项目采购需求

一、技术参数、服务内容要求：		
标的名称	数量	技术需求或者服务要求
防病毒网关	4台	1. ★标准2U 设备，千兆电口≥6个，千兆光口≥4个，万兆光口≥2个，扩展槽位≥2个，双电源，2组bypass。网络吞吐≥40G，并发连接≥700万； 2. 至少支持透明、路由、混合、旁路4种工作模式，同时支持旁路模式+在线模式部署； 3. 支持802.3ad ，可在透明、路由模式下支持多条链路带宽进行捆绑,支持LACP协议，支持5种捆绑算法（基于源地址、目的地址、源端口、目的端口等组合HASH）； 4. 支持将任意接口数据完全镜像到设备自身的其余接口,用于抓包分析,根据转发策略，支持不少于8元组（应用、用户等）进行流量镜像；支持对应用程序的识别和控制能力。应用程序特征库不少于2700种，并支持在线更新或手动更新；（投标文件中提供产品截图或官方技术说明文档）； 5. 支持一对一、一对多，多对多的NAT，且公网地址池支持轮询和源地址保持两种模式，支持夸协议NAT转换，NAT64支持：IVI、嵌入式地址、地址池三种转换方式，NAT46支持：IVI、地址方式转换方式； 6. 支持基于标准SYSLOG日志格式；支持日志外发，支持日志服务器负载，支持3种方式。（投标文件中提供产品截图或官方技术说明文档） 7. 支持IPv4/6抗应用型DOS攻击防护，如HTTP Flood、DNS query flood等攻击防护;支持抗流量型攻击防护，如syn flood、udp flood、icmp flood，tcp flood等攻击防护； 8. 支持VRF功能，可支持1024个VRF； 9. 支持集中化云向管理，可通过云平台监控设备状态、下发配置等。（投标文件中提供产品截图或官方技术说明文档） 10. 支持HTTP，FTP，POP3，SMTP，IMAP协议的病毒查杀、病毒库自动更新、虚拟脱壳、查杀可疑病毒、可疑脚本、图片病毒、查杀邮件正文、附件、网页及下载文

		件中包含的病毒； 11. 支持预定义不少于 20 种文件类型，支持自定义扫描文件类型，支持常见的压缩格式文件扫描；（投标文件中提供产品截图或官方技术说明文档） 12. 支持病毒防护沙箱联动功能，能够将灰文件信息同步云端进行分析，并且返回分析结果。 13. 支持不少于 800 万种病毒的查杀，病毒库支持在线或者离线升级。（投标文件中提供产品截图或官方技术说明文档） 14. 产品具有公安部颁发的《计算机信息系统安全专用产品销售许可证》，并在投标文件中提供证书复印件。 15. 设备生产厂商具有自主研发的反病毒引擎，提供软件著作权证明；
动态 Web 应用防火墙	2 台	一、★基本要求 1、标准 2U 机架式设备，含交流冗余电源，不少于 2 个 USB 口，不少于 1 个 RJ45 串口，不少于 2 个千兆管理口，不少于 1 个 3.5 寸热插拔硬盘位，万兆 SFPP 插槽≥4 个（至少含 4 块万兆多模光模块），网络接口扩展槽≥3 个； 2、应用层吞吐量≥6G，事务处理能力 （TPS）≥110000，每秒新建连接 （CPS ） ≥ 38000 ，并发连接数≥600000 ； 二、功能指标要求 1．在保证业务和页面展示效果的情况下，对响应页面中的 Form 表单、a 标签、Javascript 文件等关键信息的混淆，支持配置例外 URL，不对其进行混淆操作。 2．支持对 URL 生成令牌进行令牌认证，能够进行 URL 伪造校验。 3．支持全局的 URL 白名单，白名单中的 URL 默认不会去做令牌的检验。 此外，令牌都是每一次请求中随机生产的，且是一次性的令牌，无须设置过期时间。 4．★支持自动化工具识别，并能够对自动化工具访问请求配置放过、阻断、接受、伪装等处置动作。可以根据客户端环境检测，识别攻击工具，主要包括：市面上主流扫描器，如 burpsuite、nessus 等，市面上主流自动化工具 selenium、phantom js 等，脚本攻击识别。 5．支持对于自动化流量占比的实时统计、24 小时内新增 Bot 数统计、24 小时内新增重要且未处置 Bot 数统计、新增未知 Bot 数统计。 6．支持对于 bot 的风险评分、归属地统计、首次发现时间、最近活跃时间、处置

