编号：

安全防火墙设备技术需求书

1. 设备需求
2. 安全防火墙设备数量壹台
3. 设备及设备及所属软件均应有有效和合法的授权。
4. 集成商资格要求
5. 集成商为具有在中华人民共和国境内注册的独立法人的生产厂商或其直接委托的代理人。
6. 集成商需在上海地区有正式的分支机构。
7. 具备生产厂商认证的技术人员至少2名。
8. 集成商应为设备生产厂商授权的区域代理,并提供相应证书。
9. 生产厂商对本次设备提供的授权函原件。
10. 售后服务要求
11. 集成商应为安信保险股份有限公司（以下称为甲方）提供及时周到的系统技术支持。
12. 集成商应确保为甲方提供7\*24小时技术支持服务，响应时间不应该超过1小时，现场响应支持不应超过4小时。
13. 集成商所提供设备保质期均为三年（具有特殊要求的除外），集成商所提供的设备在保质期内因硬件、软件本身质量问题所造成的损坏或无法正常运行，由此产生的维修、更换硬件和软件故障排除等所需一切费用（包括工程师差旅费用等支出）由集成商负责。硬件更换后，新硬件的保质期自硬件启用之日起顺延一年。
14. 集成商应提供相应的备件支持，以便及时更换损坏硬件。
15. 集成商应在质保期后设备生命周期内有义务继续对系统设备提供维保服务，甲方将支付相应费用。
16. 针对以上要求，集成商可提供具体可行的有吸引力的合作方案。
17. 验收
18. 所有设备均需提供安装服务，所采购设备（包括软件）安装都必须由生产厂商授权集成商执行。
19. 安装前由甲方信息技术部协同甲方行政办公室对货物的品牌、数量、包装等方面进行实物验收。集成商提供的所有包装的货物均应完好无损。如遇交付前已拆封的货物，甲方有权拒绝或要求更换。集成商交货时，必需提供所有产品原厂或总代理出具的供货相关证明。
20. 集成商根据甲方技术要求在甲方信息技术部指导下进行设备安装、调试，并由甲方信息技术部进行使用性能方面的验收。
21. 设备技术指标
22. **性能及配置要求**

|  |  |
| --- | --- |
| **项目** | **技术要求** |
| 应用层吞吐量 | ≥700 |
| 并发连接数 | ≥1,000,000 |
| 每秒新建连接数 | ≥4万 |
| 设备接口 | ≥4 |
| BYPASS | 支持 |
| 尺寸 | 标准1U架构 |

1. **功能要求**

|  |  |
| --- | --- |
| 技术指标 | 指标要求 |
| 部署方式 | 支持路由，网桥，单臂，旁路，虚拟网线以及混合部署方式； |
| 网络特性 | 支持802.1Q VLAN Trunk、access接口，VLAN三层接口，子接口；  支持链路聚合功能；  支持端口联动功能，当上行/下行端口链路出现故障时，对应的另一端下行/上行端口自动切断链路； |
| 路由支持 | 支持静态路由，ECMP等价路由；  支持RIPv1/v2，OSPFv2/v3，BGP等动态路由协议；  支持多播路由协议； |
| 基础功能 | 支持连接会话展示，可针对具体的IP地址进行会话详情查询，支持封锁异常会话信息，并支持设置监听具体IP的会话记录；  访问控制规则支持基于源／目的IP，源端口，源／目的区域，用户（组），应用/服务类型，时间组的细化控制方式；  访问控制规则支持数据模拟匹配，输入源目的IP、端口、协议五元组信息，模拟策略匹配方式，给出最可能的匹配结果，方便排查故障，或环境部署前的调试；  访问控制规则支持分组管理；  支持基于应用类型，网站类型，文件类型进行带宽分配和流量控制；  支持IPSec VPN，SSL VPN，GRE，GRE over OSPF，GRE over IPSec等VPN接入方式；  支持在防火墙上配置VPN安全策略对加密隧道内的流量进行清洗； |
| Web应用安全防护 | 设备具备独立的WEB应用防护识别库；  支持HTTP 1.0/1.1，HTTPS协议的安全威胁检测；  支持服务器资产自动识别；  支持抵御SQL注入、XSS、系统命令等注入型攻击；  支持CC攻击、CSRF攻击、COOKIE攻击等攻击防护功能；  支持关联上下文，对webshell脚本上传动作进行语法，语义匹配和过滤；  支持对服务器已经被植入webshell后门之后的通信动作进行识别和阻断；  支持上传文件类型识别，防止文件后缀名修改绕过；  支持对网站的扫描防护和防止恶意爬虫攻击；支持其他类型的Web攻击，如文件包含，目录遍历，信息泄露攻击等；  支持针对网站的漏洞扫描进行防护，能够拦截漏洞扫描设备或软件对网站漏洞的扫描探测；  支持Web漏洞扫描功能，可扫描检测网站是否存在SQL注入、XSS、跨站脚本、目录遍历、文件包含、命令执行等脚本漏洞；  支持对网站黑链进行检测； |
| 僵尸主机检测 | 设备具备独立的僵尸网络识别库；  支持对终端已被种植了远控木马或者病毒等恶意软件进行检测，并且能够对检测到的恶意软件行为进行深入的分析，展示和外部命令控制服务器的交互行为和其他可疑行为；  对于未知威胁具备同云端安全分析引擎进行联动的能力，上报可疑行为并在云端进行沙盒检测，并下发威胁行为分析报告；  支持通过云端的大数据分析平台，发现和展示整个僵尸网络的构成和分布，定位僵尸网络控制服务器的地址； |
| 安全可视化 | 支持资产的自动发现以及资产脆弱性和服务器开放端口的自动识别； 支持对检测到的攻击行为按照IP地址的地理位置信息进行威胁信息动态展示，实时监测和展示最新的攻击威胁信息； 支持自动生成安全风险报表，报表内容体现被保护对象的整体安全等级，发现漏洞情况以及遭受到攻击的漏洞统计，具备有效攻击行为次数统计和攻击举证；  支持受保护业务和用户的关联安全事件展示；  支持以攻击链方式来匹配和展示资产遭受到的攻击行为； |
| 安全集中管理 | 支持安全设备的集中管理，包括配置统一下发，规则库统一更新，安全日志，流量日志实时上报等功能；  支持接入统一的安全监测平台，通过安全监测平台可以实时看到每台安全设备的详细安全状态信息， |
| 高可用性 | 双机支持A/S，A/A方式部署；  支持配置同步，会话同步和用户状态同步；  支持双机心跳线冗余； |
| 系统配置管理 | 支持以安全策略模板方式快速部署安全策略，安全策略模板支持默认模板和自定义模板等多种格式；  支持场景化的配置向导功能，可以选择不同的部署方式以及使用场景实现产品的快速实施；  支持管理员权限分级，支持安全管理员、审计员、系统管理员三种权限；  支持内置规则库的手动/自动更新；  支持邮件、短信和微信告警； |

1. **资质要求**

|  |  |
| --- | --- |
| 产品资质 | 产品应具备计算机信息系统安全专用产品销售许可证；  产品应具备ISCCC中国国家信息安全产品认证证书；  涉密信息系统产品检测证书； |

1. 报名方式

有意者请于11月9日之前将标书及相关残料送至以下地址：

上海市静安区共和新路3651号 马春霞收

商务联系人：马春霞

联系方式：021-66988267 [macx@aaic.com.cn](mailto:macx@aaic.com.cn)

技术联系人：卫金凯

联系方式：021-66988391 [weijk@aaic.com.cn](mailto:weijk@aaic.com.cn)