第二部分 技术要求

序号	设备名称	参数	单位	数量
一	网络设备			
（一）	网络设备-新建		台	
1	市区核心路由器	1.整机交换容量≥316Tbps，转发性能≥76800Mpps； 2.设备采用分布式的硬件转发和无阻塞交换技术。支持双主控、独立交换网板，交换网板总数≥4，10端口万兆接口板≥4块，配置相应的万兆10KM单模光模块； 3.业务板槽位数≥16个，单槽位≥2T线速转发不丢包，提供权威第三方报告，并加盖厂商公章； 4.设备支持100GE、50GE、25GE、10GE、40GE、GE、FE、E1、CPOS等接口类型； 5.支持IPv6路由协议，包括静态路由、OSPFv3、IS-ISv6、BGP4+等协议，支持IPv6终端的接入、IPv6访问控制列表和基于IPv6的策略路由，并提供大容量IPv6 FIB，支持SRv6，IPv4路由表容量≥25M 、IPv6路由表容量≥10M，IPv4转发表容量（FIB）≥4M、IPv6转发表容量（FIB）≥2M，并提供权威第三方报告； 6.支持SRv6 Policy中多条候选路径按优先级选择主用路径， SRv6 Policy双向隧道来回路径一致，并提供权威第三方报告； 7.支持多个SegmentList按照权重（Weiget）属性进行流量负载按比例分配； 8.支持IP/LDP/VPN/TE快速重路由/Hot-Standby，IGP、BGP以及组播路由快速收敛），支持Trunk链路分担备份，BFD链路快速检测，EthernetOAM，路由协议/端口/VLANDamping、TiLFA、Mirror SID尾节点快速保护技术，提供端到端≤30ms保护倒换； 9.支持基于时隙的FlexE分片，实现≤1G级别带宽颗粒度切片，提供第三方检测报告。	台	1
（二）	安全设备			

1	市核心出口防火墙	性能要求：网络层吞吐量≥35G，应用层吞吐量≥20G，并发连接数≥410 万，HTTP 新建连接数≥18 万，IPSec VPN 最大接入数≥4000，IPSec VPN 吞吐量≥1.2， 硬件要求：内存大小≥16G，电源：冗余电源，接口≥16 千兆电口+2 千兆光口+6 万兆光口 SFP++2 个 40G 万兆光口（含万兆光模块及 40G 光模块）； 功能要求： 1、◆可实现未知威胁检测以及防护，提供证明材料并加盖制造商公章； 2、◆支持勒索病毒检测与防御功能，提供官方检测机构出具的证书或检测报告并加盖制造商公章； 3、支持虚拟防火墙功能，支持虚拟防火墙的创建和删除； 4、支持策略生命周期管理功能，支持对安全策略修改的时间、原因、变更类型进行统一管理，提供产品功能截图证明并加盖制造商公章； 5、支持服务器漏洞防扫描功能，提供产品功能截图证明和具备 CMA/CNAS 标识的第三方检测报告并加盖制造商公章； 6、◆支持事前账号脆弱性、事中账号爆破、事后账号失陷的安全防护，提供产品功能截图和“账号安全”相关软件著作权并加盖制造商公章； 7、支持安全策略有效性分析功能，分析内容至少包括策略冗余分析、策略匹配分析、风险端口风险等内容，提供安全策略优化建议； 8、支持联动运维人员微信及时进行安全事件预警以及安全事件处置，提供功能截图及具备 CMA、CNAS 标记的检测报告并加盖制造商公章； 9、支持 X-Forworded-For 字段检测，并对非法源 IP 进行日志记录和联动封锁，提供产品功能截图证明和具备 CMA/CNAS 标识的第三方检测报告并加盖制造商公章； 10、提供至少五年产品质保及软件升级服务，提供制造商服务承诺函并加盖制造商公章；	台	2
2	市核心上网行为管理	性能要求：网络层吞吐量≥20G，应用层吞吐量≥9Gb，带宽性能≥5Gb，支持用户数≥50000，每秒新建连接数≥80000，最大并发连接数≥3200000；	台	1

