**招标公告**

业务编号：ZB/SC2022-RG186

一、招标项目内容、技术要求、计划招标时间等

（一）招标项目名称：网络安全设备采购

（二）招标采购数量：1套

（三）技术要求：详见《网络安全设备技术参数要求》，并符合国家、行业最新标准规范，满足需方现场要求。

（四）计划招标时间：2022年7月上旬（具体以招标说明书为准）

（五）报名截止时间：2022年6月28日

（六）其他：无

二、对投标单位的资质要求：

（一）具有独立法人资格或其他组织的中间商（成立一年以上）。

（二）具有独立法人资格或其他组织的生产厂家。

（三）需提供原厂项目授权书及售后服务承诺函。

三、拟签订合同主要条款

（一）交货结算方式：货到招标单位指定地点，初步验收合格入库，投标单位按招标价格开具13%增值税专用发票，发票挂账60天后招标单位以银行承兑汇票滚动支付货款。支付低于六个月承兑或银行转账时按需方财务规定收取资金占用费，需方开具6%增值税发票。产品价款的10%作为质保金，质保金在供方如约履行完毕“供方对质量负责的条件和期限”约定义务的情况下，于质保期满双方无异议后返还供方，质保金不计息。

（二）交货必须附产品合格证，持入库凭证到萍乡萍钢安源钢铁有限公司安源片物资仓库验收。

四、意向投标人提交的资格证明文件

（一）资质材料：

1.营业执照副本复印件、开户许可证复印件，如有生产许可证、体系认证证书、特种设备制造许可证等一并附上。

2.法定代表人和代理人身份证复印件及法定代表人授权委托书（授权书必须有法人章或签字及加盖公章）、承诺书。

3.投标单位开票信息。

4.原厂项目授权书及售后服务承诺函。

上述资料需加盖报名单位公章。

提交方式：发送邮件至agqhb@pxsteel.com，发邮件时请注明邮件主题名称：XXXX公司报名网络安全设备采购项目招标资质文件。网上报名如不按此要求发送邮件，招标方对邮件遗失所造成的后果不负任何责任。

五、投标方式

招标单位对意向投标单位提交的资质材料进行审查，向审查合格单位发出招标说明书，请接到招标说明书的单位按要求时间交纳相应投标保证金（30000元）、投标报名费（500元）等。中标单位的投标保证金自动转为履约保证金，履约保证金按标的金额的5%收取，多退少补。未中标单位的投标保证金在宣标后十五个工作日内一次性返还（无息）。开票信息如下：

账户名称：萍乡萍钢安源钢铁有限公司

开户行：中国建设银行股份有限公司萍乡湘东支行

账号：36001752010052504776

六、招标方信息

（一）招标单位名称：萍安钢铁设备材料公司

（二）招标项目业务负责人及联系方式：彭海春18870993466

（三）设备材料公司监督电话：李先生 0799-6356077

（四）审监法务部监督电话：王先生 0799-6356116

萍乡萍钢安源钢铁有限公司

公告时间：2022年6月20日

**[法人代表](http://www.so.com/s?q=%E6%B3%95%E4%BA%BA%E4%BB%A3%E8%A1%A8&ie=utf-8&src=wenda_link" \t "_blank)授权书**

**萍乡萍钢安源钢铁有限公司**：

是中华人民共和国合法企业，法定地址：

法定代表人 特授权 代表我公司全权办理针对贵公司网络安全设备采购招标活动（业务编号：ZB/SC2022-RG186）的投标、谈判、签约等具体工作，并签署全部的有关文件、协议及合同。

我公司对被授权人的签名负全部责任，本授权书有效期：2022年6月20日至2023年6月19日。

在撤销授权的书面通知之前，本授权书一直有效。被授权人签署的所有文件（在授权书有效期内签署的）不因授权的撤销而失效。

被授权人签字： 授权人（签章或签字）：

[身份证号](http://www.so.com/s?q=%E8%BA%AB%E4%BB%BD%E8%AF%81%E5%8F%B7&ie=utf-8&src=wenda_link" \t "_blank)： [身份证号](http://www.so.com/s?q=%E8%BA%AB%E4%BB%BD%E8%AF%81%E5%8F%B7&ie=utf-8&src=wenda_link" \t "_blank)：

