第三章 采购需求

说明：

1. 为落实政府采购政策需满足的要求

（1）本竞争性磋商采购文件所称中小企业必须符合《政府采购促进中小企业发展管理办法》（财库〔2020〕46 号）的规定。

2. “实质性要求”是指采购需求中带“▲”的条款或者不能负偏离的条款或者已经指明不满足按响应文件按无效处理的条款。

3.采购需求中出现的品牌、型号或者生产厂家仅起参考作用，不属于指定品牌、型号或者生产厂家的情形。供应商可参照或者选用其他相当的品牌、型号或者生产厂家替代，但选用的竞标产品参数性能必须满足实质性要求。

4.供应商应根据自身实际情况如实响应磋商文件，不应仅将磋商文件要求的内容简单复制粘贴作为竞标响应，应当如实响应并能够提供相关证明材料（如有）。

5.供应商必须自行为其竞标产品侵犯他人的知识产权或者专利成果的行为承担相应法律责任。

本项目核心产品：无

本项目所属行业：软件和信息技术服务业

采购预算：2,100,000.00 元

一、项目要求及技术需求				
序号	**标的的名称**	**数量**	**单位**	**▲技术要求**
1	专网防火墙维保	1	项	提供采购人在用的奇安信 NSG 系列防火墙系统应用识别库、URL 分类特征库、病毒防护特征库、入侵防御特征库升级服务及威胁情报订阅服务三年，系统原有功能及模块须予以保留。 如需提供新设备，新设备须满足以下 1-22 条要求： 1.标准 1U 设备，单电源；配置≥8 个 10/100/1000M 自适应电口，2 个 SFP 插槽，2 个 SFP+插槽，另有 2 个接口板卡扩展插槽，1 个 Console 口，防火墙吞吐≥8Gbps，并发连接数≥200 万，每秒新建连接数≥10 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。 2.提供三年硬件质保和应用识别库、URL 分类特征库、病毒防护特征库、入侵防御特征库升级服务及威胁情报订阅服务。 3.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。 4.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。 5.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。（竞标时响应文件中需提供能够体现上述功能配置选项截图） 6.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。 7.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。 8.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。 9.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。 10.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。（竞标时响应文件中需提供能够体现上述功能配置选项截图） 11.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。 12.支持服务链编排功能，支持串接链和旁路链，支持网元组的方向和位置设置。 13.支持细粒度引流策略，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。 14.支持对编排的流量进行监控，至少能从网元组、引流策略两个维度对编排流量监控统计。

				15.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.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.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.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。（竞标时响应文件中需提供能够体现上述功能配置选项截图） 19.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.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.支持作为“探针”与采购人在用的态势感知平台联动，上报网络活动产生的数据至态势感知平台；并支持接收来自态势感知平台推送的处置策略，及时拦截绕过防御措施产生的高级威胁。 22.支持与本项目中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；并支持阻断“高风险”终端网络活动的同时，提示被阻断原因及重定向自定义网址。
2	互联网出口防火墙维保	1	项	提供采购人在用的奇安信 NSG 系列防火墙系统应用识别库、URL 分类特征库、病毒防护特征库、入侵防御特征库升级服务及威胁情报订阅服务三年，系统原有功能及模块须予以保留。 如需提供新设备，新设备须满足以下 1-22 条要求： 1.标准 1U 设备，单电源；配置≥8 个 10/100/1000M 自适应电口，2 个 SFP 插槽，2 个 SFP+插槽，另有 2 个接口板卡扩展插槽，1 个 Console 口，防火墙吞吐≥8Gbps，并发连接数≥200 万，每秒新建连接数≥10 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。 2.提供三年硬件质保和应用识别库、URL 分类特征库、病毒防护特征库、入侵防御特征库升级服务及威胁情报订阅服务。 3.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。

