ICS 35.240
A.90

GA

中华人民共和国公共安全行业标准

GA/T XXXX—XXXX

信息安全技术 网络设备信息探测产品安全技术要求

Information security technology Security technical requirements for network equipment information detection products

（报批稿）

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

中华人民共和国公安部　发布

目　次

前　言

本标准按照GB/T 1.1—2009给出的规则起草。

本标准由公安部网络安全保卫局提出。

本标准由公安部信息系统安全标准化技术委员会归口。

本标准起草单位：公安部计算机信息系统安全产品质量监督检验中心（公安部第三研究所）、公安部网络安全保卫局。

本标准主要起草人：胡维娜、俞优、赵戈、王志佳、张艳、邹春明、陆臻、顾健。

信息安全技术 网络设备信息探测产品安全技术要求

1 范围

本标准规定了网络设备信息探测产品的安全功能要求、安全保障要求及等级划分要求。

本标准适用于网络设备信息探测产品的设计、开发及测试。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 18336.3-2015 信息技术 安全技术 信息技术安全评估准则 第3部分：安全保障组件

GB/T 25069-2010 信息安全技术 术语

3 术语和定义

GB/T 18336.3-2015和GB/T 25069-2010界定的以及下列术语和定义适用于本文件。

3.1

网络设备信息 network equipment information

目标网络环境内在线主机、网络设备和安全设备的端口、服务类型和版本等信息。

3.2

网络设备信息探测产品 network equipment information detection product

通过局域网连接到目标信息系统，然后对目标网络环境内的在线主机、网络设备和安全设备信息进行探测的产品。

4 网络设备信息探测产品描述

网络设备信息探测产品保护的对象是目标信息系统。该产品通常以旁路方式部署在目标网络中，通过在线采集方式收集分析在线主机、网络设备和安全设备的信息。

图1是网络设备信息探测产品的一个典型运行环境。

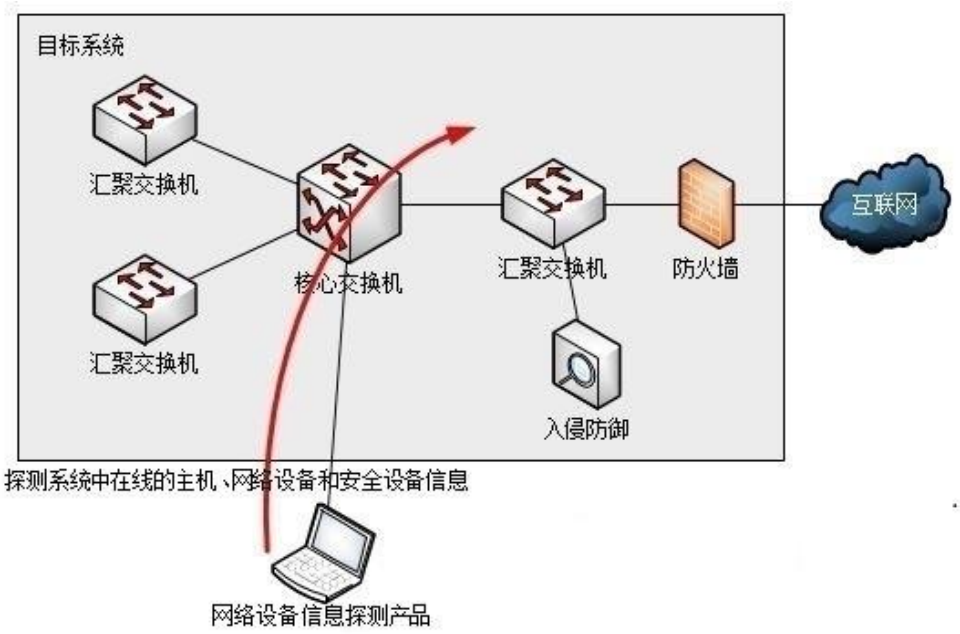

图1 网络设备信息探测产品典型运行环境

5 总体说明

5.1 安全技术要求分类

本标准将网络设备信息探测产品安全技术要求分为安全功能和安全保障要求两大类。其中，安全功能要求是对网络设备信息探测产品应具备的安全功能提出具体要求，包括信息探测、网络拓扑生成、非授权连接行为检查等；安全保障要求针对网络设备信息探测产品的开发和使用文档的内容提出具体的要求，例如开发、指导性文档、生命周期支持和测试等。

