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 …… 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

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。

3.2

第 2 层 VPN　layer 2 VPN

在网络基础设施上提供模拟局域网环境的虚拟专用网。

注：由第 2 层 VPN 链接的各个站点，能够像它们在同一个局域网上那样运行。

3.3

第 3 层交换技术　layer 3 switching

使用内部交换机制并与标准路由机制相结合或使用 MPLS 技术以建立和控制网络之间连接的技术。

3.4

第 3 层 VPN　layer 3 VPN

在网络基础设施上提供模拟广域网环境的虚拟专用网。

注：由第 3 层 VPN 链接的各个站点，能够像它们在一个专用广域网上那样运行。

3.5

专用　private

只限于授权组成员使用：在 VPN 环境中，它指 VPN 连接中的通信流。

3.6

专用网　private network

受到访问控制的网络，只限于得到授权的组成员使用。

3.7

协议封装　protocol encapsulation

通过传输包装在一个协议内的协议数据单元而将一个数据流封装在另一数据流之内。

注：在 VPN 技术中，这是可用于建立隧道的一种方法。

3.8

虚电路　virtual circuit

使用诸如 X.25、ATM 或帧中继等包或信元交换技术而建立的网络设备之间的数据通道。

4　缩略语

ACL	访问控制列表(Access Control Lists)
AH	鉴别头(Authentication Header)
ATM	异步传输模式(Asynchronous Transfer Mode)
ESP	封装安全载荷(Encapsulated Security Payload)
IDS	入侵检测系统(Intrusion Detection System)
IKE	互联网密钥交换(Internet Key Exchange)
IPX	互联网络包交换(Internetwork Packet Exchange)
ISAKMP	互联网安全关联和密钥管理协议(Internet Security Association and Key Management Protocol)
IT	信息技术(Information Technology)
L2F	第 2 层转发(协议)[Layer 2 Forwarding (Protocol)]
L2TP	第 2 层隧道协议(Layer 2 Tunneling Protocol)
LAN	局域网(Local Area Network)
LDP	标签分发协议(Label Distribution Protocol)
MPPE	微软点对点加密协议(Microsoft Point-to-Point Encryption)
MPLS	多协议标记交换(Multi-Protocol Label Switching)

NAS	网络访问服务器(Network Access Server)
NCP	网络控制协议(Network Control Protocol)
PPP	点对点协议(Point-to-Point Protocol)
PPTP	点对点隧道协议(Point-to-Point Tunneling Protocol)
SSL	安全套接层协议(Secure Sockets Layer)
VPLS	虚拟专用 LAN 服务(Virtual Private LAN Service)
VPN	虚拟专用网(Virtual Private Network)
VPWS	虚拟专用线路服务(Virtual Private Wire Service)
WAN	广域网(Wide Area Network)

5 VPN 综述

5.1 简介

作为一种网络互连方式和一种将远程用户连接到网络的方法,VPN 一直在快速发展。VPN 是一种能实现 ISO/IEC 18028-2 中所描述的通信流安全维技术的实例。其安全作为服务安全层(参见 ISO/IEC 18028-2 中的定义)的一部分来考虑。

目前存在着范围较广的 VPN 定义。按照其最简单的定义,VPN 提供一种在现有网络或点对点连接上建立一至多条安全数据信道的机制。它只分配给受限的用户组独占使用,并能在需要时动态地建立和撤销。主机网络可为专用的或公共的。

VPN 的示例表示如图 1 所示。它具有一条跨越不安全的公共网来连接两个端点的安全数据信道。

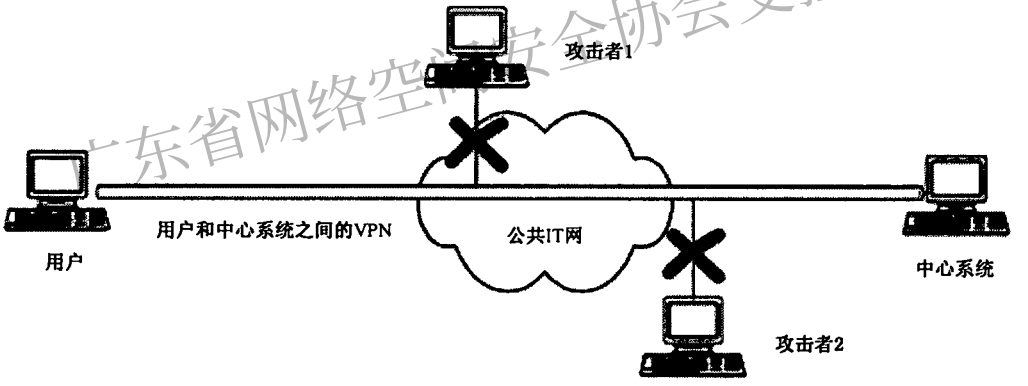

图 1 VPN 的示例表示

使用 VPN 的远程接入是在普通的点对点连接之上实现的。宜按照 GB/T 25068.4 的规定,首先在本地用户和远程位置之间建立连接。该连接可采用有线或无线网络技术的方式。

