# 采购清单

|  |  |  |  |
| --- | --- | --- | --- |
| 类型 | 参数 | 数量 | 单位 |
| VPN集中管理平台 | 1U机箱，6个千兆电口，提供：VPN动态隧道管理、VRC用户管理、设备信息管理、设备配置管理、日志管理、报表管理。可管理100台VPN设备； | 1 | 台 |
| SSL用户端许可 | 100 | 个 |
| 网页防火墙 | 标准2U硬件平台，标配网口：2千兆电口管理口，千兆业务电口\*4（含2组硬件BYPASS模块），千兆业务光口\*4（标配多模SFP模块\*2，不含硬件BYPASS模块） 硬盘容量：1T，内存：16G，USB口：USB2.0口\*2，串口：RJ45口\*1，电源：1+1热插拔冗余电源，应用吞吐量6Gbps，HTTP最大并发数35万，HTTP最大新建数3.2万，保护站点无限制 | 1 | 台 |
| 服务器HBA卡 | FC HBA卡-8Gb(QLE2560)-单端口-SFP+(含1个多模光模块)-PCIe 2.0 x4 | 16 | 块 |
| 光纤模块 | 1000BASE-LX SFP (1310nm, 10km, LC） | 4 | 个 |
| 光纤跳线 | OFC-GJFJBV-YE-LU-LU-20-10-HYW1 | 6 | 根 |
| 光纤跳线 | OFC-GJFJBV-YE-LU-LU-20-5-HYW1 | 24 | 根 |

# 参数及实施要求

## 设备参数要求

**1）VPN集中管理器**

|  |  |  |
| --- | --- | --- |
| **项目** | **技术规格要求** | **评审点** |
| 厂商资质 | **产品生产厂商需取得CMMI5资质** | **★** |
| **中国信息安全测评中心-安全工程类（三级）最高级** | **★** |
| 中国网络安全审查技术与认证中心颁发—信息系统安全集成服务（一级）最高级 |  |
| 产品生产厂商具备网络安全应急服务支撑单位证书（国家级） |  |
| 硬件要求 | 采用专用硬件架构与专用安全操作系统，基于操作系统内核的完全检测技术；专用的安全操作系统具有自主知识产权；可管理VPN数量≥100。 |  |
| **软件要求** | **采用双安全操作系统，防止配置不当系统故障造成的网络中断，充分保证了系统的稳定性。（提供截图证明并加盖原厂公章）** | **★** |
| **端口许可** | **1U机架式 ，至少配置6个10/100/1000BASE-T接口。开通所有端口及链路许可。** | **★** |
| **监控** | **支持监控现有武汉市疾控系统内天融信VPN设备的运行状态、设备资源状态、并发用户数、客户端类型分布、IPSEC隧道状态、用户流量、安全事件、区县的接入用户数监控，并通过图表展示；（提供截图证明）** | **★** |
| 报表管理 | 支持详细审计用户登录认证过程、各种认证授权错误、内网资源访问情况等信息； |  |
| 支持多级审计日志，可以灵活配置审计级别；支持将日志上传到外部日志服务器。 |  |
| 支持用户接入实时数量报表，同一天不同时间段的用户接入实时数量对比； |  |
| 宽带流量报表及网络宽带流量占比报表；用户操作数据统计： |  |
| 登陆和退出时间，操作占比等； |  |
| 同一时间段用户断线重拨数的数据统计，断线次数及占比； |  |
| 不同链路的链路地址信息等； |  |
| 同一时间段用户的网络接入占比等 |  |
| **高可用** | **支持双机热备（Active-Standby）、负载均衡（Active-Active）、连接保护（Session Protect）模式，支持系统故障自动切换和抢占功能；** | **★** |
| SSL VPN许可 | 100个SSL用户端许可 |  |
| 服务要求 | 三年硬件保修及版本升级服务，三年原厂服务。 |  |

