

采购项目技术和商务要求

一、基本概况

本项目拟定采购全网上网行为管理设备 2 台，交换机 2 台，应用交付网关 2 台，防火墙 2 台，堡垒机 1 台，VPN 设备 2 台，漏洞评估系统 1 台，加强对病毒传播、网络攻击、APT 攻击等进行纵深布防和日常网络安全运维，需对长城网入网设备、系统和拟开设网站进行审核备案，引接开放式网络测量平台等先进技术手段，拓展网络钓鱼、木马病毒、拒绝服务、域名劫持、网站攻击、安全漏洞等系统防护手段，并为 5G 智慧应用和手机管控、医院网络多种业务提供安全支撑。

二、需求内容（技术参数）

1、全网上网行为管理设备

全网行为管理聚焦企事业组织网络行为安全，实现全网资产、身份、行为可视可控，智能感知内部威胁风险，帮助用户构建有效防御体系。

2、应用交付网关

应用交付能够为用户提供包括多数据中心负载均衡、多链路负载均衡、服务器负载均衡的全方位解决方案。不仅实现对各个数据中心、链路以及服务器状态的实时监控，同时根据预设规则，将用户的访问请求分配给相应的数据中心、链路以及服务器，进而实现数据流的合理分配，使所有的数据中心、链路和服务器都得到充分的利用。应用交付还支持与各个云平台对接，实现云场景下租户的自服务负载需求。

3、堡垒机

内置运维安全管理系统，可将运维人员离散维护主机及网络设备的行为统一到该平台进行，包含系统安全以及运维的控制力。可统一部署主机和应用安全策略在；对所有用户在主机上的操作行为进行监控与记录，实时了解用户的操作行为，发现风险及时中止用户的操作，并记录下用户所有的操作

行为，用于进行事后的审查与取证。

4、VPN

集成 SSL/IPSec，采用国家密码管理局颁布的 SM1、SM2、SM3、SM4 密码算法及其协议，支持多种身份认证方式、细粒度访问权限控制等主要功能，支持配置扩展终端 agent 功能，agent 用于远程系统接入的用户身份安全、终端/数据安全、传输安全、应用权限安全和审计安全，符合国家商用密码标准。

5、漏洞评估系统

通过 WEB 漏洞扫描、系统漏洞扫描、弱口令扫描、安全基线扫描、数据库扫描这五个组件对网络里的各种元素进行安全性的检查。

6、防火墙

提供 L2-L7 层各类威胁的检测和防护，能够有效应对传统网络攻击和未知威胁攻击。

7、交换机

设备入网，支持全端口线速转发、VLAN 划分等配置管理。

详见技术参数

技术要求			
序号	技术和性能参数名称	招标参数和性能要求	备注
*1	基本要求	全网上网行为管理：2 台 交换机：2 台 应用交付网关：2 台 防火墙：2 台 堡垒机：1 台 VPN：2 台 漏洞评估系统：1 台	
	资格性条件	产品资格：国产设备	
2	配置要求		
2.1	全网上网行为管理	<p>*1. 网络层吞吐量$\geq 3\text{Gb}$，应用层吞吐量$\geq 300\text{Mb}$，带宽性能$\geq 200\text{Mb}$，支持用户数≥ 1000，每秒新建连接数≥ 2400，最大并发连接数≥ 120000，机架式设备，接口≥ 6 千兆电口+2 千兆光口 SFP</p> <p>2. 支持网关模式，支持 NAT、路由转发、DHCP、GRE、OSPF 等功能；支持网桥模式，以透明方式串接在网络中；支持电口 bypass；</p> <ul style="list-style-type: none"> • 3. 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、重定向至制定线路； <p>3. 功能描述：全网行为管理聚焦企事业单位网络行为安全，实现全网资产、身份、行为可视可控，智能感知内部威胁风险，帮助用户构建有效防御体系。</p> <p>4. 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> <p>5. 支持攻击、双机切换告警、移动终端管理告警、风险终端发现告警、web 关键字过滤告警、杀毒告警、设备流量超限告警、磁盘/CPU/内存异常告警等；</p> <p>针对单用户的行为分析（包括：应用流速趋势、应用流量排行、域名流量排行、应用时长排行、域名时长排行、行为汇总排行等）；</p> <p>6. 支持图形化查看当前内网 IP 使用情况，帮助管理员减少人工维护 IP 表的工作量；</p> <p>对网络接入的终端进行可视化管理，展示终端详细信息、异常状态等；支持查看终端类型，以及终端详细信息（厂商，系统，端口等）；支持查看终端类型分布；</p> <p>7. 支持 Teamviewer、向日葵、Anydesk、RDP 的远程应用的外发文件审计；</p> <p>8. 支持发现私接路由（或者共享软件等）共享网络的行为并支持至少以下 2 种功能：1. 支持自定义配置终端数量和冻结时间同时支持添加信任列表；2. 支持在数据中心报表中可查询通</p>	

