

ICS 35.040
CCS L 80



**NATIONAL STANDARD OF THE
PEOPLE'S REPUBLIC OF CHINA**

GB/T 31505-2015

**[Replaced by GB/T 20281-2020] 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

(English Translation)

Issued on: May 15, 2015

Implemented on: January 1, 2016

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

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

Foreword

This standard was drafted in accordance with the rules issued by GB/T 1.1-2009.

This standard was proposed by and shall be under the jurisdiction of the National Information Security Standardization Technical Committee (SAC/TC 260).

Drafting organizations of this standard. Computer Information System Security Product Quality Supervision and Inspection Center of the Ministry of Public Security, China Electronic Technology Standardization Research Institute, Beijing Venus Technology Co., Ltd., the Third Research Institute of the Ministry of Public Security.

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.

3.2

Security policy

It refers to provisions and policies related to management and protection of security domain routines.

4 Descriptions of host-based firewall and personal firewall

The host-based firewall and personal firewall is installed in the form of software on the end user's computer (including personal computers and servers), to prevent threats from the outside to the inside and from the inside to the outside.

The host-based firewall and personal firewall can not only monitor and control the network-level data flow, but also monitor and control the program, to

compensate the insufficiency of traditional defense methods such as gateway firewall and antivirus software. Generally, the host-based firewall and personal firewall on the server can also perform unified control over all nodes; implement unified security policies and responses.

5.1.1 Classification of security technical requirements

This standard divides the security technical requirements of host-based firewall and personal firewall into two major categories.

5.1.2 Security level

This standard divides the level of security function requirements according to the strength of the host-based firewall security function; divides the level of security assurance requirements according to GB/T 18336.3-2008.

5.2.1.2 Security policy revision

Products shall provide standardized security policies, which can be revised by users.

5.2.1.3 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 the application's access to the network shall include the following three methods.

5.2.1.5.1 Basic authentication

Before performing any functions related to the administrator, the product shall authenticate the user's identity.

5.2.1.5.2 Authentication failure handling

The product shall provide certain authentication failure handling measures, to prevent violent code cracking.

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

5.2.2.1.1 Version number

Developers shall provide unique identifiers for different versions of the product.

5.2.2.3.1 Description of informal function specification

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

5.2.2.3.3 Informal correspondence verification

The developer shall provide a correspondence analysis between all adjacent pairs of product security function representations.

For each adjacent pair represented by the product security function, the analysis shall explain that all related security functions represented by relatively abstract security functions shall be correctly and completely refined in the more specific security function representation.

6.1 Test environment

The test environment is as shown in Figure 1.

6.2.1.1 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.

6.2.1.3 Application network access control

The test evaluation methods and expected results of application network access control of host-based firewall and personal firewall products are as follows.

6.2.1.4 Intrusion prevention

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