ICS 35.020
L 80

中华人民共和国国家标准

GB/T 18018—1999

路由器安全技术要求

Security requirements for router

1999-11-11 发布　　2000-05-01 实施

国家质量技术监督局　发布

目　　次

前　　言

本标准规定了传输控制协议/网间协议(TCP/IP)互联网络设备——路由器的安全功能要求。

本标准的附录 A 和附录 B 均是提示的附录。

本标准由国家信息化办公室提出。

本标准由全国信息技术标准化技术委员会归口。

本标准起草单位:电子部第 30 研究所、中国国家信息安全测评认证中心。

本标准主要起草人:张建军、龚奇敏、吴世忠、吴娅若、杜明钰。

中华人民共和国国家标准

路由器安全技术要求

GB/T 18018—1999

Security requirements for router

1 范围

本标准规定了采用传输控制协议/网间协议(TCP/IP)协议路由器的安全功能技术要求。

本标准适用于路由器安全功能的设计、研制、评估和路由器产品的选购。

2 引用标准

下列标准所包含的条文,通过在本标准中引用而构成为本标准的条文。本标准出版时,所示版本均为有效。所有标准都会被修订,使用本标准的各方应探讨使用下列标准最新版本的可能性。

GB/T 9387.2—1995 信息处理系统 开放系统互连 基本参考模型 第2部分:安全体系结构

3 定义

下列定义与GB/T 9387.2中的定义相同:

审订 audit

鉴别 authentication

密钥管理 key management

4 概述

4.1 路由器使用环境

路由器是一类专用的网络设备,它连接两个或更多的计算机网络,在这些网络之间转发数据包。路由器使用数据包中的目的地址选择该数据包的下一个发往地点。

路由器的典型使用环境如图1所示。

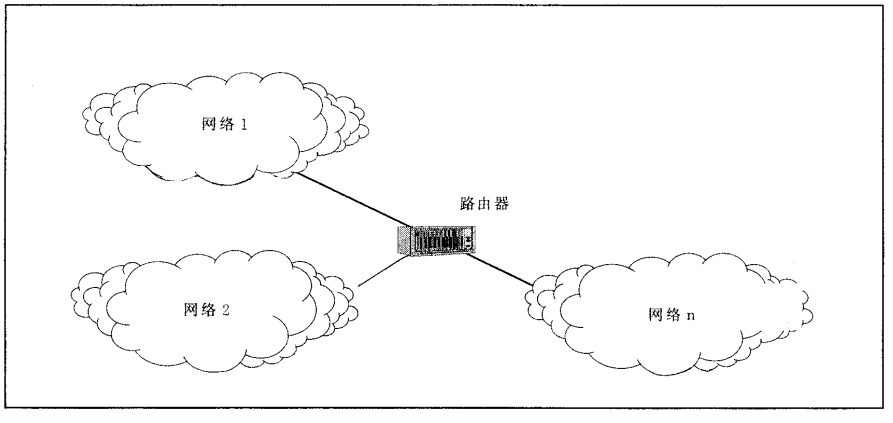

图1 路由器的典型使用环境

国家质量技术监督局1999-11-11批准 2000-05-01实施

4.2 安全目标

为防止经由路由器对网络的攻击和保护路由器自身的安全，要求达到以下全部或部分信息安全目标：

a）网络访问控制

路由器提供对网络访问控制的能力；

b）管理访问

路由器只能由授权管理员进行授权的管理；

c）审计

路由器能够记录对路由器的访问、操作；提供对网络信息流的记录和统计；

d）最小访问范围

路由器只能由管理员在路由器上执行必需的程序；

e）用户信息的保护

确保由路由器转发的用户信息的安全和保密；

f）支持密钥管理

在需要使用密码算法时，提供密钥管理的功能。

4.3 安全技术要求的描述方法

安全技术要求由安全功能类、安全功能组和安全组件三部分组成。

安全技术要求描述方法的组成如图 2 所示。

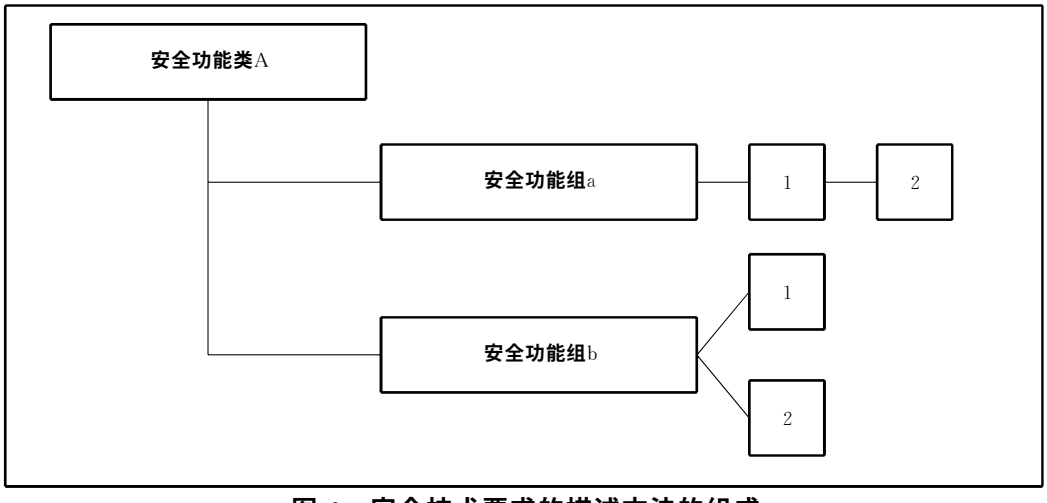

图 2 安全技术要求的描述方法的组成

该图表示安全功能类 A 包括安全功能组 a 和 b，各组分别包含 1、2 两个组件。对功能组 a，1、2 两个组件具有包含关系，2 不仅包括 1 中的安全要求，而且有所扩充。对功能组 b，1、2 两个组件相互独立，两者都可以满足功能组 b 的要求。

4.3.1 安全功能类

安全功能类的定义包括以下内容：

a）功能类的名称

每一个功能类都有一个唯一的标识名，并使用三个英文字母表示，本标准中使用该标识名唯一地标识相应的功能类。

b）功能类的描述

功能类的描述说明该功能类的内容，符合哪些安全目标的要求。功能类的描述还包括该功能类所包含的安全功能组。

4.3.2 安全功能组

安全功能组的定义包括以下内容：

a）功能组的名称

每一个功能组都有一个唯一的标识名，并使用七个字符表示，其格式为：头三个字母与该功能组所属功能类相同，后三个字母在该功能类中唯一地标识该功能组，前后两组字母之间使用下划线连接。标准中使用该名称唯一地标识相应的安全功能组。

b）功能组的描述

功能组的描述说明该功能组的内容，符合哪些安全目标的要求。功能组的描述还包括该功能组所包含的安全组件。

4.3.3 安全组件

安全组件的定义包括以下内容：

a）安全组件的标识

每一个安全组件都有一个唯一的标识名，以表示该组件所属的安全功能类、安全功能组，以及该组件在该组中的编号。

b）安全组件的描述

安全组件描述说明该组件的内容，符合哪些安全目标的要求。一般来说，每一台路由器在指定的安全功能组中只可能实现一个安全组件。

c）依赖关系

用于描述该安全组件与其他安全组件之间的关系。

4.4 路由器安全功能要求

表 1 路由器安全功能要求

编号	功能类		功能组	
	中文名称	标识名	中文名称	标识名
1	加密	FEN	密码算法	ALG
			密钥管理	KMG
2	鉴别	FIA	用户鉴别	UAU
3	审计	FAU	审计数据生成	GEN
			审计数据管理	MGT
			审计内容	CNT
4	路由器管理安全	FMS	管理员权限	RIG
			管理信息传输	TRA
			管理功能访问	FAC
			管理界面	INT
5	路由信息安全	FRS	路由信息安全	RIS
6	服务访问安全	FAS	网络互联访问	RRA
			远程用户接入	RUA
7	包过滤	FPF	包过滤	FIL
8	虚拟网络	FVN	虚拟网络	VPN
9	路由器初始化	FIN	引导	BOT
			出厂设置	DEF

4.5 参考文献

标准参考文献见附录 B。

5 加密功能类

加密功能类(FEN)包含两个功能组:密码算法功能组和密钥管理功能组。加密是安全技术的基础,也是其他安全功能组件所必须的,是保证路由器安全目标的基础。

加密功能类的组成如图 3 所示。

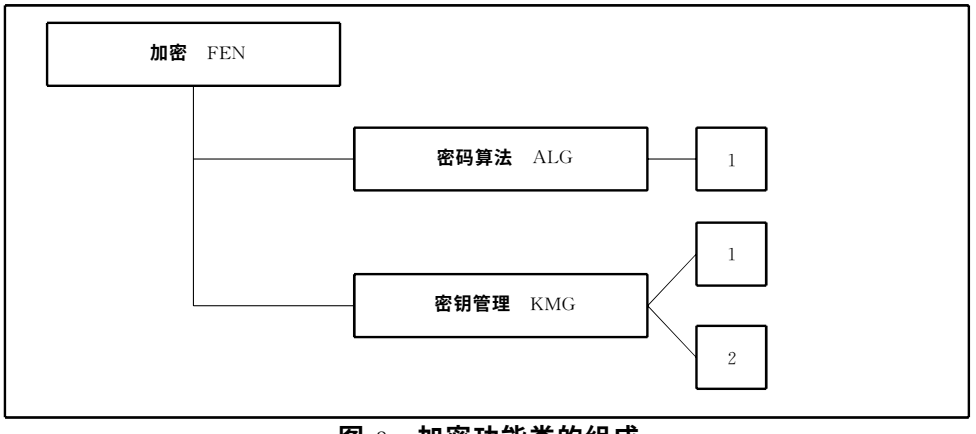

图 3 加密功能类的组成

5.1 密码算法功能组(FEN_ALG)

