ICS 35.040
L 80

中华人民共和国国家标准

GB/T 20275—2013
代替 GB/T 20275—2006

信息安全技术　网络入侵检测系统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 detection system

2013-12-31 发布　　2014-07-15 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。

本标准代替 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》。

本标准与 GB/T 20275—2006 的主要差异如下：

——标准名称修改为《信息安全技术 网络入侵检测系统技术要求和测试评价方法》；

——删除了 GB/T 20275—2006 中对主机入侵检测系统的技术要求和测试评价方法；

——删除了 GB/T 20275—2006 中的“分析方式”(见 2006 版的 6.1.1.2.2)；

——删除了 GB/T 20275—2006 中的“窗口定义”(见 2006 版的 6.2.1.4.1)；

——增加了“最大监控流量”“最大监控并发连接数”“最大监控新建 TCP 连接速率”的性能要求；

——增加了“硬件失效处理”“双机热备”的安全功能要求和测试评价方法；

——增加了“控制台鉴别”“标识唯一性”的自身安全功能要求和测试评价方法；

——调整了 GB/T 20275—2006 中“阻断能力”“系统升级”“报告定制”和“定制响应”的级别。

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。

本文件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、公安部网络安全保卫局。

本标准主要起草人：宋好好、顾健、张笑笑、李毅、吴其聪、张艳。

信息安全技术　网络入侵检测系统技术要求和测试评价方法

1　范围

本标准规定了网络入侵检测系统的技术要求和测试评价方法，要求包括安全功能要求、自身安全功能要求、安全保证要求和测试评价方法，并提出了网络入侵检测系统的分级要求。

本标准适用于网络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/T 18336.1—2008　信息技术　安全技术　信息技术安全性评估准则　第1部分：简介和一般模型

GB/T 25069—2010　信息安全技术　术语

3　术语和定义

GB/T 18336.1—2008 和 GB/T 25069—2010 中界定的以及下列术语和定义适用于本文件。

3.1

事件　event

一种系统、服务或网络状态的发生或者改变的记录信息，可作为分析安全事件的基础。

3.2

安全事件　incident

通过对事件的分析处理，从而识别出一种系统、服务或网络状态的发生，表明一次可能的违反安全规则或某些防护措施失效，或者一种可能与安全相关但以前不为人知的一种情况，极有可能危害业务运行和威胁信息安全。

3.3

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。

3.4

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。

3.5

网络入侵检测系统　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

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。

3.7

告警　alert

当攻击或入侵发生时，网络入侵检测系统向授权管理员发出的紧急通知。

3.8

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。

3.9

误报　false positives

网络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。

3.10

漏报　false negative

当攻击发生时网络入侵检测系统未告警。

4　缩略语

下列缩略语适用于本文件。

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：超文本置标语言(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)
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)
POP3：邮局协议的第三个版本(Post Office Protocol 3)
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：远程登陆网络(Telecommunication Network)
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　网络入侵检测系统等级划分

5.1　等级划分

5.1.1　第一级

本级规定了网络入侵检测系统的最低安全要求。通过简单的管理员标识和鉴别来限制对系统的功

能配置和数据访问的控制，使管理员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。本级还要求系统具有分布式部署、集中管理的能力。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较强的保护。本级还要求系统具有分级管理的能力。此外，还要求系统具有较强的抗攻击能力。

5.2 等级划分表

网络入侵检测系统的安全等级划分如表1、表2、表3所示。对网络入侵检测系统的等级评定是依据下面三个表格的综合评定得出的，符合第一级的网络入侵检测系统应满足表1、表2、表3中所标明的一级产品应满足的所有项目；符合第二级的网络入侵检测系统应满足表1、表2、表3中所标明的二级产品应满足的所有项目；符合第三级的网络入侵检测系统应满足表1、表2、表3中所标明的三级产品应满足的所有项目。

表1 网络入侵检测系统安全功能要求等级划分表

安全功能要求		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	*	*	*
	事件合并	*	*	*
	防躲避能力	—	*	*
	事件关联	—	*	*
入侵响应功能要求	安全告警	*	*	*
	告警方式	*	*	*
	定制响应	*	*	*
	排除响应	—	*	*
	全局预警	—	—	*
	阻断能力	—	*	*
	防火墙联动	—	*	*
	入侵管理	—	—	*
	其他设备联动	—	—	*

表 1（续）

安全功能要求		一级	二级	三级
管理控制功能要求	图形界面	*	*	*
	分布式部署	—	*	*
	分级管理	—	—	*
	集中管理	—	*	*
	同台管理	—	*	*
	端口分离	—	*	*
	硬件失效处理	*	*	*
	双机热备	—	*	*
	事件数据库	*	*	*
	事件分级	*	*	*
	策略配置	*	*	*
	事件库升级	*	*	*
	统一升级	*	*	*
	系统升级	—	*	*
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	报告定制	—	*	*
	事件定义	—	*	*
	协议定义	—	*	*
性能要求	误报率	*	*	*
	漏报率	*	*	*
	流量监控能力	*	*	*
	并发连接数监控能力	*	*	*
性能要求	新建 TCP 连接速率监控能力	*	*	*
	还原能力	—	—	*

注：“—”表示不具有该要求；“*”表示具有该要求。本标准对网络入侵检测系统每一等级的具体要求和测试评价方法分别进行描述，“**加粗宋体**”表示第二级、第三级增加的内容，“系统”表示网络入侵检测系统。

表 2　网络入侵检测系统自身安全功能要求等级划分表

自身安全功能要求		一级	二级	三级
身份鉴别	管理员鉴别	*	*	*
	多重鉴别机制	—	—	*
	鉴别失败的处理	*	*	*
	超时设置	—	*	*
	控制台鉴别	—	*	*
	会话锁定	—	—	*
	鉴别数据保护	*	*	*
管理员管理	标识唯一性	*	*	*
	管理员角色	—	*	*
	管理员属性定义	*	*	*
	安全行为管理	*	*	*
	安全属性管理	—	*	*
安全审计	审计日志生成	*	*	*
	审计日志可理解性	*	*	*
	审计日志查阅	*	*	*
	受限的审计日志查阅	*	*	*
	可选审计查阅	*	*	*
事件记录安全	安全管理	*	*	*
	事件记录保护	*	*	*
	事件记录存储安全	—	*	*
	数据存储告警	—	—	*
通信安全	通信保密性	*	*	*
	通信完整性	—	*	*
升级安全		—	*	*
运行安全	自我隐藏	*	*	*
	自我监测	—	*	*

注：“—”表示不具有该要求；“*”表示具有该要求。本标准对网络入侵检测系统每一等级的具体要求和测试评价方法分别进行描述，“**加粗宋体**”表示第二级、第三级增加的内容，“系统”表示网络入侵检测系统。

表 3　网络入侵检测系统安全保证要求等级划分表

安全保证要求			一级	二级	三级
配置管理	配置管理能力	版本号	*	*	*
		配置项	—	*	*
		授权控制	—	—	*
	配置管理覆盖		—	—	*
交付与运行	交付程序		—	*	*
	安装、生成和启动程序		*	*	*
开发	非形式化功能规范		*	*	*
	高层设计	描述性高层设计	—	*	*
		安全加强的高层设计	—	—	*
	非形式化对应性证实		*	*	*
指导性文档	管理员指南		*	*	*
	用户指南		*	*	*
生命周期支持			—	—	*
测试	测试覆盖	覆盖证据	—	*	*
		覆盖分析	—	—	*
	测试深度		—	—	*
	功能测试		—	*	*
	独立测试	一致性	*	*	*
		抽样	—	*	*
脆弱性分析保证	指南审查		—	—	*
	产品安全功能强度评估		—	*	*
	开发者脆弱性分析		—	*	*

注：“—”表示不具有该要求；“*”表示具有该要求。本标准对网络入侵检测系统每一等级的具体要求和测试评价方法分别进行描述，“**加粗宋体**”表示第二级、第三级增加的内容，“系统”表示网络入侵检测系统。

6　网络入侵检测系统技术要求

6.1　第一级

6.1.1　安全功能要求

6.1.1.1　数据探测功能要求

6.1.1.1.1　数据收集

系统应具有实时获取受保护网段内的数据包的能力用于检测分析。

6.1.1.1.2 协议分析

系统至少应分析基于以下协议的事件：IP、TCP、UDP、ICMP、ARP、RIP、、RPC、HTTP、FTP、TFTP、IMAP、SNMP、TELNET、DNS、SMTP、POP3、NETBIOS、NFS 等。

6.1.1.1.3 行为监测

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、文件脆弱性攻击、浏览器脆弱性攻击、应用层安全漏洞攻击等。

6.1.1.1.4 流量监测

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

系统应对收集的数据包进行分析，发现安全事件。

6.1.1.2.2 事件合并

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。

6.1.1.3 入侵响应功能要求

6.1.1.3.1 定制响应

系统应允许管理员对被检测网段中指定的目的主机定制不同的响应方式。

6.1.1.3.2 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。

6.1.1.3.3 告警方式

告警应采取屏幕实时提示、E-mail 告警、Syslog 告警等一种或几种方式。

6.1.1.4 管理控制功能要求

6.1.1.4.1 图形界面

系统应提供友好的管理员界面用于管理、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

系统事件数据库中的内容应包括事件的定义和分析内容、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

系统应提供方便、快捷的入侵检测系统策略配置方法和手段，具备策略模板、支持策略的导入和

导出。

6.1.1.4.5 事件库升级

系统应具有升级事件库的能力。

6.1.1.4.6 统一升级

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。

6.1.1.4.7 硬件失效处理

对于硬件产品，系统失效时应及时向管理员报警。

6.1.1.5 检测结果处理要求

6.1.1.5.1 事件记录

系统应保存检测到的安全事件并记录安全事件信息。

安全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、事件等级、事件类型、事件名称、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

管理员应能通过管理界面实时清晰地查看安全事件。

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管理员阅读的文本格式，如 WORD 文件、HTML 文件、文本文件等。

6.1.1.6 性能要求

6.1.1.6.1 误报率

产品应将误报率控制在应用许可的范围 15%内，不能对正常使用产品产生较大影响。

6.1.1.6.2 漏报率

系统应将漏报率控制在应用许可的范围 15%内，不能对正常使用产品产生较大影响。

6.1.1.6.3 流量监控能力

百兆系统单口监控流量≥90 Mbit/s，千兆系统单口监控流量≥0.9 Gbit/s，万兆系统单口监控流量≥9 Gbit/s。

6.1.1.6.4 并发连接数监控能力

百兆系统单口监控并发连接数≥10 万个，千兆系统单口监控并发连接数≥100 万个，万兆系统单口

监控并发连接数≥150 万个。

6.1.1.6.5 新建 TCP 连接速率监控能力

百兆系统单口监控每秒新建 TCP 连接数≥6 万个，千兆系统单口监控每秒新建 TCP 连接数≥10 万个，万兆系统单口监控每秒新建 TCP 连接数≥15 万个。

6.1.2 自身安全功能要求

6.1.2.1 身份鉴别

6.1.2.1.1 管理员鉴别

系统应在管理员执行任何与安全功能相关的操作之前对管理员进行鉴别。

6.1.2.1.2 鉴别失败的处理

当管理员鉴别尝试失败连续达到指定次数后，系统应阻止管理员进一步的鉴别请求，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。

6.1.2.1.3 鉴别数据保护

系统应保护鉴别数据不被未授权查阅和修改。

6.1.2.2 管理员管理

6.1.2.2.1 标识唯一性

系统应保证所设置的管理员标识全局唯一。

6.1.2.2.2 管理员属性定义

系统应为每一个管理员保存安全属性表，属性应包括管理员标识、鉴别数据、授权信息或管理组信息、其他安全属性等。

6.1.2.2.3 安全行为管理

系统应仅允许授权管理员对产品的功能具有禁止、修改的能力。

6.1.2.3 安全审计

6.1.2.3.1 审计日志生成

应能为下述可审计事件产生审计日志：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。

6.1.2.3.2 审计日志可理解性

审计数据的记录方式应便于管理员理解。

6.1.2.3.3 审计日志查阅

系统应为授权管理员提供提供审计日志查阅功能，方便管理员查看审计结果。

6.1.2.3.4 受限的审计日志查阅

除了具有明确的访问权限的授权管理员之外，系统应禁止所有其他用户对审计日志的访问。

6.1.2.3.5 可选审计查阅

应支持按照一定条件对审计日志进行检索或排序。

6.1.2.4 事件记录安全

6.1.2.4.1 安全管理

系统应仅允许授权管理员访问事件记录，禁止其他用户对事件记录的操作。

6.1.2.4.2 事件记录保护

在事件记录遭受攻击时，系统应能够及时通知管理员。

6.1.2.5 通信安全

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。

6.1.2.6 运行安全

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。

6.1.3 安全保证要求

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。

6.1.3.2 交付与运行

开发者应提供文档说明系统的安装、生成和启动的过程。

6.1.3.3 开发

6.1.3.3.1 非形式化功能规范

开发者应提供一个功能规范，功能规范应满足以下要求：

a) 使用非形式化风格来描述系统安全功能及其外部接口；

b) 是内在一致的；

c) 描述所有外部接口的用途与使用方法，适当时应提供效果、例外情况和错误消息的细节；

d) 完备地表示系统安全功能。

6.1.3.3.2 非形式化对应性证实

开发者应提供系统安全功能表示的所有相邻对之间提供对应性分析。

对于系统安全功能所表示的每个相邻对，分析应阐明，较为抽象的安全功能表示的所有相关安全功能，应在较具体的安全功能表示中得到正确且完备地细化。

6.1.3.4 文档要求

6.1.3.4.1 管理员指南

开发者应提供管理员指南，管理员指南应与为评估而提供的其他所有文档保持一致。

管理员指南应说明以下内容：

a) 管理员可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被控制的功能和权限；

d) 所有对与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实体的安全特性进行的改变；

g) 所有与管理员有关的 IT 环境安全要求。

6.1.3.4.2 用户指南

开发者应提供用户指南，用户指南应与为评估而提供的其他所有文档保持一致。

用户指南应说明以下内容：

a) 产品的非管理员用户可使用的安全功能和接口；

b) 产品提供给用户的安全功能和接口的使用方法；

c) 用户可获取但应受安全处理环境所控制的所有功能和权限；

d) 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。

6.1.3.5 测试

开发者应提供适合测试的系统，提供的测试集合应与其自测系统功能时使用的测试集合相一致。

6.2 第二级

6.2.1 安全功能要求

6.2.1.1 数据探测功能要求

6.2.1.1.1 数据收集

系统应具有实时获取受保护网段内的数据包的能力用于检测分析。

6.2.1.1.2 协议分析

系统至少应分析基于以下协议的事件：IP、TCP、UDP、ICMP、ARP、RIP、RPC、HTTP、FTP、TFTP、IMAP、SNMP、TELNET、DNS、SMTP、POP3、NETBIOS、NFS 等。

