



中华人民共和国国家标准

GB/T 20275—2021

代替 GB/T 20275—2013

信息安全技术 网络入侵检测系统 技术要求 and 测试评价方法

Information security technology—
Technical requirements and testing and evaluation approaches for
network-based intrusion detection system

2021-10-11 发布

2022-05-01 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	I
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 网络入侵检测系统	2
6 安全技术要求	2
6.1 要求分类与分级	2
6.2 基本级安全要求	5
6.3 增强级安全要求	12
7 测试评价方法	22
7.1 测试环境	22
7.2 测试工具	23
7.3 基本级	23
7.4 增强级	42
参考文献	71

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 20275—2013《信息安全技术 网络入侵检测系统技术要求和测试评价方法》，与 GB/T 20275—2013 相比，除结构调整和编辑性改动外，主要技术变化如下：

- a) 修改了“安全事件”的定义(见 3.1,2013 年版的 3.2)；
- b) 修改了“告警”的定义(见 3.2,2013 年版的 3.7)；
- c) 增加了“网络入侵检测系统描述”章节的内容(见第 5 章)；
- d) 调整了网络入侵检测系统的分级(见 6.1.2,2013 年版的 5.2)；
- e) 修改了“攻击行为监测”的要求(见 6.2.1.1.3 和 6.3.1.1.3,2013 年版的 6.1.1.1.3、6.2.1.1.3 和 6.3.1.1.3)；
- f) 增加了时钟同步的要求(见 6.2.1.4.9 和 6.3.1.4.9)；
- g) 增加了鉴别信息的要求(见 6.2.2.1.2 和 6.3.2.1.2)；
- h) 增加了管理地址限制的要求(见 6.2.2.1.6 和 6.3.2.1.6)；
- i) 增加了数据外发的要求(见 6.2.2.4.3 和 6.3.2.4.3)；
- j) 增加对“环境适应性要求”章节的内容,其中主要是明确了网络入侵检测系统对 IPv6 的支持能力,包括支持纯 IPv6 网络环境、IPv6 网络环境下自身管理能力和双协议栈(见 6.2.3 和 6.3.3)；
- k) 删除了“双机热备”的要求(见 2013 年版的 6.3.1.4.11)；
- l) 删除了“控制台鉴别”的要求(见 2013 年版的 6.3.2.1.5)；
- m) 增加了安全策略备份的要求(见 6.3.2.4.4)；
- n) 修改了各级的“安全保证要求”为“安全保障要求”(见 6.2.4 和 6.3.4,2013 年版的 6.1.3、6.2.3 和 6.3.3)。

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、北京天融信网络安全技术有限公司、奇安信科技集团股份有限公司、北京神州绿盟科技有限公司、启明星辰信息技术集团股份有限公司、上海国际技贸联合有限公司、网神信息技术(北京)股份有限公司、中国网络安全审查技术与认证中心、中国电子科技集团公司第十五研究所(信息产业信息安全测评中心)、上海市信息安全测评认证中心、北京山石网科信息技术有限公司、西安交大捷普网络科技有限公司、新华三技术有限公司、北京安博通科技股份有限公司、北京中科院网威信息技术有限公司、深信服科技股份有限公司、深圳市腾讯计算机系统有限公司、中国信息通信研究院、工业和信息化部计算机与微电子发展研究中心(中国软件评测中心)、华信咨询设计研究院有限公司、中国科学院信息工程研究所、中国电力科学研究院有限公司信息通信研究所、陕西省网络与信息安全测评中心、上海工业控制安全创新科技有限公司、国网新疆电力有限公司电力科学研究院。

本文件主要起草人：宋好好、顾建新、沈亮、陆臻、顾健、赖静、陈妍、曹宁、陈华平、刘彤、焦玉峰、刘志远、魏向杰、付海涛、申永波、刘健、刘艺翔、徐佟海、李宇、何建锋、杨洪起、曾祥禄、宋伟、杨柳、黄超、许子先、王榕、郭永振、孙小平、闫兆腾、严敏辉、赵少飞、倪华、李峰、舒斐、王少杰、张凯悦、顾欣、任帅、肖颖。

本文件及其所代替文件的历次版本发布情况为：

- 2006 年首次发布为 GB/T 20275—2006,2013 年第一次修订；
- 本次为第二次修订。

信息安全技术 网络入侵检测系统 技术要求和测试评价方法

1 范围

本文件规定了网络入侵检测系统的安全技术要求和测试评价方法。
本文件适用于网络入侵检测系统的设计、开发与测评。

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 信息安全技术 术语

3 术语和定义

GB/T 25069 界定的以及下列术语和定义适用于本文件。

3.1

安全事件 security incident

对网络和信息系统的或者其中的数据造成危害的事件。

3.2

告警 alert

当攻击或入侵发生时,网络入侵检测系统向授权管理员发出的信息。

3.3

支撑系统 supporting system

支撑网络入侵检测系统运行的操作系统。

4 缩略语

下列缩略语适用于本文件。

FTP:文件传输协议(File Transfer Protocol)

HTML:超文本置标语言(Hyper Text Markup Language)

HTTP:超文本传输协议(Hyper Text Transfer Protocol)

ICMP:网际控制报文协议(Internet Control Message Protocol)

IP:网际协议(Internet Protocol)

POP3:邮局协议的第三个版本(Post Office Protocol 3)

SMTP:简单邮件传送协议(Simple Mail Transfer Protocol)

SNMP:简单网络管理协议(Simple Network Management Protocol)