**百色市中医医院网络安全技术服务项目需求**

**项目内容**

本项目的服务内容包括但不仅限于：互联网出口防护服务、服务器区边界防护服务、上网行为审计服务、日志存储和审计服务、运维审计服务、数据库审计与防护服务、数据库审计与防护服务、信息安全等级保护整改及相关服务、信息系统安全等级保护测评服务等；

具体内容及需求规格清单如下：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **项号** | **货物名称** | **数量** | **单位** | **技术参数** |
| 1 | 互联网出口防护服务 | 1 | 项 | 1. 中标人在服务期间须向采购人提供并部署两套新一代防火墙，该系统一年服务期满后归中标人所有和使用。 2. 提供的新一代防火墙应具备的硬件指标：标准2U设备；配置≥6个10/100/1000M自适应电口，2个接口板卡扩展插槽， 1个Console口，配置≥1TB存储容量的企业级硬盘，配置液晶屏，含一年硬件质保，一年应用识别库、URL分类特征库、病毒防护特征库、入侵防御特征库升级及威胁情报。 3. 提供的新一代防火墙应具备的性能指标：防火墙吞吐≥8Gbps，并发连接数≥230万，每秒新建连接数≥12万/秒，包含应用控制、URL过滤、病毒防护、入侵防御、威胁情报检测等功能模块。 4. 提供的新一代防火墙应支持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. 提供的新一代防火墙应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。 6. 提供的新一代防火墙应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、邮件等方式告警 7. 提供的新一代防火墙应支持DDNS功能，支持Oray向日葵、Pubyun公云、Noip、Changeip提供的DDNS服务，将动态获取的IP地址映射为固定的域名。 8. 提供的新一代防火墙应支持DS-Lite CPE B4功能，支持成为b4或aftr角色，支持从DHCPv6服务器或手动方式获取AFTR参数。 9. 提供的新一代防火墙应支持在虚拟系统内独立配置病毒防护、漏洞利用防护、间谍软件防护、URL过滤、文件过滤、内容过滤、邮件过滤、行为管控等安全功能。并可支持对本虚系统内产生的日志进行独立审计。 10. 提供的新一代防火墙应支持基于源安全域、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。 11. 提供的新一代防火墙应支持共享上网检测功能，可以通过设置管控地址和例外地址优化管控功能，同时支持阻断或告警动作。 12. 提供的新一代防火墙应支持将其他硬件安全设备（包括但不限于防火墙、IPS、IDS、WAF、行为管理、流量探针等）加入网元组，并接受流量编排；支持将同类型安全设备划归同一网元组，组成硬件安全资源池（如WAF安全资源池），并将流量通过负载均衡（“源地址哈希”、“源目的地址哈希”，“加权源地址哈希”、“加权源目的地址哈希”、“加权地址端口哈希”、“轮询”和“权重轮询”）的方法编排给组内所有网元。 13. 提供的新一代防火墙应支持灵活的服务链编排功能，支持串接链和旁路链，支持网元组的方向和位置设置。 14. 提供的新一代防火墙应支持灵活的细粒度引流策略，可基于源安全域、目的安全域、源用户、源地址、目的地址、服务、VLAN、服务链、流量方向（内网到外网/外网到内网）的引流策略，并详细记录日志。 15. 提供的新一代防火墙应支持基于不同安全区域防御SYN Flood、UDP Flood、ICMP Flood、IP Flood、DNS Flood、HTTP Flood、NTP Query Flood 、NTP Reply Flood 和SIP Flood 攻击，并支持警告、丢弃、普通防护（首包丢弃）、增强防护（TC反弹技术）、授权服务器防护（NS重定向）、普通防护（自动重定向）、增强防护（手工确认）等多种防护措施。 16. 提供的新一代防火墙应支持DHCP协议防护；支持手动定义可信DHCP服务器IPv4和基于阈值限制DHCP请求传输速率。 17. 提供的新一代防火墙应支持IPv4和IPv6流量的HTTPS、POP3S、SMTPS、IMAPS协议进行解密，支持配置基于源安全域、目的安全域、源地址、目的地址、SSL协议服务的解密策略，动作可以设置解密或不解密。 