**中联部互联网门户网站等级保护整改项目集成服务技术需求**

## 一、项目概述

### 1、项目背景

中共中央对外联络部（简称中联部）是负责中国共产党对外工作的职能部门，也是作为中国共产党的对外工作的重要组成部分。近年来，中联部在公共宣传与信息公开等方面建立了一批非涉密信息系统，并加强了信息安全保护技术的建设，初步建立了信息安全保护体系，有效支撑了各项工作的开展。

随着信息技术的快速发展和信息化建设的不断深入，信息载体和传输途径呈现出多样性和复杂性，信息安全防护压力越来越大。为切实保护国家重要信息系统的安全，公安部、国家保密局、国家密码管理局和原国信办先后下发了《关于信息安全等级保护工作的实施意见》、《信息安全等级保护管理办法》、《关于开展全国重要信息系统安全等级保护定级工作的通知》和《关于开展信息安全等级保护安全建设整改工作的指导意见》等文件，规范和指导国家信息安全建设。信息安全工作已经成为国家信息化建设一项重要内容。

目前，中联部信息安全建设与国家相关要求仍有差距，信息安全保障体系亟待完善。因此，为贯彻落实有关文件精神和《网络安全法》等要求，保障中联部非涉密信息系统稳定运行，中联部计划开展“中联部互联网门户网站等级保护整改项目”，建立满足国家相关要求的信息安全保护体系，提高信息安全防护水平，促进中联部信息化科学健康有序发展。

### 2、项目建设目标

依据国家信息系统安全等级保护相关标准和中联部信息安全等级保护工作的总体要求，结合公安部信息安全等级保护评估中心提供的安全问题整改建议，为中联部门户网站及其他七大网站建立起相应的信息安全保护体系，使系统的网络安全、主机安全、应用安全、数据安全、物理安全的防护水平达到国家信息系统安全等级保护三级要求，保证系统安全可靠运行，具体目标如下：

（1）网络系统在结构安全、访问控制、安全审计、边界完整性检查、入侵防范、恶意代码防范、网络设备防护等方面达到三级等级保护网络安全要求。

（2）应用系统及其主机系统达到相应安全等级保护的应用安全和主机安全要求。

（3）数据的完整性、保密性、备份与恢复等达到三级等级保护数据安全要求。

（4）依据公安部信息安全等级保护评估中心提出的信息系统安全等级保护整改意见进行整改。

★投标人承诺通过本次招标整改建设，使得中联部互联网门户网站安全水平达到信息系统安全等级保护三级要求，并通过公安部信息安全等级保护评估中心的等级测评。

### 3、项目建设的必要性

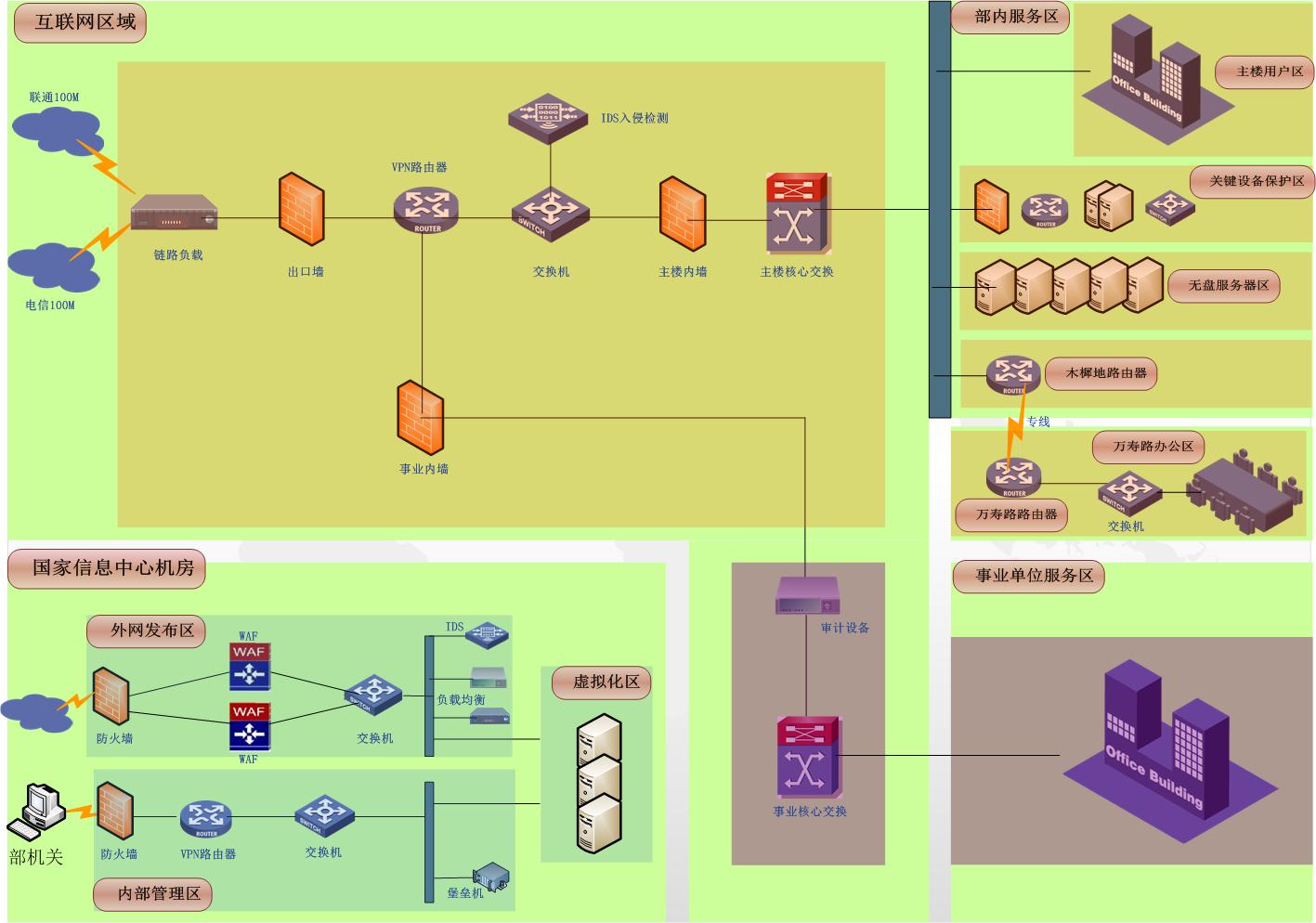
中联部门户网站等系统是国家信息系统的重要组成部分。这些信息系统所承载的应用带有社会属性，关系到国家安全、公众利益、社会稳定和其他公民组织的合法权益。因此，建设满足国家信息安全要求的信息安全等级保护体系是十分必要的，将对国家安全、社会稳定、行业发展产生积极影响。

过去的几年里，中联部信息化建设呈现快速增长的势头，信息安全也成为信息化建设重要内容。科学的信息安全等级保护可以将安全威胁控制在较小的可接受的范围，从而确保信息化建设速度和效能。本项目将对中联部信息安全技术进行梳理，通过建立和完善科学的区域化管理、统一的安全管理中心、规范的工作流程，将信息安全的身份鉴别、访问控制、安全审计、安全防范、安全运维、责任追究落到实处。