5.1.1 密码算法(FEN_ALG.1)

凡路由器中安全功能实现使用的密码算法,必须通过国家指定机构的审查。

本组件依赖于安全功能组 FEN_KMG。

5.2 密钥管理功能组(FEN_KMG)

密钥分配方案和密码算法,必须通过国家指定机构的审查。

5.2.1 人工分发密钥(FEN_KMG.1)

人工分发密钥。

5.2.2 自动分发密钥(FEN_KMG.2)

自动分发密钥。

6 鉴别功能类

鉴别功能类(FIA)包含一个功能组:用户鉴别功能组。鉴别功能是保证管理访问和访问控制目标的基础。

鉴别功能类的组成如图 4 所示。

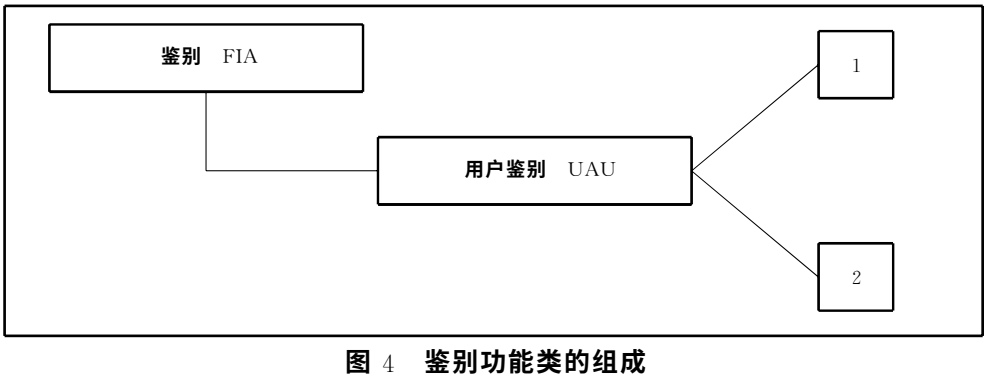

图 4 鉴别功能类的组成

6.1 用户鉴别功能组(FIA _ UAU)

6.1.1 基本鉴别(FIA _ UAU.1)

使用普通的明文口令方式实现鉴别,鉴别信息无安全保护措施。

6.1.2 强鉴别(FIA _ UAU.2)

采用经国家指定机构审批通过的鉴别协议和算法,所有鉴别信息均有相应的安全保护措施,其实现应通过国家指定机构的审查。

7 审计功能类

审计功能类(FAU)是路由器所有审计功能的基础,确保审计安全目标的实现。审计功能类包括三个功能组:审计数据生成、审计数据管理和审计内容。

审计功能类的组成如图 5 所示。

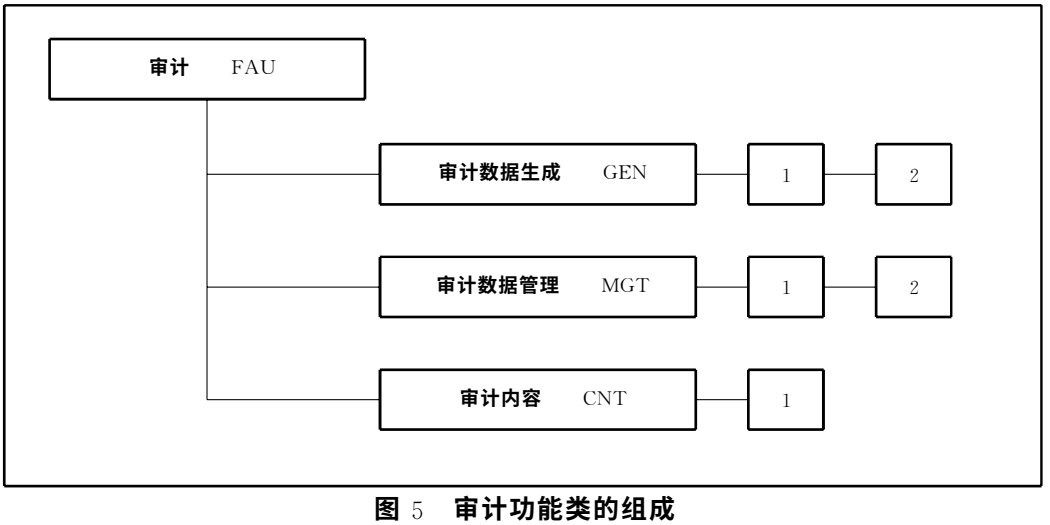

图 5 审计功能类的组成

7.1 审计数据生成功能组(FAU _ GEN)

