**终端准入系统建设招标技术规格书**

**一、工程说明**

随着集团公司的业务的发展，业务应用和网络使用对信息安全的保障要求越来越高，集团公司共有安全监测、人员定位、矿井三维、ERP、外网网站五个业务系统进行了等级保护测评，其中ERP系统须符合等级保护三级标准要求，其他四个业务系统须符合等级保护二级标准要求，根据《信息系统安全等级保护基本要求》（GB/T22239-2008），集团公司对定级的信息系统需要进行基本的安全等级保护。在等保相关控制点能够满足的条件下，尽量加强防护水平，实现安全的信息系统为集团公司的生产提供可靠的保障。

**二、设备采购清单**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 序号 | 设备名称 | 单位 | 数量 | 主要参数 | 备注 |
| 1 | 终端准入系统 | 套 | 1 | 支持15000台以上终端认证。  具有软件分发和部署功能。  应至少提供安全客户端（Agent）、安全控件、无客户端等多种可供自定义部署、管理模式。  能够实时监测并发现接入内网的PC、平板电脑、智能手机、IP设备等终端并自动归类。  支持终端入网IE重定向引导。  能通过浏览器完成身份认证、控件安装、设备注册、安全检查、检查结果展现等全流程引导管理。  具有Mac OS、Linux、iOS、Android等系统专属客户端，支持认证引导和准入管理。  支持IP/MAC/端口三者强制绑定，防止终端仿冒IP接入网络或移动设备位置。  具有NAT识别和检测机制能够及时发现网内私接的小路由器、无线AP、随身WIFI等NAT设备，能够清查真实网络终端。  支持对移动终端应用进行控制管理。  通过安全检查检测终端软件安装、使用状态。自动强制为终端安装软件。  冗余电源;标准配置2个1000MBASE-T接口(管理口、HA口)。  准入设备后台提供每日/每周/每月入网报告及报警信息。  支持热插拔的冗余双电源。 | 三年7\*24原厂保修，出具原厂盖章的服务承诺函 |

**三、设备技术指标**

**1、设备安装说明**

本次所购设备中所有安装材料均按最终现场工勘确认，所需材料均由中标方提供，施工工艺必须满足神华宁煤信息技术中心机房质量标准化标准。设备安装调试所必须的，但本方案中未提及的辅材，例如通过旁路部署利用交换机端口镜像方式获取网络流量的设备需额外配置千兆交换机等，投标方也应在本次招标中一并提供，如有漏项，后期实施时也应无偿提供。

**2、机房环境**

机房位于银川神华宁煤信息技术中心网络数据机房，采用上走线方式。

**3、设计方案**

根据设备须实现的功能采用不同的方式进行部署，串行部署的设备必须具备bypass功能，旁路部署的设备必须能够识别网内的真实流量，依据流量进行相关策略配置。详细方案设计见《网络安全系统建设项目技术方案》。



