**青岛新闻网网站漏洞扫描、IPS设备招标文件**

**（招标文件编号：QDXWW2013006）**

青岛新闻网络传播有限公司

2013年11月4日

**目录**

[第一部分 招标邀请 3](#_Toc355340798)

[第二部分 投标须知 4](#_Toc355340799)

[第三部分 投标文件 8](#_Toc355340800)

[第四部分 投标内容与要求 11](#_Toc355340801)

[第五部分 技术方案、服务及培训计划承诺 13](#_Toc355340802)

[第六部分 报价 15](#_Toc355340805)

[第七部分 投标函格式 18](#_Toc355340808)

[第八部分 资格证明文件要求 19](#_Toc355340809)

[第九部分 保密条款 22](#_Toc355340810)

[第十部分 评标方法 23](#_Toc355340811)

# 第一部分 招标邀请

青岛新闻网络传播有限公司（简称‘青岛新闻网’）本次对漏洞扫描、IPS设备进行项目招标，邀请有意参加本次招标活动的投标人参与本项目，项目招标采用综合评议法的方式。

一、招标项目: 漏洞扫描设备、IPS设备（两台）。

二、发放标书方式：

在青岛新闻网首页本站公告

三、集中答疑时间

时间：2013年11月4日至2013年11月8日。

商务：68873527

技术：82933899

四、邮箱报名

请发送邮件对本项目进行报名登记，若供应商未对本次项目进行报名则不参与招标：请同时发送到2个邮箱

3527@qingdaonews.com

wzp@qingdaonews.com

五、投标截止时间：2013年11月8日下午13：30。

六、开标时间：2013年11月8日下午14:00。

七、开标地点： **青岛市南软件园5号楼6层**

# 第二部分 投标须知

投标方在投标之前必须认真阅读本招标书所有内容，按照本招标书的要求编制投标文件。投标文件应当对本招标文件提出的实质性要求和条件做出响应。投标方因未能遵循此要求而造成的对本招标书要求投标方所提供的任何资料、信息、数据的遗漏或任何非针对招标书要求项目的报价均须自担风险并承担可能导致其标书被废弃的后果。招标文件对投标方有约束力。

定义：

货物——是指供应商按采购文件规定，向采购人提供**全新的、未使用过**的各种形态和种类的物品，包括原材料、燃料、设备、产品等。

服务——是指根据本采购文件规定，供应商必须承担的制造、运输、吊拉、安装、调试、技术协助、培训及其他各项义务。

综合评分法——是指在满足采购文件实质性要求的前提下，按照采购文件中的各项规定进行综合评审和打分，以综合得分最高的供应商为中标候选人或中标人的评审方法。

**一、投标费用**

投标方需承担与本投标有关的自身所发生的所有费用，包括标书准备、提交以及其他相关费用。无论投标结果如何，招标方不承担、分担任何相关类似费用。

投标企业在招标现场交纳2000元保证金，保证其投标被接受后对其投标书中规定的责任不得撤销或者反悔，招标结束后返还。

外聘评标专家2名，评标费（共1000元人民币）用由中标企业承担。

**二、招标文件**

本招标文件仅适用于本次招标中所叙述项目的招标。

招标文件的修改。在投标截止日期前，招标方可主动地或依据投标方要求澄清的问题而修改招标文件，并以电子邮件形式通知所有领取招标文件的每一投标方，投标方在收到该通知后应立即以邮件的形式予以确认。

为使投标方在准备投标文件时有合理的时间考虑招标文件的修改，招标方可酌情推迟投标截止日期和开标时间，并以电子邮件形式通知已邮件报名的每一投标方，投标方在收到该通知后应立即以邮件的形式予以确认。

招标文件的修改书将构成招标文件的一部分，对投标方有约束力。

**三、投标文件**

见第三部分。

**四、开标**

招标方按招标文件中规定的时间公开开标。

开标时，投标方须由法定代表人或其委托代理人（具有法定代表人签署的授权书）参加，并签到证明其出席开标会议。开标时，投标人应检查投标文件密封情况，并签字确认。

开标后，如招标人要求，投标人应对投标文件进行讲解说明，随时接受评标小组询问，并予以解答。投标方不到场讲解说明的，招标方有权宣布该投标方自动弃权。

开标后，唱标顺序随机顺序进行，招标方将组织审查投标文件是否完整，是否有计算错误，是否符合招标文件的实质性条款、条件和规定。若文字大写表示的数据与小写数字表示的有差别，则以两者较低数据为准，单价与数量乘积与合计有差别的以单价为准，投标方不得提出异议，否则招标方有权视为弃标。

