ICS 35.040
L 80

中华人民共和国国家标准

GB/T 32922—2016

信息安全技术　IPSec VPN 安全接入基本要求与实施指南

Information security technology—Baseline and implementation guide of IPSec VPN securing access

2016-08-29 发布　　2017-03-01 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

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本标准起草单位:国家信息中心、华为技术有限公司、中安网脉(北京)技术股份有限公司、网神信息技术(北京)股份有限公司、北京天融信科技股份有限公司、迈普通信技术股份有限公司。

本标准主要起草人:罗海宁、周民、吕品、冷默、黄敏、徐浩、张锐卿、任献永、徐惠清、邵国安。

引　言

本标准主要内容包括 IPSec VPN 安全接入基本要求和基于 IPSec VPN 技术建设安全接入平台或系统的实施指南，其中“基本要求”对 IPSec VPN 安全接入应用过程中有关网关、客户端以及安全管理方面提出技术要求，“实施指南”主要适用于采用 IPSec VPN 技术开展安全接入应用的机构，指导其进行基于 IPSec VPN 技术的安全接入平台或系统的需求分析、方案设计、配置实施、测试与备案、运行管理。同时，本标准也可为相关设备厂商进行产品的设计和开发提供参考。

本标准是在国家电子政务外网 IPSec VPN 安全接入应用实践基础上归纳总结并提出的技术标准，也可广泛适用于 IPSec VPN 各种应用场景。

信息安全技术　IPSec VPN 安全接入基本要求与实施指南

1　范围

本标准明确了采用 IPSec VPN 技术实现安全接入的场景，提出了 IPSec VPN 安全接入应用过程中有关网关、客户端以及安全管理等方面的要求，同时给出了 IPSec VPN 安全接入的实施过程指导。

本标准适用于采用 IPSec VPN 技术开展安全接入应用的机构，指导其进行基于 IPSec VPN 技术开展安全接入平台或系统的需求分析、方案设计、配置实施、测试与备案、运行管理，也适用于设备厂商参考其进行产品的设计和开发。

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 20518—2006　信息安全技术　公钥基础设施　数字证书格式

GB/T 25069—2010　信息安全技术　术语

GM/T 0003—2012(所有部分)　SM2 椭圆曲线公钥密码算法

GM/T 0004—2012　SM3 密码杂凑算法

GM/T 0016—2012　智能密码钥匙密码应用接口规范

GM/T 0017—2012　智能密码钥匙密码应用接口数据格式规范

GM/T 0022—2014　IPSec VPN 技术规范

GM/T 0023—2014　IPSec VPN 网关产品规范

3　术语和定义

GB/T 25069—2010 界定的以及下列术语和定义适用于本文件。

3.1

第二层隧道协议　layer 2 tunneling protocol

L2TP

一种支持 VPN 的隧道协议，本身不提供加密功能。

3.2

IP 安全协议　IP security

IPSec

一套用于保护 IP 通信的安全协议，是 IPv4 的一个可选协议系列，也是 IPv6 的组成部分之一。

3.3

虚拟专用网　virtual private network

VPN

一种在公共通信基础网络上通过逻辑方式隔离出来的网络。

3.4

安全联盟　security association

SA

两个通信实体经协商建立起来的一种协定，描述实体如何利用安全服务来进行安全的通信。

3.5

因特网密钥交换协议　internet key exchange

IKE

IPSec 体系结构中的一种主要协议，由因特网安全联盟和密钥管理协议、密钥交换协议组成。

3.6

失效对端检测　dead peer detection

DPD

一种基于数据流的、用于检测 IPSec 连接状态的方法。

3.7

数字证书可辨别名　distinguished name

DN

又称为数字证书实体特征名，用来识别公钥的实体名称，通常包括实体的通用名、组织单位、组织和国家信息。

4　缩略语

下列缩略语适用于本文件。

CA	数字证书认证中心(certificate authority)
CE	用户端边缘设备(customer edge)
DN	数字证书可辨识名(distinguished name)
DPD	失效对端检测 (dead peer detection)
IKE	因特网密钥交换协议(internet key exchange)
IPSec	IP 安全协议(internet protocol security)
LDAP	轻量级目录访问协议(light directory access protocol)
MPLS	多协议标签交换(multi-protocol label switching)
NAT	网络地址转换(network address translation)
PE	运营商边缘设备(provider edge)
PPP	点对点协议(point to point protocol)
PPTP	点对点隧道协议(point to point tunneling protocol)
SA	安全联盟(security association)
SHA	安全杂凑算法(secure hash algorithm)
SSH	安全外壳协议(secure shell)
SSL	安全套接层(secure socket layer)
VPDN	虚拟专用拨号网(virtual private dial-up networks)
VPN	虚拟专用网(virtual private network)
OCSP	在线证书状态协议(online certicifate status protocol)

