ICS 35.020
L 09

中华人民共和国国家标准

GB/T 20010—2005

信息安全技术
包过滤防火墙评估准则

Information security technology —
Packet filtering firewalls evaluation criteria

2005-11-11 发布　　2006-05-01 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

GB 17859—1999《计算机信息系统安全保护等级划分准则》是我国计算机信息系统安全等级管理的重要标准，已于1999年9月13日发布。为促进安全等级管理工作的正常有序开展，特制定一系列相关的标准。本标准是系列标准之一。

本标准文本中，黑体字表示较低等级中没有出现或增强的评估内容。

本标准的附录A中说明防火墙面临的主要威胁和对策。

本标准的附录A是资料性附录。

本标准由全国信息安全标准化技术委员会提出并归口。

本标准起草单位：北京大学软件工程国家工程中心，公安部公共信息网络安全监察局。

本标准主要起草人：王立福、刘学洋、赵学志、张劲飞、张晰。

引　言

防火墙是内部、外部两个网络之间的一个阻隔，通过允许和拒绝经过防火墙的数据流，防止不希望的、未授权的通信，并实现对进、出内部网络的服务和访问的审计和控制。防火墙对网络用户提供访问控制服务和通信安全服务，对网络用户基本上是“透明”的，并且只有授权的管理员方可对防火墙进行管理。

防火墙一般要解决的安全问题可分为被保护系统（即内部网）的安全问题和自身的安全问题。

防火墙产品主要分为两类：包过滤和应用级防火墙。本标准规定了包过滤防火墙的各级安全要求。包过滤防火墙根据安全功能策略建立包过滤规则。过滤规则的主要要素有源 IP 地址、目的 IP 地址、协议号、源端口、目的端口、连接标志和另外一些 IP 选项，以及包到达或发出的接口。

信息安全技术
包过滤防火墙评估准则

1 范围

本标准从信息技术方面规定了按照 GB 17859—1999 的五个安全保护等级对采用“传输控制协议/网间协议(TCP/IP)”的包过滤防火墙产品安全保护等级划分所需要的评估内容。

本标准适用于包过滤防火墙安全保护等级的评估,对于包过滤防火墙的研制、开发、测试和产品采购也可参照使用。

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

3 术语和定义

GB 17859—1999 确立的以及下列术语和定义适用于本标准。

3.1

主机 host

一台与防火墙相互作用的机器,它在防火墙安全功能策略控制下进行通信。

3.2

用户 user

一个在防火墙安全功能策略的控制下,通过防火墙访问外部网络或内部网络的人,此人不具有能影响防火墙安全功能策略执行的特权。

3.3

授权管理员 authorized administrator

能访问、实施、修改防火墙安全功能策略的个人,其职责仅限定于对防火墙的管理,不包括系统管理和网络管理。

3.4

可信主机 trusted host

允许授权管理员对防火墙进行远程管理的机器。

3.5

鉴别数据 authentication data

用来确认授权管理员和可信主机身份的信息。

4 安全环境

4.1 物理方面

对防火墙资源的处理限定在一些可控制的访问设备内,防止未授权的物理访问。所有与实施防火