因此，本项目对提高中联部信息安全防护水平和信息服务能力是必要的，将促进中联部信息安全和信息化建设走上可持续发展的道路。

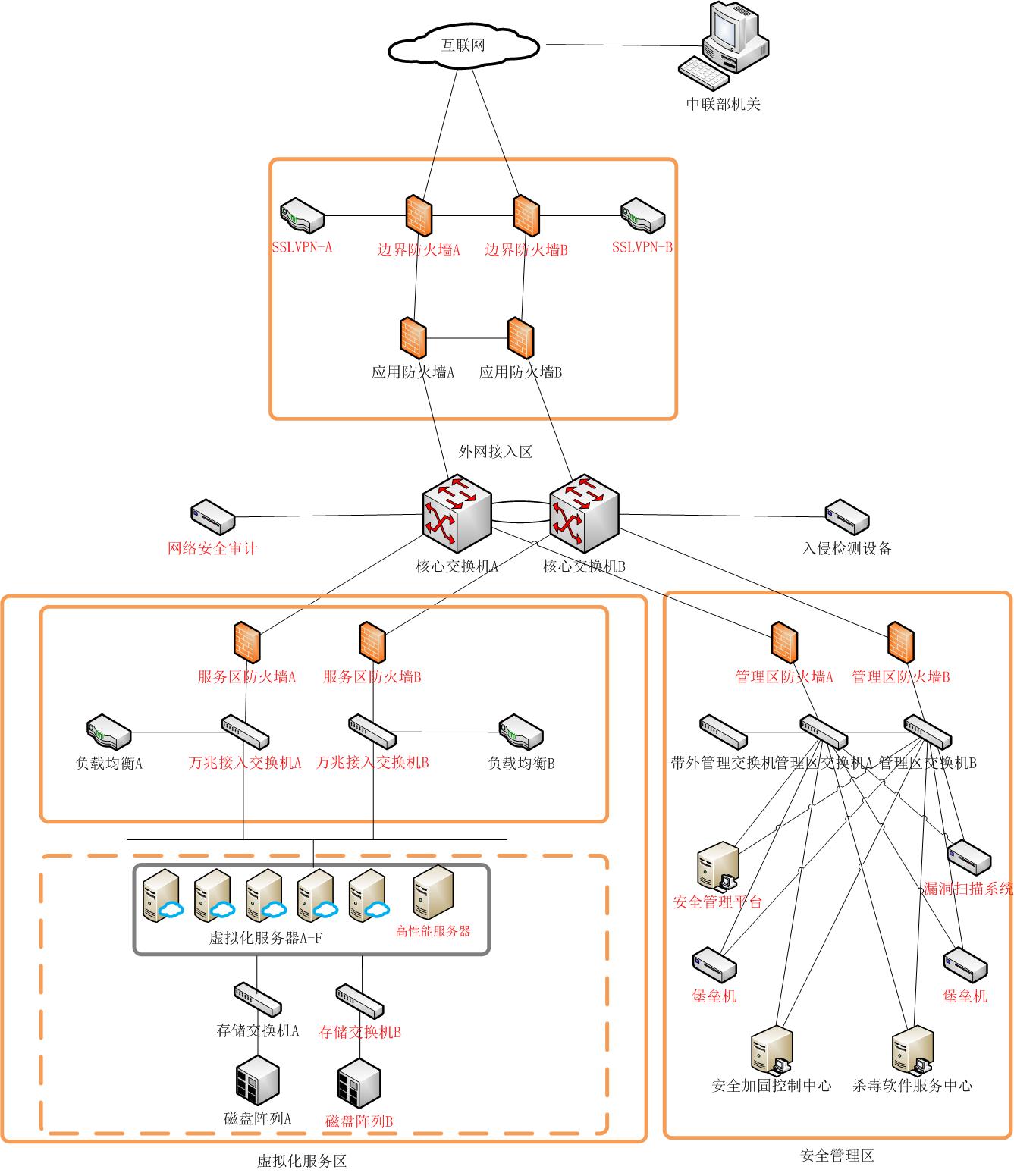
### 4、门户网站系统现状

现有中联部门户网站系统网络架构主要由内部发布-管理区、外网发布-业务区、虚拟化服务器区等安全域构成。系统拓扑简图如下：



根据公安部信息安全等级保护评估中心对中联部信息系统进行的等保预评估，目前中联部在网络安全、主机安全、应用安全以及安全管理四个环节，还存在差距。

本次改造后系统拓扑简图如下：

****

## 二、产品采购清单

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **设备名称** | **所属区域** | **数量** | **备注说明** |
| 1 | 千兆边界防火墙 | 边界接入区 | 2 | 新购，用于网络边界防护 |
| 2 | SSLVPN | 边界接入区 | 2 | 新购，用于部内用户维护接入 |
| 3 | 网络安全审计 | 核心交换区 | 1 | 新购，用于综合行为审计 |
| 4 | 千兆服务区防火墙 | 应用服务区 | 2 | 新购，用于应用服务区安全隔离 |
| 5 | 万兆接入交换机 | 应用服务区 | 2 | 新购，用于虚拟化服务器接入 |
| 6 | 光纤存储交换机 | 应用服务区 | 1 | 新购1个，与原有1个组成双机 |
| 7 | 磁盘阵列 | 应用服务区 | 1 | 新购，与原有磁盘阵列互为备份 |
| 8 | 高性能服务器 | 应用服务区 | 1 | 新购，增加计算资源 |
| 9 | 服务器硬盘 | 应用服务区 | 6 | 新购，扩充原有服务硬盘空间 |
| 10 | 万兆网卡 | 应用服务区 | 1 | 新购，实现原有虚拟服务器万兆连接，实现快速迁移 |
| 11 | 千兆安管区防火墙 | 安全管理区 | 2 | 新购，用于安全管理区安全隔离 |
| 12 | 安全管理服务器 | 安全管理区 | 1 | 新购，用于安装安全管理软件 |
| 13 | 堡垒机 | 安全管理区 | 2 | 新购，用于运维安全管理 |
| 14 | 漏洞扫描系统 | 安全管理区 | 1 | 新购，用于日常系统漏洞扫描 |
| 15 | 安全加固系统 | 安全管理区 | 1套 | 新购，实现主要主机的安全加固 |
| 16 | 安全管理平台 | 安全管理区 | 1套 | 新购，实现系统安全管理 |
| 17 | 网络杀毒软件 | 安全管理区 | 1套 | 新购，实现主机杀毒 |
| 18 | USBKEY | 安全管理区 | 30 | 新购，用于SSLVPN和堡垒机登录 |

## 三、服务采购清单

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **服务名称** | **服务类别** | **数量** | **备注** |
| 1 | 系统集成部署 | 系统集成 | 1 | 完成采购设备的集成部署工作 |
| 2 | 应用采用HTTPS协议访问 | 应用安全整改 | 1 | 实现应用HTTPS协议访问，支持信息的加密传输，提供用于加密传输的SSL数据证书 |
| 3 | 升级用户登录认证模块 | 应用安全整改 | 1 | 对现有应用系统增加口令复杂度设置，登录失败处理配置 |
| 4 | 增强数据有效性验证模块 | 应用安全整改 | 1 | 对现有应用系统增加攻击拦截验证功能，提升应用安全性 |
| 5 | 增加应用系统审计模块 | 应用安全整改 | 1 | 对现有应用系统增加应用系统审计模块，对重要用户、重要事件进行审计记录 |
| 6 | 安全配置及策略整改 | 安全策略整改 | 1 | 按照测评整改要求对门户网站中所有的安全配置及策略进行整改，满足复测要求 |
| 7 | 制定安全管理办法 | 安全管理 | 1 | 制定门户网站安全管理制度，明确安全责任 |
| 8 | 制定安全应急预案 | 安全管理 | 1 | 制定门户网站应急预案，明确安全应急处置流程 |

## 四、产品技术参数要求

### 1、千兆边界防火墙

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 指标项目 | 重要性 | 具体要求 | 证明材料 |
| 1 | 规格要求 |  | 网络层吞吐量至少8G，并发连接≥210万，每秒新建连接数≥10万，标准2U机箱，冗余电源，至少支持6个10/100/1000M自适应电口、2个SFP插槽、1个扩展槽以及1个Console口；至少含3年应用识别库、URL分类特征库、病毒防护特征库、入侵防御特征库升级服务。 |  |
| 2 | 部署方式 |  | 产品支持路由、透明、交换以及混合模式接入，满足复杂应用环境的接入需求。支持旁路模式； |  |
| 3 | 网络协议 |  | 所投产品必须支持VTEP（VxLan Tunnel EndPoint）模式接入VxLAN网络，并可作为VXLAN二层、三层网关实现VxLan网络与传统以太网的相同子网内、跨子网间互联互通；支持通过绑定VLAN、VNI（VXLAN Network Identifier）、远程VTEP，手动管理VxLan网络；支持MAC、VNI、VTEP静态绑定； |  |
| 4 | 路由协议 |  | 所投产品必须支持支持静态路由、策略路由及动态路由。策略路由支持用户自定义其优先级，动态路由应至少支持RIP v1/v2/ng， OSPFv2/v3，BGP4/4+协议；必须支持静态和动态多播路由，动态多播路由必须支持PIM-SM（稀疏模式） |  |
| 5 |  | 所投产品必须支持基于策略的路由负载，支持根据应用和服务进行智能选路，支持源地址目的地址哈希、源地址哈希、轮询、时延负载、备份、随机、流量均衡、源地址轮询、目的地址哈希、最优链路带宽负载、最优链路带宽备份、跳数负载等不少于12种路由负载均衡方式，支持基于IPv4或IPv6的TCP、HTTP、DNS、ICMP等方式的链路探测，同时TCP与HTTP可使用自定义目标端口进行测试 |  |
| 6 | 虚拟防火墙功能 | # | 所投产品必须支持将物理防火墙资源，如会话数、安全策略数、源NAT数、目的NAT数，日志存储数量以保留值及最大值的形式自动分配。（投标文件需要提供能够体现上述功能及配置选项的截图） | 是 |
| 7 |  | 所投产品必须支持虚拟防火墙逻辑接口，可以不占用物理网口的情况下实现虚拟系统之间的相互连接、访问。 |  |
| 8 | 访问控制 |  | 所投产品必须支持基于源安全域、目的安全域、源用户、源地址、源地区、目的地址、目的地区、服务、应用、隧道、时间、VLAN等多种方式进行访问控制，并支持地理区域对象的导入以及重复策略的检查 |  |
| 9 |  | 所投产品比如支持基于IPv4/v6地址、应用的会话限制，限制动作包每IP新建、每IP并发、所有IP新建、所有IP并发，且可以基于安全域指定限制方向 |  |
| 10 | 应用识别与控制 |  | 所投产品必须支持应用识别，应用特征库包含的应用数量（非应用协议的规则总数）大于2800种，可深度识别每种应用的属性，为每种应用提供预定义的风险系数，并将应用基于类型、使用场景、数据传输、风险等级等特征分类 |  |
| 11 |  | 所投产品可直观展示不同风险等级的应用在1天（24小时）或一周（7天）内传输流量的绝对数值及占全网流量的百分比。 |  |
| 12 | 病毒防护 |  | 所投产品必须能够对HTTP/FTP/POP3/SMTP/IMAP/SMB六种协议进行病毒查杀 |  |
| 13 |  | 所投产品必须支持基于MD5的自定义病毒签名；支持设置例外特征，对特定的病毒特征不进行查杀 |  |
| 14 | 入侵防御 |  | 所投产品必须支持漏洞防护功能，同时将漏洞防护特征库分类，至少包括缓冲区溢出、跨站脚本、拒绝服务、恶意扫描、SQL注入、WEB攻击等六种分类；漏洞防护支持日志、阻断、放行、重置等执行动作,可批量设置针对某一分类或全部攻击签名的执行动作；支持基于FTP、HTTP、IMAP、OTHER\_APP、POP3、SMB、SMTP等应用协议的漏洞防护 |  |
| 15 |  | 所投产品具备公安部网络安全保卫局颁发的《计算机信息系统安全专用产品销售许可证》（千兆增强级），投标文件需提供证书复印件并加盖厂商公章。 |  |

