用 户 需 求 书

一、商务要求

1、交付时间：合同签订后 30 天内。

2、交付地点：用户指定地点。

3、交付方式：免费送至用户指定地点。

4、采购资金的支付方式、时间、条件：

货到付款 30%；设备安装调试完成付 30%；项目验收付 35%；预留 5%做为质保金，项目验收合格一年后支付。

5、供应商资格要求：见招标公告

6、验收要求：按标书技术参数和国家行业标准进行验收。

7、售后服务要求：

(1) 投标人或生产厂家须在全国设立服务机构，针对使用过程中出现的故障问题，可以通过电话、网络方式先提供服务，如果解决不了的情况下需要及时赶赴现场提供服务。

(2) 提供不低 3 年的免费保修期，自验收合格之日起算。

(3) 保修期内非采购方人为因素而出现的质量问题，生产厂家负责保修、包换或者包退，并承担修理、调换或退货的实际费用。

(4) 质保期内，设备在使用过程中，如发生非人为故障，投标人或生产厂家须在接到维修通知后 2 小时内响应,24 小时内给予解决方案并委派技术工程师到达现场维修，提供免费服务。重大问题在 2 个工作日内给予解决方案，若在 2 个工作日内无法及时排除故障，生产厂家免费提供同档次的备用机供院方使用。质保期外，投标人或生产厂家须接到维修通知之后 2 个小时内响应，24 小时提供建议解决方案供采购方选择。

(5) 投标人承诺提供的每一台仪器均是全新的，厂家提供终身有偿维修、保养服务，保修范围外有偿维修，只收成本费。

(6) 投标人或生产厂家负责产品安装系统调试及人员培训。

(7) 投标人或生产厂家负责长期提供技术资料和技术支持。

(8) 生产厂家保修期外需提供终身维护，设备故障维修只收取零配件费用。

(9) 生产厂家须对院方使用人员及设备维修人员进行培训，使用人员能够熟练掌握设备的各项功能和操作，使维修人员能对设备进行日常维护和一般性故障的查找及故障的排除。

8、由于项目实施过程会涉及医院敏感信息，供应商必须提交保密承诺函。

二、技术要求：

采购清单表

序号	产品名称	数量	备注
1	上网行为管理	1 台	详细配置见《招标参数要求》
2	专线出口防火墙	1 台	详细配置见《招标参数要求》
3	日志管理系统	1 套	详细配置见《招标参数要求》
4	网络准入	1 台	详细配置见《招标参数要求》
5	主机监控与审计系统	1 套	详细配置见《招标参数要求》
6	病毒过滤网关	1 台	详细配置见《招标参数要求》
7	网络数据防泄漏	1 台	详细配置见《招标参数要求》
8	杀毒软件网络版	1 套	详细配置见《招标参数要求》
9	虚拟化平台安全防护	10 套	详细配置见《招标参数要求》

参考配置及技术要求

1.上网行为管理

序号	招标要求
1	▲配置≥4 个 10/100/1000BASE-T(100m，RJ45)（支持 BYPASS 功能）；应用层吞吐量≥500M 最大并发连接数≥51 万；包括≥1000 用户数的使用许可。含 3 年系统版本升级、URL 库及应用特征库升级许可。
2	支持路由模式、网桥模式、旁路模式。
3	支持 ISP 自动地址表（电信、移动、网通、铁通等）的策略路由的选路方式；支持 PPPoE 拨号以及负载均衡。
4	要求支持 http 代理、https 透明代理、socks5 代理、DNS 代理、ARP 代理、内网代理功能。
5	支持即插即用功能。不管电脑的 IP 如何配置，开启即插即用功能后，只要插上网线，即可上网。
6	移动终端管理：须支持识别网络中正连接的热点（手机、iPad）、支持管理员配置热点信任列表，支持发现信任列表外非法接入的热点和终端，并阻止该热点/终端上网；支持将非法热点接入网络的行为通过邮件告警通知管理员，并在数据中心支持行为记录和查询。
7	阻止私接路由：必须支持能自动发现网络中私接的有线路由器、无线路由、360wifi 等共享上网行为，能够及时对私接行为进行管控，在系统中能够实时查看管控记录和日志。
8	支持 4 出口以上的多链路负载均衡;支持基于轮询的多链路负载均衡算法；支持基于链路的上行、下行、总流量自动均衡的多链路负载均衡算法； 支持最佳路径的多链路负载均衡算法；支持智能 DNS,对内部服务器负载均衡；支持按应用服务的负载均衡。
9	必须支持详细的告警功能，包含管理员操作日志、设备状态、流量异常、违规网站、违规帖子、违规文件上传、违规邮件发送以及潜在危害的行为告警。
10	支持 DNS 链路健康检查算法；支持 ICMP 链路健康检查算法；支持 TCP 链路健康检查算法；支持自定义的链路健康检查算法。
11	要求在界面提供 ping、TraceRoute 工具进行故障排查。
12	要求系统具有完整的操作命令日志、系统事件日志、用户网络日志、黑名单日志、设备状态日志、违规行为日志。

