ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T 28451—2023
代替 GB/T 28451—2012

信息安全技术
网络入侵防御产品技术规范

Information security technology—
Technical specification for network intrusion prevention system

2023-05-23 发布　　2023-12-01 实施

国家市场监督管理总局
国家标准化管理委员会　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　缩略语 …… 2
5　概述 …… 2
6　安全技术要求 …… 3
6.1　安全功能要求 …… 3
6.2　自身安全要求 …… 5
6.3　性能要求 …… 6
6.4　环境适应性要求 …… 7
6.5　安全保障要求 …… 8
7　测评方法 …… 10
7.1　测评环境 …… 10
7.2　测评工具 …… 11
7.3　安全功能测评 …… 11
7.4　自身安全测评 …… 19
7.5　性能测评 …… 22
7.6　环境适应性测评 …… 24
7.7　安全保障评估 …… 25
8　等级划分要求 …… 31
附录 A（规范性）　网络入侵防御产品等级划分 …… 32
A.1　概述 …… 32
A.2　安全技术要求等级划分 …… 32
A.3　测评方法等级划分 …… 34

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。

本文件代替GB/T 28451—2012《信息安全技术　网络型入侵防御产品技术要求和测试评价方法》，与GB/T 28451—2012相比，除结构调整和编辑性改动外，主要技术变化如下：

a) 增加了“流量控制”要求（见6.1.1.5）；
b) 增加了“攻击数据留存”要求（见6.1.3.5）；
c) 增加了“配置备份恢复”要求（见6.1.4.6）；
d) 增加了“日志外发”要求（见6.1.4.12）；
e) 增加了“网络层吞吐量”“混合应用层吞吐量”“TCP新建连接速率”“TCP并发连接数”等性能要求的具体内容（见6.3.1，6.3.2，6.3.3和6.3.4）；
f) 增加了产品误拦截率和漏拦截率的具体要求（见6.3.5、6.3.6，2012年版的7.4）；
g) 增加了“环境适应性要求”章节的内容，其中主要是明确了产品对IPv6的支持能力，包括IPv6应用环境适应性、IPv6管理环境适应性、双协议栈，以及虚拟化支持能力（见6.4）；
h) 删除了“负载均衡”要求（见2012年版的7.3.1.4.9）；
i) 将“入侵防御产品技术要求”更改为“安全功能要求”，“产品自身安全要求”更改为“自身安全要求”，“产品保证要求”更改为“安全保障要求”（见第6章，2012年版的7和8）；
j) 更改了入侵防御产品的等级划分，由“一级、二级和三级”修改为“基本级和增强级”（见附录A，2012年版的7.1、7.2和7.3）。

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。

本文件由全国信息安全标准化技术委员会（SAC/TC 260）提出并归口。

本文件起草单位：公安部第三研究所、西安交大捷普网络科技有限公司、北京神州绿盟科技有限公司、深信服科技股份有限公司、启明星辰信息技术集团股份有限公司、蓝盾信息安全技术股份有限公司、北京天融信网络安全技术有限公司、中国网络安全审查技术与认证中心、上海市信息安全测评认证中心、中国电力科学研究院有限公司、新华三技术有限公司、奇安信网神信息技术（北京）股份有限公司。

本文件主要起草人：顾建新、武腾、邓雨、赖静、章倩、李谦、何建锋、陈宏伟、叶建伟、叶润国、王庆会、杨辰钟、雷晓峰、申永波、徐佟海、方帅、万晓兰、周飞虎。

本文件及其所代替文件的历次版本发布情况为：

——2012年首次发布为GB/T 28451—2012；
——本次为第一次修订。

信息安全技术
网络入侵防御产品技术规范

1 范围

本文件规定了网络入侵防御产品的安全技术要求和测评方法，并进行了等级划分。

本文件适用于网络入侵防御产品的设计、开发、测试和评价。

2 规范性引用文件

下列文件中的内容通过文中的规范化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 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 信息安全技术 术语

GB/T 30279—2020 信息安全技术 网络安全漏洞分类分级指南

3 术语和定义

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

3.1

网络入侵防御产品 network intrusion prevention system

以网桥或网关形式部署在网络通路上，通过分析网络流量发现具有入侵特征的网络行为，在其传入被保护网络前进行拦截的产品。

3.2

报文碎片 message fragmentation

攻击者将攻击数据隐藏在经过分段或者分片的 TCP 报文或者 IP 报文中发出，用于躲避检测的行为。

3.3

代码变形 code deformation

攻击者重写已知攻击数据、代码，或者用其他代码替代原有攻击数据中的部分内容，用于躲避检测的行为。

3.4

管理员 administrator

具备管理、配置、操作网络入侵防御产品以及查看审计记录等权限的人员。

3.5

告警 alert

当网络入侵防御产品发现有入侵行为时，通过一定的技术手段主动向管理员发出的警示类通知。