ICS 35.020
CCS L 70

DB31

上 海 市 地 方 标 准 化 指 导 性 技 术 文 件

DB31DSJ/Z 003-2024

电子政务外网网络建设规范

Specification for construction of E-government network

2024-05-15 发布

2024-06-01 实施

上海市数据局 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。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由上海市数据局提出。

本文件由上海市数据标准化技术委员会归口。

本文件起草单位：上海市大数据中心、云赛智联股份有限公司、东方有线网络有限公司、华为技术有限公司。

本文件主要起草人：杜守国、邱晨明、胡甜、夏斌、陈正伟、靳玲、甄彬、虞翱亮、邵波、赵洪业、杨昊、高丽、王韵凯、章建兵、连娅、宁庭勇、韩兆祥、李冰、彭炜、楚鑫伟、吴坚、陈姝。

电子政务外网网络建设规范

1 范围

本文件规定了电子政务外网（以下简称“政务外网”）网络的总体架构、建设要求、技术要求及安全要求。

本文件适用于指导上海市政务外网网络规划、设计、建设及运行管理。

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 22239—2019 信息安全技术 网络安全等级保护基本要求

YD/T 2484 分组增强型光传送网（OTN）设备技术要求

YD/T 3843 接入型光传送网（OTN）设备技术要求

YD/T 3966 软件定义光传送网（SDOTN）总体技术要求

3 术语和定义

下列术语和定义适用于本文件。

3.1

电子政务外网 e-government network

承载跨地区、跨部门的业务应用、信息共享、业务协同和不需在政务内网上运行的业务，与互联网逻辑隔离，满足各级部门经济调节、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。

4 缩略语

下列缩略语适用于本文件。

BGP：边界网关协议(Border Gateway Protocol)

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

DNS：域名系统 (Domain Name System)

FRR：快速重路由（Fast Reroute）

H-QOS：层次化服务质量（Hierachical Quality of Service）

IGP：内部网关协议（Interior Gateway Protocol）

IPSec：IP 安全协议（IP Security）

IPv4：网际协议版本 4（Internet Protocol version 4）

IPv6：网际协议版本 6（Internet Protocol version 6）

IS-IS：中间系统-中间系统协议（Intermediate System-to-Intermediate System）

MPLS：多协议标记交换（Multi-Protocol Label Switching）

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）
VLAN：虚拟局域网（Virtual Local Area Network）
VPN：虚拟专用网络（Virtal Private Network）
VxLAN：虚拟可扩展局域网（Virtual Extensible LAN）
SDN：软件定义网络（Software Defined Network）
SR：分段路由（Segment Routing）
SRv6：IPv6 段路由（IPv6 Segment Routing）

5　总体架构

5.1　概述

市、区政务外网由以下三部分组成，总体架构图见图1。

a)　光传输网络：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。
b)　业务网络：基于IP技术，采用数据平面和视频平面互为备份的“一网双平面”架构。
c)　管理系统承载网：基于IP技术，为市、区两级政务外网运行和安全监测支撑系统提供独立、封闭的网络。

