广西壮族自治区教育技术和信息化中心

桂教技信〔2023〕28号

关于印发《广西教育城域网接入骨干网技术指南》的通知

各市、县（市、区）电教站（中心）：

根据桂教网信〔2022〕20号文的要求，为了指导各地结合本地实际，加快推进教育城域网建设，保障广西教育网及其承载的关键信息基础设施和信息系统（网站）稳定、持续、安全的管理运维和应用，落实网络安全等级保护制度要求，做好广西教育网网络安全、数据安全、个人信息保护和未成年人信息保护等工作，我中心编制了《广西教育城域网接入骨干网技术指南》。现印发给你们，请参照执行。

未尽事宜，请与我中心联系，联系人及电话：彭远，18070900166。

附件：广西教育城域网接入骨干网技术指南

广西壮族自治区教育技术和信息化中心

2023年6月5日

广西教育城域网接入骨干网
技术指南

（Version 1.0）

广西壮族自治区教育技术和信息化中心

2023 年 6 月

目　　录

第一章 总则

1.1 编制目的

为确保广西教育网及其承载的关键信息基础设施和信息系统（网站）稳定、持续、安全的管理运维和应用，落实网络安全等级保护制度要求，做好广西教育网网络安全、数据安全、个人信息保护和未成年人信息保护等工作，结合广西教育网实际情况，制定本指南。

1.2 责任划分

广西教育网由自治区教育厅主管，由广西教育技术和信息化中心（广西教育网网络中心）负责广西教育网网络中心和骨干网的建设和管理运维。广西教育网各高校城市节点（高等学校）配合广西教育网网络中心，开展高校城市节点的管理运维工作。广西教育城域网由属地教育行政部门负责建设和管理运维。

按照“分级管理分级负责”“谁主管谁负责、谁建设谁负责、谁应用谁负责、谁运维谁负责”的原则，各级教育行政部门及其直属单位对本地区本单位城域网的网络安全工作负主体责任，领导班子主要负责人是第一责任人，主管网络安全的领导班子成员是直接责任人。

广西教育城域网由各级教育行政部门委托通信运营商建设和管理运维，各级教育行政部门和通信运营商应就本地教育城域网建设和管理运维商定双方权利和义务，划清责任范围，约定工作交接面的相关细则。