5.2 安全等级划分

网络设备信息探测产品的安全等级按照其安全功能要求和安全保障要求的强度划分为基本级和增强级，其中安全保障要求参考了GB/T 18336.3—2015。

6 安全功能要求

6.1 信息探测

6.1.1 设备探测

应采取以下方式探测指定IP范围内在线的主机、网络设备和安全设备：

a) 快速扫描，如采用 ICMP 方式；

b) 深度扫描，如采用 SNMP、telnet、SSH、CDP 等方式。

6.1.2 端口探测

应能够探测指定IP范围内的在线主机、网络设备和安全设备上的端口状态，并支持自定义探测的端口范围和探测方式。

6.1.3 设备基本信息探测

应能够获取主机的操作系统信息，以及网络设备和安全设备的系统版本、设备类型和品牌信息。

6.1.4 服务类型和版本探测

应能够探测端口的服务类型和版本。

6.2 网络拓扑生成

应能够根据探测到的信息，生成针对指定网络的拓扑图。

6.3 非授权连接行为检查

应能对非授权设备连到目标信息系统所在网络的行为进行检查，并在非授权连接行为发生时触发告警。

6.4 对目标系统所在网络环境的影响

在使用过程中应最小化占用检查目标系统的资源或所属网络的网络资源，防止影响检查目标系统业务和网络的正常运行，平均带宽占用量小于3MB/s。

6.5 探测任务管理

应提供探测任务管理功能，能够对探测任务进行暂停、停止、删除、重新开始的操作。

6.6 统计报表

应能够将探测到的信息生成报表。

6.7 IPv6 协议支持

应能够支持IPv6类型网络环境探测。

6.8 标识与鉴别

6.8.1 用户标识

应保证任何用户都具备全局唯一的标识。

6.8.2 身份鉴别

应保证任何用户在执行产品的安全功能之前都要进行身份鉴别。若产品采用网络远程方式管理，还应对管理IP地址进行限制。

6.8.3 鉴别失败处理

应提供鉴别失败处理功能，当用户连续鉴别失败达到预定义的次数时阻止用户进一步的鉴别请求。

6.8.4 超时锁定或注销

应提供用户登录超时锁定或注销功能，当用户超过预定义的时间仍没有任何操作时终止该用户当前的管理会话，需要再次进行身份鉴别才能重新进行管理操作。

6.8.5 鉴别数据保护

应保证鉴别数据以非明文形式存储，不被未授权查阅或修改。

6.9 数据安全

6.9.1 数据传输安全

若采用远程方式管理，应保证远程管理数据非明文传输；若由多个组件组成，应保证控制命令、传输数据等信息在组件间保密传输。

6.9.2 数据存储安全

应将探测到的信息存储于掉电非易失性存储介质中。

6.10 审计日志

6.10.1 日志生成

应能够对以下事件生成日志：

a) 用户鉴别，包括成功和失败；
b) 用户重要操作。

日志内容应包含：日期、时间、事件主体、事件描述等。

6.10.2 日志管理

应满足以下要求：

a) 只允许授权用户访问日志；
b) 提供按照日期、时间、事件主体等条件查询日志的功能；
c) 提供日志的存档、清空功能。

7 安全保障要求

7.1 开发

7.1.1 安全架构

开发者应提供产品安全功能的安全架构描述，安全架构描述应满足以下要求：

a) 与产品设计文档中对安全功能实施抽象描述的级别一致；
b) 描述与安全功能要求一致的产品安全功能的安全域；
c) 描述产品安全功能初始化过程为何是安全的；
d) 证实产品安全功能能够防止被破坏；
e) 证实产品安全功能能够防止安全特性被旁路。