13	支持本地数据库、POP3、AD、LDAP 或 RADIUS 等认证方式。 可将已导出的用户信息的文件、或根据规定的用户格式编辑的文件、LDAP、AD 等外部服务器的用户信息同步到设备中。 对于未创建的用户，可根据其 IP 地址、MAC 地址、主机名或者 VLAN ID 等作为新用户名自动创建帐户，并可同时绑定 IP、绑定 MAC、绑定 IP+MAC、绑定 VLAN，并自动分配到指定用户组，享有指定网络权限。 支持绑定 IP、绑定 MAC、绑定 IP+MAC、支持 VLAN 绑定。 可将认证通过的用户强制导向到企业入口网页，如组织的公告页面等。 支持账号重复登入，当超出最大登入允许数后，支持是否踢掉前一次登入。 可通过 NetbIOS 协议扫描内网的主机信息，扫描结果将列出每个主机的 IP 地址、MAC 地址和主机名等，然后可以将其加入某个用户组中，逐步完善组织结构的管理。 支持临时账号自动申请功能，方便外来的临时用户使用。支持自动审核和管理员手动审核的核定方法将临时帐户加入到组织结构中。支持网页发送和邮件方式通知临时用户账号和密码。
14	支持基于四层服务和根据特征识别的七层服务进行带宽控制和流量阻断。 能够根据 IP 地址/IP 地址范围/IP 子网/地址簿/用户组的配置来控制网络中单个用户的上行会并发会话数、下行并发会话数。 针对流量异常的用户或者 IP 地址进行用户黑名单智能控制管理。 根据每用户的“每日/每周/每月”使用的流量(上行/下行/双向)总和超过预设阀值，则自动进入黑名单。 根据每用户在连续一段时间的“上行速率/下行速率”超过预设阀值，则自动进入黑名单。 根据每用户在连续一段时间的并发会话数(上行/下行)超过预设阀值，则自动进入黑名单。 根据每用户在连续一段时间的新建会话数(上行/下行)超过预设阀值，则自动进入黑名单。控制用户滥用 P2P、防止病毒等。 对进入黑名单的用户可采取强制下线或修改“上行带宽/下行带宽/上行会话数/下行会话数”的方式对用户进行惩罚。惩罚时间到期，可正常上网。 在“一周内/一月内/一季度内”，连续进入黑名单多次（如 5 次，可配置），可对用户进行加倍惩罚，惩罚时间可以原来的 N 倍。 可根据时间段来对用户进行黑名单的控制。在生效时间段内才进行黑名单的控

	制. 在生效时间段外, 不对用户的速率和会话进行限制, 用户产生的流量也不记入黑名单的流量配额内。 可根据每日的上网时长来限制用户上网时间，并且在报表中可以详细统计用户的上网时长以及所用服务。 可通过策略来配置对内网特定用户（IP 地址/IP 地址范围/IP 子网/地址簿/用户组）访问某些外网 IP 地址（IP 地址/IP 地址范围/IP 子网/地址簿/用户组）进行白名单的控制。符合白名单规则的访问，不受防火墙规则、流控规则、上网行为规则、黑名单规则的控制。
15	提供专有的报表中心系统。 报表中心管理员的权限和用户组织结构关联，不同的管理员只能查看对应权限的用户和用户组的统计信息。 支持前五十名服务流量的实时监控。 支持将各服务分类统计，实时查看服务组流量监控图。 支持对当前活跃服务/所有服务的最新速率、最近一小时流量、最近一小时平均速率、每个服务对应有哪些用户在使用，及每个用户的使用情况的统计。 支持前五十名用户的传输速率、新建会话速率、活跃会话数的统计。 实时查看在用户的详细信息：在线流量、最新速率、会话数、上线时间等信息。 查看物理端口接收报文的情况，以及每个端口传输流量的趋势图。 分时段对设备资源，包括 CPU 使用率、内存使用率、活跃会话数、在线用户数等息进行统计分析。 分时段对物理接口的收发的流量、速率等进行统计分析。 分时段对各个服务、各个服务类型、各个用户、用户组、各个线路、各个网站、网站类型等为条件进行流量、新建会话、活跃会话进行统计分析，并进一步统计分析每种服务有哪些用户在使用，及每个用户的使用情况。 支持自动/手动报表导出功能。可导出为 Excel、HTML、PDF 格式文件。可将报表作为附件发送邮件到指定邮箱。
16	支持网页关键字过滤； 支持网页 URL 过滤； 支持文件传输（HTTP/FTP）类型过滤； 支持邮件的“发件人/主题关键字/内容关键字/附件类型”过滤(POP3/SMTP/Web Mail)； 支持 IM 即时通讯的过滤（登录/聊天/文件传输/语音聊天）； 支持网页标题记录；

	支持发贴记录、网页评论记录； 支持在搜索引擎上的搜索记录； 支持 URL 访问记录； 支持网页文件上传/下载记录； 支持邮件内容审计（POP3/SMTP/Web Mail）； 支持邮件附件审计（POP3/SMTP/Web Mail）； 支持 IM 即时通讯软件内容审计（登录/聊天记录/文件传输）； 支持 FTP 的上传和下载记录，包括用户名和文件名； 支持所有访问的会话日志记录，包括：源 IP、目的 IP、协议类型、七层应用名称、源端口、目的端口、是否进行 NAT 转换(可显示转换后的 IP 和端口)、会话产生的时间和会话持续时间； 系统能够支持 Syslog 等第三方日志服务器系统； 可记录基于个人的行为监控，包括：网页标题记录、发贴记录、网页评论记录、在搜索引擎上的搜索记录、网页文件上传记录、URL 访问记录、即时通讯的登录信息/聊天内容/文件传输记录、邮件记录（详细内容、附件）、FTP 登录信息/上传记录/下载记录； 必须支持 URL 白名单，在白名单中的 URL 不受控制以及报表记录必须支持 IM 账号白名单功能，IM 账号不在白名单，不允许登陆必须支持对用户的具体应用进行上网时长和流量配额的限制。
17	支持 SNMP 网络管理方式。
18	所投产品具备计算机信息系统安全专用产品销售许可证，要求提供复印件并加盖厂家章。
19	所投产品厂家具备国家级网络安全应急服务支撑单位证书（国家级），要求提供复印件并加盖厂家章。

