



中华人民共和国国家标准

GB [×××××]—[××××]

网络关键设备安全技术要求
通用要求

Security technical requirements for critical network devices : Common requirements

[点击此处添加与国际标准一致性程度的标识]

（报批稿）

（本稿完成日期：2020-4-13）

[××××]-[××]-[××]发布 [××××]-[××]-[××]实施

国家市场监督管理总局 发布
中国国家标准化管理委员会

目 次

前 言..... II

1 范围.....1

2 规范性引用文件.....1

3 术语和定义.....1

4 缩略语.....2

5 安全功能要求.....3

 5.1 设备标识安全.....3

 5.2 冗余、备份恢复与异常检测.....3

 5.3 漏洞和恶意程序防范.....3

 5.4 预装软件启动及更新安全.....3

 5.5 用户身份标识与鉴别.....4

 5.6 访问控制安全.....4

 5.7 日志审计安全.....4

 5.8 通信安全.....5

 5.9 数据安全.....5

 5.10 密码要求.....5

6 安全保障要求.....5

 6.1 设计和开发.....5

 6.2 生产和交付.....6

 6.3 运行和维护.....6

参考文献..... 8

前 言

本标准的全部技术内容为强制性。

本标准按照GB/T 1.1—2009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。

本标准由中华人民共和国工业和信息化部提出并归口。

网络关键设备安全技术要求 通用要求

1 范围

本标准规定了网络关键设备应满足的通用安全功能要求和安全保障要求。

本标准适用于网络关键设备，可为网络运营者采购网络关键设备时提供依据，还适用于指导网络关键设备的研发、测试等工作。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是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

3 术语和定义

GB/T 25069中界定的以及下列术语和定义适用于本文件。

3.1

网络关键设备 critical network device

支持联网功能，在同类网络设备中具有较高性能的设备，通常应用于重要网络节点、重要部位或重要系统中，一旦遭到破坏，可能引发重大网络安全风险。

注：具有较高性能是指设备的性能指标或规格符合《网络关键设备和网络安全专用产品目录》中规定的范围。

3.2

部件 component

由若干装备在一起的零件组成，能够实现特定功能的模块或组件。

3.3

恶意程序 malicious program

被专门设计用来攻击系统，损害或破坏系统的保密性、完整性或可用性的程序。

注：常见的恶意程序包括病毒、蠕虫、木马、间谍软件等。

3.4

预装软件 pre-installed software

设备出厂时安装或提供的、保障设备正常使用必须的软件。

注：不同类型设备的预装软件存在差异。路由器、交换机的预装软件通常包括引导固件、系统软件等，服务器的预装软件通常包括带外管理软件等，PLC设备的预装软件通常包括固件、编程软件等。

3.5**漏洞 vulnerability**

可能被威胁利用的资产或控制的弱点。

注：改写GB/T 29246—2017，定义2.89。

3.6**敏感数据 sensitive data**

一旦泄露、非法提供或滥用可能危害网络安全的数据。

注：网络关键设备常见的敏感数据包括口令、密钥、关键配置信息等。

3.7**健壮性 robustness**

描述网络关键设备或部件在无效数据输入或者在高强度输入等环境下，其各项功能可保持正确运行的程度。

注：改写GB/T 28457—2012，定义3.8。

3.8**用户 user**

对网络关键设备进行配置、监控、维护等操作的使用者。

3.9**私有协议 private protocol**

专用的、非通用的协议。

3.10**异常报文 abnormal packet**

各种不符合标准要求的报文。

4 缩略语

下列缩略语适用于本文件：

CPU	中央处理器（Central Processing Unit）
HTTP	超文本传输协议（Hypertext Transfer Protocol）
IP	网间互联协议（Internet Protocol）

MAC	媒体访问控制 (Media Access Control)
PLC	可编程逻辑控制器 (Programmable Logic Controller)
SNMP	简单网络管理协议 (Simple Network Management Protocol)
SSH	安全外壳协议 (Secure Shell)
TCP	传输控制协议 (Transmission Control Protocol)
UDP	用户数据报协议 (User Datagram Protocol)

