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。

5.1.4 安全管理

路由器的安全配置参数要有初始值。

安全功能应具备划分管理员级别和规定相关权限(如监视、维护配置等)的能力。例如,将管理员划分为高、低两个级别:

a) 低级别管理员对路由器的运行实施监视,并能查询路由器的当前配置;

b) 高级别管理员对路由器的运行实施监视,并能维护路由器的当前配置。

5.1.5 配置管理

开发者用路由器版本号作为它的引用标签。对路由器的每一个版本,版本号应是唯一的。

5.1.6 安全功能开发过程

开发者应提供路由器的功能规约。功能规约以非形式化风格来描述安全功能以及其外部接口,并完备地、一致地表示安全功能。

5.1.7 指导性文档

开发者应提供系统管理员的管理员指南。管理员指南应描述对于授权安全管理角色可使用的管理功能和接口、对路由器进行安全管理的方式、受控制的安全参数以及与安全操作有关的用户行为的假设。管理员指南应与为路由器评估而提供的其他所有文件保持一致。

5.1.8 测试

开发者应提供测试覆盖的证据。测试覆盖的证据应表明测试文档中所标识的测试和功能规约中所描述的安全功能之间的对应性。

5.1.9 交付和运行

开发者应以文档方式描述对路由器进行安全的安装、生成和启动的过程。

5.2 系统审计保护级

5.2.1 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。

5.2.2 身份鉴别

在管理员进入与系统会话之前,安全功能应鉴别用户身份。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。

5.2.3 客体重用

安全功能应确保数据包在被路由器系统成功转发后,没有可用的遗留信息。一般利用多次重写的办法来实现。

5.2.4 审计

路由器安全功能应能为路由器的可审计事件生成一个审计记录,并在每一个审计记录中至少记录以下信息:

——事件发生的日期和时间;

——事件的类型;

——用户身份;

——事件的结果(成功或失败)。

路由器安全功能应能维护路由器的可审计事件,但其中至少包括:

——审计功能的启动和终止事件;

——帐户管理的成功和失败;

——登录事件的成功和失败;

——对象(例如:路由表、访问控制表等)访问失败;

——系统事件的成功和失败等。

路由器安全功能应提供给已授权的管理员从审计记录中读取审计信息的能力，安全功能为管理员提供的审计记录具有唯一、明确的定义和方便阅读的格式。

路由器安全功能应能保护已存储的审计记录，避免未经授权的删除，并能监测和防止对审计记录的修改。当审计存储耗尽、失败或受到攻击时，安全功能应确保最近的审计记录在一定的时间内不会被破坏。

路由器安全功能在检测到可能有安全侵害发生时，应做出响应，如：通知管理员，向管理员提供一组遏制侵害的或采取校正的行动。

5.2.5 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。

对于提供 IP 包过滤功能的路由器，应满足以下要求：

a） 为了实现基于 IP 地址的过滤，管理员可以使用地址通配符进行过滤表的设置，实现如对 IP 协议、TCP 协议、UDP 协议、ICMP 协议和相应协议端口的过滤；

b） 具有识别内外网络地址的能力，防止外部网络冒用内部地址；

c） 具有识别低层网络地址假冒的能力；

d） 过滤表的大小只受系统资源的限制；

e） 能设置告警策略；

f） 管理员可以设置以下功能是否起作用：

1） 禁止分段过小的数据包通过，最小长度可以设置，并有一个建议值，在管理员设置值小于该值时予以提示；

2） 禁止源端路由的数据包通过；

3） 禁止数据包分段偏移值异常的数据包通过，异常偏移值可以设置，并有一个建议值，在管理员设置值小于该值时予以提示。

安全功能具备用加密的方式转发路由器运行中的数据包的能力。

5.2.6 安全功能保护

路由器应有自引导功能，在初始启动期间，不能在安全功能发挥作用之前从网络获取引导信息。路由器初始化的选项由管理员进行管理，如开放或关闭某些应用程序等。

5.2.7 安全管理

路由器的安全配置参数要有初始值。路由器安装后，安全功能应能及时提醒管理员修改配置，并能周期性地提醒管理员维护配置。

安全功能应具备划分管理员级别和规定相关权限（如监视、维护配置等）的能力。例如，将管理员划分为高、低两个级别：

a） 低级别管理员对路由器的运行实施监视，并能查询路由器的当前配置；

b） 高级别管理员对路由器的运行实施监视，并能维护路由器的当前配置。

5.2.8 配置管理

开发者用路由器版本号作为它的引用标签，并使用配置管理系统、提供管理文档。对路由器的每一个版本，版本号应是唯一的。配置管理文档应包括配置清单，它描述生成路由器的配置项。

