**中国银行间市场交易商协会内网安全工程二期项目招标文件技术说明书**

1. 项目概述
	1. 项目背景

中国银行间市场交易商协会是由市场参与者自愿组成的，包括银行间债券市场、同业拆借市场、外汇市场、票据市场和黄金市场在内的银行间市场的自律组织，会址设在北京。经过五年的发展，目前协会秘书处共下设十个部门，专职工作人员超过100名。自协会成立至今，协会内网系统一直承载着协会专职人员的日常工作，贮存着协会重要业务数据。目前，内网中部署的OA系统、非金融企业债务融资系统、做市商评价系统、会员系统等重要信息系统，对协会工作的正常运转起到着重要的作用。除此之外，结合协会未来工作发展需求，与协会有着密切业务往来的下属单位以及在外出差的协会内部人员，也存在着使用协会内网办公的需求。

* 1. 项目建设的目标

通过协会内网系统实现业务运转、信息共享、数据分析，显著提高工作效率和决策水平。内网系统已成为协会日常工作不可或缺的重要组成部分，协会内部的大量数据文件和信息都通过内网进行传递。

计算机网络的普及让信息的获取、共享和传播更加方便，但同时由于网络分布部署开放共享的特点，使得重要信息资源处于一种高风险的状态，很容易受到来自系统内部和外部的非法访问。根据相关统计资料显示：超过85%的安全威胁来自企事业单位内部，而并非由病毒和外来黑客引起。因此在网络互联互通实现信息快速交换的同时，如何加强内网的安全性，防止关键数据从网络中泄漏出去，是信息安全规划中的重点项目之一。

根据协会内网信息系统的业务特点，系统的可持续服务能力和数据安全性水平至关重要。内网信息安全建设主要完成以下工作：一是保持信息系统持续地、稳定地运行是信息安全工作的基础，需提高系统鲁棒性，在高风险区域部署安全防护系统，防范由于遭受攻击导致系统无法运行、无法提供基本服务的情况；二是防止信息系统被非法侵入，保证数据的保密性、可靠性、完整性，防止攻击者盗取或篡改重要数据；三是对内网中的各类操作进行记录，保证对于各类事件留存足够的记录供事后审计需要；四是对内网安全防护措施进行扫描，及时发现并处理可能出现的漏洞；五是对办公网络终端进行管理，限制非法外联和非法接入等行为，保护内网安全；六是建立异地灾备机制，对灾难进行预防。

* 1. 项目建设的原则

根据前述对协会内网安全现状的需求分析，提出针对性的设计及部署说明，方案的设计充分考虑了以下因素，通过合理、科学的产品设计和部署，健全的安全管理制度，最终将协会内网应用系统建设成为高可靠、高安全、高性能的系统平台：

**体系化设计原则**

系统设计应充分考虑到各个层面的安全风险，构建完整的安全防护体系，充分保证系统的安全性，在信息安全产品和技术方案在设计和实现的全过程中应该有具体的措施来充分保证其安全性。

**结构化原则**

协会内的网络系统是直接承载着协会内的所有信息交互，因此在网络的基础架构上采用了三层网络体系架构，即核心层-汇聚层-接入层。核心层主要负担整体网络的上层策略定义，数据分流、分类、安全等；汇聚层起到为核心层设备分担承载数据，减少核心层非核心数据的处理，加快内网数据的交换速度，增加核心层数据的处理能力；接入层则承担着基础用户的接入及最终策略的终端实现。

**鲁棒性原则**

对于协会内核心层的应用设备来言，如果故障将直接影响全体网络，所以对于这些重要区域的设备要考虑其安全性，不单要从软件、策略等方面考虑，还要考虑其物理方面的安全，即设备的多路负载，实现核心层设备冗余部署，保障核心系统稳定运行。

**先进性原则**

安全体系建设规模庞大，意义深远。对所需安全产品提出了很高的要求。必须认真考虑各类安全产品的技术水平、合理性、稳定性和安全性等特点。

**实用、高效、可扩展原则**

安全体系所采用的产品，便于操作、实用高效。随着技术发展，信息系统也将发生各种变化，在系统实施过程中，系统的结构、配置也会发生变化，系统的安全工程要有一定的灵活性来适应这种变化，做到层次性、体系性，既有利于系统的安全，又有利于系统的扩展。

**管理集中化原则**

对于网络主机及网络设备，无论是交换机、防火墙、还是路由器等，都应集中在统一的网络管理框架下，实现对网络的控制、管理、设置和调整，提供对网络的配置、流量监测、故障报警、网络安全和网络计费等多种管理功能。实现对全网安全状况进行全面的监控、分析、处理、维护。针对内网终端安全防护的这一薄弱环节，建设有效的网络终端设备认证、接入认证及用户身份认证机制，从终端源头上控制网络的不安全因素。安全管理平台的建设是内网信息安全的关键环节。

