## 安徽省地质实验研究所网络安全设备及服务 采购项目招标参数

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 名称 | 参数需求 | 品牌要求 | 数量 |
| 1 | 网站应用防火墙（WAF） | **1、产品硬件、接口及性能要求：**  1)产品必须为专业性WEB应用防火墙产品，而非NGAF、NGFW、UTM设备，以产品资质证书里的产品名称为准；  2)标准机架式设备，至少配置6个千兆电口（光口），内置至少两路硬件bypass；http防护能力≥1Gbps，最大并发HTTP连接数≥100万，每秒新建HTTP连接数≥1万。  **2、产品功能要求：**  1)产品应支持透明、代理模式、旁路部署，支持NAT环境下的用户识别能力，应采用基于行为分析的检测技术，对0day攻击能够很好地防范；  2)应具备对SQL注入攻击、XSS攻击的检测与防御能力；  3)应具备对爬虫检测、CGI扫描、漏洞扫描等检测与防御能力，具备XML DoS检测与防御能力（提供界面截图）；  4)应具备网页挂马检测与防御能力，具备WebShell检测与防御能力；  5)应支持Web服务器操作系统指纹信息返回保护，支持HTTP错误页面信息返回保护（提供界面截图）；  6)应支持针对重点URL的网页防篡改功能，同时不会对Web服务器及Web应用系统造成额外影响（提供界面截图）；  7)应支持多WEB服务器负载均衡功能（提供界面截图）。  **3、资质要求：**  投标产品需具有以下资质：公安部产品销售许可证、EAL3+认证、Web 应用防火墙认证证书、ISCCC颁发的产品认证证书，投标时提供加盖原厂商公章的证书复印件。  **4、产品服务要求：**  1)三年原厂免费硬件质保及售后服务支持，三年Web应用防护事件库免费在线升级；  2)投标时需提供原厂授权书和服务承诺函。 | 启明星辰/天存/绿盟/深信服 | 1套 |
| 2 | 入侵防御系统（IPS） | **1、产品硬件、接口及性能要求：**  1) )产品需为标准机架式设备，产品至少配置6个千兆电口（光口），至少具备2路内置硬件bypass，至少具有1个接口板扩展槽位，用于后期根据网络需要扩展千兆接口或者万兆接口；设备最大并发连接数≥300万，最大吞吐量≥10G，IPS混合包检测流量≥2G。  2)设备入侵防护路数不受许可限制，以适应增加接口后多路防护的需要。  **2、产品功能要求：**  1)可基于IP地址、网段、时间、VLAN、协议类型等条件设定入侵检测及响应方式，支持多种响应方式，满足客户不同的安全需求，需包括：重置、临时阻断、丢弃报文、丢弃会话等动作；  2)支持对网络蠕虫、木马后门、缓冲区溢出、间谍软件等各种攻击行为进行检测及防御；  3) 系统应单独针对SQL注入、XSS攻击提供白名单功能，允许用户对不够规范的Web应用进行放行，能够精确到检测点、属性和名称；  4) 系统应支持端口聚合/链路捆绑协议，并提供手工方式和LACP两种配置方式，基于多种负载均衡算法，增加IPS和网络设备间的带宽并提供链路冗余，使得处理流量平滑升级并提供可靠性；  5) 系统应支持高负载下的bypass功能，使得系统在CPU和内存较高情况下启动bypass功能，避免网络出现延迟和丢包等情况，提高网络可用性。并可配置启用Bypass的CPU和内存阈值，及选择取值的计算方式（最高值/平均值、时间区间等），防止设备出现Bypass状态震荡；  6) 提供WEB登录图像验证码功能，防止暴力破解；系统支持定期修改密码功能，提高密码安全性；  **3、资质要求**  投标产品需具有：公安部产品销售许可证、EAL3级认证证书、ISCCC信息安全产品强制认证证书（三级），投标时提供加盖原厂商公章的证书复印件。  **4、售后质保要求：**  1)须提供厂商三年免费质保函，包括免费提供三年原厂工程师现场技术支持服务，三年入侵特征库免费在线升级服务和硬件质保；  2)投标时需提供原厂授权书和服务承诺函。 | 启明星辰/网神/绿盟/深信服 | 1套 |
