ICS 35.030
CCS L 80

NATIONAL STANDARD OF THE PEOPLE'S REPUBLIC OF CHINA

GB/T 20279-2024

Replacing GB/T 20279-2015, GB/T 20277-2015

Cybersecurity technology - Technical specification for network and terminal separation products

网络安全技术 网络和终端隔离产品技术规范

Issued on: September 29, 2024 **Implemented on: April 1, 2025**

Issued by: State Administration for Market Regulation;
Standardization Administration of the PRC

Table of Contents

1 Scope 1
2 Normative references 1
3 Terms and definitions 1
4 Abbreviations 2
5 General 3
6 Security technical requirements 5
6.1 Security function requirements 5
6.2 Self-security requirements 9
6.3 Performance requirements 10
6.4 Security assurance requirements 11
7 Evaluation methods 13
7.1 Security function evaluation 13
7.2 Self-security evaluation 23
7.3 Performance evaluation 26
7.4 Security assurance evaluation 26
Annex A (normative) Classification of network and terminal separation products and grading of security technical requirements 33
Annex B (normative) Classification of network and terminal separation products and grading of evaluation methods 39

3 Terms and definitions

3.2 Physical disconnection is defined as the technique of using physical means to make sure that different security domains cannot be connected either directly or indirectly. The note adds that physical disconnection is applied both to physical conduction and to physical storage.

3.3 Protocol conversion is the technique of stripping the application data out of a public network protocol and encapsulating it in a private protocol proprietary to the system for transmission.

3.4 Information ferry is the data transmission technique in which information travels from the security domain of the source to an intermediate buffer area and then from that buffer area to the security domain of the destination. At any instant the buffer area is connected to one side only.

3.5 A unilateral transmission unit is a matched pair of independent sending and receiving parts, the sending part providing only a sending function and the receiving part only a receiving function; the note states that these functions are determined by physical characteristics.

3.6 to 3.10 define terminal separation products, network separation products, protocol conversion products, the gap, and network unilateral transmission products.

5 General

Network and terminal separation products fall into two families. Terminal separation products are isolation cards or isolation computers. Network separation products are divided by form and function into protocol conversion products, gaps and network unilateral transmission products; protocol conversion products and gaps are also commonly called security isolation and information exchange systems or products.

The functional aim of the whole family is to set a controlled point between different network security domains and to offer access-controlled services between them. The assets protected are the network services and resources covered by the security policy, and the product itself together with the important information held inside it.

A terminal separation product is normally an isolation card fitted into a host. An electronic switch connects, in mutually exclusive fashion, either security domain A with its hard disk 1 or security domain B with its hard disk 2, which is how the physical disconnection of the two domains is obtained. The card can also be integrated into the host so that the product takes the form of an isolation computer. This family achieves physical disconnection only by controlling the switching of the card.

A protocol conversion product is normally built as a double host: an internal processing unit, an external processing unit and a private protocol communication medium joining the two. That medium is the only physical channel trusted between the two security domains; it strips off TCP/IP and other public network protocols and carries a private protocol instead. The product provides application proxy service, protocol conversion, access control, information filtering and data exchange.

A gap is built in the same way but adds a dedicated isolation component acting as the intermediate buffer area: an isolation exchange board built around a dedicated isolation chip that contains an electronic switch and has the information ferry control logic fixed in it. The product provides application proxy service, information ferry, access control, information filtering and data exchange.

A network unilateral transmission product is a double host plus a unilateral transmission unit: a data sending processing unit, a data receiving processing unit and the unit itself. The sending unit connects to sending domain A and the receiving unit to receiving domain B, and information flows one way only, with no feedback signal of any kind. The one-way

physical transmission characteristic is fixed and cannot be altered; no software configuration or physical jumper can change the characteristic or the direction.

Network separation products may also appear as a front-end server, a protocol conversion product or gap or network unilateral transmission product, and a back-end server. The front and back servers mainly provide application proxy, access control and attack protection, while the middle element provides network isolation and data exchange.

