ICS 35.020
L 80

中华人民共和国国家标准

GB/T 25068.5—2010/ISO/IEC 18028-5:2006

信息技术　安全技术　IT网络安全 第5部分:使用虚拟专用网的跨网通信安全保护

Information technology—Security techniques—IT network security—Part 5:Securing communications across networks using virtual private networks

(ISO/IEC 18028-5:2006,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 5 部分。

本部分使用翻译法等同采用国际标准 ISO/IEC 18028-5:2006《信息技术　安全技术　IT 网络安全　第 5 部分：使用虚拟专用网的跨网通信安全保护》(英文版)。根据 GB/T 1.1—2000 的规定，做了如下一些纠错性和编辑性修改：

——第 2 章中增加了引用文件 GB/T 17901.1；

——原文第 4 章的缩略语 NAS 对应的全称中“Area Strong”和 NCP 对应的全称中“Point-to-Point”是错误的，转换为本部分时 NAS 的全称更正为“Network Access Server”，NCP 的全称更正为“Network Control Protocol”。另外为使本部分易于理解，增加了 7 个缩略语，增加的缩略语在所在页边的空白处用单竖线“|”标出。

——8.1 中增加了使用国家加密标准的规定。

这些修改不影响等同采用的一致性程度。

本部分的附录 A 为资料性附录。

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、徐铁、黄俊强、马遥、方舟、王大萌、树彬、张清江、王智、许玉娜、张国印、李健利、肖鸿江、祝宇林、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，并且宜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5部分:使用虚拟专用网的跨网通信安全保护

1　范围

GB/T 25068的本部分规定了使用虚拟专用网(VPN)连接到互联网络以及将远程用户连接到网络上的安全指南。它是根据ISO/IEC 18028-1中的网络管理导则而构建的。

本部分适用于在使用VPN时负责选择和实施提供网络安全所必需的技术控制的人员,以及负责随后的VPN安全的网络监控人员。

本部分提供VPN综述,提出VPN的安全目标,并概括VPN的安全要求。它给出安全VPN的选择、实施以及VPN安全的网络监控的指南。它也提供有关VPN所使用的典型技术和协议的信息。

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 9387(所有部分)　信息技术　开放系统互连　基本参考模型(ISO/IEC 7498,IDT)

GB/T 17901.1—1999　信息技术　安全技术　密钥管理　第1部分:框架(ISO/IEC 11770-1:1996,IDT)

GB/T 19715.1　信息技术　安全技术　信息安全管理指南　第1部分:信息技术安全概念和模型(GB/T 19715.1—2005,ISO/IEC TR 13335-1:2004,IDT)

GB/T 22081—2008　信息技术　安全技术　信息安全管理实用规则(ISO/IEC 27002:2005,IDT)

GB/T 25068.3　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(GB/T 25068.3—2010,ISO/IEC 18028-3:2005,IDT)

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 18028-1:2006　信息技术　安全技术　IT网络安全　第1部分:网络安全管理

ISO/IEC 18028-2:2006　信息技术　安全技术　IT网络安全　第2部分:网络安全体系结构

3　术语和定义

GB/T 9387(所有部分)、GB/T 19715.1和ISO/IEC 18028-1确立的以及下列术语和定义适用于GB/T 25068的本部分。

3.1

第2层交换技术　layer 2 switching

使用内部交换机制并利用第2层协议在设备之间创建和控制连接的技术。

注:它通常对于上层协议模拟局域网环境。