武汉市退役军人事务局
办公网络安全运维服务项目采购需求

一、采购背景

武汉市退役军人事务局按照全市网络安全工作要求，拟通过购买局机关办公局域网网络安全运维服务，对局域网互联网边界、局域网内部网络行为和国产化终端设备使用进行全方位、不间断监管，实时排查局域网内网络安全风险，及时进行风险管控和处理，确保局域网内基础设施环境、网络和终端设备安全、可靠。

二、服务期限

自合同签订之日起一年。

三、采购内容

服务名称：办公局域网网络安全运维服务。

四、采购要求

本次采购的服务是负责武汉市退役军人事务局的办公局域网基础设施环境、网络和终端等相关设备的维护及安全。提供服务的形式包括但不限于提供辅助设备、辅助软件和驻场人员服务等。各供应商需提供详细的运维服务方案，方案内容须包括但不限于提供服务所需的设备（包含设备品牌、型号）、软件（包含品牌、功能）和人员等详细信息，并承诺所提供的方案都是真实、有效、合法的，必须完全满足采购人的采购需求，并确保局机关办公局域网安全、稳定、高效地运行。合同签订后，供应商必须先行投入运维方案中所需设备和软件等资源，并经审核确定资源、网络和终端设备均正常运行后，采购方开始计算服务期并支付服务费用。如果所提供的资源无法确保网络和终端设备安全、稳定运行的，采购人有权以供应商虚假承诺为由终止合同并要求供应商赔偿。

（一）服务清单

序号	名称	服务内容	服务要求

1	机房基础环境运维服务	机房环境监控、强弱电等基础设施维护，IT 资产管理	驻场服务
2	网络运维服务	网络设备维护、网络架构、路由协议、链路诊断，网络 IP 地址设计与维护	驻场服务
3	终端电脑运维服务	国产化终端系统和设备维护，单位接入设备维护协调与供应商对接，终端管理制度。	驻场服务
4	安全边界服务	1、边界防护：包括 ACL 控制、应用识别与流控、入侵防御、僵尸网络检测等功能，支持联动 EDR 一键查杀，一键终端隔离等快速处置； 2、硬件要求：产品应采用国产处理器和国产操作系统； 3、性能指标：网络层吞吐量≥7Gbps，应用层吞吐量≥2Gbps，并发连接数≥300 万，每秒新建连接数≥6 万，配置不少于 5 个 10/100/1000M 以太网电口，4 个千兆光口（配模块），冗余电源。	驻场服务
5	终端行为管控服务	供应商按需提供行为管理工具，应采用国产处理器和国产操作系统，有效防止机密信息的外泄，避免不良信息的扩散，提高员工的工作效率，保障网络资源合理使用，提高网络可管理性，便于网络管理，最终实现安全、高效、健康的互联网环境。	驻场服务
6	安全运维服务	日常运维服务、安全巡检服务、安全设备配置维护、安全日志监控服务、安全数据分析、配合安全加固服务等内容。	驻场服务
7	应急保障服务	重大活动应急保障、重大安全事故处理、应急体系建立、应急演练。	驻场服务
备注	1.投入人员应由投标方发放加班工资，加班时间由采购人安排和考核。投标方须自行解决服务工作所需的交通工具，产生的使用费、保险、损耗由中标单位承担； 2.本项目属于整体运维服务项目，服务范围不仅限于现状中描述的设备维护，采购人随时新增设备也在维护范围内。		

（二）机房基础环境运维服务

1、机房日常运维管理

通过中心机房管理服务，严格控制机房人员进出、设备进出并及时登记设备与应用的配置更新情况，有助于中心机房的管理和监控，确保机房物理安全、网络及应用的正常运行。所有进出机房的人员必须遵循机房管理制度，按照机房设备操作规范对设备进行调整、操作。

2、机房基础设施运维

对机房的物理环境和设施（温湿度，供电，照明、消防、环境整洁）实施实时监控，定期对机房电力系统、空调、漏水保护等环境设施进行检查。同时，对涉及的环境设备（各类空调、消防设备、监控报警等）实时故障紧急处理、报修和后续处置。

