ICS 35.040
A 90

GA

中华人民共和国公共安全行业标准

GA/T 681—2007

信息安全技术　网关安全技术要求

Information security technology—Technical requirements of gateway

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

本标准从信息技术方面详细规定了各安全保护级别的网关系统所应具有的安全功能要求和安全保证要求。

本标准的附录 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：荆继武、冯登国、夏鲁宁、王琼霄、许良玉、聂晓峰、黄敏、高能、林璟锵、吕欣、廖洪銮。

引　言

本标准用以指导设计者如何设计和实现具有所需安全等级的网关产品，主要从对网关的安全保护等级进行划分的角度来说明其技术要求，即主要说明为实现 GB 17859—1999 中每一个安全保护等级的安全要求对网关应采取的安全技术措施，以及各安全技术要求在不同安全保护等级中的具体差异。

本标准按 GB 17859—1999 五个安全保护等级的划分，对每一个安全保护等级的安全功能技术要求和安全保证技术要求做了详细描述。文中每一级别比上一级别新增的要求以加粗字表示。

信息安全技术　网关安全技术要求

1　范围

本标准规定了按 GB 17859—1999 对网关进行安全等级保护划分所需要的详细技术要求。

本标准适用于按 GB 17859—1999 的要求所进行的网关的设计和实现。按 GB 17859—1999 的要求对网关进行的测试、配置也可参照使用。

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

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　术语和定义

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

3.1

主机　host

主机指连接到一个或多个网络的设备，它可以向任何一个网络发送和接收数据，它在网关安全功能策略控制下进行通信。

3.2

用户　user

在网关中，用户与管理员同义，是指能访问网关并对网关进行管理和维护的个人。

注：为保持文中规范性语言与已有标准的一致性如“用户-主体绑定”等，本标准仍保留“用户”这个术语，而不是统一叫做“管理员”。

3.3

授权管理员　authorized administrator

能访问、实施、修改网关安全功能策略的个人，其职责仅限定于对网关的管理。

3.4

可信主机　trusted host

允许授权管理员对网关进行远程管理的主机。

3.5

网关　gateway

网关是一种网络连接设备，实现不同网络之间的互连。

3.6

网关安全设施　trusted computing base(TCB) of gateway

在网关系统中，网关的可信计算基是网关中保护装置的总称，包括硬件、固件、软件和负责执行安全策略的组合体，在本标准中称为网关安全设施。它建立一个基本的保护环境，并提供网关所要求的附加服务。在网关系统中，网关安全设施是物理上分散、逻辑上统一分布的。