				4.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。 5.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。 6.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。 7.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。 8.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。 9.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。 10.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。 11.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。 12.支持服务链编排功能，支持串接链和旁路链，支持网元组的方向和位置设置。 13.支持细粒度引流策略，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。 14.支持对编排的流量进行监控，至少能从网元组、引流策略两个维度对编排流量监控统计。 15.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.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.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.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.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.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.支持作为“探针”与采购人在用的态势感知平台联动，上报网络活动产生的数据至态势感知平台；并支持接收来自态势感知平台推送的处置策略，及时拦截绕过防御措施产生的高级威胁。 22.支持与本项目中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；并支持阻断“高风险”终端网络活动的同时，提示被阻断原因及重定向自定义网址。
3	态势感知平台维保	1	项	提供采购人在用的奇安信 TSS 系列态势感知平台三年威胁情报更新及规则库升级，系统原有功能及模块须予以保留。 如需提供新设备，新设备须满足以下 1-13 条内容： 1.标准 2U 设备，CPU≥32 核，内存≥256G，系统盘≥960G SSD 固态硬盘，数据盘≥12＊8TB 机械硬盘，≥4 个千兆电口，≥3 个扩展插槽，最大日志处理速度≥60000eps； 2.提供三年产品维保及威胁情报及规则库升级服务。 3.支持常见协议识别并还原网络流量，用于取证分析、威胁发现，支持：http、dns、smtp、pop3、imap、webmail、DB2、Oracle、MySQL、sql server、Sybase、SMB、FTP、SNMP、telnet、nfs 等。 4.支持 TCP/UDP 会话记录、异常流量会话记录、web 访问记录、域名解析、SQL 访问记录、邮件行为、登录情况、文件传输、FTP 控制通道、SSL 加密协商、telnet 行为、IM 通信等行为描述。 5.支持自定义协议和端口，满足特殊场景下的流量抓取。 6.支持基于流量实时 IOC 匹配功能，设备具备 IOC，情报总量 370+万条。 7.支持基于工具特征的 WEBSHELL 检测，能通过系统调用、系统配置、文件的操作来及时发现威胁；如：中国菜刀、小马上传工具、小马生成器等。（竞标时响应文件中需提供能够体现上述功能配置选项截图） 8.支持基于代理程序的攻击检测，如 TCP 代理程序、HTTP 代理程序等。 9.支持与云端威胁情报中心联动，可对受害 IP、攻击 IP、IOC/规

				则 ID、文件 MD5 进行一键搜索，查看基本信息、开源情报、相关样本、可视化分析、域名解析、注册信息、关联域名、数字证书等。 10.支持从威胁情报、应用安全、系统安全和设备安全的业务场景维度对告警进行二次分析。 11.威胁情报维度分析包括：情报详情、影响资产列表、资产的行为（行为包含：DNS 解析、TCP 流量、UDP 流量、WEB 访问、文件传输）。 12.应用安全的细分维度包括：WEB 安全、数据库安全、中间件安全；系统安全的细分维度包括：暴力破解、弱口令、未授权访问、挖矿行为。 13.支持对告警进行加白，加白参数包括受害 IP、攻击 IP、威胁情报、规则、XFF、URL、威胁名称。（竞标时响应文件中需提供能够体现上述功能配置选项截图）
4	服务器区防火墙	2	套	1.标准 2U 设备，冗余电源；配置≥8 个 10/100/1000M 自适应电口，≥8 个 SFP 插槽，≥6 个 SFP+插槽，另有 2 个接口板卡扩展插槽，≥4TB 机械硬盘，≥1 个 Console 口，配置液晶屏，含三年硬件质保和应用识别库、URL 分类特征库、病毒防护特征库、入侵防御特征库升级服务及威胁情报订阅服务。 2.防火墙吞吐≥40Gbps，并发连接数≥1200 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。 3.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。 4.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。 5.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。 6.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。 7.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。 8.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。 9.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。 10.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。 11.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。 12.支持服务链编排功能，支持串接链和旁路链，支持网元组的方向和位置设置。 13.支持细粒度引流策略，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。 14.支持对编排的流量进行监控，至少能从网元组、引流策略两个维度对编排流量监控统计。 15.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.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.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.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.支持作为“探针”与采购人在用的态势感知平台联动，上报网络活动产生的数据至态势感知平台；并支持接收来自态势感知平台推送的处置策略，及时拦截绕过防御措施产生的高级威胁。 20.支持与本项目中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；并支持阻断“高风险”终端网络活动的同时，提示被阻断原因及重定向自定义网址。
5	安全管理区防火墙	1	套	1.标准 1U 设备，单电源；配置≥8 个 10/100/1000M 自适应电口，≥2 个 SFP 插槽，≥2 个 SFP+插槽，另有 2 个接口板卡扩展插槽，≥1TB 机械硬盘，≥1 个 Console 口，含三年硬件质保和应用识别库、URL 分类特征库、病毒防护特征库、入侵防御特征库升级服务及威胁情报订阅服务。 2.防火墙吞吐≥8Gbps，并发连接数≥200 万，每秒新建连接数≥

