ICS 35.240
A 90

GA

中华人民共和国公共安全行业标准

GA/T 403.1—2014
代替 GA/T 403.1—2002

信息安全技术 入侵检测产品安全技术要求 第1部分：网络型产品

Information security technology—Security technical requirements for intrusion detection products—Part 1: Network-based products

2014-03-24 发布　　2014-03-24 实施

中华人民共和国公安部　发布

目　　次

前　言

GA/T 403《信息安全技术　入侵检测产品安全技术要求》分为两个部分：

——第1部分：网络型产品；

——第2部分：主机型产品。

本部分为GA/T 403的第1部分。

本部分按照GB/T 1.1—2009给出的规则起草。

本部分代替GA/T 403.1—2002《信息技术　入侵检测产品安全技术要求　第1部分：网络型产品》，与GA/T 403.1—2002相比主要技术变化如下：

——标准名称修改为《信息安全技术　入侵检测产品安全技术要求　第1部分：网络型产品》；

——增加了网络型入侵检测产品描述(见第5章)；

——增加了安全环境，包括假设、威胁和组织安全策略(见第6章)；

——增加了安全目的，包括产品安全目的和环境安全目的(见第7章)；

——删除了对网络型入侵检测产品的性能要求(见2002年版的第7章)；

——删除了数据库支持(见2002年版的6.1.5.5)；

——修改了安全功能要求的内容(见第8章，2002年版的第8章)；

——增加了技术要求基本原理，包括安全功能要求基本原理和安全保证要求基本原理(见第10章)。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本部分由公安部网络安全保卫局提出。

本部分由公安部信息系统安全标准化技术委员会归口。

本部分起草单位：公安部计算机信息系统安全产品质量监督检验中心、蓝盾信息安全技术股份有限公司、公安部第三研究所。

本部分主要起草人：宋好好、吴其聪、李毅、顾健、胡维娜、赵云、杨辰钟。

本部分所代替标准的历次版本发布情况为：

——GA/T 403.1—2002。

引　言

GA/T 403 的本部分详细描述了与网络型入侵检测产品安全环境相关的假设、威胁和组织安全策略，定义了网络型入侵检测产品及其支撑环境的安全目的，通过基本原理论证安全功能要求能够追溯并覆盖产品安全目的，安全目的能够追溯并覆盖安全环境相关的假设、威胁和组织安全策略。

本部分基本级参照了 GB/T 18336.3—2008 中规定的 EAL2 级安全保证要求，增强级在 EAL4 级安全保证要求的基础上，将脆弱性分析要求提升到可以抵御中等攻击潜力的攻击者发起的攻击。

本部分仅给出了网络型入侵检测产品应满足的安全技术要求，但对网络型入侵检测产品的具体技术实现方式、方法等不做要求。

信息安全技术
入侵检测产品安全技术要求
第1部分:网络型产品

1 范围

GA/T 403的本部分规定了网络型入侵检测产品的安全功能要求、安全保证要求及等级划分要求。

本部分适用于网络型入侵检测产品的设计、开发及检测。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件,仅注日期的版本适用于本文件。凡是不注日期的引用文件,其最新版本(包括所有的修改单)适用于本文件。

GB 17859—1999 计算机信息系统 安全保护等级划分准则

GB/T 18336—2008(所有部分) 信息技术 安全技术 信息技术安全性评估准则

GB/T 25069—2010 信息安全技术 术语

3 术语和定义

GB 17859—1999、GB/T 18336—2008(所有部分)和GB/T 25069—2010界定的以及下列术语和定义适用于本文件。

3.1

入侵 intrusion

任何企图危害资源完整性、保密性或可用性的行为。

3.2

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网络型入侵检测产品组件。安装在网络的关键节点处,监听流经网络的数据。

3.3

控制台 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、升级事件库以及其他管理工作,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。

3.4

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。

3.5

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。

3.6

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。

3.7

强力攻击 brute force

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 Protocol）

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 网络型入侵检测产品描述

网络型入侵检测产品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，从而发现异常行为并报警。

网络型入侵检测产品采用旁路模式接入目标网络。在旁路模式下，网络型入侵检测产品旁路连接在目标网络中，网络型入侵检测产品通过采集交换机镜像口网络通讯数据工作。图1为网络型入侵检测产品旁路模式的一个典型运行环境。