5 IPSec VPN 安全接入场景

5.1 网关到网关的安全接入场景

IPSec VPN 网关到网关的对接适用于分支机构安全接入到总部网络或者机构之间的安全接入，如图 1 所示。典型应用案例参见附录 A。

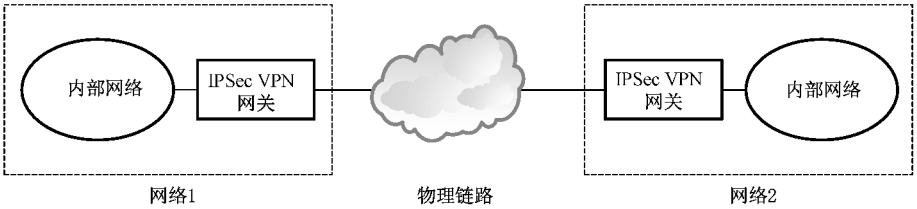

图 1 网关到网关的安全接入场景图

网络 1 和网络 2 分别部署 IPSec VPN 网关，通过 IPSec VPN 网关建立网络之间的安全传输通道。

物理链路包括互联网链路、运营商提供的无线接入链路或专线链路等。

5.2 终端到网关的安全接入场景

终端到 IPSec VPN 网关的安全接入适用于移动办公用户或者公众用户接入机构内部网络，如图 2 所示。典型应用案例参见附录 A。

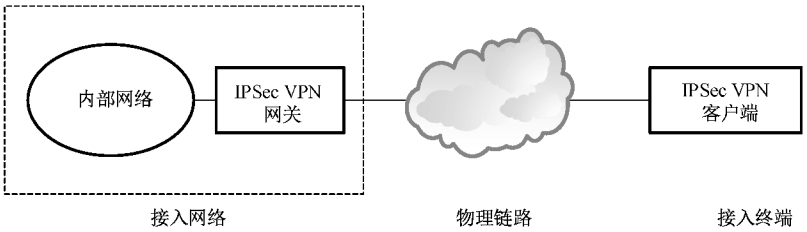

图 2 终端到网关的安全接入场景图

接入网络部署 IPSec VPN 网关，接入终端通过 IPSec VPN 客户端和 IPSec VPN 网关建立安全传输通道。IPSec VPN 客户端包含在接入终端上部署的连接网关的软件以及可选用的智能密码钥匙等硬件，接入终端可以是计算机，也可以是智能手机、平板电脑等移动智能终端设备。

物理链路包括互联网链路、运营商提供的无线链路等。

6 IPSec VPN 安全接入基本要求

6.1 IPSec VPN 网关技术要求

6.1.1 产品要求

IPSec VPN 网关产品选择基本要求如下：

a) 应符合 GM/T 0022—2014、GM/T 0023—2014 要求；

b) 应支持符合国家标准规定的对称算法，应支持遵循 GM/T 0003—2012 SM2 或 2048 位及以上的 RSA 非对称密码算法，应支持遵循 GM/T 0004—2012 SM3 或 SHA1 杂凑算法；

c) 应支持隧道模式和传输模式。

6.1.2 功能要求

IPSec VPN 网关功能要求如下：

a) VPN 功能类型：应支持 L2TP over IPSec 、IPSec over GRE 以及 IPSec over L2TP 等。

b) 产品可靠性功能：

1) 应支持双机热备方式及隧道状态同步功能；

2) 应支持 DPD 功能，隧道不可用时可重新建立。

c) 互通兼容性功能：

1) 应支持 NAT 穿越，能够双向穿透 NAT 设备；

2) 异构网关对接时应符合如下要求：

- 采用国家标准密钥协商协议时，应遵循 GM/T 0022—2014，在协商时对接网关应采用自动密钥协商机制，选择一致的协商属性，具体包括加密算法、杂凑算法、认证方式等；
- 对接网关在密钥协商时支持 NAT 穿越选项应保持一致；
- 应支持 ESP 或 AH 安全传输协议，对接网关应选择一致的传输协议。