7.1.2 功能规范

开发者应提供完备的功能规范说明，功能规范说明应满足以下要求：

a) 完全描述产品的安全功能；
b) 描述所有安全功能接口的目的与使用方法；
c) 标识和描述每个安全功能接口相关的所有参数；
d) 描述安全功能接口相关的安全功能实施行为；
e) 描述由安全功能实施行为处理而引起的直接错误消息；

f） 证实安全功能要求到安全功能接口的追溯；
g） 描述安全功能实施过程中，与安全功能接口相关的所有行为；
h） 描述可能由安全功能接口的调用而引起的所有直接错误消息。

7.1.3 实现表示

开发者应提供全部安全功能的实现表示，实现表示应满足以下要求：
a） 提供产品设计描述与实现表示实例之间的映射，并证明其一致性；
b） 按详细级别定义产品安全功能，详细程度达到无须进一步设计就能生成安全功能的程度；
c） 以开发人员使用的形式提供。

7.1.4 产品设计

开发者应提供产品设计文档，产品设计文档应满足以下要求：
a） 根据子系统描述产品结构；
b） 标识和描述产品安全功能的所有子系统；
c） 描述安全功能所有子系统间的相互作用；
d） 提供的映射关系能够证实设计中描述的所有行为能够映射到调用它的安全功能接口；
e） 根据模块描述安全功能；
f） 提供安全功能子系统到模块间的映射关系；
g） 描述所有安全功能实现模块，包括其目的及与其他模块间的相互作用；
h） 描述所有实现模块的安全功能要求相关接口、其他接口的返回值、与其他模块间的相互作用及调用的接口；
i） 描述所有安全功能的支撑或相关模块，包括其目的及与其他模块间的相互作用。

7.2 指导性文档

7.2.1 操作用户指南

开发者应提供明确和合理的操作用户指南，操作用户指南与为评估而提供的其他所有文档保持一致，对每一种用户角色的描述应满足以下要求：
a） 描述在安全处理环境中被控制的用户可访问的功能和特权，包含适当的警示信息；
b） 描述如何以安全的方式使用产品提供的可用接口；
c） 描述可用功能和接口，尤其是受用户控制的所有安全参数，适当时指明安全值；
d） 明确说明与需要执行的用户可访问功能有关的每一种安全相关事件，包括改变安全功能所控制实体的安全特性；
e） 标识产品运行的所有可能状态（包括操作导致的失败或者操作性错误），以及它们与维持安全运行之间的因果关系和联系；
f） 充分实现安全目的所执行的安全策略。

7.2.2 准备程序

开发者应提供产品及其准备程序，准备程序描述应满足以下要求：
g） 描述与开发者交付程序相一致的安全接收所交付产品必需的所有步骤；
h） 描述安全安装产品及其运行环境必需的所有步骤。

7.3 生命周期支持

7.3.1 配置管理能力

开发者的配置管理能力应满足以下要求：

a) 为产品的不同版本提供唯一的标识；
b) 使用配置管理系统对组成产品的所有配置项进行维护，并唯一标识配置项；
c) 提供配置管理文档，配置管理文档描述用于唯一标识配置项的方法；
d) 配置管理系统提供一种自动方式来支持产品的生成，通过该方式确保只能对产品的实现表示进行已授权的改变；
e) 配置管理文档包括一个配置管理计划，配置管理计划描述如何使用配置管理系统开发产品。实施的配置管理与配置管理计划相一致；
f) 配置管理计划描述用来接受修改过的或新建的作为产品组成部分的配置项的程序。

