电 信 终 端 产 业 协 会 标 准

TAF-WG9-AS0040-V1.0.0:2019

智能网关设备安全技术要求

Security Technical Requirements for Intelligent Gateway Devices

2019－06－17 发布　　2019－06－17 实施

电信终端产业协会　　发 布

目　次

前　言

本标准提出智能网关硬件、系统软件、业务功能、网管等方面的安全技术要求。

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、启明星辰信息技术集团股份有限公司、华为技术有限公司、新华三技术有限公司、烽火通信科技股份有限公司、联想（北京）有限公司、中兴通讯股份有限公司、上海诺基亚贝尔股份有限公司、北京辰信领创信息技术有限公司、北京奇虎科技有限公司、深圳市友华通信技术有限公司。

本标准/本部分主要起草人：张治兵、陈鹏、童天予、吴国燕、孙薇、彭宏明、叶郁柏、王英晨、许雯、刘鑫、李汝鑫、张亚薇、蒋皓、万晓兰、夏敏、付凯、倪平、雷慧桃、姚一楠、曹夏飞。

引　　言

随着我国宽带中国战略实施逐步深化，宽带普及率不断提升，家庭和企业网关设备使用量进入以亿计时代。近年来，随着互联网业务的多元化，物联网、智能家居等业态发展迅速，智能网关数量快速增长。巨量的智能网关设备在网运行时，应重点考虑设备安全问题可能引发的网络安全风险。国际上，由于网关设备安全问题导致的断网问题近年来频发，2017年，德国曾因为网关设备安全问题导致全国大面积断网事件，对经济运行和日常生活影响很大。本标准针对智能网关设备的典型应用场景，结合设备的功能特性，提出设备在硬件、软件、业务功能、网管等方面的安全技术要求。

智能网关设备安全技术要求

1 范围

本标准规定了智能网关设备在硬件、系统软件、业务功能、网管等方面的安全技术要求。本标准规定了智能网关设备分级安全要求。

本标准可供智能网关设备的设计和生产厂商、系统集成商、设备使用方、安全检测和安全认证机构使用。

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 智能网关设备 Intelligent gateway device

智能网关设备是指具备连通外部广域通信网络和家庭/小型企业内部局域网络功能，支持使用 APP 通过云平台等方式实现远程配置、设备控制、流量监测、终端管理等智能化管理功能，支持通过安装插件或应用实现扩展功能的设备。

4 安全技术要求

4.1 设备硬件和系统软件安全

4.1.1 标识安全

a) 硬件整机应具备唯一性标识；

b) 应对软件/固件、补丁包/升级包的版本进行唯一性标识，并保持记录；

c) 禁止在操作界面、日志、调试信息和错误提示中明文显示密钥、口令、会话标识等敏感信息；

d) 应标识每一个物理接口，并说明其功能，不应预留未标识的物理接口；

e) 关键安全功能模块不应存在功能丝印标识（详见附录 C），防止攻击者通过丝印标识了解器件特性和单板原理，从而加大攻击者识别硬件的难度。

4.1.2 接口安全

a) 不应存在可绕过正常认证机制直接进入到系统的隐秘通道；不应存在不可管理的认证/访问方式，包括用户不可管理的帐号、人机接口以及可远程访问的机机接口的硬编码口令；

[注:]智能网关设备的用户是指设备的所有者。例如，在运营商网络接入服务场景下，设备所有者通常是运营商，设备用户是指运营商，而在智能家居场景下，设备所有者是个人用户，设备用户是指最终个人用户。