		结果的标签化展示。 7．要求设备支持对于攻击者的意图标签展示、访问业务展示、访问时间线展示。 8．支持自动化流量趋势可视化展示。 9．★API 流量请求，至少实现以下功能：API 资产自发现、API 滥用监控、API 异常调用检测、API 流量检测。 1） API 资产自发现：支持自动从流量中识别 API 接口、支持手动新建识别 API 接口、支持对已有 API 接口的集中管理，包括下线、上线、删除、导入、导出等； 2） API 滥用监控：支持对 API 接口请求频率进行控制，可从每秒请求频率进行控制和指定时段内请求频率进行控制； 3） API 异常调用监测：支持对不符合预定义规律的业务接口调用检测； 4） API 接口流量监控：支持敏感 API 接口检测。 10．支持基于客户端指纹、POST 异常行为、请求资源类型、敏感 URL 路径、UA 切换、响应码、登录账号密码、注册账号密码等多个维度的被动模块检测。（投标文件中提供功能截图） 11．生物特征识别，要求针对用户的操作行为进行检测和分析，包括检测鼠标的点击、鼠标的移动、键盘输入等不低于 10 种生物特征收集。 12．系统支持基于 IP 的行为分析，针对访问的 URL 总数，以及 URL 种类，携带 UA 数量，并且对平均访问时间间隔做出统计；支持基于 URL 的行为分析，统计并展示访问 IP 总数和访问 UA 种类数。（投标文件中提供功能截图） 13．支持多种形式的锁定时间设置，能够在特殊时期提供快速运维能力，一键封堵所有 POST 请求入口，遇到紧急情况时能够一键封锁，保证站点安全。支持夜间模式、时长锁定、自定义锁定三种锁定模式。 14．★产品自有请求协议合规、文件上传和下载的合规校验，实现对业务流量的合规约束，支持基于请求 URL、扩展名、方法等属性进行合规性校验，支持对 HTTP 请求通用头部进行合规性校验，对于不合规请求，支持放过、阻断、接受、伪装等处置动作。 15．支持防护撞库、漏洞扫描、扫描器攻击、自动化攻击等威胁场景。 16．要求设备支持统计总请求数、异常请求数、正常请求数；“恶意客户端”维度，包含恶意 IP 个数、恶意指纹个数；“流量大小”维度，包含总流量大小、攻击流量及

		所占百分比。 17．支持资产风险指数视图：提供被动态应用保护系统保护的客户资产的风险指数（健康度），绘出风险为高危/中危/低危的资产分布情况。 18．支持网站流量清洗视图：提供根据资产风险指数图中统计出来的高危/中危/低危防护资产，展示这些资产的请求流量及攻击流量趋势图。 19．支持攻击源画像视图：以攻击源的视角，展示出动态应用保护系统统计的 TOP 5 的攻击源的攻击行为。内容展示：针对 TOP 5 的每个攻击源，展示的内容有： IP；攻击次数；攻击路径个数。 20．具备 IP 信誉库，包含以下 6 大类 IP 信誉，（1）DDOS 攻击；（2）安全漏洞；（3）垃圾邮件；（4）Web 攻击；（5）扫描源；（6）Botnet 客户端。（投标文件中提供功能截图） 21．支持（1）转发模式：进入该模式后，流量将不经过引擎处理直接转发，设备没有防护功能。（2）防护模式：在防护模式下，设备具有防护功能。（3）调试模式：与防护模式类似，设备也有防护功能，但是能从后台看到更多的调试信息，通常用于调试设备。 22．★支持设备引擎自检，检查每个工作线程的延迟情况，支持收集设备假死时的引擎状态信息，支持设备引擎故障自动启用转发或重启。 支持日志引擎状态自检、并发连接进程监控 、bot 日志进程检测、证书授权及状态检查等能力。 23．产品具有公安部颁发的《计算机信息系统安全专用产品销售许可证》，并在投标文件中提供证书复印件。
漏洞扫描设备	1 台	一、★基本要求 1、标准 1U 机架式设备，配置 10M/100M/1000M 自适应以太网电口扫描口≥5 个，千兆光口≥4 个，不少于 1 个接口扩展槽位。 2、支持 IPv4 和 IPv6 的不同协议部署和扫描，最大并发扫描数主机 IP≥60 个，最大并发任务数≥10 个； 3、配置 WEB 应用漏洞扫描模块，支持系统漏洞扫描和 WEB 漏洞扫描，授权可扫描总数量为无限的 IP 地址或域名，提供不少于 1 路端口扫描授权； 4、提供不少于 3 年硬件质保及系统软件升级；提供不少于 3 年系统漏洞库、Web 漏洞