7.1.1 事件记录生成(FAU _ GEN.1)

记录以下事件:

a) 审计功能的启动和终止事件;

b) 其他安全功能所要求记录的审计事件;

审计的记录至少包含以下内容:

事件发生的时间、事件类型、事件标识、事件内容。

7.1.2 用户标识生成(FAN _ GEN.2)

用户标识生成要求将审计事件与用户联系起来进行记录。

本功能组件依赖于 FIA 安全功能类。

7.2 审计数据管理功能组(FAU _ MGT)

7.2.1 基本审计数据管理(FAU _ MGT.1)

基本审计数据管理提供审计数据的存储、传送、转储的功能,审计数据具有唯一、明确定义的格式。

7.2.2 安全审计数据管理(FAU _ MGT.2)

安全审计数据管理在审计数据的管理过程中提供安全保护。

本组件依赖于 FEN 和 FIA 安全功能类。

7.3 审计内容安全功能组(FAU _ CNT)

7.3.1 审计内容(FAU _ CNT.1)

审计内容包括:

a）对通过的数据包进行统计，统计内容必须提供以下几方面的信息：

1）数据包过滤情况：通过的数据包数量、抛弃的数据包数量；

2）用户通信数据量：能够对指定的 IP 地址或低层地址进行通信数据量的统计；

3）访问记录：用户和管理员登录路由器的时间、途径，操作记录等。

b）统计报警功能：在用户统计值达到管理员设置的报警界限时进行报警。

c）日志记录功能：能够按照管理员的要求，以一定的时间间隔生成审计的记录，该记录的大小只受系统资源的限制。

d）数据截获能力：根据管理员的设置，对经由路由器转发的数据包进行监视、跟踪和截获，以供分析和故障诊断。

e）审计信息的转储：支持将审计信息转储到其他存储媒体中。

8 路由器管理安全功能类

路由器安全管理功能类(FMS)对路由器管理提出安全要求，管理活动的直接对象就是路由器。

路由器管理方式可以分为两种：远程管理和本地管理。

远程管理是指一个远程的管理站，采用标准的应用层协议(或者专用的协议)与路由器通信，实施对路由器的管理。

本地管理是指路由器与管理站使用专用的物理接口连接，该接口只供管理使用。

管理安全功能类包含四个功能组：管理权限、管理信息传送、管理功能访问及管理界面。

路由器管理安全功能类的组成如图 6 所示。

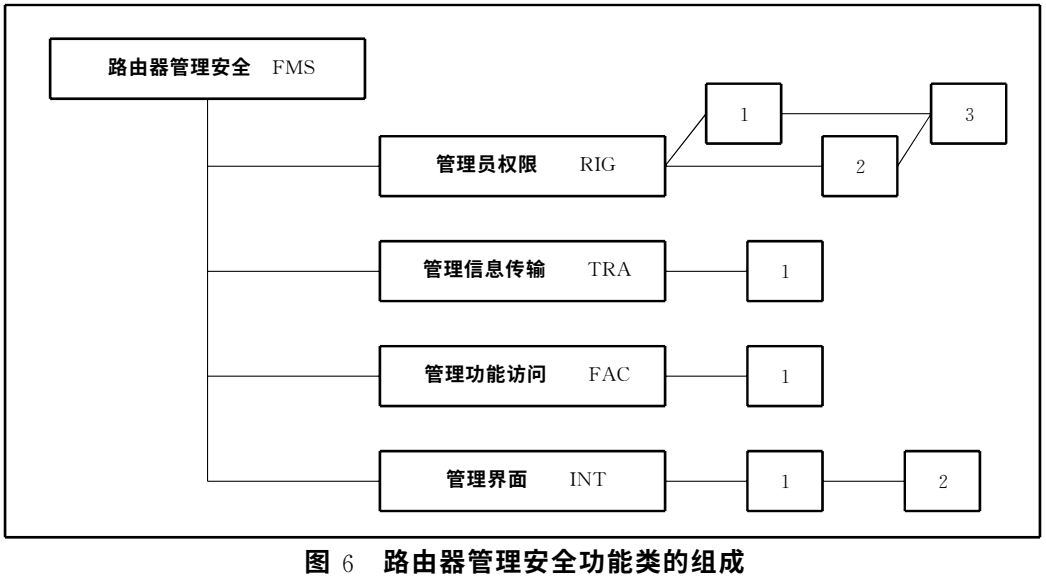

图 6 路由器管理安全功能类的组成

8.1 管理员权限功能组(M_RIG)

管理员权限指管理员对路由器所能实施的管理范围的限制。

8.1.1 三级管理(FMS_RIG.1)

