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

告警信息并进行拦截的情况，因不影响到实际入侵拦截效果，故本标准的此项定义不包含这种情况。

3.7

漏截　miss blocking

当出现产品支持的攻击行为时，入侵防御产品未实现拦截攻击的情况。

4　缩略语

ARP：地址解析协议（Address Resolution Protocol）
DNS：域名系统（Domain Name System）
FTP：文件传输协议（File Transfer Protocol）
HTTP：超文本传输协议（Hyper Text Transfer Protocol）
ICMP：网间控制报文协议（Internet Control Message Protocol）
IP：网际协议（Internet Protocol）
MSN：微软网络服务（Microsoft Service Network）
NFS：网络文件系统（Network File System）
POP3：邮局协议 3（Post Office Protocol 3）
P2P：点对点（Point to Point）
RPC：远程过程调用（Remote Procedure Call）
SMB：服务器信息块（Server Message Block）
SMTP：简单邮件传输协议（Simple Mail Transfer Protocol）
SNMP：简单网络管理协议（Simple Network Management Protocol）
TCP：传输控制协议（Transmission Control Protocol）
TFTP：简单文件传输协议（Trivial File Transfer Protocol）
UDP：用户数据报协议（User Datagram Protocol）
URL：统一资源定位器（Universal Resource Locator）

5　入侵防御产品技术要求组成

5.1　组成说明

5.1.1　第一级

本级规定了入侵防御产品的最低安全要求。产品具备基本的协议分析、入侵发现和拦截能力，并对入侵事件生成记录，通过简单的用户标识和鉴别来限制对产品的功能配置和数据访问的控制，使用户具备自主安全保护的能力，阻止非法用户危害入侵防御产品，保护入侵防御产品的正常运行。

5.1.2　第二级

本级要求划分安全管理角色，以细化对入侵防御产品的管理。加入审计功能，使得授权管理员的行为是可追踪的。产品在实现入侵发现、拦截的同时，更要求具备及时告警的功能，对于事件记录还要求能生成、输出报表，以及要求具备硬件失效处理机制。

5.1.3　第三级

本级要求入侵防御产品提供对外的通用接口，报表结果具备模板定制等功能，还要求具备多鉴别机制、升级安全、自我隐藏、负载均衡等功能，对产品的自身安全提出更高的要求，对产品的正常运行提供更强的保护。

5.1.4 性能

本项对入侵防御产品的性能要求进行了规定，覆盖所有等级。

5.2 功能和安全要求等级划分

入侵防御产品的安全等级划分如表1、表2所示。对入侵防御产品的等级评定是依据表1和表2，结合产品保证要求的综合评定得出的，符合第一级的入侵防御产品应满足表1、表2中所标明的一级产品应满足的所有项目，以及对第一级产品的相关保证要求；符合第二级的入侵防御产品应满足表1、表2中所标明的二级产品应满足的所有项目，以及对第二级产品的相关保证要求；符合第三级的入侵防御产品应满足表1、表2中所标明的三级产品应满足的所有项目，以及对第三级产品的相关保证要求。

表1 入侵防御产品功能要求等级划分表

产品功能和性能要求	功能组件	一级	二级	三级
入侵事件分析要求	数据收集	*	*	*
	协议分析	*	*	*
	入侵发现	*	*	*
	入侵逃避发现		*	*
	流量监测	*	*	*
入侵响应功能要求	拦截能力	*	*	*
	安全告警		*	*
	告警方式		*	*
	事件合并		*	*
入侵事件审计功能	事件生成	*	*	*
	事件记录	*	*	*
	报表生成		*	*
	报表查阅		*	*
	报表输出		*	*
	报表模板的定制			*
管理控制功能要求	管理界面	*	*	*
	入侵事件库	*	*	*
	事件分级	*	*	*
	事件定义		*	*
	协议定义		*	*
	流量控制		*	*
	通用接口			*
	硬件失效处理	*	*	* *
	策略配置	*	*	*
	产品升级	*	* *	* *
	管理接口独立	*	*	*
注：“*”表示具有该要求。				

表 2　入侵防御产品自身安全要求等级划分表

安全功能要求	功能组件	一级	二级	三级
标识和鉴别	用户鉴别	*	*	*
	鉴别失败的处理	*	* *	* *
	鉴别数据保护	*	*	*
	超时锁定		*	*
	多鉴别机制			*
用户管理	标识唯一性	*	*	*
	用户属性定义	*	*	*
	角色分级		*	*
安全功能保护	安全数据管理	*	*	*
	数据存储告警		*	* *
	升级安全			*
	自我隐藏			*
安全审计	审计数据生成		*	*
	审计查阅		*	*
	受限的审计查阅		*	*
注：“*”表示具有该要求。				

6　入侵防御产品的组成

6.1　入侵事件分析单元

采用相关的分析检测技术，对流入目标网络内的所有数据进行提取并分析。

6.2　入侵响应单元

根据定义的策略对入侵行为进行拦截响应。

6.3　入侵事件审计单元

在违反安全策略的入侵事件发生时，对事件发生的时间、主体和客体等信息进行记录和统计。

6.4　管理控制单元

负责入侵防御产品定制策略、审阅日志、产品状态管理，并以可视化形式提交授权用户进行管理。

7 入侵防御产品技术要求

7.1 第一级

7.1.1 产品功能要求

7.1.1.1 入侵事件分析功能要求

7.1.1.1.1 数据收集

入侵防御产品应具有实时收集流入目标网络内所有数据包的能力。

7.1.1.1.2 协议分析

入侵防御产品应对收集的数据包进行协议分析。

7.1.1.1.3 入侵发现

入侵防御产品应能发现协议中的入侵行为。

7.1.1.1.4 流量监测

入侵防御产品应对目标环境中的异常流量进行监测。

7.1.1.2 入侵响应功能要求

入侵防御产品应对发现的入侵行为进行预先拦截,防止入侵行为进入目标网络。

7.1.1.3 入侵事件审计功能要求

7.1.1.3.1 事件生成

入侵防御产品应能对拦截行为及时生成审计记录。

7.1.1.3.2 事件记录

入侵防御产品应记录并保存拦截到的入侵事件。入侵事件信息应至少包含事件名称、事件发生日期和时间、源 IP 地址、源端口、目的 IP 地址、目的端口、危害等级等内容。

7.1.1.4 管理控制功能要求

7.1.1.4.1 管理界面

入侵防御产品应提供用户界面用于管理、配置入侵防御产品。管理配置界面应包含配置和管理产品所需的所有功能。

7.1.1.4.2 入侵事件库

入侵防御产品应提供入侵事件库。事件库应包括事件名称、详细描述定义等。

7.1.1.4.3 事件分级

入侵防御产品应按照事件的严重程度对事件进行分级,以使授权管理员能从大量的信息中捕捉到危险的事件。

7.1.1.4.4 硬件失效处理

入侵防御产品应提供硬件失效处理机制。

7.1.1.4.5 策略配置

入侵防御产品应提供对入侵防御策略、响应措施进行配置的功能。

7.1.1.4.6 产品升级

入侵防御产品应具备更新、升级产品事件库的能力。

7.1.1.4.7 管理接口独立

入侵防御产品应具备独立的管理接口。

7.1.2 产品自身安全要求

7.1.2.1 标识和鉴别

7.1.2.1.1 用户鉴别

入侵防御产品应在用户执行任何与安全功能相关的操作之前对用户进行鉴别。

7.1.2.1.2 鉴别失败的处理

入侵防御产品应在用户鉴别尝试失败连续达到指定次数后，阻止用户进一步进行尝试。

7.1.2.1.3 鉴别数据保护

入侵防御产品应保护鉴别数据不被未授权查阅和修改。

7.1.2.2 用户管理

7.1.2.2.1 标识唯一性

入侵防御产品应保证所设置的用户标识全局唯一。

7.1.2.2.2 用户属性定义

入侵防御产品应为每一个用户保存安全属性表，属性应包括用户标识、鉴别数据、授权信息或用户组信息、其他安全属性等。

7.1.2.3 安全功能保护

入侵防御产品应仅限于指定的授权用户访问事件数据，禁止其他用户对事件数据的操作。

7.1.3 产品保证要求

7.1.3.1 配置管理

开发者应为入侵防御产品的不同版本提供唯一的标识。

入侵防御产品的每个版本应当使用它们的唯一标识作为标签。

7.1.3.2 交付与运行

开发者应提供文档说明入侵防御产品的安装、生成和启动。

7.1.3.3 安全功能开发

7.1.3.3.1 功能设计

开发者应提供文档说明入侵防御产品的安全功能设计。

功能设计应以非形式方法来描述安全功能与其外部接口，并描述使用外部安全功能接口的目的与方法，在需要的时候，还要提供例外情况和出错信息的细节。

7.1.3.3.2 表示对应性

开发者应在入侵防御产品安全功能表示的所有相邻对之间提供对应性分析。

7.1.3.4 指导性文档

7.1.3.4.1 管理员指南

开发者应给授权管理员提供包括以下内容的管理员指南：

a) 入侵防御产品可以使用的管理功能和接口；
b) 怎样安全地管理入侵防御产品；
c) 在安全处理环境中应进行控制的功能和权限；
d) 所有对与入侵防御产品的安全操作有关的用户行为的假设；
e) 所有受管理员控制的安全参数，如果可能，应指明安全值；
f) 每一种与管理功能有关的安全相关事件，包括对安全功能所控制的实体的安全特性进行的改变；
g) 所有与授权管理员有关的 IT 环境的安全要求。

管理员指南应与为评价而提供的其他所有文件保持一致。

7.1.3.4.2 用户指南

开发者应提供包括以下内容的用户指南：

a) 入侵防御产品的非管理用户可使用的安全功能和接口；
b) 入侵防御产品提供给用户的安全功能和接口的用法；
c) 用户可获取但应受安全处理环境控制的所有功能和权限；
d) 入侵防御产品安全操作中用户所应承担的职责；
e) 与用户有关的 IT 环境的所有安全要求。

用户指南应与为评价而提供的其他所有文件保持一致。

7.1.3.5 开发安全要求

开发者应提供包括以下内容的开发安全文件：

a) 开发安全文件应描述在入侵防御产品的开发环境中，为保护入侵防御产品设计和实现的机密性和完整性，而在物理上、程序上、人员上以及其他方面所采取的必要的安全措施；
b) 开发安全文件还应提供在入侵防御产品的开发和维护过程中执行安全措施的证据。

7.1.3.6 测试

7.1.3.6.1 范围

开发者应提供测试覆盖的分析结果。

测试覆盖的分析结果应表明测试文档中所标识的测试与安全功能设计中所描述的安全功能是对应的。

7.1.3.6.2 功能测试

开发者应测试安全功能，并提供以下测试文档：

a) 测试文档应包括测试计划、测试规程、预期的测试结果和实际测试结果。

b) 测试计划应标识要测试的安全功能，并描述测试的目标。测试规程应标识要执行的测试，并描述每个安全功能的测试概况，这些概况包括对其他测试结果的顺序依赖性。

c) 期望的测试结果应表明测试成功后的预期输出。

d) 实际测试结果应表明每个被测试的安全功能能按照规定进行运作。

7.2 第二级

7.2.1 产品功能要求

7.2.1.1 入侵事件分析功能要求

7.2.1.1.1 数据收集

入侵防御产品应具有实时收集流入目标网络内所有数据包的能力。

7.2.1.1.2 协议分析

入侵防御产品应对收集的数据包进行协议分析。

7.2.1.1.3 入侵发现

入侵防御产品应能发现协议中的入侵行为。

7.2.1.1.4 入侵逃避发现

入侵防御产品应能发现躲避或欺骗检测的行为，如 IP 碎片重组、TCP 流重组、协议端口重定位、URL 字符串变形、SHELL 代码变形等。

7.2.1.1.5 流量监测

入侵防御产品应对目标环境中的异常流量进行监测。

7.2.1.2 入侵响应功能要求

7.2.1.2.1 拦截能力

入侵防御产品应对发现的入侵行为进行预先拦截，防止入侵行为进入目标网络。

7.2.1.2.2 安全告警

入侵防御产品应在发现并拦截入侵行为时，采取相应动作发出安全警告。

7.2.1.2.3 告警方式

入侵防御产品的告警方式宜采取屏幕实时提示、E-mail 告警、声音告警等一种或多种方式。

7.2.1.2.4 事件合并

入侵防御产品应具有对高频度发生的相同安全事件进行合并告警，避免出现告警风暴的能力。

7.2.1.3 入侵事件审计功能要求

7.2.1.3.1 事件生成

入侵防御产品应能对拦截行为及时生成审计记录。

7.2.1.3.2 事件记录

入侵防御产品应记录并保存拦截到的入侵事件。入侵事件信息应至少包含事件名称、事件发生日期和时间、源 IP 地址、源端口、目的 IP 地址、目的端口、危害等级等内容。

7.2.1.3.3 报表生成

入侵防御产品应能生成详尽的结果报表。

7.2.1.3.4 报表查阅

入侵防御产品应具有浏览结果报表的功能。

7.2.1.3.5 报表输出

入侵防御产品应支持管理员按照自己的要求修改和定制报表内容，并输出成方便阅读的文件格式，至少支持以下报表文件格式中的一种或多种：DOC、PDF、HTML、XLS 等。

