# GB

NATIONAL STANDARD OF THE

PEOPLE'S REPUBLIC OF CHINA

ICS 35.040

L 80

# GB/T 31505-2015

# Information security technology - Technique requirements and testing and evaluation approaches for host-based firewall and personal firewall

信息安全技术 主机型防火墙安全技术要求和测试评价方法

**Issued on: May 15, 2015** **Implemented on: January 01, 2016**

**Issued by: General Administration of Quality Supervision, Inspection and Quarantine;**

**Standardization Administration of PRC.**

# Table of Contents

Foreword ..... 3

1 Scope ..... 4

2 Normative references ..... 4

3 Terms and definitions ..... 4

4 Descriptions of host-based firewall and personal firewall ..... 5

5 Security technical requirements ..... 5

5.1 General description ..... 5

5.2 Basic level requirements ..... 6

5.3 Enhanced level requirements ..... 13

6 Test evaluation method ..... 26

6.1 Test environment ..... 26

6.2 Basic level test ..... 26

6.3 Enhanced level test ..... 41

# Information security technology - Technique requirements and testing and evaluation approaches for host-based firewall and personal firewall

## 1 Scope

This standard specifies the security technical requirements, evaluation methods, security classification of host-based firewalls.

This standard applies to the design, development and testing of host-based firewall and personal firewall.

## 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/T 18336.3-2008 Information technology - Security techniques - Evaluation criteria for IT security - Part 3: Security assurance requirements

GB/T 25069 Information security technology - Glossary

## 3 Terms and definitions

The terms and definitions as defined in GB/T 25069 as well as the following terms and definitions apply to this document.

**3.1**

**Host-based firewall and personal firewall**

It is also known the host-based firewall or personal firewall, which is a software which runs on standalone computer. It can monitor the inbound and outbound network connections on the host; perform network address-based and application-based access control through predefined rules. It also usually has other security functions such as anti-malware, intrusion detection, network alert, etc.

#### 5.2.1.5.3 Timeout lock or logout

The product shall have login timeout lock or logout function. If there is no operation within the set time period, the session is terminated; it needs the identity authentication again for the purpose of re-operation. The maximum timeout period can only be set by an authorized administrator.

### 5.2.1.6 Security management

#### 5.2.1.6.1 Identification uniqueness

The product shall provide a unique identifier for the user; at the same time associate the user's identifier with all auditable events of the user.

#### 5.2.1.6.2 Administrator attribute definition

If the product supports policy center for distributed deployment and centralized management, the policy center shall be able to divide the roles of administrators:

a) Administrator roles with at least two different permissions, such as security officer, auditor, etc.;

b) According to different functional modules, customize various different authority roles and assign roles to administrators.

#### 5.2.1.6.3 Remote management encryption

If the product supports the policy center and implements remote management of the temporary policy center, it shall take confidential measures to protect the remote management information implemented by the policy center.

#### 5.2.1.6.4 Trusted management host

If the product supports the policy center and the console provides remote management functions, it shall be able to limit the host addresses that can be remotely managed.

### 5.2.1.7 Security audit

The product shall have a security audit function; the specific technical requirements are as follows:

a) Type of recording event:

1) Network communication information matching packet filtering rules;

2) The administrator's login success and failure;

3) The operation of changing the security policy;

When delivering each version of the product to the user, the delivery document shall describe all procedures necessary to maintain security.

#### 5.2.2.2.2 Installation, generation, startup of program

The developer shall provide documentation explaining the process of product installation, generation and startup.

### 5.2.2.3 Development

#### 5.2.2.3.1 Description of informal function specification

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

a) Use informal styles to describe product security functions and external interfaces;

b) Is internally consistent;

c) Describe the purpose and usage of all external interfaces; provide details of effects, exceptions and error messages when appropriate;

d) Completely express product security functions.