18. ★提供的新一代防火墙应支持IPv4和IPv6流量的蜜罐引流策略，支持配置基于源安全域、目的安全域、源地址、目的地址、服务、VLAN的引流策略，并支持强制导流，能够通过设置服务器和端口进行引流。 19. 提供的新一代防火墙应支持资产管理，能够通过设置资产监控、VPN、源安全域来控制资产识别范围，支持scanner或onvif类型的扫描方式和网段，实现自动或手动资产扫描；支持通过设置IP地址、MAC地址、资产类型、生效市场、厂商、位置等信息来制定黑/白名单，方便日常资产管理。 20. 提供的新一代防火墙应具备LLDP功能，可以向网络中其它节点公告自身的存在，并保存各个邻近设备的发现信息，如设备配置和设备识别等详细信息。 21. 提供的新一代防火墙应支持作为轻量级“探针”与采购人现网在用的网络威胁感知系统联动，上报网络活动产生的数据至网络威胁感知系统；并支持接收来自网络威胁感知系统推送的处置策略，及时拦截绕过防御措施产生的高级威胁。 22. 提供的新一代防火墙应支持与采购人现网在用的终端安全管理系统联动，实现基于终端健康状态的访问控制，阻断“高风险”终端网络活动。 |
| 2 | 服务器区边界防护服务 | 1 | 项 | 1. 中标人在服务期间须向采购人提供并部署两套新一代防火墙，该系统一年服务期满后归中标人所有和使用。 2. 提供的新一代防火墙应具备的硬件指标：配置≥18个10/100/1000M自适应电口，16个SFP插槽，8个SFP+插槽，4个接口板卡扩展插槽， 1个Console口，配置液晶屏，含一年硬件质保，一年应用识别库、URL分类特征库、病毒防护特征库、入侵防御特征库升级及威胁情报。 3. 提供的新一代防火墙应具备的软件指标：防火墙吞吐≥50Gbps，并发连接数≥900万，每秒新建连接数≥40万/秒，包含应用控制、URL过滤、病毒防护、入侵防御、威胁情报检测等功能模块。 4. 提供的新一代防火墙应支持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. 提供的新一代防火墙应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。 6. 提供的新一代防火墙应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、邮件等方式告警。 7. 提供的新一代防火墙应支持DDNS功能，支持Oray向日葵、Pubyun公云、Noip、Changeip提供的DDNS服务，将动态获取的IP地址映射为固定的域名。 8. 提供的新一代防火墙应支持DS-Lite CPE B4功能，支持成为b4或aftr角色，支持从DHCPv6服务器或手动方式获取AFTR参数。 9. 提供的新一代防火墙应支持在虚拟系统内独立配置病毒防护、漏洞利用防护、间谍软件防护、URL过滤、文件过滤、内容过滤、邮件过滤、行为管控等安全功能。并可支持对本虚系统内产生的日志进行独立审计。 10. 提供的新一代防火墙应支持基于源安全域、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。 11. 提供的新一代防火墙应支持共享上网检测功能，可以通过设置管控地址和例外地址优化管控功能，同时支持阻断或告警动作。 12. 提供的新一代防火墙应支持将其他硬件安全设备（包括但不限于防火墙、IPS、IDS、WAF、行为管理、流量探针等）加入网元组，并接受流量编排；支持将同类型安全设备划归同一网元组，组成硬件安全资源池（如WAF安全资源池），并将流量通过负载均衡（“源地址哈希”、“源目的地址哈希”，“加权源地址哈希”、“加权源目的地址哈希”、“加权地址端口哈希”、“轮询”和“权重轮询”）的方法编排给组内所有网元。 13. 提供的新一代防火墙应支持灵活的服务链编排功能，支持串接链和旁路链，支持网元组的方向和位置设置。 14. 提供的新一代防火墙应支持灵活的细粒度引流策略，可基于源安全域、目的安全域、源用户、源地址、目的地址、服务、VLAN、服务链、流量方向（内网到外网/外网到内网）的引流策略，并详细记录日志。 15. 提供的新一代防火墙应支持基于不同安全区域防御SYN Flood、UDP Flood、ICMP Flood、IP Flood、DNS Flood、HTTP Flood、NTP Query Flood 、NTP Reply Flood 和SIP Flood 攻击，并支持警告、丢弃、普通防护（首包丢弃）、增强防护（TC反弹技术）、授权服务器防护（NS重定向）、普通防护（自动重定向）、增强防护（手工确认）等多种防护措施。 16. 