**WEB应用防火墙、网络安全威胁检测与智能分析系统招标技术规格书**

**一、工程说明**

随着集团公司的业务的发展，业务应用和网络使用对信息安全的保障要求越来越高，集团公司共有安全监测、人员定位、矿井三维、ERP、外网网站五个业务系统进行了等级保护测评，其中ERP系统须符合等级保护三级标准要求，其他四个业务系统须符合等级保护二级标准要求，根据《信息系统安全等级保护基本要求》（GB/T22239-2008），集团公司对定级的信息系统需要进行基本的安全等级保护。在等保相关控制点能够满足的条件下，尽量加强防护水平，实现安全的信息系统为集团公司的生产提供可靠的保障。

**二、设备采购清单**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 序号 | 设备名称 | 单位 | 数量 | 主要参数 | 备注 |
| 1 | WEB应用防火墙 | 台 | 2 | 1个GE管理口，4个GE电口、4个GE光口，2个万兆口，支持BYPASS，硬盘≥500G。  应用吞吐量不小于4Gbps  HTTP并发连接不小于20万  HTTP新建连接(CPS)不小于5万  支持HTTP 0.9/1.0/1.1，完全解析HTTP事务。  支持对SSL（HTTPS）加密会话进行分析。  支持对注入、XSS、SSI指令、Webshell防护、路径穿越、爬虫、盗链、及远程文件包含的攻击防护。  支持Cookie安全机制、CSRF（跨站请求伪造）防护。  支持透明部署，旁路部署，反向代理模式以及镜像部署模式。  支持智能识别攻击者，对网站连接发起攻击的IP地址进行自动锁定禁止访问被攻击的网站。  根据产生的安全日志进行智能分析，提高人工分析效率，减小规则误判概率。  支持热插拔的冗余双电源。 | 三年7\*24原厂保修，出具原厂盖章的服务承诺函 |
| 2 | 网络安全威胁检测与智能分析系统 | 台 | 1 | 具有完全自主知识产权的专用安全操作系统，稳定可靠。  2个USB接口，1个RJ45串口，1个GE管理口，4个千兆电口，4个千兆光口，2个万兆口。  三层吞吐量≥8Gbps,应用层吞吐量≥4Gbps  最大并发连接≥200万  每秒新建会话数≥5万  系统应提供覆盖广泛的攻击特征库，可针对网络病毒、蠕虫、间谍软件、木马后门、扫描探测、暴力破解等恶意流量进行检测和阻断，攻击特征库数量至少为5000种以上.  系统应提供DoS/DDoS攻击防护能力，支持TCP/UDP/ICMP/ACK Flooding，以及UDP/ICMP Smurfing等常见的DoS/DDoS的攻击。  支持基于阈值和自学习检测。  系统应支持全面的流量分析功能，可察看网络实时流量。  系统应提供灵活的流量管理功能，可以根据用户、应用、目的IP地址、时间及带宽等因素，实现基于应用、面向对象的流量保护策略。  系统应提供基于告警设备、时间、IP地址、事件类型、用户身份等条件的日志检索功能。  支持BYPASS功能。  系统应提供基于告警设备、时间、IP地址、事件类型、用户身份等条件的日志检索功能，具备日志备份、清除和恢复功能。  系统应提供支持用户自定义的统计分析告警功能。  投标厂商应承诺至少每月定期升级攻击特征库，遇到重大安全事件，提供即时升级。  支持热插拔的冗余双电源。 | 三年7\*24原厂保修，出具原厂盖章的服务承诺函 |

**三、设备技术指标**

**1、设备安装说明**

本次所购设备中所有安装材料均按最终现场工勘确认，所需材料均由中标方提供，施工工艺必须满足神华宁煤信息技术中心机房质量标准化标准。设备安装调试所必须的，但本方案中未提及的辅材，投标方也应在本次招标中一并提供，如有漏项，后期实施时也应无偿提供。

