**开标一览表**

项目编号：GXZC2020-G1-005712-GXGS

投标人名称：广西电子政务外网政务云资源扩容采购 单位：元

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 分标 | 货物名称 | 数量 | 产地 | 品牌及厂家 | 规格型号 | 单价 | 投标报价 |
| / | 管理节点服务器 | 8台 | 深圳 | 浪潮、浪潮电子信息产业股份有限公司 | 型号NF5280M5，参数如下： 1.采用2U机架式服务器，国产自主可控，非OEM。 2.配置2颗Intel Cascade Lake系列金牌可扩展处理器5218R，每颗处理器主频2.1G，内核数20。 3.配置16条32GB DDR4-2933MHz内存。 4.配置2块600GB 10K SAS硬盘，12块960GB固态硬盘，4块1.8TB 10K SAS硬盘。 5.配置1个高性能SAS Raid卡（2GB缓存，含掉电保护功能，支持直通模式）。 6.配置双口千兆网卡×2（电口），双口万兆网卡×2（光口），配置4个万兆光模块（多模），支持OCP网络模块，支持1Gb/10Gb/25Gb速率，支持1/2/4个以太网或光纤网络接口；支持标准1Gb/10Gb/25Gb/40G/100Gb以太网络，支持1/2/4个以太网接口。 7.支持9个PCIE插槽。 8.支持4个双宽GPU。 9.配置冗余热插拔高效电源。 10.提供4个冗余热插拔风扇。独立风扇控制，采用双转子大尺寸风扇，支持免工具热插拔维护。 11.集成系统管理芯片，支持IPMI2.0、KVM over IP、虚拟媒体等管理功能。 12.提供原厂服务器管理套件。 13.支持TPM安全可信模块。 14.提供原厂3年质保服务。 15.投标产品生产厂家2019年中国X86服务器市场出货量排名前三。 | 102108 | 816864 |
| 虚拟化服务器 | 92台 | 深圳 | 浪潮、浪潮电子信息产业股份有限公司 | 型号NF5280M5，参数如下： 1.采用2U机架式服务器，国产自主可控，非OEM。 2.配置2颗Intel Cascade Lake系列金牌可扩展处理器5220R，每颗处理器主频2.2G，内核数24。 3.配置24个32GB DDR4-2933MHz内存，总内存容量为768G。 4.配置2块600GB 10K SAS硬盘。 5.配置1个高性能SAS Raid卡（2GB缓存，含掉电保护功能，支持直通模式）。 6.本次配置双口千兆网卡×2（电口），双口万兆网卡×3（光口），配置6个万兆光模块（多模），支持OCP网络模块，支持1Gb/10Gb/25Gb速率，支持1/2/4个以太网或光纤网络接口；支持标准1Gb/10Gb/25Gb/40G/100Gb以太网络，支持1/2/4个以太网接口。 7.支持9个PCIE插槽，配置2个双口16Gb FC HBA卡。 8.支持4个双宽GPU。 9.配置冗余热插拔高效电源。 10.提供4个冗余热插拔风扇。独立风扇控制，采用双转子大尺寸风扇，支持免工具热插拔维护。 11.集成系统管理芯片，支持IPMI2.0、KVM over IP、虚拟媒体等管理功能。 12.提供原厂服务器管理套件。 13.支持TPM安全可信模块。 14.提供原厂3年质保服务。 15.投标产品生产厂家2019年中国X86服务器市场出货量排名前三。 | 64133 | 5900236 |
| GPU计算服务器 | 10台 | 深圳 | 浪潮、浪潮电子信息产业股份有限公司 | 型号NF5468M5，参数如下： 1.采用4U机架式服务器，国产自主可控，非OEM。 2.配置2颗Intel Cascade Lake系列金牌可扩展处理器6230R，每颗处理器主频2.1G，内核数26。 3.配置16个32GB DDR4-2933MHz内存。 4.配置2块480GB固态硬盘，最大支持24个3.5寸硬盘槽位。 5.配置1个高性能SAS Raid卡（2GB缓存，含掉电保护功能，支持直通模式）。 6.配置四口千兆网卡×1（电口），双口万兆网卡×2（光口），配置4个万兆光模块（多模），配置2个双口16Gb FC HBA卡。 7.支持20个PCIE插槽，支持8片NVIDIA®Tesla®NVLink & PCIe V100，V100s，或支持20片NVIDIA®Tesla®T4。 8.配置4片NVIDIA®Tesla®T4。 9.配置冗余热插拔高效电源。 10.提供4个冗余热插拔风扇。独立风扇控制，采用双转子大尺寸风扇，支持免工具热插拔维护。 11.集成系统管理芯片，支持IPMI2.0、KVM over IP、虚拟媒体等管理功能。 12.提供原厂服务器管理套件。 13.支持TPM安全可信模块。 14.提供原厂3年质保服务。 15.投标产品生产厂家2019年中国X86服务器市场出货量排名前三。 | 129919 | 1299190 |
| 数据库服务器 | 10台 | 深圳 | 浪潮、浪潮电子信息产业股份有限公司 | 型号NF8480M5，参数如下： 1.采用4U机架式服务器，国产自主可控，非OEM。 2.配置4颗Intel Cascade Lake系列金牌可扩展处理器6226，每颗处理器主频2.8G ，内核数12。 3.配置24个32GB DDR4-2933MHz内存，内存总量为768G。 4.配置2块600GB 10K SAS硬盘，2块4TB 7.2K SAS硬盘，最大支持24块3.5寸硬盘。 5.配置1个高性能 SAS Raid卡（2GB缓存，含掉电保护功能，支持直通模式）。 6.配置双口千兆网卡×2（电口），双口万兆网卡×2（光口），配置6个万兆光模块（多模），支持OCP网络模块，支持1Gb/10Gb/25Gb速率，支持1/2/4个以太网或光纤网络接口；支持标准1Gb/10Gb/25Gb/40G/100Gb以太网络，支持1/2/4个以太网接口。 7.支持16个PCIE插槽。 8.配置2个双口16Gb FC HBA卡。 9.配置冗余热插拔高效电源。 10.提供4个冗余热插拔风扇。独立风扇控制，采用双转子大尺寸风扇，支持免工具热插拔维护。 11.集成系统管理芯片，支持IPMI2.0、KVM over IP、虚拟媒体等管理功能。 12.提供原厂服务器管理套件。 13.支持TPM安全可信模块。 14.提供原厂3年质保服务。 15.投标产品生产厂家2019年中国X86服务器市场出货量排名前三。 | 103494 | 1034940 |
| 服务器操作系统授权 | 100套 | 北京 | 微软、微软(中国)有限公司 | 在本项目中提供Windows server 2016中文标准版的服务器操作系统。 | 3739 | 373900 |
| 分布式存储 | 2套 | 深圳 | 浪潮、浪潮电子信息产业股份有限公司 | 型号分布式存储NF5280M5，包含如下内容： 1.分布式存储软件： 1）分布式存储软件具有自主知识产权，使用3副本策略并配置600TB可用容量授权 ； 2）支持按照指定刀片或者服务器范围，按冗余方式（副本）、组网方式、加速方式（cache介质）、存储介质等属性灵活组成多个不同的存储资源池，向上层业务提供大容量、性能和可靠性差异化的存储能力；支持块、对象和文件3种存储服务类型； 3）支持128个资源池，支持4000台存储节点，单卷最大容量可以支持250TB； 4）支持SSD Cache加速特性，包括写缓存、预读、读热点三种Cache 能力（依赖RAID卡的Cache能力不算）； 5）组网可支持10GE以太网/RoCE、56Gb/s IB； 6）支持OpenStack，包括支持OpenStack Cinder接口；支持InfiniBand高速互联网络，并且支持RDMA访问协议； 7）支持虚拟化方式部署，支持虚拟化平台包括如下3种：VMWARE、KVM、XEN；支持物理服务器方式部署； 8）分布式块存储提供的客户端支持SuSE、RedHat、Oracle Linux等通用的Linux系统； 9）块存储支持配置2副本或3副本；文件和对象存储支持EC数据保护；支持快照、自动负载均衡等功能； 10）支持硬件亚健康和故障检测和处理功能，能提前发现系统中的硬盘坏道隐患，给出相应的告警信息，并进行数据预重建，以排除隐患； 11）支持掉电数据保护功能； 12）具有独立的OM操作维护图形界面来对存储资源池进行管理，支持对块存储系统的CPU利用率、内存利用率、带宽、IOPS、时延、磁盘利用率、存储池利用率等的统计； 13）在创建资源池的时候，用户可以指定该资源池的安全等级（服务器级别安全、柜级别安全）、数据保护策略（2副本、3副本）。并且可以在Portal上直观的看到每个资源池的属性，不同的VM根据需求放入不同的资源池中。 2.每套15台存储节点，每台节点参数如下： 1）采用2U机架式服务器，国产自主可控，非OEM； 2）本次配置2颗Intel Xeon系列可扩展处理器4214，每颗处理器主频2.2G，内核数12； 3）配置4个32GB DDR4-2933MHz内存； 4）配置2块600GB 10K SAS硬盘，2块480GB固态硬盘，10块10TB 7.2K SATA硬盘； 5）配置1个高性能 SAS Raid卡（2GB缓存，含掉电保护功能，支持直通模式）； 6）本次配置双口千兆网卡×1（电口），双口万兆网卡×1（光口），配置2个万兆光模块（多模），支持OCP网络模块，支持1Gb/10Gb/25Gb速率，支持1/2/4个以太网或光纤网络接口；支持标准1Gb/10Gb/25Gb/40G/100Gb以太网络，支持1/2/4个以太网接口； 7）支持9个PCIE插槽； 8）支持4个双宽GPU； 9）配置冗余热插拔高效电源； 10）提供4个冗余热插拔风扇。独立风扇控制，采用双转子大尺寸风扇，支持免工具热插拔维护； 11）集成系统管理芯片，支持IPMI2.0、KVM over IP、虚拟媒体等管理功能； 12）提供原厂服务器管理套件； 13）支持TPM安全可信模块； 14）提供原厂3年质保服务； 15）投标产品生产厂家2019年中国X86服务器市场出货量排名前三。 | 57767 | 115534 |
| FC SAN存储 | 4台 | 深圳 | 浪潮、浪潮电子信息产业股份有限公司 | 型号AS5800G5，每2台采用镜像双活方式部署实施，总体可用存储容量600TB。每台参数如下： 1.非联合品牌或者OEM产品（投标时在投标文件中提供国家版权局颁发的计算机软件著作权登记证书复印件） 。 2.采用SAN和NAS统一集成的控制器架构，设备同时支持NAS和SAN功能。 3.本次配置控制器数量2；控制器冗余设计，支持在线更换控制器，可扩展到8个控制器。 4.控制器采用Intel Xeon处理器 ，每个控制器配置2个16核至强处理器，主频2.1G。 5.采用内置SSD盘作为存储系统盘，非机械硬盘做Raid模式；同时系统盘可以做cache数据掉电保护。 6.双控制器配置高速缓存1024GB（高速缓存不包含SSD磁盘、闪存及NAS控制器缓存等），系统最大支持3072GB高速缓存。 7.两个虚拟化控制器之间通过PCI-E 3.0内部总线连接通讯和缓存数据镜像，非外部交换设备连接。 8.配置12个16Gb FC前端主机接口，每个控制器配置12个前端IO插槽。 9.支持缓存保护，并配置BBU电池保护模组，保证掉电时Cache数据可安全写入Flash或硬盘永久保存，实现无限时断电保护Cache数据的目的。 10.配置307TB 10K SAS硬盘（单盘容量2.4TB），122TB SSD固态硬盘（单盘容量3.84TB），可用存储容量300TB。满足同一个RAID组内任意2块物理硬盘同时出现故障时不影响系统正常运行，配置热备盘2块。 11.支持RAID0，1，5，6，10等。 12.配置基于存储阵列的安全控制管理软件，以保证在SAN环境下，不同主机系统对存储阵列访问的安全性，配置无限制分区数，不得额外收取许可费用。 13.配置路径冗余管理软件，以实现主机的多通道访问以及对应用透明的自动故障通道切换功能，确保在通道发生故障的情况下，仍可以连续访问信息；且未来增加主机数量，不额外收取许可费用。 14.配置数据快照功能；数据复制功能；数据镜像功能。 15.配置自动分层功能，支持SSD、3D NAND SSD、SAS、NL-SAS四层分层架构，通过存储系统内部监测和统计功能，动态的将热点数据自动的迁移到高速的SSD硬盘上。 16.配置QoS功能，实现卷级别的IOPS或者Mbps限制。 17.配置数据在线实时压缩功能，数据写入存储的过程中能够实时的压缩，可以节省大量的磁盘空间。采用硬件压缩技术，同时采用基于时间的压缩技术，提高存储的整体性能。 18.配置存储之间的双活功能，保证采购人业务的连续性，PRO=0，RTO=0，能够达到两个站点的双读双写，实现真正的双活解决方案；双活存储数据传送采用FC协议和链路双活（非IP协议或者IP链路）。 19.可通过GUI或CLI设置阵列；可提供集中化的事件日志记录和报警、实时的Email事件通告，允许用户监控存储系统。 20.支持云备份接口，支持存储数据直接备份到公有云和私有云，无须备份软件支持。 21.所投产品生产厂家浪潮电子信息产业股份有限公司入选Gartner通用磁盘阵列存储魔力象限（供货时提供证明材料并加盖生产厂家公章）。 22.所投产品生产厂家浪潮电子信息产业股份有限公司具备SNIA存储网络工业协会会员资格（供货时提供官网链接和截图并加盖生产厂家公章）。 23.所投产品生产厂家浪潮电子信息产业股份有限公司拥有属于自身品牌的电气和电子工程师协会IEEE OUI（组织唯一标识符）地址段（供货时提供官网链接和截图并加盖生产厂家公章）。  24.存储系统在配合云管理平台作为存储资源池存使用模式下，保证开通虚拟机资源不受存储卷数量的限制。 25.提供设备原厂工程师现场安装服务和培训；设备原厂商提供3年质保和3年7×24小时现场保修服务，包括硬件保修电话支持、现场支持、软件升级。 | 1621185 | 6484740 |
