1.1

| 项目编号 | 项目名称 | 主要性能指标 | 拟提供的产品<br>主要技术性能指标响应情况 | 品牌及型号（需逐条加盖生产制造商的单位公章） | 标注“★”的条款以及招标公告中注明的主要设备的参数及品牌型号将作为公示资料同中标候选人一并公示 |
|---|---|---|---|---|---|
| 1 | 互联边界下一代防火墙（含WAF能力） | ★1、网络层吞吐量：≥100G，并发连接数：≥2000万；<br>2、标准机架式设备，配置≥3年入侵防御特征库升级，≥3年病毒过滤升级，≥3年Web应用防护规则库升级；<br>★3、设备采用国产操作系统和芯片，满足国产化要求；<br>4、配置双电源；接口要求：≥4千兆电口、≥4千兆光口（配置4个千兆多模光模块）、≥8万兆光口（配置8个万兆多模光模块）；≥4个40G光口（配置4个40G多模光模块）；<br>5、同时支持IPV4及IPV6协议；<br>6、可针对资源、目的、协议、用户、时间等进行访问控制策略配置；支持自定义安全策略，安全策略组功能；<br>7、路由协议：支持动态地址转换、静态地址转换以及端口地址转换功能，支持OSPFv2/v3等路由协议；<br>8、支持对HTTP/SMTP/POP3/FTP等协议进行病毒防御，支持针对勒索病毒进行检测并开展防御；<br>9、支持通过TCP代理及SSL代理等方式对https进行解密；<br>10、支持服务器漏洞防护，针对漏洞的扫描攻击可进行IP记录和封锁；<br>11、支持对僵尸主机进行发现，僵尸网络特征库应在百万级以上；<br>12、防火墙本地日志存储空间不足时支持日志服务器存储；<br>13、支持带外管理，保障管理网络和业务网络相互隔离；<br>14、支持Web管理、串口管理、SSH管理等方式进行管理。 | 满足 | 品牌：北京启明星辰信息安全技术有限公司<br>型号：USG-FW-12600N-20600GN | |

| | | | | |
|---|---|---|---|---|
| 2 | 互联网边界上网行为管理 | ★1、网络层吞吐量：≥40G；<br>2、标准机架式设备，配置≥3 年应用识别特征库升级<br>★3、设备采用国产操作系统和芯片，满足国产化要求；<br>4、配置双电源；接口要求：≥4 千兆电口、≥4 千兆光口（配置 4 个千兆多模光模块）、≥4 万兆光口（配置 4 个万兆多模光模块），≥2 个 40G 光口（配置 2 个 40G 多模光模块）；<br>5、支持路由、网桥、旁路等多种部署模式；<br>6、同时支持 IPV4 及 IPV6 协议；<br>7、支持客户端自动化批量安装根证书，保障 SSL 解密过程对用户透明；<br>8、对向日葵、Teamviewer、Anydesk、RDP 等远程运维工具，需审计其发送的相关附件；<br>9、流量管理策略可依据用户组、位置、终端类型、URL 类型等进行配置；<br>10、支持检测网页中包含的恶意链接，并对其进行风险提示及阻断；<br>11、支持与外部有流量交互的服务器，可对其进行行为及流量审计；<br>12、当设备存储空间不足时，可以设置独立的外置日志中心；<br>13、支持通过报表展示上网行为数据排行；<br>14、支持对 U 盘、蓝牙设备、摄像头、打印机等外设进行审计；<br>15、支持基于不同的文件类型进行识别，对不同的文件类型做流控。 | 满足 | 品牌：深信服<br>型号：<br>AC-1000-L3100 |

| | | | | |
|---|---|---|---|---|
| 3 | 互联网边界负载均衡 | ★1、吞吐量≥60Gbps，并发连接数≥80000000，新建连接数≥1000000；<br>★2、设备采用国产操作系统和芯片，满足国产化要求；<br>3、标准机架式设备，配置双电源；接口要求：≥8 千兆电口，≥4 千兆光口（配置 4 个千兆多模光模块），4 个万兆光口（配置 4 个万兆多模光模块）；≥4 个 40G 光口（配置 4 个 40G 多模光模块）；<br>4、设备可同时支持包括链路负载均衡、全局负载均衡、服务器负载均衡和 SSL 卸载的功能；<br>5、支持针对多条线路的流量均衡调度并实现链路间的冗余互备；<br>6、支持基于应用协议的智能选路并支持对应用快速切换；<br>7、设备需支持轮询、加权轮询、带宽比例、哈希、主备、首个可用、优先级等算法；<br>8、IPv6 支持双栈模式，支持 NAT46、NAT64、NAT66、FTP ALG、DNS64 等协议转换；<br>9、支持链路健康状态监测及 TCP 半连接健康检查；<br>10、支持智能 DNS 解析功能，引导访问用户从最优路径的线路接入应用系统；<br>11、内置 IP 地址库，通过 IP 地址库进行流量调度分发，实现链路负载；<br>12、支持 DNS 内网记录，可识别内网用户并对其 DNS 请求直接返回相应结果；<br>13、支持同一个虚拟服务下配置多个 IPv4 和 IPv6 地址。 | 满足 | 品牌：深信服<br>型号：<br>AD-1000-GA320 |