		硬件要求：标准 2U 机架式设备，内存大小≥24G，电源：冗余电源，接口≥4 千兆电口+4 千兆光口 SFP+2 万兆光口 SFP+（含万兆光模块）； 功能要求： 1、◆支持 PPS 异常、丢包异常、ARP 异常、内网 DOS 攻击等异常情况实时监测，显示每日异常事件个数及情况，提供产品功能截图并加盖制造商公章； 2、支持首页分析显示接入用户人数、终端类型；带宽质量分析、实时流量排名；资产类型分布、新设备发现趋势、终端违规检查项排行、终端违规用户排行，提供产品功能截图并加盖制造商公章； 3、支持客户端解密排障，自动检测解密审计不成功原因，支持针对用户认证的故障进行分析，给出错误详情以及排查建议，提供产品功能截图并加盖制造商公章； 4、◆支持首页分析显示接入用户人数、终端类型；带宽质量分析、实时流量排名；资产类型分布、新设备发现趋势、终端违规检查项排行、终端违规用户排行，提供产品功能截图并加盖制造商公章； 5、◆支持与互联网出口防火墙、双域专网防火墙、入侵防御实现认证联动，可以转发用户认证信息到防火墙、入侵防御，实现单点登录，提供证明材料并加盖制造商公章（证明材料：提供标准能力截图或不少于 30 人天的定制承诺函）； 6、支持远程应用的外发附件审计,包括 Teamviewer、向日葵、Anydesk、RDP；支持外发截屏，当用户外发附件时，会自动截取外发时刻的屏幕，并记录到文件审计日志；支持 Windows 终端打印文件行为和打印文件内容的审计，提供产品功能截图并加盖制造商公章； 7、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；用户指定应用上网流速超过预设阈值后，网关自动提醒该用户，提供产品功能截图并加盖制造商公章； 8、支持自定义测试地址，检查终端是否能 PING 通，对不满足检查要求的终端强制断网，支持向管理员告警，并弹窗提示用户，提供产品功能截图并加盖制造商公章； 9、提供至少五年软件升级及产品质保服务，提供制造商服务承诺函并加盖制造商公		

		章；		
3	市核心堡垒机	性能要求：默认包含运维授权数≥200，最大可扩展资产数≥1000，图形运维最大并发数≥200，字符运维最大并发数≥350； 硬件要求：标准 2U 机架式设备，内存大小≥8G，硬盘容量≥128GB SSD+2TB SATA，电源冗余电源，接口≥6 千兆电口+2 万兆光口 SFP+（含万兆光模块）； 功能要求： 1、◆支持动作流配置，通过动作流配置不仅实现广泛的应用接入支持还实现单点登录和审计接入，提供产品功能截图并加盖制造商公章； 2、支持静态口令认证、手机动态口令认证、Usbkey（数字证书）认证、AD 域认证、Radius 认证等认证方式；并支持各种认证方式和静态口令组合认证，提供产品功能截图并加盖制造商公章； 3、支持 Windows AD 域账号与堡垒主机账号周期比对，自动或手动删除或锁定失效的域账号； 4、支持角色自定义，并且可划分角色的管理范围，提供产品功能截图并加盖制造商公章； 5、支持 RDP 安全模式（RDP、NLA、TLS、ANY）设置，以适应 RDP-Tcp 属性中的所有功能配置，包括加密级别为客户端兼容、低、高、符合 FIPS 标准等加密级别； 6、支持跨部门的交叉授权操作，部门资源管理员可将本部门资源授权给其他部门用户，实现资源临时/长期跨部门访问； 7、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，提供产品功能截图并加盖制造商公章； 8、提供至少五年产品质保及软件升级服务，提供制造商服务承诺函并加盖制造商公章；	台	1
4	市核心日志审	性能要求:默认包含主机审计许可证书数量≥200,最大可扩展审计主机许可数≥450，	台	1