7.2.1.4 管理控制功能要求

7.2.1.4.1 管理界面

入侵防御产品应提供用户界面用于管理、配置入侵防御产品。管理配置界面应包含配置和管理产品所需的所有功能。

7.2.1.4.2 入侵事件库

入侵防御产品应提供入侵事件库。事件库应包括事件名称、详细描述定义等。

7.2.1.4.3 事件分级

入侵防御产品应按照事件的严重程度对事件进行分级，以使授权管理员能从大量的信息中捕捉到危险的事件。

7.2.1.4.4 事件定义

入侵防御产品应允许授权管理员自定义策略事件。

7.2.1.4.5 协议定义

入侵防御产品除支持默认的网络协议集外，还应允许授权管理员定义新的协议，或对协议的端口进行重新定位。

7.2.1.4.6 流量控制

入侵防御产品具备对异常流量进行控制的功能。

7.2.1.4.7 硬件失效处理

入侵防御产品应提供硬件失效处理机制。

7.2.1.4.8 策略配置

入侵防御产品应提供对入侵防御策略、响应措施进行配置的功能。

7.2.1.4.9 产品升级

入侵防御产品应具备更新、升级产品版本和事件库的能力。

7.2.1.4.10 管理接口独立

入侵防御产品应具备独立的管理接口。

7.2.2 产品自身安全要求

7.2.2.1 标识和鉴别

7.2.2.1.1 用户鉴别

入侵防御产品应在用户执行任何与安全功能相关的操作之前对用户进行鉴别。

7.2.2.1.2 鉴别失败的处理

入侵防御产品应在用户鉴别尝试失败连续达到指定次数后，阻止用户进一步进行尝试，并将有关信息生成审计事件。最多失败次数仅由授权管理员设定。

7.2.2.1.3 鉴别数据保护

入侵防御产品应保护鉴别数据不被未授权查阅和修改。

7.2.2.1.4 超时锁定

入侵防御产品应具有管理员登录超时重新鉴别功能。在设定的时间段内没有任何操作的情况下，中止或者锁定会话，需要再次进行身份鉴别才能够重新管理产品。最大超时时间仅由授权管理员设定。

7.2.2.2 用户管理

7.2.2.2.1 标识唯一性

入侵防御产品应保证所设置的用户标识全局唯一。

7.2.2.2.2 用户属性定义

入侵防御产品应为每一个用户保存安全属性表，属性应包括用户标识、鉴别数据、授权信息或用户组信息、其他安全属性等。

7.2.2.2.3 角色分级

入侵防御产品应为管理角色进行分级，不同级别的管理角色具有不同的管理权限，以增加入侵防御产品管理的安全性。

7.2.2.3 安全功能保护

7.2.2.3.1 安全数据管理

入侵防御产品应仅限于指定的授权用户访问事件数据，禁止其他用户对事件数据的操作。

7.2.2.3.2 数据存储告警

入侵防御产品应在发生事件数据存储空间将耗尽等情况时，自动产生告警，并采取措施避免事件数据丢失。

7.2.2.4 安全审计

7.2.2.4.1 审计数据生成

入侵防御产品应至少为下述可审计事件产生审计记录：

a) 试图登录入侵防御产品管理端口和管理身份鉴别请求；

b) 所有对安全策略更改的操作；

c) 修改安全属性的所有尝试。

应在每个审计记录中至少记录事件的日期和时间、事件类型、主体身份、事件的结果（成功或失败）等信息。

7.2.2.4.2 审计查阅

入侵防御产品应为授权管理员提供从审计记录中读取全部审计信息的功能，并可对审计记录进行排序。

7.2.2.4.3 受限的审计查阅

除了具有明确的读访问权限的授权管理员之外，入侵防御产品应禁止非授权用户对审计记录的读访问。

7.2.3 产品保证要求

7.2.3.1 配置管理

7.2.3.1.1 配置管理能力

开发者应使用配置管理系统并提供配置管理文档，以及为入侵防御产品的不同版本提供唯一的标识。

配置管理系统应对所有的配置项作出唯一的标识，并保证只有经过授权才能修改配置项。

配置管理文档应包括配置清单和配置管理计划。在配置清单中，应对每一配置项给出相应的描述；在配置管理计划中，应描述配置管理系统是如何使用的。实施的配置管理应与配置管理计划相一致。

配置管理文档还应描述对配置项给出唯一标识的方法，并提供所有的配置项得到有效的维护的证据。

7.2.3.1.2 配置管理范围

开发者应提供配置管理文档。

配置管理文档应说明配置管理系统至少能跟踪：入侵防御产品实现表示、设计文档、测试文档、用户文档、管理员文档和配置管理文档，并描述配置管理系统是如何跟踪配置项的。

7.2.3.2 交付与运行

7.2.3.2.1 交付

开发者应使用一定的交付程序交付入侵防御产品，并将交付过程文档化。

交付文档应描述在给用户方交付入侵防御产品的各版本时，为维护安全所必需的所有程序。

7.2.3.2.2 安装生成

开发者应提供文档说明入侵防御产品的安装、生成和启动。

7.2.3.3 安全功能开发

7.2.3.3.1 功能设计

开发者应提供文档说明入侵防御产品的安全功能设计。

功能设计应以非形式方法来描述安全功能与其外部接口，并描述使用外部安全功能接口的目的与方法，在需要的时候，还要提供例外情况和出错信息的细节。

7.2.3.3.2 高层设计

开发者应提供文档说明入侵防御产品安全功能的高层设计。

高层设计应以非形式方法表述并且是内在一致的。为说明安全功能的结构，高层设计应将安全功能分解为各个安全功能子系统进行描述，并阐明如何将有助于加强入侵防御产品安全功能的子系统和其他子系统分开。对于每一个安全功能子系统，高层设计应描述其提供的安全功能，标识其所有接口以及哪些接口是外部可见的，描述其所有接口的使用目的与方法，并提供安全功能子系统的作用、例外情况和出错信息的细节。高层设计还应标识入侵防御产品安全要求的所有基础性的硬件、固件和软件，并且支持由这些硬件、固件或软件所实现的保护机制。

7.2.3.3.3 表示对应性

开发者应在入侵防御产品安全功能表示的所有相邻对之间提供对应性分析。

7.2.3.4 指导性文档

7.2.3.4.1 管理员指南

开发者应给授权管理员提供包括以下内容的管理员指南：

a) 入侵防御产品管理员可以使用的管理功能和接口；
b) 怎样安全地管理入侵防御产品；
c) 在安全处理环境中应进行控制的功能和权限；
d) 所有对与入侵防御产品的安全操作有关的用户行为的假设；
e) 所有受管理员控制的安全参数，如果可能，应指明安全值；
f) 每一种与管理功能有关的安全相关事件，包括对安全功能所控制的实体的安全特性进行的改变；
g) 所有与授权管理员有关的 IT 环境的安全要求。

管理员指南应与为评价而提供的其他所有文件保持一致。

7.2.3.4.2 用户指南

开发者应提供包括以下内容的用户指南：

a) 入侵防御产品的非管理用户可使用的安全功能和接口；
b) 入侵防御产品提供给用户的安全功能和接口的用法；
c) 用户可获取但应受安全处理环境控制的所有功能和权限；
d) 入侵防御产品安全操作中用户所应承担的职责；

e) 与用户有关的 IT 环境的所有安全要求。

用户指南应与为评价而提供的其他所有文件保持一致。

7.2.3.5 开发安全要求

开发者应提供包括以下内容的开发安全文件：

a) 开发安全文件应描述在入侵防御产品的开发环境中，为保护入侵防御产品设计和实现的机密性和完整性，而在物理上、程序上、人员上以及其他方面所采取的必要的安全措施；

b) 开发安全文件还应提供在入侵防御产品的开发和维护过程中执行安全措施的证据。

7.2.3.6 测试

7.2.3.6.1 范围

开发者应提供测试覆盖的分析结果。

测试覆盖的分析结果应表明测试文档中所标识的测试与安全功能设计中所描述的安全功能是对应的，且该对应是完整的。

7.2.3.6.2 测试深度

开发者应提供测试深度的分析。

在深度分析中，应说明测试文档中所标识的对安全功能的测试，足以表明该安全功能和高层设计是一致的。

7.2.3.6.3 功能测试

开发者应测试安全功能，并提供以下测试文档：

a) 测试文档应包括测试计划、测试规程、预期的测试结果和实际测试结果；

b) 测试计划应标识要测试的安全功能，并描述测试的目标。测试规程应标识要执行的测试，并描述每个安全功能的测试概况，这些概况包括对其他测试结果的顺序依赖性；

c) 期望的测试结果应表明测试成功后的预期输出；

d) 实际测试结果应表明每个被测试的安全功能能按照规定进行运作。

7.2.3.6.4 独立性测试

开发者应提供证据证明，开发者提供的入侵防御产品经过独立的第三方测试并通过。

7.2.3.7 脆弱性评定

7.2.3.7.1 指南检查

开发者应提供文档。

在文档中，应确定对入侵防御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)、它们的后果以及对于保持安全操作的意义。文档中还应列出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。文档应是完整的、清晰的、一致的、合理的。

7.2.3.7.2 脆弱性分析

开发者应从用户可能破坏安全策略的明显途径出发，对入侵防御产品的各种功能进行分析并形成文档。对被确定的脆弱性，开发者应明确记录采取的措施。

对每一条脆弱性，应能够显示在使用入侵防御产品的环境中该脆弱性不能被利用。

7.3 第三级

7.3.1 产品功能要求

7.3.1.1 入侵事件分析功能要求

7.3.1.1.1 数据收集

入侵防御产品应具有实时收集流入目标网络内所有数据包的能力。

7.3.1.1.2 协议分析

入侵防御产品应对收集的数据包进行协议分析。

7.3.1.1.3 入侵发现

入侵防御产品应能发现协议中的入侵行为。

7.3.1.1.4 入侵逃避发现

入侵防御产品应能发现躲避或欺骗检测的行为，如 IP 碎片重组、TCP 流重组、协议端口重定位、URL 字符串变形、SHELL 代码变形等。

7.3.1.1.5 流量监测

入侵防御产品应对目标环境中的异常流量进行监测。

7.3.1.2 入侵响应功能要求

7.3.1.2.1 拦截能力

入侵防御产品应对发现的入侵行为进行预先拦截，防止入侵行为进入目标网络。

7.3.1.2.2 安全告警

入侵防御产品应在发现并拦截入侵行为时，采取相应动作发出安全警告。

7.3.1.2.3 告警方式

入侵防御产品的告警方式宜采取屏幕实时提示、E-mail 告警、声音告警等一种或多种方式。

7.3.1.2.4 事件合并

入侵防御产品应具有对高频度发生的相同安全事件进行合并告警，避免出现告警风暴的能力。

7.3.1.3 入侵事件审计功能要求

7.3.1.3.1 事件生成

入侵防御产品应能对拦截行为及时生成审计记录。

7.3.1.3.2 事件记录

入侵防御产品应记录并保存拦截到的入侵事件。入侵事件信息应至少包含事件名称、事件发生日期和时间、源 IP 地址、源端口、目的 IP 地址、目的端口、危害等级等内容。

7.3.1.3.3 报表生成

入侵防御产品应能生成详尽的结果报表。

7.3.1.3.4 报表查阅

入侵防御产品应具有浏览结果报表的功能。

7.3.1.3.5 报表输出

入侵防御产品应支持管理员按照自己的要求修改和定制报表内容，并输出成方便阅读的文件格式，至少支持以下报表文件格式中的一种或多种：DOC、PDF、HTML、XLS 等。

7.3.1.3.6 报表模板的定制

入侵防御产品应提供结果报表模板的定制功能。

7.3.1.4 管理控制功能要求

7.3.1.4.1 管理界面

入侵防御产品应提供用户界面用于管理、配置入侵防御产品。管理配置界面应包含配置和管理产品所需的所有功能。

7.3.1.4.2 入侵事件库

入侵防御产品应提供入侵事件库。事件库应包括事件名称、详细描述定义等。

7.3.1.4.3 事件分级

入侵防御产品应按照事件的严重程度对事件进行分级，以使授权管理员能从大量的信息中捕捉到危险的事件。

7.3.1.4.4 事件定义

入侵防御产品应允许授权管理员自定义策略事件。

7.3.1.4.5 协议定义

入侵防御产品除支持默认的网络协议集外，还应允许授权管理员定义新的协议，或对协议的端口进行重新定位。

7.3.1.4.6 流量控制

入侵防御产品具备对异常流量进行控制的功能。

7.3.1.4.7 通用接口

入侵防御产品应提供对外的通用接口，以便与其他安全设备共享信息或规范化管理。

7.3.1.4.8 硬件失效处理

入侵防御产品应在提供硬件失效处理机制的同时，还应具备双机热备的能力。

7.3.1.4.9 负载均衡

入侵防御产品应具备负载均衡功能，能够根据安全策略将网络流量均衡到多台服务器上。

7.3.1.4.10 策略配置

入侵防御产品应提供对入侵防御策略、响应措施进行配置的功能。

7.3.1.4.11 产品升级

入侵防御产品应具备更新、升级产品版本和事件库的能力。

7.3.1.4.12 管理接口独立

入侵防御产品应具备独立的管理接口。

7.3.2 产品自身安全要求

7.3.2.1 标识和鉴别

7.3.2.1.1 用户鉴别

入侵防御产品应在用户执行任何与安全功能相关的操作之前对用户进行鉴别。

7.3.2.1.2 鉴别失败的处理

入侵防御产品应在用户鉴别尝试失败连续达到指定次数后，阻止用户进一步进行尝试，并将有关信息生成审计事件。最多失败次数仅由授权管理员设定。

7.3.2.1.3 鉴别数据保护

入侵防御产品应保护鉴别数据不被未授权查阅和修改。

7.3.2.1.4 超时锁定

入侵防御产品应具有管理员登录超时重新鉴别功能。在设定的时间段内没有任何操作的情况下，中止或者锁定会话，需要再次进行身份鉴别才能够重新管理产品。最大超时时间仅由授权管理员设定。

