GB

NATIONAL STANDARD OF THE

PEOPLE'S REPUBLIC OF CHINA

ICS 35.040
L 80

GB/T 20279-2015

Replacing GB/T 20279-2006

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

信息安全技术　网络和终端隔离产品

安全技术要求

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;

Standardization Administration of the People's Republic of China.

Table of Contents

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 Shenyi 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

transmission unit consists of a pair of independent sending and receiving units, which can only work in simplex mode, sending unit only has single sending function, and receiving unit only has single receiving function, they form a creditable unilateral channel, which is free from any feedback information.

3.7

Terminal separation product

The security separation card or security separation computer which connects two different security domains simultaneously and achieves physical separation of security domains by adopting physical disconnection technology.

3.8

Network separation product

The product between two different security domains and achieving security separation of security domains and information exchange on network by adopting protocol separation technology.

3.9

Network unilateral transmission product

The only channel between two different security domains and achieving unilateral transmission of structure information physically, and it is ensured that only the information to which security policy permits for transmission may pass through, without any data transmission or feedback in the opposite direction.

4 Description of Network and Terminal Separation Products

According to form and function, network and terminal separation products may be classified into terminal separation products, network separation products and network unilateral transmission products, the purpose is to establish security control point between different network terminals and network security domains to provide controllable access service among different network terminals and network security domains. In addition, the protocol stack of network and terminal separation products of the next generation Internet network environment shall not only support IPv4 technology, but also IPv6 and IPv4/IPv6 transition technology.

The asset protected by network and terminal separation products are the network service and resources, etc. protected by security policy, in addition, the network and terminal separation products and the important data in them are also protected assets.

Figure 1 shows a typical running environment of terminal separation product. Generally,

basis for level classification. Security level emphasizes security characteristics, while environmental adaptation requirements and performance requirements are not the basis for level classification. Compared with basic-level contents, the added or changed contents in the text required by enhanced-level are bold in Song typeface.

5.2 Security Function Requirements

5.2.1 Terminal Separation Products

5.2.1.1 Requirements for basic-level

5.2.1.1.1 Access control

5.2.1.1.1.1 Definitions of security attributes

As for information storage and transmission units (mainly the storage devices and network access devices in different security domains), the only security attribute necessary for implementing security function policy shall be set for them by terminal separation products.

5.2.1.1.1.2 Modification of attributes

The security function of terminal separation product shall cover the function of modifying the parameters of attributes related to security for the authorized user of terminal equipment.

5.2.1.1.1.3 Attribute query

The security function of terminal separation product shall cover the function of providing security attribute query for the authorized user of terminal equipment.

5.2.1.1.1.4 Access authorization and rejection

The security function of terminal separation product shall cover the capability of providing clear access assurance and access rejection to the separated computer information resources. And technically ensure:

a) Separate internal and external security domains in physical transmission of information, ensure that the external security domain cannot intrude the internal security domain via network connection; and prevent internal security domain information from leaking to external security domain via network connection;

b) Separate two network environments in physical storage of information, as for the unit that information will be lost after power-off, temporary storage units such as memory and register shall be reset during network conversion，so as to prevent the remaining information from entering other network; as for the equipment that information will not be lost after power-off, storage device such

as magnetic tape unit and hard disk, the information of internal security domain and external security domain shall be stored in different storage devices; as for removable storage medium, such as CD, floppy disk and USB storage device, the user shall be reminded to intervene before external security domain conversion or forbidden to use such equipment in both security domains.

5.2.1.1.1.5 Switching signal consistency

Where the separated computer information resources are switched, for the security function of terminal separation products, the separated computer information resources shall be switched by the same signal to ensure consistency.

5.2.1.1.1.6 Password protection

Where the separated computer information resources are switched, the security function of terminal separation products shall guarantee that users must input switching password.

5.2.1.1.1.7 Physical separation of memory and USB port

If terminal separation products exist in the form of complete segregated system, the security function of terminal separation products shall be able to physically separate memory and all the USB ports to ensure that all the storage devices are physically separated and thus data security is physically ensured.

5.2.1.1.2 Non-bypass

Before security-related operation (for example, modification of security attribute) is allowed, the security function of terminal separation products shall ensure that it passes the inspection of security function policy.

5.2.1.1.3 Object reuse

When resource allocation is conducted for host connection of all the internal or external networks, the security function of terminal separation products shall ensure no provision of any information of previous connections.

5.2.1.2 Requirements for enhanced-level

5.2.1.2.1 Access control

5.2.1.2.1.1 Definitions of security attributes

As for information storage and transmission units (mainly the storage devices and network access devices in different security domains), the only security attribute necessary for security function policy shall be set for them by terminal separation products.

5.2.1.2.1.2 Modification of attributes

The security function of terminal separation product shall cover the function of modifying the parameters of attributes related to security for the authorized user of terminal equipment.

5.2.1.2.1.3 Attribute query

The security function of terminal separation product shall cover the function of providing security attribute query for the authorized user of terminal equipment.

