招 标 书

招标编号：C202006002

招标项目：民生保险边界防火墙集成采购项目

招标人：民生人寿保险股份有限公司

2020 年 7 月 22 日

公章：

招标书目录

第一部分 基本说明

1、 使用范围：招标书仅适用于招标书中所叙述项目的产品及服务。

2、 投标费用：投标人需自行承担所有与编写、提交及投标过程中有关的全部费用、风险、损失，不论投标的结果如何，招标人在任何情况下均无义务和责任承担这些费用、风险、损失。

3、 提示：投标人应认真阅读招标书中所有的事项、格式、条款和规范等要求．如果没有按照招标书要求提交全部资料或者投标书，没有对招标书做出实质性响应，该投标有可能被拒绝，其风险应由投标人自行承担．招标人对投标人提交的文件将予以保密，但不退还．

4、 招标书澄清：投标人如对招标书有疑点要求澄清，或认为有必要与投标人进行技术交流时，可以于投标截止日期 10 日前以书面形式通知投标人，招标人视情况确定技术交流，或以书面答复给要求澄清方或所有投标人．

5、 招标书修改、撤回：

(1) 投标截止日期前，招标人无论出于自己的考虑、还是出于对投标人提出的问题澄清，均可对招标书用补充文件的方式进行修改或撤回，撤回的招标书不再有效；

(2) 对招标书的修改，将以书面的形式通知投标人．补充文件为招标书的组成部分，对所有投标人具有约束力．

(3) 为满足招标项目的需要或投标人有足够的时间按招标书的要求而修正投标文件时，招标人可酌情推迟投标的截止日期和开标日期，并将此变更通知投标人．

第二部分 招标情况介绍

一、项目基本情况

1、采购单位名称：　民生人寿保险股份有限公司

2、项 目 名 称 ：　民生保险边界防火墙集成采购项目

3、项目内容：

为配合民生保险机构互联网专线组网的开展，需要在各省分公司互联网出口部署防火墙做到安全加固．根据项目需求，拟定以下防火墙采购需求：

1) 防火墙 33 台，部署在北京数据中心及各省分公司；

2) 防火墙统一管理平台 1 套，部署在北京数据中心；

3) 产品的安装、配置、调试等实施和售后服务．

4、投标申请人基本条件：

1) 投标人具备独立法人资格；

2) 具有独立承担民事责任的能力；

3) 投标人实收资本金额不能低于 1000 万元人民币；

4) 投标人须提供所投产品的原厂授权函；

5) 投标人所投产品须具备公安部颁发的《计算机信息系统安全专用产品销售许可证》

6) 投标人投标品牌厂商须连续 6 年入选 Gartner 企业级防火墙魔力象限并提供证明材料；

7) 具有履行招标项目所必需的设备和专业技术能力；

8) 具有良好执行合同的能力，并能提供长期、稳定的售后服务；

9) 具有固定的工作场所，组织机构健全，内部管理和控制制度较为完善并且执行有效；

10) 能够保守招标人及其关联方的商业秘密，维护国家金融信息安全；

11) 具有良好的职业道德记录和社会声誉，认真执行有关财务审计、税务、咨询的

法律、法规和政策规定；

12) 投标人注册地为上海或北京；

13) 投标人须具有全国配送能力.

二、投标时间、地点、联系方式

1、 投标书递交截止时间： 2020 年 8 月 4 日

2、 投标地点： 上海市虹口区塘沽路 463 号 8 楼

3、 开标地点： 上海市陆家嘴西路 99 号万向大厦 18 楼

4、 联系方式：

联系单位： 民生人寿保险股份有限公司 (招标人)

地　　址： 上海市虹口区塘沽路 463 号 8 楼 (投标书递交地址)

联 系 人： 李 主

电　　话： 021-66823193

电子邮件： lizhu1@minshenglife.com

第三部分 投标人

投标人须符合《招标公告》中投标申请人基本条件．投标人须按本招标书的要求参加投标，招标人有权利核实其提交的各项原始文件，如发现有虚假、不真实或拒绝提交原件的情形，将被取消入围资格、投标人资格、中标资格或相应的合作。

