**许昌市中级人民法院“内网安全”项目需求**

（一）项目概况

（1）项目名称：内网安全

（2）项目需求：安全审计、安全控制、服务器、交换机等

（3）采购预算：65元。

（4）招标方式：公开招标

（二）投标条件

（1）符合《政府采购法》第二十二条之规定；

（2）具有相应的经营范围；

（三）货物需求或者项目需求

**例1：**货物需求

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 序号 | 名称 | 类别 | | 详细参数与要求 | 单位 | 数量 |
| （一）．**运维安全审计系统** | | | | | | |
| （一） | **运维安全审计系统** | 总体要求 | | **硬件架构：**采用1U专用的硬件架构，硬件架构采用模块化设计，便于进行接口扩展和硬件升级；支持扩展大容量存储介质用于日志存储，存储空间不小于1TB。 | 台 | 1 |
| **系统要求：**服务器端采用嵌入式Linux系统设计，以软硬件一体的形式保证服务器安全稳定运行；  采用专用安全操作系统。 |
| **接口要求：**含6个千兆自适应电口,2个光口；  **图形会话并发：**不小于4000；  **字符会话并发：**不小于6000；  **工作模式：**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，不改变运维人员的运维习惯。 |
| 组织结构 | | **1**、AD域同步**：**支持从AD域抽取OU，方便快速建立组织结构；**2**、AD域同步**：**主帐号支持从AD域内抽取，方便快速建立主账号；**3**、用户策略：通过配置口令策略，达到指定密码有效期和限制主帐号密码强度的目的。 |
| 资源管理 | | **1**、资源统计：支持柱形图方式查看系统中不同资源所占比例；**2**、资源类型**：**unix资源、网络资源、windows资源、数据库资源、C/S资源、B/S资源、中间件资源、大型机资源；**3**、资源协议：支持SSH、TELNET、FTP、SFTP、VNC、XWINDOW、WINDOWS文件共享等协议。其中，SSH协议代理支持SecureCRT软件的Session Clone及Send To All等复杂的功能。4、自动改密：支持对unix资源、网络资源、windows资源、数据库资源、中间件资源进行密码变更。 |
| 授权管理 | | **1**、角色管理：支持自定义角色。角色可按照组节点进行定义，从而实现分层分级管理模式；**2**、岗位授权：资源授权模式基于岗位授权，授权可迁移；并可针对岗位设置相关安全策略。 |
| 单点登录SSO | | **1**、收藏夹功能：运维人员可将经常访问的资源添加到收藏夹；**2**、批量单点登录：批量单点登录资源。 |
| 安全管理 | | **1**、访问时间策略：可以配置成可访问时间段方式，也可以配置成不可访问时间段方式；**2**、地址策略:可以配置成可访问IP段方式，也可以配置成不可访问IP段方式；**3**、审计策略:根据不同设备审计安全需求，客户自定义审计范围，字符（命令、内容、录像）、图形、FTP；**4**、VPN功能:内置VPN功能，无需专用VPN硬件支持，即可方便安全地通过远程接入堡垒机。 |
| 审计管理 | | **1**、图形审计：图形资源访问时，支持键盘、剪切板、文件传输记录；**2**、字符审计：对字符命令方式的访问可以审计到所有交互内容；**3**、实时监控：操作人员对于资源的访问，审计员可以实时查看。发现高危操作时，支持实时切断当前会话。 |
| 系统配置 | | 外接存储:支持日志数据的外置存储备份，支持NFS和windows文件共享协议，远程审计存储和本地存储对审计员透明。 |
| 高可用性 | | **1**、HA：支持以Active-Standby方式部署，支持服务及应用层面的检测，支持双网卡冗余（双网卡虚拟单Ip）；**2**、集群部署：支持堡垒机集群模式部署；支持应用发布服务器的集群部署，可以设定自动选择应用发布服务器，或者由用户手动指定。 |
| 品牌要求 | | 为了便于管理，并与网络接入控制形成联动，要求与网络接入控制系统同一品牌。 |
| **★售后服务** | | **服务要求：**提供一年原厂免费安装、调试、维护、升级、应急响应服务。 |
| **（二）．网络接入控制系统** | | | | | | |
| （二） | **网络接入控制系统** | **总体要求** | | **系统架构：**  标准采用B/S架构，便利易操作管理设计；  支持VPN/拨号接入、分支机构联动管理。 | 套 | 1 |
