山航青岛分公司网络安全设备采购清单

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **设备名称** | **参数** | **数量** | **单位** |
| 1 | 防火墙 | (1)硬件要求：标准1U机架式设备，≥8个GE接口，≥8个千兆光口，≥2个万兆光口,1个Console口，≥1个USB接口，1个管理接口，配置冗余电源、冗余风扇，配置不少于1.8T的SSD盘，支持主主、主备等双机热备组网，三年硬件质保。 (2)性能要求：网络层吞吐量≥10G，IPS吞吐量≥5G，AV吞吐量≥4G，并发连接数≥220万，HTTP新建连接数≥13万，IPSecVPN吞吐量≥5G，SSlVPN最大用户数≥4000。 (3)下一代防火墙，支持应用识别，具备应用识别库升级服务、具备IPS入侵防御特征库升级服务，具备僵尸网络C&C防御服务，具备URL过滤服务，所配功能三年软件升级。 (4)安全控制与防护：支持提取命中指定策略的流量作为流量数据分析源，生成服务并根据管理员设置的替换规则自动生成符合管理员期望的安全策略。 (5)拥有自己的威胁情报中心，定期向系统推送热点威胁情报，支持在系统WebUI页面中查看热点威胁情报的详细信息。 (6)配置入侵防御功能：支持基于安全策略和安全域启用IPS功能；具备15000种以上攻击特征库规则列表；支持SQL注入、XSS防护，支持HTTP头域中的URL、Cookie、Referer、POST检查点配备防护策略；支持外链检查防护，支持自定义外链特性，类型支持HTTP、HTTPS、FTP等。 (7)支持SSL代理功能，能够解密HTTPS/POP3S/SMTPS/IMAPS流量，实现基于SSL加密流量的入侵防护过滤。 (8)配置负载均衡功能：支持在出站方向基于各链路的时延、抖动、丢包率和带宽利用率，实现智能选路、动态调整各链路的流量负载；支持用户自定义LLB模板实现对出站链路流量的控制及负载均衡；支持智能DNS功能：支持针对目的地址、子网、策略路由等实时探测，根据链路延时、丢包和抖动用自适应算法选出质量最优质链路。 (9)配置零信任功能：支持ZTNA服务端配置收集主机信息包括：操作系统版本，系统补丁，防病毒软件、状态及病毒库更新、防火墙状态、已安装和正在运行的进程或服务、文件路径、注册表信息等。 (10)支持IoT监控功能，通过分析流经设备的流量，识别视频监控专网中的网络摄像机和网络硬盘录像机等视频监控设备，并对识别出的设备进行实时监控，根据自定义配置对出现非法行为的视频监控设备进行阻断等操作。 | 2 | 台 |
| 2 | 安全DNS网关 | (1)硬件要求：CPU不少于12核心24线程，内存≥96G，芯片及操作系统均为国产。不少于2\*480G容量SSD硬盘(需做RAID1)，不少于2\*4T容量SATA硬盘 (需做RAID1)，不少于4个千兆电口，冗余电源，硬件质保三年。 (2)串联解析性能≥30,000 QPS；旁路分析性能≥100,000 QPS。提供高效稳定的DNS解析，支持DoH（DNS over HTTPS）实现数据传输的加密，保障通信安全。支持先进的域名威胁检测技术，结合云端威胁情报，对潜在的网络威胁进行实时监控和防御。支持智能识别并拦截恶意域名，防止内部网络遭受攻击。支持上网行为管理功能，防止恶意域名、黑灰产域名通信行为。提供三年的域名威胁检测订阅服务。 (3)具备DNS公网解析的运营资质，供应商对公网DNS递归解析应有具备丰富的维护经验，递归解析服务每天解析量达到千亿次，每日服务的用户数达到2000万。  (4)支持用户本地通过DoH/DoT加密协议进行域名解析，对出公网的域名解析进行加密保护，能防止第三方对DNS解析的偷窥和篡改，保护用户隐私。 (5)威胁情报数量不少于1000万条，APT情报不少于4万条；情报包括：威胁家族、威胁团伙、威胁类型、感染平台、攻击特处置建议、公开分析等。 (6)支持管理员自定义拦截策略，检测的攻击类型包含：APT、僵尸网络、木马、蠕虫、病毒、勒索、后门、挖矿、钓鱼网站、动态生成域名(DGA)等威胁类型。 (7)支持按照威胁类型、威胁等级、拦截策略配置告警通知策略；支持按照资产分组选择告警通知范围；支持配置告警发送策略，告警通知方式支持邮箱、企业微信等。 (8)支持选定时间范围内的请求域名排行，包括域名、请求次数、告警次数、拦截次数、资产数、命中策略的类型等信息；域名标签包括威胁分类、ICP备案信息、用户自定义标签；支持关联展示域名ICP备案信息，包含主办单位名称、备案号及审核时间等；支持关联展示域名WHOIS注册信息，包括注册者、注册时间、注册邮箱、过期时间等；支持关联指定域名的拦截明细日志、域名详情；支持统计指定域名最近 7 天的解析结果；支持TOP域名统计结果导出。 (9)支持识别定位内网终端IP地址；支持查询选定时间范围内的活跃资产列表，列表包括资产IP、资产分组、DNS请求数、最近请求时间、威胁等级等；支持TOP活跃资产列表导出。 (10)支持展示资产的威胁等级、威胁类型；支持展示资产最近一个月的上网解析情况，并按时段标注访问恶意域名的情况；支持资产最近一个月威胁告警的展示和导出；支持对终端IP进行打标签，维护资产处置记录；支持接入DHCP日志，自动识别和关联资产主机名和MAC地址；支持自动化行为分析，标注资产的设备类型和操作系统。 (11)支持配置威胁域名拦截策略，系统对指定的威胁域名进行拦截；可选择的情报分类包括恶意软件、挖矿、钓鱼网站等；支持自定义策略生效范围；支持定义处置动作拦截并告警、仅告警；支持自定义拦截时返回的IP地址，默认情况下提供拦截页面，并且支持用户自定义拦截页面或者跳转的URL。 (12)支持配置内容分类拦截策略，系统对指定的内容分类进行拦截；可选择的内容分类包括色情、赌博、黑灰产等；支持自定义策略生效范围；支持自定义拦截时返回的IP 地址，默认情况下提供拦截页面，并且支持用户自定义拦截页面或者跳转的URL。 (13)支持生成安全运营报告、综合分析报告、威胁事件报告、威胁告警列表等。 (14)支持用户自定义域名及解析地址，支持A和AAAA记录。DNS服务会优先自定义解析配置给客户端返回解析结果。 (15)支持对指定域名进行分组转发，支持将不同域名的请求转发至不同的DNS服务组。 | 1 | 台 |