ICS 33.050
M 30

团　体　标　准

T/TAF 046-2019

智能网关设备安全测试方法

Security testing methods for intelligent gateway devices

2019-11-20 发布　　2019-11-20 实施

电信终端产业协会　发布

目　次

前　言

本标准按照 GB/T 1.1-2009给出的规则编写。

本标准中的某些内容可能涉及专利。本标准的发布机构不承担识别这些专利的责任。

本标准由电信终端产业协会（TAF）提出并归口。

本标准起草单位：中国信息通信研究院、烽火通信科技股份有限公司、华为技术有限公司、新华三技术有限公司、启明星辰信息技术集团股份有限公司、中兴通讯股份有限公司、锐捷网络股份有限公司、北京辰信领创信息技术有限公司、联想（北京）有限公司、深圳市友华通信技术有限公司、威尔克通信实验室。

本标准主要起草人：张治兵、张亚薇、吴国燕、叶郁柏、童天予、苏燕谨、刘鑫、张瑛、王淳、陈鹏、王通源、李汝鑫、李霄鹏、罗丹、袁玉东。

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、网管等方面的安全测试方法。

智能网关设备安全测试方法

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、网管等方面的安全测试方法。

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

T/TAF 040-2019 智能网关设备安全技术要求

3 术语和定义

GB/T 25069-2010和T/TAF 040-2019中界定的术语和定义适用于本文件。

4 测试环境

测试环境如图1至图4所示。

图1 测试环境1

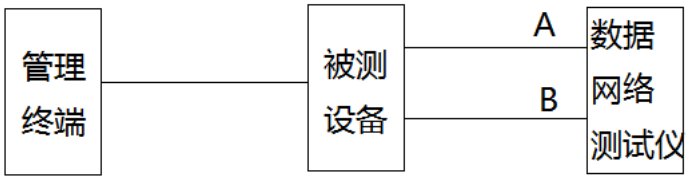


图2 测试环境2

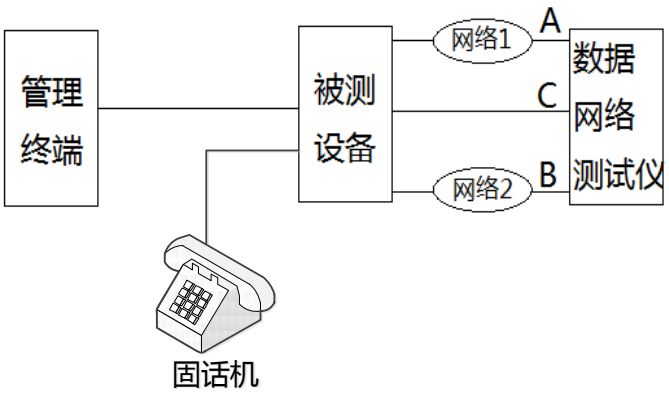


图3 测试环境3

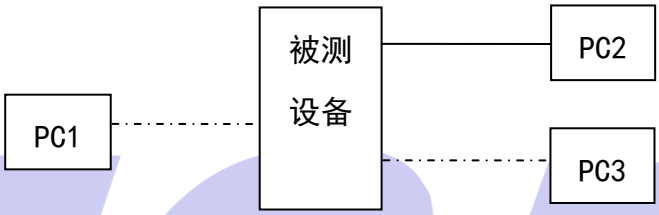


图4 测试环境4

管理终端用来对被测设备进行远程操作，包括PC、手机等设备；扫描工具用来对被测设备执行端口扫描、漏洞扫描等操作；数据网络测试仪用来构造测试相关的背景流量和攻击流量。

5 安全测试要求

5.1 设备硬件和系统软件安全

5.1.1 标识安全

测试编号： 1
测试项目：标识安全
分项目：整机唯一性标识测试
技术要求：《智能网关设备安全技术要求》4.1.1a）
测试配置：测试环境 1
测试过程： 1） 检查被测设备，查看是否具有整机唯一性标识码。
预期结果： 1） 步骤 1 中，被测设备具有整机唯一性标识码。
判定原则：测试结果应与预期结果相符，否则不符合要求。

测试编号： 2
测试项目：标识安全
分项目：版本唯一性标识测试

技术要求：《智能网关设备安全技术要求》4.1.1b）
测试配置：测试环境 1
测试过程： 1） 检查被测设备不同版本的软件/固件、补丁包/升级包的唯一性标识； 2） 检查被测设备厂家历史版本说明（官网链接或有说明历史版本的其他材料）。
预期结果： 1） 步骤 1 中，不同版本软件/固件、补丁包/升级包的版本标识存在差别，可唯一标识具体的版本； 2） 步骤 2 中，相关历史版本有记录可查。
判定原则：测试结果应与预期结果相符，否则不符合要求。

测试编号： 3
测试项目：标识安全
分项目：敏感信息安全测试
技术要求：《智能网关设备安全技术要求》4.1.1c）
测试配置：测试环境 1
测试过程： 1） 检查被测设备 web、Telnet、APP 等操作界面内容，查看是否存在明文显示密钥、口令、会话标识等敏感信息； 2） 检查系统输出的日志、调试信息，查看是否存在明文显示密钥、口令、会话标识等敏感信息； 3） 使用错误用户名/口令登录，或者执行其他可能的异常操作，查看错误提示是否存在明文显示密钥、口令、会话标识等敏感信息。
预期结果： 1） 步骤 1、2、3 中，操作界面、日志、调试信息和错误提示中都不应存在明文显示密钥、口令、会话标识等敏感信息。
判定原则：测试结果应与预期结果相符，否则不符合要求。

测试编号： 4
测试项目：标识安全
分项目：物理接口标识安全
技术要求：《智能网关设备安全技术要求》4.1.1d）
测试配置：测试环境 1
测试过程： 1） 检查被测设备每一个物理接口及相关说明材料。
预期结果： 1） 步骤 1 中，每一个物理接口均有标识，且有功能说明，不应存在未向用户声明的物理接口。
判定原则：测试结果应与预期结果相符，否则不符合要求。

测试编号： 5
测试项目：标识安全
分项目：丝印标识安全测试

技术要求：《智能网关设备安全技术要求》4.1.1e）
测试配置：测试环境 1
测试过程： 1）检查被测设备的相关材料，确认是否提供关键安全模块列表； 2）检查被测设备外观，查看关键安全模块上是否有印刷或张贴丝印标识； 3）检查被测设备内部部件，查看关键安全模块上是否有印刷或张贴丝印标识。
预期结果： 1） 步骤 2、3 中，关键安全模块上不应印刷或张贴丝印标识。
判定原则：测试结果应与预期结果相符，否则不符合要求。

5.1.2 接口安全

测试编号： 6
测试项目：接口安全
分项目：隐藏后门安全测试
技术要求：《智能网关设备安全技术要求》4.1.2a）
测试配置：测试环境 1
测试过程： 1） 检查被测设备身份鉴别相关说明材料，查看是否说明不存在可绕过正常认证机制直接进入到系统的隐秘通道，同时也不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。
预期结果： 1） 步骤 1 中，应说明被测设备存在的默认账号清单（如有），除此之外还应说明不存在可绕过正常认证机制直接进入到系统的隐秘通道，同时也不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。
判定原则：测试结果应与预期结果相符，否则不符合要求。

测试编号： 7
测试项目：接口安全
分项目：接入认证机制测试
技术要求：《智能网关设备安全技术要求》4.1.2b）
测试配置：测试环境 1
测试过程： 1） 检查被测设备访问方式相关材料，查看所有可对设备进行管理的外部通信接口； 2） 尝试通过各种外部通信接口登录被测设备。
预期结果： 1） 步骤 2 中，登录被测设备的所有外部通信接口都需要进行接入认证。
判定原则：测试结果应与预期结果相符，否则不符合要求。

测试编号： 8
测试项目：接口安全
分项目：无线通信网络开关功能测试

技术要求：《智能网关设备安全技术要求》4.1.2c）
测试配置：测试环境 1
测试过程： 1） 登录被测设备； 2） 开启无线通信网络如 WLAN、蓝牙、蜂窝、Zigbee 等接口，通过这些接口建立数据连接，进行数据传输； 3） 关闭无线通信网络如 WLAN、蓝牙、蜂窝、Zigbee 等接口，通过这些接口建立数据连接，进行数据传输。
预期结果： 1） 步骤 2、3 中，设备支持对无线通信网络如 WLAN、蓝牙、蜂窝、Zigbee 等接口进行开关控制； 2） 步骤 2 中，数据可正常传输； 3） 步骤 3 中，无法连接，数据不可传输。
判定原则：测试结果应与预期结果相符，否则不符合要求。

测试编号： 9
测试项目：接口安全
分项目：远程管理开关功能测试
技术要求：《智能网关设备安全技术要求》4.1.2d）
测试配置：测试环境 1
测试过程： 1） 登录被测设备； 2） 开启设备支持的任意一种 WAN 口远程管理方式； 3） 在 WAN 侧使用打开的远程管理方式进行操作； 4） 关闭打开的 WAN 口远程管理方式； 5） 在 WAN 侧使用关闭的远程管理方式进行操作； 6） 对厂商声明的其他 WAN 口远程管理方式执行步骤 2～5。
预期结果： 1） 步骤 2~6 中，设备支持对 WAN 口远程管理方式进行开关控制，打开之后，可对设备进行远程管理，关闭之后，不可进行远程管理。
判定原则：测试结果应与预期结果相符，否则不符合要求。

测试编号： 10
测试项目：接口安全
分项目：WLAN 认证加密测试
技术要求：《智能网关设备安全技术要求》4.1.2e）
测试配置：测试环境 3
测试过程： 1） WLAN 通过不同认证方式（WPA2/PSK/WPA3 等)登录被测设备； 2） 认证成功之后，检查所使用的密码算法。
预期结果： 1） 步骤 2 中，设备支持使用 WPA2/PSK 等方式进行安全认证； 2） 步骤 2 中，设备支持 AES-128、SM4 等至少一种安全强度较高的密码算法；

3） 步骤 2 中，设备支持 WPA3，支持 AES-192 及以上强度的密码算法。
判定原则：测试结果应与预期结果 1 相符，满足一级要求； 测试结果应与预期结果 1、2 相符，满足二级要求； 测试结果应与预期结果 1、2、3 相符，满足三级要求； 否则不符合要求。

5.1.3 硬件安全

测试编号： 11
测试项目：硬件安全
分项目：调试端口测试
技术要求：《智能网关设备安全技术要求》4.1.3a）
测试配置：测试环境 1
测试过程： 1） 提供调试接口列表，检查被测设备相关声明材料是否说明所有用于生产、调试和维修的接口要求默认禁用且用户不可激活（配置），禁用或去掉（不存在）易被攻击者利用的调试功能或组件； 2） 登录被测设备，查看是否存在可以配置生产、调试和维修的接口，是否存在调试功能或组件。
预期结果： 1） 步骤 1 中，被测设备提供了调试接口列表，有相关声明材料说明所有用于生产、调试和维修的接口要求默认禁用且用户不可激活（配置），禁用或去掉（不存在）易被攻击者利用的调试功能或组件； 2） 步骤 2 中，未发现可以配置生产、调试和维修的接口及调试功能或组件。
判定原则：测试结果应与预期结果相符，否则不符合要求

测试编号： 12
测试项目：硬件安全
分项目：芯片接口安全测试
技术要求：《智能网关设备安全技术要求》4.1.3b）
测试配置：测试环境 1
测试过程： 1） 检查设备相关说明材料，查看是否说明 JTAG 等测试或调试接口的安全防护机制，典型的防护机制包括标识隐匿、接入认证等。
预期结果： 1） 步骤 1 中，相关材料应说明 JTAG 等测试或调试芯片接口具备的安全防护机制。
判定原则：测试结果应与预期结果相符，否则不符合要求

5.1.4 开放端口和服务安全

测试编号： 13
测试项目：开放端口和服务安全

分项目：开放端口功能测试
技术要求：《智能网关设备安全技术要求》4.1.4a）
测试配置：测试环境 1
测试过程： 1） 查看被测设备默认开放端口说明材料（可以是配置手册、用户手册或交互页面）； 2） 通过端口扫描工具对设备（分别选取 LAN 侧/WAN 侧的一个接口）进行扫描，查看开放端口信息。
预期结果： 1） 步骤 1 中，通过用户手册、交互页面等至少一种方式，提供所有默认开放端口相关的列表； 2） 步骤 2 中，扫描发现的开放端口信息应包含在说明材料中。
判定原则：测试结果应与预期结果相符，否则不符合要求

测试编号： 14
测试项目：开放端口和服务安全
分项目：默认端口测试
技术要求：《智能网关设备安全技术要求》4.1.4b）
测试配置：测试环境 1
测试过程： 1）将被测设备恢复出厂设置； 2）登录被测设备，查看 Telnet、FTP、SSH v1.x、tftp、SNMPv2c 等不安全协议是否关闭； 3）使用端口扫描软件扫描被测设备。
预期结果： 1） 步骤 2 中，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； 2） 步骤 3 中，通过扫描未发现 Telnet、FTP、SSH v1.x、tftp、SNMPv2c 等不安全协议端口开放，与默认配置一致。
判定原则：测试结果应与预期结果相符，否则不符合要求

