**网络安全项目采购需求**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 序号 | 货物名称 | 数量单位 | 产品详细参数及技术要求 | 备注 | 单价 |
| 内网安全： |  |
|  | 新机房数据中心防火墙 | 1台 | 一、性能参数： 1.性能参数：网络层吞吐量≥40G，应用层吞吐量≥25G，防病毒吞吐量≥4G，IPS吞吐量≥3.5G，全威胁吞吐量≥2G，并发连接数≥400万，HTTP新建连接数≥19万。2.硬件参数：内存大小≥16G，硬盘容量≥256G SSD，电源：冗余电源，接口≥16千兆电口+6万兆光口SFP+（含光模块）。二、功能参数1、产品支持路由模式、透明模式、虚拟网线模式、旁路镜像模式等多种部署方式；支持链路健康检查功能，可基于多种协议对链路可用性进行探测；支持链路聚合功能，可以将多个物理链路组合成一个性能更高的逻辑链路接口；2、支持多链路出站负载，可基于源/目的IP、源/目的端口、协议、ISP、应用类型以及地域来进行选路的策略路由选路功能；3、产品支持IPv4/IPv6双栈工作模式，以适应IPv6发展趋势；支持IPv6访问控制策略设置，基于IPv6的IP地址、服务、域名、应用、时间等条件设置访问控制策略。 4、产品支持IPsec VPN和SSL VPN功能，为满足组网兼容性，IPSec VPN需支持IKEv1和IKEv2协议，可实现和第三方VPN的对接；5、IPSec VPN智能选路功能，根据线路质量实现线路自动切换；6、与现网内态势感知平台实现数据对接，防御联动。7、产品支持对不少于9000种应用的识别和控制，应用类型包括游戏、购物、图书百科、工作招聘、P2P下载、聊天工具、旅游出行、股票软件等类型应用进行检测与控制；8、产品支持基于IP对象的会话控制策略，实现并发连接数的合理限制；支持多维度安全策略设置，可基于时间、用户、应用、IP、域名等内容进行安全策略设置；9、支持DDoS防护策略，可对ICMP、UDP、DNS、SYN等协议进行DDOS防护；支持异常包攻击防御，异常包攻击类型至少包括Ping of Death、Teardrop、Smurf、Land、WinNuke等攻击类型；10、产品开启防病毒模块，支持对SMTP、HTTP、FTP、SMB、POP3、HTTPS、IMAP等协议进行病毒防御；11、产品支持对多重压缩文件的病毒检测能力，支持不小于12层压缩文件病毒检测与处置；12、产品支持入侵防御功能，预定义漏洞特征数量超过9000种；（提供产品界面截图）13、产品支持与现网态势感知平台联动，将本地防火墙产品产生的安全日志等数据上报至态势感知平台，并在态势感知平台进行威胁展示； 14、产品支持基于IMAP、FTP、RDP、VNC、SSH、TELNET、ORACLE、MYSQL、MSSQL等应用协议进行深度检测与防护；15、产品可扩展对常见Web应用攻击防御，攻击类型至少支持跨站脚本（XSS）攻击、SQL注入、文件包含攻击、信息泄露攻击、WEBSHELL、网站扫描、网页木马等类型，产品预定义Web应用漏洞特征库超过4000种；（提供产品界面截图） 16、产品支持用户账号全生命周期保护功能，包括用户账号入口检测、用户账号弱口令检测、用户账号暴力破解检测、失陷账号检测； 17、产品可扩展主动诱捕功能，通过伪装业务诱捕内外网的攻击行为，并联合云蜜罐获取黑客信息，并自动封锁高危IP； 18、产品支持主主、主备两种双机模式部署；19、支持应用控制策略生命周期管理，包含安全策略的变更时间、变更类型和策略变更账号，并对变更内容记录日志。三、保修及服务：1. 提供硬件三年维保，三年软件升级，三年特征库升级；
 | 新机房内网数据中心安全隔离，旁路部署 |  |
|  | 新机房数据库防火墙 | 1台 | 一：性能参数：1.吞吐能力≥2Gbps，并发数据库连接≥2000个，并发数据库流量≥200Mb/s，峰值事务处理能力≥20000QPS(条/秒)，≥16个数据库实例授权2.机箱高度：2U，≥6个千兆电口，≥4个千兆光口，硬盘≥2T\*2，内存≥32G，电源:双电源 二：功能参数：3.支持Oracle、MySQL、Mariadb、PostgreSQL、DB2、MSSqlserver、hive、hbase、kingbase、gbase8a、sybase、informix、MongoDB、达梦（DM）、人大金仓（KingBase）、ODPS、vertica、Guassdb 100/200、GreenPlum、spark、TiDB、GoldenDB、HANA、Impala、Presto、[Caché](https://baike.baidu.com/item/Cach%C3%A9/7108256?fromModule=lemma_inlink" \t "https://baike.baidu.com/item/cache%20%E6%95%B0%E6%8D%AE%E5%BA%93/_blank)等数据库支持4.为适应各种复杂的部署环境，产品部署模式上应支持软件化部署及集群部署5.支持数据库“隐身”，使黑客无法通过常用手段扫描数据库漏洞，从而达到保护数据库的目的6.支持IP组、操作系统用户名组、客户端主机名组、客户端工具名组、数据库账号组、时间组和对象组的分组管理7.支持对接安全管控平台实现规则下发。同时可在数据安全管控平台查看设备运行状态及安全策略总数、告警数量、防护资产数量、在线会话数、虚拟补丁数量、策略执行数量等（提供相关功能截图）8.支持旁路镜像部署，支持旁路阻断，在不影响客户网络环境拓扑的前提下实现数据库防护9.支持多操作日志记录(例如：攻击日志、访问控制日志、告警日志)、日志查询，可以对接日志审计平台10.支持数据库防护虚拟补丁技术，防护未升级数据库，并可以更新维护（提供相关功能截图）11.支持系统安全配置如会话锁定、超时退出、IP访问控制、密码复杂性管理等安全措施（提供相关功能截图）12.支持SNMP获取设备信息，支持资源使用报表，支持调试工具：日志下载、连通性检测、tcpdump抓包13.支持基于一定时间范围内基于同一会话、同一ip、同一用户、同一工具等维度对数据库访问频次及返回行数的限制14.自定义规则支持根据账号、数据库名、客户端工具、操作系统用户名、客户端IP、操作类型、SQL关键字等制定防护策略（提供相关功能截图）15.内置的特征策略包含缓冲区溢出、SQL注入、提权、数据库内核入侵探测等常见攻击特征，内置多种数据库安全规则16.支持用户行为建模，可通过一段时间的学习，智能建立用户行为模型，学习期结束后对业务侧正常SQL语句放行，异常SQL阻断或告警。17.产品支持与现网态势感知平台联动，将防火墙产品产生的安全日志等数据上报至态势感知平台，并在态势感知平台进行威胁展示；三、保修及服务：提供硬件三年维保，三年软件升级，三年特征库升级； | 新机房内网数据安全网关，旁路部署 |  |
