

上海市电子政务外网建设和运行管理指南

（试行）

上海市大数据中心
二〇二〇年三月

目 录

一、	引言	5
1.1	编写目的	5
1.2	编写依据	5
1.3	适用范围	6
1.4	缩略语	6
1.5	解释权	7
二、	总体架构	7
2.1	政务外网“1+16”体系	7
2.2	政务外网总体架构	8
2.3	光传输网络架构	9
2.4	业务网络架构	9
三、	电子政务外网建设规范	10
3.1	市级电子政务外网设计规范	10
3.1.1	光传输网络设计规范	10
3.1.2	业务网络设计规范	12
3.2	区电子政务外网设计规范	16
3.2.1	光传输网络设计规范	16
3.2.2	业务网络设计规范	17
3.3	市、区两级网络互联互通规范	21
3.3.1	光传输网络互联互通	21
3.3.2	业务网络互通	22
3.4	网络安全设计规范	23
3.4.1	总体规范	23
3.4.2	环境和设备安全建设规范	24
3.4.3	业务网络边界安全建设规范	25
3.4.4	安全管理中心建设规范	34
3.4.5	安全监测系统建设规范	38
3.5	IPv6 网络设计规范	39
3.5.1	总体规范	39

3.5.2	IPv6 网络方案设计	39
3.6	网络高可靠设计规范	41
3.6.1	总体规范	41
3.6.2	双平面可靠性设计规范	42
3.7	服务质量设计规范	43
3.7.1	QoS 设计原则.....	43
3.7.2	QoS 部署方案.....	44
3.8	网络管理设计规范	45
3.8.1	总体规范	45
3.8.2	网络管理	45
3.8.3	网络控制	48
3.8.4	网络分析	49
3.9	IP 地址规划和管理	49
3.9.1	IPv4 地址规划和管理	49
3.9.2	IPv6 地址规划和管理	50
3.10	DNS 域名规划和管理	58
3.10.1	域名规划和管理总体要求.....	58
3.10.2	域名结构规范.....	58
3.10.3	域名流程管理.....	59
3.10.4	域名安全防护规范.....	59
3.11	IP 路由协议	60
3.11.1	路由策略总体要求.....	60
3.11.2	IGP 路由实施.....	60
3.11.3	BGP 路由实施.....	61
3.11.4	互联网出口路由实施.....	61
3.11.5	管理路由和业务路由部署.....	61
四、	电子政务外网运行管理规范	61
4.1	运行管理单位的职责	62
4.1.1	服务受理	62
4.1.2	网络监控	62
4.1.3	技术支持	62
4.2	运行管理单位的服务内容	63

4.2.1	服务受理	63
4.2.2	网络监控	63
4.2.3	安全管理	63
4.2.4	变更管理	64
4.2.5	故障处理	65
4.2.6	故障处理升级	65
4.2.7	故障报告	66
4.2.8	资源管理	66
4.2.9	性能管理	66
4.2.10	报告管理.....	66
4.2.11	服务质量管理控制.....	67
4.3	运行和安全监测支撑系统规范	67
4.3.1	系统架构	68
4.3.2	主要功能	68
4.3.3	网络协同维护	71

一、 引言

1.1 编写目的

为深入贯彻网络强国战略思想，发挥信息化对经济社会发展的引领作用，高水平适应信息时代对政务网络基础设施的新要求，做强电子政务外网“全市一张网”，支撑上海政务服务“一网通办”、城市运行“一网统管”现代化治理体系建设，提升城市治理现代化水平，依据《国家电子政务外网建设总体规划》和《上海市公共数据和一网通办管理办法》等文件，按照国家“通过统一规划、进一步推进政务外网建设、加强协同服务，统一安全策略，尽快形成统一、完整、安全、高效的政务外网”的要求，进一步推进网络互通、数据共享、应用协同，结合我市实际，特编制本指南。

1.2 编写依据

- 1) 《国家发展改革委关于加强和完善国家电子政务工程建设管理的意见》（发改高技术〔2013〕266号）
- 2) 《国务院办公厅关于加强政府网站域名管理的通知（国办函〔2018〕55号）》
- 3) 《关于印发〈公共安全视频图像信息联网共享应用标准体系（2017版）〉和〈公共安全视频图像信息交换共享体系IP地址规划〉的通知》（中综秘〔2017〕3号）
- 4) 《推进互联网协议第六版（IPv6）规模部署行动计划》（中央办公厅，国务院办公厅，2017年11月26日）
- 5) 《IP网络技术要求网络总体》（YD/T 1170-2001）
- 6) 《国家电子政务外网IPv4地址规划》（GW0206-2015）
- 7) 《国家电子政务外网建设总体规划》（国家信息中心2009年9月）
- 8) 《国家电子政务外网IPv6地址规划（2019版）》
- 9) 《国家电子政务外网信息安全标准体系总体框架》（GW0101-2014）
- 10) 《国家电子政务外网安全等级保护基本要求》（GW0103-2014）
- 11) 《国家电子政务外网安全等级保护实施指南》（GW0104-2014）
- 12) 《国家电子政务外网安全监测体系技术规范与实施指南》（GW0203-2014）
- 13) 《信息安全技术网络安全等级保护基本要求》（GB/T 22239-2019）
- 14) 《信息安全技术网络安全等级保护安全设计技术要求》（GB/T 25070-2019）

- 15) 《信息安全技术网络安全等级保护测评要求》(GB/T 28448-2019)
- 16) 《政务网络安全监测平台总体技术要求》(T/CIIA 005-2019)
- 17) 《计算站场地安全要求》(GB/T 9361-2011)
- 18) 《计算机场地通用规范》(GB/T 2887-2011)
- 19) 《信息技术服务 运行维护 第1部分:通用要求》(GB/T 28827.1-2012)
- 20) 《信息技术服务 运行维护 第2部分:交付规范》(GB/T 28827.2-2012)
- 21) 《国家电子政务外网运维管理系统对接规范》
- 22) 《上海市公共数据和一网通办管理办法》(上海市人民政府令2018年第9号)
- 23) 《上海市人民政府办公厅关于进一步加强本市政务网站域名管理工作的通知》

1.3 适用范围

本指南作为上海市电子政务外网的技术规范建议和指导手册,适用于政务外网的建设及日常的运行维护和管理工作。

1.4 缩略语

- IPv4 网际协议版本4 (Internet Protocol version 4)
- IPv6 网际协议版本6 (Internet Protocol version 6)
- MPLS 多协议标记交换 (Multi-Protocol Label Switching)
- NAT 网络地址转换 (Network Address Translation)
- IGP 内部网关协议 (Interior Gateway Protocol)
- IS-IS 中间系统-中间系统协议 (Intermediate System-to-Intermediate System)
- OSPF 开放式最短路径优先 (Open Shortest Path First)
- BGP 边界网关协议 (Border Gateway Protocol)
- AS 自治系统 (Autonomous System)
- PE 服务提供商边缘路由器 (Provider Edge)
- VRRP 虚拟路由冗余协议 (Virtual Router Redundancy Protocol)
- Diffserv 区分服务 (Differentiated Services)
- DNS 域名系统 (Domain Name System)
- ECMP 等价多路径 (Equal-Cost Multipath Routing)
- UCMP 非等值负载分担 (Unequal Cost Multipath Routing)

FRR 快速重路由 (Fast Reroute)

QoS 服务质量 (Quality of Service)

H-QoS 层次化服务质量 (Hierarchical Quality of Service)

IPS 入侵防御系统 (Intrusion Prevention System)

DDoS 分布式拒绝服务 (Distributed Denial of Service)

IPSec IP安全协议 (IP Security)

VPN 虚拟专用网络 (Virtual Private Network)

VRF 虚拟路由转发 (Virtual Routing Forwarding)

VLAN 虚拟局域网 (Virtual Local Area Network)

VxLAN 虚拟可扩展局域网 (Virtual Extensible LAN)

SR 分段路由 (Segment Routing)

SRv6 IPv6段路由 (IPv6 Segment Routing)

SDN 软件定义网络 (Soft Defined Network)

LAC L2TP访问集中器 (L2TP Access Concentrator)

LNS L2TP网络服务器 (L2TP Network Server)

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

VPDN 虚拟私有拨号网络 (Virtual Private Dialup Networks)

OTN 光传送网 (Optical Transport Network)

SDH 同步数字体系 (Synchronous Digital Hierarchy)

1.5 解释权

本文档解释权归属于上海市大数据中心。

二、 总体架构

2.1 政务外网“1+16”体系

上海市电子政务外网按照“全市一张网”的建设要求，以“1+16”的总体架构进行设计，“1”指一张市级电子政务外网，“16”指16张区级电子政务外网。市、区两级电子政务外网遵循统一建设标准及运行管理规范，与互联网逻辑隔离，采用“一网双平面”架构，即数据平面承载数据流量，视频平面承载视频流量，在政务外网上逻辑隔离、独立运行、互为备份。

市级电子政务外网上联国家电子政务外网，下联16个区级电子政务外网，覆盖市级各部门、部分国有企业、医院和大专院校；区级电子政务外网上联市级政务外网，并覆盖区级各部门、街镇和村居。

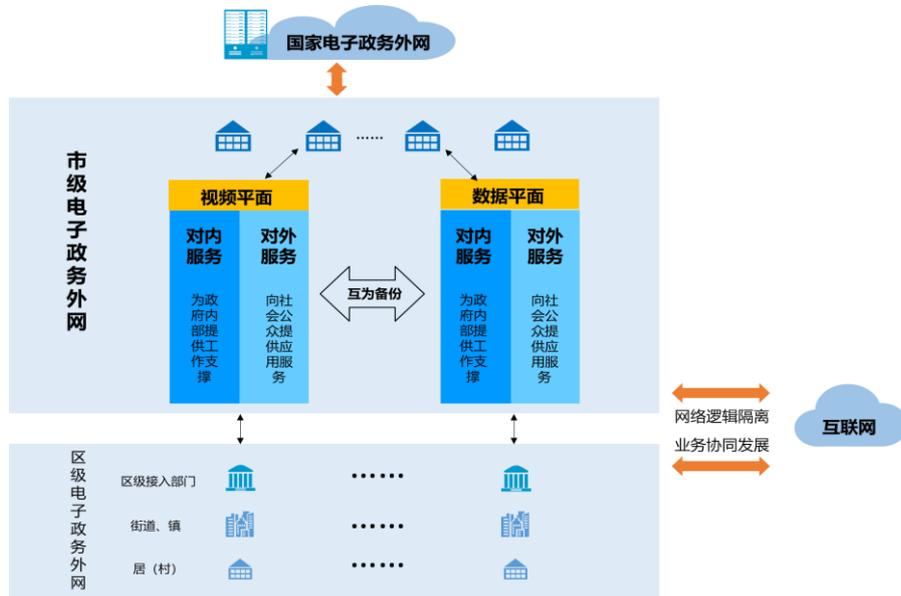


图1 上海市电子政务外网体系图

2.2 政务外网总体架构

上海市电子政务外网由底层光传输网络和上层业务网络组成。

在政务外网的重要节点采用光传输设备组建底层光传输网络。光传输设备在一对光纤中同时传输多个波长，有效提升光纤的传输容量，并提供光纤链路的自动保护和恢复能力，解决政务外网裸光纤接入光纤利用率不足、自愈保护能力差、业务调度缺乏灵活性问题。

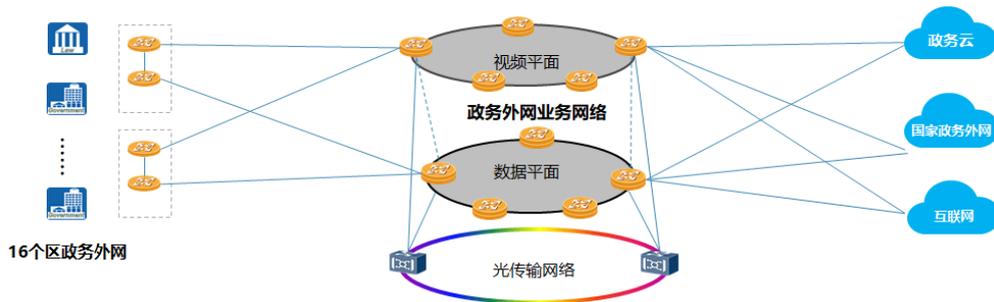


图2 上海市电子政务外网总体架构图

上层业务网络基于IP技术，采用数据平面和视频平面构建互为备份的“一网双平面”架构。数据平面、视频平面互为备份，故障时数据平面、视频平面可实现冗余保护，确保政务外网业务的灵活调度和稳定可靠运行。

2.3 光传输网络架构

光传输网络采用OTN技术组网，为上层业务网络提供大带宽、低时延、高可靠的传输通道，通过光链路保护、资源可视化、光监控等功能，提升业务网络的传输安全和网络运维管理能力。

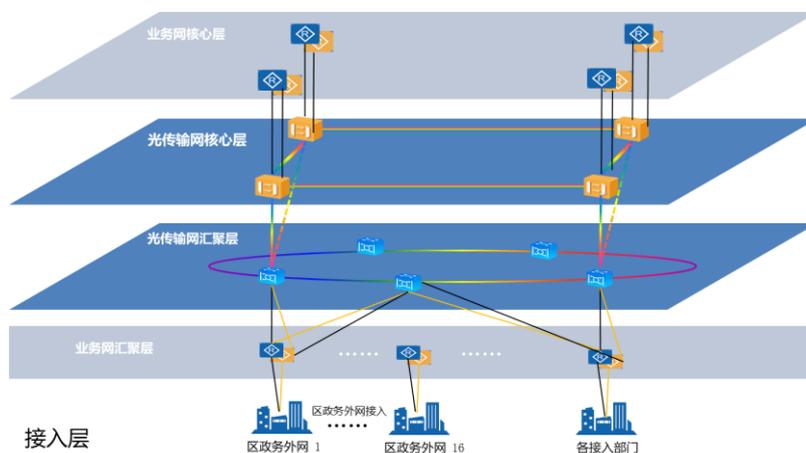


图3 上海市电子政务外网光传输网络架构图

光传输网络应采用分层组网架构进行设计，分为核心层、汇聚层、接入层。核心节点、汇聚节点的设置，可根据政务外网接入单位的物理位置分布、机房和光纤链路资源的配置等因素酌情选择。

接入层可采用单个接入节点直连至汇聚节点的方式组网，或多个接入节点与汇聚节点成环的方式组网。

2.4 业务网络架构

政务外网业务网络采用分层架构设计，在网络层次上分为核心层、汇聚层、接入层。

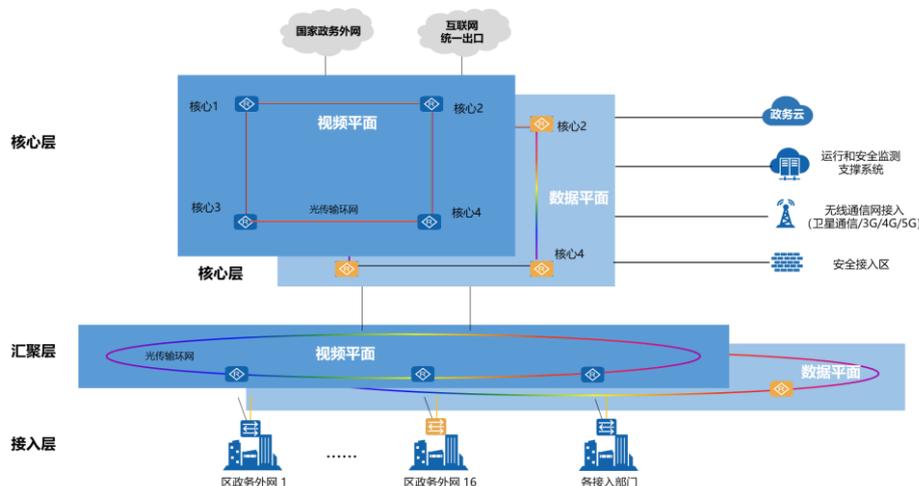


图4 上海市电子政务外网业务网络架构图

核心层主要承担高速数据交换的任务，同时提供到上一级政务外网和互联网的连接。政

政务外网与互联网之间采用安全技术逻辑隔离。

为提升网络可靠性，政务外网应至少设置两个或两个以上核心节点，并确保各个核心节点部署在不同物理位置的机房。

汇聚层主要将来自接入层的访问进行集中和汇聚，承担路由聚合和访问控制的功能。汇聚层节点的位置、数量选择可基于机房、传输资源及网络接入点的地理位置分布等因素酌情考虑。

接入层主要提供政务外网各使用单位的网络接入。市政务外网业务网络提供16个区级政务外网及市级各部门网络的接入，区政务外网业务网络提供各区级部门、街镇和村居的接入。

接入层网络采用单链路或双链路上行的方式接入政务外网业务网络汇聚层。

在政务外网建立安全接入区（分无线通信网安全接入区、安全接入区等），满足部分机构、部门通过卫星通信网、3G/4G/5G移动通信网等网络资源接入政务外网以进行数据交换的需求。

三、 电子政务外网建设规范

3.1 市级电子政务外网设计规范

3.1.1 光传输网络设计规范

3.1.1.1 光传输网络技术规范

光传输网应具备与现有网络的兼容能力，具体要求如下：

1. 采用单波速率100G及以上的OTN技术；
2. 支持带宽平滑扩容，网络具备向200G及以上带宽平滑扩容的能力；
3. 采用高可用的组网架构，具备网络自愈能力，能为各类政务应用提供安全可靠的传输网络支撑；
4. 采用保护路径和工作路径物理光纤分离的保护策略，端到端保护倒换时间小于50ms；
5. 具有SDH、分组、OTN等多种业务统一承载的能力，能提供多种业务类型接口的接入能力，具备与已建网络互联互通的能力；
6. 支持光纤线路诊断功能，能快速定位光纤线路故障；
7. 宜采用SDN技术，实现对业务和链路的快速下发和调整；
8. 应使用G. 652或G. 655规格的光缆，光缆的每公里线路衰耗在0.3dB以下。

3.1.1.2 核心节点设计

核心节点设计规范：

1. 核心节点设计要考虑未来带宽持续增长的可能性，所选择的设备要具备带宽易扩容的特点，设备宜支持集群功能；
2. 核心节点之间互联应采用高可用的组网架构，确保两个核心节点间有多条链路可达，提升网络可靠性；
3. 核心层节点设备的光层宜使用业务灵活调度的技术，减少网络组网和运维的复杂度；
4. 核心节点之间开通两个不同路由的光传输通道，对传输的业务进行冗余保护。