2.专线出口防火墙

序号	招标要求
1	▲配置≥6 个 10/100/1000MBase-T 端口、≥2 个千兆 SFP 光端口、≥2 个业务扩展插槽，防火墙吞吐率≥6Gbps、最大并发连接数≥220W ；配置病毒过滤功能，含 3 年特征库升级服务。
2	系统支持扩展病毒防御、入侵防御、应用识别、网站分类库过滤、VPN 功能、DLP 数据泄露防护功能、APT 防御功能。
3	▲配置多操作系统引导，出于安全性考虑，多系统需在设备启动过程中进行

	选择（要求提供截图进行证明），不得在 WEB 维护界面中设置系统切换选项；多个操作系统均为全功能操作系统。
4	配置路由、交换、混合、虚拟线工作模式。
5	支持静态路由、ISP 路由及动态路由协议，支持 802.1q、QinQ 模式。
6	支持基于源/目的地址、源/目的端口、用户、应用的策略路由，保证关键业务流量通过优质链路转发。
7	支持手动添加绑定，基于 IP、接口的动态探测绑定，支持跨三层 IP/MAC 绑定，IP/MAC 绑定表可导入导出。
8	支持一对一 SNAT、多对一 SNAT、一对一 DNAT、双向 NAT、NoNAT 等多种转换方式；支持 Sticky NAT 开关，使相同源 IP 的数据包经过地址转换后为其转换的源 IP 地址相同。
9	支持 IPv6 安全控制策略设置，能针对 IPv6 的目的/源地址、目的/源服务端口、区域、服务、时间、扩展头属性等条件进行安全访问规则的设置。
10	支持基于 IPv6 的应用层检测（FTP\TFTP）、病毒过滤、URL 过滤、ADS、IPS 检测。
11	▲支持在一台物理设备上划分出最大 4094 个相互独立的虚拟系统，可根据连接配额及连接新建速率为每个虚拟系统分配资源。（要求提供功能界面截图进行证明）
12	▲支持配置文件、系统服务等系统功能虚拟化，支持路由、链路聚合等网络功能虚拟化，支持安全策略、NAT 策略、带宽管理、认证策略、IPV6 功能、URL 过滤、异常行为分析、病毒过滤、内容过滤、审计、报表等安全功能虚拟化。（要求提供功能界面截图进行证明）
13	内置强大应用识别引擎，综合运用端口识别、行为识别、特征识别、关联识别等技术手段，准确识别传统应用如 P2P、web 应用、移动应用、云应用、加密应用等。
14	支持对单条访问控制策略进行最大并发连接数限制；同时支持对连接数限制策略匹配信息进行分类统计，方便管理员根据统计分析结果进行相应的防护控制。
15	为保护内部网络资源以及合理分配设备系统资源，需支持对指定的源/目的 IP 地址、MAC 地址、应用制定相应的连接限制策略，策略包含三种限制类型：单个 IP 每秒新建连接限制、单个 IP 连接数限制及连接总数限制。
16	内置高度集成的一体化智能过滤引擎技术，支持实现在同一条访问控制策略中配置传统的五元组信息、用户、域名、应用、服务、时间、安全引擎（入侵防御、URL 过滤、病毒过滤、数据防泄漏 DLP、内容过滤、文件过滤、审计、APT）的识别与控制。
17	访问控制策略执行动作支持允许、禁止及认证，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。
18	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，并且可在 WEB 界面显示检测结果：红色为冗余策略，绿色为冲突策略。
19	支持扩展 APT 防御功能模块，不依赖于攻击、恶意代码等特征库进行检测，通过沙箱技术对于未知漏洞攻击（0day/1day 漏洞）、木马、病毒具有检测能力；可根据用户环境，将 APT 工作模式设置为深度模式或者智能模式。
20	内置流量检测清洗引擎，支持基于 IP、ICMP、TCP、UDP、DNS、HTTP、NTP 等众多协议类型的防护策略；提供丰富的策略模板，且支持策略模板自定义。

21	支持基于 NTP 协议的检测清洗，包括 NTP REQUEST FLOOD、NTP REPLY FLOOD 等攻击检测，支持基于 NTP 请求限速、NTP 响应限速、源认证、会话认证的防御策略。
22	▲支持根据 DOS/DDOS 攻击行为自动添加动态黑/白名单功能，可自定义动态黑/白名单超时时间。（要求提供功能界面截图进行证明）
23	支持扩展病毒检测功能模块，支持 HTTP/SMTP/POP3/FTP/IM 等协议的病毒防御，对每种协议数据流的检测方向可选双向、上传、下载。
24	▲支持扩展 DLP 数据防泄漏引擎,可针对发送者或接收者模式配置独立的 DLP 策略，对数据进行监控识别，达到敏感数据防护目的。为提高产品的可用性，需支持识别的加密文件格式不少于 12 种;压缩文件格式不少于 25 种,如 RAR、ZIP、GZ、TAR 等；支持识别 Linux，Unix 等非 Winodws 的文件类型；支持识别异常文件格式类型；支持识别自定义文件类型。（要求提供功能界面截图进行证明）
25	支持分别针对网络层、传输层和应用层提供诊断系统网络连通性的工具，包括 PING、 TRACEROUTE、 TCP、 HTTP 和 DNS。 支持在 WEB 界面进入 CLI 模式，执行系统配置、网络诊断、过滤抓包等命令，提高管理员运维效率。
26	支持日志本地存储，可对不同类型日志设置存储空间。
27	支持将日志外发至 SYSLOG 服务器，可将多条日志合并成一条日志传送到日志服务器中。
28	日志查看可划分为管理日志、系统日志、策略日志、应用行为日志等四大模块，具体包含用户、连接、流量、NAT、审计、HA、APT、未知威胁等 20 个日志类别。
29	支持根据按照病毒防御、入侵防御、APT 防御、ADS 攻击进行威胁统计，可按照威胁类型/攻击者/受害者三种方式进行威胁排名。
30	所投产品具有公安部颁发的第二代防火墙产品计算机信息系统安全专用产品销售许可证，要求提供复印件并加盖厂家章。