| | | | | |
|---|---|---|---|---|
| 4 | 互联网边界抗Ddos | ★1、DDoS 清洗流量：≥40G；HTTP 新建事务能力（TPS）：≥30000/s；TPS 时延：≤1.3ms；<br>2、接口要求：≥8 万兆光口（配置 8 个万兆多模光），≥2 个 40G 光口（配置 2 个 40G 多模光模块），<br>★3、设备采用国产操作系统和芯片，满足国产化要求；<br>4、支持 IPV4/IPV6 双栈流量清洗；<br>5、攻击防护类型支持但不限于：SYN flood、ACK flood、ICMP flood、UDP flood；DNS query flood、DNS reply flood；HTTP GET flood（CC 攻击）、HTTP Post flood、HTTP 代理型攻击；慢速攻击、连接耗尽攻击、空连接攻击、SIP flood 攻击；URL 请求合法性进行验证，可防御 CC 及变种的能力；<br>6、支持使用智能攻击流量识别的技术进行防护，即当发生未知攻击，无需专门的撰写规则即可对这些攻击进行防护；<br>7、支持对特定的攻击包设置模板匹配的功能，支持对指定的用户进行防护，实现按需防护；<br>8、支持对站点进行分组，并对不同的组别进行独立的防护策略配置；<br>9、支持针对系统菜单项进行自定义分配功能，并且可自定义账号的编辑、只读权限；<br>10、支持导入 SSL 证书对 HTTPS 流量进行防护。 | 满足 | 品牌：深信服<br>型号：<br>AD-1000-GA220-DD |

| | | | | |
|---|---|---|---|---|
| 5 | radius 认证服务器 | 1、CPU 物理核心数≥32 个，主频≥2.4GHz；内存≥128G；提供≥12 个 3.5 寸硬盘槽位，配置≥2 块 480G SSD 硬盘，≥2 块 4T 的 HDD 硬盘；配置≥2 个万兆网口和≥2 个千兆网口，<br>★2、设备采用国产操作系统和芯片，满足国产化要求；<br>3、支持对接身份源类型，包括本地开户、AD 域、LDAP、数字证书 CA 等；支持 portal、dot1x、MAB 等认证协议；<br>4、支持 dot1x 认证的多种协议，包括：PAP、CHAP、EAP-MD5、EAP-PEAP-MSCHAPv2、EAP-PEAP-GTC、EAP-TTLS-PAP、EAP-TLS；<br>5、支持终端的上线自动发现功能；<br>6、支持 DHCP 特征识别、HTTP User Agent 特征识别和终端 MAC 地址识别终端信息；<br>7、支持分级分权，基于角色分配权限功能菜单；<br>8、支持在线用户查询，可基于用户名、用户姓名、终端 MAC、终端 IP、进行模糊查询；<br>9、支持数据库备份，完整备份，指定备份；<br>10、支持本地逃生功能，当 radius 服务器不能提供服务时，下发命令至交换机进行放行逃生。 | 满足 | 品牌（UNIS）<br>型 号 （U-Center 智能一体化运维） |

| | | | | |
|---|---|---|---|---|
| 6 | 流量控制 | ★1、网络层吞吐量：≥40G，支持用户数：≥100000；<br>2、配置双电源；接口要求：≥4 千兆电口、≥4 千兆光口（配置 4 个千兆多模光模块）、≥4 万兆光口（配置 4 个万兆多模光模块）；≥2 个 40G 光口（配置 2 个 40G 多模光模块）；<br>★3、设备采用国产操作系统和芯片，满足国产化要求；<br>4、支持网络异常情况发现：如 ARP 异常、内网 DOS、PPS 异常、异常丢包等；<br>5、流量管理策略可依据用户组、位置、终端类型、URL 类型等进行配置；<br>6、支持针对 P2P 流量管控，可对 P2P 的下行流量丢包；支持根据整体线路空闲情况，动态调整流量控制策略；<br>7、各层级流控可展示当前状态；<br>8、当设备存储空间不足时，可以设置独立的外置日志中心；<br>9、支持智能过滤，保障过滤掉大部分无用的日志；<br>10、支持限制某个用户或一组用户的流量配额；<br>11、通过流量父子通道化，保障流控划分灵活性；<br>12、可以查询流量配额并展示当前流量使用量；<br>13、支持对 U 盘、蓝牙设备、摄像头、打印机等外设进行审计。 | 满足 | 品牌：深信服<br>型号：<br>AC-1000-L3100-FC |