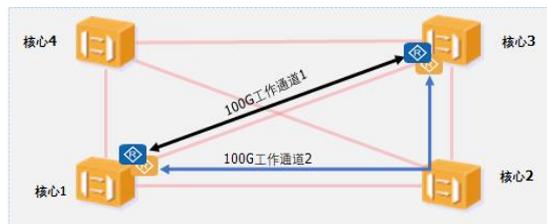


图5 光传输网络核心层组网示意图

3.1.1.3 汇聚节点设计

汇聚节点设计规范如下：

1. 汇聚节点设备选型应充分考虑机房环境的复杂性和多样性，设备需要具备低功耗，高集成度的特点，支持多样化的机房电源、机柜、空间等环境；
2. 汇聚节点之间应采用环形组网架构，每个汇聚点到相邻的核心节点之间均开通两个不同路由的光传输通道。



图6 光传输网络汇聚层组网示意图

3.1.1.4 传输设备技术规范

特性	详细描述
交叉功能	具备OTN、分组、SDH交叉功能
业务类型	FE/GE/10GE/40GE/100GE、STM-N(1/4/16/64)业务接入；单波100G速率传输；
光模块	eSFP、SFP+、SFP28、CFP、CFP2、QSFP+、QSFP28
可靠性	电源冗余、风扇冗余、交叉冗余、通信控制与时钟单元冗余；支持OTN、分组、SDH网络级保护；

3.1.2 业务网络设计规范

3.1.2.1 业务网络技术规范

政务外网业务网络应满足各接入点汇聚接入及灵活互通的需求，具体要求如下：

1. 业务网络采用核心、汇聚、接入的三层架构设计；
2. 业务网络的核心、汇聚层应承载于政务外网光传输网络之上；
3. 业务网络采用“一网双平面”的架构设计。数据平面承载网络数据流量，视频平面承载网络视频流量，两个平面在政务外网上逻辑隔离、独立运行，且互为冗余备份；
4. 应基于TCP/IP技术构建政务外网业务网络，采用支持IPv4/IPv6双栈技术的网络设备；
5. 业务网络应符合等保2.0规范的要求；
6. 应保证不同应用在业务网络的相互独立，可选用VLAN、VxLAN、VPN、网络切片等方式实现不同业务的隔离；
7. 应从多个维度考虑设备的安全自主可控，采用国产领先的网络和安全设备、系统；
8. 应采用SDN技术，实现业务快速部署，流量工程和智能流量调整能力；
9. 应基于大数据分析技术和智能检测技术，对网络中不同业务的运行状态、服务质量，做到实时监控、主动运维；

3.1.2.2 通信链路设计

上海市电子政务外网市级业务网络带宽设计如下：

链路类型	速率
核心节点之间	100Gbps
与国家电子政务外网之间	N×1Gbps 或 N×10Gbps
核心节点与下级汇聚节点之间	100Gbps
同一汇聚节点内主备冗余设备之间	100Gbps
汇聚节点与下级接入节点之间	N×1Gbps 或 N×10Gbps

3.1.2.3 核心节点设计

核心节点设计规范如下：

1. 核心层设备承担用户流量安全、高速、可靠转发的功能；
2. 核心节点设备选型应能满足面向未来业务发展平滑扩展的需要；
3. 核心节点应采用高冗余设计，保证核心网络的高可靠性。

实际设计时，核心节点数应不少于2个，每个核心节点应部署不少于两台高端路由器设备，两台设备之间不少于100G互相冗余。不同核心节点之间应有多条冗余链路，核心节点之间互联带宽应不少于100G。

3.1.2.4 汇聚节点设计

汇聚节点连接核心节点与接入节点，采用双归方式接入核心节点以提高网络可靠性。按各接入点地理位置的分布情况设置汇聚节点。每个汇聚节点部署两台高端路由器设备，两台设备之间设置带宽为100Gbps的互联链路。

汇聚节点向上通过100Gbps链路分别连接至两个核心节点，向下通过N×1Gbps或N×10Gbps链路连接各区电子政务外网，通过N×1Gbps或N×10Gbps链路连接各市级部门接入点。

3.1.2.5 接入节点设计

各区政务外网的接入设备以N×1Gbps或N×10Gbps链路连接至汇聚节点。

市级接入部门的接入设备以N×1Gbps或N×10Gbps链路连接至汇聚节点。

各市级接入节点根据实际情况选择单设备单链路、单设备双链路、或双设备双链路作为上行方式。

3.1.2.6 网络设备技术规范

1. 核心、汇聚节点设备功能要求:

特性	核心路由器	汇聚路由器
接口类型	100GE/40GE/10GE	100GE/40GE/10GE/GE/FE
IPv4	IPv4静态路由、OSPF、IS-IS、BGP等路由协议，VxLAN、GRE等隧道技术	
IPv6	IPv6静态路由，BGP4+、OSPFv3、IS-ISv6等动态路由协议，IPv4 over IPv6隧道和6PE，NAT444、NAT64，静态IPv6 DNS，指定IPv6 DNS服务器，TFTP IPv6 client	
MPLS	L2VPN、L3VPN、EVPN，LDP LSP、RSVP-TE等MPLS技术，宜支持SR-TE	
SR	宜支持如下SR技术：单域及跨BGP域的Segment Routing技术，Segment Routing与LDP混合组网，SR policy技术，SRv6承载VPN业务，SR的TI-LFA FRR技术，BFD for SR、BFD for SRv6	
可靠性	BFD故障探测技术，误码倒换，IP/IPv6/LDP/TE/VPN/VPNv6 FRR快速重路由，端口聚合，ECMP、UCMP，LDP，VRRP，NSR，关键部件冗余备份，组件可热拔插，平滑重启（GR），不中断转发（NSF），ISSU	
QoS	多级MPLS H-QoS，MPLS VPN、VLL和PWE3的QoS调度，面向TE隧道的QoS	
OAM	基于IP五元组筛选追踪业务流，对丢包、误码类故障进行实时检测，精准定位到故障点；支持EFM、CFM、Y.1731、MPLS-TP OAM技术	
其它特性	国密算法，BGP-LS、PCEP南向协议；基于Telemetry的大数据分析	

2. 防火墙设备功能要求:

特性	详细描述
接口类型	GE/10GE/40GE/100GE
基本特性	应用层协议识别、应用层包过滤（ASPF）、访问控制、状态合法性检测、地址转换NAT、黑白名单、虚拟防火墙、MPLS L3VPN、DHCPv6、ICMPv6、MLD、ND
链路/服务器负载均衡	基于ISP的路由、智能选路、链路健康检查、基于应用的QoS等（加权）轮询算法、（加权）最小连接算法、（加权）会话保持算法、服务器健康检查等
应用安全	IPS入侵防御、AV防病毒、URL过滤、文件过滤、SSL代理

特性	详细描述
地址转换	NAT44(4)、NAT64、PCP、溯源方案
IPsec VPN	手动密钥、PKI (X. 509)、IKEv2、冗余VPN网关、EAP认证、IKEv2重定向
DDoS攻击防护	SYN Flood、ICMP Flood、UDP Flood等多种DoS和DDoS攻击防范
部署及可靠性	透明、路由、混合等部署模式；主/主、主/备模式备份；双主控倒换

3. APT防御系统功能要求：

特性	详细描述
协议解析	HTTP、FTP、SMTP、POP3、IMAP4、NFS、SMB等协议的流量还原
检测文件类型	OFFICE、PE、ELF、PDF、RTF、JAVA、CHM、IMAGE (tiff、bmp、gif、jpg等)、COMPRESS (ZIP、TAR等)、HTML、JS、SCRIPT、CSS等
检测威胁类型	恶意广告软件、后门程序、病毒、漏洞利用、灰色软件、蠕虫、间谍软件、木马/僵尸网络、勒索软件、黑客工具、Rookit、钓鱼等
检测算法	Shellcode检测；文件威胁行为分类展示；文件输出动态行为进程树；基于进程主机行为与网络行为分析安全风险
攻击取证	提取出攻击释放及下载的样本文件；基于恶意样本网络行为的PCAP文件及下载
情报能力	与威胁情报系统周期更新行为库

4. SDN控制器功能要求：

特性	详细描述
IP/MPLS连接自动化	VPN专线业务自动化发放；支持对物理设备、网络隧道、VPN等的发现
资源可视	物理拓扑、逻辑拓扑可视；隧道拓扑可视；VPN业务拓扑可视；链路、隧道、VPN的连通性检测；网络资源、隧道路径、业务路径、及业务SLA的可视可管
网络优化	广域链路智能调优；MPLS隧道全局优化算路和单业务路径优化
接口开放	Restful、Netconf、SNMP等接口协议；网络运维、优化、业务所需的北向API
高可用性	本地保护和异地容灾部署；主备业务的数据一致性

3.2 区电子政务外网设计规范

3.2.1 光传输网络设计规范

3.2.1.1 光传输网络技术规范

光传输网应具备与现有网络兼容的能力，具体要求如下：

1. 采用单波速率100G及以上的OTN技术；
2. 支持带宽平滑扩容，网络具备向200G及以上带宽平滑扩容的能力；
3. 采用高可用的组网架构，具备网络自愈能力，能为各类政务应用提供安全可靠的传输网络支撑；
4. 采用保护路径和工作路径物理光纤分离的保护策略，端到端保护倒换时间小于50ms；
5. 具有SDH、分组、OTN等多种业务统一承载的能力，能提供多种业务类型接口的接入能力，具备与已建网络互联互通的能力；
6. 支持光纤线路诊断功能，能快速定位光纤线路故障；
7. 宜采用SDN技术，实现对业务和链路的快速下发和调整；
8. 应使用G. 652或G. 655规格的光缆，光缆的每公里线路衰耗在0.3dB以下。

3.2.1.2 核心节点设计

核心节点设计规范：

1. 核心层传输网络设计时需要考虑与市级政务外网传输网络的对接，核心节点设备应遵循业界统一标准，具备开放性的特点；
2. 核心节点设备选型应充分考虑机房环境的复杂性和多样性，设备需要具备低功耗，高集成度的特点，支持多样化的机房电源、机柜、空间等环境；
3. 核心节点之间的互联应采用高可用的组网架构，相邻核心节点之间开通两个不同路由的光传输通道，保证两点间多链路可达，对传输的业务进行冗余保护。

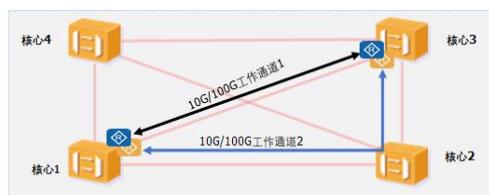


图7 光传输网络核心层组网示意图

3.2.1.3 汇聚节点设计

汇聚节点设计规范：

1. 核心节点设备选型应充分考虑机房环境的复杂性和多样性，设备需要具备低功耗，高集成度的特点，支持多样化的机房电源、机柜、空间等环境；
2. 汇聚节点之间应采用环形组网架构，每个汇聚节点到相邻的核心节点之间均开通两个不同路由的光传输通道。

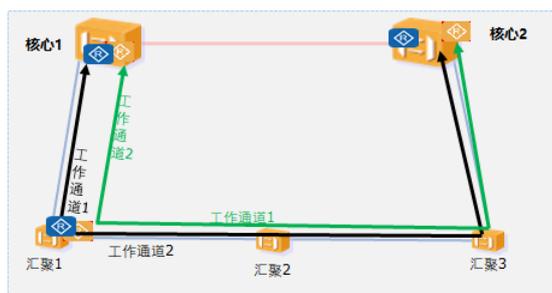


图8 光传输网络汇聚层组网示意图

3.2.1.4 传输设备技术规范

特性	详细描述
交叉功能	具备OTN、分组、SDH交叉功能
业务类型	FE/GE/10GE/40GE/100GE、STM-N(1/4/16/64)业务接入；单波10G/100G速率传输；
光模块	eSFP、SFP+、SFP28、CFP、CFP2、QSFP+、QSFP28
可靠性	电源冗余、风扇冗余、交叉冗余、通信控制与时钟单元冗余；支持OTN、分组、SDH网络级保护；

3.2.2 业务网络设计规范

3.2.2.1 业务网络技术规范

区政务外网业务网络应满足各接入单位网络汇聚接入及灵活互通的需求，具体要求如下：

1. 业务网络采用核心、汇聚、接入的三层架构设计；
2. 业务网络的核心、汇聚层应承载于政务外网光传输网络之上；
3. 业务网络采用“一网双平面”的架构设计。数据平面承载网络数据流量，视频平面

承载网络视频流量，两个平面在政务外网上逻辑隔离、独立运行，且互为冗余备份；

4. 应基于TCP/IP技术构建政务外网业务网络，采用支持IPv4/IPv6双栈技术的网络设备；

5. 业务网络应符合等保2.0规范的要求；

6. 应保证不同应用在业务网络的相互独立，可选用VLAN、VxLAN、VPN、网络切片等方式实现不同业务的隔离；

7. 应从多个维度考虑设备的安全自主可控，采用国产领先的网络和安全设备、系统；

8. 应采用SDN技术，实现业务快速部署，流量工程和智能流量调整能力；

9. 应基于大数据分析技术和智能检测技术，对网络中不同业务的运行状态、服务质量，做到实时监控、主动运维；

3.2.2.2 通信链路设计

区电子政务外网业务网络带宽设计如下：

链路类型	速率
核心节点之间	40~100Gbps
与市电子政务外网之间	N×1Gbps 或 N×10Gbps
核心节点与下级汇聚节点之间	40~100Gbps
同一汇聚节点内主备冗余设备之间	40~100Gbps
汇聚节点与下级接入节点之间	N×1Gbps 或 N×10Gbps

3.2.2.3 核心节点设计

核心节点设计规范：

1. 核心层设备承担用户流量安全、高速、可靠转发的功能；
2. 核心节点设备选型应能满足面向未来业务发展平滑扩展的需要；
3. 核心节点应采用高冗余设计，保证核心网络的高可靠性。

实际设计时，核心节点数应不少于2个，每个核心节点应部署不少于两台路由器设备，两台设备之间40Gbps~100Gbps链路互相冗余。不同核心节点之间应有多条冗余链路，核心节点之间互联带宽应不少于100Gbps。

3.2.2.4 汇聚节点设计

汇聚节点设计规范：

1. 汇聚节点采用双归方式接入核心节点以提高网络可靠性。汇聚节点向上通过40~100Gbps链路连接核心节点，向下通过N×1Gbps链路或N×10Gbps链路连接区级各部门、街镇和村居；

2. 每个汇聚节点部署两台路由器设备，两台设备之间互联链路的带宽应与汇聚节点至核心节点的链路带宽相同。

3.2.2.5 接入节点设计

区政务外网的接入节点通过N×1Gbps或N×110Gbps链路联接至汇聚节点。

各接入单位根据实际情况选择单设备单链路、单设备双链路，或双设备双链路作为上行方式。

3.2.2.6 网络设备技术规范

1. 核心、汇聚节点设备功能要求：

特性	核心路由器	汇聚路由器
接口类型	100GE/40GE/10GE/GE	100GE/40GE/10GE/GE/FE
IPv4	IPv4静态路由、OSPF、IS-IS、BGP等路由协议，VxLAN、GRE等隧道技术	
IPv6	IPv6静态路由，BGP4+、OSPFv3、IS-ISv6等动态路由协议，IPv4 over IPv6隧道和6PE，NAT444、NAT64，静态IPv6 DNS，指定IPv6 DNS服务器，TFTP IPv6 client	
MPLS	L2VPN、L3VPN、EVPN，LDP LSP、RSVP-TE等MPLS技术，宜支持SR-TE	
SR	宜支持如下SR技术：单域及跨BGP域的Segment Routing技术，Segment Routing与LDP混合组网，SR policy技术，SRv6承载VPN业务，SR的TI-LFA FRR技术，BFD for SR、BFD for SRv6	
可靠性	BFD故障探测技术，误码倒换，IP/IPv6/LDP/TE/VPN/VPNv6 FRR快速重路由，端口聚合，ECMP、UCMP，LDP，VRRP，NSR，关键部件冗余备份，组件可热拔插，平滑重启（GR），不中断转发（NSF），ISSU	

特性	核心路由器	汇聚路由器
QoS	多级MPLS H-QoS, MPLS VPN、VLL和PWE3的QoS调度, 面向TE隧道的QoS	
OAM	基于IP五元组筛选追踪业务流, 对丢包、误码类故障进行实时检测, 精准定位到故障点; 支持EFM、CFM、Y.1731、MPLS-TP OAM技术	
其它特性	国密算法, BGP-LS、PCEP南向协议; 基于Telemetry的大数据分析	

2. 防火墙设备功能要求:

特性	详细描述
接口类型	GE/10GE/40GE/100GE
基本特性	应用层协议识别、应用层包过滤(ASPF)、访问控制、状态合法性检测、地址转换NAT、黑白名单、虚拟防火墙、MPLS L3VPN、DHCPv6、ICMPv6、MLD、ND
链路/服务器负载均衡	基于ISP的路由、智能选路、链路健康检查、基于应用的Qos等(加权)轮询算法、(加权)最小连接算法、(加权)会话保持算法、服务器健康检查等
应用安全	IPS入侵防御、AV防病毒、URL过滤、文件过滤、SSL代理
地址转换	NAT44(4)、NAT64、PCP、溯源方案
IPsec VPN	手动密钥、PKI(X.509)、IKEv2、冗余VPN网关、EAP认证、IKEv2重定向
DDoS攻击防护	SYN Flood、ICMP Flood、UDP Flood等多种DoS和DDoS攻击防范
部署及可靠性	透明、路由、混合等部署模式; 主/主、主/备模式备份; 双主控倒换

3. APT防御系统功能要求:

特性	详细描述
协议解析	HTTP、FTP、SMTP、POP3、IMAP4、NFS、SMB等协议的流量还原
检测文件类型	OFFICE、PE、ELF、PDF、RTF、JAVA、CHM、IMAGE(tiff、bmp、gif、jpg等)、COMPRESS(ZIP、TAR等)、HTML、JS、SCRIPT、CSS等
检测威胁类型	恶意广告软件、后门程序、病毒、漏洞利用、灰色软件、蠕虫、间谍软件、木马/僵尸网络、勒索软件、黑客工具、Rookit、钓鱼等
检测算法	Shellcode检测; 文件威胁行为分类展示; 文件输出动态行为进程树; 基于进程主机行为与网络行为分析安全风险
攻击取证	提取出攻击释放及下载的样本文件; 基于恶意样本网络行为的PCAP文件及下载

特性	详细描述
情报能力	与威胁情报系统周期更新行为库

4. SDN控制器功能要求：

特性	详细描述
IP/MPLS 连接自动化	VPN专线业务自动化发放；支持对物理设备、网络隧道、VPN等的发现
资源可视	物理拓扑、逻辑拓扑可视；隧道拓扑可视；VPN业务拓扑可视；链路、隧道、VPN的连通性检测；网络资源、隧道路径、业务路径、及业务SLA的可视可管
网络优化	广域链路智能调优；MPLS隧道全局优化算路和单业务路径优化
接口开放	Restful、Netconf、SNMP等接口协议；网络运维、优化、业务所需的北向API
高可用性	本地保护和异地容灾部署；主备业务的数据一致性

