



中华人民共和国国家标准

GB/T 20275—2013
代替 GB/T 20275—2006

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

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

2013-12-31 发布

2014-07-15 实施

中华人民共和国国家质量监督检验检疫总局
中国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 网络入侵检测系统等级划分	2
5.1 等级划分	2
5.2 等级划分表	3
6 网络入侵检测系统技术要求	6
6.1 第一级	6
6.2 第二级	11
6.3 第三级	19
7 网络入侵检测系统测评方法	28
7.1 测试环境	28
7.2 测试工具	29
7.3 第一级	29
7.4 第二级	42
7.5 第三级	61
参考文献	85

前 言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准代替 GB/T 20275—2006《信息安全技术 入侵检测系统技术要求和测试评价方法》。

本标准与 GB/T 20275—2006 的主要差异如下：

- 标准名称修改为《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》；
- 删除了 GB/T 20275—2006 中对主机入侵检测系统的技术要求和测试评价方法；
- 删除了 GB/T 20275—2006 中的“分析方式”(见 2006 版的 6.1.1.2.2)；
- 删除了 GB/T 20275—2006 中的“窗口定义”(见 2006 版的 6.2.1.4.1)；
- 增加了“最大监控流量”“最大监控并发连接数”“最大监控新建 TCP 连接速率”的性能要求；
- 增加了“硬件失效处理”“双机热备”的安全功能要求和测试评价方法；
- 增加了“控制台鉴别”“标识唯一性”的自身安全功能要求和测试评价方法；
- 调整了 GB/T 20275—2006 中“阻断能力”“系统升级”“报告定制”和“定制响应”的级别。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本文件某些内容可能涉及专利,本文件的发布机构不承担识别这些专利的责任。

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、北京启明星辰信息安全技术有限公司、公安部网络安全保卫局。

本标准主要起草人:宋好好、顾健、张笑笑、李毅、吴其聪、张艳。

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

本标准规定了网络入侵检测系统的技术要求和测试评价方法,要求包括安全功能要求、自身安全功能要求、安全保证要求和测试评价方法,并提出了网络入侵检测系统的分级要求。

本标准适用于网络入侵检测系统的设计、开发、测试和评价。

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 18336.1—2008 信息技术 安全技术 信息技术安全性评估准则 第1部分:简介和一般模型

GB/T 25069—2010 信息安全技术 术语

3 术语和定义

GB/T 18336.1—2008 和 GB/T 25069—2010 中界定的以及下列术语和定义适用于本文件。

3.1

事件 event

一种系统、服务或网络状态的发生或者改变的记录信息,可作为分析安全事件的基础。

3.2

安全事件 incident

通过对事件的分析处理,从而识别出一种系统、服务或网络状态的发生,表明一次可能的违反安全规则或某些防护措施失效,或者一种可能与安全相关但以前不为人知的一种情况,极有可能危害业务运行和威胁信息安全。

3.3

入侵 intrusion

任何危害或可能危害资源完整性、保密性或可用性的行为。

3.4

入侵检测 intrusion detection

通过对计算机网络或计算机系统若干关键点收集信息并对其进行分析,从中发现网络或系统中是否有违反安全策略的行为和被攻击的迹象。

3.5

网络入侵检测系统 network-based intrusion detection system

以网络上的数据包作为数据源,监听所保护网络内的所有数据包并进行分析,从而发现异常行为的入侵检测系统。