



中华人民共和国国家标准

GB/T 20281—2015
代替 GB/T 20281—2006

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 and evaluation approaches for firewall

2015-05-15 发布

2016-01-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会 发布

目 次

前言	III
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 缩略语	2
5 防火墙描述	2
6 安全技术要求	2
6.1 总体说明	2
6.1.1 要求分类	2
6.1.2 安全等级	3
6.2 基本级安全要求	5
6.2.1 安全功能要求	5
6.2.2 安全保证要求	8
6.3 增强级安全要求	10
6.3.1 安全功能要求	10
6.3.2 安全保证要求	15
6.4 环境适应性要求	20
6.4.1 传输模式	20
6.4.2 下一代互联网支持(有则适用)	20
6.5 性能要求	21
6.5.1 吞吐量	21
6.5.2 延迟	21
6.5.3 最大并发连接数	22
6.5.4 最大连接速率	22
7 测试评价方法	22
7.1 测试环境	22
7.1.1 安全功能与环境适应性测试环境	22
7.1.2 性能测试环境	23
7.2 基本级安全要求测试	23
7.2.1 安全功能测试	23
7.2.2 安全保证测试	28
7.3 增强级安全要求测试	32
7.3.1 安全功能测试	32
7.3.2 安全保证测试	40
7.4 环境适应性测试	49
7.4.1 传输模式	49
7.4.2 下一代互联网支持	49

7.5 性能测试	53
7.5.1 吞吐量	53
7.5.2 延迟	53
7.5.3 最大并发连接数	54
7.5.4 最大连接速率	54
参考文献	55

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 20281—2006《信息安全技术 防火墙技术要求和测试评价方法》。

本标准与 GB/T 20281—2006 的主要差异如下：

- 修改了防火墙的描述；
- 修改了防火墙的功能分类；
- 增加了防火墙的高性能要求；
- 加强了防火墙对应用层控制能力的要求；
- 增加了下一代互联网协议支持能力的要求；
- 级别统一划分为基本级和增强级。

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：公安部计算机信息系统安全产品质量监督检验中心、北京启明星辰信息安全技术有限公司、华为技术有限公司、解放军信息安全测评认证中心、北京中科网威信息技术有限公司、北京网康科技有限公司、公安部第三研究所。

本标准主要起草人：俞优、陆臻、邹春明、顾健、沈亮、李毅、韦湘、王光宇、吕颖轩、王平。

本标准所代替标准的历次版本发布情况为：

- GB/T 20281—2006。

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安全技术要求、测试评价方法及安全等级划分。
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—2008 信息技术 安全技术 信息技术安全性评估准则 第3部分:安全保证要求

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**

部署于不同安全域之间,具备网络层访问控制及过滤功能,并具备应用层协议分析、控制及内容检测等功能,能够适用于 IPv4、IPv6 等不同的网络环境的安全网关产品。

3.2

深度包检测 **deep packet inspection**

基于应用层的流量检测和控制技术,通过读取 IP 包载荷的内容并对应用层信息进行重组,从而得到整个应用程序的内容,然后按照系统定义的策略对内容进行相应处置。

3.3

深度内容检测 **deep content inspection**

能够对应用协议进行深入解析,识别出协议中的各种要素(如 http 协议,可具体解析到如 cookie、Get 参数、Post 表单等)以及协议所承载的业务内容(如业务系统交互中包含在协议或文件中的数据内容),并对这些数据进行快速的解析,以还原其原始通信的信息。根据这些解析后的原始信息,可以检测其是否包含威胁以及敏感内容。

3.4

SQL 注入 **SQL injection**

把 SQL 命令插入到 web 表单递交或者页面请求的参数中,以达到欺骗服务器执行恶意 SQL 命令的目的。

3.5

跨站脚本 **cross site scripting**

恶意攻击者往 web 页面里插入恶意 HTML 代码,当用户浏览该页面时,嵌入 web 页面里面的 HTML 代码会被执行,从而达到恶意攻击用户的目的。