3.日志管理系统

序号	招标要求
1	▲配置日志收集、存储、查询、统计、关联分析、告警、报表等功能，包含 100 个日志源授权。
2	日志收集能力：大于 20000 条/秒； 日志存储能力：10000 条/秒存储速度；20000 条/M 存储能力（每 M 空间存储 20000 条以上日志，压缩存储，压缩比：10:1）； 综合处理能力：10000 条/秒综合处理能力。
3	支持 Syslog、SNMP Trap、Netflow、JDBC 等协议日志收集。
4	支持直接远程收集；针对特殊应用可以使用 Agent 收集。

5	系统具有防恶意暴力破解账号与口令功能；口令错误次数可设置，超过错误次数锁定，锁定时间可设置。
6	日志保存时间可以设置为：1—6 个月、一年、永久保存；灵活设置系统日志存储空间上限，达到告警上限提示管理员及时处理，达到删除上限会自动删除最旧日志释放空间。
7	可以针对不同的日志源制定不同的存储策略。
8	支持从存储空间、存储时间多维度进行动态监控。
9	支持自定义存储位置（磁盘阵列、SAN、NAS 等外部存储网络）以获取超大存储空间。
10	支持将不同设备所产生的不同格式的难以理解的日志数据进行统一格式化处理，提炼出有用信息清晰、明确的展示给管理者。
11	可以通过管理平台首页可以清晰查看到单日安全事件概况、系统逻辑拓扑图、实时告警信息。
12	可以实时查看审计中心主机的 CPU、内存、流量以及磁盘等的使用情况。
13	实时日志提供给管理员实时更新的最近的 2000 条日志信息，管理员可以进行监视、刷新、清零等基本监视条件管理。
14	支持多条件组合查询，查询结果即查即显； 支持原始日志全文检索；查询结果可将归一化日志和原始日志对比显示；支持等于、不等于、大于、小于、正则表达式等查询条件；支持为不同类型日志设置不同的查询条件和显示条件；支持在查询结果页面上直接下钻二次查询，快速定位关键日志，还可以返回上次查询条件；查询结果支持分页显示；支持查询结果导出；支持外部备份文件导入进行查询。
15	管理员可以对日志源进行查看、添加、编辑、删除以及启\禁用的操作。
16	支持黑白名单制定，被添加到黑名单列表中的 IP 地址主动发送的日志将被忽略。
17	系统内置常见安全事件关联分析规则（要求提供功能界面截图进行证明）；支持基于策略的多日志源海量日志实时关联分析，发现安全事件实时告警；提供可视化关联分析规则编辑视图，可根据实际业务编辑关联分析规则。
18	实时告警显示日志收集与分析系统最新的告警信息，日志收集与分析系统提供实时告警信息查看功能。
19	支持安全告警概况、安全告警趋势以及实时安全事件的统一展示，实时告警可根据级别、规则类型等进行分类。
20	管理员可以查看系统内置的各种类型的报表。
21	内置不少于多种报表模板，百亿级数据报表查看显示时间小于 20 秒，支持自定义报表。
22	可以定期定时发送报表到指定的邮件账户，满足了用户有规律的接收报表、定期了解设备情况的需求。
23	支持基于拓扑图的日志源相关数据信息快速查看；支持日志源在线状态监测告警，实时监测日志源的可用性；支持按照角色对日志源的综合管理权限进行授权。
24	系统支持三权分离管理模式。
25	所投产品具备计算机信息系统安全专用产品销售许可证，要求提供复印件并加盖厂家章。
26	所投产品厂家具备国家级网络安全应急服务支撑单位证书（国家级），要求提

	供复印件并加盖厂家章。

4.网络准入

序号	招标要求
1	▲配置≥6 个 10/100/1000MBase-T 端口、≥2 个千兆 SFP 光端口、≥2 个业务扩展插槽，冗余电源，≥1T 的存储空间，≥1000 用户授权。
2	支持旁路部署、串接部署等，不改变用户现有的网络结构。
3	▲双操作系统冷备支持，当常用系统出现故障可以使用备用系统恢复。（要求提供界面功能截图）
4	支持双机热备，主备无缝切换，支持双机间的数据同步。
5	客户端支持 WindowsXP（SP3, 32/64 位）、Windows7（32/64 位）、Windows8（32/64 位）、Windows8.1（32/64 位）、WindowsServer2008（32/64 位）等多种操作系统。
6	基于 802.1X 方式准入； 支持传统 PC 有线和无线认证、健康检查、动态 VLAN 划分； 支持智能终端无线准入，无需安装客户端。
7	一、系统默认检查项： 1） 系统时间检查 2） 系统运行时长检查 3） 资产验证检查，检查终端资产是否合法 4） Guest 用户检查 5） Windows 文件共享检查 6） Windows 防火墙检查 7） 必须/禁止运行进程检查 8） 必须/禁止运行服务检查 9） 必须/禁止安装软件检查 10）Windows 桌面屏保检查 11）杀毒软件版本（Avira[国内称：小红伞]、瑞星、金山毒霸、卡巴斯基、诺顿、360 杀毒）检查项 二、支持检查项分数设置： 检查项策略对象之间可通过评分制的形式对终端的健康状况做最后的评估，根据预先配置好的阈值对终端入网请求作出判断。 三、其他满足项： 1） 支持用户自定义基于（WMI、文件和注册表组成的自定义健康检查策略） 2） 支持自定义策略权重 3） 支持自定义通过或隔离策略 4） 支持自定义修复向导 5） 支持有线和无线准入的健康检查
8	1） 支持用户和 VLAN 绑定，支持用户组管理 2） 支持用户或用户组和策略绑定 3） 支持 LDAP 和 AD 域认证
9	显示当前在线用户名、VLAN、NASIP 地址、NAS 端口、终端 MAC、准入状态、得分、