3.3 市、区两级网络互联互通规范

3.3.1 光传输网络互联互通

区级电子政务外网光传输网在与市电子政务外网光传输网互通时，应能通过电层客户侧接口对接。电层客户侧接口对接有两种形式：

1. 通过传输设备的电层客户侧接口（GE/10GE/100GE，FC等）直接对接；
2. 两方的传输设备，各自通过GE/10GE/100GE接口，联接至指定的路由器或交换机设备，在该设备上完成对接。

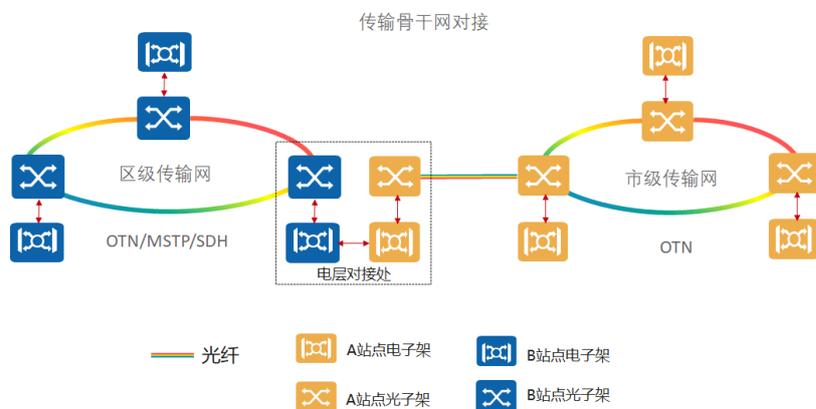


图9 光传输网络电层客户侧接口对接示意图

3.3.2 业务网络互通

3.3.2.1 互联互通架构设计

市、区两级政务外网业务网络的互联互通应通过市级政务外网提供的接入设备完成。

该接入设备与区政务外网的出口设备放置于同一机房，两者通过光纤直联。

该接入设备宜通过 $N \times 10\text{Gbps}$ 链路与市政务外网的汇聚交换机联接，宜通过 $N \times 1\text{Gbps}$ 或 $N \times 10\text{Gbps}$ 链路与区政务外网的出口设备联接。

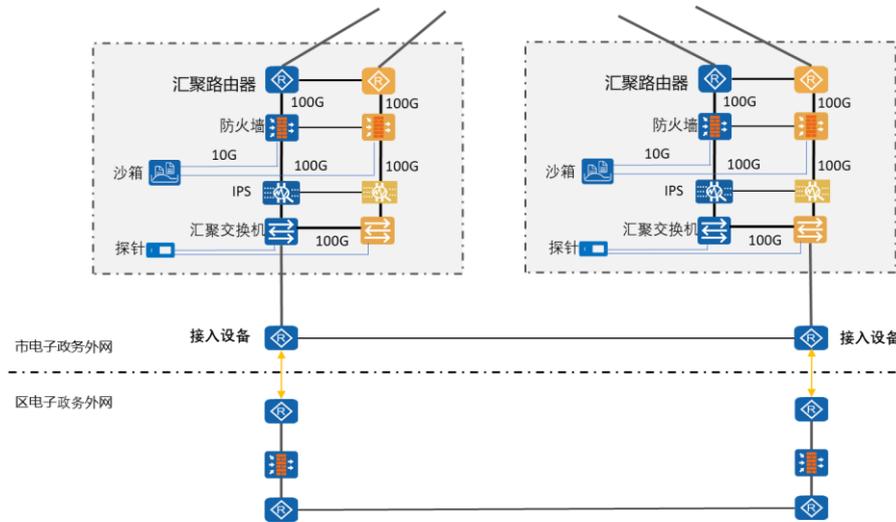


图10 市、区两级政务外网互联互通示意图

区级电子政务外网与市级电子政务外网的互联互通，应设置有安全接入区，并符合国家等保2.0的三级规范要求。

安全接入区应包含但不限于出口路由器、入侵防御、防火墙、防病毒等功能设备，实现：

1. 区级政务外网业务网络应与市级政务外网的业务网络实现视频平面、数据平面的分别互联互通；
2. 应对不同的业务应用提供QOS和路由策略保障；
3. 根据等保2.0规范的要求，配置防火墙及沙箱等安全部件，对流经的流量进行安全检测，以及实现对异常流量的采集。

3.3.2.2 互联互通技术规范

市、区两级政务外网的建设应采用标准、开放的架构和协议，确保两级政务外网的高效、稳定互通。具体要求如下：

1. 选用IS-IS/IS-ISv6、OSPF/OSPFv3、BGP (BGP4+) 作为互联协议；
2. 选用MPLS VPN、VLAN、VxLAN、EVPN、网络切片等技术实现不同政务业务子网的逻辑隔离；
3. 可选用OTN光传输网络进行市、区两级政务外网的对接；
4. 应通过SDN技术实现智能路径计算和流量调优功能，网络和应用流量的精细化管理和分析；
5. 宜采用支持SR MPLS或SRv6技术的网络设备，宜支持SR BE、SR TE、SR Policy、SR的TI-LFA FRR、BFD for SR等协议和技术。

3.4 网络安全设计规范

3.4.1 总体规范

政务外网各接入单位应在符合国家安全等级保护要求的前提下方能接入政务外网，并参照等保2.0规范的等级防护能力要求，匹配相应的网络安全防护措施：

等级	适用信息系统及行业	安全防护能力
第二级 (指导保护级)	<ul style="list-style-type: none"> ➤ 街道、镇、居(村)级单位中的重要信息系统； ➤ 区级以上国家机关、企事业单位内部一般的信息系统。 	应能免受来自外部小型组织的、拥有少量资源的威胁源发起的恶意攻击、一般的自然灾害、以及其他相当危害程度的威胁所造成的重要资源损害，能够发现重要的安全漏洞和处置安全事件，在自身遭到损害后，能够在一段时间内恢复部分功能。
第三级 (监督保护级)	<ul style="list-style-type: none"> ➤ 区级以上国家机关、企业、事业单位内部重要的信息系统； ➤ 全国联网运行的用于生产、调度、管理、指挥、作业、控制等方面的重要信息系统及这类系统在上海市的分支系统； ➤ 上海市门户网站和重要网站； ➤ 跨上海市连接的网络系统等。 	应能免受来自外部有组织的团体、拥有较为丰富资源的威胁源发起的恶意攻击、较为严重的自然灾害、以及其他相当危害程度威胁所造成的主要资源损害，能够及时发现、监测攻击行为和处置安全事件，在自身遭到损害后，能够较快恢复绝大部分功能。

上海市电子政务外网的安全防护体系由安全管理中心、业务网络边界安全、环境和设备

安全三个方面建设实现。

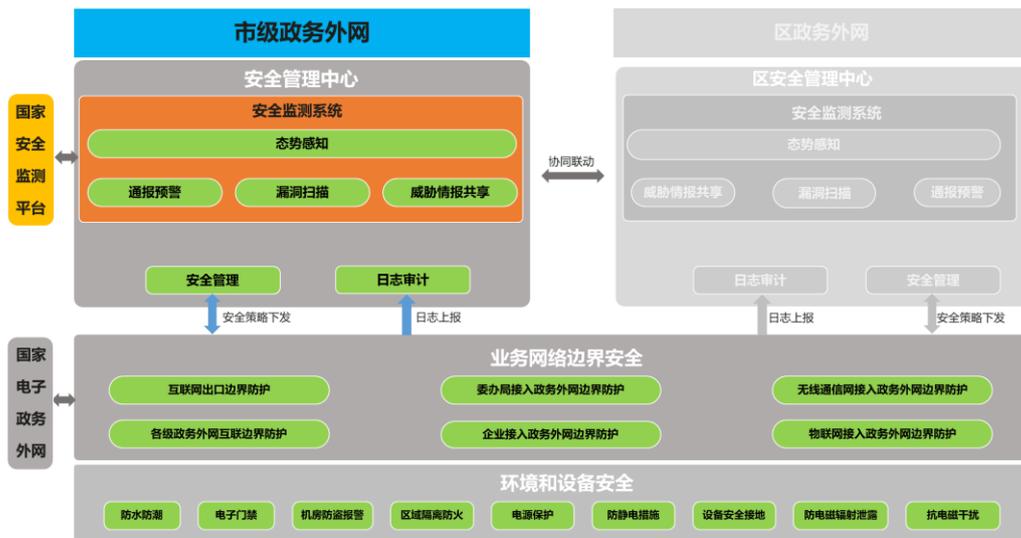


图11 政务外网安全架构图

安全管理中心包括态势感知、漏洞扫描、威胁情报共享、通报预警、安全管理和日志审计共6个子系统。其中态势感知、通报预警、漏洞扫描、威胁情报共享是国家电子政务外网要求的安全监测系统的重要组成部分。市级安全监测系统需要与国家安全监测系统以及各区级安全监测系统完成对接，实现安全事件的协同联动。

对于区级安全管理中心，威胁情报共享和漏洞扫描可以不单独建设，可选择使用市级安全监测系统提供的服务。

业务网络边界安全包括互联网出口边界防护、各级政务外网互联边界防护、各接入部门接入政务外网的边界防护、无线通信网接入政务外网的边界防护等模块。市、区两级政务外网的业务网络安全体系建设都需要遵循《信息安全技术网络安全等级保护测评要求》相关标准和规定。

对于环境和设备安全，需要考虑网络机房的防水、防潮、防火、防静电、防电磁干扰，同时机房需要有相对应的防盗、报警措施、视频监控和电子门禁系统。

3.4.2 环境和设备安全建设规范

上海市电子政务外网核心、汇聚机房的供配电系统、空调系统，在防静电、防雷、消防，防水等方面的建设，必须符合《信息安全技术网络安全等级保护测评要求》（GB/T 28448-2019）的规范要求。

- 机房选址

政务外网核心、汇聚机房地选择在具有防震、防风和防雨等能力的建筑内。机房场地应避免设在建筑物的顶层或地下室，以及用水设备的下层或隔壁。

- 机房管理

政务外网核心、汇聚机房出入口应配置电子门禁系统，控制、鉴别和记录进入的人员；

- 机房环境

政务外网核心、汇聚机房应合理规划设备安装位置，应预留足够的空间作安装、维护及操作之用。房间装修必需使用阻燃材料，耐火等级符合国家相关标准规定。机房门大小应满足系统设备安装时运输需要。机房墙壁及天花板应进行表面处理，防止尘埃脱落，机房应安装防静电活动地板。

机房安装防雷和接地线，设置防雷保安器，防止感应雷，要求防雷接地和机房接地分别安装，且相隔一定的距离；机房设置火灾自动消防系统，能够自动检测火情、自动报警，并自动灭火；机房及相关的工作房间和辅助房应采用具有耐火等级的建筑材料；机房应采取区域隔离防火措施，将重要设备与其他设备隔离开。应配备空调系统，以保持房间恒湿、恒温的工作环境；在机房供电线路上配置稳压器和过电压防护设备；提供短期的备用电力供应，UPS 应该满足在断电情况下工作 2 小时的运行要求。宜配置冗余或并行的电力电缆线路为计算机系统供电；建立备用供电系统。铺设线缆要求电源线和通信线缆隔离铺设，避免互相干扰。对关键设备和磁介质实施电磁屏蔽。

- 设备与介质管理

政务外网各级机房必须采用有效的区域监控、防盗报警系统，阻止非法用户的各种临近攻击。

3.4.3 业务网络边界安全建设规范

3.4.3.1 分级分域保护原则

上海市电子政务外网应根据联接网络对象的不同，以及承载信息系统的安全等级的不同，划分不同的安全区域和边界，并根据等保2.0规范相关要求，实施不同强度的安全保护。

3.4.3.2 网络边界划分

市、区两级政务外网应将如下区域划定为安全边界，并部署符合等保2.0三级规范要求的安全设备，予以保护：

第一类区域：政务外网到互联网的接入边界，防范从互联网对政务外网的攻击；

第二类区域：各级政务外网互联的边界，如市级政务外网到国家级政务外网、区级政务外网到市级政务外网的边界，防范非法跨级用户对政务外网的非授权访问；

第三类区域：各单位政务网接入到对应市、区政务外网的边界，防范非法跨网用户对政务外网的非授权访问；

第四类区域：3G、4G、5G以及卫星通信等无线网络接入到政务外网的边界，防范非法无线网络用户对政务外网的非授权访问；

第五类区域：部分机构、部门等单位接入到政务外网的边界，防范非法接入单位用户对政务外网的非授权访问；

3.4.3.3 互联网接入区的安全规范

互联网接入区需实现抗DDoS攻击、网络访问控制、入侵检测和防御、防病毒、APT检测、日志审计等功能，如下图所示：

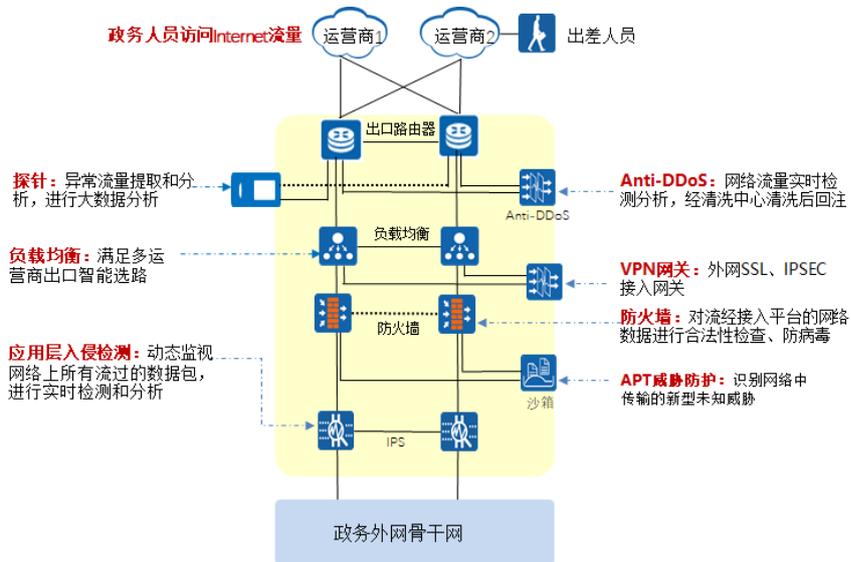


图12 互联网出口区安全设计

互联网接入区域，需要满足以下技术规范：

(1) 抗DDoS攻击

应在互联网接入区部署抗DDoS攻击设备，需要支持DDoS检测和清洗。抗DDoS攻击需

要支持常见的SYN Flood、ACK Flood、FIN/RST Flood功能，能抵抗HTTP、HTTPS Flood等攻击，并且支持流量自学习功能，可识别出超过防御阈值的攻击流量。

(2) 网络访问控制

应在互联网接入区部署防火墙，实现网络边界保护和访问控制功能。防火墙应只开放政务外网提供接入服务必需的服务端口，对流经互联网接入区域的网络数据进行合法性检查。为了保证业务的可服务性，防火墙需要双机部署，且支持性能的可扩容。防火墙需要支持IPv6协议栈、NAT64转换技术。

(3) 入侵检测和防御

宜在互联网接入区部署入侵防御系统，动态检测网络上所有流过的数据包，进行实时检测和分析，及时发现漏洞、蠕虫、木马等非法和异常行为，并且支持告警、阻断等功能。

(4) 防病毒

应在互联网接入区部署防病毒网关，及时更新病毒库，阻止病毒入侵和传播，进行及时的查杀。防病毒模块可以集成在防火墙内。

(5) APT检测

宜在互联网接入区旁路部署沙箱，针对APT高级持续威胁，利用沙箱多引擎虚拟检测技术，以及传统的安全检测技术，识别网络中传输的恶意文件和C&C攻击。沙箱应支持和防火墙联动以实现对威胁的实时阻断。

(6) VPN网关

宜在互联网接入区部署VPN网关，针对从互联网接入的远程办公用户提供SSL、IPSec等形式的VPN接入网关功能。VPN网关需支持国密算法。

(7) 探针

宜在互联网接入区部署探针，对流经网络边界的流量进行提取和还原，送至后端大数据分析系统进行安全分析，识别潜在安全攻击风险。

(8) 日志审计

支持日志审计和管理，支持日志统一格式输出，报表自动生成，支持图形化展示，并要求审计日志至少保存6个月。设备清单参考：

安全场景模块	各场景子模块	各模块所需软硬件	市级电子政务外网	区级电子政务外网
业务网络边界区	政务外网到互联网的出口边界	Anti-DDoS设备	必配	必配
		防火墙	必配	必配
		入侵检测与防御硬件	必配	必配
		防病毒硬件	必配	必配
		沙箱	选配	选配
		VPN网关	必选	必选
		探针	选配	选配
日志审计功能组件	必配	必配		

3.4.3.4 各级政务外网互联的边界安全规范

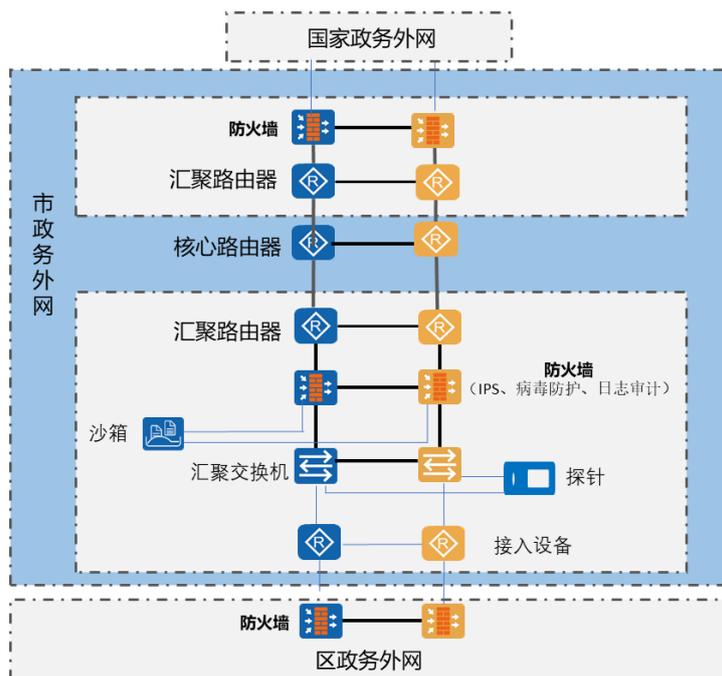


图13 区级、市级、国家级政务外网接入边界安全设计

市级政务外网接入国家政务外网，区级政务外网接入市级政务外网时，应设置安全边界，实现网络访问控制能力，阻断非法访问。

对于区级政务外网接入市级政务外网，应在市级政务外网边界设置安全接入区，需实现网络访问控制、入侵检测和防御、防病毒、APT检测、日志审计等功能，具体要求如下：

(1) 网络访问控制

应在该区域部署防火墙，实现网络边界保护和访问控制。防火墙应只开放政务外网提供接入服务必需的服务端口，对流经接入边界的网络数据进行合法性检查。为了保证业务的可服务性，防火墙需要双机部署，且支持性能的可扩容。防火墙需要支持IPv6协议栈、NAT64转换技术。