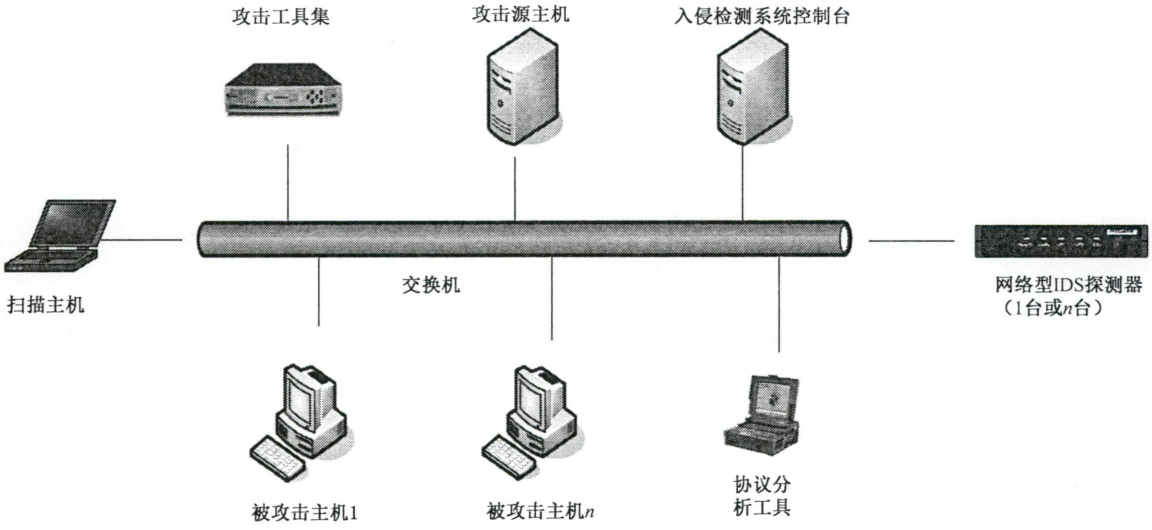

图 1　网络型入侵检测产品典型运行环境

6　安全环境

6.1　假设

网络型入侵检测产品安全环境相关的假设如表 1 所示。

表 1　假设

假设名称	假设描述
物理访问	产品的处理资源应限定在受控的访问设备内，以防止未授权的物理访问。所有实施产品安全策略相关的硬件和软件应受到保护，以免受非授权的物理更改
人员能力	授权管理员是无恶意的，训练有素的，并遵循管理员指南
连接性	产品应部署在受监测网络的出口处，能够获取到受监测网络中的所有通讯数据
安全维护	当产品的应用环境发生变化时，应立即反映在产品的安全策略中并保持其安全功能有效

6.2　威胁

网络型入侵检测产品安全环境相关的威胁如表 2 所示。

表 2　威胁

威胁名称	威胁描述
入侵攻击	网络中有可能存在未被发现的端口扫描、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、网络蠕虫攻击等攻击行为
事件记录失败	产品可能未成功记录相关安全事件；恶意用户可能通过耗尽审计数据存储空间的方法，导致事件记录的丢失或失败，从而掩盖攻击行为
非授权访问	恶意用户可能试图访问和使用产品提供的安全功能

表 2（续）

威胁名称	威胁描述
信息泄漏	恶意用户可能浏览远程授权管理员和产品之间发送的安全相关信息
暴力认证	恶意用户可能通过反复猜测鉴别数据的方法，从而获取管理员权限
漏洞攻击	恶意用户可能利用产品自身的安全机制进行攻击，导致产品权限丢失或功能故障

6.3 组织安全策略

网络型入侵检测产品安全环境相关的组织安全策略如表 3 所示。

表 3 组织安全策略

组织安全策略名称	组织安全策略描述
审计	为追踪所有与安全相关活动的责任，与安全相关的事件应记录、保存和审查
安全管理	产品应为授权管理员提供管理手段，使其以安全的方式进行管理

