GB

NATIONAL STANDARD OF THE

PEOPLE'S REPUBLIC OF CHINA

ICS 35.020

L 80

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

Issued on: June 29, 2012 **Implemented on: October 01, 2012**

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

Standardization Administration of PRC.

Table of Contents

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

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 Level 2

7.2.1 Product functional 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.

7.2.1.1.4 Intrusion evasion discovery

Intrusion prevention products shall be able to detect behaviors that evade or deceive detection, such as IP fragment reassembly, TCP stream reassembly, protocol port relocation, URL string deformation, SHELL deformation, etc.

7.2.1.1.5 Traffic monitoring

Intrusion prevention products shall monitor abnormal traffic in the target environment.

7.2.1.2 Requirements for intrusion response function

7.2.1.4 Requirements for management control function

7.2.1.4.1 Management interface

Intrusion prevention products shall provide a user interface for management and configuration of intrusion prevention products. The management configuration interface shall contain all the functions needed to configure and manage the product.

7.2.1.4.2 Intrusion event library

Intrusion prevention products shall provide an intrusion event library. The event library shall include event name, detailed description, definition, etc.

7.2.1.4.3 Event classification

Intrusion prevention products shall classify events according to their severity, so that authorized administrators can capture dangerous events from a large amount of information.

7.2.1.4.4 Event definition

Intrusion prevention products shall allow authorized administrators to customize policy events.

7.2.1.4.5 Protocol definition

In addition to supporting the default network protocol set, intrusion prevention products shall also allow authorized administrators to define new protocols or relocate the protocol ports.

7.2.1.4.6 Traffic control

Intrusion prevention products have the function of controlling abnormal traffic.

7.2.1.4.7 Hardware failure handling

Intrusion prevention products shall provide hardware failure handling mechanisms.

7.2.1.4.8 Policy configuration

Intrusion prevention products shall provide functions to configure intrusion prevention strategies and response measures.

7.2.1.4.9 Product upgrade

Intrusion prevention products shall have the ability to update and upgrade product versions and event libraries.

7.2.3.3.1 Function design

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

The functional 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.

7.2.3.3.2 High-level design

Developers shall provide documents explaining the high-level design of the security functions of intrusion prevention products.

High-level design shall be expressed in an informal way and be internally consistent. In order to explain the structure of the security function, the high-level design shall decompose the security function into each security function subsystem for description; clarify how to separate the subsystem that helps to strengthen the security function of the intrusion prevention product from other subsystems. For each security function subsystem, the high-level design shall describe the security functions it provides; identify all its interfaces and which interfaces are externally visible; describe the purpose and methods of use of all its interfaces; provide the details of the functions, exceptions, error message of the security function subsystem. The high-level design shall also identify all the basic hardware, firmware, software required by the security of intrusion prevention products; support the protection mechanisms implemented by these hardware, firmware, or software.

7.2.3.3.3 Representation correspondence

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

7.2.3.4 Guiding documents

7.2.3.4.1 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 product administrators;

b) How to securely manage intrusion prevention products;

c) The functions and permissions that shall be controlled in the secured

development environment of the intrusion prevention product;

b) The development security documents shall also provide evidence of security measures implemented during the development and maintenance of intrusion prevention products.

7.2.3.6 Test

7.2.3.6.1 Scope

Developers shall provide analysis results of test coverage.

The analysis result of test coverage shall show that the test identified in the test document corresponds to the security function described in the security function design; meanwhile the correspondence is complete.

7.2.3.6.2 Test depth

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

In the in-depth analysis, it shall be stated that the test of the security function identified in the test document is sufficient to show that the security function is consistent with the high-level design.

7.2.3.6.3 Function test

Developers shall test security functions and provide the following test documents:

a) The test document shall include the test plan, test procedures, expected test results and 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 tests 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 show 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.