7.3.2 配置管理范围

开发者应提供产品配置项列表，并说明配置项的开发者。配置项列表应包含以下内容：

a) 产品、安全保障要求的评估证据和产品的组成部分；
b) 实现表示、安全缺陷报告及其解决状态。

7.3.3 交付程序

开发者应使用一定的交付程序交付产品，并将交付过程文档化。在给用户方交付产品的各版本时，交付文档应描述为维护安全所必需的所有程序。

7.3.4 开发安全

开发者应提供开发安全文档。开发安全文档应描述在产品的开发环境中，为保护产品设计和实现的保密性和完整性所必需的所有物理的、程序的、人员的和其他方面的安全措施。

7.3.5 生命周期定义

开发者应建立一个生命周期模型对产品的开发和维护进行的必要控制，并提供生命周期定义文档描述用于开发和维护产品的模型。

7.3.6 工具和技术

开发者应明确定义用于开发产品的工具，并提供开发工具文档无歧义地定义实现中每个语句的含义和所有依赖于实现的选项的含义。

7.4 测试

7.4.1 测试覆盖

开发者应提供测试覆盖文档，测试覆盖描述应满足以下要求：

a) 表明测试文档中所标识的测试与功能规范中所描述的产品的安全功能间的对应性；
b) 表明上述对应性是完备的，并证实功能规范中的所有安全功能接口都进行了测试。

7.4.2 测试深度

开发者应提供测试深度的分析。测试深度分析描述应满足以下要求：

a) 证实测试文档中的测试与产品设计中的安全功能子系统和实现模块之间的一致性；
b) 证实产品设计中的所有安全功能子系统、实现模块都已经进行过测试。

7.4.3 功能测试

开发者应测试产品安全功能，将结果文档化并提供测试文档。测试文档应包括以下内容：

a) 测试计划，标识要执行的测试，并描述执行每个测试的方案，这些方案包括对于其他测试结果的任何顺序依赖性；
b) 预期的测试结果，表明测试成功后的预期输出；
c) 实际测试结果和预期的一致性。

7.4.4 独立测试

开发者应提供一组与其自测安全功能时使用的同等资源，以用于安全功能的抽样测试。

7.5 脆弱性评定

基于已标识的潜在脆弱性，产品能够抵抗以下攻击行为：

a) 具有基本攻击潜力的攻击者的攻击；
b) 具有增强型基本攻击潜力的攻击者的攻击。

8 不同安全等级的要求

8.1 安全功能要求

不同安全等级的网络设备信息探测产品的安全功能要求如表1所示。

表1 不同安全等级的网络设备信息探测产品的安全功能要求

安全功能要求		基本级	增强级
信息探测	设备探测	6.1.1	6.1.1
	端口探测	6.1.2	6.1.2
	设备基本信息探测	6.1.3	6.1.3
	服务类型和版本探测	6.1.4	6.1.4
网络拓扑生成		——	6.2
非授权连接行为检查		——	6.3
对目标系统所在网络环境的影响		6.4	6.4
探测任务管理		6.5	6.5
统计报表		——	6.6
IPv6 协议支持		6.7	6.7

表1（续）

安全功能要求		基本级	增强级
标识与鉴别	用户标识	6.8.1	6.8.1
	身份鉴别	6.8.2	6.8.2
	鉴别失败处理	——	6.8.3
	超时锁定或注销	——	6.8.4
	鉴别数据保护	6.8.5	6.8.5
数据安全	数据传输安全	6.9.1	6.9.1
	数据存储安全	6.9.2	6.9.2
审计日志	日志生成	6.10.1	6.10.1
	日志管理	——	6.10.2

8.2 安全保障要求

不同安全等级的网络设备信息探测产品的安全保障要求如表2所示。

表2 不同安全等级的网络设备信息探测产品的安全保障要求

安全保障要求		基本级	增强级
开发	安全架构	7.1.1	7.1.1
	功能规范	7.1.2 a) ～f)	7.1.2
	实现表示	——	7.1.3
	产品设计	7.1.4 a)～d)	7.1.4
指导性文档	操作用户指南	7.2.1	7.2.1
	准备程序	7.2.2	7.2.2
生命周期支持	配置管理能力	7.3.1 a)～c)	7.3.1
	配置管理范围	7.3.2 a)	7.3.2
	交付程序	7.3.3	7.3.3
	开发安全	——	7.3.4
	生命周期定义	——	7.3.5
	工具和技术	——	7.3.6
测试	测试覆盖	7.4.1 a)	7.4.1
	测试深度	——	7.4.2
	功能测试	7.4.3	7.4.3
	独立测试	7.4.4	7.4.4
脆弱性评定		7.5 a)	7.5 b)