d) IPv6 兼容性功能：应支持 IPv6 基本协议，支持双栈、隧道、NAT64 翻译、双栈精简技术等 IPv6 过渡技术。IPv6 过渡技术参见附录 B。

e) 数字证书认证功能：

1) 应符合 GB/T 20518—2006 证书格式；

2) 应支持受信任的 CA 机构颁发的数字证书认证；

3) 应支持 LDAP、OCSP 等在线认证方式；

4) 应支持自动下载 CRL；

5) 应支持在线或离线验证证书有效性；

6) 应支持对认证用户分组授权。

f) 设备管理功能：

1) 应支持对网关的隧道状态、在线用户状态及 CPU、内存利用率等关键运行指标的监测和管理；

2) 应支持 Syslog 等格式日志输出，提供采集与配置管理接口。

6.1.3 性能要求

根据 IPSec VPN 网关的性能不同，从高到低分成 A 类(10 万用户数)、B 类(2 万用户数)、C 类(5 000用户数)和 D 类(1 000 用户数)四类网关，以适配不同的应用场景。各类网关的性能要求应不低于如下要求：

表 1 IPSec VPN 网关性能指标分类表

性能指标	网关类别			
	A 类	B 类	C 类	D 类
加解密吞吐量(1 428 字节)[a]	20 Gbit/s	5 Gbit/s	1 Gbit/s	200 Mbit/s
加解密时延(1 428 字节)[b]	小于 1 ms	小于 10 ms	小于 20 ms	小于 50 ms
加解密丢包率(1 428 字节)[c]	5%	10%	10%	10%
每秒新建隧道数[d]	100	50	30	20

表 1（续）

性能指标	网关类别			
	A 类	B 类	C 类	D 类
最大并发隧道数[e]	100 000	20 000	10 000	5 000
单隧道最大并发连接数[f]	10 000 000	2 000 000	500 000	100 000

[a] 加解密吞吐量：分别在 64 字节以太帧长和 1 428 字节（IPv6 下为 1 408 字节）以太帧长时，IPSec VPN 网关在丢包率为 0 的条件下内网口达到的双向数据最大流量，性能数据按 1 428 字节测试获得。

[b] 加解密时延：分别在 64 字节以太帧长和 1 428 字节（IPv6 下为 1 408 字节）以太帧长时，IPSec VPN 网关在丢包率为 0 的条件下，一个明文数据流经加密变为密文，再由密文解密还原为明文所消耗的平均时间，性能数据按 1 428 字节测试获得。

[c] 加解密丢包率：分别在 64 字节以太帧长和 1 428 字节（IPv6 下为 1 408 字节）以太帧长时，在 IPSec VPN 网关内网口处于线速情况下，单位时间内错误或丢失的数据包占总发数据包数量的百分比，性能数据按 1 428 字节测试获得。

[d] 每秒新建隧道数：网关在一秒钟的单位时间内能够建立 IPSec VPN 隧道数目的最大值。

[e] 最大并发隧道数：网关同时并存的 IPSec VPN 隧道数目的最大值。

[f] 单隧道最大并发连接数：网关单条 IPSec VPN 隧道最大能够并发建立的 TCP 连接数目。

6.2 IPSec VPN 客户端技术要求

6.2.1 IPSec VPN 客户端软件要求

IPSec VPN 客户端软件要求如下：

a) 客户端密钥交换协议和安全报文协议应符合 GM/T 0022—2014 中 5.1 和 5.2 相关要求；

b) 应支持从智能密码钥匙、电子文件证书中获取证书并利用证书实现与 IPSec VPN 网关的连接；

c) 应支持国内外主流操作系统；

d) 应支持 IPv4、IPv6 等网络协议；

e) 应支持 IPSec VPN 穿越 NAT 的技术。

f) 客户端接入 IPSec VPN 网关时应符合如下要求：

1) 采用国家标准密钥协商协议，应遵循 GM/T 0022—2014，在协商时客户端应与 IPSec VPN 网关选择一致的协商属性，具体包括加密算法、杂凑算法、认证方式等；

2) 客户端在密钥协商时是否支持 NAT 穿越应与 IPSec VPN 网关保持一致；

3) 应支持扩展认证；

4) 应支持采用 DHCP over IPSec 协议获取 IP 地址；

5) 应支持 ESP 或 AH 安全传输协议，客户端应与 IPSec VPN 网关选择一致的传输协议。

6.2.2 IPSec VPN 客户端硬件要求

IPSec VPN 客户端所使用的智能密码钥匙等硬件应支持符合国家标准的算法，并符合 GM/T 0016—2012 和 GM/T 0017—2012 的相关要求。