		过共享上网的 IP、用户，并能导出报表；	
2.2	交换机	<p>*1. 性能描述：交换容量 $\geq 336\text{Gbps}/3.36\text{Tbps}$，包转发率 $\geq 96\text{Mpps}/126\text{Mpps}$。</p> <p>• 2. 接口描述：24 个 10/100/1000Base-T 自适应电口，4 个千兆 SFP 光口。</p> <p>3. 功能描述：支持全端口线速转发、VLAN 划分等配置管理</p> <p>4. 支持 MAC 地址 $\geq 32\text{K}$，支持 4K 个 VLAN，支持 STP、RSTP、MSTP 协议；</p> <p>5. 支持端口聚合，支持手工和静态 LACP；</p> <p>6. 支持堆叠技术。</p>	
2.3	应用交付网关	<p>*1. 性能描述：四层吞吐量 $\geq 2\text{Gbps}$，四层并发连接数 ≥ 3000000，4 层新建连接数 CPS ≥ 90000，7 层新建连接数 RPS ≥ 80000；</p> <p>• 2. 接口描述：机架式设备，接口 ≥ 8 千兆电口；</p> <p>3. 功能描述：应用交付能够为用户提供包括多数据中心负载均衡、多链路负载均衡、服务器负载均衡的全方位解决方案。不仅实现对各个数据中心、链路以及服务器状态的实时监控，同时根据预设规则，将用户的访问请求分配给相应的数据中心、链路以及服务器，进而实现数据流的合理分配，使所有的数据中心、链路和服务器都得到充分的利用。应用交付还支持与各个云平台对接，实现云场景下租户的自服务负载需求；</p> <p>4. 支持基于 URL 的链路调度功能，内置不少于 1000 条的国外 URL 网址库，自动更新，可查看并进行编辑。可根据 URL 将访问国外网站的请求调度到指定线路。</p> <p>设备同时支持链路负载均衡和服务器负载均衡的功能。同时处于激活可使用状态，无需额外购买相应授权；</p> <p>5. 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、加权最小流量、按主机加权最小流量、加权源 IP 哈希、带宽比例、哈希、首个可用、优先级等算法；</p> <p>6. 服务器负载状态支持投屏展示，能够显示设备的电源状态、风扇转速、磁盘温度、CPU 温度、CPU 和内存占用率、新建连接数、并发连接数、吞吐情况、SSL 新建和 SSL 吞吐数据、压缩优化和缓存优化数据；业务的健康状态、新建连接数、并发连接数、上下行流量、每秒请求数；节点池的调度算法、健康状态、新建连接数、并发连接数、上下行流量；</p> <p>7. 支持 HTTP 缓存功能，利用内存 Cache 缓存用户频繁访问的 web 内容，降低后台服务器的负载压力，提升用户访问的响应速度；</p> <p>8. 支持基于应用协议的智能选路，能对网银、游戏、视频等流量进行调度，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。</p>	