1.3 适用范围

本办法适用于各级教育行政部门和通信运营商参与广西教育城域网建设，完成本地教育城域网接入广西教育骨干网的相关工作需要。

第二章 网络建设

2.1 教育城域网

2.1.1网络架构

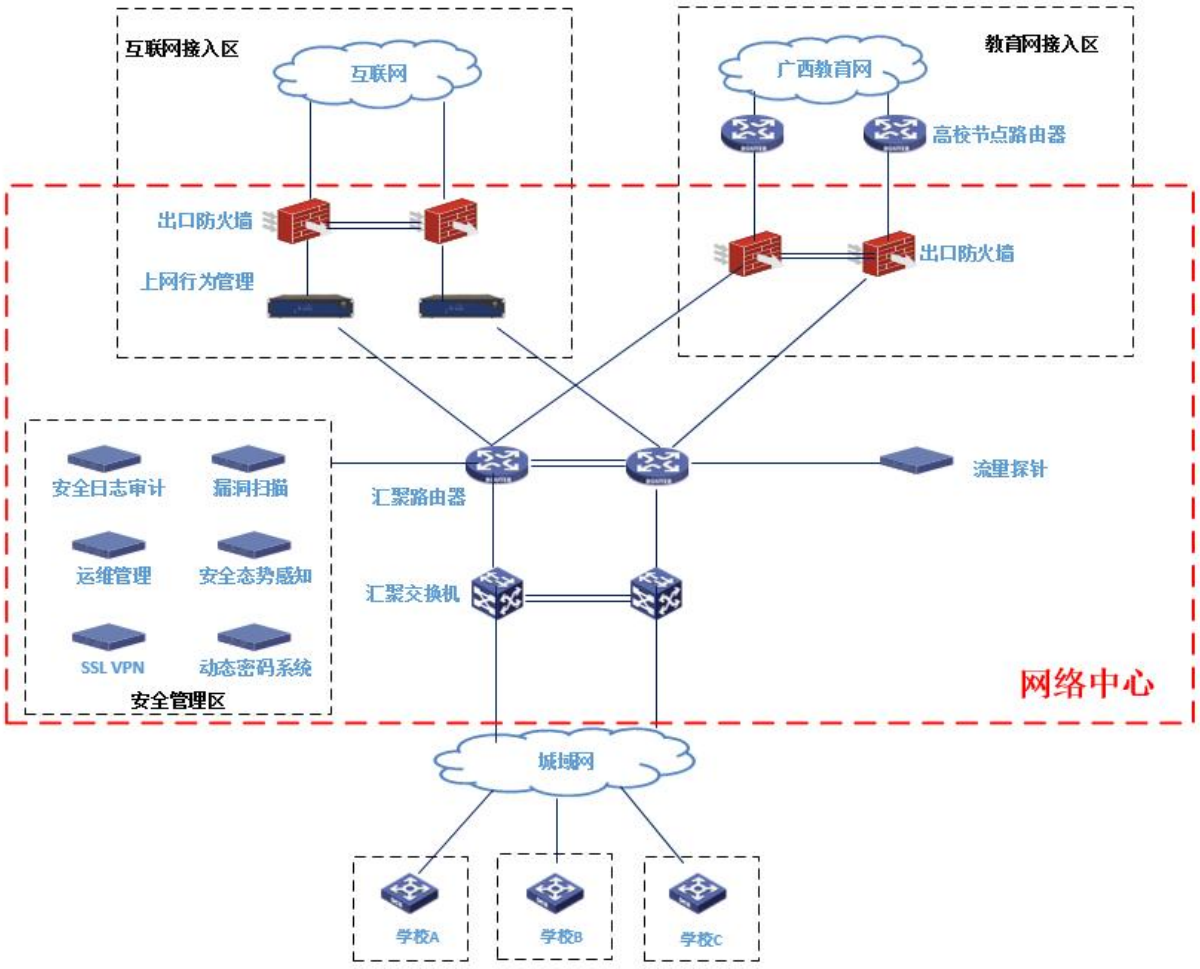

图 1-1 广西教育城域网架构图

城域网统一建设两组网络出口。一是骨干网出口，租用运营商的 IP 网络线路与广西教育骨干网互联。二是互联网出口，租用运营商的互联网接入服务。

各级各类学校通过广西教育网与广西电子政务外网互联。如果本地有大量信息系统（网站）应用部署于本地电子政务云的，应考虑城域网与属地电子政务外网的互联。

城域网与互联网出口区联接时，应通过城域网汇聚路由器设备分别与互

联网出口区的上网行为管理设备互联，采用双设备双线路冗余设计。通信运营商在提供的互联网访问服务时，提供的互联出口链路也采用双路由保护冗余设计。

城域网与骨干网对接时，应通过城域网汇聚路由器设备分别与本级高校城市节点路由器设备互联，采用双设备双线路冗余设计。

城域网汇聚交换机主要汇接学校校园网的接入设备，应使用双上联方式连接汇聚路由器，实现冗余可靠。

学校校园网设备通过通信运营商线路接入城域网汇聚交换机，接入方式根据当地实际情况选择，可采取 OTN、IPRAN、PTN、PON 等多种接入方式。

2.1.2组网要求

城域网网络规模大，组网复杂，根据当地的组网结构及采购设备的特点，采取有利于组网及通信的路由协议，可采取 ISIS、OSPF 动态路由、静态路由或多种路由协议结合等路由技术进行组网。组网时遵循以下原则：

（一）可靠性高。网络中心汇聚区采用双设备冗余设计，关键链路采用冗余备份或者负载分担。关键设备的电源、主控板等关键部件冗余备份，提高了整个网络的可靠性。

（二）可扩展性强。互联网接入区、教育网接入区、城域网汇聚区等关键设备可通过预留设备端口、插槽等用于后续扩展需求。

（三）便于管理和维护。可通过设备虚拟化、设备智能网管等技术，提升 IT 管理效率。

2.1.3 IP 地址

2.1.3.1 地址规划

由于城域网为专用网络，网络规模较大，所以整网采用统一规划的地址来规划各级 IP 地址范围。分配的 IP 地址类主要含互联网出口地址、教育网互联地址、设备标识地址、三层互联地址、网管地址、终端地址等。

城域网网络中心划分不同的网络区域，并按照方便管理和控制的原则为各网络区域分配地址。

（一）IPv4 地址规划。在申请接入广西教育骨干网时，应对城域网 IPv4 地址作出完整规划和具体分配。

（二）IPv6 地址规划。广西教育网 IPv6 地址规划将由原每个城域网规划一个/48 地址段变更为每个学校规划一个/48 地址段，具体事宜另行通知。请于申请接入广西教育骨干网时，与广西教育网网络中心联系实施建设的具体事宜。

2.1.3.2 地址管理

（一）统一规划管理。城域网运行维护单位承担全区 IP 地址的规划、申请、资源分配及备案等管理工作。

（二）专人负责管理。设置专人或组织负责管理、维护 IP 地址资源，确保 IP 地址数据的完整性、准确性、规范性和及时性。具有完整的 IP 地址规划、申请、分配、变更、回收、备案、稽核流程，形成 I P 地址的闭环管理机制。

（三）地址备案管理。应完整报备城域网 IP 地址，IP 地址报备中的地址备案类型应与地址使用用途相一致、IP 客户信息应与地址报备相一致。

2.1.4骨干网连接带宽

城域网与骨干网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。

2.1.5互联网连接带宽

城域网与互联网互联带宽设计要求：城镇学校班均出口带宽不低于 10M，有条件的农村学校班均出口带宽不低于 5M。

城域网与互联网互联带宽按实际应用需要开通，在带宽占用率达到 70%时进行扩容。

2.1.6校园网出口带宽

校园网与城域网互联设计带宽不少于 1G，首次开通时按实际应用需要开通带宽；当带宽占用率达到 70%时进行扩容。

2.1.7网络质量管理

城域网运行维护单位负责城域网网络质量和业务质量的管理工作；全面、系统、准确、及时地对城域网网络质量和设备故障情况进行分析统计，完成各项维护。

网络质量统计分析的范围主要包括城域网提供的设备能力指标、网络运行质量指标、服务质量指标（含网络容量及性能数据、流量流向数据、网络负荷、告警数据）。

应定期和不定期对城域网的网络质量进行巡检，找出影响网络质量的因素和保障质量的办法，有针对性地加强维护和服务工作，提出网络优化和规划建议。

（一）网络中心设备性能监测。监测部署于网络中心的设备性能，包括并不仅限于：CPU 及内存使用率，设备互联端口的流量、设备连接数等。当

设备 CPU 及内存使用率达 70%时，应检查设备问题，考虑更换设备，提升设备承载性能。当设备互联端口流量超过 70%时，应考虑增加端口或者更换更大容量的端口。

（二）互联网出口流量监测。监测城域网与互联网链路流量，当带宽占用率达到 70%，应及时进行扩容。

（三）学校出口流量监测。监测每所学校的校园网与城域网互联链路流量，当该接入带宽峰值达到 70%时，应及时进行扩容。

（四）网络通信质量巡检。巡检城域网内终端至互联网进行 ping 包测试，观察延迟和丢包率，如果延迟和丢包率较高，应逐段对网络进行检测查明原因，并及时修复。

2.2 校园网络

2.2.1VLAN 规划

（一）校园网应在网络交换机上部署 VLAN 技术。将一个校园网规模较大的广播域在逻辑上划分成若干个不同的、规模较小的广播域，有效的提高校园网络的安全性，减少广播风暴的危害。

（二）校园网按照业务或区域合理规划 VLAN。规划业务 VLAN、管理 VLAN 和互联 VLAN 等。

校园网的 IP 地址按照实际业务来进行 IP 地址划分，为了方便针对不同业务的流量进行精细化管理，应针对不同的业务划分不同的 VLAN 子网及对应的 IP 地址段。建议按照以下原则来划分不同 VLAN 子网（可根据不同学校的需求增减子网）：