### 2、SSLVPN

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 指标项目 | 重要性 | 具体要求 | 证明材料 |
| 1 | 规格要求 |  | 单电源，至少支持4个10/100/1000电口，标配不小于1T硬盘，支持最大并发用户数300，包含VPN授权不少于50个。 |  |
| 2 | 基本要求 |  | 支持旁路或串接部署到用户网络。 |  |
| 3 |  | 支持多链路接入、策略路由、链路聚合。 |  |
| 4 | 管理员功能 |  | 管理员可分为状态管理员，系统配置管理员，VPN管理员，应用安全管理员，防火墙管理员，IPsec管理员,日志管理员，系统维护管理员，创建管理员可以为其分配相应的管理员权限。 |  |
| 5 |  | 支持组管理员， 组管理员由系统管理员设定。组管理员可以进到配置端查看组信息，可以基于此组建立第二级的子组，可选择用户，选择主机绑定策略；设置终端安全策略；设置隧道控制策略；设置访问控制策略。 |  |
| 6 | 终端安全 |  | 支持客户端注销后自动清除所有缓存、Cookies、浏览器历史记录、保存的表单信息，实现零痕迹访问。 |  |
| 7 |  | 实现SSL VPN账号与应用系统账号的唯一绑定，VPN资源中的系统只能以指定账号登陆，加强身份认证，防止登录SSL VPN后冒名登录应用系统。 |  |
| 8 | 认证功能 |  | 支持多种认证方式，支持认证方式进行组合 |  |
| 9 |  | 支持硬件特征码绑定，特征码信息无需用户手动设置输入可自动生成，支持用户拥有多个硬件特征码信息。 |  |
| 10 |  | 支持RADIUS双机认证，管理员可定义的Radius 属性组与系统中其他组一样作为授权对象，可实时与RADIUS建立联系，保证用户数据更新，保证认证的高可用性。 |  |
| 11 |  | 支持用户长期不登录时自动锁定，被锁定后需要管理员才能解锁。 |  |
| 12 | 产品资质 |  | 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》，投标文件需提供证书复印件并加盖厂商公章。 |  |

### 3、网络安全审计

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 指标项目 | 重要性 | 具体要求 |  |
|  | 基本要求 |  | 采用专用硬件平台和专用安全操作系统，2U机架式独立硬件（非Windows平台），双电源 |  |
|  |  | 不少于2个10/100/1000BASE-TX管理口、不少于4个SFP光口，不少于6个10/100/1000BASE-T接口。其他所有接口均可作为采集口；不少于2个扩展板卡槽位； |  |
|  | 性能要求 |  | 吞吐量不少于8Gbps |  |
|  | 存储空间 |  | 内置硬盘容量2T、支持扩展双硬盘 |  |
|  | 授权 |  | 监听接口授权数量无数量限制 |  |
|  |  | 配置数据库审计模块 |  |
|  | 审计能力 |  | 支持实名审计，支持802.1x,PPPoE,AD等环境下终端IP地址和用户实名信息或主机信息绑定显示，可显示在线用户的PPPoE账号和AD域用户等信息。 |  |
|  | 支持对HTTP协议进行审计，审计内容包括：访问域，URL引用页、URL分类、http请求类型、http响应类型、请求文件、请求参数、访问行为、发布内容、请求结果、浏览器、服务器、Cookie、返回长度、代理客户端地址、代理上网服务、HTTP响应时间、源目的地址、MAC地址等。 |  |
|  | 支持应用协议行为识别，最少分为12大类，可以把应用协议分组进行审计，用户可以根据需求自行选择审计内容。 |  |
|  | 支持审计Radius协议的认证用户MAC、认证用户名、认证IP、NAS服务器IP。 |  |
|  | 支持Telnet协议的审计，审计内容包括但不限于：用户名、操作命令、返回结果、时间等。 |  |
|  | 支持对即时通讯的审计，可对使用即时消息通讯协议的网络行为审计。 |  |
|  | 支持对网络入侵行为IPS规则的管理和侦听，并对攻击信息详细审计 |  |
|  |  | 支持审计ORACLE、SQL Server、MY SQL、DB2、Sybase、Informix、Postgresql、Kingbase、Cache、Gbase、Dameng、Teradata、Oscar、Mongodb等各类主流数据库系统； |  |
|  | 系统内置SQL语法解析器，可通过正则与非正则方式分析SQL语句的操作类型，操作对象等信息； |  |
|  | 支持数据库绑定变量审计; |  |
|  | 可通过分析、提取语句中绑定变量，审计出访问数据库的源主机名、源主机用户，可监测还原SQL操作语句包括源IP地址、目的IP地址、访问时间、MAC地址、数据库用户名、客户端名称、服务端名称、数据库操作类型、数据库表名、字段名等； |  |
|  | 支持对访问数据库的设备ID、源地址、目的地址、SQL操作响应时间、数据库操作成功、失败的审计； |  |
|  | 支持对针对数据库的XSS攻击行为、SQL注入攻击行为进行审计，并进行实时报警； |  |
|  | 支持网络环境主动扫描，可自动对审计环境范围内包括IP地址、MAC地址、表名、计算机名、数据库名、程序名等在内的资源信息进行提取； |  |
|  |  | 支持330种以上国内常见应用协议行为的自动识别与审计记录。 |  |
|  |  | 支持审计规则的优先级的调整，以防止误报、漏报等发生。 |  |
|  | 支持审计策略的自定义，可将时间、源IP、目的IP、协议、端口、登陆账号、命令作为响应条件进行策略设置。 |  |
|  | 支持数据采集规则定义，对于不关心的数据可不采集，保证系统审计的稳定性与针对性。 |  |
|  | 系统内置高危SQL查询和注入、远程命令执行、跨站脚本攻击等高危指令告警规则。 |  |
|  | 支持以字段名称和字段值作为分项响应条件进行审计策略设置。 |  |
|  |  | 支持流量趋势分析、IP分组流量统计，可以对传输协议、应用协议、应用协议组、源目的地址、源目的端口进行统计分析，可以多条件组合分析。 |  |
|  | 支持基于流的流量分析功能，可对其他设备发送的Netflow进行分析，支持对Netflow v5/v9版本的流量分析。 |  |
|  | 统计报表与告警 |  | 支持WORD、PDF、CVS、EXCEL、HTML等格式导出报表。 |  |
|  | 支持邮件方式自动发送报表。 |  |
|  | 支持频率趋势图、概率统计图、饼图方式进行报表展现，并可导出统计结果报表。 |  |
|  | 支持自定义报表，可以根据不同列集生成更多有实际意义的报表（多达300多种）。 |  |
|  | 支持按照源IP地址、客户端工具等源信息生成报表。 |  |
|  | 支持审计结果多条件组合查询，可以事件发生的时间、用户、访问方式、用户IP、服务器等为查询条件进行组合。 |  |
|  |  | 支持通过邮件、syslog、SNMP方式进行告警。 |  |
|  | 支持对告警信息的发送方式进行设置，以防止告警信息过多，增加邮件服务器压力，至少具备单条发送、归并发送两种方式。 |  |
|  | 支持告警信息同时发送到多个管理对象。 |  |
|  | 支持告警阀值设置，可设置内容包括：连接数值、流量阀值、系统状态阈值。 |  |
|  | 支持报警事件插件的配置管理，例如：事件接收、外发、统计分析、存储等插件。 |  |
|  | 支持系统旁路部署下的攻击阻断；支持防火墙联动方式的阻断。 |  |
|  | 支持告警的统计分析功能，可自定义在线查看统计分析结果，并可根据统计结果生成报表。 |  |
|  | 支持告警分类，告警类型至少分为三类，例如：审计报警、日志报警、流量报警。 |  |
|  | 支持系统报警的自定义查询功能，可自定义查询系统内所有报警事件内容，包括：事件主体、事件客体、报警内容、报警级别、报警触发规则名称等。 |  |
|  | 系统功能 |  | 提供管理员权限设置和分权管理，系统可以对使用人员的操作进行审计记录，可以由审计员进行查询，具有自身安全审计功能。 |  |
|  | 用户可自定义角色，并为角色定义细粒度权限，权限可控制到菜单级。 |  |
|  | 能够对连续失败登陆进行自动锁定，锁定时间可设置。 |  |
|  | 支持系统管理员IP黑白名单，对于无权访问的IP可以隐藏设备自身IP地址。 |  |
|  | 提供审计数据管理功能，可根据时间或磁盘空间状况实现对审计数据的自动备份、删除。 |  |
|  |  | 系统应提供配置向导，简化策略配置过程。 |  |
|  | 支持WEB登录锁定配置，可自定义用户名/密码尝试次数和登录锁定时间。 |  |
|  | 支持WEB登录超时自动登出功能，可自定义WEB端登录超时时间。 |  |
|  | 支持静态密码认证，并对密码的复杂性进行强制要求，如大小写、数字、特殊字符、长度等； |  |
|  | 支持角色自定义功能，可对角色权限进行细粒度划分，权限可控制到菜单级； |  |
|  | 支持双操作系统，当常用系统出现故障可以使用备用系统恢复。 |  |
|  | 支持系统状态的监控功能，可监控系统的CPU、内存、磁盘、网口、运行状态等信息。 |  |
|  | 支持本地磁盘状态的查询和显示，可查询设备磁盘的空间利用率，可通过饼状图、柱状图显示磁盘空间占用情况。 |  |
|  | 支持磁盘规划功能，可通过饼状图、柱状图显示磁盘空间利用率，本地磁盘中的数据可根据对象进行分类并独立进行备份、清理等操作。 |  |
|  |  | 提供系统升级功能，能够通过升级包的方式实现升级。 |  |
|  |  | 支持Syslog、SNMP Trap方式向外发送审计日志。 |  |
|  | 支持以SNMP方式，将系统运行状态提供给第三方网管系统。 |  |
|  | 支持NTP时间同步。 |  |
|  | 支持原始数据包留存，可通过sftp方式从设备中取得已记录的原始数据包。 |  |
|  | 支持自动备份审计日志，可通过FTP方式外送到外部设备，备份文件进行加密，且必须导入设备才能够进行恢复查看。 |  |
|  | 部署方式 |  | 支持单点、多点、多级管理模式 。 |  |
|  | 采用B/S管理方式，不需要单独的管理设备。 |  |
|  | 一体化设备，审计、解析、管理、报警、存储均在一台物理设备上实现。 |  |
|  |  | 支持IPV6环境部署和IPV6环境下网络审计系统全部功能的审计。 |  |
|  | 资质证明 |  | 提供《计算机信息系统安全专用产品销售许可证》，并加盖原厂商公章。 |  |

