**潍坊市人民医院网络安全设备项目征集公告**

潍坊市人民医院根据《中华人民共和国政府采购法》等有关规定，对网络安全设备进行市场价格等调查征集，欢迎广大符合条件的供应商积极参与。

一、联系人：潍坊市人民医院物资采购办公室

二、联系电话：0536-8192593

三、参考要求详见附件。

四、供应商资质要求：1.提供医院现有核心安全设备厂商（防火墙、网闸、上网行为管理、核心网络交换机）出具技术服务能力证明函；2.为保障满足潍坊市卫健委的安全监管要求，支持将安全感知平台和潍坊市卫健委安全感知平台进行对接；提供设备厂商证明函并加盖公章。

五、征集方式：供应商将填写无误的附件报名表格（同时提交可编辑电子版一份），连同有效期内营业执照副本、税务登记证副本扫描后以邮件附件形式发送到潍坊市人民医院物资采购办公室邮箱wfrmgyszj@163.com,邮件主题为：项目名称+公司名称。

六、征集时间：2022年1月7日上午9点至1月11日下午3点（休息日除外）。

七、符合要求的供应商，邀请函免费发至预留的邮箱，如未收到，请务必自行电话联系物资采购办公室核实。

**备注：本次征集仅作为网络安全设备项目市场价格****等需求调查，不属于采购公开招标，望各供应商知悉。如有疑问，请拨打联系电话咨询。**

潍坊市人民医院物资采购办公室

 2022年1月6日

**附件：**

**一、项目实施要求**

本次采购为交钥匙工程，投标人必须承诺完整实现网络改造要求提出的技术要求，需要在技术方案中详细阐述方案优点与实施规划。若技术方案中存在严重隐患或者无法满足医院的征集要求，或实施过程中无法达到预期承诺，则甲方有权拒绝验收。投标人自行勘察现场，提供医院使用科室技术负责人出具的技术交流证明函。

相应设备应保证如期供货，设备提供商需协助医院完成所有设备的调试使用工作。项目实施单位应对本项目的重要性和售后服务应有充分的预估，投标人需提供技术支持服务，支持服务内容包括（1）需提供产品的使用培训（2）紧急救援服务。