| 3 | 网页防篡改系统 | **1、总体要求：**  上传文件速度：≤5ms（50K文件）；篡改检测时间：访问时实时检测；篡改恢复时间：≤6ms。  **2、功能要求：**  1)篡改检测功能：  （1）支持Windows、Linux、Unix；  （2）篡改检测和防护模块内嵌于Web服务器软件中；支持IIS、Apache、J2EE（Weblogic/Websphere）、Nginx等；  （3）同时支持外挂轮询、核心内嵌及事件触发三种篡改检测技术（提供截图证明）；  （4）具有网络校验功能，可通网络内的集中存储设备，对文件数字水印进行验证；  （5）提供水印签发工具，允许手工签发水印，并提供水印存储格式转换功能，允许其他格式的水印库导入到当前配置的水印库格式（提供截图证明）；  （6）支持预先禁止非法程序对备份/保护目录的添加/删除/修改/更名/属性变更等操作。  2)同步、发布功能：  网页发布同时自动更新水印值；支持断线/连线状态下篡改检测；支持连线状态下网页恢复；同步和断线时都不影响检测；不影响原有的网页发布系统；自动检测文件系统任何变化；文件变化自动同步到多个Web服务器；支持断线续传和失败重传；发布服务器支持Windows和Linux操作系统平台；  **3、产品资质要求：**  1）需提供公安部《计算机信息系统安全专用产品销售许可证》；  2）需提供通过公安部制定的《网站数据恢复》产品的检测并提供检验报告复印件；  3）需提供国家版权局颁发的《计算机软件著作权登记证书》；  4)需提供产品获得的《软件产品证书》；  **4、技术服务要求：**  1)提供原厂商针对本项目的授权书及产品售后服务承诺函；  2)提供3年原厂商免费升级、上门维护及应急响应服务；  3)产品原厂商需提供季度巡检服务，并出具相关季度巡检报告，重大节日前做好相应安全服务保障工作；提供7\*24小时应急响应服务，需在0.5小时内做出响应，1小时内到达现场处理。 | 天存/绿盟/安恒/深信服 | 1套 |
| 4 | 上网行为管理系统 | **1、产品硬件、接口及性能要求：**  1）标准机架设备，具备6个千兆电口（光口）；  2）吞吐量≥800Mbps；并发用户数≥1200；并发会话数≥50万；  3）设备需内置存储空间，用于存放设备产生的各种日志信息。  **2、产品功能要求：**  1）设备部署支持网关模式、镜像模式、网桥模式、多路桥接模式等多种网络模式，支持GRE、L2TP、WLTP、CAACWS、LWAPP、CAPWAP协议下的网络环境。  2）设备需支持如下用户上网认证方式：用户名/密码认证、短信认证、微信认证（用户关注微信公众号后即通过身份认证，后台记录用户ID（提供界面证明））及二维码认证（管理员扫描访客的二维码后对其网络访问授权（提供界面证明））。  3）设备需内置应用识别规则库，并保持定期更新，保证应用识别的准确率（提供产品配置界面截图证明）。  4）支持识别终端系统后台运行的进程信息，防止间谍软件的运行。  5）系统需内置预分类的URL地址库、恶意网址库（提供产品配置界面截图证明）；具备网址智能学习功能，支持根据用户训练的关键字、网址自动将未知网页分类和过滤（提供产品配置界面截图证明）。  