提供的新一代防火墙应支持DHCP协议防护；支持手动定义可信DHCP服务器IPv4和基于阈值限制DHCP请求传输速率。 17. 提供的新一代防火墙应支持IPv4和IPv6流量的HTTPS、POP3S、SMTPS、IMAPS协议进行解密，支持配置基于源安全域、目的安全域、源地址、目的地址、SSL协议服务的解密策略，动作可以设置解密或不解密。 18. 提供的新一代防火墙应支持IPv4和IPv6流量的蜜罐引流策略，支持配置基于源安全域、目的安全域、源地址、目的地址、服务、VLAN的引流策略，并支持强制导流，能够通过设置服务器和端口进行引流。 19. 提供的新一代防火墙应支持资产管理，能够通过设置资产监控、VPN、源安全域来控制资产识别范围，支持scanner或onvif类型的扫描方式和网段，实现自动或手动资产扫描；支持通过设置IP地址、MAC地址、资产类型、生效市场、厂商、位置等信息来制定黑/白名单，方便日常资产管理。 20. 提供的新一代防火墙应具备LLDP功能，可以向网络中其它节点公告自身的存在，并保存各个邻近设备的发现信息，如设备配置和设备识别等详细信息。 21. 提供的新一代防火墙应支持作为轻量级“探针”与采购人现网在用的网络威胁感知系统联动，上报网络活动产生的数据至网络威胁感知系统；并支持接收来自网络威胁感知系统推送的处置策略，及时拦截绕过防御措施产生的高级威胁。 22. 提供的新一代防火墙应支持与采购人现网在用的终端安全管理系统联动，实现基于终端健康状态的访问控制，阻断“高风险”终端网络活动。 |
| 3 | 上网行为审计服务 | 1 | 项 | 1. 中标人在服务期间须向采购人提供并部署一套上网行为管理系统，该系统一年服务期满后归中标人所有和使用。 2. 提供的上网行为管理系统应具备的硬件指标：2U设备，冗余电源；配置≥6个千兆电接口；提供2个扩展插槽；1T硬盘；含一年硬件质保及软件升级服务。 3. 提供的上网行为管理系统应具备的软件指标：适用带宽≥800Mbps，支持用户数≥10000人，并发连接数≥60万，每秒新建连接数≥35,000/秒。 4. 提供的上网行为管理系统须采用一体化引擎，避免在复杂应用场景开启多功能时的延迟损耗及性能衰减。 5. 提供的上网行为管理系统应支持静态路由、OSPF动态路由、支持策略路由；同时还支持负载均衡，链路负载均衡、DNS负载均衡。 6. 提供的上网行为管理系统在部署时应支持模式选择，可设置为Portal模式，实现Portal服务器功能； 7. 提供的上网行为管理系统应支持对网络接入的终端进行可视化管理，展示终端详细信息、异常状态等，支持查看终端类型，以及厂商、系统、端口等详细信息。 8. 提供的上网行为管理系统应支持自动扫描发现网络中已占用的IP地址，支持图形化展示某个IP地址的在线状态、当前使用者、MAC地址和活跃时间。 9. 提供的上网行为管理系统应支持通过恶意软件特征检测方式识别失陷主机并记录日志。 10. 提供的上网行为管理系统应支持识别内网的爬虫行为，并且可监控爬虫用户数趋势和爬虫请求数趋势；可查询爬虫行为详情；支持配置源IP、目的IP/域名白名单，提供更精准爬虫的检测能力。 11. 提供的上网行为管理系统的应用协议库包含的应用数量不低于15000种，其中大模型应用数量不低于3000。 12. 提供的上网行为管理系统应支持对域名服务器、数据库服务器、文件服务器、邮件服务器、Web服务器等业务系统进行传输行为监测，能够及时中断、调整或隔离一些不正常或是具有伤害性的网络资料传输行为。 13. 提供的上网行为管理系统应支持对上传到业务系统的文件进行病毒查杀，支持本地查杀及病毒文件MD5云查；本地查杀支持对PE、脚本、宏病毒查杀，支持对压缩文件内的病毒查杀。 14. 提供的上网行为管理系统应支持通过SNMP、DNS审计策略对其通信内容进行审计和控制。 15. 提供的上网行为管理系统应支持审计、控制Oracle、MySql、SqlServer、 PostgreSQL等数据库的访问与操作，包括添加、删除、修改、查询等。 16. 提供的上网行为管理系统应支持配置禁用PC热点开启功能。禁用时PC仍可以使用网络，但是无法通过随身wifi或笔记本自带功能创建热点。 17. 提供的上网行为管理系统应支持对SSH协议的流量进行解密；可根据实际需求配置指定的源/目的IP或IP段。 18. 提供的上网行为管理系统应支持通过FTP和SFTP方式将日志导出到指定服务器，日志支持SSL加密传输和ZIP压缩，通过设备USB接口导出。 19. 提供的上网行为管理系统应支持与采购人现网在用的网络威胁感知系统联动，接收来自网络威胁感知系统的封堵指令。 |