| | | | | | |
|---|---|---|---|---|---|
| 7 | 互联网蜜罐 | 1、处理器≥8 核，内存≥16G，硬盘≥2T，千兆电口≥2；<br>★2、支持国产操作系统和芯片，满足国产化要求；<br>3、支持≥10 个沙箱，支持 windows 与 linux 沙箱；沙箱支持增、删、停、重置、编辑沙箱内容；<br>4、资产管理支持查看资产信息及关联的沙箱信息；<br>5、支持 Windows、Mac、Android 反制木马，伪造敏感信息，使攻击者进行下载；<br>6、支持向特定邮箱发送邮件诱饵以及附件，感知邮件入侵行为；<br>7、支持对黑客溯源功能，形成黑客溯源、黑客画像页面；<br>8、可基于现有的设备指纹进行设备指纹碰撞；<br>9、支持记录攻击者所有攻击行为，通过时间线展示；<br>10、支持威胁事件的实时告警、并提供事件处理功能。 | 满足 | 品牌：北京启明星辰信息安全技术有限公司<br>型号：<br>CDS3600-HG | |

| | | | | | |
|---|---|---|---|---|---|
| 8 | 网页防篡改 | 1、支持≥50 台服务器授权，支持 Windows、linux 等主流操作系统网站防篡改；<br>★2. 支持国产操作系统和芯片，满足国产化要求；<br>3、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；<br>4、支持 Ipv4/IPv6 网络环境下部署管理防篡改；<br>5、支持在断线情况下对网页文件目录的防护功能；<br>6、支持网页防篡改记录同步动作日志；支持防篡改插件安装时不重启 Web 服务器；<br>7、支持 IIS、Weblogic、Websphere、Apache、Tomcat 等 Web 服务器；<br>8、支持对网站服务器的 CPU、内存、收包量、发包量等信息进行实时监控；<br>9、支持对管理角色进行增加、删除和属性修改等操作行为；<br>10、支持日志 syslog 日志外发方式。 | 满足 | 品牌：北京启明星辰信息安全技术有限公司<br>型号：WAG-WS | |

| | | | | | |
|---|---|---|---|---|---|
| 9 | DMZ 业务区边界防火墙 | ★1、网络层吞吐量：≥40G，并发连接数：≥420 万；<br>2、配置≥3 年入侵防御特征库升级，≥3 年病毒过滤升级<br>★3、设备采用国产操作系统和芯片，满足国产化要求；<br>4、配置双电源；接口要求：≥16 千兆电口、≥4 万兆光口 SFP+（配置 4 个万兆多模光模块），≥2 个 40G 光口（配置 2 个 40G 多模光模块）；<br>5、同时支持 IPV4 及 IPV6 协议；<br>6、可针对资源、目的、协议、用户、时间等进行访问控制策略配置；支持自定义安全策略，安全策略组功能；<br>7、路由协议：支持动态地址转换、静态地址转换以及端口地址转换功能，支持 OSPFv2/v3 等路由协议；<br>8、支持对 HTTP/SMTP/POP3/FTP 等协议进行病毒防御，支持针对勒索病毒进行检测并开展防御；<br>9、支持通过 TCP 代理及 SSL 代理等方式对 https 进行解密；<br>10、支持服务器漏洞防护，针对漏洞的扫描攻击可进行 IP 记录和封锁；<br>11、支持防护跨站脚本攻击、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；<br>12、防火墙本地日志存储空间不足时支持日志服务器存储；<br>13、支持带外管理，保障管理网络和业务网络相互隔离；<br>14、支持 Web 管理、串口管理、SSH 管理等方式进行管理。 | 满足 | 品牌：北京启明星辰信息安全技术有限公司<br>型号：<br>USG-FW-X-G7810 | |

| | | | | | |
|---|---|---|---|---|---|
| 10 | 数据中心全流量潜伏威胁探针 | ★1、吞吐量：≥20G；<br>★2、设备采用国产操作系统和芯片，满足国产化要求；<br>3、配置双电源，接口要求：≥4 千兆电口、≥4 万兆光口（配置 4 个万兆多模光模块）；<br>4、支持交换机旁路部署，支持同时接入多个镜像口，每个口相互独立不影响；<br>5、支持主动发现影子资产并获取操作系统、开放端口号等；<br>6、支持异常流量检测，如非标准协议运行在标准端口，标准协议运行在非标准接口等；<br>7、审计白名单支持源目 IP、源目端口和日志类型、日志来源；<br>8、提供三权分立的用户管理能力；<br>9、支持设备内置命令行管理窗口；<br>10、支持基于五元组进行流量抓包分析；<br>11、可以通过安全运营平台统一管理对接。 | 满足 | 品牌：北京启明星辰信息安全技术有限公司<br>型号：<br>NT16000-5G-S | |

