

ICS 35.240
CCS A 90

GA

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

GA/T 1557-2019

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

信息安全技术 基于IPv6的高性能网络审计系统产品安全技术要求
(English Translation)

Issued on: January 1, 1970

Implemented on: April 16, 2019

Issued by: Ministry of Public Security

Table of Contents

Foreword
1 Scope
2 Normative references
3 Terms and definitions
4 IPv6 Network Audit Product Description
5 General description
5.1 Classification of safety technical requirements
5.2 Classification of security levels
6 Safety function requirements
6.1 Information Collection
6.2 Data restoration
6.3 Audit record statistics
6.4 Audit record analysis and processing
6.5 Management control requirements
6.6 Identification and identification
6.7 Audit logs
6.8 Security management
6.9 Data storage
7 Environmental adaptability requirements
7.1 Access method
7.2 IPv6 protocol consistency
7.3 IPv6 Application Environment Adaptability
7.4 IPv6 Management Environment Adaptability
8 Performance requirements
8.1 Processing power
8.2 Network Impact
9 Security requirements
9.1 Development
9.2 Guidance documents
9.3 Life cycle support
9.4 Testing
9.5 Vulnerability assessment

10 Classification requirements

10.1 Overview Error Bookmark not defined.

10.2 Classification of safety function requirements

10.3 Security Assurance Requirement Classification Error Undefined bookmark.

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, Network Security and Protection Bureau of the Ministry of Public Security.

1 Scope

This standard specifies the security function requirements, environmental adaptability requirements, performance requirements, Security requirements and classification requirements.

This standard applies to the design, development, and testing of high-performance network audit 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 20945-2013 Information security technology Information system security audit product technical requirements and test evaluation methods GB/T 25069-2010 Information Security Technology Terminology GA/T 695-2014 Information Security Technology Network Communication Audit Product Technical Requirements

3 Terms and definitions

As defined in GB/T 18336.3-2015, GB/T 20945-2013, GB/T 25069-2010 and GA/T 695-2014 and the following terms and Definitions apply to this document.

IPv6-based high performance network audit system product Record and analyze network communications, and take corresponding actions for specific events, while supporting IPv4, IPv6 and Degree technology and high performance products.

IPv6 transition technology Technology used to ensure coexistence and interoperability of services during the transition period from IPv4 to IPv6.

IPv4/IPv6 tunneling technology Tunneling technology based on IPv4 tunnel to transfer IPv6 data packets.

Dual protocol stack technology Enable both the IPv4 protocol stack and the IPv6 protocol stack on one device.

IPv4/IPv6 network address translation Through data packet conversion, mutual access between IPv4 nodes and IPv6 nodes during the network transition period is realized.

4 IPv6 Network Audit Product Description

IPv6 network audit products collect and analyze network communication data to audit user network behaviors (such as web browsing, FTP and TELNET communication, sending and receiving mail, IM going offline, etc.), network traffic, network attacks and other behaviors are recorded and analyzed. IPv6 network Audit products can help users record user behavior and network status within the audited network, and can trace back users who violate security policy requirements.

Households. IPv6 network audit products can be applied to both IPv4 and IPv6 network environments. In addition, IPv6-based network audit products can protect products Security of itself and its important data.

Network communication audit products are divided according to the deployment mode and can be divided into two types. serial deployment and parallel deployment. In tandem deployment mode, IPv6 the network audit product is between the access client and the network server. In the bypass deployment mode, IPv6 network audit products are in parallel to visit customers on the end switch, the network communication data is obtained through the mirror port.

Figure 1 shows the typical operating environment of IPv6 network audit products deployed in series.

Figure 1 IPv6 network audit product serial deployment environment

Figure 2 shows a typical operating environment for IPv6 network audit products deployed in

parallel.

Figure 2 IPv6 network audit product parallel deployment operating environment

5.1 Classification of safety technical requirements

This standard divides the security technical requirements of IPv6 network audit products into two categories. security functions and security assurance requirements. Among them, the safety function should Qiushi put forward specific requirements for the security functions that IPv6 network audit products should have, including access methods, information collection, data restoration, and auditing.

Record statistics, audit record analysis, management control requirements, etc .; security assurance requirements are proposed for the life cycle process of IPv6 network audit products Specific requirements, such as development, instructional documentation, lifecycle support, and testing.

5.2 Classification of security levels

The security level of IPv6 network audit products is divided into basic and enhanced levels according to the strength of their security function requirements and security assurance requirements.

Among them, security requirements refer to GB/T 18336.3-2015.

6.1 Information Collection

IPv6 network audit products should be able to set network data collection policies based on audit objectives, and should include at least one of the following items.

- a) The type of IP address of the collection target;
- b) the IP address or IP address segment policy of the collection target;
- c) collection network protocol application strategy;
- d) collection transmission protocol strategy;
- e) collection and application protocol strategy;
- f) acquisition time period strategy;
- g) other.

6.2.1 Restore basic network information

IPv6 network audit products should be able to restore network information within the target network, which should include.