百年人寿保险股份有限公司

招
标
文
件

招标编号：AEONLIFE-IT-2016-015

项目名称：百年人寿 2016 年网络安全项目

二〇 一六 年 七 月 日

投标须知前附表		
项目	内容	规定
1	项目名称	百年人寿 2016 年网络安全项目
2	招标单位	百年人寿保险股份有限公司
3	招标编号	AEONLIFE-IT-2016-015
4	投标人资格	1:投标人需提供由投标人针对招标方项目的正式授权证明（须加盖投标人相应印章），包含招标方名称、招标文件名称及标书编号等基本信息。
5	供货说明	中标方需根据招标方书面通知供货。 设备质保期限：要求提供原厂硬件一年质保
6	投标有效期	30 自然日（从提交投标文件的截止之日起算）
7	投标文件份数	正本壹份，副本贰份
8	投标答疑	投标人应当于投标截止日前五日将投标疑问以书面形式传递至招标人。
9	投标文件递交截止时间	地点：大连市沙河口区体坛路 22 号诺德大厦 21 楼 时间：截至 2016 年 7 月 14 日 （投标文件递交截止时间即为投标截止时间）
10	开标时间	开标时间：2016 年 7 月 15 日。 开标地点：大连市沙河口区体坛路 22 号诺德大厦 21 楼

第一部分　招标邀请

百年人寿保险股份有限公司是经中国保险监督管理委员会批准成立的全国性人寿保险公司。公司于 2009 年 6 月 3 日正式开业，总部选址大连。公司注册资本 77.9 亿元人民币，由大连万达、融达投资、新光集团、一方地产等股东构成。强大的股东背景、良好的法人治理结构以及优秀的管理团队为百年人寿的发展奠定了坚实基础。

本公司现拟对“百年人寿 2016 年网络安全项目 ”进行招标，经前期综合考查评选，现诚挚地邀请贵公司参与本项目的投标。在正式投标前，请详细阅读本招标文件并确实遵守其中各项要求。

1.招标编号：AEONLIFE- IT-2016-015

2.招标内容：百年人寿 2016 年网络安全项目

3.投标截止日期： 2016 年 7 月 14 日，招标人拒收本截止日期后送达的投标文件。

4.投标地点： 辽宁省大连市沙河口区体坛路 22 号诺德大厦 21 楼

5.标书接收人： 李超、于广臣

联系电话： 0411-39828218

传真电话： 0411-39828777

电子邮件：lichao003@aeonlife.com.cn

yuguangchen@aeonlife.com.cn

6.联系方法：有关此次招标邀请之事宜，可以书面或传真或电子邮件形式与百年人寿沟通。

单位名称：百年人寿保险股份有限公司

地址：辽宁省大连市沙河口区体坛路 22 号诺德大厦 21 楼

邮编：116021

7.投标有效期： 30 日，从提交投标文件的截止之日起算。

第二部分 投标人须知

A.说明

一、适用范围

本招标文件仅适用于“百年人寿网络安全项目”。

“百年人寿网络安全项目”各阶段活动内容、操作要求等方面的要求详见招标书之第三部分。

二、定义

1.“招标人”系指百年人寿保险股份有限公司。

2.“投标人”系指投标人响应招标、参加投标竞争的法人或者其他组织。

B.招标文件说明

三、本招标文件的构成

招标文件由下述部分组成：

1. 招标邀请
2. 投标人须知
3. 项目需求
4. 投标文件格式
5. 书面澄清或者修改的招标文件内容

四、招标文件的澄清与修改

招标人对已发出的招标文件进行必要的澄清或者修改的，应当在招标文件要求提交投标文件截止时间至少 5 日前，以书面形式通知所有招标文件收受人。该澄清或者修改的内容为招标文件的组成部分。