如开标后发现废标致使有效投标少于两家，招标方有权宣布此次招标无效。

**五、评标**

评标小组由2名政府采购技术专家、1名新闻网技术人员、1名新闻网财务人员组成。

评标是招标工作的重要环节，评标工作在评标小组内独立进行。在投标、开标期间，投标人不得向评委询问情况，不得进行可能影响评标结果的活动。

在对投标文件进行详细评估之前，招标方将依据投标方提供的资格证明文件审查投标方。

投标文件的澄清。为了有助于对投标文件进行审查、评估和比较，招标方有权向投标方质疑，请投标方澄清其投标内容。投标方有责任按照招标方通知的时间、地点指派专人进行答疑和澄清。

评标小组通过标书对各投标方的报价、综合实力、技术方案、售后服务和其他内容进行比较，最终以各评委的算术平均分，确定商务与技术方案得分。

评标小组将遵照评标原则，公正、公平、公开地对待所有投标方，综合考虑各方面因素确定中标人。

**六、定标**

严格按照招标文件的要求和条件进行评标，择优定标，最终选择符合招标文件的要求，并且报价最合理，能提供最佳服务的投标者作为中标方。

评标小组不向落标方解释落标原因，不退还投标文件。

评标小组根据投标和评标情况，一次定标。

**七、中标通知与签订合同**

评标结束后，由招标方向中标方发送电子版中标通知书。

中标方按中标通知指定的时间、地点与青岛新闻网签订合同。招标方有权将投标中的有关约定体现在后期的商务合同中。

招标文件、中标方的投标文件及其澄清文件等，均为双方签订合同的依据。

中标方必须独立完成项目建设，不得分包。

在设备验收完成后，招标方支付合同总款的95%，余款作为质保金一年后支付。

# 第三部分 投标文件

**一、投标文件的组成和格式**

包括但不限于：

（一）商务部分

1、报价部分，见招标书第六部分；

2、投标资格证明文件，见招标书第八部分；

3、保密承诺，见招标书第九部分。

（二）技术部分

1、技术方案；

2、实施部署方案；

3、后期维护及培训。

4、设备配置清单

5、技术响应表

**二、投标文件的装订和密封**

投标方应将投标文件装订成册。

投标方应将投标文件总体密封后递交。

**三、投标文件的编写**

（一）投标方必须对本招标文件的每一项要求给予实质性的响应，否则其投标将被拒绝。投标方对本招标文件的每一项要求所给予的响应必须是唯一的，否则将视为不响应。

（二）投标语言及计量单位

投标文件及投标人和招标人就投标交换的文件和来往信件，应以中文书写。

除在招标文件的技术规格中另有规定外，计量单位应使用中华人民共和国法定计量单位（国际单位制和国家选定的其他计量单位）。

（三）投标函格式

投标人应完整地填写招标文件中的投标函格式和投标报价表及其附件，说明所提供的货物和服务、简介、来源、数量及价格和供货周期。

（四）投标人应得到货物制造厂家同意提供该货物的正式授权。

**四、投标文件的签署和印刷规定**

投标文件正本和所有的副本须打印并由投标方加盖公章并经法定代表人或其委托代理人（具有法定代表人签署的授权书）在正本上签字或盖章。

投标文件除签字外必须是印刷形式，其中不许有行间插字、涂改和增删，如有修改错漏处，必须由投标人加盖公章并经其法定代表人或其授权代表签字或盖章。

**五、投标文件的递交**

（一）投标文件的密封和标记

投标方应准备投标文件的正本一套，副本三套，在每一份投标文件上要明确注明“正本”或“副本”字样，一旦正本和副本内容有差异，以正本为准。投标文件如有电子版光盘文件应单独密封。