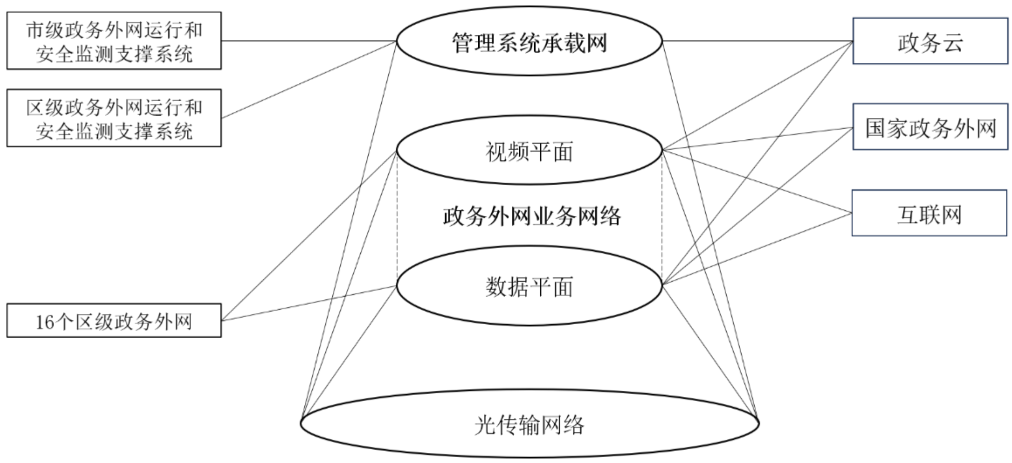

图1　政务外网总体架构图

5.2　光传输网络架构

5.2.1 光传输网络采用OTN技术组网，为业务网络提供大带宽、低时延、高可靠的传输通道。
5.2.2 光传输网络采用分层组网架构，分为核心层、汇聚层和接入层。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，设置核心节点和汇聚节点。
5.2.3 接入层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。

5.3　业务网络架构

政务外网业务网络采用分层架构，分为核心层、汇聚层和接入层：

a)　核心、汇聚层应承载于光传输网络之上；

b) 采用“一网双平面”的架构设计，数据平面承载数据流量，视频平面承载视频流量，两个平面逻辑隔离、独立运行，且互为冗余备份；

c) 核心层承担高速数据交换任务，同时与上一级政务外网和互联网连接。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，应至少设置两个或两个以上核心节点，并确保每个核心节点部署在不同物理位置的机房；

d) 汇聚层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考虑；

e) 接入层提供政务外网各使用单位的网络接入。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；

f) 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。

5.4 管理系统承载网架构

5.4.1 管理系统承载网采用IP技术组网，基于市、区两级政务外网的光传输网络实现市、区政务外网管理系统的互联互通，与业务网络采用不同光传输通道进行数据传送，实现与业务网络的波长及隔离。

5.4.2 管理系统承载网采用汇聚层、接入层两级组网架构。接入层将市、区两级政务外网的管理和分析流量统一接入，通过市、区两级光传输网络传送至管理系统承载网的汇聚层设备，再由汇聚层设备转发至市级政务外网运行和安全监测支撑系统，进行数据的综合分析及汇总呈现。

6 建设要求

6.1 光传输网络

6.1.1 基本要求

政务外网光传输网能与现有网络兼容，具体要求如下：

a) 宜采用单波速率100G及以上的OTN技术；

b) 应支持带宽平滑扩容，网络具备向200G及以上速率带宽平滑扩容的能力；

c) 应采用分层分域的组网架构，网络具有自愈能力，并为政务应用提供安全可靠的传输通道；

d) 应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；

e) 应具有多种业务统一承载的能力，提供FE、GE、155M、10GE、40GE等多种业务类型的接口，具备与已建网络互联互通的能力；

f) 应支持光纤线路诊断功能，快速定位光纤线路故障；

g) 宜采用SDN技术，实现对业务和链路的快速下发和调整；

h) 市级政务外网应使用G.652D或G.654E规格的光缆，光纤在1550nm附近的每公里线路衰耗在0.3dB以下；区级政务外网应使用G.652或G.655规格的光缆，光缆每公里线路衰耗在0.3dB以下。

6.1.2 核心节点

核心节点满足以下要求：

a) 核心层节点设备应具备带宽易扩容、升级的特点，宜支持集群功能；

b) 核心节点之间互联应采用网状或环形组网结构；

c) 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；

d) 核心节点之间开通两个不同路由的光传输通道，对承载业务进行冗余保护；

e） 区级政务外网核心层传输网络应考虑与市级政务外网传输网络的对接，应遵循业界统一标准。

6.1.3 汇聚节点

6.1.3.1 汇聚节点设备应根据机房环境的复杂性和多样性，选取低功耗、高集成度的设备。
6.1.3.2 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应开通两个不同路由的光传输通道。

6.1.4 传输设备技术要求

政务外网传输设备应符合YD/T 3966、YD/T 2484、YD/T 3843中的规定。

6.2 业务网络

6.2.1 基本要求

政务外网业务网络应满足以下要求：
a） 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；
b） 符合GB/T 22239—2019中的相关规定；
c） 不同应用在业务网络相互独立，可选用VLAN、VxLAN、VPN、网络切片等方式实现不同业务的隔离；
d） 采用国产化的网络和安全设备和系统；
e） 采用SDN技术，实现业务快速部署；
f） 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、服务质量进行实时监控和主动运维。