7.3.2.1.5 多鉴别机制

入侵防御产品应提供多种鉴别方式，或者允许授权管理员执行自定义的鉴别措施，以实现多重身份鉴别措施。多鉴别机制应同时使用。

7.3.2.2 用户管理

7.3.2.2.1 标识唯一性

入侵防御产品应保证所设置的用户标识全局唯一。

7.3.2.2.2 用户属性定义

入侵防御产品应为每一个用户保存安全属性表，属性应包括用户标识、鉴别数据、授权信息或用户组信息、其他安全属性等。

7.3.2.2.3 角色分级

入侵防御产品应为管理角色进行分级，不同级别的管理角色具有不同的管理权限，以增加入侵防御产品管理的安全性。

7.3.2.3 安全功能保护

7.3.2.3.1 安全数据管理

入侵防御产品应仅限于指定的授权用户访问事件数据，禁止其他用户对事件数据的操作。

7.3.2.3.2 数据存储告警

入侵防御产品应在发生事件数据存储器空间将耗尽等情况时，自动产生告警，并采取措施避免事件数据丢失。产生告警的剩余存储空间大小应由管理员自主设定。

7.3.2.3.3 升级安全

入侵防御产品应确保事件库和版本升级时的安全，保证升级包是由开发商提供的。

7.3.2.3.4 自我隐藏

入侵防御产品应至少提供网桥方式的接入方式，采取隐藏 IP 地址等措施使自身在网络上不可见，以降低被攻击的可能性。

7.3.2.4 安全审计

7.3.2.4.1 审计数据生成

入侵防御产品应至少为下述可审计事件产生审计记录：

a) 试图登录入侵防御产品管理端口和管理身份鉴别请求；

b) 所有对安全策略更改的操作；

c) 修改安全属性的所有尝试。

应在每个审计记录中至少记录事件的日期和时间、事件类型、主体身份、事件的结果（成功或失败）等信息。

7.3.2.4.2 审计查阅

入侵防御产品应为授权管理员提供从审计记录中读取全部审计信息的功能，并可对审计记录进行排序。

7.3.2.4.3 受限的审计查阅

除了具有明确的读访问权限的授权管理员之外，入侵防御产品应禁止非授权用户对审计记录的读访问。

7.3.3 产品保证要求

7.3.3.1 配置管理

7.3.3.1.1 配置管理能力

开发者应使用配置管理系统并提供配置管理文档，以及为入侵防御产品的不同版本提供唯一的

标识。

配置管理系统应对所有的配置项作出唯一的标识，并保证只有经过授权才能修改配置项，还应支持入侵防御产品基本配置项的生成。

配置管理文档应包括配置清单、配置管理计划以及接受计划。配置清单用来描述组成入侵防御产品的配置项。在配置管理计划中，应描述配置管理系统是如何使用的。实施的配置管理应与配置管理计划相一致。在接受计划中，应描述对修改过或新建的配置项进行接受的程序。

配置管理文档还应描述对配置项给出唯一标识的方法，并提供所有的配置项得到有效的维护的证据。

7.3.3.1.2 配置管理范围

开发者应提供配置管理文档。

配置管理文档应说明配置管理系统至少能跟踪：入侵防御产品实现表示、设计文档、测试文档、用户文档、管理员文档、配置管理文档和安全缺陷，并描述配置管理系统是如何跟踪配置项的。

7.3.3.2 交付与运行

7.3.3.2.1 交付

开发者应使用一定的交付程序交付入侵防御产品，并将交付过程文档化。

交付文档应包括以下内容：

a) 在给用户方交付入侵防御产品的各版本时，为维护安全所必需的所有程序；

b) 开发者向用户提供的产品版本和用户收到的版本之间的差异以及如何监测对产品的修改；

c) 如何发现他人伪装成开发者修改用户的产品。

7.3.3.2.2 安装生成

开发者应提供文档说明入侵防御产品的安装、生成和启动。

7.3.3.3 安全功能开发

7.3.3.3.1 功能设计

开发者应提供文档说明入侵防御产品的安全功能设计。

安全功能设计应以非形式方法来描述安全功能与其外部接口，并描述使用外部安全功能接口的目的与方法，在需要的时候，还要提供例外情况和出错信息的细节。

7.3.3.3.2 高层设计

开发者应提供文档说明入侵防御产品安全功能的高层设计。

高层设计应以非形式方法表述并且是内在一致的。为说明安全功能的结构，高层设计应将安全功能分解为各个安全功能子系统进行描述，并阐明如何将有助于加强产品安全功能的子系统和其他子系统分开。对于每一个安全功能子系统，高层设计应描述其提供的安全功能，标识其所有接口以及哪些接口是外部可见的，描述其所有接口的使用目的与方法，并提供安全功能子系统的作用、例外情况和出错信息的细节。高层设计还应标识入侵防御产品安全要求的所有基础性的硬件、固件和软件，并且支持由这些硬件、固件或软件所实现的保护机制。

7.3.3.3.3 安全功能的实现

开发者应为选定的产品安全功能子集提供实现表示。

实现表示应无歧义而且详细地定义产品安全功能，使得不需要进一步的设计就能生成该安全功能的子集。实现表示应是内在一致的。

7.3.3.3.4 低层设计

开发者应提供文档说明入侵防御产品安全功能的低层设计。

低层设计应是非形式化、内在一致的。在描述产品安全功能时，低层设计应采用模块术语，说明每一个安全功能模块的目的，并标识安全功能模块的所有接口和安全功能模块可为外部所见的接口，以及安全功能模块所有接口的目的与方法，适当时，还应提供接口的作用、例外情况和出错信息的细节。

低层设计还应包括以下内容：

a) 以安全功能性术语及模块的依赖性术语，定义模块间的相互关系；

b) 说明如何提供每一个安全策略的强化功能；

c) 说明如何将入侵防御产品加强安全策略的模块和其他模块分离开。

7.3.3.3.5 表示对应性

开发者应在入侵防御产品安全功能表示的所有相邻对之间提供对应性分析。

7.3.3.4 指导性文档

7.3.3.4.1 管理员指南

开发者应给授权管理员提供包括以下内容的管理员指南：

a) 产品管理员可以使用的管理功能和接口；

b) 怎样安全地管理入侵防御产品；

c) 在安全处理环境中应进行控制的功能和权限；

d) 所有对与入侵防御产品的安全操作有关的用户行为的假设；

e) 所有受管理员控制的安全参数，如果可能，应指明安全值；

f) 每一种与管理功能有关的安全相关事件，包括对安全功能所控制的实体的安全特性进行的改变；

g) 所有与授权管理员有关的 IT 环境的安全要求。

管理员指南应与为评价而提供的其他所有文件保持一致。

7.3.3.4.2 用户指南

开发者应提供包括以下内容的用户指南：

a) 入侵防御产品的非管理用户可使用的安全功能和接口；

b) 入侵防御产品提供给用户的安全功能和接口的用法；

c) 用户可获取但应受安全处理环境控制的所有功能和权限；

d) 入侵防御产品安全操作中用户所应承担的职责；

e) 与用户有关的 IT 环境的所有安全要求。

用户指南应与为评价而提供的其他所有文件保持一致。

7.3.3.5 开发安全要求

开发者应提供包括以下内容的开发安全文件：

a) 开发安全文件应描述在入侵防御产品的开发环境中，为保护入侵防御产品设计和实现的机密性和完整性，而在物理上、程序上、人员上以及其他方面所采取的必要的安全措施；

b） 开发安全文件还应提供在入侵防御产品的开发和维护过程中执行安全措施的证据。

7.3.3.6 测试

7.3.3.6.1 范围

开发者应提供测试覆盖的分析结果。

测试覆盖的分析结果应表明测试文档中所标识的测试与安全功能设计中所描述的安全功能是对应的，且该对应是完整的。

7.3.3.6.2 测试深度

开发者应提供测试深度的分析。

在深度分析中，应说明测试文档中所标识的对安全功能的测试，足以表明该安全功能和高层设计是一致的。

7.3.3.6.3 功能测试

开发者应测试安全功能，并提供以下测试文档：

a） 测试文档应包括测试计划、测试规程、预期的测试结果和实际测试结果。

b） 测试计划应标识要测试的安全功能，并描述测试的目标。测试规程应标识要执行的测试，并描述每个安全功能的测试概况，这些概况包括对其他测试结果的顺序依赖性。

c） 期望的测试结果应表明测试成功后的预期输出。

d） 实际测试结果应表明每个被测试的安全功能能按照规定进行运作。

7.3.3.6.4 独立性测试

开发者应提供证据证明，开发者提供的入侵防御产品经过独立的第三方测试并通过。

7.3.3.7 脆弱性评定

7.3.3.7.1 指南检查

开发者应提供文档。

在文档中，应确定对入侵防御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）、它们的后果以及对于保持安全操作的意义。文档中还应列出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。文档应是完整的、清晰的、一致的、合理的。在分析文档中，应阐明文档是完整的。

7.3.3.7.2 脆弱性分析

开发者应从用户可能破坏安全策略的明显途径出发，对入侵防御产品的各种功能进行分析并形成文档。对被确定的脆弱性，开发者应明确记录采取的措施。

对每一条脆弱性，应能够显示在使用入侵防御产品的环境中该脆弱性不能被利用。

7.4 性能要求

7.4.1 吞吐量

入侵防御产品的吞吐量视不同速率的产品有所不同，在开启产品最大策略集和不丢包的情况下，选择不同长度的数据包对入侵防御产品的吞吐量进行测试。

7.4.2 误截和漏截

7.4.2.1 误截

应在正常背景流量条件下,对入侵防御产品的误截情况进行测试。

7.4.2.2 漏截

应在正常和入侵背景混合流量条件下,对入侵防御产品的漏截情况进行测试。

8 入侵防御产品测评方法

8.1 测试环境

入侵防御产品测试的典型网络环境示意图如图 1 所示。

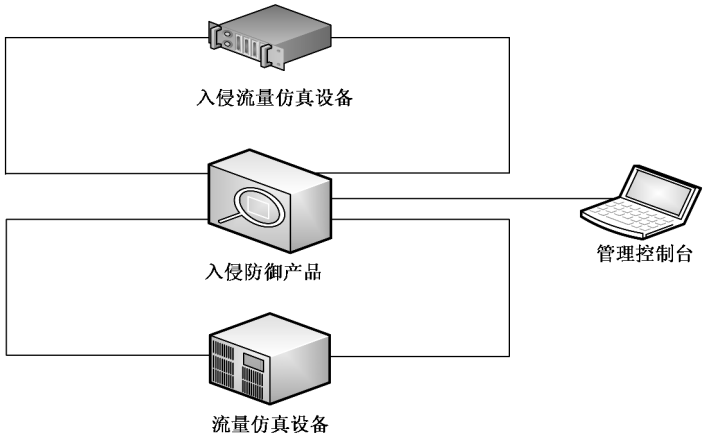

图 1 入侵防御产品测试环境示意图

测试设备包括测试所需的交换机、入侵流量仿真设备、流量仿真设备以及入侵防御产品控制台等。其中,入侵流量仿真设备、流量仿真设备可为多台模拟正常流量计算机、模拟攻击源计算机和被攻击计算机,也可以是专用测试设备。

8.2 测试工具

可用的测试工具包括但不限于:专用的网络性能分析仪生成网络背景流量;网络数据包获取软件进行包回放;扫描工具和攻击工具包。

8.3 第一级

8.3.1 产品功能测试

8.3.1.1 入侵事件分析功能测试

8.3.1.1.1 数据收集

数据收集测试:

a) 测试评价方法

检测入侵防御产品是否能够以网桥或网关方式正确接入网络,具备实时收集流入受保护网段内的数据包的能力。

b） 测试评价结果

1） 入侵防御产品应能够以网桥或网关方式接入网络；

2） 入侵防御产品应能够获取足够的网络数据包以分析入侵事件。

8.3.1.1.2 协议分析

协议分析测试：

a） 测试评价方法

1） 查看入侵防御产品的安全策略配置文档，检查安全事件的描述是否具有协议类型等属性；

2） 检查产品说明书，查找关于协议分析方法的说明，按照产品所声明的协议分析类型，抽样生成协议事件，组成攻击事件测试集；

3） 配置产品的入侵防御策略为最大策略集；

4） 发送攻击事件测试集中的所有事件，记录产品的检测结果。

b） 测试评价结果

1） 记录产品拦截入侵的相应攻击名称和类型；

2） 产品说明书中声称能够监视的协议事件主要包括以下类型：ARP、ICMP、IP、TCP、UDP、RPC、HTTP、FTP、TFTP、SNMP、TELNET、DNS、SMTP、POP3、NETBIOS、NFS、SMB、MSN、P2P 等，抽样测试应未发现矛盾之处；