1.办公室终端，含电脑、打印机、电视机等
2.计算机教室电脑
3.同步课堂设备
4.IP 广播设备
5.电子班牌设备
6.安防视频、视频会议
7.WIFI 网络
8.其他终端

2.2.2端口配置及限速

2.2.2.1 交换机组网

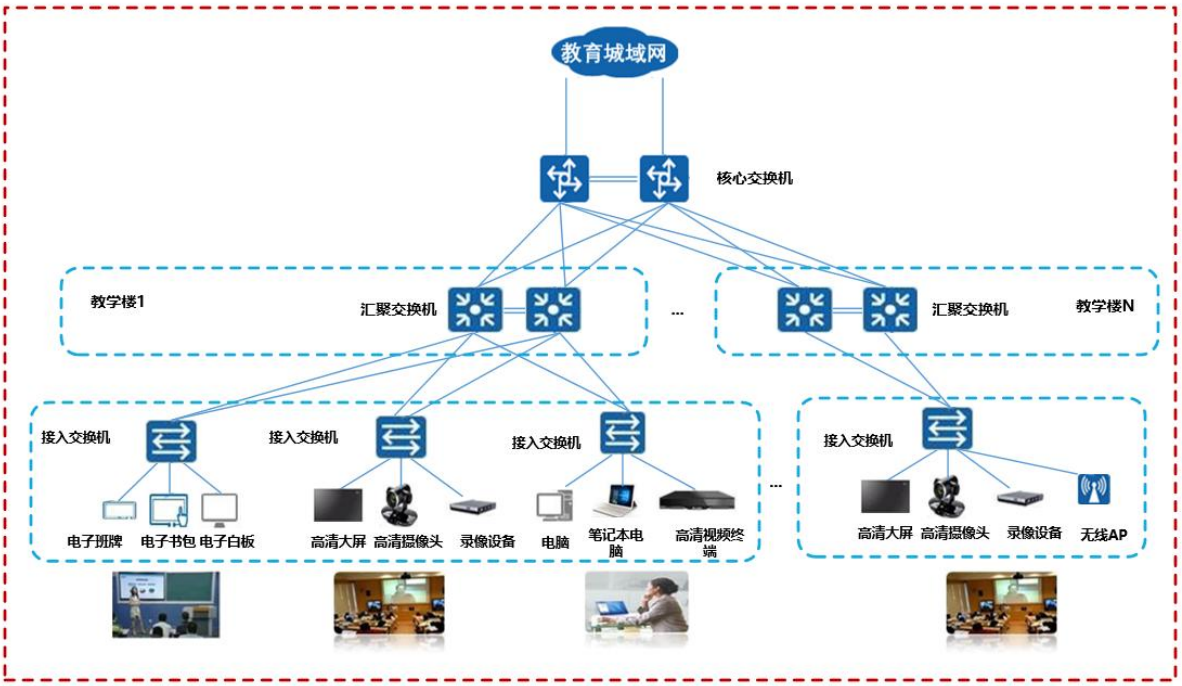

图 2-1 交换机组网的校园网示意图

2.2.2.1.1 校园网出口边界

（一）端口管理。校园网出口路由器或者交换机上检查物理端口使用情况，关闭无用物理端口。

（二）访问管理。在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝其他所有通信。在校园网出口路由器和交换机业务接口调用 ACL，只放行允许流量，拒绝所有未放行流量。

2.2.2.1.2 交换机端口限速

在校园网接入层交换机上开启端口限速，配置每个班级接入网络的端口带宽。按照以下原则进行端口限速。

（一）设区市城市、乡镇所在地的学校。教室下行带宽不少于 100M，上行带宽不少于 100M。计算机教室光纤或以太网接入校园网，下行带宽不少于 200M，上行带宽不少于 200M。

（二）农村学校（含农村不完全小学、教学点）。教室下行带宽不少于 100M，上行带宽不少于 30M。计算机教室光纤或以太网接入校园网，下行带宽不少于 200M，上行带宽不少于 60M。

2.2.2.2 全光网络组网

图 2-2 全光网络组网的校园网示意图

2.2.2.2.1 配置限速

对于全光网络的端口配置限速，可以采用账号、OLT、ONU 等方式进行限速。

（一）用户账户限速。采用运营商光纤接入的学校班级，采用 AAAA 对用户进行限速，设置每个班级的接入网络的带宽。

（二）OLT 配置限速。为保证网络畅通，对每个终端接入合理规划接入带宽，在 OLT 设备配置每个班级的接入带宽。

（三）ONU 端口限速。配置 ONU 的端口限速，设置每个班级的接入带宽。

2.2.2.2.2 MAC 地址限制

可通过配置 ONU 的 MAC 地址学习限制规则对接入终端进行限制，防止非法终端接入教育网络。

2.2.2.3 终端设备接入管理规范

对于终端设备接入校园网，为维护良好的网络质量，在终端接入管理方面应遵循以下原则。

（一）有线和无线接入方式管理。如果设备本身支持有线和无线接入，

则尽量采用有线进行接入，以保证网络质量的稳定性。

（二）无线网络接入管理。校园网内无线 WIFI 账号和密码，避免全校 WIFI 信号采用同一账号、密码，防止无线 WIFI 账号密码泄露后被非法接入消耗网络资源。

（三）校园网内网络设备级联管理。对于办公室采用小交换机、小无线路由器的问题需进行整改，应减少直至禁止多台小交换机多级级联。

第三章 网络安全体系建设

3.1 城域网

城域网应满足网络安全等级保护第二级的基本要求。为减少重复建设重复投资，避免浪费国有资产，应充分利旧通信运营商现有设备系统资源。

应在网络出口区域，针对互联网、教育网分别进行安全防护设计，包括结构安全、边界防护、访问控制、入侵防范、恶意代码防范等；在核心交换区域，针对本级城域网、下属校园网和教育机构网络的所有流量进行攻击检测、病毒木马检测、未知威胁检测等；在安全管理区域，针对本级城域网、下属校园网和教育机构网络实现安全审计、身份鉴别、授权管理、漏洞检测、终端安全管理等。