五、投标保证金

招标人在招标文件中要求投标人提交投标保证金的，投标保证金不得超过招标项目估算价的 2%。投标保证金有效期应当与投标有效期一致。

投标截止后投标人撤销投标文件的，招标人可以不退还投标保证金。

招标人最迟应当在书面合同签订后 5 日内向中标人和未中标的投标人退还投标保证金及银行同期存款利息。

六、对招标文件的疑问

对招标文件有异议的，应当在投标截止时间 5 日前提出。招标人应当自收到异议之日起 2 日内作出答复；作出答复前，应当暂停招标投标活动。

C.投标文件的编写

七、投标文件要求

投标人应仔细阅读招标文件的所有内容，按招标文件的要求提供投标文件，并保证所提供全部资料的真实、有效、关联。

如果投标人根据招标文件载明的项目实际情况，拟在中标后将中标项目的部分非主体、非关键性工作进行分包的，应当在投标文件中载明。

八、投标语言

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。

九、投标文件的组成

投标文件应包括下列部分：

1.投标书

2.投标价格表

3.投标人需提供由原厂针对招标方项目的正式授权证明（须加盖原厂相应授权印章），包含招标方名称、招标文件名称及标书编号等基本信息。

4.企业基本情况材料及资格证明文件复印件（需加盖公章），包括：

－公司营业执照复印件 1 份；

－公司税务登记证复印件 1 份；

－公司组织机构代码证复印件 1 份；

－公司近两年内成功运作的相关案例；

－…….

－其它可以证明投标人有能力履行招标文件中合同条款和执行要求规定的相关文件。

投标人应将投标文件装订成册。

十、投标文件格式

投标人应按招标文件中提供的投标文件格式填写投标书、投标价格表、投标人基本情况材料及资格证明文件，并提供产品详细方案及招标文件要求的所有内容。

十一、投标报价

1.报价方式

(1)投标者应明确说明各执行阶段每个项目的总体价格，以及价格明细。报价需由经正式授权的代表签署，并加盖投标人公司公章。

(2)投标者应按照招标人最后确定的需求报价。

2.填写时应注意下列要求：

一旦投标人中标，投标人不得以任何借口向招标人提出增加任何费用的要求。

十二、投标人基本信息

1.简述公司的基本情况、发展历史、股东情况，最近两个年度的成功案例，员工及分公司数量。

2.明确叙述公司拟参与本项目负责人与主要技术人员的简历、业绩、拟用于完成招标项目的设备及时间投入。

3.若公司将与合作伙伴一起参与本项目竞标，简述公司合作伙伴的基本情况以及将参与本项目的人员的简历和时间投入。

4.本项目联系人：

－公司名称：

－联系人姓名及职位：

－电话号码：

－传真号码：

－电子邮件地址：

十三、投标文件的签署及规定

1.投标人应准备一份正本和二份副本，在每一份投标文件上要明确注明“正本”或“副本”字样，一旦正本和副本有差异，以正本为准。同时提供全套投标文件的电子文档与正本共同封装（介质应为光盘或者 U 盘）。

2.投标文件正本和副本须打印并由经正式授权的投标人代表签字，并加盖投标人公司公章。

D.投标文件的递交

十四、投标文件的密封和标记

1.投标人应将投标人文件正本和副本分别用信封密封，并在封签处加盖投标人公章(或合同专用章)。

2.投标文件信袋封条上应写明：

(1)招标人名称、招标文件所指明的投标送达地址；

(2)招标项目名称；

(3)标书编号；

(4)投标人名称和地址；

(5)注明"开标时才能启封"，"正本"，"副本"。

3.如投标文件由专人送交，投标人应将投标文件进行密封和明确标记后，按投标邀请注明的地址送至招标人。招标人拒收投标截止时间后送达的投标文件。

E.开标和评标

十五、开标

1.开标于提交投标文件截止时间的同一时间在百年人寿保险股份有限公司职场公开进行。

2.开标时，在评标小组人员全部到齐后工作人员查验投标文件密封情况，确认无误后当众拆封，宣读投标人名称、投标价格和投标文件的其他主要内容，一式三份的招标文件必须在招标现场同时开标。开标过程应当记录，并存档备查。

十六、评标小组

招标人将针对此次招标工作成立评标小组，评标小组成员的名单在中标结果确定前应当保密。

评标小组对投标文件进行审查、质疑、评估和比较，采用综合打分法（本项目的报价将作为最主要评估因素）进行评标。

十七、投标文件的澄清

投标文件中有含义不明确的内容、明显文字或者计算错误，评标小组认为需要投标人作出必要澄清、说明的，应当书面通知该投标人。投标人的澄清、说明应当采用书面形式,并不得超出投标文件的范围或者改变投标文件的实质性内容。