3） 列举产品支持的所有入侵分析方法。

8.3.1.1.3 入侵发现

入侵发现测试

a） 测试评价方法

1） 配置入侵防御产品的入侵防御策略为最大策略集；

2） 发送产品策略集中的攻击事件，查看是否能够发现攻击事件。

b） 测试评价结果

入侵防御产品应能发现所测入侵行为。

8.3.1.1.4 流量监测

流量监测测试：

a） 测试评价方法

1） 开启入侵防御产品的流量监测功能，定义流量事件，查看流量显示界面；

2） 对某一服务器发起大流量的访问，如 FTP；

3） 对特定的端口（如 80 端口）发起大流量访问。

b） 测试评价结果

1） 可以显示出各种异常流量信息；

2） 可以显示出大流量的服务器（如 FTP 流量）；

3） 列举提供的异常流量监测内容。

8.3.1.2 入侵响应功能测试

拦截能力测试：

a） 测试评价方法

1） 选择具有不同特征的多个事件组成攻击事件测试集（不少于产品支持的攻击事件库的30%），测试入侵防御产品的防御能力。选取的事件应包括木马后门类事件、拒绝服务类

事件、缓冲区溢出类事件以及其他具有代表性的网络攻击事件，模拟入侵攻击行为；

2） 配置入侵防御产品的入侵防御策略为最大策略集；

3） 发送攻击事件测试集中的所有事件，记录测试结果。

b） 测试评价结果

1） 能够对入侵行为进行成功拦截；

2） 应能记录所拦截入侵的相应攻击。

8.3.1.3 入侵事件审计功能测试

8.3.1.3.1 事件生成

事件生成测试：

a） 测试评价方法

1） 登录控制台界面；

2） 检查管理界面，是否可以实时、清晰地查看到入侵拦截情况。

b） 测试评价结果

1） 具有查看入侵拦截事件的显示界面；

2） 显示界面具备清晰的功能区域，可显示所拦截事件的详细信息。

8.3.1.3.2 事件记录

事件记录测试：

a） 测试评价方法

1） 登录控制台界面；

2） 在显示界面上查看所记录的拦截事件的详细信息。

b） 测试评价结果

显示界面上显示的拦截事件详细信息应包括事件名称、事件发生日期和时间、源 IP 地址、源端口、目的 IP 地址、目的端口、危害等级等。

8.3.1.4 管理控制功能测试

8.3.1.4.1 管理界面

管理界面测试：

a） 测试评价方法

1） 登录控制台管理界面；

2） 查看用户界面的功能，包括管理配置界面、告警显示界面等。

b） 测试评价结果

1） 具备独立的控制台；

2） 具有配置和管理产品所有功能的管理界面和划分清晰功能区域的告警显示界面。

8.3.1.4.2 入侵事件库

入侵事件库测试：

a） 测试评价方法

检查入侵防御产品是否对入侵事件进行系统陈述，对事件进行命名以及详细描述定义。

b） 测试评价结果

1） 入侵防御产品应对所有支持的入侵事件具有命名和详细的描述定义；

2） 详细描述为人理解，不产生歧义。

8.3.1.4.3 事件分级

事件分级测试：

a） 测试评价方法

检查入侵事件库中是否对每个事件都有分级信息。

b） 测试评价结果

事件库的所有事件都具有分级信息。

8.3.1.4.4 硬件失效处理

a） 测试评价方法

检查入侵防御产品具备何种硬件失效处理机制。

b） 测试评价结果

对于产品硬件失效时，应不影响网络的通畅。

8.3.1.4.5 策略配置

策略配置测试：

a） 测试评价方法

1） 登录产品管理界面，查看产品提供的默认策略；

2） 查看是否允许编辑或修改生成新的策略；

3） 查看是否可以编辑或修改各策略的响应措施。

b） 测试评价结果

1） 产品应提供默认的策略，并可以直接应用；

2） 应允许用户编辑策略；

3） 具有供用户编辑策略的向导功能；

4） 支持策略的导入、导出；

5） 应允许用户编辑策略的不同响应措施；

6） 记录产品提供的策略种类和名称。

8.3.1.4.6 产品升级

产品升级测试：

a） 测试评价方法

检查入侵特征库的升级方式。

b） 测试评价结果

1） 入侵特征库可以进行手动或自动的在线升级；

2） 升级的过程中入侵防御产品仍可以正常拦截事件。

8.3.1.4.7 管理接口独立

管理接口独立测试：

a） 测试评价方法

检查入侵防御产品是否配备进行产品管理和网络数据通讯拦截的物理接口。

b） 测试评价结果

产品的管理接口和网络数据通讯拦截接口是不同的接口，且均能正常工作。

8.3.2 产品自身安全测试

8.3.2.1 标识和鉴别

8.3.2.1.1 用户鉴别

用户鉴别测试：

a) 测试评价方法

登录入侵防御产品，检查是否在执行所有功能之前要求首先进行身份认证。

b) 测试评价结果

1) 在用户执行任何与安全功能相关的操作之前都应对用户进行鉴别；

2) 登录之前允许做的操作，应仅限于输入登录信息、查看登录帮助等操作；

3) 允许用户在登录后执行与其安全功能相关的各类操作时，不再重复认证。

8.3.2.1.2 鉴别失败的处理

鉴别失败的处理测试：

a) 测试评价方法

1) 检查入侵防御产品的安全功能是否可定义当用户鉴别尝试失败连续达到指定次数后，采取相应的措施；

2) 尝试多次失败的用户鉴别行为，检查到达指定的鉴别失败次数后，入侵防御产品是否采取了相应的措施。

b) 测试评价结果

1) 入侵防御产品应定义当用户鉴别尝试失败连续达到指定次数后，采取相应的措施；

2) 当用户鉴别尝试失败连续达到指定次数后，入侵防御产品应阻止用户进一步尝试(如锁定该用户或者登录 IP)。

8.3.2.1.3 鉴别数据保护

鉴别数据保护测试：

a) 测试评价方法

检查入侵防御产品是否仅允许指定的授权用户查阅或修改身份鉴别数据。

b) 测试评价结果

入侵防御产品应仅允许指定的授权用户查阅或修改身份鉴别数据。

8.3.2.2 用户管理

8.3.2.2.1 标识唯一性

标识唯一性测试：

a) 测试评价方法

检查入侵防御产品的安全功能是否保证所定义的用户标识全局唯一。

b) 测试评价结果

1) 入侵防御产品应允许定义多个用户；

2) 应保证每一个用户标识是全局唯一的，不允许一个用户标识用于多个用户。

8.3.2.2.2 用户属性定义

用户属性定义测试：

a) 测试评价方法

定义多个用户，检查输入的用户信息是否都能被保存。

b) 测试评价结果

入侵防御产品应为每一个用户保存其安全属性，包括用户标识、鉴别数据（如密码）、授权信息或用户组信息、其他安全属性等。输入的用户信息无丢失现象发生。

8.3.2.3 安全功能保护

8.3.2.3.1 安全数据管理

安全数据管理测试：

a) 测试评价方法

模拟授权与非授权用户访问事件数据，入侵防御产品安全功能是否仅允许授权用户访问事件数据。

b) 测试评价结果

入侵防御产品应限制对事件数据的访问。除了具有明确的访问权限的授权用户之外，入侵防御产品应禁止所有其他用户对事件数据的访问。

8.3.3 产品保证测试

8.3.3.1 配置管理

配置管理评价：

a) 测试评价方法

评价者应审查开发者提供的配置管理支持文件是否包含以下内容：

1) 版本号，要求开发者所使用的版本号与所应表示的产品样本应完全对应，没有歧义；

2) 配置项，要求配置项应有唯一的标识，从而对入侵防御产品的组成有更清楚的描述。

b) 测试评价结果

审查记录以及最后结果（符合/不符合），开发者应提供唯一版本号和配置项。

8.3.3.2 交付与运行

交付与运行评价：

a) 测试评价方法

评价者应审查开发者是否提供了文档说明入侵防御产品的安装、生成、启动和使用的过程。用户能够通过此文档了解安装、生成、启动和使用过程。

b) 测试评价结果

审查记录以及最后结果（符合/不符合）应符合测试评价方法要求。

8.3.3.3 安全功能开发

8.3.3.3.1 功能设计

功能设计评价：

a) 测试评价方法

评价者应审查开发者所提供的信息是否满足如下要求：

1) 功能设计应当使用非形式化风格来描述产品安全功能与其外部接口；

2) 功能设计应当是内在一致的；

3） 功能设计应当描述使用所有外部产品安全功能接口的目的与方法，适当的时候，要提供结果影响例外情况和出错信息的细节；

4） 功能设计应当完整地表示产品安全功能。

评价者应确认功能设计是否是入侵防御产品安全要求的精确和完整的示例。

b） 测试评价结果

审查记录以及最后结果（符合/不符合），评价者审查内容至少包括测试评价方法中的四个方面。开发者提供的内容应精确和完整。

8.3.3.3.2 表示对应性

表示对应性评价：

a） 测试评价方法

评价者应审查开发者是否在产品安全功能表示的所有相邻对之间提供对应性分析。其中，入侵防御产品各种安全功能表示（如入侵防御产品功能设计、高层设计、低层设计、实现表示）之间的对应性是所提供的抽象产品安全功能表示要求的精确而完整的示例。产品安全功能在功能设计中进行细化，并且较为抽象的产品安全功能表示的所有相关安全功能部分，在较具体的产品安全功能表示中进行细化。

b） 测试评价结果

审查记录以及最后结果（符合/不符合），评价者审查内容至少包括功能设计、高层设计、低层设计、实现表示这四项。开发者提供的内容应精确和完整，并互相对应。

8.3.3.4 指导性文档

8.3.3.4.1 管理员指南

管理员指南评价：

a） 测试评价方法

评价者应审查开发者是否提供了供授权管理员使用的管理员指南，并且此管理员指南是否包括如下内容：

1） 入侵防御产品可以使用的管理功能和接口；

2） 怎样安全地管理入侵防御产品；

3） 在安全处理环境中应进行控制的功能和权限；

4） 所有对与入侵防御产品的安全操作有关的用户行为的假设；

5） 所有受管理员控制的安全参数，如果可能，应指明安全值；

6） 每一种与管理功能有关的安全相关事件，包括对安全功能所控制的实体的安全特性进行的改变；

7） 所有与授权管理员有关的 IT 环境的安全要求。

b） 测试评价结果

审查记录以及最后结果（符合/不符合），评价者审查内容至少包括测试评价方法中的七方面。开发者提供的管理员指南应完整。

8.3.3.4.2 用户指南

用户指南评价：

a） 测试评价方法

评价者应审查开发者是否提供了供入侵防御产品用户使用的用户指南，并且此用户指南是否

包括如下内容：

1） 入侵防御产品的非管理用户可使用的安全功能和接口；

2） 入侵防御产品提供给用户的安全功能和接口的用法；

3） 用户可获取但应受安全处理环境控制的所有功能和权限；

4） 入侵防御产品安全操作中用户所应承担的职责；

5） 与用户有关的 IT 环境的所有安全要求。

b） 测试评价结果

审查记录以及最后结果(符合/不符合)，评价者审查内容至少包括测试评价方法中的五方面。开发者提供的用户指南应完整，并与为评价而提供的其他所有文件保持一致。

8.3.3.5 开发安全要求

开发安全要求评价：

a） 测试评价方法

评价者应审查开发者所提供的信息是否满足如下要求：

1） 开发人员的安全管理：开发人员的安全规章制度，开发人员的安全教育培训制度和记录；

2） 开发环境的安全管理：开发地点的出入口控制制度和记录，开发环境的温湿度要求和记录，开发环境的防火防盗措施和国家有关部门的许可文件，开发环境中所使用安全系统必须采用符合国家有关规定的系统并提供相应证明材料；

3） 开发设备的安全管理：开发设备的安全管理制度，包括开发主机使用管理和记录，设备的购置、修理、处置的制度和记录，上网管理，计算机病毒管理和记录等；

4） 开发过程和成果的安全管理：对入侵防御产品代码、文档、样机进行受控管理的制度和记录。

b） 测试评价结果

审查记录以及最后结果(符合/不符合)，评价者审查内容至少包括测试评价方法中的四方面。开发者提供文档应完整。

8.3.3.6 测试

8.3.3.6.1 范围

范围评价：

a） 测试评价方法

评价者应审查开发者提供的测试覆盖分析结果，是否表明了测试文档中所标识的测试与安全功能设计中所描述的安全功能是对应的。

b） 测试评价结果

审查记录以及最后结果(符合/不符合)，开发者提供的测试文档中所标识的测试与安全功能设计中所描述的安全功能应对应。

8.3.3.6.2 功能测试

功能测试评价：

a） 测试评价方法

1） 评价开发者提供的测试文档，是否包括测试计划、测试规程、预期的测试结果和实际测试结果；

2） 评价测试计划是否标识了要测试的安全功能，是否描述了测试的目标；

3） 评价测试规程是否标识了要执行的测试，是否描述了每个安全功能的测试概况（这些概况包括对其他测试结果的顺序依赖性）；

4） 评价期望的测试结果是否表明测试成功后的预期输出；

5） 评价实际测试结果是否表明每个被测试的安全功能能按照规定进行运作。

b） 测试评价结果

审查记录以及最后结果（符合/不符合），评价者审查内容至少包括测试评价方法中的五方面。开发者提供的内容应完整。

8.4 第二级

8.4.1 产品功能测试

8.4.1.1 入侵事件分析功能测试

8.4.1.1.1 数据收集

数据收集测试：

a） 测试评价方法

检测入侵防御产品是否能够以网桥或网关方式正确接入网络，具备实时收集流入受保护网段内的数据包的能力。

b） 测试评价结果

1） 入侵防御产品应能够以网桥或网关方式接入网络；

2） 入侵防御产品应能够获取足够的网络数据包以分析入侵事件。

8.4.1.1.2 协议分析

协议分析测试：

a） 测试评价方法

1） 查看入侵防御产品的安全策略配置文档，检查安全事件的描述是否具有协议类型等属性；

2） 检查产品说明书，查找关于协议分析方法的说明，按照系统所声明的协议分析类型，抽样生成协议事件，组成攻击事件测试集；

3） 配置产品的入侵防御策略为最大策略集；

4） 发送攻击事件测试集中的所有事件，记录产品的检测结果。

b） 测试评价结果

1） 记录产品拦截入侵的相应攻击名称和类型；

2） 产品说明书中声称能够监视的协议事件主要包括以下类型：ARP、ICMP、IP、TCP、UDP、RPC、HTTP、FTP、TFTP、SNMP、TELNET、DNS、SMTP、POP3、NETBIOS、NFS、SMB、MSN、P2P 等，抽样测试应未发现矛盾之处；

