常州市教育科学研究院内部采购
询价通知书

项目编号：常教科内采询[2020]03号

项目名称：网站安全防护服务

常州市教育科学研究院

2020年6月

根据常州市教育科学研究内部采购规范，现对 2020 年度网站安全防护服务项目进行询价采购。特邀请符合条件的供应商参加。

一、采购项目内容及技术要求

项目编号：常教科内采询[2020]03 号

项目名称：网站安全防护（服务类）

采购预算：9.2 万元

采购需求：（后附）

二、资格条件

1.具备《中华人民共和国政府采购法》第二十二条规定的条件。

2.投标产品（服务）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》，所投产品必须为云安全、云防护类，提供复印件并加盖原厂公章；

3.投标人须具有稳定的技术服务团队和完善可靠的售后服务体系，能提供及时有效的本地化服务；

三、询价响应文件的组成及要求

（一）文件组成：

1.承诺函；（后附格式）

2.报价表；（后附格式）

3.企业营业执照及税务登记证副本复印件；

4.法定代表人身份证明复印件；（委托代理时提供法定代表人授权委托书及委托代理人身份证明复印件；）（后附法定代表人授权委托书格式）

5.响应产品配置或技术参数响应对照表；（后附格式）

6.售后服务承诺；

7.与本次询价有关的其他资料；

上述材料为必备材料，如有缺项为无效响应。

（二）文件的签署和密封要求：

1.询价响应文件为正本一份、副本一份，需装订成册；

2.询价响应文件中复印件材料需加盖公章；

3.询价响应文件须装袋密封，封口处须加盖单位公章，封面应注明采购项目编号、项目名称、采购人和响应单位名称，联系人，联系电话等。

四、综合说明

1.本次询价采购，响应单位须对采购清单报出完整且唯一的总报价。报价包含所有设备的提供、运输、装卸、安装、调试、使用培训、售后服务等一切费用。以最低报价确定成交供应商。

2.响应单位提供的所有产品应符合技术要求条款中所标称的规格、参数和标准。

3.响应单位应保证商品为全新、未使用的符合质量标准（国家、行业、企业：依据——学校的需求）的合格品。

4.请贵单位按上述要求编制询价响应文件盖章密封，并于**2020 年 6 月 30 日 10:00 前**送交至常州市教育科学研究院（常州市紫荆西路 6 号 9 号楼 203 室）。未按询价文件组成要求制作报价文件并签署的或过时递交文件的，均为无效文件。本项目将于**2020 年 6 月 30 日 17:00** 前在 常州市教育科学研究院确定成交供应商。

5.成交原则：在符合采购需求、质量和服务相等且报价未超过采购预算的前提下，以提出最低报价的响应单位为成交供应商。若最低报价相同，则依次按技术指标高优先、质量保证期长优先、交货期短优先、故障响应时间短优先的顺序排列选择成交供应商。

6.成交供应商在成交公示期结束后，在三个工作日内与常州市教育科学研究院签订合同。

7.交付使用时间：按照甲方采购需求供货，在合同签定后5个工作日内调试并交付服务。

8.付款条款：在规定的时间内安装、调试并交付使用。竣工验收合格后支付全款。

9.联系方式

（1）采购人：常州市教育科学研究院

地址：常州市紫荆西路6号9号楼203室；联系人：许老师；联系电话：0519-86909117

10.该项目信息发布在常州市教育科学研究院网站（http://jky.czedu.cn）

五、询价合同主要条款

常州市教育科学研究院内部采购项目合同

（服务类）

采购方（甲方）：常州市教育科学研究院　　供应商（乙方）：

合同编号：常教科内采询[2020]03 号　　签定地点：常州市紫荆西路 6 号 9 号楼

签定时间：　　年　　月　　日

经常州市教育科学研究院 2020 年　月　日常教科院内采询[2020]03 号的询价结果，根据《中华人民共和国政府采购法》、《中华人民共和国合同法》等法律法规的规定，甲乙双方同意就网站安全防护服务按照以下条款和条件签定本合同（以下简称“合同”）:

