ICS 35.030
CCS L 80

T/CSAC

团　　体　　标　　准

T/CSAC 026—2025

网络设备安全分级技术要求

Technical Requirements for Security Classification of Network Devices

2025－12－16 发布　　2026－01－16 实施

中国网络空间安全协会　　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。

请注意本文本的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由中国网络空间安全协会提出并归口。

本文件起草单位：武汉网络安全技术有限公司、武汉大学网络安全学院、华为技术有限公司、湖北天融信网络安全技术有限公司、国家税务总局湖北省税务局、北京航空航天大学、中移(杭州)信息技术有限公司、上海交通大学、亚信科技（成都）有限公司、北京神州绿盟科技有限公司、深信服科技股份有限公司、武汉安域信息安全技术有限公司、江苏基久网络科技有限公司、杭州默安科技有限公司。

本文件主要起草人：丁勇、高阳、胡俊理、赵波、安高峰、左世涛、周宁、王健、李诗洋、钱锋、李翔、孟楠、王勇、栾俊超、秦神祖、蔡倩楠、秦宏、关振宇、杜皓华、刘懿中、吴贤望、颜星晨、刘洞宾、张睿、张智南、杨柳、黄博、单建军、程进。

引　言

随着数字化转型进程加快，网络设备作为信息化基础设施的核心组件，其安全性直接影响整个网络体系的稳定运行。网络设备容易遭受到来自网络和其他方面的威胁，网络设备被攻击后，网络的性能和正常运行会受到很大的影响。

本文件针对网络设备提出安全分级技术要求，能够针对不同应用场景的网络设备满足相应的安全要求，显著提升整体网络安全防御能力。

网络设备安全分级技术要求

1 范围

本文件提出了网络设备的安全功能和安全保障的分级要求。

本文件适用于指导网络设备生产企业进行产品设计、开发和测试，设备用户选型与第三方评测也可参照使用。

注：本文件所指网络设备包含路由器设备、数据中心交换机设备、园区交换机设备、无线接入AP设备、无线接入AC设备、防火墙设备、抗拒绝服务攻击设备。

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/T 25069 信息安全技术 术语

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

GM/T 0005—2021 随机性检测规范

3 术语和定义

GB40050—2021、GB/T 25069 界定的以及下列术语和定义适用于本文件。

3.1

网络设备 network devices

具备连接网络功能的实体（不包含消费类终端产品）。

3.2

防护有效性 protection effectiveness

网络安全设备在模拟真实网络威胁场景下，准确检测并阻断各类攻击，保护网络系统和数据免受侵害的能力。其衡量指标通常包括但不限于攻击检测准确率、阻断率、误报率、响应时间等。

4 缩略语

下列缩略语适用于本文件。

AC：接入控制点（Access Controller）

AP：访问接入点（Access Point）

HTTPS：超文本传输安全协议（Hypertext Transfer Protocol Secure）

IP：互联网协议（Internet Protocol）

JTAG：联合测试工作组(Joint Test Action Group)

NTP：网络时间协议（Network Time Protocol）

SELinux：安全增强式Linux（Security-Enhance Linux）

SID：段ID(Segment ID)

SRv6：基于IPv6转发平面的段路由（Segment Routing IPv6）

SSH：安全外壳（Secure Shell）

SZTP：安全零接触配置（Secure Zero Touch Provisioning）

TLS：传输层安全（Transport Layer Security）

UDP：用户数据包协议（User Datagram Protocol）

URL：统一资源定位符（Uniform Resource Locator）

WAPI：无线局域网鉴权与隐私保护（Wireless Authentication and Privacy Infrastructure）
WPA：Wi-Fi保护接入（Wi-Fi Protected Access）

5 概述

网络设备安全技术要求包含安全功能要求和安全保障要求，安全功能要求分为安全功能通用要求和具体网络设备类型的安全功能扩展要求。

网络设备安全技术要求分为三级，分级标准参考附录A。第一级安全要求是基础要求，第二级安全要求项是在满足第一级安全要求基础上增加的安全要求，第三级安全要求项是在满足第二级安全要求基础上增加的安全要求。

