**政务外网网络优化升级服务采购需求**

**一、项目概况**

1.1项目名称：政务外网网络优化升级服务

1.2项目地址：临港新片区

1.3服务期限：合同签订后90天内

1.4预算金额：129.6万元

1.5项目说明：

临港新片区目前有政务外网和独立出口的互联网，政务外网和互联网逻辑隔离。采用单引擎的单一设备作为核心的网络架构。目前临港新片区没有视频专网，所有视频数据通过局域网组网，平台通过政务外网数据平面互联公安网视频网，通过对接自建视频平台、公安图像网等实现图像上传、共享。视频目前已接入约11000路，后续计划接入能力扩容至30000路。目前视频并发量为1000路，计划并发能力扩容至1500路。

浦东新区、奉贤区及其他区已经实现了政务外网视频平面、数据平面相隔离的双平面，图像网也已经搬迁到政务外网视频平面，过渡期后会影响公安视频的访问，因此亟需对政务外网网络优化升级，实现一网双平面架构。

**二、具体内容及要求**

2.1建设目标

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要求，做强电子政务“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，本次政务外网优化升级方案的建设目标聚焦于显著提升视频传输的稳定性，构建一个稳定、高效、安全的视频传输网络平台，为远程协作、应急指挥、公共服务等关键视频应用场景提供坚实的技术支撑。

确保临港新片区监控视频等数据能与市视频专网、浦东视频专网进行数据互通。

确保视频传输的高可用性与低延迟：通过优化网络拓扑结构，增加冗余链路与节点，确保政务视频会议、远程监控等视频传输活动的高可用性与超低延迟表现，即使在高峰时段或网络拥堵情况下也能保持流畅无阻。

增强视频传输的抗干扰能力：将数据流量与视频流量进行分离传输，有效抵御网络波动与突发状况对视频传输质量的影响，确保视频画面清晰稳定。

实现端到端的视频传输安全：采用严格的访问控制机制，确保视频数据在传输过程中的安全性，防止非法访问，为视频通信提供安全保障。

本次项目主要目标如下：

（1）提升新型智慧城市应用的可持续支撑能力，提升核心网络视频传输的承载能力，为建设新型智慧城市应用发展提供可持续支撑。

（2）提升政府社会管理和公共服务职能的保障能力，强化网络可靠性，形成7\*24小时不间断的政府社会管理能力和公共服务能力的网络保障。

（3）提升政务信息的综合安全防护能力，强化安全防护体系，形成对各类安全威胁的主动防御和安全态势的主动感知能力，提升政务信息服务的综合安全防护能力。

综上所述，本次项目将实施政务外网传输效能优化服务，完成“一网双平面”网络架构建设，通过4台高性能交换机和2台防火墙的部署与配置，将数据、视频流量归属分流，并达到网络冗余、高性能传输的效果，包含网络规划、网络调试、方案实施、网络互连等，确保业务连续性及传输可靠性，满足网络视频接入与并发能力扩容的需求，完成核心关键网络设备的高可用部署，建立故障切换机制，提高网络的容错能力。

结合临港新片区的实际应用和发展要求，为了保证满足使用需求，考虑到今后有较大的扩展空间，同时需具备良好的电源和网络条件。在网络系统设计时，主要应遵循以下原则：

（1）高性能：网络要求具有数据、图像、语音等多媒体实时通信能力。主干网应提供可保证的服务质量和充足的带宽，并具有发展能力，以适应未来网络技术的发展。采用核心层40G到汇聚层，10G到接入端；同时，核心层应具备100G接口扩展能力，以适应未来几年内业务需求增长对设备性能的需求。

（2）高可靠性：网络系统是日常业务和各种应用系统的基础设施，应保证工作日和重点时期不间断运行。整个网络应有足够的冗余，设备在发生故障时能以热插拔的方式在最短时间内加以修复；同时，可靠性还应充分考虑网络系统的性价比，使整个网络具有一定的容错能力，减少单点故障。