测试编号： 15
测试项目：开放端口和服务安全
分项目：不存在可绕过认证的服务端口测试
技术要求：《智能网关设备安全技术要求》4.1.4c）
测试配置：测试环境 1
测试过程： 1） 检查被测设备用户手册等相关材料，查看是否说明除了已提供的服务端口列表，不存在其他可绕过认证进入系统的端口。
预期结果： 1） 步骤 1 中，相关材料应说明除了已提供的服务端口列表，不存在其他可绕过认证进入系统的端口。
判定原则：测试结果应与预期结果相符，否则不符合要求

测试编号： 16
测试项目：开放端口和服务安全
分项目：DNS 源端口号测试
技术要求：《智能网关设备安全技术要求》4.1.4d）
测试配置：测试环境 2
测试过程： 1）登录被测设备，触发多个 DNS 请求报文的发送； 2）在 WAN 侧接口抓取 DNS 请求报文。
预期结果： 1）步骤 2 中，DNS 客户端向服务端请求服务时，源端口号应为变化值。
判定原则：测试结果应与预期结果相符，否则不符合要求

测试编号： 17
测试项目：开放端口和服务安全
分项目：非明文数据传输协议测试
技术要求：《智能网关设备安全技术要求》4.1.4e）
测试配置：测试环境 2
测试过程： 1）在 WAN 侧登录被测设备，并进行管理操作； 2）将 WAN 侧访问报文镜像到测试仪器； 3）在测试仪器上截取分析登录管理报文。
预期结果： 1）步骤 3 中，被测设备使用非明文数据传输协议对设备进行管理。
判定原则：测试结果应与预期结果相符，否则不符合要求

测试编号： 18
测试项目：开放端口和服务安全
分项目：服务安全测试
技术要求：《智能网关设备安全技术要求》4.1.4f）
测试配置：测试环境 1
测试过程： 1） 将被测设备恢复出厂设置； 2） 登录被测设备，查看 WAN 侧开启的服务比如 TR069，并在 WAN 侧开启服务，模拟访问这些服务； 3） 在 LAN 侧访问基于 WAN 侧开启的服务。
预期结果： 1） 步骤 2 中，在 WAN 侧可正常访问基于 WAN 侧开启的服务； 2） 步骤 3 中，在 LAN 侧不可访问基于 WAN 侧开启的服务。
判定原则：测试结果应与预期结果相符，否则不符合要求

5.1.5 漏洞管理安全

测试编号： 19
测试项目：漏洞管理安全
分项目：认证前提示信息测试
技术要求：《智能网关设备安全技术要求》4.1.5a）
测试配置：测试环境 1
测试过程： 1）查看被测设备用户手册，查看支持管理设备的登录方式（如 web/SSH/telnet）； 2）使用每一种登录方式登录设备，查看认证前的提示信息。
预期结果： 1）步骤 2 中，用户登录通过认证前的提示信息不包含设备软件版本等敏感信息。
判定原则：测试结果应与预期结果相符，否则不符合要求

测试编号： 20
测试项目：漏洞管理安全
分项目：中高危漏洞测试
技术要求：《智能网关设备安全技术要求》4.1.5b）
测试配置：测试环境 1
测试过程： 1） 配置被测设备开启声明的服务； 2） 在 LAN 侧、WAN 侧等所有端口使用漏洞扫描软件对设备进行漏洞扫描； 3） 检查漏洞扫描结果，是否存在已公布（90 天之前）的高危和中危漏洞。如果存在，并且有措施可避免漏洞被利用，则采取相关措施（比如修改配置）之后，再次进行漏洞扫描，并确认结果。
预期结果： 1） 步骤 2～3 中，不应存在已公布（90 天之前）的高危和中危漏洞，如果存在，在采取措施后，再次扫描，不再扫出该漏洞。
判定原则：测试结果应与预期结果相符，否则不符合要求

测试编号： 21
测试项目：漏洞管理安全
分项目：安全风险补救测试
技术要求：《智能网关设备安全技术要求》4.1.5c）
测试配置：测试环境 3
测试过程： 1） 检查并确认被测设备厂商提供关于外部报告安全问题的渠道（包括官网、管理 APP 等），确认用户可以方便获知风险报告； 2）检查历史安全问题报告，确认是否及时处理； 3）检查被测设备厂商提供的相关材料是否留存实施相关补救措施和告知用户的记录。
预期结果： 1） 步骤 1 中，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， 2） 步骤 2 中，应说明厂商在发现其设备存在漏洞等风险时，及时采取了补救措施； 3） 步骤 3 中，应说明及时告知用户风险及防范措施，并留存了实施相关补救措施和告知用户

的记录。
判定原则：测试结果应与预期结果相符，否则不符合要求

测试编号： 22
测试项目：漏洞管理安全
分项目：恶意程序测试
技术要求：《智能网关设备安全技术要求》4.1.5d）
测试配置：测试环境 1
测试过程： 1）使用杀毒软件对被测设备厂商提供的预装软件、补丁包/升级包进行恶意软件扫描检测；
预期结果： 1）步骤 1 中，应未发现预装软件、补丁包/升级包中包含恶意程序。
判定原则：测试结果应与预期结果相符，否则不符合要求

5.1.6 常见攻击防护安全

在常见攻击防护安全测试中，由于攻击流量、背景流量、发送流量时长对测试结果会造成影响。通常情况下，可设置背景流量为端口线速率的20%，攻击流量为1000FPS，发送流量时长为30秒，也可以根据设备情况选择测试参数。攻击测试对象选取1个WAN口和LAN口。

测试编号： 233
测试项目：常见攻击防护安全测试
分项目：防 DHCP flood 攻击能力测试（IPv4）
技术要求：《智能网关设备安全技术要求》4.1.6.a）1）
测试配置：测试环境 3
测试过程： 1） 按测试环境连接设备，配置被测设备最高速率各接口的 IPv4 地址； 2） 测试仪表从端口 A 到端口 B 发送背景流量，登录设备查看 CPU/内存等系统资源情况； 3） 从测试仪表端口 C 向被测设备 IPv4 地址发送 DHCP 请求报文； 4） 观察端口 B 接收报文情况，观察设备 CPU/内存等系统资源情况； 5） 停止攻击，尝试通过远程管理方式登录管理设备，观察设备状态，记录设备自动恢复时间。
预期结果： 1） 步骤 3～5 中，被测设备应对超量的 DHCP 报文进行丢弃。设备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。
判定原则：测试结果应与预期结果相符，否则不符合要求
注：攻击流量、背景流量、发送流量时长对测试结果会造成影响。

测试编号： 244
测试项目：常见攻击防护安全测试
分项目：防 DHCPv6 flood 攻击能力测试（IPv6）
技术要求：《智能网关设备安全技术要求》4.1.6.a）1）
测试配置：测试环境 3
测试过程：

1） 按测试环境连接设备，配置被测设备最高速率各接口的 IPv6 地址； 2） 测试仪表从端口 A 到端口 B 发送背景流量，登录设备查看 CPU/内存等系统资源情况； 3） 从测试仪表端口 C 向被测设备 IPv6 地址发送 DHCPv6 请求报文； 4） 观察端口 B 接收报文情况，观察设备 CPU/内存等系统资源情况； 5） 停止攻击，尝试通过远程管理方式登录管理设备，观察设备状态，记录设备自动恢复时间。
预期结果： 1） 步骤 3～5 中，被测设备应对超量的 DHCPv6 报文进行丢弃。设备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。
判定原则：测试结果应与预期结果相符，否则不符合要求
备注：攻击流量、背景流量、发送流量时长对测试结果会造成影响

测试编号： 25
测试项目：常见攻击防护安全测试
分项目：防 DNS flood 攻击测试（IPv4）
技术要求：《智能网关设备安全技术要求》4.1.6.a）2）
测试配置：测试环境 3
测试过程： 1） 按测试环境连接被测设备，配置各接口的 IPv4 地址； 2） 测试仪表从端口 A 到端口 B 发送背景流量，登录设备查看 CPU/内存等系统资源情况； 3） 从测试仪表端口 C 向被测设备 IPv4 地址发送 DNS 请求报文； 4） 观察端口 B 接收报文情况，观察设备 CPU/内存等系统资源情况； 5） 停止攻击，尝试通过远程管理方式登录管理设备，观察设备状态，记录设备自动恢复时间。
预期结果： 1）步骤 3～5 中，被测设备应对超量的 DNS 报文进行丢弃，攻击对背景流量无影响。设备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。
判定原则：测试结果应与预期结果相符，否则不符合要求

测试编号： 26
测试项目：常见攻击防护安全测试
分项目：防 DNS flood 攻击测试（IPv6）
技术要求：《智能网关设备安全技术要求》4.1.6.a）2）
测试配置：测试环境 3
测试过程： 1） 按测试环境连接被测设备，配置各接口的 IPv6 地址； 2） 测试仪表从端口 A 到端口 B 发送背景流量，登录设备查看 CPU/内存等系统资源情况； 3） 从测试仪表端口 C 向被测设备 IPv6 地址发送 DNS 请求报文； 4） 观察端口 B 接收报文情况，观察设备 CPU/内存等系统资源情况； 5） 停止攻击，尝试通过远程管理方式登录管理设备，观察设备状态，记录设备自动恢复时间。
预期结果： 1）步骤 3～5 中，被测设备应对超量的 DNS 报文进行丢弃，攻击对背景流量无影响。设备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

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。
判定原则：测试结果应与预期结果相符，否则不符合要求

测试编号： 27
测试项目：常见攻击防护安全测试
分项目：防 DNS 反射攻击能力测试（IPv4）
技术要求：《智能网关设备安全技术要求》4.1.6.a）2）
测试配置：测试环境 3
测试过程： 1）按测试环境连接被测设备，配置各接口的 IPv4 地址； 2）测试仪表从端口 A 到端口 B 发送背景流量，登录设备查看 CPU/内存等系统资源情况； 3）从测试仪表端口 C 向被测设备 IPv4 地址发送 DNS 应答报文； 4）观察端口 B 接收报文情况，观察设备 CPU/内存等系统资源情况； 5）停止攻击 30 秒后，尝试通过远程管理方式登录管理设备，观察设备状态； 6）设置限制每秒处理的 DNS 应答报文； 7）从测试仪表端口 C 向被测设备 IPv4 地址发送 DNS 应答报文； 8）观察端口 B 接收报文情况，观察设备 CPU/内存等系统资源情况； 9）停止攻击 30 秒后，尝试通过远程管理方式登录管理设备，观察设备状态。
预期结果： 1） 步骤 3～9 中，被测设备应对超量的 DNS 报文进行丢弃，攻击对背景流量无影响，限制每秒处理的 DNS 应答报文之后，设备 CPU/内存等系统资源占用下降。设备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。
判定原则：测试结果应与预期结果相符，否则不符合要求

测试编号： 28
测试项目：常见攻击防护安全测试
分项目：防 DNS 反射攻击能力测试（IPv6）
技术要求：《智能网关设备安全技术要求》4.1.6.a）2）
测试配置：测试环境 3
测试过程： 1）按测试环境连接被测设备，配置各接口的 IPv6 地址； 2）测试仪表从端口 A 到端口 B 发送背景流量，登录设备查看 CPU/内存等系统资源情况； 3）从测试仪表端口 C 向被测设备 IPv6 地址发送 DNS 应答报文； 4）观察端口 B 接收报文情况，观察设备 CPU/内存等系统资源情况； 5）停止攻击 30 秒后，尝试通过远程管理方式登录管理设备，观察设备状态； 6）设置限制每秒处理的 DNS 应答报文； 7）从测试仪表端口 C 向被测设备 IPv6 地址发送 DNS 应答报文； 8）观察端口 B 接收报文情况，观察设备 CPU/内存等系统资源情况； 9）停止攻击 30 秒后，尝试通过远程管理方式登录管理设备，观察设备状态。
预期结果： 1）步骤 3～9 中，被测设备应对超量的 DNS 报文进行丢弃，攻击对背景流量无影响，限制

每秒处理的 DNS 应答报文之后，设备 CPU/内存等系统资源占用下降。设备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。
判定原则：测试结果应与预期结果相符，否则不符合要求

