ICS 35.240.99
CCS L 67

T/CAET

中 国 教 育 技 术 协 会 团 体 标 准

T/CAET XXXX—2024

校园网网络设备安全技术要求

Security technology requirements for campus network devices

（征求意见稿）

（2025.3.20）

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

中国教育技术协会　　发 布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

本部分依据 GB/T 1.1—2020 给出的规则起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本文件由中国教育技术协会提出并归口。

本文件起草单位：中国教育技术协会网络安全专业委员会、浙江大学、清华大学、北京大学、东南大学、厦门大学、北京师范大学、西湖大学、河海大学、长江大学、教育信创实验室、华为技术有限公司、新华三集团、锐捷网络股份有限公司、深信服科技股份有限公司、绿盟科技集团股份有限公司、迈普通信技术股份有限公司、苏州盛科通信股份有限公司、创耀（苏州）通信科技股份有限公司、联软科技股份有限公司、中国人民大学附属中学、惠州市第八中学、东莞市松山湖第三小学、松山湖北区学校、乌鲁木齐市教育局。

本文件主要起草人：袁书宏、廖运华、郑海山、云霞、单康康、秦神祖、罗明、管军、余华平、田小萍、胡轶宁、万晓兰、陈育锋、王洪军、王俊杰、郑嘉俊、李晓杰、郑宇、赖昱全、欧劲、姚湘斌、阿布都瓦依提。

校园网网络设备安全技术要求

1 范围

本文件给出了校园网网络设备的自身安全要求、安全功能要求以及安全保障要求，网络设备的范围为交换机、路由器、无线局域网产品、防火墙、抗拒绝服务攻击产品、入侵防御系统。

本文件适用于校园网网络设备研发、生产、服务、检测、采购。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB 40050—2021 网络关键设备安全通用要求