| 业务网核心交换机 | 4台 | 深圳 | Huawei、华为技术有限公司 | 型号CloudEngine 16808，参数如下： 1.设备性能：支持交换容量645Tbps，支持包转发率230400Mpp。 2.硬件规格：正交网板设计，Clos交换架构，整机业务板槽位数8个，独立主控引擎2个，独立的交换网槽位6个，独立的风扇框数量3个，可拔插电源模块槽位10个。 3.设备配置：提供主控引擎2块，提供交换网板5块，交流电源模块4块，可拔插风扇框3个，40GE QSFP+接口36个，10GE以太网SFP+接口48个，40GE QSFP+多模光模块12个，万兆多模光模块32个，40GMPO线缆12根。 4.CPU和交换芯片均为国产芯片。 5.信元交换：支持信元交换，流量可以负载分担到多块交换网，提高交换网利用效率。 6.二层功能：支持M-LAG或vPC等类似技术（跨框链路聚合，要求配对设备有独立的控制平面，不能用堆叠等多虚一技术实现）。 7.三层功能：支持RIP、OSPF、ISIS、BGP等IPv4、IPV6动态路由协议。 8.支持IP报文分片重组。 9.可靠性：支持BFD（Bidirectional Forwarding Detection）小于3.3ms检测间隔。 10.DC特性：支持Vxlan，且支持BGP EVPN特性，支持ESI（Ethernet Segment Identifier）多归接入，支持缓存的微突发状态统计。 11.安全性：支持微分段，支持NSH，支持Vxlan ARP广播抑制。 12.流量分析：支持sflow，支持Netstream。 13.配置和维护：支持Telemetry，支持VxLAN OAM：VxLAN ping，VxLAN tracert。 14.提供原厂3年质保服务。 | 452021 | 1808084 |
| 业务网接入交换机 | 4台 | 深圳 | Huawei、华为技术有限公司 | 型号CloudEngine 6881E-48S6CQ，参数如下： 1.设备性能：交换容量4.8Tbps，包转发率2000Mpps。 2.硬件规格：高度1U，固定接口交换机，10GE光端口数量48个，40/100 GE 光接口6个，标准USB接口1个，ETH管理接口1个，可拔插电源模块槽位2个，可拔插风扇模块槽位4个。 3.设备配置：提供万兆多模光模块48个，提供40GE多模光模块4个，提供可拔插交流电源模块2个，提供可拔插风扇模块4个，提供40G MPO线缆4根。 4.芯片：CPU和LSW交换芯片均为国产芯片。 5.规格表项：支持MAC地址256K，ACL规格表项30K，ARP表项256K，Ipv4路由FIB表256K，Ipv6路由FIB表80K，VxLAN隧道2000，VNI数量8K。 6.二层功能：支持M-LAG或vPC等类似技术（跨框链路聚合，要求配对设备有独立的控制平面，不能用堆叠等多虚一技术实现）。 7.三层功能：支持RIP、OSPF、ISIS、BGP等IPv4、IPV6动态路由协议。 8.IP报文：支持IP报文分片重组。 9.可靠性：支持（Bidirectional Forwarding Detection）小于3.3ms检测间隔。 10.DC特性：支持Vxlan，且支持BGP EVPN特性，支持QinQ Access VXLAN，支持ESI（Ethernet Segment Identifier）多归接入。 11.安全性：支持防止Dos、arp攻击和ICMP攻击，支持支持微分段。 12.流量分析：支持sflow，支持Netstream。 13.配置和维护：支持SNMP V1/V2/V3、Telnet、RMON、SSH，支持Telemetry，支持配置回滚。 14.提供原厂3年质保服务。 | 73346 | 293384 |
| 管理网控制交换机 | 4台 | 深圳 | Huawei、华为技术有限公司 | 型号CloudEngine S5735-S48T4X，参数如下： 1.设备性能：交换容量432Gbps，转发性能144Mpps。 2.设备配置：提供千兆电口48个，万兆SFP+光口4个，配置标准USB接口1个，ETH管理接口1个，支持模块化可插拔电源槽位2个，提供可拔插交流电源模块2个。 3.规格表项：支持MAC地址16K，支持ARP表项8K，支持Ipv4路由FIB表8K，Ipv6路由FIB表3K。 4.IP路由：支持OSPF、OSPFv3、BGP、BGP4+等路由协议。 5.纵向虚拟化：支持纵向虚拟化，作为纵向子节点零配置即插即用。 6.安全：支持802.1x、MAC认证和Portal认证，支持 IPSec对管理报文加密，支持CPU保护功能。 7.网络管理：支持SNMP v1/v2/v3、Telnet、RMON、SSHv2，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。 | 10085 | 40340 |
| 管理网带内管理交换机 | 4台 | 深圳 | Huawei、华为技术有限公司 | 型号CloudEngine S5735-S48T4X，参数如下： 1.设备性能：交换容量432Gbps，转发性能144Mpps。 2.设备配置：提供千兆电口48个，万兆SFP+光口4个，配置标准USB接口1个，ETH管理接口1个，支持模块化可插拔电源槽位2个，提供可拔插交流电源模块2个。 3.规格表项：支持MAC地址16K，支持ARP表项8K，支持Ipv4路由FIB表8K，Ipv6路由FIB表3K。 4.IP路由：支持OSPF、OSPFv3、BGP、BGP4+等路由协议。 5.纵向虚拟化：支持纵向虚拟化，作为纵向子节点零配置即插即用。 6.安全：支持802.1x、MAC认证和Portal认证，支持 IPSec对管理报文加密，支持CPU保护功能。 7.网络管理：支持SNMP v1/v2/v3、Telnet、RMON、SSHv2，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。 8.提供原厂3年质保服务。 | 10085 | 40340 |
| 管理网带外管理交换机 | 4台 | 深圳 | Huawei、华为技术有限公司 | 型号CloudEngine S5735-S48T4X，参数如下： 1.设备性能：交换容量432Gbps，转发性能144Mpps。 2.设备配置：提供千兆电口48个，万兆SFP+光口4个，配置标准USB接口1个，ETH管理接口1个，支持模块化可插拔电源槽位2个，提供可拔插交流电源模块2个。 3.规格表项：支持MAC地址16K，支持ARP表项8K，支持Ipv4路由FIB表8K，Ipv6路由FIB表3K。 4.IP路由：支持OSPF、OSPFv3、BGP、BGP4+等路由协议。 5.纵向虚拟化：支持纵向虚拟化，作为纵向子节点零配置即插即用。 6.安全：支持802.1x、MAC认证和Portal认证，支持 IPSec对管理报文加密，支持CPU保护功能。 7.网络管理：支持SNMP v1/v2/v3、Telnet、RMON、SSHv2，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。 8.提供原厂3年质保服务。 | 10085 | 40340 |
| 存储网接入交换机 | 4台 | 深圳 | Huawei、华为技术有限公司 | 型号CloudEngine 6881E-48S6CQ，参数如下： 1.设备性能：交换容量4.8Tbps，包转发率2000Mpps。 2.硬件规格：10GE光端口数量48个，40/100 GE光接口6个，标准USB接口1个，ETH管理接口1个，可拔插电源模块槽位2个，可拔插风扇模块槽位4个。 3.设备配置：提供万兆多模光模块48个，提供40GE多模光模块4个，提供可拔插交流电源模块2个，提供可拔插风扇模块4个，提供40G MPO线缆4根。 4.芯片：CPU和LSW交换芯片均为国产芯片。 5.规格表项：支持MAC地址256K，ACL规格表项30K，ARP表项256K，Ipv4路由FIB表256K，Ipv6路由FIB表80K，VxLAN隧道2000，VNI数量8K。 6.二层功能：支持M-LAG或vPC等类似技术（跨框链路聚合，要求配对设备有独立的控制平面，不能用堆叠等多虚一技术实现）。 7.三层功能：支持RIP、OSPF、ISIS、BGP等IPv4、IPV6动态路由协议； 8.IP报文：支持IP报文分片重组。 9.可靠性：支持（Bidirectional Forwarding Detection）小于3.3ms检测间隔。 10.DC特性：支持Vxlan，且支持BGP EVPN特性，支持QinQ Access VXLAN，支持ESI（Ethernet Segment Identifier）多归接入。 11.安全性：支持防止Dos、arp攻击和ICMP攻击，支持支持微分段。 12.流量分析：支持sflow，支持Netstream。 13.配置和维护：支持SNMP V1/V2/V3、Telnet、RMON、SSH，支持Telemetry，支持配置回滚。 14.提供原厂3年质保服务。 | 73346 | 293384 |
| 存储网管理交换机 | 4台 | 深圳 | Huawei、华为技术有限公司 | 型号CloudEngine S5735-S48T4X，参数如下： 1.设备性能：交换容量432Gbps，转发性能144Mpps。 2.设备配置：提供千兆电口48个，万兆SFP+光口4个，配置标准USB接口1个，ETH管理接口1个，支持模块化可插拔电源槽位2个，提供可拔插交流电源模块2个。 3.规格表项：支持MAC地址16K，支持ARP表项8K，支持Ipv4路由FIB表8K，Ipv6路由FIB表3K。 4.IP路由：支持OSPF、OSPFv3、BGP、BGP4+等路由协议。 5.纵向虚拟化：支持纵向虚拟化，作为纵向子节点零配置即插即用。 6.安全：支持802.1x、MAC认证和Portal认证，支持 IPSec对管理报文加密，支持CPU保护功能。 7.网络管理：支持SNMP v1/v2/v3、Telnet、RMON、SSHv2，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。 | 196601 | 786404 |
| 存储网光纤交换机 | 8台 | 深圳 | 浪潮、浪潮电子信息产业股份有限公司 | 型号FS8600，参数如下： 1.光纤通道端口：支持端口64个端口。本次配置48口32G FC接口，激活48口并配置48×32多模SPF模块模块。 2.冗余电源：配置双电源。 3.接口光模块特性：FC端口速度支持自动检测功能，可后向兼容32、16、10、8和4Gbps 光纤通道链路；可在线热插拔。 4.多链路捆绑功能：支持基于帧的干线合并，每条ISL中继最多8个32 Gbps SFP+端口，每条ISL中继最多有2个128 Gbps QSFP端口。 5.可管理性： （1）支持SNMPv1/v3、Telnet、Web管理／GUI界面； （2）支持D\_Port离线诊断、E\_Ports间前向纠错（FEC）以及IO Insight。 7.SAN路由支持：支持光纤通道（FC）集成路由功能。 8.兼容性：能够支持著名存储厂家的主流盘阵设备。 9.光纤交换机实现负载均衡方式部署。 10.提供原厂3年质保服务。 | 190896 | 1527168 |
| 应用负载均衡 | 4台 | 深圳 | 深信服、深信服科技股份有限公司 | 型号AD-1000-I482，参数如下： 1.性能参数：4层吞吐量25Gbps，并发连接数20000000，4层新建连接数CPS550000，7层新建连接数 RPS250000，7层新建连接数RPS（开启连接池）570000。硬件参数：规格：2U，电源：冗余电源，接口：8千兆电口，8千兆光口SFP，4万兆光口。 2.部署方式支持串接部署、旁路部署；支持三角传输模式。 3.设备形态独立专业负载设备，非插卡式扩展的负载均衡设备。 4.提供针对多条出口线路的链路负载均衡功能，实现inbound和outbound流量的均衡调度，以及链路之间的冗余互备。 5.支持静态IP和PPPOE两种线路接入方式。 6.提供针对多站点业务发布的全局负载均衡功能，通过智能DNS等机制实现公网用户对多个数据中心或单个数据中心多条线路的最佳访问。 7.支持被动式健康检查，可根据对业务流量的观测采样，辅助判断应用服务器健康状况；对常规HTTP应用可配置基于反映URL失效的HTTP响应状态码的观测判断机制，对于复杂应用可配置基于RST关闭连接和零窗口等异常TCP传输行为的观测判断机制。 8.支持主动探测方式与被动观测方式结合使用的服务器健康检查手段。 9.对Oracle数据库和Weblogic中间件的关键性能指标监控，并通过报表的形式多维度实时展现关键性能参数。 10、支持图片优化技术，通过对图片格式的转换，减少传输流量，提升web页面加载速度。无需改动服务器端的图片源文件，可根据浏览器种类自动识别转换类型，将图片转换为对应支持的WebP或JPEG格式。 11.支持DNS透明代理功能，可基于负载均衡算法代理内网用户进行DNS请求转发，避免单运营商DNS解析出现单一链路流量过载，平衡多条运营商线路的带宽利用率。 12.支持基于链路流量负荷情况的繁忙保护机制，能根据链路的上行/下行带宽占用率情况执行对出站/入站流量的高级调度策略。 13.支持服务器浪涌保护，支持面向服务器健康度的弹性调控机制，可通过监控业务流中的TCP传输异常来衡量服务器节点的有效性，尝试对性能不足的服务器临时开启过载保护，动态调节服务器的负载。 14.支持实时漏洞检测功能，通过对实时流量进行安全性分析来评估业务系统的漏洞风险。 15.提供原厂3年质保服务。 | 148500 | 594000 |