第四部分 投标书

一、投标报价（重要）

投标人按照招标人要求的内容，分别核算并报价，此报价应包含税金、成本费、包装费、保险费、运输费和伴随服务费及有可能产生的一切费用，为招标人最终向投标人支付的金额。

二、投标书编写说明

1、投标书的编写：投标人应仔细阅读招标书，了解招标书的要求。在完全了解要求的条件后，**按投标书样式统一格式、顺序编制投标书，装订成册，并加盖公章。**

2、投标书包括下述内容（详见“三、投标书内容”部分）：

(1) 投标函；

(2) 开标一览表（用于唱标）；

(3) 规格性能、技术、商务偏离表；

(4) 资格文件；

(5) 质量、商务及售后承诺；

(6) 其他文件；

(7) 资格预审文件。

3、资格证明文件及相关说明：

(1) 投标人应按照要求出具相关证明文件，以证明投标人是合格的，而且一旦其投标被接受，投标人有能力履行招标书中的每一项内容，并遵守投标书中的全部内容，保证履行合同。

(2) 投标人提供的上述文件必须真实有效，否则应承担相关责任，一经发现，招标人有权取消其中标资格或终止相应的合作。

4、投标书报价

5、 投标书有效期：投标书自开标之日起 60 天内有效。

6、 投标书的书写要求：

(1) 投标书正本和所有副本须用不褪色的墨水书写或打印，装订成册。

(2) 投标书的书写应清楚工整，凡修改处应由投标全权代表盖章。

(3) 字迹潦草、表达不清、未按要求填写或可能导致非唯一理解的内容可以被拒绝或视为废标。

(4) 投标书应按招标书中的具体要求由法定代表人、法人授权代表签字及投标人盖章。

7、下述任何一种情形，均可能被招标人视为无效的投标书：

(1) 投标人提供的投标书不完整；

(2) 投标书未按招标书的规定签署；

(3) 未按规定报价；

(4) 投标人对招标书的要求未做出实质性响应；

(5) 投标人不按照招标人的通知要求参加询标事宜；

(6) 以联合体形式投标未说明及提供相应文件的；

(7) 法律、法规规定的其他情况。

8、投标人有下列情况之一，其投标被视为废标。投标人给招标人造成损失的，招标人有索赔的权利，损失超过投标，还应当对超过部分予以赔偿。

(1) 投标人提供的有关资格、资质证明文件不真实或提供虚假资料；

(2) 投标人在有效投标期内撤回投标；

(3) 在整个投标过程中，投标人有企图影响招标结果的任何活动；

(4) 投标人以任何的方式诋毁其他投标人，排挤其他投标人的公平竞争；

(5) 投标人串通投标，投标人向招标人、用户、评标小组成员提供不正当利益；

(6) 投标人以他人名义投标或者以其他方式弄虚作假；

(7) 中标人不按规定签订合同；

(8) 违反法律、法规规定的其他情况。

三、投标书内容

注：需按下列顺序装订投标书

（一）投标书封面（格式）

投 标 书

项 目 名 称：

投 标 单 位：

投标人全权代表：

全权代表联系方式：

(手机、邮箱)

投标人： (公章)

年 月 日

（二）目录

说明：请根据标书实际内容编制目录

（三）正文

1、投标函

投 标 函

致：　　(招标人)

根据贵方为_____项目招标采购货物及服务的投标书_____（招标编号），全权代表_____（全名）　　_(职务）经投标人正式授权并代表依据中华人民共和国法律在　　(注册地址）注册的投标人_____（投标人名称）提交下述文件正本一份和副本一式__六___份。

(1) 开标一览表

(2) 产品/服务说明

(3) 商务偏离表、技术偏离表

(4) 资格证明文件

(5) 质量、商务及服务承诺

(6) 其它文件：其他要求或自行提供的文件

(7) 资格预审文件

投标人、全权代表宣布同意如下：

(1) 按照招标书中的一切内容，提供符合要求的产品/服务。

(2) 投标人将按招标书的规定、要求及投标人文件的每一项要求或承诺，按期、按质、按量履行合同责任和义务。

(3) 投标人已详细审查全部招标书，包括修改文件（如需要修改）以及全部参考资料和有关附件，我们完全理解并同意这些内容。投标人同意提供按照贵方可能要求的与其投标有关的一切数据或资料，并保证提供的投标书均真实、完整，不存在任何虚假事项，投标人完全理解不一定要接受最低价格的投标或受到的任何投标。并自行承担与投标及相关过程中涉及的全部费用、风险、损失。

