上 海 海 事 大 学

自动化集装箱码头仿真实验室

网络安全系统与安全认证服务项目服务需求



上 海 海 事 大 学

二〇二〇年三月

一、投标条件

1. 投标单位必须提供针对本项目相关授权书原件和软硬件保修的服务承诺书。

2. 投标方应认真阅读采购书中所有的事项、格式、条款和技术规范等。投标方没有按照标书要求提交全部资料，或者没有做出实质性响应，上海海事大学有权拒绝投标方参与采购洽谈。投标方可以在投标文件中建议不同的标准、型号和系统集成方案，但建议方案的合理性和先进性应该相当于或超过招标文件中的要求。

二、具体技术要求如下：

上海海事大学离岸工研究院云桌面项目分为普通云桌面和3D云桌面两个需求。其中普通云桌面主要用于云桌面办公，使用瘦终端接入云桌面系统进行软件开发等工作，同时用于外部开发人员接入到学校内网进行开发工作，保证接入安全，保证数据安全；3D云桌面主要用于发布码头3D仿真软件界面，保证能够任何地方接入到学院3D云桌面，显示仿真软件运行画面。为保证3D云桌面系统网络安全，需要对当前网络进行安全防护，具体设备及配置要求如下：

**（所列★指标均为关键指标，低于下列配置或不响应，用户有权拒绝投标方参与采购洽谈）：**

1. 下一代防火墙

|  |  |
| --- | --- |
| 技术指标 | 指标要求 |
| 硬件参数 | 三层吞吐量3.5Gbps，应用层吞吐量550Mbps；并发连接数200W，新建连接数6W； 1U尺寸； 4个千兆电口，2个千兆光口。1个串口（RJ45），2个USB 2.0， |
| 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； |
| 基础功能 | 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；  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  ★支持根据国家/地区来进行地域访问控制；（需提供相关功能截图证明）  VPN支持在防火墙上配置安全策略对加密隧道内的流量进行清洗； |
| 入侵防护功能 | ★入侵防护漏洞规则特征库数量在7000条以上；（需提供相关功能截图证明）  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；  具备防护常见网络协议（SSH、FTP、RDP、VNC、Netbios）和数据库（MySQL、Oracle、MSSQL）的弱密码扫描功能；  支持同防火墙访问控制规则进行联动，可以针对检测到的攻击源IP进行联动封锁，支持自定义封锁时间；  ★可提供最新的威胁情报信息，能够对新爆发的流行高危漏洞进行预警和自动检测，发现问题后支持一键生成防护规则； |
| 病毒防护 | 支持基于流引擎查毒技术，可以针对HTTP、FTP、SMTP、POP3等协议进行查杀；能实时查杀大量文件型、网络型和混合型等各类病毒；并采用新一代虚拟脱壳和行为判断技术，准确查杀各种变种病毒、未知病毒；内置1000万条以上的病毒样本 （需提供相关功能截图证明）  支持对常见压缩文件格式的检测，如zip，rar，7z  支持杀毒文件类型自定义  支持杀毒白名单功能，可以根据URL或者IP进行排除不检测病毒  支持检测到病毒后支持记录日志、阻断连接 |
| 僵尸主机检测 | ★设备具备独立的热门威胁库，防护类型包括木马远控、恶意脚本、勒索病毒、僵尸网络、挖矿病毒等，特征总数在60万条以上；（需提供相关功能截图证明）  ★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；（需提供相关功能截图证明）  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；（需提供相关功能截图证明）  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； |
| 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；  支持邮件、短信和微信告警； |
| 资质要求 | 为保障网络出口下一代防火墙产品的先进性，要求厂商具备CMMI5级别证书，确保软件开发成熟度，投标时需提供证书复印件、或可查询链接截图 |

