一、技术要求			
项号	货物名称	数量及单位	主要技术参数及性能（配置）要求
1	防火墙①	2 台	<p>▲1. 多核 AMP+架构，标准 2U 设备，冗余电源；配置≥8 个 SFP 插槽（含 8 个千兆多模光模块），4 个万兆光口（含 4 个万兆多模光模块），另有 2 个接口板卡扩展插槽，1 个 Console 口，支持液晶屏，配置≥128GB 的 SSD 硬盘，含 3 年硬件质保和 IPS 入侵防御、病毒防护升级服务；</p> <p>▲2. 防火墙吞吐≥42Gbps，并发连接数≥600 万，每秒新建连接数≥50 万/秒，包含应用控制、URL 过滤、病毒防护、入侵防御、威胁情报检测等功能模块；</p> <p>3. 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；</p> <p>4. 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；</p> <p>5. 须支持基于 IP、应用、服务的策略路由进行智能选路，支持源地址目的地址哈希、源地址哈希、时延负载、最优链路带宽负载、最优链路带宽备份、跳数等不少于 12 种路由负载均衡方式；</p> <p>6. 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；</p> <p>◆7. 必须支持对应用层 Flood 攻击提供多种防护措施，包括：告警、丢弃、普通防护、增强防护及授权设备防护等；</p> <p>8. 必须支持 DS-Lite CPE B4 功能，支持成为 b4 或 aftr 角色，支持从 DHCPv6 设备或手动方式获取 AFTR 参数；</p> <p>9. 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；</p> <p>10. 须支持共享上网检测功能，支持共享接入检测和共享接入管控功能，可以通过设置管控地址和例外地址优化管控功能，同时支持阻断或告警动作；</p> <p>11. 支持对最多 6 级的压缩文件进行解压查杀；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；</p>

		<p>◆12. 须支持与云端联动，至少实现病毒云查杀、URL 云识别、应用云识别、云沙箱、威胁情报云检测等功能；</p> <p>13. 须支持支持漏洞防护功能，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；</p> <p>14. 须支持 IPv4 和 IPv6 流量的 HTTPS、POP3S、SMTPS、IMAPS 协议进行解密，支持配置基于源安全域、目的安全域、源地址、目的地址、SSL 协议服务的解密策略，动作可以设置解密或不解密，并可基于安全域、IPv4 和 IPv6 地址进行例外设置；</p> <p>◆15. 必须支持与杀毒软件或终端管理软件联动，实现基于终端健康状态的访问控制；</p> <p>16. 须支持基于主机或威胁情报视图，统计网络中确认被入侵、攻破的主机数量，至少可查看被入侵、攻破的时间、威胁类别、情报来源、威胁简介、被入侵、攻破的主机 IP、用户名、资产等信息；并对威胁情报发现的恶意主机执行自动阻断；</p> <p>17. 须支持接收针对突发重大安全事件的“应急响应消息”，针对该消息可以选择“自动”或“手动”处理，处置方法至少包括基于漏洞的处置和基于威胁情报的处置；</p> <p>18. 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，产品需支持限制特定主机调用 Restful API；</p> <p>19. 须支持业务接口下 Netflow 功能，能够通过 Netflow 实现对网络进行监控，对接口流量进行抓包，并在可将 Netflow 抓包文件数据外发；</p> <p>20. 须支持资产管理，能够通过设置资产监控、VPN、源安全域来控制资产识别范围，支持 scanner 或 onvif 类型的扫描方式和网段，实现自动或手动资产扫描；支持通过设置 IP 地址、MAC 地址、资产类型、生效时长、厂商、位置等信息来制定黑/白名单，便于日常资产管理。</p>
2	防火墙②	<p>2 台</p> <p>▲1. 多核 AMP+架构，标准 2U 设备，冗余电源；配置≥6 个 10/100/1000M 自适应电口，4 个 SFP 插槽（含 4 个千兆多模光模块），另有 2 个接口板卡扩展插槽，1 个 Console 口，支持液晶屏，配置 128GB 的 SSD 硬盘，含 3 年硬件质保和 IPS 入侵防御、病毒防护升级服务；</p> <p>▲2. 防火墙吞吐≥10Gbps，并发连接数≥260 万，每秒新建连接数≥18 万/</p>

		<p>秒，包含应用控制、URL 过滤、病毒防护、入侵防御、威胁情报检测等功能模块；</p> <p>3. 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；</p> <p>4. 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；</p> <p>5. 支持基于 IP、应用、服务的策略路由进行智能选路，支持源地址目的地址哈希、源地址哈希、时延负载、最优链路带宽负载、最优链路带宽备份、跳数等不少于 12 种路由负载均衡方式；</p> <p>6. 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；</p> <p>▲7. 必须支持对应用层 Flood 攻击提供多种防护措施，包括：告警、丢弃、普通防护、增强防护及授权设备防护等；</p> <p>8. 产品必须支持 DS-Lite CPE B4 功能，支持成为 b4 或 aftr 角色，支持从 DHCPv6 设备或手动方式获取 AFTR 参数；</p> <p>9. 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；</p> <p>10. 产品支持共享上网检测功能，支持共享接入检测和共享接入管控功能，可以通过设置管控地址和例外地址优化管控功能，同时支持阻断或告警动作；</p> <p>11. 产品支持对最多 6 级的压缩文件进行解压查杀；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；</p> <p>▲12. 需支持与云端联动，至少实现病毒云查杀、URL 云识别、应用云识别、云沙箱、威胁情报云检测等功能；</p> <p>13. 产品支持支持漏洞防护功能，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；</p>
--	--	--