7.2.3.6.4 Independence test

The developer shall provide evidence to prove that the intrusion prevention product provided by the developer has been independently tested and passed by a third-party test.

deceive detection, such as IP fragment reassembly, TCP stream reassembly, protocol port relocation, URL string deformation, SHELL deformation.

7.3.1.1.5 Traffic monitoring

Intrusion prevention products shall monitor abnormal traffic in the target environment.

7.3.1.2 Requirements for intrusion response function

7.3.1.2.1 Interception capability

Intrusion prevention products shall intercept the discovered intrusion in advance, to prevent the intrusion from entering the target network.

7.3.1.2.2 Security alert

Intrusion prevention products shall take corresponding actions to issue security alerts when they discover and block intrusions.

7.3.1.2.3 Alert mode

The alert methods of intrusion prevention products should adopt one or more methods such as real-time screen prompts, E-mail alerts, sound alerts.

7.3.1.2.4 Event merge

Intrusion prevention products shall have the ability to combine alerts for the same security events that occur frequently to avoid alert storms.

7.3.1.3 Requirements for intrusion event audit function

7.3.1.3.1 Event generation

Intrusion prevention products shall be able to generate audit records in time for interception behavior.

7.3.1.3.2 Event record

Intrusion prevention products shall record and save intercepted intrusion events. The intrusion event information shall at least include the name of the event, the date and time of the event, the source IP address, source port, destination IP address, destination port, hazard level, etc.

7.3.1.3.3 Report generation

Intrusion prevention products shall be able to generate detailed results reports.

7.3.1.3.4 Report review

Intrusion prevention products shall ensure the security of the event library and version upgrade; ensure that the upgrade package is provided by the developer.

7.3.2.3.4 Self-hiding

Intrusion prevention products shall at least provide bridge access methods and take measures such as hiding IP addresses to make themselves invisible on the network, to reduce the possibility of being attacked.

7.3.2.4 Security audit

7.3.2.4.1 Audit data generation

Intrusion prevention products shall at least generate audit records for the following auditable events:

a) Attempt to log in to the intrusion prevention product management port and manage the identity authentication request;

b) All operations to change the security policy;

c) All attempts to modify security attributes.

At least the date and time of the event, the type of event, the identity of the subject, the result (success or failure) of the event shall be recorded in each audit record.

7.3.2.4.2 Audit review

Intrusion prevention products shall provide authorized administrators with the function of reading all audit information from audit records; they can sort audit records.

7.3.2.4.3 Restricted audit access

In addition to authorized administrators with clear read access rights, intrusion prevention products shall prohibit unauthorized users from reading audit records.

7.3.3 Product assurance requirements

7.3.3.1 Configuration management

7.3.3.1.1 Configuration management capabilities

Developers shall use configuration management systems and provide configuration management documents; meanwhile provide unique identification for different versions of intrusion prevention products.

7.3.3.2.2 Installation generation

Developers shall provide documentation explaining the installation, generation and activation of intrusion prevention products.

7.3.3.3 Security function development

7.3.3.3.1 Function design

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

The security 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.

7.3.3.3.2 High-level design

Developers shall provide documents explaining the high-level design of the security functions of intrusion prevention products.

The high-level design shall be expressed in an informal way and is internally consistent. In order to explain the structure of the security function, the high-level design shall decompose the security function into various security function subsystems for description; clarify how to separate the subsystems that help strengthen the product security function from other subsystems. For each security function subsystem, the high-level design shall describe the security functions it provides; identify all its interfaces and which interfaces are externally visible; describe the purpose and methods of use of all its interfaces; provide the details of functions, exceptions, error messages of the security function subsystem. The high-level design shall also identify all the basic hardware, firmware and software required by the security of intrusion prevention products; support the protection mechanisms implemented by these hardware, firmware or software.

7.3.3.3.3 Realization of security functions

Developers shall provide implementation representations for the selected subset of product security features.

