

报价表

序号	项目名称	数量 ①	品牌、生 产厂家及 国别	型号规格、详细技术参数、 性能配置	单价 (元) ②	单项合价 (元) ③=①× ②	备注
1	运维管理区 与DMZ区域 防火墙	1台	品牌：网神 生产厂家：奇安信网神信息 技术（北京）股份有限公司 国别：中国	NSG4000-TG35M-QW 、2U 1. ★标准 2U 设备，配置 16 个 10/100/1000 Base-T 自适应电口，4 个 SFP 千兆光口，4 个 SFP+ 万兆光口，2 块千兆多模光模块，2 块万兆多模光模块，含 25 个 IPsecVPN 并发隧道数（最大支持 3000）和 25 个 SSLVPN 并发用户数（最大支持 500），另有 2 个接口扩展槽，1 个 Console 口，不少于 1TB 硬盘容量，冗余电源；提供三年硬件质保，三年应用识别库、URL 分	149500	149500	



				<p>类库、病毒特征库、入侵防御特征库升级；</p> <p>2. ★ 防火墙吞吐量 18Gbps，并发连接数 500 万，每秒新建连接数 15 万/秒，含应用控制、URL 过滤、病毒防护、入侵防御等功能模块；</p> <p>3. 产品支持路由、透明、交换以及混合模式接入，满足复杂应用环境的接入需求；</p> <p>4. 支持静态路由、动态路由、策略路由，动态路由包括 RIP v1/v2/ng、OSPF、BGP 等；</p> <p>5. 支持防御 IP 地址欺骗，可将 IP 与安全域关联，即指定 IP 或网段从特定安全域流量流入，否则视为 IP 地址欺骗；</p> <p>6. 支持在 IPv6 环境下配</p>			
--	--	--	--	--	--	--	--

			<p>置安全策略、SSL 解密策略等规则,实现漏洞防护、间谍软件防护、URL 过滤、反病毒、内容过滤、文件过滤、邮件过滤、行为管控及带宽管理;</p> <p>7. 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;</p> <p>8. ★支持上传、下载、双向的文件内容过滤;内容过滤至少支持 html、doc、docx、xls、xlsx、ppt、pptx、chm、7z 等多种常见文件类型,提供相关证明材料(包括但不限于彩页、产品功能界面截图、官网截图证明等);</p>		
--	--	--	---	--	--

			<p>9. 支持冗余策略分析功能，系统可自动检测别列出与某一策略存在冗余关系的其他策略；</p> <p>10. 支持全面的 NAT 转换能力，支持对源目的地址、端口的转换；包括一对一，一对多，多对一，多对多地址转换方式；</p> <p>11. ★支持虚拟防火墙功能，支持在虚系统内进行病毒防护、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，提供相关证明材料（包括但不限于彩页、产品功能界面截图、官网截图证明等）；</p> <p>12. ★支持与云端联动，</p>		
--	--	--	--	--	--

			<p>实现病毒云查杀、URL 云识别、应用云识别、云沙箱等功能，以通过安全云系统提升识别库数量级，补充本地识别库，并加快防火墙对威胁的识别速度,提供相关证明材料(包括但不限于彩页、产品功能界面截图、官网截图证明等);</p> <p>13. 支持面板下的异常、威胁、重点关注监控、接口信息、系统信息、内容日志、威胁日志、URI 过滤日志、邮件过滤日志、并发连接数;</p> <p>14. 支持实现 HTTP、FTP、POP3、SMTP、IMAP、SMB 六种应用协议的双向内容过滤,支持预定义敏感信息库及自定义敏感信息库两种方式进</p>		
--	--	--	--	--	--

			<p>行敏感信息定义，支持阻断及日志两种处理动作；</p> <p>15. ★漏洞防护特征库要求包含高危漏洞攻击特征，至少包括“永恒之蓝”、“震网三代”、“暗云3”、“Struts”、“Struts2”、“Xshell 后门代码”以及对应的攻击的名称、CVEID、CNNVDID、严重性、影响的平台、类型、描述等详细信息，提供相关证明材料（包括但不限于彩页、产品功能界面截图、官网截图证明等）；</p> <p>16. 支持自定义漏洞签名；可标识自定义漏洞的CVE 编号或 CNNVD 编号；支持自定义基于TCP、UDP、HTTP 协议的漏洞，并根据各协议的报文结构，指定一个或多个字段</p>			
--	--	--	---	--	--	--

12-1-1

			<p>的特征值；支持自定义漏洞的源端口范围及目的端口范围；</p> <p>17. ★支持与防病毒系统或终端安全管理系统进行联动，增强防火墙对应用特征及木马特征的识别，实现基于终端健康状态的访问控制，提供相关证明材料(包括但不限于彩页、产品功能界面截图、官网截图证明等)；</p> <p>18. 支持双系统备份，且在系统切换中可实现配置的自动迁移；</p> <p>19. 支持基于受害主机的一键式阻断链接、记录日志等处置动作，处置周期至少包括 1 天、7 天、30 天、90 天、永久等；</p> <p>20. ★支持统计网络中确认失陷的主机及有风险但</p>			
--	--	--	---	--	--	--