1.合同内容：乙方负责提供下列服务　　单位：元

项号	服务内容	服务期限	价格	备注
				一年服务期满后双方若无异议可自动续签

2.合同价格：按此次成交价格执行

3.合同范围

包括了所有服务项目、有关材料、设施设备和相关技术资料。

4.权利保证

乙方应保证在为甲方提供该服务时不受第三方提出侵犯其专利权、版权、商标权或其他权利的起诉。一旦出现侵权，乙方应承担全部责任。

5.质量保证

乙方所提供的服务时间和质量应按国家有关部门最新颁布的相关标准及规范为准；

6.验收

（1）乙方应当在服务结束后规定时间内向甲方提出验收要求，甲方应在收到验收要求 15 个工作日内进行质量验收。

（2）服务的验收项目包括：服务时间、服务内容、服务规范和被服务对象满意度等；

（3）由于不可抗力而使服务内容和时间产生变化的，乙方应将相关凭证保存好，并在验收前统一提交给甲方。乙方不能提交相关凭证的，视为未按合同约定提供服务，由乙方负责限时补齐，因此导致逾期交付的，由乙方承担相关的违约责任；

（4）验收的标准：按国家相关标准、行业通行标准承诺执行。

7.付款

竣工验收合格后支付全款。

8.售后服务

乙方应按照国家有关法律法规规章和“三包”规定以及合同所附的“服务承诺”提供服务。

除上述规定外，还应提供下列服务。

（1）在合同规定的期限内对所提供服务项目实行定期回访；

（2）乙方接到甲方投诉后，应在按规定的服务水平和响应速度到达现场进行处理；

（4）除合同另有规定之外，由服务项目产生的衍生费用均已含在合同价款中，甲方不再另行进行支付；

9.违约责任

（1）合同一方不履行合同义务或者履行合同义务不符合约定的，应当承担继续履行、采取补救措施或者赔偿损失等违约责任。如果乙方未能履行合同规定的任何义务，甲方有权从履约保证金中取得补偿。

①甲方违反合同规定，无正当理由拒绝接受服务的，甲方向乙方偿付拒收合同款总值的百分之五违约金；

②乙方未按规定期限提供服务的，应与甲方协商，甲方仍需求的，乙方应立即提供相关服务并应按照逾期时间支付每天合同价万分之四的违约金，同时承担甲方因此遭致的损失费用；

③乙方不能提供服务（逾期超过五天视为不能提供服务）、提供服务不合格或不符合合同约定的，甲方有权解除合同，乙方返还甲方已支付款项，并向甲方偿付合同款总值的百分之五违约金，违约金不足以补偿损失的甲方有权要求乙方补足；因提供服务不合格或不符合合同约定的，乙方应在收到甲方发出解除合同通知之日起五日内，自行承担解除合同所引发的一切费用。甲方不承担因解除合同导致乙方产生的一切损失。

（2）乙方所提供的服务侵犯第三方的知识产权，乙方应向甲方支付已付货款部分百分之五违约金；导致甲方为此参与诉讼或仲裁，乙方另应支付甲方为此引发的律师费、诉讼费、调查费、差旅费等一切费用。

