项目采购需求

一 名称

2026 年广东省北江流域管理局网络安全维护专项项目采购需求书

二 项目业主情况

项目业主名称：广东省北江流域管理局

地址：广东省佛山市三水区西南街道防汛路御涛园一座

联系人：钟锦雄

联系电话：0757-89816323

三 中介服务名称

2026 年广东省北江流域管理局网络安全维护专项项目

四 对中介服务机构的资质要求

无

五 服务内容和服务要求

1 服务内容

本项目总预算 30 万元。

本项目需要提供安全情况网关、应急响应服务，并对局网络安全设备提供运维服务，内容包括例行巡检、日常维护、响应支持、故障处理等，确保局网络安全、硬件设备可用性和稳定性达标。

（1） 安全情报服务

在网络出口部署一台安全情报网关设备，提供一年服务，要求如下:

1) 标准 1U 机架式设备，内存≥16G; 硬盘≥1T; 默认 bypass 口≥2 对。威胁防护流量≥500M。Console 口≥1 个，千兆电口≥8 个，万兆光口≥2 个。

2) 设备支持旁路部署、网桥部署、虚拟网线部署、混合部署多种部署方式;

3) 支持对多种类型的入侵攻击进行检测和防护，包括侦查、漏洞利用、病毒攻击、建立通信隧道、网站后门&shell、连接远控地址、木马远控、远控工具流量、挖矿、僵尸网络行为、蠕虫攻击、勒索攻击、数据窃取、尝试下载恶意文件、钓鱼、对外攻击、攻击持久化操作等;

4) 支持应对外部攻击 IP 高频扫描的扫描防护功能，可自定义设置 IP 在特定时间内扫描次数超过某个阈值后判定为扫描 IP，自动支持 IP 封禁动作，并支持自定义封禁时间;

5) 内置 0DAY 检测规则模式，支持高危 0day 漏洞检测，支持 0day 检出数量不少于 200 个;

6) 支持针对钓鱼场景的专项防护，设备具备钓鱼场景的策略设置、防护效果的专项界面。

7）支持针对 APT 场景的专项防护，设备具备 APT 场景的策略设置、防护效果的专项界面。

8）持续追踪数百个 APT 组织的攻击行为和痕迹，支持对于 APT 攻击行为的检测及拦截;

9）支持旁路模式下阻断威胁连接,包括 TCP 连接阻断和 UDP 连接阻断，阻断率高达 99%以上;

10）支持通过 API 接口调用的方式和三方设备进行联动，通过联动对 OneSIG 黑白名单进行增、删、改、查操作，实现威胁自动化联动封禁;

11）支持在国家级攻防演练场景下，自动获取攻击队情报信息，检测且拦截攻击队攻击行为;

12）2022 年国家国防演练内置超过 1W 条以上情报;

13）支持按照情报可信度自定义入站拦截防护策略，包括高可信重保攻击 IP 和中可信重保攻击 IP，支持设置拦截连接、仅告警不拦截和放行不记录三种拦截防护设置;

14）支持按照资产和时间维度进行安全概况筛选，可监控最近一小时、最近一天、最近一周、最近一月的安全概况;

15）支持展示当前威胁检出数、威胁拦截数、告警但未拦截的威胁数、各威胁类型的拦截防护比例

16）支持展示出站威胁中失陷主机总数、失陷威胁类型，包

括 APT、挖矿、钓鱼、勒索等，支持展示 TOP5 外联地址分布;

17) 支持展示外部攻击总数，外部攻击类型，包括 0day、Wbshe11、黑名单等; 支持展示 TOP5 威胁来源和 TOP 攻击事件;

18) 支持资产对象分组管理，支持自定义资产类型，支持手动录入资产或文件批量录入资产，支持资产信息一键导出功能;

19) 支持绑定资产组设置威胁防护策略，可针对情报检测、规则检测和黑白名单分别设置对应的防护策略,防护策略包括拦截连接、仅告警不拦截、放行不记录三种类型，以应对各类安全防护场景需求;