| | | | | |
|---|---|---|---|---|
| 11 | 核心全流量采集分析系统 | ★1、实时检测网络流量≥40Gbps；<br>2、接口：≥8 个万兆光口（配置 8 个万兆多模光模块），≥350TB 容量（可通过集群实现）；<br>★3、设备采用国产操作系统和芯片，满足国产化要求；<br>4、可基于源目的 MAC 地址、源目的 IP 地址、端口号、协议、数据包内容等对流量进行精细化过滤；<br>5、支持原始通讯数据包回放，能提供服务端离线数据包导入模式；<br>6、支持统计检索指定时间范围的应用、主机、IP 会话、TCP/UDP 会话的通讯流量信息；<br>7、支持对链路 IP 主机进行回溯分析；<br>8、可通过 IP+端口、URL、数据流特征值等方式自定义应用；<br>9、支持 DNS 解析统计功能；<br>10、支持自动判断 ARP 攻击，拒绝服务攻击，DOS 攻击等可疑会话行为；<br>11、支持对网络中的总体流量异常、关键主机流量异常以及关键应用流量异常进行监控和报警；<br>12、支持异常访问警报，可按 IP、端口、应用及协议元素定义访问规则。 | 满足 | 品牌：深信服<br>型号：<br>SIP-Y-L2200H-AY |

| | | | | |
|---|---|---|---|---|
| 12 | 核心业务可视化分析系统 | 1、实时检测网络流量≥40Gbps，业务监控管理授权≥20 个，应用授权≥60 个（可通过集群实现）；<br>★2、设备采用国产操作系统和芯片，满足国产化要求；<br>3、支持对前端回溯设备的管理，能够展示前端设备信息；能够为每个应用配置集中配置性能监控警报；<br>4、支持会话数据流多段分析功能；<br>5、支持网络设备信息获取，可配置路由器、交换机等网络设备信息；<br>6、支持对于有安全威胁流量交互的 IP 地址进行连线并预警提示；<br>7、支持数据包回查，并支持多条件组合进行特征回查；<br>8、支持针对各网段专线线路以图形化进行质量监控。 | 满足 | 品牌：深信服<br>型号：<br>SIP-Y-L2200H-VN |

| | | | | | |
|---|---|---|---|---|---|
| 13 | 省干网全流量潜伏威胁探针 | ★1、吞吐量：≥10G；<br>★2、设备采用国产操作系统和芯片，满足国产化要求；<br>3、配置双电源，接口要求：≥4 千兆电口、≥4 千兆光口 SFP（配置 4 个千兆多模光模块）、≥8 万兆光口 SFP+（配置 8 个万兆多模光模块）；<br>4、支持旁路部署，探针支持接入多个镜像口；<br>5、支持主动发现影子资产并获取操作系统、开放端口号等；<br>6、支持检测标准端口运行非标准协议，非标准端口运行标准协议的异常流量检测；<br>7、审计白名单支持源目 IP、源目端口和日志类型、日志来源；<br>8、提供三权分立的用户管理能力；<br>9、支持设备内置简单命令行管理窗口；<br>10、支持基于五元组进行流量抓包分析。<br>11、可以通过安全运营平台统一管理对接。 | 满足 | 品牌：北京启明星辰信息安全技术有限公司<br>型号：<br>NT16000-HG-5G-H | |

| | | | | |
|---|---|---|---|---|
| 14 | 日志审计 | 1、配置≥600 个日志审计源，支持平滑升级扩容，平均处理能力（每秒日志解析能力 EPS）≥10000EPS，日志审计系统软件；支持在国产操作系统和芯片环境部署，满足国产化要求；<br>2、系统应基于大数据平台架构，支持 IPv6；<br>3、支持自定义规则解析，包括通过正则、分隔符、json、xml 等，支持对结果字段的新增、合并、映射；<br>4、系统可通过自身内置的采集器进行日志采集，支持从不同类型系统采集到的日志进行标准化分析；<br>5、支持网络安全设备、交换设备、路由设备、操作系统、应用系统、虚拟环境等的收集；<br>6、系统能够对异构日志格式进行统一化处理并保存统一化处理后的日志数据；<br>7、系统支持设置日志存储备份策略，可设置备份周期、备份日志类型等；<br>8、支持将不同设备上采集的日志进行关联分析，发现可能的风险；<br>9、支持显示单事件详细信息和事件原始信息，支持事件详情中任意字段作为查询条件；<br>10、系统支持统计分析报表与多种文件格式导出。 | 满足 | 品牌：深信服<br>型号：<br>SIP-Logger-L2000 |

