1、谈判报价表

谈判报价表

采购项目编号：BSZC2020-J1-000224-GXGS_

采购项目名称：机房安全等级升级改造采购

序号	货物名称	数量①	品牌及规格型号、生产厂家及国别	技术参数及性能配置	单价（元）②	单项合价（元）③=①×②
1	防火墙	1 台	深信服、AF-1000-B/1600-Q9、深信服科技股份有限公司、中国	一、▲性能参数： 1、性能指标：网络层吞吐 12 Gbps，应用层吞吐量 1.5 Gbps，并发连结数 200W，新建连接数（CPS）8 W； 包含：防火墙软件基础级；防火墙软件增强级模块（WEB 应用防护及 IPS 入侵防御功能）；开通网关杀毒功能；三年网关杀毒升级许可，三年最新威胁防护规则库更新；提供三年系统软件升级，设备提供三年硬件质保；并且开通传统防火墙、IPS、WEB 防护、网关杀毒功能支持 500M 运营商线路带宽性能。 2、硬件指标：1U 设备，单电源，6 个千兆电口+2 个千兆光口，支持 1 个扩展槽； 二、功能参数： 1、支持 RIPv1/v2，OSPFv2/v3，BGP 等动态路由协议；支持静态路由，ECMP 等价路由；支持多播/组播路由协议； 2、▲支持多链路出站负载，支持基于源/目的 IP、源/目的端口、协议、ISP、应用类型以及国家/地域来进行选路的策略路由选路功能； 3、支持 IPv4 / v6 NAT 地址转换，支持源目的地址转换，目的地址转换和双向地址转换；支持 NAT64、NAT46 地址转换； 4、访问控制规则支持模拟策略匹配，输入源目的 IP、端口、协议五元组信息，模拟策略匹配方式，给出最可能的匹配结果，方便排查故障，或环境部署前的调	102,900.00	102,900.00

				试； 5、能够识别管控的应用类型超过 1200 种，应用识别规则总数超过 3000 条；支持基于应用类型，网站类型，文件类型进行带宽分配和流量控制，支持基于时间、认证用户和 VLAN 进行流量控制； 6、设备具备独立的入侵防护漏洞规则特征库，特征总数在 7000 条以上；支持同防火墙访问控制规则进行联动，可以针对检测到的攻击源 IP 进行联动封锁，支持自定义封锁时间； 7、支持 Land、Smurf、Fraggle、WinNuke、Ping of Death、Tear Drop、IP Spoofing 攻击防护，支持 SYN Flood、IPv4 和 IPv6 ICMP Flood、UDP Flood、DNS Flood、ARP Flood 攻击防护，支持 IP 地址扫描，端口扫描防护，支持 ARP 欺骗防护功能、支持 IP 协议异常报文检测和 TCP 协议异常报文检测； 8、支持对常见应用服务（HTTP、FTP、SSH、SMTP、IMAP、POP3、 RDP、Rlogin、SMB、Telnet）和数据库软件（MySQL、Oracle、MSSQL）的口令暴力破解防护功能； 9、具备对常见网络协议(SSH、FTP、RDP、VNC、Netbios) 和数据库(MySQL、Oracle、MSSQL)的弱密码扫描功能； 10、设备具备独立的威胁库，支持木马、勒索软件、蠕虫、挖矿病毒等种类，特征总数在 50 万条以上；支持恶意域名重定向功能，用于 DNS 代理服务器场景下定位内网感染僵尸网络病毒的真实主机 IP 地址；支持对终端已被种植了远控木马或者病毒等恶意软件进行检测，并且能够对检测到的恶意软件行为进行深入的分析，展示和外部命令控制服务器的交互行为和其他可疑行为； 11、支持业务安全和用户安全的风险展示；支持全网实时热点事		

				件展示；支持在同一个界面对全网所有服务器和主机的安全状况进行风险评估，支持对当前所有业务的安全防护状态进行动态保护； 12、▲支持资产的自动发现以及资产脆弱性和服务器开放端口的自动识别，支持包含敏感数据业务的识别；支持对检测到的攻击行为按照 IP 地址的地理位置信息进行威胁信息动态展示，实时监测和展示最新的攻击威胁信息； 13、支持自动生成安全风险报表，报表内容体现被保护对象的整体安全等级，发现漏洞情况以及遭受到攻击的漏洞统计，具备有效攻击行为次数统计和攻击举证； 14、支持抵御 SQL 注入、XSS 攻击、网页木马、网站扫描、WEBSHELL、跨站请求伪造、系统命令注入、文件包含攻击、目录遍历攻击、信息泄露攻击、WEB 整站系统漏洞等攻击； 15、支持企业安全能力图谱，可展示设备对资产防护的有效性，对当前的风险预测、风险防御、风险检测能力进行展示，并对当前资产安全状态进行评级；同时展示当前设备的安全能力等级，展示每日安全能力的更新情况； 16、可扩展支持接入统一的安全监测平台，通过安全监测平台可以实时看到每台安全设备的详细安全状态信息，包括安全评分级别、最近有效事件、有效事件趋势、用户安全统计、服务器安全统计和攻击来源统计； 17、可提供最新的威胁情报信息，能够对新爆发的流行高危漏洞进行预警和自动检测，发现问题后支持一键生成防护规则； 18、▲支持采用无特征 AI 检测技术对恶意勒索病毒及挖矿病毒等热点病毒进行检测，给出基于 AI 技术的病毒检测报告； 19、支持对企业所有的网站提供保护情况的总览，包括哪些网站		

				当前保护措施不足，哪些网站在有效保护中，当前的漏洞、恶意扫描、web 攻击及篡改事件发生的总体情况，同时风险要可定位到某个网站，并可以对网站面临的威胁给出处理方式；		
2	WEB 应用安全防护系统	1 台	深信服、WAF-1000-DA00-P9、深信服科技股份有限公司、中国	一、▲性能参数： 1、性能指标：网络层吞吐量 4Gbps，应用层吞吐量 600Mbps，http 并发连结数 20W，http 新建连接数（CPS）4000； 2、硬件指标：1U 设备，单电源，10 个千兆电口；3 年硬件质保，3 年软件升级，3 年最新威胁防护规则库更新（包含 Web 应用防护识别库、实时漏洞分析识别库、热门威胁库、应用识别库、URL 分类库更新） 二、功能参数： 1、支持 RIPv1/v2，OSPFv2/v3，BGP 等动态路由协议；支持静态路由，ECMP 等价路由；支持多播/组播路由协议； 2、支持多链路出站负载，支持基于源/目的 IP、源/目的端口、协议、ISP、应用类型以及国家/地域来进行选路的策略路由选路功能； 3、支持 IPv4 / v6 NAT 地址转换，支持源目的地址转换，目的地址转换和双向地址转换；支持 NAT64、NAT46 地址转换； 4、访问控制规则支持模拟策略匹配，输入源目的 IP、端口、协议五元组信息，模拟策略匹配方式，给出最可能的匹配结果，方便排查故障，或环境部署前的调试； 5、能够识别管控的应用类型超过 1200 种，应用识别规则总数超过 3000 条；支持基于应用类型，网站类型，文件类型进行带宽分配和流量控制，支持基于时间、认证用户和 VLAN 进行流量控制； 6、设备具备独立的入侵防护漏洞规则特征库，特征总数在 7000 条以上；支持同防火墙访问控制	93,800.00	93,800.00