	终端 IP 地址、上线时间。
10	1) 支持统一下发客户端的网络配置（配置项包括：IP、网关和 DNS 子网掩码等信息） 2) 支持客户端 IP/MAC 绑定 3) 支持客户端基于 IP/VLAN 动态下发
11	1) 用户认证日志 包括认证用户、VLAN、NASIP、NAS 端口、终端 MAC、准入状态、认证时间等信息。 可自定义时间查询，时间可进行微调。 2) 用户健康检查日志 包括认证用户、VLAN、NASIP、NAS 端口、准入状态、健康检查得分、认证时间、详情等信息，其中在详情里面可以详细地看到该用户各项检查的结果。 3) 系统日志 系统日志包括用户操作的审计日志和系统错误信息等。
12	1) 支持网络主机名配置 可添加准入系统网络主机 IP 和主机名。 2) 支持网络管理 控制网络准入系统的 IP 接口、路由管理、系统访问控制管理，满足固定 IP 地址访问系统。 3) 支持系统服务管理 对 TopNAC 上的服务进行管理，可以进行的操作有启动服务、禁用服务、重启服务，系统页面展现无需后台操作。 4) 支持系统许可证管理 显示系统基本信息和许可证信息，可以实现查询系统基本信息、获取系统状态、注册、导入许可证等功能。 5) 支持系统状态管理 以图形化的形式查看系统状态：cpu 利用率、内存利用率、硬盘利用率。 6) 支持系统授权管理 包括系统用户管理和系统权限管理，实现系统用户的添加以及用户权限的分配。 7) 支持系统安装包管理 安装包列表中列出了产品出厂时灌装的数据包，详细介绍了数据包的信息：版本、编译次数、支持平台、所属分支、状态等等。可以选择某个已安装的数据包“更新”、“卸载”，未安装的可以选择“安装”，也可以选择安装包“上传”。 8) 支持系统时间设置 包括：系统日期、系统时间、当前时区，以及同步系统时间。可将当前用户使用的计算机系统时间调整为与服务器系统时间一致。
13	所投产品具备计算机信息系统安全专用产品销售许可证

5.主机监控与审计系统

序号	招标要求
1	▲配置 1 套管理端，800 个客户端。可对网络中的计算机资产进行管理，能够监控系统端口、进程、软硬件信息、补丁等内容，具有补丁分发功能，能够对终端用户文件操作行为、打印行为、网络访问行为进行监控审计，可以对计算机的外设及接口进行控制。
2	配置补丁管理与软件分发功能，具体包含补丁管理（微软操作系统）和软件分发功能。
3	配置系统管理与监控功能，具体包含文件监控、设备端口监控、打印监控、拨号监控、硬件监控、软件监视、外联监控、HTTP 监控、共享监视、流量监控、进程监控、端口监视、性能监视、网络配置监控、主机防火墙。必选。
4	配置移动介质管理功能，具体包含外存管理、针对 U 盘和指定安全 U 盘的注册、标签管理、授权、审计功能。
5	配置网络准入管理功能，具体包含基于 802.1X、自有防火墙和 ARP 的准入认证功能。
6	提供资产创建、出库、领用、调拨、借出、维修、退库、报废等全生命周期化管理，不同过程节点可操作维护。 资产信息包括：资产属性、产使用状态、资产类型、资产品牌、资产型号、主要配置、条形码编号、资产序列号、资产快速服务号、所在网络、责任部门、责任人、使用部门、使用人、物理位置、操作系统、IP 地址、MAC 地址、网关、子网掩码、DNS1、DNS2、供货单位、供货单位联系方式、出厂日期、保修截止日期、购置时间、入库时间、申请价格、投标价格、实际购买价格、资产来源、资产设备容量、跃点数、临时资产准入过期时间等。
7	可以监控终端安装与否等信息； 对已登记、未登记用户进行监控，支持对客户端进行远程协助、重启、关机等操作； 运行监控中可以查看已登记、未登记在线终端的相关信息，包括：名称、类型、IP/MAC、版本、上线历史、漏洞、资产关联、验证情况等； 按部门、按组进行全局终端信息统计，以图形化方式展示，可统计终端软硬件、进程、端口、补丁等信息。
8	按部门类型和操作系统类型进行列表和柱状图统计补丁安装情况； 支持对补丁文件分类，补丁分为已验证、未验证和正在验证三种类型，“已验证”类中又分为安全更新程序、关键更新程序、更新程序、更新程序集、更新包和工具； 支持指定主机的补丁检测时间（主机启动时检测或间隔一定时间定时检测）、下载的补丁类型（安全更新程序、关键更新程序、工具、更新程序、更新程序集和更新包）、下载的补丁级别、补丁安装前提示、安装后重启。
9	支持文件监控策略。对不同磁盘类型及指定文件夹下的文件和文件夹的创建、修改、删除、移动、打开、读取、执行、重命名等操作可以有选择地禁止和审计，可设置例外项。 支持针对终端存储的 word、pdf、ppt、Excel、rtf、文本文件等进行全盘关键字检查，对含有制定关键字的文档进行禁止发送、禁止拷贝等管控，同时

	将文档信息上报服务器。支持复合关键字检索，支持检查范围定义及违规提示。
10	支持外联监控策略。支持 http、telnet、ping 三种方式检测主机违规外联行为，可设定检测周期、外联检测地址、违规处理方式（不处理、重启、断网、提示）。
11	支持 FTP 方式的软件分发，可指定下发时间、分发后的处理方式（不安装、立即执行、强制安装）。
12	▲要求所投产品具备计算机信息系统安全专用产品销售许可证（主机监测三级），提供复印件并加盖厂家章。
13	所投产品厂家具备国家级网络安全应急服务支撑单位证书（国家级），要求提供复印件并加盖厂家章。

