ICS 35.240.01
CCS L 70

DB51

四　川　省　地　方　标　准

DB 51/T 3121–2023

电子政务外网技术规范

Technical specification for E–government network

2023 – 10 – 11 发布　　2023 – 11– 12 实施

四川省市场监督管理局　发 布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

本文件由四川省大数据中心提出、归口并解释。

本文件起草单位：四川省大数据中心、成都市大数据中心、德阳市政务服务和大数据管理局、德阳市旌阳区行政审批局、德阳市旌阳区数字化中心、成都市标准化研究院、华为技术有限公司、新华三技术有限公司。

本文件主要起草人：唐志恩、周学立、陈雅维、郑 畅、谷 磊、刘 伟、杜 勇、李艳芳、杨 超、刘 欣、徐 辉、王先勇、李 超、赵 斌、赵红瑛、邓星月、吴小斌、赵紫冰、曾 艳、刘 莎、左汪敬、杨玖宏、李茂春、武 林、丰春霞、王永江、曲凯飞、陈 冉、张 勇、邹昌盛、耿文鑫、庞明君、刘林涛、王婵、张艺帆。

电子政务外网技术规范

1 范围

本文件规定了电子政务外网（以下简称政务外网）网络建设的术语与定义、缩略语、总体要求、网络技术架构、IP地址分配、自治域及路由、虚拟专用网、部门局域网接入、政务外网机房建设和运维体系建设。

本文件适用于指导四川省行政范围内，省级、市级、县级政务外网网络的设计、建设和运维管理。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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 21061 国家电子政务网络技术和运行管理规范

GB/T 22239 信息安全技术 网络安全等级保护基本要求

GB/T 25069 信息安全技术 术语

GB/T 25647 电子政务术语

GB/T 32910.3 数据中心 资源利用 第3部分：电能能效要求和测量方法

GB 50174—2017 数据中心设计规范

3 术语和定义

GB/T 25069、GB/T 25647界定的以及下列术语和定义适用于本文件。

3.1

电子政务外网 E-government network

服务于各级党委、人大、政府、政协、法院和检察院等政务部门，满足其经济调节、市场监管、社会管理和公共服务等方面需要的政务公用网络。

3.2

广域网 wide area network

用于纵向覆盖省、市、县各层级行政区域，由各级行政区域内广域骨干节点设备和节点设备之间的长途线路组成的网络。

3.3

城域网 metropolitan area network

用于实现本级行政区域内的政务部门的横向连接的网络，包括中央、省、市、县四级城域网，各级城域网通过纵向广域网实现互联。

3.4

IPv6 单栈 IPv6 single stack

网络中所有终端、网络设备仅工作在IPv6模式，其对应模式为IPv4单栈模式、IPv4和IPv6双栈模式。

3.5

威胁情报 threat intelligence

收集、评估和应用关于安全威胁、威胁分子、攻击利用、恶意软件、漏洞和漏洞指标的数据集合。

3.6

Option A 方式 Option A mode

一种MPLS/SRv6不同域之间对接的方式，即本区域边界路由器把其他区域边界路由器看作自己的VPN接入设备。

4 缩略语

以下缩略语适用于本文件。

ARP：地址解析协议（Address Resolution Protocol）
AS：自治系统（Autonomous System）
BGP：边界网关协议（Border Gateway Protocol）
BGP-LS: 边界网关协议链路状态（Border Gateway Protocol Link-state）
EVPN：下一代虚拟专用网络（Ethernet Virtual Private Network）
FlexE：灵活以太网（Flexible Ethernet）
GRE：通用路由封装协议（Generic Routing Encapsulation）
H-QoS：分层服务质量（Hierarchical Quality of Service）
IDC：互联网数据中心（Internet Data Center）
iFIT：随流检测（in-situ Flow Information Telemetry）
ISIS：中间系统到中间系统（Intermediate System to Intermediate System）
IPSec VPN：互联网协议安全协议虚拟专用网络（Internet Protocol security virtual private network）
IPv4：互联网协议第4版(Internet Protocol version 4)
IPv6：互联网协议第6版(Internet Protocol version 6)
IPv6+：基于IPv6下一代互联网的升级（IPv6 Plus）
LACP：链路汇聚控制协议（Link Aggregation Control Protocol）
LDP：标签分发协议（Label Distribution Protocol）
MPLS：多协议标记交换（Multi-Protocol Label Switching）
MSTP：多业务传送平台（Multi-Service Transport Platform）
NAT：网络地址转换（Network Address Translation）
OSPF：开放式最短路径优先（Open Shortest Path First）
OTN：光传送网（Optical Transport Network）
QoS：服务质量（Quality of Service）
RSVP-TE：基于流量工程扩展的资源预留协议（Resource Reservation Protocol-Traffic Engineering）
SDH：同步数字体系（Synchronous Digital Hierarchy）
SDN：软件定义网络（Soft Defined Network）
SLA：服务级别协议（Service Level Agreement）
SNMP：简单网络管理协议（Simple Network Management Protocol）
SRv6：IPv6段路由（IPv6 Segment Routing）
VLAN：虚拟局域网（Virtual Local Area Network）
VPN：虚拟专用网络（Virtual Private Network）
VRRP：虚拟路由冗余协议（Virtual Router Redundancy Protocol）
VRRPv3：虚拟路由冗余协议第三版（VRRP version 3）