(4) 投标自开标日起有效期为六十个自然日。

(5) 与本投标有关的一切正式往来通讯请寄：

地址：_____

邮编：_____电话：_____

投标人全权代表姓名、职务：_____

投标人名称（公章）：

_____

法定代表人签字：

日期：_____年___月___日

全权代表签字：_____

2、开标一览表（格式：须唯一且单独封装）

开标一览表

招标项目名称：　　招标人：

投标人名称：

服务名称	规格、详细配置和要求	单位	数量	价格（含税）	补充说明
（请填写相关服务条目）					
厂家免费提供的其					

他服务	
项目总报价（含贵公司在投标函项下的一切设备和服务的价款）	大写：人民币　　（小写￥　　）

除上述列明费用外，无其他任何再需要支出费用。

本项目的付款方式为：

1）本项目采购合同签订后，收到开具合同30%金额的增值税发票后30个工作日内，支付总价款的30%；

2）稳定运行三个月后进行验收，验收合格后，在收到合同60%金额发票并且完成入库后的30个工作日内，凭发票及验收单支付合同金额的60%；

3）运行满一年后，收到合同10%金额发票的30个工作日内，支付合同金额的10%。

投标人(盖章)：

授权代表签字：

年　　月　　日

3、产品/服务说明

请提供应标产品或服务的介绍信息，包含规格型号，功能等。

4、商务偏离表

商 务 条 款 偏 离 表

序号	谈判文件的商务条款	响应文件的商务条款	说明
1	付款条件及周期：		
2	享有的服务：		
3	所投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》		

注：

1、在本表中，需对谈判文件的全部商务条款做出响应，而不仅仅是对偏离项的响应。

2、在本表中，与“谈判文件的商务条款”栏比较，如无偏离，“响应文件的商务条款”栏可具体填写响应内容或“同意”、“接受”等字样，如有偏离，则必须填写具体的偏离内容.

5、技术偏离表

请补充技术要求.

技术要求偏离表

序号	谈判文件的技术要求	响应文件的技术方案	说明

1	投标品牌厂商连续 6 年入选 Gartner 企业级防火墙魔力象限；		
2			
3			

注：

1、在本表中，需对谈判文件的技术要求全部做出响应，而不仅仅是对偏离项的响应。

2、在本表中，与“谈判文件的技术要求”栏比较，如无偏离，“响应文件的技术方案”栏可具体填写响应内容或“同意”、“接受”等字样，如有偏离，则必须填写具体的偏离内容。

3、对于技术要求(包括其他部分的内容)，如有偏离或替代方案的，也要求增列入此表，否则表示投标人完全接受，对投标人有约束力。

6、投标人资格声明（格式）

投标人资格声明

1、名称及概况

(1) 公司名称：_____

(2) 公司注册地址：_____

(3) 注册日期：_____

(4) 实收资本：_____

(5) 主要负责人姓名：_____

2、 产品/服务设施：

_____

3、产品/服务经验：

_____

4、近三年主要客户的名称：

_____

5、主要项目：

_____

6、其它情况：

兹证明上述声明真实、正确的，并提供了全部能提供的材料和数据，我们同意遵照贵方要求出示有关证明文件。

公司名称：_____（盖章）

电话：_____

日期：_____年_____月_____日

7、法定代表人授权书（格式）

法定代表人授权书

（招标人）_____：

现委派我公司_____（姓名、职务）参加贵方组织的_____招标活动，全权代表我单位处理投标、竞标、应标及后期的执行、完成和保修等事宜，以本公司名义全权处理一切与之有关的事务。

附全权代表情况：

姓　　名：_____　　身份证号：_____

职　　务：_____　　邮　编：_____

通讯地址：_____

电　　话：_____

投标人（盖章）：

法定代表人（签字）：

日期：　　年　　月　　日

8、质量、商务及服务承诺

(1) 对投标产品/服务质量保证的措施、方法；

(2) 对投标产品售后服务承诺及此招标项目的特殊服务政策；

(3) 到货时间/项目完成时间；

(4) 项目实施方案（人员架构、实施步骤及内容、初步计划安排、设备、培训、维保等）

(5) 拟投入本项目的人员名单和简历。

9、其他文件

(1) 近三年的同种业务类合同（供应商可覆盖保密内容）；

(2) 公安部颁发的《计算机信息系统安全专用产品销售许可证》；

(3) 投标品牌连续 6 年入选 Gartner 企业级防火墙魔力象限的证明材料；

(4) 投标人认为需要填写和提交规定的文件以外的其它有关资料、说明或声明；

(5) 投标人认为需要对招标项目提出其他科学、经济、合理的意见或建议。

10、资格预审文件（格式：须唯一且单独封装）

(1) 资格文件为招标人评价、判断、确定投标人的资格和能力的组成文件。资格预审项下文件，将于收到招标文件后拆封，由我司提前进行资质审核，对于不符合要求的投标文件，该投标有可能被拒绝，其风险由投标人自行承担；