5.2.1.2.1.4 Access authorization and rejection

The security function of terminal separation product shall provide the capability of clear access assurance and access rejection to the separated computer information resources. And technically ensure:

a) Separate internal and external security domains in physical transmission of information, ensure that the external security domain cannot intrude the internal security domain via network connection; and prevent internal security domain information from leaking to external security domain via network connection;

b) Separate two network environments in physical storage of information, as for the unit that information will be lost after power-off, temporary storage units such as memory and register shall be reset during network conversion，so as to prevent the remaining information from entering other network; as for the equipment that information will not be lost after power-off, storage device such as magnetic tape unit and hard disk, the information of internal security domain and external security domain shall be stored in different storage devices; as for removable storage medium, such as CD, floppy disk and USB storage device, the user shall be reminded to intervene before external security domain conversion or forbidden to use such equipment in both security domains.

5.2.1.2.1.5 Illegal external link of network

Security function of terminal separation products shall guarantee that users, in the intranet state, monitor whether user network is connected with the Internet at any time, and immediately disable the network and give a warning if discovered to ensure intranet security.

5.2.1.2.1.6 Switching signal consistency

Where the separated computer information resources are switched, for the security function of terminal separation products, the separated computer information resources shall be switched by the same signal to ensure consistency.

5.2.1.2.1.7 Illegal exchange of hard disk

The security function of terminal separation product shall identify the hard disk of corresponding network during initial installation, so as to ensure correspondence of hard disk and network and the security of intranet hard disk data.

5.2.1.2.1.8 Password protection

Where the separated computer information resources are switched, the security function of terminal separation products shall guarantee that users must input switching password.

5.2.1.2.1.9 Physical separation of memory and USB port

If terminal separation products exist in the form of complete segregated system, the security function of terminal separation products shall physically separate memory and all the USB ports to ensure that all the storage devices are physically separated and thus data security is physically ensured.

5.2.1.2.2 Non-bypass

Before security-related operation (for example, modification of security attribute) is allowed, the security function of terminal separation product shall ensure that it passes the inspection of security function policy.

5.2.1.2.3 Object reuse

Where resource allocation is conducted for host connection of all the internal or external networks, the security function of the terminal separation products shall guarantee no provision of any previously connected information content.

5.2.2 Network Separation Product

5.2.2.1 Requirements for basic-level

5.2.2.1.1 Access control

5.2.2.1.1.1 Basic information flow control policy

As for all the operations between the subject, object and subject and object of network separation product, network separation product shall be able to implement the following end-to-end basic information flow control policies:

a) The information flow sent and received between all subjects and objects shall implement network layer protocol stripping and be reduced to application layer data.

j) Service port:

k) Usage time or period;

l) Content keywords.

5.2.2.1.4.2 Initialization of attributes

The security function of network separation product shall contain the function of initializing the authorized administrator and host attributes by using default.

5.2.2.1.4.3 Modification of attributes

The security function of network separation product shall only provide the authorized administrator with the function of modifying the following (including but not limited to) parameters:

a) Relationship between identification and role (e.g.: configuration administrator, etc.);

b) Source address, destination address, transport layer protocol and requested service (e.g.: access control attributes such as source port number or destination port number);

c) The configured security parameters (e.g.: maximum authentication failure times and other data).

5.2.2.1.4.4 Attribute query

The security function of network separation product shall only provide the authorized administrator with the following query functions:

a) Source address, destination address, transport layer protocol and requested service (e.g.: access control attributes such as source port number or destination port number);

b) Keywords;

c) The information of such host transferring information via network separation product;

5.2.2.1.4.5 Initialization of authentication data

The security function of network separation product shall provide the initialization function for authentication data of authorized administrator according to the specified authentication mechanism and shall ensure only allowing the authorized administrator to use these functions.

5.2.2.1.4.6 Authentication time

Prior to any operation requested by all authorized administrators, the security function of network separation product shall ensure conducting identity authentication over each authorized administrator.

5.2.2.1.4.7 Minimum feedback

During authentication, the security function of network separation product shall only provide user with minimum feedback.

5.2.2.1.4.8 Authentication failure handling

After specific times of authentication failure, the security function of network separation product shall be able to terminate the process that the host trying to login establishes a session. The maximum failure times shall be set by authorized administrator only.

5.2.2.1.5 Audit

5.2.2.1.5.1 Generation of audit data

The security function of network separation product shall be able to generate an audit record for the following auditable events, including the occurrence date and time of the events, event type, subject identity, successful event or failed event and other information:

a) Turn-on and turn-off of audit function;

b) Any attempt to carry out operation for audit record, including turning off the audit function or subsystem, and the identification of affected object;

c) Any attempt for reading, modifying or damaging audit records;

d) All the requests for operation execution on the objects covered by separation product regulation (hosts on internal or external network), and the identification of affected objects;

e) All the attempts to modify security attributes, and the new values of modified security attributes;

f) All the requests for using the authentication data management mechanism in security function;

g) All the requests for the access to authentication data, and the objective of request for access;

h) Any use of authentication mechanism;

network), the security function of network separation product shall set a security zone for its execution environment and shall separate the security zones of all subjects (hosts on internal or external network) within the control range of network separation product.