6.2.1.1.3 行为监测

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、文件脆弱性攻击、浏览器脆弱性攻击、应用层安全漏洞攻击等。

6.2.1.1.4 流量监测

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。

6.2.1.2 入侵分析功能要求

6.2.1.2.1 数据分析

系统应对收集的数据包进行分析，发现安全事件。

6.2.1.2.2 事件合并

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。

6.2.1.2.3 防躲避能力

系统应能发现躲避或欺骗检测的行为，如 IP 碎片分片、TCP 流分段、URL 字符串变形、shell 代码变形等。

6.2.1.2.4 事件关联

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。

6.2.1.3 入侵响应功能要求

6.2.1.3.1 定制响应

系统应允许管理员对被检测网段中指定的目的主机定制不同的响应方式。

6.2.1.3.2 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。

6.2.1.3.3 告警方式

告警应采取屏幕实时提示、E-mail 告警、Syslog 告警等一种或几种方式。

6.2.1.3.4 阻断能力

系统在监测到网络上的非法连接时，可进行阻断。

6.2.1.3.5 排除响应

系统应允许管理员定义对被检测网段中指定的目的主机不予告警。

6.2.1.3.6 防火墙联动

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。

6.2.1.4 管理控制功能要求

6.2.1.4.1 图形界面

系统应提供友好的管理员界面用于管理、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。

6.2.1.4.2 事件数据库

系统事件数据库中的内容应包括事件的定义和分析内容、详细的漏洞修补方案、可采取的对策等。

6.2.1.4.3 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。

6.2.1.4.4 策略配置

系统应提供方便、快捷的入侵检测系统策略配置方法和手段，具备策略模板、支持策略的导入和导出。

6.2.1.4.5 事件库升级

系统应具有升级事件库的能力。

6.2.1.4.6 统一升级

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。

6.2.1.4.7 硬件失效处理

对于硬件产品，系统失效时应及时向管理员报警。

6.2.1.4.8 分布式部署

系统应具有分布式部署的能力。

6.2.1.4.9 集中管理

系统应设置集中管理中心，对分布式的入侵检测系统进行统一集中管理。

6.2.1.4.10 端口分离

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。

6.2.1.4.11 双机热备

对于硬件产品，系统应提供双机热备功能。

6.2.1.4.12 系统升级

系统应具有升级系统程序的能力。

6.2.1.5 检测结果处理要求

6.2.1.5.1 事件记录

系统应保存检测到的安全事件并记录安全事件信息。

安全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、事件等级、事件类型、事件名称、事件详细描述以及解决方案建议等。

6.2.1.5.2 事件可视化

管理员应能通过管理界面实时清晰地查看安全事件。

6.2.1.5.3 报告生成

系统应能生成详尽的检测结果报告。

6.2.1.5.4 报告查阅

系统应具有浏览检测结果报告的功能。

6.2.1.5.5 报告输出

检测结果报告应可输出成方便管理员阅读的文本格式，如 WORD 文件、HTML 文件、文本文件等。

6.2.1.6 产品灵活性要求

6.2.1.6.1 报告定制

系统应支持授权管理员定制报告内容。

6.2.1.6.2 事件定义

系统应允许授权管理员自定义事件，并应提供方便、快捷的定义方法。

6.2.1.6.3 协议定义

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。

6.2.1.7 性能要求

6.2.1.7.1 误报率

产品应将误报率控制在应用许可的范围 15%内，不能对正常使用产品产生较大影响。

6.2.1.7.2 漏报率

系统应将漏报率控制在应用许可的范围 15%内，不能对正常使用产品产生较大影响。

6.2.1.7.3 流量监控能力

百兆系统单口监控流量≥90 Mbps，千兆系统单口监控流量≥0.9 Gbps，万兆系统单口监控流量≥9 Gbps。

6.2.1.7.4 并发连接数监控能力

百兆系统单口监控并发连接数≥10 万个，千兆系统单口监控并发连接数≥100 万个，万兆系统单口监控并发连接数≥150 万个。

6.2.1.7.5 新建 TCP 连接速率监控能力

百兆系统单口监控每秒新建 TCP 连接数≥6 万个，千兆系统单口监控每秒新建 TCP 连接数≥10 万个，万兆系统单口监控每秒新建 TCP 连接数≥15 万个。

6.2.2 自身安全功能要求

6.2.2.1 身份鉴别

6.2.2.1.1 管理员鉴别

系统应在管理员执行任何与安全功能相关的操作之前对管理员进行鉴别。

6.2.2.1.2 鉴别失败的处理

当管理员鉴别尝试失败连续达到指定次数后，系统应阻止管理员进一步的鉴别请求，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。

6.2.2.1.3 鉴别数据保护

系统应保护鉴别数据不被未授权查阅和修改。

6.2.2.1.4 超时设置

系统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，锁定或终止会话，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。

6.2.2.1.5 控制台鉴别

系统应在通过控制台对引擎执行任何与安全功能相关的操作之前对控制台进行鉴别。

6.2.2.2 管理员管理

6.2.2.2.1 标识唯一性

系统应保证所设置的管理员标识全局唯一。

6.2.2.2.2 管理员属性定义

系统应为每一个管理员保存安全属性表，属性应包括：管理员标识、鉴别数据、授权信息或管理组信息、其他安全属性等。

6.2.2.2.3 安全行为管理

系统应仅允许授权管理员对产品的功能具有禁止、修改的能力。

6.2.2.2.4 管理员角色

系统应设置多个角色，并应保证每一个角色标识是全局唯一的。

6.2.2.2.5 安全属性管理

系统应仅允许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。

6.2.2.3 安全审计

6.2.2.3.1 审计日志生成

应能为下述可审计事件产生审计日志：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 审计日志可理解性

审计数据的记录方式应便于管理员理解。

6.2.2.3.3 审计日志查阅

系统应为授权管理员提供提供审计日志查阅功能，方便管理员查看审计结果。

6.2.2.3.4 受限的审计日志查阅

除了具有明确的访问权限的授权管理员之外，系统应禁止所有其他用户对审计日志的访问。

6.2.2.3.5 可选审计查阅

应支持按照一定条件对审计日志进行检索或排序。

6.2.2.4 事件记录安全

6.2.2.4.1 安全管理

系统应仅允许授权管理员访问事件记录，禁止其他用户对事件记录的操作。

6.2.2.4.2 事件记录保护

在事件记录遭受攻击时，系统应能够及时通知管理员。

6.2.2.4.3 事件记录存储安全

系统应在发生事件记录存储器空间将耗尽等情况时，应采取相应措施保证已存储事件记录可用和后续事件记录的存储。

6.2.2.5 通信安全

6.2.2.5.1 通信保密性

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。

6.2.2.5.2 通信完整性

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）被篡改后，系统应确保及时发现、并通知管理员。

6.2.2.6 升级安全

系统应确保事件库和系统升级时的安全，应防止得到错误的或伪造的升级包。

6.2.2.7 运行安全

6.2.2.7.1 自我隐藏

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。

6.2.2.7.2 自我监测

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，包括硬件工作状态监测、组件连接状态监测等，以验证产品自身执行的正确性。

6.2.3 安全保证要求

6.2.3.1 配置管理

6.2.3.1.1 版本号

开发者应为系统的不同版本提供唯一的标识。

6.2.3.1.2 配置项

开发者应使用配置管理系统并提供配置管理文档。

配置管理文档应包括一个配置清单，配置清单应唯一标识组成系统的所有配置项并对配置项进行描述，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维护的证据。

6.2.3.2 交付与运行

6.2.3.2.1 交付程序

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。

交付文档应描述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。

6.2.3.2.2 安装、生成和启动程序

开发者应提供文档说明系统的安装、生成和启动的过程。

6.2.3.3 开发

6.2.3.3.1 非形式化功能规范

开发者应提供一个功能规范，功能规范应满足以下要求：

a) 使用非形式化风格来描述系统安全功能及其外部接口；
b) 是内在一致的；
c) 描述所有外部接口的用途与使用方法，适当时应提供效果、例外情况和错误消息的细节；
d) 完备地表示系统安全功能。

6.2.3.3.2 描述性高层设计

开发者应提供系统安全功能的高层设计，高层设计应满足以下要求：

a) 表示应是非形式化的；
b) 是内在一致的；
c) 按子系统描述安全功能的结构；
d) 描述每个安全功能子系统所提供的安全功能性；
e) 标识安全功能所要求的任何基础性的硬件、固件或软件，以及在这些硬件、固件或软件中实现的支持性保护机制所提供功能的一个表示；
f) 标识安全功能子系统的所有接口；
g) 标识安全功能子系统的哪些接口是外部可见的。

6.2.3.3.3 非形式化对应性证实

开发者应提供系统安全功能表示的所有相邻对之间提供对应性分析。

对于系统安全功能所表示的每个相邻对，分析应阐明，较为抽象的安全功能表示的所有相关安全功能，应在较具体的安全功能表示中得到正确且完备地细化。

6.2.3.4 文档要求

6.2.3.4.1 管理员指南

开发者应提供管理员指南，管理员指南应与为评估而提供的其他所有文档保持一致。

管理员指南应说明以下内容：

a） 管理员可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被控制的功能和权限；

d） 所有对与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实体的安全特性进行的改变；

g） 所有与管理员有关的 IT 环境安全要求。

6.2.3.4.2 用户指南

开发者应提供用户指南，用户指南应与为评估而提供的其他所有文档保持一致。

用户指南应说明以下内容：

a） 产品的非管理员用户可使用的安全功能和接口；

b） 产品提供给用户的安全功能和接口的使用方法；

c） 用户可获取但应受安全处理环境所控制的所有功能和权限；

d） 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。

6.2.3.5 测试

6.2.3.5.1 覆盖证据

开发者应提供测试覆盖的证据。

在测试覆盖证据中，应表明测试文档中所标识的测试与功能规范中所描述的系统的安全功能是对应的。

6.2.3.5.2 功能测试

开发者应测试安全功能，将结果文档化并提供测试文档。

测试文档应包括以下内容：

a） **测试计划，应标识要测试的安全功能，并描述测试的目标；**

b） **测试过程，应标识要执行的测试，并描述每个安全功能的测试概况，这些概况应包括对于其他测试结果的顺序依赖性；**

c） **预期的测试，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。**

6.2.3.5.3 独立测试

6.2.3.5.3.1 一致性

开发者应提供适合测试的系统，提供的测试集合应与其自测系统功能时使用的测试集合相一致。

6.2.3.5.3.2 抽样

开发者应提供一组相当的资源，用于安全功能的抽样测试。

6.2.3.6 脆弱性分析保证

6.2.3.6.1 系统安全功能强度评估

开发者应对指导性文档中所标识的每个具有安全功能强度声明的安全机制进行安全功能强度分析，并说明安全机制达到或超过定义的最低强度级别或特定功能强度度量。

6.2.3.6.2 开发者脆弱性分析

开发者应执行脆弱性分析，并提供脆弱性分析文档。

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提供文档。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，应有证据显示在使用系统的环境中，该脆弱性不能被利用。在文档中，还需证明经过标识脆弱性的系统可以抵御明显的穿透性攻击。

6.3 第三级

6.3.1 安全功能要求

6.3.1.1 数据探测功能要求

6.3.1.1.1 数据收集

系统应具有实时获取受保护网段内的数据包的能力用于检测分析。

6.3.1.1.2 协议分析

系统至少应分析基于以下协议的事件：IP、TCP、UDP、ICMP、ARP、RIP、RPC、HTTP、FTP、TFTP、IMAP、SNMP、TELNET、DNS、SMTP、POP3、NETBIOS、NFS 等。

6.3.1.1.3 行为监测

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、文件脆弱性攻击、浏览器脆弱性攻击、应用层安全漏洞攻击等。

6.3.1.1.4 流量监测

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。

6.3.1.2 入侵分析功能要求

6.3.1.2.1 数据分析

系统应对收集的数据包进行分析，发现安全事件。

6.3.1.2.2 事件合并

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。

6.3.1.2.3 防躲避能力

系统应能发现躲避或欺骗检测的行为，如 IP 碎片分片、TCP 流分段、URL 字符串变形、shell 代码变形等。

6.3.1.2.4 事件关联

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。

6.3.1.3 入侵响应功能要求

6.3.1.3.1 定制响应

系统应允许管理员对被检测网段中指定的目的主机定制不同的响应方式。

6.3.1.3.2 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。

6.3.1.3.3 告警方式

告警应采取屏幕实时提示、E-mail 告警、Syslog 告警等一种或几种方式。

6.3.1.3.4 阻断能力

系统在监测到网络上的非法连接时，可进行阻断。

6.3.1.3.5 排除响应

系统应允许管理员定义对被检测网段中指定的目的主机不予告警。

6.3.1.3.6 防火墙联动

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。

6.3.1.3.7 全局预警

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。

6.3.1.3.8 其他设备联动

系统应具有与其他网络设备或网络安全部件（如漏洞扫描、交换机）按照设定的策略进行联动的能力。

6.3.1.4 管理控制功能要求

6.3.1.4.1 图形界面

系统应提供友好的管理员界面用于管理、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。

6.3.1.4.2 事件数据库

系统事件数据库中的内容应包括事件的定义和分析内容、详细的漏洞修补方案、可采取的对策等。

6.3.1.4.3 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。

6.3.1.4.4 策略配置

系统应提供方便、快捷的入侵检测系统策略配置方法和手段，具备策略模板、支持策略的导入和导出。

6.3.1.4.5 事件库升级

系统应具有升级事件库的能力。

6.3.1.4.6 统一升级

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。

6.3.1.4.7 硬件失效处理

对于硬件产品，系统失效时应及时向管理员报警。

6.3.1.4.8 分布式部署

系统应具有分布式部署的能力。

6.3.1.4.9 集中管理

系统应设置集中管理中心，对分布式的入侵检测系统进行统一集中管理。

6.3.1.4.10 端口分离

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。

6.3.1.4.11 双机热备

对于硬件产品，系统应提供双机热备功能。

6.3.1.4.12 系统升级

系统应具有升级系统程序的能力。

6.3.1.4.13 分级管理

系统应具有分级管理的能力；支持可选择、可配置需要多级之间同步的数据类型。

6.3.1.5 检测结果处理要求

6.3.1.5.1 事件记录

系统应保存检测到的安全事件并记录安全事件信息。

安全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、事件等级、事件类型、事件名称、事件详细描述以及解决方案建议等。