10.争议的解决

（1）因服务质量问题发生争议的，应当邀请国家认可的权威机构对服务质量进行鉴定。符合质量标准的，鉴定费由甲方承担；不符合质量标准的，鉴定费由乙方承担；

（2）因履行本合同引起的或与本合同有关的争议，甲、乙双方应首先通过友好协商解决，如果协商不能解决争议，向甲方所在地有管辖权的人民法院提起诉讼。

11.附加条款

本项目不得分包、转包，如有分包、转包，一旦查实甲方有权终止合同。

12.合同生效及其它

（1）合同经甲乙双方法定代表人签字（或盖章）并加盖公章（或合同章）后生效；

（2）本合同一经签订，甲乙双方不得擅自变更、中止本合同；

（3）除发生不可抗力情况或因法律、政策原因导致甲方不能履行合同外，甲乙双方不得放弃或拒绝履行合同。

（4）合同在执行过程中出现的未尽事宜，双方在不违背本合同的原则下协商解决，协商结果以书面形式盖章记录在案，作为本合同的附件，与本合同具有同等效力；

（5）合同正本一式贰份，具有同等法律效力，甲乙双方各执一份；

（6）本合同应按照中华人民共和国的现行法律进行解释。

采购方（甲方）

单位名称：常州市教育科学研究院

单位地址：常州市紫荆西路 6 号

法定代表人签字（或盖章）：

项目经办人签字：

联系电话：0519-86695189

供应商（乙方）

单位名称：

单位地址：

法定代表人签字（或盖章）：

委托代理人签字（或盖章）：

电话：

帐号：

开户行：

格式 1、报价表（格式）

报 价 表

项号	服务内容	服务期限	价格	备注

响应单位（盖章）：

联系人：

联系电话：

法定代表人（或委托代理人）签字：

日期：　　年　　月　　日

格式 2、承诺函（格式）

承 诺 函

致：_____（采购单位名称）

我方已仔细阅读了贵方组织的_____（项目名称）_____（项目编号：_____）的询价通知书的全部内容，现正式递交下述文件参加贵方组织的本次采购活动：

响应文件正本一份、副本一份。

据此函，签字人兹宣布：

1.我方同意自本项目询价通知书规定的响应截止时间起遵循本承诺函。

2.我方在此声明，所递交的响应文件及有关资料内容完整、真实和准确。同意应贵方要求提供与本响应有关的任何数据或资料。若贵方需要，我方愿意提供我方作出的一切承诺的证明材料。

3.我方承诺已经具备《中华人民共和国政府采购法》中规定的参加政府采购活动的供应商应当具备的条件：

（1）具有独立承担民事责任的能力；

（2）具有良好的商业信誉和健全的财务会计制度；

（3）具有履行合同所必需的设备和专业技术能力；

（4）有依法缴纳税收和社会保障资金的良好记录；

（5）参加政府采购活动前三年内，在经营活动中没有重大违法记录；

（6）法律、行政法规规定的其他条件。

4.我方对提供的标的物拥有完整的物权，并且负有保证第三人不得向贵方主张任何权利（包括知识产权）的义务。

5.如我方成交，我方承诺在收到成交通知书后，在成交通知书规定的期限内，根据询价通知书、我方的响应文件及有关澄清承诺书的要求与采购人订立书面合同，并及时缴纳履约保证金，按照合同约定承担完成合同的责任和义务。

6.我方已详细审核询价通知书，我方知道必须放弃提出含糊不清或误解问题的权利。

7.我方完全理解贵方不一定接受报价最低的供应商为成交供应商的行为。

8.我方将严格遵守《中华人民共和国政府采购法》第七十七条的规定，即供应商有下列情形之一的，处以采购金额千分之五以上千分之十以下的罚款，列入不良行为记录名单，在一至三年内禁止参加政府采购活动，有违法所得的，并处没收违法所得，情节严重的，由工商行政管理机关吊销营业执照；构成犯罪的，依法追究刑事责任：

（1）提供虚假材料谋取成交的；

（2）采取不正当手段诋毁、排挤其他供应商的；

（3）与采购人、其他供应商或者采购代理机构恶意串通的；

（4）向采购人、采购代理机构行贿或者提供其他不正当利益的；

（5）在招标采购过程中与采购人进行协商谈判的；

（6）拒绝有关部门监督检查或提供虚假情况的。

供应商（盖单位公章）：

法定代表人或其委托代理人（签字）：

地址：

电话：

传真：

邮政编码：

开户名称：

开户银行：

银行账号：

____年____月____日

格式 3、法定代表人授权委托书（格式）

法定代表人授权委托书

致：_____（采购单位名称）

本人____（姓名）____系____（供应商名称）____的法定代表人，现授权____（姓名和职务）____为我方委托代理人。委托代理人根据授权，以我方名义签署、澄清、说明、补正、递交、撤回、修改贵方组织的____（项目名称）____（项目编号：_____）项目的响应文件、签订合同和处理一切有关事宜，且委托代理人在参加该项目过程中的一切言行，视为法定代表人的意思表示，即视为供应商的意思表示，其法律后果由我方承担。

本授权书于_____年_____月_____日签字生效，委托期限：_____。

委托代理人无转委托权。

委托代理人在授权委托书有效期内签署的所有文件不因授权委托的撤销而失效，本授权委托书的有效期与委托代理人的代理期限一致。

供应商（盖单位公章）：

法定代表人（签字）：

法定代表人身份证号码：

委托代理人（签字）：

委托代理人身份证号码：

格式 4、产品配置或技术参数响应对照表（格式，可根据项目情况调整）

产品功能技术参数响应对照表

序号	功能名称	采购功能技术参数要求	响应产品功能技术参数描述	是否符合（填“符合”或“不符合”