6 第一级安全要求

6.1 安全功能要求

路由器设备、数据中心交换机设备、园区交换机设备、无线接入AP设备、无线接入AC设备安全功能要求应符合GB 40050—2021中第5章的规定。

防火墙设备、抗拒绝服务攻击产品设备安全功能要求应符合GB 42250—2022中第4章和第5章的规定。

6.2 安全保障要求

路由器设备、数据中心交换机设备、园区交换机设备、无线接入AP设备、无线接入AC设备安全保障要求应符合GB 40050—2021中第6章的规定。

防火墙设备、抗拒绝服务攻击产品设备安全保障要求应符合GB 42250—2022中第6章的规定。

7 第二级安全要求

7.1 安全功能要求

7.1.1 安全功能通用要求

7.1.1.1 默认安全

本项要求包括：

a) 不应预留任何的未公开帐号，所有帐号都应被系统管理，如果存在默认帐号，应在产品资料中明示；
b) 不应存在绕过正常认证机制直接进入系统的隐秘通道，如：组合键、鼠标特殊敲击、连接特定接口，使用特定客户端、使用特殊 URL 等；
c) 应默认关闭 Telnet、FTP、SNMP v1/v2c、HTTP 等使用明文传输协议的网络管理功能；
d) 应默认支持安全的密码算法。

7.1.1.2 软件完整性

应支持启动时通过数字签名对启动软件的完整性和真实性进行校验。

7.1.1.3 访问控制

本项要求包括：

a) 新建账号默认应不授予任何权限或者只授予最小权限；
b) 长时间不登录的帐号应禁用或禁止登录；
c) 所有能对系统进行远程管理的人机接口以及跨信任网络的机机接口应支持安全的接入认证机制并缺省启用，应在关闭认证机制时设置风险提示；
d) 应支持管理面、控制面和用户面间的安全隔离功能；
e) 应禁用硬件调试接口(如 JTAG)的接入访问。

7.1.1.4 身份认证

本项要求包括：

a) 对所有能接入设备的认证凭据应支持修改；
b) 用户口令应支持配置长度为 10 个字符，包含数字，字母或特殊字符至少两种组合；
c) 使用数字证书实现身份认证时应验证对端证书的有效性，包括有效期、信任链、吊销状态等；
d) 管理员修改自己口令时应验证旧口令并确认新口令。

7.1.1.5 漏洞防利用

本项要求包括：

a) 应支持栈保护功能，以防护栈溢出类型的攻击；
b) 应支持数据执行保护功能，以防护代码注入类型的攻击；
c) 应支持地址空间随机化功能，以防护固定地址类型的攻击。

7.1.1.6 数据保护

本项要求包括：

a) 不应在 URL、错误消息、安全日志、调试信息中打印敏感数据；
b) 应支持使用安全密码算法对敏感数据进行保护，密码算法安全强度应达到 120 bits；
c) 对敏感数据进行存储时，在不需要还原明文的场景，应使用不可逆算法加密，在需要还原的场景，应采用安全的可逆算法进行加密；
d) 应支持输入敏感数据时非原文显示；
e) 宜支持安全通信协议，保障承载数据的保密性,完整性。
注：常见的安全通信协议包括互联网协议安全（IPSec）、媒体访问控制安全（MACSec）、TLS、数据包传输层安全（DTLS）等

7.1.1.7 流量防攻击

本项要求包括：

a) 应支持防护大流量攻击的能力；
b) 应支持防护非法报文(如邻居发现非法报文)攻击的能力；
c) 应支持防护地址欺骗报文(如 IP 地址欺骗)攻击的能力。

7.1.1.8 协议安全

本项要求包括：

a) 管理协议(SSH、HTTPS 等)应支持安全的协议版本（如 SSHv2）和安全的密码算法；
b) 支持 Web 管理时应支持防御常见的 Web 攻击，如跨站脚本攻击（XSS）、跨站请求伪造（CSRF）、命令注入、路径穿越、会话固定等；
c) 控制协议实现应支持使用安全密码算法进行协议报文认证。
注：常见的控制协议包括边界网关协议（BGP）、内网网关协议（IGP）等

