国家电子政务外网标准

GW0202—2014

国家电子政务外网安全接入平台技术规范

Technical Requirements for Securing Access Platform of

National E-Government Network

2014－11－13 发布　　2015－1－1 实施

国家电子政务外网管理中心

目　次

前　言

为指导国家电子政务外网（以下简称“政务外网”）安全接入平台设计和建设，根据我国有关法律、法规和技术规范，结合政务外网实际应用需求及产品部署经验，编制本规范。

本规范包括安全接入平台概述、基础框架、基本要求、建设指南、接入模式及接入流程、典型部署案例等内容。

本规范由国家电子政务外网管理中心提出并归口。

本规范起草单位：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、网神信息技术（北京）股份有限公司、北京天融信科技有限公司、华为技术有限公司、北京国联天成信息技术有限公司。

本规范主要起草人：罗海宁、冷默、邵国安、周民、吕品、徐惠清、任献永、张锐卿、黄敏、孙涛元、赵燕杰、刘歆、吴科科。

引　言

为了满足各级政务部门的移动办公、远程访问、现场执法以及相关企事业单位和工作人员利用公众网络安全接入到政务外网的业务需求，规范中央、省（自治区、直辖市）、地（市）、县级政务外网建设运维单位建设安全接入平台，特编制本规范。

国家电子政务外网安全接入平台技术规范

1 范围

本规范适用于指导各级政务外网建设运维单位进行安全接入平台的规划、设计、选型及实施等工作，也可作为政务外网职能部门进行指导、监督和检查的依据。

2 规范性引用文件

下列文件中的条款通过本规范的引用而成为本规范的条款。凡是标注日期的引用文件，其后所有的修改（不包括勘误的内容）或修订版均不适用于本规范。凡是不标注日期的引用文件，其最新版本适用于本规范。

GB/T 22239-2008 《信息安全技术 信息系统安全等级保护基本要求》

GM/T 0022-2014 《IPSec VPN 技术规范》

GM/T 0023-2014 《IPSec VPN 网关产品规范》

GM/T 0024-2014 《SSL VPN 技术规范》

GM/T 0025-2014 《SSL VPN 网关产品规范》

《国家电子政务外网 IPSec VPN 安全接入技术要求与实施指南》（政务外网[2011]11 号）

《国家电子政务外网安全等级保护基本要求》（政务外网[2011]15 号）

《国家电子政务外网安全等级保护实施指南》（政务外网[2014]1 号）

《商用密码管理条例》（国务院 273 号令）

3 术语和定义

GB/T 25069-2010 确立的以及下列术语和定义适用于本规范。

3.1

AAA

AAA 是 Authentication（验证）、Authorization（授权）和 Accounting（记账）三个英文单词的简称，验证是验证用户是否可以获得访问权限，确定哪些用户可以访问网络；授权确定用户可以使用哪些服务；记账记录用户使用网络资源的情况。

3.2

RADIUS 协议

RADIUS 是 Remote Authentication Dial-In User Service（远程用户拨号认证服务）的简称，是目前应用较广泛的 AAA 协议，是同时兼顾验证、授权、计费三种服务的一种网络传输协议。

3.3

AD

AD 是 Active Directory（活动目录）的简称，是 Windows 平台服务器核心组件之一，活动目录是一种目录服务,它可将网络中各种对象组合起来进行管理。它存储有关网络对象的信息，例如用户、组、计算机、共享资源、打印机和联系人等信息，使管理员和用户可以方便的查找和使用这些网络信息。

3.4

VPDN

VPDN 是 Virtual Private Dial-up Networks（虚拟专用拨号网）的简称，是电信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。

3.5

安全管理平台 Security Operation Center

安全管理平台是通过采用多种技术手段，收集和整合各类网络设备、安全设备、操作系统等安全事件，并运用关联分析技术、智能推理技术和风险管理技术，实现对安全事件信息的深度分析，能快速做出智能响应，实现对安全风险进行统一监控分析和预警处理。

3.6

移动终端管理系统 Mobile Device Management

移动终端管理系统为移动智能终端设备提供注册、激活、使用、淘汰各个环节的远程管理支撑，实现用户身份与设备的绑定管理、设备安全策略配置管理、设备应用数据安全管理等功能

4 缩略语

下列缩略语适用于本规范。

CA	数字证书认证中心（Certificate Authority）
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）
SSL	安全套接层（Secure Socket Layer）
VPN	虚拟专用网（Virtual Private Network）
OCSP	在线证书状态协议(Online Certificate Status Protocol)
SOC	安全管理平台（Security Operation Center）
VRF	VPN路由转发（VPN Routing Forwarding）
SNMP	简单网络管理协议（Simple Network Management Protocol）
L2TP	第二层隧道协议（Layer 2 Tunneling Protocol）
LNS	L2TP网络服务器（L2TP Network Server）
APP	智能终端应用程序（Application）
MDM	移动终端管理系统（ Mobile Device Management）

