ICS35.040
L 80

中华人民共和国国家标准

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

Information security technology-
Techniques requirements and testing and evaluation approaches for intrusion detection system

2006-05-31 发布　　2006-12-01 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

（略）

信息安全技术
入侵检测系统技术要求和测试评价方法

1 范围

本标准规定了入侵检测系统的技术要求和测试评价方法，技术要求包括产品功能要求、产品安全要求、产品保证要求，并提出了入侵检测系统的分级要求。

本标准适用于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 17859-1999 计算机信息系统安全保护等级划分准则

GB/T 5271.8-2001 信息技术 词汇 第8部分：安全（idt ISO 2382-8:1998）

GB/T 18336.1-2001 信息技术 安全技术 信息技术安全性评估准则 第一部分：简介和一般模型（idt ISO 15408-1:1999）

3 术语和定义

GB 17859-1999、 GB/T 5271.8-2001和 GB/T 18336.1-2001 确立的以及下列术语和定义适用于本标准。

3.1

事件 incident

信息系统中试图改变目标状态，并造成或可能造成损害的行为。

3.2

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。

3.3

入侵检测 intrusion detection

通过对计算机网络或计算机系统中的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。

3.4

入侵检测系统 intrusion detection system

用于监测信息系统中可能存在的影响信息系统资产的行为的软件或软硬件组合。它通常分为主机型和网络型两种，由控制台、探测器和/或主机代理组成。

3.5

网络型入侵检测系统 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。

3.6

主机型入侵检测系统 host-based intrusion detection system

以系统日志、应用程序日志等作为数据源，或者通过其他手段（如监督系统调用）从所在的主机收集信息进行分析，从而发现异常行为的入侵检测系统。

3.7

探测器 sensor

用于收集可能指示出入侵行为或者滥用信息系统资源的实时事件，并对收集到的信息进行初步分析的入侵检测系统组件。

注：网络型入侵检测系统的探测器安装在网络的关键节点处，监听流经网络的数据；主机型入侵检测系统的探测器以主机代理的形式安装在主机系统上，收集主机的运行状态和主机信息。

3.8

IDS控制台 IDS management console

用于探测器管理、策略配置、数据管理、告警管理、事件响应、升级事件库以及其它管理工作，并对入侵行为进行深层次分析的入侵检测系统组件。一个控制台可以管理多个探测器。

3.9

用户 user

是使用入侵检测系统的授权管理员、审计员的统称。

3.10

攻击特征 attack signature

入侵检测系统预先定义好的能够发现一次攻击正在发生的特定信息。

3.11

告警 alert

当攻击或入侵发生时，入侵检测系统向授权管理员发出的紧急通知。

3.12

响应 response

当攻击或入侵发生时，针对信息系统及存储的数据采取的保护并恢复正常运行环境的行为。

3.13

误报 false positives

入侵检测系统在未发生攻击时告警，或者发出错误的告警信息。

3.14

漏报 false negative

当攻击发生时入侵检测系统未告警。

3.15

强力攻击 brute force

是一种利用合法字符的各种组合序列，通过应用程序反复尝试各种可能的组合来试图破解加密信息（如密码、密钥）的方法。强力攻击通过穷举法而非智能策略来达到目的，是一种有效而耗时的攻击手法。

4 缩略语

下列缩略语适用于本标准：

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

HTML	超文本标记语言	Hypertext Markup Language
HTTP	超文本传送协议	Hypertext Transfer Protocol
ICMP	网际控制报文协议	Internet Control Message Protocol
IDS	入侵检测系统	Intrusion Detection System
IMAP	因特网消息访问协议	Internet Message Access Protocal
IP	网际协议	Internet Protocol
NFS	网络文件系统	Network File System
NNTP	网络新闻传送协议	Network News Transfer Protocol
POP	邮局协议	Post Office Protocol
RIP	路由选择信息协议	Routing Information Protocol
RPC	远程过程调用	Remote Procedure Call
SMTP	简单邮件传送协议	Simple Mail Transfer Protocol
SNMP	简单网络管理协议	Simple Network Management Protocol
TCP	传输控制协议	Transport Control Protocol
TELNET	远程登陆	Telnet
TFTP	普通文件传送协议	Trivial File Transfer Protocol
UDP	用户数据报协议	User Datagram Protocol

5 入侵检测系统等级划分

5.1 等级划分说明

5.1.1 第一级

本级规定了入侵检测系统的最低安全要求。通过简单的用户标识和鉴别来限制对系统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，阻止非法用户危害系统，保护入侵检测系统的正常运行。

5.1.2 第二级

本级划分了安全管理角色，以细化对入侵检测系统的管理。加入审计功能，使得授权管理员的行为是可追踪的。同时，还增加了保护系统数据、系统自身安全运行的措施。

5.1.3 第三级

本级通过增强审计、访问控制、系统的自身保护等要求，对入侵检测系统的正常运行提供更强的保护。本级还要求系统具有分布式部署、多级管理、集中管理、以及支持安全管理中心的能力。此外，还要求系统具有较强的抗攻击能力。

5.2 安全等级划分

5.2.1 网络型入侵检测系统安全等级划分

网络型入侵检测系统的安全等级划分如表 1、表 2 所示。对网络型入侵检测系统的等级评定是依据下面两个表格，结合产品保证要求的综合评定得出的，符合第一级的网络型入侵检测系统应满足表 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；符合第二级的网络型入侵检测系统应满足表 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；符合第三级的网络型入侵检测系统应满足表 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　网络型入侵检测系统产品功能要求等级划分表

产品功能要求	功能组件	一级	二级	三级
数据探测功能要求	数据收集	*	*	*
	协议分析	*	*	*
	行为监测	*	*	*
	流量监测	*	*	*
入侵分析功能要求	数据分析	*	*	*
	分析方式	*	*	*
	防躲避能力		*	*
	事件合并		*	*
	事件关联			*
入侵响应功能要求	安全告警	*	*	*
	告警方式	*	*	*
	排除响应		*	*
	定制响应		*	*
	全局预警			*
	阻断能力	*	*	*
	防火墙联动		*	*
	入侵管理			*
	其它设备联动			*
管理控制功能要求	图形界面	*	*	*
	分布式部署		*	*
	多级管理			*
	集中管理		*	*
	同台管理		*	*
	端口分离		*	*
	事件数据库	*	*	*
	事件分级	*	*	*
	策略配置	*	*	*
	产品升级	*	*	*
	统一升级	*	*	*
检测结果处理要求	事件记录	*	*	*
	事件可视化	*	*	*
	报告生成	*	*	*
	报告查阅	*	*	*
	报告输出	*	*	*

产品灵活性要求	窗口定义		*	*
	报告定制	*	*	*
	事件定义		*	*
	协议定义		*	*
	通用接口		*	*
性能指标要求	漏报率	*	*	*
	误报率	*	*	*
	还原能力			*
注：“*”表示具有该要求。				

表2　网络型入侵检测系统产品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
身份鉴别	用户鉴别	*	*	*
	多鉴别机制			*
	鉴别失败的处理	*	*	*
	超时设置		*	*
	会话锁定		*	*
	鉴别数据保护			*
用户管理	用户角色	*	*	*
	用户属性定义		*	*
	安全行为管理		*	*
	安全属性管理			*
安全审计	审计数据生成		*	*
	审计数据可用性		*	*
	审计查阅		*	*
	受限的审计查阅		*	*
事件数据安全	安全数据管理	*	*	*
	数据保护	*	*	*
	数据存储告警			*
通信安全	通信完整性	*	*	*
	通信稳定性	*	*	*
	升级安全	*	*	*
产品自身安全	自我隐藏	*	*	*
	自我保护	*	*	*
	自我监测		*	*
注：“*”表示具有该要求。				

5.2.2 主机型入侵检测系统安全等级划分

主机型入侵检测系统的安全等级划分如表 3、表 4 所示。对主机型入侵检测系统的等级评定是依据下面两个表格，结合产品保证要求的综合评定得出的，符合第一级的主机型入侵检测系统应满足表 3、表 4 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；符合第二级的主机型入侵检测系统应满足表 3、表 4 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；符合第三级的主机型入侵检测系统应满足表 3、表 4 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3 主机型入侵检测系统产品功能要求等级划分表