6.3 安全管理要求

6.3.1 系统管理要求

系统管理要求按照不同安全性要求，分为基本要求和增强要求，具体如下：

a) 基本要求：
   1) 应对 IPSec VPN 设备运行状况、网络流量、用户行为、管理员行为等进行日志记录；
   2) 应对管理员进行角色设置与权限分离；
   3) 应对网络设备的管理员登录地址进行限制；
   4) 身份鉴别信息应具有不易被冒用的特点，口令应有复杂度要求并定期更换；
   5) 应启用 IPSec VPN 登录失败处理功能，设置采取结束会话、限制非法登录次数和当网络登录连接超时自动退出等措施；
   6) 当对 IPSec VPN 设备进行远程管理时，应采用 SSH、SSL 等安全方式保护传输安全。
b) 增强要求：对于安全性要求较高的情况，如安全等级保护第三级及以上的信息系统应用 IPSec VPN 时，除满足基本要求外，还应符合以下要求：
   1) 应按照业务服务的重要性来指定带宽分配优先级别；
   2) 应根据设备记录数据进行分析，并定期由第三方审计系统生成审计报表；
   3) 应对管理员身份认证采取两种或两种以上组合鉴别技术；
   4) 应由内部人员或上级单位定期进行安全检查，检查内容包括现有安全技术措施的有效性、安全配置与安全策略的一致性等；
   5) IPSec VPN 客户端应采用由国家认证的 CA 中心所颁发的证书实现 IKE 协商；
   6) IPSec VPN 客户端的证书应采用智能密码钥匙等硬件介质。

6.3.2 数字证书管理要求

6.3.2.1 设备数字证书管理

设备证书应遵循 PKI 相关标准，将单位、区域等关键信息在证书 DN 中列出。

网关的设备证书的有效期宜大于网关的生命周期。

6.3.2.2 客户端数字证书管理

IPSec VPN 客户端证书宜采用智能密码钥匙等硬件介质承载的证书。

客户端证书应遵循 PKI 相关标准，将用户、单位、区域等关键信息在证书 DN 中列出。

客户端证书丢失或损坏时，应当及时到证书颁发部门办理挂失、吊销、重新注册等手续。

6.3.3 地址管理要求

6.3.3.1 地址规划

应对 IPSec VPN 网关及客户端地址进行统一规划，遵循唯一性、连续性和可扩展性原则。

6.3.3.2 地址分配

客户端可从网关的 DHCP 地址池中获取地址，网关外网口地址宜采用公网地址或对外服务地址，网关内网口地址宜采用私有地址或内部互联地址。

6.3.4 其他要求

密钥管理、数据管理、人员管理和设备管理应符合 GM/T 0022—2014 中 6.3 的相关要求。

7 实施指南

7.1 概述

基于 IPSec VPN 技术建设安全接入平台或系统的实施过程可划分为需求分析、方案设计、配置实

施、测试与备案、运行管理等五个阶段。

7.2 需求分析

7.2.1 IPSec VPN 设备功能与性能需求

根据业务系统数量、业务流量等现状，提出满足业务需求的 IPSec VPN 设备的功能、性能指标要求。

7.2.2 管理需求

从设备管理、密钥管理、证书管理、权限管理、配置管理、日志管理等方面提出相应的管理需求。

7.3 方案设计

7.3.1 概述

方案设计是在需求分析基础上，对建设实施方案进行设计，并完成方案设计文档。

7.3.2 接入方案设计

通过分析业务系统需求，结合机构当前网络拓扑，设计 IPSec VPN 安全接入的实现方式，包括网关、客户端的部署位置、链路拓扑、连接方式等。

7.3.3 管理方案设计

根据需求分析结果和 6.3 的要求进行管理方案设计。

7.4 配置实施

7.4.1 实施准备

在部署实施前，需做好以下准备：

a) 设备选型：根据需求分析结果，按 6.1 要求对 IPSec VPN 网关进行选型，并要求网关设备厂商按 6.2 要求提供 IPSec VPN 客户端软件；IPSec VPN 设备应选用国家主管部门认证许可的产品；

b) 数字证书申请：申请 IPSec VPN 设备证书、管理员证书和客户端证书；

c) IP 地址申请：申请 IPSec VPN 网关地址池、对外服务 IP 地址及设备管理 IP 地址；

d) 备份链路申请：可根据业务系统重要性，向不同的运营商申请备份链路；

e) 割接与回退方案制定：在实施前，应制定网络割接和设备上线方案，制定应急情况下割接或上线不成功时恢复到原有网络的方案。

7.4.2 IPSec VPN 设备部署

根据接入方案完成网关和客户端等设备的部署。

IPSec VPN 网关一般部署在互联网出口，外网口连接互联网，内网口连接内部网络。

在接入终端上安装 IPSec VPN 客户端软件，如采用数字证书，还应导入证书或连接配备的智能密码钥匙等硬件介质。

7.4.3 IPSec VPN 设备配置

IPSec VPN 设备部署完毕后，应完成设备地址配置、证书导入、VPN 隧道配置、VPN 策略配置、集

中管理配置、接入用户授权和认证服务器配置等。

7.4.4 系统联调

组织 IPSec VPN 网关与网关对接调试，网关与客户端对接调试，应按照 6.1.2、6.2、6.3 的要求调整网关或客户端配置，还应根据需要与认证、授权、设备集中管理等其他系统进行联调。