3） 列举产品支持的所有入侵分析方法。

8.4.1.1.3 入侵发现

入侵发现测试：

a） 测试评价方法

1） 配置入侵防御产品的入侵防御策略为最大策略集；

2） 发送产品策略集中的攻击事件，查看是否能够发现攻击事件。

b） 测试评价结果

入侵防御产品应能发现所测入侵行为。

8.4.1.1.4 入侵逃避发现

入侵逃避发现测试：

a) 测试评价方法

1) 利用入侵检测躲避工具进行攻击，测试入侵防御产品是否对入侵事件进行拦截；

2) 将入侵事件的协议端口进行重定位，检查入侵防御产品是否对入侵事件进行拦截。

b) 测试评价结果

1) 入侵防御产品能够拦截经过分片、乱序之后的入侵事件；

2) 入侵防御产品能够正确地拦截经过逃避处理的 HTTP 入侵事件；

3) 入侵防御产品能够对重定位协议端口之后的入侵事件进行拦截。

8.4.1.1.5 流量监测

流量监测测试：

a) 测试评价方法

1) 开启入侵防御产品的流量监测功能，定义流量事件，查看流量显示界面；

2) 对某一服务器发起大流量的访问，如 FTP；

3) 对特定的端口（如 80 端口）发起大流量访问。

b) 测试评价结果

1) 可以显示出各种异常流量信息；

2) 可以显示出大流量的服务器（如 FTP 流量）；

3) 列举提供的异常流量监测内容。

8.4.1.2 入侵响应功能测试

8.4.1.2.1 拦截能力

拦截能力测试：

a) 测试评价方法

1) 选择具有不同特征的多个事件组成攻击事件测试集（不少于产品支持的攻击事件库的 30%），测试入侵防御产品的防御能力。选取的事件应包括：木马后门类事件、拒绝服务类事件、缓冲区溢出类事件以及其他具有代表性的网络攻击事件，模拟入侵攻击行为；

2) 配置入侵防御产品的入侵防御策略为最大策略集；

3) 发送攻击事件测试集中的所有事件，记录测试结果。

b) 测试评价结果

1) 能够对入侵行为进行成功拦截；

2) 应能记录所拦截入侵的相应攻击。

8.4.1.2.2 安全告警

安全警告测试：

a) 测试评价方法

1) 从已有的事件库中选择具有不同特征的多个事件，组成攻击事件测试集，模拟入侵攻击行为；

2) 触发产品的入侵防御策略中特定的安全事件，查看是否有拦截告警信息；

3） 查看告警事件的信息。

b） 测试评价结果

1） 可以显示告警信息；

2） 事件的详细解释应能便于理解。

8.4.1.2.3 告警方式

告警方式测试：

a） 测试评价方法

1） 登录产品管理界面，查看产品告警方式的选择；

2） 依次选择各种告警方式，测试是否能够按照指定的方式告警。

b） 测试评价结果

可以采取屏幕实时提示、声音告警、SNMP trap 消息、E-mail 告警、运行指定应用程序等告警方式中的一种或多种。记录并列出所有告警方式。

8.4.1.2.4 事件合并

事件合并测试：

a） 测试评价方法

1） 连续触发同一条事件，查看告警显示的情况，是否能将同一事件进行合并显示；

2） 检测产品是否具有事件合并的能力，如只显示告警信息的事件名称、发生的次数、源 IP（目的是查看某一事件在这个 IP 上发生了多少次）。

b） 测试评价结果

产品可以根据需要进行同类告警事件的合并。

8.4.1.3 入侵事件审计功能测试

8.4.1.3.1 事件生成

事件生成测试：

a） 测试评价方法

1） 登录控制台界面；

2） 检查管理界面，是否可以实时、清晰地查看到入侵拦截情况。

b） 测试评价结果

1） 具有查看入侵拦截事件的显示界面；

2） 显示界面具备清晰的功能区域，可显示所拦截事件的详细信息。

8.4.1.3.2 事件记录

事件记录测试：

a） 测试评价方法

1） 登录控制台界面；

2） 在显示界面上查看所记录的拦截事件的详细信息。

b） 测试评价结果

界面上显示的拦截事件详细信息应包括事件名称、事件发生日期和时间、源 IP 地址、源端口、目的 IP 地址、目的端口、危害等级等。

8.4.1.3.3 报表生成

报表生成测试：

a) 测试评价方法

1) 查看报表生成功能，查看报表的生成方式；

2) 查看生成报表的内容。

b) 测试评价结果

1) 具有生成报表的功能；

2) 提供默认的模板以供快速生成报表；

3) 生成的报表宜包含表格形式、柱状图、饼图等，并宜生成日报、周报等汇总报表。

8.4.1.3.4 报表查阅

报表查阅测试：

a) 测试评价方法

检查入侵防御产品提供的查阅、浏览检测结果报表的功能。

b) 测试评价结果

1) 提供查阅、浏览检测结果报表的功能；

2) 可以根据事件名称、IP 地址、时间等条件进行查询。

8.4.1.3.5 报表输出

报表输出测试：

a) 测试评价方法

1) 检查管理员是否能够按照自己的要求修改和定制报表内容；

2) 检查入侵防御产品支持的报表输出格式。

b) 测试评价结果

1) 入侵防御产品应支持管理员按照自己的要求修改和定制报表内容；

2) 报表应可输出成方便用户阅读的格式，如 DOC、PDF、HTML、XLS 等。

8.4.1.4 管理控制功能测试

8.4.1.4.1 管理界面

管理界面测试：

a) 测试评价方法

1) 登录控制台管理界面；

2) 查看用户界面的功能，包括管理配置界面、告警显示界面等。

b) 测试评价结果

1) 具备独立的控制台；

2) 具有配置和管理产品所有功能的管理界面和划分清晰功能区域的告警显示界面。

8.4.1.4.2 入侵事件库

入侵事件库测试：

a) 测试评价方法

检查入侵防御产品是否对入侵事件进行系统陈述，对事件进行命名以及详细描述定义。

b） 测试评价结果

1） 入侵防御产品应对所有支持的入侵事件具有命名和详细的描述定义；

2） 详细描述为人理解，不产生歧义。

8.4.1.4.3 事件分级

事件分级测试：

a） 测试评价方法

检查入侵事件库中是否对每个事件都有分级信息。

b） 测试评价结果

事件库的所有事件都具有分级信息。

8.4.1.4.4 事件定义

事件定义测试：

a） 测试评价方法

1） 查看入侵防御产品设置，是否提供自定义事件界面，是否允许基于产品默认事件修改生成新的事件；

2） 自定义生成新的入侵特征；

3） 按照新生成的入侵特征发送相应的入侵事件，检查产品能否拦截。

b） 测试评价结果

1） 入侵防御产品允许用户自定义事件，或者可基于产品默认事件修改生成新的入侵事件；

2） 入侵防御产品能够检测到新定义的事件并拦截。

8.4.1.4.5 协议定义

协议定义测试：

a） 测试评价方法

1） 查看入侵防御产品设置，是否提供自定义协议的界面，是否允许基于已有协议修改生成新的协议，是否允许对协议的端口进行重新定位拦截；

2） 自定义生成新的协议；

3） 按照新生成的协议类型发送相应的入侵事件，检查产品能否拦截。

b） 测试评价结果

1） 入侵防御产品允许用户自定义协议，或者可基于产品提供的已有协议修改生成新的协议，或者允许对协议的端口进行重新定位；

2） 入侵防御产品能够检测到新定义的协议事件并拦截。

8.4.1.4.6 流量控制

流量控制测试：

a） 测试评价方法

1） 开启入侵防御产品的流量控制功能；

2） 对某一服务器发起大流量的访问，如 P2P。

b） 测试评价结果

入侵防御产品允许针对异常流量实现流量控制功能。

8.4.1.4.7 硬件失效处理

硬件失效处理测试：

a） 测试评价方法

检查入侵防御产品具备何种硬件失效处理机制。

b） 测试评价结果

对于产品硬件失效时，应不影响网络的通畅。

8.4.1.4.8 策略配置

策略配置测试：

a） 测试评价方法

1） 打开菜单，查看产品提供的默认策略；查看是否允许编辑或修改生成新的策略；

2） 查看是否可以编辑或修改各策略的响应措施。

b） 测试评价结果

1） 产品应提供默认的策略，并可以直接应用；

2） 应允许用户编辑策略；

3） 具有供用户编辑策略的向导功能；

4） 支持策略的导入、导出；

5） 应允许用户编辑策略的不同响应措施；

6） 记录产品提供的策略种类和名称。

8.4.1.4.9 产品升级

产品升级测试：

a） 测试评价方法

检查入侵防御产品的版本和入侵特征库的升级方式。

b） 测试评价结果

1） 入侵防御产品程序版本和入侵特征库可以进行手动或自动的在线升级；

2） 升级的过程中入侵防御产品仍可以正常拦截事件。

8.4.1.4.10 管理接口独立

管理接口独立测试：

a） 测试评价方法

检查入侵防御产品是否配备进行产品管理和网络数据通讯拦截的物理接口。

b） 测试评价结果

产品的管理接口和网络数据通讯拦截接口是不同的接口，且均能正常工作。

8.4.2 产品自身安全测试

8.4.2.1 标识和鉴别

8.4.2.1.1 用户鉴别

用户鉴别测试：

a） 测试评价方法

登录入侵防御产品，检查是否在执行所有功能之前要求首先进行身份认证。

b） 测试评价结果

1） 在用户执行任何与安全功能相关的操作之前都应对用户进行鉴别；

2） 登录之前允许做的操作，应仅限于输入登录信息、查看登录帮助等操作；

3） 允许用户在登录后执行与其安全功能相关的各类操作时，不再重复认证。

8.4.2.1.2 鉴别失败的处理

鉴别失败的处理测试：

a） 测试评价方法

1） 检查入侵防御产品的安全功能是否可定义用户鉴别尝试的最大允许失败次数；

2） 检查产品的安全功能是否可定义当用户鉴别尝试失败连续达到指定次数后，采取相应的措施；

3） 尝试多次失败的用户鉴别行为，检查到达指定的鉴别失败次数后，入侵防御产品是否采取了相应的措施。

4） 检查日志记录中是否包括用户或者登录 IP 被锁定等鉴别失败处理措施的审计信息。

b） 测试评价结果

1） 入侵防御产品应具备定义用户鉴别尝试的最大允许失败次数的功能；

2） 入侵防御产品应定义当用户鉴别尝试失败连续达到指定次数后，采取相应的措施；

3） 当用户鉴别尝试失败连续达到指定次数后，入侵防御产品应阻止用户进一步尝试（如锁定该用户或者登录 IP）。

4） 最多失败次数仅由授权管理员设定，日志记录中应包括鉴别失败处理措施的审计信息。

8.4.2.1.3 鉴别数据保护

鉴别数据保护测试：

a） 测试评价方法

检查入侵防御产品是否仅允许指定的授权用户查阅或修改身份鉴别数据。

b） 测试评价结果

入侵防御产品应仅允许指定的授权用户查阅或修改身份鉴别数据。

8.4.2.1.4 超时锁定

超时锁定测试：

a） 测试评价方法

1） 检查入侵防御产品是否具有管理员登录超时重新鉴别功能；

2） 设定管理员登录超时重新鉴别的时间段，检查登录用户在设定的时间段内没有任何操作的情况下，入侵防御产品是否终止了会话，用户是否需要再次进行身份鉴别才能够重新管理和使用产品。

b） 测试评价结果

1） 入侵防御产品应具有登录超时重新鉴别功能；

2） 任何登录用户在设定的时间段内没有任何操作的情况下，应被终止了会话，用户需要再次进行身份鉴别才能够重新管理和使用入侵防御产品；

3） 最大超时时间仅由授权管理员设定。

8.4.2.2 用户管理

8.4.2.2.1 标识唯一性

标识唯一性测试：

a） 测试评价方法

检查入侵防御产品的安全功能是否保证所定义的用户标识全局唯一。

b) 测试评价结果

1) 入侵防御产品应允许定义多个用户；

2) 应保证每一个用户标识是全局唯一的，不允许一个用户标识用于多个用户。

8.4.2.2.2 用户属性定义

用户属性定义测试：

a) 测试评价方法

定义多个用户，检查输入的用户信息是否都能被保存。

b) 测试评价结果

入侵防御产品应为每一个用户保存其安全属性，包括用户标识、鉴别数据（如密码）、授权信息或用户组信息、其他安全属性等。输入的用户信息无丢失现象发生。

8.4.2.2.3 角色分级

角色分级测试：

a) 测试评价方法

1) 设置多个不同级别角色的用户，进行不同级别内容的操作请求；

2) 检查入侵防御产品的安全功能是否提供角色分级的用户。

b) 测试评价结果

入侵防御产品应提供分级角色的用户，分级角色覆盖范围互不相同。

8.4.2.3 安全功能保护

8.4.2.3.1 安全数据管理

安全数据管理测试：

a) 测试评价方法

模拟授权与非授权用户访问事件数据，入侵防御产品安全功能是否仅允许授权用户访问事件数据。

b) 测试评价结果

入侵防御产品应限制对事件数据的访问。除了具有明确的访问权限的授权用户之外，入侵防御产品应禁止所有其他用户对事件数据的访问。

8.4.2.3.2 数据存储告警

数据存储告警测试：

a) 测试评价方法

1) 检查入侵防御产品安全功能是否具有存储器剩余空间将耗尽的告警功能；

2) 人为地将存储产品的事件数据存储器空间耗至产品默认的告警值以下，查看入侵防御产品是否告警，查看入侵防御产品是否提供防止事件记录丢失的措施。

b) 测试评价结果

1) 入侵防御产品在发生事件数据存储器空间将耗尽的情况时，自动产生告警；

2) 在发现事件数据存储器空间将耗尽时，入侵防御产品还应提醒用户采取措施避免事件丢失，可选择例如转存已有事件数据、仅记录重要的事件数据、或者不记录新的事件数据等措施之一。

