秦皇岛市医疗保障局医疗保障信息化建设与能力提升项目采购需求

一、 项目名称：秦皇岛市医疗保障局医疗保障信息化建设与能力提升项目。

二、 投标最高限价：578.92 万元。

三、 项目主要内容：为了全面贯彻国家和河北省关于医疗保障工作和信息化建设战略决策部署，按照国家医疗保障局全国一体化的视频会议的要求及河北省医疗保障局关于加快推进我省医疗保障中心建设工作的通知，结合我市医疗保障工作及信息化的需求，决定在全市范围内建设统一的医疗保障视频系统。我市医疗保障视频系统须与省医保局视频系统做到无缝数字对接,把省市县三级视频会议系统建设为一个可管可调可控的整体系统，做到省市县完全数字互联互通，实现省局对市县局的高清视频会议、视频培训、应急指挥调度等功能。

四、 设备清单和功能参数要求

A 包：医疗保障系统视频会议（指挥中心）设备采购(105 万元）

序号	产品名称	单位	数量	单价	总价(元)	功能描述
1	液晶电视 1	台	2	7000	14000	屏幕尺寸≥75 英寸， 分辨率≥3840×2160， 刷新率≥60Hz，可视视角水平视角≥178°， 垂直视角≥176°， 需根据现场使用情况定制支架。
2	高清视频矩阵	台	1	18000	18000	HDMI2.0 版本（支持 4K@60Hz YUV4:4:4） 支持 3D，LED 显示屏 带宽达 18Gbps 兼容 HDCP2.2/1.4 支持 HDR10 八路 HDMI 输入，八路 HDMI 输出和八路 SPDIF

						音频提取 任意八路信号可以切换到八路高清显示 支持面板按钮,本地红外,RS232 控制,IP 控制,Web GUI 控制 支持杜比 TureHD 和 DTS-HD 主音频 1U 机架设计，简易安装
3	无线图像传输器	套	1	5000	5000	输出分辨率支持单画面 4K@60fps 以上视频输出 视频编码/解码 H.264,H.265 硬解码 无线传输通信协议 IEEE 802.11 a/g/n/ac 投屏方式：硬件投屏、软件投屏 内存容量 4GB 存储容量 16GB HDMI OUT：2 个 LINE OUT：1 个 兼容的发射端类型:支持 SM01 无线投屏(Windows, macOS)；支持手机/平板投屏(Android/iOS)
4	数字调音台	台	1	30000	30000	不少于 20 路输入 不少于 14 路输出 不小于 5 英寸液晶高清触摸显示屏 100mm 电动推杆 6 组 DCA 功能，可将任意输入编辑为一组操作 可进行远程控制 可接入多轨道录音模块、DANTE 传输模块等
5	会议话筒	套	1	6500	6500	载波频率:UHF550-980MHz 调制方式:FM 发射功率:高功率档：10dBm，低功率档：5dBm 最大调制度:±45KHz S/N 信噪比:≥105dB 频率响应:40Hz-18KHz 发射机数量:≥4 只
6	反馈抑制器	台	1	5000	5000	采样率：优于 48kHz 动态范围：>109dB，A 计权 频率响应：20Hz-20KHz,±0.5dB 总谐波失真+ 噪声：典型值 0.003% 滤波器数量：大于 24 个/通道

7	音箱	支	2	5000	10000	频率范围(-10dB)：70Hz-21kHz 频率响应(±3dB)：75Hz-20kHz 覆盖角度(水平×垂直)：110° × 110° 分频模式：被动模式 承受功率(连续/节目/峰值)：180W/360W/720W 系统灵敏度：94dB(1w@1m) 最大声压级：120dB 峰值/115dB 连续 额定阻抗：8Ω
8	多通道数字功放	台	1	5000	5000	立体声功率：8Ω/300W×2 ;4Ω/450W×2 桥接功率：8Ω/900W 并接功率：2Ω/900W 总谐波失真：1KHz＜0.05% 互调失真：60Hz/7kHz-4/1 <0.08% 频率响应：30Hz-18kHz <+/-1dB 功率带宽：±1dB /30Hz-18kHz 相位响应：30Hz-18kHz<+/-8 度 信噪比：1KHz，0.775V 输入， A 计权 ≥95dB 阻尼系数： 1kHz >500 转换速率：1us/1ms 窄脉冲,32dB 增益>25V/us 输入阻抗： 1KHz,平衡输入 20k ohm 最低负载阻抗： 立体声>3ohm； 桥接>6ohm 分离度：1KHz，0.775V 输入 >75dB 共模抑制：正常工作条件，1KHz >80dB
9	MCU 多点控制单元	台	1	250000	220000	高性能硬件，采用嵌入式、非 Windows 的操作系统；整机支持 7×24 小时不间断运行。 提供 10 点 1080P30fps 接入能力，最大接入容量不少于 25 个 1080P60fps 全编全解会场接入能力，仅需扩展许可即可增加呼叫并发数量，无需更换硬件，呼叫带宽不低于 6M。 具备至少 2 个 1000Mbps RJ-45 接口，且能够同时支持 IPV4 和 IPV6。 支持 ITU-T H.261、H.263、H263+、H.264 HP、H.264 SVC 视频协议，支持不同终端以 H.264 highprofile 或 H.264SVC 协议同时接入同一个会议。支持 ITU-T G.711a、G.711u、G.722、G.728、G.722.1C、G.729a、G719 音频协议，支持 20Khz 以上频响的双声道宽频语音协议；支持 1080P60 帧、1080P30 帧、720P60 帧、720P30 帧，并向下兼容 4CIF、CIF 图像格式。要求采用全新的硬件平台，支持全编全解技术，每个参会会场均能够独立观看不同的 1080P 60fps 多画面图。 能够支持对称的 1080P 多画面功能，保证在多

						画面场景下实现终端和 MCU 之间收、发均是 1080P 图像。 支持 H.239 双流标准，动态桌面辅流画面可达到 1080P 60fps 效果。 支持 IP 网络丢包时修复机制，确保丢包达到 10%时图像无马赛克现象，丢包达到 20%时，会议依然能够正常召开，要求投标方明确说明实现机制，以及对于网络丢包适应能力的量化指标。 确保网络丢包达到 70%的时候，音频不受影响，会议可以以音频形式正常召开，要求投标方明确说明实现机制，以及对于网络丢包适应能力的量化指标。 支持每个参会终端均以不同的协议、不同的带宽、不同的音视频编码、不同的清晰度同时加入到一个会议中，且同时能够支持多组会议，会议组数不受混网、混速数量的限制。 支持终端多画面自定义，可以设置每个会场独特的多画面组合方式。 多点控制单元支持资源池热备功能，详细描述实现机制及原理。 实现中文滚动字幕，标示会议提示信息，在分屏显示多画面时可在整幅画面进行文字的滚动功能，同时可更改文字的大小及位置。 实现自定义轮询功能，在会议中可以指定哪些会场参加轮询和指定哪些会场不参加轮询，同时可指定轮询顺序。
10	备份 MCU 系统	套	1	130000	160000	符合 ITU 的 H.323 以及 IETF 的 SIP 标准。 采用虚拟化部署方式，支持 VMWare、 Hyper-V 等虚拟化环境安装部署，支持异地灾备。 支持 H.460 防火墙穿越协议。 支持 TLS 安全认证。 支持 XMPP 协议。 支持不少于 1000 个设备 H.323 或 SIP 注册 。 支持动态资源分配；可与 MCU 多点控制单元组成资源池市县热备，如 MCU 多点控制单元出现问题时，备份 MCU 系统可接管会议，不影响会议的继续召开。 支持注册终端通过 E.164 或 SIP 短号实现公私网互通；或非注册终端通过 IP 地址直接呼叫实现公私网互通。 具备黑白名单功能，可根据 IP 地址对注册终端权限进行控制。 支持 ITU-T H.323、IETF SIP 协议。 多点会议支持对称 1080P60fps 会议的召开，

						多个终端参会，查看终端接收和发送的视频都为1080P分辨率。 视频编解码支持H.261、H.263、H.263+、H.264、H.264 High Profile、SVC协议。 支持ITU-T G.711、G.729A、G.722、G.722.1、G.722.1 Annex C、G.719等音频编解码标准。 具备虚拟的会议特服号码，可以调用MCU资源，视频终端只需拨打相应的特服号码即可加入相应的会议。 可以集中对软件终端和硬件终端将行呼叫的管理，和呼叫的带宽控制。 可以使用Web浏览器便可以随时随地加入远程会议或接访，系统与硬件视频会议系统声音、视频、内容无缝互联互通。 支持基于IE，Chrome，Firefox，Safari等主流浏览器的音视频接入应用。 支持基于Windows、Mac等主流操作系统的视频应用，无需安装软件。 支持即时会议，会议预约，会议控制，会议内容的共享等功能。 提供API接口。 提供1台用于部署本系统的服务器，配置不低于2颗Intel XEON 4114处理器，64G内存，2600G 10K SAS 2.5寸硬盘，2G缓存RAID卡，支持raid5，四个千兆网口，导轨，2550W，含部署系统所需的操作系统、虚拟化软件等。
11	视频会议管控平台	套	1	88000	88000	*支持在两台服务器上安装，并支持双机热备份功能，自动同步配置，故障自动切换。 *支持对多台MCU进行智能热备配置，可以在主MCU故障时，备份MCU自动接管会议，保证会议系统的高稳定性。（用户保留现场测试权力） 支持MCU自动级联组会，用户只需选择参会会场，MCU自动级联组会，可扩展支持控制5级MCU自动级联组会。 *支持双终端热备份，双终端独立部署，同时入会。当主终端故障时，支持自动快速切换到备份终端，保证会场会议的稳定。当无故障时，备份终端可以增加会场的分屏画面。 支持WEB远程登陆管理，支持对全网视频会议设备进行统一管理，支持显示所有视频会议终端的在线状态（离线，在线，通话等），同时可以监控系统使用和空闲容量等。 支持分级分权管理，分级管理权限角色种类至少包括6种角色，并且可以由用户根据实际需

						要进行用户帐号权限设置。 支持预约创建视频会议，用户创建视频会议的申请内容至少包含会议名称、会议密码、统一呼叫号、会议类型、召开时间、会议时长、最大带宽、是否会议录制、会议字幕、主办部门、联系方式等。 支持会议的审批功能，并且要求有全局控制是否开启审批会议功能；审批人审批完成后要求能够查看自己的审批历史内容；系统支持高权限角色用户自动召集会议，无需审批流程。 支持会议通知功能，当预约会议成功后，系统自动发送邮件通知各会场终端管理者。 支持会议统计功能，包括会议次数，会议时长，会议使用的终端设备的完整数据统计，会议结束后会自动生成相关会议的统计结果，并自动生成报告。 支持主会场会议模式和讨论会议模式；支持指定或断开指定会场发送双流。 *支持会议点名功能，批量选择点名会场，一键快速切换会场点名；会议点名时，主会场观看被点名会场画面，被点名会场看主会场画面，同时被点名会场麦克风打开，其他没轮到点名的会场麦克风被静音。 *支持“一键”广播分会场，MCU 级联会议中需要下级MCU分会场发言时可以实现一键广播分会场。 支持主会场画面多分屏全网定制轮询功能，支持设置主会场多分屏画面，每个分屏画面都可以定制轮询不同的分会场画面，不管分会场连接在哪一级 MCU，均可以按照指定的顺序进行轮询，轮询随时可以调整，不会中断会议。 *支持会场预监功能，支持实时预览监控和主会场不同的分会场画面，同时监控终端不参与会议中正常的广播和点名等操作，不影响会议。预监会场可个性化定义多分屏画面，且可以实现定制轮询。 *支持通过 Pad 创建发起会议，并对会议进行操控，支持通过 Pad 对会场情况进行预监。
12	视频准入防火墙	台	1	28000	28000	*标准机架式设备，单电源，千兆电口≥4 个，内存≥2GB，硬盘≥64G SSD，RJ45 串口≥1 个，USB 口≥2 个，吞吐量≥6Gbps，并发连接数≥80 万，新建连接数≥1.5 万，4M 码流视频准入路数≥256，提供 3 年硬件质保，3 年软件授权。 支持串接、旁路两种部署方式。 具备主动探测与被动流量识别技术。