|  | 新机房数据中心入侵防御IPS | 1台 | 一、性能参数：1. ≥2U机架式设备，双电源，系统提供≥1个RJ45串口，1个1000M独立管理口和1个HA口≥，2个USB接口；工作接口≥8个千兆电口+6个千兆SFP光口+2个万兆SFP+光口（含光模块），剩余不少于1个扩展槽位；
2. 在入侵防御和防病毒功能开启下，网络吞吐量不小于6G，新建HTTP连接数不小于6万，并发HTTP会话数不小于300万；

二、功能参数：1. 系统入侵防御事件库事件数量不少于5000条。
2. 系统应支持DHCP功能，包括DHCP服务器和DHCP中继功能，并可以作为客户端获得IP地址，满足自动化管理的需要；
3. 系统应支持虚拟IPS功能，不同的用户可以方便定制满足自身要求的检测模版；
4. 系统应提供口令保护功能，能够探测和阻止恶意暴力口令猜测行为，要求支持至少20种应用特征的口令穷举猜测；
5. 系统应支持弱口令检测功能，需支持至少8种网络协议并支持至少7种弱口令检测元素；
6. 系统应支持无线攻击检测和防护功能扩展，可手工或自动识别和区分内部AP和外部AP，也可以手工或自动识别合法终端，并基于此设定无线准入策略，通过射频信号阻止非法AP、终端的接入。支持无线扫描、欺骗、DoS、破解等常见无线网络攻击行为的检测、告警、阻断功能，同时支持多种类型流氓AP的检测与阻断；
7. 系统应支持自定义事件升级内容。针对新增加的事件特征，针对不同级别的事件，用户可以选择是否自动升级到自定义策略中。升级界面中至少包含高中低三种级别事件的升级启用选项。并支持可自动修改动作为通过，满足业务高连续要求下的事件监测要求。
8. 基于行为分析的C&C通道（隐蔽通道）检测机制，能够发现网络中的存在的隐蔽通道。提供C&C通道的危险级别、连接建立时间、连接持续时间、控制端IP地址和端口、受控端IP地址和端口等信息。提供各种响应动作：阻断会话、临时阻断和抓包分析等（提供功能界面截图）；
9. 系统内置恶意样本快速检测功能，无需搭配硬件检测模块，能对流经的HTTP、FTP、邮件协议中包含的office文档、图片文档及压缩文档进行恶意代码快速检测，对可疑文件进行报警，报警信息应包括源目的IP、协议类型、文件基本信息、危险等级及文件的应用的详细信息（如邮件的发件人、收件人、标题等），方便对恶意文件进行追踪。
10. 系统应支持单独的恶意样本检测规则升级功能，方便对恶意样本检测功能进行扩充。
11. 与现网内态势感知平台实现数据对接，防御联动。
12. 针对SQL注入和XSS攻击，设备应支持在线事件分析功能。SQL注入至少提供攻击位置、攻击方法、解码后数据、攻击域、影响的数据库等，XSS攻击至少提供协议字段、攻击数据、解码后数据、攻击域、编码方式等；
13. 系统应针对SQL注入、XSS攻击提供白名单功能。XSS攻击白名单能够精确到检测点、属性和名称。SQL注入白名单并支持至少10类和70个配置项目；
14. 系统需具有多种防web扫描能力，防止攻击者通过扫描发现Web网站中的缺陷从而发起精确攻击，至少包括如下能力：防爬虫、防止CGI和漏洞扫描等，并支持阻断扫描行为和并记录日志，系统支持设置至少4个级别的扫描容忍度/扫描敏感度，方便安全管理者采用不同安全级别的行为控制；
15. 系统应支持敏感信息防护功能，识别信息和文件中的关键字、身份证、手机号码、固定电话号码、银行卡、IP地址等敏感信息，并支持文件指纹识别和白名单功能，并说明支持的应用情况和处理方式（提供功能界面截图）；
16. 系统应支持高负载下的bypass功能，使得系统在CPU和内存较高情况下启动bypass功能，避免网络出现延迟和丢包等情况，提高网络可用性。并可配置启用Bypass的CPU和内存阈值，及选择取值的计算方式（最高值/平均值、时间区间等），防止设备出现Bypass状态震荡。并支持二层回退。
17. 集中管理中心需提供多种报表格式，满足客户对不同格式的需求，需包括：html、doc、xls、CSV和pdf；
18. 系统应提供系统监控和趋势曲线图展示，至少支持内存占用率、CPU占用率、总流量、每秒新建连接数、并发会话数的趋势图，可按照1小时、6小时、12小时、1-7天等时间段展示趋势曲线；

三、保修及服务：提供硬件三年维保，三年软件升级，三年特征库升级； | 新机房内网数据中心入侵防御，旁路部署 |  |
|  | 新机房内网Web应用防墙WAF | 1台 | 一、性能参数：1. ≥2U机架式设备，双电源，≥1个千兆管理口，1个千兆HA口，1个RJ45串口；配置≥4个千兆自适应电口+4个SFP接口（含光模块）+4个万兆SFP+接口（含光模块）；剩余扩展插槽不少于1个；
2. 整机最大吞吐量≥17Gbps，应用层吞吐量≥7Gbps，整机最大并发HTTP连接数≥400万，每秒新建HTTP连接数≥9万；

二、功能参数：1. 支持智能部署，上线WAF设备能够自动感知Web网站IP和端口；
2. 支持安装向导式部署，按照该部署方式可直接部署完成；
3. 支持NAT环境下的用户识别能力，应支持链路绑定功能，应支持对Web相关应用协议进行自定义，并提供详细协议分析变量；
4. 支持大屏展示能力，可满足客户对WAF产品大屏展示要求；
5. 具备Web恶意扫描防护的检测与防御能力，专利级别防护能力；
6. 具备API防护，可支持API协议合规、API访问速率限制等功能；
7. 具备检测到攻击日志可高亮显示，有利于用户比较直观看到攻击脚本；
8. 上报日志中有日志解码工具，通过解码工具可准确查看攻击语句，有利于用户查看和分析攻击日志（提供功能界面截图）；
9. 支持人机识别功能，通过发起JS挑战，来识别机器对网站的操作还是人为操作，可以防护一下自动化工具防止恶意软件对网站的资源消耗；