**二、参考参数要求**

|  |  |  |  |
| --- | --- | --- | --- |
| 编号 | 类型 | 参考参数 | 数量 |
| 1 | VPN设备 | 1. 千兆电口≥6个，千兆光口≥4个，冗余电源， SSLVPN加密流量≥400Mbps，SSLVPN并发用户数≥6000，最大并发会话数≥160w；SSL VPN接入授权100套;
2. 支持IPv6/IPv4协议下的网关模式、单臂模式、双机模式、集群模式的部署；
3. 投标设备应为独立的专业VPN设备，采用标准SSL、TLS 协议，同时支持IPSec VPN、SSLVPN两种VPN，非插卡或防火墙带VPN模块设备。同时支持软件化交付；
4. 支持PC终端包括微软、苹果各个操作系统，并完整支持该操作系统下的各种IP层以上的B/S和C/S应用；
5. 支持文档WEB化管理，用户可通过任意浏览器，对存储服务器的文件进行管理操作（包括：上传、下载、删除、重命名、剪切、复制、粘贴、新建文件目录），而不需要额外安装FTP、文档共享软件等应用程序客户端；
6. 支持Syslog（系统日志）服务器，可将管理员日志，系统日志、用户日志输出到syslog服务器中；
7. 可支持虚拟门户功能，在一台设备上配置不同的访问域名、IP地址，以及不同的使用界面，实现一台设备为多个不同用户群体服务的的使用效果；
8. 产品应提供环境检测、自动修复工具，支持对Windows的环境兼容性一键检测能力，以及对检测结果进行一键修复的能力，避免由于用户操作系统环境存在问题影响SSL VPN的使用，减轻运维工作；
9. 产品应提供HTTPS驱动病毒查杀工具，支持对Windows环境下的针对HTTPS拦截监听的驱动病毒进行扫描查杀，避免因为HTTPS驱动病毒导致无法正常接入和使用SSL VPN；
10. 支持针对不同的web页面进行数据优化，支持动态压缩技术，基于数据流进行压缩，减少不必要的数据传输；
11. 针对B/S资源支持WebCache技术，动态缓存页面元素，提高Web页面响应速度。支持流缓存技术，实现网关与网关、网关与移动客户端之间进行多磁盘、双向、基于分片数据包的字节流缓存加速，削减冗余数据，降低带宽压力的同时提高访问速度；支持共享流缓存功能，实现多分支网关在总部共享流缓存数据，提高流缓存效果
12. 支持与本次征集要求符合的安全感知平台设备联动，同步用户信息，包括用户登录、登出、分配IP、访问资源记录的日志数据，实现远程接入用户与安全事件关联分析，定位异常用户（需提供截图证明并）
13. 供应商需承诺提供原厂现场安装及培训服务,提供原厂针对本项目的授权原件与三年售后服务承诺函。
 | 1台 |
| 2 | 上网行为管理 | 1. 网络层吞吐量≥10Gb，并发连接数≥600000，支持用户数≥6000，准入用户授权3000人；千兆电口≥6个，万兆光口≥2个，并配置≥2个万兆多模光模块， RJ45串口≥1个，支持BYPASS；内存≥8G，硬盘≥1TB；USB口≥2个，URL&应用识别规则库升级≥5年许可；
2. 部署模式：支持网关、网桥、旁路模式部署；网关模式，支持NAT、路由转发、DHCP、GRE、OSPF等功能，必须支持两台及两台以上设备同时做主机的部署模式；
3. 二维码认证：支持二维码认证，担保人扫描访客的二维码后对其网络访问授权；支持访客填写信息、担保人填写信息、免填写信息三种模式；
4. 用户自注册和自管理：密码登录支持用户自注册；支持用户信息自管理Web界面，终端用户可以自己修改当前账号的绑定手机、绑定邮箱、密码等信息；支持用户可查看和管理到当前账号的终端绑定关系；可限制新接入用户只能在某个IP段、MAC段范围内登录；
5. 终端安全合规检查：至少支持补丁检查、杀毒软件安装检查、操作系统检查、文件要求检查、注册表项检查、软件配置检查、进程检查七项；并且可设定检查不通过的终端不能接入网络，同时提醒终端客户即时进行修复；