职务： 职务：

电话： 电话：

单位名称：（公章）

签署日期：2022-6-20

**承诺书**

**萍乡萍钢安源钢铁有限公司：**

我司自愿参与网络安全设备采购项目（业务编号：ZB/SC2022-RG186）的投（议）标，现承诺如下：

一、我司将遵循公平、公正、公开及诚实信用的原则参加本项目投（议）标，理解并接受贵公司的开标、评标、定标等相关规定。

二、我司按本项目招（议）标公告要求提供的所有法人资料及有关材料均真实有效、合法持有，不存在失效、虚假的情况。

三、严格遵守贵司的有关规定，投（议）标中不围标、不串标、不泄标，以及不排挤其他投标人参与公平竞争。

四、在本项目投（议）标有效期之内不撤回投标，中标后在贵司规定的期限内签订合同，全面履行合同义务。

若违反上述承诺内容，我司自愿接受贵司处理（如：取消投标中标资格、没收[投标或履约保证金](http://zhidao.baidu.com/search?word=%E6%8A%95%E6%A0%87%E4%BF%9D%E8%AF%81%E9%87%91&fr=qb_search_exp&ie=utf8" \t "_blank)），并承担由此造成贵司的经济损失赔偿及法律责任。

承诺单位（公章）：

法定代表人或委托代理人（签名）：

日期： 2022年6月20日

**网络安全设备技术参数要求**

一、网络安全设备技术参数要求

以下主要产品必须提供原厂项目授权书及售后服务承诺函原件

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **序号** | **设备名称** | **参考**  **型号** | **设备参数** | **数量** | **单位** | **备注** |
| **1** | 容灾备份一体机 | MSBK3012 | 1.四路机架式软硬件一体化架构，集备份管理软件，备份服务器和备份存储于一体，无需配置独立备份服务器，无需配置外置备份存储；  2.支持一台设备备份多个服务器，且能够在资源范围内接管多个业务。  3.基于Linux64位系统(非Windows或Unix)的专用容灾备份存储设备，减少病毒感染机率，确保系统稳定。  4.配置≥4颗Intel Xeon Gold 6330H @2.0GHz，24核处理器或以上系列；内存≥512GB；≥4个千兆以太网电口、≥2个万兆以太网光口（含多模模块）；实配≥2块480GBSSD、≥30块2.4TB10KSAS硬盘；  5.实配：备份软件一套（含≥50TB软件授权许可）；不限备份客户端数量，不限数据库备份数量，支持Vmware、华三等国内外主流虚拟化平台无代理备份。配置整机备份/裸机恢复模块，配置重复数据删除模块,配置LAN-Free备份模块；  6.支持主流的数据库备份恢复，包括但不限于Oracle、SQLServer、MySQL等主流数据库应用。  7.提供对文件、操作系统、数据库、应用软件、虚拟化的备份保护。  8.应急接管和容灾演练的虚拟机，均可通过备份设备的WEB页面直接进行图形化的管理，无需安装任何插件，包括开机、断电、重启、远程控制等功能。  9.支持写缓存镜像技术，写缓存能够临时留存CPU高速计算生成的临时数据；  10.支持在线备份Oracle的redolog和archivelog，提供准实时的数据保护和精准的任意时间点恢复，RPO≈0的安全防护能力，RTO＜15分钟的快速恢复功能；支持Oracle日志解析，可以界面化展现Oracle事务中的SCN和具体事务操作，并选择准确的SCN号来确定数据恢复点。通过日志解析获取事务具体操作的SQL语句，实现在线创建事务日志撤销作业，需提供功能截图。  11.支持LAN、WAN、SAN、IP-SAN、FC-SAN等各种系统架构  12.针对系统的高危操作（如：恢复作业、清理备份集等）前要求输入四位或以上的随机数字验证码，待验证通过后才能执行操作，防止人为误操作危害数据，需提供功能截图。  13.本次含设备含安装实施服务，提供3年原厂软硬件质保。  14. 3年7\*24小时服务 | 1 | 套 | 用于容灾备份  推荐品牌：爱数，鼎甲 |