6.3.1.5.2 事件可视化

管理员应能通过管理界面实时清晰地查看安全事件。

6.3.1.5.3 报告生成

系统应能生成详尽的检测结果报告。

6.3.1.5.4 报告查阅

系统应具有浏览检测结果报告的功能。

6.3.1.5.5 报告输出

检测结果报告应可输出成方便管理员阅读的文本格式，如 WORD 文件、HTML 文件、文本文件等。

6.3.1.6 产品灵活性要求

6.3.1.6.1 报告定制

系统应支持授权管理员定制报告内容。

6.3.1.6.2 事件定义

系统应允许授权管理员自定义事件，并应提供方便、快捷的定义方法。

6.3.1.6.3 协议定义

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。

6.3.1.7 性能要求

6.3.1.7.1 误报率

产品应将误报率控制在应用许可的范围 15%内，不能对正常使用产品产生较大影响。

6.3.1.7.2 漏报率

系统应将漏报率控制在应用许可的范围 15%内，不能对正常使用产品产生较大影响。

6.3.1.7.3 流量监控能力

百兆系统单口监控流量≥90 Mbps，千兆系统单口监控流量≥0.9 Gbps，万兆系统单口监控流量≥9 Gbps。

6.3.1.7.4 并发连接数监控能力

百兆系统单口监控并发连接数≥10 万个，千兆系统单口监控并发连接数≥100 万个，万兆系统单口监控并发连接数≥150 万个。

6.3.1.7.5 新建 TCP 连接速率监控能力

百兆系统单口监控每秒新建 TCP 连接数≥6 万个，千兆系统单口监控每秒新建 TCP 连接数≥10 万个，万兆系统单口监控每秒新建 TCP 连接数≥15 万个。

6.3.1.7.6 还原能力

系统应对入侵行为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，系统应保证入侵行为的获取和还原能够正常进行。

6.3.2 自身安全功能要求

6.3.2.1 身份鉴别

6.3.2.1.1 管理员鉴别

系统应在管理员执行任何与安全功能相关的操作之前对管理员进行鉴别。

6.3.2.1.2 鉴别失败的处理

当管理员鉴别尝试失败连续达到指定次数后，系统应阻止管理员进一步的鉴别请求，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。

6.3.2.1.3 鉴别数据保护

系统应保护鉴别数据不被未授权查阅和修改。

6.3.2.1.4 超时设置

系统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，锁定或终止会话，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。

6.3.2.1.5 控制台鉴别

系统应在通过控制台对引擎执行任何与安全功能相关的操作之前对控制台进行鉴别。

6.3.2.1.6 多重鉴别机制

系统应提供多种鉴别方式，以实现多重身份鉴别措施。

6.3.2.1.7 会话锁定

系统应允许管理员锁定当前的交互会话，锁定后需要再次进行身份鉴别才能够重新管理产品。

6.3.2.2 管理员管理

6.3.2.2.1 标识唯一性

系统应保证所设置的管理员标识全局唯一。

6.3.2.2.2 管理员属性定义

系统应为每一个管理员保存安全属性表，属性应包括：管理员标识、鉴别数据、授权信息或管理组信息、其他安全属性等。

6.3.2.2.3 安全行为管理

系统应仅允许授权管理员对产品的功能具有禁止、修改的能力。

6.3.2.2.4 管理员角色

系统应设置多个角色，并应保证每一个角色标识是全局唯一的。

6.3.2.2.5 安全属性管理

系统应仅允许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 安全审计

6.3.2.3.1 审计日志生成

应能为下述可审计事件产生审计日志：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。

6.3.2.3.2 审计日志可理解性

审计数据的记录方式应便于管理员理解。

6.3.2.3.3 审计日志查阅

系统应为授权管理员提供提供审计日志查阅功能，方便管理员查看审计结果。

6.3.2.3.4 受限的审计日志查阅

除了具有明确的访问权限的授权管理员之外，系统应禁止所有其他用户对审计日志的访问。

6.3.2.3.5 可选审计查阅

应支持按照一定条件对审计日志进行检索或排序。

6.3.2.4 事件记录安全

6.3.2.4.1 安全管理

系统应仅允许授权管理员访问事件记录，禁止其他用户对事件记录的操作。

6.3.2.4.2 事件记录保护

在事件记录遭受攻击时，系统应能够及时通知管理员。

6.3.2.4.3 事件记录存储安全

系统应在发生事件记录存储器空间将耗尽等情况时，应采取相应措施保证已存储事件记录可用和后续事件记录的存储。

6.3.2.4.4 事件记录存储告警

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，产生告警的剩余存储空间大小应由管理员自主设定。

6.3.2.5 通信安全

6.3.2.5.1 通信保密性

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。

6.3.2.5.2 通信完整性

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）被篡改后，系统应确保及时发现、并通知管理员。

6.3.2.6 升级安全

系统应确保事件库和系统升级时的安全，应防止得到错误的或伪造的升级包。

6.3.2.7 运行安全

6.3.2.7.1 自我隐藏

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。

6.3.2.7.2 自我监测

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，包括硬件工作状态监测、组件连接状态监测等，以验证产品自身执行的正确性。

6.3.3 安全保证要求

6.3.3.1 配置管理

6.3.3.1.1 配置管理能力

6.3.3.1.1.1 版本号

开发者应为系统的不同版本提供唯一的标识。

6.3.3.1.1.2 配置项

开发者应使用配置管理系统并提供配置管理文档。

配置管理文档应包括一个配置清单，配置清单应唯一标识组成系统的所有配置项并对配置项进行描述，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维护的证据。

6.3.3.1.1.3 授权控制

开发者提供的配置管理文档应包括一个配置管理计划，配置管理计划应描述如何使用配置管理系统。实施的配置管理应与配置管理计划相一致。

开发者应提供所有的配置项得到有效地维护的证据，并应保证只有经过授权才能修改配置项。

6.3.3.1.2 配置管理覆盖

配置管理范围至少应包括系统交付与运行文档、开发文档、指导性文档、生命周期支持文档、测试文档、脆弱性分析文档和配置管理文档，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。

配置管理文档至少应能跟踪上述内容，并描述配置管理系统是如何跟踪这些配置项的。

6.3.3.2 交付与运行

6.3.3.2.1 交付程序

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。

交付文档应描述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。

6.3.3.2.2 安装、生成和启动程序

开发者应提供文档说明系统的安装、生成和启动的过程。

6.3.3.3 开发

6.3.3.3.1 非形式化功能规范

开发者应提供一个功能规范，功能规范应满足以下要求：

a) 使用非形式化风格来描述系统安全功能及其外部接口；

b) 是内在一致的；

c) 描述所有外部接口的用途与使用方法，适当时应提供效果、例外情况和错误消息的细节；

d) 完备地表示系统安全功能。

6.3.3.3.2 高层设计

6.3.3.3.2.1 描述性高层设计

开发者应提供系统安全功能的高层设计，高层设计应满足以下要求：

a) 表示应是非形式化的；

b) 是内在一致的；

c) 按子系统描述安全功能的结构；

d) 描述每个安全功能子系统所提供的安全功能性；

e) 标识安全功能所要求的任何基础性的硬件、固件或软件，以及在这些硬件、固件或软件中实现的支持性保护机制所提供功能的一个表示；

f) 标识安全功能子系统的所有接口；

g) 标识安全功能子系统的哪些接口是外部可见的。

6.3.3.3.2.2 安全加强的高层设计

开发者提供的安全加强的高层设计应满足以下要求：

a) **描述系统的功能子系统所有接口的用途与使用方法，适当时应提供效果、例外情况和错误消息的细节；**

b) **把系统分成安全策略实施和其他子系统来描述。**

6.3.3.3.3 非形式化对应性证实

开发者应提供系统安全功能表示的所有相邻对之间提供对应性分析。

对于系统安全功能所表示的每个相邻对，分析应阐明，较为抽象的安全功能表示的所有相关安全功能，应在较具体的安全功能表示中得到正确且完备地细化。

6.3.3.4 文档要求

6.3.3.4.1 管理员指南

开发者应提供管理员指南，管理员指南应与为评估而提供的其他所有文档保持一致。

管理员指南应说明以下内容：

a) 管理员可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被控制的功能和权限；

d) 所有对与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实体的安全特性进行的改变；
g) 所有与管理员有关的 IT 环境安全要求。

6.3.3.4.2 用户指南

开发者应提供用户指南，用户指南应与为评估而提供的其他所有文档保持一致。
用户指南应说明以下内容：
a) 产品的非管理员用户可使用的安全功能和接口；
b) 产品提供给用户的安全功能和接口的使用方法；
c) 用户可获取但应受安全处理环境所控制的所有功能和权限；
d) 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。

6.3.3.5 生命周期支持

开发者应提供开发安全文档。
开发安全文档应描述在系统的开发环境中，为保护系统设计和实现的保密性和完整性所必需的所有物理的、程序的、人员的和其他方面的安全措施，并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 测试覆盖

6.3.3.6.1.1 覆盖证据

开发者应提供测试覆盖的证据。
在测试覆盖证据中，应表明测试文档中所标识的测试与功能规范中所描述的系统的安全功能是对应的。

6.3.3.6.1.2 覆盖分析

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功能规范中所描述的系统的安全功能之间的对应性是完备的。

6.3.3.6.2 测试深度

开发者应提供测试深度的分析。
深度分析应证实测试文档中所标识的测试足以证实该系统的功能是依照其高层设计运行的。

6.3.3.6.3 功能测试

开发者应测试安全功能，将结果文档化并提供测试文档。
测试文档应包括以下内容：
a) 测试计划，应标识要测试的安全功能，并描述测试的目标；
b) 测试过程，应标识要执行的测试，并描述每个安全功能的测试概况，这些概况应包括对于其他测试结果的顺序依赖性；
c) 预期的测试，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。

6.3.3.6.4 独立测试

6.3.3.6.4.1 一致性

开发者应提供适合测试的系统，提供的测试集合应与其自测系统功能时使用的测试集合相一致。

6.3.3.6.4.2 抽样

开发者应提供一组相当的资源，用于安全功能的抽样测试。

6.3.3.7 脆弱性分析保证

6.3.3.7.1 指南审查

开发者应提供指导性文档，指导性文档应满足以下要求：

a) 标识所有可能的系统运行模式（包括失败或操作失误后的运行）、它们的后果以及对于保持安全运行的意义；

b) 是完备的、清晰的、一致的、合理的；

c) 列出关于预期使用环境的所有假设；

d) 列出对外部安全措施（包括外部程序的、物理的或人员的控制）的所有要求。

6.3.3.7.2 系统安全功能强度评估

开发者应对指导性文档中所标识的每个具有安全功能强度声明的安全机制进行安全功能强度分析，并说明安全机制达到或超过定义的最低强度级别或特定功能强度度量。

6.3.3.7.3 开发者脆弱性分析

开发者应执行脆弱性分析，并提供脆弱性分析文档。

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提供文档。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，应有证据显示在使用系统的环境中，该脆弱性不能被利用。在文档中，还需证明经过标识脆弱性的系统可以抵御明显的穿透性攻击。

7 网络入侵检测系统测评方法

7.1 测试环境

网络入侵检测系统功能测试的典型网络拓扑结构如图 1 所示。

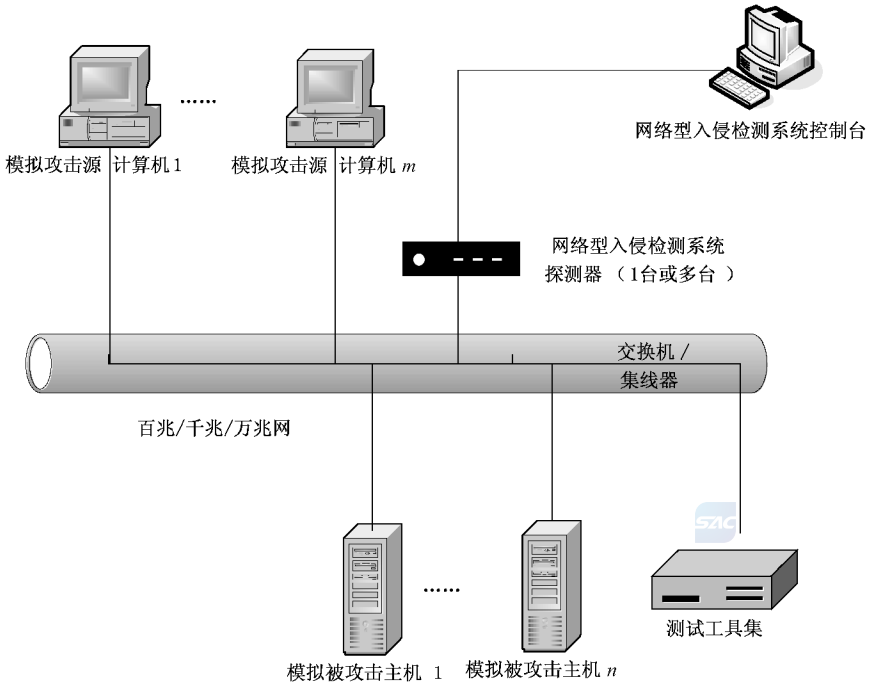

图 1　网络入侵检测系统功能测试典型网络拓扑图

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，以及网络入侵检测系统控制台、网络入侵检测系统探测器等。其中，模拟攻击源计算机和模拟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：生成网络背景流量的专用网络性能分析仪；进行包回放的网络数据包获取软件；测试产品报警能力的扫描和攻击工具包。