				规则进行联动，可以针对检测到的攻击源 IP 进行联动封锁，支持自定义封锁时间； 7、支持 Land、Smurf、Fraggle、WinNuke、Ping of Death、Tear Drop、IP Spoofing 攻击防护，支持 SYN Flood、IPv4 和 IPv6 ICMP Flood、UDP Flood、DNS Flood、ARP Flood 攻击防护，支持 IP 地址扫描，端口扫描防护，支持 ARP 欺骗防护功能、支持 IP 协议异常报文检测和 TCP 协议异常报文检测； 8、支持对常见应用服务（HTTP、FTP、SSH、SMTP、IMAP、POP3、 RDP、Rlogin、SMB、Telnet）和数据库软件（MySQL、Oracle、MSSQL）的口令暴力破解防护功能； 9、具备对常见网络协议(SSH、FTP、RDP、VNC、Netbios) 和数据库(MySQL、Oracle、MSSQL)的弱密码扫描功能； 10、设备具备独立的热门威胁库，支持木马、勒索软件、蠕虫、挖矿病毒等种类，特征总数在 50 万条以上；支持恶意域名重定向功能，用于 DNS 代理服务器场景下定位内网感染僵尸网络病毒的真实主机 IP 地址；支持对终端已被种植了远控木马或者病毒等恶意软件进行检测，并且能够对检测到的恶意软件行为进行深入的分析，展示和外部命令控制服务器的交互行为和其他可疑行为； 11、支持业务安全和用户安全的风险展示；支持全网实时热点事件展示；支持在同一个界面对全网所有服务器和主机的安全状况进行风险评估，支持对当前所有业务的安全防护状态进行动态保护； 12、支持资产的自动发现以及资产脆弱性和服务器开放端口的自动识别，支持包含敏感数据业务的识别；支持对检测到的攻击行为按照 IP 地址的地理位置信息		

				进行威胁信息动态展示，实时监测和展示最新的攻击威胁信息； 13、支持自动生成安全风险报表，报表内容体现被保护对象的整体安全等级，发现漏洞情况以及遭受到攻击的漏洞统计，具备有效攻击行为次数统计和攻击举证； 14、▲支持抵御 SQL 注入、XSS 攻击、网页木马、网站扫描、WEBSHELL、跨站请求伪造、系统命令注入、文件包含攻击、目录遍历攻击、信息泄露攻击、WEB 整站系统漏洞等攻击； 15、支持企业安全能力图谱，可展示设备对资产防护的有效性，对当前的风险预测、风险防御、风险检测能力进行展示，并对当前资产安全状态进行评级；同时展示当前设备的安全能力等级，展示每日安全能力的更新情况； 16、可扩展支持接入统一的安全监测平台，通过安全监测平台可以实时看到每台安全设备的详细安全状态信息，包括安全评分级别、最近有效事件、有效事件趋势、用户安全统计、服务器安全统计和攻击来源统计； 17、可提供最新的威胁情报信息，能够对新爆发的流行高危漏洞进行预警和自动检测，发现问题后支持一键生成防护规则； 18、支持采用无特征 AI 检测技术对恶意勒索病毒及挖矿病毒等热点病毒进行检测，给出基于 AI 技术的病毒检测报告； 19、▲为构建边界安全联动防护体系，建设统一安全管理运营中心，要求所投 WEB 应用安全防护系统、入侵防御系统、防火墙、上网行为管理具备联动效应； 20、▲支持对企业所有的网站提供保护情况的总览，包括哪些网站当前保护措施不足，哪些网站在有效保护中，当前的漏洞、恶意扫描、web 攻击及篡改事件发生的总体情况，同时风险要可定		

				位到某个网站，并可以对网站面临的威胁给出处理方式；		
3	入侵防御系统	1 台	深信服、NIPS-1000-DA00-9Q、深信服科技股份有限公司、中国	一、▲性能参数： 网络层吞吐量 4Gbps，IPS 吞吐量 1.5Gbps，并发连结数 180W，新建连接数（CPS）4W；硬件参数：1U 设备，单电源，10 个千兆电口；包含：网络入侵防御系统软件，3 年最新威胁防护规则库更新，3 年硬件质保及软件升级； 二、功能参数： 1、支持 802.1Q VLAN Trunk、access 接口类型，VLAN 三层接口和子接口；支持链路聚合功能，可将多条物理链路聚合成一条带宽更高的逻辑链路使用；支持端口联动功能，当上行/下行端口链路出现故障时，对应的另一端下行/上行端口自动切断链路； 2、支持采用无特征 AI 检测技术对恶意勒索病毒及挖矿病毒等热点病毒进行检测，给出基于 AI 技术的病毒检测报告； 3、支持 URL 过滤和文件过滤功能，URL 过滤支持 GET，POST 请求过滤和 HTTPS 网站过滤，文件过滤支持文件上传和下载过滤； 4、支持针对 SMTP、POP3、IMAP 邮件协议的内容检测，如邮件附件病毒检测、邮件内容恶意链接检测，邮件异常账号检测等，支持根据邮件附件类型进行文件过滤；支持针对 HTTP、FTP 协议内容检测与病毒查杀； 5、支持对服务器和客户端的漏洞攻击防护，支持 XSS 攻击、SQL 注入等 WEB 攻击行为进行有效防护； 6、▲设备具备独立的入侵防护漏洞规则特征库，特征总数在 7000 条以上；支持同防火墙访问控制规则进行联动，可以针对检测到的攻击源 IP 进行联动封锁，支持自定义封锁时间； 7、支持 Land、Smurf、Fraggle、WinNuke、Ping of	66,900.00	66,900.00