b) 对于可对设备进行管理的外部通信接口，应提供接入认证机制；

c) 支持控制无线通信网络如 WLAN、蓝牙、蜂窝、Zigbee 等接口进行数据连接的开关功能；

d) 支持 WAN 口远程管理方式的开关功能，例如 WAN 口的 WEB、APP 等管理方式应支持开启和关闭；

e) 通过 WLAN 方式接入设备，应支持使用加密方式进行认证：

1) 设备支持安全的认证方式，例如 WPA2/PSK 等；

2) 设备支持 AES-128、SM4 等至少一种安全强度较高的密码算法；

3) 设备支持 WPA3，支持 AES-192 及以上强度的密码算法。

4.1.3 硬件安全

a) 所有用于生产、调试和维修的接口要求默认禁用且用户不可激活，禁用或去掉易被攻击者利用的调试功能或组件；

b) JTAG 等测试芯片接口应具有相关安全防护机制。

4.1.4 开放端口和服务安全

a) 应提供所有开放端口相关的列表用于说明开放端口的功能，并通过交互页面、用户手册等至少一种方式体现；

b) 基于最小开放原则，默认关闭不是系统业务所必需的端口，默认关闭 Telnet、FTP、SSH v1.x、tftp、SNMPv2c 等不安全协议端口；

c) 不应存在可绕过认证直接进入系统的通信端口；

d) DNS 客户端向服务端请求服务时，源端口号应为变化值，避免因此遭受欺骗攻击；

e) WAN 侧应支持使用非明文数据传输协议对设备进行管理；

f) WAN 侧开放的 TR069 等服务应只在 WAN 侧可访问。

4.1.5 漏洞管理安全

a） 在用户登录通过认证前的提示信息应避免包含设备软件版本、型号等敏感信息，如：可通过支持关闭提示信息或者用户自定义等安全措施；

b） 不应存在已公布（90 天之前）的高危和中危漏洞或具备有效措施防范漏洞安全风险；

c） 智能网关设备提供者应提供接收外部报告安全问题的有效渠道，发现其设备存在漏洞等风险时，应当立即采取补救措施，及时告知用户风险及防范措施，并留存实施相关补救措施和告知用户的记录；

d） 预装软件、补丁包/升级包应不包含恶意程序。

4.1.6 常见攻击防护安全

a） 应支持安全措施（例如采用限制用户会话连接数量等），以防范资源消耗型拒绝服务类攻击，设备应在受到拒绝服务类攻击时不死机，不重启，远程管理(如 TR069,智能平台)功能正常，设备不能脱管，在停止攻击后可恢复到正常状态，自动恢复的延迟时间应低于 30 秒；

1） 应能够提供防 DHCP flood 攻击和反射攻击的能力，支持对在单位时间内处理的 DHCP 应答报文的数量进行限制；

2） 应能够提供防 DNS flood 攻击和反射攻击的能力，支持对在单位时间内处理的 DNS 应答报文的数量进行限制；

3） 应能够提供防 NTP flood 攻击和反射攻击的能力，支持对在单位时间内处理的 NTP 应答报文的数量进行限制；

4） 应能够提供防 SYN flood 攻击和反射攻击的能力，支持对在单位时间内处理的 SYN 应答报文的数量进行限制。

b） 应支持防火墙功能，支持对防火墙规则的配置，并支持基于以下过滤规则：

1） 应支持根据源 MAC 地址、目的 MAC 地址进行报文过滤；

2） 应支持根据源 IP 地址及范围段、目的 IP 地址及范围段进行报文过滤；

3） 应支持根据 IP 源端口及范围段、目的端口及范围段进行报文过滤；

4） 应支持根据 IP 包的传输层协议类型进行报文过滤，并至少具有 TCP/UDP/ICMP 的选项；

5） 应支持对匹配规则的报文进行处理模式的选择,且对匹配规则的报文的处理模式提供允许和禁止 2 种选项，且默认为禁止模式；

6） 应支持对 TOS/DSCP 报文进行过滤的功能。

c） 应支持 DMZ 功能；

d） 应支持用户身份鉴别失败处理功能，防范用户凭证猜解攻击；

1） 支持当连续非法登录尝试次数达到限制时锁定用户；

2） 支持设置连续非法登录尝试次数限制，并当达到限制时锁定用户，支持设置锁定用户时长；

3） 支持用户登录会话数量限制功能，支持设置用户登录会话数量；。

e） 应提供防端口扫描功能，支持开启和关闭防端口扫描功能；

f） 智能网关应支持对插件资源权限限制功能，智能插件应运行在非特权容器模式。智能插件使用资源应受控（如 CPU，session，socket，RAM，flash），即系统需优先保证远程管理（如 TR069、智能平台）所必须的资源，以便在智能插件进程被攻击后，能够通过管理平台对异常插件进行控制。