测试编号： 29
测试项目：常见攻击防护安全测试
分项目：防 NTP flood 攻击能力测试（IPv4）
技术要求：《智能网关设备安全技术要求》4.1.6.a）3）
测试配置：测试环境 3
测试过程： 1） 按测试环境连接被测设备，配置各接口的 IPv4 地址； 2） 测试仪表从端口 A 到端口 B 发送背景流量，登录设备查看 CPU/内存等系统资源情况； 3） 从测试仪表端口 C 向被测设备 IPv4 地址发送 NTP 请求报文； 4） 观察端口 B 接收报文情况，观察设备 CPU/内存等系统资源情况； 5） 停止攻击 30 秒后，尝试通过远程管理方式登录管理设备，观察设备状态。
预期结果： 1） 步骤 3～5 中，被测设备应对超量的 NTP 报文进行丢弃，攻击对背景流量无影响。设备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。
判定原则：测试结果应与预期结果相符，否则不符合要求

测试编号： 30
测试项目：常见攻击防护安全测试
分项目：防 NTP flood 攻击能力测试（IPv6）
技术要求：《智能网关设备安全技术要求》4.1.6.a）3）
测试配置：测试环境 3
测试过程： 1） 按测试环境连接被测设备，配置各接口的 IPv6 地址； 2） 测试仪表从端口 A 到端口 B 发送背景流量，登录设备查看 CPU/内存等系统资源情况； 3） 从测试仪表端口 C 向被测设备 IPv6 地址发送 NTP 请求报文； 4） 观察端口 B 接收报文情况，观察设备 CPU/内存等系统资源情况； 5） 停止攻击 30 秒后，尝试通过远程管理方式登录管理设备，观察设备状态。
预期结果： 1) 步骤 3～5 中，被测设备应对超量的 NTP 报文进行丢弃，攻击对背景流量无影响。设备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。
判定原则：测试结果应与预期结果相符，否则不符合要求

测试编号： 31
测试项目：常见攻击防护安全测试
分项目：防 NTP 反射攻击能力测试（IPv4）

技术要求：《智能网关设备安全技术要求》4.1.6.a）3）
测试配置：测试环境 3
测试过程： 1) 按测试环境连接被测设备，配置各接口的 IPv4 地址； 2) 测试仪表从端口 A 到端口 B 发送背景流量，登录设备查看 CPU/内存等系统资源情况； 3) 从测试仪表端口 C 向被测设备 IPv4 地址以发送 NTP 应答报文； 4) 观察端口 B 接收报文情况，观察设备 CPU/内存等系统资源情况； 5) 停止攻击 30 秒后，尝试通过远程管理方式登录管理设备，观察设备状态； 6) 设置限制每秒处理的 NTP 应答报文； 7) 从测试仪表端口 C 向被测设备 IPv4 地址以发送 NTP 应答报文； 8) 观察端口 B 接收报文情况，观察设备 CPU/内存等系统资源情况； 9) 停止攻击 30 秒后，尝试通过远程管理方式登录管理设备，观察设备状态。
预期结果： 1) 步骤 3～9 中，被测设备应对超量的 NTP 报文进行丢弃，攻击对背景流量无影响，限制每秒处理的 NTP 应答报文之后，设备 CPU/内存等系统资源占用下降。设备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。
判定原则：测试结果应与预期结果相符，否则不符合要求

测试编号： 32
测试项目：常见攻击防护安全测试
分项目：防 NTP 反射攻击能力测试（IPv6）
技术要求：《智能网关设备安全技术要求》4.1.6.a）3）
测试配置：测试环境 3
测试过程： 1) 按测试环境连接被测设备，配置各接口的 IPv6 地址； 2) 测试仪表从端口 A 到端口 B 发送背景流量，登录设备查看 CPU/内存等系统资源情况； 3) 从测试仪表端口 C 向被测设备 IPv6 地址发送 NTP 应答报文； 4) 观察端口 B 接收报文情况，观察设备 CPU/内存等系统资源情况； 5) 停止攻击 30 秒后，尝试通过远程管理方式登录管理设备，观察设备状态； 6) 设置限制每秒处理的 NTP 应答报文； 7) 从测试仪表端口 C 向被测设备 IPv6 地址发送 NTP 应答报文； 8) 观察端口 B 接收报文情况，观察设备 CPU/内存等系统资源情况； 9) 停止攻击 30 秒后，尝试通过远程管理方式登录管理设备，观察设备状态。
预期结果： 1) 步骤 3～9 中，被测设备应对超量的 NTP 报文进行丢弃，攻击对背景流量无影响，限制每秒处理的 NTP 应答报文之后，设备 CPU/内存等系统资源占用下降。设备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。
判定原则：测试结果应与预期结果相符，否则不符合要求

测试编号： 33

测试项目：常见攻击防护安全测试
分项目：防 SYN flood 攻击能力测试（IPv4）
技术要求：《智能网关设备安全技术要求》4.1.6.a）4）
测试配置：测试环境 3
测试过程： 1) 按测试环境连接被测设备，配置各接口的 IPv4 地址； 2) 测试仪表从端口 A 到端口 B 发送背景流量，登录设备查看 CPU/内存等系统资源情况； 3) 从测试仪表端口 C 向被测设备 IPv4 地址发送 TCP SYN 报文； 4) 观察端口 B 接收报文情况，观察设备 CPU/内存等系统资源情况； 5) 停止攻击 30 秒后，尝试通过远程管理方式登录管理设备，观察设备状态。
预期结果： 1) 步骤 3～5 中，被测设备应对超量的 TCP SYN 报文进行丢弃，攻击对背景流量无影响。设备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。
判定原则：测试结果应与预期结果相符，否则不符合要求

测试编号： 34
测试项目：常见攻击防护安全测试
分项目：防 SYN flood 攻击能力测试（IPv6）
技术要求：《智能网关设备安全技术要求》4.1.6.a）4）
测试配置：测试环境 3
测试过程： 1) 按测试环境连接被测设备，配置各接口的 IPv6 地址； 2) 测试仪表从端口 A 到端口 B 发送背景流量，登录设备查看 CPU/内存等系统资源情况； 3) 从测试仪表端口 C 向被测设备 IPv6 地址发送 TCP SYN 报文； 4) 观察端口 B 接收报文情况，观察设备 CPU/内存等系统资源情况； 5) 停止攻击 30 秒后，尝试通过远程管理方式登录管理设备，观察设备状态。
预期结果： 1) 步骤 3～5 中，被测设备应对超量的 TCP SYN 报文进行丢弃，攻击对背景流量无影响。设备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。
判定原则：测试结果应与预期结果相符，否则不符合要求

测试编号： 35
测试项目：常见攻击防护安全测试
分项目：根据源 MAC 地址、目的 MAC 地址进行报文过滤测试
技术要求：《智能网关设备安全技术要求》4.1.6.b）1）
测试配置：测试环境 2
测试过程： 1) 登录被测设备，设置过滤源 MAC 地址报文； 2) 在测试仪器端口 A 发送以被过滤的 MAC 为源 MAC 的报文，在测试仪器端口 B 观察（A 和 B 分属 LAN 侧和 WAN 侧）； 3) 删除过滤源 MAC 地址报文设置；

4) 在测试仪器端口 A 发送以被过滤的 MAC 为源 MAC 的报文，在测试仪器端口 B 观察； 5) 设置过滤目的 MAC 地址报文； 6) 在测试仪器端口 A 发送以被过滤的 MAC 为目的 MAC 的报文，在测试仪器端口 B 观察（端口 B 和端口 A 都在 LAN 侧）； 7) 删除过滤目的 MAC 地址报文设置； 8) 在测试仪器端口 A 发送以被过滤的 MAC 为目的 MAC 的报文，在测试仪器端口 B 观察。
预期结果： 1) 步骤 1~8 中，设备根据源 MAC 地址、目的 MAC 地址进行报文过滤。开启过滤功能，则对应源 MAC 地址、目的 MAC 地址的报文被丢弃，取消过滤功能，则对应源 MAC 地址、目的 MAC 的报文被正常转发。
判定原则：测试结果应与预期结果相符，否则不符合要求

测试编号： 256
测试项目：常见攻击防护安全测试
分项目：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测试（IPv4）
技术要求：《智能网关设备安全技术要求》4.1.6.b）2）
测试配置：测试环境 2
测试过程： 1) 登录被测设备，设置过滤源 IP 地址（IPv4）报文； 2) 在测试仪器端口 A 发送以被过滤的 IP 为源 IP 的报文，在测试仪器端口 B 观察； 3) 删除过滤源 IP 地址报文设置； 4) 在测试仪器端口 A 发送以被过滤的 IP 为源 IP 的报文，在测试仪器端口 B 观察； 5) 设置过滤源 IP 地址范围报文； 6) 在测试仪器端口 A 发送以在被过滤范围的 IP 和不在过滤范围的 IP 为源 IP 的报文，在测试仪器端口 B 观察； 7) 删除过滤源 IP 地址范围报文； 8) 在测试仪器端口 A 发送以在被过滤范围的 IP 和不在过滤范围的 IP（比如 1.1.1.200）为源 IP 的报文，在测试仪器端口 B 观察； 9) 设置过滤目的 IP 地址报文； 10) 在测试仪器端口 A 发送以被过滤的 IP 为目的 IP 的报文，在测试仪器端口 B 观察； 11) 删除过滤目的 IP 地址报文设置； 12) 在测试仪器端口 A 发送以被过滤的 IP 为目的 IP 的报文，在测试仪器端口 B 观察； 13) 设置过滤目的 IP 地址范围报文； 14) 在测试仪器端口 A 发送以在被过滤范围的 IP 和不在过滤范围的 IP 为目的 IP 的报文，在测试仪器端口 B 观察； 15) 删除过滤目的 IP 地址范围报文； 16) 在测试仪器端口 A 发送以在被过滤范围的 IP 和不在过滤范围的 IP 为目的 IP 的报文，在测试仪器端口 B 观察。
预期结果： 1) 步骤 1~16 中，设备根据源 IP 地址及范围段、目的 IP 地址及范围段进行报文过滤。开启过滤功能，则对应源 IP 地址或源 IP 地址在被过滤源地址范围内、目的 IP 地址或目的地址在被过滤的目的地址范围内的报文被丢弃，不在被过滤源目的 IP 范围内的报文正常转

发，取消过滤功能，则对应源 IP 地址或源 IP 地址在被过滤源地址范围内、目的 IP 地址或目的地址在被过滤的目的地址范围内的报文被正常转发。
判定原则：测试结果应与预期结果相符，否则不符合要求

测试编号： 267
测试项目：常见攻击防护安全测试
分项目：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测试（IPv6）
技术要求：《智能网关设备安全技术要求》4.1.6.b）2）
测试配置：测试环境 2
测试过程： 1) 登录被测设备，设置过滤源 IP 地址（IPv6）报文； 2) 在测试仪器端口 A 发送以被过滤的 IP 为源 IP 的报文，在测试仪器端口 B 观察； 3) 删除过滤源 IP 地址报文设置； 4) 在测试仪器端口 A 发送以被过滤的 IP 为源 IP 的报文，在测试仪器端口 B 观察； 5) 设置过滤源 IP 地址范围报文； 6) 在测试仪器端口 A 发送以在被过滤范围的 IP 和不在过滤范围的 IP 为源 IP 的报文，在测试仪器端口 B 观察； 7) 删除过滤源 IP 地址范围报文； 8) 在测试仪器端口 A 发送以在被过滤范围的 IP 和不在过滤范围的 IP 为源 IP 的报文，在测试仪器端口 B 观察； 9) 设置过滤目的 IP 地址报文； 10) 在测试仪器端口 A 发送以被过滤的 IP 为目的 IP 的报文，在测试仪器端口 B 观察； 11) 删除过滤目的 IP 地址报文设置； 12) 在测试仪器端口 A 发送以被过滤的 IP 为目的 IP 的报文，在测试仪器端口 B 观察； 13) 设置过滤目的 IP 地址范围报文； 14) 在测试仪器端口 A 发送以在被过滤范围的 IP 和不在过滤范围的 IP 为目的 IP 的报文，在测试仪器端口 B 观察； 15) 删除过滤目的 IP 地址范围报文； 16) 在测试仪器端口 A 发送以在被过滤范围的 IP 和不在过滤范围的 IP 为目的 IP 的报文，在测试仪器端口 B 观察。
预期结果： 1) 步骤 1~16 中，设备根据源 IP 地址及范围段、目的 IP 地址及范围段进行报文过滤。开启过滤功能，则对应源 IP 地址或源 IP 地址在被过滤源地址范围内、目的 IP 地址或目的地址在被过滤的目的地址范围内的报文被丢弃，不在被过滤源目的 IP 范围内的报文正常转发，取消过滤功能，则对应源 IP 地址或源 IP 地址在被过滤源地址范围内、目的 IP 地址或目的地址在被过滤的目的地址范围内的报文被正常转发。
判定原则：测试结果应与预期结果相符，否则不符合要求

测试编号： 38
测试项目：常见攻击防护安全测试
分项目：根据 IP 源端口及范围段、目的端口及范围段进行报文过滤测试
技术要求：《智能网关设备安全技术要求》4.1.6.b）3）
测试配置：测试环境 2