				10 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。 3.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。 4.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。 5.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。 6.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。 7.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。 8.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。 9.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。 10.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。 11.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。 12.支持服务链编排功能，支持串接链和旁路链，支持网元组的方向和位置设置。 13.支持细粒度引流策略，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。 14.支持对编排的流量进行监控，至少能从网元组、引流策略两个维度对编排流量监控统计。 15.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.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.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.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.支持作为“探针”与采购人在用的态势感知平台联动，上报网络活动产生的数据至态势感知平台；并支持接收来自态势感知平台推送的处置策略，及时拦截绕过防御措施产生的高级威胁。 20.支持与本项目中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；并支持阻断“高风险”终端网络活动的同时，提示被阻断原因及重定向自定义网址。
6	入侵防御系统	2	套	1. 2U 机箱，冗余电源；配置≥8 个 10/100/1000M 自适应电口，≥8 个千兆 SFP 插槽，≥6 个万兆 SFP+插槽，2 个扩展插槽，≥1 个 Console 口，≥2 个 USB 接口，≥4T 机械硬盘；配置液晶屏，提供三年硬件维保、入侵防御特征库升级、应用识别库升级和威胁情报订阅服务。 2.网络层吞吐≥40Gbps，入侵防御吞吐≥6Gbps，并发链接≥800 万，新建速率≥20 万/秒。 3.产品支持路由、旁路、交换以及混合模式接入。 4.支持基于 IPv4 或 IPv6 的 TCP、HTTP、DNS、ICMP、Radius 方式的链路探测联动，同时 TCP 与 HTTP 可使用自定义目标端口进行测试；支持 BFD 联动。（竞标时响应文件中需提供能够体现上述功能配置选项截图） 5.支持 IPv4 和 IPv6 的静态 DNS 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域名和 IP 对应关系，代理 DNS 服务器返回查询结果。 6.支持 4in6 隧道过渡技术，至少包含 DS-Lite 协议中的 b4 和 aftr 能力，以及支持从 DHCPv6 服务器或手动方式获取 AFTR 参数。 7.支持命中时间分析和安全策略推荐，命中时间分析展示被命中的安全策略的名称、状态、命中数、策略创建时间、首次命中时间和最近命中时间；安全策略推荐可以指定策略流量，分析后自动生成源地址精度安全策略。 8.支持应用识别，应用特征库包含的应用数量（非应用协议的规则总数）大于 3000 种，可深度识别每种应用的属性，为每种应用提供预定义的风险系数，并将应用基于类型、数据传输、风险等级等特征分类。 9.支持对应用的文件传输行为进行上传、下载、双向的文件类型

