采购内容及需求

一、系统现状描述

目前，杭州市卫生数据中心 IT 架构逐步完善，对运维专业性需求显著增加；IT 系统数量多，复杂度高，系统之间关联性强，系统的实时性、可用性、稳定性、可靠性要求很高。构建安全的运行网络，提高信息系统的运维效率，确保各系统的高效、稳定运行。

经过若干年的建设,现在业务系统平台已经由传统的 X86 模式进化为虚拟化平台模式，使用效率大大提高，管理也较为方便，但是在不断的建设中，也注意到需要对虚拟化平台采取一定程度的防护措施，经过技术分析， 针对虚拟化和云端的建设方面，急需加强防护，并且紧跟目前的信息安全形势，在我单位 IT 人员不足的情况下，针对日益增多的各方网络黑客，APT 攻击等层次不穷的情况，采用外部服务支撑的方式来进行。

本次项目的目的是通过安全服务，保证各类软硬件设施及信息系统的安全、高效、稳定地运行，降低硬件事故风险，通过电脑维护服务保障杭州市卫健委及杭州市卫生信息中心日常办公过程中涉及的相关信息化工作能够正常开展。

二、项目实施内容

主要内容：

1、虚拟化防护系统扩容；

2、虚拟化软件安全套件扩容；

3、安全运维防护服务。

三、项目建设清单

序号	产品类型	数量	配置要求
1	虚拟化防护系统扩容	1 套	详见技术参数表
2	虚拟化软件安全套件扩容	1 套	详见技术参数表
3	安全运维防护服务	1 套	详见技术参数表

四、总体技术指标要求

1、虚拟化防护系统扩容

指标	指标项

品牌要求	投标产品有公安部的安全产品销售许可证,必须是自主开发，拥有自主知识产权，市场主流的，非 OEM 产品，具有先进性,并成熟可靠
数量要求	提供至少 12 CPU（虚拟化杀毒和虚拟化补丁）的原厂授权许可，提供 12 个节点 AV+DPI 双模块的原厂授权三年许可。
兼容性要求	原有虚拟化防护软件扩容，可兼容使用，统一平台管理。
管理控制台要求	能够在一个管理控制台上管理多个异构虚拟化安全策略。可以在一个管理控制台中同时管理如下虚拟化平台的安全策略： Vmware Citrix 华三 CAS 华为 Fusionsphere KVM
功能要求	产品要求提供完整的主机安全防护，实现实体服务器防御和虚拟服务器的主机防御，包括防火墙、防病毒、虚拟补丁技术等功能，同时支持扩展完整性监控和日志审计功能；
	产品必须具有 防火墙功能，不依赖分布式交换机可以无代理运行,并且可集中控管防火墙策略，策略定制可以针对 IP,Mac 地址或通讯端口,可保护所有基于 IP 通讯协议（TCP、UDP、 ICMP 等）和所有框架类型（IP、ARP 等）。
	产品必须具有 DPI(深度内容检测)功能，不依赖分布式交换机可以无代理运行,必须可以同时保护操作系统和应用服务（数据库，Web，DHCP 等）
	产品必须具有操作系统虚拟补丁功能，不依赖分布式交换机可以无代理运行,在服务器尚无安装补丁前,提供针对此补丁攻击的防护能力。
	具备特征库更新功能，实时追踪并保护最新动态威胁：提供自动扫描功能，针对服务器弱点、漏洞进行安全检测并自动形成防护,产品必须能够防御应用层攻击、SQL Injection 及

