国家电子政务外网标准

GW0201—2011

国家电子政务外网 IPSec VPN 安全接入技术要求与实施指南

Technical Requirements and Implementation Guide for IPSec VPN Securing Access of National E-Government Network

2011－11-1 发布　　2011－11－1 实施

国家电子政务外网管理中心

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 IPSec VPN 整体框架和基本原则 4
4.1 政务外网整体框架 4
4.2 政务外网 IPSec VPN 整体框架 7
4.3 基本原则 9
5 IPSec VPN 技术要求 11
5.1 IPSec VPN 网关技术要求 11
5.2 IPSec VPN 客户端技术要求 12
5.3 IPSec VPN 设备管理要求 12
5.4 IPSec VPN 证书管理要求 13
5.5 IPSec VPN 设备准入测试要求 14
5.6 IPSec VPN 等级保护合规性要求 14
6 IPSec VPN 建设实施 15
6.1 需求分析阶段 16
6.2 详细设计阶段 17
6.3 配置实施阶段 18
6.4 测试与备案阶段 19
7 IPSec VPN 接入过程管理 19
7.1 接入与业务开通 19
7.2 业务变更 20
7.3 运行管理 21
7.4 业务撤销 21
8 典型应用场景 22
8.1 不具备专线条件的政务部门接入到政务外网 23
8.2 移动办公用户接入政务外网 24
8.3 某级政务部门 IPSec VPN 网关级联应用 24
8.4 接入数据交换服务区 25

附录 A：负载均衡技术要求 27

附录 B：IPSec VPN 与 MPLS VPN 对接方式 28

附录 C：IPSec VPN 客户端使用环境说明 29

前　言

为指导各地在电子政务外网建设过程中正确合理地部署 IPSec VPN 设备，根据我国有关法律、法规和技术规范，落实国家电子政务外网（以下简称“政务外网”）建设对 IPSec VPN 安全接入的技术要求，并结合政务外网建设实际的应用需求及产品部署经验编制本指南。

本指南由国家电子政务外网管理中心提出并归口。

本指南起草单位：国家电子政务外网管理中心、中安网脉（北京）技术股份有限公司、华为技术有限公司、网神信息技术（北京）股份有限公司、迈普通信技术股份有限公司、北京天融信科技有限公司。

本指南主要起草人：周民、邵国安、罗海宁、吕品、林惠民、朱圣波、曹晖、王旭、张锐卿。

引　言

为了满足中央、省（自治区、直辖市）、地（市）、县各级政务部门使用 IPSec VPN 技术实现安全接入政务外网的需求，特编制本指南用以规范各级政务部门 IPSec VPN 技术体系的建设，保证各级政务部门业务应用的顺利开展。本指南包括 IPSec VPN 系统整体框架、基本原则、技术要求、建设实施、过程管理和典型应用场景等主要内容，规范了 IPSec VPN 技术实施的核心内容和技术要点，适用于指导各级政务部门进行 IPSec VPN 安全接入体系的规划设计、设备选型、建设实施、运行维护和管理等工作。

IPSec VPN 安全接入技术要求与实施指南

1 范围

本指南适用于国家电子政务外网 IPSec VPN 安全接入体系规划设计、设备选型、建设实施、运行维护和管理。为政务外网各级建设运维单位、各级政务外网接入单位提供应用指导和参考。

2 规范性引用文件

下列文件中的条款通过本指南的引用而成为本指南的条款。凡是注明日期的引用文件，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指南。凡是不注明日期的引用文件，其最新版本适用于本指南。

中共中央办公厅、国务院办公厅关于转发《国家信息化领导小组关于我国电子政务建设指导意见》的通知（中办发[2002]17 号）

《国家信息化领导小组关于加强信息安全保障工作的意见》（中办发[2003]27 号）

中共中央办公厅、国务院办公厅关于转发《国家信息化领导小组关于推进国家电子政务网络建设的意见》的通知（中办发[2006]18 号）

国务院 273 号令《商用密码管理条例》（1999 年 10 月）

国家发改委、财政部《关于推进国家电子政务外网建设工作的通知》（发改高技[2009]988 号）

关于印发《国家电子政务总体框架》的通知（国信[2006]2 号）

关于印发《电子政务保密管理指南》的通知（国保发[2007]5 号）

关于印发《信息安全等级保护管理办法》的通知（公通字 [2007] 43 号，公安部、国家保密局、国家密码管理局、国务院信息化工作办公室联合发布）

国家密码管理局《IPSec VPN 技术规范》（2008 年 1 月）

《计算机信息系统安全保护等级划分准则》（GB 17859-1999）

《信息安全技术 网络基础安全技术要求》（GB/T 20270-2006）

《信息安全技术 操作系统安全技术要求》（GB/T 20272-2006）

《信息安全技术 信息系统通用安全技术要求》（GB/T 20271-2006）

《信息安全技术 终端计算机系统安全等级技术要求》（GA/T 671-2006）

《信息安全技术 信息系统安全管理要求》（GB/T 20269-2006）

《信息安全技术 信息系统安全工程管理要求》（GB/T 20282-2006）

《信息系统安全等级保护基本要求》（GB/T 22239-2008）

《信息系统安全等级保护定级指南》（GB/T 22240-2008）

3 术语和定义

下列术语和定义适用于本指南。

3.1

国家电子政务外网

国家电子政务外网，横向连接各级党委、人大、政府、政协、法院和检察院等政务部门，纵向覆盖中央、省、地（市）、县，为部门业务应用提供网络承载服务，支持业务网络的互联互通，支持跨地区、跨部门的业务应用、信息共享和业务协同，满足各级政务部门社会管理、公共服务等方面的需要。政务外网是政务部门的业务专网，主要运行政务部门面向社会的专业性服务业务和不需在内网上

运行的业务，通过安全防护措施实现与互联网逻辑隔离。包括中央级政务外网和地方政务外网，二者均由相应的广域骨干网和城域网构成。中央广域骨干网连接 31 个省、自治区、直辖市和新疆生产建设兵团的省级广域骨干网。地方政务外网主要包括联通省、地（市）、县的广域骨干网、相关城市城域网及其部门接入网。

3.2

虚拟专用网络 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。它是一组封闭的网络网段，即使与开放系统或其它 VPN 共享同一主干网络，其通信也是保持分离的。所谓“虚拟”指网络连接特性是逻辑的而不是物理的。在一个虚拟网内，所有用户共享相同的安全策略、优先级服务和管理策略。VPN 技术可用于网关与网关之间的连接、网关与端点之间的连接、端点与端点之间的连接。

3.3

基于 IP 安全协议的虚拟专用网络 IP Security VPN（IPSec VPN）

IPSec VPN 指采用 IPSec 协议来实现远程接入的一种 VPN 技术，IPSec 是互联网工程任务组（IETF, Internet Engineer Task Force）安全标准协议，是一个范围广泛、开放的虚拟专用网安全协议，它提供所有在网络层上的数据保护，为接入的两端提供透明的安全通信，能够支撑最为全面的业务应用。

3.4

IPSec VPN 服务网关

部署在政务外网城域网与互联网的边界，为接入单位提供接入服务的IPSec VPN网关设备。

3.5

IPSec VPN 接入网关

部署在政务外网接入单位局域网边界，向IPSec VPN服务网关发起连接的IPSec VPN网关设备。

3.6

基于多协议标签交换技术的虚拟专用网 Multi-Protocol Label Switching VPN（MPLS VPN）

MPLS VPN 是一种基于 MPLS（Multiprotocol Label Switching，多协议标记交换）技术的 IP 虚拟专用网络，是在网络路由和交换设备上应用 MPLS 技术，简化核心路由器的路由选择方式，利用结合传统路由技术的标记交换实现的 IP 虚拟专用网络，可用来构造宽带的 Intranet、Extranet，满足多种灵活的业务需求。

3.7

运营商边缘设备 Provider Edge（PE)

MPLS 骨干网边缘路由器，它相当于标签边缘路由器（LER），负责 VPN 业务接入，处理 VPN 路由。PE 路由器连接 CE 路由器和 P 路由器，是最重要的网络节点。用户的流量通过 CE 路由器流入用户网络，或者通过 P 路由器流到 MPLS 骨干网。

3.8

用户端边缘设备 Customer Edge（CE）

MPLS 网络在用户边缘的接入设备，CE 路由器通过连接一个或多个 PE 路由器，为用户端网络提供接入服务。CE 路由器通常是一台 IP 路由器，它与连接的 PE 路由器建立邻接关系，不参与 VPN 路由。

3.9

VPN 路由转发 VPN Routing Forwarding（VRF）

VRF，也称为 VPN 路由和转发表。在 PE 路由器上，为每个 PE 直接相连的 VPN 生成一份路由和转发表。每个 VRF 仅存有所隶属 VPN 的路由信息。

3.10

基于安全套接层协议的虚拟专用网 Security Socket Layer VPN（SSL VPN）

SSL VPN 指采用 SSL 协议来实现远程接入的一种 VPN 技术。SSL 协议是基于 WEB 应用的安全协

议，它包括：服务器认证、客户认证（可选）、SSL 链路上的数据完整性和 SSL 链路上的数据保密性。

3.11

点到点协议 Point to Point Protocol（PPP）

PPP协议是TCP/IP网络协议集合中的一个子协议，主要用来创建电话线路以及ISDN拨号接入ISP的连接，具有多种身份验证方法、数据压缩和加密以及通知IP地址等功能。

3.12

点对点隧道协议 Point-to-Point Tunneling Protocol（PPTP）

PPTP协议是在PPP协议的基础上开发的一种点对点隧道协议，支持多协议虚拟专用网（VPN），可以通过密码身份验证协议（PAP）、可扩展身份验证协议（EAP）等方法使远程用户通过拨入ISP直接连接Internet或通过其他公众网络访问企业网部网络。

3.13

二层隧道协议 Layer 2 Tunneling Protoco（L2TP）

L2TP 是一种支持 VPN 的隧道协议。它本身不提供任何的加密或保密功能，需要通过其它加密协议保证其隧道内数据的机密性、完整性。

3.14

虚拟专用拨号网 Virtual Private Dial-up Networks（VPDN）

是电信类运营商基于拨号用户的虚拟专用拨号网业务，利用 L2TP、IP 网络的承载功能结合相应的认证和授权机制建立起来的虚拟专用网，一般不具有加密的安全功能。

3.15

3G 拨号接入

3G（3rd Generation）是指第三代数字通信技术，本指南特指利用 3G 通信技术拨号，通过运营商构建 3G 专网接入到用户网络中，并非是用 3G 拨号终端接入到互联网后再访问用户网络。

3.16

国密 SM1 算法 SM1 Cryptographic Algorithm

国密 SM1 算法是由国家密码管理局编制的一种商用密码分组标准对称算法。该算法分组长度和密钥长度都为 128 比特，算法安全保密强度及相关软硬件实现性能与 AES 相当，该算法不公开，仅以 IP 核的形式存在于芯片中。采用该算法的系列芯片、智能 IC 卡、智能密码钥匙、加密卡、加密机等安全产品，目前广泛应用于我国电子政务、电子商务及国民经济的各个应用领域。

3.17

安全哈希算法 Secure Hash Algorithm（SHA）

SHA 算法由美国国家安全局（NSA）所设计，美国国家标准与技术研究院（NIST）发布。SHA 算法可划分为 SHA-1、SHA-224、SHA-256、SHA-384 和 SHA-512（后四者通常并称 SHA2），可将一个最大 2^64 位（2305843009213693952 字节）信息，转换成一串 160 位（20 字节）的散列值（摘要信息），是目前应用最广泛的 HASH 算法。

3.18

安全联盟 Security Association（SA）

安全联盟是两个通信实体经协商建立起来的一种协定，它描述了实体如何利用安全服务来进行安全的通信。安全联盟包括了执行各种网络安全服务所需要的所有信息，例如 IP 层服务（如头认证和载荷封装）、传输层和应用层服务或者协商通信的自我保护。