(2) 资格证明文件提交要求：按照“提交文件一览表”顺序依次提供原件彩色扫描件或复印件（照片提供原件），每页均需注明“与原件一致”（文字需手写或盖原件相符章）并在注明文字上加盖公章。(审计报告、照片、公司简介、

合同、公司章程可以骑缝章方式盖章）

(3) 无法提供的文件应提供情况说明并加盖公章，否则视为无该部分内容；

(4) 需提交文件一览表：

序号	提 交 文 件 内 容
1	营业执照（副本）
2	法定代表人身份证
3	公司章程
4	上一年度完整的审计报告（无审计报告的提供说明，并提交上一年度财务报表，包括资产负债表、利润表和现金流量表）
5	授权代表身份证
6	公安部颁发的《计算机信息系统安全专用产品销售许可证》
7	投标品牌连续 6 年入选 Gartner 企业级防火墙魔力象限的证明材料
8	公司办公场所租赁（或购买）证明（名称同供应商名称或同注册地不一致时，提供说明）
9	公司办公实景照片（包括外景、室内近景等不同角度 5 张 6 寸以上照片）
10	
11	

四、投标书制作、封装、递交

1、份数：投标书一式六份（其中正本一份，副本五份）

2、 密封与标记：投标人应将投标书正本和副本分别装入信袋内加以密封，并在封签处加盖投标人公章．未按本须知招标密封、标记和投递的招标书，招标人不对其可能产生的后果负责．

3、 投标书信袋封条上应写明：

(1) 招标人、招标书所指明的投标送达地址；

(2) 招标项目名称、编号；

(3) 投标企业名称和地址；

(4) 注明“开标时才能启封”，“正本”，“副本”．

4、 为方便开标唱标，投标人应将开标一览表单独密封，并在信封上表明“开标一览表”字样，然后再装入正本招标书密封袋中．

5、 投标人必须在招标书规定的投标截止时间前送达指定的投标地点．

6、 在投标截止日期以后送达的投标书，招标人有权拒绝接收．

第五部分 开标、评标

1、开标

(1) 开标：招标人根据招标书规定的时间、地点主持公开开标，届时请投标的代表参加（参加的投标代表是法人授权书授权的代表）。

(2) 开标时当众开启投标书，并将投标书正本中的“开标一览表”及招标人认为必要的内容当众公开唱标。并当场宣读评标原则和评标注意事项。

(3) 招标人作开标记录，并由投标人、招标人签字确认，存档备查。结束开标会议。

2、评标

(1) 开标会议结束后，评标小组进行评标。

(2) 评标小组评标时，投标人对投标进行详细讲解介绍，并接受有关质询；

(3) 投标书进行审查、评审和比较，评标小组对所有投标人的投标书采用相同程度和标准评标，评标的依据为招标书和投标书，并以综合分值计分的方式对投标人评选。评标注意事项：

