附件5 产品需求

**公有云防火墙需求（2台）**

|  |  |
| --- | --- |
| 指标项 | 指标要求 |
| ★总体要求 | 使用自有开发的安全操作系统，而非通用操作系统，设备部件中不包含美光产品； |
| 设备质保期不低于5年，设备原厂需提供针对本项目的原厂服务承诺函，并加盖原厂公章； |
| 接口和性能 | ★防火墙实配≥4个10GE接口，1个管理口； |
| ★并发连接数≥400万；  ★每秒新建连接数≥18万； |
| ★整机处理能力≥20Gbps； |
| 支持透明、路由、旁路部署方式； |
| 支持VLAN类型接口，支持二层透明部署，支持旁挂部署； |
| ★支持静态路由、策略路由、OSPF路由协议； |
| 支持链路接口聚合功能，将2个或者更多的物理链路组合成一个有更高带宽的逻辑链路； |
| 支持nat地址映射技术； |
| 安全特性 | ★实配IPS功能、具备应用特征识别功能; |
| 访问控制 | ★访问控制策略支持基于源/目的IP，源/目的端口，源/目的区域，用户（组），应用/服务类型的细化控制方式； |
| 路由、NAT | 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IPv4/IPv6 双栈； |
| 管理功能 | 支持Web管理、串口管理、SSH管理等多种不同方式； |
| 权限管理 | 支持管理员角色与权限管理。可针对不同管理员所管理的各功能模块设定不同的管理权限； |
| 日志功能 | 支持管理员审计日志的分类实现； |
| ★日志存储时间不少于180天； |
| 支持查看CPU使用率、内存使用率、磁盘使用率、CF使用率、风扇状态、电源状态、CPU温度、主板温度； |

**用户区出口、互联网入口防火墙需求（4台）**

|  |  |
| --- | --- |
| 指标项 | 指标要求 |
| ★总体要求 | 使用自有开发的安全操作系统，而非通用操作系统，设备部件中不包含美光产品； |
| 实配冗余电源； |
| 含5年软硬件质保，5年规则库升级服务，设备原厂需提供针对本项目的原厂服务承诺函，并加盖原厂公章； |
| 接口和性能 | ★防火墙实配≥8个1GE电接口，≥4个10GE光接口，光接口至少配备4个光模块； |
| ★并发连接数≥400万；  ★每秒新建连接数≥18万； |
| ★整机处理能力≥20Gbps ；具备L2-L7层防护能力，应用层处理能力≥16Gbps； |
| ★支持透明、路由、旁路部署方式； |
| 支持VLAN类型接口，支持二层透明部署，支持旁挂部署； |
| ★支持静态路由、策略路由、RIP、OSPF、BGP、ISIS等路由协议； |
| 支持虚拟防火墙技术； |
| 支持链路接口聚合功能，将2个或者更多的物理链路组合成一个有更高带宽的逻辑链路； |
| 支持IPV6隧道； |
| 支持nat地址映射技术； |
| 安全特性 | ★实配IPS功能，实配IPS吞吐不少于10G; 实配AV功能，实配AV吞吐量不少于4G； |
| 支持防止DoS & DDoS攻击； |
| 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；  支持最大50层的病毒压缩文件检测和阻断，提供第三方检测报告 |
| 可识别应用层协议数量≥6000种，支持URL识别能力和URL地址识别库，云端URL识别库≥1亿，系统预定义IPS签名数量≥20000，CVE和CNNVD编号的签名条目数不得少于10000； |
| 访问控制 | ★访问控制策略支持基于源/目的IP，源/目的端口，源/目的区域，用户（组），应用/服务类型的细化控制方式； |
| 支持对HTTP，FTP，SMTP，POP3协议进行病毒文件检测； |
| 支持针对单个IP连接数限制； |
| 支持基于源、目的、应用三种条件做会话数限制； |
| ★对现有防火墙进行访问控制策略梳理、优化； |
| ★路由、NAT | 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IPv4/IPv6 双栈； |
| 支持路由类型、协议类型、网络对象、国家地区等条件进行自动选路的策略路由； |
| ★VPN | 支持IPSec VPN； |
| 支持基于路由的 VPN； |
| 产品支持IPSec VPN智能选路功能，根据线路质量和应用实现自动链路切换； |
| ★管理功能 | 易于安装和管理，提供命令行和图形化用户接口（GUI）； |
| 支持Web管理、串口管理、SSH管理等多种不同方式； |
| 支持Syslog、SNMP V1/2/3； |
| 集中管理 | 支持集中管理，可以集中下发防火墙策略；防火墙集中管理的范围包括防火墙设备状态监控、日志存储、日志搜索、日志审计、设备配置、策略配置、版本管理等； |
| 权限管理 | 支持管理员角色与权限管理。可针对不同管理员所管理的各功能模块设定不同的管理权限； |
| 日志功能 | ★产品支持多条件的安全日志组合查询，查询条件包括但不限于日志类型、日志级别、生成时间； |
| 产品支持多种安全日志存储方式，至少包括防火墙本机、日志服务器等不同方式； |
| 支持管理员审计日志的分类实现； |
| ★日志存储时间不少于180天； |
| 运行状态监控 | 支持集中的防火墙运行状态监控功能： |
| 能够动态监控防火墙的处理器、内存、存储设备的当前状态； |
| 能够动态监控防火墙各端口的流量和数据包数量； |
| 能够动态监控防火墙当前并发连接数； |
| 支持查看CPU使用率、内存使用率、磁盘使用率、CF使用率、风扇状态、电源状态、CPU温度、主板温度； |
| 报表功能 | 支持报表功能，支持标准的报表模版，支持定制报表； |
| 定制报表 | 支持业务流量趋势报表的导出功能，添加报表导出任务后，系统可按照报表任务指定的周期和报表格式自动导出报表，并将报表发送至指定的收件人，同时支持手动导出报表； |