**2）网页防火墙**

|  |  |  |
| --- | --- | --- |
| **项目** | **技术规格要求** | **评审点** |
| 资质要求 | [产品需获得公安部产品销售许可证](#_销售许可证) |  |
| [产品需获得国家涉密产品资质证书](#_21、涉密资质) |  |
| 产品需获得国家信息安全测评中心颁发的信息技术产品安全测评证书 |  |
| 产品需获得《网络关键设备和网络安全专用产品安全认证证书》 |  |
| **产品需获得IPv6金牌认证证书** | **★** |
| 产品必须为市场占有率前三品牌，需提供国外权威第三方分析机构WAF产品市场分析报告 |  |
| 原厂商具有软件能力成熟度模型集成CMMI5认证 |  |
| 硬件规格 | 产品必须为专业性WEB应用防火墙设备及专业性WEB应用防火墙资质，而非NGAF、NGFW、UTM设备及资质 |  |
| 标配2千兆电口管理口，千兆业务电口\*4（含2组硬件BYPASS模块），千兆业务光口\*4 |  |
| 网络层吞吐率≥6G；  最大并发HTTP连接数≥35万；  每秒新建HTTP连接数≥3.2万 |  |
| 部署模式 | 支持透明串接、反向代理、旁路引流部署、旁路镜像审计部署 |  |
| 高可用 | 支持集群模式、主-主模式、主备模式、硬件BYPASS、软件BYPASS |  |
| 保护对象 | 支持多条链路数据的防护，防护网段数量不限 |  |
| **支持保护站点快速向导配置部署，提供界面截图** | **★** |
| Web服务自发现 | 支持自动发现现网环境中存在的Web业务系统，记录服务器的IP、Port、域名等信息 |  |
| HTTPS防护 | 置SSL硬件加速卡，实现对HTTPS的加解密，提供设备对HTTPS的处理性能，提供界面截图和设备外观截图 |  |
| 攻击检测 | 能够识别恶意请求含：跨站脚本(XSS)、注入式攻击（包括SQL注入、命令注入 、Cookie 注入、代码注入、LDAP注入、SSI注入文件注入等）、跨站请求伪造等应用攻击行为 |  |
| Webshell检测 | 内置主流Webshell特征库，对文件上传内容进行检查，防止恶意Webshell上传，对已经上传的webshell发起请求的行为进行拦截阻断 |  |
| **敏感信息隐藏拦截** | **内置身份证、银行卡、手机号等服务器敏感信息库，对服务器响应敏感内容进行隐藏，并支持自定义敏感词，提供界面截图** | **★** |
| 智能攻击者锁定 | 支持智能识别攻击者，对网站连接发起攻击的IP地址进行自动锁定禁止访问被攻击的网站；可配置攻击者识别策略和算法以及攻击者锁定时间，提供界面截图并加盖公司公章 |  |
| **WEB访问流程合规防护** | **可实现访问流程的校验，向网站提交表单前必须先访问指定页面，并等待可配置的时间长度后才能正常提交表单，需提供第三方测评机构（必须是公安部三所、国家保密局、ISCCC其中一家）的检测报告** | **★** |
| **CC防护功能** | **可根据URL、请求头字段、目标IP、请求方法等多种组合条件对CC攻击进行检测，检测指标为URL访问速率和URL访问集中度；可根据IP、IP+URL和IP+User\_Agent等算法对客户端进行检测，并支持应用层字段解析和自定义检测字段功能，支持挑战模式，支持基于地址位置的识别，支持对特定的IP地址进行CC规则白名单放行，支持CC慢攻击防护，通过学习业务流量模型，在业务流量异常时开启CC防护，并支持启动配置阈值，需提供第三方测评机构（必须是公安部三所、国家保密局、ISCCC其中一家）的检测报告** | **★** |
| **地图态势分析** | **按地理区域对攻击次数等进行统计，通过地图展示，并在地图上可以指定某一地理区域进行访问控制，阻断此区域 IP的访问，需提供第三方测评机构（必须是公安部三所、国家保密局、ISCCC其中一家）的检测报告** | **★** |
| **云端联动** | **支持云端威胁情报联动，可主动发现包括僵尸IP、代理IP、扫描IP、黑产IP、C&C等恶意IP发起的访问行为，针对访问行为进行日志记录通知客户，实时统计威胁情报的攻击攻击类型占比和攻击的频率，提供界面截图。** | **★** |
| WAF与云端高防中心联动，通过WAF一键开启防护，实现3-7的DDOS安全防护，最高可提供1T抗D服务，提供界面截图。 |  |
| 日志分析 | 根据产生的安全日志进行智能分析，提高人工分析效率，减小规则误判概率，提供界面截图。 |  |
| 访问审计 | 具备审计网站正常访问流量的能力，提供按小时，天、月份生成用户的访问数据；能记录、查询所有用户对网站的访问情况，包括访问的URL、客户端IP、服务器返回的状态码。上述功能须提供界面截图。 |  |
| 服务要求 | 三年硬件保修及版本升级服务，三年原厂服务。 |  |