投标文件须加盖公章，所有投标文件均须加盖骑缝章（公章）。投标文件须密封，并在密封袋加盖公章。

（二）投标文件的递交

投标方将投标文件进行密封和标记后，按投标邀请函注明的地址在投标截止时间之前专人送至招标方。招标方将拒绝接受投标截止时间后提交的投标文件。

# 第四部分 投标内容与要求

经过前期调研市场，我们针对每种设备选择如下品牌：

漏洞扫描设备： 绿盟 网神

IPS设备： TippingPoint 绿盟 启明星辰

**漏洞扫描设备参数**

|  **指标** | **指标项** | **规格要求** |
| --- | --- | --- |
| 设备基本要求 | 硬件及软件 | ★采用专用硬件架构与专用安全操作系统。 |
| 网络接口 | 100M电口接入 具备专用管理口 |
| 授权 | 授权可扫描至少1500个独立IP或独立域名 |
| 处理能力 | 扫描性能 | 平均扫描速度大于10IP/分钟，并发60IP扫描 |
| 支持对多个扫描任务并发执行，支持多任务自动调度；单个任务允许扫描的最大扫描范围不小于一个B类网段 |
| 漏 洞 检 测 能 力 | 能够扫描发现网络设备，服务器以及防火墙中的安全漏洞。对网络设备和操作系统网络层漏洞的扫描在不更改任何的配置和安装任何类似探针的软件，也不需要提供任何的访问权限的情况下正常工作 |
| 可以在扫描过程中人工指定包括http、Ftp、SNMP、SMB等常见协议的登陆口令，登陆到相应的系统中对特定应用进行深入扫描 |
| 内置不同的策略模板，如针对Unix、Windows服务器，便于用户定制扫描策略。用户可定义扫描范围，扫描策略 |
| 漏洞知识库漏洞信息大于2800条，提供详细的漏洞描述和对应的解决方案描述；漏洞知识库与国际CVE标准兼容，并提供CVE Compatible证书；漏洞知识库和漏洞检测规则支持手动升级和自动升级，支持本地升级和在线升级，在线升级支持代理方式升级；至少每两周进行一次定期升级 |
| 支持常见的操作系统漏洞扫描：AIX、BSD、HP-UX、Linux、MacOS、Solaris、UNIX、Windows、Centos等；支持数据库漏洞扫描：MS SQL Server、Oracle、DB2、Mysql、PostGreSQL等支持网络设备漏洞扫描：Cisco、H3C、防火墙等★能够扫描常见的网络安全客户端软件（网络防病毒Symantec、TrendMicro、McAfee）的安全漏洞能够扫描常见的应用软件漏洞（如IE浏览器、MSN、Mozilla Firefox、MS Office、多媒体播放器和各种P2P下载软件）的安全漏洞。★需具备对VMware主流虚拟化管理软件的漏洞扫描能力。★产品需支持Linux系统下的本地登录扫描功能。 |
| ★支持WEB应用漏洞扫描，提供多种Web应用漏洞的安全检测，如SQL注入、跨站脚本、网站挂马、网页木马、CGI漏洞等。支持Javascript解析引擎，能从Javascript代码中分析出url，支持自定义Cookie进行深入检测，支持基于basic、NTLM、Cookie等认证方式的Web应用系统安全扫描 |
| ★支持和微软WSUS补丁系统的联动，能够在发给主机管理员的邮件中附带自动配置WSUS的注册表文件，方便进行自动化的补丁修补 |
| ★提供扫描占用网络带宽控制措施，并请描述具体实现技术和带宽占用指标。 |
| 日志及管理 | 支持被扫描系统的资产管理，可采取多种方式自动发现网络资产的信息，并能够结合资产管理的情况进行扫描和分析。能够对已有资产进行查阅和管理，可以手工增加新的资产信息，能够把资产管理和组织结构或者网络拓扑结构紧密结合；支持IP地址、域名和资产树等多种资产管理方式；支持通过Excel文件将地址导入到资产树功能；能够通过形象的图示将资产的风险值和的风险等级直观地展现出来，并且能够将节点、风险及对应责任人相关联。 |
| 能够定制临时、周期性扫描任务自动扫描网段，找出系统或配置上的漏洞和不安全因素。 |
| 支持高级数据分析，能够进行历史数据查询、汇总查看、对比分析等，方便进行多个扫描任务或多个IP风险对比，能够在多个历史任务中，很快的检索到需要关注的资产IP点 |
| 支持管理通知，扫描任务运行结束时向指定电子邮箱地址发送邮件通知 |
| 支持在线、离线报表，对综述、主机、漏洞、趋势等信息进行分类显示；支持HTML、EXCEL、WORD格式输出报表 |
| 扫描报告中应包括针对发现的安全漏洞的详细说明、补救方法步骤、补丁文件的互联网下载连接、以及国际安全组织关于该漏洞的说明或连接 |
| 服务 | 具备当地技术支持机构，本地具备2名以上的原厂工程师，能够提供本地化快速服务响应及支持 |
| 企业资质、相关标准及相关规范 | 提供资质证明的有效复印件。 |
| 厂商需有自己的专业安全漏洞研究团队，能够独立发现Microsoft、CISCO等国际著名厂商的重大安全漏洞，并自行跟踪、维护安全漏洞库。 |

