采购需求表

1. 委托采购需求说明（需实现的功能或目的；需满足的服务标准、期限效率等要求）：

## 项目背景

上海音乐学院分为零陵路和汾阳路两个校区，两校之间通过专线互联实现互通，默认流量将从零陵路出口统一转发。零陵校区总出口部分节点设备为单设备运行，没有冗余和备份。为进一步提高校园网的安全性和可靠性，避免因某节点的设备宕机造成业务中断，希望通过本次建设对校园网出口方面进行升级加固，建设完成后能提升校园网运行的稳定性、安全性和可靠性，使得校园网络的基础环境和安全性达到最优。

## 项目建设内容

本项目拟采购网络产品如下：

|  |  |  |
| --- | --- | --- |
| 序号 | 产品名称 | 数量/单位 |
| 1 | 万兆防火墙 | 1台 |

提供的网络产品需要与现网防火墙进行兼容，能够与现网防火墙形成主备冗余模式，解决当前网络的冗余性差、监测预警能力薄弱等问题，进一步提高学校内部和外部网络的稳定性、安全性和可靠性。

## 产品参数要求

1. **万兆防火墙**

|  |  |
| --- | --- |
| **功能项** | **功能要求说明** |
| 硬件规格要求 | 支持冗余电源2U机箱，内存≥16G，硬盘≥64GB MSATA+480GB SSD。接口：千兆电口≥6、万兆光口SFP+≥4 |
| 性能要求 | ★网络层吞吐量≥ 40G。应用层吞吐量≥12G。并发连接数≥400万。新建连接数≥22万。 |
| 工作模式 | 产品支持路由模式、透明模式、虚拟网线模式、旁路镜像模式等多种部署方式。 |
| 链路状态检测 | 产品支持链路健康检查功能，支持基于多种协议对链路可用性进行探测，探测协议至少包括DNS解析、ARP探测和PING方式。 |
| 路由特征 | 产品支持策略路由负载，支持基于服务、ISP地址、应用、地域等维度进行智能选路，保证关键业务流量通过优质链路转发，支持加权流量、带宽比例、线路优先等负载均衡调度算法。 |
| DNS代理 | 产品支持DNS透明代理功能，避免单运营商DNS解析出现单一链路流量过载，平衡多条运营商线路的带宽利用率。 |
| NAT功能 | 产品支持支持源地址转换SNAT，目的地址转换DNAT和双向NAT等功能， 支持一对一、一对多、多对一等形式的。 |
| VPN功能 | 产品支持IPsec VPN和SSL VPN功能。 |
| 为满足组网兼容性，IPSec VPN需支持IKEv1和IKEv2协议，支持基于主模式和野蛮模式建立加密隧道。 |
| 产品支持IPSec VPN智能选路功能，根据线路质量实现自动链路切换。 |
| 产品支持多种SSL VPN用户认证方式，至少包括本地密码认证、LADP认证和硬件特征码认证。 |
| 访问控制 | 产品支持多维度安全策略设置，可基于时间、用户、应用、IP、域名等内容进行安全策略设置。 |
| 应用控制 | 产品支持对不少于9880种应用的识别和控制，应用类型包括游戏、购物、图书百科、工作招聘、P2P下载、聊天工具、旅游出行、股票软件等类型应用进行检测与控制。 |
| 流量控制 | 产品支持基于地区维度设置流控策略，实现多区域流量批量快速管控功能。 |
| 访问控制策略 | 产品支持多维度安全策略设置，可基于时间、用户、应用、IP、域名等内容进行安全策略设置。 |
| DDoS防护 | 产品支持对ICMP、UDP、DNS、SYN等协议进行DDOS防护。 |
| 产品支持异常包攻击防御，异常包攻击类型至少包括Ping of Death、Teardrop、Smurf、Land、WinNuke等攻击类型。 |
| 文件过滤 | 产品支持对文件传输行为进行安全过滤，支持基于上传、下载、双向的文件内容过滤，内容过滤类型至少支持网页、脚本、压缩文件、图片、可执行文件、适配、文本等常见文件类型。 |
| 加密流量安全防护 | 产品支持对HTTPS协议加密流量进行解密，支持配置基于区域、对象、业务类型、服务器IP/端口的解密策略。 |
| 入侵防御 | ▲产品预定义漏洞特征数量超过7600种，支持在产品漏洞特征库中以漏洞名称、漏洞ID、漏洞CVE标识、危险等级和漏洞描述等条件快速查询特定漏洞特征信息，支持用户自定义IPS规则。（需提供产品功能截图证明） |
| 产品支持基于IMAP、FTP、RDP、VNC、SSH、TELNET、ORACLE、MYSQL、MSSQL等应用协议进行深度检测与防护。 |
| 产品支持僵尸主机检测功能，产品预定义特征库超过110万种，可识别主机的异常外联行为。 |
| Web安全防护 | 产品支持对常见Web应用攻击防御，攻击类型至少支持跨站脚本（XSS）攻击、SQL注入、文件包含攻击、信息泄露攻击、WEBSHELL、网站扫描、网页木马等类型，产品预定义Web应用漏洞特征库超过3320种。 |
| 产品支持未知威胁检测能力，需提供公安部计算机信息系统安全产品质量监督检验中心、中国信息安全测评中心、中华人民共和国国家版权局、公安部信息安全产品检测中心之中任意一家检测机构出具关于“未知威胁检测”的证书或检测报告。 |
| 产品支持对请求报文头的X-Forward-For字段检测，并对非法源IP进行日志记录和联动封锁。 |
| 账号安全 | 产品支持用户账号全生命周期保护功能，包括用户账号多余入口检测、用户账号弱口令检测、用户账号暴力破解检测、失陷账号检测，防止因账号被暴力破解导致的非法提权情况发生。 |
| 策略有效性分析 | 产品支持安全策略有效性分析功能，分析内容至少包括策略冗余分析、策略匹配分析、风险端口风险等内容，提供安全策略优化建议。 |
| 策略生命周期管理 | ▲产品支持策略生命周期管理功能，支持对安全策略修改的时间、原因、变更类型进行统一管理，便于策略的运维与管理。（需提供产品功能截图证明） |
| 双机部署 | 产品支持主主、主备两种双机模式部署。 |
| 管理方式 | 产品支持Web管理、串口管理、SSH管理等多种不同方式。 |
| 双因素认证 | ▲产品支持管理员双因素认证功能，用户通过用户名/密码和Key等不同方式登陆产品管理界面。 |
| 产品资质 | ▲要求所投产品具备中国国家信息安全产品认证证书，提供证明材料。 |

