



中华人民共和国国家标准

GB/T 20281—2006

信息安全技术 防火墙技术要求和测试评价方法

Information security technology—
Technique requirements and testing and evaluation approaches for
firewall products

2006-05-31 发布

2006-12-01 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 符号和缩略语	2
5 技术要求	3
5.1 总体说明	3
5.1.1 技术要求分类	3
5.1.2 安全等级	3
5.2 功能要求	3
5.2.1 一级产品功能要求	3
5.2.2 二级产品功能要求	5
5.2.3 三级产品功能要求	7
5.3 性能要求	9
5.3.1 吞吐量	9
5.3.2 延迟	9
5.3.3 最大并发连接数	10
5.3.4 最大连接速率	10
5.4 安全要求	10
5.4.1 一级产品安全要求	10
5.4.2 二级产品安全要求	11
5.4.3 三级产品安全要求	11
5.5 保证要求	12
5.5.1 说明	12
5.5.2 一级产品保证要求	12
5.5.3 二级产品保证要求	13
5.5.4 三级产品保证要求	15
6 测评方法	17
6.1 总体说明	17
6.2 功能测试	18
6.2.1 测试环境与工具	18
6.2.2 包过滤	18
6.2.3 状态检测	19
6.2.4 深度包检测	19
6.2.5 应用代理	19
6.2.6 NAT	19
6.2.7 IP/MAC 地址绑定	20
6.2.8 动态开放端口	20

6.2.9	策略路由	20
6.2.10	流量统计	20
6.2.11	带宽管理	21
6.2.12	双机热备	21
6.2.13	负载均衡	21
6.2.14	VPN	21
6.2.15	协同联动	21
6.2.16	安全审计	22
6.2.17	管理	22
6.3	性能测试	23
6.3.1	测试环境与工具	23
6.3.2	吞吐量	23
6.3.3	延迟	23
6.3.4	最大并发连接数	24
6.3.5	最大连接速率	24
6.4	安全性测试	24
6.4.1	测试环境与工具	24
6.4.2	抗渗透	24
6.4.3	恶意代码防御	24
6.4.4	支撑系统	25
6.4.5	非正常关机	25
6.5	保证要求测试	25
6.5.1	配置管理	25
6.5.2	交付与运行	25
6.5.3	安全功能开发过程	25
6.5.4	指导性文档	25
6.5.5	生命周期支持	26
6.5.6	测试	26
6.5.7	脆弱性评定	26
附录 A(资料性附录)	防火墙介绍	27
A.1	概述	27
A.2	工作模式	27
A.2.1	路由模式	27
A.2.2	透明模式	27
A.3	工作环境	27

前 言

本标准的附录 A 为资料性附录。

本标准由全国信息安全标准化技术委员会提出并归口。

本标准由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负责起草。

本标准主要起草人：李京春、钟力、郑传波、付志峰、锁延锋、桂坚勇、陆驿。

信息安全技术

防火墙技术要求和测试评价方法

1 范围

本标准规定了采用“传输控制协议/网际协议(TCP/IP)”的防火墙类信息安全产品的技术要求和测试评价方法。

本标准适用于采用“传输控制协议/网际协议(TCP/IP)”的防火墙类信息安全产品的研制、生产、测试和评估。

2 规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件,其随后所有的修改单(不包括勘误的内容)或修订版均不适用于本标准,然而,鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡不注日期的引用文件,其最新版本适用于本标准。

GB/T 5271.8 信息技术 词汇 第8部分:安全(GB/T 5271.8—2001, idt ISO/IEC 2382-8:1998)

GB 17859 计算机信息系统安全保护等级划分准则

GB/T 18336.3 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 18336.3—2001, idt ISO/IEC 15408-3:1999)

3 术语和定义

GB/T 5271.8、GB 17859 和 GB/T 18336.3 确立的以及下列术语和定义适用于本标准。

3.1

防火墙 **firewall**

一个或一组在不同安全策略的网络或安全域之间实施访问控制的系统。

3.2

内部网络 **internal network**

通过防火墙隔离的可信任区域或保护区域,通常是指单位内部的局域网。

3.3

外部网络 **external network**

通过防火墙隔离的不可信任区域或非保护区域。

3.4

非军事区 **demilitary zone**

一个网络对外提供网络服务的部分,受防火墙保护,通过防火墙与内部网络和外部网络隔离,执行与内部网络不同的安全策略,也有的称为安全服务网络(secure service network)。

3.5

安全策略 **security policy**

有关管理、保护和发布敏感信息的法律、规定和实施细则。

3.6

授权管理员 **authorized administrator**

具有防火墙管理权限的用户,负责对防火墙的系统配置、安全策略、审计日志等进行管理。