一些 VPN 作为一种管理服务来提供。在这种 VPN 中,安全可靠的连通性、管理和寻址功能(与专用网上的相同)是在共享的基础设施上提供的。因此,可能需要考虑本部分所指明的附加安全控制来增强 VPN。

穿越 VPN 的数据和代码宜只限于使用 VPN 的组织,且宜与下层网络的其他用户保持分离。属于其他用户的数据和代码不宜有访问同一 VPN 信道的可能。当可能需要评测附加安全控制的范围时,宜考虑拥有或提供 VPN 的组织在保密性和其他安全方面的可信度。

5.2 VPN 类型

如上所述,有多种方式来表示 VPN 类型。

从体系结构角度,VPN 包括:

——单一的点对点连接(例如客户端经由站点网关远程接入组织网络,或者一个站点网关连接到另一个站点网关);

——点对云连接(例如,通过 MPLS 技术实施)。

从 OSI 基本参考模型角度,VPN 主要有三种类型:

——第 2 层 VPN 提供模拟的局域网设施,它使用运行在主机网络(例如提供商网络)上的 VPN 连接来链接组织的站点或提供到组织的远程连接。提供商在该领域通常提供的服务包括虚拟专用线路服务(VPWS)或虚拟专用局域网服务(VPLS)。VPWS 提供模拟的"有线连接";VPLS 提供更完整的模拟局域网服务。

——第 3 层 VPN 提供一种模拟的广域网设施。它也使用在网络基础设施上运行的 VPN。它为站点提供模拟的"OSI 网络层"连通性。值得关注的是,它具有在公共基础设施上使用专用 IP 寻址方案的能力,而这种做法在"正常"的公共 IP 连接上是不允许的。在第 3 层 VPN 中,专用地址能够在公共网络上经由 NAT(网络地址转换)而被使用,虽然这种做法确实可行,却能够使 IPsec VPN 的建立和使用变得复杂。

——高层 VPN 用于保护跨公共网络交易的安全。通常它们在通信的应用之间提供一条安全信道,以确保交易期间数据的保密性和完整性。这种类型也可称作第 4 层 VPN,因为 VPN 连接通常建立在 TCP 之上,而 TCP 为第 4 层协议。

附录 A 进一步描述各种类型 VPN 通常所使用的特定技术和协议。

5.3 VPN 相关技术

VPN 是使用物理网络的系统资源(例如,通过使用加密和/或穿越真实网络的虚拟网络的隧道链接)构建的。

VPN 能在其所属组织控制下的专用网内完整实现,能穿越公共域中的网络实现,或能穿越以上两种网络的组合实现(VPN 完全有可能在现有的专用广域网上构建。由于通常可提供成本相对较低的互联网访问,这使得这种公共网络系统逐渐成为很多应用程序中支持广域 VPN 和远程接入 VPN 的经济有效工具)。另一种方案是,这种信道可使用穿越互联网服务提供商网络而构建的安全隧道来建立。在这种情况下,公共的互联网就有效地成为下层传输系统。对于 VPN 的保密性,这意味着不确定度更高。

隧道是联网设备之间的数据通道,是跨越现有的网络基础设施而建立的。它对正常的网络操作是透明的,在很多实际场合,其用法能够类似于正常网络连接。需要时,隧道能够容易地打开或关闭,而不必对下层的物理网络基础设施进行任何更改。因此,用隧道创建的 VPN 比基于物理链接的网络更加灵活。

能使用以下技术创建隧道:

——虚电路;

——标签交换;

——协议封装。

为虚电路而创建的隧道,通常使用包交换技术(例如帧中继或 ATM)作为租用线路在常规的广域网设施中建立。这些技术确保隧道之间的数据流是分离的。

标签交换是创建隧道的另一种方式。流经一个隧道的所有数据包都被分配一个识别标签。这种标签确保每个标签不同的包都将被穿过网络的特定路径排除在外。

虽然隧道所使用的技术确实保证隧道与下层网络之间的数据流适当分离,但却不能满足一般的保密性要求。如果需要保密性,就需要使用加密技术来提供所需的安全级别。

隧道也能够使用协议封装技术来创建,即一个协议的数据单元被包装和承载在另一个协议中。例如,一个 IP 包被使用 IPsec ESP 协议的隧道模式来包装。在插入附加的 IP 头后,这种包再在 IP 网络上传输。

VPN 隧道能在 OSI 模型的不同层上创建。虚电路在第 2 层上形成隧道。标签交换技术允许隧道在第 2 或第 3 层上创建。协议封装技术能在除物理层之外的所有层上使用(多数在第 3 层及以上实施)。