The realization means that the product security function shall be defined unambiguously and in detail, so that a subset of the security function can be generated without further design. Implementation representation shall be internally consistent.

7.3.3.3.4 Low-level design

function;

g) All IT environment security requirements related to authorized administrators.

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

7.3.3.4.2 User guide

The developer shall provide a user guide that includes the following:

a) Security functions and interfaces available to non-administrative users of intrusion prevention products;

b) The usage of security functions and interfaces provided by intrusion prevention products to users;

c) All functions and permissions that users can obtain but shall be controlled by the secured processing environment;

d) The responsibilities of users in the secured operation of intrusion prevention products;

e) All security requirements of the IT environment related to users.

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

7.3.3.5 Development security requirements

Developers shall provide development security documents including the following:

a) The development security documents shall describe the necessary physical, procedural, personnel and other aspects of the security measures necessary to protect the confidentiality and integrity of the design and implementation of the intrusion prevention product in the development environment of the intrusion prevention product;

b) The development of security documents shall also provide evidence of security measures implemented during the development and maintenance of intrusion prevention products.

7.3.3.6 Test

7.3.3.6.1 Scope

b) Test evaluation results

1) Intrusion prevention products shall be able to access the network by means of bridges or gateways;

2) Intrusion prevention products shall be able to obtain enough network data packets to analyze intrusion events.

8.3.1.1.2 Protocol analysis

Protocol analysis test:

a) Test evaluation method

1) Check the security policy configuration document of the intrusion prevention product; check whether the description of the security event has attributes such as protocol type;

2) Check the product manual; find the description of the protocol analysis method; take sample to generate protocol events according to the protocol analysis type declared by the product, to form the attack event test set;

3) Configure the product's intrusion prevention strategy as the maximum strategy set;

4) Send all events in the attack event test set; record the product's detection results.

b) Test evaluation results

1) Record the corresponding attack name and type of the product intercepted intrusion;

2) The protocol events that can be monitored in the product manual mainly include the following types: ARP, ICMP, IP, TCP, UDP, RPC, HTTP, FTP, TFTP, SNMP, TELNET, DNS, SMTP, POP3, NETBIOS, NFS, SMB, MSN, P2P, etc.; sampling test shall not find any contradictions;

3) List all intrusion analysis methods supported by the product.

8.3.1.1.3 Intrusion discovery

Intrusion discovery test

a) Test evaluation method

1) Configure the intrusion prevention strategy of the intrusion prevention

b) Test evaluation results

1) Be able to successfully intercept the intrusion;

2) It shall be able to record the corresponding attacks of intercepted intrusions.

8.3.1.3 Intrusion event audit function test

8.3.1.3.1 Event generation

Event generation test:

a) Test evaluation method

1) Log in to the console interface;

2) Check the management interface, to see if the intrusion interception situation can be viewed in real time and clearly.

b) Test evaluation results

1) Has a display interface for viewing intrusion interception events;

2) The display interface has a clear functional area, which can display detailed information of intercepted events.

8.3.1.3.2 Event record

Event recording test:

a) Test evaluation method

1) Log in to the console interface;

2) View the detailed information of the recorded interception event on the display interface.

b) Test evaluation results

The detailed information of the intercepted event displayed on the display interface shall include the name of the event, the date and time the event occurred, the source IP address, the source port, the destination IP address, the destination port, the damage level, etc.

8.3.1.4 Management control function test

8.3.1.4.1 Management interface

a) Test evaluation method

Check what hardware failure handling mechanism the intrusion prevention product has.

b) Test evaluation results

When the product hardware fails, it shall not affect the smoothness of the network.

8.3.1.4.5 Policy configuration

Strategy configuration test:

a) Test evaluation method

1) Log in to the product management interface, to view the default policy provided by the product;

2) Check whether to allow editing or modification to generate a new policy;

3) Check whether it can edit or modify the response measures of each policy.

b) Test evaluation results

1) The product shall provide a default strategy and can be directly applied;

2) Users shall be allowed to edit policies;

3) Has a wizard function for users to edit policies;

4) Support the import and export of policies;

5) Users shall be allowed to edit different response measures of the policies;

6) Record the types and names of policies provided by the product.