7.1.1.9 证书安全

本项要求包括：

a) 使用时应支持检查数字证书的有效期；
b) 应支持数字证书的导入、更新、替换、删除功能及对证书信息的查询功能；
c) 应支持数字证书的吊销功能。

7.1.1.10 密钥安全

本项要求包括：

a) 密钥的用途应单一化，即一个密钥应只用于一种用途（如：加密、认证、散列等），如加密的密钥不能用于认证；
b) 应支持手动更新密钥的能力；
c) 应支持密钥全生命周期的安全管理，包含生成、分发、使用、存储、销毁等阶段；
d) 密码算法中使用到的随机数应满足 GM/T 0005—2021。

7.1.1.11 日志审计

本项要求包括：

a) 应支持安全日志转发到日志服务器的应支持安全通道传输；
b) 宜支持与 NTP 服务器的安全通信，确保时间同步。

7.1.1.12 安全删除

应删除内存、存储介质上中不再使用的数据。

7.1.2 路由器设备安全功能扩展要求

应支持单播反向路径转发（URPF）功能过滤IP源地址欺骗报文，不应让其在网络中传播。

7.1.3 数据中心交换机设备安全功能扩展要求

本项要求包括：

a) 数据中心交换机跨设备链路聚合应支持安全的认证和完整性保护措施；
b) 数据中心交换机智能无损存储网络应支持安全的认证和完整性保护措施；
c) 零配置开局方案宜具备安全能力保证开局安全。

7.1.4 园区交换机设备安全功能扩展要求

本项要求包括：

a) 园区交换机应支持 802.1X、MAC、Portal 等认证方式验证接入用户的合法性；
b) 零配置开局方案宜具备安全能力保证开局安全。

7.1.5 无线接入 AP 设备安全功能扩展要求

7.1.5.1 AP 接入安全

本项要求包含：

a) 应支持 AP 首次以证书认证方式接入，且支持一机一证；
b) 应支持 AP 和 AC 间的控制隧道加密功能。

7.1.5.2 无线用户接入安全

本项要求包括：

a) 应支持 WPA、WPA2、WPA3 安全策略机制；
b) 应支持 WAPI 认证，且 WAPI 证书公私钥由 AC/AP 自己产生；
c) 应支持管理帧加密保护。

7.1.5.3 设备检测能力

本项要求包括：

a) 应支持合法/非法 AP 检测；
b) 宜支持合法/非法网桥检测；
c) 宜支持合法/非法 STA 检测；
d) 宜支持合法/非法 Ad-hoc 检测。

7.1.5.4 设备反制能力

本项要求包括：

a) 应支持对非法 AP 或干扰 AP 进行反制；
b) 宜支持对非法 STA 或干扰 STA 进行反制；
c) 宜支持对 Ad-hoc 设备进行反制。

7.1.6 无线接入 AC 设备安全功能扩展要求

本项要求包含：

a) 应支持 AC 和 AP 间的控制隧道加密功能；
b) 应支持 802.1X、MAC、Portal 等认证方式验证接入用户的合法性。

7.1.7 防火墙设备安全功能扩展要求

7.1.7.1 入侵威胁检测能力

产品应具备入侵威胁检测，攻击检测有效性不低于85%，本项要求包括：
a) WEB 类攻击检测能力；
b) 系统漏洞类攻击检测能力；
c) 僵木蠕攻击检测能力。

7.1.7.2 病毒威胁检测能力

产品应具备病毒威胁检测能力，攻击检测有效性不低于 85%，本项要求包括：
a) PE 类流行病毒检测能力；
b) WEB 类流行病毒检测能力；
c) PDF 类流行病毒检测能力。

7.1.7.3 攻击防逃逸能力

产品应具备攻击防逃逸检测能力，攻击检测有效性不低于85%，本项要求包括：
a) 网络层攻击防逃逸检测能力；
b) 传输层攻击防逃逸检测能力；
c) 应用层攻击防逃逸检测能力。

7.1.8 抗拒绝服务攻击设备安全功能扩展要求

7.1.8.1 网络层拒绝服务攻击防护能力

产品应具备拒绝服务攻击检测和防护能力，攻击防护有效性不低于85%，本项要求包括：
a) Fragment Flood；
b) Land；
c) Teardrop；
d) Smurf；
e) Ping of death.