	Cross-site 跨网站程序代码改写的攻击。
	产品必须提供包含攻击来源、攻击时间及试图利用什么方式进行攻击等必要信息，并在事件发生时，立即自动通知管理员。
	产品可以通过在整个虚拟环境中安装单一拷贝来达到保护所有虚拟环境中 Guest OS 和应用的功能。
	产品必须和虚拟化环境的 WMotion，Storage VMotion 以及 HA 集成，能够自动感知和保护虚拟环境的变更和迁移。
	产品支持完整性监控，能够监控操作系统和关键应用包括注册表项、关键目录、特定目录变更，以防范恶意修改
	产品支持对主机的日志审计，包括收集和分析操作系统和应用程序日志中的安全事件 ；协助遵循规范(PCI DSS 10.6) 优化识别埋在多个日志项下的重要安全事件； 将事件转至 SIEM 系统或中央日志服务器，做关联性分析、报告和归档；侦测可疑行为、收集数据中心的安全事件和管理操作，并使用 OSSEC 语法来建立高级规则；投标时现场提供原厂截图加盖公章
	产品必须具有集中控管的功能，能够统一的管理和配置，并且日志能够统一的在集中控管平台上呈现；投标时现场提供原厂截图加盖公章
操作系统支持	Microsoft Windows 2000 (32 位) ， XP (32 /64 位) ，Vista (32/64 位) ，Windows 7；Windows Server 2003 (32/64 位)，Windows Server 2008 (32/64 位) ，主流各类 linux 和 UNIX 操作系统
虚拟化系统支持	支持基于 VMware6.0& 6.5 NSX 虚拟化平台底层的无代理安全防护功能，而非在每台虚拟机中部署安全软件实现防护功能
	今后可扩展支持华三，华为，微软， Citrix，等主流虚拟化平台的无代理安全防护。
	可以用有代理模式支持 Docker，Container

应用防护支持	产品必须可以保护以下类型数据库服务器，Oracle, MySQL, Microsoft SQL Server, Ingres。 产品必须可以保护以下类型邮件服务器，Microsoft Exchange Server, Merak, IBM Lotus Domino, Mdaemon, Ipswitch, Imail, MailEnable Professional。 产品必须可以保护以下类型文件服务器，Ipswitch, War FTP Daemon, Allied Telesis。 产品必须可以保护以下类型备份服务器，Computer Associates, Symantec, EMC。 产品必须可以保护以下类型存储服务器，Symantec, Veritas。
原厂资质和服务要求	厂商已通过 ISO 20K 的质量体系认证（投标时现场提供证明材料加盖公章）。 厂商具有 CMMI5 证书。（投标时现场提供证明材料加盖公章） 厂商具有国家安全工程类一级资质。（投标时现场提供证明材料加盖公章） 厂商可根据用户需求提供高级别的服务承诺，如大客户专署服务、主动式服务、快速响应服务、在线技术支持服务等，可提供 5×8 乃至 7×24 小时的专业防毒服务。
其他要求	投标商不得随意扩大所投产品的技术功能及性能，以官网公布的资料为准；技术偏离表需逐条应答，签订合同前需提供功能性测试。最终用户为：杭州市卫生信息中心，原厂三年质保服务。

2、虚拟化软件安全套件扩容

项目	招标参数要求
	本项目需要与用户现有虚拟化资源池无缝融合为一个整体虚拟化资源池，符合用户数据中心虚拟化应用建设要求，最终实现应用的灵活部署和资源的自由动态调配，为用户内部

总体要求	各类应用的使用提供资源保障。 投标人必须提供充分的证明，包括但不限于用户证明等材料，以表明所提供的网络虚拟化软件能够与用户现有的虚拟化资源池融合，必须包括 1、满足将用户已有虚拟化平台内现有生产服务器与本次新上线服务器进行不停机在线资源整合的需要； 2、满足扩容后整体虚拟化平台内已有业务系统的按需在线不停机迁移的需要，并实现扩容后整体虚拟化平台内业务无中断的软硬件维护需要； 3、在一个完整的界面内能够对新旧 2 个虚拟化资源池进行统一的监控和集中管理
	本次采购网络虚拟化软件高级版共 6 CPU 授权，要求是独立软件产品，原厂非 OEM 产品，非硬件厂商捆绑销售软件。
基本功能	从底层硬件分离网络并对网络基础架构应用虚拟化原则，能够在软件中重现整个网络连接环境，包括每个虚拟网络中的 L2、L3 和 L4－L7 网络服务。能够为 L2－L7 服务提供分布式逻辑体系结构，从而可以在部署虚拟机时以编程方式调配这些服务，并跟随虚拟机移动。
	支持内嵌于虚拟化平台软件(Hypervisor)的逻辑网络及安全构件，包含建立逻辑交换机 (Logical Switch)、逻辑路由器(Logical Router)、逻辑防火墙(Logical Firewall)等虚拟网络环境功能，各逻辑交换机、路由器、防火墙功能需分散至各虚拟化平台软件所在的服务器上执行。
	创建可按需分配、使用和重新调整其用途的灵活的网络容量池。
	在软件中部署相互之间完全隔离并与数据中心中的其他更改完全隔离的网络。
	在虚拟机启动时自动应用安全策略，在迁移虚拟机时移动安全策略，在取消调配虚拟机时删除安全策略
	可按需提供基于虚机的网络边界网关的网络边界网关(Edge