加密技术可用于为基于虚电路、协议封装和标签交换的隧道提供附加安全级别。

5.4 安全方面

虽然对于普通的网络用户，隧道是隐藏的，但并非不可见，因此不是内在安全的。用于构建隧道的基本划分过程(划分为虚电路或标签交换通道)或封装过程，在攻击者使用网络分析器或探测器进行确定性检测时，不能得到保护。如果隧道没有使用加密技术实现，则这些攻击者将能访问其通信流。即便使用了加密技术，也不能隐藏隧道及其端点的存在。此外，也可能不必保护隧道端点免受未授权的逻辑和/或物理访问。因此，为了实现安全的 VPN，必须根据组织安全策略和风险承受级别对隧道应用安全控制措施。

是否接受这种脆弱性将取决于组织的安全策略。

5.4.1 虚电路

用于建立下层安全信道的安全控制可使用常规广域电信设施中的虚电路，例如租用线路，它使用帧中继或 ATM 等技术。在这些技术中，对于电信操作人员保持私人用户的租用线路设施与所提供的公共访问互联网服务之间分离的程度而言，其下层网络也是基本安全的。虚电路中使用的技术使通道内在具有一定程度的保密性，但不具有绝对的安全性。在这种传统虚电路上构建的 VPN 被认为相对不大可能受到损害，因为安全违规或攻击通常需要源自提供商的核心网络之内。

5.4.2 标签交换

标签交换 VPN 的安全问题包括：

——标签交换网络上承载的 VPN 之间的地址空间和路由的分离；

——确保标签交换网络核心的内部结构对外部网络是不可见的(例如，对潜在攻击者可用的信息加以限制)；

——提供对拒绝服务攻击的抵抗；

——提供对未授权访问攻击的抵抗；

——抵御标签欺骗(虽然有可能从外部将错误标签插入到标签交换网中，但由于地址分离，所以欺骗包只能损害产生欺骗包的 VPN)。

5.4.3 协议封装

使用协议封装保持的密级取决于封装协议的属性。例如，如果使用仅具有 AH 协议的 IPsec 隧道来创建隧道，因为被第三方拦截的任何数据都清晰可见，所以它不提供保密性。这是因为 AH 协议只鉴别通信双方。

5.4.4 加密

密码学通用安全方面的指南参见 ISO/IEC 18028-1:2006、GB/T 17901.1—1999 和 GB/T 22081—2008。有关特定算法和协议的信息在其他出版物中论及，并且宜考虑作为安全 VPN 选择的一部分(见第 8 章)。

5.4.5 完整性保护

没有完整性保护的加密包能受到篡改。因此，易于改变的通信流，无论其是否被加密，也宜得到完整性保护。

6 VPN 安全目标

VPN 的主要安全目标是抵御未授权访问，因而 VPN 才能用于完成更多的网络安全目标：

——防护网络中的和与网络相连的系统中的信息以及它们所使用的服务；

——保护支撑网络基础设施；

——保护网络管理系统。

ISO/IEC 18028-1:2006 讨论与 VPN 相关的关键安全风险。

7 VPN 安全要求

为实现上述第 6 章中概述的目标，VPN 的实施方式宜确保：

——在 VPN 端点之间传输的数据和代码的保密性；

——在 VPN 端点之间传输的数据和代码的完整性；

——VPN 用户和管理员的真实性；

——VPN 用户和管理员的授权；

——VPN 端点和网络基础设施的可用性。

总之，这意味着用于构建 VPN 的下层隧道宜按照满足安全目标的方式实现。图 2 中概括这些安全目标。

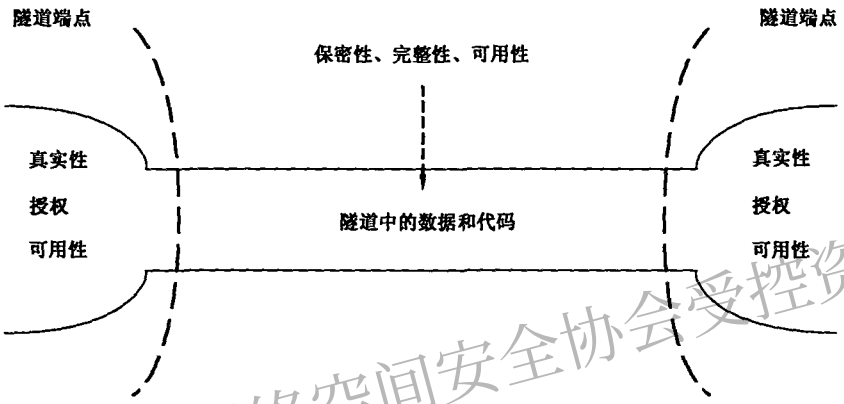

图 2 映射到下层隧道上的 VPN 一般安全要求

以下将详细讨论这些要求。

ISO/IEC 18028-1 也讨论用于实现安全 VPN 的安全控制类型。

7.1 保密性

隧道中正在传输的数据和代码的保密性不宜受到损害。使用隧道技术可能意味着正在传输的数据和代码对网络中的其他用户是不可见的。然而，这并不意味着这种通信流一直是保密的，特别是隧道中的数据和代码流不能抵御使用数据分析器或探测器进行的确定的检测。因此保持隧道中正在传输的数据和代码的保密性关键依赖于这种检测发生的可能性。总之，这是支持 VPN 的下层网络中存在的可信度因素。它将依赖于传输网络的所有权而变化。如果传输网络未处于可信域(有关可信域的更多信息参见 ISO/IEC 18028-1:2006)，或者如果认为被传输的数据和代码是敏感的，就可能需要采取附加安全控制措施来进一步保护保密性。在这些情况下，所采用的隧道机制宜支持加密，或者所发送的项在 VPN 上传输前宜离线加密。隧道端点的安全也不宜被忽视(见 7.6)。