4.1.7 系统升级安全

a） 应支持本地或远程升级；

b） 应支持因断网、使用错误的固件导致升级异常时可恢复到正常状态；

c） 应支持因升级过程中断电导致升级异常时可恢复到正常状态；

d） 远程升级应支持升级数据加密传输；

e） 采取措施防止非授权用户对设备进行系统和桌面的刷写、修改或安装。例如，使用安卓系统的智能网关，可采取默认禁用 USB 调试（ADB）模式等措施；

f） 产品对外发布的软件（包含软件包/补丁包），需具备完整性保护、来源真实性验证机制（建议采用数字签名，至少支持哈希值验证），并且在安装、升级过程中对软件进行完整性验证；

g） 软件镜像支持主备分区，当主分区镜像破坏时，设备应能从备份分区启动；

h） 升级操作仅授权用户可实施；实施升级操作时，应有明确的信息告知操作者，并提供同意和取消的选项，在操作者确认同意后才能实施升级。

[注：]授权用户包括 WAN 侧的用户和 LAN 侧的用户，WAN 侧既包括运营商用户通过 TR069 升级，也包括个人用户通过云平台升级。

i） 应支持向设备使用者提示正在进行远程升级的功能，防止用户因升级带来的无法上网而异常断电。

4.2 业务功能安全

4.2.1 通信协议安全

a） 应提供防非法报文攻击能力，基础通信协议和网络管理协议应具备一定的健壮性；

1） 基础通信协议（如 IPv4/v6，ICMP，TCP，UDP 等）具备一定的健壮性；

2） 网络管理协议（如 SSH/Telnet、HTTP/HTTPS、SNMP、FTP/SFTP 等）具备一定的健壮性；

b） 应能够对特定协议的广播风暴（例如 DHCP，ARP，IGMP 等）进行抑制；

c） 支持家庭网络组网协议时，应支持对新设备进行鉴权认证，如：通过手机 APP 等方式进行鉴权确认；

d） 支持家庭网络组网协议时，应支持使用密钥交换协议交换密钥。

4.2.2 应用业务安全

a） 应支持防止用户做源的组播，禁止用户端口向WAN侧发出IGMP Query和组播数据报文；

b） 语音业务应终结于智能网关（提供Z接口接模拟话机），语音业务宜与INTERNET接入业务隔离（如用VLAN隔离）。在此配置下，通过LAN侧端口应不能访问语音业务；

c） WLAN功能应支持网络隔离，例如支持访客网络和家庭网络隔离，用于智能设备快连配网和家庭网络隔离等；

4.3 网管安全

4.3.1 身份鉴别与授权

a）对访问控制主体进行唯一性身份标识和鉴别；

b）支持使用口令方式进行鉴别；

c）支持设置口令修改周期；

d）设备出厂时应预置不同的默认口令，或者在用户首次管理设备时提示修改默认口令或设置口令；

e）设置新的用户账户时，该账户可使用的登录方式应默认限制为一种，支持用户增加、关闭、修改账户可使用的登录方式，如：在WEB管理界面下新增一个用户账户，该账户默认仅支持通过指定的方式登录，用户可增加支持其他的方式登录，也可配置关闭已开启的登录方式；

f）同一个用户账户应仅能通过一种方式登录或管理设备；例如：用户A在使用WEB方式登录设备后，在WEB会话有效的同时，用户A不可以通过SSH等其他方式登录或管理设备；

g）支持口令复杂度检查和提醒功能。开启口令复杂度检查功能时，口令长度应不少于8位，且至少包含2种不同类型字符；

h）应对所有用户口令的存储、显示进行非明文处理；

i）应对所有用户鉴别信息的传输进行非明文处理；

j）应不存在预置的且不允许用户更改的默认用户身份鉴别信息，不存在未向设备用户公开的身份鉴别信息；

k）支持登录用户空闲超时锁定或自动退出等措施，以防范会话空闲时间过长；

l）支持对用户身份鉴别信息的抗重放功能；

m）设备进行用户身份鉴别时提供最少的反馈，应避免提示 “用户名错误”、“口令错误”等可能被用于降低口令猜解复杂度的信息；

n）提供登录历史功能，成功登录后设备主动显示该账号最近的登录信息，如登录日期、时间、IP、结果、方式等。

4.3.2 访问控制安全

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，支持权限等级设置和管理，控制不同等级用户对设备的配置、数据的查看和相关功能的执行，阻止非授权用户的操作；