1) 评标小组判断投标书的响应性仅基于投标书本身而不靠外部证据；

2) 评标小组将拒绝被确定为非实质性响应的投标，投标人不能通过修改或撤销与招标书的不符之处而使其投标成为实质性响应的投标；

3) 评标小组有权选择和拒绝投标人中标。评标小组无义务向投标人进行任何有关评标的解释；

4) 评标过程严格保密。凡是属于审查、澄清、评价和比较的有关资料以及授标建议等均不得向投标人或其他无关的人员透露；

5) 投标人在评标过程中，所进行的企图影响评标结果的不符合招标规定的活动，可能导致其被取消中标资格。

(4) 评标小组依次与投标人谈判，在遵循公平、合理的原则下，评标小组可根据实际需要修改评标程序或方式。

(5) 评标时除考虑投标报价以外，还将综合考虑以下因素：

1) 公司资质

2) 技术力量和服务质量

3) 对招标书中付款条件和付款方式的响应

4) 投标人的综合实力、业绩和信誉等

5) 其它相关因素

3、标书的澄清

(1) 为有助于投标书的审查、评价、比较，评标小组有权请投标人就投标书中的有关问题予以说明和澄清．投标人有责任按照招标人通知时间地点派专人进行答疑．

(2) 投标人对要求说明和澄清问题应以书面形式明确答复，并应有法人授权代表的签署。

(3) 投标人的澄清文件是投标书的组成部分，并替代投标书中被澄清的部分．

(4) 允许对投标书中不清楚问题进行澄清，不允许对技术、商务、价格等实质性内容进行修改．澄清要通过书面方式进行。

4、确定中标人

(1) 招标人将根据评标小组提出的书面评标报告和推荐的中标候选人确定中标人，也可以授权评标小组直接确定中标人。

(2) 确定的中标人将授予符合下列条件之一的投标人：

1) 评标综合得分最高者；

2) 能够最大限度地满足招标书中规定的各项综合评价标准；

3) 能够满足招标实质性要求，并且经评审投标价格最低或较低，但是投标价格低于成本的除外；

4) 中标人数量，由招标人确定，并可以确定备选中标人.

5、中标通知

投标书有效期内，招标人将以《中标通知书》通知中标人中标．投标书有效期满后，未收到《中标通知书》投标书者，为落标，招标人不解释落标原因，不退回投标书．

《中标通知书》将作为签订合同的依据．

第六部分 签订合同

1、签订合同

中标人收到《中标通知书》后，按《中标通知书》中规定的时间地点与买方签订合同，逾期或自《中标通知书》发出后超过 15 天未就签署合同事宜达成一致的，视为中标人单方放弃合作。招标书、投标书、评标过程中形成的书面文件均作为签订合同的依据。

2、商务条款和合同内容

投标人应对商务条款和技术要求做出明确回应，除非在投标文件中明确说明不接受合同全部或部分（若有）条款，否则视为接受合同条款。（双方可在后续进一步协商合同具体条款，以双方签订内容为准）。

第七部分 设备规格及技术要求

1、数据中心防火墙（数量 3 套）

设备类别	功能	技术要求及指标
数据中心防火墙	资质要求	要求投标厂商连续 6 年入选 Gartner 企业级防火墙魔力象限（提供证明材料）
		需提供公安部颁发的《计算机信息系统安全专用产品销售许可证》（千兆）防火墙（提供证明材料）
		投标产品自正式商用起超过 2 年时间；
	硬件要求	支持通过集中管理平台进行批量管理
		配备至少 6 个千兆电口、至少 4 个 SFP 口；配置单独的带外管理口和 HA 口，不占用业务端口
		支持至少 2 个通用扩展槽.
		双冗余电源
	性能要求	防火墙吞吐≥8Gbps
		IPsec 吞吐≥3Gbps
		最大并发连接≥300 万
		每秒新建连接≥12 万
		IPsec 隧道数≥6000 条
	管理控制	支持指定一个 IP 地址范围的主机为可信任主机，只有该地址范围的主机可以对设备进行管理
	访问控制功能	支持基于安全域的方式进行访问控制，制定基于域间和域内的访问策略，支持基于 5 元组信息和应用层识别的方式实现访问控制
	虚拟系统	支持虚拟防火墙技术，可对每个虚拟系统分配系统资源，同时支持 cpu 虚拟化，支持防火墙、IPSec VPN、SSL VPN 功能，支持监控统计
	接入模式	支持透明、路由、混合、旁路四种工作模式
		支持在旁路模式下对流量进行统计、扫描、记录和会

		话重置
	智能链路负载均衡	支持智能链路负载均衡技术，可动态探测链路响应速度并选择最优链路进行转发
	多链路负载均衡	支持基于源、基于源和目的、基于会话等多种负载均衡模式
	服务器负载均衡	支持服务器的负载均衡，提供加权轮询、加权最小连接数、加权散列等多种负载均衡方式
	策略管理	支持对防火墙策略命中次数进行统计，支持防火墙策略冗余检查
	路由协议	OSPF、BGP、ISIS 和 RIP（动态路由协议非透传）支持策略路由、支持 ISP 路由并内置多运营商路由表
		支持 IPv4 和 IPv6 双栈协议
		支持 IPV6 静态路由及 OSPFv3、BGP for IPV6、ISIS for IPV6、RIPng 等 IPV6 动态路由协议
		支持基于动态端口应用协议的策略路由，可将 P2P 应用引流到低价值链路上，提升链路的利用率和用户的服务质量。
	应用识别与管控	识别 4000+应用，访问控制精度到应用功能，例如：区分微信的文字和语音。应用识别与入侵检测、防病毒、内容过滤相结合，提高检测性能和准确率。
	防病毒	支持实时病毒连接阻断，病毒事件记录
		支持对 SSL 加密流量进行病毒过滤
		支持超过 90 万的病毒特征库，病毒库可以在线更新、本地更新。
		支持多种协议和应用的攻击检测和防御针对 HTTP、FTP、SMTP、IMAP、POP3、TELNET、TCP、UDP、DNS、RPC、FINGER、MSSQL、ORACLE、NNTP、DHCP、LDAP、VOIP、NETBIOS、TFTP 等，能够实时监控多种网络攻击并根据配置对网络攻击进行阻断等操作，有效防护常见已知攻击对用户网络造成的业务中断、信息泄露以及拒绝服务等。
		支持大病毒文件的扫描：压缩类型有 GZIP、BZIP2、