	Gateway)，为虚拟机提供路由器、防火墙、负载均衡器(Load-Balancer)、VPN 等网络功能，以及 NAT、DHCP 等网络服务。
	提供与网络封装覆盖(Overlay)的交换机制(VXLAN)，可支持在不限定网络设备品牌的基础上封装超过 5000 个逻辑交换机，且修改逻辑交换机时不需要对底层的实体网络进行设定的更改。方案内的 VXLAN 机制无需 3 层 Multicast 机制即可运转。
	路由器功能支持静态路由、OSPF/BGP 等动态路由协议。路由器可支持多路径传输机制 (Equal-Cost-Multi-Path) 。
	VPN 功能支持点到点的 L2VPN 或 IPSEC VPN 服务，也可以支持供终端使用的 SSL-VPN 技术。
	VPN 功能支持点对点的 L2 或 L3 VPN，也支持由终端设备连线的 SSL-VPN。
	VXLAN VTEP 支持多网卡的负载均衡机制，可基于 LACP、MAC 或 IP 作为分配条件。
	VXLAN VTEP 的控制平面支持组播和单播的复制功能。
	网络虚拟化平台可建立基于 VXLAN 的 L2 逻辑交换机及 L3 的逻辑路由器的功能。
	提供 VXLAN L2 交换机到 VLAN 的桥接功能。
	逻辑交换机需支持 IP 和 MAC 绑定机制。
	逻辑路由器需支持分布式的功能，由 vSphere 直接判断虚拟网络内三层东西向的端到端通信
	支持分布式防火墙的功能，由 vSphere 直接判断虚拟网络的在线访问能力。
	支持网络边界的软件功能，包含均衡均衡、NAT 等功能。
	支持 DHCP Server 功能
	提供 Web-Based GUI 界面管理网络虚拟化平台。
	可使用 Restful API 整合网络虚拟化平台。
	支持逻辑交换机与实体环境的逻辑网络 (VLAN) 间的桥接

	功能 (L2 Bridging)
防火墙功能	hypervisor 内嵌的分布式防火墙架构，防火墙功能支持采用虚拟化环境参数(Cluster / Logical Network / VM)，也可以动态的按照虚拟机的操作系统、名称 (OS Name / VM Name)等条件，作为防火墙规则来源端与目的端进行设定 。
	防火墙功能支持基于用户登录 AD 的身份组进行网络策略的设定，即可以支持基于身份的防火墙功能，基于身份的防火墙同时需要支持多会话功能，在同一个 VM 内可以为不同用户分配不同的应用或会话访问策略
	防火墙可设定规则将封包转送给第三方安全软件进行防病毒、入侵防护、网页检查等机制，延伸安全防火墙的功能。
	支持可视化的流量监控并可以自动推荐应用的防火墙策略，可以在图形界面下选择每个会话创建、修改和删除相关的防火墙安全策略
	支持 IP Spoofing guard 防止 IP 欺骗，同时支持 DHCP Snooping 和 ARP Snooping 功能
负载均衡	方案内逻辑负载均衡器可支持以下功能 • TCP / UDP / HTTP / HTTPS 等协议的负载均衡机制 • 会话保持 (Session Persistent) 机制 • 负载均衡机制支持 Round-Robin / IP Hash / Least Connection / URL 等方式进行 • 可以后端应用服务器进行健康检查(Health Check) • 可进行 SSL 负载的卸载(SSL Termination)
	可通过 Application Rules 进行灵活的负载均衡策略，如：根据 URL 内特定的字符进行屏蔽、特定的 URL 重定向特定的 VIP Pool、主 VIP Pool down 重定向到备份 VIP Pool 等，支持所有 HA-Proxy 所有的 application rules 和语法
容灾和双活功能	可以和 vSphere6.0 以上版本无缝集成，支持跨数据中心的容灾、双活或多活架构，构建跨数据中心跨 vCenter 资源池，跨 vCenter 数量要求至少 6 个或以上