**4、网络安全设备详细技术要求**

**4.1 终端准入系统**

|  |  |  |  |
| --- | --- | --- | --- |
| **指标项** | | | **功能描述** |
| **基本要求** | **系统要求** |  | 具有独立自主知识产权，须为标准机架式硬件产品，除自身硬件设备外，产品功能的实现无需额外增加服务器等设备。 |
| **性能要求** |  | 标准机架结构;CPU 2颗Xeon E5-2603 v3 以上，32G DDR4内存。配置冗余电源;4个千兆光口、4个千兆电口; 每秒事务数(TPS):≥25000(次/秒),最大吞吐量:≥2Gbps,最大并发连接数:20000(条); |
| **高可用性** |  | 1. 准入设备必须具备HA模式，HA须支持主备机心跳IP检测及虚地址管理模式。 2. 要求设备在发生异常的情况下能够快速切换到Bypass模式，从而有效地保证网络链路的畅通。 |
| **终端部署** |  | 1. 准入设备应至少提供安全客户端（Agent）、无客户端等多种可供自定义部署、管理模式。**（功能截图）** 2. 安全客户端模式部署时，客户端程序应支持功能定制，以降低系统资源耗用，提升客户端兼容性。 |
| **准入**  **架构** | **终端发现** |  | 1. 能够实时监测并发现接入内网的PC、平板电脑、智能手机、IP设备等终端，能够在第一时间隔离阻断并通知管理员。**（功能截图）** 2. 对自动发现的终端能够按照类别自动归类，以方便网络终端的统计管理。**（功能截图）** 3. 要求支持对路由器、无线、AP、HUB等环境下的终端发现。 4. 系统能够准确的自动识别常见的Windows、Linux、MAC OSX、IOS和Android系统，并可以生成树形结构等易于管理的设备列表。（提供系统截图） |
| **准入技术** |  | 1. 准入设备须原生支持802.1x标准协议，无需第三方RADIUS服务器支持。 2. 要求支持基于源IP设置准入控制白名单，并且支持基于源IP设置准入控制流程。 3. 准入设备支持通过切换端口VLAN方式管理终端接入。 4. 准入设备可支持端口镜像准入技术，通过对交换机镜像数据的实时分析，能够及时发现并阻断非授权终端的接入。 |
| **定向引导** |  | 1. 支持终端入网IE重定向引导，当用户访问网页时能够自动转向到指定的页面或地址。 2. 可根据用户的实际环境自定义非80端口的Web服务端口号及用户重定向引导。 3. 能通过客户端完成身份认证、设备注册、安全检查、检查结果展现等全流程引导管理。（功能截图） 4. 具有Mac OS、Linux、iOS、Android等系统专属客户端，支持认证引导和准入管理。（功能截图） |
| **边界**  **管理** | **IP/MAC绑定** |  | 具有入网设备自动学习功能，支持IP/MAC/端口三者强制绑定，以及违规终端VLAN隔离机制，防止终端仿冒IP接入网络或移动设备位置。 |
| **主机防火墙** |  | 1. 终端在准入通过后访问域严格受管理员策略控制。 |
| **设备特征指纹** | **设备特征指纹** |  | 1. 具有非智能IP终端信息库，能够精准识别网络打印机、网络摄像头、IP电话等设备，并根据设备特征进行自动匹配和归类。 2. 通过伪造合法IP或MAC地址的非法设备和行为，能够被即时发现并阻断。 3. 具备硬件接口控制功能，控制外设接口的使用，管理员启用或禁用光驱、U盘、USB接口等硬件设备。 |
| **设备私接管理** | **NAT设备** |  | 1. 具有NAT识别和检测机制能够及时发现网内私接的小路由器、无线AP、随身WIFI等NAT设备，帮助清查通过网中网隐藏的真实网络终端。（功能截图） 2. 对通过NAT入网的计算机可以实现准入控制。 |
| **Hub管理** |  | 1. 在发现内网私接的Hub、傻瓜交换机等非网管设备，当多台计算机通过Hub接入网络时，能够及时产生告警通知管理员。 2. 支持Hub下多个终端需分别认证才能入网和只需一台认证即可全部入网两种认证机制。 |
| **网络**  **管理** | **设备识别** |  | 1. 支持自动识别网络设备类型，包括：交换机、路由器、防火墙等。 2. 支持设备管理模板的定义功能，能够通过SNMP、SSH、TELNET等方式自动、批量添加网络设备。 |
| **终端网络拓扑** |  | 1. 准入设备支持交换机到终端计算机的网络拓扑管理功能，能够自动绘制出网络拓扑图。**（功能截图）** 2. 能够在拓扑图上选取设备查看其基本状态信息、设备型号、所处位置、子节点、路由表、ARP表等信息。**（功能截图）** |
| **交换机状态展现** |  | 1. 支持可网管型交换机面板图形化展现各接口状态（up、down、trunk等），以及各接口下联的终端详细信息（IP、地址、MAC地址等）。 2. 能够支持自上而下逐级查找终端的具体位置、安全状态、认证用户、上下线时间等信息。 |
| **终端**  **入网**  **管理** | **终端识别** |  | 支持当前主流智能终端设备的安全准入控制，能够自动识别主流手机、智能终端等设备。 |
| **来宾管理** |  | 能够提供来宾角色选择，能够设定来宾设备的访问权限和入网时长，提供临时入网码，支持来宾设备与受访人员进行一对一绑定功能，并可以生成对应的审计报表。 |
| **接入审核** |  | 1.要求支持对在线终端状态提供图形化实时分析报表，分析内容包含未注册终端数、等待认证的终端数、未通过安检的终端数、等待审核的终端数等。  2.能够针对不同的角色或部门、操作系统、设备类别有选择的开启入网审核功能，待审核的用户或设备必须经过管理员审批才能入网。 |
| **资源**  **管理** | **软件检查** |  | 1. 通过安全检查检测终端软件安装、使用状态 2. 自动强制为终端安装软件 3. 软件产品授权，支持进行windows、office、WPS的产品授权信息进行检查（功能截图） |
| **IP地址管理** |  | 1. 提供IP地址分配表，能够通过图示直观的查看各网段中未分配、开机、关机的数量和分布情况。 2. 能够直接、快捷的查看全网终端历史上线、下线、在线时长等详细的IP使用情况。 |
| **运维**  **管理** | **管理角色控制** |  | 1.准入设备须采用系统管理员、安全管理员、审计员三权分立机制，防止单个角色管理者权限滥用。  2. 支持管理员密码复杂度设置，支持管理员帐户登录尝试次数限制和超时限制，其中尝试次数和时间都可以根据需要进行自定义。 |
| **移动存储管理** |  | 1. 支持移动存储设备管理：对移动存储设备进行注册、挂失、分配管理，指定其使用范围及时间，规范内网移动存储设备使用安全；（功能截图） 2. 支持加密移动存储设备：对移动存储设备进行文件系统级别加密，可选密码不可恢复，使用专用工具进行读写，可限定其使用范围，查看其审计记录。（功能截图） |
| **网络诊断工具** |  | 支持通过Web管理界面提供ping、抓包、traceroute、nslookup等功能，并可以设置命令参数进行相关调试。 |
| **消息群发** |  | 能够支持在指定的一台或者多台终端计算机上产生桌面消息通知，该消息会立即弹出在用户桌面上，对用户进行提醒。 |
| **软件分发** |  | 1. 准入设备应具有软件分发和部署功能，管理员可以预定义软件分发的路径、运行参数、是否执行等任务策略，以提升软件部署效率。 2. 能够自动判断并统计软件分发、部署的成功率，支持进程、注册表、安装路径等多种参数的组合判断。 |
| **安全管理报表** |  | 1. 准入设备后台能够按周、月、年统计安全状况走势图。 2. 准入设备后台提供每日入网报告、每周入网报告、每月入网报告。 |
| **报警**  **报表**  **管理** | **报警信息** |  | 1. 可以提供紧急、重要、次要、提示等多个级别自定义报警模式。 2. 支持系统报警、网络报警、终端报警等类别，超过10种以上自定义报警类型。 3. 支持Syslog报警信息的定向输出。 |
| **案例要求** | |  | 提供至少3个10000点以上大规模部署案例的项目证明。 |
| **资质要求** | |  | 1. 公安部《计算机信息系统安全专用产品销售许可证》 2. 国家保密局《涉密信息系统产品检测证书（网络访问控制产品）》 3. 国家版权局《计算机软件著作权登记证书》 |