3、机房 IT 资产管理

通过对机房 IT 资产的梳理，整理分类资产台帐。通过安全策略限制不同区域间的访问，仅根据需要开放实际的访问，确保网络及业务系统的安全。

（三）网络运维服务

1、日常网络运维服务

建立标准规范，对网络建设进行统一的标准配置，确保网络配置的标准化。日常维护期间，对网络发生的故障，包括链路、设备故障、网络安全系统问题等要进行及时判断和响应，快速处理，确保网络运转正常。网络设备资料整理，配置参数整理；根据设备的特点设计并建立设备配置管理文档；及时更新发生变更的设备配置，保持设备配置文档与实际设备配置的一致性。

2、全局网络监测和故障处理

需安排具备 CISAW（信息安全保障人员认证证书）或网络与信息安全管理员资质的技术人员对全网络链路运行状态监测，出现故障协助外单位进行故障排查，现场处理。建立网络巡检制度，每月一次对于网络运行状态、主要 IT 资产进行例行巡检，规范 IT 网络配置标准化、资产明细化。

3、网络整体及出口流量分析

定期对网络流量进行采集，分析出包括互联网出口、各分支结构入口、接入

层入口流量的主要数据类型。通过分析得出通往各个端口的正常流量和非正常流量以及相关的处理措施。同时，通过对网络带宽使用率与网络协议等方面的分析，并结合历史数据，能够分析得出网络使用情况的趋势，通过分析及时发现潜在问题，并提供相应解决方案与建议。

（四） 终端电脑维护服务

根据用户要求，对办公网接入终端进行维护。硬件设备故障检测、故障排除。硬件故障：保修期内协助客户进行设备报修、维修、更换和升级；保修期外协助和推荐客户进行设备选型或购买厂家维保服务。

- 网络的配置和修改。
- 系统的重装与备份。
- 系统安全策略的设置。
- 磁盘及系统注册表的清理等。
- 制定软件系统使用标准、使用规则，以及权限控制方法。
- 软件故障恢复、依据客户需求安装常用办公、工具软件（不能违反版权）。软件和系统补丁安装。
- 协助用户进行数据备份。
- 在使用软件方面提供技术支持、培训。

（五）安全边界服务

供应商按需提供的安全边界防护工具，需提供入侵防御功能，有效地为网内终端提供安全防护；同时开启 APT 检测功能，定位网络中的傀儡机，保障内部网络安全；开启实时被动扫描功能，对网络中的所有流量进行应用层的安全分析，防范安全威胁事件的发生，彻底全面的保证办公网的安全。

服务所需设备技术标准

功能项	详细要求
链路聚合	支持手动和 LACP 链路紫合，可根据源/目的 MAC、源/目的 IP、源/目的端

	口、五元组、端口轮询等条件提供不少于 10 种链路负载算法；
DNSDoctoring	▲支持 DNSDoctoring 功能，能够将来自内部网络的域名解析请求定向到真实内网资源，提高访问效率，同时支持通过配置多条 DNSDoctoring，实现内网资源服务器的负载均衡；（提供功能截图）
访问控制	▲提供策略分析功能，支持策略命中分析、策略冗余分析、策略冲突检查、策略包含分析，可在 WEB 界面显示检测结果；（提供功能截图及具备 CNAS 标识的关于“策略冗余/冲突检测”的产品功能检测报告并提供检测规则冲突技术的知识产权证书）
	▲支持一体化安全策略配置，可以通过一条策略实现五元组、源 MAC、源地区、目的地区、域名、应用、服务、时间、长连接、并发会话、WEB 认证、IPS、AV、URL 过滤、邮件安全、数据过滤、文件过滤、审计、APT 等功能配置,简化用户管理；（提供功能截图证明，提供具备 CNAS 标识的关于“基于策略的长连接”的产品功能检测报告）
	提供策略查询功能，支持五元组快速查询以及针对策略名、源/目的区域、源/目的地址、服务、对象、未命中时间等条件进行细粒度检索；
用户管控	支持设置密码有效性，如首次登陆修改密码、密码定期修改、密码有效时间等设置，用户忘记密码时，支持密码找回；
行为分析	内置行为分析功能，对会话、流里等数据进行统计分析，建立业务行为基线，对异常行为进行告警；支持行为分析监控展示，可展示不同行为分析策略的实时数据和基线数据趋势；
升级维护	支持软件版本本地备份，可备份多个系统版本文件，支持对软件版本进行快速升级及回滚；
系统诊断	支持在 WEB 界面进行网络诊断，支持 PING、TRACEROUTE、TCP、HTTP、DNS 诊断方式；
设备状态	支持 CPU 利用率、内存利用率、磁盘利用率、会话数告警及 CPU 利用率、内存利用率、磁盘利用率等硬件资源实时利用率及其历史使用情况追踪；
访问控制	支持 IPv6 安全控制策略设置，能针对 IPv6 的目的/源地址、目的/源服务端口、区域、服务、时间、扩展头属性等条件进行安全访问规则的设置；（提供功能截图证明，提供具备 CNAS 标识的关于“基于 IPV6 扩展头的访问控制”的产品功能检测报告）

