1.项目名称：铜仁市公安局边界接入平台驻地外链路项目

2.项目编号：TRZFCG-2021-021

3.公示期限（不少于 2 个工作日）：

2021 年 1 月 15 日-2021 年 1 月 18 日

4.采购预算：1200000.00 元（最高限价 1179000.00 元）

5.采购预算确定依据:

铜仁市直政府采购（集中采购）申请表

6.采购人名称: 铜仁市公安局

联系地址: 铜仁市公安局

项目联系人:林警官

联系电话: 19110688693

7.采购代理机构全称:铜仁市公共资源交易中心

联系地址:铜仁市公共服务中心四楼（川硐麒龙国际会展城）

项目联系人:张琰

联系电话:0856-3912922

8.任何单位和个人对本项目采购文件需求公示有异议的，可在公示期限内，反馈意见给代理机构。

用户需求见附件

1、 评分标准细则

序号	评分因素及权重	分值	评分标准	说明

1	报价部分30%	30分	以本次最低投标报价为基准价，投标报价得分=(评标基准价／投标报价)×价格权值×100。对符合财库[2011]181号文规定的小型和微型企业产品的价格给予10%的扣除，用扣除后的价格参与评审。	中小企业（监狱企业、残疾人福利性单位视同小微企业）须提供《中小企业声明函》《残疾人福利性单位申明函》《监狱企业证明》（数据电文形式原件或原件扫描件）。 共同评分因素
2	技术部分45%	45分	1、供应商投标产品的技术参数完全满足招标文件中货物类产品技术指标的得45分； 2、供应商投标产品的技术参数不满足招标文件中货物类技术参数及要求的，则在45分的基础上，按以下原则扣分，扣完为止：供应商投标产品的技术参数每有一项不满足采购文件中加“▲”号的技术参数及要求的，扣5分；供应商投标产品的技术参数每有一项不满足采购文件技术参数及要求中未加“▲”号的技术参数及要求的，扣1分。	技术类评分因素
3	项目建设方案4%	4分	根据供应商提供的项目建设方案(内容包含施工质量、施工进度、技术支持体系、项目培训、验收方案、实施流程）等提供详细的设计和阐述且方案完全符合本项目要求的得4分，跟本项目内容无关或偏离的一项扣1分，扣完为止，不提供不得分。	技术类评分因素
4	产品厂家能力、资质12%	12分	1、投标产品（可信边界安全网关）制造商是入围“通过公安部组织测试的接入平台安全产品”的生产厂商，提供入围截图证明材料的得2分，未提供不得分（要求提供证明材料并加盖原厂商公章）； 2、投标产品（防火墙）制造商同时具备CNCERT/CC网络安全应急服务支撑单位（国家级）、CNCERT网络安全信息通报单位、CNCERT反网络诈骗领域应急服务支撑单位、CNNVD技术支撑单位（一级最高）的得5分，缺一项不得分。（提供有效证明文件复印件或扫描件并加盖原制造商公章）； 3、投标产品（入侵防御系统）制造商同时具备ISO9001:2015质量管理体系、ISO20000:2011信息技术服务管理体系、ISO27001:2013信息安全管理体系、ISO14000环境管理体系认证、ISO18000职业健康安全管理体系的得5分，缺一项不得分。（提供有效证明文件复印件或扫描件并加盖原制造商公章）。	技术类评分因素
5	投标人履约能力及	8分	1、投标人同时具有ISO9001质量管理体系认证证书和信息安全服务资质认证证书的得2分，不满足则不得	共同评分因素