5 概述

政务外网安全接入平台是利用 Internet、移动通信网络（如 2G、3G、4G）、VPDN 等基础网络，面向不具备专线接入条件的各级政务部门、企事业单位、移动办公人员、现场执法人员和公众用户，提供安全接入到政务外网网络或业务的服务平台。

政务外网安全接入平台由各级政务外网建设运维单位负责建设运维，部署于政务外网互联网接入区与公用网络区（或专用网络区）之间，采取中央、省、地市分级建设，有需求的县级单位可参考建设。接入政务外网的政务部门原则上使用本级政务外网安全接入平台公共设施，如有独立的互联网出口，有远程安全接入需求建设安全接入平台时也应参照本规范。

6 基础框架

6.1 平台架构

政务外网安全接入平台架构如图 1 所示：

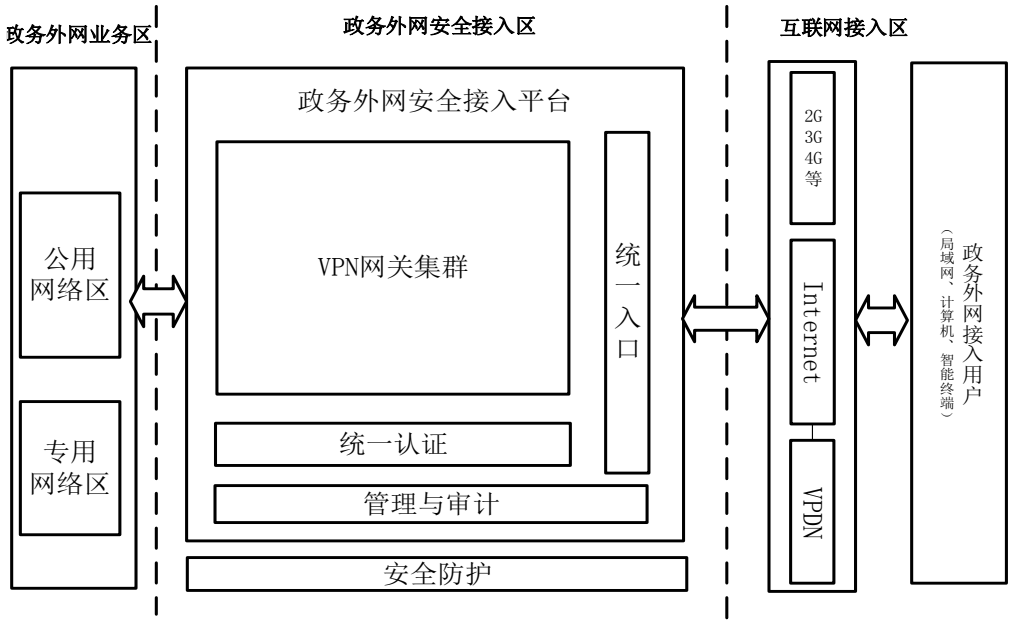


图 1 安全接入平台架构示意图

政务外网安全接入平台架构包含如下内容：

a) 互联网接入区

包括 Internet、移动通信网（2G\3G\4G 等）、VPDN 等基础网络环境。

政务外网接入用户通过上述基础网络连接到安全接入平台。

b) 政务外网安全接入区

1）统一入口：为接入用户提供服务接口或链路接口。

2）VPN 网关集群：采用负载均衡技术实现 IPSec VPN、SSL VPN 等网关集群，为用户提供安全接入服务。

3）统一认证：采用 RADIUS、LDAP 等认证协议实现基于数字证书的身份认证，为网关集群用户身份统一认证和权限管理提供支撑。

4）管理与审计：提供安全接入平台的运行情况监测、用户行为审计和安全接入平台设备的配置管理功能。

5）安全防护：通过使用网络访问控制、入侵检测与防御、防病毒等安全措施实现基础安全防护。

c) 政务外网业务区

安全接入平台的 VPN 网关采用虚拟子接口、VRF 等方式实现与政务外网公用网络区、专用网络区的网络和业务对接。

6.2 功能框架

政务外网安全接入平台的基本功能框架如图2所示：

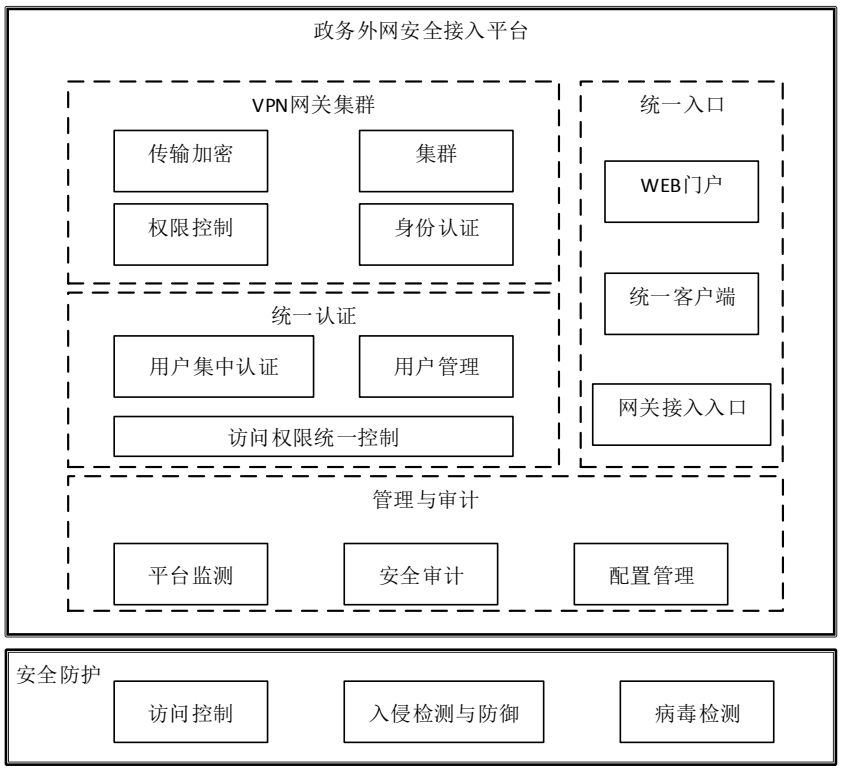


图2 安全接入平台功能框架图

政务外网安全接入平台的基本功能模块包括如下内容：