						*支持视频终端主动扫描，并且扫描间隔时间可设置。 支持通过 IP、MAC、白名单、802.1X 协议等对接入设备进行认证。 支持视频终端监测，能实时获取视频终端状况和连接链路状况。 支持视频终端在资产管理界面上搜索、分组、自定义标签等。 支持通过识别、分析网络中的视频流量和非视频流量发现异常设备，并进行实时告警和阻断，避免非摄像机资源及非法前端资源连入视频传输专网。 访问控制 支持识别 IPC 是否采用 GB28181 标准接入，对不符合国标的终端可进行告警和阻断。 *支持对<<GB 35114-2017 公共安全视频监控联网信息安全技术要求>>视频协议的信令进行控制，如标准中明确规定的 SIP 视频协议中注册 REGISTER，邀请 INVITE 等信令的访问控制。 支持基于应用类型，网站类型，文件类型进行流量控制，支持基于 IP 段、时间、国家/地区、认证用户、子接口和 VLAN 进行流量控制。 访问控制规则支持模拟策略匹配，输入源目的 IP、端口、协议五元组信息，模拟策略匹配方式，给出最可能的匹配结果，方便排查故障，或环境部署前的调试。 支持接入摄像头如海康、大华等设备安全性检查，弱口令和摄像头高危漏洞等安全风险并提供防御能力。 *具备独立的入侵防护漏洞规则特征库，特征总数在 7300 条以上。 支持自动生成综合安全风险报表，报表内容体现被保护对象的整体安全等级，发现漏洞情况以及遭受到攻击的统计，具备有效攻击行为次数统计和攻击举证。 支持以安全策略模板方式快速部署安全策略，安全策略模板支持默认模板和自定义模板等多种格式。 支持场景化的配置向导功能，可以选择不同的部署方式以及使用场景实现产品的快速实施。 支持邮件、短信等多种告警方式。
13	中控主机	套	1	24000	24000	前置液晶屏可显示设备状态、IP 地址，可以有效快速连接主机。 前置红外学习窗口，可直接进行红外码学习；

						主板卡处理速度：64 位四核,CPU≥1.2GHz；内存≥1G，闪存≥8G。 采用 Linux 系统架构，更稳定，更安全。 支持 HTTPS 通讯方式，无需外加 PC 中转。 内嵌讯飞离线语音合成技术，可实时播报文字转语音通过扩声系统进行互动播报。 具备 3.5mm 立体声音频输出接口，可做 MP3 等格式的无损音频文件播放使用。 前置 LED 状态指示灯直观反映连接状态，包含 LED 灯显示串口发送/接收信号、红外发送信号、继电器开关信号、IO 开关信号。 不低于 8 路 RS-232，不低于 8 路 RELAY、不低于 8 路 IR、不低于 8 路 I/O。 1 路 EC-BUS 总线接口,提供对外 12V/3A 供电,并支持总线数据通讯；提供 2 路 USB 接口，用于扩展和固件升级。 支持按键反馈、拉条功能，信号切换支持人性化拖拽式控制功能。
14	时序电源	台	1	1500	1500	十六路受控电源 电源输入总容量：AC220V 20A,只有一个插座连接负载时可承受负载能力 2KW（VA） 定时器控制信号：短路信号,低电平激活 动作时间间隔：0.4S~0.5S 可控制电源输出：十六路（CH11~CH16） 功能控制：定时器控制信号输入口一个,电源开关一个
15	录播主机	台	1	42000	42000	最大支持≥2 路高清输入接口，≥3 路标准 RJ-45 接口： 内置存储容量≥1T 支持网络直播、点播 支持 1080P、720P、480P 等多种录制格式
16	控制室显示屏	台	1	2000	2000	≥24 寸显示屏 显示分辨率：≥1280×720 屏幕比例：16:9 光源类型：LED HDMI 接口（含定制支架）
17	控制电脑	台	1	5000	5000	Intel 酷睿 I5-8500CPU （3.0GHz、六核），8GB DDR4 内存，1TB 硬盘，2G 独立显卡，USB 键鼠，21 寸宽屏液晶显示器。
18	交换机	台	1	2000	2000	千兆以太网交换机，24 个 10/100/1000Base-T 以太网端口，4 个 1000Base-X SFP 千兆以太网端口，背板带宽：330Gbps/3.6Tbps，包转发率包转发率：96Mpps/126Mpps，支持全双工，支持基于端口的 VLAN,支持用户分级管理和口令保护，支持 802.1X，支持端口安全。

19	机柜	台	1	4000	4000	标准 42U 网络机柜，黑色网孔门，含 2 个 8 位 PDU
20	无线 AP	套	1	1000	1000	支持 802.11a/b/g/n/ac 协议，支持 802.11ac/a/n 和 802.11b/g/n 双频并发，2.4G 传输速率 300Mbps，5G 传输速率 867Mbps，整机传输速率 1167Mbps；内置矩阵式智能天线；1 个 10/100/1000Mbps 的以太网口；接入用户数最大为 256 个。
21	操作台	个	1	3000	3000	根据现场情况定制。
22	高清视频会议终端	台	9	30000	270000	采用分体式结构设计；终端采用为嵌入式操作系统，非 PC 结构不受电脑病毒感染。 具备不少于 3 路高清视频输入接口，不少于 3 路高清视频输出接口。 至少具备 2 组音频输入接口，可接入数字麦克风或线性电平，支持立体声；至少具备 2 路音频输出，可接调音台或数字媒体矩阵等音频设备，支持立体声。 遵循 ITU-T H.323，SIP 协议，支持 H.261、H.263、H.264 HP、H.264 SVC 视频协议。 支持 ITU-T G.711、G.722、G.728、G.719 等 20Khz 以上频响的双声道宽频语音协议。 终端满足 CIF、4CIF（704×576）、720P（1280×720）、1080P（1920×1080）等图像格式；帧率可达 1080P 60fps。 2M 速率下可以实现 HD 1920×1080P 60fps 高清效果。 配置与终端同一品牌的 360 度全向数字麦克风，拾音范围不小于 6 米。 配置与终端同一品牌高清摄像机，配置要求如下：≥200 万像素，≥1/2.33 CMOS，12 倍光学变焦，支持 1080P 60 帧，720P 30 帧，720P 60 帧，支持高清输出。 预置位个数不少于 10 个，提供本地和远端摄像头预置位的存储与调用，可在显示屏上显示已存储的预置位图像，方便快速调用。 终端具有 H.239 双流收发，辅流内容分辨率支持 1080P@60fps。 采用音视频线缆连接方式发送双流时，同时本端也能同步输出双流音视频。 系统具备音频输入/输出诊断功能，便于设备安装和调试；支持宽带音频协议下立体声方式传输音频；具备自动增益控制、自动回声抑制（AEC）、自动噪音抑制（ANS）功能。 实现 IP 网络丢包时修复机制，确保丢包达到

						20%时图像无马赛克现象，丢包达到70%时，会议声音不受影响，依然能够正常召开。 支持通过鼠标、触摸屏方式对双流内容进行标注。
23	液晶电视2	台	9	3000	27000	屏幕尺寸:≥55英寸 分辨率:≥3840×2160 屏幕比例:宽屏，比例 16:9 刷新率:≥60Hz 可视视角:水平视角≥178°，垂直视角≥178°
24	电视推车	套	9	1000	9000	冷轧钢材质，称重不低于60公斤，高度不低于1.7米，可安装32-70寸电视，顶部带摄像机托盘，下部带终端托盘
25	辅材	批	1	30000	30000	设备安装所需的各种线材和接插件，符合广电颁布的标准，屏蔽线缆屏蔽效果达到95%以上，信号在传输中能过滤杂波，抗干扰。接插件和设备接口配套，不能松动。
26	施工费	项	1	40000	40000	含市局及9个下级局点设备安装调试、运输、培训等相关费用。
27	合计					

B包：医疗保障系统核心业务区横向网络设备采购（185.92万元）

序号	产品名称	功能描述		数量	单位	单价	总价（元）
一	路由接入区						
1	医保专网路由器（专线）	转发性能	≥330Mpps	2	台	50000	100000
		整机交换容量	≥650Gbps				
		内存	≥8G				
		固定GE接口	≥10GE（Combo）				
		二层协议	支持Ethernet，Ethernet II，VLAN(VLAN-BASED PORT VLAN，VOICE VLAN，Guest VLAN)，802.3x，802.1p，802.1Q，802.1x，STP(802.1D)，RSTP(802.1w)，MSTP(802.1s)，PPP、PPPoE Client、PPPoE Server、HDLC、DDR、Modem、ISDN等				
		IPv4路由	静态路由				
			动态路由协议：RIPv1/v2、OSPFv2、BGP、IS-IS				

序号	产品名称	功能描述		数量	单位	单价	总价（元）
			路由迭代				
			路由策略				
			ECMP（等价多路径）				
			组播路由协议：IGMPV1/V2/V3，PIM-DM，PIM-SM，MBGP，MSDP				
		IPv6	支持 Ipv6 ND，Ipv6 PMTU，Ipv6 FIB，Ipv6 ACL，NAT-PT，Ipv6 隧道，6PE、DS-LITE；				
			IPv6 隧道技术：手工隧道，自动隧道，GRE 隧道，6to4，				
			静态路由				
			动态路由协议：RIPng，OSPFv3，IS-ISv6，BGP4+				
			IPv6 组播协议：MLD V1/V2，PIM-DM，PIM-SM				
		可靠性	支持 NSR、GR				
			支持 VRRP、VRRPv3				
			支持基于多链路的负载分担与备份				
			支持 NQA 同路由、VRRP 和接口备份的联动功能，实现端到端链路的检测与备份功能				
			支持 BFD 快速链路检测的主控主备倒换				
2	VPN 综合网关	*性能参数	标准机架设备≥1U，内存≥8G，硬盘容量≥64GB SSD，冗余电源，千兆电口≥6 个，千兆光口 SFP≥4 个；整机吞吐量≥1.2Gbps，并发用户数≥10000，提供接入授权 1500 个，提供 3 年硬件质保，3 年软件升级。	2	台	150000	300000
		部署模式	支持 IPv6/IPv4 协议下的网关模式、单臂模式、主备模式、集群模式、分布式集群模式的部署。				
		*商用密码支持	产品应支持国家商用密码算法包括：SM1、SM2、SM3、SM4 算法。				
		登录策略	可支持个性化登录策略，在一台设备上配置不同的访问域名、IP 地址，以及不同的使用界面，实现一台设备为多个不同用户群体服务的的使用效果；				
			支持单点登录功能（SSO），支持移动用户登录 VPN 后再登录内部 B/S、C/S 应用系统时不需要二次重复认证。支持针对 B/S 单点登录用户名密码加密传输，保证安全；支持针对不同的访问资源设定不同的 SSO 用户名和密码，支持用户自行修改 SSO 账号。				
		*环境检测	*产品应提供环境检测、自动修复工具，支持对 Windows 的环境兼容性一键检测能力，以及对检测结果进行一键修复的能力，避免由于用户操作系统环境存在问题影响 SSL VPN 的使用，减轻运维工作。				
		终端安全	产品必须支持防中间人攻击，产品可在用户登				