		库升级服务。 5、产品具有公安部颁发的《计算机信息系统安全专用产品销售许可证》，并在投标文件中提供证书复印件。 二、功能指标要求 1．支持检测的漏洞数大于230000条，兼容CVE、CNCVE、CNNVD、CNVD、Bugtraq等主流标准。（投标文件中提供相关证明截图） 2．同时支持远程扫描和采用SMB、SSH、RDP、Telnet等协议对Windows、Linux等系统进行登录扫描； 3．内置不同的漏洞模板针对Unix、Windows操作系统、网络设备和防火墙等模板，同时支持用户自定义扫描范围和扫描策略；支持自动模板匹配技术。 4．提供高级漏洞模板过滤器，支持将符合筛选条件的漏洞自动加入到自定义漏洞模板中，及后续插件升级包中的漏洞也可以自动加入到模板中。 5．支持扫描国产操作系统、应用及软件的安全漏洞，如华为欧拉、open欧拉、统信、麒麟、bclinux、达梦、南大通用、人大金仓、神通、金蝶、东方通。 6．支持专门针对DNS服务的安全漏洞检测，包括DNS投毒等漏洞检测能力；支持“幽灵木马”检测。（投标文件中提供功能截图） 7．支持专门针对已有攻击利用代码的漏洞检测，检测用户资产是否存在可利用的漏洞。（投标文件中提供功能截图） 8．具备单独口令猜测扫描任务，支持多种口令猜测方式，包括利用RDP、SMB、TELNET、FTP、SSH、POP3、TOMCAT、SQL SERVER、MYSQL、ORACLE、SYBASE、DB2、SNMP、Onvif、RTSP、ActiveMQ、IMAP、MongoDB、SMTP等协议进行口令猜测，允许外挂用户提供的用户名字典、密码字典和用户名密码组合字典。 9．支持智能端口挖掘，可以智能发现非默认端口启动的服务。 10．支持扫描时间段控制，只在指定时间段内执行任务，未完成任务在下一时间段自动继续执行。 11．支持立即执行、定时执行、周期执行扫描任务，自定义的周期时间可精确至每*月第*个星期*的*点*分。 12．★支持断点续扫，可对已完成的扫描任务中没有被覆盖到的目标重新下发扫描任务。

