR设计包括如下几点：

3.7.3.1在两个核心站点各选择一台P设备作为RR反射器，拟在广西教育数据中心和广西师范大学两个核心节点上进行部署；

3.7.3.2所有的其他PE/P设备均与两台核心P设备建立MP-BGP邻居关系；

3.7.3.3两台RR设备设置为同样的Cluster ID防止环路；

3.7.3.4将所有其他的PE/P设备均指定为RR client，并且仅与两台RR路由器建立MP-BGP连接；

3.7.3.5使用P/PE设备的Loopback接口的IPv6地址建立BGP邻居。

3.7.4 SRv6隧道设计

SRv6 隧道包含两种类型：SRv6 BE（SRv6 Best Effort）和SRv6 TE（SRv6 Traffic Engineering），其中SRv6 BE是使用IGP/BGP选路算法计算得到的最优IPv6路径，该最优IPv6路径天然支持ECMP。SRv6 TE使用通过约束计算得到的满足一定SLA要求的路径，通常由控制器进行路径计算，然后下发到路由器。SRv6 BE适合对于SLA要求不高或者对路径无要求的业务场景；SRv6 TE适合对SLA要求较高的业务场景，以及不同业务之间有路径分离诉求的场景。

在教育骨干网中，不同业务的SLA承载诉求是同时存在的，并且有些业务在正常转发时对路径无要求，但是在网络拥塞或者有安全攻击时又需要指定路径，因此通常需要组合使用SRv6 BE和SRv6 TE路径，结合业务和场景来选择使用不同类型的路径。

3.8 QoS（Quality of Service，服务质量）设计

随着网络承载的业务逐渐增加，网络流量激增，会导致网络拥塞，转发时延增加，严重时还会产生丢包，将导致实时类多媒体业务质量下降甚至不可用，因此为保障教学工作顺利开展，教育骨干网需具备为关键教学业务提供专用带宽的能力，支持端到端针对关键教学业务提供网络切片，对关键教学业务进行带宽硬隔离，同时针对非关键教学业务还需具备QoS能力，为不同的业务提供端到端的差异化服务质量保证。

在路由器/交换机上对关键业务部署IP QoS策略，为不同业务定义差异化服务等级，并在IP报文头的QoS字段进行标记，保证网络拥塞时高优先级的重要业务得到优先处理，网络上所有路由器/交换机对具有相同QoS参数的业务采取相同的优先级调度策略。

教育骨干网针对不同的教学业务划分如下三个服务等级：

1.关键业务：教育骨干网端到端进行网络切片，独享网络带宽，确保教学业务质量，如视频教学、视频教研等业务。

2.次优业务：通过QoS策略优先保障，共享网络带宽，当网络发生拥塞时优先转发，如教学资源系统、教学管理系统等。

3.普通业务：尽力转发，共享网络带宽，当网络发生拥塞时，调度优先级别低。如课件资料下载、互联网访问等。

3.9传输线路配置

根据教育骨干网组网需求，核心环三个节点，每个节点之间2条专线，每条专线带宽不低于10G，总计需6条专线。汇聚节点总计13个，其中南宁市2个节点、桂林市节点、贵港市节点与核心节点属于同一机房，采用直连光纤互联，其余9个城市节点每个节点至核心节点需要2条专线，每条专线带宽不少于1G，共计需18条专线。

从保证传输网络安全性和可靠性方面进行考虑，核心环节点之间以及核心节点与汇聚节点之间的链路承载在至少2家运营商的传输网络上，以保证传输网络有较高的冗余性，一旦出现其中1家运营商网络故障的时候，另1家运营商的传输网络仍然能保证教育骨干网的正常运行。

3.10数据设备配置

3.10.1核心节点路由器

按照教育骨干网组网需要，3个核心节点各配置2台核心路由器，总计需6台核心路由器。

3.10.2汇聚节点路由器

13个汇聚节点根据容量需求不同，需配置不同配置的汇聚路由器，总计需26台汇聚路由器。其中桂林、梧州、钦州、贵港、玉林、百色、河池节点所接入学校数超过1000个，教室数大于5000个，要求汇聚路由器配置更高的性能。

3.10.3同节点路由器厂家选择

同节点路由器在实际部署时有可能出现同厂家或者异厂家两种情况，具体优缺点对比如下：

同节点路由器同/异厂家优缺点对比表

|  | 优点 | 缺点 |
| --- | --- | --- |
| 同厂家 | 便于实现设备主备、堆叠、集群等部署，后续升级不影响业务运行，便于管理维护，提高了节点整体冗余性、可用性、可维护性等。 | 若出现大的设备软件系统性故障，可能导致整个节点瘫痪。 |
| 异厂家 | 不同的业务承载在不同厂家的设备上，若其中一个厂家设备出现故障导致业务中断，不影响另一个厂家设备承载的业务。 | 设备难以进行主备、堆叠、集群等部署，管理维护复杂，由于是单点设备，存在设备故障、设备升级等导致承载业务中断的风险较高。 |

综合以上对比分析，考虑到同节点同厂家设备可以实现主备、堆叠、集群等部署，在可靠性、安全性等方面已有较大的冗余性，可维护性方面更具灵活性，未来设备升级更平滑，且出现系统性缺陷的概率较低，因此，采用同节点同厂家路由器进行部署。

3.10.4虚拟化一体机

本项目日常运维工作中，涉及到网络管理、安全管理、统一身份认证、上网日志留存、远程运维等各种业务软件，这些业务软件均需要计算资源和存储资源，为了保障本项目当前及未来3年的运维需求，本次设计在教育骨干网的3个核心节点和10个高校城市节点配置虚拟化一体机，为项目管理和运维业务提供相应计算资源和存储资源。

3.10.5教育骨干网网络设备需求汇总

教育骨干网网络设备表

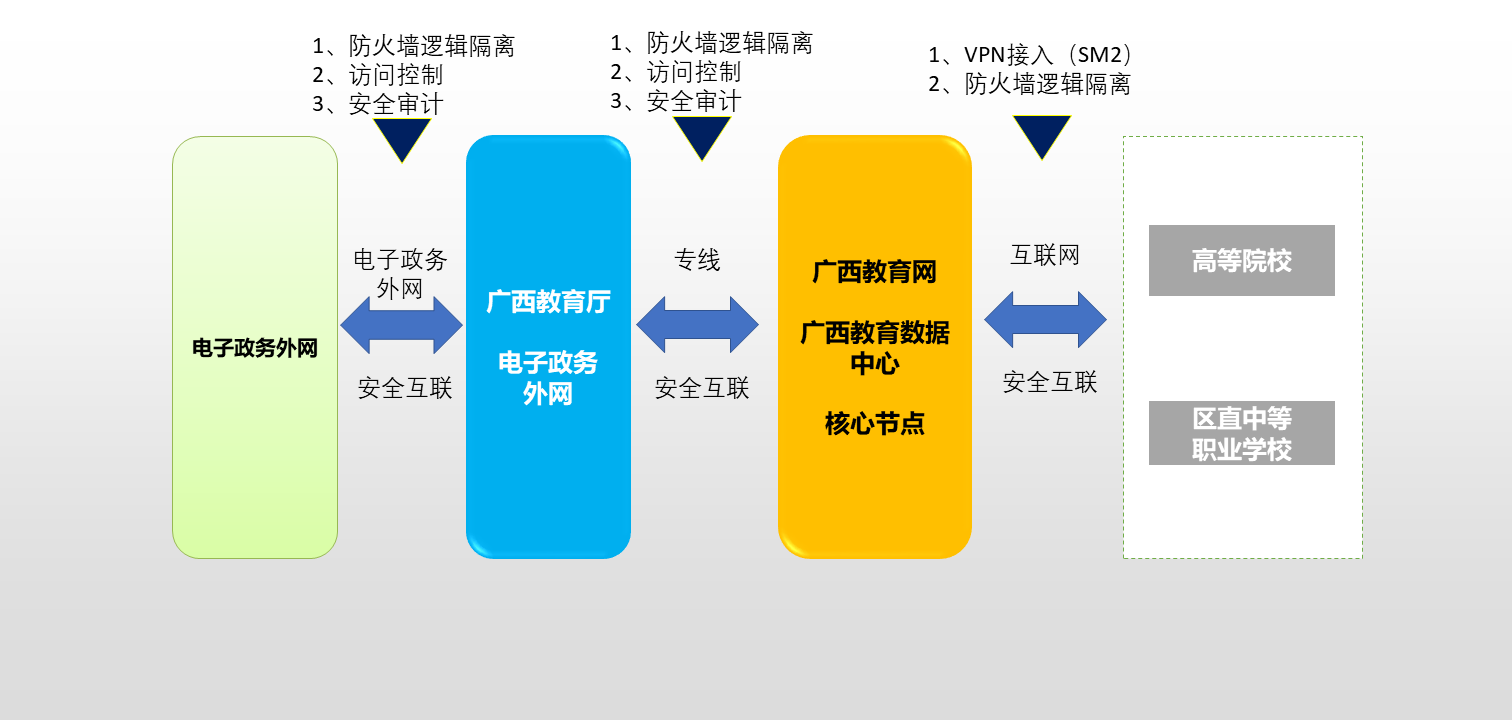
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 货物名称 | 数量 | 单位 | 说明 |
| 1 | 核心路由器 | 6 | 台 | 广西教育数据中心、广西大学、广西师范大学各2台 |
| 2 | 市级汇聚路由器 | 26 | 台 | 南宁4台，柳州、桂林、梧州、钦州（含北海、防城）、贵港、玉林、百色、贺州、河池、来宾、崇左各2台 |
| 3 | 网络运维  管理软件 | 1 | 套 | 厂家网管软件1套 |
| 4 | 虚拟化一体机 | 13 | 套 | 包含服务器、超融合管理软件、计算虚拟化软件、存储虚拟化软件、一体化管理软件、网路交换机 |

**四、电子政务外网互联设计要求**

为贯彻落实《国务院办公厅关于印发政务信息系统整合共享实施方案的通知》（国办发〔2017〕39号）精神，按照自治区政府相关要求，广西教育厅OA办公、公文流转两个业务系统需要部署在政务云，同时实现自治区教育系统各高等院校、区直中等职业学校安全、便捷接入。教育网与电子政务外网之间，采用逻辑隔离和边界防护手段，实现双向数据交换。安全接入方案和设备应符合《国家电子政务外网信息安全标准体系框架》中的安全标准。

4.1接入方案

4.1.1高等院校、区直中等职业学校接入电子政务外网方案



高等院校、区直中等职业学校接入电子政务外网示意图

依照《广西电子政务外网市、县级节点技术规范》（2019修订版）的要求，学校属于B 类用户，各学校在访问OA以及公文流转业务时通过防火墙设置与其互联网出口流量的做强逻辑隔离。

在广西教育数据中心建立独立安全域，在该安全域部署两台VPN设备，选用的VPN设备支持SM2加密算法。各高等院校、区直中等职业学校通过VPN设备接入到广西教育数据中心。并通过防火墙、入侵防御、安全审计设备，对该区域进行重点安全防护。

广西教育数据中心通过专线连接到教育厅的电子政务外网出口，在经过访问控制、入侵防范和安全审计后访问部署在电子政务外网的OA、公文流转系统。

现阶段各高等院校、区直中等职业学校通过互联网VPN拨号访问电子政务外网。待教育网建设完善后，改为从通过教育网VPN拨号访问电子政务外网。

4.1.2各级教育行政管理部门访问教育应用系统接入方案要求

目前，广西各级教育行政管理部门通过电子政务外网接入点就近接入电子政务外网，并通过电子政务外网互联网出口访问广西教育数据中心的相关应用系统。待教育网建设完善后，各级教育行政管理部门改为通过电子政务外网的互联交换区直连教育网访问相关应用系统。

4.2安全防护方案要求

根据《接入政务外网的局域网安全技术规范》（GW0206-2014），电子政务外网边界为广西教育厅的本地局域网与本级政务外网城域网的接入边界，接入单位局域网应通过防火墙系统、入侵防御系统和安全审计系统等与政务外网进行逻辑隔离并对局域网进行安全防护。

具体要求包括：

4.2.1访问控制

4.2.1.1根据会话状态信息为数据流提供明确的允许/拒绝访问能力，控制粒度至少达到端口级。

4.2.1.2应对用户设置有限的权限访问政务外网资源，并限制政务外网地址访问局域网。

4.2.1.3对外提供服务节点时，应设置公用网络业务DMZ区，对该区单独实施安全策略，允许公用网络区访问内部业务区，禁止内部业务区服务器向外访问。

4.2.2入侵防范

4.2.2.1进行病毒过滤和入侵防御，并及时升级病毒和攻击特征库；

4.2.2.2对病毒和入侵攻击行为进行实时告警及阻断。

4.2.3安全审计

4.2.3.1记录攻击源IP、攻击类型、攻击目的IP、攻击时间等关键信息。

4.2.3.2记录公用网络访问行为、网络地址转换日志等信息。

4.2.3.3审计信息保存6个月。

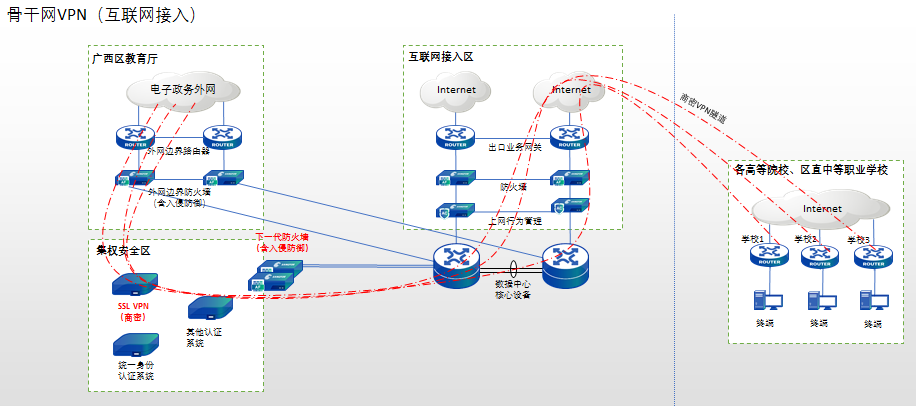
根据上述要求，本项目将构建“集权安全区”，将VPN、RSA、统一身份认证、堡垒机等集权业务集中在该区域，并进行重点安全防护。

在集权安全区部署2台SSL VPN：用于自治区范围内各高等院校、区直中等职业学校的接入。对于所有学校的接入，结合SSL VPN身份认证安全机制、终端安全控制机制、高强度加密机制、细粒度授权机制，保证应用仅可由指定用户、使用指定安全级别的终端、访问到指定应用的强控制。

在集权安全区部署2台下一代防火墙：下一代防火墙可针对用户的上网终端提供安全威胁过滤、木马恶意流量检测、DMZ服务器保护、NAT、路由等安全防护功能。面向应用层设计，能够精确识别用户、应用和内容，具备完整安全防护能力，能够全面替代传统防火墙，并具有强劲应用层处理能力的全新网络安全设备。解决了传统安全设备在应用识别、访问控制、内容安全防护等方面的不足，同时开启所有功能后性能不会大幅下降。作为传统防火墙的升级替代产品，下一代防火墙不同于工作在L2-L4层的传统防火墙，可以对全网流量进行双向深入数据内容层面的全面透析。在安全策略制定方面，区域别于传统防火墙五元组安全策略，下一代防火墙可对L2-L7层更多的元素（如，用户、应用类型、URL、数据内容等）制定双向的安全访问策略，使安全策略更精细、更有效，且满足业务的合规性；在安全防护能力方面，提升了传统的抗攻击的能力，不仅能防护网络层的攻击，针对来源更广泛、攻击更容易、危害更大的应用层攻击也可以进行防护，实现L2-L7层的安全防护。

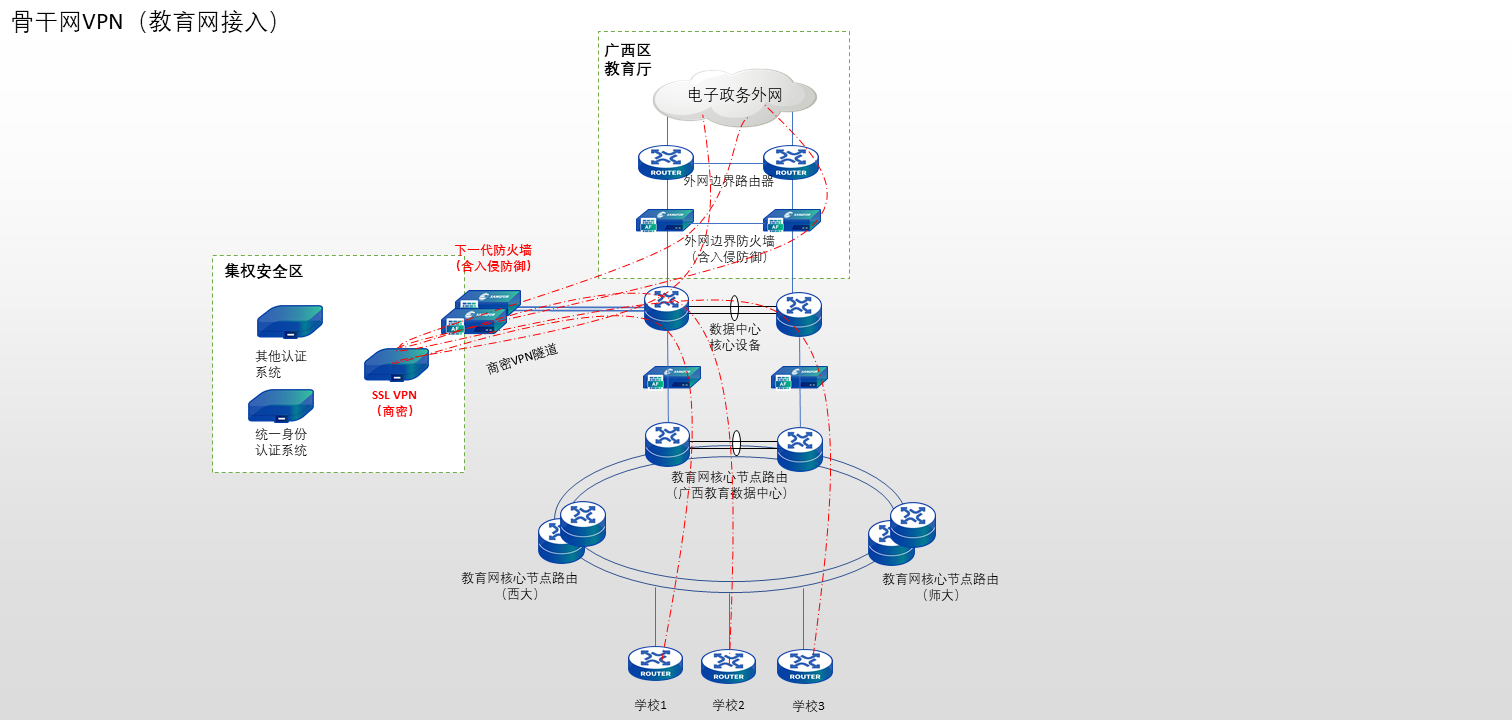
4.2.4高等院校、区直中等职业学校接入电子政务外网安全防护

现阶段各高等院校、区直中等职业学校通过互联网VPN拨号访问电子政务外网，访问路由如下图。



高等院校、区直中等职业学校（互联网接入）访问电子政务外网路由图

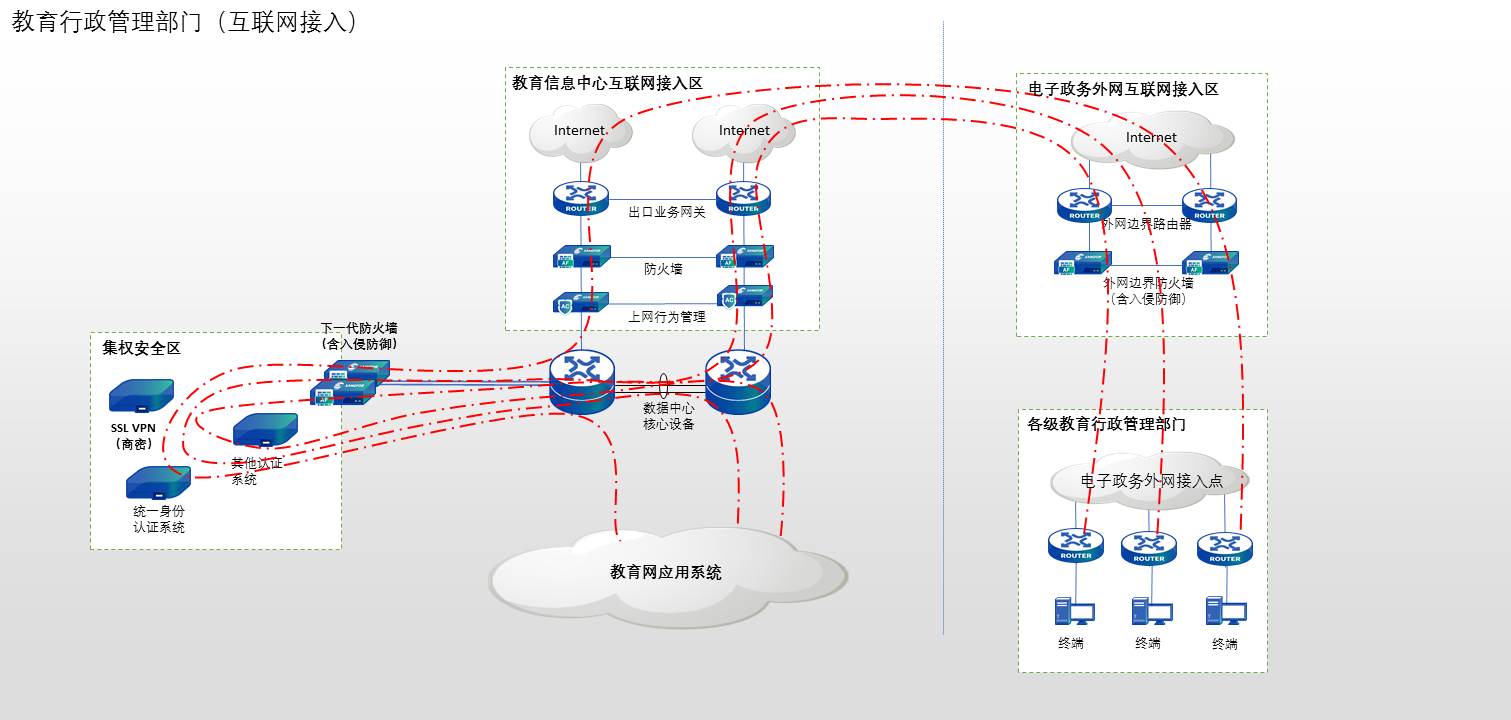
待教育网建设完善后，各高等院校、区直中等职业学校改为通过教育网VPN拨号访问电子政务外网，访问路由如下图。