6.2.2 通信链路

政务外网业务网络带宽要求见表1。

表1 业务网络带宽要求

分类	链路类型	速率
市级业务网络	核心节点之间	100Gbps
	与国家政务外网之间	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
区级业务网络	核心节点之间	40 Gbps～100Gbps
	与市政务外网之间	N×1Gbps 或 N×10Gbps
	核心节点与下级汇聚节点之间	40 Gbps～100Gbps
	同一汇聚节点内主备冗余设备之间	40 Gbps～100Gbps
	汇聚节点与下级接入节点之间	N×1Gbps 或 N×10Gbps

6.2.3 核心节点

核心节点应满足如下要求：

a) 核心层设备支持用户流量安全、高速、可靠转发的功能；
b) 核心节点设备选型满足面向未来业务发展平滑扩展的需要；
c) 核心节点采用高冗余设计，保证核心网络的高可靠性；
d) 核心节点数不少于2个，每个核心节点部署不少于两台路由器设备。市级两台设备之间不少于100G链路互相冗余，区级两台设备之间为40Gbps～100Gbps链路互相冗余。不同核心节点之间应有多条冗余链路，市级核心节点之间互联带宽不少于100G，区级不少于40Gbps～100Gbps。

6.2.4 汇聚节点

汇聚节点采用双归方式接入核心节点，每个汇聚节点部署两台路由器设备。

市级政务外网汇聚节点向上通过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。

区级政务外网汇聚节点向上通过40Gbps～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。

6.2.5 接入节点

政务外网的接入设备以N×1Gbps或N×10Gpbs链路连接至汇聚节点。

各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。

6.3 管理系统承载网

管理系统承载网应承载于光传输网络之上，并与业务网络采用不同的光传输通道进行数据传送，实现与业务网络的波长级隔离部署。

管理系统承载网应支持IPv4/IPv6双栈技术，并通过SRv6隧道实现端到端直达。

管理系统承载网应支持智能检测技术，实现网络智能运维。

管理系统承载网应具备为市、区两级政务云系统管理数据互连、全市非涉密灾备数据的传输提供扩展能力，应逐步建立网络主备设备、链路的冗余保护机制，确保网络具备面向未来的带宽升级能力和业务调度管理能力。

6.4 市、区两级网络互连互通

6.4.1 光传输网络互联互通

市、区两级政务外网光传输网通过电层客户侧接口对接，对接方式如下：
a) 通过传输设备的电层客户侧接口（GE/10GE/100GE、FC等）直接对接；
b) 两方传输设备通过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。

6.4.2 业务网络互联互通

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，该接入设备与区级政务外网的出口设备放置于同一机房，两者通过光纤直联。接入设备宜通过N×10Gbps链路与市级政务外网的汇聚交换机联接，宜通过N×1Gbps或N×10Gbps链路与区级政务外网的出口设备联接。

市、区两级政务外网互联互通应设置安全接入区，并符合GB/T 22239—2019中规定的第三级安全要求。安全接入区应包括但不限于出口路由器、入侵防御、防火墙、防病毒等功能设备。

市、区两级政务外网建设满足以下要求：
a) 应选用IS-IS/IS-ISv6、OSPF/OSPFv3、BGP(BGP4+)作为互联协议；
b) 应选用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；

c) 可选用OTN光传输网络进行市、区两级政务外网的对接；
d) 应通过SDN技术实现智能路径计算和流量调优功能，以及网络和应用流量的精细化管理和分析；
e) 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。

6.4.3 管理系统承载网互联互通

管理系统承载网的汇聚层和接入层基于市、区两级光传输网的对接，实现市、区两级政务外网管理数据的互联互通。市、区两级光传输网对接方式如下：

a) 宜采用光传输设备的彩光技术对接（单个波长λ的波分侧信号80km内直接对接，两者采用同一波长，λ1～λ40可选），即市、区两级政务外网的光传输环网设备线路侧彩光口（λ1）直接互联；
b) 可采用光传输设备的灰光技术对接（如OTU2灰光），即市、区两级政务外网的光传输环网设备线路侧模块（OTU2灰光）直接互联。