7 安全目的

7.1 产品安全目的

表 4 定义了产品的安全目的。这些安全目的旨在对应已标识的威胁或组织安全策略。

表 4 产品安全目的

产品安全目的名称	产品安全目的描述	对应的威胁或组织安全策略
入侵检测	产品应通过数据收集、协议分析对目标网络中的网络数据进行分析，检测出入侵攻击	入侵攻击
事件记录	产品应记录和统计攻击行为，记录应具有精确的日期和时间；且产品应提供基本的防止事件记录丢失或失败的措施	事件记录失败
身份认证	在允许用户访问产品功能之前，产品应对用户身份进行唯一的标识和鉴别	非授权访问
安全管理	产品应向授权管理员提供以安全方式进行管理的有效手段	安全管理
信息保密	如果产品允许通过相连网络对其进行远程管理，那么它应保证远程管理信息的保密性	信息泄漏
鉴别失败处理	产品应具备安全机制防止恶意用户反复猜测鉴别数据	暴力认证
操作系统加固	为更好地防范产品自身的漏洞，产品应确保底层支撑系统的可靠性和稳定性	漏洞攻击
审计	产品应记录自身安全相关的事件，以便追踪安全相关行为的责任，并应提供方法审查所记录的数据	审计

7.2 环境安全目的

表5定义了非技术或程序方法进行处理的安全目的。6.1确定的假设被包含在环境安全目的中。

表5 环境安全目的

环境安全目的名称	环境安全目的描述	对应的假设或威胁
物理访问	产品的处理资源应限定在受控的访问设备内，以防止未授权的物理访问。所有实施产品安全策略相关的硬件和软件应受到保护，以免受非授权的物理更改	物理访问
人员能力	管理员是无恶意的，训练有素的，并遵循管理员指南	人员能力
连接性	产品应能够采集目标网络中所有的网络通讯数据	连接性
安全维护	当产品的应用环境发生变化时，应立即反应在产品的安全策略中并保持其安全功能有效	安全维护