测试过程： 1) 登录被测设备，设置过滤源 IP 端口（包括 IPv4 和 IPv6)报文； 2) 在测试仪器端口 A 发送以被过滤的端口为源端口的报文，在测试仪器端口 B 观察； 3) 删除过滤源 IP 端口报文设置； 4) 在测试仪器端口 A 发送以被过滤的端口为源端口的报文，在测试仪器端口 B 观察； 5) 设置过滤源 IP 端口范围报文； 6) 在测试仪器端口 A 发送以在被过滤范围的端口和不在过滤范围的端口为源端口的报文，在测试仪器端口 B 观察； 7) 删除过滤源 IP 端口范围报文； 8) 在测试仪器端口 A 发送以在被过滤范围的端口和不在过滤范围的端口为源端口的报文，在测试仪器端口 B 观察； 9) 设置过滤目的 IP 端口报文； 10) 在测试仪器端口 A 发送以被过滤的端口为目的端口的报文，在测试仪器端口 B 观察； 11) 删除过滤目的 IP 端口报文设置； 12) 在测试仪器端口 A 发送以被过滤的端口为目的端口的报文，在测试仪器端口 B 观察； 13) 设置过滤目的 IP 端口范围报文； 14) 在测试仪器端口 A 发送以在被过滤范围的端口和不在过滤范围的端口为目的端口的报文，在测试仪器端口 B 观察； 15) 删除过滤目的 IP 端口范围报文； 16) 在测试仪器端口 A 发送以在被过滤范围的端口和不在过滤范围的端口为目的端口的报文，在测试仪器端口 B 观察。
预期结果： 1) 步骤 1~16 中，设备根据源端口及范围段、目的端口及范围段进行报文过滤。开启过滤功能，则对应源端口或源端口在被过滤源端口范围内、目的端口或目的端口在被过滤的目的端口范围内的报文被丢弃，不在被过滤源目的端口范围内的报文正常转发，取消过滤功能，则对应源端口或源端口在被过滤源端口范围内、目的端口或目的端口在被过滤的目的端口范围内的报文被正常转发。
判定原则：测试结果应与预期结果相符，否则不符合要求

测试编号： 279
测试项目：常见攻击防护安全测试
分项目：根据 IP 包的传输层协议类型进行报文过滤测试
技术要求：《智能网关设备安全技术要求》4.1.6.b）4）
测试配置：测试环境 2
测试过程： 1) 登录被测设备，设置基于传输层协议（比如 TCP/UDP/ICMP)过滤规则（包括 IPv4 和 IPv6）； 2) 在测试仪器端口 A 发送以被过滤的传输层协议（比如 TCP/UDP/ICMP)的报文，在测试仪器端口 B 观察； 3) 删除过滤基于传输层协议（比如 TCP/UDP/ICMP)设置，在测试仪器端口 A 发送以被过滤的传输层协议（比如 TCP/UDP/ICMP)的报文，在测试仪器端口 B 观察。
预期结果： 1) 步骤 1~3 中，设备根据传输层协议进行报文过滤。开启过滤功能，则对应传输层协议的报

文被丢弃，取消过滤功能，则对应传输层协议的报文被正常转发。
判定原则：测试结果应与预期结果相符，否则不符合要求

测试编号： 40
测试项目：常见攻击防护安全测试
分项目：选择处理模式的测试
技术要求：《智能网关设备安全技术要求》4.1.6.b）5）
测试配置：测试环境 2
测试过程： 1) 登录设备，查看设备是否支持对匹配规则的报文进行处理模式的选择； 2) 查看设备是否对匹配规则的报文的处理模式提供允许和禁止 2 种选项，且默认为禁止转发模式。
预期结果： 1) 步骤 1 中，设备支持对匹配规则的报文进行处理模式的选择； 2) 步骤 2 中，设备对匹配规则的报文的处理模式提供允许和禁止 2 种选项，且默认为禁止转发模式。
判定原则：测试结果应与预期结果相符，否则不符合要求

测试编号： 41
测试项目：常见攻击防护安全测试
分项目：根据 IP 包的传输层协议类型进行报文过滤测试（IPv4）
技术要求：《智能网关设备安全技术要求》4.1.6.b） 6）
测试配置：测试环境 2
测试过程： 1) 登录被测设备，设置基于 TOS/DSCP 值（比如 TOS 为 2，DSCP 为 10)过滤报文； 2) 在测试仪器端口 A 发送以被过滤的 TOS/DSCP 值（比如 TOS 为 2，DSCP 为 10)的报文，在测试仪器端口 B 观察； 3) 删除过滤基于 TOS/DSCP 值（比如 TOS 为 2，DSCP 为 10)设置，在测试仪器端口 A 发送以被过滤的 TOS/DSCP 值（比如 TOS 为 2，DSCP 为 10)的报文，在测试仪器端口 B 观察。
预期结果： 1) 步骤 1~3 中，设备根据 TOS/DSCP 值进行报文过滤。开启过滤功能，则对应 TOS/DSCP 值的报文被丢弃，取消过滤功能，则对应 TOS/DSCP 值的报文被正常转发。
判定原则：测试结果应与预期结果相符，否则不符合要求

测试编号： 42
测试项目：常见攻击防护安全测试
分项目：根据 IP 包的传输层协议类型进行报文过滤测试（IPv6）
技术要求：《智能网关设备安全技术要求》4.1.6.b） 6）
测试配置：测试环境 2
测试过程： 1) 登录被测设备，设置基于 Traffic Class 值过滤报文； 2) 在测试仪器端口 A 发送以被过滤的 Traffic Class 值的报文，在测试仪器端口 B 观察；

3) 删除过滤基于 Traffic Class 值设置，在测试仪器端口 A 发送以被过滤的 Traffic Class 值的报文，在测试仪器端口 B 观察。
预期结果： 1) 步骤 1~3 中，设备根据 Traffic Class 值进行报文过滤。开启过滤功能，则对应 Traffic Class 值的报文被丢弃，取消过滤功能，则对应 Traffic Class 值的报文被正常转发。
判定原则：测试结果应与预期结果相符，否则不符合要求

测试编号： 43
测试项目：常见攻击防护安全测试
分项目：DMZ 功能测试
技术要求：《智能网关设备安全技术要求》4.1.6.c）
测试配置：测试环境 2
测试过程： 1) 登录被测设备，设置基于端口映射 DMZ 功能（比如外网映射端口为 8023，内网为主机 23 端口）； 2) 在测试仪器端口 A 发送目的端口为外网映射端口（比如 8023）的报文，在测试仪器端口 B 观察； 3) 设置基于整机映射 DMZ 功能； 4) 在测试仪器端口 A 发送任一个目的端口（比如 9021）的报文，在测试仪器端口 B 观察。
预期结果： 1) 在步骤 2 中，可以观察到对应目的端口的报文被转成指定内网主机的指定端口（比如 8023 转成 23）； 2） 在步骤 4 中，可以观察到对应目的端口的报文被转成指定内网主机的相同端口（比如 9021 转成 9021）。
判定原则：测试结果应与预期结果相符，否则不符合要求

测试编号： 44
测试项目：常见攻击防护安全测试
分项目：用户身份鉴别失败处理功能测试
技术要求：《智能网关设备安全技术要求》4.1.6.d）1）2）
测试配置：测试环境 1
测试过程： 1) 登录被测设备，设置非法登录尝试次数，设置锁定时间； 2) 使用错误用户/密码登录设备多次，之后使用正确用户/密码登录； 3) 等锁定时间之后，再次登录。
预期结果： 1) 在步骤 2 中，连续非法登录尝试次数达到限制时，锁定对应用户的 IP 地址，直接拒绝再次登录； 2) 在步骤 3 中，等锁定时间之后，允许再次登录。
判定原则：测试结果应与预期结果相符，否则不符合要求

测试编号： 45

测试项目：常见攻击防护安全测试
分项目：用户登录会话数量限制功能测试
技术要求：《智能网关设备安全技术要求》4.1.6.d）3）
测试配置：测试环境 1
测试过程： 1) 登录被测设备，设置登录会话数量（比如为 3）； 2) 使用多个终端（超过设置数量，比如 5）同时登录。
预期结果： 1）在步骤 2 中，只允许指定数量的终端正常登录，超过指定数量的终端登录被拒绝。
判定原则：测试结果应与预期结果相符，否则不符合要求

测试编号： 46
测试项目：常见攻击防护安全测试
分项目：端口防扫描功能测试
技术要求：《智能网关设备安全技术要求》4.1.6.e）
测试配置：测试环境 1
测试过程： 1) 登录被测设备，确认设备未启用端口防扫描功能，开启部分协议端口（比如 SSH、SNMP 等）； 2) 使用端口扫描工具对 WAN 侧和 LAN 侧在设定条件下进行扫描，遍历 TCP、UDP 服务端口； 3) 在设备上，开启端口防扫描功能； 4） 再次使用端口扫描工具对 WAN 侧和 LAN 侧在设定条件下进行扫描，遍历 TCP、UDP 服务端口，同时访问开放的端口（比如 SSH、SNMP 等）。
预期结果： 1) 在步骤 2、4 中，没开启防端口扫描功能之前，可以扫描到开放的端口，开启防端口扫描功能之后，无法扫描到开放的端口，但开放的端口可以正常访问。
判定原则：测试结果应与预期结果相符，否则不符合要求
注：设定条件根据设备关于该功能的描述进行定义。

测试编号： 47
测试项目：常见攻击防护安全测试
分项目：插件资源权限限制功能测试
技术要求：《智能网关设备安全技术要求》4.1.6.f）
测试配置：测试环境 2
测试过程： 1) 登录被测设备，下载并安装设备支持的插件； 2) 通过远程管理（如 TR069、智能平台）对设备进行控制，关闭插件。
预期结果： 1) 在步骤 2 中，能够通过管理平台对插件进行控制（关闭插件）。
判定原则：测试结果应与预期结果相符，否则不符合要求

5.1.7 系统升级安全

测试编号： 48
测试项目：系统升级安全
分项目：本地升级测试
技术要求：《智能网关设备安全技术要求》4.1.7a）
测试配置：测试环境 1
测试过程： 1）下载升级软件到本地； 2）登录被测设备，选择本地软件进行升级； 3）升级成功之后重启设备，检查是否升级成功。
预期结果： 1）步骤 2～3 中，支持采用本地方式进行软件升级。
判定原则：测试结果应与预期结果相符，否则不符合要求

测试编号： 49
测试项目：系统升级安全
分项目：远程升级测试
技术要求：《智能网关设备安全技术要求》4.1.7a）
测试配置：测试环境 1
测试过程： 1) 登录被测设备，指定存放升级软件的服务器 IP 地址（需通过 WAN 访问）； 2) 点击选择远程升级软件； 3) 升级成功之后重启设备，检查是否升级成功。
预期结果： 1）步骤 2～3 中，支持使用远程服务器上的软件进行升级。
判定原则：测试结果应与预期结果相符，否则不符合要求

测试编号： 50
测试项目：系统升级安全
分项目：断网可恢复测试
技术要求：《智能网关设备安全技术要求》4.1.7b）
测试配置：测试环境 1
测试过程： 1) 登录被测设备，指定存放升级软件的服务器 IP 地址（需通过 WAN 访问）； 2) 点击选择远程升级软件，在升级过程中，断开 WAN 网络，设备升级超时失败； 3) 升级失败之后重启设备，检查设备是否继续使用未升级前的软件版本正常启动运行。
预期结果： 1） 步骤 2-3 中，设备升级因断网导致失败，重启之后可恢复到正常状态。
判定原则：测试结果应与预期结果相符，否则不符合要求

测试编号： 51

测试项目：系统升级安全
分项目：软件错误可恢复测试
技术要求：《智能网关设备安全技术要求》4.1.7b）
测试配置：测试环境 1
测试过程： 1) 登录被测设备，使用本地错误软件进行升级； 2) 升级失败之后，重启设备，检查设备是否继续使用未升级前的软件版本正常启动运行。
预期结果： 1） 步骤 2 中，使用错误软件升级导致失败，重启之后可恢复到正常状态。
判定原则：测试结果应与预期结果相符，否则不符合要求

测试编号： 52
测试项目：系统升级安全
分项目：断电恢复测试（远程）
技术要求：《智能网关设备安全技术要求》4.1.7c）
测试配置：测试环境 1
测试过程： 1) 登录被测设备，指定存放升级软件的服务器 IP 地址（需通过 WAN 访问）； 2) 点击选择远程升级软件，在升级过程中断开设备电源； 3) 插上电源，重启设备，检查设备是否继续使用未升级前的软件版本正常启动运行。
预期结果： 1） 步骤 2-3 中，设备升级因断电导致失败，重启之后可恢复到正常状态。
判定原则：测试结果应与预期结果相符，否则不符合要求

测试编号： 53
测试项目：系统升级安全
分项目：断电恢复测试（本地）
技术要求：《智能网关设备安全技术要求》4.1.7c）
测试配置：测试环境 1
测试过程： 1) 登录被测设备，使用本地软件升级设备； 2) 在升级过程中断开设备电源； 3) 插上电源，重启设备，检查设备是否继续使用未升级前的软件版本正常启动运行。
预期结果： 1）步骤 2-3 中，设备升级因断电导致失败，重启之后可恢复到正常状态。
判定原则：测试结果应与预期结果相符，否则不符合要求

