ICS 35.020
L 80

中华人民共和国国家标准

GB/T 25068.3—2010/ISO/IEC 18028-3:2005

信息技术　安全技术　IT网络安全 第3部分:使用安全网关的网间通信安全保护

Information technology—Security techniques—IT network security—Part 3:Securing communications between networks using security gateways

(ISO/IEC 18028-3:2005,IDT)

2010-09-02 发布　　2011-02-01 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

目　　次

前　言

GB/T 25068在《信息技术　安全技术　IT网络安全》总标题下，拟由以下5个部分组成：

——第1部分：网络安全管理；

——第2部分：网络安全体系结构；

——第3部分：使用安全网关的网间通信安全保护；

——第4部分：远程接入的安全保护；

——第5部分：使用虚拟专用网的跨网通信安全保护。

本部分为GB/T 25068的第3部分。

本部分使用翻译法等同采用国际标准ISO/IEC 18028-3:2005《信息技术　安全技术　IT网络安全　第3部分：使用安全网关的网间通信安全保护》(英文版)。根据GB/T 1.1—2000的规定，做了如下一些编辑性修改：

——第2章中增加了引用文件“ISO/IEC TR 15947”；

——在3.6中对“内容过滤”加以说明，并在6.5中补充了内容过滤的内容“关键字过滤”，为今后技术发展预留了空间；

——删除了第4章中缩略语S/MIME英文名称中的“protocol”，以与GB/T 25068.4—2010中2.34定义的同一术语S/MIME统一。另外，增加了一些缩略语，增加的缩略语在所在页边的空白处用单竖线“|”标出。

本部分由全国信息安全标准化技术委员会(TC 260)提出并归口。

本部分起草单位：黑龙江省电子信息产品监督检验院、中国电子技术标准化研究所、哈尔滨工程大学、北京励方华业技术有限公司、山东省标准化研究院。

本部分主要起草人：王希忠、张国印、李健利、王向辉、黄俊强、马遥、方舟、王大萌、树彬、张清江、王智、许玉娜、刘亚东、邱意民、王运福。

引　言

通信和信息技术业界一直在寻找经济有效的全面安全解决方案。安全的网络应受到保护，免遭恶意和无意的攻击，并且应满足业务对信息和服务的保密性、完整性、可用性、抗抵赖、可核查性、真实性和可靠性的要求。保护网络安全对于适当维护计费或使用信息的准确性也是必要的。产品的安全保护能力对于全网的安全（包括应用和服务）是至关重要的。然而，当更多的产品被组合起来以提供整体解决方案时，互操作性的优劣将决定这种解决方案的成功与否。安全不仅是对每种产品或服务的关注，还必须以促进全面的端到端安全解决方案中各种安全能力交合的方式来开发。因此，GB/T 25068 的目的是为 IT 网络的管理、操作和使用及其互连等安全方面提供详细指南。组织中负责一般 IT 安全和特定 IT 网络安全的人员应能够调整 GB/T 25068 中的材料以满足他们的特定要求。GB/T 25068 的主要目标如下：

——GB/T 25068.1 定义和描述网络安全的相关概念，并提供网络安全管理指南——包括考虑如何识别和分析与通信相关的因素以确立网络安全要求，还介绍可能的控制领域和特定的技术领域（在 GB/T 25068 的后续部分中涉及）；

——GB/T 25068.2 定义一个标准的安全体系结构，它描述一个支持规划、设计和实施网络安全的一致框架；

——GB/T 25068.3 定义使用安全网关保护网络间信息流安全的技术；

——GB/T 25068.4 定义保护远程接入安全的技术；

——GB/T 25068.5 定义对使用虚拟专用网（VPN）建立的网络间连接进行安全保护的技术。

GB/T 25068.1 与涉及拥有、操作或使用网络的所有人员相关。除了对信息安全（IS）和/或网络安全及网络操作负有特定责任的，或对组织的全面安全规划和安全策略开发负有责任的管理者和管理员外，还包括高级管理者和其他非技术性管理者或用户。

GB/T 25068.2 与涉及规划、设计和实施网络安全体系结构方面的所有人员（例如 IT 网络管理者、管理员、工程师和 IT 网络安全主管）相关。

GB/T 25068.3 与涉及详细规划、设计和实施安全网关的所有人员（例如 IT 网络管理者、管理员、工程师和 IT 网络安全主管）相关。

GB/T 25068.4 与涉及详细规划、设计和实施远程接入安全的所有人员（例如 IT 网络管理者、管理员、工程师和 IT 网络安全主管）相关。

GB/T 25068.5 与涉及详细规划、设计和实施 VPN 安全的所有人员（例如 IT 网络管理者、管理员、工程师和 IT 网络安全主管）相关。

信息技术　安全技术　IT网络安全
第3部分:使用安全网关的
网间通信安全保护

1　范围

GB/T 25068的本部分规定了各种安全网关技术、组件和各种类型的安全网关体系结构。它还提供安全网关的选择和配置指南。

尽管个人防火墙使用类似的技术,但因为它不作为安全网关使用,所以它不在本部分的范围之内。

本部分适用于技术和管理人员,例如IT管理者、系统管理员、网络管理员和IT安全人员。本部分提供的指南有助于用户正确地选择最能满足其安全要求的安全网关体系结构类型。

2　规范性引用文件

下列文件中的条款通过GB/T 25068的本部分的引用而成为本部分的条款。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部分,然而,鼓励根据本部分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部分。

GB/T 25068.4　信息技术　安全技术　IT网络安全　第4部分:远程接入的安全保护(GB/T 25068.4—2010,ISO/IEC 18028-4:2005,IDT)

ISO/IEC TR 15947　信息技术　安全技术　IT入侵检测框架

3　术语和定义

下列术语和定义适用于本部分。

3.1

报警　alert

“即时”指示信息系统和网络可能受到攻击或因意外事件、故障或人为错误而处于危险之中。

3.2

攻击者　attacker

故意利用技术性和非技术性安全控制措施的脆弱性,以窃取或损害信息系统和网络,或者损害合法用户对信息系统和网络资源可用性的任何个人。

3.3

审计　audit

依照期望对事实进行的正规调查、正规检验或验证,以确认它们之间的符合性和一致性。

3.4

审计日志　audit logging

为了评审和分析以及持续监视而收集有关信息安全事态的数据。

3.5

非军事区　demilitarised zone;DMZ

插在网络之间作为“中立区”的安全主机或小型网络(也称为屏蔽子网或边界网络)。

注:它形成一个安全缓冲区。