6. 杀软检测：有插件能够检测杀软是否运行，版本号，支持20款杀毒软件检查，对于违规终端，至少支持禁止上网、提示用户、限制用户权限、违规修复等违规处理方式；无插件方式检测，无需终端安装准入插件，通过流量检查杀软是否运行，支持360安全卫士、金山毒霸、火绒安全、腾讯电脑管家、小红伞等多种杀软检查；
7. 非法外联检测与管控：至少支持拨号行为、双网卡行为、有4G网卡、有无线网卡行为、连接非法wifi行为、使用非法网关行为、连接外网行为、自定义外联行为8种外联方式的检查与管控；检测终端计算机到发生违规外联行为，可及时告警或上报，支持发送告警邮件、断网的违规处理配置；用户违规断网后，重启PC可恢复网络连接，支持U盘等外设管控；
8. Web访问质量监测：针对内网用户的web访问质量进行检测，对整体网络提供清晰的整体网络质量评级，支持以列表形式展示访问质量差的用户名单，支持对单用户进行定向web访问质量检测；
9. P2P智能流控：支持通过抑制P2P的上行流量，来减缓P2P的下行流量，从而解决网络出口在做流控后仍然压力较大的问题；；
10. 支持IP管理功能，管理员可以查看每个IP的详细使用情况，支持查看当前内网IP使用情况，帮助管理员减少人工维护IP表的工作量
11. 应用特征库：设备内置应用识别规则库，支持超过10000条应用规则数，支持超过6000种以上的应用，1000种以上移动应用，保证应用识别的准确率；
12. SSL加密内容审计和过滤：支持旁路部署，识别并过滤SSL加密的钓鱼网站、非法网站等，对加密HTTPS、POP3-SSL 、POP3、IMAP 、IMAP-SSL、SMTP-SSL、SMTP邮件内容的审计，能够基于关键字、发件人地址等识别和过滤使用邮件客户端外发SSL加密邮件的行为（需提供自主知识产权证明及相关功能截图证明）；
13. 能够对新浪微博、腾讯微博、网易微博等进行细分控制，如：登录、浏览、发微博、上传附件；.能够对teamview、QQ远程桌面等远程控制应用做细分控制，如：接受对方远程控制；能够对Github、百度网盘、百度文库等网络应用的上传动作进行细分控制（所有功能必须提供产品界面截图）；
14. 支持与本次符合征集要求的安全感知平台设备进行联动响应，同步认证用户关联安全事件；支持浏览器推送用户提醒与冻结用户上网；（需提供相关功能截图证明）；
15. 供应商需承诺提供原厂现场安装及培训服务,提供原厂针对本项目的授权原件与三年售后服务承诺函。
 | 1台 |
| 3 | 态势感知与探针 | 1. 标准机架式设备，系统盘≥240G SSD，硬盘≥32TB，千兆电口≥4个；串口≥1个，USB口≥3个，VGA接口≥1个，配置冗余电源，配置特征库软件5年许可;
2. 支持感知业务/服务器资产，可定义IP地址、所属分支、主机名、责任人、责任人邮箱、所属业务、操作系统、服务与端口等信息，并支持基于流量自动识别操作系统、开放的服务与端口。
3. 支持流量实时分析漏洞功能，漏洞分析类型包含配置错误漏洞、OpenSSH漏洞、OpenLDAP、数据库、Web应用等，页面上必须展示业务脆弱性风险分布、漏洞类型分析、漏洞态势与危害和处置建议，并支持导出脆弱性感知报告；
4. 支持基于攻击者和受害者的视角展示横向威胁态势，并可通过链接方式互相跳转并直接查询相关日志记录，包括数据包的详细内容查看；
5. 支持基于可视化的形式展示内部威胁的影响面，通过大数据分析和关联检索技术，直观展示失陷主机攻击链与被攻击链；
6. 平台具备独立邮件威胁模块，支持机器学习技术发现主机发送可疑附件的邮件行为、伪造发件人发送邮件、发送钓鱼网站邮件和垃圾邮件等行为，包含接收恶意邮件TOP5、恶意附件TOP5、危害和处置建议；支持对恶意邮件详情分析，包含收件人账号、恶意邮件数量、发件人账号、附件名称、病毒名称、恶意链接名称等，并支持导出分析结果；