#### 5.2.2.3.2 Descriptive high-level design

Developers shall provide high-level designs for product security functions; high-level designs shall meet the following requirements:

a) Representation shall be informal;

b) Is internally consistent;

c) Describe the structure of the security function based on subsystem;

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

e) Identify any basic hardware, firmware or software required by the security function, as well as a representation of the functions provided by the supporting protection mechanisms implemented in these hardware, firmware or software;

f) Identify all interfaces of the security function level;

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

packet. When the same type and code field are matched, it will be processed according to the packet processing method in the corresponding rule;

2) According to the local port (including single port and <or> port range) and <or> remote port (including single port and <or> port range) in the UDP network data packet, perform rule matching;

3) According to the local port (including single port and <or> port range) and <or> remote port (including single port and <or> port range) in the TCP network data packet, as well as the flag bit of the TCP data packet, perform rule matching filter.

d) Filter actions include:

1) Interception;

2) Access;

3) Continue to match the next rule.

#### 5.3.1.2 Revision of security rules

The product shall provide default security rules, which can be revised by users:

a) Users can choose to use or abandon the security rules as provided by the host-based firewall and personal firewall;

b) Users can add, delete, modify custom security rules according to the format requirements in 5.3.1.1.

#### 5.3.1.3 Application network access control

The security function of the product shall be able to control the permission of each application on the host to use the network; the control of application access to the network shall include the following three methods:

a) Access allowed: Allow the application to use the network;

b) Access prohibited: Prohibit the application from using the network;

c) Inquiry when accessing the network: When the application accesses the network, it shall be able to provide users with detailed reports and inquiries about the access operations it will perform; meanwhile it can accordingly handle the behavior of the application accessing the network according to the query results.

#### 5.3.1.4 Intrusion prevention

**c) It shall contain rationality, that is, to demonstrate that the model is consistent with all security policies that can be modeled and is complete;**

**d) It shall clarify the correspondence between the security policy model and the functional specification, that is, to demonstrate that the security functions in all functional specifications are consistent with the security policy model and are complete.**

#### 5.3.2.4 Guiding documents

##### 5.3.2.4.1 Administrator guide

The developer shall provide an administrator guide, which shall be consistent with all other documents provided for evaluation.

The administrator guide shall state the following:

a) Management functions and interfaces available to the administrator;

b) How to manage products securely;

c) Functions and permissions that shall be controlled in a secured processing environment;

d) All assumptions about user behavior related to the secured operation of the product;

e) All security parameters controlled by the administrator, if possible, it shall indicate the security value;

f) Every security-related event related to the management function, including changes to the security characteristics of the entity controlled by the security function;

g) All IT environment security requirements related to administrators.

##### 5.3.2.4.2 User guide

The developer shall provide a user guide, which shall be consistent with all other documents provided for evaluation.

The user guide shall state the following:

a) Security functions and interfaces available to non-administrator users of the product;

b) How to use the security functions and interfaces provided by the product

**The analysis result of the test coverage shall show that the correspondence between the test identified in the test document and the security function of the product described in the functional specification is complete.**

#### 5.3.2.6.2 Test: High-level design

The developer shall provide in-depth analysis of the test.

In-depth analysis shall confirm that the tests identified in the test document are sufficient to verify that the product's functionality is operating according to its high-level design.

#### 5.3.2.6.3 Function test

Developers shall test security functions, document the results and provide test documentation.

The test document shall include the following:

a) The test plan shall identify the security functions to be tested and describe the test objectives;

b) During the testing process, it shall identify the tests to be performed and describe the test overview of each security function; the test overview shall include the order dependency on other test results;

c) The expected test results shall show the expected output after the test is successful;

d) The actual test results shall show that each security function tested can operate in accordance with provisions.

#### 5.3.2.6.4 Independence test

##### 5.3.2.6.4.1 Consistency

Developers shall provide products suitable for testing; the test set provided shall be consistent with the test set used in self-testing product functions.

##### 5.3.2.6.4.2 Sampling

Developers shall provide a set of considerable resources for sampling testing of security functions.

