ICS 33.040.40
CCS M 32

NATIONAL STANDARD OF THE PEOPLE'S REPUBLIC OF CHINA

GB/T 44810.3-2024

Technical requirement for IPv6 network security equipment-Part 3: Intrusion prevention system (IPS)

IPv6网络安全设备技术要求 第3部分：入侵防御系统（IPS）

Issued on: October 26, 2024 **Implemented on: February 1, 2025**

Issued by: State Administration for Market Regulation;
Standardization Administration of the PRC

Table of Contents

Foreword

This document is in accordance with the provisions of GB/T 1.1-2020 "Guidelines for standardization work Part 1: Structure and drafting rules for standardization documents". Drafting is required.

This document is Part 3 of GB/T 44810 "Technical Requirements for IPv6 Network Security Equipment". GB/T 44810 has been published as follows part. Part 1: Firewall;- Part 2: Web Application Protection System (WAF);- Part 3: Intrusion Prevention Systems (IPS). - Please note that some of the contents of this document may involve patents. The issuing organization of this document does not assume the responsibility for identifying patents.

This document is proposed by the Ministry of Industry and Information Technology of the People's Republic of China.

This document is under the jurisdiction of the National Communications Standardization Technical Committee (SAC/TC 485).

This document was drafted by: China Academy of Information and Communications Technology, Huawei Technologies Co., Ltd., Beijing Shenzhou Green Alliance Technology Co., Ltd., Beijing Tian Rongxin Network Security Technology Co., Ltd., Zhengzhou Xindajiean Information Technology Co., Ltd., Beijing Haohan Deep Information Technology Co., Ltd.

Computer Network Emergency Response Technology Coordination Center, China Telecom Group Co., Ltd., Tianyi Security Technology Co., Ltd., Hangzhou Di Pu Technology Co., Ltd., Beijing Tonghe Shiyi Telecommunications Science and Technology Research Institute Co., Ltd., National Industrial Information Security Development Research Center, China Welfare Institute International Peace Maternal and Child Health Hospital, Beijing Yuanzhidian Information Security Technology Co., Ltd., New H3C Technologies Co., Ltd., Shenzhen Da School, Beijing Trustworthy Huatai Information Technology Co., Ltd., and Hangzhou Anheng Information Technology Co., Ltd.

The main drafters of this document are: Dong Yue, Dai Fangfang, Wang Yuchen, Li Xiang,

Chen Hongwei, Zhao Yuezheng, Bi Cheng, Wang Yan, Liu Weihua, Pang Shaomin, Chen Luying, Shi Guixin, Yan Hanbing, Kang He, Gong Chao, Wu Qing, Zuo Hong, Lu Yunpeng, Wang Xinping, Cheng Xi, Yu Guo, Chen Changjie, Ji Xinhua, Yang Zhiwei, Shi Chenwei, Wan Xiaolan, Du Jun, Duan Guna, and Tian Lidan.

Introduction

According to the Notice on Accelerating the Scale Deployment and Application of Internet Protocol Version 6 (IPv6), in order to better cope with the complex network environment, In order to meet the security challenges brought by the proliferation of IPv6 and the expansion of user scale, China has developed a series of IPv6 security standards.

Among them, GB/T 44810 "Technical Requirements for IPv6 Network Security Equipment" is to standardize the applicability of network security products in IPv6.

The technical standard is planned to consist of three parts.

Part 1: Firewall. The purpose is to ensure the effective application of firewalls in the new network environment after IPv6 deployment.

Part 2: Web Application Protection System (WAF). The purpose is to protect the Web application protection system after IPv6 deployment.

Effective application of WAF in the new network environment.

Part 3: Intrusion Prevention System (IPS). The purpose is to ensure that the Intrusion Prevention System (IPS) is used in the new network after IPv6 is deployed.

Effective application in network environment.

Technical Requirements for IPv6 Network Security Equipment Part 3: Intrusion Prevention System (IPS)

1 Scope

This document specifies the security technical requirements for an intrusion prevention system that supports IPv6.

This document applies to the design, development, deployment, use, maintenance, and testing of IPv6-enabled intrusion prevention systems.

2 Normative references

GB/T 25069-2022

GB/T 28451-2023

GB/T 44810.1-2024

3 Terms and Definitions

The terms and definitions defined in GB/T 25069-2022, GB/T 28451-2023 and the following apply to this document.

3.1 Security incident

An incident that causes harm to networks and information systems or the data contained therein.

4 Abbreviations

The following abbreviations apply to this document.

API. Application Programming Interface CC. Challenge Collapsar CSRF. Cross-site request forgery DNS. Domain Name System HTTP. Hypertext Transfer Protocol HTTPS. Hypertext Transfer Protocol Secure ICMP. Internet Control Messages Protocol IP. Internet Protocol IPv6.Internet Protocol Version 6 NDP. Neighbor Discovery Protocol SIP. Session Initialization Protocol SQL. Structured Query Language TCP. Transmission Control Protocol UDP. User Datagram Protocol