ICS 33.050
CCS M 30

团　体　标　准

T/TAF 248—2024

光传送网设备安全测试方法

Security test methods for optical transport network equipment

2024-09-02 发布　　2024-09-02 实施

电信终端产业协会　发布

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 1
5　测试环境 2
6　安全功能测试方法 2
6.1　操作系统安全 2
6.2　软件安全 6
6.3　身份鉴别与访问控制 8
6.4　通信安全 13
6.5　数据安全 17
6.6　防护能力 19
6.7　日志审计和管理 26
7　安全保障评估方法 29
7.1　设计和开发 29
7.2　生产和交付 35
7.3　运行和维护 37
参考文献 39

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专利的责任。

本文件由电信终端产业协会提出并归口。

本文件起草单位：中国信息通信研究院、华为技术有限公司、成都泰瑞通信设备检测有限公司、武汉网锐检测科技有限公司、中兴通讯股份有限公司、上海泰峰检测认证有限公司、北京通和实益电信科学技术研究所有限公司、博鼎实华（北京）技术有限公司、郑州信大捷安信息技术股份有限公司、深圳信息通信研究院、烽火通信科技股份有限公司、北京邮电大学。

本文件主要起草人：路晔绵、张治兵、吴荣春、刘欣东、刁汝楠、陈鹏、吴翔宇、龚志红、陈玺、周继华、任华、宋祥烈、张大超、刘刚、刘向东、刘为华、刘献伦、唐伟生、靳涛、邓科、张杰、王伟。

光传送网设备安全测试方法

1 范围

本文件规定了针对光传送网（OTN）设备的安全测试方法，包括安全功能测试和安全保障评估。
本文件适用于光传送网设备的测试、评估与认证。

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 25069-2022 信息安全技术 术语
GB 40050-2021 网络关键设备安全通用要求
T/TAF 230-2024 光传送网设备安全技术要求
ISO/IEC 9899:2018 C语言规范（Programming languages — C）

3 术语和定义

GB/T 25069-2022和T/TAF 230-2024界定的术语和定义适用于本文件。

4 缩略语

下列缩略语适用于本文件。
AES：高级加密标准（Advanced Encryption Standard）
ARP：地址解析协议（Address Resolution Protocol）
ASLR：地址空间布局随机化（Address Space Layout Randomization）
CN：通用名称（Common Name）
CSR：证书签名请求（Certificate Signing Request）
CVE：通用漏洞披露（Common Vulnerabilities & Exposures）
DoS：拒绝服务（Denial of Service）
DTLS：数据包传输层安全性协议（Datagram Transport Layer Security）
FTP：文件传输协议（File Transfer Protocol）
GOT：全局偏移表（Global Offset Table）
HTTP：超文本传输协议（Hypertext Transfer Protocol）
ICMP：因特网控制报文协议（Internet Control Message Protocol）
IP：网际互连协议（Internet Protocol）
IT：互联网技术（Internet Technology）
LTS：长期支持（Long Term Support）

NX：不可执行（No-eXecute）
OTN：光传送网（Optical Transport Network）
PC：个人计算机（Personal Computer）
PCB：印制电路板（Printed Circuit Board）
PIE：地址无关可执行（Position-Independent Executable）
RADIUS：远程用户拨号认证服务（Remote Authentication Dial In User Service）
SFTP：安全文件传输协议（Secret File Transfer Protocol）
SHA：安全散列算法（Secure Hash Algorithm）
SNMP：简单网络管理协议（Simple Network Management Protocol）
SSH：安全外壳协议（Secure Shell）
SSL：安全套接层（Secure Socket Layer）
SYN：同步序列编号（Synchronize Sequence Numbers）
TACACS：终端访问控制器访问控制系统（Terminal Access Controller Access-Control System）
TCP：传输控制协议（Transmission Control Protocol）
TLS：传输层安全协议（Transport Layer Security）
UDP：用户数据报协议（User Datagram Protocol）
UID：用户身份证明（User Identification）

5 测试环境

测试环境架构见图1，其中互联设备不是必需设备，根据实际网络部署情况确保测试终端、管理终端、被测设备可联通即可。

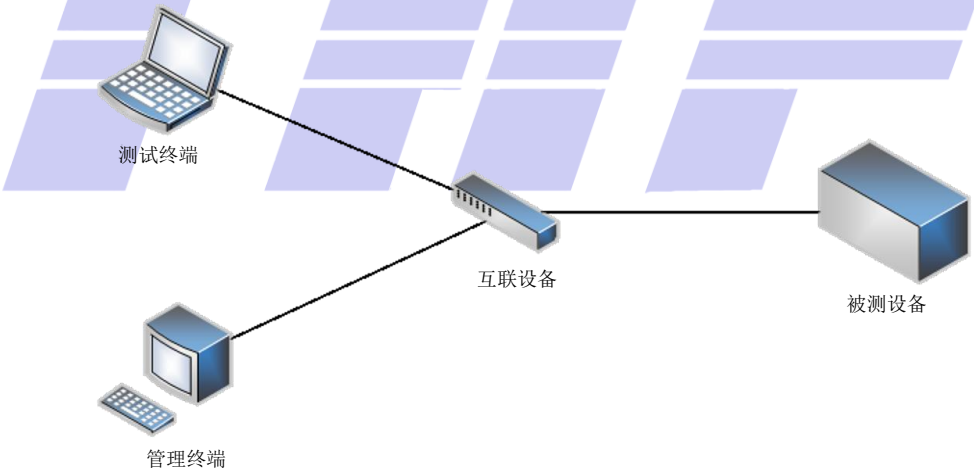

图 1 测试环境

测试终端可通过互联设备直接操作被测设备，或通过管理终端对被测设备进行管理操作，测试终端上安装有测试所需的工具。

6 安全功能测试方法

6.1 操作系统安全

6.1.1 操作系统隔离能力

该检测项包含如下内容：

a) 安全要求：

操作系统隔离能力要求见T/TAF 230-2024 5.2.1 a)，即：

应使用具备用户态进程与操作系统内核隔离能力的操作系统。

b) 预置条件：

1) 厂商提供访问设备操作系统的安全途径，如安全shell；

2) 若是自研操作系统，厂商还需提供自研操作系统隔离相关设计的说明文档。

c) 检测方法：

连接设备，查询验证设备操作系统使用的版本；若是自研操作系统，检查隔离相关说明文档，并验证设备上的操作系统版本。

d) 预期结果：

若使用非自研操作系统，设备使用的操作系统应支持用户态与内核态隔离，如Linux、QNX、RT-Thread smart版等，禁止使用不支持用户态和内核态隔离的操作系统，如vxworks、RT-Thread标准版等；若使用自研操作系统，隔离说明文档中应明确支持用户态与内核态隔离，且设备上实际使用的操作系统版本为支持用户态与内核态隔离的版本。

e) 判定原则：

测试结果应与预期结果相符，否则不符合要求。

6.1.2 禁止特权用户远程访问

该检测项包含如下内容：

a) 安全要求：

禁止特权用户远程访问要求见T/TAF 230-2024 5.2.1 b)，即：

若支持多用户机制，应禁止操作系统特权用户远程访问设备。

b) 预置条件：

1) 设备支持多账号机制；

2) 厂商提供访问设备操作系统的安全途径，如安全shell。

c) 检测方法：

查看操作系统特权账号登录方式，或尝试使用操作系统特权账号进行远程登录，确认是否禁止使用特权账号远程访问设备。

d) 预期结果：

操作系统特权账号显示为禁止登录，或使用操作系统特权账号无法进行远程登录。

e) 判定原则：

测试结果应与预期结果相符，否则不符合要求。

6.1.3 调试工具去除

该检测项包含如下内容：

a) 安全要求：

调试工具去除要求见T/TAF 230-2024 5.2.1 c)，即：

应限制或去除操作系统中的调试能力或工具。

b) 预置条件：

厂商提供访问设备操作系统的安全途径，如安全shell。

c) 检测方法：
查找系统中是否存在具备调试能力的工具，或是否可使用调试功能。
d) 预期结果：
系统里未搜到任何调试工具，调试功能无法使用。
e) 判定原则：
测试结果应与预期结果相符，否则不符合要求。

6.1.4 文件和文件夹权限

该检测项包含如下内容：
a) 安全要求：
文件和文件夹权限要求见T/TAF 230-2024 5.2.1 d)，即：
若存在文件系统，应限定操作系统可执行文件及其所属文件夹的写权限仅创建当前文件的主体可拥有。
b) 预置条件：
1) 设备存在文件系统；
2) 厂商提供访问设备操作系统的安全途径，如安全shell。
c) 检测方法：
查看设备上二进制可执行文件权限设置是否合理。
d) 预期结果：
二进制可执行文件的写权限仅创建当前文件的主体可拥有或者不允许进行写操作。
e) 判定原则：
测试结果应与预期结果相符，否则不符合要求。

6.1.5 ASLR配置

该检测项包含如下内容：
a) 安全要求：
ASLR配置要求见T/TAF 230-2024 5.2.1 e)，即：
操作系统应默认开启ASLR配置以加强系统安全性。
b) 预置条件：
1) 厂商提供访问设备操作系统的安全途径，如安全shell；
2) 厂商提供查看ASLR配置的途径，如相关操作命令。
c) 检测方法：
通过输入命令等方式查看操作系统是否开启ALSR。
d) 预期结果：
系统开启了ALSR。
e) 判定原则：
测试结果应与预期结果相符，否则不符合要求。

6.1.6 进程所属用户及用户组管理

该检测项包含如下内容：
a) 安全要求：
进程所属用户及用户组管理要求见T/TAF 230-2024 5.2.1 f)，即：
若支持多用户和用户组机制，应为不同风险等级的进程分配不同的用户和用户组。

b) 预置条件：
   1) 设备支持多用户和用户组机制；
   2) 厂商提供访问设备操作系统的安全途径，如安全shell。
c) 检测方法：
   1) 查看系统当前运行进程对应的用户信息；
   2) 查看步骤1）中检出的用户对应的用户组信息。
d) 预期结果：
   1) 结果中存在不同的用户（至少存在一个非特权用户），存在不同的进程分属于不同用户；
   2) 用户分属于至少2个用户组。
e) 判定原则：
   测试结果应与预期结果相符，否则不符合要求。