GB 42250—2022 信息安全技术 网络安全专用产品安全技术要求

GB/T 18018—2019 信息安全技术 路由器安全技术要求

GB/T 20281—2020 信息安全技术 防火墙安全技术要求和测试评价方法

GB/T 21050—2019 信息安全技术 网络交换机安全技术要求

GB/T 25069—2010 信息安全技术 术语

GB/T 32907—2016 信息安全技术 SM4分组密码算法

GB/T 33565—2024 网络安全技术 无线局域网接入系统安全技术要求

GB/T 36342—2018 智慧校园总体框架

GM/T 0002—2012 SM4分组密码算法

GM/T 0004—2012 SM3密码杂凑算法

3 术语和定义

GB/T 20281—2020、GB/T 25069—2010界定的以及下列术语和定义适用于本文件。

3.1

绿色上网 green internet

用先进技术，如DNS过滤、URL过滤、深度包检测等，自动识别和阻止不良网站，确保学生和教师在校园网络中上网时的安全与健康。

3.2

防挖矿 anti-mining

通过技术手段防止未经用户同意或用户不知情的情况下使用该用户设备挖掘加密货币，并以隐蔽或不易察觉的方式使用其设备计算资源的行为。

4 缩略语

下列缩略语适用于本标准。

AC：接入控制器（Access Controller）

AP：接入点（Access Point）

BRAS：宽带远程接入服务器（Broadband Remote Access Server）

CERNET：中国教育和科研计算机网（China Education and Research Network）

CPU：中央处理器（Central Processing Unit）

C&C：命令与控制攻击（Command and Control）

FPGA：现场可编程门阵列（Field-Programmable Gate Array）

FTP：文件传输协议（File Transfer Protocol）

HTTP：超文本传输协议（Hyper Text Transfer Protocol）
ID：身份（Identification）
IP：网际协议（Internet Protocol）
IPoE：以太网承载IP协议（IP over Ethernet）
IPSec：互联网协议安全（Internet Protocol Security）
MACSec：媒体访问控制安全（Media Access Control Security）
MD5：消息摘要算法第5版（Message Digest Algorithm 5）
NP：网络处理器（Network Processor）
PPPoE：以太网上的点对点协议（Point-to-Point Protocol Over Ethernet）
RC4：Rivest加密算法4（Rivest Cipher 4）
SHA-1：安全散列算法1（Secure Hash Algorithm 1）
SNMPv1：简单网络管理协议版本1（Simple Network Management Protocol Version 1）
SNMPv2：简单网络管理协议版本2（Simple Network Management Protocol Version 2）
SNMPv3：简单网络管理协议版本3（Simple Network Management Protocol Version 3）
SSHv1：安全外壳协议1（Secure Shell Version 1）
SSHv2：安全外壳协议2（Secure Shell Version 2）
SZTP：安全零接触开局（Secure Zero Touch Provisioning）
TLS1.0：传输层安全1.0（Transport Layer Security 1.0）
TLS1.1：传输层安全1.1（Transport Layer Security 1.1）
VPN：虚拟专用网（Virtual Private Network）
VLAN：虚拟局域网（Virtual Local Area Network）
VRRP：虚拟路由器冗余协议（Virtual Router Redundancy Protocol）
URL：统一资源定位符（Uniform Resource Locator）
USB：通用串行总线（Universal Serial Bus）
WAPI：无线局域网鉴权与隐私保护（Wireless Authentication and Privacy Infrastructure）
WPA2：Wi-Fi保护接入2（Wi-Fi Protected Access 2）
WPA3：Wi-Fi保护接入3（Wi-Fi Protected Access 3）
XFF：转发来源（X-Forwarded-For）

5 概述

5.1 校园网网络架构及设备

校园网网络逻辑架构示意图如图1所示，一般由接入区、核心交换区、分校互联区、数据中心区以及互联网出口区等构成。

a) 接入区，负责教学区（如办公室、教室、实验室、图书馆、会议室、报告厅等）、生活区（入食堂、宿舍、体育馆等）和物联区（如门禁、闸机、水表、电表等）的终端设备接入，主要使用交换机、无线局域网 AP 等；
b) 核心交换区，负责校园网络各功能区的数据交换，主要使用交换机、无线局域网 AC、BRAS 路由器、态势感知探针，BRAS 路由器可部署在互联网出口区；
c) 分校互联区，负责分校区接入，主要使用防火墙、交换机、态势感知探针等；
d) 数据中心区，包括安全管理区和业务应用区，主要使用交换机、防火墙、抗拒绝服务攻击产品、入侵防御系统、态势感知、数据库审计、安全日志审计、漏洞扫描等；
e) 互联网出口区，负责通过 CERNET 和运营商网络实现互联网连接，主要使用防火墙、抗拒绝服务攻击产品、路由器、入侵防御系统等。

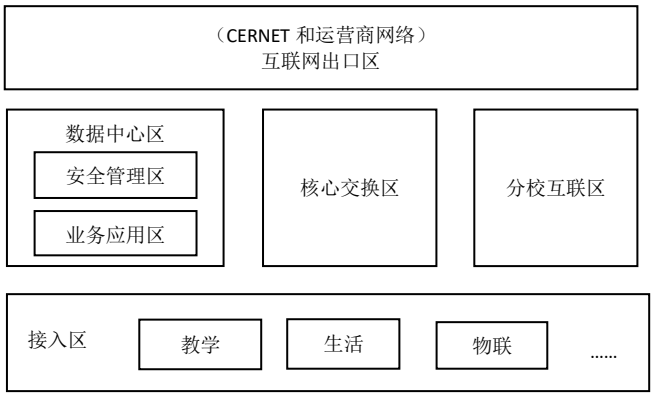

图1　校园网网络逻辑架构示意图

本标准旨在对校园网络中承担网络信息传输的网络设备进行安全技术要求定义，包括路由器、交换机、无线局域网产品、防火墙、抗拒绝服务攻击产品、入侵防御系统。

5.2　网络设备安全概述

5.2.1　概述

校园信息系统安全体系包括物理安全、网络安全、主机安全、应用安全和数据安全（见GB/T 36342—2018 5.6.2）。网络设备是校园网络基础设施重要组成部分，网络设备安全是校园网络安全的基础。

网络设备安全通常由网络设备自身安全、安全功能和安全保障构成，包括网络设备的软件和硬件，如图2所示。基于校园网络逻辑架构以及信息流，校园网络设备通常提供的安全功能包括终端接入安全、链路传输安全、网络出口安全等服务。

