GB

NATIONAL STANDARD OF THE

PEOPLE'S REPUBLIC OF CHINA

ICS 35.040
L 80

GB/T 20277-2015

Replacing GB/T 20277-2006

Information Security Technology - Testing and Evaluation Approaches of Network and Terminal Separation Products

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 given in GB/T 1.1-2009.

This Standard replaces GB/T 20277-2006 “Information Security Technology - Testing and Evaluation Techniques of Separation Components of Network and Terminal Equipment”.

Compared with GB/T 20277-2006, this Standard has the main differences as follows:

— Classification was amended into terminal separation products, network separation products and network unilateral transmission products;

— Level was uniformly divided into base level and enhanced level;

— Add testing contents of next generation Internet Protocol support capability.

Please note that some of the content of this document may involve patents. The issuing organization of this document does not undertake the responsibility to identify any or all such patent rights.

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.

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

The previous edition of the standard superseded by this Standard is as follows:

— GB/T 20277-2006.

Information Security Technology - Testing and Evaluation Approaches of Network and Terminal Separation Products

1 Scope

This Standard specifies testing and evaluation approaches of network and terminal separation products according to technical requirements of GB/T 20279-2015.

This Standard is applicable to testing and evaluation of network and terminal separation products developed according to security class requirements of GB/T 20279-2015.

2 Normative References

The following documents are essential to the application of this document. For the dated documents, only the versions with the dates indicated are applicable to this document; for the undated documents, only the latest version (including all the amendments) are applicable to this standard.

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

GB/T 20279-2015 Information Security Technology - Security Technical Requirements of Network and Terminal Separation Products

GB/T 25069-2010 Information Security Technology - Glossary

3 Terms and Definitions

For the purpose of this Standard, terms and definitions established in GB 17859-1999, GB/T 25069-2010 and GB/T 20279-2015 apply.

5 Security Function Testing

5.1 Overall Description

5.1.1 Classification of testing and evaluation approaches

In this Standard, according to technical requirements of GB/T 20279-2015, requirements for testing and evaluation approaches of network and terminal separation products are classified into four categories: security function, security assurance, environmental adaptation and performance requirements.

5.1.2 Security level

Corresponding to GB/T 20279-2015, security level is classified into base level and enhanced level in this Standard. Compared with contents of base level, added or changed contents of requirements for the enhanced level are expressed in "bold Song typeface" in the main body.

5.2 Terminal Separation Products

5.2.1 Base-level testing

5.2.1.1 Access control

5.2.1.1.1 Definition of security attribute

Testing and evaluation approaches and expected results of the definition of security attribute of terminal separation products are as follows:

a) Testing and evaluation approaches:

Documents provided by developers are assessed; for information storage and transmission components, security attribute necessary for terminal separation products is assessed and specific contents are stated. Definition of security attribute of products is tested, tested results are recorded and it is judged whether the results are fully in accordance with the requirements for the above testing and evaluation approaches.

b) Expected results:

For the products, security attribute shall be able to be set and shall at least include network switching mode in different security domains, security zones of such storage devices as optical drive and floppy drive, network equipment access type and other security attributes mentioned in documents of the developers.

5.2.1.1.2 Attribute modification

Testing and evaluation approaches and expected results of attribute modification of terminal separation products are as follows:

a) Testing and evaluation approaches

Documents provided by developers are assessed, including detailed description on attribute modification. Modification operation is conducted for the security attribute and functions of product modification and security-related attribute parameters are tested, including security domain network switching. Testing results are recorded and it is judged whether such results are fully in accordance with the requirements for the above testing and evaluation approaches.

b) Expected results:

For the products, parameters of security-related attribute shall be able to be modified and shall at least include security domain network switching.

5.2.1.1.3 Attribute query

Testing and evaluation approaches and expected results of attribute query of terminal separation products are as follows:

a) Testing and evaluation approaches:

Documents provided by developers are assessed, including detailed description on attribute modification. Query operation is conducted for the security attribute and query functions of security attribute by terminal separation product users are tested, including query on one security domain network state. Testing results are recorded and it is judged whether such results are fully in accordance with the requirements for the above testing and evaluation approaches.

b) Expected results:

Terminal separation product users shall be able to make query on the security attribute, at least including query on one security domain network state.

5.2.1.1.4 Access authorization and rejection

Testing and evaluation approaches and expected results of access authorization and rejection of terminal separation products are as follows:

a) Testing and evaluation approaches:

Testing is conducted according to the detailed description on access authorization and rejection provided by developers:

1) Physical conduction and partition testing of information: where terminal separation products are in security domain A network state, they attempt to connect with security domain A network and security domain B network; products are guaranteed to be able to mutually access to security domain A network host, but not security domain B network host; where terminal separation products are in security domain B network state, they attempt to connect with security domain A network and security domain B network, the products are guaranteed to be able to mutually access to security domain B network host, but not security domain A network host;

2) Physical storage and partition testing of information: for components that may lose information after power interruption, such as memory, register and other temporary storage components, their zeroization function at network transformation are tested; for equipment that will not lose information after power interruption, such as tape drive, hard disk and other storage devices, information of security domain A network and security domain B network is separately stored in different storage devices, for example, hard disk, terminal separation products prepare one independent hard disk for security domain A network and security domain B network respectively; for such removable storage media as optical disk, floppy disk and USB hard disk, before network transformation, users are prompted to interfere or prohibit that these equipment can be used in both of the network;

3) Testing results are recorded and it is judged whether such results are fully in accordance with the requirements for the above testing and evaluation approaches.

b) Expected results:

1) Physical conduction and partition testing of information: where terminal separation products are in security domain A network state, they attempt to connect with security domain A network and security domain B network; products shall be guaranteed to be able to mutually access to security domain A network host, but not security domain B network host; where terminal separation products are in security domain B network state, they attempt to connect with security domain A network and security domain B network, the products shall be guaranteed to be able to mutually access to security domain B network host, but not security

domain A network host;

2) Physical storage and partition testing of information: for components that may lose information after power interruption, such as memory, register and other temporary storage components, their zeroization function at network transformation shall be tested; for equipment that will not lose information after power interruption, such as tape drive, hard disk and other storage devices, information of security domain A network and security domain B network shall be separately stored in different storage devices, for example, hard disk, terminal separation products shall prepare one independent hard disk for security domain A network and security domain B network respectively; for such removable storage media as optical disk, floppy disk and USB hard disk, before network transformation, users shall be prompted to interfere or prohibit that these equipment can be used in both of the network.

5.2.1.1.5 Switching signal consistency

Testing and evaluation approaches and expected results of switching signal consistency of terminal separation products are as follows:

a) Testing and evaluation approaches:

Documents provided by developers are assessed, including detailed description on switching signal consistency. Where the separated computer information resources are switched, for security function of terminal separation products, the separated computer information resources shall be switched by the same signal to ensure consistency is tested. Testing results are recorded and it is judged whether such results are fully in accordance with the requirements for the above testing and evaluation approaches.

b) Expected results:

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

5.2.1.1.6 Password protection

Testing and evaluation approaches and expected results of password protection of terminal separation products are as follows:

a) Testing and evaluation approaches:

Documents provided by developers are assessed, including detailed

description on password protection. Where the separated computer information resources are switched, the security function of terminal separation products to guarantee that users must input switching password and verify validity of password protection by guessing password is tested. Testing results are recorded and it is judged whether such results are fully in accordance with the requirements for the above testing and evaluation approaches.

b) Expected results:

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

5.2.1.1.7 Physical isolation of memory and USB port

Testing and evaluation approaches and expected results of physical isolation of memory and USB port of terminal separation products are as follows:

a) Testing and evaluation approaches:

Documents provided by developers are accessed, including detailed description on physical isolation of memory and USB port. If the terminal separation products exist in the form of complete isolation system, it is tested that the security function of terminal separation products can physically isolate the memory and all the USB ports to ensure that all the storage devices are physically isolated and thus physically guaranteeing data security. Validity of isolation is verified by observing hardware configuration information. Testing results are recorded and it is judged whether such results are fully in accordance with the requirements for the above testing and evaluation approaches.

b) Expected results:

If the terminal separation products exist in the form of complete isolation system, the security function of terminal separation products shall be able to physically isolate the memory and all the USB ports to ensure that all the storage devices are physically isolated and thus physically guaranteeing data security.

5.2.1.2 Non-bypass

Testing and evaluation approaches and expected results of non-bypass of terminal separation products are as follows:

a) Testing and evaluation approaches:

a) Testing and evaluation approaches:

Documents provided by developers are assessed; for information storage and transmission components, security attribute necessary for terminal separation products is assessed and specific contents are stated. Definition of security attribute of products is tested, testing results are recorded and it is judged whether the results are fully in accordance with the requirements for the above testing and evaluation approaches.

b) Expected results:

The products shall be able to be set with security attributes and shall at least include network switching mode in different security domains, security zones of such storage devices as optical drive and floppy drive, network equipment access type and other security attributes mentioned in documents of the developer.

5.2.2.1.2 Attribute modification

Testing and evaluation approaches and expected results of attribute modification of terminal separation products are as follows:

a) Testing and evaluation approaches:

Documents provided by developers are assessed, including detailed description on attribute modification. The security attribute is modified and functions of product modification and security-related attribute parameters are tested, including security domain network switching. Testing results are recorded and it is judged whether such results are fully in accordance with the requirements for the above testing and evaluation approaches.

b) Expected results:

For the products, parameters of security-related attribute shall be able to be modified and shall at least include security domain network switching.

5.2.2.1.3 Attribute query

Testing and evaluation approaches and expected results of attribute query of terminal separation products are as follows:

a) Testing and evaluation approaches:

Documents provided by developers are assessed, including detailed description on attribute modification. Query operation is conducted for the security attribute and query functions of security attribute by terminal

separation product users are tested, including query on one security domain network state. Testing results are recorded and it is judged whether such results are fully in accordance with the requirements for the above testing and evaluation approaches.

b) Expected results:

Terminal separation product users shall be able to make query on the security attribute, at least including query on one security domain network state.

5.2.2.1.4 Access authorization and rejection

Testing and evaluation approaches and expected results of access authorization and rejection of terminal separation products are as follows:

a) Testing and evaluation approaches:

Testing is conducted according to the detailed description on access authorization and rejection provided by developers:

1) Physical conduction and partition testing of information: where terminal separation products are in security domain A network state, they attempt to connect with security domain A network and security domain B network; products are guaranteed to be able to mutually access to security domain A network host, but not security domain B network host; where terminal separation products are in security domain B network state, they attempt to connect with security domain A network and security domain B network, the products are guaranteed to be able to mutually access to security domain B network host, but not security domain A network host;

2) Physical storage and partition testing of information: for components that may lose information after power interruption, such as memory, register and other temporary storage components, their zeroization function at network transformation are tested; for equipment that will not lose information after power interruption, such as tape drive, hard disk and other storage devices, information of security domain A network and security domain B network is separately stored in different storage devices, for example, hard disk, terminal separation products prepare one independent hard disk for security domain A network and security domain B network respectively; for such removable storage media as optical disk, floppy disk and USB hard disk, before network transformation, users are prompted to interfere or prohibit that these equipment can be used in both of the network;

3) Testing results are recorded and it is judged whether such results are fully in accordance with the requirements for the above testing and evaluation approaches.

b) Expected results:

1) Physical conduction and partition testing of information: where terminal separation products are in security domain A network state, they attempt to connect with security domain A network and security domain B network. Products shall be guaranteed to be able to mutually access to security domain A network host, but not security domain B network host; where terminal separation products are in security domain B network state, they attempt to connect with security domain A network and security domain B network, the products shall be guaranteed to be able to mutually access to security domain B network host, but not security domain A network host;

2) Physical storage and partition testing of information: for components that may lose information after power interruption, such as memory, register and other temporary storage components, zeroization shall be conducted at network transformation to prevent legacy information from tampering network; for equipment that will not lose information after power interruption, such as tape drive, hard disk and other storage devices, information of security domain A network and security domain B network shall be separately stored in different storage devices, for example, hard disk, terminal separation products shall prepare one independent hard disk for security domain A network and security domain B network respectively; for such removable storage media as optical disk, floppy disk and USB hard disk, before network transformation, users shall be prompted to interfere or prohibit that these equipment can be used in both of the network.

5.2.2.1.5 Illegal external link of network

Testing and evaluation approaches and expected results of the illegal external link of network of terminal separation products are as follows:

a) Testing and evaluation approaches:

Documents provided by developers are assessed, including detailed description on the illegal external link of network. Generation of illegal external link event is simulated, it is tested that the security function of terminal separation products can 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. Testing

results are recorded and it is judged whether such results are fully in accordance with the requirements for the above testing and evaluation approaches.

b) Expected results:

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.

5.2.2.1.6 Switching signal consistency

Testing and evaluation approaches and expected results of switching signal consistency of terminal separation products are as follows:

a) Testing and evaluation approaches:

Documents provided by developers are assessed, including detailed description on switching signal consistency. Where the separated computer information resources are switched, security function of terminal separation products to switch the separated computer information resources by the same signal is tested to ensure consistency function. Testing results are recorded and it is judged whether such results are fully in accordance with the requirements for the above testing and evaluation approaches.

b) Expected results:

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

5.2.2.1.7 Illegal replacement of hard disk

Testing and evaluation approaches and expected results of illegal replacement of hard disk of terminal separation products are as follows:

a) Testing and evaluation approaches:

It is assessed whether the documents provided by developers include detailed description on illegal replacement of hard disk. Such security function of terminal separation products that can conduct unique identification for hard disk of corresponding network at initial installation is tested to guarantee one-to-one correspondence between the hard disk and the network and ensure hard disk data security of the intranet. Hard disk of

are physically isolated and thus physically guaranteeing data security. Validity of isolation is verified by observing hardware configuration information. Testing results are recorded and it is judged whether such results are fully in accordance with the requirements for the above testing and evaluation approaches.

b) Expected results:

If the terminal separation products exist in the form of complete isolation system, the security function of terminal separation products shall be able to physically isolate the memory and all the USB ports to ensure that all the storage devices are physically isolated and thus physically guaranteeing data security.

