

ICS 35.240
CCS A 90

GA

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

GA/T 1542-2019

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

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
(English Translation)

Issued on: January 1, 1970

Implemented on: January 9, 2019

Issued by: Ministry of Public Security

Table of Contents

Foreword	
1 Scope	
2 Normative references	
3 Terms and definitions	
4 Acronyms	
5 Product Description of High-Performance Network Intrusion Prevention System Based on IPv6	
6 General description	
6.1 Classification of safety technical requirements	
6.2 Security Level Classification	
7 Safety function requirements	
7.1 Functional requirements for intrusion event analysis	
7.2 Intrusion event response function requirements	
7.3 Intrusion event audit function requirements	
7.4 Management control function requirements	
8 Requirements for own safety functions	
8.1 Identification and authentication	
8.2 Security management	
8.3 Audit logs	
9 Environmental adaptability requirements	
9.1 Supporting Pure IPv6 Network Environment	
9.2 Self-management in IPv6 network environment	
9.3 Supporting IPv6 Transition Network Environment (Optional)	
10 Performance requirements	
10.1 Throughput	
10.2 Delay	
10.3 Maximum concurrent connections	
10.4 Maximum connection rate	
10.5 Missing and Missing	
11 Security requirements	
11.1 Development	
11.2 Guidance Documents	

- 11.3 Life cycle support
- 11.4 Testing
- 11.5 Vulnerability assessment
- 12 Different security level requirements
 - 12.1 Safety function requirements
 - 12.2 Self-safe function requirements
 - 12.3 Security 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.

This standard was drafted. Computer Information System Security Product Quality Supervision and Inspection Center of the Ministry of Public Security.

1 Scope

This standard specifies the security function requirements, self-security function requirements, and environmental protection requirements of high-performance network-based intrusion prevention system products based on IPv6.

Environmental adaptability requirements, performance requirements, security requirements, and classification.

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

2 Normative references

The following documents are essential for the application of this document. For dated references, 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 guidelines Part 3. Security assurance components GB/T 25069-2010 Information Security Technology Terminology GB/T 28451-2012 information security

technology network intrusion prevention products technical requirements and test evaluation methods

3 Terms and definitions

The following terms and definitions defined in GB/T 18336.3-2015, GB/T 25069-2010 and GB/T 28451-2012 apply to this document Pieces.

IPv6-based high performance network intrusion product prevention system product
Deployed in the form of a transparent bridge or gateway on the network path, and analyzes network traffic to discover network behavior with intrusion characteristics.

Products that are intercepted before being transmitted to the protected network can be applied to different high-performance network application scenarios such as IPv4 and IPv6.

Security incident Analyze and process the event to identify the occurrence of a system, service, or network status, indicating a possible security breach Failure of regulations or certain protective measures, or a situation that may be safety related but previously unknown, is likely to endanger business operations and threats to information security.

Intrusion

Any act that endangers or may endanger the integrity, confidentiality, or availability of the resource.

Alert

When an attack or intrusion event is detected, the high-performance intrusion prevention system sends an urgent notification to an authorized administrator.

False positive

When no attack event occurs, the intrusion prevention system products intercept normal network traffic.

Omission false negative when an attack event occurs, the intrusion prevention system does not intercept it.

4 Acronyms

The following abbreviations apply to this document.

IPv6. Internet Protocol Version 6 NFS. Network File System TFTP. Trivial File Transfer Protocol

5 Product Description of High-Performance Network Intrusion Prevention System Based on IPv6

This standard proposes the security function requirements and security assurance requirements of IPv6-based high-performance network intrusion prevention system products. Network access Intrusion prevention products are usually deployed at the exit of the protected network in bridge, routing, or transparent mode, dividing the network into external and internal networks. Product functions it is to establish a security protection point between the internal and external networks. By analyzing the content of network communication data, according to the predefined attack defense rules and other defenses, Protection strategy, analyze and filter network communication data, resist attacks from external networks, protect internal network user resources or internal network servers, and provide a secure access service request or response to the protected network. In addition, intrusion prevention suitable for the next generation Internet network environment the product's protocol stack, in addition to supporting IPv4, should also support IPv6, IPv4/IPv6 transition technologies, and have high processing performance.

Assets protected by network intrusion prevention products are network services and user resources protected by security policies. In addition, intrusion prevention products it and its important data are also protected assets.

Figure 1 below is a typical deployment environment of network intrusion prevention products. The figure on the left is an enterprise intranet protection scenario.

Protect enterprise users from threats from the Internet. The picture on the right is a key server protection scenario. Network intrusion prevention products protect key servers from Under external threat.

Intranet

IPS

Router

Firewall

Client area

IPS

Router

Firewall

Server area

Figure 1 Typical operating environment of network intrusion prevention system products