### 5.3.2.7 Vulnerability assessment

#### 5.3.2.7.1 Misuse

1) Configure filtering rules based on different packet directions, to generate corresponding network sessions;

2) Configure filtering rules based on different remote IP addresses, to generate corresponding network sessions;

3) Configure filtering rules based on different protocol types, to generate corresponding network sessions;

4) Configure filtering rules for different filtering actions, to generate corresponding network sessions;

5) Configure user-defined filter rules, the filter condition is a combination of some or all of the above filter conditions, to generate the corresponding network session;

6) Record the test results and make a judgment on whether the results fully meet the requirements of the above-mentioned test evaluation methods.

b) Expected result:

The product shall be able to implement correct IP packet filtering according to the configured security rules.

#### 6.2.1.2 Revision of security rules

The test evaluation methods and expected results of the security rule revision of host-based firewall and personal firewall products are as follows:

a) Test evaluation method:

1) Perform network connectivity testing according to the default protection policy as provided by the product;

2) Change the default policy and perform the network connectivity test again, until it covers all the policy sets provided by the product;

3) Add, delete, modify custom security rules, to test network connectivity;

4) Record the test results and make a judgment on whether the results fully meet the requirements of the above-mentioned test evaluation methods.

b) Expected result:

The product shall be able to implement new security policies in accordance with the revised security rules.

2) It shall be ensured that each administrator ID is globally unique; it is not allowed to use one administrator ID for multiple administrators.

#### 6.2.1.6.2 Administrator attribute definition

The test evaluation methods and expected results defined by the administrator attribute of the host-based firewall and personal firewall products are as follows:

a) Test evaluation method: Check whether the security function of the system allows the definition of multiple roles of administrators. Record the test results and make a judgment on whether the results fully meet the requirements of the above-mentioned test evaluation methods.

b) Expected result:

1) The system shall allow administrators with multiple roles to be defined;

2) Each role can have multiple administrators; each administrator can only belong to one role;

3) It shall be ensured that each role identification is globally unique; one role identification is not allowed to be used for multiple roles.

#### 6.2.1.6.3 Remote management encryption

The test evaluation methods and expected results of remote management encryption for host-based firewall and personal firewall products are as follows:

a) Test evaluation method: Check whether the remote management data of the host-based firewall and personal firewall product is transmitted confidentially. Record the test results and make a judgment on whether the results fully meet the requirements of the above-mentioned test evaluation methods.

b) Expected result: The product can ensure the confidential transmission of remote management data.

#### 6.2.1.6.4 Trusted management host

The test evaluation methods and expected results of the trusted management host for host-based firewall and personal firewall products are as follows:

a) Test evaluation method: Check whether the host-based firewall and personal firewall product can restrict the host address that can be remotely managed. Record the test results and make a judgment on whether the results fully meet the requirements of the above-mentioned test evaluation methods.

- The content of the network communication information log matching the filtering rules shall include the following information: communication date and time, filtering action, remote IP address, local port, remote port, remarks;

- Other logs shall record the date, time, user identification, event description and results of the event; if remote login is used to manage the product, the log content shall include the address of the management host.

3) Log management:

- The host-based firewall and personal firewall product shall be able to query the content of the network communication information log matching the filtering rules according to the communication date and time, filtering actions, remote IP address, local port, remote port;

- The host-based firewall and personal firewall product shall be able to query other log content according to the date and time of the event, user identification, event description, result and other conditions;

- Restart the host after shutting down, the log record shall not disappear;

- When the remaining data storage space reaches the threshold, the host-based firewall and personal firewall product shall be able to provide an alarm function;

- Before the data storage space is exhausted, host-based firewall and personal firewall products shall be able to use automatic dumping and other methods to back up data to other storage spaces.