5.2.2.2 Non-bypass

Testing and evaluation approaches and expected results of non-bypass of terminal separation products are as follows:

a) Testing and evaluation approaches:

Documents provided by developers are assessed, including detailed description on non-bypass. Before security-related operation (for example, modification of security attribute) is permitted to be conducted, the security function of the terminal separation products to ensure that they pass the inspection of security function policy is tested. Testing results are recorded and it is judged whether such results are fully in accordance with the requirements for the above testing and evaluation approaches.

b) Expected results:

Before security-related operation (for example, modification of security attribute) is permitted to be conducted, the security function of terminal separation products shall ensure that they pass the inspection of security function policy.

5.2.2.3 Object reuse

Testing and evaluation approaches and expected results of object reuse of terminal separation products are as follows:

a) Testing and evaluation approaches:

Documents provided by developers are assessed, including detailed description on object reuse. Where resource allocation is conducted for host connection of all the internal or external networks, the security function of the

the initialization methods provided by developers, it is checked whether the initialization results are consistent with those stated in the documents. Testing results are recorded and it is judged whether such results are fully in accordance with the requirements for the above testing and evaluation approaches.

b) Expected results:

Testing results shall be judged fully in accordance with the requirements of the above testing and evaluation approaches, initialization process and results of testing and checking shall meet those stated in the documents.

5.3.1.4.3 Attribute modification

Testing and evaluation approaches and expected results of attribute modification of network separation products are as follows:

a) Testing and evaluation approaches:

Testing is conducted according to the detailed description on attribute modification provided by developers:

1) It is tested that source address, destination address, transport layer protocol and requested service (such access control attributes as source port number or destination port number) as well as configured security parameters (at least including: such data as maximum authentication failure times) can be modified as an authorized administrator;

2) It is tested whether the modified setting is valid;

3) Testing results are recorded and it is judged whether such results are fully in accordance with the requirements for the above testing and evaluation approaches.

b) Expected results:

1) It is tested that source address, destination address, transport layer protocol and requested service (such access control attributes as source port number or destination port number) as well as configured security parameters (at least including: such data as maximum authentication failure times) shall be able to be modified as an authorized administrator;

2) The modified setting shall be able to be valid.

5.3.1.4.4 Attribute query

Testing and evaluation approaches and expected results of attribute query of network separation products are as follows:

a) Testing and evaluation approaches:

Documents provided by developers are assessed, including detailed description on attribute query. It is tested that source address, destination address, transport layer protocol and requested service (such access control attributes as source port number or destination port number) as well as configured security parameters (at least including: such data as maximum authentication failure times) can be queried as an authorized administrator. Testing results are recorded and it is judged whether such results are fully in accordance with the requirements for the above testing and evaluation approaches.

b) Expected results:

Source address, destination address, transport layer protocol and requested service (such access control attributes as source port number or destination port number) as well as configured security parameters (at least including: such data as maximum authentication failure times) shall be able to be queried as an authorized administrator.

5.3.1.4.5 Initialization of authentication data

Testing and evaluation approaches and expected results of initialization of authentication data of network separation products are as follows:

a) Testing and evaluation approaches:

Documents provided by developers are assessed, including detailed description on authentication mechanism of network separation products. They are logged in as an authorized administrator and an ordinary user respectively according to detailed description on authentication mechanism of network separation products provided by developers and it is tested whether this component provides initialization function of authentication data. Testing results are recorded and it is judged whether such results are fully in accordance with the requirements for the above testing and evaluation approaches.

b) Expected results:

Network separation products are logged in as an authorized administrator and an ordinary user and the products shall be provided with initialization function of authentication data.

5.3.1.4.6 Authentication time

Testing and evaluation approaches and expected results of authentication time of network separation products are as follows:

a) Testing and evaluation approaches:

Documents provided by developers are assessed, including detailed description on authentication mechanism of network separation products. Multiple authorized administrators are set and the products are logged in as these authorized administrators respectively; it is tested that, before any operation requested by all the authorized administrators, network separation products conduct identity authentication for each authorized administrator. Testing results are recorded and it is judged whether such results are fully in accordance with the requirements for the above testing and evaluation approaches.

b) Expected results:

Before any operation requested by all the authorized administrators, network separation products shall conduct identity authentication for each authorized administrator.

5.3.1.4.7 Minimum feedback

Testing and evaluation approaches and expected results of minimum feedback of network separation products are as follows:

a) Testing and evaluation approaches:

Documents provided by developers are assessed, including detailed description on authentication mechanism of network separation products. They are logged in as authorized administrator and ordinary user respectively and correct or wrong password is input; it is tested that the network separation products have the minimum feedback information. Testing results are recorded and it is judged whether such results are fully in accordance with the requirements for the above testing and evaluation approaches.

b) Expected results:

They are logged in as authorized administrator and ordinary user respectively and correct or wrong password is input; the network separation products shall have the minimum feedback information.

5.3.1.4.8 Authentication failure handling

Network separation products shall be able to accurately record such relevant operations as access, operation, modification, closure and repeated failed attempt of different modules of products by different roles of users.

5.3.1.5.2 Audit record management

Testing and evaluation approaches and expected results of audit record management of network separation products are as follows:

a) Testing and evaluation approaches:

Documents provided by developers are assessed, including evaluation on necessary relevant documents (such as: product instructions and product testing documents). Audit operation is conducted by simulating authorized administrator and security function of network separation products to permit the authorized administrator to file, delete and empty the audit records is tested. Testing results are recorded and it is judged whether such results are fully in accordance with the requirements for the above testing and evaluation approaches.

b) Expected results:

Network separation products shall be able to permit the authorized administrator to file, delete and empty the audit records.

5.3.1.5.3 Intelligible format

Testing and evaluation approaches and expected results of intelligible format of network separation products are as follows:

a) Testing and evaluation approaches:

Documents provided by developers are assessed, including evaluation on necessary relevant documents (such as: product instructions and product testing documents). Security function of network separation products is checked so that all the audit data stored in permanent audit records may be intelligible (at least including intelligible description contents and audit data itself). Testing results are recorded and it is judged whether such results are fully in accordance with the requirements for the above testing and evaluation approaches.

b) Expected results:

Network separation products shall make all the audit data stored in permanent audit records intelligible (at least including intelligible description contents and audit data itself).

5.3.1.5.4 Limitation of access to audit record

Testing and evaluation approaches and expected results of limitation of access to audit record of network separation products are as follows:

a) Testing and evaluation approaches:

It is assessed whether documents provided by developers include evaluation on necessary relevant documents (such as: product instructions and product testing documents). Audit records are accessed by simulating authorized and unauthorized administrators and security function of network separation products to only permit the authorized administrator to access to the audit records is tested. Testing results are recorded and it is judged whether such results are fully in accordance with the requirements for the above testing and evaluation approaches.

b) Expected results:

Network separation products shall only permit the authorized administrator to access to the audit records.

5.3.1.5.5 Optional retrieval of audit data

Testing and evaluation approaches and expected results of optional retrieval of audit data of network separation products are as follows:

a) Testing and evaluation approaches:

It is assessed whether documents provided by developers include evaluation on necessary relevant documents (such as: product instructions and product testing documents). It is tested whether security function of network separation products itself provides audit retrieval tool and can conduct correct searching and sorting on audit data according to logical combination of subject ID (identifier), object ID, date and time. Testing results are recorded and it is judged whether such results are fully in accordance with the requirements for the above testing and evaluation approaches.

b) Expected results:

Network separation products themselves shall provide audit retrieval tools and be able to conduct correct searching and sorting on audit data according to logical combination of subject ID (identifier), object ID, date and time.

5.3.1.5.6 Audit data loss prevention

Testing and evaluation approaches and expected results of audit data loss prevention

of network separation products are as follows:

a) Testing and evaluation approaches:

1) Testing is conducted according to relevant documents provided by developers (such as: product instructions and product testing documents):

— Such security function of network separation products that stores the generated audit record in a permanent audit record and limit the number of lost audit events due to failure and attack is tested (it is tested whether means and limitation are provided);

— Operation related to excessive consumption of audit capacity is simulated and it is tested that the network separation products send out warning message where the audit storage capacity reaches the preset warning value and guarantee to avoid other auditable behaviors beyond audit behaviors adopted by the authorized administrator;

2) For the maximum audit storage capacity causing audit data loss due to failure or storage depletion, developers of network separation products provide corresponding analysis result (it is checked whether the audit data loss is estimated);

3) Testing results are recorded and it is judged whether such results are fully in accordance with the requirements for the above testing and evaluation approaches.

b) Expected results:

1) Network separation products that shall be able to store the generated audit record in a permanent audit record and limit the number of lost audit events due to failure and attack is tested (it is tested whether means and limitation are provided);

2) Network separation products shall send out warning message where the audit storage capacity reaches the preset warning value and guarantee to avoid other auditable behaviors beyond audit behaviors adopted by the authorized administrator;

3) For the maximum audit storage capacity causing audit data loss due to failure or storage depletion, developers of network separation products shall provide corresponding analysis result and such result shall be in accordance with actual testing results.

5.3.1.6 Domain isolation

Testing and evaluation approaches and expected results of domain isolation of network separation products are as follows:

a) Testing and evaluation approaches:

1) Documents provided by developers are assessed, including evaluation on necessary relevant documents (such as: product instructions and product testing documents):

— Network separation products protect themselves from interference and tampering by untrusted subject;

— Network separation products isolate security zones of each subject within the control range;

2) Documents are checked and it is verified whether they are true;

3) Testing results are recorded and it is judged whether such results are fully in accordance with the requirements for the above testing and evaluation approaches.

b) Expected results:

1) Network separation products shall be able to protect themselves from interference and tampering by untrusted subject;

2) Network separation products shall be able to isolate security zones of each subject within the control range.

5.3.1.7 Fault tolerance

Testing and evaluation approaches and expected results of fault tolerance of network separation products are as follows:

a) Testing and evaluation approaches:

Documents provided by developers are assessed, including evaluation on necessary relevant documents (such as: product instructions and product testing documents): fault-tolerant capability of network separation products in active/standby mode is tested; where one host is abnormal due to failure of such hardware as power supply and CPU or software error, the fault tolerance function is able to automatically switch the current security service function to another standby host and continue to operate to ensure availability of the security function.

in accordance with the requirements for the above testing and evaluation approaches.

b) Expected results:

Approvals of cryptographic algorithm provided by developers shall be official and effective approvals from the SEMC.

5.3.2 Enhanced-level testing

5.3.2.1 Access control

5.3.2.1.1 Enhanced information flow control policy

Testing and evaluation approaches and expected results of enhanced information flow control policy of network separation products are as follows:

a) Testing and evaluation approaches:

1) Documents provided by developers are assessed, including detailed description on enhanced information flow control policy. Information flow supported by generation equipment is simulated, all the operations for the subject, object and those between the subject and the object of network separation products are tested, basic information flow control policy of network separation products can execute the following end-to-end enhanced information flow control policy:

— All the information flows sent and received between the subject and the object execute network layer protocol stripping and are reduced to application layer data; whether the reduced application layer data includes larger attachment accompanied with the application layer, for example, e-mail attachment larger than 20M;

— Prior to communication between the subject and the object, multi-factor identity authentication based on user name/password and digital certificate shall be conducted for the authorized user of the subject; after such authentication is passed, whether all the information flows sent and received between the subject and the object are transmitted after they are permitted by the security policy control;

2) Testing results are recorded and it is judged whether such results are fully in accordance with the requirements for the above testing and evaluation approaches.

b) Expected results:

For all the operations for the subject, object and those between the subject and the object of network separation products, basic information flow control policy of network separation products shall be able to execute the following end-to-end enhanced information flow control policy:

1) All the information flows sent and received between the subject and the object shall execute network layer protocol stripping and be reduced to application layer data; the reduced application layer data shall include larger attachment accompanied with the application layer, for example, e-mail attachment larger than 20M;

2) Prior to communication between the subject and the object, multi-factor identity authentication based on user name/password and digital certificate shall be conducted for the authorized user of the subject; after such authentication is passed, all the information flows sent and received between the subject and the object shall be transmitted after they are permitted by the security policy control.

5.3.2.1.2 Enhanced information flow control function

Testing and evaluation approaches and expected results of enhanced information flow control function of network separation products are as follows:

a) Testing and evaluation approaches:

Documents provided by developers are assessed, including detailed description on enhanced information flow control function. Information flow supported by generation equipment is simulated, it is tested whether the security function policy of network separation products may execute the following enhanced information flow control function and provide definite access assurance capability and access rejection capability. Including:

1) Network separation products may 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. or not;

2) Network separation products may conduct compliance inspection on passing information flow of such application protocols as HTTP, FTP, SMTP, POP3, SQL, RSTP and SIP;

3) Network separation products may filter the protocol signaling and parameter keywords of passing information flows of such application protocols as HTTP, FTP, SMTP, POP3, SQL, RSTP and SIP;

4) Network separation products may configure 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;

5) Network separation products may 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 on the other end, and finally write them in the database of destination host to realize database synchronization;

6) Network separation products may identify the application type of the subject, conduct information flow control via access to application control list, and prohibit access to the object by unauthorized application;

7) Network separation products may conduct physical time division switching for internal and external network data transmission link by disconnecting TCP/IP connection, i.e., internal and external network are prohibited to be connected with the special separation component on physical link at the same time.

b) Expected results:

1) Network separation products shall be able to conduct information flow control by configuring access control list. The elements of access control list shall include: source IP address, destination IP address, source port, destination port and protocol No.;

2) Network separation products shall be able to conduct compliance inspection on passing information flow of such application protocols as HTTP, FTP, SMTP, POP3, SOL, RSTP and SIP;

3) Network separation products shall be able to filter the protocol signaling and parameter keywords of the passing information flows of such application protocols as HTTP, FTP, SMTP, POP3, SOL, RSTP and SIP;

4) Network separation products shall be able to configure 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;

5) Network separation products shall be able to 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 on the other end, and finally write them in the database of destination host to realize database synchronization;

6) Network separation products shall be able to identify the application type of the subject, conduct information flow control via access to application control list, and prohibit access to the object by unauthorized application;

7) Network separation products shall be able to conduct physical time division switching for internal and external network data transmission link by disconnecting TCP/IP connection, i.e., internal and external network are prohibited to be connected with the special separation component on physical link at the same time.