		13．支持复用已有任务配置用于新的扫描任务。 14．支持风险告警和风险闭环处理，可在集中告警平台灵活配置告警内容、告警方式、告警资产范围等，支持邮件和页面告警，支持单个或批量修改风险状态。（投标文件中提供功能截图） 15．★支持自定义风险值计算标准配置，可对主机风险等级评定标准和网络风险等级评定标准进行自定义。 16．支持通过仪表盘直观展示资产风险值、主机风险等级分布、资产风险趋势、资产风险分布趋势等内容，并可查看详情。 17．支持不同用户角色权限管理，区分系统管理员、普通用户、审计管理员等角色，不同管理员拥有不同的管理权限。 18．报表能提供针对不同角色的默认模板，离线报告支持 HTML、WORD、EXCEL、PDF、XML 等格式，报告可以直接下载或自动通过邮件直接发送给相应管理人员。 19．支持多用户分级权限管理，可为每个用户角色分配账号、任务级的权限分配、允许登录的 IP 范围和允许扫描的 IP 范围等。 20．提供审计功能，能够对登录日志、操作日志和异常报告进行记录和查询。 21．提供灵活的报表自定义，可定制报表标题、封面 logo、报表页眉和页脚、报表各章节显示内容。（投标文件中提供功能截图） 22．支持高级数据分析，可对同一 IP 的两次扫描结果进行风险对比分析，并可在线查看同一 IP 的多次历史扫描结果。 23．★提供 Web 应用扫描能力，提供多种 Web 应用漏洞的安全检测，如 SQL 注入、跨站脚本、网站挂马、网页木马、CGI 漏洞等。 支持登录预录制功能，能够根据用户操作，录制并指定 Web 扫描 url，使产品能够扫描和分析一些常规页面爬取程序检测不到的 url。
二、商务条款要求：		
★合同履行期限		合同签订后 15 天内交货；设备到货验收后 15 天内完成安装调试。技术支持、售后服务及质量保障期 3 年，从项目验收合格之日起计算。
★交货地点		广西区内采购人指定地点。
★报价要		投标报价指货物、标准附件、备品备件、专用工具、运输、安装、调试、验收等

求	各种费用和售后服务、税金及其它所有成本费用的总和。
项目系统集成要求	1、 中标人须完成中标产品的安装调试、线缆部署等系统集成工作，本项目采购的设备的相应配件（譬如光纤线、电源线等）若与使用单位环境不符，中标人及中标品牌厂家需更换为符合环境的同等或更高级别配件；部署新增软硬件设备不得对现有系统造成影响，不得影响业务系统正常运行； 2、 中标人在实施前，须提供详细的安装实施方案给采购人审核，经采购人确认后，方可进行项目实施。中标供应商完成所供软硬件的安装部署还需根据采购人的要求按成以下集成工作： （1）根据应用系统实际情况设置相关策略，完成防病毒网关、远程安全评估系统、Web应用防护系统部署调试工作； （2）对新购网络安全设备与现有网络安全相关软硬件设备环境进行集成联调及调优工作；须与采购人系统内网络安全相关软硬件设备的服务商等进行积极主动的合作，服从采购人的统一协调，完成项目的各个阶段；实施部署完成后提交采购人完整的配置文档。 （3）安装部署阶段，至少提供具备3年以上网络安全行业从业经历的3名服务工程师保障本项目的实施工作，其中一名工程师需是所供产品原厂工程师，一名工程师需获得CISP注册信息安全专业人员证书。
售后服务要求	（1）安装实施服务：中标人必须按照本项目的要求，完成中标产品的安装部署实施工作。要求中标人确保中标产品能在采购人现有网络环境安全、可靠、稳定的运行，不影响现有业务系统的正常使用；实施过程中如中标产品可能会对现有业务系统有重大影响的，中标人应提前三天将涉及到这个环节的实施方案提交给采购人，经过采购人认可并商定实施时间后，方能按照商定的时间进行实施。 （2）质保期内技术支持服务：提供7*24小时技术支持服务，电话服务请求的响应时间应少于1小时，在接到报故障后，应在2小时内派技术人员到现场，进行故障排查及修复工作。在质保期内由中标人提供中标产品的定期特征库升级服务；对于软件版本的重大升级，需由原厂技术工程师亲自上门实施，确保中标产品的稳定运行；重要病毒需要紧急处置的，需由原厂工程师在24小时内提供紧急处置服务。 （3）异常故障分析服务：采购人的网络环境发生调整导致中标产品不可用时，中标人要协调原厂技术工程师提供紧急现场服务，1小时内到达指定现场，分析故障原因