（3）标准化：所有网络设备和路由协议都应符合有关国际标准以保证不同厂家网络设备之间的互操作性和网络系统的开放性。

（4）可扩充性和可扩展性：所有网络设备不但满足当前需要，并在扩充模块后，满足可预见将来需求。网络设计要考虑网络系统应用和今后网络的发展，便于向更新技术的升级与衔接。要留有扩充余量，包括端口数量和带宽的升级能力。整体网络采用模块设计，保证新增职能部门、业务服务器的扩展灵活性，避免网络故障或网络威胁对整个业务与办公系统的影响。

（5）易管理性：网络设备应易于管理，易于维护，操作简单，易学，易用，便于进行网络配置，发现故障。

（6）支持多媒体：支持文本、语音、图形、图像及音频、视频等多种媒体信息的传输、查询服务，具有多种基于优先级队列的QoS保证，多媒体应用对服务质量有很高的要求，如带宽，延迟，延迟的变化等，需要网络对服务质量（QoS）有很好的支持。

（7）安全性：政务领域的数据、文件、视频多数具有较高的安全性需求，因此，网络系统必须提供较高的安全防护能力，对使用的信息进行严格的权限管理，在技术上提供先进的、可靠的、全面的安全方案和应急措施，最大程度上确保系统的安全运行。同时符合国家关于网络安全标准和管理条例。

（8）实用性：系统优化建设首先要从系统的实用性角度出发，未来信息传输都将依赖于计算机网络系统，所以系统设计必须具有很强的实用性，满足不同用户信息服务的实际需要，具有很高的性能价格比，能为多种应用系统提供强有力的支持平台；同时应很好地利用现有设备资源，保护已有投资。

遵从《上海市电子政务外网建设和运行管理指南》指导意见，按照“一网双平面”的架构对政务外网优化升级，从硬件设备上满足完全冗余架构，并配备防火墙安全设备，极大地提升临港新片区政务外网的稳定性、高效性、安全性，全方位补齐临港新片区一网双平面的视频层。

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，建设一张大带宽、高可靠、支持IPv6的视频专网，全面服务于临港新片区“一网通办”和“一网统管”。

网络架构示意图如下：



新建的视频专网作为视频专用网络，综合承载视频监控等多种业务，在临港新片区形成“横向到边、纵向到底”的覆盖全区的视频采集感知网络。临港新片区电子政务外网上联市级政务外网，并覆盖各部门、街镇和村居。

网络结构示意图如下：



同时，提供相应的技术保障服务，验收合格后，对系统提供不少于1年的免费维保服务，其中硬件设备不少于3年的免费维保服务。包括定期健康检查、配置优化及故障响应等技术支持，保障系统持续稳定运行。

在管委会核心机房部署两台40G核心级交换机，同一机房的核心交换机通过40G互联，在数据平面和视频平面上，两个机房的核心交换机两两一组分别做数据业务、视频业务双平面。

在城运中心数据机房部署两台40G核心级交换机，同一机房的核心交换机通过40G互联，在数据平面和视频平面上，两个机房的核心交换机两两一组分别做数据业务、视频业务双平面。

数据平面、视频平面采用主备的方案，数据流量由数据平面承载，当数据平面上的链路或设备发生故障时，业务会转发到视频平面上进行备份；当视频平面上的链路或设备发生故障时，业务会转发到数据平面上进行备份。

核心交换机基于模块化理念进行设计，采用模块化多进程空间系统结构，和基于多处理器并行处理机制以及空分交换结构的硬件体系结构，实现强劲的系统性能和高可靠性融合。核心交换机应支持多个业务槽位，具备100GE、40GE、10GE、GE等各种丰富的接口模块，并全面支持IPV6、MPLS VPN、组播、带宽控制、流量分析等业务功能。核心交换机应使整个系统具备高可靠性、高扩展性、强大的业务能力等特点，可以满足各种IP承载网的建设需求。同时，每台核心交换机的电源、风扇以及主控交换板均选择1+1冗余配置，避免因这三种关键模块中任一模块出现单点故障使整台设备宕机，造成业务中断。