| | | | | | |
|---|---|---|---|---|---|
| 15 | 数据库审计 | 1、数据库实例个数：≥100 个，≥70000 条 SQL/s；<br>★2、设备采用国产操作系统和芯片，满足国产化要求；<br>3、配置双电源，接口要求：≥4 千兆电口、≥4 千兆光口 SFP（配置 4 个千兆多模光模块）、≥2 万兆光口 SFP+（配置 2 个万兆多模光模块）；<br>4、支持主流数据库，如 Oracle、SQL-Server、DB2、Informix、Sybase、MySQL、达梦、人大金仓 kingbase、南大通用 Gbase、Teradata、Cache、MongoDB 等；<br>5、支持数据采集功能，至少能根据需要审计的数据库目标设置数据采集策略；<br>6、能够审计以下事件：数据库用户操作、数据库数据操作、数据库结构操作、数据库返回结果；<br>7、提供统计功能，支持以数据库标识和事件类型为条件统计审计事件；<br>8、能够把审计结果生成审计记录，数据库事件审计记录应包括：日期时间、客户端标识、数据库标识、操作命令、操作结果等；<br>9、能够把统计结果生成报表，并支持 HTML、PDF、WORD、EXCEL 等文件格式中的一种进行导出；<br>10、能够设置事件分级策略以区分事件的安全级别，审计记录应事件分级信息；<br>11、告警响应：支持屏幕告警、邮件告警、SNMP trap 告警、声光电告警、短信告警等方式中的一种。 | 满足 | 品牌：北京启明星辰信息安全技术有限公司<br>型号：DA-FT-3000UR | |

| | | | | |
|---|---|---|---|---|
| 16 | 运维审计（堡垒机） | 1、本次配置管理设备数授权≥600 个，支持字符并发≥300，支持图形并发≥200，支持国密算法；<br>★2、设备采用国产操作系统和芯片，满足国产化要求；<br>3、接口要求：≥6 千兆电口、≥2 万兆光口 SFP+（配置 2 个万兆多模光模块）；<br>4、支持通过动作流配置提供应用接入，以实现单点登录和审计接入；<br>5、用户登录认证方式支持多种认证方式和静态口令组合认证；<br>6、内置三员角色的同时支持角色灵活自定义，划分管理角色的管理范畴；<br>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员逐级审批；<br>8、支持定期变更目标设备口令；<br>9、支持用户执行高危命令时需要管理员审批后才允许执行；<br>10、支持手动和自动定期备份配置信息，支持配置信息本地备份及异地 FTP 备份；<br>11、支持 web 页面直接发起运维，无须安装任何控件；<br>12、支持生成报表展示用户和资源的授权关系，并提供 EXCEL、WORD、PDF、HTML 等格式导出。 | 满足 | 品牌：深信服<br>型号：<br>OSM-1000-L2600 |

| | | | | | |
|---|---|---|---|---|---|
| 17 | 主机防病毒 | 1、本次需配置服务器端授权≥3000个；管理控制中心采用 B/S 架构，直接通过 web 接入进行管理；<br>★2、支持包括但不限于国产操作系统和芯片，满足国产化要求；<br>3、可以对终端的操作系统、应用软件、监听端口、主机账户等进行统计；<br>4、针对 WebShell 具备实时发现能力，发现后可进行自动隔离或者上报；<br>5、可以根据勒索病毒的一般演进过程进行分步骤防护，并同步勒索病毒处置情况；<br>6、支持录入资产并划分给相关责任人，以便于进行终端资产管理；<br>7、支持客户端按计划错峰及灰度升级，避免网络拥堵；<br>8、支持与安全运营平台联动，在安全运营平台下发快速查杀任务；<br>9、支持配置不同的权限角色，并配置可管辖的终端范围；<br>10、支持导出终端风险报告，从整体分析全网安全状况；<br>11、具备主机侧系统层、应用层行为数据采集能力，不同攻击阶段的主要攻击手法检测，对攻击事件深度分析；<br>12、支持主机安全检查基线，自定义基线的合规性检查，并对不合规的检查项提供设置建议。 | 满足 | 品牌：北京启明星辰信息安全技术有限公司；<br>型号：EDR-8000-CONPR | |