| 综合安全接入网关 | 4台 | 深圳 | Huawei、华为技术有限公司 | 型号USG6655E，参数如下： 1.硬件架构：设备高度1U，支持可拔插交流电源模块2个，支持可插拔风扇模块4个。 2.性能要求：吞吐量40Gbps，最大并发连接数1200万，每秒新建连接数40万，IPSec吞吐量30Gbps，IPSec VPN隧道15000。 3.配置要求：提供千兆电口16个，万兆SFP+光口12个，40GE接口2个，可插拔交流电源模块2个，可插拔风扇模块4个，光模块-SFP+-10G-多模模块（850nm，0.3km，LC）4个，SSL VPN并发数授权100个，虚拟防火墙数量1000个，提供IPS、AV特征库升级授权36个月，提供URL远程查询升级36个月，固态硬盘 240GB。 4为适应机房部署规范，设备采用前后风道设计。 5.策略管控：能够基于时间、用户/用户组/安全组、应用层协议、地理位置、IP地址、端口、域名组、URL分类、接入类型、终端类型、设备组、内容安全统一界面进行安全策略配置。 6.策略管理：支持将基于端口的安全策略转换为基于应用的安全策略，分析设备策略风险，及冗余策略，提供安全策略优化建议。 7.入侵防御：基于特征检测，支持超过8000种特征的攻击检测和防御，支持对常见应用服务（HTTP、FTP、SSH、SMTP、IMAP）和数据库软件（MySQL、Oracle、MSSQL）的口令暴力破解防护功能，支持恶意域名过滤，实现对C&C进行阻断。 8.病毒防护：可以支持HTTP、FTP、SMTP、POP3、IMAP、NFS等协议的病毒防护。 9.加密流量安全防护：支持对HTTPS、POP3S、SMTPS、IMAPS加密流量代理解密后，并进行内容过滤，审计，安全防护，支持加密流量解密后镜像给第三方设备做审计，安全检测。 10.沙箱联动：支持与沙箱联动，实现对APT攻击的防御功能。 11.智能威胁防御：支持网络安全智能分析系统联动，做态势感知，全网威胁展示，并能针对威胁生成阻断策略。 12.硬件提供原厂3年质保服务。 | 183966 | 735864 |
| 管理区防火墙 | 2台 | 北京 | 绿盟、北京神州绿盟科技有限公司 | 型号NFNX5-CH7355-X60，参数如下： 1.基本配置 （1）产品采用2U标准19"机架式硬件平台，交流冗余电源，配置8个SFP+万兆光口（含8块万兆多模光模块），一个接口扩展槽，1个RJ45串口，2个RJ45管理口，2个USB接口； （2）产品网络吞吐量40Gbps；应用层吞吐量25Gbps，最大并发连接数1200万，每秒新建会话数50万； （3）配置防病毒、入侵防御功能模块，提供3年软件升级、IPS特征库、防病毒特征库升级及硬件质保服务； 2.功能指标 （1）部署能力：支持虚拟线、二层透明、三层、PPPoE、混合、旁路监听接入方式，适应各种网络环境需求，同时支持配置向导； （2）提供基于源/目的IP地址、安全区、应用/应用过滤器、协议/端口、时间、用户、安全模板/模板组的精细粒度的安全访问控制； （3）支持基于策略的双向NAT、动态/静态NAT、端口PAT，支持多对一及多对多的映射； （4）支持静态路由；支持RIP、OSPF、BGP等动态路由协议；支持基于源/目的地址、接口的、基于服务的策略路由；支持Vlan路由，能够在不同的VLAN虚接口间实现路由功能；支持单臂路由，可通过单臂模式接入网络，并提供路由转发功能；支持ISP路由，反向路由； （5）提供默认模板的数量7种，包括针对WEB服务器防护模板、针对windows服务器防火墙模板、针对UNIX服务器防护模板。web服务器防护模板规则数量2152条； （6）支持对入侵规则库的分类组织和管理，包括：攻击手段/技术/流行度/危险度/服务类型； （7）支持对1743种应用平台及2622种的应用进行识别和控制，支持5大类，比如：商业系统、协作应用、一般网络应用、媒体等及28子类，比如：认证服务、数据库、ERP-CRM、软件更新、电子邮件、VOIP视频、游戏等；支持自定义应用； （8）支持木马病毒、蠕虫病毒、宏病毒、脚本病毒等各种病毒的查杀，支持文件名称、类型及病毒名称的白名单，支持以文件扫描方式查杀病毒。支持HTTP、FTP、POP3、SMTP协议的病毒查杀； （9）支持列表显示在线资产信息，包括用户、浏览器版本、操作系统及版本、杀毒软件情况、网络应用使用情况及网络流量情况；并支持对高风险资产一键建立访问拦截策略和流量控制策略； （10）支持应用过滤器，支持4个维度进行过滤，比如：应用类别、实现技术、风险等级、标签，并且能够将通过应用过滤器筛选出来的应用直接生成模板供用户统一管理使用； （11）可生成内网资产风险报表，提供高风险资产top10，提供操作系统等相关资产信息的数据统计和报表展示； （12）支持对每条策略命中数据包的统计显示，通过数据包命中数判断策略的命中频率，同时也支持对匹配上策略的会话的超时控制功能，可指定为永不超时，也可以指定确定的范围【5～7200】秒； （13）可自定义操作系统、浏览器、杀毒软件的风险等级，并支持预置风险等级；可为每个内网主机生成风险指数，通过数字直观展示内网主机的风险状态；资产风险涵盖了操作系统、浏览器、杀毒软件、应用、流量、服务等内容；可针对高风险资产提供屏蔽功能，阻止其连接互联网； （14）支持事件关联分析，能够对防火墙的日志进行关联分析，在事件关联分析中，可以设置自定义应用、目的IP、源IP，即使不在TOPN里面，同样可以进行统计及数据挖掘。针对事件关联分析，可以提供多种入口，比如基于应用、目的IP、源IP、用户、攻击事件等； （15）所有部件包括检测引擎、规则库、管理控制台等均可升级，同时支持在线和离线两种升级方式，在线升级的过程不影响或中断检测。在线升级支持实时在线升级和定时在线升级；离线升级支持控制台、串口、SSH等多种方式。 3.其他要求 （1）所投产品绿盟NF防火墙系统V6.0具有中华人民共和国公安部的《计算机信息系统安全专用产品销售许可证》； （2）所投产品生产厂家北京神州绿盟科技有限公司在信息安全领域有着丰富的经验与先进的技术，具备对操作系统、应用系统或网络设备的漏洞进行发现、验证的能力，生产厂家自己发现的安全漏洞超过30个，并在CVE官网上能查询到相关漏洞信息（供货时提供CVE官方链接以及查询结果截图并加盖生产厂家公章）； （3）所投产品生产厂家北京神州绿盟科技有限公司为OWASP应用安全联盟成员之一（供货时提供证明材料并加盖生产厂家公章）； （4）所投产品生产厂家北京神州绿盟科技有限公司具备国家信息安全服务（安全开发类）二级及以上资质（供货时提供有效资质证书复印件或相关证明材料并加盖生产厂家公章）； （5）为保障安全运维能力，所投产品生产厂家北京神州绿盟科技有限公司具备CCRC信息系统安全运维一级服务资质（供货时提供有效证明材料并加盖生产厂家公章）； （6）供货时提供所投产品生产厂家北京神州绿盟科技有限公司广西当地办事处的国家计算机网络应急技术处理协调中心提供的漏洞研究证明（CNVD）证书复印件并加盖生产厂家公章。 | 166570 | 333140 |
| 网络分流器 | 2台 | 成都 | 迈普、迈普通信技术股份有限公司 | 型号T6100-48XF2QP，参数如下： 1.标准19英寸1U机架式结构。 2.配置48个10Gb SFP+光口，2个40Gb QSFP光口，2个100G QSFP（兼容40G）光口。 3.配置冗余电源。 4.配置4个40G光模块，20个万兆光模块，12个万兆光转电模块。 5.所有端口均可配置为输入输出，可以设置为1：N、M：N、N：1等模式，M支持任意端口，N支持任意端口。 6.接收输入端口的40GE/10GE/1GE的克隆数据，对接收数据进行复制、汇聚、过滤、处理并从1GE/10GE/40GE端口输出给后端分析设备。 7.支持多台分流器矩阵式多级的管理和部署。支持多台分流器集群统一，实现一个管理IP登陆界面，可以配置不同集群分流器设备。 8.可通过WEB图形方式查询CPU使用率、内存使用率、端口状态，接口性能统计包含当前发送报文数、当前接收报文数、当前发送字节数、当前接收字节数、接口当前发送/接收速率等统计指标。实时流量统计、基于规则的流量统计、历史峰值流量统计、流量阈值告警等。 9.支持WEB管理界面下的抓包存储下载功能。报文实时存储功能，对任意输入口的全部数据包或者ACL规则匹配的数据包执行捕获存储，捕获数据包格式兼容Wireshark/Sniffer等主流报文分析工具；系统提供界面对已捕获的数据报文进行列表展现及删除/下载处理。 10.支持WEB可视化管理，Web方式支持分流器所有功能配置。 11.支持consle/ssh/telnet登录管理。支持AAA认证授权功能；支持NTP客户端和服务端，广播模式和对等体模式部署；支持syslog日志输出，支持SNMP管理。 12.支持端口出方向和入方向的IPV4和IPv6多元组流规则过滤，过滤规则多元组包括L2～L4层所有字段匹配，支持源MAC/目的MAC/VLAN/Cos（vlan优先级）/以太类型/协议/源IP/目的IP/源端口/目的端口/tcp flag/ip优先级（precedence、tos/dscp）和分片标识等多元组匹配。 13.支持隧道（IP-in-IP/Vxlan/GRE）内层数据匹配识别和过滤。 14.支持ACL规则匹配host精准规则容量10000条。 15.支持全数据采集，支持异常流量（IP/TCP/UDP/CRC/SYS flood）错包和超长帧9000字节的数据采集。 16.支持基于端口和基于数据流的VLAN溯源标记功能。 17.支持剥离封装功能，支持VLAN/VXLAN/Fabric path/L2VPN-MPLS/L3VPN-MPLS/VN-TAG/GRE/IP-IN-IP封装剥离。 18.支持隧道剥离后的进行特定VLAN标识再封装。 19.支持出端口数据的VXLAN再封装。 20.支持基于（Smac/Dmac/Vlan/Eth-type/Sip/Dip/Protocol/l4-src-port/l4-dst-port）的任意一种或者几种组合的负载均衡，支持VXLAN/GRE/IP-IN-IP隧道内层的负载均衡，支持基于MAC和IP的同源同宿功能。 21.硬件提供原厂3年质保服务。 | 118974 | 237948 |
| 态势感知探针 | 2台 | 北京 | 网神、网神信息技术（北京）股份有限公司 | 型号为NGSOC-NDS9000-TZ15M，参数如下： 1.冗余电源，标准配置1个10/100/1000M专用管理接口，1个Console口，共8个接口扩展板卡插槽，12个万兆光口（满配光模块），4个千兆光口（满配光模块），4个千兆电口。支持液晶面板实时显示，可通过液晶屏直观查看基本信息。 2.满足如下性能：同时开启网络流量采集、威胁数据采集和日志上报功能情况下，吞吐量15Gbps，HTTP并发连接数1000万，HTTP新建连接速率40万/秒。 3.提供三年系统升级，特征库升级、威胁情报库升级。 4.能够与现有监测分析平台进行对接，实现无缝数据对接与分析。 5.支持数据采集策略配置，支持基于源地址、目的地址、应用、流量采样比、时间进行选择数据采集对象，可以针对采集对象进行网络流量数据采集和威胁检测数据采集，网络流量数据采集支持自定义流量载荷字节数。 6.支持针对流量数据和威胁检测数据可灵活配置外发对象，外发对象包括大数据分析平台及第三方存储对象。 7.支持基于SSL协议的HTTPS流量进行解密，可添加基于源地址、目的地址的解密策略；支持明文流量镜像；支持添加SSL入站检查配置文件；SSL入站检查配置文件中指定SSL解密证书。 8.支持TCP流量采集提取，支持解析、生成及外发TCP流量日志；包括：传感器序列号、TCP数据流的结束方式、TCP数据流开始的时间、源IP、源端口、目的IP、目的端口、源mac、目的mac、协议、上行字节数、下行字节数、客户端系统信息、服务端系统信息、TCP 流的统计信息等字段。 9.支持UDP流量日志采集提取，支持解析、生成及外发UDP流量日志；包含：传感器序列号、UDP数据流开始的时间、UDP数据流结束的时间、源ip、源端口、目的ip、目的端口、源mac、目的mac、协议、上行字节数、下行字节数、上行包数、下行包数字段。 10.支持VXLAN、GRE、VLAN报文解析。 11.硬件提供原厂3年质保服务。 | 178392 | 356784 |