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　安全功能测试

7.3.1.1　数据探测功能测试

7.3.1.1.1　数据收集

对数据收集的测试评价方法与预期结果如下：

a）　测试评价方法：

1）　打开系统的安全策略配置，配置受保护网段；

2）　对受保护网段发起攻击；

3）　检查是否具有实时获取受保护网段内的数据包的能力。

b）　预期结果：系统应能够获取足够的网络数据包以分析安全事件。

7.3.1.1.2 协议分析

对协议分析的测试评价方法与预期结果如下：

a) 测试评价方法：

1) 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；

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，组成安全事件测试集；

3) 配置系统的检测策略为最大策略集；

4) 发送安全事件测试集中的所有事件，记录系统的检测结果。

b) 预期结果：

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分析的协议的事件至少包括以下类型：IP、TCP、UDP、ICMP、ARP、RIP、RPC、HTTP、FTP、TFTP、IMAP、SNMP、TELNET、DNS、SMTP、POP3、NETBIOS、NFS 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

对行为监测的测试评价方法与预期结果如下：

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，组成安全事件测试集。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)、文件脆弱性攻击类事件(如 MS-Office 文件脆弱性)、浏览器脆弱性攻击类事件(如 MS-IE 浏览器脆弱性)、应用层安全漏洞攻击以及其他具有代表性的网络安全事件，测试系统；

2) 配置系统的检测策略为最大策略集；

3) 发送安全事件测试集中的所有事件，记录系统的检测结果。

b) 预期结果：

1) 对安全事件测试集的攻击，系统应报告相应的安全事件，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

对流量监控的测试评价方法与预期结果如下：

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) 预期结果：

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

对数据分析的测试评价方法与预期结果如下：

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，组成安全事件测试集。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，以及其他具有代表性的安全事件；
2） 配置系统的检测策略为最大策略集；
3） 发送安全事件测试集中的所有事件，记录系统的检测结果。

b） 预期结果：
1） 对安全事件测试集的攻击，系统应报告相应的安全事件，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 事件合并

对事件合并的测试评价方法与预期结果如下：

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） 预期结果：
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。

7.3.1.3 入侵响应功能测试

7.3.1.3.1 定制响应

对定制响应的测试评价方法与预期结果如下：

a） 测试评价方法：
1） 系统应允许管理员对被检测网段中指定的目的主机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，检查系统是否允许管理员设置仅对被检测网段中指定的目的主机进行告警。

b） 预期结果：管理员可以定制仅监控符合指定条件的目的主机。

7.3.1.3.2 安全告警

对安全告警的测试评价方法与预期结果如下：

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） 预期结果：
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。

7.3.1.3.3 告警方式

对告警方式的测试评价方法与预期结果如下：

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） 预期结果：可以采取屏幕实时提示、Syslog 告警、SNMP trap 消息、E-mail 告警、运行指定应用程序等一种或几种告警方式。记录并列出所有告警方式。

7.3.1.4 管理控制功能测试

7.3.1.4.1 图形界面

对图形界面的测试评价方法与预期结果如下：

a） 测试评价方法：
1） 登录控制台界面；
2） 查看管理员界面的功能，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） 预期结果：
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

对事件数据库的测试评价方法与预期结果如下：

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） 预期结果：
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） 数据库中的内容应包括事件的定义和分析内容、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

对事件分级的测试评价方法与预期结果如下：

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) 检查界面显示的安全事件是否具备事件级别信息。

b) 预期结果：

1) 事件库的所有事件都具有分级信息；

2) 界面显示的安全事件，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

对策略配置的测试评价方法与预期结果如下：

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) 预期结果：

1) 系统应提供默认的策略，并可以直接应用；

2) 应允许管理员编辑策略；

3) 具有供管理员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 事件库升级

对事件库升级的测试评价方法与预期结果如下：

a) 测试评价方法：

1) 检查产品说明书，查看事件特征库的升级方式；

2) 对特征库进行手动或自动的在线升级。

b) 预期结果：

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) 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

对统一升级的测试评价方法与预期结果如下：

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) 预期结果：

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。

7.3.1.4.7 硬件失效处理

对硬件失效处理的测试评价方法与预期结果如下：

a) 测试评价方法：检查系统具备何种硬件失效处理机制，如硬件失效后，系统具有相应的报警

措施。

b） 预期结果：系统应提供硬件失效处理机制，如硬件失效后，系统具有相应的报警措施。

7.3.1.5 检测结果处理要求

7.3.1.5.1 事件记录

对事件记录的测试评价方法与预期结果如下：

a） 测试评价方法：

1） 检查系统是否具有记录事件的数据库，系统应保存检测到的安全事件并记录安全事件信息；

2） 检查数据库是否具有维护功能。

b） 预期结果：

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） 记录的安全事件信息应包含以下内容：事件发生时间、源地址、目的地址、事件等级、事件类型、事件名称、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

对事件可视化的测试评价方法与预期结果如下：

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安全事件；

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） 预期结果：

1） 具有查看安全事件的图形化界面；

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

对报告生成的测试评价方法与预期结果如下：

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） 预期结果：

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

对报告查阅的测试评价方法与预期结果如下：

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） 预期结果：

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

对报告输出的测试评价方法与预期结果如下：

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） 预期结果：
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管理员阅读的格式，如 WORD 文件、HTML 文件、文本文件等；
3） 报告最好为中文。

7.3.1.6 性能要求

7.3.1.6.1 误报率

对误报率的测试评价方法与预期结果如下：

a） 测试评价方法：
1） 在指定的网络带宽（百兆网络、千兆网络、或厂商声明的其他网络带宽）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、或厂商声明的其他网络带宽）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、或厂商声明的其他网络带宽）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、或厂商声明的其他网络带宽）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，查看系统是否报警。
6） 依据已有的事件库，生成多个已知的安全事件，查看系统是否正确报告出了事件名称。

b） 预期结果：
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，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，系统所报告的安全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，并记录误报率。

7.3.1.6.2 漏报率

对漏报率的测试评价方法与预期结果如下：

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，组成安全事件测试集，发送安全事件测试集中的所有事件，记录系统的检测结果；
2） 可选取部分安全事件作为测试基线；选取 64 字节、128 字节、512 字节、1518 字节大小的正常数据包作为背景流量（例如 HTTP 流量），分别以满负荷背景流量的 20%、40%、60%、80%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） 预期结果：
1） 对安全事件测试集的所有攻击，系统应报告相应的安全事件，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，并记录漏报率。

7.3.1.6.3 流量监控能力

对监控流量的测试评价方法与预期结果如下：

a） 测试评价方法：
1） 选取部分安全事件作为测试基线；加载相应的背景流量——百兆 90 Mbps、千兆 0.9 Gbps、万兆 9 Gbps（例如 HTTP 流量），将选取的基线攻击发送多次（如 1 000 次），记录系统的检测结果。

b） 预期结果：
1） 对测试基线的事件，在加载相应的背景流量——百兆 90 Mbps、千兆 0.9 Gbps、万兆 9 Gbps（例如 HTTP 流量），系统单个监听口应检测到相应的攻击次数（如 1 000 次）并报告；
2） 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。

7.3.1.6.4 并发连接数监控能力

对监控并发连接数的测试评价方法与预期结果如下：

a） 测试评价方法：
1） 选取部分安全事件作为测试基线；加载相应的背景流量——百兆 10 万并发连接数、千兆 100 万并发连接数、万兆 150 万并发连接数（例如 HTTP 流量），将选取的基线攻击发送多次（如 1 000 次），记录系统的检测结果。

b） 预期结果：
1） 对测试基线的事件，在加载相应的背景流量——百兆 10 万并发连接数、千兆 100 万并发连接数、万兆 150 万并发连接数（例如 HTTP 流量），系统单个监听口应检测到相应的攻击次数（如 1 000 次）并报告；
2） 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。

7.3.1.6.5 新建 TCP 连接速率监控能力

对监控新建 TCP 连接速率的测试评价方法与预期结果如下：

a) 测试评价方法：

1) 选取部分安全事件作为测试基线；加载相应的背景流量——百兆每秒新建 TCP 连接数 6 万个、千兆每秒新建 TCP 连接数 10 万个、万兆每秒新建 TCP 连接数 15 万个(例如 HTTP 流量)，将选取的基线攻击发送多次(如 1 000 次)，记录系统的检测结果。

b) 预期结果：

1) 对测试基线的事件，在加载相应的背景流量——百兆每秒新建 TCP 连接数 6 万个、千兆每秒新建 TCP 连接数 10 万个、万兆每秒新建 TCP 连接数 15 万个(例如 HTTP 流量)，系统单个监听口应检测到相应的攻击次数(如 1 000 次)并报告；

2) 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 自身安全功能测试

7.3.2.1 身份鉴别

7.3.2.1.1 管理员鉴别

对管理员鉴别的测试评价方法与预期结果如下：

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) 预期结果：

1) 在管理员执行任何与安全功能相关的操作之前都应对管理员进行鉴别；

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) 允许管理员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

对鉴别失败的处理的测试评价方法与预期结果如下：

a) 测试评价方法：

1) 检查系统的安全功能是否可定义管理员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管理员鉴别尝试失败连续达到指定次数后，采取相应的措施、阻止管理员进一步的鉴别请求；

3) 尝试多次失败的管理员鉴别行为，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) 预期结果：

1) 系统应具备定义管理员鉴别尝试的最大允许失败次数的功能；

2) 系统应定义当管理员鉴别尝试失败连续达到指定次数后，采取相应的措施(如锁定该账号)；

3) 当管理员鉴别尝试失败连续达到指定次数后，系统应锁定该账号，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。

7.3.2.1.3 鉴别数据保护

对鉴别数据保护的测试评价方法与预期结果如下：

a) 测试评价方法：

1） 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；
2） 以非授权管理员的身份尝试查阅或修改身份鉴别数据。

b） 预期结果：
1） 系统应仅允许指定的角色查阅或修改身份鉴别数据；
2） 非授权管理员无法查阅或修改身份鉴别数据。

7.3.2.2 管理员管理

7.3.2.2.1 标识唯一性

对标识唯一性的测试评价方法与预期结果如下：

a） 测试评价方法：
1） 尝试定义多个管理员；
2） 尝试添加一个已有标识的管理员；
3） 检查系统是否提示该标识管理员已存在，拒绝具有相同标识管理员的添加。

b） 预期结果：
1） 系统应允许定义多个管理员；
2） 应保证每一个管理员标识是全局唯一的，不允许一个管理员标识用于多个管理员。

7.3.2.2.2 管理员属性定义

对管理员属性定义的测试评价方法与预期结果如下：

a） 测试评价方法：定义分属于不同角色的多个管理员，检查输入的管理员信息是否都能被保存。

b） 预期结果：系统应为每一个管理员保存其安全属性，包括：管理员标识、鉴别数据（如密码）、授权信息或管理员组信息、其他安全属性等。输入的管理员信息无丢失现象发生。

7.3.2.2.3 安全行为管理

对安全行为管理的测试评价方法与预期结果如下：

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） 预期结果：
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。

7.3.2.3 安全审计

7.3.2.3.1 审计日志生成

对审计日志生成的测试评价方法与预期结果如下：

a） 测试评价方法：结合开发者文档，使用不同角色管理员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。审查审计日志的正确性。

b） 预期结果：
1） 系统应至少为下述可审计事件产生审计日志：鉴别失败等重大事件、升级时间和版本号等；

2） 应在每个审计日志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。

7.3.2.3.2 审计日志可理解性

对审计日志可理解性的测试评价方法与预期结果如下：

a） 测试评价方法：审查产品安全功能是否使审计日志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） 预期结果：系统应提供为人理解的审计日志。

7.3.2.3.3 审计日志查阅

对审计日志查阅的测试评价方法与预期结果如下：

a） 测试评价方法：

1） 以授权管理员身份尝试从审计日志中读取全部审计信息；

2） 审查产品安全功能是否为授权管理员提供从审计日志中读取全部审计信息的功能。

b） 预期结果：系统应为授权管理员提供从审计日志中读取全部审计信息的功能。

7.3.2.3.4 受限的审计日志查阅

对受限的审计日志查阅的测试评价方法与预期结果如下：

a） 测试评价方法：模拟授权与非授权管理员访问审计日志，产品安全功能是否仅允许授权管理员访问审计日志。

b） 预期结果：系统应限制审计日志的访问。除了具有明确的访问权限的授权管理员之外，系统应禁止所有其他用户对审计日志的访问。

7.3.2.3.5 可选审计查阅

对可选审计查阅的测试评价方法与预期结果如下：

a） 测试评价方法：审查产品是否能够支持按照一定条件，例如时间、事件级别、攻击源等对审计日志进行检索或排序。

b） 预期结果：系统应应支持按照一定条件对审计日志进行检索或排序。

7.3.2.4 事件记录安全

7.3.2.4.1 安全管理

对安全管理的测试评价方法与预期结果如下：

a） 测试评价方法：模拟授权与非授权管理员访问事件记录，产品安全功能是否仅允许授权管理员访问事件记录。

b） 预期结果：系统应限制对事件记录的访问。除了具有明确的访问权限的授权管理员之外，系统应禁止所有其他用户对事件记录的访问。

7.3.2.4.2 事件记录保护

对事件记录保护的测试评价方法与预期结果如下：

a） 测试评价方法：从已有的事件库中选择具有不同特征的多个事件，组成安全事件测试集，进行测试，对系统生成的事件记录进行破坏，检查系统是否能够及时通知管理员。

b） 预期结果：对系统生成的事件记录进行破坏后，系统能够及时通知管理员。

7.3.2.5 通信保密性

对通信保密性的测试评价方法与预期结果如下：

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保密性的描述。

b) 预期结果：

1) 系统在各组件之间传输数据（如配置和控制信息、告警和事件数据等）时，数据应能够被正常传输；

2) 开发者文档中提供了为保证各组件之间通信保密性所采取措施的详细描述，数据在传输过程中非明文显示。列举系统为保证通信保密性所采取的措施。

7.3.2.6 自我隐藏

对自我隐藏的测试评价方法与预期结果如下：

a) 测试评价方法：检查开发者文档中对系统自身安全的描述。

b) 预期结果：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。

7.3.3 安全保证测试

7.3.3.1 配置管理

对配置管理的测试评价方法与预期结果如下：

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：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完全对应，没有歧义。

b) 预期结果：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。

7.3.3.2 交付与运行

对交付与运行的测试评价方法与预期结果如下：

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) 预期结果：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 开发