### 4、千兆服务区防火墙

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 指标项目 | 重要性 | 具体要求 | 证明材料 |
| 1 | 规格要求 |  | 网络层吞吐量至少8G，并发连接≥210万，每秒新建连接数≥10万，标准2U机箱，冗余电源，至少支持6个10/100/1000M自适应电口、2个SFP插槽、1个扩展槽以及1个Console口；至少含3年应用识别库、URL分类特征库、病毒防护特征库、入侵防御特征库升级服务。 |  |
| 2 | 部署方式 |  | 产品支持路由、透明、交换以及混合模式接入，满足复杂应用环境的接入需求。支持旁路模式； |  |
| 3 | 网络协议 |  | 所投产品必须支持VTEP（VxLan Tunnel EndPoint）模式接入VxLAN网络，并可作为VXLAN二层、三层网关实现VxLan网络与传统以太网的相同子网内、跨子网间互联互通；支持通过绑定VLAN、VNI（VXLAN Network Identifier）、远程VTEP，手动管理VxLan网络；支持MAC、VNI、VTEP静态绑定； |  |
| 4 | 路由协议 |  | 所投产品必须支持支持静态路由、策略路由及动态路由。策略路由支持用户自定义其优先级，动态路由应至少支持RIP v1/v2/ng， OSPFv2/v3，BGP4/4+协议；必须支持静态和动态多播路由，动态多播路由必须支持PIM-SM（稀疏模式） |  |
| 5 |  | 所投产品必须支持基于策略的路由负载，支持根据应用和服务进行智能选路，支持源地址目的地址哈希、源地址哈希、轮询、时延负载、备份、随机、流量均衡、源地址轮询、目的地址哈希、最优链路带宽负载、最优链路带宽备份、跳数负载等不少于12种路由负载均衡方式，支持基于IPv4或IPv6的TCP、HTTP、DNS、ICMP等方式的链路探测，同时TCP与HTTP可使用自定义目标端口进行测试 |  |
| 6 | 虚拟防火墙功能 | # | 所投产品必须支持将物理防火墙资源，如会话数、安全策略数、源NAT数、目的NAT数，日志存储数量以保留值及最大值的形式自动分配。（投标文件需要提供能够体现上述功能及配置选项的截图） | 是 |
| 7 |  | 所投产品必须支持虚拟防火墙逻辑接口，可以不占用物理网口的情况下实现虚拟系统之间的相互连接、访问。 |  |
| 8 | 访问控制 |  | 所投产品必须支持基于源安全域、目的安全域、源用户、源地址、源地区、目的地址、目的地区、服务、应用、隧道、时间、VLAN等多种方式进行访问控制，并支持地理区域对象的导入以及重复策略的检查 |  |
| 9 |  | 所投产品比如支持基于IPv4/v6地址、应用的会话限制，限制动作包每IP新建、每IP并发、所有IP新建、所有IP并发，且可以基于安全域指定限制方向 |  |
| 10 | 应用识别与控制 |  | 所投产品必须支持应用识别，应用特征库包含的应用数量（非应用协议的规则总数）大于2800种，可深度识别每种应用的属性，为每种应用提供预定义的风险系数，并将应用基于类型、使用场景、数据传输、风险等级等特征分类 |  |
| 11 |  | 所投产品可直观展示不同风险等级的应用在1天（24小时）或一周（7天）内传输流量的绝对数值及占全网流量的百分比。 |  |
| 12 | 病毒防护 |  | 所投产品必须能够对HTTP/FTP/POP3/SMTP/IMAP/SMB六种协议进行病毒查杀 |  |
| 13 |  | 所投产品必须支持基于MD5的自定义病毒签名；支持设置例外特征，对特定的病毒特征不进行查杀 |  |
| 14 | 入侵防御 |  | 所投产品必须支持漏洞防护功能，同时将漏洞防护特征库分类，至少包括缓冲区溢出、跨站脚本、拒绝服务、恶意扫描、SQL注入、WEB攻击等六种分类；漏洞防护支持日志、阻断、放行、重置等执行动作,可批量设置针对某一分类或全部攻击签名的执行动作；支持基于FTP、HTTP、IMAP、OTHER\_APP、POP3、SMB、SMTP等应用协议的漏洞防护 |  |
| 15 |  | 所投产品具备公安部网络安全保卫局颁发的《计算机信息系统安全专用产品销售许可证》（千兆增强级），投标文件需提供证书复印件并加盖厂商公章。 |  |

### 5、万兆接入交换机

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 重要性 | 指标项目 | 具体要求 | 证明材料 |
| 1 | # | 基本指标 | 交换容量≥2.56Tbps |  |
| 2 |  | 包转发率≥1080Mpps |  |
| 3 | # | 支持48个10/100/1000/10000BASE-T接口； |  |
| 4 |  | 支持≥2个扩展插槽 |  |
| 5 |  | 扩展槽支持万兆、40G板卡 |  |
| 6 |  | 设备高度≤2U； |  |
| 7 |  | 配置需求 | 配置模块化冗余电源； |  |
| 9 |  | 配置模块化冗余风扇，且通风方式为后前通风或前后通风； |  |
| 10 |  | 电源模块与风扇模块均支持热插拔； |  |
| 11 |  | 网络基础功能 | 支持静态路由、RIP、OSPF、BGP；支持等价路由、路由策略、VRRP、策略路由；支持STP/RSTP/MSTP协议；支持STP Root Guard；支持BPDU Guard； |  |
| 12 |  | 支持对端口接收报文的速率和发送报文的速率进行限制；支持报文重定向；支持灵活的队列调度算法，可以同时基于端口和队列进行设置，支持SP、WRR、SP+WRR、WFQ、SP+WFQ多种模式；支持报文的802.1p和DSCP优先级重新标记； |  |
| 13 |  | 大二层功能 | 支持OpenFlow功能； |  |
| 14 |  | 支持VxLAN二层互通、VxLAN集中式网关三层互通功能 |  |
| 15 |  | 支持基于EVPN的分布式二、三层网关功能； |  |
| 16 |  | 虚拟化 | 支持多虚一技术(N:1)，N≥9； |  |
| 17 |  | 支持纵向虚拟化，能够实现组网与自动化上线功能、自动配置功能、集中式转发和本地转发功能、PE下线后的报文持续转发功能、故障设备替换功能； |  |
| 18 |  | 管理功能 | 支持基于Console、SSH、telnet的命令行配置； |  |
| 19 |  | 安全性 | 支持CPU保护功能； |  |