开发者应提供配置管理文档。配置管理文档应说明配置管理系统至少能跟踪以下几项：路由器实现的表示、设计文档、测试文档、用户文档、管理员文档和配置管理文档。配置管理文档应描述配置管理系统是如何跟踪配置项的。

5.2.9 安全功能开发过程

开发者应提供路由器的功能规约。功能规约以非形式化风格来描述安全功能以及其外部接口，并

完备地、一致地表示安全功能。

开发者应提供路由器安全功能的高层设计。高层设计应按子系统描述安全功能及其结构，并标识安全功能子系统的所有接口。高层设计还应标识实现安全功能所要求的基础性的硬件、固件和软件。

开发者应提供路由器安全功能的功能规约与高层设计之间的对应性分析，该分析应证明功能规约表示的所有相关安全功能都在高层设计中得到正确且完备的细化。

5.2.10 指导性文档

开发者应提供系统管理员的管理员指南。管理员指南应描述对于授权安全管理角色可使用的管理功能和接口、对路由器进行安全管理的方式、受控制的安全参数以及与安全操作有关的用户行为的假设。管理员指南应与为路由器评估而提供的其他所有文件保持一致。

5.2.11 生存周期支持

开发者提供开发安全文件。开发安全文件应描述在路由器的开发环境中，用以在物理上、程序上、人员上以及其他方面上保护路由器设计和实现的保密性和完整性所必要的安全措施，并提供执行安全措施的证据。

5.2.12 测试

开发者应提供测试覆盖的证据。测试覆盖的证据应表明测试文档中所标识的测试和功能规约中所描述的安全功能之间的对应性。

开发者应提供测试深度的分析。在深度分析中应给出：对于测试文档所标识的测试，足以说明安全功能的实现和高层设计是一致的。

开发者应测试安全功能，并提供测试结果的文档。测试文档应包括测试计划、测试程序描述，预期的测试结果和实际测试结果；测试计划应标识要测试的安全功能，描述要执行的安全目标；测试过程描述应标识要执行的测试，并描述每个安全功能的测试概况，这些概况包括对于其他测试结果的顺序依赖性；期望的测试结果应表明成功测试运行后的预期输出；实际测试的结果应阐明了每个被测试的安全功能已按照规定进行运作了。

5.2.13 脆弱性分析

开发者应提供指南性文档和分析文档。指南性文档应确定对路由器的所有可能的操作方式（包括失败和操作失误后的操作）的后果以及对于保持安全操作的意义，并列出所有目标环境的假设和所有的外部安全措施（包括外部程序的、物理的或人员控制）要求。所述内容应是完备的、清晰的、一致的、合理的，并在分析文档应阐明指南性文档是完备的。

