

中华人民共和国公共安全行业标准

GA/T ××××.2—2002

---

信息技术--入侵检测产品技术要求  
第2部分：主机型产品

Information technology---Technical requirements for intrusion detection products  
Part 2 : Host-based products

(报批稿)

××××-××-××发布

××××-××-××实施

---

中华人民共和国公安部 发布



## 目 次

前 言 .....	II
引 言 .....	III
1 范围 .....	1
2 规范性引用文件 .....	1
3 术语和定义 .....	1
4 主机型入侵检测产品的组成和分级 .....	1
4.1 产品组成 .....	1
4.2 产品分级 .....	1
5 工作环境 .....	2
5.1 系统接入 .....	2
5.2 工作环境安全 .....	2
5.3 管理人员 .....	2
6 功能要求 .....	2
6.1 基本级主机型入侵检测产品组件功能要求 .....	2
6.2 增强级主机型入侵检测产品扩展功能要求 .....	4
7 性能要求 .....	5
7.1 误报率 .....	6
7.2 漏报率 .....	6
7.3 平均响应时间 .....	6
7.4 稳定性 .....	6
7.5 CPU 资源占用量 .....	6
7.6 存储空间资源占用量 .....	6
7.7 内存占用量 .....	6
7.8 用户登录和资源访问 .....	6
7.9 网络通信 .....	6
8 安全功能要求 .....	6
8.1 安全功能组件 .....	6
8.2 安全审计 .....	7
8.3 标识和鉴别 .....	7
8.4 安全管理 .....	7
8.5 安全功能保护 .....	7
9 安全保证要求 .....	8
9.1 配置管理保证 .....	8
9.2 操作保证 .....	8
9.3 开发过程保证 .....	8
9.4 指南文件保证 .....	8

## 前 言

GAT××××《信息技术 入侵检测产品技术要求》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 xxxx的第二部分。

本部分由公安部公共信息网络安全监察局提出。

本部分由公安部信息系统安全标准化技术委员会归口。

本部分由北京中科网威信息技术有限公司、公安部第三研究所负责起草。

本部分主要起草人：曾明、潘玉珣、杨威、余立新、肖江、刘兵、丁宇征。

## 引 言

本部分是 GAT××××的第 2 部分。本部分规定了主机型入侵检测产品的技术要求。

入侵检测产品的目的是发现入侵行为。它通过对计算机网络中的若干关键点或被监测主机系统收集安全相关信息并对其进行分析,从而发现网络和系统中违反安全策略的行为和被攻击的迹象。当把入侵检测产品看成是完成一定安全目标的系统时,我们又可称之为入侵检测系统(IDS)。与其它安全产品相比,入侵检测产品具有更强的智能分析功能。入侵检测产品能简化管理员的工作,保障网络的安全运行。



# 信息技术---入侵检测产品技术要求

## 第2部分：主机型产品

### 1 范围

GA/T××××的本部分规定了采用传输控制协议/网间协议(TCP/IP)的主机型入侵检测产品的工作环境、功能要求、性能要求、安全功能要求和安全保证要求。

本部分适用于主机型入侵检测产品的研制、开发、测评和采购。

### 2 规范性引用文件

下列文件中的条款通过本部分的引用而成为本部分的条款。凡是注日期的引用文件,其随后所有的修改单(不包括勘误的内容)或修订版均不适用于本部分。然而,鼓励根据本部分达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件,其最新版本适用于本部分。

