GB

NATIONAL STANDARD OF THE

PEOPLE'S REPUBLIC OF CHINA

ICS 35.040

L 80

GB/T 20281-2020

Replacing GB/T 20010-2005, GB/T 20281-2015, GB/T 31505-2015 and GB/T 32917-2016

Information Security Technology - Security Technical Requirements and Testing Assessment Approaches for Firewall

信息安全技术 防火墙安全

技术要求和测试评价方法

Issued on: April 28, 2020 **Implemented on: November 1, 2020**

Issued by: State Administration for Market Regulation;

Standardization Administration of the People's Republic of China.

Table of Contents

Information Security Technology - Security Technical Requirements and Testing Assessment Approaches for Firewall

1 Scope

This Standard specifies the classification, security technical requirements, and testing assessment methods for firewall.

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

2 Normative References

The following documents are indispensable to the application of this document. In terms of references with a specified date, only versions with a specified date are applicable to this document. In terms of references without a specified date, the latest version (including all the modifications) is applicable to this document.

GB/T 18336.3-2015 *Information Technology - Security Techniques - Evaluation Criteria for IT Security - Part 3: Security Assurance Components*

GB/T 25069-2010 *Information Security Technology - Glossary*

3 Terms and Definitions

What is defined in GB/T 25069-2010, and the following terms and definitions are applicable to this document.

3.1 Firewall

Firewall refers to a network security product that analyzes the passing data flow and implements access control and security protection functions.

NOTE: in accordance with different security purposes and implementation principles, it is generally divided into network-based firewall, WEB application firewall, database firewall and host-based firewall, etc.

3.2 Network-based Firewall

Network-based firewall is a network security product that is deployed between different security domains, analyzes the passing data flow, and possess network layer and application layer access control, and security protection functions.

possesses access control and security protection functions. It is mainly divided into network-based firewall, WEB application firewall, database firewall and host-based firewall, or a combination of them.

The security technical requirements of firewall are divided into four categories: security function requirements, self-security requirements, performance requirements and security assurance requirements. Specifically speaking, security function requirements propose specific requirements for the security functions that a firewall shall possess, including networking and deployment, network layer control, application layer control, attack protection, and security audit and analysis. Self-security requirements propose specific requirements for the security of firewall, including identity identification and authentication, management capabilities, management audit, management modes and security support system. Performance requirements stipulate the performance indexes that a firewall shall achieve, including throughput, delay, connection rate and number of concurrent connections. Security assurance requirements propose specific requirements for the life cycle process of a firewall, including development, guidance documents, life cycle support, testing and vulnerability assessment.

The level of firewall is divided into the basic level and the enhanced level. Security functions and the strength of its own security, as well as the level of security assurance requirements are the specific bases for classification. The level highlights the security characteristics. Specifically speaking, the content of security assurance requirements of basic-level products corresponds to Level-EAL2 of GB/T 18336.3-2015; the content of security assurance requirements of enhanced-level products corresponds to Level-EAL4+ of GB/T 18336.3-2015. The specific security technical requirements and classification of the various types of firewalls (hereinafter referred to as “products”) are detailed in Appendix A; the testing and assessment method, and classification are detailed in Appendix B.

6 Security Technical Requirements

6.1 Security Function Requirements

6.1.1 Networking and deployment

6.1.1.1 Deployment mode

The products shall support the following deployment mode:

a) Transparent transfer mode;

b) Routing forward mode;

c) Reverse proxy mode.

6.1.1.2 Routing

b) The virtual subsystem can respectively maintain the routing table, security policy and log system;

c) Limit the resource usage quota of the virtual subsystems.

6.1.1.4.2 Virtualization deployment

If the products are in the form of virtualization, then, they shall support deployment on a virtualization platform and accept unified management of the platform, which include, but are not limited to:

a) Support deployment on a virtualization platform, such as: VMware ESXi, KVM, Citrix Xenserver and Hyper-V, etc.

b) Combine the virtualization platform to achieve elastic extension and retraction of product resources; in accordance with the load of virtualization products, dynamically adjust the resources;

c) Combine the virtualization platform to achieve failure migration; when the virtualization products fail, they shall be able to implement automatic update and replacement.

6.1.1.5 IPv6 support (optional)

6.1.1.5.1 Support IPv6 network environment

If the products support IPv6, they shall support normal operation in IPv6 network environment, and be able to effectively operate their security function and self-security function.

6.1.1.5.2 Protocol consistency

If the products support IPv6, they shall satisfy the requirements for IPv6 protocol consistency, which at least include IPv6 core protocol, IPv6 NDP protocol, IPv6 Autoconfig protocol and ICMPv6 protocol.

6.1.1.5.3 Protocol robustness

If the products support IPv6, they shall satisfy the requirements for the robustness of IPv6 protocol and resist the attacks of malformed protocol packets in IPv6 network environment.