				过滤，应用至少包含即时通讯、常用协议、文件共享、论坛、博客、网页邮件、微博七种分类。（竞标时响应文件中需提供能够体现上述功能配置选项截图） 10.支持基于 Flood 攻击和恶意扫描的流量自学习能力，可自定义开始时间、学习时长、查看学习结果，并根据学习结果一键生成 DDOS 防护策略。 11.支持 RA 管控策略，用于防止 RA 攻击。支持基于源 MAC、SSLA MAC、源地址、VLAN、前缀、跳数等条件进行 RA 管控。能够基于 M 标记、O 标记进行置位和不置位检测管控。 12.支持弱口令检测，支持主动检测和被动检测两种检测方式；支持基于网段、协议、用户名字典、弱口令字典进行完整扫描，执行方式包含手动和自动；能够基于数字、字母、数字和字母、自然顺序、键盘顺序、特殊字符、用户名、重复字符等进行弱口令检测。 13.支持暴力破解能力，至少支持 FTP、IMAP、WEBLOGIC、VNC、Telnet、RLOGIN、RDP 等 14 种协议，且可手动设置攻击频率、持续检测时间，并支持日志、阻断、放行、重置和加入动态黑名单的处置动作。 14.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。
7	Web 应用防火墙	1	套	1.标准 2U 机箱，冗余电源，具有液晶面板，1TB 硬盘。配置≥4 个千兆 10/100/1000M 自适应电口，≥4 个千兆 SFP 插槽，≥2 个万兆 SFP+插槽，≥1 个 Console 口，≥2 个 USB 口，另有 1 个扩展插槽。支持 Web 安全保护≥512 个站点。含三年 WAF 软件特征库服务及硬件质保服务。 2.网络吞吐量≥10Gbps，应用层处理能力≥6Gbps，网络并发连接数≥400 万，HTTP 并发≥150 万，HTTP 新建连接数≥60000/s。 3.支持在旁路镜像阻断模式下，可配置多组阻断以及镜像口，对检测到的攻击进行旁路阻断，并可指定对端设备 MAC 地址。 4.支持产品页面一键断网（禁止访问）功能，在特殊情况下，实现对特定网站的快速下线。 5.支持防暴力破解功能，可支持频率阈值，动态令牌以及频率阈值+动态令牌等三种方式实现暴力破解防护。 6.支持地域访问控制功能，支持根据国家、地区、城市等元素进行地域访问控制，并可自定义访问过期时长。 7.产品具备蜜罐防御功能，提供伪造的后台管理系统页面防御功能。（竞标时响应文件中需提供能够体现上述功能配置选项截图） 8.支持检测并清洗的攻击类型：IP 攻击，TCP 攻击，UDP 攻击，ICMP 攻击，DNS 攻击，HTTP 攻击等 20 多种 DDoS 攻击类型。 9.支持入侵防护功能，并提供入侵防护特征库，特征库需要提供 22 种类型并提供至少 14000 条入侵检测特征库。（竞标时响应文件

				中需提供能够体现上述功能配置选项截图） 10.支持虚拟补丁功能，支持导入 appscan 和 RayScan 扫描器的扫描结果生成 WAF 的规则，对此类网站漏洞直接防护。 11.支持智能封禁，通过对网站发起的攻击次数、危害级别两个维度进行算法分析与识别，进行智能封禁，并自定义攻击者封禁时间。 12.支持非法 URL 外联检测功能，针对特定外联 URL 进行监控或阻断，并且支持自定义 URL 地址。 13.产品具备 HTTP 访问控制，可根据实际网络状况自定义请求方法等参数的访问控制规则，支持设置 HTTP 0.9/1.0/1.1/2.0 版本和 10 多种 http 访问控制方法。 14.支持系统状态实时展示，需支持转发、过载、防护等三种系统状态。 15.支持攻击态势大屏实时展示，可通过产品自带的实时态势监测模块进行攻击态势地图展示，包含对源地址、源地域、目标资产、安全防护攻击类型、攻击趋势、HTTP 并发请求及实时事件的动画统计。（竞标时响应文件中需提供能够体现上述功能配置选项截图） 16.支持日志快速响应功能，日志具备一键黑名单设置以及一键白名单排除功能。
8	堡垒机系统	1	套	1、国产化产品，2U 硬件，冗余电源；配置≥6 个千兆电口，≥4 个千兆光口，≥1 个接口扩展槽，硬盘容量≥4T，配置国密密码卡，配置液晶屏；提供三年标准售后维保服务； 2、具备≥50 路图形会话或 500 路字符会话并发，可管理设备数量≥500 个，配置 500 个资源授权许可； 3、具备多因子认证，方式包括手机令牌、手机短信、动态令牌、国密 USBKey、指纹识别等多因子认证方式； 4、具备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；（竞标时响应文件中需提供能够体现上述功能配置选项截图） 5、具备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； 6、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；（竞标时响应文件中需提供能够体现上述功能配置选项截图） 7、具备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； 8、具备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；（竞标时响应文件中需提供能够体现上述功能配置选项截图） 9、申请工单具备文件管理、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； 10、具备采用国密算法进行重要数据加解密，包括但不限于用户信息、资源账户等； 11、具备水印功能，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，具备在 H5 运维 SSH、RDP、TELNET、VNC、应用发布等资源时显示水印； 12、具备专属手机 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； 13、堡垒机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； 14、产品须内置硬件国密加密卡对日志信息和访问控制信息进行完整性保护；
9	日志审计系统	1	套	1. 标准 1U 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；提供三年硬件质保和软件升级服务。 2. 综合日志处理性能≥4000EPS，日志采集处理均值≥11000EPS，提供 210 个审计节点授权许可。 3. 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。 4. 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。 5. 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。 6. 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。（竞标时响应文件中需提供能够体现上述功能配置选项截图） 7. 系统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。 8. 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。 9. 针对匹配的多条范化策略，系统支持用户手工设置策略匹配优先级。（竞标时响应文件中需提供能够体现上述功能配置选项截图） 10. 日志解析字段内置 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。