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

GB/T xxxx.1-2002 信息技术 入侵检测产品技术要求 第1部分:网络型产品

### 3 术语和定义

GB/T 5271.8-2001和 GA/T xxxx.1-2002确立的术语和定义适用于GA/T xxxx的本部分。

### 4 主机型入侵检测产品的组成和分级

#### 4.1 产品组成

##### 4.1.1 事件产生单元 (IDS\_GEN)

获取主机数据信息,使入侵检测产品能捕获策略定制的主机状态信息。该单元通过在主机系统上的代理实现基本功能。

##### 4.1.2 事件分析单元 (IDS\_ANL)

采用分析检测技术,通过收集主机的运行状态与已指定的基本状态进行比较,从而检测可能存在的攻击。

##### 4.1.3 响应单元 (IDS\_RSP)

响应单元对检测到的事件作出反应,通常有报警、记录和主动保护三种反应手段。通过在主机系统上的代理实现其基本功能。

##### 4.1.4 审计单元 (IDS\_FAU)

审计单元在违反安全策略的事件发生时,对事件发生的时间、主体和客体信息等进行审计和记录。

##### 4.1.5 管理控制单元 (IDS\_MAN)

管理控制单元负责策略定制、日志审阅和系统状态管理,并以可视化形式提交给授权用户进行管理。

#### 4.2 产品分级

对主机型入侵检测产品分成两个级别,即基本级和增强级。

##### a) 基本级

具备基本的入侵检测功能,对所保护对象具有可靠的保护功能。

##### b) 增强级

除具备基本级的产品各项要求外,在功能要求和性能要求上,有扩展的或更高的要求。

## 5 工作环境

### 5.1 系统接入

5.1.1 主机型入侵检测产品的代理端应被正确安装在受保护主机上，代理端和管理端处于连通状态。

5.1.2 应具备严格的访问控制机制，非授权人员不能管理入侵检测产品。

### 5.2 工作环境安全

5.2.1 应防止对入侵检测产品非授权的物理访问。

5.2.2 入侵检测产品的安装应由授权管理人员实施。

5.2.3 入侵检测产品的安装应实行严格的控制管理。

### 5.3 管理人员

5.3.1 指定一个或多个能胜任工作的人员来管理入侵检测产品及其所含信息的安全。

5.3.2 入侵检测产品只能被授权用户访问。

## 6 功能要求

### 6.1 基本级主机型入侵检测产品组件功能要求

#### 6.1.1 基本级主机型入侵检测产品功能组件

主机型入侵检测产品功能组件要求分为事件产生单元组件要求、事件分析单元组件要求、响应单元组件要求、审计单元组件要求和管理控制单元组件要求共 5 类。各类功能组件如表 1 所示。

表 1 基本级主机型入侵检测产品功能组件

功能组件	组件要求
IDS_GEN.1	数据采集
IDS_GEN.2	数据采集的实时性
IDS_ANL.1	统计分析
IDS_ANL.2	异常分析
IDS_ANL.3	主机系统日志分析
IDS_ANL.4	文件完整性分析
IDS_ANL.5	分析记录
IDS_RSP.1	报警
IDS_RSP.2	报警记录
IDS_FAU.1	审计记录
IDS_FAU.2	审计纪录的创建、储存和删除
IDS_FAU.3	审计记录查询
IDS_FAU.4	审计记录保存

表1 基本级主机型入侵检测产品功能组件（续）

功能组件	组件要求
IDS_FAU.5	数据库支持
IDS_MAN.1	管理功能
IDS_MAN.2	远程管理
IDS_MAN.3	身份鉴别和认证
IDS_MAN.4	易用性

## 6.1.2 事件产生单元组件要求 (IDS\_GEN)

### 6.1.2.1 IDS\_GEN.1 获取策略定制的目标主机的各种状态信息。

事件产生单元应至少从目标主机收集以下信息：

- a) 目标系统的启动和关闭；
- b) 主机的资源使用情况；
- c) 系统的日志，审计的变化情况；
- d) 标识和鉴别事件；
- e) 服务请求；
- f) 网络通信流量；
- g) 安全配置的改变；
- h) 策略定制的事件。

