



中华人民共和国公共安全行业标准

GA/T 1543—2019

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

2019-01-13 发布

2019-01-13 实施

中华人民共和国公安部 发布

目 次

前言	III
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 网络设备信息探测产品描述	1
5 总体说明	2
5.1 安全技术要求分类	2
5.2 安全等级划分	2
6 安全功能要求	2
6.1 信息探测	2
6.2 网络拓扑生成	3
6.3 非授权连接行为检查	3
6.4 对目标系统所在网络环境的影响	3
6.5 探测任务管理	3
6.6 统计报表	3
6.7 IPv6 协议支持	3
6.8 标识与鉴别	3
6.9 数据安全	4
6.10 审计日志	4
7 安全保障要求	4
7.1 开发	4
7.2 指导性文档	5
7.3 生命周期支持	6
7.4 测试	6
7.5 脆弱性评定	7
8 不同安全等级的要求	7
8.1 安全功能要求	7
8.2 安全保障要求	8

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對象是目标信息系统。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。