### 6、光纤存储交换机

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 重要性 | 指标项目 | 具体要求 | 证明材料 |
| 1 | # | 端口 | 24端口交换机，8端口激活； |  |
| 2 | # | 接口模块 | 8个8Gb短波SFP； |  |
| 3 |  | 电源 | 单电源； |  |
| 4 |  | 软件支持 | 含Web tools、Zoning软件授权； |  |
| 5 | ★ | 双机 | 与采购人现有博科Brocade300型号光纤存储交换机组成双机，统一对外提供服务。 |  |

### 7、磁盘阵列

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 重要性 | 指标项目 | 具体要求 | 证明材料 |
|  |  | 品牌 | 知名存储品牌，具有自主研发能力，非OEM产品，存储软件具有软件著作权证书 |  |
|  |  | 产品描述 | 多控制器SAN+NAS一体化光纤存储阵列，同时支持SAN和NAS功能（不允许通过额外配置NAS网关方式实现） |  |
|  | # | 体系架构 | 盘控分离；控制器冗余设计，支持在线更换控制器；在线升级存储系统，无须停机，具备控制器故障自动切换和自动重建功能，无单点故障影响数据的有效性。 |  |
|  | # | 控制器 | 本次配置控制器数量≥2，控制器扩展能力≥16，提供控制器扩展能力截图。 | 是 |
|  |  | 掉电保护 | 支持缓存保护，并配置BBU电池保护模组，保证掉电时Cache数据可安全写入Flash或内置SSD硬盘永久保存，实现无限时断电保护Cache数据的目的。 |  |
|  |  | 数据一致性检测 | 从主机端口到硬盘全路径支持基于硬件的并符合业界标准的T10-PI数据一致性检测，保障数据的一致性 |  |
|  | # | 系统缓存 | 双控配置高速缓存≥128GB（缓存不包含SSD磁盘、PCI-E SSD、压缩缓存、NAS缓存等） |  |
|  |  | 后端接口 | 双控配置8个48Gbps SAS3.0磁盘接口 |  |
|  |  | 主机接口 | 本次配置4个8Gb FC主机接口,8个10Gb iSCSI (SFP+)主机接口；配置8个1GE主机接口（电口） |  |
|  | # | 磁盘配置 | 配置11块2.5寸10000转2.4TB SAS盘；配置3块960GB SSD盘。 |  |
|  |  | 磁盘扩展 | 双控最大支持≥1800块企业级硬盘 |  |
|  |  | 在线实时数据压缩 | 支持在线实时压缩功能，必须通过扩展独立压缩卡方式实现 |  |
|  |  | RAID配置 | 支持RAID0/1/5/6/10/50/60及分布式raid，且多种raid可共存于同一磁盘柜； 支持业务无中断的在线转换RAID级别； 支持两种热备技术，热备盘或者热备空间。 |  |
|  |  | 高速磁盘故障恢复 | 采用高速多对多磁盘故障恢复方式，提高恢复速度的同时，可保证磁盘复期间应用的性能。 |  |
|  |  | 管理软件 | 配置图形界面管理软件，支持多种语言（至少包括简体中文和英文），支持多台设备集中管理，支持存储资源管理分析和资源使用历史记录分析，支持性能管理等功能，支持WEB管理，支持CLI管理。支持多种事件通知功能。 |  |
|  |  | 多路径软件 | 配置多路径软件授权，支持存储多路径故障切换、存储多路径故障恢复、存储多路径负载均衡，实现主机与存储设备之间的高可用性，高吞吐率 |  |
|  | # | 自动精简 | 配置全容量许可精简功能，实现存储空间超分配，精简粒度32K、64K、128K、256K可调节，支持创建单卷≥256TB的容量 |  |
|  |  | 克隆 | 配置全容量许可的克隆功能 |  |
|  |  | 快照 | 配置全容量许可快照功能，有效预防各种软故障的发生，快照无需预留空间，后续扩容无需额外购买许可 |  |
|  |  | 卷备份 | 配置全容量许可卷备份功能，有效预防各种软故障的发生，无需预留空间。 |  |
|  | # | QoS | 配置存储QoS授权许可，支持单卷的IOPS、Bandwidth的限制设定 |  |
|  |  | 卷镜像 | 配置卷镜像功能，可实现存储内部，或者不同存储之间的数据同步功能，当其中一个卷离线时，可实现业务无中断。 |  |
|  | # | 自动分层 | 支持存储4层数据自动分层功能，系统自动将动态热点数据提升至高速盘中，以解决动态数据热点的性能问题。 |  |
|  |  | 远程容灾复制 | 支持存储远程复制功能，至少必须包含同步、异步周期和异步复制三种主流模式。 |  |
|  |  | 存储双活 | 支持构建存储双活系统，实现RPO=0,RTO=0，保障数据零丢失，业务零中断。 |  |
|  |  | 存储虚拟化 | 支持存储虚拟化功能，可以整合异构厂商的存储阵列，通过虚拟化功能将存储资源统一管理和分配。 |  |
|  |  | SSD缓存加速 | 支持SSD二级缓存加速功能 |  |
|  | # | 虚拟化支持 | 支持VMware虚拟化场景，获得VAAI/VASA认证，提供vmware官网认证截图和链接。 | 是 |
|  | # | OpenStack | 获得OpenStack Cinder兼容性认证，提供OpenStack官方官网截图及链接。 | 是 |
|  | # | SMI-S | 获得SMI-S v1.6或以上版本的CTP认证并提供截图证明。 | 是 |
|  |  | 电源风扇 | 配置冗余电源、风扇 |  |

### 8、高性能服务器

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 重要性 | 指标项 | 具体要求 | 证明材料 |
| **1** |  | 类型 | 4路2U机架式服务器 |  |
| **2** | ★ | CPU | 核数≥16，主频≥2.1GHz，性能不低于Xeon SP Gold 6130 |  |
| **3** | ★ | CPU数量 | 共配置4颗CPU |  |
| **4** | # | 内存 | DDR4带ECC，主频需>=2666MHz，单条32GB，容量>=256GB |  |
| **5** |  | 内存扩展 | 内存插槽最大可支持>=48 |  |
| **6** | # | 硬盘 | 每台配置：SAS硬盘>=300GB\*2, >=15000RPM;支持热插拔。 |  |
| 硬盘槽位最大可支持>=26 |  |
| **7** | # | SAS RAID控制器 | >=4GB缓存，带Flash或cache备份功能，支持RAID 0/1/5/0+1 |  |
| **8** |  | 网卡 | 4个万兆电口网卡，4口千兆电口网卡 |  |
| **9** |  | HBA卡 | 配置双8Gb接口，配置光模块 |  |
| **10** | # | PCI-E 扩展槽 | 最大可支持10个 |  |
| **11** | # | GPU卡 | 最大支持4块单宽GPU卡 |  |
| **12** |  | 冗余电源 | 满配电源，通过80 Plus认证，高达94%/能效转换率 |  |
| **13** |  | 冗余风扇 | 满配风扇，最大支持6个N+1冗余热插拔风扇 |  |
| **14** |  | 远程管理卡 | 配置独立的远程管理控制端口，支持远程监控图形界面, 可实现与操作系统无关的远程对服务器的完全控制，包括远程的开机、关机、重启、更新Firmware、虚拟软驱、虚拟光驱操作 |  |
| **15** |  | 虚拟化软件 | 支持VMware vSphere6.0及以上等虚拟化软件 |  |

### 9、服务器硬盘

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 重要性 | 指标项目 | 具体要求 | 证明材料 |
| 1 |  | 接口 | 服务器用SAS硬盘，支持热插拔 |  |
| 2 |  | 速率 | >=15000RPM |  |
| 3 |  | 容量 | >=600GB |  |

### 10、万兆网卡

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 重要性 | 指标项目 | 具体要求 | 证明材料 |
| 1 |  | 接口 | 支持PCI-E接口，每块网卡配置双万兆电口 |  |
| 2 |  | 速率 | ≥10GB |  |
| 3 |  | 支持的操作系统 | 支持Windows linux主流操作系统及虚拟化软件系统 |  |