8 安全功能要求

8.1 数据探测功能要求

8.1.1 数据收集

产品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。

8.1.2 协议分析

产品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。

8.1.3 行为监测

产品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。

8.1.4 流量监测

产品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。

8.2 入侵分析功能要求

8.2.1 数据分析

产品应对收集的数据包进行分析，发现攻击事件。

8.2.2 分析方式

产品应以模式匹配、协议分析、人工智能等一种或多种方式进行入侵分析。

8.2.3 防躲避能力

产品应能发现躲避或欺骗检测的行为，如IP碎片重组，TCP流重组，协议端口重定位，URL字符

串变形，shell 代码变形等。

8.2.4 事件合并

产品应具有对高频度发生的相同安全事件进行合并告警，避免出现告警风暴的能力。

8.2.5 事件关联

产品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。

8.3 入侵响应功能要求

8.3.1 安全告警

当产品检测到入侵时，应自动采取相应动作以发出安全警告。

8.3.2 告警方式

产品应能通过屏幕实时提示、E-mail、声音等方式告警。

8.3.3 排除响应

产品应允许管理员定义对被检测网段中指定的目标主机或特定的事件不予告警，降低误报。

8.3.4 定制响应

产品应允许管理员对被检测网段中指定的目标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。

8.3.5 防火墙联动

产品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。

8.3.6 全局预警

产品应具有全局预警功能，通过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。

8.3.7 入侵管理

产品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。

8.3.8 其他设备联动

产品应具有与其他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。

8.4 管理控制功能要求

8.4.1 图形界面

产品应提供图形化的管理界面用于管理、配置产品。管理配置界面应包含配置和管理产品所需的所有功能。

8.4.2 事件数据库

产品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。

8.4.3 事件分级

产品应按照事件的严重程度将事件分级。

8.4.4 策略配置

产品应提供产品策略配置方法和手段。

8.4.5 产品升级

产品应具有更新、升级产品和事件库的能力。

8.4.6 统一升级

产品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。

8.4.7 分布式部署

产品应具有本地或异地分布式部署、远程管理的能力。

8.4.8 集中管理

产品应设置集中管理中心，对分布式、多级部署的入侵检测产品进行统一集中管理，形成多级管理结构。

8.4.9 同台管理

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

8.4.10 端口分离

产品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。

8.4.11 双机热备

如果产品为硬件，应提供硬件失效处理机制，具备双机热备能力。

8.4.12 多级管理

产品应具有多级管理的能力。

8.5 检测结果处理要求

8.5.1 事件记录

产品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。

8.5.2 事件可视化

管理员应能通过管理界面实时清晰地查看入侵事件。

8.5.3 报告生成

产品应能生成详尽的检测结果报告。

8.5.4 报告查阅

产品应具有浏览检测结果报告的功能。

8.5.5 报告输出

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

8.6 产品灵活性要求

8.6.1 报告定制

产品应支持授权管理员按照自己的要求修改和定制报告内容。

8.6.2 窗口定义

产品应支持管理员自定义窗口显示的内容和显示方式。

8.6.3 事件定义

产品应允许授权管理员自定义事件，或者对默认提供的事件做修改，并应提供定义方法。

8.6.4 协议定义

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

8.6.5 通用接口

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

8.7 身份鉴别

8.7.1 管理员鉴别

产品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。

8.7.2 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，产品应锁定该账号或登录 IP。最多失败次数仅由授权管理员设定。

8.7.3 鉴别数据保护

产品应保护鉴别数据不被未授权查阅和修改。

8.7.4 超时设置

产品应具有管理员登录超时重新鉴别功能。在设定的时间段内没有任何操作的情况下，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。

8.7.5 多鉴别机制

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

8.7.6 会话锁定

产品应允许管理员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。

8.8 管理员管理

8.8.1 标识唯一性

产品应保证所设置的管理员标识全局唯一。

8.8.2 用户属性定义

产品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。

8.8.3 安全行为管理

产品应仅允许授权管理员对产品的功能具有禁止、修改的能力。

8.8.4 管理员角色

产品应设置多个角色，不同的角色具有不同的管理权限，以增加产品管理的安全性。

8.8.5 安全属性管理

产品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。

8.9 安全审计

8.9.1 审计数据生成

产品应能为下述可审计事件产生审计记录：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。

8.9.2 审计数据可用性

审计数据的记录方式应便于管理员理解。

8.9.3 审计查阅

产品应为授权管理员提供从审计记录中读取全部审计信息的功能。

8.9.4 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，产品应禁止所有非授权管理员对审计记录的读访问。

8.10 事件数据安全

8.10.1 安全数据管理

产品应仅限于指定的授权角色访问事件数据，禁止其他管理员对事件数据的操作。

8.10.2 数据保护

产品应在遭受攻击时，能够完整保留已经保存的事件数据。

8.10.3 数据存储安全

产品应在发生事件数据存储器空间将耗尽等情况时，采取措施避免最新事件数据丢失。

8.10.4 数据存储告警

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

8.11 通信安全

8.11.1 通信完整性

产品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）不被泄露或篡改。

8.11.2 通信稳定性

产品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。

8.11.3 升级安全

产品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。

8.12 产品自身安全

8.12.1 自我隐藏

产品应采取隐藏探测器 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。

8.12.2 自我监测

产品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。

9 安全保证要求

9.1 配置管理

9.1.1 部分配置管理自动化

配置管理系统应提供一种自动方式来支持产品的生成，通过该方式确保只能对产品的实现表示进行已授权的改变。

配置管理计划应描述在配置管理系统中所使用的自动工具，并描述在配置管理系统中如何使用自

动工具。

9.1.2 配置管理能力

9.1.2.1 版本号

开发者应为产品的不同版本提供唯一的标识。

9.1.2.2 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产品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。

9.1.2.3 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。

9.1.2.4 产生支持和接受程序

开发者提供的配置管理文档应包括一个接受计划，接受计划应描述用来接受修改过的或新建的作为产品组成部分的配置项的程序。

配置管理系统应支持产品的生成。

9.1.3 配置管理范围

9.1.3.1 配置管理覆盖

配置管理范围至少应包括产品实现表示、设计文档、测试文档、指导性文档、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。