6.1.1.5.4 Support IPv6 transition network environment

If the products support IPv6, they shall support operation in one or multiple of the following IPv6 transition network environments:

a) Protocol translation: inter-translation between IPv4 and IPv6;

b) Tunnel: encapsulate IPv6 in IPv4 to traverse IPv4 network, such as: IPv6 over IPv4, IPv6 to IPv4, ISATAP, etc.

6.1.2 Network layer access

6.1.2.1 Access control

6.1.2.1.1 Packet filtering

The requirements for the products' packet filtering function are as follows:

a) Security policy shall adopt the principle of least security, namely, unless explicitly permitted, otherwise prohibited;

b) Security policy shall include source IP address and destination IP address-based access control;

c) Security policy shall include source port and destination port-based access control;

d) Security policy shall include protocol type-based access control;

e) Security policy shall include MAC address-based access control;

f) Security policy shall include time-based access control;

g) Support user-defined security policy, which includes some or all combinations of MAC address, IP address, port, protocol type and time.

6.1.2.1.2 Network address translation

The requirements for the products' network address translation are as follows:

a) Support SNAT and DNAT;

b) SNAT shall implement "many-to-one" address translation, so that when the internal network host accesses the external network, its source IP address is translated;

c) DNAT shall implement "one-to-many" address translation, which maps the IP address / port of DMZ to the legal IP address / port of the external network, so that the external network host can implement access to the DMZ server by accessing the mapped address and port;

d) Support dynamic SNAT technology; implement "many-to-many" SNAT.

6.1.2.1.3 State detection

The products shall support state detection technology-based packet filtering function

and have the capability of state detection.

6.1.2.1.4 Dynamic open port

The products shall support dynamic port opening of protocols, which include, but are not limited to:

a) FTP protocol;

b) Audio and video protocols, for example, H.232.

6.1.2.1.5 IP / MAC address binding

The products shall support automatic and manual binding of IP / MAC address. When the IP address and MAC address of the host are inconsistent with that in the IP / MAC binding table, the passage of the traffic shall be prevented.

6.1.2.2 Traffic management

6.1.2.2.1 Bandwidth management

The products shall support the function of bandwidth management and be able to adjust the bandwidth occupied by the client side in accordance with the policy, which includes, but is not limited to:

a) Impose restrictions based on source IP, destination IP, application type and traffic rate or total amount of traffic of a time period;

b) Set up guaranteed bandwidth in accordance with source IP, destination IP, application type and time period;

c) When the network is idle, automatically relieve the traffic limit; when the total bandwidth occupancy rate exceeds the threshold, automatically initiate the limit.

6.1.2.2.2 Control of number of connections

The products shall support restriction of the maximum number of concurrent sessions and the rate of newly established connections for a single IP, so as to prevent the generation of a large number of illegal connections from affecting network performance.

6.1.2.2.3 Session management

When a session is inactive for a certain time, or after a session ends, the products shall terminate the session.

6.1.3 Application layer control

6.1.3.1 User management and control

The products with a feature library shall support protection against other attacks from the application layer, which include, but are not limited to:

a) Operating system vulnerability protection;

b) Middleware vulnerability attack protection;

c) Control vulnerability attack protection.

6.1.4.6 Automated tool threat protection

The products with a feature library shall support the protection against attacks initiated by automated tools, which include, but are not limited to:

a) Network scanning behavior protection;

b) Application scanning behavior protection;

c) Protection of vulnerability exploitation tools.

6.1.4.7 Attack escape protection

The products shall support the detection and interception of attacks that have been processed by the escape technology.

6.1.4.8 External system collaborative protection

The products shall provide a linkage interface and be able to be linked with other network security products through the interface, for example, implementing security policy issued by other network security products.

6.1.5 Security audit, warning and statistics

6.1.5.1 Security audit

The products shall support the function of security audit, which includes, but is not limited to:

a) Log event type:

   1) Access requests matched by product security policy;

   2) Detected attack behavior.

b) Log content:

   1) The date and time of the occurrence of the event;

   2) The subject, object and description of the event, in which, data packet log includes protocol type, source address, destination address, source port

b) In real-time or in the form of reports, output statistical results.

6.1.5.3.2 Application traffic statistics

The products shall support a graphical interface to display application traffic, which includes, but is not limited to:

a) In accordance with IP, time period and application type, or a combination of the above conditions, conduct statistics of the application traffic;

b) In the form of reports, output statistical results;

c) Compare the statistical results of different time periods.

6.1.5.3.3 Attack event statistics

The products shall support a graphical interface to display attack events, which includes, but is not limited to:

a) In accordance with attack event type, IP and time period, or a combination of the above conditions, conduct statistics of the attack event;

b) In the form of reports, output statistical result.

