# 福建省肿瘤医院

# 网络安全防火墙设备网超品牌论证公告

# 第一部分 须知前附表

|  |  |
| --- | --- |
| **序号** | **主　　　要　　　内　　　容** |
| 1 | 项目名称：网络安全防火墙设备 |
| 2 | 调研报名时间：2024年4月24日至4月30日 (节假日除外)8：00-12：00或14：00-17：00(北京时间）  调研会时间： 2024年5月15日 9:00 |
| 3 | 文件正本壹份,副本壹份胶装并密封加盖投标人公章。文件未胶装将视为无效。 |
| 4 | 文件递交处：福建省肿瘤医院网络技术中心 |
| 5 | 上述时间、地点如有变动，以单位届时通知为准。 |
| 6 | 采购报名、采购调研等采购过程中有任何异议，可联系我院监督科室。电话：83660063-8407；83660063-8467。 |

地　址： 福建省福州市福马路420号

福建省肿瘤医院科研楼四楼网络技术中心

邮　编：350014

报名联系电话：0591-83660063-8822

联系人：钱 工、金 工

第二部分 具体要求

**一、采购内容**

|  |  |  |  |
| --- | --- | --- | --- |
| **合同包** | **名称** | **数量** | **预算（万元）** |
| **（一）** | 网络安全防火墙设备 | 1项 | 80 |

**二、技术及服务要求**

（一）合同包（一）

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **项目** | **数量** | **技术参数要求** |
| 1 | 内网万兆防火墙 | 2台 | 1.2U标准机架式设备，模块化设计；标配≥2个千兆电口，≥4个SFP+万兆接口，≥3个网络模块扩展槽，≥2个USB口，≥1个控制口，≥16G内存、≥128G SSD、≥4T企业级硬盘，冗余电源；整机最大网络吞吐≥30Gbps，最大并发连接数≥500万，每秒新建连接数≥8万，全威胁处理吞吐≥4Gbps；支持入侵防护及病毒防护功能;  2.支持IPv4和IPv6双栈，具有独立的IPv6路由、IPv6对象、IPv6安全策略配置；支持IPv6 over IPv4、IPv6 TO IPv4遂道,支持6TO6地址转换；  3.支持多ISP线路接入，支持链路主备切换和自动负载均衡，支持ARPing、Ping、HTTPing等多种方法进行链路状态检测；用户认证支持Web认证、客户端认证，支持本地和LDAP、RADIUS等第三方认证，支持用户自助注册；  4.内置威胁情报库，包含恶意域名、恶意IP等情报信息，可高效识别威胁；内置全球IP地域库,可根据地域库对来自或访问特定地域的IP进行控制，支持地域取反操作；  5.支持黑名单机制，可快速添加或导入恶意IP、域名，进行永久或临时封锁；  6.支持单用户和多用户的最大带宽限制、最大新建会话限制、最大并发会话限制；支持基于用户、地址、服务、应用的流量控制，支持保证带宽、三级弹性带宽控制；  7.基于连接状态检测机制，可根据客户端、服务端、网络服务等条件统计分析当前连链接状态；支持分别对IPV4、IPV6的连接进行统计分析。  8.提供三年IPS、AV、应用识别特征库升级服务；三年硬件质保。  9.支持与我院现有态势感知平台实现联动处置，形成自动封堵策略，提升网络安全协同防御水平；（提供承诺函，并承担定制接口所需费用） |
| 2 | 内网无线防火墙 | 2台 | 1.2U标准机架式设备，标配≥1个管理口、≥1个IPMI接口、≥16个千兆电口、≥6个SFP+接口、支持≥4对bypass；≥2个扩展槽，≥2个USB口，≥1个控制口，≥16G内存、≥64G SSD、≥4T企业级硬盘，冗余电源；含三年IPS、AV、应用识别特征库升级服务、三年质保。  2.支持IPv4和IPv6双栈，具有独立的IPv6路由、IPv6对象、IPv6安全策略配置；支持IPv6 over IPv4、IPv6 TO IPv4遂道,支持6TO6地址转换；  3.支持多ISP线路接入，支持链路主备切换和自动负载均衡，支持ARPing、Ping、HTTPing等多种方法进行链路状态检测；用户认证支持Web认证、客户端认证，支持本地和LDAP、RADIUS等第三方认证，支持用户自助注册；  4.内置威胁情报库，包含恶意域名、恶意IP等情报信息，可高效识别威胁；内置全球IP地域库,可根据地域库对来自或访问特定地域的IP进行控制，支持地域取反操作；  5.支持黑名单机制，可快速添加或导入恶意IP、域名，进行永久或临时封锁；  6.支持单用户和多用户的最大带宽限制、最大新建会话限制、最大并发会话限制；支持基于用户、地址、服务、应用的流量控制，支持保证带宽、三级弹性带宽控制；  7.基于连接状态检测机制，可根据客户端、服务端、网络服务等条件统计分析当前连链接状态；支持分别对IPV4、IPV6的连接进行统计分析。  8.提供三年IPS、AV、应用识别特征库升级服务；三年硬件质保。  9.支持与我院现有态势感知平台实现联动处置，形成自动封堵策略，提升网络安全协同防御水平；（提供承诺函，并承担定制接口所需费用） |