5.2.2.1.7 Fault tolerance

Network separation product shall possess the fault-tolerant capability in active/standby mode. When one host is out of order due to failure of power supply, CPU and other hardware or software error, the fault tolerance function shall automatically switch the current security service function to another standby host which will continue to work and ensure the availability of security function.

5.2.2.1.8 Data integrity

The security function of network separation product shall protect the authentication data and data transmission policy stored in equipment against any unauthorized retrieval, modification and damage.

5.2.2.1.9 Cryptographic support

The security function of network separation product shall ensure the functions related to cryptographic algorithm it provides meeting the relevant requirements of the national competent cryptogram department.

5.2.2.2 Requirements for enhanced-level

5.2.2.2.1 Access control

5.2.2.2.1.1 Control policy for enhanced information flow

In allusion to subject, object and all operations between subject and object via network separation product, the information flow control policy of network separation product shall be able to execute the following control policies for end-to-end enhanced information flow:

a) All the information flows sent and received between subject and object shall undergo network layer protocol stripping and be reduced to application layer data, including larger attachments carried by application layer, e.g., e-mail attachment larger than 20M;

b) Identity authentication shall be carried out to the users authorized by the subject based on multiple factors such as user name/password and digital certificate prior to communication between subject and object; after identity authentication is passed, all the information flows sent and received between subject and object may be transmitted after being controlled and allowed by the security policy;

c) Authorized administrator shall use independent management interface and shall pass identity authentication, afterwards the management information sent between authorized administrator and network separation product may be transmitted after being allowed by the security policy.

5.2.2.2.1.2 Control function for enhanced information flow

The security function policy of network separation product shall be able to execute the following control functions for enhanced information flows and to provide specific access assurance capability and access rejection capability. Including:

a) Conduct information flow control by configuring access control list. The elements of access control list include: source IP address, destination IP address, source port, destination port and protocol No.;

b) Conduct compliance inspection on the information flows complying with such application protocols as HTTP, FTP, SMTP, POP3, SQL, RSTP and SIP;

c) Filter the protocol signaling and parameter keywords of the information flows complying with such application protocols as HTTP, FTP, SMTP, POP3, SQL, RSTP and SIP;

d) Configure the file synchronization task, read files from source host according to the parameters of synchronization task configured on network separation product, and ferry and transmit the files to destination host to realize file synchronization;

e) Configure the database synchronization task, read data from database of source host according to the parameters of synchronization task configured on network separation product, reduce data into files, and then ferry and transmit the files to the network of the other end, write them in the database of destination host to realize database synchronization;

f) Recognize the application type of subject, conduct information flow control via accessing to application control list, and prohibit access to object by unauthorized application;

g) Conduct physical time division switching to data transmission link of internal and external network by disconnecting the TCP/IP connection, i.e., internal and external network cannot connect with the special separation unit on physical link at the same time.

5.2.2.2.1.3 Mandatory access control

The security function of network separation product shall control the direct access of authorized administrator to relevant security function data via authorized administrator and the sensitivity label of security function data controlled by authorized administrator.

5.2.2.2.1.4 Residual information protection

When network separation product is making resource allocation for host connection of all the internal or external networks, the security function of network separation product shall ensure the resource it allocates not providing any information content generated in previous connection activities.

5.2.2.2.1.5 Non-bypass

Before security-related operation (for example, modification of security attribute, information transmission from host of internal network to host of external network, etc.) is allowed to be conducted, the security function of network separation product shall ensure that it passes the inspection of security function policy.

5.2.2.2.2 Attack resistance

Network separation product shall be able to defend against various DoS/DDoS attacks, and shall be able to recognize and defend against such attacks as SYN Flood and ICMP Flood.

5.2.2.2.3 Security management

5.2.2.2.3.1 Distinguishing of security management roles

The security functions of network separation product:

a) It shall distinguish the security-related management function from other functions;

b) It shall include all the functions necessary for installation, configuration and management of the security function of separation product, in which, it shall at least include: addition and deletion of subject (host sending information) and object (host receiving information), retrieval of security attributes, distribution, modification and revocation of security attributes, and retrieval and management of audit data;

c) It shall limit the ability of executing security-related management function as a kind of security management responsibility, which has a set of specially authorized responsibilities about function and response;

d) It shall be able to separate the authorized administrator in charge of executing management function from all other individuals or systems that use the

Network separation product shall inspect the complexity of password generated by authorized administrator by adopting password verification mechanism, the password strength shall ensure the password length being greater than 6 bits, and the password type shall be the communication of digits + capital and small letters.