5 总体要求

5.1 政务外网应采用扁平化网络架构，减少网络层级，并具备可扩展性、开放性和兼容性。

5.2 政务外网应具备高可用性、高可靠性、高安全性、高可管理性，并具备向 IPv6 单栈的演进能力。

5.3 省级和市级政务外网应符合 GB/T 22239 第三级安全要求，县级政务外网应符合 GB/T 22239 第二级安全要求。

6 网络技术架构

6.1 网络总体架构

政务外网骨干网络应按照省级广域网、市级广域网和县级广域网三级建设，省级广域网连接中央广域网，网络总体架构如图1所示。

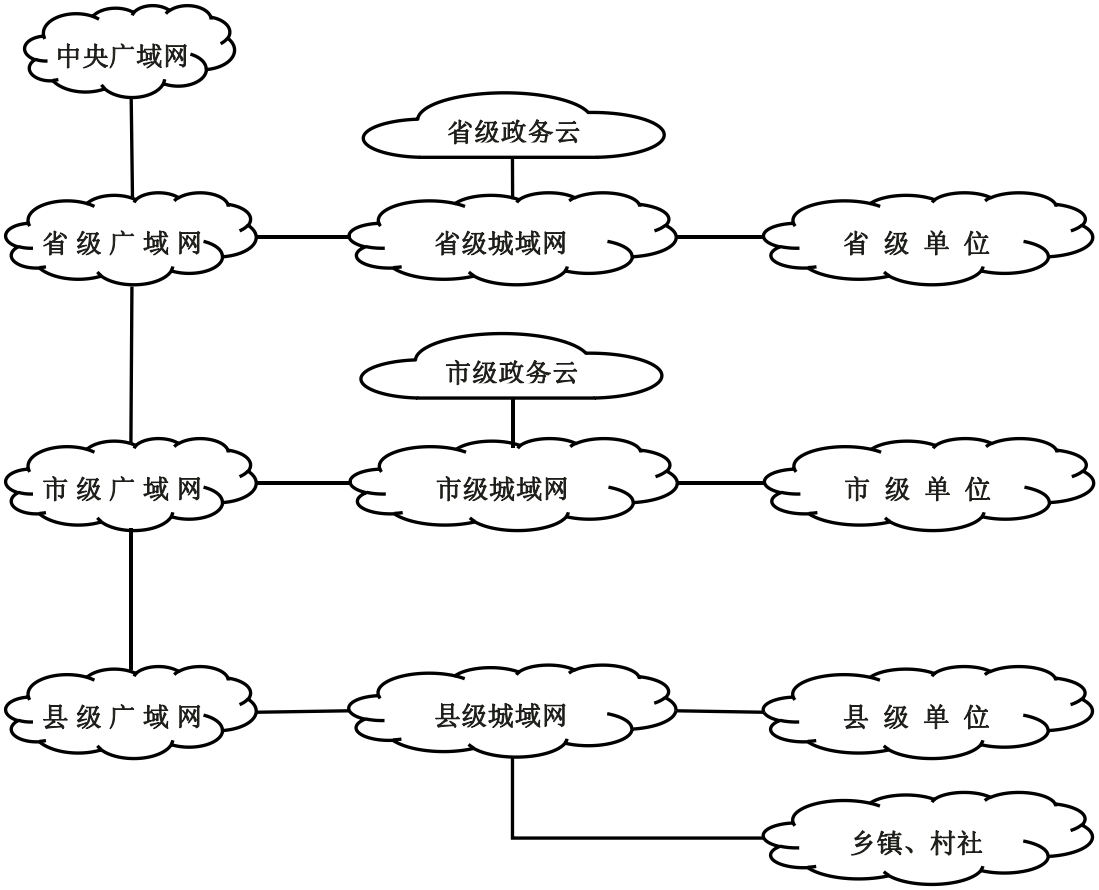

图 1 政务外网网络总体架构图

6.2 省级政务外网

6.2.1 网络架构

6.2.1.1 网络架构图

省级政务外网应分为省级广域网和省级城域网，网络架构如图2所示。

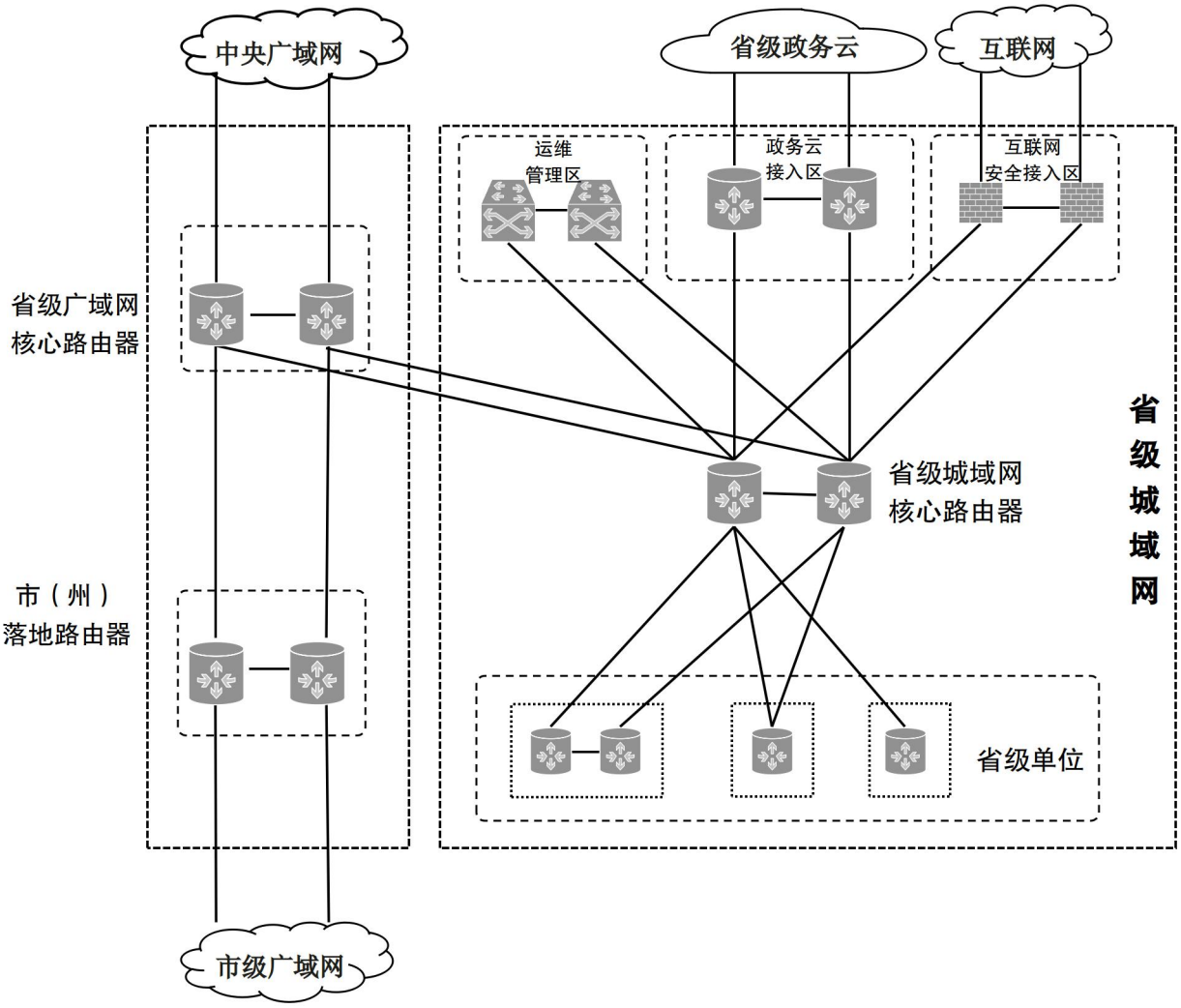

图 2　省级政务外网架构图

6.2.1.2　省级广域网

省级广域网由省–市节点的设备组成，广域网核心路由器应采用双设备冗余结构，省级广域网核心路由器纵向上连接中央广域网，向下连接市级广域网，横向连接省级城域网。

6.2.1.3　省级城域网

省级城域网扁平化部署，省级城域网核心路由器应采用冗余设备组网，主要包括但不限于以下业务区域：

a)　政务云接入区
　1)　政务云接入区用于连接本级政务云数据中心、省级部门整合云数据中心；
　2)　各数据中心宜通过专线，采用双设备双链路方式连接至政务云接入区汇聚设备。
b)　省级单位接入区
　1)　省级城域网核心路由器直连到省级广域网核心路由器，应采用冗余设备组网；

2) 接入设备应采用支持 SRv6 的路由器，满足政务外网向 IPv6 单栈演进；
3) 根据各省级接入单位业务类型和需求，可采用单线路或双线路接入。

c) 互联网安全接入区