5.3.2.1.3 Mandatory access control

Testing and evaluation approaches and expected results of mandatory access control of network separation products are as follows:

a) Testing and evaluation approaches:

Documents provided by developers are assessed, including designed mandatory access control model. Sensitivity labels of the subject and the object are set according to the mandatory access control model and corresponding mandatory access control rules are obtained according to the mandatory access control model. Testing results are recorded and it is judged whether such results are fully in accordance with the requirements of the above testing and evaluation approaches.

b) Expected results:

At the access to the object as the authorized subject and unauthorized subject, mandatory access control rules shall be able to take effect.

5.3.2.1.4 Residual information protection

Testing and evaluation approaches and expected results of residual information protection of network separation products are as follows:

a) Testing and evaluation approaches:

Documents provided by developers are assessed, including detailed description on residual information protection. Where resource allocation is conducted for host connection of all the internal or external networks, the security function of the network separation products that can guarantee no

2) Simulated attack equipment is adopted to, through network separation products, initiate attack flow supporting 10% bandwidth stated in the products (at least including SYN Flood and ICMP Flood etc.) and meanwhile, through network separation products, establish normal transmission services and last for 1min;

3) The passing ratio of denial of service attack packets and the ratio of successful establishment of normal business are inspected.

b) Expected results:

1) Network separation products are possessed of anti-denial service attack capability;

2) The passing ratio of attack packets is not greater than 5% and the success rate of establishment of normal business is not less than 90%.

5.3.2.3 Security management

5.3.2.3.1 Distinguishing of security management roles

Testing and evaluation approaches and expected results of distinguishing of security management roles of network separation products are as follows:

a) Testing and evaluation approaches:

Testing is conducted according to the detailed description on distinguishing of security management roles provided by developers:

1) At least two classes of user roles are provided for products, of which at least one class is administrator role and these two classes of user roles are guaranteed to be different from each other. The evaluator tests whether these two classes of user roles are different and one class belongs to administrator role;

2) An ordinary user not authorized with security management role is created and operations related to security management function are executed therewith; and network separation products reject its operation;

3) Security management role is granted for this user and operations related to security management function again are executed [shall include all the functions necessary for installation, configuration and management of the security function itself of network separation products, in which, it shall at least include: addition and deletion of subject (host sending message) and object (host receiving message), retrieval of security attributes, distribution, modification and revocation of security attributes,

retrieval and management of audit data]; it is tested whether network separation products permit its operation;

4) Testing results are recorded and it is judged whether such results are fully in accordance with the requirements for the above testing and evaluation approaches.

b) Expected results:

1) At least two classes of user roles shall be provided for products, of which at least one class shall be administrator role and these two classes of user roles shall be guaranteed to be different from each other;.

2) Network separation products shall reject the ordinary user not authorized with security management role to execute the operations related to security management function;

3) Security management role is granted for this user and operations related to security management function again are executed [shall include all the functions necessary for installation, configuration and management of the security function itself of network separation products, in which, it shall at least include: addition and deletion of subject (host sending message) and object (host receiving message), retrieval of security attributes, distribution, modification and revocation of security attributes, retrieval and management of audit data]; network separation products shall permit its operation.

5.3.2.3.2 Management function

Testing and evaluation approaches and expected results of management function of network separation products are as follows:

a) Testing and evaluation approaches:

1) Documents provided by developers are assessed, including detailed description on management function. It is logged in as an authorized administrator and it is tested that the following operations can be conducted:

— Setting and updating the security-related data;

— Installation and initialization of network separation products;

— System startup and shutdown;

— Backup and recovery of system configuration information.

2) Testing results are recorded and it is judged whether such results are fully in accordance with the requirements for the above testing and evaluation approaches.

b) Expected results:

Network separation products shall be able to execute the above operations and various backup of network separation products (such as backup of security configuration and backup of audit records) may be completed through automated tool. If network separation products support remote management of external or internal interface, they attempt to close internal and external interfaces or one of them and configure remote management address and they shall permit execution of such operations; where the host address that has never been authorized with remote management attempts to conduct remote management, network separation products shall reject it; encryption protection shall be conducted for remote management session.

5.3.2.3.3 Independent management interface

Testing and evaluation approaches and expected results of independent management interface of network separation products are as follows:

a) Testing and evaluation approaches:

Documents provided by developers are assessed, including detailed description on independent management interface. It is tested, after network separation product connects with the authorized administrator by using management interface which is independent of communication interface, and the authorized administrator passes identity authentication, whether trusted path between the authorized administrator and network separation products is established in the ways of multi-factor identity authentication and encryption, and whether other users are prohibited to access to management interface without authorization. Testing results are recorded and it is judged whether such results are fully in accordance with the requirements for the above testing and evaluation approaches.

b) Expected results:

Network separation products shall connect with the authorized administrator by using management interface which is independent of communication interface; and the authorized administrator, after passing identity authentication, shall establish the trusted path between the authorized administrator and network separation products in the ways of multi-factor identity authentication and encryption and other users shall be prohibited to access to management interface without authorization.

5.3.2.4 Identification and authentication

5.3.2.4.1 Sensitivity label

Testing and evaluation approaches and expected results of sensitivity label of network separation products are as follows:

a) Testing and evaluation approaches:

Documents provided by developers are assessed, including detailed description on documents related to label. Sensitivity label is set for the subject and the object according to documents provided by developers. Testing results are recorded and it is judged whether such results are fully in accordance with the requirements for the above testing and evaluation approaches.

b) Expected results:

Products shall support sensitivity label for the subject and the object.

5.3.2.4.2 Definition of basic security attribute

Testing and evaluation approaches and expected results of definition of basic security attribute of network separation products are as follows:

a) Testing and evaluation approaches:

Documents provided by developers are assessed, including data transmission and control component and application layer data acquisition and receiving component consisting system for each authorized administrator, for which network separation products provide a set of unique security attribute necessary for the execution of security function policy; and specific contents are stated. It is tested whether the products are set with these security attributes, at least including security attributes of authorized administrator, data transmission and control component consisting system, application layer data acquisition and receiving component and other security attributes mentioned in documents of developers. If the products are set with security attribute within specified range and security attributes existing in documents of developers, such judgment shall be deemed as acceptable. Testing results are recorded and it is judged whether such results are fully in accordance with the requirements of the above testing and evaluation approaches.

b) Expected results:

For each authorized administrator, network separation products shall have

a) Testing and evaluation approaches:

Documents provided by developers are assessed, including detailed description on attribute initialization. Initialization is conducted according to the initialization methods provided by developers, it is checked whether the initialization results are consistent with those stated in the documents. Testing results are recorded and it is judged whether such results are fully in accordance with the requirements for the above testing and evaluation approaches.

b) Expected results:

Testing results shall be judged fully in accordance with the requirements of the above testing and evaluation approaches, initialization process and results of testing and checking shall meet those stated in the documents.

5.3.2.4.5 Attribute modification

Testing and evaluation approaches and expected results of attribute modification of network separation products are as follows:

a) Testing and evaluation approaches:

1) It is tested that source address, destination address, transport layer protocol and requested service (such access control attributes as source port number or destination port number) as well as configured security parameters (at least including: such data as maximum authentication failure times) can be modified;

2) It is tested whether the modified setting is valid;

3) Testing results are recorded and it is judged whether such results are fully in accordance with the requirements for the above testing and evaluation approaches.

b) Expected results:

1) Source address, destination address, transport layer protocol and requested service (such access control attributes as source port number or destination port number) as well as configured security parameters (at least including: such data as maximum authentication failure times) shall be able to be modified as an authorized administrator;

2) The modified setting shall be able to be valid.

5.3.2.4.6 Attribute query

Testing and evaluation approaches and expected results of attribute query of network separation products are as follows:

a) Testing and evaluation approaches:

Documents provided by developers are assessed, including detailed description on attribute query. It is tested that source address, destination address, transport layer protocol and requested service (such access control attributes as source port number or destination port number) as well as configured security parameters (at least including: such data as maximum authentication failure times) can be modified as an authorized administrator. Testing results are recorded and it is judged whether such results are fully in accordance with the requirements for the above testing and evaluation approaches.

b) Expected results:

Source address, destination address, transport layer protocol and requested service (such access control attributes as source port number or destination port number) as well as configured security parameters (at least including: such data as maximum authentication failure times) shall be able to be queried as an authorized administrator.

5.3.2.4.7 Initialization of authentication data

Testing and evaluation approaches and expected results of initialization of authentication data of network separation products are as follows:

a) Testing and evaluation approaches:

Documents provided by developers are assessed, including detailed description on authentication mechanism of network separation products. They are logged in as an authorized administrator and an ordinary user respectively according to detailed description on authentication mechanism of network separation products provided by developers and it is tested whether this component provides initialization function of authentication data. Testing results are recorded and it is judged whether such results are fully in accordance with the requirements for the above testing and evaluation approaches.

b) Expected results:

Network separation products are logged in as an authorized administrator and an ordinary user and the products shall be provided with initialization function of authentication data.

5.3.2.4.8 Authentication time

Testing and evaluation approaches and expected results authentication time of network separation products are as follows:

a) Testing and evaluation approaches:

Documents provided by developers are assessed, including detailed description on authentication mechanism of network separation products. Multiple authorized administrators are set and the products are logged in as these authorized administrators respectively; it is tested that, before any operation requested by all the authorized administrators, network separation products conduct identity authentication for each authorized administrator. Testing results are recorded and it is judged whether such results are fully in accordance with the requirements for the above testing and evaluation approaches.

b) Expected results:

Before any operation requested by all the authorized administrators, network separation products shall conduct identity authentication for each authorized administrator.

5.3.2.4.9 Minimum feedback

Testing and evaluation approaches and expected results of minimum feedback of network separation products are as follows:

a) Testing and evaluation approaches:

Documents provided by developers are assessed, including detailed description on authentication mechanism of network separation products. They are logged in as authorized administrator and ordinary user respectively and correct or wrong password is input; it is tested that the network separation products have the minimum feedback information. Testing results are recorded and it is judged whether such results are fully in accordance with the requirements for the above testing and evaluation approaches.

b) Expected results:

They are logged in as authorized administrator and ordinary user respectively and correct or wrong password is input; the network separation products shall have the minimum feedback information.

5.3.2.4.10 Multi-authentication mechanism

Testing and evaluation approaches and expected results of multi-authentication mechanism of network separation products are as follows:

a) Testing and evaluation approaches:

Documents provided by developers are assessed, including detailed description on authentication mechanism of network separation products. They are logged in as an authorized administrator and an ordinary user respectively according to detailed description on authentication mechanism of network separation products provided by developers and it is verified whether multi-authentication mechanism function is provided. Testing results are recorded and it is judged whether such results are fully in accordance with the requirements for the above testing and evaluation approaches.

b) Expected results:

Network separation products shall be provided with multi-authentication mechanism.

5.3.2.4.11 Authentication failure handling

Testing and evaluation approaches and expected results of authentication failure handling of network separation products are as follows:

a) Testing and evaluation approaches:

Documents provided by developers are assessed, including detailed description on authentication mechanism of network separation products. They are logged in wrong user name - password; after certain times of authentication failures, it is tested that the network separation products terminate the process to attempt to log in the host and establish sessions. They are logged in as authorized administrator and ordinary user respectively and setting function of maximum failure times provided by this component is tested and such maximum failure times are only set by the authorized administrator. Testing results are recorded and it is judged whether such results are fully in accordance with the requirements for the above testing and evaluation approaches.

b) Expected results:

They are logged in wrong user name - password. After certain times of authentication failures, the network separation products shall be able to terminate the process to attempt to log in the host and establish sessions. They are logged in as authorized administrator and ordinary user respectively and the products shall provide setting function of maximum failure times and such maximum failure times shall be only set by the

and un-inferable way.

5.3.2.4.14 Password strength

Testing and evaluation approaches and expected results of password strength of network separation products are as follows:

a) Testing and evaluation approaches:

Documents provided by developers are assessed, including detailed description on password strength of network separation products. It is tested that the network separation products adopt password verification mechanism for inspection on password complexity generated by the authorized administrator and whether the password strength guarantees that the password length is greater than 6 bits and the password type is a combination of numbers + capital and small letters. Moreover, effectiveness of measures is verified by simulating the password to login. Testing results are recorded and it is judged whether such results are fully in accordance with the requirements for the above testing and evaluation approaches.

b) Expected results:

Network separation products shall adopt password verification mechanism for inspection on password complexity generated by the authorized administrator, the password strength shall guarantee that the password length is greater than 6 bits and the password type shall be a combination of numbers + capital and small letters.