9.1.3.2 问题跟踪配置管理覆盖

配置管理范围应包括安全缺陷，确保安全缺陷置于配置管理系统之下。

9.2 交付与运行

9.2.1 交付程序

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。

9.2.2 修改检测

交付文档应描述如何提供多种程序和技术上的措施来检测修改，或检测开发者的主拷贝和用户方所收到版本之间的任何差异。还应描述如何使用多种程序来发现试图伪装成开发者，甚至是在开发者没有向用户方发送任何东西的情况下，向用户方交付产品。

9.2.3 安装、生成和启动程序

开发者应提供文档说明产品的安装、生成和启动的过程。

9.3 开发

9.3.1 功能规范

9.3.1.1 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产品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，适当时提供效果、例外情况和错误消息的细节；
d) 完备地表示产品安全功能。

9.3.1.2 充分定义的外部接口

功能规范应包括安全功能是完备地表示的合理性。

9.3.2 高层设计

9.3.2.1 描述性高层设计

开发者应提供产品安全功能的高层设计，高层设计应满足以下要求：

a) 表示是非形式化的；
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。

9.3.2.2 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) 描述产品的功能子系统所有接口的用途与使用方法，适当时提供效果、例外情况和错误消息的细节；
b) 把产品分成安全策略实施和其他子系统来描述。

9.3.3 安全功能实现的子集

实现表示应当无歧义而且详细地定义安全功能，使得无须进一步设计就能生成安全功能。实现表示应是内在一致的。

9.3.4 描述性低层设计

开发者应提供产品安全功能的低层设计，低层设计应满足以下要求：

a) 表示是非形式化的；
b) 是内在一致的；
c) 按模块描述安全功能；
d) 描述每个模块的用途；

e) 根据所提供的安全功能性和对其他模块的依赖关系两方面来定义模块间的相互关系；
f) 描述每个安全策略实施功能是如何被提供的；
g) 标识安全功能模块的所有接口；
h) 标识安全功能模块的哪些接口是外部可见的；
i) 描述安全功能模块所有接口的用途和用法，适当时提供效果、例外情况和错误消息的细节；
j) 把产品分为安全策略实施模块和其他模块来描述。

9.3.5 非形式化对应性证实

开发者应提供产品安全功能表示的所有相邻对之间的对应性分析。

对于产品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。

9.3.6 非形式化产品安全策略模型

开发者应提供安全策略模型，安全策略模型应满足以下要求：
a) 表示是非形式化的；
b) 描述所有能被模型化的安全策略的规则与特征；
c) 包含合理性，即论证该模型相对所有能被模型化的安全策略来说是一致的，而且是完备的；
d) 阐明安全策略模型和功能规范之间的对应性，即论证所有功能规范中的安全功能对于安全策略模型来说是一致的，而且是完备的。

9.4 指导性文档

9.4.1 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) 怎样安全地管理产品；
c) 在安全处理环境中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，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。

9.4.2 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。

9.5 生命周期支持

9.5.1 安全措施标识

开发者应提供开发安全文档。

开发安全文档应描述在产品的开发环境中，为保护产品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，并应提供在产品的开发和维护过程中执行安全措施的证据。

9.5.2 开发者定义的生命周期模型

开发者应建立一个生命周期模型对产品的开发和维护进行的必要控制，并提供生命周期定义文档描述用于开发和维护产品的模型。

9.5.3 明确定义的开发工具

开发者应明确定义用于开发产品的工具，并提供开发工具文档无歧义地定义实现中每个语句的含义和所有依赖于实现的选项的含义。

9.6 测试

9.6.1 测试覆盖

9.6.1.1 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产品的安全功能是对应的。

9.6.1.2 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产品的安全功能之间的对应性是完备的。

9.6.2 测试：高层设计

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产品的功能是依照其高层设计运行的。

9.6.3 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。

9.6.4 独立测试

9.6.4.1 一致性

开发者应提供适合测试的产品，提供的测试集合应与其自测产品功能时使用的测试集合相一致。

9.6.4.2 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。

9.7 脆弱性评定

9.7.1 误用

9.7.1.1 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) 标识所有可能的产品运行模式(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。

9.7.1.2 分析确认

开发者应提供分析文档论证指导性文档是完备的。

9.7.2 产品安全功能强度评估

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。

9.7.3 脆弱性分析

9.7.3.1 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，对产品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产品的环境中，该脆弱性不能被利用。

