上海港湾学校网络专用防火墙项目

技术要求

## 项目概述

上海港湾学校计划采购一台网络防火墙设备，部署在网络出口区域，与学校现有的华为网络防火墙设备双机部署，同时实现搭建数据中心DMZ区域，实现数据中心的安全隔离。

## 技术要求

|  |  |
| --- | --- |
| 指标项 | 指标要求 |
| 智能威胁防御 | 具有未知威胁的检测能力，支持与云沙箱联动（三年升级服务），实现对APT攻击的防御功能； |
| 硬件架构 | 采用多核架构，自研芯片；（提供官网截图) |
| IPV6 | 支持IPv6协议栈、IPV6穿越技术、IPV6路由协议； |
| 支持IPv6 over IPv4 GRE隧道，6RD隧道； |
| 协议识别 | 支持识别国标SIP协议及主流安防厂家的私有协议； |
| 数据安全 | 支持数据防泄露，对传输的文件和内容进行识别过滤，对内容与身份证、信用卡、银行卡、社会安全卡号等类型进行匹配； |
| 支持DNS过滤，提高WEB网页过滤的性能； |
| 支持SafeSearch，过滤掉Google等搜索引擎返回的不健康的内容； |
| DDoS防护 | 支持HTTP、HTTPS、DNS、SIP等应用层Flood攻击，支持流量自学习功能，可设置自学习时间，并自动生成DDoS防范策略；（提供功能截图） |
| NAT | 支持全面NAT功能，对多种应用层协议支持ALG功能，包括ILS、DNS、PPTP、SIP、FTP、ICQ、RTSP、QQ、MSN、MMS等； |
| 支持源NAT自动探测并排除NAT-IP地址池中无效地址（防封杀）； |
| 支持源NAT地址池使用率超限告警； |
| 支持三元组NAT smart-fullcone； |
| 入侵防御及病毒防护 | 基于特征检测，支持超过8000种特征的攻击检测和防御；（提供功能截图） |
| 支持基于场景进行策略入侵防御的模板定制； |
| 支持对常见应用服务（HTTP、FTP、SSH、SMTP、IMAP）和数据库软件（MySQL、Oracle、MSSQL）的口令暴力破解防护功能； |
| 支持恶意域名过滤，实现对C&C进行阻断； |
| 可以支持HTTP、FTP、SMTP、POP3、IMAP、NFS等协议的病毒防护； |
| 反病毒&入侵防御License试用，在试用期内反病毒和入侵防御功能可用，升级服务可用。 |
| 可靠性 | 支持BFD链路检测，支持BFD与VRRP联动实现双机快速切换，支持BFD与OSPF联动实现双机快速切换；（提供功能截图） |
| 支持HA平滑升级，升级窗口中支持不同版本的软件形成双机热备； |
| 多出口智能选路 | 可根据目的地址智能优选运营商链路，支持主备接口配置以及按比例分配的负载分担方式； |
| 配置要求 | ★实配：千兆电口≥16，千兆光口≥6，万兆光口≥6，硬盘≥240G SSD，配置双电源**（必须提供产品官方链接和截图，未提供废标处理）**； |
| 兼容性 | ★与学校现有的网络防火墙实现双机部署，提供主备方案**（必须提供，未提供废标处理）**。 |

## 公司资质要求

* 在中国境内注册的合格法人机构，并具有相应的经营范围
* 符合《中华人民共和国政府采购法》第二十二条规定的供应商；
* 在上海市有固定的服务点。
* ★需提供制造厂商针对本项目的授权函**（必须提供，未提供废标处理）**；

## 投标文件组成

* 报价单（附件二）
* 营业执照、税务登记证、组织机构代码证或“三证合一”的营业执照
* 招标要求的其他材料