| **系统性能：**  要求服务器采用嵌入式Linux系统设计；  提供断电保护机制，如心跳、Bypass等；  客户端支持X32\X64平台的 Win2000/2003/XP/Vista/WIN7操作系统；  终端与服务器、控制平台之间策略更新时间小于4秒钟。 |
| **配置要求：**  要求必须为软硬一体设备，1U机型服务器  并发会话数：≥1200000  标配6个千兆电口，具有一个扩展槽位，支持4个端口千兆光纤扩展卡或2个万兆光口扩展卡。 |
| **客户端要求：**  要求客户端必须支持在线下载一键式安装，提升安装效率；  **★**要求全功能模块客户端安装包不得超过30M，减少对资源的占用。 |
| **部署要求**  支持旁路、网桥、网关3种部署方式,必须支持端口镜像旁路及串接方式部署；  支持HUB及无线AP环境部署条件,兼容所有网络设备,支持傻瓜式交换机和路由器；  设备部署过程中不能改变原有网络结构及网络、安全等设备的配置；  支持多级级联管理，独立级联数据汇总服务器，统一管理平台  支持负载均衡，同一网段内部署多台准入服务器，统一平台管理，自定义管辖IP范围。 |
| **平台要求:**  准入控制、终端安全、DLP数据安全防护、MDM（移动终端管理）系统可在同一平台展示（须提供同一平台的界面截图并加盖原厂商公章）。 |
| **功能要求** | | **准入技术**  要求采用NACP准入技术（即思科的NAC和微软的NCP技术相结合），以支持所有可网管及非可网管网络设备，进而达到管理无盲区；  支持阻断跨NAT路由器下未安装插件的计算机，放行合法的计算机。 |
| **身份鉴别：**支持组合身份鉴别方式，可根据用户、密码进行身份鉴别，支持LDAP、AD域联动身份鉴别、Email账号密码身份鉴别、USB Key身份鉴别、短信验证码身份鉴别等技术进行单一和组合方式对入网用户进行鉴别控制。 |
| **安全测评：**必须支持对入网终端移动存储介质、光驱介质、3G上网卡、硬盘系统分区、网络监听端口、IP/MAC 绑定、ARP欺骗、恶意代码防范、操作系统补丁、来宾账户、口令安全、黑名单口令、Windows防火墙、超时重新登录、计算机名称、系统服务、远程桌面、系统时间、AD域环境、共享资源、telnet、剩余信息保护、非法进程、合法进程、安装程序、禁止安装程序等做详细的安全测评，通过测评允许入网，不通过则提供一键式智能修复快速入网。 |
| **违规报警：**必须支持终端用户的硬件发生变化即刻报警、终端用户接入移动存储介质后即刻报警、终端用户插入光盘后即刻报警、终端用户接入3G无线上网卡后即刻报警、终端用户IP&MAC地址发生变化后即刻报警、违规外联即刻报警、终端用户未安装恶意代码防范程序即刻报警、终端用户存在操作系统漏洞即刻报警，报警同时可进行阻断所有网络连接、关闭计算机、放置隔离区、发通知信息、邮件或短信方式通知管理员等操作。 |
| **终端网络通信域**：必须支持设置合法终端和非法终端之间的通信规则、终端用户和来宾用户之间的通信规则、部门之间的通信规则、设置自定义IP地址过滤通信规则、设置终端用户离线时的通信规则等。 |
| **安全管理：**设置终端用户是否禁用所有USB存储设备、设置终端用户是否禁止使用便携式设备、设置终端用户是否禁用所有光驱介质、设置终端用户是否禁用所有无线网卡、设置终端用户是否禁用所有3G无线上网卡、设置终端用户是否禁用手机代理上网、设置终端用户是否禁用调制解调器、设置终端用户是否禁用蓝牙设备、设置终端用户是否禁止使用其它网卡（除与服务器连接应用的网卡）、设置终端用户是否禁止使用打印机、设置终端用户是否禁止进入windows系统的安全模式、设置终端用户是否禁止修改IP地址、设置终端用户是否启用IP/MAC绑定、设置终端用户IP防火墙，控制终端计算机仅可以通信的IP范围，兼容内外网网段、设置终端用户的程序黑白名单策略、设置终端用户是否启用定时关机功能、设置终端用户是否启用规范计算机名功能、设置终端用户的文件操作审计功能、设置终端用户的浏览网站审计功能、设置终端用户的应用程序审计功能、设置终端用户是否启用超时锁屏功能。 |
| **USB存储介质管理：**必须支持设置终端用户禁止使用USB移动存储介质；设置终端用户仅允许只读访问USB存储介质；设置终端用户允许读写访问USB存储介质；将USB存储介质划分为内部分区和外部分区，在单位网络内可以同时使用内部和外部分区，在单位网络外只能使用外部分区。 |
| **资产维护：**必须支持软硬兼资产统计、终端维护申请、终端维护报表、终端维护统计、消息推送、文件分发、远程协助等。 |