高等院校、区直中等职业学校（教育网接入）访问电子政务外网路由图

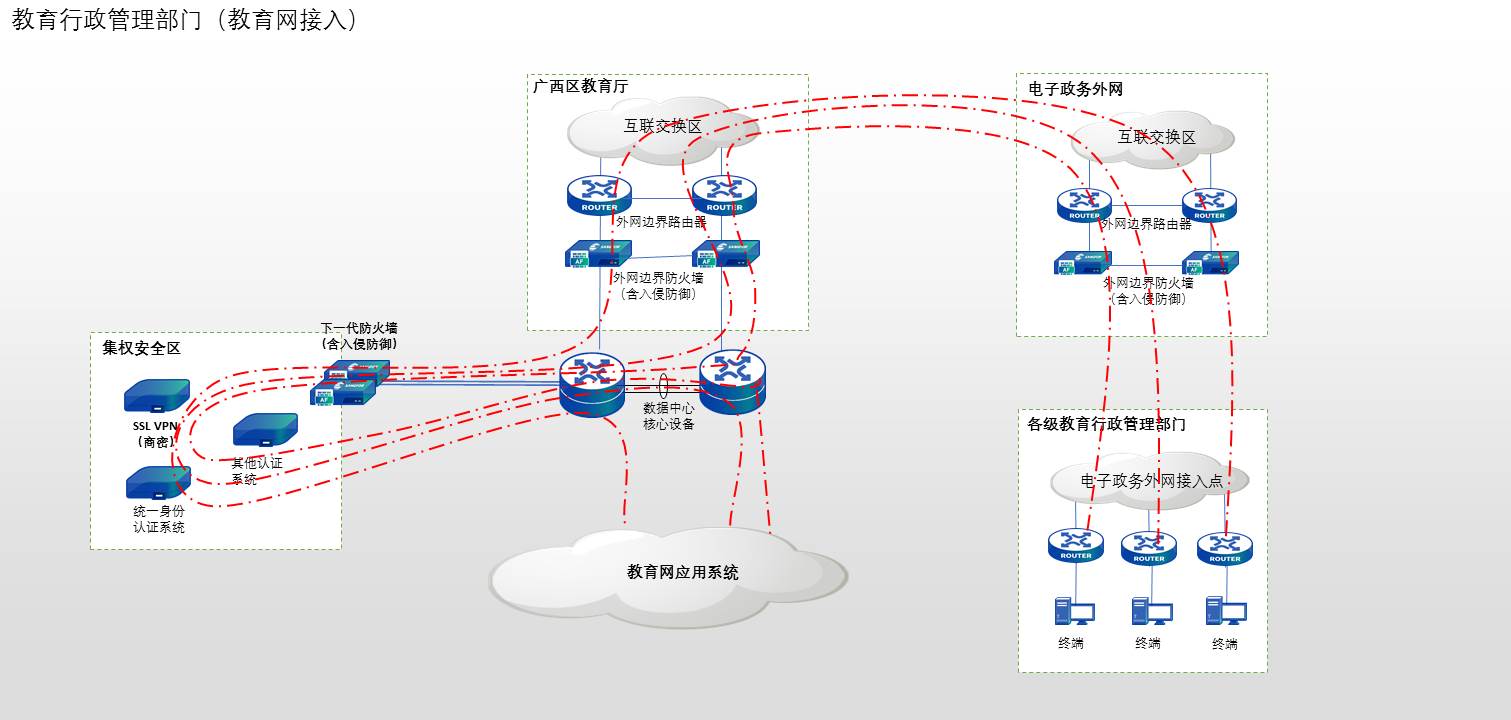
4.2.5各级教育行政管理部门访问教育应用系统安全防护

目前，广西各级教育行政管理部门通过电子政务外网接入点就近接入电子政务外网，并通过电子政务外网互联网出口访问广西教育数据中心的相关应用系统，访问路由如下图。



教育行政管理部门（互联网接入）访问教育应用系统路由图

待教育网建设完善后，各级教育行政管理部门改为通过电子政务外网的互联交换区直连教育网访问相关应用系统，访问路由如下图。



教育行政管理部门（教育网接入）访问教育应用系统路由图

4.3主要防护技术要求

4.3.1以下一代防火墙为核心的边界防护设计

传统的安全建设往往通过大量不同品类的硬件设备堆叠进行边界防护体系的构建，这造成各个安全功能的脱节和割裂，无法实现主动防御和智能联动。此次设计方案要求通过在物理边界部署下一代防火墙设备，提供主动的、实时的防护。方案在功能区边界构建以防火墙为核心的融合安全防御体系。

融合不是单纯的功能叠加，而是依照业务开展过程中会遇到的各类风险，所提供的对应安全技术手段的融合，能够为业务提供全流程的保护，融合安全包括从事前的资产风险发现，策略有效性检测，到事中所应具备的各类安全防御手段，以及事后的持续检测和快速响应机制。



防护设计结构图

4.3.2以SSL VPN为核心的安全接入

访问控制：采用SSL VPN对应用进行安全发布，避免需要将服务器直接挂在公网上造成的风险。用户在外需要进行内网接入时，可直接通过浏览器打开网页完成SSL VPN登录及安全隧道的建立，如同登录网银、邮箱一般符合日常的网络使用习惯，容易上手。而SSL协议是目前公认安全等级较高的网络安全协议之一，现今网上银行基本都采用SSL协议进行数据传输保护，对于数据传输采用标准的AES、RSA、RC4等加密算法对传输数据进行加密，安全性有保障。

认证安全：在系统安全认证方面，采用登录SSL VPN身份验证、权限划分、登录应用身份验证的主线进行保障。SSL VPN接入认证方式可采用用户名密码、USB KEY、短信认证、动态令牌、CA认证、LDAP认证、RADIUS认证等两种或多种认证的组合，多重组合软硬结合确保接入身份的确定性。在用户接入SSL VPN后进行应用访问权限的划分对于享有访问权限的应用系统采用主从账号绑定SSL VPN登录账号和应用系统账号。用户只可采用指定的账号访问应用系统。由于登录SSL VPN的身份已通过多重认证的确认，而后又进行指定应用账号访问，即可保障登录应用系统的人员的身份。

服务器区隔离保护：将SSL VPN设备以单臂方式部署，通过配置使数据流经由SSL VPN后走向内网服务器区，对办公网与服务器区这两个不同安全级别的区域进行隔离。由于SSL VPN设备对外只开放443端口，从而可屏蔽掉其他端口的攻击。SSL VPN的数据流处理方式可隐藏内网服务器区结构，并对服务器访问的IP、域名进行伪装。SSL VPN在进行用户对服务器区发起的访问时，采用SSL VPN登录认证、细粒度应用访问授权、传输数据加密，从数据安全的角度提供隔离保护。

**五、IP地址规划**

IP地址规划关系到全网的通信质量，必须为全网的资源进行统一规划，所以需要尽可能的保证业务的连续性。

5.1 IP地址规划目标

5.1.1建立高效的网络路由。

5.1.2有效利用有限的IP地址资源。

5.1.3支持网络技术的演变和发展。

5.2 IP地址规划原则

5.2.1简单性：地址的分配应该简单，避免在主干上采用复杂的掩码方式。

5.2.2连续性：为同一个网络区域分配连续的网络地址，便于采用路由收敛及CIDR(Classless Inter-Domain Routing，无类别域间路由)技术缩减路由表的表项，提高路由器的处理效率。

5.2.3可扩充性：为一个网络区域分配的网络地址应该具有一定的容量，便于主机数量增加时仍然能够保持地址的连续性。

5.2.4灵活性：地址分配不应该基于某个网络路由策略的优化方案，应该便于多数路由策略在该地址分配方案上实现优化。

5.2.5可管理性：地址的分配应该有层次，某个局部的变动不要影响上层、全局。

5.2.6安全性：网络内应按工作内容划分成不同网段即教育城域网以便进行管理。

5.3网络IP地址分类

5.3.1设备管理/协议地址——Loopback 接口地址，SRv6 Locator地址。

5.3.2互联地址——即链路地址，通常配置在网络设备之间互联的接口上。

5.3.3业务地址——即终端、服务器地址段。

5.4 IPv6地址规划原则

在IPv6网络中，IPv6地址规划遵循如下原则。

统一性原则：全网的所有IP地址统一规划，包括业务地址，平台地址，网络地址等。

唯一性原则：每个地址都能够做到全网唯一。IPv6地址中，有三类单播地址可供选择：Global Unicast Address，Unique Local Address，Link-Local Address。Global Unicast Address是全球唯一的地址，使用范围是最广；Unique Local Address类似IPv4的10.0.0.0/8，172.16.0.0/12和192.168.0.0/16网段，是私网可用地址，但不能发布到internet上；Link-Local Address是单链路范围内唯一的地址，只能在链路范围内使用，在运维方面非常不方便（例如不能从远端设备ping这个网段）。考虑到IPv6地址空间足够大，业务地址推荐使用Global Unicast Address，不做NAT转换，网络互连地址也推荐使用Global Unicast Address。

分离原则：业务地址和网络地址分开规划，方便在网络边缘进行路由控制和流量安全控制。

层次化和聚合原则：地址必须能够在不同的IGP/BGP之间被聚合发布，聚合会指数级减少网络中的路由数量，并且降低一个路由域中的路由震荡对其他路由区域的影响。

安全性原则：为了达到IPv6地址可快速溯源，需要在IPv6地址中嵌入关键的溯源信息，包括地址属性，地址所属地域等信息。另外为了方便地进行地址的过滤，需要梳理出于安全原因需要根据地址过滤流量的场景，将这些场景包括到IPv6地址规划中，例如前面分离原则中提到的业务地址和网络地址分离。

可演进性原则：地址规划时应在每个地址段内预留一定的地址空间用于业务未来发展，如果预留不足，则未来的地址扩充可能会导致地址无法满足前面的聚合性，安全性等原则。

可读性原则：由于IPv6地址通常以16进制（4bits）的形式书写，因此IPv6地址规划时以4bits为单位（也称为ibble）进行划分，方便后续查看。

教育网使用私有地址，由自治区教育厅统一规划分配至各设区市级教育城域网、县级教育城域网、高等学校。教育城域网主管教育行政管理部门负责统一规划分配网内的学校和其它教育机构的IP地址。教育骨干网的路由IP使用中国教育和科研计算网（CRENET）IP地址。

教育网全网支持IPv6部署和应用，支持IPv6和IPv4双栈协议。

**六、系统安全建设方案要求**

6.1系统安全总体目标

本项目系统安全建设的最终目标是使教育骨干网符合国家网络安全等级保护第三级要求，教育城域网符合国家网络安全等级保护第二级要求。

本项目根据等级保护指导思想，以技术保障为基础、以管理运营为抓手、以监测预警为核心、以协同响应为目标规划网络安全防御体系并落地为具体的安全建设方案。将物理和环境、网络和通信、设备和计算安全、应用和数据安全、安全策略和管理制度、安全管理机构和人员、安全建设管理、安全运维管理等各个层面的安全需求，转化为可以实现的技术防护能力、安全管理措施和安全运营手段，为教育网的安全运行保驾护航。

6.2安全体系架构

6.2.1设计原则

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，构建网络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。在网络系统的安全设计环节重点把握如下原则：

6.2.1.1统一性、整体性

教育网是一个有机的整体，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。

对整个网络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。

6.2.1.2一致性

网络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，是网络系统的安全设计的必要前提条件。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。

6.2.1.3多重保护性

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。

6.2.1.4适应性及灵活性

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。

6.2.2设计思路

本项目将根据网络安全等级保护相关要求，通过分析系统的实际安全需求，结合其业务信息的实际特性，并依据及参照相关政策标准，设计安全保障体系方案，综合提升系统的安全保障能力和防护水平，确保教育网的安全稳定运行。具体设计将遵循以下思路开展。

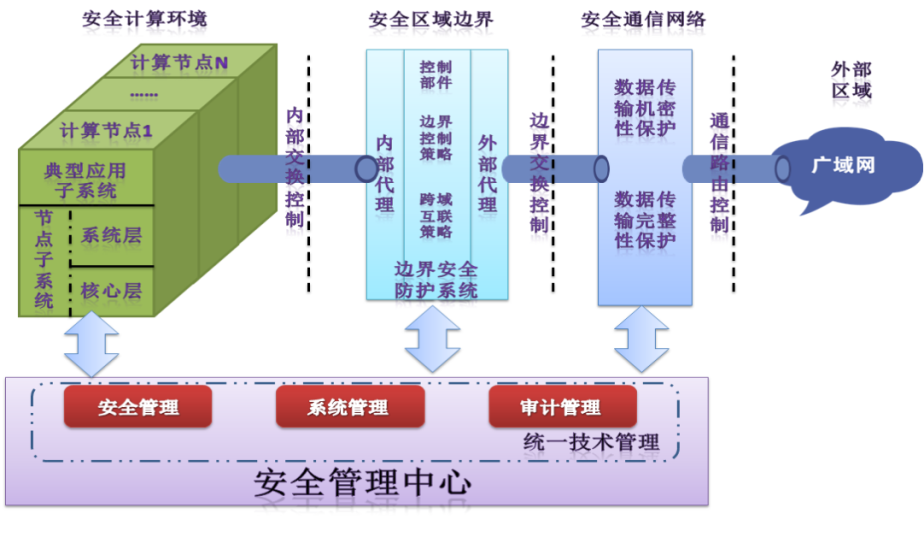
6.2.2.1将合规要求与业务风险分析相结合的设计思路

安全风险分析是识别网络系统面临安全威胁和系统脆弱性的方法，通过风险分析方法可以全面掌握网络系统面临安全风险的全貌，并根据安全风险等级确定信息安全建设的重点。

在完成基于资产风险分析的基础上，对网络系统现状进行实际调研，掌握网络系统防护现状与等级保护基线要求间的实际差距，结合安全风险评估的方法，对网络系统进行全面的资产、脆弱性、威胁和业务风险等方面系统化的评估分析，发现基于业务的安全风险问题。将差距分析结果与风险评估结果进行充分结合与提炼，综合形成能够符合等级保护建设要求并充分保障业务安全的建设需求。

6.2.2.2纵深防御的安全体系设计思路

安全体系建设的思路是根据分区分域防护的原则，按照层次化的纵深防御的思想，建设网络系统安全等级保护深度防御体系。



纵深防御安全体系图

按照信网络统业务处理过程将系统划分成安全计算环境、安全区域边界和安全通信网络三部分，以计算节点为基础对这三部分实施保护，构成由安全管理中心支撑下的计算环境安全、区域边界安全、通信网络安全所组成的“一个中心，三重防护”结构。

6.2.2.3体系化安全保障框架设计思路

一个完整的网络安全体系应该是安全技术、安全管理、安全运营的结合，三者缺一不可。为了实现对网络系统的多层保护，真正达到网络安全保障的目标，国内外安全保障理论也在不断的发展之中，根据网络系统的实际情况，参照国际安全控制框架的有关标准，形成符合教育网需要的安全保障体系框架。

在方案设计中“三个体系”（安全技术体系、安全管理体系和安全运营体系）各自相对独立，又相互依赖和互补，共同形成整体的安全保障体系框架。

6.2.3总体安全策略

6.2.3.1安全技术体系总体策略

（1）以《网络安全等级保护基本要求》中第三级（教育骨干网）和第二级（教育城域网）保护要求为控制要求，建设基础安全技术体系框架。

（2）安全技术体系建设覆盖物理环境、通信网络、区域边界、计算环境和安全管理中心五个方面。

（3）通过采用成熟可靠的安全技术及安全产品，结合专业技术人员的安全技术经验和能力，系统化的搭建安全技术体系，确保技术体系的安全性与可用性的有机结合，达到适用性要求。

6.2.3.2安全管理体系总体策略

（1）建立网络安全领导小组和工作组，形成等级保护基本要求的网络安全组织体系职责。

（2）建立网络安全管理制度和策略体系，形成符合等级保护基本要求的安全管理制度要求。

（3）建立符合系统生命周期的安全需求、安全设计、安全建设和安全运维的运行管理要求。

（4）系统安全建设过程应落实等级保护定级、备案、建设整改、测评等管理要求。

（5）系统安全运营过程应落实等级保护监督检查的管理要求。

6.2.3.3安全运营体系总体策略

（1）通过互联网等领域所形成的新技术适当提升安全能力，强化风险应对（监测、预警、防护、处置、溯源等）能力。

（2）建立规范的信息化安全运营体系，以安全视角规范教育网安全运营的整个过程，形成安全业务标准与流程。

（3）建立网络安全运营中心，安全运营实行分级保障，加强安全运营的可持续性建设。

6.2.4总体安全设计

6.2.4.1技术防护措施

整个技术防护体系采取的主要安全措施如下：

（1）采用防火墙系统对区域边界进行访问控制，根据业务需求，设置访问控制策略，定期进行安全策略的优化和维护。

（2）采用入侵防御系统，并开启防火墙的AV模块（或部署防病毒网关），对网络入侵行为和网络层病毒进行检测和阻断，并进行告警。

（3）采用专业抗APT攻击系统实现对新型网络攻击行为的检测、发现，并结合专家服务进行分析处置。

（4）采用一体化终端安全管理系统、虚拟机化安全管理平台实现对物理主机、虚拟主机的安全防护，并对终端进行集中安全管控、集中病毒管理、统一补丁管理和安全审计。

（5）采用SSL VPN实现对远程通信传输、远程终端数据的安全防护，实现基于互联网的传输加密和数据安全，并进行远程接入用户身份认证和访问控制。

（6）采用堡垒机实现对设备的集中管理和运维审计，并实现运维管理日志的集中存储和安全运维。

（7）应用系统开发同步考虑相关安全功能的实现，对重要的业务数据和系统鉴权数据进行加密存储。

（8）采用应用身份认证系统实现对应用的双因素认证，并通过集成SSL VPN实现应用数据的传输安全。

（9）采用网络审计系统、数据库审计系统、上网行为审计系统、一体化终端安全管理系统的审计功能实现对用户行为审计的全覆盖，并满足远程访问和上网行为审计需求。

（10）采用态势感知与安全运营平台和抗APT攻击系统实现全网安全设备日志和安全事件的统一分析和告警，实现对高级威胁和未知威胁的发现、检测和告警，并提供安全事件报表。