20) 支持出入站场景下自定义黑名单，支持域名及 IP 的手动录入和批量导入，支持按照 IP 地理位置进行出入站黑名单配置，支持自定义设置黑名单生效时间，支持黑名单一键导出;

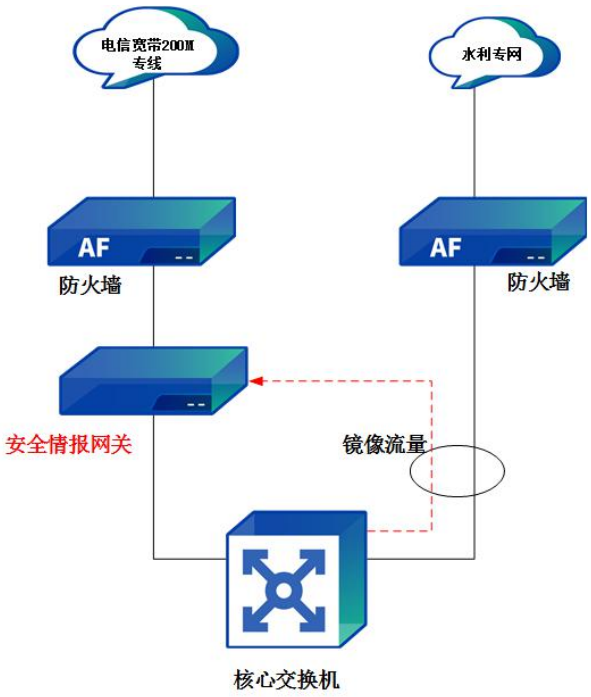
21) 可支持封禁策略 20W 条以上，支持封禁 IP 百万级;

22) 黑名单支持封禁 IPV6 地址;

23) 支持在威胁明细列表视角下，出站威胁及入站威胁 IP、域名、规则一键添加白名单;

24) 支持通过 API 调用的方式进行防护策略控制，通过策略 API 可与现有安全建设产品集成，实现自动化的联动封禁策略;

安全情报网关部署拓扑结构图以下:



（2） 应急响应服务

1）服务概述：当发生外部黑客入侵、数据泄露、木马病毒等突发安全事件时，提供包括事件检测与分析、风险抑制、问题处置、入侵溯源、协助业务恢复的服务，能够协助用户快速止损，最大化降低安全事件带来的影响。

2）具体服务内容：

①配合北江局开展汛前网络安全检查工作，配合采购方做好水利部及广东省组织的网络安全检查整改工作。

②在水利部、公安部、省水利厅组织举办的网络安全攻防演练期间，派驻一名网络安全工程师参加防守；在两会期间，派驻一名网络安全工程师参加防守；其他地方组织的网络安全攻防演练期间，提供远程值守服务。

③配合做好等级保护复测评的整改完善。

应急事件处置

WEB 安全事件：B/S 类信息系统或网站遭受恶意入侵，利用网站进行反动信息、赌博、黄色等信息发布，传播危害国家安全、社会稳定和公共利益的内容的安全事件；

恶意程序事件：蓄意制造、传播恶意程序，或是因受到恶意程序的影响而导致的信息安全事件。恶意程序是指插入到信息系统中的一段程序，恶意程序危害系统中数据、应用程序或操作系统的保密性、完整性或可用性，或影响信息系统的正常运行；

网络攻击事件：通过网络或其他技术手段，利用信息系统的配置缺陷、协议缺陷、程序缺陷或使用暴力攻击对信息系统实施攻击，并造成信息系统异常或对信息系统当前运行造成潜在危害的信息安全事件；