			<p>不能完全确认为失陷的主机数量及风险等级状态，支持查看失陷时间、威胁类别、情报来源、威胁简介、失陷主机 IP、用户名、资产等信息，并支持一键跳转处置，提供相关证明材料(包括但不限于彩页、产品功能界面截图、官网截图证明等)；</p> <p>21. 基于源目地址、源目端口、协议、域名、URL 多维度的一键式快速运维处置；</p> <p>22. 日志支持模糊搜索和按精确策略条件搜索，协助定位异常行为，并通过带条件跳转实现指定行为在分析中心中的关联活动展示，确认异常行为是否具有威胁；</p> <p>23. 支持基于网络活动，</p>			
--	--	--	---	--	--	--

				威胁活动、阻止活动等多维关联统计及分析，发现异常行为。			
2	日志审计系统	1台	品牌：网神 生产厂家：奇安信网络安全信息 技术（北京）股份有限公司 国别：中国	LAS-R33M、1U 1. ★标准 1U 机架式设备，配置 ≥ 6 个 10/100/1000M Base-T 自适应电口，另有 2 个接口扩展插槽，1 个 Console 口，不少于 4TB 磁盘存储空间，交流电源；日志采集能力 ≥ 10000EPS，日志综合处理能力 ≥ 5000EPS；配置日志审计节点许可 ≥ 75 个，提供三年质保服务；提供及终端安全管理功能，配置 Windows 客户端授权 ≥ 400 个，Windows 服务器授权 ≥ 40 个，含 3 年软件升级及病毒库升级服务；	248500	248500	

			<p>2. ★界面采用 B/S 模式，无需安装客户端，使用 IE 浏览器访问管理中心，浏览器端无需安装 Java 运行环境；</p> <p>3. 支持对各类网络设备、安全设备、工作站、存储设备、机房设备、其他设备、中间件、数据库、防病毒系统、服务器系统的日志、事件、告警等安全信息进行全面的审计；</p> <p>4. ★支持通过 Syslog、SNMP Trap、Netflow V5、JDBC、WMI、文件\文件夹读取、Kafka 等多种方式完成各种日志的收集功能，提供相关证明材料(包括但不限于彩页、产品功能界面截图、官网截图证明等)；</p> <p>5. 支持对资产日志进行</p>			
--	--	--	--	--	--	--

			<p>过滤，设置允许接收和拒绝接收日志，并可以对资产设置一定时间范围内未收到事件后进行主动告警；</p> <p>6. ★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，提供相关证明材料(包括但不限于彩页、产品功能界面截图、官网截图证明等)；</p> <p>7. 支持对日志进行归一化处理并保留原始日志，方便用户对关键日志快速定位和事后取证；</p> <p>8. ★支持日志范化策略，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，保证最佳范化策略匹配，提</p>		
--	--	--	--	--	--

供相关证明材料（包括但不限于彩页、产品功能界面截图、官网截图证明等）；

9. ★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，提供相关证明材料（包括但不限于彩页、产品功能界面截图、官网截图证明等）；

10. 具备全文检索的大数据处理能力，能够对事件进行非格式化的文本式处理，可将原始信息进行自动索引，快速搜索分析各类安全事件；

11. 支持对事件依据其源目的 IP 和端口等各类字段信息进行深入的事件追踪调查，支持无限次数的

			<p>追踪调查；</p> <p>12. 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，且属性可增加或减少；</p> <p>13. 具备完善的基于规则的关联分析引擎，能够提供逻辑关联、统计关联和递归关联三种关联分析能力；</p> <p>14. 支持单事件关联和多事件关联，能够针对多个不同类型不同来源的安全事件进行综合关联分析；</p> <p>15. 支持柱状图、饼图、折线图、面积图、堆积图、环状图、数值图、地图、3D 地球等形式的统计信息可视化展示，并可将统计结果保存为仪表板和报</p>		
--	--	--	---	--	--

			<p>表等；</p> <p>16. 支持告警管理，告警规则可以自定义，告警可查询；支持告警归并，有效抑制重复告警，归并规则可自定义；</p> <p>17. 支持按周期的方式选择备份，支持原始日志与分析后日志分离，支持历史日志恢复导入；</p> <p>18. 提供丰富的报表管理功能，预定义了针对各类服务器、网络设备、防火墙、入侵检测系统、防病毒系统、终端安全管理系统、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；</p> <p>19. ★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</p>		
--	--	--	---	--	--

			<p>运维报告，提供相关证明材料(包括但不限于彩页、产品功能界面截图、官网截图证明等)；</p> <p>20. 支持基于角色的权限管理机制，通过角色定义支持多用户访问；支持三权分立，包括系统管理员、安全管理员、审计管理员。</p>			
<p>总报价 (人民币大写): <u>叁拾玖万捌仟元整</u> (¥ <u>398000.00</u> 元)</p>						
<p>交货时间: 自签订合同之日起 30 天内安装调试完毕并交付使用。</p>						
<p>交付地点: 梧州市内采购人指定地点。</p>						

报价人: 广西启维科技有限公司

