**一、项目名称**

上海交通大学医学院附属新华医院内网核心防火墙及安全设备采购项目

**二、项目参数:**

**（一）项目内容及要求**

1. 服务要求

1、服务期限：合同签订后45天。

2、服务地址：上海市杨浦区控江路1665号

1. 项目技术需求

**一、项目名称**

上海交通大学医学院附属新华医院内网核心防火墙及安全设备采购项目

**二、项目参数**

（一）项目概述

本次采购目标是为了加强核心网络的安全防护能力及新型威胁的发现能力，旨在：

1. 强化核心与边界的防护：通过部署核心防火墙设备，加强网络边界的访问控制，有效阻止非法访问和潜在威胁。
2. 未知威胁检测：通过部署蜜罐设备，增强对已知、未知威胁的检测能力，同时，蜜罐也可做为本地威胁情报源。
3. 持续安全运营：通过MSS系统服务，全天候、全方位对网络安全进行监测运营，提升安全事件处置能力和处置效率。

（二）设备清单

|  |  |  |
| --- | --- | --- |
| 序号 | 采购内容 | 数量 |
| 1 | 核心防火墙（核心产品） | 2台 |
| 2 | MSS系统（安全运营托管服务） | ≥50个点授权 |
| 3 | 蜜罐 | 1台 |