产品功能要求	功能组件	一级	二级	三级
数据探测功能要求	数据收集	*	*	*
	行为监测	*	*	*
入侵分析功能要求	数据分析	*	*	*
入侵响应功能要求	安全告警	*	*	*
	告警方式	*	*	*
	阻断能力	*	*	*
管理控制功能要求	图形界面	*	*	*
	集中管理		*	*
	同台管理		*	*
	事件数据库	*	*	*
	事件分级	*	*	*
	策略配置	*	*	*
	产品升级	*	*	*
检测结果处理要求	事件记录	*	*	*
	事件可视化	*	*	*
	报告生成	*	*	*
	报告查阅	*	*	*
	报告输出	*	*	*
产品灵活性要求	窗口定义		*	*
	报告定制	*	*	*
	事件定义		*	*
	通用接口		*	*
性能指标要求	稳定性	*	*	*
	CPU 资源占用量	*	*	*
	内存占用量	*	*	*
	用户登录和资源访问	*	*	*
	网络通信	*	*	*
注：“*”表示具有该要求。				

表4　主机型入侵检测系统产品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
身份鉴别	用户鉴别	*	*	*
	多鉴别机制			*
	鉴别失败的处理	*	*	*
	超时设置		*	*
	会话锁定		*	*
	鉴别数据保护			*
用户管理	用户角色	*	*	*
	用户属性定义		*	*
	安全行为管理		*	*
	安全属性管理			*
安全审计	审计数据生成		*	*
	审计数据可用性		*	*
	审计查阅		*	*
	受限的审计查阅		*	*
事件数据安全	安全数据管理	*	*	*
	数据保护	*	*	*
	数据存储告警			*
通信安全	通信完整性	*	*	*
	通信稳定性	*	*	*
	升级安全	*	*	*
产品自身安全	自我保护	*	*	*
注：“*”表示具有该要求。				

6　入侵检测系统技术要求

注：第6、7两章对每一等级的具体要求分别进行描述。其中“**加粗宋体**”表示所描述的内容在该级中第一次出现。

6.1　第一级

6.1.1　产品功能要求

6.1.1.1　数据探测功能要求

6.1.1.1.1　数据收集

网络型入侵检测系统应具有实时获取受保护网段内的数据包的能力。获取的数据包应足以进行检测分析。

主机型入侵检测系统应具有实时获取一种或多种操作系统下主机的各种状态信息的能力。

6.1.1.1.2　协议分析

网络型入侵检测系统至少应监视基于以下协议的事件：IP、ICMP、ARP、RIP、TCP、UDP、RPC、HTTP、FTP、TFTP、IMAP、SNMP、TELNET、DNS、SMTP、POP3、NETBIOS、NFS、NNTP等。

6.1.1.1.3　行为监测

网络型入侵检测系统至少应监视以下攻击行为：端口扫描、强力攻击、木马后门攻击、拒绝服务

攻击、缓冲区溢出攻击、IP 碎片攻击、网络蠕虫攻击等。

主机型入侵检测系统至少应监视以下行为：端口扫描、强力攻击、缓冲区溢出攻击、可疑连接等。

6.1.1.1.4 流量监测

网络型入侵检测系统应监视整个网络或者某一特定协议、地址、端口的报文流量和字节流量。

6.1.1.2 入侵分析功能要求

6.1.1.2.1 数据分析

网络型入侵检测系统应对收集的数据包进行分析，发现攻击事件。

主机型入侵检测系统应将收集到的信息进行分析，发现违反安全策略的行为，或者可能存在的入侵行为。

6.1.1.2.2 分析方式

网络型入侵检测系统应以模式匹配、协议分析、人工智能等一种或多种方式进行入侵分析。

6.1.1.3 入侵响应功能要求

6.1.1.3.1 安全告警

当系统检测到入侵时，应自动采取相应动作以发出安全警告。

6.1.1.3.2 告警方式

告警可以采取屏幕实时提示、E-mail 告警、声音告警等几种方式。

6.1.1.3.3 阻断能力

系统在监测到网络上的非法连接时，可进行阻断。

6.1.1.4 管理控制功能要求

6.1.1.4.1 图形界面

系统应提供友好的用户界面用于管理、配置入侵检测系统。管理配置界面应包含配置和管理产品所需的所有功能。

6.1.1.4.2 事件数据库

系统的事件数据库应包括事件定义和分析、详细的漏洞修补方案、可采取的对策等。

6.1.1.4.3 事件分级

系统应按照事件的严重程度将事件分级，以使授权管理员能从大量的信息中捕捉到危险的事件。

6.1.1.4.4 策略配置

应提供方便、快捷的入侵检测系统策略配置方法和手段。

6.1.1.4.5 产品升级

系统应具有及时更新、升级产品和事件库的能力。

6.1.1.4.6 统一升级

网络型入侵检测系统应提供由控制台对各探测器的事件库进行统一升级的功能。

6.1.1.5 检测结果处理要求

6.1.1.5.1 事件记录

系统应记录并保存检测到的入侵事件。

入侵事件信息应至少包含以下内容：事件发生时间、源地址、目的地址、危害等级、事件详细描述以及解决方案建议等。

6.1.1.5.2 事件可视化

用户应能通过管理界面实时清晰地查看入侵事件。

6.1.1.5.3 报告生成

系统应能生成详尽的检测结果报告。

6.1.1.5.4 报告查阅

系统应具有全面、灵活地浏览检测结果报告的功能。

6.1.1.5.5 报告输出

检测结果报告应可输出成方便用户阅读的文本格式，如字处理文件、HTML 文件、文本文件等。

6.1.1.6 产品灵活性要求

6.1.1.6.1 报告定制

系统应支持授权管理员按照自己的要求修改和定制报告内容。

6.1.1.7 主机型入侵检测系统性能要求

6.1.1.7.1 稳定性

主机型入侵检测系统在主机正常工作状态下都应该工作稳定，不应造成被检测主机停机或死机现象。

6.1.1.7.2 CPU 资源占用量

主机型入侵检测系统的 CPU 占有率不应明显影响主机的正常工作。

6.1.1.7.3 内存占用量

主机型入侵检测系统占用内存空间不应影响主机的正常工作。

6.1.1.7.4 用户登录和资源访问

主机型入侵检测系统不应影响所在目标主机上的合法用户登录及文件资源访问。

6.1.1.7.5 网络通信

主机型入侵检测系统不应影响所在目标主机的正常网络通信。

6.1.1.8 网络型入侵检测系统性能要求

6.1.1.8.1 误报率

网络型入侵检测系统应按照指定的测试方法、测试工具、测试环境和测试步骤测试产品的误报率。产品应将误报率控制在应用许可的范围，不能对正常使用产品产生较大影响。

6.1.1.8.2 漏报率

网络型入侵检测系统应按照指定的测试方法、测试工具、测试环境和测试步骤，在正常网络流量下和各种指定的网络背景流量下，分别测试产品未能对指定的入侵行为进行告警的数据。系统应将漏报率控制在应用许可的范围，不能对正常使用产品产生较大影响。

6.1.2 产品安全要求

6.1.2.1 身份鉴别

6.1.2.1.1 用户鉴别

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。

6.1.2.1.2 鉴别失败的处理

当用户鉴别尝试失败连续达到指定次数后，系统应锁定该帐号，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。

6.1.2.2 用户管理

6.1.2.2.1 用户角色

系统应设置多个角色，并应保证每一个用户标识是全局唯一的。

6.1.2.3 事件数据安全

6.1.2.3.1 安全数据管理

系统应仅限于指定的授权角色访问事件数据，禁止其它用户对事件数据的操作。

6.1.2.3.2 数据保护

系统应在遭受攻击时，能够完整保留已经保存的事件数据。

6.1.2.4 通信安全

6.1.2.4.1 通信完整性

系统应确保各组件之间传输的数据（如配置和控制信息、告警和事件数据等）不被泄漏或篡改。

6.1.2.4.2 通信稳定性

应采取点到点协议等保证通信稳定性的方法，保证各部件和控制台之间传递的信息不因网络故障而丢失或延迟。

6.1.2.4.3 升级安全

系统应确保事件库和版本升级时的通信安全，应确保升级包是由开发商提供的。

6.1.2.5 产品自身安全

6.1.2.5.1 自我隐藏

网络型入侵检测系统应采取隐藏探测器 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。

6.1.2.5.2 自我保护

主机型入侵检测系统应具有自我保护功能（如防止程序被非法终止，停止告警）。

6.1.3 产品保证要求

6.1.3.1 配置管理

开发者应为系统的不同版本提供唯一的标识。

系统的每个版本应当使用它们的唯一标识作为标签。

6.1.3.2 交付与运行

开发者应提供文档说明系统的安装、生成和启动的文档。

6.1.3.3 安全功能开发

6.1.3.3.1 功能设计

开发者应提供系统的安全功能设计文档。

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。

6.1.3.3.2 表示对应性

开发者应在产品安全功能表示的所有相邻对之间提供对应性分析。

6.1.3.4 文档要求

6.1.3.4.1 管理员指南

开发者应提供授权管理员使用的管理员指南。

管理员指南应说明以下内容：

a) 系统可以使用的管理功能和接口；
b) 怎样安全地管理系统；
c) 在安全处理环境中应进行控制的功能和权限；
d) 所有对与系统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。