3.19

因特网密钥交换协议 Internet Key Exchange（IKE）

因特网密钥交换协议（IKE）是一份符合因特网协议安全（IPSec）标准的协议。它常用来确保虚拟专用网络 VPN 与远端网络或者宿主机进行交流时的安全。

3.20

失效对端检测 Dead Peer Detection（DPD）

DPD 是一种基于数据流的检测方法。通过发送 DPD 检测报文，检测 IPSec 连接状态。如果检测到 IPSec 连接中断，则启用备用的 IPSec 隧道。

3.21

数字证书 Digital Certificate

由证书认证机构签名的，包含公开密钥拥有者的信息、公开密钥、签发者信息、有效期以及一些扩展信息的数字文件。

3.22

数字证书认证中心 Certificate Authority（CA）

数字证书认证中心是提供网络身份证的权威、可信、公正的第三方机构，专门负责发放、管理参与网上活动的实体所需的身份数字证明。

3.23

数字证书注册审批机构 Registration Authority（RA）

RA 系统是 CA 的证书发放、管理的延伸，负责证书申请者的信息录入、审核以及证书发放等工作，并对发放的证书完成相应的管理功能。

3.24

数字证书注册审批受理点 RA Terminal

RA 的下属机构，直接面向最终证书用户，进行用户身份审核、数字证书的受理和发放工作。

3.25

数字证书可辨识名 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，一般使用 X.500 标准，在 Internet 中保证唯一，一般具体指主体的通用名、组织单位、组织和国家信息。

3.26

轻量级目录访问协议 Light Directory Access Protocol（LDAP）

轻量级目录访问协议是跨平台的、标准的协议，用于规范和优化访问目录服务的一个标准，通常作为一个集中的地址本使用，实现了指定数据结构的特殊数据库，极大优化了查询性能。

3.27

安全外壳协议 Secure Shell（SSH）

是由 IETF 的网络工作小组（Network Working Group）所制定的，建立在应用层和传输层基础上的安全协议。SSH 是目前较可靠、较普遍使用的，为远程登录会话和其它网络服务提供加密传输的安全协议。

3.28

网络地址转换 Network Address Translation（NAT）

一种将私有（保留）地址转化为合法 IP 地址的转换技术，它被广泛应用于各种类型 Internet 接入方式和各种类型的网络中。NAT 不仅解决了 IP 地址不足的问题，而且还能够有效地避免来自网络外部的攻击，隐藏并保护网络内部的计算机。

4 IPSec VPN 整体框架和基本原则

4.1 政务外网整体框架

4.1.1 网络框架

政务外网按照管理层次划分，可分为中央级、省级、地市级、县级政务外网。网络框架如图 4-1 所示。

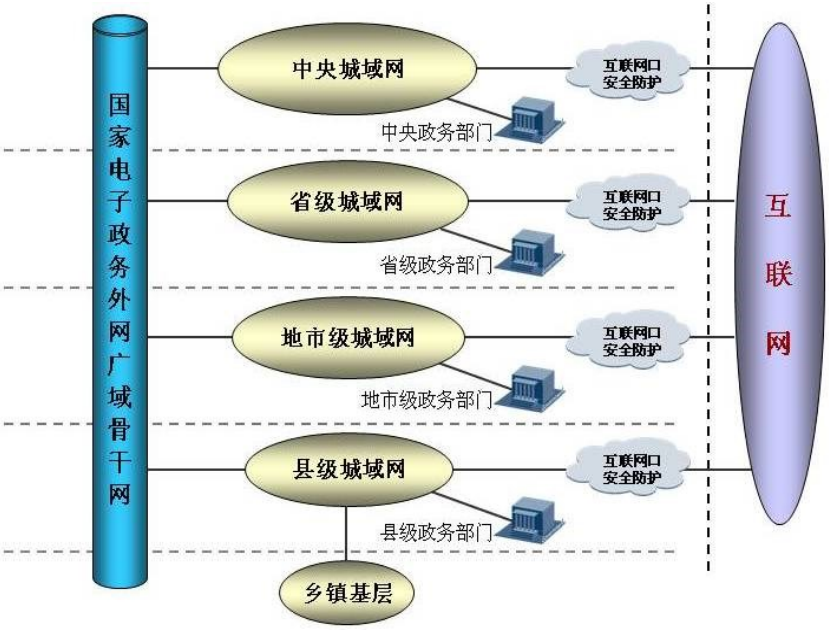

图 4-1 政务外网网络框架

4.1.2 业务网络模型

根据政务外网所承载的业务和系统服务的类型的不同，在逻辑上，政务外网划分为专用网络区、公用网络区和互联网接入区三个功能域，分别提供专用 VPN 业务，政务外网互联互通业务和互联网业务。如图 4-2 所示。

a） 专用网络区：是依托国家政务外网基础设施，为有特定需求的部门或业务设置的VPN网络区域，实现不同部门或不同业务之间的相互隔离，VPN业务主要为少数中央部门的敏感数据传输提供安全通道。中央级政务外网采用MPLS VPN技术将敏感业务数据与其它数据安全隔离，用于满足横向、纵向及“自上而下”或“自下而上”的业务需求，为中央政务部门与各省（自治区、直辖市）、地（市）、县相关部门的互联互通提供安全通道。该区域主要采用私有地址，在骨干网上采取标签进行交换。

b） 公用网络区：即采用国家政务外网注册地址（59地址）的网络区域，是国家政务外网的主干道，实现各部门、各地区互联互通，为跨地区、跨部门的业务应用提供支撑平台；国家政务外网承载网仅路由国家政务外网注册地址。

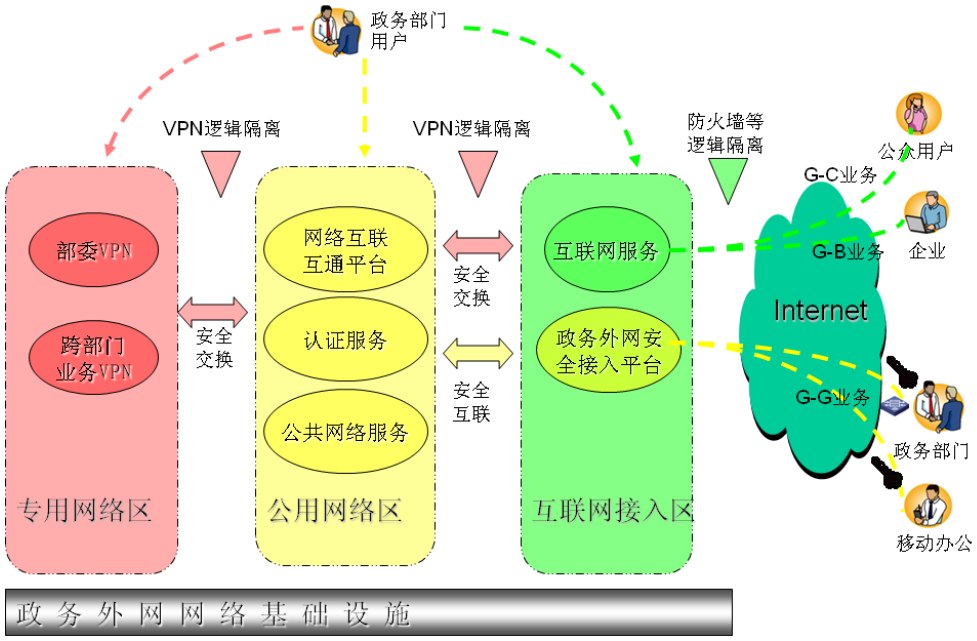

图 4-2 政务外网逻辑区域划分图

c） 互联网接入区：是各级政务部门通过逻辑隔离安全接入互联网的网络区域，满足各级政务部门利用互联网的需要。同时也是移动办公的公务人员通过数字证书认证，安全接入政务外网的途径。在互联网接入区，采取了综合的安全防护措施，采用防火墙系统、入侵防御系统和网络防病毒系统，对互联网接入业务提供一定的安全防护。中央和地方分级出口，中央级政务外网采取BGP协议与主要运营商进行互联，为中央部门单位提供互联网业务服务，各地政务外网自行设置出口，采取NAT技术，通过静态路由连接本地互联网。中央级政务外网主干网不路由地方互联网业务。

4.1.3 政务外网 VPN 建设整体需求

作为承载各级政务部门各种业务的公用网络，政务外网全网采用VPN技术保证不同部门不同业务之间的安全性与隔离性。如图4-3所示。

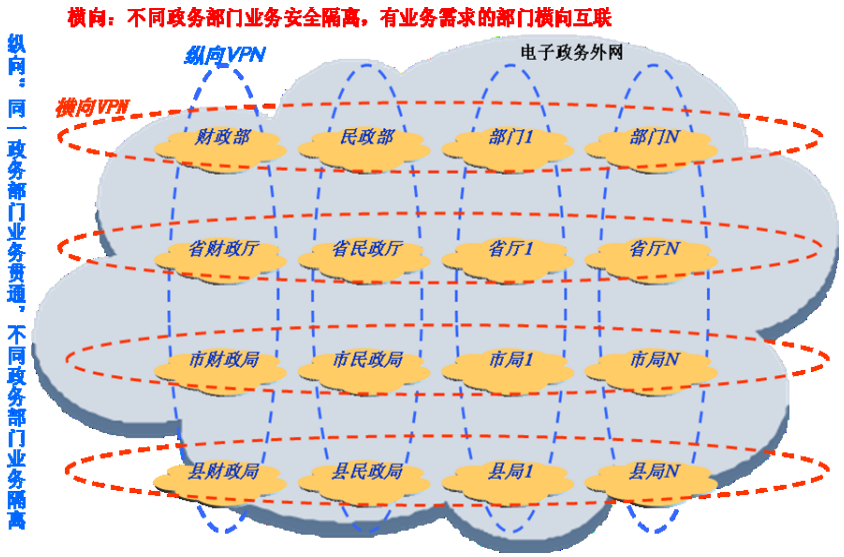

图 4-3 政务外网 VPN 隔离示意图

在政务外网骨干网上，通过MPLS VPN技术实现如下功能：

a） 纵向实现同一政务部门的业务贯通以及不同政务部门业务的安全隔离。

b） 横向实现不同政务部门业务的安全隔离以及有业务需求的部门间的横向互联。

对于不具备专线条件的部门或用户接入采用IPSec VPN技术实现如下功能：

a） 部门网络就近接入到当地政务外网建设运维单位安全接入平台，纵向实现业务贯通，横向实现部门间互联。

b） 移动办公人员属地化接入到所属地安全接入平台，实现远程访问授权资源。

4.2 政务外网 IPSec VPN 整体框架

4.2.1 政务外网 IPSec VPN 接入需求

各级政务部门可以通过互联网 IPSec VPN 接入政务外网，尤其是不具备专线接入政务外网条件的政务部门以及一些偏远地区，以保证各项业务的贯通，同时实现不同部门不同业务的安全隔离。

另一方面，众多政务部门均有人员出差或移动办公的需求，部分政务部门需要相应群体的公众或企业机构上报相关数据，这就要求政务外网为移动办公用户提供 IPSec VPN 接入服务。

政务外网 IPSec VPN 体系建设主要满足如下需求：

a） 纵向互通：各下级政务部门通过IPSec VPN与其所属的上级政务部门互通；

b） 横向互通：各政务部门通过IPSec VPN与有业务需求的其它政务部门互通；

c） 移动办公接入：各政务部门移动办公用户和上报数据的单位、公众用户通过IPSec VPN系统安全接入政务外网；

d） 安全隔离：各级政务部门及移动办公用户的互联网IPSec VPN接入体系与政务外网骨干网上的MPLS VPN体系安全对接，一一映射，以保证本部门的数据通过互联网IPSec VPN接入政务外网之后，只能按照需求进入该部门所属的MPLS VPN通道，保证各部门业务安全隔离。

4.2.2 政务外网 IPSec VPN 建设体系

不具备专线条件接入政务外网的各级政务部门、移动办公用户以及上报数据的单位、公众用户通过IPSec VPN 安全接入平台接入政务外网，构成了政务外网 IPSec VPN 建设体系，如图 4-4 所示。

