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

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

中华人民共和国
国家标准
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
GB/T 25068.5—2010/ISO/IEC 18028-5:2006
*
中国标准出版社出版发行
北京复兴门外三里河北街 16 号
邮政编码:100045
网址 www.spc.net.cn
电话:68523946　68517548
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230　1/16　印张 1.25　字数 35 千字
2011 年 1 月第一版　2011 年 1 月第一次印刷
*
书号:155066·1-40820　定价 21.00 元

GB/T 25068.5-2010

目　　次

前言 …… Ⅰ
引言 …… Ⅱ
1　范围 …… 1
2　规范性引用文件 …… 1
3　术语和定义 …… 1
4　缩略语 …… 2
5　VPN 综述 …… 3
5.1　简介 …… 3
5.2　VPN 类型 …… 3
5.3　VPN 相关技术 …… 4
5.4　安全方面 …… 5
6　VPN 安全目标 …… 5
7　VPN 安全要求 …… 6
7.1　保密性 …… 6
7.2　完整性 …… 6
7.3　鉴别 …… 6
7.4　授权 …… 7
7.5　可用性 …… 7
7.6　隧道端点 …… 7
8　安全 VPN 选择指南 …… 7
8.1　法规和法律方面 …… 7
8.2　VPN 管理方面 …… 7
8.3　VPN 体系结构方面 …… 7
9　安全 VPN 实施指南 …… 9
9.1　VPN 管理考量 …… 9
9.2　VPN 技术考量 …… 9
附录 A（资料性附录）　实现 VPN 所使用的技术和协议 …… 11
A.1　导言 …… 11
A.2　第 2 层 VPN …… 11
A.3　第 3 层 VPN …… 12
A.4　高层 VPN …… 13
A.5　典型 VPN 协议安全特点比较 …… 13
参考文献 …… 15

参　考　文　献

[1] GB/T 18794.1—2002　信息技术　开放系统互连　开放系统安全框架　第 1 部分：概述（idt ISO/IEC 10181-1:1996）
[2] ISO/IEC 27005, Information technology—Information security risk management
[3] GB/T 17903.1—2008　信息技术　安全技术　抗抵赖　第 1 部分：概述（ISO/IEC 13888-1:2004, IDT）
[4] ISO/IEC TR 14516:2002, Information technology—Security techniques—Guidelines for the use and management of Trusted Third Party services
[5] ISO/IEC TR 15947, Information technology—Security techniques—IT intrusion detection framework
[6] ISO/IEC 18043, Information technology—Security techniques—Selection, deployment and operations of intrusion detection systems
[7] GB/Z 20985—2007　信息技术　安全技术　信息安全事件管理指南（ISO/IEC TR 18044:2004, MOD）
[8] NIST-800 NIST Special Publications 800 series on Computer Security, USA
[9] RFC 1352 SNMP Security Protocols, IETF, July 1992
[10] RFC 1661 Point-to-Point Protocol, IETF, July 1994
[11] RFC 1918 Address Allocation for Private Internets, IETF, February 1996
[12] RFC 2196 Site Security Handbook, IETF, September 1997
[13] RFC 2341 Cisco Layer Two Forwarding (Protocol) "L2F" (historic), IETF, May 1998
[14] RFC 2401 Security Architecture for the Internet Protocol, IETF, November 1998
[15] RFC 2402 Authentication Header, IETF, November 1998
[16] RFC 2406 Encapsulating Security Protocol, IETF, November 1998
[17] RFC 2407 IPsec Domain of Interpretation (IPsec Dol), IETF, November 1998
[18] RFC 2408 Internet Security Association and Key Management Protocol (ISAKMP), IETF, November 1998
[19] RFC 2409 Internet Key Exchange (IKE), IETF, November 1998
[20] RFC 2411 IP Security Document Roadmap, IETF, November 1998
[21] RFC 2637 Point-to-Point Tunneling Protocol (informational), IETF, July 1999
[22] RFC 2661 Layer 2 Tunneling Protocol, IETF, August 1999
[23] RFC 2828 Internet Security Glossary, IETF, May 2000
[24] RFC 3031 Multi-Protocol Label Switching Architecture, IETF, January 2001
[25] RFC 3032 MPLS Label Stack Encoding, IETF, January 2001
[26] RFC 3036 Label Distribution Protocol (LDP) Specification, IETF, January 2001
[27] X.25 Interface between Data Terminal Equipment (DTE) and Data Circuit-terminating Equipment (DCE) for terminals operating in the packet mode and connected to public data networks by dedicated circuit, ITU-T, October 1996

表 A.1（续）

VPN 类型	技术/协议	用户鉴别	数据加密	密钥管理	完整性检查
第 3 层 VPN	IPSec	基于证书（包） 预共享密钥	可协商 若干算法（包）	IKE	可协商
	具有 L2TP 的 IPsec	基于证书（包） 预共享密钥	可协商 若干算法（包）	IKE	可协商
	MPLS	—	—	—	—
高层 VPN	SSL	基于证书	可协商	可协商	可协商
	安全壳	系统生成的密钥对（非证书）	可协商	与数据发送方交换公钥	可协商

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。