6.1.3.4.2 用户指南

开发者应提供用户指南。

用户指南应说明以下内容：

a) 系统的非管理用户可使用的安全功能和接口；
b) 系统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) 系统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。

6.1.3.5 开发安全要求

开发者应提供开发安全文件。

开发安全文件应描述在系统的开发环境中，为保护系统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。开发安全文件还应提供在系统的开发和维护过程中执行安全措施的证据。

6.1.3.6 测试

6.1.3.6.1 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。

6.1.3.6.2 功能测试

开发者应测试安全功能，并提供相应的测试文档。

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。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，这些概况包括对其它测试结果的顺序依赖性。期望的测试结果应表明测试成功后的预期输出。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。

6.2 第二级

6.2.1 产品功能要求

6.2.1.1 入侵分析功能要求

6.2.1.1.1 防躲避能力

网络型入侵检测系统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。

6.2.1.1.2 事件合并

网络型入侵检测系统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。

6.2.1.2 入侵响应功能要求

6.2.1.2.1 排除响应

网络型入侵检测系统应允许用户定义对被检测网段中指定的主机或特定的事件不予告警，降低误报。

6.2.1.2.2 定制响应

网络型入侵检测系统应允许用户对被检测网段中指定的主机或特定的事件定制不同的响应方式，以对特定的事件突出告警。

6.2.1.2.3 防火墙联动

网络型入侵检测系统应具有与防火墙进行联动的能力，可按照设定的联动策略自动调整防火墙配置。

6.2.1.3 管理控制功能要求

6.2.1.3.1 分布式部署

网络型入侵检测系统应具有本地或异地分布式部署、远程管理的能力。

6.2.1.3.2 集中管理

系统应设置集中管理中心，对分布式、多级部署的入侵检测系统进行统一集中管理，形成多级管理结构。

6.2.1.3.3 同台管理

对同一个厂家生成的产品，如果同时具有网络型入侵检测系统和主机型入侵检测系统，二者可被同一个控制台统一进行管理。

6.2.1.3.4 端口分离

网络型入侵检测系统的探测器应配备不同的端口分别用于产品管理和网络数据监听。

6.2.1.4 产品灵活性要求

6.2.1.4.1 窗口定义

系统应支持用户自定义窗口显示的内容和显示方式。

6.2.1.4.2 事件定义

系统应允许授权管理员自定义事件，或者对开发商提供的事件作修改，并应提供方便、快捷的定义方法。

6.2.1.4.3 协议定义

网络型入侵检测系统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。

6.2.1.4.4 通用接口

系统应提供对外的通用接口，以便与其它安全设备（如网络管理软件、防火墙等）共享信息或规范化联动。

6.2.2 产品安全要求

6.2.2.1 身份鉴别

6.2.2.1.1 超时设置

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，终止会话，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。

6.2.2.1.2 会话锁定

系统应允许用户锁定自己的交互会话，锁定后需要再次进行身份鉴别才能够重新管理产品。

6.2.2.2 用户管理

6.2.2.2.1 用户属性定义

系统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（如密码）、授权信息或用户组信息、其它安全属性等。

6.2.2.2.2 安全行为管理

系统应仅限于已识别了的指定的授权角色对产品的功能具有禁止、修改的能力。

6.2.2.3 安全审计

6.2.2.3.1 审计数据生成

应能为下述可审计事件产生审计记录：审计功能的启动和关闭，审计级别以内的所有可审计事件（如鉴别失败等重大事件）等。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。

6.2.2.3.2 审计数据可用性

审计数据的记录方式应便于用户理解。

6.2.2.3.3 审计查阅

系统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。

6.2.2.3.4 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，系统应禁止所有其它用户对审计记录的读访问。

6.2.2.4 产品自身安全

6.2.2.4.1 自我监测

网络型入侵检测系统在启动和正常工作时，应周期性地、或者按照授权管理员的要求执行自检，以验证产品自身执行的正确性。

6.2.3 产品保证要求

6.2.3.1 配置管理

6.2.3.1.1 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地维护的证据。

6.2.3.1.2 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：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。

6.2.3.2 交付与运行

6.2.3.2.1 交付

开发者应使用一定的交付程序交付产品，并将交付过程文档化。

交付文档应描述在给用户方交付产品的各版本时，为维护安全所必需的所有程序。

6.2.3.2.2 安装生成

开发者应提供文档说明系统的安装、生成和启动的文档。

6.2.3.3 安全功能开发

6.2.3.3.1 功能设计

开发者应提供系统的安全功能设计文档。

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。

6.2.3.3.2 高层设计

开发者应提供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它子系统分开。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。高层设计还应标识系统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。

6.2.3.3.3 表示对应性

开发者应在产品安全功能表示的所有相邻对之间提供对应性分析。

6.2.3.4 文档要求

6.2.3.4.1 管理员指南

开发者应提供授权管理员使用的管理员指南。

管理员指南应说明以下内容：

a) 产品管理员可以使用的管理功能和接口；

b) 怎样安全地管理系统；
c) 在安全处理环境中应进行控制的功能和权限；
d) 所有对与系统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。

6.2.3.4.2 用户指南

开发者应提供用户指南。

用户指南应说明以下内容：

a) 系统的非管理用户可使用的安全功能和接口；
b) 系统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) 系统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。

6.2.3.5 开发安全要求

开发者应提供开发安全文件。

开发安全文件应描述在系统的开发环境中，为保护系统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。开发安全文件还应提供在系统的开发和维护过程中执行安全措施的证据。

6.2.3.6 测试

6.2.3.6.1 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。**

6.2.3.6.2 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。

6.2.3.6.3 功能测试

开发者应测试安全功能，并提供相应的测试文档。

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。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，这些概况包括对其它测试结果的顺序依赖性。期望的测试结果应表明测试成功后的预期输出。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。

6.2.3.6.4 独立性测试

开发者应提供证据证明，开发者提供的系统经过独立的第三方测试并通过。

6.2.3.7 脆弱性评定

6.2.3.7.1 指南检查

开发者应提供文档。

在文档中，应确定对系统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。

6.2.3.7.2 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，对系统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，应能够显示在使用系统的环境中该脆弱性不能被利用。

6.3 第三级

6.3.1 产品功能要求

6.3.1.1 入侵分析功能要求

6.3.1.1.1 事件关联

网络型入侵检测系统应具有把不同的事件关联起来，发现低危害事件中隐含的高危害攻击的能力。

6.3.1.2 入侵响应功能要求

6.3.1.2.1 全局预警

网络型入侵检测系统应具有全局预警功能，控制台可在设定全局预警的策略后，将局部出现的重大安全事件通知其上级控制台或者下级控制台。

6.3.1.2.2 入侵管理

网络型入侵检测系统应具有全局安全事件的管理能力，可与安全管理中心或网络管理中心进行联动。

6.3.1.2.3 其它设备联动

网络型入侵检测系统应具有与其它网络设备和网络安全部件（如漏洞扫描，交换机）按照设定的策略进行联动的能力。

6.3.1.3 管理控制功能要求

6.3.1.3.1 多级管理

网络型入侵检测系统应具有多级管理、分级管理的能力。

6.3.1.4 网络型入侵检测系统性能要求

6.3.1.4.1 还原能力

网络型入侵检测系统应对 **HTTP、FTP、SMTP、POP3、Telnet** 等主要的网络协议通信进行内容恢复和还原；当背景数据流低于网络有效带宽的 **80%**时，系统应保证数据的获取和还原能够正常进行。

6.3.2 产品安全要求

6.3.2.1 身份鉴别

6.3.2.1.1 多鉴别机制

系统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。

6.3.2.1.2 鉴别数据保护

应保护鉴别数据不被未授权查阅和修改。

6.3.2.2 用户管理

6.3.2.2.1 安全属性管理

系统应仅限于的已识别了的指定的授权角色可以对指定的安全属性进行查询、修改、删除、改变其默认值等操作。

6.3.2.3 事件数据安全

6.3.2.3.1 数据存储告警

系统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用户自主设定。

6.3.3 产品保证要求

6.3.3.1 配置管理

6.3.3.1.1 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，以及为系统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，**还应支持系统基本配置项的生成。**