a) 统一入口：通过WEB门户提供安全接入所需的注册、审核、软件下载等功能，为用户提供PC机、移动智能终端统一接入客户端，设置网关设备接入入口，实现接入用户统一接入；

b) VPN网关集群：提供终端到网关或网关到网关的传输加密、身份认证、权限控制等功能，通过负载均衡、链路汇聚实现VPN网关集群；

c) 统一认证：为安全接入的身份认证和权限控制提供支撑，提供用户集中认证、用户管理、访问权限统一控制等功能；

d) 管理与审计:提供安全接入平台的运行情况监测、平台设备的配置管理和用户行为审计等功能；

e) 安全防护：为安全接入平台提供访问控制、入侵检测与防御、防病毒等基础安全防护功能。

7 基本要求

7.1 统一入口

7.1.1 WEB 门户

安全接入平台提供 WEB 方式接入服务入口，实现如下功能：

a) 提供统一的接入用户注册申请页面，申请成功后，注册信息可提交至LDAP、RADIUS等系统；

b) 提供IPSec VPN统一客户端、移动终端安全接入软件（APP）的发布、更新、下载等；

c) 提供SSL VPN登录页面；

d) 提供信息发布、移动智能终端消息推送；

e) 面向用户单位的业务应用，提供WebService等标准协议服务接口；

f) WEB门户页面应采用Html5等标准同时兼容并适配PC机、移动智能终端的主流浏览器。

7.1.2 统一客户端

a) PC机用户采用IPSec VPN接入时应使用政务外网统一IPSec VPN客户端，该客户端应兼容《国家电子政务外网IPSec VPN安全接入技术要求与实施指南》中的网关设备并符合该标准中相关要求，应支持IKE协议，符合《IPSec VPN技术规范》“5.1 密钥协商”章节要求。；
b) 智能终端用户采用统一的移动终端安全接入软件（APP），内嵌移动终端管理模块，支持不同安全需求的认证与加密方式，多种网络接入模式，如VPDN拨号、IPSec VPN拨号采用专用SSL客户端软件接入。

7.1.3 网关接入

政务部门局域网非专线接入到政务外网时，应使用网关对网关方式接入，接入部署设备应符合《国家电子政务外网IPSec VPN安全接入技术要求与实施指南》“5.1 IPSec VPN网关技术要求”章节要求。