		<p>14. 产品支持 IPv4 和 IPv6 流量的 HTTPS、POP3S、SMTPS、IMAPS 协议进行解密，支持配置基于源安全域、目的安全域、源地址、目的地址、SSL 协议服务的解密策略，动作可以设置解密或不解密，并可基于安全域、IPv4 和 IPv6 地址进行例外设置；</p> <p>▲15. 必须支持与杀毒软件或终端管理软件联动，实现基于终端健康状态的访问控制；</p> <p>16. 支持基于主机或威胁情报视图，统计网络中确认被入侵、攻破的主机数量，至少可查看被入侵、攻破的时间、威胁类别、情报来源、威胁简介、被入侵、攻破的主机 IP、用户名、资产等信息；并对威胁情报发现的恶意主机执行自动阻断；</p> <p>17. 须支持接收针对突发重大安全事件的“应急响应消息”，针对该消息可以选择“自动”或“手动”处理，处置方法至少包括基于漏洞的处置和基于威胁情报的处置；</p> <p>18. 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，产品需支持限制特定主机调用 Restful API；</p> <p>19. 须支持业务接口下 Netflow 功能，能够通过 Netflow 实现对网络进行监控，对接口流量进行抓包，并在可将 Netflow 抓包文件数据外发；</p> <p>20. 须支持资产管理，能够通过设置资产监控、VPN、源安全域来控制资产识别范围，支持 scanner 或 onvif 类型的扫描方式和网段，实现自动或手动资产扫描；支持通过设置 IP 地址、MAC 地址、资产类型、生效时长、厂商、位置等信息来制定黑/白名单，便于日常资产管理。</p>
3	安全管理防火墙	<p>2 台</p> <p>▲1. 多核 AMP+架构，标准 2U 设备，冗余电源；配置≥6 个 10/100/1000M 自适应电口，4 个 SFP 插槽（含 4 个千兆多模光模块），另有 2 个接口板卡扩展插槽，1 个 Console 口，支持液晶屏，配置 128GB 的 SSD 硬盘，含 3 年硬件质保和 IPS 入侵防御、病毒防护升级服务；</p> <p>▲2. 防火墙吞吐≥10Gbps，并发连接数≥260 万，每秒新建连接数≥18 万/秒，包含应用控制、URL 过滤、病毒防护、入侵防御、威胁情报检测等功能模块；</p> <p>3. 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；</p> <p>4. 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；</p>

		<p>5. 支持基于 IP、应用、服务的策略路由进行智能选路，支持源地址目的地址哈希、源地址哈希、时延负载、最优链路带宽负载、最优链路带宽备份、跳数等不少于 12 种路由负载均衡方式；</p> <p>6. 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；</p> <p>▲7. 必须支持对应用层 Flood 攻击提供多种防护措施，包括：告警、丢弃、普通防护、增强防护及授权设备防护等。</p> <p>8. 必须支持 DS-Lite CPE B4 功能，支持成为 b4 或 aftr 角色，支持从 DHCPv6 设备或手动方式获取 AFTR 参数；</p> <p>9. 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；</p> <p>10. 支持共享上网检测功能，支持共享接入检测和共享接入管控功能，可以通过设置管控地址和例外地址优化管控功能，同时支持阻断或告警动作。</p> <p>11. 支持对最多 6 级的压缩文件进行解压查杀；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；</p> <p>▲12. 需支持与云端联动，至少实现病毒云查杀、URL 云识别、应用云识别、云沙箱、威胁情报云检测等功能；</p> <p>13. 支持支持漏洞防护功能，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；</p> <p>14. 支持 IPv4 和 IPv6 流量的 HTTPS、POP3S、SMTPS、IMAPS 协议进行解密，支持配置基于源安全域、目的安全域、源地址、目的地址、SSL 协议服务的解密策略，动作可以设置解密或不解密，并可基于安全域、IPv4 和 IPv6 地址进行例外设置；</p> <p>▲15. 必须支持与杀毒软件或终端管理软件联动，实现基于终端健康状态的访问控制；</p> <p>16. 支持基于主机或威胁情报视图，统计网络中确认被入侵、攻破的主机数量，至少可查看被入侵、攻破的时间、威胁类别、情报来源、威胁简介、</p>
--	--	---

		<p>被入侵、攻破的主机 IP、用户名、资产等信息；并对威胁情报发现的恶意主机执行自动阻断；</p> <p>17. 需支持接收针对突发重大安全事件的“应急响应消息”，针对该消息可以选择“自动”或“手动”处理，处置方法至少包括基于漏洞的处置和基于威胁情报的处置；</p> <p>18. 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，产品需支持限制特定主机调用 Restful API；</p> <p>19. 支持业务接口下 Netflow 功能，能够通过 Netflow 实现对网络进行监控，对接口流量进行抓包，并在可将 Netflow 抓包文件数据外发；</p> <p>20. 支持资产管理，能够通过设置资产监控、VPN、源安全域来控制资产识别范围，支持 scanner 或 onvif 类型的扫描方式和网段，实现自动或手动资产扫描；支持通过设置 IP 地址、MAC 地址、资产类型、生效时长、厂商、位置等信息来制定黑/白名单，便于日常资产管理。</p>
4	威胁态势感知流量采集探针	1 台 <p>▲1. 标准 2U 机架式设备，配置 6 个千兆网口，单电源，1TB 企业硬盘。含系统软件一套，含 3 年产品维保服务；</p> <p>▲2. 系统吞吐量≥1Gbps，含 3 年威胁情报更新授权与规则升级授权及产品维保服务；</p> <p>3. 支持常见协议识别并还原网络流量，用于取证分析、威胁发现，支持：http、dns、smtp、pop3、imap、webmail、DB2、Oracle、MySQL、sql server、Sybase、SMB、FTP、SNMP、telnet、nfs、ICMP、SSL、SSH 等；</p> <p>4. 支持对流量中出现文件传输行为进行发现和还原，并记录文件 MD5 发送至分析设备，如可执行文件（EXE、DLL、OCX、SYS、COM、apk、bin 等）、压缩格式文件（RAR、ZIP、GZ、7Z、tar 等）、文档类型文件（word、excel、pdf、rtf、ppt、txt 等）；</p> <p>5. 支持常见数据库协议的识别或还原：DB2、Oracle、SQL Server、MySQL、PostgreSQL 等协议；</p> <p>◆6. 支持自定义协议和端口，满足特殊场景下的流量抓取；</p> <p>7. 支持基于流量实时 IOC 匹配功能，设备具备主流的 IOC，情报总量 200+ 万条；</p> <p>8. 支持基于 webshell 函数的攻击检测，如文件包含漏洞、任意文件写入、任意目录读取、任意文件包含、preg_replace 代码执行等；</p> <p>◆9. 支持基于工具特征的 WEBSHELL 检测，能通过系统调用、系统配置、文件的操作来及时发现威胁；如：中国菜刀、小马上传工具、小马生成器等；</p>