				11. 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。（竞标时响应文件中需提供能够体现上述功能配置选项截图） 12. 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。 13. 系统支持即席在线查询，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。 14. 可以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。 15. 支持将统计结果保存为仪表板、报表和策略，提供可编辑的自定义仪表板。 16. 系统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。
10	VPN（综合网关）	1	套	1. 2U设备，冗余电源，配置≥6个千兆电口，≥4个千兆SFP插槽，≥1个扩展槽，配置国密密码卡，≥4TB机械硬盘，配置≥250个并发用户授权，提供3年质保。 2.支持UDP+TCP单包授权机制，UDP+TCP方式默认不开放端口，可避免业务应用的端口被扫描，进而避免利用端口对业务应用发起攻击的风险。 3.支持通过输入安全码激活客户端，完成SPA敲门。安全码可支持共享码、一人一码两种模式。 4.提供用户概览统计能力，包括用户总数、启用用户数、锁定用户数、禁用用户数等信息，提升管理员运维能力。 5.支持用户身份属性的自定义扩展，以便管理员可以根据自身需要对用户属性扩展，而不需要重新部署或升级系统程序。 6.支持用户身份打标签，以实现对不同的用户打不同标签，并可以基于标签进行访问控制。 7.提供设备概览统计能力，包括终端总数、启用终端数、锁定终端数、禁用终端数等信息。提供设备绑定概览统计能力，包括绑定总数、管理员绑定数、申请绑定数、自助绑定数等信息，提升管理员运维能力。（竞标时响应文件中需提供能够体现上述功能配置选项截图） 8.支持设备审批概览统计能力，管理员能够明确知道总数、待审批数、已通过数、已驳回数等信息。 9.支持PC端发起访问应用的采集，能够对应用进行标记为可信或不可信，可用于访问控制策略，从而实现基于访问进程的细粒度控制措施。 10.支持UOS、Kylin、Linux端操高危端口、运行的软件、零信任客户端版本、运行的杀毒软件、运行的远控软件、运行的虚拟机软件、安装的防病毒软件等环境感知和采集，以实现基于终端安全状况的访问控制措施。 11.支持应用概览统计能力，包括应用总数、WEB应用数、隧道应

				用数等信息，提升管理员的运维能力。 12.支持 WEB 应用支持数据传递，可通过 URL、Header、Cookie 自定参数传递，以满足应用对特定参数的需要，从而实现对现网应用无需修改即可正常访问。 13.支持设备认证，提供认证策略配置，可根据是否签发设备、导入设备、绑定设备进行设备认证。 14.支持应用限流限速功能，支持通过限制请求并发设置阈值、通过限制请求速度来设置阈值、通过限制单位时间内的请求数设置阈值、限制响应传输速率设置阈值、通过限制请求大小设置阈值。（竞标时响应文件中需提供能够体现上述功能配置选项截图） 15.支持预防 synflood 攻击、忽略 icmp 回显请求、并支持开启 ProxyProtocol 来识别并传递源 IP 地址。(竞标时响应文件中需提供能够体现上述功能配置选项截图） 16.支持与本项目终端安全管理系统联动，可以基于本项目终端安全管理系统对终端设备评分实现动态访问控制，提升终端安全管控能力。
11	终端安全管理系统	1	套	1. 软件形式交付，包含控制中心和客户端软件。控制中心能够实现对客户端的集中管理，包括终端统一部署、策略配置、任务分发、集中监控、日志报表等功能；支持根据客户端点数的增加进行横向扩展；具备防病毒、补丁管理、主机防火墙、终端管控、移动存储、停服系统加固等功能，含 3000 个参照或相当于 windows 客户端授权；提供一年的特征库升级及维保服务。 2. 客户端支持安装参照或相当于 Windows XP_SP3 及以上/Windows Vista/Windows 7/Windows 8/Windows 10。 3. 支持终端用户和管理员是一套账号管理系统，简化账号管理复杂度，一个账号解决所有身份认证，既可以用于终端登录，也可以用于管理中心。 4. 管理控制中心当登录账号输入密码错误次数超过锁定阈值后账号将被锁定，且可设置锁定时间，该时间内账号登录请求不被接受。同时应支持双因子认证登录方式，提高安全性（竞标时响应文件中需提供能够体现上述功能配置选项）。 5. 客户端主程序、病毒库版本支持按分组和多批次进行灰度更新，保持完成终端能力更新。 6. 支持对进程防护、注册表防护、驱动防护、U 盘安全防护、邮件防护、下载防护、IM 防护、局域网文件防护、网页安全防护、勒索软件防护。 7. 支持对压缩包内的病毒扫描，支持多层压缩包的扫描，可自定义配置压缩包的扫描层数，至少 10 层模式下的扫描。（竞标时响应文件中需提供能够体现上述功能配置选项截图） 8. 支持自动阻止远程登录行为，防护黑客远程爆破和拦截恶意的远程登录。 9. 支持无文件攻击防护、文档攻击防护、横移渗透攻击防护、内存攻击防护。