十八、对投标文件的评估和比较

1.招标人及其组织的评标小组将对实质性响应的投标文件进行评估和比较。

2.评标时除考虑投标价格外，还将考虑以下因素：

(1) 设备运行的稳定性，及其设备的性能。

(2) 产品的售后服务，其中包括：实施人员资质，后期维护人员资质是否有本地化服务等

十九、保密

1.有关投标文件的审查、澄清、评估和比较以及有关授予合同的意向的一切情况都不得透露给任何投标人或与上述评标工作无关的人员。

2.本项目招标书属于招标人所有。未经招标人的书面许可，不得将本项目招标书的任何内容以任何形式泄露给任何其它第三方，否则，投标人应承担给招标人造成的所有损失。

F.中标和合同

二十、定标准则

中标人的投标应当符合下列条件之一：

1.能够最大限度地满足招标文件中规定的各项综合评价标准；

2.能够满足招标文件的实质性要求，并且经评审的投标价格最低；但是投标价格低于成本的除外。

二十一、中标结果的通知

招标人负责向中标人发出《中标通知书》，并同时将中标结果通知所有未中标的供应人。投标人如对评标过程有异议或对评标结果不服可向招标人合规经营部投诉。

二十二、合同的签订和履约保证金

招标人和中标人应当自《中标通知书》发出之日起三十日内，按照招标文件和中标人的投标文件订立书面合同。

招标文件要求中标人提交履约保证金的，中标人应当提交。

二十三、否决投标

有下列情形之一的，评标小组否决其投标：

1.投标文件未经投标单位盖章和单位负责人签字；

2.投标联合体没有提交共同投标协议；

3.投标人不符合国家或者招标文件规定的资格条件；

4.同一投标人提交两个以上不同的投标文件或者投标报价，但招标文件要求提交备选投标的除外；

5.投标报价低于成本或者高于招标文件设定的最高投标限价；

6.投标文件没有对招标文件的实质性要求和条件作出响应；

7.投标人有串通投标、弄虚作假、行贿等违法行为。

第三部分　项目需求

一、服务商简介

二、百年人寿 2016 年网络安全项目　项目要求

1、设备需求，详见《包一附件 2：防毒墙设备产品技术参数》、《包二附件 3：SSL VPN 设备产品技术参数》、《包三附件 4：WAF 设备产品技术参数》、《包四附件 5：DDOS 设备产品技术参数》、

2、招标方采购设备的型号和数量，投标方参考本招标文件的《附件 6：投标价格表》填写。

3、制定详细的百年人寿网络安全项目现场实施方案和现场技术支持流程，必须保证现场实施。

4、设备送货，安装、调试服务的费用由投标方承担。

5、百年人寿此次采购的网络安全项目，投标设备必须保证稳定高效的性能，并要保证在设备主备切换时，保证业务的不中断。

6、投标方在设备保修期内为招标方免费提供维保服务，具体要求如下：

（1）服务范围：维保服务覆盖《附件 4：投标价格表》清单中的设备和自带软件。

（2）服务工程师：技术维保工程师应具备上述维保对象的硬件系统、软件系统、管理/操作系统等方面的知识，具备相应的技术资格认证，并有 3 年以上从业经验；

（3）服务级别：7×24 技术服务支持，备件第二天到现场。

（4）故障响应及处理：

- 对系统性能严重损坏，接到支持需求必须立即做出回应；
- 对系统运行正常，仅受到有限的影响或未受到严重影响，接到支持需求必须在 30 分钟内做出回应；

（5）备品备件：按照原厂商承诺提供服务。

（6）现场巡检：每年进行一次设备现场巡检。

（7）产品升级：提供产品升级评估和现场升级服务，包括网络设备 OS 系统版本升级、升级方案提供与升级后验收。

（8）特殊要求：提供特殊时段（春节、劳动节、国庆节、年终、招标方重大应用测试、投产），以及系统变更和迁移、系统升级等的现场支持服务。

（9）建立与招标方的沟通机制，现场支持指定专人负责。

（10）在保修期内，投标方应无偿并迅速替换由于部件缺陷及制造工艺等问题而发生故障的产品。如因产品有设计、生产之缺陷而造成设备的性能和质量与合同规定不符，投标方将协调原厂商来排除缺陷，修理或替换出现故障的部件、元件和设备，所有费用由投标方承担。