### 6.1.2.2 IDS\_GEN.2 数据采集应具有实时性。

## 6.1.3 事件分析单元组件要求 (IDS\_ANL)

### 6.1.3.1 IDS\_ANL.1 入侵检测产品应能进行统计分析，将事件关联起来分析，发现违反安全策略的行为。

6.1.3.2 IDS\_ANL.2 入侵检测产品应能进行异常分析，将获取的当前主机状态信息与已建立的基准状态信息比较，发现可能存在的入侵行为。基准状态信息应至少包含主机正常工作状态的以下信息：

- a) 用户活动；
- b) 系统资源使用；
- c) 文件及对象的安全事件；
- d) 网络应用服务；
- e) 通信连接；
- f) 系统日志。

### 6.1.3.3 IDS\_ANL.3 入侵检测产品应分析主机系统日志记录，发现违反安全策略的事件。

### 6.1.3.4 IDS\_ANL.4 入侵检测产品应进行文件完整性分析，能检测到任何企图破坏文件完整性的行为。

### 6.1.3.5 IDS\_ANL.5 在每个分析结论中应至少记录以下信息：结果的日期和时间，结果类型，数据源鉴定。

## 6.1.4 响应单元组件要求 (IDS\_RSP)

6.1.4.1 IDS\_RSP.1 当策略中被定义为报警的攻击事件发生时，系统应以消息或邮件等形式向管理人员发送报警信息。报警信息至少应包含以下内容：

- a) 事件标识；
- b) 事件主体；
- c) 事件客体；
- d) 事件发生时间；
- e) 事件类型；
- f) 事件危险级别。

6.1.4.2 IDS\_RSP.2 当策略中定义为记录的事件发生时，响应单元应将事件信息以文件或数据库记录等形式记录下来。记录信息至少应包含 IDS\_RSP.1 中所含内容。

## 6.1.5 审计单元组件要求 (IDS\_FAU)

### 6.1.5.1 IDS\_FAU.1 审计功能应为以下可审计事件产生审计记录：

- a) 审计功能的开启和关闭；
- b) 符合基本级审计的所有下列可审计事件：
  - 任何对审计进行的操作；
  - 所有对安全策略更改的操作；

- 修改安全属性的所有尝试；
- 任何对鉴别机制的使用；
- 所有对鉴别资料的请求访问；
- 所有对审计数据读取不成功尝试；
- 鉴别机制的使用；
- 用户鉴别机制的使用；
- 对角色中用户组的修改。

c) 在系统安全策略中定义的其它需要审计的事件。

审计功能生成的每一条审计记录至少应记录以下信息：事件时间，事件类型，主体身份和事件结果（成功或失败）。

6.1.5.2 IDS\_FAU.2 管理员应可创建、储存、删除和清空审计纪录。

6.1.5.3 IDS\_FAU.3 提供授权管理人员对日志信息的查询、审阅功能。提供的信息应至少包括以下内容：

- a) 事件标识；
- b) 事件主体；
- c) 事件客体；
- d) 事件发生时间。

6.1.5.4 IDS\_FAU.4 审计记录的保存应满足以下要求：

- a) 将审计记录存储到永久性的存储媒体中；
- b) 自动统计审计记录的存储空间，发现存储空间快耗尽时提前通知管理人员；
- c) 审计单元向管理员提供可定制的资料备份功能及策略。

6.1.5.5 IDS\_FAU.5 入侵检测产品至少应支持一种流行的数据库。

6.1.6 管理控制单元组件要求（IDS\_MAN）

6.1.6.1 IDS\_MAN.1 入侵检测产品应包含配置和管理入侵检测产品安全功能所需的所有功能，至少包括：

- a) 系统状态定制；
- b) 增加，删除和定制入侵检测策略；
- c) 查阅当前策略配置；
- d) 查阅和管理审计资料。

6.1.6.2 IDS\_MAN.2 入侵检测产品应提供远程管理功能。

6.1.6.3 IDS\_MAN.3 管理控制单元应提供鉴别认证机制，在用户登录管理控制台之前对用户进行鉴别认证。当管理控制单元与引擎是通过网络连接时，管理控制单元与引擎间建立通信会话之前应进行鉴别认证。

6.1.6.4 IDS\_MAN.4 入侵检测产品提供给授权用户的管理功能应简单易用。

6.2 增强级主机型入侵检测产品扩展功能要求

6.2.1 增强级主机型入侵检测产品扩展组件

增强级主机型入侵检测产品扩展组件由表2所列项目组成，增强级主机型入侵检测产品除了应满足基本级主机型入侵检测产品组件要求外，还应满足表2所列的扩展组件要求。

表 2 增强级主机型入侵检测产品功能组件

扩展功能组件	扩展功能组件要求
IDS_ANL_IMP.1	分析单元身份鉴别
IDS_ANL_IMP.2	概率统计分析
IDS_ANL_IMP.3	数据挖掘
IDS_RSP_IMP.1	主动保护能力

