**2024-023参数附件**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 设备名称 | 基础参数 | 数量 | 单位 |
| 1 | 零信任控制平台 | 1. ★性能参数：接入授权不少于3000点，设备最大支持并发用户数应不少于4000点，方便后续扩容。
2. ★硬件参数：规格：1U，内存大小≥16G，硬盘容量≥128G SSD，电源：冗余电源，接口≥6千兆电口+4千兆光口SFP。
3. 为适应复杂多样的内部业务系统，web模式下发布应用资源时，应支持透明代理、智能改写等模式，以合理适配较规范化的业务系统及复杂老旧的非常规站点。
4. 在业务应用兼容性良好的情况下，支持以隧道模式发布http/https协议的资源，以增加在隧道模式下发布的资源的URL级别审计能力，同时支持为隧道资源添加WEB水印以及单点登录功能。
5. 为了不改变员工原有使用习惯，保障员工的使用体验，需支持以下主流浏览器访问WEB资源。
6. 支持用户自主配置是否开启开机自启动零信任客户端。
7. 支持新增/删除/修改管理组，内置审计管理员、安全管理员、系统管理员等管理组；通过管理组管理权限的配置，实现管理员分级分权。
8. 支持管理员在控制台查看“用户状态”，支持筛选异常状态的用户，如爆破锁定、ACL锁定、异地登录等，支持管理员手动解锁用户。
9. 解决软件产品的漏洞问题，在软件开发的每个关键点嵌入安全要素，通过安全需求分析、安全设计、安全编码、安全测试等专业手段，解决各阶段可能出现的安全问题，有效减少软件产品潜在的漏洞数量，提高软件产品安全质量，要求所投产品制造厂商具备中国网络安全审查技术与认证中心的软件安全开发服务的一级服务资质。（需提供证明材料并加盖厂商公章）
10. 为证明所投产品的自身安全性，应具备国家计算机网络应急技术处理协调中心出具的安全众测无漏洞证明文件。（需提供证明材料并加盖厂商公章）
11. 具备CDN接入能力，客户端可以经过设置第三方的CDN下载，同时支持获取CDN加速前的访问IP。（需提供第三方权威检测机构出具的带CNAS标识的检测报告证明并加盖厂商公章）
12. 为防止自动化工具进行密码猜测所投零信任VPN控制平台，支持图形校验码功能，图形校验码可选择中文或英文。（需提供产品功能截图证明并加盖厂商公章）
13. ★提供三年产品质保，三年软件升级。
 | 1 | 台 |
| 2 | 零信任接入网关 | 1. ★性能参数：最大理论加密流量≥600Mbps，最大理论https并发连接数（个）≥60000，理论https新建连接数（个/秒）≥400。
2. ★硬件参数：规格：1U，内存大小≥16G，硬盘容量≥128G SSD，电源：冗余电源，接口≥6千兆电口+4千兆光口SFP。
3. 支持配置同IP用户连续登录错误超过上限时锁定IP，并于指定时长后自动恢复。
4. 支持查看当前设备运行状态，包括但不限于设备硬件状态（CPU、内存、磁盘占比等）、实时网络吞吐、历史网络吞吐峰值等信息，便于管理员掌握设备整体运行情况。
5. 支持告警信息设置，告警事件应包含但不限于： CPU使用率超过80%、内存使用率超过80%、磁盘占用率超过80%、本机网卡异常、序列号即将到期、控制中心连通异常、集群故障等。
6. 支持配置邮箱服务器，告警事件支持邮件通知管理员。
7. 支持IPV4/IPV6双栈网络IP配置，可自主选择配置LAN口或WAN口。为了保护设备的安全，可支持默认限制所有IP通过WAN口访问系统，支持通过配置IP白名单的方式来放通WAN口接入的特殊需求。
8. 支持在控制台上提供命令面板，内嵌常规的网络配置和排障命令，方便运维人员对设备进行维护，网络测试以及故障排查。
9. 解决软件产品的漏洞问题，在软件开发的每个关键点嵌入安全要素，通过安全需求分析、安全设计、安全编码、安全测试等专业手段，解决各阶段可能出现的安全问题，有效减少软件产品潜在的漏洞数量，提高软件产品安全质量，要求所投产品制造厂商具备中国网络安全审查技术与认证中心的软件安全开发服务的一级服务资质。（需提供证明材料并加盖厂商公章）
10. 为证明产品的软件成熟性与先进性，应提供由中国软件协会颁发的年度优秀软件产品证书。（需提供证明材料并加盖厂商公章）
11. 支持TLS协议检查，确保所有传输的数据都经过加密。（需提供产品功能截图证明并加盖厂商公章）
12. ★提供三年产品质保，三年软件升级。
 | 1 | 台 |