

清镇市人民检察院检察工作网及互联网等级
保护建设项目
工程量清单

(封面)

项目序列号： P5201002024000C2B

采购单位： 清镇市人民检察院

投标单位： 贵州嘉益科技有限公司

法定代表人：

编制人员：

贺娟

编制日期： 2024 年 11 月 20 日

采购清单及技术参数

品目编号：YGCQ-ZC-2024-20-779-公							品目名称：清镇市人民检察院工作网及互联网登记保护建设项目				
编号	采购货物	单位	数量	单价	合价	控制单价（非必填）	是否允许超过控制价	产地	品牌	型号	生产厂家
一	工作网	批	1				否	/	/	/	/
1.1	防火墙(千兆)	台	2	77200	154400		否	深圳市南山区	深信服	AF-1000-L1600-1K	深信服科技股份有限公司
1.2	防火墙IPS模块	套	2	8000	16000		否	深圳市南山区	深信服	IPS-2	深信服科技股份有限公司
1.3	防火墙AV模块	套	2	8000	16000		否	深圳市南山区	深信服	AV-2	深信服科技股份有限公司
1.4	防火墙(百兆)	台	2	37000	74000		否	北京市海淀区	启明星辰	USG-FWGZX-1000DP-G006(百兆)	北京启明星辰信息安全技术有限公司
1.5	防火墙(百兆)IPS模块	套	2	7000	14000		否	北京市海淀区	启明星辰	二年入侵防御升级	北京启明星辰信息安全技术有限公司
1.6	防火墙(百兆)AV模块	套	2	7000	14000		否	北京市海淀区	启明星辰	二年入侵防御升级	北京启明星辰信息安全技术有限公司
1.7	运维安全管理系统	台	1	110000	110000		否	深圳市南山区	深信服	OSM-1000-L1600-1K	深信服科技股份有限公司
1.8	日志审计系统	台	1	137000	137000		否	北京市西城区	奇安信	网神SecFox日志收集与分析系统LAS-PKQ2M/V5.0	奇安信网络信息安全技术(北京)股份有限公司
1.9	交换机	台	1	8700	8700		否	广东省深圳市	华为	S5735-L24T4S-A-V2	华为技术有限公司
二	互联网	批	1				否	/	/	/	/
2.1	下一代防火墙(利旧)	台	1				否	福建省福州市	锐捷	RG-WALL1600-S3700	锐捷网络股份有限公司
2.2	防火墙防病毒及入侵防御授权	套	1	9600	9600		否	福建省福州市	锐捷	RG-WALL1600-S3700V2.0-IPS/AV-1Y	锐捷网络股份有限公司

[illegible]

规格、技术参数明细表

编号：一	货物名称：工作网
详细参数：	

编号：1.1	货物名称：防火墙(千兆)
详细参数：	
1、★自主可控要求：要求芯片及操作系统自主可控； 2、★标准机架式设备，内存8G，接口6千兆电口； 3、★性能要求：网络层吞吐量4G，应用层吞吐量2G，防病毒吞吐量600M，IPS吞吐量600M，并发连接数200万，HTTP新建连接数4.5万； 4、支持自主知识产权的专用操作系统，应用多核并行处理技术保障产品处理性能； 5、支持路由模式、透明模式、虚拟网线模式、旁路镜像模式等多种部署方式； 6、支持路由类型、协议类型、网络对象、国家地区等条件进行自动选路的策略路由； 7、支持基于国家/地区的流量管理功能； 8、支持基于网络区域、网络对象、MAC地址、服务、应用、域名等维度进行访问控制策略设置； 9、产品支持CC攻击防护功能，保障针对CC攻击的检测效果； 10、支持对SMTP、HTTP、FTP、SMB、POP3、HTTPS、IMAP等协议进行病毒防御； 11、▲产品内置超过4500种WEB应用攻击特征，支持对跨站脚本（XSS）攻击、SQL注入、文件包含攻击、信息泄露攻击、WEBSHELL、网站扫描、网页木马等攻击类型进行防护（提供具有资质的第三方机构出具的检测报告并加盖原厂商公章）； 12、产品内置不低于12000种漏洞规则，同时支持在控制台界面通过漏洞ID、漏洞描述等条件查询漏洞特征信息，支持用户自定义IPS规则； 13、▲产品支持服务器漏洞防扫描功能，并对扫描源IP进行日志记录和联动封锁（提供具有资质的第三方机构出具的检测报告并加盖原厂商公章）； 14、当主机故障时，双机切换时不丢包，并可实现双机部署下升级不断网。	

编号：1.2	货物名称：防火墙IPS模块
详细参数：	
1、支持基于策略的入侵检测与防护，可针对不同的源目IP地址、源MAC地址、服务、时间、安全域、用户等，采用不同的入侵防护策略； 2、支持无需重启IPS引擎的情况下灵活修改策略，保障在配置维护的时候也能够进行攻击保护； 3、内置IPS特征库，特征规则数量不少于3,600条，特征库可按分组进行管理，连续10条以上特征库数量； 4、支持细粒度的自定义IPS特征功能，要求支持DNS\HTTP\FTP\TFTP\TELNET\SNMP\POP3\SMTP\IMAP\等17大类应用层协议的自定义，可以精准设置各个协议字段内容，例如字符内容、偏移、长度等细粒度的参数。	