10. 具备未知威胁的检测和防护能力，具备0day攻击防御能力；
11. 与现网内态势感知平台实现数据对接，防御联动。
12. 具备语义防护、AI智能防护、算法防护功能；
13. 具备蜜罐检测功能，诱使攻击方对它实施攻击，从而可以对攻击行为进行捕获和阻断（提供功能界面截图）；
14. 具备业务合规功能，可对业务进行恶意试探、恶意撞库、恶意登录等行为进行检测及拦截；
15. 具备API接口的解析及防护，支持JSON、XML格式等覆盖大部分常用场景的API接口需求；
16. 具备网站一键关停功能（非关闭接口，不影响其他网络使用），满足特殊时期网站紧急关停的需求，网站一键切换到维护模式。
17. 支持获取Web安全事件的原始攻击信息；支持B/S管理方式Web管理界面；
18. 具备多设备拓扑显示功能，可以在界面上以图形化的方式显示当前的部署拓扑；
19. 支持SSL加密传输，实配https传输加密和身份认证功能。

三、保修及服务：提供硬件三年维保，三年软件升级，三年特征库升级； | 新机房内网数据中心Web应用防护监测，旁路部署 |  |
|  | 新机房内网用户区防火墙 | 1台 | 一、性能参数： 1.性能参数：网络层吞吐量≥20G，应用层吞吐量≥9G，防病毒吞吐量≥1.5G，IPS吞吐量≥1.3G，全威胁吞吐量≥1G，并发连接数≥200万，HTTP新建连接数≥9万。2.硬件参数：规格1U，内存大小≥8G，硬盘容量≥128G SSD，电源：单电源，接口≥8千兆电口+2万兆光口SFP+（含光模块）。二、功能参数1、产品支持路由模式、透明模式、虚拟网线模式、旁路镜像模式等多种部署方式；支持链路健康检查功能，可基于多种协议对链路可用性进行探测；支持链路聚合功能，可以将多个物理链路组合成一个性能更高的逻辑链路接口；2、支持多链路出站负载，可基于源/目的IP、源/目的端口、协议、ISP、应用类型以及地域来进行选路的策略路由选路功能；3、产品支持IPv4/IPv6双栈工作模式，以适应IPv6发展趋势；支持IPv6访问控制策略设置，基于IPv6的IP地址、服务、域名、应用、时间等条件设置访问控制策略。 4、产品支持IPsec VPN和SSL VPN功能，为满足组网兼容性，IPSec VPN需支持IKEv1和IKEv2协议，可实现和第三方VPN的对接；5、IPSec VPN智能选路功能，根据线路质量实现线路自动切换；6、产品支持对不少于9880种应用的识别和控制，应用类型包括游戏、购物、图书百科、工作招聘、P2P下载、聊天工具、旅游出行、股票软件等类型应用进行检测与控制；7、产品支持基于IP对象的会话控制策略，实现并发连接数的合理限制；支持多维度安全策略设置，可基于时间、用户、应用、IP、域名等内容进行安全策略设置；8、支持DDoS防护策略，可对ICMP、UDP、DNS、SYN等协议进行DDOS防护；支持异常包攻击防御，异常包攻击类型至少包括Ping of Death、Teardrop、Smurf、Land、WinNuke等攻击类型；9、产品开启防病毒模块，支持对SMTP、HTTP、FTP、SMB、POP3、HTTPS、IMAP等协议进行病毒防御；10、产品支持对多重压缩文件的病毒检测能力，支持不小于12层压缩文件病毒检测与处置；11、产品支持入侵防御功能，预定义漏洞特征数量超过9000种； 12、产品支持与现网态势感知平台联动，将本地防火墙产品产生的安全日志等数据上报至态势感知平台，并在态势感知平台进行威胁展示； 13、产品支持基于IMAP、FTP、RDP、VNC、SSH、TELNET、ORACLE、MYSQL、MSSQL等应用协议进行深度检测与防护；14、产品可扩展对常见Web应用攻击防御，攻击类型至少支持跨站脚本（XSS）攻击、SQL注入、文件包含攻击、信息泄露攻击、WEBSHELL、网站扫描、网页木马等类型，产品预定义Web应用漏洞特征库超过4000种；15、产品支持用户账号全生命周期保护功能，包括用户账号入口检测、用户账号弱口令检测、用户账号暴力破解检测、失陷账号检测；16、产品可扩展 主动诱捕功能，通过伪装业务诱捕内外网的攻击行为，并联合云蜜罐获取黑客信息，并自动封锁高危I····P； 17、产品支持主主、主备两种双机模式部署；18、与现网内态势感知平台实现数据对接，防御联动。19、支持应用控制策略生命周期管理，包含安全策略的变更时间、变更类型和策略变更账号，并对变更内容记录日志。（提供产品界面截图）三、保修及服务：提供硬件三年维保，三年软件升级，三年特征库升级； | 新机房内网终端用户区安全隔离 |  |
|  | 雁山公共卫生救治中心内网防火墙 | 1台 | 一、性能参数： 1.性能参数：网络层吞吐量≥20G，应用层吞吐量≥9G，防病毒吞吐量≥1.5G，IPS吞吐量≥1.3G，全威胁吞吐量≥1G，并发连接数≥200万，HTTP新建连接数≥9万。2.硬件参数：规格1U，内存大小≥8G，硬盘容量≥128G SSD，电源：单电源，接口≥8千兆电口+2万兆光口SFP+（含光模块）。二、功能参数1、产品支持路由模式、透明模式、虚拟网线模式、旁路镜像模式等多种部署方式；支持链路健康检查功能，可基于多种协议对链路可用性进行探测；支持链路聚合功能，可以将多个物理链路组合成一个性能更高的逻辑链路接口；2、支持多链路出站负载，可基于源/目的IP、源/目的端口、协议、ISP、应用类型以及地域来进行选路的策略路由选路功能；3、产品支持IPv4/IPv6双栈工作模式，以适应IPv6发展趋势；支持IPv6访问控制策略设置，基于IPv6的IP地址、服务、域名、应用、时间等条件设置访问控制策略。 