7.1.8.2 传输层拒绝服务攻击防护能力

产品应具备拒绝服务攻击检测和防护能力，攻击防护有效性不低于85%，本项要求包括：
a) SYN Flood；
b) UDP Flood；
c) ICMP Flood；
d) TCP 反射；
e) UDP 反射；
f) DNS 反射；
g) ACK Flood。

7.1.8.3 会话层拒绝服务攻击防护能力

产品应具备拒绝服务攻击检测和防护能力，攻击防护有效性不低于85%，本项要求包括：
a) TCP 空连接；
b) 不完整 TLS 会话。

7.1.8.4 应用层拒绝服务攻击防护能力

产品应具备拒绝服务攻击检测和防护能力，攻击防护有效性不低于85%，本项要求包括：
a) DNS Flood；

b) HTTP Flood。

7.2 安全保障要求

7.2.1 脆弱性评估

本项要求包括：

a) 应对网络设备基础安全质量进行评估，对默认安全、协议安全、漏洞防利用等安全功能要求进行风险进行识别和管理；
b) 应使用业界知名组件或具有同等安全测试能力的工具，如 openvas、secvas、awvs、nmap 等工具，在默认安全、协议安全、漏洞防利用等领域开展扫描和评估；
c) 评估结果应完成分析，对于不安全配置、未公开账号等问题，应有对应的解决方法和规避措施。

8 第三级安全要求

8.1 安全功能要求

8.1.1 安全功能通用要求

8.1.1.1 默认安全

本项要求包括：

a) 不应存在用户界面不可见或产品资料未描述的未公开的公网 IP 地址；
b) 配置不安全密码算法或者协议时可支持安全提示或者告警；
c) 不应存在用于数据加解密的硬编码密钥；
d) 不应默认使用不安全密码算法。
注：常见的不安全密码算法包括 MD5（Message-Digest Algorithm 5）、RC4（Rivest Cipher 4）、DES（Data Encryption Standard，数据加密标准）等。

8.1.1.2 软件完整性

本项要求包括：

a) 应支持升级时通过数字签名对软件包或补丁进行完整性和真实性进行校验；
b) 可支持对安装过程中软件版本降级进行安全提示或者告警；
c) 可支持安全启动功能，设备启动时由不可被篡改的硬件可信根作为数字签名校验的起点，逐级校验启动链上软件的完整性和真实性；
d) 可支持在设备运行时对内存代码段进行验证，确保运行的软件不被篡改；
e) 可支持内核模块加载时进行完整性校验。

8.1.1.3 访问控制

本项要求包括：

a) 所有在外部可见的能对系统进行管理的物理接口（如串口、管理网口等）应具备接入认证机制；
b) 对于跨信任网络且重要的机机接口应提供接入认证机制，标准协议没有认证机制的除外；
c) 如果系统提供开放编程功能（如 python、tcl 等），宜采用强度较高的安全隔离机制（如沙箱、非特权容器）；
d) 可支持采用强制访问控制机制(如 SELinux)对包含重要数据的文件和目录进行保护；
e) 设备可支持基于硬件的安全执行环境(Trusted Execution Environment,TEE)，用于隔离高安全业务或者数据。

8.1.1.4 身份认证

本项要求包括：

a) 应支持配置账号过期时间功能；

b) 用户口令应支持配置长度为 12 个字符，包含数字、字母或特殊字符至少两种组合；
c) 应具备弱口令字典功能，避免用户使用弱口令字典中的任何口令；
d) 使用口令鉴别方式时，用户配置的新口令应支持与最后使用的若干个口令进行比较，如果相同则不允许配置；
e) 执行对系统或应用有重大影响的操作前可支持二次认证，重大影响的操作包括重启设备、清空所有配置等。