8.3.1.4.6 Product upgrade

Product upgrade test:

a) Test evaluation method

Check the upgrade method of the intrusion signature database.

b) Test evaluation results

1) The intrusion signature database can be manually or automatically

there is no ambiguity;

2) Configuration items. The configuration items are required to have a unique identification, so as to have a clearer description of the composition of intrusion prevention products.

b) Test evaluation results

For review records and final results (conformity/nonconformity), the developer shall provide a unique version number and configuration items.

8.3.3.2 Delivery and operation

Delivery and operation evaluation:

a) Test evaluation method

The evaluator shall review whether the developer has provided documentation explaining the process of installation, generation, startup, use of intrusion prevention products. Users can understand the installation, generation, startup and use process through this document.

b) Test evaluation results

The review records and final results (conformity/nonconformity) shall meet the requirements of the test evaluation method.

8.3.3.3 Security function development

8.3.3.3.1 Function design

Functional design evaluation:

a) Test evaluation method

The evaluator shall review whether the information provided by the developer meets the following requirements:

1) Functional design shall use informal styles to describe product security functions and their external interfaces;

2) The functional design shall be internally consistent;

3) The functional design shall describe the purpose and method of using all external product security functional interfaces; where appropriate, provide details of the results affecting exceptions and error messages;

4) The functional design shall completely express the product security function.

administrator guide includes the following:

1) Management functions and interfaces that can be used by intrusion prevention products;

2) How to securely manage intrusion prevention products;

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

4) All assumptions about user behavior related to the secured operation of intrusion prevention products;

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

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

7) All the security requirements of the IT environment related to authorized administrators.

b) Test evaluation results

Review records and final results (conformity/nonconformity), the review content of the evaluator includes at least seven aspects of the test evaluation method.

The administrator guide as provided by the developer shall be complete.

8.3.3.4.2 User guide

User guide evaluation:

a) Test evaluation method

The reviewer shall review whether the developer provides a user guide for users of intrusion prevention products; whether this user guide includes the following:

1) Security functions and interfaces available to non-administrative users of intrusion prevention products;

2) The usage of security functions and interfaces provided by intrusion prevention products to users;

3) All functions and permissions that users can obtain but shall be

codes, documents, prototypes.

b) Test evaluation results

Review records and final results (conformity/nonconformity); the review content of the evaluator includes at least four aspects of the test evaluation method.

The documentation provided by the developer shall be complete.

8.3.3.6 Test

8.3.3.6.1 Scope

Range evaluation:

a) Test evaluation method

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

b) Test evaluation results

Review records and final results (conformity/nonconformity); the test identified in the test document provided by the developer shall correspond to the security function described in the security function design.

8.3.3.6.2 Function test

Function test evaluation:

a) Test evaluation method

1) Evaluate whether the test documents provided by the developer include test plans, test procedures, expected test results, actual test results;

2) Evaluate whether the test plan identifies the security function to be tested and whether it describes the test objectives;

3) Evaluate whether the test procedure identifies the test to be performed; whether it describes the test profile of each security function (the profile includes the order dependence on other test results);

4) Evaluate whether the expected test result shows the expected output after the test is successful;

5) Evaluate whether the actual test results show that each tested security function can operate according to requirements.

b) Test evaluation results

1) Be able to successfully intercept the intrusion;

2) It shall be able to record the corresponding attacks of intercepted intrusions.

8.4.1.2.2 Security alert

Security warning test:

a) Test evaluation method

1) Select multiple events with different characteristics from the existing event library to form an attack event test set, to simulate intrusion attacks;

2) Trigger a specific security event in the product's intrusion prevention policy, to check whether there is interception alert information;

3) Check the information of the alert event.

b) Test evaluation results

1) It can display the alert information;

2) The detailed explanation of the event shall be easy to understand.