4.2.2.1 安全接入平台建设

安全接入平台由 IPSec VPN 网关（含 SSL 功能）、基于 LDAP 或 RADIUS 的认证服务器、VPN 管理服务器等设备或软件构建而成，应具备对接入用户（含数字证书 KEY）和接入网关统一的身份认证与权限管理，并按接入网关类型和访问业务需求来配置 VPN 策略的功能。多台 IPSec VPN 设备可以与 IPSec VPN 负载均衡设备搭建形成 VPN 网关集群，通过对集群网关的负载均衡管理，设置负载策略灵活分配隧道，满足大量用户接入的高性能、高可靠性要求。同时，应增加防火墙、入侵检测、病毒防护、安全审计等措施，用于满足基本防护、安全监测与行为审计等方面的安全需求。安全接入与交换平台设置在政务外网互联网出入口和政务外网之间的单独区域内，采取严格的安全策略，保证通过互联网入口进入政务外网的信息和行为安全可控。中央、省、地市政务外网中心分别建设，最终形成全国全网统一管理的安全接入综合平台，实现全网政务用户移动办公便捷接入、各级机构局域网快速接入、各类业务数据安全高效交换等整体安全服务目标。

4.2.2.2 接入体系建设

政务外网的 IPSec VPN 接入体系建设分为如下几个方面：

a） 政务部门接入政务外网：对于不具备专线接入条件的各级政务部门使用IPSec VPN接入政务外网，应采用IPSec VPN网关对网关部署模式；

b） 移动办公用户接入政务外网：中央、省、地市、县等各级政务部门的出差及移动办公人员通过IPSec VPN接入本级政务外网，可采用IPSec VPN客户端对网关模式；

c） 上报数据的单位、公众用户接入政务外网：各单位、公众用户接入到对口部门归属地的IPSec VPN服务网关进行数据上报，可采用IPSec VPN客户端对网关模式。

政务外网 IPSec VPN 体系整体框架如图 4-5 所示。

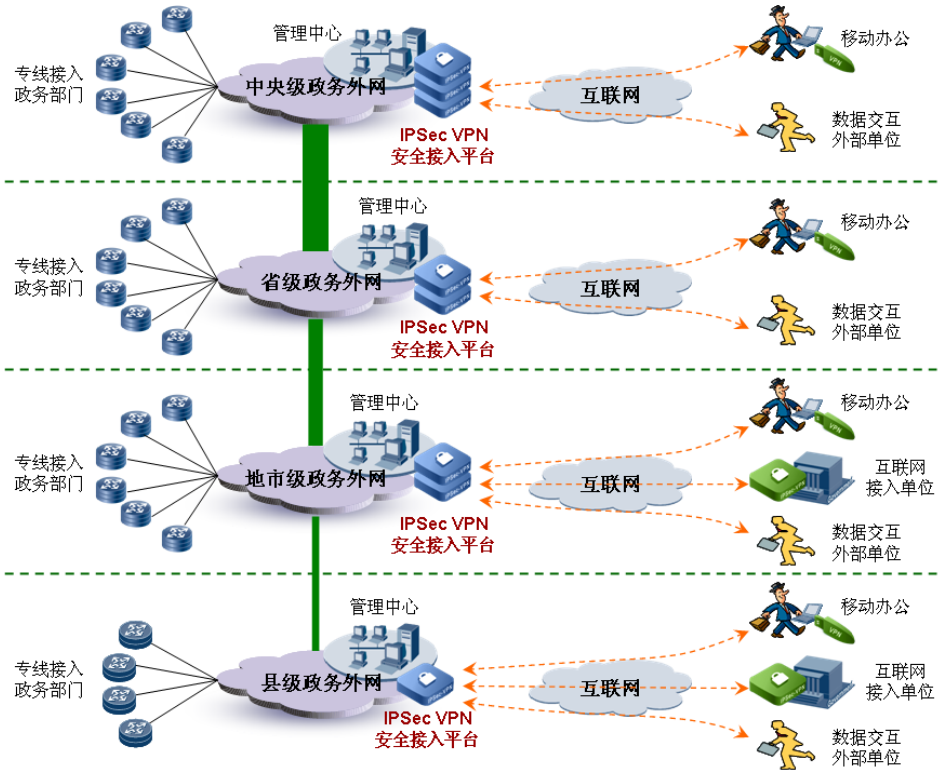

图 4-4 政务外网 IPSec VPN 建设体系示意图

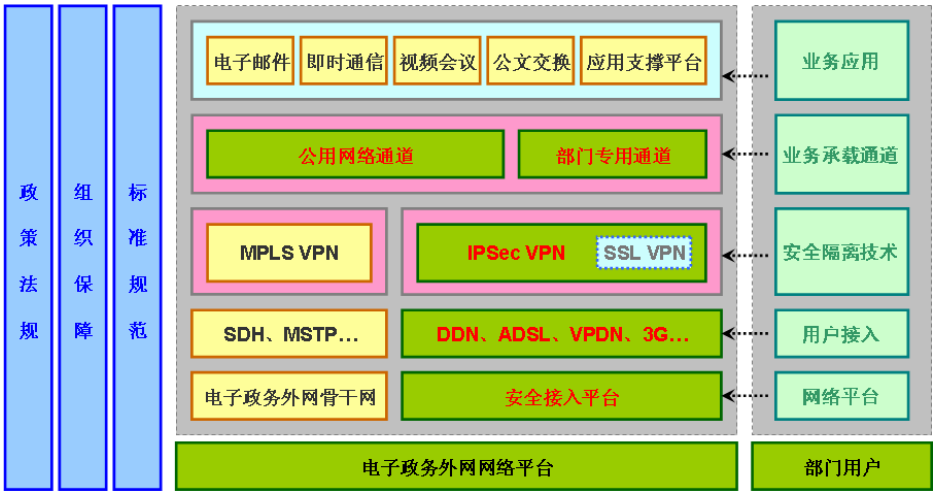

图 4-5 政务外网 IPSec VPN 体系整体框架示意图

4.2.3 政务外网 IPSec VPN 技术规范体系构成

政务外网 IPSec VPN 技术规范体系主要由基本原则、技术要求和实施指南构成。基本原则是实施指南的基础前提，实施指南中的建设实施和接入过程管理是从 IPSec VPN 建设运行管理到开展业务不同角度的指导性说明。各级政务部门在建设政务外网 IPSec VPN 安全接入体系过程中，应参考政务外网 IPSec VPN 技术规范框架（图 4-6），从建设、运行、管理各个环节对应遵照规范开展工作。

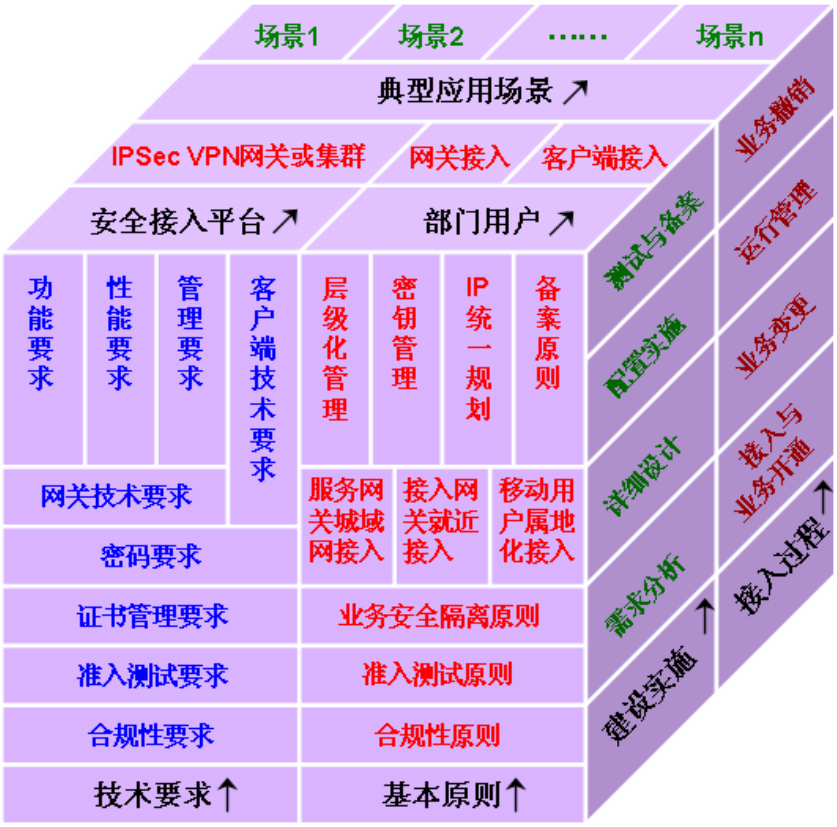

图 4-6 政务外网 IPSec VPN 技术规范框架

4.3 基本原则

对于不具备专线条件接入政务外网的各级政务部门和移动办公用户，可以采用互联网等接入方式作为政务外网的补充接入方式，组网原则遵循优先使用 IPSec VPN 技术体系组网，保证互联网等接入业务的安全性，实现政务外网的完整性覆盖。

4.3.1 部署原则

4.3.1.1 服务网关城域网接入原则

IPSec VPN 服务网关应部署在所属的政务外网城域网中互联网出口处，不能部署在政务外网广域骨干网。

4.3.1.2 接入网关就近接入原则

通过互联网 IPSec VPN 接入政务外网的政务部门，其出口部署的 IPSec VPN 接入网关就近接入到其所属的本级政务外网服务网关上。如本级政务外网无服务网关，可申请接入到上级政务外网服务网关。

4.3.1.3 移动办公用户属地化接入原则

政务外网 IPSec VPN 将为移动办公用户提供安全便捷的接入方案，满足用户出差、移动办公时安全访问政务外网的需求，接入时应当遵循属地化接入原则，分为两种情况：

a） 各级政务部门移动办公的接入情况。此类用户需遵循属地化接入原则，从归属地IPSec VPN服务网关接入；如北京政务部门的移动办公用户出差办公，均通过互联网连接到北京政务外网的IPSec VPN服务网关，接入到北京市政务外网。

b） 外部单位用户与相关政务部门有数据交互的接入情况。此类用户接入到对口部门归属地的IPSec VPN服务网关进行数据交互，如果该对口部门属于地市级，则此类用户从该地市级IPSec VPN服务网关接入。

4.3.1.4 IP 地址统一规划原则

IPSec VPN 接入体系的 IP 地址主要涉及网关地址池及设备管理地址（不包括互联网接入地址），应

遵循国家政务外网的统一规划管理，各级政务外网建设运维单位应严格按照地址规划要求统一分配使用。

4.3.1.5 业务安全隔离原则

不同政务部门不同业务的访问需遵循安全加密隔离原则，政务外网应与互联网逻辑隔离。

在政务外网的广域网，启用 MPLS VPN 隔离各部门及各业务，MPLS VPN 终结在 PE 上。在互联网通过 IPSec VPN 隧道隔离，各部门业务通过独立的 IPSec VPN 隧道连接到政务外网。应在 IPSec VPN 网关和 PE 之间设置相关的策略或启用相关的功能，达到各部门的访问流量端到端隔离的效果。不同政务部门业务流量在通过 IPSec VPN 网关及 PE 设备之后，只能进入本部门所在政务外网骨干网上的 MPLS VPN 通道之中，或者根据需要进入相应的信息共享 MPLS VPN 通道，而不会流向其它部门的私有 MPLS VPN 通道中，以保证不同部门不同业务的安全隔离。如图 4-7 所示。

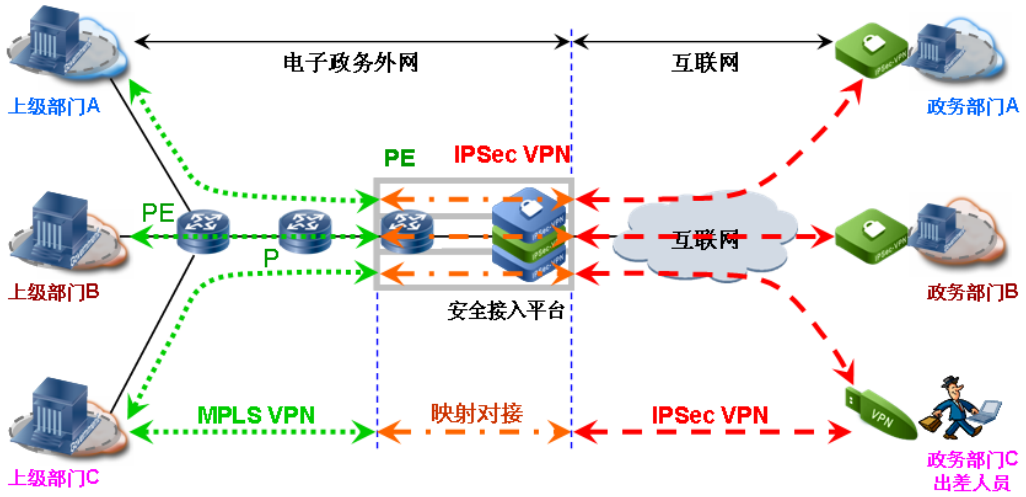

图 4-7 业务安全隔离示意图

4. 3. 2 管理原则

4.3.2.1 遵循国家密码管理原则

严格遵循《商用密码管理条例》、国家密码管理局《商用密码产品使用管理规定》、《IPSec VPN 技术规范》以及相关密钥管理制度。

4.3.2.2 等级保护合规性原则

根据不同政务部门业务系统的不同等级，在遵循国家信息安全等级保护相关制度的前提下，IPSec VPN 体系的部署实施应满足本指南“5.6 IPSec VPN 等级保护合规性要求”。