带宽管理	▲支持链路和四层通道嵌套的流量控制功能，可基于上下行区域、地址、地理对象、用户/用户组、服务/服务组、应用/应用组和时间等配置带宽策略，支持带宽策略优先级和针对 IP、应用设置白名单；（提供功能截图证明，提供具备 CNAS 标识的关于“基于地区的流量控制”的产品功能检测报告）
产品资质	▲考虑产品稳定性，选用市场认可度高的产品，要求提供权威机构评选防火墙产品近 5 年市场占有率前三排名证明文件；（提供有效证明文件）
	▲防火墙产品具备密码检测认证证书；（提供资质证明文件并加盖厂商公章）
	▲防火墙产品具备销售许可证；（提供资质证明文件并加盖厂商公章）
	▲产品具备节能认证；（提供证书复印件）
厂商资质	▲为保障产品质量要求产品厂商通过 TL9000 认证证书和 ISO9001 认证证书；（提供有效证书复印件）
	▲为保障国产化平台对接特性，要求产品厂商具备中国信息安全测评中心颁发的安全开发类二级认证；（提供有效证书文件）
	▲为保障产品后期实施交付、服务能力，要求产品厂商具备信息系统建设及服务能力评估（CS4）认证证书；（提供资质证明文件）

（六）终端行为管理服务

供应商按需提供行为管理工具，供应商按需提供行为管理工具，应采用国产处理器和国产操作系统，有效防止机密信息的外泄，避免不良信息的扩散，提高员工的工作效率，保障网络资源合理使用，提高网络可管理性，便于网络管理，最终实现安全、高效、健康的互联网环境。

服务所需设备技术标准

功能项	功能要求说明
硬件参数	1U 标准机架式设备，采用国产处理器和国产操作系统；网络层吞吐量≥10Gbps，带宽性能≥300Mbps，终端准入用户数≥1200，最大并发连接数≥400 万，配置千兆电口≥10 个、光电复用接口≥4 个，扩展槽位≥2 个，硬盘≥1T，冗余电源；

