



# 中华人民共和国公共安全行业标准

GA/T 683—2007

---

## 信息安全技术 防火墙安全技术要求

Information security technology—  
Technical requirements for firewall security

2007-03-20 发布

2007-05-01 实施

---

中华人民共和国公安部 发布

## 目 次

前言 .....	V
引言 .....	VI
1 范围 .....	1
2 规范性引用文件 .....	1
3 术语、定义和缩略语 .....	1
3.1 术语和定义 .....	1
3.2 缩略语 .....	1
4 第一级安全要求 .....	2
4.1 安全功能要求 .....	2
4.1.1 防火墙自身自主访问控制 .....	2
4.1.2 身份鉴别 .....	2
4.1.3 安全管理 .....	2
4.1.4 访问控制功能 .....	2
4.1.5 网络地址转换(NAT)功能 .....	3
4.1.6 策略路由 .....	3
4.1.7 流量统计 .....	3
4.1.8 报表 .....	3
4.2 安全保证要求 .....	3
4.2.1 配置管理 .....	3
4.2.2 交付和运行 .....	3
4.2.3 开发 .....	3
4.2.4 指导性文档 .....	3
4.2.5 生命周期支持 .....	3
4.2.6 测试 .....	3
5 第二级安全要求 .....	4
5.1 安全功能要求 .....	4
5.1.1 防火墙自身自主访问控制 .....	4
5.1.2 身份鉴别 .....	4
5.1.3 安全管理 .....	4
5.1.4 访问控制功能 .....	5
5.1.5 审计 .....	5
5.1.6 网络地址转换(NAT)功能 .....	5
5.1.7 策略路由 .....	6
5.1.8 流量统计 .....	6
5.1.9 带宽管理 .....	6
5.1.10 报表 .....	6
5.1.11 抗攻击功能 .....	6

5.1.12	动态开放端口	6
5.1.13	可靠性	6
5.2	安全保证要求	6
5.2.1	配置管理	6
5.2.2	交付和运行	7
5.2.3	开发	7
5.2.4	指导性文档	7
5.2.5	生命周期支持	7
5.2.6	测试	7
5.2.7	脆弱性评定	7
6	第三级安全要求	8
6.1	安全功能要求	8
6.1.1	防火墙自身自主访问控制	8
6.1.2	身份鉴别	8
6.1.3	安全管理	8
6.1.4	访问控制功能	9
6.1.5	标记	9
6.1.6	审计	9
6.1.7	简单网络管理协议(SNMP)的保护	10
6.1.8	网络地址转换(NAT)功能	10
6.1.9	策略路由	10
6.1.10	流量统计	10
6.1.11	带宽管理	10
6.1.12	报表	11
6.1.13	抗攻击功能	11
6.1.14	非正常关机	11
6.1.15	动态开放端口	11
6.1.16	可靠性	11
6.2	安全保证要求	11
6.2.1	配置管理	11
6.2.2	交付和运行	12
6.2.3	开发	12
6.2.4	指导性文档	12
6.2.5	生命周期支持	12
6.2.6	测试	13
6.2.7	脆弱性评定	13
7	附加安全功能	13
7.1	虚拟专用网(VPN)功能	13
7.2	与IDS联动功能	13
7.3	防病毒网关功能	13
7.4	反垃圾邮件功能	14

附录 A (资料性附录) 安全要求对照表 .....	15
A.1 组成与相互关系 .....	15
A.2 防火墙安全等级的划分 .....	15
A.3 附加安全功能 .....	16
参考文献 .....	17

## 前 言

本标准是从信息技术方面详细规定了各安全保护级别的防火墙所应具有的安全功能要求和安全保证要求。

本标准中附录 A 为资料性附录。

本标准由公安部公共信息网络安全监察局提出。

本标准由公安部信息系统安全标准化技术委员会归口。

本标准起草单位：中国科学院研究生院信息安全国家重点实验室。

本标准主要起草人：戴英侠、何申、左晓栋。

## 引 言

防火墙是重要的网络边界保护设备,制定公共安全行业防火墙安全技术要求对于指导防火墙产品的研发、采购和部署,保障公共安全行业网络安全具有重要的意义。

本标准对公共安全行业使用的防火墙提出了分等级的安全技术要求。

本标准仅对一到三级安全保护等级做了技术要求,与 GB 17859—1999《计算机信息系统 安全保护等级划分准则》的对应关系是,第一级对应用户自主保护级,第二级对应系统审计保护级,第三级对应安全标记保护级。

本标准文本中,加粗字体表示较低等级中没有出现或增强的技术要求。

# 信息安全技术

## 防火墙安全技术要求

### 1 范围

本标准分三个等级规定了防火墙的安全技术要求。安全等级从第一级到第三级逐级增高,对防火墙的安全要求也逐步增强。

本标准适用于公共安全行业对防火墙产品的研发、生产。同时也可适用于对防火墙产品的采购和部署。

### 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。凡是不注日期的引用文件,其最新版本适用于本标准。

GB 17859—1999 计算机信息系统 安全保护等级划分准则

GB/T 18336.1—2001 信息技术 安全技术 信息技术安全性评估准则 第1部分:简介和一般模型

### 3 术语、定义和缩略语

#### 3.1 术语和定义

GB 17859—1999 和 GB/T 18336.1—2001 确立的以及下列术语和定义适用于本标准。

##### 3.1.1

#### 防火墙 fire wall

防火墙是在网络之间执行访问控制策略的一个或一组组件的集合,是一种重要的网络防护设备,属于用户网络边界的安全保护设备。

#### 3.2 缩略语

下列缩略语适用于本标准。

FTP	File Transfer Protocol	文件传输协议
ICMP	Internet Control Message Protocol	Internet 控制消息协议
IDS	Intrusion Detection System	入侵检测系统
IPS	Intrusion Prevention System	入侵防御系统
IPSec	Internet Protocol Security	IP 安全协议
MIB	Management Information Base	管理信息库
NAT	Network Address Translation	网络地址转换
PAT	Port Address Translation	端口地址转换
RTP	Real-time Transport Protocol	实时传输协议
RTSP	Real Time Streaming Protocol	实时流协议
SIP	Session Initiation Protocol	会话初始化协议
SNMP	Simple Network Management Protocol	简单网络管理协议
SQL	Structured Query Language	结构化查询语言