		TAR、ZIP 和 RAR）、PE（支持的加壳类型有 ASPack 2.12、UPack 0.399、UPX 的所有版本以及 FSG 的 1.3、1.31、1.33 和 2.0 版本）、HTML、Mail、RIFF、CryptFF 和 JPEG
	高可用性（HA）	支持 A-S 模式，A-A 模式，支持非对称路由场景
		支持命令行主备切换，优先级可以设置
		支持基于接口、HTTP、PING、ARP、DNS、TCP 等监测对象实现 HA 切换
	NAT	支持源 NAT 地址池利用率超高告警（提供产品有效配置及验证截图，并对配置进行解释描述）
		支持多种 NAT 地址转换方式，包括：静态一对一地址转换以及端口转换、源地址转换(SNAT)、目的地址转换(DNAT)
		支持 IPV6 及 IPV4 地址互转，支持 NAT6to4、NAT4 to 6、NAT6 to 6
		支持 NAT444 模式，支持导出 NAT444 静态映射表
	TCP 处理机制	TCP 三次握手建立阶段与四次握手关闭阶段各个超时时间可自定义，通过 TCP 处理机制自定义可提高对业务系统的兼容性和稳定性。

2、 省分公司防火墙（数量 30 套）

设备类别	功能	技术要求及指标
省分公司防火墙	资质要求	要求投标厂商连续 6 年入选 Gartner 企业级防火墙魔力象限 **（提供证明材料）**
		需提供公安部颁发的《计算机信息系统安全专用产品销售许可证》（千兆）防火墙 **（提供证明材料）**
		投标产品自正式商用起超过 2 年时间；
	基础要求	支持通过集中管理平台进行批量管理
		配备至少 9 个千兆电口
		双冗余电源
	性能要求	防火墙吞吐≥1.5Gbps（可扩展到 2Gbps）

		IPsec 吞吐≥700Mbps
		最大并发连接≥60 万（可扩展到 100 万）
		每秒新建连接≥2.5 万
		IPsec 隧道数≥2000 条
	管理控制	支持指定一个 IP 地址范围的主机为可信任主机，只有该地址范围的主机可以对设备进行管理
	访问控制功能	支持基于安全域的方式进行访问控制，制定基于域间和域内的访问策略，支持基于 5 元组信息和应用层识别的方式实现访问控制
	接入模式	支持透明、路由、混合、旁路四种工作模式
		支持在旁路模式下对流量进行统计、扫描、记录和会话重置
	智能链路负载均衡	支持智能链路负载均衡技术，可动态探测链路响应速度并选择最优链路进行转发
	多链路负载均衡	支持基于源、基于源和目的、基于会话等多种负载均衡模式
	服务器负载均衡	支持服务器的负载均衡，提供加权轮询、加权最小连接数、加权散列等多种负载均衡方式
	策略管理	支持对防火墙策略命中次数进行统计，支持防火墙策略冗余检查
	路由协议	OSPF、BGP、ISIS 和 RIP（动态路由协议非透传）支持策略路由、支持 ISP 路由并内置多运营商路由表
		实配支持 IPv4 和 IPv6 双栈协议
		支持 IPV6 静态路由及 OSPFv3、BGP for IPV6、ISIS for IPV6、RIPng 等 IPV6 动态路由协议
		支持基于动态端口应用协议的策略路由，可将 P2P 应用引流到低价值链路上，提升链路的利用率和用户的服务质量。
	应用识别与管控	识别 4000+应用，访问控制精度到应用功能，例如：区分微信的文字和语音。应用识别与入侵检测、防病毒、内容过滤相结合，提高检测性能和准确率。