6.1.7 进程特权最小化

该检测项包含如下内容：

a) 安全要求：
   进程特权最小化要求见T/TAF 230-2024 5.2.1 g)，即：
   设备上运行的进程应根据业务诉求最小化使用系统特权（如capability特权）。
b) 预置条件：
   1) 厂商提供访问设备操作系统的安全途径，如安全shell；
   2) 厂商提供进程对系统特权的使用说明。
c) 检测方法：
   1) 查看设备上运行的进程使用的系统特权；
   2) 查看每个非特权用户下的进程是否最小化使用系统特权。
d) 预期结果：
   1) 成功获得每个进程使用的系统特权信息；
   2) 每个非特权用户的进程已最小化使用系统特权，进程按需使用特权，所有使用的特权均说明了使用原因，且原因合理。
e) 判定原则：
   测试结果应与预期结果相符，否则不符合要求。

6.1.8 强制访问控制机制

该检测项包含如下内容：

a) 安全要求：
   强制访问控制机制要求见T/TAF 230-2024 5.2.1 h)，即：
   操作系统应使用强制访问控制机制（例如SELinux），控制关键资源（例如加密密钥）的访问权限。
b) 预置条件：
   1) 厂商提供访问设备操作系统的安全途径，如安全shell；
   2) 厂商提供查看强制访问控制机制配置的途径，如相关操作命令。
c) 检测方法：
   连接并登陆设备，检查设备强制访问控制机制的启闭状态。
d) 预期结果：
   系统开启了强制访问控制机制。

e） 判定原则：
测试结果应与预期结果相符，否则不符合要求。

6.2 软件安全

6.2.1 通用安全漏洞扫描

该检测项包含如下内容：

a） 安全要求：
通用安全漏洞扫描要求见T/TAF 230-2024 5.2.2 a），即：
满足T/TAF 230-2024一级要求的设备中不应存在已公布的中危及以上级别安全漏洞，或具备补救措施防范漏洞风险；满足T/TAF 230-2024二级及三级要求的设备中不应存在已公布的所有级别安全漏洞，或具备补救措施防范漏洞风险。

b） 预置条件：
1） 测试机上已安装主流安全漏洞扫描工具；
2） 设备处于出厂默认配置。

c） 检测方法：
使用主流漏洞扫描工具，更新漏洞库后，对设备系统开展已知漏洞扫描测试。

d） 预期结果：
满足一级要求的设备的扫描结果中不存在中危及以上级别安全漏洞，或具备补救措施防范漏洞风险；满足二级及三级要求的设备的扫描结果中不存在所有级别的安全漏洞，或具备补救措施防范漏洞风险。

e） 判定原则：
测试结果应与预期结果相符，否则不符合要求。

6.2.2 软件包病毒扫描

该检测项包含如下内容：

a） 安全要求：
软件包病毒扫描要求见T/TAF 230-2024 5.2.2 b），即：
设备软件包中不应存在病毒等恶意代码。

b） 预置条件：
厂商提供软件包发布件。

c） 检测方法：
使用主流杀毒软件，更新病毒库后执行软件包扫描。

d） 预期结果：
扫描结果无病毒，未发现病毒。

e） 判定原则：
测试结果应与预期结果相符，否则不符合要求。

6.2.3 安全启动

该检测项包含如下内容：

a） 安全要求：
安全启动要求见T/TAF 230-2024 5.2.2 c），即：
设备应支持安全启动，在设备启动时逐级校验软件完整性。

b) 预置条件：

1) 获取设备软件包；

2) 产品资料中声明安全启动功能，提供安全启动方案介绍；

3) 厂商提供设备软件包修改方式及相应的工具；

4) 厂商提供设备尝试加载运行修改后软件包的方式及相应的工具；

5) 厂商提供查看安全启动中完整性验证是否成功的方式。

c) 检测方法：

分别篡改安全启动中不同阶段加载代码，修改至少1个字节内容后保存，并将篡改后的文件提供给设备，重启设备，查看设备是否加载运行篡改后的代码文件；每次篡改一个阶段的文件，其他阶段的文件保证未被修改。

d) 预期结果：

设备尝试加载运行篡改后的代码失败；

e) 判定原则：

测试结果应与预期结果相符，否则不符合要求。

6.2.4 升级包完整性验证

该检测项包含如下内容：

a) 安全要求：

升级包完整性验证要求见T/TAF 230-2024 5.2.2 d)，即：

设备加载软件升级包、补丁等文件时，应验证文件的完整性，拒绝加载被篡改的文件。

b) 预置条件：

设备正常管理。

c) 检测方法：

1) 使用厂商提供的正常软件升级包或补丁包，尝试加载到设备上；

2) 打开软件升级包或补丁包，修改至少1个字节内容后保存，尝试加载篡改后的升级包&补丁包到设备上。

d) 预期结果：

1) 软件升级包或补丁包加载成功；

2) 篡改后的升级包或补丁包不能加载到设备上。

e) 判定原则：

测试结果应与预期结果相符，否则不符合要求。

6.2.5 升级包签名验证

该检测项包含如下内容：

a) 安全要求：

升级包签名验证要求见T/TAF 230-2024 5.2.2 e)，即：

应使用数字签名技术验证软件升级包、补丁等文件的完整性和来源。

b) 预置条件：

1) 设备正常管理；

2) 厂商提供升级包、补丁等文件的完整性和来源验证说明文档。

c) 检测方法：

1) 查看升级包、补丁等文件的完整性和来源验证说明文档，查看是否使用数字签名技术；

2) 使用厂商提供的正常软件升级包或补丁包，尝试加载到设备上；

3) 打开软件升级包或补丁包，修改至少1个字节内容后保存，修改位置选取数字签名字段，尝试加载篡改后的升级包&补丁包到设备上。

d) 预期结果：

1) 文档中声明使用数字签名技术验证软件升级包、补丁等文件的完整性和来源；
2) 软件升级包或补丁包加载成功；
3) 篡改后的升级包或补丁包不能加载到设备上。

e) 判定原则：

测试结果应与预期结果相符，否则不符合要求。

6.2.6 基于硬件保护的信任根

该检测项包含如下内容：

a) 安全要求：

基于硬件保护的信任根要求见T/TAF 230-2024 5.2.2 f)，即：
应基于硬件机制保护安全启动使用的信任根不被篡改。

b) 预置条件：

1) 产品资料中声明安全启动功能，提供安全启动方案介绍；
2) 厂商提供安全启动相关模块代码。

c) 检测方法：

1) 查看安全启动方案相关文档，查看是否使用硬件机制保护安全启动使用的信任根不被篡改；
2) 检查安全启动相关模块代码，查看是否使用了方案文档中提到硬件机制保护安全启动使用的信任根。

d) 预期结果：

1) 文档中声明使用硬件机制保护安全启动使用的信任根不被篡改；
2) 安全启动代码中使用了方案文档中提到的硬件机制保护安全启动信任根。

e) 判定原则：

测试结果应与预期结果相符，否则不符合要求。

6.3 身份鉴别与访问控制

6.3.1 账号唯一性

该检测项包含如下内容：

a) 安全要求：

账号唯一性要求见T/TAF 230-2024 5.2.3 a)，即：
应对设备用户进行身份标识和鉴别，身份标识应具有唯一性。

b) 预置条件：

设备可正常管理。

c) 检测方法：

预先创建测试账号A，再次新建账号A（和原账号同名）。

d) 预期结果：

创建账号时，如果系统中已有同名账号，创建失败。

e) 判定原则：

测试结果应与预期结果相符，否则不符合要求。

6.3.2 用户管理

该检测项包含如下内容：

a) 安全要求：

用户管理要求见T/TAF 230-2024 5.2.3 b)，即：

若支持多用户，应具备创建、禁用（或主动锁定）、删除账号的能力，且相应操作应仅由具备安全管理员组权限的管理员账号方可实施。

b) 预置条件：

1) 设备可正常管理；

2) 厂商提供资料，对设备用户管理功能进行说明。

c) 检测方法：

1) 查看厂商提供的资料说明，确认设备是否具备用户管理功能（创建、修改、删除、禁用账号等）；

2) 使用管理员账号登录设备，尝试新增、修改、禁用、删除管理员账号以及普通账号；

3) 新增普通账号A（非管理员角色），尝试使用普通用户A进行用户管理操作。

d) 预期结果：

1) 设备提供分级或者分角色的用户管理功能，并且只能通过具备管理员组权限的管理员进行用户管理操作；

2) 管理员账号具备设备用户管理能力，可以正常新增、修改、禁用、删除管理员账号以及普通账号；

3) 操作失败，普通账号A（非管理员角色）无法进行用户管理操作。

e) 判定原则：

测试结果应与预期结果相符，否则不符合要求。

6.3.3 长期未用账号禁用

该检测项包含如下内容：

a) 安全要求：

长期未用账号禁用要求见T/TAF 230-2024 5.2.3 c)，即：

应支持自动禁用长期未使用的账号。

b) 预置条件：

设备可正常管理。

c) 检测方法：

1) 使用管理员账号登录系统，新建账号A，设置账号A的无活动禁用时间，尝试使用账号A登录系统；

2) 退出账号A，通过管理员账号登录，通过设置系统时间或其他方式，使设备时间超过账号A的无活动禁用时间，再次尝试登录账号A。

d) 预期结果：

1) 账号A可以正常登录到被测设备；

2) 登录失败，设备自动禁用长时间未登录使用的账号。

e) 判定原则：

测试结果应与预期结果相符，否则不符合要求。

6.3.4 角色权限管理

该检测项包含如下内容：

a) 安全要求：

角色权限管理要求见T/TAF 230-2024 5.2.3 d)，即：

应支持账号角色管理，对每个账号分配合适的角色，不同的角色具备不同的权限，应仅允许经过身份鉴别的账号执行权限范围内的操作。

b) 预置条件：

1) 设备可正常管理；
2) 厂商提供资料，对设备用户功能进行说明。

c) 检测方法：

1) 查看厂商提供的资料说明，确认设备是否具备角色权限管理机制；
2) 使用管理员账号登录设备，创建不同角色的测试账号，使用不同角色的测试账号登录设备，根据资料或者产品提供的不同权限对应的操作指令描述，分别尝试下发不同权限范围内的操作指令。