响应单位（盖章）：

联系人：

联系电话：

法定代表人（或委托代理人）签字：

日期：　　年　　月　　日

采购需求

1、项目背景

为提升常州教育科学研究院数据中心网络应用系统安全防护水平，拟采购网站云安全防御平台服务，要求如下：

2. 技术需求

2.1 实现各类 WEB 攻击技术防护

通过云防御技术，将常州教育网站群纳入到云安全防御平台，防止来自于 Web 应用层的攻击，拦截常见的 Web 漏洞攻击、防止通过 Web 漏洞试图入侵服务器、危害用户等恶意行为，例如：SQL 注入、XSS 跨站、获取敏感信息、利用开源组件漏洞的攻击等常见的攻击行为。

同时，平台须可以提供 0Day，nDay 漏洞防护，当发现有未公开的 0Day 漏洞，或者刚公开但未修复的 nDay 漏洞被利用时，可以在发现漏洞到修复漏洞这段空档期对漏洞增加虚拟补丁，抵挡黑客的攻击，防护系统安全。

为了预防 Web 系统遭遇极端攻击（被植入后门）而导致攻破，平台需要有相关安全技术进行防护，当发现 Web 系统被攻破时，能够进行页面内容恢复。

2.2 对双向 SSL 的防护支持

云安全防御平台须可以防护HTTP应用系统，基于HTTPS的应用系统，在网络环境常规的设备无法识别传输的应用数据，识别来自应用层的攻击。平台需要能良好的支持HTTPS协议并能对SSL数据流进行中继，实现对HTTPS的全面支持。

2.3 多工作模式的支持

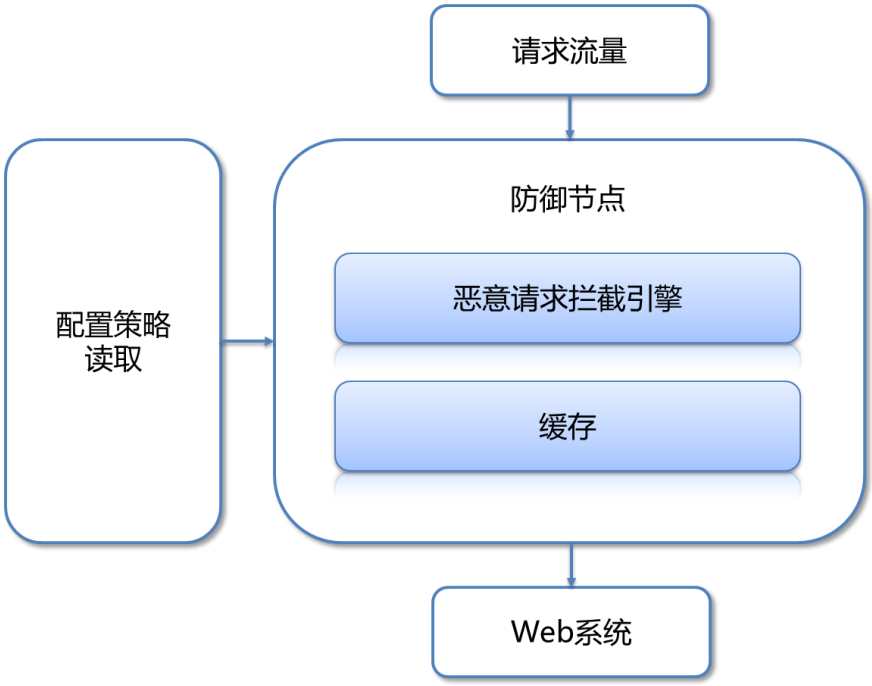
云安全防御平台须支持检测和阻断多工作模式随意调整切换的功能，在检测模式下，所有安全策略规则都只是对应用流量数据包进行检测，并告警，而不做任何阻断功能；在阻断模式下，所有的安全策略规则同时可以提供用户对单条规则的配置：阻断（默认）或者仅检测。管理员可以根据监控情况，实时进行调整。