5.3.2.5 Audit

5.3.2.5.1 Generation of audit data

Testing and evaluation approaches and expected results of generation of audit data of network separation products are as follows:

a) Testing and evaluation approaches:

Documents provided by developers are assessed, including evaluation on necessary relevant document (such as: product instructions and product testing documents). According to documents of developers, different roles of users are used to simulate such relevant operations as access, operation, modification, closure and repeated failed attempt of different modules. Correctness of audit records is checked. Testing results are recorded and it is judged whether such results are fully in accordance with the requirements for the above testing and evaluation approaches.

b) Expected results:

Network separation products shall be able to accurately record such relevant operations as access, operation, modification, closure and repeated failed attempt of different modules of products by different roles of users.

5.3.2.5.2 Security audit analysis

Testing and evaluation approaches and expected results of security audit analysis of network separation products are as follows:

a) Testing and evaluation approaches:

1) Documents provided by developers are assessed, including detailed description on security audit analysis of network separation products. It is tested whether security audit analysis covers:

— Classification statistics on the application used during operation on the object by the subject covered by network separation product rules (hosts on internal or external network);

— Statistics on application flow and the flow of each application type by network separation products;

— Statistics on occupancy rate of CPU, memory and disc by network separation products;

— Statistics on online user list and online user duration.

2) Testing results are recorded and it is judged whether such results are fully in accordance with the requirements for the above testing and evaluation approaches.

b) Expected results:

1) Classification statistics shall be conducted on the application used during operation on the object by the subject covered by network separation product rules (hosts on internal or external network);

2) Network separation products shall conduct statistics on total application flow and the flow of each application type;

3) Network separation products shall conduct statistics on occupancy rate of CPU, memory and disc.

4) Statistics on online user list and online user duration shall be provided.

5.3.2.5.3 User identity association

Testing and evaluation approaches and expected results of user identity association of network separation products are as follows:

a) Testing and evaluation approaches:

Documents provided by developers are assessed, including evaluation on necessary relevant documents (such as: product instructions and product testing documents). Different roles of users are used to execute all the operations related to product function and it is tested that the security function of network separation product can associate each auditable event with the user identity causing such event. Testing results are recorded and it is judged whether such results are fully in accordance with the requirements for the above testing and evaluation approaches.

b) Expected results:

Network separation products shall be able to associate each auditable event with the user identity causing such event.

5.3.2.5.4 Audit record management

Testing and evaluation approaches and expected results of audit record management of network separation products are as follows:

a) Testing and evaluation approaches:

Documents provided by developers are assessed, including evaluation on necessary relevant documents (such as: product instructions and product testing documents). Audit operation is conducted by simulating authorized administrator and security function of network separation products to permit the authorized administrator to file, delete and empty the audit records is tested. Testing results are recorded and it is judged whether such results are fully in accordance with the requirements for the above testing and evaluation approaches.

b) Expected results:

Network separation products shall be able to permit the authorized administrator to file, delete and empty the audit records.

5.3.2.5.5 Intelligible format

Testing and evaluation approaches and expected results of intelligible format of network separation products are as follows:

a) Testing and evaluation approaches:

Documents provided by developers are assessed, including evaluation on necessary relevant documents (such as: product instructions and product testing documents). Security function of network separation products is checked so that all the audit data stored in permanent audit records may be intelligible (at least including intelligible description contents and audit data itself). Testing results are recorded and it is judged whether such results are fully in accordance with the requirements for the above testing and evaluation approaches.

b) Expected results:

Network separation products shall make all the audit data stored in permanent audit records intelligible (at least including intelligible description contents and audit data itself).

5.3.2.5.6 Limitation of access to audit record

Testing and evaluation approaches and expected results of basic limitation of access to audit record of network separation products are as follows:

a) Testing and evaluation approaches:

Documents provided by developers are assessed, including evaluation on necessary relevant documents (such as: product instructions and product testing documents). Audit records are accessed by simulating authorized and unauthorized administrators and security function of network separation products to only permit the authorized administrator to access to the audit records is tested. Testing results are recorded and it is judged whether such results are fully in accordance with the requirements for the above testing and evaluation approaches.

b) Expected results:

Network separation products shall only permit the authorized administrator to access to the audit records.

5.3.2.5.7 Optional retrieval of audit data

Testing and evaluation approaches and expected results of optional retrieval of audit data of network separation products are as follows:

a) Testing and evaluation approaches:

Documents provided by developers are assessed, including evaluation on

b) Expected results:

1) Network separation products that shall be able to store the generated audit record in a permanent audit record and limit the number of lost audit events due to failure and attack is tested (it is tested whether means and limitation are provided);

2) Network separation products shall send out warning message where the audit storage capacity reaches the preset warning value and guarantee to avoid other auditable behaviors beyond audit behaviors adopted by the authorized administrator;

3) For the maximum audit storage capacity causing audit data loss due to failure or storage depletion, developers of network separation products shall provide corresponding analysis result and such result shall be in accordance with actual testing results.

5.3.2.6 Domain isolation

5.3.2.6.1 Basic domain isolation

Testing and evaluation approaches and expected results of basic domain isolation of network separation products are as follows:

a) Testing and evaluation approaches:

1) Documents provided by developers are assessed, including evaluation on necessary relevant documents (such as: product instructions and product testing documents);

— Network separation products protect themselves from interference and tampering by untrusted subject;

— Network separation products isolate security zones of each subject within the control range.

2) Documents are checked and it is verified whether they are true;

3) Testing results are recorded and it is judged whether such results are fully in accordance with the requirements for the above testing and evaluation approaches.

b) Expected results:

1) Network separation products shall be able to protect themselves from interference and tampering by untrusted subject;

2) Network separation products shall be able to isolate security zones of each subject within the control range.

5.3.2.6.2 Enhanced domain isolation

Testing and evaluation approaches and expected results of enhanced domain isolation of network separation products are as follows:

a) Testing and evaluation approaches:

Documents provided by developers are assessed, including evaluation on necessary relevant documents (such as: product instructions and product testing documents). It is tested that the security function of network separation products is marked as high security level by its own security zone, the authorized administrator and all the subjects covered by the network separation products (host on the internal or external network), after being authorized, it can only read documents and programs stored in this zone, but can't delete or modify them, whether mandatory access control policy may be adopted and the authorized administrator may modify the access policy. Testing results are recorded and it is judged whether such results are fully in accordance with the requirements for the above testing and evaluation approaches.

b) Expected results:

The security function of network separation products shall be marked as high security level by its own security zone, the authorized administrator and all the subjects covered by the network separation products (host on the internal or external network), after being authorized, can only read documents and programs stored in this zone, but can't delete or modify them, mandatory access control policy shall be able to be adopted and the authorized administrator can't modify the access policy.

5.3.2.7 Fault tolerance

5.3.2.7.1 Basic fault tolerance

Testing and evaluation approaches and expected results of basic fault tolerance of network separation products are as follows:

a) Testing and evaluation approaches:

Documents provided by developers are assessed, including evaluation on necessary relevant documents (such as: product instructions and product testing documents). Fault-tolerant capability of network separation products in active/standby mode is tested; where one host is abnormal due to failure of

such hardware as power supply and CPU or software error, the fault tolerance function is able to automatically switch the current security service function to another standby host and continue to operate to ensure availability of the security function. Testing results are recorded and it is judged whether such results are fully in accordance with the requirements for the above testing and evaluation approaches.

b) Expected results:

Network separation products shall be possessed of the fault-tolerant capability in active/standby mode. Where one host is abnormal due to failure of such hardware as power supply and CPU or software error, the fault tolerance function shall be able to automatically switch the current security service function to another standby host and continue to operate to ensure availability of the security function.

5.3.2.7.2 Enhanced fault tolerance

Testing and evaluation approaches and expected results of enhanced fault tolerance of network separation products are as follows:

a) Testing and evaluation approaches:

Documents provided by developers are assessed, including evaluation on necessary relevant documents (such as: product instructions and product testing documents). Fault-tolerant capability of network separation products in active/standby mode is tested; where two hosts provide security service function for the internal and external network simultaneously and one host is abnormal due to failure of such hardware as power supply and CPU or software error, the other host shall be able to continue to provide security service function to ensure availability of the security function. Testing results are recorded and it is judged whether such results are fully in accordance with the requirements for the above testing and evaluation approaches.

b) Expected results:

Network separation products shall be possessed of fault-tolerant capability in active/active mode; where two hosts provide security service function for the internal and external network simultaneously and one host is abnormal due to failure of such hardware as power supply and CPU or software error, the other host shall be able to continue to provide security service function to ensure availability of the security function.

5.3.2.8 Data integrity

Testing and evaluation approaches and expected results of data integrity of network

successful establishment of normal business are inspected.

b) Expected results:

1) Network unilateral transmission products are possessed of anti-denial service attack capability;

2) The passing ratio of attack packets is not greater than 5% and the success rate of establishment of normal business is not less than 90%.

5.4.1.3 Security management

5.4.1.3.1 Distinguishing of security management roles

Testing and evaluation approaches and expected results of distinguishing of security management roles of network unilateral transmission products are as follows:

a) Testing and evaluation approaches:

Documents provided by developers are assessed, including detailed description on distinguishing of security management roles. It is tested whether the security function of network unilateral transmission products includes:

1) They are able to distinguish the security-related management function from other functions;

2) All the functions necessary for installation, configuration and management of the security function of network unilateral transmission products, including: addition and deletion of subject (host sending message) and object (host receiving message), retrieval of security attributes, distribution, modification and revocation of security attributes, retrieval and management of audit data;

3) They limit the capability to execute security-related management function as a kind of security management responsibility, which has a set of specially authorized responsibilities about function and response;

4) They are able to separate the authorized administrator in charge of executing management function from all other individuals or systems that use the separation component;

5) They only permit the authorized administrator to undertake the security management responsibility;

6) They permit the authorized administrator to undertake security

products, among which the backup capability is supported by automated tools;

— Setting such availability parameters of separation component as dual-machine hot standby;

— They are able to limit address that may be subject to remote management and protect remote management session via encryption, if remote management is supported.

2) Testing results are recorded and it is judged whether such results are fully in accordance with the requirements for the above testing and evaluation approaches.

b) Expected results:

Network unilateral transmission products shall be able to provide the authorized administrator with the following management functions:

1) Setting and updating the security-related data;

2) Executing the initialization, system startup and shutdown, and backup and recovery functions of network unilateral transmission products, among which the backup capability shall be supported by automated tools;

3) Setting such availability parameters of separation component as dual-machine hot standby;

4) If remote management is supported, they shall be able to:

— Limit the address that may be subject to remote management;

— Protect remote management session via encryption.

5.4.1.3.3 Independent management interface

Testing and evaluation approaches and expected results of basic independent management interface of network unilateral transmission products are as follows:

a) Testing and evaluation approaches:

Documents provided by developers are assessed, including detailed description on independent management interface. It is tested, after network unilateral transmission products connect with the authorized administrator by using management interface which is independent of communication interface, and the authorized administrator passes identity authentication,

whether trusted path between the authorized administrator and network separation products is established in the ways of multi-factor identity authentication and encryption, and whether other users are prohibited to access to management interface without authorization. Testing results are recorded and it is judged whether such results are fully in accordance with the requirements for the above testing and evaluation approaches.

b) Expected results:

Network unilateral transmission products shall connect with the authorized administrator by using management interface which is independent of communication interface; and the authorized administrator, after passing identity authentication, establishes the trusted path between the authorized administrator and network separation products in the ways of multi-factor identity authentication and encryption and other users are prohibited to access to management interface without authorization.

5.4.1.4 Identification and authentication

5.4.1.4.1 Definition of security attribute

Testing and evaluation approaches and expected results of definition of security attribute of network unilateral transmission products are as follows:

a) Testing and evaluation approaches:

1) Documents provided by developers are assessed, including detailed description on definition of security attribute. It is tested that, for each authorized administrator, the security function of network unilateral transmission products is a set of unique and necessary security attributes provided for execution of security function policy, including but not limited to:

— Equipment network parameters: including interface address and gateway address etc.;

— Equipment interface attributes: interface types (such as: management interface and communication interface) and interface rate etc.;

— Security management parameters: management console address and management modes (such as: SSH and SSL) etc.;

— Security parameters: maximum authentication failure times and management idle timeout;

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

— System parameters: size of log memory space and equipment name etc.;

— User role attributes: authorized administrator, authorized auditor and authorized user etc.;

— User management attributes: user name, user role and user password etc.

2) Testing results are recorded and it is judged whether such results are fully in accordance with the requirements for the above testing and evaluation approaches.

b) Expected results:

For each authorized administrator, the security function of network unilateral transmission products shall provide it with a set of unique and necessary security attributes provided for execution of the security function policy, including but not limited to:

1) Equipment network parameters: including interface address and gateway address etc.;

2) Equipment interface attributes: interface types (such as: management interface and communication interface) and interface rate etc.;

3) Security management parameters: management console address and management modes (such as: SSH and SSL) etc.;

4) Security parameters: maximum authentication failure times and management idle timeout;

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

6) System parameters: size of log memory space and equipment name etc.;

7) User role attributes: authorized administrator, authorized auditor and authorized user etc.;

8) User management attributes: user name, user role and user password

etc.

5.4.1.4.2 Attribute initialization

Testing and evaluation approaches and expected results of attribute initialization of network unilateral transmission products are as follows:

a) Testing and evaluation approaches:

Documents provided by developers are assessed, including detailed description on attribute initialization. The function that conducts initialization for the authorized administrator and host attributes by default values provided by the security function of the network unilateral transmission products is tested. Testing results are recorded and it is judged that whether such results are fully in accordance with the requirements for the above testing and evaluation approaches.

b) Expected results:

The security function of network unilateral transmission products shall be able to provide the function of initializing the authorized administrator and host attributes by default values.