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系统的配置项。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地维护的证据。

6.3.3.1.2 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：系统实现表示、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。

6.3.3.2 交付与运行

6.3.3.2.1 交付

开发者应使用一定的交付程序交付系统，并将交付过程文档化。

交付文档应包括以下内容：

a) 在给用户方交付系统的各版本时，为维护安全所必需的所有程序；

b）开发者的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。

6.3.3.2.2 安装生成

开发者应提供文档说明系统的安装、生成和启动的文档。

6.3.3.3 安全功能开发

6.3.3.3.1 功能设计

开发者应提供系统的安全功能设计文档。

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。

6.3.3.3.2 高层设计

开发者应提供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它子系统分开。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。高层设计还应标识系统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。

6.3.3.3.3 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。

6.3.3.3.4 低层设计

开发者应提供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) 说明如何将系统加强安全策略的模块和其它模块分离开。

6.3.3.3.5 表示对应性

开发者应在产品安全功能表示的所有相邻对之间提供对应性分析。

6.3.3.4 文档要求

6.3.3.4.1 管理员指南

开发者应提供授权管理员使用的管理员指南。

管理员指南应说明以下内容：

a) 产品管理员可以使用的管理功能和接口；

b) 怎样安全地管理系统；

c) 在安全处理环境中应进行控制的功能和权限；

d) 所有对与系统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。

6.3.3.4.2 用户指南

开发者应提供用户指南。

用户指南应说明以下内容：

a) 系统的非管理用户可使用的安全功能和接口；

b) 系统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) 系统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。

6.3.3.5 开发安全要求

开发者应提供开发安全文件。

开发安全文件应描述在系统的开发环境中，为保护系统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。开发安全文件还应提供在系统的开发和维护过程中执行安全措施的证据。

6.3.3.6 测试

6.3.3.6.1 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。

6.3.3.6.2 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。

6.3.3.6.3 功能测试

开发者应测试安全功能，并提供相应的测试文档。

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。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，这些概况包括对其它测试结果的顺序依赖性。期望的测试结果应表明测试成功后的预期输出。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。

6.3.3.6.4 独立性测试

开发者应提供证据证明，开发者提供的系统经过独立的第三方测试并通过。

6.3.3.7 脆弱性评定

6.3.3.7.1 指南检查

开发者应提供文档。

在文档中，应确定对系统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。**

6.3.3.7.2 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，对系统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，应能够显示在使用系统的环境中该脆弱性不能被利用。

7 入侵检测系统测评方法

7.1 测试环境

入侵检测系统功能测试的典型网络拓扑结构如图1所示。

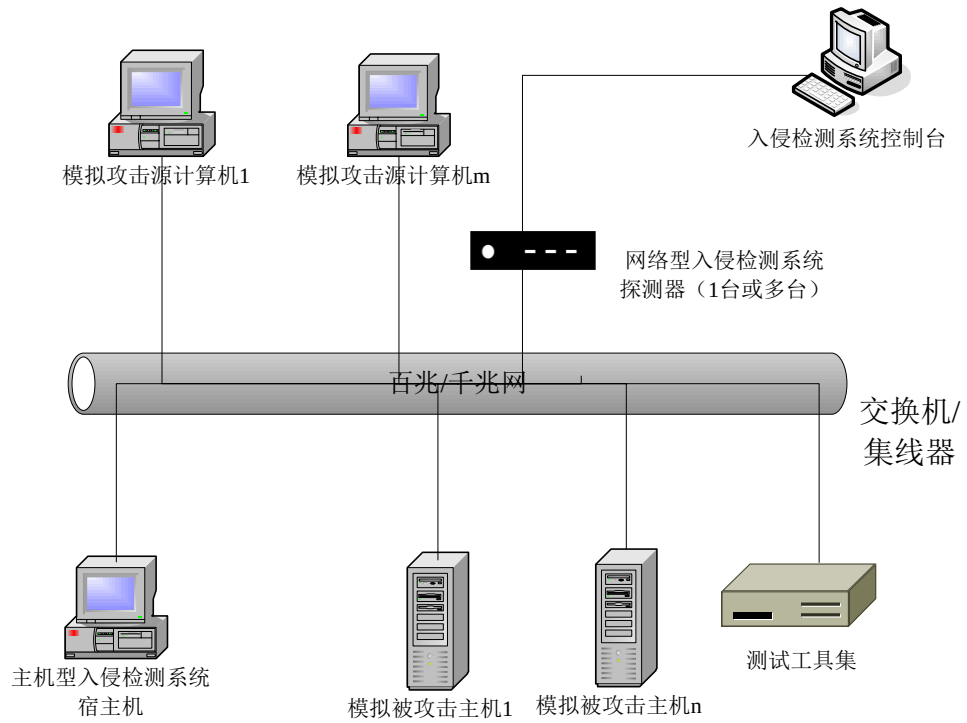

图1 入侵检测系统功能测试典型网络拓扑图

测试设备包括测试所需的交换机、测试工具集、模拟攻击源计算机、模拟被攻击计算机、主机型入侵检测系统宿主机，以及入侵检测系统控制台、网络型入侵检测系统探测器等。其中，模拟攻击源计算机和被攻击计算机可以为多台，并可安装不同的操作系统和应用软件。

7.2 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测试产品报警能力。

只要有利于科学、公正、可重复地得到入侵检测系统的测试结果，可采取多种测试工具和测试方法对系统进行测试。

7.3 第一级

7.3.1 产品功能测试

7.3.1.1 数据探测功能测试

7.3.1.1.1 数据收集

a) 测试评价方法：

1） 对网络型入侵检测系统，检查是否具有实时获取受保护网段内的数据包的能力；

2） 对主机型入侵检测系统，针对主机进行指定的操作（至少包括远程登录，猜测口令，访问服务，删除文件等），检查系统是否能够收集到这些信息。

b) 测试评价结果：

1） 网络型入侵检测系统应能够获取足够的网络数据包以分析入侵事件；

2） 主机型入侵检测系统应能够获得一种或多种操作系统的各种操作和状态信息。

7.3.1.1.2 协议分析

a) 测试评价方法：

1） 打开网络型入侵检测系统的安全策略配置，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） 配置系统的检测策略为最大策略集；

4） 发送攻击事件测试集中的所有事件，记录系统的检测结果。

b) 测试评价结果：

1） 记录系统报告的攻击名称和类型；

2） 产品说明书中声称能够监视的协议的事件至少包括以下类型：IP、ICMP、ARP、RIP、TCP、UDP、RPC、HTTP、FTP、TFTP、IMAP、SNMP、TELNET、DNS、SMTP、POP3、NETBIOS、NFS、NNTP 等，抽样测试应未发现矛盾之处；

3） 列举系统支持的所有入侵分析方法。

7.3.1.1.3 行为监测

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。选取的事件应包括：端口扫描类事件（如 TCP 端口扫描、UDP 端口扫描、ICMP 分布式主机扫描等）、拒绝服务类事件（如 SYNFLOOD、UDPFLOOD、ICMPFLOOD、IGMP 拒绝服务等）、后门类事件（如 BO、Netbus、Dolly 等）、蠕虫类事件（如红色代码、冲击波、振荡波等）、溢出类事件（如 FTP_命令溢出、SMTP_HELO_缓冲区溢出、POP3_foxmail_5.0_缓冲区溢出、Telnet_Solaris_telnet_缓冲区溢出、HTTP_IIS_Unicode_漏洞、MSSQL2000_远程溢出、FTP_AIX_溢出漏洞等）、强力攻击和弱口令类事件（如 SMTP、HTTP、FTP、

MSSQLSERVER、FTP_弱口令、POP3_弱口令等）、以及其它具有代表性的网络攻击事件，测试网络型入侵检测系统；

2）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。选取的事件应包括：端口扫描类事件、强力攻击类事件、缓冲区溢出类事件、可疑连接、以及其它具有代表性的主机攻击事件，测试主机型入侵检测系统；