1) 互联网安全接入区连接本地通信运营商，为不具备专线接入条件的接入单位和有移动接入需求的单位提供接入政务外网的服务；
2) 接入用户可通过互联网、移动通信网等基础网络连接到互联网安全接入区，经安全接入平台访问政务外网；
3) 安全接入平台建设应参照 GW 0202 中规定的要求，安全设备应支持国产密码算法，满足自主可控要求。

d) 运维管理区
1) 运维管理区是集中建设的独立运维管理区域，应包括运维管理平台和安全管理平台，运维管理区与城域网核心设备相连；
2) 运维管理区流量与其他网络流量逻辑隔离，宜采用带外管理；
3) 部署运维管理平台，对各网络设备进行统一运维管理，对运维管理行为进行审计；
4) 部署安全管理平台，通过流量采集、日志采集、获取威胁情报等方式，实时监测政务外网安全运行状态，智能分析安全趋势，及时对网络安全事件告警，对网络安全风险进行预警。

6.2.2 通信线路及带宽

6.2.2.1 省级广域网

建设符合以下要求：

a) 省到市（州）广域网线路总带宽应不低于 3Gbps，带宽使用率不高于 60%；
b) 省级广域网核心路由器应采用两条及以上的不同运营商的物理线路下联各市（州）落地路由器；
c) 线路类型可选择 OTN、MSTP、SDH 或裸光纤等；
d) 每年应对带宽使用率进行评估，并根据需求适时对带宽进行扩容。

6.2.2.2 省级城域网

建设应符合以下要求：

a) 省级城域网核心路由器与省级广域网核心路由器之间的连接线路总带宽应不低于 20Gbps；
b) 省级城域网核心路由器之间相互连接的线路总带宽应不低于 40Gbps；
c) 省级接入单位接入到省级城域网核心路由器的单条物理线路带宽应不低于 1Gbps；
d) 省级城域网核心路由器与政务云接入设备采用口字形互连，总带宽应不低于 20Gbps；
e) 线路类型可选择 OTN、MSTP、SDH 或裸光纤等；
f) 每年应对带宽使用率进行评估，并根据需求适时对带宽进行扩容。