7、关于人员配置。讲标人员必须是投标方配备本项目经理，否则将视为自动放弃投标；同时，投标文件中需要提供配备本项目的工程师和实施人员的类似项目经历，以及专业能力 证明。

8、投标方须具有厂商针对百年人寿项目原厂授权。

9、培训及指导提高：必须由原厂工程师安排培训，百年人寿预计 2 人/次。产品报价中包含此项费用；

10、质保期限：要求为原厂提供，一年质保 。

三、报价

1.投标人应提供完整详尽的计划方案、详细报价（单价、数量、等），以及付款方式。

第四部分　投标文件格式

附件 1：项目投标书

致：百年人寿保险股份有限公司

根据贵方为 百年人寿 2016 年网络安全项目 招标邀请，签字代表(全名、职务)经正式授权并代表投标人_____(投标人名称、地址)全权办理对上述项目的投标、谈判、签约等具体工作，并签署全部有关的文件、协议及合同。

提交下述文件正本一份和副本一式二份。

1.投标价格表。

2.公司基本情况材料及资格证明文件复印件。

据此函，签字代表以及投标人宣布同意如下：

1.投标人将按招标文件的规定履行合同责任和义务。

2.投标人已详细审查全部招标文件，包括修改文件(如有的话)以及全部参考资料和有关附件。我们完全理解并同意放弃对这方面有不明及误解的权利。

3.投标自提交投标文件的截止之日起有效期为 30 日。

4.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，完全理解贵方不一定要接受最低价的投标或收到的任何投标。

5.与本投标有关的一切正式往来通讯请寄：

地址：　　邮编：

电话：　　传真：

投标人代表签字：

投标人代表职务：

投标人名称：

(公章)：

日期：　　年　　月　　日

全权代表签字：

附件 2：防毒墙设备产品技术参数

指标项	技术规格要求
支持协议	HTTP, HTTPs, FTP, SMTP, Pop3
威胁扫描	侦测各种文件类型病毒包括木马，间谍软件，灰色软件，Rootkits 等
	专用的网络钓鱼检测
	Java Applet and ActiveX 检测
	URL 信誉评估
	URL 分类过滤
	垃圾邮件检测
病毒识别码	3,000,000+种病毒识别码，每年约新增 750,000+识别码
	全球病毒实验室+本地病毒实验室支持
策略支持	针对不同用户分组利用策略分类管理
部署	透明网桥/简单透明模式
更新来源	全球升级架构以及本地升级源的设计，降低升级带宽使用
日志管理	包含病毒日志，URL 阻止/访问日志，性能日志，系统事件日志等
	支持 Syslog 协议，可配置传输内容
	可按照时间，协议，威胁类型等查询条件查询日志
报表系统	提供日/周/月图形化报表，以及实时图形化报表
	提供违例事件/间谍软件/清除/流量/URL 过滤等报告
通知类别	URL 访问警告通知及 URL 阻止通知
	扫描通知，Applet/ActiveX 安全通知等
	数据库阈值监视警告，硬盘容量阈值监视警告，带宽阈值监视警告等
安全性	通过加密的 SSL 命令行远程管理
	通过加密的 SSL 访问管理控制台
	管理控制台访问控制
可靠性	硬盘支持 RAID 技术
	支持冗余电源
	提供流量过载保护
产品	产品获国家公安部销售许可证
	自主开发，拥有自主知识产权
	获国产软件登记证
安全标准	CCC，CE 欧盟/中国 RoHS、欧盟 REACH（领先环保认证标准）
最大在线吞吐量	600M
推荐用户数	1000