| **安全审计：**必须支持对系统账户登录审计、系统账户操作记录审计、终端用户登陆审计、移动用户登陆审计、来宾用户登陆审计、新用户入网审批审计、移动用户入网审批审计、文件操作审计、浏览网站审计、应用程序审计等。 |
| **系统安全**：支持对系统管理账户限制登陆IP地址，密码最低长度和复杂性；支持对系统管理账户设置非法登陆失败限制次数、锁定时长和超时自动登出功能；支持实时检测服务器硬盘剩余空间，超过管理员配置的阔值自动报警；支持数据库自动维护机制，自动清除旧数据；支持数据库手动、自动备份；支持服务器级联管理，下属服务器数据自动向上级上传数据，上级可向下属单位下发策略性安全要求。 |
| **★售后服务** | | **服务要求：**提供一年原厂免费安装、调试、维护、升级、应急响应服务。 |
| **（三）．服务器** | | | | | | |
| （三） | **服务器** | **规格要求** | | 机架服务器高度为2U；  2 颗IntelXeonE5；2.00GHz 处理器；  64G DDR3 内存；3块3TB的3.5寸SATA盘；  配置高性能RAID 卡，支持RAID0、1、10、5、50、6、60等多种级别；双冗余交流电源；服务器管理软件，包含windows server 2012 标准版软件；DVD光驱和导轨；  3年标准+售后质保服务 | 台 | 3 |
| **（四）.接入层交换机** | | | | | | |
| （四） | **接入层交换机** | **总体要求** | | **1.**★**硬件规格：**48个10/100/1000M电口、4个千兆 SFP光接口（独立非复用）；  **2. ★设备性能：**交换容量≥256G包转发率≥132Mpps；  **3.** ★**MAC表容量**≥30K；  **4. 管理维护：**1个Console配置口、1个micro USB配置接口、1个Reset键；  **5. 防雷能力**≥7KV。 | 台 | 20 |
| **功能要求** | | **1.二层功能：**支持4K个VLAN，支持基于MAC、IP子网的VLAN、支持protocol vlan、支持private valn、支持voice vlan、支持Super vlan，QINQ等；支持端口的负载均衡、支持LACP，每个链路聚合组支持8个端口。支持STP/RSTP/MSTP。多对一的端口镜像，远程端口镜像RSPAN，流镜像；  **2. 三层协议：**支持DHCP SERVER,支持静态路由、RIPV1/V2动态路由；  **3. ACL&QOS功能：**支持标准、扩展ACL，基于MAC的ACL、基于时间的ACL等；支持IP+MAC+端口的绑定，支持SP、WRR、SP+WRR、DWRR、SDWRR等队列技术；  **4. 虚拟化功能：**支持纵向虚拟化功能，本机可以作为核心交换机的端口扩展板卡进行配置统一管理,与核心设备配合虚拟成一台设备。（提供技术实现原理说明和官网功能介绍截图证明）；  **5.设备管理：**支持SNMP、TELNET、CONSOLE、SSH管理、WEB等方式管理；  **6. ★绿色节能：**具备ROHS（Restriction of Hazardous Substances）证书；  **6.产品资质：**具备IPV4入网许可证。 |
| **（五）．机柜** | | | | | | |
| **（五）** | **机柜** | | **规格要求** | **机房机柜尺寸：**  **1.长（深）：**1.2米  **2.宽：**0.6米  **3.高：**2米 | 台 | 2 |

（四）相关要求

1、投标人须提供**运维安全审计系统、网络接入控制系统**计算机软件著作权登记证书和公安部计算机信息系统安全专用产品销售许可证，否则为**无效投标。**

2、投标人投标文件中须提供“货物需求”中的接入层交换机IPV4入网许可证原件或复印件加盖生产厂家公章；MAC表容量、 防雷能力、提供官网截图和链接说明，虚拟化功能：提供技术实现原理说明和官网功能介绍截图证明，以上说明需加盖生产厂家公章，否则为**无效投标**。

3、投标人投标文件中须提供“运维安全审计系统”、“网络接入控制系统”、“接入层交换机”生产厂家针对本项目授权文件及售后服务证明，并加盖生产厂家公章，否则为**无效投标**。

（五）付款方式

经验收合格付合同总价款的90%，剩余10%满半年无质量问题一次付清。

 （六）采购单位联系方式及地址

     联系人：陈先生        联系电话：0374-2929015