扩展功能组件	扩展功能组件要求
IDS_RSP_IMP.2	与其它网络安全产品的互动
IDS_FAU_IMP.1	可选审计查阅
IDS_FAU_IMP.2	选择性审计
IDS_FAU_IMP.3	分级审计查阅
IDS_FAU_IMP.4	审计信息加密存储
IDS_MAN_IMP.1	策略管理工具
IDS_MAN_IMP.2	组件间通信加密
IDS_MAN_IMP.3	管理角色分级
IDS_MAN_IMP.4	鉴别尝试限制

## 6.2.2 事件分析单元扩展功能要求 (IDS\_ANL\_IMP)

6.2.2.1 IDS\_ANL\_IMP.1 分析单元应具备身份鉴别能力,除具有明确访问权限的用户外,分析单元应禁止其它用户对分析单元的访问。

6.2.2.2 IDS\_ANL\_IMP.2 入侵检测产品应具备概率统计的分析能力,对不规则或频繁出现的事件进行统计分析。

6.2.2.3 IDS\_ANL\_IMP.3 入侵检测产品应具备数据挖掘能力,能对存在关联的事件进行分析,发现可能存在的入侵。

## 6.2.3 响应单元扩展功能要求 (IDS\_RSP\_IMP)

6.2.3.1 IDS\_RSP\_IMP.1 入侵检测产品应具备主动保护能力,当违反安全策略的事件发生时,响应单元能够提供主动保护功能,防范进一步的入侵行为,可采取的保护动作如下:

- a) 锁定用户的登录;
- b) 阻断用户的通信;
- c) 调用授权用户预先定义的操作。

6.2.3.2 IDS\_RSP\_IMP.2 入侵检测产品应能与其它网络安全产品配合工作,对发现的入侵行为采取联合行动,保证系统的安全。

## 6.2.4 审计单元扩展功能要求 (IDS\_FAU\_IMP)

6.2.4.1 IDS\_FAU\_IMP.1 审计单元应具有通过日期和时间、主体身份、事件类型、相关事件成功或失败等信息对审计数据进行分类的能力。

6.2.4.2 IDS\_FAU\_IMP.2 审计单元应根据以下属性的审计事件集合中包含或排斥可审计事件:

- a) 事件类型;
- b) 审计列表中任意可选项。

6.2.4.3 IDS\_FAU\_IMP.3 除具有明确访问权限的用户外,审计单元应禁止其他用户对审计数据的访问。

6.2.4.4 IDS\_FAU\_IMP.4 审计信息应能加密存储。

## 6.2.5 管理控制单元扩展功能要求 (IDS\_MAN\_IMP)

6.2.5.1 IDS\_MAN\_IMP.1 入侵检测产品应为用户提供定制安全策略和验证安全策略的工具。

6.2.5.2 IDS\_MAN\_IMP.2 当管理控制单元与其它单元是通过网络连接时,管理控制单元与其它组件间的通信应建立安全加密连接。

6.2.5.3 IDS\_MAN\_IMP.3 入侵检测产品应按照管理权限的不同将管理员分级。

6.2.5.4 IDS\_MAN\_IMP.4 管理单元应设定一个用户授权管理员用户可修改的鉴别尝试次数,当达到或超过规定的不成功鉴别尝试次数时,管理控制单元应阻止用户的进一步鉴别尝试,直到授权管理员恢复该用户的被鉴别能力。

## 7 性能要求

### 7.1 误报率

主机型入侵检测产品的技术文档应标明该产品的误报率，并指明相应的测试方法、测试工具、测试环境和测试步骤。

### 7.2 漏报率

主机型入侵检测产品的技术文档应标明该产品的漏报率，并指明相应的测试方法、测试工具、测试环境和测试步骤。

### 7.3 平均响应时间

入侵检测产品应保证对事件及时进行响应。

### 7.4 稳定性

基于主机的入侵检测产品在主机任何工作状态下都应该工作稳定，工作时不应对其它系统的工作产生影响，且易于安装和干净卸载。不应造成被检测主机停机或死机现象。

### 7.5 CPU 资源占用量

在主机负载高峰情况下，入侵检测产品不应明显影响主机正常处理工作速度。

### 7.6 存储空间资源占用量

入侵检测产品占用存储空间不应影响主机正常存储能力。

### 7.7 内存占用量

入侵检测产品占用内存空间不应影响主机正常工作能力。

### 7.8 用户登录和资源访问

入侵检测产品不应影响所在目标主机上的合法用户登录及文件资源访问。

### 7.9 网络通信

入侵检测产品不应影响所在目标主机的合法网络通信。

## 8 安全功能要求

### 8.1 安全功能组件

主机型入侵检测产品的安全功能组件由表3所列项目组成。

表 3 主机型入侵检测产品安全功能组件

安全功能组件	安全功能要求
IDS_FAU_SAR.1	审计查阅
IDS_FAU_SAR.2	有限审计查阅
IDS_FAU_STG.1	审计数据可用性保证
IDS_FAU_STG.2	审计数据丢失防范
IDS_FIA_UAU.1	鉴别时效
IDS_FIA_AFL.1	鉴别失败处理

IDS_FIA_ATD.1	用户属性定义
IDS_FMT_MOF.1	安全功能管理
IDS_FMT_SMR.1	安全角色
IDS_FPT_ITC.1	数据传输加密
IDS_FPT_RVM.1	安全策略不可旁路性