c） 支持访问用户的黑白名单配置。支持 MAC 地址绑定等安全策略管理用户访问受控资源的权限；

d） 基于 MAC 地址的接入控制（包括 LAN 和 WLAN）条目容量应不少于 30 条；

e） 对软件升级、配置修改、日志审计、设备重启等涉及设备安全的重要功能，仅授权用户可使用。

4.3.3 WEB 管理安全

设备支持 WEB 管理方式时：

a） 支持采用 WEB 方式在外部网络对设备进行远程管理时，应支持使用 HTTPS 方式；

b） 采用 WEB 方式在内部网络对设备进行本地管理可支持 HTTPS 方式；

c） 支持 4.3.1 节身份鉴别与授权要求；

d） 支持 4.3.2 节访问控制安全要求。根据用户的分级权限，向不同级别用户展示不同的 WEB 管理页面，如参数配置、数据查看和相关功能执行等；

e） WEB 应用会话标识应具备随机性、唯一性，会话标识有效长度不少于 192 比特，用户名和口令认证通过后应更换会话标识；

f） 具备安全措施防范 Cookie 敏感信息被窃取、Cookie 信息明文传输、Cookie 有效期过长等导致的安全问题；

g） 支持记录 WEB 访问日志。

4.3.4 Telnet 管理安全

设备支持 Telnet 管理方式时：

a） Telnet 功能默认处于关闭状态；

b） 支持 4.3.1 节身份鉴别与授权要求；

c） 支持 4.3.2 节访问控制安全要求；同一个账号应只允许一个账号登录会话，拒绝第二个用户登录会话；

d） 支持记录 telnet 访问日志。

4.3.5 SNMP 管理安全

支持 SNMP 管理方式时：

a） 应支持 SNMPv3 协议；SNMP v3 协议的服务端应默认禁用 noauth_nopriv(不认证也不加密)、auth_nopriv(认证不加密)这两种不安全的接入方式；

b） Community 复杂度符合 4.3.1 节 d）的口令安全要求；

c） 支持 4.3.2 节的访问控制要求；支持配置用户不同权限（只读/读写），支持配置用户可访问的 MIB 库资源（用 OID 前缀标识），支持采用 ACL（访问控制列表）保护 SNMP 访问权限；

d） 应支持 SNMP 访问日志的记录；

e） 认证失败时，支持发送认证失败信息；

f） 支持防范针对 SNMP 的拒绝服务攻击。

4.3.6 TR069 远程管理安全

设备支持 TR069 管理方式时：

a） 应组合使用 SSL/TLS 加密、WWW-Authentication 等方式保证设备与远程管理平台接口安全；

b） 支持记录 TR069 访问日志；

c） TR069 远程管理功能应终结于 WAN 侧；

d） 支持证书认证的方式。

4.3.7 日志审计安全

a） 应提供日志记录功能，对关键操作行为进行记录，关键操作行为应包括：

1） 增加/删除账户；

2） 修改鉴别信息；

3） 修改配置（DNS、IP 地址等）；

4） 用户登录/注销；

5） 重启/关闭设备；

6） 文件上传/下载（支持时）；

7） 用户权限修改（支持时）；

8） 关闭日志审计功能（支持时）；

9） 开启日志审计功能（支持时）；

10）其他（支持时）；

b） 应提供日志信息本地存储功能；当审计存储达到极限或失败时，可采取覆盖旧的日志，保留新的日志等措施，确保最新的日志记录在一定时间内不被破坏；

c） 日志信息本地存储能力应不低于 500 条；

d） 日志记录功能应记录必要的日志要素，主要包括事件发生的日期和时间、主体、类型、结果等；

e） 应采取措施保护用户操作日志，防止日志内容被修改，防止未经授权的操作；

f） 支持日志信息上传到远程管理平台，日志传输应支持加密方式；

g） 应支持本地日志信息断电不丢失。

4.4 应用软件安全

4.4.1 应用安装安全

a） 智能网关仅允许用户通过预置的指定渠道获取应用，采取措施防范用户安装未经认证的应用；

b） 如智能网关设备使用安卓系统，应采取措施防止用户通过 ADB 方式安装未经认证的应用。

4.4.2 应用数据安全

a） 智能网关允许用户通过指定的应用和方式对系统配置信息进行备份和恢复，防范用户通过非指定方式操作配置信息；

b） 设定配置信息文件权限，防范未经授权的下载、篡改、删除等操作；

c） 对设备提供者通过设备收集用户信息数据的，应当向用户明示并取得用户同意。

5 分级安全要求

在不同应用场景和不同的客户需求场景下，不同的智能网关设备支持的安全能力存在差异。分级安全要求根据智能网关设备所支持的安全能力的程度，将设备安全能力自低到高划分为一级、二级、三级，共三个等级。