**2、机房环境**

机房位于银川神华宁煤信息技术中心网络数据机房，采用上走线方式。

**3、设计方案**

根据设备须实现的功能采用不同的方式进行部署，串行部署的设备必须具备bypass功能，旁路部署的设备必须能够识别网内的真实流量，依据流量进行相关策略配置。详细方案设计见《网络安全系统建设项目技术方案》。





**4、网络安全设备详细技术要求**

**4.1 WEB应用防火墙详细技术要求**

|  |  |
| --- | --- |
| 指标项 | 详细说明 |
| 设备要求 | 专用机架式硬件设备，系统硬件为全内置封闭式结构，稳定可靠，用户界面、配置和管理等，均为中文，易于理解，并有详尽的中文技术文档。产品为专业的WEB应用防护系统产品； |
| 1\*GE电管理口，8\*工作口（4\*GE电口，4\*GE光口），2个万兆口，硬盘容量≥500G，标配1+1冗余电源，电源可热插拔。 |
| 应用吞吐量不小于4Gbps；  HTTP并发连接不小于20万；  HTTP新建连接(CPS)不小于5万。 |
| 部署能力要求 | 支持透明部署，旁路部署。 |
| 防护功能要求 | 支持HTTP 0.9/1.0/1.1，完全解析HTTP事务。 |
| 支持对SSL（HTTPS）加密会话进行分析。 |
| 支持对HTTP协议的异常元素、异常参数、非法编码和解码的灵活控制与处理。 |
| 支持针对主流Web服务器及插件的已知漏洞防护。Web服务器应覆盖主流服务器：apache、tomcat、IIS、weblogic等；。 |
| 支持对注入、XSS、SSI指令、Webshell防护、路径穿越及远程文件包含的攻击防护。 |
| 支持CSRF（跨站请求伪造）防护。提供配置界面截图。 |
| 支持爬虫防护，实现对100种以上的爬虫特征进行识别和阻断，防止页面因爬虫而引起信息泄露等问题。 |
| 支持盗链防护，有效识别网页盗链行为，避免用户网页资源被滥用。 |
| 支持扫描防护。 |
| 支持Cookie安全机制。提供配置界面截图证明。 |
| 支持敏感关键字自定义功能。 |
| 支持URL ACL。对多种HTTP方法执行访问控制，包括：GET、POST、HEAD、PUT、DELETE等。 |
| 支持TCP Flood防护和HTTP Flood防护。提供配置界面截图证明。 |
| 智能攻击者锁定 | 可配置攻击者识别策略和算法  可配置将攻击者直接加入网络黑名单  可展示攻击者发生的时间和攻击者终端信息。 |
| 防御动作 | 针对触发安全规则的行为进行阻断并发出告警页面；  能将攻击者列入网络黑名单进行网络阻断该IP的访问；  对攻击报文丢弃。 |
| 日志与报表要求 | 根据产生的安全日志进行智能分析，提高人工分析效率，减小规则误判概率。 |
| 支持基于时间、IP、端口、动作、事件类型、URI、方法等条件的日志查询。 |
| 支持在安全日志中带有客户端真实IP地址，便于IP溯源。提供配置界面截图证明。 |
| 支持日志分时段导出、全部导出或者清空。提供配置界面截图证明。 |
| 管理功能要求 | 支持标准SNMP trap和Syslog接口。 |
| 支持与时间服务器同步。提供配置界面截图证明。 |
| 能对账户进行安全策略配置，包括口令复杂度和口令生存期。提供配置界面截图证明。支持超时重新认证机制并能够定义用户认证尝试的最大允许失败次数  支持SSL的Web界面、SSH、Console、WebShell多种方式 |
| 投标方资质 | 投标方应具备足够的信息安全服务技术实力及安全服务保障能力，获得中国信息安全测评中心颁发的信息安全服务一级资质证书。  说明：要求提供有效证书的复印件 |
| 产品资质 | 投标产品应具有中华人民共和国公安部颁发的《计算机信息系统安全专用产品销售许可证》，提供有效证书的复印件。 |
| 投标产品应具有中华人民共和国国家版权局颁发的《计算机软件著作权登记证》，提供有效证书的复印件。 |
| 投标产品应该是经过市场考验的成熟产品，产品上市时间不少于4年。须提供销售许可证或软件著作权证书等有效证明材料。 |
| 产品成熟度要求 | 投标产品应该是被广泛应用的成熟产品，在国内市场具有较高的市场份额。 |
| 投标产品应该是经过市场考验的成熟产品，产品上市时间不少于4年。须提供销售许可证或软件著作权证书等有效证明材料。 |