| 4 | 日志存储和审计服务 | 1 | 台 | 1. 中标人在服务期间须向采购人提供并部署一套日志收集与审计系统，该系统一年服务期满后归中标人所有和使用。 2. 提供的日志收集与审计系统应具备的硬件指标：标准2U机箱，配置≥6个10/100/1000M Base-T自适应电口，≥2个扩展槽，带1个Console口，4TB磁盘存储硬盘，冗余电源；提供一年硬件质保和软件升级服务。 3. 提供的日志收集与审计系统应具备的软件指标：综合日志处理性能≥3000EPS，提供60个审计节点授权许可。 4. 提供的日志收集与审计系统应采用B/S模式，无需安装客户端，使用WEB浏览器访问管理中心，浏览器端无需安装Java运行环境。支持chrome浏览。 5. 提供的日志收集与审计系统应支持通过Syslog、SNMP Trap、Netflow V5、ODBC/JDBC、Agent代理(Windows/Linux)、WMI、(S)FTP、文件共享(SMB、NetBIOS)、文件\文件夹读取、Kafka等多种方式完成各种日志的收集功能，支持多行日志采集合并为一行。 6. 提供的日志收集与审计系统应支持自定义资产类型及资产属性；支持对资产自定义标签，支持对标签内容进行查询和管理。 7. 提供的日志收集与审计系统应支持对资产IP地址的地理信息进行管理，支持单个IP、IP段设置行政区及经纬度**。** 8. 提供的日志收集与审计系统应提供页面可视化编辑归一化策略，对页面查看的日志编辑归一化策略，所见即所得，也支持通过归一化文件的导入来支持归一化,不需修改系统程序。 9. 提供的日志收集与审计系统应支持正则表达式、Key-Value、JSON日志解析，支持日志自动化辅助范化。 10. 提供的日志收集与审计系统针对匹配的多条范化策略，应支持用户手工设置策略匹配优先级**。** 11. 提供的日志收集与审计系统的日志解析字段应内置130个字段，属性字段可扩展，用户可根据审计需要自行创建字段，字段类型包括IP、字符串、整型等15种，可选择映射函数等。内置及新增的所有字段均可参与查询、关联分析和报表统计。 12. 提供的日志收集与审计系统应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**。** 13. 提供的日志收集与审计系统应支持对日志中的源和目的IP地址进行自动补全，补全IP地址的资产、国家、区域和城市等信息。 14. 提供的日志收集与审计系统应支持即席在线查询，支持嵌套查询，可针对查询结果任意回退，收敛事件范围；用户可根据需要配置事件显示的字段内容等。查询结果可支持加密导出。 15. 提供的日志收集与审计系统应支持以图形化的方式展示日志属性之间的聚合关系，并支持手动选择日志属性，显示多维事件分析图；属性可增加或减少，且支持图片大小调整。 16. 提供的日志收集与审计系统应支持将统计结果保存为仪表板、报表和策略，提供可编辑的灵活强大的自定义仪表板。 17. 提供的日志收集与审计系统应支持提供安全运维报告，帮助运维人员快速生成日常日志分析和运维报告。 |
| 5 | 运维审计服务 | 1 | 项 | 1. 中标人在服务期间须向采购人提供并部署一套运维安全管理系统，该系统一年服务期满后归中标人所有和使用。 2. 提供的运维安全管理系统应具备的硬件指标：配置≥6个千兆电口，≥2个接口扩展槽，硬盘容量≥4T；内存≥8G，USB口≥2个，配置液晶屏；提供一年硬件质保。 3. 提供的运维安全管理系统应具备的软件指标：最大支持150路图形会话或400路字符会话并发，可管理设备数量≥300个，配置100个资源授权许可。 4. 提供的运维安全管理系统采用旁路部署，不得影响业务环境，支持HA双机部署，支持集群部署，支持跨地域、跨数据中心分级部署，支持异地灾备部署。 5. 提供的运维安全管理系统应支持微信小程序动态口令认证方式登录堡垒机，且当用户需要使用手机令牌登录时，需要强制绑定手机令牌。 6. 提供的运维安全管理系统应支持应用发布防跳转功能，进行http/https访问过程时运维人员仅允许访问授权地址。 7. 提供的运维安全管理系统应支持云主机资源批量导入，包括阿里云、百度云、华为云、腾讯云、Ucloud、AWS、Azure云平台的资源，支持设置优先导入公网和内网IP设置，支持导入同时批量新建标签。 8. 提供的运维安全管理系统应支持对数据库协议访问操作进行控制，可基于库、表、命令实现对数据库操作的细粒度访问控制，执行动作包括但不限于断开连接、拒绝执行、动态授权、允许执行。 9. 