**特殊说明：投标公司必须出具厂家针对此项目的授权。**

**IPS设备招标参数（1）**

|  **指标** | **指标项** | **规格要求** |
| --- | --- | --- |
| 设备基本要求 | 硬件及软件 | ★采用标准机架式硬件架构，冗余双电源。 |
| 链路、接口 | ★至少提供2路千兆电口防御，独立管理接口，支持光口扩展，支持Bypass，保证业务不中断。最大支持16路防御 |
| 吞吐量、处理能力 | ★吞吐量>=2Gbps，最大并发Tcp连接数200万，每秒新建连接数>=6万，时延<100us |
| 其他要求 | ★设备须支持IPv6/IPv4双协议栈功能，能同时辨识IPv4和IPv6通讯流量。支持IPv6环境下攻击检测技术和基于IPv6地址格式的安全控制策略。 |
| IPS相关功能 | 入侵检测引擎具备融合模式匹配、协议分析、异常检测、会话关联分析，以及抗IDS/IPS逃逸等多种技术，准确识别各种黑客入侵，为用户提供2~7层深度入侵防御。 |
| 支持IP碎片重组、TCP流重组、流量状态追踪，基于智能、深入的协议分析，能够有效检测运行在非标准端口的协议、木马，以及基于Smart Tunnel（智能隧道）的应用协议；能够适应不同的网络环境，支持VLAN 802.1Q、BGP、MPLS、QinQ、PPPOE等特殊封装协议。支持非对称路由环境下攻击检测。 |
| 设备应具备融合模式匹配、协议分析、异常检测、会话关联分析，以及抗IDS/IPS逃逸等多种技术，准确识别各种黑客入侵，为用户提供2~7层深度入侵防御。事件分析功能要求采用高级模式匹配、协议分析、异常检测、会话关联分析技术对网络数据进行分析，具备碎片重组、TCP流重组、统计分析能力；具备分析采用躲避入侵检测技术的通信数据的能力，采用基于行为分析的检测技术，对零时差攻击能够很好防范。具备协议自动识别功能，具备规则用户自定义功能，可以对应用协议进行用户自定义，可对110余种协议进行详细的字段解码匹配。 |
| ★设备应提供覆盖广泛的攻击特征库，能够针对2800种以上的攻击行为、异常事件，以及网络资源滥用流量，进行检测和防御。系统携带的攻击特征库须获得CVE-Compatible兼容性认证 |
| 在保障合法应用正常运转的前提下，提供对网络病毒、蠕虫、间谍软件、木马后门、刺探扫描、暴力破解等恶意流量的检测和阻断；具备基于“漏洞保护”的虚拟补丁功能，融合协议异常检测能力，有效抵御缓冲区溢出攻击以及各类未知攻击；设备应具备零日攻击防护能力；有效抵御SQL注入、D.o.S、僵尸网络等多种常见的应用层安全威胁 |
| 设备应提供先进的DoS/DDoS攻击防护能力，支持双向阻断TCP/UDP/ICMP/ACK Flooding，以及UDP/ICMP Smurfing等常见的DoS/DdoS的攻击。主动防御CC等应用层DoS攻击，能够阻挡或限制未经授权的应用程序触发的带宽消耗。 |
| ★支持web信誉功能，持续评估、分析国内网站，一旦嵌有恶意程序的网站出现，保护用户的访问不受侵害，有效拦截Web威胁，恶意web站点库每周更新，要求不小于50万的恶意站点库，需提供产品配置截图和官方升级页面截图。要求设备生产厂商是云安全联盟（CSA）成员，恶意站点库与国际同步。 |
| ★设备应能识别超过700种的各类网络应用，至少应包括：商业系统类应用、协作类应用、互联网应用、媒体类应用等。须提供界面截图。设备应支持灵活的应用管理策略配置功能，实现基于IP地址、用户、时间、应用等多维度的全面、细致监控。设备应支持细粒度的自定义应用功能，支持的参数至少应包括：搜索范围、数据传输方向、特征数据等。为实现精确匹配，必须支持与、或等逻辑运算。须提供界面截图。 |
| 支持基于对象的虚拟系统（VIPS），针对不同的网络环境和安全需求，制定不同的入侵防御规则和响应方式，实现面向不同对象的智能化入侵防御。 |
| 日志管理及报表 | 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。并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。 |
| ★具备用户身份识别能力，支持基于用户身份进行策略配置、日志记录与查询；支持自动与手动获取用户信息列表并生成组织结构图。须提供界面截图。 |
| ★针对访问网络资源的终端用户，系统应提供增强的身份认证功能，支持RADIUS、LDAP、AD域等接口，及第三方认证平台，实现更灵活、更安全的认证控制。须提供界面截图。 |
| 具备自定义报表功能，支持交叉统计和多元组合查询详细事件，支持导出WORD\EXCEL\PDF \HTML 等常用公文处理格式 |
| ★设备应具备地址簿功能，在报表中直观显示IP地址所处国家、地区或某个部门。支持自定义私有IP地址库和导入外部公网IP地址库。须提供界面截图。 |
| 支持规则的在线升级和离线升级、自动升级和手动升级。要求每周至少一次规则更新，提供官方升级页面截图。 |
| 基于B/S的管理架构，灵活方便，适合在任何IP可达地点远程管理，Web界面支持 IE、FireFox、chrome等主流浏览器；支持基于C/S架构的“安全中心”管理，提供图形用户界面，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控制台或日志数据库中，不会因网络断开而丢失日志信息。 |
| 服务 | 提供3年的硬件保修及软件免费升级服务。 |

