GB

NATIONAL STANDARD OF THE

PEOPLE'S REPUBLIC OF CHINA

ICS 35.040
L 80

GB/T 20281-2015

Replacing GB/T 20281-2006

Information Security Technology - Security Technical Requirements and Test-evaluation methods for Firewall

信息安全技术　防火墙安全技术要求

和测试评价方法

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 is drafted in accordance with the rules given in GB/T 1.1-2009.

This Standard replaces GB/T 20281-2006 *Information Security Technology Technique Requirements and Test-evaluation methods for Firewall Products*.

Compared with GB/T 20281-2006, this Standard has the main changes as follows:

— The description of firewall is modified;

— Functional classification of firewall is modified;

— Requirements for high performance of firewall are added;

— Requirements for capacity of firewall to control the application layer are strengthened;

— The requirements of next generation Internet Protocol for the support capability are added;

— It is uniformly divided into basic-grade and reinforced-grade.

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: Ministry of Public Security Computer Information System Security Product Quality Supervision Testing Center, Venustech Co., Ltd., Huawei Technology Co., Ltd., National Liberation Army Information Security Evaluation and Certification Center, Netpower Co., Ltd., Beijing NetentSec Co., Ltd. AND the Third Research Institute of The Ministry of Public Security.

Chief drafting staffs of this Standard: Yu You, Lu Zhen, Zou Chunming, Gu Jian, Shen Liang, Li Yi, Wei Xiang, Wang Guangyu, Lv Yingxuan and Wang Ping.

The previous edition replaced by this Standard is as follows:

— GB/T 20281-2006.

Information Security Technology - Security Technical Requirements and Test-evaluation methods for Firewall

1 Scope

This Standard specifies the firewall in terms of security technical requirements, test-evaluation methods and security grade division.

This Standard is applicable to design, development and testing of firewalls.

2 Normative References

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

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

GB/T 25069-2010 Information Security Technology - Glossary

3 Terms and Definitions

For the purposes of this document, the terms and definitions established in GB/T 25069-2010 AND the following ones apply.

3.1

Firewall

Security gateway products which are allocated among security domains to control and filter the access to network layer and with the function of application layer protocol analysis, control and contents testing, which are applicable to IPv4 and IPv6.

3.2

Deep packet inspection

It is based on flow testing and control technology of application layer and will obtain all the application program contents by reading IP packet loads and reconstructing the information of application layer; then it also deals with the contents depending on the

policy of system definition.

3.3

Deep content inspection

It is able to make a deep analysis for application protocol, identifies all elements therein (such as HTTP protocol, specifically cookie, Get parameters and Post form) and all the protocol service (such as data contents included in the protocol or documents in the business system interaction) and then analyze quickly the data to restore the original communicating information. It can also test whether threat or sensitive contents are included based on the original information.

3.4

SQL injection

Its purpose is to cheat the server into doing malicious SQL command by inserting SQL command into submittal or page request parameters of web form.

3.5

Cross site scripting

A type of injection, in which the malicious HTML code is injected into a web page by the malicious attacker. The HTML code will be executed when the user browses the page so as to realize malicious attack to the user.

4 Abbreviated Terms

For the purpose of this document, the following abbreviated terms apply.

DPI: Deep packet inspection

DCI: Deep content inspection

SQL: Structured Query Language

XSS: Cross Site Scripting

5 Firewall Description

The firewall is to establish security control points in security fields, analyze and filter data flow through firewall according to predefine access control policy and security protection policy, and provide controllable visit service request to the protected security field. The firewall protocol suite compatible with the next generation of net atmosphere supports not only IPv4 technology but also IPv6, IPv4/IPv6 transition technology.

	management capacity	Configuration item	*	*
		Authorization control	—	*
		Generation support and acceptance programs	—	*
	Configuration management scope	Configuration management coverage	—	*
		Problems tracking configuration management coverage	—	*
Delivery and operation	Delivery programs		*	*
	Modification detection		—	*
	Installation, generating and starting programs		*	*
Development	Functional specification	Non-formalized functional specification	*	*
		Well-defined external interface	—	*
	High-level design	Descriptive high-level design	*	*
		Security strengthened high-level design	—	*
	Subset of security function realization		—	*
	Descriptive low-level design		—	*
	Non-formalized correspondence verification		*	*
	Security policy model of non-formalized products		—	*
Instructive document	Administrator manual		*	*
	User guide		*	*
Life cycle support	Security measures identification		—	*
	Developer defined life cycle model		—	*
	Well-defined development tool		—	*
Testing	Testing coverage	Coverage evidence	*	*
		Coverage analysis	—	*
	Testing: high-level design		—	*
	Functional test		*	*
	Independent testing	Consistency	*	*
		Sampling	*	*
Vulnerability assessment	Misuse	Guide review	—	*
		Analysis validation	—	*
	Product security function strength assessment		*	*
	Vulnerability analysis	Vulnerability analysis for developer	*	*
		Independent vulnerability analysis	—	*
		Intermediate resistibility	—	*
Note: "*" means the requirements are provided; "—" N/A.				

6.2 Security Requirements for Basic-grade

6.2.1 Security Function Requirements

6.2.1.1 Network layer control

6.2.1.1.1 Packet filtering

Package filtering requirements for firewall:

a) The security policy shall adopt the minimum security principle, i.e. forbid unless otherwise explicitly allowed;

b) Security policy shall cover access control on the basis of source IP address and destination IP address;

c) Security policy shall cover access control on the basis of source port and destination port;

d) Security policy shall cover access control on the basis of protocol type;

e) Security policy shall cover access control on the basis of time;

f) User-defined security policy shall be supported and it may be partial or complete combination of IP address, port, protocol type and time.

6.2.1.1.2 NAT

The firewall shall be provided with NAT Function and the specific technical requirements are as follows:

a) Support bidirectional NAT: SNAT and DNAT;

b) SNAT shall at least realize "many to one" address conversion so that the source IP address can be converted as intranet host visits extranet;

c) DNAT shall at least realize "many to one" address conversion, in which DMZ IP address/port are mapped as legal IP address/port of extranet and extranet host can visit DMZ server by visiting the mapped address and port.

6.2.1.1.3 State inspection

With state inspection functions, the firewall shall support the access control on the basis of state inspection technology.

6.2.1.1.4 Policy routing

If the firewall is provided with multiple network interfaces with the identical attribute (such as extranet interfaces, intranet interfaces or DMZ network interfaces), it shall be provided with routing functions on the basis of source and destination IP policy.

6.2.1.1.5 Dynamic open port

With dynamic open port, the firewall shall support FTP in either active mode or passive mode.

6.2.1.1.6 IP/MAC address binding

The firewall shall support the automatic or manual binding (by administrators) of IP /MAC address; it shall be able to inspect whether IP address is embezzled and

intercept the visits of host embezzling IP address through the firewall.

6.2.1.1.7 Traffic and session management

6.2.1.1.7.1 Traffic statistics

The firewall shall be provided with traffic statistics functions:

a) The firewall can make correct traffic statistics according to IP address, network service, time and protocol type or their combination;

b) The firewall can output traffic statistical result in real time or in report form.

6.2.1.1.7.2 Connection control

The firewall shall be able to set maximum concurrent sessions number of single IP to prevent network performance from being influenced by a large amount of illegal connection.

6.2.1.1.8 Anti-denial of service attack

The firewall shall be provided with anti-denial of service attack and the specific technical requirements are as follows:

a) ICMP Flood attack;

b) UDP Flood attack;

c) SYN Flood attack;

d) TearDrop attack;

e) Land attack;

f) Ultra-large ICMP data attack.

6.2.1.1.9 Network scanning protection

The firewall can inspect and record the scanning action carried out to all the firewalls and protected networks.

6.2.1.2 Application layer protocol control

The firewall shall be able to identify and control all kinds of application types and support the common applications like HTTP, FTP, TELNET, SMTP and POP3.