8.4.2.4 安全审计

8.4.2.4.1 审计数据生成

审计数据生成测试：

a) 测试评价方法

结合开发者文档，使用不同角色用户模拟对入侵防御产品不同模块进行访问、运行、修改、关闭以及重复失败尝试等相关操作，检查入侵防御产品提供了对哪些事件的审计。审查审计记录的正确性。

b) 测试评价结果

1) 入侵防御产品应至少为下述可审计事件产生审计记录：身份鉴别的尝试、安全策略更改的操作、修改安全属性的尝试；

2) 应在每个审计记录中至少记录如下信息：事件的日期和时间、事件类型、主体身份、事件的结果(成功或失败)等。

8.4.2.4.2 审计查阅

审计查阅测试：

a) 测试评价方法

审查产品安全功能是否为授权管理员提供从审计记录中读取全部审计信息的功能，是否能对审计记录进行排序。

b) 测试评价结果

入侵防御产品应为授权管理员提供从审计记录中读取全部审计信息的功能，并可以对审计记录进行排序。

8.4.2.4.3 受限的审计查阅

受限的审计查阅测试：

a) 测试评价方法

模拟授权与非授权管理员访问审计记录，入侵防御产品安全功能是否仅允许授权管理员访问审计记录。

b) 测试评价结果

入侵防御产品应限制审计记录的访问。除了具有明确的读访问权限的授权管理员之外，入侵防御产品应禁止所有其他用户对审计记录的读访问。

8.4.3 产品保证测试

8.4.3.1 配置管理

8.4.3.1.1 配置管理能力

配置管理能力评价：

a) 测试评价方法

评价者应审查开发者所提供的文档是否包含以下内容：

1) 开发者应使用配置管理系统并提供配置管理文档，以及为入侵防御产品的不同版本提供唯一的标识。

2) 配置管理系统应对所有的配置项作出唯一的标识，并保证只有经过授权才能修改配置项。

3） 配置管理文档应包括配置清单、配置管理计划。配置清单用来描述组成入侵防御产品的配置项。在配置管理计划中，应描述配置管理系统是如何使用的。实施的配置管理应与配置管理计划相一致。

4） 配置管理文档还应描述对配置项给出唯一标识的方法，并提供所有的配置项得到有效的维护的证据。

b） 测试评价结果

审查记录以及最后结果（符合/不符合），评价者审查内容至少包括测试评价方法中的四方面。开发者提供的配置管理内容应完整。

8.4.3.1.2 配置管理范围

配置管理范围评价：

a） 测试评价方法

评价者应审查开发者提供的配置管理支持文件是否包含配置管理范围，要求将入侵防御产品的实现表示、设计文档、测试文档、用户文档、管理员文档、配置管理文档等置于配置管理之下，从而确保它们的修改是在一个正确授权的可控方式下进行的。评价者应审查开发者交付的文档是否包含以下内容：

1） 开发者所提供的配置管理文档应展示配置管理系统至少能跟踪上述配置管理之下的内容；

2） 文档应描述配置管理系统是如何跟踪这些配置项的；

3） 文档还应提供足够的信息表明达到所有要求。

b） 测试评价结果

审查记录以及最后结果（符合/不符合）符合测试评价方法要求，评价者测试和审查内容至少包括测试评价方法中的三方面。

8.4.3.2 交付与运行

8.4.3.2.1 交付

交付评价：

a） 测试评价方法

评价者应审查开发者是否使用一定的交付程序交付入侵防御产品，并使用文档描述交付过程，并且评价者应审查开发者交付的文档是否包含在给用户方交付入侵防御产品的各版本时，为维护安全所必需的所有程序。

b） 测试评价结果

测试记录以及最后结果（符合/不符合）应符合测试评价方法要求，开发者应提供完整的文档描述所有交付的过程（文档和程序交付）。

8.4.3.2.2 安装生成

安装生成评价：

a） 测试评价方法

评价者应审查开发者是否提供了文档说明入侵防御产品的安装、生成、启动和使用的过程。用户能够通过此文档了解安装、生成、启动和使用过程。

b） 测试评价结果

审查记录以及最后结果（符合/不符合）应符合测试评价方法要求。

8.4.3.3 安全功能开发

8.4.3.3.1 功能设计

功能设计评价：

a) 测试评价方法

评价者应审查开发者所提供的信息是否满足如下要求：

1) 功能设计应当使用非形式化风格来描述产品安全功能与其外部接口；
2) 功能设计应当是内在一致的；
3) 功能设计应当描述使用所有外部产品安全功能接口的目的与方法，适当的时候，要提供结果影响例外情况和出错信息的细节；
4) 功能设计应当完整地表示产品安全功能。

评价者应确认功能设计是否是入侵防御产品安全要求的精确和完整的示例。

b) 测试评价结果

审查记录以及最后结果(符合/不符合)，评价者审查内容至少包括测试评价方法中的四个方面。开发者提供的内容应精确和完整。

8.4.3.3.2 高层设计

高层设计评价：

a) 测试评价方法

评价者应审查开发者所提供的信息是否满足如下要求：

1) 高层设计应采用非形式化的表示；
2) 高层设计应当是内在一致的；
3) 入侵防御产品高层设计应当描述每一个安全功能子系统所提供的安全功能，提供了适当的体系结构来实现入侵防御产品安全要求；
4) 入侵防御产品的高层设计应当以子系统的观点来描述产品安全功能的结构，定义所有子系统之间的相互关系，并把这些相互关系适当地作为数据流、控制流等的外部接口来表示；
5) 高层设计应当标识入侵防御产品安全要求的任何基础性的硬件、固件和/或软件，并且通过支持这些硬件、固件或软件所实现的保护机制，来提供产品安全功能表示。

b) 测试评价结果

审查记录以及最后结果(符合/不符合)，评价者审查内容至少包括测试评价方法中的五个方面。开发者提供的高层设计内容应精确和完整。

8.4.3.3.3 表示对应性

表示对应性评价：

a) 测试评价方法

评价者应审查开发者是否在产品安全功能表示的所有相邻对之间提供对应性分析。其中，入侵防御产品各种安全功能表示(如入侵防御产品功能设计、高层设计、低层设计、实现表示)之间的对应性是所提供的抽象产品安全功能表示要求的精确而完整的示例。产品安全功能在功能设计中进行细化，并且较为抽象的产品安全功能表示的所有相关安全功能部分，在较具体的产品安全功能表示中进行细化。

b) 测试评价结果

测试记录以及最后结果(符合/不符合),评价者审查内容至少包括功能设计、高层设计、低层设计、实现表示这四项。开发者提供的内容应精确和完整,并互相对应。

8.4.3.4 指导性文档

8.4.3.4.1 管理员指南

管理员指南评价:

a) 测试评价方法

评价者应审查开发者是否提供了供授权管理员使用的管理员指南,并且此管理员指南是否包括如下内容:

1) 入侵防御产品可以使用的管理功能和接口;
2) 怎样安全地管理入侵防御产品;
3) 在安全处理环境中应进行控制的功能和权限;
4) 所有对与入侵防御产品的安全操作有关的用户行为的假设;
5) 所有受管理员控制的安全参数,如果可能,应指明安全值;
6) 每一种与管理功能有关的安全相关事件,包括对安全功能所控制的实体的安全特性进行的改变;
7) 所有与授权管理员有关的 IT 环境的安全要求。

b) 测试评价结果

测试记录以及最后结果(符合/不符合),评价者审查内容至少包括测试评价方法中的七方面。开发者提供的管理员指南应完整。

8.4.3.4.2 用户指南

用户指南评价:

a) 测试评价方法

评价者应审查开发者是否提供了供入侵防御产品用户使用的用户指南,并且此用户指南是否包括如下内容:

1) 入侵防御产品的非管理用户可使用的安全功能和接口;
2) 入侵防御产品提供给用户的安全功能和接口的用法;
3) 用户可获取但应受安全处理环境控制的所有功能和权限;
4) 入侵防御产品安全操作中用户所应承担的职责;
5) 与用户有关的 IT 环境的所有安全要求。

b) 测试评价结果

测试记录以及最后结果(符合/不符合),评价者审查内容至少包括测试评价方法中的五方面。开发者提供的用户指南应完整,并与为评价而提供的其他所有文件保持一致。

8.4.3.5 开发安全要求

开发安全要求评价:

a) 测试评价方法

评价者应审查开发者所提供的信息是否满足如下要求:

1) 开发人员的安全管理:开发人员的安全规章制度,开发人员的安全教育培训制度和记录;
2) 开发环境的安全管理:开发地点的出入口控制制度和记录,开发环境的温湿度要求和记录,开发环境的防火防盗措施和国家有关部门的许可文件,开发环境中所使用安全系统必

须采用符合国家有关规定的系统并提供相应证明材料；

3） 开发设备的安全管理：开发设备的安全管理制度，包括开发主机使用管理和记录，设备的购置、修理、处置的制度和记录，上网管理，计算机病毒管理和记录等；

4） 开发过程和成果的安全管理：对入侵防御产品代码、文档、样机进行受控管理的制度和记录。

b） 测试评价结果

测试记录以及最后结果（符合/不符合），评价者审查内容至少包括测试评价方法中的四方面。开发者提供文档应完整。

8.4.3.6 测试

8.4.3.6.1 范围

范围评价：

a） 测试评价方法

1） 评价者应审查开发者提供的测试覆盖分析结果，是否表明了测试文档中所标识的测试与安全功能设计中所描述的安全功能是对应的；

2） 评价测试文档中所标识的测试，是否完整。

b） 测试评价结果

审查记录以及最后结果（符合/不符合），开发者提供的测试文档中所标识的测试与安全功能设计中所描述的安全功能应对应，并且标识的测试应覆盖所有安全功能。

8.4.3.6.2 测试深度

测试深度评价：

a） 测试评价方法

评价开发者提供的测试深度分析，是否说明了测试文档中所标识的对安全功能的测试，足以表明该安全功能和高层设计是一致的。

b） 测试评价结果

测试记录以及最后结果（符合/不符合），评价者测试和审查与安全功能相对应的测试，这些测试应能正确保证测试出的安全功能符合高层设计的要求。

8.4.3.6.3 功能测试

功能测试评价：

a） 测试评价方法

1） 评价开发者提供的测试文档，是否包括测试计划、测试规程、预期的测试结果和实际测试结果；

2） 评价测试计划是否标识了要测试的安全功能，是否描述了测试的目标；

3） 评价测试规程是否标识了要执行的测试，是否描述了每个安全功能的测试概况（这些概况包括对其他测试结果的顺序依赖性）；

4） 评价期望的测试结果是否表明测试成功后的预期输出；

5） 评价实际测试结果是否表明每个被测试的安全功能能按照规定进行运作。

b） 测试评价结果

测试记录以及最后结果（符合/不符合），评价者审查内容至少包括测试评价方法中的五方面。开发者提供的内容应完整。

8.4.3.6.4 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入侵防御产品，且提供的入侵防御产品是否适合测试。

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入侵防御产品。

8.4.3.7 脆弱性评定

8.4.3.7.1 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入侵防御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。

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。

8.4.3.7.2 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，对入侵防御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，评价是否能够显示在使用入侵防御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。

8.5 第三级

8.5.1 产品功能测试

8.5.1.1 入侵事件分析功能测试

8.5.1.1.1 数据收集

数据收集测试：

a) 测试评价方法

检测入侵防御产品是否能够以网桥或网关方式正确接入网络，具备实时收集流入受保护网段

内的数据包的能力。

b） 测试评价结果

1） 入侵防御产品应能够以网桥或网关方式接入网络；

2） 入侵防御产品应能够获取足够的网络数据包以分析入侵事件。

8.5.1.1.2 协议分析

协议分析测试：

a） 测试评价方法

1） 查看入侵防御产品的安全策略配置文档，检查安全事件的描述是否具有协议类型等属性；

2） 检查产品说明书，查找关于协议分析方法的说明，按照产品所声明的协议分析类型，抽样生成协议事件，组成攻击事件测试集；

3） 配置产品的入侵防御策略为最大策略集；

4） 发送攻击事件测试集中的所有事件，记录产品的检测结果。

b） 测试评价结果

1） 记录产品拦截入侵的相应攻击名称和类型；

2） 产品说明书中声称能够监视的协议事件主要包括以下类型：ARP、ICMP、IP、TCP、UDP、RPC、HTTP、FTP、TFTP、SNMP、TELNET、DNS、SMTP、POP3、NETBIOS、NFS、SMB、MSN、P2P 等，抽样测试应未发现矛盾之处；

3） 列举产品支持的所有入侵分析方法。

8.5.1.1.3 入侵发现

入侵发现测试：

a） 测试评价方法

1） 配置入侵防御产品的入侵防御策略为最大策略集；

2） 发送产品策略集中的攻击事件，查看是否能够发现攻击事件。

b） 测试评价结果

入侵防御产品应能发现所测入侵行为。

8.5.1.1.4 入侵逃避发现

入侵逃避发现测试：

a） 测试评价方法

1） 利用入侵检测躲避工具进行攻击，测试入侵防御产品是否对入侵事件进行拦截；

2） 将入侵事件的协议端口进行重定位，检查入侵防御产品是否对入侵事件进行拦截。

b） 测试评价结果

1） 入侵防御产品能够拦截经过分片、乱序之后的入侵事件；

2） 入侵防御产品能够正确地拦截经过逃避处理的 HTTP 入侵事件；

3） 入侵防御产品能够对重定位协议端口之后的入侵事件进行拦截。

8.5.1.1.5 流量监测

流量监测测试：

a） 测试评价方法

1） 开启入侵防御产品的流量监测功能，定义流量事件，查看流量显示界面；

2） 对某一服务器发起大流量的访问，如 FTP；

3） 对特定的端口(如 80 端口)发起大流量访问。

b） 测试评价结果

1） 可以显示出各种异常流量信息；

2） 可以显示出大流量的服务器(如 FTP 流量)；

3） 列举提供的异常流量监测内容。

8.5.1.2 入侵响应功能测试

8.5.1.2.1 拦截能力

拦截能力测试：

a） 测试评价方法

1） 选择具有不同特征的多个事件组成攻击事件测试集(不少于产品支持的攻击事件库的 30%)，测试入侵防御产品的防御能力。选取的事件应包括：木马后门类事件、拒绝服务类事件、缓冲区溢出类事件以及其他具有代表性的网络攻击事件，模拟入侵攻击行为；