（11）采用防火墙集中管理与分析平台实现全网防火墙的自动化策略优化、下发、维护，实现策略可视化。

（12）采用数字证书认证系统（教育CA、广西政务CA等）进行教育网用户的身份认证，实现多因素身份认证。

6.2.4.2网络安全保护等级标准

根据《关于广西教育行业网络安全等级保护工作实施意见》的要求，教育行业网络安全保护等级要求如下：

教育行政管理部门网络安全保护等级表

| 序号 | 分类 | 信息系统 | 安全保护等级 | | |
| --- | --- | --- | --- | --- | --- |
| 自治区级 | 地市 | 区县 |
| A1 | 政务  管理类 | (01)办公与事务处理 | 第二级 | 第二级 | 第一级 |
| A2 | (02)公文与信息交换 | 第三级 | 第二级 | 第一级 |
| A3 | (03)人事管理 | 第二级 | 第二级 | 第一级 |
| A4 | (04)财务管理 | 第二级 | 第二级 | 第一级 |
| A5 | (05)资产管理 | 第二级 | 第二级 | 第一级 |
| A6 | (06)信访管理 | 第二级 | 第二级 | 第一级 |
| A7 | (07)档案管理 | 第二级 | 第二级 | 第一级 |
| A8 | (08)党务管理 | 第二级 | 第二级 | 第一级 |
| A9 | (09)科研管理 | 第二级 | 第二级 | 第一级 |
| A10 | (10)教育统计管理 | 第二级 | 第二级 | 第一级 |
| A11 | (11)决策支持 | 第二级 | 第二级 | 第一级 |
| A12 | (12)应急指挥 | 第二级 | 第二级 | 第一级 |
| A13 | (13)舆情监测与管理 | 第二级 | 第二级 | 第一级 |
| A14 | (14)高等教育招生计 | 第二级 | 第二级 | 第一级 |
| A15 | (15)普通高校招生网 | 第三级 | 第三级 | 第一级 |
| A16 | (16)教育考试考务管理与服务 | 第三级 | 第二级 | 第一级 |
| A17 | (17)评审、表彰管理 | 第二级 | 第二级 | 第一级 |
| A18 | 学校  管理类 | (01)学校管理 | 第二级 | 第二级 | 第一级 |
| A19 | (02)学科、专业管理 | 第二级 | 第二级 | 第一级 |
| A20 | (03)教学改革管理 | 第二级 | 第二级 | 第一级 |
| A21 | (04)教学质量评估 | 第二级 | 第二级 | 第一级 |
| A22 | (05)校园安全与稳定管理 | 第二级 | 第二级 | 第一级 |
| A23 | (06)教育经费监管 | 第二级 | 第二级 | 第一级 |
| A24 | 学生  管理类 | (01)学生学籍管理 | 第三级 | 第二级 | 第一级 |
| A25 | (02)招生录取管理 | 第三级 | 第三级 | 第一级 |
| A26 | (03)学生资助管理 | 第三级 | 第二级 | 第一级 |
| A27 | (04)学位授予管理 | 第三级 | 第二级 | 第一级 |
| A28 | 教师  管理类 | (01)教师基本信息管 | 第二级 | 第二级 | 第一级 |
| A29 | (02)教师资格认定管 | 第二级 | 第二级 | 第一级 |
| A30 | (03)教师培训管理 | 第三级 | 第二级 | 第一级 |
| A31 | (04)教师教育管理 | 第二级 | 第二级 | 第一级 |
| A32 | (05)教师职称管理 | 第二级 | 第二级 | 第一级 |
| A33 | 综合  服务类 | (01)门户网站 | 第三级 | 第二级 | 第一级 |
| A34 | (02)论坛、社区类网站 | 第二级 | 第二级 | 第一级 |
| A35 | (03)教育教学资源 | 第二级 | 第二级 | 第一级 |
| A36 | (04)毕业、就业信息管理 | 第二级 | 第二级 | 第一级 |
| A37 | (05)电子邮件 | 第二级 | 第二级 | 第一级 |
| A38 | (06)视频服务 | 第二级 | 第二级 | 第一级 |
| A39 | (07)安防监控 | 第二级 | 第二级 | 第一级 |
| A40 | (08)内网门户与身份 | 第二级 | 第二级 | 第一级 |
| A41 | (09)公共数据库 | 第二级 | 第二级 | 第一级 |
| A42 | (10)运维管理 | 第二级 | 第二级 | 第一级 |

6.3安全技术体系

6.3.1安全物理环境

物理安全是整个网络系统安全的前提，可能面临的物理安全风险有：地震、水灾、火灾、电源故障、电磁辐射、设备故障、人为物理破坏等，这些风险都可能造成系统的崩溃。因此，物理安全必须具备环境安全、设备物理安全和防电磁辐射等物理支撑环境，保护网络设备、设施、介质和信息免受自然灾害、环境事故以及人为物理操作失误或错误导致的破坏、丢失，防止各种以物理手段进行的违法犯罪行为。

等级保护基本要求对系统的物理安全要求较为严格，主要涉及的方面包括环境安全（防火、防水、防雷击等）设备和介质的防盗窃防破坏等方面。具体包括：物理位置选择、物理访问控制、防盗窃和防破坏、防雷击、防火、防水和防潮、防静电、温湿度控制、电力供应和电磁防护等十个控制点。

网络中心机房建设应严格按照国家对信息系统机房的建设标准，机房应在各方面满足等级保护的相关要求。

教育网所涉及的服务器、存储设备、网络设备、软件系统等软硬件均位于中国境内，符合网络安全等级保护对云计算安全的扩展要求。

6.3.2安全通信网络

参照等级保护的要求对系统安全区域进行划分设计，实现内部办公、数据共享交换与外部接入区域之间的安全隔离，并对核心区域进行冗余建设，用以保障关键业务系统的可用性与连续性。

安全域是由安全保护对象中安全计算环境和安全区域边界综合组成，根据安全域的描述可以把保护对象进行进一步的划分，同时使整个网络逻辑结构清晰。

安全域可以根据其更细粒度的防护策略，进一步划分成安全子域，其关键是能够区分防护重点，形成重要资源重点保护的策略。

6.3.2.1业务保障原则

安全域方法的根本目标是能够更好的保障网络上承载的业务。在保证安全的同时，还要保障业务的正常运行和运行效率。

6.3.2.2适度安全原则

在安全域划分时会面临有些业务紧密相连，但是根据安全要求又要将其划分到不同安全域的矛盾，必须综合考虑业务隔离的难度和合并安全域的风险，从而给出合适的安全域划分。

6.3.2.3结构简化原则

安全域方法的直接目的和效果是要将整个网络变得更加简单，简单的网络结构便于设计防护体系。

6.3.2.4等级保护原则

安全域的划分要做到每个安全域的信息资产价值相近，具有相同或相近的安全等级安全环境安全策略等。

6.3.2.5立体协防原则

安全域的主要对象是网络，但是围绕安全域的防护需要考虑在各个层次上立体防守，包括在物理链路网络主机系统应用等层次；同时，在部署安全域防护体系的时候，要综合运用身份鉴别访问控制检测审计链路冗余内容检测等各种安全功能实现协防。

6.3.2.6生命周期原则

对于安全域的划分和布防不仅仅要考虑静态设计，还要考虑不断地变化；另外，在安全域的建设和调整过程中要考虑工程化的管理。

6.3.3安全区域边界

6.3.3.1边界访问控制

（1）边界防护与访问控制

针对新的边界安全威胁，边界访问控制已经成为基本安全措施，必不可少，但为了更加有效的应对当前的网络威胁，防火墙设备应当更加智能化、联动化，以满足安全有效性和防御实时性的切实需求。

当前，下一代防火墙技术已经逐步成熟，通过相关功能实现及策略配置，可实现上述要求，防火墙主要功能及配置要求如下：

1）访问控制

能够基于IP、安全域、VLAN、时间、用户、地理区域、服务协议及应用等多种方式进行访问控制，一条安全策略可配置应用控制、入侵防护、URL过滤、病毒检测、内容过滤、网络行为管理等高级访问控制功能。能对HTTP、SMTP、POP3、IMAP、FTP、TELNET协议进行细粒度的控制，过滤不受信任的网络行为。

2）应用层访问控制

能实现文件过滤、URL过滤、邮件过滤等、实现针对主要的应用协议如HTTP、FTP、POP3、SMTP、IMAP等的双向内容传输过滤，可预定义或自定义敏感信息库进行敏感信息定义。

3）入侵防范

对于主要攻击能进行防护，包括：Flood（SYN Flood、ICMP Flood、UDP Flood、IP Flood）、恶意扫描（禁止tracert、IP地址扫描攻击、端口扫描）、欺骗防护（IP欺骗、DHCP监控辅助检查）、异常包攻击（Ping of Death、Teardrop、IP选项、TCP异常、Smurf、Fraggle、Land、Winnuke、DNS异常、IP分片、ICMP管控（禁止ICMP分片、禁止路由重定向报文、禁止不可达报文、禁止超时报文、ICMP报文大小限制）、应用层Flood（DNS Flood、HTTP Flood）、SYN Cookie等。

4）负载均衡

作为主要的链路设施，能实现基于IP、ISP、应用、用户、服务等的多链路负载均衡，DNS流量的负载均衡，基于服务器地址的负载均衡。

5）高可靠性

具备双机热备功能，在路由和透明模式下能支持“主-备”、“主-主”模式，能实现接口联动，链路探测。

6）动态QoS功能

可配置带宽限制策略。策略类型包括共享型和独享型，用户优先级分为高、中、低，服务类型包括应用层的多种协议。在用户都满足保证带宽情况下，高优先级用户将抢占中、低优先级用户带宽，中优先级用户将抢占低优先级用户带宽。当网络中存在空闲带宽时，防火墙系统会根据当前网络带宽分配情况，自动将空闲带宽分配给重要业务，保证重要业务的正常访问。

7）支持IPv6

能够支持完整的双栈协议，支持IPv6下的多种功能，包括网络功能和安全功能，包括IPv6接口、IPv6路由、IPv6认证管理、IPv6日志管理、IPv6 VPN、IPv6安全功能及安全策略等。

8）虚拟防火墙

具备虚拟系统功能，即将防火墙虚拟成多个相互隔离并独立运行的虚拟防火墙，每一个虚拟系统都可以为用户提供定制化的安全防护功能，并可配备独立的管理员账号。

9）协同联动

能够与终端安全管理系统、云端的URL库、病毒库、应用识别库等资源进行联动，提升对已知威胁的识别效率，并能对在终端发现的威胁从网络层及时阻断。

10）日志管理

对各类日志，如流量日志、威胁日志、URL过滤日志、邮件过滤日志、行为日志等进行分析和日志外发，能基于IP、用户、接口、地区、应用等过滤条件搜索自定义时间段内的历史日志。

各安全区域都应针对自身业务特点设定访问控制策略，下表表述了各安全区域之间的访问控制关系，在对各网络安全区域设置安全策略时，可以此为参考原则进行设置：

网络安全区域设置安全策略参考表

| 目的源 | 边界接入区 | 核心网络区 | 前置服务区 | 安全接入区 | 安全云资源池 | 安全管理区 | 互联网接入区 | 应用服务器区 | 数据库服务区 |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 边界  接入区 | — | 授权 | 互通 | 授权 | 禁止 | 禁止 | 互通 | 禁止 | 禁止 |
| 核心  网络区 | 互通 | — | 互通 | 授权 | 互通 | 互通 | 互通 | 互通 | 互通 |
| 前置  服务区 | 禁止 | 禁止 | — | 互通 | 互通 | 禁止 | 禁止 | 互通 | 禁止 |
| 安全  接入区 | 互通 | 互通 | 授权 | — | 授权 | 授权 | 授权 | 授权 | 授权 |
| 安全  云资源池 | 互通 | 禁止 | 互通 | 授权 | — | 授权 | 禁止 | 禁止 | 互通 |
| 安全  管理区 | 互通 | 互通 | 禁止 | 授权 | 互通 | — | 互通 | 互通 | 互通 |
| 互联网  接入区 | 互通 | 互通 | 互通 | 授权 | 授权 | 互通 | — | 禁止 | 禁止 |
| 应用  服务区 | 禁止 | 互通 | 互通 | 授权 | 互通 | 互通 | 禁止 | — | 授权 |
| 数据库  服务区 | 互通 | 授权 | 禁止 | 授权 | 禁止 | 互通 | 禁止 | 禁止 | — |

访问控制策略应根据网络及业务变化和单位的安全基线进行合理配置和及时调整，及时删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化。

防火墙部署在各安全域边界，在互联网接入边界、安全管理区边界、核心业务区边界均需单独部署防火墙设备，设置严格的访问控制规则，并定期进行策略的检查和优化。

（2）边界隔离与访问控制

通过部署防火墙或开通虚拟化防火墙服务来实现网络边界的安全访问控制，该组件集成了访问控制、用户授权访问、虚拟系统、行为管理、应用层综合安全防护等功能，并支持与威胁感知、安全管理中心等智能联动，实现一体化的智能安全防护，核心功能包括：

1）智慧发现。通过与其他安全系统的协同联动，借助外部的威胁情报、大数据分析等能力，对本地网络流量所产生的数据进行深入的检测和分析，从而及时发现传统防护手段无法检测到的威胁。

2）智慧调查。系统对运行过程中所产生的多维数据进行自动关联，并利用可视化和递进式数据钻取的设计，给用户提供了分析线索、发现异常、回溯事件等一系列分析面板，降低了用户对风险、威胁、异常进行分析的难度。

3）智慧处置。基于“智慧调查”的分析回溯结果，对受害主机或可确定的攻击源执行一键式的处置，并对处置后的结果进行持续监控，完成威胁管理的闭环操作。

通过主动网络扫描或渗透测试等方式验证网络隔离有效性。

防火墙部署在各安全域边界，在互联网接入边界、安全管理区边界、核心业务区边界均需单独部署防火墙设备，设置严格的访问控制规则，并定期进行策略的检查和优化。

6.3.3.2边界入侵防范

（1）边界入侵防御

1）安全风险

随着国家信息化的发展，网络攻击活动也愈演愈烈，而网络攻击造成的破坏性因信息化程度的高度集中也越来越大。主要呈现如下趋势：网络应用越来越复杂，单纯的依靠端口识别应用以达到攻击检测的目的不再有效；网络带宽的快速增长给入侵防护系统的处理能力带来挑战，仅依靠防火墙这样的边界防护设备实现网络攻击检测已经远远不能满足要求，具备大流量业务并发处理能力的专业设备尤其重要；除具备针对网络层/传输层的基础攻击防护外，针对应用层深度识别和防御能力越发重要。

因此，如何有效的对网络攻击行为、异常行为进行监测防御，是边界安全的重要一环。

2）控制要求

根据等级保护的要求，针对“安全区域边界”和“安全计算环境”的防护要求包括：

①应在关键网络节点处检测、防止或限制从外部发起的网络攻击行为。

②应在关键网络节点处检测、防止或限制从内部发起的网络攻击行为。

③检测到攻击行为时，记录攻击源IP、攻击类型、攻击目标、攻击时间，在发生严重入侵事件时应提供报警。

④应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。

3）控制措施

在网络区域的边界处，需要通过部署入侵防御设备对网络攻击行为进行检测与阻断，并及时产生报警和详尽的报告。

入侵防御设备需要具备以下功能：

①具备新一代检测分析技术

新一代检测引擎能结合异常检测与攻击特征数据库检测的技术，同时也包含了深层数据包检查能力，除了检查第四层数据包外，更能深入检查到第七层的数据包内容，以阻挡恶意攻击的穿透，同时不影响正常程序的工作。

②多层多类型攻击检测

可以检测多层多种类型攻击，如应用型攻击：包括Web cc、http get flood、DNS query flood等攻击；流量性攻击：包括SYN Flood、UDP Flood、ICMP Flood 、ARP Flood、Frag Flood、Stream Flood等攻击；蠕虫连接型攻击；普通常见攻击：包括ipspoof、sroute、land、TCP标志位攻击、fraggle攻击、winnuke、queso、sf\_scan、null\_scan、xmas\_scan、ping-of-death、smurf、arp-reverse-query、arp-spoofing等。

③双向攻击检测

通过对进出网络的流量进行采集分析，可对由内向外发起的网络攻击行为和由外向内发起的网络攻击行为均进行检测和告警。

④日志告警和阻断

网络入侵防御系统除了需要能检测辨别出各种网络入侵攻击，保护网络及服务器主机的安全外，还需要提供完整的取证信息，提供客户追查黑客攻击的来源，这些信息包括黑客攻击的目标主机、攻击的时间、攻击的手法种类、攻击的次数、黑客攻击的来源IP地址等，并提供包括Email/SNMP trap/声音等方式的告警。对于在线部署模式，可以对攻击行为进行实时阻断。

⑤高可用性

对于在线部署模式的设备，当出现软件故障、硬件故障、电源故障时，系统bypass电口自动切换到直通状态以保障网络可用性，能够避免单点故障，不会影响业务。

4）设备部署

入侵防御系统支持在线部署和旁路部署，针对广西自治区教育厅的网络环境及业务需求，通过在互联网接入边界部署入侵防御系统，实现对网络事件的检测，入侵防御系统采用串接方式部署在防火墙和核心交换机之间，能够有效检测和阻断入侵攻击。

（2）高级威胁攻击检测

1）安全风险

近年来，具备国家和组织背景新型网络攻击日益增多，其中最为典型的为APT攻击，而APT攻击采用的攻击手法和技术都是未知漏洞、未知恶意代码等未知行为，在这种情况下，依靠已知特征、已知行为模式进行检测的IDS、IPS在无法预知攻击特征、攻击行为模式的情况下，理论上就已无法检测APT攻击。

APT攻击的隐蔽性、持久性和复杂性远超普通的网络攻击行为，且针对的往往是政府、企业、金融等单位的关键应用系统，正式由于APT攻击的这些特点，其造成的破坏性往往也是巨大的，使单位、行业乃至国家安全面临严峻挑战，必须采用专门的技术措施对这类攻击进行检测、发现和分析，并能够追踪溯源。

2）控制要求

面对新的安全威胁形势，新等级保护标准中除了对边界攻击检测能力提出要求外，还明确提出了对高级威胁攻击和未知攻击的检测、发现能力，应采取技术措施对网络行为进行分析，实现对网络攻击特别是新型网络攻击行为的分析。

3）控制措施

通过部署专业的APT检测设备，实现对新型网络攻击行为的发现、分析、追溯的能力，设备所需具备的功能包括：

①APT攻击发现

由于APT攻击的复杂性和背景的特殊性，仅依赖于单一企业的数据经常无法有效的发现APT攻击，难以做到真正的追踪溯源，而从互联网数据进行发掘和分析，由于任何攻击线索都会有相关联的其他信息被互联网数据捕捉到，所以从互联网进行挖掘可极大提升未知威胁和APT攻击的检出效率，而且由于数据的覆盖面更大，可以做到攻击的更精准溯源。

②APT攻击定位、溯源与阻断

用威胁情报的形式对各种攻击中常出现的特点和背景信息进行记录和传输，而威胁情报将通过统一的规范化格式将攻击中出现的多种攻击特征进行标准化，可对未来扩展攻击特征并进行精准攻击定位和溯源提供支撑。