d) 预期结果：

1) 设备具备角色权限管理机制，不同角色权限范围不同；
2) 不同角色的测试账号只能下发对应权限范围内的操作指令，不能越权下发权限范围外的操作指令。

e) 判定原则：

测试结果应与预期结果相符，否则不符合要求。

6.3.5 口令安全策略

该检测项包含如下内容：

a) 安全要求：

口令安全策略要求见T/TAF 230-2024 5.2.3 e)，即：

使用口令鉴别方式时，应满足以下要求：

1) 应支持首次登录设备时强制修改默认口令或设置口令；
2) 应支持设置口令生存周期；
3) 应支持口令复杂度检查及长度检查，其中满足T/TAF 230-2024一级要求的设备，口令应至少包含如下字符中的三种：大写字母、小写字母、数字、特殊字符，长度至少为8个字符；满足T/TAF 230-2024二级及三级要求的设备，口令应至少包含如下字符中的四种：大写字母、小写字母、数字、特殊字符，长度至少为12个字符；
4) 应提供口令防暴力破解机制；
5) 用户修改口令应重新进行身份鉴别。

b) 预置条件：

1) 设备可正常管理；
2) 厂商提供资料，对设备口令安全策略进行说明。

c) 检测方法：

1) 查看厂商提供的资料说明，确认设备是否具备口令安全策略；
2) 将设备恢复出厂设置，如果设备存在默认账号，使用出厂默认账号首次登陆设备，观察是否需要修改口令；如果设备不存在默认账号，观察是否需要设置登录账号；
3) 创建设备账号A，使用不符合复杂度要求或者长度要求的口令；
4) 创建设备账号A，使用符合复杂度要求或者长度要求的口令；
5) 登陆账号A，尝试修改自身口令，观察是否重新对当前用户进行身份鉴别；

6） 修改账号A的口令为满足复杂度要求的字符串；
7） 修改账号A的口令有效期，通过设置系统时间或其他方式，使设备时间超过账号A的口令有效期，再次使用账号A登录设备；
8） 使用管理员账号登录，新建测试账号B，使用错误口令登录账号B；
9） 连续多次使用错误的口令登录账号B；
10） 使用正确的口令登录账号B。

d） 预期结果：
1） 设备应具备口令安全策略机制，包括口令符合复杂度要求，周期更换口令；支持口令防暴力破解机制；支持first login机制；
2） 存在默认账号的设备提示用户需要修改口令，未修改默认口令无法操作设备；不存在默认账号的设备，需要强制用户设置账号和口令后才能操作设备；
3） 创建账号A失败；
4） 创建账号A成功；
5） 需要输入当前用户口令才能修改成功；
6） 修改成功；
7） 无法登录设备；
8） 登录失败；
9） 设备提供防暴力破解机制，将攻击PC IP地址或者攻击账号锁定；
10） 在攻击IP或者账号锁定期间，使用正确的口令也无法登录，锁定结束后，才可以继续登录。

e） 判定原则：
测试结果应与预期结果相符，否则不符合要求。

6.3.6 鉴别失败反馈

该检测项包含如下内容：

a） 安全要求：
鉴别失败反馈要求见T/TAF 230-2024 5.2.3 f），即：
当出现鉴别失败时,设备应提供无差别反馈,避免提示“用户名错误”“口令错误”等类型的具体信息。

b） 预置条件：
设备可正常管理。

c） 检测方法：
使用错误口令登录账号A。

d） 预期结果：
登录失败，不会明确提示是用户名错误还是口令错误。

e） 判定原则：
测试结果应与预期结果相符，否则不符合要求。

6.3.7 远程认证管理

该检测项包含如下内容：

a） 安全要求：
远程认证管理要求见T/TAF 230-2024 5.2.3 g），即：
应支持远程认证管理方式。

b) 预置条件：
   1) 设备可正常管理；
   2) 厂商提供资料，对设备用户功能进行说明。
c) 检测方法：
   1) 查看厂商提供的资料说明，确认设备是否具备远程账号认证管理机制；
   2) 在设备上配置远程账号认证管理功能，并且与远程账号认证管理服务器正常通信，使用远程服务器上的账号A以及正确的口令登录设备；
   3) 使用远程服务器上的账号A以及错误的口令登录设备；
   4) 尝试使用设备本地账号B以及对应的口令登录设备；
   5) 构造设备与远程账号认证管理服务器通信中断，分别尝试使用远程账号认证管理服务器上的账号A和设备本地账号B登录设备。
d) 预期结果：
   1) 设备支持远程账号认证管理机制（例如：RADIUS、TACACS等）；
   2) 登录成功并且能够下发权限范围内的操作；
   3) 登录失败；
   4) 登录失败；
   5) 设备具备逃生机制，当设备与远程账号管理服务器通信中断时，远程账号A登录失败，本地账号B登录成功。
e) 判定原则：
   测试结果应与预期结果相符，否则不符合要求。

6.3.8 远程认证管理安全通道

该检测项包含如下内容：

a) 安全要求：
   远程认证管理安全通道要求见T/TAF 230-2024 5.2.3 h)，即：
   远程认证管理应支持使用安全的传输通道进行交互，如基于DTLS、TLS保护的RADIUS、TACACS认证等。
b) 预置条件：
   1) 设备可正常管理；
   2) 厂商提供资料，对设备用户功能进行说明。
c) 检测方法：
   1) 查看厂商提供的资料说明，确认设备是否支持安全的远程账号管理通道；
   2) 设备上配置安全的远程账号管理通道，并且与远程账号认证管理服务器正常通信，使用远程服务器上的账号A登录设备，测试过程中抓取设备与远程服务器通信报文。
d) 预期结果：
   1) 设备支持安全的远程账号管理通道（例如：使用基于DTLS、TLS保护的RADIUS）；
   2) 账号A能成功登录设备，设备与远程服务器之间通信报文加密传输（例如：使用TLS、DTLS等），无法截获通信数据明文。
e) 判定原则：
   测试结果应与预期结果相符，否则不符合要求。

6.3.9 弱口令字典

该检测项包含如下内容：

a) 安全要求：
弱口令字典要求见T/TAF 230-2024 5.2.3 i)，即：
应具备用户弱口令字典管理功能，并支持用户自行配置弱口令字典内容。
b) 预置条件：
设备可正常管理。
c) 检测方法：
1) 查询设备上是否存在预置的弱口令字典；
2) 创建设备账号A，使用预置弱口令字典中的口令，观察是否创建成功；
3) 创建设备账号A，使用非预置弱口令字典范围内的口令（符合设备其他口令安全策略）；
4) 修改账号A的口令，使用弱口令字典中的口令作为新口令；
5) 在设备上新增弱口令字典内容（新增口令符合其他口令安全策略），创建账号B，使用刚添加到弱口令字典中的字符作为口令。
d) 预期结果：
1) 设备上预置有弱口令字典，内容包含业界或设备商常用的弱口令；
2) 创建失败；
3) 创建成功；
4) 修改失败；
5) 弱口令字典添加成功，创建账号B失败。
e) 判定原则：
测试结果应与预期结果相符，否则不符合要求。

6.4 通信安全

6.4.1 通信主体身份认证

该检测项包含如下内容：
a) 安全要求：
通信主体身份认证要求见T/TAF 230-2024 5.2.4.1，即：
光传送网设备应对连接至管理接口的设备或系统（如网管系统）进行身份认证，仅允许合法主体接入管理接口。
b) 预置条件：
厂商提供资料，对连接至管理接口的设备或系统（如网管系统）的身份认证机制进行说明。
c) 检测方法：
1) 根据具体身份认证机制的设计，使用具备合法身份的设备或系统尝试连接至被测设备的管理接口；
2) 使用不具备合法身份的设备或系统尝试连接至被测设备的管理接口。
d) 预期结果：
1) 具备合法身份的设备或系统可成功连接被测设备管理接口；
2) 不具备合法身份的设备或系统连接被测设备管理接口被拒绝。
e) 判定原则：
测试结果应与预期结果相符，否则不符合要求。

6.4.2 通信协议安全

6.4.2.1 TLS/SSH 协议支持

该检测项包含如下内容：

a) 安全要求：

TLS/SSH协议支持要求见T/TAF 230-2024 5.2.4.2 a)，即：

应支持安全的TLS/SSH协议版本，并使用安全的加密算法套件。

b) 预置条件：

厂商提供资料，对设备管理通道进行说明。

c) 检测方法：

1) 对于支持TLS服务的设备，使用TLS协议扫描工具，扫描设备支持TLS协议的管理端口；

2) 对于支持SSH服务的设备，使用Nmap或类似工具扫描设备支持SSH协议的管理端口。

d) 预期结果：

1) 扫描结果显示设备支持的TLS版本为安全版本，未使用不安全协议（TLSv1.1、TLSv1.0、SSLv3、SSLv2）；同时设备支持的TLS协议算法套件为安全密码算法套件，未发现不安全密码算法套件；

2) 扫描结果显示设备支持的SSH协议版本为安全版本，支持的算法套件为安全密码算法套件，未发现不安全密码算法套件。

e) 判定原则：

测试结果应与预期结果相符，否则不符合要求。

6.4.2.2 SNMP 协议支持

该检测项包含如下内容：

a) 安全要求：

SNMP协议支持要求见T/TAF 230-2024 5.2.4.2 b)，即：

应支持安全的SNMP协议版本，并使用安全的加密算法套件。

b) 预置条件：

厂商提供资料，对设备管理通道进行说明。

c) 检测方法：

1) 在设备上查询SNMP相关配置；

2) 使用SNMP协议管理设备，通过Wireshark或类似抓包工具捕获设备交互的SNMP报文。

d) 预期结果：

1) 设备对外管理面通道使用安全协议SNMPv3进行加密保护，默认未使用不安全协议（SNMPv1、SNMPv2c）；SNMPv3协议默认使用安全的SHA-512、SHA-384、SHA-256认证算法和AES256、AES192、AES128加密算法；