**特殊说明：招标要求中标注“★”的部分为必须满足项，投标公司必须出具厂家针对此项目的授权。**

**IPS设备招标参数（2）**

|  **指标** | **指标项** | **规格要求** |
| --- | --- | --- |
| 设备基本要求 | 硬件及软件 | ★采用标准机架式硬件架构，冗余双电源。 |
| 链路、接口 | ★至少提供4路千兆电口防御，独立管理接口，支持光口扩展，支持Bypass，保证业务不中断。 |
| 吞吐量、处理能力 | ★吞吐量不小于1Gbps，最大并发Tcp连接数150万，每秒新建连接数>=4万，时延<100us |
| 其他要求 | ★设备须支持IPv6/IPv4双协议栈功能，能同时辨识IPv4和IPv6通讯流量。支持IPv6环境下攻击检测技术和基于IPv6地址格式的安全控制策略。 |
| IPS相关功能 | 入侵检测引擎具备融合模式匹配、协议分析、异常检测、会话关联分析，以及抗IDS/IPS逃逸等多种技术，准确识别各种黑客入侵，为用户提供2~7层深度入侵防御。 |
| 支持IP碎片重组、TCP流重组、流量状态追踪，基于智能、深入的协议分析，能够有效检测运行在非标准端口的协议、木马，以及基于Smart Tunnel（智能隧道）的应用协议；能够适应不同的网络环境，支持VLAN 802.1Q、BGP、MPLS、QinQ、PPPOE等特殊封装协议。支持非对称路由环境下攻击检测。 |
| 设备应具备融合模式匹配、协议分析、异常检测、会话关联分析，以及抗IDS/IPS逃逸等多种技术，准确识别各种黑客入侵，为用户提供2~7层深度入侵防御。事件分析功能要求采用高级模式匹配、协议分析、异常检测、会话关联分析技术对网络数据进行分析，具备碎片重组、TCP流重组、统计分析能力；具备分析采用躲避入侵检测技术的通信数据的能力，采用基于行为分析的检测技术，对零时差攻击能够很好防范。具备协议自动识别功能，具备规则用户自定义功能，可以对应用协议进行用户自定义，可对110余种协议进行详细的字段解码匹配。 |
| ★设备应提供覆盖广泛的攻击特征库，能够针对2800种以上的攻击行为、异常事件，以及网络资源滥用流量，进行检测和防御。系统携带的攻击特征库须获得CVE-Compatible兼容性认证 |
| 在保障合法应用正常运转的前提下，提供对网络病毒、蠕虫、间谍软件、木马后门、刺探扫描、暴力破解等恶意流量的检测和阻断；具备基于“漏洞保护”的虚拟补丁功能，融合协议异常检测能力，有效抵御缓冲区溢出攻击以及各类未知攻击；设备应具备零日攻击防护能力；有效抵御SQL注入、D.o.S、僵尸网络等多种常见的应用层安全威胁 |
| 设备应提供先进的DoS/DDoS攻击防护能力，支持双向阻断TCP/UDP/ICMP/ACK Flooding，以及UDP/ICMP Smurfing等常见的DoS/DdoS的攻击。主动防御CC等应用层DoS攻击，能够阻挡或限制未经授权的应用程序触发的带宽消耗。 |
| ★支持web信誉功能，持续评估、分析国内网站，一旦嵌有恶意程序的网站出现，通过独特的防护技术保护用户的访问不受侵害，有效拦截Web威胁，恶意web站点库每周更新，要求不小于50万的恶意站点库，需提供产品配置截图和官方升级页面截图。要求设备生产厂商是云安全联盟（CSA）成员，恶意站点库与国际同步。 |
| ★设备应能识别超过700种的各类网络应用，至少应包括：商业系统类应用、协作类应用、互联网应用、媒体类应用等。须提供界面截图。设备应支持灵活的应用管理策略配置功能，实现基于IP地址、用户、时间、应用等多维度的全面、细致监控。设备应支持细粒度的自定义应用功能，支持的参数至少应包括：搜索范围、数据传输方向、特征数据等。为实现精确匹配，必须支持与、或等逻辑运算。须提供界面截图。 |
