ICS 33.040.40
CCS M 32

中华人民共和国国家标准

GB/T 44810.3—2024

IPv6网络安全设备技术要求 第3部分:入侵防御系统(IPS)

Technical requirement for IPv6 network security equipment—Part 3:Instrusion prevention system(IPS)

2024-10-26 发布　　2025-02-01 实施

国家市场监督管理总局
国家标准化管理委员会　发布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

本文件是GB/T 44810《IPv6网络安全设备技术要求》的第3部分。GB/T 44810已经发布了以下部分：

——第1部分：防火墙；

——第2部分：Web应用防护系统（WAF）；

——第3部分：入侵防御系统（IPS）。

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专利的责任。

本文件由中华人民共和国工业和信息化部提出。

本文件由全国通信标准化技术委员会（SAC/TC 485）归口。

本文件起草单位：中国信息通信研究院、华为技术有限公司、北京神州绿盟科技有限公司、北京天融信网络安全技术有限公司、郑州信大捷安信息技术股份有限公司、北京浩瀚深度信息技术股份有限公司、国家计算机网络应急技术处理协调中心、中国电信集团有限公司、天翼安全科技有限公司、杭州迪普科技股份有限公司、北京通和实益电信科学技术研究所有限公司、国家工业信息安全发展研究中心、中国福利会国际和平妇幼保健院、北京元支点信息安全技术有限公司、新华三技术有限公司、深圳大学、北京可信华泰信息技术有限公司、杭州安恒信息技术股份有限公司。

本文件主要起草人：董悦、戴方芳、王雨晨、李翔、陈宏伟、赵粤征、毕程、王龑、刘为华、庞韶敏、陈陆颖、石桂欣、严寒冰、康和、龚超、吴庆、左虹、路云鹏、王欣萍、程曦、余果、陈昌杰、季新华、杨志卫、史晨伟、万晓兰、杜君、段古纳、田丽丹。

引　言

根据《关于加快推进互联网协议第六版（IPv6）规模部署和应用工作的通知》，为更好面对网络复杂化和用户规模扩大化带来的安全挑战，推动IPv6网络安全工作的标准化，我国制定了一系列IPv6安全标准。其中，GB/T 44810《IPv6网络安全设备技术要求》是为规范在IPv6中网络安全产品的适用性的技术标准，拟由三个部分构成。

——第1部分：防火墙。目的在于IPv6部署后，保障防火墙在新的网络环境中的有效应用。

——第2部分：Web应用防护系统（WAF）。目的在于IPv6部署后，保障Web应用防护系统（WAF）在新的网络环境中的有效应用。

——第3部分：入侵防御系统（IPS）。目的在于IPv6部署后，保障入侵防御系统（IPS）在新的网络环境中的有效应用。

IPv6 网络安全设备技术要求
第 3 部分:入侵防御系统(IPS)

1 范围

本文件规定了支持 IPv6 的入侵防御系统的安全技术要求。

本文件适用于支持 IPv6 的入侵防御系统的设计、开发、部署、使用、维护与测试。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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 25069—2022 信息安全技术 术语

GB/T 28451—2023 信息安全技术 网络入侵防御产品技术规范

GB/T 44810.1—2024 IPv6 网络安全设备技术要求 第 1 部分：防火墙

3 术语和定义

GB/T 25069—2022、GB/T 28451—2023 界定的以及下列术语和定义适用于本文件。

3.1

安全事件 incident

对网络和信息系统或者其中的数据造成危害的事件。

4 缩略语

下列缩略语适用于本文件。

API：应用程序编程接口（Application Programming Interface）

CC：挑战黑洞（Challenge Collapsar）

CSRF：跨站请求伪造（Cross-site request forgery）

DNS：域名系统（Domain Name System）

HTTP：超文本传输协议（Hypertext Transfer Protocol）

HTTPS：安全超文本传输协议（Hypertext Transfer Protocol Secure）

ICMP：网间控制报文协议（Internet Control Messages Protocol）

IP：互联网协议（Internet Protocol）

IPv6：互联网协议第六版（Internet Protocol Version 6）

NDP：邻居发现协议(Neighbor Discovery Protocol)

SIP：会话初始协议（Session initialization Protocol）

SQL：结构化查询语言（Structured Query Language）

TCP：传输控制协议（Transport Control Protocol）

UDP：用户数据报协议（User Datagram Protocol）