3）配置系统的检测策略为最大策略集；

4）发送攻击事件测试集中的所有事件，记录系统的检测结果。

b) 测试评价结果：

1）对攻击事件测试集的攻击，系统应报告相应的入侵事件，包括事件名称、攻击源地址、目地址、事件发生时间、重要级别等信息；

2）记录系统报告的攻击名称和类型。

7.3.1.1.4 流量监测

a) 测试评价方法：

1）开启流量显示功能，定义流量事件，查看流量显示界面，显示流量变化；

2）对某一服务器发起大流量的攻击，如 ping flood；

3）对特定的端口（如 80 端口）发起拒绝服务攻击。

b) 测试评价结果：

1）可以显示出各种流量信息；

2）可以显示出正在遭受攻击（如 ping flood）的服务器；

3）可以显示出网络中正遭受的拒绝服务攻击；

4）列举提供的流量监测内容，如流量事件、不同协议的流量显示曲线等。

7.3.1.2 入侵分析功能测试

7.3.1.2.1 数据分析

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。选取的事件应包括扫描类事件、拒绝服务类事件、后门类事件、蠕虫类事件、溢出类事件、暴力猜解和弱口令类事件、以及其它具有代表性的攻击事件；

2）配置系统的检测策略为最大策略集；

3）发送攻击事件测试集中的所有事件，记录系统的检测结果。

b) 测试评价结果：

1）对攻击事件测试集的攻击，系统应报告相应的入侵事件，包括事件名称、攻击源地址、目地址、事件发生时间、重要级别等信息；

2）记录系统报告的攻击名称和类型。

7.3.1.2.2 分析方式

a) 测试评价方法：

1）检查系统的事件库；

2）打开系统的安全策略配置，检查安全事件的描述是否具有协议类型等属性；

3）检查产品说明书，查找关于产品分析方法的说明，按照系统所声明的各类分析方法，在系统中进行检查确认。

b) 测试评价结果：

1）应具备安全事件库；

2） 列举系统支持的所有入侵分析方法。

7.3.1.3 入侵响应功能测试

7.3.1.3.1 安全告警

a) 测试评价方法：

1） 触发一定的安全事件，查看是否有告警信息；

2） 检查报警界面的显示信息是否分级别显示；

3） 查看报警信息的详细记录；

4） 查看报警事件的详细解释。

b) 测试评价结果：

1） 可以显示告警信息；

2） 报警信息可以分为高、中、低等级别显示；

3） 对于每条报警信息记录详细的参数；

4） 对于每条报警事件能够给出详细解释和建议解决方案；

5） 事件的详细解释最好为中文。

7.3.1.3.2 告警方式

a) 测试评价方法：

1） 打开菜单，查看告警方式的选择；

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。记录并列出所有告警方式。

7.3.1.3.3 阻断能力

a) 测试评价方法：

1） 检查系统的响应策略配置界面是否具有阻断选项；

2） 选中对攻击事件的阻断选项，检查系统在监测到相应攻击时是否进行阻断。

b) 测试评价结果：

1） 能够对监测到的非法连接配置阻断选项；

2） 在监测到网络上的非法连接时，可成功进行阻断。

7.3.1.4 管理控制功能测试

7.3.1.4.1 图形界面

a) 测试评价方法：

1） 登录控制台界面；

2） 查看用户界面的功能，包括管理配置界面、报警显示界面等；

3） 通过界面配置控制台和探测器的连接。

b) 测试评价结果：

1） 具备独立的控制台；

2） 具有图形化的管理界面；

3） 具备划分清晰功能区域的报警显示界面。

7.3.1.4.2 事件数据库

a) 测试评价方法：

1） 检查系统是否把检测到的事件存储到相应的数据中；

2） 检查系统支持的数据库格式。

b) 测试评价结果：

1） 系统提供存储安全事件的数据库，除部署单独的数据库服务器外，正常情况下不须单独安装第三方数据库；

2） 数据库应包括事件定义和分析、详细的漏洞修补方案、可采取的对策等内容；

3） 列举系统支持的数据库格式。

7.3.1.4.3 事件分级

a) 测试评价方法：

1） 打开系统的事件库，检查是否每个事件都有分级信息；

2） 检查界面显示的攻击事件是否具备事件级别信息。

b) 测试评价结果：

1） 事件库的所有事件都具有分级信息；

2） 界面显示的攻击事件，都以文字或色彩等形式显示了事件级别。

7.3.1.4.4 策略配置

a) 测试评价方法：

1） 打开菜单，查看系统提供的默认策略；

2） 查看是否允许编辑或修改生成新的策略。

b) 测试评价结果：

1） 系统应提供默认的策略，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） 记录系统提供的策略种类和名称。

7.3.1.4.5 产品升级

a) 测试评价方法：

1） 检查事件特征库的升级方式；

2） 检查控制台的升级方式；

3） 检查探测器的升级方式。

b) 测试评价结果：

1） 特征库可以进行手动或自动的在线升级；

2） 升级的过程中探测器可以正常检测事件；

3） 应通过控制台来下发探测器的升级程序；

4） 列举事件库升级的方式、承诺的升级频率。

7.3.1.4.6 统一升级

a) 测试评价方法：从主控制台做特征库升级，来查看控制台是否可以在升级后将特征库下发给其下级控制台；

b) 测试评价结果：

1） 支持上级控制台将升级信息下发给下级控制台；

2） 提供由控制台对各探测器的事件库进行统一升级的功能。

7.3.1.5 检测结果处理要求

7.3.1.5.1 事件记录

a) 测试评价方法：

1） 检查系统是否具有记录事件的数据库，系统应记录并保存检测到的入侵事件；

2） 检查数据库是否具有维护功能。

b) 测试评价结果：

1） 系统具有记录事件的数据库。列举系统支持的数据库类型；

2） 具有数据库的自动或手工维护功能；

3） 记录的入侵事件信息应包含以下内容：事件发生时间、源地址、目的地址、危害等级、事

件详细描述以及解决方案建议等。

7.3.1.5.2 事件可视化

a) 测试评价方法：

1）登录控制台界面；

2）检查通过界面，是否可以实时、清晰地查看到正在发生的入侵事件；

3）触发一定的安全事件，查看报警界面的显示信息是否分级别显示。

b) 测试评价结果：

1）具有查看入侵事件的图形化界面；

2）显示界面具备清晰的功能区域，显示的信息包括事件名称、事件类型、事件级别、协议类型、发生时间、响应方式、相关参数，以及源和目的 IP 地址、MAC 地址、端口号等内容；

3）报警信息可以分为不同级别（如高、中、低等）显示。

7.3.1.5.3 报告生成

a) 测试评价方法：

1）查看报告生成功能，查看报告的生成方式；

2）查看生成报告的内容。

b) 测试评价结果：

1）具有生成报告的功能；

2）提供默认的模板以供快速生成报告；

3）生成的报告包含表格形式、柱状图、饼图等，并可生成日报、周报等汇总报告。

7.3.1.5.4 报告查阅

a) 测试评价方法：**检查系统提供的查阅、浏览检测结果报告的功能。**

b) 测试评价结果：

1）提供查阅、浏览检测结果报告的功能；

2）可以根据事件名称、IP 地址、时间等条件进行查询。

7.3.1.5.5 报告输出

a) 测试评价方法：

1）检查报告是否可输出；

2）检查系统支持的输出格式。

b) 测试评价结果：

1）系统提供输出检测结果报告的功能；

2）报告应可输出成方便用户阅读的格式，如字处理文件、HTML 文件、文本文件等；

3）报告最好为中文。

7.3.1.6 产品灵活性要求

7.3.1.6.1 报告定制

a) 测试评价方法：**查看系统设置，是否支持报告内容的自定义。**

b) 测试评价结果：

1）系统允许用户定制报告类别、报告内容、报告风格等内容；

2）列举系统支持的定制内容。

7.3.1.7 主机型入侵检测系统性能要求

7.3.1.7.1 稳定性

a) 测试评价方法：**连续运行主机型入侵检测系统至少 7 天，检查是否造成被检测主机停机或死机。**

b) 测试评价结果：**在主机正常工作状态下，系统应工作稳定，不应造成被检测主机停机或死机现象。**

7.3.1.7.2 CPU 资源占用量

a) 测试评价方法：

1）打开 CPU 监测工具（如 windows 平台的任务管理器等）；

2）运行主机型入侵检测系统的多项主要功能，记录在各种操作下 CPU 的利用情况。

b) 测试评价结果：**CPU 占有率不应明显影响主机的正常工作。**

7.3.1.7.3 内存占用量

a) 测试评价方法：

1）打开内存监测工具；

2）运行主机型入侵检测系统的多项主要功能，记录在各种操作下内存的利用情况。

b) 测试评价结果：**系统占用内存空间应在可接受的范围之内。**

7.3.1.7.4 用户登录和资源访问

a) 测试评价方法：

1）打开主机型入侵检测系统的网络访问监测和文件检测功能；

2）对被检测的主机进行合法用户登录（本地及远程）、合法文件访问等操作，检查是否能够顺利完成。

b) 测试评价结果：**系统不应影响所在目标主机上的合法用户登录及文件资源访问。**

7.3.1.7.5 网络通信

a) 测试评价方法：

1）打开主机型入侵检测系统的网络访问监控功能；

2）对被检测的主机进行一系列的远程通信操作，检查是否能够顺利完成。

b) 测试评价结果：**系统不应影响所在目标主机上的正常网络通信。**

7.3.1.8 网络型入侵检测系统性能要求

7.3.1.8.1 误报率

a) 测试评价方法：

1）在指定的网络带宽（百兆网络、千兆网络、或厂商声明的其它网络带宽）测试环境下，分别以 64 字节、128 字节、512 字节、1518 字节大小的 TCP 数据包作为背景流量数据包，分别以满负荷背景流量的 25%、50%、75%、99%作为背景流量强度，随机选择攻击的源地址、目的地址和端口，测试产品探测器在各环境下对网络数据包的最大收集能力。可测试多次取平均值，以 PPS（每秒能够处理的数据包个数）为单位记录；