序号	产品名称	功能描述		数量	单位	单价	总价（元）
			录 SSL VPN 时智能判断存在中间人攻击行为，断开被攻击的连接，并可提示异常现象；				
			支持客户端注销后自动清除所有缓存、Cookies、浏览器历史记录、保存的表单信息，实现零痕迹访问；				
			*产品应提供 HTTPS 驱动病毒查杀工具，支持对 Windows 环境下的针对 HTTPS 拦截监听的驱动病毒进行扫描查杀，避免因为 HTTPS 驱动病毒导致无法正常接入和使用 SSL VPN。				
		权限、服务器安全	产品应具有用户/用户组细粒度的权限分配功能：可以针对被访问资源的 IP 地址、端口、提供的服务、URL 地址等进行权限控制；针对同一 B/S 资源，可对不同用户做到细致到 URL 级别的授权；				
			支持主从认证账号绑定，必须实现 SSL VPN 账号与应用系统账号的唯一绑定，VPN 资源中的系统只能以指定账号登陆，加强身份认证，防止登录 SSL VPN 后冒名登录应用系统。				
		线路配置	必须支持至少 4 条以上的外网多线路配置；并在设备单臂部署模式下，多线路接入前置网关，仅依靠 SSLVPN 设备同样可实现 SSLVPN 接入用户的多线路自动优选功能。				
		传输协议	支持非对称式部署的传输协议优化技术（单边加速），不用在用户终端上安装任何插件和软件，即可提升用户访问应用服务的速度；				
			*支持 HTP 快速传输协议，大幅优化无线环境（CDMA、GPRS、WIFI、3G）、高丢包、高延等恶劣网络环境下传输速度及效率；支持根据网络境自动选择并切换至最优的传输协议。				
		身份认证	支持基于硬件指纹特征的认证方式（非 MAC 地址绑定），可实现用户与终端的绑定，支持终端接入审批，仅允许审批通过的终端接入 VPN；支持用户自助审批；支持设置用户可允许接入的终端数量。				
		日志记录	支持独立日志中心进行 SSLVPN 实时日志记录，可详细记录用户访问资源记录（用户、主机 IP、资源、时间）、管理员日志（管理员、主机 IP、时间、管理行为、对象）、系统日志、告警日志；可根据用户名、主机 IP 等信息进行用户行为查询；可提供用户组/用户流量排行及查询、资源流量排行及查询、资源活跃程度、用户活跃程度等记录；提供暴破登录记录；可提供用户登陆 SSLVPN 采用非绑定账号访问应用系统				

序号	产品名称	功能描述		数量	单位	单价	总价（元）
			的记录。				
二	边界防护子区						
1	交换机	业务端口	≥24 个 10/100/1000Base-T 自适应以太网端口，4 个万兆 SFP+口	2	台	8000	16000
		交换容量	≥580Gbps				
		包转发率	≥200Mpps				
		端口聚合	支持 GE 端口聚合				
			支持 10GE 端口聚合				
			支持 40G 聚合				
			支持静态聚合				
			支持动态聚合				
		VLAN	支持基于端口的 VLAN				
			支持基于 MAC 的 VLAN				
			基于协议的 VLAN				
			基于 IP 子网的 VLAN				
		IP 路由	支持静态路由				
			支持 RIPv1/v2，RIPng				
			支持 OSPFv1/v2				
			支持 BGP4，BGP4+ for IPv6				
			支持 IS-IS				
			支持等价路由，策略路由				
			支持 VRRP				
		IPv6	支持 ND（Neighbor Discovery）				
			支持 PMTU				
			支持 IPv6-Ping，IPv6-Tracert，IPv6-Telnet，IPv6-TFTP				
			支持手动配置 Tunnel				
			支持 6to4 tunnel				
2	入侵检测系统	*性能参数	标准机架式设备≥1U，单电源，内存≥4G，硬盘容量≥64G，千兆电口≥6 个，千兆光口 SFP≥4 个，IPS 吞吐量≥650M，并发连接数≥1800000，新建连接数≥60000，提供 3 年硬件质保，3 年软件升级。	2	台	78000	156000
		部署方式	支持路由模式、透明网桥部署、旁路部署、单臂部署以及混合部署等多种方式。				
		网络特性	支持 802.1Q VLAN Trunk、access 接口类型，VLAN 三层接口和子接口；				
			支持链路聚合功能，可将多条物理链路聚合成一条带宽更高的逻辑链路使用；				
			支持端口联动功能，当上行/下行端口链路出现故障时，对应的另一端下行/上行端口自动切断链路。				

序号	产品名称	功能描述		数量	单位	单价	总价（元）
		路由支持	支持静态路由协议，支持 OSPF 动态路由协议，支持路由异常告警功能，支持 DHCP 中继；				
			*支持多链路出站负载，支持基于源/目的 IP、源/目的端口、协议、ISP、应用类型以及国家地域来进行选路的策略路由选路功能。				
		应用识别与流量控制	*支持基于应用类型，网站类型，文件类型进行带宽分配和流量控制，支持基于时间、地域、认证用户、子接口和 VLAN 等因素实现对象的流量控制。				
		URL 过滤	内置海量 URL 分类库，包含非法及不良网站、成人内容、网上购物、微博论坛等分类，实现全面高效的不良网站过滤。				
		*入侵防护功能	*设备具备独立的入侵防护漏洞规则特征库，特征总数在 7400 条以上；				
		僵尸主机检测	设备具备独立的热门威胁库，支持木马、勒索软件、蠕虫、挖矿病毒等种类，特征总数在 105 万条以上；				
			支持木马远控类、恶意链接类、移动安全类、异常流量类僵尸网络行为的检测。				
		安全可视化	支持全网实时热点事件 TOP10 展示；				
			支持基于攻击阶段图的方式来匹配并展示当前用户遭受到攻击的具体所处状态，并详细给出针对性处理建议，便于用户快速响应安全问题。				
		用户认证	支持本地密码认证，LDAP、Radius 等服务器外部密码认证方式；支持基于域、Proxy、Pop3、Web、Radius 单点登录方式。				
		安全集中管理	支持安全设备的集中管理，包括配置统一下发，规则库统一更新，安全日志实时上报与展示等功能。				
		产品联动	*支持与终端安全产品实现联动，当防火墙发现僵尸网络或者勒索病毒违规向主控端连接时，可实现防火墙联动 EDR 对终端进行扫描和取证，对威胁进行隔离、处置，同时在防火墙上展示威胁处理的详情结果。				
3	防火墙	性能参数	*标准机架式设备≥1U，单电源，内存≥8G，硬盘容量≥64G，千兆电口≥6 个，千兆光口 SFP≥2 个，网络层吞吐量≥12G，应用层吞吐量≥1.5G，并发连接数≥ 2000000，新建连接数（CPS）≥80000，提供 3 年硬件质保，3 年软件升级。	2	台	120000	240000
		部署模式	支持路由，网桥，虚拟网线，旁路镜像，单臂，以及混合部署方式；支持接口 bypass 功能。				
		路由支持	支持多链路出站负载，支持基于源/目的 IP、				

序号	产品名称	功能描述		数量	单位	单价	总价（元）
			源/目的端口、协议、ISP、应用类型以及国家/地域来进行选路的策略路由选路功能。				
		访问控制	访问控制规则支持基于源 / 目的 IP，源端口，源 / 目的区域，用户（组），应用/服务类型，时间组的细化控制方式，支持长连接功能并可以配置连接时长；				
			*访问控制策略支持模拟策略匹配，输入源目的IP、端口、协议五元组信息，模拟策略匹配方式，给出最可能的匹配结果，方便排查故障，或环境部署前的调试。				
		防病毒	*支持采用无特征 AI 检测技术对恶意勒索病毒及挖矿病毒等热点病毒进行检测；				
			支持在业务防护场景，监测服务器外连流量，防止服务器非法下载。				
		Web 应用防御	支持对 HTTP 异常请求协议检测和防护攻击，检测内容包含 HTTP 请求信息的方法及参数长度等；				
			具备识别与阻断外部扫描器发起的服务器恶意扫描行为，可对扫描器地址进行自定义封堵；				
			*支持网站防篡改功能，可防止攻击者非授权修改网站目录文件。				
		DoS/DDoS 攻击防护	支持 SYN Flood、UDP Flood、ICMP Flood、DNS Flood、ICMP Flood、ICMPv6 Flood 攻击防护；并支持自定义防护的目的 IP 丢包阈值、源 IP 封锁阈值和封锁时间。				
		僵尸主机检测	*设备具备独立的僵尸网络与病毒防护库，防护类型包括木马远控、恶意脚本、勒索病毒、僵尸网络、挖矿病毒等，特征总数在 105 万条以上，支持自定义僵尸网络规则库；				
			支持对终端已被种植了远控木马或者病毒等进行检测，多种维度展示失陷外联风险，包括但不限于高级威胁检测、夜间外联检测、高频攻击检测、恶意外联检测、可以进程文件定位；				
			支持失陷风险的自动化处置，当同一个终端或者网络内不同的终端，反复连接同一个域名，会将域名和进程进行绑定，当再次发现终端某一进程访问相同域名的时候，可以将域名关联的恶意文件进程进行自动化处理。				
		漏洞攻击防护	*设备具备独立的入侵防护漏洞规则特征库，特征总数在 7400 条以上，支持自定义漏洞攻击规则库；				
			可提供最新的威胁情报信息，能够对新爆发的流行高危漏洞进行预警和自动检测，发现问题				