此类管理设置高、中、低三个级别的管理员：

a）低级别管理员只能对路由器的运行实施监视；

b）中级别管理员可以对路由器的运行实施监视，查询路由器当前的配置；

c）高级别管理员可以对路由器的运行实施监视，查询路由器当前的配置，对路由器进行配置。

8.1.2 二级管理(FMS_RIG.2)

此类管理设置高、低两个级别的管理员：

a）低级别管理员可以对路由器的运行实施监视，查询路由器当前的配置；

b）高级别管理员可以对路由器的运行实施监视，查询路由器当前的配置，对路由器进行配置。

8.1.3 分工管理(FMS_RIG.3)

此类管理将管理员分为若干组，每一组的管理员只能完成某一方面的管理工作，每个组成员的管理工作不能相互替代。每一组内的管理员权限还可进一步细分。

8.2 管理信息传输安全功能组(FMS_TRA)

管理信息传输是指管理信息在管理站与路由器之间的传输。

8.2.1 安全传输(FMS_TRA.1)

路由器具有对管理信息传输安全的保障。对支持虚拟专网的路由器，在使用手册中必须以醒目方式提醒用户以虚拟专网方式传输管理信息。

本组件依赖于 FEN、FIA、FVN 功能类。

8.3 管理功能访问功能组(FMS_FAC)

管理功能的访问是指路由器只能由授权的管理站和管理员进行管理。

8.3.1 管理身份鉴别(FMS_FAC.1)

对于远程管理，路由器必须实现对管理站的身份鉴别和管理员的身份鉴别。对于本地管理，路由器必须实现对管理员身份的鉴别。

本安全组件依赖于 FEN 和 FIA 安全功能组。

8.4 管理界面安全功能组(FMS_INT)

管理界面是指管理员用于实施路由器管理的人机界面，本标准只规定由路由器直接提供的管理界面的安全要求。

8.4.1 基本管理界面(FMS_INT.1)

基本管理界面提供以下界面功能：

a）管理员登录；

b）界面超过规定时间后仍无操作时，自动降低管理员级别至最低级别，或锁定界面，或退出管理界面。时间可由管理员设置；

c）不同级别或不同职责的管理员其可以使用的命令相互间不可见。

本组件依赖于 FEN、FIA 安全功能类。

8.4.2 扩充管理界面(FMS_INT.2)

扩充管理界面除 FMS_INT.1 的功能外，还提供以下功能：

a）周期性要求管理员确认身份；

b）周期性提醒管理员修改出厂默认配置。

本组件依赖于 FEN、FIA 安全功能类。

9 路由信息安全功能类

路由信息是路由器有效工作的重要组成部分，确保路由信息的正确性、有效性是路由信息安全的目的。

路由信息安全功能类(FRS)包含一个功能组：路由信息安全。

路由信息安全功能类的组成如图 7 所示。

图 7 路由信息安全功能类

9.1 路由信息安全功能组(FRS_RIS)

9.1.1 路由信息鉴别(FRS_RIS.1)

路由器提供对路由信息的鉴别。

本组件依赖于 FIA 功能类。

9.1.2 路由信息加密(FRS_RIS.2)

路由器提供对路由信息的加密。

本组件依赖于 FEN 功能类。

9.1.3 路由信息的鉴别和加密(FRS_RIS.3)

路由器提供对路由信息的鉴别和加密。

本组件依赖于 FEN、FIA 功能类。

10 服务访问安全功能类

路由器提供两类服务:网络互联和用户远程接入服务。

服务访问安全功能类(FAS)包含两个功能组:网络互联和远程用户接入。

服务访问安全功能类的组成如图 8 所示。

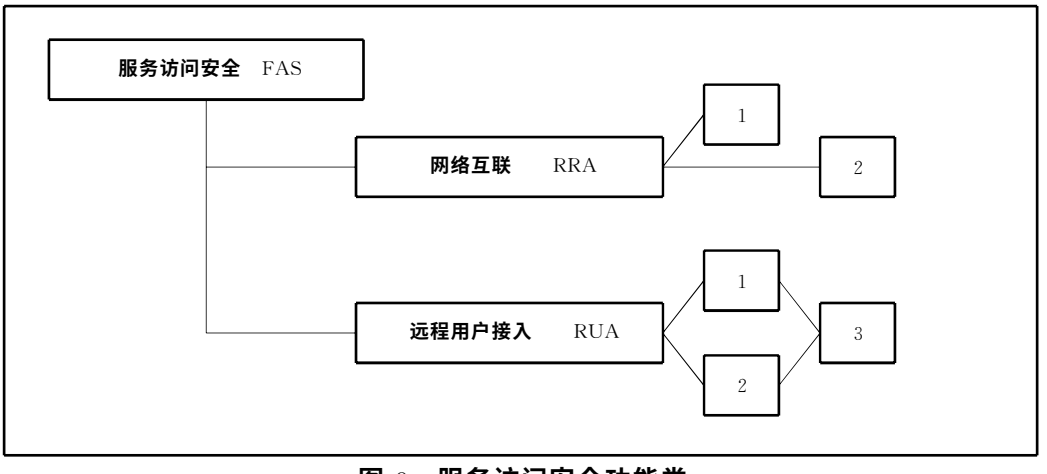

图 8 服务访问安全功能类

10.1 网络互联访问安全功能组(FAS_RRA)