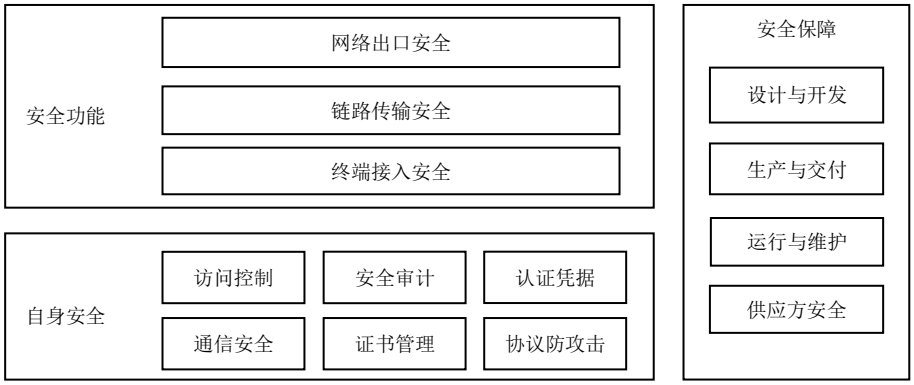

图2　网络设备安全框架

5.2.2　自身安全

自身安全是指网络设备自身具备安全纵深防御能力和安全事件可视可管能力，为网络提供安全稳定网络服务，包括访问控制、通信安全、安全审计、认证凭据、证书管理等。

5.2.3　安全功能

5.2.3.1　终端接入安全

终端接入安全是指负责终端接入的网络设备具备终端认证鉴权、终端识别可视、接入防私接、访问控制与用户管理能力等安全能力，确保终端接入安全。

5.2.3.2　链路传输安全

链路传输安全是指网络设备无线链路（终端到无线局域网AP）和有线链路（无线局域网AP到无线局域网AC、接入交换机到核心交换机）具备端到端链路安全保障。无线局域网AP支持终端WPA2\WPA3\WAPI

链路传输安全；有线链路支持端到端逐跳部署MACSec保护，采用符合GB/T 32907（GM/T 002）的加密算法。

5.2.3.3 网络出口安全

网络出口安全是指校园网络南北向出口网络设备和网络内各分区东西向网络设备具备安全识别和防御能力，包括具备通信加密、抗拒绝服务攻击、身份认证鉴权、绿色上网、防挖矿等能力。

5.2.4 安全保障

安全保障是指在网络设备的设计与开发、生产与交付、运行与维护，以及关键部件供应方等方面符合相关的安全要求，以保障网络设备安全。

6 自身安全要求

6.1 访问控制

网络设备支持以下访问控制要求：

a) 所有在设备外部可见的能对系统进行管理的物理接口（如串口、USB 接口、管理网口等）应具备接入认证机制，并默认启用；
b) 所有在设备外部可见的能对系统进行管理的物理接口（如串口、USB 接口、管理网口等）应支持关闭；
c) 应支持登录用户会话空闲超时锁定或自动退出等安全策略，支持管理员身份鉴别尝试次数限制；
d) 当出现鉴别失败时，设备应提供无差别反馈，避免提示“用户名错误”、“口令错误”等具体信息；
e) 宜支持安全零配置部署 SZTP 功能。

6.2 通信安全

6.2.1 默认安全

网络设备支持以下默认安全要求：

a) 应默认关闭不安全的算法，例如 RC4、DES、3DES、AES-CBC、MD5、SHA-1 等；
b) 当配置不安全密码算法时应有安全提示或告警；
c) 应默认关闭不安全协议的网络管理功，例如 Telnet、SSHv1、SNMPv1、SNMPv2、HTTP、FTP、TLS1.0、TLS1.1 等；
d) 当配置不安全协议时应有安全提示或告警。

6.2.2 管理通信协议安全

网络设备支持以下管理通信协议安全要求：

a) 在使用 Web 管理时，应支持并默认启用 HTTPS；
b) 在使用 SSH 管理时，应支持并默认启用 SSHv2；
c) 在使用 SNMP 管理时，应支持并默认启用 SNMPv3；
d) 应支持使用上述至少一种非明文数据传输协议对设备进行管理；
e) 应支持管理平面隔离，阻断从互联网或接入设备发起的请求，应支持的技术包括：
    1) 管理协议服务端进程支持监听指定 IP；
    2) 管理协议支持从限定的 VPN 接入；
    3) 管理协议支持从限定的 VLAN 接入；
    4) 管理协议支持 ACL。