				Death、Tear Drop、IP Spoofing 攻击防护，支持 SYN Flood、IPv4 和 IPv6 ICMP Flood、UDP Flood、DNS Flood、ARP Flood 攻击防护，支持 IP 地址扫描，端口扫描防护，支持 ARP 欺骗防护功能、支持 IP 协议异常报文检测和 TCP 协议异常报文检测； 8、支持对常见应用服务（HTTP、FTP、SSH、SMTP、IMAP、POP3、 RDP、Rlogin、SMB、Telnet）和数据库软件（MySQL、Oracle、MSSQL）的口令暴力破解防护功能； 9、支持连接会话展示，可针对具体的 IP 地址进行会话详情查询，支持封锁异常会话信息，并支持设置监听具体 IP 的会话记录； 10、▲支持根据国家/地区来进行地域访问控制，保障业务访问安全性； 11、支持业务安全和用户安全的风险展示；支持全网实时热点事件展示；支持在同一个界面对全网所有服务器和主机的安全状况进行风险评估，支持对当前所有业务的安全防护状态进行动态保护； 12、支持关键文件保护功能，能够过滤文件的上传和下载行为，以防止非法外传和下载行为。能识别的文件类型应包含至少以下几类：音频视频类文件、图片类文件、文本类文件、压缩文件、应用程序类文件等； 13、支持自动生成安全风险报表，报表内容体现被保护对象的整体安全等级，发现漏洞情况以及遭受到攻击的漏洞统计，具备有效攻击行为次数统计和攻击举证； 14、▲支持蜜罐功能，即恶意域名重定向至蜜罐 IP 地址，监听对蜜罐地址的访问，用于 DNS 代理服务器场景下定位内网感染僵尸网络病毒的真实主机 IP 地址；		

				15、支持在同一个界面对全网所有服务器的安全状况进行风险评估，支持对当前所有业务的安全防护状态进行动态保护，支持对所有已被入侵和受控的设备进行风险监测与分析，针对风险生成待办事件，从而实现快速响应与处置；支持手动评估功能，自动展示最终的风险； 16、可扩展支持接入统一的安全监测平台，通过安全监测平台可以实时看到每台安全设备的详细安全状态信息，包括安全评分级别、最近有效事件、有效事件趋势、用户安全统计、服务器安全统计和攻击来源统计； 17、▲可提供最新的威胁情报信息，能够对新爆发的流行高危漏洞进行预警和自动检测，发现问题后支持一键生成防护规则； 18、▲支持与同全网安全态势感知平台实现联动，产品支持以标准 syslog 形式上传到全网态势感知平台，供全网安全态势感知系统进行深度关联分析并对恶意威胁实现联动封锁；		
4	服务器防火墙（病毒过滤网关）	2 台	深信服、AF-1000-B1800-Q9、深信服科技股份有限公司、中国	一、▲性能参数： 1、性能指标：网络层吞吐量 18 Gbps，应用层吞吐量 2.5 Gbps，并发连结数 200W，新建连接数（CPS）12W；　包含：防火墙软件基础级；防火墙软件增强级模块（WEB 应用防护及 IPS 入侵防御功能）；提供三年系统软件升级，设备提供三年硬件质保；并且开通传统防火墙、IPS、WEB 防护功能支持 700M 运营商线路带宽性能。 2、硬件指标：1U 设备，单电源，6 个千兆电口+2 个万兆光口，支持 2 个扩展槽；支持 802.1Q VLAN Trunk、access 接口，VLAN 三层接口，子接口；支持链路聚合功能，可将多条物理链路聚合成一条带宽更高的逻辑链路使用；支持端口联动功能，当上行/下行端口链路出现故障时，对应的另一端下行/上行端	124,000.00	248,000.00

				口自动切断链路； 二、功能参数： 1、支持 RIPv1/v2，OSPFv2/v3，BGP 等动态路由协议；支持静态路由，ECMP 等价路由；支持多播/组播路由协议； 2、▲支持多链路出站负载，支持基于源/目的 IP、源/目的端口、协议、ISP、应用类型以及国家/地域来进行选路的策略路由选路功能； 3、支持 IPv4 / v6 NAT 地址转换，支持源目的地址转换，目的地址转换和双向地址转换；支持 NAT64、NAT46 地址转换； 4、访问控制规则支持模拟策略匹配，输入源目的 IP、端口、协议五元组信息，模拟策略匹配方式，给出最可能的匹配结果，方便排查故障，或环境部署前的调试； 5、能够识别管控的应用类型超过 1200 种，应用识别规则总数超过 3000 条；支持基于应用类型，网站类型，文件类型进行带宽分配和流量控制，支持基于时间、认证用户和 VLAN 进行流量控制； 6、设备具备独立的入侵防护漏洞规则特征库，特征总数在 7000 条以上；支持同防火墙访问控制规则进行联动，可以针对检测到的攻击源 IP 进行联动封锁，支持自定义封锁时间； 7、支持 Land、Smurf、Fraggle、WinNuke、Ping of Death、Tear Drop、IP Spoofing 攻击防护，支持 SYN Flood、IPv4 和 IPv6 ICMP Flood、UDP Flood、DNS Flood、ARP Flood 攻击防护，支持 IP 地址扫描，端口扫描防护，支持 ARP 欺骗防护功能、支持 IP 协议异常报文检测和 TCP 协议异常报文检测； 8、支持对常见应用服务（HTTP、FTP、SSH、SMTP、IMAP、POP3、 RDP、Rlogin、SMB、Telnet）和数据库软件		

				（MySQL、Oracle、MSSQL）的口令暴力破解防护功能； 9、具备对常见网络协议(SSH、FTP、RDP、VNC、Netbios）和数据库(MySQL、Oracle、MSSQL)的弱密码扫描功能； 10、▲设备具备独立的威胁库，支持木马、勒索软件、蠕虫、挖矿病毒等种类，特征总数在50万条以上；支持恶意域名重定向功能，用于DNS代理服务器场景下定位内网感染僵尸网络病毒的真实主机IP地址；支持对终端已被种植了远控木马或者病毒等恶意软件进行检测，并且能够对检测到的恶意软件行为进行深入的分析，展示和外部命令控制服务器的交互行为和其他可疑行为； 11、支持业务安全和用户安全的风险展示；支持全网实时热点事件展示；支持在同一个界面对全网所有服务器和主机的安全状况进行风险评估，支持对当前所有业务的安全防护状态进行动态保护； 12、支持资产的自动发现以及资产脆弱性和服务器开放端口的自动识别，支持包含敏感数据业务的识别；支持对检测到的攻击行为按照IP地址的地理位置信息进行威胁信息动态展示，实时监测和展示最新的攻击威胁信息； 13、支持自动生成安全风险报表，报表内容体现被保护对象的整体安全等级，发现漏洞情况以及遭受到攻击的漏洞统计，具备有效攻击行为次数统计和攻击举证； 14、支持抵御SQL注入、XSS攻击、网页木马、网站扫描、WEBSHELL、跨站请求伪造、系统命令注入、文件包含攻击、目录遍历攻击、信息泄露攻击、WEB整站系统漏洞等攻击； 15、支持企业安全能力图谱，可展示设备对资产防护的有效性，对当前的风险预测、风险防御、风险检测能力进行展示，并对当		