6.2 Self-security Requirements

6.2.1 Identity identification and authentication

The security requirements for the products' identity identification and authentication include, but are not limited to:

a) Identification and authentication of user's identity; the identity label is unique;

b) Security protection of user identity authentication information; guaranteed confidentiality of the user's authentication information during the storage and transfer process;

c) It shall have the function of login failure processing, such as: limiting the number of consecutive illegal login attempts and other related measures;

d) It shall have the function of login timeout processing, which automatically logs out when the login connection times out;

e) When password-based identity authentication is adopted, it is required to check the complexity of the password set by the user, so as to ensure that the user password meets certain complexity requirements;

f) When there is a default password in the product, it shall prompt the user to modify the default password, so as to reduce the risk of the user's identity

6.2.4 Management mode

The security requirements for the products' management mode include, but are not limited to:

a) Support local management through console port;

b) Support remote management through the network interface, and can limit the IP and MAC addresses for remote management;

c) During the remote management process, all communication data between the management side and the products shall be transferred in non-plain text;

d) Support the monitoring and management of SNMP network management protocol;

e) Support the separation of management interface and business interface;

f) Support centralized management; through the centralized management platform, implement the monitoring of the operating status, issue security policy, upgrade system versions and feature library versions.

6.2.5 Security support system

The security requirements for the products' support system include, but are not limited to:

a) Make necessary cuts without providing redundant components or network services;

b) During the restart process, the security policy and log information shall not be lost;

c) Do not contain already-known medium and high-risk security vulnerabilities.

6.3 Performance Requirements

6.3.1 Throughput

6.3.1.1 Network layer throughput

The network layer throughput of hardware products varies with products of different rates. See the specific index requirements below:

a) The bi-directional throughput rate index that a pair of ports with corresponding rates shall achieve:

1) In terms of 64-byte short packets, 100 M products: not less than 20% of linear speed; 1 G and 10 G products: not less than 35% of linear speed;

6.4.1 Development

6.4.1.1 Security architecture

The developer shall provide a security architecture description of the products' security functions. The security architecture description shall satisfy the following requirements:

a) Consistent with the scope of the description of security functions in the product design document;

b) Thoroughly describe the self-protection and non-bypassing security mechanism adopted by the products.

6.4.1.2 Functional specification

The developer shall provide a complete functional specification description, which shall satisfy the following requirements:

a) In accordance with the product type, clearly describe the security functions defined in 6.1 and 6.2;

b) Identify and describe the purpose, usage and related parameters of all the security function interfaces of the products;

c) Describe all behaviors related with the security function interfaces during the implementation of the security functions;

d) Describe all direct error messages that might be caused by the invocation of the security function interfaces.

6.4.1.3 Product design

The developer shall provide a product design document, which shall satisfy the following requirements:

a) Through the subsystems, describe the product structure, identify and describe all subsystems of the products' security functions; describe the interactions among the subsystems;

b) Provide the correspondence between the subsystems and the security function interfaces;

c) Through the implementation module, describe the security functions, identify and describe the purpose, related interfaces and return values of the implementation module; describe the interface that implements the interactions and invocations among the modules;

d) Provide the correspondence between the implementation module and the

a) Provide unique identification for different versions of products;

b) Use the configuration management system to maintain and uniquely identify all configuration items that constitute the products;

c) Provide a configuration management document, which describes the method used to uniquely identify configuration items;

d) The configuration management system provides an automatic mode to support the generation of the products; through automated measures, ensure that the configuration items merely accept authorized changes;

e) The configuration management document includes a configuration management scheme, which describes the procedure used to receive modified or newly established configuration items as a constituent part of the products. The configuration management scheme describes how to use the configuration management system to develop the products, and the configuration management implemented by the developer shall eb consistent with the configuration management scheme.

6.4.3.2 Scope of configuration management

The developer shall provide a list of product configuration items and state the developer of the configuration items. The list of product configuration items shall include the following content:

a) Evaluation basis of products and their constituent parts, and security assurance requirements;

b) Implementation expression, security defect report and its solution status.

6.4.3.3 Delivery procedure

The developer shall adopt a certain delivery procedure to deliver the products and document the delivery process. When delivering various versions of the products to the user, the delivery document shall describe all procedures necessary to maintain security.

6.4.3.4 Development security

The developer shall provide a development security document. The development security document shall describe all physical, procedural, personnel and other aspects of security measures necessary to protect the confidentiality and integrity of product design and implementation in the product development environment.

6.4.3.5 Definition of life cycle

The developer shall establish a life cycle model to implement necessary control of

b) Expected results:

1) Under the transparent transfer mode, the security policies take effect;

2) Under the routing forward mode, the security policies take effect;

3) Under the reverse proxy mode, the security policies take effect.

c) Result determination:

When the actual testing and assessment result is consistent with the relevant expected result, it shall be determined to be conformant, otherwise, it shall be determined to be non-conformant.