6.3 安全审计

网络设备支持以下安全审计要求：

a) 应支持安全日志记录功能，对用户关键操作，如增加和删除账户、修改鉴别信息、修改关键配置、用户登录和注销、用户权限修改、重启和关闭设备、软件更新等行为进行记录；
b) 安全日志审计记录中应记录必要的日志要素，至少包括事件发生日期和时间、主体（如登录 账号等）、事件描述（如类型、操作结果等）、源 IP 地址（采用远程管理方式时）等，为查阅和分析提供足够的信息；
c) 不应在日志中明文或弱加密记录敏感数据，如用户口令、SNMP 团体名、Web 会话 ID 以及私钥等；
d) 应支持对安全日志进行安全防护，保护审计数据的完整性，防止被未经授权的查看、输出、修改或删除；
e) 安全日志宜单独存储，管理员不应具备删除和修改日志的权限；
f) 宜支持对非法用户登录、非授权行为操作等攻击场景记录审计日志并上报态势感知平台。

6.4 认证凭据

网络设备支持以下认证凭据要求：
a) 使用口令鉴别方式时，应具备口令防暴力破解机制；
b) 使用口令鉴别方式时，应支持口令复杂度检查功能，口令长度不少于 8 位、且至少包含 2 种不同类型字符；
c) 使用口令鉴别方式时，不应明文回显用户输入的口令信息；
d) 使用口令鉴别方式时，应支持首次管理设备时强制修改默认口令或设置口令，或支持随机的初始口令；
e) 使用口令鉴别方式时，应支持设置口令生存周期；
f) 认证凭据（如口令和私钥等）不应明文存储在系统介质中，应加密保护并提供访问控制；
g) 不应在日志、调试信息、错误提示中明文显示认证凭据；
h) 设备如存在默认口令，应在产品资料中公开；
i) 宜支持弱口令字典功能，避免用户使用弱口令字典中的任何口令。

6.5 证书管理

网络设备支持以下数字证书管理要求：
a) 应支持和网管配合实现对数字证书的集中化、可视化的全生命周期管理；
b) 在数字证书即将过期前应支持发送安全提示或者告警，提示运维人员更新证书；
c) 宜支持对接证书管理系统，实现数字证书的自动申请和更新功能。

6.6 协议防攻击

网络设备支持以下协议防攻击要求：
a) 应支持抗大流量协议报文攻击，对大流量应采用限速、丢弃或优先级调度等策略，防止设备受攻击，如 BGP 等路由协议报文流量攻击；
b) 应支持抗畸形报文能力，进行报文的合法性校验，对于目标是本设备的畸形报文应丢弃，畸形报文包括但不限于：
   1) 超长包，例如包长大于 65535 字节；
   2) 超短包；
   3) 链路层错误包；
   4) 网络层错误包；
   5) 上层协议错误包；
   6) 不可识别的扩展头字段等；
   7) LAND 攻击报文；
   8) TCP 标志位非法攻击报文；
   9) ARP REPLY 攻击报文；
   10) 非法 ND 报文。

7 安全功能要求

7.1 总体要求

校园网网络设备应符合教育行业信息系统安全等级要求，并应具备满足校园网网络各功能区对网络设备的安全功能要求。

7.2 交换机安全要求

7.2.1 接入区安全

7.2.1.1 终端接入安全

交换机支持以下终端接入认证鉴权安全要求，实现访问控制和用户管理，满足校园网教学区、生活区和物联区终端接入安全：

a) 应支持 MAC 地址认证；
b) 应支持 802.1X 认证；
c) 应支持 Portal 认证；
d) 应支持对风险终端进行阻断，防止非法非合规的终端接入；
e) 应支持对物联终端进行被动指纹识别和主动探测扫描，实现物联终端识别，保障台账清晰；
f) 应支持私接行为检测。

7.2.1.2 链路传输安全

交换机支持以下链路传输安全要求，实现安全传输，满足校园网接入区安全：

a) 应支持 MACSec，实现校园网从无线局域网 AP 到核心交换机的链路逐跳 MACSec 加密部署；
b) MACSec 宜支持 GB/T 32907—2016（GM/T 002—2012），或国家密码管理主管部门认可的密码算法。

7.2.2 核心交换区安全

7.2.2.1 终端接入安全

交换机支持以下安全要求，满足核心交换区安全：

a) 应支持用户准入认证及基于 IP 地址的身份溯源，认证包括 MAC 地址认证、802.1X 认证和 Portal 认证；
b) 宜支持策略联动和业务随行，实现哑终端接入、移动设备接入和集中式 IP 地址分配等多种接入方式。