4、产品支持IPsec VPN和SSL VPN功能，为满足组网兼容性，IPSec VPN需支持IKEv1和IKEv2协议，可实现和第三方VPN的对接；5、IPSec VPN智能选路功能，根据线路质量实现线路自动切换；6、产品支持对不少于9880种应用的识别和控制，应用类型包括游戏、购物、图书百科、工作招聘、P2P下载、聊天工具、旅游出行、股票软件等类型应用进行检测与控制；7、产品支持基于IP对象的会话控制策略，实现并发连接数的合理限制；支持多维度安全策略设置，可基于时间、用户、应用、IP、域名等内容进行安全策略设置；8、支持DDoS防护策略，可对ICMP、UDP、DNS、SYN等协议进行DDOS防护；支持异常包攻击防御，异常包攻击类型至少包括Ping of Death、Teardrop、Smurf、Land、WinNuke等攻击类型；9、产品开启防病毒模块，支持对SMTP、HTTP、FTP、SMB、POP3、HTTPS、IMAP等协议进行病毒防御；10、产品支持对多重压缩文件的病毒检测能力，支持不小于12层压缩文件病毒检测与处置；11、产品支持入侵防御功能，预定义漏洞特征数量超过9000种； 12、产品支持与现网态势感知平台联动，将本地防火墙产品产生的安全日志等数据上报至态势感知平台，并在态势感知平台进行威胁展示； 13、产品支持基于IMAP、FTP、RDP、VNC、SSH、TELNET、ORACLE、MYSQL、MSSQL等应用协议进行深度检测与防护；14、产品可扩展对常见Web应用攻击防御，攻击类型至少支持跨站脚本（XSS）攻击、SQL注入、文件包含攻击、信息泄露攻击、WEBSHELL、网站扫描、网页木马等类型，产品预定义Web应用漏洞特征库超过4000种；15、产品支持用户账号全生命周期保护功能，包括用户账号入口检测、用户账号弱口令检测、用户账号暴力破解检测、失陷账号检测；（提供产品界面截图） 16、产品可扩展 主动诱捕功能，通过伪装业务诱捕内外网的攻击行为，并联合云蜜罐获取黑客信息，并自动封锁高危I····P； 17、产品支持主主、主备两种双机模式部署；18、与现网内态势感知平台实现数据对接，防御联动。19、支持应用控制策略生命周期管理，包含安全策略的变更时间、变更类型和策略变更账号，并对变更内容记录日志。三、保修及服务：提供硬件三年维保，三年软件升级，三年特征库升级； | 雁山公共卫生救治中心网络接入安全隔离 |  |
|  | 终端准入（含终端安全管理）控制系统 | 1套 | 1、2U设备，6个千兆电口，2个USB口，2个网卡扩展插槽，可实现网关准入，802.1x准入， Portal准入和 DHCP准入模式，至少支持2000个终端并发，授权数≥2000个（PC桌面终端≥1600个，安卓亚终端≥400个）；配置终端管理模块，授权数≥2000个（PC桌面终端1600个，安卓亚终端400个），与准入在统一平台集成部署，一个客户端统一管理，也可单独部署客户端。2、支持有线或无线网络环境下的准入认证与管理。3、支持多类型终端统一管控，支持Windows、信创操作系统、安卓系统的设备准入控制。（提供产品功能截图）4、支持系统内置用户系统认证入网用户身份，支持口令、UKEY认证方式，支持通过第三方认证源认证入网用户身份，至少支持AD域、Ldap认证。5、支持通过数据包的IPID、客户端在线、UDP探测、小路由方式判断终端合法性。6、支持定义受保护的服务器范围，非法终端无法访问受保护的服务器，支持以IP地址段、IP+MAC、仅MAC形式添加。7、支持通过产品控制台配置准入服务器的开启状态，支持管理、仅审计、不管理三种状态。开启管理后，未安装客户端或未授权的终端访问服务器时，需产生审计日志，并且阻止访问网络。8、支持设置保留IP与MAC地址绑定，当绑定的终端上线时，确保保留IP地址分配给此终端。9、正式用户主要用于有客户端的终端进行身份认证，正式用户列表具备用户组和用户的建立、修改、删除、导入，用户支持移动组；可以对用户进行启用和停用，支持有效期设置；支持为每个用户签发证书、下载证书用于用户制作UKEY身份认证。支持定义用户角色，用户密码复杂度配置。10、支持远程协助功能，可支持直接远程或者终端确认两种远程模式，管理员在发起远程时可配置远程控制理由，支持远程控制时内外网文件的双向传输，支持远程控制时在服务端和客户端之间进行双向文件传输；11、支持Windows和国产终端文件分发功能，管理员可配置文件分发参数，可设置分发文件的存放位置、失败重发，支持限制终端在资源占用率不高于70%时才接收并运行文件。12、可将不同版本的同一软件汇总统计安装情况，并且支持以软件维度统一对安装的终端下发软件卸载任务；13、支持Windows进程红名单保护功能，红名单提供必须启动和进程保护两种控制模式。（提供产品功能截图）14、支持客户端外设信息自动上报，并由控制中心汇总展示，支持对外设信息进行分类，例外等处理；15、支持对终端外联安全进行防护，可禁止客户端修改IP、修改MAC、禁止终端创建热点、禁止多SSID同时连接、禁止有线无线网卡共用。16、产品具备终端违规外联检测能力，支持解析域名、PING探测地址、TCP建立连接三种外联探测方式，支持以分钟单位设置探测时间间隔，支持以IP或域名方式设置探测地址，可对违规终端即时报警，处置。违规外联处罚规则，包括客户端违规外联后弹框提示、断开网络、关机、断开网络+终端锁屏、终端锁屏。17、支持开启或禁用组策略编辑器、注册表编辑器、阻止添加打印机、关闭系统还原、系统共享、用户共享、任务管理器、账户自动登录、远程修改注册表、远程协助、远程桌面、系统防火墙、U盘自动播放等本地安全策略。18、支持自定义壁纸，在客户端原有壁纸的基础上，支持显示基本信息如算机名称、IP、MAC、归属部门、使用人、手机、邮箱等信息。三、保修及服务：提供硬件三年维保，三年软件升级； | 内网用户终端认证加管理授权 |  |
|  | 新机房零信任VPN 网关（国密） | 1台 | 1. 性能参数：
2. 规格≥1U，内存大小≥16G，硬盘容量≥128G SSD，电源：冗余电源，接口≥6千兆电口+4千兆光口SFP。

二、功能参数要求1. 支持B/S-WEB资源纯浏览器访问，支持http/https等资源免客户端接入，便于用户无感接入；支持对外发布为HTTP/HTTPS资源。
2. 支持CS隧道TCP协议资源接入，支持发布TCP协议资源（包括FTP、TELNET、RDP、SMTP/POP3邮箱及其他常规CS应用）。
3. 支持发布多IP网段，支持同一个资源发布多个IP网段和IP。
4. 支持不同平台的终端同时在线，管理员可设置可同时在线的终端个数，不能超过设定的终端个数。
5. 支持全终端浏览器接入并访问WEB资源，支持IE8及以上版本浏览器访问WEB资源；支持CHROME 69及以上版本访问WEB资源；支持EDGE、FIREFOX、OPERA、SAFARI等其他主流浏览器访问WEB资源；支持ANDROID、IOS各大手机厂商的自带浏览器访问WEB资源；支持国产操作系统浏览器接入并访问WEB资源。（提供相关功能截图）