| 租户堡垒机 | 2套 | 杭州 | 浙江齐治股份有限公司、浙江齐治股份有限公司 | 型号RIS-M3-5000，参数如下： 1.基本配置 （1）RIS-M3-5000具备公安部出具的产品销售许可证； （2）RIS-M3-5000具备公安部出具的销售许可证检测报告； （3）RIS-M3-5000具备国家保密局涉密信息系统安全保密测评中心出具的《涉密信息系统产品检测证书》； （4）RIS-M3-5000具备具备国家版权局出具的著作权登记证书； 2.部署/硬件 （1）RIS-M3-5000形态为2U标准硬件； （2）RIS-M3-5000具体配置如下： Ø硬盘：4×4T SATA；内存：32G；电源：冗余电源；网络接口：2个千兆电口；支持6000字符并发，2000图形并发；2台实现HA部署模式； （3）RIS-M3-5000提供2000个授权License，支持可管理2000个目标设备对象，License计算方式以一个IP计算为一个目标对象授权，不按硬件、系统操作系统链接方式、数据库、中间件访问方式计算目标设备对象。 3.功能 （1）用户管理 RIS-M3-5000具备用户管理功能，支持以下具体功能： 1）支持根据功能模块来自定义用户角色，并内置超级管理员、配置管理员、审计管理员、自动化管理员和操作员五种角色； 2）内置动态令牌认证、USBKEY认证和手机令牌认证； 3）支持X.509证书认证方式； 4）支持国密动态令牌认证方式，满足国密标准的身份认证要求； 5）支持与AD、LDAP、RADIUS、短信网关的第三方认证系统联动认证； 6）支持双因子组合认证，可以将两种认证组合为全新的双因子身份认证方式，而非一种双因素认证； 7）支持用户账号的批量导入和批量导出； 8）支持对用户属性信息在页面中直接批量修改； 9）支持AD账号的定期自动化同步，当AD域中的账号有变更时，会被自动同步的系统中，并加入预定义的用户分组； 10）具备账号密码的防爆力破解功能，可在用户持续输错若干次密码后，自动锁定账号或者客户端，锁定时长能够自定义； 11）支持对用户账号登录IP、登录终端MAC地址的限制； 12）提供可自定义短信网关认证对接的接口。 （2）资产管理 RIS-M3-5000具备资产管理功能，具体支持以下功能： 1）支持动态全景视图管理，管理员在设置好资产的层级关系后，系统可自动生成动态全景树状视图； 2）支持资产属性多个层级的标签化管理； 3）支持对资产信息和资产属性在页面中直接批量修改； 4）支持AS400的TN5250协议资产管理、代填和命令审计； 5）支持资产添加后的一键网络端口连通性测试、ping连通性测试和资产登录测试； 6）支持目标资产的自动化跳转登录和账号切换登录； 7）支持应用发布功能，可集中管控各类B/S、C/S应用； 8）支持等价资产管理和等价账号管理，当等价关系设定后，其中一台资产内的账号密码发生变更，等价的资产、账号密码随之自动变更； 9）支持对IPV6资产的管理。 （3）权限管控 RIS-M3-5000具备权限管控功能，支持以下功能： 1）支持基于ABAC模式的动态权限管控，管理员可基于用户属性、资产属性、系统账号属性来创建弹性动态权限规则，只要满足相关属性的用户、资产、账号即会被自动赋予对应访问权限； 2）支持对web系统资产可限制其访问的URL； 3）支持对通过rdp协议登录到目标资产后的剪贴板控制，可限制剪贴板的文件上行、字符上行、文件下行、字符下行操作； 4）支持变更单管理功能，管理员可以基于使用人、资产、系统账号、到期时间，来上传、创建值班表模式的权限变更单，变更单无需审批，但可以自动生成时效性的访问权限； 5）支持按用户/用户组/资产/资产组查看访问权限，权限内容含资产、账号、规则模板及对应的权限策略名称，并可通过EXCEL导出相应权限关系； 6）支持基于A/B角管理模式的双人复核，当用户登录到目标资产时，必须经过复核人的复核确认后才能正常操作；当会话复核人发现操作存在风险，可实时暂停； 7）支持高危命令权限控制，当用户试图去执行高危命令时，会被系统自动给予告警、放行、拒绝、切断会话、转发给管理员复核；高危命令权限控制支持命令黑白名单和命令正则表达式。 （4）电子工单 RIS-M3-5000具备电子工单功能，支持以下具体功能： 1）内置资产访问工单：用户填写包含工单标题、工单描述、需要访问的资产、需要使用的系统账号、需要访问的时间段的电子工单，经审批通过后可自动生成时效性的访问权限； 2）内置密码获取工单：申请人可根据需要填写包含目标资产名称、系统账号名称、使用时间段的密码工单；管理员对密码工单审批通过后，系统自动将密码获取链接发送给申请人；申请人打开链接后，可凭借登录密码+解密密码，获取对应的账号密码；工单过期后，系统自动对该账号进行改密操作。 （5）资产访问 RIS-M3-5000具备资产访问功能，支持以下具体功能： 1）支持以树状结构方式展现用户可访问的资产信息； 2）支持资产一键收藏功能，以便用户通过系统进行快捷资产登录； 3）支持批量启动功能，可一次性登录选择好的目标资产； 4）支持自定义资产访问参数，如桌面分辨率、需要映射的磁盘、会话启动方式等； 5）支持图形会话的自动TLS加密； 6）支持会话多人共管模式，当前运维人员可以邀请其他用户共享或者协助当前操作会话； 7）支持通过苹果电脑的浏览器web方式启动rdp会话和SSH会话； 8）支持显示当前资产的连接数量和会话基本信息，便于运维员了解即将访问的资产会话连接情况； 9）支持在web页面批量访问RDP资产，且是html5方式运维； 10）支持用户单来源地址限制，使得同一用户帐号同时只被允许从一个IP地址访问； 11）支持会话负载限制，防止任意图形会话、字符会话、数据库会话因为占用资源过高导致系统过载甚至宕机。 （6）行为审计 RIS-M3-5000具备行为审计功能，支持以下具体功能： 1）具备命令识别方面的先进性技术，可实现对命令行操作行为的100%记录； 2）具备数据库审计方面的先进性技术，可实现对oracle、sqlserver、mysql数据库客户端操作行为的100%的SQL语句解析审计，非键盘记录； 3）支持从任一条sql语句开始，可录像式的回放用户操作过程； 4）支持64倍速播放功能； 5）支持IPv6资产的运维审计日志； 6）支持对用户命令操作的输入输出，在同一界面展示，并能自动以不同颜色标记出被系统拒绝、切断的操作； 7）具备OCR图形识别技术，可以对图形操作过程中的键盘鼠标操作、剪贴板操作、标题栏操作三大类信息，进行文本审计； 8）支持图形会话的按标题和大小进行切片展示功能，管理员点击任意切片，即可直接定位到对应操作片段； 9）支持文件传输审计，可以完整记录用户通过系统进行的SFTP、剪切板、磁盘映射、rz/sz四大类文件传输操作，并可对传输的文件信息进行留存，以便于事后审计； 10）支持二次检索功能，可根据检索结果调整检索条件进一步缩小检索范围，提高检索精度； 11）支持将多个会话的操作片段进行一键合并和基于时间的操作排序重组。 （7）统计报表 RIS-M3-5000具备统计报表功能，支持以下具体功能： 1）管理员可以手动定制报表模版，并支持根据不同模版自动生成日报、周报、月报，报表内容自动发送给相关管理员； 2）可以统计出某段时间内，用户执行高危命令的情况； 3）报表支持HTML、excel、pdf格式导出。 （8）自动改密 RIS-M3-5000具备自动改密功能，支持以下具体功能： 1）支持对网络设备、服务器、AD域账号的动态自动改密功能，可基于资产属性和账号属性创建弹性动态改密规则，只要满足相关属性的资产和账号即会被自动纳入改密计划； 2）支持自定义密码规则，包括密码策略、是否分段保管、密码备份方式等，密码策略包括随机生成相同密码、随机生成不同密码、指定密码、密码集；密码备份方式支持分段加密外发到邮箱或者文件服务器； 3）支持便捷的expect自定义改密命令的模式，保证字符改密的易用性； 4）支持历史账号密码留存； 5）支持账号密码定期自动备份。 （9）网盘传输 RIS-M3-5000具备网盘传输功能，支持以下具体功能： 1）免客户端：支持通过web页面直接进行文件的上传和下载，无需在本地安装应用程序、客户端； 2）配额管理：支持全局修改用户profile空间配额，用户存放的文件大小不能超过该配额； 3）文件分享：用户可以将自己profile中的文件，直接分享给其他用户； 4）网盘传输：支持用户将暂存在个人profile中的文件，一键上传到目标系统或者一键下载到用户本地； 5）传输进度可视化：支持在web页面上通过进度条的方式展示传输进展。 （10）产品部署 RIS-M3-5000具备产品部署功能，支持以下具体功能： 1）支持active-standby方式的HA部署； 2）支持多A集群部署，且系统内置负载均衡，无需用户另置负载均衡设备； 3）支持跨地域的多A集群模式和HA模式部署； 4）支持总分部署模式，即提供堡垒机管理总中心+分支节点的部署模式，且中心支持HA和集群，节点支持单机或HA。 （11）系统管理 RIS-M3-5000具备系统管理功能，支持以下具体功能： 1）系统语言支持中英文自由切换； 2）支持同一堡垒机用户只能从一个IP地址访问堡垒机，并且支持开关功能； 3）支持定期自动备份审计数据至文件服务器，定期清理过期的审计日志； 4）支持在Web界面自定义设置字符、图形、Web等服务的网络端口； 5）支持在Web界面中查看系统的负载，磁盘占用空间以及关键进程的健康状态； 6）支持三级以上的部门分权管理，使得不同部门的管理员只能管理自己部门的账号、资产、权限及审计日志。 （12）API接口 RIS-M3-5000支持API接口功能，系统具备登录认证、访问权限、用户账号、目标资产、操作审计、定期改密、命令复核的标准API接口。 （13）售后服务 RIS-M3-5000支持提供软硬件3年质保服务。 | 188350 | 376700 |
| 管理堡垒机 | 1台 | 北京 | 绿盟、北京神州绿盟科技有限公司 | 型号OSMSNX3-1000C-C，参数如下： 1.基本配置 （1）所投产品具备公安部的《计算机信息系统安全专用产品销售许可证》（身份鉴别（网络）类）； （2）标准2U机架式设备，含交流冗余电源，1个RJ45串口，1个RJ45管理口，2个USB接口，配置6个GE电口，4个千兆光口，字符并发会话数350个，图形并发会话数800个；硬盘容量2TB，设备最大支持管理3000个设备，配置管理300台设备授权许可； （3）含3年硬件质保及软件升级服务。 2.功能指标 （1）采用物理旁路模式部署，不影响网络结构，支持IP和端口DNAT网络环境部署，通过映射后的IP和端口信息能够访问堡垒机；支持域名方式web访问到堡垒机，并支持托管设备运维操作； （2）系统默认自带三权分立用户，系统管理员、运维管理员和审计管理员权限相互制约。系统管理员负责对系统进行参数设置和维护，不可见托管设备和审计日志等信息；运维管理员负责运维人员和托管设备管理，可对运维行为进行分析，不能管理系统设置和维护；审计管理员负责所有用户行为分析和审计，不可运维托管设备和修改运维人员权限，不可修改系统配置； （3）堡垒机具有用户角色权限自定义功能，可对用户进行细粒度权限划分，可细分用户录入管理员，设备录入管理员，设备账号管理员，运维权限管理员，运维审批管理员，运维审计管理员，普通运维人员和审计员； （4）支持设备访问授权和命令执行授权：除用户身份认证外，对特定目标设备访问与特定命令的执行还需要高级管理员授权才能访问。授权审批方式支持web和手机APP审批； （5）支持对不同用户设置不同的认证方式，即可配置用户1使用本地认证，用户2使用LDAP认证，其他所有用户使用RADIUS认证； （6）支持原厂自研的APP动态密码用户验证，使得动态密码随机种子得到有效的安全保护； （7）用户登录堡垒机支持多种认证方式，包括本地静态密码认证、LDAP认证、RADIUS认证、证书认证、USBKEY认证、短信认证、手机APP动态密码认证等身份认证方式；支持可知因素和不可知因素的双因素认证； （8）支持管理员以用户为基准，直接查询、新建或编辑与该用户相关的策略，支持查询该用户有权限运维的所有设备，且支持以设备访问中的设备为基准，直接查询该设备的所有审计信息、直接查询并编辑与该设备相关的策略、有权限运维该设备的所有普通用户； （9）支持对托管设备所有设备账号密码手动批量备份； （10）支持自动发现运维人员运维过程中创建的幽灵账号（后门账号）行为，并以列表方式向设备管理员展示托管设备中所有的幽灵账号（后门账号）信息； （11）支持本地字符客户端程序，如putty，xshell，securecrt等客户端直接访问堡垒机选取托管设备进行运维，支持本地字符客户端程序一键快速访问目标托管设备进行运维； （12）支持实时监控通过SSH、SFTP、RDP、VNC、Telnet、FTP、X11等协议的操作行为，对监控到的非法操作可实时手工切断； （13）支持自动发现运维人员离职后遗留不用孤儿账号，并以列表方式向管理员展示托管设备中所有的僵尸账号，支持自定义未使用天数； （14）支持SSH（V1、V2）TELNET，Rlogin等字符型、RDP、VNC、X11等图形化远程操作协议，支持FTP、SFTP、SCP、Samba等文件传输协议，支持RDP、VNC的客户端直接访问堡垒机，FTP客户端Wincp直接访问堡垒机；支持Oracle、MS SQL Server、IBM DB2、Sybase、IBM Informix Dynamic Server、MySql、PostgreSQL等数据库；支持HTTP、HTTPS操作审计，HTTP/HTTPS协议可以直接代理； （15）支持Telnet、SSH审计内容：包括访问起始和终止时间、用户名、用户IP地址、目标设备IP、设备名称、协议类型、事件等级及操作内容回放； （16）支持RDP、VNC协议审计内容：包括访问起始和终止时间、用户名、用户IP地址、目标设备IP、设备名称、协议/应用类型、事件等级、操作内容等；支持操作内容录像回放； （17）支持填写特权密码，从普通管理模式进入到特权模式； （18）支持SQL语句级别审计，审计内容包括时间、用户、类型、用户IP、设备IP、数据库账号、数据库客户端名称和SQL关键字等信息，并可通过SQL语句审计结果定位数据库运维操作录像回放； （19）文件操作审计内容：包括访问起始和终止时间、用户名、用户IP地址、目标设备IP、设备名称、协议类型、事件等级、操作内容（如对文件的上传、下载、删除、修改等操作等）； （20）提供周期生成报表，用于审计或者上报，提供给用户按照自定义规则自动周期生成报表的功能。 