测试编号： 54
测试项目：系统升级安全
分项目：数据加密传输测试
技术要求：《智能网关设备安全技术要求》4.1.7d）

测试配置：测试环境 2
测试过程： 1) 登录被测设备，指定存放升级软件的服务器 IP 地址（需通过 WAN 访问）； 2) 将 WAN 访问数据镜像到测试仪器端口 B，点击选择远程升级软件，查看端口 B 接收到的报文是否是明文。
预期结果： 1） 步骤 2 中，升级数据支持加密传输。
判定原则：测试结果应与预期结果相符，否则不符合要求

测试编号： 55
测试项目：系统升级安全
分项目：非授权用户修改系统测试
技术要求：《智能网关设备安全技术要求》4.1.7e）
测试配置：测试环境 1
测试过程： 1） 查看被测设备是否存在安全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，例如是否存在 USB 调试模式开关。若存在，观察是否默认关闭 USB 调试模式
预期结果： 1） 步骤 1 中，被测设备禁止非授权用户对设备进行系统和桌面的刷写、修改或安装，默认禁止 USB 调试（ADB）模式等，开启 USB 调试模式需要经过授权。
判定原则：测试结果应与预期结果相符，否则不符合要求

测试编号： 56
测试项目：系统升级安全
分项目：软件验证测试
技术要求：《智能网关设备安全技术要求》4.1.7f）
测试配置：测试环境 1
测试过程： 1） 通过工具改写升级软件部分字节； 2） 登录被测设备，使用被改写的软件对设备进行升级。查看设备是否进行完整性校验，升级是否失败。
预期结果： 1）步骤 2 中，升级过程中对软件进行完整性验证，升级失败。
判定原则：测试结果应与预期结果相符，否则不符合要求

测试编号： 57
测试项目：系统升级安全
分项目：软件镜像主备分区测试
技术要求：《智能网关设备安全技术要求》4.1.7g）
测试配置：测试环境 1
测试过程： 1）登录被测设备，采用删除或其他方式破坏主分区软件镜像；

2）重启被测设备，查看设备是否能正常启动，运行是否正常。
预期结果： 1）步骤 2 中，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。
判定原则：测试结果应与预期结果相符，否则不符合要求

测试编号： 58
测试项目：系统升级安全
分项目：升级保护机制测试
技术要求：《智能网关设备安全技术要求》4.1.7h）
测试配置：测试环境 1
测试过程： 1） 检查被测设备用户手册，确认设备所有升级方式（包括 WAN 侧 TR069，云平台升级，本地升级等）； 2） 尝试使用每种方式进行升级，查看是否都要求进行认证登录； 3） 检查每种升级之前，是否需确认； 4） 如确认不同意，检查是否可以升级； 5） 如确认同意，检查是否可以升级。
预期结果： 1）步骤 1~2 中，每种方式升级之前都要求进行认证； 2）步骤 3-5 中，每种方式升级之前都需确认，同意之后才可以升级，不同意时升级取消。
判定原则：测试结果应与预期结果相符，否则不符合要求

测试编号： 59
测试项目：系统升级安全
分项目：升级提示功能测试
技术要求：《智能网关设备安全技术要求》4.1.7i）
测试配置：测试环境 1
测试过程： 1) 登录被测设备，通过本地和远程两种方式进行升级操作； 2) 查看被测设备是否有在显著地方提示用户升级可能造成的风险，例如可能出现短暂无法上网、请勿断电重启设备、避免升级异常等。
预期结果： 1）步骤 2 中，有升级风险提示。
判定原则：测试结果应与预期结果相符，否则不符合要求

5.2 业务功能安全

5.2.1 通信协议安全

测试编号： 60
测试项目：通信协议安全测试
分项目：基础通信协议健壮性测试（WAN 侧基础通信协议）
技术要求：《智能网关设备安全技术要求》4.2.1 a）1）

测试配置：测试环境 3
测试过程： 1) 测试仪表连接被测设备 WAN 侧； 2) 检查被测设备有关 IPv4/v6、TCP、UDP、ICMPv4/v6 等基础通信协议健壮性测试证据，包括第三方测试报告或自测报告等材料； 3) 抽取部分进行验证，每个协议验证性测试时间不低于 2 小时或测试用例不少于 1 万个。
预期结果： 1) 步骤 2 中，应具备该协议覆盖全字段的健壮性测试记录； 2) 步骤 3 中，验证测试时设备无死机、重启、业务终止等运行异常问题； 3) 步骤 3 中，抽取的所有测试用例都通过。
判定原则：测试结果应与预期结果相符，否则不符合要求

测试编号： 61
测试项目：通信协议安全测试
分项目：基础通信协议健壮性测试（LAN 侧基础通信协议）
技术要求：《智能网关设备安全技术要求》4.2.1 a）1）
测试配置：测试环境 3
测试过程： 1) 测试仪表连接被测设备 LAN 侧； 2) 检查被测设备有关 IPv4/v6、TCP、UDP、ICMPv4/v6 等基础通信协议健壮性测试证据，包括第三方测试报告或自测报告等材料； 3) 抽取部分进行验证，每个协议验证性测试时间不低于 2 小时或测试用例不少于 1 万个。
预期结果： 1) 步骤 2 中，应具备该协议覆盖全字段的健壮性测试记录； 2) 步骤 3 中，验证测试时设备无死机、重启、业务终止等运行异常问题； 3) 步骤 3 中，抽取的所有测试用例都通过。
判定原则：测试结果应与预期结果相符，否则不符合要求

测试编号： 62
测试项目：通信协议安全测试
分项目：网络管理协议健壮性测试（WAN 侧网络管理协议）
技术要求：《智能网关设备安全技术要求》4.2.1 a）2）
测试配置：测试环境 3
测试过程： 1) 测试仪表连接被测设备 WAN 侧； 2) 检查被测设备有关 SSH/Telnet、HTTP/HTTPS、SNMP、FTP/SFTP 等网络管理协议（支持时）健壮性测试证据，包括第三方测试报告或自测报告等材料； 3) 抽取部分进行验证，每个协议验证性测试时间不低于 2 小时或测试用例不少于 1 万个。
预期结果： 1） 步骤 2 中，应具备该协议覆盖全字段的健壮性测试记录； 2） 步骤 3 中，验证测试时设备无死机、重启、业务终止等运行异常问题； 3） 步骤 3 中，抽取的所有测试用例都通过。

判定原则：测试结果应与预期结果相符，否则不符合要求

测试编号： 63
测试项目：通信协议安全测试
分项目：网络管理协议健壮性测试（LAN 侧网络管理协议）
技术要求：《智能网关设备安全技术要求》4.2.1 a）2）
测试配置：测试环境 3
测试过程： 1) 测试仪表连接被测设备 LAN 侧； 2) 检查被测设备有关 SSH/Telnet、HTTP/HTTPS、SNMP、FTP/SFTP 等网络管理协议（支持时）健壮性测试证据，包括第三方测试报告或自测报告等材料； 3) 抽取部分进行验证，每个协议验证性测试时间不低于 2 小时或测试用例不少于 1 万个。
预期结果： 4) 步骤 2 中，应具备该协议覆盖全字段的健壮性测试记录； 5) 步骤 3 中，验证测试时设备无死机、重启、业务终止等运行异常问题； 6) 步骤 3 中，抽取的所有测试用例都通过。
判定原则：测试结果应与预期结果相符，否则不符合要求

测试编号： 64
测试项目：通信协议安全测试
分项目：抵御特定协议广播风暴能力测试（WAN）
技术要求：《智能网关设备安全技术要求》4.2.1 b）
测试配置：测试环境 3
测试过程： 1) 被测设备开启 ARP、IGMP 报文抑制功能（若被测设备默认支持，则该步骤跳过）； 2) LAN 侧开启抓包并使用网络分析仪从 LAN 侧发送 ARP Request 报文，请求的 IP 为被测设备本地的 IP 地址，速率大于步骤 1 设置的抑制速率，同时通过 WEB 访问被测设备； 3) 停止抓包，并分析抓包文件； 4) LAN 侧开启抓包并使用网络分析仪从 WAN 侧（组播通道）发送 IGMP QUERY 报文，速率大于步骤 1 设置的抑制速率，同时通过 WEB 访问被测设备； 5) 停止抓包，并分析抓包文件。
预期结果： 1) 步骤 4，在发送 ARP Request 报文过程中，WEB 可以正常访问被测设备； 2) 步骤 5，被测设备抑制 ARP Request 速率符合配置； 3) 步骤 4，在发送 IGMP QUERY 报文过程中，WEB 可以正常访问被测设备； 4) 步骤 5，被测设备抑制送 IGMP QUERY 速率符合配置。
判定原则：测试结果应与预期结果相符，否则不符合要求

测试编号： 65
测试项目：通信协议安全测试
分项目：抵御特定协议广播风暴能力测试（IPv6）
技术要求：《智能网关设备安全技术要求》4.2.1 b）

测试配置：测试环境 3
测试过程： 1) 被测设备开启 ND 报文抑制功能（若被测设备默认支持，则该步骤跳过）； 2) LAN 侧开启抓包并使用网络分析仪从 LAN 侧发送 ND Request 报文，请求的 IP 为被测设备本地的 IP 地址，速率大于步骤 1 设置的抑制速率，同时通过 WEB 访问被测设备； 3) 停止抓包，并分析抓包文件； 4) LAN 侧开启抓包并使用网络分析仪从 WAN 侧（组播通道）发送 IGMPv6 QUERY 报文，速率大于步骤 1 设置的抑制速率，同时通过 WEB 访问被测设备； 5) 停止抓包，并分析抓包文件。
预期结果： 1) 步骤 4，在发送 ND Request 报文过程中，WEB 可以正常访问被测设备； 2) 步骤 5，被测设备抑制 ND Request 速率符合配置； 3) 步骤 4，在发送 IGMPv6 QUERY 报文过程中，WEB 可以正常访问被测设备； 4) 步骤 5，被测设备抑制送 IGMPv6 QUERY 速率符合配置。
判定原则：测试结果应与预期结果相符，否则不符合要求

测试编号： 66
测试项目：通信协议安全测试
分项目：抵御特定协议广播风暴能力测试（LAN）
技术要求：《智能网关设备安全技术要求》4.2.1 b）
测试配置：测试环境 3
测试过程： 1) 被测设备开启 DHCP、ARP、IGMP 报文抑制功能（若网关默认支持，则该步骤跳过） 2) 使用测试工具从 LAN 侧发送 DHCP Request 攻击报文，速率大于步骤 1 设置的抑制速率，同时通过 WEB 访问被测设备。 3) 停止发包，并分析抓包文件 4) LAN 侧开启抓包并使用网络分析仪从 LAN 侧发送 ARP Request 报文，请求的 IP 为网关本地的 IP 地址，速率大于步骤 1 设置的抑制速率，同时通过 WEB 访问网关。 5) 停止抓包，并分析抓包文件 6) LAN 侧开启抓包并使用网络分析仪从 WAN 侧（组播通道）发送 IGMP QUERY 报文，速率大于步骤 1 设置的抑制速率，同时通过 WEB 访问被测设备。 7) 停止抓包，并分析抓包文件
预期结果： 1) 步骤 2，在发送 DHCP Request 报文过程中，WEB 可以正常访问被测设备 2) 步骤 3，被测设备抑制 DHCP Request 速率符合配置 3) 步骤 4，在发送 ARP Request 报文过程中，WEB 可以正常访问被测设备 4) 步骤 5，被测设备抑制 ARP Request 速率符合配置 5) 步骤 4，在发送 IGMP QUERY 报文过程中，WEB 可以正常访问被测设备 6) 步骤 5，被测设备抑制送 IGMP QUERY 速率符合配置
判定原则：测试结果应与预期结果相符，否则不符合要求

测试编号： 67

测试项目：通信协议安全测试
分项目：家庭网络组网协议测试
技术要求：《智能网关设备安全技术要求》4.2.1 c
测试配置：测试环境 3
测试过程： 1) 组网设备向被测设备发起连接请求； 2) 对支持使用手机 APP 进行连接确认的，确认 APP 上是否有设备连接确认提示，并需要用户手动进行确认后接入； 3) 对支持使用其他方式进行连接确认的，确认相应的方式是否提供设备连接确认提示，并需要用户手动进行确认后接入
预期结果： 1) 步骤 2、3 有设备连接确认提示，并需要用户手动进行确认后接入
判定原则：测试结果应与预期结果相符，否则不符合要求