7.2.1.2 Routing

7.2.1.2.1 Static routing

The testing and assessment methods of static routing are as follows:

a) Testing and assessment methods:

1) Set up a static route in the products;

2) Send data packets matching the above-mentioned routing policy to the products.

b) Expected results:

1) The products support the set static route;

2) The products forward the data packets matching the policy in accordance with the routing policy.

c) Result determination:

When the actual testing and assessment result is consistent with the relevant expected result, it shall be determined to be conformant, otherwise, it shall be determined to be non-conformant.

7.2.1.2.2 Policy routing

The testing and assessment methods of policy routing are as follows:

a) Testing and assessment methods:

1) Set up a source and destination IP-based policy route in the products; send data packets matching the above-mentioned routing policy to the products;

DMZ zone.

b) Expected results:

The products support the load balancing function and can balance network access to multiple servers.

c) Result determination:

When the actual testing and assessment result is consistent with the relevant expected result, it shall be determined to be conformant, otherwise, it shall be determined to be non-conformant.

7.2.1.4 Device virtualization

7.2.1.4.1 Virtual system

The testing and assessment methods of virtual system are as follows:

a) Testing and assessment methods:

1) In the products, set up multiple subsystems; respectively set up administrators for the various subsystems; verify whether the administrators can only manage the subsystems, to which, they belong, and cannot manage other subsystems;

2) For the various subsystems, set up routing tables, security policies and generate logs; verify whether the various subsystems independently maintain their own routing tables, security policies and log systems;

3) For the various subsystems, set up usage quotas; verify whether the subsystems cannot use resources that exceed the quota.

b) Expected results:

1) The virtual subsystems can set up their own administrators; implement management configuration for the current subsystem without configurating or managing other subsystems;

2) The virtual subsystems can independently work and maintain their routing tables, security policies and log systems;

3) Resource usage quota can be allocated to the virtual subsystems.

c) Result determination:

When the actual testing and assessment result is consistent with the relevant expected result, it shall be determined to be conformant, otherwise, it shall be determined to be non-conformant.

security functions can normally work in Ipv6 network environment;

2) Simulate Ipv6 network environment; verify whether the products support the implementation of self-management in Ipv6 network environment.

b) Expected results:

1) The products support normal operation in pure Ipv6 network environment;

2) The products support the implementation of self-management in Ipv6 network environment.

c) Result determination:

When the actual testing and assessment result is consistent with the relevant expected result, it shall be determined to be conformant, otherwise, it shall be determined to be non-conformant.

7.2.1.5.2 Protocol consistency

The testing and assessment methods of protocol consistency are as follows:

a) Testing and assessment methods:

1) Under the routing mode, use protocol consistency test tool to test the consistency of the products' Ipv6 core protocol;

2) Under the routing mode, test the consistency of the products' Ipv6 NDP protocol;

3) Under the routing mode, test the consistency of the products' Ipv6 Autoconfig protocol;

4) Under the routing mode, test the consistency of the products' ICMPv6 protocol.

b) Expected results:

1) The products pass the consistency test of Ipv6 core protocol;

2) The products pass the consistency test of Ipv6 NDP protocol;

3) The products pass the consistency test of Ipv6 Autoconfig protocol;

4) The products pass the consistency test of ICMPv6 protocol.

c) Result determination:

When the actual testing and assessment result is consistent with the relevant

the Ipv6 terminal can communicate with the products through the ISATAP tunnel.

b) Expected results:

1) The communication in the Ipv4 and Ipv6 protocol transition environment is normal;

2) The communication is normal in at least one of the tunnel environments: Ipv6 over Ipv4 tunnel, Ipv6 to Ipv4 tunnel and ISATAP tunnel.

c) Result determination:

When the actual testing and assessment result is consistent with the relevant expected result, it shall be determined to be conformant, otherwise, it shall be determined to be non-conformant.

7.2.2 Network layer control

7.2.2.1 Access control

7.2.2.1.1 Packet filtering

The testing and assessment methods of packet filtering are as follows:

a) Testing and assessment methods:

1) Initialize the products' packet filtering policy; conduct mutual access operations among the hosts of various areas; check whether the products' default security policy is prohibited;

2) Set up source IP address and destination IP address-based access control policy; generate corresponding network sessions to verify whether the policy takes effect;

3) Set up source port and destination port-based access control policy; generate corresponding network sessions to verify whether the policy takes effect;

4) Set up protocol type-based access control policy; generate corresponding network sessions to verify whether the policy takes effect;

5) Set up MAC address-based access control policy; generate corresponding network sessions to verify whether the policy takes effect;

6) Set up time-based access control policy; generate corresponding network sessions to verify whether the policy takes effect;

7) Make attempts to set up a MAC address, IP address, port, protocol type

2) Use the automatic binding or manual binding function to bind the UP and MAC address of the host in the intranet;

3) Respectively generate a session with correct IP / MAC binding and a session with IP theft; check the validity of the binding.

b) Expected results:

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

2) After IP / MAC address binding, the security policy can be correctly executed; IP theft behaviors can be found.

c) Result determination:

When the actual testing and assessment result is consistent with the relevant expected result, it shall be determined to be conformant, otherwise, it shall be determined to be non-conformant.