5 安全功能要求

5.1 设备标识安全

网络关键设备应满足以下要求：

- a) 硬件整机和主要部件应具备唯一性标识。

示例：路由器、交换机的主要部件可包括主控板卡、业务板卡、交换网板、风扇模块、电源、存储系统软件的板卡、硬盘或闪存卡等。服务器的主要部件可包括中央处理器、硬盘、内存、风扇模块、电源等。PLC 的主要部件可包括电源模块、CPU 模块、网络通信信息模块、输入输出模块等。常见的唯一性标识方式包括序列号等。

- b) 应对预装软件、补丁包/升级包的不同版本进行唯一性标识。

示例：常见的版本唯一性标识方式包括版本号等。

5.2 冗余、备份恢复与异常检测

网络关键设备应满足以下要求：

- a) 应支持设备整机主备切换功能或关键部件应支持冗余功能，应提供自动切换功能，在设备或关键部件运行状态异常时，切换到冗余设备或冗余部件以降低安全风险。

示例：路由器、交换机支持冗余功能的关键部件可包括主控板卡、交换网板、电源模块、风扇模块等。服务器支持冗余功能的关键部件可包括硬盘、电源模块、风扇模块等。PLC 支持冗余功能的关键部件可包括电源模块、CPU 模块、网络通信信息模块、输入输出模块等。

- b) 应支持对预装软件、配置文件的备份与恢复功能，使用恢复功能时支持对预装软件、配置文件的完整性检查。

- c) 应支持识别异常状态，产生相关错误提示信息。

5.3 漏洞和恶意程序防范

网络关键设备应满足以下要求：

- a) 不应存在已公布的漏洞，或具备补救措施防范漏洞安全风险。
b) 预装软件、补丁包/升级包不应存在恶意程序。
c) 不应存在未声明的功能和访问接口（含远程调试接口）。

5.4 预装软件启动及更新安全

网络关键设备应满足以下要求：

- a) 应支持启动时完整性校验功能，确保系统软件不被篡改。
b) 应支持设备预装软件更新功能。
c) 应具备安全功能，保障软件更新操作的安全。

示例：安全功能可包括用户授权、更新操作确认、更新过程控制等，例如仅指定授权用户可实施更新操作、实施更新操作的用户需经过二次鉴别、支持用户选择是否进行更新、对更新操作进行二次确认或延时生效等。

- d) 应具备安全功能，以防范软件在更新过程中被篡改。

示例：安全功能可包括采用非明文的信道传输更新数据、支持软件包完整性校验等。

- e) 应有明确的信息告知用户软件更新过程的开始、结束以及更新的内容。

5.5 用户身份标识与鉴别

网络关键设备应满足以下要求：

- a) 应对用户进行身份标识和鉴别，身份标识应具有唯一性。

示例：常见的身份鉴别方式包括：口令、共享密钥、数字证书或生物特征等。

- b) 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，支持设置口令生存周期，支持口令复杂度检查功能，用户输入口令时，不应明文回显口令。

示例：口令复杂度检查要求可包括：长度要求，例如长度不小于8位；字符类型要求，例如包含数字、小写字母、大写字母、标点符号、特殊符号中的至少两类；口令与账号无关性要求，例如口令不包含账号等。

- c) 应支持启用安全策略或具备安全功能，以防范用户鉴别信息猜解攻击。

示例：安全策略或安全功能可包括默认开启口令复杂度检查功能、限制连续的非法登录尝试次数或支持限制管理访问连接的数量、双因素鉴别（例如口令+证书、口令+生物鉴别等）等措施，当出现鉴别失败时，设备提供无差别反馈，避免提示“用户名错误”、“口令错误”等类型的具体信息。