(2) 入侵检测和防御

应在该区域部署入侵防御系统，动态检测网络上所有流过的数据包，进行实时检测和分

析，及时发现漏洞、蠕虫、木马等非法和异常行为，并且支持告警、阻断等功能。

(3) 防病毒

应在该区域部署防病毒网关，及时更新病毒库，阻止病毒入侵和传播，进行及时的查杀。防病毒模块可以集成在防火墙内。

(4) APT检测

宜在该区域旁路部署沙箱，针对APT高级持续威胁，利用沙箱多引擎虚拟检测技术，以及传统的安全检测技术，识别网络中传输的恶意文件和C&C攻击。沙箱应支持和防火墙联动以实现威胁的实时阻断。

(5) 探针

宜在该区域部署探针，对流经网络边界的流量进行提取和还原，送至后端大数据分析系统进行安全分析，识别潜在安全攻击风险。

(6) 日志审计

支持日志审计和管理，支持日志统一格式输出，报表自动生成，支持图形化展示，并要求审计日志至少保存6个月。

设备清单参考：

安全场景模块	各场景子模块	各模块所需软硬件	市级电子政务外网	区级电子政务外网
业务网络边界区	各级政务外网安全互联边界	防火墙	必配	必配
		入侵检测与防御硬件	必配	必配
		防病毒硬件	必配	必配
		沙箱	选配	选配
		探针	选配	选配
		日志审计功能组件	必配	必配

3.4.3.5 各单位接入政务外网边界的安全规范

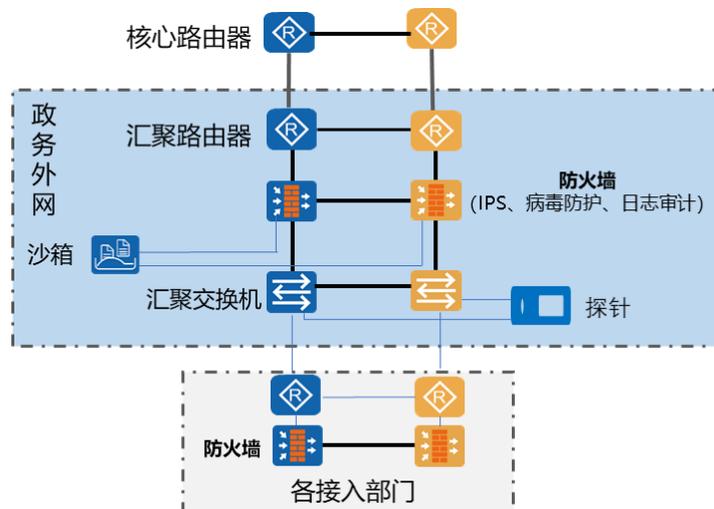


图14 各单位政务外网接入边界安全设计

对于各单位网络接入到政务外网，应在政务外网边界设置安全接入区，需实现网络访问控制、入侵检测和防御、防病毒、APT检测、日志审计等功能，具体要求如下：

(1) 网络访问控制

应在该区域部署防火墙，实现网络边界保护和访问控制。防火墙应只开放政务外网提供接入服务必需的服务端口，对流经接入边界的网络数据进行合法性检查。为了保证业务的可服务性，防火墙需要双机部署，且支持性能的可扩容。防火墙需要支持IPv6协议栈、NAT64转换技术。

(2) 入侵检测和防御

应在该区域部署入侵防御系统，动态检测网络上所有流过的数据包，进行实时检测和分析，及时发现漏洞、蠕虫、木马等非法和异常行为，并且支持告警、阻断等功能。

(3) 防病毒

应在该区域部署防病毒网关，及时更新病毒库，阻止病毒入侵和传播，进行及时的查杀。防病毒模块可以集成在防火墙内。

(4) APT检测

宜在该区域旁路部署沙箱，针对APT高级持续威胁，利用沙箱多引擎虚拟检测技术，以及传统的安全检测技术，识别网络中传输的恶意文件和C&C攻击。沙箱应支持和防火墙联动以实现威胁的实时阻断。

(5) 探针

宜在该区域部署探针，对流经网络边界的流量进行提取和还原，送至后端大数据分析系统进行安全分析，识别潜在安全攻击风险。

(6) 日志审计

支持日志审计和管理，支持日志统一格式输出，报表自动生成，支持图形化展示，并要求审计日志至少保存6个月。

设备清单参考：

安全场景模块	各场景子模块	各模块所需软硬件	市级电子政务外网	区级电子政务外网
业务网络边界区	各单位接入政务外网边界	防火墙	必配	必配
		入侵检测与防御硬件	必配	必配
		防病毒硬件	必配	必配
		沙箱	选配	选配
		探针	选配	选配
		日志审计功能组件	必配	必配

3.4.3.6 无线通信网络接入政务外网边界的安全规范

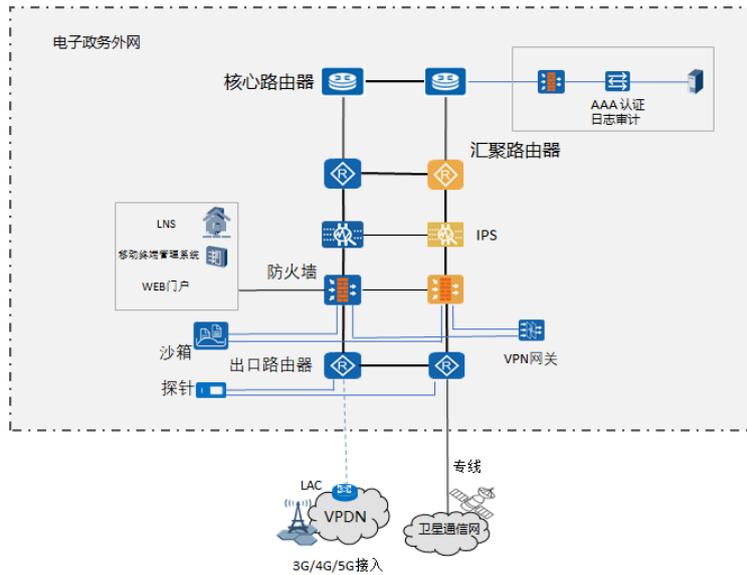


图15 无线通信网络接入区安全设计

对于通过3G/4G/5G等移动通信网络、卫星通信网等无线方式接入电子政务外网的，应建立无线网络安全接入区。安全接入区应实现网络访问控制、AAA认证、VPN接入、入侵检测和防御、APT检测和日志审计功能，具体要求如下：

（1）AAA认证

无线网络安全接入区须以保证通信畅通为前提，基于业务风险分析，进行安全认证和边界重点威胁防御。

在该区域部署AAA服务器，用于无线通信网络用户的认证、授权功能。

（2）VPN网关

对于需要使用拨号接入政务外网的无线通信网用户，须在该区域部署SSL VPN、IPSec VPN或L2TP over IPSec等VPN网关设备，满足无线通信网络用户的安全接入要求。

（3）网络访问控制

应在该区域部署防火墙，实现网络边界保护和访问控制。防火墙应只开放政务外网提供接入服务必需的服务端口，对流经接入边界的网络数据进行合法性检查。为了保证业务的可服务性，防火墙需要双机部署，且支持性能的可扩容。防火墙需要支持IPv6协议栈、NAT64转换技术。

（4）入侵检测和防御

应在该区域部署入侵防御系统，动态检测网络上所有流过的数据包，进行实时检测和分析，及时发现漏洞、蠕虫、木马等非法和异常行为，并且支持告警、阻断等功能。

(5) 防病毒

应在该区域部署防病毒网关，及时更新病毒库，阻止病毒入侵和传播，进行及时的查杀。防病毒模块可以集成在防火墙内。

(6) APT检测

宜在该区域旁路部署沙箱，针对APT高级持续威胁，利用沙箱多引擎虚拟检测技术，以及传统的安全检测技术，识别网络中传输的恶意文件和C&C攻击。沙箱应支持和防火墙联动以实现威胁的实时阻断。

(7) 探针

宜在该区域部署探针，对流经网络边界的流量进行提取和还原，送至后端大数据分析系统进行安全分析，识别潜在安全攻击风险。

(8) 日志审计

支持日志审计和管理，支持日志统一格式输出，报表自动生成，支持图形化展示，并要求审计日志至少保存6个月。

设备清单参考：

安全场景模块	各场景子模块	各模块所需软硬件	市级电子政务外网	区级电子政务外网
业务网络边界区	无线通信网络接入政务外网边界	防火墙	必配	必配
		AAA认证软件	必配	必配
		入侵检测与防御硬件	必配	必配
		防病毒硬件	必配	必配
		沙箱	选配	选配
		探针	选配	选配
		日志审计功能组件	必配	必配

3.4.3.7 政务外网安全接入区边界的安全规范

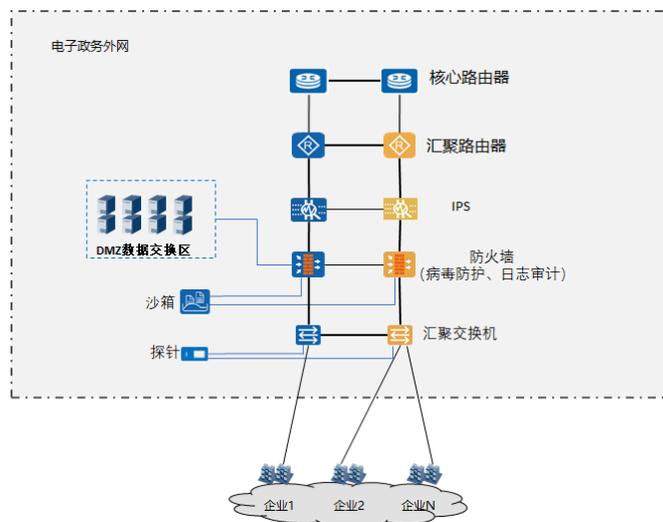


图16政务外网安全接入边界设计

其它机构、部门接入政务外网需求的，需要通过安全接入区接入电子政务外网。在安全接入区，需要实现网络访问控制、防病毒、入侵检测和防御、APT检测、日志审计等功能。具体要求如下：

(1) 网络访问控制

应在该区域部署防火墙，实现网络边界保护和访问控制。防火墙应只开放政务外网提供接入服务必需的服务端口，对流经接入边界的网络数据进行合法性检查。为了保证业务的可服务性，防火墙需要双机部署，且支持性能的可扩容。防火墙需要支持IPv6协议栈、NAT64转换技术。

(2) 入侵检测和防御

应在该区域部署入侵防御系统，动态检测网络上所有流过的数据包，进行实时检测和分析，及时发现漏洞、蠕虫、木马等非法和异常行为，并且支持告警、阻断等功能。

(3) 防病毒

应在该区域部署防病毒网关，及时更新病毒库，阻止病毒入侵和传播，进行及时的查杀。防病毒模块可以集成在防火墙内。

(4) APT检测

宜在该区域旁路部署沙箱，针对APT高级持续威胁，利用沙箱多引擎虚拟检测技术，以及传统的安全检测技术，识别网络中传输的恶意文件和C&C攻击。沙箱应支持和防火墙联动以实现威胁的实时阻断。

(5) 探针

宜在该区域部署探针，对流经网络边界的流量进行提取和还原，送至后端大数据分析系统进行安全分析，识别潜在安全攻击风险。

(6) 日志审计

支持日志审计和管理，支持日志统一格式输出，报表自动生成，支持图形化展示，并要求审计日志至少保存6个月。

设备清单参考：

安全场景模块	各场景子模块	各模块所需软硬件	市级电子政务外网	区级电子政务外网
业务网络边界区	政务外网安全接入区边界	防火墙	必配	必配
		入侵检测与防御硬件	必配	必配
		防病毒硬件	必配	必配
		沙箱	选配	选配
		探针	选配	选配
		日志审计功能组件	必配	必配

3.4.4 安全管理中心建设规范

根据等保2.0规范要求，市、区两级政务外网应建设安全管理中心，对网络设备、安全设备进行运维管理，对安全事件进行事件分析、风险分析、通报和预警。

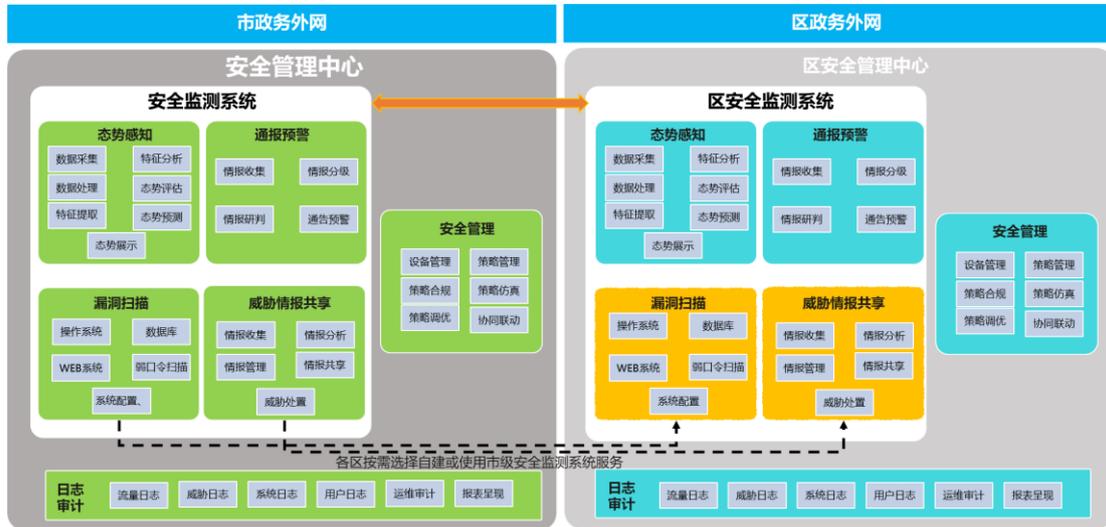


图17 市、区两级安全管理中心架构图

安全管理中心包含态势感知、通报预警、威胁情报共享、漏洞扫描、安全管理控制、日志审计系统共6个模块，实现电子政务外网的全网威胁可视化、通报预警和统一安全运营能力。其中，态势感知、通报预警、威胁情报共享、漏洞扫描作为安全监测系统的关键部件，需要实现与国家政务外网安全监测系统的互通与信息共享。

对于区安全管理中心，漏洞扫描和威胁情报共享子系统可选择自建或使用市级安全检测系统提供的服务。其他子系统均需单独建设。

应通过市、区两级安全监测系统的对接，实现市、区两级安全管理中心的信息交互和协同联动。

市、区两级政务外网安全监测系统各模块的建设要求如下：

模块	包含组件	市政务外网建设要求	区政务外网建设要求
态势感知	探针、大数据分析、安全分析、可视化展示	必选	以下两种方案选择其一。 方案 1：各区部署探针 方案 2：各区部署探针和分析系统
通报预警	可由态势感知子系统提供通报预警接口	必选	必选
威胁情报共享	可由态势感知子系统提供威胁情报共享接口	必选	可选

模块	包含组件	市政务外网建设要求	区政务外网建设要求
漏洞扫描	漏洞扫描设备	必选	可选
安全管理控制	安全管理软件	必选	必选
日志审计系统	日志审计软件，服务器	必选	必选

3.4.4.1 态势感知

态势感知子系统须能从多维度 and 可视化方式，对上海全市政务外网进行全方位、全天候安全威胁感知和呈现。



图18 态势感知子系统架构图

态势感知子系统组成宜包括数据采集层、数据存储和挖掘层、态势展现层。数据采集层通过部署探针、接收安全设备日志、漏洞扫描设备扫描日志等方式获取原始数据；数据存储挖掘层建立在大数据分析系统之上，对IP地址库、GIS地图库、恶意IP、恶意文件库、资产库等基础数据信息进行安全和威胁的深度挖掘。态势展现层对安全分析结果进行威胁态势可视化呈现、通报预警和威胁情报的共享和发布。

市、区两级政务外网均应在汇聚节点及网络区域的边界部署探针，在安全管理中心部署态势感知大数据分析系统。市、区两级政务外网基于网络流量大小选择探针，选择标准如下：

流量大小	探针规格
≤1Gbps	1Gbps
1Gbps-5Gbps	5Gbps

流量大小	探针规格
5Gbps-10Gbps	10Gbps

态势感知子系统应能对网站及主机漏洞、流量异常、扫描探查、弱点攻击、僵尸网络、数据泄露、APT攻击等各类安全攻击、威胁事件进行多视角的态势感知呈现，实现网站安全态势感知、内网威胁态势感知、Web站点态势感知、脆弱性态势感知等功能。

3.4.4.2 通报预警

通报预警子系统可基于态势感知子系统的态势展现模块进行接口开发，或单独建设开发。通报预警子系统对安全态势、威胁和漏洞情况进行汇总、分类、分级和研判处理，自动形成通报报告，并及时将情况上报给上级安全管理中心，通告给本级政务外网主管单位和接入单位。从而实现对本级使用部门、上级单位、下级单位的通告预警。

通报预警按照安全风险、影响程度分为高危、中危和低危事件。

3.4.4.3 威胁情报共享

威胁情报共享子系统可基于态势感知子系统的态势展现模块进行开发，或单独建设开发。威胁情报共享子系统实现安全情报的收集、情报分析与处理、情报数据管理等。情报信息主要包括恶意样本病毒、恶意IP/URL/MD5库，黑客组织信息、攻击方法手段、安全资讯等。

威胁情报共享子系统应能通过多种通道和技术搜集政务外网的安全情报信息，并共享给安全管理控制系统用于实时阻断、隔离相关攻击源。

3.4.4.4 漏洞扫描

漏洞扫描子系统可部署单独的漏洞扫描设备进行漏洞扫描，或集成在态势感知系统内部相关功能模块。

漏洞扫描子系统应支持对操作系统、数据库、网络设备、安全设备、Web系统、弱口令等的漏洞扫描，支持对系统配置进行基线核查，并且能为系统管理员提供漏洞的详细报告和解决方案。漏洞扫描子系统需要支持资产自动发现功能，支持远程自动升级以及本地升级最新漏洞库。