各安全能力等级对应的安全要求详见表1。

一级：对应智能网关设备第一级安全能力要求，共包含74项安全要求；

二级：对应智能网关设备第二级安全能力要求，共包含108项安全要求；

三级：对应智能网关设备第三级安全能力要求，共包含134项安全要求。

每一等级定义了智能网关设备在相应等级对应的安全能力的最小集合，设备支持该等级标识的所有安全能力才能标识为该级别，对于该级别中标识可能存在不适用情形的项目除外。

表1. 智能网关设备安全技术要求与安全等级对应关系表

安全技术要求				安全等级		
				一级	二级	三级
每级需支持的功能项数量				74	108	134
4.1设备硬件和系统软件安全	4.1.1标识安全	4.1.1a）整机唯一性标识		√	√	√
		4.1.1b）版本唯一性标识		√	√	√
		4.1.1c）禁止明文显示敏感信息			√	√
		4.1.1d）标识物理接口		√	√	√
		4.1.1e）不应存在功能丝印标识				√
	4.1.2接口安全	4.1.2a）隐藏后门安全		√	√	√
		4.1.2b）接入认证机制		√	√	√
		4.1.2c）无线通信网络开关功能		√	√	√
		4.1.2d）远程管理开关功能			√	√
		4.1.2e）WLAN方式接入设备要求	1）	√	√	√
			2）		√	√
			3）			√
	4.1.3硬件安全	4.1.3a）默认禁用调试端口		√	√	√
		4.1.3b）测试芯片接口安全防护				√
	4.1.4开放端口和服务安全	4.1.4a）开放端口功能		√	√	√
		4.1.4b）最小开放原则			√	√
		4.1.4c）禁止绕过认证		√	√	√
		4.1.4d）源端口号应为变化值				√
		4.1.4e）非明文数据传输协议		√	√	√
		4.1.4f）TR069功能隔离		√	√	√
	4.1.5漏洞安全	4.1.5a）认证前提示信息		√	√	√
		4.1.5b）中高危漏洞		√	√	√
		4.1.5c）安全风险告知		√	√	√
		4.1.5d）不包含恶意程序		√	√	√

	4.1.6常见攻击防护安全	4.1.6a）拒绝服务类攻击			√
		4.1.6b）防火墙功能			√
		4.1.6c）支持DMZ		√	√
		4.1.6d）防范用户凭证猜解攻击 1）	√	√	√
		4.1.6d）防范用户凭证猜解攻击 2）		√	√
		4.1.6d）防范用户凭证猜解攻击 3）			√
		4.1.6e）防端口扫描功能		√	√
		4.1.6f）插件资源权限限制功能			√
	4.1.7系统升级安全	4.1.7a）本地或远程升级	√	√	√
		4.1.7b）断网和软件错误可恢复		√	√
		4.1.7c）断电恢复			√
		4.1.7d）数据加密传输	√	√	√
		4.1.7e）禁止非授权用户修改系统	√	√	√
		4.1.7f）完整性保护机制	√	√	√
		4.1.7g）软件镜像主备分区			√
		4.1.7h）升级保护机制	√	√	√
		4.1.7i）升级提示功能	√	√	√
4.2业务功能安全	4.2.1通信协议安全	4.2.1a）防非法报文攻击能力 1）		√	√
		4.2.1a）防非法报文攻击能力 2）			√
		4.2.1b）抑制广播风暴	√	√	√
		4.2.1c）鉴权认证	√	√	√
		4.2.1d）密钥交换协议		√	√
	4.2.2应用业务安全	4.2.2a）防止用户做源的组播	√	√	√
		4.2.2b）语音业务	√	√	√
		4.2.2c）WLAN功能支持网络隔离			√
	4.3.1身份鉴别与授权	4.3.1a）唯一性身份标识和鉴别	√	√	√
		4.3.1b）口令方式鉴别	√	√	√
		4.3.1c）设置口令修改周期			√
		4.3.1d）默认口令	√	√	√
		4.3.1e）登录方式		√	√
		4.3.1f）一个用户唯一登录方式		√	√
		4.3.1g）口令复杂度检查和提醒	√	√	√
		4.3.1h）鉴别信息存储显示非明文处理	√	√	√
		4.3.1i）鉴别信息传输非明文处理		√	√
		4.3.1j）鉴别信息后门安全	√	√	√
		4.3.1k）空闲超时锁定自动退出	√	√	√
		4.3.1l）鉴别信息安全保护		√	√
		4.3.1m）身份鉴别最少反馈	√	√	√
		4.3.1n）登录历史功能			√