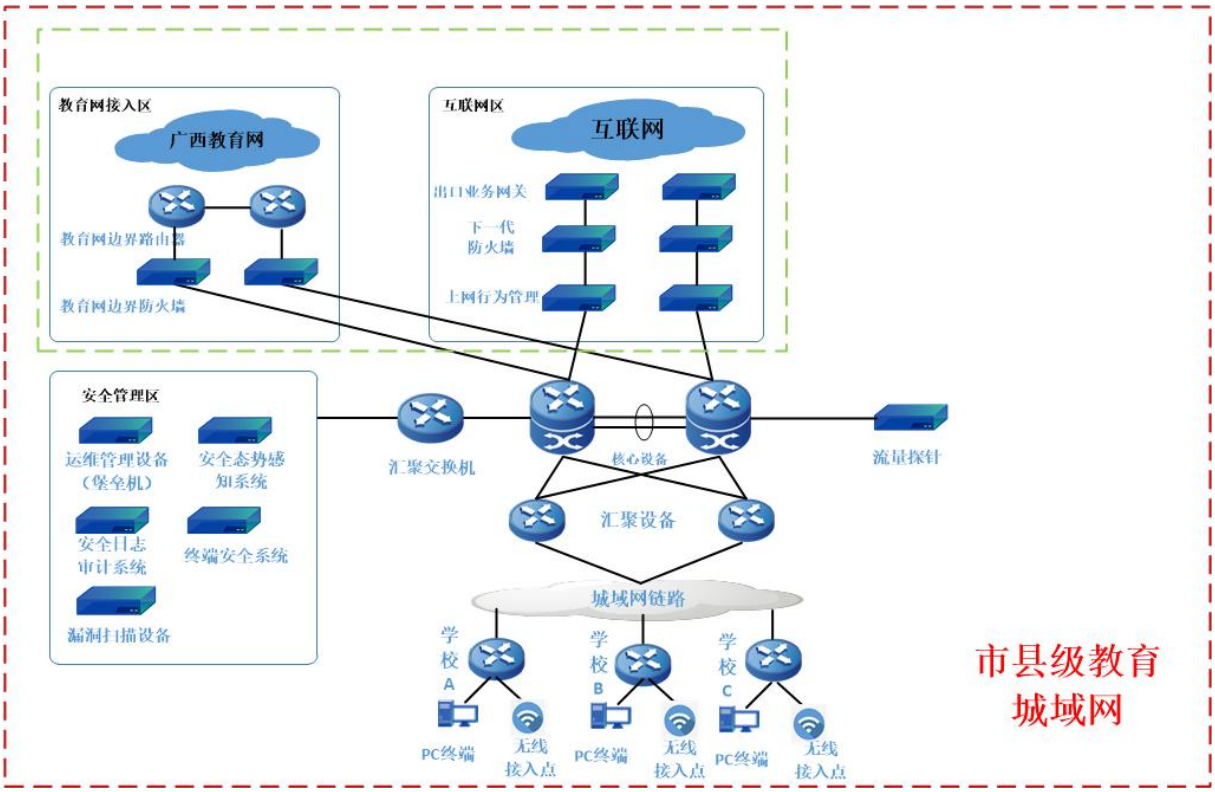

图 3-1 教育城域网安全防护示意图

（一）安全物理环境。

本项目城域网网络中心的物理位置位于各级教育行政部门租用通信运营商的机房，其中网络汇聚点的物理访问控制、防盗窃和防破坏、防雷击、防火、防水和防潮、防静电、电力供应的相关资源应充分利旧通信运营商现有机房设备系统。

（二）安全通信网络。

根据等保 2.0 网络架构相关要求，本次建设对接入服务设计了资源保证、优先处理等保障，包括并不仅限于：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。各地城域网分不同的城域网或网段，并按照方便管理和控制的原则为各城域网、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，以堆叠或 1+1 保护方式工作。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。

（三）网络安全区域边界。

根据等保建设分区分域的设计思路，将网络分为教育网接入区、互联网区、安全管理区。

根据等保 2.0 规范中边界防护、访问控制、入侵防范的要求，在互联网接入区边界、教育网接入区边界分别部署下一代防火墙，以双机冗余方式运行，实行不同边界网络严格的访问控制，将所有不安全的或不符合安全规则的数据包屏蔽，杜绝越权访问，防止各类非法攻击行为。启用入侵防御功能，实现 2~7 层数据的安全检测和阻断防护，提供对内部攻击、外部攻击和误操作的实时监控，实时、主动拦截黑客攻击、蠕虫、僵尸网络、后门木马、DOS 等恶意流量。

在互联网出口双机部署上网行为管理系统，针对本级城域网、下属校园网和教育机构网络的终端的上网行为的管理、带宽的限制和内容的审计等，根据业务需要调整应用访问和带宽利用率，同时防止敏感数据泄密和非法访问行为。上网行为管理系统应配置开放接口，可以使用公开标准接口或公开标准协议，应与广西教育数据中心核心节点的统一身份认证系统进行对接，实现对城域网内师生访问入网的准入认证，确保入网访问的身份安全。

（四）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”，并在该区域部署相关设备系统。

1.在安全管理区部署安全日志审计系统。配置可以接收所有日志对象，包括本级城域网内设备、下属校园网和教育机构网络出口设备，实时采集不同厂商的安全设备、网络设备产生的日志信息，并将这些信息汇集到审计中心，进行集中化存储、备份、查询、审计、告警、响应，出具丰富的报表报告，获悉城域网的整体安全运行状况，实现全生命周期的安全管理。

2.在安全管理区部署运维管理系统。配置可以访问所有管控对象，包括本级城域网内设备、下属城域网内设备，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，并需要对高危操作进行授权审批。