6）系统需能识别并过滤SSL加密的钓鱼网站、金融购物网站、非法网站等。  7）系统必须能识别执行脚本的网页，并过滤脚本中隐藏木马等程序的网页。  8）具备动态流量控制功能：设置流量策略后，仍可根据整体线路或流量通道实际空闲/繁忙情况自动启用/停止使用流量控制策略，以提升带宽利用率（提供产品配置界面截图证明）。  9）具备基于应用类型、网站类型、文件类型划分与分配带宽的功能（提供产品配置界面截图证明）。  10）具备审计QQ、webqq、miniqq、webmsn、qqmail等即时通信软件的功能。  11）支持以USB-Key方式验证接入数据中心的管理员身份并分配管理员的日志审计权限。  12）支持IP/MAC的跨三层交换机的绑定。  13）集成无线控制器功能，方便后期扩展无线，可基于SSID的进行上网权限控制和流控。  **3、资质及服务要求：**  1）提供公安部公共信息网络安全监察局颁发的《计算机信息系统安全专用产品销售许可证》（复印件加盖生产厂家公章）。  2）产品提供三年免费软、硬件质保，免费三年备件和上门服务（含系统升级、URL库及应用协议库升级服务等），投标时提供产品原厂授权书和免费质保服务承诺函原件。 | 网康/深信服 | 1套 |
| 5 | 数据备份一体机 | **1、设备配置：**  1）2U机架式；CPU≥1颗64位Intel八核处理器、32GB高速缓存；千兆网口≥2；硬盘位≥8，支持硬件RAID0、1、10、5、50、6等，并支持全局热备盘；支持企业级SAS硬盘、SATA硬盘和SSD固态硬盘混插；配置≥8块4TB企业级SATA硬盘。  2）设备系统和软件需安装在2块120GB企业级SSD磁盘上，不占用前面板的槽位。  **2、功能描述：**  1）支持Windows/Linux/UNIX平台，支持操作系统的在线备份；支持SQLServer、Oracle、Mysql、DB2、AD等常见数据库的在线备份；  2）备份系统需支持web方式登录，确保登录与访问安全（提供此功能截图并加盖原厂商公章）；  3）支持对SQL Server、Oracle等主流应用的在线实时备份保护；  4）支持传输加密和存储加密功能，支持数据库压缩功能（投标时提供该项功能截图并加盖原厂公章）；  **3、异地数据容灾：**  1）支持D2D2R 备份数据异地容灾，通过本地脱机备份然后容灾到异地；支持一对一、一对多、多对一以及多对多等多种容灾复制方式；可通过机器码进行设备的识别与绑定，实现两台或多台设备之间备份数据的自动远程复制，从而提高数据的安全性（提供此功能截图并加盖原厂商公章）；  2）支持异地备份数据的安全管理机制，介质服务器需要得到本地的备份一体机授权许可后，才可以浏览、恢复本地传输过去的备份数据，最大限度避免备份数据的泄密可能(提供此功能截图并加盖原厂商公章)。  **4、软件许可：**  要求投标产品的许可授权，实现Windows和Linux平台下的定时备份，不限制需要备份的服务器、PC机、虚拟机的数量，不限制数据库的数量与类型。（提供上述许可的原厂承诺函，并加盖原厂公章或投标专用章）  **5、资质要求：**  1）要求所投产品具有软件著作权登记证书，软件产品登记证书；要求备份软件具有中国国家信息安全产品认证证书（ISCCC）；要求备份软件通过公安部信息安全专用产品检测，具备公安部颁发的《计算机信息系统安全专用产品销售许可证》；  2）投标时提供以上证书复印件，并加盖原厂商公章。  **6、原厂商服务和授权**  1）提供设备3年质保，提供原厂工程师安装、实施、培训服务。  2）提供原厂工程师一年无限次免费上门服务；提供四年原厂免费邮件和电话技术支持服务。  3）提供原厂商针对本项目的授权函与服务承诺函，服务承诺函中必须包含以上原厂服务。 | 爱数/黑方/曙光 | 1套 |
