## 防火墙设备采购用户需求书

## 项目概况

信息安全技术网络安全等级保护评测要求GB/T 28448-2019(等级保护2.0)在网络架构、访问控制中明确提出，需要在重要网络区域与其他网络区域之间应采取可靠的技术隔离手段；目前我院的互联网出口防火墙设备老旧，存在高危漏洞，无法更新修复系统漏洞以及病毒特征库。本项目将根据国家网络安全法相关要求，结合我院互联网出口实际安全需求与业务发展特性，建立符合系统实际安全需求的边界防御系统，对本院互联网出口防火墙和民航院区出口防火墙进行更换，全面提升系统的安全保障能力和防护水平，确保系统的安全稳定运行，保障医院各项业务正常运营。

## 需求清单

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **内容** | **数量** | **维保期** |
| 1 | 防火墙设备 | 2台 | 硬件质保三年，包含 三年入侵防御、病毒库、应用识别库、特征库等三年更新授权。 |

## 功能参数

|  |  |
| --- | --- |
| 性能要求 | ▲多核AMP+架构，网络处理能力≥10G，应用层处理能力≥6G，并发连接≥260万，每秒新建连接≥18万/秒， 安全功能模块全开吞吐量≥3.4G。（提供产品彩页证明或官网链接截图证明） |
| 规格要求 | ▲不大于2U机箱，冗余电源，标准配置≥6个10/100/1000M自适应电口，≥4个SFP插槽（含4个SFP千兆光模块），≥两个扩展槽，≥1个Console口，支持液晶屏（提供产品彩页证明或官网链接截图证明） |
| 维保服务 | 提供三年硬件维保及软件升级服务 |
| 授权要求 | 含应用控制、URL过滤、病毒防护、入侵防御、威胁情报检测、IPSec VPN（≥25个并发隧道数）、SSL VPN（≥25个并发用户数）；具备3年全功能模块升级订阅服务包（威胁情报数据订阅服务、应用识别库、URL分类特征库、病毒防护特征库、入侵防御特征库升级服务） |
| 部署模式 | 产品支持路由、透明、交换以及混合模式接入，满足复杂应用环境的接入需求。支持旁路模式； |
| 网络协议 | 所投产品必须支持VTEP（VxLan Tunnel EndPoint）模式接入VxLAN网络，并可作为VXLAN二层、三层网关实现VxLan网络与传统以太网的相同子网内、跨子网间互联互通；支持通过绑定VLAN、VNI（VXLAN Network Identifier）、远程VTEP，手动管理VxLan网络；支持MAC、VNI、VTEP静态绑定（投标文件需要提供能够体现上述功能的截图）； |
| 所投产品必须支持MPLS流量透传；支持针对MPLS流量的安全审查，包括漏洞防护、反病毒、间谍软件防护、内容过滤、URL过滤、基于终端状态访问控制等安全防护功能；（投标文件需要提供能够体现上述功能及配置选项的截图） |
| 所投产品必须支持支持通过802.3ad协议、轮询、热备等方式将多个物理口绑定为一个逻辑接口，实现接口级的冗余，并可根据：源目的MAC组合、MAC和IP组合或TCP/UDP端口组合等方式实现负载和备份（投标文件需提供能够体现上述组合方式的配置选项截图） |
| 路由协议 | 所投产品必须支持支持静态路由、策略路由及动态路由。策略路由支持用户自定义其优先级，动态路由应至少支持RIP v1/v2/ng， OSPFv2/v3，BGP4/4+协议；必须支持静态和动态多播路由，动态多播路由必须支持PIM-SM（稀疏模式） |
| ▲所投产品必须支持基于策略的路由负载，支持根据应用和服务进行智能选路，支持源地址目的地址哈希、源地址哈希、轮询、时延负载、备份、随机、流量均衡、源地址轮询、目的地址哈希、最优链路带宽负载、最优链路带宽备份、跳数负载等不少于12种路由负载均衡方式，支持基于IPv4或IPv6的TCP、HTTP、DNS、ICMP等方式的链路探测，同时TCP与HTTP可使用自定义目标端口进行测试（投标文件需要提供能够体现上述功能及配置选项的截图） |
| 所投产品必须支持ISP路由负载均衡，最大可支持8条链路负载，支持自定义负载权重，支持基于优先级的ISP路由链路备份；支持基于IPv4或IPv6的TCP、HTTP、DNS、ICMP等方式的链路探测，同时TCP与HTTP可使用自定义目标端口进行测试 |
| 访问控制 | 所投产品必须支持基于源安全域、目的安全域、源用户、源地址、源地区、目的地址、目的地区、服务、应用、隧道、时间、VLAN等多种方式进行访问控制，并支持地理区域对象的导入以及重复策略的检查 |
| 所投产品比如支持基于IPv4/v6地址、应用的会话限制，限制动作包每IP新建、每IP并发、所有IP新建、所有IP并发，且可以基于安全域指定限制方向 |
| 应用识别与控制 | 所投产品必须支持应用识别，应用特征库包含的应用数量（非应用协议的规则总数）大于2800种，可深度识别每种应用的属性，为每种应用提供预定义的风险系数，并将应用基于类型、使用场景、数据传输、风险等级等特征分类（投标文件需要提供能够体现上述功能及配置选项的截图） |
| 所投产品可直观展示不同风险等级的应用在1天（24小时）或一周（7天）内传输流量的绝对数值及占全网流量的百分比。 |