	计	可用存储量≥4TB（RAID1 模式），平均每秒处理日志数（eps）最大性能≥3500； 硬件要求：标准 2U 机架式设备，内存大小≥32G，硬盘容量≥128G minisata+4T SATA*2，电源：冗余电源，接口≥6 千兆电口+2 万兆光口 SFP+（含万兆光模块）； 功能要求： 1、◆支持通过正则、分隔符、json、xml 的可视方式进行自定义规则解析，支持对解析结果字段的新增、合并、映射，提供产品功能截图并加盖制造商公章； 3、支持设置过滤条件，过滤无用日志，减少发送到核心服务器的安全事件数，减少对网络带宽和数据库存储空间的占用； 4、支持日志批量转发，并且可以转发到第三方平台，支持转发原始日志和已解析日志的两种日志，提供产品功能截图并加盖制造商公章； 5、支持网站攻击、漏洞利用、拒绝服务、主机脆弱性等进行内置关联分析规则，关联分析规则数量不少于 350 条，提供产品功能截图并加盖制造商公章； 6、为实时监控系统日志传输率和日志留存的合规性，要求产品可对首页进行自定义； 7、支持多种输入方式、可根据时间、事件等级进行组合查询。根据设定的设备、地址、ID 等进行具体条件搜索。可设置定时刷新频率，根据刷新时间实时接入日志事件，提供产品功能截图并加盖制造商公章； 8、提供至少五年产品质保及软件升级服务，提供制造商服务承诺函并加盖制造商公章；		
5	市核心网络审计	性能要求：网络层吞吐量≥8Gb，应用层吞吐量≥1.1Gb，带宽性能≥750Mb，每秒新建连接数≥12000，最大并发连接数≥500000； 硬件要求：内存大小≥8G，接口≥6 千兆电口+2 万兆光口 SFP+。 功能要求： 1、◆支持 PPS 异常、丢包异常、ARP 异常、内网 DOS 攻击等异常情况实时监测，显示每日异常事件个数及情况，提供产品功能截图并加盖制造商公章； 2、支持首页分析显示接入用户人数、终端类型；带宽质量分析、实时流量排名；资	台	1

		产类型分布、新设备发现趋势、终端违规检查项排行、终端违规用户排行，提供产品功能截图并加盖制造商公章； 3、支持客户端解密排障，自动检测解密审计不成功原因，支持针对用户认证的故障进行分析，给出错误详情以及排查建议，提供产品功能截图并加盖制造商公章； 4、支持首页分析显示接入用户人数、终端类型；带宽质量分析、实时流量排名；资产类型分布、新设备发现趋势、终端违规检查项排行、终端违规用户排行，提供产品功能截图并加盖制造商公章； 5、◆支持与互联网出口防火墙、双域专网防火墙、入侵防御实现认证联动，可以转发用户认证信息到防火墙、入侵防御，实现单点登录，提供证明材料并加盖制造商公章（证明材料：提供标准能力截图或不少于 30 人天的定制承诺函）； 6、支持远程应用的外发附件审计,包括 Teamviewer、向日葵、Anydesk、RDP；支持外发截屏，当用户外发附件时，会自动截取外发时刻的屏幕，并记录到文件审计日志；支持 Windows 终端打印文件行为和打印文件内容的审计，提供产品功能截图并加盖制造商公章； 7、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；用户指定应用上网流速超过预设阈值后，网关自动提醒该用户，提供产品功能截图并加盖制造商公章； 8、支持自定义测试地址，检查终端是否能 PING 通，对不满足检查要求的终端强制断网，支持向管理员告警，并弹窗提示用户，提供产品功能截图并加盖制造商公章； 9、提供至少五年软件升级及产品质保服务，提供制造商服务承诺函并加盖制造商公章；		
6	电源线	ZARVV 1*240　黑/红/蓝	米	55
7	集成服务	包括设备安装、调试等服务	项	1