1. 终端检测响应平台

|  |  |  |
| --- | --- | --- |
| 技术指标 | | 指标要求 |
| 产品整体概 述 | 产品形态 | 产品是软件形态，包含管理平台和终端Agent软件；  Agent软件支持32位和64位的Windows系统和64位的Linux系统。 |
| 部署方式 | 管理平台无需安装任何其他软件和专用设备硬件，采用基于X86服务器或虚拟服务器即可完成平台部署；终端Agent软件可以通过软件安装或虚拟机模板的方式进行安装。 |
| 平台管理可视化 | 简化终端管理 | 支持自动收集终端资产状况，包括：主机名、在线/离线状态、最近登录时间、最近登录的用户名；支持在控制台上启用、禁用、重启、远程卸载和移除终端agent，方便管理员对终端agent的远程管理； |
| 全网风险可视 | 支持控制台动态显示当前未处理的勒索病毒数量、暴力破解数量及其各自影响的终端数量，支持点击对应的威胁类别，下钻到响应中心对应的威胁事件列表； |
| 安全策略  一体化 | 支持安全策略一体化配置，通过一条策略即可实现不同安全功能的配置，包括：终端病毒查杀的文件扫描配置、暴力破解的威胁处置方式和Windows系统下信任区文件目录配置；（提供界面截图） |
| 日志与  报表  管理 | 多维度日志查询 | 支持根据统计周期、终端名称、IP地址、脚本命令名称和执行结果查询全网终端脚本执行日志，内容包括：任务名称、任务执行脚本名称、执行类型、执行时间、执行状态和脚本执行日志的导出； |
| 可视化报表 | 支持图形化显示全网终端安全概览，包括：风险终端总数、未处理威胁终端数、已处理威胁数、未处理威胁数等； |
| 系统管 理 | 产品安装升级场景化 | 支持管理平台更新检测、自动下载升级和离线导入升级包升级；  支持agent的错峰升级，可根据实际情况控制agent同时升级的最大数量，避免大量终端程序同时更新造成网络拥堵或I/O风暴； |
| 威胁检测与响应能力 | 终端病毒查杀 | 支持通过管理平台下发立即扫描杀毒的任务，可针对某一台终端，也可针对某一组终端进行扫描杀毒；  具备基于多维度轻量级的无特征检测技术，多引擎协同工作，包括：基于AI技术的自研引擎、基于家族基因分析的特征检测引擎、基于虚拟执行和操作系统环境仿真技术的行为引擎、基于大数据分析平台的云查引擎。（提供界面截图）  支持极速、均衡、低耗三种扫描模式，以控制扫描时对业务系统CPU资源的占用；（提供界面截图） |
| 支持展示勒索病毒事件、木马病毒事件、蠕虫病毒事件和其他病毒文件事件及其详情，包括：病毒文件名称，事件等级，受感染的文件，发现时间，检测引擎，文件Hash值，文件大小，文件创建时间。 |
| 支持对风险终端进行终端隔离，避免感染终端对内网其他主机的病毒传播； |
| 服务器WebShell检测 | WebShell文件的检查综合利用文件信誉库、静态分析、机器学习、运行行为分析对文件进行判断。 |
| 支持配置WebShell检测开启或关闭；  支持配置WebShell实时扫描，一旦发现WebShell文件，自动隔离或仅上报不隔离。（提供界面截图） |
| 支持展示终端检测到的WebShell事件及事件详情，包括：恶意文件名称，事件等级，受感染的文件，发现时间，检测引擎，文件类型，文件名，文件Hash值，文件大小，文件创建时间，检测依据；（提供界面截图） |
| USB设备扫描 | 支持插入U盘时主动扫描U盘文件；支持U盘窗口信息展示：剩余空间、总空间； |
| 暴力破解检测 | 基于Agent的RDP和SSH登录日志检测的暴力破解入侵检测； |
| 支持单个攻击源和分布式攻击源的暴力破解检测；  支持开启暴力破解实时检测，自动封堵攻击源的IP地址，封停时间支持配置；  （提供界面截图） |
| 基线合规检查 | 支持windows系统永恒之蓝漏洞（MS17-010）的检测；  针对Linux系统提供如下安全基线合规检查：身份鉴别、访问控制、安全审计、 SSH策略检测、入侵防范、恶意代码防范； |
| 支持可视化展示终端的基线合规检查结果。 |
| 文件实时监控 | 支持对来自Internet、E-mail或是光盘、移动存储、网络等各种入口渠道病毒进行实时检测；  支持在安全策略中配置Windows系统下的信任文件或目录，添加至信任区的文件或目录在文件实时监控时将被跳过，以提升查杀效率和降低误杀率； |
| 微隔离-  流量访问控 制 | 微隔离流量可视 | 支持微隔离功能主界面图形化显示业务系统、服务器及流量详情；  支持图形化显示服务器间流量关系，包括访问详情、流量趋势等； |
| 微隔离流量可控 | 支持对业务系统配置微隔离策略规则；  支持指定微隔离策略的适用区域：单个终端、任意终端、指定IP网段、业务系统、应用角色。 |
| 微隔离策略管理 | 支持定时备份和手动备份mgr的微隔离配置（微隔离策略、业务系统、服务器、IP组、应用角色、服务列表、安全配置、系统维护配置）和微隔离数据（访问关系、访问详情）。 |
| 联动响应能力 | 与同厂商下一代防火墙设备进行联动 | 支持多台同厂商防火墙通过配置终端检测响应管理平台IP地址实现与平台的联动，实现端网安全联动；  支持管理员在同厂商下一代防火墙平台查看其下发的查杀任务中各个终端的查杀状态；查看查杀结果，统一进行处置 |
| 资质要求 | | 为保障终端检测与响应平台厂商的应急响应服务能力，要求厂商应是国家互联网应急响应中心网络安全应急服务国家级支撑单位；提供可查询链接截图或证书复印件（加盖厂商公章） |