4.3网管安全	4.3.2访问控制安全	4.3.2a）访问控制策略		√	√	√
		4.3.2b）分级分权控制机制				√
		4.3.2c）黑白名单配置			√	√
		4.3.2d）MAC地址的接入控制			√	√
		4.3.2e）重要功能访问控制		√	√	√
	4.3.3WEB管理安全Opt	4.3.3a）外部网络支持HTTPS方式		√	√	√
		4.3.3b）支持关闭启用管理方式		√	√	√
		4.3.3c）本地管理支持HTTPS方式				√
		4.3.3d）身份鉴别与授权要求	4.3.1a）	√	√	√
			4.3.1b）	√	√	√
			4.3.1c）			√
			4.3.1d）	√	√	√
			4.3.1e）		√	√
			4.3.1f）		√	√
			4.3.1g）	√	√	√
			4.3.1h）	√	√	√
			4.3.1i）		√	√
			4.3.1j）	√	√	√
			4.3.1k）	√	√	√
			4.3.1l）		√	√
			4.3.1m）	√	√	√
			4.3.1n）			√
		4.3.3e）访问控制安全要求	4.3.2a）	√	√	√
			4.3.2b）			√
			4.3.2c）		√	√
			4.3.2d）		√	√
			4.3.2e）	√	√	√
		4.3.3f）WEB应用会话标识			√	√
		4.3.3g）WEB访问日志		√	√	√
	4.3.4Telnet管理安全Opt	4.3.4a）默认关闭状态		√	√	√
		4.3.4b）身份鉴别与授权要求	4.3.1a）	√	√	√
			4.3.1b）	√	√	√
			4.3.1c）			√
			4.3.1d）	√	√	√
			4.3.1e）		√	√
			4.3.1f）		√	√
			4.3.1g）	√	√	√
			4.3.1h）	√	√	√
			4.3.1i）		√	√

			4.3.1j）	√	√	√
			4.3.1k）	√	√	√
			4.3.1l）		√	√
			4.3.1m）	√	√	√
			4.3.1n）			√
		4.3.4c）访问控制安全要求	4.3.2a）	√	√	√
			4.3.2b）			√
			4.3.2c）		√	√
			4.3.2d）		√	√
			4.3.2e）	√	√	√
		4.3.4d）记录telnet访问日志		√	√	√
	4.3.5SNMP管理安全[Opt]	4.3.5a）SNMP管理方式		√	√	√
		4.3.5b）Community复杂度		√	√	√
		4.3.5c）访问控制要求		√	√	√
		4.3.5d）SNMP访问日志		√	√	√
		4.3.5e）认证失败信息			√	√
		4.3.5f）防拒绝服务攻击			√	√
	4.3.6TR069远程管理安全[Opt]	4.3.6a）接口安全				√
		4.3.6b）记录访问日志				√
		4.3.6c）管理功能终结				√
		4.3.6d）证书认证功能				√
	4.3.7日志审计安全	4.3.7a）日志记录功能	1）~5）	√	√	√
			6）~10）[Opt]		√	√
		4.3.7b）日志本地存储		√	√	√
		4.3.7c）日志存储能力				√
		4.3.7d）日志要素		√	√	√
		4.3.7e）操作日志保护		√	√	√
		4.3.7f）日志信息上传			√	√
		4.3.7g）日志断电不丢失		√	√	√
4.4应用软件安全	4.4.1应用安装安全	4.4.1a）防范安装未经认证的应用		√	√	√
		4.4.1b）安卓系统应用安全		√	√	√
	4.4.2应用数据安全	4.4.2a）操作配置信息		√	√	√
		4.4.2b）配置信息文件权限			√	√
		4.4.2c）收集用户信息数据		√	√	√

[注1:]表格中标注[Opt]的表示该项目可能存在不适用情况。在标注[Opt]的项目中，如设备未提供项目所述功能，则属于不适用的情形。例如某设备未提供Telnet登录功能，则“4.3.4Telnet管理安全”整项要求不适用于该设备。

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
2018-10-31	V1.0.0	标准草案
2019-01-09	V2.0.0	根据征求意见稿讨论的意见和编制组意见进行了修改
2019-01-15	V3.0.0	根据报批稿讨论的意见进行了修改