	综合实力8%		分（提供有效认证复印件或扫描件并加盖投标人公章）； 2、投标人获得公安放管服政务信息化应用创新、先进案例类奖项的得2分（提供有效证明材料复印件或扫描件并加盖投标人公章） 3、投标人针对本项目技术实施及管理团队中，至少需2名具有CISP认证的注册信息安全工程师，且项目经理需同时具有CISP和PMP认证证书，完全满足条件的得2分，不满足则不得分（提供项目人员相关资质证明材料和在职社保缴纳证明）； 4、投标人具有部级公安机关单位边界系统项目建设案例，提供一个案例得2分，最多得2分，不提供不得分（要求提供与公安机关直签案例合同复印件或扫描件）。	
6	节能、环保1%	1分	对投标产品属于“节能产品清单”或“环保产品清单”有效期内中的产品（强制采购产品除外），在招标采购评审工作过程中，给予适当加分，即在总得分基础上，每一项加0.3分；如投标产品同时属于“节能产品清单”和“环保产品清单”两个清单中产品的，每一项加0.5分，最高不得超过1分。（须提供国家确定的认证机构出具的在有效期内的节能产品认证证书复印件、环境标志产品认证证书复印件）	

用户需求

一、 建设背景

随着公安信息化建设的不断深入开展，公安信息网（简称公安内网）与外部网络进行信息交换的需求越来越旺盛。公安机关派出分支机构或人员为社会企事业单位和公众服务越来越普遍，公安机关也在政务服务中心开设了户籍、出入境、交管等相关业务的服务窗口；同时随着“放管服”便民业务的强力推进，政务服务中心户籍、交管、出入境自助业务办理接入公安网进行信息查询录入的需求也进一步旺盛。

由于这些业务区域多数处于公共区域中，不具备公安网直接接入的条件，“放管服”便民业务系统的物理安全、网络安全和应用安全不能得到很好的保障。公安部在开展公安内外网信息交互的过程中，充分考虑到随之而来的各类安全隐患，为确保公安内网的网络安全，严令禁止单独使用网闸，防火墙等违规接入手段进行公安信息网的接入，并指定边界接入平台为公安信息网数据接入和交互的唯一通道。同时，根据公安部《关于规范公安信息网联接政务（行政）服务中心和公安业务自助办理终端审批管理工作的通知》（公传发【2018】658号）要求：政

务服务中心或自助业务终端需间接接入公安信息网并强化落实“一机一责任人”安全管理责任。

因此，为实现公安内网与其他网络进行安全、高效的信息交换，需要按照公安部的统一要求，建立符合标准的公安信息通信网边界接入平台，统一身份认证，集中授权管理，规范接入方式，实现公安信息网外部信息的采集、交换。

二、建设目标

通过本项目建设，主要实现如下目标：

1、 满足政策合规性

公安机关政务（行政）服务中心、警务服务站点、交管车驾管业务等成为公安深化“放管服”改革工作的主阵地。根据公安部关于印发《公安信息网安全管理规定（试行）的通知》（公通字【2017】8 号）、《关于进一步规范公安机关以外单位联接公安信息网和使用公安信息资源审批管理工作的通知》（公传发【2018】473 号）、《关于规范公安信息网联接政务（行政）服务中心和公安业务自助办理终端审批管理工作的通知》（公传发【2018】658 号）、《关于进一步加强驾驶人场地考试及考试系统规范管理的通知》（公交管【2018】439 号）等文件要求：公安信息网为专用网络，未经公安部批准不得将公安信息网延伸到公安机关以外的单位、公安机关驻地外办公点，须通过公安边界接入平台接入公安信息网。

2、 保障业务连续性

公安“放管服”改革工作作为方便人民群众和企业办事的重要窗口、是公安机关提供对外服务的主要途径，政务服务中心公安窗口、各警种业务自助办理终端机、交警车驾管服务所（站）等日均业务受理量不断增加，群众和企业对于“放管服”改革工作推行的新模式、新业务的依赖度和适应度日益提升。一旦该类业务服务出现中断、不稳定运行等情况带来的受理服务积压问题，将影响“放管服”改革工作的成果，因此，对业务受理相关的网络、安全、应用等系统的实时性、稳定性提出了更高要求。