### 11、千兆安管区防火墙

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 指标项目 | 重要性 | 具体要求 | 证明材料 |
| 1 | 规格要求 |  | 网络层吞吐量至少8G，并发连接≥210万，每秒新建连接数≥10万，标准2U机箱，冗余电源，至少支持6个10/100/1000M自适应电口、2个SFP插槽、1个扩展槽以及1个Console口；至少含3年应用识别库、URL分类特征库、病毒防护特征库、入侵防御特征库升级服务。 |  |
| 2 | 部署方式 |  | 产品支持路由、透明、交换以及混合模式接入，满足复杂应用环境的接入需求。支持旁路模式； |  |
| 3 | 网络协议 |  | 所投产品必须支持VTEP（VxLan Tunnel EndPoint）模式接入VxLAN网络，并可作为VXLAN二层、三层网关实现VxLan网络与传统以太网的相同子网内、跨子网间互联互通；支持通过绑定VLAN、VNI（VXLAN Network Identifier）、远程VTEP，手动管理VxLan网络；支持MAC、VNI、VTEP静态绑定； |  |
| 4 | 路由协议 |  | 所投产品必须支持支持静态路由、策略路由及动态路由。策略路由支持用户自定义其优先级，动态路由应至少支持RIP v1/v2/ng， OSPFv2/v3，BGP4/4+协议；必须支持静态和动态多播路由，动态多播路由必须支持PIM-SM（稀疏模式） |  |
| 5 |  | 所投产品必须支持基于策略的路由负载，支持根据应用和服务进行智能选路，支持源地址目的地址哈希、源地址哈希、轮询、时延负载、备份、随机、流量均衡、源地址轮询、目的地址哈希、最优链路带宽负载、最优链路带宽备份、跳数负载等不少于12种路由负载均衡方式，支持基于IPv4或IPv6的TCP、HTTP、DNS、ICMP等方式的链路探测，同时TCP与HTTP可使用自定义目标端口进行测试 |  |
| 6 | 虚拟防火墙功能 |  | 所投产品必须支持将物理防火墙资源，如会话数、安全策略数、源NAT数、目的NAT数，日志存储数量以保留值及最大值的形式自动分配。（投标文件需要提供能够体现上述功能及配置选项的截图） | 是 |
| 7 |  | 所投产品必须支持虚拟防火墙逻辑接口，可以不占用物理网口的情况下实现虚拟系统之间的相互连接、访问。 |  |
| 8 | 访问控制 |  | 所投产品必须支持基于源安全域、目的安全域、源用户、源地址、源地区、目的地址、目的地区、服务、应用、隧道、时间、VLAN等多种方式进行访问控制，并支持地理区域对象的导入以及重复策略的检查 |  |
| 9 |  | 所投产品比如支持基于IPv4/v6地址、应用的会话限制，限制动作包每IP新建、每IP并发、所有IP新建、所有IP并发，且可以基于安全域指定限制方向 |  |
| 10 | 应用识别与控制 |  | 所投产品必须支持应用识别，应用特征库包含的应用数量（非应用协议的规则总数）大于2800种，可深度识别每种应用的属性，为每种应用提供预定义的风险系数，并将应用基于类型、使用场景、数据传输、风险等级等特征分类 |  |
| 11 |  | 所投产品可直观展示不同风险等级的应用在1天（24小时）或一周（7天）内传输流量的绝对数值及占全网流量的百分比。 |  |
| 12 | 病毒防护 |  | 所投产品必须能够对HTTP/FTP/POP3/SMTP/IMAP/SMB六种协议进行病毒查杀 |  |
| 13 |  | 所投产品必须支持基于MD5的自定义病毒签名；支持设置例外特征，对特定的病毒特征不进行查杀 |  |
| 14 | 入侵防御 |  | 所投产品必须支持漏洞防护功能，同时将漏洞防护特征库分类，至少包括缓冲区溢出、跨站脚本、拒绝服务、恶意扫描、SQL注入、WEB攻击等六种分类；漏洞防护支持日志、阻断、放行、重置等执行动作,可批量设置针对某一分类或全部攻击签名的执行动作；支持基于FTP、HTTP、IMAP、OTHER\_APP、POP3、SMB、SMTP等应用协议的漏洞防护 |  |
| 15 |  | 所投产品具备公安部网络安全保卫局颁发的《计算机信息系统安全专用产品销售许可证》（千兆增强级），投标文件需提供证书复印件并加盖厂商公章。 |  |

### 12、安全管理服务器

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 重要性 | 指标项目 | 具体要求 | 证明材料 |
| 1 |  | 类型 | 2路2U机架式服务器 |  |
| 2 | ★ | CPU | 核数≥12，主频≥2.1GHz |  |
| 3 | ★ | CPU数量 | 共配置2颗CPU |  |
| 4 | # | 内存 | DDR4带ECC，主频需>=2400MHz，单条32GB，容量>=64GB |  |
| 5 |  | 内存扩展 | 内存插槽最大可支持>=12 |  |
| 6 | ★ | 硬盘 | 每台配置：SAS硬>=600GB\*6, >=10000RPM,支持热插拔。 |  |
|  | 硬盘槽位最大可支持>=16 |  |
| 7 | # | SAS RAID控制器 | >=2GB缓存，带Flash或cache备份功能，支持RAID 0/1/5/0+1 |  |
| 8 | # | 网卡 | 4口千兆电口网卡 |  |
| 9 |  | PCI-E 扩展槽 | 最大可支持10个 |  |
| 10 |  | GPU卡 | 支持8块单宽GPU卡 |  |
| 11 |  | 冗余电源 | 满配电源 |  |
| 12 |  | 冗余风扇 | 满配风扇 |  |
| 13 |  | 远程管理卡 | 配置独立的远程管理控制端口，支持远程监控图形界面, 可实现与操作系统无关的远程对服务器的完全控制，包括远程的开机、关机、重启、更新Firmware、虚拟软驱、虚拟光驱等操作 |  |

### 13、堡垒机

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 指标项目 | 重要性 | 具体要求 | 证明材料 |
| 1 | 规格要求 |  | 至少配置4个千兆电口、支持2个接口扩展槽位，至少内置4TB硬盘，单电源，支持液晶屏，图形并发不小于100，字符并发不小于300，包含100个被管资源数授权。 |  |
| 2 | 部署方式 |  | 物理旁路，逻辑串联模式，不影响正常业务流量 |  |
| 3 |  | HA双机热备 |  |
| 4 |  | 支持基于水平可扩展的集群化架构设计与部署，支持跨地域、跨数据中心，多层次部署。 |  |
| 5 |  | 支持NAT地址映射部署，通过映射后的IP地址访问堡垒机 |  |
| 6 | 用户 |  | 支持多因子方式认证，包括手机短信、手机令牌、USBKEY、动态令牌。 |  |
| 7 |  | 支持微信小程序手机令牌 |  |
| 8 |  | 支持用户的IP地址（黑名单或白名单）和MAC地址限制（黑名单或白名单）限制，非法地址无法登陆 |  |
| 9 | 资源管理 |  | 支持SSH、RDP、TELNET、VNC、FTP、SFTP、SCP、x11、Rlogin协议主机，支持发布MySQL、SQL Server、Oracle、IE、Firefox、Chrome、VNC Client、SecBrowser、VSphere Client类型应用。 |  |
| 10 |  | 支持资源按标签管理，每个用户可以给每个资源打10个标签 |  |
| 11 |  | 支持导入阿里云、华为云、腾讯云和Ucloud等平台云主机 |  |
| 12 |  | 支持TELNET、SSH协议资源使用普通账户自动切换到root（或enable）账户 |  |
| 13 | # | 无需安装任何客户端，便可windows、linux、MAC OS等类操作系统登录堡垒机，并访问管理资源；支持IE、Edge、Chrome、FireFox、Safari等主流浏览器， |  |
| 14 |  | 支持查看改密日志，了解改密账户总数、改密成功数量、改密失败数量和未修改数量 |  |
| 15 | 策略 |  | 访问控制策略基于用户、用户组、资源账户、账户组、有效期、文件管理控制、文件传输控制（上传、下载）、RDP剪切板控制、时间限制、IP限制进行设置。 |  |
| 16 |  | 访问控制策略支持配置双人授权候选人，针对核心设备，需要管理员现场审批才能操作。 |  |
| 17 |  | 支持查看改密日志，了解改密账户总数、改密成功数量、改密失败数量和未修改数量；改密日志支持下载，查看改密前后密码变化 |  |
| 18 | 运维 |  | 批量登录：支持SSH、RDP、TELNET、VNC协议资源的批量登录功能； |  |
| 19 |  | 提供类似云盘形式的文件存储，支持RDP、SSH、VNC协议类型主机的文件上传和下载，并进行审计； |  |
| 20 | # | 会话协同：运维过程中支持会话协同，可邀请其他用户参与、协助操作。会话协同过程中，支持参与者控制会话，同时支持创建者强制获取控制权。支持多个参与者使用相同的会话邀请链接进入会话。 |  |
| 21 |  | 预置命令：支持字符协议预置命令功能，可添加15个经常使用的命令在系统当中。 |  |
| 22 | 审计 |  | 系统内置多种系统报表和运维报表模板，支持按日、周、月为周期，自动生成报表。 |  |
| 23 |  | 对剪切板拷贝文件行为和文本信息内容的记录，并支持通过搜索文本内容关键字定位审计回放。 |  |
| 24 |  | 离线回放重现运维人员对资源的所有操作过程，并支持回放文件下载到本地播放，在线回放过程支持播放速度调整、拖动、暂停、停止、重新播放等播放控制操作。 |  |
| 25 | 产品资质 |  | 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》，投标文件需提供证书复印件并加盖厂商公章。 |  |