	防病毒	支持实时病毒连接阻断，病毒事件记录
		支持对 SSL 加密流量进行病毒过滤
		支持超过 90 万的病毒特征库，病毒库可以在线更新、本地更新
		支持多种协议和应用的攻击检测和防御针对 HTTP、FTP、SMTP、IMAP、POP3、TELNET、TCP、UDP、DNS、RPC、FINGER、MSSQL、ORACLE、NNTP、DHCP、LDAP、VOIP、NETBIOS、TFTP 等，能够实时监控多种网络攻击并根据配置对网络攻击进行阻断等操作，有效防护常见已知攻击对用户网络造成的业务中断、信息泄露以及拒绝服务等。
		支持大病毒文件的扫描：压缩类型有 GZIP、BZIP2、TAR、ZIP 和 RAR）、PE（支持的加壳类型有 ASPack 2.12、UPack 0.399、UPX 的所有版本以及 FSG 的 1.3、1.31、1.33 和 2.0 版本）、HTML、Mail、RIFF、CryptFF 和 JPEG
	高可用性（HA）	支持 A-S 模式，A-A 模式，支持非对称路由场景
		支持命令行主备切换，优先级可以设置
		支持基于接口、HTTP、PING、ARP、DNS、TCP 等监测对象实现 HA 切换
	NAT	支持源 NAT 地址池利用率超高告警（提供产品有效配置及验证截图，并对配置进行解释描述）
		支持多种 NAT 地址转换方式，包括：静态一对一地址转换以及端口转换、源地址转换(SNAT)、目的地址转换(DNAT)
		支持 IPV6 及 IPV4 地址互转，支持 NAT6to4、NAT4 to 6、NAT6 to 6
		支持 NAT444 模式，支持导出 NAT444 静态映射表
	TCP 处理机制	TCP 三次握手建立阶段与四次握手关闭阶段各个超时时间可自定义，通过 TCP 处理机制自定义可提高对业务系统的兼容性和稳定性。

3、 防火墙统一管理平台（1 套）

要求：统一管理平台应与防火墙同一品牌。

类别	功能分类	功能项
设备管理	登录方式	支持 HTTP/HTTPS/SSH 登录方式管理
		支持本地和 radius 账户登录
	设备管理要求	支持对 50 套的 NGFW 等安全设备进行集中的管理。
		支持 VFW 集中管理。
		支持通过IP/域名的方式从设备主动注册防火墙或NIPS设备。
		支持设备主机名称、设备序列号、管理 IP、设备运行时间、接口状态、并发连接、新建连接以及包转发率等相关信息显示
		支持曲线图显示设备的 CPU 利用率、内存使用率、会话数、总流量、攻击数以及病毒数
		配置历史对比：基于高效文件比较算法,对两个配置文件进行快速比较，高亮显示差异内容。
		配置文件恢复：支持配置文件单台/批量的导出、导入，支持通过本地的配置文件来恢复设备的配置。
		配置文件自动收集：支持按照天、周、月自动收集设备上的配置。
		配置变更管理：基于 4W（Who、When、What\where）的审计方法，实时记录文件配置变更的内容。
		配置锁定
		troubleshooting：通过 DNS 查询、ping、traceroute 等方式进行网络排错
		设备 session 查看
		升级管理：支持对管理的防火墙、VFW 进行软件版本批量升级，支持对 APP、AV 和 URL 特征库进行批量升级。
		支持防火设备自动化巡检
策略管理	策略管理要求	支持对设备策略规则的统一集中管理，可以管理所有设备的策略规则，包括查看、编辑、删除设备本身的策略