				前资产安全状态进行评级；同时展示当前设备的安全能力等级，展示每日安全能力的更新情况； 16、可扩展支持接入统一的安全监测平台，通过安全监测平台可以实时看到每台安全设备的详细安全状态信息，包括安全评分级别、最近有效事件、有效事件趋势、用户安全统计、服务器安全统计和攻击来源统计； 17、可提供最新的威胁情报信息，能够对新爆发的流行高危漏洞进行预警和自动检测，发现问题后支持一键生成防护规则； 18、支持采用无特征 AI 检测技术对恶意勒索病毒及挖矿病毒等热点病毒进行检测，给出基于 AI 技术的病毒检测报告； 19、支持对企业所有的网站提供保护情况的总览，包括哪些网站当前保护措施不足，哪些网站在有效保护中，当前的漏洞、恶意扫描、web 攻击及篡改事件发生的总体情况，同时风险要可定位到某个网站，并可以对网站面临的威胁给出处理方式；		
5	上网行为管理	1 台	深信服、AC-1000-B1400-PM、深信服科技股份有限公司、中国	一、▲性能参数： 1、性能指标：网络吞吐量 1.2Gb、支持带宽 400Mb、支持用户数 2500、每秒新建数 8000、最大并发数 400000； 2、硬件指标：1U 规格；单电源，4 个千兆电口，4 个千兆光口，1 个串口(RJ45)，2 个 USB2.0，4G 内存，SATA 硬盘 1TB;包含：3 年软件升级硬件质保，3 年规则库升级 二、功能参数： 1、支持网关模式、网桥模式、旁路模式、多路桥接模式，以及两台及两台以上设备同时做主机的部署模式； 2、支持绑定 IP 认证、绑定 MAC 认证，及 IP/MAC 绑定认证等；支持当用户 MAC 地址变动时，需要重新认证； 3、▲支持 P2P 智能流控，通过抑制 P2P 的上行流量，来减缓	102,000.00	102,000.00

				P2P 的下行流量，从而解决网络出口在做流控后仍然压力较大的问题； 4、支持基于时间段的带宽划分与分配策略；支持对单个用户/用户组设置日流量、月流量配额功能； 5、支持二维码认证，管理员扫描访客的二维码后对其网络访问授权； 6、支持网页内容审计后的网页快照功能； 7、支持根据外发文件类型、关键字等条件的过滤告警，支持对 HTTP、FTP、Email 附件方式外发文件的识别、报警、过滤等管理措施； 8、▲支持 Web 访问质量检测，针对内网用户的 web 访问质量进行检测，对整体网络提供清晰的整体网络质量评级；支持以列表形式展示访问质量差的用户名单； 9、支持基于通道流速、通道总用户数、通道活跃用户数等维度的流速趋势分析报表；支持基于时间/用户/用户组/上行/下行/总体等维度的域名流量、域名访问排行； 10、支持给应用识别规则库里的每一种应用列上图标，至少能识别 2700 种主流应用，且能将识别的应用智能分类，标签分类至少包含安全风险、高带宽消耗、发送电子邮件、降低工作效率、外发文件泄密风险、主流论坛和微博发帖 6 大类；易于管理员了解应用的特征和进行策略配置； 11、支持开启直通后，流量控制模块依然生效，避免全部数据直通导致线路流量过大； 12、支持以“剩余带宽”“带宽比例”“平均分配”“优先前面的线路”四种负载策略；支持线路故障检测； 13、支持检测 windows 重要补丁的安装情况，并反馈检测结果； 14、支持在设置流量策略后，根据整体线路或者某流量通道内的		

				空闲情况，自动启用和停止使用流量控制策略，以提升带宽的高使用率； 15、支持审计用户在 SSL 加密网页、论坛、BBS 上的发帖内容； 16、支持将非法热点接入网络的行为通过邮件告警通知管理员，并在数据中心支持行为记录和查询； 17、▲支持基于“流量”、“流速”、“时长”设置配额，当配额耗尽后，将用户加入到指定的流控黑名单惩罚通道中； 18、▲针对单用户的行为分析（包括：应用流速趋势、应用流量排行、域名流量排行、应用时长排行、域名时长排行、行为汇总排行等）；		
6	网络审计	1 台	深信服、DAS-1000-A620-PM、深信服科技股份有限公司、中国	一、▲性能参数： 1、性能指标：吞吐量≥2Gbps，数据库流量比≥500Mb/s，SQL 吞吐（峰值）≥30000 条 SQL 语句/s，日志检索≥100000 条/秒，含 100 个主机审计许可证书（可扩展到 150 个主机审计许可），处理性能 3000 条/秒；支持获取各种主流网络及数据库访问行为，支持 Syslog、WMI、SNMP trap、文本、JDBC/ODBC 和 LAS-1000 专用协议等协议事件日志，支持通过日志导入、SFTP、SMB 等协议获取各类文件型日志，支持会话数据解码和分析，支持普通以太头解析、支持 PPPoE、VLAN、VLAN QinQ、支持 TCP、UDP、ICMP、ICMPv6、SCTP、IGMP 等，支持 HTTP、DNS、邮件等； 2、硬件指标：1U 规格；硬盘≥2TB；单电源；标配≥6 个千兆电口，2 个千兆光口；含三年硬件质保软件升级及规则库升级； 二、功能参数： 1. ▲支持 Oracle 数据库审计、SQL-Server 数据库审计、DB2 数据库审计、MySQL 数据库审计，东华 Cache 数据库，支持同时审计多种数据库及跨多种数据库平	76,300.00	76,300.00