8.1.1.5 漏洞防利用

本项要求包括：
a) 宜支持地址无关可执行功能，以防护固定地址类型的攻击；
b) 宜支持 GOT 表保护功能，以防护 GOT 表被覆盖修改；
c) 可支持从程序文件中剥离调试符号；
d) 可支持控制流完整性 CFI，以防护 ROP 攻击。

8.1.1.6 数据保护

本项要求包括：
a) 应支持输入敏感数据(如口令、私钥、对称密钥)时防拷贝功能；
b) 可支持存储安全日志、配置文件时通过密码算法实现完整性保护。

8.1.1.7 协议安全

管理协议(SSH、HTTPS 等)可支持非全零监听。

8.1.1.8 证书安全

本项要求包括：
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) 可支持在数字证书即将过期前发送安全提示或者告警，提示运维人员更新证书；
c) 可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。

8.1.1.9 密钥安全

本项要求包括：
a) 应支持密钥在临近过期前自动更新或者提醒管理员手动更新；
b) 对密钥做加密的密码算法的安全强度应不小于被加密密钥本身所用于密码算法的安全强度；
c) 密钥管理可采用层次化的保护方式；
d) 可支持对设备根密钥进行安全防护。

8.1.1.10 安全配置管理

本项要求包括：
a) 应支持对不安全协议或者算法进行查询，并提供修复建议；
b) 应支持和网管配合对安全配置的集中核查能力，支持核查结果可视化呈现。

8.1.1.11 日志审计

安全日志应单独存储，管理员不应具备删除安全日志的权限。

8.1.1.12 主机入侵检测

设备可支持主机入侵检测，对非法用户登录、OS 提权、关键文件篡改等攻击场景进行检测，并上报日志。

8.1.2 路由器设备安全功能扩展要求

路由器可支持SRv6报文鉴别功能，本项要求包括：
a) 可支持 SRv6 域内 SID 空间统一分配，不将 SRv6 域内的 SID 地址暴露到 SRv6 域外；

b） 可支持 SRv6 源节点对流量进行过滤，丢弃源地址或目的地址是 SRv6 域内的 SID 地址的报文。

8.1.3 数据中心交换机设备安全功能扩展要求

可支持安全零配置部署SZTP功能。

8.1.4 园区交换机设备安全功能扩展要求

可支持安全零配置部署SZTP功能。

8.1.5 无线接入 AP 设备安全功能扩展要求

8.1.5.1 AP 接入安全

本项要求包括：

a） 应支持 AP 和 AC 双向认证；

b） 应支持 AP 和 AC 间的数据隧道加密功能，且开启后整机转发性能不低于未开启的 50%。

8.1.5.2 无线用户接入安全

可支持通过物理层防护进行空口防侦听。

8.1.5.3 非法攻击检测能力

本项要求包括：

a） 应支持暴力破解攻击检测；

b） 应支持泛洪攻击检测，包括对认证请求帧、去认证帧、关联请求帧、去关联帧、重关联请求帧、探测帧、Action 帧、Eapol start 和 Eapol logoff 等报文进行泛洪攻击检测；