2.4 智能 DNS

云安全防御平台须支持智能 DNS，智能 DNS 负责探查各节点状态，各个防御节点使用基于 DNS 的负载均衡，负载均衡依赖节点状态信息的汇报，根据现有负载自动调度的算法。防御节点需要每分钟会自动上报自身的运行状态信息，包括但不限于 CPU、内存、磁盘占用、Load 状态、内外网流量、HTTP 访问的 QPS 等。这些信息会被汇总，作为平衡节点负载的依据。DNS 调度时依据节点的配置不同，动态调整节点权重，从而引导流量。

2.5 防护信息同步

云安全防御平台须支持防护信息同步，平台可读取配置信息，恶意请求拦截引擎调用相应的检测模块（例如 CC 攻击检测、规则检测、智能攻击识别、各类访问控制模块等）对请求进行过滤，依据配置信息判断是否将请求转入缓存响应。同时防护节点需要定期获取云端的安全评级云内的高危 IP 信息，并加入相应的访问控制库，同步至本地防护节点。



2.6 规则防御

云安全防御平台须提供基于 HTTP 包检测规则匹配的传统防护方式，由代理服务器接收的 HTTP 请求/响应的双向流量均经过云安全防御平台的检测。主要包括一些常见 Web 漏洞防护，例如：SQL 注入、跨站脚本、代码执行、路径遍历等漏洞。同时还需要包括一些特殊漏洞的防护规则，可以第一时间发现 0day/1day 漏洞的爆发趋势并将其转化为防御规则，迅速响应并提供相应的虚拟补丁。从而节省了单台设备升级规则的时效性问题，极大缩短的安全空白期。

2.7 IP 访问控制

云安全防御平台须支持基于 IP 的访问控制对网站进行防护，可将内网的 IP 地址进行分类，我方业务系统管理员可根据来源 IP 进行访问控制。需要同样支持对某些安全 IP 地址通过白名单的方式允许其正常访问。

2.8 智能攻击识别

云安全防御平台须支持智能攻击识别，通常一些自动化工具会有一些相应特征，比如检测某些漏洞用的 Payload，Http 请求头部会增加特定字段。使用特定 Referer 或者 UA，访问指定路径。云安全防御平台可以通过检测 HTTP 信息基于行为和规则对访问者是否为自动化攻击工具进行识别，并屏蔽这些攻击。

2.9WebShell 防护

云安全防御平台须支持网站后门 WebShell 防护，WebShell 是指黑客攻击网站后为了长期控制在网站上放置的一些隐蔽的后门程序，可以通过 web 访问这些程序绕过传统防火墙的检测从而达到长期控制网站服务器的目的。这类后门通常有一定的页面特征，云安全防御平台支持通过相应的规则匹配，一旦发现有后门程序上传或者被访问，则对这些请求直接屏蔽。

2.10 协同防御

云安全防御平台须支持协同防御，云安全防御平台防护的网站内只要有一个网站遭受攻击，则攻击者 IP 将会被记录，并会被防护的所有网站所屏蔽。

2.11 关键资源防护

云安全防御平台须支持关键资源防护，云安全防御平台爬虫对我方指定的 URL 或者文件、图片等进行爬取，并将结果存入云安全防御平台缓存服务器内，一旦发现安全问题，则会立即用缓存原本的内容进行替换，确保网站发布内容的安全性。

2.14 撞库防护

云安全防御平台须支持撞库防护，“撞库”攻击是指的攻击者利用从其他网站窃取的真实用户名/密码，对网站实行批量化自动攻击。大多数用户密码无法做到一站一密，所以通过撞库可以获取大量窃用户资料。