8.4.1.2.3 Alert mode

Alert mode test:

a) Test evaluation method

1) Log in to the product management interface, to view the selection of product alert methods;

2) Select various alert methods in turn, to test whether the alert can be made in the specified manner.

b) Test evaluation results

One or more of the alert methods including real-time screen prompts, sound alerts, SNMP trap messages, E-mail alerts, running specified applications can be adopted. Record and list all alert methods.

8.4.1.2.4 Event merge

Event merge test:

8.4.1.4.3 Event classification

Event classification test:

a) Test evaluation method

Check whether there is classification information for each event in the intrusion event database.

b) Test evaluation results

All events in the event library have classification information.

8.4.1.4.4 Event definition

Event definition test:

a) Test evaluation method

1) Check the intrusion prevention product settings, whether to provide a custom event interface; whether to allow the generation of new events based on the product default event modification;

2) Custom-generate new intrusion features;

3) Send the corresponding intrusion events according to the newly generated intrusion characteristics, to check whether the product can be intercepted.

b) Test evaluation results

1) Intrusion prevention products allow users to customize events, or can modify and generate new intrusion events based on product default events;

2) Intrusion prevention products can detect and intercept newly defined events.

8.4.1.4.5 Protocol definition

Protocol definition test:

a) Test evaluation method

1) Check the intrusion prevention product settings, whether to provide a custom protocol interface, whether to allow the generation of new protocols based on existing protocol modifications, whether to allow relocation and interception of protocol ports;

IP is locked.

b) Test evaluation results

1) Intrusion prevention products shall have the function of defining the maximum allowed number of failures for user authentication attempts;

2) Intrusion prevention products shall define corresponding measures to be taken when user authentication attempts fail for a specified number of consecutive times;

3) When the user authentication attempts fail for a specified number of consecutive times, the intrusion prevention product shall prevent the user from further attempts (such as locking the user or logging in to the IP).

4) The maximum number of failures can only be set by the authorized administrator; the log record shall include audit information for identifying failure handling measures.

8.4.2.1.3 Authentication data protection

Identification data protection test:

a) Test evaluation method

Check whether the intrusion prevention product allows only designated authorized users to view or modify the identification data.

b) Test evaluation results

Intrusion prevention products shall only allow designated authorized users to view or modify identity authentication data.

8.4.2.1.4 Timeout lock

Timeout lock test:

a) Test evaluation method

1) Check whether the intrusion prevention product has the function of re-authentication after the administrator login timeout;

2) Set the time period for administrator login timeout re-authentication, to check whether the intrusion prevention product terminates the session when the logged-in user has no operation within the set time period; whether the user needs to be authenticated again to be able to re-manage and use the product.

sort audit records.

8.4.2.4.3 Restricted audit access

Restricted audit review test:

a) Test evaluation method

Simulate authorized and unauthorized administrators to access audit records, to see whether the security function of intrusion prevention products allows only authorized administrators to access audit records.

b) Test evaluation results

Intrusion prevention products shall restrict access to audit records. Except for authorized administrators with clear read access rights, intrusion prevention products shall prohibit all other users from reading audit records.

8.4.3 Product assurance test

8.4.3.1 Configuration management

8.4.3.1.1 Configuration management capabilities

Configuration management capability evaluation:

a) Test evaluation method

The evaluator shall review whether the documentation provided by the developer contains the following:

1) Developers shall use configuration management systems and provide configuration management documents; meanwhile provide unique identifications for different versions of intrusion prevention products.

2) The configuration management system shall make a unique identification for all configuration items and ensure that configuration items can only be modified after authorization.