	支持和数据中心底层网络网络的解耦合，主备数据中心可以采用任意物理厂商的硬件网络设备
	支持跨数据中心跨 vCenter 的 VXLAN 二层扩展,分布式路由，支持防火墙安全策略的统一配置管理，VM 跨数据中心迁移时需要保证安全策略不需要任何变更
	支持长距离的 Vxlan 扩展(roud trip 时延需要支持 150ms)，支持跨 VDS、跨 vCenter 的迁移
	和 VMware 的 SRM 结合，支持计算资源、网络资源的跨数据中心容灾，同时支持计算资源、网络资源的自动化切换
	支持基于特定虚拟机的端口限速，支持跨 VC 的 QOS 跟随，当虚拟机跨 vCenter 迁移到另外一个数据中心后，原来的基于虚拟机的限速功能仍然有效
	支持基于基于 Location 的出口路由策略，即根据数据中心的 Location ID，即不同数据中心的主机基于路由信息里面的 Location ID 决定出口路由
运维和故障诊断	控制通道的健康检查：提供控制器到服务器、网络虚拟化管理器到服务器之间的健康检查和状态的实时监控功能
	提供基于图形化界面的端到端路径跟踪功能，支持二层 Unicast、三层 Unicast、二层广播、二层组播等，同时可以图形化显示端到端路径。支持 TCP、UDP 和 ICMP，同时可以设置 TCP Flag
	支持图形化界面的灵活抓包功能，抓包位置可以根据需要灵活配置，抓包位置包括：主机的 vmnic、vmknic，VM 的 vnic,dvfilter、dvport 等。
	方案内支持包括 Port Mirror (RSPAN/ERSPAN)，Netflow/IPFIX 等网络流量监控功能，并可进行网络状态设定的备份和还原。
	所有网络、安全的功能及策略、配置由统一的控制器 (Controller) 集中控制 。控制器数量需支持 3 台或以上，且具备高可用机制，在单一控制器失效时仍可以维持系统的

	正常运作。 当所有控制器全部失败时，数据平面数据转发不受任何影响而且当此时如网络拓扑发生变化，VM 的通信必须仍然不受影响
管理功能	管理系统可提供标准的网页应用程序编程接口 (restful API)或可与现有的工作流系统 (vCenter Orchestrator)的自动化流程来供外部的云管理平台进行调用。管理者可使用内嵌虚拟化平台管理软件 (vCenter)的图形界面进行设定与管理，或通过云管理平台 (Cloud Management Platform)如 vRealize Automation 产品，自动化的进行虚拟网络与安全的部署。
	可以与流量可视化工具集成如 vRNI，支持全网流量的实时和历史监控，可以根据 VLAN/VXLAN、端口组、安全组、IP 地址等相关信息进行选择并查看，历史流量至少可以追溯到 30 天以上，可以根据流量推荐防火墙安全策略并支持策略的导出
	可与企业现有的 Log 审计分析系统(Log Insight)进行整合，并可以将各网络服务包含逻辑交换机、路由器、防火墙、边界网关的状态通过仪表板与图表方式来展现，并提供提供审计日志的搜索与分析功能。
质保	原厂质保三年

3、安全运维防护服务

（1）完成虚拟化防护系统扩容、虚拟化软件安全套件扩容后杭州市卫生数据中心所有虚拟化环境的实施、测试、演练，并完成定期巡检。

（2）根据杭州市卫健委、杭州市卫生信息中心要求对所有进行现场安全检查技术工作的现场人员支持。进行协助完成卫生系统的信息安全检查情况梳理、整改内容整理核实，协助完成日常安全制度建设、台账管理等情况，协助等级保护开展。

