**防火墙采购****需求**

**—、项目需求预（概）算**

采购项目：防火墙采购

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 序号 | 项目类别 | 采购项目名称 | 数量 | 是否进口 | 预算金额（元） |
| 1 | 通用设备 | 防火墙  硬件参数：标准1U机架式设备，双冗余电源，≥8个GE千兆电口，≥8个SFP千兆光口，≥2个SFP+万兆光口，≥2个USB3.0接口，≥1个CON口，≥1个MGT口；  性能参数：吞吐量≥16Gbps、并发连接数≥250万，IPS吞吐量≥10Gbps，AV吞吐量≥6.5Gbps，IPSEC隧道数≥6000，SSL VPN用户数最大4000；  功能参数：标配防火墙、攻击防护、智能DNS解析、链路负载均衡、服务器负载均衡、IPSEC及SSL VPN功能，支持Android、iOS等移动设备通过VPN安全接入，可扩展防病毒、入侵防御、流量管理、URL过滤功能模块。  本次配置三年原厂硬件保修、IPS特征库、AV特征库、Ti（威胁情报）特征库、应用特征库升级、软件升级维护服务。成交后须提供原厂三年售后服务承诺函。 | 1台 | 否 | 96500 |

说明：项目类别分为医用设备、通用设备、工程、服务、维修、维保、耗材。

是否为专项资金：

是□ 金额（元）：财政专项资金 元 否☑

是否为进口产品：是□ 否☑

是否面向中小企业：是☑ 否□

**二、项目需求概况：**

（一）、项目需求调查：（项目的必要性、可行性）

**1、项目背景：**随着医院信息化的发展，物理环境的规模不断扩大、设备数量激增。对于医院的业务系统来说，具备的功能也越来越多，交互方式也变得越来越复杂。医院目前的互联网出口路由器使用年限较长，现在该路由器自身存在一些问题：一方面设备的吞吐、新建等性能已无法满足现在的带宽需求，另一方面，对于应用识别、病毒过滤以及攻击防护的粒度上无法应对新业务等。互联网出口路由器直接与互联网连接，是我院互联网接入安全防护的第一道关卡，承载了全院互联网资源的接入及控制，同时也面临着来自互联网的的安全威胁，因此，我互联网接入边界对安全防护系统的稳定性、安全性、多功能提出了需求：

1、边界安全访问控制

在缺乏访问控制的前提下很容易受到非法和越权的访问，虽然大多数应用都实现了身份认证和授权访问的功能，但是这种控制只体现在应用层，有可能通过网络层或者传输层的流量监听或者劫持，获得上层的身份和口令信息，从而对业务系统进行非法及越权访问，破坏业务的正常运行，或非法获得相关秘密，造成泄露。

1. 应用识别

针对丰富的网络应用，传统的基于协议和端口的检测手段已不能满足网络安全建设的需求， 因此对网络出口应用识别和精准控制提出了新的挑战。

1. 多链路链路负载均衡

随着网络的发展，考虑的网络接入的高可靠性，多条链路接入成为必然。在多出口的情况下， 如何进行高效的链路负载，充分发挥高带宽，多冗余，高效率的访问，也是目前和将来需要考虑的问题。

1. 应用层安全检测

近年来网络攻击的多样性、复杂性逐步递增，这也就意味着安全设备具备入侵防御、病毒过滤和僵尸病毒检测等安全功能，能够及时地、有效地检测出正在发生的安全威胁，保障业务不受侵犯，安全运行。

**2、项目实施的必要性：**随着2017年6月1日《中华人民共和国网络安全法》和2019年12月1日《信息安全技术网络安全等级保护要求》的正式施行，对各单位关键信息基础设施保护提出了较高的要求。医院互联网在提供对外访问业务的同时却严重缺乏相应的安全机制和专业的安全防护设备，无法应对新型网络攻击行为，一旦遭受攻击，将带来极大的危害，一方面影响业务系统的稳定运行，另一方面甚至会导致医院核心业务数据的泄漏，所以目前需要对互联网出口进行安全防护。