附件 3：SSL VPN 设备产品技术参数

项目	指标	具体功能要求
接口	电口	≧6 个千兆电口
	光口	≧4 个千兆光口
技术规范	安装空间	2U
	冗余电源	冗余电源
	硬盘	500G
性能参数	SSLVPN 加密速度	≧480Mbps
	SSLVPN 并发用户数	≧3800
	SSLVPN 每秒新建用户数	≧400
	IPSecVPN 加密速度	≧255Mbps
	IPSecVPN 隧道数	≧1000
	防火墙吞吐量	≧2.5Gbps
	最大并发会话数目	≧2,500,000
	无故障时间	≥100,000 小时
安全性要求	因部分数据属于我单位机密数据，一旦外泄会对我单位造成不良影响，投标设备需支持沙盒技术，强制受保护的指定资源仅可在沙盒桌面下使用；	
安全性要求	为遵循系统建设安全性原则，为避免 VPN 接入用户的越权访问，投标产品必须实现 SSL VPN 账号与业务系统账号的唯一绑定，防止不良用户登录 SSL VPN 后用其他人的用户名登录应用系统。	
安全性要求	为满足国密办指导文件要求，保证数据传输过程安全性，要求投标产品可扩展支持中国国家标准的商用密码算法（简称“国密”），包括：SM2、SM3、SM4。	
易用性要求	我单位后续会继续进行智能终端的办公 APP 开发以满足移动办公需要。考虑到数据传输过程中的加密问题，要求所投设备厂商必须可以提供针对 Windows、Andriod、IOS 智能终端第三方应用程序（APP）的 SSL VPN 软件开发包（SDK）以保证接入安全	
易用性要求	我单位存在已开发完成的 APP，因无专业研发人员持续开发，要求所投设备必须支持对我单位正在使用的办公系统 APP 进行安全加固。自动加固或者手动加固均可以，但为保证交付进度，自动加固要求投标人在1日内完成，手动加固要求投标人在3日以内完成，否则视作虚假应标。	
易用性要求	为保证我单位加固后的业务系统能够正常上架使用，要求投标产品厂商或投标集成商能够提供企业应用商店功能，将加固后的 Android/IOS APP 发布上线；要求企业应用商店功能支持 C/S、B/S 两种架构以满足我单位不同用户的使用习惯；要求该功能必须为投标厂商或者投标集成商开发而非第三方平台；	

附件 4：WAF 设备产品技术参数

指标项	指标要求
规格	标准专用千兆硬件平台 标配 1+1 冗余电源，电源可热插拔
网口数量	标配： 4*工作口（2*GE 电口，2*GE 光口），端口可扩展
性能参数	网络吞吐量系统最高处理能力 6000Mbps 应用吞吐量不小于 6000Mbps HTTP 并发连接 30 万 HTTP 新建连接(CPS)3 万
部署方式	透明桥部署：防护口不占用 IP 地址，实现完全透明部署，无需以先终结用户的 TCP 会话后再发起新的 TCP 会话到服务器方式处理，并支持路由不对称场景
	透明代理部署：防护口不占用 IP 地址，实现应用层透明部署，支持 TCP 连接复用，并优化服务器会话处理改善服务器处理性能
	端口镜像部署：镜像服务器流量即可实现安全审计和告警
	反向代理部署：可支持代理和路由牵引两种模式，客户端源 IP 可采用透明和非透明两种转发机制，非透明可指定字段进行识别，支持多台 WAF 设备冗余和集群部署
	路由模式部署：可支持静态路由、动态路由分发，无缝路由切换
	支持链路聚合，提升网络带宽、增加容错性和链路负载均衡
	支持 VLAN 子接口，业务口可承载多个 VLAN 通道
高可用性	支持全透明集群模式、主-主模式、主备模式、硬件 BYPASS、软件 BYPASS
保护对象	支持多条链路数据的防护，防护网段数量不限
	支持以域名和 IP 多种方式进行防护
	支持 ipv4/ipv6 双协议栈
WEB 服务自发现	支持 WEB 站点服务自动侦测功能
	支持识别 VLAN 信息
防御功能	能够识别恶意请求含：跨站脚本(XSS)、注入式攻击（包括 SQL 注入、命