2） 配置入侵防御产品的入侵防御策略为最大策略集；

3） 发送攻击事件测试集中的所有事件，记录测试结果。

b） 测试评价结果

1） 能够对入侵行为进行成功拦截；

2） 应能记录所拦截入侵的相应攻击。

8.5.1.2.2 安全告警

安全告警测试：

a） 测试评价方法

1） 从已有的事件库中选择具有不同特征的多个事件，组成攻击事件测试集。模拟入侵攻击行为；

2） 触发产品的入侵防御策略中特定的安全事件，查看是否有拦截告警信息；

3） 查看告警事件的信息。

b） 测试评价结果

1） 可以显示告警信息；

2） 事件的详细解释应能便于理解。

8.5.1.2.3 告警方式

告警方式测试：

a） 测试评价方法

1） 打开菜单，查看产品告警方式的选择；

2） 依次选择各种告警方式，测试是否能够按照指定的方法告警。

b） 测试评价结果

可以采取屏幕实时提示、声音告警、SNMP trap 消息、E-mail 告警、运行指定应用程序等告警方式中的一种或多种。记录并列出所有告警方式。

8.5.1.2.4 事件合并

事件合并测试：

a） 测试评价方法

1） 连续触发同一条事件，查看告警显示的情况，是否能将同一事件进行合并显示；
2） 设置事件合并的规则，将某些内容进行合并，如只显示告警信息的事件名称、发生的次数、源 IP(目的是查看某一事件在这个 IP 上发生了多少次)。

b） 测试评价结果
产品可以根据需要进行同类告警事件的合并。

8.5.1.3 入侵事件审计功能测试

8.5.1.3.1 事件生成

事件生成测试：

a） 测试评价方法
1） 登录控制台界面；
2） 检查管理界面，是否可以实时、清晰地查看到入侵拦截情况。

b） 测试评价结果
1） 具有查看入侵拦截事件的显示界面；
2） 显示界面具备清晰的功能区域，可显示所拦截事件的详细信息。

8.5.1.3.2 事件记录

事件记录测试：

a） 测试评价方法
1） 登录控制台界面；
2） 在显示界面上查看所记录的拦截事件的详细信息。

b） 测试评价结果
显示界面上显示的拦截事件详细信息应包括事件名称、事件发生日期和时间、源 IP 地址、源端口、目的 IP 地址、目的端口、危害等级等。

8.5.1.3.3 报表生成

报表生成测试：

a） 测试评价方法
1） 查看报表生成功能，查看报表的生成方式；
2） 查看生成报表的内容。

b） 测试评价结果
1） 具有生成报表的功能；
2） 提供默认的模板以供快速生成报表；
3） 生成的报表宜包含表格形式、柱状图、饼图等，并宜生成日报、周报等汇总报表。

8.5.1.3.4 报表查阅

报表查阅测试：

a） 测试评价方法
检查入侵防御产品提供的查阅、浏览检测结果报表的功能。

b） 测试评价结果
1） 提供查阅、浏览检测结果报表的功能；
2） 可以根据事件名称、IP 地址、时间等条件进行查询。

8.5.1.3.5 报表输出

报表输出测试：

a) 测试评价方法

1) 检查管理员是否能够按照自己的要求修改和定制报表内容；

2) 检查入侵防御产品支持的报表输出格式。

b) 测试评价结果

1) 入侵防御产品应支持管理员按照自己的要求修改和定制报表内容；

2) 报表应可输出成方便用户阅读的格式，如 DOC、PDF、HTML、XLS 等。

8.5.1.3.6 报表模板的定制

报表模板的定制测试：

a) 测试评价方法

检查入侵防御产品是否提供报表模板的定制功能。

b) 测试评价结果

1) 入侵防御产品提供定制报表模板的功能；

2) 定制新的报表模板，按照新的报表模板生成结果报表。

8.5.1.4 管理控制功能测试

8.5.1.4.1 管理界面

管理界面测试：

a) 测试评价方法

1) 登录控制台管理界面；

2) 查看用户界面的功能，包括管理配置界面、告警显示界面等。

b) 测试评价结果

1) 具备独立的控制台；

2) 具有配置和管理产品所有功能的管理界面和划分清晰功能区域的告警显示界面。

8.5.1.4.2 入侵事件库

入侵事件库测试：

a) 测试评价方法

检查入侵防御产品是否对入侵事件进行系统陈述，对事件进行命名以及详细描述定义。

b) 测试评价结果

1) 入侵防御产品应对所有支持的入侵事件具有命名和详细的描述定义；

2) 详细描述为人理解，不产生歧义。

8.5.1.4.3 事件分级

事件分级测试：

a) 测试评价方法

检查入侵事件库中是否对每个事件都有分级信息。

b) 测试评价结果

事件库的所有事件都具有分级信息。

8.5.1.4.4 事件定义

事件定义测试：

a) 测试评价方法

1) 查看入侵防御产品设置，是否提供自定义事件界面，是否允许基于产品默认事件修改生成新的事件；

2) 自定义生成新的入侵特征；

3) 按照新生成的入侵特征发送相应的入侵事件，检查产品能否拦截。

b) 测试评价结果

1) 入侵防御产品允许用户自定义事件，或者可基于产品默认事件修改生成新的入侵事件；

2) 入侵防御产品能够检测到新定义的事件并拦截。

8.5.1.4.5 协议定义

协议定义测试：

a) 测试评价方法

1) 查看入侵防御产品设置，是否提供自定义协议的界面，是否允许基于已有协议修改生成新的协议，是否允许对协议的端口进行重新定位拦截；

2) 自定义生成新的协议；

3) 按照新生成的协议类型发送相应的入侵事件，检查产品能否拦截。

b) 测试评价结果

1) 入侵防御产品允许用户自定义协议，或者可基于产品提供的已有协议修改生成新的协议，或者允许对协议的端口进行重新定位；

2) 入侵防御产品能够检测到新定义的协议事件并拦截。

8.5.1.4.6 流量控制

流量控制测试：

a) 测试评价方法

1) 开启入侵防御产品的流量控制功能；

2) 对某一服务器发起大流量的访问，如 P2P。

b) 测试评价结果

入侵防御产品允许针对异常流量实现流量控制功能。

8.5.1.4.7 通用接口

通用接口测试：

a) 测试评价方法

1) 查看入侵防御产品，是否支持与其他安全设备的信息共享或者规范化管理；

2) 可提供产品自己定义的对外开放通用接口，以支持与其他安全设备的共享信息或规范化管理。

b) 测试评价结果

1) 入侵防御产品支持一个或多个信息共享或规范化管理接口协议，其中可包括产品自己定义的对外通用接口；

2) 入侵防御产品支持与其他安全设备的共享信息或规范化管理；

3) 列举入侵防御产品支持的所有通用接口。

8.5.1.4.8 硬件失效处理

硬件实效处理测试：

a) 测试评价方法

1) 检查入侵防御产品具备何种硬件失效处理机制；

2) 部署双机热备的环境，关闭其中一台设备，查看另一设备是否可以及时工作。

b) 测试评价结果

1) 对于产品硬件失效时，应不影响网络的通畅；

2) 对于双机热备进行部署的环境，当出现一台设备宕机的情况，应不影响网络的通畅和防御能力。

8.5.1.4.9 负载均衡

负载均衡测试：

a) 测试评价方法

1) 设置入侵防御产品负载均衡策略；

2) 使用协议分析仪，检查网络流量是否达到负载均衡效果。

b) 测试评价结果

入侵防御产品应能实现网络流量的负载均衡。

8.5.1.4.10 策略配置

策略配置测试：

a) 测试评价方法

1) 打开菜单，查看产品提供的默认策略；

2) 查看是否允许编辑或修改生成新的策略；

3) 查看是否可以编辑或修改各策略的响应措施。

b) 测试评价结果

1) 产品应提供默认的策略，并可以直接应用；

2) 应允许用户编辑策略；

3) 具有供用户编辑策略的向导功能；

4) 支持策略的导入、导出；

5) 应允许用户编辑策略的不同响应措施；

6) 记录产品提供的策略种类和名称。

8.5.1.4.11 产品升级

产品升级测试：

a) 测试评价方法

检查入侵防御产品的版本和入侵特征库的升级方式。

b) 测试评价结果

1) 入侵防御产品程序版本和入侵特征库可以进行手动或自动的在线升级；

2) 升级的过程中入侵防御产品仍可以正常拦截事件。

8.5.1.4.12 管理接口独立

管理接口独立测试：

a） 测试评价方法

检查入侵防御产品是否配备进行产品管理和网络数据通讯拦截的物理接口。

b） 测试评价结果

产品的管理接口和网络数据通讯拦截接口是不同的接口，且均能正常工作。

8.5.2 产品自身安全测试

8.5.2.1 标识和鉴别

8.5.2.1.1 用户鉴别

用户鉴别测试：

a） 测试评价方法

登录入侵防御产品，检查是否在执行所有功能之前要求首先进行身份认证。

b） 测试评价结果

1） 在用户执行任何与安全功能相关的操作之前都应对用户进行鉴别；

2） 登录之前允许做的操作，应仅限于输入登录信息、查看登录帮助等操作；

3） 允许用户在登录后执行与其安全功能相关的各类操作时，不再重复认证。

8.5.2.1.2 鉴别失败的处理

鉴别失败的处理测试：

a） 测试评价方法

1） 检查入侵防御产品的安全功能是否可定义用户鉴别尝试的最大允许失败次数；

2） 检查产品的安全功能是否可定义当用户鉴别尝试失败连续达到指定次数后，采取相应的措施；

3） 尝试多次失败的用户鉴别行为，检查到达指定的鉴别失败次数后，入侵防御产品是否采取了相应的措施；

4） 检查日志记录中是否包括用户或者登录 IP 被锁定等鉴别失败处理措施的审计信息。

b） 测试评价结果

1） 入侵防御产品应具备定义用户鉴别尝试的最大允许失败次数的功能；

2） 入侵防御产品应定义当用户鉴别尝试失败连续达到指定次数后，采取相应的措施；

3） 当用户鉴别尝试失败连续达到指定次数后，入侵防御产品应阻止用户进一步尝试（如锁定该用户或者登录 IP）；

4） 最多失败次数仅由授权管理员设定，日志记录中应包括鉴别失败处理措施的审计信息。

8.5.2.1.3 鉴别数据保护

鉴别数据保护测试：

a） 测试评价方法

检查入侵防御产品是否仅允许指定的授权用户查阅或修改身份鉴别数据。

b） 测试评价结果

入侵防御产品应仅允许指定的授权用户查阅或修改身份鉴别数据。

8.5.2.1.4 超时锁定

超时锁定测试：

a） 测试评价方法

1） 检查入侵防御产品是否具有管理员登录超时重新鉴别功能；
2） 设定管理员登录超时重新鉴别的时间段，检查登录用户在设定的时间段内没有任何操作的情况下，入侵防御产品是否终止了会话，用户是否需要再次进行身份鉴别才能够重新管理和使用产品。

b） 测试评价结果
1） 入侵防御产品应具有登录超时重新鉴别功能；
2） 任何登录用户在设定的时间段内没有任何操作的情况下，应被终止了会话，用户需要再次进行身份鉴别才能够重新管理和使用入侵防御产品；
3） 最大超时时间仅由授权管理员设定。

8.5.2.1.5 多鉴别机制

多鉴别机制测试：

a） 测试评价方法
1） 检查入侵防御产品的安全功能是否提供多种鉴别方式；
2） 检查入侵防御产品是否提供允许授权管理员执行自定义鉴别措施的功能；
3） 检查多鉴别机制是否可同时使用。

b） 测试评价结果
1） 入侵防御产品应提供至少 2 种鉴别方式，列举入侵防御产品提供或支持的所有鉴别方式；
2） 入侵防御产品应允许授权管理员执行自定义的鉴别措施，以实现多重身份鉴别措施；
3） 多鉴别机制应该能够同时使用。

8.5.2.2 用户管理

8.5.2.2.1 标识唯一性

标识唯一性测试：

a） 测试评价方法
检查入侵防御产品的安全功能是否保证所定义的用户标识全局唯一。

b） 测试评价结果
1） 入侵防御产品应允许定义多个用户；
2） 应保证每一个用户标识是全局唯一的，不允许一个用户标识用于多个用户。

8.5.2.2.2 用户属性定义

用户属性定义测试：

a） 测试评价方法
定义分属于不同角色的多个用户，检查输入的用户信息是否都能被保存。

b） 测试评价结果
入侵防御产品应为每一个用户保存其安全属性，包括用户标识、鉴别数据（如密码）、授权信息或用户组信息、其他安全属性等。输入的用户信息无丢失现象发生。

8.5.2.2.3 角色分级

角色分级测试：

a） 测试评价方法
1） 设置多个不同级别角色的用户，进行不同级别内容的操作请求；

2） 检查入侵防御产品的安全功能是否提供角色分级的用户。

b） 测试评价结果

入侵防御产品应提供分级角色的用户，分级角色覆盖范围互不相同。

8.5.2.3 安全功能保护

8.5.2.3.1 安全数据管理

安全数据管理测试：

a） 测试评价方法

模拟授权与非授权用户访问事件数据，入侵防御产品安全功能是否仅允许授权用户访问事件数据。

b） 测试评价结果

入侵防御产品应限制对事件数据的访问。除了具有明确的访问权限的授权用户之外，入侵防御产品应禁止所有其他用户对事件数据的访问。

8.5.2.3.2 数据存储告警

数据存储告警测试：

a） 测试评价方法

1） 检查入侵防御产品安全功能是否具有存储器剩余空间将耗尽的告警功能；

2） 检查入侵防御产品安全功能是否允许用户设定产生告警的剩余存储空间的大小；

3） 人为地将存储产品的事件数据存储器空间耗至设定的告警值以下，查看入侵防御产品是否告警。

b） 测试评价结果

1） 入侵防御产品在发生事件数据存储器空间将耗尽的情况时，自动产生告警；

2） 入侵防御产品允许用户设定产生告警的剩余存储空间的大小；

3） 在发现事件数据存储器空间将耗尽时，入侵防御产品还应提醒用户采取措施避免事件丢失，可选择例如转存已有事件数据、仅记录重要的事件数据、或者不记录新的事件数据等措施之一。