对APT攻击的定位、溯源和阻断离不开专业的安全分析团队，需要能够针对用户网内发现的APT攻击等行为进行深度挖掘和分析，减少损失。

③未知恶意代码检测

针对新型攻击和病毒，需要采用机器学习等人工智能算法，通过恶意代码智能检测技术，对海量程序样本进行自动化分析，解决大部分未知恶意程序的发现问题。

④未知漏洞攻击检测

可采用基于沙箱的未知漏洞攻击检测引擎对客户端应用中已知漏洞和未知漏洞的攻击利用进行检测。

4）设备部署

APT攻击检测设备旁路部署在核心交换机上，对用户网络中的流量进行全量检测和记录，所有网络行为都将以标准化的格式保存于数据平台，云端威胁情报和本地文件威胁鉴定器分析结果与本地分析平台进行对接，为用户提供基于情报和文件检测的威胁发现与溯源的能力。

5）云计算边界入侵防御

通过主机入侵防御组件对云内流量包进行检测过滤，主要功能包括：

●支持多种针对系统、应用漏洞的入侵防御规则，并定期更新规则库。

●对已知的漏洞进行虚拟修补，在虚拟机系统及应用不进行安全补丁升级的情况下，防御针对漏洞的攻击。

●系统自动侦测虚拟机系统的内容，动态的调整用于检测的入侵检测的规则库，提高检测的效率。

●自动更新功能，及时防御针对最新漏洞的攻击。

a）东西向攻击防护

通过虚拟化安全的主机防火墙组件对云内主机间的流量进行流量识别、业务关系拓扑、网络访问控制、安全策略管理等安全防护能力。

●对虚机进行微隔离，不但能控制南北向流量，还可以控制云平台内部虚拟机之间的东西向流量。

●按照IP 地址、端口、流量类型以及流量方向来配置防火墙规则。

b）高级威胁感知系统

高级威胁感知系统基于自有的多维度海量互联网数据，进行自动化挖掘与云端关联分析，提前洞悉各种安全威胁，并向客户推送定制的专属威胁情报。同时结合部署在客户本地的软、硬件设备，系统能够对未知威胁的恶意行为实现早期的快速发现，并可对受害目标及攻击源头进行精准定位，最终达到对入侵途径及攻击者背景的研判与溯源。

c）可视化分析告警

通过对异常流量的汇总采集分析，检测出外部-内部或内部-外部的异常攻击行为，并通过可视化展示或告警方式通知管理员。

●支持海量安全日志数据的分析及查询。

●安全威胁地图，描述安全威胁发生的地理位置。

●网络流量地图，对网络的新增连接、数据流量、地理位置的分析及数据挖掘。

●以虚拟机、操作系统、应用程序、攻击类型、恶意代码类型、地理位置、时间等多个维度。

●对文件、网络的海量安全数据进行关联性分析，并辅以多种图表形式，对同一数据进行描述，便于用户理解。

●支持安全事件的数据挖掘，便于管理人员及时准确的找到攻击源，阻断安全威胁。

6.3.3.3边界完整性检测

（1）网络安全准入

针对网络层的非授权连接行为管控可以通过网络安全准入系统（NAC）进行控制，网络安全准入系统需实现以下功能：

1）安全管理与访问控制

利用网络安全准入系统的动态检测技术和安全策略管理，针对接入用户和终端进行网络访问控制功能。不符合安全策略的计算机终端进行隔离，并友好提示，提供向导式的安全修复指引。拦截可疑的计算机终端或设备、恶意尝试认证的用户，支持强制下线和账号锁定功能。对接入用户进行动态VLAN的分配管理，有效的对网络访问权限进行控制。

2）终端安全合规检查

网络安全准入系统的安全检查策略会检测终端入网安全状态，能快速定位发现入网计算机终端的安全合规状态，并利用其本地防火墙隔离管控技术立即将这个设备与网络上的其它设备隔离起来，只能够访问修复区，同时依照策略进行引导修复。对于已授权合规终端，如发现运行阶段又不符合安全检查策略，可调用周期检查或定时检查引擎，对该终端的安全状态进行二次检查，期间如发现不合规进行再次隔离，禁止其访问企业核心资源，可提供安全检查结果详情和全网安全状态统计等日志报表。

3）访客注册申请

针对外来人员临时性的访问需求，能够进行访客入网管理，包括访客用户注册申请、访客认证、用户审批流程，经管理员审批或系统自动审批后才能认证入网，审批结果可邮件通知用户。

4）第三方认证源联动

能够实现多种认证源认证方式，包括本地用户、AD认证、LDAP认证、Email认证、Http认证适应用户不同网络环境，满足用户实名制认证、集中统一管理的入网需求。

5）认证绑定管理

支持多种条件绑定认证，即用户和终端、交换机、VLAN、交换机端口等进行绑定认证、提高入网安全强度。

6）设备例外管理

用户网络中存在大量的哑终端设备，如：网络打印机、视频会议系统等设备，并分散在各地，能够提供设备的白名单管理，当添加到白名单的合法设备可以直接接入网络，反之非法设备不允许接入，此方式可适应于多种认证技术方式，如：Portal和802.1X认证方式。

7）强制隔离

用户正常的802.1x认证成功后，如果认证会话没有过期网络会持续可用，系统专有的认证客户端可以实时接收认证服务器的控制指令，管理员可以在任何时候强制在线的用户和终端下线、注销当前登录的网络，确保非正常情况下可对终端入网进行控制和强制隔离处理。

网络安全准入系统（NAC）采用旁路部署，通过监听来发现和评估哪些终端入网是否符合遵从条件，判断哪些终端是否允许安全访问企业核心资源，不符合会被自动拦截要求认证或安装客户端才能进行访问，并可配置入网安全检查策略，不符合进行隔离和修复，达到合规入网的管理规范要求。

（2）违规外联检测

对于终端的非法外联可以通过终端安全管理系统或者采用专业的上网行为管理设备进行控制。终端安全管理系统可对终端的外联端口、外联能力进行检查和阻断，上网行为管理设备通过在网络出口处进行安全策略的配置，限制单位用户的外联访问行为，具体功能如下：

1）上网行为管理系统

a）URL访问审计与过滤

采用URL分类数据库，通过管理员配置基于URL分类的控制策略（策略条件可包括用户、部门、时间段、访问类别、URL关键字、网页内容关键字、下载文件类型等），进行WEB访问控制，发现非法访问可进行阻断、记录或报警。

b）应用控制

通过应用特征与行为特征对应用进行识别。所谓应用特征，是指在成序列的数据包的应用层信息中，存在有规律的字节特征，它可以唯一地标识某种应用协议，行为特征，是指连续多个包或者多个并发的网络连接表现出来的某种行为模式具有一定规律性，通过这些行为模式可以识别特征值不明显的应用类型。通过精细化的控制策略设置，可以实现对单位应用访问的精细化管理。

c）内容审计和过滤

对内容的审计可以有效控制信息的传播范围，控制敏感信息的泄露，避免可能引起的安全风险，内容审计和过滤包括邮件收发审计和过滤、论坛发帖审计和过滤、搜索引擎关键字审计和过滤、HTTP文件传输审计和过滤、FTP文件传输审计和过滤等。

d）共享接入监控

共享接入是指使用NAT等技术将一个网络出口共享到多个主机，共享接入监控能够对接入网络的设备做观察、控制，能够检测到一个用户或IP所共享的终端数量，并可以对数量做策略控制，以达到掌控用户终端数量的目的，在监控到用户使用的终端数后，可以对此进行控制，屏蔽该用户的上网流量。

e）日志审计

能够完整地记录内网用户网络访问的日志，包括上网时间、网络流量、Web访问记录、接收与发送的邮件等等。为进一步的查询统计与报表分析提供了完整的基础信息。

2）终端安全管理系统

为了防止计算机终端用轻易通过拨号、私设代理、多网卡通讯等非法外联手段，造成内部机密外泄的情况发生，终端安全管理系统提供非法外联管控功能，可根据探测类型，使用对应的技术手段如域名解析，对传入的ip或是网址进行连接，如果连接成功则根据策略处理措施，进行对应的提示、断网或关机处理。

a）外联设备控制（可以禁用终端上可能运行的外联设备——冗余有线网卡、移动数据网卡、MODEM设备、ISDN设备、ADSL设备、WIFI及SSID例外）

b）外联能力探测（选择探测方式发现终端是否具有外联能力）

c）外联控制措施（发现终端具有外联能力后的处理措施——提示、断网、关机）

上网行为管理系统可以串接和旁路镜像部署在单位的互联网出口处，在串接模式下，串接方式能实现对上网行为的控制，并完整审计所有上网数据。串接包括网桥和网关两种模式，采用网桥模式时，当单位拥有两个互联网出口，且单位内部不同教育城域网需要通过不同的互联网出口连接互联网时，上网行为管理系统可提供双入双出，双网桥的部署模式。通过一台设备即可同时管控两条链路内的用户互联网行为。

（3）边界恶意代码检测

下一代防火墙一般均具有专业的AV模块，能在网络重要节点处（如互联网入口）进行病毒的检测和清除，但考虑到部分单位已有的防火墙性能不高，也可以采用专业的防病毒网关，在网络边界处进行病毒的检测和阻断。

下一代防火墙通过启用一体化安全防护策略，将反病毒、漏洞防护、防间谍软件、恶意URL防护等功能集成到一条策略，并基于优越的架构设计保障高性能的安全能力。

通过在互联网边界启用下一代防火墙的漏洞防护、防间谍软件、反病毒、URL过滤等功能，基于本地安全引擎，能高效拦截常见漏洞入侵、间谍软件、病毒、木马、钓鱼网站、恶意URL访问等网络威胁。

同时，防火墙通过云端协同可以极大提升特征库数量级，补充本地识别库，并提升防火墙对高级威胁的识别能力，提高防火墙拦截的精确度和高效性。

防火墙的特征库能够支持自动升级，定期进行病毒库的升级和系统的更新。

为实现对病毒的实时阻断，在互联网边界需串接防火墙，开启AV模块，或在防火墙后串接专业的防病毒网关，实现从网络层检测和阻断恶意代码。

（4）网络安全审计

网络安全审计系统通过镜像获取通过核心交换机上流量数据对整个网络的流量进行审计分析，对用户的行为进行审计。包括以下内容：

●对用户的HTTP、邮件、FTP、TELNET等应用进行审计。

●对远程桌面、QQ远程等远程访问行为进行审计。

●对用户的互联网访问行为进行审计。

●本地日志可以FTP、USB等方式导出，支持将日志发送至外置日志存储系统，确保日志记录满足合规要求。

网络安全事件的踪迹一般都分布在网络的边界设备、安全设备、访问控制设备的日志中，除对网络流量中用户的行为进行审计分析外，发现网络安全事件也是网络安全审计的重要目标，集中安全审计系统通过收集网络设备、安全设备、服务器、应用系统等的日志信息，结合网络流量日志进行关联分析，可以快速发现网络安全事件，并进行定位和报警。

云服务客户根据需求选择开通日志审计、云安全运维审计等审计系统，对云上用户访问行为、操作行为、安全运维审计等行为进行细粒度的日志审计、存储、分析等。

1）综合日志审计

①提供覆盖到每个用户的安全审计功能，对应用系统重要安全事件进行审计。

②保证无法单独终端审计进程，避免非授权和未预期地删除、修改或覆盖审计记录。

③审计记录的内容至少应包括事件的日期、时间、发起者信息、类型、描述和结果等。

④应提供对审计记录数据进行统计、查询、分析及生成审计报表的功能。

⑤日志审计功能应能提供给用户访问行为审计、审计信息查询、审计信息分析等模块，以及异常行为管理和配置与管理等供管理员使用的模块。

2）访问行为审计

对系统访问行为数据进行收集、整理的基础上进行分析和审计。包括：用户标识与鉴别、自主访问控制的所有操作记录、重要用户行为（如用超级用户命令改变用户身份，删除系统表）、系统资源的异常使用、重要系统命令的使用（如删除文件、数据库中的记录）等。

3）审计信息查询

查询范围应包括日期与时间、触发事件的主体与客体、事件的类型、事件中请求的来源、事件的结果等内容。

审计人员应能够通过内置的查询定义器方便地制作新的查询操作、搜索范围以及查询结果的表现形式，如列表、分组排列、柱状图、饼状图等。通用数据查询系统可以保存或按指定格式导出（如Excel或XML）查询结果，支持对查询结果的分析加工。用户还可以在查询结果范围内进行再查询。

4）异常行为管理

系统应提供异常行为注册、调整、删除和查询等功能，应具备对系统中的异常行为进行分类、注册、定义影响级别、配置报警方式（如短信、邮件和其它方式）的功能。

5）系统配置与管理

配置与管理模块为后台管理员、审计人员和业务操作员提供对系统进行管理、配置的功能。主要应包括：配置查询条件、需要监控的资源以及报警方式等。对于查询条件，应能通过简单定义就可以实现复杂的查询条件组合查找需要的数据，还应可以自动跟踪查询与该数据相关联的明细数据；另外，系统应还可以通过配置实现对于重要应用系统和系统资源监控的添加和删除。

6.3.4安全计算环境

6.3.4.1主机身份鉴别与访问控制

针对主机的双因素身份鉴别一般可采用专业的终端安全登录产品，终端安全登录产品可结合现有的CA系统实现基于数字证书的双因素认证，终端安全登录产品所使用的密码设备应符合国家密码管理相关要求。

针对主机访问控制的要求，采用服务器加固系统，并进行以下安全配置：

（1）启用访问控制功能，依据安全策略控制用户对资源的访问；

（2）根据管理用户的角色分配权限，实现管理用户的权限分离，仅授予管理用户所需的最小权限；

（3）严格限制默认帐户的访问权限，重命名系统默认帐户，修改这些帐户的默认口令；

（4）及时删除多余的、过期的帐户，避免共享帐户的存在；

（5）对重要信息资源设置敏感标记；

（6）依据安全策略严格控制用户对有敏感标记重要信息资源的操作。

对重要的主机系统采用专业的主机安全加固系统对主机进行整体安全防护，设置强制安全访问控制策略，从而使操作系统达到B1级高安全级别。对数据库进行安全配置，对于存储大量敏感数据的数据库采用安全数据库或数据库防火墙进行保护。

6.3.4.2一体化终端安全防护

综合分析单位面临的终端安全风险，需要一个综合的终端安全管理系统，以应对不同层面的安全需求，满足合规要求，而满足这些安全需求的同时，又不会割裂这些系统之间的关系，使得他们能在统一的安全环境里执行一致的安全策略，并互相协同，发挥最大的安全防护效率。

采用终端安全管理系统作为终端合规管控一体化解决方案。通过建设恶意代码防范体系、落实终端安全管理技术措施、启用统一终端运维、开启安全审计功能，来建设终端合规一体化体系，一体化终端安全管理的建设内容如下：

（1）终端恶意代码防护

全网部署终端安全管理系统客户端代理，通过集中管理端实现对病毒查杀策略、病毒库的统一升级管理。通过采用云查杀引擎、未知病毒检测等新技术，解决传统防病毒软件本地特征库对新型病毒查杀效果不明显的问题。

（2）终端统一安全管控

在终端安全管理系统的控制中心制定策略，进行全网终端的流量监控、非法外联监控、应用程序黑白名单控制、外设管控、桌面安全加固等。

（3）终端软件管理

通过策略配置和日志报表功能，管理员可以掌握网内软件使用情况，及时发现异常，保证企业内部网软件的正常运行和软件安全性，支持单位软件的统一分组、定时分发，并可实现自动安装应用以及强制卸载应用，帮助管理员按照企业规定管理终端用户软件的安装。

（4）统一补丁升级和管理

网络中存在各种不同类型的操作系统及不同版本的操作系统都需要进行全面的补丁管理，终端安全管理系统控制中心对全网计算机进行漏洞扫描把计算机与漏洞进行多维关联，根据终端或漏洞进行分组管理，并且能够根据不同的计算机分组与操作系统类型将补丁错峰下发，并能实现对补丁库的统一升级和管理。

（5）终端统一安全运维

终端安全管理系统统一运维功能，实现全网终端硬件资产管理，并且通过远程协助功能，当终端需要远程帮助的时候，运维人员向终端用户发送远程控制请求，等终端用户确认后，协助IT维护人员高效的完成终端运维工作。

（6）终端综合审计

终端安全管理系统通过综合审计功能，对终端用户的行为进行审计，审计内容包括软件使用日志、外设使用日志、开关机日志、系统帐号日志、文件操作日志、文件打印日志、邮件记录日志等；并提供报表功能，对终端安全日志、漏洞修复、病毒日志、木马查杀、插件清除、安全配置、文件及应用日志、终端事件告警等信息进行报表统计。

在网络内部部署终端安全管理系统控制中心和终端，终端通过控制中心连接到升级服务器进行升级、更新等。终端根据控制中心制定的安全策略，进行杀毒、修复漏洞、运维管控、移动存储管理等安全操作。

6.3.4.3主机脆弱性评估与检测

漏洞扫描系统针对传统的操作系统、网络设备、防火墙、远程服务等系统层漏洞进行渗透性测试。测试系统补丁更新情况，网络设备漏洞情况，远程服务端口开放等情况并进行综合评估，在黑客发现系统漏洞前提供给客户安全隐患评估报告，提前进行漏洞修复，提前预防黑客攻击事件的发生。

通过部署漏洞扫描系统，可以帮助用户快速建立针对自己网络的安全风险评估体系。

（1）发现内部资产

帮助用户快速发现内部资产，避免未知资产带来的安全风险，实现内部IT资产的标识和分类管理，方便安全扫描策略的部署何风险评估的进行

（2）实现针对内部网络的脆弱性评估

通过漏洞知识库以及多样的漏洞扫描策略，针对网络设备、系统主机、应用程序等存在的漏洞和风险进行有效评估，并生产完善的评估报告，帮助用户建立起高效的安全漏洞管理解决方案。

（3）建立完善的漏洞管理和风险评估体系

通过定期的漏洞扫描和漏洞验证帮助用户形成规范的全网漏洞管理体系，并辅以风险报表以及解决方案建议，为用户提供完整的从漏洞发现、验证、修复建议的流程。

（4）解决漏洞原因造成的安全问题

实时漏洞扫描，定期安全漏洞评估帮助用户及时修复当前系统中存在的漏洞，避免漏洞问题造成的安全威胁和带来的安全隐患。

漏洞扫描系统可旁路部署在待评估网络中的核心交换机上，网络可达待评估的主机、网络设备和系统软件。

6.3.4.4虚拟机安全防护

针对虚拟主机可以采用虚拟化安全管理系统对虚拟主机进行统一的安全防护。

（1）虚拟化安全管理系统可以实现以下功能。

1）恶意软件防护。无需在虚拟机内部安装杀毒软件，防止其受病毒、间谍软件、木马和其他恶意软件的侵害。能实现恶意代码特征库的自动更新。

2）进程管控。支持白名单和黑名单方式，可针对不同的用户场景灵活配置管控规则，未被允许的进程将无法使用，彻底阻止勒索软件或其他恶意软件执行。

3）防火墙。对虚机进行微隔离，不但能控制南北向流量，还可以控制云平台内部虚拟机之间的东西向流量。按照IP 地址、端口、流量类型以及流量方向来配置防火墙规则。

4）应用控制。对应用协议进行分类，针对分类配置阻断、放行策略，对于新增的应用，能自动应用分类的配置策略。自动更新应用解析的规则库，不断增加新应用的支持，及时识别更新后的网络应用。

5）入侵防护。对已知的漏洞进行虚拟修补，在虚拟机系统及应用不进行安全补丁升级的情况下，防御针对漏洞的攻击。防护SQL 注入，跨站脚本攻击及其他的利用Web 应用程序漏洞的攻击，并能及时防御针对最新漏洞的攻击。

