



中华人民共和国公共安全行业标准

GA/T 1542—2019

信息安全技术 基于 IPv6 的高性能网络 入侵防御系统产品安全技术要求

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

2019-01-09 发布

2019-01-09 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 的高性能网络入侵防御系统产品描述	2
6 总体说明	3
6.1 安全技术要求分类	3
6.2 安全等级划分	3
7 安全功能要求	3
7.1 入侵事件分析功能要求	3
7.2 入侵事件响应功能要求	3
7.3 入侵事件审计功能要求	4
7.4 管理控制功能要求	4
8 自身安全功能要求	5
8.1 标识与鉴别	5
8.2 安全管理	6
8.3 审计日志	6
9 环境适应性要求	7
9.1 支持纯 IPv6 网络环境	7
9.2 IPv6 网络环境下自身管理	7
9.3 支持 IPv6 过渡网络环境(可选)	7
10 性能要求	7
10.1 吞吐率	7
10.2 延迟	8
10.3 最大并发连接数	8
10.4 最大连接速率	8
10.5 误截和漏截	8
11 安全保障要求	8
11.1 开发	8
11.2 指导性文档	9
11.3 生命周期支持	10
11.4 测试	11

11.5	脆弱性评定	11
12	不同安全等级要求	11
12.1	安全功能要求	11
12.2	自身安全功能要求	12
12.3	安全保障要求	13

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。

本标准主要起草人：顾建新、邵东、付文彬、顾健、张笑笑、顾玮。

信息安全技术 基于 IPv6 的高性能网络 入侵防御系统产品安全技术要求

1 范围

本标准规定了基于 IPv6 的高性能网络型入侵防御系统产品的安全功能要求、自身安全功能要求、环境适应性要求、性能要求、安全保障要求以及等级划分。

本标准适用于基于 IPv6 的高性能网络型入侵防御系统产品的设计、开发及测试。

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

GB/T 28451—2012 信息安全技术 网络型入侵防御产品技术要求和测试评价方法

3 术语和定义

GB/T 18336.3—2015、GB/T 25069—2010 和 GB/T 28451—2012 界定的以及下列术语和定义适用于本文件。

3.1

基于 IPv6 的高性能网络型入侵防御系统产品 **IPv6-based high performance network intrusion prevention system product**

以透明网桥或网关形式部署在网络通路上,通过分析网络流量发现具有入侵特征的网络行为,在其传入被保护网络前进行拦截的产品,能够适用于 IPv4、IPv6 等不同的高性能网络应用场景。

3.2

安全事件 **security 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

告警 **alert**

当发现攻击或入侵事件时,高性能入侵防御系统向授权管理员发出的紧急通知。

3.5

误截 **false positive**

在未出现攻击事件时,入侵防御系统产品对正常网络流量进行拦截的行为。