- d) 应支持启用安全策略或具备安全功能，以防止用户登录后会话空闲时间过长。

示例：安全策略或安全功能可包括登录用户空闲超时后自动退出等。

- e) 应对用户身份鉴别信息进行安全保护，保障用户鉴别信息存储的保密性，以及传输过程中的保密性和完整性。

5.6 访问控制安全

网络关键设备应满足以下要求：

- a) 默认状态下应仅开启必要的服务和对应的端口，应明示所有默认开启的服务、对应的端口及用途，应支持用户关闭默认开启的服务和对应的端口。

- b) 非默认开放的端口和服务，应在用户知晓且同意后才可启用。

- c) 提供用户分级分权控制机制。

注：分级分权是指用户权限可分为多个等级，可为设备配置用户、审计用户等分配相互独立的权限。

- d) 在用户访问受控资源时，支持设置访问控制策略并依据设置的访问控制策略进行授权和访问控制，确保访问和操作安全。

注：受控资源是需要相应权限才可访问的资源。

示例：访问控制策略可包括通过IP地址绑定、MAC地址绑定等安全策略限制可访问的用户等。

- e) 对涉及设备安全的重要功能，仅授权高权限等级用户使用。

示例：涉及设备安全的重要功能可包括补丁管理、固件管理、日志审计、时间同步等。

5.7 日志审计安全

网络关键设备应满足以下要求：

- a) 应提供日志审计功能，对用户关键操作行为和重要安全事件进行记录，用户操作日志记录功能应不能被关闭，应支持对安全事件进行告警提示。

示例：用户关键操作可包括增/删账户、修改鉴别信息、修改关键配置、文件上传/下载、用户登录/注销、用户权限修改、重启/关闭设备、编程逻辑下载、运行参数修改等。

- b) 应提供日志信息本地存储功能，支持日志信息输出。
- c) 日志审计功能应记录必要的日志要素，为查阅和分析提供足够的信息。
 示例：日志要素可包括事件发生的日期和时间、主体、类型、结果、源 IP 地址等。
- d) 应具备对日志在本地存储和输出过程进行保护的安全功能，防止日志内容被未经授权的查看、输出或删除。
 示例：常见的日志保护安全功能包括用户授权访问控制等。
- e) 应提供本地日志存储空间耗尽处理功能。
 示例：本地日志存储空间耗尽时常见的处理功能可包括：剩余存储空间低于阈值时进行告警、循环覆盖等。
- f) 不应在日志中明文或者弱加密记录敏感数据。

5.8 通信安全

网络关键设备应满足以下要求：

- a) 应支持与管理系统（管理用户）建立安全的通信信道/路径，保障通信数据的保密性、完整性。
- b) 应满足通信协议健壮性要求，防范异常报文攻击。
 示例：通信协议通常包括 IPv4/v6、TCP、UDP 等基础通信协议，SNMP、SSH、HTTP 等网络管理协议、路由协议、工业控制协议等专用通信协议，以及其他网络应用场景中的专用通信协议。
- c) 应支持时间同步功能。
- d) 应不存在未声明的私有协议。
- e) 应具备抵御常见重放类攻击的能力。
 示例：常见重放类攻击可包括各类网络管理协议的身份鉴别信息重放攻击、设备控制数据重放攻击等。

5.9 数据安全

网络关键设备应满足以下要求：

- a) 应具备对存储在设备上的敏感数据进行安全保护的功能。
- b) 应具备对用户产生且存储在设备中的数据进行授权删除的功能，支持在删除前对该操作进行确认。
 示例：用户产生且存储在设备中的数据通常包括日志、配置文件等。

5.10 密码要求

本标准凡涉及密码算法的相关内容，按国家有关法规实施。

6 安全保障要求

6.1 设计和开发

网络关键设备提供者：

- a) 应在设备设计和开发环节识别安全风险，制定安全策略。
 示例：设备设计和开发环节的常见安全风险可包括但不限于：开发环境的安全风险、第三方组件引入的安全风险、开发人员导致的安全风险等。
- b) 应建立设备安全设计和开发操作规程，保障安全策略落实到设计和开发的整个过程。
- c) 应建立配置管理程序及相应配置项清单，配置管理系统应能跟踪内容变更，并对变更进行授权和控制。
- d) 应采取措施防范设备被植入恶意程序。

- e) 应采取措施防范设备被设置隐蔽的接口或功能模块。
- f) 应采取措施防范第三方关键部件、固件或软件可能引入的安全风险。
- g) 应采用漏洞扫描、病毒扫描、代码审计、健壮性测试、渗透测试和安全功能验证的方式对设备进行安全性测试。
- h) 应对已发现的安全缺陷、漏洞等安全问题进行修复，或提供补救措施。

6.2 生产和交付

网络关键设备提供者：

- a) 应在设备生产和交付环节识别安全风险，制定安全策略。
 示例：生产和交付环节的常见安全风险可包括但不限于：自制或采购的组件被篡改、伪造等风险，生产环境存在的安全风险、设备被植入的安全风险、设备存在漏洞的安全风险、物流运输的风险等。
- b) 应建立并实施规范的设备生产流程，在关键环节实施安全检查和完整性验证。
- c) 应建立和执行规范的设备完整性检测流程，采取措施防范自制或采购的组件被篡改、伪造等风险。
- d) 应对预装软件在安装前进行完整性校验。
- e) 应为用户提供验证所交付设备完整性的工具或方法，防范设备交付过程中完整性被破坏的风险。