| **2** | 企业版杀毒软件 | 终端安全管理系统V2.0企业版 | 1.控制中心，多级中心，全网威胁趋势展示，终端管理，查杀任务管理、全网日志、远程控制管理、外设管理、全网终端防火墙统一调度策略，文件分发，消息通知等。  2.病毒查杀，操作系统损坏或破破坏修复，文件实时监控，宏病毒查杀，病毒启发式扫描，恶意程序或行为监控，U盘保护及禁用，下载保护，邮件监控，系统加固，恶意软件安装拦截，浏览器保护，自动黑客入侵拦截并告警，本机对外攻击检测，恶意网站拦截，远程桌面登录二次防护，本身外设备管控（可禁用或强制启用），全网终端防火墙可通过控制台统一管理，可下发防火墙策略进行IP协议控制，IP黑名单，终端登陆二次验证，可统一下发指令对终端右键管理，垃圾清理，文件粉碎，弹窗广告拦截，启动项管理，网络流量管理，漏洞自动修复，文件分发，消息通知。  3.软件升级(\*3年); | 300 | 点 | 用于windows服务器及重要岗位计算机  推荐品牌：火绒，360 |
| **3** | 核心交换机 | H3C-S7506E-X | 1.交换容量≥153Tbps，包转发率≥36000 Mpps；  2.整机业务槽位≥6个，独立交换网板，双主控，双电源，双风扇；  3.以太网接口可配置千兆电口，千兆光口，万兆光口、万兆电口、40G接口、100G接口；可扩容防火墙、IPS、LB、SSL VPN插卡；  4.采用正交设计，业务板卡与交换网板采用完全正交设计(90度)，跨线卡业务流量通过正交连接器直接上交换网板，背板走线降低为零；  5.多虚一技术(N:1)，最大可达到4框虚拟化技术，此次实现2框虚拟化技术；  6.配置双主控，双电源，满配交换网板，≥48个千兆电口，≥24个千兆光口，≥16个万兆光口；两根3米万兆堆叠线，6个万兆单模光模块，24个千兆单模光模块；  9.能与现有核心交换机进行堆叠；  10. 提供三年原厂质保服务。 | 1 | 台 | 用于容灾备份机房  推荐品牌：H3C，华为 |
| **4** | 堡垒机 | TopSAG | 1.1U,6个千兆电口，2个千兆光口，1个console口。2个扩展槽位,200资源授权，用户数不限制；运维管理系统永久授权； 2.采用物理旁路部署，不改变现有网络结构；支持双机部署，保证系统发生故障时的可用性；支持自建集群部署：支持无缝横向扩展，轻松应对高并发需求； 3.支持用户的增删改查、锁定、激活，进行用户全生命周期管理，支持用户批量导入和导出；支持用户清理功能 4.支持系统管理员、保密管理员、密码管理员、安全审计员、保密员、运维管理员、操作员七种角色，同时也可按需分配角色权限，权限间相互制约； 5.支持资源分类和资源系统类型管理：内置常见资源分类和资源系统类型，可自定义添加资源分类、资源系统类型和资源服务类型； 6.支持对已添加的设备账号进行密码托管，从而实现单点登录功能；自动对数据库、Windows、Linux等设备进行账号改密，改密支持手动和定期任务，密码配置支持全局策略和手工指定，密码复杂度支持按策略随机生成； 7.支持按照用户、用户组、资产、资产组、管理协议、资产账号进行一对一、一对多、多对一、多对多授权；支持会话、指令、剪切板上下行、文件上传下载的约束行为；支持对用户/IP/mac地址/登录时间进行控制； 8.支持内置工单运维，操作员可根据工作需求临时申请设备运维工单，管理员审批后可直接运维，过期失效；支持对运维时间、运维地址、运维操作指令、操作行为的限定，触发策略后进行告警、再审、阻断等； 9.支持地址、时间、指令单独组配置，进行批量管理；支持访问SSH、RDP、Telnet、FTP、SFTP、VNC、数据库等资产；支持无须记忆多个设备账号和密码，实现账号密码代填功能；支持自动、半自动、手动三种登录方式；支持进行协议/工具扩展； 10.支持字符协议SSH、TELNET和文件传输协议FTP、SFTP的协议审计，审计详细的操作指令及操作录像，同时可根据每条指令快速定位其操作录像；支持通过应用发布实现数据库操作的命令级审计和图形审计的双重审计效果；自动对Windows、Linux等设备进行账号改密，可设定周期性改密； | 1 | 台 | 用于运维管理  推荐品牌：深信服，天融信，奇安信 |