8.5.2.3.3 升级安全

升级安全测试：

a） 测试评价方法

1） 尝试用产品所允许的各种方法升级事件库和产品软件版本，检查升级过程是否正常；

2） 检查升级包是否具有开发商的签名提示，证明该升级包是由开发商提供的合法升级包；

3） 检查开发者文档中对保证升级安全的描述。

b） 测试评价结果

1） 入侵防御产品能够利用其提供的各种方法正常升级事件库和产品软件版本；

2） 升级包具有开发商的签名提示；

3） 开发者文档中提供了为事件库和版本升级安全所采取措施的详细描述；

4） 列举产品提供的事件库和版本升级手段。

8.5.2.3.4 自我隐藏

自我隐藏测试：

a） 测试评价方法

1） 检查开发者文档中对入侵防御产品自身安全的描述；

2） 将产品以网桥方式接入网络，检查 IP 隐藏情况。

b） 测试评价结果

入侵防御产品应能采用网桥方式隐藏 IP 地址，使自身在网络上不可见。

8.5.2.4 安全审计

8.5.2.4.1 审计数据生成

审计数据生成测试：

a） 测试评价方法

结合开发者文档，使用不同角色用户模拟对入侵防御产品不同模块进行访问、运行、修改、关闭以及重复失败尝试等相关操作，检查入侵防御产品提供了对哪些事件的审计。审查审计记录的正确性。

b） 测试评价结果

1） 入侵防御产品应至少为下述可审计事件产生审计记录：身份鉴别的尝试、安全策略更改的操作、修改安全属性的尝试；

2） 应在每个审计记录中至少记录如下信息：事件的日期和时间、事件类型、主体身份、事件的结果（成功或失败）等。

8.5.2.4.2 审计查阅

审计查阅测试：

a） 测试评价方法

审查产品安全功能是否为授权管理员提供从审计记录中读取全部审计信息的功能，是否能对审计记录进行排序。

b） 测试评价结果

入侵防御产品应为授权管理员提供从审计记录中读取全部审计信息的功能，并可以对审计记录进行排序。

8.5.2.4.3 受限的审计查阅

受限的审计查阅测试：

a） 测试评价方法

模拟授权与非授权管理员访问审计记录，入侵防御产品安全功能是否仅允许授权管理员访问审计记录。

b） 测试评价结果

入侵防御产品应限制审计记录的访问。除了具有明确的读访问权限的授权管理员之外，入侵防御产品应禁止所有其他用户对审计记录的读访问。

8.5.3 产品保证测试

8.5.3.1 配置管理

8.5.3.1.1 配置管理能力

配置管理能力评价：

a) 测试评价方法

评价者应审查开发者所提供的文档是否包含以下内容：

1) 开发者应使用配置管理系统并提供配置管理文档，以及为产品的不同版本提供唯一的标识；

2) 配置管理系统应对所有的配置项作出唯一的标识，并保证只有经过授权才能修改配置项，还应支持产品基本配置项的生成；

3) 配置管理文档应包括配置清单、配置管理计划以及接受计划。配置清单用来描述组成产品的配置项。在配置管理计划中，应描述配置管理系统是如何使用的。实施的配置管理应与配置管理计划相一致。在接受计划中，应描述对修改过或新建的配置项进行接受的程序；

4) 配置管理文档还应描述对配置项给出唯一标识的方法，并提供所有的配置项得到有效的维护的证据。

b) 测试评价结果

审查记录以及最后结果(符合/不符合)，评价者审查内容至少包括测试评价方法中的四方面(内容还涉及到基本配置项生成以及接受计划控制能力)。开发者提供的配置管理内容应完整。

8.5.3.1.2 配置管理范围

配置管理范围评价：

a) 测试评价方法

评价者应审查开发者提供的配置管理支持文件是否包含配置管理范围，要求将入侵防御产品的实现表示、设计文档、测试文档、用户文档、管理员文档、配置管理文档等置于配置管理之下，从而确保它们的修改是在一个正确授权的可控方式下进行的。评价者应审查开发者交付的文档是否包含以下内容：

1) 开发者所提供的配置管理文档应展示配置管理系统至少能跟踪上述配置管理之下的内容；

2) 文档应描述配置管理系统是如何跟踪这些配置项的；

3) 文档还应提供足够的信息表明达到所有要求；

4) 问题跟踪配置管理范围，除产品配置管理范围描述的内容外，要求特别强调对安全缺陷的跟踪。

b) 测试评价结果

审查记录以及最后结果(符合/不符合)符合测试评价方法要求，评价者应审查产品受控于配置管理。

8.5.3.2 交付与运行

8.5.3.2.1 交付

交付评价：

a) 测试评价方法

评价者应审查开发者是否使用一定的交付程序交付产品，并使用文档描述交付过程，并且评价者应审查开发者交付的文档是否包含以下内容：

1) 在给用户方交付产品的各版本时，为维护安全所必需的所有程序；

2) 产品版本变更控制的版本和版次说明、实际产品版本变更控制的版本和版次说明、监测产

品程序版本修改说明；

3） 检测试图伪装成开发者向用户发送产品的方法描述。

b） 测试评价结果

测试记录以及最后结果(符合/不符合)应符合测试评价方法要求，开发者应提供完整的文档描述所有交付的过程(文档和程序交付)，并包括产品详细版本、版次说明，以及发现非授权修改产品的方法，评测员进行审查确认。

8.5.3.2.2 安装生成

安装生成评价：

a） 测试评价方法

评价者应审查开发者是否提供了文档说明产品的安装、生成、启动和使用的过程。用户能够通过此文档了解安装、生成、启动和使用过程。

b） 测试评价结果

审查记录以及最后结果(符合/不符合)应符合测试评价方法要求。

8.5.3.3 安全功能开发

8.5.3.3.1 功能设计

功能设计评价：

a） 测试评价方法

评价者应审查开发者所提供的信息是否满足如下要求：

1） 功能设计应当使用非形式化风格来描述产品安全功能与其外部接口；

2） 功能设计应当是内在一致的；

3） 功能设计应当描述使用所有外部产品安全功能接口的目的与方法，适当的时候，要提供结果影响例外情况和出错信息的细节；

4） 功能设计应当完整地表示产品安全功能。

b） 测试评价结果

审查记录以及最后结果(符合/不符合)，评价者审查内容至少包括测试评价方法中的四个方面。开发者提供的内容应精确和完整。

8.5.3.3.2 高层设计

高层设计评价：

a） 测试评价方法

评价者应审查开发者所提供的信息是否满足如下要求：

1） 高层设计应采用非形式化的表示；

2） 高层设计应当是内在一致的；

3） 产品高层设计应当描述每一个产品安全功能子系统所提供的安全功能，提供了适当的体系结构来实现产品安全要求；

4） 产品的高层设计应当以子系统的观点来描述产品安全功能的结构，定义所有子系统之间的相互关系，并把这些相互关系适当地作为数据流、控制流等的外部接口来表示；

5） 高层设计应当标识产品安全要求的任何基础性的硬件、固件和/或软件，并且通过支持这些硬件、固件或软件所实现的保护机制，来提供产品安全功能表示。

b） 测试评价结果

审查记录以及最后结果(符合/不符合),评价者审查内容至少包括测试评价方法中的五个方面。开发者提供的高层设计内容应精确和完整。

8.5.3.3.3 安全功能的实现

安全功能的实现评价:

a) 测试评价方法

评价者应审查开发者所提供的信息是否满足如下要求:

1) 开发者应当为选定的产品安全功能子集提供实现表示;
2) 开发者应当为整个产品安全功能提供实现表示;
3) 实现表示应当无歧义地定义一个详细级别的产品安全功能,该产品安全功能的子集无须选择进一步的设计就能生成;
4) 实现表示应当是内在一致的。

b) 测试评价结果

审查记录以及最后结果(符合/不符合),评价者审查内容至少包括测试评价方法中的四个方面。开发者提供的安全功能实现内容应精确和完整。

8.5.3.3.4 低层设计

低层设计评价:

a) 测试评价方法

评价者应审查开发者所提供的产品安全功能的低层设计是否满足如下要求:

1) 低层设计的表示应当是非形式化的;
2) 低层设计应当是内在一致的;
3) 低层设计应当以模块术语描述产品安全功能;
4) 低层设计应当描述每一个模块的目的;
5) 低层设计应当以所提供的安全功能性和对其他模块的依赖性术语定义模块间的相互关系;
6) 低层设计应当描述如何提供每一个产品安全策略强化功能;
7) 低层设计应当标识产品安全功能模块的所有接口;
8) 低层设计应当标识产品安全功能模块的哪些接口是外部可见的;
9) 低层设计应当描述产品安全功能模块所有接口的目的与方法,适当时,应提供影响、例外情况和出错信息的细节;
10) 低层设计应当描述如何将产品分离成产品安全策略加强模块和其他模块。

b) 测试评价结果

审查记录以及最后结果(符合/不符合),评价者审查内容至少包括测试评价方法中的十个方面。开发者提供的低层设计内容应精确和完整。

8.5.3.3.5 表示对应性

表示对应性评价:

a) 测试评价方法

评价者应审查开发者是否在产品安全功能表示的所有相邻对之间提供对应性分析。其中,各种产品安全功能表示(如产品功能设计、高层设计、低层设计、实现表示)之间的对应性是所提供的抽象产品安全功能表示要求的精确而完整的示例。本元素仅仅要求产品安全功能在功能设计中进行细化,并且要求较为抽象的产品安全功能表示的所有相关安全功能部分,在较具体

的产品安全功能表示中进行细化。

b) 测试评价结果

测试记录以及最后结果(符合/不符合),评价者审查内容至少包括功能设计、高层设计、低层设计、实现表示这四项。开发者提供的内容应精确和完整,并互相对应。

8.5.3.4 指导性文档

8.5.3.4.1 管理员指南

管理员指南评价:

a) 测试评价方法

评价者应审查开发者是否提供了供授权管理员使用的管理员指南,并且此管理员指南是否包括如下内容:

1) 产品可以使用的管理功能和接口;
2) 怎样安全地管理产品;
3) 在安全处理环境中应进行控制的功能和权限;
4) 所有对与产品的安全操作有关的用户行为的假设;
5) 所有受管理员控制的安全参数,如果可能,应指明安全值;
6) 每一种与管理功能有关的安全相关事件,包括对安全功能所控制的实体的安全特性进行的改变;
7) 所有与授权管理员有关的 IT 环境的安全要求。

b) 测试评价结果

测试记录以及最后结果(符合/不符合),评价者审查内容至少包括测试评价方法中的七方面。开发者提供的管理员指南应完整。

8.5.3.4.2 用户指南

用户指南评价:

a) 测试评价方法

评价者应审查开发者是否提供了供入侵防御产品用户使用的用户指南,并且此用户指南是否包括如下内容:

1) 产品的非管理用户可使用的安全功能和接口;
2) 产品提供给用户的安全功能和接口的用法;
3) 用户可获取但应受安全处理环境控制的所有功能和权限;
4) 产品安全操作中用户所应承担的职责;
5) 与用户有关的 IT 环境的所有安全要求。

b) 测试评价结果

测试记录以及最后结果(符合/不符合),评价者审查内容至少包括测试评价方法中的五方面。开发者提供的用户指南应完整。

8.5.3.5 开发安全要求

开发安全要求评价:

a) 测试评价方法

评价者应审查开发者所提供的信息是否满足如下要求:

1) 开发人员的安全管理:开发人员的安全规章制度,开发人员的安全教育培训制度和记录;

2） 开发环境的安全管理：开发地点的出入口控制制度和记录，开发环境的温湿度要求和记录，开发环境的防火防盗措施和国家有关部门的许可文件，开发环境中所使用安全产品必须采用符合国家有关规定的产品并提供相应证明材料；

3） 开发设备的安全管理：开发设备的安全管理制度，包括开发主机使用管理和记录，设备的购置、修理、处置的制度和记录，上网管理，计算机病毒管理和记录等；

4） 开发过程和成果的安全管理：对产品代码、文档、样机进行受控管理的制度和记录。

b） 测试评价结果

测试记录以及最后结果（符合/不符合），评价者审查内容至少包括测试评价方法中的四方面。开发者提供文档应完整。

8.5.3.6 测试

8.5.3.6.1 范围

范围评价：

a） 测试评价方法

1） 评价者应审查开发者提供的测试覆盖分析结果，是否表明了测试文档中所标识的测试与安全功能设计中所描述的安全功能是对应的；

2） 评价测试文档中所标识的测试，是否完整。

b） 测试评价结果

审查记录以及最后结果（符合/不符合），开发者提供的测试文档中所标识的测试与安全功能设计中所描述的安全功能应对应，并且标识的测试应覆盖所有安全功能。

8.5.3.6.2 测试深度

测试深度评价：

a） 测试评价方法

评价开发者提供的测试深度分析，是否说明了测试文档中所标识的对安全功能的测试，足以表明该安全功能和高层设计是一致的。

b） 测试评价结果

测试记录以及最后结果（符合/不符合），评价者测试和审查与安全功能相对应的测试，这些测试应能正确保证测试出的安全功能符合高层设计的要求。

8.5.3.6.3 功能测试

功能测试评价：

a） 测试评价方法

1） 评价开发者提供的测试文档，是否包含测试计划、测试规程、预期的测试结果和实际测试结果；

2） 评价测试计划是否标识了要测试的安全功能，是否描述了测试的目标；

3） 评价测试规程是否标识了要执行的测试，是否描述了每个安全功能的测试概况（这些概况包括对其他测试结果的顺序依赖性）；

4） 评价期望的测试结果是否表明测试成功后的预期输出；

5） 评价实际测试结果是否表明每个被测试的安全功能能按照规定进行运作。

b） 测试评价结果

测试记录以及最后结果（符合/不符合），评价者审查内容至少包括测试评价方法中的五方面。

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。

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。

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.gb168.cn
服务热线:010-68522006
2012 年 10 月第一版
*
书号:155066·1-45543

GB/T 28451-2012