6）DDoS防护。对TCP、UDP和ICMP Flood攻击的防护，能针对每台虚拟机单独进行流量清洗。

（2）虚拟化安全管理系统由管理中心和安全组件两部分组成。

1）管理中心。接收安全组件上传的安全事件和网络流量日志，通过多维度、细粒度的大数据分析，并以可视化的形式展现给用户，从而帮助用户对已知威胁进行溯源，并对未知威胁进行预警。

2）安全组件。安装在网络中心每个计算节点、物理服务器上，接收管理中心配置的安全策略，对虚拟机或物理终端进行文件、网络和系统的安全防护，并将安全事件及行为日志上传到管理中心进行分析。

6.3.4.5应用身份鉴别与访问控制

因此，需要实现对应用系统访问的双因素认证，采用身份认证服务系统可以实现对用户身份的统一管理和多种方式组合的强身份认证。

身份认证服务系统可以与安全接入网关（SSL VPN）共同构建应用身份解决方案，该解决方案主要实现以下功能：

（1）多因素身份认证

根据不同的应用场景，可以提供动态口令、数字证书、指纹、二维码等身份安全机制。

（2）口令传输安全加密

身份认证系统与终端间传输的认证信息进行加密处理，加密算法采用RSA、DES、3DES、AES等多种加密算法组合。为了满足国家信息安全的需要，系统同时支持SM系列国密算法，大大降低了认证信息被劫持、被破译的风险。

（3）数据传输加密

在用户通过认证接入SSL VPN后，客户端和服务端通信，传输的数据都默认使用安全的SSL传输技术。确保用户账号密码、动态秘钥、应用数据传输的高安全性及稳定性。同时支持移动终端隧道控制策略，实现移动终端连接VPN以后，移动终端数据只能走VPN，不能访问互联网，从而实现防止数据泄密。

同时，为了满足国密办信息安全的相关规定，加强密码算法的安全性。SSL VPN完整支持国密算法，包括 SM1、SM2、SM3、SM4。

（4）访问控制

为不同职责人员匹配不同业务应用，精细化访问控制技术能够细粒度控制接入可以到用户级、资源级，甚至下到URL和文件级的权限，这样不同的用户拥有不同的访问权限。

（5）虚拟工作区

为防止工作区的数据遗落到个人数据区，SSL VPN采用虚拟工作区进行数据分离。个人数据与企业数据进行隔离，落地数据加密，第三方应用或转发到其它设备当中无法打开查看。启用虚拟工作区之后，终端数据落地加密，数据采用AES256或者SM4加密算法，防止终端数据被拷贝出去而造成数据泄密。

当VPN客户端被卸载、设备进行了Root或者设备超过一定时间不能连接上网关的情况下，移动终端数据可以远程擦除，防止数据泄密。

身份认证系统分为两部分组成：硬件平台与客户端APP。硬件平台采用旁路部署在企业内网，与用户的业务系统/认证系统做到网络可达。

6.3.4.6 WEB应用安全防护

可以采用WEB应用防火墙对WEB应用进行安全防护。WEB防火墙可针对WEB应用实现以下防护功能。

（1）漏洞防护

Web应用防火墙能够对SQL注入、跨站脚本、代码执行、目录遍历、脚本源代码泄露、CRLF注入、COOKIE篡改、URL重定向等多种漏洞攻击进行有效防护。

（2）攻击防护

Web应用防火墙能够对用户请求提供多重检查机制和智能分析，确保对高安全风险级别攻击事件的准确识别率。针对Flood攻击、SQL注入、跨站脚本、目录遍历等主要攻击手段，WAF系统提供了有效识别、阻断并告警。

（3）网页代码检查

Web应用防火墙能够对用ASP、ASPX、JSP、PHP、CGI等语言编写的页面，对用SQL Server、MySQL、Oracle等数据构建的网站进行检查，能够在客户网站被挂马之前发现网站的脆弱点，从而使客户可以未雨绸缪，避免挂马事件的发生。

（4）访问加速

Web应用防火墙通过在现有的互联网中增加一层新的网络架构，将网站服务器内容缓存到系统内存中，使用户可以就近取得所需内容，降低服务器的压力，解决互联网拥挤的状况，提高用户访问服务器的响应速度。从而解决由于网络带宽小、用户访问量大、网点分布不均等原因所造成的用户访问网站响应速度慢的问题。

（5）挂马检测

多数攻击者在成功入侵并不采取直接的网站篡改，为了获取更多的经济利益往往采取比较隐蔽的方式，其最终目的是为了盗取用户的敏感信息，如各类账号密码，甚至使用户电脑沦为攻击者的“肉鸡”。一旦网站服务器成为传播病毒木马的“傀儡帮凶”，将会严重影响到网站的公众信誉度。

（6）网页防篡改

Web应用防火墙内置有网页防篡改监控平台，可以对网页防篡改客户端进行实时监控。当网页防篡改客户端与Web应用防火墙的网络中断时，网页文件会被自动锁定，所有“写”的权限进行封锁，只有“读”的权限。当网络恢复中，所有相关权限会自动下发，网站正常恢复更新。

为云平台互联网业务服务部署云端网站安全防护系统对Web攻击进行拦截，防止数据库被拖库、网页被恶意篡改、网站被挂马、被挂链接、网站敏感信息泄露等网站安事件的发生。在前置服务区采用纯透明串行模式部署Web应用防火墙，交换机上串行接入Web应用防火墙，所有Web请求和恶意访问攻击均由Web应用防火墙来承担处理，清洗、过滤后Web应用防火墙向真实的服务器提交请求并将响应进行整形、压缩等处理后送交给请求客户端。这样可以很好的防范来自互联网的威胁，保护网站的安全、稳定、高性能运行。

6.3.4.7应用开发安全与审计

在系统开发过程中，应当在设计阶段同步考虑安全功能的设计，并在系统编码阶段同步实现安全功能，按照等级保护的要求，应用系统应具备以下安全功能：

（1）身份鉴别

应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，鉴别信息具有复杂度要求并定期更换。

应提供并启用登录失败处理功能，多次登录失败后应采取必要的保护措施。

应强制用户首次登录时修改初始口令。

用户身份鉴别信息丢失或失效时，应采用技术措施确保鉴别信息重置过程的安全。

应采用两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用动态口令、密码技术或生物技术来实现。

（2）访问控制

应提供访问控制功能，对登录的用户分配账号和权限。

应重命名或删除默认账户，修改默认账户的默认口令。

应及时删除或停用多余的、过期的账户，避免共享账户的存在。

应授予不同账户为完成各自承担任务所需的最小权限，并在它们之间形成相互制约的关系。

应由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则。

访问控制的粒度应达到主体为用户级，客体为文件、数据库表级、记录或字段级。

应对敏感信息资源设置安全标记，并控制主体对有安全标记信息资源的访问。

（3）安全审计

应提供安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计。

审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息。

应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。

应确保审计记录的留存时间符合法律法规要求。

应对审计进程进行保护，防止未经授权的中断。

（4）入侵防范

应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求。

（5）数据完整性

应采用校验码技术或密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等。

应采用校验码技术或密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等。

（6）数据保密性

应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等。

应采用密码技术保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等。

（7）剩余信息保护

应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。

应保证存有敏感数据的存储空间被释放或重新分配前得到完全清除。

（8）个人信息保护

应仅采集和保存业务必需的用户个人信息。

应禁止未授权访问和非法使用用户个人信息。

第三方软件开发商应具备相应的开发资质，在应用开发过程中采用安全开发过程管理，并采用代码安全检测工具在开发过程中进行代码安全检测与审计，并要求第三方开发厂商提供系统源代码。

6.3.4.8数据加密与保护

等级保护制度中，对于数据安全的防护要求主要是从完整性和保密性进行规范的，并主要定义了数据在传输和存储环节的安全要求，包括：

应采用校验技术或密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等。

应采用校验技术或密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等。

应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等。

应采用密码技术保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等。

数据的完整性和保密性保护措施可以在应用系统开发过程中同步采取基于密码技术的相关功能实现，但数据保护是个复杂的过程，由于数据的分散性和流动性，在终端、网络、数据库等各层面也需要采用相关的数据防护措施。

通过以下具体的技术保护手段，在数据和文档的生命周期过程中对其进行安全相关防护，确保内部数据在整个生命周期的过程中的安全。

（1）加强对于数据的分级分类管理

对关键敏感数据须设置标记，对于重要的数据应对其本身设置相应的认证机制。

（2）加强对于数据的授权管理

对文件系统的访问权限进行一定的限制；对网络共享文件夹进行必要的认证和授权。除非特别必要，可禁止在个人的计算机上设置网络文件夹共享。

（3）数据和文档加密

保护数据和文档的另一个重要方法是进行数据和文档加密。数据加密后，即使别人获得了相应的数据和文档，也无法获得其中的内容。

网络设备、操作系统、数据库系统和应用程序的鉴别信息、敏感的系统管理数据和敏感的用户数据应采用加密或其他有效措施实现传输保密性和存储保密性。

当使用便携式和移动式设备时，应加密或者采用可移动磁盘存储敏感信息。

（4）加强对数据和文档日志审计管理

使用审计策略对文件夹、数据和文档进行审计，审计结果记录在安全日志中，通过安全日志就可查看哪些组或用户对文件夹、文件进行了什么级别的操作，从而发现系统可能面临的非法访问，并通过采取相应的措施，将这种安全隐患减到最低。

（5）进行通信保密

用于特定业务通信的通信信道应符合相关的国家规定，密码算法和密钥的使用应符合国家密码管理规定。

对于存在大量敏感信息的系统，还可针对信息系统和数据在使用过程中面临的具体风险进行整体地分析，采用专业的数据防泄密系统对数据进行全生命周期防护。

6.3.4.9数据访问安全审计

数据库审计系统能够对业务网络中的各种数据库进行全方位的安全审计，具体包括：

（1）数据访问审计。记录所有对保护数据的访问信息，包括文件操作、数据库执行SQL语句或存储过程等。系统审计所有用户对关键数据的访问行为，防止外部黑客入侵访问和内部人员非法获取敏感信息。

（2）数据变更审计。统计和查询所有被保护数据的变更记录，包括核心业务数据库表结构、关键数据文件的修改操作等等，防止外部和内部人员非法篡改重要的业务数据。

（3）用户操作审计。统计和查询所有用户的登录成功和失败尝试记录，记录所有用户的访问操作和用户配置信息及其权限变更情况，可用于事故和故障的追踪和诊断。

（4）违规访问行为审计。记录和发现用户违规访问。支持设定用户黑白名单，以及定义复杂的合规规则，支持告警。

数据库审计系统旁路部署在服务器区，对数据库访问行为进行审计。

6.3.4.10数据备份与恢复

等级保护制度中，针对数据的备份和恢复要求，应用数据的备份和恢复应具有以下功能：

（1）应提供重要数据的本地数据备份与恢复功能。

（2）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地。

（3）应提供重要数据处理系统的热冗余，保证系统的高可用性。

数据库区作为内网系统中最为关键的区域，存储着重要的信息数据，分布着学籍系统数据库、教师管理数据库、综合教务系统数据库、学生就业信息系统数据库等，所有需要安装数据库的业务系统的操作数据会实时的存储于数据库中，故对数据区的保护为重中之重。再者为了数据更加安全的角度考虑，可以将数据库中的数据定向到存储区域的磁盘阵列中，更加长久安全的保护了重要数据。

为了实现网络中心改造后虚拟化架构子系统的资源优化和高可用功能，通过搭建存储区域网络来满足虚拟机文件和的存储需求。存储区域利用2台光纤交换机和2套磁盘阵列系统来构建，磁盘阵列用来存储DMZ区域中所有虚拟机文件及服务器区虚拟机文件。

而分布式存储系统利用多台PC服务器中的存储空间聚合成一个能够给应用服务器以及数据库服务器提供统一访问接口和管理界面的存储池，应用及数据库可以通过该访问接口非常容易的管理存储池后端物理存储设备上所有的磁盘，充分发挥存储设备的性能和磁盘利用率。

6.4安全管理体系

6.4.1安全管理制度

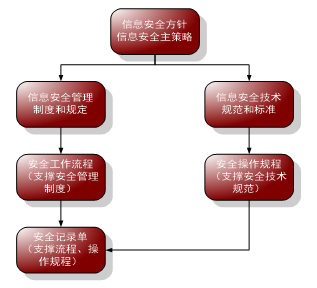
6.4.1.1安全策略和制度体系

（1）建设思路

安全技术措施的有效实施需要安全管理制度的助力，同样，安全管理制度的落实也常常需要技术措施的支撑，两者是相辅相成，相互关联的，等级保护对于安全制度体系的建设要求参照了ISO 27001的相关标准，即安全管理制度体系自上而下分为安全策略、管理制度和操作规程、记录表单，单位需要建设符合单位实际情况的管理制度体系，应覆盖物理、网络、主机系统、数据、应用、建设和运维等管理内容，并对管理人员或操作人员执行的日常管理操作建立操作规程。

（2）建设内容

单位信息安全管理制度体系应结合实际业务需要，建立符合本单位实际情况的安全制度体系，需包括信息安全方针、安全策略、安全管理制度、安全技术规范以及流程等，如下所示。



安全管理制度体系图

1）安全方针和策略

包括：最高方针，纲领性的安全策略主文档，陈述本策略的目的、适用范围、信息安全的管理意图、支持目标以及指导原则，信息安全各个方面所应遵守的原则方法和指导性策略。

2）安全管理制度

包括：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，是必须具有可操作性，而且必须得到有效推行和实施的。

3）安全技术标准和规范

包括：各个安全等级区域网络设备、主机操作系统和主要应用程序的应遵守的安全配置和管理的技术标准和规范。技术标准和规范将作为各个网络设备、主机操作系统和应用程序的安装、配置、采购、项目评审、日常安全管理和维护时必须遵照的标准，不允许发生违背和冲突。

4）安全流程和操作规程

为信息安全建立相关的流程，保证安全运营可以遵照标准流程制度执行，主要的内容包括。

a）流程制定。建立健全流程管理制度，主要包括的流程有安全事件处置流程、安全风险评估流程、安全事件应急响应流程、安全事件溯源取证流程、安全设备上线交割流程等。

b）流程变更维护。定期的维护和修订相关的管理制度。

c）流程发布。根据需要，定期发布变更后的全套流程到相关的组织范围内，并对发布的流程进行相关的培训。

5）安全记录单

安全记录单是落实安全流程和操作规程的具体表单，根据不同等级信息系统的要求可以通过不同方式的安全记录单落实并在日常工作中具体执行。主要包括日常操作的记录、工作记录、流转记录以及审批记录等。

6.4.1.2制度文件管理

（1）建设思路

制度文件需要正式发布并进行定期评审修订和版本控制。信息安全管理制度应该得到单位负责人的签发和认可，只有被正式发布并真正落实的管理制度才能促使单位安全管理能力的提升和安全技术措施的有效运行。

（2）建设流程

信息安全管理制度体系是不断改进和完善的过程，包括以下：

1）制定和发布

安全制度系列文档制定后，必须有效发布和执行。发布和执行过程中除了要得到管理层的大力支持和推动外，还必须要有合适的、可行的发布和推动手段，同时在发布和执行前对每个人员都要做与其相关部分的充分培训，保证每个人员都知道和了解与其相关部分的内容。

安全制度在制定和发布过程中，应当实施以下安全管理：

●安全管理制度应具有统一的格式，并进行版本控制。

●安全管理职能部门应组织相关人员对制定的安全管理制度进行论证和审定。

●安全管理制度应通过正式、有效的方式发布。

●安全管理制度应注明发布范围，并对收发文进行登记。

必须要注意到这是一个长期、艰苦的工作，需要付出艰苦的努力，而且由于牵扯到许多部门和绝大多数员工，可能需要改变工作方式和流程，所以推行起来的阻力会相当大；同时安全策略本身存在的缺陷，包括不切实可行，太过复杂和繁琐，部分规定有缺欠等，都会导致整体策略难以落实，需要不断改进。

2）评审和修订

网络安全领导小组应组织相关人员对于信息安全制度体系文件进行评审，并确定其有效执行期限。同时应指定信息安全职能部门每年审视安全策略系列文档，具体检查内容包括：

●信息安全策略中的主要更新。

●信息安全标准中的主要更新。信息安全标准不需要全部更新，可以仅对因变更而受影响的部分进行更新；如果必要，可以使用年度审视／更新流程对信息安全标准做一次全面更新。

●安全管理组织机构和人员的安全职责的主要更新。

●操作流程的主要更新。

●各类管理规定、管理办法和暂行规定的主要更新。

●用户协议的主要更新等等。

6.4.2安全管理机构

6.4.2.1网络安全组织机构及职责

（1）建设思路

网络安全管理机构是行使单位网络安全管理智能的重要机构，一般由网络安全管理领导机构和执行机构构成，网络安全领导机构需确保整个组织贯彻单位的网络安全方针、策略和制度等。等级保护制度中明确规定“单位应成立指导和管理网络安全工作的委员会或领导小组，其最高领导由单位主管领导担任或授权。”并设立网络安全管理的职能部门。

（2）建设内容

单位应根据管理工作需要设立安全管理机构，但至少应包括网络安全领导小组和网络安全管理职能部门，其工作职责分工如下：

1）网络安全领导小组

网络安全领导小组是网络安全工作的最高领导决策机构，负责网络安全工作的宏观管理，其最高领导由单位主管领导担任或授权，职责如下：

贯彻执行国家关于网络安全工作的方针、政策，组织落实网络安全体系建设工作的目标、方针、政策。

审定网络安全相关策略、规范及管理规定。

监督、检查网络安全相关制度的落实与执行情况。

协调指挥网络安全重大突发事件的应急处理。

完成上级单位交办的有关工作。

2）网络安全管理部门

网络安全管理部门负责落实网络安全领导小组各项决策，协调组织各项网络安全工作，具体职责如下：

负责网络安全日常工作的协调和处理。

负责网络安全总体规划设计与实施。

组织网络安全管理规定的编制。

督促网络安全重大突发事件应急预案的落实。

组织网络安全培训的相关工作。

完成网络安全领导小组交办的有关事项。

6.4.2.2岗位职责及授权审批

（1）建设思路

网络安全管理应落实岗位安全责任，网络安全组织机构及职责明确了组织层面的管理职责，但管理职责的落实需要层层落实到人，等级保护中明确要求要“设立安全主管、安全管理各个方面的负责人岗位，并定义各负责人的职责”，并设立系统管理员、审计管理员和安全管理员，并明确岗位工作职责。

（2）建设内容

根据单位实际情况，设立相关的网络安全管理岗位，但至少应包括安全主管以及“三员”（系统管理员、审计管理员和安全管理员），且“三员”工作职责需分工明确，互相监督，安全管理员需专职，不得兼任其他岗位工作。

三员的岗位职责如下：

1）安全管理员

安全管理员不能兼任网络管理员、系统管理员，其职责是：

组织网络系统的安全风险评估工作，并定期进行系统漏洞扫描，形成安全现状评估报告。

定期编制网络安全状态报告，向网络安全领导小组报告网络安全整体情况。

负责核心网络安全设备的安全配置管理工作。

编制网络安全设备和系统的运行维护标准。

负责网络系统安全监督及网络安全管理系统、补丁分发系统和防病毒系统的日常运行维护工作

负责沟通、协调和组织处理网络安全事件，确保网络安全事件能够及时处置和响应。

2）系统管理员

系统管理员不能兼任安全管理员，其职责是：

负责网络及网络安全设备的配置、部署、运行维护和日常管理工作。

负责编制网络及网络安全设备的安全配置标准。

能够及时发现、处理网络、网络安全设备的故障和相关安全事件，并能根据流程及时上报，减少网络安全事件的扩大和影响。

负责服务器的日常安全管理工作，确保服务器操作系统的漏洞最小化，保障服务器的安全稳定运行。

负责编制服务器操作系统的安全配置标准。

能够及时发现、处理服务器和操作系统相关安全事件，并能根据流程及时上报，减少网络安全事件的扩大和影响。

3）安全审计员

安全审计员的职责是：

定期审计网络安全制度执行情况，收集和分析网络系统日志和审计记录，及时报告可能存在的问题。

对安全、网络、系统、应用、数据库管理员的操作行为进行监督，对安全职责落实情况进行检查。

单位可根据实际管理需要进行岗位职责的细化，如将系统管理和网络管理工作分别由不同的人负责，对重要的应用系统设置业务系统管理员，对机房、数据库、信息资产进行专门的管理，设置机房管理员、数据库管理员、网络资产管理员等，并明确岗位职责。