| **5** | 日志审计 | TopAudit | 1.1U,7个千兆电口,日志采集处理速度≥5000EPS，包含≥50个日志源授权。≥16G内存；≥250G SSD 系统盘；数据存储容量≥4T；提供三年原厂质保服务； 2.支持安全设备、网络设备、中间件、服务器、数据库、操作系统、业务系统等不少于26类300种日志对象的日志数据采集；支持Syslog、SNMP Trap、Netflow、JDBC、WMI、FTP、SFTP、SCP、文件等方式进行数据采集；支持通过Agent采集日志数据 3.基于时间轴展示数据分布，能够通过时间轴进行查询分析。 4.支持日志归一化处理，将不同设备所产生的不同格式的难以理解的日志数据进行统一格式化处理，提炼出有用信息清晰、明确的展示给管理者；支持日志转发给第三方系统平台，支持设置多个日志转发IP地址，支持转发格式化日志或仅转发原始日志； 5.支持查询结果快速统计，可自定义统计主题规则，支持将多个主题添加为一个统计任务，以分、时、周、月、年定时执行自动统计，将统计结果报表发送到指定邮箱； 6.内置系统运行相关告警规则，包括检测到新日志源、节点掉线、主动日志源长期不外发日志、存储上限告警、主机认证失败等，可启用/禁用规则；支持安全告警概况、安全告警趋势的统一展示，实时告警可根据级别、规则类型等进行分类； 支持邮件、Snmp Trap、声音、声光、短信、一信通响应、数据库响应等多种告警方式，支持报警内容引用字段变量参数。 7.系统内置上百种报表模版，支持自动实现智能报表创建，每添加一个日志源，系统自动分析日志源类型进行相应报表创建，无需人工干预，报表和资产一一对应； 8.支持按照日志源名称、IP地址、日志源类型、接受时间及状态等维度对日志源列表进行排序； 9.支持为日志源指定类型、名称、IP地址、收集节点、收集方式、以及日志源启停状态等属性信息；支持以业务角度将日志源进行分组，支持在日志查询时以业务组进行查询，支持在首页拓扑展示时以业务组进行展示； 10.支持基于拓扑图的日志源相关数据信息快速查看；支持通过拓扑下钻查看对应日志源的日志、报表、告警数据。 | 1 | 台 | 用于日志审计保留  推荐品牌：深信服，天融信，奇安信 |
| **6** | web应用防火墙（WAF） | TopWAF | 1.1U,6个千兆电口， 2个千兆光口,单电源,2个扩展槽位,应用层吞吐≥500M，网络层吞吐≥3.5G，并发连接≥90万，含3年产品特征库升级许可。 2.采用专用硬件架构与安全操作系统，基于操作系统内核的完全检测技术；产品为专业性 Web 应用安全防护系统硬件设备，而非下一代防火墙\UTM 类设备集成的 WEB 防护功能模块。 3.支持虚拟线接入，无论任何网络环境可强制数据从一个接口转发到另一个接口，支持提取客户端真实IP头；自动尝试匹配X-Forwarded-For, X-Real-IP, Cdn-Src-Ip 用以获取真实客户端IP。 4.支持HTTP/HTTPS站点防护，在代理模式下支持HTTPS流量解析，支持SSL卸载功能。支持网络层访问控制，支持基于源IP 地址、目的IP 地址、源端口、目的端口、协议类型及目的区域、地理区域等条件的访问控制。 5.支持应用层访问控制功能，针对 HTTP请求字段进行过滤，包括HTTP协议版本，请求方法，Cookie信息等。支持多重编码检查功能，可对多重的编码均进行安全防御检查，有效防止攻击绕过WAF。 6.