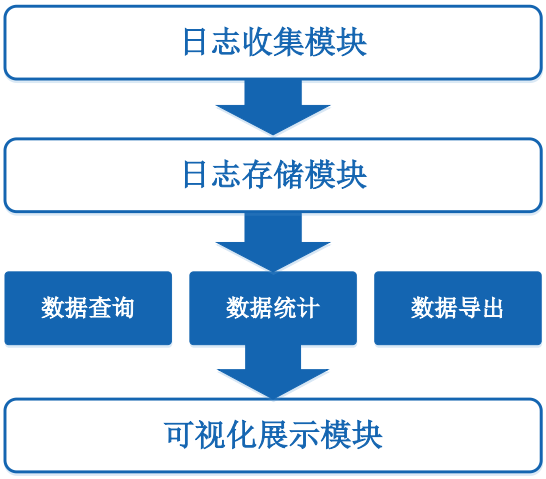
云安全防御平台须可基于攻击者对登陆请求的频率次数来判断是否发生撞库攻击，当检测判定为撞库攻击时，云安全防御平台可以屏蔽掉这类攻击来保证网站的数据安全。

2.15 后台防护

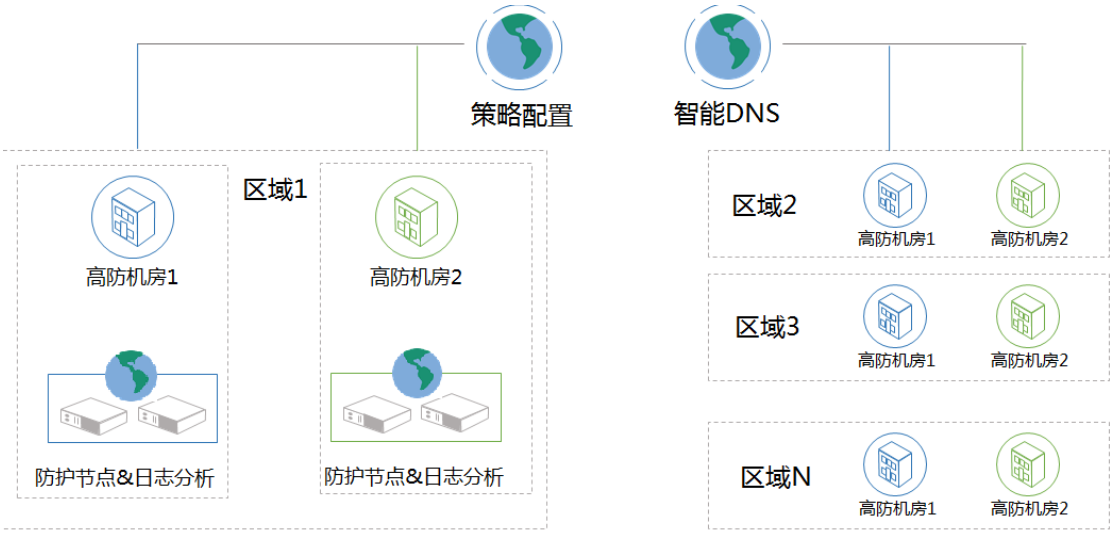
云安全防御平台须支持后台防护，一般攻击者可以利用一些后台猜解工具对网站后台地址进行搜索，云安全防御平台可基于 IP 和 URL 实现颗粒度较细的访问控制策略，对网站后台进行保护。并且需要我方可以自定义设置指定后台可访问的 IP。

2.16 数据存储

云安全防御平台须支持日志存储，并支持可视化展示，整体架构示意图：



2.17 网络设计



云安全防御平台网络设计示意图

云安全防御平台须支持通过 CNAME 或其他方式进行流量牵引。在我方网站群的 DNS 服务器上做 CNAME 别名解析，将网站别名指向云安全防御平台别名服务器，通过我方网站群的 DNS 服务器上的别名指向云安全防御平台的别名服务器，再由云安全防御平台的别名服务器负责分发至各个防护节点。

2.18 IPv6 攻击云防护

须支持在不改变网站既有配置情况下，无缝提供访客 IPV6 访问，提供截图证明；

提供 IPV6 DNS 解析服务，该 IPV6 DNS 具有抗 DNS DDoS 能力，提供截图证明；

提供 IPV6 攻击防护能力，可抵御常见得 WEB 攻击类型，提供截图证明。

2.19 网站安全加速服务(以 20TB 为单位报单价，本次采购数量为 1)