### 6.2.2 Security assurance evaluation

#### 6.2.2.1 Configuration management

##### 6.2.2.1.1 Version number

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

a) Test evaluation method:

1) The evaluator shall review whether the configuration management support file provided by the developer contains the following content: version number; the version number used by the developer shall be completely corresponding to the product sample that shall be

a) Test evaluation method:

The evaluator shall review the test coverage evidence provided by the developer. In the test coverage evidence, whether it shows that the test identified in the test document corresponds to the security function of the product described in the functional specification.

b) Expected result:

The content of the document provided by the developer shall meet the above requirements.

#### 6.2.2.5.2 Function test

The test evaluation methods and expected results of the functional test are as follows:

a) Test evaluation method:

1) The evaluator shall review the test documentation provided by the developer, to see whether it includes the test plan, test procedures, expected test results and actual test results;

2) The evaluator shall review whether the test plan identifies the security function to be tested and whether it describes the test objectives;

3) The evaluator shall review whether the test procedure identifies the test to be performed and whether it describes the test profile of each security function (the profile includes the order dependency on other test results);

4) The evaluator shall review whether the expected test results indicate the expected output after the test is successful;

5) The evaluator shall review whether the actual test results show that each tested security function can operate according to provisions.

b) Expected result:

The content of the document provided by the developer shall meet the above requirements.

#### 6.2.2.5.3 Independence test

##### 6.2.2.5.3.1 Consistency

The consistency test evaluation methods and expected results are as follows:

The testing and evaluation methods and expected results of developer vulnerability analysis are as follows:

a) Test evaluation method:

1) The evaluator shall review the vulnerability analysis document provided by the developer, to see whether it analyzes the various functions of the product from the obvious ways that the user may violate the security policy;

2) The evaluator shall review whether the developer clearly records the measures taken for the identified vulnerability;

3) For each vulnerability, the evaluator shall review whether there is sufficient evidence to prove that the vulnerability cannot be used in the environment where the product is used.

b) Expected result:

The documentation provided by the developer shall meet the above requirements.

## 6.3 Enhanced level test

### 6.3.1 Security function test

#### 6.3.1.1 IP packet filtering

The test evaluation methods and expected results of IP packet filtering of host-based firewall and personal firewall products are as follows:

a) Test evaluation method:

1) Configure packet filtering rules based on different packet directions, to generate corresponding network sessions;

2) Configure packet filtering rules based on different remote IP addresses, to generate corresponding network sessions;

3) Configure packet filtering rules based on different protocol types, to generate corresponding network sessions;

4) Configure packet filtering rules for different filtering actions, to generate corresponding network sessions;

5) Configure user-defined packet filtering rules, the filtering conditions are part or all of the combination of 1) ~ 5) filtering conditions, to generate

corresponding program access operations;

3) Ask when configuring an application to access the network, to generate the corresponding program access operation;

4) Record the test results and make a judgment on whether the results fully meet the requirements of the above-mentioned test evaluation methods.

b) Expected result:

The product shall be able to control the network access behavior of the application according to the access control rules.

#### 6.3.1.4 Rapid network cutoff/recovery

**The test evaluation methods and expected results of the rapid network cutoff/recovery of host-based firewall and personal firewall products are as follows:**

**a) Test evaluation method:**

**1) Desktop management: Perform rapid network recovery/cutoff operations, respectively;**

**2) Policy center: Randomly select some nodes, to perform rapid network recovery/cut-off operations on the selected nodes in the product policy center;**

**3) Record the test results and make a judgment on whether the results fully meet the requirements of the above test evaluation methods.**

**b) Expected result:**

**The product shall be able to execute corresponding policies based on rapid cutoff/recovery operations.**

#### 6.3.1.5 Intrusion prevention

The test evaluation methods and expected results of the intrusion prevention of host-based firewall and personal firewall products are as follows:

a) Test evaluation method:

1) Configure intrusion prevention rules; use network attack tools to simulate attacks, to check whether the product can correctly detect attacks;

#### 6.3.1.9.1 Identification uniqueness

The test evaluation methods and expected results of the uniqueness of the host-based firewall and personal firewall products are as follows:

a) Test evaluation method:

Check whether the security function of the system ensures that the defined administrator ID is globally unique. Record the test results and make a judgment on whether the results fully meet the requirements of the above-mentioned test evaluation methods.

b) Expected result:

1) The system shall allow multiple administrators to be defined;

2) It shall be ensured that each administrator ID is globally unique; it is not allowed to use one administrator ID for multiple administrators.