7. 具备勒索病毒、挖矿专项检测，可实时查看挖矿各个攻击阶段，包括感染挖矿病毒、与控制端建立通信、获取挖矿任务、尝试挖矿、挖矿成功等；并支持挖矿币种分布、挖矿风险态势、受影响主机等维度分析统计；
8. 支持大屏轮播，支持不同视角展示全网安全态势，包括综合安全态势、分支安全态势、安全事件态势、网络攻击态势、外连风险态势、横向威胁态势、脆弱性态势、资产态势等态势，至少具备10种以上大屏（需提供大屏数量及轮播相关功能截图证明）；
9. 协助等级保护能力，支持对等级保护建设整改过程中系统定级、差距评估、备案、整改、测评过程中产生的文档结论进行统计归档，并使用可视化的统一界面进行展现与管理，最大程度发挥安全措施的保护能力；
10. 具备僵尸网络识别能力，支持基于威胁活动链的形式展现主机的安全状况，能够直观地展示主机正处于被黑客入侵的哪个阶段，是否已经被利用、以及威胁的程度，行为规则在30万条以上；
11. 支持接入防火墙、上网行为管理、终端EDR、WAC无线控制器、DAS数据库审计和潜伏威胁探针等设备,并支持在页面中显示安全组件接入的数量和状态；
12. 探针设备镜像流量处理能力≥3Gbps，千兆电口≥6个，万兆光口≥2个，并配置≥2个万兆多模光模块，USB接口≥2个，RJ45串口≥1个，特征库软件5年升级许可，标准机架式设备；
13. 为保障数据对接，探针设备必须与安全态势感知系统为同一品牌；
14. 探针设备能够识别应用类型超过1000种，应用识别规则总数超过2500条，具备亿万级别URL识别能力。漏洞利用规则特征库数量在3000条以上，漏洞利用特征具备中文相关介绍，包括但不限于漏洞描述，漏洞名称，危险等级，影响系统等，对应CVE编号；
15. 探针设备支持敏感数据泄密功能检测能力，支持敏感信息自定义，支持根据文件类型和敏感关键字进行信息过滤；
16. 探针设备可提供网络流量的会话级视图,根据网络流量的正常行为轮廓特征建立正常流量模型,判别流量是否出现异常,对原始流记录进行异常检测,可发现网络蠕虫、网络水平扫描、网络垂直扫描、IP地址扫描，端口扫描，ARP欺骗，IP协议异常报文检测和TCP协议异常报文等常见网络异常流量事件类型;
17. 探针设备支持对终端种植了远控木马或者病毒等恶意软件进行检测，并且能够对检测到的恶意软件行为进行深入的分析，展示和外部命令控制服务器的交互行为和其他可疑行为；
18. 支持与现有网络行为管理联动响应，快速定位终端用户，针对终端用户进行弹窗提醒；支持与防火墙进行联动响应，支持平台自动下发安全策略到防火墙上，阻断攻击流量；
19. 供应商需承诺提供原厂现场安装及培训服务,提供原厂针对本项目的授权原件与三年售后服务承诺函。
 | 1套 |
| 4 | WAF设备 | 1. 产品应采用1U专用机架式硬件设备，系统硬件为全内置封闭式结构,非NGFW、NGAF等下一代防火墙或UTM安全网关产品。6个千兆电口,2对千兆电口Bypass并配置≥2个千兆多模光模块。最大吞吐能力≥6000Mbps， 并发会话数≥220万,网络延迟≤ 0.1毫秒 可防护IP数量不限，≥5年特征库升级许可；
2. 透明部署（基于透明网桥），需即插即用，无需做任何配置即可防护。支持旁路部署。透明部署时，在VLAN Trunk链路下，支持2条以上链路的检测与防御，并支持https协议解码。策略路由（支持流量牵引）支持反向代理部署,支持透明代理部署。代理模式下，支持输入HTTP页面自动跳转到HTTPS页面。（提供界面截图，并加盖厂商公章）
3. 离线模式：设备后所有网站离线；基于IP的网站离线；基于域名的网站离线；可绑定设备厂家微信公众号实现设备快速离线操作；可通过扫描设备界面二维码进行快速离线的设备绑定