新增两台40G防火墙，一台放置在临港办公中心核心机房的视频层，一台放置在城运中心核心机房的视频层，对视频层网络进行数据管理及安全防护，也可在目前过渡阶段对数据平面和视频平面起到数据互通的通道。

网络升级优化后的总体图如下：



（1）村居等下连单位的IP保持不变，在出口防火墙上新增视频平面出口，可以流畅的互通数据平面及视频平面。

（2）临港新片区视频汇聚平台IP保持不变，在出口防火墙上新增视频平面出口，可以流畅的互通数据平面及视频平面。

2.2需求清单

（1）需求汇总表

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 需求名称 | 单位 | 数量 |
| 1 | 核心交换机 | 台 | 4 |
| 2 | 视频层面防火墙 | 台 | 2 |
| 3 | 实施和维护服务 | 套 | 1 |

（2）详细技术要求

核心交换机

| 序号 | 参数类型 | 详细技术参数 |
| --- | --- | --- |
| 1 | ▲交换容量 | ≥ 400Tbps  |
| 2 | ▲包转发率 | ≥ 170000Mpps |
| 3 | 硬件架构 | 正交CLOS架构 |
| 4 | 交换网板≥5 |
| 5 | 风扇冗余，拔出一块风扇，系统温度保持正常 |
| 6 | 主控板冗余，倒换时间0ms |
| 7 | 电源模块冗余，倒换时间0ms |
| 8 | 板卡配置 | 支持FW/IPS/SSL VPN/ACG等安全板卡 |
| 9 | 虚拟化 | 支持4框虚拟化技术 |
| 10 | 支持跨设备链路聚合 |
| 11 | 支持1虚多技术 |
| 12 | QoS | 支持精细化的流量监管，粒度可达8K |
| 13 | 支持流量整形Shapping |
| 14 | ACL | 支持VLAN ACL |
| 15 | 支持全局 ACL |
| 16 | 可靠性 | 支持RRPP功能 |
| 17 | 支持ERPS环网技术 |
| 18 | 可视化 | 支持INT流量可视化功能，提供第三方测试报告 |
| 19 | 支持Telemetry流量可视化功能 |
| 20 | 融合 | 支持融合 AC 功能： 无需额外配置单独硬件，在交换机上实现对AP 的接入控制和管理，有线无线用户的统一认证管理，最大 AP上线数≥ 12K，最大 Client 上线数≥60K |
| 21 | 支持多业务融合板卡，能够与设备紧耦合无需外部连线，支持融合鹰视功能，实现对摄像头等物联终端统一识别、认证和管理 |
| 22 | MPLS | 支持L3 VPN |
| 23 | 支持VLL |
| 24 | ▲安全特性 | 支持ARP防攻击 |
| 25 | 支持MACsec加密技术，提供第三方测试报告 |
| 26 | 支持SNMPv1/v2/v3 |
| 27 | 支持端口镜像/流镜像/VLAN镜像 |
| 28 | 具备CPU防攻击能力，保障CPU工作安全，提供第三方测试报告 |
| 29 | IPv6 | 支持RIPng、OSPFv3、BGP4+、IS-ISv6协议，支持IPv6策略路由；支持DHCPv6功能、IPv6 portal功能、IPv6管理功能； 支持基于IPv4\IPv6的VRRP功能 |
| 30 | ▲实配 | 配备双引擎、双电源千兆以太网电口≥48个万兆以太网光口≥48个100G以太网光接口≥8个40G多模光模块≥2个 |