3、 强化业务安全管理

通过公安“放管服”改革工作的推进，对于过程中的重要数据采集、重要流程管控都需要结合实际工作需求和现行标准规范进行明确和细化。

依据公安信息网安全管理和公安机关保密工作有关规定，开展“放管服”便民业务的政务服务中心、24h 自助业务办理服务区、交管服务站等应当依据《公安信息网安全管理规定（试行）》要求，并按照国家保密规定和标准，通过符合标准规范的安全技术手段和措施间接接入公安信息网。政务服务中心内的公安业务终端禁止连接互联网或其他网络，确保人、机、业务专用。公安业务自助办理终端应当在确保物理环境安全的基础上，指定公安民警作为设备专门安全责任人，加强日常安全监管，强化安全防护，提升行为审计和异常访问的检测能力。办公终端用户应当为公安民警或授权使用的警务辅助人员。

4、 实现业务安全接入

（1）可信身份认证

以终端、用户以及业务为对象，对于每个对象赋予唯一的身份标识，做为外部接入对象的唯一身份标识，对接入对象实行“户口式”管理。接入、访问对象必须进行身份认证：人员身份认证基于公安机关颁发的警员数字身份证书；终端设备通过设备硬件和环境指纹匹配；业务通过登记证号认证。认证协议应基于安全的双向认证协议。未通过身份认证的业务终端不能进入业务访问。

（2）访问权限控制

业务终端的网络连接应止于符合标准规范的安全接入平台内，无法直接访问公安信息网或与公安信息网交换信息。

通过身份认证的对象只能访问安全接入平台内的指定设备，并且只能进行允许的操作，非授权的访问应被阻断。同时应实现基于白名单的细粒度访问控制。按照安全策略规定的白名单格式授权访问，其余应明确禁止。

（3）数据机密性与完整性

在网络传输过程中，业务终端与安全接入平台间通信内容必须实现机密性保护。同时，必须保证传输过程中报文的完整性，并具备防止重发攻击、篡改和伪造等功能。

三、建设内容

本项目将严格依照《公安信息通信网边界接入平台安全规范（试行）》(公信通[2007]191号)中关于政府办公大厅等公安机关驻地外业务安全接入的要求，建设满足公安机关政务（行政）服务中心、社区警务室、农村警务室等安全接入公安信息网的边界系统。主要建设内容包括边界相关安全软、硬件设备和服务，详细清单如下表：

序号	**招标产品名称**	数量
1	防火墙	1 台
2	入侵防御系统	1 台
3	可信边界安全网关	2 台
4	终端安全接入服务系统	1 套
5	集控探针	1 台
6	集中监控管理系统	1 套
7	交换机	2 台
8	业务配置移动终端	1 台
9	边界链路测评服务	2 次

四、产品详细功能清单

序号	**招标产品名称**	**技术参数**	**数量**

1	防火墙	1.硬件规格：标准 2U 机箱，冗余电源，标准配置 6 个 10/100/1000M 自适应电口，4 个 SFP 插槽，另有 2 个接口板卡扩展插槽，最大支持 22 个接口，1 个 Console 口，支持液晶屏，含三年硬件维保服务；配置万兆光口≥2 个。 2.性能规格：多核 AMP+架构，网络层吞吐量 10G，并发连接≥260 万，每秒新建连接数 18 万； 3.产品支持 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.产品支持 MPLS 流量透传；支持针对 MPLS 流量的安全审查，包括漏洞防护、反病毒、间谍软件防护、内容过滤、URL 过滤、基于终端状态访问控制等安全防护功能； 5.产品支持 MTU≥9000byte 的巨型帧 Jumbo Frame； ▲6. 产品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（投标文件需要提供能够体现上述功能及配置选项的截图并加盖原厂商公章）； 7.产品支持在源地址转换过程中，对 SNAT（源地址转换）使用的地址池利用率进行监控，并在地址池利用率超过阈值时，通过 SNMP Trap、邮件、声音、短信等方式告警； 8.支持出站的 DNS 代理功能，支持在不更改内网终端设备 DNS 服务器地址设置的情况下，将 DNS 解析请求发送至指定的 DNS 服务器，并代理原 DNS 服务器返回解析结果； 9.产品支持 DNS64 功能；支持 IPv6 入站的 DNS 代理功能，即从指定的入接口或源 ISP 接收到的 DNS 解析请求，设备可根据自定义的 IP、域名对应关系，代理 DNS 服务器返回查询结果； 10.产品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； 11.产品支持基于不同安全区域防御 DNS Flood、HTTP Flood 攻击，并支持警告、阻断、首包丢弃、TC 反弹技术、NS 重定向、自动重定向、手工确认等多种防护措施； 12.产品支持漏洞防护功能，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； 13.产品的漏洞防护特征库包含高危漏洞攻击特征，至少包括“永恒之蓝”、“震网三代”、“暗云 3”、“Struts”、“Struts2”、“Xshell 后门代码”以及对应的攻击的名称、CVEID、CNNVDID、严重性、影响的平台、类型、描述等详细信息； ▲14.产品支持自定义 TCP、UDP、HTTP 协议的漏洞特征，漏洞特征可通过多个字段以文本或正则表达式的形式进行有序和无序匹配，并可自定义漏洞的源、目的端口范围；同时可标识自定义漏洞的 CVE 编号或 CNNVD 编号（提供能够体现上述功能及配置选项的截图并加盖原厂商公章）； 15.产品支持基于主机或威胁情报视图，统计网络中确认被入侵、攻破的主机数量，至少可查看被入侵、攻破的时间、威胁类别、情报来源、威胁简介、被入侵、攻破的主机 IP、用户名、资产等信息；并对威胁情报发现的恶意主机执行自动阻断；	1 台