5.2.2.2.5 Audit

5.2.2.2.5.1 Generation of audit data

The security function of network separation product shall be able to generate an audit record for the following auditable events, including the occurrence date and time of the events, event type, subject identity, successful event or failed event and other information:

a) Turn-on and turn-off of audit function;

b) Any attempt to carry out operation for audit record, including turning off the audit function or subsystem, and the identification of affected objects;

c) Any attempt for reading, modifying or damaging audit records;

d) All the requests for operation execution on the objects covered by separation product regulation (hosts on internal or external network), and the identification of affected objects;

e) All the attempts to modify security attributes, and the new values of modified security attributes;

f) All the requests for using the authentication data management mechanism in security function;

g) All the requests for the access to authentication data, and the objective of request for access;

h) Any use of authentication mechanism;

i) All the attempts for using the identification mechanism;

j) All the modifications (setting and update) of the configuration parameters of security function, whatever success or failure, and the new values of configuration parameters;

k) Termination of session connection as the identification attempt failure times exceed the set limit, and the identifier used for session connection.

5.2.2.2.5.2 Security audit analysis

The security function of network separation product shall provide the following statistical analysis functions:

a) **Statistics on the application types used during operation on objects by the subjects covered by separation product regulation (hosts on internal or external network);**

b) **Statistics on the total flow of network separation product and the flow of each application type;**

c) **Statistics on occupancy rate of CPU, internal memory and disc of network separation product;**

d) **Online user list and statistics on online user duration.**

5.2.2.2.5.3 User identity association

The security function of network separation product shall be able to associate each auditable event with the user identity causing this event.

5.2.2.2.5.4 Audit record management

The security function of network separation product shall enable the authorized administrator to file, delete and empty the audit record.

5.2.2.2.5.5 Intelligible format

The security function of network separation product shall make all audit data stored in permanent audit record be intelligible.

5.2.2.2.5.6 Limitation of access to audit record

The security function of network separation product shall only allow the authorized administrator to access the audit record.

5.2.2.2.5.7 Optional retrieval of audit data

The security function of network separation product shall provide the audit retrieval tool for searching and sequencing the audit data according to subject ID, object ID, data and time and the logical combination of these parameters.

5.2.2.2.5.8 Audit data loss prevention

As for the maximum audit storage capacity causing audit data loss due to failure or storage depletion of capacity, the developer of network separation product shall provide corresponding analysis result. Moreover, the security function of network separation product shall:

other host shall continue to provide security service function and ensure the availability of security function.

5.2.2.2.8 Data integrity

The security function of network separation product shall protect the authentication data and data transmission policy stored in equipment against any unauthorized retrieval, modification and damage.

5.2.2.2.9 Cryptographic support

The security function of network separation product shall ensure the functions related to cryptographic algorithm it provides meeting the relevant requirements of the national competent cryptogram department.

5.2.3 Network Unilateral Transmission Product

5.2.3.1 Requirements for basic-level

5.2.3.1.1 Access control

5.2.3.1.1.1 Control policy for information flow

Network unilateral transmission product shall encapsulate the network information flow stripping protocol of data sender again and unilaterally transmit it into the network destination host of information receiver.

5.2.3.1.1.2 Control function for basic information flow

The security function policy of network unilateral transmission product shall be able to execute the following control functions for basic information flows and to provide specific access assurance capability and access rejection capability. Including:

a) Configure the security attribute value of unilateral synchronization task to achieve unilateral transmission from clear source data to target data. By default, network unilateral transmission product shall reject the unilateral transmission of any data;

b) Explicitly reject the access if the source host IP address, destination host IP address or service type contained in information flow mismatches the security attribute value of unilateral synchronization task;

c) Conduct virus scanning for data content of unilateral transmission to cut off the transmission of virus data;

d) Conduct keyword inspection on data content of unilateral transmission to cut off the transmission of illegal data;

e) Conduct identity authentication for the subject sending and receiving data flow to avoid access of illegal data;

f) Support such service types as unilateral transmission of files and unilateral transmission of database.

5.2.3.1.1.3 Unilateral transmission assurance

The security function of network unilateral transmission product shall construct the only channel for information unilateral transmission in physical mode to achieve information unilateral transmission. That is to say, information can only be transmitted from one security domain to another security domain, and it shall be ensured that no information transmission or feedback occurs in the opposite direction. As for the unilateral transmission unit, its data sending unit is only provided with single data sending function and its data receiving unit is only provided with single data receiving function, and there is no software or hardware which is potential to lead to the change of physical characteristics.

5.2.3.1.1.4 Residual information protection

Where resource allocation is conducted by network unilateral transmission product for newly created unilateral synchronization task, the security function shall ensure the resource it allocates not providing any information content generated by previous unilateral synchronization tasks.

5.2.3.1.1.5 Non-bypass

Before security-related operation (for example, modification of security attributes, creation of synchronization task, etc.) is allowed to be conducted, the security function of network unilateral transmission product shall ensure that it passes the inspection of security function policy.

