**采购需求**

一、采购清单

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 货物名称 | 数量 | 单位 |
| 1 | 网络出口防火墙（核心产品） | 1 | 台 |

二、技术参数

|  |  |
| --- | --- |
| **序号** | **技术参数** |
| 1 | 1、产品硬件架构采用标准机架框式模块化架构设备，要求主控模块、防火墙安全业务模块相互分离。  ★2、单台设备实配主控模块≥2个，console管理口≥2个，满配电源模块，满配风扇模块。  ★3、实配：100G光口≥8个（满配多模模块），万兆光口≥40个（满配单模模块），千兆电口≥2个，千兆光接口≥2个（满配单模模块）。  4、整机可用接口模块槽位≥3个，支持扩展100G、40G、10G板卡。  ★5、整机吞吐量≥600Gbps，并发连接数≥9000万，每秒新建连接（HTTP）数≥360万。  ★6、整机具备可承载70G以上出口流量的安全防护能力。  7、设备实配IPSec VPN、SSL VPN、L2TP VPN、GRE、GRE over IPSec功能，实配不少于128个并发SSL VPN用户授权。要求设备对IPSec VPN功能支持自定义协议端口。  8、稳定性要求：设备电源模块和风扇模块支持热插拔；支持主主、主备模式双机部署；具备BFD功能，BFD可与静态路由、OSPF、BGP进行联动，实现快速检测互联设备通信故障并进行预设业务切换。  9、设备具备IPv6特性，具备OSPFv3、BGP4+、IS-IS动态路由和IPv6静态路由功能。访问控制、攻击防护、应用识别、URL过滤、入侵防御等功能均需支持IPv6业务场景。对每个IPv6用户具备通IPv4用户一致的上下行流量统计、会话统计等功能，具备IPv6日志审计功能。  10、实配IPv4和IPv6双栈功能，IPv6无需授权开通。实现IPv6与IPv4互访，支持IPv4／IPv6 NAT地址转换，支持源地址一对一、多对多、多对一转换，目的地址一对一转换，支持NAT46和NAT64技术。  11、故障检测和快速恢复要求：设备实配链路故障无感知自动切换功能，检测到链路故障时设备自动按照预配的切换策略将流量转发至备份线路。故障链路恢复后，自动切换回原线路。  12、链路负载均衡功能要求：（1）实配ISP流量调度功能，对于出方向流量，可以基于目的地址运营商属性进行选路，具备ISP信息库自动升级功能。（2）具备综合分析出口链路带宽利用率、线路丢包率、抖动和延迟时间，智能选择高质量链路转发数据。（3）具备基于应用类型的负载均衡功能，根据应用类型选择不同的出口线路，并支持在多个选定出口线路上实现负载分担。  13、设备能够与我校认证计费系统对接，实现基于认证系统中的用户名、学工号和IP、MAC地址的关联，便于进行日志查询和定位，实现上网用户实名制日志审计。  14、访问控制功能要求：设备实配会话控制功能，支持基于源IP、目的IP、服务类型和应用协议等多种条件配置会话数限制策略和新建会话速率控制策略。具备单条控制策略可基于传统五元组以及用户名称、角色类型、应用类型、域名等元素实现访问控制。  15、入侵防御功能要求：设备实配对HTTP、FTP、SMTP、IMAP、POP3、TELNET、TCP、UDP、DNS、RPC、FINGER、MSSQL、ORACLE、NNTP、DHCP、LDAP、VoIP、NETBIOS、TFTP、SUNRPC 和MSRPC 等常用协议及应用的攻击防御；具备8000种以上攻击特征库规则列表，其中4000种以上HTTP 特征库规则列表。具备缓冲区溢出、SQL注入、请求伪造攻击（CSRF）、XSS防护。 具备CC攻击防御。具备对基于SSL加密流量的入侵防御。具备特征库表的更新服务。  16、威胁分析功能要求：要求设备厂商具备较全面的威胁情报能力，具备识别僵尸网络、APT攻击、勒索软件和挖矿等多种威胁类型能力。具备威胁情报库的自动更新服务。  17、日志功能要求：具备将日志按照类型分开记录和显示，实现NAT日志、会话日志、策略路由日志、威胁日志、URL 日志、事件日志、配置日志、文件过滤日志、内容过滤日志、上网行为审计日志等类型日志的记录、查询、导出等功能，提供第三方数据对接接口，具备同时向不少不5个外部日志接收系统的Syslog输出能力。  18、实配RESTful接口，实现自定义对接第三方应用。支持通过API方式与第三方平台联动，实现平台调用封堵能力。  ★19、实配病毒过滤服务≥5年，入侵防御特征库服务≥5年，应用特征库服务≥5年，URL库升级服务≥5年，威胁情报升级服务≥5年，ISP信息库升级服务≥5年，原厂质保服务≥5年。提供原厂质保服务承诺。  20、实施要求：（1）配合学校完成安全策略梳理，制定详细的割接实施方案（包括防火墙、相关核心交换机等设备的配置和操作步骤），割接完成后的业务测试方案以及割接回退预案。（2）实施过程中需具备完整的文档管理能力，包括但不限于：开箱报告、实施文档、测试文档、培训文档等。（3）实施完成后，提供不少于2天、5人次的原厂商认证的工程师安装配置等实操培训课程，场地、交通等与培训相关的费用均由投标人承担。 |