**四、技术服务**

1、投标方投标时必须有原厂针对本项目授权书原件，售后服务承诺函，无原厂授权书取消投标资格，原厂商直接投标不需要。货到现场必须由原厂工程师验货确认后，方可上架安装。

2、投标方在所做标书内必须提交针对本次设备购置的详细技术方案，必须承诺中标后，在施工前了解神华宁煤集团的网络状况并提交详细的施工组织方案，待方案通过后，严格按照施工组织方案进行施工，不得无故延误工期。

3、投标方必须承诺现场施工期间及售后服务时由有相关证书的工程师安装调试设备，不得派遣无资格证书的人员。

4、投标方必须具有独立的法人资质。投标方产品必须具有公安部《计算机信息系统安全专用产品销售许可证》，国家保密局《涉密信息系统产品检测证书（网络访问控制产品）》，国家版权局《计算机软件著作权登记证书》，注册资金在1000万以上，具有三个以上的同类同规模工程业绩。

5、投标方所提供的设备是必须是国产设备，如果设备外包装损坏或设备外壳损坏投标方必须无条件更换设备。

6、投标方对所投产品的扩展能力做详细说明。

7、实施期间，中标方负责系统的综合调试，须对一切与合同有关的供货设备及技术接口、技术服务等问题负全部责任。凡与合同设备相连接的其它设备装置及软件，中标方有提供接口和技术配合的义务，所发生的费用已包含在投标报价中，招标方不承担中标价格以外的任何费用。

8、投标方应承诺：合同签订后，如招标方需追加购置合同清单内的设备及其附件，所提供的设备及其附件的价格不高于合同价格。

9、培训

投标方应对招标方指定人员提供系统使用、维护等方面的免费培训,培训所需的培训、交通、食宿等各项费用均由中标方承担，培训的时间招标方和中标方共同商议。详细要求如下：

9.1、在不影响施工进度的情况下，中标方应该在安装调试过程中为招标方的技术人员进行现场培训，使招标方的技术人员掌握设备使用技术。培训时间为2-3天，培训费、场地由中标方解决。

9.2、提供中标设备的4人7天原厂培训，往返交通、食宿费、培训费等全部费用由中标方承担。

10、售后服务

1）投标方对所提供的设备应提供原厂保修服务，保修期为3年，保修期从安装上架开机运行时计算。在保修期内，投标方应无偿并迅速更换非人为因素损坏的整机设备和相关配件，并解决因软件及操作等产生的相关问题。

2）投标方应提供保修期以后的维保办法及维保报价。

3）在接到设备故障通知后，投标方应在1小时内做出响应，及时进行提导并提供解决方案，如需要上门维护必须在24小时以内到达现场。