**3、建设目标：**积极响应国家、卫健委的号召，符合国家政策和国家对网络信息安全建设的规定，通过依据等级保护 2.0 的建设，使我院网络满足《网络安全法》《网络安全等级保护条例》等要求，提升我院信息系统安全建设，为我院的后续发展提供系统安全保障。通过在互联网区域边界部署下一代防火墙设备实现对内部以及外部网络的应用层面的攻击防护和新型网络攻击行为，保障内部业务系统的安全，通过本次建设，可以改善我院DMZ区域的网络接入环境，提升了DMZ区域业务的服务质量，符合法律法规的要求规定，对数据中心内部相关应用做必要的安全措施，提供基本的安全保障。

（二）、技术要求：

1、需求配置清单

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 序号 | 产品名称 | 描述 | 数量 | 单位 | 备注 |
| 1 | 防火墙 | 硬件参数：标准1U机架式设备，双冗余电源，≥8个GE千兆电口，≥8个SFP千兆光口，≥2个SFP+万兆光口，≥2个USB3.0接口，≥1个CON口，≥1个MGT口；  性能参数：吞吐量≥16Gbps、并发连接数≥250万，IPS吞吐量≥10Gbps，AV吞吐量≥6.5Gbps，IPSEC隧道数≥6000，SSL VPN用户数最大4000；  功能参数：标配防火墙、攻击防护、智能DNS解析、链路负载均衡、服务器负载均衡、IPSEC及SSL VPN功能，支持Android、iOS等移动设备通过VPN安全接入，可扩展防病毒、入侵防御、流量管理、URL过滤功能模块。  本次配置三年原厂硬件保修、IPS特征库、AV特征库、Ti（威胁情报）特征库、应用特征库升级、软件升级维护服务。 | 1 | 台 |  |

2、功能及性能要求

|  |  |
| --- | --- |
| 参数名称 | 参数要求 |
| 基本要求 | 标准机架式设备，双冗余电源，≥8个GE千兆电口，≥8个SFP千兆光口，≥2个SFP+万兆光口，≥2个USB3.0接口，≥1个CON口，≥1个MGT口；本次须提供8个光转电模块和2个万兆光模块。 |
| 基本要求 | 吞吐量≥16Gbps、并发连接数≥250万，IPS吞吐量≥10Gbps，AV吞吐量≥6.5Gbps，IPSEC隧道数≥6000，SSL VPN用户数最大4000； |
| 其它要求 | 须提供中国网络安全审查技术与认证中心颁发的《网络关键设备和网络安全专用产品安全认证证书》，提供证书复印件并加盖原厂公章证明 |
| 基本要求 | 配置三年原厂硬件保修、IPS特征库、AV特征库、Ti（威胁情报）特征库、应用特征库升级、软件升级维护服务。验收时须提供原厂三年售后服务承诺函。 |
| 基本要求 | 须与现有防火墙实现热备双机冗余，保障网络高可用性，避免单点故障导致医院业务系统中断。 |
| 功能要求 | 支持针对HTTP、SMTP、IMAP、POP3、VOIP、NETBIOS等多种协议和应用的攻击检测和防御，提供多种特征的攻击检测和防御，特征库支持网络实时更新 |
| 功能要求 | 防火墙应支持IoT监控功能，通过分析流经设备的流量，识别网络中视频监控设备（如网络摄像机和NVR（网络硬盘录像机）），并对识别出的设备进行实时监控，根据自定义配置对出现非法行为的网络视频监控设备进行阻断等操作。 |
| 功能要求 | 为保证产品的多元化扩展能力，产品应支持容器化服务能力，支持第三方Docker镜像版本的导入和更新，支持第三方Docker运行信息查看，支持第三方Docker的停止、重启操作能力。 |

1. 、商务要求：

无

（四）、可能涉及的运行维护、升级更新、备品备件、耗材等后续采购情况

产品为成熟的硬件产品，本次要求提供三年原厂运行维护和升级更新服务，无其它硬件和耗材的采购。超过三年后的维护和更新需额外购买厂商服务。

（五）、付款方式

项目验收合格后，凭项目合同等额发票，30日内付合同款95%。

项目验收合格三年后，系统运行正常，收到保证金付款申请单后，30日内付合同款5%。