7.3.3.3.1 非形式化功能规范

对非形式化功能规范的测试评价方法与预期结果如下：

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) 预期结果：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 非形式化对应性证实

对非形式化对应性证实的测试评价方法与预期结果如下：

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、底层设计、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) 预期结果：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

对管理员指南的测试评价方法与预期结果如下：

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) 预期结果：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

对用户指南的测试评价方法与预期结果如下：

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) 预期结果：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 测试

对测试的测试评价方法与预期结果如下：

a) 测试评价方法：评价者应评价开发者提供的测试系统，提供的测试集合是否与其自测系统功能时使用的测试集合相一致，提供的执行测试及其结果是否与其自测系统功能时执行的测试及其结果相一致。

b) 预期结果：审查记录以及最后结果（符合/不符合），开发者应提供适合测试的系统，提供的测试集合应与其自测系统功能时使用的测试集合相一致，提供的执行测试及其结果与其自测系统功能时执行的测试及其结果相一致。

7.4 第二级

7.4.1 安全功能测试

7.4.1.1 数据探测功能测试

7.4.1.1.1 数据收集

对数据收集的测试评价方法与预期结果如下：

a) 测试评价方法：

1) 打开系统的安全策略配置，配置受保护网段；

2) 对受保护网段发起攻击；

3) 检查是否具有实时获取受保护网段内的数据包的能力。

b) 预期结果：系统应能够获取足够的网络数据包以分析安全事件。

7.4.1.1.2 协议分析

对协议分析的测试评价方法与预期结果如下：

a) 测试评价方法：

1) 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；

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，组成安全事件测试集；

3) 配置系统的检测策略为最大策略集；

4) 发送安全事件测试集中的所有事件，记录系统的检测结果。

b) 预期结果：

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分析的协议的事件至少包括以下类型：IP、TCP、UDP、ICMP、ARP、RIP、、RPC、HTTP、FTP、TFTP、IMAP、SNMP、TELNET、DNS、SMTP、POP3、NETBIOS、NFS 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。

7.4.1.1.3 行为监测

对行为监测的测试评价方法与预期结果如下：

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，组成安全事件测试集。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)、文件脆弱性攻击类事件(如 MS-Office 文件脆弱性)、浏览器脆弱性攻击类事件(如 MS-IE 浏览器脆弱性)、应用层安全漏洞攻击以及其他具有代表性的网络安全事件,测试系统;

2) 配置系统的检测策略为最大策略集;

3) 发送安全事件测试集中的所有事件,记录系统的检测结果。

b) 预期结果:

1) 对安全事件测试集的攻击,系统应报告相应的安全事件,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。

7.4.1.1.4 流量监测

对流量监测的测试评价方法与预期结果如下:

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) 预期结果:

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。

7.4.1.2 入侵分析功能测试

7.4.1.2.1 数据分析

对数据分析的测试评价方法与预期结果如下:

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,组成安全事件测试集。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,以及其他具有代表性的安全事件;

2) 配置系统的检测策略为最大策略集;

3) 发送安全事件测试集中的所有事件,记录系统的检测结果。

b) 预期结果:

1) 对安全事件测试集的攻击,系统应报告相应的安全事件,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。

7.4.1.2.2 事件合并

对事件合并的测试评价方法与预期结果如下:

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） 预期结果：

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。

7.4.1.2.3 防躲避能力

对防躲避能力的测试评价方法与预期结果如下：

a） 测试评价方法：**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**。

b） 预期结果：

1） **系统能够检测出经过分片、乱序之后的安全事件**；

2） **系统能够正确地报出经过规避的扫描 HTTP 事件**。

7.4.1.2.4 事件关联

对事件关联的测试评价方法与预期结果如下：

a） 测试评价方法：**连续生成多个不同的低危害事件，查看系统是否能自动将这些同类低危害事件关联起来，生成高危害事件**。

b） 预期结果：**系统可以对同类但不同的事件进行关联，从低危害事件中发现隐含的高危害攻击**。

7.4.1.3 入侵响应功能测试

7.4.1.3.1 定制响应

对定制响应的测试评价方法与预期结果如下：

a） 测试评价方法：

1） 系统应允许管理员对被检测网段中指定的目的主机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，检查系统是否允许管理员设置仅对被检测网段中指定的目的主机进行告警。

b） 预期结果：**管理员可以定制仅监控符合指定条件的目的主机**。

7.4.1.3.2 安全告警

对安全告警的测试评价方法与预期结果如下：

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） 预期结果：

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。

7.4.1.3.3 告警方式

对告警方式的测试评价方法与预期结果如下：

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） 预期结果：可以采取屏幕实时提示、Syslog 告警、SNMP trap 消息、E-mail 告警、运行指定应用程序等一种或几种告警方式。记录并列出所有告警方式。

7.4.1.3.4 阻断能力

对阻断能力的测试评价方法与预期结果如下：

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） **选中对安全事件的阻断选项，检查系统在监测到相应攻击时是否进行阻断。**

b） 预期结果：

1） **能够对监测到的非法连接配置阻断选项；**

2） **在检测到网络上的非法连接时，可成功进行阻断。**

7.4.1.3.5 排除响应

对排除响应的测试评价方法与预期结果如下：

a） 测试评价方法：

1） **打开菜单，检查系统是否允许管理员设置对被检测网段中指定的目的主机不予告警；**

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） 预期结果：**管理员可以定制不监控符合指定条件的目的主机。**

7.4.1.3.6 防火墙联动

对防火墙联动的测试评价方法与预期结果如下：

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） 预期结果：

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。**

7.4.1.4 管理控制功能测试

7.4.1.4.1 图形界面

对图形界面的测试评价方法与预期结果如下：

a） 测试评价方法：

1） 登录控制台界面；
2） 查看管理员界面的功能，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） 预期结果：
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。

7.4.1.4.2 事件数据库

对事件数据库的测试评价方法与预期结果如下：

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） 预期结果：
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） 数据库中的内容应包括事件的定义和分析内容、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。

7.4.1.4.3 事件分级

对事件分级的测试评价方法与预期结果如下：

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） 检查界面显示的安全事件是否具备事件级别信息。

b） 预期结果：
1） 事件库的所有事件都具有分级信息；
2） 界面显示的安全事件，都以文字或色彩等形式显示了事件级别。

7.4.1.4.4 策略配置

对策略配置的测试评价方法与预期结果如下：

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） 预期结果：
1） 系统应提供默认的策略，并可以直接应用；
2） 应允许管理员编辑策略；
3） 具有供管理员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。

7.4.1.4.5 事件库升级

对事件库升级的测试评价方法与预期结果如下：

a) 测试评价方法：

1) 检查产品说明书，查看事件特征库的升级方式；

2) 对特征库进行手动或自动的在线升级。

b) 预期结果：

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) 列举事件库升级的方式、承诺的升级频率。

7.4.1.4.6 统一升级

对统一升级的测试评价方法与预期结果如下：

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) 预期结果：

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。

7.4.1.4.7 硬件失效处理

对硬件失效处理的测试评价方法与预期结果如下：

a) 测试评价方法：检查系统具备何种硬件失效处理机制，如硬件失效后，系统具有相应的报警措施。

b) 预期结果：系统应提供硬件失效处理机制，如硬件失效后，系统具有相应的报警措施。

7.4.1.4.8 分布式部署

对分布式部署的测试评价方法与预期结果如下：

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) 预期结果：

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**。

7.4.1.4.9 集中管理

对集中管理的测试评价方法与预期结果如下：

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) **检查集中管理中心是否可以同时管理并设置所有控制台和探测器，查看是否有可以显示部署情况的信息**（**如拓扑图**）。

b) 预期结果：

1) **控制台可以管理所有为其部署的探测器**；

2) **集中管理中心可以管理部署的控制台**；

3) **可以正确显示系统部署的拓扑**。

7.4.1.4.10 端口分离

对端口分离的测试评价方法与预期结果如下：

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

b) 预期结果：**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**。

7.4.1.4.11 双机热备

对双机热备的测试评价方法与预期结果如下：

a) 测试评价方法：**按照产品部署方案进行双机热备环境部署，关闭其中一台设备，查看另一设备是否可以及时工作**。

b) 预期结果：**对于双机热备部署的环境，当出现一台设备宕机的情况，应不影响网络用户的正常使用**。

7.4.1.4.12 系统升级

对系统升级的测试评价方法与预期结果如下：

a) 测试评价方法：

1) **检查控制台的升级方式**；
2) **尝试对控制台进行升级**；
3) **检查探测器的升级方式**；
4) **尝试通过控制台对探测器下发升级程序**。

b) 预期结果：

1) **升级的过程中探测器可以正常检测事件**；
2) **应通过控制台来下发探测器的升级程序**。

7.4.1.5 检测结果处理要求

7.4.1.5.1 事件记录

对事件记录的测试评价方法与预期结果如下：

a) 测试评价方法：

1) 检查系统是否具有记录事件的数据库，系统应保存检测到的安全事件并记录安全事件信息；
2) 检查数据库是否具有维护功能。

b) 预期结果：

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) 记录的安全事件信息应包含以下内容：事件发生时间、源地址、目的地址、事件等级、事件类型、事件名称、事件详细描述以及解决方案建议等。

7.4.1.5.2 事件可视化

对事件可视化的测试评价方法与预期结果如下：

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安全事件；
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) 预期结果：

1) 具有查看安全事件的图形化界面；

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。

7.4.1.5.3 报告生成

对报告生成的测试评价方法与预期结果如下：

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） 预期结果：

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。

7.4.1.5.4 报告查阅

对报告查阅的测试评价方法与预期结果如下：

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） 预期结果：

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。

7.4.1.5.5 报告输出

对报告输出的测试评价方法与预期结果如下：

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） 预期结果：

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管理员阅读的格式，如 WORD 文件、HTML 文件、文本文件等；报告最好为中文。

7.4.1.6 产品灵活性要求

7.4.1.6.1 报告定制

对报告定制的测试评价方法与预期结果如下：

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） 预期结果：

1） **系统允许管理员定制报告类别、报告内容、报告风格等内容**；

2） **列举系统支持的定制内容**。

7.4.1.6.2 事件定义

对事件定义的测试评价方法与预期结果如下：

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安全事件，检查系统能否报警。**

b） 预期结果：

1） **系统允许管理员自定义事件，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。**

7.4.1.6.3 协议定义

对协议定义的测试评价方法与预期结果如下：

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安全事件，检查系统能否报警。**

b） 预期结果：

1） **系统允许管理员自定义协议，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。**

7.4.1.7 性能要求

7.4.1.7.1 误报率

对误报率的测试评价方法与预期结果如下：

a） 测试评价方法：

1） 在指定的网络带宽（百兆网络、千兆网络、或厂商声明的其他网络带宽）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、或厂商声明的其他网络带宽）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、或厂商声明的其他网络带宽）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、或厂商声明的其他网络带宽）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，查看系统是否报警。

6） 依据已有的事件库，生成多个已知的安全事件，查看系统是否正确报告出了事件名称。

b） 预期结果：

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，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，系统所报告的安全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，并记录误报率。

7.4.1.7.2 漏报率

对漏报率的测试评价方法与预期结果如下：

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，组成安全事件测试集，发送安全事件测试集中的所有事件，记录系统的检测结果；

2） 可选取部分安全事件作为测试基线；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 20%、40%、60%、80%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） 预期结果：

1） 对安全事件测试集的所有攻击，系统应报告相应的安全事件，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，并记录漏报率。

7.4.1.7.3 流量监控能力

对监控流量的测试评价方法与预期结果如下：

a） 测试评价方法：

1） 选取部分安全事件作为测试基线；加载相应的背景流量——百兆 90 Mbps、千兆 0.9 Gbps、万兆 9 Gbps（例如 HTTP 流量），将选取的基线攻击发送多次（如 1 000 次），记录系统的检测结果。

b） 预期结果：

1） 对测试基线的事件，在加载相应的背景流量——百兆 90 Mbps、千兆 0.9 Gbps、万兆 9 Gbps（例如 HTTP 流量），系统单个监听口应检测到相应的攻击次数（如 1 000 次）并报告；

2） 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。

7.4.1.7.4 并发连接数监控能力

对监控并发连接数的测试评价方法与预期结果如下：

a） 测试评价方法：

1） 选取部分安全事件作为测试基线；加载相应的背景流量——百兆 10 万并发连接数、千兆 100 万并发连接数、万兆 150 万并发连接数（例如 HTTP 流量），将选取的基线攻击发送

多次(如 1 000 次),记录系统的检测结果。

b) 预期结果:

1) 对测试基线的事件,在加载相应的背景流量——百兆 10 万并发连接数、千兆 100 万并发连接数、万兆 150 万并发连接数(例如 HTTP 流量),系统单个监听口应检测到相应的攻击次数(如 1 000 次)并报告;

2) 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。

7.4.1.7.5 新建 TCP 连接速率监控能力

对监控新建 TCP 连接速率的测试评价方法与预期结果如下:

a) 测试评价方法:

1) 选取部分安全事件作为测试基线;加载相应的背景流量——百兆每秒新建 TCP 连接数 6 万个、千兆每秒新建 TCP 连接数 10 万个、万兆每秒新建 TCP 连接数 15 万个(例如 HTTP 流量),将选取的基线攻击发送多次(如 1 000 次),记录系统的检测结果。

b) 预期结果:

1) 对测试基线的事件,在加载相应的背景流量——百兆每秒新建 TCP 连接数 6 万个、千兆每秒新建 TCP 连接数 10 万个、万兆每秒新建 TCP 连接数 15 万个(例如 HTTP 流量),系统单个监听口应检测到相应的攻击次数(如 1 000 次)并报告;

2) 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。

7.4.2 自身安全功能测试

7.4.2.1 身份鉴别

7.4.2.1.1 管理员鉴别

对管理员鉴别的测试评价方法与预期结果如下:

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) 预期结果:

1) 在管理员执行任何与安全功能相关的操作之前都应对管理员进行鉴别;

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) 允许管理员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。

7.4.2.1.2 鉴别失败的处理

对鉴别失败的处理的测试评价方法与预期结果如下:

a) 测试评价方法:

1) 检查系统的安全功能是否可定义管理员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管理员鉴别尝试失败连续达到指定次数后,采取相应的措施、阻止管理员进一步的鉴别请求;

3) 尝试多次失败的管理员鉴别行为,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) 预期结果:

1) 系统应具备定义管理员鉴别尝试的最大允许失败次数的功能;

2) 系统应定义当管理员鉴别尝试失败连续达到指定次数后,采取相应的措施(如锁定该账号);

3) 当管理员鉴别尝试失败连续达到指定次数后,系统应锁定该账号,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。

7.4.2.1.3 鉴别数据保护

对鉴别数据保护的测试评价方法与预期结果如下：

a） 测试评价方法：

1） 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；

2） 以非授权管理员的身份尝试查阅或修改身份鉴别数据。

b） 预期结果：系统应仅允许指定的角色查阅或修改身份鉴别数据。

1） 系统应仅允许指定的角色查阅或修改身份鉴别数据；

2） 非授权管理员无法查阅或修改身份鉴别数据。

7.4.2.1.4 超时设置

对超时设置的测试评价方法与预期结果如下：

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，检查登录管理员在设定的时间段内没有任何操作的情况下，系统是否锁定或终止了会话，管理员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） 预期结果：

1） **系统应具有登录超时重新鉴别功能；**

2） **任何登录管理员在设定的时间段内没有任何操作的情况下，应被锁定或终止了会话，管理员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。**

7.4.2.1.5 控制台鉴别

对控制台鉴别的测试评价方法与预期结果如下：

a） 测试评价方法：**通过控制台连接引擎，检查是否在执行所有功能之前要求首先进行控制台认证。**

b） 预期结果：

1） **在通过控制台连接引擎执行任何与安全功能相关的操作之前都应对控制台进行鉴别；**

2） **控制台连接引擎后，允许通过控制台执行与安全功能相关的各类操作时，不再重复认证。**

7.4.2.2 管理员管理

7.4.2.2.1 标识唯一性

对标识唯一性的测试评价方法与预期结果如下：

a） 测试评价方法：

1） 尝试定义多个管理员；

2） 尝试添加一个已有标识的管理员；

3） 检查系统是否提示该标识管理员已存在，拒绝具有相同标识管理员的添加。

b） 预期结果：

1） 系统应允许定义多个管理员；

2） 应保证每一个管理员标识是全局唯一的，不允许一个管理员标识用于多个管理员。

7.4.2.2.2 管理员属性定义

对管理员属性定义的测试评价方法与预期结果如下：

a） 测试评价方法：定义分属于不同角色的多个管理员，检查输入的管理员信息是否都能被保存。

b） 预期结果：系统应为每一个管理员保存其安全属性，包括：管理员标识、鉴别数据（如密码）、授权信息或管理员组信息、其他安全属性等。输入的管理员信息无丢失现象发生。

7.4.2.2.3 安全行为管理

对安全行为管理的测试评价方法与预期结果如下：

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） 预期结果：

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。

7.4.2.2.4 管理员角色

对管理员角色的测试评价方法与预期结果如下：

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管理员。**

b） 预期结果：

1） **系统应允许定义多个角色的管理员；**

2） **每个角色可以具有多个管理员，每个管理员只能属于一个角色；**

3） **应保证每一个角色标识是全局唯一的，不允许一个角色标识用于多个角色。**

7.4.2.2.5 安全属性管理

对安全属性管理的测试评价方法与预期结果如下：

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） 预期结果：

1） **系统应仅允许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。**

7.4.2.3 安全审计

7.4.2.3.1 审计日志生成

对审计日志生成的测试评价方法与预期结果如下：

a） 测试评价方法：结合开发者文档，使用不同角色管理员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。审查审计日志的正确性。

b) 预期结果：

1) 系统应至少为下述可审计事件产生审计日志：鉴别失败等重大事件、升级时间和版本号等；

2) 应在每个审计日志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 审计日志可理解性

对审计日志可理解性的测试评价方法与预期结果如下：

a) 测试评价方法：审查产品安全功能是否使审计日志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) 预期结果：系统应提供为人理解的审计日志。

7.4.2.3.3 审计日志查阅

对审计日志查阅的测试评价方法与预期结果如下：

a) 测试评价方法：

1) 以授权管理员身份尝试从审计日志中读取全部审计信息；

2) 审查产品安全功能是否为授权管理员提供从审计日志中读取全部审计信息的功能。

b) 预期结果：系统应为授权管理员提供从审计日志中读取全部审计信息的功能。

7.4.2.3.4 受限的审计日志查阅

对受限的审计日志查阅的测试评价方法与预期结果如下：

a) 测试评价方法：模拟授权与非授权管理员访问审计日志，产品安全功能是否仅允许授权管理员访问审计日志。

b) 预期结果：系统应限制审计日志的访问。除了具有明确的访问权限的授权管理员之外，系统应禁止所有其他用户对审计日志的访问。

7.4.2.3.5 可选审计查阅

对可选审计查阅的测试评价方法与预期结果如下：

a) 测试评价方法：审查产品是否能够支持按照一定条件，例如时间、事件级别、攻击源等对审计日志进行检索或排序。

b) 预期结果：系统应应支持按照一定条件对审计日志进行检索或排序。

7.4.2.4 事件记录安全

7.4.2.4.1 安全管理

对安全管理的测试评价方法与预期结果如下：

a) 测试评价方法：模拟授权与非授权管理员访问事件记录，产品安全功能是否仅允许授权管理员访问事件记录。

b) 预期结果：系统应限制对事件记录的访问。除了具有明确的访问权限的授权管理员之外，系统应禁止所有其他用户对事件记录的访问。

7.4.2.4.2 事件记录保护

对事件记录保护的测试评价方法与预期结果如下：

a) 测试评价方法：从已有的事件库中选择具有不同特征的多个事件，组成安全事件测试集，进行测试，对系统生成的事件记录进行破坏，检查系统是否能够及时通知管理员。

b) 预期结果：对系统生成的事件记录进行破坏后，系统能够及时通知管理员。

7.4.2.4.3 事件记录存储安全

对事件记录存储安全的测试评价方法与预期结果如下：

a) 测试评价方法：

1) **检查系统安全功能是否具有存储器剩余空间将耗尽时保证已存储事件记录可用和后续事件记录的存储的功能；**

2) **人为将存储产品事件数据的存储器空间耗至产品默认的告警值以下，查看系统是否提供保证已存储事件记录可用和后续事件记录的存储的措施。**

b) 预期结果：

1) **系统在发生事件数据存储器空间将耗尽的情况时，保证已存储事件记录可用和后续事件记录的存储；**

2) **在发现事件数据存储器空间将耗尽时，系统还应提醒管理员采取措施保证已存储事件记录可用和后续事件记录的存储，可选择例如转存已有事件记录、仅记录重要的事件数据数据等措施之一。**

7.4.2.5 通信保密性

对通信保密性的测试评价方法与预期结果如下：

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保密性的描述。

b) 预期结果：

1) 系统在各组件之间传输数据（如配置和控制信息、告警和事件数据等）时，数据应能够被正常传输；

2) 开发者文档中提供了为保证各组件之间通信保密性所采取措施的详细描述，数据在传输过程中非明文显示。列举系统为保证通信保密性所采取的措施。

7.4.2.6 通信完整性

对通信完整性的测试评价方法与预期结果如下：

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) 预期结果：

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。列举系统为保证通信完整性所采取的措施。**

7.4.2.7 升级安全

对升级安全的测试评价方法与预期结果如下：

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，防止得到错误的或伪造的升级包；

3) 检查开发者文档中对保证升级安全的描述。

b) 预期结果：

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系统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系统升级手段。

7.4.2.8 自我隐藏

对自我隐藏的测试评价方法与预期结果如下：

a) 测试评价方法：检查开发者文档中对系统自身安全的描述。

b) 预期结果：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。

7.4.2.9 自我监测

对自我监测的测试评价方法与预期结果如下：

a) 测试评价方法：

1) 检查开发者文档中对系统自身安全的描述；

2) 检查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，包括硬件工作状态监测、组件连接状态监测等。

b) 预期结果：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 安全保证测试

7.4.3.1 配置管理

7.4.3.1.1 版本号

对版本号的测试评价方法与预期结果如下：

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：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完全对应，没有歧义。

b) 预期结果：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。

7.4.3.1.2 配置项

对配置项的测试评价方法与预期结果如下：

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) 配置管理系统应对所有的配置项作出唯一的标识；

2) 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；

3) 配置管理文档还应描述对配置项给出唯一标识的方法。

b) 预期结果：**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两方面。**

7.4.3.2 交付与运行

7.4.3.2.1 交付程序

对交付程序的测试评价方法与预期结果如下：

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：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) 预期结果：**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、生成和启动程序

对安装、生成和启动程序的测试评价方法与预期结果如下：

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) 预期结果：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 开发

7.4.3.3.1 非形式化功能规范

对非形式化功能规范的测试评价方法与预期结果如下：

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) 预期结果：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 描述性高层设计

对描述性高层设计的测试评价方法与预期结果如下：

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) **表示应是非形式化的；**
2) **是内在一致的；**
3) **按子系统描述安全功能的结构；**
4) **描述每个安全功能子系统所提供的安全功能性；**
5) **标识安全功能所要求的任何基础性的硬件、固件或软件，以及在这些硬件、固件或软件中实现的支持性保护机制所提供功能的一个表示；**

6） **标识安全功能子系统的所有接口；**

7） **标识安全功能子系统的哪些接口是外部可见的。**

b） 预期结果：**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 非形式化对应性证实

对非形式化对应性证实的测试评价方法与预期结果如下：

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、底层设计、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） 预期结果：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，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

对管理员指南的测试评价方法与预期结果如下：

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） 预期结果：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，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

对用户指南的测试评价方法与预期结果如下：

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) 预期结果：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，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 测试

7.4.3.5.1 覆盖证据

对覆盖证据的测试评价方法与预期结果如下：

a) 测试评价方法：**评价者应审查开发者提供的测试覆盖证据，在测试覆盖证据中，是否表明测试文档中所标识的测试与功能规范中所描述的系统的安全功能是对应的。**

b) 预期结果：**审查记录以及最后结果（符合/不符合），开发者提供的测试覆盖证据，应表明测试文档中所标识的测试与功能规范中所描述的系统的安全功能是对应的。**

7.4.3.5.2 功能测试

对功能测试的测试评价方法与预期结果如下：

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) 预期结果：**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，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。**

7.4.3.5.3 独立测试

7.4.3.5.3.1 一致性

对一致性的测试评价方法与预期结果如下：

a) 测试评价方法：评价者应评价开发者提供的测试系统，提供的测试集合是否与其自测系统功能时使用的测试集合相一致，提供的执行测试及其结果是否与其自测系统功能时执行的测试及其结果相一致。

b) 预期结果：审查记录以及最后结果（符合/不符合），开发者应提供适合测试的系统，提供的测试集合应与其自测系统功能时使用的测试集合相一致，提供的执行测试及其结果与其自测系统功能时执行的测试及其结果相一致。

7.4.3.5.3.2 抽样

对抽样的测试评价方法与预期结果如下：

a) 测试评价方法：**评价开发者是否提供一组相当的资源，用于安全功能的抽样测试。**

b) 预期结果：**审查记录以及最后结果（符合/不符合），开发者应提供一组相当的资源，用于安全功能的抽样测试。**

7.4.3.6 脆弱性分析保证

7.4.3.6.1 系统安全功能强度评估

对系统安全功能强度评估的测试评价方法与预期结果如下：

a) 测试评价方法：**评价者应审查开发者提供的指导性文档，是否对所标识的每个具有安全功能强度声明的安全机制进行了安全功能强度分析，是否说明了安全机制达到或超过定义的最低强度级别或特定功能强度度量。**

b) 预期结果：**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。开发者应对指导性文档中所标识的每个具有安全功能强度声明的安全机制进行安全功能强度分析，并说明安全机制达到或超过定义的最低强度级别或特定功能强度度量。**

7.4.3.6.2 开发者脆弱性分析

对开发者脆弱性分析的测试评价方法与预期结果如下：

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) 预期结果：**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。开发者提供的脆弱性分析文档应完整。**

7.5 第三级

7.5.1 安全功能测试

7.5.1.1 数据探测功能测试

7.5.1.1.1 数据收集

对数据收集的测试评价方法与预期结果如下：

a) 测试评价方法：

1) 打开系统的安全策略配置，配置受保护网段；

2) 对受保护网段发起攻击；

3) 检查是否具有实时获取受保护网段内的数据包的能力。

b) 预期结果：系统应能够获取足够的网络数据包以分析安全事件。

7.5.1.1.2 协议分析

对协议分析的测试评价方法与预期结果如下：

a) 测试评价方法：

1) 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；

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，组成安全事件测试集；

3) 配置系统的检测策略为最大策略集；

4) 发送安全事件测试集中的所有事件，记录系统的检测结果。

b) 预期结果：

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分析的协议的事件至少包括以下类型：IP、TCP、UDP、ICMP、ARP、RIP、、RPC、HTTP、FTP、TFTP、IMAP、SNMP、TELNET、DNS、SMTP、POP3、NETBIOS、NFS 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。