编号：1.3	货物名称：防火墙AV模块
详细参数：	
1、支持基于策略的病毒扫描与防护，可针对不同的源目IP地址、源MAC地址、服务、时间、安全域、用户等，采用不同的病毒防护策略； 2、支持应用协议自识别，可以实现HTTP,SMTP,FTP,POP3,IMAP,FTP,WEBMAIL多种应用协议下的病毒防护，支持自定义非标准端口下应用协议的病毒防护； 3、支持隔离病毒源地址，防止病毒源主机访问内部网络，提高网络整体安全性； 4、支持多接口可旁路的病毒文件传输监听检测方式，可并行监听并检测多个接口、多个网段内的病毒传输行为，用于高可靠性要求的旁路应用环境。	

编号：1.4	货物名称：防火墙(百兆)
详细参数：	
1、★自主可控要求：要求芯片及操作系统自主可控； 2、★标配4个10/100/1000M Base-TX，2个千兆光口；内置64G SSD硬盘； 3、★整体吞吐2.4G，整机并发连接数430万，每秒新建8万/秒； 4、支持路由、透明、旁路、混合工作模式； 5、支持静态路由，动态路由（OSPF、RIP、BGP、ISIS等），VLAN间路由，单臂路由，组播路由等； 6、▲支持基于应用及WEB地址URL的策略路由，可实现为不同的应用类型智能选择相应的链路； 7、支持链路聚合功能，支持802.3ad和静态轮询、热备等多种模式，MAC、MAC&IP、IP&Port多种聚合负载算法； 8、支持同一个地址对象中可以包含IP、IP段、IP range、排除地址等多种类型； 9、▲支持一体化安全策略配置，可以通过一条策略实现用户认证、IPS、AV、URL过滤、协议控制、流量控制、并发、新建限制、垃圾邮件过滤、审计等功能,简化用户管理； 10、支持针对策略中的源、目的地址进行新建限制，可以针对单IP(或地址范围)进行新建控制； 11、支持基于策略的入侵检测与防护，可针对不同的源目IP地址、源MAC地址、服务、时间、安全域、用户等，采用不同的入侵防护策略； 12、支持专业的HTTP Flood攻击防护：可以实现get和post的攻击防护，且get防护算法支持4类；支持独立url处理动作；以上防护功能均可以基于聚类分析、可信度、回探等多种防御机制。	

编号：1.5	货物名称：防火墙(百兆)IPS模块
详细参数：	
1、支持基于策略的入侵检测与防护，可针对不同的源目IP地址、源MAC地址、服务、时间、安全域、用户等，采用不同的入侵防护策略； 2、支持无需重启IPS引擎的情况下灵活修改策略，保障在配置维护的时候也能够进行攻击保护； 3、内置IPS特征库，特征规则数量不少于3,600条，特征库可按分组进行管理，连续10条以上特征库数量； 4、支持细粒度的自定义IPS特征功能，要求支持DNS\HTTP\FTP\TFTP\TELNET\SNMP\POP3\SMTP\IMAP\等17大类应用层协议的自定义，可以精准设置各个协议字段内容，例如字符内容、偏移、长度等细粒度的参数。	

编号：1.6	货物名称：防火墙(百兆)AV模块
详细参数：	
1、支持基于策略的病毒扫描与防护，可针对不同的源目IP地址、源MAC地址、服务、时间、安全域、用户等，采用不同的病毒防护策略； 2、支持应用协议自识别，可以实现HTTP,SMTP,FTP,POP3,IMAP,FTP,WEBMAIL多种应用协议下的病毒防护，支持自定义非标准端口下应用协议的病毒防护； 3、支持隔离病毒源地址，防止病毒源主机访问内部网络，提高网络整体安全性； 4、支持多接口可旁路的病毒文件传输监听检测方式，可并行监听并检测多个接口、多个网段内的病毒传输行为，用于高可靠性要求的旁路应用环境。	

编号：1.7	货物名称：运维安全管理系统
详细参数：	
1、★自主可控要求：要求芯片及操作系统自主可控； 2、★设备配置6个千兆电口，4千兆光口SFP；要求配置50个资产运维授权数，最大可扩展资产运维授权数150个；配置三年软件升级及硬件质保。 3、★设备图形运维最大并发数100，字符运维最大并发数200； 4、支持通过动作流配置提供广泛的应用接入支持，无论被接入的资源如何设计登录动作，通过动作流配置都可以实现单点登陆和审计接入； 5、支持在授权基础上自定义访问审批流程，可设置一级或多级审批人，每级审批可指定通过投票数，需逐级审批通过才可最终发起运维操作； 6、图形资源访问时，支持键盘、剪切板、窗口标题、文件传输记录，并且对图形资源的审计回放时，可以从某个键盘、剪切板、窗口标题、文件传输记录的指定位置开始回放； 7、内置三员角色的同时支持角色灵活自定义，可根据用户实际的管理特性或特殊的安全管理组织架构，划分管理角色的管理范畴； 8、支持一对一、一对多、多对多授权，如将单个资产授权多个用户，一个用户授予多个资产，用户组向资产组授权； 9、▲支持命令审批规则，用户执行高危命令时需要管理员审批后才允许执行；命令审批规则可以指定运维人员、访问设备、设备账号及命令审批人； 10、支持web页面直接发起运维，无需安装任何控件，并同时支持调用SecureCRT、Xshell、Putty、WinSCP、FileZilla、RDP等客户端工具实现单点登陆，不改变运维人员操作习惯； 11、全面支持IPV6，设备自身可以配置IPV6地址供客户端访问，并且支持目标设备配置IPV6地址实现单点登陆和审计； 12、▲支持web页面直接发起运维，无需安装任何控件，支持调用SecureCRT、Xshell、Putty、WinSCP、FileZilla、RDP等客户端工具实现单点登陆，不改变运维人员操作习惯。	