视频层面防火墙

| 序号 | 参数类型 | 详细技术参数 |
| --- | --- | --- |
| 1 | ▲硬件架构 | 采用多核架构，具备可插拔冗余电源模块，冗余风扇模块（多核架构需提供证明材料） |
| 2 | 存储 | 支持SSD硬盘不小于480G，HDD硬盘不小于1T |
| 3 | 可靠性 | 支持配置自动备份和回滚，通过FTP发送到指定服务器（提供功能截图） |
| 4 | 扩展性 | 要求具备接口扩展能力 |
| 5 | ▲实配 | 实配千兆电口≥8个，万兆光口≥8个，40G光口≥4个；1年IPS/AV/应用特征识别升级服务授权 |
| 6 | ▲性能要求 | 吞吐量不低于30Gbps 并发连接数至少1600 万 新建连接数至少50万 开启IPS及AV后，吞吐性能至少16Gbps |
| 7 | 升级服务 | 整机同时具备防火墙、服务器负载均衡、入侵防御、防病毒、应用识别和web应用防护（WAF）、威胁情报等功能 |
| 8 | 部署模式 | 实现路由模式、透明（网桥）模式、混合模式 |
| 9 | 路由实现 | 支持静态路由、策略路由、RIP、OSPF、BGP、IS-IS等路由协议（提供功能截图） |
| 10 | NAT功能 | 支持一对一、多对一、多对多等多种形式的NAT，支持DNS、FTP、H.323、RTSP、ILS、PPTP、SIP、SQLNET、MGCP、RSH、ICMP差错报文、TFTP、RTSP、SCTP、XDMCP、NBT、SCCP、HTTP等多种NAT ALG功能。 NAT地址池支持动态探测和可用地址分配（提供功能截图） |
| 11 | 支持NAT44、NAT46、NAT64、NAT66 |
| 12 | VPN | 可基于每个SSL VPN用户的会话连接数、连接时间和流量阀值进行细颗粒度的管控。（提供功能截图） |
| 13 | 支持IPsec VPN智能选路，根据隧道质量调度流量。（提供功能截图） |
| 14 | 支持SSL的版本包括TLS1.0、TLS1.1、TLS1.2、TLS1.3（提供功能截图） |
| 15 | 安全策略 | 支持基于域名的安全策略模糊匹配（提供功能截图） |
| 16 | 支持一体化安全策略，能够基于源/目的安全域、源IP/MAC地址、目的IP地址、地区、服务、时间、用户/用户组、应用层协议、五元组、内容安全（WAF、IPS、数据过滤、文件过滤、AV、URL过滤和APT防御等）统一界面进行安全策略配置 |
| 17 | 支持基于源安全域、目的安全域、源IP/MAC地址、目的IP地址、用户、应用、终端、服务、VRF和时间段进行策略冗余分析， 冲突策略分析以及命中率统计。 |
| 18 | WEB应用防护 | 支持为Web应用提供基于 HTTP 和 HTTPS 的流量防护。对来自Web应用程序客户端的各类请求进行内容检测和验证，确保其安全性与合法性，对非法的请求予以实时阻断，从而对各类网站进行有效防护。 |
| 19 | 应用识别 | 支持至少9000条以上的应用识别，且提示风险类型及风险级别，便于用户根据实际情况进行上网行为管理。（提供功能截图） |
| 20 | URL过滤 | 设备提供海量预分类的URL地址库，支持根据URL类别实现URL过滤； |
| 21 | 设备支持管理者自定义新的URL地址和URL分类； |
| 22 | 支持联动云端URL地址库进行全面实施核查。（提供功能截图） |
| 23 | 入侵防御 | 支持超过18000条以上特征的攻击检测和防御（提供功能截图） |
| 24 | APT | 支持沙箱（云沙箱或本地沙箱）联动（提供功能截图） |
| 25 | 威胁情报 | 支持IP信誉库、DNS信誉库、URL信誉库 |
| 26 | 支持挖矿行为检测和勒索病毒检测（提供功能截图） |
| 27 | 数据安全 | 支持数据防泄露，对传输的文件和内容进行识别过滤，对内容与身份证号、信用卡号、银行卡号、手机号等类型进行匹配。（提供功能截图） |
| 28 | 流量控制 | 可支持基于应用层协议设置流控策略，包括设置最大带宽、保证带宽、协议流量优先级等。要求支持带宽通道独占以及共享管理模式,支持父子带宽策略。（提供功能截图） |
| 29 | 共享上网管理 | 支持多用户共享上网行为管理（提供功能截图） |
| 30 | IPv6 | 支持IPv6下的访问控制、IPsec VPN、DDoS防护等安全功能 |
| 31 | ▲负载均衡 | 多出口智能选路，支持基于链路权重、带宽、配置优先级、链路质量、用户业务、运营商、域名、时间、DSCP、PPPoE、DNS、地址加权HASH等智能选路方式 |
| 32 | 支持智能DNS解析功能，引导访问用户从最优路径的线路接入应用系统 |
| 33 | 诊断中心 | 支持基于接口及IP的报文捕获，并将捕获到的报文生成Wireshark（一种网络封包分析软件）可识别的.cap后缀文件，保存到本地或外部服务器，供用户分析诊断出入设备的流量 |
| 34 | ▲虚拟化能力 | 所投设备须支持虚拟防火墙功能：支持虚拟防火墙的创建、启动、关闭、删除功能；可独立分配CPU/内存等计算资源；虚拟防火墙可独立管理，独立保存配置。（提供功能截图） |
| 35 | 支持2台设备堆叠成一台设备使用，实现统一管理，统一配置，所投设备支持高可靠性（包含主备/主主模式）部署。（提供功能截图） |
| 36 | 设备管理 | 支持SNMPv1、SNMPv2、SNMPv3、RMON等网络管理协议，并且支持通过网管软件远程进行设备软件升级、配置等 |
| 37 | 为了保证整个网络的可靠稳定，要求本次采购的安全设备支持A/S，A/A方式部署，支持配置同步和会话同步；  |
| 38 | 提供开放API接口（RESTful，NetConf），可编程管理防火墙，不再仅依赖网管软件。 |