2）在指定的网络带宽（百兆网络、千兆网络、或厂商声明的其它网络带宽）测试环境下，分别以 64 字节、128 字节、512 字节、1518 字节大小的 UDP 数据包作为背景流量数据包，分别以满负荷背景流量的 25%、50%、75%、99%作为背景流量强度，随机选择攻击的源地址、目的地址和端口，测试产品探测器在各环境下对网络数据包的最大收集能力。可测试多次取平均值，以 PPS（每秒能够处理的数据包个数）为单位记录；

3）在指定的网络带宽（百兆网络、千兆网络、或厂商声明的其它网络带宽）测试环境下，用模拟的真实网络数据包作为背景流量数据包，分别以满负荷背景流量的 25%、50%、75%、99%作为背景流量强度，随机选择攻击的源地址、目的地址和端口，测试产品探测器在各环境下对网络数据包的最大收集能力。可测试多次取平均值，以 PPS（每秒能够处理的数据包个数）为单位记录；

4）在指定的网络带宽（百兆网络、千兆网络、或厂商声明的其它网络带宽）测试环境下，测试系统分别针对 TCP 和 HTTP 协议能够建立的真实会话连接数。可测试多次取平均值，

以每秒能够建立的连接数为单位记录；

5）利用误报测试工具或通过人工构造数据包的方式，生成虚假的攻击包，查看网络型入侵检测系统是否报警；

6）依据已有的事件库，生成多个已知的攻击事件，查看网络型入侵检测系统是否正确报告出了事件名称。

b) 测试评价结果：

1）记录在指定的网络带宽背景流量下，系统能够处理的 TCP 数据包的最大值；

2）记录在指定的网络带宽背景流量下，系统能够处理的 UDP 数据包的最大值；

3）记录在指定的网络带宽背景流量下，系统能够处理的真实模拟的网络数据包的最大值；

4）记录系统分别针对 TCP 和 HTTP 协议能够建立的真实会话连接的最大值。

5）对虚假的攻击包，网络型入侵检测系统不应该报警，如果有报警，则该条报警就是误报；

6）对已知的攻击，系统所报告的入侵事件名称应正确无误，否则即为误报；

7）记录测试的事件总数量和系统的误报数量。

7.3.1.8.2 漏报率

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，发送攻击事件测试集中的所有事件，记录系统的检测结果；

2）可选取部分攻击事件作为测试基线；选取 64 字节、128 字节、512 字节、1518 字节大小的数据包作为背景流量，分别以满负荷背景流量的 25％、50％、75％、99％作为背景流量强度，将选取的基线攻击发送多次（如 100 次），记录系统的检测结果。

b) 测试评价结果：

1）对攻击事件测试集的所有攻击，系统应报告相应的入侵事件，未报告的事件即为漏报；

2）对测试基线的事件，系统应检测到相应的攻击次数（如 100 次）并报告，未报告的事件即为漏报；

3）记录测试的事件总数量（总发送次数）和系统漏报的攻击数量。

7.3.2 产品安全测试

7.3.2.1 身份鉴别

7.3.2.1.1 用户鉴别

a) 测试评价方法：登录系统，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。

7.3.2.1.2 鉴别失败的处理

a) 测试评价方法：

1）检查系统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）检查系统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（如锁定该帐号）；

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，系统是否采取了相应的措施，并生成了审计事件。

b) 测试评价结果：

1）系统应具备定义用户鉴别尝试的最大允许失败次数的功能；

2）系统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（如锁定该帐号）；

3）当用户鉴别尝试失败连续达到指定次数后，系统应锁定该帐号，并将有关信息生成审计事

件；

4） 最多失败次数仅由授权管理员设定。

7.3.2.2 用户管理

7.3.2.2.1 用户角色

a) 测试评价方法：检查系统的安全功能是否允许定义多个角色的用户。

b) 测试评价结果：

1） 系统应允许定义多个角色的用户；

2） 每个角色可以具有多个用户，每个用户只能属于一个角色；

3） 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。

7.3.2.3 事件数据安全

7.3.2.3.1 安全数据管理

a) 测试评价方法：模拟授权与非授权角色访问事件数据，产品安全功能是否仅允许授权角色访问事件数据。

b) 测试评价结果：系统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角色之外，系统应禁止所有其它用户对事件数据的访问。

7.3.2.3.2 数据保护

a) 测试评价方法：连续运行系统至少 48 小时，并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，进行测试，检查系统的事件数据是否出现丢失现象。

b) 测试评价结果：系统能够完整保留已经保存的事件数据。

7.3.2.4 通信安全

7.3.2.4.1 通信完整性

a) 测试评价方法：

1） 在系统的各组件中传输配置和控制信息、告警和事件数据等信息，检查接收是否正常；

2） 检查开发者文档中对保证各组件之间通信完整性的描述。

b) 测试评价结果：

1） 系统应在各组件之间传输的数据（如配置和控制信息、告警和事件数据等）时，数据能够被正常传输；

2） 开发者文档中提供了为保证各组件之间通信完整性所采取措施的详细描述，数据在传输过程中不丢失、不被篡改。列举系统为保证通信完整性所采取的措施。

7.3.2.4.2 通信稳定性

a) 测试评价方法：

1） 在系统的各部件和控制台之间传递信息，人为制造网络故障，检查信息传递是否正常；

2） 检查开发者文档中对保证各部件和控制台之间传递信息的通信稳定性的描述。

b) 测试评价结果：

1） 系统在各部件和控制台之间传递信息时，不因网络故障而丢失或延迟，数据能够被正常传输；

2） 开发者文档中提供了为保证通信稳定性所采取措施的详细描述。列举系统为保证通信稳定性所采取的措施。

7.3.2.4.3 升级安全

a) 测试评价方法：

1） 尝试用系统所允许的各种方法升级事件库和系统软件版本，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） 系统能够利用其提供的各种方法正常升级事件库和系统软件版本；

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） 列举系统提供的事件库和版本升级手段。

7.3.2.5 产品自身安全

7.3.2.5.1 自我隐藏

a) 测试评价方法：检查开发者文档中对网络型入侵检测系统自身安全的描述。

b) 测试评价结果：网络型入侵检测系统应采取隐藏探测器 IP 地址等措施使自身在网络上不可见。

7.3.2.5.2 自我保护

a) 测试评价方法：检查开发者文档中对主机型入侵检测系统自身安全的描述。

b) 测试评价结果：主机型入侵检测系统应具有自我保护功能，能够防止程序被非法终止、被非法设置停止告警等行为。

7.3.3 产品保证测试

7.3.3.1 配置管理

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，从而对系统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。

7.3.3.2 交付与运行

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系统的安装、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。

7.3.3.3 安全功能开发

7.3.3.3.1 功能设计

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系统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。

7.3.3.3.2 表示对应性

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，系统各种安全功能表示（如系统功能设计、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、底层设计、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。

7.3.3.4 文档要求

7.3.3.4.1 管理员指南

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） 系统可以使用的管理功能和接口；

2） 怎样安全地管理系统；

3） 在安全处理环境中应进行控制的功能和权限；

4） 所有对与系统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。

7.3.3.4.2 用户指南

a) 测试评价方法：

评价者应审查开发者是否提供了供系统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） 系统的非管理用户可使用的安全功能和接口；

2） 系统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） 系统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。

7.3.3.5 开发安全要求

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，开发环境的温室度要求和记录，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：对系统代码、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。