五、服务与培训要求

1、质量保证：

（1）投标产品必须是符合国家技术规范和质量标准的合格产品，满足采购人的使用需求，并具有可靠的售后服务体系，质量可靠、使用安全。

（2）投标人保证其提供的产品中所有预装和为本项目安装的软件均为具有合法版权或使用权的正版软件且无质量瑕疵；

（3） 在质保期内，如遇软件产品升级、改版，应免费提供更新、升级服务，中标商项目必须按照采购人要求完成所有点设备实施，并且在质保期内每一个月进行一次新增设备的实施。

2、要求投标人提供的服务不得低于标准服务，即与投标产品制造厂商通过网站等对外公布的有效服务标准相一致（投标人不得另行制作网页）。在标准服务基础上，投标人还应达到以下标准：

（1） 投标产品制造厂商应具有完善的服务保障体系（在最终供货地有直接设立或授权的售后服务机构，配备有足够的、有相应资质的专业技术人员）；供应商也应就投标货物的品质和服务对采购机构和采购人负责。

（2） 投标人应明确说明此次投标的服务策略，提供此次投标货物的服务计划（售后服务内容、等级、相关服务指标、售后服务组织机构及人员安排情况及其联络信息）。

（3） 在质保期内供应商必须为最终用户提供技术服务热线（7*24 小时），负责解答用户在设备使用中遇到的问题，并及时提出解决问题的建议和操作方法。技术服务热线支持应是中文服务。

（4） 在投标货物质保期内，供应商应提供不低于 7*24 小时的现场质保和技术支持服务，对故障即时响应，3 小时以内到现场，4 小时以内解决问题；不能当场修复的，必须采取提供备品、备件或备机等措施，以保证采购人的正常使用。如果逾期未作出响应，供应商应承担由于故障所造成的全部损失。

（5） 当投标货物发生非人为因素严重故障时，供应商应当免费在七日内将补充或者更换的货物运抵发生故障的货物所在地，由此产生的一切相关费用由供应商负担。

（6） 质保期内所有因更换或修理设备或部件而导致设备停止运行的时间应从其质保期内扣除。

（7） 供应商在质保期内安装的任何产品，必须是其投标产品制造厂商原产的或是经其认可的。

（8） 所有的替代零配件必须是新的未使用和未经修复的，除非最终用户提供书面许可，否则不可使用此范围外的其他（非新的）配件。

（9） 供应商必须为维修和技术支持所未能解决的问题和故障提供正式的升级方案。

（10）在质保期内，供应商有责任解决所提供的投标设备和软件系统的任何问题，在质保期满后，当需要时，供应商仍须对因投标设备本身的固有缺陷和瑕疵承担相应责任。

3、对产品服务要求的有效响应将被视为投标人对其所投标产品的服务承诺，如果中标，须将服务承诺列入合同的产品服务条款。

4、投标人须保证所提供硬件产品包括相关附件为相应硬件厂家原装正品，软件产品为相关厂家正版软件，符合国家有关规定。投标人须保证所提供产品具有合法的版权或使用权，本项目采购的产品，如在本项目范围内使用过程中出现版权或使用权纠纷，应由中标人负责，采购人不承担责任。

5、项目所涉及的设备及软件到货时，须提供原厂商的供货证明，注明供货对象为杭州市卫生信息中心，杭州市卫生信息中心是所有设备的最终用户。

六、技术服务要求

1、投标人应确保其技术建议以及所提供的产品的完整性、实用性，保证全部系统及时投入正常运行。否则若出现因投标人提供的设备不满足要求、不合理，或者其所提供的技术支持和服务不全面，而导致系统无法实现或不能完全实现的状况，投标人负全部责任。

2、如果产品在质保期内发生产品故障，投标人应及时予以响应（免费上门服务），否则采购人将自行采取必要的措施，由此产生风险和费用由投标人承担。保修期从采购人对产品验收合格之日起开始计算。