信息破坏事件：通过网络或其他技术手段，造成信息系统中的信息被篡改、假冒、泄漏、窃取等而导致的信息安全事件；

应急时效要求

特别重大事件（Ⅰ级），5 分钟作出响应，提供远程 7*24 小时响应服务、1 小时到达现场进行应急响应服务；

重大事件（Ⅱ级），10 分钟作出响应，提供远程 7*24 小时、2 小时到达现场进行应急响应服务；

较大突发事件（Ⅲ级），30 分钟作出响应，提供远程 7*24 小时响应服务、4 小时到达现场进行应急响应服务；

一般性突发事件（Ⅳ级），30 分钟作出响应，提供远程 7*24 小时响应服务、远程无法解决时，在 4 小时到达现场进行应急响应服务。

3）服务交付物

《应急响应报告》《网络安全整改方案》。

（3） 巡检服务

对安全设备进行巡检巡查、配置优化、规则库更新等工作；并从技术角度开展安全评估，结合现在网络安全设备最佳方案，对客户的网络设备、安全设备进行安全配置的核查，识别出现有安全配置与普适性规范或行业规范的安全配置要求之间的差距，并提供相关优化建议。

具体服务内容:

①对北江局网络进行每月一次的安全检测与完善，包括对网络设备和安全设备日常运行监测、安全管理策略配置，网络事件监控与分析，网络各类操作行为监控与审计等，提交检测报告，并对存在问题及时进行整改完善。

②对北江局服务器设备进行每月一次的安全检测，包括服务器日常运行监测、服务器操作系统漏洞扫描及监测，提交检测报告，并针对设备存在问题及时进行整改与完善。

③对北江局外网应用系统及数据库进行每月一次的安全检测，包括日常安全监测、安全漏洞扫描、渗透测试及人工审计，及时响应和处理应用系统运行中发生的安全突发事件和安全隐患，提交检测报告，针对系统存在问题及时进行整改与完善。

④对北江局进行每月一次的安全检测，包括日常安全监测、安全漏洞扫描、渗透测试及人工审计，及时响应和处理网站运行中发生的安全突发事件和安全隐患，提交检测报告，针对存在问题及时进行整改与完善。

（4） 安全设备续保

序号	设备名称	厂家	型号	采购日期	授权到期时间	是否续保	备注
1	堡垒机	绿盟	OSMSNX3-200C-C	2018/11/18	2026/12/23	是	产品质保
2	安全感知平台	深信服	SIP-1000-B400	2022/8/31	2026/9/1	是	规则库升级+产品质保
3	潜伏威胁探针	深信服	STA-100-B2100-H	2022/8/31	2026/9/1	是	规则库升级+产品质保
4	外网防	深		2022/	2026/9/	是	规则库升级

	火墙	信服	AF-1000-B1810	1/25	1		+产品质保
5	云镜网络资产脆弱性扫描系统	深信服	YJ-1000-B1120	2022/8/5	2026/8/31	是	规则库升级+产品质保

2 服务要求

（1）提供免费技术服务热线，并安排专业技术人员在工作时间内为我方解答有关技术问题，并保证在半小时内给予答复。

（2）服务方在我方正常工作时间内提供工程师现场支持服务；工作日下班时间及非工作日（周六、周日及节假日、汛期期间）提供必要服务时间外的应急支持服务。

（3）响应速度:

服务工程师在接到需要现场处理的报障后，需在 30 分钟内响应，4 小时内赶到现场，如无法在上述时间内赶到现场的，服务方应及时说明原因并报业主方相关部门备案。

（4）维修服务时限:

1)工程师对单个设备故障修复时间平均不超过 4 小时(硬件修复标准为对故障设备硬件进行维修或备件进行替换后，使设

备恢复正常工作;软件修复标准为对软件系统进行修复或重新安装配置后，使系统恢复正常运行），单台终端设备故障持续时间超过 4 小时未能修复时,服务方应及时说明原因并将有关情况报业主方备案，对无法维修的需进行更换。

2）保证服务响应及维修效率，每次设备修复后，应保证 5 个工作日内该台设备不发生同一故障影响设备正常运行（间歇性故障除外）。

（5）洪水期间时，按我局的要求增加现场值守，实行 24 小时值班，保证系统正常运行。

3 管理要求

（1） 运维人员值班要求

建立 24 小时线上值班制度，要求服务方在工作时间和非工作时间（包括节假日），妥善做好维护应急方案和值班安排，并将值班安排提前书面告知用户方,所安排的值班人员应该具备一定的技术能力和应急处置能力,能够处理或者协助处理突发的系统事件。