开发者应对用于路由器的、并具有安全功能强度声明的安全机制（例如口令机制）进行安全功能强度分析。安全功能强度分析应证明安全机制达到了所声明的强度。

开发者应实施脆弱性分析，并提供脆弱性分布的文档。对所有已标识的脆弱性，文档应说明它们在所期望的路由器使用环境中不能被利用。

5.2.14 交付和运行

开发者应以文档方式描述对路由器进行安全的安装、生成和启动的过程。

开发者以文档的形式将路由器（系统）或其部分提供给用户，为维护安全性应使用一定的分发程序。分发文档应向用户说明这一程序。

5.3 安全标记保护级

5.3.1 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。

5.3.2 强制访问控制

路由器安全功能应通过管理员和路由器安全功能数据的敏感标记，控制管理员对相关安全功能数据的直接访问。

5.3.3 标记

路由器对所有客体(路由表、访问表、审计记录、管理员属性表等)和主体(管理员以及所启动的程序)都指定并维护敏感标记。

5.3.4 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管理员身份、远程管理站身份等。

安全功能应对所有鉴别信息提供安全保护措施(如对管理员身份进行加密),以防止管理员身份鉴别数据的泄露。

安全功能应周期性地确认管理员身份,如果管理员未进行操作的时间超过一定时限,当管理员再次操作时,安全功能应对管理员身份重新进行鉴别。时限由授权管理员设置。

当管理员被鉴别时,安全功能仅反馈鉴别是否成功或其他简单信息。

安全功能应检测到管理员登录鉴别失败的出现,当达到预先所规定的次数时,安全功能应采取一定的措施如锁定界面、中断链接或锁定账号。

5.3.5 客体重用

安全功能应确保数据包在被路由器系统成功转发后,没有可用的遗留信息。一般利用多次重写的办法来实现。

5.3.6 审计

路由器安全功能应能为路由器的可审计事件生成一个审计记录,并在每一个审计记录中至少记录以下信息:

——事件发生的日期和时间;

——事件的类型;

——用户身份;

——事件的结果(成功或失败)。

路由器安全功能应能维护路由器的可审计事件,但其中至少包括:

——审计功能的启动和终止事件;

——帐户管理的成功和失败;

——登录事件的成功和失败;

——对象(例如:路由表、访问控制表等)访问失败;

——系统事件的成功和失败等。

路由器安全功能应提供给已授权的管理员从审计记录中读取审计信息的能力,安全功能为管理员提供的审计记录具有唯一、明确的定义和方便阅读的格式。

路由器安全功能应能保护已存储的审计记录,避免未经授权的删除,并能监测和防止对审计记录的修改。当审计存储耗尽、失败或受到攻击时,安全功能应确保最近的审计记录在一定的时间内不会被破坏。

当审计记录超过预定的限制值时,路由器安全功能应采取相应的行动,如:给授权管理员产生警告。

路由器安全功能应能监控可审计事件,并指出潜在的侵害。

路由器安全功能在检测到可能有安全侵害发生时,应做出响应,如:通知管理员,向管理员提供一组遏制侵害的或采取校正的行动。

5.3.7 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。

对于提供 IP 包过滤功能的路由器,应满足以下要求:

a) 为了实现基于IP地址的过滤，管理员可以使用地址通配符进行过滤表的设置，实现如对IP协议、TCP协议、UDP协议、ICMP协议和相应协议端口的过滤；
b) 具有识别内外网络地址的能力，防止外部网络冒用内部地址；
c) 具有识别低层网络地址假冒的能力；
d) 过滤表的大小只受系统资源的限制；
e) 能设置告警策略；
f) 管理员可以设置以下功能是否起作用：
   1) 禁止分段过小的数据包通过，最小长度可以设置，并有一个建议值，在管理员设置的值小于该值时给予提示；
   2) 禁止源端路由的数据包通过；
   3) 禁止数据包分段偏移值异常的数据包通过，异常偏移值可以设置，并有一个建议值，在管理员设置值小于该值时予以提示。

