



中华人民共和国公共安全行业标准

GA/T 1728—2020

信息安全技术 基于 IPv6 的高性能网络 入侵检测系统产品安全技术要求

Information security technology—Security technical requirements for IPv6-based
high-performance network intrusion detection system products

2020-05-13 发布

2020-08-01 实施

中华人民共和国公安部 发布

目 次

- 前言 III
- 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 基于 IPv6 的高性能网络入侵检测系统产品描述 2
- 6 总体说明 3
 - 6.1 安全技术要求分类 3
 - 6.2 安全等级 3
- 7 安全功能要求 3
 - 7.1 数据探测功能要求 3
 - 7.2 入侵分析功能要求 4
 - 7.3 入侵响应功能要求 4
 - 7.4 管理控制功能要求 5
 - 7.5 检测结果处理要求 6
 - 7.6 产品灵活性要求 6
 - 7.7 身份鉴别 7
 - 7.8 管理员管理 7
 - 7.9 安全审计 8
 - 7.10 事件数据安全 8
 - 7.11 通信安全 8
 - 7.12 产品自身安全 8
- 8 网络环境适应性要求 9
 - 8.1 支持纯 IPv6 网络环境 9
 - 8.2 IPv6 网络环境下自身管理 9
 - 8.3 支持 IPv6 过渡网络环境(可选) 9
- 9 性能要求 9
 - 9.1 误报率 9
 - 9.2 漏报率 9
 - 9.3 监控流量 9
 - 9.4 监控并发连接数 10
 - 9.5 监控新建 TCP 连接速率 10
 - 9.6 还原能力 10
- 10 安全保障要求 10
 - 10.1 开发 10
 - 10.2 指导性文档 11

10.3	生命周期支持	11
10.4	测试	12
10.5	脆弱性评定	13
11	不同安全等级的要求	13
11.1	安全功能要求	13
11.2	安全保障要求	15

前 言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准由公安部网络安全保卫局提出。

本标准由公安部信息系统安全标准化技术委员会归口。

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、公安部第三研究所、网神信息技术(北京)股份有限公司。

本标准主要起草人：宋好好、顾建新、武腾、邹春明、陆臻、沈亮、顾健、李博、杨柳。

信息安全技术 基于 IPv6 的高性能网络 入侵检测系统产品安全技术要求

1 范围

本标准规定了基于 IPv6 的高性能网络入侵检测系统产品的安全功能要求、环境适应性要求、性能要求、安全保障要求及安全等级划分。

本标准适用于基于 IPv6 的高性能网络入侵检测系统产品的设计、开发与测试。

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 18336.3—2015 信息技术 安全技术 信息技术安全评估准则 第3部分:安全保障组件
GB/T 25069—2010 信息安全技术 术语

3 术语和定义

GB/T 18336.3—2015 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

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

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。