附件1：

服务内容

区域范围：大通区人民政府机房及机关大院，其他办公区：综治中心、社工部、财政教育院、残联院、西综合楼、党校、市场监管局、龙腾公司。

（一）安全巡检服务

上述区域范围网络接入点9个，共划分Vlan 19个，涵盖有线网络和无线网络，包含统一网络安全设备和统一网络管理平台。互联网、电子政务外网、2条专线接入，其中互联网和电子政务外网“双线接入、两网合一、逻辑隔离”，省信息报送专网为物理隔离。要求各投标人应自行勘察现场，了解实际网络及设备实际现状。

1、设备概况

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 设备名称 | 品牌 | 备注 |
| 1 | 安全网关 | 深信服 | 基础网络 |
| 2 | 行为管理 | 深信服 |
| 3 | 核心交换机 | 华为 |
| 4 | 接入24口交换机 | 华为 |
| 5 | 接入48口交换机 | 华为 |
| 6 | 无线控制器 | 华为 | 无线覆盖 |
| 7 | 接入24口POE交换机 | 华为 |
| 8 | 无线AP（面板） | 华为 |
| 9 | 无线AP（壁挂） | 华为 |
| 10 | 服务器 | Dell |  |
| 11 | 机房监控 | 海康威视 |  |
| 12 | 机房报警、门禁、供电 | 萤石、中控、易事特 |  |
| 13 | 网络运维管理系统 | \ | 自行开发 |

2、技术规范

|  |  |
| --- | --- |
| 名称 | 技术要求 |
| 技术标准 | 提供现场安全巡检服务，包含网络环境安全配置、硬件、中间件，对设备日志进行分析，安全设备策略备份与梳理等，提供详细的巡检报告。 包含但不仅限于以下：1.设备负载状态、性能使用、日志告警的检查与分析；2.对设备的应用控制策略、安全防护策略、安全合规性检查；3.对无线设备的巡检要覆盖每个汇聚点、对每个设备的运行状态、信号覆盖、地址分配、认证策略和安全接入的检查。4.对应用防火墙、行为管理设备安全策略、认证策略、上网策略的优化，对网络安全接入及内部业务系统安全访问维护；5.对安全设备的运行状态、安全事件、攻击事件及安全漏洞进行分析，发现严重问题需要1小时内提出处置建议或整改方案。 |
| 风险评估 | 对现有网络构架及安全设备的配置、技术、管理等方面进行风险评估，梳理不足之处，提出安全整改建议或规划。 |
| 风险加固 | 针对存在的风险进行安全加固处理，对设备的自身的安全配置进行加固，对设备的安全策略进行梳理、验证和优化等工作。重点发现应用层业务流程和逻辑上的安全漏洞和敏感信息泄露的风险，并提供加固建议。 |

3、资质要求

防火墙、核心交换机、无线控制器、行为管理为核心重要设备，为了保证服务的安全性，要求服务方提供现有机房核心设备相关服务能力资质证书、至少两种核心设备技术服务人员认证证书证明。

4、时限要求

服务期内，服务方提供不少于每2个月安全巡检1次。

（二）应急响应服务

1、服务内容

服务期内，为保障大通区政府的网络安全正常运行：1、根据工作实际需要，服务方通过现场和远程支持形式对系统设备遇到的突发事件、影响较大事件、大面积断网进行紧急分析和解决；2、特殊时期发生问题现场分析判断紧急解决；3、区机关网络设备发生故障，应在约定时间内解决。如设备故障无法解决，当使用单位现有设备无法满足网络安全防御能力时，服务方需能够提供如下网络安全应急设备：AF(下一代防火墙设备<更高性能>)、SSL-VPN(虚拟专用网络设备)、AC(上网行为管理设备)、WOC(广域网优化设备)、三层网络交换设备。目的是以最短时间，确认发生突发严重故障的原因并及时解决，由客观原因无法解决的，由双方协商解决。4、上述情况以外出现的问题，由客观原因无法解决的，由双方协商解决。

2、时限要求

服务期间服务方提供7\*24小时技术支持服务，包括应急响应时5分钟以内的电话响应，30分钟以内的远程支持和90分钟以内的现场服务。如果产生严重后果，视情况严重程度，按照合同金额的1%-5%进行赔偿或按照相关法律法规处罚。

（三）防火墙升级服务

为了保证大通区网络出口安全要求，对在用的深信服AF-1000-B1810防火墙设备进行服务升级1年（含云智订阅软件、网关杀毒、软件升级、产品质保）。