1. 24口接入交换机要求
   * + 24个10/100/1000Base-T以太网端口，4个万兆SFP+
     + 交流供电，支持RPS冗余电源
     + 交换容量：336Gbps/3.36Tbps
     + 包转发率：108Mpps/126Mpps
2. 安全测试评估报告

针对应用系统模拟黑客行为进行渗透测试验证，找出应用系统安全漏洞、逻辑漏洞等风险点，给出整改建议；

通过专有漏洞扫描设备，对服务器、信息系统等进行扫描，提供漏洞扫描报告；

提供一次针对网络结构、网络设备、安全设备、服务器、数据库等资产的安全检查，找出安全风险，提供安全整改建议。

1. 测试安装技术及客户端：
   * + 硬件升级技术支持与测试。
     + 系统安装及基础软件配置，确保正常使用。
     + 防火墙部署安装调试，包含杀毒软件与防火墙联动设置，确保服务器硬件环境搭建，交换机部署，机房线路整改管理，及相关控制平台安装调试。
     + 对客户端电脑进行全部测试安全性及测试
     + 对服务器进行安全保护操作，并确保更新补丁。
     + 提供相关安全整体解决方案培训与控制平台管理基础培训
2. 代码服务器部署技术要求
   * + SVN服务器底层系统安装及操作系统基本安全调试
     + SVN服务软件安装部署，部署稳定版本软件
     + SVN代码版本库建立，根据客户使用场景建立代码库，并测试功能完整性
     + SVN服务器用户建立及权限分配，确保用户能够使用但权限不超过限制
     + 代码服务器备份设定，保证SVN代码库和用户权限备份到其他服务器上
3. 安全代理服务器

主要用于扩展机房已有服务器硬件，满足桌面云后台服务器运行要求，具体参数如下：

|  |  |
| --- | --- |
| **服务器硬件扩容要求** | |
| **指标项** | **指标要求** |
| 内存\*4 | * 浪潮（INSPUR）浪潮原厂内存 服务器主机专用配件 16G DDR4 2400T/2666V |
| PCI-SSD系统盘\*2 | * 英特尔® 固态盘 400GB，半高 PCIe 3.0，20 纳米，MLC顺序读取（最高）2700 MB/s 顺序写入（最高） 1080 MB/s |
| SATA 数据盘\*4 | * 3.5寸企业级硬盘，SATA 6G接口，7200转 6T容量 |