		规则，创建共享策略规则并集中下发等。
		支持单一设备的策略管理，可以管理单设备的策略规则，包括查看、编辑、删除设备本身的策略规则和策略下发等。
		所有规则操作配置在一个页面上完成，无需页面跳转，快速添加需要的地址和服务;对于海量安全规则，根据对象条件，快速定位规则。
		支持安全策略冗余检测和无用的对象检测,策略利用率、策略操作审计记录。
		VSYS 策略集中管理
		策略快照与回滚
		支持策略分组和策略导入导出
		策略匹配分析
		支持批量添加私有策略
		支持策略应用关联,可以将共享策略应用到多台设备的头部/尾部，可以批量替换设备策略配置，可以将策略应用到其他共享策略的头部。
NAT 配置	NAT 配置要求	支持防火墙、VSYS、VFW 上私有和共享 NAT 规则的配置下发，支持 NAT 继承
路由配置	路由配置要求	支持防火墙、VSYS、VFW 上私有和共享静态路由的配置下发
IPS 配置	IPS 策略集中管理	支持防火墙、VSYS、VFW 和 NIPS 私有和公有威胁防护策略创建和管理并在策略中调用,支持威胁防护列表维护
AV 配置	AV 策略集中管理	支持防火墙和 VFW 上私有和公有 AV 策略创建
URL 配置	URL 规则集中管理	支持防火墙、VSYS 和 VFW 上私有和公有 URL 规则创建和管理并在策略中调用
QoS 配置	QoS 规则集中管理	支持防火墙和 VFW 的 QoS 规则创建和管理
AAA 配置	AAA 配置管理	支持在防火墙和 VFW 上对象中配置 AAA 服务器，支

		持 AAA 服务器的创建删除和配置修改。
用户配置	用户配置管理	支持在防火墙和 VFW 上本地 AAA 服务器上的用户和用户组的创建、修改和删除，支持批量导入本地用户。支持外部 AAA 服务器上的用户的同步和查看。
角色配置	角色配置管理	支持在防火墙和 VFW 上创建、修改和删除角色，支持角色映射管理的创建修改和删除。
HA 状态管理	防火墙 HA 状态管理	能够支持的 HA 模式： Active-Passive，Active-Active。
设备监控	设备监控要求	支持实时的流量监控，并在客户端通过饼状图或者柱状图直观显示：
		支持设备接口（TOP 10）流量查看，
		支持指定接口 TOP 10 IP 流量查看，支持指定 IP 的 TOP 10 应用的流量查看
		支持指定接口 TOP 10 应用查看，支持指定应用的 TOP 10 IP 的流量查看
		支持实时的攻击情况监控，支持饼状图或者柱状图直观显示：
		支持设备接口遭受攻击（TOP 10）查看；
		支持指定接口发起攻击 TOP 10 IP 查看，支持指定 IP 发起的 TOP 10 攻击类型查看；
		支持指定接口 TOP 10 攻击类型查看，支持发起指定攻击类型的 TOP 10 IP 查看。
		支持 VPN 状态监控，支持 VPN 拓扑图呈现
		支持实时的被管理设备的受病毒攻击情况监控，支持饼状图直观显示。
日志管理	日志管理要求	安全管理中心平台可接收设备发送的多种日志信息，经过系统处理后，用户可进行多维度、多条件的浏览，日志根据颜色区分级别。
		支持日志搜索功能，搜索条件记录和书签。
		支持日志导入、日志备份、可读日志导出、日志清理功能。

查询管理	查询管理要求	支持查看历史监控信息，通过定义历史查询条件，包括指定查询参数和设置查询时间，进行历史数据统计和分析。
		可历史数据统计包括：流量统计分析、攻击统计分析、病毒统计分析、上网行为统计分析
统计报表	统计报表要求	提供直观、丰富的统计报表，通过对设备信息、网络访问和用户行为进行综合分析，为用户呈现全方位、多角度的统计数据和图表。
		支持按照天、周、月、季等周期生成周期性统计报表，统计粒度可达到分钟、小时和天，并能够通过邮件发送给指定人员。
		支持统计的报表内容包括： 设备状态、流量报表、网页浏览审计报表、即时通信审计报表、 网络行为审计报表、病毒过滤审计报表、设备的病毒数统计信息
		支持自定义报表任务和系统的预定义报表任务。
告警响应	告警响应要求	支持基于攻击次数、病毒数阈值、特征事件、关键字、日志级别等多种告警条件定义。
		支持邮件、短信告警等方式。
权限管理	权限管理	基于角色的用户管理
		基于设备(或 VSYS)的权限管理
IPv6	IPv6 要求	支持 IPv6 的设备配置管理
		支持 IPv6 的日志采集和查询
		支持 IPv6 的监控数据采集和呈现
管理能力	管理设备能力	支持 50 台设备的管理能力。
环境要求	部署环境要求	提供硬件设备或虚拟版本（支持 Vmware 或 KVM 环境部署）

4、所有应标的硬件设备及软件平台均需要提供 AV 功能许可，投标商提供现场安装、配置、调试以及后续技术支持服务，同时提供五年的软硬件原厂维保支持服务。