6.2.3 网络设备

省级政务外网核心网络设备应支持表A.1所述功能和要求。

6.3 市级政务外网

6.3.1 网络架构

6.3.1.1 网络架构图

市级政务外网应分为市级广域网和市级城域网，网络架构如图3所示。

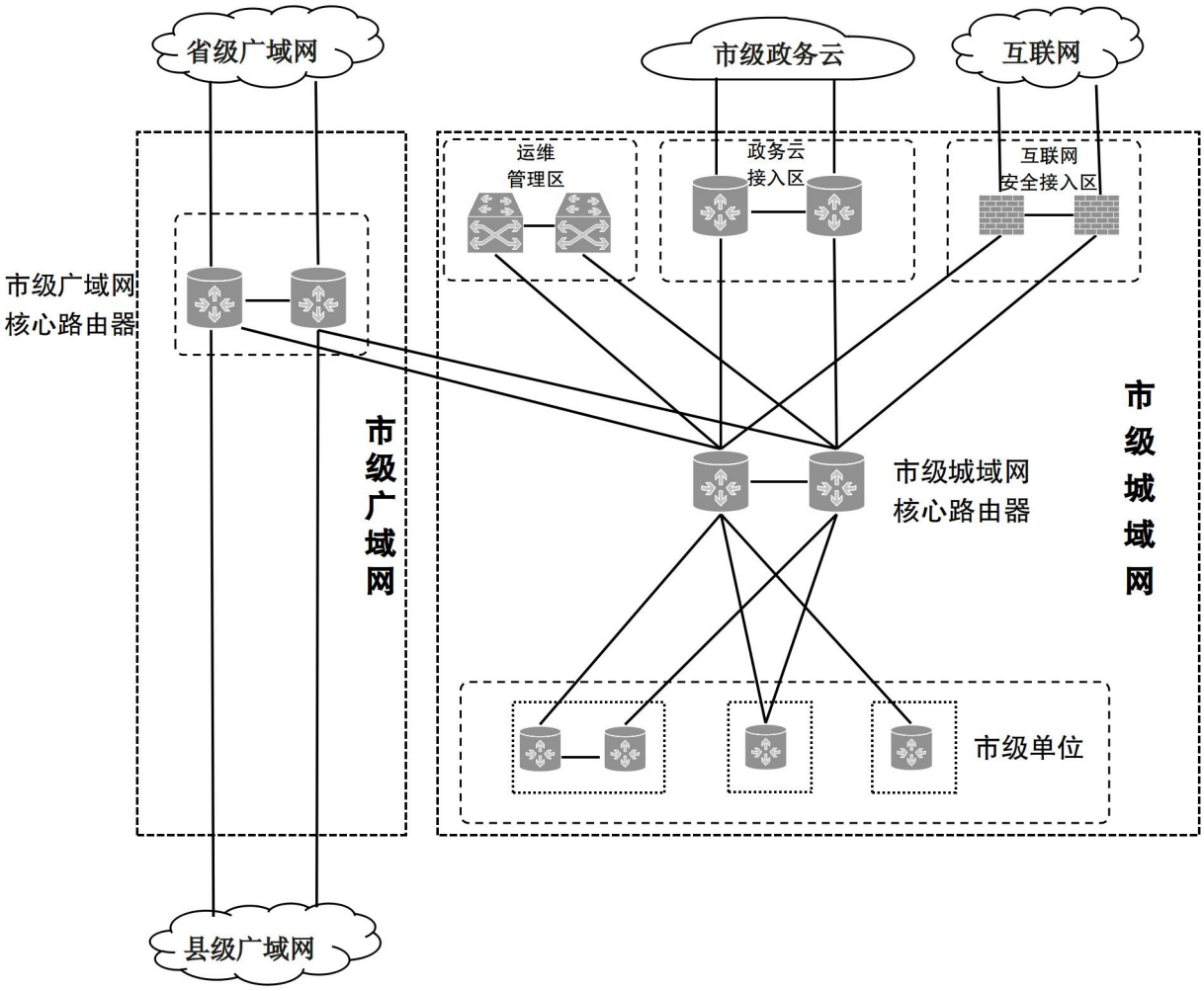

图 3　市级政务外网架构图

6.3.1.2　市级广域网

市级广域网核心路由器应采用双设备冗余结构，市级广域网核心路由器纵向上连接省级广域网，向下连接县级广域网，横向连接市级城域网。

6.3.1.3　市级城域网

市级城域网扁平化部署，市级城域网核心路由器应采用冗余设备组网，可建设如下业务区域：

a)　政务云接入区

市级政务云接入区用于连接本级政务云数据中心，政务云数据中心宜通过专线，采用双设备双链路方式连接至政务云接入区汇聚设备。

b)　互联网安全接入区

1)　互联网安全接入区连接本地通信运营商，为不具备专线接入条件的接入单位和有移动接入需求的单位提供接入政务外网的服务；

2) 接入用户可通过互联网、移动通信网等基础网络连接到互联网安全接入区，经安全接入平台访问政务外网；
3) 安全接入平台建设应参照 GW 0202 要求，安全设备应支持国产密码算法。

