ICS 35.040
A 90

GA

中华人民共和国公共安全行业标准

GA/T 682—2007

信息安全技术
路由器安全技术要求

Information security technology—
Technical requirements for router 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

本标准与GB/T 20011—2005《信息安全技术　路由器安全评估准则》均为与路由器有关的信息安全标准，两者的基本区别是，前者主要适用于指导路由器产品安全性的设计和实现，后者主要适用于路由器安全等级的评估。

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：戴英侠、左晓栋、何申。

引　言

路由器是重要的网络互连设备，制定路由器安全技术要求对于指导路由器产品安全性的设计和实现，保障网络安全具有重要的意义。

本标准分三个等级规定了路由器的安全技术要求。安全等级由低到高，安全要求逐级增强。

本标准与 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
路由器安全技术要求

1 范围

本标准分等级规定了路由器的安全功能要求和安全保证要求。

本标准适用于路由器产品安全性的设计和实现，对路由器产品进行的测试、评估和管理也可参照使用。

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、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

路由器 router

网络节点设备，工作在网络层，通过路由选择算法决定流经数据的存储转发，并具备访问控制和安全扩展功能。

3.1.2

简单网络管理协议 simple network management protocol

简单网络管理协议（SNMP）是一系列协议组和规范，提供了一种从网络上的设备中收集网络管理信息的方法，也为设备向网络管理工作站报告问题和错误提供了一种方法。

3.1.3

单播逆向路径转发 unicast reverse path forwarding

单播逆向路径转发（URPF）通过获取包的源地址和入接口，以源地址为目的地址，在转发表中查找源地址对应的接口是否与入接口匹配，如果不匹配，则认为源地址是伪装的，丢弃该包。其功能是防止基于源地址欺骗的网络攻击行为。

3.2 缩略语

下列缩略语适用于本标准。

ACL Access Control List 访问控制列表

ALG Application Layer Gateway 应用网关

IDS Instrusion Detection System 入侵检测系统

IPSec Internet Protocol Security Internet 协议安全

MPLS Multi-Protocol Label Switching 多协议标记交换