				台操作； 2. ▲支持客户端程序、数据库用户、操作类型、数据库名表名、响应时间、返回行数等实现对敏感数据库操作的精细监控； 3.支持 HTTP 请求审计，可指定 GET、POST、URL、响应码进行精细审计。 4.支持时间段、源 IP、客户端程序、业务系统、数据库用户、数据库名、操作类型、表名、返回行数、影响行数、响应时长、响应码等对数据库日志进行精细检索。 5.内置大量 SQL 以及 M 语言规则，包括如下：导出方式窃取、备份方式窃取、导出可执行程序、备份方式写入恶意代码、系统命令执行、读注册表、写注册表、暴露系统信息、高权存储过程、执行本地代码、常见运维工具使用 grant、业务系统使用 grant、客户端 sp_addrolemember 提权等； 6.支持自定义数据库安全策略，可根据业务需要自定义各种场景的安全规则，对于违规的数据库访问可进行实时警告和阻断。 7.可以对 SQL 语句以及 M 语言进行安全检测，并识别当前的 SQL 操作是否有暴库、撞库等严重性安全问题，如果命中了安全风险规则，那么可根据动作进行阻断、告警、记录等操作，可提示管理员作出相应的防御措施。 8.支持执行 SQL 语句失败分析，包括登录失败排行，SQL 语句失败排行。 9.支持吞吐量分析，包括 SQL 语句吞吐量排行、SQL 语句吞吐量趋势、SQL 操作类型吞吐量排行、SQL 操作类型吞吐量趋势、数据库用户吞吐量排行、数据库用户吞吐量趋势、业务主机吞吐量排行、业务主机吞吐量趋势。 10.支持指定源 IP、时间日期、客户端程序、业务系统、数据库用户、操作类型等精细日志查询。		

				11.支持同时审计多种数据库及跨多种数据库平台操作；可以对SQL语句进行安全检测，并识别当前的SQL操作是否有暴库、撞库等严重性安全问题，如果命中了安全风险规则，那么可根据动作进行阻断、告警、记录等操作，可提示管理员作出相应的防御措施。		
7	日志审计	2套	深信服、LAS-1000-A600-P9、深信服科技股份有限公司、中国	一、▲性能参数： 1、性能指标：含100个以上主机审计许可证书，处理性能3000条/秒；支持获取各种主流网络及数据库访问行为，支持Syslog、WMI、SNMP trap、文本、JDBC/ODBC和LAS-1000专用协议等协议事件日志，支持通过日志导入、SFTP、SMB等协议获取各类文件型日志，支持会话数据解码和分析，支持普通以太头解析、支持PPPoE、VLAN、VLAN QinQ、支持TCP、UDP、ICMP、ICMPv6、SCTP、IGMP等，支持HTTP、DNS、邮件等； 2、硬件指标：2U规格；单电源；标配≥6个千兆电口；包含三年硬件质保软件升级及规则库升级； 二、功能参数： 1、要求为一个完整的软硬件一体化产品；无需用户另行提供服务器、操作系统、数据库、防火墙软件、及用户手动升级系统补丁； 2、提供旁路接入模式，设备部署不影响原有网络结构； 3. 支持通过页面直接将日志文件导入或以syslog方式接收日志信息，支持日志类型：UNIX、WINDOWS事件[2000、2003、2008、XP、VISTA、Win7及以上版本]、网络及安全设备[Cisco、Array、Juniper、H3C、神州数码、绿盟、天融信、安氏领信、网神]、AS400日志、数据库访问[Mysql]、WEB访问[Apache、IIS、Tomcat、Nginx、Weblogic、Resin、	71,000.00	142,000.00

				Websphere]、文件访问[VSftpd、Pureftpd、NCftpd、IISftpd、Proftpd、Glftpd、Serv-u]、数据库服务[Oracle、Mssql、Mysql、DB2、Informix、Sybase]、WEB 服务[Apache、Tomcat、Nginx、Weblogic、Resin、Websphere]； 4、支持 SNMP 日志采集，支持日志类型：网络及安全设备[深信服、Cisco、Array、Juniper、H3C、神州数码、绿盟、天融信、安氏领信、网神] 5、 支持镜像数据采集，支持类型：数据库模块[Oracle、Mssql、Mysql、DB2、Informix、Sybase、DM]、文件传输模块[FTP、SMB、HTTP]、邮件模块[SMTP、POP、HTTP]、即时通讯模块[淘宝旺旺、MSN、QQ]、远程控制模块[Telnet]、网站访问模块[网页浏览]； 6、▲支持文本型日志文件定时采集，可自动将日志文件采集到系统中分析存储； 7、支持以图表方式（饼图、柱图、曲线图）显示当日日志数据分布情况；支持自定义配置实时监控的日志类型； 8、支持对所添加的资产进行实时监控，并能以不同图标显示发生的事件及告警； 9、支持以图表方式（饼图、柱图、曲线图、清单列表）显示当日安全事件及告警日志数据分布情况； 10、支持管理员自定义审计报表模板；支持多种方式的查询检索，包括：日志检索、事件检索、告警检索、高级检索及文件检索； 11、支持按日志文件的名称、内容进行检索，并提供页面下载原始日志文件；支持查询模版创建、修改、删除功能； 12、支持内置归并策略，对 HTTP 数据进行自动归并处理； 13、支持内置关联分析策略，可		

				设定用户在规定时间内连续多次输入错误口令产生告警或事件； 14、▲支持数据策略，可设定采集多种 WEB 访问数据，包括：脚本访问、样式访问、图片访问及地理数据访问； 15、 规则条件设定支持逻辑运算符与支持正则表达式； 16、 支持自定义三层业务策略：支持通过该策略配置，识别数据库三层架构中用户信息；		
8	漏洞扫描	2 台	深信服、BVT-1000-A620-PM、深信服科技股份有限公司、中国	一、▲性能参数： 1、性能指标：包含 100 台以上设备资产安全配置检查和变更检查授权，漏扫和 WEB 漏扫功能授权数量无限制；含安全配置核查、漏洞扫描、配置变更检查、WEB 漏洞扫描、弱口令检测五大引擎。功能包括：任务管理、检测报告、结果对比，告警分析、综合报表、综合仪表板等。 2、硬件指标：1U 设备，6 电 2 光（可定制扩展），单电源 250W（可定制冗余电源）。包含：基线核查系统软件，3 年软件升级硬件质保，规则库升级。 二、功能参数： 1、通过 SSL 加密对数据传输等进行处理，HTTPS 方式，采用 B/S 架构操作，支持 IPV6。 2、基线检查和变更检查支持远程检查，SSH、TELENT、SMB、离线检查，支持跳转机跳转，口令批量录入。 3、支持支持一次性任务、立即任务、周期任务等多种调度方式； 4、 ▲支持漏洞扫描、安全基线检查、变更检查的三合一任务，三者也可任意组合执行任务； 5、基线检查支持系统类型包括主机类：windows、Unix、solaris、HP-Unix、AIX、Linux 等；网络设备：华为、H3C、Cisco、Juniper、中兴等；防火墙：华为、天融信、H3C、Fortigate、Cisco、Juniper、迪普防火墙等；数据	57,900.00	115,800.00