7.5 测试与备案

应制定测试方案，设备部署后对网关、客户端各项功能、性能等进行测试。

测试完成后，应对详细测试结果、测试报告进行备案。

采用国家商用密码产品时，应按照单位主管部门要求进行产品信息备案。

7.6 运行管理

7.6.1 系统维护管理

系统正式投入运行后，应清除系统中临时数据或参数。

应建立针对系统日常维护的安全管理和系统维护制度。

应定期检查 IPSec VPN 设备的配置信息、日志信息。

7.6.2 运行监测

对 IPSec VPN 设备进行实时监测，发现运行过程中的问题和故障。主要监测内容如下：

a) 网络状况：网络链路状况、IP 地址情况；

b) 设备状况：VPN 隧道状况、CPU 与内存等可用资源、策略有效性；

c) 系统状况：业务系统有效性、证书使用状况；

d) 用户行为：用户在线情况、访问对象、访问过程、历史登录信息。

当监测到告警信息时，应记录告警发生时间、告警类型、告警内容等信息，并及时处理和跟踪。

7.6.3 资源管理

对网络拓扑结构、技术方案、系统配置、网络 IP 地址规划和设备型号、证书信息、所承载的业务系统情况等资源信息进行登记，定期对照核查，及时更新维护。

7.6.4 备份与恢复

应制定备份方案，对 IPSec VPN 网关设备配置、安全策略配置等重要数据进行定期备份。

应制定应急预案，定期开展应急恢复演练，应急启动后按照预案应急流程组织应急响应和系统恢复，应急结束后应整理报告并备案，必要时应追究事件责任。

7.6.5 变更与撤销

应建立 IPSec VPN 网关配置修改、客户端增减、应用资源授权范围调整、接入链路调整等变更事项的业务流程，按照流程变更部署。

在 IPSec VPN 安全接入业务撤销时，应清除接入设备的配置信息、用户数据、系统日志等，并回收为用户分配的 IP 地址等。

附 录 A
（资料性附录）
典型应用案例

本附录描述了政务外网基于 IPSec VPN 的典型应用案例，其他行业可以参照实施。

通过部署 IPSec VPN 安全接入系统，为政务外网用户提供从互联网等公众网络可信接入政务外网的安全隧道，满足不具备专线接入条件的部门接入政务外网和政务用户出差或移动办公的接入需求，延伸政务外网的覆盖范围。

各级政务外网划分公用网络区、专用网络区等内部区域和互联网接入区等外部区域。在政务外网互联网接入区集中部署 IPSec VPN 服务网关或网关集群，提供 IPSec VPN 接入网关的接入或移动办公的接入服务。

政务外网使用 IPSec VPN 的典型应用，如图 A.1 所示。

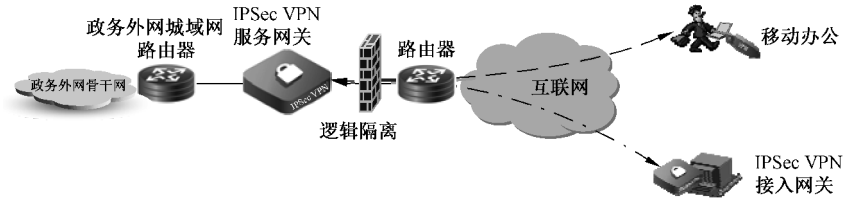

图 A.1 政务外网 IPSec VPN 典型应用示意图

IPSec VPN 网关的部署要点有以下几个方面：

a) 部署位置：IPSec VPN 服务网关的外联接口一般连接到防火墙等与互联网逻辑隔离的安全设备，内联接口连接到政务外网内部区域。IPSec VPN 网关应支持与政务外网 MPLS VPN 多业务域环境的对接。外部接入的 IPSec VPN 接入网关一般部署在远端待接入的局域网互联网出入口处；

b) IP 地址：IPSec VPN 网关外联接口 IP 地址使用互联网地址，IPSec VPN 网关内联接口 IP 地址采用政务外网统一分配的地址。远端接入的 IPSec VPN 接入网关外联口 IP 地址为互联网地址，内联口 IP 地址采用地址池内的地址或者远端局域网地址。IPSec VPN 客户端的 IP 地址一般由 IPSec VPN 网关分配；

c) 接入方式：IPSec VPN 网关一般要求支持网关和客户端两种接入方式；

d) 性能考虑：IPSec VPN 网关的性能需要满足实际的带宽及同时接入 IPSec VPN 网关和客户端数量要求。根据需要可以部署 IPSec VPN 网关集群。