		16.产品支持基于主机或威胁情报视图，统计网络中存在安全风险的主机数量以及对应的风险等级，至少可查看遭遇风险的时间、威胁类别、情报来源、威胁简介、失陷主机 IP、用户名、资产等信息； 17.设备提供关联分析面板，可将 Top 应用、Top 威胁、Top URL 分类、Top 源地址、Top 目的地址等信息关联，并支持以任意元素于为过滤条件且不少于 35 个维度进行数据钻取； ▲18.设备支持基于网络活动，威胁活动、阻止活动等多维关联统计及分析，发现异常行为(提供包含上述信息的多维关联分析面板截图并加盖原厂商公章)； 19.设备支持自定义一个或多个过滤条件，防火墙上的全部日志进行模糊检索或指定条件的精确检索，快速定位特定目标当前行为是否存在异常，网络中是否存在异常等问题，并可记录一个或者多个自定义过滤条件历史； 20.产品支持将告警信息以 SNMP Trap、邮件、声音、短信等形式通知管理员，告警信息的范围至少包括配置变更、病毒事件、攻击事件、异常事件、CPU 利用率、内存利用率、硬盘利用率、接口带宽利用率、NAT 利用率等； 21.产品支持与本地以及云端沙箱联动，检测文件中携带的未知威胁，并接受沙箱下发的处置策略； ▲22.产品集中管理平台支持安全策略下发、设备统一监控、日志管理、告警管理、报表管理、权限管理等功能，提供产品截图并提供权威测试机构检测报告（提供能够体现上述功能的截图以及对应的检测报告并加盖原厂商公章）； ▲23.产品具备国家信息安全测评中心颁发的《信息技术产品安全测评证书》（千兆 或 万兆 EAL4+）。（提供证书复印件并加盖厂商公章）在中国信息安全测评中心产品测评平台可查。	