提供的运维安全管理系统应不限操作系统类型，无需安装任何客户端插件，使用浏览器通过H5方式即可直接运维SSH、RDP、Telnet、VNC、Rlogin、SFTP资源。 10. 提供的运维安全管理系统应支持H5运维过程中通过群发命令，实现同时运维多台资源设备。 11. 提供的运维安全管理系统应支持运维过程中邀请其他用户参与、协助操作；会话协同过程中，协同者可以申请控制会话，创建者可以强制获取控制权。 12. 提供的运维安全管理系统应支持以云盘形式在堡垒机上存储常用文件，实现操作端、堡垒机和目标资源三者之间文件共享。 13. 提供的运维安全管理系统申请工单时应支持文件管理、RDP剪切板、磁盘映射、键盘审计、剪切板审计（上行、下行）、显示水印、上传、下载权限、OCR识别申请。 14. 提供的运维安全管理系统应支持工单审批时，设置多级审批模式，需要逐级进行审批，最大支持5级。 15. 支持水印功能，避免数据泄露无法追责。 16. 提供的运维安全管理系统应支持水印功能，用户在运维或者是监控、查看会话时，H5页面会将用户的登录名作为水印展示，避免数据泄露无法追责，支持在H5运维SSH、RDP、TELNET、VNC、应用发布等资源时显示水印。 17. 提供的运维安全管理系统应支持专属手机App远程管理（非浏览器方式），可在App端实现用户管理、主机管理、工单审批、告警消息、会话管理等功能。 18. 提供的运维安全管理系统内置文件病毒扫描能力，实现本地上传文件到堡垒机网盘、主机上传文件到堡垒机网盘的文件传输扫描，针对病毒文件，可以执行信任、删除等操作，并生成审计记录。 |
| 6 | 数据库审计与防护服务 | 1 | 项 | 1. 中标人在服务期间须向采购人提供并部署一套数据库审计与防护系统，该系统一年服务期满后归中标人所有和使用。 2. 提供的数据库审计与防护系统应具备的硬件指标：标准2U机箱，冗余电源；标配≥6个千兆自适应电口，1个Console口，支持2个扩展槽位，配置液晶屏；内置4TB存储硬盘；提供一年软件升级和硬件维保。 3. 提供的数据库审计与防护系统应具备的软件指标：SQL审计处理能力（速率）≥34000SQL/S。 4. 提供的数据库审计与防护系统应可同时支持IPv4和IPv6的网络环境下数据库的审计。 5. 提供的数据库审计与防护系统应支持的数据库：Oracle、SQL-Server、DB2、Informix、Sybase、MySQL、PostgreSQL、达梦、人大金仓、南大通用Gbase、神舟通用、Caché、REDIS。 6. 提供的数据库审计与防护系统应支持通过Agent审计到回环接口的流量**。** 7. 提供的数据库审计与防护系统应支持旁路阻断功能（非串联方式），阻断功能具备两种模式：宽松模式、严格模式。 8. 提供的数据库审计与防护系统应支持C/S架构COM、COM+、DCOM组件的审计，可提取应用层工号（账号）的身份信息，精确定位到人。 9. 提供的数据库审计与防护系统应支持白名单管理，根据白名单支持数据库操作命令（包括select、create、delete等40种以上命令）；语句长度、语句执行回应、语句执行时间、返回内容、返回行数、数据库名、应用账户、服务器端口、客户端操作系统主机名、客户端操作系统用户名、客户端MAC、客户端IP、客户端端口、客户端进程名、时间、数据库表、包、存储过程、函数、视图、字段、索引等二十四种以上条件。 10. 提供的数据库审计与防护系统应支持全文检索数据库solr的审计，可审计到solr的查询、插入行为的操作信息。 11. 提供的数据库审计与防护系统内置敏感数据类型，可自动发现业务环境中数据库对象中包含敏感数据类型，进行敏感数据级别的定义；支持敏感数据自定义，支持同步敏感数据扫描结果中的敏感数据，支持自定义敏感规则，可根据配置字段包括操作类型、敏感配置（保护对象所属的敏感数据）主体信息（访问工具、访问IP、客户端MAC、操作系统主机名、操作系统用户名）、规则生效时间进行敏感字段的操作行为监控与审计。 12. 提供的数据库审计与防护系统内置疑似SQL注入、跨站脚本攻击、字段猜测、代码更改、等近500种风险审计规则库，无需单独配置，直接调用。 13. 提供的数据库审计与防护系统应支持重复操作的统计审计规则，可根据在一定的时间内，重复某项操作达到设定的统计次数进行规则审计告警。 14. 提供的数据库审计与防护系统应支持操作语句系列的组合审计规则，可根据某一客体的操作行为序列，连续操作了设定的语句序列时进行规则审计告警。 15. 提供的数据库审计与防护系统应支持全库检索、条件检索和关键字检索，检索效率达到1亿条数据二十秒内检索出结果，快速定位相应的审计会话内容。 |