## 8.2 安全审计

### 8.2.1 IDS\_FAU\_SAR.1 审计查阅

入侵检测产品应提供授权用户访问审计数据的能力。

### 8.2.2 IDS\_FAU\_SAR.2 有限审计查阅

入侵检测产品应明确用户对审计数据的访问权限，为不同权限的用户提供相应的访问权限。

### 8.2.3 IDS\_FAU\_STG.1 审计数据可用性保证

#### 8.2.3.1 IDS\_FAU\_STG.1.1 入侵检测产品应保护存储的审计数据，避免未授权的删除。

#### 8.2.3.2 IDS\_FAU\_STG.1.2 入侵检测产品应能检测到对审计数据的修改。

#### 8.2.3.3 IDS\_FAU\_STG.1.3 在审计存储资源耗尽、失败或受到攻击时，入侵检测产品应确保审计数据不被破坏。

### 8.2.4 IDS\_FAU\_STG.2 审计数据丢失防范

当审计数据存储空间接近或到达规定值时，入侵检测产品应向授权管理员发送报警信息。

## 8.3 标识和鉴别

### 8.3.1 IDS\_FIA\_UAU.1 鉴别时效

#### 8.3.1.1 IDS\_FIA\_UAU.1.1 入侵检测产品在用户被鉴别前应允许用户执行与入侵检测产品安全无关的操作。

#### 8.3.1.2 IDS\_FIA\_UAU.1.2 入侵检测产品应确保用户在执行与入侵检测产品安全相关的任何操作之前，该用户已被成功的鉴别。

### 8.3.2 IDS\_FIA\_AFL.1 鉴别失败处理

#### 8.3.2.1 IDS\_FIA\_AFL.1.1 当用户的失败登录次数超过允许的尝试鉴别次数时，入侵检测产品应能加以检测。

#### 8.3.2.2 IDS\_FIA\_AFL.1.2 当用户的失败登录次数超过允许的尝试鉴别次数时，入侵检测产品应阻止该用户的进一步登录尝试，直至授权管理员恢复对该用户的鉴别能力。

### 8.3.3 IDS\_FIA\_ATD.1 用户属性定义

入侵检测产品应对管理角色赋予执行安全策略所必需的安全属性，安全属性包括：

- a) 唯一用户身份；
- b) 鉴别数据；
- c) 授权；
- d) 其它安全属性。

## 8.4 安全管理

### 8.4.1 IDS\_FMT\_MOF.1 安全功能管理

入侵检测产品应确保只有授权管理员拥有对安全功能进行修改和配置的权利。

### 8.4.2 IDS\_FMT\_SMR.1 安全角色

入侵检测产品的安全角色可以管理操作系统，但该角色并不拥有更改入侵检测产品配置选项的权限，应将入侵检测产品的安全角色和操作系统的用户区分开。

## 8.5 安全功能保护

### 8.5.1 IDS\_FPT\_ITC.1 数据传输加密

入侵检测产品应能对各组件间的通信数据进行加密。

### 8.5.2 IDS\_FPT\_RVM.1 IDS 安全策略不可旁路性

入侵检测产品应确保用户对系统安全功能的访问都受到安全策略的制约。

## 9 安全保证要求

### 9.1 配置管理保证

9.1.1 开发者应使用配置管理系统。

9.1.2 开发者应提供配置管理手册。

9.1.3 配置手册应包括一个配置目录。

9.1.4 配置目录应包含入侵检测产品的各个配置项目的描述。

9.1.5 厂商所提供的信息应满足在内容和表达上的所有要求。

### 9.2 操作保证

9.2.1 开发者应以文件方式说明入侵检测产品的安装、配置和启动的过程。