安全功能具备用加密的方式转发路由器运行中的数据包的能力。

通过实施一定的信息流控制策略（例如禁止一切没有得到明确允许的信息流），安全功能防止数据包规避IP包过滤策略而流经路由器。

安全功能应能为传送的数据包产生完整性标记，并能建立一定机制（如可信信道），来判别并保护数据包交换的完整性。

5.3.8 可信路径

安全功能应在已达到二级的路由器之间建立一条可信路径，该路径具有对安全数据的保护能力。对于要求安全性的数据包，应通过此路径进行传输。

安全功能应能和（远程）用户间建立一条可信路径，它提供数据保护，并在逻辑上明显不同于其他路径，从而实现用户的（远程）接入、（远程）管理等功能。

安全功能应能对路由器转发的数据包产生原发证据，并能验证它的有效性。原发证据是与发送数据包的路由器的属性相关联的。

安全功能应能对路由器接受的数据包产生接收证据，并能验证它的有效性。接收证据是与接收数据包的路由器的属性相关联的。

5.3.9 安全功能保护

路由器应有自引导功能，在初始启动期间，不能在安全功能发挥作用之前从网络获取引导信息。路由器初始化的选项由管理员进行管理，如开放或关闭某些应用程序等。

路由器安全功能应保护需经过网络传输的路由器安全功能数据（如：路由表数据，访问控制表数据等），防止此类数据被泄漏及篡改。路由器安全功能应能支持路由器间的可信鉴别。

路由器发生失败或中断后，安全功能应使其进入维护方式，并具备将路由器返回到一个安全状态的能力。

安全功能应能为自身的应用提供可靠的时间戳，以支持身份鉴别、安全审计等其他各种安全功能的实现。

5.3.10 安全管理

路由器的安全配置参数要有初始值。路由器安装后，安全功能应能及时提醒管理员修改配置，并能周期性地提醒管理员维护配置。

安全功能应具备划分管理员级别和规定相关权限（如监视、维护配置等）的能力。例如，将管理员划分为高、中、低三个级别：

a) 低级别管理员只能对路由器的运行实施监视；
b) 中级别管理员对路由器的运行实施监视，并能查询路由器的当前配置；
c) 高级别管理员对路由器的运行实施监视，并能维护路由器的当前配置。

安全功能支持将管理员的权限范围进行分工，即限定管理员只能完成某一方面的工作，各项工作之间不可互相替代。

对于路由器中主体和客体所具有的敏感标记，安全功能只允许授权的管理员建立和维护这些敏感标记。

5.3.11 配置管理

开发者应使用配置管理系统，并提供配置管理计划。配置管理系统应确保对路由器的实现表示只能进行已授权的改变；配置管理计划应描述在配置管理系统中使用的工具软件，并描述如何使用这些工具。

开发者用路由器版本号作为它的引用标签，并使用配置管理系统、提供管理文档。对路由器的每一个版本，版本号应是唯一的。配置管理文档应包括配置清单和一个配置管理计划和接受计划。配置清单描述生成路由器的配置项，配置管理计划描述系统是怎样使用的，接受计划描述用来接受修改过的或新建的配置项的程序。

开发者应提供配置管理文档。配置管理文档应说明配置管理系统至少能跟踪以下几项：路由器实现的表示、设计文档、测试文档、用户文档、管理员文档和配置管理文档。配置管理文档应描述配置管理系统是如何跟踪配置项的。

5.3.12 安全功能开发过程

开发者应提供路由器的功能规约。功能规约以非形式化风格来描述安全功能以及其外部接口，并完备地、一致地表示安全功能。功能规约应给出每一安全功能的接口定义，用以证明完备地描述了路由器安全功能。

开发者应提供路由器安全功能的实现表示。实现表示应是内在一致的，并且无歧义地定义了详细的路由器安全功能。

开发者应提供路由器安全功能的高层设计。高层设计应按子系统描述安全功能及其结构，并标识安全功能子系统的所有接口。高层设计还应标识实现安全功能所要求的基础性的硬件、固件和软件。高层设计还应描述安全功能子系统所有接口及使用接口的目的和方法，并详细描述接口的返回结果、例外情况和错误信息等，以及如何将路由器中有助于增强安全策略的子系统分离出来。

开发者应提供路由器安全功能的低层设计。低层设计应以模块术语描述安全功能，并描述每一个模块的目的、接口和相互间的关系。低层设计还应描述如何将路由器中有助于增强安全策略的模块分离出来。

开发者提供的相邻两阶段开发文档应提供对相邻的路由器安全功能表示之间的对应性分析，该对应性分析应阐明上一阶段的安全功能表示在下一阶段文档中得到正确而完备地细化。

开发者应提供安全策略模型，并阐明该模型和路由器功能规约之间的对应性，这一对应性是一致和完备的。安全策略模型是非形式化的。该模型应描述所有可以模型化的安全策略的规则和特征，并包括一个基本原理，即阐明该模型对于所有可模型化的安全策略来说，是与其一致的，而且是完备的。

5.3.13 指导性文档

开发者应提供系统管理员的管理员指南。管理员指南应描述对于授权安全管理角色可使用的管理功能和接口、对路由器进行安全管理的方式、受控制的安全参数以及与安全操作有关的用户行为的假设。管理员指南应与为路由器评估而提供的其他所有文件保持一致。

5.3.14 生存周期支持

开发者应提供开发安全文件。开发安全文件应描述在路由器的开发环境中，用以在物理上、程序上、人员上以及其他方面上保护路由器设计和实现的保密性和完整性所必要的安全措施，并提供执行安全措施的证据。