4.3.2.3 层级化管理原则

IPSec VPN 体系的管理遵循集中指导、层级化管理原则。

建立全局的政务外网安全管理体系，包括中央、省、地市、县四级管理体系，各级政务外网建设运维单位分别负责该级 IPSec VPN 体系的管理，并按照层级化管理方式层层负责，也可以根据实际情况集中统一管理，如省级或地市级可以集中统一管理本省或本市的各级 IPSec VPN 体系，确保政务外网 IPSec VPN 技术体系的规范统一。

4.3.2.4 准入测试原则

政务外网 IPSec VPN 技术体系相关产品在入网前应通过由国家电子政务外网管理中心统一组织的准入测试，技术要求参见本指南 “5.5 IPSec VPN 设备准入测试要求”。

4.3.2.5 备案原则

业务单位成功申请并接入 IPSec VPN 体系之后，本级政务外网建设运维单位应登记备案并上报上级建设运维单位。

5 IPSec VPN 技术要求

5.1 IPSec VPN 网关技术要求

5.1.1 功能要求

a） 支持VPN类型：采用IPSec VPN，支持SSL VPN功能，支持L2TP 、PPTP等隧道协议。

b） 产品可靠性：支持双机热备、集群部署、备份与切换等技术保证不间断的网络应用；支持隧道断线自动重建；具备单机双电源冗余（A类和B类IPSec VPN网关至少应满足，其它类可选），减少电源故障造成的业务中断。

c） 安全性：基于标准IPSec协议开发，并严格遵循国家密码管理局制定的《IPSec VPN技术规范》。支持政务外网CA的X.509证书格式；支持对称加密算法，如SM1等；支持非对称算法，如SM2等；支持摘要算法，如SM3、SHA1等；支持隧道模式和传输模式；采用自动密钥协商机制，硬件设备间互联校验采取证书或预共享密钥方式。IPSec VPN网关和VPN客户端支持NAT穿越功能、支持DPD功能。

d） 互通兼容性：支持MPLS VPN多业域环境的对接；与通过国家电子政务外网管理中心准入测试的其它IPSec VPN设备能够互联互通；支持NAT穿越，采用标准协议，能够双向穿透NAT设备，具有良好的兼容性。

e） 统一智能管理：支持对IPSec VPN设备的集中监控和管理，支持Syslog格式日志输出，提供安全管理平台采集与配置管理接口；支持外部认证用户基于角色的授权，支持对外部认证用户分组授权。

f） 性能管理：支持有效监视IPSec VPN设备的运行性能，提供丰富的性能管理功能。包括支持对IPSec VPN网关CPU利用率等关键指标的监视；集中监控隧道状态、设备状态和移动办公用户状态；支持对用户关心的性能参数设定阈值，当超过设定的阈值后，系统将会发送性能告警，使网络管理人员及时发现和消除网络中的隐患。

g） 证书认证：支持国家电子政务外网数字证书认证；支持X.509协议；支持自动下载CRL；支持在线或离线验证证书。

h） 资质要求：具备国家密码管理局颁发的《商用密码生产定点单位证书》、《商用密码销售许可证》、《商用密码产品型号证书》。

5.1.2 性能要求

5.1.2.1 A 类 IPSec VPN 网关指标要求

支持总体功能要求的同时，A 类 IPSec VPN 网关可用于省级，属于高配，应支持以下要求：支持 4 个千兆光口、4 个千兆电口。主要性能指标如下：

a） IPsec VPN隧道数≥5000个；

b） SM1加密性能≥200Mbps；

c） 最大并发连接数≥200万；

d） 认证时间小于1s；

e） 隧道建立时间小于1s；

f） 吞吐量≥2Gbps；

g） 延时小于50ms。

5.1.2.2 B 类 IPSec VPN 网关指标要求

支持总体功能要求的同时，B 类 IPSec VPN 网关可用于省级，属于低配，还可用于地市级，属于高配，应支持以下要求：支持不少于 6 个千兆电口。主要性能指标如下：

a） IPsec VPN隧道数≥3500个；

b） SM1加密性能≥100Mbps；

c） 最大并发连接数≥100万；

d） 认证时间小于1s；
e） 隧道建立时间小于1s；
f） 吞吐量≥800Mbps；
g） 延时小于50ms。

5.1.2.3 C 类 IPSec VPN 网关指标要求

支持总体功能要求的同时，C 类 IPSec VPN 网关可用于地市级，属于低配，还可用于县级，属于高配，应支持以下要求：支持不少于 4 个千兆电口。主要性能指标如下：

a） IPsec VPN隧道数≥1000个；
b） SM1加密性能≥50Mbps；
c） 最大并发连接数≥50万；
d） 认证时间小于1s；
e） 隧道建立时间小于1s；
f） 吞吐量≥200Mbps；
g） 延时小于50ms。

5.1.2.4 D 类 IPSec VPN 网关指标要求

支持总体功能要求的同时，D 类 IPSec VPN 网关可用于县级，属于低配，应支持以下要求：支持不少于 4 个百兆电口。主要性能指标如下：

a） IPsec VPN隧道数≥600个；
b） SM1加密性能≥30Mbps；
c） 最大并发连接数≥10万；
d） 认证时间小于1s；
e） 隧道建立时间小于1s；
f） 吞吐量≥100Mbps；
g） 延时小于50ms。

5.2 IPSec VPN 客户端技术要求

5.2.1 IPSec VPN 客户端软件平台要求

IPSec VPN 客户端软件与证书应用及 Key 驱动的接口应遵照国家密码管理局规范、政务外网对相关接口的统一要求，支持从 USB Key 中获取证书并利用证书实现与 IPSec VPN 网关的连接。客户端软件应支持常见操作系统，如：Windows 2000、Windows XP、Windows Vista、Windows7。客户端软件应支持自动生成配置文件，仅需要输入少量关键性参数即可完成复杂的配置，应支持 IPSec VPN 穿越 NAT 的技术，实现局域网中访问 IPSec VPN 服务网关的需求，客户端网络环境应保证稳定，要求丢包率低、满足带宽要求（不低于 128Kbps）。开放标准协议端口，如 UDP500、UDP4500 等。

5.2.2 IPSec VPN 客户端硬件要求

IPSec VPN 客户端硬件应按照国家电子政务外网 CA 统一要求选择，常见的硬件为 USB Key，也可选择桌面密码机、PCI 密码卡等。客户端硬件应支持 SM1 算法。

5.2.3 认证方式要求

IPSec VPN 客户端支持的 IPSec VPN 网关接入认证方式：

a） 支持基于数字证书的认证接入；
b） 支持基于数字证书和口令的双因子认证接入；
c） 支持预共享密钥认证接入。

5.2.4 互联网应用隔离要求

IPSec VPN 客户端接入政务外网时，应与互联网应用隔离。IPSec VPN 客户端在访问互联网应用时，应与政务外网隔离。

5.3 IPSec VPN 设备管理要求

5.3.1 密钥管理

5.3.1.1 设备密钥

设备密钥的产生应由 IPSec VPN 设备（包括 IPSec VPN 网关、IPSec VPN 客户端、USB Key、桌面密码机、PCI 密码卡等）自身产生或者由 CA 产生并导入设备。设备密钥应保存在非易失性存储装置中（如 IPSec VPN 网关、USB Key），其私钥应有安全保护措施。

设备密钥产生方式确定证书申请的二种模式：

自身产生模式：由 IPSec VPN 设备在本地生成 PKCS#10 文件，向 CA 申请证书，证书颁发后再通过离线方式导入设备。

CA 产生模式：由 CA 生成包含用户证书及私钥的 PKCS#12 文件，通过离线方式导入设备。

5.3.1.2 工作密钥

工作密钥由 IKE 第一阶段协商产生，需支持自动更新，更新应当不影响 IPSec 数据通信，更新时间应可配置。

根据国家密码管理局相关标准要求，更新时间不大于 24 小时。

5.3.1.3 会话密钥

会话密钥由 IKE 第二阶段协商产生，需支持自动更新，更新条件可以基于该密钥存在的时间，也可以基于用该密钥保护的数据量，更新参数应可配置。

根据国家密码管理局相关标准要求，更新时间不大于 1 小时。

5.3.2 设备管理

IPSec VPN 设备应提供安全措施，保证密码算法、密钥、关键数据的存储安全。除必需的通信接口和管理接口以外，不提供任何可供调试、跟踪的外部接口。内部的调试、检测接口应在产品定型后封闭。

IPSec VPN 设备遗失需要尽快反馈给相关的管理部门，争取在第一时间做相应的安全处理，吊销证书防止非法接入。

5.3.3 权限管理

IPSec VPN 设备应按照不同管理权限设置管理员、操作员角色。设备的安全策略配置、设备密钥的生成、导入、备份和恢复等操作应由管理员完成。

5.3.4 配置数据管理

IPSec VPN 设备的所有配置数据应保证其在设备中的完整性、可靠性。可在管理界面对配置数据进行配置和管理，管理员进入管理界面应通过身份认证。

5.3.5 日志管理

IPSec VPN 设备应提供日志功能，日志可被查看、导出。

日志内容包括：

a） 操作行为，包括登录认证、参数配置、策略配置、密钥管理等操作。

b） 安全事件，安全联盟的协商成功、协商失败、过期等事件。

c） 异常事件，解密失败、完整性校验失败等异常事件的统计。

5.4 IPSec VPN 证书管理要求

IPSec VPN 证书管理要求遵循国家电子政务外网管理中心认证办公室的相关规范。

设备证书主体信息和个人证书的主体信息遵循《证书认证机构（CA）命名空间规范》前提下，将单位信息和区域信息在证书 DN 中体现，以便 IPSec VPN 设备对应证书信息进行授权和控制。

设备证书从本地的政务外网 CA（RA）获取，如果本地没有应从上一级政务外网 CA（RA）或直接从国家政务外网 CA 获取。

网关的证书时限应超过网关的使用时限（建议不少于五年）。

IPSec VPN 证书管理流程如图 5-1 所示。

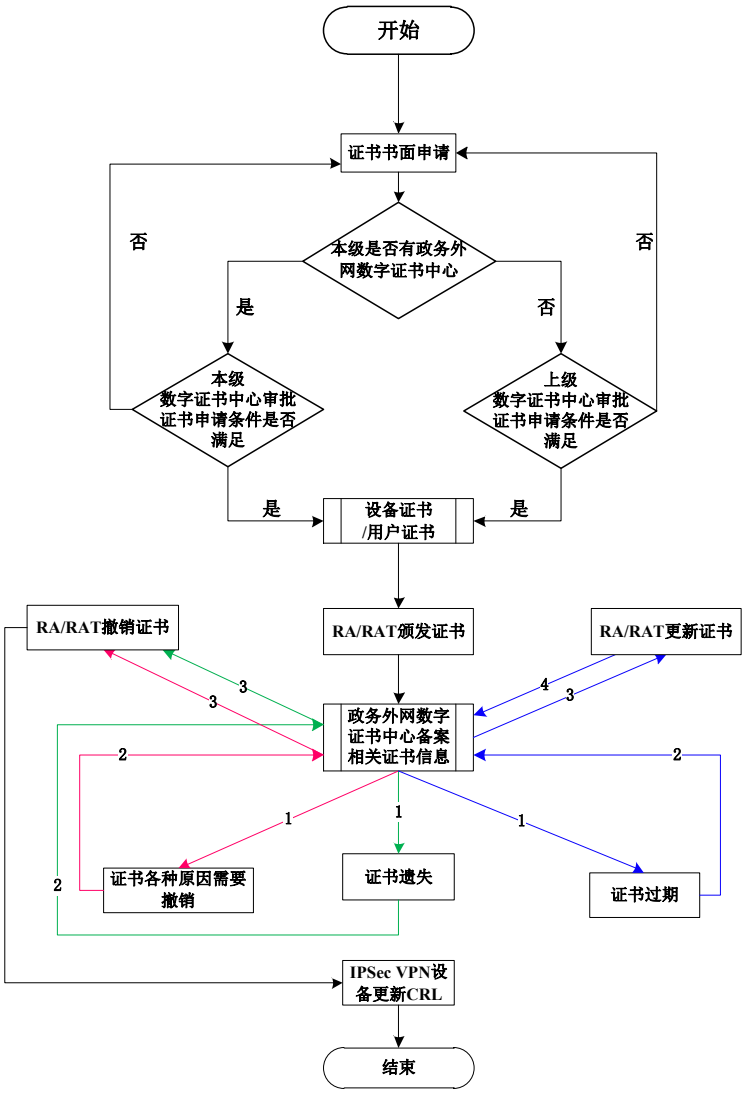

图 5-1 IPSec VPN 证书管理流程图

5.5 IPSec VPN 设备准入测试要求

IPSec VPN 设备及生产厂商应具备国家密码管理局颁发的相应资质，符合政务外网 IPSec VPN 设备技术要求，并通过国家电子政务外网管理中心的准入测试，达到 IPSec VPN 设备准入政务外网的基本条件。

