负载均衡技术参数要求

| **指标** | **指标项** | **规格要求** |
| --- | --- | --- |
|  | 知识产权 | \*国产品牌，具备完整自主知识产权； |
| **硬件规格** | \*投标产品应至少提供6个10/100/1000M自适应电口和4个千兆光口，配4千兆多模光模块需要时可扩展4个万兆接口或14个千兆电口；  |
| 性能要求 | **吞吐量** | **\*设备最大四层吞吐不低于10Gbps；**  |
| 最大并发连接数 | \*不少于800万。 |
| **每秒新建连接数** | **\*每秒四层新建不少于30万/秒** |
| 功能要求 | 部署模式 | 支持路由、旁路部署，以及三角传输 |
| 设备形式 | 必须独立专业负载设备，非插卡式负载均衡设备。 |
| 高可用性 | 支持AA，AP工作模式，IP地址可在设备间漂移，根据设备状态将流量牵引到主设备。支持包括半连接，全连接会话信息全状态同步；支持会话保持信息同步；以保障业务不间断切换。 |
| 支持标准VRRP协议。 |
| N+1集群部署：可以实现两台以上设备集群部署，一台设备充当在线备份，各设备可以是不同的软件版本和型号，实现弹性扩展。 |
| 多合一功能集成 | 单一设备即可同时支持包括链路负载均衡、服务器负载均衡，全局负载，应用加速，智能DNS，单边加速、虚拟化等功能。无需额外购买相应授权。 |
| L4服务器负载均衡 | 支持SNMP方式动态读取服务器运行状态进行算法调节；支持轮询、加权轮询、加权最小连接、动态反馈、源IP哈希等算法。 |
| SIP负载分担（基于UDP及TCP的负载分担）；流媒体负载分担（RTSP\MMS） |
| 对于源，目的IP相同的UDP访问，可以对每个报文进行分类转发，保证流量负载的均衡性。可以对Radius等接入认证服务器做基于每用户的负载均衡，并且保证每个用户的请求分发到相同的服务器。 |
| 服务器过载保护：支持服务器每秒新建连接和会话数限制，保证分担任务不超过其负载能力。 |
| 支持通过Vcenter自动获取虚拟机状态，并将流量根据配置的负载均衡算法自动分配到各虚拟机。支持虚拟机管理，可监控虚拟机cpu占用率，内存占用率，健康状况，连接数等的状态；并根据以上条件对虚拟机进行关闭，挂起，重启，开启等操作。 |
| L7服务器负载均衡 | 通过应用层代理，可解析客户端请求内容， 并根据客户端请求头域做内容分发，将访问不同内容的请求代理到相应服务器上；并将响应数据代理到对应客户端。例如对图片类、文字类的请求，分别转发到对应的图片、文字服务器，支持基于Cookie、User-Agent、URL、HTTP头的分担模式 |
| 服务器敏感信息保护：HTTP头擦除、重定向信息改写、COOKIE加密设备接收到的HTTP流量时，可以按指定的规则对其内容进行管理，完成对出入的HTTP流量的检查、过滤、修改。主要包括：合规性检查、报文内容修改、重定向等功能。 |
| 支持Http协议重写：可以把HTTP请求自动重写为HTTPS协议，实现HTTP到HTTPS的无缝切换 |
| 对于客户端与服务器需要多次交互过程才能完成交易的访问（特别是身份认证系统）；可以根据上一次交互过程的处理结果，分发后续的客户请求，保证相关的客户端请求都由一台服务器完成，支持基于IP地址、Cookie、SSL session id、Server-ID in URL Query、Custermer-ServerID、Rule Based等模式。 |
| 服务器健康检查 | 支持主动式健康检查，包括ICMP、TCP、UDP、FTP、HTTP、HTTPS、LDAP、NTP、POP3、Radius、SMTP、SNMP以及自定义的多重服务器健康检查机制。 |
| 基于业务的状态检查：允许用户自定义检查数据流使之贯穿整个业务系统，允许用户设置GET\POST方法模拟客户提交内容，并自定义服务器返回数据检查点来判断业务系统是否工作正常。 |
| 支持定期生成服务器健康状态报表。 |
| 应用系统加速 | 免费开通压缩、缓存、TCP连接复用、SSL协议卸载等功能，无需额外购买相应授权。 |
| 支持SPDY技术，通过HTTP协议的增强，实现数据流的多路复用、请求优先级及HTTP报头压缩技术，用以最小化延迟、提升网络速度、优化用户的网络使用体验。保障系统安全性的同时，实现业务加速效果。；  |
| 支持将客户端发送的多个HTTP请求封装在一个TCP数据包内，减少网络负载，避免单个HTTP延迟导致的重传、阻塞。实现http协议加速。 |