| 支持基于对象的虚拟系统（VIPS），针对不同的网络环境和安全需求，制定不同的入侵防御规则和响应方式，实现面向不同对象的智能化入侵防御。 |
| 日志管理及报表 | 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。并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。 |
| ★具备用户身份识别能力，支持基于用户身份进行策略配置、日志记录与查询；支持自动与手动获取用户信息列表并生成组织结构图。须提供界面截图。 |
| ★针对访问网络资源的终端用户，系统应提供增强的身份认证功能，支持RADIUS、LDAP、AD域等接口，及第三方认证平台，实现更灵活、更安全的认证控制。须提供界面截图。 |
| 具备自定义报表功能，支持交叉统计和多元组合查询详细事件，支持导出WORD\EXCEL\PDF \HTML 等常用公文处理格式 |
| ★设备应具备地址簿功能，在报表中直观显示IP地址所处国家、地区或某个部门。支持自定义私有IP地址库和导入外部公网IP地址库。须提供界面截图。 |
| 支持规则的在线升级和离线升级、自动升级和手动升级。要求每周至少一次规则更新，提供官方升级页面截图。 |
| 基于B/S的管理架构，灵活方便，适合在任何IP可达地点远程管理，Web界面支持 IE、FireFox、chrome等主流浏览器；支持基于C/S架构的“安全中心”管理，提供图形用户界面，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控制台或日志数据库中，不会因网络断开而丢失日志信息。 |
| 服务 | 提供3年的硬件保修及软件免费升级服务。 |

**特殊说明：招标要求中标注“★”的部分为必须满足项，投标公司必须出具厂家针对此项目的授权，否则按废标处理。**

要求：

**1、带星号的指标必须满足，否则视为无效投标。**

**2、设备要求提供原产三年质保服务，厂家初始安装服务。**

**3、合同签署后一个月内应到货，否则合同失效。**第五部分 技术方案、服务及培训计划承诺

投标方根据招标文件要求及自身情况，就项目的售后服务进行承诺，承诺书须盖章，承诺内容包括但不限于以下几点：

一、对用户的人员培训；

二、系统出现故障的响应（响应方式、时间、费用负担）；

三、提供3年原厂质保服务。(★)

四、其他服务优惠措施

### 技术响应表

单位全称（公章）： 包号：

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 采购文件要求 | 投标文件响应 | 偏离情况 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

注：供应商应根据投标设备的性能指标、对照采购文件要求在“偏离情况”栏注明“正偏离”、“负偏离”或“无偏离”。

全权代表签名： 日 期：

### 设备配置清单

单位全称（公章）： 包号：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 设备名称 | 品牌 | 规格型号 | 性能及指标 |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

