**采购项目服务需求及技术要求**

**一、服务需求**

本项目将根据国家网络安全相关法律要求，分析安庆市疾控中心信息系统、业务系统的实际安全需求，结合其业务的实际特性，建立符合系统实际安全需求的网络安全保障体系框架，设计安全保障体系方案，综合提升系统的安全保障能力和防护水平，确保系统的安全稳定运行。

本项目以等级标准化为基础，结合当前信息系统安全保障理论的最佳实践，采用新的信息安全保护技术，按照体系化的信息安全防护策略进行的整体规划，同时强化风险应对（监测、预警、处置、溯源等）能力，建设一套完整的“事前有防范、事中有应对、事后有追溯”的安全防御平台，并后续进行配套建设人才培养体系，合理的安全运营管理，实现新形势下安全管理上台阶、安全技术见实效、综合实力有提升的建设成效，形成具有主动防御和协同运营能力的新一代网络安全保障平台，实现信息系统长期安全稳定的运行。

**二、技术参数要求**

|  |  |  |
| --- | --- | --- |
| **序号** | **功能及技术指标** | **详细技术参数** |
| 1 | 产品架构 | 采用非X86 64位多核高性能处理器和高速存储器；主控模块内存≥1G；1U盒式设备（提供正面产品照片）要求所投型号官网可查，提供查询链接。 |
| 2 | 性能要求 | 所投产品全威胁处理性能支持不小于200M出口带宽场景，每秒新建连接数≥2万，并发连接数≥10万。IPSec VPN隧道数≥500；IPSEC VPN加密性能≥300M。 |
| 3 | 硬件要求 | 实配千兆以太网电接口≥8个，千兆光口≥2个，硬盘槽位≥1个。 |
| 4 | 配置要求 | 实配硬盘≥500GB，实配入侵防御、防病毒、应用识别、URL过滤功能授权，全部功能提供不少于3年免费特征库升级服务，实配15个SSL VPN接入授权 |
| 5 | 安全策略 | 支持一体化安全策略：可基于地址、服务、应用、用户、时间、VRF等属性，配置入侵防御、数据过滤、文件过滤、防病毒、URL过滤、日志记录、会话老化时间等高级访问控制功能。（提供功能截图） |
| 6 | 攻击防护 | 支持DDoS流量阈值学习。启用学习功能后，系统将自动分析当前流量并计算出各种攻击类型的防范阈值，管理员可参考学习结果设置阈值。学习功能支持学习时长、学习模式、周期学习及自动应用等功能。（提供功能截图） |
| 7 | 防病毒 | 基于病毒特征进行检测，实现病毒库手动和自动升级，报文流处理模式，实现病毒日志和报表。 支持基于文件协议、邮件协议（SMTP/POP3/imap)、共享协议（NFS/SMB）的病毒功能（提供功能截图）。可基于病毒特征进行检测、动作响应、提供报表。 |
| 8 | URL过滤 | 支持海量预分类的URL地址库，支持根据URL类别实现URL过滤； 支持管理者自定义新的URL地址和URL分类； 支持联动云端URL地址库进行全面实施核查（提供功能截图）。 |
| 9 | 共享上网管理 | 支持多用户共享上网行为管理；对通过NAT或代理进行共享上网的行为进行识别和管理，并可显示出IP、用户、VRF、状态和剩余时间等信息 |
| 10 | 用户行为画像 | 提供基于用户名（或用户IP地址）实现对用户行为统一分析界面，采用饼状图对访问应用流量、网站访问集中分析展示，包含基于时间轴的访问行为轨迹(应用账号、行为内容等)，关联账号（微信、QQ）等相关用户行为审计内容（要求提供配置截图） |
| 11 | 负载均衡 | 支持DNS透明代理功能，可基于负载均衡算法代理内网用户进行DNS请求转发，避免单运营商DNS解析出现单一链路流量过载，平衡多条运营商线路的带宽利用率。（提供功能截图） |
| 12 | 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。（提供功能截图） 支持网页诊断功能，用于当内网用户访问网页出现故障时，对网络进行基本的诊断，并给出故障原因。（提供功能截图） 支持报文示踪功能，支持真实流量、导入报文、构造报文等方式，用于分析和追踪设备中各个安全业务模块（如：攻击防范、uRPF、会话管理和连接数限制等）对报文的处理过程，通过查看报文示踪记录的详细信息，有利于管理员对网络故障的快速排查和定位。（提供功能截图） |
| 13 | 厂商资质 | 设备制造厂商符合信息技术服务管理体系符合ISO/IEC 20000-1：2011标准，符合信息安全管理体系符合ISO/IEC 27001：2013标准；要求提供证书复印件并加盖设备制造厂商公章 |
| 14 | 设备制造厂商符合能源管理体系ISO 50001:2018标准，能提供有效证书的复印件 |
| 15 | 设备制造厂商具备CNNVD（中国国家信息安全漏洞库）一级支撑单位资质，能提供有效证书的复印件。 |
| 16 | 设备制造厂商具备CNVD（中国国家信息安全漏洞共享平台）技术组成员资质，并成为CNVD漏洞信息报送突出贡献单位，能提供有效证书的复印件。 |
| 17 | 设备制造厂商应具备承担信息安全等级保护安全建设工作的能力，具有《信息安全等级保护安全建设服务机构能力评估合格证书》，能提供有效证书的复印件。 |
| 18 | 产品资质 | 所投产品须具备公安部颁发的第二代防火墙《计算机信息系统安全专用产品销售许可证》（增强级），能提供有效证书的复印件 |
| 19 | 所投产品须具备中国网络安全审查技术与认证中心的IT产品信息安全认证证书（评估保障级为EAL4增强级），能提供有效证书的复印件 |
| 20 | 所投产品须具备具备全球IPv6委员会颁发的IPv6证书，能提供有效证书的复印件 |
| 21 | 所投产品须具备CNNVD颁发的CNNVD兼容性资质证书，能提供有效证书的复印件 |
| 22 | 产品能力 | 所投产品最近连续三年入围Gartner企业防火墙魔力四象限，提供有效证明材料。 |
| 23 | 所投产品最近连续四年在IDC中国安全市场排名进入前三，能提供IDC数据授权引用书复印件 |
| 24 | 安全平台 | 安全专线平台可靠性方面要求提供7×24服务，采用高可用性方案，冗余配置，保证系统无单点故障点，发生故障后自动切换。 |
| 25 | 应用软件系统需连续7×24小时不间断工作，出现故障及时告警，具有完整的操作权限管理功能和完善的系统安全机制。 |
| 26 | 安全专线平台与安全网关设备进行无缝对接，通过系统对安全网关相关的数据进行采集，采集协议包括但不限于Syslog、AAA、Netstream、snmp等方式。（提供功能截图） |
| 27 | 支持网络设备的基本管理功能接口，不仅限于策略配置、任务下发、病毒库更新、访问控制、特征库更新。 |
| 28 | 平台支持对设备直接进行命令行远程操作，例如支持web、ssh、telnet。（提供功能截图） |