				库：Mysql、DB2、Oracle、Sqlserver、Sybase 等；中间件：Tomcat、IIS、Webservices、Apache、Weblogic、Resin、Nginx 等； 6、在安全基线违规列表中，选择某个违规信息，可进一步查看该违规的详细信息和解决方案。 7、变更检查支持检查重要文件、文件夹、注册表、启动项、进程等详细信息以及变更状态。 8、 支持根据实际情况设置任意检查结果作为变更基线，后续变更任务将以当前基线作为变更与否的比较标准，支持与自身或其他设备的同类型变更项进行比对，检查设备间核心配置项的异同之处； 9、 能够识别出运行的服务和端口，内置漏洞库 46000 条。支持 CVE 等编号，拥有完备的知识体系。 10、能够扫描主流虚拟机管理系统的安全漏洞，如：VMWare ESXi。 11、 支持 WEB 应用弱点检测，支持主流安全漏洞扫描，如：SQL 注入、跨站脚本攻击、网页木马、系统命令执行漏洞、信息泄露、资源位置预测漏洞、目录遍历漏洞、配置不当漏洞、弱密码、内容欺骗漏洞、外链、暗链、等类型漏洞；支持 WEB1.0，WEB2.0 扫描；支持对网站资产管理，快捷网站扫描 12、任务报告展示：支持四合一多维度展示任务详情，并支持导出 Word、PDF、HTML 等多种报表。 13、 ▲历次任务比对：支持对周期任务的多次执行任务结果进行比对，比对结果中详细展示报告间的异同之处； 14、以列表的方式展示告警，支持告警策略自定义，告警声音设置，告警过滤策略。 15、 ▲支持告警复核（针对已确认的告警进行系统自动检查，通过系统执行相关任务精确确认		

				告警是否已经清除）； 16、支持三权分立方式的授权，即管理员只负责完成设备的系统配置，安全管理员配置核查，审计员负责对系统本身的用户操作日志管理和审计。		
9	数据网闸	1 台	深信服、GAP-1000-A600-PM、深信服科技股份有限公司、中国	一、▲性能参数： 1、性能指标：吞吐量 500Mbps，最大并发连接数 5 万。标配提供文件交换、数据库访问和同步、视频交换、组播代理、访问交换等功能模块，“双主机+隔离卡”架构，单主机硬件信息： 2、硬件指标：2U 规格；6 个电口，冗余电源 100W。包含：安全隔离与信息交换系统软件，3 年软件升级硬件质保，3 年规则库升级。 二、功能参数： 1、采用 2+1 系统架构即内网单元+外网单元+FPGA 专用隔离硬件。不能采用网线等形式直通，采用基于 linux 内核的多核多线程专用安全操作系统，加固内核； 2、▲设备支持透明、代理及路由三种工作模式，管理员可依据实际网络状况进行相应的部署。 3、▲支持的数据库种类包括 ORACLE、SQLSERVER、MYSQL、SYBASE 等主流数据库支持多种关系型数据库通信。支持 SQL 语句的白名单； 4、▲系统支持数据库同步应用，支持 ORACLE、SQLSERVER、MYSQL、SYBASE、DB2、POSTGRESQL 等多种主流国外数据库的同步和国产达梦数据库、人大金仓数据库的同步； 5、支持 TCP 应用层数据单向传输的控制，保证 TCP 应用数据的 0 反馈，以满足二次防护对数据传输的安全性需求； 6、支持 DCS/SCADA 生产网络与办公网络之间的 OPC 应用数据的传输。支持同步、异步监测数据的传输，只需绑定固定的一个起始端口即可满足动态端口的数据	57,000.00	57,000.00

				传输； 7、支持根据时间自动切换的安全策略。支持时间段以 24 小时制，支持以星期为周期，支持指定时间点一次性运行； 8、系统提供 ping ，traceroute ，TCP 端口探测、抓包等工具方便管理员在配置策略或调整网络时排查问题； 9、产品内置各类应用支持模块，无须用户增加投资，功能模块至少包含：邮件模块、安全浏览模块、视频交换模块、数据库访问模块、数据库同步模块、文件交换模块、OPC 模块、MODBUS 模块、WINCC 模块、组播代理模块、用户自定义应用模块等各类应用模块,并可控制相应应用协议的的动作、参数、内容。		
10	48 口千兆三层交换机	4 台	信锐网科、RS5300-48T-4F、深圳市信锐网科技术有限公司 、中国	1、 ▲ 48 个千兆电口，4 个 SPF+万兆光口，包含 4 个 SFP 千兆多模光模块； **2、工作温度：0° C～50° C，存储温度：-40° C～70° C；** 3、交换性能：336Gbps/3.36Tbps，包转发率：132Mpps/166Mpps； 4、支持胖瘦一体化，支持智能交换机和普通交换机两种工作模式，可以根据不同的组网需要，随时进行切换； **5、▲可通过配置静态 IP 地址，DHCP Option43 方式，DNS 域名，二层广播方式发现控制器平台；** 6、支持通过控制器平台一键替换“按钮”即可完成故障设备替换； 7、支持 STP、RSTP、MSTP 协议，支持 IGMP v1/v2/v3 Snooping； 8、支持 IEEE 802.3az 标准的 EEE 节能技术； 9、支持 32K MAC 地址，支持 MAC 地址自动学习； 10、 支持 M-LAG 技术，跨设备链路聚合，配对的设备有独立的控制平面；	14,500.00	58,000.00

				11、 支持通过控制器平台查看交换机端口负载情况； 12、支持防网关 ARP 欺骗，管理员分级管理，支持防止 DOS、ARP 攻击功能； 13、支持通过 APP 进行远程管理，并且可以修改交换机网络配置； 14、支持通过在控制器平台的 Web 页面对交换机进行可视化管理查看，包括交换机的端口状态及配置、vlan 信息； 15、▲支持通过控制器平台图形化操作对交换机端口状态的开启与关闭； 16、 支持安全状态页面中统计显示联动事件次数及详情； 17、支持终端的 MAC 与交换机端口变更检测； 18、支持交换机端口终端类型变更后，通过 APP、短信告警； 19、支持通过控制器平台查看交换机面板端口工作状态，通过端口颜色显示状态即可判断端口是否在线工作；		
11	双机热备软件	1 套	应用交付软件、中国	具有单点故障容错能力的系统平台，采用主服务发生故障时备服务器接管的机制，实现在线故障自动切换，达到了系统 7×24 小时不间断运行，避免因系统停机造成的损失。	11,000.00	11,000.00
12	全网态势感知	1 台	深信服、SIP-1000-E600-PM、深信服科技股份有限公司、中国	一、▲性能参数： 1、设备采用外观≥1U 的机架式服务器，配置 16TB 企业级硬盘、1 块 128G SSD 系统盘，标配≥6 个千兆电口，配置单电源，包含一套潜伏威胁探针系统；包含：3 年软件升级硬件质保，3 年规则库升级； 二、功能参数： 1、支持自动识别网络内部主机网段和外网网段；支持通过流量中的应用内容自动区分网络内部网段 IP 是属于 PC 还是服务器； 2、▲支持基于流量实时漏洞功能，漏洞分析类型包含配置错误漏洞、OpenSSH 漏洞、目录遍历	318,000.00	318,000.00