	令注入 、Cookie 注入等)、跨站请求伪造等应用攻击行为
	能够识别服务端响应内容导致的缺陷：敏感信息泄露、已有的网页后门、错误配置、目录浏览等缺陷
	能基于访问行为特征进行分析，能识别盗链、爬虫攻击的能力
	能识别网站中的网页木马程序，通过策略可防止木马网页被用户访问
	内置主流 Webshell 特征库，对上传内容进行检查，防止恶意 Weshell 上传
	支持丰富的自定义规则，可以针对多个条件组合，形成深度的 WEB 防护规则
	支持服务器隐藏 可配置删除服务器响应头信息
	支持 Cookie 安全机制，支持 Cookie 自学习 支持 Cookie Httponly 支持 Cookie 防篡改、防劫持
智能自学习功能	支持网站自学习建模功能，能通过自学习形成网站 URL 树； 通过自学习能生成安全防护策略； 通过自学习能发现参数的名称、类型、匹配频率； 可配置匹配到自学习特征后放行； 可配置匹配不到自学习特征直接阻断请求；
智能攻击者锁定	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 可配置攻击者识别策略和算法 可配置攻击者锁定时间 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所在的地理位置
虚拟补丁自动生成	支持导入扫描器结果形成 WAF 策略 扫描器扫出的漏洞信息可直接导入 WAF，形成专用防护规则
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

	告警页面支持重定向至其它 URL
	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
WEB 访问行为合规	支持对访问流程的校验 可配置页面合规页面流程 可配置页面思考时间 发现访问违反合规的直接被拦截并产生告警日志
CC 防护功能	支持多种算法检测方法：对指定 URL 访问速率、对指定 URL 访问集中度检测 支持多种条件匹配算法：可基于 URL、请求头字段、目标 IP、请求方法等多种组合条件进行检测 检测对象支持 IP 或 IP+URL 算法,IP 可支持 X_Forwarded-For 字段解析，并支持自定义检测字段功能 支持挑战模式,客户端访问时 WAF 发起 302 重定向与 js 挑战验证是真实客户还是 CC 工具发起的访问 支持学习业务流量模型，在业务流量异常时开启 CC 防护，并支持启动配置阈值 支持基于地理位置的识别，可设置不同地理区域的检测算法 支持统计访问流量信息，进行人机对抗
篡改监控	系统提供防篡改功能,能够防止被篡改内容被浏览者访问到,一旦检测到被篡改，实时发送告警信息给管理员。
安全审计	能详细记录攻击事件的 HTTP 请求头信息，含请求的 URL、UserAgent、POST 内容，cookie 等所有的请求头内容
	能详细记录服务器响应头信息，服务器响应内容
日志分析	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
报表	根据 PCI-DSS 要求，对用户的应用进行合规性评估，生成合规报表

	支持自定义报表、定时报表、支持各类导出格式（WORD,PDF 等）
	报表可自动发至管理员邮箱
告警方式	支持 Syslog、手机短信、邮件等多种告警方式
访问审计	具备审计网站正常访问流量的能力，提供按小时，日期、月份生成报表
	能记录、查询所有用户对网站的访问情况
	能分析出访问量最大的 URL，IP 地址
	能分析出访问流量最大的文件类型
加速功能	系统内嵌应用加速模块，通过对各类静态页面及部分脚本高速缓存，提高访问速度
	支持响应内容压缩，并支持对压缩的响应内容识别
SSL 透明代理	支持 HTTPS 服务器的防护，可支持第三方认证机构颁发的证书链，WEB 应用防火墙前端与后端均为 HTTPS 加密链路，实现 HTTPS 应用系统的防御
	部署在 SSL 网关后面，能够解析到真实的访问者 IP，并能对真实的 IP 进行防护和阻断
负载均衡	工作在代理模式时，对保护的多台负载 WEB 服务器，达到平均分发、按比例分发、热备等多种负载均衡模式。
设备管理	配置变更时不影响在线业务
	规则库支持手工、在线升级两种方式，在线升级可支持规则定时检查新版本和在线更新，确保 WAF 能够针对新型的、突发型的 Web 攻击进行防护
	支持 HTTPS 方式进行设备管理
	设备管理采用管理员与审计员分离
	操作界面支持全中文界面
	支持集中管理，对多台 WAF 进行统一管理，实现日志收集、策略分发等功能
	支持 LDAP 认证
	与风暴中心交互，对用户安全情况进行分析并提供安全预警、反馈机制

