

ICS 35.040
CCS A 90

GA

**INDUSTRY STANDARD OF THE
PEOPLE'S REPUBLIC OF CHINA**

GA/T 1728-2020

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

信息安全技术 基于IPv6的高性能网络入侵监测系统产品安全技术要求
(English Translation)

Issued on: May 13, 2020

Implemented on: August 1, 2020

Issued by: Ministry of Public Security

Table of Contents

Preface	
1 Scope	
2 Normative references	
3 Terms and definitions	
4 Abbreviations	
5 Product description of high-performance network intrusion detection system based on IPv6	
6 General description	
6.1 Classification of safety technical requirements	
6.2 Security Level	
7 Safety function requirements	
7.1 Data detection function requirements	
7.2 Intrusion analysis function requirements	
7.3 Intrusion response function requirements	
7.4 Management control function requirements	
7.5 Requirements for processing test results	
7.6 Product flexibility requirements	
7.7 Identification	
7.8 Administrator Management	
7.9 Security Audit	
7.10 Incident Data Security	
7.11 Communication Security	
7.12 Product safety	
8 Network environment adaptability requirements	
8.1 Support pure IPv6 network environment	
8.2 Self-management under IPv6 network environment	
8.3 Support IPv6 transition network environment (optional)	
9 Performance requirements	
9.1 False alarm rate	
9.2 Underreporting rate	
9.3 Monitoring traffic	
9.4 Monitoring the number of concurrent connections	

9.5 Monitoring the rate of newly created TCP connections

9.6 Reduction ability

10 Security requirements

10.1 Development

10.2 Guiding documents

10.3 Life Cycle Support

10.4 Test

10.5 Vulnerability assessment

11 Requirements for different security levels

11.1 Safety function requirements

11.2 Safety assurance requirements

Foreword

This standard was drafted in accordance with the rules given in GB/T 1.1-2009.

This standard was proposed by the Cyber Security Bureau of the Ministry of Public Security.

This standard is under the jurisdiction of the Information System Security Standardization Technical Committee of the Ministry of Public Security.

Drafting organizations of this standard. Computer Information System Security Product Quality Supervision and Inspection Center of the Ministry of Public Security, the Third Research Institute of the Ministry of Public Security, and Wang Shenxin Information Technology (Beijing) Co., Ltd.

1 Scope

This standard specifies the security function requirements, environmental adaptability requirements, performance of IPv6-based high-performance network intrusion detection system products Requirements, security requirements and security classification.

This standard applies to the design, development and testing of high-performance network intrusion detection system products based on IPv6.

2 Normative references

The following documents are indispensable for the application of this document. For dated reference documents, only the dated version applies to this document.

For undated references, the latest version (including all amendments) applies to this

document.

GB/T 18336.3-2015 Information Technology Security Technology Information Technology Security Assessment Criteria Part 3: Security Assurance Components GB/T 25069-2010 Information Security Technical Terms

3 Terms and definitions

The following terms and definitions defined in GB/T 18336.3-2015 and GB/T 25069-2010 apply to this document.

event

A record of the occurrence or change of a system, service or network status can be used as the basis for analyzing security incidents.

Security incident

Through the analysis and processing of the incident, the occurrence of a system, service or network state can be identified, indicating a possible security breach Failure of rules or certain protective measures, or a previously unknown situation that may be related to safety, is likely to endanger business operations and Threat information security.

Invalidate

Any behavior that endangers or may endanger the integrity, confidentiality or availability of resources.

Intrusion detection

By collecting information and analyzing several key points in the computer network or computer system, discover the network or system Whether there are violations of security policies and signs of attacks.

detector

Used to collect real-time events that may indicate intrusions or abuse of information system resources, and to conduct preliminary analysis of the collected information Intrusion detection system components.