7 技术要求

7.1 IP 地址规划和管理

7.1.1 IPv4 地址规划

7.1.1.1 IPv4 地址分类

政务外网使用的IPv4网络地址分为以下两类：

a) 国家政务外网互联共享地址（59.X.X.X）应以区级政务外网为单位向市级政务外网管理单位申请；
b) 市政务外网本地网络地址（10.X.X.X/16）应以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，若增加应向政务外网管理单位申请。视频专网（含视频共享平台）IP 地址为10.224.0.0/16，视频终端地址IP地址范围为10.166.0.0/16-10.171.0.0/16。

7.1.1.2 IPv4 地址分配和变更

7.1.1.2.1 IPv4地址由政务外网管理单位统一分配。

7.1.1.2.2 IPv4地址发生变更时，应向政务外网管理单位进行书面申请，变更后的IPv4地址由政务外网管理单位统一分配。

7.1.1.2.3 IPv4地址存在冲突时，应向政务外网管理单位进行申请变更。

7.1.2 IPv6 地址规划

7.1.2.1 IPv6 地址组成

IPv6地址由128位二进制数组成，采用十六进制表示。IPv6地址格式为x:x:x:x:x:x:x:x，其中x为一个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。

7.1.2.2 IPv6 地址区域划分

IPv6地址分为固定前缀区、自定义前缀区、主机地址区共三个区域，具体规划详见附录A。三个区域要求如下：

a) 固定前缀区共30位，包括固定前缀、类型域和区划域-省市；

b) 自定义前缀区用于标识政务外网内部各子网，共计34位，包括区划域-区县、部门域和子网域；
c) 主机地址区用于标识政务外网内各种设备网络接口，共计64位。

7.1.2.3 IPv6 地址分配管理

IPv6地址分配应遵循“先申请，后使用”的原则，由政务外网管理单位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应为本系统市、区级单位进一步分配IPv6地址块。

路由设备的互联地址和Loopback地址应由政务外网管理单位统一分配。

7.2 DNS 域名规划和管理

7.2.1 DNS 域名应符合以下规则要求：

a) 国家政务外网采用 cegn.cn 作为根域名，上海市政务外网采用 sh.cegn.cn 作为国家政务外网根域的子域；
b) 市级接入单位采用上海市政务外网的子域名“委办局.sh.cegn.cn” 作为域名，如市统计局域名为“tjj.sh.cegn.cn”；
c) 各区接入单位采用上海市政务外网的子域名“区名.sh.cegn.cn”作为域名，上海市各区政务外网域名见附录 B；
d) 政务外网域名原则上不超过 5 段，如“主机名.单位名.sh.cegn.cn”；
e) 接入上海市政务外网的四级域名（四级域名.sh.cegn.cn）应向政务外网管理单位申请并向 sh.cegn.cn 域注册，各区可基于上海市政务外网建设子域（四级域名.sh.cegn.cn）；
f) 域名优先注册顺序为各单位中文简称首字母、各单位英文简称以及其它能够标识本单位的字符或数字组合，已注册域名不可重复注册。

7.2.2 域名服务应支持IPv4/IPv6域名查询（A/AAAA记录查询），且IPv6和IPv4的域名查询互不影响。域名服务应支持AAAA请求递归查询。

7.3 IP 路由协议

7.3.1 政务外网 IGP 路由协议宜采用 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。

7.3.2 政务外网应分离业务网络路由和用户路由。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。

7.4 IPv6 网络设计

7.4.1 IPv6 网络协议

政务外网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。

7.4.2 IPv6 协议部署和业务访问

政务外网业务网络设备应支持IPv4/IPv6双栈技术，同时支持IPv4和IPv6网络的接入。

7.4.3 IPv6 安全要求

IPv6网络应具备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。

7.5 网络管理

7.5.1 基本要求

政务外网应引入网络管理系统，具备以下功能：

a) 支持配置、性能、故障、安全、日志等管理功能；

b) 支持流量动态调整、隧道带宽动态调整、隧道路径控制和调优、节点和链路流量控制、维护窗口业务保障等网络控制功能；

c) 支持应用流量采集与呈现、网络故障仿真、流量预测等网络分析功能。

7.5.2 配置管理

网络设备和业务的配置管理应包含以下内容：

a) 支持根据用户需求查询、修改、备份网络设备信息，包括系统信息、路由信息、接口信息以及VPN信息；

b) 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；

c) 提供统一拓扑发现功能，支持全网监控，实时监控所有网络设备的运行状况；

d) 支持业务自动化发放、部署及按需调整，支持的业务类型包括动态L3 VPN、动态TE隧道、QOS/H-QOS；支持的业务组合包括动态L3 VPN、动态TE隧道和QOS/H-QOS的组合部署。

