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

GB/T 28451—2012

中华人民共和国
国家标准
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
GB/T 28451—2012
*
中国标准出版社出版发行
北京市朝阳区和平里西街甲2号(100013)
北京市西城区三里河北街16号(100045)
网址 www.spc.net.cn
总编室:(010)64275323　发行中心:(010)51780235
读者服务部:(010)68523946
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230　1/16　印张 4　字数 117 千字
2012年10月第一版　2012年10月第一次印刷
*
书号:155066·1-45543　定价 54.00 元

GB/T 28451-2012

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 …… 2
5　入侵防御产品技术要求组成 …… 2
5.1　组成说明 …… 2
5.2　功能和安全要求等级划分 …… 3
6　入侵防御产品的组成 …… 4
6.1　入侵事件分析单元 …… 4
6.2　入侵响应单元 …… 4
6.3　入侵事件审计单元 …… 4
6.4　管理控制单元 …… 4
7　入侵防御产品技术要求 …… 5
7.1　第一级 …… 5
7.2　第二级 …… 8
7.3　第三级 …… 14
7.4　性能要求 …… 20
8　入侵防御产品测评方法 …… 21
8.1　测试环境 …… 21
8.2　测试工具 …… 21
8.3　第一级 …… 21
8.4　第二级 …… 29
8.5　第三级 …… 42
8.6　性能测试 …… 58

b）　测试评价结果

分别记录入侵防御产品在不丢包的情况下，各吞吐量性能值。

8.6.2　误截和漏截测试

8.6.2.1　误截测试

误截测试：

a）　测试评价方法

1）　配置入侵防御产品的入侵防御策略集为最大；

2）　以主流应用协议按照不同比例进行混合作为正常背景流量，流量比例如 Packets（HTTP 38％、HTTPs 35％、DNS 13％、SMTP 7％、other 7％）、Bytes（HTTP 51％、HTTPS 35％、SMTP 9％、DNS 4％、other 1％）；

3）　对入侵防御产品进行流量模拟，保持入侵防御产品持续运行一段时间（例如：72h），记录产品的误截情况。

b）　测试评价结果

1）　分析记录与之对应的正常流量，确定误截情况。记录入侵防御产品拦截的入侵事件名称、发生时间、详细解释、个数等。

2）　开发商提交的误截允许范围应符合误截测试情况。

8.6.2.2　漏截测试

漏截测试：

a）　测试评价方法

1）　配置入侵防御产品的入侵防御策略集为最大；

2）　对应于入侵防御产品入侵事件库，选取入侵防御产品能够正常防御的多个网络远程入侵完整行为（不同类型的且较为常见的攻击事件）组成入侵事件测试集；

3）　按照吞吐量测试值的 80％作为背景流量，混合攻击流量，测试入侵防御产品的漏截情况，记录入侵防御产品入侵拦截的结果。

b）　测试评价结果

1）　记录入侵防御产品拦截的入侵事件名称、发生时间和数量，分析记录与之对应的模拟入侵事件；

2）　记录测试中入侵事件的总数量和入侵防御产品拦截的总数量，确定漏截情况；

3）　开发商提交的漏截允许范围应符合漏截测试情况。

开发者提供的内容应完整。

8.5.3.6.4 独立性测试

独立性测试评价：

a) 测试评价方法

评价者应审查开发者是否提供了用于测试的产品，且提供的产品是否适合测试。

b) 测试评价结果

测试记录以及最后结果(符合/不符合)，开发者应提供能适合第三方测试的产品。

8.5.3.7 脆弱性评定

8.5.3.7.1 指南检查

指南检查评价：

a) 测试评价方法

评价者应审查开发者提供的文档，是否满足了以下要求：

1) 评价文档是否确定了对产品的所有可能的操作方式(包括失败和操作失误后的操作)，是否确定了它们的后果，以及是否确定了对于保持安全操作的意义；
2) 评价文档是否列出了所有目标环境的假设以及所有外部安全措施(包括外部程序的、物理的或人员的控制)的要求；
3) 评价文档是否完整、清晰、一致、合理；
4) 评价开发者提供的分析文档，是否阐明文档是完整的。

b) 测试评价结果

测试记录以及最后结果(符合/不符合)符合测试评价方法要求。开发者提供的评价文档应完整，并且通过分析文档等方式阐明文档是完整的。

8.5.3.7.2 脆弱性分析

脆弱性分析评价：

a) 测试评价方法

1) 评价开发者提供的脆弱性分析文档，是否从用户可能破坏安全策略的明显途径出发，对产品的各种功能进行了分析；
2) 对被确定的脆弱性，评价开发者是否明确记录了采取的措施；
3) 对每一条脆弱性，评价是否有证据显示在使用产品的环境中该脆弱性不能被利用。

b) 测试评价结果

测试记录以及最后结果(符合/不符合)符合测试评价方法要求。开发者提供的脆弱性分析文档应完整。

8.6 性能测试

8.6.1 吞吐量

吞吐量测试：

a) 测试评价方法

1) 配置入侵防御产品的入侵防御策略集为最大；
2) 配置一条或者多条数据流，分别按照 64 字节、512 字节、1518 字节进行 UDP 双向吞吐量测试。

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。