（2） 组织实施要求

为使项目按质、按量、按时及有序实施，投标人应建立完善、稳定的项目团队、内部组织管理方式及管理机构、协调机制、技术基础，支撑保障要求及其他相关要求。在机制保障方面，成立组织实施小组和项目专家组的双轨制的组织模式。在项目日常

管理和条件保障方面，从行政组织、后勤保障和支撑条件各方面创造良好的服务环境，确保项目的顺利实施。

（3） 文档管理要求

中选人应在项目完成时，将本项目所有文档、资料汇集成册交付给采购人，所有文件要求用中文书写或有完整的中文注释。验收后，中选人按国家、省以及采购人档案管理要求，向采购人提供装订成册的纸质文档至少 3 套，电子文档 1 套。

（4） 质量保证要求

为保证本项目能按时高质的顺利完成，规避项目风险或将风险降至最低程度，投标人应建立项目质量管理体系，包括但不限于质量目标、质量指标、岗位责任、问题处理计划、质量评价、整改完善等内容。

（5） 保密要求

1）中选人应签订保密协议，对其因身份、职务、职业或技术关系而知悉的采购人商业秘密和党政机关保密信息应严格保守，保证不被披露或使用，包括意外或过失。

2）中选人不得以竞争为目的、或出于私利、或为第三人谋利而擅自保存、披露、使用采购人商业秘密和党政机关保密信息；不得直接或间接地向无关人员泄露采购人的商业秘密和党政机关保密信息；不得向不承担保密义务的任何第三人披露采购人的商业秘密和党政机关保密信息。中选人在从事政府项目时，不得

擅自记录、复制、拍摄、摘抄、收藏在工作中涉及的保密信息，严禁将涉及政府项目的任何资料、数据透露或以其他方式提供给项目以外的其他方或中标人内部与该项目无关的任何人员。

3）除采购人书面表明为非保密信息外，中选人从采购人获取或在合作过程中所知悉、接触的所有信息及材料，均视为保密信息。

4）如违反上述规定，采购人有权对成交中选人采取相应的处罚措施并有权依法追究其法律责任。

（6） 安全生产要求

中选人应建立健全安全生产责任制，明确各级管理人员和员工的安全生产职责。根据国家法律法规和行业标准，制定和完善安全生产规章制度和操作规程。定期对员工进行安全生产教育培训，提高员工的安全意识和操作技能。

4 其他要求

（1） 服务响应要求

中选人须充分考虑广东省北江流域管理局的地理位置的重要性，在防汛、抗旱等应急响应下，需要提供充足的服务人员，安排 7*24 小时的驻场服务，确保网络安全设备的正常运行。

六 合同履行地点和方式

提供服务的时间：合同签订后一年服务期。

提供服务的地点：广东省佛山市。

提供服务的方式：现场服务,远程值守服务，提供工作日工作时间、汛期值班、防洪应急期间的响应服务。

七 公开选取方式和计价标准

1.公开选取方式：方案择优选取。

2.报价方式：报总价。

八 服务时间

本项目采购合同自双方盖公章后生效。本项目服务期为一年，自合同生效之日起开始计算。

九 验收

12 月采购人组织项目年终验收，根据考核结果情况，支付合同余款。

1 验收标准

在服务期内出现的所有问题全部完成处理,网络安全设备设施安全、稳定、正常运行，可供业务人员正常使用。按本需求书和合同等相关文件的要求完成各项服务工作任务,并已提交相关记录资料予采购方审核通过。

2 考核指标

（1）考核原则

根据客观公正、科学规范、注重实效、定性与定量相结合的考核原则进行考核。

（2）考核对象

本项目运维服务中选人。

（3）考核机构

考核小组由广东省北江流域管理局分管领导担任组长，考核组成员由局科信办相关人员组成。

（4）考核方法

考核采用扣分制，根据运维单位的工作情况及事件实时记录，每半年将扣分情况通报给运维单位。运维单位如对考核结果有不同意见，可在收到通知后五个工作日内进行书面申诉，由考核小组进行仲裁。