2.4	防火墙	<p>*1. 性能描述：网络层吞吐量$\geq 12\text{G}$，应用层吞吐量$\geq 4.4\text{G}$，防病毒吞吐量$\geq 1\text{G}$，IPS 吞吐量$\geq 800\text{M}$，全威胁吞吐量$\geq 650\text{M}$，并发连接数≥ 200 万，HTTP 新建连接数≥ 8 万；</p> <p>• 2. 接口描述：接口≥ 6 千兆电口+2 千兆光口 SFP；</p> <p>3. 功能描述：提供 L2-L7 层各类威胁的检测和防护，能够有效应对传统网络攻击和未知威胁攻击；</p> <p>4. 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；</p> <p>5. 支持与国家位置信息结合设置安全策略，识别流量发起的国家或地区的位置信息，根据流量发起的国家或地区的访问位置信息实现对不同区域访问的差异化控制；</p> <p>6. 支持基于地区维度设置流控策略，实现多区域流量批量快速管控功能；</p> <p>7. 支持勒索病毒检测与防御功能，预定义漏洞特征数量超过 6000 种，支持在产品漏洞特征库中以漏洞名称、漏洞 ID、漏洞 CVE 标识、危险等级和漏洞描述等条件快速查询特定漏洞特征信息，支持用户自定义 IPS 规则；</p> <p>8. 支持对文件传输行为进行安全过滤，支持基于上传、下载、双向的文件内容过滤，内容过滤类型至少支持网页、脚本、压缩文件、图片、可执行文件、适配、文本等常见文件类型。</p>	
2.5	堡垒机	<p>*1. 性能描述：默认包含运维授权数≥ 50，最大可扩展资产数≥ 150，图形运维最大并发数≥ 100，字符运维最大并发数≥ 200。</p> <p>*2. 接口描述：机架式设备，硬盘容量$\geq 1\text{T}$ SATA，接口≥ 6 千兆电口。</p> <p>3. 功能描述：内置运维安全管理系统，可将运维人员离散维护主机及网络设备的行为统一到该平台进行，包含系统安全以及运维的控制力。可统一部署主机和应用安全策略在；对所有用户在主机上的操作行为进行监控与记录，实时了解用户的操作行为，发现风险及时中止用户的操作，并记录下用户所有的操作行为，用于进行事后的审查与取证。</p> <p>4. 采用物理旁路部署，不改变现有网络结构，系统各模块支持以 B/S 方式管理，采用 https 加密方式访问；支持 SSHv1、SSHv2、TELNET、RDP、VNC、FTP、SFTP、RDP 磁盘映射、RDP 剪切板，支持通过协议前置机进行协议扩展，至少支持扩展 KVM、Vmware、数据库、http/https、CS 应用等</p> <p>5. 支持通过动作流配置，接入的用户的登录动作可通过动作流配置都可以实现单点登陆和审计接入；</p> <p>6. 用户登陆认证方式支持静态口令认证、手机动态口令认证、Usbkey（数字证书）认证、AD 域认证、Radius 认证等认证方式；并支持各种认证方式和静态口令组合认证；</p> <p>7. 支持 unix 资源、windows 资源、网络设备资源、数据库资源、C/S 资源、B/S 资源；支持批量导入、导出资源信息；支持手动添加、删除、编辑、查询资源，支持变更默认运维端口，支持网络设备 enable 和 unix 主机 su 等身份切换的单点登录功能；</p>	