9.2.2 用户手册中应详尽描述入侵检测产品的安装、配置和启动运行所必需的基本步骤。

9.2.3 厂商所提供的信息应满足内容和表述上的所有要求。

### 9.3 开发过程保证

#### 9.3.1 入侵检测产品和安全策略

9.3.1.1 开发者应提供入侵检测产品的功能规范。

9.3.1.2 开发者应提供入侵检测产品的安全策略。

9.3.1.3 功能规范应以非形式方法来描述安全策略。

9.3.1.4 功能规范应以非形式方法来表述所有外部安全功能接口的语法和定义。

9.3.1.5 厂商所提供的信息应满足内容和表述上的所有要求。

9.3.1.6 产品的功能规范与安全策略应保证一致。

9.3.1.7 产品安全功能的表述应包含安全目标中的每一项功能要求。

#### 9.3.2 高层设计描述

9.3.2.1 开发者应提供入侵检测产品安全功能的高层设计。

9.3.2.2 高层设计应以非形式方法表述。

9.3.2.3 高层设计应描述功能的每一个系统提供的安全功能。

9.3.2.4 高层设计应标明功能子系统的接口。

9.3.2.5 高层设计应说明安全功能所需的所有底层硬件、固件和软件，以及所实现的保护机制所提供的功能。

9.3.2.6 厂商所提供的信息应满足内容和表述上的所有要求。

9.3.2.7 功能的表述应包含安全目标中的每一项功能要求。

#### 9.3.3 非形式的一致性要求

9.3.3.1 开发者应证明所提供的对功能的扼要表述是准确和一致的，并且完整地反应了安全目标中的功能要求。

9.3.3.2 对于同一功能的两个相邻层的表述，开发者应证明在较高层抽象表述的所有部分在较底层抽象中得到了细化。

9.3.3.3 对于同一功能的两个相邻层的表述，其对应关系可以用非形式方法表述。

9.3.3.4 厂商所提供的信息应满足内容和表述上的所有要求。

### 9.4 指南文件保证

#### 9.4.1 管理员指南

9.4.1.1 开发者应提供满足系统管理者需要的管理员指南。

9.4.1.2 管理员指南应描述如何以安全的方式管理入侵检测产品。

9.4.1.3 对于应该控制在安全处理环境中的功能和特权，管理员指南应有警告。

- 9.4.1.4 管理员指南应对如何有效地使用安全功能提供指导。
- 9.4.1.5 管理员指南应说明两种类型功能之间的差别：一种是允许管理员配置安全参数，而另一种是只允许管理员获得信息。
- 9.4.1.6 管理员指南应描述管理员控制下的所有参数。
- 9.4.1.7 管理员指南应描述各类需要执行安全功能的安全相关事件，包括在安全功能控制下改变实体的安全特性。
- 9.4.1.8 管理员指南应包括安全功能如何相互作用的指导。
- 9.4.1.9 管理员指南应包括怎样安全配置入侵检测产品的指令。
- 9.4.1.10 管理员指南应描述在入侵检测产品的安全安装过程中可能使用的所有配置选项。
- 9.4.1.11 管理员指南应充分描述与安全管理相关的详细过程。
- 9.4.2 用户指南
  - 9.4.2.1 开发者应提供用户指南。
  - 9.4.2.2 用户指南应描述用户可使用的安全功能和接口。
  - 9.4.2.3 用户指南应包含使用入侵检测提供的安全功能和指导。
  - 9.4.2.4 对于应该控制在安全的处理环境中的功能和特权，用户指南应有警告。
  - 9.4.2.5 用户指南应描述那些用户可见的安全功能之间的相互作用。
  - 9.4.2.6 用户指南应与提交评估的所有其它文件一致。
  - 9.4.2.7 所提供的信息应能满足在内容和描述上的所有要求。