序号	产品名称	功能描述		数量	单位	单价	总价（元）
			后支持一键生成防护规则。				
		安全可视	支持针对用户安全的风险汇总，将失陷类的安全事件按照已失陷、高风险、中风险、低风险等优先级展示给管理员，并通过威胁性和确定性的维度展示失陷主机风险的分布情况；				
			支持自动生成安全风险报表，报表内容体现被保护对象的整体安全状况，基于业务和用户安全的风险分析，并提供安全评分细则和危害说明，可以通过报表全面了解业务和用户的安全风险和安全评级状况。				
		产品联动	*支持与 PC 终端管理和服务器 EDR 产品实现联动，当下一代防火墙发现僵尸网络或者勒索病毒违规向主控端连接时，可实现下一代防火墙联动对终端进行扫描和取证，对威胁进行隔离、处置，同时在下一代防火墙上展示威胁处理的详情结果。				
三	应用服务区						
1	防病毒软件服务器端	*产品形态	提供服务器端软件 LINUX 系统授权 10 个，Windows Server 系统授权 50 个	1	套	37200	37200
			产品可以纯软件交付，包含管理控制中心软件及终端客户端软件，其中管理控制中心可云化部署。				
		服务器端	支持 Windows Server 2003/Windows Server 2008 /Windows Server 2008 R2 /Windows Server 2012 /Windows Server 2016，CentOS /Ubuntu Debian /RHEL /SUSE /Red Flag Asianux Server/Oracle Linux 等操作系统。				
		终端安全可视	采用 B/S 架构的管理控制中心，具备终端安全可视，终端统一管理，统一威胁处置，统一漏洞修复，威胁响应处置，日志记录与查询等功能；				
			*支持全网风险展示，包括但不限于未处理的勒索病毒数量、暴力破解数量、WebShell 后门数量、高危漏洞及其各自影响的终端数量。				
		终端管理	支持展示终端资产状况，包括：主机名、在线/离线状态、IPv4 地址、MAC 地址、操作系统、终端 agent 版本、病毒库版本、最近登录时间、最近登录的用户名；终端信息变更能自动更新；				
			支持以安全策略模板方式对指定终端组快速部署安全策略，安全策略模板支持默认模板和自定义模板；				
			*支持安全策略一体化配置，通过一条策略即可实现不同安全功能的配置，包括：终端病毒查				

序号	产品名称	功能描述		数量	单位	单价	总价（元）
			杀的文件扫描配置、文件实时监控的参数配置、WebShell 检测和威胁处置方式、暴力破解的威胁处置方式和 Windows 白名单信任目录。				
		资产管理	*支持全网视角的终端资产统一清点，清点信息包括操作系统、应用软件、监听端口和主机账户，其中操作系统、应用软件和监听端口支持从资产和终端两个视角进行统计和展示；				
			支持收集并展示单个终端的基本信息，包括：主机名、在线/离线状态、IPv4 地址、MAC 地址、操作系统、终端 agent 版本、病毒库版本、最近登录时间、最近登录的用户名；终端信息变更能自动更新。				
		管理员管理	支持配置不同的权限角色，支持超级管理员、普通管理员（管理）、审计管理员（查看）三种权限，并配置可管辖的终端范围				
		升级管理	*支持客户端的错峰升级或灰度升级，可根据实际情况控制客户端同时升级的最大数量，避免大量终端程序同时更新造成网络拥堵或 I/O 风暴				
		漏洞修复及补丁管理	支持对终端的漏洞情况进行扫描，并查看漏洞具体情况及 KB 号，并显示具体修复情况				
		勒索病毒专防	*基于勒索病毒攻击过程，建立多维度立体防护机制，提供事前入侵防御-事中反加密-事后检测响应的完整防护体系，展示勒索病毒处置情况，对勒索病毒及变种实现专门有效防御。				
		微隔离流量可视	支持图形化显示业务系统、服务器及流量详情；				
			流量线详情支持展示该流量线对应的微隔离策略；图形化显示服务器间流量关系，包括访问详情、流量趋势等。				
		微隔离流量可控	服务器详情支持展示服务器的资源状态（CPU 占有率、内存占有率和磁盘率）、流量分布 Top5、该服务器开放的服务。				
		*产品联动	*支持与防火墙设备进行端网联动，通过管理平台下发快速查杀任务；通过防火墙查看其下发的查杀任务的查杀结果，并查杀出的病毒进行处置；				
2	防病毒软件 PC 端	*产品形态	提供 PC 端软件授权≥1000 个；	1	套	120000	120000
			产品可以纯软件交付，包含管理控制中心软件及终端客户端软件，其中管理控制中心可云化部署。				
		终端安全可视	采用 B/S 架构的管理控制中心，具备终端安全可视，终端统一管理，统一威胁处置，统一漏				

序号	产品名称	功能描述		数量	单位	单价	总价（元）
			洞修复，威胁响应处置，日志记录与查询等功能；				
			*支持全网风险展示，包括但不限于未处理的勒索病毒数量、暴力破解数量、WebShell 后门数量、高危漏洞及其各自影响的终端数量。				
		终端管理	支持展示终端资产状况，包括：主机名、在线/离线状态、IPv4 地址、MAC 地址、操作系统、终端 agent 版本、病毒库版本、最近登录时间、最近登录的用户名；终端信息变更能自动更新；				
			支持以安全策略模板方式对指定终端组快速部署安全策略，安全策略模板支持默认模板和自定义模板；				
			*支持安全策略一体化配置，通过一条策略即可实现不同安全功能的配置，包括：终端病毒查杀的文件扫描配置、文件实时监控的参数配置、WebShell 检测和威胁处置方式、暴力破解的威胁处置方式和 Windows 白名单信任目录。				
		资产管理	*支持全网视角的终端资产统一清点，清点信息包括操作系统、应用软件、监听端口和主机账户，其中操作系统、应用软件和监听端口支持从资产和终端两个视角进行统计和展示；				
			支持收集并展示单个终端的基本信息，包括：主机名、在线/离线状态、IPv4 地址、MAC 地址、操作系统、终端 agent 版本、病毒库版本、最近登录时间、最近登录的用户名；终端信息变更能自动更新。				
		管理员管理	支持配置不同的权限角色，支持超级管理员、普通管理员（管理）、审计管理员（查看）三种权限，并配置可管辖的终端范围				
		升级管理	*支持客户端的错峰升级或灰度升级，可根据实际情况控制客户端同时升级的最大数量，避免大量终端程序同时更新造成网络拥堵或 I/O 风暴				
		漏洞修复及补丁管理	支持对终端的漏洞情况进行扫描，并查看漏洞具体情况及 KB 号，并显示具体修复情况				
		勒索病毒专防	*基于勒索病毒攻击过程，建立多维度立体防护机制，提供事前入侵防御-事中反加密-事后检测响应的完整防护体系，展示勒索病毒处置情况，对勒索病毒及变种实现专门有效防御。				
		微隔离流量可视	业务系统详情支持展示流量分布 Top5、业务流量排行 Top5(发送，接收)、业务访问趋势（发送流速、接收流速和用户数）；				

序号	产品名称	功能描述		数量	单位	单价	总价（元）
			流量线详情支持展示该流量线对应的微隔离策略；图形化显示服务器间流量关系，包括访问详情、流量趋势等。				
		微隔离流量可控	提供对业务系统之间、业务系统内不同应用角色之间、业务系统内相同应用角色之间的访问控制策略配置。				
		*产品联动	*支持与防火墙设备进行端网联动，通过管理平台下发快速查杀任务；通过防火墙查看其下发的查杀任务的查杀结果，并查杀出的病毒进行处置；				
3	服务器密码机	产品形态	2U 机架式设备；	2	台	150000	300000
			*RJ-45 10/100/1000M ×2，光纤网口 10G ×2				
			液晶显示屏				
		基础要求	支持 SM2 非对称算法，SM3 杂凑算法，SM1、SM4、SM7 对称算法，并兼容国际算法 RSA、3DES、AES ；				
			密码机 API 接口符合《GM/T0018 密码设备应用接口规范》，同时支持 PKCS#11、MS-CSP、JCE 等国际标准接口；				
			保证关键密钥在任何时候不以明文形式出现在设备外，密钥备份文件受备份密钥的加密保护；				
			能够与河北省医疗保障局统一下发的证书综合管理系统 FCMS 进行无缝对接				
		功能要求	支持通过双物理噪声源生成真随机数，支持密钥的生成、导入、删除、备份和恢复；				
			支持数据加密和数据解密，支持 SM1、SM4、SM7 等国产算法和 3DES、AES 等国际通用算法；支持 ECB、CBC、CFB、OFB 等多种对称加密模式；				
			支持消息鉴别码的产生和验证，支持 MAC 产生及验证；				
			支持 TCP/IP 协议；				
			支持数据摘要，支持 SM3、MD5、SHA-1、SHA-2 等杂凑算法；				
			支持数字签名和数字签名验证，支持利用内部生成的 RSA/ECC 密钥对或外部 RSA/ECC 密钥对请求数据进行数字签名和验证；				
			支持基于 RSA/ECC 密码算法的数字信封功能，并支持数字信封转换功能；				
			支持液晶屏显示设备网络信息、CPU 占用等信息；				
		设备管理与安全性	支持安全通道访问密码机，支持国密 SSL 通道；				
			具有用户管理功能，对访问用户分级管理，提高密码设备自身的安全性；				

序号	产品名称	功能描述		数量	单位	单价	总价（元）
			支持物理防撬密钥保护，非法撬动密码机机箱会触发密钥自毁功能，保护密码机内部密钥安全；				
			支持连接密码和白名单，实现了密码机对应用服务器的授权认证，进一步提高了系统的安全性；				
			设备支持 B/S 和命令界面对设备进行管理；				
		可靠性要求	MTBF ＞ 40000h；				
			具备双冗余热插拔电源				
			支持双主模式（Active-Active）和多机集群；				
		性能要求	SM1 加解密速率>1.1Gbps				
			SM2 密钥对产生速率>11000 对/秒				
			SM2 签名速率>61500 次/秒				
			SM2 验签速率>46500 次/秒				
			SM2 加密速率>6700 次/秒				
			SM2 解密速率>8000 次/秒				
			SM3 计算 Hash 速率>850Mbps				
			SM4 加解密速率>7Gbps				
			1024 位 RSA 密钥对产生速率>150 对/秒				
			1024 位 RSA 签名速率>6200 次/秒				
			1024 位 RSA 验证速率>45000 次/秒				
			2048 位 RSA 密钥对产生速率＞ 30 对/秒				
			2048 位 RSA 签名速率>3600 次/秒				
			2048 位 RSA 验证速率＞ 20000 次/秒				
			最大并发数≥4000				
4	USB KEY	芯片类型	采用高技能、高容量内嵌智能芯片（32 位高性能智能卡芯片）	500	个	60	30000
		接口类型	标准 USB2.0 接口设备，兼容支持 USB1.0 接口、USB3.0 接口				
		用户存储空间	用户存储空支持 128K				
		操作系统	支持 Windows XP/ Win7/ Win8.1/ Win10/Server 2003/2008/2012				
		内置安全算法	支持 RSA（1024/2048 位）				
			支持 SM1/SM2/SM3/SM4，SSF33（256 位）系列算法				
			支持 DES，3DES，AES128/192/256				
			支持 SHA1/SHA256/SHA384/SHA512				
		数据存储时间	安全加密数据存储，至少 10 年				
		权限管理	提供自动锁死功能，支持远程解锁				
5	应用服	外形	2U 机架式服务器	3	台	60000	180000