6.病毒过滤网关

序号	招标要求
1	▲配置≥6 个 10/100/1000BASE-T 接口、≥4 个 SFP 接口、≥2 个可插拔的扩展槽（其中 4 个电口支持 Bypass），配置模块化双冗余电源，整机吞吐：≥3Gbps；并发连接：≥220 万；防病毒吞吐（HTTP）：≥800Mbps；设备内置快速扫描与深度扫描双防病毒引擎,包含 3 年的快速扫描与深度扫描病毒库升级服务许可。
2	▲设备必须为专业的防病毒网关产品，非防火墙/下一代防火墙、UTM、IPS 等具有防病毒功能模块的产品，并出具网关防病毒类产品销售许可证书及公安部计算机病毒防治产品检验中心的检测报告。
3	▲配置多操作系统引导，出于安全性考虑，多系统需在设备启动过程中进行选择，不得在 WEB 维护界面中设置系统切换选项（要求提供功能界面截图进行证明）。
4	要求设备配置旁路、串接、混合（旁路+串接）三种部署模式； 旁路部署可进行病毒监测及日志记录，串接模式可同时进行病毒监测、病毒过滤及日志记录。
5	要求基于多核多平台并行安全操作系统。
6	内嵌双引擎杀毒技术，可单独采用流杀毒（快速扫描）引擎或文件型杀毒（深度扫描）引擎，也可同时支持两种杀毒引擎，能够根据不同的被检测协议采用不同杀毒引擎。
7	能够防御病毒、木马、蠕虫，且支持对压缩数据、加壳病毒的查杀。
8	能够支持对 SMTP、POP3、IMAP、HTTP 和 FTP 协议进行病毒扫描和过滤，有效地防止可能的病毒威胁。
9	支持病毒隔离功能，管理员可以方便的管理隔离区，可以选择把隔离区的内容发送给管理员或者删除；可以实时检测到日益泛滥的蠕虫攻击，并对其进行实时阻断，从而有效防止内部网络因遭受蠕虫攻击而陷于瘫痪。
10	要求支持信任站点功能，网关针对信任站点不做病毒扫描，以降低病毒扫描引擎的负担。
11	支持 IPv4 和 IPv6 双栈协议的病毒扫描和过滤。
12	支持智能检测应用协议的病毒行为，采用智能方式准确扫描常用协议任意端口

	的病毒传输行为，而非通过传统手动配置协议端口绑定形式进行病毒扫描。
13	支持多接口旁路的病毒传输监听检测方式，可并行监听并检测多个网段内的病毒传输行为，用于高吞吐量、高可靠性要求的旁路应用环境。
14	支持通过采用 java 的 Commons FileUpload 或其他类似控件的 OA、CRM 及其他基于 WEB 的应用系统（包括 WEBMAIL）上传文件时的病毒查杀。
15	▲要求提供病毒检测率不低于 98%的第三方证明文件，提供复印件并加盖厂家章。
16	要求深度扫描及快速扫描引擎具有独立的病毒库，深度扫描及快速扫描病毒库总数相加大于 600 万（要求提供功能截图证明，并加盖厂家章）。 要求具有独立的蠕虫防护规则库，并可通过手动或自动方式进行升级。
17	要求能够根据文件内容识别文件真实类型，有效的阻断非法类型的文件进入单位网络，能够防止通过修改文件扩展名的方式逃避过滤。
18	采用邮件地址与 IP 地址的黑、白名单技术实时检测垃圾邮件并阻止其进入企业网络，为企业节省宝贵的带宽。
19	提供完整的病毒日志、访问日志和系统日志等记录，并可根据日志数据生成多种格式的统计图形化统计报表。
20	提供强大的监控功能，可以监控系统资源、网络流量、当前会话数、当前病毒扫描信息等。
21	报警配置用于当病毒突然爆发时，可向网络管理员发送报警信息，需支持邮件报警、声音报警、SNMP 等报警方式。
22	要求具有配置文件自动定时上传到指定外部服务器功能。
23	▲所投产品具备病毒过滤网关 IPv6 Ready2 资质认证，要求资质必须为防病毒网关的专用资质，非 UTM 或防火墙资质，要求提供复印件并加盖厂家章。
24	所投产品厂家具备国家级网络安全应急服务支撑单位证书（国家级），要求提供复印件并加盖厂家章。

7.网络数据防泄漏

序号	招标要求
1	基于深度内容识别技术的网络数据防泄漏产品，支持旁路部署。
2	▲标准机架式服务器，≥8 个千兆电口（配置 bypass 功能），≥2 个扩展插槽，≥1T 硬盘空间。
3	▲DLP 检测吞吐率≥200Mbps，识别文件类型≥1000 种，支持提取文件内容的文件类型≥300 种。
4	系统支持 HTTP、SMTP、POP3、IMAP、FTP、SMB、IM 等协议的识别。
5	系统支持精确识别 Webmail 应用的关键信息，如发件人、收件人、抄送人、主题、正文、附件等。系统支持精确识别网盘上传的文件。
6	系统支持精确识别社交网络的关键信息，主题、正文、附件等。
7	系统支持识别的文件类型数量不少于 1000 种；系统支持识别的文件内容格式