基于 CDN 的基础网络架构，可以通过缓存、压缩、智能 DNS 解析等方式提升访问速度，提供截图证明；

自动对未开启 Gzip 压缩的页面进行压缩，减少页面传输大小 90%以上，加快网页访问速度，提供截图证明；

将页面缓存到节点上让访客就近访问，提升网页访问速度，提供截图证明；

在浏览器中执行键盘操作刷新缓存，提供截图证明。

2.19 技术参数

1、提供 https 方式登录 Web 配置管理界面，并提供网站接入向导功能；
2、 提供基于 CDN 的基础网络架构，可以通过缓存、压缩、智能 DNS 解析等方式提升访问速度；
3、 提供自动对未开启 Gzip 压缩的页面进行压缩，减少页面传输大小 90%以上，加快网页访问速度；
4、 提供在浏览器中执行键盘操作刷新缓存；
5、 提供对 404 页面进行内容优化，提升用户体验、降低跳出率

6、 提供 Web 攻击行为防护功能，包括但不限于以下类型：SQL 注入、命令注入、跨站脚本、代码执行、路径遍历等；

7、 提供 IP 屏蔽功能，用户可对指定 IP 进行屏蔽，并设置屏蔽时长；

8、 提供自动化攻击工具及扫描器的智能识别功能，用户可自定义对扫描 IP 进行定时屏蔽；

9、 提供境外访问控制功能，用户可选择限制所有境外 IP 访问；

10、 提供关键资源保护功能，用户以 URL 形式自定义网站的关键资源，并对关键资源进行监控，一旦关键资源被篡改，立刻自动复原；

11、 提供防止攻击者上传、访问 WebShell 功能，用户可自定义对使用 WebShell 攻击或试图访问 WebShell 的 IP 进行定时屏蔽；

12、 提供按照访问时间防御的功能，用户可自定义时间段对关键资源进行监控，一旦关键资源被篡改，立刻自动复原；

13、 提供网站永久在线功能，即网站不能访问时，平台提供网站首页映像，访问者可以访问到首页；

14、 提供撞库防护功能，根据访问频率识别出攻击者的撞库行为，避免网站数据泄露；

15、 提供关键字过滤功能，检查网站内容，发现敏感信息、反动言论和淫秽内容自动替换，用户可自定义敏感关键词；

16、 提供防盗链功能，保护网站图片、压缩包等资源文件不被其它站点盗用；

17、 提供 HTTPS 网站防护功能，用户可自助上传 SSL 证书到防护服务器；

18、 提供特殊端口防护功能，用户可对网站的非 80 端口自助添加配置；

19、 提供网站访问情况信息展示功能，包括但不限于以下信息：请求数、总流量、网站浏览人数、搜索引擎引导量、遭受攻击次数等；

20、 提供网站被攻击情况信息展示功能，包括但不限于以下信息：攻击发生时间、攻击次数、攻击目标 URL、攻击 IP 及归属地、攻击类型等；

21、 提供攻击信息可视化展示功能，以地理坐标视图的方式实时展示攻击信息，包括但不限于以下信息：攻击源所在地，攻击目标域名，目标所在地、攻击次数、攻击类型等；

22、 提供良好的用户访问体验，平台在国内拥有不少于 30 个防护节点，且覆盖移动、电信、联通国内三大主流运营商，须现场登录平台管理后台展示证明；

23、生产厂商具备工信部颁发的中华人民共和国增值电信业务经营许可证（互联网接入服务业务、内容分发网络业务类）；

24、产品生产厂商为安全联盟成员单位；

25、投标产品具备公安部颁发的《计算机信息系统安全专用产品销售许可证》（云安全、云防护类）

26、支持在不改变网站既有配置得情况下，无缝提供访客 IPV6 访问，提供截图证明；

27、提供 IPV6 DNS 解析服务，该 IPV6 DNS 具有抗 DNS DDoS 能力，提供截图证明；

28、提供 IPV6 攻击防护能力，可抵御常见得 WEB 攻击类型，提供截图证明。

29、云防护产品具备全球 IPv6Forum 论坛颁发的《IPv6Enabled 认证》证书

30、云防护产品入围《江苏省符合信息安全等级保护二级以上标准（非涉密信息系统）

网络安全产品与服务推荐目录》
***注：所投产品必须满足上述所有要求，否则视作未实质响应采购技术需求。**

3、服务内容

域名数	1 个主域名（可添加不少于 7 条子域名）
服务周期	2020 年 6 月 30 日前完成部署，自部署完成验收合格后一年

（全文完）