**4.2网络安全威胁检测与智能分析系统详细技术要求**

|  |  |  |
| --- | --- | --- |
| 类别 | 参数 | 功能及技术描述 |
| 硬件  指标 | 系统平台 | 系统应为机架式独立IPS硬件设备，全内置封闭式结构，具有完全自主知识产权的专用安全操作系统，稳定可靠。 |
| 网络接口 | 2个USB接口，1个RJ45串口，1个GE管理口，4个千兆电口，4个千兆光口，2个万兆口。 |
| 产品  性能 | 吞吐量 | 三层吞吐量≥8Gbps,应用层吞吐量≥4Gbps |
| 最大并发TCP会话 | 最大并发连接≥200万 |
| 每秒新增TCP会话 | 每秒新建会话数≥5万。 |
| 类别 | 参数 | 功能及技术描述 |
| 入侵  检测  和  高级  威胁  防护 | 入侵检测 | 系统应提供覆盖广泛的攻击特征库，可针对网络病毒、蠕虫、间谍软件、木马后门、扫描探测、暴力破解等恶意流量进行检测和阻断，攻击特征库数量至少为5000种以上。须提供界面截图。 |
| 系统应支持多种抗逃避检测技术 |
| 系统应提供入侵行为特征的自定义接口，可根据用户需求定制相应的检测和阻断规则。 |
| 系统应能够有效抵御SQL注入等多种常见的应用层安全威胁 |
| DoS/DDoS | 系统应提供DoS/DDoS攻击防护能力，支持TCP/UDP/ICMP/ACK Flooding，以及UDP/ICMP Smurfing等常见的DoS/DDoS的攻击 |
| 支持基于阈值和自学习检测 |
| 高级威胁防护 | 支持独立的web攻击特征库、应用识别库、IPS漏洞攻击特征库、敏感信息防泄漏特征库、僵尸网络特征库和URL库，提供服务器异常告警功能。须提供界面截图。 |
| 系统应提供关键文件保护功能，能够识别、阻断通过自身的关键文件，以防止非法外传行为。能识别的关键文件类型应包含至少以下几类：文档类如Excel、PDF、Word等，压缩文件类如CAB、GZIP、RAR、ZIP、JAR等，图像类如BMP、GIF、JPEG等，音频视频类如MP3、AVI、MKV、MP4、MPEG、WMV等，脚本类如BAT、CMD、WSF等，程序类如APK、DLL、EXE、JAVA\_CLASS等。须提供界面截图。 |
| 系统应提供基于信誉的僵尸网络防护能力，具备可以持续升级的信誉库，IPS通过信誉库内的恶意网站IP、C&C服务器地址的信誉值执行相应的防护动作。 |
| 系统应提供URL分类库，提供中英文网页过滤数据库，实现高风险、不良网站过滤。 |
| 系统应提供在线病毒检测和阻断能力。 |
| 带宽  优化 | 应用识别 | 系统应能识别主流的应用程序，识别种类不少于3000种。须提供界面截图。 |
| 流量分析 | 系统应支持全面的流量分析功能，可察看网络实时流量，包括：流量协议分布、流量IP分布、自定义察看某种流量TOP10、常见流量TOP10等；同时应支持生成日、周和月的流量报表，以便了解一段时间的流量情况。 |
| 流量管理 | 系统应提供灵活的流量管理功能，可以根据用户、应用、目的IP地址、时间及带宽等因素，实现基于应用、面向对象的流量保护策略。通过流量许可和优先级控制，阻断一切非授权用户流量，并结合最小带宽保证、最大带宽限制、会话限制和每IP设置等功能，有效保证关键应用全天候畅通无阻。须提供界面截图。 |
| 响应  能力 | 攻击响应 | 系统应提供丰富的响应方式，包括：会话阻断、IP隔离、邮件通知等功能，满足用户各种响应需求。 |
| 高可  靠性 | BYPASS方案 | 系统网络接口应具备内置fail-open特性，产品出现故障时，能自动转变成通路，不影响业务流量的正常传输。 |
| 系统应支持外置BYPASS硬件设备，扩展形成完整的BYPASS解决方案 |
| 系统支持软件BYPASS功能，系统软件故障时，系统自动实现旁路保护，避免网络中断等事故的发生。 |
| 设备自身安全性 | 投标设备应支持热插拔的冗余双电源，避免电源硬件故障时设备宕机，提高设备可用性。 |