	不少于 300 种。
8	系统支持识别的加密文件格式不少于 12 种（要求提供功能界面截图，并加盖厂家章）。
9	系统支持的压缩文件格式不少于 25 种，如 RAR、ZIP、GZ、TAR 等。
10	系统支持识别 Linux，Unix 等非 Winodws 的文件类型；支持图片格式识别。 系统支持识别自定义文件类型。
11	系统支持关键字方式识别敏感内容；支持*通配符、忽略大小写、中、英文、多模关键字、某一范围内相邻关键字组合的匹配方式。 系统支持数据标识符方式识别敏感内容。
12	系统支持数据库指纹方式精确识别敏感内容。即通过对数据库表关键列内容创建指纹后，当外发数据中含有该数据库表中某行中的几列数据则可判断外发敏感结构化数据。 系统支持文档内容指纹方式精确识别敏感内容。
13	▲系统支持机器学习方式识别敏感内容（要求提供功能界面截图，并加盖厂家章）。即通过对样本文挡，使用机器学习方法提取公共特征后，当外发数据中包含类似该特征时，判断其数据含有敏感内容。
14	▲系统支持基于图片内容指纹方式精确识别敏感内容（要求提供功能界面截图，并加盖厂家章）。通过对待保护图片内容生成指纹后，与外发图片内容的指纹匹配相似度，如果相似度超过一定阈值则可判断外发敏感文档内容。
15	▲系统支持扩展图片 OCR 方式识别图片文字（要求提供功能界面截图，并加盖厂家章）。
16	系统支持识别简体中文、繁体中文、英文、日、韩、藏、维、蒙、彝、阿拉伯等种语言。
17	系统支持识别文档多层嵌套方式逃避检测行为，支持识别文件多层压缩方式逃避检测行为；支持识别文件加密方式逃避检测行为；支持识别邮件密送行为；支持识别文档的页眉页脚隐藏敏感信息的行为；支持识别敏感信息标识为隐藏段落方式的泄露行为；支持识别修改文件扩展名方式逃避检测的行为。
18	系统支持识别图片格式嵌入敏感文档方式。
19	系统支持识别截屏、拍照成图片的方式泄漏敏感信息行为。
20	系统支持识别拷贝文档部分内容方式泄漏敏感信息行为。
21	▲系统支持识别少量多次泄漏敏感信息行为（要求提供功能界面截图，并加盖厂家章）。
22	系统支持根据事件上下文作为前置条件执行响应动作，如事件类型、事件匹配次数、传输协议、事件严重性等。
23	支持满足实际工作所需要的复杂策略，单条策略可以包含多个规则，内部规则之间可以通过 “AND/OR”，“条件”以及“排除”的逻辑组合在一起。不仅能够基于内容来制定策略，还能结合发送者/接收者，文件特征，通讯协议等来制定策略。支持针对特定数据内容，如：关键字、文件类型、文件大小、协议等条件进行例外处理。
24	系统提供丰富的报表功能.包括最近 30 天事件、全部事件、本周事件、本月事件、按策略汇总、按策略趋势汇总、按协议汇总、按协议趋势汇总、按周和状态汇总、按策略和状态汇总、按周和策略汇总、最近 30 天高危发送者、高严重性的高危发送者等事件报表。
25	系统记录事件信息足够详细，如状态、协议、附件、事件状态、匹配次数、

	发送者（邮箱，IP，用户名）、接收者（邮箱，IP，用户名）、发生时间、主题、严重性、违规策略等信息。
26	支持基于角色的权限管理。比如：系统管理员，策略管理员，审计人员等，每类用户拥有不同的权限。
27	系统提供 SNMP 接口，供第三方的网管系统集成。系统提供 syslog 接口，供第三方事件管理系统集成。
28	▲所投产品具备计算机信息系统安全专用产品销售许可证，要求资质必须为数据泄露防护产品专用资质（资质中指明“数据泄露防护产品”），非“主机信息泄露防护”或者“访问控制”类资质，要求提供复印件并加盖厂家章。
29	▲所投产品厂家具备国家级网络安全应急服务支撑单位证书（国家级），要求提供复印件并加盖厂家章。

8.杀毒软件网络版

序号	招标要求
1	▲配置≥800 个 window PC 客户端杀毒授权，≥100 个 Windwos Server 操作系统杀毒授权，≥10 个 Linux 操作系统杀毒授权，≥1 个系统管理中心。
2	安装在终端 PC 上，具有多种安装方式，部署简单方便，支持多语言，如中文简体、中文繁体、英文。
3	支持的 Windows 系列系统 Windows2000(Professional/Server/Advance Server) Windows XP (Professional/Home) Windows Server 2003 Windows Server 2008 Windows Server 2012 Windows Vista Windows 7 Windows 8 支持 64 位操作系统，如 Windows XP-64、Windows Server 2003-64，Vista-64
4	▲配置系统加固、应用程序控制、木马行为防御木马入侵拦截（网站拦截）、木马入侵拦截、智能防御自定义白名单、自我保护等主动防御策略下发等功能（要求提供截图证明）。
5	集成主动防御功能和安全软件自我保护功能，阻断未知病毒和各种网络威胁的入侵。
6	支持 Office/IE/Lotus Notes 等嵌入杀毒；支持用户添加嵌入杀毒的应用程序；支持 MSN Messenger、AOL Messenger、FlashGet、NetAnts、NetVampire、WinZip、WellGet、WinRAR 等工具的嵌入式杀毒功能。
7	自持可疑文件上报功能，如果用户觉得某个文件比较可疑，可将此文件上报给防毒厂商进行检查分析和处理。
8	U 盘防护和自动免疫功能，防止病毒通过 U 盘在网络内传播，支持对 U 盘设备进行登记管理，只有添加到信任列表的 U 盘才能在终端上使用。
9	客户端动态资源分配，该功能可以有效的降低网络版对系统资源（内存）的