在明确岗位职责过程中，单位需梳理在网络安全管理过程中需要授权审批的事项，并根据各个部门和岗位的职责明确授权审批部门和批准人等，对于系统变更、重要操作、物理访问和系统接入等重要事项建立审批程序，按照审批程序执行审批过程，对重要活动建立逐级审批制度，并定期审查，及时更新相关信息。

6.4.2.3内部沟通和外部合作

（1）建设思路

网络安全管理工作不是孤立的，在单位业务工作中离不开安全管理工作的保障，同样，网络安全管理工作也离不开单位业务部门的配合，要使网络安全管理工作顺利开展，需“加强各类管理人员、组织内部机构和网络安全管理部门之间的合作与沟通，定期召开协调会议，共同协作处理网络安全问题”，加强内部沟通。

同时，单位的网络安全工作也需要得到外部专家和技术力量的支持，包括监管部门、供应商、业界专家及其他安全组织等。

（2）建设内容

聘请专家和外部顾问成员，这些成员需要对网络安全或相关领域有丰富地知识和经验，如安全技术、电子政务、等级保护或质量管理等。专家和外部顾问负责对网络安全重要问题的决策提供咨询和建议。

同时加强与供应商、业界专家、专业的安全公司等安全组织的合作和沟通。建立外联单位联系列表，包括外联单位名称、合作内容、联系人和联系方式等信息。

6.4.2.4安全审核与检查

（1）建设思路

网络安全管理工作是否有效，安全制度和规范是否得到落实需要单位网络安全管理部门定期进行检查，以便及时发现问题，持续改进和提升网络安全管理能力。按照等级保护的要求，单位网络安全检查可分为定期常规安全检查和定期全面安全检查，安全检查工作需进行认真准备，保留记录。

（2）建设内容

单位可根据实际情况，进行安全检查工作安排。包括：

1）定期进行常规安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况。

2）定期进行全面安全检查，检查内容包括现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等；由于单位人员及安全技术能力有限，全面安全检查可请专业的安全厂商协助完成。

3）制定安全检查表格实施安全检查，汇总安全检查数据，形成安全检查报告，并对安全检查结果进行通报。单位也可参照上级单位或自行制定安全检查评价指标，以便量化考核安全工作的执行情况。

6.4.3安全管理人员

6.4.3.1内部人员安全管理

（1）建设思路

人是网络安全工作的主体，也是网络安全威胁的主要来源，调查发现，越来越多的网络安全事件是由内部人员的恶意或工作疏忽导致，因此，加强人员安全管理是网络安全管理工作的重中之重，其中，尤其需要加强对内部人员的安全教育和审核。

（2）建设内容

针对内部人员的安全管理需从人员的录用、安全培训和教育、技能考核和调用、离岗审核等全过程进行安全管理，具体管理要求包括：

1）录用前

指定或授权专门的部门或人员负责人员录用。

应对被录用人员的身份、安全背景、专业资格或资质等进行审查，对其所具有的技术技能进行考核。

与被录用人员签署保密协议，与关键岗位人员签署岗位责任协议。

2）工作期间

对各类人员进行安全意识教育和岗位技能培训，并告知相关的安全责任和惩戒措施。

针对不同岗位制定不同的培训计划，对安全基础知识、岗位操作规程等进行培训。

定期对不同岗位的人员进行技能考核。

3）调离岗

及时终止离岗人员的所有访问权限，取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备。

办理严格的调离手续，并承诺调离后的保密义务后方可离开。

6.4.3.2外部人员安全管理

（1）建设思路

在日常业务工作中，单位越来越多地与外部单位人员进行业务合作和往来，外部人员包括指软件开发商，硬件供应商，系统集成商，设备维护商和服务提供商，以及实习生、临时工、调用人员等。这些人员由于工作需要需临时或短期访问单位内部网络，进出单位工作场所，非内部人员由于流动性强，背景情况不明，给单位网络系统的安全带来较大隐患，必须建立严格的物理和网络访问授权审批制度，并有效执行。

（2）建设内容

单位应制定外部人员物理访问和网络接入的管理制度，并记录相关内容，具体要求如下：

1）在外部人员物理访问受控区域前先提出书面申请，批准后由专人全程陪同，并登记备案。

2）在外部人员接入受控网络访问系统前先提出书面申请，批准后由专人开设账户、分配权限，并登记备案。

3）外部人员离场后及时清除其所有的访问权限。

4）获得系统访问授权的外部人员应签署保密协议，不得进行非授权操作，不得复制和泄露任何敏感信息。

6.4.4安全建设管理

6.4.4.1系统定级和备案

（1）建设思路

根据新等级保护制度的要求，二级以上（含二级）信息系统在定级工作中需要组织相关部门和有关安全技术专家对定级结果的合理性和正确性进行论证和审定，新建信息系统在规划阶段就可根据信息系统将承载的业务的重要程度对信息系统进行定级，按照相应等级进行等级保护安全体系设计和建设，对二级以上（含二级）信息系统还需按照教育行政管理部门的要求进行备案。

（2）建设内容

为了进一步明确信息系统定级、备案的相关责任和流程，应明确系统定级、备案和系统测评流程，包括以下内容

1）明确定级备案责任部门和责任人。

2）跟教育部门沟通明确定级备案相关材料要求和格式。

3）制定系统定级和备案工作的时间计划。

4）定级评审相关单位和专家联系和确定。

5）组织定级评审工作，并获得上级或相关部门的批准。

为确保系统等级保护定级备案工作的规范性和专业性，可选择专业的等级保护咨询服务完成相关工作。

6.4.4.2系统安全方案设计

（1）建设思路

按照“三同步”的原则，网络安全需要与信息化建设同步规划、同步建设、同步使用，在系统建设规划阶段需明确安全建设的目标和建设需求并进行安全规划方案的设计，安全方案应经过评审，经过批准后才能实施。

（2）建设内容

安全方案设计需根据安全保护等级选择基本安全措施，依据风险分析的结果补充和调整安全措施。

安全方案应根据保护对象的安全保护等级及与其他级别保护对象的关系进行安全整体规划和安全方案设计，设计内容应包含密码技术相关内容，并形成配套文件。

安全建设项目根据实际建设阶段需设计不同的安全方案，包括总体建设规划方案、详细设计方案、建设实施方案等，安全方案需组织相关部门和有关安全专家对安全整体规划及其配套文件的合理性和正确性进行论证和审定，经过批准后才能正式实施。

6.4.4.3安全产品采购管理

（1）建设思路

网络安全产品的采购和使用应符合国家的有关规定，对于密码产品的采购和使用需符合国家密码主管部门的要求，并预先对产品进行选型测试，确定产品的候选范围，并定期审定和更新候选产品名单。

（2）建设内容

需严格按照设备采购管理流程和政府设备采购目录来采购相应的安全产品；并且在搭建的模拟系统中对这些安全设备和软件进行测试和试运行验证，以防止产生对系统产生不可预见的影响。

6.4.4.4外包软件开发管理

（1）建设思路

对于外包软件开发由于开发过程可控，在系统上线后可能引发各种安全问题，且难以从源头解决，因此，在等级保护制度中，对于外包软件开发明确要求应在软件交付前检测其中可能存在的恶意代码，并要求开发单位提供软件设计文档和使用指南，对于三级系统的外包软件开发还要求开发单位提供软件源代码，并审查软件中可能存在的后门和隐蔽信道。

（2）建设内容

针对外包软件开发可选择专业的安全公司作为第三方进行开发过程的安全管理，包括协助开发单位建立安全开发制度和流程，并在软件开发的关键节点进行代码检测，代码检测采用自动化工具+专家审核的检测方式，既提高检测准确性和效率，又能发现系统逻辑错误等问题。

6.4.4.5工程实施管理

（1）建设思路

网络系统安全建设过程中，涉及产品安装部署、功能启用、策略配置、与应用系统集成等各方面工作，安全工程建设整个过程本身还需要安全可控，需要由专门的部门或人员负责工程实施过程的管理，并制定安全工程实施方案，控制工程实施过程。对于三级信息系统，等级保护还明确要求需通过第三方工程监理控制项目的实施过程。

（2）建设内容

本项目实施周期较长，在实施过程中将通过招投标方式确定第三方监控单位，并指定专门的项目安全工作负责人，制定项目管理制度和项目实施方案。

6.4.4.6测试及交付管理

（1）建设思路

项目建设完成后在正式上线前应进行系统测试，应制订测试验收方案，并依据测试验收方案实施测试验收，形成测试验收报告，按照等级保护的要求，应进行上线前的安全性测试，并出具安全测试报告，安全测试报告应包含密码应用安全性测试相关内容。

在系统交付时，应制定系统交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点，对负责系统运行维护的技术人员进行相应的技能培训，提供建设过程文档和运行维护文档。

（2）建设内容

由于本系统的复杂性，在系统及各子系统交付时，要制定交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点；对负责运行维护的技术人员进行相应的技能培训；确保提供建设过程中的文档和指导用户进行运行维护的文档。

系统安全性测试选择专业的安全公司进行系统上线前安全检测，并针对安全风险及时采取措施整改。

6.4.4.7系统等级测评

（1）建设思路

在系统建设完成后，按照等级保护的要求必须选择国家认可的测评机构对信息系统进行等级测评，并在系统运行过程中定期进行测评，对于三级系统要求每年测评一次，二级系统要求每两年自行完成测评一次，对发现不符合相应等级保护标准要求的及时整改，并在发生重大变更或级别发生变化时进行等级测评。

（2）建设内容

系统上线运行后，选择经过国家认可的等级保护测评机构进行测评，由于测评工作的专业性和复杂性，选择专业安全厂商协助单位进行测评工作，如在正式测评前协助单位进行自测和整改等。

6.4.4.8服务供应商选择

（1）建设思路

来自供应链的安全威胁已经越来越引起人们的关注，加强对供应链的管理是新等级保护制度的变化之一，等级保护制度规定要确保服务供应商的选择符合国家的有关规定；与选定的服务供应商签订相关协议，明确整个服务供应链各方需履行的网络安全相关义务；并定期监督、评审和审核服务供应商提供的服务，并对其变更服务内容加以控制。

（2）建设内容

确保选择有相应资质的安全服务商、安全集成商、系统集成商和软件开发商，并与其签订协议，明确相关安全义务和责任。

6.4.5安全运维管理

按照等级保护要求，日常安全运维管理主要从环境管理、资产管理、介质管理、资产维护管理、漏洞和风险管理、网络和系统安全管理、防病毒管理、配置管理、密码管理、变更管理、备份与恢复管理、安全事件处置管理、应急预案管理、外包运维管理几个方面进行考虑。

6.5安全运营体系

只有安全技术体系和安全管理体系，并不能充分保障系统的安全性，这是因为：一方面，无论是技术控制措施还是管理制度，都需要人来落地操作，这类事情就是运营工作；如果出现不会操作、操作不好或违规操作的情况，而且安全管理者也没有能力对操作行为进行监控，那就必将导致技术体系无法真正发挥威力，也会导致管理体系难以落地；另一方面，技术体系的控制措施，主要通过软硬件系统来实现；然而，还有不少技术控制措施，需要通过人的专业服务来实现；专业安全服务是一类特殊的安全操作，也属于运营体系范畴。总之，安全运营体系的作用是支撑、连通技术体系和管理体系，使之真正发挥效能。

紧跟信息化发展趋势，充分利用安全产品、网络产品的数据收集、关联、分析等自动化分析能力，结合企业云端大数据资源及安全威胁情报信息，形成一套规范有序、高效运转、快速响应的安全运营体系，提升对未知威胁感知和防御能力，有效防御各种新型攻击，是新形势下网络安全保障工作的重要环节。

6.5.1日常安全运营

日常安全运营是安全运营体系的基石，只有日常做好了安全运营工作，才能及时识别、研判、处置各类安全隐患和安全事件，将风险扼杀在萌芽状态；否则，在重大事件期间，就容易出现安全问题层出不穷、疲于应付的状态。

日常安全运营工作可分为风险管控、监控分析、安全运维三大类：

6.5.1.1风险管控

风险管控是一个安全风险管理过程，包括：风险识别、风险分析、风险处置。要想做好风险分析，又需要从资产识别、威胁识别分析、脆弱性识别分析、已有安全措施确认来入手。

当前环境下，业务和人员上网的趋势势不可挡，所以，资产识别的核心工作是识别暴露在互联网的资产，特别是违规暴露、隐匿暴露的情况。本项安全控制措施，通过互联网资产发现服务来落地实现。

威胁识别分析，是识别、分析威胁源头、威胁入侵方式、威胁后果（安全事件），是发现、分析、确诊“真实发生”的安全问题；这有别于“脆弱性识别分析”只是发现信息系统自身的脆弱性，而这种脆弱性是否能够利用、是否已被利用则不得而知。从这个角度看，威胁识别分析是安全运营体系的刚需。因此，在安全运营体系设计中，突出了威胁识别分析的控制措施。全流量订阅分析服务和Web失陷检测服务，就是这一控制措施的落地服务。

脆弱性识别分析，是识别、分析网元设备（网络设备、操作系统、中间件、数据库）和应用系统自身的安全弱点，包括漏洞和不安全配置；区别于威胁识别分析，尽管有脆弱性问题并不代表一定会受到入侵，但脆弱性问题的识别、分析和整改，仍是整个安全体系的重要一环，也是安全运营体系的关键控制措施。本控制措施，通过基础安全评估服务、渗透测试服务，进行黑盒的脆弱性检测；再辅以白盒的代码安全检测，实现了脆弱性分析实现方法的全覆盖。

已有安全措施的确认，也是通过基础安全评估服务，实现控制措施的落地。

6.5.1.2监控分析

风险管控工作，离不开及时的监控分析，实际上监控分析和风险管控工作是联动的，监控分析发现的问题，导入风险管理流程。监控分析的关键是及时性。监控分析又可以分为几个维度：

（1）预警预测。预警预测在安全运营体系中的作用日渐突出，本质原因是漏洞本身难以避免，也是黑客入侵的核心方法之一；在目前这种基于移动互联网的、信息快速扩散的环境下，谁能及时获取安全情报、未雨绸缪及时整改，谁就掌握了先机，减轻甚至避免了严重损失。此项控制措施是通过“安全预警通告服务”来落地实现的。

（2）内网威胁监控。在目前勒索病毒、APT攻击盛行的情况下，每个组织都不应对安全威胁掉以轻心，威胁监控是刚需性的控制措施，是确诊组织是否被入侵、如何被入侵、遭受了哪些损失的关键方法；此项控制措施是通过周期性的“流量订阅分析服务”来落地实现，服务监控到的结果，导入风险管控流程进行处理。

（3）Web监测。Web是目前主要互联网应用模式，因为B/S架构的半开放性特点，网站安全的问题较为严重，需要设计控制措施及时发现网站的可用性、脆弱性等各类安全问题。本控制措施通过网站云监测服务来落地实现。

（4）安全态势监控。通过实时收集安全事件的分布情况、分类情况、损失情况等数据，研判分析安全体系的薄弱环节，以及安全态势的发展情况。本控制措施，通过态势感知与安全运营平台运营分析服务来落地实现。

6.5.1.3安全运维

安全运维工作中，大部分是基础的运营服务，它们的服务对象主要是组织中的安全软硬件设备。通过安全运维服务，解决安全软硬件设备“不会用”、“用不好”的最后一公里问题，真正发挥安全防御体系的威力。此类服务，本方案中主要是驻场运维服务、安全巡检服务、态势感知与安全运营平台基础运营服务。

应急响应服务是一个高阶运营服务，和驻场运维、安全巡检、态势感知与安全运营平台基础运营工作密切相关，它针对已经发生或可能发生的安全事件进行检测、分析、协调、处理，是安全对抗的重要一环。应急响应服务是最考验工程师和服务单位能力的安全服务之一，也是安全运营体系和整个等级保护安全体系的刚需环节，原因是：由于攻防的不对称性，面对APT类攻击，任何安全防御体系都有可能被击穿，这时候，应急响应服务就至关重要，它是整个等级保护安全体系的托底控制措施。

6.5.2重大安全事件保障

一方面，重大事件期间，面临着更严峻的内、外部安全威胁，非常考验组织的安全运营能力，重大事件保障工作是组织安全运营能力的练兵场和试金石。

另一面，重大事件期间，网络安全工作的能见度大幅提升，安全运营工作如果能在此时发力，就能起到事半功倍的效果。

“重要时期安全保障服务”发展至今，已经是一个覆盖重保工作部署、现场安全值守、事件分析研判、应急处置等的多模块服务，可以根据需求进行灵活组合。

6.6本期安全系统

本项目统筹规划教育骨干网和广西教育数据中心的网络安全设计和建设，统一实施网络安全的管理和运维。依据《信息安全技术网络安全等级保护基本要求》（GBT22239-2019）等标准规范要求，教育骨干网的网络安全保护等级定级第三级，按网络安全等级保护第三级的要求进行设计、建设、管理和运维。

本项目需要具备较为全面的安全防护能力，要对安全物理环境、安全通信网络、网络安全区域边界、安全管理中心和安全计算环境（应用安全除外）分别进行设计，最终目标是使教育骨干网符合网络安全等级保护第三级要求，教育城域网符合网络安全等级保护第二级要求。

教育骨干网3个核心节点各自具有独立的安全域，教育骨干网主要承担教育城域网的接入，重点考虑网络链路的可用性，因此安全区域划分为网络接入区、安全防护区。

网络接入区：由边界网络设备组成，承担双线路接入、负载均衡的功能。

安全防护区：由安全防护设备组成，承担入侵攻击阻断、威胁感知等功能。

安全域划分示意图如下：



接入设备

核心节点A

核心节点C

态势感知

安全防护区

网络接入区



ADS



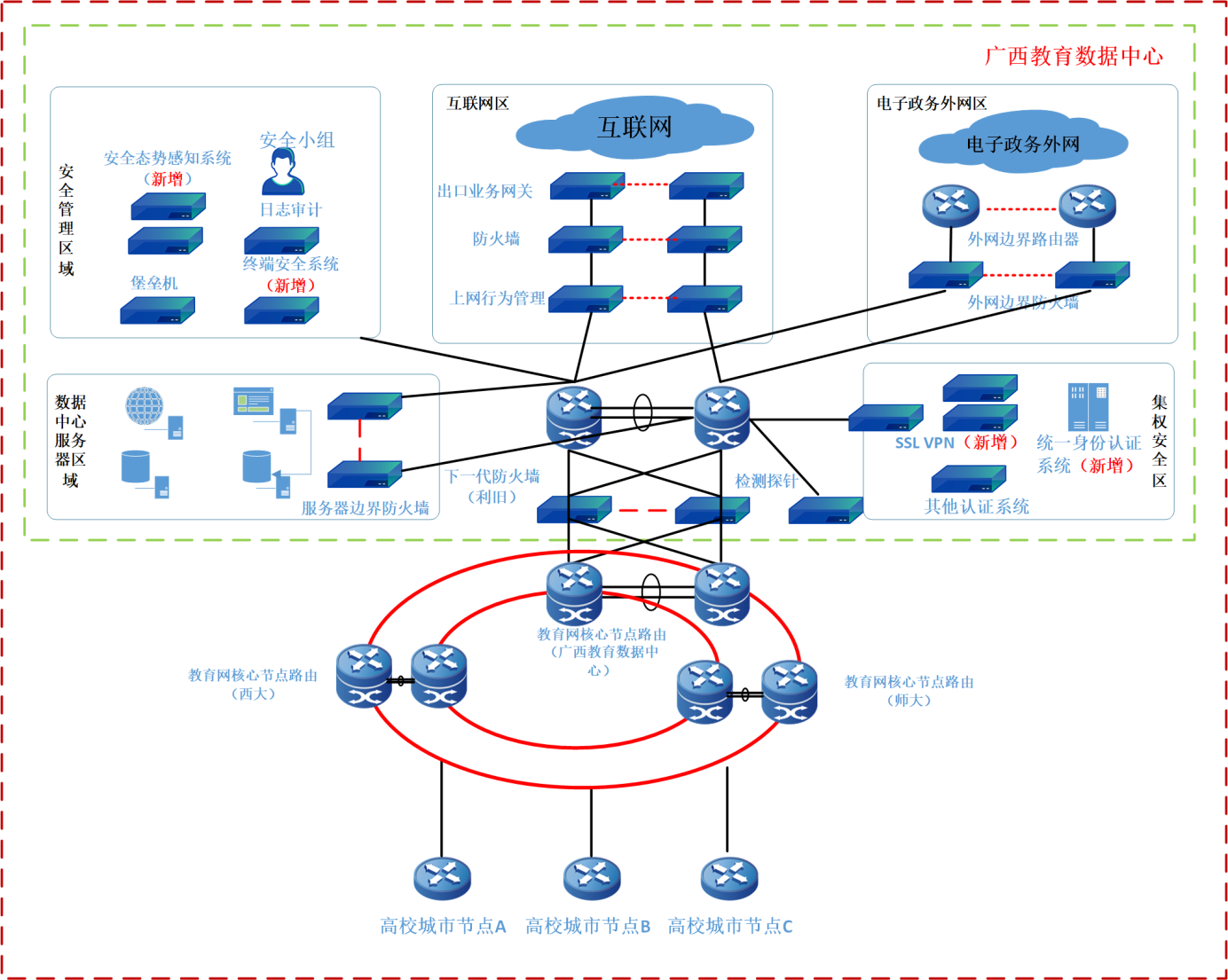
UTS

堡垒机

安全域划分示意图

广西教育数据中心核心节点是整个教育网最核心的部分，其安全建设将影响广西教育网全域的安全性，现阶段需要对自身的网络安全情况建立运营机制，以便后续教育城域网建设后对广西教育网进行整体监管。广西大学、广西师范大学两个核心节点，作用主要是帮助广西教育数据中心核心节点分担流量，因此只做网络建设，不做安全系统建设。