6.2.1.3 Security operation and maintenance management

6.2.1.3.1 Operation and maintenance management

The firewall shall be provided with management function and the specific technical

requirements are as follows:

a) Management security:

1) The firewall shall support password discrimination method of authorized administrator and the password setting is in accordance with security requirements:

2) The firewall shall ensure each of authorized administrator, trusted host, host and users is subjected to unique identity identification prior to any operation required by all the authorized administrators, trusted hosts, hosts and users;

3) With login failure handling function, the firewall shall terminate the session established by the trusted hosts or users after identity authentication is subjected to a given maximum authentication failure frequency;

4) The firewall shall provide a set of unique security attribute for each specified authorized administrator, trusted host, host and users necessary to implement security policy.

b) Management mode:

1) Support local management by console port;

2) Support remote management by network interface and limit network interface to perform remote management;

3) During the remote management, all the communication data between management end and firewall shall not be subjected to plaintext transport.

c) Management capacity:

1) Provide data parameters to set and modify security management to the authorized administrators;

2) Provide functions to set, query and modify security policies to the authorized administrators;

3) Provide functions to manage and audit logs to authorized administrator.

6.2.1.3.2 Security audit

The firewall shall be provided with security audit function and the specific technical requirements are as follows:

a) Record event type:

1) Visit request, which is permitted or rejected by firewall policy;

2) Visit request in breach of security, initiated from intranet, extranet and DMZ zone to get through or reach the firewall;

3) Request to log in the firewall management port and manage identity authentication;

4) Important management configuration operation: add/delete/modify administrator, save/delete audit logs, modify security policy and configuration parameters etc.

b) Log contents:

1) Event time, including year, month, day, hour, minute and second;

2) Event subject, object and description, data packet shall include protocol type, source address, destination address, source port and destination port.

c) Log management:

1) Authorized administrator is only one to access to log;

2) Administrators shall be able to archive, delete and empty logs;

3) Provide tools to consult the logs, have capacity to search the audit events by time, date, subject ID and object ID and allow only authorized administrator to use the tools;

4) Support statistical analysis and report generation functions;

5) Audit events shall be stored in the nonvolatile medium in case of power down and the authorized administrator shall be informed when the memory space reaches threshold.

6.2.1.3.3 Security management

6.2.1.3.3.1 Management interface independence

The firewall shall be provided with independent management interface and separated from the service interfaces.

6.2.1.3.3.2 Security support system

Bottom support system of firewall shall meet the following requirements:

a) Be ensured that no redundant network service is provided by the support system;

b) Be free of security vulnerability which result in product authority loss and denial of service.

6.2.1.3.3.3 Exception handling mechanism

The firewall shall meet the following technical requirements when it is restarted from power down and forced shut-down and other abnormal conditions:

a) The security policy restores to the state saved before shutdown;

b) The log information will not lose;

c) Administrator re-authenticates.

6.2.2 Security Assurance Requirements

6.2.2.1 Configuration management

6.2.2.1.1 Revision

The developer shall provide unique identification for the products versions.

6.2.2.1.2 Configuration item

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

Configuration management document shall include one configuration list which shall identify uniquely all the configuration items constituting products and describe them and methods to make a unique identification for configuration item and provide evidence of configuration items have been well maintained.

6.2.2.2 Delivery and operation

6.2.2.2.1 Delivery programs

The developer shall deliver products by some delivery programs and document the delivery process.

Delivery document shall be described as all programs necessary to maintain security when delivering products versions to the users.

6.2.2.2.2 Installation, generating and starting programs

The developer shall provide installation, generating and starting programs of document description products.

6.2.2.3 Development

6.2.2.3.1 Non-formalized functional specification

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

a) Describe product security function and external interface by non-formalized form;

b) Be intrinsically consistent;

c) Describe purpose and application method of all the external interfaces and provide effects, exceptions and error message details in due course;

d) Represent product security function completely.

6.2.2.3.2 Descriptive high-level design

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

a) Non-formalized representation;

b) Be intrinsically consistent;

c) Describe security function construction according to subsystems;

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

e) Identify any fundamental hardware, firmware and/or software as required by security function, and one representation of function provided by supportive protection mechanism which is realized by them.

f) Identify all the interfaces of security function subsystems;

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

6.2.2.3.3 Non-formalized correspondence verification

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

For each adjacency pairs, all the security functions shall be illustrates and correct and complete security functions are obtained.

6.2.2.4 Instructive document

6.2.2.4.1 Administrators manual

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

The administrators manual shall cover the following contents:

a) Management function and interface which is accessible to administrators;

b) How to safely manage products;

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

d) All assumptions of users' behavior concerned with security operation;

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

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

g) All IT environmental security requirements concerned with administrators.

6.2.2.4.2 User guide

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

The user guide shall cover the following contents:

a) Security function and interface which is accessible to non-administrators;

b) Security function and interface usage which is available to user;

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

d) Responsibility of users who shall bears in product security operation;

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

6.2.2.5 Testing

6.2.2.5.1 Coverage evidence

The developer shall provide testing Coverage evidence.

The security function for testing and functional specification in test document are corresponding in testing coverage evidence.

6.2.2.5.2 Functional testing

The developer shall test the security function and document the results and provide test document.

6.3.1.1.4 Policy Routing

If the firewall is provided with multiple network interfaces with the identical attribute (such as extranet interfaces, intranet interfaces or DMZ network interfaces), it shall be provided with routing functions and specific technical requirements are shown as follows:

a) Routing on the basis of source and destination IP policy;

b) **Routing on the basis of next-hop interfaces;**

c) **Policy routing on the basis of protocol and port;**

d) **Policy routing on the basis of application type;**

e) **Automatic selection of optimal circuit on the basis of multilink loadings.**

6.3.1.1.5 Dynamic open port

The firewall shall be provided with dynamic open port and the specific technical requirements are as follows:

a) Support FTP in active mode and passive mode;

b) **Support video conference established by H.323 protocol;**

c) **Support SQL *NET database protocol.**

6.3.1.1.6 IP/MAC address binding

The firewall shall support the automatic or manual binding (by administrators) of IP /MAC address; it shall be able to inspect whether IP address is embezzled and intercept the visits of host embezzling IP address through the firewall.

6.3.1.1.7 Traffic and session management

6.3.1.1.7.1 Traffic statistics

The firewall shall be provided with traffic statistics functions:

a) The firewall can make correct traffic statistics according to IP address, network service, time and protocol type or their combination;

b) The firewall can output traffic statistical result in real time or in report form.

6.3.1.1.7.2 Bandwidth management

The firewall shall be provided with bandwidth management function and dynamically adjust client occupied bandwidth according to the policy and

network flow.

6.3.1.1.7.3 Connection control

The firewall shall be able to set maximum concurrent sessions number of single IP to prevent network performance from being influenced by a large amount of illegal connection.

6.3.1.1.7.4 Session management

The firewall shall be able to actively release occupied state table resource as the session is in non-active state for a while or after the session ends

6.3.1.1.8 Anti-denial of service attack

The firewall shall be provided with anti-denial of service attack and the specific technical requirements are as follows:

a) ICMP Flood attack;

b) UDP Flood attack;

c) SYN Flood attack;

d) TearDrop attack;

e) Land attack;

f) Ultra-large ICMP data attack.

6.3.1.1.9 Network scanning protection

The firewall shall be able to test and defend scanning action and the specific technical requirements are as follows:

a) Testing and recording scanning action include the scanning to all the firewalls and protected networks;

b) **Defend against scanning action.**

6.3.1.2 Application layer control

6.3.1.2.1 User control

The firewall shall be provided with network access control function on the basis of user /user group and the specific technical requirements for the user authentication methods it supports are specified as follows:

a) **Support local authentication methods;**

b) **Authenticate the system in conjunction with the third party, such as the**

authentication methods on the basis of radius and LDAP servers.

