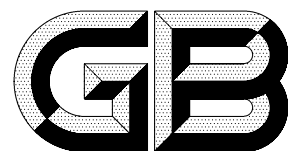


ICS 35.040  
L 80



# 中华人民共和国国家标准

GB/T 18020—1999

---

## 信 息 技 术 应用级防火墙安全技术要求

Information technology—  
Security requirements for application level firewall

1999-11-11 发布

2000-05-01 实施

---

国家质量技术监督局 发布

## 目 次

前言 .....	Ⅲ
1 范围 .....	1
2 引用标准 .....	1
3 定义和记法约定 .....	1
3.1 定义 .....	1
3.2 记法约定 .....	1
4 应用级防火墙概述 .....	1
5 安全环境 .....	2
5.1 安全条件假定 .....	2
5.2 安全威胁 .....	2
6 安全目标 .....	3
6.1 信息技术安全目标 .....	3
6.2 非信息技术安全目标 .....	4
7 安全要求 .....	4
7.1 功能要求 .....	4
7.2 保证要求 .....	9
8 基本原则.....	13
8.1 信息技术安全目标的基本原则.....	13
8.2 非信息技术安全目标的基本原则.....	13
8.3 信息技术功能要求的基本原则.....	14
8.4 保证要求基本原则.....	16

## 前 言

本标准规定了网络安全设备——应用级防火墙的安全技术要求。

本标准由国家信息化办公室提出。

本标准由全国信息技术标准化技术委员会归口。

本标准起草单位：国家信息中心、中国国家信息安全测评认证中心。

本标准主要起草人：叶红、吴亚非、吴世忠、陈晓桦、李正男、严望佳。

# 中华人民共和国国家标准

## 信息技术 应用级防火墙安全技术要求

GB/T 18020—1999

### Information technology— Security requirements for application level firewall

#### 1 范围

本标准规定了应用级防火墙的安全技术要求。

本标准适用于应用级防火墙安全功能的研制、开发、测试、评估和产品采购。

#### 2 引用标准

下列标准所包含的条文,通过在本标准中引用而构成为本标准的条文。本标准出版时,所示版本均为有效。所有标准都会被修订,使用本标准的各方应探讨使用下列标准最新版本的可能性。

GB/T 9387.2—1995 信息处理系统 开放系统互连 基本参考模型 第2部分:安全体系结构

#### 3 定义和记法约定

本章给出本标准中使用的术语和记法约定。

##### 3.1 定义

###### 3.1.1 用户 user

在防火墙之外,但与防火墙相互作用的人,他不具有影响防火墙安全策略执行的特权。

###### 3.1.2 授权管理员 authorized administrator

任何具有旁路或绕过防火墙安全策略权限的授权人,本标准中的“授权管理员”严格定义为防火墙的管理员,他不具有网络管理的职责。

###### 3.1.3 主机 host

在防火墙之外,但与防火墙相互作用的计算机,它不具有影响防火墙安全策略执行的特权。

###### 3.1.4 可信主机 trusted host

任何具有旁路或绕过防火墙安全策略权限的授权计算机。

##### 3.2 记法约定

细化:用于增加某一功能要求的细节,从而进一步限制该项要求。对功能要求的细化用**黑体字**表示。示例见 7.1.2.3。

选择:用于在对某一功能要求的陈述中,突出一个或多个选项,用带下划线的斜体字表示。示例见 7.1.5.2。

赋值:用于将一个特定值赋给某个未定参数,如某个口令字的长度。赋值出现在方括号中,[要赋予的值]表示某个值。示例见 7.1.1.3。

#### 4 应用级防火墙概述

本标准规定了应用级防火墙在低风险(敏感但不保密)环境下的最低安全要求。明确了应用级防火