2) 设备交互的SNMP报文使用SNMPv3协议，内容经过加密，不能看到明文通信内容。

e) 判定原则：

测试结果应与预期结果相符，否则不符合要求。

6.4.2.3 SFTP 协议支持

该检测项包含如下内容：

a) 安全要求：

SFTP协议支持要求见T/TAF 230-2024 5.2.4.2 c)，即：

应支持安全的SFTP协议，并使用安全的加密算法套件。

b) 预置条件：

厂商提供资料，对设备管理通道进行说明。

c) 检测方法：
   1) 对于支持SFTP服务端功能的设备，使用Nmap或类似工具扫描设备支持SSH协议的管理端口；
   2) 对于支持SFTP客户端的设备，通过操作触发SFTP协议交互，通过Wireshark或类似抓包工具，抓取SFTP协议交互报文，检查设备发送的protocol报文和Key Exchange Init报文。
d) 预期结果：
   1) 扫描结果显示设备支持的SSH版本为安全版本，同时设备支持的SSH协议算法套件为安全密码算法套件，未发现不安全密码算法套件；
   2) protocol报文中设备支持的SSH协议版本为安全版本，Key Exchange Init报文中，设备携带的支持算法套件为安全密码算法套件，未发现不安全密码算法套件。
e) 判定原则：
   测试结果应与预期结果相符，否则不符合要求。

6.4.3 证书使用

6.4.3.1 基于证书的身份认证

该检测项包含如下内容：

a) 安全要求：
   基于认证的身份认证要求见T/TAF 230-2024 5.2.4.3 a)，即：
   设备应支持基于数字证书的身份认证机制。
b) 预置条件：
   1) 设备可正常管理；
   2) 厂商提供证书导入/更新操作界面或命令行，并提供操作指导。
c) 检测方法：
   1) 构建基于设备证书认证设备身份的场景，在设备和验证方使用配套的证书，验证方验证设备身份；
   2) 通过证书替换功能单独替换设备数字证书，再次尝试在验证方验证设备身份；
   3) 更新验证方侧使用的证书，与步骤2）中替换的设备证书匹配，再次尝试在验证方验证设备身份。
d) 预期结果：
   1) 设备身份验证成功；
   2) 设备身份验证失败；
   3) 设备身份验证成功。
e) 判定原则：
   测试结果应与预期结果相符，否则不符合要求。

6.4.3.2 设备证书正确性校验

该检测项包含如下内容：

a) 安全要求：
   设备证书正确性校验要求见T/TAF 230-2024 5.2.4.3 b)，即：
   设备导入数字证书时，应对证书正确性进行校验。
b) 预置条件：
   1) 设备可正常管理；

2） 设备提供基于证书的身份认证；
3） 厂商提供证书导入/更新操作界面或命令行，并提供操作指导。

c） 检测方法：
尝试导入与设备证书请求文件（CSR）不匹配的证书（例如：不同的公私钥，不同的CN名称等）。

d） 预期结果：
导入证书到设备上失败。

e） 判定原则：
测试结果应与预期结果相符，否则不符合要求。

6.4.3.3 设备证书更新

该检测项包含如下内容：

a） 安全要求：
设备证书更新要求见T/TAF 230-2024 5.2.4.3 c)，即：
设备应支持数字证书的更新或替换。

b） 预置条件：
1） 设备可正常管理；
2） 设备提供基于证书的身份认证；
3） 厂商提供证书导入/更新操作界面或命令行，并提供操作指导。

c） 检测方法：
1） 重新进行设备数字证书申请，生成新证书；
2） 将步骤1）生成的证书导入设备；
3） 将步骤2）导入的数字证书应用到需要使用数字证书的特性中，验证数字证书是否生效。例如数字证书应用于某个协议端口（例如TLS），使用扫描工具（例如testssl）对设备使用证书的端口进行扫描，查看扫描结果是否显示新导入的证书生效。

d） 预期结果：
1） 证书生成成功；
2） 导入证书成功；
3） 证书应用成功。

e） 判定原则：
测试结果应与预期结果相符，否则不符合要求。

6.4.3.4 吊销证书的处理

该检测项包含如下内容：

a） 安全要求：
吊销证书的处理要求见T/TAF 230-2024 5.2.4.3 d)，即：
设备应支持吊销证书的处理。

b） 预置条件：
1） 设备可正常管理；
2） 设备提供基于证书的身份认证；
3） 厂商提供证书导入/更新操作界面或命令行，并提供操作指导。

c） 检测方法：
1） 导入包含设备当前证书的吊销列表文件到设备；
2） 尝试使用被吊销的证书与设备建立连接。

d) 预期结果：
1) 设备导入吊销列表成功；
2) 连接失败。
e) 判定原则：
测试结果应与预期结果相符，否则不符合要求。

6.4.3.5 设备证书过期告警

该检测项包含如下内容：
a) 安全要求：
设备证书过期告警要求见T/TAF 230-2024 5.2.4.3 e)，即：
应支持设备证书过期告警。
b) 预置条件：
1) 设备可正常管理；
2) 设备提供基于证书的身份认证。
c) 检测方法：
修改设备系统时间，使设备上数字证书即将或已经过期。
d) 预期结果：
设备支持证书即将或已经过期提示功能（例如：上报告警、事件等），提示用户证书即将或已经过期，需要及时处理和更新。
e) 判定原则：
测试结果应与预期结果相符，否则不符合要求。

6.4.3.6 证书可视化管理

该检测项包含如下内容：
a) 安全要求：
证书可视化管理要求见T/TAF 230-2024 5.2.4.3 f)，即：
应支持查询证书状态、证书有效期、证书应用场景等信息。
b) 预置条件：
1) 设备可正常管理；
2) 设备提供基于证书的身份认证。
c) 检测方法：
检查产品是否提供设备证书状态、证书有效期、证书应用场景等信息的途径。
d) 预期结果：
产品提供了查看设备上的证书信息的途径，查询结果中的证书信息至少包括：证书序列号、证书有效期、颁发者信息、使用者信息、证书的应用场景。
e) 判定原则：
测试结果应与预期结果相符，否则不符合要求。

6.5 数据安全

6.5.1 敏感数据匿名处理

该检测项包含如下内容：
a) 安全要求：

敏感数据匿名处理要求见T/TAF 230-2024 5.2.5 a)，即：
设备上的敏感数据（如口令、私钥等）不应在操作时进行明文显示。

b) 预置条件：
厂商提供敏感数据清单和配置界面。

c) 检测方法：
1) 通过配置界面/命令行进行涉及敏感数据的相关操作，例如：新增账号，修改账号密码、配置协议认证密钥等，检查配置界面、菜单、命令行回显信息；
2) 查询设备操作日志、安全日志。

d) 预期结果：
1) 配置界面、菜单、命令行回显中对敏感数据进行匿名化处理（例如回显*号，或者不回显输入的字符等），不会明文回显输入字符；
2) 设备操作日志和安全日志中针对敏感数据进行匿名化处理（例如以*号代替），不会明文记录输入的敏感信息。

e) 判定原则：
测试结果应与预期结果相符，否则不符合要求。

6.5.2 敏感数据加密存储

该检测项包含如下内容：

a) 安全要求：
敏感数据加密存储要求见T/TAF 230-2024 5.2.5 b)，即：
设备上的敏感数据（如口令、私钥等）应进行加密存储。

b) 预置条件：
1) 设备正常管理；
2) 厂商提供敏感数据清单和存储有敏感数据的配置文件查看方式；
3) 厂商提供数据加密存储模块的源代码。

c) 检测方法：
1) 查看存储有敏感数据的配置文件中的内容；
2) 对设备源码进行审视，检查进行数据加密存储的逻辑。

d) 预期结果：
1) 厂商定义的敏感数据配置文件中使用密文保存；
2) 设备处理函数中使用安全的加密算法进行加密存储。

注：在不需要还原数据的场景可使用安全的不可逆算法对数据进行加密。

e) 判定原则：
测试结果应与预期结果相符，否则不符合要求。

6.5.3 传输加密

该检测项包含如下内容：

a) 安全要求：
传输加密要求见T/TAF 230-2024 5.2.5 c)，即：
设备应支持传输加密（如OTNSec）能力，保护传输数据的机密性。

b) 预置条件：
设备已启用传输加密。

c) 检测方法：

构建业务数据窃听场景，其中接收者可与被测设备正常通信，且已配置为可正确解密加密后的业务数据；窃听者未配置解密功能；被测设备发送数据，对比接收者和窃听者收到的数据。

d) 预期结果：

接收者收到的数据信息与窃听者不同。

e) 判定原则：

测试结果应与预期结果相符，否则不符合要求。

6.5.4 传输加密算法

该检测项包含如下内容：

a) 安全要求：

传输加密算法要求见T/TAF 230-2024 5.2.5 d)，即：

传输数据的加密，应使用安全强度不弱于128bit的密码算法。

b) 预置条件：

1) 设备支持业务数据传输加密；

2) 厂商提供业务数据加密模块的代码。

c) 检测方法：

检视业务加密模块的代码，查看是否对业务数据进行加密，观察其加密过程使用的加密算法及其强度。

d) 预期结果：

业务数据使用了加密保护，且算法安全强度大于或等于128bit。

e) 判定原则：

测试结果应与预期结果相符，否则不符合要求。

6.5.5 密钥管理

该检测项包含如下内容：

a) 安全要求：

密钥管理要求见T/TAF 230-2024 5.2.5 e)，即：

应采用多级密钥管理机制，保护密钥的机密性。

b) 预置条件：

1) 厂商提供密钥管理机制相关资料；

2) 厂商提供密钥管理相关源代码。

c) 检测方法：

1) 检视厂商提供的资料和设备代码，查看是否具有独立的密钥管理组件或服务；

2) 检视设备代码，查看设备密钥管理是否具备多级密钥设计，是否对密钥的机密性进行保护，密钥管理机制实现是否与厂商提供的设备密钥管理资料一致；

3) 检视设备代码，查看密钥管理机制是否包含密钥派生、密钥更新、密钥销毁等一个或多个环节的内容。

d) 预期结果：

1) 设备具有密钥管理机制，且具有单独的密钥管理组件或服务；

2) 设备密钥管理机制至少具备两层密钥设计，下层密钥可用于保护上层密钥的机密性，例如只存在设备根密钥和应用层密钥两层密钥的系统，设备根密钥可用于应用层密钥的加密保护；