4. 高性能攻击特征检测引擎
5. 基于智能用户行为识别的动态防护机制，识别并彻底阻断黑客的攻击行为
6. 自动学习并构建网站的URL模型，禁止违反现有模型的尝试行为
7. 支持更新、修正现有URL模型
8. IPv6协议通过和防护
9. 支持IPV4到IPV6的协议转换
10. 支持透明模式、反向代理模式下的HTTPS协议防护，加载证书后由系统在本地完成HTTPS解密过滤再加密转发到服务器，无需服务器端做任何改动。
11. 支持非标准的443端口的HTTPS协议防护。
12. 支持解析通过代理服务器访问用户的真实IP地址，默认支持X-Real-IP或X-Forwarded-For字段的值作为真实来源IP地址，同时支持用户自定义字段名称。
13. 系统提供完善的内置规则，支持用户自定义防护策略集，针对不同的来源/目的IP，目的URL选择不用的策略集，提供高度灵活的自定义规则向导，适用于高级用户
14. 能够对SQL注入、CGI、跨站脚本（XSS）进行应用层漏洞扫描
15. 支持任意碎片组包，支持超长报文组包（默认30M）
16. ASCII编码的还原，Unicode编码的还原，各种混淆编码的还原
17. 蠕虫、缓冲区溢出、CGI信息扫描、目录遍历等WEB通用攻击防护
18. 支持对恶意扫描行为开启防扫描功能，用户可自定义防护等级。
19. SQL注入及XSS攻击防护，跨站请求伪造（CSRF）攻击防护，爬虫防护、恶意扫描防护、Cookie安全、服务器信息伪装/过滤、缓冲区溢出、HTTP请求类型过滤、Webshell行为拦截
20. 能够智能识别木马上传行为，支持自定义上传文件的大小、后缀名。用户可自定义对上传脚本文件的处理方式：直接拦截，智能识别。支持木马上传日志，记录上传时间，源地址，目的地址，目的URL，拦截原因。支持将木马文件直接下载至本地进行人工分析。
21. 以源网页镜像比对方式进行防篡改检测和恢复，而非视觉恢复。无需在服务器端安装代理软件，支持FTP/SFTP连接方式，支持文件、目录排除，支持设置检测优先级，支持多个防篡改用户。（提供截图并加盖原厂公章）
22. 支持对虚拟机中的任意数量网站进行防护，使多个虚拟机共用一个IP地址
23. 恶意代码过滤、支持敏感关键字过滤，用户可自定义关键字内容
24. 记录登陆过程中使用的弱密码
25. 检测网站的备案情况，对于通过备案网站放行，未通过备案禁止访问
26. 基于规则的ACL、来源IP的ACL、目的IP的ACL、目的URL的ACL、支持基于时间的计划任务
27. 丢弃数据包、阻断TCP连接、禁止恶意IP的后续访问
28. 来源IP攻击防护，Rerferer攻击防护，特定URL攻击防护，CC防护的访问控制（黑、白名单）
29. TCP/UDP Flood防护，基于最大上限阀值设置，而非DDOS特征库
30. 安全报表（入侵统计、按入侵类别统计、被攻击主机、攻击来源IP和地理位置、页面访问次数、网络接口流量趋势）
31. 报表提供对防护Web网站中已经存在Webshell文件的告警功能
32. 按事件类型、统计目标或周期类型条件进行统计
33. 支持将生成的报表以HTML、Word等通用格式输出
34. 获得国家保密局涉密信息系统安全保密测评中心颁发的《涉密信息系统产品检测证书》，并出具加盖厂商公章的复印件。
35. 获得中国信息安全认证中心颁发的符合ISCCC-IR-007:2011要求的《IT产品信息安全认证证书》，并出具加盖厂商公章的复印件
36. 产品获得OWASP（互联网安全研究中心开源Web安全应用项目组）颁发的《WEB应用防火墙认证证书》，并出具加盖厂商公章的复印件。
37. 获得公安部颁发的web应用防火墙产品（增强级）的《计算机信息系统安全专用产品销售许可证》，并出具加盖厂商公章的复印件