- 9.4.3 测试保证
  - 9.4.3.1 独立测试
    - 9.4.3.1.1 应由评估者或具有专业知识的团体支持的独立实验室进行入侵检测产品的测试。
    - 9.4.3.1.2 应对入侵检测产品进行相符性独立测试，证明安全功能是按照规定运行的。
    - 9.4.3.1.3 应对入侵检测产品进行抽样独立测试，通过随机抽样对抽样产品进行测试，证明安全功能是按照规定运行的。
    - 9.4.3.1.4 应对入侵检测产品进行完全独立性测试，通过重复所有开发者的测试，证明安全功能是按照规定运行的。
  - 9.4.3.2 测试覆盖面非形式分析
    - 9.4.3.2.1 开发者应提供一个对测试覆盖范围的分析。
    - 9.4.3.2.2 测试覆盖面分析应证明测试文件中确定的测试项目能覆盖入侵检测所有的安全功能。
    - 9.4.3.2.3 所提供的信息应能满足在内容和表述上的所有要求。
  - 9.4.3.3 功能测试
    - 9.4.3.3.1 开发者应测试入侵检测产品的功能，并记录结果。
    - 9.4.3.3.2 开发者应提供测试文件。
    - 9.4.3.3.3 测试文件应有测试计划、测试过程描述和测试结果组成。
    - 9.4.3.3.4 测试文件应确定将要测试的产品功能，并描述将要达到的测试目标。
    - 9.4.3.3.5 测试过程的描述应确定将要进行的测试，并描述测试每一安全功能的实际情况。
    - 9.4.3.3.6 测试文件的测试结果应给出每一项测试的预期结果。
    - 9.4.3.3.7 开发者得到的测试结果应能证明每一项安全功能和设计目标相符。
    - 9.4.3.3.8 提供的信息应满足在内容和表述上的所有要求。
  - 9.4.3.4 测试—功能规范
    - 9.4.3.4.1 开发者应提供对测试深度的分析。
    - 9.4.3.4.2 深度分析应证明测试文件中确定的测试充分表明了入侵检测产品的运行符合安全功能规范。
    - 9.4.3.4.3 提供的信息应满足在内容和表述上的所有要求。

#### 9.4.4 脆弱性分析保证

##### 9.4.4.1 入侵检测安全功能强度的评估

9.4.4.1.1 开发者应确定入侵检测适合作安全功能强度分析的安全机制。

9.4.4.1.2 开发者应对确定的每一机制进行安全功能强度分析。加密和鉴别机制应符合有关规定和国家标准。

9.4.4.1.3 对于安全功能对抗威胁的能力，入侵检测安全功能强度分析应能判定所标明的安全机制对其产生的影响。

9.4.4.1.4 入侵检测安全功能强度分析应证明所标明的安全功能强度与安全目标是一致的。

9.4.4.1.5 所提供的信息应满足在内容和表述上的所有要求。

9.4.4.1.6 所有需要强度分析的安全机制应已确定。

9.4.4.1.7 各项强度声明应已确认。

##### 9.4.4.2 开发者脆弱性分析

9.4.4.2.1 开发者应从用户可能破坏安全策略的明显途径方面，对入侵检测的各种功能进行分析并提供文件。

9.4.4.2.2 开发者应明确记录对被确定的脆弱性的处置。

9.4.4.2.3 对每一条脆弱性应有证据显示该脆弱性在使用入侵检测产品的环境中不能被利用。

9.4.4.2.4 所提供的信息应符合证据在内容和表述上的所有要求。

9.4.4.2.5 应在开发者脆弱性分析的基础上进行渗透测试，以确保明显的薄弱点已得到加强。

---