附件一

绍兴市医保专网安全接入网关服务参数要求

一、项目概况

为落实浙江省医疗保障局《浙江省“智慧医保”网络市级安全接入区建设指南》、《浙江省“智慧医保”网络定点医药机构链路接入指南》、《浙江省“智慧医保”网络终端接入指南》等文件要求，根据绍兴市医疗保障局智慧医保网络安全项目建设规范，需在二级及以上定点医药机构构建安全防护体系，利用边界防护手段，严格规范网络系统的数据传输及应用。本次服务为我院提供网络安全、链路安全、故障排查、运维监管、威胁防护等综合服务，并为专网的运维和定点医药机构的安全接入及监管提供有力的技术支撑。

二、项目主要内容

安全运维服务要求

|  |  |  |
| --- | --- | --- |
| 服务名称 | 功能或服务描述 | 数量 |
| 边界安全服务 | 服务内容：提供医保专网边界安全服务，包括但不限于：安全网关统一接入、统一管理，设备软硬件维护，软件版本升级、各类特征库升级服务，日志转换、发送及分析服务，每日网关健康度检查等。频次：1次/天 | 1年 |
| 安全巡检服务 | 服务内容：提供现场巡检服务；每月不少于1人天现场巡检。频次：1次/月 | 1年 |
| 安全运营及加固 | 服务内容：安全运营：每月对绍兴市妇幼保健院医保专网安全事情分析，形成安全分析报告。安全加固：根据安全检查、安全监测等报告，制定针对绍兴市妇幼保健院特色的安全加固方案及处置意见，提升安全保障能力。频次：1次/月 | 1年 |