7.5.3 性能管理

网络设备和业务的性能管理应包括以下内容：

a) 性能监控：支持创建、修改、删除、挂起、恢复性能监控实例功能；支持性能监控实例分组管理功能；支持调度差异化性能策略；

b) 设置性能监视门限值：支持性能参数越过或低于一定的门限值时，发出告警通知；

c) 性能分析和管理：支持对性能数据进行分析、统计和计算性能指标；支持管理性能数据、查看历史性能、性能数据转储。

7.5.4 故障管理

网络设备和业务的故障管理应包括以下内容：

a) 故障信息采集：支持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、门限告警、设备/端口/链路状态变化告警等；

b) 故障监视：支持监视网元和网络路由，出现故障时进行显示；

c) 故障处理过程管理：记录故障产生、变化、消除过程等排错行为；

d) 故障信息的查询与统计。

7.5.5 安全管理

安全管理应包括以下内容：

a) 用户权限管理：管理不同职责的用户对系统和资源的操作权限；

b) 用户维护和监控：在权限维护期内，根据需要查看或编辑用户信息、角色信息、操作集信息等，并实时监控用户会话及用户操作；

c) 远端认证：通过配置AAA认证协议实现与第三方系统的对接；

d) 账号安全策略：支持对用户的帐号进行登录或锁定策略的设置；

e) 密码安全策略：支持设置密码的复杂度、更新周期、字符限制等；

f) 登录IP地址控制策略：支持根据需要设置登录IP地址控制策略，限制用户仅从特定IP地址区间登录系统；

g) 登录时间控制策略：支持根据需要设置登录时间控制策略，限制用户仅在特定的时间段内登录系统。

7.5.6 日志管理

应支持自动记录系统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。日志导出格式应统一，能自动生成报表，支持图形化展示。审计日志应至少保存6个月。

日志应由政务外网管理单位统一管理。

7.5.7 IPv6 网管系统

IPv6网管系统应满足以下要求：

a) 支持IPv4地址对各种IPv6地址类型设备的识别和管理；
b) 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；
c) 支持对双栈设备进行IPv4及IPv6的关联，使双栈设备资源、性能、故障等数据与历史数据平滑关联；
d) 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、流量等信息。

8 安全要求

8.1 网络边界

8.1.1 网络边界划分

政务外网可根据联接网络对象以及承载信息系统的安全等级，划分为以下五种不同的安全区域和边界：

a) 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；
b) 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；
c) 第三类区域：各单位政务网接入到对应市、区级政务外网的边界，防范非法跨网用户对政务外网的非授权访问；
d) 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；
e) 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。

8.1.2 网络边界管理要求

8.1.2.1 政务外网接入单位应当在符合国家网络安全等级保护要求的前提下接入政务外网，并采取安全措施，保障本单位网络安全。

8.1.2.2 政务外网管理单位应当建立运行和安全监测支撑系统，支持系统运行状态上报、告警上报、安全事件上报、风险上报、案例上报、威胁情报共享、预警通报、漏洞上报等功能。