7.3.3.6 测试

7.3.3.6.1 范围

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。

7.3.3.6.2 功能测试

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（这些概况包括对其它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。

7.4 第二级

7.4.1 产品功能测试

7.4.1.1 入侵分析功能测试

7.4.1.1.1 防躲避能力

a) 测试评价方法：

1）利用入侵检测躲避工具进行攻击，测试系统是否对攻击进行报警；

2）将攻击事件的协议端口进行重定位，检查系统是否对攻击进行报警。

b) 测试评价结果：

1）系统能够检测出经过分片、乱序之后的攻击事件；

2）系统能够正确地报出经过规避的扫描 HTTP 事件；

3）系统能够对重定位协议端口之后的攻击进行报警。

7.4.1.1.2 事件合并

a) 测试评价方法：

1）连续触发同一条事件，查看报警显示的情况，是否是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，如只显示报警信息的事件名称、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：

1）可以根据需要进行同类事件的合并；

2）可以按照设置显示报警信息的事件名称、发生的次数、源 IP 等信息。

7.4.1.2 入侵响应功能测试

7.4.1.2.1 排除响应

a) 测试评价方法：

1）打开菜单，检查系统是否允许用户设置对被检测网段中指定的主机或特定的事件不予告警；

2）设置事件过滤条件，将某条不关心的事件在显示信息中过滤掉。

b) 测试评价结果：用户可以定制不监控符合指定条件的主机或特定的事件。

7.4.1.2.2 定制响应

a) 测试评价方法：

1）网络型入侵检测系统应允许用户对被检测网段中指定的主机或特定的事件定制不同的响应方式，以对特定的事件突出告警；

2）打开菜单，检查系统是否允许用户设置仅对被检测网段中指定的主机或特定的事件进行告警。

b) 测试评价结果：**用户可以定制仅监控符合指定条件的主机或特定的事件。**

7.4.1.2.3 防火墙联动

a) 测试评价方法：

1）检查系统的响应策略配置界面是否具有防火墙联动选项；

2）配置防火墙联动策略；

3）检查系统在监测到相应攻击时是否与防火墙进行了联动。

b) 测试评价结果：

1）能够与防火墙联动，在发生指定的安全事件时，成功地按照设定的联动策略自动调整防火墙配置；

2）列举系统支持的防火墙联动协议；

3）列举系统已经实现联动的防火墙品牌。

7.4.1.3 管理控制功能测试

7.4.1.3.1 分布式部署

a) 测试评价方法：**配置系统的分布式部署模式，测试系统是否能够部署在本地或异地的至少两个子网内，在网络连通的情况下是否可以统一管理探测器。**

b) 测试评价结果：

1）可以正常配置至少两个子网的系统部署结构；

2）分布式部署的探测器可被控制台统一管理。

7.4.1.3.2 集中管理

a) 测试评价方法：

1）部署至少 2 个控制台；

2）选取至少一个控制台，为其部署至少 2 个探测器；

3）检查控制台是否可以同时管理并设置所有下级控制台和探测器，查看是否有可以显示部署情况的信息（如拓扑图）。

b) 测试评价结果：

1）控制台可以管理所有为其部署的探测器；

2）总控制台可以管理其下级控制台，形成多级管理结构；

3）可以正确显示系统部署的拓扑。

7.4.1.3.3 同台管理

a) 测试评价方法：**同时部署同一个厂家的网络型入侵检测系统和主机型入侵检测系统（如果同时提供），检查是否能被同一个控制台进行管理；**

b) 测试评价结果：**同一厂家的网络型入侵检测系统和主机型入侵检测系统能够被同一个控制台进行管理。**

7.4.1.3.4 端口分离

a) 测试评价方法：**检查网络型入侵检测系统是否配备进行产品管理和网络数据监听的端口。**

b) 测试评价结果：**系统的产品管理端口和网络数据监听端口是不同的端口，且均能正常工作。**

7.4.1.4 产品灵活性要求

7.4.1.4.1 窗口定义

a) 测试评价方法：

1）查看系统设置，是否支持自定义窗口模式；

2）指定一个服务器地址，单独定义一个界面将所有目的地址为这个服务器的安全事件显示在这个界面中。

b) 测试评价结果：

1）系统允许用户定制窗口的显示方式、布局等；

2）用户可以自己定制只显示某一地址的报警界面。

7.4.1.4.2 事件定义

a) 测试评价方法：

1）查看系统设置，是否提供自定义事件界面，是否允许基于系统默认事件修改生成新的事件；

2）自定义生成新的事件；

3）按照新生成的事件发送相应的攻击事件，检查系统能否报警。

b) 测试评价结果：

1）系统允许用户自定义事件，或者可基于系统默认事件修改生成新的事件；

2）系统能够检测到新定义的事件并报警。

7.4.1.4.3 协议定义

a) 测试评价方法：

1）查看系统设置，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；

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攻击事件，检查系统能否报警。

b) 测试评价结果：

1）系统允许用户自定义协议，或者可基于系统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）系统能够检测到新定义的协议事件并报警。

7.4.1.4.4 通用接口

a) 测试评价方法：

1）查看系统，是否在设置与防火墙等安全设备的联动策略时明确支持了共享或联动协议；

2）可提供系统自己定义的对外开放通用接口，以支持与其它安全设备的共享信息或规范化联动。

b) 测试评价结果：

1）系统支持一个或多个共享或联动接口协议，其中可包括系统自己定义的对外通用接口；

2）系统支持与网络管理软件、防火墙等设备的共享信息或规范化联动；

3）列举系统支持的所有通用接口。

7.4.2 产品安全测试

7.4.2.1 身份鉴别

7.4.2.1.1 超时设置

a) 测试评价方法：

1）检查系统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，系统是否终止了会话，用户是否需要再次进行身份鉴别才能够重新管理和使用系统。

b) 测试评价结果：

1）系统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系统；

3）最大超时时间仅由授权管理员设定。

7.4.2.1.2 会话锁定

a) 测试评价方法：**登录系统，检查是否允许用户锁定自己的交互会话。锁定后是否需要再次进行身份鉴别才能够重新管理系统。**

b) 测试评价结果：

1）系统应允许用户锁定自己的交互会话；

2）锁定后，用户需要再次进行身份鉴别才能够重新管理系统。

7.4.2.2 用户管理

7.4.2.2.1 用户属性定义

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：**系统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、其它安全属性等。输入的用户信息无丢失现象发生。**

7.4.2.2.2 安全行为管理

a) 测试评价方法：

1）检查系统的安全功能是否明确规定仅限于指定的授权角色对系统的功能具有禁止、修改的能力；

2）检查指定的授权角色对系统的功能进行禁止、修改等操作前，是否先登录才能操作。

b) 测试评价结果：

1）系统应仅限于已识别了的指定的授权角色对系统的功能进行禁止、修改；

2）指定的授权角色对系统的功能进行禁止、修改等操作前，应先登录才能操作。

7.4.2.3 安全审计

7.4.2.3.1 审计数据生成

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系统不同模块进行访问、运行、修改、关闭以及重复失败尝试等相关操作，检查系统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）系统应至少为下述可审计事件产生审计记录：审计功能的启动和关闭，鉴别失败等重大事件等；

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。

7.4.2.3.2 审计数据可用性

a) 测试评价方法：**审查产品安全功能是否使审计记录中的所有审计数据可为人所理解（至少包括能为人理解的描述内容以及审计数据本身）。**

b) 测试评价结果：**系统应提供为人理解的审计记录。**

7.4.2.3.3 审计查阅

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。**

b) 测试评价结果：**系统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。**

7.4.2.3.4 受限的审计查阅

a) 测试评价方法：模拟授权与非授权管理员访问审计记录，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：系统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，系统应禁止所有其它用户对审计记录的读访问。

7.4.2.4 产品自身安全

7.4.2.4.1 自我监测

a) 测试评价方法：

1）检查开发者文档中对网络型入侵检测系统自身安全的描述；

2）检查网络型入侵检测系统探测器是否在启动和正常工作时能够周期性地、或者按照授权管理员的要求执行自检。

b) 测试评价结果：网络型入侵检测系统在启动和正常工作时，应周期性地、或者按照授权管理员的要求执行自检。

7.4.3 产品保证测试

7.4.3.1 配置管理

7.4.3.1.1 配置管理能力

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）开发者应使用配置管理系统并提供配置管理文档，以及为系统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系统的配置项。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地维护的证据。

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。

7.4.3.1.2 配置管理范围

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：

系统配置管理范围，要求将系统的实现表示、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。为此要求：

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。

7.4.3.2 交付与运行

7.4.3.2.1 交付

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系统，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） 在给用户方交付系统的各版本时，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）。**