10.1.1 低层协议鉴别(FAS_RRA.1)

利用低层协议提供的鉴别机制实现网络互联路由器之间的鉴别。

10.1.2 虚拟专网鉴别(FAC_RRA.2)

利用虚拟专网技术实现路由器之间的鉴别。

本组件依赖于 FVN 功能类。

10.2 远程用户接入安全功能组(RUA)

10.2.1 远程用户鉴别(FAS_RUA.1)

路由器提供对远程用户身份的鉴别。

本组件依赖于 FIA 功能类。

10.2.2 远程用户数据加密(FAS_RUA.2)

路由器提供对远程用户数据的加密。

本组件依赖于 FEN 功能类。

10.2.3 远程用户身份的鉴别和数据加密(FAS_RUA.3)

路由器提供对远程用户身份的鉴别和数据加密。

本组件依赖于 FIA、FEN 功能类。

11 包过滤功能类

包过滤功能类(FPF)包含一个功能组:包过滤。

包过滤功能类的组成如图 9 所示。

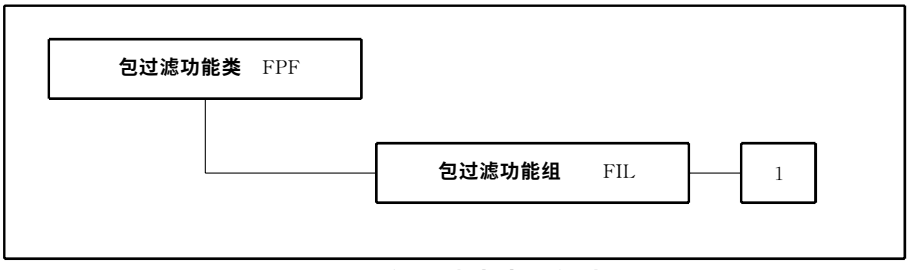

图 9 包过滤安全功能类

11.1 包过滤安全功能组(FPF_FIL)

11.1.1 IP 包过滤(FPF_FIL.1)

支持 IP 包过滤功能的路由器,必须满足以下要求:

a) 实现基于 IP 地址的过滤。用户可以使用地址通配符进行过滤表的设置,实现对网间协议(IP)、传输控制协议(TCP)、用户数据报协议(UDP)、互连控制消息协议(ICMP)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功能;

d) 能够设置告警策略;

e) 过滤表的大小只受系统资源的限制;

f) 具有以下功能,并且管理员可以设置其是否起作用:

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。

12 虚拟专网功能类

虚拟专网功能类(FVN)包含一个功能组:虚拟专网。

虚拟专网功能类的组成如图 10 所示。

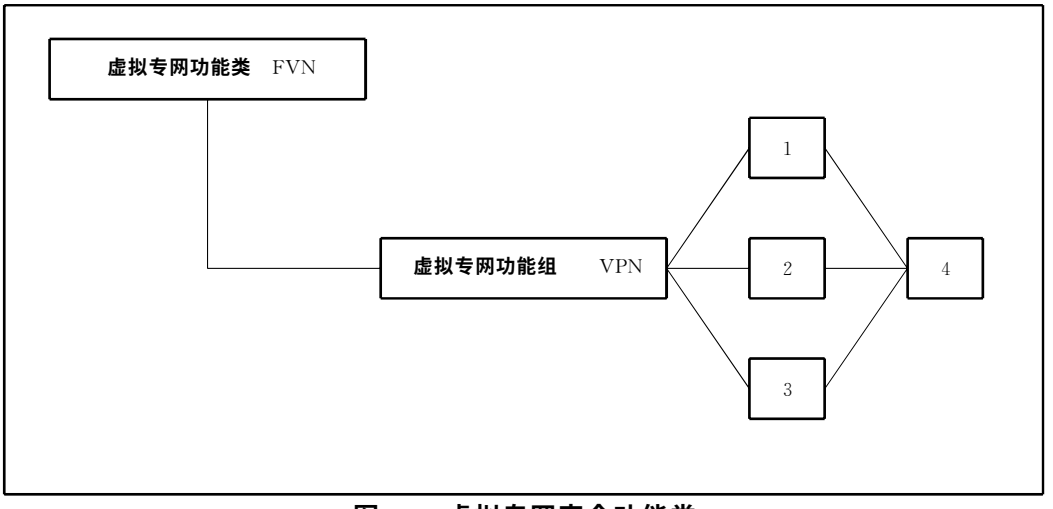

图 10 虚拟专网安全功能类

12.1 虚拟专网功能组(FVN _ VPN)