准入测试要点如下：

a） 遵循国家密码管理局《IPSec VPN技术规范》，并应与国家电子政务外网管理中心认定的IPSec VPN基准产品互联互通。

b） IPSec VPN设备应支持政务外网MPLS多业务域的接入。

c） 应支持政务外网CA颁发的证书格式，可利用证书属性实现分域分组授权。

5.6 IPSec VPN 等级保护合规性要求

5.6.1 基本要求

基于 IPSec VPN 所承载已定级业务系统的最高安全保护等级，规范 IPSec VPN 设备等级保护基本要求和算法与密钥要求。

5.6.2 第二级要求

5.6.2.1 IPSec VPN 设备等级保护基本要求

a） IPSec VPN设备的业务处理能力具备冗余空间，满足业务高峰期及后期业务扩展需要；
b） 基于网段的粒度控制数据流，提供明确允许/拒绝访问的能力；
c） 基于用户和系统之间的允许访问规则，允许或拒绝用户对受控系统进行资源访问；
d） 对IPSec VPN设备运行状况、网络流量、用户行为等进行日志记录；
e） 对VPN的审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其它与审计相关的信息；
f） 应对网络设备的管理员登录地址进行限制；
g） 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；
h） 口令应符合以下条件：数字、字母、符号混排，无规律的方式；
i） 管理员用户口令的长度至少为8位；
j） 管理员用户口令至少每月度更换1次，更新的口令至少5次内不能重复；
k） 启用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；
l） 当对网络设备进行远程管理时，应采取必要措施，如SSH方式等，以防止鉴别信息在网络传输过程中被窃听。

5.6.2.2 IPSec VPN 设备算法与密钥要求

a） 第二级IPSec VPN设备宜使用国家密码管理局标准IKE协商机制。

IPSec VPN 算法与密钥要求：对称算法可采用 SM1 算法，非对称算法可采用 SM2 等算法，摘要算法建议使用 SHA1，建议启用完整性保护策略。

b） 网关必须使用证书方式，客户端可以使用预共享密钥方式。预共享密钥应符合以下条件：

1）数字、字母、符号混排，无规律的方式；

2）预共享密钥的长度至少为 8 位；

3）设备 IKE ID 信息，应包含区域信息、单位信息、部门信息、设备信息（或个人身份信息），建议以如下格式实现：设备信息（或个人信息）.部门信息.单位信息.区域信息。

5.6.3 第三级要求

5.6.3.1 IPSec VPN 设备等级保护基本要求

在满足第二级系统的要求之上，并符合以下要求。

a） 按照对业务服务的重要次序来指定带宽分配优先级别，保证在网络发生拥堵的时候优先保护重要要求。
b） 能够根据设备记录数据进行分析，并由第三方审计系统生成审计报表；
c） 应由内部人员或上级单位定期进行全面安全检查，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、安全管理制度的执行情况等。

5.6.3.2 IPSec VPN 设备算法与密钥要求

第三级 IPSec VPN 设备必须符合国密标准算法和密钥要求。

IPSec VPN 客户端，强制要求通过政务外网 CA 颁发的证书实现 IKE 协商，加密算法必须使用 SM1 算法，并结合口令认证。客户端启动 IPSec VPN 访问政务外网的同时，应不能访问互联网。

6 IPSec VPN 建设实施

国家电子政务外网 IPSec VPN 的建设，不仅要满足国家相关政策、法规的要求，还要考虑到接入单位所在地政务外网建设情况，立足实际需求，逐步完成实施。

IPSec VPN 的建设实施主要包括需求分析、详细设计、配置实施、测试与备案四个阶段。在每个阶段对政务外网建设运维单位和政务外网接入单位进行职责认定和划分，对整个建设实施过程进行总体把握和实时监控。

建设实施过程的流程图如图 6-1 所示。

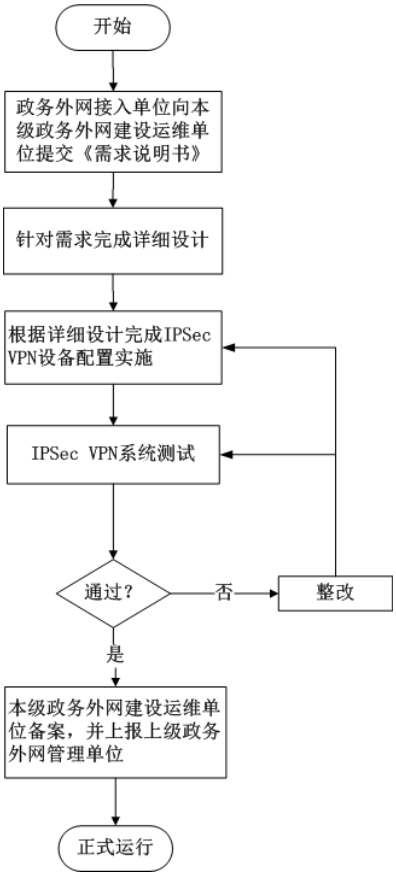

图 6-1 建设实施过程流程图

6.1 需求分析阶段

本阶段主要工作是政务外网接入单位根据自身的网络情况和业务需求，结合政务外网组网原则，向本级政务外网建设运维单位提交需求申请。本级政务外网建设运维单位根据相关建设原则对提交的需求申请进行审定。

政务外网接入单位应从以下几个方面考虑实际需求。

6.1.1 本地政务外网建设现状与需求

了解当地政务外网建设现状，分析各部门对应用系统的安全建设需求，理顺各业务系统的关系。如果本级政务外网已经建设完毕，接入单位直接通过本级政务外网即可实现各级部门纵向、横向的互联互通。对于不具备专线条件的接入单位，考虑使用 IPSec VPN 设备通过互联网接入政务外网。此时应先理清自身的业务系统，确定需要接入政务外网的业务系统数量、所需带宽、具体接入方式（IPSec VPN 网关接入方式或 IPSec VPN 客户端接入方式），再参考本指南“8 典型应用场景”章节的具体实例，选择适合实际接入需求的 IPSec VPN 设备部署方式。

6.1.2 业务系统安全现状与需求

了解已有业务系统的具体情况和重要程度，重点关注需要接入政务外网的业务系统。对于重要业务系统应加强安全防护，给予重点保护，保证接入政务外网的业务系统数据的机密性、完整性和可用性。

6.1.3 IPSec VPN 设备的功能、性能需求

政务外网接入单位根据业务系统运行状态、日常业务流量等现状，提出政务外网 IPSec VPN 设备功能要求和性能指标要求。

6.1.4 等级保护合规性需求

在 IPSec VPN 设备的需求分析过程中，应充分考虑到等级保护的相关要求。IPSec VPN 设备的功能应符合信息安全等级保护相关要求，并与其承载的业务系统最高安全保护等级相一致。

6.1.5 需求提交与审定

政务外网接入单位应仔细梳理自身的实际需求，如开通业务系统的类型和数量、业务流量占用带宽、IPSec VPN 设备选择、认证证书等，生成《需求说明书》，提交本级政务外网建设运维单位。

本级政务外网建设运维单位收到接入单位提交的《需求说明书》后，首先根据接入网关就近接入原则、移动办公用户属地化接入原则，确认提交需求的政务外网接入单位在其管辖区域，然后进一步考虑接入单位的网络建设情况、业务系统情况，结合政务外网 IPSec VPN 设备功能、性能指标，评估接入单位需求的合理性、可行性，提出审定意见。

具体分为以下两种情况：

a） 政务外网接入单位了解自身网络建设、业务系统状况，IPSec VPN的接入方式也符合其实际需求，IPSec VPN设备满足其对功能和性能的需求，政务外网建设运维单位同意需求申请。

b） 政务外网接入单位对自身情况不了解，仅提出接入申请，政务外网建设运维单位对接入单位进行调研后，提出合理化建议。如接入单位需将整个单位局域网或专网接入，则建议其部署IPSec VPN网关设备接入政务外网；如接入单位仅需单终端接入或是移动办公用户接入，则建议其安装IPSec VPN客户端接入政务外网。

6.2 详细设计阶段

详细设计阶段的主要工作是在需求分析结论的基础上，对建设实施过程进行详细设计，并完成详细设计文档。整个详细设计阶段分为技术方案设计和管理方案设计两个方面。

6.2.1 技术方案设计

技术方案设计主要是将 IPSec VPN 建设的技术体系、建设原则、技术要求落实到产品功能上，使得 IPSec VPN 设备的选择、实施具有依据。主要包括以下内容。

6.2.1.1 政务外网网络建设

政务外网接入单位经过前期的调研需求，已经了解本级政务外网建设情况，也理清自身的业务系统状况，确定业务接入方式。根据实际情况，可采用 IPSec VPN 网关接入或 IPSec VPN 客户端接入。接入单位需要向政务外网建设运维单位申请 IPSec VPN 网关 IP 地址，地址规划应遵守《国家电子政务外网 IP 地址及域名管理办法》。

6.2.1.2 业务系统分析

政务外网接入单位应梳理自身业务系统。IPSec VPN 设备的选型，应充分考虑接入 IPSec VPN 的业务系统数量，业务流量等情况。根据业务系统的重要性，建议在不同的运营商各申请一条互联网出口链路，互为备份，对重要业务系统进行保障。

6.2.1.3 IPSec VPN 设备功能

IPSec VPN 设备的功能请参考本指南“5 IPSec VPN 技术要求”相关章节的内容。

6.2.1.4 IPSec VPN 设备性能

政务外网网络分中央、省、地市、县四个级别。不同级别的网络，不同的业务系统对 IPSec VPN 设备的性能要求也不同。经过前期的测试，IPSec VPN 设备划分为 A、B、C、D 四个级别（见表 6-1），接入单位可根据接入业务量大小，接入用户数量等指标衡量，选择适合自身需求的 IPSec VPN 设备。

6.2.1.5 信息安全等级保护要求

IPSec VPN 设备需考虑等级保护相关要求。具体请参见本指南“5.6 IPSec VPN 等级保护合规性要求”章节。

表 6-1 各档 IPSec VPN 设备性能指标分类表

不同档设备参数	A	B	C	D
建议应用范围	中央级高配	省级低配	地市级低配	县级低配

	省级高配	地市级高配	县级高配	
	3000 用户数的政务部门	1500 用户数的政务部门	500 用户数的政务部门	300 用户数的政务部门
IPSec VPN 隧道数	5000	3500	1000	600
SM1 加密性能	200Mbps	100 Mbps	50 Mbps	30 Mbps
最大并发连接数	200 万	100 万	50 万	10 万
吞吐量	2Gbps	800 Mbps	200 Mbps	100 Mbps