附件 5：DDOS 设备产品技术参数

防护能力	规格描述
清洗性能	4GB
最大清洗链路	4 路千兆
硬件规格	要求标准机架式 2U 设备
网络端口	8 个千兆光口，4 个 100/1000M 以太网电口
抗攻击功能	采用自主知识产权的抗拒绝服务攻击算法，包括流量触发技术、协议分析技术、主机识别技术、连接跟踪技术、端口防护技术等，实现对 SYN Flood，UDP Flood，ICMP Flood，IGMP Flood，Fragment Flood，HTTP Proxy Flood，CC Proxy Flood，Connection Exhausted 等各种常见的攻击行为均可有效识别，并通过集成的机制实时对这些攻击流量进行处理及阻断，保护服务主机免于攻击所造成的损失。
防护模式要求	对于同类 DDOS 攻击流量，根据部署情况和防护需求能够进行不同防护模式的切换，如对 SYN flood 攻击的保护，可以灵活选择重传防护机制或 100%真实源探测防护机制。需提供设备截图
通用报文过滤	除了提供专业的 DOS/DDOS 攻击检测及防护外，还应该提供面向报文的通用规则匹配功能，可设置的域包括地址、端口、标志位，关键字等，极大的提高了通用性及防护力度。
应用层协议防护	支持对应用层协议高级防护（如：FTP,SMTP,POP3,HTTP 等），并且能够通过自定义协议类型防护特定应用层协议（如网游、语音、即时通讯相关协议等），系统应具有常用应用层协议（如 HTTP、FTP、GAME、DNS 等）防护模块
特定服务防护	抗拒绝服务系统内置的各种服务器插件（如针对游戏、DNS 服务器、邮件服务器、web 服务器等）并经过分析被保护主机服务特点，配置不同参数进行防护；利用连接跟踪、TCP 重传机制、SYN 分级保护机制实现对连接型 FLOOD 的防护；支持协议自定义防护功能；支持插件定制功能。 需提供设备截图。
CC 类的全连接攻击	通过内置插件、协议自定义、黑名单管理及灵活的规则设置，对 CC 类的各种代理 ip 型攻击、僵尸网络攻击具备良好的防御效果。
流量分析监测	通过曲线,图表条，可以实时的看到当前网络的流量,数据包、拦截的数据包、累计流量等信息；除了对设备本身的入口流量进行实施监控外，还需要能够实时显示网络中被保护主机的进出流量，这样可以准确的了解到每个主机当前的网络流量情况，更准确的进行配置调整，实现更好的防护效果。

防护算法和功能	无防护 IP 数量限制； 可选择是否使用状态检测方式，进而可提高通讯效率和性能； 为提高防护性能和针对未来 DDoS 攻击的变形，采用智能识别和指纹识别技术，不需要特征匹配方式，不需要基于特定规则，针对末知攻击无需进行手工进行规则匹配就可进行防护
	在串联部署中，设备支持网络隐身，业务流量处理和设备管理功能分离。抗 DDoS 工作端口不设置 IP，提高自身安全性。
	特殊的 WEB 防护模块，可设置有攻击时自动启用，无攻击时自动取消。
自定义功能	支持协议定义，可针对不同的服务类型编写协议定义，自行定制防护策略
	支持域名黑白名单功能
	可以通过设置忽略国外 IP 访问
需求定制	全局防护功能可根据用户需求进行模块化定制和选择。
防护特性	主机识别：可自动识别其保护的各个主机及其地址。实现某台主机受到攻击不会影响其它主机的正常服务。
流量控制	主要是针对攻击流量限制： 紧急触发状态： 针对攻击频率较高的攻击防护模式，此模式将更为严格过滤攻击； 简单过滤流量限制 ：是针对某些显见的攻击报文做的一种过滤模式，目前可以过滤内容完全相同的报文，及使用真实地址进行攻击的报文； 忽略主机流量限制 ：用于限制忽略主机的流量，当某个忽略主机的流量超过设置值，超过的流量将被丢弃； 伪造源流量限制 ：用于限制内网攻击。当某数据包的原 MAC 地址不同于系统记录到的 MAC 地址，该数据包将被认为是伪造源流量，超过设置值的伪造源流量将被丢弃。
端口防护	建立在连接跟踪模块上的端口防护体制，针对不同的端口应用，提供不同的防护手段，使得运行在同一服务器上的不同服务，都可以受到完善的 DOS/DDOS 攻击保护。
连接控制	根据攻击的流量和连接数阀值来设置触发防护选项，连接数阀值可以根据不同情况来灵活控制。
连接跟踪能力	每个进出的连接，会根据其源地址进行分类，并显示给用户，方便用户对受保护主机状态的监控。同时还提供连接超时，重置连接等辅助功能，弥补了 TCP 协议本身的不足，使您的服务器在攻击中游刃有余
包过滤	数据包规则过滤(可对端口和 TCP SYN,FIN,PSH,ACK 等标志位过滤) 数据包内容细致过滤(数据包内关键字过滤,支持明文和十六进制)
	提供基于多种对象的访问控制规则，以及根据业务类型制定分组策略