5.4.1.4.3 Attribute modification

Testing and evaluation approaches and expected results of attribute modification of network unilateral transmission products are as follows:

a) Testing and evaluation approaches:

Documents provided by developers are assessed, including detailed description on attribute modification. The function of modifying the following (including but not limited to) parameters provided by the security function of the network unilateral transmission products only for the authorized administrator is tested:

1) Relationship between identification and role (for example, configuration administrator);'

2) Security attribute values of subject (data acquirer) and object (data receiver);

3) Configured security parameters (such data as maximum authentication failure times);

4) Testing results are recorded and it is judged whether such results are

2) Security attribute values of subject (data acquirer) and object (data receiver);

3) Configured security parameters.

5.4.1.4.5 Initialization of authentication data

Testing and evaluation approaches and expected results of initialization of authentication data of network unilateral transmission products are as follows:

a) Testing and evaluation approaches:

Documents provided by developers are assessed, including detailed description on initialization of authentication data. The function of initialization of the authentication data provided according to specified authentication mechanism by the network unilateral transmission products for the authorized administrator is tested and they ensure to only permit the authorized administrator to use such function. Testing results are recorded and it is judged that whether such results are fully in accordance with the requirements for the above testing and evaluation approaches.

b) Expected results:

Network unilateral transmission products shall provide the authorized administrator with the function of initialization of authentication data according to the specified authentication mechanism and shall ensure that only permit the authorized administrator can use such function.

5.4.1.4.6 Authentication time

Testing and evaluation approaches and expected results of authentication time of network unilateral transmission products are as follows:

a) Testing and evaluation approaches:

Documents provided by developers are assessed, including detailed description on authentication time. It is tested that, before any operation requested by all the authorized administrators, the network unilateral transmission products ensures to conduct identity authentication for each authorized administrator. Testing results are recorded and it is judged whether such results are fully in accordance with the requirements for the above testing and evaluation approaches.

b) Expected results:

Before any operation requested by all the authorized administrators, network

unilateral transmission products shall ensure to conduct identity authentication for each authorized administrator.

5.4.1.4.7 Minimum feedback

Testing and evaluation approaches and expected results of minimum feedback of network unilateral transmission products are as follows:

a) Testing and evaluation approaches:

Documents provided by developers are assessed, including detailed description on minimum feedback. Where the network unilateral transmission products conduct identification, the security function that only provides the minimum feedback for users is tested. Testing results are recorded and it is judged that whether such results are fully in accordance with the requirements for the above testing and evaluation approaches.

b) Expected results:

Where the network unilateral transmission products conduct identification, the security function shall only provides the minimum feedback for users.

5.4.1.4.8 Authentication failure handling

Testing and evaluation approaches and expected results of authentication failure handling of network unilateral transmission products are as follows:

a) Testing and evaluation approaches:

Documents provided by developers are assessed, including detailed description on authentication failure handling. They are logged in wrong user name - password; after certain times of authentication failures, it is tested that the network unilateral transmission products terminate the process to attempt to log in the host and establish sessions. They are logged in as authorized administrator and ordinary user respectively and setting function of maximum failure times provided by this component is tested and such maximum failure times are only set by the authorized administrator. Testing results are recorded and it is judged whether such results are fully in accordance with the requirements for the above testing and evaluation approaches.

b) Expected results:

Developers shall provide relevant documents, whose contents shall conform to actual conditions. Actual conditions of the maximum failure times shall conform to the setting value. The maximum failure times, or default value of permissible maximum failure times that can be set and other measures for

preventing brute-force guessing of password shall be able to be set.

5.4.1.4.9 Timeout re-authentication

Testing and evaluation approaches and expected results of timeout re-authentication of network unilateral transmission products are as follows:

a) Testing and evaluation approaches:

Documents provided by developers are assessed, including detailed description on timeout re-authentication. Login timeout of products are set according to those stated in the documents provided; if without any operation within the set period, sessions are terminated and the products can be re-operated only after identity authentication again. Whether the maximum timeout may only be set by the authorized administrator is tested. Testing results are recorded and it is judged whether such results are fully in accordance with the requirements for the above testing and evaluation approaches.

b) Expected results:

Developers shall provide relevant documents, whose contents shall conform to actual conditions. If without any operation within the set period, sessions shall be terminated and the products can be re-operated only after identity authentication again. The maximum timeout only may be set by the authorized administrator.

5.4.1.4.10 Anti-replay

Testing and evaluation approaches and expected results of anti-replay of network unilateral transmission products are as follows:

a) Testing and evaluation approaches:

Documents provided by developers are assessed, including detailed description on anti-replay. It is tested whether the authentication mechanism of network unilateral transmission products is possessed of anti-replay capability, and whether the authorized administrator and other users can't pass the identification again by copying authentication information of last time. Testing results are recorded and it is judged whether such results are fully in accordance with the requirements for the above testing and evaluation approaches.

b) Expected results:

The authentication mechanism of network unilateral transmission products

shall be possessed of anti-replay capability so that the authorized administrator and other users cannot pass the authentication again by copying the authentication information last time.

5.4.1.4.1 1 Protected authentication feedback

Testing and evaluation approaches and expected results of protected authentication feedback of network unilateral transmission products are as follows:

a) Testing and evaluation approaches:

Documents provided by developers are assessed, including detailed description on protected authentication feedback. It is tested that such sensitive information as password input by the authorized administrator of network unilateral transmission products in the process of identification is displayed in login input interface of authentication information in an invisible and un-inferable way. Testing results are recorded and it is judged whether such results are fully in accordance with the requirements for the above testing and evaluation approaches.

b) Expected results:

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

5.4.1.5 Audit

5.4.1.5.1 Generation of audit data

Testing and evaluation approaches and expected results of generation of audit data of network unilateral transmission products are as follows:

a) Testing and evaluation approaches:

1) Documents provided by developers are assessed, including detailed description on generation of audit data. The security function of network unilateral transmission products that can generate audit records for the following auditable events is tested:

— Starting and closing of audit function;

— Any attempt of operation for audit record, including closing audit function or subsystem, and the identification of affected object;

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

— All the requests to use the authentication data management mechanism in security function;

— All the requests to access to authentication data, and the objective of access request;

— Any use of authentication mechanism;

— All the attempts to use identification mechanism;

— All the modifications (setting and update) to the configuration parameter of security function, whatever success or not, and the new value of configuration parameter.

2) For each audit record whether the security function shall at least record the following information: generation date and time of event, type of event, subject identity and successful or failed event;

5.4.1.5.2 User identity association

Testing and evaluation approaches and expected results of user identity association of network unilateral transmission products are as follows:

a) Testing and evaluation approaches:

Documents provided by developers are assessed, including evaluation on user identity association. Different roles of users are used to execute all the operations related to product function and it is tested whether the security function of network unilateral transmission products can associate each auditable event with the user identity causing such event. Testing results are recorded and it is judged whether such results are fully in accordance with the requirements for the above testing and evaluation approaches.

b) Expected results:

Products are able to associate each auditable event with the user identity causing such event.

5.4.1.5.3 Audit record management

Testing and evaluation approaches and expected results of audit record management of network unilateral transmission products are as follows:

a) Testing and evaluation approaches:

Documents provided by are assessed, including detailed description on audit record management. The authorized administrator is used to conduct audit operation and the security function of network unilateral transmission products to permit the authorized administrator to file, delete and empty the audit records is tested. Testing results are recorded and it is judged that whether such results are fully in accordance with the requirements for the above testing and evaluation approaches.

b) Expected results:

Network unilateral transmission products shall permit the authorized administrator to file, delete and empty the audit records.

5.4.1.5.4 Intelligible format

Testing and evaluation approaches and expected results of intelligible format of network unilateral transmission products are as follows:

a) Testing and evaluation approaches:

Documents provided by developers are assessed, including detailed description on intelligible format. It is checked whether the security function of network unilateral transmission products can make all the audit data stored in permanent audit records intelligible (at least including intelligible description contents and audit data itself). Testing results are recorded and it is judged whether such results are fully in accordance with the requirements for the above testing and evaluation approaches.

b) Expected results:

The security function of network unilateral transmission products shall make all the audit data stored in permanent audit records intelligible.

5.4.1.5.5 Limitation of access to audit record

Testing and evaluation approaches and expected results of limitation of access to audit record of network unilateral transmission products are as follows:

a) Testing and evaluation approaches:

Documents provided by developers are assessed, including detailed description on limitation of access to audit record. Audit records are accessed by simulating authorized and unauthorized administrators and security function of network unilateral transmission products to only permit the authorized administrator to access to audit records is tested. Testing results are recorded and it is judged whether such results are fully in

accordance with the requirements for the above testing and evaluation approaches.

b) Expected results:

The security function of network unilateral transmission products shall only permit the authorized administrator to access to the audit records.

5.4.1.5.6 Optional retrieval of audit data

Testing and evaluation approaches and expected results of optional retrieval of audit data of network unilateral transmission products are as follows:

a) Testing and evaluation approaches:

Documents provided by developers are assessed, including detailed description on optional retrieval of audit data. It is tested that the network unilateral transmission products themselves provide audit retrieval tool; the audit retrieval tool can conduct correct searching and sorting on audit data according to logical combination of subject ID (identifier), object ID, date and time. Testing results are recorded and it is judged whether such results are fully in accordance with the requirements for the above testing and evaluation approaches.

b) Expected results:

The security function of network unilateral transmission products shall provide such audit retrieval tool that can conduct searching and sequencing for the audit data according to such parameters as subject ID (identifier), object ID, date and time as well as logical combination of these parameters.

5.4.1.5.7 Audit data loss prevention

Testing and evaluation approaches and expected results of audit data loss prevention of network unilateral transmission products are as follows:

a) Testing and evaluation approaches:

1) It is tested that the security function of unilateral transmission equipment that can store the generated audit records in a permanent audit record and limit number of lost audit events due to failure and attack (it is tested whether means and limitation are provided);

2) Operation related to excessive consumption of audit capacity is simulated and it is tested that the unilateral transmission equipment sends out warning message where the audit storage capacity reaches

the preset warning value and guarantees to avoid other auditable behaviors beyond audit behaviors adopted by the authorized administrator;

3) Testing results are recorded and it is judged whether such results are fully in accordance with the requirements for the above testing and evaluation approaches.

b) Expected results:

Developers shall provide relevant documents, whose contents shall conform to actual conditions. The security function of network unilateral transmission products shall store the generated audit records in a permanent audit record and limit the number of lost audit events due to failure and attack; for the maximum audit storage capacity of audit data loss due to failure or storage depletion, the developers of network unilateral transmission products shall provide corresponding analysis results.

5.4.1.6 Domain isolation

Testing and evaluation approaches and expected results of domain isolation of network unilateral transmission products are as follows:

a) Testing and evaluation approaches:

Documents provided by developers are assessed, including detailed description on basic domain isolation. In order to protect security function of network unilateral transmission products against interference and tampering by untrusted subject (host on internal or external network), the security function of network unilateral transmission products may set a security zone for its execution environment and separate the security zones of all the subjects (host on internal or external network) within the control range of network unilateral transmission products. Testing results are recorded and it is judged whether such results are fully in accordance with the requirements for the above testing and evaluation approaches.

b) Expected results:

In order to protect the security function of network unilateral transmission products against interference and tampering by untrusted subject (host on internal or external network), the security function of network unilateral transmission products shall set a security zone for its execution environment and separate the security zones of all subjects (host on internal or external network) within the control range of network unilateral transmission products.

5.4.1.7 Configuration data protection

5.4.2.1.1 Information flow control policy

Testing and evaluation approaches and expected results of information flow control policy of network unilateral transmission products are as follows:

a) Testing and evaluation approaches:

1) Documents provided by developers are assessed, including detailed description on basic information flow control policy. It is tested whether the network unilateral transmission products are provided with the following information flow control policy:

— Network unilateral transmission products are able to strip the network information flow of data sender, and unilaterally transmit it to the network destination host of information receiver after reducing it to raw data;

— Network unilateral transmission products may actively access to the source host according to security attribute value of unilateral synchronization task and read data after they pass the identity authentication; after they unilaterally transmit the data to receiving terminal, they may complete identity authentication for connection of destination host and write the data in the destination host;

— Network unilateral transmission products are able to be built with information flow receiving service and unilaterally transmit it to the network destination host of the information receiver after converting it to raw data.

2) Testing results are recorded and it is judged whether such results are fully in accordance with the requirements for the above testing and evaluation approaches.

b) Expected results:

1) Network unilateral transmission products shall be able to strip the network information flow of data sender, and unilaterally transmit it to the network destination host of information receiver after reducing it to raw data;

2) Network unilateral transmission products shall be able to actively access to the source host according to security attribute value of unilateral synchronization task and read data after they pass the identity authentication; after they unilaterally transmit the data to receiving terminal, they complete identity authentication for connection of destination host and write the data in the destination host;

3) Network unilateral transmission products shall be able to be built with information flow receiving service and unilaterally transmit it to the network destination host of the information receiver after converting it to raw data.