测试编号： 68
测试项目：通信协议安全测试
分项目：家庭网络组网协议测试
技术要求：《智能网关设备安全技术要求》4.2.1d）
测试配置：测试环境 3
测试过程： 1) 组网设备接入被测设备 2) 使用抓包工具抓取组网设备与被测设备间的交互报文，分析抓包文件
预期结果： 1) 步骤 2 中，设备发现和认证阶段可以使用明文交互，认证通过后所有消息均需加密传输，支持使用密钥交换协议交换密钥。
判定原则：测试结果应与预期结果相符，否则不符合要求

5.2.2 应用业务安全

测试编号： 69
测试项目：应用业务安全测试
分项目：防止用户做源的组播能力测试
技术要求：《智能网关设备安全技术要求》4.2.2a）
测试配置：测试环境 3
测试过程： 1) 关闭被测设备 IGMP 组播代理，用户端口向 WAN 侧发送 IGMP Query 和组播数据报文，观察是否转发 2) 开启被测设备 IGMP 组播代理，用户端口向 WAN 侧发送 IGMP Query 和组播数据报文，观察是否转发
预期结果： 1) 用户发送的 IGMP Query 和组播数据报文不会往 WAN 侧转发 2) 用户发送的 IGMP Query 和组播数据报文会往 WAN 侧转发

判定原则：测试结果应与预期结果相符，否则不符合要求

测试编号： 70
测试项目：应用业务安全测试
分项目：语音业务测试
技术要求：《智能网关设备安全技术要求》4.2.2 b）
测试配置：测试环境 3
测试过程： 1) 支持 Z 接口的被测设备，网关配置 INTERNET 业务和语音业务（业务 VLAN 不同）； 2) Z 接口接固话机，测试是否能进行语音业务； 3) Z 接口接固话机进行语音业务，LAN 口接 PC 进行 INTERNET 业务，观察 Z 口的语音业务及 LAN 口的 INTERNET 业务是否进行了隔离。
预期结果： 1) 步骤 2 中，Z 接口接固话机，可进行语音业务； 2) 步骤 3 中，Z 接口的语音业务与 LAN 口的 INTERNET 业务已进行了隔离（如 VLAN 隔离或物理接口隔离），LAN 口无法进行语音业务，Z 口无法进行 INTERNET 业务。
判定原则：测试结果应与预期结果相符，否则不符合要求

测试编号： 71
测试项目：应用业务安全测试
分项目：WLAN 网络隔离功能测试
技术要求：《智能网关设备安全技术要求》4.2.2 c）
测试配置：测试环境 4
测试过程： 1) 被测设备配置网络隔离功能（如访客网络） 2) PC1 通过无线连接家庭网络，PC2 通过有线连接 LAN 接入家庭网络，PC3 通过无线连接访客网络 3) PC1 与 PC3 相互进行 PING 诊断 4) PC2 与 PC3 相互进行 PING 诊断
预期结果： 1) 步骤 3 PING 不能互通； 2) 步骤 4 PING 不能互通。
判定原则：测试结果应与预期结果相符，否则不符合要求

5.3 网管安全

5.3.1 身份鉴别与授权

测试编号： 72
测试项目：身份鉴别与授权测试
分项目：口令方式鉴别安全测试
技术要求：《智能网关设备安全技术要求》4.3.1a）4.3.1b）

测试配置：测试环境 1
测试过程： 1) 登录被测设备，输入正确的用户名、口令、SNMP 团体名等鉴别信息，尝试登录与操作； 2) 登录被测设备，输入错误的用户名、口令、SNMP 团体名等鉴别信息，尝试登录与操作； 3) 尝试创建已存在的用户。
预期结果： 1) 步骤 1 中，登陆成功，可对设备进行操作与管理； 2) 步骤 2 中，登录失败，无法对设备进行操作与管理； 3) 步骤 3 中，创建失败，用户身份标识具有唯一性。
判定原则：测试结果应与预期结果相符，否则不符合要求

测试编号： 28
测试项目：身份鉴别与授权测试
分项目：口令修改周期测试
技术要求：《智能网关设备安全技术要求》4.3.1c）
测试配置：测试环境 1
测试过程： 1) 对使用口令鉴别方式的设备，设置口令修改周期。
预期结果： 1) 设备应支持设置口令修改周期。
判定原则：测试结果应与预期结果相符，否则不符合要求

测试编号： 74
测试项目：身份鉴别与授权测试
分项目：默认口令测试
技术要求：《智能网关设备安全技术要求》4.3.1d）
测试配置：测试环境 1
测试过程： 1) 将两台同版本的被测设备均恢复出厂配置； 2) 检查两台被测设备默认口令信息。
预期结果： 1) 设备出厂时应预置不同的默认口令，如默认口令相同则需在用户首次管理设备时提示修改默认口令或设置口令
判定原则：测试结果应与预期结果相符，否则不符合要求

测试编号： 75
测试项目：身份鉴别与授权测试
分项目：登录方式能力测试
技术要求：《智能网关设备安全技术要求》4.3.1e）
测试配置：测试环境 1
测试过程： 1) 设置新的用户账户，如：在 WEB 管理界面下新增一个用户账户；

2) 增加、关闭、修改该用户账户可使用的登录方式。
预期结果： 1) 步骤 1 中，新建账户可使用的登录方式应默认限制为一种，该账户默认仅支持通过指定的方式登录； 2) 步骤 2 中，可增加支持其他的方式登录，也可配置关闭或修改已开启的登录方式。
判定原则：测试结果应与预期结果相符，否则不符合要求

测试编号： 76
测试项目：身份鉴别与授权测试
分项目：同一用户会话方式唯一性测试测试
技术要求：《智能网关设备安全技术要求》4.3.1f）
测试配置：测试环境 1
测试过程： 1）确认被测设备可支持 WEB、SSH 或 Telnet 等多种登录方式； 2) 用户 A 使用 WEB、SSH 或 Telnet 其中一种方式登录设备； 3)保持用户 A 的登录会话有效； 4)使用户 A 通过与 2）中不同的方式登录管理设备。
预期结果： 1) 步骤 4 中，用户 A 不可以登录或管理设备。
判定原则：测试结果应与预期结果相符，否则不符合要求

测试编号： 77
测试项目：身份鉴别与授权测试
分项目：口令复杂度检查和提醒功能测试
技术要求：《智能网关设备安全技术要求》4.3.1g）
测试配置：测试环境 1
测试过程： 1) 对使用口令鉴别方式的设备，尝试更改口令为低于 8 位的口令，查看被测设备反馈； 2) 尝试更改口令为高于 8 位但仅包括 1 种类型字符的口令，查看设备反馈； 3) 尝试更改口令为高于 8 位同时包括 2 种不同类型字符的口令，查看设备反馈。
预期结果： 1) 步骤 1 中设备应反馈口令复杂度不符合、口令修改失败相关的信息提示； 2) 步骤 2 中设备应反馈口令复杂度不符合、口令修改失败相关的信息提示； 3) 步骤 3 中设备应反馈口令修改成功。
判定原则：测试结果应与预期结果相符，否则不符合要求

测试编号： 78
测试项目：身份鉴别与授权测试
分项目：口令存储和显示非明文处理测试
技术要求：《智能网关设备安全技术要求》4.3.1h）
测试配置：测试环境 1
测试过程：

1) 根据被测设备厂商提供的材料，记录用户口令在设备上的存储方式和显示方式； 2) 分别验证各方式下用户口令的存储和显示是否处于非明文状态。
预期结果： 1) 步骤 1 中，形成口令存储和显示方式记录表； 2) 步骤 2 中，用户口令以非明文方式存储和显示。
判定原则：测试结果应与预期结果相符，否则不符合要求

测试编号： 79
测试项目：身份鉴别与授权测试
分项目：鉴别信息传输非明文处理
技术要求：《智能网关设备安全技术要求》4.3.1i）
测试配置：测试环境 1
测试过程： 1) 登录被测设备，抓包并分析用户口令、SNMP 团体名等鉴别信息是否加密传输。
预期结果： 1) 用户鉴别信息以密文方式传输。
判定原则：测试结果应与预期结果相符，否则不符合要求

测试编号： 80
测试项目：身份鉴别与授权测试
分项目：鉴别信息后门安全测试
技术要求：《智能网关设备安全技术要求》4.3.1j）
测试配置：测试环境 1
测试过程： 1) 检查被测设备有关身份鉴别相关材料； 2）更改预置的默认用户身份鉴别信息。
预期结果： 1) 步骤 1 中，应声明默认的身份鉴别信息，并说明不存在未向用户公开的身份鉴别信息； 2）步骤 2 中，默认的用户身份鉴别信息可修改成功。
判定原则：测试结果应与预期结果相符，否则不符合要求

测试编号： 81
测试项目：身份鉴别与授权测试
分项目：空闲超时能力测试
技术要求：《智能网关设备安全技术要求》4.3.1k）
测试配置：测试环境 1
测试过程： 1)配置被测设备启用防范空闲时间过长的功能，登录设备后，对设备长时间（超过空闲时长）不做任何操作。
预期结果： 1)步骤 1 中，设备支持登录用户空闲超时锁定或自动退出等安全策略。
判定原则：测试结果应与预期结果相符，否则不符合要求

测试编号： 29
测试项目：身份鉴别与授权测试
分项目：抗重放功能测试
技术要求：《智能网关设备安全技术要求》4.3.1l）
测试配置：测试环境 1
测试过程： 1) 通过 WEB、SSH 或 Telnet 其中一种方式远程登录被测设备； 2) 抓取并保存登录报文； 3) 退出登录； 4) 重新发送步骤 2 中的保存的登录报文； 5） 查看是否登录成功。
预期结果： 1) 步骤 5 中，登录失败。
判定原则：测试结果应与预期结果相符，否则不符合要求

测试编号： 83
测试项目：身份鉴别与授权测试
分项目：最少无差别信息测试
技术要求：《智能网关设备安全技术要求》4.3.1m）
测试配置：测试环境 1
测试过程： 1) 登录被测设备，输入正确的用户名与错误的密码； 2) 登录被测设备，输入错误的用户名，输入密码。
预期结果： 1)步骤 1、2 中，提示鉴别失败，两次登录，设备应返回最少且无差别信息。
判定原则：测试结果应与预期结果相符，否则不符合要求

测试编号： 84
测试项目：身份鉴别与授权测试
分项目：登录历史功能测试
技术要求：《智能网关设备安全技术要求》4.3.1n）
测试配置：测试环境 1
测试过程： 1) 以 WEB（LAN 侧和 WAN 侧）及 APP 等方式登录被测设备，检查成功登录后设备能否主动显示该账号最近的登录信息。
预期结果： 1) 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。
判定原则：测试结果应与预期结果相符，否则不符合要求

5.3.2 访问控制安全

测试编号： 85
测试项目：访问控制安全测试
分项目：默认访问控制策略测试
技术要求：《智能网关设备安全技术要求》4.3.1a）
测试配置：测试环境 1
测试过程： 1) 将被测设备恢复出厂设置； 2) 登录设备，对比设备安全相关材料检查设备默认的安全访问控制策略； 如设备有默认的访问控制策略，测试是否生效；如设备支持用户首次使用时设置访问控制策略，设置访问控制策略，并测试其是否生效。
预期结果： 1) 步骤 2 中，设备有默认的访问控制策略，或者支持用户首次使用时设置访问控制策略； 2) 步骤 3 中，如设备有默认的访问控制策略，设置的策略应可生效；如用户首次使用时可设置访问控制策略，设置的策略应可生效。
判定原则：测试结果应与预期结果相符，否则不符合要求

测试编号： 86
测试项目：访问控制安全测试
分项目：分级分权控制机制
技术要求：《智能网关设备安全技术要求》4.3.2b）和 e)
测试配置：测试环境 1
测试过程： 1) 设置不同权限级别的用户，并以不同权限用户登录，查看不同权限用户所具有的操作权限； 2) 以管理员用户权限登录被测设备，尝试执行软件升级、配置修改、设备重启等涉及设备安全的重要功能； 3) 以低权限用户登录被测设备，尝试执行软件升级、配置修改、设备重启等涉及设备安全的重要功能。 4) 设置同一权限级别的用户 U1 与用户 U2，并设置 U1 具有 C1 操作权限，U2 具有 C2 操作权限，C1 和 C2 是不同的操作； 5) U1 进行 C1 操作，U2 进行 C1 操作； 6) U1 进行 C2 操作，U2 进行 C2 操作。
预期结果： 1) 步骤 1 中，设备提供用户分级分权控制机制，不同权限用户登录后具有不同的操作权限； 2) 步骤 2 中，管理员用户能执行软件升级、配置修改、设备重启等涉及设备安全的重要功能； 3) 步骤 3 中，低权限用户不能执行软件升级、配置修改、设备重启等涉及设备安全的重要功能； 4) 步骤 4 中，设置成功； 5) 步骤 5 中，U1 操作成功，U2 操作失败； 6) 步骤 6 中，U1 操作失败，U2 操作成功。
判定原则：测试结果应与预期结果 1 相符，满足一级要求； 测试结果应与预期结果 1、5、6 相符，满足三级要求；