按照政务外网中部署 IPSec VPN 设备的几类实际需求，划分四种场景。

典型应用场景一：不具备专线条件的政务部门接入到政务外网

不具备专线条件接入政务外网的政务部门或其他单位使用 IPSec VPN 网关，通过互联网链路接入政务外网。如图 A.2 所示。

IPSec VPN 网关按照就近接入原则，通过互联网接入到本级政务外网的 IPSec VPN 服务网关，如本级政务外网无 IPSec VPN 服务网关，可申请接入上一级政务外网的 IPSec VPN 服务网关。

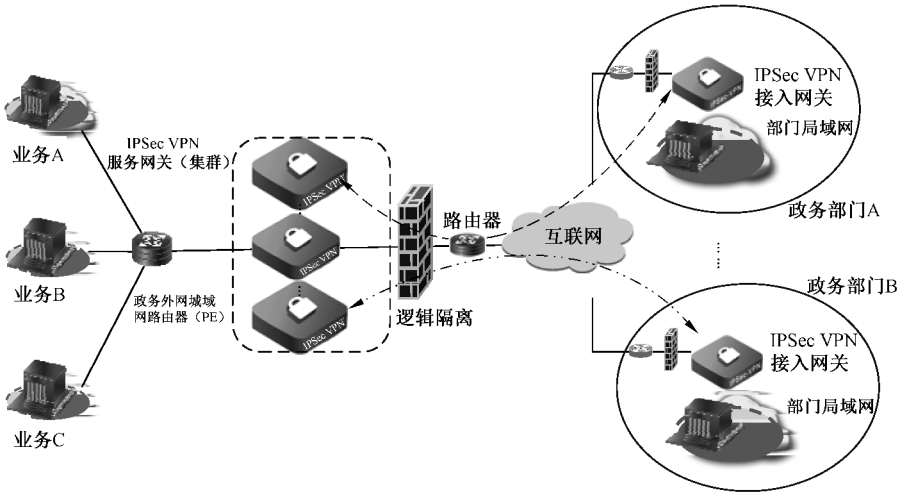

图 A.2　政务外网 IPSec VPN 网关典型应用场景一

典型应用场景二：移动办公用户接入政务外网

移动办公用户以 IPSec VPN 客户端方式接入 IPSec VPN 服务网关，按照属地化原则接入到政务外网。如图 A.3 所示。其他需要以 IPSec VPN 客户端方式接入 IPSec VPN 服务网关的用户，参照此场景。

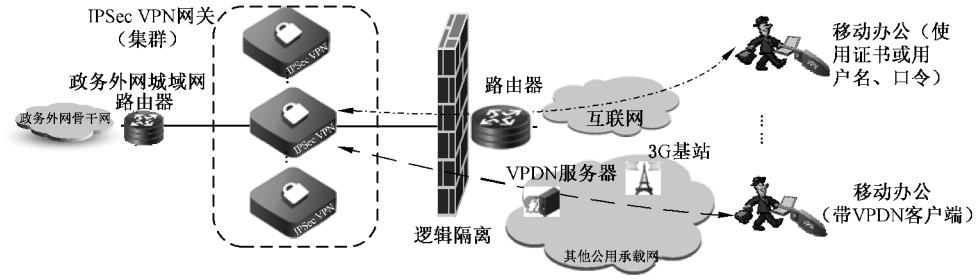

图 A.3　政务外网 IPSec VPN 网关应用场景二

部署要点如下：

a）　移动办公用户分别采用用户名、口令方式或采用证书方式连接到 IPSec VPN 服务网关。一般所访问的应用系统安全保护等级为第二级的，可以使用用户名、口令的方式连接 IPSec VPN 服务网关；应用系统安全保护等级为第三级的，要采用证书方式连接到 IPSec VPN 服务网关；