6.3.1.2.2 Application protocol control

The firewall shall be able to identify and control all kinds of application types and the specific technical requirements are as follows:

a) Common applications like HTTP, FTP, TELNET, SMTP and POP3;

b) **Instant chat, P2P streaming media, network streaming media, online game and stock software;**

c) **Escape or tunnel encryption;**

d) **User-defined application types.**

6.3.1.2.3 Application contents control

The firewall shall be able to identify and filter mainstream application contents and the specific technical requirements are as follows:

a) **Make an access control over document type on the basis of HTTP, FTP, SMTP and POP3 applications, including uploading and downloading documents;**

b) **Make an access control over keywords on the basis of HTTP, FTP, TELNET, SMTP and POP3 applications;**

c) **Applications of other types.**

6.3.1.2.4 Malicious code protection

The firewall shall be provided with malicious code detection function and the specific technical requirements are as follows:

a) **Support malicious code detection, such as worm virus, Trojan horse, website malicious code which are transported by at least http, IM, FTP and mail so as to monitor virus based on different protocols;**

b) **Filter malicious websites, built-in malicious website library, timely update and define malicious websites and classify illegal or harmful websites like adult type or gambling type;**

c) **Detect and intercept malicious codes accompanying HTTP webpage and email.**

6.3.1.2.5 Application attack protection

The firewall shall be provided with deep packet inspection function to defend against attacks from application layer and the specific technical requirements

1) Authorized administrator is only one to access to log;

2) Administrators shall be able to archive, delete and empty logs;

3) Provide tools to consult the logs, have capacity to search the audit events by time, date, subject ID and object ID and allow only authorized administrator to use the tools;

4) Support statistical analysis and report generation functions;

5) Audit events shall be stored in the nonvolatile medium in case of power down and the authorized administrator shall be informed when the memory space reaches threshold.

6.3.1.3.3 Security management

6.3.1.3.3.1 Management interface independence

The firewall shall be provided with independent management interface and separated from the service interfaces.

6.3.1.3.3.2 Security support system

Bottom support system of firewall shall meet the following requirements:

a) Be ensured that no redundant network service is provided by the support system;

b) Be free of security vulnerability which result in product authority loss and denial of service.

6.3.1.3.3.3 Exception handling mechanism

The firewall shall meet the following technical requirements when it is restarted from power down and forced shut-down and other abnormal conditions:

a) The security policy restores to the state saved before shutdown;

b) The log information will not lose;

c) Administrator re-authenticates.

6.3.1.3.4 High availability

6.3.1.3.4.1 Double-machine hot-standby

The firewall shall be provided with double-machine hot-standby; the standby firewall shall timely act and work in replace of main firewall when the main firewall is power off or under other faults.

6.3.1.3.4.2 Load balancing

The firewall shall support load balancing functions to balance network flow to different servers according to security policy.

6.3.2 Security Assurance Requirements

6.3.2.1 Configuration management

6.3.2.1.1 Partial configuration management automatization

Configuration management system shall provide one automatic mode to generate the products and ensure that only authorized modification can be made to the realization representation.

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

6.3.2.1.2 Configuration management capacity

6.3.2.1.2.1 Revision

The developer shall provide unique identification for the products versions.

6.3.2.1.2.2 Configuration item

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

Configuration management document shall include one configuration list which shall identify uniquely all the configuration items constituting products and describe them and methods to make a unique identification for configuration item and provide evidence of configuration items have been well maintained.

6.3.2.1.2.3 Authorization control

The configuration management document shall include one configuration management plan which shall describe how to use configuration management system. The configuration management shall correspond with the configuration management plan.

The developer shall provide evidence that all the configuration items are effectively maintained and ensure that configuration items will be modified only after the authorization.

6.3.2.1.2.4 Generation support and acceptance programs

The configuration management document provided by the developer shall include one acceptance plan which shall describe the programs to accept the modified or newly built configuration items constituting the products.

Configuration management system shall support the products generation.

6.3.2.1.3 Configuration management scope

6.3.2.1.3.1 Configuration management coverage

Configuration management scope shall at least include: realization representation, design document, test document, guiding document and configuration management document to ensure that modification is carried out in a correctly authorized and controllable mode.

Configuration management document shall be able to track above contents and describe how configuration management system tracks these configuration items.

6.3.2.1.3.2 Problems tracking configuration management coverage

Configuration management scope shall include security defect which shall be under the configuration management system.

6.3.2.2 Delivery and operation

6.3.2.2.1 Delivery programs

The developer shall deliver products by some delivery programs and document the delivery process.

Delivery document shall be described as all programs necessary to maintain security when delivering products versions to the users.

6.3.2.2.2 Modification detection

Delivery document shall describe how to provide multiple procedures and technically measures to detect the modification or main copying of the developer and any differences of versions received by the users. It shall also describe how to use multiple procedures to disguise into the developer and deliver products to user side as the developer does not deliver anything to the user side.

6.3.2.2.3 Installation, generating and starting programs

The developer shall provide installation, generating and starting programs of document description products.

6.3.2.3 Development

6.3.2.3.1 Functional specification

6.3.2.3.1.1 Non-formalized functional specification

following requirements:

a) **Non-formalized representation;**

b) **Describe rule and feature of security policy which can be modeled;**

c) **Contain rationality, namely demonstrate this model is consistent and complete against all the modeled security policy;**

d) **Clarify the correspondence between security policy model and functional specification, that's so say, demonstrate the security function in the functional specification is consistent and complete with respect to the security policy model.**

6.3.2.4 Instructive documents

6.3.2.4.1 Administrator manual

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

The Administrator manual shall cover the following contents:

a) Management function and interface which is accessible to administrators;

b) How to safely manage products;

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

d) All assumptions of users' behavior concerned with security operation;

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

f) Each security-related event concerned with management function, including modification to security characteristics of security function controlling entity;

g) All IT environmental security requirements concerned with administrators.

6.3.2.4.2 User guide

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

The user guide shall cover the following contents:

a) Security function and interface which are accessible to non-administrators of products;

b) Application method of security function and interface which is available to user;

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

d) Responsibility of users who shall bears in product security operation;

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

6.3.2.5 Life cycle support

6.3.2.5.1 Security measures identification

The developer shall provide development security documents.

Development security documents shall describe physical, procedural, personnel and otherwise security measures necessary to protect the product design and realize confidentiality and integrity in the development environment and shall provide an evidence to perform security measures in the product development and maintenance.

6.3.2.5.2 Developer defined life cycle model

The developer shall establish one life cycle model to make a necessary control over the development and maintenance of products and provide models described in the life cycle documents to develop and maintain products.

6.3.2.5.3 Well-defined development tool

The developer shall clearly define the product development tools and provide unambiguous definition of each statement and meaning of options in the development tool documents.

6.3.2.6 Testing

6.3.2.6.1 Testing coverage

6.3.2.6.1.1 Coverage evidence

The developer shall provide test coverage evidence.

The security function for testing and functional specification in test document are corresponding in test coverage evidence.

6.3.2.6.1.2 Coverage analysis

The developer shall provide analysis result on testing coverage.

The analysis result of testing coverage shall indicate it is complete correspondence between security function of product as described in testing

and function specification in testing documents.

6.3.2.6.2 Testing: high-level design

The developer shall provide testing depth analysis.

The depth analysis shall demonstrate that the tests identified in the test documents are enough to proof the function is also consistent with its high-level design.

6.3.2.6.3 Function testing

The developer shall test the security function and document the results and provide test document.

The test document shall include the following items:

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

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

c) Expected test result shall indicate the expected output after the successful test;

d) Actual test result shall indicate each security function to be test can operate as required.

6.3.2.6.4 Independent testing

6.3.2.6.4.1 Consistency

The developer shall provide products suitable for the test and use the same test suites as those in the self-check.

6.3.2.6.4.2 Sampling

The developer shall provide a group of equivalent resource for sampling testing of security function.

6.3.2.7 Vulnerability assessment

6.3.2.7.1 Misuse

6.3.2.7.1.1 Guide review

The developer shall provide instructive documents which shall meet the following requirements:

c) Abnormal message of other protocols.

6.4.2.4 Self-management under IPv6 network environment

Firewall shall support self-management under IPv6 network environment.

6.4.2.5 Support IPv6 transition network environment (optional)

6.4.2.5.1 Double protocol stack

Firewall shall support IPv4 /IPv6 double stack network environment and work normally under IPv4 /IPv6 double stack network environment.

6.4.2.5.2 Protocol conversion

Firewall shall support IPv4 / IPv6 network interconversion and work normally under protocol conversion network environment.

6.4.2.5.3 Tunnel

6.4.2.5.3.1 6 over 4

Firewall shall support 6 over 4 network environment and work normally under 6 over 4 network environment.