互联网出口抗DDOS需求（2台）

|  |  |  |
| --- | --- | --- |
| 需求 | 要点 | 详细说明 |
| 部署要求 | 硬件 | 为硬件设备，具有完全自主知识产权的专用安全操作系统，稳定可靠；  设备部件中不包含美光产品；  关键部件冗余设计，实配冗余电源；  ★支持设备在断电, 过载及重启时自动Bypass功能,保障业务正常；  ★设备同时支持ipv4与ipv6防护；  ★含5年软硬件质保，5年规则库升级服务，设备原厂需提供针对本项目的原厂服务承诺函，并加盖原厂公章； |
| 端口 | ★支持多个接口同时运行, 设备形态≤1U，单台实配1G电接口≥8（包含硬件bypass端口），10G光接口≥2，光口须满配光模块。  支持接口扩展，最少可扩展至12个1G接口（即至少6路接入）；  端口支持状态联动和端口捆绑；  专用带外管理接口； |
| 性能 | ★设备攻击清洗能力≥3Gbps ，最大并发连接数≥200万；  每秒新建连接数≥30000，小包防御能力≥150万； |
| 部署 | 支持透明串联部署，  支持旁路部署方式； |
| 防护要求 | 防护要求 | ★支持基本的网络层、应用层DDOS攻击检测及防护，包括但不限于：SYN Flood、UDP Flood、ICMP Flood、DNS Flood、HTTP Flood、HTTPS Flood等；  ★具备DNS防护功能，具备不少于4种针对缓存DNS服务器及授权DNS服务器专用的DNS防护手段；  支持HTTP CC攻击防护，需支持配置防护类型、POST反弹、周期、防护阈值、黑/白名单生效时间、黑名单阈值等策略；  支持空连接攻击防护，包括TCP、HTTPS空连接攻击防护；  对IP地址扫描、端口扫描、漏洞扫描等行为识别，并加入黑名单；  支持肉鸡防护，对源IP的URL进行识别防护肉鸡攻击。  支持自定义放大攻击防护功能。支持对DNS、SSDP、NTP、CLADP、MEMCACHED等常见反射放大攻击进行识别防护，同时支持用户自定义攻击特征进行反射放大攻击防护；  支持针对协议头中各字段配置自定义过滤策略，字段包括但不限于：Method、Cookie、Host、Referer、Request URI、Verion、User-Agent等；  支持通过异常流量清洗运营管理平台，综合管理整网硬件设备策略部署，一键部署检测策略、防护策略、告警策略以及黑洞策略模版，针对相同类型业务可快速部署防护策略，简化固化日常运维管理流程，提升抗DDOS攻击响应速度；  可对IPv6环境下的攻击防范；  支持根据报文特征进行自定义攻击防护类型，通过这种方式防护未知攻击防护，可提供基于报文长度、报文ID、TTL、源IP、目的IP、序列号、确认号、源端口、目的端口、flag标记、key偏移、key长度等进行匹配的模式匹配规则； |
| 管理要求 | 管理方式 | 系统支持集中管理，可以支持http，https登陆，使用web操作，可多用户同时登陆管理中心； |
| 认证类型 | 设备登录认证支持本地认证和Radius认证。 |
| 设备运行展示 | 可视性，直观展示当前及历史的设备运行状态（包括CPU、内存使用情况）；  能实时显示攻击事件、流量、系统运行状况等信息等； |
| 日志报表和网管 | ★日志保存时间不少于180天；  系统支持以中文图表形式输出流量报表、安全报表、综合报表；支持doc、excel、pdf等格式的报表生成，并支持通过邮件等多种方式输出，并对日志可通过多种方式进行进行聚合，包括但不限于源地址、目的地址、威胁名称等；  支持自动抓包及特征提取功能，抓包分析维度至少包括协议、源IP、目的IP、源/目的端口等； |
| 升级更新 | 支持配置文件导入导出，用于设备配置备份和紧急恢复。  系统升级方式，至少提供自动在线升级、离线升级两种方式之一；  无已知安全漏洞，后期如有漏洞需及时制定升级方案进行相关升级； |
| 其他要求 | 标准服务 | 标准技术支持服务，包括但不限于方案设计，产品配置安装，硬件质保, 技术400电话，功能软件升级，产品培训等； |

