|  |  |
| --- | --- |
| 设备名称 | 要求 |
| 国密SSL VPN | 关键技术要求：具备 IPsec、SSL VPN 商密功能，采用专用的IPSEC/SSL二合一商密产品；设备要求1+1冗余部署，双机热备，并使用VPN集群保障业务可靠性；SSL VPN最大并发数≥8000个；平台具备高度兼容性，支持手机、电脑、平板接入，兼容主流操作系统和浏览器；标准机架式设备，千兆电口≥6个，千兆光口SFP≥4，双电源；加密流量：350Mbps，最大并发会话数：150W；点到点 IPsec VPN隧道数≥4000个；SSL VPN授权数≥500个关键功能要求：统一入口：通过 WEB 门户提供安全接入所需的注册、审核、软件下载等功能，为用户提供PC机、移动智能终端统一接入客户端，设置网关设备接入入口，实现接入用户统一接入；VPN网关集群：提供终端到网关或网关到网关的传输加密、身份认证、权限控制等功能，通过负载均衡、链路汇聚实现VPN网关集群；统一认证：为安全接入的身份认证和权限控制提供支撑，提供用户集中认证、用户管理、访问权限统一控制等功能，支持包括短信认证等多种身份认证；管理与审计：提供安全接入平台的运行情况监测、平台设备的配置管理和用户行为审计等功能；安全防护：具备基于状态监测技术的防火墙功能，能够抵抗常见的网络攻击，能够进行包过滤或WAN、LAN、DMZ口之间访问控制；为了避免人为配置错误，产品必须支持对防火墙的过滤规则能够进行在线虚拟测试。 |
| 入侵防御设备 | 关键技术要求：配置基于专业多核硬件平台，非X86硬件平台，提供不少于12个千兆电口,不少于12个千兆光口，不少于4个万兆光口，设备扩展槽位≥1，支持并配置冗余双交流电源，根据光接口数量，满配千兆、万兆单模光模块；开启防护策略后整机网络层吞吐量≥20G，并发连接数≥2000万，新建连接数≥30万；支持虚拟IPS，数量不少于4；攻击特征库数量≥3000+，病毒特征库数量≥8000+，支持的协议识别数量≥800+关键功能要求：通过对流经该关键路径上的网络数据流进行4到7层的深度分析，能精确、实时地识别并阻断或限制黑客、蠕虫、病毒、木马、DoS/DDoS、扫描、间谍软件、协议异常、网络钓鱼、P2P、IM、网游等网络攻击或网络滥用，同时具备带宽管理和URL过滤功能 |
| WEB应用防火墙 | 关键技术要求：标准机架式结构型；配置4个千兆光口，6个千兆电口，2个万兆光口，双电源；应用层吞吐≥2Gbps，并发连接≥200万关键功能要求：支持对HTTP/HTTPS协议检测。配置包含SQL注入、XSS、CSRF等WEB攻击防护功能、URL访问控制功能、防盗链功能、DDOS攻击防护功能、网页防篡改功能、服务器负载均功能、报表分析及告警功能；支持IPv4静态路由、RIP V1/V2、OSPF、BGP，支持IPv6静态路由、RIPng、OSPFv3、BGP4+，支持IPv4和IPv6环境下的策略路由。支持IPv6手动隧道、6to4隧道和ISATAP隧道；与现有设备实现冗余；审计功能：审核统计经过设备的HTTP报文数量及会话，对出现问题进行分析，提出分析报告； 访问控制功能：用来对Web应用平台访问进行控制，包含网络层的访问控制以及应用层的访问控制； 网络管理：提供反向代理模式、转发控制、诊断工具等功能； Web攻击防护功能：Web防火墙核心功能，为Web应用平台提供安全防护，阻止攻击对应用平台造成不必要的损失 |
| 防病毒管理系统 | 防病毒系统\_服务端：建设防病毒系统一级管理中心平台，在结算中心业务网分别部署防病毒系统二级管理中心平台，支持虚拟化环境部署。管理中心平台实现集成可视化威胁数据概览、分区分域管理、终端统一运维管控、中心集中管理、威胁日志报表、策略配置、报表查看等功能。系统支持常用Windows, Windows Server,Linux以及麒麟、红旗、红帽等操作系统；支持定制防护策略以及策略细粒度配置；具有反病毒底层技术，反病毒引擎为本地反病毒引擎，不依赖云查杀；支持勒索病毒诱捕；支持横向渗透防护；含三年升级许可；具有场地无限终端授权防病毒系统\_客户端：提供客户端安全包；支持检测病毒木马、未知恶意代码，有效防御APT攻击，支持对蠕虫病毒、恶意软件、广告软件、勒索软件、引导区病毒、BIOS病毒的查杀。要求支持提供防病毒、补丁管理、运维管控等功能，支持系统支持常用Windows, Windows Server,Linux 以及麒麟、红旗、红帽等操作系统；含三年升级许可；具有场地无限终端授权 |