6. 支持在登录上线后，持续、动态检测终端环境安全，不符合后注销用户或锁定用户。
7. 支持按角色授权，支持按用户、用户组、安全组进行角色授权，简化权限管理。
8. 支持依赖站点一键启用，自动采集。
9. 支持针对不同的WEB（B/S）应用开启WEB水印；水印内容包括：用户名+当前日期。（提供相关功能截图）
10. 支持异常环境下，要求增强认证；异常时间段。管理员在新建或修改本地用户密码时，必须符合强密码规则，不能设置弱密码。管理员在新建或修改本地用户密码时，必须符合强密码规则，不能设置弱密码。
11. 支持按资源粒度划分权限，如指定某管理员仅能管理指定3个应用。
12. 支持全面的日志记录，支持用户登录日志（登录、注销，含MAC地址、终端类型、浏览器类型等）；支持管理员操作日志（含管理员、接入IP、时间、管理行为、对象）；支持资源访问日志（用户、源IP、URL、时间）。
13. 支持虚拟IP对接，支持以虚拟IP方式，访问真实的业务系统，便于流量分析类设备进行流量分析 ；支持虚拟IP池，用户首次连接时分配虚拟IP，后续用户与虚拟IP绑定，便于用户访问行为追溯。

三、aTrust代理网关功能要求1. 支持首次登录强制修改密码，支持配置密码最长使用周期（到期后需要修改密码）。
2. 支持开启SSH进行远程运维，且开启后会定期关闭SSH，以免运维人员进行远程运维后，忘记关闭SSH，带来潜在风险。
3. 支持告警信息设置，包含以下几个方面：CPU使用率超过80%、内存使用率超过80%、磁盘占用率超过80%、序列号即将到期（提前15天提醒）、在线用户数已达购买授权数。
4. 发布WEB资源，支持审计访问日志（用户、源IP、URL、时间、get请求、post请求、端口）。
5. 支持管理员操作日志（含管理员、接入IP、时间、管理行为、对象）。
6. 支持接入IP限制（即接入控制台的IP白名单），限制后，从浏览器、SSH或SNMP等方式接入管理台时，都必须在上述IP白名单范围内接入。
7. 支持商密加密算法SM2、SM3、SM4。

四、保修及服务：提供硬件三年维保，三年软件升级； | 运维用户远程接入 |  |
|  | 日志审计系统存储扩容 | 1项 | 安恒态势感知日志审计模块硬盘扩容6块6T硬盘，含原厂硬盘容量授权。 | 内网日志收集与分析 |  |
|  | 新机房漏洞扫描系统 | 1套 | 一、性能参数：1. 软硬一体化≥1U标准机架式设备，配置内存≥16G，硬盘≥2T\*1，≥6个千兆电口。

二、功能参数1. 支持系统扫描、弱口令扫描、Web扫描、数据库扫描，任务并发数≥10，最大并发主机数≥90，授权可扫描总数量不多于512个无限制范围IP地址；
2. 支持用户自定义系统名称、版权信息和系统的Logo信息，而无需进行定制化；
3. 漏洞知识库支持自定义编辑，可编辑漏洞描述、修复建议、漏洞等级等内容，在扫描结果和导出报告中应展示编辑后的内容
4. 厂商漏洞特征库大于230000条；提供详细的漏洞描述和对应的解决方案描述；漏洞知识库与CVE、CNNVD、Bugtraq、CNCVE、CNVD等国际、国内漏洞库标准兼容（需提供相关功能截图证明）；
5. 系统内置不同的策略模板如针对Linux操作系统、Windows操作系统、工控、大数据、虚拟化、数据库扫描等模板，同时允许用户定制扫描策略模板。
6. 具备弱口令扫描功能，支持弱口令扫描协议数量≥22种，包括FTP、SMB、RDP、SSH、TELNET、SMTP、IMAP、POP3、Oracle、MySQL、MSSQL、DB2、REDIS、MongoDB、Sybase、Rlogin、RTSP、SIP、Onvif、Weblogic、Tomcat、SNMP等协议进行弱口令扫描，允许用户自定义用户、密码字典（需提供相关功能截图证明）；
7. 支持多种网站认证方式：支持包括Basic、Digest、DigestIE、NTLM、GSS-Negotiate、Bearer在内的认证方式，支持HTTP和SOCKS代理，并支持各种代理的认证方式。
8. 支持授权管理，对已知用户名和密码的资产可预先进行配置存放至授权管理模块，下发扫描任务时能对该部分资产的授权信息进行同步
9. 支持自定义扫描策略模板，可以将自定义策略模板导出备份，也可以导入备份的策略模板，能够对策略模板进行编辑、另存为新的模板。
10. 支持在线查看报告和离线导出报告，报告导出可将弱口令隐藏不以明文的形式展现至报告。
11. 支持对用户有效期进行详细设置，可以设置不限制，也可以设置每天的哪个时段、每周的周几至周几、每月几号至几号才能正常使用；
12. 支持常见Web漏洞类型的扫描，包括SQL注入、跨站脚本、命令执行、命令注入、代码注入、弱口令、目录遍历、URL跳转、文件包含、反序列化漏洞、文件上传、CSRF跨站请求伪造、信息泄露等。支持OWASP TOP10等主流安全漏洞；
13. 支持将漏洞以紧急、高危、中危、低危、信息进行危害程度的分类，并且可根据用户需要自定义漏洞等级；
14. 支持多种网站认证方式：支持包括Basic、Digest、DigestIE、NTLM、GSS-Negotiate、Bearer在内的认证方式，支持HTTP和SOCKS代理，并支持各种代理的认证方式；
15. 数据库扫描支持的检测类型大于10种，至少包括弱口令、执行权限过大、访问控制漏洞、提权漏洞、缓冲区溢出漏洞、缺省配置、访问权限绕过、PL-SQL注入、危险程序、安全信息查看等。
16. 产品支持与现网态势感知平台联动，将漏洞报告等数据上报至态势感知平台，并在态势感知平台进行威胁展示。

三、保修及服务：提供硬件三年维保，三年软件升级，三年特征库升级； | 内外网系统及设备漏洞扫描  |  |
|  | 授时服务器 | 2台 | 1.输入信号来自北斗GPS卫星的定时信号； 网络输出路数：2路；物理接口：RJ45，10M/100M自适应；操作系统Windows Linux等主流系统；NTP 请求量；＞8000 次/秒；用户容量：支持数万台客户端；授时精度 1-10ms（典型值 1ms）；管理功能：Web 管理；软件监控管理记录功能：支持最新 20000 条 NTP 日志记录功能；其它功能：防火墙保护，SYN-flood 防御，软硬件看门狗设计，QoS 功能（流量监控），中英文选择功能，实时查看 NTP 运行状态，网络诊断，1PPS脉冲信号 1 路 TTL，同步误差≤30ns ，485串口2路，串口 TOD 1 路 DB9，RS232C，年月日时分秒地理位置信息DB9接口；提供中国计量科学研究院计量证书。2.保修及服务：提供硬件三年维保。 | 时间同步服务 |  |