**3）服务器HBA卡**

|  |  |  |
| --- | --- | --- |
| **项目** | **技术规格要求** | **评审点** |
| 硬件规格 | 单口光纤通道卡 |  |
| 8Gb光纤通道 |  |
| 总线接口PCle2.0\*4 |  |
| 带SFP+,多模光模块，FC |  |
| 适用于华为2、5系列服务器 |  |

★为重要指标项，1项不满足或无法提供证明扣2分，非★项每项不满足或无法提供证明的扣1分，扣完为止。

## 实施要求

1）依据采购人现状情况和本次购买设备，合理有效的进行全局总体规划，并最终实施交付，按照总体规划方案进行逐一部署和迁移割接。

2）投标人对所投货物技术响应提供承诺，如所供货物技术参数与投标文件中技术参数不符，中标人自行承担法律责任。

3）投标人必须针对技术要求及设备参数进行逐条响应说明。所有要求提供的截图及证明文件，都必须提供真实的证明材料并加盖投标人公章。

4）测试及验收方案：测试及验收方案完整全面、科学合理，测试方案能结合项目建设情况，对系统的重难点有分部、分项目的测试验收计划，项目验收流程清楚。

5）售后服务和培训方案：投标人在省内有完善的服务网点，针对系统和架构优化调整后提供详细的巡检方案（包含计划、人员）及应急响应措施。提供7×24小时售后技术支持，有完善的故障解决方案和巡检方案。

# 评分规则

|  |  |  |  |
| --- | --- | --- | --- |
| 评标项目 | 评标分项 | 分值 | 子项目及分值 |
| 报价得分  （50） | / | 50分 | 价格分统一采用低价优先法计算，即满足招标文件要求且投标价格最低的有效投标报价为评标基准价，其价格分为满分。其它投标人的价格分统一按照下列公式计算：投标报价得分=（评标基准价/投标报价）\*价格权值  (根据国家及武汉市关于促进中小型企业发展暂行办法，对小型和微型企业产品的价格给予6%的扣除，用扣除后的价格参与评审；后附中小企业声明函) |
| 商务得分（10） | 对招标文件的响应程度 | 3分 | 投标文件编制完整，逐页有连续页码、有详细目录、目录与有关材料装订顺序对应清晰、查阅方便，按招标要求进行比较，优得3分，一般得  1分，差得0分。 |
| 团队实力 | 2分 | 投标人配备的实施团队成员具有信息安全资质和项目服务经理资质认证的，每1名得0.5分，最多2分。 |
| 资质认证 | 5分 | 投标人同时拥有ISO20000信息技术服务管理体系、ISO27000信息安全管理体系标准认证的得5分，拥有其中一项得2分，没有不得分。 |
| 技术得分（40） | 投标产品及技术满足度 | 30分 | 根据投标人所投产品技术指标响应情况进行评分。★为重要指标项，1项不满足或无法提供证明扣2分，非★项每项不满足或无法提供证明的扣1分，扣完为止。 |
| 供货及验收  方案 | 5分 | 根据投标人供货方案及验收方案进行评分：  供货方案合理、完整确保能按期供货、安装；验收方案的调试科学、合理、完整；上述供货及验收方案可行性高，有保障措施的得5分，有缺陷或不合理的得2分，差或无供货及验收方案的得0分。 |
| 售后服务及质量保证 | 5分 | 投标人承诺提供7×24小时电话售后服务，接采购人通知2小时内派技术人员到达现场，24小时内解决问题的，得3分。  投标人所投网络安全设备，提供3年及以上原厂质保的，每项产品得1分，最多2分，3年以下不得分。 |