6.2.1.6 信息安全等级保护要求

IPSec VPN 设备需考虑等级保护相关要求。具体请参见本指南“5.6 IPSec VPN 等级保护合规性要求”章节。

6.2.2 管理方案设计

管理方案设计主要是满足实施过程中的安全管理需要，以保证安全技术建设的同时，安全管理的同步建设。主要包括以下内容。

6.2.2.1 IPSec VPN 设备准入测试

政务外网接入单位选择的 IPSec VPN 设备必须通过国家电子政务外网管理中心统一组织的准入测试。无论在功能还是性能上，都能满足政务外网的要求。

准入测试原则上每年组织一次，具体时间及方式应遵循国家电子政务外网管理中心的相关要求。

6.2.2.2 IPSec VPN 设备管理要求

IPSec VPN 设备管理需要从多个方面来考虑。如设备密钥管理、数据管理、操作人员管理、证书管理、VPN 体系层级化管理等。具体要求请参见本指南“5 IPSec VPN 技术要求”相关章节。

6.2.2.3 IPSec VPN 客户端要求

IPSec VPN 客户端需要满足软件运行平台、USB Key 支持、接入认证模式、IPSec VPN 同互联网应用隔离等四个方面的技术要求，具体请参见本指南“5.2 IPSec VPN 客户端技术要求”章节。

6.3 配置实施阶段

配置实施阶段的主要工作是按照详细设计方案的要求，完成 IPSec VPN 建设实施。根据政务外网建设的政策、标准要求、配置安全策略，保证接入单位之间的互联互通以及信息共享等业务的安全。

6.3.1 实施准备

在建设实施之前，政务外网接入单位需要落实以下几个方面的工作：

a） 证书申请。

政务外网接入单位应向本级政务外网建设运维单位申请IPSec VPN设备证书和操作员证书。

b） IP地址申请。

政务外网接入单位应向本级政务外网建设运维单位申请IPSec VPN设备网关地址池及设备管理IP地址。

c） 备份链路申请。

为保证重要业务系统的安全接入，政务外网接入单位可以考虑向不同的运营商申请备份链路。请相关电信运营商勘查线路并开通。

d） 稳定保障。

在实施前，应制定网络割接方案，应急回退方案等，以保障接入业务系统运行的稳定性、连贯性。

6.3.2 IPSec VPN 设备部署

政务外网接入单位根据详细设计方案中 IPSec VPN 设备的接入方式完成设备的部署。

a）网关接入方式。

IPSec VPN 网关部署在政务外网接入单位的互联网出口。

b）客户端接入方式。

在单终端、移动办公用户终端安装 IPSec VPN 客户端。用户采用用户名、口令方式或证书方式连接到政务外网建设运维单位的 IPSec VPN 服务网关。

在设备部署时，会涉及到接入单位的中心机房、局域网、互联网接入等方面的业务变更，应遵循本指南“7 IPSec VPN 接入过程管理”相关内容。

6.3.3 IPSec VPN 设备配置

IPSec VPN 设备部署完毕后，政务外网接入单位应配置安全策略，确保接入单位能够连接至本级政务外网，并实现与上、下级政务部门的互联互通，同时保证本地业务的安全。政务外网建设运维单位应审定政务外网接入单位 IPSec VPN 的安全策略，确保 IPSec VPN 设备承载的业务系统与接入单位提交的需求相一致。

6.3.4 系统联调

IPSec VPN 设备需要与相关的系统、应用进行联调测试。如统一身份鉴别、授权访问控制、设备集中管理等应用。通过系统联调，有效保证 IPSec VPN 链路通畅，承载业务运行稳定，设备维护方便快捷。

6.4 测试与备案阶段

系统投入使用后应在本级政务外网建设运维单位的主持下对 IPSec VPN 设备各项功能、性能，业务支撑等进行测试，确保政务外网接入单位的安全需求得到满足。

配置实施完毕后，本级政务外网建设运维单位应及时备案，并上报上级政务外网建设运维单位。

7 IPSec VPN 接入过程管理

IPSecVPN 接入过程管理是按照业务流程进行生命周期的全过程管理，也是对政务外网接入单位和政务外网建设运维单位在采用 IPSec VPN 设备接入与应用的整个过程说明。本章详细说明接入与业务开通、业务变更、运行管理、业务撤销等四个阶段需各个单位相互协作的流程与主要内容，具体如下：

7.1 接入与业务开通

利用 IPSec VPN 设备接入政务外网必须符合本规范以及国家电子政务外网管理中心的入网要求。流程上首先应提出申请，提供所需材料，经过本级政务外网建设运维单位审定后，方可接入。整个流程包括准备与确认阶段、配置实施阶段、业务开通与备案阶段三个步骤，如图 7-1 所示。

7.1.1 准备与确认阶段

政务外网接入单位与当地政务外网建设运维单位进行沟通，进入准备接入阶段，讨论开通业务系统类型、开通业务系统数量、IP 地址申请、证书申请、带宽需求等内容，确定以上相关内容后，并开始接入与业务开通方案设计。证书优先采用政务外网证书管理中心颁发的证书，根据实际情况，可以使用用户原有 CA 系统颁发的证书。

7.1.2 配置实施阶段

严格按照接入与业务开通方案的设计目标执行，严格按照实施文档进行，向政务外网建设运维单位提出实施协助申请单，并做好相应记录。

7.1.3 业务开通与备案阶段

在配置实施阶段结束后，进行测试，向政务外网建设运维单位提出网络连通性测试协助申请单，并形成以下测试文档：

a）《设备测试报告》；

b）《网络连通性测试报告》；

c）《业务系统访问测试报告》。

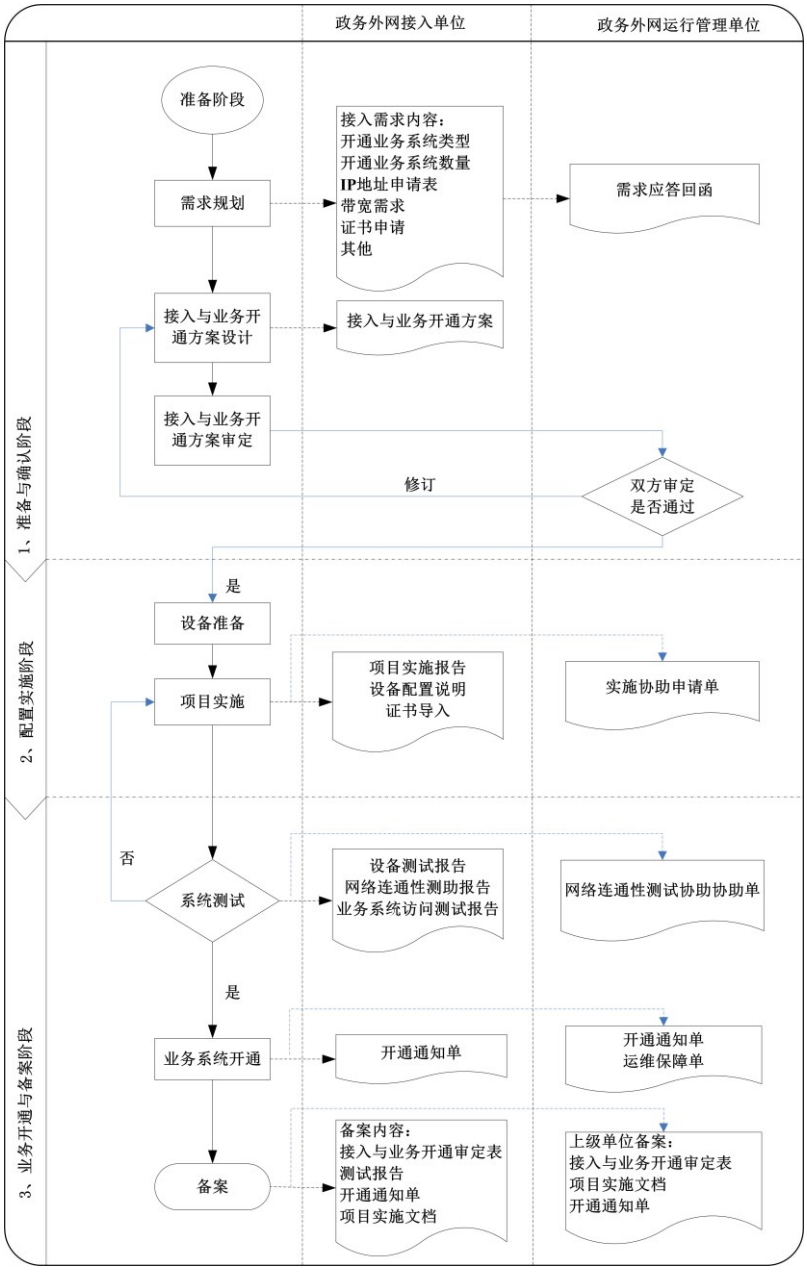

图 7-1 IPSec VPN 接入政务外网流程图

系统在通过测试后进入运行阶段并备案，备案过程中至少包含以下材料：

a） 《接入与业务开通审定表》；

b） 《建设实施文档》；

c） 《开通验收报告》。

在 IPSec VPN 接入与业务开通的过程注意以下事项：

a） 接入设备选用通过国家电子政务外网管理中心准入测试的IPSec VPN设备，以保障设备的互通性、可用性、稳定性、安全性，满足政务外网业务承载的正常运行要求；

b） 接入设备要进行相关登记与备案，并确定设备运维负责人；

c） 根据不同的应用场景选用相应的设备。

7.2 业务变更

政务外网接入单位在对 IPSec VPN 配置、移动办公客户端增减、业务系统的调整、证书的更新、

接入带宽调整、IPSec VPN 接入改为专网接入等进行变更时，需发起业务变更申请，政务外网建设运维单位应及时处理业务变更申请并实施，变更单位在进行业务变更操作时要有相应的应急保障与恢复措施。业务变更流程如图 7-2 所示。

7.3 运行管理

7.3.1 运行管理原则

设备运维部门应综合利用各种 IT 运维支撑工具提供的确保 IPSec VPN 设备和应用系统安全、高效、经济运行的服务，并且按照“谁运行谁负责，谁使用谁负责”的原则落实责任到人。运行管理主要包括运行监控、安全管理、配置管理。

7.3.2 运行监控

按照层级化管理原则，各级运行维护部门应对本级政务外网的 IPSec VPN 设备进行实时监控，及时发现故障并组织处理和跟踪反馈。

主要监控内容如下：

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。

当出现 IPSec VPN 设备告警时，应记录告警发生时间、告警类型、告警信息、告警发现人等信息，并启动故障管理，重大故障应及时向上级部门汇报。

7.3.3 安全管理

按照层级化管理原则，各级政务外网建设运维单位应负责定期检查 IPSec VPN 设备的访问控制策略与日志信息，发现安全问题，追查问题根源并及时解决。

定期备份设备的配置信息，定期对设备的日志信息进行备份保存，便于日后事件的追查、分析，重大安全事件应及时向相关部门汇报。

7.3.4 配置管理

各级政务外网接入单位应建立配置管理信息库，对 IPSec VPN 资源进行记录和统一管理。资源管理信息库记录的信息应至少包括：系统配置、技术方案、网络拓扑结构、网络 IP 地址规划和使用情况、设备型号、证书信息、所承载的业务系统等。

7.4 业务撤销

7.4.1 业务撤销分类

业务撤销分为两类，永久撤销和临时撤销。在撤销过程中要有相应的应急保障措施。用户的业务撤销流程如图 7-3 所示。

7.4.2 永久撤销

当政务外网接入单位已具备专线接入政务外网条件或者不再有政务外网应用需求时，可以申请外网业务撤销。外网接入单位需填写《业务撤销申请表》与《业务撤销方案》，经政务外网建设运维单位主管领导批准后，方可以进行业务撤销操作，中断用户网络与政务外网的连接。外网业务撤销后，本级政务外网建设运维单位将清除外网接入设备的敏感信息，并回收为用户分配的外网 IP 地址。

7.4.3 临时撤销

如政务外网接入单位因特殊事件（如：黑客攻击、网页篡改等安全事件）影响业务系统正常运行，应主动上报并中断外网连接。若影响范围已经扩大，且接入单位未主动上报并中断连接的，经政务外网建设运维单位的主管领导批准，运维部门可以采取紧急中断接入单位网络连接的措施。当接入单位出现的问题解决后，接入单位需提交材料申请恢复网络连接。经政务外网建设运维单位批准后方可恢复网络连接。