序号	产品名称	功能描述		数量	单位	单价	总价（元）
	务器	处理器	2 颗英特尔至强银牌 4214(2.2GHz/12-core/16.5MB/85W)处理器				
		内存	128G DDR4 RDIMM 内存				
		硬盘	3 块 480G SSD 硬盘，5 块 1.2T SAS 10K rpm 硬盘				
		网络	2 个千兆电口，2 个万兆光口				
		电源	2 个 550W 交流电源模块				
		安装套件	机架安装导轨				
6	防病毒系统服务器	外形	2U 机架式服务器	1	台	40000	40000
		处理器	2 颗英特尔至强银牌 4214(2.2GHz/12-core/16.5MB/85W)处理器				
		内存	64G DDR4 RDIMM 内存				
		硬盘	3 块 600G SAS 10K rpm 硬盘				
		网络	2 个千兆电口，2 个万兆光口				
		电源	2 个 550W 交流电源模块				
		安装套件	机架安装导轨				
7	数据库软件	基础	所投产品应入选《安可替代工程核心产品名录-1-2020》基础通用产品数据库类目录。	1	套	120000	120000
		兼容性	数据库产品应能够兼容多种硬件体系，可运行于龙芯系列，飞腾系列，申威系列，以及兆芯、鲲鹏、海光等多种不同 CPU 架构的服务器设备，兼容主流 Linux 如麒麟、UOS、中科方德、凝思、深之度、普华、思普等多种国产 Linux 系列操作系统。				
			支持多种开发语言 C/C++、Python、JAVA、.Net、Go、PHP、Node.js 等。				
		扩展性	*数据库产品具备高可扩展性，支持多种集群模式，如：主备集群、读写分离集群、共享存储集群。				
			*数据库产品的共享存储集群，最大可支持 8 节点，集群 7*24 小时运行无故障率可达 99.99%。在 x86 平台和国产平台可达到 2 节点性能是单机的 2 倍。支持 SAN/DAS 存储模式，支持分钟级故障切换，支持故障恢复自动重加入。				
			*单表可支持大于 2000 列字段的表。				
		高性能	*单机单表可支持不低于 140TB 数据，万亿行数据的批量装载、数据插入、更新、查询、删除，单机支持不低于 60000 物理并发连接，				
			*具备高性处理能力，单机数据库事务处理能力 TPMC 值能达到 120 万级别。				
8	服务操作系统	内核版本	操作系统内核版本 4.4 以上	2	套	10000	20000
		符合 POSIX 标准	符合 POSIX 标准				

序号	产品名称	功能描述		数量	单位	单价	总价（元）
		LSB 标准	符合 LSB4.0 标准				
		文件系统	支持 Ext3、Ext4、GFS2、XFS、NTFS 等文件系统				
		中文处理	符合 i18n 技术和标准；支持 GB2312、GBK 等中文字符编码；符合最新国家标准字符集 GB18030-2005				
		服务器兼容性	支持国产厂商服务器产品，如联想、浪潮、航天科工、宝德、长城等				
		虚拟化	支持 KVM、Docker、LXC 等虚拟化方式				
		性能要求	无作业任务运行时 CPU 使用率小于 2.1%，内存使用率小于 6.4%，打开空进程时间小于 1ms				
		集群支持	支持通过通用的集群软件（如高可用、负载均衡、高性能计算）搭建大规模服务器集群				
		中间件	支持金蝶、中创、东方通等国产中间件				
		数据库	支持达梦、人大金仓、神通、南大通用等国产数据库				
		电子公文	支持华迪、华宇、浪潮、东华、神码、太极等国产电子公文交换系统				
		存储管理	支持国产存储设备及存储管理系统，如华为、浪潮、同有、鼎甲、曙光、鲸鲨、中兴等				
		SOA 架构	支持 JMX、JMS、J2CA、WebService 等集成标准				
		备份还原	支持对普通分区、系统分区等的备份还原				
		系统工具	提供图形化的配置工具能够满足网络配置、网络代理、打印机配置、声音配置、输入法设置、日期时间设置、用户账号设置、电源管理、系统检测、默认应用程序、开机启动、鼠标键盘、显示器配置、个性化配置等				
		安装方式	支持光盘、U 盘、网络、Live-CD 等安装				
		防病毒软件	支持国产防病毒软件，如辰信领创、瑞星、奇安信等				
		安全等级	支持符合 RFC2528、X.509 标准的安全认证机制；通过公安部信息安全产品检测中心操作系统第四级结构化保护级认证				
		私有数据隔离保护	提供面向用户私有数据的隐藏隔离保护机制				
		应用程序执行控制	只有经过合法认证且完整的应用程序、内核模块、链接库才能执行、加载和调用				
四	数据交换区						
1	物理隔离网闸	系统基本架构	*采用三机系统结构，内外端机为 TCP/IP 网络协议的终点，阻断 TCP/IP 协议的直接贯通。内外端机之间采用专用硬件和专用协议进行连接，不可编程。网闸以软硬件结合的方式，有效地隔断内外网络间直接的连接，防止信息无	2	台	100000	200000

序号	产品名称	功能描述		数量	单位	单价	总价（元）
			限制交换。				
		操作系统	*采用专用安全操作系统，系统基于可信安全操作平台，内核级主动防御；				
			采用对象互斥和线程守护技术，保护主要进程的安全性和稳定性。				
			不采用通用的指令库和函数库，只提供有限的内部调试用指令函数。				

C包：医疗保障系统骨干网络（政务外网）设备采购参数（120万元）

序号	产品类型	招标参数	数量	单位	单价	总价（元）
1	市级路由器	包转发率≥5000Mpps 架构：双主控； 接口：实配千兆光口≥4个，千兆电口≥4； 槽位数：槽位数≥8 整机功耗≤650W 电源：电源数量≥2 虚拟化 ：支持虚拟化特性，将物理上两台设备虚拟化成一台逻辑设备； 广域网优化：支持对HTTP/FTP等TCP业务流量进行优化传输技术，提高广域网带宽利用率； URL过滤黑名单功能：支持对终端用户域名访问控制功能； 支持openflow功能：支持openflow功能；支持GRE、MPLS VPN，路由协议支持OSPF/RIP/IS-IS/BGP等，支持IPV6； 基于域的防火墙：支持划分安全域，用于管理防火墙设备上安全需求相同的多个接口； IPS入侵防御功能：支持对已知网络攻击进行安全防御，提高网络安全性 ADVPN功能：通过动态VPN技术，实现动态获取对端分支节点当前的公网地址，从而实现两个节点之间动态建立跨越IP核心网络的ADVPN隧道简化VPN网络部署复杂度和提高管理效率； GDVPN功能：支持密钥和IPSEC安全策略集中管理，基于IPSEC安全模型，属于同一组的所有成员共享相同的策略及密钥； VXLAN功能：支持VXLAN数据中心特性； 短信开局：支持利用短信下发的方式实现设备开局部署； U盘0配置部署：支持利用U盘0配置方式实现设备开局部署； 嵌入式自动化：支持对系统软硬部件的内部事件、状态进行监控，出现特定事件后能够自动调整网络设备业务和控制策略，实现智能自动化控制； 支持对系统软硬件的内部事件、状态进行监控，出现问题时收集实时信息并自动修复将实时信息发送到指定服务器.	2	台	63000	126000

		硬件设备原厂三年免费质保维修。				
2	市级防火墙	配置要求： 1、采用专用多核硬件平台，双冗余电源； 2、2U 设备机架设备，不少于 6 个 10/100/1000M 自适应千兆电接口及 12 个 combo 接口； 3、防火墙整机吞吐量≥12Gbps； 4、每秒新建 HTTP 连接数≥28 万； 5、最大并发连接数≥320 万； 6、配置≥60GSSD 硬盘；开通三年防病毒；开通三年入侵防御； 7、支持并开通 SSLVPN 功能，投标产品实配 SSLVPN 并发用户数不少于 2000 个； 8、支持基于硬件 Hypervisor 技术的底层虚拟化，各个虚拟防火墙之间完全隔离，可运行不同的防火墙版本，拥有完全独立的 CPU、内存、接口等资源。 9、支持策略预编译技术，在大量防火墙访问控制策略情况下整机性能不受影响。 10、支持基于接口/安全域、地址、用户、服务、应用和时间的会话控制策略，包括总连接数控制、每秒总新建连接数控制、每 IP 总连接数控制、每 IP 新建连接数控制。 11、支持防扫描功能，可基于管理员设定的阈值识别 TCP、UDP 及 PING 扫描，并自动对发起扫描的主机进行限制。 12、支持路由、透明及混合部署模式，支持 IPV6 协议； 13、支持常见 DOS 攻击防护及 ARP 攻击防护； 14、支持与威胁情报云联动，基于实时更新的威胁情报提供安全防护功能，支持基于 IP、域名的威胁情报查询和实时防护，提供基于威胁情报的内网风险主机/失陷主机一键处理功能； 15、支持基于威胁情报云的动态防护功能，防火墙支持将用户对互联网的访问信息发送至威胁情报云进行实时情报查询及防护。 16、支持与内网终端安全管理系统的联动功能； 17、支持与 IDS 设备的联动，可接收 IDS 产品发送的动态访问控制策略； 18、支持基于线路和多层通道嵌套的带宽管理，至少四层管道嵌套的流控； 19、提供 SQL 注入攻击、XSS 攻击的检测和防御功能，对 Web 服务系统提供保护； 20、系统通过了 CVE 兼容性认证，采用先进的模式匹配及协议分析技术实现对网络报文的分析； 21、支持碎片重组、TCP 流重组及报文统计分析能力； 22、支持扩展 APT 检测模块，采用沙箱检测技术，对未知木马、病毒、恶意代码具有精确的检测效果，实现对未知威胁、高级持续威胁和 ODAY 攻击的有效防护。 23、具备沙盒检测技术，对未知木马、病毒、恶意代码具有	2	台	131000	262000

		精确的检测效果，支持10种以上文件格式的动态分析能力，可对exe、rtf、pdf、xls（x）、ppt（x）、doc（x）、pps（x）、swf、rar、zip等常见的格式进行动态沙箱分析； 24、具备协议自动识别功能，可对运行在非标准端口上的常见业务提供入侵检测及防御功能；入侵防御事件库至少应包括木马后门、缓冲溢出攻击、脚本攻击、拒绝服务攻击、间谍软件及网络数据库攻击等的特征事件；支持入侵防御事件库在线自动升级和手工导入； 25、支持防火墙策略的自动导入；防火墙冗余安全策略分析；防火墙安全策略收敛分析；防火墙策略命中频次分析；防火墙潜在冲突策略分析； 26、不依赖木马特征库，通过会话行为的检测手段检测木马软件发起的会话行为并告警，同时告知发起的源IP和访问的目的IP，分析出怀疑木马通道的原因和相关会话信息； 27、支持静态路由、动态路由（RIP、OSPF、BGP4）； 28、支持基于入接口、源地址、目标地址、服务端口、应用类型的策略路由。 29、支持链路负载均衡，提供轮询、加权轮询、哈希等多种负载均衡算法； 30、支持通过ICMP、TCP、DNS和HTTP协议实现对链路可用性的多重健康检查； 31、支持主-主和主-备模式，主备模式下支持基于设备优先级的主设备抢占功能。 32、支持防火墙集中管理，包括统一状态监控、配置下发、配置自动备份及回滚、版本统一升级、特征库统一升级等功能。 33、支持集中策略分析，通过集中策略分析，实现： 集中对所有防火墙安全策略进行冗余分析，可分析出哪些安全策略是不必要的冗余配置. 集中对所有防火墙安全策略进行收敛分析，也称宽松策略分析。能够支持查看任何一条宽松策略的流量详细信息. 集中对所有防火墙安全策略进行命中频率分析，辅助用户快速完成策略次序的调整，从而达到优化防火墙处理性能的目的. 集中对所有防火墙安全策略进行潜在冲突分析，辅助用户快速完成策略的调整，从而达到防火墙访问控制的目的。 售后服务要求： 要求提供原厂的3年质保和3年免费升级服务，中标后提供原厂售后服务承诺书加盖原厂公章；提供原厂上门安装调试服务，并由原厂工程师配合完成等保检查备案事宜；				