7.5.1.1.3 行为监测

对行为监测的测试评价方法与预期结果如下：

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，组成安全事件测试集。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）、文件脆弱性攻击类事件（如 MS-Office 文件脆弱性）、浏览器脆弱性攻击类事件（如 MS-IE 浏览器脆弱性）、应用层安全漏洞攻击以及其他具有代表性的网络安全事件，测试系统；
2） 配置系统的检测策略为最大策略集；
3） 发送安全事件测试集中的所有事件，记录系统的检测结果。

b） 预期结果：
1） 对安全事件测试集的攻击，系统应报告相应的安全事件，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。

7.5.1.1.4 流量监测

对流量监测的测试评价方法与预期结果如下：

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） 预期结果：
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。

7.5.1.2 入侵分析功能测试

7.5.1.2.1 数据分析

对数据分析的测试评价方法与预期结果如下：

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，组成安全事件测试集。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，以及其他具有代表性的安全事件；
2） 配置系统的检测策略为最大策略集；
3） 发送安全事件测试集中的所有事件，记录系统的检测结果。

b） 预期结果：
1） 对安全事件测试集的攻击，系统应报告相应的安全事件，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。

7.5.1.2.2 事件合并

对事件合并的测试评价方法与预期结果如下：

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） 预期结果：
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。

7.5.1.2.3 防躲避能力

对防躲避能力的测试评价方法与预期结果如下：

a） 测试评价方法：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。

b） 预期结果：
1） 系统能够检测出经过分片、乱序之后的安全事件；
2） 系统能够正确地报出经过规避的扫描 HTTP 事件。

7.5.1.2.4 事件关联

对事件关联的测试评价方法与预期结果如下：

a） 测试评价方法：连续生成多个不同的低危害事件，查看系统是否能自动将这些同类低危害事件关联起来，生成高危害事件。

b） 预期结果：系统可以对同类但不同的事件进行关联，从低危害事件中发现隐含的高危害攻击。

7.5.1.3 入侵响应功能测试

7.5.1.3.1 定制响应

对定制响应的测试评价方法与预期结果如下：

a） 测试评价方法：
1） 系统应允许管理员对被检测网段中指定的目的主机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，检查系统是否允许管理员设置仅对被检测网段中指定的目的主机进行告警。

b） 预期结果：管理员可以定制仅监控符合指定条件的目的主机。

7.5.1.3.2 安全告警

对安全告警的测试评价方法与预期结果如下：

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) 预期结果：

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。

7.5.1.3.3 告警方式

对告警方式的测试评价方法与预期结果如下：

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) 预期结果：可以采取屏幕实时提示、Syslog 告警、SNMP trap 消息、E-mail 告警、运行指定应用程序等一种或几种告警方式。记录并列出所有告警方式。

7.5.1.3.4 阻断能力

对阻断能力的测试评价方法与预期结果如下：

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) 选中对安全事件的阻断选项，检查系统在监测到相应攻击时是否进行阻断。

b) 预期结果：

1) 能够对监测到的非法连接配置阻断选项；

2) 在检测到网络上的非法连接时，可成功进行阻断。

7.5.1.3.5 排除响应

对排除响应的测试评价方法与预期结果如下：

a) 测试评价方法：

1) 打开菜单，检查系统是否允许管理员设置对被检测网段中指定的目的主机不予告警；

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) 预期结果：管理员可以定制不监控符合指定条件的目的主机。

7.5.1.3.6 防火墙联动

对防火墙联动的测试评价方法与预期结果如下：

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） 预期结果：

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。

7.5.1.3.7 全局预警

对全局预警的测试评价方法与预期结果如下：

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他控制台是否可以收到预警信息。**

b） 预期结果：

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。**

7.5.1.3.8 其他设备联动

对其他设备联动的测试评价方法与预期结果如下：

a） 测试评价方法：

1） **查看系统是否具有与其他网络设备或网络安全部件（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） 预期结果：

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。**

7.5.1.4 管理控制功能测试

7.5.1.4.1 图形界面

对图形界面的测试评价方法与预期结果如下：

a） 测试评价方法：

1） 登录控制台界面；

2） 查看管理员界面的功能，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） 预期结果：

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。

7.5.1.4.2 事件数据库

对事件数据库的测试评价方法与预期结果如下：
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） 预期结果：
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） 数据库中的内容应包括事件的定义和分析内容、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。

7.5.1.4.3 事件分级

对事件分级的测试评价方法与预期结果如下：
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） 检查界面显示的安全事件是否具备事件级别信息。
b） 预期结果：
1） 事件库的所有事件都具有分级信息；
2） 界面显示的安全事件，都以文字或色彩等形式显示了事件级别。

7.5.1.4.4 策略配置

对策略配置的测试评价方法与预期结果如下：
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） 预期结果：
1） 系统应提供默认的策略，并可以直接应用；
2） 应允许管理员编辑策略；
3） 具有供管理员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。

7.5.1.4.5 事件库升级

对事件库升级的测试评价方法与预期结果如下：
a） 测试评价方法：
1） 检查产品说明书，查看事件特征库的升级方式；
2） 对特征库进行手动或自动的在线升级。
b） 预期结果：
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） 列举事件库升级的方式、承诺的升级频率。

7.5.1.4.6 统一升级

对统一升级的测试评价方法与预期结果如下：
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） 预期结果：
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。

7.5.1.4.7 硬件失效处理

对硬件失效处理的测试评价方法与预期结果如下：
a） 测试评价方法：检查系统具备何种硬件失效处理机制，如硬件失效后，系统具有相应的报警措施。
b） 预期结果：系统应提供硬件失效处理机制，如硬件失效后，系统具有相应的报警措施。

7.5.1.4.8 分布式部署

对分布式部署的测试评价方法与预期结果如下：
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） 预期结果：
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。

7.5.1.4.9 集中管理

对集中管理的测试评价方法与预期结果如下：
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） 检查集中管理中心是否可以同时管理并设置所有控制台和探测器，查看是否有可以显示部署情况的信息（如拓扑图）。
b） 预期结果：
1） 控制台可以管理所有为其部署的探测器；
2） 集中管理中心可以管理部署的控制台；
3） 可以正确显示系统部署的拓扑。

7.5.1.4.10 端口分离

对端口分离的测试评价方法与预期结果如下：
a） 测试评价方法：检查系统是否配备进行产品管理和网络数据监听的端口。
b） 预期结果：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。

7.5.1.4.11 双机热备

对双机热备的测试评价方法与预期结果如下：

a) 测试评价方法：按照产品部署方案进行双机热备环境部署，关闭其中一台设备，查看另一设备是否可以及时工作。

b) 预期结果：对于双机热备部署的环境，当出现一台设备宕机的情况，应不影响网络用户的正常使用。

7.5.1.4.12 系统升级

对系统升级的测试评价方法与预期结果如下：

a) 测试评价方法：

1) 检查控制台的升级方式；

2) 尝试对控制台进行升级；

3) 检查探测器的升级方式；

4) 尝试通过控制台对探测器下发升级程序。

b) 预期结果：

1) 升级的过程中探测器可以正常检测事件；

2) 应通过控制台来下发探测器的升级程序。

7.5.1.4.13 分级管理

对分级管理的测试评价方法与预期结果如下：

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) **有选择地配置从下级控制台读取事件记录、数据类型到上级控制台的数据库中。**

b) 预期结果：

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、数据类型。**

7.5.1.5 检测结果处理要求

7.5.1.5.1 事件记录

对事件记录的测试评价方法与预期结果如下：

a) 测试评价方法：

1) 检查系统是否具有记录事件的数据库，系统应保存检测到的安全事件并记录安全事件信息；

2) 检查数据库是否具有维护功能。

b) 预期结果：

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) 记录的安全事件信息应包含以下内容：事件发生时间、源地址、目的地址、事件等级、事件类型、事件名称、事件详细描述以及解决方案建议等。

7.5.1.5.2 事件可视化

对事件可视化的测试评价方法与预期结果如下：

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安全事件；

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) 预期结果：

1) 具有查看安全事件的图形化界面；

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。

7.5.1.5.3 报告生成

对报告生成的测试评价方法与预期结果如下：

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) 预期结果：

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。

7.5.1.5.4 报告查阅

对报告查阅的测试评价方法与预期结果如下：

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) 预期结果：

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。

7.5.1.5.5 报告输出

对报告输出的测试评价方法与预期结果如下：

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) 预期结果：

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管理员阅读的格式，如 WORD 文件、HTML 文件、文本文件等；报告最好为中文。

7.5.1.6 产品灵活性要求

7.5.1.6.1 报告定制

对报告定制的测试评价方法与预期结果如下：

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) 预期结果：

1） 系统允许管理员定制报告类别、报告内容、报告风格等内容；
2） 列举系统支持的定制内容。

7.5.1.6.2 事件定义

对事件定义的测试评价方法与预期结果如下：

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安全事件，检查系统能否报警。

b） 预期结果：
1） 系统允许管理员自定义事件，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。

7.5.1.6.3 协议定义

对协议定义的测试评价方法与预期结果如下：

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安全事件，检查系统能否报警。

b） 预期结果：
1） 系统允许管理员自定义协议，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。

7.5.1.7 性能要求

7.5.1.7.1 误报率

对误报率的测试评价方法与预期结果如下：

a） 测试评价方法：
1） 在指定的网络带宽（百兆网络、千兆网络、或厂商声明的其他网络带宽）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、或厂商声明的其他网络带宽）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、或厂商声明的其他网络带宽）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、或厂商声明的其他网络带宽)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，查看系统是否报警。

6) 依据已有的事件库，生成多个已知的安全事件，查看系统是否正确报告出了事件名称。

b) 预期结果：

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，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，系统所报告的安全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，并记录误报率。

7.5.1.7.2 漏报率

对漏报率的测试评价方法与预期结果如下：

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，组成安全事件测试集，发送安全事件测试集中的所有事件，记录系统的检测结果；

2) 可选取部分安全事件作为测试基线；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 20%、40%、60%、80%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) 预期结果：

2) 对安全事件测试集的所有攻击，系统应报告相应的安全事件，未报告的事件即为漏报；

3) 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；

4) 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，并记录漏报率。

7.5.1.7.3 流量监控能力

对监控流量的测试评价方法与预期结果如下：

a) 测试评价方法：

1) 选取部分安全事件作为测试基线；加载相应的背景流量——百兆 90 Mbps、千兆 0.9 Gbps、万兆 9 Gbps(例如 HTTP 流量)，将选取的基线攻击发送多次(如 1 000 次)，记录系统的检测结果。

b) 预期结果：

1) 对测试基线的事件，在加载相应的背景流量——百兆 90 Mbps、千兆 0.9 Gbps、万兆 9 Gbps(例如 HTTP 流量)，系统单个监听口应检测到相应的攻击次数(如 1 000 次)并报告；

2) 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。

7.5.1.7.4 并发连接数监控能力

对监控并发连接数的测试评价方法与预期结果如下：

a) 测试评价方法：

1) 选取部分安全事件作为测试基线；加载相应的背景流量——百兆 10 万并发连接数、千兆 100 万并发连接数、万兆 150 万并发连接数(例如 HTTP 流量)，将选取的基线攻击发送多次(如 1 000 次)，记录系统的检测结果。

b) 预期结果：

1) 对测试基线的事件，在加载相应的背景流量——百兆 10 万并发连接数、千兆 100 万并发连接数、万兆 150 万并发连接数(例如 HTTP 流量)，系统单个监听口应检测到相应的攻击次数(如 1 000 次)并报告；

2) 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。

7.5.1.7.5 新建 TCP 连接速率监控能力

对监控新建 TCP 连接速率的测试评价方法与预期结果如下：

a) 测试评价方法：

1) 选取部分安全事件作为测试基线；加载相应的背景流量——百兆每秒新建 TCP 连接数 6 万个、千兆每秒新建 TCP 连接数 10 万个、万兆每秒新建 TCP 连接数 15 万个(例如 HTTP 流量)，将选取的基线攻击发送多次(如 1 000 次)，记录系统的检测结果。

b) 预期结果：

1) 对测试基线的事件，在加载相应的背景流量——百兆每秒新建 TCP 连接数 6 万个、千兆每秒新建 TCP 连接数 10 万个、万兆每秒新建 TCP 连接数 15 万个(例如 HTTP 流量)，系统单个监听口应检测到相应的攻击次数(如 1 000 次)并报告；

2) 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。

7.5.1.7.6 还原能力

对还原能力的测试评价方法与预期结果如下：

a) 测试评价方法：

1) **开启系统的内容还原(回放)功能，检查可还原的入侵行为；**

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

b) 预期结果：

1) **系统具有内容回放功能；**

2) **对可回放的入侵行为，可以进行内容恢复和事件还原(回放)。**

7.5.2 自身安全功能测试

7.5.2.1 身份鉴别

7.5.2.1.1 管理员鉴别

对管理员鉴别的测试评价方法与预期结果如下：

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) 预期结果：

1) 在管理员执行任何与安全功能相关的操作之前都应对管理员进行鉴别；

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） 允许管理员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。

7.5.2.1.2 鉴别失败的处理

对鉴别失败的处理的测试评价方法与预期结果如下：

a） 测试评价方法：
1） 检查系统的安全功能是否可定义管理员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管理员鉴别尝试失败连续达到指定次数后，采取相应的措施、阻止管理员进一步的鉴别请求；
3） 尝试多次失败的管理员鉴别行为，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） 预期结果：
1） 系统应具备定义管理员鉴别尝试的最大允许失败次数的功能；
2） 系统应定义当管理员鉴别尝试失败连续达到指定次数后，采取相应的措施（如锁定该账号）；
3） 当管理员鉴别尝试失败连续达到指定次数后，系统应锁定该账号，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。

7.5.2.1.3 鉴别数据保护

对鉴别数据保护的测试评价方法与预期结果如下：

a） 测试评价方法：
1） 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；
2） 以非授权管理员的身份尝试查阅或修改身份鉴别数据。

b） 预期结果：系统应仅允许指定的角色查阅或修改身份鉴别数据。
1） 系统应仅允许指定的角色查阅或修改身份鉴别数据；
2） 非授权管理员无法查阅或修改身份鉴别数据。

7.5.2.1.4 超时设置

对超时设置的测试评价方法与预期结果如下：

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，检查登录管理员在设定的时间段内没有任何操作的情况下，系统是否锁定或终止了会话，管理员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） 预期结果：
1） 系统应具有登录超时重新鉴别功能；
2） 任何登录管理员在设定的时间段内没有任何操作的情况下，应被锁定或终止了会话，管理员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。

