

ICS 35.020
CCS L 80



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

GB/T 28451-2012

**Information security technology -- Technical requirements and
testing and evaluation approaches for network-based intrusion
prevention system products**

信息安全技术 网络型入侵防御产品技术要求和测试评价方法
(English Translation)

Issued on: June 29, 2012

Implemented on: October 1, 2012

**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 Abbreviations...	6
5 Technical requirements for intrusion prevention products.....	6
5.1 Description of composition...	6
5.2 Classification of functional and security requirements...	7
6 Composition of intrusion prevention products...	9
6.1 Intrusion event analysis unit...	9
6.2 Intrusion response unit...	9
6.3 Intrusion event audit unit...	9
6.4 Management control unit...	9
7 Technical requirements for intrusion prevention products.....	10
7.1 Level 1...	10
7.2 Level 2...	15
7.3 Level 3...	24
8 Evaluation methods of intrusion prevention products...	35
8.1 Test environment...	35
8.2 Test tool...	36
8.3 Level 1...	36
8.4 Level 2...	50
8.5 Level 3...	75
8.6 Performance test...	104

1 Scope

This standard specifies the functional requirements of network-based intrusion prevention products, the product's own security requirements, the product assurance requirements; it also proposes the classification requirements for intrusion prevention products.

This standard applies to the design, development, testing and evaluation of network-based intrusion prevention products.

2 Normative references

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

GB 17859-1999 Classified criteria for security protection of computer information system

GB/T 25069-2010 Information security technology - Glossary

3 Terms and definitions

The terms and definitions as defined in GB/T 25069-2010 and GB 17859-1999 as well as the following terms and definitions apply to this document.

3.1

Network-based intrusion prevention system products

It is a product that is deployed on a network path in the form of a bridge or a gateway, finds network behaviors with intrusive characteristics by analyzing network traffic, intercepts them before they enter the protected network.

This level specifies the minimum-security requirements for intrusion prevention products. The product has basic protocol analysis, intrusion detection and interception capabilities; generates records of intrusion events; restricts the control of product function configuration and data access through simple user identification and authentication, so that users have the ability to independently protect and prevent illegal users from harming the intrusion prevention products and protect the normal operation of intrusion prevention products.

5.1.2 Level 2

This level requires the division of security management roles, to refine the management of intrusion prevention products. The audit function is added, to make the actions of authorized administrators traceable. While the product realizes intrusion detection and interception, it also requires the function of timely warning. For event records, it also requires the ability to generate and output reports, as well as a hardware failure handling mechanism.

5.1.3 Level 3

This level requires intrusion prevention products to provide a general interface to the outside world; report results have functions such as template customization. It also requires functions such as multiple authentication mechanisms, upgrade security, self-hiding, load balancing; puts forward higher requirements for the product's own security. Provide strong

protection for the normal operation of the product.

5.1.4 Performance

This item specifies the performance requirements of intrusion prevention products, covering all levels.

5.2 Classification of functional and security requirements

The security classification of intrusion prevention products is as shown in Table

1 and Table 2. The grade evaluation of intrusion prevention products is based on Table 1 and Table 2, combined with the comprehensive evaluation of product assurance requirements. The intrusion prevention products that meet the level

1 requirements shall meet all the items that the level 1 products shall comply with as indicated in Table 1 and Table 2, as well as the relevant assurance requirements for the level 1 product. The intrusion prevention products that meet the level 2 requirements shall meet all the items that the level 2 products shall comply with as indicated in Table 1 and Table 2, as well as the relevant assurance requirements for the level 2 product. The intrusion prevention products that meet the level 3 requirements shall meet all the items that the level 3 products shall comply with as indicated in Table 1 and Table 2, as well

7.1.3.3.1 Function design

Developers shall provide documents explaining the security function design of intrusion prevention products.

Function design shall describe the security function and its external interface in an informal way; describe the purpose and method of using the external security function interface; provide details of exceptions and error messages when needed.

7.1.3.3.2 Representation correspondence

The developer shall provide a correspondence analysis between all adjacent pairs represented by the security function of the intrusion prevention product.

7.1.3.4 Guiding documents

7.1.3.4.1

Administrator guide

The developer shall provide the authorized administrator with an administrator guide including the following.

- a) Management functions and interfaces that can be used by intrusion prevention products;
- b) How to securely manage intrusion prevention products;

- c) The functions and permissions that shall be controlled in the secured processing environment;
- d) All assumptions about user behavior related to the secured operation of intrusion prevention products;
- 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 features of the entity controlled by the security function;
- g) All IT environment's security requirements related to authorized administrators.

The Administrator guide shall be consistent with all other documents provided for evaluation.

7.1.3.4.2

User guide a) The test document shall include the test plan, test procedures, expected test results, actual test results.

b) The test plan shall identify the security functions to be tested and describe the objectives of the test. The test procedure shall identify the test to be performed and describe the test profile of each security function, which includes the sequential dependence of other test results.

c) The expected test result shall indicate the expected output after the test is successful.

d) The actual test results shall show that each tested security function can operate according to requirements.

7.2.1.1 Requirements for intrusion event analysis function

7.2.1.1.1

Data collection

Intrusion prevention products shall have the ability to collect all data packets flowing into the target network in real time.

7.2.1.1.2

Protocol analysis

Intrusion prevention products shall perform protocol analysis on the collected data packets.

7.2.1.1.3

Intrusion discovery

Intrusion prevention products shall be able to detect intrusions in the protocol.