## 技术方案要求

在项目总体设计上要求采用行业内先进的技术，做到功能完善、系统先进、安全稳定、拓展性强，兼容和开放性强。为此，要求如下：

1. 为保证项目的实施能满足学校目前及未来的需求，本项目为非纯设备采购项目，投标人须充分理解学校网络现状，结合学校现状及本次项目建设内容，提供合理、完整、详细的技术设计方案，包括但不限于详细设计方案、设备规划方案、实施方案等。
2. 为提高学校原有设备的利用率，保护学校原有设备的投资，投标人提供的设备必须能和学校现有的硬件设备兼容，须提供详细的兼容方案。
3. 招标文件中相关技术参数和服务要求为基本要求，并非充分条件，各投标人应根据自身所提供产品补充完善相关细节，但所投产品的性能及参数指标不得低于招标要求。

## 售后服务

1. 售后服务期：售后服务质保期三年，质保日期从验收报告日起计算；在服务质保期内，若在此期间有任何质量问题发生，中标方应免费提供维修和更换服务。中标方负责全部的设备维护、维修和其他故障处理，保证数据中心的正常运行，在接到用户服务要求时，必须在30分钟内电话响应，3小时内现场响应服务。
2. 主要设备需提供不少于3年的原厂质保服务，需提供原厂盖章的售后服务承诺函。
3. 投标人应响应本次项目售后服务要求并在投标文件中提供详细具体的售后服务方案（包括但不限于售后服务承诺、服务流程、服务内容、应急措施和方案等），也可视自身能力在投标文件中提供更优、更合理的售后服务承诺。

## 培训要求

项目实施完成后，由投标人安排组织，为招标人提供现场技术培训，投标书中需提供完整的培训方案和培训计划。

培训内容包括（但不限于）：系统的拓扑结构、软硬件的的安装、配置方法，常见故障的处理等。

二、采购需求清单（可根据需求修改清单格式）

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 名称 | 规格型号 | 数量 | 备注 |
| 　1 | 　万兆防火墙 | 　 | 1　 | 　 |