7.2.2.2 Traffic management

7.2.2.2.1 Bandwidth management

The testing and assessment methods of bandwidth management are as follows:

a) Testing and assessment methods:

1) Set up a source IP, destination IP, application type and time period-based traffic policy on the products; send traffic that matches the policy to the products and gradually increase the traffic, until the traffic changes from within the allowable range to exceeding the policy range;

2) Set up a source IP, destination IP, application type and time period-based assurance bandwidth policy on the products; send traffic that matches the policy to the products and keep the traffic above the assured bandwidth, then, send other traffics to the products; try to seize the bandwidth used by the above-mentioned traffic;

3) Set up a total traffic bandwidth limit policy on the products; set up a bandwidth limit for a specific traffic in it. Before and after the products' total traffic bandwidth occupancy rate reaches the threshold, respectively verify whether the bandwidth policy of the above-mentioned specific traffic automatically starts and stops.

b) Expected results:

1) The source IP, destination IP, application type and time period-based traffic rate or total traffic policy takes effect;

a) Testing and assessment methods:

1) Set up session timeout time on the products;

2) Through the products, establish a session connection, and no longer operate on the session, until the timeout time is reached, then, verify whether the above-mentioned session is closed.

b) Expected results:

1) The products can configurate the session timeout time (or set a default value) of the various protocols;

2) After the inactive time of the already-connected session reaches the timeout time, the connection is automatically closed by the products.

c) Result determination:

When the actual testing and assessment result is consistent with the relevant expected result, it shall be determined to be conformant, otherwise, it shall be determined to be non-conformant.

7.2.3 Application layer control

7.2.3.1 User management and control

The testing and assessment methods of user management and control are as follows:

a) Testing and assessment methods:

1) Locally add the user on the products; set up a local user authentication-based network access policy; generate a session request that matches the policy; verify whether the session can only be established after user authentication is successful;

2) Configurate third-party authentication servers, such as Radius and LDAP, on the products; set up third-party user authentication-based network access policy; generate a session request that matches the policy; verify whether the session can only be established after user authentication is successful.

b) Expected results:

1) The products support the local user authentication-based network access control function;

2) The products support the third-party authentication-based network access control function.

5) The application-based (with escape or tunnel encryption features) access control policy takes effect;

6) Support the customized applications; the customized application-based access control policy takes effect.

c) Result determination:

When the actual testing and assessment result is consistent with the relevant expected result, it shall be determined to be conformant, otherwise, it shall be determined to be non-conformant.

7.2.3.3 Application content control

7.2.3.3.1 WEB application

The testing and assessment methods of WEB application are as follows:

a) Testing and assessment methods:

1) Set up an URL-based access control policy on the products; through the products, access the corresponding URL; verify whether the policy takes effect and verify whether there is a classified URL library;

2) Set up an HTTP transfer content keyword-based access control policy on the products; through the products, access the webpage that contains the corresponding keyword; verify whether the policy takes effect;

3) Set up a request mode-based (HTTP GET, POST, PUT and HEAD) access control policy on the products; through the products, send HTTP GET, POST, PUT and HEAD requests; verify whether the policy takes effect;

4) Set up an HTTP request file type-based access control policy on the products; through the products, use HTTP protocol to request the corresponding type of file; verify whether the policy takes effect;

5) Set up a field length-based (general-header, request-header and response-header, etc. in HTTP protocol) access control policy on the products; through the products, send data packets exceeding the corresponding length of HTTP protocol header; verify whether the policy takes effect;

6) Set up an HTTP upload file type-based access control policy on the products; through the products, use HTTP protocol to upload the corresponding type of file; verify whether the policy takes effect;

7) Set up an HTTP request frequency-based access control policy on the

attack packets and the proportion of normal HTTP connections that are successfully established;

4) Through the products, send TearDrop attack traffic (the traffic is 10% of the product interface rate), meanwhile, through the products, establish normal HTTP connections (the new connection rate is 100 connections/s, the duration is 60 s), check the proportion of the passed denial service attack packets and the proportion of normal HTTP connections that are successfully established;

5) Through the products, send Land attack traffic (the traffic is 10% of the product interface rate), meanwhile, through the products, establish normal HTTP connections (the new connection rate is 100 connections/s, the duration is 60 s), check the proportion of the passed denial service attack packets and the proportion of normal HTTP connections that are successfully established;

6) Through the products, send Ping of Death attack traffic (the traffic is 10% of the product interface rate), meanwhile, through the products, establish normal HTTP connections (the new connection rate is 100 connections/s, the duration is 60 s), check the proportion of the passed denial service attack packets and the proportion of normal HTTP connections that are successfully established;

7) Through the products, send CC attack traffic; verify whether the products support the identification and defense against CC attack.

b) Expected results:

1) Support the identification and defense against ICMP Flood attack, and the proportion of passed attack packets is not greater than 5%; the proportion of successfully established normal connections is not lower than 90%;

2) Support the identification and defense against UDP Flood attack, and the proportion of passed attack packets is not greater than 5%; the proportion of successfully established normal connections is not lower than 90%;

3) Support the identification and defense against SYN Flood attack, and the proportion of passed attack packets is not greater than 5%; the proportion of successfully established normal connections is not lower than 90%;

4) Support the identification and defense against TearDrop attack, and the proportion of passed attack packets is not greater than 5%; the proportion of successfully established normal connections is not lower than 90%;

5) Support the identification and defense against Land attack, and the

WEB application; verify whether the products can identify and defense against this type of attack;

8) Through the products, initiate the hotlinking attack to the destination WEB application; verify whether the products can identify and defense against this type of attack;

9) Through the products, initiate the OS command injection attack to the destination WEB application; verify whether the products can identify and defense against this type of attack;

10) Through the products, initiate WEBshell attack to the destination WEB application; verify whether the products can identify and defense against this type of attack;

11) Through the products, initiate the deserialization attack to the destination WEB application; verify whether the products can identify and defense against this type of attack.

b) Expected results:

1) The products can identify and defense against the SQL injection attack;

2) The products can identify and defense against the XSS attack;

3) The products can identify and defense against the third-party component vulnerability attack;

4) The products can identify and defense against the directory traversal attack;

5) The products can identify and defense against the Cookie injection attack;

6) The products can identify and defense against the CSRF attack;

7) The products can identify and defense against the file containment attack;

8) The products can identify and defense against the hotlinking attack;

9) The products can identify and defense against the OS command injection attack;

10) The products can identify and defense against the WEBshell attack;

11) The products can identify and defense against the deserialization attack.

c) Result determination:

When the actual testing and assessment result is consistent with the relevant

a) Testing and assessment methods:

1) On the products, initiate the malicious code protection strategy; through the products, initiate Trojan attack to the destination network or object; verify whether the products can detect and intercept the malicious code;

2) On the products, initiate the malicious code protection strategy; use the modes of HTTP webpage download, email sending and receiving to spread the malicious code through the products; verify whether the products can detect and intercept the malicious code.

b) Expected results:

1) The products can detect and intercept the Trojan behavior;

2) The products can detect and intercept the malicious code carried by HTTP webpages and emails.

c) Result determination:

When the actual testing and assessment result is consistent with the relevant expected result, it shall be determined to be conformant, otherwise, it shall be determined to be non-conformant.

7.2.4.5 Attack protection of other applications

The testing and assessment methods of attack protection of other applications are as follows:

a) Testing and assessment methods:

1) On the products, initiate a corresponding application attack protection policy; use an application attack simulator; through the products, initiate common CVE vulnerability attack of the operating system to the destination network or object; verify whether the products can identify and defense against this type of application attack;

2) Through the products, initiate common CVE vulnerability attack of the middleware to the destination network or object; verify whether the products can identify and defense against this type of application attack;

3) Through the products, initiate common CVE vulnerability attack of the controls to the destination network or object; verify whether the products can identify and defense against this type of application attack.

b) Expected results:

1) The products can identify and defense against the vulnerability attack of

2) The log records include: the date and time of the occurrence of the event; the subject, object and description of the event; the protocol type, source address, destination address, source port and destination port of the packet logs; the description of the attack event;

3) The products are only allowed to be accessed by authorized administrators, and provide functions of log review and export; provide the function of audit event query in accordance with the conditions of date, time, subject and object, etc.; the logs are stored in the power-off non-volatile storage medium; the log storage period is set to be not less than 6 months; when the storage space reaches the threshold, it can notify the authorized administrator; the logs support automated backup to other storage devices.

c) Result determination:

When the actual testing and assessment result is consistent with the relevant expected result, it shall be determined to be conformant, otherwise, it shall be determined to be non-conformant.

7.2.5.2 Security warning

The testing and assessment methods of security warning are as follows:

a) Testing and assessment methods:

1) Use various attack simulators to respectively generate the attack events in 6.1.4;

2) Verify whether the products can warn of attacks, and whether the products can initiate combined warning to the same warning events that occur at a high frequency;

3) Verify whether the warning message contains the subject, object and description of the event, the level of hazard, and the date and time of the occurrence of the event.

b) Expected results:

1) The products can initiate warning to attack event and initiate combined warning to the same attack events that occur at a high frequency;

2) The products' warning message include the subject, object and description of the event, the level of hazard, and the date and time of the occurrence of the event.

c) Result determination:

2) Verify whether the statistical results can be output in the form of reports;

3) Verify whether the products support comparison of statistical results in different time periods.

b) Expected results:

1) The products can conduct statistics of application traffic in accordance with the IP addresses, time periods and protocol types, or, a combination of the above-mentioned conditions;

2) The products can output the statistical results in the form of reports;

3) The products support comparison of statistical results in different time periods.

c) Result determination:

When the actual testing and assessment result is consistent with the relevant expected result, it shall be determined to be conformant, otherwise, it shall be determined to be non-conformant.