6.4.2.5.3.2 6 to 4

Firewall shall support 6 to 4 network environment and work normally under 6 to 4 network environment.

6.4.2.5.3.3 ISATAP

Firewall shall support ISATAP network environment and work normally under ISATAP network environment.

6.5 Performance Requirements

6.5.1 Throughput

Firewall throughput depends on the speed rate and the specific indexes are required as follows:

a) In case of no packet loss, a pair of ports shall reach two-way throughput index:

1) For 64-byte short packet, 10M and 100M firewall shall not be less than 20% of line-speed; 1000M and 100000M firewall shall not be less than 35% of line-speed;

2) For 512-byte middle long packet, 10M and 100M firewall shall not be less

than 70% of line-speed; 1000M and 100000M firewall shall not be less than 80% of line-speed;

3) For 1518-byte long packet, 10M and 100M firewall shall not be less than 90% of line-speed; 1000M and 100000M firewall shall not be less than 95% of line-speed.

b) In case of no packet loss, as for 1 518byte long packet of high-performance firewall, throughput reaches at least 80 Gbit/s;

c) For the firewall compatible with the next generation of internet, throughput under IPv6 network environment shall meet above-mentioned indexes.

6.5.2 Delay

Firewall delay depends on the speed rate and the specific indexes are required as follows:

a) As for 64-byte short packet, 512-byte middle long packet, 1518-byte long packet, 10M and 100M firewall delay shall not exceed 500μs at maximum ;

b) As for 64-byte short packet, 512-byte middle long packet, 1518-byte long packet, 1000M, 100000M and high-performance firewall delay shall not exceed 90μs at maximum;

c) For the firewall compatible with the next generation of internet, delay under IPv6 network environment shall meet above-mentioned indexes.

6.5.3 Maximum Concurrent Connections

Maximum concurrent connections depend on the speed rate and the specific indexes are required as follows:

a) Maximum concurrent connections of 10M firewall shall not be less than 1000;

b) Maximum concurrent connections of 100M firewall shall not be less than 10,000;

c) Maximum concurrent connections of 1000M firewall shall not be less than 100,000;

d) Maximum concurrent connections of 100000M firewall shall not be less than 1,000,000;

e) Maximum concurrent connections of high-performance firewall shall not be less than 8,000,000;

f) For the firewall compatible with the next generation of internet, maximum concurrent connections under IPv6 network environment shall meet above-mentioned indexes.

The test-evaluation methods and expected results of state inspection are as follows:

a) Test-evaluation methods:

1) Configure and start up the state inspection module of firewall;

2) Configure the packet filtering policy and allow the network session under specific condition to pass through firewall;

3) Generate a complete network session in compliance with this specific condition;

4) Generate one or more of data packets (not the first SYN packet from the connection request) in the network session in compliance with this specific condition.

b) Expected results:

1) The firewall makes access control according to the state table;

2) A complete network session in compliance with the above-mentioned specific condition can pass through the firewall;

3) One or more of data packets (not the first SYN packet from the connection request) in the network session in compliance with this specific condition cannot pass through the firewall.

7.2.1.1.4 Policy routing

The test-evaluation methods and expected results of policy routing are as follows:

a) Test-evaluation methods:

1) Configure the firewall policy routing according to the source and destination address parameters;

2) Generate corresponding network session and inspect the validity of policy routing.

b) Expected results:

1) The above-mentioned policy routing policy is supported;

2) The firewall policy routing works normally.

7.2.1.1.5 Dynamic open port

The test-evaluation methods and expected results of dynamic open port are as follows:

a) Test-evaluation methods:

1) Set the dynamic open port policy of firewall based on FTP application;

2) The intranet host accesses extranet through FTP (including active mode and passive mode), inspect whether the firewall can timely open the dynamic port used for FTP data connection and whether the network session connection is normal.

b) Expected results:

FTP works normally and dynamic port used for FTP data connection is opened.

7.2.1.1.6 IP/MAC address binding

The test-evaluation methods and expected results of IP/MAC address binding are as follows:

a) Test-evaluation methods:

1) Set up IP/MAC address binding policy for the firewall;

2) Bind the IP of intranet host with MAC address through automatic binding or manual binding function;

3) Generate sessions of correct IP/MAC binding and IP address embezzlement respectively to inspection the validity of binding.

b) Expected results:

1) IP/MAC address can be bound automatically or manually;

2) IP/MAC address after binding can correctly execute the security policy and discover IP address embezzlement.

7.2.1.1.7 Traffic and session management

7.2.1.1.7.1 Traffic statistics

The test-evaluation methods and expected results of traffic statistics are as follows:

a) Test-evaluation methods:

1) Configure firewall traffic statistical policy and generate corresponding network traffic;

2) Inspect whether the firewall can make traffic statistics and how to output the statistical result.

b) Expected results:

1) The firewall can make correct traffic statistics according to IP address, network service, time and protocol type or their combination;

2) The firewall can output traffic statistical result in real time or in report form.

7.2.1.1.7.2 Connection control

The test-evaluation methods and expected results of connection control are as follows:

a) Test-evaluation methods:

1) Configure the maximum concurrent sessions of single IP;

2) Initiate a large number of TCP connections from specified intranet host to extranet server or from extranet to DMZ server to make the connections of single IP exceed the set limit.

b) Expected results:

1) The firewall can set the maximum connections of single IP address;

2) The connections can be established normally if the TCP connections initiated from single IP address are within the range of set value;

3) TCP connections cannot be established again if the TCP connections initiated from single IP address exceed the set value.

7.2.1.1.8 Anti-denial of service attack

The test-evaluation methods and expected results of anti-denial of service attack are as follows:

a) Test-evaluation methods:

1) Configure and start up the anti-denial of service attack function of firewall;

2) Adopt simulated attack device, initiate firewall statement to support 10% of the bandwidth attack traffic (at least including ICMP Flood, UDP Flood, SYN Flood, TearDrop, Land and Ping of Death etc.) through firewall device, at the same time, establish normal TCP connection (new connection rate of 100 pcs/s) through firewall, and continue for 1min;

3) Inspect the passing ratio of denial of service attack packets and the ratio of successful establishment of normal TCP connections.

a) Test-evaluation methods:

1) Generate the following events and inspect whether the firewall records the following logs:

— Access the service of intranet and security zone from extranet and access the extranet, security zone and firewall itself from intranet;

— Initiate data packets prohibited by firewall security policy from intranet, extranet and security zone;

— Try to log in the firewall management port and make identity authentication;

— Add/delete/modify administrator, save/delete audit logs, modify security policy and configuration parameters etc.

— Forge IP data packets with IP packet simulator and generate nonstandard protocol data packets with the protocol types other than TCP, UDP and ICMP;

— Try to log in the firewall management port and make wrong operations such as inputting wrong password;

— Access UDP (such as DNS) and ICMP (such as ping) protocols for many times;

— Make FTP connection.

2) Try to access logs from local or remote management port as unauthorized administrator;

3) Log in as an authorized administrator, check whether the logs can be read, saved, deleted and cleaned;

4) Check whether the firewall can retrieve and sort audit events;

5) Check whether the firewall is provided with the function to backup audit records and whether the logs can be saved in safe and permanent places;

6) Test whether the firewall can only manage logs with log management tools;

7) Inspect the statistic analysis and report generation functions of firewall.

b) Expected results:

1) The firewall records the above-mentioned events exactly;

2) The unauthorized administrator can't access logs;

3) The authorized administrator can read, save, delete and clean the logs;

4) The firewall can retrieve and sort audit events;

5) The logs can be saved in safe places;

6) The firewall can only use log management tools to manage logs and ensure logs safe;

7) The firewall supports statistic analysis and report generation functions.

7.2.1.3.3 Security management

7.2.1.3.3.1 Management interface independence

The test-evaluation methods and expected results of management interface independence are as follows:

a) Test-evaluation methods:

1) Inspect whether the firewall is provided with independent management interface;

2) Inspect whether the firewall can close the management service of service interface.

b) Expected results:

1) The firewall can be configured with independent management interface;

2) The firewall can close the management service of service interface.