3) 设备密钥管理存在密钥派生、密钥更新、密钥销毁等一个或多个环节的内容。

e） 判定原则：
测试结果应与预期结果相符，否则不符合要求。

6.6 防护能力

6.6.1 管理端口防攻击

6.6.1.1 防 ARP 攻击

该检测项包含如下内容：

a） 安全要求：
防ARP攻击要求见T/TAF 230-2024 5.2.6.1 a)c)，即：
1） 应具备防ARP攻击能力；
2） 应具备流量控制功能，在设备遭受DoS攻击时，保证设备正常运行。

b） 预置条件：
设备正常管理。

c） 检测方法：
针对设备管理端口，构造ARP类型的DoS攻击流量，持续60s。

d） 预期结果：
DoS攻击期间设备不复位，停止攻击后，设备能正常恢复管理。

e） 判定原则：
测试结果应与预期结果相符，否则不符合要求。

6.6.1.2 防报文 DoS 攻击

该检测项包含如下内容：

a） 安全要求：
防报文DoS攻击要求见T/TAF 230-2024 5.2.6.1 b)c)，即：
1） 应具备防ICMP/UDP/TCP SYN报文DoS攻击能力；
2） 应具备流量控制功能，在设备遭受DoS攻击时，保证设备正常运行。

b） 预置条件：
设备正常管理。

c） 检测方法：
1） 挑选设备对外提供的TCP通信服务端口，构造TCP类型的DoS攻击流量攻击设备管理端口，例如：TCP SYN FLOOD\SYN ACK FLOOD等；
2） 挑选设备对外提供的UDP通信服务端口，构造UDP类型的DoS攻击流量攻击设备管理端口，例如：UDP FLOOD\UDP FRAGMENT FLOOD等。

d） 预期结果：
1） DoS攻击期间设备不复位，停止攻击后，设备能正常恢复管理；
2） DoS攻击期间设备不复位，停止攻击后，设备能正常恢复管理。

e） 判定原则：
测试结果应与预期结果相符，否则不符合要求。

6.6.2 暴露面最小化

6.6.2.1 默认开放服务和端口

该检测项包含如下内容：

a) 安全要求：

默认开放服务和端口要求见T/TAF 230-2024 5.2.6.2 a)及GB 40050-2021 5.6 a)，即：

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) 预置条件：

1) 设备运行于默认状态，默认状态为设备出厂设置时的配置状态；

2) 厂商提供所有默认开启的服务、对应的端口及用途、管理员权限账号的说明材料。

c) 检测方法：

1) 使用扫描工具对设备进行全端口扫描，查看默认状态开启的服务和对应的端口，是否与厂商提供的说明材料内容一致、是否仅开启必要的服务和对应的端口；

2) 配置设备，关闭默认开启的端口和服务，使用扫描工具对设备再次进行扫描，查看扫描结果，检查默认开启的端口和服务是否被关闭。

d) 预期结果：

1) 默认状态下，设备仅开启了必要的服务和对应的端口，默认开启的服务和端口与厂商提供的说明材料内容一致；

2) 用户可以自行关闭默认开启的服务和对应的端口。

e) 判定原则：

测试结果应与预期结果相符，否则不符合要求。

6.6.2.2 开启非默认开放服务和端口

该检测项包含如下内容：

a) 安全要求：

开启非默认开放服务和端口要求见T/TAF 230-2024 5.2.6.2 b)及GB 40050-2021 5.6 b)，即：

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。

b) 预置条件：

1) 设备运行于默认状态，默认状态为设备出厂设置时的配置状态；

2) 厂商提供设备非默认开放端口和服务对应关系的说明材料；

3) 厂商提供说明材料，说明开启非默认开放端口和服务的配置方式，以及如何让用户知晓和同意开启非默认开放端口和服务。

c) 检测方法：

按照厂商提供的说明材料，配置设备，开启非默认开放的端口和服务，确认是否经过用户知晓且同意才可启用。

d) 预期结果：

非默开放的端口和服务，应在用户知晓且同意后才可启用。

e) 判定原则：

测试结果应与预期结果相符，否则不符合要求。

6.6.2.3 调试接口

该检测项包含如下内容：

a) 安全要求：

调试接口要求见T/TAF 230-2024 5.2.6.2 c)，即：

设备主控板上不应存在调试接口或调试接口不可用。

b) 预置条件：
厂商提供产品资料或实现方案。
c) 检测方法：
1) 查看厂商资料中设备主控板物理接口描述；
2) 查看主控板硬件接口及PCB板，是否存在硬件调试接口；若存在，查看是否可用。
d) 预期结果：
1) 资料中显示主控板不存在硬件调试接口，或即使存在但已采取措施使其不可用；
2) 主控板硬件接口及PCB板未发现资料中声明存在的调试接口之外的硬件调试接口，已发现的调试接口不可用。
e) 判定原则：
测试结果应与预期结果相符，否则不符合要求。

6.6.2.4 标识丝印

该检测项包含如下内容：
a) 安全要求：
标识丝印要求见T/TAF 230-2024 5.2.6.2 d)，即：
设备主控板上不应存在调试接口的标识丝印。
b) 预置条件：
无。
c) 检测方法：
检查被测设备主控板PCB板，查看关键安全模块上是否有印刷或张贴调试接口标识丝印。
d) 预期结果：
被测设备主控板的PCB板无调试接口标识丝印。
e) 判定原则：
测试结果应与预期结果相符，否则不符合要求。

6.6.3 备份恢复与冗余

6.6.3.1 本地备份

该检测项包含如下内容：
a) 安全要求：
本地备份要求见T/TAF 230-2024 5.2.6.3 a)，即：
应支持设备本地备份及备份导出功能，实现异常场景业务恢复。
b) 预置条件：
设备正常部署。
c) 检测方法：
1) 触发设备数据库备份导出功能，观察是否备份成功；
2) 设备清库，然后使用步骤1）中备份的数据库来恢复，观察是否可以恢复成功。
d) 预期结果：
1) 数据备份成功；
2) 数据恢复成功。
e) 判定原则：
测试结果应与预期结果相符，否则不符合要求。

6.6.3.2 备份数据完整性保护

该检测项包含如下内容：

a) 安全要求：
备份数据完整性保护要求见T/TAF 230-2024 5.2.6.3 b)，即：
应提供对备份文件进行完整性保护的措施。

b) 预置条件：
设备支持备份功能。

c) 检测方法：
1) 使用数据库备份导出功能，导出备份数据；
2) 修改导出的数据内容，尝试使用修改后的数据内容进行恢复。

d) 预期结果：
1) 数据可以备份成功；
2) 因完整性校验，备份恢复失败。

e) 判定原则：
测试结果应与预期结果相符，否则不符合要求。

6.6.3.3 资源冗余设计

该检测项包含如下内容：

a) 安全要求：
资源冗余设计要求见T/TAF 230-2024 5.2.6.3 c)及GB 40050-2021 5.2 a)，即：
设备整机应支持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。

b) 预置条件：
1) 厂商提供支持冗余和自动切换的部件清单；
2) 被测设备关键部件配置冗余。

c) 检测方法：
按照厂商提供的关键冗余部件说明文档，分别拔掉或关闭处于运行状态的关键部件，等待一段时间并观察被测设备的工作状态，查看被测设备是否能够自动启用备用关键部件。

d) 预期结果：
被测设备可以自动启用备用关键部件，工作正常。

e) 判定原则：
测试结果应与预期结果相符，否则不符合要求。

6.6.3.4 备份模式

该检测项包含如下内容：

a) 安全要求：
备份模式要求见T/TAF 230-2024 5.2.6.3 d)，即：
应支持定时备份和手动备份两种模式。

b) 预置条件：
设备正常部署。

c) 检测方法：
1) 手动触发设备数据库备份导出功能，观察是否备份成功；

2） 查看设备数据库是否支持定时备份功能，使能定时备份功能，配置定时备份时间，到时间后查看是否可以备份成功。

d） 预期结果：

1） 手动备份成功；

2） 定时备份成功。

e） 判定原则：

测试结果应与预期结果相符，否则不符合要求。

6.6.4 异常检测能力

6.6.4.1 账号暴力破解检测

该检测项包含如下内容：

a） 安全要求：

账号暴力破解检测要求见T/TAF 230-2024 5.2.6.4 a)，即：

应具备账号暴力破解入侵行为的检测和告警能力。

b） 预置条件：

开启入侵检测相关功能。

c） 检测方法：

1） 验证产品是否支持账号暴力破解入侵检测，且支持对暴力破解的相关配置；

2） 暴力破解达到最小登录速率和登录次数的阈值，观察是否有相应的告警或事件。

d） 预期结果：

1） 入侵检测功能支持账号暴力破解入侵检测；且支持相关配置如最小尝试登录次数、最小尝试登录速率等；

2） 可看到上报了暴力破解告警或事件，并且能够看到详细的描述（包含但不限于：登录次数、攻击速率、登录方式、登录源IP、攻击发生时间、暴力破解使用的账号、告警或事件名称/级别、被攻击设备IP/名称等）。