2	入侵防御系统	1.硬件规格： 2U 机箱：冗余电源：自带 1 个液晶屏：1 个 HA 电口及 1 个管理口（非业务口） ：四个扩展槽：含三年硬件维修；配置万兆光口≥2 个。 2.性能规格：IPS 吞吐 7600M：并发链接≥750 万： 3.支持实时显示用户流量 TOP10，支持最近 10 分钟、1 小时、24 小时跨度的应用统计，统计指标包括：平均速率（上行、下行、双向、双向占比）、实时速率、实时包速率、连接数，并支持一键跳转显示趋势图、关联用户、关联会话； 4.支持本地 DNS 解析，DNS 自学习安全缓存，DNS 静态缓存；支持 DDNS 动态域名； 5.可实现基于 IP 地址、服务端口、IP 协议、物理端口、DSCP 值、IP 优先级、TOS 值、TTL 值、ICMP 类型、分片状态、TCP 状态、时间等安全策略的状态包过滤，支持源地址、目的地址的取反操作； ▲6.支持黑名单，根据报文的源 IP 地址、掩码进行报文过滤；支持白名单，根据报文的源 IP 地址、掩码让报文通过，支持 IPS 业务、防垃圾邮件、防病毒、应用安全和流量控制五个业务（提供相应截图证明并加盖原厂商公章）； 7.支持应用识别、入侵防护、关键字过滤、URL 过滤、AV 等安全模块一次性扫描，系统整体性能几乎不受功能的增加而降低； 8.支持 2000 多种应用特征库，可准确识别各种 IM、P2P、网络游戏、流媒体、股票等应用； 9.可基于 TCP/ICMP/UDP 协议自定义攻击特征，可阻挡蠕虫、木马、间谍软件、广告软件、缓冲区溢出、扫描、非法连接、SQL 注入、XSS 跨站脚本等多种攻击； 10.支持对单个攻击事件保存其原始报文以供取证分析； 11.提供 IPS 事件日志和报表，报表支持 PDF、TXT、HTML、CSV、DOCX 格式，并提供导出功能； 11.支持基于多种方式划分的负载均衡，如按照服务器、链路、应用等不同方面划分； ▲13.支持故障链路/服务/端口/不参加调度和故障恢复链路自动加入调度（提供相应截图证明并加盖原厂商公章）； ▲14.实时 Top 应用，支持最近 10 分钟、1 小时、24 小时跨度的应用统计，统计指标包括：平均速率（上行、下行、双向、双向占比）、实时速率、实时包速率、连接数，并支持趋势图、关联用户、关联会话（提供相应截图证明并加盖原厂商公章）； 15.支持向联动主机下发阻断策略，报文在联动主机上被阻断；	1 台

3	可信边界安全网关	1.标准机架式设备：标配 6 个千兆网口+2 个万兆网口，具有冗余电源； 2.性能：新建连接数：≥5500 次/秒，并发连接数：≥100000，SSL 事物处理速率：≥6000 次/秒，加密宽带吞吐：≥3Gbps，支持接入用户数：≥50000； 3、支持与公安各警种政务服务系统无缝对接； 4、支持应用保护：保护 B/S 应用和业务、保护 HTTPS 应用和业务、保护 C/S 应用和业务、保护数据库服务、保护视频流服务； 5、支持 DNS 代理：用户可自定义虚拟 DNS 服务同时向客户端下发解析策略； 6、支持多种用户接入认证方式：包含用户名口令、USBkey、用户名+口令+短信、文件数字证书+口令等认证方式。支持第三方接入认证，至少包含 LDAP、AD、Radius、TACACS+等认证方式； 7、密码算法支持：支持 RSA1024/RSA2048、AES256、SHA-1/SHA-2 密码算法，支持国家密码管理局颁布的 SM2、SM3、SM4 密码算法； 8、支持对接入业务对象资源进行“户口”式的统一管理，支持业务资料、链路资料、接入单位资料管理；管理员可以添加、修改、删除资料数据，为人员、设备、业务建立互相绑定，进一步增强安全性 ▲9、支持警务自助业务安全接入，通过与终端安全接入服务系统联动实现向警务自助终端分配固定唯一 IP 标识并与终端在内网注册备案 IP 一一对应绑定（提供网关与终端安全接入服务系统联动详细功能截图，并加盖原厂商公章）； 10、支持制定接入设备的安全准入审核策略，检测设备安全达标情况，阻止不合规的终端接入； ▲11、支持服务状态自检测,包括服务端引擎检测、客户端自检测、客户端检测日志展示,提高故障诊断能力，便于后期系统运维和故障定位（提供产品的“服务端引擎检测、客户端自检测、客户端检测日志展示”功能界面截图，并加盖生产厂商公章）； 12、为保证接入业务的连续性及可靠性，支持双机热备和负载均衡； 13、支持管理员和用户日志审计，并支持发送审计日志到第三方审计系统； ▲14、支持交管类业务安全接入，具有公安交管综合应用的边界安全管理模块，实现各类车驾管业务的安全管理和无缝接入（公安交管综合应用边界安全管理模块需通过公安部安全检测并提供检测报告加盖原厂商公章）； ▲15、应满足《GA216.1-1999 计算机信息系统安全产品第一部分：安全功能检测身份鉴别类》和国家保密标准《涉及国家秘密的信息系统安全中间件产品技术要求》（秘密）提供证明文件并加盖厂商公章； 16、产品具有《计算机软件著作权登记证书》，证书中明确产品名称包含“安全网关”，并加盖生产厂商公章；	2 台
4	终端安全接入服务系统	1、 软件系统，部署于公安政务服务各警务自助终端； 2、 适配公安政务服务各警种自助终端（治安、交管、出入境等）； ▲3、支持与边界网关联动通过向警务自助终端分配固定唯一 IP 标识并结合终端属性消息传递，配合业务系统实现对自助终端的注册备案（提供终端属性消息传递实现自助终端注册备案详细功能截图，并加盖原厂商公章）； 4、提供终端信息提取等功能，实现对接入终端的安全认证和设备指纹信息提取； 5、支持警务自助终端证书应用代理和证书授权管理，由责任警员对其管理的自助终端进行授权； 6、操作系统支持 Windows、Linux、Android、IOS； ▲7、支持与边界网关对接实现终端接入流程的注册、审批等线上管理工作（提供终端接入线上注册、审批详细功能截图，并加盖公章）； ▲8、产品具备国家版权局颁发的“终端安全应用代理”《计算机软件著作权登记证书》（提供证书复印件，并加盖厂商公章）	1 套