开发者应建立用于开发和维护路由器的生存周期模型，并提供生存周期定义文档。生存周期定义文件应描述用于开发和维护路由器的模型，该模型应给出开发和维护路由器的必要的控制。

开发者应描述用于开发路由器所使用的工具和参照标准，并提供关于已选择的开发工具选项的描述文档。开发工具文档应明确说明所有开发工具选项的含义。

5.3.15 测试

开发者应提供测试覆盖的分析。测试覆盖的分析应表明测试文档中所标识的测试和功能规约中所描述的安全功能之间的对应性，并说明该对应性是完备的。

开发者应提供测试深度的分析。在深度分析中应给出：对于测试文档所标识的测试，足以说明安全功能的实现和高层设计是一致的。

开发者应测试安全功能，并提供测试结果的文档。测试文档应包括测试计划、测试程序描述，预期的测试结果和实际测试结果；测试计划应标识要测试的安全功能，描述要执行的安全目标；测试过程描述应标识要执行的测试，并描述每个安全功能的测试概况，这些概况包括对于其他测试结果的顺序依赖性；期望的测试结果应表明成功测试运行后的预期输出；实际测试的结果应阐明每个被测试的安全功能已按照规定进行运作了。

5.3.16 脆弱性分析

开发者应提供指南性文档和分析文档。指南性文档应确定对路由器的所有可能的操作方式（包括失败和操作失误后的操作）的后果以及对于保持安全操作的意义，并列出所有目标环境的假设和所有的外部安全措施（包括外部程序的、物理的或人员控制）要求。所述内容应是完备的、清晰的、一致的、合理的，并在分析文档应阐明指南性文档是完备的。

开发者应对用于路由器的、并具有安全功能强度声明的安全机制（例如口令机制）进行安全功能强度分析。安全功能强度分析应证明安全机制达到了所声明的强度。

开发者应实施脆弱性分析，并提供脆弱性分布的文档。对所有已标识的脆弱性，文档应说明它们在所期望的路由器使用环境中不能被利用。

5.3.17 交付和运行

开发者应以文档方式描述对路由器进行安全的安装、生成和启动的过程。

开发者以文档的形式将路由器（系统）或其部分提供给用户，为维护安全性应使用一定的分发程序。分发文档应向用户说明这一程序，并描述如何使用各种方法和技术措施来监测对系统的修改，或者描述开发者的主拷贝和用户所收到的版本之间的差异。

附 录 A
（资料性附录）
路由器面临的威胁和对策

A.1 路由器可能面对的主要威胁

a） 未授权的用户尝试避开路由器的安全措施，存取路由器中的数据信息；
b） 未授权的用户猜测鉴别信息，从而利用此信息发起对路由器的攻击；
c） 未授权的用户使用未经许可的服务，使信息通过路由器（位于内部网络的出口），导致内部网络的资源被非法利用；
d） 未授权用户使用虚假 IP 地址，使信息流通过路由器；
e） 未授权用户查阅、修改或删除远程管理员与路由器之间传送的安全相关信息；
f） 管理员没有及时审阅审计信息，致使攻击者未能被发现；
g） 未授权用户通过使用耗费尽审计数据的存储容量方式，导致审计数据的丢失或无法继续记录审计数据；
h） 未授权用户向路由器发送攻击性数据包或在一定的时间间隔里，向路由器发送数量巨大的垃圾数据包，以此大量耗费路由器的系统资源，使其不能正常工作；
i） 路由器的重新启动导致路由信息的破坏；
j） 用户信息被转发到未授权的网络实体。

A.2 抵御威胁的方法

a） 只有授权管理员才可以登录系统。只有授权管理员才能对受保护资源（包括路由表、访问控制表、审计记录等）进行访问和修改；
b） 根据一定的原则，对受保护的资源确定访问权限；
c） 系统管理员应该监视与安全有关的事件。

GB/T 20011—2005

参 考 文 献

[1] GB/T 18018—1999 路由器安全技术要求

[2] ISO/IEC 15408：1999（所有部分） Common Criteria for Information Technology Security Evaluation

GB/T 20011-2005

*

书号：155066・1-27495