**分层次建设原则**

考虑到协会信息系统安全建设的周期性，在内网安全体系建设中，必须为后期安全建设进行考虑。

**开放性和标准化原则**

在结构上实现真正开放，基于国际开放式标准，开放的网络使用户可以自由地选择不同厂家的产品，不会受到某些厂家专有技术的限制，最大程度地保护用户的利益。网络的设计基于国际标准，网络设计采用标准的接口和规范、协议，使不同厂家的设备可以顺利地连接。

**保护现有投资原则**

在本次网络设计方案中，应最大化的保护原有的投资，避免因为增加新型设备而将原有设备闲置。

**规范性**

符合公安部和中国人民银行等上级机构信息安全建设规范，符合ITIL，ISO9001等国际相关质量和安全规范。

1. 所需硬件设备及软件
	1. 漏洞扫描系统

产品需求：

|  |  |
| --- | --- |
| 产品 | 数量 |
| 漏洞扫描系统 | 1套 |

漏洞扫描系统配置和集成要求如下：

|  |  |
| --- | --- |
| 指标体系 | 指标项 |
| **端口** | ≥2个千兆电口，适用于千兆流量网络扫描 |
| **内存** | ≥1G |
| **漏洞分析** | 可全面检可猜测的账号和口令、缺失的安全补丁、木马后门、开启的不安全服务、不正当的配置、不正确的系统登陆权限等 |
| **漏洞管理** | 漏洞数目≧3000条，并提供相应的漏洞知识库，定期发布漏洞更新包 |
| **扫描性能** | 1、扫描对象：主流的操作系统（windows/linux/unix等）、主流的数据库（sql server/oracle等）、主流的应用服务（www/ftp/telnet/smtp等）、网络接入设备（路由器、交换机等）、网络安全设备（防火墙、IDS等）；2、支持多任务并发扫描，多主机并发扫描，多线程并发扫描；3、负面影响：网络性能影响比率＜3%，主机性能影响比率＜5%，网络带宽占有量≦30k/s。 |
| **扫描内容** | 检查结果的内容包括主机信息、端口信息、账号信息、服务信息、漏洞信息等，能为漏洞修补工作提供指导，为风险管理提供数据支持。 |
| **产品资质** | 《计算机信息系统安全专用产品销售许可证》《涉密信息系统产品检测证书》《计算机软件著作权登记证书》（具备国内自主知识产权）《国家信息安全测评信息安全服务资质证书（二级）》 |

* 1. 数据库审计系统

产品需求：

|  |  |
| --- | --- |
| 产品 | 数量 |
| 数据库审计系统 | 1套 |

数据库审计系统配置和集成要求如下：

|  |  |
| --- | --- |
| 指标体系 | 指标项 |
| **性能指标** | 1、支持数据库实例数≥42、支持Oracle、SQL server、DB2、Mysql等主流数据库B/S架构，采用HTTPS方式远程安全管理3、≥100/1000M\*4个自适应以太网口；4、存储空间大于1T，可以满足客户3-6个月的日志存储要求；日志可以导出； |
| **细粒度审计** | 1、通过对不同数据库的SQL语义分析，提取出SQL中相关的要素（用户、SQL操作、表、字段、视图、索引、过程、函数、包**…**）2、不仅对数据库操作请求进行实时审计，而且还可对数据库执行状态、返回结果、返回内容进行完整的还原和审计3、实时监控来自各个层面的所有数据库活动，包括来自应用系统发起的数据库操作请求、来自数据库客户端工具的操作请求以及通过远程登录服务器后的操作请求等 |
| **HTTP请求审计** | 支持HTTP请求审计，提取URL、POST/GET值、cookie、操作系统类型、浏览器类型、原始客户端IP、MAC地址、提交参数等； |
| **历史记录查询** | 1、支持不限次数任意多重条件组合查询；2、查询条件根据登录用户、源IP地址、数据库对象（分为数据库用户、表、字段）、操作时间、SQL操作命令、返回的记录数或受影响的行数、关联表数量、SQL执行结果、SQL执行时长、报文内容等灵活组合3、支持查询结果导出（excel、word、pdf等）4、支持查询模版创建、修改、删除功能； |
| **报表系统** | 系统提供丰富的报表系统，方便维护人员使用。 |
| **产品资质要求** | 《计算机信息系统安全专用产品销售许可证》《涉密信息系统产品检测证书》《计算机软件著作权登记证书》（具备国内自主知识产权）《国家信息安全测评信息安全服务资质证书（二级）》 |