3.4.4.5 安全管理控制

安全管理中心应部署安全管理控制子系统。安全管理控制子系统以独立软件的形式部署在服务器或虚拟机上。具体应具备以下能力：

1. 设备管理

对设备的统一管理应支持以下能力：设备自动发现、设备的增删改查、双机热备组、设备组的增删改查、设备配置的一致性对比、设备单点登录，设备版本升级，设备配置文件备份。

2. 策略管理

支持安全策略的管理，通过设置对应的匹配条件，包括源/目的安全区域、源/目的地址、服务、时间段来实现政务外网的安全策略管控。在执行动作上可以设置允许或禁止。同时也可以配置上对应的安全配置文件做内容安全防护，可对策略组视图和设备视图进行策略快速管理，策略变更统计、配置一致性统计、部署状态统计等管理能力。

3. 策略合规性检查

支持定义白名单、风险规则、混合规则等检查方式。策略提交后，匹配定义好的检查规则，及时反馈检查结果、安全等级等信息给安全审批责任人。支持低风险策略自动审批。

4. 策略仿真

应能通过学习业务互访关系，对比待部署策略，以模拟部署的方式，在策略部署前评估策略对业务的影响，以降低策略部署后对业务带来的风险。

5. 协同联动

应支持安全管理控制系统联动态势感知子系统，以实现威胁检测结果自动转化为安全策略，并将安全策略下发到安全设备，实现安全设备的闭环联动处置。

3.4.4.6 日志审计系统

安全日志系统须单独建设，提供集中化的统一日志管理系统，收集政务外网设备的日志信息，提供流量日志、威胁日志、系统日志、管理员运维日志的日志审计功能。

按照等保要求，审计日志留存时间需满足至少6个月。

3.4.4.7 设备清单参考

安全场景模块	各场景子模块	各模块所需软硬件	市级电子政务外网	区级电子政务外网
安全管理中心	态势感知	大数据分析软件	必配	必配
		安全分析系统软件	必配	必配
		可视化系统软件	必配	必配
		探针	必配	必配
	通报预警	通报预警系统软件	必配	必配
	威胁情报共享	威胁情报共享系统软件	必配	选配
	安全管理	安全管理软件	必配	必配
日志审计	日志审计功能组件	必配	必配	

3.4.5 安全监测系统建设规范

根据国家《政务网络安全监测平台总体技术要求》，上海市需建立市、区两级安全监测系统，以具备完整的数据采集预处理、数据分析、数据总线、展示与应用，系统运行管理等功能。

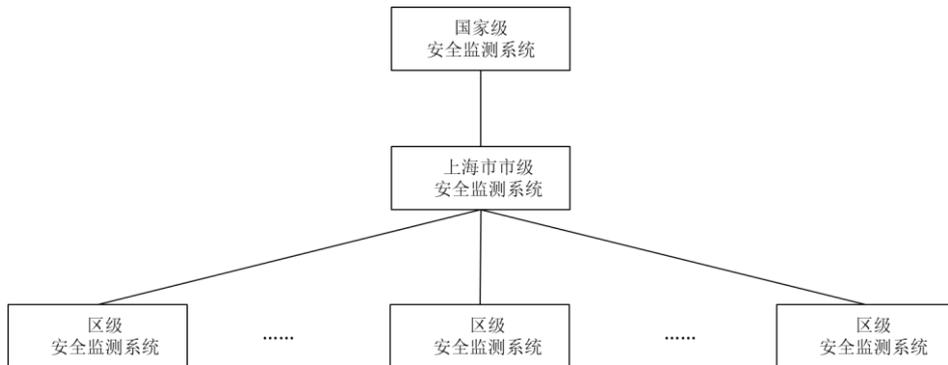


图19 市电子政务外网安全监测系统架构图

3.4.5.1 市级安全监测系统

市级政务网络安全监测系统应采用旁路部署探针的架构，对区级电子政务外网接入、市级接入部门网络接入、互联网接入等区域进行流量、日志等维度信息的数据采集处理。

市级政务安全监测系统应按要求和国家级政务安全监测系统进行数据的级联对接。

3.4.5.2 区级安全监测系统

区级政务外网可不单独建设监测分析系统，但须部署相应的监测系统或监测探针。监测系统或监测探针主要针对区级电子政务外网、区级接入部门网络、互联网出口等区域进行流量、日志等维度信息的数据采集、预处理。

区级网络安全监测系统或监测探针应按国家《政务网络安全监测平台总体技术要求》要

求与市级安全监测系统所需数据的级联对接。

3.4.5.3 监测系统功能规范

市区两级监测系统采集区域应包括互联网访问区、各单位网络、政务外网边界等网络区域，以及基础支撑系统、业务系统、托管业务等应用。

数据采集内容应包含必要的网络流量、IT设施的日志，资产信息、威胁情报、漏洞信息、下级系统上报的数据等。其对应的数据格式和不同级别系统对应的接口规范，应满足国家《政务网络安全监测平台总体技术要求》的标准和要求。

3.5 IPv6 网络设计规范

3.5.1 总体规范

政务外网业务网络的设计，应遵循《推进互联网协议第六版（IPv6）规模部署行动计划》的标准和要求，网络设备、安全设备、DNS、运维支撑系统等均应支持IPv4/IPv6双栈技术。

在进行双栈设计时，网络设备的IPv6转发性能须满足业务线速转发的要求。

3.5.2 IPv6 网络方案设计

3.5.2.1 IPv6网络协议设计

所有业务网络设备应同时支持OSPF/IS-IS、OSPFv3/IS-ISv6、BGP/BGP4+协议，即同时支持IPv4及IPv6内外部路由协议，以满足双栈情况下的路由转发。

在所有业务网络设备上开启IPv4/IPv6双栈，配置IPv4/IPv6双栈接口地址，运行IPv4/IPv6双栈路由协议，保持IPv4和IPv6路由表。

在网络采用SR MPLS技术作为转发协议时，通过SR隧道统一承载IPv4、IPv6的VPN业务，设备应支持OSPF、IS-IS、EVPN技术，并通过BFD检测，加快OSPF、IS-IS协议的路由收敛。

当网络采用SRv6技术作为转发协议时，通过SRv6隧道统一承载IPv4、IPv6的VPN业务，设备应支持IS-ISv6、EVPN等技术，并通过BFD检测，加快IPv6路由的收敛。

3.5.2.2 DNS服务器设计

DNS服务器应支持IPv4/IPv6域名查询（A/AAAA记录查询），且IPv6的DNS查询不影响IPv4

的DNS查询。

DNS服务器应支持AAAA请求递归查询。

3.5.2.3 IPv6协议部署和业务访问设计

在所有业务网络设备上均启用IPv4/IPv6双栈技术，同时支持IPv4和IPv6网络的接入。当政务云等业务系统进行IPv6改造时，可通过在业务系统侧（云数据中心网络上），旁挂NAT64防火墙和DNS64设备，实现：

- IPv4用户访问IPv4业务系统，无须地址转换；
- IPv6用户访问IPv6业务系统，无须地址转换；
- IPv4用户访问IPv6业务系统，或IPv6用户访问IPv4业务系统，由防火墙做NAT转换。

3.5.2.4 IPv6安全设计

IPv6安全设计应具备IPv6基本防护能力、IPv6安全过滤、IPv6安全管理、IPv6流量监测和告警等功能。

1. IPv6基本防护能力要求如下：

- 1) 具备IPv6访问控制安全策略管理功能；
- 2) 具备IPv6报文检测功能；
- 3) 具备不同协议的ICMPv6消息识别和过滤，包括PMTU、ND协议；
- 4) 具备合法的IPv6分片包转发功能；
- 5) 具备SYN Flood/UDP Flood/ICMPv6 Flood等IPv6安全防护能力；
- 6) 具备IPv6防病毒功能；
- 7) 具备IPv6入侵检测和防御功能。

2. IPv6安全过滤能力要求如下：

- 1) 支持针对IPv6地址和IPv6地址段的攻击流量的检测和过滤功能；
- 2) 支持针对IPv6数据包的深度报文检测功能；
- 3) 支持对IPv6流量的主动探测功能；
- 4) 支持基于IPv6地址的五元组流量过滤及黑白名单等攻击流量的过滤方式；
- 5) 支持基于IPv6流量统计特征、IPv6报文内容特征匹配、重定向检测等多种技术，发现IPv6攻击流量。

3. IPv6安全管理功能要求如下：

1) 应具备登录受限功能，支持通过ACL等方式限定可登录的IPv6地址；

2) 支持按被攻击IPv6地址/IPv6地址段的TopN分析、攻击流量趋势分析、明细数据分析的报表统计功能；

4. IPv6流量监测与告警功能要求如下：

1) 支持对IPv6流量的数据流分析功能；

2) 支持对IPv6异常流量进行溯源取证分析；

3) 具备IPv6流量日志审计功能。

3.5.2.5 网管系统设计规范

网管系统可不进行IPv6地址改造，仍保留IPv4地址，但应支持对各种IPv6地址类型设备的识别和管理。

网管系统应支持对IPv6设备和双栈设备的性能、资源、故障等数据采集能力，满足对IPv6设备和双栈设备的性能管理、资源管理、故障管理及分析等功能。

网管系统应支持对双栈设备进行IPv4及IPv6的关联，使得双栈设备的各种资源、性能、故障等数据能够与历史数据平滑关联。

网管系统应支持通过基于IPv4的SNMP访问相关设备IPv6 MIB，通过IPv6 MIB获得IPv6配置和流量等相关信息。

3.6 网络高可靠设计规范

3.6.1 总体规范

为实现网络故障时业务在200ms内快速切换的目标，应按以下要求进行网络设计和配置：

1. 基础设施要求

1) 核心、汇聚采用两个或两个以上节点配置，且每个节点必须配置2台核心、汇聚设备。有条件的区域，宜采用物理地址不同的机房安装核心、汇聚设备。如因条件限制，核心、汇聚设备安装在同一机房，必须保证机房有2路（或以上）市电接入，核心、汇聚设备从不同列头柜引电，不同列头柜不使用同一开关；

2) 核心、汇聚机房场地的选择、结构防火、机房内部装修、机房专用设备、火灾报警及消防设施，及其它安全防护和管理，应符合《计算站场地安全要求》的要求。核心、汇聚

机房环境条件、机房供电、机房建筑结构应符合《电子计算机场地通用规范》要求，功能区域齐全且相对独立，UPS不间断电源至少能保障2小时不中断供电；

3) 核心、汇聚设备的关键板卡要按主备冗余的要求进行配置，包括主控板、电源板、交换板、风扇等；

4) 核心、汇聚设备出局的传输线路，必须保证2个以上不同物理路由。路由器上行和横联链路应避免传输同路由，下行和横联链路应避免传输同路由。

2. 网络层要求

1) 路由器和交换机的三层链路必须能快速感知链路中断。裸光纤直连链路可通过物理层快速感知故障；专线链路必须部署双向链路检测BFD。捆绑链路必须部署BFD检测捆绑成员链路技术；

2) 动态路由协议检测到链路故障后，宜在50ms内启动SPF重算路由。如设备支持，还须部署FRR快速重路由技术；

3) ECMP路由设计。设备的上行链路宜采用等价路径，物理双路由。正常运行时流量负载均衡，链路故障时毫秒级切换。特殊场景宜部署UCMP非等价负载分担，适用链路带宽不一致场景；

4) VRRP业务应避免与心跳链路使用同一链路承载，或者多链路同单板；

5) 路由器、交换机、防火墙要按照不同应用场景中的路由条目需求配置业务板卡，每个VPN应设置路由前缀限制和标签规格限制；

6) BGP路由必须设置收发策略控制，防止地址冲突和流量模型错误；

7) IGP Metric度量值要结合网络链路带宽和平面合理设置，全网统一规划；

8) 对于底层采用传输线路的IP链路，在使用传输线路的IP接口部署误码检测和倒换，确保传输线路质量劣化时，业务不受影响；

9) 部署FRR快速重路由技术，降低链路或设备故障时对承载业务的影响。

3.6.2 双平面可靠性设计规范

为确保政务外网对政务业务的高可靠承载，政务外网除了考虑在各业务节点部署双设备、双链路外，应采用数据平面和视频平面互为备份的“一网双平面”高可靠架构组网。通常情况下，数据平面、视频平面互为冗余备份；发生故障时，故障平面上的业务可自动倒换至未发生故障的平面。

双平面在设计中应遵循如下原则：

1. 视频平面定位于承载政务视频会议、公共安全视频监控传输与共享等业务，数据平面定位于承载政务办公业务、互联网访问等业务；

2. 两个平面的网络架构、性能、建设和运营管理标准等宜保持一致；

3. 设备或链路故障时，优选本平面内的冗余设备或链路进行切换。本平面无法备份时再选择第二平面倒换；

4. 应从接入部门的接入设备起，对视频和数据业务进行分离；

5. 接入设备的工作模式有以下几种：

1) 接入设备工作在二层网络模式时，在其三层网关双设备部署两个VRRP组，视频和数据流量部署网关时分别选择两个不同的VRRP组进行二层转发，以形成二层网络双平面。如VRRP组一，配置设备1为主、设备2为备，视频流量选择VRRP组一；VRRP组二，配置设备2为主、设备1为备，数据流量选择VRRP组二。

2) 接入设备工作在IP模式（静态路由部署），通过配置静态路由的主备链路选择下一跳，此时将视频、数据流量的静态路由配置为相反的下一跳，以实现视频、数据流量分离到不同平面；

3) 接入设备工作在PE模式时，在导入不同VPN路由到IGP协议时，通过设置不同Cost值实现业务分离。如A平面默认承载数据业务，B平面默认承载视频业务，则视频流量设置A平面路由Cost值大于B平面；

6. 宜在全网部署BFD快速故障检测技术，BFD应配置为与VRRP、静态路由、OSPF、ISIS、BGP、MPLS、SR等协议联动。宜部署支持硬件BFD发包功能的设备，加速BFD报文发送速率；

7. 应在两个平面间部署IP FRR、VPN FRR等快速重路由技术；

8. 网络流量设计规则时应保持往返流量路径一致；

9. 应采用标准技术组网。

3.7 服务质量设计规范

政务外网须提供差异化服务能力，宜通过QoS、网络切片等技术实现敏感数据、高SLA要求业务的带宽保障、业务隔离诉求。

3.7.1 QoS 设计原则

上海市电子政务外网的QoS总体设计原则如下：

1. 采用轻载方式保障网络服务质量，建议链路月平均日峰值利用率不超过50%；
2. 采用DiffServ作为网络突发拥塞时QoS保证方式；
3. 识别用户侧流量，调度重要业务进PQ队列，调度普通业务进默认队列尽力转发。

3.7.2 QoS 部署方案

各区电子政务网络启用DiffServ，结合H-QoS技术实现对网络中VPN业务的不同业务流，提供差分QoS保障。

1. 确定QoS的信任域，在信任域边界按业务保障要求进行流分类/优先级标记；
2. 根据PHB做全网的拥塞管理和调度；
3. 政务外网的业务类型及优先级设置如下：

业务类别	优先级	队列	业务特征	队列调度
协议报文、控制管理	7/6	CS6/CS7	丢包、时延非常敏感，带宽需求低	PQ
实时应用类（语音）	5	EF	低时延，能容忍少量丢包，小带宽	PQ
实时应用类（视频）	5	EF	低时延，丢包敏感，大带宽	WFQ
业务管理类	4	AF4	低时延，丢包敏感，小带宽	WFQ
社会服务类	3	AF3	低时延，丢包敏感，小带宽	WFQ
业务协同类	2	AF2	实时性低，丢包容忍度高，小带宽	WFQ
日常办公类	1	AF1	实时性低，丢包容忍度高，小带宽	WFQ
互联网访问	0	BE	实时性低，丢包容忍度高，中等带宽	LPQ

4. 基于VPN进行的QoS设计

基于VPN-Instance对VPN去往其他所有PE设备的网络侧流量进行总带宽限制和保证；基于Peer对VPN去往其他不同PE设备的流量分别进行控制。

5. VPN内业务QoS

在Ingress-PE上针对各VPN的流量按照优先级映射成AF、EF、BE等不同业务流，根据不同业务流进行队列调度、拥塞避免和流量整形（用户级别），也可以分别映射到出端口的不同类别的流队列中（端口级别），从而在出端口实现各VPN流量中不同种类的业务流的整体队列调度。

6. 网络基础带宽资源质量保障

对敏感数据和SLA要求高的业务，可采用网络切片或其它网络基础资源隔离技术，将网络划分为多个独立的逻辑业务平面以进行业务隔离。每个平面拥有独立的带宽资源，各独立平面间的带宽不能相互抢占。

7. 网络缓存要求

网络设备应支持大缓存功能，确保当网络流量突发时，超出转发速率的数据包能缓存在设备中不被丢弃，保证关键业务无丢包。

3.8 网络管理设计规范

3.8.1 总体规范

上海市电子政务外网应引入SDN智能化运维管理系统，形成网络“管、控、析”协同的运维管理体系。

3.8.2 网络管理

3.8.2.1 功能、对象和协议/工具

网络管理应能实现如下的配置、故障、性能、安全、审计功能。

功能	描述
配置管理	自动发现网络拓扑结构，构造和维护网络系统的配置。监测网络被管对象的状态，完成网络关键设备配置的语法检查，配置自动生成和自动配置备份系统，对于配置的一致性进行严格的检验
故障管理	过滤、归并网络事件，有效地发现、定位网络故障，给出排错建议与排错工具，形成整套的故障发现、告警与处理机制
性能管理	采集、分析网络对象的性能数据，监测网络对象的性能，对网络线路质量进行分析。同时，统计网络运行状态信息，对网络的使用发展作出评测、估计，为网络进一步规划与调整提供依据
安全管理	结合使用用户认证、访问控制、数据传输、存储的保密与完整性机制，以保障网络管理系统本身的安全。维护系统日志，使系统的使用和网络对象的修改有据可查。控制对网络资源的访问
日志管理	网络的故障、操作日志要按要求保存，为合规审计提供有效依据

网络管理使用的协议和工具如下：

协议和工具	描述
ICMP	用于设备/主机的可达性检测
SNMP	所有 IP 网络设备必须支持 SNMP v2c 或 SNMP v3，支持把 SNMP Trap 发送到网管系统，并允许从网管系统进行 SNMP 查询
FTP	设备/主机的远程文件访问
SSH	设备/主机的远程安全登录

协议和工具	描述
Netconf	控制器和转发器之间的通信协议
Syslog	支持 Syslog 的设备应将各类信息发送到网管系统
Netstream	采集接口的流信息，提供给应用流分析系统进行统计分析
其他	比如主机支持的各种远程管理工具
SDN 控制器	与所有网络设备管理口安全互联，对网络进行集中管控