编号：1.8	货物名称：日志审计系统
详细参数：	
1、★自主可控要求：要求芯片及操作系统自主可控； 2、★内存：16GB； 3、★网络接口数：1个管理口、5个千兆电口和4个千兆光口； 4、性能：日志处理性能（平均）3000EPS，配置35个日志源授权； 5、支持审计各种网络设备（路由器、交换机等）配置日志、运行日志、告警日志等； 6、支持审计各种安全设备（防火墙、IDS、IPS、VPN、防病毒网关，网闸，防DDOS攻击，Web应用防火墙等）配置日志、运行日志、告警日志等； 7、▲为了便于资产管理，支持对资产IP地址（含内网IP）的地理信息进行管理，设置单IP及IP段行政区及经纬度，支持地图显示； 8、为了便于管理员审计，支持日志解析字段内置150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； 9、支持通过Syslog、JDBC/ODBC、WMI、(S)FTP、文件共享(SMB、NetBIOS)、文件/目录读取、NetflowV5、Kafka、SNMPTrap、WebService等多种方式完成各种日志的收集功能，支持页面文件导入，支持多行日志采集合并为一行； 10、支持正则表达式、JSON、Key-Value、分隔符4种解析方案，支持日志自动化辅助规范化； 11、对于枚举类型的范化字段，数据字典中的字典表可根据需要自定义扩展； 12、为了便于管理员的维护，支持对日志中的源和目的IP地址进行自动补全，补全IP地址的国家、区域和城市等信息； 13、为了便于管理员审计，用户点击事件任意属性字段，可以该字段为条件对事件进行统计分析，并展示Top20排序，排序支持正序和倒序，并可对统计内容进行点击下钻； 14、▲为了便于管理员维护，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； 15、系统提供可编辑的灵活强大的自定义仪表板；支持仪表板导入导出，支持仪表板共享、复制，可将仪表板共享给其他用户； 16、为了直观地为管理员提供决策和分析的数据基础，帮助管理员掌握网络及业务系统的状况，报表可以保存为html/excel/word/pdf/rtf/png等多种格式，支持丰富的报表管理功能，预定义了针对各类服务器、数通设备、安全设备、数据库、策略变更、流量、设备事件趋势以及总体报表，满足等保等其他合规性要求；根据时间、数据类型等生成报表，提供打印、导出以及邮件送达等服务。	

编号：1.9	货物名称：交换机
详细参数：	
1、★自主可控要求：关键CPU自主可控； 2、★交换容量672Gbps，包转发率126Mpps； 3、★24个千兆电口，4个千兆光口； 4、▲支持MAC地址32K，IPv4 FIB表项4K，支持RIP、RIPng、OSPF、OSPFv3路由协议（提供具有资质的第三方机构出具的检测报告并加盖原厂商公章）； 5、支持IPv6、支持IPv4/IPv6双栈； 6、支持SNMP v1/v2/v3、Telnet、RMON，支持通过命令行、Web、中文图形化配置软件等方式进行配置和管理。	

编号：二	货物名称：互联网
详细参数：	

编号：2.1	货物名称：下一代防火墙（利旧）
详细参数：	
利旧	

编号：2.2	货物名称：防火墙防病毒及入侵防御授权
详细参数：	
防火墙 病毒库、入侵防御攻击库升级服务授权1年	

编号：2.3	货物名称：入侵检测防御系统（利旧）
详细参数：	
利旧	

编号：2.4	货物名称：日志审计系统
详细参数：	
利旧	

编号：2.5	货物名称：安全认证和运维审计系统（利旧）
详细参数：	
利旧	

编号：三	货物名称：其他
详细参数：	

编号：3.1	货物名称：集成
详细参数：	

- 1、网络线路整改、机房线路铺设；
- 2、终端设备安全加固(终端策略整改、防病毒安装、高危漏洞处理)；
- 3、安全产品上架安装、策略配置、系统调试；
- 4、交换机安装、策略配置、系统调试；
- 5、培训文档制作；
- 6、设备、线缆标识标签制作粘贴；
- 7、等级保护测评资料制作；
- 8、配合等级保护测评中心进行等级保护测评。