#### 6.3.1.9.2 Administrator attribute definition

The test evaluation methods and expected results of the administrator attribute definition of the host-based firewall and personal firewall products are as follows:

a) Test evaluation method:

Define multiple administrators who belong to different roles, to check whether the entered administrator information can be saved. Record the test results and make a judgment on whether the results fully meet the requirements of the above-mentioned test evaluation methods.

b) Expected result:

The system shall save the security attributes for each administrator, including: administrator identification, authentication data (such as password), authorization information or administrator group information, other security attributes, etc. The entered administrator information is not lost.

#### 6.3.1.9.3 Remote management encryption

The test evaluation methods and expected results of remote management encryption for host-based firewall and personal firewall products are as follows:

a) Test evaluation method:

Check whether the remote management data of the host-based firewall and personal firewall product is transmitted confidentially. Record the test

The test evaluation methods and expected results of the security audit of host-based firewall and personal firewall products are as follows:

a) Test evaluation method:

1) Simulate and generate various audit events;

2) Check the log content and format;

3) Perform log query, backup and other operations according to the product manual;

4) Record the test results and make a judgment on whether the results fully meet the requirements of the above-mentioned test evaluation methods.

b) Expected result

1) Type of recording event:

- Host-based firewall and personal firewall products shall be able to record network communication information that matches the filtering rules;

- The host-based firewall and personal firewall product shall be able to record identity authentication and measures taken to prohibit further attempts because the number of authentication failures exceeds the threshold;

- Host-based firewall and personal firewall products shall be able to record the addition, deletion, modification, deployment of security policies;

- The host-based firewall and personal firewall product shall be able to record the addition, deletion, modification of users and roles;

- Host-based firewall and personal firewall products shall be able to record, backup, delete logs;

- The host-based firewall and personal firewall product shall be able to record other operations of the administrator.

2) Log content:

- The content of the network communication information log matching the filtering rules shall include the following information: communication date and time, filtering action, remote IP address, local port, remote port, remarks;

**The content of on-site activity evidence provided by the developer shall meet the above requirements.**

#### 6.3.2.1.2 Configuration management capabilities

##### 6.3.2.1.2.1 Version number

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

a) Test evaluation method:

1) The evaluator shall review whether the configuration management support file provided by the developer contains the following content: version number; the version number used by the developer shall be completely corresponding to the product sample that shall be represented; meanwhile there is no ambiguity;

2) The evaluator shall check on site whether the product sample has a unique version number in the configuration management activities; whether the version number corresponds exactly to the description of the product sample and configuration management support documents.

b) Expected result:

The documents and on-site activity evidence provided by the developer shall meet the above requirements.

##### 6.3.2.1.2.2 Configuration items

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

a) Test evaluation method:

1) The evaluator shall review the configuration management document provided by the developer, to see whether it includes a configuration checklist and a configuration management plan. Whether the configuration list describes all the configuration items that make up the system;

2) The evaluator shall check on site whether the configuration items in the configuration management system are consistent with the description of the configuration list; whether the configuration management system uniquely identifies all configuration items; whether the configuration management system maintains the configuration items;

3) The evaluator shall review the configuration management document

verification are as follows:

a) Test evaluation method:

1) The evaluator shall review whether the developer provides a correspondence analysis between all adjacent pairs of product security function representation;

2) Among them, the correspondence between the various security function representations of the system (such as system function design, high-level design, low-level design, implementation representation) is an accurate and complete example of the security function representation requirements of the provided abstract product;

3) The product security function is refined in the functional design; all relevant security function parts of the more abstract product security function representation are refined in the more specific product security function representation.

b) Expected result:

The content of the document provided by the developer shall meet the above requirements.