7.2.5.3.3 Attack event statistics

The testing and assessment methods of attack event statistics are as follows:

a) Testing and assessment methods:

1) In different time periods, send mixed traffic that contains multiple IP addresses and multiple attacks to the products; make attempts to conduct statistics of attack events in accordance with the type of attack events, IP addresses and time periods, or, a combination of the above-mentioned conditions;

2) Verify whether the statistical results can be output in the form of reports.

b) Expected results:

1) The products can conduct statistics of attack events in accordance with the type of attack events, IP addresses and time periods, or, a combination of the above-mentioned conditions;

2) The products can output the statistical results in the form of reports.

c) Result determination:

When the actual testing and assessment result is consistent with the relevant expected result, it shall be determined to be conformant, otherwise, it shall be determined to be non-conformant.

period, the products automatically withdraw;

5) The administrator needs to pass the identity authentication measures, for example, password authentication; there are also requirements for the strength of the password;

6) When the products have a default password, the products can prompt the user to modify the default password;

7) The products support two-factor authentication.

c) Result determination:

When the actual testing and assessment result is consistent with the relevant expected result, it shall be determined to be conformant, otherwise, it shall be determined to be non-conformant.

7.3.2 Management capabilities

The testing and assessment methods of management capabilities are as follows:

a) Testing and assessment methods:

1) Verify whether the products provide authorized administrators with the function of setting up and modifying security management parameters;

2) Verify whether the products provide authorized administrators with the function of setting up, querying and modifying various security policies;

3) Verify whether the products provide authorized administrators with the function of managing audit logs;

4) Verify whether the products support the upgrade of their own system and various feature libraries;

5) Verify whether the products support system time synchronization from the NTP server;

6) Verify whether the products support sending logs and warning messages to the log server through the SYSYLOG protocol;

7) Verify whether the products distinguish the roles of administrators and whether the roles can be divided into system administrators, security operators and security auditors, and whether the three types of administrator roles and permissions are mutually restricted;

8) Verify whether the products provide the function of policy validity testing to authorized administrators.

b) Expected results:

1) The products' support system has been trimmed as necessary, and redundant components or network services are not provided;

2) During the restart process, the security policy and log information are not lost;

3) The products do not contain already-known medium and high-risk security vulnerabilities.

c) Result determination:

When the actual testing and assessment result is consistent with the relevant expected result, it shall be determined to be conformant, otherwise, it shall be determined to be non-conformant.

7.4 Performance Testing and Assessment

7.4.1 Throughput

7.4.1.1 Network layer throughput

The testing and assessment methods of network layer throughput are as follows:

a) Testing and assessment methods:

1) Use a performance tester to connect the products' interface; test the throughput under the bi-directional UDP protocol (respectively under the condition of 64-byte, 512-byte and 1,518-byte) of a pair of ports at the corresponding rate without packet loss;

2) Test the throughput under the whole-machine bi-directional UDP protocol (1,518-byte) of high-performance 10 G products without packet loss.

b) Expected results:

The network layer throughput is not lower than the corresponding requirements in 6.3.1.1.

c) Result determination:

When the actual testing and assessment result is consistent with the relevant expected result, it shall be determined to be conformant, otherwise, it shall be determined to be non-conformant.

7.4.1.2 Mixed application layer throughput

The testing and assessment methods of mixed application layer throughput are as

7.4.2 Delay

The testing and assessment methods of HTTP throughput are as follows:

a) Testing and assessment methods:

1) Use a performance tester to connect the products' interface;

2) Test the delay of a pair of ports at the corresponding rate respectively of 64-byte, 512-byte and 1,518-byte under the condition of 90% maximum network throughput.

b) Expected results:

The delay is not lower than the corresponding requirements in 6.3.2.

c) Result determination:

When the actual testing and assessment result is consistent with the relevant expected result, it shall be determined to be conformant, otherwise, it shall be determined to be non-conformant.

7.4.3 Connection rate

7.4.3.1 TCP new connection rate

The testing and assessment methods of TCP new connection rate are as follows:

a) Testing and assessment methods:

1) Use a performance tester to connect the products' interface; test the products' TCP new connection rate;

2) Test the whole-machine TCP new connection rate of high-performance 10 G products.

b) Expected results:

The TCP new connection rate is not lower than the corresponding requirements in 6.3.3.1.

c) Result determination:

When the actual testing and assessment result is consistent with the relevant expected result, it shall be determined to be conformant, otherwise, it shall be determined to be non-conformant.