5.4.2.1.2 Basic information flow control function

Testing and evaluation approaches and expected results of basic information flow control function of network unilateral transmission products are as follows:

a) Testing and evaluation approaches:

Documents provided by developers are assessed, including detailed description on basic information flow control function. The security function policy of network unilateral transmission products that may execute the following basic information flow control function and provide definite access assurance capability and access rejection capability is tested. Including:

1) Network unilateral transmission products may realize unilateral transmission from clear source data to target data by configuring the security attribute value of unilateral synchronization task. By default, network unilateral transmission products reject the unilateral transmission of any data;

2) 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;

3) Network unilateral transmission products are able to conduct virus scanning for data content of unilateral transmission to cut off the transmission of data containing virus;

4) Network unilateral transmission products are able to conduct keyword inspection on data content of unilateral transmission to cut off the transmission of illegal data;

5) Network unilateral transmission products are able to conduct identity authentication for the subject sending and receiving data flow to avoid access to illegal data;

6) Network unilateral transmission products are able to support such service types as document unilateral transmission and database unilateral transmission.

b) Testing results are recorded and it is judged whether such results are fully in accordance with the requirements for the above testing and evaluation

approaches.

c) Expected results:

1) Network unilateral transmission products shall be able to realize unilateral transmission from clear source data to target data by configuring the security attribute value of unilateral synchronization task. By default, for the configuration of unilateral synchronization task, network unilateral transmission products reject the unilateral transmission of any data;

2) They shall 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;

3) Network unilateral transmission products shall be able to conduct virus scanning for data content of unilateral transmission to cut off the transmission of data containing virus;

4) Network unilateral transmission products shall be able to conduct keyword inspection on data content of unilateral transmission to cut off the transmission of illegal data;

5) Network unilateral transmission products shall be able to conduct identity authentication for the subject sending and receiving data flow to avoid access to illegal data;

6) Network unilateral transmission products shall be able to support such service types as document unilateral transmission and database unilateral transmission.

5.4.2.1.3 Enhanced information flow control function

Testing and evaluation approaches and expected results of enhanced information flow control function of network unilateral transmission products are as follows:

a) Testing and evaluation approaches:

1) Documents provided by developers are assessed, including detailed description on enhanced information flow control function. The security function policy of network unilateral transmission products that may execute the following enhanced information flow control function and provide definite access assurance capability and access rejection capability is tested. Including:

— Network unilateral transmission products are able to analyze multiple data coding formats, identify whether the documents contain non-text data and cut off or release it according to the security policy configured by the authorized administrator;

— Network unilateral transmission products are able to support such service types as document unilateral transmission, database unilateral transmission, e-mail unilateral transmission and agency receiving unilateral transmission;

— Network unilateral transmission products are able to periodically complete unilateral transmission of data according to preset time.

2) Testing results are recorded and it is judged whether such results are fully in accordance with the requirements for the above testing and evaluation approaches.

b) Expected results:

1) Network unilateral transmission products shall be able to conduct unilateral transmission of data in the environment of IPv4/IPv6;

2) Network unilateral transmission products shall be able to analyze multiple data coding formats, identify whether the documents contain non-text data and cut off or release it according to the security policy configured by the authorized administrator;

3) Network unilateral transmission products shall be able to support such service types as document unilateral transmission, database unilateral transmission, e-mail unilateral transmission and agency receiving unilateral transmission;

4) Network unilateral transmission products shall be able to periodically complete unilateral transmission of data according to preset time.

5.4.2.1.4 Unilateral transmission guarantee

The testing and evaluation approaches and expected results of unilateral transmission guarantee of network unilateral transmission products are as follows:

a) Testing and evaluation approaches:

According to those stated in the documents provided, it is inspected that the products provide unique channel for construction of unilateral information transmission in a physical way, i.e., the information only can be transmitted from one security domain to another security domain and guarantees no any

synchronization task, the security function that can guarantee no provision of any information content generated in previously unilateral synchronization task in their allocated resources is tested. Testing results are recorded and it is judged whether such results are fully in accordance with the requirements for the above testing and evaluation approaches.

b) Expected results:

Where network unilateral transmission products allocate resources for newly-created unilateral synchronization task, the security function shall guarantee no provision of any information content generated in previous unilateral synchronization in their allocated resources.

5.4.2.1.7 Non-bypass

Testing and evaluation approaches and expected results of non-bypass of network unilateral transmission products are as follows:

a) Testing and evaluation approaches:

Documents provided by developers are accessed, including mechanisms and measures for the network unilateral transmission products to ensure non-bypass of security policy, i.e., before any security-related operation is permitted to be executed, it must pass through the inspection by security policy. The documents shall analyze and confirm that network unilateral transmission products indeed control each access request of terminal equipment users, without other approaches that possibly bypass the network unilateral transmission products. Testing results are recorded and it is judged whether such results are fully in accordance with the requirements for the above testing and evaluation approaches.

b) Expected results:

Products are free of other approaches that possibly bypass the network unilateral transmission products.

5.4.2.1.8 Data integrity assurance

Testing and evaluation approaches and expected results of data integrity assurance of network unilateral transmission products are as follows:

a) Testing and evaluation approaches:

Documents provided by developers are assessed, including detailed description on all the interfaces and services outward provided by network unilateral transmission products. It is tested whether the network unilateral

transmission products are provided with integrity protection in the process of unilateral data transmission to ensure data integrity of unilateral transmission without any feedback information. Testing results are recorded and it is judged whether such results are fully in accordance with the requirements for the above testing and evaluation approaches.

b) Expected results:

Network unilateral transmission products shall be provided with integrity protection in the process of unilateral data transmission to ensure data integrity of unilateral transmission without any feedback information.

5.4.2.2 Anti-attack

Testing and evaluation approaches and expected results of anti-attack of network unilateral transmission products are as follows:

a) Testing and evaluation approaches:

1) Anti-attack function of network unilateral transmission products is configured and put into service;

2) Simulated attack equipment is adopted to, through network unilateral transmission products, initiate attack flow supporting 10% bandwidth stated in the products (at least including SYN Flood and ICMP Flood etc.) and meanwhile, through network separation products, establish normal transmission services and continue for 1min;

3) The passing ratio of denial of service attack packets and the ratio of successful establishment of normal business are inspected.

b) Expected results:

1) Network unilateral transmission products are possessed of anti-denial service attack capability;

2) The passing ratio of attack packets is not greater than 5% and the success rate of establishment of normal business is not less than 90%.

5.4.2.3 Security management

5.4.2.3.1 Distinguishing of security management roles

Testing and evaluation approaches and expected results of distinguishing of security management roles of network unilateral transmission products are as follows:

a) Testing and evaluation approaches:

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

1) Relationship between identification and role;

2) Security attribute values of subject (data acquirer) and object (data receiver);

3) Configured security parameters.

5.4.2.4.6 Initialization of authentication data

Testing and evaluation approaches and expected results of initialization of authentication data of network unilateral transmission products are as follows:

a) Testing and evaluation approaches:

Documents provided by developers are assessed, including detailed description on initialization of authentication data. The function of initializing the authentication data provided according to specified authentication mechanism by the network unilateral transmission products for the authorized administrator is tested and it is ensured that only the authorized administrator is permitted to use such function. Testing results are recorded and it is judged that whether such results are fully in accordance with the requirements for the above testing and evaluation approaches.

b) Expected results:

Network unilateral transmission products shall provide the authorized administrator with the function of initialization of authentication data according to the specified authentication mechanism and shall ensure that only permit the authorized administrator can use such function.

5.4.2.4.7 Authentication time

Testing and evaluation approaches and expected results of authentication time of network unilateral transmission products are as follows:

a) Testing and evaluation approaches:

Documents provided by developers are assessed, including detailed description on authentication time. It is tested that, before any operation requested by all the authorized administrators, the network unilateral transmission products ensures to conduct identity authentication for each authorized administrator. Testing results are recorded and it is judged whether such results are fully in accordance with the requirements for the

above testing and evaluation approaches.

b) Expected results:

Before any operation requested by all the authorized administrators, network unilateral transmission products shall ensure to conduct identity authentication for each authorized administrator.

5.4.2.4.8 Minimum feedback

Testing and evaluation approaches and expected results of minimum feedback of network unilateral transmission products are as follows:

a) Testing and evaluation approaches:

Documents provided by developers are assessed, including detailed description on minimum feedback. Where the network unilateral transmission products conduct identification, the security function that only provides the minimum feedback for users is tested. Testing results are recorded and it is judged that whether such results are fully in accordance with the requirements for the above testing and evaluation approaches.

b) Expected results:

Where the network unilateral transmission products conduct identification, the security function shall only provide the minimum feedback for users.

5.4.2.4.9 Authentication failure handling

Testing and evaluation approaches and expected results of authentication failure handling of network unilateral transmission products are as follows:

a) Testing and evaluation approaches:

Documents provided by developers are assessed, including detailed description on authentication failure handling. They are logged in wrong user name - password; after certain times of authentication failures, it is tested that unilateral transmission equipment terminates the process to attempt to log in the host and establish sessions. They are logged in as authorized administrator and ordinary user respectively and setting function of maximum failure times provided by this component is tested and such maximum failure times are only set by the authorized administrator. Testing results are recorded and it is judged whether such results are fully in accordance with the requirements for the above testing and evaluation approaches.

b) Expected results:

b) Expected results:

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

5.4.2.4.12 Anti-replay

Testing and evaluation approaches and expected results of anti-replay of network unilateral transmission products are as follows:

a) Testing and evaluation approaches:

Documents provided by developers are assessed, including detailed description on anti-replay. It is tested whether the authentication mechanism of network unilateral transmission products is possessed of anti-replay capability and whether the authorized administrator and other users can't pass the identification by copying authentication information of last time. Testing results are recorded and it is judged that whether such results are fully in accordance with the requirements for the above testing and evaluation approaches.

b) Expected results:

The authentication mechanism of network unilateral transmission products shall be possessed of anti-replay capability so that the authorized administrator and other users cannot pass the authentication again by copying the authentication information of last time.

5.4.2.4.13 Protected authentication feedback

Testing and evaluation approaches and expected results of protected authentication feedback of network unilateral transmission products are as follows:

a) Testing and evaluation approaches:

Documents provided by developers are assessed, including detailed description on protected authentication feedback. It is tested that such sensitive information as password input by the authorized administrator of network unilateral transmission products in the process of identification is displayed in login input interface of authentication information in an invisible and un-inferable way. Testing results are recorded and it is judged whether such results are fully in accordance with the requirements for the above testing and evaluation approaches.

b) Expected results:

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

5.4.2.4.14 Password strength

Testing and evaluation approaches and expected results of password strength of network unilateral transmission products are as follows:

a) Testing and evaluation approaches:

Documents provided by developers are assessed, including detailed description on password strength of network separation products. It is tested that the network unilateral transmission products adopt password verification mechanism for inspection on password complexity generated by the authorized administrator and whether the password strength guarantees that the password length is greater than 6 bits and the password type is a combination of numbers + capital and small letters. Moreover, effectiveness of measures is verified by simulating the password login. Testing results are recorded and it is judged whether such results are fully in accordance with the requirements for the above testing and evaluation approaches.

b) Expected results:

Network unilateral transmission products shall adopt password verification mechanism for inspection on password complexity generated by the authorized administrator and the password strength shall guarantee that the password length is greater than 6 bits and the password type is a combination of numbers + capital and small letters.

5.4.2.5 Audit

5.4.2.5.1 Generation of audit data

Testing and evaluation approaches and expected results of generation of audit data of network unilateral transmission products are as follows:

a) Testing and evaluation approaches:

1) Documents provided by developers are assessed, including detailed description on generation of audit data. It is tested that the security function of network unilateral transmission products can generate audit records for the following auditable events:

— Starting and closing of audit function;

— Any attempt of operation for audit record, including closing audit function or subsystem, and the identification of affected object;

— Any attempt to read, modify and destroy audit records;

— All the requests to execute operation for the subjects covered by access authorization and rejection rules, and the identification of affected object;

— All the attempts to modify security attribute, and the new value of modified security attribute;

— All the requests to use the authentication data management mechanism in security function;

— All the requests to access to authentication data, and the objective of access request;

— Any use of authentication mechanism;

— All the attempts to use identification mechanism;

— All the modifications (setting and update) to the configuration parameter of security function, whatever success or not, and the new value of configuration parameter.

2) For each audit record, whether the security function can record the following information: generation date and time of event, type of event, subject identity and successful or failed event;

3) Testing results are recorded and it is judged whether such results are fully in accordance with the requirements for the above testing and evaluation approaches.

b) Expected results:

1) Security function of the network unilateral transmission products shall be able to generate audit records for the following auditable events:

— Starting and closing of audit function;

— Any attempt of operation for audit record, including closing audit function or subsystem, and the identification of affected object;

— Any attempt to read, modify and destroy audit records;

— All the requests to execute operation for the subjects covered by access authorization and rejection rules, and the identification of affected object;

— All the attempts to modify security attribute, and the new value of modified security attribute;

— All the requests to use the authentication data management mechanism in security function;

— All the requests to access to authentication data, and the objective of access request;

— Any use of authentication mechanism;

— All the attempts to use identification mechanism;

— All the modifications (setting and update) to the configuration parameter of security function, whatever success or not, and the new value of configuration parameter;

2) For each audit record, security function shall at least record the following information: generation date and time of event, type of event, subject identity and successful or failed event;

5.4.2.5.2 User identity association

Testing and evaluation approaches and expected results of user identity association of network unilateral transmission products are as follows:

a) Testing and evaluation approaches:

Documents provided by developers are assessed, including evaluation on user identity association. Different roles of users are used to execute all the operations related to product function and it is tested whether the security function of network unilateral transmission products can associate each auditable event with the user identity causing such event. Testing results are recorded and it is judged whether such results are fully in accordance with the requirements for the above testing and evaluation approaches.

b) Expected results:

Products are able to associate each auditable event with the user identity causing such event.

5.4.2.5.3 Audit record management

description on elimination of access to audit record. Audit records are accessed by simulating authorized and unauthorized administrators and security function of network separation products to only permit the authorized administrator to access to the audit records is tested. Testing results are recorded and it is judged whether such results are fully in accordance with the requirements for the above testing and evaluation approaches.

b) Expected results:

The security function of network unilateral transmission product shall only permit the authorized administrator to access to the audit record.