				漏洞、OpenLDAP 等操作系统、数据库、Web 应用等，页面上支持展示业务脆弱性风险分布、漏洞类型分析、漏洞态势与危害和处置建议，并支持导出脆弱性感知报告； 3、支持自动识别已知服务器，通过被动检测机制，对经过探针的流量进行分析，识别已知服务器对外提供的所有服务、已开放端口及端口传输的协议/应用等； 4、支持通过镜像流量检测 web 流量中是否存在可截获的口令信息，分析 web 业务系统是否存在明文传输情况，避免因明文传输导致信息泄露的风险； 5、支持流量分析实时发现操作系统、数据库、web 应用等存在的漏洞风险，看清网络脆弱性，并支持生成漏洞检测报告。具备僵尸网络识别能力，行为规则近 40 万条； 6、支持通过云端沙盒对全球威胁情报源进行验证，提取有效信息形成规则定期更新到僵尸网络识别库，增量提升检测能力；支持 DNSFlow 分析引擎，利用机器学习算法结合威胁情报，能够从大量的样本中进行学习，总结其伪装的规律，从而发现伪装的恶意 DNS 协议； 7、▲具备安全日志分析引擎、DnsFlow 行为分析引擎、HttpFLow 分析引擎、NetFLow 分析引擎、MailFLow 分析引擎、SmbFLow 分析引擎、威胁情报分析关联引擎、第三方安全检测引擎、文件威胁检测引擎等； 8、支持检测业务的异常行为，从而识别业务是否已失陷被控制，并设立失陷等级和威胁等级展示当前业务的状态和产生的威胁程度；支持检测网络内部用户的异常行为，要求能够基于僵尸网络识别库，检测用户是否存在风险； 9、▲支持检测主机与 C&C 服务器通信行为，支持区分国内外区		

				域；支持检测从未知站点下载可执行文件、访问恶意链接、使用IRC协议进行通信、浏览最近30天注册域名、下载文件格式与实际文件不符、基于行为检测的木马远控、比特币挖矿等可疑访问行为，支持区分国内外区域和显示可疑行为访问趋势； 10、支持检测违规访问策略黑名单或违反了白名单，或者违反了下一代防火墙中的应用控制策略的行为；支持检测服务器对外发起的远程登录、远程桌面、数据库等风险应用访问；支持检测主机对外发起的攻击行为； 11、支持对服务器、客户端的各种应用发起的漏洞攻击进行检测，包括20种攻击类型共9000+以上规则； 12、支持以图形化大屏的服务器与漏洞实时态势，包括但不限于漏洞等级分布、TOP5漏洞、服务器操作系统分布、影响服务器的数量、被访问服务器TOP5、实时漏洞发现更新、业务对外开放TOP5端口； 13、▲支持接入防火墙、上网行为管理、终端EDR、WAC无线控制器、DAS数据库审计和潜伏威胁探针等设备,并支持在页面中显示安全组件接入的数量和状态； 14、支持提供PDF格式报表形式的摘要报告，包含总体摘要、安全感知详情、UEBA行为画像、安全规划建设建议等，从整体展示安全状况，快速了解业务和网络的安全风险支持对业务的外连行为进行监测，以可视化的方式展示业务外连的地域分布、是否存在风险、外连趋势等； 15、▲支持基于用户/业务维度的访问关系梳理，可呈现该用户/业务已经通过哪些应用、协议和端口访问了哪些业务，这些访问是否是攻击、违规、远程登陆等行为，IT人员可清晰的看出已对哪些业务存在影响，也能推导当前用户是否已失陷（或可		

				疑）； 16、支持检索接入设备传输过来的所有安全日志，可基于时间、攻击类型、严重等级等选择项进行组合查询，可基于具体设备、来源/目的所属、IP 地址、特征 ID、URL 进行具体条件搜索； 17、支持以邮件的形式及时将发现的失陷业务、失陷用户、攻击成功事件等安全事件进行告警，支持根据安全事件类型配置发送间隔和触发条件； 18、支持管控接入探针的统一升级，可展示当前所有接入探针的规则库日期、是否过期等，并支持禁用指定探针的升级； 19、▲为了保证设备间的功能联动性，需支持与本项目上网行为管理、防火墙设备进行联动响应，同步上网行为管理设备认证用户，实现与安全事件关联。		
13	设备软件升级	1 项	软件升级服务、中国	原有设备软件升级： 1、防火墙墙设备增加网关杀毒功能，并且开通三年病毒库更新，三年设备软件升级、3 年 URL 规则库升级。 2、VPN 设备型号为 VPN-2050-YX，3 年软件升级服务、3 年规则科升级服务 3、应用交付设备型号为 AD-2200-KY，3 年软件升级服务、3 年规则科升级服务	27,900.00	27,900.00
14	云盾（政府网站综合防护系统）	1 套	深信服、云盾、深信服科技股份有限公司、中国	1、实时带宽：10Mb/s、防护域名数量：1 个、为用户网站提供云端的 Web 应用安全防护、网页篡改监测与自动化处置、入侵防御、CC 攻击防护、独享防护、防绕过、失陷监测、安全可视化、动态防护、定向防护、实时对抗、应急对抗；3 年服务质保及升级服务； 2、支持页面响应监测，通过固定的频率模拟用户请求访问被监控站点，实时获取站点的响应状态和请求详情，精准的探测出网站的各种异常 5 分钟检测一次，当连续 3 次访问失败时判断为业	51,500.00	51,500.00

				务不可用； 3、支持页面响应监测，通过固定的频率模拟用户请求访问被监控站点，实时获取站点的响应状态和请求详情，精准的探测出网站的各种异常 5 分钟检测一次，当连续 3 次访问失败时判断为业务不可用； 4、支持对目标站点提供 7×24 小时网页黑链监测能力。发现网页黑链事件第一时间通过微信通知用户，监测内容能够在报告中进行呈现； 5、▲支持安全替身及永久在线，即当网站因为服务器故障、线路故障、电源等问题出现无法连接时，可自动替换为云防护节点中的缓存页面，所有访问均为缓存页面。支持一键开启、一键关闭； 6、▲支持严格策略和宽松策略可选择配置。严格策略：当任何页面发生篡改时，如反共黑客、赌博、色情、黑链等内容，将自动使用缓存页面；宽松策略：只有首页发生篡改时，如反共黑客、赌博、色情等内容，将自动使用缓存页面；其他子页面发生篡改将会被隔离，无法访问该页面； 7、▲当网站出现紧急安全事件时，可在一分钟内通过展示界面一键完成关停，防止产生恶劣影响； 8、▲通过信通院 IPv6 支持度检测，达到运营及网络地址翻译（NAT）技术要求 NAT64； 9、支持对特定 URL 的 ip 请求频率进行自定义限速设置，防止 cc 攻击、秒杀防刷； 10、支持对常见 http 应用服务的口令暴力破解防护功能；针对 web 服务漏洞攻击的防护，比如 IIS, apache 等服务器各种漏洞防护;具备 http 应用服务的弱密码扫描功能； 支持同访问控制规则进行联动，可以针对检测到的攻击源 IP 进行联动封锁； 11、支持敏感信息泄露检查，对		