3) Configuration management documents shall include configuration lists and configuration management plans. The configuration list is used to describe the configuration items that make up the intrusion prevention product. In the configuration management plan, it shall describe how the configuration management system is used. The configuration management implemented shall be consistent with the configuration management plan.

products; provide product security function representation by supporting the protection mechanisms implemented by these hardware, firmware, or software.

b) Test evaluation results

Review records and final results (conformity/nonconformity); the review content of the evaluator includes at least five aspects of the test evaluation method. The high-level design content provided by the developer shall be accurate and complete.

8.4.3.3.3 Representation correspondence

Indicates corresponding evaluation:

a) Test evaluation method

The evaluator shall review whether the developer provides a correspondence analysis between all adjacent pairs of product security function representations. Among them, the correspondence between various security function representations of intrusion prevention products (such as intrusion prevention product function design, high-level design, low-level design, implementation representation) is an accurate and complete example of the abstract product security function representation requirements provided. Product security functions are refined in the functional design; all relevant security function parts of the more abstract product security function representations are refined in the more specific product security function representations.

b) Test evaluation results

Test records and final results (conformity/nonconformity); the review content of the evaluator includes at least four items: functional design, high-level design, low-level design, realization. The content provided by the developer shall be accurate and complete; meanwhile correspond to each other.

8.4.3.4 Guiding documents

8.4.3.4.1 Administrator guide

Administrator guide evaluation:

a) Test evaluation method

The reviewer shall review whether the developer provides an administrator guide for authorized administrators; whether this

the requirements of the high-level design.

8.4.3.6.3 Function test

Functional test evaluation:

a) Test evaluation method

1) Evaluate whether the test documents provided by the developer include test plans, test procedures, expected test results, actual test results;

2) Evaluate whether the test plan identifies the security function to be tested and whether it describes the test objectives;

3) Evaluate whether the test procedure identifies the test to be performed; whether it describes the test profile of each security function (the profile includes the order dependence on other test results);

4) Evaluate whether the expected test result shows the expected output after the test is successful;

5) Evaluate whether the actual test results show that each tested security function can operate according to requirements.

b) Test evaluation results

Test records and final results (conformity/nonconformity); the review content of the evaluator includes at least five aspects of the test evaluation method.

The content provided by the developer shall be complete.

8.4.3.6.4 Independence test

Independence test evaluation:

a) Test evaluation method

The evaluator shall review whether the developer provides an intrusion prevention product for testing; whether the provided intrusion prevention product is suitable for testing.

b) Test evaluation results

Test records and final results (conformity/nonconformity); developers shall provide intrusion prevention products suitable for third-party testing.

8.4.3.7 Vulnerability assessment

events after evasion processing;

3) Intrusion prevention products can intercept intrusion events after relocating protocol ports.

8.5.1.1.5 Traffic monitoring

Traffic monitoring test:

a) Test evaluation method

1) Turn on the traffic monitoring function of intrusion prevention products; define traffic events; view the traffic display interface;

2) Initiate large traffic access to a server, such as FTP;

3) Initiate heavy traffic access to a specific port (such as port 80).

b) Test evaluation results

1) It can display various abnormal traffic information;

2) Servers with large traffic (such as FTP traffic) can be displayed;

3) List the abnormal traffic monitoring content provided.

8.5.1.2 Intrusion response function test

8.5.1.2.1 Interception capability

Interception ability test:

a) Test evaluation method

1) Select multiple events with different characteristics to form an attack event test set (not less than 30% of the attack event library supported by the product), to test the defense capabilities of intrusion prevention products. The selected events shall include: Trojan horse backdoor events, denial of service events, buffer overflow events and other representative network attack events, to simulate intrusion attacks;

2) Configure the intrusion prevention policy of the intrusion prevention product as the maximum policy set;

3) Send all events in the attack event test set and record the test results.

b) Test evaluation results

1) Be able to successfully intercept the intrusion;

2) Set event merging rules to merge certain content, such as displaying only the event name of the alert information, the number of occurrences, the source IP (the purpose is to see how many times a certain event has occurred on this IP).

b) Test evaluation results

The product can merge similar alert events as needed.