3.在核心交换区部署检测探针。通过网络流量镜像在内部对用户到业务资产、业务的访问关系进行识别，基于捕捉到的网络流量对内部进行初步的攻击识别、违规行为检测与内网异常行为识别。同时，可以将检测数据与分析结果上传至广西教育数据中心核心节点进行汇总分析。

4.在安全管理区域部署安全态势感知系统，对检测探针的数据和各个安全设备日志进行收集，并通过可视化的形式为用户呈现内网业务资产及针对内网关键业务资产的攻击与潜在威胁，安全态势感知系统支持下发策略至防火墙等安全设备，对攻击进行一键封锁，并形成安全问题工单，派发工单通知内部运维人员进行处置，通过该系统对现网所有安全系统进行统一安全管理。

安全态势感知系统应配置开放接口，可以使用公开标准接口或公开标准协议，应与广西教育数据中心核心节点的安全态势感知系统共享交换数据，在广西教育数据中心核心节点可以实现对广西教育网全网安全的可视化和感知管控。

5.在安全管理区部署漏洞扫描系统，配置可以访问所有检测对象，包括本级城域网内设备、下属校园网和教育机构的出口设备，评估各个网络区域的安全状况，包括现有的网络设备和安全设备，以及后续增加的 WEB 应用、服务器区域、数据库等。通过漏洞扫描系统，能够主动对网络中的资产进行细致深入的漏洞检测、分析，并能提供专业、有效的漏洞防护建议，帮助运维管理人员落实安全整改问题。

（五）安全计算环境。

根据等保 2.0 技术要求中安全审计的要求，在安全管理区部署安全日志审计系统，该设备和本章节“（四）安全管理中心”描述的日志审计为同一台设备，为避免方案理解错误而造成重复建设特此说明。

3.2 校园网

在校园网安全设计中，高等院校、区直中等职业学校主要考虑接入城域网边界安全，其他部分由学校按照相关标准规范自行建设；中小学学校和其它教育机构，主要考虑校园网边界安全防护部分和终端安全部分，对于校园网内部的安全审计与管理，由学校自行根据实际需要自主建设。按照设备部署方式，校园网边界安全防护主要分为两类。

（一）实体设备类。该类适用于已经部署了边界安全防护设备，或班级

规模较大的中小学，教育资源和教育服务需求较高，需要通过硬件设备进行防护的。该类学校接入设备原来已采购的，可以继续复用，需要将防护设备的管理权限提交至上级城域网的运维管理系统中实现统一管理，将防护设备的日志上传至上级城域网的安全日志审计系统和安全态势感知平台中进行分析。

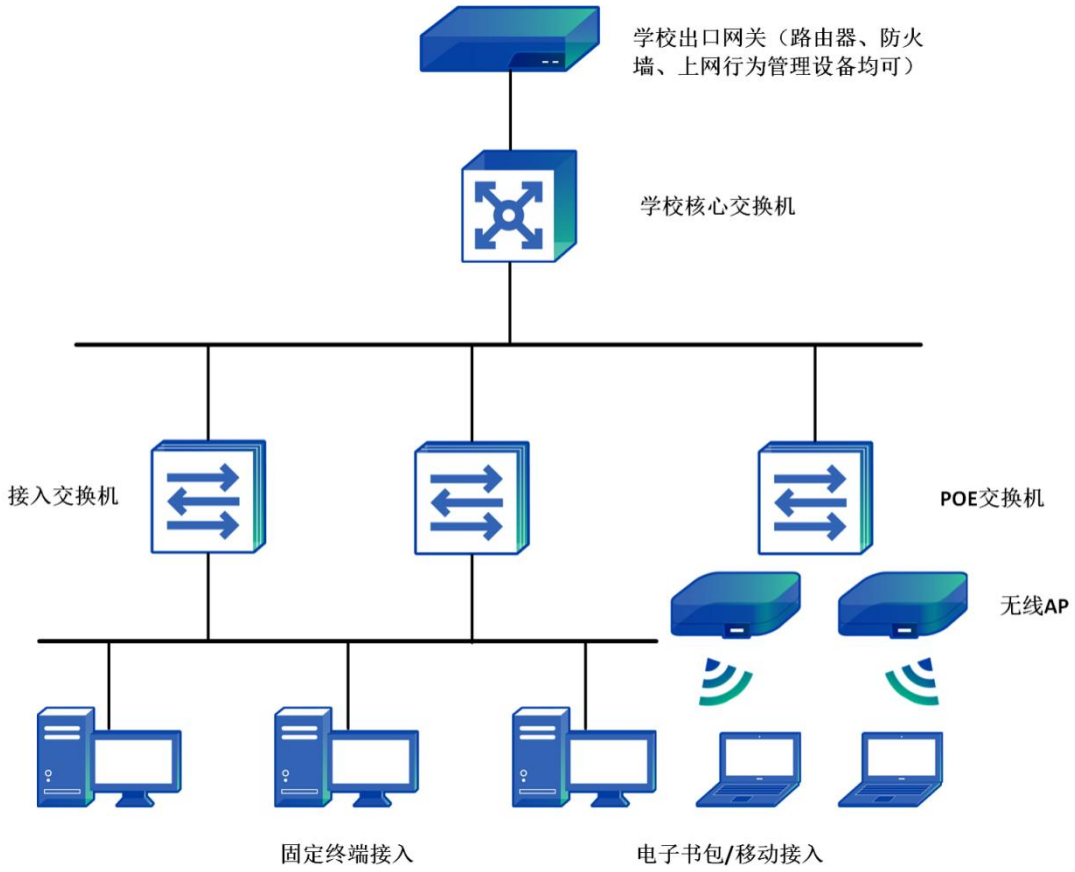

图 3-2 校园网实体设备安全防护示意图

在校园网边界部署硬件下一代防火墙，进行策略配置，实行访问控制，将所有不安全的或不符合安全规则的数据包屏蔽，杜绝越权访问，防止各类非法攻击行为。启用入侵防御功能，实现 2~7 层数据的安全检测和阻断防护，提供对内部攻击、外部攻击和误操作的实时监控，实时、主动拦截黑客攻击、蠕虫、僵尸网络、后门木马、DOS 等恶意流量。