5.2.3.1.1.6 Data integrity assurance

Network unilateral transmission product shall be provided with integrity protection function for data unilateral transmission process, to ensure the integrity of unilaterally transmitted data under the premise of no feedback information.

5.2.3.1.2 Attack resistance

Network unilateral transmission product shall be able to defend against various DoS/DDoS attacks, and shall be able to recognize and defend against such attacks as SYN Flood and ICMP Flood.

5.2.3.1.3 Security management

5.2.3.1.3.1 Distinguishing of security management roles

The security functions of network unilateral transmission product:

a) It shall distinguish the security-related management function from other functions;

b) It shall include all the functions necessary for installation, configuration and management of the security function of network unilateral transmission product, in which, it shall at least include: addition and deletion of subject (host sending information) and object (host receiving information), retrieval of security attributes, distribution, modification and revocation of security attributes, retrieval and management of audit data;

c) It shall limit the ability of executing security-related management function as a kind of security management responsibility, which has a set of specially authorized responsibilities about function and response;

d) It shall be able to separate the authorized administrator in charge of executing management function from all other individuals or systems that use the separation unit;

e) It shall only allow the authorized administrator to undertake the security management responsibility;

f) It shall allow the authorized administrator to undertake security management responsibility only after a specific request is put forward.

5.2.3.1.3.2 Management function

The security function of network unilateral transmission product shall provide the authorized administrator with the following management functions:

a) Setting and updating the security-related data;

b) Executing the initialization, system startup and shutdown, and backup and recovery functions of network unilateral transmission product, among which the backup capability shall be provided with support of automated tools;

c) Setting such availability parameters as dual-machine hot standby;

d) If remote management is provided, then it shall be capable of:

1) Restricting the address being able to conduct remote management;

2) Protecting remote management session via encryption.

5.2.3.1.3.3 Independent management interface

Network unilateral transmission product shall connect with the authorized administrator

The security function of network unilateral transmission product shall protect the authentication data and data transmission policy stored in equipment against any unauthorized retrieval, modification and damage.

5.2.3.1.8 Running status monitoring

The security function of network unilateral transmission product shall be able to monitor the status of LAN and WAN host of unilateral transmission product in real time, such as CPU utilization rate, internal memory occupancy rate, storage space, etc.

5.2.3.2 Requirements for enhanced-level

5.2.3.2.1 Access control

5.2.3.2.1.1 Control policy for information flow

Network unilateral transmission product shall encapsulate the network information flow stripping protocol of data sender again and unilaterally transmit it into the network destination host of information receiver.

5.2.3.2.1.2 Control function for basic information flow

The security function policy of network unilateral transmission product shall be able to execute the following control functions for basic information flows and to provide specific access assurance capability and access rejection capability. Including:

a) Configure the security attribute value of unilateral synchronization task to achieve unilateral transmission from clear source data to target data. By default, network unilateral transmission product shall reject the unilateral transmission of any data;

b) Explicitly reject the access if the source host IP address, destination host IP address or service type contained in information flow mismatches the security attribute value of unilateral synchronization task;

c) Conduct virus scanning for data content of unilateral transmission to cut off the transmission of virus data;

d) Conduct keyword inspection on data content of unilateral transmission to cut off the transmission of illegal data;

e) Conduct identity authentication for the subject sending and receiving data flow to avoid access of illegal data;

f) Support such service types as unilateral transmission of files and unilateral transmission of database.

5.2.3.2.1.3 Control function for enhanced information flow

The security function policy of network unilateral transmission product shall be able to execute the following control functions for enhanced information flows and to provide specific access assurance capability and access rejection capability. Including:

a) Analyze the code format of multiple data, recognize if the document includes non-text type data, and cut off or release according to the security policy configured by the authorized administrator;

b) Support such service types as file unilateral transmission, database unilateral transmission, e-mail unilateral transmission and agency receiving unilateral transmission, etc.;

c) Complete data unilateral transmission at the specified time according to preset time periodicity.

5.2.3.2.1.4 Unilateral transmission assurance

Network unilateral transmission product shall construct the only channel for information unilateral transmission in physical mode to achieve information unilateral transmission. That is to say, information can only be transmitted from one security domain to another security domain, and it shall be ensured that no information transmission or feedback occurs in the opposite direction. As for the unilateral transmission unit, its data sending unit is only provided with single data sending function and its data receiving unit of them is only provided with single data receiving function, and there is no software or hardware which is potential to lead to the change of physical characteristics.

5.2.3.2.1.5 Mandatory access control

Network unilateral transmission product shall be able to structure a mandatory access control model according to the type of unilateral synchronization task, the security function shall be able to recognize the sensitivity label of user and application data, and shall be able to implement mandatory access control policy according to label.

5.2.3.2.1.6 Residual information protection

Where resource allocation is conducted by network unilateral transmission product for newly created unilateral synchronization task, the security function shall ensure the resource it allocates not providing any information content generated by previous unilateral synchronization tasks.