Security function, self-security, performance and security assurance requirements are each divided into a basic grade and an enhanced grade. The strength of the security functions and of the self-security, together with the level of the assurance requirements, are the criteria for the division; compared with the basic grade the enhanced grade adds or strengthens items. The requirements applicable to each product family and their grading are given in Annex A, and the evaluation methods and their grading in Annex B.

6.1 Security function requirements

6.1.1.1 Information flow control policy: when switching the isolated computer information resources the product makes the user enter a switching password; before business data is transmitted the accessing user or device is authenticated, either by password, digital certificate or biometric information, or by a combination of two or more factors.

6.1.1.2 Information flow control function: the product cuts the internal and external domains apart in physical transmission so that the outside cannot enter the inside over a network connection and inside information cannot leak outward. In physical storage the two network environments are also cut apart: volatile parts such as memory and registers are zeroed on switching, non-volatile devices such as hard disks and memory cards keep internal and external information on separate storage devices, and for removable media such as optical discs, floppy disks and USB storage the user is prompted to intervene, or the device is forbidden, before the domain is switched. Access control policy elements include IP address, port and protocol type, TCP, UDP and application layer protocols among them, and by default the product refuses all data transmission. Further items cover data synchronisation tasks, proxy reception, timed periodic transmission, protocol conversion with a private protocol carrying a consistency check, physical time-division switching of the internal and external links so that both networks are never connected to the dedicated isolation component at once, and construction by physical means of the single one-way channel with no reverse transmission or feedback.

6.1.1.3 to 6.1.1.8 add illegal external connection detection with alarm, consistency of the switching signal, detection and alarm on illegal swapping of the hard disks, physical isolation of memory and of all USB ports where the product is a whole-machine isolation system, non-bypassability of the security policy check, and object reuse, under which a newly allocated resource carries no content from any earlier connection.

6.1.2 Application and protocol support: at least two of each type are supported, drawn from file transfer protocols such as HTTP, FTP and SMB, mail protocols such as SMTP and POP3, database protocols, audio and video protocols such as SIP and RTSP, industrial control protocols such as Modbus and OPC, internet of things protocols such as MQTT and JMS, service invocation protocols such as API and Web services, and encrypted protocols such as HTTPS and FTPS. Which of these apply depends on the product family and its field of use.

6.1.3 Information filtering is specified per protocol family: command filtering, keyword filtering of the transmitted content, file type filtering, and, for image files, recognition and filtering of non-image data hidden inside them; for mail, protocol conformance checking and keyword filtering of subject and attachments plus attachment type filtering; for databases, command filtering, keyword filtering and, as a recommendation, masking of table field content; for audio and video, signalling filtering and, as a recommendation, filtering by media coding format; and matching provisions for industrial control, internet of things, service invocation and encrypted protocols.

6.1.4 to 6.1.8 cover sensitivity labels with mandatory access control, denial of service attack protection against ICMP flood, SYN flood, UDP flood and ping of death, malicious code protection with a signature library, security isolation split into domain isolation and label isolation, high availability split into a main and standby failover mode and a cluster mode, and data integrity in storage and in transmission.

6.1.9 Security audit and analysis: the recorded event types are access requests matched by the policy, access requests blocked by the policy, and detected attacks. Log content includes the date and time, the subject, object and description, with packet logs carrying protocol type, source and destination address and source and destination port, and a description of the attack. Logs are reachable by the authorised administrator only, can be queried by date, time, subject and object, are held on non-volatile storage for not less than six months, raise an alarm to the administrator when the storage threshold is reached, and can be backed up automatically to other storage. Alarms merge repeated identical events to avoid an alarm storm and are delivered by sound and light, screen prompt, mail or short message, carrying subject, object, description, level, date and time. Statistics are shown on a graphical interface by IP, time span and application type, by attack event type, IP and time span, and by processor, memory and disk occupancy, with report output.

6.1.10 to 6.1.12 add an interconnection interface for sharing information with other security devices, operation in an IPv6 environment and in a dual IPv4 and IPv6 stack environment, and, where the internal or external host supports it, deployment in a virtualised environment with unified platform management and elastic resource adjustment.

6.2 Self-security requirements

6.2.1 Identification and authentication: user identities are uniquely identified; authentication