ICS 33.040.40;33.200
M 54

中华人民共和国国家标准

GB/T 26269—2010

网络入侵检测系统技术要求

Technical requirements for network intrusion detection system

2011-01-14 发布　　2011-06-01 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

本标准是网络入侵检测系统系列标准之一。该系列标准的名称如下：

——网络入侵检测系统技术要求；

——网络入侵检测系统测试方法。

本标准的附录A为资料性附录。

本标准由中华人民共和国工业和信息化部提出。

本标准由中国通信标准化协会归口。

本标准起草单位：工业和信息化部电信研究院、北京启明星辰信息技术有限公司、北京电信规划设计院有限公司、华为技术有限公司。

本标准起草人：落红卫、楚建梅、吴海民、陈萍、苗福友、刘册、夏俊杰。

引　言

网络入侵检测系统是指从IP网络的若干关键点收集信息并对其进行分析，从中发现网络中是否有违反安全策略的行为或遭到入侵的迹象，并依据既定的策略采取一定措施的系统。

网络入侵检测技术是网络动态安全的核心技术，相关设备和系统是整个安全防护体系的重要组成部分。目前，防火墙是静态安全防御技术，但对网络环境下日新月异的攻击手段缺乏主动的监测和响应。而网络入侵检测系统能对网络入侵事件和过程做出实时响应，和防火墙并列为网络与信息安全的核心设备。

网络入侵检测系统技术要求

1 范围

本标准规定了网络入侵检测系统的系统结构、检测内容、响应方式、系统管理、日志审计、自身安全、性能指标和物理安全。

本标准适用于网络入侵检测系统及相关设备。

2 规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件，其随后所有的修改单(不包括勘误的内容)或修订版均不适用于本标准，然而，鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本标准。

GB 4943—2001 信息技术设备的安全

GB 9254—2008 信息技术设备的无线电骚扰限值和测量方法

GB/T 17618—1998 信息技术设备抗扰限值和测量方法

3 术语和定义

下列术语和定义适用于本标准。

3.1

报警 alert

报警是指网络入侵检测系统在检测到入侵行为时，发布给具有系统管理角色实体的消息。

3.2

攻击 attack

攻击是指任何危及计算机资源与网络资源完整性、机密性或可用性的行为。

3.3

自动响应 automated response

自动响应是指网络入侵检测系统在发现攻击行为后自发采取的保护行为。

3.4

躲避 evasion

躲避是指入侵者发动攻击，而又不希望被发现而采取的行为。

3.5

漏报 false negatives

漏报是指一个攻击事件未被网络入侵检测系统检测到而造成的错误。

3.6

误报 false positives

误报是指系统把正常行为作为入侵攻击而进行报警，或者把一种攻击错误报告为另一种攻击而导致系统错误响应。

3.7

防火墙 firewall

在网络之间执行访问控制策略的一个或一组设备。