

ICS 35.240
CCS A 90

GA

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

GA/T 1543-2019

**Information security technology - Security technical
requirements for network equipment information detection
products**

信息安全技术 网络设备信息探测产品安全技术要求
(English Translation)

Issued on: January 1, 1970

Implemented on: January 13, 2019

Issued by: Ministry of Public Security

Table of Contents

Foreword
1 Scope
2 Normative references
3 Terms and definitions
4 Network Device Information Detection 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 detection
6.2 Network topology generation
6.3 Checking unauthorized connection behavior
6.4 Impact on the network environment where the target system is located
6.5 Detection task management
6.6 Statistical reports
6.7 IPv6 protocol support
6.8 Identification and identification
6.9 Data Security
6.10 Audit logs
7 Security requirements
7.1 Development
7.2 Guidance documents
7.3 Life cycle support
7.4 Testing
7.5 Vulnerability assessment
8 Requirements for different security levels
8.1 Safety Function Requirements
8.2 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 (No. 3 Research Institute of the Ministry of Public Security) Ministry of Cyber Security and Protection.

1 Scope

This standard specifies the security function requirements, security guarantee requirements, and classification requirements for network equipment information detection products.

This standard applies to the design, development, and testing of network equipment information detection products.

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

3 Terms and definitions

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

Network equipment information Ports, service types, and versions of online hosts, network devices, and security devices in the target network environment.

Network equipment information detection product Connect to the target information system through the local area network, and then enter the online host, network equipment and security device information in the target network environment.

Probing products.

4 Network equipment information detection product description

The object of network equipment information detection products protection is the target information system. The product is usually deployed in the target network in a bypass mode.

Collect and analyze information of online hosts, network devices and security devices through online collection methods.

Figure 1 is a typical operating environment for network equipment information detection products.

Figure 1 Typical operating environment of network equipment information detection products

5.1 Classification of safety technical requirements

This standard divides the security technical requirements of network equipment information detection products into two categories. security functions and security assurance requirements. Among them, the safety function Capability requirements are specific requirements for the security functions that network equipment information detection products should have, including information detection, network topology generation, non-Authorized connection behavior checks, etc .; security guarantees require specific requirements for the development and use of the content of the network equipment information detection products.

Requirements, such as development, instructional documentation, lifecycle support, and testing.

5.2 Classification of security levels

The security level of network equipment information detection products is divided into basic level and increased level according to the strength of its security function requirements and security assurance requirements.

Strong, in which the security requirements refer to GB/T 18336.3-2015.

6.1.1 Device detection

The following methods should be used to detect hosts, network devices, and security devices that are online within the specified IP range.

- a) Quick scanning, such as ICMP;
- b) Deep scanning, such as SNMP, telnet, SSH, CDP and so on.

6.1.2 Port detection

It should be able to detect the port status on online hosts, network devices, and security devices in the specified IP range, and support custom-detected endpoints.

Mouth range and detection method.

6.1.3 Equipment basic information detection

It should be possible to obtain host operating system information, as well as system version, device type, and brand information for network and security devices.

6.1.4 Service Type and Version Detection

It should be able to detect the service type and version of the port.

6.2 Network topology generation

It should be able to generate a topology map for the specified network based on the detected information.

6.3 Unauthorized connection behavior check

It should be able to check the behavior of unauthorized devices connected to the network where the target information system is located, and trigger a report when unauthorized connection occurs police.

6.4 Impact on the network environment where the target system is located

In the process of use, it should minimize the occupation of the resources of the inspection target system or the network resources of the network to which they belong to prevent the impact of the inspection target system industry.

Services and the normal operation of the network, the average bandwidth consumption is less than 3MB/s.

6.5 Detection task management

It shall provide the detection task management function, which can suspend, stop, delete, and restart the detection task.

6.6 Statistical Report

It should be possible to report the detected information.