



中华人民共和国国家标准

GB/T 44810.2—2024

IPv6 网络安全设备技术要求 第 2 部分：Web 应用防护系统（WAF）

Technical requirement for IPv6 network security equipment—
Part 2: Web application firewall (WAF)

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 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 1
- 5 功能性要求 2
 - 5.1 Web 应用内容控制 2
 - 5.2 攻击防护 2
 - 5.3 安全审计、告警与统计 3
 - 5.4 异常应急处置 4
- 6 性能要求 4
 - 6.1 HTTP 吞吐量 4
 - 6.2 HTTP 请求速率 5
 - 6.3 HTTP 并发连接数 5
- 7 兼容性要求 5
 - 7.1 部署 5
 - 7.2 接口 5
 - 7.3 界面 5
 - 7.4 数据存储 5
- 8 可靠性要求 5
- 9 自身安全性要求 5
- 参考文献 6

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2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、北京神州绿盟科技有限公司、华为技术有限公司、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、中国移动通信集团有限公司、中移（杭州）信息技术有限公司、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、新华三技术有限公司、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：戴方芳、董悦、姜剑、胡俊涛、王雨晨、李翔、黄雅静、寇增杰、刘为华、庞韶敏、曹政、石桂欣、温森浩、康和、王建民、付炎永、陈东、梁芳、程晋雪、吴庆、左虹、韩娟、刘鑫涌、孙军、王冲华、陈昌杰、陈磊、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 2 部分：Web 应用防护系统（WAF）

1 范围

本文件规定了支持 IPv6 的 Web 应用防护系统（WAF）的技术要求。

本文件适用于支持 IPv6 的 Web 应用防护系统（WAF）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 20281—2020 信息安全技术 防火墙安全技术要求和测试评价方法

GB/T 25069—2022 信息安全技术 术语

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 20281—2020 界定的以及下列术语和定义适用于本文件。

3.1

Web 应用防护系统 Web application firewall

部署于 Web 服务器前端，对流经的 HTTP/HTTPS 访问和响应数据进行解析，具备 Web 应用的访问控制及安全防护功能的网络安全产品。

注：Web 应用防护系统通常也称为“Web 应用防火墙”。

4 缩略语

下列缩略语适用于本文件。

CC：挑战黑洞（Challenge Collapsar）

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

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）

IP：互联网协议（Internet Protocol）

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

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

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

URL：统一资源定位器（Uniform Resource Locator）

WAF：Web 应用防护系统（Web Application Firewall）

XML：可扩展标记语言（Extensible Markup Language）

XSS：跨站脚本（Cross Site Scripting）