7.2 VPN 网关集群

7.2.1 网关要求

VPN 网关应具有国家密码管理局颁发的《密码产品型号证书》。

a) IPSec VPN网关
   1) 应符合国家密码管理局发布的《IPSec VPN技术规范》（GM/T 0022-2014）和《IPSec VPN网关产品规范》（GM/T 0023-2014）；
   2) 应符合《国家电子政务外网IPSec VPN安全接入技术要求与实施指南》“5 IPSec VPN技术要求”。
b) SSL VPN网关
   1) 应符合国家密码管理局发布的《SSL VPN技术规范》（GM/T 0024-2014）和《SSL VPN网关产品规范》（GM/T 0025-2014）；
   2) 应支持政务外网证书、用户名/密码、短信、动态口令等认证方式，并支持双因子认证等混合认证模式；
   3) 应支持访问权限设置；
   4) 应支持VPN集群部署；
   5) 应支持隧道模式，并且能够实现和MPLS VPN无缝对接；
   6) 可通过发布虚拟桌面、虚拟应用或提供SDK的方式，为智能终端提供接入接口,并与统一客户端软件实现集成；
   7) 支持标准SNMP v3管理协议，支持Syslog等标准日志格式导出，可通过安全管理平台进行集中监控和管理。

7.2.2 集群要求

多台VPN网关可通过负载均衡设备组成IPSec VPN网关集群或SSL VPN网关集群。

负载均衡服务应符合以下要求：

a) 通过负载均衡设备链路负载功能，将VPN网关的接入请求根据IP地址、端口等策略分配到集群中相应网关设备，实现网关的自动调度。
b) 负载均衡设备与VPN网关、LNS网关、Portal服务器应使用内部IP地址互联，通过地址映射将互联网地址作为对外提供服务的IP地址。
c) 负载均衡设备应满足如下要求：
   1) 支持最小连接数、轮询、比例、最快响应、哈希、预测、观察、动态比例等负载均衡算法；
   2) 支持设备状态检测，用于检查设备、应用和内容的可用性；
   3) 支持集群服务域名智能解析；
   4) 支持带宽控制；
   5) 支持冗余备份。

7.2.3 传输加密

应采用 IPSec VPN 或 SSL VPN 进行传输加密防护，加密算法应符合国家密码管理局相关规范要求。

7.2.4 身份认证

安全接入平台应对接入的用户和接入的设备进行身份认证：

a) 用户身份认证

用户身份应由VPN网关或网关集群提交至统一认证平台认证，要求如下：

1) 支持数字证书、用户名/口令、短信、动态口令等多种用户身份认证方式。数字证书应由政务外网数字认证中心颁发；

2) 支持LDAP、RADIUS、AD等第三方认证系统；

3) 由网关解析证书中用户名等辨识信息，通过RADIUS或LDAP协议把认证信息传送到统一认证平台，并支持群组认证。

b) 设备身份认证

1) IPSec VPN网关对网关接入身份认证应采用数字证书认证方式，设备数字证书由政务外网数字认证中心颁发；

2) 智能终端设备通过移动终端管理系统注册认证，并通过SSL VPN实现访问隧道认证。

7.2.5 权限控制

安全接入平台应对接入的用户和设备进行权限控制：

a) 用户权限控制

1) 根据接入业务需求，对用户访问权限进行控制，阻止用户访问非授权资源；

2) 根据用户的属性查询授权信息，确定授予用户的服务资源，包括给用户分配IP地址、用户可访问的IP地址和服务等。

b) 设备接入控制

对设备的接入采取访问控制措施，根据设备数字证书属性设置接入设备的授权资源及访问权限阻止非授权访问。

7.3 统一认证平台

统一认证平台为VPN网关、LNS拨号接入设备提供支撑，一般包含LDAP或RADIUS认证服务器、短信网关等。

中央、省级安全接入平台，可建设独立的统一认证平台。县级安全接入平台可采用VPN网关内置的认证服务模块实现用户的身份认证。

统一认证平台要求如下：

a) 支持标准LDAP、RADIUS、OCSP等认证协议；

b) LDAP认证服务器应提供证书认证和用户名/口令认证，RADIUS认证服务器应提供用户名/口令认证；

c) 应建立统一的用户认证信息库，用于用户集中认证、访问权限统一控制；

d) 用户认证信息应包括证书用户信息、用户名、口令、用户单位、邮箱、手机号码等；

e) 支持用户信息维护、在线用户管理等用户管理功能；

f) 支持IP地址统一管理、统一分配，支持动态、静态IP地址分配，用户按指定地址组动态分配IP；

g) 可扩展支持第三方认证组件，如动态口令、短信认证组件；

h) 支持负载均衡或冗余备份；

i) RADIUS数据库应与LDAP数据库进行关联，可基于某个用户标识进行同步更新；

j) 应支持分级管理，支持省、地市等各级统一认证平台可远程同步用户信息，并分角色管理。

7.4 接入终端

接入终端通过VPN接入政务外网时，应由VPN客户端阻断其他的互联网应用。

a) PC机

PC机包括办公使用的台式电脑、笔记本等设备，接入政务外网时应满足如下要求：

1) 满足相应的信息系统安全等级保护中关于终端安全的相关要求，以及接入业务单位的接入终端安全要求；

2) 接入到安全等级保护要求为第三级的政务外网业务应用系统时，应使用证书认证方式；

3) 使用证书方式协商时，证书应使用政务外网数字认证中心统一颁发的数字证书，并由硬件设备承载。

b) 智能终端

智能终端接入政务外网时需满足以下要求：

1) 平板电脑、智能手机等移动智能终端，应安装安全防护软件并达到相关安全要求后方可接入；

2) 智能终端需集成移动终端管理模块，用于终端注册及远程管理。

7.5 管理与审计

对安全保护等级确定为第三级的政务外网，其安全接入平台，可建设独立的安全管理与审计平台；县级安全接入平台可使用各类安全接入、安全防护设备自身配置的安全审计模块实现安全管理、审计功能。