7.4.3.2 HTTP request rate

number of TCP concurrent connections;

2) Test the number of whole-machine TCP concurrent connections of high-performance 10 G products.

b) Expected results:

The number of TCP concurrent connections is not lower than the corresponding requirements in 6.3.4.1.

c) Result determination:

When the actual testing and assessment result is consistent with the relevant expected result, it shall be determined to be conformant, otherwise, it shall be determined to be non-conformant.

7.4.4.2 Number of HTTP concurrent connections

The testing and assessment methods of the number of HTTP concurrent connections are as follows:

a) Testing and assessment methods:

1) Use a performance tester to connect the products' interface;

2) Test the number of HTTP concurrent connections.

b) Expected results:

The number of HTTP concurrent connections is not lower than the corresponding requirements in 6.3.4.2.

c) Result determination:

When the actual testing and assessment result is consistent with the relevant expected result, it shall be determined to be conformant, otherwise, it shall be determined to be non-conformant.

7.4.4.3 Number of SQL concurrent connections

The testing and assessment methods of the number of SQL concurrent connections are as follows:

a) Testing and assessment methods:

1) Use a performance tester to connect the products' interface;

2) Test the number of SQL concurrent connections of the products.

a) Testing and assessment methods:

Check the operation user guide evidence provided by the developer; check whether the information provided by the developer satisfies all the requirements for the content and form of the evidence:

1) Whether the functions and privileges (including appropriate warning information) that the users have access to are described;

2) Whether how to use the available interfaces provided by the products in a secured mode is described; whether the method for the users to operate the products' security functions and interfaces (including the security value of configuration parameters) is described;

3) Whether all possible states of product operation, including operation-induced failures or operational errors are identified and described;

4) Whether the security policy that must be executed to implement the products' security objectives is described.

b) Expected results:

The information provided by the developer satisfies the requirements described in 6.4.2.1.

c) Result determination:

When the actual testing and assessment result is consistent with the relevant expected result, it shall be determined to be conformant, otherwise, it shall be determined to be non-conformant.

7.5.2.2 Preparation procedure

The testing and assessment methods of preparation procedure are as follows:

a) Testing and assessment methods:

Check the preparation procedure evidence provided by the developer; check whether the information provided by the developer satisfies all the requirements for the content and form of the evidence:

1) Whether all the steps necessary to securely receive the delivered products consistent with the developer's delivery procedure are described;

2) Whether all the steps necessary to securely install the products and the operating environment are described.

The information and on-site activity evidence content provided by the developer satisfies the requirements described in 6.4.3.1.

c) Result determination:

When the actual testing and assessment result is consistent with the relevant expected result, it shall be determined to be conformant, otherwise, it shall be determined to be non-conformant.

7.5.3.2 Scope of configuration management

The testing and assessment methods of configuration management scope are as follows:

a) Testing and assessment methods:

Check the configuration management scope evidence provided by the developer; check whether the information provided by the developer satisfies all the requirements for the content and form of the evidence:

1) Check whether the list of configuration items provided by the developer contains the evaluation evidence of the products' security assurance requirements, the product components and the corresponding developer;

2) Check whether the list of configuration items provided by the developer contains implementation expression, security defect report, resolution status and the corresponding developer.

b) Expected results:

The information and on-site activity evidence content provided by the developer satisfies the requirements described in 6.4.3.2.

c) Result determination:

When the actual testing and assessment result is consistent with the relevant expected result, it shall be determined to be conformant, otherwise, it shall be determined to be non-conformant.

7.5.3.3 Delivery procedure

The testing and assessment methods of delivery procedure are as follows:

a) Testing and assessment methods:

Check the delivery procedure evidence provided by the developer; check whether the information provided by the developer satisfies all the requirements for the content and form of the evidence:

When the actual testing and assessment result is consistent with the relevant expected result, it shall be determined to be conformant, otherwise, it shall be determined to be non-conformant.

7.5.3.5 Definition of Life cycle

The testing and assessment methods of life cycle definition are as follows:

a) Testing and assessment methods:

Check the life cycle definition evidence provided by the developer; check whether the information provided by the developer satisfies all the requirements for the content and form of the evidence:

1) Check on the site whether the developer uses the life cycle model to control the development and maintenance of the products as necessary;

2) Check whether the life cycle definition document provided by the developer describes the model used for product development and maintenance.

b) Expected results:

The information and on-site activity evidence content provided by the developer satisfies the requirements described in 6.4.3.5.

c) Result determination:

When the actual testing and assessment result is consistent with the relevant expected result, it shall be determined to be conformant, otherwise, it shall be determined to be non-conformant.

7.5.3.6 Tools and technology

The testing and assessment methods of tools and technology are as follows:

a) Testing and assessment methods:

Check the tools and technology evidence provided by the developer; check whether the information provided by the developer satisfies all the requirements for the content and form of the evidence:

1) Check on the site whether the developer explicitly defines tools used for product development;

2) Check whether the development tool document that unambiguously defines the meaning of each statement in the implementation and the meaning of all implementation-dependent options is provided.

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

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