5.4.2.5.6 Optional retrieval of audit data

Testing and evaluation approaches and expected results of optional retrieval of audit data of network unilateral transmission products are as follows:

a) Testing and evaluation approaches:

Documents provided by developers are assessed, including detailed description on optional retrieval of audit data. It is tested that the network unilateral transmission products themselves provide audit retrieval tool; the audit retrieval tool can conduct correct searching and sorting on audit data according to logical combination of subject ID (identifier), object ID, date and time. Testing results are recorded and it is judged whether such results are fully in accordance with the requirements for the above testing and evaluation approaches.

b) Expected results:

The security function of network unilateral transmission products shall provide such audit retrieval tool that can conduct searching and sequencing for the audit data according to such parameters as subject ID (identifier), object ID, date and time as well as logical combination of these parameters.

5.4.2.5.7 Audit data loss prevention

Testing and evaluation approaches and expected results of audit data loss prevention of network unilateral transmission products are as follows:

a) Testing and evaluation approaches:

1) It is tested that the security function of unilateral transmission equipment that can store the generated audit records in a permanent audit record and limit number of lost audit events due to failure and attack (it is tested whether means and limitation are provided);

2) Operation related to excessive consumption of audit capacity is simulated and it is tested that the unilateral transmission equipment sends out warning message where the audit storage capacity reaches the preset warning value and guarantees to avoid other auditable behaviors beyond audit behaviors adopted by the authorized administrator.

3) Testing results are recorded and it is judged whether such results are fully in accordance with the requirements for the above testing and evaluation approaches.

b) Expected results:

Developers shall provide relevant documents, whose contents shall conform to actual conditions. The security function of network unilateral transmission products shall store the generated audit records in a permanent audit record and limit the number of lost audit events due to failure and attack; for the maximum audit storage capacity of audit data loss due to failure or storage depletion, the developers of network unilateral transmission products shall provide corresponding analysis results.

5.4.2.6 Domain isolation

5.4.2.6.1 Basic domain isolation

Testing and evaluation approaches and expected results of basic domain isolation of network unilateral transmission products are as follows:

a) Testing and evaluation approaches:

Documents provided by developers are assessed, including detailed description on basic domain isolation. In order to protect security function of network unilateral transmission products against interference and tampering by untrusted subject (host on internal or external network), the security function of network unilateral transmission products may set a security zone for its execution environment and separate the security zones of all the subjects (host on internal or external network) within the control range of network unilateral transmission products. Testing results are recorded and it is judged whether such results are fully in accordance with the requirements for the above testing and evaluation approaches.

b) Expected results:

In order to protect the security function of network unilateral transmission products against interference and tampering by untrusted subject (host on internal or external network), the security function of network unilateral

transmission products shall be able to set a security zone for its execution environment and separate the security zones of all subjects (host on internal or external network) within the control range of network unilateral transmission products.

5.4.2.6.2 Enhanced domain isolation

Testing and evaluation approaches and expected results of enhanced domain isolation of network unilateral transmission products are as follows:

a) Testing and evaluation approaches:

Documents provided by developers are assessed, including detailed description on enhanced domain isolation. In order to protect the security function of network separation products against interference and tampering by untrusted subjects (hosts on internal or external network), it is tested that the security function of network unilateral transmission products may set a security zone for its execution environment. Mandatory access control policy is adopted and this security zone is marked as high security level, and the authorized administrator and all the subjects covered by network separation product (hosts on internal or external network), after being authorized, are only able to read the files and programs stored in this zone but unable to make any deletion or modification; the authorized administrator is unable to modify the access policy. Testing results are recorded and it is judged whether such results are fully in accordance with the requirements for the above testing and evaluation approaches.

b) Expected results:

In order to protect the security function of network separation products against interference and tampering by untrusted subjects (hosts on internal or external network), the security function of network unilateral transmission products shall set a security zone for its execution environment. Mandatory access control policy is adopted and this security zone shall be marked as high security level, and the authorized administrator and all the subjects covered by network separation product (hosts on internal or external network), after being authorized, are only able to read the files and programs stored in this zone but unable to make any deletion or modification; the authorized administrator is unable to modify the access policy.

5.4.2.7 Fault tolerance

Testing and evaluation approaches and expected results of fault tolerance of network unilateral transmission products are as follows:

a) Testing and evaluation approaches:

Documents provided by developers are assessed, including detailed description on fault tolerance. Fault-tolerant capability of network unilateral transmission products in active/standby mode is tested; where one host is abnormal due to failure of such hardware as power supply and CPU or software error, the fault tolerance function is able to automatically switch the current security service function to another standby host and continue to operate to ensure availability of the security function. Testing results are recorded and it is judged whether such results are fully in accordance with the requirements for the above testing and evaluation approaches.

b) Expected results:

Network unilateral transmission products shall be possessed of the fault-tolerant capability in active/standby mode. Where one host is abnormal due to failure of such hardware as power supply and CPU or software error, the fault tolerance function shall be able to automatically switch the current security service function to another standby host and continue to operate to ensure availability of the security function.

5.4.2.8 Configuration data protection

Testing and evaluation approaches and expected results of configuration data protection of network unilateral transmission products are as follows:

a) Testing and evaluation approaches:

Documents provided by developers are assessed, including detailed description on configuration data protection. It is tested that the network unilateral transmission products can protect authentication data and data transmission policy stored in the equipment against unauthorized retrieval, modification and corruption. Testing results are recorded and it is judged that whether such results are fully in accordance with the requirements for the above testing and evaluation approaches.

b) Expected results:

Developers shall provide relevant documents, whose contents shall conform to actual conditions. Network unilateral transmission products shall be able to protect authentication data and data transmission policy stored in the equipment against unauthorized retrieval, modification and corruption.

5.4.2.9 Running state monitoring

Testing and evaluation approaches and expected results of running state monitoring

The documents provided by developers and content of site activity evidence shall meet the above-mentioned requirements.

6.1.1.2 Configuration item

Testing and evaluation approaches and expected results of configuration item are as follows:

a) Testing and evaluation approaches:

1) Evaluators shall check whether the configuration management documents provided by developers include configuration list and configuration management plan and whether the configuration list describes all the configuration items consisting of the system;

2) Evaluators shall inspect on site whether the configuration items in configuration management system are consistent with those described in the configuration list, whether the configuration management system makes unique identification for all the configuration items and whether the configuration management system maintains the configuration items;

3) Evaluators shall check whether the configuration management documents provided by developers describe the method for unique identification of configuration items.

b) Expected results:

The documents provided by developers and content of site activity evidence shall meet the above-mentioned requirements.

6.1.2 Delivery and operation

6.1.2.1 Delivery program

Testing and evaluation approaches and expected results of delivery program are as follows:

a) Testing and evaluation approaches:

1) Evaluators shall inspect on site whether the developers deliver products with certain delivery program;

2) Evaluators shall check whether the developers describe the delivery process with documents, whether the documents include the following contents: all programs required for maintaining security upon delivery of different versions of system to the users.

b) Expected results:

The documents provided by developers and content of site activity evidence shall meet the above-mentioned requirements.

6.1.2.2 Program installation, generation and startup programs

Testing and evaluation approaches and expected results of program installation, generation and startup are as follows:

a) Testing and evaluation approaches:

1) Evaluators shall check whether the developer provides documents to describe the installation, generation, startup and use process of the system;

2) Evaluators confirm whether the programs can be installed, generated and started correctly according to the method described in the documents.

b) Expected results:

The documents provided by developers and content of site activity evidence shall meet the above-mentioned requirements.

6.1.3 Development

6.1.3.1 Non-formalized functional specification

Testing and evaluation approaches and expected results of non-formalized functional specification are as follows:

a) Testing and evaluation approaches:

Evaluators shall check the following contents of non-formalized functional specification and confirm whether the functional design is the accurate and complete example of security function requirements:

— Describe the security function and external interface of products in non-formalized form;

— Be intrinsically consistent;

— Describe the purpose and method to use all the external interfaces of products and provide influence details of results on exceptions and error message in due course;

— Function design shall completely represent product security function.

b) Expected results:

The contents of documents provided by developers shall meet the above-mentioned requirements.

6.1.3.2 Descriptive high-level design

Testing and evaluation approaches and expected results of descriptive high-level design are as follows:

a) Testing and evaluation approaches:

Evaluators shall check the following contents of descriptive high-level design:

— Represent in non-formalized form;

— Be intrinsically consistent;

— Describe security function construction according to subsystems;

— Describe the security function provided by each security function subsystem;

— Identify any fundamental hardware, firmware or software as required by security function, and a representation of function provided by the supporting protection mechanism realized in these hardware, firmware or software.

— Identify all the interfaces of security function subsystems;

— Identify which interfaces of security function subsystems are externally visible.

b) Expected results:

The contents of documents provided by developers shall meet the above-mentioned requirements.

6.1.3.3 Non-formalized correspondence verification

Testing and evaluation approaches and expected results of non-formalized correspondence verification are as follows:

a) Testing and evaluation approaches:

1) Evaluators shall check whether the developer provides correspondence

analyses between all the adjacency pairs represented by product security function;

2) In which, the correspondence between various security function representations (such as system function design, high-level design, low-level design and realization representation) of the system is a accurate and complete example required by security function representation of provided abstract products.

3) Product security function is refined in function design, and all the security function-related parts in relatively abstract product security function representation are refined in relatively specific product security function representation.

b) Expected results:

The contents of documents provided by developers shall meet the above-mentioned requirements.

6.1.4 Instructive documents

6.1.4.1 Administrator manual

Testing and evaluation approaches and expected results of administrator manual are as follows:

a) Testing and evaluation approaches:

Evaluators shall check whether the developers provide the administrator guide for authorized administrator and whether this administrator guide includes the following contents:

— Operable management functions and interface of products;

— Product instructions on security functions and interfaces for administrators;

— Function and authority which shall be controlled in the security handling environment;

— All assumptions of users' behaviors concerning product security operation;

— For all the safety parameters controlled by administrators, if possible, security values shall be indicated;

— Each security-related event in connection with management function,

developers indicates that testing identified in the testing document is corresponding to the security function of the product described in the functional specification.

b) Expected results:

The contents of documents provided by developers shall meet the above-mentioned requirements.

6.1.5.2 Function testing

Testing and evaluation approaches and expected results of function testing are as follows:

a) Testing and evaluation approaches:

1) Evaluators shall check whether testing documents provided by developers include testing plan, test specification, expected testing result and actual testing result;

2) Evaluators shall check whether the testing plan identifies the security function to be tested and whether it describes the testing objective;

3) Evaluators shall check whether the testing specification identifies the test to be carried out and whether it describes the general testing conditions (including sequence dependency on other testing results) of each security function;

4) Evaluators shall check whether the expected testing result shows the expected output after the testing is successful;

5) The evaluator shall check whether actual testing result indicates that each tested security function can operate as required.

b) Expected results:

The contents of documents provided by developers shall meet the above-mentioned requirements.

6.1.5.3 Independent testing

6.1.5.3.1 Consistency

Testing and evaluation approaches and expected results of consistency are as follows:

a) Testing and evaluation approaches:

1) Evaluators shall check testing products provided by developers;

2) Evaluators shall check whether the testing sets provided by developers are consistent with those used for self-testing system function.

b) Expected results:

Developers shall provide the products suited for third-party testing and meet the above-mentioned requirements.

6.1.5.3.2 Sampling

Testing and evaluation approaches and expected results of sampling are as follows:

a) Testing and evaluation approaches:

Evaluators shall check whether the developers provide a group of equivalent resources for sampling testing of security function.

b) Expected results:

Resources provided by developers shall meet the above-mentioned requirements.

6.1.6 Vulnerability assessment

6.1.6.1 Product security function strength assessment

Testing and evaluation approaches and expected results of product security function strength assessment are as follows:

a) Testing and evaluation approaches:

Evaluators shall check whether instructive documents provided by developers make security function strength analysis on each identified safety mechanism with security function strength statement and whether describe the measurement for the security mechanism reaching or exceeding the defined minimum strength grade or specific function strength.

b) Expected results:

Documents provided by developers shall meet the above-mentioned requirements.

6.1.6.2 Developer vulnerability analysis

Testing and evaluation approaches and expected results of developer vulnerability

analysis are as follows:

a) Testing and evaluation approaches:

1) Evaluators shall check whether vulnerability analysis documents provided by developers make analyses on all kinds of product functions from the obvious approach in which the users may destroy security policy;

2) The evaluator shall check whether the developers explicitly record measures taken for the determined vulnerability;

3) For each vulnerability, evaluators shall check whether there is enough evidence to prove that this vulnerability cannot be used in the product service environment and verify it.

b) Expected results:

Documents provided by developers shall meet the above-mentioned requirements. Products provided shall pass the vulnerability testing verification.

6.2 Enhanced-Level Testing

6.2.1 Configuration management

6.2.1.1 Partial configuration management automatization

Testing and evaluation approaches and expected results of partial configuration management automatization are as follows:

a) Testing and evaluation approaches:

1) Evaluators shall check whether the configuration management system provides an automatic mode to support product generation and whether such mode can ensure only authorized modification to product realization representation.

2) Evaluators shall check whether configuration management plan describes automated tool used in the configuration management system and the usage method of such tool.

b) Expected results:

Contents of site activity evidence provided by developers shall meet the above-mentioned requirements.

6.2.1.2 Configuration management capability

6.2.1.2.1 Version number

Testing and evaluation approaches and expected results of version number are as follows:

a) Testing and evaluation approaches:

1) Evaluators shall check whether the configuration management supporting documents provided by developers contain version number and request that version number used by developers shall be completely corresponding to that of the product sample which shall be represented, without ambiguity;

2) Evaluators shall inspect on site whether the product samples in configuration management activity are provided with unique version number and whether the version number is completely corresponding to the product sample and description of configuration management supporting documents.

b) Expected results:

The documents provided by developers and content of site activity evidence shall meet the above-mentioned requirements.

