ICS 35.020
L 09

中华人民共和国国家标准

GB/T 20011—2005

信息安全技术
路由器安全评估准则

Information security technology —
Routers security 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

中 华 人 民 共 和 国
国 家 标 准
信息安全技术
路由器安全评估准则
GB/T 20011—2005
*
中国标准出版社出版发行
北京西城区复兴门外三里河北街16号
邮政编码:100045
http://www.spc.net.cn
电话:63787337、63787447
2006年5月第一版 2006年5月电子版制作
*
书号:155066·1-27495

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中说明路由器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，张昕，葛佳，赵学志，刘学洋。

引　言

路由器是在开放系统互连参考模型(OSI/RM)第三层——网络层上实现中继的一种网络互连设备。它根据网络层的信息,采用某种路由算法,为在网络上传送的数据包从若干条路由中选择一条到达目的地的通路。

为了准确有效的转发数据包,路由器应创建和维护路由表。路由表通过路由协议来获得路由信息,以支持动态的路由选择。常用的路由协议有:路由信息协议 RIP、开放式最短路径优先协议 OSPF、边界网关协议 BGP 等。

路由器通过访问控制表,按确定的一组访问规则,允许或拒绝信息流通过一个或多个路由器接口。

信息安全技术
路由器安全评估准则

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中的前三个等级，对路由器产品安全保护等级划分所需要的评估内容。

本标准适用于路由器安全保护等级的评估，对路由器的研制、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 所确立的术语和定义适用于本标准。

4 安全环境

4.1 物理方面

对路由器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。所有与实施路由器安全策略相关的硬件和软件应受到保护以免于未授权的物理修改。

4.2 人员方面

有一个或多个能胜任的授权用户来管理路由器及所包含的信息。管理员遵从管理员指南实施管理，可能有偶然的失误，但不是恶意或敌对。

4.3 连通性方面

用户可以通过网络使用路由器。

5 评估内容

5.1 用户自主保护级

5.1.1 自主访问控制

安全功能将执行自主访问控制策略。通过管理员属性表，控制不同管理员对路由器的配置数据和其他数据的查看、修改，以及对路由器上程序的执行，阻止非授权管理员进行上述活动。

5.1.2 身份鉴别

在管理员进入与系统会话之前，安全功能应鉴别管理员身份。对于远程会话，需要被鉴别的信息包括网络接入的管理员身份、远程管理站身份等。

5.1.3 用户数据保护

路由器运行过程中，安全功能提供对特定类型数据包的鉴别功能，以确认数据包的有效性。

对于路由器转发的数据包，安全功能应监视数据包中用户数据的完整性，防止用户数据在路由器上存储转发期间被破坏。