| 7 | 信息安全等级保护整改及相关服务 | 1 | 项 | 一、等级保护咨询  1、执行科学的评估方法和分析体系  执行科学的评估方法和分析体系，包含项目的准备及启动、信息系统识别及现状调查、明确等保评估的信息系统范围、制定等保评估工作计划、收集并分析信息系统资料、信息系统安全等级的确定、生成信息系统网络拓扑图、编写定级报告和备案信息。对信息系统的安全现状进行等级保护差距测评，分析信息系统保护现状和信息安全等级保护基本要求之间的差距，为通过信息系统等级保护奠定基础。提交《等级保护差距测评报告》。制定我单位安全需求分析、安全建设与改建方案的制定、制作原信息系统产品加固方案、测评不符合及部分符合项整改建议、制作新的网络拓扑图、制作安全需求分析报告、编制并确认整体信息系统整改方案。  2、建立信息安全等级保护管理体系  根据《信息安全等级保护管理办法》和《信息系统安全等级保护基本要求》，参照《信息系统安全管理要求》、《信息系统安全工程管理要求》等标准规范要求，结合等级保护测评报告提出的安全管理体系与等级保护基本要求之间的差距，在信息安全管理制度、安全管理机构、人员安全管理、系统建设管理、系统运维管理等方面指导并协助建立健全符合相应等级要求的安全管理制度。提交《信息安全等级保护管理制度包》。  3、协助信息安全等级保护技术整改  协助我单位进行信息安全等级保护安全技术整改。根据《信息安全等级保护管理办法》和《信息系统安全等级保护基本要求》，结合等级保护测评报告提出的安全防护现状与等级保护基本要求之间的差距，综合重要信息系统的特点，明确安全需求，设计符合相应等级要求的信息系统安全技术建设整改方案，协助开展信息安全等级保护安全技术措施建设，落实相应的物理安全、网络安全、主机安全、应用安全和数据安全等安全保护技术措施。对高风险、高威胁整改完善后进行现场测评工作并出具最终报告。提交《等级保护差距整改建议》。  根据项目整体目标和要求，进行安装部署调试服务，包括本次采购的设备以及业主现有的设备、主机、网络设备、安全设备和维护端设备系统，以及新增的安全设备/软件进行安全策略调整、优化，包括身份鉴别、访问控制、入侵防范、日志审计、资源管理、保密管理等进行优化。协助测评，测评公司现场实施评估和测评的时候要有安服人员在场，测评公司提出的整改需求，安服人员要及时的完成整改，保障测评全过程的顺利进行。  4、协助我单位进行三级等保测评的准备和整改工作：  协助我单位进行三级等保测评的准备和整改工作。按照等级保护测评的标准，做好相关的调试整改，必须依照以下标准：《信息安全等级保护管理办法》、《信息系统安全等级保护定级指南》、《信息系统安全等级保护基本要求》、《计算机信息系统安全保护等级划分准则》（GB17859-1999）、《信息安全技术信息系统通用安全技术要求》（GB/T20271-2006）、《信息安全技术网络基础安全技术要求》（GB/T20270-2006）、《信息安全技术操作系统安全技术要求》（GB/T20272-2006）、《信息安全技术数据库管理系统安全技术要求》（GB/T20273-2006）、《信息安全技术服务器技术要求》、《信息安全技术终端计算机系统安全等级技术要求》（GA/T671-2006）等。对我单位系统安全漏洞扫描（通过专业工具）、生成信息系统漏洞扫描报告，并协助测评机构对我单位信息系统进行准备和整改。在等级保护准备和整改过程中，应采用访谈、检查、测试、工具扫描等国际国内认可的先进方法和手段进行，并与国家相关规范及标准的要求相符。必须采用专业的国内安全扫描设备及软件产品辅助整改工作的完成。  对测评机构提供的第一次等保测评报告进行整改。测评机构提供的第一次等保测评报告结论为不符合的，最终要达到“基本符合”。协调信息系统优化调整（优化、调整及加固）、信息安全产品部署（上架、安装及调试）、协助建立信息系统安全管理机构、编制信息系统安全管理制度（完善）、培训信息系统安全管理人员。  编写信息系统建设规划、制定信息系统运维管理制度。编写好我单位的信息系统等保所需的所有资料，包括不限于制度、流程、文件、各种记录表、登记表等所有相关文件资料。  