3	县区路由器	1、转发性能：≥15Mpps； 2、配置≥2 个千兆光口，≥4 个千兆电口； 3、冗余电源； 4、网络互联：二层协议：ARP，Ethernet，Ethernet II，VLAN（VLAN-BASED PORT VLAN，VOICE VLAN，Guest VLAN），802.3x，802.1p，802.1Q，802.1x，STP(802.1D) ，RSTP(802.1w)，MSTP(802.1s) 5、IPv4 路由：静态路由、动态路由协议：RIPv1/v2、OSPFv2、BGP、IS-IS、路由迭代、路由策略、ECMP（等价多路径）。 6、IPv6 路由：支持 Ipv6 ND，Ipv6PMTU，Ipv6 FIB，Ipv6 ACL，NAT-PT，Ipv6 隧道，6PE、DS-LITE； 7、IP 协议：IP 服务支持单播转发/组播转发，TCP，UDP，IP Option，IP Unnumber，策略路由，Netstream，sFlow 等 IP 路由：静态路由，动态路由 RIP、OSPF、IS-IS、BGP，组播协议 IGMP、PIM-DM、PIM-M、MBGP 等，路由策略 8、安全特性：PPPoEClient&Server，PORTAL，802.1x、Local 认证，RBAC、Radius，Tacacs ASPF，ACL，FILTER、连接数限制 9、可靠性：支持 VRRP、VRRPv3 支持基于带宽的负载分担与备份 支持基于用户（IP 地址）的负载分担与备份 支持 NQA 同路由、VRRP 和接口备份的联动功能，实现端到端链路的检测与备份功能； 支持 GRE、MPLS VPN，路由协议支持 OSPF/RIP/IS-IS/BGP 等 10、3/4G 无线：支持 3/4GLTE Modem，支持 TD-SCDMA、CDMA2000/EVDO、WCDMA/HSPA+网络。 11、MPLS：协议：LDP、Static LSP。 L3VPN：跨域 MPLSVPN（Option1/2/3）、嵌套 MPLSVPN、分层 PE（HoPE）、CE 双归属、MCE、多角色主机等。 L2VPN： Martini、Kompella、CCC 和 SVC 方式、MPLSTE、RSVP TE。 12、语音：支持 FXS/FXO/E&M/E1/T1，支持 R2，DSS1，Q.sig，Digital E&M 等。 支持 G.711、G.723、G.726、G.729AB、AMR-NB、GSM-FR、iLBC、RT-Audio 等。 支持丰富的语音业务、语音备份，DTMF 传输支持 RFC2833，智能拨号路由器，FXS 和 FXO 的 1:1 绑定，断电逃生，SIP Sever 本地存活，IVR 等。 13、服务、管理与维护：支持 SNMP V1/V2c/V3，MIB，SYSLOG，RMON。 支持命令行管理，文件系统管理， Dual Image。 支持 DHCP， FTP，HTTP，ICMP，UDP public， UDP private， TCP public， TCP private， SNMP 等协议测试。 支持 console 口登录，支持 telnet（VTY）登录，支持 SSH 登录，支持 FTP 登录。	9	台	27200	244800

		14、虚拟化：支持虚拟化特性，将物理上两台设备虚拟化成一台逻辑设备； 15、广域网优化：支持对 HTTP/FTP 等 TCP 业务流量进行优化传输技术，提高广域网带宽利用率； URL 过滤黑名单功能：支持对终端用户域名访问控制功能； 17、支持 openflow 功能：支持 openflow 功能； 基于域的防火墙：支持划分安全域，用于管理防火墙设备上安全需求相同的多个接口； IPS 入侵防御功能：支持对已知网络攻击进行安全防御，提高网络安全性 19、ADVPN 功能：通过动态 VPN 技术，实现动态获取对端分支节点当前的公网地址，从而实现两 个节点之间动态建立跨越 IP 核心网络的 ADVPN 隧道简化 VPN 网络部署复杂度和提高管理效率； 20、GDVPN 功能：支持密钥和 IPSEC 安全策略集中管理，基于 IPSEC 安全模型，属于同一组的所有 成员共享相同的策略及密钥； 21、VXLAN 功能：支持 VXLAN 数据中心特性； 短信开局：支持利用短信下发的方式实现设备开局部署； U 盘 0 配置部署：支持利用 U 盘 0 配置方式实现设备开局部署； 22、嵌入式自动化：支持对系统软硬部件的内部事件、状态进行监控，出现特定事件后能够自动调整网络设备业务和控制策略，实现智能自动化控制 支持对系统软硬件的内部事件、状态进行监控，出现问题时收集实时信息并自动修复将实时信息发送到指定服务器 23、硬件设备原厂三年免费质保维修。				
4	县区防火墙	配置要求： 1、采用专用多核硬件平台； 2、1U 设备，不少于 6 个 10/100M/1000M 自适应千兆电接口； 3、防火墙整机吞吐量≥3Gbps； 4、每秒新建 HTTP 连接数≥16 万； 5、最大并发连接数≥200 万； 6、开通三年防病毒，开通三年入侵防御； 7、支持并开通 SSLVPN 功能，投标产品实配 SSLVPN 并发用户数不少于 1000 个； 8、支持基于硬件 Hypervisor 技术的底层虚拟化，各个虚拟防火墙之间完全隔离，可运行不同的防火墙版本，拥有完全独立的 CPU、内存、接口等资源。 9、支持策略预编译技术，在大量防火墙访问控制策略情况下整机性能不受影响。 10、支持基于接口/安全域、地址、用户、服务、应用和时间的会话控制策略，包括总连接数控制、每秒总新建连接数控制、每 IP 总连接数控制、每 IP 新建连接数控制。 11、支持防扫描功能，可基于管理员设定的阈值识别 TCP、	9	台	51200	460800

		UDP 及 PING 扫描，并自动对发起扫描的主机进行限制。 12、支持路由、透明及混合部署模式,支持 IPV6 协议； 13、支持常见 DOS 攻击防护及 ARP 攻击防护； 14、支持与威胁情报云联动，基于实时更新的威胁情报提供安全防护功能，支持基于 IP、域名的威胁情报查询和实时防护，提供基于威胁情报的内网风险主机/失陷主机一键处理功能； 15、支持基于威胁情报云的动态防护功能，防火墙支持将用户对互联网的访问信息发送至威胁情报云进行实时情报查询及防护。 16、支持与内网终端安全管理系统的联动功能； 17、支持与 IDS 设备的联动，可接收 IDS 产品发送的动态访问控制策略；18、支持基于线路和多层通道嵌套的带宽管理，至少四层管道嵌套的流控； 19、提供 SQL 注入攻击、XSS 攻击的检测和防御功能，对 Web 服务系统提供保护； 20、系统通过了 CVE 兼容性认证，采用先进的模式匹配及协议分析技术实现对网络报文的分析； 21、支持碎片重组、TCP 流重组及报文统计分析能力； 22、支持扩展 APT 检测模块，采用沙箱检测技术，对未知木马、病毒、恶意代码具有精确的检测效果，实现对未知威胁、高级持续威胁和 ODAY 攻击的有效防护。 23、具备沙盒检测技术，对未知木马、病毒、恶意代码具有精确的检测效果，支持 10 种以上文件格式的动态分析能力，可对 exe、rtf、pdf、xls（x）、ppt（x）、doc（x）、pps（x）、swf、rar、zip 等常见的格式进行动态沙箱分析； 24、具备协议自动识别功能，可对运行在非标准端口上的常见业务提供入侵检测及防御功能；入侵防御事件库至少应包括木马后门、缓冲溢出攻击、脚本攻击、拒绝服务攻击、间谍软件及网络数据库攻击等的特征事件；支持入侵防御事件库在线自动升级和手工导入； 25、支持防火墙策略的自动导入；防火墙冗余安全策略分析；防火墙安全策略收敛分析；防火墙策略命中频次分析；防火墙潜在冲突策略分析； 26、不依赖木马特征库，通过会话行为的检测手段检测木马软件发起的会话行为并告警，同时告知发起的源 IP 和访问的目的 IP，分析出怀疑木马通道的原因和相关会话信息； 27、支持静态路由、动态路由（RIP、OSPF、BGP4）； 28、支持基于入接口、源地址、目标地址、服务端口、应用类型的策略路由。 29、支持链路负载均衡，提供轮询、加权轮询、哈希等多种负载均衡算法； 30、支持通过 ICMP、TCP、DNS 和 HTTP 协议实现对链路可用性的多重健康检查； 31、支持主-主和主-备模式，主备模式下支持基于设备优先				

		级的主设备抢占功能。 32、支持防火墙集中管理，包括统一状态监控、配置下发、配置自动备份及回滚、版本统一升级、特征库统一升级等功能。 33、支持=集中策略分析，通过集中策略分析，实现： 集中对所有防火墙安全策略进行冗余分析，可分析出哪些安全策略是不必要的冗余配置. 集中对所有防火墙安全策略进行收敛分析，也称宽松策略分析。能够支持查看任何一条宽松策略的流量详细信息. 集中对所有防火墙安全策略进行命中频率分析，辅助用户快速完成策略次序的调整，从而达到优化防火墙处理性能的目的. 集中对所有防火墙安全策略进行潜在冲突分析，辅助用户快速完成策略的调整，从而达到防火墙访问控制的目的。 售后服务要求： 要求提供原厂的3年质保和3年免费升级服务，中标后提供原厂售后服务承诺书加盖原厂公章；提供原厂上门安装调试服务，并由原厂工程师配合完成等保检查备案事宜；				
5	集成运维费	负责市区及县区设备安装、调试、运输以及后期网络设备、安全设备、线路日常操作、维护、故障处理等。				106400

D包：医疗保障系统骨干网络（专线）设备采购参数（120万元）

序号	产品类型	招标参数	数量	单位	单价	总价（元）
1	市级路由器	1) 包转发率≥6000Mpps 2) 架构：控制转发物理分离，双主控； 3) 接口： 实配千兆光口≥14个，千兆电口≥8，数据版软件授权*1 4) 槽位数：槽位数≥8 板卡种类：支持通道化E1、非通道化E1、异步串口、同异步串口、等广域网接口扩展； 5) 整机功耗≤650W 6) 电源：电源数量≥2 虚拟化IRF ：支持虚拟化特性，将物理上两台设备虚拟化成一台逻辑设备； 广域网优化：支持对HTTP/FTP等TCP业务流量进行优化传输技术，提高广域网带宽利用率； 7) URL过滤黑名单功能：支持对终端用户域名访问控制功能； 8) 支持openflow功能：支持openflow功能；	2	台	74500	149000