7.2.1.3.3.2 Security support system

The test-evaluation methods and expected results of security support system are as follows:

a) Test-evaluation methods:

1) Inspect documents and determine the open port declared by the firewall;

2) Make port and security scanning and analysis to the firewall with professional scanner.

b) Expected results:

1) All provided documents shall declare the open port and service of firewall;

2) The firewall does not open excessive ports and network services through port and security scanning;

3) The scanning result shall not include medium and high-risk security vulnerabilities.

7.2.1.3.3.3 Exception handling mechanism

The test-evaluation methods and expected results of exception handling mechanism are as follows:

a) Test-evaluation methods:

1) Record current state of the firewall, such as security policy etc., save configuration and connect the firewall through management interface;

2) Directly disconnect power supply of the firewall and connect the power supply again and start up;

3) Try to make management through the interface again and inspect the security policy, log information etc.

b) Expected results:

1) Once more identity authentication is required when checking the firewall policy configuration etc. through management interface again;

2) The security policy restores to the state saved before shutdown;

3) The log information before shutdown cannot lose.

7.2.2 Security Assurance Testing

7.2.2.1 Configuration management

7.2.2.1.1 Version number

The test-evaluation methods and expected results of version number are as follows:

a) Test-evaluation methods:

1) The valuator shall check whether the configuration management supporting documents provided by the developer are provided with version number and request that version number used by developer shall be in full equivalence with the product sample which it represents, without ambiguity;

2) The valuator shall inspect on site whether the product samples in configuration management activity are provided with unique version number and whether the version number is in full equivalence with the

completely.

b) Expected results:

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

7.2.2.3.2 Descriptive high-level design

The test-evaluation methods and expected results of descriptive high-level design are as follows:

a) Test-evaluation methods:

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

1) Represent in non-formalized form;

2) Be intrinsically consistent;

3) Describe structure of security function according to subsystems;

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

5) Identify any fundamental hardware, firmware and/or software as required by security function, and a representation of function provided by the supportive protection mechanism which is realized by them.

6) Identify all interfaces in security function subsystems;

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

b) Expected results:

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

7.2.2.3.3 Non-formalized correspondence verification

The test-evaluation methods and expected results of non-formalized correspondence verification are as follows:

a) Test-evaluation methods:

1) The valuator shall check whether the developer provides correspondence analysis among all the adjacency pairs represented by product security function.

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

3) Refine the product security function in functional design, and refine all the security function-related parts in relatively abstract product security function representation in relatively specific product security function representation.

b) Expected results:

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

7.2.2.4 Instructive documents

7.2.2.4.1 Administrator manual

The test-evaluation methods and expected results of administrator manual are as follows:

a) Test-evaluation methods:

The valuator shall check whether the developer provides the administrator manual for authorized administrator and whether this administrator manual includes the following contents:

1) Useable management functions and interfaces;

2) Usage of security functions and interfaces which are available to the administrator;

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

4) All assumptions of users' behavior concerned with security operation;

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

6) Every security-related event concerned with management function, including that security characteristics of body controlled by security function are modified;

7) All IT environmental security requirements concerned with authorized administrators.

b) Expected results:

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

7.2.2.4.2 User guide

The test-evaluation methods and expected results of user guide are as follows:

a) Test-evaluation methods:

The valuator shall check whether the developer provides the administrator manual for users and whether this user guide includes the following contents:

1) Security functions and interfaces which are accessible to non-administrative users;

2) Usage of security function and interface which is available to users;

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

4) Responsibilities which shall be undertook by users in product security operation;

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

b) Expected results:

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

7.2.2.5 Testing

7.2.2.5.1 Coverage evidence

The test-evaluation methods and expected results of **coverage evidence** are as follows:

a) Test-evaluation methods:

The valuator shall check the test coverage evidence provided by the developer and whether the test coverage evidence indicates that identified test in the test document is corresponding to product security function as described in functional specification.

b) Expected results:

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

7.2.2.5.2 Function testing

requirements and the firewall provided shall pass the vulnerability test.

7.3 Security Requirements Testing at Reinforced-grade

7.3.1 Security Function Testing

7.3.1.1 Network layer control

7.3.1.1.1 Packet filtering

The test-evaluation methods and expected results of packet filtering are as follows:

a) Test-evaluation methods:

1) Inspect the default security policy of firewall;

2) **Configure the packet filtering policy based on MAC address to generate corresponding network session;**

3) Configure the packet filtering policy based on source IP address and destination IP address to generate corresponding network session;

4) Configure the packet filtering policy based on source port and destination port to generate corresponding network session;

5) Configure the packet filtering policy based on protocol type to generate corresponding network session;

6) Configure the packet filtering policy based on time to generate corresponding network session;

7) Configure the user-defined packet filtering policy to generate corresponding network session, with the filtering condition being the combination of partial or all filtering conditions of 2)~6).

b) Expected results:

1) The firewall adopts the minimum security principle, i.e. forbid unless otherwise explicitly allowed;

2) The firewall can filter according to MAC address;

3) The firewall can filter according to source IP address and destination IP address;

4) The firewall can filter according to source port and destination port;

5) The firewall can filter according to protocol types;

6) The firewall can filter according to time;

7) The firewall can filter according to user-defined policy.

7.3.1.1.2 NAT

The test-evaluation methods and expected results of NAT are as follows:

a) Test-evaluation methods:

1) Set "many to one" and **"many to many" SNAT** respectively for intranet user to access extranet host, and inspect whether the intranet host can pass through the firewall and access extranet host;

2) Set the "one to many" DNAT for extranet user to access DMZ server, and inspect whether the extranet host can pass through the firewall and access DMZ server;

3) Set the protocol analyzer in intranet, extranet and DMZ, inspect the source address, destination address and information in header of the data packet before and after passing through the firewall NAT function to verify the validity of address translation function of the firewall.

b) Expected results:

1) The intranet host can access extranet host through SNAT;

2) The extranet host can access DMZ server through DNAT;

3) Realize "many to one" SNAT, **"many to many" SNAT**, "one to many" DNAT and correct transformation of source address and destination address of the data packet.

7.3.1.1.3 State inspection

The test-evaluation methods and expected results of state inspection are as follows:

a) Test-evaluation methods:

1) Configure and start up the state inspection module of firewall;

2) Configure the packet filtering policy and allow the network session under specific condition to pass through firewall;

3) Generate a complete network session in compliance with this specific condition;

4) Generate one or more of data packets (not the first SYN packet from the connection request) in the network session in compliance with this specific condition.

b) Expected results:

1) The firewall does access control according to the state table;

2) A complete network session in compliance with the above-mentioned specific condition can pass through the firewall;

3) One or more of data packets (not the first SYN packet from the connection request) in the network session in compliance with this specific condition cannot pass through the firewall.

7.3.1.1.4 Policy routing

The test-evaluation methods and expected results of policy routing are as follows:

a) Test-evaluation methods:

1) Configure firewall policy routing according to parameters such as source and destination address, **next-hop interface, protocol and port or application types**;

2) Generate corresponding network session and inspect the validity of policy routing;

3) **Generate relatively large load of traffic on different outer network links and inspect whether the optimal line can be selected automatically according to loading conditions.**

b) Expected results:

1) The above-mentioned policy routing policy is supported;

2) **The firewall can automatically select the outer network link with fewer loads;**

3) The firewall policy routing works normally.

7.3.1.1.5 Dynamic open port

The test-evaluation methods and expected results of dynamic open port are as follows:

a) Test-evaluation methods:

1) Set firewall dynamic open port policy to support the following applications;

2) The intranet host accesses extranet through FTP (including active mode and passive mode), inspect whether the firewall can timely open the dynamic port used for FTP data connection and whether the network session connection is normal;

b) Expected results:

1) The firewall can set the maximum connections of single IP address;

2) The connections can be established normally if the TCP connections initiated from single IP address are within the range of set value;

3) TCP connections cannot be established again if the TCP connections initiated from single IP address exceed the set value.