3.8.2.2 配置管理

对网络设备和业务的配置管理，应包含以下内容：

1. 支持根据用户需求查询、修改网络设备的系统信息、路由信息、接口信息以及VPN信息，并对已配置完毕的信息进行备份。

2. 支持配置比对功能。通过SDN控制器和设备配置进行比对，控制器自动发现与控制器配置不同步的设备，并提醒运维人员进行配置同步。

3. 提供统一拓扑发现功能，支持全网监控，可以实时监控所有网络设备的运行状况，通过流量调优技术实现网络带宽均衡和保障高优先级业务的SLA质量。

4. 支持业务自动化发放、部署及按需调整；

1) 支持的业务类型：动态L3 VPN、动态TE隧道、QOS/H-QOS；

2) 支持的业务组合：支持动态L3 VPN、动态TE隧道和QOS/H-QOS的组合部署；

3) 业务下发流程：SDN控制器通过Netconf/BGP-LS/PCEP等标准的南向协议连接网络设备，按需自动化的配置，支持分钟级实施完成；

4) 业务可视：支持对以上业务类型的基本信息可视，包括业务告警、运行状态、部署状态、管理状态、客户名称、组网类型；支持对网络层、协议层和隧道层物理/逻辑连接可视；支持对告警、物理节点、具体协议的详细信息可视。

3.8.2.3 性能管理

网管系统对网络设备和业务的性能管理，应包括以下内容：

1. 性能监控：

1) 支持创建/修改/删除/挂起/恢复性能监控实例功能，将资源与性能监控模板绑定，创建成功后开始采集资源的性能数据；

- 2) 支持性能监控实例分组管理功能;
- 3) 支持差异化的性能调度策略,按时间段和采集周期,在指定的时间段和采集周期内采集性能数据;
- 4) 支持性能参数包括:对隧道、线路和设备的流量、延时、抖动、丢包率、可用率、CPU利用率、内存等性能参数;
 2. 支持设置性能监视门限值:当性能参数越过或低于一定的门限值时,发出告警通知;
 3. 支持性能分析和管理:对性能数据进行分析、统计、计算性能指标。对性能数据管理功能,包括查看实时性能,浏览资源对象的实时性能,宜支持分析突发或者短期趋势;查看历史性能:浏览资源对象在一段时间内的性能,宜支持分析长期趋势;支持性能数据转储:支持自动转储或手工转储性能数据,以节省数据库空间。

3.8.2.4 故障管理

对网络设备和业务的故障管理,应支持以下内容:

1. 故障信息采集:采集网元设备的告警信息,包括设备故障告警、链路故障告警、各种门限告警、设备/端口/链路状态变化告警等;
2. 故障监视:对网元和网络路由进行监视,出现故障时进行显示;
3. 故障处理过程管理:记录排错行为,包括故障产生,变化,消除过程;
4. 故障信息的查询与统计。

3.8.2.5 安全管理

安全管理包含对用户权限和系统安全策略的管理。安全管理应包含如下相关功能:

1. 支持用户权限管理功能,管理不同职责的用户对系统和资源的操作权限;
2. 支持用户维护和监控功能,在权限维护期内,根据需要查看或编辑用户信息、角色信息和操作集信息等,并可实时监控用户会话及用户操作,保证系统安全性;
3. 支持远端认证功能,系统可以通过配置AAA认证协议实现与第三方系统的对接。对接成功后,系统不再通过用户管理功能进行用户鉴权,在登录时用户鉴权由3A系统实现;
4. 支持账号安全策略,对用户的帐号进行登录或锁定策略的设置,合理设置可提升系统访问的安全性;
5. 支持密码安全策略,设置密码的复杂度、更新周期、字符限制等,避免用户设置过

于简单的密码或长时间不修改密码，以提高系统访问安全性；

6. 支持登录IP地址控制策略，管理员可根据需要设置登录IP地址控制策略，限制用户只能从特定IP地址区间登录系统，以提高系统的安全性；

7. 支持登录时间控制策略，安全管理员可根据需要设置登录时间控制策略，限制用户只能在特定的时间段内登录系统，以提高系统的安全性。

3.8.2.6 日志管理

日志管理应支持系统自动记录其运行过程中的安全日志、系统日志和操作日志，同时提供查询日志、导出日志和转储日志功能。日志导出要求格式统一，能自动生成报表，支持图形化展示。

日志管理应支持查询、导出、管理模板和日志转储功能。

审计日志至少能保存6个月。

3.8.3 网络控制

网络控制应包含如下功能：

1. 应支持流量动态调整功能：

1) 支持自动流量调优。流量采集分析模块定期从网络设备收到隧道和链路的带宽流量信息，如果发现某个链路的流量超过阈值，通知调优控制模块计算调优路径；

2) 流量调优时应支持基于多路径约束因子对网络上不同隧道路径进行综合计算；

3) 支持自定义流和TOP N流作为流量调整对象；

4) 具有操作权限的客户，支持手工流量调优，支持对自定义流或TOP N流进行调优，支持单流和批量流调优；

2. 支持隧道带宽动态调整功能；

3. 支持隧道路径控制，通过SDN控制器指定端到端转发节点和路径。匹配的业务流量按照指定路径转发；

4. 支持隧道路径调优控制：链路故障场景时，控制器自动触发故障调优，自动切换到提前规划好的路径上；链路拥塞场景，支持优先通过手动调整入隧道的业务流量来控制路径；

5. 支持节点、链路流量控制：当需要对节点或链路维护时，能自动将节点或链路上的流量调整到其他路径，当维护结束后，再进行全局流量重新优化；

6. 支持维护窗口业务保障：支持界面选择，设置维护的网元节点或者链路，以及维护窗口起止时间；维护窗口内，控制器支持针对经过维护网元节点/链路上的隧道重新计算路径，而且新的路径绕开待维护操作的网元/链路。

3.8.4 网络分析

网络分析应具备如下功能：

1. 支持应用流量采集与呈现功能，支持通过定制化报表输出分析结果；
2. 支持网络故障仿真：在网管系统界面上选择模拟故障发生的某个网元或者物理链路，控制器自动计算故障发生后网络新的拓扑和流量分布，并显示故障前后的差异变化信息；
3. 支持流量预测功能：网管系统采集网络的业务流量和带宽占用信息，基于所采集的历史流量大数据信息，计算出未来一段时间内的流量和带宽变化趋势。根据这个趋势信息，网络管理人员可以对网络链路带宽的调整提前做出判断。

3.9 IP 地址规划和管理

3.9.1 IPv4 地址规划和管理

3.9.1.1 IPv4地址规划总体原则

上海市电子政务外网正在使用的IPv4网络地址分为两类：

1. 国家政务外网互联共享地址

指国家政务外网管理中心分配给上海市政务外网各级部门机构使用的提供信息服务的主机地址，该地址能够在整个政务外网内被访问。共享地址（59. X. X. X）原则上以区级政务外网为单位分配，需要向上海市大数据中心申请。

2. 市政务外网本地网络地址

指上海市市、区两级政务外网、各部门各机构接入网络所使用的链路地址（网络设备间的点对点互联地址）、设备管理地址、应用服务器地址等。此地址（10. X. X. X/16）在上海市政务外网内部使用，不用于互联网和国家政务外网。

市政务外网本地网络地址使用必须向上海市大数据中心申请，由大数据中心根据工单申请进行延续性分配。对地址使用规划如下：

1. 10. X. X. X/16地址以1个B类地址为单位，按需分配给各区政务外网及接入单位使用，

若增加需要向上海市大数据中心申请。

2. 视频专网（含视频共享平台），及视频终端地址规划如下表，根据工单开具的顺序依次分配。

类型	地址	类型	地址
视频专网 IP 地址	10.224.0.0/16	视频终端 IP 地址	10.166.0.0/16-10.171.0.0/16

3.9.1.2 地址的分配和变更

新接入上海市电子政务外网的单位，其IP地址在开通时由市大数据中心统一分配。

已接入上海市电子政务外网的单位，其IP地址若需变更，应向市大数据中心书面申请，变更的IP地址由市大数据中心统一分配。

3.9.1.3 IP地址冲突及解决措施

可能存在的IP地址冲突的情况：

- 1) 市级接入部门网络在接入市政外网前已使用了10. x. x. x的IP地址段；
- 2) 区级接入部门网络在接入市政外网前已使用了10. x. x. x的IP地址段。

解决措施如下：

- 1) 10. 0. 0. 0/8地址为政务外网专用地址，要求新接入政务外网的单位，将出口IP地址更改为市大数据中心统一分配的新IP地址；
- 2) 接入部门IP地址在市政外网内未被分配使用的，原则上保持IP地址不作更改。

3.9.2 IPv6 地址规划和管理

3.9.2.1 IPv6地址总体规划

IPv6地址长度为128的二进制位，采用十六进制表示方式。IPv6地址的表示格式为x:x:x:x:x:x:x，其中x是一个4位十六进制整数，每一个十六进制整数对应4位二进制整数。

例如：ABCD:EF01:2345:6789:4137:DA12:3241:AC32所表示的二进制IPv6地址如下图所示：

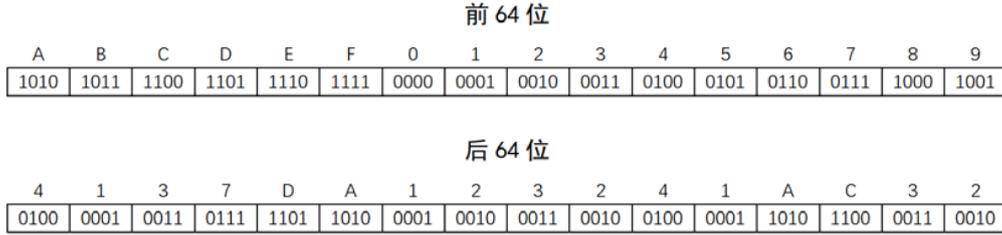


图20 十六进制地址示意图

3.9.2.2 地址区域划分

IPv6地址分为三个区域：固定前缀区、自定义前缀区、主机地址区。

目前国家信息中心向中国互联网络信息中心（CNNIC）申请的IPv6地址段为240B:8000::/21，其中240B:8000::/24是全国政务外网预分配的地址段。

国家信息中心已为各省/直辖市政务外网分配/30掩码的IPv6地址段，如上海市为240B:803C::/30。

自定义前缀区是上海市电子政务外网内部标识各个子网的标识符，共计34bits。通过对自定义前缀区进行区隔划分，兼顾不同种类设备、不同行政层级单位的地址分配，实现IPv6地址分类和层级管理。

主机地址区是用于标识政务外网内各种设备网络接口的标识符，共计64 bits。末级单位应以自定义前缀区的子网地址块为最小单位对主机地址进行分配使用。

3.9.2.3 地址分配管理

IPv6地址分配遵循“先申请，后使用”的原则，由上海市电子政务外网统一分配各系统单位的IPv6地址前缀，并为每个系统单位分配足够容量的地址块。各系统市级以上单位须按照本方案的分配原则，为本系统市、区级单位进一步分配IPv6地址块。

各市区级单位须在上海市电子政务外网IPv6地址管理系统中上报登记已分配的IPv6地址，防止重复使用。

网络中各类路由设备的互联地址和Loopback地址由上海市大数据中心统一分配。

3.9.2.4 IPv6地址具体规划

政务外网IPv6地址具体规划如下表：

地址空间	国家信息中心给省市的 30 位掩码 IPv6 地址段			行政区划	上海政务外网划分		EUI-64
	固定前缀	类型域-T	区划域-省市	区划域-区县	部门域- -WWW	子网域- -YY	主机域
长度 (bit)	20	4	6	14	12	8	64
IPv6 地址前缀位数	1-20	21-24	25-30	31-44	45-56	57-64	65-128

政务外网IPv6地址段结构为：240B:8TZZ:ZZZW:WWYY::/64，其结构性编址方式，分为以下五个字段：

- a) 1-24位，类型域，240B:8T
- b) 25-44位，区划域，ZZ:ZZZ
- c) 45-56位，部门域，W:WW
- d) 57-64位，子网域，YY
- e) 65-128位，主机域，规划为接口标识，支持IEEE EUI-64规范

1. 类型域（T码）编码规范

240B:80	政务外网网络平台
240B:81	基础数据业务
240B:82	视频会议业务
240B:83	视频监控业务
240B:84 - 240B:87	预留

2. 区划域（Z码）编码规范

区划域ZZ:ZZZ用于标识中央、省、市、县四级行政区域，区划码规则如下：

将民政部颁布的6位县级以上行政区划代码分为3段：AA.BB.CC，其中AA使用附录编码替换（详见附录A），并转化为6位二进制字符，BB.CC分别转化为7位二进制字符，合计20位进制字符，最后按4位一组转换成16进制字符，生成区划域Z码。

例如：上海市区划域编码：

310000（上海市行政区划代码）=> 31-00-00（分段）=> 15-00-00（查附录）=>
001111-0000000-0000000（分别转化成二进制，位数不够前补零）=>
0011-1100-0000-0000-0000（四位一组）=> 3C000（转换成16进制区划码）

行政大区									
华北	北京市	天津市	河北省	山西省	内蒙古				
	01	02	03	04	05	06	07	08	
东北	辽宁省	吉林省	黑龙江省						
	9	10	11	12	13	14			
华东	上海市	江苏省	浙江省	安徽省	福建省	江西省	山东省		
	15	16	17	18	19	20	21	22	23
华中	河南省	湖北省	湖南省	广东省	广西	海南省			
	25	26	27	28	29	30	31	32	33
西南	重庆市	四川省	贵州省	云南省	西藏				
	34	35	36	37	38	39	40	41	
西北	陕西省	甘肃省	青海省	宁夏	新疆	兵团			
	42	43	44	45	46	47	48	49	
台湾	台湾省								
	50	51	52	53					
特区	香港	澳门							
	54	55	56	57	58				

图21 省级地址AA对照表

附上海1+16区划编码：

	中心城区	行政区划代码	区划编码 ZZ:ZZZ	二进制区划码
1	上海市	310000	3C:000	0011-1100-0000-0000-0000
2	黄浦区	310101	3C:081	0011-1100-0000-1000-0001
3	浦东新区	310115	3C:08F	0011-1100-0000-1000-1111
4	徐汇区	310104	3C:084	0011-1100-0000-1000-0100
5	长宁区	310105	3C:085	0011-1100-0000-1000-0101
6	静安区	310106	3C:086	0011-1100-0000-1000-0110
7	普陀区	310107	3C:087	0011-1100-0000-1000-0111
8	虹口区	310109	3C:089	0011-1100-0000-1000-1001
9	杨浦区	310110	3C:08A	0011-1100-0000-1000-1010
10	闵行区	310112	3C:08C	0011-1100-0000-1000-1100
11	宝山区	310113	3C:08D	0011-1100-0000-1000-1101
12	嘉定区	310114	3C:08E	0011-1100-0000-1000-1110
13	金山区	310116	3C:090	0011-1100-0000-1001-0000
14	松江区	310117	3C:091	0011-1100-0000-1001-0001
15	青浦区	310118	3C:092	0011-1100-0000-1001-0010
16	奉贤区	310120	3C:094	0011-1100-0000-1001-0100
17	崇明区	310230	3C:11E	0011-1100-0001-0001-1110

3. 部门域（W码）建议编码规范

上海市各委、办、局部门、单位和机构的部门域分配，应遵循《国家电子政务外网IPv6

地址规划（2019版）》规定，并遵循如下分配原则：

- 1) 上海市各政务部门使用其所对应的中央部委或机构的部门域；
- 2) 当上海市部门或机构对应多个中央部委或机构时，按其应用所联接的中央部委或机构的部门域逐个应用分配地址。
- 3) 上海市独立设置的、在中央没有对应部委或机构的部门和机构，按其党政属性归属到市委办公厅或市政府办公厅，按两厅的部门域分配地址；

《国家电子政务外网IPv6地址规划（2019版）》对部门域的规划如下：

A类为政府部门，W1码为1-5。上海市各政府部门使用的部门域W1、W2与国家电子政务外网管理中心对中央政务部门分配的W1、W2部门域保持一致。

W1W2	中央政务部门	上海市对应的政务部门
10	国务院办公厅	上海市人民政府办公厅
11	外交部	上海市人民政府外事办公室
12	国防部	
13	国家发展和改革委员会	上海市发展和改革委员会
14	教育部	上海市教育委员会
15	科学技术部	上海市科学技术委员会
16	工业和信息化部	上海市经济和信息化委员会
17	国家民族事务委员会	上海市民族和宗教事务局
18	公安部	上海市公安局
19	国家安全部	上海市国家安全局
1A	民政部	上海市民政局
1B	司法部	上海市司法局
1C	财政部	上海市财政局
1D	人力资源和社会保障部	上海市人力资源和社会保障局
1E	自然资源部	上海市规划和自然资源局
1F	生态环境部	上海市生态环境局
20	住房和城乡建设部	上海市住房和城乡建设管理委员会
21	交通运输部	上海市交通委员会
22	水利部	上海市水务局（上海市海洋局）
23	农业农村部	上海市农业农村委员会
24	商务部	上海市商务委员会
25	文化和旅游部	上海市文化和旅游局
26	国家卫生健康委员会	上海市卫生健康委员会
27	退役军人事务部	上海市退役军人事务局
28	应急管理部	上海市应急管理局
29	中国人民银行	中国人民银行上海总部
2A	审计署	上海市审计局
2B	国有资产监督管理委员会	上海市国有资产监督管理委员会
2C	海关总署	上海海关

W1W2	中央政务部门	上海市对应的政务部门
2D	国家税务总局	上海市税务局（原上海市地方税务局）
2E	国家市场监督管理总局	上海市市场监督管理局
2F	国家广播电视总局	上海市文化和旅游局
30	国家体育总局	上海市体育局
31	国家统计局	上海市统计局
32	国家国际发展合作署	
33	国家医疗保障局	上海市医疗保障局
34	国务院参事室	上海市人民政府参事室
35	国家机关事务管理局	上海市机关事务管理局
36	国务院港澳事务办公室	上海市人民政府港澳事务办公室
37	国务院研究室	上海市人民政府研究室
38	新华通讯社	新华社上海分社
39	中国科学院	上海科学院
3A	中国社会科学院	上海社会科学院
3B	中国工程院	
3C	国务院发展研究中心	上海市人民政府发展研究中心
3D	中央广播电视总台	中央广播电视总台上海总站
3E	中国气象局	上海市气象局
3F	中国银行保险监督管理委员会	中国银行保险监督管理委员会上海监管局
40	中国证券监督管理委员会	中国证券监督管理委员会上海监管局
41	国家信访局	中共上海市委、上海市人民政府信访办公室
42	国家粮食和物资储备局	上海市粮食和物资储备局
43	国家能源局	国家能源局华东监管局
44	国家国防科技工业局	上海市国防科技工业办公室
45	国家烟草专卖局	上海烟草专卖局
46	国家移民管理局	上海市出入境管理局
47	国家林业和草原局	上海市绿化和市容管理局
48	国家铁路局	上海铁路局
49	中国民用航空局	
4A	国家邮政局	上海市邮政管理局
4B	国家文物局	上海市文物局
4C	国家中医药管理局	上海市中医药管理局
4D	国家煤矿安全监察局	
4E	国家外汇管理局	国家外汇管理局上海市分局
4F	国家药品监督管理局	上海市药品监督管理局
50	国家知识产权局	上海市知识产权局
~5F	预留	