| **外网安全：** |  |
|  | 新机房外网服务器区防火墙模块升级 | 1项 | 原有深信服AF-2000-B2150防火墙扩容网关杀毒模块1项，网关杀毒升级许可1年。 | 新机房外网服务器区安全隔离 |  |
|  | 新机房互联网边界防火墙 | 1台 | 一、性能参数： 1.≥1U机架式设备，双电源；配置≥12个千兆电口(含1对电口Bypass），≥1个管理电口，≥12个千兆光口；2.网络吞吐量≥8Gbps，最大并发连接数≥300万，每秒新建HTTP连接数≥10万。二、功能参数：1. 具有透明、路由、混合、旁路、虚拟线工作模式；支持端口镜像功能，支持入流量、出流量和双向流量等维度镜像。
2. 支持IPv4/v6双栈协议的源地址转换、目的地址转换、双向NAT、NAT44、NAT66、NAT46、NAT64等地址转换。
3. 支持4G USB插卡接入，实现4G连接与有线链路之间互为备份。并支持在4G接口上运行IPSec VPN。
4. 支持标准IPsec VPN和快速IPsecVPN，标准IPsecVPN认证方式包括但不限于国密认证、数字证书和预共享密钥；同品牌设备快速IPsecVPN对接时加密算法等参数无需配置，自动生成，仅需配置保护子网、共享密钥、IP地址。
5. 支持一体化安全策略：可基于设备接口/安全域、地址、服务、应用、用户、时间等属性，配置入侵防御、病毒防护、URL过滤、应用过滤、日志记录、会话老化时间、终端过滤等高级访问控制功能。
6. 内置8600条以上IPS规则库，以及对应IPS规则的攻击类型、严重程度、CVE编号、CNNVD编号、协议、操作系统、发布年份、漏洞厂商等详细信息，可自定义攻击特征库，并支持对攻击进行本地报文存储便于事后回溯。
7. 支持独立的Web防护模块，提供防盗链、CSRF攻击、CC攻击、应用隐藏、网页防篡改等防护；支持HTTP协议的精确访问控制，可针对Method、Referer、User-Agent、Cookie、Url-args等字段设置内容。
8. 内置7000种以上应用规则，其中移动应用不少于2200个；支持针对应用动作的细粒度控制；支持对应用的文件传输行为进行上传、下载、双向的文件类型过滤；支持对FTP、Telnet、DNS等协议的相关操作命令进行过滤控制。（提供相关截图证明）
9. 支持基于流量和时长的流量限额功能，针对超过限额的用户，可选择禁止上网或加入至惩罚流控通道
10. 支持本地认证、Portal认证、Radius认证、LDAP认证、POP3认证、AD域单点登录、短信认证、微信认证、APP认证、二维码认证、互联网钉钉认证、混合认证和免认证，其中本地认证支持用户自注册；微信认证支持通过小程序获取手机号。
11. 支持用户全天行为分析，一个界面同时展示用户名、用户组、在线时长、虚拟身份（如QQ号码、微博账号等）、日志关联情况、全天流量使用分布、网站访问类别分布、全天关键网络行为轴等信息。
12. 支持防网络共享行为，针对私接路由器和非法无线热点行为进行识别和阻断；并针对私接网络行为，惩罚方式包括但不限于无操作、阻断和限速。（提供相关截图证明）
13. 支持持文件缓存，缓存文件形式不限于视频、APP等；设备智能解析用户流量，针对域名或者文件请求，设备推送文件至终端，帮助用户缓解互联网出口压力，实现文件下载加速的效果。

三、保修及服务：1. 提供硬件三年维保，三年软件升级，三年特征库升级；
 | 新机房互联网接入安全隔离 |  |
|  | 雁山公共卫生救治中心外网边界防火墙 | 1台 | 一、性能参数： 1.网络层吞吐量≥4G，应用层吞吐量≥2G，防病毒吞吐量≥600M，IPS吞吐量≥600M，全威胁吞吐量≥450M，并发连接数≥200万，HTTP新建连接数≥6万。2.硬件参数：规格≥1U，内存大小≥4G，硬盘容量≥128G SSD，电源：单电源，接口≥8千兆电口+2千兆光口SFP。二、功能参数1、产品支持路由模式、透明模式、虚拟网线模式、旁路镜像模式等多种部署方式；支持链路健康检查功能，可基于多种协议对链路可用性进行探测；支持链路聚合功能，可以将多个物理链路组合成一个性能更高的逻辑链路接口；2、支持多链路出站负载，可基于源/目的IP、源/目的端口、协议、ISP、应用类型以及地域来进行选路的策略路由选路功能；3、产品支持IPv4/IPv6双栈工作模式，以适应IPv6发展趋势；支持IPv6访问控制策略设置，基于IPv6的IP地址、服务、域名、应用、时间等条件设置访问控制策略。 4、产品支持IPsec VPN和SSL VPN功能，为满足组网兼容性，IPSec VPN需支持IKEv1和IKEv2协议，可实现和第三方VPN的对接；5、IPSec VPN智能选路功能，根据线路质量实现线路自动切换；6、产品支持对不少于9000种应用的识别和控制，应用类型包括游戏、购物、图书百科、工作招聘、P2P下载、聊天工具、旅游出行、股票软件等类型应用进行检测与控制；7、产品支持基于IP对象的会话控制策略，实现并发连接数的合理限制；支持多维度安全策略设置，可基于时间、用户、应用、IP、域名等内容进行安全策略设置；8、支持DDoS防护策略，可对ICMP、UDP、DNS、SYN等协议进行DDOS防护；支持异常包攻击防御，异常包攻击类型至少包括Ping of Death、Teardrop、Smurf、Land、WinNuke等攻击类型；9、产品开启防病毒模块，支持对SMTP、HTTP、FTP、SMB、POP3、HTTPS、IMAP等协议进行病毒防御；10、产品支持对多重压缩文件的病毒检测能力，支持不小于12层压缩文件病毒检测与处置；11、产品支持入侵防御功能，预定义漏洞特征数量超过9000种； （提供产品界面截图）12、产品支持与态势感知平台联动，将本地防火墙产品产生的安全日志等数据上报至态势感知平台，并在态势感知平台进行威胁展示； 13、产品支持基于IMAP、FTP、RDP、VNC、SSH、TELNET、ORACLE、MYSQL、MSSQL等应用协议进行深度检测与防护；14、产品可扩展对常见Web应用攻击防御，攻击类型至少支持跨站脚本（XSS）攻击、SQL注入、文件包含攻击、信息泄露攻击、WEBSHELL、网站扫描、网页木马等类型，产品预定义Web应用漏洞特征库超过4000种； 15、产品支持用户账号全生命周期保护功能，包括用户账号入口检测、用户账号弱口令检测、用户账号暴力破解检测、失陷账号检测；（提供产品界面截图） 16、产品可扩展主动诱捕功能，通过伪装业务诱捕内外网的攻击行为，并联合云蜜罐获取黑客信息，并自动封锁高危IP；（提供产品界面截图） 17、产品支持主主、主备两种双机模式部署；18、支持应用控制策略生命周期管理，包含安全策略的变更时间、变更类型和策略变更账号，并对变更内容记录日志。三、保修及服务：提供硬件三年维保，三年软件升级，三年特征库升级； | 雁山外网接入安全隔离（雁山） |  |