8.1.2.3 政务外网管理单位应当依托政务外网运行和安全监测支撑系统，开展网络安全监测、大数据分析、态势感知、预警通报等网络安全管理工作。

8.1.3 网络边界区域安全要求

不同的安全区域应采取不同强度的安全保护措施，具体见表 2。

表 2 网络边界区域安全保护措施

安全保护措施类别		第一类区域	第二类区域	第三类区域	第四类区域	第五类区域
抗 DDoS 攻击	应在该接入区域部署抗 DDoS 攻击设备，支持 DDoS 检测和清洗。支持抵抗常见的 SYN Flood、ACK Flood、FIN/RST Flood 功能，能抵抗 HTTP、HTTPS Flood 等攻击，且支持流量自学习功能，可识别超过防御阈值的攻击流量。	√				
AAA 认证	应在该接入区域部署 AAA 服务器，用于无线通信网络用户的认证、授权功能。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。				√	
网络访问控制	应在该接入区域部署防火墙，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。防火墙应双机部署，且支持性能的可扩容。防火墙应支持 IPv6 协议栈、NAT64 转换技术。	√	√	√	√	√
入侵检测和防御	应在该接入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，及时发现漏洞、蠕虫、木马等非法和异常行为，并支持告警、阻断等功能。	√	√	√	√	√
防病毒	应在该接入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。防病毒模块可集成在防火墙内。	√	√	√	√	√
APT 检测	宜在该接入区域旁路部署沙箱，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对威胁的实时阻断。	√	√	√	√	√
VPN 网关部署	宜在该接入区域部署 VPN 网关，针对从互联网接入的远程办公用户或拨号接入的无线通信网用户，提供 SSL、IPSec 等形式的 VPN 接入网关功能。VPN 网关应支持国密算法。	√			√	
探针部署	宜在该接入区域部署探针，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。	√	√	√	√	√
日志审计	支持日志审计和管理，支持日志统一格式输出、报表自动生成及图形化展示，且审计日志至少保存 6 个月。	√	√	√	√	√

8.2 安全管理中心

8.2.1 基本要求

8.2.1.1 市、区两级政务外网应建设安全管理中心。安全管理中心应包含态势感知、通报预警、威胁情报共享、漏洞扫描、安全管理控制、日志审计共 6 个子系统。

8.2.1.2 区级安全管理中心的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。

8.2.2 态势感知

态势感知子系统宜包括数据采集层、数据存储和挖掘层、态势展现层，具体功能如下：

a) 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；
b) 数据存储和挖掘层：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；
c) 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、区两级政务外网应在汇聚节点及网络边界区域部署探针，探针规格要求见表 3。

表 3 探针规格要求

流量大小	探针规格
≤1Gbps	1Gbps
1Gbps-5Gbps	5Gbps
5Gbps-10Gbps	10Gbps

8.2.3 通报预警

8.2.3.1 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。
8.2.3.2 通报预警子系统应对安全态势、威胁和漏洞情况进行汇总、分类、分级和研判处理，并自动形成通报报告。
8.2.3.3 通报预警按照安全风险和影响程度分为高危、中危和低危事件。

8.2.4 威胁情报共享

8.2.4.1 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接口开发，或单独建设开发。
8.2.4.2 威胁情报共享子系统应对安全情报进行收集、分析与处理、数据管理等。情报信息包括恶意样本、恶意 IP/URL/MD5 库、黑客组织信息、攻击方法手段、安全资讯等。

8.2.5 漏洞扫描

8.2.5.1 漏洞扫描子系统可单独部署漏洞扫描设备，或集成在态势感知子系统内部相关功能模块。
8.2.5.2 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，支持系统配置基线核查、资产自动发现、远程自动升级、本地升级最新漏洞库等功能。

8.2.6 安全管理控制

安全管理控制子系统应以独立软件的形式部署在服务器或虚拟机上，并具备以下功能：

a) 设备管理：支持设备自动发现、设备及设备组的增删改查、设备配置一致性对比、设备单点登录、设备版本升级、设备配置文件备份；

b) 策略管理：支持设置源/目的安全区域、源/目的地址、服务、时间段等匹配条件；支持对策略组视图和设备视图进行策略快速管理；支持策略变更统计、配置一致性统计、部署状态统计等；

c) 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；支持低风险策略自动审批；

d) 策略仿真：支持通过学习业务互访关系，对比待部署策略，并模拟部署方式，评估策略对业务的影响；

e) 协同联动：支持安全管理控制子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。

8.2.7 日志审计

安全日志子系统应支持流量日志、威胁日志、系统日志、管理员运维日志的审计功能。

附 录 A
（规范性）
IPv6 地址编码规则

A.1 IPv6 地址规划

政务外网 IPv6 地址具体规划见表 A.1，其段结构为：240B:8TZZ:ZZZW:WWYY::/64，分为以下五个字段：

a) 1-24 位，类型域，240B:8T，用于标识政务外网各类业务；
b) 25-44 位，区划域，ZZ:ZZZ，用于标识中央、省、市、县四级行政区域；
c) 45-56 位，部门域，W:WW，用于标识各级政务部门、乡镇及以下行政区域；
d) 57-64 位，子网域，YY，由各级政务部门自行规划分配；
e) 65-128 位，主机域，规划为接口标识，支持 IEEE EUI-64 标准，可根据接口 MAC 地址自动生成唯一标识。