8.5.1.3 Intrusion event audit function test

8.5.1.3.1 Event generation

Event generation test:

a) Test evaluation method

1) Log in to the console interface;

2) Check the management interface, to see if the intrusion interception situation can be viewed in real time and clearly.

b) Test evaluation results

1) It has a display interface for viewing intrusion interception events;

2) The display interface has a clear functional area, which can display detailed information of intercepted events.

8.5.1.3.2 Event record

Event recording test:

a) Test evaluation method

1) Log in to the console interface;

2) View the detailed information of the recorded interception event on the display interface.

b) Test evaluation results

The detailed information of the intercepted event displayed on the display interface shall include the name of the event, the date and time the event occurred, the source IP address, the source port, the destination IP address, the destination port, the level of damage.

8.5.1.3.3 Report generation

b) Test evaluation results

Intrusion prevention products shall be able to achieve load balancing of network traffic.

8.5.1.4.10 Policy configuration

Strategy configuration test:

a) Test evaluation method

1) Open the menu, to view the default policy provided by the product;

2) Check whether to allow editing or modification to generate a new policy;

3) Check whether it can edit or modify the response measures of each policy.

b) Test evaluation results

1) The product shall provide a default policy and can be directly applied;

2) Users shall be allowed to edit policies;

3) Has a wizard function for users to edit policies;

4) Support the import and export of policies;

5) Users shall be allowed to edit different response measures of the policies;

6) Record the types and names of policies provided by the product.

8.5.1.4.11 Product upgrade

Product upgrade test:

a) Test evaluation method

Check the version of the intrusion prevention product and the upgrade method of the intrusion signature database.

b) Test evaluation results

1) Intrusion prevention product's program version and intrusion signature database can be manually or automatically upgraded online;

2) Intrusion prevention products can still intercept events normally during the upgrade process.

2) Check whether the security function of the product can define that when user authentication attempts fail for a specified number of consecutive times, corresponding measures will be taken;

3) Try user authentication behaviors that have failed multiple times, to check whether the intrusion prevention product has taken corresponding measures after reaching the specified number of authentication failures;

4) Check whether the log records include audit information for authentication failure handling measures such as the user or the login IP is locked.

b) Test evaluation results

1) Intrusion prevention products shall have the function of defining the maximum allowed number of failures for user authentication attempts;

2) Intrusion prevention products shall define corresponding measures to be taken when user authentication attempts fail for a specified number of consecutive times;

3) When user authentication attempts fail for a specified number of consecutive times, the intrusion prevention product shall prevent the user from further attempts (such as locking the user or logging in to the IP);

4) The maximum number of failures can only be set by the authorized administrator; the log record shall include audit information for identifying failure handling measures.

8.5.2.1.3 Authentication data protection

Identification data protection test:

a) Test evaluation method

Check whether the intrusion prevention product allows only designated authorized users to view or modify the identification data.

b) Test evaluation results

Intrusion prevention products shall only allow designated authorized users to view or modify identity authentication data.

8.5.2.1.4 Timeout lock

Timeout lock test:

8.5.2.4.3 Restricted audit access

Restricted audit review test:

a) Test evaluation method

Simulate authorized and unauthorized administrators to access audit records, to see whether the security function of intrusion prevention products allows only authorized administrators to access audit records.

b) Test evaluation results

Intrusion prevention products shall restrict access to audit records. Except for authorized administrators with clear read access rights, intrusion prevention products shall prohibit all other users from reading audit records.