2.3 网络实施要求

（1）实施要求

采购“一网双平面”系统实施服务，依托于“一网双平面”的架构，将政务外网业务流量按其数据、视频归属分流到两个平面上分别承载，整体的业务的流量模型将变得明晰，从而分流策略、业务保障策略和业务备份策略的部署就有了得以实施的基础，同时也有利于后续管理。

所采购的系统实施服务含设备调试，网络规划、网络部署，以及与上级单位的网络对接、IP申请等。提供针对性的详细拓扑结构，主要体现以下几方面:

1) 一网双平面网络架构设计(数据、视频分流设计）: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，建设一张大带宽、高可靠、支持IPv6的视频专网，全面服务于临港新片区“一网通办”和“一网统管”。

2) 核心节点高可靠性设计（可靠性设计、路由策略设计）:网络系统是日常业务和各种应用系统的基础设施，应保证工作日和重点时期不间断运行。整个网络，特别是核心设备，应有足够的冗余，设备在发生故障时能以热插拔的方式在最短时间内加以修复；同时，可靠性还应充分考虑网络系统的性价比，使整个网络具有一定的容错能力，减少单点故障。

3) 安全设计（可靠性设计、兼容性设计、贴合等保2.0三级等保要求）：政务领域的数据、文件、视频多数具有较高的安全性需求，因此，网络系统必须提供较高的安全防护能力，对使用的信息进行严格的权限管理，在技术上提供先进的、可靠的、全面的安全方案和应急措施，最大程度上确保系统的安全运行。同时符合国家关于网络安全标准和管理条例。

（2）网络割接要求

投标人必须提供整个网络割接的详细步骤、回退方案、得到用户批准后方可实施。

（3）兼容性要求

为了最大限度保护现有投资，投标人必须提供投标设备与主流网络系统的兼容性方案。

（4）实施团队要求

本次项目的交付需要团队提供项目开发、产品实施、系统迁移、运维保障等各种职责和角色的技术人员。为保障整个项目的交付和运维的顺利，需要整个团队的人员配置都具备较高的技术能力、经验和资质要求。

1）实施团队人员要求

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 角色 | 主要职责 | 人员数量 | 人员要求 | 驻场要求 |
| 项目负责人 | 负责项目总体质量和进度控制 | 1人 | 具备网络实施项目3年以上工作经验，不低于本科学历。 | 不驻场 |
| 技术负责人 | 负责项目实施的技术管理 | 1人 | 具备同类型项目工作经验，不低于本科学历。 | 不驻场 |
| 实施经理 | 负责现场实施人员安排，处理现场问题，上报施工进度、质量情况 | 2人 | 具备同类型项目工作经验，不低于本科学历。 | 不驻场 |