认证管理	支持本地认证、Portal 认证、邮件认证、短信认证、微信认证、钉钉认证，企业微信认证、CAS 认证、APP 认证、IC 卡认证、二维码认证、混合认证等实名制特性；支持上网用户自注册和自动录入，支持关联管理员终端，可以通过终端接受自注册、终端注册、终端绑定的审批通知；
功能要求	▲支持透明、路由、旁路、聚合、虚拟网线等部署模式，支持多种模式混合部署和单种模式部署；修改部署模式无需重启设备；（请提供第三方测试报告，及对应的功能截图）；
	支持应用控制、带宽管理、URL 过滤、非法行为阻断、数据防泄漏、行为审计等多项功能，支持有效控制 QQ、微信、P2P 下载、在线视频、股票软件等上网行为；
	▲内置应用分类库，应用数量≥10000 种。其中移动应用≥5000 种，即时消息应用≥200 种，默认预置≥10 种应用标签，SaaS 应用≥900 种，对 SaaS 应用有默认分类标签；（请提供第三方测试报告，及对应的功能截图）
	支持通道化的 QoS，支持基于用户、应用、源/目的地址、地理位置、时间、终端型号等维度进行带宽控制。支持流量限额以日、月为单位配置。支持流量限额功能，进行日流量总额、月流量总额、当日使用时长、当月使用时长等限额类型进行流量管理；针对达到限额阀值的用户进行弹窗提醒，管理员可选择禁止上网或者加入至惩罚流控通道；
	支持针对搜索引擎、http、网页内容进行关键字过滤并实时生成日志记录，日志级别包括但不少于紧急、告警、严重、通知、信息、调试、不记录等，方便管理员快速区分用户上网行为属性和定位日志级别。支持针对虚拟账号进行黑、白名单管理；
	▲支持在设备旁路部署时针对违规上网行为进行阻断过滤；支持在设备旁路部署时针对内网上网用户进行实名身份认证，旁路认证方式包括但不限于本地 WEB 认证、Portal Server 认证、短信认证、免认证、混合认证、单点登录等；（请提供第三方测试报告，及对应的功能截图）
	支持自定义 URL 过滤，包括恶意 URL 白名单、恶意 URL 黑名单、URL 白名单等，并支持 URL 的模糊匹配。内置恶意 URL 特征库，管理员可基于策略快速过滤恶意 URL。
产品资质	▲产品具备中国网络安全审查技术与认证中心颁发的“中国国家信息安全产品认证证书”；（提供证书复印件）
	▲产品具备 IPv6 Ready Logo 认证证书；（提供证书复印件）
	▲产品制造商符合《信息系统建设和服务能力评估体系能力要求》，能力

	达到优秀级（CS4）；（提供证书复印件）
	▲产品制造商具备中国网络安全审查技术与认证中心颁发的数据安全管理认证证书；（提供证书复印件）

（七）安全运维服务

通过工具实时接收设备报警信息，要求对安全设备及网络设备产生的安全报警进行及时处理和记录。

根据应用的调整，在安全设备上对策略进行及时调整并测试，根据实际应用，清理无用的安全配置。

周期性对安全设备进行日志查看分析，对日志中暴露的问题进行策略调整。

对安全设备进行预防性巡检，要求检测系统性能及运行状况，查验安全设备的日志文件，监控网络流量。及时发现系统的各种报警信息，并做出相应的处理和记录，如网络流量异常，要及时做出分析，提出解决方案；每次预防性检查要有详细的记录，并向采购人提交检测报告。

当安全设备出现系统故障时，能及时响应。迅速分析故障原因，协助采购人更换故障设备及部件，并立即进行处理。

定期对安全设备的配置进行备份，配置更改后按照服务流程体系进行记录。

梳理现有的信息安全相关的管理制度，结合对信息系统安全性的需求以及信息系统安全等级保护的相关要求，提供完整的信息安全管理体系框架，主要包含：

信息安全管理手册、组织人员安全管理制度、系统建设安全管理制度、系统运维安全管理制度、系统应急管理制度等。帮助用户建设完整的、层次性的信息安全管理体系。

（八）应急保障服务

1.应急处置服务

在项目服务周期内，如果发现异常信息以及严重新病毒、攻击时，及时提供预警信息并上报事务局，采取相应的应急处理措施、应对方法、专杀工具等，防

止重大网络故障、攻击行为等的扩散，限制影响范围。

2.重大活动保障服务

在重大节日、大型活动等重要活动期间，根据局机关统一要求，由服务方根据需要安排技术人员进行值班。加班费和补贴要符合国家相关标准，由服务方统一支付。

3.完善应急预案机制

建立完善各类安全事件应急处置专项预案及编制要求，建立预案审核机制，对信息安全应急预案进行审核，提出预案修改完善的建议，配合建立信息安全事件应急演练的环境建设

（八）其他要求

1、投标人须符合《政府采购法》第二十二条的规定。

2、投标人须具备或高于有效期内的信息技术服务三级（ITSS)资质、信息系统安全集成三级（CCRC）资质、信息系统安全运维三级（CCRC）资质，技术服务人员需提供有效期内的技术资格证书。

3、付款方式：按与采购人签订的合同约定内容进行付款。

武汉市退役军人事务局

2024 年 9 月 13 日