		<p>10. 支持多种攻击检测，能更全面的从流量中发现威胁，如：SQL 注入、XSS、信息泄露、间谍软件、协议异常、网络欺骗、黑市工具、代码执行等；</p> <p>11. 具备数据包完整性检测、碎片重组检测、编码检测能力、高级逃逸 AET 检测等防逃逸检测能力；</p> <p>◆12. 支持基于网络请求的语义分析检测，能够将网络请求拆分后从请求头、响应头、请求体、响应体等四方面请求内容，提升对未知威胁检测能力；</p> <p>13. 支持基于 IP 地址的旁路阻断，能够在实时镜像的流量中发现恶意 IP 并实现实时阻断；</p> <p>14. 支持 AES256、SM4 数据传输加密，确保数据传输的安全性；</p> <p>15. 支持自定义弱口令字典，支持 HTTP、HTTPS、Telnet、FTP、POP、SMTP、IMAP 等协议的自定义弱口令检测；</p> <p>16. 支持威胁告警信息发送给 syslog 设备，支持将威胁告警、威胁等级、网络日志、攻击结果、威胁类型等日志传输给 KAFKA、威胁分析平台；</p> <p>17. 支持与安全分析平台进行联动，统一进行情报、规则的升级。</p>
5	威胁态势感知系统分析平台	<p>1 台</p> <p>▲1. 标准 2U 机架式设备，配置≥4 个千兆电口，内存≥128G，≥3 个 USB3.0 接口，≥1 个 DB9 Console 接口，冗余电源，960G SSD + 8*4TB SATA 存储硬盘。含 3 年威胁情报更新授权及产品维保服务；</p> <p>▲2. 处理能力≥10,000eps；</p> <p>3. 支持告警的深度行为分析，行为包括 DNS 解析行为、TCP/UDP 交互行为、WEB 访问行为、传输文件行为；</p> <p>4. 支持以攻击者的维度进行分析，对攻击者进行画像，画像内容包括地理位置信息、国家信息、所属组织、使用的攻击手段、攻击的所有资产；</p> <p>5. 支持从威胁情报、应用安全、系统安全和设备安全的业务场景维度对告警进行攻击带外分析；</p> <p>6. 威胁情报维度分析包括：情报详情、影响资产列表、资产的行为（行为包含：DNS 解析、TCP 流量、UDP 流量、WEB 访问、文件传输）；</p> <p>7. 应用安全的细分维度包括：WEB 安全、数据库安全、中间件安全；系统安全的细分维度包括：暴力破解、弱口令、未授权访问、挖矿行为；</p> <p>◆8. 支持对告警进行加白，加白参数包括受害 IP、攻击 IP、威胁情报、规则、XFF、URL、威胁名称；</p> <p>9. 支持与云端威胁情报中心联动，可对攻击 IP、C&C 域名和恶意样本 MD5 进行一键搜索，查看基本信息、相关样本、关联 URL、可视化分析、域名解析、注册信息、关联域名、数字证书等；</p>

		<p>10. 支持可疑代理分析：能够发现 socks、http、reDuh、Regeory Tunnel、Tunna 等代理类型；</p> <p>11. 支持异常登录行为检测，检测内容包括：源 ip、账号、登录资产 IP、使用协议、登录结果等信息，且能进行异常时间配置；</p> <p>12. 支持明文密码泄露行为检测，检测内容包含：登录账号 IP、账号、密码、使用协议；</p> <p>13. 支持非常用请求方法分析，展示源 ip、目的 ip、域名、访问链接、请求方法、状态码、最近访问时间等信息；</p> <p>14. 支持对 mysql、mssql、oracle、sybase 等常见数据库高危操作行为分析，其能自定义规则；</p> <p>15. 支持检索异常报文、域名解析、文件传输、FTP 控制通道、LDAP 行为、登录动作、邮件行为、MQ 流量、网络阻断、数据库操作、SSL 加密协商、TCP 流量、Telnet 行为、UDP 流量、WEB 访问等网络流量日志，并可基于时间、IP、端口、协议、上下行负载等多重字段组合进行日志检索；</p> <p>16. 支持对任意线索的自定义拓线及溯源取证分析，支持以可视化分析画布形式展示拓线过程并支持结果快照导出；支持对于给定线索的溯源结果展示，包括但不限于攻击溯源、失陷主机分析、暴力破解分析、弱口令分析等；</p> <p>17. 支持大屏展示网络攻击态势，包括整体网络风险指数、告警总数、攻击次数、攻击 IP 数、攻击源国家/地区 TOP5、攻击态势，并支持自动翻转的攻击全景地图展示；</p> <p>18. 支持大屏展示整体资产风险态势，包含资产树结构、资产分类、开放服务统计、网段管理、资产风险趋势、资产风险状态；</p> <p>◆19. 支持工作流程自定义编排，支持联动服务管理，支持 python 语言与 javascript 语言在 web 页面编辑联动服务；</p> <p>20. 支持编排处置日志记录，记录处置时间、受害 ip、攻击 ip、告警类型、威胁名称、域名、处置策略、告警来源等信息；</p> <p>21. 提供告警展示场景，支持展示场景的切换。每个告警展示场景中支持自定义页面数据展示的范围，方便管理人员的日常运维工作；</p> <p>◆22. 支持与防火墙进行联动，发现威胁事件后支持对攻击 IP、恶意域名和受害资产的流量进行阻断（将策略下发给防火墙，由防火墙执行阻断）；</p> <p>23. 支持与同品牌终端安全管理软件（云锁服务器安全管理系统（私有云版）客户端功能授权）进行联动，发现威胁事件后支持与控制中心进行指令下发执行终端隔离和扫描操作。</p>
--	--	--