e） 判定原则：

测试结果应与预期结果相符，否则不符合要求。

6.6.4.2 操作系统入侵检测

该检测项包含如下内容：

a） 安全要求：

操作系统入侵检测要求见T/TAF 230-2024 5.2.6.4 b)，即：

应具备常见操作系统入侵行为的检测和告警能力。

b） 预置条件：

开启入侵检测相关功能。

c） 检测方法：

1） 对系统中的关键文件进行权限提升操作，观察是否有相应的告警或事件；

2） 对系统中的shell文件进行权限提升操作，观察是否有相应的告警或事件；

3） 在系统中添加超级用户（如UID为0的用户），观察是否有相应的告警或事件。

d） 预期结果：

1) 可看到上报了文件权限提升的告警或事件，且能够看到详细的描述（包含但不限于：入侵发生时间、操作的文件路径、操作内容和结果、告警或事件类型/名称/级别、被攻击设备IP/名称等）；
2) 可看到上报了shell权限提升的告警或事件，且能够看到详细的描述（包含但不限于：入侵发生时间、操作的文件路径、操作内容和结果、告警或事件类型/名称/级别、被攻击设备IP/名称等）；
3) 可看到上报了非法超级用户的告警或事件，且能够看到详细的描述（包含但不限于：入侵发生时间、创建的用户信息、告警或事件类型/名称/级别、被攻击设备IP/名称等）。

e) 判定原则：
测试结果应与预期结果相符，否则不符合要求。

6.6.4.3 异常账号行为告警

该检测项包含如下内容：

a) 安全要求：
异常账号行为告警要求见T/TAF 230-2024 5.2.6.4 c)，即：
应支持对异常账号操作行为的检测和告警。

b) 预置条件：
开启入侵检测相关功能。

c) 检测方法：
1) 对账号A进行暴力破解尝试，之后使用正确的口令对账号A进行登录操作，观察是否有相应的告警或事件；
2) 使用账号A创建新的账号B，观察是否有相应的告警或事件；
3) 使用账号B登录设备，观察是否有相应的告警或事件；
4) 使用账号B修改自身账号口令，观察是否有相应的告警或事件；
5) 使用账号A删除新建账号B，观察是否有相应的告警或事件。

d) 预期结果：
1) 可看到上报了与异常账号A登录相关的告警或事件；并且能够看到详细的描述（包含但不限于：登录方式、登录源IP、攻击发生时间、尝试登录的账号、告警或事件名称/级别、被攻击设备IP/名称等）；
2) 可看到上报了异常账号创建的告警或事件，并且能够看到详细的描述（包含但不限于：登录方式、登录源IP、攻击发生时间、进行操作的账号、尝试创建的账号、告警或事件名称/级别、被攻击设备IP/名称等）；
3) 可看到上报了非授权账号登录的告警或事件，并且能够看到详细的描述（包含但不限于：登录方式、登录源IP、攻击发生时间、操作的非授权账号、告警或事件名称/级别、被攻击设备IP/名称等）；
4) 可看到上报了非授权更改口令的告警或事件，并且能够看到详细的描述（包含但不限于：登录方式、登录源IP、攻击发生时间、操作的非授权账号、告警或事件名称/级别、被攻击设备IP/名称等）；
5) 可看到上报了非授权删除账号的告警或事件，并且能够看到详细的描述（包含但不限于：登录方式、登录源IP、攻击发生时间、进行操作的账号、操作的非授权账号、告警或事件名称/级别、被攻击设备IP/名称等）。

e) 判定原则：
测试结果应与预期结果相符，否则不符合要求。

6.6.5 安全配置管理

该检测项包含如下内容：

a) 安全要求：

安全配置管理要求见T/TAF 230-2024 5.2.6.5，即：

光传送网设备应支持安全配置管理能力，应提供安全配置基线管理、安全配置核查功能。

b) 预置条件：

1) 设备恢复到出厂设置后掉电重新启动；
2) 产品配套资料包含产品安全配置加固指导文档。

c) 检测方法：

1) 使用安全配置核查功能查看设备支持的协议是否包含telnet、FTP、HTTP等不安全协议，是否将这些不安全协议关闭；
2) 如果设备支持telnet功能，检查设备是否可以进行telnet登录；
3) 查看安全配置核查结果中设备使用的TLS版本号（如使用）、SNMP版本号（如使用）、SSH版本号（如使用）；
4) 查看安全配置核查结果中TLS（如使用）、SSH（如使用）是否包含不安全算法，以及对应的提示；
5) 修改安全配置基线或设备相关配置，使得设备实际使用的TLS（如使用）、SNMP（如使用）、SSH（如使用）版本与安全基线不一致，并观察安全配置核查结果；
6) 修改安全配置基线或设备相关配置，使得设备实际使用的TLS（如使用）、SSH（如使用）的算法与安全基线不一致，并观察安全配置核查结果；
7) 如果设备具备telnet登录功能，修改设备支持telnet登陆，观察安全配置核查结果；
8) 修改安全配置基线或设备相关配置，使得设备实际使用的TLS（如使用）、SNMP（如使用）、SS（如使用）H协议版本与安全基线一致，并观察安全配置核查结果；
9) 修改安全配置基线或设备相关配置，使得设备实际使用的TLS（如使用）和SSH（如使用）的算法与安全基线一致，并观察安全配置核查结果；
10) 如果设备具备telnet登录功能，配置telnet为非风险项，观察安全配置核查结果。

d) 预期结果：

1) 不支持telnet、FTP、HTTP等不安全协议或在安全配置核查模块可看到这些协议的状态为关闭；
2) 设备支持telnet功能时，默认情况下无法进行telnet登录；
3) TLS、SNMP、SSH协议使用的版本为安全版本；
4) TLS和SSH的算法套扫描结果中，不包含SHA-1、AES-CBC等不安全算法套件：
5) 安全配置核查结果中可以看到TLS、SNMP、SSH版本为不安全的协议版本的提示；
6) 安全配置核查结果中可以看到TLS、SSH协议使用不安全的算法的提示；
7) 如果设备具备telnet登录功能，安全配置核查结果中可以看到开启telnet的风险提示；
8) 安全配置核查结果中可以看到TLS、SNMP、SSH协议版本为不安全的协议版本的提示消失；
9) 安全配置核查结果中可以看到TLS、SSH协议使用不安全的算法的提示消失；
10) 如果设备具备telnet登录功能，安全配置核查结果中可以看到开启telnet的风险提示消失。

e) 判定原则：

测试结果应与预期结果相符，否则不符合要求。

6.7 日志审计和管理

6.7.1 日志记录内容

该检测项包含如下内容：

a) 安全要求：

日志记录内容要求见T/TAF 230-2024 5.2.7 a)，即：

应支持对管理员用户活动、操作指令等操作记录日志，记录应包括用户ID、时间、事件类型等。

b) 预置条件：

设备正常管理。

c) 检测方法：

1) 使用管理员账号登录设备，进行用户管理操作，例如：添加用户A，并且修改用户A属性，查询设备日志；

2) 对设备进行业务配置，查询设备日志。

d) 预期结果：

1) 设备日志中记录了用户登录、增加用户、修改用户属性操作，日志记录中包含了操作发生的时间、操作者IP地址、操作用户、操作的类型、操作的结果等内容；

2) 设备日志中记录了业务配置操作，日志记录中包含了操作发生的时间、操作者IP地址、操作用户、操作的类型、操作的结果等内容。

e) 判定原则：

测试结果应与预期结果相符，否则不符合要求。

6.7.2 日志访问权限控制

该检测项包含如下内容：

a) 安全要求：

日志访问权限控制要求见T/TAF 230-2024 5.2.7 b)，即：

应仅允许管理员用户访问和查看日志信息。

b) 预置条件：

设备正常管理。

c) 检测方法：

1) 使用管理员账号登录设备，进行日志查询操作；

2) 新增普通用户A，使用普通用户A登录设备，进行日志查询操作。

d) 预期结果：

1) 查询成功，管理员用户可以查询设备日志；

2) 查询失败，非管理员用户不能查询设备日志。

e) 判定原则：

测试结果应与预期结果相符，否则不符合要求。

6.7.3 日志删除和修改保护

该检测项包含如下内容：

a) 安全要求：

日志删除和修改保护要求见T/TAF 230-2024 5.2.7 c)，即：

应禁止对安全操作相关日志的删除和修改。

b) 预置条件：

设备正常管理。

c) 检测方法：

1) 登录设备，尝试下发删除文件或者初始化文件命令，对记录安全操作的相关日志文件进行删除和初始化；

2) 尝试通过直接修改文件或者下载文件覆盖等方式篡改安全操作相关日志文件。

d) 预期结果：

1) 无删除或者初始化安全操作相关日志的操作途径；或者删除或初始化日志失败，检查日志信息无变化；

2) 无修改或覆盖安全操作相关日志文件途径，或修改/覆盖日志文件的操作失败。

e) 判定原则：

测试结果应与预期结果相符，否则不符合要求。

6.7.4 日志备份协议

该检测项包含如下内容：

a) 安全要求：

日志备份协议要求见T/TAF 230-2024 5.2.7 d)，即：

应支持基于安全传输协议的日志备份机制，例如基于TLS的Syslog协议，并将日志记录实时传输到服务器。

b) 预置条件：

1) 设备正常管理；

2) 厂商提供日志机制设计相关资料。

c) 检测方法：

1) 检查设备资料，确认设备是否支持安全的日志传输协议（如SYSLOG over TLS）；

2) 在设备上进行操作生成日志，触发设备与日志服务器进行交互，在服务器上通过Wireshark、TCPDUMP或类似工具抓包；

3) 构造设备与日志服务器中断场景。

d) 预期结果：

1) 设备支持安全的日志传输协议；

2) 日志服务器上能收到设备上的操作日志信息，设备和日志服务器之间传输的报文内容进行了加密，日志信息不会明文发送；加密传输使用的协议和算法套件为业界推荐的安全协议和加密算法套件；

