电 信 终 端 产 业 协 会 标 准

TAF-WG9-AS0029-V1.0.0:2018

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

2018-11-05 发布　　2018-11-05 实施

电信终端产业协会　　发 布

目 录

前　言

本标准是网络关键设备安全系列标准之一，该系列标准结构预计如下：

《网络关键设备安全技术要求 通用要求》

《网络关键设备安全技术要求 路由器设备》

《网络关键设备安全测试方法 路由器设备》

《网络关键设备安全技术要求 交换机设备》

《网络关键设备安全测试方法 交换机设备》

...

本标准提出各类网络关键设备通用的、基本的安全要求，不分等级。《网络关键设备安全技术要求 路由器设备》、《网络关键设备安全技术要求 交换机设备》等各类设备的安全标准内容分为基本级要求和增强级要求。

本标准/本部分由电信终端产业协会（TAF）提出并归口。

本标准/本部分起草单位：中国信息通信研究院、华为技术有限公司、新华三技术有限公司、中兴通讯股份有限公司、北京启明星辰信息安全技术有限公司、联想移动通信科技有限公司。

本标准/本部分主要起草人：张治兵、周开波、张亚薇、倪平、孙薇、陈鹏、叶郁佰、童天予、杨达、周继华、李汝鑫、万晓兰、付凯、蒋皓、李莉。

引　言

为推进《网络安全法》的落地实施，本标准提出网络关键设备应满足的通用安全技术要求。

网络关键设备通常应用于网络中的重要节点位置或国家重要的网络系统中，一旦遭到破坏，可能严重危害国家安全、国计民生、公共利益。例如整系统吞吐量和路由表容量达到较高指标的高端路由器设备、控制器指令执行时间达到较高指标的可编程逻辑控制器（PLC设备）等。本标准属于网络关键设备安全技术要求系列标准中的通用标准，对各类网络关键设备，除满足本标准要求，还应满足相应的设备安全标准要求。例如对于路由器设备，除了满足本标准要求，还应满足《网络关键设备安全技术要求 路由器设备》和《网络关键设备安全测试方法 路由器设备》。

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技术要求。

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，仅所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 25069-2010 信息安全技术 术语

3　术语和定义

GB/T 25069-2010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

是指通常应用于网络中的重要节点位置或国家重要的网络系统中，面临较多的安全威胁，一旦遭到破坏，可能严重危害国家安全、国计民生、公共利益的网络设备。

3.2　恶意程序 malware

一种企图通过执行非授权过程来破坏信息系统保密性、完整性和可用性的软件或固件。常见的恶意程序包括病毒、蠕虫、木马或其它影响设备安全的程序代码。恶意程序也包括间谍软件和广告软件。

3.3　预装软件 preset software

网络关键设备的预装软件是指设备出厂时安装的软件和正常使用必须的配套软件，包括固件、系统软件、应用软件、配套的管理软件等。

4　安全技术要求

4.1　标识安全

网络关键设备：

a)　硬件整机和主要部件应具备唯一性标识；

示例：主要部件可包括主控板卡、业务板卡、系统软件存储部件等。

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，并保持记录。

4.2　冗余与备份恢复安全

网络关键设备：

a） 部分关键部件应支持冗余功能，在设备运行状态异常可能影响网络安全时，可通过启用备用部件防范安全风险；

示例：支持冗余功能的部分关键部件可包括主控板卡、业务板卡、电源模块等部件。

b） 涉及设备安全的软件、配置文件等应支持备份与恢复功能。

4.3 漏洞与缺陷管理安全

网络关键设备：

a） 部分关键部件应不存在已公布的高危和中危漏洞或具备有效措施防范漏洞安全风险；

示例：部分关键部件可包括 CPU、硬盘、系统软件存储部件等。

b） 预装软件应不存在已公布的高危和中危漏洞或具备有效措施防范漏洞安全风险；

c） 预装软件存在暂未修复的已知漏洞或安全缺陷时，应明确告知用户风险及防范措施；

d） 预装软件、补丁包/升级包应不存在恶意程序；

e） 应不存在未向用户声明的功能和隐蔽通道。

4.4 软件更新安全

网络关键设备：

a） 应支持设备软件更新功能；

b） 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等措施，更新过程中用户可以选择中止更新，支持用户选择是否进行更新，支持用户对软件降级使用等；