7.3.1.1.7.4 Session management

The test-evaluation methods and expected results of session management are as follows:

a) **Test-evaluation methods:**

1) **The firewall shall be provided with acquiescent session time-out mechanism, or require documents to describe the time-out end time of each protocol or configure the time-out end time of each protocol;**

2) **Initiate connection session from client host to server not passing through the firewall and confirm that the session will not be disconnected within the timeout set by the firewall;**

3) **Establish corresponding connection session from specified host of intranet to extranet server or from extranet to DMZ server and make no other operations to the session, check state of the session through the host.**

b) **Expected results:**

1) **The firewall shall be provided with acquiescent session time-out mechanism or may configure timeout end time for each protocol;**

2) **The session established by the test host within the timeout set by the firewall is in connection state.**

7.3.1.1.8 Anti-denial of service attack

The test-evaluation methods and expected results of anti-denial of service attack are as follows:

a) Test-evaluation methods:

1) Configure and start up the anti-denial of service attack function of firewall;

2) Adopt simulated attack device, initiate firewall statement to support 10%

of the bandwidth attack traffic (at least including ICMP Flood, UDP Flood, SYN Flood, TearDrop, Land and Ping of Death etc.) through firewall device, at the same time, establish normal TCP connection (new connection rate of 100 pcs/s) through firewall, and continue for 1min;

3) Inspect the passing ratio of denial of service attack packets and the ratio of successful establishment of normal TCP connections.

b) Expected results:

1) The firewall is provided with anti-denial of service attack capacity;

2) The passing ratio of attack packets is no greater than 5% and the successful establishment ratio of normal connections is not less than 90%.

7.3.1.1.9 Network scanning protection

The test-evaluation methods and expected results of network scanning protection are as follows:

a) Test-evaluation methods:

1) Make port and vulnerability scanning to the business interface and management interface of the firewall respectively;

2) Configure all allow rules and make port and vulnerability scanning to protected network.

b) Expected results:

1) The firewall can inspect and record the scanning to all the interfaces and protected networks;

2) **The firewall can resist the scanning to protected networks.**

7.3.1.2 Application layer control

7.3.1.2.1 User control

The test-evaluation methods and expected results of user control are as follows:

a) **Test-evaluation methods:**

1) **Add user and user group at local firewall;**

2) **Configure third-party authentication server, configure and quote third-party authentication server on the firewall;**

3) **Configure user access control based on local authentication and**

third-party authentication server.

b) **Expected results:**

1) **The firewall can make user access control according to local authentication;**

2) **The firewall can make user access control according to third-party authentication server.**

7.3.1.2.2 Application protocol control

The test-evaluation methods and expected results of application protocol control are as follows:

a) Test-evaluation methods:

1) Configure and start up the application access control to the firewall;

2) Configure respectively to allow forbid common applications such as HTTP, FTP, TELNET, SMTP and POP3 etc.

3) **Configure respectively to allow and forbid instant chatting application, P2P streaming media application, network streaming media application, online game and stock software;**

4) **Configure respectively to allow and forbid application of escaping or tunnel encryption characteristics, such as HTTPS access, over-wall software, VPN access etc.;**

5) **Try user-defined application types and configure to allow and forbid user-defined applications.**

b) Expected results:

1) The firewall is provided with the application access control function;

2) The firewall can make access control based on common applications such as HTTP, FTP, TELNET, SMTP and POP3 etc.; instant chatting application, P2P streaming media application, network streaming media application, online game and stock software; application with the characteristics of escaping or tunnel encryption; and user-defined application types.

7.3.1.2.3 Application contents control

The test-evaluation methods and expected results of application contents control are as follows:

a) **Test-evaluation methods:**

5) Input wrong password during the login process, after the maximum number of failures (such as 5) set by the firewall is reached, check whether the firewall can terminate the trusted hosts or users to establish sessions and forbid the failed users to access;

6) Check whether the management information of firewall is secure with the protocol analyzer;

7) Check whether the firewall supports encrypted remote management style and whether the unencrypted remote management style may be closed;

8) Check whether the firewall supports to distinguish the administrator roles.

b) Expected results:

1) The firewall supports both the local management style and the remote management style;

2) The administrator needs to pass through the identity authentication like password authentication and there are requirements for password strength;

3) **The firewall supports two-factor authentication;**

4) The firewall ensures to make unique identification to the administrator, host and user etc. before operation of the administrator;

5) After the maximum number of failures (such as 5) set by the firewall is reached, the firewall terminates the trusted hosts or users to establish sessions and forbid the failed users to access;

6) The sessions between administrator and firewall in remote management are secure;

7) The firewall supports the remote management session not in plaintext and the remote management style in plaintext may be closed.

8) The firewall administrators at least include and configuration management audit administrators and mutually independent authorities.

7.3.1.3.2 Security audit

The test-evaluation methods and expected results of security audit are as follows:

a) Test-evaluation methods:

1) Generate the following events and inspect whether the firewall records the following logs:

— Access the service of intranet and security zone from extranet and access the extranet, security zone and firewall itself from intranet;

— Initiate data packets prohibited by firewall security policy from intranet, extranet and security zone;

— Try to log in the firewall management port and make identity authentication;

— Add/delete/modify administrator, save/delete audit logs, modify security policy and configuration parameters etc.

— Forge IP data packets with IP packet simulator and generate nonstandard protocol data packets with the protocol types other than TCP, UDP and ICMP;

— Try to log in the firewall management port and make wrong operations such as inputting wrong password;

— Access UDP (such as DNS) and ICMP (such as ping) protocols for many times;

— Make FTP connections;

— Initiate attacks from extranet area.

2) Try to access logs from local or remote management port as unauthorized administrator;

3) Log in as an authorized administrator, check whether the logs can be read, saved, deleted and cleaned;

4) Check whether the firewall can retrieve and sort audit events;

5) Check whether the firewall is provided with the function to backup audit records and whether the logs can be saved in a safe and permanent place;

6) Test whether the firewall can only manage logs with log management tools;

7) Inspect the statistic analysis and report generation function of firewall.

b) Expected results:

1) The firewall records the above-mentioned events exactly;

2) The unauthorized administrator can't access logs;

3) The authorized administrator can read, save, delete and clean the logs;

4) The firewall can retrieve and sort audit events;

5) The logs can be saved in safe places;

6) The firewall can only use log management tools to manage logs and ensure logs safe;

7) The firewall supports statistic analysis and report generation functions.

7.3.1.3.3 Security management

7.3.1.3.3.1 Management interfaces independence

The test-evaluation methods and expected results of management interfaces independence are as follows:

a) Test-evaluation methods:

1) Inspect whether the firewall is provided with independent management interface;

2) Inspect whether the firewall can close the management service of service interface.

b) Expected results:

1) The firewall can be configured with independent management interface;

2) The firewall can close the management service of service interface.

7.3.1.3.3.2 Security support system

The test-evaluation methods and expected results of security support system are as follows:

a) Test-evaluation methods:

1) Inspect product documents and determine the open port declared by the firewall;

2) Make port and security scanning and analysis to the firewall with professional scanner.

b) Expected results:

1) All provided documents shall declare the open port and service of firewall;

2) The firewall does not open excessive ports and network services through port and security scanning;

The evidence contents of documents provided by the developer and site activities shall meet the above-mentioned requirements.

7.3.2.1.2 Configuration management capacity

7.3.2.1.2.1 Version number

The test-evaluation methods and expected results of version number are as follows:

a) Test-evaluation methods:

1) The valuator shall check whether the configuration management supporting documents provided by the developer are provided with version number and request that version number used by developer shall be full equivalence with the product sample which it represents, without ambiguity;

2) The valuator shall inspect on site whether the product samples in configuration management activity are provided with unique version number and whether the version number is in full equivalence with the product sample and description in configuration management supporting documents.

b) Expected results:

The evidence contents of documents provided by the developer and site activities shall meet the above-mentioned requirements.

7.3.2.1.2.2 Configuration item

The test-evaluation methods and expected results of configuration item are as follows:

a) Test-evaluation methods:

1) The valuator shall check whether the configuration management documents provided by the developer include configuration list and configuration management plan and whether the configuration list describes all the configuration items to compose the system;

2) The valuator shall inspect on site whether the configuration items in configuration management system are consistent with the description of configuration list, whether the configuration management system makes unique identification to each configuration item and whether the configuration management system maintains the configuration items;

3) The valuator shall check whether the configuration management documents provided by the developer describe the method to make unique identification to configuration items.

b) Expected results:

The evidence contents of documents provided by the developer and site activities shall meet the above-mentioned requirements.