| 网络攻击防护 | ▲所投产品必须支持基于不同安全区域防御SYN Flood、UDP Flood、ICMP Flood、IP Flood、DNS Flood、HTTP Flood攻击，并支持警告、丢弃、普通防护（首包丢弃）、增强防护（TC反弹技术）、授权服务器防护（NS重定向）、普通防护（自动重定向）、增强防护（手工确认）等多种防护措施（投标文件需要提供能够体现上述功能及配置选项的截图） |
| 所投产品必须支持可配置阈值的基于安全域或基于二层接口局域网广播防护，防止局域网内广播和多播数据包泛滥（投标文件需要提供能够体现上述功能及配置选项的截图） |
| 所投产品必须支持DHCP协议防护；支持手动定义可信DHCP服务器IPv4和基于阈值限制DHCP请求传输速率（投标文件需要提供能够体现上述功能及配置选项的截图） |
| 所投产品必须支持基于安全区域的异常包攻击防御，异常包攻击类型至少包括Ping of Death、Teardrop、IP选项、TCP异常、Smurf、Fraggle、Land、Winnuke、DNS异常、IP分片等；并可在设备页面显示每种攻击类型的丢包统计结果（投标文件需要提供能够体现上述攻击防护类型及丢包统计结果的截图） |
| 所投产品必须支持防御基于安全域的IP地址欺骗攻击，指定IP或网段必须从特定安全域流入 |
| 病毒防护 | 所投产品必须能够对HTTP/FTP/POP3/SMTP/IMAP/SMB六种协议进行病毒查杀；本地病毒库规模大于3000万 |
| 所投产品必须支持对最多6级的压缩文件进行解压查杀 |
| ▲所投产品必须支持基于MD5的自定义病毒签名；支持设置例外特征，对特定的病毒特征不进行查杀（投标文件需要提供能够体现上述功能及配置选项的截图） |
|
| 入侵防御 | 所投产品必须支持漏洞防护功能，同时将漏洞防护特征库分类，至少包括缓冲区溢出、跨站脚本、拒绝服务、恶意扫描、SQL注入、WEB攻击等六种分类；漏洞防护支持日志、阻断、放行、重置等执行动作,可批量设置针对某一分类或全部攻击签名的执行动作；支持基于FTP、HTTP、IMAP、OTHER\_APP、POP3、SMB、SMTP等应用协议的漏洞防护（投标文件需要提供能够体现漏洞防护特征库分类信息、支持的执行动作以及支持的应用协议的截图） |
| 所投产品必须支持在设备漏洞防护特征库直接查阅攻击的名称、CVEID、CNNVDID、CWEID、严重性、影响的平台、类型、描述、解决方案建议等详细信息；（投标文件需要提供能够在设备上显示以上内容详细信息的截图） |
| 所投产品必须支持自定义TCP、UDP、HTTP协议的漏洞特征，漏洞特征可通过多个字段以文本或正则表达式的形式进行有序和无序匹配，并可自定义漏洞的源、目的端口范围；同时可标识自定义漏洞的CVE编号或CNNVD编号。（投标文件需要提供能够体现上述功能及配置选项的截图） |
| 所投产品必须支持自定义基于TCP、UDP、HTTP协议的间谍软件特征。间谍软件特征可通过多个字段以文本或正则表达式的形式进行有序和无序匹配；并可自定义间谍软件的源、目的端口范围（投标文件需要提供能够体现上述功能及配置选项的截图） |
| 运维管理 | 所投产品必须支持双系统备份，且在系统切换中可实现配置的自动迁移；可记录不同时间点的历史配置文件。（投标文件需提供历史配置文件＞2个设备截图） |
| 所投产品必须支持将告警信息以SNMP Trap、邮件、声音、短信等形式通知管理员，告警信息的范围至少包括配置变更、病毒事件、攻击事件、异常事件、失陷主机告警、并发数告警、CPU利用率、内存利用率、硬盘利用率、接口带宽利用率、NAT端口池利用率等；（投标文件需要提供能够体现上述功能及配置选项的截图） |
| 所投产品必须提供可明文或加密方式调用的Restful API，并可指定Restful API使用的本地端口；为确保设备管理的安全性，所投产品必须支持限制特定主机调用Restful API（投标文件需要提供能够体现上述功能及配置选项的截图）支持定义第三方设备、平台通过调用Restful API 至少可配置所投设备的访问控制策略、源NAT策略、目的NAT策略、静态路由、高可用以及区域、地址、服务、时间、用户对象等功能（投标文件必须提供所投产品的Restful API使用说明并加盖公司公章） |
| 产品资质 | 所投产品具备《计算机软件著作权登记证书》 |
| 所投产品具备国家信息安全测评中心颁发的《信息技术产品安全测评证书》（EAL4+） |
| 所投产品具备公安部网络安全保卫局颁发的《计算机信息系统安全专用产品销售许可证》（增强级） |
| 具备《中国国家信息安全产品认证证书》（增强级） |
| 具备中国信息安全测评中心颁发的《国家信息安全漏洞库兼容性资质证书》 |
| 厂商资质 | 国家互联网应急中心颁发的网络安全应急服支撑单位证书（反网络诈骗领域） |
| 中国信息安全测评中心颁发的信息安全服务资质（云计算安全类）证书 |
| 中国信息协会颁发的信息化能力及信用评价证书（一级） |
| ITSS云计算服务能力（SAAS服务）标准符合性证书 |