1)考核累计扣分在10分(含)以内的部分，每扣1分，折减合同结算金额人民币100元。

2)考核累计扣分超过10分的部分，每扣1分，折减合同结算金额人民币2000元。

考核总得分低于80(不含)，视为不合格单位，甲方有权终止合同。

费用折减的具体金额，由采购人根据生效的考核结果文件(如经审定的考核评分表及通报文件)在相应阶段的付款结算中直接予以扣除，并书面通知中选人。

服务期结束时再次考核，考核情况作为明年评选参考依据。

考核评分表

序号	考核内容	分数	说明	得

		(100 分)		分
	应急响应服务: 当发生网络安全事件时,提供包括事件检测与分析、风险抑制、问题处置、协助业务恢复的服务		1、设备出现故障应在 2 小时内响应，4 小时内到达现场。（违反一次扣 2 分） 2、出现故障无法正常运行，要求在 8 小时内处理完成，使网络安全设备正常使用。（违反一次扣 2 分）	
	巡检服务: 对网络安全设备进行检查、优化,并做好配置数据备份。		1、每月至少对系统作一次全面巡检,维护人员未能按采购人要求对网络安全设备进行巡检维护的。（违反一次扣 2 分） 2、每季至少对系统作一次设备版本检查、升级,设备数据备份。(违反一次扣 2 分）	
	安全情报服务: 部署阻断扫描入侵行为、0day 攻击等高级威胁,以提升网络威胁防护的能力和效率。		1、未按要求提供 0day 安全情报服务扣 5 分; 2、提供安全情况服务未达要求扣 2 分。	
	安全设备续保: 对 5 台网络安全设备续保		1、未按要求进行续保扣 10 分; 2、未完全按要求续保的,每少一台设备扣 5 分。	
	得到厅级以上部门表彰		每次加 1 分	

	的			
	防洪期间做好信息保障工作,工作突出的		每次加 1 分	
	对维护工作有创新的		每次加 1 分	
	额外工作完成出色的		每次加 1 分	
总得分				

十 结算方式

1 付款方式

（1）计量

本项目报价除备用金在合同终止时按经采购人确认的实际累计金额计列结算外,其他维护过程中产生所有费用均为总价承包。

（2）支付

i.首次支付

合同签订后，支付合同额的 90%。

ii.年终结算

本年底由采购方组织年终考核，根据考核结果的实际使用情况，支付合同余款。

iii.付款方式：采购方在完成考核并收到服务方付款申请后，10个工作日内办理支付手续。每次付款前，服务方应提交有效税务发票。

iv.项目（设备）通知单，项目（设备）确认签证，考核结果等作为支付申请的依据。

十一 违约责任

一方不履行合同义务或者履行合同义务不符合约定的，应当承担继续履行、采取补救措施或者赔偿损失等违约责任。

一方未按照约定支付合同款的，对方可以要求其支付合同款。

十二 补充合同和解决争议方式

采购合同中如有未尽事宜，双方协商一致后可以签订补充合同，但补充合同不得与《中华人民共和国合同法》和广东省网上中介服务超市相关管理制度相抵触。

对于合同履行中出现的纠纷，双方应协商解决。协商不成的，通过诉讼的方式解决。

十三 备注

1 如果监督管理部门对有关服务已经拟定“合同范本”，业主单位、中选中介服务机构应当使用有关“合同范本”；如果

监督管理部门未有“合同范本”，业主单位、中选中介服务机构应当根据《中华人民共和国合同法》等法律法规的规定自行拟定合同。

2　合同的实质性内容，应当与采购公告、采购结果的内容一致。合同的实质性内容是指合同标的、数量、质量、价款或者报酬、履行期限、履行地点和方式、违约责任和解决争议方法等。

3　合同的变更、终止等，适用《中华人民共和国合同法》等法律法规的规定。