安全管理与审计平台要求如下：

a) 支持对平台整体运行情况、异常事件和行为的实时监测，并提供电子邮件、短信等告警功能；

b) 支持对用户接入行为和平台设备系统日志、运行日志、告警日志的审计；

c) 支持使用标准 SNMP v3 对平台设备配置的集中管理；

d) 支持监测与审计包括接入设备、安全设备、服务器主机、数据库等；

e) 支持终端上线时间、下线时间、登录账号等重要操作的日志审计；

f) 支持对智能终端设备的软硬件信息收集，记录硬件变更信息，并可远程管理与接入相关的数据和配置；

g) 支持日志统一格式输出，报表生成功能，支持图形化展示功能；

h) 监测和审计日志应至少保存 6 个月；

7.6 安全防护

7.6.1 网络访问控制

应在安全接入平台的网络入口、内部安全域边界部署防火墙实现网络边界保护和访问控制。

防火墙应只开放安全接入平台提供接入服务必需的服务端口（如标准IPSec VPN服务端口UDP 500、4500，统一入口WEB门户与标准SSL VPN服务端口为TCP 80,TCP 443，对流经接入平台的网络数据进行包过滤检测。

7.6.2 入侵检测与防御

应在安全接入平台的网络入口处部署入侵检测探测器或入侵防御系统，动态监视网络上流过的所有数据包，进行实时检测和分析，及时发现非法或异常行为，并且执行告警、阻断等功能并记录相应的事件日志，并能够与防火墙进行联动。

7.6.3 防病毒

在安全接入平台的网络入口处部署防病毒网关，及时更新病毒库，阻止病毒侵入和传播情况，进行及时的查杀。

8 建设指南

8.1 建设目标

建设政务外网安全接入体系，通过分层建设、属地化接入的方式，为不具备专线接入条件的政务部门提供接入政务外网的方案，扩大政务外网的覆盖范围，提升政务外网安全接入服务能力，满足各级政务部门横向和纵向业务需求；同时为公务员、现场执法、应急处置及企事业单位相关人员等提供移动办公、现场执法、数据上报等业务的安全接入服务。