	占用，可降低扫描病毒对用户使用计算机的影响。
10	支持对上网时间及时长进行精细化限制。
11	白名单管理工具，通过此工具将企业信任的文件、网址等添加到信任列表，防止误报、误拦，最大程度的方便用户。
12	支持病毒库无缝主动式智能升级。支持客户端从互联网直接升级。升级过程支持增量升级，以减少升级时带来的网络流量；可设置升级周期和升级时间范围，保证及时升级并避免升级时占用网络带宽影响用户正常业务的通讯；可任意调整升级时的数据包大小，以解决窄带网络的升级问题。
13	支持文件监控、邮件监控一体化实时监控：文件监控支持“智能监控”和“强制杀毒”两种模式；邮件监控支持多端口设置功能，可以对设置的所有端口的进行邮件监控。网页监控支持监控网页脚本来检测恶意网页内容并提示用户进行处理。
14	支持电脑安全评测功能,让用户全面了解自己计算机,引导用户增强其安全性，防止病毒入侵。
15	支持病毒查杀时目录排出功能，支持空闲查杀、异步查杀、断点查杀、后台查杀，支持快捷杀毒功能，支持开机扫描功能，支持关键点扫描，具有病毒隔离系统，保护无法查杀的带毒文件。
16	支持密码保护设置，防止客户端用户关闭实时监控或卸载杀毒软件等。
17	所投产品厂家具备公安部销售许可证（网络版防病毒产品-一级品），要求提供复印件并加盖厂家章。
18	▲所投产品厂家具备国家级网络安全应急服务支撑单位证书（国家级），要求提供复印件并加盖厂家章。

9.虚拟化平台安全防护

序号	招标要求
1	▲配置≥2 颗物理 CPU 授权的虚拟化分布式防火墙,实现虚拟化平台内部东西向流量的安全防护；配置集中管理平台，用于对所有虚拟化分布式防火墙进行统一管理。
2	采用专用安全操作系统，基于操作系统内核的完全检测技术；专用的安全操作系统具有自主知识产权。
3	软件采用模块化结构设计，可以根据需要组合，可以扩展防病毒、入侵防御、安全审计等功能。
4	支持主流服务器虚拟化平台部署，包括 Vmware NSX/ESXi、Xenserver、Kvm 等。
5	以虚拟机方式部署，工作于虚拟机内部，保护虚拟机间安全访问。
6	支持 vDFW 的集中管理、策略下发、事件收集、日志审计、报表统计等。
7	支持软件 license 授权模式，可按需扩展虚拟设备和虚拟设备扩展功能。
8	每套虚拟防火墙性能：并发连接数≥100 万，防火墙吞吐（2 核）≥8G。
9	支持从虚拟化平台获取虚拟机信息，包括虚拟机名字，ip 地址，并应用于安全策略配置。

10	▲防护范围包括物理网络进出虚拟机和同一物理服务器上虚拟网络中虚拟机之间的网络流量。
11	支持根据虚拟机的迁移、复制情况下，同步调整相关安全策略，使虚拟机始终处于虚拟化防火墙保护之下。
12	支持虚拟机通信量（源地址，目的地址，源端口，目的端口）Top50 排名。
13	支持基于虚拟化 Hypervisor 层状态检测防护墙。
14	支持当虚拟化安全网关出现异常时，可在 Hypervisor 层 bypass 虚拟机流量，不中断业务通信。
15	防火墙功能： 支持基于用户、IP、应用、时间、协议等方式的策略控制； 支持基于域名的访问控制策略； 支持 IP/MAC 绑定； 支持基于策略的连接统计、报文统计、连接数限制等； 支持策略分组管理； ▲为防止用户私接无线路由器、随身 WIFI 等设备产生安全隐患，要求防火墙具有防共享接入的功能，能够有效识别并阻断共享接入行为（提供配置界面截图证明及专利证明，并加盖厂家章）； 支持动态端口协议，如 H.323、SIP、FTP、RTSP、SQL*NET、MMS、RPC、TFTP、PPTP。
16	▲设备可自实现检测防火墙规则是否冲突，支持在系统界面上开启规则冲突检测功能，在出现策略冲突时，能够在 WEB 界面进行警告（提供功能界面截图，并加盖厂家章），从而效防止防火墙系统内部规则冲突造成网络不稳定（提供具备自主知识产权的官方有效证明，并加盖厂家章）。
17	网络病毒过滤功能： 支持 HTTP，FTP，POP3，SMTP，IMAP 协议的病毒查杀； 支持超过 150 万种流行病毒的查杀，定期更新和升级病毒库； 支持快速扫描和完全扫描两种查杀方式。
18	入侵检测及防御功能： 支持非法报文和统计型报文攻击； 支持 TOPSEC 联动协议，可与 IDS 设备联动； 支持基于应用协议的入侵检测； 支持超过 3800 种内置入侵检测库，可定期自动升级。
19	内容过滤功能： 支持对 HTTP、FTP、SMTP、POP3、IMAP 协议的深度内容过滤； 支持 DNS 过滤和 DNS 代理； 支持 WEB 重定向； 支持隐藏 HTTP、FTP、SMTP、POP3、TELNET 等服务器版本信息； 支持反垃圾邮件过滤，包括黑白名单、实时黑名单、反向 DNS、灰名单等技术。
20	支持基于策略的保证带宽和限制带宽； 支持基于用户、IP、应用等方式的带宽策略； 支持 DSCP 和 COS 报文设置。
21	支持 Welf、Syslog 格式的日志； 支持日志分级和按类型输出； 支持通过第三方软件查看日志。

22	支持 WEBUI、Telnet、Ssh、集中管理等多种方式的设备管理； 支持 SNMP 管理和监控； 支持邮件、NETBIOS、SNMP 等多种方式的报警； 支持配置文件恢复和备份。
23	▲要求所投产品具备销售许可证，要求提供复印件并加盖厂家章。
24	▲所投产品厂家具备国家级网络安全应急服务支撑单位证书（国家级），要求提供复印件并加盖厂家章。
25	