7.3.2.1.2.3 Authorization control

The test-evaluation methods and expected results of authorization control are as follows:

a) **Test-evaluation methods:**

1) **The valuator shall check whether the configuration management plan documents provided by the developer describe the application method of configuration management system;**

2) **The valuator shall check on site whether configuration management activities conducted are consistent with the description of configuration management plan documents;**

3) **The valuator shall check evidences provided by the developer, which shall indicate that configuration items are maintained effectively. The valuator shall check on site whether the configuration items can be modified only through authorization.**

b) **Expected results:**

The evidence contents of documents provided by the developer and site activities shall meet the above-mentioned requirements.

7.3.2.1.2.4 Generation support and acceptance programs

The test-evaluation methods and expected results of generation support and acceptance programs are as follows:

a) **Test-evaluation methods:**

1) **The valuator shall check whether configuration management documents provided the developer include one acceptance plan and whether the acceptance plan describes the programs to accept the modified or newly built configuration items constituting the products.**

2) **The valuator shall check on site whether the configuration management system supports the product generation.**

b) **Expected results:**

The evidence contents of documents provided by the developer and site activities shall meet the above-mentioned requirements.

7.3.2.1.3 Configuration management scope

7.3.2.1.3.1 Configuration management coverage

The test-evaluation methods and expected results of configuration management coverage are as follows:

a) **Test-evaluation methods:**

1) **The valuator shall check whether the configuration management supporting documents provided by the developer describe the product configuration management scope which shall at least include configuration items such as product realization representation, design document, test document, instructive document, configuration management document etc. to ensure these configuration items are modified in a correct, authorized and controllable mode;**

2) **The valuator shall check on site whether the configuration management system used by the developer can at least track contents under the above-mentioned configuration management;**

3) **The valuator shall check whether the configuration management supporting documents provided by the developer describe the method of configuration management system to track configuration items.**

b) **Expected results:**

The evidence contents of documents provided by the developer and site activities shall meet the above-mentioned requirements.

7.3.2.1.3.2 Problems tracking configuration management coverage

The test-evaluation methods and expected results of problems tracking configuration management coverage are as follows:

a) **Test-evaluation methods:**

The valuator shall check whether the developer will incorporate security defects in configuration management scope and whether the developer tracks security defects.

b) **Expected results:**

The evidence contents of documents provided by the developer and site activities shall meet the above-mentioned requirements.

7.3.2.2 Delivery and operation

The test-evaluation methods and expected results of well-defined external interface are as follows:

a) **Test-evaluation methods:**

The valuator shall check whether the correspondence of functional specification and security function provided by the developer can represent security function completely and reasonably.

b) **Expected results:**

The documents provided by the developer shall meet above-mentioned requirements.

7.3.2.3.2 High-level design

7.3.2.3.2.1 Descriptive high-level design

The test-evaluation methods and expected results of descriptive high-level design are as follows:

a) Test-evaluation methods:

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

1) Represent in non-formalized form;

2) Be intrinsically consistent;

3) Describe security function construction according to subsystem;

4) Describe security functionality provided by each security function subsystem;

5) Identify any fundamental hardware, firmware or software as required by security function, and one representation of function provided by supportive protection mechanism which is realized by them;

6) Identify all interfaces of security function subsystem;

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

b) Expected results:

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

7.3.2.3.2.2 Security strengthened high-level design

The test-evaluation methods and expected results of security strengthened high-level design are as follows:

a) **Test-evaluation methods:**

1) **The valuator shall check whether the high-level design describes the purpose and method to use all interfaces of function subsystem and effects, exceptions and error message details in due course;**

2) **The valuator shall check whether the high-level design describes the system from two aspects: i.e. security policy implementation and other subsystems.**

b) **Expected results:**

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

7.3.2.3.3 Subset of security function realization

The test-evaluation methods and expected results of security function realization subset are as follows:

a) **Test-evaluation methods:**

The valuator shall check whether realization representation provided by the developer defines security function unambiguously and in detail so as to generate security function without further design. The realization representation shall be intrinsically consistent.

b) **Expected results:**

The documents provided by the developer shall meet above-mentioned requirements.

7.3.2.3.4 Descriptive low-level design

The test-evaluation methods and expected results of descriptive low-level design are as follows:

a) **Test-evaluation methods:**

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

1) **Represent in non-formalized form;**

2) **Be intrinsically consistent;**

3) **Describe security function according to modules;**

4) **Describe purpose of each module;**

5) **Define interrelationship among modules by the provided security function and dependence terms to other modules;**

6) **Describe how each security policy implementation function is provided;**

7) **Identify all interfaces of security function module;**

8) **Identify which interfaces are externally visible in security function modules;**

9) **Describe the purpose and method to use all the interfaces of security function modules and provide effects, exceptions and error message details in due course;**

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

b) **Expected results:**

The documents provided by the developer shall meet above-mentioned requirements.

7.3.2.3.5 Non-formalized correspondence verification

The test-evaluation methods and expected results of non-formalized correspondence verification are as follows:

a) Test-evaluation methods:

1) The evaluator shall check whether the developer provides corresponding analysis among all the adjacency pairs represented by product security function;

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

3) Refine the product security function in functional design, and refine all the security function-related parts in relatively abstract product security function representation in relatively specific product security function representation.

b) Expected results:

The test-evaluation methods and expected results of security measures identification are as follows:

a) **Test-evaluation methods:**

1) **The valuator shall check development security documents provided by the developer, and whether the documents describe all the physical, procedural, personnel and otherwise security measures necessary protect the system design and realize confidentiality and integrity in the system development environment;**

2) **The evaluation shall on site inspect the development environment of products and inspect whether the developer ensures the product design and accomplished confidentiality and integrity by physical, procedural, personnel and otherwise security measures and whether the security measures are implemented effectively.**

b) **Expected results:**

The documents provided by the developer shall meet above-mentioned requirements.

7.3.2.5.2 Developer defined life cycle model

The test-evaluation methods and expected results of developer defined life cycle model are as follows:

a) **Test-evaluation methods:**

1) **The developer shall provide an evidence that the life cycle model is used to make a necessary control over the development and maintenance of products and the valuator shall check the evidence;**

2) **The valuator shall check whether the life cycle definition documents provided by the developer describe the model to develop and maintain the product.**

b) **Expected results:**

The documents provided by the developer shall meet above-mentioned requirements.

7.3.2.5.3 Well-defined development tool

The test-evaluation methods and expected results of well-defined development tool are as follows:

a) **Test-evaluation methods:**

The valuator shall check whether the developer clearly defines the tools to develop the products and whether provides unambiguous definition of each statement and meaning of options in the development security documents.

b) **Expected results:**

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

7.3.2.6 Testing

7.3.2.6.1 Testing coverage

7.3.2.6.1.1 Coverage evidence

The test-evaluation methods and expected results of coverage evidence are as follows:

a) Test-evaluation methods:

The valuator shall check testing coverage evidence provided by the developer and check whether the evidence indicates it is complete correspondence between security function of product as described in functional specification and the testing identified in testing documents.

b) Expected results:

The documents provided by the developer shall meet above-mentioned requirements.

7.3.2.6.1.2 Coverage analysis

The test-evaluation methods and expected results of coverage analysis are as follows:

a) **Test-evaluation methods:**

1) **The valuator shall check testing coverage analysis result provided by the developer and check whether the analysis result indicates it is complete correspondence between security function of product as described in functional specification and the testing identified in testing documents;**

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

b) **Expected results:**

The documents provided by the developer shall meet above-mentioned requirements.

7.3.2.6.2 Testing: high-level design

The test-evaluation methods and expected results of testing depth are as follows:

a) **Test-evaluation methods:**

The valuator shall check whether the testing depth analysis provided by developer and whether it indicates that it is consistent between security function and high-level design according to the testing on the security function identified in the testing document.

b) **Expected results:**

The documents provided by the developer shall meet above-mentioned requirements.