8.2 建设原则

8.2.1 部署原则

政务外网安全接入平台部署应遵循以下原则：

a) 分级部署原则

安全接入体系分为中央级、省级、地市级三级平台，由国家电子政务外网管理中心提出规范，各级政务外网建设运维单位分别建设和运维。

b) 属地化接入原则

通过公众网络访问到政务外网的各类用户和各种终端，应通过本级属地安全接入平台接入到政务外网。

8.2.2 管理原则

a) 等级保护合规性原则

安全接入平台作为政务外网的一部分，应按照同级政务外网的信息安全等级保护要求进行建设和整改。

b) 层级化管理原则

政务外网安全接入平台的管理遵循统一规划、分层分级的管理原则，由各级政务外网建设运维单位负责管理和维护。

c) 统一测试选型原则

国家电子政务外网管理中心定期组织安全接入平台相关设备的技术测试、产品选型与发布，各级政务外网单位应按照发布目录进行产品选型和部署。

8.3 建设内容

安全接入平台应结合业务需求，按照第 7 章设计实现 VPN 网关集群、统一入口、统一认证平台、管理与审计、安全防护等主体模块，分别选型、部署相应的软硬件产品。

中央、省、地市分别建设本级安全接入平台，形成政务外网安全接入体系。县级可通过市级平台接入，有条件的县级政务外网也可自行建设。

通过建设各级安全接入平台，全国政务外网形成统一的安全接入体系，如图 3 所示。

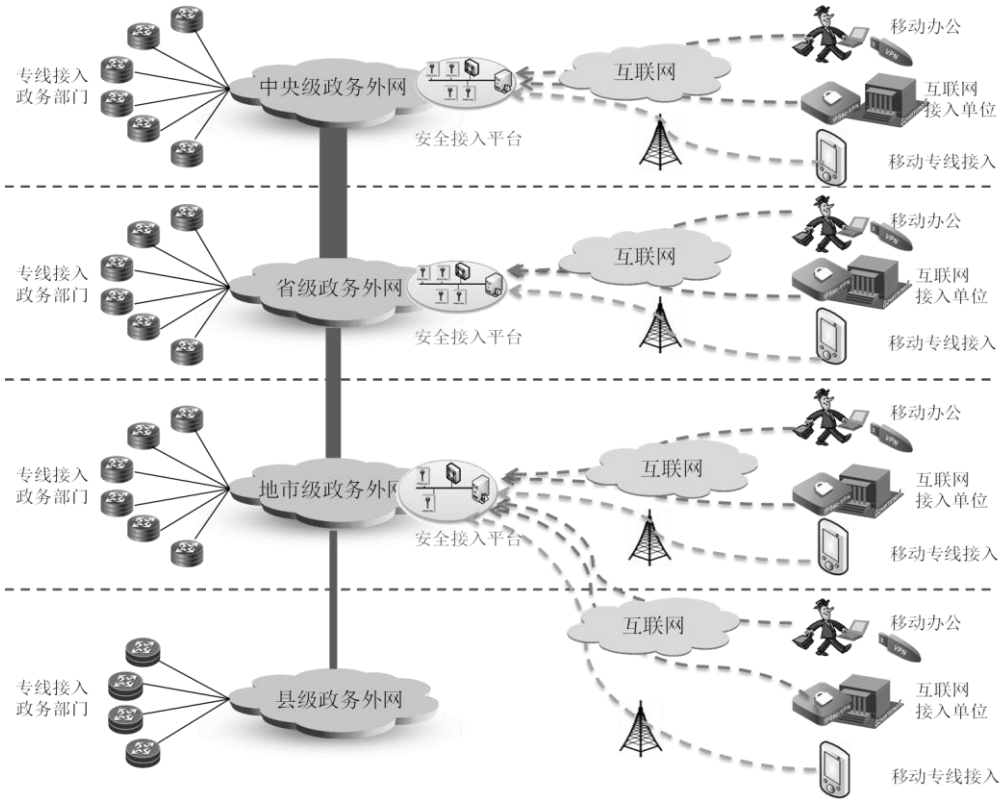


图 3 政务外网安全接入体系示意图

附 录 A
（资料性附录）
接入模式及接入流程

A.1 接入模式设计

IPSec VPN 和 SSL VPN 可应用于不同业务接入场景：

a) IPSec VPN

主要应用于非专线接入政务外网的单位，采用网关对网关接入进行组网以及远程终端接入进行长时间连接、数据上报、视频会议等非WEB方式访问的业务。对于专线接入单位，当专线发生故障时，应急情况下也可采用网关对网关接入方式，通过Internet或移动通信网的VPDN实现业务的不中断传输。

b) SSL VPN

主要应用于接入终端WEB方式接入政务外网，访问业务系统、远程桌面管理、远程办公等。

c) VPDN专线接入

用户可使用智能终端通过VPDN专线接入，VPDN专线接入和Internet接入类似，统一从政务外网安全接入平台入口进入，根据认证需求不同，运营商提供VPDN两种建设方案，分别为自建LNS和完全外包，自建LNS可对接入用户进行二次认证，便于对用户接入管理和审计管理。各级安全接入平台依据用户所要访问的业务应用系统的安全情况应采取IPSec VPN或SSL VPN网关对传输链路进行加密，VPDN专线接入时应满足如下要求：

1） 根据VPDN线路所属运营商不同，由中央级、省级等具备条件的单位独立建设LNS设备，用于实现身份认证、传输加密的要求；
2） 运营商侧认证服务应向用户单位提供审核本单位手机号码权限；
3） 用户拨通VPDN专线后，应断开其与Internet的路由，保证网络访问通道的唯一性；
4） 使用VPDN时，由安全接入平台统一认证服务分配用户IP地址。

政务外网建设单位按照远程组网、业务远程访问、数据传送等不同业务需求，可选择使用不同的接入模式组建安全接入平台，满足身份认证、授权管理、传输加密等安全要求。

A.2 接入流程设计

a) 网关对网关接入

网关对网关接入模式适用于不具备政务外网专线接入条件的单位，通过IPSec VPN网关接入政务外网，具体接入流程可设计如下：

1） 接入单位通过公众网络登录安全接入平台门户发起申请，由本级政务外网运维单位审核通过后下发接入网关配置信息、设备证书等；
2） 接入网关向安全接入平台IPSec VPN网关集群服务网关发起连接请求；
3） 服务网关通过认证平台对接入网关进行认证，认证成功后双方建立隧道；
4） 接入单位用户通过VPN设备建立的安全隧道访问政务外网业务。