5.2.3.2.1.7 No-bypass

Before security-related operation (for example, modification of security attributes, creation of synchronization task, etc.) is allowed to be conducted, the network unilateral transmission product shall ensure that it passes the inspection of security

function policy.

5.2.3.2.1.8 Data integrity assurance

Network unilateral transmission product shall be provided with integrity protection for data unilateral transmission process, to ensure the integrity of unilaterally transmitted data under the premise of no feedback information.

5.2.3.2.2 Attack resistance

Network unilateral transmission product shall be able to defend against various DoS/DDoS attacks, and shall be able to recognize and defend against such attacks as SYN Flood and ICMP Flood.

5.2.3.2.3 Security management

5.2.3.2.3.1 Distinguishing of security management roles

The security functions of network unilateral transmission product:

a) It shall distinguish the security-related management function from other functions;

b) It shall include all the functions necessary for installation, configuration and management of the security function of network unilateral transmission product, in which, it shall at least include: addition and deletion of subject (host sending information) and object (host receiving information), retrieval of security attributes, distribution, modification and revocation of security attributes, retrieval and management of audit data;

c) It shall limit the ability of executing security-related management function as a kind of security management responsibility, which has a set of specially authorized responsibilities about function and response;

d) It shall be able to separate the authorized administrator in charge of executing management function from all other individuals or systems that use the separation unit;

e) It shall only allow the authorized administrator to undertake the security management responsibility;

f) It shall allow the authorized administrator to undertake security management responsibility only after a specific request is put forward.

5.2.3.2.3.2 Management function

The security function of network unilateral transmission product shall provide the authorized administrator with the following management functions:

e) Parameter configuration of external trusted IT product, including: parameters of time synchronization server, parameters of log server, etc.;

f) System parameters: size of log memory space, equipment name, etc.;

g) Role attributes of user: authorized administrator, authorized auditor, authorized user, etc.;

h) User management attributes: user name, user role, user password, etc.

5.2.3.2.4.3 Initialization of attributes

The security function of network unilateral transmission product shall provide the function of initializing the authorized administrator and host attributes by using default.

5.2.3.2.4.4 Modification of attributes

The security function of network unilateral transmission product shall only provide the authorized administrator with the function of modifying the following (including but not limited to) parameters:

a) Relationship between identification and role (e.g.: configuration administrator, etc.);

b) Security attribute values of subject (data collector) and object (data receiver);

c) The configured security parameters (e.g.: maximum authentication failure times and other data).

5.2.3.2.4.5 Attribute query

The security function of network unilateral transmission product shall only provide the authorized administrator with the following queries:

a) Relationship between identification and role;

b) Security attribute values of subject (data collector) and object (data receiver);

c) All the configured security parameters.

5.2.3.2.4.6 Initialization of authentication data

The security function of network unilateral transmission product shall provide the initialization function for authentication data of authorized administrator according to the specified authentication mechanism and shall ensure only allowing the authorized administrator to use these functions.

5.2.3.2.4.7 Authentication time

Prior to any operation requested by all authorized administrators, the security function of network unilateral transmission product shall ensure conducting identity authentication over each authorized administrator.

5.2.3.2.4.8 Minimum feedback

During authentication, the security function of network unilateral transmission product shall only provide user with minimum feedback.

5.2.3.2.4.9 Authentication failure handling

After specific times of authentication failure, the security function of network unilateral transmission product shall be able to terminate the process that the host trying to login establishes a session. The maximum failure times shall be set by authorized administrator only.

5.2.3.2.4.10 Timeout re-authentication

The security function of network unilateral transmission product shall be provided with lock or logout function for login timeout. Without any operation within the set time period, the security function of network unilateral transmission product shall terminate the session, and shall require an identity authentication again for reoperation. The maximum timeout shall only be set by authorized administrator.

5.2.3.2.4.11 Multi-authentication mechanism

The security function of network unilateral transmission product shall provide two or more than two types of authentication mechanisms to support multiple identity authentication of users in the case that network subject of sender sends data to the network of receiver via information flow receiving service built in network unilateral transmission product.

5.2.3.2.4.12 Anti-replay

The authentication mechanism of network unilateral transmission product shall possess anti-replay ability so that the authorized administrator and other users cannot pass the authentication again by copying and using the authentication information of last time.

5.2.3.2.4.13 Protected authentication feedback

Password and other sensitive information input by the authorized administrator of network unilateral transmission product during identification process shall be displayed on login input interface of authentication information in an invisible and un-inferable way.

5.2.3.2.4.14 Password strength

5.3.1.3.3 Informal correspondence verification

The developer shall provide correspondence analysis among all the adjacency pairs represented by product security function.

For each adjacency pair represented by product security function, the analysis shall clarify that all relevant security functions represented by relatively abstract security function shall be refined correctly and completely in relatively specific security function representation.

5.3.1.4 Instructive documents

5.3.1.4.1 Administrator manual

The developer shall provide administrator manual which shall be kept consistent with other files submitted for evaluation.