表 A.1 IPv6 地址规划

地址空间	省市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

A.2 类型域（T 码）

类型域（T码）用于标识政务外网各类业务（T表示十六进制字符，取值范围为0-7），编码规则见表A.2。

表 A.2 类型域（T 码）编码规则

地址编码	业务系统类型
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

A.3 区划域（Z 码）

区划域 ZZ:ZZZ 用于标识中央、省、市、县四级行政区域（Z_1、Z_2、Z_3、Z_4、Z_5分别表示十六进制字符，取值范围为 00000-FFFFF）。

以民政部行政区划代码为基础，将 6 位十进制字符（区划代码）县级以上行政区划代码分为 3 段：AA.BB.CC，其中 AA 编码详见图 A.1，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 位二进制字符，最后按 4 位一组转换成 5 位十六进制字符，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（详见图 A.1）=>001111-0000000-0000000（分别转化成二进制，位数不够前补零）=>0011-1100-0000-0000-0000（4 位一组）=> 3C000（转换成十六进制区划码）。

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	24
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 A.1 省级地址 AA 对照表

按以上规则，上海 1+16 区划域编码见表 A.3。

表 A.3 上海 1+16 区划域编码

序号	区域	行政区划代码	区划域编码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

表 A.3 上海 1+16 区划域编码（续）

序号	区域	行政区划代码	区划域编码 ZZ:ZZZ	二进制区划码
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

A.4 部门域（W 码）

部门域（W 码）用于标识各级政务部门、乡镇及以下行政区域（W_1、W_2、W_3 分别表示十六进制字符，取值范围为 000-FFF），编码规则如下：

a) 各政务部门使用其所对应的中央部委或机构的部门域，具体对应关系见 A.6；

b) 当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；

c) 独立设置且在中央未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。

A.4 子网域（Y 码）

子网域（Y码）用于标识不同系统类型所属的业务子网（Y_1、Y_2分别表示十六进制字符，取值范围为 00-FF），各级政务部门根据实际情况自行分配。

A.5 主机域

65～128 位为主机域，规划为接口标识，可根据接口 MAC 地址自动生成唯一标识，支持 EUI-64 标准。

A.6 部门域分配规则

A 类（W_1=1-5）为市级政务部门，用于上海市各政务部门使用的部门域，W_1、W_2 与中央部委或机构的 W_1、W_2 部门域保持一致。对应关系见表 A.4。

表 A.4 A 类部门域

W_1W_2	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
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

表 A.4 A 类部门域（续）

W_1W_2	中央政务部门	上海市对应的政务部门
36	中共中央港澳事务办公室	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	国家金融监督管理总局	国家金融监管总局上海监管局
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	国家矿山安全监察局	
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
51	国家数据局	上海市数据局
52	国家疾病预防控制局	上海市疾控局
53	国家消防救援局	
54	供销总社	上海市供销合作总社
～5F	预留	

B 类（W_1=6）用于标识党委、人大、政协、高检、高法、群团、民主党派等具体见表 A.5。

表 A.5 B 类部门域

$W_1W_2W_3$	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 中华人民共和国国家监察委员会机关	中共上海市纪律检查委员会 上海市监察委员会
601	中共中央办公厅	中共上海市委办公厅
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	中共中央统一战线工作部	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	中央国家安全委员会办公室	
609	中央网络安全和信息化委员会办公室	中共上海市委网络安全和信息化委员会办公室
60A	中央军民融合发展委员会办公室	中共上海市委军民融合发展委员会办公室
60B	中共中央台湾工作办公室	中共上海市委台湾工作办公室
60C	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
60D	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
60E	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
60F	中央和国家机关工作委员会	中共上海市市级机关工作委员会
610	中央党校	中共上海市委党校
611	中共党史和文献研究院	中共上海市委党史研究室
612	人民日报社	人民日报社上海分社
613	求是杂志社	
614	光明日报社	光明日报社上海记者站
615	中国浦东干部学院	
616	中国井冈山干部学院	
617	中国延安干部学院	
618	中央社会主义学院	上海市社会主义学院
619	中共中央社会工作部	中共上海市社会工作委员会
61A	国家档案局	上海市档案局
61B	国家密码管理局	上海市密码管理局
～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