b) 移动接入

移动接入模式适用于移动办公人员、现场执法人员、公众用户等通过公众网络访问政务外网业务，具体接入流程可设计如下：

1） 接入单位通过公众网络登录安全接入平台门户发起申请，由本级政务外网运维单位审核通过后根据接入业务不同下发接入必需资源，如统一业务入口或者SSL VPN服务地址、客户端软件、用户证书等；
2） IPSec VPN接入用户通过客户端发起请求，SSL VPN接入用户通过WEB方式发起请求，智能终端用户利用移动终端安全接入软件（APP）发起请求；
3） 网关通过认证平台对接入用户进行认证，认证成功后双方建立安全连接；
4） 接入用户通过VPN网关建立的安全连接访问政务外网业务。

c) VPDN移动专线接入

适用于智能终端用户通过移动通信网的VPDN方式接入或PC端用户通过ADSL等方式，接入用户需先通过Internet登录安全接入平台门户申请VPDN账号，在账号审核成功后，具体接入流程设计如下：

1） VPDN用户向LNS发起拨号并通过认证建立隧道；

2） VPDN隧道建立成功后，用户向SSL VPN网关发起请求；

3） 网关通过认证平台对VPDN用户进行认证，认证成功后双方建立安全连接；

4） VPDN用户须通过VPN设备建立的加密隧道安全连接访问政务外网业务。

附 录 B
（资料性附录）
典型部署案例

B.1 省级安全接入平台的典型部署

如图B.1所示：

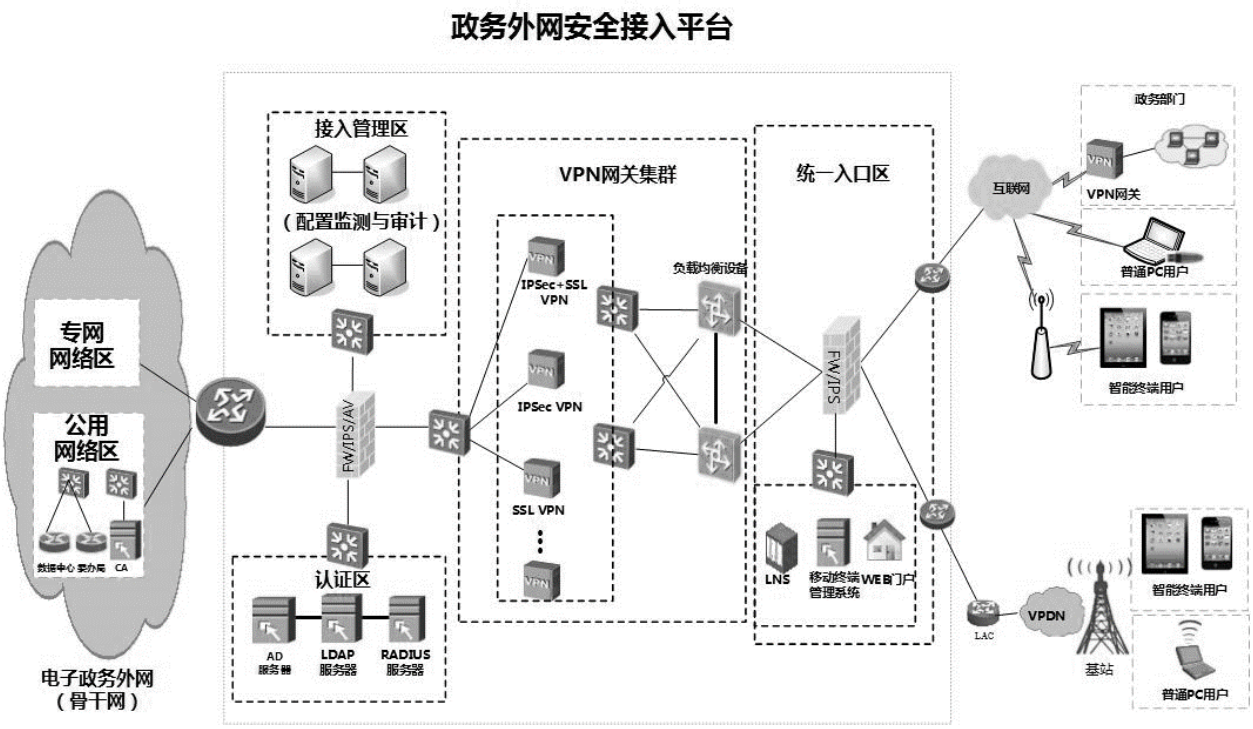


图 B.1 省级安全接入平台典型部署示意图

省级安全接入平台划分为四个区域进行部署。

1） 统一入口区由防火墙、VPDN接入所需的LNS路由器、移动终端管理系统、门户组成；防火墙实现安全接入平台的访问控制；移动终端管理系统用于接入智能终端的策略下发，远程擦除；门户提供用户注册申请、客户端软件下载、SSL VPN登录、业务异常申报等功能。