7.2 完整性

隧道中所传输的数据和代码的完整性不宜受到损害。用于实现 VPN 隧道的机制宜支持所传输数据和代码的完整性检查，使用的技术包括消息验证码、消息鉴别码和防止重放机制等。如果隧道实施不可用这类保护，或者如果传输的数据和代码特别敏感，那么完整性保护控制宜在终端系统中实现，因而完整性保护就以端到端的方式提供。

7.3 鉴别

隧道的建立和操作过程宜得到鉴别控制的支持，从而能保证隧道的每一端都正在与正确的伙伴端点(可能是一个远程访问系统)通信以及所接收的数据和代码来自正确的得到授权的源。这些安全控制包括，例如，密码保护、密码挑战保护、基于安全证书的系统、安全密钥交换规程、数据原发鉴别码和防止重放机制。

7.4 授权

隧道的建立和操作过程宜得到访问控制的支持，诸如 ACL，从而能保证隧道的每一端都正在与得到授权的伙伴端点（可能是一个远程接入系统）通信以及所接收的数据和代码来自得到授权的源。对穿越已建立隧道的数据通道的访问进行控制超出了隧道机制的范畴，宜由端系统中的适当访问控制来处理。

7.5 可用性

隧道的可用性，以及 VPN 的可用性，是支撑网络基础设施和端点系统的可用性的功能。对抗特定于隧道机制的拒绝服务攻击的安全控制措施，宜在任何可能之处结合使用。

对于特定的服务级协定，宜检验多种弹性隧道备用。

7.6 隧道端点

对于 VPN 端点的安全要求也宜考虑。通常每个 VPN 端点宜确保在主机网络与 VPN 之间只有受控的网络通信流。这通常意味着关闭路由和至少也使用包过滤器或防火墙技术。更多细节见 8.3.1（端点安全）和 8.3.2（终止点安全）。

8 安全 VPN 选择指南

8.1 法规和法律方面

与网络连接和 VPN 使用相关的国家法规法律的安全要求，特别是国家加密标准的使用规定，都应予以考虑：

这包括关注以下方面的法规和/或法律：

——隐私/数据的保护；

——密码技术的使用；

——操作风险管理/治理。

8.2 VPN 管理方面

在考虑 VPN 的使用及其对管理、控制和终端用户安全面的影响时，组织中其职责与 VPN 相关的所有人员都宜明白其业务要求和利益。此外，他们和 VPN 的所有其他用户宜意识到这种连接的安全风险以及相关控制域。业务要求和利益可能影响在如下过程中的很多决定和行动：考虑 VPN 连接，识别潜在的控制域，然后是最终的选择、设计、实施和维护安全控制。因此，在整个选择过程中，都需考虑这些业务要求和利益。

有关安全服务管理框架和整个网络安全管理的详细指南见 ISO/IEC 18028-1:2006，且作为“安全管理面”的一部分在 ISO/IEC 18028-2:2006 中论及。

8.3 VPN 体系结构方面

选择 VPN 时，下列体系结构方面宜得到处理：

——端点安全；

——终止点安全；

——恶意软件保护；

——鉴别；

——入侵检测系统；

——安全网关（包括防火墙）；

——网络设计；

——其他连通性；

——隧道分离；

——审计日志和网络监控；

——技术脆弱性管理。

下面逐一概述这些方面。

8.3.1 端点安全

VPN 的功能是提供一条安全跨越一些网络介质的安全通信信道。但是，建立 VPN 的时候却不可能监视其数据流包含的内容。如果任何一个端点受到损害，这种损害可能扩散到跨越 VPN 的会话。

端点安全不仅适用于设备本身，也适用于这些设备上的应用程序以及与使用相关的规程/物理方面。

一些用于远程接入的端点用户设备（例如移动/远程工作计算设备）可能未受到与 VPN 相同的管理控制。这些设备可能被连接到不同的网络，例如，在不同时段获得互联网和组织专用网的访问权。这些网络可能带来额外的风险，宜给予考量以确保应用适当的安全控制。在考虑此类端点设备的安全时，宜考虑 GB/T 22081—2008 中的安全控制，这些安全控制与以下方面相关：

——设备安全；

——抵御恶意代码和移动代码；

——设备使用人员的信息安全意识的培养、教育和培训；

——VPN 相关技术和设备的技术脆弱性管理；

宜考虑其他控制，例如包过滤或个人防火墙。

8.3.2 终止点安全

影响 VPN 安全的关键因素之一是如何在每个端点终止 VPN。如果终止点直接设在端点的核心（例如，处于网络的安全区），安全直接取决于远程伙伴的安全。如果终止点设在非安全区中某处，通信就可能被轻易地欺骗。