**三、服务要求**

1.远程运维：服务期内提供7\*24小时安全设备的远程运维服务；

2.免费升级：服务期内提供安全设备的定期提醒、远程协助升级软件、免费的特征库升级；

3.只换不修：服务期内非人为因素导致安全设备故障或损坏，提供参数对应的安全设备进行更换；

4.弹性扩容：如果互联网专线带宽提速或其他原因导致安全设备性能不适用，可以通过每月增加相应的服务费用升级替换为与现有带宽相匹配的安全设备；

5.专家应急响应：当客户端出现故障并对客户端造成一定影响时，有专家远程协助客户完成网络故障的诊断、处理，避免出现发生网络攻击时无保障状态，可出具以下文档：

-提供故障诊断报告，给出故障现象、故障诊断、处理建议；如，协助联通判断网络中断的原因（内网设备/外网线路）；

-提供故障处理报告，记录安全产品故障的故障现象、处理过程、处理结果。

6.事件云预警：推送安全设备的满负荷运行、异常流量和异常用户访问等安全事件，并提供解决建议；

7.安全云巡检：展示软硬件的在用功能、运行情况、生命周期及安全防护效果；

8.安全云评估：协助用户定期评估安全设备的健壮度和安全大数据，提供客户网络的安全分析报告。

三、商务要求

**1.合同履行期限：**合同签订后15日历日内完成软件、设备供货安装实施工作。

**2.其他说明和要求**

成交人按照合同交付用户的所有软件产品不得侵犯任何第三方的知识产权和其他合法权益。成交人对用户正常使用这些交付物的合法性负责。为合法使用这些交付物，用户如果需要支付与成交人所签合同总额以外的费用，成交人应该事先在其响应文件中说明，且相关费用应包含报价中。

**3.项目验收**

将按照预先并得到确认的验收方案进行验收。

**验收方式：**由采购人、成交单位共同组织验收。

**验收要求：**以本响应文件中规定术参数、功能清单为基本要求。