（二）虚拟化体设备类。该类适用于不具备硬件部署环境、不具备人员基本维护能力的，或班级规模较小的，或教育资源和教育服务需求较低，不需要进行针对性安全防护的中小学学校（教育机构）。该类学校校园网出口不部署实体设备，而是在上级城域网中部署安全管理区，以流量监控的方式实现对每个校园网的安全监控和风险识别，统一汇总分析展示。

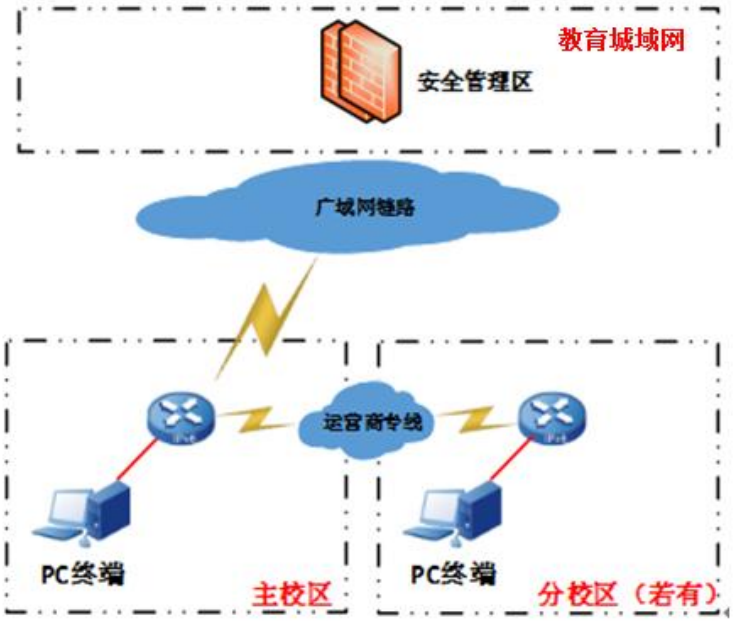

图 3-3 校园网虚拟化体设备安全防护示意图

在城域网内安全管理区为校园网配置安全防护设备，通过流量监控方式针对校园网进行统一监管，对存在的安全风险及时告警，并且可对于发现问题的学校流量采取控制措施，限制访问，防止各类非法攻击行为。

启用入侵防御功能，实现 2~7 层数据的安全检测和阻断防护，提供对内部攻击、外部攻击和误操作的实时监控，实时、主动拦截黑客攻击、蠕虫、僵尸网络、后门木马、DOS 等恶意流量；启用网络防病毒功能，实现进出网络边界数据的木马病毒、蠕虫病毒、宏病毒、脚本病毒等各种病毒的查杀，以及 HTTP、FTP、POP3、SMTP 协议的病毒的检测查杀。

3.3 安全策略设置

序号	设备名称	配置策略基线
1	互联网 出口防火墙	1.双机部署，避免单点故障。 2.禁止 any-any 策略。 3.根据应用 vlan 规划设置访问控制策略，对不同 vlan 之间网络流量进行逻辑隔离。 4.开启入侵防御、Web 应用防御策略，实现互联网边界安全防护。
2	上网行为管理	1.双机部署，避免单点故障。 2.设置互联网访问策略，禁止对非法网页、应用（涉黄、涉赌类网页及应用）进行访问。 3.设置流量控制策略： （1）对于 web 流媒体、下载工具、P2P 相关、视频 APP 如抖音及快手等的流量单 IP 不超过 10M； （2）将重要教学应用对应的 IP 地址段如同步课堂、IP 广播、安防视频等设置为高优先级，根据当地流量使用需要，保证此类 IP 地址每个的带宽

		达到 2M-4M； （3）将一般的 web 网页、邮件访问设备中优先级； （4）将 web 流媒体、下载工具、P2P 相关、视频 APP 如抖音及快手等流量设置为低优先级； 4.开启审计策略，对互联网访问行为进行审计，满足公安部 158 号令。
3	城域网出口防火墙	1.双机部署，避免单点故障。 2.禁止 any-any 策略。 3.根据应用 vlan 规划设置访问控制策略，对不同 vlan 之间网络流量进行逻辑隔离。 4.开启入侵防御、Web 应用防御策略，实现互联网边界安全防护。
4	安全日志审计	1.各级教育行政部门运营业务系统的物理主机、虚拟主机、操作系统、应 2.用软件等相关组件开启审计策略。 3.各级教育行政部门负责的网络设备如交换机、路由器等设备开启审计策略。 4.各级教育行政部门负责的网络安全设备如防火墙、上网行为管理、漏洞扫描、堡垒机等设备开启审计策略。 5.配置安全日志审计设备，实现对上述日志的同步对接。 设置访问白名单，在城域网内仅允许运维管理人员的 IP 地址登录。
5	漏洞扫描	1 梳理各级教育行政部门信息化资产，包括业务系统、网络设备、安全设备的信息，形成资产台账。 2.每季度定期对业务系统、网络设备、网络安全设备进行自我检测、评估。 3.对新上线的业务系统、应用进行网络安全监测与评估。 4.在重大活动、节假日前期，对业务系统、网络设备、网络安全设备进行自我检测、评估。 5.针对每次扫描后的漏洞进行处置，消除隐患。
6	运维管理设备（堡垒机）	设置运维管理策略，运维管理人员、外包人员、第三方服务商针对务系统、网络设备、网络安全设备的运维、调试工作，均需通过堡垒机接入。
7	态势感知系统及流量探针	1.探针镜像城域网核心交换的全部流量，并与态势感知系统对接，实现城域网内全流量的实时安全监测。 2.城域网态势感知与自治区态势感知平台对接，实现安全数据上报。 3.一旦发现安全脆弱性、安全事件，及时处置上报。 4.设置访问白名单，在城域网内仅允许运维管理人员的 IP 地址登录。
8	校园网网络边界安全设备	1.禁止 any-any 策略。 2.根据应用 vlan 规划设置访问控制策略，对不同 vlan 之间网络流量进行逻辑隔离。