c） 应具备安全功能防范软件更新过程被篡改；

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；

d） 应有明确的信息告知用户软件更新过程的开始与结束。

4.5 默认状态安全

网络关键设备：

a） 出厂应预装满足功能需求且安全风险较低的软件版本；

b） 出厂默认开放的端口和服务应明示用户，满足最小够用原则。

4.6 身份标识与鉴别

网络关键设备应：

a） 对访问控制主体进行身份标识和鉴别；

b） 支持使用口令方式进行鉴别，用户首次管理设备时提示修改默认口令或设置口令，支持设置口令修改周期；

c） 支持启用安全策略或具备安全功能，以防范用户凭证猜解攻击；

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、双因素鉴别等措施。

d） 支持启用安全策略或具备安全功能，以防范会话空闲时间过长；

示例：安全策略或安全功能可包括登录用户空闲超时锁定或自动退出等措施。

e） 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和传输的保密性和完整性。

4.7 访问控制安全

网络关键设备应：

a） 在出厂时设置默认安全的访问控制策略，或支持用户首次使用时设置访问控制策略；

b） 提供用户分级分权控制机制；

c） 在用户访问受控资源时，依据设置的访问控制策略进行控制，确保访问和操作安全；

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。

d） 对涉及设备安全的重要功能，仅授权的高权限等级用户可使用。

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。

4.8 日志审计安全

网络关键设备：

a） 应提供日志审计功能，对用户关键操作行为进行记录；

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、开启/关闭日志审计功能、用户登录/注销、用户权限修改、重启/关闭设备等；

b） 应提供日志信息本地存储功能，支持日志信息输出功能；

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、结果等。

d） 应提供日志分析功能或为日志分析功能提供接口；

e） 用户操作日志应受到保护，防止日志内容被修改，防止未经授权的操作；

f） 不应在日志中明文记录用户口令等敏感数据。

4.9 通信安全

网络关键设备：

a） 管理系统（管理用户）与设备之间的通信信道/路径应保证数据的保密性、完整性和可用性；

b） 应具备抵御常见资源消耗类攻击的能力；

示例：常见资源消耗类攻击可包括 SYN Flood 攻击、Ping Flood 攻击等。

c） 应满足一定的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 等网络管理协议以及 NTP、BGP、OSPF 等专用通信协议；

d） 应支持时间同步功能，并具备安全功能或措施防范针对时间同步功能的攻击；

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身份鉴别重放攻击等。

4.10 数据安全

网络关键设备：

a） 应对存储在设备上的数据提供分级管理功能，对用户口令等敏感数据具备安全防护措施；

b） 应具备删除使用数据和配置信息的功能，应为使用者提供确认使用数据删除状态的功能；

c） 具有收集设备使用者信息功能的，应当向使用者明示并取得同意；

d） 涉及用户个人信息和国家重要数据的，应当遵守国家相关规定。

附 录 A
（规范性附录）
标准修订历史

修订时间	修订后版本号	修订内容
2018-5-18	V0.9.0	第一次征求意见，按照会议讨论情况修改
2018-8-27	V1.0.0	第二次征求意见，按照会议讨论情况修改
2018-10-19	V2.0.0	按照会员单位反馈意见进行修改

附 录 B
（资料性附录）

参 考 文 献

1) ITU-T X.805 端到端通信服务安全框架
2) GB/T 18336-2015 信息技术 安全技术 信息技术安全性评估准则
3) YD/T 1359-2005 路由器设备安全技术要求——高端路由器（基于 IPv4）
4) YD/T 1439-2006 路由器设备安全测试方法－高端路由器
5) YD/T 1906-2009 IPv6 网络设备安全技术要求——核心路由器
6) YD/T 2045-2009 IPv6 网络设备安全测试方法——核心路由器
7) 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
8) 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
9) 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
10) 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
11) GB/T18018-2007 信息安全技术 路由器安全技术要求
12) GB/T20011-2005 信息安全技术 路由器安全评估准则
13) GB/T 21050-2007 信息安全技术 网络交换机安全技术要求（评估保证级 3）
14) GB/T 21028-2007 信息安全技术 服务器安全技术要求
15) GB/T 25063-2010 信息技术安全 服务器安全测评要求
16) 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