注：1、必须后附原厂印制的产品彩页等图片介绍资料

2、必须有产品技术性能及加工设备、工艺的详细描述

全权代表签名： 日期：

# 第六部分 报价

本部分描述了对投标方报价的要求，招标方已制定标准格式的报价表，投标方应特别加以注意。

一、所有投标均须按给定的清单格式以人民币报价，不接受企业自行制定的报价格式；

二、投标单位应按招标单位提供的要求及资料，计算项目的总价。因发生错误造成的损失由投标方自行承担，如果招标方发现了计算错误会要求投标方澄清；

三、项目的报价必须是唯一的(★)；

四、总报价及单价允许打折扣。但必须在相应的表中表达清楚，必要时应加以说明；
 五、除另有规定，投标报价应包括设备、劳务、管理、材料、运输、安装、维护、保险、利润、税金、政策性文件规定的所有风险、责任等各项应有费用；

六、投标价格采用价格固定方式，投标单位所填写的单价和合价在合同实施期间不因市场变化因素而变动。投标方自行考虑材料涨价风险；

七、投标方如需用外汇购入某些投标物，须折合人民币计入报价中。

### 开标一览表

 项目名称： ；

|  |  |  |
| --- | --- | --- |
| **序号** | **费用名称** | **报价（元）** |
| 1 | 设备仪器费 |  |
| 2 | 运输费 |  |
| 4 | 税费 |  |
| 5 | 其他费用（列明细） |  |
| 总计 |  |
| 6 | 供货期 |  |
| 7 | 质保期 |  |

供应商名称（盖公章）：

供应商法定代表人或被授权代表：（签字）

时间： 年 月 日

### 投标报价明细表

单位全称（公章）： 标项：

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 序号 | 设备名称 | 品牌 | 规格型号 | 单位及数量 | 单 价（元） | 总 价（元） |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  | …… |  |  |  |  |  |
|  | 专用耗材 |  |  |  |  |  |
| 设备仪器费合计 | 小写： |
| 大写： |

注：该表格中的“设备仪器费合计”必须与附件13：《开标一览表》中的“设备仪器费”相等。

全权代表签名： 日 期：

# 第七部分 投标函格式

**致：青岛新闻网**

根据贵方关于漏洞扫描、IPS设备招标的有关文件，我公司作为投标方正式授权 （姓名和职务）代表我公司参加贵公司组织的漏洞扫描、IPS设备招标，并为此：

1、按照贵方招标文件要求提交下述文件正本一份，副本三份：

商务文件；

技术文件；

2、遵守贵方招标文件和我方投标文件中所有规定和承诺；

3、向贵方提供与本项目招标相关的一切数据、情况和技术资料；

4、如我公司中标，将严格按照招标文件、投标文件及双方签定的合同履行义务。

投标单位： （公章）

法定代表人：（签字或盖章）

日 期： 年 月 日

# 第八部分 资格证明文件要求

**一、投标方应具备以下资格:**

（一）具备独立法人资格（营业执照、税务登记证明等）；

（二）注册资金不低于贰佰万元人民币(含贰佰万)，具有良好的财务、资金状况；

（三）投标人须提供完善的本地化售后服务（青岛市辖区外注册的投标人开标时须提供青岛地区直属分支机构营业执照副本原件或青岛地区售后服务协议原件）。

**二、投标方应提供以下资格证明文件:**

（一）营业执照复印件；

（二）税务登记证复印件（含国税、地税）；

（三）证明投标人是合格的，厂商对该项目的授权书；

（四）同类项目：投标人提供的与本次采购相同类别的业绩合同；业绩合同、中标通知书及验收单。

（六）投标函、投标单位资格声明、资格声明函；

（七）其他相关资质。

**三、授权委托书（格式）**

 公司授权 （被授权人的姓名、职务）为本公司的合法代理人，代表本公司参加抗DDos攻击、SSL VPN接入、堡垒机设备招投标，并以本公司名义处理一切与之有关的事务。

本授权书有效期为 年 月 日起至 年 月 日止，特此声明。

法人代表签字盖章：

职 务：

单位名称：

地 址：

代理人（被授权人）签字盖章：

职 务：

单位名称：

地 址：

**四、公司基本情况介绍**

1、企业从事售前售后服务的人员力量投入情况；

2、企业管理体系；

**五、供应商同类项目实施情况一览表**

单位全称（公章）：

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 采购单位名称 | 设备或项目名称 | 采购数量 | 单价 | 合同金额（万元） | 附件页码 | 采购单位联系人及联系电话 |
| 合同 | 验收报告 |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
| 备注 | 须提供供应商同类项目合同复印件、验收报告及采购中标通知书。 |