注：需与现有防火墙做资源、策略同步，保障业务连续性。

（三）技术参数

1. 核心防火墙
	1. ▲专有硬件平台：国产品牌，采用机框式模块化分布式硬件架构设计，要求主控模块、安全业务模块相互分离的机框式设备，基于高性能硬件平台和专业安全操作系统。（提供厂商官方网站证明截图及链接并加盖原厂公章）
	2. 本次设备需每台配置不少于2块系统主控模块，支持电源、风扇冗余，整机前后通风，所有模块需支持热插拔。
	3. 设备接口及存储要求：要求单台设备配置万兆接口≥32个，100GE接口（100G和40G速率可切换）≥4个，此外，具备至少一个业务接口板卡的扩展槽位。提供≥1T SSD硬盘。
	4. ▲硬件及性能要求：本次配置设备尺寸≤3U标准[机柜](https://zhida.zhihu.com/search?content_id=229152733&content_type=Article&match_order=1&q=42U%E6%9C%BA%E6%9F%9C&zd_token=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc3MiOiJ6aGlkYV9zZXJ2ZXIiLCJleHAiOjE3NDI5MTUwNjksInEiOiI0MlXmnLrmn5wiLCJ6aGlkYV9zb3VyY2UiOiJlbnRpdHkiLCJjb250ZW50X2lkIjoyMjkxNTI3MzMsImNvbnRlbnRfdHlwZSI6IkFydGljbGUiLCJtYXRjaF9vcmRlciI6MSwiemRfdG9rZW4iOm51bGx9.FlvF6K3DVsniPr3uHQA-DFAeoq8FNBMIHAkyW6xMKg8&zhida_source=entity)，吞吐量≥300Gbps，最大并发会话数≥9000万，每秒新建(HTTP)连接数≥130万，IPS吞吐量≥130Gbps，AV吞吐量≥80Gbps。（提供相关证明材料加盖原厂公章）
	5. VPN功能：支持IPsec VPN，IPsec VPN无需额外授权，IPSec VPN隧道数≥10000条，要求设备IPSEC VPN功能支持自定义协议端口，保障VPN正常使用。
	6. ▲零信任功能：产品具备零信任VPN功能，零信任访问具备单独的策略界面，可根据不同标签类型进行资源授权。（提供相关证明材料加盖原厂公章）
	7. 基本功能
		1. 支持DHCPv6，静态路由、策略路由、RIPng、OSPFv3等IPv6协议
		2. 支持隧道、DNS64/NAT64等多种过渡技术。
	8. NAT功能：源NAT/目的NAT支持策略命中数分析功能，支持显示NAT策略创建时间、命中数、首次命中时间、最近一次命中时间、未命中天数等信息，并可针对分析结果，对NAT策略进行删除或禁用。
	9. 支持SSL代理功能，至少能够解密HTTPS、POP3S、SMTPS、IAMPS协议流量。
	10. 策略运维
		1. 安全策略支持命中数分析功能，支持显示策略创建时间、命中数、首次命中时间、最近一次命中时间、未命中天数等信息，并可针对分析结果，对策略进行删除或禁用，支持策略冗余性检查功能。便于管理员维护防火墙策略
		2. ▲支持图形化的策略助手功能，能够提取命中指定策略ID的流量作为流量数据分析源，并根据用户设置的聚合规则聚合数据流量列表，最后自动生成符合用户期望的安全策略规则（提供第三方检测报告截图加盖原厂公章）
	11. ▲AI智能运维：支持智能运维助手功能，管理员可通过设备webUI界面的运维助手实现知识问答，设备配置咨询，IP威胁情报查询等能力，且上述能力在同一个对话框即可实现，无需切换不同页面（提供产品功能界面截图加盖原厂公章）
	12. ★质量保证期：≥3年硬件原厂维修服务及特征库三年更新升级服务，及需提供原厂出具的售后服务承诺函。（格式自拟）
	13. ★投标人需提供核心防火墙的原厂授权书（格式自拟）
2. MSS系统
	1. 授权服务内资产数≥50个
	2. 首次安全评估：提供暴露面梳理，投标人应使用安全工具对招标人服务资产开展互联网暴露面探测，以梳理资产面向互联网的开放情况，快速发现违规暴露在互联网中的资产及存在的风险并进行处置，实现对暴露面资产可管可控，降低暴露面资产的风险。投标人应具备互联网暴露面梳理的服务工具，该工具应当支持全资产和精确资产两种模式暴露资产收集模式，收集到的暴露面信息至少包括域名、域名标题、IP地址、开放端口、资产指纹、网站截图、移动端暴露面，并且能采集对应暴露资产的访问截图向招标人举证，及对应暴露资产存在的漏洞
	3. 脆弱性管理
		1. 高危可利用漏洞防护：针对服务范围内资产扫描到的高危可利用漏洞，投标人应当为招标人做好每一个高危可利用漏洞的防护工作，包括但不限于为招标人提供漏洞修复方案和安全设备防护策略，以及帮助招标人配置防护规则，保证招标人不因此出现重大事件和损失；
		2. 提供服务平台具备高危可利用漏洞防护规则的证明，并且支持对扫描到的高危可利用漏洞能够自动匹配漏洞防护规则
	4. 威胁管理
		1. 7\*24小时威胁鉴定：投标人应当具备云端检测和分析平台，通过采集招标人安全设备和工具的安全告警和安全日志，结合大数据分析、人工智能等技术手段，为招标人提供7\*24小时持续不间断的安全威胁分析鉴定，同时在用户界面进行展示；
		2. 受影响资产排查与加固：安全专家应当结合威胁情报主动排查是否对服务资产造成影响并通知用户，及时协助进行安全加固。
		3. 安全策略检查：投标人的安全专家每月对招标人的安全设备的防护策略进行检查，确保安全设备上的安全策略始终处于最优水平，针对威胁能起到最好的防护效果。投标人云端服务平台应当具备丰富的策略检查工具，支持排查安全设备防护策略配置的合理性。
	5. 网站监测
		1. 包含一个域名的网站监测服务
		2. 持续对网站主要页面进行监测，精准匹配敏感信息，发现网页敏感词事件第一时间通过微信服务群主动通知用户，同时监测内容自动记录在报告中
		3. 支持对目标站点的网页黑链篡改、网页挂马进行监测，发现后提供安全专家人工验证；
		4. 对目标站点进行实时篡改监测，首页每5分钟一次，全站每3天一次，一旦发现被篡改第一时间通过微信服务群进行告警
		5. 支持同时从内网及互联网侧自动化收集安全托管服务资产内的网站的对外暴露信息，包括但不限于：IP、域名、端口、指纹等。
		6. 支持对安全托管服务资产内的网站系统的服务器进行系统漏洞检测，包括：操作系统、网络设备、数据库等的漏洞扫描，支持选择紧急漏洞进行单独评估
		7. 自动持续对网站的可用性进行探测，网站的首页url保持每10分钟探测一次，及时发现断网故障，微信服务群主动告警通知
	6. 服务频率：7\*24小时持续专家服务，威胁发现及时响应
	7. ★Mss系统兼容性：支持对现有的态势感知系统、防火墙无缝联动（需提供承诺函，格式详见第五章中“12、★承诺函格式”）
	8. ★质量保证期：≥1年的系统维护更新升级服务，及需提供原厂出具的售后服务承诺函。（格式自拟）
	9. ★投标人需提供MSS系统的原厂授权书（格式自拟）
3. 蜜罐
	1. 操作系统：具有完全自主知识产权的专用安全操作系统，稳定可靠
	2. 知识产权：应为国产品牌，具备自主知识产权，所有配置界面、事件描述及手册均为中文；
	3. 硬件规格：标准2U机架式设备，全内置封闭式结构，CPU ≥8核心；内存≥32G；硬盘≥2T；≥6个千兆接口；冗余电源
	4. 系统架构
		1. 组件形态：每种组件都既支持软件安装包的方式部署在现有虚拟机上，也支持提供硬件的方式部署。
		2. 分离式部署：支持将诱捕节点、实体蜜罐、管理平台分别部署在不同的服务器上
	5. 诱捕端
		1. 节点覆盖面：支持覆盖≥10个网段的诱捕节点，每个网段≥1个具有独立IP的诱捕节点，支持扩充
		2. 伪装能力：通过页面配置可以动态变更诱捕节点上所暴露的端口及服务
		3. 捕获能力：支持诱捕节点捕获基于tcp, udp, icmp多种协议的探测和攻击
		4. 多节点能力：支持通过管理端web界面在一个诱捕主机上创建多个具有独立ip地址诱捕节点，并且为每个节点配置不同的开放端口和对应的蜜罐服务
		5. ipv6支持：支持捕获攻击者对诱捕节点ipv6地址的访问，同时界面上能展示攻击源的ipv6地址
		6. 攻击转移能力：支持将对诱捕节点开放端口的访问重定向到后端集中部署的实体蜜罐中
		7. 诱饵：支持撒放在真实主机上，并引向蜜罐的诱饵。诱饵撒放的系统支持windows和linux，每个系统至少各支持3种诱饵
		8. 模板配置：支持创建修改删除节点的情景模板，支持将情景模板应用于节点的端口开放策略，支持将诱捕节点的端口开放策略保存至情景模板
		9. 资源要求：支持将诱捕端程序安装在cpu 1核，内存256mb，磁盘10g的低配机器上
	6. 支持的蜜罐
		1. 支持ftp、samba、telent、ssh、rdp、rsync等多种系统服务类蜜罐
		2. 支持mysql、redis、mongodb等常用数据库蜜罐
		3. 支持4种及以上web类蜜罐
		4. 至少支持永恒之蓝网络攻击工具等漏洞蜜罐
	7. 蜜罐端
		1. 捕获能力：支持捕获所有流经蜜罐的流量包，提供下载功能；需要同时支持以天为单位，流经所有蜜罐的总流量包，以及以某个攻击源对某个蜜罐访问为维度的流量包，两种均需支持显示和下载
		2. 管理能力：支持批量创建蜜罐，单次创建多个不同种类的蜜罐
	8. 威胁溯源：支持获取内网某个攻击源所在主机的信息，包括并不限于ip地址，操作系统，开放的端口和服务等信息
	9. 管理需求
		1. 白名单管理：支持白名单功能，提供对源IP、目标IP、目标端口、协议，进行白名单配置管理
		2. 一键开关：支持一键开关，临时不开放所有诱捕节点对外的伪装服务
	10. ★质量保证期：≥3年硬件原厂维修服务及特征库三年更新升级服务，及需提供原厂出具的售后服务承诺函。（格式自拟）
	11. ★投标人需提供蜜罐的原厂授权书（格式自拟）