		基于域的防火墙：支持划分安全域，用于管理防火墙设备上安全需求相同的多个接口； 9） IPS 入侵防御功能：支持对已知网络攻击进行安全防御，提高网络安全性 10） ADVPN 功能：通过动态 VPN 技术，实现动态获取对端分支节点当前的公网地址，从而实现两 个节点之间动态建立跨越 IP 核心网络的 ADVPN 隧道简化 VPN 网络部署复杂度和提高管理效率； 11） GDVPN 功能：支持密钥和 IPSEC 安全策略集中管理，基于 IPSEC 安全模型，属于同一组的所有 成员共享相同的策略及密钥； 12） VXLAN 功能：支持 VXLAN 数据中心特性； 13)支持 GRE、MPLS VPN，路由协议支持 OSPF/RIP/IS-IS/BGP 等，支持 IPV6； 短信开局：支持利用短信下发的方式实现设备开局部署； U 盘 0 配置部署：支持利用 U 盘 0 配置方式实现设备开局部署； 够自动调整网络设备业务和控制策略，实现智能自动化控制 支持对系统软硬件的内部事件、状态进行监控，出现问题时收集实时信息并自动修复将实时信息发送到指定服务器 14）硬件设备原厂三年免费质保维修。				
2	县区路由器	1、转发性能：16Mpps 2、USB2.0：2，支持 3/4G Modem 扩展； 3、要求配置 3 个千兆电口可光电复用，2 千光口，配置双主控板卡； 4、CON：1； 5、AUX：1； 6、冗余电源：内置（AC/DC/PoE），N+1 备份； 7、网络互联：二层协议：ARP，Ethernet，Ethernet II，VLAN（VLAN-BASED PORT VLAN，VOICE VLAN，Guest VLAN），802.3x，802.1p，802.1Q，802.1x，STP(802.1D) ，RSTP(802.1w)，MSTP(802.1s) 8、IPv4 路由：静态路由、动态路由协议：RIPv1/v2、OSPFv2、BGP、IS-IS、路由迭代、路由策略、ECMP（等价多路径）。 9、IPv6 路由：支持 Ipv6 ND，Ipv6 PMTU，Ipv6 FIB，Ipv6 ACL，NAT-PT，Ipv6 隧道，6PE、DS-LITE； 10、IP 协议：IP 服务支持单播转发/组播转发，TCP，UDP，IP Option，IP Unnumber，策略路由，Netstream，sFlow 等 IP 路由：静态路由，动态路由 RIP、OSPF、IS-IS、BGP，组播协议 IGMP、PIM-DM、PIM-M、MBGP 等，路由策略 11、安全特性：PPPoE Client&Server，PORTAL，802.1x、Local 认证，RBAC、Radius，Tacacs ASPF，ACL，FILTER、连接数限制 12、可靠性：支持 VRRP、VRRPv3 支持基于带宽的负载分担与备份	9	台	27400	246600

		支持基于用户（IP 地址）的负载分担与备份				
		支持 NQA 同路由、VRRP 和接口备份的联动功能，实现端到端链路的检测与备份功能				
		13、3/4G 无线：支持 3/4GLTE Modem，支持 TD-SCDMA、CDMA2000/EVDO、WCDMA/HSPA+网络。				
		14、MPLS：协议：LDP、Static LSP。				
		L3VPN：跨域 MPLS VPN（Option1/2/3）、嵌套 MPLS VPN、分层 PE（HoPE）、CE 双归属、MCE、多角色主机等。				
		L2VPN： Martini、Kompella、CCC 和 SVC 方式、MPLS TE、RSVP TE。				
		15、语音：支持 FXS/FXO/E&M/E1/T1，支持 R2，DSS1，Q.sig，Digital E&M 等。				
		支持 G.711、G.723、G.726、G.729AB、AMR-NB、GSM-FR、iLBC、RT-Audio 等。				
		支持丰富的语音业务、语音备份，DTMF 传输支持 RFC2833，智能拨号路由器，FXS 和 FXO 的 1:1 绑定，断电逃生，SIP Sever 本地存活，IVR 等。				
		16、服务、管理与维护：支持 SNMP V1/V2c/V3，MIB，SYSLOG，RMON。				
		支持命令行管理，文件系统管理， Dual Image。				
		支持 DHCP，FTP，HTTP，ICMP，UDP public，UDP private，TCP public，TCP private，SNMP 等协议测试。				
		支持 console 口登录，支持 telnet（VTY）登录，支持 SSH 登录，支持 FTP 登录。				
		17、虚拟化 IRF ：支持虚拟化特性，将物理上两台设备虚拟化成一台逻辑设备；				
		18、 广域网优化：支持对 HTTP/FTP 等 TCP 业务流量进行优化传输技术，提高广域网带宽利用率；				
		19、 URL 过滤黑名单功能：支持对终端用户域名访问控制功能；				
		20、支持 openflow 功能：支持 openflow 功能；				
		基于域的防火墙：支持划分安全域，用于管理防火墙设备上安全需求相同的多个接口；				
		21、 IPS 入侵防御功能：支持对已知网络攻击进行安全防御，提高网络安全性				
		22、ADVPN 功能：通过动态 VPN 技术，实现动态获取对端分支节点当前的公网地址，从而实现两				
		个节点之间动态建立跨越 IP 核心网络的 ADVPN 隧道简化 VPN 网络部署复杂度和提高管理效率；				
		23、GDVPN 功能：支持密钥和 IPSEC 安全策略集中管理，基于 IPSEC 安全模型，属于同一组的所有				
		成员共享相同的策略及密钥；				
		24、VXLAN 功能：支持 VXLAN 数据中心特性；				
		短信开局：支持利用短信下发的方式实现设备开局部署；				
		U 盘 0 配置部署：支持利用 U 盘 0 配置方式实现设备开局部				

		署；				
		够自动调整网络设备业务和控制策略，实现智能自动化控制				
		支持对系统软硬件的内部事件、状态进行监控，出现问题时收集实时信息并自动修复将实时信息发送到指定服务器				
		硬件设备原厂三年免费质保维修。				
3	市级防护墙	配置要求： 1、采用专用多核硬件平台，双冗余电源； 2、2U 设备机架设备，不少于 6 个 10/100/1000M 自适应千兆电接口及 12 个 combo 接口； 3、防火墙整机吞吐量≥12Gbps； 4、每秒新建 HTTP 连接数≥28 万； 5、最大并发连接数≥320 万； 6、配置≥60GSSD 硬盘；开通三年防病毒；开通三年入侵防御； 7、支持并开通 SSLVPN 功能，投标产品实配 SSLVPN 并发用户数不少于 2000 个； 8、支持基于硬件 Hypervisor 技术的底层虚拟化，各个虚拟防火墙之间完全隔离，可运行不同的防火墙版本，拥有完全独立的 CPU、内存、接口等资源。 9、支持策略预编译技术，在大量防火墙访问控制策略情况下整机性能不受影响。 10、支持基于接口/安全域、地址、用户、服务、应用和时间的会话控制策略，包括总连接数控制、每秒总新建连接数控制、每 IP 总连接数控制、每 IP 新建连接数控制。 11、支持防扫描功能，可基于管理员设定的阈值识别 TCP、UDP 及 PING 扫描，并自动对发起扫描的主机进行限制。 12、支持路由、透明及混合部署模式，支持 IPV6 协议； 13、支持常见 DOS 攻击防护及 ARP 攻击防护； 14、支持与威胁情报云联动，基于实时更新的威胁情报提供安全防护功能，支持基于 IP、域名的威胁情报查询和实时防护，提供基于威胁情报的内网风险主机/失陷主机一键处理功能； 15、支持基于威胁情报云的动态防护功能，防火墙支持将用户对互联网的访问信息发送至威胁情报云进行实时情报查询及防护。 16、支持与内网终端安全管理系统的联动功能； 17、支持与 IDS 设备的联动，可接收 IDS 产品发送的动态访问控制策略； 18、支持基于线路和多层通道嵌套的带宽管理，至少四层管道嵌套的流控； 19、提供 SQL 注入攻击、XSS 攻击的检测和防御功能，对 Web 服务系统提供保护； 20、系统通过了 CVE 兼容性认证，采用先进的模式匹配及协议分析技术实现对网络报文的分析； 21、支持碎片重组、TCP 流重组及报文统计分析能力；	2	台	125000	250000

		22、支持扩展 APT 检测模块，采用沙箱检测技术，对未知木马、病毒、恶意代码具有精确的检测效果，实现对未知威胁、高级持续威胁和 ODAY 攻击的有效防护。				
		23、具备沙盒检测技术，对未知木马、病毒、恶意代码具有精确的检测效果，支持 10 种以上文件格式的动态分析能力，可对 exe、rtf、pdf、xls（x）、ppt（x）、doc（x）、pps（x）、swf、rar、zip 等常见的格式进行动态沙箱分析；				
		24、具备协议自动识别功能，可对运行在非标准端口上的常见业务提供入侵检测及防御功能；入侵防御事件库至少应包括木马后门、缓冲溢出攻击、脚本攻击、拒绝服务攻击、间谍软件及网络数据库攻击等的特征事件；支持入侵防御事件库在线自动升级和手工导入；				
		25、支持防火墙策略的自动导入；防火墙冗余安全策略分析；防火墙安全策略收敛分析；防火墙策略命中频次分析；防火墙潜在冲突策略分析；				
		26、不依赖木马特征库，通过会话行为的检测手段检测木马软件发起的会话行为并告警，同时告知发起的源 IP 和访问的目的 IP，分析出怀疑木马通道的原因和相关会话信息；				
		27、支持静态路由、动态路由（RIP、OSPF、BGP4）；				
		28、支持基于入接口、源地址、目标地址、服务端口、应用类型的策略路由。				
		29、支持链路负载均衡，提供轮询、加权轮询、哈希等多种负载均衡算法；				
		30、支持通过 ICMP、TCP、DNS 和 HTTP 协议实现对链路可用性的多重健康检查；				
		31、支持主-主和主-备模式，主备模式下支持基于设备优先级的主设备抢占功能。				
		32、支持防火墙集中管理，包括统一状态监控、配置下发、配置自动备份及回滚、版本统一升级、特征库统一升级等功能。				
		33、支持集中策略分析，通过集中策略分析，实现：				
		集中对所有防火墙安全策略进行冗余分析，可分析出哪些安全策略是不必要的冗余配置.				
		集中对所有防火墙安全策略进行收敛分析，也称宽松策略分析。能够支持查看任何一条宽松策略的流量详细信息.				
		集中对所有防火墙安全策略进行命中频率分析，辅助用户快速完成策略次序的调整，从而达到优化防火墙处理性能的目的.				
		集中对所有防火墙安全策略进行潜在冲突分析，辅助用户快速完成策略的调整，从而达到防火墙访问控制的目的。				
		售后服务要求：				
		要求提供原厂的 3 年质保和 3 年免费升级服务，中标后提供原厂售后服务承诺书加盖原厂公章；提供原厂上门安装调试服务，并由原厂工程师配合完成等保检查备案事宜；				
4	县区防	配置要求：	9	台	49370	444330