7.4.3.2.2 安装生成

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系统的安装、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。

7.4.3.3 安全功能开发

7.4.3.3.1 功能设计

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系统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。

7.4.3.3.2 高层设计

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） 系统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系统安全要求；

4） 系统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，并把这些相互关系将适当地作为数据流、控制流等的外部接口来表示；

5） 高层设计应当标识系统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。**

7.4.3.3.3 表示对应性

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，系统各种安全功能表示（如系统功能设计、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、底层设计、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。

7.4.3.4 文档要求

7.4.3.4.1 管理员指南

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） 系统可以使用的管理功能和接口；
2） 怎样安全地管理系统；
3） 在安全处理环境中应进行控制的功能和权限；
4） 所有对与系统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。

7.4.3.4.2 用户指南

a) 测试评价方法：

评价者应审查开发者是否提供了供系统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） 系统的非管理用户可使用的安全功能和接口；
2） 系统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） 系统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。

7.4.3.5 开发安全要求

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，开发环境的温室度要求和记录，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：对系统代码、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。

7.4.3.6 测试

7.4.3.6.1 范围

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。**

7.4.3.6.2 测试深度

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。**

7.4.3.6.3 功能测试

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（这些概况包括对其它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。

7.4.3.6.4 独立性测试

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系统，且提供的系统是否适合测试。**

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系统。**

7.4.3.7 脆弱性评定

7.4.3.7.1 指南检查

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，是否确定了对系统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。**

7.4.3.7.2 脆弱性分析

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，对系统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系统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。**

7.5 第三级

7.5.1 产品功能测试

7.5.1.1 入侵分析功能测试

7.5.1.1.1 事件关联

a) 测试评价方法：**连续生成多个低风险的事件，如：在单位时间内多次尝试登录服务器失败，查看系统是否进行报警。**

b) 测试评价结果：**系统可以对看似无关的同类事件进行报警。**

7.5.1.2 入侵响应功能测试

7.5.1.2.1 全局预警

a) 测试评价方法：

1）打开菜单，检查系统是否具有进行全局预警的功能设置；

2）设置全局预警功能，在某下级控制台触发一条全局预警事件，查看上级控制台及其它控制台是否可以收到预警信息。

b) 测试评价结果：

1）具有全局预警功能；

2）上级控制台可以向下级控制台发送预警信息，下级控制台可以接收到上级下发的预警信息。

7.5.1.2.2 入侵管理

a) 测试评价方法：

1）网络型入侵检测系统应具有全局安全事件的管理能力，可与安全管理中心或网络管理中心进行联动；

2）检查系统的响应策略配置界面是否具有安全管理中心或网络管理中心联动选项；

3）配置安全管理中心或网络管理中心联动策略；

4）检查系统在监测到相应攻击时是否向安全管理中心或网络管理中心发送通知。

b) 测试评价结果：

1）具备与安全管理中心或网络管理中心联动选型；

2）能够在发生指定的安全事件时，向安全管理中心或网络管理中心发送相关信息；

3）列举系统支持的联动协议，以及已经实现联动的安全管理中心或网络管理中心品牌。

7.5.1.2.3 其它设备联动

a) 测试评价方法：

1）查看系统是否具有与其它网络设备和网络安全部件（如漏洞扫描，交换机）按照设定的策略进行联动的设置；

2）设置联动策略；

3）检查系统是否能够与指定的网络安全部件进行联动。

b) 测试评价结果：

1）入侵检测与漏洞扫描的联动，可以将事件与漏洞扫描结果进行关联，调整风险值，对于有效的攻击给出较高的风险值，对于无效的攻击给出较低的风险值；

2）入侵检测与交换机的联动，可以通过重新配置交换机抵御确认的攻击；

3）检测到系统所声明的联动功能；

4）列举系统已经实现联动的网络设备和网络安全部件的品牌。

7.5.1.3 管理控制功能测试

7.5.1.3.1 多级管理

a) 测试评价方法：

1）配置多级管理模式，至少满足控制台——控制台（或探测器）——探测器的两级部署结构；

2） 上级控制台可以设置查看下级（控制台及探测器）上报哪些事件；查看是否有可以显示部署情况的信息（如拓扑图）；

3） 有选择地从下级控制台读取事件记录到上级控制台的数据库中。

b) 测试评价结果：

1） 可以正常配置至少两级的系统部署结构；

2） 可以正确显示系统部署的拓扑；

3） 上级控制台可以设置查看下级（控制台及探测器）上报的事件。

7.5.1.4 网络型入侵检测系统性能要求

7.5.1.4.1 还原能力

a) 测试评价方法：

1） 开启网络型入侵检测系统的内容还原（回放）功能，检查可还原的协议类型；

2） 在指定的网络带宽（百兆网络、千兆网络、或厂商声明的其它网络带宽）测试环境下，抽样测试还原的效果。

b) 测试评价结果：

1） 系统具有内容回放功能；

2） 对 HTTP、FTP、SMTP、POP3、Telnet 等可回放的网络协议通信，可以进行内容恢复和事件还原（回放）。

7.5.2 产品安全测试

7.5.2.1 身份鉴别

7.5.2.1.1 多鉴别机制

a) 测试评价方法：

1） 检查系统的安全功能是否提供多种鉴别方式；

2） 检查系统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） 系统应提供至少 2 种鉴别方式。列举系统提供或支持的所有鉴别方式；

2） 系统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。

7.5.2.1.2 鉴别数据保护

a) 测试评价方法：检查系统是否仅允许指定的角色查阅或修改身份鉴别数据。

b) 测试评价结果：系统应仅允许指定的角色查阅或修改身份鉴别数据。

7.5.2.2 用户管理

7.5.2.2.1 安全属性管理

a) 测试评价方法：

1） 检查系统的安全功能是否明确规定仅限于指定的授权角色对指定的安全属性进行查询、修改、删除、改变其默认值等操作；

2） 检查指定的授权角色对指定的安全属性进行查询、修改、删除、改变其默认值等操作前，是否先登录才能操作。

b) 测试评价结果：

1） 系统应仅限于已识别了的指定的授权角色对指定的安全属性进行查询、修改、删除、改变其默认值等操作；

2） 指定的授权角色对指定的安全属性进行查询、修改、删除、改变其默认值等操作前，应先登录才能操作。

7.5.2.3 事件数据安全

7.5.2.3.1 数据存储告警

a) 测试评价方法：

1）检查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）人为地将存储系统的事件数据存储器空间耗至设定的告警值以下，查看系统是否告警。

b) 测试评价结果：

1）系统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）系统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，系统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。

7.5.3 产品保证测试

7.5.3.1 配置管理

7.5.3.1.1 配置管理能力

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地维护的证据。

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。

7.5.3.1.2 配置管理范围

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）产品配置管理范围，要求将产品的实现表示、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。为此要求：

——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；

——文档应描述配置管理系统是如何跟踪这些配置项的；

——文档还应提供足够的信息表明达到所有要求。

2）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。

7.5.3.2 交付与运行

7.5.3.2.1 交付

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。**

7.5.3.2.2 安装生成

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。

7.5.3.3 安全功能开发

7.5.3.3.1 功能设计

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。

7.5.3.3.2 高层设计

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，并把这些相互关系将适当地作为数据流、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。

7.5.3.3.3 安全功能的实现

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。

7.5.3.3.4 低层设计

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它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它模块。

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。**

7.5.3.3.5 表示对应性

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、底层设计、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。

7.5.3.4 文档要求

7.5.3.4.1 管理员指南

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。

7.5.3.4.2 用户指南

a) 测试评价方法：

评价者应审查开发者是否提供了供系统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。

7.5.3.5 开发安全要求

7.5.3.5.1 开发安全

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，开发环境的温室度要求和记录，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。

7.5.3.6 测试

7.5.3.6.1 范围

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。

7.5.3.6.2 测试深度

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。

7.5.3.6.3 功能测试

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（这些概况包括对其它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。

7.5.3.6.4 独立性测试

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。

7.5.3.7 脆弱性评定

7.5.3.7.1 指南检查

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。**

7.5.3.7.2 脆弱性分析

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。

参考文献

[1] GB/T 18336.2-2001 信息技术 安全技术 信息技术安全性评估准则 第二部分：安全功能要求（idt ISO 15408-2:1999）

[2] GB/T 18336.3-2001 信息技术 安全技术 信息技术安全性评估准则 第三部分：安全保证要求（idt ISO 15408-3:1999）