B类用于标识党委、人大、政协、高检、高法、群团、民主党派等，W1码为6。

W1W2W3	中央政务部门	上海市对应的政务部门
党委部门		
600	中共中央纪律检查委员会机关	上海市纪委监委
601	中共中央办公厅	中共上海市委办公厅

W1W2W3	中央政务部门	上海市对应的政务部门
602	中共中央组织部	中共上海市委组织部
603	中共中央宣传部	中共上海市委宣传部
604	中共中央统战部	中国共产党上海市委员会统一战线工作部
605	中共中央对外联络部	
606	中共中央政法委员会机关	中共上海市委政法委员会
607	中共中央政策研究室	
608	中共中央台湾工作办公室	中共上海市委台湾工作办公室
609	中共中央对外宣传办公室	中共上海市委对外宣传办公室(市政府新闻办公室)
60A	中共中央财经委员会办公室	中共上海市委财经工作委员会办公室
60B	中共中央外事工作委员会办公室	中共上海市委外事工作委员会办公室
60C	中共中央机构编制委员会办公室	中共上海市委机构编制委员会办公室
60D	中央和国家机关工作委员会	中共上海市委市级机关工作委员会
60E	中央党校	中国共产党上海市委员会党校
60F	中共党史和文献研究院	中共上海市委党史研究室
610	中央编译局	
611	人民日报社	人民日报社上海分社
612	求是杂志社	
613	光明日报社	光明日报社上海记者站
614	中国浦东干部学院	
615	中国井冈山干部学院	
616	中国延安干部学院	
~61F	预留	
人大、政协、高法、高检机构		
620	全国人民代表大会	上海市人大常委会办公厅
621	中国人民政治协商会议	上海市政协办公厅
622	最高人民法院	上海市高级人民法院
623	最高人民检察院	上海市人民检察院
~62F	预留	
群众团体		
630	中华全国总工会机关	上海市总工会
631	共青团中央委员会机关	共青团上海市委员会
632	中华全国妇女联合会机关	上海市妇女联合会
633	中国文学艺术界联合会机关	上海市文学艺术界联合会
634	中国科学技术协会	上海市科学技术协会
635	中国国际贸易促进委员会(中国国际商会)机关	上海市国际贸易促进委员会
636	中国残疾人联合会机关	上海市残疾人联合会
637	中华全国新闻工作者协会机关	
638	中华全国台湾同胞联谊会机关	上海市台湾同胞联谊会
~63F	预留	

W1W2W3	中央政务部门	上海市对应的政务部门
民主党派		
640	中国国民党革命委员会中央委员会机关	中国国民党革命委员会上海市委员会
641	中国民主同盟中央委员会机关	中国民主同盟上海市委员会
642	中国民主建国会中央委员会机关	中国民主建国会上海市委员会
643	中国民主促进会中央委员会机关	中国民主促进会上海市委员会
644	中国农工民主党中央委员会机关	中国农工民主党上海市委员会
645	中国致公党中央委员会机关	致公党上海市委
646	九三学社中央委员会机关	九三学社上海市委员会
647	台湾民主自治同盟	台湾民主自治同盟上海市委员会
~64F	预留	

C类预留，用于标识部队、武警、央企、国企等，W1码为7。

D类预留，结合区划域，用于标识中央政务部门非对口的地方其他政务部门。

当W1取值为A-F时，为乡镇以下行政区划或基层借用部门域，由各区县自行分配。

如各部门选择由国家条线分配的IPv6地址段，须向上海市大数据中心报备。

4. 子网域（Y码）编码规范

子网域由各级政务部门自行分配。

5. 主机域

65~128位为主机域，规划为接口标识，支持EUI-64规范。

3.9.2.5 政务外网网络平台地址各字段值使用的原则

类型域值为240B:80时，标识IPv6地址为政务外网网络平台地址，包括网络设备的端口IP地址、DNS服务器IP地址、网络管理、运营和支撑系统IP地址等，其区划域、部门域、主机域的设置遵循以下原则：

1. 根据设备或网络的管理权归属设置区划码。

如上海市市级政务外网的管理权归属于市级政府部门，设备之间的接口地址区划码均应设置为3C:000（上海市区划码），并通过将子网域从1依次增加来区分网络设备的多个子网和不同接口。

2. 根据接入区或接入部门的区划码/部门码填写跨区、跨部门、跨机构的链路地址。

上海市市级政务外网与各区、各接入部门对接的接口地址，或区级政务外网与各区级接入部门对接的接口地址，应根据接入区、接入部门的区划码、部门码填写。如徐汇区接入到市级政务外网，该链路上网络设备对接的接口地址按徐汇区的区划码3C:084填写。

3. 点到点链路按/127掩码配置

为避免遍历攻击及简化配置，P2P（inter-router）的接口地址应按/127位掩码配置，主机域的前63位（65~127位）设置为0，如下表：

地址空间	EUI-64	
	主机域	P2P2 LINK
位数（bit）	63	1
IPV6 前缀位置	65~127	128
取值	0	0~1

如徐汇区与上海市政务外网网络设备的互联接口地址为：240B:803C:0840:0001::0/127、240B:803C:0840:0001::1/127。

4. 网管、DNS等配套设施应根据资产归属部门或设备的管理权归属设置区划域、部门域，主机域采用64-EUI编码处理。

3.10 DNS 域名规划和管理

3.10.1 域名规划和管理总体要求

根据《国务院办公厅关于加强政府网站域名管理的通知（国办函〔2018〕55号）》和《上海市人民政府办公厅关于进一步加强本市政务网站域名管理工作的通知》要求，上海市各区人民政府办公室、市政府各部门办公室是本地区、本部门所属政府网站域名管理的责任主体。政府网站主办单位要按照“谁开设、谁申请、谁使用、谁负责”的原则管理政府网站域名。一个政府网站原则上只注册一个中文域名和一个英文域名，如已有多个符合要求的域名，应明确主域名。不得将已注册的政府网站域名擅自转给其他单位或个人使用，闲置的域名要及时注销。

3.10.2 域名结构规范

1. 政府网站应使用以“.gov.cn”为后缀的英文域名和“.政务”为后缀的中文域名，不得使用其他后缀的域名。

2. 各区政府门户网站要使用“www.□□□.gov.cn”结构的英文域名，其中□□□为本地区、本部门名称拼音或英文对应的字符串(下同)。市政府各部门政府网站不单独使用顶级英文域名，要统一使用“中国上海”门户网站的下级英文域名，结构为“□□□.sh.gov.cn”。其中，

○○○为本部门名称拼音或英文对应的字符串（下同）。

3. 政府网站各栏目、频道、专题以及基于互联网开设的业务系统、管理系统等原则上使用本级网站同一级域名。其中，区政府门户网站的栏目等使用“www.□□□.gov.cn/.../...”结构的域名；市政府各部门网站的栏目等使用“○○○.□□□.gov.cn/.../...”结构的域名。

4. 政府网站中文域名结构应为“△△△.政务”，其中△△△为网站主办单位的中文机构全称或规范化简称（下同）。政府网站各栏目、频道等使用同一级域名，其结构为“△△△.政务/.../...”。

3.10.3 域名流程管理

1. 域名注册流程。各区政府门户网站注册“.gov.cn”“.政务”域名的，须经本地区主要负责人同意，并向市政府办公厅提交政府网站域名业务申请，由市政府办公厅审核同意后，统一向国家域名注册管理机构提交申请。市政府各部门网站申请“中国上海”门户网站下级域名的，须经本部门主要负责人同意，并向市政府办公厅提交政府网站域名业务申请，经市政府办公厅审核同意后，由市大数据中心按照审批意见，统一分配下级域名。

2. 域名注销流程。注销域名为“.cn”“.政务”的，须经本地区、本部门主要负责人同意，并向市政府办公厅提交政府网站域名业务申请，由市政府办公厅审核同意后，统一向国家域名注册管理机构申请注销；域名为其他顶级域名的，由域名持有者联系相应的注册机构自行注销。

3. 域名信息变更报备。政府网站域名持有者变更，须经政府网站主管单位同意；联系人等注册信息发生变更的，要在变更后的20个工作日内向政府网站主管单位报备。区政府门户网站域名相关信息变更的，政府网站主管单位要及时通知国家域名注册管理机构更新信息。

3.10.4 域名安全防护规范

1. 加强域名解析安全防护。政府网站主办单位要积极采取域名系统(DNS)安全协议技术、抗攻击技术等措施，防止域名被劫持、被冒用，确保域名解析安全。要委托具有应急灾备、抗攻击等能力的域名解析服务提供商进行域名解析，鼓励对政府网站域名进行集中解析。使用内容分发网络(CDN)服务的，应当要求服务商将境内用户的域名解析地址指向其境内节点，不得指向境外节点。

2. 加强监测处置。政府网站主办单位要加强对政府网站域名安全的日常监测和定期检查评估，及时发现域名被劫持、被冒用等安全问题，健全完善处置机制，提高应急响应处置能力。

3.11 IP 路由协议

上海市政务外网IGP路由协议建议采用IS-IS、OSPF等路由协议同时承载IPv4和IPv6路由，域间路由协议采用MP-BGP协议。此外，核心层部署路由器做RR反射器（或核心路由器兼做RR），各汇聚路由器与RR建立iBGP关系；出口路由器与国家政务外网建立EBGP邻居，互相通告路由。

3.11.1 路由策略总体要求

政务外网路由策略的总体要求为：

1. 政务外网应实现业务网络路由和用户路由分离。IGP负责承载设备之间的互联链路、Loopback、网管等的承载网路由；BGP负责承载区政务外网和接入部门网络、数据中心等的用户路由。管理上层次分明，从而避免用户路由震荡影响业务网络路由，保证局部的变动不影响上层路由配置和全局路由配置。

2. 区级政务外网业务网络路由和用户路由可以由IGP统一承载。当具备条件时，也可以与市级政务外网保持一致，进行业务网络路由和用户路由的分离。

3. 路由设计应能反映出整个网络的层次结构，并与自治域、各节点子网的IP地址分配相结合，做到合理的路由聚合，减少路由表的长度，减轻路由更新给设备带来的负荷，提高路由稳定性。

4. 在同一AS内，应根据网络流量分担、分布与路由备份需要，统一规划路由Metric值，实现路由策略。

5. 合理规划IGP区域。对于新建网络，在单管理域设备数量较少时，可以配置为单区域。

3.11.2 IGP 路由实施

市、区两级政务外网在各自治域内根据网络规模自行划分IGP路由区域。在网元数量不多、网络规模不大的情况下，路由协议不需划分区域或层次，核心层和汇聚层设备可规划在同一个路由区域或层次内，并将该自治域内设备的Loopback地址映射为全网唯一的标识地

址，以实现IGP协议承载Loopback、互联链路等业务网络路由。

3.11.3 BGP 路由实施

自治域内，所有PE运行MP-BGP承载VPNv4、VPNv6和EVPN路由，选取两台核心设备兼做路由反射器（RR）或设置独立RR。骨干层所有PE路由器与这两台RR建立iBGP关系。

不同的AS域，需要运行EBGP协议，互相通告路由。

3.11.4 互联网出口路由实施

IPv4互联网出口：出口路由器配置静态默认路由，或通过BGP向运营商发布本地IPv4路由，并接收互联网路由或默认路由。出口防火墙配置IPv4公网地址池，进行IPv4公私网地址转换。使用多运营商出口的网络启用负载均衡功能，将对外访问流量按照运营商IP地址归属或自定义策略进行路径优化和带宽优化。政务外网其他设备通过IGP或IBGP从出口路由器学习IPv4默认路由。

IPv6互联网出口：出口路由器通过BGP向运营商发布本地IPv6路由，并接收互联网路由或默认路由，出口防火墙仅配置IPv6路由和安全规则。政务外网其他设备通过IGP或IBGP从出口路由器学习IPv6默认路由。

3.11.5 管理路由和业务路由部署

管理路由：政务外网核心层及汇聚层的三层设备选取loopback作为管理接口，在IGP协议中宣告即可；政务外网的二层设备，建议单独创建一个管理地址，通过接入的三层网关宣告到IGP协议中。

业务路由：政务外网PE设备与接入设备对接，需要在PE上将接入用户的路由信息直接宣告到BGP中。条件允许的，PE接入的用户网段可以先在本地做路由聚合，然后宣告到BGP中。此外，政务外网中会承载多种VPN业务，须将各接入用户的路由在不同的VPN下宣告。

四、 电子政务外网运行管理规范

上海市电子政务外网市级网络由市大数据中心负责运行管理，各区电子政务外网由区政务外网管理单位负责运行管理。

上海市电子政务外网的各级运行管理单位，应向政务外网的各级使用单位和部门提供服

务受理、网络监控、安全管理、变更管理、故障处理、资源管理、性能管理、流程管理和报告管理等服务。

4.1 运行管理单位的职责

4.1.1 服务受理

1. 受理网络使用单位和部门提出的服务请求；
2. 记录服务请求信息和网络使用单位、部门的意见；
3. 对职责内的服务请求进行处理；
4. 跟踪或监控服务请求处理过程并向网络使用单位和部门反馈；
5. 与网络使用单位和部门确认并关闭服务请求；
6. 提供各类网络服务信息、故障统计等信息。

4.1.2 网络监控

1. 负责对网络运行情况进行实时监控、可视化呈现；
2. 负责发现和报告网络故障；
3. 负责网络监控任务单的资源配置并组织完成任务；
4. 负责网管系统技术资料的收集、整理和归档工作。

4.1.3 技术支持

1. 负责网络的维护、安全运行和支撑工作；
2. 负责对网络故障进行及时诊断、定位和排查；
3. 组织实施网络业务的变更，制定维护作业计划并落实；
4. 负责各类网络资源的动态维护与管理；
5. 负责分析研究网络运行状态，周期性形成网络运行的分析报告；
6. 负责网络的评估，提出升级、改造方案并组织实施；
7. 制定网络应急保障预案并进行演练、实施；
8. 负责收集、整理本级网络及下一级上报的网络数据，形成网络运行维护数据资源，并对接上报至上一级网络运行维护数据资源库；
9. 负责技术资料的收集、整理和归档工作。

4.2 运行管理单位的服务内容

4.2.1 服务受理

1. 受理网络使用单位和部门的所有服务请求，如业务咨询、业务变更和故障申告等；
2. 应答网络使用单位和部门提出的业务咨询，提供相关信息；
3. 对于网络使用单位和部门提出的网络业务申请和故障申告，启动变更管理和故障管理服务，并跟踪服务过程，及时向网络使用单位、部门反馈处理状态和结果；
4. 记录服务请求与执行过程中的各种信息，按规定发布信息并归档。

4.2.2 网络监控

1. 对电子政务网络进行实时监控、实时呈现，及时发现故障、诊断并定位故障，并组织处理和跟踪反馈；
2. 实时监控各项网络运行性能指标，记录网络运行数据，并提供对网络运行状态的分析与预警判断，主动预防并干预可能的网络故障风险因素，事后支持运行状态追溯与分析管理；
3. 当出现网络设备告警或性能劣化告警时，应记录事件中告警发生时间、告警类型、告警信息和告警发现人等信息，并具备判断告警是否影响电子政务网络的使用。必要时启动故障管理服务。

4.2.3 安全管理

1. 安全管理制度
 - 1) 制定各类管理规定、管理办法和暂行规定。
 - 2) 制定严格的制定与发布流程，方式，范围等，制度需要统一格式并进行有效版本控制；发布方式需要正式、有效并注明发布范围，对收发文进行登记。
2. 安全管理机构
 - 1) 制定安全管理机构的组织形式和运作方式，明确岗位职责；
 - 2) 设置安全管理岗位，设立系统管理员、网络管理员、安全管理员等岗位；成立指导和管理信息安全工作的委员会或领导小组，其最高领导由单位主管领导委任或授权；制定文件明确安全管理机构各个部门和岗位的职责、分工和技能要求。
 - 3) 建立授权与审批制度；

- 4) 建立内外部沟通合作渠道；
- 5) 定期进行全面安全检查，特别是系统日常运行、系统漏洞和数据备份等。

3. 人员安全管理

根据基本要求制定人员录用，离岗、考核、培训几个方面的规定，并严格执行；规定外部人员访问流程，并严格执行。

4. 系统建设管理

制定系统建设管理制度，包括：系统定级、安全方案设计、产品采购和使用、自行软件开发、外包软件开发、工程实施、测试验收、系统交付、系统备案、等级评测、安全服务商选择等方面。

5. 系统运维管理

进行网络系统日常运行维护管理，包括：环境管理、资产管理、介质管理、设备管理、监控管理和安全管理中心、网络安全管理、系统安全管理、恶意代码防范管理、密码管理、变更管理、备份与恢复管理、安全事件处置、应急预案管理等，使系统始终处于相应等级安全状态中。

4.2.4 变更管理

各级运行管理单位应对网络使用单位、部门的变更申请进行处理，包括网络接入、业务开通、业务关闭和业务变更：

1. 网络接入

受理网络使用单位和部门的网络接入申请，并进行网络接入操作，更新资源管理信息库，并向网络使用单位和部门反馈网络接入操作完成信息。

2. 业务开通

受理网络使用单位和部门提出的业务开通申请，并进行业务开通操作，更新资源管理信息库，并反馈给网络使用单位和部门。

3. 业务关闭

受理网络使用单位和部门的业务关闭申请，并进行业务关闭操作，更新资源管理信息库，并反馈给网络使用单位和部门。

4. 业务变更

受理网络使用单位和部门的业务变更申请，并进行业务变更操作，更新资源管理信息库，并反馈给网络使用单位和部门。

4.2.5 故障处理

各级运行管理单位受理本级的故障申告。故障处理流程如下：

1. 接到故障申请后，应记录故障信息，并生成故障单。故障单的内容至少包括：电子政务外网用户标识码、业务类型、电路代号、业务通达方向、故障发生时间、故障现象描述、申告人或联系人等信息；
2. 对故障进行预处理；
3. 对于重大故障，应启动应急预案，并及时分析总结故障处理情况；
4. 应及时向故障申告人反馈故障进程；
5. 故障解决后，进行记录并与故障申告人确认故障解决。