5	集控探针	1、支持采集多种设备的运行状态信息； 2、支持对多种设备的流量信息采集； 3、支持 SYSLOG 协议； 4、支持 SNMP v2/SNMP v3 协议； 5、稳定性运行时间(MTBF) >50000 小时； 6、性能：数据库容量≥200GB；最大支持业务数量≥1000 个；最大监控并发用户数量≥5000 个；最大审计用户数量≥200000 个；最大业务审计记录数≥10000000 条。	1 台
6	集中监控管理系统	1.标准机架式设备，10/100/1000Mbps 电口≥4 个； 2.稳定性运行时间(MTBF)＞50000 小时； 3.最大支持业务数量≥2000； 4.最大监控管理业务数量≥5000； 5.最大审计数据量 500G； 6.应用数据吞吐量≥800Mbps。	1 套
7	交换机	1. 交换容量≥336Gbps，整机转发性能≥108Mpps， 2 . 端口要求 24 个千兆电口，4 个万兆光口。	2 台
8	业务配置移动终端	i5-10210U/≥8G 内存/256G SSD 硬盘/UHD620/指纹识别/56wh 电池/TPM 芯片/1.38KG/三年保修	1 台
9	边界链路测评服务	根据公安信息通信网边界接入平台安全规范要求进行链路测评	2 次

五、 商务及售后

（一） 商务要求：

1、质保期（验收合格后开始计算）：设备质保期为 3 年。

2、付款方式：完成采购合同签订，设备到货上架、调试完成，并将接入业务配置完成，经过验收之后付款 90%，待三年服务期限完成之后再支付余下的款项 10%。

3、验收方法和标准：服务产品验收按照中华人民共和国现行通用产品的市场规范、验收规范和验收标准及合同要求执行。

(二) 服务要求：

1、项目交付时间和地点：在合同签订后 10 个工作日内完成项目实施及政务中心接入工作，地点由铜仁市公安局指定。

2、供应商就设备及软件的安装、调试、操作、维修、保养等对使用方维修技术人员进行培训。

3、对采购的软硬件设备均提供 3 年免费质保，质保期内免费提供软件升级；质保期内提供 7*24 小时电话技术支持服务；对于无法远程解决的技术问题或设备软硬件故障问题需在 1 小时响应，4 小时到达服务现场进行处理。