7.5.2.1.5 控制台鉴别

对控制台鉴别的测试评价方法与预期结果如下：

a) 测试评价方法：通过控制台连接引擎，检查是否在执行所有功能之前要求首先进行控制台认证。

b) 预期结果：

1) 在通过控制台连接引擎执行任何与安全功能相关的操作之前都应对控制台进行鉴别；

2) 控制台连接引擎后，允许通过控制台执行与安全功能相关的各类操作时，不再重复认证。

7.5.2.1.6 多重鉴别机制

对多重鉴别机制的测试评价方法与预期结果如下：

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) 预期结果：

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。**

7.5.2.1.7 会话锁定

对会话锁定的测试评价方法与预期结果如下：

a) 测试评价方法：**登录系统，检查是否允许管理员锁定当前的交互会话。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) 预期结果：

1) **系统应允许管理员锁定当前的交互会话；**

2) **锁定后，管理员需要再次进行身份鉴别才能够重新管理系统。**

7.5.2.2 管理员管理

7.5.2.2.1 标识唯一性

对标识唯一性的测试评价方法与预期结果如下：

a) 测试评价方法：

1) 尝试定义多个管理员；

2) 尝试添加一个已有标识的管理员；

3) 检查系统是否提示该标识管理员已存在，拒绝具有相同标识管理员的添加。

b) 预期结果：

1) 系统应允许定义多个管理员；

2) 应保证每一个管理员标识是全局唯一的，不允许一个管理员标识用于多个管理员。

7.5.2.2.2 管理员属性定义

对管理员属性定义的测试评价方法与预期结果如下：

a) 测试评价方法：定义分属于不同角色的多个管理员，检查输入的管理员信息是否都能被保存。

b) 预期结果：系统应为每一个管理员保存其安全属性，包括管理员标识、鉴别数据（如密码）、授权信息或管理员组信息、其他安全属性等。输入的管理员信息无丢失现象发生。

7.5.2.2.3 安全行为管理

对安全行为管理的测试评价方法与预期结果如下：

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) 预期结果：

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。

7.5.2.2.4 管理员角色

对管理员角色的测试评价方法与预期结果如下：

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管理员。

b) 预期结果：

1) 系统应允许定义多个角色的管理员；

2) 每个角色可以具有多个管理员，每个管理员只能属于一个角色；

3) 应保证每一个角色标识是全局唯一的，不允许一个角色标识用于多个角色。

7.5.2.2.5 安全属性管理

对安全属性管理的测试评价方法与预期结果如下：

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) 预期结果：

1) 系统应仅允许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 安全审计

7.5.2.3.1 审计日志生成

对审计日志生成的测试评价方法与预期结果如下：

a) 测试评价方法：结合开发者文档，使用不同角色管理员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。审查审计日志的正确性。

b) 预期结果：

1) 系统应至少为下述可审计事件产生审计日志：鉴别失败等重大事件、升级时间和版本号等；

2) 应在每个审计日志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。

7.5.2.3.2 审计日志可理解性

对审计日志可理解性的测试评价方法与预期结果如下：

a) 测试评价方法：审查产品安全功能是否使审计日志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) 预期结果：系统应提供为人理解的审计日志。

7.5.2.3.3 审计日志查阅

对审计日志查阅的测试评价方法与预期结果如下：

a) 测试评价方法：

1) 以授权管理员身份尝试从审计日志中读取全部审计信息；

2) 审查产品安全功能是否为授权管理员提供从审计日志中读取全部审计信息的功能。

b) 预期结果：系统应为授权管理员提供从审计日志中读取全部审计信息的功能。

7.5.2.3.4 受限的审计日志查阅

对受限的审计日志查阅的测试评价方法与预期结果如下：

a) 测试评价方法：模拟授权与非授权管理员访问审计日志，产品安全功能是否仅允许授权管理员访问审计日志。

b) 预期结果：系统应限制审计日志的访问。除了具有明确的访问权限的授权管理员之外，系统应禁止所有其他用户对审计日志的访问。

7.5.2.3.5 可选审计查阅

对可选审计查阅的测试评价方法与预期结果如下：

a) 测试评价方法：审查产品是否能够支持按照一定条件，例如时间、事件级别、攻击源等对审计日志进行检索或排序。

b) 预期结果：系统应应支持按照一定条件对审计日志进行检索或排序。

7.5.2.4 事件记录安全

7.5.2.4.1 安全管理

对安全管理的测试评价方法与预期结果如下：

a) 测试评价方法：模拟授权与非授权管理员访问事件记录，产品安全功能是否仅允许授权管理员访问事件记录。

b) 预期结果：系统应限制对事件记录的访问。除了具有明确的访问权限的授权管理员之外，系统应禁止所有其他用户对事件记录的访问。

7.5.2.4.2 事件记录保护

对事件记录保护的测试评价方法与预期结果如下：

a) 测试评价方法：从已有的事件库中选择具有不同特征的多个事件，组成安全事件测试集，进行测试，对系统生成的事件记录进行破坏，检查系统是否能够及时通知管理员。

b) 预期结果：对系统生成的事件记录进行破坏后，系统能够及时通知管理员。

7.5.2.4.3 事件记录存储安全

对事件记录存储安全的测试评价方法与预期结果如下：

a) 测试评价方法：

1) 检查系统安全功能是否具有存储器剩余空间将耗尽时保证已存储事件记录可用和后续事件记录的存储的功能；

2) 人为将存储产品事件数据的存储器空间耗至产品默认的告警值以下，查看系统是否提供保证已存储事件记录可用和后续事件记录的存储的措施。

b) 预期结果：

1) 系统在发生事件数据存储器空间将耗尽的情况时，保证已存储事件记录可用和后续事件记录的存储；

2) 在发现事件数据存储器空间将耗尽时，系统还应提醒管理员采取措施保证已存储事件记录可用和后续事件记录的存储，可选择例如转存已有事件记录、仅记录重要的事件数据数据等措施之一。

7.5.2.4.4 事件记录存储告警

对事件记录存储告警的测试评价方法与预期结果如下：

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管理员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) 预期结果：

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) **系统允许管理员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，系统还应提醒管理员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。**

7.5.2.5 通信保密性

对通信保密性的测试评价方法与预期结果如下：

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保密性的描述。

b) 预期结果：

1) 系统在各组件之间传输数据（如配置和控制信息、告警和事件数据等）时，数据应能够被正常传输；

2) 开发者文档中提供了为保证各组件之间通信保密性所采取措施的详细描述，数据在传输过程中非明文显示。列举系统为保证通信保密性所采取的措施。

7.5.2.6 通信完整性

对通信完整性的测试评价方法与预期结果如下：

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) 预期结果：

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。列举系统为保证通信完整性所采取的措施。

7.5.2.7 升级安全

对升级安全的测试评价方法与预期结果如下：

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，防止得到错误的或伪造的升级包；

3） 检查开发者文档中对保证升级安全的描述。

b） 预期结果：

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系统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系统升级手段。

7.5.2.8 自我隐藏

对自我隐藏的测试评价方法与预期结果如下：

a） 测试评价方法：检查开发者文档中对系统自身安全的描述。

b） 预期结果：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。

7.5.2.9 自我监测

对自我监测的测试评价方法与预期结果如下：

a） 测试评价方法：

1） 检查开发者文档中对系统自身安全的描述；

2） 检查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，包括硬件工作状态监测、组件连接状态监测等。

b） 预期结果：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。

7.5.3 安全保证测试

7.5.3.1 配置管理

7.5.3.1.1 配置管理能力

7.5.3.1.1.1 版本号

对版本号的测试评价方法与预期结果如下：

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：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完全对应，没有歧义。

b） 预期结果：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。

7.5.3.1.1.2 配置项

对配置项的测试评价方法与预期结果如下：

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) 配置管理系统应对所有的配置项作出唯一的标识；

2) 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；

3) 配置管理文档还应描述对配置项给出唯一标识的方法。

b) 预期结果：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三方面。

7.5.3.1.1.3 授权控制

对授权控制的测试评价方法与预期结果如下：

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) **配置管理系统应保证只有经过授权才能修改配置项；**

2) **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；**

3) **配置管理文档还应提供所有的配置项得到有效维护的证据。**

b) 预期结果：**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三方面。开发者提供的配置管理内容应完整。**

7.5.3.1.2 配置管理覆盖

对配置管理覆盖的测试评价方法与预期结果如下：

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，要求将系统的交付与运行文档、开发文档、指导性文档、生命周期支持文档、测试文档、脆弱性分析文档和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) 预期结果：**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 交付程序

对交付程序的测试评价方法与预期结果如下：

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：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) 预期结果：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)。

7.5.3.2.2 安装、生成和启动程序

对安装、生成和启动程序的测试评价方法与预期结果如下:

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) 预期结果: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 开发

7.5.3.3.1 非形式化功能规范

对非形式化功能规范的测试评价方法与预期结果如下:

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) 预期结果: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

7.5.3.3.2.1 描述性高层设计

对描述性高层设计的测试评价方法与预期结果如下:

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) 表示应是非形式化的;
2) 是内在一致的;
3) 按子系统描述安全功能的结构;
4) 描述每个安全功能子系统所提供的安全功能性;
5) 标识安全功能所要求的任何基础性的硬件、固件或软件,以及在这些硬件、固件或软件中实现的支持性保护机制所提供功能的一个表示;
6) 标识安全功能子系统的所有接口;
7) 标识安全功能子系统的哪些接口是外部可见的。

b) 预期结果: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。

7.5.3.3.2.2 安全加强的高层设计

对安全加强的高层设计的测试评价方法与预期结果如下:

a) 测试评价方法:

评价者应审查开发者所提供的安全加强高层设计是否满足如下要求:

1） **描述系统的功能子系统所有接口的用途与使用方法，适当时应提供效果、例外情况和错误消息的细节；**

2） **把系统分成安全策略实施和其他子系统来描述。**

b） 预期结果：**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两个方面。**

7.5.3.3.3 非形式化对应性证实

对非形式化对应性证实的测试评价方法与预期结果如下：

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、底层设计、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） 预期结果：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，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

对管理员指南的测试评价方法与预期结果如下：

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） 预期结果：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，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

对用户指南的测试评价方法与预期结果如下：

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） 预期结果：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，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 生命周期支持

对生命周期支持的测试评价方法与预期结果如下：

a） 测试评价方法：**评价者应审查开发者所提供的开发安全文档是否满足如下要求：描述在系统的开发环境中，为保护系统设计和实现的保密性和完整性所必需的所有物理的、程序的、人员的和其他方面的安全措施，并应提供在系统的开发和维护过程中执行安全措施的证据。**

b） 预期结果：**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，开发者提供的开发安全文档应完整。**

7.5.3.6 测试

7.5.3.6.1 测试覆盖

7.5.3.6.1.1 覆盖证据

对覆盖证据的测试评价方法与预期结果如下：

a） 测试评价方法：评价者应审查开发者提供的测试覆盖证据，在测试覆盖证据中，是否表明测试文档中所标识的测试与功能规范中所描述的系统的安全功能是对应的。

b） 预期结果：审查记录以及最后结果（符合/不符合），开发者提供的测试覆盖证据，应表明测试文档中所标识的测试与功能规范中所描述的系统的安全功能是对应的。

7.5.3.6.1.2 覆盖分析

对覆盖分析的测试评价方法与预期结果如下：

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） 预期结果：**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

对测试深度的测试评价方法与预期结果如下：

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） 预期结果：**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，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

对功能测试的测试评价方法与预期结果如下：

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） 预期结果：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，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 独立测试

7.5.3.6.4.1 一致性

对一致性的测试评价方法与预期结果如下：

a） 测试评价方法：评价者应评价开发者提供的测试系统，提供的测试集合是否与其自测系统功能时使用的测试集合相一致，提供的执行测试及其结果是否与其自测系统功能时执行的测试及其结果相一致。

b） 预期结果：审查记录以及最后结果（符合/不符合），开发者应提供适合测试的系统，提供的测试集合应与其自测系统功能时使用的测试集合相一致，提供的执行测试及其结果与其自测系统功能时执行的测试及其结果相一致。

7.5.3.6.4.2 抽样

对抽样的测试评价方法与预期结果如下：

a） 测试评价方法：评价开发者是否提供一组相当的资源，用于安全功能的抽样测试。

b） 预期结果：审查记录以及最后结果（符合/不符合），开发者应提供一组相当的资源，用于安全功能的抽样测试。

7.5.3.7 脆弱性分析保证

7.5.3.7.1 指南审查

对指南审查的测试评价方法与预期结果如下：

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） 预期结果：**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 系统安全功能强度评估

对系统安全功能强度评估的测试评价方法与预期结果如下：

a) 测试评价方法：评价者应审查开发者提供的指导性文档，是否对所标识的每个具有安全功能强度声明的安全机制进行了安全功能强度分析，是否说明了安全机制达到或超过定义的最低强度级别或特定功能强度度量。

b) 预期结果：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。开发者应对指导性文档中所标识的每个具有安全功能强度声明的安全机制进行安全功能强度分析，并说明安全机制达到或超过定义的最低强度级别或特定功能强度度量。

7.5.3.7.3 开发者脆弱性分析

对开发者脆弱性分析的测试评价方法与预期结果如下：

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) 预期结果：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。开发者提供的脆弱性分析文档应完整。

参 考 文 献

[1] GB/T 18336.2—2008 信息技术 信息技术安全性评估准则 第2部分:安全功能要求(ISO/IEC 15408-2:2005, IDT)

[2] GB/T 18336.3—2008 信息技术 信息技术安全性评估准则 第3部分:安全保证要求(idt ISO/IEC 15408-3:2005, IDT)

中 华 人 民 共 和 国
国 家 标 准
信息安全技术 网络入侵检测系统
技术要求和测试评价方法
GB/T 20275—2013
*
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(100029)
北京市西城区三里河北街16号(100045)
网址:www.gb168.cn
服务热线:400-168-0010
010-68522006
2014年5月第一版
*
书号:155066·1-49157

GB/T 20275-2013