				10. 支持不少于三个杀毒引擎混合使用，提高病毒检出率。 11. 支持对终端当扫描到感染型病毒、顽固木马时，自动进入深度查模式，可设置禁止终端用户管理路径或文件白名单、禁止终端用户管理扩展名白名单、扫描时不允许终端用户暂停或停止扫描任务。 12. 支持扫描资源占用设置，可设置不限制、均衡型、低资源三种模式。 13. 支持开启自动修复漏洞，包括开机时修复，并支持随机延迟执行、间隔修复和按时间段修复，可设置延迟时间、间隔修复时间和修复时间段。 14. 支持按照补丁的维度统计补丁安装情况，包括补丁号、系统类型、补丁类型、补丁级别、补丁名称、补丁描述、发布日期、发布状态、文件数量、发现补丁次数、已安装补丁次数、忽略补丁次数、卸载补丁次数、未更新补丁库。并支持导出统计报表。 15. 支持预先设置好补丁灰度发布批次漏洞修复策略，每当控制台更新补丁库，根据企业环境自动先推送给第一个小批次分组，如无问题自动推送给下一个批次，直到推送给全网。（竞标时响应文件中需提供能够体现上述功能配置选项截图） 16. 支持主机防火墙功能，通过添加 IP、域名规则、支持允许/拒绝规则、支持任意流向拦截和允许，支持 TCP、UDP、TCP+UDP、ICMP、多播和组播，支持自定义端口范围、支持自定义目标 IP，支持输入 IP 范围。 17. 支持展示防火墙上报日志，展示终端基础信息、拦截规则名称、拦截时间、操作、协议、源地址，目的 IP/域名、源端口、目的端口。 18. 支持对外设进行多维度的放行，包括设备名称、PID/VID、实例路径，通过添加实现例外或加黑。（竞标时响应文件中需提供能够体现上述功能配置选项截图） 19. 支持对终端节能管理，支持对长时间运行、定时关机、空闲节能、工作时间外开机等节能类型设定策略，支持仅提示、关机、注销、锁定、关闭显示器、锁定+关闭显示器、休眠和睡眠处理。并支持提示倒计时弹窗，可设置在终端取消后下一次提醒时间。 20. 支持对网卡进行防护，支持阻止终端修改 IP 地址、使用动态 IP 地址、热点创建和 IPV6 地址使用等，可自定义提示内容和生效时间。 21. 支持管理员设置自动审批客户端注册请求；不同分组可设置不同审批规则。 22. 支持移动存储介质外出管理，并可以设置外出使用权限与有效时间。（竞标时响应文件中需提供能够体现上述功能配置选项截图） 23. 支持 U 盘与终端进行点对点的授权，可以控制单个 U 盘在不同终端上拥有不同的使用权限。 24. 支持针对参照或相当于 Windows XP、Windows7 系统带来安全