9.7.3.2 独立的脆弱性分析

开发者应提供文档证明经过标识脆弱性的产品可以抵御明显的穿透性攻击。

9.7.3.3 中级抵抗力

开发者应提供文档证明产品可以抵御中级强度的穿透性攻击，并提供证据说明对脆弱性的搜索是系统化的。

10 技术要求基本原理

10.1 安全功能要求基本原理

表 6 说明了安全功能要求的充分必要性的基本原理，即每个产品安全目的都至少有一个安全功能要求与其对应，每个安全功能要求都至少解决了一个产品安全目的，因此安全功能要求是充分和必要的。表 6 中的“√”即表明对应关系。

表 6 安全功能要求基本原理

安全功能要求		入侵检测	事件记录	身份认证	安全管理	信息保密	鉴别失败处理	操作系统加固	审计
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	√							
	防火墙联动	√							
	全局预警	√							
	入侵管理								
	其他设备联动	√							
管理控制功能要求	图形界面	√							
	事件数据库	√							
	事件分级	√							
	策略配置	√							
	产品升级				√			√	
	统一升级				√				
	分布式部署	√							
	集中管理	√							
	同台管理	√							
	端口分离	√						√	
	双机热备				√				
	多级管理	√							

表 6（续）

安全功能要求		入侵检测	事件记录	身份认证	安全管理	信息保密	鉴别失败处理	操作系统加固	审计
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		√						
	窗口定义	√							
	事件定义	√							
	协议定义	√							
	通用接口	√							
身份鉴别	管理员鉴别			√					
	鉴别失败的处理						√		
	鉴别数据保护				√				
	超时设置				√				
	多鉴别机制			√					
	会话锁定				√				
管理员管理	标识唯一性			√	√				
	用户属性定义				√				
	安全行为管理				√				
	管理员角色				√				
	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				√				
	数据存储安全				√				
	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				√			√	
	自我监测				√			√	

10.2 安全保证要求基本原理

安全保证要求参照了 GB/T 18336.3—2008 中的相关要求。

11 等级划分要求

11.1 概述

按照网络型入侵检测产品的安全功能要求强度，将网络型入侵检测产品安全功能要求划分成基本级和增强级；安全保证要求基本级参照了 EAL2 级安全保证要求，增强级在 EAL4 级安全保证要求的基础上，将脆弱性分析要求提升到可以抵御中等攻击潜力的攻击者发起的攻击。

11.2 安全功能要求等级划分

网络型入侵检测产品的安全功能要求等级划分如表 7 所示。

表 7 网络型入侵检测产品安全功能要求等级划分表

安全功能要求		基本级	增强级
数据探测功能要求	数据收集	8.1.1	8.1.1
	协议分析	8.1.2	8.1.2
	行为监测	8.1.3	8.1.3
	流量监测	8.1.4	8.1.4
入侵分析功能要求	数据分析	8.2.1	8.2.1
	分析方式	8.2.2	8.2.2
	防躲避能力	—	8.2.3
	事件合并	—	8.2.4
	事件关联	—	8.2.5
入侵响应功能要求	安全告警	8.3.1	8.3.1
	告警方式	8.3.2	8.3.2
	排除响应	—	8.3.3
	定制响应	—	8.3.4
	防火墙联动	—	8.3.5
	全局预警	—	8.3.6
	入侵管理	—	8.3.7
	其他设备联动	—	8.3.8
管理控制功能要求	图形界面	8.4.1	8.4.1
	事件数据库	8.4.2	8.4.2
	事件分级	8.4.3	8.4.3
	策略配置	8.4.4	8.4.4
	产品升级	8.4.5	8.4.5
	统一升级	8.4.6	8.4.6