二、风险评估  1、主机漏洞扫描服务  （1）内容：对被评估对象进行系统检测，利用漏洞特征，发现检查对象可能存在的主机漏洞及脆弱性;  （2）支持扫描对象包括：操作系统、数据库、应用系统、网络设备、虚拟化设备  1、主机操作系统扫描  包括 WINDOWS、SOLARIS、AIX、LINUX、SCO、SGI等  2、数据库系统扫描  包括 MS-SQL、ORACLE、MYSQL、INFORMIX、SYBASE、DB2等  3、应用系统扫描  包括WWW、E-mail、DNS、FTP等的安全性进行漏洞扫描  4、网络设备  包括防火墙、路由器、交换机、IPS、IDS、堡垒机等  2、WEB漏洞扫描服务  （1）内容：利用专业级WEB应用扫描工具对被评估对象进行应用检测，以发现网站应用层面可能存在的技术漏洞；包括WEB容器识别，如：Apache、tomcat、Weblogic、WebSphere和Ngix等；支持多种服务端语言探测，如：PHP、JSP、ASP、ASPX和.NET等；支持WEB前端框架探测，如：jQuery、Bootstrap、HTML5等；支持WEB后端开发框架探测，如：Django、Rails、ThinkPHP、Struts等； 支持WEB业务应用探测，如：BBS、CMS和BLOG等（备注：逻辑类漏洞主要通过人工渗透测试完成）  （2）支持扫描对象包括：B/S架构类应用漏洞，主要包括：SQL注入、XSS跨站脚本攻击、应用系统弱口令、敏感文件下载、后台用户枚举等  3、基线配置检查服务 根据国家监管部门以及行业监管部门下发的关于行业信息安全技术指引，提炼指引中涉及到的重点安全要素，结合企业信息安全现状分析，制定相应的基线标准。对信息系统安全要求、漏洞、病毒等进行安全评估及差距分析，以评估系统现状与监管部门技术要求标准存在的差距。  （1）内容：对被评估对象进行配置规范检查，通过与标准基线比对，发现配置层面的安全隐患。  （2）支持扫描对象包括：操作系统、数据库、应用程序、网络设备；  四、应急响应服务  针对安全事件发生时，及时，准确的解决安全事件，化解安全危机、将安全事件的风险及损失降到最低。安全事件是指在客户信息系统中出现的影响业务正常运行的任何异常事件。例如：破坏系统的完整性、系统资源拒绝服务、通过渗透或者入侵的方式来对系统进行非法访问，系统资源的滥用以及任何可能对系统造成损害的行为等。提交《应急响应报告》。  （1）内容：在甲方遇到突发安全事件的时候，采取适当的响应策略及时遏制安全事件的影响，恢复业务到正常服务状态，保存证据和追查来源等。例如：勒索病毒、信息窃取、拒绝服务攻击、网络流量异常等。  （2）过程：5\*8 小时现场响应、7\*24小时电话响应  五、安全培训服务  通过培训使普通员工了解信息安全基础知识和防护技能，使技术人员了解信息安全风险评估和信息安全等级保护的有关国家政策和技术发展趋势，以及常见的攻击手段及防范方法。提交个性化培训材料，如：《信息安全意识漫谈小册子》、《信息安全培训视频》、《信息安全宣传海报图片》。  内容：提供进阶式、由浅入深式的安全培训  阶段一：【针对全员】信息安全意识增强培训  通过一些具体数据和通俗易懂的案例讲解使管理层了解目前国内外在不同领域的信息安全相关形势，以及信息安全对于企业的重要意义  阶段二：【针对IT人员】信息安全认识误区介绍  通过信息安全案例分析，形象的比喻与事例纠正以往对于信息安全的认识误区（如：信息安全就是计算机与网络安全、信息安全就是安全产品加安全技术、信息安全一劳永逸等。）  阶段三：【针对IT人员】常见攻击手段及防范方法  1. 在分析漏洞原理的同时，结合实际漏洞利用进行操作演示。  备注：培训主题可由用户自定义  六、维护调试服务  针对我单位现有的安全设备，要求能提供1名专职人员服务  1、针对我单位现有的所有安全设备，调试安装应用识别规则库的服务  2、针对我单位现有的所有安全设备，提供调试安装服务  3、已有产品的渠道设备巡检服务；  5、提交《安全设备巡检报告》 |
| 8 | 信息系统安全等级保护测评服务 | 1 | 项 | 提供具有等级保护测评资质的单位对HIS系统进行测评服务，协助业主顺利通过等保测评（信息安全等级保护：3级）。  一、总体要求  依照《网络安全等级保护基本要求》（GB/T22239-2019）、《信息系统安全等级保护测评准则》、自治区公安厅《关于开展全区政府信息系统安全等级保护检查工作的函》（桂公函[2009]429号）的要求，对百色市政府电子政务外网按照网络安全等保2.0要求进行信息安全等级保护三级测评，出具符合国家信息安全等级保护管理部门规范要求、公安机关认可的信息系统安全等级测评报告。  