ICS 35.020
L 80

# 中华人民共和国国家标准

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

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

2012-06-29 发布　　2012-10-01 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

本标准按照 GB/T 1.1—2009 给出的规则起草。

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这些专利的责任。

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、北京神州绿盟科技有限公司、福建省海峡信息技术有限公司、沈阳东软系统集成工程有限公司、北京安氏领信科技发展有限公司、网御神州科技(北京)有限公司。

本标准主要起草人:沈亮、顾建新、俞优、顾健、袁智辉、韩鹏、张章学、于江、杜永峰、段继平。

# 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

## 1　范围

本标准规定了网络型入侵防御产品的功能要求、产品自身安全要求和产品保证要求，并提出了入侵防御产品的分级要求。

本标准适用于网络型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 17859—1999　计算机信息系统　安全保护等级划分准则

GB/T 25069—2010　信息安全技术　术语

## 3　术语和定义

GB/T 25069—2010 和 GB 17859—1999 界定的以及下列术语和定义适用于本文件。

3.1

**网络型入侵防御产品　network-based intrusion prevention system products**

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

**TCP 流重组　TCP reassembly**

攻击者将发送的攻击数据分别在一个会话连接中的多个数据包发出，用来躲避入侵防御系统的检测行为。

3.3

**SHELL 代码变形　SHELL deformation**

针对缓冲区溢出攻击，攻击者用其他方式替代原有程序指令并以一种伪随机的方式结合到一起，用来躲避入侵防御系统的检测行为。

3.4

**管理员　administrator**

对使用入侵防御产品的授权操作员、安全员、审计员等的统称。

3.5

**告警　alert**

当入侵防御产品发现有入侵行为时，向用户发出的紧急通知。

3.6

**误截　false blocking**

入侵防御产品在未发生攻击时对会话进行拦截的情况。对于在出现攻击时未发出或者发出错误的