**Waf需求（1台）**

|  |  |
| --- | --- |
| 指标项 | 具体参数要求 |
| 硬件要求 | ★标配网口≥4个千兆自适应电口（含bypass），4个千兆自适应光口（含bypass）；  ★含5年软硬件质保，5年规则库升级服务，设备原厂需提供针对本项目的原厂服务承诺函，并加盖原厂公章；  标准机架式硬件设备≤2U；  硬盘容量≥2TB；  USB口≥2 ；  串口：RJ45口\*1 带外管理端口》1个100\1000M自适应电口；  电源：双电源。 |
| ★性能要求 | 网络吞吐量≥8Gbps；  HTTP应用吞吐量≥6Gbps，HTTPS应用吞吐量≥1.5Gbps；  HTTP最大并发数≥35万； HTTPS最大并发数≥6.5万； |
| 部署方式 | 支持透明桥接、透明代理、反向代理、旁路部署等多种部署模式。 |
| 运行模式 | 透明桥部署下，不修改任何数据包，不维持TCP会话，设备故障时不中断TCP连接 |
| 链路聚合 | 支持Portchannel |
| 服务自发现 | 支持自动发现网络环境中存在的Web业务系统，记录服务器的IP、Port、域名等信息。 |
| 联动阻断 | 支持与现有态势感知平台对接，发送安全日志至态势感知平台进行汇总分析，同时支持与态势感知联动实现对未知威胁的感知拦截。 |
| 威胁情报 | 支持威胁情报库在线同步，可主动发现恶意IP发起的访问行为，并进行告警和拦截，威胁情报库支持离线更新。 |
| ★C&C攻击防御 | 可有效进行C&C攻击防御，支持根据细粒度检测条件对CC攻击进行检测和防护:匹配条件由URL参数、请求头部字段、目的IP、请求方法、地理位置组成；测量指标由请求速率、请求集中度、请求离散度组成;客户端检测对象由IP、IP+URL、IP+UserAgent等参数组成;支持从请求头字段获取真实源IP地址。 |
| 客户端安全防护 | 支持客户端安全防护，插入特殊的HTTP报头以保护客户端免受相应攻击，增加安全报头如X-Frame-0ptions、X-Content-Type-Options、Content-Security-Policy，以免客户端免受相应攻击。 |
| Webshell检测 | 内置Webshell检测规则，可以对上传的文件内容进行检查，防止恶意Webshell文件上传，对已经上传的Webshell发起请求的行为进行拦截阻断。 |
| ★Web应用安全防护 | 可防御OWASP TOP 10所公布的WEB应用程序安全风险，如：Web蠕虫、缓冲区溢出、自动化漏洞扫描攻击、恶意编码、强制登录、目录遍历、WEB平台及WEB应用程序已知漏洞、Cookie注入、XSS、CSRF、SQL注入、XML注入、OS命令注入、文件包含、代码注入、SSRF、敏感目录访问、可疑文件访问、未授权文件上传、恶意文件上传 |
| Web应用模型学习 | 支持流量学习技术，自动创建合法用户对Web应用的行为的安全模型，模型包括URL、参数等信息 |
| 流量学习的安全模型能够根据应用的更新迭代再次自动更新 |
| ★系统支持根据流量学习自动生成安全策略，能据此够检测到偏离流量学习的访问，安全策略不依赖于特征（库）升级 |
| 智能语义分析 | 内置对SQL注入、XSS攻击检测的语义分析规则。 |
| 扫描器安全检测 | 内置安全规则可有效识别Acunetix、nessus 、WebScan、Webdump、AppScan等扫描器的扫描行为。 |
| ★Bot识别 | 内置安全规则可有效识别baidu、google等常见网络爬虫的访问行为。 |
| 敏感数据泄漏防护 | 支持定制个人敏感信息数据，对服务器返回的敏感个人信息数据进行拦截并进行敏感信息替换。 |
|
| 日志分析 | 支持网站正常流量审计能力，支持记录、查询所有用户对网站的访问情况，包括访问的URL、客户端IP、服务器返回的状态码。 |
| ★Bypass功能 | 设备支持不少于4个电口和2个光口的Bypass功能，同时具备软件假死状态时流量自动放通功能 |
| 规则库更新 | 规则库支持手工、在线升级两种方式，在线升级可支持规则定时检查新版本和在线更新，确保WAF能够针对新型的、突发型的Web攻击进行防护，规则库平滑更新，无需设备重新启动或重启服务 |

**备注：★项为必须满足项。**