二、项目基本原则  符合国家等级保护和国家相关法律，指出防范的方针和保护的原则；测评方案的设计与实施应依据国内、国际的相关标准进行；测评服务商工作中的过程和文档，具有很好的规范性，可以便于项目的跟踪和控制；测评的方法和过程要在双方认可的范围之内，安全咨询的进度要按照进度表进度的安排，保证采购方对于服务工作的可控性；安全体系设计的范围和内容应当整体全面，包括安全涉及的各个层面，避免由于遗漏造成未来的安全隐患；测评工作应尽可能小的影响系统和网络的正常运行，不能对招标方各系统的运行和业务的正常提供产生显著影响；对测评过程中获得的采购方数据和结果数据严格保密，未经授权不得泄露给任何单位和个人，不得利用此数据进行任何侵害采购方利益的行为。  三、等级保护测评标准  等级保护测评过程中，必须依照以下标准：  《计算机信息系统安全保护等级划分准则》（GB 17859-1999)  《网络安全等级保护基本要求》（GB/T22239-2019）  《网络安全等级保护测评要求》（GB/T28448-2019）  《网络安全等级保护测评过程指南》（GB/T28449-2018)  《网络安全等级保护设计技术要求》（GB/T25070-2019）  《网络安全等级保护测试评估技术指南》（GB/T 36627-2018）。  四、测评主要内容  信息系统的安全等级测评内容应包括技术和管理两大类，其中技术类应包括对物理安全、网络安全、主机安全、应用安全和数据安全及备份恢复等方面的测评，管理类测评应包括对安全管理制度、安全管理机构、人员安全管理、系统建设管理和系统运维管理等方面的测评。  五、测评方法  在测评实施过程中，应采用访谈、检查和测试、渗透测试等测评方法进行，并与国家相关规范及标准的要求相符。  访谈是指测评人员通过引导信息系统相关人员进行有目的的（有针对性的）交流以帮助测评人员理解、分析或取得证据的过程；  检查是指测评人员通过对测评对象（如管理制度、操作记录、安全配置等）进行观察、查验、分析以帮助测评人员理解、分析或取得证据的过程；  测试是测评人员使用预定的方法/工具使测评对象产生特定的行为，通过查看和分析结果以帮助测评人员获取证据的过程；  渗透测试是模拟黑客的攻击方法，对受保护对象的应用系统、主机、网络进行攻击，从而验证测评对象的弱点、技术缺陷或漏洞的一种评估方法。  六、实施要求  本项目要求成交测评方，进行信息安全等级保护测评并信息安全等级保护评估报告，并作为项目业主验收的依据。  成交供应商应对整个系统进行安全功能验证、配置扫描、漏洞扫描、代码扫描等安全测评，对整个系统承载设备进行全方面扫描；应针对本项目制定完整的实施方案，包括但不限于进度安排、人力资源计划、质量保证、风险管理、沟通管理等内容。  （一）项目的资源配置  竞标人须在其技术文件中清晰陈述对于该项目的资源配置情况，包括：  1、项目组配备人员的能力与资质  2、测评环境构建方案  竞标人应在其技术文件中陈述拟安排的资源和可用性保障条件，明确拟投入项目人员的专业背景、项目实践经验、资质及技术能力说明、并提供相关人员资质证书复印件及原件备查。  安全评测应采用业界主流的测评工具进行测评，由竞标人提供，如果出现知识产权问题，责任归竞标人。  （二）工作流程  竞标人的技术文件中须清晰描述其如何安排项目的工作流程，包含但不限于以下环节：  1. 测评调研：对被测系统进行调研，熟悉测评需求。  2. 测评准备：测评方案、测评脚本等的编制和准备。  3. 测评方案评审：成交供应商、招标单位对测评方案进行评审。  4. 测评执行：完成测评方案中要求的所有内容，并填写详细测评记录。  5. 测评报告提交：提交正式信息安全等级保护评估报告。  （三）质量控制和保障  竞标人技术文件中须清晰陈述其对项目实施质量控制和质量保障的方法、控制的目标、内容与流程、项目沟通制度、对于变更的管理等。  七、测评结果  （一）在测评结束时必须提供信息系统的《信息安全等级保护测评报告》，内容包括但不仅限于以下方面：  1、物理安全情况及问题分析；2、网络安全情况及问题分析；3、主机系统情况及问题分析；4、应用安全情况及问题分析；5、数据安全及备份恢复情况及问题分析；6、安全管理制度情况及问题分析；7、安全管理机构情况及问题分析；8、人员安全管理风险分析；9、系统建设管理情况及问题分析；10、系统运维管理情况及问题分析；11、数据安全情况及问题分析；12、安全建设整改建议。  （二）提交原始评估数据包括但不仅限于：  1、主机安全测评数据；2、网络安全测评数据。3、主机安全测评数据；4、应用安全测评数据；5、数据安全测评数据；6、安全管理测评数据。  （三）提供所测评系统一式三份信息系统等级测评报告。  ★1、测评完成后，出具符合等保2.0相关技术标准要求、国家网络安全等级保护管理部门规范要求且公安机关认可的网络安全等级保护测评报告，纸质版3份、电子版（docx格式）1份，扫描版（PDF格式）1份。 |