第四章 商用密码安全应用

城域网的商用密码安全应用建设应按《广西教育网建设项目技术方案》的要求进行设计，预留项目建设预算，以及相关建设安排，待教育部和国家密码管理局的教育密码服务应用试点项目下达实施后再进行具体建设。

第五章 城域网接入骨干网

5.1 目标任务

城域网接入广西教育骨干网。通过连接广西教育网高校城市节点，实现市县城域网接入骨干网，连接广西教育数据中心、中国教育和科研计算机网（CERNET）、广西电子政务外网。

5.2 骨干网拓扑

广西教育骨干网由 100G 和 10G 光纤线路组成，连接 3 个核心节点、10 个高校城市节点，覆盖全区的 12 个设区市，实现双环贯通。

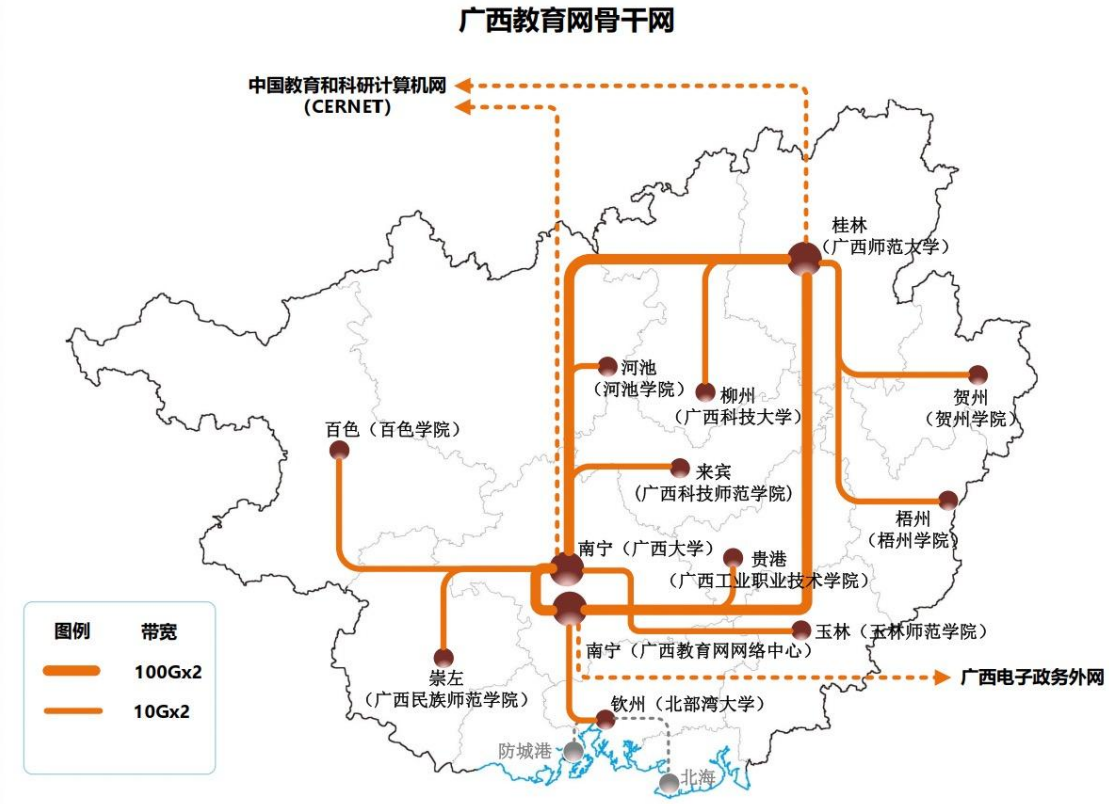

图 4-1 广西教育网骨干网示意图

5.3 城域网接入骨干网

各市县城域网通过裸纤或者传输数字链路连接所在设区市的广西教育网高校城市节点，原则上以千兆光接口上联高校城市节点设备。为了应对未来业务的扩展，骨干网节点路由器通过子接口与城域网设备连接，城域网接入设备和链路须支持子接口或者 trunk 口，支持 802.1Q 封装类型。