3、特别提示：如招标文件中遗漏了必须具备的设备、配件或服务，请投标人在投标文件中指出，并提出解决方案供采购人、采购机构参考；中标人有义务保证采购人系统的完整性，如项目实施过程中因缺少设备、配件或服务导致采购人系统无法正常运行，中标人须承诺免费提供。

七、验收要求

由招标人根据国家标准及招标文件要求进行验收

文档的提交应覆盖以下内容，电子文档是成果不可分割的部分。要求如下文档：

1、项目实施前：需求分析报告；施工方案、项目实施计划；

2、项目实施期间：项目实施工作单、故障诊断及排除记录、项目实施过程中衍生的其它相关资料；

3、项目实施后：系统试运行和自测报告、故障诊断与排除手册、工作总结报告；

4、培训期间：培训计划、用户使用手册、管理员使用手册；

八、服务标准

本项目需执行的国家相关标准、行业标准、地方标准或者其他标准、规范。

九、商务要求

1、报价要求：有关本项目建设所需的一切费用、税均计入报价。《开标一览表》是报价的唯一载体。招标代理机构将不接受有选择的报价。

2、本项目合同甲方为采购人，乙方为中标\成交供应商，合同款支付给乙方。

3、履约保证金：签订合同后3个工作日内，中标人须向招标人缴纳相当于合同总额5%的履约保证金。待项目验收后1年后，无质量、服务问题，由招标人向中标人退还。

4、合同款支付：

1、第一期付款：合同签订后 15 日内完成所有设备的到货；设备清点验货后 15 个工作日内完成安装调试、系统集成，初验合格后进入试运行；并出具初步验收报告后 10 个工作日内，中标人凭招标人签字盖章的支付通知书、初验报告向甲方办理合同总额 40%的货款结算手续。

2、第二期付款：系统投入试运行，培训、系统正常运转 1 个月后，提交全部报告材料，并通过最终验收，出具项目终验报告后。中标人凭招标人签字盖章的支付通知书、发票复印件、终验报告向甲方办理合同总额 60%的货款结算手续。

5、质量保证金：无。

6、采购人拟定了采购合同，见采购文件的“第四章 采购合同”，供应商应对合同内容进行审核，如有偏离，请在响应文件的。“偏离表”中反映。

十、落实政府采购政策

1、本项目对符合财政扶持政策的中小企业（小型、微型）、监狱企业、残疾人福利性单位给予价格优惠扶持，价格优惠扶持见《第三章 评分办法》。

2、满足转发财政部 工业和信息化部关于印发《政府采购促进中小企业发展暂行办法》的通知（浙财采监[2012]11 号）的规定的中小企业可享受优惠扶持。

满足关于政府采购支持监狱企业发展有关问题的通知（财库[2014]68 号）的规定的供应商可享受优惠扶持。

满足关于促进残疾人就业政府采购政策的通知（财库[2017]141 号）的规定的供应商可享受优惠扶持。

3、节能产品、环境标志产品的强制采购政策

根据财政部、国家发展和改革委员会、生态环境部等部门公布的政府采购节能产品、环境标志产品品目清单的规定，依据品目清单和认证证书实施政府优先采购和强制采购。

采购人拟采购的产品属于品目清单范围内的强制采购品目的，供应商提供的产品应具有国家确定的认证机构出具的、处于有效期之内的节能产品、环境标志产品认证证书，并在响应文件中提供该产品节能产品、环境标志产品认证证书，否则无效。（注：本项目执行最新政府采购节能产品、环境标志产品品目清单。）

4、节能产品、环境标志产品的优先采购政策

根据财政部、国家发展和改革委员会、生态环境部等部门公布的政府采购节能产品、环境标志产品品目清单的规定、依据品目清单和认证证书实施政府优先采购和强制采购。采购人拟采购的产品属于品目清单范围内的优先采购品目的，供应商提供的产品应具有国家确定的认证机构出具的、处于有效期之内的节能产品、环境标志产品认证证书，并在响应文件中提供该产品节能产品、环境标志产品认证证书。（注：本项目执行最新政府采购节能产品、环境标志产品品目清单。）

采购文件中所有带▲的内容是采购人提出的实质性条款，响应文件若出现负偏差，将被评审小组认定为无效。