VPN 终止的标准方法包括：

——使用外部防火墙终止设施在防火墙上终止：适用于点对点的连通性（例如在 2 个网络之间）。（GB/T 25068.3 中进一步讨论防火墙）；

——在中间区部署专门的 VPN 端点，允许其有进一步处理来自 VPN 信息的能力（例如，决定是否许可访问安全区中的应用/系统）。中间区终止可能允许更多地控制 VPN 及其用户。

在以上任何一种情况下，VPN 端点在允许访问前都宜鉴别实体（例如用户或设备）。对于为设置 VPN 链接而在端点之间进行的鉴别，这是一种附加鉴别。例如，对用户而言，这种鉴别通常包括用户名和口令，也可能要求使用附加形式的鉴别（称作“强鉴别”），例如令牌、卡或生物技术。

8.3.3 恶意软件保护

一旦表明信息系统无任何恶意软件，那么引入此类代码的唯一途径就是通过数据（或可执行代码）。VPN 端点提供良好的控制点来实现恶意软件保护，以控制此类代码的传输。

更多有关抵御（包括病毒、蠕虫和特洛伊木马）恶意代码的信息见 GB/T 22081—2008。

8.3.4 鉴别

鉴别是建立 VPN 的关键阶段之一。必然地，每一端宜鉴别预期的会话伙伴（换言之，需要相互鉴别）。这能用几种方法实现：

——预共享密钥。此方法可提供便捷性，因为一旦设置这种密钥，就无需更多的管理。然而，如果它们受到损害，就可能被滥用（例如中间人攻击）。

——证书。这种方法提供更大的灵活性和弹性，尤其是在部署 PKI 备份以简化密钥管理、撤销和重发时。

有关鉴别和对鉴别使用基于密码服务的更多信息参见 ISO/IEC 18028-1:2006、GB/T 17901.1—1999 和 GB/T 22081—2008。

8.3.5 入侵检测系统（IDS）

宜考虑入侵检测系统（IDS）技术的需要。IDS 能在 VPN 的两端实现，以检测可能的入侵。然后 IDS 报警能由任何适当的机制发出，也可作为审计跟踪的一部分被记录（和管理）。值得注意的是，甚至

一些个人防火墙也有作为简单的入侵防护系统(IPS)的资质,用于阻止对未授权应用的网络接入。

有关 IDS 的更多信息参见 ISO/IEC 18028-1:2006、ISO/IEC TR 15947 和 ISO/IEC 18043。

8.3.6 安全网关

对于适当安全网关(包括防火墙)技术的选择宜予以仔细考虑以支持 VPN 的部署。

有关安全网关(包括防火墙)的信息参见 GB/T 25068.3。

8.3.7 网络设计

VPN 任何一端的网络设计宜支持上面讨论的终止点安全的目标。特别是,VPN 通常宜在外部防火墙上(例如在网络边界)或在自己的中间区内被终止。

更多有关信息参见 ISO/IEC 18028-1:2006、ISO/IEC 18028-2:2006、GB/T 25068.3 和 GB/T 25068.4。

8.3.8 其他连通性

对于 VPN 端点的任何更多的连通性宜予以考虑。在 VPN 的任何一个端点,如果有其他连通性存在,则从该信道发起的安全漏洞可能攻击本地系统,并经由该 VPN 攻击远程系统。通过正确的网络设计和防火墙的使用,能够降低这种可能性。然而,最有效的控制是没有任何不必要的连通性。对于在远程/居家系统中使用调制解调器而言,这种考量尤为急迫。

对于组织网络与提供支持、故障诊断等服务的第三方组织之间的连通性宜予以特别关注,对于服务提供商环境的安全控制宜作为合同安排的一部分而确立。这类控制宜确保一个与服务提供商的其他操作和顾客环境在物理上和逻辑上分隔的环境。更多信息见 GB/T 22081—2008 中 6.2。

更多有关信息参见 GB/T 25068.3。

8.3.9 隧道分离

情况允许时,宜避免分离隧道。分离隧道是指单一连接(通常是互联网)支持 VPN 和其他连接(VPN 或其他)的能力。在这种情形下,因为攻击来自其他隧道,所以远程网络安全有受到损害的风险;这种情形类似于在两个网络之间提供路由的、具有双网卡的个人计算机。总之,通过 VPN 产品"接管"网络连接能够避免隧道分离。

8.3.10 审计日志和网络监控

与其他安全技术相同的是,所选择的 VPN 解决方案宜维护适当的审计日志,以分析该端点处的所有行动。它与网络产生的其他审计日志一样,宜用于评审安全事件的迹象。

宜小心以确保审计日志本身是被保护的、与被评估的风险相当、抵御篡改和滥用。如果审计日志将被用于法律诉讼,那么其完整性应不容质疑。

更多有关审计日志和网络监控的信息参见 ISO/IEC 18028-1:2006 和 GB/T 22081—2008。

8.3.11 技术脆弱性管理

与其他复杂系统一样,网络环境也不能免于出错。在 VPN 等网络中,技术脆弱性在频繁使用的组件中出现,并为之发布。利用这些技术脆弱性能严重影响 VPN 的安全,大多数影响可以在可用性和保密性领域观察到。因此所有的 VPN 设备宜具有技术脆弱性管理。