6	云锁服务器安全管理系统（私有云版）客户端功能授权	60 套 <p>1. 为了保证采购人业务的连续性，要求云锁服务器安全管理系统可无缝对接采购人原有系统并进行扩容无须重启，本次扩容包含 60 点授权及三年升级维保服务。</p> <p>▲2. 支持 Windows Server 2003 sp2/R2 x86/x64、Windows Server 2008 sp1 及以上/R2 x86/x64、Windows Server 2012~2019 sp1 及以上/R2 x86/x64、CentOs 5.0 及以上 x86/x64、RHEL 5.5 及以上 x86/x64、Ubuntu 14.04 及以上 x86/x64、SUSE 11 及以上版本 x86/x64 等操作系统；</p> <p>3. 支持自我防护技术，即使客户端被意外关闭，防护依然有效；</p> <p>4. 支持全量资产的关键字及语法搜索，支持检索的语法包括但不限于：服务器资产类、进程资产类、账号资产类、软件应用类、web 资产类、web 服务类、web 框架、数据库类、端口资产类、网络连接类、启动服务类、安装包类、计划任务类、环境变量类、内核类、类库资产类、注册表类、证书资产类进行检索。支持至少 5 个搜索历史的保存；</p> <p>5. 支持以列表的形式，统一列出 Windows/Linux 服务器的进程连接资产，并可查看进程名称、协议、IP 地址、源端口、目标端口、目标 IP、连接状态、同步时间等信息；</p> <p>6. 可通过自动、手动的任务设置，对局域网内服务器的服务器进行扫描（支持 ARP、Ping、Nmap 扫描方式，并支持离线分析），并自动获取服务器相关信息，包括 MAC 地址、设备类型、未知主机 IP、操作系统、发现方式、首次发现时间等信息；</p> <p>7. 学习每台服务器的网络外连行为、命令执行行为、文件创建行为，并形成图形化的时间轴行为基线，对于偏离行为以外的动作进行告警；</p> <p>8. 支持服务器防火墙功能，可对服务器定制访问策略，包括允许本地 IP/端口访问指定 IP/端口、禁止本地 IP/端口访问指定 IP/端口，并可设置访问放心，并支持 TCP、UDP、ICMP 等协议。并根据设置的规则进行访问告警；</p> <p>◆9. 支持设置端口的暴露控制规则，包括但不限于：禁止/允许外网暴露、禁止/允许内网暴露等策略，并支持例外端口的添加；</p> <p>◆10. 可对服务器杀毒引擎进行设置，支持本地查杀、控制中心查杀的设置与切换，并可对某台服务器的查杀规则进行详细设置；</p> <p>11. 以攻击者视角、受害者视角展示恶意扫描的事件，包括：服务器名称、负责人、所属部门、操作地址、最近发生时间、受害 IP、攻击 IP 等信息，并将事件加入黑名单或白名单，还可对受害的 IP 进行防端口扫描、屏蔽扫描器等设置；</p> <p>12. 支持对内存堆栈调用行为特征的分析，可有效检测常见工具的内存</p>
---	--------------------------	--

		<p>WebShell 攻击，并对内存攻击行为告警及处置；</p> <p>13. 支持查看提权的详情，并以图形化的形式展示提权进程树信息，用于本地提权的溯源；</p> <p>14. 支持 OOB 带外攻击检测，并支持黑域名的添加与同步；</p> <p>15. 支持实时监控服务器上发生的无文件攻击（漏洞型攻击、灰色工具型攻击、潜伏型攻击）事件，并对无文件攻击事件进行加白、标记处置等操作；</p> <p>16. 支持 RASP（应用运行时自防护），可通过将脚本解析器语言注入到 ASP、PHP、Java 语言中，并细粒度的监控应用脚本行为及函数调用上下文信息，对上下文信息进行分析判断，及时发现恶意代码和漏洞利用行为；</p> <p>17. 支持通过插件的方式，工作于 IIS、Apache、Nginx 等 web 中间件内部，通过判断流量特征和 WAF 规则引擎，对访问流量进行监控或防护，阻断 SQL 注入、XSS、漏洞利用等 Web 攻击；</p> <p>▲18. 可对系统防护（包括但不限于：文件监控与防护、操作系统加固、入侵检测）、应用防护（包括但不限于：高级防护、应用漏洞防护、URL 控制）、网络防护（防端口扫描、微蜜罐）进行统一的设置及模板管理，并对各类防护策略以模板形式下发；</p> <p>19. 支持记录当前所有服务器产生的事件日志，并支持全量日志的关键字及语法搜索，支持检索的语法包括但不限于：服务器相关参数、访问主体相关参数、网络相关参数、操作相关参数、客体相关参数、登陆日志相关参数等进行检索，并支持返回上次筛选的关键词；</p> <p>20. 支持以柱状图的形式展示某段时间内的日志数量，并在柱状图下方展示具体的日志事件，并在日志上方以标签形式展示服务器名称、IP 地址、日志类型、日志等级、拦截状态等信息；可查看某条日志的具体攻击全路径。</p>
7	防火墙(出口)	<p>1 台</p> <p>▲一、性能参数：</p> <p>1. 性能参数：网络层吞吐量：≥20G，应用层吞吐量：≥8G，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：≥220 万，HTTP 新建连接数：≥15 万，SSL VPN 推荐用户数 IPSec 最大隧道数：1000，IPSec VPN 吞吐量：≥400M；</p> <p>2. 硬件参数：采用多核并行处理架构；规格：1U，内存大小：≥8G，配置 3 块≥32G 内存条性能不足时备用，硬盘容量：≥128G minisata SSD，电源：单电源，接口：10 千兆电口+6 千兆光口 SFP。开通 WEB 应用、IPS 防护、网关杀毒功能，包含 3 年软件升级、硬件质保、规则库升级服务。</p> <p>二、功能参数：</p> <p>1. 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</p>

		<p>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；</p> <p>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；</p> <p>3. 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；</p> <p>4. 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；</p> <p>▲5. IPsec VPN 智能选路功能，根据线路质量实现线路自动切换；</p> <p>6. 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；</p> <p>7. 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；</p> <p>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；</p> <p>9. 可扩展防病毒模块，支持对 SMTP、HTTP、FTP、SMB、POP3、HTTPS、IMAP 等协议进行病毒防御；</p> <p>10. 可扩展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；</p> <p>▲11. 支持入侵防御功能，预定义漏洞特征数量超过 9000 种；</p> <p>12. 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；</p> <p>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；</p> <p>▲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；</p> <p>◆15. 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；</p>
--	--	--

		<p>▲16.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;</p> <p>17.产品支持主主、主备两种双机模式部署;</p> <p>▲18.支持和医院原来出口防火墙组成双机部署,形成主主运行模式,当一台设备出现故障时另一台无缝接管,不中断业务;</p> <p>◆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;</p> <p>▲20.须作为安全组件接入医院正在使用的的安全感知管理平台,并进行功能联动,结合此次扩容的安全运营服务进行联动封锁、访问控制。</p>
8	上网行为审计系统	<p>1台</p> <p>▲一、AC性能参数:</p> <p>1.性能参数:网络层吞吐量:≥10Gb,应用层吞吐量:≥1.5Gb,带宽性能:≥1Gb,IPSEC VPN加密性能(最高性能):≥200Mb,支持用户数:≥6000,包转发率:≥132Kpps,每秒新建连接数:≥14000条,最大并发连接数:600000条;</p> <p>2.硬件参数:规格:1U,内存大小:≥8G,配置3块≥32G内存条性能不足时备用;硬盘容量:≥64G SSD+960G SSD,电源:单电源,接口:6千兆电口+2万兆光口 SFP+。包含3年软件升级、硬件质保、规则库升级服务。</p> <p>二、AC功能参数:</p> <p>▲1.须保障设备可靠性,必须支持两台及两台以上设备同时做主机的部署模式;</p> <p>▲2.须满足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;</p> <p>▲3.为提高运维管理效率,降低运维难度,须提供图形化排障工具,便于管理员排查策略错误等故障;</p> <p>◆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;</p> <p>◆5.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;</p> <p>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;</p> <p>▲7.为便于及时掌握网内情况及问题排查,须支持查看当前设备的线路状</p>