	火墙	1、采用专用多核硬件平台，双电源；				
		2、1U 设备，不少于 6 个 10/100M/1000M 自适应千兆电接口及 1 个接口扩展槽位；				
		3、防火墙整机吞吐量≥4Gbps；				
		4、每秒新建 HTTP 连接数≥20 万；				
		5、最大并发连接数≥220 万；				
		6、开通三年防病毒，开通三年入侵防御；				
		7、支持并开通 SSLVPN 功能，投标产品实配 SSLVPN 并发用户数不少于 1000 个；				
		8、支持基于硬件 Hypervisor 技术的底层虚拟化，各个虚拟防火墙之间完全隔离，可运行不同的防火墙版本，拥有完全独立的 CPU、内存、接口等资源。				
		9、支持策略预编译技术，在大量防火墙访问控制策略情况下整机性能不受影响。				
		10、支持基于接口/安全域、地址、用户、服务、应用和时间的会话控制策略，包括总连接数控制、每秒总新建连接数控制、每 IP 总连接数控制、每 IP 新建连接数控制。				
		11、支持防扫描功能，可基于管理员设定的阈值识别 TCP、UDP 及 PING 扫描，并自动对发起扫描的主机进行限制。				
		12、支持路由、透明及混合部署模式，支持 IPV6 协议；				
		13、支持常见 DOS 攻击防护及 ARP 攻击防护；				
		14、支持与威胁情报云联动，基于实时更新的威胁情报提供安全防护功能，支持基于 IP、域名的威胁情报查询和实时防护，提供基于威胁情报的内网风险主机/失陷主机一键处理功能；				
		15、支持基于威胁情报云的动态防护功能，防火墙支持将用户对互联网的访问信息发送至威胁情报云进行实时情报查询及防护。				
		16、支持与内网终端安全管理系统的联动功能；				
		17、支持与 IDS 设备的联动，可接收 IDS 产品发送的动态访问控制策略；18、支持基于线路和多层通道嵌套的带宽管理，至少四层管道嵌套的流控；				
		19、提供 SQL 注入攻击、XSS 攻击的检测和防御功能，对 Web 服务系统提供保护；				
		20、系统通过了 CVE 兼容性认证，采用先进的模式匹配及协议分析技术实现对网络报文的分析；				
		21、支持碎片重组、TCP 流重组及报文统计分析能力；				
		22、支持扩展 APT 检测模块，采用沙箱检测技术，对未知木马、病毒、恶意代码具有精确的检测效果，实现对未知威胁、高级持续威胁和 ODAY 攻击的有效防护。				
		23、具备沙盒检测技术，对未知木马、病毒、恶意代码具有精确的检测效果，支持 10 种以上文件格式的动态分析能力，可对 exe、rtf、pdf、xls（x）、ppt（x）、doc（x）、pps（x）、swf、rar、zip 等常见的格式进行动态沙箱分析；				
		24、具备协议自动识别功能，可对运行在非标准端口上的常				

		见业务提供入侵检测及防御功能；入侵防御事件库至少应包括木马后门、缓冲溢出攻击、脚本攻击、拒绝服务攻击、间谍软件及网络数据库攻击等的特征事件；支持入侵防御事件库在线自动升级和手工导入；				
		25、支持防火墙策略的自动导入；防火墙冗余安全策略分析；防火墙安全策略收敛分析；防火墙策略命中频次分析；防火墙潜在冲突策略分析；				
		26、不依赖木马特征库，通过会话行为的检测手段检测木马软件发起的会话行为并告警，同时告知发起的源 IP 和访问的目的 IP，分析出怀疑木马通道的原因和相关会话信息；				
		27、支持静态路由、动态路由（RIP、OSPF、BGP4）；				
		28、支持基于入接口、源地址、目标地址、服务端口、应用类型的策略路由。				
		29、支持链路负载均衡，提供轮询、加权轮询、哈希等多种负载均衡算法；				
		30、支持通过 ICMP、TCP、DNS 和 HTTP 协议实现对链路可用性的多重健康检查；				
		31、支持主-主和主-备模式，主备模式下支持基于设备优先级的主设备抢占功能。				
		32、支持防火墙集中管理，包括统一状态监控、配置下发、配置自动备份及回滚、版本统一升级、特征库统一升级等功能。				
		33、支持=集中策略分析，通过集中策略分析，实现：				
		集中对所有防火墙安全策略进行冗余分析，可分析出哪些安全策略是不必要的冗余配置.				
		集中对所有防火墙安全策略进行收敛分析，也称宽松策略分析。能够支持查看任何一条宽松策略的流量详细信息.				
		集中对所有防火墙安全策略进行命中频率分析，辅助用户快速完成策略次序的调整，从而达到优化防火墙处理性能的目的.				
		集中对所有防火墙安全策略进行潜在冲突分析，辅助用户快速完成策略的调整，从而达到防火墙访问控制的目的。				
		售后服务要求：				
5	全市网络环境运维服务	要求提供原厂的 3 年质保和 3 年免费升级服务，中标后提供原厂售后服务承诺书加盖原厂公章；提供原厂上门安装调试服务，并由原厂工程师配合完成等保检查备案事宜；				110070
		负责市区及县区设备安装、调试、运输以及后期网络设备、安全设备、线路日常操作、巡检、故障处理等。				

E 包：医疗保障“两定”单位医保结算网络网闸设备(48 万元)

分类	特性/功能	详细描述	数量	单位	单价	总价（元）
产品架构	★系统基本架构	采用“2+1”系统结构，内外端机为 TCP/IP 网络协议的终点，阻断 TCP/IP 协议的直接贯通；内外端机之间采用专用硬件和专用协议进行连接，不可编程；网闸以软硬件结合的方式，有效地隔断内外网络间直接的连接，防止信息无限制交换。	2	台	240000	480000
	★安全体系结构	仲裁审计系统部署于内端机上，通用协议无法通过外端机直接连接到仲裁系统；支持主动仲裁方式。				
	★操作系统	系统基于可信免疫操作系统，能够对内外两个主机系统提供多层次、高强度的安全防护，保护其重要文件、数据不受黑客侵袭； 操作系统基于 Linux 标准操作系统精简、强化； 采用对象互斥和线程守护技术，保护主要进程的安全性和稳定性； 不采用通用的指令库和函数库，只提供有限的内部调试用指令函数。				
功能要求	安全上网功能	提供安全的上网访问，支持 HTTP 协议及代理等； 访问控制对象：源地址、目标地址、源端口、目的端目、域名、URL、访问方式、时间等； 内容过滤：关键字过滤； 脚本过滤：javascript、Applet、ActiveX 等； 提供用户名/密码认证方式。				
	安全邮件功能	提供安全的邮件访问，支持 POP3、SMTP 协议； 支持邮件主题过滤； 支持附件传输进行控制； 支持邮件大小控制。				
	文件传输功能	提供安全的文件传输功能，支持 FTP 等文件传输协议； 支持用户名/密码认证； 支持用户名/IP-MAC 绑定。				
	文件同步功能	可通过专用客户端或共享方式提供安全的文件同步功能； 占用系统资源少，文件交换效率高，不会频繁的进行磁盘扫描； 支持 windows 平台和 linux 平台； 支持一对多或多对一传输； 支持目录内子目录同步，至多支持 32 级目录。				
	数据库访问功能	提供对多种主流数据库（SQL、ORACLE、DB2、SYBASE 等）数据库系统的安全访问； 无需修改数据库工作模式或服务器注册表； 支持用户查询、修改、添加、删除等操作； 支持全表复制、增量更新、全表更新等。				

	自定义功能	支持用户基于标准 TCP、UDP 开发的自定义协议软件； 无需对自定义协议软件进行二次修改开发； 可以根据需求开发新的专用协议处理过滤功能；				
	★安全管理	支持运维管理设备的跨网运维，能够实时开启、关闭运维通道； 支持 SNMP 协议，可与标准网管平台无缝兼容； 支持配置系统账号和应用账号，系统账号用于系统管理员使用，应用账号供应用通道使用； 单个物理接口上有多个地址时，可自主选择由哪个地址作为源地址发包与服务器进行通讯； 支持多网口冗余功能，可提供链路冗余和负载均衡； 支持扩展可信模块，对内外端主机系统进行可信锁定。				
	★系统管理	管理端采用 B/S 结构； 管理端：用于通道建立、策略制定等； 审计端：用于日志查询、分析、导出等； 安全终端管理：可通过串口终端管理方式对网闸进行维护； 支持指纹认证登录； 仅允许通过内端机的管理口对网闸进行配置管理和审计日志。				
性能配置	★接口要求	内网≥6 个 10/100/1000M RJ45 接口，2 个千兆 SFP 光口，1 个串口，2 个 USB 口； 外网≥6 个 10/100/1000M RJ45 接口，2 个千兆 SFP 光口，1 个串口，2 个 USB 口；				
	★性能指标	网络吞吐量≥1000Mbps； 系统整体时延：<1ms； 所有协议通道并发连接数≥60000。				
	售后要求	提供≥3 年硬件质保，≥3 年软件升级。				

五、 供货周期及保修：合同签订后 10 天，保修期 3 年。

六、 系统设备需满足的服务标准、期限、效率要求

1、保修期内非采购人的人为原因而出现产品质量及安装问题，由中标人负责包修、包换或包退，保修期 1 年（自安装验收合格之次日起计）。中标人应在收到采购人故障通知后派员到现场维修，由此产生的一切费用均由中标人承担。

2、关于现场维修。本次采购的商品，除原厂家已承诺在保修期内提供现场维修外，其余均要求由中标人在3年内提供现场维修服务。在保修期内，货物如出现质量问题，接到通知后，中标人须在2小时内响应派技术人员上门维修，对1个工作日不能修复的，必须采取临时调换等措施，以保证使用单位的正常工作。原厂家承诺的服务措施（如400电话等），可作为中标人的技术和服务支持，但中标人不得以此为由拒绝提供第一时间的服务。在保修期外，如有维修、换件等问题，中标人须在8小时内响应并派技术人员上门维修且仅收不高于市场价格的费用。

3、对本次采购提出的售后服务要求，投标人或原厂家的承诺与此不符的，必须以采购人的要求为准，除非投标人在投标书中正式声明拒绝，否则均视为认同，并将在合同中载明。

4、要求中标供应商成交价包含设备安装、调试、布线、验收等一切事宜及费用，包含所需辅材及施工中所涉及其他必需内容，因项目环境、用户现状勘查不明导致的错项、漏项均由供应商自行承担，采购方不再另行支付。

5、培训要求：

（1）在设备投入使用前，中标人需对采购人系统管理人员提供具有针对性的系统培训，以保证设备的各项功能让采购人完全掌握，能够胜任系统的全部运行、操作、维护以及故障分析处理。

（2）投标人应提供全面、详细的培训方案。培训方案至少包括如下内容：培训计划、培训大纲、培训人数等。

（3）提供主要设备的原厂培训，培训人数2人，培训时间不少于1天。

七、系统设备验收标准

1．主要设备外形包装验收：

每台设备有独立的包装，包装外观完好，无破损、变形，否则视为产品不合格。

2．主要设备开箱检验：

根据包装箱中的装箱单查验设备及其附件，包装箱中应有产品合格证、保修卡。根据技术配置要求，从设备外观检验设备是否符合要求，外观是否有划伤或者磨损，否则则视为不合格。

3．系统设备安装检验：

前端摄像机等设备、后端中心设备等按照用户要求安装指定位置。

4．网线等线路施工检验：

系统所有的强电、弱电、接地综合布线及所有需用物品。使用正规厂商生产的品牌线材、插座、镀金水晶头等材料，线缆留有充足长度方便日后维修。

八、其它要求

供货时需提供主要设备生产厂商针对本项目的售后服务承诺函原件。