				上传和下载文件进行检查，如发现直接下载文件对客户进行预警，可自定义文件类型，如rar，zip，execl，word 等； 12、支持出云随机 IP，保证业务的稳定性，提升系统并发量； 13、▲支持以微信公众号的方式对篡改、黑链、网站不可用等安全事件进行实时告警，支持微信端内容的及时推送； 14、支持 Web 漏洞扫描功能，可扫描检测网站是否存在 SQL 注入、XSS、跨站脚本、目录遍历、文件包含、命令执行等脚本漏洞； 15、支持提供风险处置、攻击详情以及漏洞详情操作界面，实时查看风险状态，以便及时调整安全策略。		
15	全网行为管理	1 台	深信服、AC-1000-B1190-Q9、深信服科技股份有限公司、中国	一、▲性能参数： 1、性能指标：网络吞吐量 500Mb、支持管理用户数 800、每秒新建数 2400、最大并发数 120000； 2、硬件指标：1U 规格；单电源，4 个千兆电口，1 个串口（RJ45），2 个 USB2.0，4G 内存，SATA 硬盘 1TB;包含：3 年软件升级硬件质保，3 年安全规则库升级。 二、功能参数： 1、支持网关模式、网桥模式、旁路模式、多路桥接模式，以及两台及两台以上设备同时做主机的部署模式； 2、支持绑定 IP 认证、绑定 MAC 认证，及 IP/MAC 绑定认证等；支持当用户 MAC 地址变动时，需要重新认证； 3、▲支持 P2P 智能流控，通过抑制 P2P 的上行流量，来减缓 P2P 的下行流量，从而解决网络出口在做流控后仍然压力较大的问题； 4、支持基于时间段的带宽划分与分配策略；支持对单个用户/用户组设置日流量、月流量配额功能；	53,900.00	53,900.00

				5、▲支持二维码认证，管理员扫描访客的二维码后对其网络访问授权； 6、▲支持 Web 访问质量检测，针对内网用户的 web 访问质量进行检测，对整体网络提供清晰的整体网络质量评级；支持以列表形式展示访问质量差的用户名单； 7、支持基于通道流速、通道总用户数、通道活跃用户数等维度的流速趋势分析报表；支持基于时间/用户/用户组/上行/下行/总体等维度的域名流量、域名访问排行； 8、▲支持给应用识别规则库里的每一种应用列上图标，至少能识别 2700 种主流应用，且能将识别的应用智能分类，标签分类至少包含安全风险、高带宽消耗、发送电子邮件、降低工作效率、外发文件泄密风险、主流论坛和微博发帖 6 大类；易于管理员了解应用的特征和进行策略配置； 9、▲支持将非法热点接入网络的行为通过邮件告警通知管理员，并在数据中心支持行为记录和查询； 10、▲支持基于“流量”、“流速”、“时长”设置配额，当配额耗尽后，将用户加入到指定的流控黑名单惩罚通道中； 11、▲针对单用户的行为分析（包括：应用流速趋势、应用流量排行、域名流量排行、应用时长排行、域名时长排行、行为汇总排行等）；		
16	网络机柜	2 个	金盾、ND61042-MB、广州南盾通讯设备有限公司、中国	**标准 42U 宽 600mm*深 1070mm*高 2045mm** 符合 ANSI/EIA RS-310-D、DIN41491:PART1、DIN41494:PART7、GB/T3047.2-92 标准，ETSI 标准 承载：静承载重达 300KG-800kg	7,500.00	15,000.00

				防护等级：IP20； 主要材料：Q235-A.F 优质冷轧钢板制作； 厚度：方孔条 1.5mm，安装梁 1.2mm，其他 1.0mm； 表面处理：脱脂→酸洗→磷化→静电喷涂。		
17	等保保护测评服务	1 项		邀请具有等级保护测评资质的测评单位进行等级保护测评服务，基于等保 2.0 最新标准（网络安全等级保护：2 级）主要内容为物理安全评估，网络安全测评，主机安全测评，应用安全测评，数据安全及备份恢复测评，安全管理制度评估，安全管理机构评估，人员安全管理评估，系统建设管理评估，安全运维管理评估等。 注：若成交供应商没有相应资质提供等级保护测评服务的，须邀请具有安全等级测评资质的第三方机构进行测评，但测评的第三方机构必须经业主认同方可进行。	160,000.00	160,000.00
18	机房综合整改	1 项		包含 6 大内容： 1、机房环境改造部份； 2、机房综合布线系统部份； 3、门禁监控部分； 4、动力环境监控部分； 5、防雷改造部分 ； 6、系统集成技术服务 。 注：供应商应就上述 6 项内容作出完整唯一报价，项目完结后，	280,000.00	280,000.00

				供应商的此次报价将作为最终的结算价格。		
总报价：人民币 壹佰玖拾捌万元整（￥1980000.00 元）						
交货期：分批次交货，签订合同后根据业主指定时间指定地点分批次交货。						
交货地点：采购人指定地点。						
质保期：按国家有关产品“三包”规定执行“三包”，自货物验收合格之日起计算，产品质保期3年。若厂家免费质保期超过此年限的，合同履行过程中按厂家规定执行。						

注：1.所有价格均用人民币表示，单位为元，精确到小数点后两位数。

2.各供应商必须就“项目采购需求和说明”中所有内容作完整唯一报价，否则，其响应文件无效。

3.此表的总报价是所有需采购方支付的本次采购标的金额总数，即竞标总价。竞标总价须包含完成用户需求要求所有内容的全部费用。

4.若此表由多页构成的，需逐页加盖供应商公章。

供应商：广西天驰科技有限责任公司

地址：柳州市飞鹅二路1号谷埠街国际商城K1栋9-18号　　邮编：545000

电话：0772-2818271　传真：0772-2818271

法定代表人或委托代理人：（签字）

日期：2020年6月9日