表 A.5 B 类部门域（续）

$W_1W_2W_3$	中央政务部门	上海市对应的政务部门
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	中国共产主义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	中国作家协会机关	上海市作家协会
635	中国科学技术协会机关	上海市科学技术协会
636	中华全国归国华侨联合会机关	上海市归国华侨联合会
637	中国法学会机关	上海市法学会
638	中国人民对外友好协会机关	上海市人民对外友好协会
639	中华全国新闻工作者协会机关	上海市新闻工作者协会
63A	中华全国台湾同胞联谊会机关	上海市台湾同胞联谊会
63B	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
63C	中国残疾人联合会机关	上海市残疾人联合会
63D	中国红十字会总会机关	上海市红十字会
63E	中国人民外交学会机关	上海公共外交协会
63F	中国宋庆龄基金会机关	上海市宋庆龄基金会
640	黄埔军校同学会机关	上海市黄埔军校同学会
641	欧美同学会（中国留学人员联谊会）机关	上海市欧美同学会
642	中国思想政治工作研究会机关	上海市思想政治工作研究会
643	中华职业教育社机关	上海中华职业教育社
644	中华全国工商业联合会机关	上海市工商业联合会
645	中国计划生育协会机关	上海市计划生育协会
～64F	预留	
民主党派		
650	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
651	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
652	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

表 A.5 B 类部门域（续）

$W_1W_2W_3$	中央政务部门	上海市对应的政务部门
653	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
654	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
655	中国致公党中央委员会机关	中国致公党上海市委员会
656	九三学社中央委员会机关	九三学社上海市委员会
657	台湾民主自治同盟	台湾民主自治同盟上海市委员会
～65F	预留	

C类（W_1=7），用于标识部队、武警、央企、国企等。

D类（W_1=8），结合区划域（Z码），用于标识地方在中央没有对口的部门。

预留（W_1=9），未来政务外网业务发展，预留规划。

当W_1取值为A-F时，表示乡镇以下行政区划或基层组织借用部门域。

附 录 B
（规范性）
上海市各区政务外网域名

上海市各区政务外网域名详见表B.1。

表B.1 上海市各区政务外网域名

序号	区域	区政务外网域名
1	浦东新区	pdq.sh.cegn.cn
2	黄浦区	hpq.sh.cegn.cn
3	静安区	jaq.sh.cegn.cn
4	徐汇区	xhq.sh.cegn.cn
5	长宁区	cnq.sh.cegn.cn
6	普陀区	ptq.sh.cegn.cn
7	虹口区	hkq.sh.cegn.cn
8	杨浦区	ypq.sh.cegn.cn
9	宝山区	bsq.sh.cegn.cn
10	闵行区	mhq.sh.cegn.cn
11	嘉定区	jdq.sh.cegn.cn
12	金山区	jsq.sh.cegn.cn
13	松江区	sjq.sh.cegn.cn
14	青浦区	qpq.sh.cegn.cn
15	奉贤区	fxq.sh.cegn.cn
16	崇明区	cmq.sh.cegn.cn

参考文献

[1] GB/T 25070—2019 信息安全技术网络安全等级保护安全设计技术要求
[2] GB/T 28448—2019 信息安全技术网络安全等级保护测评要求
[3] YD/T 1170—2001 IP网络技术要求-网络总体
[4] DB52/T 1619—2021 电子政务外网与业务网融合规范
[5] DB23/T 3343—2022 电子政务外网IP地址规范
[6] DB32/T 3514.1—2019 电子政务外网建设规范 第1部分：网络平台
[7] DB65/T 4536.1—2022 电子政务外网建设规范 第1部分：网络架构
[8] DB37/T 4630.1—2023 电子政务外网 第1部分：总体要求
[9] GW0209—2019 国家电子政务外网IPv6地址规划（试行版）
[10] 上海市电子政务外网管理办法（沪府办〔2020〕33号）