			<p>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；</p> <p>8. 为帮助及时掌握用户 WEB 访问质量，须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</p> <p>9. 须支持通过 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；</p> <p>10. 须支持 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；</p> <p>▲11. 须能够对新浪微博、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；</p> <p>▲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）；</p> <p>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；</p> <p>◆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；</p> <p>▲15. 为构建统一安全运营服务中心，所投产品须开通接口与安全运营平台对接，达到安全威胁及时发现上报，安全管理中心能实时对设备进行风险预警告知和安全策略下发处置；</p> <p>▲16. 须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。</p>
9	防火墙③	2 台	<p>▲一、性能参数：</p> <p>1. 性能参数：网络层吞吐量：≥30G，应用层吞吐量：≥15G，防病毒吞吐量：≥2.5G，IPS 吞吐量：≥2.5G，全威胁吞吐量：≥1.7G，并发连接数：≥410 万，HTTP 新建连接数：≥16 万，SSL VPN 推荐用户数（单独购买）：≥35 条，SSL VPN 最大用户数（单独购买）：120 条，SSL VPN 最大理论加密流量（单独购买）：300M，IPSec VPN 最大接入数：4000 条，IPSec VPN 吞吐量：1.2G。</p> <p>2. 硬件参数：产品采用多核并行处理架构，规格：2U，内存大小：≥16G，</p>

		<p>配置 3 块≥32G 内存条性能不足时备用；硬盘容量：≥64G SSD+480G SSD，电源：冗余电源，接口：16 千兆电口+6 万兆光口 SFP+、含 6 个光纤线-多模-LC-LC-3M;6 个万兆多模-850-300m-双纤。开通 WEB 应用、IPS 防护、网关杀毒功能，包含 3 年软件升级、硬件质保、规则库升级服务。</p> <p>二、功能参数：</p> <ol style="list-style-type: none">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. 可扩展防病毒模块，支持对 SMTP、HTTP、FTP、SMB、POP3、HTTPS、IMAP 等协议进行病毒防御；10. 可扩展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. 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、
--	--	--

		<p>MSSQL 等应用协议进行深度检测与防护；</p> <p>▲14. 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；</p> <p>◆15. 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；</p> <p>▲16. 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；</p> <p>▲17. 支持主主、主备两种双机模式部署，为构建统一安全运营服务中心，所投产品须开通接口与安全运营平台对接，达到安全威胁及时发现上报，安全管理中心能实时对设备进行风险预警告知和安全策略下发处置；</p> <p>18. 支持网站防篡改功能，可防止攻击者非授权篡改文件系统。支持网页恶意链接检测功能，有效识别网页盗链/黑链的行为，避免用户网页资源被滥用；</p> <p>▲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。</p>
10	日志审计系统	<p>1 台</p> <p>▲一、性能参数：</p> <p>1. 性能参数：默认包含主机审计许可证书数量：≥200 条，最大可扩展审计主机许可数：≥450 条，可用存储量：≥4TB（RAID1 模式），平均每秒处理日志数（eps）最大性能：≥2000 条；</p> <p>2. 硬件参数：规格：2U，内存大小：≥32G，配置 3 块≥32G 内存性能不足时备用；硬盘容量：≥64G minisata+4T SATA2 块，电源：单电源，接口：6 千兆电口+2 万兆光口 SFP+。包含 3 年软件升级、硬件质保、规则库升级服务。</p> <p>二、功能参数：</p> <p>1. 支持安全设备、网络设备、中间件、服务器、数据库、操作系统、业务系统等不少于 720 种日志对象的日志数据采集；</p> <p>◆2. 支持通过 syslog、SNMP Trap、JDBC、WMI、webservice、FTP、文件\文件夹读取、Kafka 等多种方式完成日志收集；</p> <p>▲3. 支持通过正则、分隔符、json、xml 的可视方式进行自定义规则解析，支持对解析结果字段的新增、合并、映射；</p> <p>4. 支持日志文件备份到外置存储节点，支持 NFS、NAS、ISCSI 三种存储方式，并可查看外置存储容量、状态等信息；</p> <p>▲5. 支持通配符、范围搜索、字段等多种输入方式、搜索框模糊搜索、指</p>

		<p>定语段进行语法搜索；可根据时间、严重等级等进行组合查询；可根据具体设备、来源/目的所属（可具体到外网、内网资产等）、IP 地址、特征 ID、URL 进行具体条件搜索；支持可设置定时刷新频率，根据刷新时间显示实时接入日志事件；</p> <p>◆6. 支持解码小工具，按照不同的解码方式解码成不同的目标内容，编码格式包括 base64、Unicode、GBK、HEX、UTF-8 等；</p> <p>▲7. 支持单条事件进行展开，显示事件详细信息和事件原始信息，支持事件详情中任意字段作为查询条件无限制进行二次检索分析；</p> <p>8. 支持内置规则作为模板新建规则，支持调整规则等级，支持通过事件的任意字段制定规则创建策略，支持审计策略命中后可以定义告警并通过相应方式转发，如：邮件、短信等；</p> <p>9. 为构建统一安全运营服务中心，要求所提供产品开通接口与安全运营平台对接，达到安全威胁及时发现上报，安全管理中心能实时对设备进行风险预警告知和安全策略下发处置；</p> <p>10. 内置主机安全报表（linux）、主机安全报表（windows）、数据库安全报表、网络设备安全报表、应用安全报表五种；支持提供日报、周报、月报和自定义时间导出报表；</p> <p>11. 支持可视化展示，包括数据分布、安全事件趋势图、关联规则告警趋势图、接入设备概况等，可提供设备专项分析场景。如防火墙外部攻击场景分析、VPN 账号异常场景分析、Windows 服务器主机异常场景分析等，通过设备专项页面对每一台设备安全情况深度专业化分析；</p> <p>12. 提供管理员账号创建、修改、删除，并可针对创建的管理员进行权限设置；支持 IP 免登录，指定 IP 免认证直接进入平台；支持只允许某些 IP 登录平台；支持页面权限配置和资产范围配置，用于管理账号权限，满足用户三权分立的需求；支持 usb-key 认证。</p>
11	云镜网络资产脆弱性扫描系统(漏扫)	<p>▲一、性能参数：</p> <p>1. 性能指标：系统漏扫授权 IP 数：≥2000 条，WEB 漏扫授权 URL 数：≥400 条；性能指标：主机漏扫最大并发 IP 数：≥120 条，WEB 漏扫最大并发 URL 数：≥10 条。</p> <p>2. 硬件参数：规格：2U，内存大小：16G，配置 3 块 32G 内存性能不足时备用；硬盘容量：128GB SSD+ 2TB SATA，电源：冗余电源，接口：6 千兆电口+2 万兆光口 SFP+。包含 3 年软件升级、硬件质保、规则库升级服务。</p> <p>二、功能参数：</p> <p>1. 支持全局风险统计功能，通过扇形图、条状图、标签、表格等形式直观</p>