3) 设备上报告警信息，提示用户设备与日志服务器连接中断。

e) 判定原则：

测试结果应与预期结果相符，否则不符合要求。

6.7.5 日志文件访问控制

该检测项包含如下内容：

a) 安全要求：

日志文件访问控制要求见T/TAF 230-2024 5.2.7 e)，即：

应对日志文件进行访问控制，应仅限创建文件的主体进行读写操作，其所属用户组仅可进行读操作，其他用户不可进行读写操作。

b) 预置条件：

设备正常管理。

c） 检测方法：
登录设备，检查日志文件的访问权限设置。
d） 预期结果：
日志文件访问权限设置合理，仅限创建文件的主体进行读写操作，其所属用户组仅可进行读操作，其他用户不可进行读写操作。
e） 判定原则：
测试结果应与预期结果相符，否则不符合要求。

7 安全保障评估方法

7.1 设计和开发

7.1.1 开源软件恶意程序扫描

该检测项包含如下内容：
a） 安全要求：
开源软件恶意程序扫描要求见T/TAF 230-2024 5.3.1 a)，即：
设备使用的开源软件应经过主流杀毒软件扫描，以确保无恶意程序植入。
b） 预置条件：
厂商提供所用的开源软件清单和开源软件病毒扫描材料。
c） 检测方法：
查看厂商提供的材料，确认是否具备开源软件病毒扫描的记录。
d） 预期结果：
材料中体现了厂商已对所有使用的开源软件进行了病毒扫描；查看开源软件病毒扫描记录，扫描结果无病毒，扫描所用杀毒软件为业界主流杀毒软件。
e） 判定原则：
测试结果应与预期结果相符，否则不符合要求。

7.1.2 开源软件漏洞修复

该检测项包含如下内容：
a） 安全要求：
开源软件漏洞修复要求见T/TAF 230-2024 5.3.1 b)，即：
应对已发现的开源软件的安全漏洞进行及时修复，或提供补救措施。
b） 预置条件：
厂商提供所用的开源软件清单和开源软件漏洞修复清单。
c） 检测方法：
查看厂商提供的开源软件漏洞修复清单，检查其中已修复的漏洞，厂商是否有相关的漏洞感知、影响分析、修复记录、漏洞公告等资料和测试记录。
d） 预期结果：
材料中体现了厂商已对所有使用的开源软件进行了漏洞扫描；针对已修复的开源软件CVE漏洞，厂商记录有漏洞录入时间、漏洞分析记录、漏洞修复记录，官网发布有此漏洞已修复清单。
e） 判定原则：
测试结果应与预期结果相符，否则不符合要求。

7.1.3 开源软件开源使用声明

该检测项包含如下内容：

a) 安全要求：
开源软件开源使用声明要求见T/TAF 230-2024 5.3.1 c)，即：
使用开源软件应提供对外开源使用声明，并保证用户在获取产品软件包时可获取该内容。

b) 预置条件：
无。

c) 检测方法：
从厂商的软件包获取地址或软件包中获取开源软件使用声明。

d) 预期结果：
可成功获取开源软件使用声明。

e) 判定原则：
测试结果应与预期结果相符，否则不符合要求。

7.1.4 开源软件许可证

该检测项包含如下内容：

a) 安全要求：
开源软件许可证要求见T/TAF 230-2024 5.3.1 d)，即：
应确保提供所有使用的开源软件的许可证，且履行许可证要求。

b) 预置条件：
厂商随软件包发布产品开源软件声明材料。

c) 检测方法：
获取开源软件使用声明，查看其中是否写明产品所使用的开源软件及其版权和许可证信息。

d) 预期结果：
开源软件使用声明中包括开源软件名称、版本、copyright、许可证（license）和Written Offer等信息。

e) 判定原则：
测试结果应与预期结果相符，否则不符合要求。

7.1.5 第三方软件安全风险防范

该检测项包含如下内容：

a) 安全要求：
第三方软件安全风险防范要求见T/TAF 230-2024 5.3.1 e)，即：
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。

b) 预置条件：
厂商提供防范第三方关键部件、固件或软件可能引入的安全风险的说明材料。

c) 检测方法：
查看厂商提供的防范第三方关键部件、固件或软件可能引入的安全风险的说明材料，分析验证防范措施的有效性，确认措施的实施记录。

d) 预期结果：
厂商能够提供防范第三方关键部件、固件或软件可能引入的安全风险的说明材料，验证了防范措施的有效性，留存了措施的实施记录。

e） 判定原则：

测试结果应与预期结果相符，否则不符合要求。

7.1.6 开源软件版本管理

该检测项包含如下内容：

a） 安全要求：

开源软件版本管理要求见T/TAF 230-2024 5.3.1 f)，即：

应对设备使用的开源软件进行管理，保证设备使用的开源软件为开源社区官网或官方托管网站的正式发布版本，核心软件所用开源软件应优先选择开源社区官网或官方托管网站LTS版本或稳定版本，不应使用已停止维护的开源软件版本。

b） 预置条件：

1） 厂商提供所用的开源软件清单；

2） 厂商提供开源软件使用规范；

3） 厂商提供最终产品中所用开源软件扫描结果。

c） 检测方法：

1） 查看厂商提供的开源软件使用规范，查看是否规定核心软件使用的开源软件版本选择规则，是否选用正式版本，并优先选用开源社区或官方托管网站LTS版本或稳定版本，不含有非正式版本（如：Beta（测试版本）、Released candidate（最终测试版本））；

2） 查看厂商提供的被测设备中所用开源软件的扫描结果，比对开源软件社区或官方托管网站的信息，验证设备中核心软件使用的开源软件是否优先选择LTS版本或稳定版本。

d） 预期结果：

1） 开源软件使用规范中明确了开源软件版本选择规则，其中核心软件使用的开源软件优先选用开源社区或官方托管网站LTS版本或稳定版本；

2） 被测设备核心软件使用的开源软件版本属于开源社区或官方托管网站LTS版本或稳定版本，开源社区或官方托管网站无LTS版本或稳定版本时，设备所用开源软件至少为正式发布版本。

e） 判定原则：

测试结果应与预期结果相符，否则不符合要求。

7.1.7 开源软件源码可追溯

该检测项包含如下内容：

a） 安全要求：

开源软件源码可追溯要求见T/TAF 230-2024 5.3.1 g)，即：

应提供措施确保设备使用的开源软件源码可追溯到来源社区。

b） 预置条件：

厂商提供开源软件使用规范。

c） 检测方法：

查看开源软件引入流程或开源软件管理系统，查看是否记录开源软件源码来源的社区，或是否可检查开源软件源码来源的社区。

d） 预期结果：

开源软件引入流程或管理系统中已记录开源软件源码来源的社区，或存在检查开源软件源码来源社区的途径。

e） 判定原则：

测试结果应与预期结果相符，否则不符合要求。

7.1.8 开源软件版本归一

该检测项包含如下内容：

a) 安全要求：

开源软件版本归一要求见T/TAF 230-2024 5.3.1 h)，即：

应对设备使用的开源软件版本进行管理，确保设备使用的开源软件版本归一，不应在产品中使用同一开源软件的不同版本。

b) 预置条件：

1) 厂商提供所用的开源软件清单；
2) 厂商提供开源软件使用规范；
3) 厂商提供开源软件归一性的证明材料。

c) 检测方法：

审核厂商提供的开源软件归一性证据，验证设备实际使用的开源软件版本归一。

d) 预期结果：

开源软件归一性证据中显示，产品中使用的同一开源软件的版本一致。

e) 判定原则：

测试结果应与预期结果相符，否则不符合要求。

7.1.9 开源软件清单正确性

该检测项包含如下内容：

a) 安全要求：

开源软件清单正确性要求见T/TAF 230-2024 5.3.1 i)，即：

应维护设备所用开源软件清单，并确保设备实际所用开源软件及其版本与开源软件清单一致。

b) 预置条件：

1) 厂商提供所用的开源软件清单；
2) 厂商提供开源软件清单正确性管理相关说明文档；
3) 厂商提供开源软件清单正确性验证材料。

c) 检测方法：

1) 审核厂商提供的开源软件清单正确性管理相关说明文档，明确开源软件清单正确性管理措施；
2) 审核提供的证明开源软件清单正确性的材料，验证设备软件中实际使用的开源软件与开源软件清单的一致性。

d) 预期结果：

1) 相关文档中明确了应保证设备实际所用开源软件及其版本与开源软件清单一致；
2) 证明开源软件清单正确性的材料中显示，实际开源软件列表与厂商提供的开源软件清单具备一致性。

e) 判定原则：

测试结果应与预期结果相符，否则不符合要求。

7.1.10 开源软件生命周期管理

该检测项包含如下内容：

a) 安全要求：

开源软件生命周期管理要求见T/TAF 230-2024 5.3.1 j)，即：
应针对所用开源软件的生命周期制定管理机制，明确开源软件生命周期关键节点（如停止维护、停止服务等），并根据关键节点对开源软件进行维护（如升级、更换其他软件等）。

b) 预置条件：
厂商提供开源软件使用规范。

c) 检测方法：
查看厂商提供的材料，确认是否在产品开发过程中，实现开源软件生命周期管理。

d) 预期结果：
资料显示，在产品开发过程中，实现开源软件生命周期管理，对即将停止维护、停止服务的开源软件进行升级、更换等处理。

e) 判定原则：
测试结果应与预期结果相符，否则不符合要求。

7.1.11 开源软件漏洞管理机制

该检测项包含如下内容：

a) 安全要求：
开源软件漏洞管理机制要求见T/TAF 230-2024 5.3.1 k)，即：
应建立完善的开源软件漏洞管理机制，包括以下内容：
1) 应实现漏洞感知可追溯，将所有已发现漏洞进行记录并入库；
2) 应实现漏洞影响范围可追溯，可根据漏洞信息查询到受漏洞影响的产品；
3) 应实现漏洞修改发布过程可追溯，对技术方案修补、结果验证、公告发布等环节进行流程跟踪。

b) 预置条件：
厂商提供说明材料，说明开源软件漏洞修复管理机制。

c) 检测方法：
查看厂商提供的说明材料，确认是否建立漏洞管理规范，提供对开源软件漏洞的完善管理机制。

d) 预期结果：
厂家具备漏洞管理规范，提供对开源软件漏洞的完善管理机制，包括但不限于漏洞感知收录、漏洞评估分级规则、涉及产品版本排查流程、漏洞修复流程、厂商官网发布版本漏洞已修复清单等。