7.2.2.2 链路传输安全

交换机支持以下链路传输安全要求，实现安全可靠传输，满足校园网核心交换区安全：

a) 应支持 MACSec，实现校园网从无线局域网 AP 到核心交换机的链路逐跳 MACSec 加密部署；
b) 应支持堆叠或 M-LAG 跨设备的链路聚合，实现设备间高可靠；
c) 应支持 CPU 保护机制，包括协议报文识别过滤、协议报文限速和 CPU 端口队列限速，防止拒绝服务攻击、非法接入以及控制平面过载等安全威胁；
d) MACSec 宜支持 GB/T 32907—2016（GM/T 002—2012），或国家密码管理主管部门认可的密码算法。

7.3 路由器安全要求

7.3.1 互联网出口区安全

路由器支持以下网络出口安全要求，满足互联网出口区安全：

a) IPSec 应支持 GB/T 32905—2016（GM/T004—2012）、GB/T 32907—2016（GM/T 002—2012），或国家密码管理主管部门认可的密码算法，实现传输通信安全；
b) 路由协议应支持 GB/T 32905—2016（GM/T 004—2012）或国家密码管理主管部门认可的密码算法认证，保障路由安全；
c) 应支持 VRRP 网关热备协议，实现互联网出口路由器高可靠性。

7.3.2 核心交换区安全

路由器作为用户接入认证设备时，支持以下安全要求，满足校园网终端接入安全：

a) 应支持基于 MAC 哈希的 PPPoE 和 IPoE Session 负载分担，保障业务稳定性；
b) 应支持用户准入认证及基于 IP 地址的身份溯源，认证包括 MAC 地址认证、802.1X 认证和 Portal 认证；
c) 应支持 CPU 保护机制，包括协议报文识别过滤、协议报文限速和 CPU 端口队列限速，防止拒绝服务攻击、非法接入以及控制平面过载等安全威胁；
d) 应支持异地容灾，距离不受限，保障业务高可靠。

7.4 无线局域网产品安全要求

7.4.1 终端接入安全

无线局域网产品支持以下安全要求，满足终端接入安全：

a) 无线局域网 AC 应支持终端认证鉴权，实现访问控制和用户管理；
b) 无线局域网 AP 应支持客户自定义证书，设备证书可替换；
c) 无线局域网 AP 宜支持接入终端可视；
d) 无线局域网 AP 宜支持通过物理层防护进行空口防侦听。

7.4.2 链路传输安全

无线局域网产品支持以下安全要求，满足链路传输安全：

a) 无线局域网 AP 应支持 WPA2、WPA3、WAPI 安全传输协议，实现 AP 和终端的链路安全；
b) 无线局域网 AP 宜支持 MACSec，保障有线链路端到端逐跳部署 MACSec 保护；
c) 无线局域网 AC 宜支持冗余高可靠。

7.5 防火墙安全要求

7.5.1 互联网出口区安全

防火墙支持以下网络出口安全要求，满足校园网互联网绿色上网安全：

a) 应支持已知 URL 过滤和未知恶意 URL 动态识别；
b) 应支持应用精准识别及封堵；
c) 应支持恶意文件识别与阻断及日志记录；
d) 应支持翻墙 VPN 识别及阻断；
e) 应支持 IPv4 和 IPv6 访问控制；
f) 应支持 NAT；
g) 应支持通过 IPSec 进行多校区安全互联；
h) IPSec 应支持 GB/T 32905—2016（GM/T004—2012）、GB/T 32907—2016（GM/T 002—2012），或国家密码管理主管部门认可的密码算法；
i) 路由协议应支持 GB/T 32905—2016（GM/T 004—2012）或国家密码管理主管部门认可的密码算法。

7.5.2 数据中心区安全

7.5.2.1 安全管理区安全

防火墙支持以下网络出口安全要求，满足校园网数据中心安全管理区安全：

a) 应支持恶意文件识别与阻断及日志记录；
b) 应支持 IPv4 和 IPv6 访问控制。

7.5.2.2 业务应用区安全

防火墙支持以下网络出口安全要求，满足校园网数据中心业务应用区安全：

a) 应支持针对已知和未知勒索病毒的检测与实时阻断，具备防勒索能力；
b) 应支持针对已知和未知挖矿病毒的检测与实时阻断，具备防挖矿能力；

c） 应支持对传输的文件和内容进行识别过滤，具备数据防泄露能力；
d） 应支持 IPv4 和 IPv6 访问控制。

7.6 入侵防御系统安全要求

入侵防御系统支持以下网络出口安全要求，满足校园网数据中心区安全和互联网出口区安全：
a） 应支持 C&C、挖矿域名、勒索域名、钓鱼域名、Sinkhole 域名、恶意站点、Compromised 域名、DGA 域名、新 NOD 域名等过滤；
b） 应支持 XFF 识别能力；
c） 应支持 tar、zip、gzip、tgz 压缩检测；
d） 应支持应用识别能力；
e） 应支持攻击取证、全流抓包、攻击片段取证；
f） 应支持关联签名检测。