				隐患的设计机制进行加固性修复，支持远程漏洞攻击防护、本地钓鱼攻击防护和浏览器漏洞攻击防护。
12	计算机终端防护升级平台切换及终端客户端的安装	1	项	提供采购人在用的奇安信天擎终端安全管理系统升级替换服务，将版本升级至最新采购版本，升级范围包括控制中心及客户端。
13	重大事件保障服务	1	项	在重要时期为关键信息系统提供：组织架构设计、积极防御、实时检测、响应处置、攻击预测等安全服务，以提高组织的网络安全保障能力，保障重大活动的顺利进行。
14	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。采购人供给全部材料后 10 日内供应商提交《等级保护差距测评报告》。制定采购人安全需求分析、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《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）、《信息安全技术 网络安全等级保护实施指南》（GB/T 25058-2019）、《信息安全技术 网络安全等级保护测评要求》（GB/T 28448-2019），参照《信息系统安全管理要求》（GB/T 20269-2006）、《信息系统安全工程管理要求》（GB/T 20282-2006）等标准和规范要求，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。采购人供给全部材料后 10 日内供应商提交《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 协助采购人进行信息安全等级保护安全技术整改。根据《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）、《信息安全技术 网络安全等级保护实施指南》（GB/T 25058-2019）、《信息安全技术 网络安全等级保护测评要求》（GB/T 28448-2019），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。采购人供给全部材料后 10 日内供应商提交《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，对新增的安全设备/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、协助采购人进行三级等保测评的准备和整改工作： 协助采购人进行三年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：《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）、《信息安全技术 网络安全等级保护实施指南》（GB/T 25058-2019）、《信息安全技术 网络安全等级保护测评要求》（GB/T 28448-2019）、《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）等。对采购人系统安全漏洞扫描（通过专业工具）、生成信息系统漏洞扫描报告，并协助测评机构对采购人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法和手段进行，并与国家相关规范及标准的要求相符。采用安全扫描设备及软件产品辅助整改工作的完成。 对测评机构提供的等保测评报告进行整改。测评机构提供的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。编写好采购人的信息系统等保所需的所有资料，包括但不限于制度、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 ⑤采购人供给全部材料后 10 日内供应商提交《漏洞扫描报告》。 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）采购人供给全部材料后 10 日内供应商提交《WEB 应用扫描报告》。 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； （3）采购人供给全部材料后 10 日内供应商提交《安全配置检查报告》。 三、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。采购人供给全部材料后 10 日内供应商提交《应急响应报告》。 （1）内容：在采购人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 四、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。采购人供给全部材料后 10 日内供应商提交训材料，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》等。 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 五、驻场维护调试服务 针对采购人现有的安全设备，要求供应商能提供 1 名驻采购人现场人员在现场 1 年的安全分析服务； 1、针对采购人现有的所有安全设备，调试安装应用识别规则库的服务 2、针对采购人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、采购人供给全部材料后 10 日内供应商提交《安全设备巡检报告》
15	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系统进行测评服务，协助采购人顺利通过三年等保测评（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）、《信息安全技术 网络安全等级保护实施指南》（GB/T 25058-2019），广西壮族自治区公安厅《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；测评供应商工作中的过程和文档，具有规范性，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，保证采购人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

				不能对采购人各系统的运行和业务的正常提供产生影响；对测评过程中获得的采购人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人利益的行为。 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) 《网络安全等级保护安全设计技术要求》(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 本项目要求成交供应商，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，并作为项目采购人验收的依据。 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 竞标供应商须在其竞标时的响应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

				竞标供应商应在其竞标时的响应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、并在签订合同时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测评工具进行测评，由竞标供应商提供，如果出现知识产权问题，责任归竞标供应商。 （二）工作流程 竞标供应商的竞标时的响应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、采购人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 竞标供应商的竞标时的响应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）提供测评当年所测评系统一式六份信息系统等级测评报告，持续三年。

				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 6 份、电子版（docx 格式）1 份，扫描版（PDF 格式）1 份，持续三年。