		<p>展示资产风险分布、漏洞风险等级分布等信息，并可查看详情；</p> <p>2. 支持全局风险统计时段自定义，展示近 3 个月、6 个月、1 年或自定义统计区间的风险分布和详情，时间跨度不限制；</p> <p>3. 支持从“高危”、“中危”、“低危”、“安全”四个安全级别展示资产的风险分布情况；</p> <p>4. 支持从主机视角呈现当前关键资产的漏洞风险信息，可从“高”、“中”、“低”、“信息”四个等级划分漏洞风险等级，支持客户对于重要资产标记为“核心资产”，便于根据资产价值确定修复优先级；</p> <p>◆5. 支持全面扫描、资产发现、系统漏洞扫描、弱口令扫描、WEB 漏洞扫描、基线配置核查六种任务类型；</p> <p>6. 支持资产发现功能，可基于 IP 地址、IP 网段、IP 范围、URL 等方式进行资产发现扫描，支持 EXCEL 格式批量导入；</p> <p>7. 支持检测的漏洞数大于 10000 条，兼容 CVE、CNNVD、CNVD、Bugtraq 等主流标准；</p> <p>8. 支持紧急漏洞进行单独评估，实现紧急漏洞批量排查，包括 Microsoft Windows RDP 远程代码执行漏洞(CVE-2019-0708)、OpenSSL Heartbleed 心脏滴血漏洞 (CVE-2014-0160)、Windows SMB 远程代码执行漏洞 (MS08-067)、Windows SMB 远程代码执行漏洞 (MS17-010) 等；</p> <p>9. 内置不同的系统漏洞模板，包括高可利用系统漏洞、原理检测系统漏洞、中间件漏洞、数据库漏洞等类型，支持报表形式展示漏洞模板风险等级分布概览；</p> <p>10. 系统漏洞扫描支持高级配置功能，可支持端口扫描策略配置、UDP 扫描启用、危险插件扫描启用等配置功能；</p> <p>11. 系统漏洞扫描支持任务立即执行和指定时间执行两种执行方式，且指定时间可以精确到分钟；</p> <p>12. 支持行业通用标准 OWASP，支持通用 WEB 漏洞检测，如：SQL 注入、XSS、目录遍历、本地/远程文件包含漏洞、安全配置错误、命令执行、敏感信息泄露等；</p> <p>13. 内置不同的 WEB 漏洞模板，包括高可利用 WEB 漏洞、通用应用漏洞、SQL 注入漏洞、XSS 注入漏洞等类型，支持报表形式展示漏洞模板风险等级分布概览；</p> <p>14. WEB 漏洞扫描支持高级配置功能，可支持 fuzz 测试启用、WEB 访问策略、WEB 爬行策略等配置功能。支持并发线程数、超时限制、目录深度、链接总数自定义配置；</p>
--	--	--

		<p>◆15. 支持对系统漏洞、WEB 漏洞、基线配置、弱口令进行扫描和分析，可同时输出包含系统漏洞扫描、WEB 漏洞扫描、基线配置核查、弱口令扫描结果的报表；</p> <p>▲16. 为构建统一安全运营服务中心，所投产品须开通接口与安全运营平台对接，达到安全威胁及时发现上报，安全管理中心能实时对设备进行风险预警告知和安全策略下发处置。</p>
12	运维安全管理系统（堡垒机）	1 台 <p>▲一、性能参数：</p> <p>1. 性能参数：默认包含运维授权数：≥200 条，最大可扩展资产数：≥1000 条，图形运维最大并发数：≥200 条，字符运维最大并发数：≥350 条；</p> <p>2. 硬件参数：规格：2U，内存大小：≥8G，配置 3 块≥32G 内存条性能不足时备用；硬盘容量：≥64GB SSD+2TB SATA，电源：单电源，接口：6 千兆电口+2 万兆光口 SFP+。包含 3 年软件升级、硬件质保、规则库升级服务。</p> <p>二、功能参数：</p> <p>1. 物理旁路单臂部署，以逻辑网关方式工作；不改变现有网络结构</p> <p>◆2. 支持从 windows AD 域抽取用户账号作为主账号，支持一次性抽取和周期性抽取两种方式；</p> <p>3. 支持一对一、一对多、多对多授权，如将单个资产授权多个用户，一个用户授予多个资产，用户组向资产组授权；</p> <p>4. 同时支持本地口令认证、LDAP 认证、AD 认证、短信认证、Radius、usbkey、动态口令认证；</p> <p>◆5. 支持定期变更目标设备真实口令，支持自定义口令变更周期和口令强度。口令变更方式至少支持手动指定固定口令、通过密码表生成口令、依照设备挂载的口令策略生成随机口令、依照密码策略生成同一口令等方式；</p> <p>6. 支持密码策略设置，可自定义密码复杂程度，可设置密码中包含数字、字母、符号及禁用关键字等内容；</p> <p>7. 支持口令有效期设置，用户账号口令到期强制用户修改自身口令；</p> <p>8. 支持运维审计自查询功能，用户可查看自身的运维审计历史；</p> <p>9. 支持自定义报表，可记录审计报表模板，可生成图形报表，并提供 EXCAL、CSV、WORD、PDF、HTML 等格式导出；</p> <p>10. 支持 windows 系统、网络设备、linux/unix 系统、数据库等设备账号的收集功能；</p> <p>11. 全面支持 Windows、linux、国产麒麟系统、Android、IOS、Mac OS 等客户端，实现跨终端适应性 BYOD (Bring Your Own Device)；</p> <p>12. 支持云端快速部署，实现远程运维管理的规范化；可按照运维人员数量，</p>