b）　证书一般应采用政务外网 CA 颁发的证书；

c）　对于只连接政务外网特定业务系统，不接入政务外网的移动办公用户，可采用 SSL VPN 方式连接到 IPSec VPN 服务网关，此时，IPSec VPN 服务网关需启用 SSL VPN 功能；

d）　在 VPDN 拨号、3G 网络等其他公众网络连接情况下，移动办公用户需要先连通 VPDN 或以其他形式连通网络，再连接 IPSec VPN 服务网关。

典型应用场景三：某级政务部门 IPSec VPN 网关级联应用

某级政务部门的 IPSec VPN 服务网关接受来自本级 IPSec VPN 接入网关或客户端的连接，同时又作为 IPSec VPN 接入网关远程联入上一级政务外网 IPSec VPN 服务网关。此 IPSec VPN 网关的配置既要满足接入需求作为服务网关使用同时又要作为接入网关接入到上级服务网关，是一个复合配置。如图 A.4 所示。根据实际情况，也可采用本级政务部门同时部署两台网关，一台是上联的接入网关，另一台是本地服务网关。

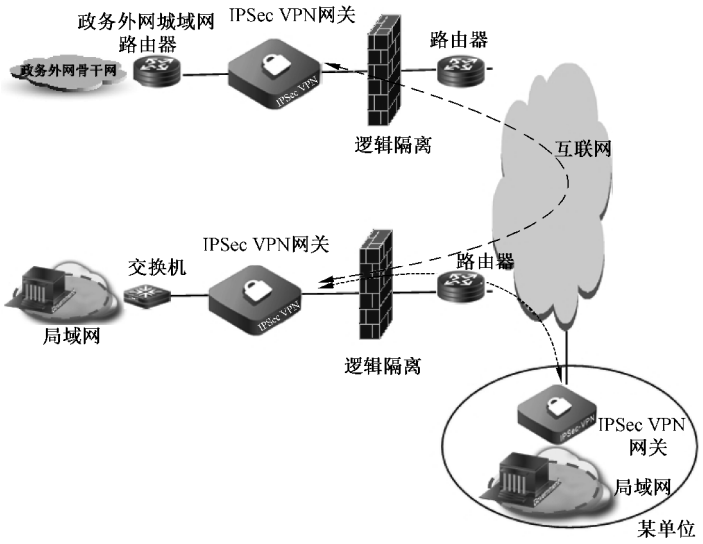

图 A.4　政务外网 IPSec VPN 网关应用场景三

附 录 B
（资料性附录）
IPv6 过渡技术

实现 IPv4 与 IPv6 共存期的应用互访和平滑演进是实现 IPv4 向 IPv6 成功过渡的基础。在整个网络过渡时期，将会有多种不同技术得到应用，以满足过渡时期的不同需求。根据实现机制的不同，过渡技术主要包括双栈、隧道技术和翻译技术。在实际应用中，一般会综合考虑网络、用户、业务、升级成本等诸多因素，将三种过渡技术结合使用，以制定合理的网络过渡解决方案。IPSec 隧道在穿越不同种的网络时有以下场景。

场景一：传输模式 IPSec 6over4 隧道

传输模式 IPSec 6over4 隧道是在 IPv6 over IPv4 隧道基础上嵌套 IPSec 隧道，以此增强传输隧道的安全性。

在 IPv4 网络向 IPv6 网络过渡的初期，IPv4 网络已被大量部署，而 IPv6 网络只是散布在世界各地的一些孤岛。利用隧道技术可以在 IPv4 网络上创建隧道，从而实现 IPv6 孤岛之间的互连。在 IPv4 网络上用于连接 IPv6 孤岛的隧道称为 IPv6 over IPv4 隧道。为了保证 IPv6 报文安全地通过 IPv4 网络，可以利用 IPSec 技术提供保护。

如图 B.1 所示，IPv6 报文到达 IPSec VPN 后，设备会利用 IPv6 over IPv4 技术为报文封装 IPv4 报文头，然后利用 IPSec 技术为报文增加 IPSec 报文头。封装后的报文可以安全穿越 IPv4 网络，到达对端设备后再进行解封装，然后 IPv6 报文会被继续转发到目的端，从而实现了隔离 IPv6 网络安全地互通。