| | | | | | |
|---|---|---|---|---|---|
| 18 | 零信任远程安全接入系统 | **零信任控制中心**<br>★1、单台性能要求：并发用户数：≥15000，新建用户数（个/秒）：≥400；<br>2、本次配置并发接入授权：≥40000（可通过集群实现）；<br>★3、设备采用国产操作系统和芯片，满足国产化要求；<br>4、配置双电源，内存容量：≥16G，接口要求：≥4 千兆电口、≥4 千兆光口（配置 4 个千兆多模光模块）；支持 SM2、SM3、SM4 等商用密码算法，提供国家密码管理局商用密码检测中心出具的商用密码认证证书；<br>5、可自建集群扩展接入能力，依赖自身集群即可实现工作负载；<br>6、通过单包授权拒绝非授权用户的连接，隐藏服务端口，避免敲门放大问题；<br>7、具备主动防御能力，内置基于 SSH、FTP、HTTP 等协议的欺骗服务；<br>8、支持根据风险日志生成会话拓扑图和事件报告，展示关联的 IP、账号、终端；<br>9、支持识别扫描行为，包括目录扫描、端口扫描等，发现后可通知管理员锁定相关账号；<br>10、可通过配置 CDN 地址，实现零信任客户端的快速获取；<br>11、连接后仍可根据应用类型、应用访问进程等进行动态访问控制，包括阻止访问、注销登录、锁定账号等；<br>12、相关告警事件可通过邮件通知管理员；<br>13、设备可以自主检查安全状态及策略配置，统计正常情况、异常情况和告警情况，自动生成巡检报告；<br>14、支持管理员在控制台远程获取在线终端的日志；<br>15、支持提供 SNMP 服务来对接运维监控设备；<br>16、支持提供命令面板，内嵌常规网络配置和排障命令；<br>17、支持与多重身份认证系统对接，支持反向 OAuth 对接及票据注入等； | 满足 | 零信任控制中心<br>品牌：北京启明星辰信息安全技术有限公司<br>型号：<br>eTrust-SDP-G-HG9800<br><br>零信任代理网关<br>品牌：北京启明星辰信息安全技术有限公司<br>型号：<br>eTrust-SDP-G-HG4800 | |

| | | | | | |
|---|---|---|---|---|---|
| | | 18、支持将用户访问零信任系统的认证及策略类请求加密流量解密后镜像给外部系统提升溯源及审计能力；<br>19、支持 SPA 单包授权技术，用户获取独特安全码，隐藏零信任端口。<br>**零信任代理网关**<br>★1、单台性能要求：最大加密流量：≥2.5Gbps，并发用户数（个）：≥25000，https 并发连接数（个）：≥200000；<br>2、支持 SM2、SM3、SM4 等商用密码算法，提供国家密码管理局商用密码检测中心出具的商用密码认证证书；<br>3、配置双电源，内存容量：≥32G，接口要求：≥4 千兆电口、≥4 千兆光口（配置 4 个千兆多模光模块）、≥4 万兆光口（配置 4 个万兆多模光模块）<br>★4、设备采用国产操作系统和芯片，满足国产化要求；<br>5、支持 IPV4/IPV6 双栈网络 IP 配置；可自建集群扩展接入能力，依赖自身集群即可实现工作负载；<br>6、支持将用户访问资源的相关流量解密后镜像给外部安全设备进行分析，如态势感知；<br>7、支持点击图像校验码机制，防止机器人攻击；<br>8、针对高危端口进行检查： SSH 端口开启、控制台接入 IP 限制情况、SNMP 指定 IP 地址接入；<br>9、支持 TLS 协议检查；<br>10、支持检查设备是否开启自动备份功能；<br>11、支持查看设备运行状态，包括 CPU、内存、磁盘占比等。 | | | |

| | | | | | |
|---|---|---|---|---|---|
| 19 | 零信任远程安全运维系统（运维） | 1、本次配置≥1000 并发接入授权及≥1000 运维沙箱授权；支持 SM2、SM3、SM4 等商用密码算法，提供国家密码管理局商用密码检测中心出具的商用密码认证证书；<br>2、内存容量：≥16G，接口要求：≥6 千兆电口、≥2 千兆光口 SFP（配置 2 个千兆多模光模块）；<br>★3、设备采用国产操作系统和芯片，满足国产化要求；<br>4、同时支持 IPV4 及 IPV6 协议；可自建集群扩展接入能力，依赖自身集群即可实现工作负载；<br>5、通过单包授权拒绝非授权用户的连接，隐藏服务端口，避免敲门放大问题；<br>6、可通过配置 CDN 地址，实现零信任客户端的快速获取；<br>7、连接后仍可根据应用类型、应用访问进程等进行动态访问控制，包括阻止访问、注销登录、锁定账号等；<br>8、相关告警事件可通过邮件通知管理员；<br>9、设备可以自主检查安全状态及策略配置，统计正常情况、异常情况和告警情况，自动生成巡检报告；<br>10、支持工作空间与个人空间的网络访问权限隔离；<br>11、支持沙箱准入策略，在内网环境使用时不需要启用沙箱；<br>12、支持管理员在控制台远程获取在线终端的日志；<br>13、支持提供 SNMP 服务来对接运维监控设备；<br>14、支持提供命令面板，内嵌常规网络配置和排障命令；<br>15、支持 SPA 单包授权技术，用户获取独特安全码，隐藏零信任端口。 | 满足 | 品牌：北京启明星辰信息安全技术有限公司<br>型号：eTrust-SDP-AHG780 | |