有关脆弱性管理的更多信息参见 ISO/IEC 18028-1:2006 和 GB/T 22081。

9 安全 VPN 实施指南

9.1 VPN 管理考量

有关实施安全服务管理框架和网络安全管理的详细指南参见 ISO/IEC 18028-1:2006。本部分也讨论 VPN 的高级安全风险以及与降低这些风险相关的安全控制组。ISO/IEC 18028-2:2006 讨论那些需要跨越管理、控制和终端用户安全面的网络安全活动。

9.2 VPN 技术考量

完成安全 VPN 的实施需要系统地考虑目标中所确定的因素。宜特别考虑以下实施方面:

——承载协议的选择;

——硬件对软件；

——VPN 设备管理。

下面逐一讨论这些方面。

附录 A 提供各种类型 VPN 经常使用的特定技术和协议的更多信息。

9.2.1 承载协议选择

宜基于以下方面选择适当的安全承载协议：

——业务要求；

——互操作性(正式标准或专用标准)；

——市场洞察力；

——已知弱点；

——健壮性。

9.2.2 VPN 装置

宜考虑 VPN 装置的使用。在小规模的 VPN(例如单用户至中心系统)中，VPN 的功能由软件解决方案来实现是适当的。在很多情况下，使用装置来提供 VPN 功能可能具有显著的优点，例如，简化管理，通常可在更加安全坚固的平台上操作。也可能是所要求的某种形式的鉴别平台(例如目录、PKI 或 RADIUS)，例如，它将只允许授权用户连接到中心位置。

9.2.3 VPN 设备管理

宜正确地管理 VPN 设备。VPN 设备管理是有关设置和监控 VPN 设备所需过程的通用术语。设置 VPN 设备包括：将其配置为网络配置和所需的端口/应用访问、安装证书(例如为更高层 VPN)和像对待其他任何网络设备那样对 VPN 设备进行连续网络监控。

使用光盘、磁盘等移动媒体的 VPN 部署宜受到控制，例如，创建交付和接收日志以及实现对媒体复用(日期/时间失效等)或媒体可使用次数的限制。

9.2.4 VPN 安全监控

VPN，尤其是当其作为进入公司网络的远程接入信道而使用时，如果未得到精心的管理和控制，会给网络安全管理带来特别的挑战。

宜考虑隧道自身、其端点还有流经隧道的数据和代码，以防止将其作为一条便捷的进入网络的安全通道提供给攻击者。

为使网络安全控制保持有效，至关重要的是，对包括 VPN 在内的安全实施进行系统的网络监控以及网络管理者或管理员能够对实际的或怀疑的信息安全事件进行检测和做出反应。

此外，宜实施以下一至多个措施：

——入侵检测系统；

——安全/事件警告；

——安全/审计日志；

——常规检测；

——培训用户，使其识别和报告信息安全事件。

重要的是认识到网络安全是一个动态概念。因此，至关重要的是，安全人员始终跟上该领域的进展且 VPN 及支撑技术一直在使用供应商所提供的最新安全补丁和修正。

有关上述所有内容的更多信息参见 ISO/IEC 18028-1:2006、ISO/IEC TR 15947、ISO/IEC 18043、GB/Z 20985 和 GB/T 22081—2008。

附 录 A
（资料性附录）
实现 VPN 所使用的技术和协议

A.1 导言

本资料性附录提供用于实现 VPN 的典型技术和协议的示例。本附录未打算提供一个完全列表，或把一个技术或协议提升到其他技术或协议之上。

A.5 概括比较 VPN 协议的安全特点。

A.2 第 2 层 VPN

A.2.1 帧中继

帧中继是基于 X.25 的包交换技术。在帧中继中，用于数据传输的帧的大小是可变的。此外，任何差错控制机制均只由发送端和接收端负责，从而使数据得以高速传输。它使用两种类型的电路来传输数据：永久式虚电路(PVC)和交换式虚电路(SVC)。PVC 是穿过专用网(例如网络服务提供商所拥有的网络)的虚拟通道。在这种通道中，连接的端点由网络管理员规定。SVC 是更短暂的虚拟通道(通常穿过外联网)。在这种通道中，连接的端点由网络用户在呼叫发起时规定。

A.2.2 异步传输模式(ATM)

ATM 是基于 PVC 的数字转换技术，它能支持音频、视频和数据信号。为了实现该目的，它使用固定大小的帧或包。这些包(或“信元”)在传输之前被排队，并被异步处理，不考虑其他相关信元。这使得 ATM 传输的速度比其他交换技术快。

A.2.3 多协议标签交换(MPLS)