示例：验证所交付设备完整性的工具或方法可包括防拆标签、数字签名/证书等。

- f) 应为用户提供操作指南和安全配置指南等指导性文档，以说明设备的安装、生成和启动的过程，并对设备功能的现场调试运行提供详细的描述。
- g) 应提供设备服务与默认端口号的映射关系说明。
- h) 应声明设备中存在的私有协议并说明其用途，私有协议不应存在所声明范围之外的用途。
- i) 交付设备前，发现设备存在已知漏洞应当立即采取补救措施。

6.3 运行和维护

网络关键设备提供者：

- a) 应识别在运行环节存在的设备自身安全风险（不包括网络环境安全风险），以及对设备进行维护时引入的安全风险，制定安全策略。
- b) 应建立并执行针对设备安全事件的应急响应机制和流程，并为应急处置配备相应的资源。
- c) 在发现设备存在安全缺陷、漏洞等安全风险时，应采取修复或替代方案等补救措施，按照有关规定及时告知用户并向有关主管部门报告。
- d) 在对设备进行远程维护时，应明示维护内容、风险以及应对措施，应留存不可更改的远程维护日志记录，记录内容应至少包括维护时间、维护内容、维护人员、远程维护方式及工具。

示例：远程维护可包括对设备的远程升级、配置修改、数据读取、远程诊断等操作。

- e) 在对设备进行远程维护时，应获得用户授权，并支持用户中止远程维护，应留存授权记录。

示例：获得用户授权的方式可包括鉴别信息授权、书面授权等。

- f) 在涉及个人信息和重要数据的收集和处理时，应满足国家法律、行政法规等的规定。
- g) 应为用户提供对补丁包/升级包的完整性、来源真实性进行验证的方法。
- h) 应为用户提供对废弃（或退役）设备中关键部件或数据进行不可逆销毁处理的方法。
- i) 应为用户提供废弃（或退役）设备回收或再利用前的关于安全风险控制方面的注意事项。
- j) 对于维修后再销售或提供的设备或部件，应对设备或部件中的用户数据进行不可逆销毁。

- k) 应在国家法律、行政法规等规定或合同约定的期限内，为设备提供持续的安全维护，不应以业务变更、产权变更等原因单方面中断或终止安全维护。
- 1) 应在国家法律、行政法规等规定或合同约定的期限内，向用户告知设备生命周期终止时间。

参 考 文 献

- [1] GB/T 18018-2019 信息安全技术 路由器安全技术要求
 - [2] GB/T 18336-2015 信息技术 安全技术 信息技术安全评估准则
 - [3] GB/T 20011-2005 信息安全技术 路由器安全评估准则
 - [4] GB/T 21028-2007 信息安全技术 服务器安全技术要求
 - [5] GB/T 21050-2019 信息安全技术 网络交换机安全技术要求
 - [6] GB/T 25063-2010 信息技术安全 服务器安全测评要求
 - [7] GB/T 33008.1-2016 工业自动化和控制系统网络安全 可编程序控制器(PLC) 第1部分：系统要求
 - [8] GB/T 36470-2018 信息安全技术 工业控制系统现场测控设备通用安全功能要求
 - [9] YD/T 1359-2005 路由器设备安全技术要求——高端路由器（基于IPv4）
 - [10] YD/T 1439-2006 路由器设备安全测试方法—高端路由器
 - [11] YD/T 1629-2007 具有路由功能的以太网交换机设备安全技术要求
 - [12] YD/T 1630-2007 具有路由功能的以太网交换机设备安全测试方法
 - [13] YD/T 1906-2009 IPv6网络设备安全技术要求——核心路由器
 - [14] YD/T 2042-2009 IPv6网络设备安全技术要求——具有路由功能的以太网交换机
 - [15] YD/T 2043-2009 IPv6网络设备安全测试方法——具有路由功能的以太网交换机
 - [16] YD/T 2045-2009 IPv6网络设备安全测试方法——核心路由器
 - [17] 3GPP TS 33.117 Catalogue of general security assurance requirements
 - [18] ITU-T X.805 Security architecture for systems providing end-to-end communications
-