c) 统一互联网出口
1) 市级政务外网可根据本地实际建设统一互联网出口，为接入单位提供互联网访问服务；
2) 统一互联网出口应由两家及以上通信运营商提供互联网接入服务；
3) 统一互联网出口应配置防火墙、入侵防御、防病毒、行为审计等安全设备，应与政务外网实现逻辑隔离。

d) 运维管理区
1) 运维管理区是集中建设的独立运维管理区域，应包括运维管理平台和安全管理平台，运维管理区与城域网核心设备相连；
2) 运维管理区流量与其他网络流量逻辑隔离，条件允许的情况下，宜采用带外管理；
3) 部署运维管理平台，对各网络设备进行统一运维管理，对运维管理行为进行审计；
4) 部署安全管理平台，通过流量采集、日志采集、获取威胁情报等方式，实时监测政务外网安全运行状态，网络安全事件告警，对网络安全风险进行预警。

e) 市级单位接入区
1) 市级城域网核心路由器直连到市级广域网核心路由器，应采用冗余设备组网；
2) 接入设备应采用支持 SRv6 的路由器，满足政务外网向 IPv6 单栈演进；
3) 根据各市级接入单位业务类型和重要程度，可采用单线路或双线路接入。

6.3.2 通信链路及带宽

6.3.2.1 市级广域网

建设应符合以下要求：

a) 市级到县级广域网线路总带宽宜不低于 1Gbps；
b) 市级广域网核心路由器宜采用两条及以上不同运营商的物理线路下连各县级广域网核心路由器；
c) 线路类型可选择 MSTP、SDH 或裸光纤等；
d) 每年应对带宽使用率进行评估，并根据需求适时对带宽进行扩容。

6.3.2.2 市级城域网

建设应符合以下要求：

a) 市级城域网核心路由器与本级广域网核心路由器之间的连接线路总带宽应不低于 10Gbps；
b) 城域网核心路由器之间相互连接的线路总带宽应不低于 20Gbps；
c) 市级接入单位与城域网核心路由器之间的线路总带宽应不低于 100Mbps，宜达到 1Gbps；
d) 线路类型可选择 OTN、MSTP、SDH 或裸光纤等；
e) 每年应对带宽使用率进行评估，并根据需求适时对带宽进行扩容。