The administrator manual shall cover the following contents:

a) Management functions and interfaces which are accessible to administrators;

b) How to safely manage products;

c) The functions and authorities that shall be controlled in the security handling environment;

d) All assumptions of users' behaviors concerned with safe operation of product;

e) All the security parameters controlled by administrators, if possible, security values shall be indicated;

f) Every security-related event concerned with management function, including the modification of security characteristics of the entity controlled by security function;

g) All IT environmental security requirements concerned with administrators.

5.3.1.4.2 User guide

The developer shall provide user guide which shall be kept consistent with other files submitted for evaluation.

The user guide shall cover the following contents:

a) Security functions and interfaces which are accessible to non-administrators of the product;

b) The usage methods of the security functions and interfaces which the product

provides to the users;

c) All the functions and authorities which are available to users and controlled by security handling environment;

d) The responsibilities which the users shall bear in product safe operation;

e) All security requirements of IT environment concerned with users.

5.3.1.5 Test

5.3.1.5.1 Test coverage

The developer shall provide the evidence for test coverage.

It shall be shown in evidence for test coverage that the test identified in test document is corresponding to the product security function described in functional specification.

5.3.1.5.2 Functional test

The develop shall test the security function, document the results and provide test document.

The test documents shall include the following items:

a) The test plan, which shall identify the security function to be tested and describe the objective of test;

b) The test process, which shall identify the test to be executed, and describe the test overview of each security function, including the order dependence on other test results;

c) Expected test result, which shall indicate the expected output after the success of test;

d) Actual test result, which shall indicate that each tested security function can operate as required.

5.3.1.5.3 Independent test

5.3.1.5.3.1 Consistency

The developer shall provide products suitable for the test and provide the same test set as those used in the product self-test.

5.3.1.5.3.2 Sampling

The developer shall provide a group of equivalent resources for sample testing of security function.

5.3.1.6 Vulnerability assessment

5.3.1.6.1 Product security function strength assessment

The developer shall make an security function strength analysis to each security mechanism with notice of security function strength identified in the instructive documents and explain the measurement for the security mechanism reaching or exceeding the defined minimum strength grade or specific function strength.

5.3.1.6.2 Vulnerability analysis for developers

The developer shall execute vulnerability analysis and provide vulnerability analysis documents.

The developer shall make analysis and document to all kinds of product functions from the obvious approach in which the users may damage security policy. For determined vulnerability, the developer shall explicitly record the taken measures.

For each vulnerability, there shall be evidence to prove that this vulnerability cannot be used in the environment of using product.

5.3.2 Requirements for Enhanced-level

5.3.2.1 Configuration management

5.3.2.1.1 Partial configuration management automatization

Configuration management system shall provide one automatic mode to support the generation of products and ensure that only authorized change can be made to the realization representation of products.

Configuration management plan shall describe the automated tools used and how to use them in configuration management system.

5.3.2.1.2 Configuration management capability

5.3.2.1.2.1 Version number

The developer shall provide unique identification for the different product versions.

5.3.2.1.2.2 Configuration items

The developer shall use configuration management system and provide configuration management documents.

Configuration management document shall include a configuration list, which shall identify uniquely all the configuration items constituting products and describe them and the methods to make a unique identification for configuration items and provide

5.3.2.2.2 Modification detection

Delivery document shall describe how to provide multiple procedural and technical measures to detect the modification or the difference between the main copy of the developer and the version received by the user. It shall also describe how to use multiple programs to discover product delivery to the user in the disguise of the developer or when the developer does not send anything to the user.

5.3.2.2.3 Installation, generation and startup programs

The developer shall provide document to describe the installation, generation and startup process of the product.

5.3.2.3 Development

5.3.2.3.1 Functional specification

5.3.2.3.1.1 Informal functional specification

The developer shall provide one functional specification which shall meet the following requirements:

a) Describe the security function and external interface of products in informal form;

b) Be intrinsically consistent;

c) Describe the purpose and usage methods of all the external interfaces, and provide the details of effect, exceptions and error messages in due course;

d) Represent the product security functions completely.

5.3.2.3.1.2 Well-defined external interface

Functional specification shall cover that rationality of security function represented completely.

5.3.2.3.2 High level design

5.3.2.3.2.1 Descriptive high level design

The developer shall provide the high level design of product security functions, which shall meet the following requirements:

a) The representation shall be informal;

b) Be intrinsically consistent;

c) Describe the structure of security function according to subsystems;

d) Describe the security function provided by each security function subsystem;

e) Identify any fundamental hardware, firmware or software required by security function, and one representation of the function provided by the supportive protection mechanism realized by these hardware, firmware or software;

f) Identify all the interfaces of security function subsystems;

g) Identify which interfaces are externally visible in security function subsystems.