12.1.1 IP 鉴别(FVN _ VPN.1)

路由器使用 IP 包鉴别技术实现虚拟网络。

本组件依赖于 FIA 功能类。

12.1.2 IP 净荷加密(FVN _ VPN.2)

路由器使用 IP 净荷加密技术(只对用户数据包中的数据加密)实现虚拟网络。

本组件依赖于 FEN 功能类。

12.1.3 IP 承载加密(FVN _ VPN.3)

路由器使用 IP 承载加密技术(对完整用户数据包加密,并添加新的数据包头)实现虚拟网络。

本组件依赖于 FEN 功能类。

12.1.4 IP 加密和鉴别(FVN _ VPN.4)

路由器同时使用 IP 加密和鉴别技术实现虚拟网络。

本组件依赖于 FIA、FEN 安全功能类。

13 路由器初始化安全功能类

路由器初始化安全功能类(FIN)包括两个功能组:引导和出厂配置。

路由器初始化安全功能类的组成如图 11 所示。

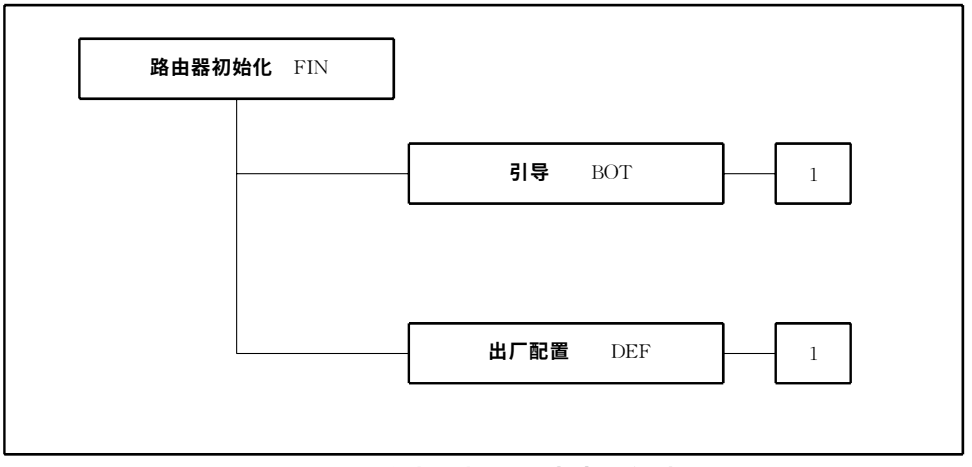

图 11 路由器初始化安全功能类

13.1 引导安全功能组(FIN _ BOT)

13.1.1 **引导**(FIN _ BOT.1)

引导。路由器的引导必须满足以下要求:

a) **路由器必须具有自引导功能,不能使用网络引导,尤其不能在路由器的自身安全功能发挥作用之前从网络获取引导信息;**

b) **路由器引导应用程序必须同路由器的管理相关,并且管理员可以根据需要开放或关闭某些应用程序。**

13.2 **出厂配置安全功能组**(FIN _ DEF)

13.2.1 **出厂配置**(FIN _ DEF.1)

路由器所有的配置参数(尤其是安全配置参数)要有出厂配置,用户安装路由器后应及时提醒用户修改。在路由器使用手册中必须明确列出所有的出厂默认配置参数,并提醒用户修改这些配置参数。