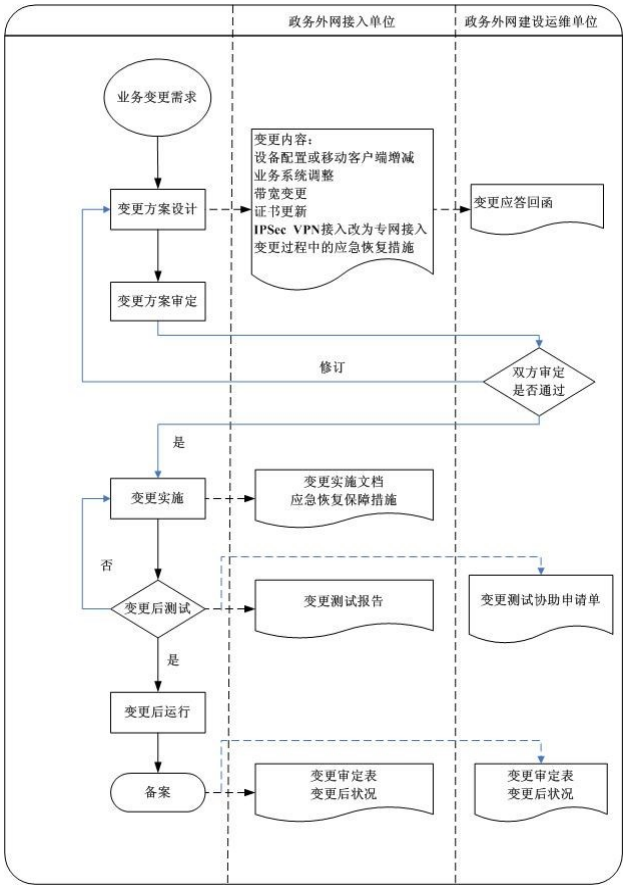

图 7-2 IPSec VPN 业务变更流程图

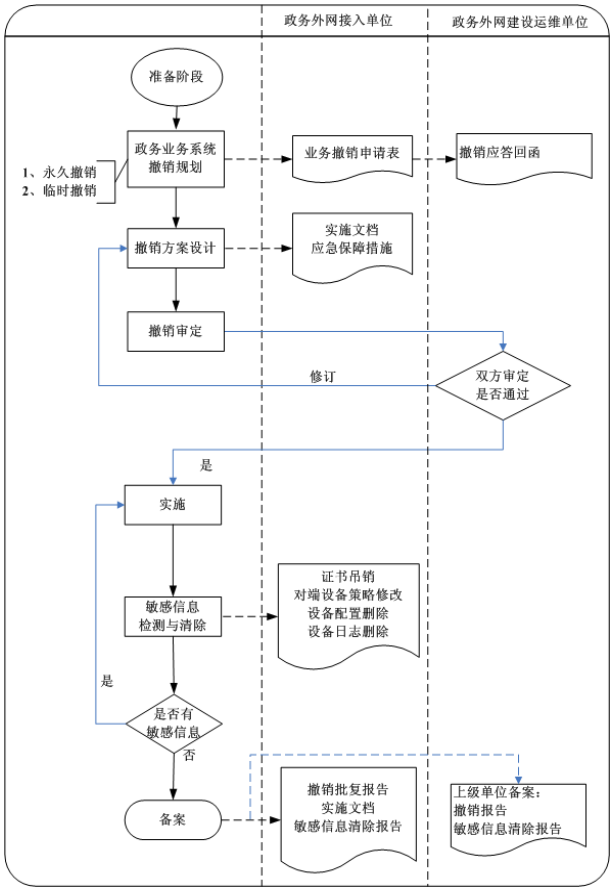

图 7-3 IPSec VPN 业务撤销流程图

8 典型应用场景

通过部署 IPSec VPN 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需求，延伸政务外网的覆盖范围。

一般各级政务外网划分了公用网络区、专用网络区和互联网接入区。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，通过政务外网互联网出口，提供统一 IPSec VPN 接入服务。

政务外网使用 IPSec VPN 的典型应用，如图 8-1 所示。

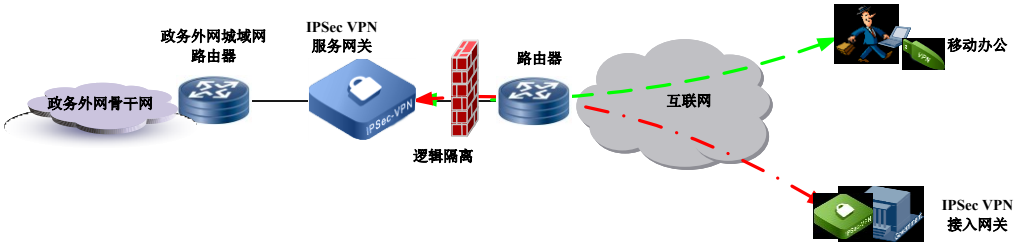

图8-1　政务外网IPSec VPN典型应用示意图

IPSec VPN网关具有外联接口和内联接口。一般，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城域网。外部接入的IPSec VPN接入网关一般部署在局域网或城域网互联网的出入口处。

b） IP地址：IPSec VPN服务网关外联接口IP地址使用互联网地址，IPSec VPN服务网关内联接口后的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，内联口后的IP地址直接全部采用地址池内的地址或者经过NAT转换后的地址池的地址。IPSec VPN客户端的IP地址一般由IPSec VPN服务网关分配。

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

d） 性能要求：IPSec VPN服务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。根据需求，IPSec VPN服务网关可以集群部署。

按照政务外网中部署IPSec VPN设备的几类实际需求情况，划分了四种场景，分别描述部署要点。

8.1 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它单位使用 IPSec VPN 网关，通过互联网线路接入政务外网。如图 8-2 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。

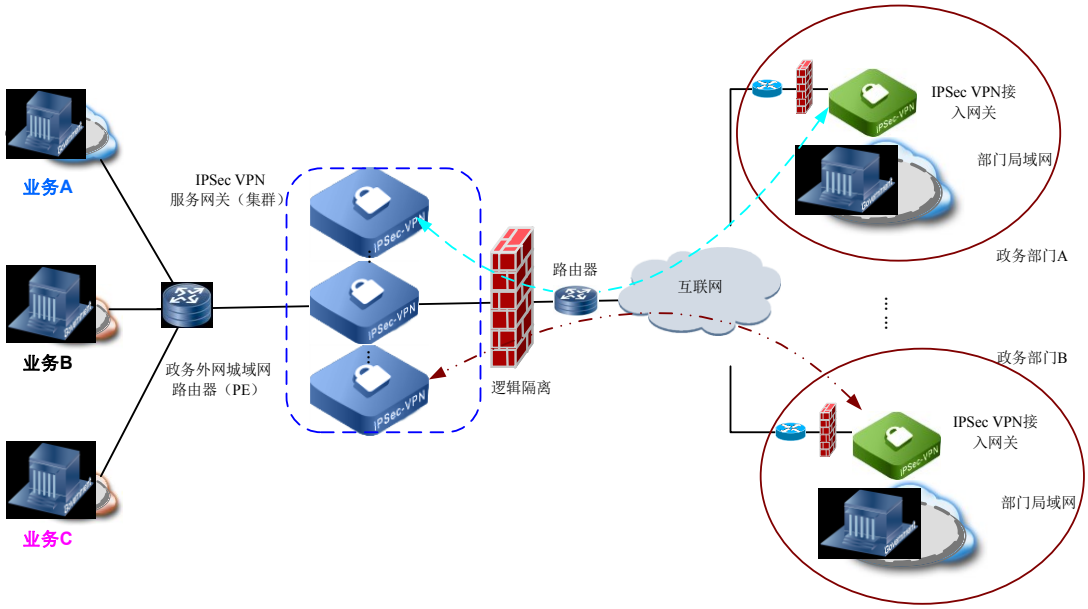

图 8-2 政务外网 IPSec VPN 网关典型应用场景一

具体实施要点参见表 8-1。

表 8-1 典型应用场景一的实施要点

	接入位置	IP 地址	性能要求	其他要求
IPSec VPN服务网关（集群）	在政务外网互联网接入区内，一般部署在防火墙之后	政务外网运维单位统一分配（不包括外联接口的互联网地址）	根据接入的IPSec VPN 网关和客户端的数量、带宽，采用单机或集群方式部署	内联 PE 接口，采用VLAN子接口或采用 VRF 区分不同应用，实现 IPSec VPN 与 MPLS VPN 安全对接
IPSec VPN接入网关	1、部署在外部接入单位局域网的互联网出入口处 2、按照就近接入原则，通过互联网接入到本级政务外网的 IPSec	1、内部局域网的地址采用政务外网统一分配的地址池内地址 2、内部局域网的地址可以根	满足用户业务需求、带宽需要	

	VPN 服务网关或本级无条件时申请接入上级 IPSec VPN 服务网关	据需要经过 NAT 转换为地址池内的地址		

8.2 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 8-3 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。

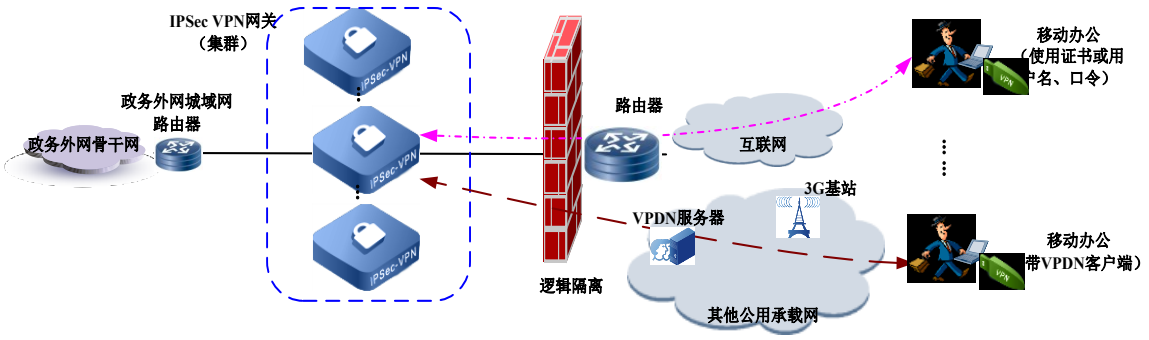

图 8-3 政务外网 IPSec VPN 网关应用场景二

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联通VPDN或以其他形式联通网络，然后再连接到IPSec VPN服务网关。

具体实施要点参见表8-2。

表 8-2 典型应用场景二的实施要点

	接入位置	IP 地址	性能要求	其他要求
IPSec VPN 服务网关	在政务外网互联网接入区内，一般部署在防火墙之后	政务外网运维单位统一分配（不包括外联接口的互联网地址）	根据接入的 IPSec VPN 网关和客户端的数量和带宽，采用单机或集群方式部署	1、内联 PE 接口，采用 VLAN 子接口或采用 VRF 区分不同应用数据； 2、根据业务需要，启用 SSL VPN 功能。
移动办公	遵循属地化接入原则，从归属地 IPSec VPN 服务网关接入	IPSec VPN 服务网关分配	满足用户业务需求、带宽需要	1、移动办公、单终端办公用户采用用户名、口令方式或证书方式连接到 IPSec VPN 网关； 2、在 VPDN、3G 接入等其他公众网络连接情况下，移动办公用户需要先联通 VPDN 等网络，然后再连接到 IPSec VPN 网关。