7.7 抗拒绝服务攻击产品安全要求

抗拒绝服务攻击产品支持以下网络出口安全要求，满足校园网互联网出口区安全：
a） 应支持流量基线学习；
b） 应支持异常流量清洗；
c） 应支持定制差异化防护策略；
d） 应支持防御策略调优；
e） 应支持 HTTPS 加密攻击不解密防御；
f） 应支持 IPv4 和 IPv6 防护。

8 安全保障要求

8.1 总体要求

网络设备的安全保障要求应符合相关产品国家标准定义的安全保障要求，包括GB 40050—2021、GB 42250—2022、GB/T 21050—2019、GB/T 18018—2019、GB/T 33565—2024。对网络设备的关键软件和硬件供应方提出相关安全要求，提升网络设备安全保障。

8.2 供应方要求

8.2.1 软件供应安全

网络设备的操作系统、整机软件、软件完整性和漏洞管理支持以下要求：
a） 应具备网络设备整机软件知识产权；
b） 应具备漏洞和开源软件管理机制；
c） 软件完整性保护支持以下要求：
  1） 网络设备整机供应商应随设备软件版本发布数字签名，并提供签名验证工具，保证其完整性和真实性，确保软件不被篡改；
  2） 在设备软件更新时应校验软件的数字签名，且校验不可关闭，保证其完整性和真实性，确保软件不被篡改；
  3） 在设备启动时应校验软件的数字签名，且校验不可关闭，保证其完整性和真实性，确保软件不被篡改。
d） 漏洞防利用应支持以下要求：
  1） 设备软件和补丁不存在病毒、木马等恶意程序；
  2） 设备不存在已知漏洞，或对已知漏洞具备补救措施。

8.2.2 硬件供应安全

网络设备核心芯片通常指路由器、交换机、无线局域网产品等网络设备中负责网络报文处理器的转发/交换芯片、Wi-Fi基带芯片，以及负责网络设备系统控制的CPU，它们直接影响设备的性能和安全性，各网络设备的核心芯片如表1所示。

注1：转发/交换芯片，即网络设备中负责报文转发交换处理的IC芯片和框式网络设备交换网板交换IC芯片的统称，通常包括NP、FPGA、ASIC。

注2：Wi-Fi基带芯片，即用于实现无线局域网通信功能的IC芯片，主要负责处理和传输符合802.11系列标准的无线信号，实现设备间的无线数据通信。

表1　网络设备核心芯片

核心芯片	路由器	交换机	无线局域网产品		网络安全产品		
			无线局域网AC	无线局域网AP	防火墙	抗拒绝服务攻击产品	入侵防御系统
CPU	√	√	√	√	√	√	√
转发/交换芯片	√	√	√	/	/	/	/
Wi-Fi基带芯片	/	/	/	√	/	/	/
FPGA	√	√	√	/	√	√	√
注1：√表示是相关网络设备的核心芯片，/表示不涉及。 注2：上述核心芯片可能集成在一个SoC芯片，也可能是独立芯片。 注3：如FPGA未作为转发交换或协处理器功能使用，或整机未使用FPGA芯片，则不做要求。							

网络设备及其核心芯片供应方安全支持以下要求：

a)　网络设备整机供应商应提供网络设备核心芯片品牌和型号；

b)　核心芯片供应商不应存在因政治、外交、贸易限制等因素中断产品供应及必要的技术支持服务的风险；

c)　核心芯片供应商不应存在对中国境内注册厂商或用户停止供应核心芯片、技术支持的先例；

d)　网络设备整机供应商使用非自研核心芯片时，宜具备多元化供应能力，保障供应持续稳定。

参 考 文 献

[1] SSIIA/T 001—2024 信息技术应用创新 数据通信网络设备技术要求
[2] GB/T 36630.1—2018 信息安全技术 信息技术产品安全可控评价指标 第1部分：总则
[3] GB/T 39204—2022 信息安全技术 关键信息基础设施安全保护要求
[4] 高等学校数字校园建设规范（试行）
[5] 教育行业信息系统安全等级保护定级工作指南（试行）