



中华人民共和国国家标准

GB/T 18018—2019
代替 GB/T 18018—2007

信息安全技术 路由器安全技术要求

Information security technology—
Technical requirement for router security

2019-08-30 发布

2020-03-01 实施

国家市场监督管理总局
中国国家标准化管理委员会 发布

目 次

前言	I
1 范围	1
2 规范性引用文件	1
3 术语和定义、缩略语	1
3.1 术语和定义	1
3.2 缩略语	1
4 第一级安全技术要求	2
4.1 安全功能要求	2
4.2 安全保障要求	3
5 第二级安全技术要求	4
5.1 安全功能要求	4
5.2 安全保障要求	7
6 第三级安全技术要求	8
6.1 安全功能要求	8
6.2 安全保障要求	11
附录 A (资料性附录) 安全要求对照表	14

前 言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准代替 GB/T 18018—2007《信息安全技术 路由器安全技术要求》。

本标准与 GB/T 18018—2007 相比,除编辑性修改外主要技术变化如下:

- 修改了第 2 章规范性引用文件(见第 2 章,2007 年版的第 2 章);
- 修改了 3.2 缩略语(见 3.2,2007 年版的 3.2);
- 修改了 4.1.2.1 管理员鉴别(见 4.1.2.1,2007 年版的 4.1.2.1);
- 增加了 4.1.3.2 管理协议设置、4.1.4 设备安全防护、4.1.5 安全功能保护;
- 修改了 5.1.2.1 管理员鉴别、5.1.3.1 权限管理(见 5.1.2.1、5.1.3.1,2007 年版的 5.1.2.1、5.1.3.1);
- 增加了 5.1.3.2 管理协议设置、5.1.4 设备安全防护、5.1.5 网络安全防护、5.1.6 安全功能保护;
- 修改了 6.1.2.1 管理员鉴别、6.1.4.1 权限管理(见 6.1.2.1、6.1.4.1,2007 年版的 6.1.2.1、6.1.4.1);
- 增加了 6.1.2.2 设备登录口令管理、6.1.2.3 证书验证、6.1.3.2 数据存储、6.1.3.3 数据传输、6.1.3.4 敏感数据、6.1.4.2 管理协议设置、6.1.5 设备安全防护、6.1.6 网络安全防护、6.1.7 安全功能保护;
- 删除了 5.1.8 路由认证、6.1.10 路由认证;分别调整到 5.1.5.2 和 6.1.6.2 中;
- 删除了第 7 章附加安全功能。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本标准起草单位:中国科学院软件研究所、华为技术有限公司、新华三技术有限公司、迈普通信技术股份有限公司、中国科学院信息工程研究所、北京大学软件与微电子学院、中国电子技术标准化研究院。

本标准主要起草人:卿斯汉、陈驰、付天福、王博、杨银柱、李晶林、何斌、王利明、赵志宇、王惠莅、罗锋盈、周启明、沈晴霓、文伟平、马书南。

本标准所代替标准的历次版本发布情况为:

- GB/T 18018—1999、GB/T 18018—2007。

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障要求。

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

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件,仅注日期的版本适用于本文件。凡是不注日期的引用文件,其最新版本(包括所有的修改单)适用于本文件。

GB 17859—1999 计算机信息系统安全保护等级划分准则

GB/T 18336.1~18336.3—2015 信息技术 安全技术 信息技术安全性评估准则

3 术语和定义、缩略语

3.1 术语和定义

GB 17859—1999 和 GB/T 18336.1~18336.3—2015 界定的以及下列术语和定义适用于本文件。

3.1.1

路由器 **router**

主要的网络节点设备,承载数据流量,通过路由选择算法决定流经数据的转发处理,并可以通过集成防火墙等功能模块提供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**

一系列协议组和规范,提供了一种从网络上的设备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**

为防止基于源地址欺骗的网络攻击,以源地址为目的地址,在转发表中查找源地址对应接口是否与入接口匹配的动作。

3.2 缩略语

下列缩略语适用于本文件。

HTTPS 安全套接字层超文本传输协议(Hyper Text Transfer Protocol over Secure Socket Layer)

IKE Internet 密钥交换协议(Internet Key Exchange Protocol)

IPSec Internet 协议安全(Internet Protocol Security)

LDAP 轻量级目录访问协议(Lightweight Directory Access Protocol)