8.5.3 Product assurance test

8.5.3.1 Configuration management

8.5.3.1.1 Configuration management capabilities

Configuration management capability evaluation:

a) Test evaluation method

The evaluator shall review whether the documentation provided by the developer contains the following:

1) Developers shall use a configuration management system and provide configuration management documents; meanwhile provide unique identifications for different versions of the product;

2) The configuration management system shall uniquely identify all configuration items; ensure that configuration items can only be modified with authorization; it shall also support the generation of basic product configuration items;

3) Configuration management documents shall include configuration checklists, configuration management plans, acceptance plans. The configuration list is used to describe the configuration items that make up the product. In the configuration management plan, it shall describe how the configuration management system is used. The configuration management implemented shall be consistent with the configuration management plan. In the acceptance plan, it shall describe the procedure for accepting modified or newly created configuration items;

review that the product is controlled by configuration management.

8.5.3.2 Delivery and operation

8.5.3.2.1 Delivery

Delivery evaluation:

a) Test evaluation method

The evaluator shall review whether the developer uses a certain delivery procedure to deliver the product; use documents to describe the delivery process; the evaluator shall review whether the documentation delivered by the developer contains the following content:

1) When delivering each version of the product to the user, all procedures necessary to maintain security;

2) The version and edition description of the product version change control, the version and edition description of the actual product version change control, the version modification description of the monitoring product program;

3) The description on the detection method of attempting to pretend to be the developer sending the product to the user.

b) Test evaluation results

The test records and final results (conformity/nonconformity) shall meet the requirements of the test evaluation method. The developer shall provide a complete document describing all the delivery processes (document and program delivery), including the detailed version of the product, the version description, the method of identifying discovery of authorized modification; the evaluator performs review and confirm.

8.5.3.2.2 Installation generation

Installation generation evaluation:

a) Test evaluation method

The evaluator shall review whether the developer has provided documentation describing the process of product installation, generation, startup, use. Users can understand the installation, generation, startup, use process through this document.

b) Test evaluation results

a) Test evaluation method

The evaluator shall review whether the information provided by the developer meets the following requirements:

1) Security management of developers: Security rules and regulations for developers, security education and training systems and records for developers;

2) Security management of the development environment: The entrance and exit control system and records of the development site, the temperature and humidity requirements and records of the development environment, the fire prevention and anti-theft measures of the development environment, the licensing documents of the relevant state departments. The security products used in the development environment must be the product which complies with the relevant national regulations; provide corresponding certification materials;

3) Security management of development equipment: Development equipment's security management system, including development host's use management and records, equipment purchase, repair, disposal systems and records, Internet management, computer virus management and records, etc.;

4) Security management of development process and results: Systems and records for controlled management of product codes, documents, prototypes.

b) Test evaluation results

Test records and final results (conformity/nonconformity); the review content of the evaluator includes at least four aspects of the test evaluation method.

The documentation provided by the developer shall be complete.

8.5.3.6 Test

8.5.3.6.1 Scope

Range evaluation:

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

5) Evaluate whether the actual test results show that each tested security function can operate according to requirements.

b) Test evaluation results

Test records and final results (conformity/nonconformity); the review content of the evaluator includes at least five aspects of the test evaluation method.

The content provided by the developer shall be complete.

8.5.3.6.4 Independence test

Independence test evaluation:

a) Test evaluation method

The evaluator shall review whether the developer provides a product for testing and whether the product provided is suitable for testing.

b) Test evaluation results

Test records and final results (conformity/nonconformity); the developer shall provide products that are suitable for third-party testing.

8.5.3.7 Vulnerability evaluation

8.5.3.7.1 Guide review

Guide inspection evaluation:

a) Test evaluation method

The evaluator shall review the documentation provided by the developer to see if the following requirements are met:

1) Whether the evaluation document has determined all possible operation modes of the product (including the operation after failure and operation error); whether they have determined their consequences; whether they have determined the significance of maintaining secured operation;

2) Whether the evaluation document lists all the assumptions of the target environment and the requirements of all external security measures (including external procedural, physical or human control);

3) Whether the evaluation document is complete, clear, consistent, reasonable;

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

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