表 7（续）

安全功能要求		基本级	增强级
管理控制功能要求	分布式部署	—	8.4.7
	集中管理	—	8.4.8
	同台管理	—	8.4.9
	端口分离	—	8.4.10
	双机热备	—	8.4.11
	多级管理	—	8.4.12
检测结果处理要求	事件记录	8.5.1	8.5.1
	事件可视化	8.5.2	8.5.2
	报告生成	8.5.3	8.5.3
	报告查阅	8.5.4	8.5.4
	报告输出	8.5.5	8.5.5
产品灵活性要求	报告定制	8.6.1	8.6.1
	窗口定义	—	8.6.2
	事件定义	—	8.6.3
	协议定义	—	8.6.4
	通用接口	—	8.6.5
身份鉴别	管理员鉴别	8.7.1	8.7.1
	鉴别失败的处理	8.7.2	8.7.2
	鉴别数据保护	8.7.3	8.7.3
	超时设置	—	8.7.4
	多鉴别机制	—	8.7.5
	会话锁定	—	8.7.6
管理员管理	标识唯一性	8.8.1	8.8.1
	用户属性定义	8.8.2	8.8.2
	安全行为管理	8.8.3	8.8.3
	管理员角色	—	8.8.4
	安全属性管理	—	8.8.5
安全审计	审计数据生成	—	8.9.1
	审计数据可用性	—	8.9.2
	审计查阅	—	8.9.3
	受限的审计查阅	—	8.9.4
事件数据安全	安全数据管理	8.10.1	8.10.1
	数据保护	8.10.2	8.10.2
	数据存储安全	—	8.10.3
	数据存储告警	—	8.10.4

表 7（续）

安全功能要求		基本级	增强级
通信安全	通信完整性	8.11.1	8.11.1
	通信稳定性	8.11.2	8.11.2
	升级安全	8.11.3	8.11.3
产品自身安全	自我隐藏	8.12.1	8.12.1
	自我监测	8.12.2	8.12.2

11.3 安全保证要求等级划分

网络型入侵检测产品的安全保证要求等级划分如表 8 所示。

表 8 网络型入侵检测产品安全保证要求等级划分表

安全保证要求			基本级	增强级
配置管理	部分配置管理自动化		—	9.1.1
	配置管理能力	版本号	9.1.2.1	9.1.2.1
		配置项	9.1.2.2	9.1.2.2
		授权控制	—	9.1.2.3
		产生支持和接受程序	—	9.1.2.4
	配置管理范围	配置管理覆盖	—	9.1.3.1
		问题跟踪配置管理覆盖	—	9.1.3.2
交付与运行	交付程序		9.2.1	9.2.1
	修改检测		—	9.2.2
	安装、生成和启动程序		9.2.3	9.2.3
开发	功能规范	非形式化功能规范	9.3.1.1	9.3.1.1
		充分定义的外部接口	—	9.3.1.2
	高层设计	描述性高层设计	9.3.2.1	9.3.2.1
		安全加强的高层设计	—	9.3.2.2
	安全功能实现的子集		—	9.3.3
	描述性低层设计		—	9.3.4
	非形式化对应性证实		9.3.5	9.3.5
	非形式化产品安全策略模型		—	9.3.6
指导性文档	管理员指南		9.4.1	9.4.1
	用户指南		9.4.2	9.4.2
生命周期支持	安全措施标识		—	9.5.1
	开发者定义的生命周期模型		—	9.5.2
	明确定义的开发工具		—	9.5.3

表 8（续）

安全保证要求			基本级	增强级
测试	测试覆盖	覆盖证据	9.6.1.1	9.6.1.1
		覆盖分析	—	9.6.1.2
	测试：高层设计		—	9.6.2
	功能测试		9.6.3	9.6.3
	独立测试	一致性	9.6.4.1	9.6.4.1
		抽样	9.6.4.2	9.6.4.2
脆弱性评定	误用	指南审查	—	9.7.1.1
		分析确认	—	9.7.1.2
	产品安全功能强度评估		9.7.2	9.7.2
	脆弱性分析	开发者脆弱性分析	9.7.3.1	9.7.3.1
		独立的脆弱性分析	—	9.7.3.2
		中级抵抗力	—	9.7.3.3

中华人民共和国公共安全
行业标准
信息安全技术
入侵检测产品安全技术要求
第1部分：网络型产品
GA/T 403.1—2014

*

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.spc.net.cn
总编室：(010)64275323　发行中心：(010)51780235
读者服务部：(010)68523946

中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销

*

开本 880×1230　1/16　印张 1.75　字数 44 千字
2014年5月第一版　2014年5月第一次印刷

*

书号：155066·2-27089　定价　27.00 元

GA/T 403.1-2014