	并提出解决方案，故障处置过程复杂的，原厂技术工程师要提出临时解决方案，确保采购人网络的正常运行。 （4）重要时期网络安全保障服务：中标人在采购人指定的重要时期提供24小时不间断的网络安全保障服务，服务期不少于5天，服务期内由技术工程师监控中标产品的运行状态，对可能出现影响业务稳定性的安全风险能提供24小时不间断的监测、处理、分析、溯源、应急处置等服务，确保网络安全。 （5）培训服务：中标人负责对采购人指定的技术人员进行技术培训，培训内容包括产品操作、维护、简单维修和其他采购单位要求的内容，经培训应能进行日常运行维护工作。
★付款方式	签订合同之日起 15 个工作日内，采购人预付款合同总金额的 60%；所有货物验收合格并交付正常使用后，采购人根据项目验收标准及本项目合同罚则条款进行考核，按考核结果对合同服务费进行核算后，15 个工作日内支付合同剩余款项。 采购人付款前，中标人应向采购人开具等额有效的增值税发票，采购人未收到发票的，有权不予支付相应款项直至中标人提供合格发票，并不承担延迟付款责任。
验收方式及标准	（一）验收条件 本需求书中包含的设备按期完成安装、部署、配置，以及组织管理和项目文档满足本采购文件的规定要求。 （二）验收标准 以本需求书中相关内容及其要求为依据，作为项目验收标准。供应商是否按照本招标需求书中定义的各项要求开展各项设备安装部署工作，工作流程和结果是否符合采购人质量管理要求，是否在规定时间内提交相关工作文档。 （三）验收流程 符合项目验收条件后，供应商可提出项目验收书面申请。向采购人提交验收申请。 向采购人整理提交项目相关管理、技术文档。 采购人对项目工作内容及文档进行验收，项目验收通过后，采购人出具项目验收报告。
安全保障和罚责要求	★1.信息安全保密要求 （1）必须严格遵守国家税务总局广西壮族自治区税务局的安全保密制度。 （2）项目人员需保证遵守国家有关版权和知识产权保护的政策、法律、法规和制

	度。 （3）项目人员应对本项目中接触到的国家税务总局广西壮族自治区税务局所有的知识产权、商业秘密、技术成果等信息负保密义务。未经国家税务总局广西壮族自治区税务局书面同意，不得向社会公众或第三方通过任何途径出示、泄露，不得许可使用，不得对上述信息进行复制、传播、销售；保证不向外泄漏任何相关数据，不向外泄漏任何保密的技术资料。如出现支持人员泄密事件，中标人应负有连带责任。 （4）中标供应商须与国家税务总局广西壮族自治区税务局签署合同项目实施期间的信息保密协议。 （5）项目人员必须与国家税务总局广西壮族自治区税务局签署合同项目实施期间的信息保密承诺书。 ★2.中标人运维人员在合同期间应严格按采购人的网络安全和数据安全相关规定开展工作，由于中标人运维人员网络安全工作落实不到位引发安全事件的，采购人将视安全事件严重情况按合同金额的20%-30%的比例进行扣减。 安全事件具体内容主要包括(但不限于)以下内容： （1）因补丁升级、漏洞修复、系统杀毒、数据备份、应用监控、网络监控等工作未落实到位，发生服务器被控制和应用系统被攻破的安全事件，被主管部门通报的。 （2）因违规进行税费数据查询、导出和拷出等操作造成敏感数据泄漏，以及发生非法窃取数据行为。 （3）因运维操作处置不当导致重要应用系统发生严重卡顿、停用的重大事件。 ★3.罚责条款：项目建设和运维过程中，因系统在对接、运行等服务中，导致其他系统受到影响的，由中标人负责组织相关服务厂商共同排查，明确问题根源、责任并报告采购人。中标人无法判定问题根源的，由中标人承担全部责任。采购人将根据问题的轻重、中标人责任的大小，扣除不高于合同款5%服务金额。
其他要求	1.中标人须在项目实施中负责解决全部技术问题。若投标文件中的设计或实施方案出现不合理或不完整的情况，中标人有责任和义务提出补充修改方案并征得采购人同意后付诸实施，所需费用由投标人承担，采购人不再支付任何费用。 2. 投标人可以根据项目要求，在投标文件中提供包括但不限于：项目实施方案、技术方案、售后服务方案等