法定代表人签字：　　　　　 时 间：

**六、资信及商务响应表**

单位全称（公章）： 标项：

|  |  |  |  |
| --- | --- | --- | --- |
| 项目 | 采购文件要求 | 是否响应 | 供应商的承诺或说明 |
| 售后服务保障要求 |  |  |  |
| 备品备件及耗材等要求 |  |  |  |
| 质保期 |  |  |  |
| 交货时间及地点 |  |  |  |
| 付款条件 |  |  |  |
| 质量管理、企业信用要求 |  |  |  |
| 能力或业绩要求 |  |  |  |

全权代表签名： 日期：

# 第九部分 保密条款

一、非经招标方书面许可，不得将本文件及技术需求说明书的任何内容透露给招标方以外的第三方；

二、非经招标方书面许可，中标方不得将因项目获得的所有信息拷贝或透露给招标方以外的第三方；

三、投标方必须针对以上保密条款书面承诺，并在投标文件商务方案中说明。

# 第十部分 评标方法

本次评标采用综合评分法，评标委员会成员综合评定各投标人提交的投标文件，由评标委员会根据评分标准进行打分，确定中标人。（后附评分标准）

综合评分法，是指在能够满足招标文件实质性要求的前提下，按照招标文件中规定的各项因素进行综合评审打分后，技术得分为去掉最高和最低分后的平均值，评标委员会将确定评标总得分最高的投标人为中标候选人或者中标人的评标方法。

综合评分法的评分因素、分值（各项因素分值之和为100分）：

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|

|  |  |  |
| --- | --- | --- |
| 项 目 | 分数 | 评 分 办 法 |
| 商务部分50分 | 投标报价 | 40 | 对招标文件做出实质性响应的所有合格投标人中的最低报价作为本次评标的评审基准价。投标价等于评审基准价的得满分值40分，其他投标人的价格得分按下面的公式计算：W=（Cmin/C）×A，其中W-投标人的投标报价得分总值；Cmin-评审基准价；C-投标人的有效投标报价；A-标准权分数（40分）。备注：投标人报价超出采购预算的,其投标报价得分为0分。 |
| 项目经验 | 10 | 自2010年1月1日至今（以合同签订日为准）完成的同类项目，每提供一项得2.5分；开标当日需提供合同原件，未提供原件不计分。（投标文件中须同时附相应材料的复印件） |
| 技术部分50分 | 产品品质 | 10 | 设备选型及产品综合质量等级要求的前提下，必须满足国家、行业的相关规定，通过比较产品性能、品牌、声誉度、产品稳定性、维护成本等各方面因素，由评标委员会成员根据投标文件的情况酌情打分。满分为10分：a.优级〈产品技术成熟、质量可靠、市场占有率前三名〉10-8分；b.良级（产品技术较为成熟、质量较可靠、市场占有率较高[4至10名]及有一定品牌知名度）：7-5分；c.一般级（产品技术、质量均可靠、有市场占有率及品牌）：4-1分。 |
| 技术方案 | 25 | 根据投标人对招标文件技术指标的响应程度，包括所投设备性能指标、参数、数量等，由评标委员会成员根据投标文件的情况酌情打分。满分为25分：a.满足及优于采购要求的得16-25分；b.有较少负偏离但不构成实质性偏离/偏差的得7-15分；c.有较大负偏离即构成实质性偏离的得1-6分。 |
| 施工组织措施 | 5 | 工期安排合理得0.75分，工序衔接合理得0.75分，进度控制点设置合理得0.5分，质量安全保证体系完善得0.5分，施工方案合理先进得0.5分，应急组织方案合理先进得0.5分，劳动力组织均衡得0.5分，工期安排、工序衔接、进度较合理的得1分。 |
| 售后服务方案 | 10 | 根据在青岛地区售后服务机构设置与常驻售后服务人员配备情况（投标文件中须附相关材料证明）及投标人售后服务措施、质保期限承诺、售后服务等情况，由评委酌情打分，满分7分，3年保修服务外，每增加一年免费保修得3分。无厂家授权0分 |
| 合 计 | 100 |  |

 |