MPLS 是一种为在网络间路由选择中使用而开发的技术，即把标签分配给每个数据通道或流，并用于交换连接，覆盖常规的路由选择协议机制。它通常使基于 IP 的 VPN 能够跨越基于 ATM 的网络而部署。在传输期间，接受 IP 包的初始 MPLS 设备使用分配到的 MPLS 标签将 IP 包封装。随后，这个 MPLS 标签而非实际的 IP 头，被用于跨越广域网按路线发送这些包。在基于 ATM 网络的边缘，当这种包将访问基于 IP 的外部基础设施(例如互联网)时，其 MPLS 标签再被剥离。

MPLS 支持服务等级(CoS)和服务质量(QoS)，使不同类型的通信流(例如音频、视频、消息)按不同的优先级在网络上传输。

在将 MPLS 技术用于音频/视频等高带宽通信流时，主要的风险是有可能造成信号质量差，其原因是端到端的延迟，尤其是在使用不同的网络承载和转换时。

MPLS 是在一系列的 IETF RFC 中定义的，这些协议包括 RFC 3031(多协议标签交换体系)、RFC 3032(MPLS 标签栈编码)和 RFC 3036[标签分发协议(LDP)规范]。

A.2.4 点对点协议(PPP)

PPP 被设计成跨越拨号接入或专门的点对点连接来发送数据。PPP 把 IP、IPX(互联网包交换协议)和 NetBEUI 包封装在 PPP 帧之内，然后跨越点对点链接来传输 PPP 封装的包。PPP 通常用作客户端设备与远程接入服务器之间的拨号接入协议。

OSI 的第 2 层协议严重依赖于最初为 PPP 规定的特点。

其细节见 IETF RFC 1661(点对点协议)。

A.2.5 第 2 层转发(L2F)协议

L2F 是一个传输协议，它允许拨号接入服务器构造 PPP 中的拨号接入通信流，并在广域网链接上将它传输到一台 L2F 服务器(路由器)。然后，L2F 服务器将其解包并置入网络。L2F 与 L2TP 不同，

它没有指定的客户端。注意:L2F 仅在强制隧道中起作用。L2F 不提供数据保密性;通信流作为明文传输。L2F 最终将被 L2TP 取代。

其细节见 IETF RFC 2341[思科第 2 层转发(协议)"L2F"]。

A.2.6 第 2 层隧道协议(L2TP)

L2TP 允许 IP、IPX 或 NetBEUI 通信流被加密,然后在支持点对点数据报交付的任何介质(诸如 IP、X.25、帧中继或 ATM 等)上发送。

L2TP 是一个网络协议,它封装在 IP、X.25、帧中继或异步传输网络(ATM)上发送的 PPP 帧之中。当 L2TP 被配置为使用 IP 作为其数据报传输时,它可用作互联网上的一种隧道协议。L2TP 也能直接在各种广域网介质(诸如帧中继)上使用而没有 IP 传输层。IP 互联网上的 L2TP 使用 UDP 和一系列的 L2TP 隧道维护消息。L2TP 也使用 UDP 把被 L2TP 封装的 PPP 帧作为隧道数据发送。被封装的 PPP 帧的载荷能被加密和/或压缩。

图 A.1 描述 PPP 帧及控制消息在 L2TP 控制和数据信道上的关系。L2TP 使用两种类型的消息:控制消息和数据消息。控制消息用于信道和呼叫的建立、维护及清除。数据消息用于封装隧道上承载的 PPP 帧。控制消息使用 L2TP 内可靠的控制信道来保证交付,在发生包丢失时,数据消息不被重传。PPP 帧在不可靠的数据信道上传输,首先用 L2TP 头封装 PPP 帧,然后使用 UDP、帧中继、ATM 等进行包传输。控制消息在可靠的 L2TP 控制信道上发送,该信道在同一包传输上传输带内包。

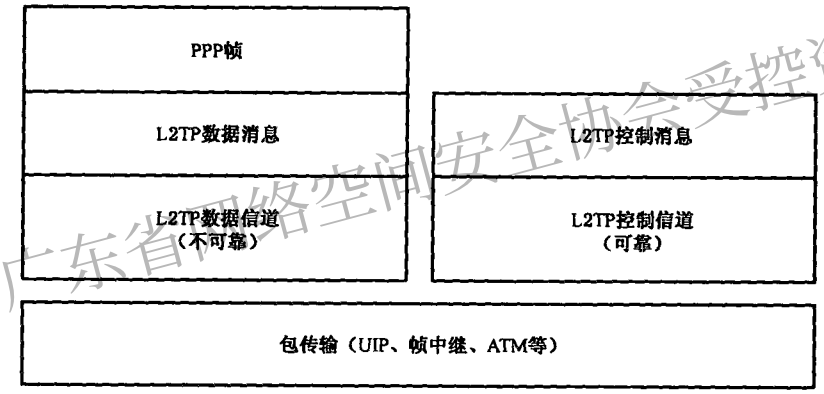

图 A.1 第 2 层隧道协议的结构

传统上,安全的 VPN 是使用专门的硬件和 L2TP 等专有协议而设置的。这类 VPN 具有已知的安全脆弱性,很多安全 VPN 的实施代之以在 IPsec 或 SSL 上构建。