否则不符合要求。

测试编号： 87
测试项目：访问控制安全测试
分项目：黑白名单配置能力测试
技术要求：《智能网关设备安全技术要求》4.3.2c）
测试配置：测试环境 2
测试过程： 1) 在被测设备上配置黑名单策略，例如将 MAC 地址 M1 列入黑名单； 2) 使用 MAC 地址为 M1 的设备连接被测设备，观察结果； 3) 删除黑名单配置，在被测设备上配置白名单策略，例如将 MAC 地址 M2 列入白名单； 4) 使用 MAC 地址为 M2 的设备连接被测设备，观察结果； 5) 使用 MAC 地址为 M3 的设备（M1、M2、M3 为不同的 MAC 地址）连接被测设备，观察结果。
预期结果： 1) 步骤 2 中，连接失败； 2) 步骤 4 中，连接成功； 3) 步骤 5 中，连接失败。
判定原则：测试结果应与预期结果相符，否则不符合要求

测试编号： 88
测试项目：访问控制安全测试
分项目：MAC 地址的接入控制容量测试
技术要求：《智能网关设备安全技术要求》4.3.2d）
测试配置：测试环境 2
测试过程： 1) 在被测设备上配置 MAC 地址过滤规则（包括 LAN 和 WLAN），共配置 30 条规则； 2) 登录网关查看过滤规则表，查看 MAC 地址过滤规则条数是否包含了全部 30 条规则； 3) 使用测试仪发送 31 条流，其中 30 条命中 MAC 过滤规则，1 条不命中，查看收包的结果。
预期结果： 1) 可以成功配置至少 30 条规则； 2) 网关过滤规则表中包含了全部 30 条规则； 3) 测试仪接收端应仅收到 1 条不命中过滤规则的流。
判定原则：测试结果应与预期结果相符，否则不符合要求

5.3.3 WEB 管理安全

测试编号： 89
测试项目：WEB 管理安全测试
分项目：远程管理 HTTPS 测试
技术要求：《智能网关设备安全技术要求》4.3.3a）4.3.3b）
测试配置：测试环境 1
测试过程：

1) 确保外部网络与设备 WAN 侧 IP 可互通； 2) 在外部网络使用 HTTPS 访问设备 WEB 管理页面。
预期结果： 1) 使用 HTTPS 方式可成功访问 WEB 管理页面。
判定原则：测试结果应与预期结果相符，否则不符合要求

测试编号： 90
测试项目：WEB 管理安全测试
分项目：本地管理 HTTPS 测试
技术要求：《智能网关设备安全技术要求》4.3.3b）
测试配置：测试环境 1
测试过程： 1） 确保内部网络与设备 LAN 侧 IP 可互通； 2） 在内部网络使用 HTTPS 访问设备 WEB 管理界面。
预期结果： 1) 使用 HTTPS 方式可成功访问 WEB 管理页面。
判定原则：测试结果应与预期结果相符，否则不符合要求

测试编号： 91
测试项目：WEB 管理安全测试
分项目：身份鉴别与授权测试
技术要求：《智能网关设备安全技术要求》4.3.3c）
测试配置：测试环境 1
测试过程： 1) 参考 5.3.1 节中身份鉴别与授权的用例对 WEB 系统做鉴权测试。
预期结果： 1) 符合 5.3.1 节身份鉴别与授权用例要求。
判定原则：测试结果应与预期结果相符，否则不符合要求

测试编号： 92
测试项目：WEB 管理安全测试
分项目：访问控制安全测试
技术要求：《智能网关设备安全技术要求》4.3.3d）
测试配置：测试环境 1
测试过程： 1) 参考 5.3.2 节中访问控制安全测试方法对 WEB 访问控制安全进行测试。
预期结果： 1) 符合 5.3.2 节访问控制安全测试方法的各项预期结果。
判定原则：测试结果应与预期结果相符，否则不符合要求

测试编号： 93
测试项目：WEB 管理安全测试

分项目：WEB 应用会话标识安全测试
技术要求：《智能网关设备安全技术要求》4.3.3e）
测试配置：测试环境 1
测试过程： 1) 访问被测设备管理页面，记录登录前的会话标志； 2) 输入用户名密码登录网关管理页面，记录登录后的会话标志； 3) 退出登录，记录下一次登录前的会话标志； 4) 输入用户名密码登录网关管理页面，记录登录后的会话标志。
预期结果： 1) 用户名和口令认证通过后应更换会话标识，步骤 1 和步骤 2 中的会话标志不同； 2) 观察步骤 1、2、3、4 中记录的会话标志，四次记录的会话标志均不同，WEB 应用会话标识具备随机性、唯一性，会话标识有效长度不少于 192 比特。
判定原则：测试结果应与预期结果相符，否则不符合要求

测试编号： 94
测试项目：WEB 管理安全测试
分项目：Cookie 安全措施
技术要求：《智能网关设备安全技术要求》4.3.3f）
测试配置：测试环境 1
测试过程： 1) 清除浏览器 cookie 信息； 2) 输入正确的用户名及密码登录 WEB 管理页面； 3) 抓取登录过程的报文； 4) 查看登录成功后记录的 cookie 信息； 5) 检查 cookie 是否保存用户名及密码信息； 6) 检查 cookie 有效期设置是否合理（注销后即失效）； 7) 检查 cookie 中是否有 HttpOnly 属性； 8) 检查 cookie 中是否有 Secure 属性（WAN 侧）。
预期结果： 1) 步骤 5 中，获取到报文中的 cookie 记录的密码等敏感信息是加密的； 2) 步骤 5 中，未保存用户名及密码； 3) 步骤 6 中，cookie 有效期设置合理（注销后即失效）； 4) 步骤 7 中，cookie 有 HttpOnly 属性，且为 true； 5) 步骤 8 中，cookie 有 Secure 属性，且为 true。
判定原则：测试结果应与预期结果相符，否则不符合要求

测试编号： 95
测试项目：WEB 管理安全测试
分项目：WEB 访问日志测试
技术要求：《智能网关设备安全技术要求》4.3.3g）
测试配置：测试环境 1
测试过程：

1)检查网关日志记录功能，对关键操作行为进行记录，关键操作行为应包括：增加/删除账户；修改鉴别信息；修改配置（DNS、IP 地址等）；用户登录/注销；重启/关闭设备。
预期结果： 1) 步骤 1 中，列出的关键操作均有记录日志
判定原则：测试结果应与预期结果相符，否则不符合要求

5.3.4 Telnet 管理安全

测试编号： 96
测试项目：Telnet 管理安全测试
分项目：Telnet 功能默认状态测试
技术要求：《智能网关设备安全技术要求》4.3.4a）
测试配置：测试环境 1
测试过程： 1) 将被测设备恢复到出厂默认状态； 2) PC 连接到被测设备的 LAN 口，查看能否进行 Telnet 登录； 3) 被测设备配置路由 WAN 连接，获取正确的公网 IP，查看能否在公网使用该公网 IP 进行 Telnet 登录。
预期结果： 1) 步骤 2 中，Telnet 登录失败(不能出现用户名密码输入界面)； 2) 步骤 3 中，Telnet 登录失败(不能出现用户名密码输入界面)。
判定原则：测试结果应与预期结果相符，否则不符合要求

测试编号： 97
测试项目：Telnet 管理安全测试
分项目：身份鉴别与授权测试
技术要求：《智能网关设备安全技术要求》4.3.4b）
测试配置：测试环境 1
测试过程： 1) 参考 5.3.1 节中身份鉴别与授权的用例对 Telnet 做鉴权测试。
预期结果： 1) 符合 5.3.1 节身份鉴别与授权用例要求。
判定原则：测试结果应与预期结果相符，否则不符合要求

测试编号： 98
测试项目：Telnet 管理安全测试
分项目：访问控制安全测试
技术要求：《智能网关设备安全技术要求》4.3.4c）
测试配置：测试环境 3
测试过程： 1) 打开 Telnet 开关； 2) 获取到正确的 Telnet 登录用户名和密码；

3) 第一个用户登录 Telnet，并保持连接状态； 4) 使用第二个用户登录 Telnet； 5) 参考 5.3.2 节的测试用例对 Telnet 进行访问控制安全测试。
预期结果： 1) 步骤 4 中，第二个用户无法登录 Telnet； 2) 步骤 5 中，符合 5.3.2 节对应的预期结果。
判定原则：测试结果应与预期结果相符，否则不符合要求

测试编号： 99
测试项目：Telnet 管理安全测试
分项目：Telnet 访问日志测试
技术要求：《智能网关设备安全技术要求》4.3.4d）
测试配置：测试环境 3
测试过程： 1)登录到被测设备的 Telnet 服务； 2)查看访问日志记录。
预期结果： 1)步骤 2 中，可查询到 Telnet 访问的日志。
判定原则：测试结果应与预期结果相符，否则不符合要求

5.3.5 SNMP 管理安全

测试编号： 100
测试项目：SNMP 管理安全测试
分项目：SNMPv3 协议测试
技术要求：《智能网关设备安全技术要求》4.3.5a）
测试配置：测试环境 1
测试过程： 1) 确认被测设备支持 SNMP 协议； 2) 使用网管工具连接被测设备； 3) 抓包查看 SNMP 协议的类型； 4) 查看服务器端使用的认证方式。
预期结果： 1) 步骤 3 中，被测设备支持 SNMPv3 协议连接第三方网管； 2) 步骤 4 中，查看到的服务端默认使用 authPriv（既认证又加密）的接入方式，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；
判定原则：测试结果应与预期结果相符，否则不符合要求

测试编号： 101
测试项目：SNMP 管理安全测试
分项目：Community 复杂度测试
技术要求：《智能网关设备安全技术要求》4.3.5b）

测试配置：测试环境 1
测试过程： 1) 被测设备开启 Community 复杂度检查功能，修改网关设备 Community 值。
预期结果： 1) 被测设备开启 Community 复杂度检查功能时，Community 长度应不少于 8 位，且至少包含 2 种不同类型字符。
判定原则：测试结果应与预期结果相符，否则不符合要求

测试编号： 102
测试项目：SNMP 管理安全测试
分项目：访问控制安全测试
技术要求：《智能网关设备安全技术要求》4.3.5c）
测试配置：测试环境 1
测试过程： 1) 配置 SNMP 用户不同权限（只读/读写）； 2) 配置 SNMP 用户可访问的 MIB 库资源（用 OID 前缀标识）； 3) 配置 ACL（访问控制列表）。
预期结果： 1) 支持配置用户不同权限（只读/读写）； 2) 支持配置用户可访问的 MIB 库资源（用 OID 前缀标识）； 3) 支持采用 ACL（访问控制列表）保护 SNMP 访问权限。
判定原则：测试结果应与预期结果相符，否则不符合要求

测试编号： 103
测试项目：SNMP 管理安全测试
分项目：SNMP 访问日志测试
技术要求：《智能网关设备安全技术要求》4.3.5d）
测试配置：测试环境 1
测试过程： 1) 登录网关 SNMP 服务 2) 检查网关 SNMP 访问日志 3) 登出网关 SNMP 服务 4) 检查网关 SNMP 访问日志
预期结果： 1) 步骤 2 中，记录了登录 SNMP 服务的日志 2) 步骤 3 中，记录了登出 SNMP 服务的日志
判定原则：测试结果应与预期结果相符，否则不符合要求

测试编号： 104
测试项目：SNMP 管理安全测试
分项目：认证失败测试
技术要求：《智能网关设备安全技术要求》4.3.5e）

测试配置：测试环境 1
测试过程： 1) 确认被测设备启用认证失败消息（Trap）发送功能，使用错误的认证信息访问网关 SNMP 服务
预期结果： 1) 被测设备发送认证失败消息
判定原则：测试结果应与预期结果相符，否则不符合要求

测试编号： 105
测试项目：SNMP 管理安全测试
分项目：SNMP 拒绝服务攻击测试
技术要求：《智能网关设备安全技术要求》4.3.5f）
测试配置：测试环境 1
测试过程： 1) 向被测设备以一定的速率发送 SNMP 攻击包（读取/写入 OID 信息）； 2) 观察被测设备运行状态。
预期结果： 1) 步骤 2 中，被测设备不死机、不重启、且能够正常转发数据。
判定原则：测试结果应与预期结果相符，否则不符合要求
备注：发送速率对测试结果有影响，攻击流量为 1000FPS，发送流量时长为 30 秒，也可以根据设备情况选择测试参数

5.3.6 TR069 远程管理安全

测试编号： 106
测试项目：TR069 远程管理安全测试
分项目：接口安全测试
技术要求：《智能网关设备安全技术要求》4.3.6a）
测试配置：测试环境 1
测试过程： 1) 在被测设备上正确配置以下参数： ① ACS URL ② 网关访问 ACS 的用户名及密码 ③ ACS 访问网关的用户名及密码 2) 被测设备发起连接 ACS 请求，查看能否连接成功
预期结果： 1) 步骤 2 中，被测设备与 ACS 成功建立 SSL/TLS 安全通道； 2) 步骤 2 中，被测设备发起 WWW-Authentication 认证，并通过认证；
判定原则：测试结果应与预期结果相符，否则不符合要求