附　录　B
（资料性附录）
智能网关典型应用场景示意图

智能网关设备通常用在家庭或小型企业的网络出入口，如图1所示。图1中左边虚线框里包括云服务平台和集中管理平台两种典型的网络侧平台，云服务平台目前主要在智能家居场景中使用，集中管理平台目前主要在运营商接入场景中使用。

典型的智能网关设备包含基于安卓系统、Linux系统等开源操作系统平台，可进行插件/软件的安装和运行，支持路由、WLAN接入、IPTV、光纤接入等部分功能。智能网关典型使用场景主要包括两类，一类是运营商提供网络接入服务时，由运营商为家庭或小型企业提供的网关设备，这种情况下设备的所有权和控制权通常属于运营商，设备用户指的是运营商，例如运营商O批量购买了设备制造企业M的智能网关设备，通过提供网络接入服务部署设备入户，设备企业M的用户是运营商O；另一类是在智能家居场景下，通常是最终用户直接向设备制造企业购买智能网关设备后部署在家里，这种情况下设备的所有权和控制权通常属于最终用户，设备用户指的是最终使用设备的个人。

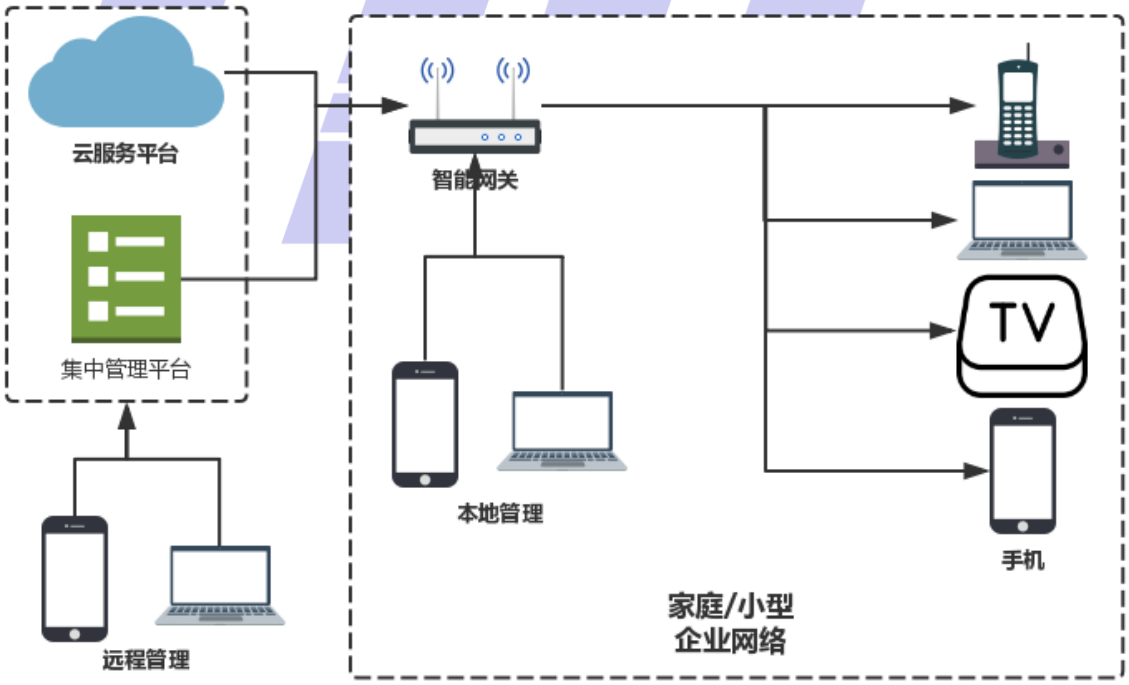

图1. 智能网关的典型应用场景

附 录 B
（资料性附录）
典型功能丝印标识

网络产品涉及的典型功能丝印标识包括：

1)...UART口
2)...IIC接口（SCL、SDA）
3)...SPI总线接口（SDI、SDO、SCLK、CS）
4)...JTAG调试接口
5)...SW调试接口
6)...网卡PYH接口
7)...RESET
8)...USB接口
9)...天线接口ANT
10).其他

此处列出的是较为常见的功能丝印标识，设备可能存在仅涉及上述部分标识的情况，对于未涉及的接口应按照不适用处理。

参 考 文 献