▲二、商务要求	
合同签订时间	自成交通知书发出之日起 25 日内。
合同履约期限	服务期限：签订合同之日起 90 日历日内整改完成测评通过，自项目测评通过并验收合格之日起运维期持续 3 年；
后续服务要求	1.本项目成交供应商须提供不少于 3 年系统运维服务，在运维期内应当为采购人提供以下技术支持和服务： 1.1 电话咨询，成交供应商应当为采购人提供技术援助电话，解答采购人在使用中遇到的问题，及时为采购人提出解决问题的建议。 1.2 在 1 年的驻场维护调试服务之后的现场响应，采购人遇到使用或技术问题，电话咨询不能解决的，成交供应商应在 24 小时内到达现场进行处理，到达现场后 48 小时内解决问题，恢复正常使用。 1.3 技术升级，在运维期内，如果成交供应商的产品或服务升级，成交供应商应及时通知采购人，并提供相应的系统升级服务，费用均包含在最后报价中，采购人不再另行支付。 1.4 运维期内成交供应商为采购人所提供的所有技术支持和服务以及上门维修、更换零部件费用均包含在最后报价中，采购人不再另行支付。 2.其他服务要求：成交供应商应当为采购人提供终身技术援助电话，解答采购人在使用中遇到的问题，及时为采购人提出解决问题的建议。 3.培训：成交供应商须对其提供产品或服务的使用和操作应尽培训义务。成交供应商应提供对采购人的基本培训，使采购人使用人员熟练掌握所培训内容，熟练掌握全部功能，培训的相关费用包括在最后报价中，采购人不再另行支付。 4.供应商竞标时必须于响应文件中提供后续服务承诺，承诺至少包含以上内容。
交付地点	广西百色市右江区内采购人指定地点。
报价要求	竞标报价应当包含满足本次竞标全部采购需求所应提供的服务的价格；包含所有服务、产品成本、投入人员、劳务、住宿、管理、交通、安装调试、咨询、检验、测评、技术培训、技术资料、整改服务、验收、维护、必要的保险费用、利润、各项税费、政策性文件规定及合同包含的所有风险、责任等各项所有费用。合同费用已包含因项目需要召开的专家审查会、测评服务、验收过程中产生的相关费用等，合同费用在合同期间不予调整。
付款方式	1.无预付款；

	2.合同签订后，成交供应商提供整改服务的工作量达到60%的10个工作日内，采购人支付合同价款的20%； 3. 完成服务配套软件平台搭建并通过网络安全三级等级保护测评及驻场人员到位，成交供应商提供合法发票后的10个工作日内采购人支付合同价款的20%； 4. 自项目通过网络安全三级等级保护测评并验收合格之日起运维期每满1年后的10个工作日内，采购人向成交供应商支付合同总金额的20%（3年共计支付合同总金额的60%）。 5.每次付款前成交供应商应开具同等金额发票给采购人。
服务承诺要求	供应商请尽量在响应文件中提供及时响应的项目服务承诺，服务承诺可包括：测评通过期限、运维期，服务过程中设施设备使用时常见、多发的故障、问题及服务工作的重点、难点和解决方法，服务响应时间；拟投入本项目人员、供应商的技术力量、定期维护、技术培训、保密措施、问题解决方法和确保服务的质量水平，在运维期外提供维修、运维方案、提供保障服务等。
安全与保密要求	1.成交供应商在服务期间应遵守采购人单位的保密制度，履行包括在运维期结束后承诺保密义务，并承担相应的涉密责任。 2.成交供应商的驻点工作人员在提供服务过程中，对所接触到的所有数据信息负有保密义务。
三、与实现项目目标相关的其他要求	
（一）供应商的履约能力要求	
信誉、管理体系	供应商可结合“第四章 评标方法及评标标准”自行提供。
业绩	供应商可结合“第四章 评标方法及评标标准”自行提供。
（二）验收标准	
1.验收标准：符合现行国家相关标准、行业标准、地方标准或者其他标准、规范，以及本项目的竞争性磋商文件要求、响应文件承诺。 2.验收过程中所产生的一切费用均由成交供应商负责承担。报价时应考虑相关费用。 3.采购人在验收时将对照竞争性磋商文件的技术要求及响应文件承诺情况进行全面核对检验，如不符合竞争性磋商文件的技术需求及要求以及提供虚假承诺的，按相关规定做退货处理及违约处理，成交供应商承担所有责任和费用，采购人保留进一步追究责任的权利。	
（三）其他要求	
1. 供应商承诺拟投入本项目的项目经理、技术管理人员，成交供应商如更换服务组成员，需要书面提前通知采购人，按照竞争性磋商文件的技术要求，变更的人员必须具备专业知识与技能，经采购人同意	

后才能更换人员；否则视为违约。

2. 成交供应商应遵守《中华人民共和国保守国家秘密法》，严格执行保密制度，不得向第三方泄露其在提供服务期间获得采购人的技术、商业机密，否则须承担因此产生的全部责任。

3. 根据本项目需求，供应商可在响应文件中提供针对本项目的项目实施方案、技术培训方案。

注：上述项目实施方案、技术培训方案评分详见第四章“评标办法及评标标准”。