38.供应商需承诺提供原厂现场安装及培训服务,提供原厂针对本项目的授权原件与三年售后服务承诺函。 | 1台 |
| 5 | 防火墙 | 1. 2U标准机架式外观，产品采用X86架构；提供≥14个千兆网口、≥4个千兆光口，≥2个万兆光口，并配置2个万兆多模光模块；网络层吞吐量≥26Gbps，并发连接数≥800万；提供抗DDOS功能、入侵防御、异常行为检测、邮件防护功能；提供入侵防御特征库5年升级许可；
2. 支持路由、交换、虚拟线、Listening、混合工作模式；支持手动和LACP链路聚合，可根据源/目的mac、源/目的IP、源/目的端口、五元组、端口轮询等条件提供不少于10种链路负载算法。
3. 支持根据入接口、源/目的IP地址/地址对象、源/目的端口、协议、用户、应用、选路算法、探测、度量值、权重等多种条件设置策略路由；
4. 支持异常行为检测功能，通过统计智能学习算法，对特定地址对象建立监控策略，基于新建、并发、流量等数据进行比较判定和告警；（提供截图并加盖厂商公章）
5. 支持一体化安全策略配置，可以通过一条策略实现五元组信息源MAC、域名、地理区域、应用、服务、时间、长连接、并发会话、WEB认证、IPS、AV、URL过滤、WAF、邮件安全、数据过滤、文件过滤、审计、防代理、APT等功能配置,简化用户管理；支持策略的允许、禁止及认证动作，对符合条件的流量进行Web认证，在策略中可设置用户Web认证的门户地址；（提供截图并加盖厂商公章）
6. 支持访问控制策略的允许、禁止和认证动作选择；提供智能策略分析功能，支持策略命中分析、策略冗余分析、策略冲突检查；（提供截图并加盖厂商公章）
7. 支持IPv4/IPv6双栈工作模式；支持IPv4/v6双栈IP/MAC静态和动态探测绑定，支持跨三层绑定，支持IP/MAC绑定表导入导出；支持根据IPv6的目的/源地址、目的/源服务端口、区域、服务、时间、扩展头属性等条件设置安全访问规则；支持基于IPv6的病毒防御、入侵防御、URL过滤、ADS、WAF、流量控制、连接限制、文件过滤、数据过滤、邮件安全等；
8. 配置虚拟化防火墙功能，授权数不少于20个；支持配置文件、系统服务、路由、链路聚合、安全策略、NAT策略、带宽管理、认证策略、IPV6功能、URL过滤、病毒过滤、WAF、内容过滤、审计、报表、防代理等安全功能虚拟化；（提供截图并加盖厂商公章）
9. 支持针对IP、ICMP、TCP、UDP、DNS、HTTP、NTP等协议进行DDOS防护；包括但不限于：HTTPFlood、HTTP新建连接Flood、HTTP并发连接Flood、HTTPURICC等攻击检测，支持UDP关联认证，要求所有去往服务器的UDP报文，必须首先与该服务器的TCP端口建立TCP连接，对源地址进行合法性认证；支持静态白名单和动态黑名单功能。
10. 支持邮件安全防护功能，可进行匿名发件人、收发件人同名、非标客户端、收/发件人频率、收/发件IP频率、邮件长度、附件名称、附件数量检测，支持黑、白名单检测；（提供截图并加盖厂商公章）
11. 内置防代理功能，防止网络用户通过代理主机实现攻击、避免计费等行为；
12. 内置内容过滤功能，支持基于http、ftp、telnet、smtp、pop3等协议的内容过滤策略，可对FTP上传/下载的文件名进行过滤，同时支持过滤FTP信令：上传文件、下载文件、删除文件、重命名文件、创建目录、删除目录、列出目录等，邮件过滤支持对发件人、收件人、主题、内容、附件等进行过滤；（提供截图并加盖厂商公章）
13. 为保证外网病毒防护能力，要求防火墙能够与外网出口现有防病毒网关进行联动，根据防病毒网关的检测结果自动封禁问题终端和病毒URL的访问。
14. 供应商需承诺提供原厂现场安装及培训服务,提供原厂针对本项目的授权原件与三年售后服务承诺函。
 | 2台 |
| 6 | 网闸 | 1. 2U标准机架式设备，标配双电源；内外端机双侧液晶屏；采用‘2+1’隔离方式，内外端机之间采用专用硬件和专用协议进行连接，不可编程；内外端机各提供接口≥6个千兆网口，≥4个千兆接口，≥2个万兆接口，并配置≥2个万兆多模光模块，≥1个扩展槽位；网络吞吐量≥10Gbps；并发连接数≥100万。
2. 提供安全浏览模块、文件传输模块、文件同步模块、邮件访问模块、VOIP访问模块、数据库访问模块、数据库同步模块、自定义访问模块、数据中心模块。
3. 提供状态信息监控，以图表形式实时展现内外端机的CPU、内存、硬盘利用率、流量和会话数，提供在线用户监控，可实时展现内外端机在线用户名称、IP地址、认证服务器名称、客户端类型和在线时间信息，并可根据管理需要手动强制指定用户下线；
4. 提供有客户端和无客户端两种文件同步方式，无客户端方式无需在用户服务器上安装任何插件，网闸不开放任何服务端口；支持基于文件大小和文件修改时间的同步策略，可手动指定上下限阈值；支持文件名和文件类型的黑白名单过滤，文件类型过滤基于文件特征识别，非扩展名识别，且支持不小于50种文件类型识别；支持文件同步信息统计，包括每个任务的开始时间、同步数据量、同步成功数、同步失败数，并能够以图表的方式进行实时可视化展现。（提供截图并加盖厂商公章）
5. 提供数据库同步功能，提供多种主流数据库系统如：ORACLE、SQLSERVER、MYSQL、达梦数据库的同步；支持一对一、一对多、多对一方式的数据库同步；支持同构、异构数据库之间的同步，同步可具体设置到字段级别；支持自动读取数据库表名和字段名，无需手动录入表名和字段名，降低配置复杂度；支持数据库同步冲突策略处理，包括覆盖、忽略、以源为准、以目的为准等处理方式。（提供截图并加盖厂商公章）
6. 提供安全防护功能，提供连接保护，支持基于源和目的IP地址的并发连接数和新建连接数控制，并可以手动设置相关阈值，超过阈值后可选限制和警告两种处理方式；（提供截图并加盖厂商公章）
7. 管理端通过独立的管理口与网闸内端机相连，策略统一从内端机下发，不允许采用外端机上的任何网络接口进行管理；
8. 为保证运维的简便性，提供ping、traceroute、tcp、http、dns等诊断诊断测试工具，支持设备健康记录和调试信息的导出；
9. 提供安全邮件功能，支持访问控制日志记录和告警功能；支持最大活动会话数的控制和统计；支持IPV6扩展头的安全设置；支持发件人、收件人、邮件标题、邮件正文、邮件附件等数据内容过滤，支持允许、阻断、告警三种处理方式；
10. 为保障内外网隔离攻击防护能力，要求网闸能够与现有内网核心防火墙进行联动，根据核心防火墙提供攻击者的五元组进行自动封锁。

11.供应商需承诺提供原厂现场安装及培训服务,提供原厂针对本项目的授权原件与三年售后服务承诺函。 | 2台 |