### 14、漏洞扫描系统

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 指标项目 | 重要性 | 具体要求 | 证明材料 |
| 1 | 规格要求 |  | 标准1U机架式，1T硬盘，液晶面板显示，配置至少4个10/100/1000M自适应电口，2个扩展插槽, 2个USB口，1个Console口，单电源。Web扫描域名无限制，Web扫描任务并发数支持至少15个域名。系统扫描IP地址无限制，支持扫描A类、B类、C类地址，系统扫描至少支持100个IP地址并行扫描；至少含三年漏洞特征库升级服务。 |  |
| 2 | 系统架构 |  | 产品具备B/S架构设计，并采用SSL加密通信方式，用户可以通过浏览器远程方便的对产品进行管理。 |  |
| 3 |  | 产品界面友好，提供多种界面主题风格、可以定义导航栏、页面、页脚等细节，提供个性化的管理界面 |  |
| 4 | 网络适应性 |  | 产品具备旁路部署方式，不影响网络结构 |  |
| 5 |  | 产品具备DNS配置，本地可以对互联网远端的Web网站进行漏洞扫描 |  |
| 6 | 资产探测 |  | 产品具备以树形结构方式管理，针对树形结构的资产呈现资质风险 |  |
| 7 |  |  | 产品具备对检测耗时、起始/结束时间、检测进度、网页数、漏洞数、检测周期等详细信息提供实时在线状态查询 |  |
| 8 |  |  | 产品需支持多种扫描方式，提供对IP、域名、安全域、批量检测等目标扫描方式 |  |
| 9 | 系统扫描 |  | 产品应具备操作系统、数据库、网络设备等主流系统的漏洞库列表，并提供至少20种以上的漏洞库分类（请提供相应截图证明） | 是 |
| 10 |  | 产品漏洞库列表数量必须大于20000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CVE、CNCVE、CNNVD、CNVD、Bugtraq等主流标准兼容 |  |
| 11 |  | 产品具备对主流的数据库软件的漏洞检查，支持Oracle、MySQL、SQL server、DB2等数据库的安全漏洞检查，并提供至少3000种相关漏洞库 |  |
| 12 |  | 产品具备对DNS服务的安全漏洞检查，包括DNS缓存中毒、DNS拒绝服务漏洞、签名欺骗等至少100种以上的相关漏洞库 |  |
| 13 | Web安全 |  | 产品具备基于OWASP组织发布的TOP 10攻击类型进行Web漏洞分类 |  |
| 14 |  | 产品具备对网页暗链、敏感词汇、网站木马的检测 |  |
| 15 |  | 产品具备对网站目录进行扫描识别，并用树形结构展示网站架构 |  |
| 16 |  | 产品需支持对Web网站漏洞扫描的同时，查看网站漏洞情况和Web目录结构，数据进行实时同步呈现 |  |
| 17 | 口令破解 |  | 产品具备专用的口令破解字典，包括密码字典、用户名字典、组合字典多种口令破解字典 |  |
| 18 |  | 产品具备SMB、TELNET、FTP、SSH、POP3、MSSQL、MYSQL、ORACLE、DB2、SNMP协议进行口令猜测 |  |
| 19 |  | 产品具备字典上传功能，基于协议、口令类型的字典自定义设置 |  |
| 20 | 产品资质 |  | 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》，投标文件需提供证书复印件并加盖厂商公章。 |  |

### 15、安全加固系统

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 重要性 | 指标项目 | 具体要求 | 证明材料 |
|  | # | 总体要求 | 4台服务器授权，对文件进程账号管理网络访问进行统一控制 |  |
|  |  | 监控内容 | 对系统的CPU、内存、磁盘、网络资源进行监控，当这些资源的使用状况超过设置的阀值时将进行报警，以提前发现资源不足、滥用问题 |  |
|  |  | 配置管理 | 配置可以导入导出，可以保存文本格式供留档 |  |
|  |  | 管理平台 | 可以提供B/S和C/S两种管理模式选择。 |  |
|  |  | 密码管理 | 账户密码保护，设定密码复杂度要求、密码长度、最长周期、最短周期。 |  |
|  |  | 完整性检查 | 可以针对文件、服务进行定期完整性检查，发现异常及时告警。 |  |
|  |  | 文件强制访问控制 | 具备内核级文件/目录强制访问控制。允许对文件/目录配置用户或进程以读、写、禁止访问等权限访问的安全策略。还可以通过角色控制，对主体客体的标记来设置不同权限，来实现对文件的细致化的管理控制 |  |
|  |  | 进程强制访问控制 | 提供防止非法中断进程的功能。 |  |
|  |  | 日志 | 审计功能可以记录安全策略的修改、以及与之相关的任何违规操作。并提供日志查询、删除、备份和导出。支持文件、服务的完整性检查。 |  |
|  |  | 日志集中 | 通过syslogd的结合可以把日志集中到第三方日志服务器 |  |
|  |  | 报警 | 利用邮件等方式对违反策略的行为进行报警 |  |
|  |  | 认证方式 | 运用ukey证书和密码进行双重身份认证。 |  |
|  |  | 三权分立 | 能够限制超级用户的权限，分割为安全管理员,操作员,审计员,相互制约。 |  |
|  |  | 系统自防护 | 保护系统自身进程不被异常终止、伪造、信息注入。 |  |
|  |  | 可操作性 | 完全兼容系统，专业的、人性化的操作界面，运行开销小，不会引起能察觉的系统延时，对用户透明。 |  |
|  |  | 资质 | 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》，投标文件需提供证书复印件并加盖厂商公章。 |  |