**6.3.2.3.6 Informal product security policy model**

**The test evaluation methods and expected results of the informal product security policy model are as follows:**

**a) Test evaluation method:**

**The evaluator shall review the following content of the security policy model:**

**- Use informal style to express;**

**- Describe all the rules and characteristics of the security policy that can be modeled;**

**- It shall include rationality, that is, to demonstrate that the model is consistent with all security policies that can be modeled, and is complete;**

**- Clarify the correspondence between the security policy model and the functional specification, that is, demonstrate that the security functions in all functional specifications are consistent and complete for the security policy model.**

The evaluator shall review the test coverage evidence provided by the developer. In the test coverage evidence, whether it shows that the test identified in the test document corresponds to the security function of the product described in the functional specification.

b) Expected result:

The content of the document provided by the developer shall meet the above requirements.

**6.3.2.6.1.2 Coverage analysis**

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

**a) Test evaluation method:**

**1) The evaluator shall review the test coverage analysis results provided by the developer, to see whether it shows that the test identified in the test document corresponds to the security function described in the security function design;**

**2) Evaluate whether the test identified in the test document is complete.**

**b) Expected result:**

**The content of the document provided by the developer shall meet the above requirements.**

**6.3.2.6.2 Test: High-level design**

**The test evaluation methods and expected results of the test depth are as follows:**

**a) Test evaluation method:**

**The evaluator shall review the in-depth test analysis provided by the developer, to see whether the test on the security function identified in the test document is sufficient to show that the security function is consistent with the high-level design.**

**b) Expected result:**

**The content of the document provided by the developer shall meet the above requirements.**

**6.3.2.6.3 Function test**

The sampling test evaluation methods and expected results are as follows:

a) Test evaluation method:

The evaluator shall review whether the developer provides a set of equivalent resources for sample testing of security functions.

b) Expected result:

The resources provided by the developer shall meet the above requirements.

**6.3.2.7 Vulnerability assessment**

**6.3.2.7.1 Misuse**

**6.3.2.7.1.1 Guideline review**

**The test evaluation methods and expected results of the guideline review are as follows:**

**a) Test evaluation method:**

**1) The evaluator shall review the guidance documents and analysis documents provided by the developer, to see whether it explains all possible operation methods of the product (including operations after failure and operation errors); whether it have determined their consequences; whether it determines the significance of maintaining secured operation;**

**2) The evaluator shall review the guidance documents and analysis documents provided by the developer, to see whether it lists all the assumptions of the target environment and the requirements of all external security measures (including external program, physical or human control);**

**3) The evaluator shall review whether the documentation provided by the developer is complete, clear, consistent, reasonable;**

**4) Evaluate whether the analysis document provided by the developer is complete or not.**

**b) Expected result:**

**The documentation provided by the developer shall meet the above requirements.**

**6.3.2.7.1.2 Analysis confirmation**

3) For each vulnerability, the evaluator shall review whether there is sufficient evidence to prove that the vulnerability cannot be used in the environment where the product is used.

b) Expected result:

The documentation provided by the developer shall meet the above requirements.

#### 6.3.2.7.3.2 Independent vulnerability analysis

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

**a) Test evaluation method:**

**The evaluator shall perform a penetration test on the basis of the vulnerability analysis documentation provided by the developer, to verify whether the identified product vulnerability can withstand obvious penetration attacks.**

**b) Expected result:**

**The product resources provided by the developer shall meet the above requirements.**

#### 6.3.2.7.3.3 Intermediate resistance

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

a) Test evaluation method:

The evaluator shall analyze whether the product can withstand mid-strength penetrating attacks based on the vulnerability analysis documentation provided by the developer and the results of the independent penetration test; whether it indicates that the search for vulnerability is systematic.

b) Expected result:

Analysis records and final results (conformity/nonconformity); the developer shall provide a complete vulnerability analysis document.

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



**------ The End ------**