

ICS 35.040
CCS L 80



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

GB/T 32917-2016

**Information security technology -- Security technique
requirements and testing and evaluation approaches for WEB
application firewall**

信息安全技术 WEB应用防火墙安全技术要求与测试评价方法
(English Translation)

Issued on: August 29, 2016

Implemented on: March 1, 2017

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

Table of Contents

Foreword...	4
Introduction...	5
1 Scope...	6
2 Normative references...	6
3 Terms, definitions and abbreviations...	6
3.1 Terms and definitions...	6
3.2 Abbreviations...	7
4 Security technical requirements...	7
4.1 Basic level...	7
4.1.1 Security function requirements...	7
4.1.2 Self-security protection...	10
4.1.3 Security assurance requirements...	11
4.2 Enhanced level...	16
4.2.1 Security function requirements...	16
4.2.2 Self-security protection...	19
4.2.3 Security assurance requirements...	21
4.3 Performance requirements...	26
4.3.1 HTTP throughput...	26
4.3.2 HTTP maximum request rate...	27
4.3.3 Maximum number of concurrent HTTP connections...	27
5 Test evaluation method...	27
5.1 Test environment...	27
5.2 Basic level...	29
5.2.1 Evaluation method for security function requirements test...	29
5.2.2 Self-security protection test evaluation method...	35
5.2.3 Test evaluation methods for security assurance requirements...	40
5.3 Enhanced level...	49
5.3.1 Test evaluation method of security function requirements...	49
5.3.2 Test evaluation method of self-security protection...	56
5.3.3 Test evaluation method of security assurance requirements...	62
5.4 Performance test evaluation method...	72
5.4.1 HTTP throughput...	72

5.4.2 HTTP maximum request rate...	73
5.4.3 Maximum number of concurrent HTTP connections...	73

1 Scope

This standard specifies the security function requirements, self-security protection requirements, performance requirements, security assurance requirements of WEB application firewalls; provides corresponding test evaluation methods.

This standard applies to the design, production, testing and procurement of WEB application firewalls.

2 Normative references

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

GB/T 25069-2010 Information security technology - Glossary

3.1 Terms and definitions

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

3.1.1

WEB application firewall

It is an information security product that performs protocol and content filtering on all WEB server access requests to WEB servers and WEB server responses based on pre-defined filtering rules and security protection rules, thereby realizing security protection functions for WEB servers and WEB applications.

3.1.2

WEB server

A Web server is a program that provides services to clients (such as browsers) that make requests. When a web browser (client) connects to the server and requests resources, the server will process the request and send the resources to the browser. The web server uses HTTP to communicate with the web browser. Commonly used web servers are Apache and Internet information server.

3.2 Abbreviations

The following abbreviations apply to this document.

CSRF. Cross-site Request Forgery

HTTP. Hypertext Transfer Protocol

HTTPS. Hypertext Transfer Protocol over Secure Socket Layer

SSL. Secure Socket Layer

SQL. Structured Query Language

URL. Uniform Resource Locator

WEB. World Wide Web

XSS Cross Site Scripting

4.1.1.3 Other functions

4.1.1.3.1

Custom error page function

It shall be possible to customize the error page returned by the WEB server.

4.1.2.2 Security audit

4.1.2.2.1

Audit data generation

The following audit logs shall be generated.

4.1.2.2.2

Audit log management function

Management functions such as backup and query of audit data shall be provided.

4.1.2.2.3

Comprehensible format

All audit records can be understood.

4.1.2.2.4

Prevention of loss of audit data

Log information shall be stored in a permanent storage medium. When the storage space is exhausted, corresponding measures shall be taken to ensure that the audit data is not lost.

4.1.2.3 Statistics function

It shall have the following statistical functions.

4.1.2.4 Remote management encryption

When remote management is required, the remote management communication shall be encrypted and protected.

4.1.2.5 Condition monitoring

During startup and normal work, self-checks shall be performed periodically or in accordance with the requirements of authorized administrators, including hardware working status monitoring, software module status monitoring, etc.;

when abnormal working status is detected, the administrator shall be alerted.

4.1.2.6 Dual-system hot backup

It shall have the dual-system hot backup function. When the main WEB application firewall fails, the standby WEB application firewall shall discover and take over the main WEB application firewall in time.

4.1.3.1 Development

4.1.3.1.1

Security architecture

The developer shall provide a description of the security architecture of the product's security functions; the security architecture's description shall meet the following requirements.

4.1.3.1.2

Functional specification

The developer shall provide a complete functional specification; the functional specification shall meet the following requirements.

4.1.3.1.3

Product design

Developers shall provide product design documents; the product design documents shall meet the following requirements.