3.其他 （1）所投产品具有中华人民共和国公安部的《计算机信息系统安全专用产品销售许可证》； （2）所投产品生产厂家在信息安全领域有着丰富的经验与先进的技术，具备对操作系统、应用系统或网络设备的漏洞进行发现、验证的能力，生产厂家自己发现的安全漏洞超过30个，并在CVE官网上能查询到相关漏洞信息（供货时提供CVE官方链接以及查询结果截图并加盖生产厂家公章）； （3）所投产品生产厂家为OWASP应用安全联盟成员之一（供货时提供证明材料并加盖生产厂家公章）； （4）所投产品生产厂家具备国家信息安全服务（安全开发类）二级及以上资质（供货时提供有效资质证书复印件或相关证明材料并加盖生产厂家公章）； （5）为保障安全运维能力，所投产品生产厂家具备CCRC信息系统安全运维一级服务资质（供货时提供有效证明材料并加盖生产厂家公章）。 29.供货时提供所投产品生产厂家广西当地办事处的国家计算机网络应急技术处理协调中心提供的漏洞研究证明（CNVD）证书复印件并加盖生产厂家公章。 | 94300 | 94300 |
| 网络审计 | 2台 | 北京 | 绿盟、北京神州绿盟科技有限公司 | 型号SASNX5-6012B-C，参数如下： 1.基本配置 （1）标准2U机架式设备，冗余交流电源；配置4路审计授权，4个千兆电口，4个万兆光口（配置4块万兆多模光模块）；最大检测能力10Gbps；峰值入库能力30000/S； （2）提供3年原厂商售后维护服务，含软硬件维护和系统软件、规则库升级服务。 2.功能指标 （1）支持审计ORACLE、SQL Server、MY SQL、DB2、Sybase、Informix、Postgresql等各类主流数据库系统； （2）灵活的审计策略：支持基于IP地址、时间、用户/用户组、数据库用户名、数据库类型、数据库表名、字段名、关键字等组合审计策略，并实时告警响应； （3）支持同时审计多种数据库及跨多种数据库平台操作；支持实时审计用户对数据库系统所有操作；支持分析、提取SQL语句中绑定变量，并可完全监测还原SQL操作语句包括源IP地址、目的IP地址、访问时间、MAC地址、数据库用户名、客户端类型、数据库操作类型、数据库表名等； （4）审计对象包括网页浏览、网络言论、电子邮件、即时通讯、文件传输、服务器操作等； （5）支持集中管理，系统应提供专门的安全中心负责集中管理多台审计设备的审计事件的存储、分析；安全中心支持基于IP地址、时间、用户名、数据库操作类型、操作命令、数据库名、数据表名、字段名、关键字等条件的审计日志搜索查询分析； （6）支持HTTP网页浏览及关键字搜索审计：记录用户网站访问行为包括源IP地址、目的IP地址、访问时间、URL、网页浏览时间等，并提供网页还原功能； （7）本次投标产品绿盟安全审计系统：支持电子邮件审计：支持SMTP、POP3、WEBMAIL等协议，支持基于邮箱地址、邮件主题、邮件内容、附件名的关键字审计功能；可记录邮箱地址、邮件主题、邮件内容、邮件附件、源IP地址、目的IP地址等信息；邮件附件格式支持DOC、PDF、ZIP、RAR、TXT、html、htm、office等；也可以无条件完全记录所有邮件内容和附件； （8）支持基于论坛主题、发帖内容的关键字审计功能；支持基于用户/用户组、时间、关键字等多种组合审计策略，可记录源IP地址、目的IP地址、发帖论坛、发帖人、主题、发帖时间、发帖内容等，并提供内容还原功能； （9）支持文件传输审计：支持HTTP、FTP协议，支持基于用户/用户组、时间、关键字等多种组合审计策略，用户可自定义下载文件类型，对文件上传、下载类型进行审计，可记录日志包括源IP地址、目的IP地址、时间、传输文件名等； （10）支持TELNET、FTP等业务操作进行命令级审计，支持基于IP地址、用户组、时间、关键字等组合审计策略。TELNET：可记录源IP地址、目的IP地址、帐号、和命令等；FTP：可记录源IP地址、目的IP地址、帐号、命令及上传下载文件名等； （11）支持IPv6协议，可识别IPv6协议的数据流，支持基于IPv6地址格式的审计策略，支持IPv6网络流量审计； （12）支持用户身份信息智能关联技术，可将用户各种身份信息与其终端IP地址进行智能关联形成用户身份信息库，从而提高事件定位的精确度； （13）用户信息来源可基于邮件用户、第三方认证用户、即时通讯用户、远程登陆用户、网站登录用户、数据库用户等；用户认证可支持AD、Radius、LDAP、EPS等认证； （14）时间对象类型可支持基于每天、每个工作日、每周、每月进行设置； （15）日志分析功能：内容审计日志可支持基于时间范围、事件类型、级别、源地址、目的地址、源MAC、目的MAC、源端口、目的端口、用户、关联用户、URL、站点、标题、接口等进行分析；数据库审计日志可支持时间范围、子类型、级别、源地址、目的地址、源MAC、目的MAC、源端口、目的端口、用户、关联用户、接口、登陆用户、客户端、SQL语句进行分析； （16）运行日志查询条件包括：时间范围、日志类型、日志级别、日志内容等进行查询； （17）基于B/S的管理架构，灵活方便，适合在任何IP可达地点远程管理； （18）支持带外管理（OOB）功能，可以通过专用管理口，进行引擎管理，解决远程应急管理的需求； （19）支持历史版本回滚功能，系统内建历史版本库，可保留最近升级的两个历史版本，并支持回滚到任一历史版本，提高产品升级过程的可靠性； （20）提供丰富的响应方式，包括：丢弃数据包、阻断会话、邮件报警、短信报警、控制台显示、日志数据库记录、写入XML文件，运行用户自定义命令等，满足用户各种响应需求； （21）提供标准snmp trap、snmp agent（v1、v2c、v3）和syslog接口，可接受第三方管理平台的集中事件管理； （22）提供实时在线升级、离线升级多种升级方式。在线升级包括立即升级和定时升级。 3.其他 （1）所投产品绿盟安全审计系统V5.6具有中华人民共和国公安部的《计算机信息系统安全专用产品销售许可证》； （2）所投产品生产厂家北京神州绿盟科技有限公司在信息安全领域有着丰富的经验与先进的技术，具备对操作系统、应用系统或网络设备的漏洞进行发现、验证的能力，生产厂家自己发现的安全漏洞超过30个，并在CVE官网上能查询到相关漏洞信息（供货时提供CVE官方链接以及查询结果截图并加盖生产厂家公章）； （3）所投产品生产厂家北京神州绿盟科技有限公司为OWASP应用安全联盟成员之一（供货时提供证明材料并加盖生产厂家公章）； （4）所投产品生产厂家北京神州绿盟科技有限公司具备国家信息安全服务（安全开发类）二级及以上资质（供货时提供有效资质证书复印件或相关证明材料并加盖生产厂家公章）； （5）为保障安全运维能力，所投产品生产厂家北京神州绿盟科技有限公司具备CCRC信息系统安全运维一级服务资质（供货时提供有效证明材料并加盖生产厂家公章）。 30.供货时提供所投产品生产厂家北京神州绿盟科技有限公司广西当地办事处的国家计算机网络应急技术处理协调中心提供的漏洞研究证明（CNVD）证书复印件并加盖生产厂家公章。 | 108730 | 217460 |
| 漏洞扫描 | 3台 | 北京 | 绿盟、北京神州绿盟科技有限公司 | 型号RSASNX3-E-X60，参数如下： 1.性能指标 （1）产品采用2U标准19"机架式硬件平台，具有6个100/1000M电口工作口，4个SFP光口（含SFP多模光模块），具有一个专用RJ45配置串口，硬盘容量1TB； （2）产品支持IPv4和IPv6的不同协议部署，最大并发扫描主机数90个IP，最大并发任务数15；配置系统漏洞扫描功能，配置Web应用扫描模块，对Web应用提供专业的漏洞、挂马检测和分析；授权可扫描总数量为无限的IP地址或域名，提供4路端口扫描授权； （3）提供产品原生产厂家的3年免费售后服务，免费售后维护服务含软硬件维护和系统软件、规则库、特征库升级服务。产品的安装、培训由原厂商工程师完成实施，并提供原厂商工程师的现场技术支持。 2.功能指标 （1）支持多路扫描功能，可以同时对多个隔离业务子网进行扫描； （2）支持扩展web漏洞扫描功能，并对漏洞扫描可输出同时包含漏洞扫描结果的报表； （3）支持以资产为中心的风险扫描和风险分析； （4）支持先通过调用通用扫描插件，然后识别目标设备的操作系统类别，将相应的扫描插件加载到内存中进行调用，从而提高扫描插件加载速度； （5）支持检测的漏洞数180000条； （6）支持采用SMB、SSH、RDP、Telnet、HTTP/HTTPS、WinRM等协议对被检查设备进行登录扫描； （7）支持通过多种维度对漏洞进行检索，包括：CVE ID、BUGTRAQ ID、CNCVE ID、CNVD ID、CNNVD ID、MS编号、风险等级、漏洞名称、是否使用危险插件、漏洞发布日期等信息； （8）支持将符合筛选条件的漏洞自动加入到自定义漏洞模板中，及后续插件升级包中的漏洞也可以自动加入到模板中； （9）支持自动模板匹配，能够自动识别扫描对象类型，针对对象类型匹配不同的漏洞模板，如Unix、Linux、Windows操作系统，网络设备等模板； （10）支持扫描国产操作系统、应用及软件的安全漏洞，如红旗、麒麟、起点操作系统； （11）支持针对大数据组件框架的漏洞检测； （12）支持专门针对DNS服务的安全漏洞检测，包括DNS投毒等漏洞检测能力；支持“幽灵木马”检测； （13）支持专门针对已有攻击利用代码的漏洞检测，检测用户资产是否存在可利用的漏洞； （14）支持Oracle、MySQL、MS SQL、DB2、Sybase数据库漏洞检查； （15）具备单独口令猜测扫描任务，支持多种口令猜测方式，包括利用SMB、TELNET、FTP、SSH、POP3、TOMCAT、SQL SERVER、MYSQL、ORACLE、SYBASE、DB2、SNMP等协议进行口令猜测，允许外挂用户提供的用户名字典、密码字典和用户名密码组合字典； （16）支持扫描时间段控制，只在指定时间段内执行任务，未完成任务在下一时间段自动继续执行； （17）支持复用已有任务配置用于新的扫描任务； （18）每半个月进行一次漏洞库升级； （19）具有标准的数据接口支持，方便与第三方安全产品或管理平台进行数据采集和调用； （20）支持通过资产树对资产进行分级管理，支持设备权重和等保级别设置，可在资产树上直接指定主机开展扫描任务； （21）支持风险告警和风险闭环处理，可在集中告警平台灵活配置告警方式、告警条件、告警资产范围等，支持单个或批量修改风险状态； （22）支持通过仪表盘直观展示资产风险值、主机风险等级分布、资产风险趋势、资产风险分布趋势等内容，并可查看详情； （23）支持在线报表，在线查看展示各节点和主机资产风险分布、漏洞分布、配置合规和脆弱账号信息，在线查看设备风险详情； （24）支持按IP范围、起止时间、任务名称、任务状态、漏洞模板、用户等筛选扫描任务，并对筛选结果进行汇总，和生成在线及离线报表； （25）支持实现显示扫描结果，包括扫描进度、主机存活数、预计扫描时间、漏洞风险信息等。 3.产品资质及其他 （1）所投产品绿盟远程安全评估系统V6.0具有中华人民共和国公安部的《计算机信息系统安全专用产品销售许可证》； （2）所投产品生产厂家北京神州绿盟科技有限公司在信息安全领域有着丰富的经验与先进的技术，具备对操作系统、应用系统或网络设备的漏洞进行发现、验证的能力，生产厂家自己发现的安全漏洞超过30个，并在CVE官网上能查询到相关漏洞信息（供货时提供CVE官方链接以及查询结果截图并加盖生产厂家公章）； （3）所投产品生产厂家北京神州绿盟科技有限公司为OWASP应用安全联盟成员之一（供货时提供证明材料并加盖生产厂家公章）； （4）所投产品生产厂家北京神州绿盟科技有限公司具备国家信息安全服务（安全开发类）二级及以上资质（供货时提供有效资质证书复印件或相关证明材料并加盖生产厂家公章）； （5）为保障安全运维能力，所投产品生产厂家北京神州绿盟科技有限公司具备CCRC信息系统安全运维一级服务资质（供货时提供有效证明材料并加盖生产厂家公章）； （6）供货时提供所投产品生产厂家北京神州绿盟科技有限公司广西当地办事处的国家计算机网络应急技术处理协调中心提供的漏洞研究证明（CNVD）证书复印件并加盖生产厂家公章。 | 133980 | 401940 |