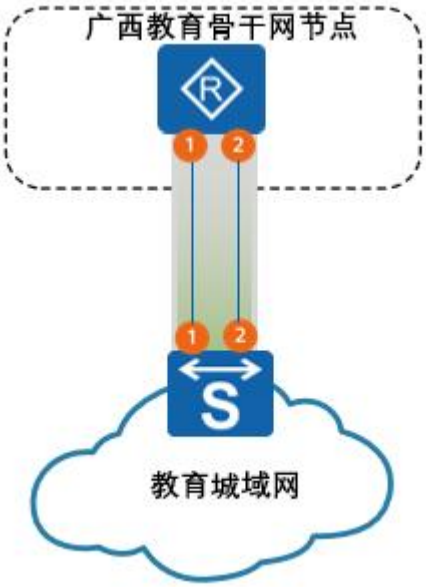

图 4-2 广西教育城域网接入骨干网示意图

5.4 接入路由配置

5.4.1 IP 地址分配

由广西教育网网络中心统一分配 IP 地址，用于广西教育骨干网与市县城域网的互联。请于申请接入广西教育骨干网时，与广西教育网网络中心联系实施建设的具体事宜。

5.4.2 城域网端的路由配置

5.4.2.1 广西教育网 IPv4 路由配置

在市县城域网的出口路由设备上配置路由，将以下列表中的 IPv4 网络路由指向广西教育网。

备注：以下地址前缀指向广西教育网			
序号	网段/前缀长度	网段	掩码
1	1.51.0.0/16	1.51.0.0	255.255.0.0
2	1.184.0.0/15	1.184.0.0	255.254.0.0
3	42.244.0.0/14	42.244.0.0	255.252.0.0
4	49.52.0.0/14	49.52.0.0	255.252.0.0
5	49.120.0.0/14	49.120.0.0	255.252.0.0
6	49.140.0.0/15	49.140.0.0	255.254.0.0
7	49.208.0.0/15	49.208.0.0	255.254.0.0
8	49.232.0.0/14	49.232.0.0	255.252.0.0
9	58.116.0.0/14	58.116.0.0	255.252.0.0
10	58.128.0.0/13	58.128.0.0	255.248.0.0
11	58.154.0.0/15	58.154.0.0	255.254.0.0
12	58.192.0.0/12	58.192.0.0	255.240.0.0
13	59.64.0.0/12	59.64.0.0	255.240.0.0
14	101.4.0.0/14	101.4.0.0	255.252.0.0
15	101.76.0.0/15	101.76.0.0	255.254.0.0
16	110.64.0.0/15	110.64.0.0	255.254.0.0
17	111.114.0.0/15	111.114.0.0	255.254.0.0
18	111.116.0.0/15	111.116.0.0	255.254.0.0
19	111.186.0.0/15	111.186.0.0	255.254.0.0
20	113.54.0.0/15	113.54.0.0	255.254.0.0
21	114.212.0.0/15	114.212.0.0	255.254.0.0
22	114.214.0.0/16	114.214.0.0	255.255.0.0
23	115.24.0.0/14	115.24.0.0	255.252.0.0
24	115.154.0.0/15	115.154.0.0	255.254.0.0
25	115.156.0.0/15	115.156.0.0	255.254.0.0
26	115.158.0.0/16	115.158.0.0	255.255.0.0
27	116.13.0.0/16	116.13.0.0	255.255.0.0
28	116.56.0.0/15	116.56.0.0	255.254.0.0
29	117.106.0.0/15	117.106.0.0	255.254.0.0
30	117.112.0.0/13	117.112.0.0	255.248.0.0
31	118.202.0.0/15	118.202.0.0	255.254.0.0
32	118.228.0.0/15	118.228.0.0	255.254.0.0
33	118.230.0.0/16	118.230.0.0	255.255.0.0
34	120.94.0.0/15	120.94.0.0	255.254.0.0
35	121.48.0.0/15	121.48.0.0	255.254.0.0
36	121.52.160.0/19	121.52.160.0	255.255.224.0
37	121.192.0.0/14	121.192.0.0	255.252.0.0
38	121.248.0.0/14	121.248.0.0	255.252.0.0
39	122.204.0.0/14	122.204.0.0	255.252.0.0
40	125.216.0.0/13	125.216.0.0	255.248.0.0
41	162.105.0.0/16	162.105.0.0	255.255.0.0
42	166.111.0.0/16	166.111.0.0	255.255.0.0
43	171.84.0.0/14	171.84.0.0	255.252.0.0
44	175.185.0.0/16	175.185.0.0	255.255.0.0
45	175.186.0.0/15	175.186.0.0	255.254.0.0
46	180.84.0.0/15	180.84.0.0	255.254.0.0

47	180.201.0.0/16	180.201.0.0	255.255.0.0
48	180.208.0.0/15	180.208.0.0	255.254.0.0
49	183.168.0.0/15	183.168.0.0	255.254.0.0
50	183.170.0.0/16	183.170.0.0	255.255.0.0
51	183.172.0.0/14	183.172.0.0	255.252.0.0
52	202.4.128.0/19	202.4.128.0	255.255.224.0
53	202.38.64.0/18	202.38.64.0	255.255.192.0
54	202.38.140.0/23	202.38.140.0	255.255.254.0
55	202.38.184.0/21	202.38.184.0	255.255.248.0
56	202.38.192.0/18	202.38.192.0	255.255.192.0
57	202.112.0.0/13	202.112.0.0	255.248.0.0
58	202.120.0.0/15	202.120.0.0	255.254.0.0
59	202.127.216.0/21	202.127.216.0	255.255.248.0
60	202.127.224.0/19	202.127.224.0	255.255.224.0
61	202.179.240.0/20	202.179.240.0	255.255.240.0
62	202.192.0.0/12	202.192.0.0	255.240.0.0
63	203.91.120.0/21	203.91.120.0	255.255.248.0
64	210.25.0.0/17	210.25.0.0	255.255.128.0
65	210.25.128.0/18	210.25.128.0	255.255.192.0
66	210.26.0.0/15	210.26.0.0	255.254.0.0
67	210.28.0.0/14	210.28.0.0	255.252.0.0
68	210.32.0.0/12	210.32.0.0	255.240.0.0
69	211.64.0.0/13	211.64.0.0	255.248.0.0
70	211.80.0.0/13	211.80.0.0	255.248.0.0
71	211.153.0.0/16	211.153.0.0	255.255.0.0
72	218.192.0.0/13	218.192.0.0	255.248.0.0
73	219.216.0.0/13	219.216.0.0	255.248.0.0
74	219.224.0.0/13	219.224.0.0	255.248.0.0
75	219.242.0.0/15	219.242.0.0	255.254.0.0
76	219.244.0.0/14	219.244.0.0	255.252.0.0
77	222.16.0.0/12	222.16.0.0	255.240.0.0
78	222.192.0.0/12	222.192.0.0	255.240.0.0
79	222.249.0.0/16	222.249.0.0	255.255.0.0
80	223.2.0.0/15	223.2.0.0	255.254.0.0
81	223.128.0.0/15	223.128.0.0	255.254.0.0

5.4.2.2 广西教育网 IPv6 路由配置

在市县城域网的出口路由设备上配置路由，并将以下列表中的 IPv6 默认路由指向广西教育网。

备注：将 IPv6 默认路由指向广西教育网	
网段/前缀长度	掩码
::/0	0

5.4.2.3 广西教育网内网路由配置

在市县城域网的出口路由设备上配置路由，并将以下列表中的路由指向广西教育网。

备注：将以下路由指向广西教育网	
网段/前缀长度	掩码
100.64.0.0/12	255.240.0.0

5.4.2.4 广西电子政务外网路由配置

在市县城域网的出口路由设备上配置路由，并将以下列表中的广西电子政务外网的路由指向广西教育网。

备注：将广西电子政务外网的业务地址路由指向广西教育网	
网段/前缀长度	掩码
59.211.0.0/16	255.255.0.0