## 项目工期要求

设备须在合同签订后15天内完成供货，试运行30天正常后，申请项目验收。

## 项目实施要求

1. 在系统验收通过前，须派驻不少于1名经验丰富的工程师现场驻点实施。
2. 实施过程应严格执行相关的规范，并保证安全。
3. 应在规定的时间内，保证质量，完成系统建设。
4. 实施过程中应科学、合理地掌握与其他工作的协调、交叉。

## 售后服务要求

1. 免费维保
	1. 从项目总体验收合格之日（从双方代表终验签字之日起计算）起，提供三年免费的设备维保服务。
	2. 维保期内须每季度需安排工程师实地对系统巡检一次，安排经验丰富的、任职一年以上的运维工程师提供巡检服务，并确保巡检驻点时间不低于1个工作日。
2. 技术服务

为确保为本设备稳定正常运行，需长期提供优良的技术支持，保修期间的维护服务不收取任何额外费用，保修期后的具体服务价格双方另行协商。

1. 系统维护与支持的具体内容如下：

（1）电话支持

对设备的运行、维护提供24小时的实时技术支持。以热线电话或Email、传真等方式随时回答用户各种技术问题并在48小时内提出解决方案。需提供7X24小时内的全天服务热线。

（2）远程技术支持

当系统出现故障，需提供7X24小时的远程技术服务。

（3）现场服务

当系统运行环境出现严重故障，或因更换服务器等原因需要重新搭建系统时，通过远程支持不能及时解决问题时，需要派技术支持人员赶赴现场，协助用户完成故障排除、升级或迁移操作，对系统进行完整性检查并跟踪运行。

（4）故障响应

7 x 24小时的实时故障响应。对于电话方式无法解决的问题或系统发生严重故障时，质保期内出现质量问题，需在接到通知后的2小时内给予响应，4小时内响应到场，48小时内完成维护（以上响应时间不含从出发到达甲方的路途时间），并承担维护的费用。

1. 定期跟踪

项目验收完毕后，需定期电话、现场跟踪系统使用情况，听取意见和建议，及时分析系统存在的问题，并随时给予解决。必要时，需派遣技术人员去现场解决存在的问题。

1. 系统升级

维保期间需每季度定期巡检服务，做到有问题早发现早解决。并及时向用户通报设备系统软件升级情况，若需要对系统软件升级，需提供升级版本和相应的支持服务。

1. 🟊系统安全

必须配合需求方对设备进行安全检测时发现的安全隐患进行限期修复，在等保测评中发现的系统漏洞、安全漏洞等做整改并安全加固。

## 验收要求

1. 验收标准：系统验收以招标文件的技术要求、中标人投标文件的项目需求说明、实施方案、技术方案为依据。
2. 在项目实施过程中，包括维护服务时期，服务商交付待安装设备或者变更，必须在系统管理人员的监督下才能进行用户现场实施。
3. 项目交付应在合同规定时间内，将采购范围内所界定的工作完成，并协助采购人制定相应管理规范，在通过双方认可验收后，交付给采购人，其中包括：符合项目目标和相应的技术要求、业务需求，并能保持设备稳定、运行良好。足以确保设备正常运行所需的管理、运营及维护有关的配套技术文件。
4. 项目验收时，设备入网上线完成后，正式进入30天试运行期，试运行结束后，由服务商和用户共同对设备进行验收。

## 其它要求

培训要求：

1、培训内容与课程要求

对设备的使用，操作，维护进行培训。培训时提供安装使用维护说明书，以确保需求方能够对系统有足够的了解和熟悉，能够独立进行系统的日常维护和管理。培训所需一切资料由服务商提供。

2、培训费用

培训过程中所发生的一切费用（含培训教材费）均包含在报价中。

3、本项目中全部含税费用均包含在报价中。