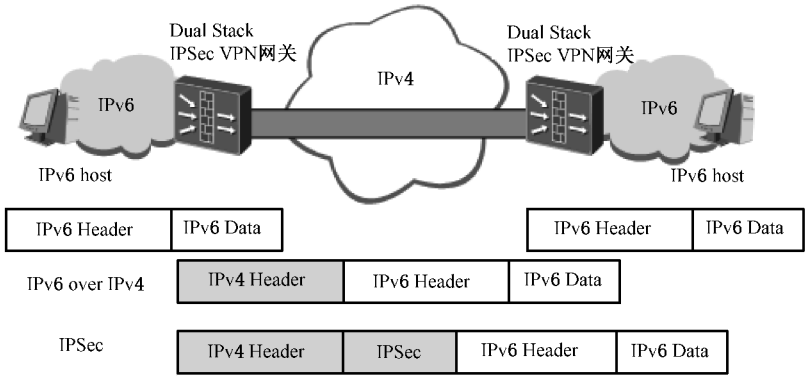

图 B.1 传输模式 IPSec 6over4 隧道组网图

传输模式 IPSec 6over4 隧道封装 IPv6 报文分为两个阶段：首先借助 IPv6 over IPv4 技术为报文封装 IPv4 报文头，然后在 IPv4 报文头后插入 IPSec 报文头。由于这两个阶段相对独立，所以 IPSec 6over4 隧道可以根据 IPv6 over IPv4 隧道的不同分类，适用于多种网络过渡初期场景。根据创建隧道方式的不同，常用 IPv6 over IPv4 隧道模式如下所示。

- IPv6 over IPv4 GRE 隧道
- IPv6 over IPv4 手动隧道
- IPv6 over IPv4 自动隧道
- 6to4 隧道
- 6RD 隧道
- ISATAP 隧道

场景二：隧道模式 IPSec 6over4 隧道

隧道模式 IPSec 6over4 可以同时实现 IPv6 over IPv4 隧道和 IPSec 隧道，增强了传输隧道的安全性。

如图 B.2 所示，IPv6 报文到达 IPSec VPN 网关后，设备会利用 IPSec 6over4 技术为报文封装新的 IPv4 报文头，并插入 IPSec 报文头。封装后的报文可以安全穿越 IPv4 网络，到达对端设备后再进行解封装，然后 IPv6 报文会被继续转发到目的端，从而实现了隔离 IPv6 网络安全地互通。

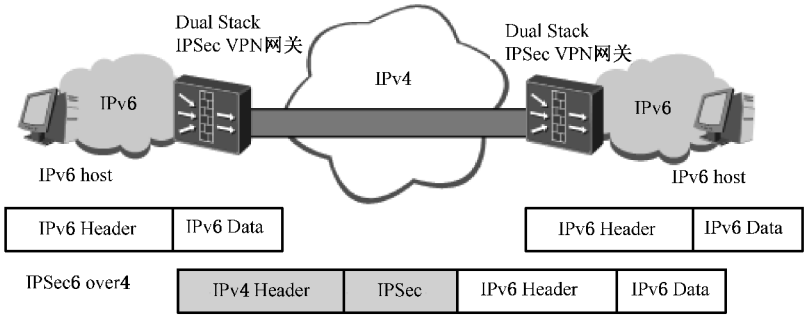

图 B.2　隧道模式 IPSec 6over4 隧道原理图

隧道模式 IPSec 6over4 隧道不同于传输模式 IPSec 6over4 隧道，它并不借助 IPv6 over IPv4 技术为报文封装 IPv4 报文头，而是同时为 IPv6 报文增加 IPv4 报文头和 IPSec 报文头。隧道的两端为 Tunnel接口，不同物理接口的流量可以按照静态路由或策略路由找到对应的 Tunnel 接口，经过加密或解密处理后继续转发。

参 考 文 献

[1] GB/T 20269—2006 信息安全技术 信息系统安全管理要求
[2] GB/T 20270—2006 信息安全技术 网络基础安全技术要求
[3] GB/T 20271—2006 信息安全技术 信息系统通用安全技术要求
[4] GB/T 20272—2006 信息安全技术 操作系统安全技术要求
[5] GB/T 20282—2006 信息安全技术 信息系统安全工程管理要求
[6] GB/T 22239—2008 信息安全技术 信息系统安全等级保护基本要求
[7] GB/T 22240—2008 信息安全技术 信息系统安全等级保护定级指南
[8] GB/T 25068.1—2012 信息技术 安全技术 IT 网络安全 第 1 部分:网络安全管理
[9] GB/T 25068.2—2012 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
[10] GB/T 25068.3—2010 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
[11] GB/T 25068.4—2010 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
[12] 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
[13] GB/T 28456—2012 IPSec 协议应用测试规范
[14] GB/T 29240—2012 信息安全技术 终端计算机系统通用安全技术要求与测试评价方法
[15] 商用密码产品使用管理规定(国家密码管理局,2007 年 5 月)