#### **漏洞扫描、堡垒机、可信网关(VPN)、安全管理云服务器技术需求**

## 一.采购产品一览表

|  |  |  |
| --- | --- | --- |
| 序号 | 名称 | 数量（台） |
| 1 | 漏洞扫描 | 1 |
| 2 | 堡垒机 | 1 |
| 3 | 可信网关(VPN) | 1 |
| 4 | 安全管理云服务器 | 1 |

## 二.技术指标

## 1）漏洞扫描

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 重要性 | 指标项 | 指标要求 |
|  | ★ | 硬件规格 | 1U机架式设备，含交流单电源模块，1个RJ45串口，1个GE管理口，≥4个电口扫描口，4个光口 |
|  | ★ | 性能规格 | 授权扫描点数≥1000点，系统支持最大扫描速度≥1000 ip/h，最大并发任务数≥10，最大并发扫描数≥60，最大存储任务数≥8000 |
|  | # | 漏洞检测 | 支持检测的漏洞数大于240000条，兼容CVE、CNCVE、CNNVD、CNVD、Bugtraq等主流标准，需提供web功能界面截图 |
|  | # | 产品应支持通过多种维度对漏洞进行检索，包括：CVE ID、BUGTRAQ ID、CNCVE ID、CNVD ID、CNNVD ID、MS 编号、风险等级、漏洞名称、是否使用危险插件、漏洞发布日期等信息。需提供web功能界面截图 |
|  | # | 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。需提供web功能界面截图 |
|  | # | 扫描管理 | 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，需提供web功能界面截图。 |
|  | # | 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，需提供web功能界面截图 |
|  | # | 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，需提供web功能界面截图 |
|  | # | 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，需提供web功能界面截图 |
|  | # |  | 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，需提供web功能界面截图 |
|  | # |  | 提供多种报表类型，包括综述报表和主机报表，需提供web功能界面截图 |
|  |  | 产品资质 | 公安部颁发的《计算机信息系统安全专用产品销售许可证(增强级)》 |
|  |  | 中国信息安全测评中心颁发的《国家信息安全测评信息技术产品安全测评证书(EAL3+级)》 |

## 2）堡垒机

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 重要性 | 指标项 | 指标要求 |
| 1 | ★ | 基本规格 | 标准2U机架式；CPU e3 1225，内存16GB，6个千兆电口；4个千兆光口板卡，支持1个接口扩展槽位；内置4TB硬盘；冗余电源。  |
| 2 | # | 节点授权数量 | 最大支持500路图形会话或1000路字符会话并发。 |
| 3 | # | 系统包含≥300个授权，  |
| 4 |  | 部署模式 | 需支持物理旁路、HA双机热备；需支持基于水平可扩展的集群化架构设计与部署。 |
| 5 |  | 产品资质 | 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，品类：运维安全产品（增强级） |

## 3）可信网关（VPN）

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 重要性 | 指标项 | 指标要求 |
| 1 | ★ | 基本规格 | 软硬一体化设备，标准2U机箱，2个千兆电口，4个千兆光口，2个扩展槽，6个USB接口，冗余电源，支持RAID0,1,10，集成BMC模块，支持IPMI2.0，对外提供1个1000 Mbps RJ45管理网口 |
| 2 | ★ | 性能要求 | 最大支持并发用户数（个）：1800，含300在线SSLVPN用户授权,300用户管理认证授权。 |
| 3 | # | 功能要求 | 含链路加密、访问控制、门户式单点登录、轻量级EMM、日志追溯等功能。 |
| 4 |  | 提供集中配置、管理、会话、授权等能力；可和外部身份与访问管理平台实现认证、权限策略管理等能力；基于身份、环境、终端、应用、行为评估实现动态访问控制。 |
| 5 |  | 可与云桌面管理系统形成联动，提供多种终端接入，实现安全的远程办公。 |
| 6 |  | 产品资质 | 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。 |

## 4）安全管理云服务器

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 重要性 | 指标项 | 指标要求 |
| 1 | ★　 | 基本规格 | 软硬一体化设备，标准2U机箱，冗余电源，1个MGT口，1个HA口，2口千兆电口，2个千兆光口，3个扩展插槽 |
| 2 | ★　 | 性能要求 | 最大理论加密流量（Mbps）：480，最大理论并发用户数（个）：1600，HTTPS并发连接数（个/秒）：48000；300用户管理认证授权。 |
| 3 |  | 功能要求 | 能对云桌面设备进行全面风险监控，包括终端身份环境标识、系统环境感知、应用环境感知等，识别云桌面设备上发起访问的应用程序身份，支持自动采集终端上发起访问的应用程序信息，可根据应用签名等信息评估风险，设置可信应用或不可信应用。可与终端杀毒软件进行深度融合，进一步增强终端安全和管控能力，能够在登录阶段、访问阶段获取到终端安全评分（木马病毒、漏洞检测等），避免不安全终端接入该系统对业务应用访问，缓解恶意终端访问和数据泄露等安全风险。 |
| 4 |  | 实现应用的可信接入，提供业务应用访问安全通道服务、应用数据加解密服务、应用隐藏服务；根据身份、环境、终端、应用、行为等属性及可信环境感知状态，动态控制用户的应用访问，保证业务应用访问的安全策略控制及强制实施。。 |
| 5 |  | 产品资质 | 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，品类：访问控制。 |

## 三.服务要求

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 内容 | 重要性 | 服务要求标准 | 证明材料要求 |
|  | 原厂售后服务承诺函 | ★ | 本次投标产品提供原厂三年免费整机保修服务的原厂商售后服务承诺函。 | 是 |
|  | 投标人服务标准 | ★ | 投标人承诺电话报修后2小时内上门服务、12小时内排除故障。所有软件、硬件提供验收合格后起三年免费原厂维保。 | 是 |
|  | 集成标准及工勘要求 |  | 负责完成本项目所采购设备的到货、调试、验收、上架、安装、网络接入、操作系统安装配置等。 | 是 |