| 可自动识别移动终端的访问，并将请求的图片进行优化，将图片进行转码后传输，减少图片传输的流量，并适配移动终端展现。  |
| 支持对WEB服务器的浪涌保护功能，通过控制缓存请求连接的速率， 阻止猛增的大量请求进入您的服务器，从而防止服务器过载，在服务器达到其最大容量时，提示页面，使后续用户自动等待，避免反复刷新。 |
| 全局负载 | 支持标准DNS服务器功能，支持多种DNS 记录 ，包括A ，NS，CNMAE，TXT，MX，PTR记录。支持DNS 授权区域，可将DNS名称空间划分为区域来进行管理。可转发DNS请求，支持 forward-only  forward-first 两种DNS转发模式。 |
| 基于DNS方式，在不同地域数据中心之间实现流量牵引； |
| 支持地域优先、静态就近性、动态就近性、基于权重、基于session、基于服务器数量；  |
| 支持配置信息同步、状态信息同步 |
| 多链路负载均衡 | 至少支持对10条以上链路进行流量均衡，不需要额外的授权。 |
| 通过TCP丢包预测，快速重传和恢复机制，提高TCP协议的数据传输速度，当广域网链路出现延时和丢包的情况时，可明显改变TCP传输效率，提升传输速率不用在用户终端上安装任何插件和软件，即可提升链路访问速度，节省带宽资源。 |
| 智能DNS：实现链路智能Inbound访问，避免跨运营商访问。 |
| 支持内网用户上网DNS透明代理，DNS透明代理对内网用户访问外网资源的DNS解析过程进行优化，可以通过对多条链路发起DNS请求探测，根据探测结果结和预先设定的策略，将DNS请求转发到不同的服务器，避免出现因为DNS导向问题导致的某条链路拥塞，某条链路空闲的情况。 |
| 根据用户实时访问情况，动态探测每条链路到用户访问服务的的目标可达性，及延迟信息；并计算出最佳访问链路。并且随着链路质量的变化，可自动调整重新选择最佳发送链路。 |
| 业务的带宽保障：在链路拥塞时，支持对指定业务分配优先级，高优先级的业务优先处理，可以实现对指定业务的带宽保证，链路空闲时，所有业务可以任意使用带宽，链路拥塞时，可保障指定业务使用带宽。 |
| 应用路由：支持常见流媒体，P2P软件，网络游戏， IM ，股票软件的检测识别；可将对相应流量分配到期望的目标链路；并可进行速率控制。 |
| 网络特性 | 支持动态路由协议RIP，OSPF，BGP，不需要单独授权。 |
| 支持且提供设备虚拟化功能：一台物理设备可以虚拟出多台设备使用；各虚拟设备间完全隔离，分别具有独立的管理员及配置，可运行相同或不同的业务。 支持虚拟设备CPU，内存，网络I/O等计算资源按需分配，支持VLan Tag 及接口的虚拟网络隔离。 |
| 支持V4/V6双栈，支持V4/V6地址转换,支持前缀地址转换，IVI，地址池，IPv4和IPv6混合环境下的四层服务器负载，链路负载，健康检查。支持DNSv6，支持基于IPV6地址的七层内容交换（URL负载、HTTP头擦除、重定向信息改写等功能）。 |
| 支持802.1Q VLAN，STP生成树协议 |
| 支持SNMP V1/V2/V3协议 |
| 可编程脚本语言 | 通过标准的TCL语言实现业务逻辑的可编程控制，通过编程方式支持根据任意数据段内容的负载均衡、HTTP头部内容按需改写等功能。可提供操作界面及工作原理说明 |
| 安全功能 | 标准四层防火墙功能：支持连接状态跟踪，可以根据五元组进行源和目标的基于状态的访问控制，支持时间表功能；具备防四层DDoS攻击能力； |
| 七层防火墙：通过代理方式解析HTTP请求， 可以根据头域中浏览器类型，Cookies，HTTP Header，目标URL进行访问控制；可以对访问请求进行丢弃，重置，以及重定向到其他页面；  |
| HTTP访问速率限制：通过代理方式解析HTTP请求，根据限速规则可以限制某个浏览器每秒钟对某个页面发送的HTTP请求数，超过这个数量将进行重置或重定向处理；可以有效防止用脚本对某个固定页面的反复刷新； |
| 防HTTP-DDoS：使用动态脚本鉴别技术，区分是正常的浏览器还是代理攻击程序，有效防止CC类攻击；  |
| 支持检测SQL/XSS注入变种/变形深层攻击行为，并进行告警，阻断等精确防御。 |
| 报表统计功能 | 内置硬盘≥1T |
| 支持标准SYSLOG格式日志信息，可以根据预置条件自动把日志信息发送给远端服务器。 |
| 支持统计虚拟服务和真实服务器的流量、访问次数、并发连接数。 |
| 支持自动或手动生成HTML和PDF两种格式报表；  |
| 界面及安全管理 | 支持全中文的管理界面和HTTPS方式登录、用户角色管理、多级授权管理。 |