7.3.2.6.3 Function testing

The test-evaluation methods and expected results of function testing are as follows:

a) Test-evaluation methods:

1) Whether the developer provides test documents including testing plan, testing specification, expected testing result and actual testing result;

2) Whether the developer identifies the security function being testing and describes testing the objective of testing in the testing plan;

3) Whether the developer identifies the testing to be executed, and describes the test overview of every security function, including the order dependency on other testing results in the testing specification;

4) Whether the expected testing result in the testing document provided by the developer indicates the expected output after the successful test;

5) Whether the actual testing result in the testing document provided by the developer indicates the each security function being tested can operate as required.

b) Expected results:

The documents provided by the developer shall meet above-mentioned requirements.

7.3.2.6.4 Independent testing

7.3.2.7.3.1 Vulnerability analysis for the developer

The test-evaluation methods and expected results of vulnerability analysis for the developer are as follows:

a) Test-evaluation methods:

1) The valuator shall check whether vulnerability analysis documents provided by the developer make analysis to all kinds of product functions from the obvious approach in which the users may damage security policy;

2) The valuator shall check whether the developer records explicitly measures taken to certain vulnerability;

3) To each vulnerability, the valuator shall check whether there is enough evidence to prove this vulnerability cannot be used in the product service environment.

b) Expected results:

The documents provided by the developer shall meet the above-mentioned requirements and the products provided shall pass the vulnerability test.

7.3.2.7.3.2 Independent vulnerability analysis

The test-evaluation methods and expected results of independent vulnerability analysis are as follows:

a) **Test-evaluation methods:**

The valuator shall carry out penetrability testing on the basis of vulnerability analysis documents provided by the developer and inspect whether the vulnerability of identified products can resist obvious penetrability attack.

b) **Expected results:**

The product resources provided by the developer shall meet the above-mentioned requirements and the products shall be able to resist identified penetrability attacks.

7.3.2.7.3.3 Intermediate resistibility

The test-evaluation methods and expected results of intermediate resistibility are as follows:

a) **Test-evaluation methods:**

The valuator shall analyze whether the products can resist the

penetrability attack of intermediate strength and whether the vulnerability searching is systematic according to vulnerability analysis documents provided by the developer and results of the independent penetrability testing.

b) **Expected results:**

The developer shall provide complete vulnerability analysis documents and the products shall be able to resist the penetrability attack of intermediate strength.

7.4 Environmental Adaptation Testing

7.4.1 Transmission Mode

7.4.1.1 Transparent mode

The test-evaluation methods and expected results of transparent mode are as follows:

a) Test-evaluation methods:

1) Configure the working mode of firewall as transparent (bridge) mode;

2) Configure the testing host addresses for intranet and extranet as the same network segment address;

3) Configure security policies like package filtering rules and inspect whether the firewall security policies are effective in transparent mode.

b) Expected results:

1) The firewall supports working in transparent (bridge) mode;

2) The firewall can work normally in transparent mode.

7.4.1.2 Routing mode

The test-evaluation methods and expected results of routing mode are as follows:

a) Test-evaluation methods:

1) Configure the working mode of firewall as routing mode;

2) Configure security policies like package filtering rules and inspect whether the firewall security policies are effective in transparent mode.

b) Expected results:

1) The firewall supports working in routing mode;

2) The firewall can work normally in routing mode.

7.4.2 Next Generation of Internet Support

7.4.2.1 Support pure IPv6 network environment

The test-evaluation methods and expected results of support pure IPv6 network environment are as follows:

a) Test-evaluation methods:

Simulate pure IPv6 network environment, detect whether the firewall can support pure IPv6 network environment and whether its security functions can work normally under pure IPv6 network environment.

b) Expected results:

The firewall can support pure IPv6 network environment and work normally under pure IPv6 network environment.

7.4.2.2 Protocol consistency

7.4.2.2.1 IPv6 Core protocol consistency

The test-evaluation methods and expected results of IPv6 Core protocol consistency are as follows:

a) Test-evaluation methods:

1) If the firewall works in routing mode, connect the firewall and protocol consistency tester in series;

2) Select IPv6 Core protocol consistency testing suite on protocol consistency tester, test the mandatory items and record the testing result;

3) If the firewall works in bridge mode, connect the firewall, protocol consistency tester and any one set of router in series;

4) Select IPv6 Core protocol consistency testing suite on protocol consistency tester, test the mandatory items and record the testing result;

5) Connect protocol consistency tester with router in series and test the IPv6 Core protocol consistency again;

6) Compare to see whether the two IPv6 Core protocol consistency results are consistent with each other.

b) Expected results:

1) If the firewall works in routing mode, all mandatory items in IPv6 Core

b) Expected results:

1) If the firewall works in routing mode, all mandatory items in IPv6 PMTU protocol consistency pass the testing;

2) If the firewall works in bridge mode, the two IPv6 PMTU protocol consistency results are consistent.

7.4.2.2.5 ICMPv6 protocol consistency

The test-evaluation methods and expected results of ICMPv6 protocol consistency are as follows:

a) Test-evaluation methods:

1) If the firewall works in routing mode, connect the firewall and protocol consistency tester in series;

2) Select ICMPv6 protocol consistency testing suite on protocol consistency tester, test the mandatory items and record the testing result;

3) If the firewall works in bridge mode, connect the firewall, protocol consistency tester and any one set of router in series;

4) Select ICMPv6 protocol consistency testing suite on protocol consistency tester, test the mandatory items and record the testing result;

5) Connect protocol consistency tester with router in series and test the ICMPv6 protocol consistency again;

6) Compare to see whether the two ICMPv6 protocol consistency results are consistent.

b) Expected results:

1) If the firewall works in routing mode, all mandatory items in ICMPv6 protocol consistency pass the testing;

2) If the firewall works in bridge mode, the two ICMPv6 protocol consistency results are consistent.

7.4.2.3 Protocol toughness

The test-evaluation methods and expected results of protocol toughness are as follows:

a) Test-evaluation methods:

7.4.2.5.2 Protocol conversion

The test-evaluation methods and expected results of protocol conversion are as follows:

a) Test-evaluation methods:

Simulate the network environment of IPv4 and IPv6 protocols interconversion and detect whether the firewall can support IPv4 and IPv6 protocols interconversion and work normally under IPv4/IPv6 protocol conversion network environment.

b) Expected results:

The firewall can support IPv4 and IPv6 protocols interconversion and work normally under IPv4/IPv6 protocol conversion network environment.

7.4.2.5.3 Tunnel

7.4.2.5.3.1 6over4

The test-evaluation methods and expected results of 6over4 are as follows:

a) Test-evaluation methods:

Simulate 6over4 tunnel network environment and detect whether the firewall can support 6over4 tunnel and work normally under 6over4 tunnel network environment.

b) Expected results:

The firewall can support 6over4 tunnel and work normally under 6over4 tunnel network environment.

7.4.2.5.3.2 6to4

The test-evaluation methods and expected results of 6to4 are as follows:

a) Test-evaluation methods:

Simulate 6to4 tunnel network environment and detect whether the firewall can support 6to4 tunnel and work normally under 6to4 tunnel network environment.

b) Expected results:

The firewall can support 6to4 tunnel and work normally under 6to4 tunnel network environment.

7.4.2.5.3.3 ISATAP

throughput for 64-byte, 512-byte and 1518-byte packets with performance tester.

b) Expected results:

The two-way average delay under 90% of the maximum throughput is not less than corresponding requirements in 6.5.2.

7.5.3 Maximum Concurrent Connections

The test-evaluation methods and expected results of maximum concurrent connections are as follows:

a) Test-evaluation methods:

1) Connect a pair of interfaces of the firewall with the performance tester;

2) Configure the working mode of the firewall as routing mode and configure one two-way all-pass rule;

3) Test the maximum TCP concurrent connections which can be maintained by the firewall with performance tester.

b) Expected results:

The testing result is not less than corresponding requirements in 6.5.3.

7.5.4 Maximum Connection Rate

The test-evaluation methods and expected results of maximum connection rate are as follows:

a) Test-evaluation methods:

1) Connect a pair of interfaces of the firewall with the performance tester;

2) Configure the working mode of the firewall as routing mode and configure one two-way all-pass rule;

3) Test the maximum TCP new connection rate of the firewall with performance tester.

b) Expected results:

The testing result is not less than corresponding requirements in 6.5.4.

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

_____ END _____

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

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