三、技术参数

|  |  |  |
| --- | --- | --- |
| 服务类别 | 服务名称 | 招标参数要求 |
| 服务工具要求 | 服务要求 | 安全服务响应时间要求：1、普通安全问题，半小时内远程响应2、重要安全问题（影响业务），1小时内上门处置 |
| 边界安全服务 | 边界安全工具要求：网络层吞吐量≥20G，应用层吞吐量≥15G，防病毒吞吐量≥2G，IPS吞吐量≥2G，全威胁吞吐量≥1.5G，并发连接数≥350万，HTTP新建连接数≥16万，IPSec VPN 最大接入数≥1000，IPSec VPN吞吐量≥1G。提供软件升级服务1年，产品质保1年。1U设备，兆芯KX U6580A（2.5GHz，8核），银河麒麟V10.0，紫光 8G，创见 128G SSD，欧陆通 350W冗余电源，接口：6千兆电口+4万兆光口。 支持路由、透明、虚拟网线、旁路镜像、混合等多种部署方式，适应复杂使用环境的接入要求。具备链路聚合功能，将2个或者更多物理链路组合成一个更高带宽的逻辑链路接口，提高链路带宽和链路可靠性。具备ARP代理功能，对指定地址的ARP请求使用指定接口的MAC地址应答，实现保护内网主机。支持IPv4／IPv6下NAT地址转换，包括支持源地址转换SNAT，目的地址转换DNAT和双向地址转换双向NAT， 支持一对一、一对多、多对一等多种转换方式。支持基于对象、区域和地域维度设置安全访问控制策略，允许或拒绝特定国家或者地区的对象访问内部网络，保障业务重大时期安全可靠性。产品内置应用特征识别库，支持不少于9000种应用规则，支持对游戏、P2P下载工具、聊天工具、网上银行、视频软件、股票软件、木马控制软件等类型应用进行检测与控制。（需提供产品功能截图证明）产品支持多维度流量控制功能，支持基于国家、地域的流量控制策略，保证关键业务带宽日常需求。（需提供产品功能截图证明和具备CMA/CNAS标识的第三方检测报告）支持IPSec VPN，SSL VPN，GRE等VPN接入方式；IPSec VPN支持国密算法；IPsec VPN支持双机环境下vpn组网；支持在防火墙上配置VPN安全策略对加密隧道内的流量进行清洗；支持产品支持对ICMP、UDP、DNS、SYN等协议进行DDOS防护，支持IP地址扫描和端口扫描攻击防护。支持异常包攻击防御，异常包攻击类型至少包括Ping of Death、Teardrop、Smurf、Land、WinNuke等攻击类型。产品内置不低于13000种漏洞规则，同时支持在控制台界面通过漏洞ID、漏洞名称、危险等级、漏洞CVE标识、漏洞描述等条件查询漏洞特征信息，支持用户自定义IPS规则。（需提供产品功能截图证明和具备CMA/CNAS标识的第三方检测报告）具备僵尸网络检测功能，可基于僵尸网络检测引擎发现主机的异常外联行为，并提供威胁等级和非法外联次数作为举证。支持应用控制策略生命周期管理，包含安全策略的变更时间、变更类型和策略变更用户，并对变更内容记录日志，方便策略的管理和运维。支持Web服务器自动侦测功能，根据Web服务器在线状态、端口使用状态、Web服务器之间的互访关系生成业务资产列表，同时展示内网资产访问的风险等级。（需提供产品功能截图证明）支持三权分立功能，根据用户权限分为安全管理员、审计员、系统管理员三种角色；支持管理员双因素认证，包含用户名/密码和Key等不同方式。产品支持用户账号安全保护功能，包括用户账号多余入口检测、用户账号弱口令检测、用户账号暴力破解检测、失陷账号检测，防止因账号被暴力破解导致的非法提权情况发生，提供产品相关功能截图和第三方权威机构关于账号保护的产品检测报告或相关证书证明。 |
| 服务接入要求 | 总体要求安全接入设备需符合信创环境使用要求，支持主备链路同时接入，并按照规范统一接入集中安全管控平台，实现统一策略下发，版本升级，特征库升级，实时监控，网络告警，硬件告警，安全告警，离线告警等，实现数据对接，安全事件闭环处置。具体要求如下：功能要求1、集中管控：设备通电之后通过简单配置即可完成设备接入，后续配置均可通过集中管理平台远程下发配置及策略更新，支持设置黑白名单管理功能，对设备与定点机构接入设备的 IP、MAC 地址进行限制和绑定。2、接入方式：支持有线VPN 方式或无线VPDN 方式拨入医保网络，建立的隧道必须采用国密数字证书进行认证。并可实时探测有线无线链路质量，当前链路不满足时立即切换至其他可用链路，保证业务不中断。3、安全运维：为保障运维的便捷性，在紧急情况或特殊情况下，接入安全网关的主要配置信息具备从 U 盘获取的能力，运维人员可以使用U 盘完成配置向导快速开局能力，接入医保专网。4、安全防护：访问控制策略支持基于源/目的IP，源/目的端口，源/目的区域，用户（组），服务类型的细化控制方式，设备支持对于病毒、木马的攻击防护，配置相关的授权应用特征库、IPS库、防病毒库及日志加密、转换及分析功能，为医保专网提供整体安全保障，减少来自网络的安全威胁。5、加密：为保证医保专网数据传输安全，需支持IPSec VPN、、L2TP VPN、GRE VPN、SSL VPN，并支持国密算法SM2、SM3、SM4。6、设备监测：可被集中管控平台管控，检测项涵盖设备运行状态、VPN链路状态、设备接口流量状态及设备告警事件的外发等。平台对接要求1.与集中安全管控制平台对接，并在5 分钟内周期性上报接入安全网关的性能和状态指标数据，至少包含：设备编码、设备系统版本、设备厂商及设备型号、CPU 利用率、内存利用率、总流量、网卡负载（lan口，wan口，虚拟网口，4G网口等）、当前安全链路类型（物理链路，VPN 链路，VPDN 链路等）、设备业务 IP，设备当前接入的终端信息（IP，Mac，设备名称等）等信息。2.与集中安全管控制平台对接，并在30 秒内上报接入安全网关的日志及告警事件信息，上报数据至少包含：设备编码、切换日志、设备日志、安全事件类型、事件发生时间等。3.与集中安全管控制平台对接，实现对接入智能安全网关的固件、软件版本、特征库的统一升级及安全策略下发，安全事件处置。 |
|  | 安全专线 | 抗D技术要求：重保期间提供抗DDOS服务，需具备互联网管道侧清洗防护能力，提供1G大流量攻击清洗防护。采用近源式清洗、分布式清洗，具有全国调动防护能力。具有城域网近目的清洗、城域网、骨干网二级协同联动能力，在全球部署有清洗中心，全球清洗中心数量≥50个（提供具有 CNAS 认可的三方测试证明材料复印件并加盖投标人公章）。 |

备注：相关截图和证明材料请以附件方式提供。

附件二

|  |
| --- |
| 报价单 |
|
| 询价单位 | 绍兴市妇幼保健院　 | 联系人 | 王老师 |
| 联系电话 | （0575）88217200 | 日期 |  |
| 序号 | 货物/服务/项目 名称 | 规格 | 数量 | 单价 | 总价 | 备注 |
| 1 | 　 | 　 | 　 | 　 | 　 | 　 |
| 2 | 　 | 　 | 　 | 　 | 　 | 　 |
| 3 | 　 | 　 | 　 | 　 | 　 | 　 |
| 金额合计 ：  |
| 人民币：（大写） |
| 交货期 | 　 | 是否含税 | 　 |
| 保修期 | 　 | 付款方式 | 　 |
| 备注（其他优惠情况说明） | 　　 |
| 供应商信息 |
| 供应商名称： |
| 公司性质 | □生产厂家 □授权代理商 | 代理证有效期 | 至 年 月 日 |
| 联系人 |  | 联系电话 |  |
| 单位地址 |  | 传真 |  |
| 纳税人识别号 |  | 税号 |  |
| 开户行 |  | 账号 |  |
| 法人代表 |  | 邮政编码 |  |
| 供应商名称（公章） |