|  | 雁山公共卫生救治中心出口上网行为管理 |  | 一、AC性能参数：1、性能指标：网络层吞吐量≥5.8Gbps，带宽性能≥500Mb，并发连接数≥50W，新建连接数≥10000；2、硬件指标：1U规格；存储≥28GB MSATA；单电源；标配≥6个千兆电口；二、AC功能参数：1、为保障设备高可靠性能，必须支持两台及两台以上设备同时做主机的部署模式。2、为满足IPv6改造需求，支持部署在IPv6环境中，设备接口及部署模式均支持ipv6配置，所有核心功能（上网认证、应用控制、流量控制、内容审计、日志报表等）都支持IPv6；3、为提高运维管理效率，降低运维难度，需要提供图形化排障工具，便于管理员排查策略错误等故障4、为提高运维管理效率，密码登录支持用户自注册，通过Web页面申请注册新账号，管理员审批后新账号可用，自注册同时支持portal认证和802.1x认证（提供产品界面截图）；5、为提高用户使用体验，支持DNS透明代理，能够基于用户、域名、目标DNS，指定代理策略生效，代理策略可以设置为：重定向至DNS服务器、解析为IP、丢弃、重定向至指定线路；6、为便于内部人员快速上线和投入使用，需要支持IPsec VPN支持与LDAP服务器、Radius服务器结合认证7、为便于及时掌握网内情况及问题排查，需要支持查看当前设备的线路状态，线路带宽利用率以及当前策略的引流流量分布和实时的引流策略，支持下钻设置线路流控策略；8、为帮助及时掌握用户WEB访问质量，需支持针对内网用户的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、为保障用户使用体验，需支持通过OAuth认证协议对接，支持阿里钉钉，口袋助理，企业微信第三方账号授权认证，支持企业微信、口袋助理、钉钉 这三个平台支持同步组织结构，用户通过企业微信、口袋助理、钉钉认证上线，本地会创建与认证服务器上对应的用户组，用户会上线到对应创建的组（提供产品界面截图）； 10、为提高系统易用性，需支持radius、AD、POP3、Proxy、PPPOE、 H3C IMC/CAMS、锐捷 SAM、城市热点等系统进行认证单点登录，简化用户操作，可强制指定用户、指定IP段的用户必须使用单点登录；11、为提高安全性同时保障员工使用体验，需要能够对新浪微博、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12、为提升网络安全性，需支持基于802.1x的外部CA证书认证，同时支持在线证书状态查询（OCSP）；13、为降低运维人员运维压力，需支持以图表方式显示移动终端接入趋势14、为帮助管理员减少人工维护IP表的工作量，需支持图形化查看当前内网IP使用情况；15、为协助网络内资产梳理，需支持自动发现网络里面的终端，并获取IP、Mac、厂商、操作系统、开放服务、开放端口等信息，设备必须支持PC、移动设备、哑终端、专用设备的发现和型号识别：至少支持Windows、Linux、MAC、瘦客户机等PC；至少支持手机、平板等移动设备；至少支持服务器、交换机、无线控制器等7类网络设备；至少支持打印机、投影仪、电视、摄像头、门禁系统等10类哑终端16、为帮助了解内部人员审计情况，需要支持首页分析显示接入用户人数、终端类型、认证方式；资产类型分布、新设备发现趋势、终端违规检查项排行、终端违规用户排行；带宽质量分析、实时流量排名；泄密风险、违规访问、共享上网等行为风险情况。三、保修及服务：提供硬件三年维保，三年软件升级，三年特征库升级； | 雁山外网网络管理 |  |
|  | 新机房外网攻击预警平台 | 1套 | 一、性能参数： 1.硬件参数：软硬一体化≥2U标准机架式设备，配置内存≥16G，硬盘≥2T\*1，≥2个千兆管理口、≥4个千兆电业务网口，支持双电源。2.性能参数：吞吐率：网络层≥1Gbps，WEB检测：HTTP最大并发数≥7万/秒，邮件检测：邮件处理数≥100万封/24小时。二、功能参数1. 支持IPv4和IPv6网络环境下的部署，可同时对IPv4和IPv6网络流量分析检测；
2. 支持风险数据包保存功能，可存留会话的请求和相应数据包，帮助用户还原攻击过程，进行取证和关联分析；
3. 支持COAP、MQTT等物联网协议解析和审计；支持GOOSE、MODBUS等工控协议解析和审计；
4. 支持HTTP、SMB、SMTP、IMAP、POP3、FTP、TELNET、RADMIN、SSH、RDP、ORACLE、MSSQL、SYBASE、MYSQL、DB2、PostgreSQL、LDAP、MQTT等协议的暴力破解，能识别出登录次数、账户信息、爆破成功与否的攻击状态；
5. 支持将分析到的SMB远程溢出攻击、扫描行为、Web后门访问、隧道通信、暴力破解、挖矿、远控工具利用等攻击成功事件同步到防火墙，实现APT深度威胁分析与所投防火墙联动阻断（提供相关截图证明）；
6. 支持HTTP密码明文传输和HTTP 密码Base64传输检测，能识别出登录页面URL、账户和明文密码；
7. 支持灵活添加组合白名单，细化白名单影响面，包括IP和检测引擎大类、检测引擎大类子类、规则ID等颗粒度的组合白名单，支持至少8种白名单类型。
8. 可通过攻击源、攻击目的对攻击路线进行统计，包括攻击的行为、告警，并以直观的图形化形式展示；