6.3.3 网络设备

市级政务外网核心网络设备应支持表A.1所述功能和要求。

6.4 县级政务外网

6.4.1 网络架构

6.4.1.1 网络架构图

县级政务外网由县级广域网核心路由器和县级城域网组成，乡镇级、村社级统一接入县级政务外网，网络架构如图4所示。

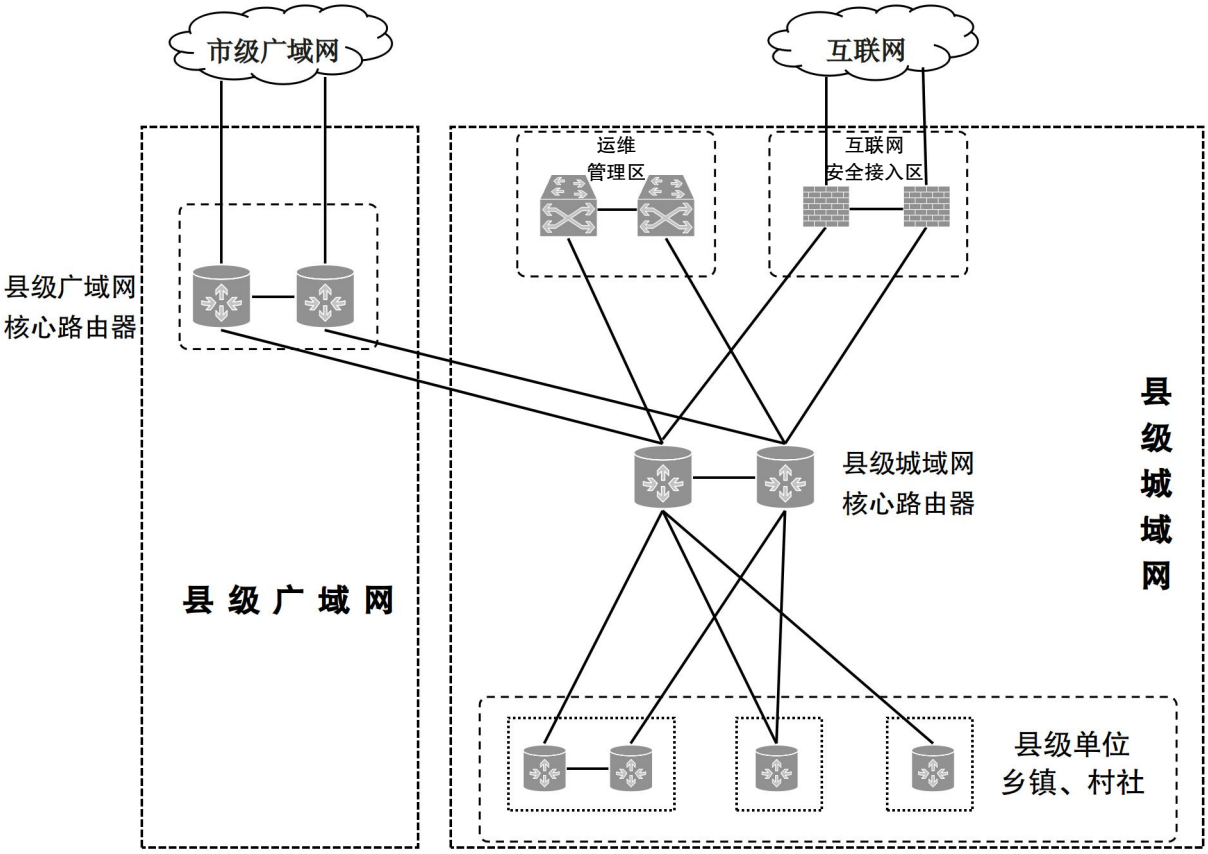

图 4 县级政务外网架构图

6.4.1.2 县级广域网

县级广域网核心路由器应采用双设备冗余结构，县级广域网核心路由器纵向上连接市级广域网，横向连接县级城域网。

6.4.1.3 县级城域网

县级城域网扁平化部署，县级城域网核心路由器应采用双设备冗余组网，县级城域网可根据实际情况建设以下业务区域：

a) 互联网安全接入区
   1) 互联网安全接入区连接本地通信运营商，为不具备专线接入条件的接入单位、不具备专线接入条件的乡镇、村社以及有移动接入需求的单位提供接入政务外网的服务；
   2) 接入用户可通过互联网、移动通信网等基础网络连接到互联网安全接入区，经安全接入平台访问政务外网；
   3) 安全接入平台建设应参照 GW 0202 要求，安全设备应支持国产密码算法。
b) 统一互联网出口

1) 县级政务外网根据本地实际可建设统一互联网出口，为接入单位、乡镇、村社提供互联网访问服务；
2) 统一互联网出口应由两家及以上通信运营商提供互联网接入服务；
3) 统一互联网出口应配置防火墙、入侵防御、防病毒、行为审计等安全设备，应与政务外网实现逻辑隔离。

c) 运维管理区
1) 运维管理区是集中建设的独立运维管理区域，应包括运维管理系统和必要的安全设备，运维管理区与城域网核心设备相连；
2) 运维管理区流量与其他网络流量逻辑隔离，条件允许的情况下，宜采用带外管理；
3) 有条件的县级政务外网可部署运维管理平台，对各网络设备进行统一运维管理，对运维管理行为进行审计；
4) 有条件的县级政务外网可部署安全管理平台，通过流量采集、日志采集、获取威胁情报等方式，实时监测政务外网安全运行状态，对网络安全事件告警，对网络安全风险进行预警。

d) 县级单位、乡镇、村社接入区
1) 根据各县级接入单位业务类型和重要程度，可采用单线路或双线路直接接入城域网核心路由器；
2) 接入设备应采用支持 SRv6 的路由器，满足政务外网向 IPv6 单栈演进；
3) 乡镇、村社统一接入县级城域网，可根据基础通信设施情况，结合业务需求，采用专线或 VPN 方式接入；
4) 采用专线接入的乡镇、村社，可根据接入数量采用直接接入城域网核心路由器或先统一汇聚后再接入城域网核心路由器；
5) 采用 VPN 方式接入的乡镇、村社，统一接入到互联网安全接入区。

6.4.2 通信链路及带宽

建设应符合以下要求：

a) 县级城域网核心路由器与本级广域网核心路由器之间的连接线路总带宽应不低于 10Gbps；
b) 县级城域网核心路由器之间相互连接的线路总带宽应不低于 10Gbps；
c) 城域网接入层设备与核心层设备之间的线路总带宽应不低于 100Mbps；
d) 线路类型可选择 MSTP、SDH 或裸光纤等；
e) 每年应对带宽使用率进行评估，并根据需求适时对带宽进行扩容。

6.4.3 网络设备

县级政务外网核心网络设备应支持表A.1所述功能和要求。

7 IP 地址分配

7.1 地址管理

IP地址的总体规划应由省级政务外网管理单位负责，并符合以下要求：

a) 省级政务外网管理单位负责全省政务外网 IP 地址分配工作；
b) 市级政务外网管理单位负责本级及以下网络 IP 地址资源的二次分配和管理工作；

c) 各级接入单位接入政务外网使用的 IP 地址原则上向本级政务外网管理单位申请，乡镇、村社接入单位接入政务外网使用的 IP 地址向县级政务外网管理单位申请；
d) IP 地址规划和分配要求参照 GW 0207 和 GW 0209 的规定执行。

7.2 分配原则

政务外网IP地址分配应遵循如下原则：
a) 政务外网 IP 地址的分配应以省、市（州）、县（市、区）为基本单元，市（州）及其下辖县（市、区）分配使用的地址段应连续；
b) 分配给同一接入单位的地址段应连续，应符合 IP 地址 VLSM（变长子网掩码）原则，确有特殊需求的，由接入单位提出申请。

7.3 IPv4 地址

7.3.1 地址类型

政务外网IPv4地址应分为全局业务地址、设备管理地址和省内地址三大类：
a) 全局业务地址是用于部署供全网访问的应用系统及广义服务设备（包括 IP 存储、MCU、视频终端等）的 IP 地址，包括国家各部委要求部署的国家到省、市、县特殊纵向业务（如视频会议系统），各级节点对省、国家发布的公共业务，各级政务云相关应用系统，接入单位出口 NAT 资源池等；
b) 设备管理地址作为网络设备全局管理地址，主要用于网络设备的互联和管理；
c) 省内地址主要用于访问省内政务外网节点，不能直接访问省外政务外网，跨省访问需使用 NAT 技术将 10 段地址转换为 59 段地址。