| 系统各组件之间应采用加密安全通道进行通讯，防止窃听，确保整个系统的安全性。 |
| 日志  和  报表 | 日志管理 | 系统应支持日志缓存，在网络通讯中断的情况下，网络引擎先将检测到的攻击行为保存在本地，等网络恢复正常后再自动同步到管理平台，不会因网络断开而丢失日志信息。 |
| 系统应具备实时的日志归并功能，可以根据用户需要，按照告警事件的源/目的IP、事件类型等信息，对告警日志执行归并，有效抵御告警风暴。 |
| 系统应提供基于告警设备、时间、IP地址、事件类型、用户身份等条件的日志检索功能，具备日志备份、清除和恢复功能。系统应具备递归查询功能，在查询结果中再次输入查询条件获得更详细的查询结果，进行细粒度分析。 |
| 统计分析告警 | 系统应提供统计分析告警功能，针对告警事件能够按照攻击事件、危险程度等条件进行绝对值统计分析和环比统计分析并产生告警，告警参数应支持用户自定义。提供遭受攻击最多服务器、攻击类型分布、攻击最多来源IP、服务器安全说明、服务器安全分析等内容服务器安全报表须提供界面截图。 |
| 自定义分布统计模型 | 系统应提供自定义分布统计模型功能，可自定义实时分布统计中的数据类型，实现灵活的数据展现和统计分析。须提供界面截图。 |
| 报表系统 | 系统应提供丰富的报表功能，支持TopN事件、TopN源地址、TopN目的地址、TopN服务、事件类型分布与趋势、危险程度分类统计与趋势、风险级别统计与趋势以及交叉报表等多种报表模板；为便于分析，还应支持用户自定义报表模版，能够按照用户需求生成各种风格的统计报表。 |
| 系统应提供定时自动发送报表功能，支持在指定的时间内将生成的报表以html、excel、pdf等通用格式通过邮件发送给指定的管理员，以减少日常维护工作量。须提供界面截图。 |
| 管理  功能 | 管理方式 | 系统应提供基于Web的远程GUI管理，可以在任何IP可达地点，以简单、直观的方式完成策略配置、警报查询、攻击响应、集中管理等各种任务。 |
| 系统支持带外管理（OOB）功能，可以通过专用管理口，进行NIPS引擎管理。 |
| 系统应提供标准snmp trap（V1、V2、V3）和syslog接口，可接受第三方管理平台的集中事件管理。 |
| 系统监控 | 系统应具备系统运行状态监控功能，能够实时查看CPU使用率、内存使用率、磁盘剩余空间、系统运行时间、接口状态、流量等信息。 |
| 系统应具备系统健康状态异常告警机制，能够实时监控系统CPU、内存等关键部件的状态，并在发现异常状况时通过声音、邮件、短信等多种方式及时通知管理员。要求告警触发条件可设置。须提供界面截图。 |
| 升级功能 | 系统应提供多种升级方式，至少提供自动在线升级、离线升级两种方式 |
| 投标厂商应承诺至少每月定期升级攻击特征库，遇到重大安全事件，提供即时升级。厂商官方站点需同时提供升级包下载页面，并提供详细的升级事项说明。 |
| 部署  能力 | 部署模式 | 系统应支持旁路及串行两种工作模式，能够快速部署在网络环境中。 |
| 产品  成熟  度证  明 | 上市时间 | 投标产品应该是经过市场考验的成熟产品，产品上市时间不少于4年。须提供上市销售许可证或软件著作权证书等有效证明材料。 |
| 市场占有率 | 投标产品应该是被广泛应用的成熟产品，在国内市场具有较高的市场份额。 |
| 市场荣誉 | 投标产品应该是被认可的成熟产品，如获得国、内外奖项可提供相应证明。 |
| 产品资质 | 投标产品应具有中华人民共和国公安部颁发的《计算机信息系统安全专用产品销售许可证》，提供有效证书的复印件。 |
| 投标产品应具有中华人民共和国国家版权局颁发的《计算机软件著作权登记证》，提供有效证书的复印件。 |
| 投标方  实力  证明 | 投标方资质 | 投标方应具备足够的信息安全服务技术实力及安全服务保障能力，获得中国信息安全测评中心颁发的信息安全服务一级资质证书。  说明：要求提供有效证书的复印件 |

