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 …… Ⅲ
引言 …… Ⅳ
1　范围 …… 1
2　规范性引用文件 …… 1
3　术语和定义 …… 1
4　缩略语 …… 2
5　网络型入侵检测产品描述 …… 2
6　安全环境 …… 3
6.1　假设 …… 3
6.2　威胁 …… 3
6.3　组织安全策略 …… 4
7　安全目的 …… 4
7.1　产品安全目的 …… 4
7.2　环境安全目的 …… 5
8　安全功能要求 …… 5
8.1　数据探测功能要求 …… 5
8.2　入侵分析功能要求 …… 5
8.3　入侵响应功能要求 …… 6
8.4　管理控制功能要求 …… 6
8.5　检测结果处理要求 …… 7
8.6　产品灵活性要求 …… 8
8.7　身份鉴别 …… 8
8.8　管理员管理 …… 9
8.9　安全审计 …… 9
8.10　事件数据安全 …… 10
8.11　通信安全 …… 10
8.12　产品自身安全 …… 10
9　安全保证要求 …… 10
9.1　配置管理 …… 10
9.2　交付与运行 …… 11
9.3　开发 …… 12
9.4　指导性文档 …… 13
9.5　生命周期支持 …… 14
9.6　测试 …… 14
9.7　脆弱性评定 …… 15
10　技术要求基本原理 …… 16

10.1 安全功能要求基本原理 …… 16
10.2 安全保证要求基本原理 …… 18
11 等级划分要求 …… 18
11.1 概述 …… 18
11.2 安全功能要求等级划分 …… 18
11.3 安全保证要求等级划分 …… 20

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。