ICS 35.040
L 80

中华人民共和国国家标准

GB/T 20281—2020
代替 GB/T 20010—2005,GB/T 20281—2015,GB/T 31505—2015 和 GB/T 32917—2016

信息安全技术　防火墙安全技术要求和测试评价方法

Information security technology—Security technical requirements and testing assessment approaches for firewall

2020-04-28 发布　　2020-11-01 实施

国家市场监督管理总局
国家标准化管理委员会　发布

目　　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准代替 GB/T 20010—2005《信息安全技术　包过滤防火端评估准则》、GB/T 20281—2015《信息安全技术　防火墙安全技术要求和测试评价方法》、GB/T 31505—2015《信息安全技术　主机型防火墙安全技术要求和测试评价方法》、GB/T 32917—2016《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》。本标准以 GB/T 20281—2015 为主，整合了 GB/T 20010—2005、GB/T 31505—2015 和 GB/T 32917—2016 的部分内容，与 GB/T 20281—2015 相比，除编辑性修改外主要技术变化如下：

——增加了网络型防火墙、数据库防火墙、WEB 应用防火墙和主机型防火墙的定义(见第 3 章)；

——修改了概述(见第 5 章，2015 年版的第 5 章)；

——增加了“设备虚拟化”要求(见 6.1.1.4)；

——修改了“应用内容控制”的要求(见 6.1.3.3，2015 版的 6.2.1.2、6.3.1.2)；

——增加了“攻击防护”的要求(见 6.1.4)；

——增加了“安全审计与分析”的要求(见 6.1.5)；

——增加了“混合应用层吞吐量”“HTTP 吞吐量”“HTTP 请求速率”“SQL 请求速率”“HTTP 并发连接数”“SQL 并发连接数”性能要求(见 6.3.1.2、6.3.1.3、6.3.3.2、6.3.3.3、6.3.4.2、6.3.4.3)；

——增加了规范性附录(见附录 A、附录 B)。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本标准起草单位：公安部第三研究所、奇安信科技集团股份有限公司、北京天融信网络安全技术有限公司、网神信息技术(北京)股份有限公司、北京神州绿盟科技有限公司、杭州美创科技有限公司、北京网康科技有限公司、中国信息安全研究院有限公司、中国电子技术标准化研究院、中国网络安全审查技术与认证中心、中国信息安全测评中心、国家计算机网络与信息安全管理中心、北京安华金和科技有限公司、深信服科技股份有限公司、启明星辰信息技术集团股份有限公司、沈阳东软系统集成工程有限公司、新华三技术有限公司、蓝盾信息安全技术股份有限公司、北京中安星云软件技术有限公司、上海上讯信息技术股份有限公司。

本标准主要起草人：俞优、王志佳、邹春明、陆臻、沈亮、陆磊、顾健、吴云坤、熊瑛、雷晓锋、叶晓虎、周杰、王伟、陈华平、吴亚东、谢建业、王猛、谌德俊、潘云、申永波、杨晨、王晖。

本标准所代替标准的历次版本发布情况为：

——GB/T 20010—2005；

——GB/T 20281—2006、GB/T 20281—2015；

——GB/T 31505—2015；

——GB/T 32917—2016。

信息安全技术　防火墙安全技术要求和测试评价方法

1　范围

本标准规定了防火墙的等级划分、安全技术要求及测评方法。

本标准适用于防火墙的设计、开发与测试。

2　规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本(包括所有的修改单)适用于本文件。

GB/T 18336.3—2015　信息技术　安全技术　信息技术安全评估准则　第3部分：安全保障组件

GB/T 25069—2010　信息安全技术　术语

3　术语和定义

GB/T 25069—2010界定的以及下列术语和定义适用于本文件。

3.1

防火墙　firewall

对经过的数据流进行解析，并实现访问控制及安全防护功能的网络安全产品。

注：根据安全目的、实现原理的不同，通常可分为网络型防火墙、WEB应用防火墙、数据库防火墙和主机型防火墙等。

3.2

网络型防火墙　network-based firewall

部署于不同安全域之间，对经过的数据流进行解析，具备网络层、应用层访问控制及安全防护功能的网络安全产品。

3.3

WEB应用防火墙　web application firewall

部署于WEB服务器前端，对流经的HTTP/HTTPS访问和响应数据进行解析，具备WEB应用的访问控制及安全防护功能的网络安全产品。

3.4

数据库防火墙　database firewall

部署于数据库服务器前端，对流经的数据库访问和响应数据进行解析，具备数据库的访问控制及安全防护功能的网络安全产品。

3.5

主机型防火墙　host-based firewall

部署于计算机(包括个人计算机和服务器)上，提供网络层访问控制、应用程序访问限制和攻击防护功能的网络安全产品。