6.2.1.2.2 Configuration item

Testing and evaluation approaches and expected results of configuration item are as follows:

a) Testing and evaluation approaches:

1) Evaluators shall check whether the configuration management documents provided by developers include configuration list and configuration management plan and whether the configuration list describes all the configuration items consisting of the system;

2) Evaluators shall inspect on site whether the configuration items in configuration management system are consistent with those described in the configuration list, whether the configuration management system makes unique identification for all the configuration items and whether the configuration management system maintains the configuration items;

3) Evaluators shall check whether the configuration management documents provided by developers describe the method for unique

b) Expected results:

The documents provided by developers and content of site activity evidence shall meet the above-mentioned requirements.

6.2.1.3 Configuration management scope

6.2.1.3.1 Configuration management coverage

Testing and evaluation approaches and expected results of configuration management coverage are as follows:

a) Testing and evaluation approaches:

1) Evaluators shall check whether configuration management supporting documents provided by developers state product configuration management scope and such configuration management scope shall at least include such configuration items as product realization representation, design document, testing document, instructive document and configuration management document to ensure that these configuration items are modified in a correctly authorized controllable way;

2) Evaluators shall inspect on site whether the configuration management system used by developers can at least track contents under the above-mentioned configuration management;

3) Evaluators shall check whether the configuration management supporting documents provided by developers describe the tracking method of configuration management system for configuration items.

b) Expected results:

The documents provided by developers and content of site activity evidence shall meet the above-mentioned requirements.

6.2.1.3.2 Issue tracking configuration management coverage

Testing and evaluation approaches and expected results of issue tracking configuration management coverage are as follows:

a) Testing and evaluation approaches:

Evaluators shall check whether developers incorporate security defects in the configuration management scope and whether they track the security defects.

1) Evaluators shall check whether the developers provide correspondence analyses between all the adjacency pairs represented by product security function;

2) In which, the correspondence between various security function representations (such as system function design, high-level design, low-level design and realization representation) of the system is a accurate and complete example required by security function representation of provided abstract products.

3) Product security function is refined in function design, and all the security function-related parts in relatively abstract product security function representation are refined in relatively specific product security function representation.

b) Expected results:

The contents of documents provided by developers shall meet the above-mentioned requirements.

6.2.3.6 Non-formalized product security policy model

Testing and evaluation approaches and expected results of non-formalized product security policy model are as follows:

a) Testing and evaluation approaches:

Evaluators shall check the following contents of security policy model:

— Represent in non-formalized form;

— Describe rules and characteristics of all security policies which can be modeled;

— Contain rationality, i.e., demonstrate that this model is consistent and complete for all the security policies which can be modeled;

— Clarify the correspondence between security policy model and functional specification, i.e., demonstrate all the security functions in the functional specification are consistent and complete for the security policy model.

b) Expected results:

The contents of documents provided by developers shall meet the above-mentioned requirements.

6.2.4 Instructive documents

6.2.4.1 Administrator manual

Testing and evaluation approaches and expected results of administer manual are as follows:

a) Testing and evaluation approaches:

Evaluators shall check whether the developer provides the administrator guide for authorized administrator and whether this administrator guide includes the following contents:

— Operable management functions and interface of products;

— Product instructions on security functions and interfaces for administrators;

— Function and authority which shall be controlled in the security handling environment;

— All assumptions of users' behaviors concerning product security operation;

— For all the safety parameters controlled by administrators, if possible, security values shall be indicated;

— Each security-related event in connection with management function, including change in security characteristics of the entity controlled by security function;

— All security requirements of IT environment concerning authorized administrator.

b) Expected results:

The contents of documents provided by developers shall meet the above-mentioned requirements.

6.2.4.2 User manual

Testing and evaluation approaches and expected results of user manual are as follows:

a) Testing and evaluation approaches:

Evaluators shall check whether the developers provide the user manual for users and whether this user manual includes the following contents:

— Security functions and interfaces which are available to non-administrative users;

— Product instructions on security functions and interfaces for users;

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

— Responsibility of users who shall bear in product security operation;

— All security requirements of IT environment concerning the users.

b) Expected results:

The contents of documents provided by developers shall meet the above-mentioned requirements.

6.2.5 Life cycle support

6.2.5.1 Security measure identification

Testing and evaluation approaches and expected results of security measure identification are as follows:

a) Testing and evaluation approaches:

1) Evaluators shall check whether development security documents provided by developers describe all the physical, procedural, personnel security measures and otherwise necessary for protecting the system design and realized confidentiality and integrity in the development environment of the system;

2) Evaluators shall inspect the development environment of products on site and inspect whether the developers ensure the product design and realized confidentiality and integrity by physical, procedural, personnel security measures and otherwise and whether such security measures are implemented effectively.

b) Expected results:

The contents of documents provided by developers shall meet the above-mentioned requirements.

6.2.5.2 Developer-defined life cycle model

Testing and evaluation approaches and expected results of developer-defined life cycle model are as follows:

functional specification.

b) Expected results:

The contents of documents provided by developers shall meet the above-mentioned requirements.

6.2.6.1.2 Coverage analysis

Testing and evaluation approaches and expected results of coverage analysis are as follows:

a) Testing and evaluation approaches:

1) Evaluators shall check whether the testing coverage analysis provided by developers indicate that the testing identified in the testing documents is corresponding to the security function described in security function design.

2) Evaluate whether the testing identified in the testing documents is complete.

b) Expected results:

Contents of documents provided by developers shall meet the above-mentioned requirements.

6.2.6.1.3 Testing: high-level design

Testing and evaluation approaches and expected results of testing depth are as follows:

a) Testing and evaluation approaches:

Evaluators shall check whether the testing depth analysis provided by developers indicates that security function testing identified in testing documents is enough to prove that this security function and high-level design are consistent with each other.

b) Expected results:

The contents of documents provided by developers shall meet the above-mentioned requirements.

6.2.6.1.4 Function testing

Testing and evaluation approaches and expected results of function testing are as

follows:

a) Testing and evaluation approaches:

1) Whether testing documents provided by developers include testing plan, test specification, expected testing result and actual testing result;

2) Whether the testing plan identifies the security function to be tested and whether it describes the testing objective;

3) Whether the testing specification identifies the test to be carried out and whether it describes the general testing conditions (including sequence dependency on other testing results) of each security function;

4) Whether the expected testing result shows the expected output after the testing is successful;

5) Whether actual testing result in testing documents provided by developers indicates that each tested security function can operate as required.

b) Expected results:

The contents of documents provided by developers shall meet the above-mentioned requirements.

6.2.6.2 Independent testing

6.2.6.2.1 Consistency

Testing and evaluation approaches and expected results of consistency are as follows:

a) Testing and evaluation approaches:

1) Evaluators shall check testing products provided by developers;

2) Evaluators shall check whether the testing sets provided by developers are consistent with those used for self-testing system function.

b) Expected results:

Developers shall provide the products suited for third-party testing and meet the above-mentioned requirements.

6.2.6.2.2 Sampling

Testing and evaluation approaches and expected results of sampling are as follows:

a) Testing and evaluation approaches:

Evaluators shall check whether the developers provide a group of equivalent resources for sampling testing of security function.

b) Expected results:

Resources provided by developers shall meet the above-mentioned requirements.

6.2.7 Vulnerability assessment

6.2.7.1 Misuse

6.2.7.1.1 Manual checking

Testing and evaluation approaches and expected results of manual checking are as follows:

a) Testing and evaluation approaches:

1) Evaluators shall check whether instructive documents and analysis documents provided by developers describe all possible operation modes (including operation after failure and mis-operation), and determine their consequences and the significance to maintain security operation;

2) Evaluators shall check the instructive documents and analysis documents provided by developers list the requirements for all assumption for object environments and all external security measures (including external program control, physical or personnel control);

3) Evaluators shall check whether documents provided by developers are complete, clear, consistent and reasonable;

4) Evaluate whether analysis documents provided by the developer state the documents are complete.

b) Expected results:

Documents provided by developers shall meet the above-mentioned requirements.

6.2.7.1.2 Analysis confirmation

Testing and evaluation approaches and expected results of analysis confirmation are as follows:

a) Testing and evaluation approaches:

Evaluate whether the analysis documents, demonstrative and instructive documents provided by developers are complete.

b) Expected results:

Documents provided by developers shall meet the above-mentioned requirements.

6.2.7.2 Product security function strength assessment

Testing and evaluation approaches and expected results of product security function strength assessment are as follows:

a) Testing and evaluation approaches:

Evaluators shall check whether instructive documents provided by developers make security function strength analysis on each identified safety mechanism with security function strength statement and whether describe the measurement for the security mechanism reaching or exceeding the defined minimum strength grade or specific function strength.

b) Expected results:

Documents provided by developers shall meet the above-mentioned requirements.

6.2.7.3 Vulnerability analysis

6.2.7.3.1 Developer vulnerability analysis

Testing and evaluation approaches and expected results of developer vulnerability analysis are as follows:

a) Testing and evaluation approaches:

1) Evaluators shall check whether vulnerability analysis documents provided by developers make analyses on all kinds of product functions from the obvious approach in which the users may destroy security policy;

2) Evaluators shall check whether the developers explicitly record measures taken for the determined vulnerability;

a) Testing and evaluation approaches:

1) Network separation products/network unilateral transmission products are connected with protocol robustness tester in series;

2) IPv6 malformed packet attack is selected on protocol robustness tester and testing results are recorded;

3) ICMPv6 malformed packet attack is selected on protocol robustness tester and testing results are recorded;

4) Other protocol malformed packet attacks are selected on protocol robustness tester and testing results are recorded.

b) Expected results:

1) Network separation products/network unilateral transmission products can defend against IPv6 malformed packet attack;

2) Network separation products/network unilateral transmission products can defend against ICMPv6 malformed packet attack;

3) Network separation products/network unilateral transmission products can defend against other protocol malformed packet attacks.

7.1.4 Self-management in IPv6 network environment

Testing and evaluation approaches and expected results of self-management in IPv6 network environment are as follows:

a) Testing and evaluation approaches:

IPv6 network environment is simulated and it is detected whether the separation products/network unilateral transmission products can support self-management in IPv6 network environment.

b) Expected results:

Network separation products/network unilateral transmission products can support self-management in IPv6 network environment.

7.2 IPv6 Transition Network Environment Support

7.2.1 Double protocol stack

Testing and evaluation approaches and expected results of double protocol stack are as follows:

a) Testing and evaluation approaches:

Coexisting network environment of IPv4 and IPv6 protocols are simulated and it is detected whether the network separation products/network unilateral transmission products can support IPv4 and IPv6 protocols simultaneously and work normally in IPv4/IPv6 double stack network environment.

b) Expected results:

Network separation products/network unilateral transmission products can support IPv4 and IPv6 protocols simultaneously and work normally in IPv4/IPv6 double stack network environment.

7.2.2 Protocol conversion

Testing and evaluation approaches and expected results of protocol conversion are as follows:

a) Testing and evaluation approaches:

Interconversion network environment of IPv4 and IPv6 protocols are simulated and it is detected whether the network separation products/network unilateral transmission products can support interconversion of IPv4 and IPv6 interconversion and work normally in IPv4/IPv6 protocol conversion network environment.

b) Expected results:

Network separation products/network unilateral transmission products can support interconversion of IPv4 and IPv6 protocols and work normally in IPv4/IPv6 protocol conversion network environment.

7.2.3 Tunnel

7.2.3.1 60ver4

Testing and evaluation approaches and expected results of 60ver4 are as follows:

a) Testing and evaluation approaches:

Network environment of 60ver4 tunnel is simulated and it is detected whether the separation products/network unilateral transmission products can support 60ver4 tunnel and work normally in 60ver4 tunnel network environment.

b) Expected results:

Network separation products/network unilateral transmission products can

support 60ver4 tunnel and work normally in 60ver4 tunnel network environment.

7.2.3.2 6to4

Testing and evaluation approaches and expected results of 6to4 are as follows:

a) Testing and evaluation approaches:

Network environment of 6to4 tunnel is simulated and it is detected whether the separation products/network unilateral transmission products can support 6to4 tunnel and work normally in 6to4 tunnel network environment.

b) Expected results:

Network separation products/network unilateral transmission products can support 6to4 tunnel and work normally in 6to4 tunnel network environment.

7.2.3.3 ISATAP

Testing and evaluation approaches and expected results of ISATAP are as follows:

a) Testing and evaluation approaches:

Network environment of ISATAP tunnel is simulated and it is tested whether the network separation products/network unilateral transmission products can support ISATAP tunnel and work normally in ISATAP tunnel network environment.

b) Expected results:

Network separation products/network unilateral transmission products can support ISATAP tunnel and work normally in ISATAP tunnel network environment.

8 Performance Testing

8.1 Exchange Rate

Testing and evaluation approaches and expected results of exchange rate of network separation products are as follows:

a) Testing and evaluation approaches:

Detailed description on exchange rate of network separation products is checked. Exchange rate of network separation products is tested by testing

tool or special testing equipment.

b) Expected results:

Performance indexes for exchange rate of network separation products shall reach the minimum requirements specified in 5.5.1 of GB/T 20279-2015.

8.2 Hardware Switching Time

Testing and evaluation approaches and expected results of hardware switching time of network separation products are as follows:

a) Testing and evaluation approaches:

Detailed description on hardware switching time of network unilateral transmission products is checked. Switching time of network separation products is tested by testing tool or special testing equipment.

b) Expected results:

Performance indexes for hardware switching time of network separation products shall reach the minimum requirements specified in 5.5.2 of GB/T 20279-2015.

References

[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 Requirements for End-Equipment Isolate Components

_____ END _____

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

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