（四）安装及服务要求

1. 更换内网防火墙两台

现有内网防火墙已无法满足当前业务需求，处理能力和并发连接数存在瓶颈。本次更换为新一代防火墙，提高数据吞吐能力，增强威胁防御功能，并支持更精细的访问控制策略。

1. 新增虚拟防护诱捕系统

增加虚拟防护诱捕系统，通过模拟真实系统环境，引诱攻击者，并实时捕获其攻击手法和行为模式。提升医院的攻击检测能力，分析潜在威胁来源，并为安全策略优化提供数据支撑。

1. 搭建人工安全运营体系

构建医院专属的人工安全运营体系，包括建立安全监测与预警机制、优化日志分析与溯源能力、完善应急响应流程，并引入托管安全服务，通过人工+自动化的协同运营以提升整体安全管理水平。

1. 搭建人工安全运营体系，提升安全管理与响应能力

建立7×24小时安全监测机制，实时分析安全日志、识别异常行为，并通过托管安全服务增强整体安全管理能力。此外，还将完善医院信息安全事件的应急响应流程，提高对突发安全事件的处置能力，确保在安全威胁发生时能够快速发现、精准研判、高效处置。保障医院核心业务系统安全运行，提升医疗服务质量

1. 符合行业监管要求，提升医院网络安全合规性

严格遵循《网络安全法》《数据安全法》《医院网络安全防护指南》等相关政策法规。本项目通过优化安全架构、完善安全管理机制，确保医院的信息系统符合行业安全标准和法规要求，提高整体网络安全合规性，降低因安全漏洞导致的法律及监管风险。

（五）售后要求

（1）响应时间：7\*24小时电话及现场响应，包括法定节假日。

（2）非工作日，当系统出现严重故障，投标人按7\*24\*2小时响应服务，派工程师到现场响应服务。

（3）提供热线支持服务及远程故障诊断服务。

（4）提供≥3年备件支持服务。

（5）提供原厂备件及支持服务。

（6）技术咨询：使用中遇到操作、工作流程不清晰、系统维护等技术上问题时，提供咨询服务，技术人员将负责详细解答。

（7）软件版本升级：质保期内有新版本软件推出时，进行现有模块功能的版本升级。

1. 最高限价

人民币210万元

1. 资格条件

1、应为法人、其他组织或者自然人，具有独立承担民事责任的能力；法人的分支机构以自己的名义参与本项目采购活动时，应提供依法登记的相关证明文件和由法人出具的对本项目采购活动承担全部直接责任的授权书；自然人应提供身份证明文件；

2、参加采购活动前三年内，在经营活动中没有重大违法记录；

3、本次采购不接受联合体响应。

4、未被列入“信用中国”网站(www.creditchina.gov.cn)失信被执行人名单、重大税收违法失信主体和中国政府采购网(www.ccgp.gov.cn)政府采购严重违法失信行为记录名单的供应商。

五、付款方式

交货验收合格并开具正规发票后，招标方根据医院付款流程，支付合同款项100%。