4.2.6 故障处理升级

各级运行管理单位应制定故障升级制度。故障升级以故障对用户业务的影响程度为依据，在同级内升级。如有必要，应向上一级运行管理单位提交升级报告，并对故障升级情况进行记录。故障升级记录中应包括：故障的上报人、升级时间、升级对象、通报内容、升级反馈时间及修复时间等。故障报告内容应包括：严重影响网络使用单位、部门通信的网络故障、故障处理超时、疑难故障处理不当等信息。

需升级的电子政务外网重大故障分为四类：

1. I类：电子政务网络重大通信故障，网间通信故障，各种自然灾害、突发事件等导致大量业务受阻的故障；
2. II类：由于网络资源提供者的原因造成电子政务网络业务全阻或部分阻断；
3. III类：重要链路在通信保障期间发生的故障；
4. IV类：由于网络资源提供者的原因造成的独立故障。

需升级的业务网络重大故障分为四类：

1. I类：网络完全拥塞；
2. II类：网络处理能力及用户的业务运作有严重影响；
3. III类：网络故障对重要的用户业务运作造成影响；
4. IV类：网络故障对多数用户业务运作造成影响。

4.2.7 故障报告

故障处理完成后，应以多种形式（例如书面形式）提供统一格式的故障处理报告和网络质量运行报告，并由运行管理单位提供给网络使用单位和部门。

故障处理报告应至少包括：用户名称、用户编码、故障申告时间、业务恢复时间、故障历时、故障处理过程、故障原因、处理结果及改进措施或建议。

网络质量运行报告应至少包括电子政务网络整体运行情况、租用电路运行报表、用户故障申告报表、重点故障原因分析、措施及建议。

4.2.8 资源管理

1. 各级运行管理单位应建立资源管理信息库，对电子政务网络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、网络拓扑结构、网络IP地址使用情况、设备型号、端口资源、板卡型号、编码信息、软件配置、位置信息等；

2. 运行管理单位在向网络使用单位、部门提供服务的过程中，应及时更新资源信息库，并保留修改记录；

3. 运行管理单位应每季度向网络使用单位、部门提供资源管理报告。资源管理报告应至少包括：资源清单、资源变更情况；

4. 下级运行管理单位应定期向上级运行管理单位提供本级的资源管理报告。

4.2.9 性能管理

1. 各级运行管理单位应向网络使用单位、部门提交网络性能分析报告和性能优化建议报告；

2. 各级运行管理单位应针对性能优化建议报告与网络的使用单位、部门进行充分的沟通，由其确定是否实施。如需实施，则需协调相关单位、部门共同完成实施操作，并由网络使用单位、部门组织验收。

4.2.10 报告管理

各级运行管理单位应提供定期和不定期两种报告给网络使用单位、部门。其中：

1. 定期报告

A. 季度运行报告：包括每季度电子政务网络和设备的整体性能，各项服务执行情况，

下个季度服务改进计划和性能优化建议。季度运行报告应在每季度初提交；

B. 年度运行报告：包括上一年度电子政务网络和设备的年度整体性能，整体服务情况总结，新年度服务改进计划和性能优化建议。每年一月份提供上一年度运行报告。

2. 不定期报告

A. 故障管理、变更管理、资源管理服务过程中提交的报告。包括故障处理报告、变更管理报告、资源管理报告等；

B. 网络使用单位、部门应及时反馈各种交付报告的意见和建议；

C. 各级运行管理单位将该级及下一级的上述报告进行搜集整理后，向上一级运行管理单位上报；

D. 各级运行管理单位应对重要信息进行保存。这些信息包括：网络运行报告、统计分销数据、重大故障记录、网络资源数据。

4.2.11 服务质量管理控制

各级运行管理单位应制定各种规范和制度，各级网络的使用单位、个人需遵循此类规范和制度。

规范和制度应包括：各种操作规范、行为规范、语音规范、人员管理制度、考勤管理制度、文档管理制度、保密管理制度等。

4.3 运行和安全监测支撑系统规范

市、区两级政务外网运行管理单位，须部署基于软件定义网络技术、具备支持防御新型未知网络攻击、大数据安全分析能力的政务外网运行和安全监测支撑系统。政务外网运行和安全监测支撑系统还应具备对市、区两级政务外网运行状况统一管理的能力，通过建设统一监控管理、资源管理、工单管理、可视化决策中心等功能，提升运行维护故障处理的服务质量，实现网络业务质量和服务过程的实时呈现及规范化管理。

市、区两级政务外网运行和安全监测支撑系统须按照国家电子政务外网《运行支撑平台对接与实施规范》规范要求，分别完成与国家、市、区政务外网运维管理功能的对接工作；须按照《政务网络安全监测平台总体技术要求》（T/CIA 005-2019）的规范要求，分别完成国家、市、区各级安全监测系统的对接工作。市、区政务外网运行和安全监测支撑系统需预留对其他运行管理支撑系统的互通接口。

政务外网运行和安全监测支撑系统由建设该系统的运行管理单位负责日常维护和管理。

4.3.1 系统架构

政务外网运行和安全监测支撑系统总体架构分为服务与展示层、核心功能层、数据采集层和资源层。其中，服务与展示层提供系统的统一入口，并提供综合展示界面；核心功能层提供统一监控、统一资源管理、集中工单管理、统一安全管理、系统内部的分级协同能力，以及对外的系统接口；采集层采集告警数据、配置数据、性能数据等，供上层调用；资源层是系统需要纳管的对象，包括网络设备、安全设备、机房环境等。

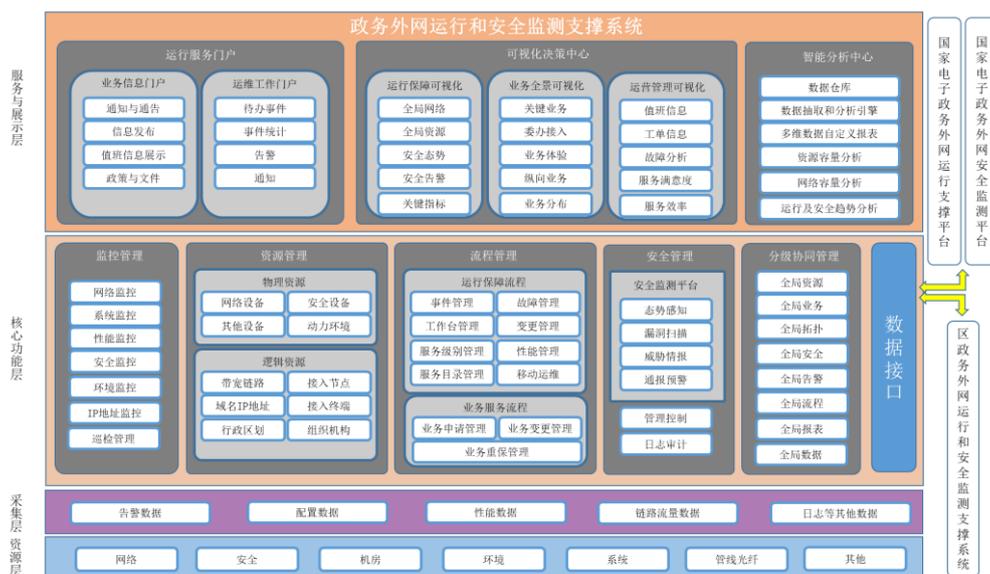


图22 政务外网运行和安全监测支撑系统架构图

4.3.2 主要功能

运行和安全监测支撑系统应具备如下主要功能模块：

1. 资源层

资源层实现对电子政务外网的全栈式纳管，主要包括网络设备、安全设备、机房的环境动力等设备，还要包括网络控制器等网管类系统。

2. 采集层

采集层应通过SNMP协议、SFTP、部署探针等方式，与网络控制器或纳管设备进行对接，实现对外部系统和中央网络系统的基础设施软硬件及各种应用开展数据采集、上报工作，内容应包含告警数据、配置数据、性能数据、链路流量数据及日志等其他数据。

其中，告警数据、配置数据、配置对象上下联关系数据应从各网络控制器北向接口获取，需整理分析各网络控制器的北向接口格式及数据规格，针对各网络控制器的数据规格，进行定制的适配器设计。适配器负责完成各网络控制器与运行和安全监测支撑系统的数据交互。

对于性能数据的获取，应支持通过SFTP方式从网络控制器获取；对于链路流量数据的获取，应支持部署探针的方式获取。

3. 核心功能层

核心功能层需具备监控管理、资源管理、流程管理、安全管理及分级协同管理五大核心能力及对外系统接口。各模块要求如下：

1) 监控管理模块：应能实现对上海电子政务外网整体运行状况的及时监控与主动预警，能对网络故障进行有效定位，提供对设备及业务运行状况的辅助分析能力。

功能至少包含：

- 对采集层上报的网络、系统、性能、安全、环境、IP地址资源等运行、告警信息进行汇聚、分析、管理。以图片、文字、数据等方式展现各时间点的性能情况，并具备搜索功能，回顾历史某一时间点性能情况；以图片、文字、数据等方式直观呈现告警位置，便于判断故障是否可能对业务造成影响；
- 对采集层上报的告警信息进行处理，实现包括告警记录自动存档、历史呈现、告警自动生成工单等；
- 对采集层上报的告警信息进行归纳合并，将满足规则的告警信息合并成一组，以入库第一条告警信息作为主告警，后面根据合并规则入库的告警均归纳合并为同组告警。各项告警信息均可提供详细告警描述，并支持向运维人员提供多种形式的告警信息查询的功能；
- 系统支持巡检管理模块，可根据运维需要自定义巡检内容、时间、频率等，以实现自动化巡检及管理工作的开展。

2) 资源管理模块：应能将监控管理模块中要求的各项被管理资源形成统一的资源管理库。其中，物理资源包括网络设备、安全设备、机房动力环境等资源信息，所对应的详细信息包括但不限于：资产名称、资产版本、资产物理位置、维保信息、生命周期等。逻辑资源包含带宽链路、接入节点、域名IP地址、接入终端、行政区划和组织机构等资源信息，所对应的详细信息包括但不限于：名称、地址、组织归属、所属关系等。其管理功能至少应包括：

- 所有设备统一实现生命周期管理，实时同步资源信息，满足资源的高效供给和动态调度的需求；
- 提供灵活的检索引擎，可以通过多个字段组合过滤信息，也可以自定义搜索字段；
- 带有内置的设备配置模型模板，并支持手工录入信息和导入信息；

- 资源库可以对资源进行管理，包括资源间的链接关系、依赖关系、主从关系和父子关系等。

3) 流程管理模块：应能提供敏捷的运维管理流程，提升流程处理的协作能力，支持各级信息化部门维护工作的全流程化，实现工作任务可计量、可考核、可评估，提高整体效率。流程管理分为运行保障流程及业务服务流程，运行保障流程应至少包括事件管理、故障管理、工作台管理（服务请求管理）、变更管理等流程，还应包含服务级别管理、服务目录管理、移动运维功能；业务服务流程至少包括业务申请、业务变更管理、业务重保等流程，以实现从业务申请到业务发放和变更的端到端流程保障。功能至少应包括：

- 内置相关流程模型，并支持用户通过图形化页面操作对流程进行自定义配置、测试和发布，从而建立复杂的所见即所得流程。宜支持通过图形界面简单拖拉拽的方式编排流程流过程；
- 支持服务等级承诺（SLA）策略的设计和定义；
- 流程管理提供服务统计功能，支持线图、柱状图、饼图等多种形式展示近期工单的产生情况、闭环情况、进展情况；
- 支持排班设定及管理；
- 支持移动运维，支持在移动终端上查看工单及进行工单审批等操作。

4) 安全管理：将电子政务外网安全设备的日志、探针获取的流量信息进行大数据关联分析，整体评估市电子政务外网的网络安全状态。安全管理功能模块须至少包含安全监测系统、管理控制模块和日志审计模块，其中安全监测系统须至少包含态势感知模块、漏洞扫描模块、威胁情报共享模块和通报预警模块。安全管理功能至少包括：

- 支持安全设备日志的收集、汇总、分析和检索查询；
- 支持对网络设备、安全设备的运营管理和安全策略的集中管理；
- 通过Restful API等标准接口向服务与展示层提供安全态势、设备运行状态、安全告警、威胁情报等安全监测信息；
- 通过数据接口模块实现与国家电子政务外网安全监测系统、区电子政务外网运行和安全监测支撑系统的信息共享和数据交互。

5) 分级协同管理：将监控管理模块、资源管理模块、安全管理模块和流程管理模块中的信息进行联动、协同处置，实现全局数据融合处理。同时能够通过各模块联动，将全局资源、全局业务、全局报表、全局数据进行融合调用。如，通过资源管理模块与监控管理模块的联动，实现全局告警在全局拓扑中可视；通过监控管理模块与流程管理模块联动，

实现全局告警自动生成工单，帮助全局流程流转。

6) 数据接口：提供对外Restful API等标准接口，将核心功能层各模块数据上报给国家电子政务外网运行支撑系统及国家电子政务外网安全监测系统，同时接收各区电子政务外网运行和安全监测支撑系统的上报信息。

4. 服务与展现层

服务与展示层提供运行服务门户功能模块、可视化决策中心功能模块和智能分析中心功能模块，为用户提供服务界面及功能入口，提供全网运行情况及决策信息展示，并利用大数据分析技术提供多维度的运行状态分析及趋势研判支撑。各模块要求如下：

1) 运行服务门户

为政务外网运行和安全监测支撑系统提供统一鉴权的服务入口，包含业务信息门户和运维工作门户。业务信息门户应具备用户公告、值班信息公告、政策与文件公告等功能；运维工作门户支持运维人员进行个性化显示信息的定制，包括待办事件、事件统计等信息。

2) 可视化决策中心

从运行保障、业务全景、运营管理三个维度，形成可视化专题，通过大屏呈现等方式，帮助电子政务外网主管单位和运营维护人员随时了解现网运行状况，以辅助做出网络调整、优化等决策。

- 运行保障可视化：拉通各维度运维数据，提供资源、资产、安全态势、安全告警、关键运行指标等信息的可视化展示，具备至少三层下钻能力；
- 业务全景可视化专题：从业务视角、各委办接入的质量情况、量化的业务体验情况、纵向承载重点业务的网络设备运行健康度情况、各业务在线用户、并发请求数、流量占用等维度进行业务的可视化呈现；
- 运营管理可视化专题：对值班排班信息、工单处理情况和服务效率、故障类型和数量、工单处理的服务满意度等进行统计及呈现；

3) 智能分析中心

调用核心层以及采集层生成的数据，通过大数据等智能分析技术，生成定制的分析报告，为运维管理提供决策和调优依据。

4.3.3 网络协同维护

按照国家电子政务外网“统筹建设、分级负责、属地管理”的制度要求，上海市电子政务外网运行和安全监测支撑系统需要与国家电子政务外网运行支撑系统进行运维管理功能

的对接，实现对网络设备、链路、主机设备等资源的运行状态监控和综合管理。各区电子政务外网运行和安全监测支撑系统应与市电子政务外网运行和安全监测支撑系统进行运维管理功能的对接，以实现国家电子政务外网管理中心对上海市全市电子政务外网的统一监控和管理。

4.3.3.1 运维管理功能对接整体框架

上海市电子政务外网运行和安全监测支撑系统运行管理功能的对接结构，应遵循《国家电子政务外网运维管理系统对接规范》（征求意见稿）规范要求，如下所示：

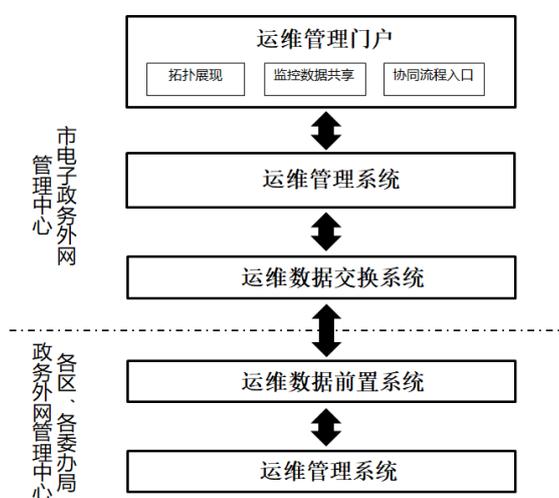


图23 运维管理功能对接整体框架

运维数据交换系统的作用是收集、存储运维数据交换前置系统传来的运维数据。

运维数据前置系统的作用是对接当地的运维管理系统，采集运维数据，并传送给指定的运维数据交换系统。

运维数据交换系统和运维数据前置系统配合使用。

4.3.3.2 运维管理功能对接的数据内容

上海市电子政务外网运维管理功能的对接数据类型，应遵循《国家电子政务外网运维管理系统对接规范》（征求意见稿）所规定的运维数据类型，包括接入节点数据、设备配置数据、设备子资源配置数据、拓扑关系数据、设备性能数据、设备端口性能数据、设备告警事件、设备端口告警事件等。

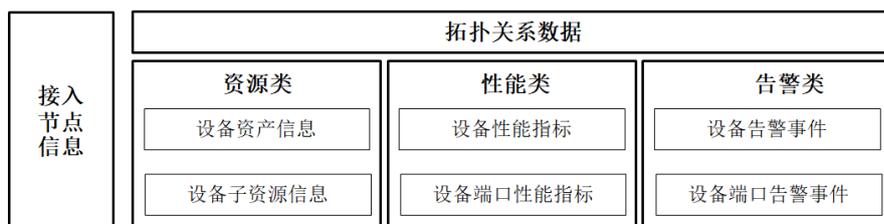


图24 运维管理功能数据类型

各类型数据在对接过程中的详细字段及字段值，应遵循《国家电子政务外网运维管理系统对接规范》（征求意见稿）中对交互字段的描述、定义和规则。

4.3.3.3 运维管理功能对接的模式

按照《国家电子政务外网运维管理系统对接规范》（征求意见稿）规定，根据场景不同，有三种不同的运维功能对接模式：

1. 同构模式：对接双方使用相同品牌的运维系统。

此模式下，“运维数据交换系统”和“运维数据交换前置系统”都是运维系统的功能之一，无需再额外单独部署，可以通过运维系统已有的功能实现对接。

2. 异构模式：对接双方使用的运维系统品牌不同。

此模式下，需要在各区安装一套“运维数据交换前置系统”，并对现网的运维系统进行接口开发，以实现运维数据在两套不同运维系统之间的传递。

接口开发的流程、规范应符合国家电子政务外网运维管理系统对接规范的规定。

3. 过渡模式：运维系统暂不具备对接条件，应通过安装与上海市电子政务外网运维管理系统版本相同的运维系统，在过渡期间先满足对接需要。