	可对单个 IP 与服务器的连接数进行限制，对连接进行严格的时间控制，同时可以清除服务器上的残余连接
	支持面向报文的通用规则匹配功能，可设置的域包括地址、端口、标志位，关键字等，极大的提高了通用性及防护力度。同时，内置了若干预定义规则，涉及局域网防护、漏洞检测等多项功能，易于使用。
设备监控	显示当前活动 TCP 连接状态
	全局及单 IP 流量统计
	全局及单 IP 报文统计
	关键端口流量统计
	报警事件统计
	可以详细的看到每一个正常的连接和攻击的连接所有信息，并且可以组合查找排序每个连接，通过这个功能专业人员可以发现已知和未知的异常的攻击
	除了可以通过管理界面了解设备监控信息，还提供集中监控软件，可以实现多台集中监控，满足大型系统和集群系统的管理需求。
部署方式	支持串联部署
	支持旁路部署
	单台设备可支持双链路接入部署模式
	支持透明/路由接入模式
	支持集群部署方式,可实现多路并行处理,提高防护的容量,满足大型网络应用需求
日志管理	显示详细日志时间，并记录该时间内设备的状态及操作记录。“全部”记录到的所有日志信息；“重要事件”记录重启信息；“防护事件”记录是否进入防护状态及相关防护信息；“普通事件”记录网络使用流量、CPU 和内存，以及各项操作权限(登录、修改密码、修改保存下载配置等）所进行的操作记录。
日志分析	支持按主机、按时间、按攻击类型等分析、查询，支持日志分析内容输出下载
日志服务	支持 Syslog 日志服务器和专用管理器日志服务
	支持通过邮件自动发送日志
报警	支持窗口闪动、铃声告警、邮件通知、SNMP Trap、Syslog 等报警方式，支持根据报警条件：总流量报警、总连接报警、单墙流量报警、单墙连接报警、主机流量报警、主机连接报警，支持攻击频率报警：SYN 频率报警、ACK 频率报警、UDP 频率报警、ICMP 频率报警、Frag 频率报警、New-Tcp 频率报警、New-UDP 频率报警。
售后服务	具体描述
服务时间	7*24 实时应急响应，24 小时有专业工程师值班服务。
服务方式	电话、网络远程、上门服务等多种方式。

附件 6：投标价格表

投标人名称：

项目名称： 百年人寿 2016 年网络安全 项目

招标编号： AEONLIFE-IT-2016-015

包一：

序号	产品型号	产品描述	单价 (人民币)	数量	投标总价 (人民币)
1		**防毒墙**		2	
总计					

包二：

序号	产品型号	产品描述	单价 (人民币)	数量	投标总价 (人民币)
1		**SSL VPN 设备**		1	
总计					

包三：

序号	产品型号	产品描述	单价 (人民币)	数量	投标总价 (人民币)
1		**WAF 设备**		2	
总计					

包四：

序号	产品型号	产品描述	单价 (人民币)	数量	投标总价 (人民币)
1		**DDOS 设备**		2	
总计					

投标人代表签字：

职务： 日期：

附件 6：投标人基本情况及资格证明文件

公司基本情况

1.公司名称：_____ 电话号码：_____

2.地址：_____ 传真：_____

3.注册资金：_____ 经济性质：_____

4.营业注册执照号：_____

(随本表格附交一份最新营业执照副本的复印件并加盖公章)

5.公司简介

(自行描述)

6.其它