

ICS 35.040
CCS L 80



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

GB/T 20279-2015

**Information security technology -- Security technical
requirements of network and terminal separation products**

信息安全技术 网络和终端隔离产权安全技术要求

(English Translation)

Issued on: May 15, 2015

Implemented on: January 1, 2016

**Issued by: General Administration of Quality Supervision, Inspection and
Quarantine of the People's Republic of China**

Table of Contents

1 Scope...	4
2 Normative References...	4
3 Terms and Definitions...	4
4 Description of Network and Terminal Separation Products...	6
5 Security Technical Requirements...	9
5.1 Overall Description...	9
5.1.1 Classification of Security Technical Requirements...	9
5.1.2 Security Level...	9
5.2 Security Function Requirements...	10
5.2.1 Terminal Separation Products...	10
5.2.2 Network Separation Product...	13
5.2.3 Network Unilateral Transmission Product...	30
5.3 Security Assurance Requirements...	45
5.3.1 Requirements for Basic-level...	45
5.3.2 Requirements for Enhanced-level...	49
5.4 Environmental Adaptation Requirements...	57
5.4.1 Next generation internet Support (if any)...	57
5.4.2 Support IPv6 Transition Network Environment (optional)...	58
5.5 Performance Requirements...	59
5.5.1 Exchange Rate...	59
5.5.2 Hardware Switching Time...	59
Bibliography...	60

Foreword

This Standard was drafted according to the rules specified in GB/T 1.1-2009.

Please pay attention that some contents of this document may involve patents. The issuing organization of this Standard does not undertake the responsibility to identify these patents.

This Standard replaces GB/T 20279-2006 "Information Security Technology Security Techniques Requirements of Separation Components of Network and Terminal

Equipment".

The main differences between this Standard and GB/T 20279-2006 are as follows.

- The products were classified into terminal separation products, network separation products and network unilateral transmission products;
- The products were uniformly divided into basic-level and enhanced-level;
- The description of terminal separation products, network separation products and network unilateral transmission products were added;
- The requirement of the capability of supporting next generation internet protocol was added;
- The basic principles of technical requirements were added in appendix, including basic principles of security function requirements and basic principles of security assurance requirements.

This Standard was proposed by and shall be under the jurisdiction of National Technical Committee on Information Technology Security of Standardization Administration of China (SAC/TC 260).

Drafting organizations of this Standard. Quality Supervision Testing Center of Computer Information System Security Products of the Ministry of Public Security, Zhuhai Victory Idea Co., Ltd., Nanjing Shenxi Network Technology Co., Ltd. AND The Third Research Institute of Ministry of Public Security.

Chief drafters of this Standard. Lu Zhen, Gu Jian, Yu You, Li Xuan, Deng Qi, Zuo Anji, Lu Wenli and Liu Bin.

Information Security Technology-Security Technical
Requirements of Network and Terminal Separation
Products

1 Scope

This Standard specifies the security function requirements, security assurance requirements, environmental adaptation requirements and performance requirements of network and terminal separation products.

This Standard is applicable to the design, development and test of network and terminal separation products.

2 Normative References

The following documents are essential for the application of this document. For the dated references, only the dated editions apply to this document. For undated references, the latest editions (including amendments) apply to this document.

GB 17859-1999 Classified Criteria for Security Protection of Computer Information System

GB/T 18336.3-2008 Information Technology - Security Techniques - Evaluation Criteria For IT Security - Part 3.Security Assurance Requirements

GB/T 25069-2010 Information Security Technology - Glossary

3 Terms and Definitions

For the purpose of this Standard, the following terms and definitions as well as those defined in GB 17859-1999 and GB/T 25069-2010 apply.

3.1

Security domain

The computer or network area with the same security protection demand and security policy.

3.2

Physical disconnection

The case that the networks in different security domains cannot be directly or indirectly connected.

Note: In one physical network environment, the physical disconnection of networks in different security domains shall technically ensure disconnection of information in physical transmission and physical storage.

3.3

Protocol conversion

The separation and reestablishment of protocol. Separate the application data in the network-based common protocol from one end of separation product in a certain security domain, package to transmit special system protocol to the other end of separation product in other security domain, then separate the special protocol and package it into the required format.

3.4

Protocol separation

The networks in different security domains are physically connected, it is ensured that the protected information is logically separated through protocol conversion, and only the information with limited content required by the system for transmission may pass through.

3.5

Information ferry

It is a mode of information exchange, physical transmission channel only exists during transmission.

Note: During data transmission, the information is transmitted to the middle cache, the connection between middle cache and the security domain of the information destination is cut;

and then connect the transmission channel between middle cache and the security domain of

the information destination, transmit the information to the security domain of the information

destination, and physically cut the connection between the security domain of information source and middle cache. Middle cache is only connected with security domain at one end at

any one time.

3.6

Unilateral transmission unit

A pair of transmission units with physical unilateral transmission characteristic, this