其细节见 IETF RFC 2661(第 2 层隧道协议)。

A.3 第 3 层 VPN

A.3.1 IPSec

IPSec 是由 IETF 作为端到端的机制而设计的框架,用以保证基于 IP 通信的数据安全。IPSec 定义 OSI 第 3 层协议的标准,该标准支持穿越 IP 互联网络信息的安全传输。能够将 IPSec 想象为提供给 TCP 层之下 IP 的可选层。IPSec 层由每个硬件设备上的安全策略和收发双方之间的协商安全关联来控制。

IPSec 提供两个独立的协议来保证数据保密性和数据完整性。鉴别头(AH)协议提供源鉴别和完整性,不提供加密。封装安全载荷(ESP)协议提供鉴别,它也提供完整性和/或加密。两个协议都能以传输模式或隧道模式实施。在 ESP 的传输模式中,只有 OSI 传输层的数据得到保护;在隧道模式中,整个 IP 包被封装。AH 协议保护整个 IP 包。AH 和 ESP 协议均能提供重放保护。

IPSec 隧道包括隧道客户端和隧道服务器,两者均被配置为使用 IPSec 隧道和协商加密机制。使用 IPsec ESP 隧道模式时,允许 IP 数据报被加密,然后被封装到另一 IP 数据报内,然后穿越专用或公共 IP 互连网络(如互联网)被发送。收到以后,隧道服务器处理明文 IP 头,验证被封装数据报的完整性,给被封装的数据报解密,以找回原始载荷 IP 包。IPSec 隧道模式具有下列特点和限制:

——它只支持 IP 通信流；

——它由安全策略(一组过滤—匹配规则)控制。这种安全策略按照偏好和可用鉴别方法的顺序，来建立可用的加密和隧道机制。只要有通信流，两台机器就进行相互鉴别，然后协商要使用的加密方法。此后，所有的通信流都使用协商加密机制加密，然后被包装到隧道头中。

IPSec 也包含一个支持鉴别、授权、安全关联协商、密钥建立和管理的组件。

IPsec 协议涵盖 VPN 设置过程的各个方面，从初始的密钥协商直至最后的隧道设置。它将允许选择大量的加密和完整性解决方案。IPsec 的复杂性已经导致大量的歧义、矛盾、低效率和弱点(例如，在跨越一组端点预共享密钥之处，会话设置对中间人攻击和欺骗攻击的脆弱性)。共同的问题通常起源于由 IPsec 复杂性所造成的弱配置。

IPsec 已在一系列的 IETF RFC 中定义，特别是 RFC 2401、2402 和 2406。

A.4 高层 VPN

A.4.1 安全套接层(SSL)

SSL 通常用于保护跨网交易的安全，且已在 Web 浏览器/服务器技术中普遍使用。它作为插在应用层与 TCP/IP 层之间的一层运行，普遍与超文本传输协议(HTTP)一起使用，此处被称作安全超文本传输协议(HTTPS)。

用于 VPN 通信流的 SSL 协议与用于保护浏览器数据流安全的协议相同。公钥基础设施(PKI，可为专用的或公共的)将向每个 VPN 端点颁发证书。在 SSL 端点发送证书之处，接收方可使用 PKI 设施来鉴别证书及发送方的真实性。如果进行了相互鉴别，这些证书将允许排除中间人攻击，但在一个 SSL 端点证书跨越多个设备共享之处，仍可能易于被欺骗。

作为 SSL 会话设置的一部分，两个端点协商一个加密软件包，该加密包是一个预定义的加密、散列和密钥交换方法的组合，它将为交换数据的保密性和完整性规定实际的保护级别。

A.4.2 安全壳

安全壳与 Unix 系统有历史渊源，它通过创建并维护安全的 VPN，来获得对命令行界面和其他正在运行应用程序的安全访问权。它依赖每个参与系统来生成一个非对称密钥对，来保护私钥的本地安全并与要求向第一个系统发送数据的系统共享公钥。

公钥不同于 SSL 和 IPsec，它并不在正规的 PKI 中鉴别。相反，公钥被用于给鉴别发送方所使用的信息进行“签名”以及创建生成的、在两个系统上共享的密钥。这时，选择一个对称加密算法，并生成一个密钥用于数据传输。也存在其他鉴别机制，例如口令鉴别。安全壳也可用在计算机系统之间，以创建可被其他协议直接使用的安全隧道。

A.5 典型 VPN 协议安全特点比较

表 A.1 提供典型 VPN 协议安全特点的比较。

表 A.1 VPN 基本协议和 VPN 功能范围

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 2 层 VPN	帧中继	—	—	—	—
	ATM	—	—	—	—
	MPLS	—	—	—	—
	PPP	—	—	—	—
	L2F	—	—	—	—
	L2TP	简单、类似 CHAP	—	—	—

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

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

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