e) 判定原则：
测试结果应与预期结果相符，否则不符合要求。

7.1.12 安全编译选项

该检测项包含如下内容：

a) 安全要求：
安全编译选项要求见T/TAF 230-2024 5.3.1 l)，即：
设备所用软件编译时应开启安全编译选项，包括但不限于PIE、NX等。

b) 预置条件：
1) 测试终端正确安装checksec或类似安全测试工具，并获取设备软件包；
2) 由厂商提供解包工具或脚本。

c) 检测方法：

1) 使用厂商提供的解包工具或脚本对软件包解包；
2) 使用checksec或类似工具检查解包后文件的编译选项。

d) 预期结果：
1) 解包完成；
2) 查看checksec检查结果中每一行的文件，首先排除操作系统内核文件(如.ko结尾的文件)，然后在剩下的文件中检查每一列的检查结果是否符合以下内容，若符合则测试通过：
所有文件均为Full RELRO（开启GOT表只读保护）；
所有文件均为NX enabled（开启堆栈不可执行保护）；
所有文件均不是NO PIE（地址随机化开启）。
若使用其他工具，工具运行结果中显示PIE、NX等机制已开启。

e) 判定原则：
测试结果应与预期结果相符，否则不符合要求。

7.1.13 安全函数占比

该检测项包含如下内容：

a) 安全要求：
安全函数占比要求见T/TAF 230-2024 5.3.1 m)，即：
设备软件应在代码中使用安全的字符串操作函数，其中安全字符串操作函数所占比例不低于20%时满足T/TAF 230-2024二级要求，安全字符串操作函数所占比例不低于40%时满足T/TAF 230-2024三级要求。

b) 预置条件：
厂商提供软件包及解包工具。

c) 检测方法：
解析代码，统计代码中所有使用安全函数和不安全函数的调用次数，然后汇总后得到总的安全函数使用率数据。

注：安全字符串操作函数范围见ISO/IEC 9899:2018标准的K3.7章节，包括memcpy_s、memmove_s、strcpy_s、strncpy_s、strcat_s、strncat_s、strtok_s、memset_s、strerror_s、strerrorlen_s、strnlen_s；对应的非安全字符串操作函数为memcpy、memmove、strcpy、strncpy、strcat、strncat、strtok、memset、strerror、strerrorlen、strnlen。

d) 预期结果：
被测试对象的总体安全函数使用率【安全函数/（非安全函数+安全函数）】高于20%（二级）或40%（三级）。

e) 判定原则：
测试结果应与预期结果相符，否则不符合要求。

7.1.14 设备证书一机一证

该检测项包含如下内容：

a) 安全要求：
设备证书一机一证要求见T/TAF 230-2024 5.3.1 n)，即：
应保证设备证书一机一证。

b) 预置条件：
1) 设备可正常管理；
2) 设备提供基于证书的身份认证。

c) 检测方法：
检查设备数字证书申请功能，是否支持与设备绑定。
d) 预期结果：
设备证书申请或签发过程可保证设备证书与当前设备一一绑定（例如，可通过在证书中携带当前设备唯一性标识达到与当前设备绑定），满足一机一证要求。
e) 判定原则：
测试结果应与预期结果相符，否则不符合要求。

7.1.15 开源软件漏洞管理 IT 化

该检测项包含如下内容：
a) 安全要求：
开源软件漏洞管理IT化要求见T/TAF 230-2024 5.3.1 o)，即：
应实现开源软件漏洞修复过程的信息化管理（使用IT系统），包含开源软件漏洞感知、影响分析和修复记录等内容的管理。
b) 预置条件：
厂商提供设备软件包含的开源软件漏洞IT管理机制证明材料。
c) 检测方法：
查看厂商是否具备IT化的开源软件漏洞管理系统，是否包括漏洞感知、影响分析、修复记录等内容。
d) 预期结果：
厂商具备IT化的开源软件漏洞管理系统，功能包括收集录入漏洞、触发各产品开展漏洞影响评估和分级、归档评估记录、IT化跟踪漏洞修复记录、官网发布漏洞已修复清单等。
e) 判定原则：
测试结果应与预期结果相符，否则不符合要求

7.2 生产和交付

7.2.1 安全加固指导

该检测项包含如下内容：
a) 安全要求：
安全加固指导要求见T/TAF 230-2024 5.3.2 a)，即：
应为用户提供安全配置加固指导文档，列出设备安全风险项及对应的手工加固指导。
b) 预置条件：
无。
c) 检测方法：
1) 查看厂商是否提供安全配置加固指导文档；
2) 查看安全配置加固指导文档中是否列出设备安全风险项及对应的手工加固指导。
d) 预期结果：
1) 厂商提供了安全配置加固指导文档，或在其他文档中包含了安全配置加固指导相关内容；
2) 文档中列出了设备安全风险项及对应的手工加固指导。
e) 判定原则：
测试结果应与预期结果相符，否则不符合要求。

7.2.2 端口使用说明

该检测项包含如下内容：

a) 安全要求：

端口使用说明要求见T/TAF 230-2024 5.3.2 b)，即：

应提供设备开放端口使用说明，并提供设备服务与设备默认端口的映射关系说明。

b) 预置条件：

厂商提供端口使用说明。

c) 检测方法：

1) 查看厂商提供的端口使用说明中是否包含设备所有开放端口的使用说明；

2) 查看厂商提供的说明材料，确认是否明确描述默认开放的端口信息及对应服务的映射关系。

d) 预期结果：

1) 说明材料中包含所有开放端口的使用说明；

2) 厂商提供的说明材料中明确描述了默认开放的端口信息及对应服务的映射关系。

e) 判定原则：

测试结果应与预期结果相符，否则不符合要求。

7.2.3 漏洞修复和补救

该检测项包含如下内容：

a) 安全要求：

漏洞修复和补救要求见T/TAF 230-2024 5.3.2 c)，即：

交付设备前，应对设备进行漏洞扫描，发现设备存在已知漏洞应当立即采取补救措施。

b) 预置条件：

厂商提供漏洞扫描及处理的相关资料。

c) 检测方法：

1) 检查厂商提供的设备交付前相关流程的说明材料，查看是否包含漏洞扫描及补救措施相关内容；

2) 检查厂商提供的漏洞扫描报告及补救措施和验证材料，查看扫描出的漏洞是否都已进行合理处置。

d) 预期结果：

1) 厂商提供的说明材料中包含漏洞扫描及补救措施相关内容；

2) 厂商提供的漏洞扫描报告中的漏洞均已被合理处置。

e) 判定原则：

测试结果应与预期结果相符，否则不符合要求。

7.2.4 恶意程序防范

该检测项包含如下内容：

a) 安全要求：

恶意程序防范要求见T/TAF 230-2024 5.3.2 d)，即：

应在交付前对设备软件包进行病毒扫描，确保其中不存在病毒等恶意代码。

b) 预置条件：

厂商提供病毒扫描的相关资料。

c) 检测方法：

1) 检查厂商提供的设备交付前相关流程的说明材料，查看是否包含病毒扫描相关内容；

2） 检查厂商提供的病毒扫描报告，查看是否存在病毒等恶意代码。

d） 预期结果：

1） 厂商提供的说明材料中包含病毒扫描相关内容；

2） 厂商提供的病毒扫描报告结果中显示不存在病毒等恶意代码，扫描所用杀毒软件为业界主流杀毒软件。

e） 判定原则：

测试结果应与预期结果相符，否则不符合要求。

7.3 运行和维护

7.3.1 漏洞公告及反馈途径

该检测项包含如下内容：

a） 安全要求：

漏洞公告及反馈途径要求见T/TAF 230-2024 5.3.3 a)，即：

应向用户提供漏洞反馈渠道、漏洞处理流程和设备漏洞安全公告查看途径。

b） 预置条件：

无。

c） 检测方法：

查看厂商是否向用户提供漏洞反馈渠道，是否提供漏洞处理流程说明和漏洞安全公告查看途径。

d） 预期结果：

厂商向用户提供漏洞反馈渠道，并提供漏洞处理流程说明和漏洞安全公告查看途径（例如网站公告）。

e） 判定原则：

测试结果应与预期结果相符，否则不符合要求。

7.3.2 安全维护要求

该检测项包含如下内容：

a） 安全要求：

安全维护要求见T/TAF 230-2024 5.3.3 b)，即：

应在约定的期限内，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。

b） 预置条件：

厂商提供说明材料，说明与客户约定的安全维护要求。

c） 检测方法：

检查厂商提供的说明材料，确认是否包括在约定的期限内为设备提供持续的安全维护的说明，是否说明不以业务变更、产权变更等原因单方面中断或终止安全维护。

d） 预期结果：

说明材料中明确包含在约定的期限内为设备提供持续的安全维护，且不以业务变更、产权变更等原因单方面中断或终止安全维护等内容。

e） 判定原则：

测试结果应与预期结果相符，否则不符合要求。

7.3.3 生命周期终止

该检测项包含如下内容：

a) 安全要求：
生命周期终止要求见T/TAF 230-2024 5.3.3 c)，即：
应向用户告知设备生命周期终止时间。

b) 预置条件：
厂商提供说明材料，说明向用户告知设备生命周期终止时间。

c) 检测方法：
检查厂商提供的说明材料，确认是否明确要求设备应通过合适的方式（例如：网站公告等）向用户提前告知设备生命周期终止时间。

d) 预期结果：
说明材料中明确了厂商通过合适的方式（例如：网站公告等）向用户提前告知设备生命周期终止时间。

e) 判定原则：
测试结果应与预期结果相符，否则不符合要求。

参 考 文 献

[1] T/TAF 088-2023 网络关键设备安全通用检测方法
[2] NIST SP 800-57 Part 1 Rev.5 Recommendation for Key Management: Part 1 - General

电信终端产业协会团体标准

光传送网设备安全测试方法

T/TAF 248—2024

*

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