| 6 | 交换机 | 标准机架式设备，千兆以太网交换机，背板带宽256Gbps，包转发率66Mpps，固化24个10/100/1000Base-T以太网端口和4个1000Base-X以太网端口，可网管，支持端口聚合。 | H3C/华为/锐捷 | 1台 |
| 7 | 渗透测试和应急服务 | 1. **资产梳理服务：**   对机房内信息资产进行梳理，为我单位提供合法的信息系统资产管理工具软件并安装使用，将梳理统计的输出文档结果整合到资产管理工具里，实现信息系统资产详细信息的动态维护，在相关资产属性信息出现变更的情况下，能够第一时间更新进资产管理系统，解决长时间运维后资产信息变动导致的资产统计表格信息不准确的问题。   1. **渗透测试服务：**   对网站等对互联网提供访问服务的系统进行渗透测试，模拟黑客在互联网上对系统进行黑盒渗透测试，主要用于发现OA系统、网站系统、其他互联网业务应用系统可能存在的口令明文传输、暴力破解、认证绕过、SQL注入、溢出、XSS、目录泄露、敏感文件下载、旁站等安全问题。出具渗透测试报告，根据渗透测试的结果提供修复建议方法，并协助用户与开发商一起修复存在的安全漏洞。提供服务的公司需具有专业的安全服务团队，具备漏洞挖掘能力，自主获取CNVD国家信息安全漏洞共享平台原创漏洞证明证书不少于5个（提供证书复印件）。   1. **应急响应服务：**   当网络设备、安全设备、服务器设备、操作系统、业务应用系统等发生异常状况时，要求服务商在故障发生15分钟以内提供远程或者电话解决。对电话解决不了的故障，要求于1小时之内安排专业工程师到达现场解决。应急服务结束后需提供《异常问题应急响应处置报告》。  当网站等应用系统出现被黑客入侵、挂马、篡改等安全事件之后，提供分析、取证、追踪、恢复、加固等全方位的技术支持服务。对操作系统和网站日志进行深入分析，发现入侵的痕迹，明确黑客入侵的时间线、IP地址，定位黑客入侵的方式、利用点，梳理黑客入侵进入业务系统之后的行为和动作，出具详尽的分析报告。根据分析结果，清理后门和木马程序，删除黑客上传或生成的文件，协助修补互联网应用相关漏洞，完善相关安全防护策略，加固安全防护体系。  应急响应服务工程师须具备协议分析、流量分析、疑难故障分析定位、蠕虫病毒木马分析、黑客入侵分析等专业技术能力，服务人员需具有ISCCC中国信息安全认证中心颁发的信息安全保障人员-应急服务（专业级）证书和工信部颁发的高级网络信息安全工程师认证证书，提供两种证书的复印件。  服务期限：自合同签订后一年。   1. **网站加固系统：**   部署在网站服务器上，对操作系统、网站应用系统进行综合安全检测和防护，设置多个安全监测点、防护规则围栏，完整记录攻击事件，回溯攻击路径。   1. **应用漏洞跟踪、站点安全监测：**   利用漏洞平台监测工具，每日自动化追踪CNVD（国家信息安全漏洞共享平台）、CNNVD（中国国家信息安全漏洞库）、wooyun（乌云安全漏洞报告平台）、补天漏洞响应平台、漏洞盒子等互联网第三方漏洞平台提交的最新的漏洞。针对互联网应用最新暴露在第三方漏洞平台的相关漏洞信息进行及时的记录和验证，形成《漏洞报告表》，并在第一时间通知用户；协助用户到相关漏洞平台注册认领相应漏洞，获取漏洞相关细节；协助用户联系相关应用开发商，沟通说明应用漏洞情况，要求应用开发商修补相关漏洞；在应用开发商修补相应漏洞后，对其修补的效果进行进一步的验证，以明确漏洞修补的有效性。 |  | 1批 |