		<p>8. 支持 RDP 安全模式（RDP、NLA、TLS、ANY）设置，以适应 RDP-Tcp 属性中的所有功能配置，包括加密级别为客户端兼容、低、高、符合 FIPS 标准等加密级别；</p> <p>9. 支持一对一、一对多、多对多授权；支持按授权名称、用户名称、用户账号、资源名称、资源地址、资源账号查询已授权信息；支持生成授权报表和可访问外部资源报表，报表详细展示用户和资源的授权关系，并提供 EXCEL、WORD、PDF、HTML 等格式导出；</p> <p>10. 支持命令黑名单，对字符型设备（如 linux/unix/网络设备）的高危命令执行进行阻断；支持配置资源访问时间规则；支持对文件传输类协议进行传输控制；</p> <p>11. 在图形资源访问时，具备键盘、剪切板、窗口标题、文件传输记录功能，并且对图形资源的审计回放时，可以从某个键盘、剪切板、窗口标题、文件传输记录的指定位置开始回放；</p> <p>12. 支持从 WEB 页面设置多端口绑定，防止单网卡或单网线故障发生。</p>	
2.6	VPN	<p>*1. 性能参数：最大理论加密流量（Mbps）≥ 350，最大理论并发用户数≥ 8000，IPSec 加密最大流量（Mbps）≥ 200，设备整机理论最大吞吐量$\geq 1.2\text{Gbps}$，设备整机理论最大并发会话数$\geq 150\text{W}$；</p> <p>• 2. 接口描述：机架式设备，接口≥ 6千兆电口+4千兆光口 SFP，配置冗余电源；</p> <p>3. 功能描述：集成 SSL/IPSec，采用国家密码管理局颁布的 SM1、SM2、SM3、SM4 密码算法及其协议，支持多种身份认证方式、细粒度访问权限控制等主要功能，支持配置扩展终端 agent 功能，agent 用于远程系统接入的用户身份安全、终端/数据安全、传输安全、应用权限安全和审计安全，符合国家商用密码标准；</p> <p>4. 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；</p> <p>5. 支持防中间人攻击，可在用户登录 SSLVPN 时智能判断存在中间人攻击行为，断开被攻击的连接，并可提示异常现象；</p> <p>6. 支持主从认证账号绑定，必须实现 SSL VPN 账号与应用系统账号的唯一绑定，VPN 资源中的系统只能以指定账号登陆，加强身份认证，防止登录 SSL VPN 后冒名登录应用系统。</p>	
2.7	漏洞评估系统	<p>*1. 性能参数：系统漏扫最大可添加 IP 或域名数≥ 508（2 个 C 类网段地址数量） 系统扫描 IP 并发≥ 50；Web 漏扫最大可添加网站数≥ 16；Web 扫描并发，数据库扫描并发，基线检测并发，口令破解并发。</p> <p>• 2. 接口描述：机架式设备，CONSOLE 口≥ 1个，USB 口≥ 2个；100/1000M 电口≥ 4个；固态硬盘$\geq 32\text{G}$；</p> <p>3. 功能描述：通过 WEB 漏洞扫描、系统漏洞扫描、弱口令扫描、安全基线扫描、数据库扫描这五个组件对网络里的各种元素进行安全性的检查。</p> <p>4. 支持全面扫描、资产发现、系统漏洞扫描、弱口令扫描、WEB</p>	

		漏洞扫描、基线配置核查六种任务类型，其中全面扫描支持系统漏洞扫描、WEB 漏洞扫描、弱口令扫描同时执行； 5. 支持域管理功能，系统默认数据域、内置终端接入域、运维管理域、其他业务域、核心业务域、核心交换域、对外服务域、外联域、互联网出口域等，可根据客户实际情况进行自定义管理； 6. 支持检测的漏洞数 ≥ 230000 条，兼容 CVE、CNNVD、CNVD、Bugtraq 等主流标准；支持操作系统、网络设备、数据库、中间件等漏洞扫描；支持多种系统漏洞检测技术；支持采用 SMB、RDP、Telnet、SSH 等协议对系统进行登录扫描。	
商务要求(均为实质性响应条款，不接受负偏离)			
3	售后条款		
3.1	保修年限	免费提供原厂维保不少于 3 年	
3.2	维修响应时间	7*24 小时维保服务，紧急事件 2 小时到场	
3.3	升级与软件维护	维保期间免费升级维修	
3.4	交货期	合同签订后 1 个月内	
3.5	付款方式	签订合同后不付款，物质到货上线部署后付合同金额的 70%，验收完成后付合同金额的 25%，质量保证金为合同金额的 5%。	
<p>备注：1.商务条款及硬件部分不接受负偏离。</p> <p>2.加注“*”、“.”号的技术指标均需提供证明材料。</p> <p>3.技术和商务指标为文字性描述内容则提供全部响应承诺。</p> <p>4.供应商须提供相关技术指标证明材料予以佐证（证明材料不限于产品规格表、制造商官方网站发布的产品信息、说明书等或检测机构出具的检测报告等技术资料支持的、产品彩页、技术白皮书、厂家出具的技术证明文件、实物照片、软件功能截图等）。</p>			