支持对文件的上传下载进行控制，包括上传及下载最大文件大小、文件扩展名、MIME类型等进行控制；支持对上传文件内容进行病毒检测的功能。支持DDoS攻击动态黑名单功能，检测到DDoS攻击将其攻击源自动加入黑名单。 7.Web界面直观查看WAF扩展卡、接口状态、接口流量、管理口、HA口及业务口的运行状态。支持对防护的WEB服务器进行健康检查，可以实时监测服务器的活跃状态，并且可定期备份健康记录。 日志支持以syslog和welf两种格式向远端日志服务器发送日志，日志传输可加密，且管理员可以配置加密密码。 8.针对攻击日志，可对任意一条编辑其行为动作，包括阻断记录日志、阻断不记录日志、继续、警告、临时或永久跳转到某一重定向页面等动作。 9.支持集中管理功能，管理中心支持节点信息监控，节点管理，节点策略配置等功能，方便客户日常运维。 10.支持双机热备，包括主备、主主负载均衡、连接保护等模式。支持两台WAF配置同步，包括全局同步和策略同步两种同步方式。支持同一台WAF上下接口状态联动(一个接口down另外一个接口也同步down) 。 | 1 | 台 | 对外应用，web映射防护  推荐品牌：深信服，天融信，奇安信 |
| **7** | 漏洞扫描 | TopScanner 7000 | 1.1U,6个千兆电口，2个千兆光口，1个console,冗余电源,2个扩展槽位,2个USB口，≥16G内存，≥1T硬盘，50个域名扫描，并发扫描3个Web扫描任务，并发扫描5个系统扫描任务，并发扫描80个IP地址，含1年规则库升级许可，支持分布式部署。 含3年综合漏扫规则库升级许可 2.支持扫描主流操作系统、Web服务器、数据库、网络主机、移动设备、应用及软件的安全漏洞；支持限制webui、ssh、telnet方式登陆最大并发管理数，超出限额时，处理策略可选提示不能登陆和踢掉最不活跃的用户 3.支持首页全面展示风险分布及趋势图表，包括主机风险分布、站点风险分布、漏洞风险分布、漏洞top10、资产风险值趋势、资产风险分布趋势 4.支持扫描系统漏洞数量大于140000种，web漏洞数量大于2200种,数据库大于2500种，CVE漏洞数大于60000，产品漏洞库应涵盖目前的安全漏洞和攻击特征，漏洞库具备至少CVE、CNCVE、CNVD、BUGTRAQ、CNNVD编号； 5.登录扫描支持ssh、smb、snmp、esxi、mysql、db2、postgresql、mssql、ftp、imap、pop3、pop2、rsh、rexec、rlogin、smtp、telent、gbase、dmdb、oracle等类型； 6.支持DB2、FTP、IMAP、MSSQL、MYSQL、Oracle、POP3、POSTGRES、RDP、Redis、RTSP、SMB、SMTP、SNMP、SSH、TELNET、TOMAT等的弱口令探测 7.支持站点组、单站点风险在线报表和站点特有属性配置站点信息包含但不限于：代理、认证、访问策略、爬取策略、指纹选项等信息 8.支持自定义路径，对有爬取限制链接进行深度扫描，添加指定的站点url，便于爬取到更多的页面；支持排除后缀名，可自定义无需爬取的文件后缀名，即引擎爬虫不对如下特定的链接爬取 9.主机报表支持展示主机风险、漏洞信息，及主机详细的端口信息、端口Banner信息、安装软件信息、操作系统类型；支持扫描任务中自动生成报表，包含html、pdf、word、excel、wps等多种格式类型，可通过设置邮箱自动发送 10.支持在线报表，可详细展示任务**综述**信息、站点列表、漏洞列表、对比分析及参考标准，漏洞分布支持风险等级过滤查看 | 1 | 台 | 用于内网漏洞扫描  推荐品牌：深信服，天融信，奇安信 |
| **8** | 机柜 | 42U服务器机柜 | 尺寸：宽600mm，深1000mm，高2055mm。 | 2 | 件 | 用于放置备份一体机和核心交换机 |
| **9** | 辅材 |  | 千兆网线、光纤跳线、PUD插座等 | 1 | 批 |  |