ICS 35.040
L 80

中华人民共和国国家标准

GB/T 25068.5—2021
代替 GB/T 25068.5—2010

信息技术　安全技术　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—Network security—Part 5:Securing communications across networks using virtual private networks

(ISO/IEC 27033-5:2013,MOD)

2021-03-09 发布　　2021-10-01 实施

国家市场监督管理总局
国家标准化管理委员会　发布

目　　次

前　言

GB/T 25068《信息技术　安全技术　网络安全》分为以下5个部分：

——第1部分：综述和概念；

——第2部分：网络安全设计和实现的指南；

——第3部分：参考网络场景 风险、设计技术和控制要素；

——第4部分：使用安全网关的网间通信安全保护；

——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。

注：GB/T 25068可能还会有其他部分。这些部分可能覆盖的主题包括局域网、城域网、宽带网、网页寄存、互联网电子邮件、接入第三方组织的路由。这些部分主要涉及威胁、设计技术和控制等问题。

本部分按照GB/T 1.1—2009给出的规则起草。

本部分代替GB/T 25068.5—2010《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》。

本部分与GB/T 25068.5—2010相比，主要技术差异如下：

——修改了规范性引用文件(见第2章，2010年版的第2章)；

——删除了术语“第2层交换技术”“第2层VPN”“第3层交换技术”“第3层VPN”“专用网”，增加了术语“隧道”(见第3章，2010版的第3章)；

——增加了缩略语“TePA”“TISec”等(见第4章)；

——修改了第5章标题，由“VPN综述”改为“概述”(见第5章，2010年版的第5章)；

——修改了第6章标题，由“VPN安全目标”改为“安全威胁”(见第6章，2010年版的第6章)；

——修改了第7章标题，由“VPN安全要求”改为“安全要求”(见第7章，2020年版的第7章)；

——增加了我国密码算法相关的使用规定，以与我国密码管理相关规定相适应(见第7章)；

——增加了第8章“安全控制”(见第8章)；

——将第8章“安全VPN选择指南”和第9章“安全VPN实施指南”合并为第9章“VPN相关技术”(见第9章，2010年版的第8章和第9章)；

——增加了第10章“产品选择指南”(见第10章)。

本部分使用重新起草法修改采用ISO/IEC 27033-5：2013《信息技术　安全技术　网络安全　第5部分：使用虚拟专用网的跨网通信安全保护》。

本部分与ISO/IEC 27033-5：2013的技术性差异及其原因如下：

——关于规范性引用文件，本部分做了具有技术性差异的调整，以适应我国的技术文件，调整的情况集中反映在第2章“规范性引用文件”中，具体调整如下：

- 删除了ISO/IEC 27001：2005、ISO/IEC 27002：2005、ISO/IEC 27005：2011；
- 增加引用了GB/T 9387(所有部分)、GB/T 22080—2016、GB/T 31722—2015(见第3章)；
- 增加引用了GB/T 22081(见第3章、9.4.2、9.4.4、9.4.5)；
- 增加引用了GB/T 17901.1—2020(见9.4.5)。

——第3章增加了部分术语。

——修改了第4章中的缩略语。

——删除了国际文件中第5章“文档结构”，并依次调整余后各章的编号。

——第5章增加了对我国IPSec VPN国家标准和SSL VPN密码行业标准的引用。

——第7章增加了我国密码算法相关的使用规定，以与我国密码管理相关规定相适应。

——第8章增加了对附录A的引用。

——修改了第9章的标题。

本部分还做了下列编辑性修改：

——增加了资料性附录A，给出了满足VPN安全使用目标的典型应用，该附录给出了一种IP安全可信技术(TISec)，其目标是为IP网络端到端的访问和通信提供安全保障，对如何实现安全可靠的VPN提供指导；

请注意本部分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。

本部分由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本部分起草单位：西安西电捷通无线网络通信股份有限公司、中关村无线网络安全产业联盟、重庆邮电大学、中国电子技术标准化研究院、黑龙江省网络空间研究中心、国家无线电监测中心检测中心、福建省无线电监测站、中国通用技术研究院、国家密码管理局商用密码检测中心、国家信息技术安全研究中心、珠海许继电气有限公司、许继集团有限公司、天津市无线电监测站、北京计算机技术及应用研究所。

本部分主要起草人：杜志强、芦亮、黄振海、王月辉、陶洪波、陈志宇、于光明、铁满霞、张变玲、许玉娜、曲家兴、龙昭华、李琴、李明、颜湘、罗鹏、简练、张强、吴冬宇、赵晓荣、郑骊、许福明、刘科伟、方舟、李冬、傅强、王栋、熊克琦、朱正美、刘景莉、赵慧、郭上华、赵奕、李玉娇。

本部分所代替标准的历次发布情况为：

——GB/T 25068.5—2010。

信息技术　安全技术　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)连接到互联网和将远程用户连接到网络上的安全要求,以及在使用VPN提供网络安全时所必需的控制技术的选择、实施和监控指南。

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人员,以及随后的VPN安全的网络监控人员。

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/T 9387(所有部分)　开放系统互连　基本参考模型[ISO 7498(所有部分)]

GB/T 17901.1—2020　信息技术　安全技术　密钥管理　第1部分:框架(ISO/IEC 11770-1:2010,MOD)

GB/T 22080—2016　信息技术　安全技术　信息安全管理体系　要求(ISO/IEC 27001:2013,IDT)

GB/T 22081　信息技术　安全技术　信息安全控制实践指南(GB/T 22081—2016,ISO/IEC 27002:2013,IDT)

GB/T 25068.1—2020　信息技术　安全技术　网络安全　第1部分:综述和概念(ISO/IEC 27033-1:2015,IDT)

GB/T 31722—2015　信息技术　安全技术　信息安全风险管理(ISO/IEC 27005:2008,IDT)

3　术语和定义

GB/T 9387(所有部分)、GB/T 22080—2016、GB/T 22081、GB/T 25068.1—2020、GB/T 31722—2015界定的以及下列术语和定义适用于本文件。

3.1

专用　private

仅限于授权用户使用。

3.2

隧道　tunnel

在联网的设备之间,隐藏在其它可见性更高的协议内部的数据路径。

3.3

虚拟专用网　virtual private network

基于物理网络系统资源,通过隧道技术构建的、受限使用的虚拟网络。