本次安全系统建设按照等保2.0框架当中“一个中心，三重防护”的思想进行设计，广西教育数据中心核心节点的安全防护示意图如下：



教育骨干网广西教育数据中心核心节点安全防护示意图

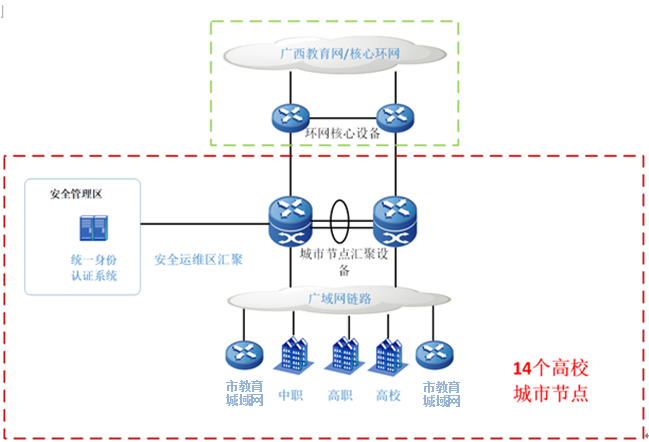
6.6.1安全物理环境

本次项目建设教育骨干网的物理位置位于广西教育数据中心、教育网广西节点（广西大学、广西师范大学）、各高校城市节点的机房，其中数据中心物理访问控制、防盗窃和防破坏、防雷击、防火、防水和防潮、防静电、为适度控制、电力供应的相关内容均利旧现有机房设备。

6.6.2安全通信网络

（1）根据等保2.0网络架构相关要求，对接入服务设计了资源保证、优先处理等保障。包括：保证主要网络设备的业务处理能力具备冗余空间，通过QoS机制满足业务高峰期、优先级业务的需要；对业务服务的重要次序来指定带宽分配优先级别，保证在网络发生拥堵的时候优先保护重要主机。教育骨干网分不同的教育城域网或网段，并按照方便管理和控制的原则为各教育城域网、网段分配地址段。重要网段与其他网段之间采取可靠的技术隔离或边界防护措施。业务类网络设备（交换机、防火墙、路由器）成对部署，以虚拟化、堆叠、1+1保护等方式工作。根据实际情况尽可能配置备份的路由或应急路由（最少2个）。在路由可达时，当由于某种原因主路由失效时候，可以使用备份路由或应急路由继续提供网络服务。

（2）根据等保通信传输相关要求，新增SSL VPN设备。用于自治区范围内各高等院校、区直中等职业学校与电子政务外网的接入，实现数据传输的加密。



教育骨干网高校城市节点安全防护示意图

6.6.3网络安全区域边界

根据等保建设分区分域的设计思路，将网络分为国家教育专网接入区、电子政务外网区、安全管理区，以及集权安全区。根据边界防护、访问控制、入侵防范的要求，在国家教育专网接入区、电子政务外网区利旧原有防火墙，在集权安全区新增2台下一代防火墙。

虽然安全审计提出对访问互联网用户行为审计的要求，因为教育骨干网不建设互联网接入服务，所以不做上网行为管理建设。

根据网络设备的安全审计要求，在路由器、交换机和防火墙等设备上启用日志审计功能，并利旧安全管理区的日志审计设备。

6.6.4安全管理中心

按照等保“一个中心三重防护”建设思路，一个中心是指“安全管理中心”。根据安全管理中心相关要求，划分“安全管理区”。通过利旧技信中心现有负载均衡、态势感知、堡垒机、入侵防御、审计系统等设备，协助教育骨干网设备进行统一的安全防护。另外，在广西教育数据中心核心节点安全管理区域规划设计满足如下要求：

（1）根据等保系统管理要求，在该区域新增运维安全管理系统。配置可以访问所有管控对象，包括教育城域网内设备，以及直属管理的校园网出口设备，通过逻辑上将管理人员与目标设备分离，建立“人->管理主账号->授权->目标从账号->目标设备”的管理模式；在此模式下，通过基于唯一身份标识的集中账号与访问控制策略，与各网络设备、安全设备，以及后续增加的服务器和数据库等进行连接，实现集中精细化运维操作管控与审计，并对高危操作进行授权审批。

（2）根据等保集中管控要求，在该区域新增安全态势感知系统。教育网可以通过安全态势感知系统实现整个教育网的安全运营，借助安全可视和安全事件工单制实现各级党组党委责任分明，权责明确；通过安全运营机制不断发现教育网的安全问题，并且不断完善安全防御体系，保持教育网的健壮性；通过安全态势感知系统现有内置的驻留程序实现对终端设备的入网认证信息同步，保证教育网终端设备可视安全可控。**同时，教育骨干网新增安全态势感系统需要和广西教育数据中心实现一体化管理运维，实现完整有效、更全面、更直观可视的展示**。

（3）根据等保集中管控要求，在该区域新增统一身份认证管理系统。统一身份认证管理系统强调以人为中心进行访问控制，提供统一身份管理、统一身份认证、统一门户/单点登录(SSO)、集中应用授权、审计与分析等功能，让认证更简易、身份更安全、应用访问更可控。同时，实现身份全生命周期管理，降低管理员账号开户、变更、销户等带来的运维复杂度，让管理更高效。未通过身份认证的用户、设备禁止接入教育网和互联网，仅能在接入的教育城域网内限时使用。本项目统一身份认证管理系统通过教育部省级部署的全国教育管理信息系统（全国中小学生学籍信息管理系统、全国学前教育管理信息系统、全国中等职业学校学生管理信息系统、全国教师管理信息系统）获取身份数据，根据个人分配的账号密码比对用户身份实现鉴权登录。支持同步身份到安全态势感知平台进行统一展示，确保发现安全问题及攻击威胁时，能第一时间定位到终端位置及使用人，方便运维人员进行快速处理，实现安全问题的快速闭环。

（4）根据安全管理的要求，在安全管理区（广西教育数据中心和高校城市节点机房）部署终端安全管理系统管理端，在本级教育城域网、下属教育城域网内终端上部署终端安全管理系统，实现教育城域网内主机终端病毒的查杀，使主机终端免受病毒、特洛伊木马和其它恶意程序的侵袭，不让其有机会透过文件及数据的分享进而散布到整个教育城域网的网络环境，具备完整的病毒扫描防护功能，对主流系统平台下进行完整病毒查杀；同时终端安全管理系统还具备进程管理、软件管理、补丁管理、外设管理等功能，能够实现主机终端入侵防范的能力，统一下发应用软件，统一实现漏洞修复，以及非法外联的管控。

6.6.5安全计算环境

（1）根据等保2.0技术要求中身份鉴别的要求，在“安全管理区”新增统一身份认证管理系统、在“集权安全区”新增SSL VPN设备，上述两种设备与本章节教育骨干网安全设计中“安全通信网络建设”以及“安全管理中心建设”中提到的SSL VPN和统一身份认证系统是相同设备，为避免方案理解错误而造成重复建设特此说明。

（2）根据等保2.0技术要求中访问控制的要求，在“集权管理区”新增下一代防火墙，上述设备与本章节教育骨干网安全设计中“网络安全区域边界建设”中提到的下一代防火墙是相同设备，为避免方案理解错误而造成重复建设特此说明。

（3）根据等保2.0技术要求中安全审计的要求，利旧广西教育数据中心“安全管理区”中原有日志审计系统，并开启所有安全设备的日志记录功能。

**七、运行维护建设方案**

7.1运维建设原则

为加强教育系统党组织对教育信息化工作的领导，落实网络安全主体责任，需明确主要负责人为运维工作的第一负责人，按照谁主管谁负责、谁应用谁负责、谁建设谁负责、谁运维谁负责的原则，确立分级运维制度，同时建立统筹协调的领导体制机制。完善信息化工作的规章制度，制订应急预案，开展应急演练，确保安全保障常态化、日常化。全面落实网络安全等级保护制度。加强网络安全技术防范，做到领导到位、机构到位、人员到位、责任到位、措施到位，实现有效、高效运维的目标。

7.2总体运维方案

广西教育网由教育骨干网、教育城域网和校园网三部分构成。运维方案如下：

7.2.1教育骨干网运维方案

自治区教育厅委托自治区教育技信中心建设教育骨干网管理运维系统，对教育骨干网各节点和各接入点实施监控，管理网络日常流量承载，运营商负责教育骨干网网络线路的管理运维。

7.2.2远程运维方案

远程运维服务是一种智能技术支持服务，以远程专家与智能工具相结合的方式，将技术知识体系和售后维护经验应用于用户网络问题处理中，帮助用户快速准确恢复网络，提高用户网络可用性。

广西教育骨干网在保障网络正常运行中的地位十分重要，管理运维技术要求高。正常状态下，系统安装调试交付使用后，除确有必要外，一般不作网络系统基础配置的变更。当出现特殊情况时，一般需要系统原厂商提供远程，甚至现场技术救援。因此，针对教育骨干网项目管理运维采购专业远程运维服务。

7.2.3教育骨干网控制器

借助教育骨干网控制器可以实现对教育骨干网的智能运维管理：

控制器支持通过界面和北向进行端到端的业务发放，实现业务开通一键式下发，具备以下能力：

7.2.3.1.资源池化。提前规划参数资源池，业务发放过程中，自动分配资源。屏蔽网络细节。资源池支持与网络设备同步，确保自动申请的资源不会与现网冲突。

7.2.3.2.灵活选路。支持按照全网带宽均衡，Cost最优，时延最优进行路径选择，方便用户选取最优路径。当自动选路不满足用户诉求时，还支持用户在线设置必径/非必经结点和链路，调整路径。

7.2.3.3.E2E跨域SR。支持自动收集跨AS域的全网L3拓扑，自动完成跨域隧道的算路和建立。

7.2.3.4.VPN业务可视。控制器支持对于VPN业务实现360度可视。

7.2.3.5.VPN业务路径跨层可视。自动展示站点间业务与隧道的关联关系。隧道逐跳路径可视。

7.2.3.6.业务运维信息中心。支持用户察看业务告警，业务关联绑定的隧道，业务站点下路由协议的配置全部信息。

7.2.3.7.业务诊断中心。支持启动RFC2544， Y.1564业务诊断。

7.2.3.8.隧道路径智能调整。控制器支持对于隧道路径智能调整。

7.2.3.9.SLA可保障。支持多因子约束算路。使隧道的业务路径可以按照带宽、时延、链路可用度、SRLG、主备分离、正反共路SLA保障算路。同时支持多种约束算路一起算路而不降低算法效率。

7.2.3.10.隧道可管可控。支持用户多维度规划自己的业务路径，保障业务流量可以按照用户期望的路径运行。

7.2.3.11.显示路径。支持用户指定必经/非必经业务路径，严格执行用户规划路径。

7.2.3.12.亲和属性。支持在三层拓扑上标示亲和属性，形成基于亲和属性的逻辑拓扑，指定亲和属性算路，可以保障业务路径只包含该亲和属性的链路。使用亲和属性算路，可以用于多业务之间的隔离。

7.2.3.13.隧道锁定。用户支持将规划好的隧道路径进行锁定。保障该隧道途径链路发生故障时，控制器重新算路快速恢复业务。当原有故障恢复时，还会将业务调整回原有锁定路径。这样就保证业务流量尽可能符合用户规划，同时又具备快速恢复高可靠。

7.2.3.14.质量感知。支持基于真实业务流的端到端和五元组粒度的网络丢包、时延检测，网络质量劣化时，能够针对劣化业务转发路径还原，并自动进行故障定位定界和告警。

7.2.4计算资源和存储资源

本项目日常运维工作中，涉及到网络管理、安全管理、统一身份认证、上网日志留存、远程运维等各种业务软件，这些业务软件均需要计算资源和存储资源，为了保障本项目当前及未来3年的运维需求，本次设计在教育骨干网的3个核心节点和10个高校城市节点配置虚拟化一体机，为项目管理和运维业务提供相应计算资源和存储资源。

7.2.5可视化运维能力

统一的可视化运维能力涉及到多个运营商、厂家等运维能力的整合，是一个长期建设完善的过程。因此，在建设初期，由运营商在各自运维系统上为教育行政管理部门开设账号，各级教育部门按照分权分域进行管理，可以查看所辖教育城域网内的网络拓扑、设备告警、线路告警以及流量监控等信息，实时查看网络运行状态，初步做到网络全程可见、可管、可控。随着教育网搭建成熟后，可以考虑引入第三方集成厂家，对各个运营商提供的运维数据进行集成展示，真正做到运维可视一张图，为运维提供直观化的管理手段。

7.3网络安全运维要求

落实各级教育行政管理部门网络安全责任，分级管理分级负责。按统一的技术规范建设教育网网络安全管理系统，对敏感数据和网络信息进行安全管控。各级教育行政管理部门具备网络应用态势感知、快速反应和处置能力，配置有互联网出口的教育管理机构必须承担相应网络安全责任，按相关法规、标准和规范的要求建设实名制认证、应用管理等技术系统，并负责处置相关网络安全事件和事故。

7.4运营商网络运维要求

7.4.1属地化售后服务

为广西教育网提供线路服务的运营商，需建立专属售后维护机制，在各市县均设立有售后服务机构，提供相应的售后服务工作。

根据线路故障等级分为：教育骨干网故障、教育城域网故障，并遵循以下故障处理原则：

7.4.1.1教育骨干网故障

如由运营商主动发现的教育骨干网故障，由运营商自治区级负责人向自治区教育厅负责人或授权人报备故障情况；如首先发现故障的是自治区教育厅，由自治区教育厅的负责人或授权人通知运营商自治区级专职客户经理，运营商客户经理协调相关部门进行故障处理。

故障处理过程中，运营商客户经理每30分钟主动反馈故障处理情况；故障处理完成后30分钟内，客户经理向教育厅负责人或授权人口头反馈故障原因和处理结果后，3个工作日内按客户需要提交故障处理书面报告。

7.4.1.2故障升级

当各市县教育城域网故障未在要求时限内修复时，上升为自治区级故障，由运营商市县级专职客户经理通知自治区区级专职客户经理，运营商自治区级专职客户经理第一时间向广西教育厅的负责人或授权人报备，同时协调相关部门进行故障处理。

7.4.2业务恢复时限

业务故障指影响教育网线路运行，影响业务正常使用的故障，包括业务中断和一般故障。业务中断故障是指教育网专线业务至少一个局向通信全阻的情况；一般故障是指未全阻情况下的其他故障，如业务性能劣化。

业务恢复时限指自各级教育管理机构提出故障投诉时或出现监控告警时起，至网络业务恢复正常所需要的时间，如采用PTN/IPRAN接入方式，业务恢复时限和及时率要求见下表（单位：小时）。

业务恢复时限和及时率表

|  |  |
| --- | --- |
| 故障类别 | 市区 |
| 教育骨干网 | ≤4 |
| 一般故障（含性能劣化） | ≤24 |

注：业务恢复时间的统计可剔除不可抗力原因、各级教育管理机构自身网络原因及业务挂起的时长。

7.4.3故障处理反馈

故障处理反馈指从各级教育管理机构提出故障申告时起，运营商按照相应的要求向各级教育管理机构反馈故障处理过程，要求见下表。

故障处理反馈表

|  |  |
| --- | --- |
| 故障处理反馈 | 处理要求 |
| 阶段反馈故障处理情况 | 按各级教育管理机构需要，每30分钟反馈 |
| 口头反馈故障原因和处理结果 | 故障处理完成后30分钟内向各级教育管理机构反馈 |

根据影响业务的程度，在故障处理结束后运营商按需向各级教育管理机构提交故障处理的书面报告；如需提供，需在故障处理结束后3个工作日内提供故障报告。

7.4.4日常维护服务

日常维护服务是运营商为教育网提供的主动性维护服务，服务内容主要包括：网络运行监控服务、业务日常巡检、技术咨询与支撑、网络运行分析报告、客户端应急演练、售后服务联席会议、故障预警等内容。

7.4.4.1网络运行监控

网络监控服务指运营商向各级教育行政管理部门提供7x24小时的设备层、电路层等网络监控，获取各类告警、故障信息，实时响应并及时恢复、解决。电路层监控，只向专线类业务提供。

7.4.4.2业务巡检

业务巡检指运营商对业务运行情况开展主动性、预防性的检查，对涉及的设备告警、性能、运行状态进行检查分析。同时核对工程技术资料、电路资料、电路参数、维护路由、终端设备和内部组网等，保持客户资料的准确性和可用性，对客户端网络资源进行预警。

广西教育骨干网节点及教育城域网汇聚节点巡检周期为每半年一次。巡检后由运营商出具巡检报告，由各级教育行政管理部门签字确认。

7.4.4.3技术咨询与支撑

技术咨询与支撑指在业务使用过程中由运营商专业技术专家向各级教育行政管理部门提供技术咨询和支撑，及时解决业务使用过程中遇到的疑难技术问题。

7.4.4.4网络服务报告

网络服务报告是指根据各级教育管理机构需要，对网络在一段时间内的运行情况进行总结和分析。网络服务报告包括三类：网络运行分析报告、专项故障分析报告、业务分析与优化报告。

网络服务报告表

|  |  |
| --- | --- |
| 服务内容 | 金牌级服务 |
| 网络运行分析报告 | 按需提供，不高于每半年1次 |
| 专项故障分析报告 | 按需提供 |
| 业务分析与优化报告 | 按需提供 |

7.4.4.5应急演练服务

应急演练是指假想客户端网络可能出现的问题，而进行的应急电路调度或者主备业务的倒换测试。这里的客户端网络是指运营商负责维护的设备和电路。网络应急演练周期规定为按各级教育管理机构需要，不高于每半年一次，如遇“两会”等重大活动或节假日重要通信保障，可根据需求增加测试次数。

7.4.4.6售后服务联席会议

售后服务联席会议指运营商业务部门组织定期与各级教育管理机构共同对售后服务的质量进行检查和评估，对服务项目进行总结，形成备忘录/会议纪要。

7.4.4.7故障预警

（1）运营商专线预警功能

故障发生后，系统会实时关联出运营商客户“运营商编号、运营商名称、运营商级别，预警业务、故障类型、故障开始时间、目前处理进度，当前处理人，当前处理人联系电话”等信息，所有告警均通过短信、生成ESOP任务方式对客户经理、进行通知。