		<p>调整云端服务器配置；</p> <p>13. 支持告警对外转发，转发方式支持 syslog、SNMP 等方式；</p> <p>14. 支持 NTP 系统时间同步配置，保证审计日志拥有可靠的时间戳；</p> <p>15. 支持手动和自动定期备份配置信息，支持配置信息本地备份及异地 FTP 备份，支持系统配置还原，可以还原至任意备份点。</p>
13	安全运营服务	<p>1 套</p> <p>▲1. 服务资产数量：≥100 IP 资产；服务频率：1 年，7*24 小时；</p> <p>▲2. 需配置态势感知平台、防火墙、上网行为审计、终端杀毒软件、VPN、云镜资产脆弱扫描系统、日志审计等安全设备，通过其发现的资产信息，首次进行服务范围内资产的全面梳理（梳理的信息包含支撑业务系统运转的操作系统、数据库、中间件、应用系统的版本，类型，IP 地址；应用开放协议和端口；应用系统管理方式、资产的重要性以及网络拓扑），并将信息录入到安全运营平台中进行管理；当资产发生变更时，安全专家对变更信息确认与更新；</p> <p>3. 漏洞优先级排序：投标方需提供客观的漏洞修复优先级指导，不能以漏洞危害等级作为唯一的修复优先级排序依据。排序依据包含但不限于资产重要性、漏洞等级以及威胁情报（漏洞被利用的可能性）三个维度；</p> <p>4. 漏洞验证：提供漏洞验证服务，针对发现的漏洞进行验证，验证漏洞在已有的安全体系发生的风险及分析发生后可造成的危害。针对已经验证的漏洞，自动生成漏洞工单，安全专家跟进漏洞状态，各个处理进度透明，方便招标方清晰了解当前漏洞的处置状态，将漏洞处理工作可视化；</p> <p>5. 漏洞修复建议：针对存在的漏洞提供修复建议，能够提供精准、易懂、可落地的漏洞修复方案；</p> <p>6. 服务催单：针对服务平台生成的工单，招标方可按需催单，服务平台采用短信等方式通知安全专家，督促供应商第一时间处理；</p> <p>◆7. 漏洞复测：需提供漏洞复测措施，及时检验漏洞真实修复情况。复测措施可按需针对指定漏洞，指定资产等小范围进行，降低漏洞复测时的潜在影响范围；</p> <p>◆8. 对发现的漏洞建立状态追踪机制，自动化持续跟踪漏洞情况，清晰直观地展示漏洞的修复情况，遗留情况以及漏洞对比情况，使得采购人可做到漏洞的可视、可管、可控；</p> <p>9. 实时监测网络安全状态，对攻击事件自动化生成工单，及时进行分析与预警。攻击事件包含境外黑客攻击事件、暴力破解攻击事件、持续攻击事件；</p> <p>10. 策略调整：安全专家根据安全事件分析的结果以及处置方式，根据用户</p>

		<p>授权情况按需对安全组件上的安全策略进行调整工作；</p> <p>11. 基于主动响应和被动响应流程，对页面篡改、通报、断网、webshell、黑链等各类严重安全事件进行应急响应和处置的解决方案；</p> <p>12. 须为用户提供服务监控门户，在门户中用户可查看业务安全状态，处置中的失陷事件以及针对这些事件的处置进度，处置责任人、联系方式等信息，方便用户时刻了解投标方的服务效果；</p> <p>13. 须有可视化的措施监督安全专家的服务水平，从工单的响应、工单的审核以及工单处理等维度判断服务是否出现停滞；</p> <p>14. 服务进度督促：针对服务平台生成的工单，招标方可按需催单，服务平台采用短信方式通知安全专家，督促供应商第一时间处理；</p> <p>15. 通过态势感知系统，可随时查看业务资产安全状态，在线展示所有事件监测结果、防御过程和防御结果；</p> <p>◆16. 本项目使用服务工具支持将收集的安全日志上传到态势感知系统上，并支持在该平台上对服务工具进行管理；</p> <p>17. 为了保证安全监测的效果，需要态势感知系统具备检测规则的自定义功能，以满足日益复杂的安全趋势所带来的安全需求；</p> <p>▲18. 交付内容：</p> <p>(1) 交付物名称：《安全服务运营报告》，报告频率：每周一次；</p> <p>(2) 交付物名称：《首次威胁分析与处置报告》，报告频率：共一次；</p> <p>(3) 交付物名称：《事件分析与处置报告》，报告频率：按采购人需求提供，不限次数；</p> <p>(4) 交付物名称：《安全通告》，报告频率：按需触发，不限次数；</p> <p>(5) 交付物名称：《综合分析报告》，报告频率：每月一次；</p> <p>(6) 交付物名称：《季度汇报 PPT》，报告频率：每季度一次；</p> <p>(7) 交付物名称：《年度汇报 PPT》，报告频率：每年一次；</p> <p>说明：中标人中标后须按照上述频率要求提供服务成果，确保满足采购人的安全需求。如中标人未能按时提供服务成果，采购人有权终止合同，中标人将承担一切后果并赔偿采购人因此产生的全部损失。</p>
▲商务要求		
质保期	按国家有关规定实行“三包”，除招标文件有特别规定外，保修期不少于 1 年。	
售后技术服务要求	<p>1. 按国家有关产品“三包”规定执行“三包”，免费送货上门、免费进行安装调试。保修期内免费提供售后服务，不收取维修、差旅、零配件等一切费用。保修期满后，中标人提供终身维修服务，只收取零配件费，配件以厂家最优惠价格提供。</p> <p>2. 中标供应商须协助采购人进行安装前的准备工作。</p>	