14 路由器安全级别的划分

路由器安全级别的划分应依据路由器安全功能的实现情况。本标准提供一个建议性的划分规则,见附录 A。

附 录 A
（提示的附录）
路由器安全级别划分的建议规则

对于指定的路由器，一般只能满足指定安全功能组的一个安全组件的要求，因而根据路由器对标准中安全功能组件的满足情况，将路由器划分为三个级别：

Ⅰ级：为最高级别，达到该级别的路由器其满足的安全功能要求最为全面，该级别的路由器将满足所有安全功能组中最为全面的安全组件的要求；

Ⅱ级：达到该级别的路由器将满足所有安全功能组中至少一个安全组件的要求；

Ⅲ级：为路由器的最低安全级别，该级别的路由器无法满足某些安全功能类的要求，同时满足其他功能类中安全功能组最低安全组件的要求。

由于本标准只考虑路由器对标准中所规定的安全功能要求的满足情况，故分级标准不考虑诸如密码算法强度等涉及安全性能方面的因素。

各级别的要求如表 A1 所示。

表 A1 路由器安全级别划分表

安全功能类	Ⅲ级	Ⅱ级	Ⅰ级
FEN	无	FEN_ALG.1	FEN_ALG.1
		FEN_KMG.1	FEN_KMG.1
		FEN_KMG.2	FEN_KMG.2
FIA	FIA_UAU.1	FIA_UAU.2	FIA_UAU.2
FAU	FAU_GEN.1	FAU_GEN.1	FAU_GEN.1
		FAU_GEN.2	FAU_GEN.2
	FAU_MGT.1	FAU_MGT.2	FAU_MGT.2
	FAU_CNT.1	FAU_CNT.1	FAU_CNT.1
FMS	FMS_RIG.1	FMS_RIG.1	FMS_RIG.3
	FMS_RIG.2	FMS_RIG.2	
	无	FMS_TRA.1	FMS_TRA.1
		FEN_ALG.1	FEN_ALG.1
		FEN_KMG.1	FEN_KMG.1
		FEN_KMG.2	FEN_KMG.2
		FIA_UAU.2	FIA_UAU.2
		FVN_VPN.1	FVN_VPN.4
		FVN_VPN.2	
		FVN_VPN.3	
	FMS_FAC.1	FMS_FAC.1	FMS_FAC.1
	FIA_UAU.1	FIA_UAU.2	FIA_UAU.2
		FEN_ALG.1	FEN_ALG.1
		FEN_KMG.1	FEN_KMG.1
		FEN_KMG.2	FEN_KMG.2
	FMS_INT.1	FMS_INT.2	FMS_INT.2
		FIA_UAU.2	FIA_UAU.2
		FEN_ALG.1	FEN_ALG.1
		FEN_KMG.1	FEN_KMG.1
		FEN_KMG.2	FEN_KMG.2

表 A1(完)

安全功能类	Ⅲ级	Ⅱ级	Ⅰ级
FRI	无	FRS_RIS.1 FRS_RIS.2 FIA_UAU.1 FIA_UAU.2 FEN_ALG.1 FEN_KMG.1 FEN_KMG.2	FRS_RIS.3 FIA_UAU.2 FEN_ALG.1 FEN_KMG.1 ENV_KMG.2
FAS	FAS_RRA.1	FAS_RRA.1 FAS_RRA.2 FVN_VPN.1 FVN_VPN.2 FVN_VPN.3 FIA_UAU.1 FEN_ALG.1 FEN_KMG.1 FEN_KMG.2	FAS_RRA.2 FVN_VPN.4 FIA_UAU.2 FEN_ALG.1 FEN_KMG.1 FEN_KMG.2
	FAS_RUA.1 FIA_UAU.1	FAS_RUA.1 FAS_RUA.2 FAS_RUA.3 FIA_UAU.2 FEN_ALG.1 FEN_KMG.1 FEN_KMG.2	FAS_RUA.1 FAS_RUA.2 FAS_RUA.3 FIA_UAU.2 FEN_ALG.1 FEN_KMG.1 FEN_KMG.2
FFL	无	FPF_FIL.1	FPF_FIL.1
FVN	无	FVN_VPN.1 FVN_VPN.2 FVN_VPN.3 FIA_UAU.2 FEN_ALG.1 FEN_KMG.1 FEN_KMG.2	FVN_VPN.4 FIA_UAU.2 FEN_ALG.1 FEN_KMG.1 FEN_KMG.2
FIN	FIN_BOT.1	FIN_BOT.1	FIN_BOT.1
	FIN_DEF.1	FIN_DEF.1	FIN_DEF.1

附 录 B
(提示的附录)
参 考 文 献

RFC 2154 带数字签名的 OSPF 路由协议

RFC 2138 拨号用户服务远程鉴别

RFC 1994 PPP 询问握手鉴别协议

RFC 1969 PPP 的 DES 加密协议

RFC 1968 PPP 加密控制协议

RFC 1828 使用键控 MD5 的 IP 鉴别

RFC 1827 IP 封装安全载荷

RFC 1826 IP 鉴别头
RFC 1825 互联网协议的安全体系协议
RFC 2094 组密钥管理协议体系结构
RFC 2093 组密钥管理协议规范
RFC 2085 使用 HMAC-MD5 防止重放的 IP 鉴别
RFC 2082 RIP-2 的 MD5 鉴别
RFC 1723 RIP 协议版本 2
RFC 2025 简单公开密钥 GSS-API 机制
RFC 1964 Kerberos 版本 5GSS-API 机制
RFC 1938 一次性口令系统

中 华 人 民 共 和 国
国 家 标 准
路 由 器 安 全 技 术 要 求
GB/T 18018—1999
*
中 国 标 准 出 版 社 出 版
北京复兴门外三里河北街 16 号
邮政编码：100045
电　　话：68522112
中国标准出版社秦皇岛印刷厂印刷
新华书店北京发行所发行　各地新华书店经售

*
开本 880×1230　1/16　印张 1¼　字数 30 千字
2000 年 6 月第一版　2000 年 6 月第一次印刷
印数 1—1 600
*
书号：155066·1-16687　定价 13.00 元
*
标 目 410—24

GB/T 18018-1999