| | | | | | |
|---|---|---|---|---|---|
| 20 | 视频网闸 | ★1、网络层吞吐量：≥10G，并发连接数：≥50W；<br>★2、设备采用国产操作系统和芯片，满足国产化要求；<br>3、双主机架构，单主机接口要求：≥6 千兆电口，≥4 千兆光口（配置 4 个千兆多模光模块），≥2 万兆光口（配置 2 个万兆多模光模块），配置双电源；<br>4、 产品内置多类应用支持模块，并可控制相应应用协议的动作、参数、内容；<br>5、 支持文件交换容错和告警功能，交换出错能够自动重传；<br>6、 支持 GB 28181 视频通信国家标准及相关厂商协议规范；<br>7、 支持的数据库种类包括 ORACLE、SQLSERVER、MYSQL、SYBASE 等主流数据库；<br>8、 支持 TCP 应用层数据单向传输的控制，满足二次防护对数据传输的安全性需求；<br>9、 采取系统策略配置管理员、安全管理员与日志管理员三种角色分立的权限分配模式；<br>10、 支持 TCP/IP 以上的应用层协议，支持自定义的 TCP、UDP 协议的数据隔离交换；<br>11、 系统可存储和审计包含：系统日志；管理日志；网络活动日志；入侵报警及处理日志；访问控制日志。 | 满足 | 品牌：北京启明星辰信息安全技术有限公司<br>型号：<br>GAP-6000-G8500-HG | |

| | | | | | |
|---|---|---|---|---|---|
| 21 | 数据中心潜伏威胁探针 | ★1、吞吐量：≥10G；<br>★2、设备采用国产操作系统和芯片，满足国产化要求；<br>3、配置双电源，接口要求：≥4 千兆电口、≥4 千兆光口（配置 4 个千兆多模光模块）、≥8 万兆光口（配置 8 个万兆多模光模块）；<br>4、支持交换机旁路部署，支持同时接入多个镜像口，每个口相互独立不影响；<br>5、支持主动发现影子资产并获取操作系统、开放端口号等；<br>6、支持异常流量检测，如非标准协议运行在标准端口，标准协议运行在非标准接口等；<br>7、审计白名单支持源目 IP、源目端口和日志类型、日志来源；<br>8、提供三权分立的用户管理能力；<br>9、支持设备内置命令行管理窗口；<br>10、支持基于五元组进行流量抓包分析。<br>11、可以通过安全运营平台统一管理对接。 | 满足 | 品牌：北京启明星辰信息安全技术有限公司<br>型号：<br>NT16000-HG-5G-H | |

| | | | | | |
|---|---|---|---|---|---|
| 22 | 零信任远程安全运维系统（运维） | 1、本次配置≥200 并发接入授权及≥200 运维沙箱授权；支持 SM2、SM3、SM4 等商用密码算法，提供国家密码管理局商用密码检测中心出具的商用密码认证证书。；<br>2、内存容量：≥16G；接口要求：≥6 千兆电口、≥2 千兆光口 SFP（配置 2 个千兆多模光模块）；<br>★3、设备采用国产操作系统和芯片，满足国产化要求；<br>4、同时支持 IPV4 及 IPV6 协议；可自建集群扩展接入能力，依赖自身集群即可实现工作负载；<br>5、通过单包授权拒绝非授权用户的连接，隐藏服务端口，避免敲门放大问题；<br>6、可通过配置 CDN 地址，实现零信任客户端的快速获取；<br>7、连接后仍可根据应用类型、应用访问进程等进行动态访问控制，包括阻止访问、注销登录、锁定账号等；<br>8、相关告警事件可通过邮件通知管理员；<br>9、设备可以自主检查安全状态及策略配置，统计正常情况、异常情况和告警情况，自动生成巡检报告；<br>10、支持工作空间与个人空间的网络访问权限隔离；<br>11、支持沙箱准入策略，在内网环境使用时不需要启用沙箱；<br>12、支持管理员在控制台远程获取在线终端的日志；<br>13、支持提供 SNMP 服务来对接运维监控设备；<br>14、支持提供命令面板，内嵌常规网络配置和排障命令；<br>15、支持 SPA 单包授权技术，用户获取独特安全码，隐藏零信任端口。 | 满足 | 品牌：北京启明星辰信息安全技术有限公司<br>型号：<br>eTrust-SDP-AHG780 | |