5.3.2.3.2.2 Security strengthened high level design

The security strengthened high level design provided by developer shall meet the following requirements:

a) Describe the purpose and method to use all the interfaces of product function subsystem and provide the details of effect, exceptions and error messages in due course;

b) Describe products from two aspects: i.e. security policy implementation and other subsystems.

5.3.2.3.3 Subset of security function realization

The developer shall provide realization representation for the selected security function subset. Realization representation shall be unambiguous and define security function in detail so as to generate security function with no need of further design. Realization representation shall be intrinsically consistent.

5.3.2.3.4 Descriptive low level design

The developer shall provide low level design of security function which shall meet the following requirements:

a) The representation shall be informal;

b) Be intrinsically consistent;

c) Describe security function according to modules;

d) Describe the purpose of each model;

e) Define the interrelationship between models according to the provided security function and the dependence to other models;

f) Describe how each security policy implementation function is provided;

g) Identify all interfaces of security function module;

h) Identify which interfaces are externally visible in security function module;

i) Describe the purpose and usage methods of all the interfaces and provide the details of effect, exceptions and error messages in due course;

j) Describe products from two aspects: i.e. security policy implementation module and other modules.

5.3.2.3.5 Informal correspondence verification

The developer shall provide correspondence analysis among all the adjacency pairs represented by product security function.

For each adjacency pair represented by product security function, the analysis shall clarify that all relevant security functions represented by relatively abstract security function shall be refined correctly and completely in relatively specific security function representation.

5.3.2.3.6 Informal product security policy model

The developer shall provide security policy model which shall meet the following requirements:

a) The representation shall be informal;

b) Describe the rules and features of all security policies which can be modeled;

c) Contain rationality, i.e. demonstrating that this model is consistent and complete with respect to all the modeled security polices;

d) Clarify the correspondence between security policy model and functional specification, i.e., demonstrating that the security functions in all the functional specification are consistent and complete with respect to the security policy model.

5.3.2.4 Instructive documents

5.3.2.4.1 Administrator manual

The developer shall provide administrator manual which shall be kept consistent with other files submitted for assessment.

The administrator manual shall cover the following contents:

5.4.1.2.2 IPv6 NDP protocol consistency

Network separation product / network unilateral transmission product shall support IPv6 NDP protocol consistency.

5.4.1.2.3 IPv6 Autoconfig protocol consistency

Network separation product / network unilateral transmission product shall support IPv6 Autoconfig protocol consistency.

5.4.1.2.4 IPv6 PMTU protocol consistency

Network separation product / network unilateral transmission product shall support IPv6 PMTU protocol consistency.

5.4.1.2.5 ICMPv6 protocol consistency

Network separation product / network unilateral transmission product shall support ICMPv6 protocol consistency.

5.4.1.3 Protocol toughness

Network separation product / network unilateral transmission product shall ensure protocol robustness to resist the attack of abnormal protocol message under IPv6 network environment. Abnormal protocol messages include:

a) IPv6 abnormal message;

b) ICMPv6 abnormal message;

c) Abnormal message of other protocols.

5.4.1.4 Self-management under IPv6 network environment

Network separation product / network unilateral transmission product shall support self-management under IPv6 network environment.

5.4.2 Support IPv6 Transition Network Environment (optional)

5.4.2.1 Double protocol stack

Network separation product / network unilateral transmission product shall support IPv4 /IPv6 double stack network environment and be able to work normally under IPv4/IPv6 double stack network environment.

5.4.2.2 Protocol conversion

Network separation product / network unilateral transmission product shall support the interconversion between IPv4 and IPv6 networks and be able to work normally under

protocol conversion network environment.

5.4.2.3 Tunnel

5.4.2.3.1 6over4

Network separation product / network unilateral transmission product shall support 6over4 network environment and be able to work normally under 6over4 network environment.

5.4.2.3.2 6to4

Network separation product / network unilateral transmission product shall support 6to4 network environment and be able to work normally under 6to4 network environment.

5.4.2.3.3 ISATAP

Network separation product / network unilateral transmission product shall support ISATAP network environment and be able to work normally under ISATAP network environment.

5.5 Performance Requirements

5.5.1 Exchange Rate

The exchange rate of network separation product shall be greater than 1,000 Mbit/s.

5.5.2 Hardware Switching Time

The hardware switching time of network separation product shall be less than 5 ms.

Bibliography

[1] GB/T 18336.1-2008 Information Technology - Security Techniques - Evaluation criteria for IT security - Part 1: Introduction and General Model (ISO/IEC 15408-1: 2005, IDT)

[2] GB/T 18336.2-2008 Information Technology - Security Techniques - Evaluation Criteria for IT Security - Part 2: Security Functional Requirements (ISO/IEC 15408-2: 2005, IDT)

[3] GB/T 22239-2008 Information Security Technology - Baseline for Classified Protection of Information System Security

[4] GA 370-2001 Security Technical Requirements of Terminal Equipment

_____ END _____

This is an excerpt of the PDF (Some pages are marked off intentionally)

------ The End ------