### 16、安全管理平台

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 指标项目 | 重要性 | 具体要求 | 证明材料 |
| 1 | 基本要求 |  | 该系统为一套统一的、完整的软件产品，采用B/S架构。其中，管理中心内嵌数据库，用户无需另外安装数据库管理系统；管理客户端基于浏览器，无需安装其他客户端软件，至少包含50个点的授权。 |  |
| 2 | 性能 | # | 事件采集不低于30000条/秒；事件处理不低于10000条/秒；数据库中数据量不小于50G时数据查询结果返回时间小于3秒 |  |
| 3 | 管理范围 |  | 能够集中监控网络中的主机设备、网络设备、安全设备、应用系统。具体包括：交换机、路由器、防火墙、Windows服务器、AIX服务器、Linux服务器、HP-UX服务器、Solaris服务器、SQL Server、Oracle、DB2、Sybase、MySQL数据库系统、webshpere/ weblogic中间件、Mail/Web/FTP/DNS/DHCP/WINS和LDAP服务。 |  |
| 4 | 资产管理 |  | 可对网络中的IP资产进行管理，支持以安全域的方式对资产进行分组，资产的属性包括安全CIA指标，支持自定义资产属性，可根据需要对资产属性进行任意扩展。 |  |
| 5 | 综合拓扑管理 | # | 支持网络拓扑发现，自动生成网络拓扑图，支持分层显示和全局显示两种展现方式。在全局显示模式下，能够在一个拓扑图上显示三层、二层网络设备和终端设备。拓扑图上能够显示节点之间的链路连接，并标示流量值。如果节点出现故障，拓扑图节点能够显示为红色。支持对拓扑图的鸟瞰、缩放、导出、导入、更换底图、编辑。内置ping、tracerouter、telnet等常用工具，可直接调用。通过拓扑地图，用户可以调用设备的http接口、telnet接口、ssh/ssh2接口实现对设备的直接访问和控制。 |  |
| 6 | 机房物理视图管理 |  | 支持机房和机架物理拓扑显示，用户可以直观地看到每个机架上的每台设备的运行状态，出现问题就会闪烁告警。用户点击机架上的每个设备，可以进入这个设备的明细监控界面。支持拓扑图和机架视图中的设备的双向定位。支持机房3D图形显示 |  |
| 7 | 真实设备面板图 |  | 用户可以看到设备的面板图，并可以针对面板上的接口进行实时监控和设置，进行形象化管理。 |  |
| 8 | 智能监控频道 | # | 从总体上把握网络中各种IT资源整体运行情况的界面。通过智能监控频道，用户可以快速导航到系统的各个功能界面，可以看到当前企业和组织的整体健康等级。用户可以自定义频道，每个频道都能够自由组织视图，包括视图的布局和显示的内容。监控频道中的每个窗口都能够移动、放大、缩小，窗口中显示的统计和摘要信息都能够点击、下钻、查看明细。监控频道能够最大化显示，作为运维中心的主控界面，在大屏幕或者投影银幕上呈现出来（要求提供产品功能截图） | 是 |
| 9 | 主机监控 |  | 能对主机操作系统进行监控。不仅能够检测主机性能，还能够检测主机安装的软件信息、主机进程信息、主机网络连接信息、主机服务运行信息等。 |  |
| 10 | 网络和安全设备监控 |  | 网络设备属性，网络设备状态监控，网络性能监控，cpu利用率监控，内存利用率监控，接口监控，设备面板管理，可以对重点设备的重点端口进行流量监控，且可以配置告警阈值。 |  |
| 11 | 日志采集 |  | 通过 SNMP Trap、Syslog、数据库、文件、NetFlow等多种方式完成数据收集功能。 |  |
| 12 | 日志归一化处理 |  | 日志收集后进行字段和安全等级的归一化处理，并保留原始日志，方便用户对关键日志快速定位。（要求提供产品功能截图） | 是 |
| 13 | 日志历史查询 |  | 所有日志采用统一的日志查询界面，简单实用，快捷方便。用户可以自定义各种查询场景，并以树形结构组织。 |  |
| 14 | 日志实时分析和统计 |  | 监控管理人员可以通过日志分析对来自企业和组织所有的日志进行实时查询、分析和统计，从而快速识别安全事故。所有的日志分析结果都以场景的方式列举出来，管理人员可以方便的在各种分析场景之间快速切换，提高分析工作的效率。管理员可以自定义日志分析的场景。对于分析结果可以通过柱图、饼图、曲线图等形式形象地展示出来，自动实时刷新。  日志实时分析必须在内存中完成，而不借助数据库和文件系统系统内置超过30种查询场景。 |  |
| 15 | 事件追溯 | # | 在实时监视中，对于关联事件，用户可以进行追溯，查看导致该关联事件的所有原始事件（要求提供产品功能截图） | 是 |
| 16 | 事件定位 |  | 能够在世界地图上实时定位事件源/目的IP地址的地理位置（包括二维及三维显示方式）（要求提供产品功能截图） | 是 |
| 17 | 事件趋势分析 |  | 用户可以对关心的事件IP地址进行趋势分析，对一段时间内的网络流量或者网络连接数进行时间切片统计，并描绘趋势曲线 |  |
| 18 | 事件可视化 |  | 系统能够将数千条事件记录及其这些事件之间的关联关系变成一幅事件图，形象地展现出当前网络安全状态，一目了然。（要求提供产品功能截图） | 是 |
| 19 | 事件调查 |  | 在实时监视中，管理员通过事件调查工具可以对某条感兴趣的日志中的源IP地址、目的IP地址、或者目的端口进行相关性日志检索。 |  |
| 20 | 事件分配 |  | 用户在实时监视的过程中如果发现某条事件的相关属性需要持续予以关注，可以将该事件分配到黑白名单中。 |  |
| 21 | 关联规则 |  | 提供可视化的规则编辑器，利用编辑器，可灵活方便地生成任意关联分析规则。（要求提供产品功能截图）  规则分为系统预定义规则和用户自定义规则两大类；用户在制定规则的时候，既可以设定审计的触发条件，也可以设定触发审计后的自动响应动作；规则编写支持各种运算符，还支持引用外部资源，包括过滤器、资产属性、自定义资源、递归规则、过滤器插件、黑白名单，等等。用户可以对规则触发条件设置计数。 | 是 |
| 22 | 告警与响应管理 |  | 自动采集和存储IT计算环境中的各类告警信息，并将所有的告警记录按发生时间、告警状态、事件类型、事件等级、源设备IP、源设备类型等信息列表显示，对告警信息进行分析和统计。产生的告警信息能够通过邮件、短信、控制台弹出窗口、snmp trap、执行预定义参数脚本程序的方式进行自动化响应。 |  |
| 23 | 产品资质 |  | 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》，投标文件需提供证书复印件并加盖厂商公章。 |  |

### 17、网络杀毒软件

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 重要性 | 指标项目 | 具体要求 | 证明材料 |
|  | # | 基本要求 | 可安装10台服务器授权 |  |
|  |  | 支持操作系统 | 支持Windows系列、Linux系列的多种主流操作系统平台，支持64位操作系统 |  |
|  |  | 管理控制台 | 支持系统的集中管理、策略配置、报表查看等功能。可安装在Windows Server 2008/Windows Server 2012上。 |  |
|  |  | 管理控制台支持实时显示客户端的状态，并可导出已安装所有客户端详细报表 |  |
|  |  | 升级方式 | 支持病毒库无缝主动式智能升级，支持全网统一自动升级，不需要人为干涉 |  |
|  |  | 产品资质 | 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》，投标文件需提供证书复印件并加盖厂商公章。 |  |

### 18、USBKEY

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 重要性 | 指标项目 | 具体要求 | 证明材料 |
|  |  | 基本要求 | 提供USBKEY介质及数字证书，证书确保与提供的SSLVPN、堡垒机产品配合使用。 |  |
|  |  | 产品算法 | 支持国密SM2算法，支持RSA 1024、2048位长密钥。 |  |
|  |  | 证书认证 | 支持在线认证 |  |

## 五、服务技术要求

### 1、项目组团队及成员要求

（1）投标人必须有详细项目管理组织架构，项目组成员不少于12人（包括2名驻场人员）。

（2）项目组成员具有网站等级保护建设或整改项目经验，具有修改门户应用系统的能力。

（3）项目组中除了项目经理外至少有一名成员具有高级工程师职称，至少有3名工程师具有网站等级保护建设或整改项目经验，提供最终用户证明材料或运维服务合同中列有相关人员名单。

### 2、系统集成部署要求

（1）根据招标人要求，提供门户系统整体集成部署方案，重点说明如何做好新旧设备的整合，确保系统停机时间小于24小时。

（2）根据系统集成方案，完成设备的到货、上架、布线、加电、联调测试等工作，所有集成所需线缆包含在系统集成费中。

（3）协助招标人开展培训准备工作，完成要求的培训工作。

（4）协助招标人开展整体试运行、验收工作，完成等保复测工作。

（5）合同签订之日起40日内设备到货，90日内完成系统集成调试工作。

（6）集成调试工作完成后，提供系统软件的安装、设备调试、使用等培训。

### 3、系统二次开发及策略设置要求

（1）应用采用HTTPS协议访问：对系统中重要的数据、报文或会话过程采用经国家密码管理局认可的密码技术进行加密，保证通信过程中数据的完整性。通过系统改造，实现应用系统通过HTTPS协议访问，支持信息的加密传输，提供用于加密传输的SSL数字证书。

（2）升级用户登录认证：对现有应用系统增加口令复杂度设置，登录失败处理设置，提升应用系统的安全性。

（3）增强数据有效性验证：对现有应用系统增加攻击拦截验证功能，提升应用安全性。对系统功能类模块增加数据有效性检验，使之符合基本逻辑校验、并对SQL注入类攻击用到的特殊字符以及脚本语句等进行校验，保证系统数据的完整性。

（4）增加应用系统审计模块：对现有应用系统增加应用系统审计模块，对重要用户、重要事件进行审计记录。

（5）安全配置及策略整改：按照门户系统测评整改要求对门户网站中所有的安全配置及策略进行整改，满足等保复测要求。

（6）合同签订之日起60日内完成系统二次开发和策略设置工作。

### 4、管理制度编写要求

（1）制定门户网站安全管理制度：明确安全责任单位、责任人，制定安全岗位，进行安全事件分类，制定安全事件处理流程等。

（2）制定门户网站安全应急预案：明确安全应急处置流程，提供安全应急演练方案等。

（3）合同签订之日起30日内完成管理制度编写工作。

### 5、售后服务要求

★（1）本次招标采购的全部软硬件产品及技术服务需要提供自项目验收之日起3年保修期。

（2）投标人承诺提供自项目验收之日起半年驻场服务，提供5\*8小时驻场工程师2名，工程师需具有大学本科学历，具有安全设备运维经验和软件开发经验，驻场服务地点为招标人设备托管机房。

（3）投标人承诺在保修期内提供重大活动期间的重保服务。

（4）保修期内，设备故障发生后，自接到通知起，工作时间（按告知时间计算）中标人应在1小时内到现场，非工作时间（如晚间、周末、节假日等）中标人应在6小时内到现场；到达现场后，最长24小时解决问题。