2）投标人应针对本项目提供不少于1人的质保期间支撑人员；投标人的相关服务人员需具备相应的服务能力。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 角色 | 主要职责 | 人员数量 | 人员要求 | 驻场要求 |
| 维护工程师 | 负责项目运行维护 | 1人 | 熟悉项目各环节并完成基本维护，每个月对完成一次巡检并出具巡检报告 | 不驻场 |

（5）实施进度要求

|  |  |  |
| --- | --- | --- |
| 序号 | 工作内容 | 时间计划要求 |
| 1 | 制定实施及割接方案 | 签订合同后10个自然日 |
| 2 | 设备到货 | 签订合同后20个自然日 |
| 3 | 完成政务网升级改造割接及进入试运行（设备安装调试及试运行） | 签订合同后40个自然日 |
| 4 | 项目初步验收 | 签订合同后70个自然日 |
| 5 | 项目最终验收 | 初步验收完20个自然日 |
| 6 | 转入运维期 | 验收合格后系统提供不少于1年的免费维保服务，其中硬件设备不少于3年的免费维保服务。 |

**三、售后服务要求**

投标方设有备件库，可向采购人提供及时周到的快速备件更换服务，当设备出现影响业务的紧急故障时，应采购人要求立即派遣工程技术人员用最快捷的交通工具前往现场，进行备件的现场更换与安装。

具体备件要求：

|  |  |  |
| --- | --- | --- |
| 服务级别 | 受理时间 | 响应处置时间 |
| 7×24×1小时到达 | 30分钟内受理 | 1小时内到达，2小时内故障处理完毕 |

投标方为采购人每季度提供一次对设备及网络进行全面检查的巡检服务，为采购人获得设备运行的第一手资料，最大可能地发现存在的隐患，并有针对性地提出预警及解决建议，使采购人能够提早预防，最大限度降低运营风险，巡检可包括的内容如下（详细巡检计划及范围由服务经理与采购人提前协商制定）：

|  |  |
| --- | --- |
| 编号 | 巡检内容 |
| 1 | 硬件运行状态检查项目 |
| 单板状态检查 | 电源模块状态检查 | 风扇状态检查 |
| 整机指示灯状态检查 | 机框防尘网检查 | 机房温度、湿度检查 |
| 设备地线检查 |  |  |
| 2 | 软件运行情况检查项目 |
| 设备运行情况检查 | 网络报文分析 | 设备对接运行状况检查 |
| 路由运行情况检查 |  |  |
| 3 | 网络整体运行情况调查 |
| 网络运行问题调查 | 网络变更情况调查 | 网络历史故障调查 |
| 注：以上巡检内容根据设备具体情况会有所不同 |

**四、供应商要求**

供应商应具有本项目所需要的建设、维护和实施能力，符合在项目所在地开展本项目采购需求要求的建设服务内容所需的集成、安装、施工等相关管理要求，符合、承认并承诺履行本磋商文件各项规定，供应商应当具有类似项目建设管理经验。

1、在项目实施期间，供应商应严格执行国家、地方、行业有关本项目业务管理和安全作业的法律、法规和制度并按规定承担相应的费用。供应商因违反规定等原因造成的一切损失和责任由供应商自行承担。

2、供应商在项目实施期间，应按项目实际进度与环节落实所对应项目整体及各环节管理工作，按照规范做好项目实施期间相关管理与实施记录。

3、参与本项目的工作人员应严格遵循采购人的安全制度，保障采购人资料和设备的安全。供应商如需进入采购人机房工作，只能在采购人规定的工作区域内对项目涉及的设备进行操作，严禁触动与项目无关的任何设备（包括任何操作行为），如需跨区操作必须得到采购人项目联系人确认。

4、供应商在项目实施期间必须遵守采购人的规章制度并提供实施人员名单。