9. 支持识别流量中的个人敏感信息，包括身份证、银行卡、手机号、港澳通行证等，并展示传输信息的协议、网站域名、URL、客户端IP、服务端IP，便于用户发现敏感信息的传输安全隐患和处置；（提供相关截图证明）。
10. 支持SQL注入、命令注入、跨站脚本、代码注入、WEB扫描或爬虫、网页篡改、系统/服务配置不当、SSRF攻击检测、XXE注入检测；
11. 支持通过智能语义分析引擎，对XSS跨站脚本、SQL注入攻击和OGNL注入攻击进行检测；
12. 支持doc, xls, ppt, swf, pdf, rar, zip, rar, exe, vbs, scr、ps1、elf、mach-O、EML、MHT等多种文件解析；
13. 支持沙箱逃逸检测，当恶意文件进行逃逸尝试，在沙箱报告中进行体现；
14. 与现网内中心防火墙、WEB应用防火墙、互联网防火墙实现数据对接，防御联动。

三、保修及服务：提供硬件三年维保，三年软件升级，三年特征库升级； | 外网攻击预警与分析 |  |
|  | 新机房外网日志审计系统 | 1套 | 一、性能参数：1.硬件配置：≥4个千兆业务电口，≥2个千兆管理电口，≥1个Console口，内存：8GB，磁盘：2T\*1，单电源；2.设备支持资产数≥70，平均日志处理能力2000EPS，最大日志处理能力4000EPS。二、功能参数1. 支持Syslog、SNMP Trap、HTTP、ODBC/JDBC、WMI、FTP、SFTP协议日志收集；支持阿里云SLS日志的采集
2. 可通过接收协议限制日志接收速率，包括Http接收、syslog接收、SNMPtrap接收、TCP接收、WMI接收、aliyun接收。
3. 支持使用代理(Agent)方式提取日志并收集；安装包支持界面下载，且安装支持可视化向导。
4. 支持对Agent进行统一管控，包括卸载、升级、启动及停止操作，支持将日志收集策略统一分发。
5. 支持目前主流的网络安全设备、交换设备、路由设备、操作系统、应用系统等；
6. 支持常见的虚拟机环境日志收集，包括Xen、VMWare、Hyper-V等。（提供相关截图证明）。
7. 可以基于日志等级进行过滤，可以通过自定义配置过滤掉用户不关心的日志；
8. 支持对收集到的重复日志进行自动聚合归并，减少日志量，支持可由用户定义和修改的日志聚合归并逻辑规则;
9. 内置5000+解析规则，支持对收集的5000+设备类型日志进行解析（标准化、归一化），解析维度多达200+，解析规则可以根据客户要求定制扩展；（提供相关截图证明）。
10. 支持磁盘空间阈值告警，当磁盘使用率达到设定的阈值时可产生并外发告警；资产性能监控异常告警，对于监控的资产系统资源进行监测当指定指标使用率达到设定的阈值时可产生并外发告警；。
11. 内置综合性自动化审计报告，支持用户自定义报表，自定义的报表支持多个统计维度的数据集合，支持报表导出为PDF和Word格式文件。
12. 具备公安部颁发的综合日志审计分析平台《计算机信息系统安全专用产品销售许可证》；

三、保修及服务：提供硬件三年维保，三年软件升级； | 外网日志收集与分析 |  |
|  | 新机房应用交付网关（负载均衡） | 1台 | 一、性能参数： 1.4层吞吐量（默认网口）≥2Gbps，四层并发连接数≥3000000，4层新建连接数 CPS≥90000，7层新建请求数 RPS≥80000。2.硬件参数：规格1U，内存大小≥4G，硬盘容量≥128G MSATA SSD，电源：单电源，接口≥6千兆电口+2千兆光口SFP。二、功能参数1、IPv6改造方案能够解决天窗问题，支持一条策略匹配多个外链网站，同时外链和网站子链发生修改时支持自动识别并做主动修改，不允许通过人工解析配置的方式解决天窗问题；2、部署方式支持串接部署、旁路部署；支持三角传输模式。3、设备形态必须独立专业负载设备，非插卡式扩展的负载均衡设备。4、单一设备可同时支持包括链路负载均衡、全局负载均衡和服务器负载均衡的功能。三种功能同时处于激活可使用状态，无需额外购买相应授权5、提供针对多站点业务发布的全局负载均衡功能，通过智能DNS等机制实现公网用户对多个数据中心或单个数据中心多条线路的最佳访问。6、支持轮询、加权轮询、按主机加权轮询、加权最小连接、按主机加权最小连接、动态反馈、最快响应、最小流量、加权最小流量、按主机加权最小流量、带宽比例、哈希、主备、首个可用、优先级等算法7、通过某种编程语言（如lua）实现自定义的流量编排，对IP、TCP、UDP、SSL、HTTP和HTTPS等类型的流量进行分发、修改和统计等操作8、支持图片优化技术，通过对图片格式的转换，减少传输流量，提升web页面加载速度。无需改动服务器端的图片源文件，可根据浏览器种类自动识别转换类型，将图片转换为对应支持的WebP或JPEG格式，优化加速效果。（提供设备操作界面截图证明材料）9、支持静态IP和PPPOE两种线路接入方式。10、支持跨设备健康状态监视（透明监视），同时支持IPv4和IPv611、支持基于管理员自定义的时间计划来进行出站访问的流量调度分发；12、支持跨数据中心集群和跨数据中心会话保持13、支持cookie加密，提升cookie安全性；14、支持被动式健康检查，可根据对业务流量的观测采样，辅助判断应用服务器健康状况；对常规HTTP应用可配置基于反映URL失效的HTTP响应状态码的观测判断机制，对于复杂应用可配置基于RST关闭连接和零窗口等异常TCP传输行为的观测判断机制。（提供设备操作界面截图证明材料）15、支持网站页面IP形式和域名形式外部链接的正常访问；支持静态和动态网站页面静态和动态引用站外内容的正常显示；支持静态和动态网站页面静态和动态外部链接的无限级正常跳转。三、保修及服务：提供硬件三年维保，三年软件升级； | 互联网出口线路负载，路由转发 |  |
|  | 总价（含税及人工等） |  |

**安装部署及服务要求：中标方需提供设备及系统的安装实施部署，包含网络架构调整优化、原有网络及安全设备的位置调整；原有设备和新建系统的策略配置，各设备和系统之间的联调；根据客户需求提供三年策略和配置优化调整服务。**

**报价文件中所承诺的货物性能参数、技术规格、功能必须与实际交付产品完全一致或高于采购要求，确认中标后中标公司提供第16项攻击预警平台产品的测试设备，逐项测试核对产品招标参数规格及功能，如出现不满足标书要求或产品与投标产品不一致，按虚假应标处理，并追究法律责任。**