c） 宜支持欺骗攻击检测。

8.1.6 无线接入 AC 设备安全功能扩展要求

本项要求包括：

a） 应支持 AC 和 AP 双向认证；

b） 应支持 AC 和 AP 间的数据隧道加密功能，且开启后整机转发性能不低于未开启的 50%。

8.1.7 防火墙设备安全功能扩展要求

8.1.7.1 拒绝服务攻击防护能力

产品应具备拒绝服务攻击检测和防护能力，攻击防护有效性不低于95%，本项要求包括：

a） SYN Flood；

b） UDP Flood；

c） ICMP Flood；

d） HTTP Flood；

e） HTTPS Flood；

f） SIP Flood；

g） DNS Query Flood。

8.1.7.2 入侵威胁检测能力

产品应具备入侵威胁检测，攻击检测有效性不低于95%，本项要求包括：

a） WEB 类攻击检测能力；

b） 系统漏洞类攻击检测能力；

c） 僵木蠕攻击检测能力；

d） 自定义攻击检测能力。

8.1.7.3 病毒威胁检测能力

产品应具备病毒威胁检测能力，攻击检测有效性不低于95%，本项要求包括：

a) PE 类流行病毒检测能力；
b) WEB 类流行病毒检测能力；
c) PDF 类流行病毒检测能力；
d) ELF 类流行病毒检测能力。

8.1.7.4 攻击防逃逸能力

产品应具备攻击防逃逸检测能力，攻击检测有效性不低于95%，本项要求包括：
a) 网络层攻击防逃逸检测能力；
b) 传输层攻击防逃逸检测能力；
c) 应用层攻击防逃逸检测能力；
d) 内容安全攻击防逃逸检测能力；
e) 组合攻击防逃逸检测能力。

8.1.8 抗拒绝服务攻击设备安全功能扩展要求

8.1.8.1 网络层拒绝服务攻击防护能力

产品应具备拒绝服务攻击检测和防护能力，攻击防护有效性不低于95%，本项要求包括：
a) Fragment Flood；
b) Land；
c) Teardrop；
d) Smurf；
e) Ping of death；
f) IPv6 扩展头攻击；
g) 其它网络层拒绝服务攻击。

8.1.8.2 传输层拒绝服务攻击防护能力

产品应具备拒绝服务攻击检测和防护能力，攻击防护有效性不低于95%，本项要求包括：
a) SYN Flood；
b) UDP Flood；
c) ICMP Flood；
d) TCP 反射；
e) UDP 反射；
f) DNS 反射；
g) NTP 反射；
h) SSDP 反射；
i) ACK Flood；
j) RST Flood；
k) 其他传输层拒绝服务攻击。

8.1.8.3 会话层拒绝服务攻击防护能力

产品应具备拒绝服务攻击检测和防护能力，攻击防护有效性不低于 95%，本项要求包括：
a) TCP 空连接；
b) 不完整 TLS 会话；
c) SSL 连接攻击；
d) 其它会话层拒绝服务攻击。

8.1.8.4 应用层拒绝服务攻击防护能力

产品应具备拒绝服务攻击检测和防护能力，攻击防护有效性不低于95%，本项要求包括：
a) DNS Flood；
b) HTTP Flood；

c) HTTPS Flood；
d) HTTP 慢速攻击；
e) 其它应用层拒绝服务攻击。

8.2 安全保障要求

8.2.1 脆弱性评估

本项要求包括：
a) 应对网络设备开展攻防渗透验证，对于默认安全、协议安全、漏洞防利用等安全功能要求，评估实现上是否存在安全漏洞；
b) 应使用业界知名 cvss 评估方法对设备安全漏洞进行定级评估，确认漏洞攻击路径，按漏洞场景定级漏洞影响；
c) 攻防测试中发现的中危及以上等级的安全漏洞应进行修复或提供规避方案，宜对攻防测试中发现的提示问题进行修复或提供规避方案。

附录 A（资料性） 网络设备安全技术要求分级标准

根据网络设备应对安全风险的能力和受到破坏后可能造成的影响范围，将网络设备的安全技术要求划分为3级：

一级：能够抵御低级别安全风险，这些风险不会导致对国家安全、公共利益的危害，满足该等级的网络设备可用于通用网络场景；

二级：能够抵御中级别安全风险，这些风险可能导致对公共利益的危害，但不会危害到国家安全，满足该等级的网络设备可用于央企等中大型企业网络；

三级： 能够抵御高级别风险，这些风险可能导致对国家安全的危害，或导致对公共利益的严重危害，满足该等级的网络设备可用于关键基础设施网络。

参 考 文 献

[1] GB/T 20275—2021 信息安全技术 网络入侵检测系统技术要求和测试测评方法
[2] 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
[3] GB/T 41267—2022 网络关键设备安全技术要求 交换机设备
[4] GB/T 41269—2022 网络关键设备安全技术要求 路由器设备
[5] 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
[6] GB/T 28448—2019 信息安全技术 网络安全等级保护测评要求
[7] GB/T 44810.1—2024 IPv6网络安全设备技术要求 第1部分：防火墙