1. **其他要求**

1、本项目为交钥匙工程，设备安装、系统集成、软件客户化均由乙方负责。提供各设备上架调试、系统集成等软硬件安装安装工作，同时结合医院现有设备及应用情况，实施现有及本项目规划、等保安全、系统集成、数据迁移、协助完成医院评审工作包括但不限于三级等保评审、电子病历评审、互联互通评审等各项工作。

2、本项目系统需符合《信息安全技术网络安全等级保护基本要求》GB/T22239-2019（三级）要求（下文简称：三级等保2.0），并在三级等保2.0评审中协助完成本系统评审工作。在我院网络安全应急、攻防保障中，需提供技术驻点服务，次数不限。

3.为保证对接兼容性，供应商须承诺本次采购的防火墙支持与医院内网部署的安全感知与运营管理平台无缝对接、配合，实现网络安全运维自动告警、阻断，提升安全防护能力和抗攻击水平，并承担定制接口所需费用；若涉及需对医院现有系统平台进行改造的，经采购人同意后，由成交人负责，因此产生的费用由成交人自行承担。成交后均按响应承诺执行，否则按虚假应标处理(供应商仅在响应表中体现此项要求或未按要求提供承诺函的均按未提供处理)；

4.为保证对接兼容性，供应商须承诺本次采购的内网万兆防火墙支持与医院现有的内网核心防火墙无缝对接，实现高效、安全、可靠的安全配置导入导出功能，确保防火墙安全配置能够顺利迁移或恢复。成交后均按响应承诺执行，否则按虚假应标处理(供应商仅在响应表中体现此项要求或未按要求提供承诺函的均按未提供处理)；

5.为了方便管理和维护，提升运维管理工作效率，供应商须承诺防火墙厂商具有集中管理软件，可支持对本次部署的防火墙、医院现有的医保接入防火墙、政务外网接入防火墙等进行安全策略统一下发、集中管理，版本及特征库统一升级，状态集中监控；成交后均按响应承诺执行，否则按虚假应标处理(供应商仅在响应表中体现此项要求或未按要求提供承诺函的均按未提供处理)；

6.本项目涉及的安全设备安装调试并经验收合格后，应对采购方的相关人员提供关于系统应用时技术和操作方面的培训。相关培训费用应包含在投标总价中。

1. **调研说明**

报名参加本次调研的供应商、厂家需提供如下相关资料。

1、报名请携带加盖公章的项目文件回执单、营业执照复印件、公司简介。

2、参与项目调研供应商代表的个人授权函（需加盖供应商公章）和身份证复印件。

3、分别提供“信用中国”网站（www.creditchina.gov.cn）、“中国政府采购网”网站（http://www.ccgp.gov.cn/search/cr/）信用记录查询截图，无不良记录并加盖公章（截图查询日期必须在该公告日期内）。

4、提供业绩清单及近3年省内同类项目中标书；

5、本调研会的报价仅做为本项目公开招标的预算限价；不做参与投标的限制条件；

6、上述各参数将做为本项目招标的主要参数，不代表本项目公开招标的最终参数；

7、参加调研会的公司应准备PPT材料（含方案介绍、安全能力、应用案例、报价等）、技术参数等材料，每公司讲解时间30分钟（含答疑10分钟）；同时上述材料须交予院方留档（提供U盘留档）。

**项目文件回执单**

请有意向参与的公司在项目公示期内携带回执单至福建省肿瘤医院网络技术中心报名。

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 项目名称 | 数量 | 品牌及型号 |
| 1 |  |  |  |
| 2 |  |  |  |

公司名称：

联系人：

联系电话：

公司盖章：

福建省肿瘤医院

年 月 日