* 1. 堡垒机

产品需求：

|  |  |
| --- | --- |
| 产品 | 数量 |
| 堡垒机系统 | 2套 |

堡垒机系统配置和集成要求如下：

|  |  |
| --- | --- |
| 指标体系 | 指标项 |
| **硬件指标** | 旁路代理模式，不影响正常业务流量；B/S架构，采用HTTPS方式远程安全管理，无需安装客户端；≥100/1000M\*4个自适应以太网口；系统自带内部存储，内存不少于4G，存储空间不低于500GB |
| **操作行为记录** | 1、针对SSH、Telnet、Rlogin、FTP/SFTP、数据库操作进行记录及审计，记录发生时间、源IP、目标IP、源端口、目标端口、操作指令、运维审计系统用户、目标服务器账号、访问结果等信息；2、针对RDP、VNC、X11等图形终端操作的连接情况进行记录及审计详细记录访问开始时间、源IP、目标IP、源端口、目标端口、运维审计系统用户、目标服务器账号等信息。 |
| **访问控制及异常告警** | 支持根据IP地址、时间、用户名、操作指令等内容设定安全事件规则；支持以屏幕、邮件、SYSLOG等方式实时发送告警信息。 |
| **实时监控** | 1、实时会话监控列表：显示会话连接状态（连接中、退出、阻断），显示会话来源、目标地址、帐号及访问人信息等；2、同步监控操作过程：支持对操作过程进行同步监控，执行会话回放、监控操作；3、系统状态监控：实时监控审计系统CPU、内存、磁盘的使用情况；4、审计系统监控：记录审计系统自身的管理操作，保障审计系统自身安全。 |
| **支持协议** | ssh、telnet、ftp、sftp、rdp、vnc、X11、HTTP、HTTPS、SQL\*Plus、PL/SQL、MS SQL Server等 |
| **历史记录查询** | 1、支持快速查询和高级查询功能；2、高级检索支持不限次数任意多重条件组合查询；3、支持查询模版创建、修改、删除功能；4、支持根据查询结果直接定位历史会话回放。 |
| **报表系统** | 系统提供丰富的报表系统，方便维护人员使用。 |
| **产品资质要求** | 《计算机信息系统安全专用产品销售许可证》《IT产品信息安全认证证书》 |

* 1. 终端管理系统

产品需求：

|  |  |
| --- | --- |
| 产品 | 数量 |
| 终端管理系统 | 800份客户端授权 |

终端管理系统配置和集成要求如下：

|  |  |
| --- | --- |
| 指标体系 | 指标项 |
| **终端操作系统支持** | 1、Windows2000、XP、Win7、2003、Vista、20082、支持微软平台的32位及64位OS, 支持中、英文及其他语言的操作系统3、支持Linux操作系统的客户端 |
| **基本要求** | 1、管理后台要求支持中文界面及联机中文帮助，客户端要求支持中文、英文。2、客户端所有进程所占用内存不得超过30M，CPU正常情况下占用不得超过3%。3、可在1分钟内自动发现非法接入设备，并向控制中心发出告警。 |
| **业务安全保护** | 针对重要文件，对以下操作进行权限控制，包括：1. 将文件另存到本地硬盘或其它存储介质；
2. 通过剪贴簿复制信息到其它应用；

3、通过进程间通信，将信息转移到其它软件。在授权情况下，允许将信息以加密形式保存到本地硬盘，加密文件包含授权信息 |
| **终端防泄密管理** | 1. 对非授权外联进行管理
2. 对外设接口进行管理
3. 对移动存储介质进行管理
 |
| **自动运维功能** | 1、支持设备的自动发现及终端客户端的自助安装。2、可根据设备的IP、MAC等信息，定位设备所在的位置。3、软件分发支持带宽优化及控制、支持各种格式安装包，支持Multicast方式的分发以节约带宽。4、能够实现补丁的自动更新、卸载和回退。支持补丁更新详细信息统计，包括未打补丁情况汇总统计，补丁安装情况统计等。 |
| **网络接入管理** | 1. 支持依据账户、策略检查结果，控制终端对网络访问；

2、非法接入网络的终端，其所发数据包，直接被网络准入控制设备拒绝，不会影响网络运行；3、接入后，能通过网络设备直接控制终端的网络访问权限，包括切换网络交换机端口的VLAN或自动给网络设备端口下载ACL； |
| **产品资质要求** | 著作权登记证书公安部销售许可证国家保密局涉密资质 |