**四、技术服务**

1、投标方投标时必须有原厂针对本项目授权书原件，售后服务承诺函，无原厂授权书取消投标资格，原厂商直接投标不需要。货到现场必须由原厂工程师验货确认后，方可上架安装。

2、投标方在所做标书内必须提交针对本次设备购置的详细技术方案，必须承诺中标后，在施工前了解神华宁煤集团的网络状况并提交详细的施工组织方案，待方案通过后，严格按照施工组织方案进行施工，不得无故延误工期。

3、投标方必须承诺现场施工期间及售后服务时由有相关证书的工程师安装调试设备，不得派遣无资格证书的人员。

4、投标方必须具有独立的法人资质。投标方必须具有中国信息安全测评中心颁发的信息安全服务一级资质，注册资金在1000万以上，具有三个以上的同类同规模工程业绩。

5、投标方所提供的设备是必须是国产设备，如果设备外包装损坏或设备外壳损坏投标方必须无条件更换设备。

6、投标方对所投产品的扩展能力做详细说明。

7、实施期间，中标方负责系统的综合调试，在系统上线运行一个月内对设备性能进行压力测试，并出具满足招标文件要求的性能测试报告。须对一切与合同有关的供货设备及技术接口、技术服务等问题负全部责任。凡与合同设备相连接的其它设备装置及软件，中标方有提供接口和技术配合的义务，所发生的费用已包含在投标报价中，招标方不承担中标价格以外的任何费用。

8、投标方应承诺：合同签订后，如招标方需追加购置合同清单内的设备及其附件，所提供的设备及其附件的价格不高于合同价格。

9、培训

投标方应对招标方指定人员提供系统使用、维护等方面的免费培训,培训所需的培训、交通、食宿等各项费用均由中标方承担，培训的时间招标方和中标方共同商议。详细要求如下：

9.1、在不影响施工进度的情况下，中标方应该在安装调试过程中为招标方的技术人员进行现场培训，使招标方的技术人员掌握设备使用技术。培训时间为2-3天，培训费、场地由中标方解决。

9.2、提供中标设备的原厂培训4人7天CISP的培训，往返交通、食宿费、培训费等全部费用由中标方承担。

10、售后服务

1）投标方对所提供的设备应提供原厂保修服务，保修期为3年，保修期从安装上架开机运行时计算。在保修期内，投标方应无偿并迅速更换非人为因素损坏的整机设备和相关配件，并解决因软件及操作等产生的相关问题。

2）投标方应提供保修期以后的维保办法及维保报价。

3）在接到设备故障通知后，投标方应在1小时内做出响应，及时进行提导并提供解决方案，如需要上门维护必须在24小时以内到达现场。