2） LNS路由器提供VPDN专线用户二次认证功能。

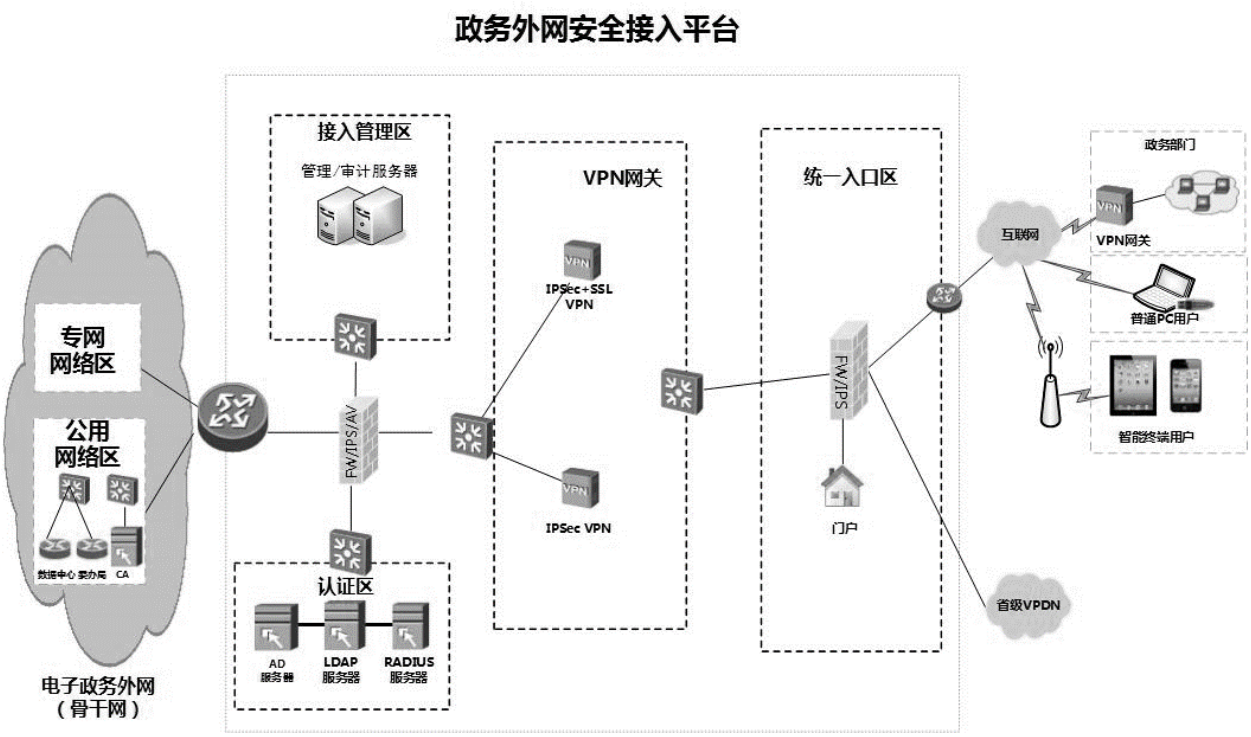
3） VPN网关集群是由IPSec VPN网关、SSL VPN网关组成的VPN网关池，实现用户的身份认证、权限管理、传输加密；负载均衡设备提供VPN网关的负载分配。

4） 接入管理区部署配置管理系统、监测系统、安全审计系统，实现平台设备的配置管理、安全接入平台的运行监测和接入用户行为审计。

5） 认证区部署LDAP、RADIUS等认证系统，实现接入用户的统一认证授权功能。如果已建设政务外网CA，LDAP可从CA导入证书条目、证书注销列表等信息用于用户证书有效性检查协助认证。

B.2 地（市）级安全接入平台的典型部署

如图B.2所示：



图B.2地（市）级安全接入平台典型部署示意图

地（市）级安全接入平台划分为四个区域进行部署。

1） 统一入口区由防火墙、门户组成；防火墙实现安全接入平台的访问控制。门户提供用户注册申请、客户端软件下载、SSL VPN登录、业务异常申报等功能，如有移动接入需求，应增加必要移动终端管理系统；

2） VPN网关由IPSec VPN网关和SSL VPN网关组成，实现用户的身份认证、权限管理、传输加密；

3） 接入管理区配置管理/审计服务器，实现VPN网关的配置管理、安全接入平台的运行监测、用户的接入审计和安全接入平台的安全审计；

4） 认证区配置LDAP、RADIUS等认证服务器，实现接入用户的统一认证功能。

地（市）VPDN用户可通过省级安全接入平台接入。

县级安全接入平台可参照地（市）级安全接入平台部署。