| 防病毒及主机安全 | 1套 | 成都 | 亚信安全、亚信科技(成都)有限公司 | 型号Deep Security 10.0 AV，参数如下： 1.提供204颗物理CPU的授权和20个客户端授权，3年维保升级服务。 2.支持VMWARE、华为、华三、Citrix、其它KVM等虚拟化平台采用无代理部署方式，不需要在Windows虚拟机上安装客户端程序，跟传统防病毒相比，能减少对系统资源（CPU、内存、磁盘、网络）的利用率。 3.满足所有本期扩容新增的云虚拟主机、宿主服务器的防病毒及主机安全加固。产品支持Windows各操作系统平台，包括Windows XP（32/64Bit）Windows Server 2003 R2 SP2（32/64Bite）Windows 7 （32/64Bit）Windows Server 2008（32/64Bit）Windows Server 2008 R2 64、Windows 8（32/64Bit）Windows 8.1（32/64Bit）Windows 10（32/64Bit）Windows Server 2012（64Bit）Windows Server 2012 R2（64Bit）Windows Server 2016（64Bit）Windows Server 2019（64Bit）。支持Linux操作系统，包括Red Hat Enterprise Linux、CentOS Linux、Oracle Linux、SUSE Linux、Ubuntu Linux、Debian Linux、Cloud Linux、Amazon Linux、中标麒麟、银河麒麟、普华Linux、华为欧拉、中兴Linux等。 4.支持防恶意程序和Web信誉，可以阻止用户访问恶意Web站点。 5.控制台可独立完成管理、升级功能，并针对内网客户提供独立升级代理工具。 6.控制台首页可展示：登录用户摘要、所防护计算机状态、升级情况、登录历史记录等。支持不同账户通过添加\删除Widget方式自定义首页内容来提供运维效率。可根据目前流行攻击类型（如：勒索病毒）在首页提供专项展示。 7.控制台提供110多种类型告警事件类型，并且可通过SMTP发送告警信息给指定运维人员。并且支持基于分组或者计算机进行过滤。 8.为了保证管理服务连续性，产品支持HA高可用：支持控制台高可用，用于故障恢复及转移；产品支持数据（SQL-Serve、Oracle）集群，用于恢复。 9.支持分别配置实时扫描、手动扫描和预设扫描、恶意软件扫描；支持不同类型的恶意软件配置不同处理动作；支持配置实时扫描生效时间段。 10.支持扫描嵌入式Microsoft Office 对象配置；支持扫描例外配置进程镜像文件列表；持可疑文件外发沙盒模块分析。 11.检查可疑活动和未授权的更改（包括勒索软件），并提供备份、恢复勒索软件加密的文件。 12.支持Web信誉支持配置打开/关闭Web信誉，支持设置Web信誉安全级别，包括高、中和低，支持配置阻止未经安全测试的页面。 13.支持Web信誉支持配置监控的Web页面端口、Web页面链接，配置阻止Web页面是否显示本地通知，配置阻止Web页面是否触发警报。 14.产品支持更新的多级部署，分流冗余节省带宽，更新速度快。 15.产品支持自定义升级某一个或者某一些客户端的病毒码，而不是只能一次升级所有客户端的病毒码。 | 490661 | 490661 |
| 云租户安全资源池 | 2套 | 深圳 | 深信服、深信服科技股份有限公司 | 型号安全资源池，参数如下： 1.安全资源池硬件平台 （1）服务器参数：规格：采用2U机架式服务器，CPU：配置2颗Silver 4214R 2.40 GHz可扩展处理器，每颗处理器主频2.40G，内核数12，内存：配置4条32GB DDR4 2666内存，系统盘：配置1块128GB SATA SSD，缓存盘：配置1块480GB硬盘，数据盘：配置2块2TB硬盘，标配盘位数：8，电源：冗余电源，接口：6千兆电口+2万兆光口。总共5台服务器，包含三年软件升级、规则库升级、硬件维保； （2）交换机：24个10G SFP+万兆光口，24个SFP千兆光口，2个40GE QSFP+光口；交换容量2.56Tbps/23.04Tbps，包转发率720Mpps，支持全端口线速转发；支持NAC统一管理、统一查看状态、VLAN等配置管理；支持终端识别、终端准入、安全防护及安全画像可视；支持胖瘦一体化；配置双电源模块。3年硬件保修服务； （3）CDN交换机：型号：星融元 NX306P-48S-AC-3Y-1PD，接口：6×100G QSFP28，48×10G SFP+，220V交流1+1，风扇3+1；3年保修服务；提供的硬件能支撑并满足安全资源池及组件的使用； （4）软件系统可以部署在裸金属架构上，无需绑定操作系统即可搭建云安全服务平台；平台虚拟化内核采用基于KVM底层开发，云安全服务平台和国内主流云平台实现解耦合，适用于Vmware、华为云、华三云、阿里云、国云Gcloud等国内主流云平台； （5）具备关键安全组件双机功能，保障安全组件高可用，具备虚拟机卡死及蓝屏的检测功能并实现自动重启，无需人工干预减少运维工作量； （6）平台具备安全需求弹性扩展，安全灵活部署，按需交付。安全功能以基于不同安全需求以安全组件的形式交付； （7）具备单级部署，无需安装任何其他软件和专用设备硬件，采用基于X86服务器即可完成平台部署，采用旁路部署模式，可以通过策略路由实现流量牵引； （8）可根据实际业务环境定义业务安全区域，包括运维管理区域、对外发布区域、出口边界区域、服务器区域等，简化运维管理。 2.基础授权 （1）安全组件资源120个授权，组件内容包括下一代防火墙、IPS、WAF和数据库审计、网页防篡改、日志审计等；各类型组件的数量可依据业务需求进行配置，包含安全组件三年软件升级、规则库升级： 1）下一代防火墙组件提供基本的安全防御，包括但不限于4～7层访问控制、入侵防御、病毒过滤、网页防篡改等安全功能； 2）下一代防火墙组件支持无特征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）下一代防火墙组件支持抵御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； 4）IPS组件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； 5）IPS组件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； 6）IPS组件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； 7）WAF组件支持网站防篡改功能，可防止攻击者非授权篡改文件系统。支持网页恶意链接检测功能，有效识别网页盗链/黑链的行为，避免用户网页资源被滥用； 8）WAF组件支持自定义Web应用防护规则，通过基于正则表达式自定义规则匹配方向、动作、字符串、危险等级、动作、攻击影响、描述等； 9）数据库审计组件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； 10）数据库审计组件支持吞吐量分析，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； 11）网页防篡改资源，支持主流Windows和linux系统，一个授权支持防护一台服务器（不能超过5个目录），通过文件底层驱动技术对Web站点目录提供全方位的保护，防止黑客、病毒等对目录中的网页、电子文档、图片、数据库等任何类型的文件进行非法篡改和破坏：提供自我保护机制，网页防篡改客户端需有第三方认证码方可卸载；同时支持防护模式和监控模式两种模式的防篡改模式；系统支持在断线情况下对网页文件目录的防护功能；应支持文件多线程同步，并可以设置文件空闲同步时间周期、发布时间周期等设置；应采用基于文件过滤驱动保护技术、事件触发机制相结合方式的网页防篡改功能；支持各类网页文件的保护，包括静态和动态网页以及各类文件信息；支持对指定文件夹以及子文件夹的保护，避免上传非法文件及木马等恶意文件或插入恶意代码；支持日志超出阈值告警，可设定日志存储空间；同时支持数字水印及文件驱动过滤两种篡改检测技术； 12）日志审计资源，系统通过监测及采集信息系统中的系统安全事件、用户访问行为、系统运行日志、系统运行状态等各类信息，经过规范化、过滤、归并和告警分析等处理后，以统一格式的日志形式进行集中存储和管理，结合丰富的日志统计汇总及综合分析功能，实现对信息系统整体安全状况的全面审计：系统从不同设备或系统中所获得的各类日志、事件中抽取相关片段准确和完整地映射至安全事件的标准字段；对安全事件重新定级。能根据统一的安全策略，按照安全设备识别名、事件类别、事件级别等所有可能的条件及各种条件的组合对事件严重级别进行重定义；系统既可以完全收集采集对象上的日志信息，也支持在安全事件收集引擎上设置过滤条件，可过滤出无关安全事件，满足根据实际业务需求减少采集对象发送到核心服务器的安全事件数，从而减少对网络带宽和数据库存储空间地占用；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、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】；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】；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；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。 | 853864 | 1707728 |
| 数据安全交换平台 | 1套 | 北京 | 科博、中铁信安（北京）信息安全技术有限公司 | 型号CopSDP-WF/WB和CopGap200-T10000，参数如下： 1.整体配置 （1）科博安全数据交换平台是由3套万兆前后置代理系统（科博安全数据交换系统）和2台万兆双向网闸（科博安全隔离与信息交换系统COPGAP200）组成。 （2）前后置代理系统与双向网闸组成跨网数据交换系统，具备有中国软件测评中心出具的功能测试报告。 2.前后置代理系统 我公司投标产品科博安全数据交换系统是由一台前置安全代理系统和一台后置安全代理系统组成，技术参数如下： （1）系统架构：采用2U机架式专用服务器及安全加固操作系统。前后置硬件配置2.4G志强六核64位处理器；32G内存；6块900G企业级硬盘，专用RAID阵列卡；4个千兆电口，4个万兆光口。 （2）协议支持：我公司投标产品科博安全数据交换系统支持标准协议支持：支持POP3、SMTP邮件传输协议；支持FTP等文件传输协议；支持HTTP/HTTPS等Web传输协议；支持HTTP应用改写功能，适应各种不同Web应用场景；支持单通道同时容纳多个Web应用的能力；支持WebService传输协议。扩展协议支持：支持基于TCP、UDP协议的非标准应用协议；支持专用的HTP安全传输协议；提供用户自定义应用的开发和支持。 （3）服务调用摆渡支持：我公司投标产品科博安全数据交换系统支持基于WebService、HTTP协议的服务调用模式；服务调用模式在跨网隔离交换系统内部采用文件同步实现。 （4）个人文件传输：我公司投标产品科博安全数据交换系统支持内外网用户的双向个人文件交换，包括从内到外和从外到内；支持C/S模式客户端发送和接收功能；支持个人文件的人工审核功能；支持用户及多级部门管理功能；支持用户导入导出功能；支持用户及部门的排序和移动功能；支持客户端用户路径和自启动设置功能；支持客户端用户的个人文件接收提醒功能；支持服务端传输日志查看功能；支持用户将同一文件发送给多个用户的功能；支持与第三方用户管理系统联动，实现统一用户管理。 （5）应用文件传输：我公司投标产品科博安全数据交换系统支持支持基于FTP、SCP、SFTP、Samba等方式的文件同步；支持对文件及目录的同步，目录层次没有限制，文件大小没有限制；支持同一个目录的文件双向同步；支持备份、复制及移动传输模式；提供内置FTP服务，使外网到内网的文件交换更为快捷；提供内置SAMBA服务，使外网到内网的文件交换更为方便快捷；支持主动传输模式（拉模式）、被动传输模式（推模式）及混合传输模式；提供专有的外置程序，实现高效文件同步功能。 （6）数据库同步：我公司投标产品科博安全数据交换系统支持同构和异构数据库同步功能；支持基于向导式的数据库同步任务配置；支持Oracle（8i、9i、10g、11g）数据库同步；支持SQLServer（2000、2005、2008）数据库同步；支持DB2（V9）及以上数据库同步；支持MySql（V5）及以上数据库同步；支持达梦数据库同步；支持神舟通用数据库同步；支持南大通用数据库同步；支持人大金仓数据库同步；支持数据库单向全量及增量同步；支持数据库双向全量及增量同步；支持字段级数据库同步；支持一对多数据库同步；支持基于特定值触发的数据库同步功能；支持数据库同步冲突处理机制。 （7）对云平台的支持：我公司投标产品科博安全数据交换系统支持云平台HDFS分布式文件同步；支持云平台HBASE分布式数据库同步。 （8）音视频协议支持：我公司投标产品科博安全数据交换系统支持音视频信令双向交换；支持音视频数据流单向传输；支持国际主流视频控制协议SIP、H323、RTSP、RTMP、HLS（HTTP Live Streaming）；支持GB/T28181-2011<<安全防范视频监控联网系统信息传输、交换、控制技术要求>>、GB/T28181-2016<<公共安全视频监控联网系统信息传输、交换、控制技术要求>>标准规定的音视频协议；支持与市面常见的音视频信息系统对接。 （9）访问控制：我公司投标产品科博安全数据交换系统支持对客户端IP/MAC进行过滤检查；支持基于五元组（源地址、源端口、目的地址、目的端口、协议）的访问控制机制；支持对应用访问时间进行控制。 （10）Web协议过滤：我公司投标产品科博安全数据交换系统支持URL长度及关键字过滤；支持标准协议命令过滤；支持协议数据返回类型过滤；支持协议内容还原安全检查；支持协议内容还原病毒查杀。 （11）邮件协议过滤：我公司投标产品科博安全数据交换系统支持邮件发件人及收件人过滤；支持邮件标题及主体内容过滤；支持邮件附件大小和类型控制；支持邮件附件关键字检查；支持邮件附件病毒防护。 （12）FTP协议过滤：我公司投标产品科博安全数据交换系统支持对访问用户过滤；支持标准协议命令过滤；支持文件内容过滤、文件格式深度检查功能；支持文件病毒扫描功能。 （13）WebService协议过滤：我公司投标产品科博安全数据交换系统支持标准协议命令过滤；支持IP绑定认证及专有服务接口认证；支持SOAP函数名过滤，支持函数参数检查；支持对请求内容及响应内容进行检查。 （14）音视频安全过滤：我公司投标产品科博安全数据交换系统支持对信令命令的检查过滤功能，包括标准音视频协议命令及扩展的控制操作命令、回放控制命令、设备控制命令、设备查询命令等；支持对信令消息体的检查过滤功能；支持音频编码格式的检查过滤功能；支持视频编码格式的检查过滤功能。 （15）文件传输控制：我公司投标产品科博安全数据交换系统支持内容过滤、文件格式深度检查功能；支持文件病毒扫描功能；支持个人文件的人工审核功能；支持文件发送接收传输通道加密功能；支持个人文件在服务器端的存储加密功能；支持个人文件在接收时自动解密功能；支持客户端用户个人发送接收日志查看功能；支持客户端用户密码修改功能；个人用户在登录个人文件传输客户端时，支持通过USB Key进行身份认证。 （16）安全管理：我公司投标产品科博安全数据交换系统支持B/S模式安全管理（HTTPS）、SSH、串口管理。 （17）分权管理：我公司投标产品科博安全数据交换系统支持不同管理员不同角色的分权管理机制，实现互相制约，互相审计。 （18）日志管理：我公司投标产品科博安全数据交换系统提供详尽的日志功能；提供对日志数据丰富的审计功能；提供日志信息的加密存储功能。支持与第三方日志系统对接，实现基于syslog、snmp的日志推送。 （19）双机热备：我公司投标产品科博安全数据交换系统支持双机热备，主设备出现故障时，从设备迅速接替工作，保证业务持续性。 （20）网口聚合：我公司投标产品科博安全数据交换系统支持平衡轮循环策略、主备份策略、平衡策略、广播策略、动态链路聚合、适配器传输负载均衡和适配器适应性负载均衡七种聚合模式。 （21）我公司投标产品科博安全数据交换系统具备公安部颁发的有效期内的销售许可证。 （22）我公司投标产品科博安全数据交换系统具备计算机软件著作权登记证书。 （23）我公司投标产品科博安全数据交换系统提供软硬件3年的维护及更新服务。 3.双向网闸 我公司投标产品科博安全隔离与信息交换系统COPGAP200与投标产品科博安全数据交换系统均为同一厂商同品牌产品，确保两者之间无缝耦合，可实现整体可信，保证了跨网数据交换系统稳定性及性能。 （1）系统结构：科博安全隔离与信息交换系统COPGAP200采用“2+1”结构，内外端机都采用安全的LINUX操作系统，内外端机之间采用FPGA隔离卡及光纤线路连接。" （2）我公司投标产品科博安全隔离与信息交换系统COPGAP200采用标准机架式服务器架构标准2.5U设备，硬件配置CPU：Xeon 3.3GHz（4核）×2；内存：64；硬盘：1TB×2；8个千兆电口，4个万兆光口； （3）专有协议通信：我公司投标产品科博安全隔离与信息交换系统COPGAP200设备内外端之间不允许有任何TCP/IP等网络协议，在采用专用隔离卡的基础上，使用API进行原始数据交换，支持各类上层应用的数据摆渡。 （4）协议支持：我公司投标产品科博安全隔离与信息交换系统COPGAP200支持常见的HTTP/HTTPS、POP3/SMTP、FTP、WebService等网络应用协议；支持标准TCP、UDP协议；提供用户自定义应用的开发和支持。 （5）文件同步：我公司投标产品科博安全隔离与信息交换系统COPGAP200支持文件同步功能，支持基于FTP/SCP/SFTP/SAMBA等方式的文件同步，支持对多个文件的同步，同步目录层数没有限制，支持移动、复制、备份等同步方式。 （6）数据库同步：我公司投标产品科博安全隔离与信息交换系统COPGAP200支持数据库同步功能，支持同构和异构数据库同步功能；支持常见关系型数据库（Oracle、SQLServer、DB2、MySql）同步，支持数据库单向、双向、增量及全表同步；支持字段级、表级同步，提供数据库同步冲突解决方案。 （7）访问控制：我公司投标产品科博安全隔离与信息交换系统COPGAP200支持对客户端IP/MAC进行过滤检查；支持基于五元组（源地址、源端口、目的地址、目的端口、协议）的访问控制机制；支持对应用访问时间进行控制。 （8）协议过滤：我公司投标产品科博安全隔离与信息交换系统COPGAP200支持对标准应用协议的命令、协议数据进行审查和控制。 （9）文件传输控制：我公司投标产品科博安全隔离与信息交换系统COPGAP200支持文件内容过滤、文件格式深度检查功能及病毒扫描功能。 （10）密码控制：我公司投标产品科博安全隔离与信息交换系统COPGAP200支持密码控制，客户端身份认证支持国密SM2、SM3、SM4算法，提供双向认证机制；支持客户端文件传输国密算法加密。 （11）专有安全通道：我公司投标产品科博安全隔离与信息交换系统COPGAP200提供私有安全通信协议支持，实现网闸与前后置服务器之间双向身份认证及数据通信加密，构建前后置加网闸的可信体系。 （12）病毒防护：我公司投标产品科博安全隔离与信息交换系统COPGAP200支持病毒防护选配的防病毒模块能对来往应用数据进行病毒查杀。 （13）安全管理：我公司投标产品科博安全隔离与信息交换系统COPGAP200支持B/S模式安全管理（HTTPS）、SSH、串口管理。 （14）分权管理：我公司投标产品科博安全隔离与信息交换系统COPGAP200支持不同管理员不同角色的分权管理机制，实现互相制约，互相审计。 （15）日志管理：我公司投标产品科博安全隔离与信息交换系统COPGAP200提供详尽的日志功能；提供对日志数据丰富的审计功能；提供日志信息的加密存储功能。支持与第三方日志系统对接，实现基于syslog、snmp的日志推送。 （16）双机热备：我公司投标产品科博安全隔离与信息交换系统COPGAP200支持双机热备，主设备出现故障时，从设备迅速接替工作，保证业务持续性。 （17）集群负载：我公司投标产品科博安全隔离与信息交换系统COPGAP200具备自负载功能，无需使用第三方负载均衡设备。支持多台设备集群提升平台性能。 （18）国产化支持：我公司投标产品科博安全隔离与信息交换系统COPGAP200个人文件传输客户端支持中标麒麟等国产化操作系统。 （19）接口：我公司投标产品科博安全隔离与信息交换系统COPGAP200配置8个千兆电口，4个万兆光口； （20）通讯带宽：我公司投标产品科博安全隔离与信息交换系统COPGAP200通讯带宽：9Gbps。 （21）访问延时及并发：我公司投标产品科博安全隔离与信息交换系统COPGAP200应用访问延时6ms，并发连接数20万； （22）我公司投标产品科博安全隔离与信息交换系统COPGAP200具备公安部颁发的有效期内的销售许可证。 （23）我公司投标产品科博安全隔离与信息交换系统COPGAP200具备计算机软件著作权登记证书。 （24）我公司投标产品科博安全隔离与信息交换系统COPGAP200具备国家保密局科技测评中心颁发的有效期内的涉密信息系统产品检测证书。 （25）我公司投标产品科博安全隔离与信息交换系统COPGAP200具备国家密码管理局颁发的有效期内的密码检测证书。 （26）我公司投标产品科博安全隔离与信息交换系统COPGAP200的原厂商具备质量管理体系应符合GB/T19001-2016/ISO9001：2015标准； （27）我公司投标产品科博安全隔离与信息交换系统COPGAP200提供软硬件3年的维护及更新服务。 | 1290947 | 1290947 |
| 云平台 | 1套 | 济南 | 浪潮、浪潮云信息技术股份公司 | 为本项目配置云平台1套，采用浪潮云ICP平台，型号浪潮云ICP平台V3.0，参数如下：  1.云平台具备功能  （1）平台架构  1）虚拟化平台采用Openstack+KVM的虚拟化技术路线，具有成熟、稳定和开放的特点；  2）平台组件和产品管理组件均采用容器部署架构，通过Kubernetes进行统一管理，实现自动化安装、快速升级，保证架构的灵活高效。  （2）平台兼容性  1）支持X86和ARM架构资源统一管理，支持通过同一套虚拟化平台进行统一调度；  2）云平台具有高度适配能力和兼容性，支持飞腾、鲲鹏等多品牌CPU；  3）云平台支持基于统信UOS、银河麒麟、中标麒麟等国产操作系统部署。  （3）平台开放性  云平台提供统一的标准接口，包含但不限于虚拟化平台、运营管理平台、运维管理平台、服务产品等标准接口，具备与云监管部门和第三方平台对接的能力。  （4）平台生命周期管理  云平台软件为稳定可靠的最新商用版本，同时要支持平台及服务产品版本自动化升级、部署、回滚。  （5）R版本兼容性认证  云平台通过OpenStack兼容性认证，提供R版本的OpenStack云平台，以降低平台漏洞数量、保障系统可靠性。  （6）云计算解决方案引领级  云平台通过电子标准化院云计算解决方案引领级认证，保证平台的先进性、稳定性和可靠性。  （7）授权  提供云平台授权数160个节点，按照云平台所有管理的计算设备、存储设备、管理设备物理节点之和计算。  2.虚拟化管理  （1）虚拟化资源管理  1）支持对资源池vCPU、内存、磁盘等虚拟化资源总量和使用量的监控，支持对每台宿主机资源vCPU、内存、磁盘等资源的总量、使用量、实例数量的监控；  2）支持对资源池宿主机进行管理，支持宿主机关闭服务功能，支持对已关闭的宿主机上的虚拟机进行疏散；  3）支持主机聚合管理，支持在主机聚合中添加、移除计算节点；  4）支持虚拟机镜像导入功能，镜像类型包括ISO、OVA、QCOW2、PLOOP-Virtuozzo、VDI、VHD、VMDK、AKI-Amazon、AMI-Amazon、ARI-AmazonRamdisk、Docker等；镜像权限可设置为公有、私有两种类型；  5）提供虚拟机实例的生命周期管理，主要包括虚机实例的创建、开启、关闭、编辑实例名称、调整实例大小、暂停实例、挂起实例、废弃实例、锁定实例、删除实例、重建实例、软/硬重启、接口分离/连接、绑定和解绑浮动IP等功能；  6）支持用户快速定位虚拟机功能，可以支持按照虚拟机名称、IP、ID、镜像名称、运行状态、实例类型名称等多种方式快速定位虚拟机；  7）支持虚拟机创建均衡分布算法和亲和性策略，能够实现不同物理主机分布扩展虚拟机；  8）虚拟机之间能做到隔离保护，当一个虚拟机发生故障不会影响同一个物理机上的其它虚拟机运行，每个虚拟机上的用户权限只限于本虚拟机之内，以保障云平台的安全性；  9）支持根据应用系统的性能需求，灵活调整虚拟机的资源配置，包括调整vCPU个数，内存大小，磁盘卷个数，扩展磁盘卷的容量等；  10）提供虚拟机热迁移功能，虚拟机支持在使用同一共享存储的宿主机之间迁移，迁移的过程不影响用户使用；  11）支持虚拟机重建功能，通过镜像/快照重建虚拟机；  12）虚拟机数据盘支持跨存储迁移功能，适用于不同存储之间、同一存储不同介质之间的离线迁移；  13）平台资源不足时支持动态增加物理服务器扩展云平台资源，新增物理服务器资源被自动识别，并加入到平台的资源池中，扩展过程对平台业务无影响；  14）支持虚拟CPU与物理服务器CPU比例配置；支持虚拟内存与物理服务器内存比例配置；  15）支持创建虚拟机时指定网络、IP地址和允许/禁止的端口，支持未开启DHCP协议场景使用指定IP地址配置虚拟机；  16）支持虚拟机配置NUMA，解决CPU资源分布不均衡可能引起的性能瓶颈，支撑海量高负载数据运算；  17）支持虚拟机配置大页内存，降低缺页中断数，提高TLB命中率，提高计算性能；  18）支持虚拟机CPU和宿主机CPU绑定，宿主机可灵活配置供虚拟机绑定的CPU；  19）支持GPU透传及GPU虚拟化，虚拟机可使用宿主机物理GPU或使用vGPU，支持主流GPU卡Nvidia T4/P40，提供多种类型配置。  （2）虚拟存储资源管理  1）为了满足不同的存储类型需求，支持对块、文件、对象三种存储类型的统一管理；存储资源池单盘IOPS指标1000；  2）平台支持分布式存储和集中存储两种存储架构，具备为数据提供多份副本（不少于三副本）或冗余磁盘阵列的功能，支持基于副本数据进行还原操作；  3）支持扩展、分离数据存储，支持硬盘和存储节点的离线/在线扩展和分离；  4）支持卷的生命周期管理，包括创建、删除、容量扩展、创建快照、数据备份、修改卷类型、挂载和分析、跨项目转让功能；卷的创建支持指定卷来源为空白卷、快照、镜像、卷等，支持指定卷类型、卷大小、可用域等；  5）避免集群单点故障，管理层支持冗余设计，分布式存储采用多Master设计，有3个及以上的存储Master控制节点；  6）分布式存储支持数据传输过程中的用户鉴权处理，保证数据传输安全性。  （3）虚拟网络资源管理  1）核心骨干设备、出口设备、骨干线路等支持冗余备份，云内骨干线路带宽40Gb，服务器业务带宽10Gb×2，核心骨干设备满足无缝扩容需求；  2）云平台划分独立的业务网络、存储网络、服务产品管理调度网络、宿主机运维网络、物理节点带外管理网络等，不同网络之间逻辑隔离；业务网络和存储网络采用万兆冗余链路；  3）支持大二层架构组网，虚拟机具备二层迁移能力；  4）提供网络虚拟化功能，实现集中化网络控制和按需管理，具备弹性扩展能力，支持自动化网络部署；  5）支持为指定项目创建虚拟网络，网络类型支持Local、Flat、VLAN、GRE、VXLAN、Geneve等；支持配置共享网络为不同项目所共用；支持同一虚拟网络下创建多个虚拟子网；  6）具有虚拟路由功能，支持为虚拟路由器配置普通路由规则，支持自定义策略路由功能；  7）支持为指定端口绑定IP/MAC地址，降低ARP欺骗的风险；  8）支持网络拓扑管理功能，通过拓扑自定义网络结构，创建路由、创建网络和虚拟机实例；  9）具备流量编排能力，支持透明服务链技术，可实现虚拟网元业务的东西向和南北向引流功能；  10）提供虚拟安全组功能，支持根据网络协议类型（如TCP、UDP、HTTP、HTTPS、IMAP、POP3等）流向、端口或端口范围、远端CIDR或远端安全组、以太网类型等创建访问控制策略；支持为虚拟机实例的不同虚拟接口配置不同安全组；  11）支持浮动IP管理，为指定虚拟实例接口绑定浮动IP，实现外部网络访问。  3.产品管理  （1）部署架构  产品和平台支撑组件均采用微服务架构部署，通过Kubernetes进行统一管理，具备微服务自主知识产权。  （2）部署安装  1）支持CI/CD管道，并提供部署和配置管理工具、Git库和代码检视管理系统、任务自动化工具、软件中心仓库，实现持续集成、持续测试以及持续交付；  2）部署过程中支持根据所选平台和服务产品版本自动计算所需的关联依赖组件，并动态选择介质文件进行自动在线部署，或输出离线安装包；  3）云平台部署过程支持动态根据环境信息自动生成定制化配置，无需运维人员主动维护相关配置。  （3）高可用  1）产品采用冗余架构部署，支持负载能力，包括无状态负载（Deployment）有状态负载（StatefulSet）任务（Job）定时任务（CronJob）等多种类型的应用负载管理，创建工作负载时允许创建特权容器，且支持YAML方式创建；  2）云平台使用的资源仓库采用高可用方式部署，避免单点故障。  （4）升级管理  1）支持服务产品离线和在线升级功能，支持通过远程仓库在线部署和升级平台服务产品；支持通过介质包完成离线部署和升级需求；  2）支持针对无状态负载（Deployment）和有状态负载（StatefulSet）进行升级，可以查看单个无状态负载（Deployment）和有状态负载（StatefulSet）的版本记录列表，选择某个历史版本可以回滚；  3）支持滚动、蓝绿、灰度发布策略，并支持自定义流量规则，可按照流量权重或复杂Header平滑切换流量，且可自助上/下线不同版本的应用。  4.运营管理  （1）自助服务  提供面向政务云租户（含用户）和政务云监管人员的统一接入门户，用户可自行登录服务门户使用平台提供的服务。  （2）多资源池接入  提供多资源池接入管理能力，支持将多资源池的资源进行统一管理和服务发放。  （3）服务目录  平台具备完善的服务目录，展示当前云中心服务目录中所有服务，并提供服务简介、规格说明、每种规格对应年服务费、快速申请功能，帮助用户正确的获取所需服务。  （4）业务流程  平台具备资源申请与审批业务流程，资源申请包括资源的申请、变更和注销，资源审批包括待办流程和已办流程。资源申请和审批均支持按申请单号、起止时间，申请单状态等条件查询。  （5）报表分析  平台具备报表分析功能，具体包括云服务统计分析、云服务器利用率统计等。云服务统计分析包括：业务办理统计、上云一级部门统计、各部门上云业务系统统计、部门年服务费统计和云服务年服务费统计等。云服务器利用率统计包括：CPU使用率（峰值/平均/谷值）、内存使用率（峰值/平均/谷值）、磁盘使用率和流量速率（发送/接收）等。  （6）费用统计  平台具备费用统计功能，按照服务目录中服务名称，逐条展示每个规格、每个实例的计费信息。报表包括服务名称、规格、实例名称、计费开始时间、单价、服务费金额；查询条件包括一级部门、二级部门、服务分类、服务名称、时间，并支持将查询出的费用统计信息导出至Excel。  （7）系统管理  平台具备系统管理功能，具体包括用户与角色（角色管理、用户管理、全局策略）、组织机构管理（组织类型管理、组织视角管理、组织结构规则维护、组织机构参数维护）、资源管理、日志管理和系统配置（系统配置、电子签名、协议管理）等。  （8）通知公告  平台具备通知公告功能，公告包括公告标题、发布部门和发布时间等；操作查看、编辑和删除；查询条件包括标题、公告时间等。  （9）项目维护  支持以项目的维度对资源进行申请和维护，查询条件包括：一级部门、二级部门和项目名称等。  （10）登录安全策略  基于安全性考虑，应对密码输入错误次数进行校验，如果连续输入密码错误次数超过限定次数账号将被锁定。  5.运维管理  （1）告警展现  支持按告警对象、级别、规则名称等查看告警事件。  （2）告警查询  支持按指定字段模糊查询告警、按指定字段排序告警以及配置告警列表展示字段。  （3）告警处理  支持用户更新告警级别、编辑告警备注、编辑告警经验。  （4）告警自定义  1）支持告警规则自定义，告警规则包括：告警名称、服务组件、告警级别、告警周期、推送终端、告警表达式、规则状态、告警短信提醒、详细描述、概要描述等；  2）支持告警规则的模糊、精确匹配。  （5）告警归并  提供重复告警的归并功能，即多条同源告警合并成一条告警呈现，提供告警的首次发生时间、最后发生时间、发生次数等信息。  （6）告警设置  支持设置告警级别、告警阈值能力，支持设置告警规则，有符合规则的告警，自动按照预置的告警级别进行告警。  （7）告警通知  支持短信、微信通知，以及按照告警规则的告警静默。  （8）资源监控  1）支持并提供物理资源、虚拟资源监测功能，实现管理层面、资源类别层面的多维度资源监控与管理；  2）支持并提供对计算资源、存储资源、网络资源的性能及运行状况进行实时监测，并以图形化的形式展示资源状态与利用效率，提供实时性能数据和历史数据查询，查询支持精确和模糊查询；  3）对平台主机聚合及计算节点容量全量数据进行实时监控及告警，支持按内存分配率和CPU分配率进行筛选、展示；  4）支持数据中心查看虚拟机概况，支持搜索查看单个虚拟机信息；  5）支持物理主机关联设备查询功能；  6）支持自定义日志关键字监控，支持监控节点多节点部署。  （9）报表管理  支持周期性生成报表，立即生成报表，周期类型包括天、周、月、季度。只需要设置一次报表参数，即可周期提供报表数据。  （10）统一设备管理  统一管理包括数据中心服务器、应用、网络设备（路由器、交换机、防火墙）。  （11）设备分组  提供设备分组能力，支持将多台设备划入一个分组，以简化后续对这些设备的批量操作。  （12）服务器管理  提供服务器以及各部件基本信息、健康状态的展示功能；提供网口性能、服务器功耗、CPU占用率/内存占用率等指标分析。  （13）存储管理  支持查看和统计存储空间使用情况，包括磁盘空间分配、存储池利用率；支持主机实际存储、虚拟机存储空间使用率查看。  （14）安全管理  提供用户创建、删除、查看、修改等功能，缺省提供admin用户作为超级用户；提供角色创建、修改、删除及查看等功能；提供用户管理、登录鉴权、安全策略等。  （15）网络拓扑  可图形化展示设备网络拓扑信息，并可查看设备基础、接口信息；可通过不同颜色标记异常设备。  （16）变更管理  提供服务产品版本、平台参数变更流程管理，提供变更信息、变更流程状态跟踪以及变更历史信息查询、展示。  （17）值班巡检  1）提供值班队列管理功能，包括：值班人员管理、值班模式管理、排班与交接班管理、值班日历导出、调班申请等；  2）提供巡检统计功能，根据巡检报告总数、成功巡检次数、失败巡检次数、巡检动态等方面进行统计展示；  3）巡检报告可推送至相关责任人邮箱。  （18）审计管理  1）提供对堡垒机的登录日志、操作日志、离线日志等审计日志进行展示；  2）提供敏感操作定义功能，并对敏感操作进行展示；  3）实时展示堡垒机的链接状态，并对超过2小时的长链接堡垒机进行单独展示。  （19）日志管理  提供日志展示平台，并可自定义筛选条件，日志包括服务产品日志及平台运行、操作日志。 | 2880000 | 2880000 |
| 集成实施服务1项 | 1项 | 南宁 | 浪潮、浪潮软件集团有限公司 | 1.我公司如中标，承诺对采购的货物进行总集成实施。按项目监理方要求开展集成实施服务和提供相关文档资料。 2.本项目为交钥匙工程，我公司将确保项目交付时能通过网络安全等级保护第三级测评，能提供完整、安全可靠的云服务。项目采购需求中的技术要求，我公司视为保证项目运行所需的最低要求；如有遗漏，我公司在投标时在投标文件中予以补充；否则，一旦中标将视为我公司认同遗漏部分并免费提供。 | 3000180 | 3000180 |
| 运维管理服务1项 | 1项 | 南宁 | 浪潮、浪潮软件集团有限公司 | 我公司承诺对集成好的政务云平台提供8年期的免费运维管理服务。提供的运维管理服务水平能达到壮美广西政务云统一的服务绩效考核指标体系评分“良好”以上水平。 | 0 | 0 |
| 机柜租赁 | 23个 | 南宁 | 浪潮、浪潮软件集团有限公司 | 1.我公司在本项目中提供的机柜租赁服务满足以下基本要求：单机柜功率4KW，42U，提供2路以上供电，包含一年制冷、供电费用。提供标准供电排插，插头安数和插头个数可所部署设备情况变更及调整，满足设备部署需求，每个机柜初始状态下提供10个10A插口，10个16A插口。 2. 我公司在本项目中提供的机柜在机房的位置区域相对独立，与企业、个人租用机柜隔离，提供独立冷通道，冷通道及机柜带锁，实现设备安全保护。 3.本项目所在机房环境满足以下要求：机房按照A级机房标准建设、运营。 （1）机房配电三级保障，双路备份，一级保障：双路市电接入，2N结构供配电模式。正常工作状态每路带载50%负荷，其中一路市电失电后，另一路市电可承担100%负荷。二级保障：在线式2N模式UPS，市电中断后可持续为IT设备、空调制冷系统、安防系统、消防系统等提供不间断电源，保证满载运行30分钟以上。三级保障：配置大型高压柴油发电机组，采用N+1冗余配置，双路市电停电后自动启动； （2）制冷系统保障。制冷设备采用国际一线品牌，水冷机组、循环水泵、末端空调等相关设备采用N+X冗余配置并采用双电源供电方式，蓄冷罐按满负荷供冷15分钟设计，保障市电停电后持续供冷； （3）安全保障优势，360度全方位无死角视频录像监控，走廊和出入口设置有红外入侵防盗设备，所有设备状态集中在监控室时时监控，一旦有异常情况，通过声、光、电等方式报警，值班工程师立即响应处理。 | 52500 | 1207500 |
| 合计金额大写：叁仟肆佰柒拾捌万元整 ￥34,780,000.00 | | | | | | | |
| 交付使用期：自合同签订之日起120个日历日安装调试完毕通过验收并交付使用。 | | | | | | | |

**注：**

**1.报价一经涂改，应在涂改处加盖单位公章或投标专用章或者由法定代表人或授权委托人签字或盖章，否则其投标作无效标处理。**

**2.“开标一览表”应单独用文件袋（盒、箱）密封并单独递交。**

**3.投标文件电子版以U盘或光盘装载与纸质版“开标一览表”一并装入同一密封袋中。**

**4.投标时必须在“投标报价明细表”中列明第1项（广西电子政务外网政务云资源扩容）中所有设备的品牌、型号、生产厂家全称。**

法定代表人或委托代理人签字：

投标人公章：浪潮软件集团有限公司

2021年1月26日