（2）故障累计预警

针对每月有累计故障考核的业务，结合运营商编码及专线名称，如X运营商的专线名称为xx，可以设置月累计故障值为2，当同一运营商的同一专线名称收到告警大于等于2次，则给该运营商客户的客户经理进行预警，通过发短信、生成任务单方式进行预警。

（3）预警报表统计查询功能

平台可按照“运营商编号、运营商名称、运营商级别，预警业务、故障类型、故障开始时间、目前处理进度，当前处理人，故障解决时间，当前处理人联系电话”进行统计，查询字段为“运营商编号、运营商名称、运营商级别，预警业务、故障类型、故障开始时间、目前处理进度、故障解决时间”进行查询，定期分析运营商客户故障情况，并对故障情况进行分析，对故障发生超过设定门限专线进行预警重点保障，形成故障发生可监控、处理过程可管理、处理结果可分析优化的闭环管理机制。

7.4.5应急维护保障

运营商需要充分、积极、有效地应对各种自然灾害、突发事件造成的通信设备瘫痪，做好在各种紧急情况下的重要客户网络应急通信保障和处理工作，保证教育网在出现重大通信故障时，合理、高效、迅速地恢复通信，缩短电路阻断历时，要求运营商将针对教育网特点制定相应网络安全的应急处理预案，提供多种应急处置方案。

应急预案维护标准是要求在预案的基础上，能以最短的维护时限完成教育网故障网络的修复工作，同时要保证预案的可执行性、资源准确性、调度及时性。

7.5运维权限规划

统一由运营商进行教育城域网，以及网络线路部分的维护，针对学校规模较大，如学生人数超过1000人以上的中小学等有较强个性化运维需求的学校，运营商可开放一些运维管理平台的账号，分配二级账号。

**八、软硬件配置**

8.1选型基本原则

8.1.1国产化原则

根据《鼓励软件产业和集成电路产业发展的若干政策》中规定，国家投资的重大工程和重点应用系统，应优先由国内企业承担，在同等性能价格比条件下应优先采用国产软硬件系统。

8.1.2开放性和扩展性原则

一方面，系统将与各部门的业务系统及数据库相连接，要采用开放性、标准化的设备、软件及信息资源；另一方面，系统对于未来可能增添的新的子系统、新的数据库、新的功能、新的用户都要留有接口和二次开发API，并符合电子政务相关技术标准，系统可以随形势的发展而不断成长扩大。

8.1.3先进性和成熟性原则

信息技术尤其是软件技术发展迅速，新理念、新体系、新技术迭相推出，这造成了新的、先进的技术和成熟的技术之间的矛盾。而大规模、全局性的应用系统，其功能和性能要求具有综合性。因此，在产品选用方面要求先进性和成熟性的统一，以满足系统在很长的生命周期内有持续的可维护性和可扩展性。

8.1.4可靠性原则

在社会向信息时代迅速发展的同时也有潜在危机，即对信息技术的依赖程度越高，系统失效可能造成的危害和影响也就越大。因此，本系统的软硬件选择在尽可能有限的投资条件下，从系统结构、网络结构、技术措施、设备选型以及厂商的技术服务和维修响应能力等方面综合考虑，确保系统整体运行的可靠性。

8.2硬件选型原则

系统硬件平台是支撑应用系统运行的核心基础设施，主要包括高性能服务器、高容量存储设备和其他相关软硬件设备。其中，高性能服务器用于提供快速、可靠的计算，高容量存储设备用于容纳存储相关数据。硬件平台性能的好坏将直接影响到应用系统的运行效果。

由于应用系统的复杂性和特殊性，对于其硬件平台设计需要采用如下的原则：

8.2.1统一性

明确应用系统在规划期内的规模，对整个应用系统的模块、用户、流程进行分析，确定总体需求，从而定义出其硬件平台对应的架构和配置。

8.2.2高可用性

要求硬件平台具有单点失效保护，能够实现故障预警、报警，具有良好的故障应急处理能力。如在出现有限个数的服务器、磁盘、存储设备或交换机故障等情况下，系统可以继续运行，不影响业务处理。

8.2.3高扩展性

由于应用系统建设是一个长期持续的过程，日后随着城市规模扩大和业务量的增长，用户数可能会超出预期，当硬件平台的处理能力不够时，要求可以在原有架构的基础上实现灵活扩展。硬件平台的扩展性主要分成两类：纵向扩展和横向扩展。纵向扩展是指通过增加硬件设备的CPU、内存、通道和板卡等资源来提高原有设备的处理能力；横向扩展是指通过购买新的设备和原有设备并行工作，通过负载分担来实现处理能力扩展。

8.2.4高安全性

能够实现良好的信息安全能力，能够应用灵活的安全策略，如对不同用途的服务器进行安全分区以实现不同程度的隔离等。

8.2.5高可维护性

维护便捷简单，尽量减少宕机时间，特别是减少进行故障修复、系统扩展和变更时的宕机时间，能够提供友好、全面的监控工具。

8.2.6合适性价比

在满足需求并符合上述原则的前提下，良好的性价比是关键。各家硬件各有所长，关键是需要关注满足应用系统需求的技术，而不是一味追求先进技术，只要能解决主要问题，满足需求和原则，有合适的价格，就可以着重考虑。

8.3软件选型原则

8.3.1系统软件

8.3.1.1．操作系统。服务器运行安全、稳定、可靠，硬件设备兼容性优异，支持多种软件集成，拥有高效完善网络功能和图形工作平台等。

8.3.1.2．数据库软件。具有高可靠性，开放可扩展，编程接口符合国际通用标准，支持多个操作系统平台部署，拥有高效并发控制机制，提供查询优化策略，支持故障恢复，提供备份和还原，支持多媒体数据存储，提供全文检索功能，支持数据仓库，支持数据库集群等。

8.3.2平台软件

8.3.2.1．安全软件。技术安全可控，具有高度安全可靠性，开放可扩展，嵌入式安全管理，可信消息管控等。

8.3.2.2．基础中间件。技术安全可控，提供API接口，并符合行业通用标准，开放可扩展。基于J2SE的Java语言，提供HTTP/HTTPS服务、Servlet/JSP服务、SOAP/WS服务、远程调用服务、SOA服务总线、安全服务和日志服务，支持集群和负载均衡。

8.3.2.3．交换处理中间件。技术安全可控，提供API接口，符合SOA标准，开放可扩展。提供数据存取、交换、访问、通讯、处理等功能，提供分布式服务。

8.3.2.4．资源目录交换中间件。技术安全可控，提供API接口，并符合LDAP和SOA标准，开放可扩展。提供资源目录发现，资源目录状态监测，资源目录状态存储，资源目录索引，分布式资源目录检索等功能。

8.4软硬件配置参考清单

本项目软硬件配置参考清单如下表：

**A分标**

| 序号 | 子系统名称 | 分类 | 产品名称 | 配置参数 | 单位 | 数量 |
| --- | --- | --- | --- | --- | --- | --- |
| 1 | 教育骨干网 | 线路 | 线路租用 | 1. ≥10G点对点专线，租用期：3年。  2. 透明传输电路，上下行带宽对等，传输电路与互联网（公网）隔离。  3. 具备自愈环保护，具备双路由保护。  4. 相关网络设备满足可平滑升级的要求。  5. 传输设备要求具有全网网管监控功能，并实行7\*24小时实时监控；用户端可实时监测电路状况，线路监控设备由服务商提供。所有接入设备由服务商提供，所有电路经由服务商汇聚后提供给用户使用。  6. 网络参数要求：  ▲（1）端到端电路的传输比特差错率(误码率)：≤1.0×10E－7；  ▲（2）全年网络阻断时长不超过24小时；  ▲（3）端到端电路丢包率≤1%；  （4）端到端电路平均网络延时≤50ms、时延抖动率≤10ms。  7. 保证网络的畅通，负责运营商到用户单位主干光缆所有设备的免费运行维护，如光端机、转换器等设备；免费培训传输知识，指导采购方技术人员做好日常维护。  8. 用户网络需要扩展或升级时，免费提供相应解决方案等技术支持。  9. 以未约定的其它服务质量指标，则由中标供应商按信息产业部《电信服务质量标准（试行）》的质量要求，为采购人提供相应的服务质量。 | 条 | 3 |
| 2 | 线路租用 | 1. ≥1G点对点专线，租用期：3年。  2. 透明传输电路，上下行带宽对等，传输电路与互联网（公网）隔离。  3. 具备自愈环保护，具备双路由保护。  4. 相关网络设备满足可平滑升级的要求。  5. 传输设备要求具有全网网管监控功能，并实行7\*24小时实时监控；用户端可实时监测电路状况，线路监控设备由服务商提供。所有接入设备由服务商提供，所有电路经由服务商汇聚后提供给用户使用。  6. 网络参数要求：  ▲（1）端到端电路的传输比特差错率(误码率)：≤1.0×10E－7；  ▲（2）全年网络阻断时长不超过24小时；  ▲（3）端到端电路丢包率≤1%；  （4）端到端电路平均网络延时≤50ms、时延抖动率≤10ms。  7. 保证网络的畅通，负责运营商到用户单位主干光缆所有设备的免费运行维护，如光端机、转换器等设备；免费培训传输知识，指导采购方技术人员做好日常维护。  8. 用户网络需要扩展或升级时，免费提供相应解决方案等技术支持。  9. 以未约定的其它服务质量指标，则由中标供应商按信息产业部《电信服务质量标准（试行）》的质量要求，为采购人提供相应的服务质量。 | 条 | 9 |
| 3 | 网络数据交换和管理服务 | 核心数据交换服务 | 1.满足核心数据交换服务需要。  2.主控冗余设计且满配，电源冗余设计且满配，要求所有业务板卡及电源、风扇均可热插拔。 3.配置≥4独立交换网板或性能相同或更优的产品。  4.整机支持业务载板插槽≥8个。 5.配置10G光口≥10个，≥40G的光口≥4个（分布在至少2个业务槽位）；10G单模光模块≥10个，≥40G的单模光模块≥4个；所配光口和光模块要与组网连接线路和网络管理运维要求匹配。 6.支持网络资源、隧道路径、业务路径、及业务SLA的可视可管；支持广域网智能调优。  7.支持SRv6，提供SRv6承载VPN业务能力。提供SRv6 Policy功能，具备网络定制化服务和差异化服务能力。 | 台 | 6 |
| 4 | 汇聚数据交换服务 | 1.满足汇聚数据交换服务需要。  2.主控冗余设计且满配，电源冗余设计且满配，要求所有业务板卡及电源、风扇均可热插拔。 3.配置≥2独立交换网板或性能相同或更优的产品。  4.整机支持业务载板插槽≥8个。 5.配置万兆光口≥4个，千兆光口≥10个；配置万兆单模光模块≥4个，千兆单模光模块≥10个；所配光口和光模块要与组网连接线路和网络管理运维要求匹配。 6.支持网络资源、隧道路径、业务路径、及业务SLA的可视可管；支持广域网智能调优。  7.支持SRv6，提供SRv6承载VPN业务能力。提供SRv6 Policy功能，具备网络定制化服务和差异化服务能力。 | 台 | 26 |
| 5 | 网络管理服务 | 1.系统支持大规模设备管理能力，可管理≥20000台网元；系统支持多种设备的管理，包括并不仅限于交换机、路由器、防火墙、WLAN、服务器、存储、IP话机、摄像头等；实配50个设备授权。  2.配置配套操作系统与数据库，以及配套的部署硬件设备。  3.提供告警、性能、有线无线资源、用户终端定位信息等报表管理能力。  4.网络质量监控：系统支持基于真实流的IP网络实时监测能力（非模拟报文监测或者探针式监测），监测结果可实时在拓扑上显示；  5.提供设备原厂不少于50台路由器、交换机等网络设备3年实时远程监控运维服务。 | 套 | 1 |
| 6 | 网络控制服务 | 1.包含管理、控制和分析集成的统一云化架构，管理授权覆盖教育骨干网不少于50台路由器、交换机等网络设备。支持统一的Portal来访问所有的组件，包括设备管理，业务发放，网络优化，网络监控与仿真分析。  2.支持根据实时采集的网络状态和性能数据，按照链路带宽、质量、亲和属性等策略进行网络优化。  3.支持自动发现网络设备及链接关系，生成全网的网络拓扑、支持实时更新网络的拓扑变化；具备从业务到隧道再到链路，分层路径检视与可视化的能力。  4.支持提供业务性能和质量的统计报告及可视化呈现，包括并不仅限于丢包、时延、抖动。  5.配置与控制器匹配的处理设备和存储设备的支撑系统。 | 1 |
| 7 | 网络安全管理服务 | SSL VPN应用服务 | 1.满足电子政务外网接入应用服务需要。  2.电源冗余设计且满配，≥6个千兆电口，≥4个千兆光口，且满配光模块。  3.内存≥8G，硬盘SSD≥64G；加密流量（Mbps）≥400，并发用户数≥6000，IPSec加密流量（Mbps）≥200，设备整机吞吐量≥1.5Gbps，设备整机并发会话数≥160万。  4.支持主从账号绑定，实现SSL VPN账号与应用系统账号的唯一绑定，VPN资源中的系统只能以指定账号登陆。  5.提供环境检测、自动修复工具，支持终端桌面环境兼容性一键检测能力，以及对检测结果进行一键修复的能力。 | 台 | 2 |
| 8 | 集权安全区网络安全隔离服务 | 1.满足区域网络安全隔离服务需要。  2.≥6千兆电口，≥2万兆光口，且满配光模块。  3.网络层吞吐量≥25G，应用层吞吐量≥3G，并发连接数≥2200000，新建连接数（CPS）≥200000。  4.支持基于对象、区域和地域维度设置安全访问控制策略，允许或拒绝特定国家或者地区的对象访问内部网络，保障业务重大时期安全可靠性。  5.产品内置IPS检测引擎，支持口令暴力破解、僵尸网络、恶意软件、服务器与终端漏洞攻击等检测和防护，支持≥7000种特征规则。  6.可以与安全态势感知系统和原有终端安全系统联动，实现对高危IP、端口的封堵。 | 台 | 2 |
| 9 | 配件 | / | 42U标准机柜；系统集成所需的配件、配线等，所配的配件器材要与组网连接线路和网络管理运维要求匹配。 | 批 | 1 |

**B分标**

| 序号 | 子系统名称 | 分类 | 产品名称 | 配置参数 | 单位 | 数量 |
| --- | --- | --- | --- | --- | --- | --- |
| 1 | 教育骨干网 | 线路 | 线路租用 | 1. ≥10G点对点专线，租用期：3年。  2. 透明传输电路，上下行带宽对等，传输电路与互联网（公网）隔离。  3. 具备自愈环保护，具备双路由保护。  4. 相关网络设备满足可平滑升级的要求。  5. 传输设备要求具有全网网管监控功能，并实行7\*24小时实时监控；用户端可实时监测电路状况，线路监控设备由服务商提供。所有接入设备由服务商提供，所有电路经由服务商汇聚后提供给用户使用。  6. 网络参数要求：  ▲（1）端到端电路的传输比特差错率(误码率)：≤1.0×10E－7；  ▲（2）全年网络阻断时长不超过24小时；  ▲（3）端到端电路丢包率≤1%；  （4）端到端电路平均网络延时≤50ms、时延抖动率≤10ms。  7. 保证网络的畅通，负责运营商到用户单位主干光缆所有设备的免费运行维护，如光端机、转换器等设备；免费培训传输知识，指导采购方技术人员做好日常维护。  8. 用户网络需要扩展或升级时，免费提供相应解决方案等技术支持。  9. 以未约定的其它服务质量指标，则由中标供应商按信息产业部《电信服务质量标准（试行）》的质量要求，为采购人提供相应的服务质量。 | 条 | 3 |
| 2 | 线路租用 | 1. ≥1G点对点专线，租用期：3年。  2. 透明传输电路，上下行带宽对等，传输电路与互联网（公网）隔离。  3. 具备自愈环保护，具备双路由保护。  4. 相关网络设备满足可平滑升级的要求。  5. 传输设备要求具有全网网管监控功能，并实行7\*24小时实时监控；用户端可实时监测电路状况，线路监控设备由服务商提供。所有接入设备由服务商提供，所有电路经由服务商汇聚后提供给用户使用。  6. 网络参数要求：  ▲（1）端到端电路的传输比特差错率(误码率)：≤1.0×10E－7；  ▲（2）全年网络阻断时长不超过24小时；  ▲（3）端到端电路丢包率≤1%；  （4）端到端电路平均网络延时≤50ms、时延抖动率≤10ms。  7. 保证网络的畅通，负责运营商到用户单位主干光缆所有设备的免费运行维护，如光端机、转换器等设备；免费培训传输知识，指导采购方技术人员做好日常维护。  8. 用户网络需要扩展或升级时，免费提供相应解决方案等技术支持。  9. 以未约定的其它服务质量指标，则由中标供应商按信息产业部《电信服务质量标准（试行）》的质量要求，为采购人提供相应的服务质量。 | 条 | 9 |
| 3 | 网络安全服务 | 统一身份认证服务 | 1.满足身认证服务服务需要。  2.电源冗余设计且满配，≥4个千兆电口，≥2个千兆光口，且满配光模块。 3.支持并发用户数≥100000。 4.支持统一认证/统一门户/单点登录/多因子认证等功能；支持用户添加自定义属性管理；支持应用权限管理；支持行为日志审计；支持密码自助找回、支持账号自助注册；支持用户信息自助修改。 5.与本项目投标所用到的安全态势感知、上网行为管理、下一代防火墙、SSL VPN等需要用到身份信息的设备和系统实现数据对接和联动。 | 台 | 26 |
| 4 | 安全态势感知服务 | 1.满足教育网安全态势感知管理服务需要。  2.具备对威胁的实时监测、预警与处置能力，提供API及其他数据接口，可接收各个教育城域网的资产信息、安全事件、脆弱性风险等信息，实现广西教育网网络中心和广西教育数据中心网络安全一体化管理运维，以及信息融合展示。 3.支持与广西教育数据中心现有广西教育网络安全管理信息系统对接，上传安全日志和工单通报，工单通报内容包括事件描述、事件危害、所属单位、事件等级、处理时间、通报时间等信息。 | 台 | 1 |
| 5 | 虚拟化数据处理和存储服务 | 服务器 | 配置≥2颗24核CPU模块，≥192GB 内存模块，≥2块300G SAS HDD硬盘，≥96T SATA HDD硬盘，≥3块960GB SSD 硬盘，≥2端口千兆电口网卡，≥2块2端口万兆光口网卡含光模块，≥1块2G缓存RAID卡含掉电保护模块，冗余电源。 | 套 | 39 |
| 6 | 超融合管理软件 | 配置2颗CPU管理授权；提供用户自助服务界面，用户能够通过自助服务门户完成云资源申请、使用、修改、销毁等操作；兼容主流虚拟化平台。 |
| 7 | 计算虚拟化软件 | 配置2颗物理CPU授权许可；提供统一的虚拟机管理界面，在同一界面上提供虚拟机启动、暂停、恢复、休眠、重启、关闭、关闭电源、克隆、迁移、备份、模板导出、快照等功能；配置虚拟化安全防护功能模块。 |
| 8 | 存储虚拟化软件 | 配置2颗物理CPU授权许可；采用分布式的软件定义存储架构，在通用x86服务器部署，把所有服务器硬盘组织成一个虚拟存储资源池，提供分布式存储服务，无需独立的元数据及控制器节点。 |
| 9 | 网络交换机 | ≥14个万兆光口，≥8个千兆电口，满配光模块，配套系统集成所需的线材。 | 台 | 26 |
| 10 | 一体化管理软件 | 配置1套管理软件；提供广西教育网网络中心统一管理≥45套虚拟化一体机系统的许可；集成云管理能力，对外提供一套集云资源、云服务、云运营、云运维为一体的管理平台。 | 套 | 1 |
| 11 | 配件 | / | 42U标准机柜；系统集成所需的配件、配线等，所配的配件器材要与组网连接线路和网络管理运维要求匹配。 | 批 | 1 |