| | | | | | |
|---|---|---|---|---|---|
| 23 | 关键业务区边界防火墙 | ★1、网络层吞吐量：≥40G，并发连接数：≥420 万；<br>2、配置≥3 年入侵防御特征库升级，≥3 年病毒过滤升级；<br>★3、设备采用国产操作系统和芯片，满足国产化要求；<br>4、配置双电源；接口要求：≥4 千兆电口、≥4 万兆光口 SFP+（配置 4 个万兆多模光模块），≥2 个 40G 光口（配置 2 个 40G 多模光模块）；<br>5、同时支持 IPV4 及 IPV6 协议；可针对资源、目的、协议、用户、时间等进行访问控制策略配置；支持自定义安全策略，安全策略组功能；<br>6、路由协议：支持动态地址转换、静态地址转换以及端口地址转换功能，支持 OSPFv2/v3 等路由协议；<br>7、支持对 HTTP/SMTP/POP3/FTP 等协议进行病毒防御，支持针对勒索病毒进行检测并开展防御；<br>8、支持通过 TCP 代理及 SSL 代理等方式对 https 进行解密；<br>9、支持服务器漏洞防护，针对漏洞的扫描攻击可进行 IP 记录和封锁；<br>10、支持防护跨站脚本攻击、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；<br>11、防火墙本地日志存储空间不足时支持日志服务器存储；<br>12、支持带外管理，保障管理网络和业务网络相互隔离；<br>13、支持 Web 管理、串口管理、SSH 管理等方式进行管理。 | 满足 | 品牌：北京启明星辰信息安全技术有限公司<br>型号：<br>USG-FW-N-G7810 | |

| | | | | | |
|---|---|---|---|---|---|
| 24 | 安全运营平台（含SOAR） | 1、安全运营平台存储容量：≥100T（可通过集群实现），单台要求：配置双电源，内存：≥256GB，单台接口要求：≥4千兆电、≥2万兆光口（配置2个万兆多模光模块）；<br>★2、设备采用国产操作系统和芯片，满足国产化要求；<br>3、支持接入并管理日志采集器、流量采集器；支持探索出网络拓扑结构，并进行网络拓扑的绘制；<br>4、支持用户自定义关联规则，针对简单事件和复杂事件的关联分析功能；<br>5、支持导出PDF、WORD等格式的风险报告；<br>6、支持联动防火墙访隔离主机、封锁域名/URL/IP，并支持针对威胁事件触发手动联动、自动联动等联动响应方式；<br>7、支持文件分析，至少包括常见的文档类、脚本类、多媒体类、可执行程序；<br>8、支持不同视角展示全网态势，包括综合大屏、资产大屏、事件大屏、攻击大屏等；<br>9、支持对SIEM日志进行关联分析并将结果进行展示；<br>10、支持对事件执行剧本和动作，可以通过自动化处置预案对不同类型的事件和告警进行联动处置，并提供剧本流程设计服务；<br>11、支持灵活自定义编排威胁的响应处置流程，并支持多种执行节点包括：动作调度、剧本应用、决策器、过滤器、人工审批、人工录入等必要的关键节点，应支持与边界防火墙、上网行为管理、主机防病毒等安全组件进行联动处置。 | 满足 | 品牌：北京启明星辰信息安全技术有限公司<br>型号：TSOC-CSA-XDR8800XC | |

| | | | | |
|---|---|---|---|---|
| 25 | TAP 交换机 | ★1、满足信创要求，采用通用国产化 CPU 芯片，冗余电源和风扇；<br>2、25G/10G/GE 接口不少于 48 个（多模万兆光模块≥48 个）、100G/40G 接口数量不少于 8 个（100G 多模光模块≥6 个，40G 多模光模块≥2 个）<br>★3、整机吞吐不少于 2T，时延指标要求为不超过 10us，IPv4/IPv6 规则数量不少于 100W，去重性能不低于 400G<br>4、支持分光器输出及镜像链路接入，支持单、双纤输入输出<br>5、单台设备支持一对一、一对多、多对一、多对多等方式的流量汇聚和流量复制功能，支持将输入流量复制后进行不同过滤后输出<br>6、支持至少三级流量过滤，分别通过入口物理端口过滤，芯片内部环回接口过滤，出口物理端口过滤<br>7、设备所有业务接口支持自定义配置输入/输出(I/O）模式，可配置为输入端口用于接收流量，并支持纤收、发，也可配置为输出端口用于将流量输出到其他设备。<br>8、支持匹配 DSCP、ToS、CoS、TCP 标志<br>9、支持匹配 VXLAN VNI、GRE Key、GRE VSI 标签<br>10、支持至少匹配 4 层 VLAN Tag、匹配 3 层 MPLS 标签，并且不影响报文线速转发性能 | 满足 | 品牌（UNIS）<br>型号（S7800XP-48Y8C-G） |