8.3 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 8-4 所示。

根据实际情况，也可采用本级政务部门部署一台上联 IPSec VPN 接入网关，同时部署另外一台 IPSec VPN 服务网关。

具体实施要点参见表 8-3。

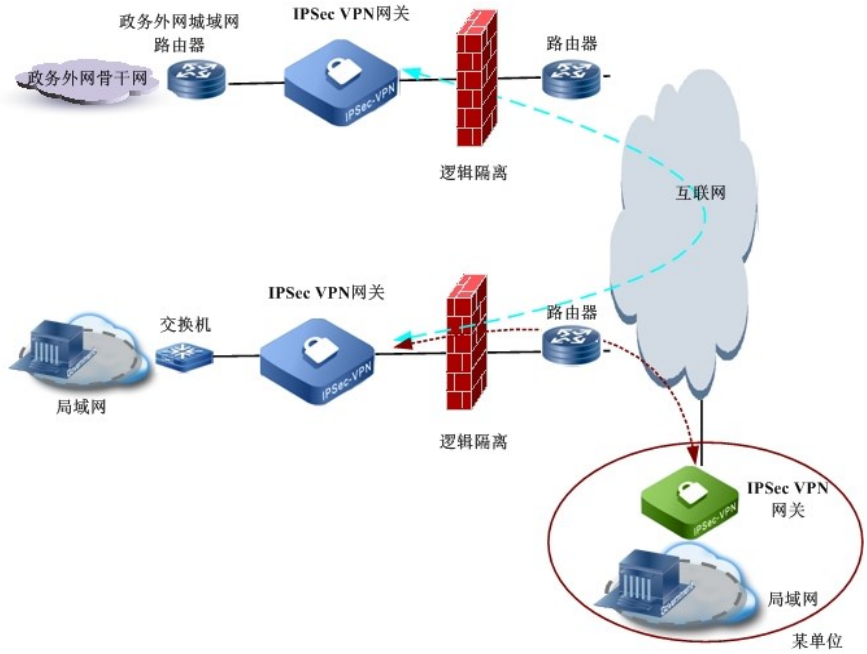

图 8-4　政务外网 IPSec VPN 网关应用场景三

表 8-3 典型应用场景三的实施要点

	接入位置	IP 地址	性能要求	其他要求
本级政务外网 IPSec VPN 服务网关	在政务外网互联网接入区内，一般部署在防火墙之后	政务外网运维单位统一分配（不包括外联接口的互联网地址）	根据接入的 IPSec VPN 网关和客户端的数量和带宽，采用单机或集群方式部署	接受来自（本级）IPSec VPN 接入网关或客户端的连接，同时又作为一个独立的 IPSec VPN 接入网关远程联入上一级政务外网互联网接入区的 IPSec VPN 服务网关
上级政务外网 IPSec VPN 服务网关	在政务外网互联网接入区内，一般部署在防火墙之后	政务外网运维单位统一分配（不包括外联接口的互联网地址）	根据接入的 IPSec VPN 网关和客户端的数量和带宽，采用单机或集群方式部署	内联 PE 接口，采用 VLAN 子接口或采用 VRF 区分不同应用数据

8.4　接入数据交换服务区

在有数据交换需求情况下，可以在 IPSec VPN 服务网关后面单独建立一个与政务外网骨干网逻辑隔离的数据交换区，方便单位、用户在此进行数据交换。

通过与 IPSec VPN 服务网关建立 IPSec VPN 隧道，用户接入到数据交换区，不直接接入政务外网骨干网，完成数据交换。如图 8-5 所示。

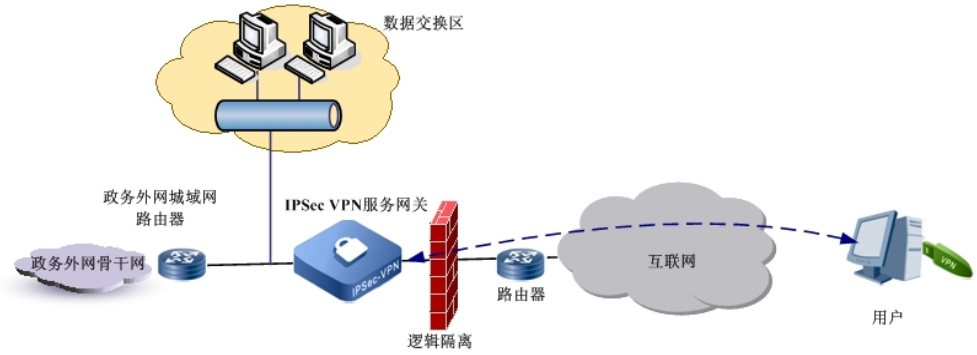

图 8-5　政务外网 IPSec VPN 网关应用场景四

实施要点参见表 8-4。

表 8-4 典型应用场景四的实施要点

	接入位置	IP 地址	性能要求	其他要求
IPSec VPN 服务网关	在政务外网互联网接入区内，内部接入政务外网城域网和数据交换区	政务外网运维单位统一分配（包括数据共享区的 IP 地址）	根据接入的 IPSec VPN 网关和客户端的数量和带宽，采用单机或集群方式部署	内联 PE 接口，采用 VLAN 子接口或采用 VRF 区分不同应用，实现 IPSec VPN 与 MPLS VPN 安全对接
接入网关或移动用户	接入到对口部门归属地的 IPSec VPN 服务网关	政务外网运维单位统一分配，或接入的 IPSec VPN 服务网关分配	满足用户业务需求、带宽需要	

附录 A：负载均衡技术要求

（资料性附录）

在 IPSec VPN 网关集群化部署时，可以采用负载均衡技术。该方案综合使用反向路由注入、DPD、NAT 等技术，将流量在各个 VPN 网关间进行分担。该方案适用于使用 2 台以上的 VPN 网关部署负载均衡的情况，下面以 3 台 VPN 网关（网关 1、网关 2、网关 3）为例进行说明，如图 A-1 所示。

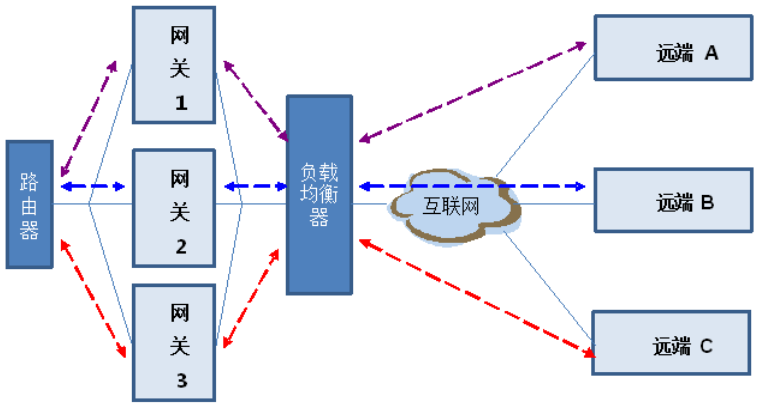

图 A-1 IPSec VPN 负载均衡技术示意图

方案说明如下：

a） 网关1、网关2、网关3使用同一份设备证书。网关1、网关2、网关3外部地址分别为IP1、IP2、IP3，负载均衡器外部地址为IP4，配置负载均衡器将到地址IP4的报文进行目的地址转换（转换为到IP1、IP2或IP3的报文）。

b） 远端A、远端B、远端C（VPN网关或VRC）的对端VPN网关地址都配置为 IP4。

c） 网关1、网关2、网关3和远端A、远端B、远端C上使能DPD便于探测隧道对端是否存活并据此决定是否重新协商。

d） 对于从路由器到远端（图中从左至右方向）的路由，有两种解决方案：

方案一： 网关 1、网关 2、网关 3 上使用反向路由注入功能，这使得 IPSec SA 建立后到被保护的远端网络的路由被加入路由表。网关 1、网关 2、网关 3 和路由器之间配置动态路由协议允许重分发反向路由注入功能加入的到远端网络的路由。

方案二： 在网关 1、网关 2、网关 3 上配置 NAT，使用不同的地址池，对从 IPSec 隧道出来的报文进行源地址转换（反方向则进行目的地址转换）。在路由器 R 上配置静态路由将到网关 1、网关 2、网关 3 各自地址池中地址的报文路由到对应的网关。

附录 B：IPSec VPN 与 MPLS VPN 对接方式

（资料性附录）

IPSec VPN 与 MPLS VPN 可以通过 VRF 方式或子接口方式实现对接。

方案一：基于 VRF 方式。

IPSec VPN 设备与 MPLS VPN 采用 VRF 方式实现对接，其具体实现有两种方式：

一种是 IPSec VPN 服务网关作为 MCE，IPSec 数据解封装后导入到指定的 VRF 中，VRF 接收到数据后根据 IPSec SA 将数据加密封装发送到相连的 PE 设备的 VRF 中。IPSec VPN 网关用于 MCE 的方式下，在网关与 PE 之间配置多个以太子接口，每个子接口均对应一个 VRF，在 IPSec VPN 网关 VRF 上配置基于 VRF 的静态路由或动态路由，IPSec VPN 网关接收到 IPSec 数据解封装后根据 SA 获取到注入的 VRF 信息，将数据转发到对应的 VRF 中，再通过路由查找将数据转发给所连接的 PE 设备，再封装 MPLS VPN 标签和其他头部信息后转发。

另外一种是 IPSec VPN 服务网关作为 MPLS VPN 中的 PE，IPSec 数据解封装后导入指定的 VRF 封装 VPN 标签，再封装 MPLS 相关头部信息后，转发到 MPLS VPN 网络中。

IPSec VPN 网关若支持 IPSec VPN 动态路由注入功能，结合 VRF 动态路由协议，可以很好的适应 IPSec VPN 同 MPLS VPN 的对接，在 VPN 网关备份负载分担环境中能自动适应 IPSec 隧道的变化，减少配置工作以及步骤工作量。

不同的 IPSec VPN 用户接入到不同的专用网络区域，可以通过证书的 DN 信息来区别不同类型用户来实现。只有符合 DN 要求的才能建立对应的 IPSec 隧道，实现专用网络之间用户隔离。预共享方式下，可以通过配置积极模式将 IKE ID 设置不同类型来实现。

方案二：基于子接口方式。

在 IPSec VPN 网关上配置若干个地址池，根据接入用户所属的组，分配到不同的地址范围。在 IPSec VPN 网关与 MPLS VPN 相连的网口配置相应的子接口，每个子接口与 PE 设备的子接口一一对应，而且属于同一个 VLAN，每个子接口的 IP 地址不在同一网段。在 IPSec VPN 网关上针对不同的源 IP 地址和目的 IP 地址配置相应的策略路由。

外部加密数据到达 IPSec VPN 网关后根据 VPN 策略匹配相应的隧道，数据解密完成后，再根据源、目的地址，匹配对应的策略路由，然后通过某一个子接口发送给 PE 设备。PE 设备会根据接收的子接口将数据再封装到对应的 MPLS VPN 隧道中。同时在 IPSec VPN 网关建立状态表。

从 PE 设备发送到 IPSec VPN 网关的数据，首先会查询中已建立的状态表，根据目的 IP，送入相应的隧道做加密操作，然后发往隧道的对端设备。

附录 C：IPSec VPN 客户端使用环境说明

（资料性附录）

在客户端环境方面，操作系统、软件安装配置、网络速度、软件兼容性等因素都直接影响客户端使用效果。

IPSec VPN 网关的客户端软件一般支持常见的 Windows 操作系统（其他类型智能终端的系统的支持方式见页末），如：Windows XP、Windows 7，其他操作系统兼容性较差。

用户首次使用客户端软件，除了安装软件外，一般需要手动配置软件的关键参数，可要求网关厂商按照固定配置生成配置文件直接内置到软件安装过程中，避免复杂的人工配置。

用户的互联网接入环境的速度和稳定性对 IPSec VPN 拨号连接与访问速度有较大的影响，应保证客户端所使用的网络环境网速相对稳定、丢包率低，并应满足用于 IPSec VPN 的基本带宽要求，一般不低于 128Kbps。

用户网络中有边界防火墙等相关访问控制设备的，必须开放 IPSec 标准协议端口，如 UDP500、UDP4500 等，个别厂商有定制端口，也应相应开放。

用户终端的操作系统中需要开放 IPSec 相关系统服务，安装的软件防火墙、杀毒软件等也需要开放客户端软件访问。

特别地，对于智能终端如手机、平板电脑等接入到 IPSec VPN 服务网关的需求，可采用如下三种方式解决：

方式一：部分终端系统（如苹果、安卓等）自身集成 IPSec VPN 客户端，可以采用预共享的方式直接与服务网关建立连接。

方式二：将终端设备通过无线 Wifi 等技术接入到 IPSec VPN 接入网关内所在局域网络中，再通过 IPSec VPN 接入网关与服务网关建立连接。

方式三：采用 SSL VPN 的方式直接与开启了 SSL 功能的 IPSec VPN 服务网关建立连接。