7.3.2 地址转换

政务外网地址转换应遵循如下原则：
a) 宜在用户接入端网络边界设备做地址转换，在分配给用户的地址段中取 1 个 59 段地址作为转换地址池，用于单个用户单位访问政务外网；
b) 如市级或县级政务外网统一做地址转换，可在边界设备或核心设备上实现地址转换，在本级 59 段地址范围内选择若干个连续 IP 地址作为转换地址池，用于城域网内各接入单位访问政务外网；
c) 地址转换设备的地址转换记录日志应保存 180 天以上，宜设立专用的日志服务器进行存储。

7.3.3 虚拟专网地址

虚拟专网区内的IP地址由业务应用部门负责规划，原则上不得采用59地址段、100地址段和10地址段。

7.4 IPv6 地址

政务外网网络及安全设备应支持IPv6协议，IPv6地址编址参照GW 0209。

8 自治域及路由

8.1 自治域

政务外网组建独立自治系统，采用全局AS号，自治域号码范围为64905—64934，自治域号码分配原则如下：

a) 各市级政务外网自治域号码由省级政务外网管理单位在国家规划的基础上进行统一管理和二次分配；
b) 政务外网自治域号码不应重复。

8.2 路由

路由设计应反映整个网络的层次结构，并与自治域、各地子网的IP地址分配相契合，具体要求如下：

a) 政务外网域内路由协议宜采用静态路由、OSPF 或者 ISIS，域间路由协议宜采用 BGP；
b) 路由应支持向 IPv6 单栈演进，可采用 IPv6+方案，基于 SRv6 技术同时承载 IPv4、IPv6 业务，宜采用支持 SDN 的网络架构。

9 虚拟专用网

9.1 总体要求

虚拟专用网是政务外网内部采用MPLS VPN、SRv6 VPN、IPsec VPN或网络切片等技术将各业务隔离构建的虚拟网络，为有特殊需求的纵向或横向业务系统提供专网服务，政务外网应支持跨域对接，具备支撑省、市、县三级纵向虚拟专用网的能力。

9.2 MPLS 或 SRv6 VPN 技术

为满足不同接入单位的业务承载需求，可在政务外网基础网络之上构建不同的业务虚拟专用网，具体要求如下：

a) 省、市、县三级纵向虚拟专用网的规划部署由省级政务外网管理单位统一负责；
b) 省、市、县级路由器的管理、配置和维护由本级政务外网管理单位负责；
c) 虚拟专网业务跨域对接宜采用 Option A 方式。

9.3 部门自建 IPsec VPN 技术

政务部门可根据自身需求，依托政务外网建设自有IPsec VPN隧道，并满足以下要求：

a) IPsec VPN 业务由用户部门自行建设和维护；
b) 政务外网应支持承载 IPsec VPN 业务；
c) 建设技术规范应参照 GW 0201 的规定执行。

9.4 网络切片技术

9.4.1 采用技术原则

对政务外网中敏感数据和SLA要求高的业务，可采用网络切片技术，将网络划分为多个独立的逻辑业务平面，每个逻辑业务平面应拥有独立的带宽资源，形成虚拟专用网，可根据业务类型、保障级别定义网络切片模型，宜采用基于业务类型的分类。

9.4.2 基于业务类型分类

根据业务类型分为四类切片，即政务服务、视频监控、视频会议、办公服务，见表1。

表 1 基于业务类型的网络切片

切片类型	业务描述
政务服务	各政务单位对外服务，如社保、公积金、车管等各类服务
视频监控	各级部门视频监控业务的接入和调阅服务
视频会议	各级政务部门内、部门之间高品质视频会议通讯服务
办公服务	各级政务部门办公、具有统一互联网出口的政务外网为用户提供互联网访问服务

9.4.3 基于保障级别分类

网络保障级别分为1、2、3级，保障要求见表2，单位/业务都可以按照3个级别根据用户需求基于网络切片进行保障。

表 2 基于保障级别的网络切片

保障等级	保障要求
1级	共享带宽，网络时延<30ms，丢包率<10^{-3}，抖动<20ms
2级	保障带宽，网络时延<10ms，丢包率<10^{-4}，抖动<10ms
3级	独享带宽，网络时延<5ms，丢包率<10^{-5}，抖动<5ms

10 部门局域网接入

10.1 局域网接入架构

接入单位接入政务外网，应采用防火墙等安全设备做到安全隔离与防护，结构见图5。

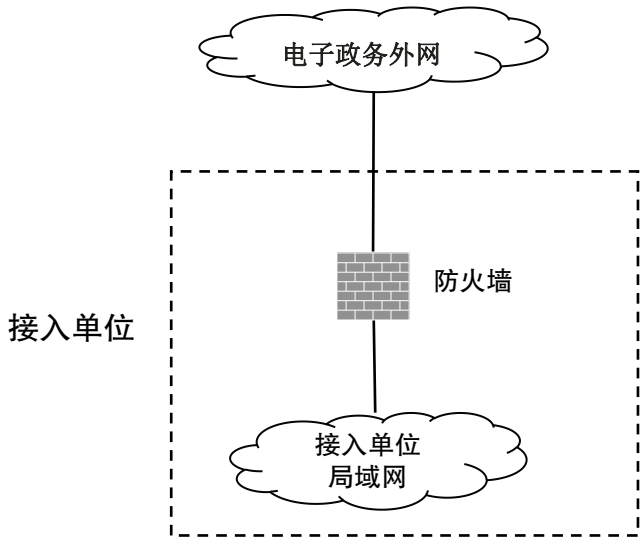

图 5 局域网接入架构图

10.2 局域网接入

接入政务外网的局域网应满足以下要求：

a) 防火墙由接入单位提供，主要有两个用途：
   1） 逻辑隔离：配置安全访问策略，将接入单位局域网与政务外网进行安全隔离；
   2） 地址转换：将接入单位局域网内部地址转换成政务外网IP地址。
b) 互联网隔离要求：如接入单位有独立互联网出口，则互联网和政务外网之间应通过安全设备做到逻辑隔离和安全防护。