	<p>3. 提供建设安装资料并作相应的指导。</p> <p>4. 免费提供操作及维护培训。在安装、使用过程中，因产品质量问题所造成采购人损失的，中标供应商应当赔偿采购人的一切经济损失。</p> <p>5. 设备必须为全新、未使用的原装产品，符合国家各项有关质量标准制造的产品。</p> <p>6. 投标人根据各自的实际情况对质量保证及售后服务方案做出更优的详细承诺。</p> <p>7. 售后服务：</p> <p>（1）由中标人负责派专业技术人员到现场进行设备安装、调试，达到正常运作要求，保证正常使用。在安装调试过程中，中标人应派专业技术人员对安装进行同步指导，并负责全套机组的调试运行，达到验收要求。在质保期内，仪器、设备出现问题或采购人有服务需求的，中标人应在 30 分钟内响应；需要到现场维修的，应在 12 小时内到达仪器现场；一般故障应在 24 小时内解决，重大故障在 48 小时内解决，一周内未维修好的重大问题或其它无法迅速解决的问题须在一周内解决或提出明确解决方案。质保期内免费提供维护和保养服务并提供技术援助电话和售后服务电话，维修、换货中所有产生的一切费用由中标方承担。质保期外终身维护，零配件只收取成本费。</p> <p>（2）中标人提供 24 小时×365 天免费维修服务热线支持。每半年至少提供一次维护保养，并提供维护保养报告单；维护保养须检查设备的安全、设备清洁保养、设备性能测试、运行状态检查等，质保期内需更换的损耗品由中标人免费提供。</p> <p>（3）提供中文操作手册、维护手册、维修手册、备件清单、零部件、维修密码等维护维修必需的材料和信息，售后服务承诺书中根据采购人的实际情况对质量保证及售后服务方案做出详细服务承诺、提供详细的售后服务计划。</p> <p>（4）在保质期以后，中标人应提供备件和维修服务。</p>
交货时间及地点	<p>1. 交货时间：自签订合同之日起 30 天内完成安装、调试，通过验收并完成上线运行、交付使用。</p> <p>2. 交付地点：采购人（北海市人民医院）指定地点。</p>
付款方式	<p>签订合同后 10 个工作日内采购人向中标供应商支付至合同金额的 40%，自硬件交货、安装调试完成，整体项目验收通过后 15 个工作日内采购人向中标供应商支付至合同金额的 98%，验收合格一年后 10 个工作日内采购人向中标供应商支付至合同金额的 100%。</p>
验收要求	<p>1. 验收过程中所产生的一切费用均由中标人承担。报价时应考虑相关费用。中标供应商必须就采购需求中所有要求提供的证明文件作为货物性能参考依据，所有证明文件复印件须加盖投标人公章或投标专用章。验收时须提供生产厂家的彩页、检测报告或其他证明复印件（原件备查），如有发现所提供的证明材料内容与要求的设备功能不相符，追究其虚假应标的法律责任。</p>

	<p>2. 验收标准：</p> <p>(1) 中标供应商需承诺对于所提供产品保证均为全新、未使用的原装产品，产品所有功能均常使用，并符合国家相关质量标准要求，如出现以次充好等违约现象，由此引发出的费用及其他经济损失全部由中标供应商自行承担。</p> <p>(2) 交货时所有产品均严格按招标文件上的技术参数实质的要求、中标供应商响应和承诺的技术参数及性能和国家等有关标准进行验收。</p> <p>(3) 所有货物按时全部交送到采购人指定地点后，由采购人组织相关人力、中标供应商配合，按照招标文件、中标供应商投标文件、合同等文件资料对项目进行全面验收。</p> <p>(4) 采购人对货物安装验收合格后，双方共同签署验收书。验收标准应符合中国有关的国家、地方、行业标准。因本项目验收发生的邀请国家认可的质量检测机构、邀请专家及相关人员及检验费等费用由中标供应商承担。</p> <p>3. 采购人保留对中标人所提供产品、服务进行全面测试的权利，如有不满足招标文件及投标文件要求的视同虚假应标，中标人须承担所有责任和采购人的损失，采购人保留进一步追究责任的权利。</p> <p>4. 验收时，中标人需向采购人提供完整的技术资料，包括但不限于系统使用说明、详细设计说明书、功能测试报告等。</p> <p>5. 采购人有权委托有资质的第三方检测机构进行检验。其检查结果将作为验收标准的组成部分之一。</p> <p>6. 测试及检验：检验和测试在产品使用地进行；如果任何被检验或测试的产品不能满足采购要求的，采购人可以拒绝接受该产品，中标人需承担被采购人终止合同的一切风险和费用。</p>
<p>质量要求</p>	<p>1. 质量达到招标文件要求及投标文件响应内容。</p> <p>2. 中标人所提供的货物型号、技术规格、技术参数等质量必须与投标文件承诺相一致。</p> <p>3. 中标人所提供的货物必须是全新、未使用的原装产品，且在正常安装、使用和保养条件下，其使用寿命期内各项指标均达到质量要求。</p>
<p>其他要求</p>	<p>机房内具有各种专业设施设备共同运行，实施过程中须确保进入机房内安装调试实施的操作安全性，包括设备用电安全，网络安全，线路安全、实施安全等。</p>
<p>投标人的资信要求表</p>	
<p>政策性加分条件</p>	<p>符合节能环保等国家政策要求等</p>
<p>资料证明</p>	<p>投标时若有，请提供由产品厂家编写的、完整的、中文版的性能参数描述等</p>

文件	<p>有关说明文件或产品彩页。当投标文件承诺的货物性能参数与该货物厂家提供的性能参数不符合时，以厂家出具的为准。符合要求的产品说明文件应该是出厂装箱的产品说明书，或从产品厂家官方网页下载、打印的有产品详细说明的相关 PDF、HTML 彩打文件(打印时必须保留页面页脚的网址链接内容)；符合要求的产品彩页必须是厂家编写印刷的公开发售宣传铜版彩页，或厂家编写的公开发售宣传图册，或厂家编写由中标人自行打印并加盖厂家公章的彩色说明文件。</p>
<p>投标报价 要求</p>	<p>1. 投标报价为投标人在采购人指定地点交付所投产品时所产生的费用总和；包括货款、标准附件、备品备件、专用工具、包装、运输、装卸、保险、税金、货到就位以及安装、调试、培训、保修、设备接口费等一切税金和费用；</p> <p>2. 评标委员会认为投标人的投标报价明显低于其他通过符合性审查投标人的投标报价，有可能影响产品质量或者不能诚信履约的，应当要求其在评标现场合理的时间提供书面说明，必要时提交相关证明材料；投标人不能证明其投标报价合理性的，评标委员会应当将其作为无效投标处理。</p>
进口产品	本项目不接受进口产品投标。
核心产品	防火墙①、防火墙②