测试编号： 107
测试项目：TR069 远程管理安全测试

分项目：记录访问日志能力测试
技术要求：《智能网关设备安全技术要求》4.3.6b）
测试配置：测试环境 1
测试过程： 1)将被测设备连接到远程管理平台； 2)查看访问日志记录。
预期结果： 1)步骤 2 中，访问日志记录包含 TR069 交互的日志。
判定原则：测试结果应与预期结果相符，否则不符合要求

测试编号： 108
测试项目：TR069 远程管理安全测试
分项目：管理功能终结能力测试
技术要求：《智能网关设备安全技术要求》4.3.6c）
测试配置：测试环境 3
测试过程： 1)配置 WAN 侧的 TR069 远程管理功能，配置智能网关连上 TR069 远程管理平台； 2)检查 LAN 侧是否支持 TR069 远程管理，检查 TR069 远程管理平台能否管理到被测设备的 LAN 侧。
预期结果： 1) 步骤 1 中，WAN 侧应支持 TR069 远程管理功能； 2) 步骤 2 中，LAN 侧应不支持 TR069 远程管理，TR069 远程管理平台不能管理到被测设备的 LAN 侧，只能管理被测设备的 WAN 侧。
判定原则：测试结果应与预期结果相符，否则不符合要求

测试编号： 109
测试项目：TR069 远程管理安全测试
分项目：证书认证功能测试
技术要求：《智能网关设备安全技术要求》4.3.6d）
测试配置：测试环境 1
测试过程： 1. 在被测设备上正确配置以下参数： ① ACS URL ② 智能网关访问 ACS 的用户名及密码 ③ ACS 访问智能网关的用户名及密码 2) 让被测设备用正确的证书发起连接请求，查看能否连接成功；
预期结果： 1)步骤 2 中，被测设备与远程管理平台能连接成功
判定原则：测试结果应与预期结果相符，否则不符合要求

5.3.7 日志审计安全

测试编号： 110
测试项目：日志审计安全测试
分项目：日志记录功能测试（应支持的操作行为）
技术要求：《智能网关设备安全技术要求》4.3.7a）1)~5)
测试配置：测试环境 1
测试过程： 1) 触发下述操作行为（关键操作），检查被测设备是否记录日志： 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；
预期结果： 1） 步骤 1 中，列出的关键操作均有记录日志。
判定原则：测试结果应与预期结果相符，否则不符合要求

测试编号： 3011
测试项目：日志审计安全测试
分项目：日志记录功能测试（可支持的操作行为）
技术要求：《智能网关设备安全技术要求》4.3.7a）6)~10)
测试配置：测试环境 1
测试过程： 1) 触发下述操作行为（关键操作），检查被测设备是否记录日志： ① 文件上传/下载（支持时）； ② 用户权限修改（支持时）； ③ 关闭日志审计功能（支持时）； ④ 开启日志审计功能（支持时）； ⑤ 其他（支持时）；
预期结果： 1） 如网关支持步骤 1 中列出的关键操作，则对应的操作需记录日志。
判定原则：测试结果应与预期结果相符，否则不符合要求

测试编号： 3112
测试项目：日志审计安全测试
分项目：日志本地存储测试
技术要求：《智能网关设备安全技术要求》4.3.7b）
测试配置：测试环境 1
测试过程： 1) 触发日志记录操作，检查被测设备本地是否能够存储日志信息； 2) 触发记录日志操作使得审计存储达到极限或失败，检查新记录的日志是否丢失。
预期结果： 1) 步骤 1 中，被测设备应能够支持本地存储日志信息；

2) 步骤 2 中，当审计存储达到极限或失败时，设备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。
判定原则：测试结果应与预期结果相符，否则不符合要求

测试编号： 3213
测试项目：日志审计安全测试
分项目：日志存储能力测试
技术要求：《智能网关设备安全技术要求》4.3.7c）
测试配置：测试环境 1
测试过程： 1) 触发日志记录操作，使被测设备应记录日志的条目超过 500 条，检查日志文件存储能力。
预期结果： 1) 日志信息本地存储能力应不低于 500 条。
判定原则：测试结果应与预期结果相符，否则不符合要求

测试编号： 3314
测试项目：日志审计安全测试
分项目：日志要素测试
技术要求：《智能网关设备安全技术要求》4.3.7d）
测试配置：测试环境 1
测试过程： 1) 检查已记录的日志信息，确认是否包括事件发生的日期和时间、主体、类型、结果等信息。
预期结果： 1) 操作日志包含了操作日期和时间、操作主体、操作人 IP（适用时）、操作内容等信息；操作日志内容与所作操作一致。
判定原则：测试结果应与预期结果相符，否则不符合要求

测试编号： 3415
测试项目：日志审计安全测试
分项目：日志保护能力测试
技术要求：《智能网关设备安全技术要求》4.3.7e）
测试配置：测试环境 1
测试过程： 1) 以管理员身份登录被测设备，尝试修改操作日志； 2) 查看日志是否被修改； 3) 尝试删除操作日志； 4) 查看日志是否被删除。
预期结果： 1) 步骤 2 和 4 中，操作日志应该不能被修改和删除。
判定原则：测试结果应与预期结果相符，否则不符合要求

测试编号： 35

测试项目：日志审计安全测试
分项目：日志信息上传测试
技术要求：《智能网关设备安全技术要求》4.3.7f）
测试配置：测试环境 1
测试过程： 1) 在网关的 WAN 口开启抓包； 2) 触发家庭网关上传日志文件操作； 3) 分析抓取的数据包中是否有明文日志信息。
预期结果： 1) 步骤 2 中，日志可以上传到远程管理平台； 2) 步骤 3 中，抓取的数据包中没有明文日志信息。
判定原则：测试结果应与预期结果相符，否则不符合要求

测试编号： 3617
测试项目：日志审计安全测试
分项目：日志断电保护能力测试
技术要求：《智能网关设备安全技术要求》4.3.7g）
测试配置：测试环境 1
测试过程： 1) 查看被测设备的本地日志信息，并导出保存； 2) 将被测设备断电后加电； 3) 待设备启动后再次查看被测设备的本地日志信息，并导出保存； 4) 比较步骤 1 和步骤 3 中的日志。
预期结果： 1) 步骤 4 中，步骤 1 中存储在本地的日志信息未丢失。
判定原则：测试结果应与预期结果相符，否则不符合要求

5.4 应用软件安全

5.4.1 应用安装安全

测试编号： 118
测试项目：应用安装安全测试
分项目：安装未经认证的应用测试
技术要求：《智能网关设备安全技术要求》4.4.1a）
测试配置：测试环境 1
测试过程： 1) 准备未认证的安装包； 2) 将安装包放在预置可下载位置； 3) 执行下载任务，下载完成后，安装软件。
预期结果： 1) 步骤 3 中，执行下载指令后，被测设备反馈该安装包未经认证，查看安装结果，提示安装失败，系统中未发现该软件。

判定原则：测试结果应与预期结果相符，否则不符合要求

测试编号： 119
测试项目：应用安装安全测试
分项目：安卓系统应用安全测试
技术要求：《智能网关设备安全技术要求》4.4.1b）
测试配置：测试环境 1
测试过程： 1) 通过数据接口连接被测设备，查看 ADB 是否默认关闭； 2) 打开被测设备的 ADB 调试模式； 3) 在测试终端准备用于测试的 APK 文件，通过命令安装 APK 文件，例如执行命令“adb install 路径+包名.apk”。
预期结果： 1) 步骤 1 中，ADB 开关默认关闭。 2) 步骤 2 中无法打开 ADB 调试模式或者步骤 3 中无法成功安装 APK 文件。
判定原则：测试结果应与预期结果相符，否则不符合要求

5.4.2 应用数据安全

测试编号： 120
测试项目：应用数据安全测试
分项目：操作配置信息测试
技术要求：《智能网关设备安全技术要求》4.4.2a）
测试配置：测试环境 1
测试过程： 1) 通过厂商声明的方式或应用备份配置信息； 2) 删除配置信息； 3) 根据被测设备提示对配置信息进行恢复； 4) 通过厂商未声明的其他方式或应用备份配置信息。
预期结果： 1) 步骤 1 中，备份成功并显示备份位置或可查看的位置，在指定位置发现配置文件； 2) 步骤 2 中，备份信息删除成功，在指定位置可看到文件已删除； 3) 步骤 3 中，备份信息恢复成功，查看配置文件信息与备份前配置信息一致； 4) 步骤 4 中，提示备份失败，未在指定位置发现配置文件。
判定原则：测试结果应与预期结果相符，否则不符合要求

测试编号： 121
测试项目：应用数据安全测试
分项目：配置信息文件权限能力测试
技术要求：《智能网关设备安全技术要求》4.4.2b）
测试配置：测试环境 1
测试过程：

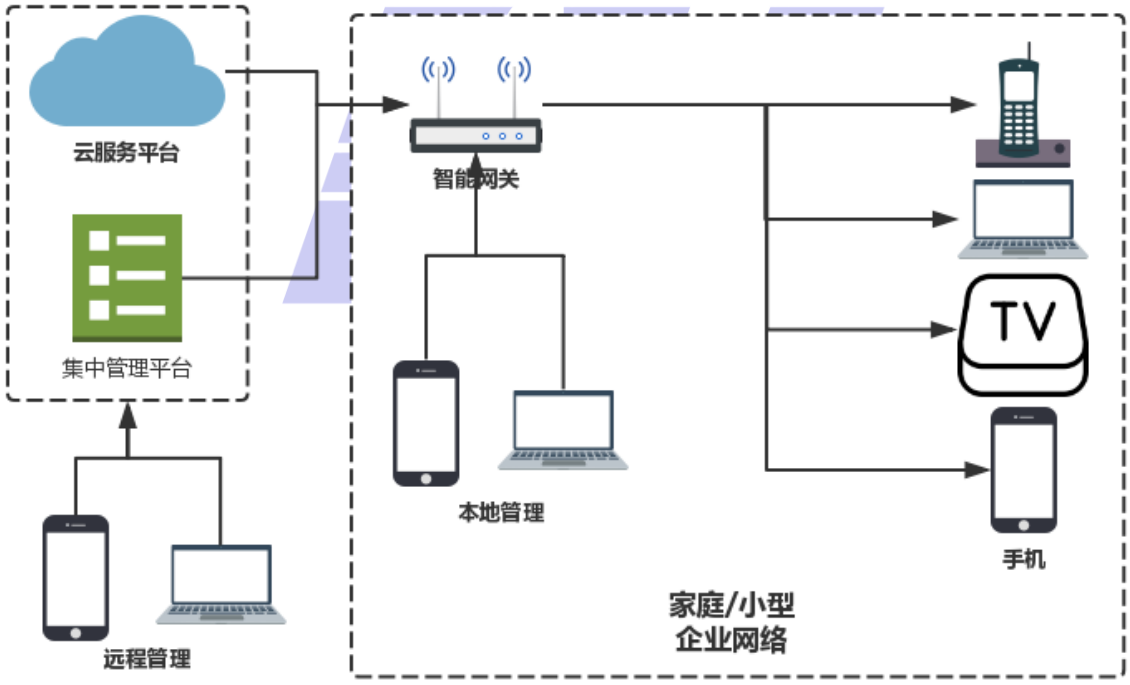
1) 在管理员权限下设定配置文件权限为只读； 2) 使用未授权的账号登录管理终端，下载配置文件； 3) 使用未授权的账号登录管理终端，编辑配置文件； 4) 使用未授权的账号登录管理终端，删除配置文件。
预期结果： 1) 步骤 2 中，提示该账号没有下载权限； 2) 步骤 3 中，提示该账号没有编辑权限； 3) 步骤 4 中，提示该账号没有删除权限。
判定原则：测试结果应与预期结果相符，否则不符合要求

测试编号： 3722
测试项目：应用数据安全测试
分项目：收集用户信息数据测试
技术要求：《智能网关设备安全技术要求》4.4.2c）
测试配置：测试环境 1
测试过程： 1) 查看隐私声明、说明书或其他相关材料，确认是否说明被测设备收集用户信息数据； 2) 对通过被测设备收集用户信息数据的，确认是否向用户明示并取得用户同意。
预期结果： 如果设备收集了用户信息， 1） 步骤 1 中，应明确说明设备是否收集用户信息数据； 2） 步骤 2 中，应向用户明示并取得用户同意才能收集。
判定原则：测试结果应与预期结果相符，否则不符合要求

附录 A
（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A.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A.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。

电信终端产业协会团体标准

智能网关设备安全测试方法

T/TAF 046—2019

*

电信终端产业协会印发
地址：北京市西城区新街口外大街 28 号
电话：010-82052809
电子版发行网址：www.taf.org.cn