2.5 传统防火墙

产品需求：

|  |  |
| --- | --- |
| 产品 | 数量 |
| 传统防火墙 | 1套 |

|  |  |
| --- | --- |
| 技术参数 | 指标和性能 |
| **接口配置** | 不少于4千兆RJ45接口；8个百兆RJ45接口  |
| **最大并发连接数** | 100万 |
| **工作模式** | 支持透明工作模式，路由/NAT工作模式和基于三层交换技术的混合工作模式。 |
| **接口与安全域** | 支持至少1000个VLAN接口和基于802.1q协议的Trunk封装；支持PPPOE接口，支持自动拨号和按需拨号两种连接方式，对PPPOE连接提供高可用性支持（包括HA和冗余接口）；支持以太网通道技术，通过多个接口的绑定来实现增加带宽和链路备份；支持环回接口，可以通过环回接口对设备进行管理，便于监控和调试，参与动态路由选举； |
| **网络服务** | 支持DNS Client，DNS中继代理和DNS静态缓存功能，用于提供DNS服务；支持DHCP Client，DHCP中继代理和DHCP服务器功能，用于提供DHCP服务。 |
| **Sflow技术** | 支持基于Sflow的网络流量监控技术，可作为Sflow代理与异常流量分析设备进行联动。 |
| **带宽管理** | 支持按照虚拟系统，接口和策略设定QoS规则，通过设定最大带宽，保证带宽，优先级和DSCP值来确保重要业务和应用不被延迟或丢弃，保证网络高效运行。 |
| **策略** | 支持根据安全域，IP地址，MAC地址，以太网帧类型，协议，端口和时间对IP数据包进行控制；支持基于域名的包过滤控制；支持长连接，可针对策略单独设置ICMP，TCP SYN,TCP FIN,TCP EST,TCP CLOSE和UDP的超时时间；支持基于IP地址和MAC地址的黑名单功能，提供临时黑名单和永久黑名单功能，通过简单有效的规则对异常地址进行控制；支持IP/MAC绑定功能；支持基于IP地址和MAC地址的信任地址功能； |
| **路由** | 支持静态路由功能；支持多个策略路由表，以入口，TOS，源IP地址，和服务作为策略条件，用户可根据不同策略控制数据流向；支持基于路由的负载均衡技术并提供多方式链路探测功能；支持内部网关路由协议RIP和OSPF和外部网关路由协议BGP。支持CIDR，路由汇总，路由过滤，路由重发布等功能。 |
| **NAT** | 支持地址映射功能；支持一对一，多对一和多对多的源地址转换以及端口转换功能；支持一对一，一对多的目的地址转换以及端口转换功能；支持策略NAT功能，可将方向，源IP地址，目的IP地址，协议，端口和服务类型值做为策略匹配条件，提供精确的地址转换服务；支持基于DNAT的负载均衡技术并提供多方式链路探测功能；支持DNS和NAT的联动。 |
| **动态端口支持** | 可针对FTP，TFTP，SIP，H.323，RTSP，Tuxedo和Oralce协议设置动态端口打开功能。 |
| **攻击防御** | 可以检测并阻止攻击者对受保护网络的探测行为，如ip address sweep，TCP SYN port scan，TCP null scan，TCP xmas scan和TCP FIN scan等；支持拒绝服务攻击防御，如SYN Cookie，WinNuke， Ping of Death，Teardrop，ICMP Flood，UDP Flood，SYN Flood，Land ，SMURF ，TCP RST；支持可疑数据包检测与防御，包括：IP碎片数据包攻击，IP选项数据包攻击（记录路由选项，时间戳选项，严格源路由选项，宽松源路由选项，路由跟踪选项）等。 |
| **产品资质** | 《计算机信息系统安全专用产品销售许可证》《计算机软件著作权登记证书》《国家信息安全测评信息安全服务资质证书（二级）》 |

* 1. 交换机

|  |  |
| --- | --- |
| 产品 | 数量 |
| 交换机 | 3台 |

产品需求：

拟采购和生产同样配置的交换机，搭建交换机冗余系统。

1. 运行管理
	1. 服务要求

本项目投标方案包含的各项软件、硬件设备，皆要求投标人提供整体实施服务，为客户提供交钥匙工程，提供项目整体方案的设计规划、实施、维护的全生命期服务。

* 1. 保修期要求

 保修期从项目终验合格之日起计算，提供三年免费维护服务。卖方所提供的系统发生故障后，买方应立即通知卖方。正常工作日内，卖方对买方的系统故障的技术支持的有效响应时间不超过2小时，到达现场维护不超过4小时。

1. 项目实施要求

到货与安装地点：中国银行间市场交易商协会指定地点。

到货时间：自合同签订之日起15天内到货。

安装时间：自所有产品到货之日起15天内完成安装。

1. 培训要求

中标人应为项目提供设备、系统的用户培训服务。

（1）中标人对招标人进行全面的设备使用及维护培训，直至完全熟练掌握。

（2）技术培训费用应包含在投标总价中。