10.3 终端

终端应满足以下要求：

a) 接入单位应采用安全技术手段，阻止非法用户接入政务外网；
b) 终端管理由各接入单位负责；
c) 移动智能终端接入政务外网应参照 GW 0206 标准要求。

11 政务外网机房

应满足以下要求：

a) 机房节能应符合 GB/T 32910.3 的规定，电能能效要求和测量方法中的一级节能要求或同类标准要求；
b) 机房应支持多家运营商线路接入；
c) 机房可采用自建、租用具备独立管理区域的 IDC 机房等方式；
d) 省级政务外网机房标准应符合 GB 50174—2017 中 A 级要求或同类标准要求；
e) 市级政务外网节点机房标准应符合 GB 50174—2017 中 B 级要求或同类标准要求；
f) 县级和其他政务外网机房的基础设施应按基本需求配置，在基础设施正常运行情况下，应保证政务外网运行不中断。

12 运维监测体系

12.1 网络运维体系

网络运维体系建设应遵循如下原则：

a) 运维管理平台应具备如下能力：
   1) 对政务外网运行状态的监控，包括对网络设备、安全设备、主机、存储设备、数据库、中间件、应用系统等进行集中监控和管理；
   2) 采集各类告警数据、性能数据和配置数据，进行统一的分析、查询、报告和展示；
   3) 建立故障管理、问题管理、变更管理、配置管理等服务工作流程；
b) 运维管理平台建设应符合 GB/T 21061 相关要求；
c) 省级和市级政务外网应建设本级运维管理平台，县级政务外网可建设本级运维管理平台；
d) 本级运维管理平台应与上级运维管理平台进行对接，上报相关运行数据。

12.2 安全监测体系

建设省-市两级安全监测平台，对运行环境、网络设备、安全设备、操作系统、应用系统等资源进行实时安全监测，形成覆盖省、市、县政务外网三级安全监测体系，并符合以下要求：

a) 安全监测平台建设技术规范应参照 GW 0203 标准要求；
b) 安全监测平台的对接要求可参照 GW 0204 等；
c) 省级和市级政务外网应建设本级安全监测平台；
d) 具备建设条件的县级政务外网可建设本级安全监测平台，不具备建设条件的县级政务外网纳入所属市级安全监测平台进行统一监测；
e) 本级安全监测平台应与上级平台进行对接，将监测信息上报给上级安全监测平台，上报信息包括但不限于：设备运行状态、风险状况、安全策略修改情况、漏洞、告警、重大安全事件、合规性分析以及信息安全统计指标等信息；
f) 下级安全监测平台可从上级平台中获取相关推送信息。

附 录 A
（规范性）
政务外网核心网络设备要求

政务外网核心网络设备要求见表A.1。

表 A.1 政务外网核心网络设备要求表

项目	技术要求	
业务板接口类型	支持所选择的通信链路	
网络互连	局域网协议	支持以太网协议、基本VLAN等
	链路层协议	支持LACP等
网络协议	IP服务	支持ARP、IP包过滤、策略路由等
	IP路由	支持OSPF、OSPFv3、IS-IS、 IS-ISv6、BGPv4、BGP4+等
	IPv6特性	支持IPv6的IP服务和IP路由功能
业务隧道	SRv6	支持SRv6-TE Policy，SRv6 BE等协议和转发能力
	MPLS	支持LDP、RSVP-TE等MPLS标签分发协议
	VPN	支持GRE、BGP-VPN、BGP-EVPN、MPLS VPN等
设备可靠性	冗余	双主控、电源模块冗余
	其他特性	支持VRRP、VRRPv3
服务质量保障	QoS	支持层次化QoS（H-QoS）
	网络切片	支持FlexE、信道化子接口
	业务质量检测	支持iFIT随流检测技术
网络管理	管理协议	支持SDN、Telemetry、BGP-LS、SNMP等

参 考 文 献

[1] GW 0015—2022 政务外网终端一机两用安全管控技术指南
[2] GW 0201 国家电子政务外网IPsec VPN安全接入技术要求与实施指南
[3] GW 0202 国家电子政务外网安全接入平台技术规范
[4] GW 0203 国家电子政务外网安全监测体系技术规范与实施指南
[5] GW 0204 国家电子政务外网安全管理系统技术要求与接口规范
[6] GW 0206 接入政务外网的局域网安全技术规范
[7] GW 0207 国家电子政务外网IPv4地址地方分配部署指南
[8] GW 0209 国家电子政务外网IPv6地址规划（试行版）
[9] 政务外网安全监测平台基本数据定义和级联接口技术要求（V2.0）
[10] GB/T 21064 电子政务系统总体设计要求
[11] GB/T 30850.3 电子政务标准化指南 第3部分：网络建设