**流量控制技术参数要求**

1. **资质要求**

|  |  |
| --- | --- |
|  | **资质名称** |
| 产品资质 | 《ISO 9001质量管理体系认证证书》 |
| 《计算机信息系统安全专用产品销售许可证》 |
| 《中国国家信息安全产品认证证书》（CCC认证或3C认证） |
| 《URL过滤自主知识产权证书》 |
| 《互联网内容审计自主知识产权证书》 |
|  |

1. **设备管理**

|  |  |  |
| --- | --- | --- |
| 一级特性 | 二/三级特性 | 招标说明 |
| 硬件参数 | 硬件接口 | 不少于4千兆电口、4千兆光口； |
| 性能规格 | 吞吐≥1.6G；支持带宽≥800M；最大并发连接≥200万；最大新建连接≥80000个/S；适用用户数5000人； |
| 专业流控 | / | 具备完备的流控功能 |
| 部署模式 | 网桥模式 | 设备支持网桥串接部署。支持网桥单链路、网桥多链路、镜像、重定向、网桥镜像混合和网桥聚合链路工作模式 |
| 旁路模式 | 设备支持旁路部署。支持单网口旁路监听、双网口旁路监听和聚合端口旁路监听工作模式 |
| 部署环境 | 支持IPV6环境 | 支持能够在同时有IPV4和IPV6的链路环境部署,并能够对所有链路上的流量按具体应用（如迅雷、QQ等）、用户进行识别、管理并统计。 |
| 支持MPLS环境部署 | 支持能够部署在MPLS链路中，并至少对具备2级标签的MPLS格式报文按具体应用（如迅雷、QQ等）进行识别、管理并统计。 |
| 支持GRE Tunnel环境部署 | 支持能够部署在GRE Tunnel链路中，并对报文按具体应用（如迅雷、QQ等）进行识别、管理并统计。 |
| 支持802.1q和802.1p环境部署 | 支持能够部署在802.1q及802.1p链路中，并对802.1q和802.1p格式的报文按具体应用（如迅雷、QQ等）进行识别、管理并统计。 |
| 可靠性 | 双系统冗余热备 | 支持核心系统应固化在电子芯片内，在硬盘损坏的情况下，系统应该能够正常运行管理。 |
| 双机冗余热备 | 支持支持双机热备部署方式，主机故障备机自动接管，策略依然有效，上网用户无感知。 |
| 桥口同步UP/DOWN | 支持当链路上游设备发生中断时，设备内外网口能够同步UP/DOWN，以便下游设备感知到网络异常，并借助OSPF机制实现流量的链路切换保护。 |
| 旁路保护 | 支持支持内置电口旁路和外置光口旁路，并且电口、光口支持同时旁路，电口支持独立旁路。 |
| 提供一键式Bypass按钮，以便巡检时快速手动触发旁路保护。 |
| 运维管理 | 管理方式 | 支持基于https加密的中文图形化管理界面。 |
| 支持设备及日志管理界面均支持基于IE与非IE内核的多种浏览器管理，管理终端不得安装插件，便于跨平台移动管理。 |
| 硬件接口 | 支持具备可管理的硬件串口:设备面板必须提供RJ-45或RS-232硬件串口，可供管理员通过超级终端用串口登陆配置系统，提供设备出厂化恢复功能。 |
| 日志&统计 | 日志中心 | 支持分布部署多台设备的用户上网日志，能够统一汇总到日志中心进行分析，同时要求日志中心支持Oracle大型数据库。 |
| 集中管理 | 支持能够对至少100台设备进行集中管理，包括集中监控各设备的运行状态、分析全网流量的应用分布、分析全网流量的设备分布、对所管理设备进行批量策略下发和调整、对所管理设备进行批量升级。 |
| 升级服务 | 软件升级 | 支持系统版本在线升级，并在界面实时展现升级完成百分比进度。 |
| 应用协议库升级 | 应用协议库每周发布一次更新。 |
| 支持应用协议库的自动与手动更新，支持自定义更新时间计划。 |
| 在界面上可以查看升级历史记录和版本更新情况。 |
| 在官网上有公开的应用协议库更新情况详细说明。 |

1. **功能特性**

|  |  |  |
| --- | --- | --- |
| 一级特性 | 二/三级特性 | 招标说明 |
| 设备状态 | 分析系统状态 | 支持展示CPU、内存、硬盘使用率，CPU使用率能够展示每颗CPU核的使用率 |
| 支持通过设备界面，一键式生成和导出系统运行健康状态报告，报告内容应包括：操作界面服务进程、底层系统服务进程、数据库读写、网卡数据包收发等各种进程以及系统工作模块的运行状态。 |
| 网络分析 | 分析网络负载 | 支持对系统、链路、通道、应用、用户、流速走势和指标进行分析。 |
| 支持对系统、应用、用户的总连接数和新建连接数走势和指标进行分析。 |
| 支持对系统、用户的总包速率和64B小包速率走势和指标进行分析。 |
| 支持对系统活跃IP数走势和指标进行分析。 |
| 支持在相同时间范围条件下，监控和报告等界面展现的流速趋势峰值保持一致。 |
| 分析流量构成 | 支持对应用及用户的流速排名、连接排名、包速率排名进行分析，可选择的TOP排名数量不小于100。 |
| 支持基于应用大类，进行流速走势、排名、累计流量百分比等分析。 |
| 支持基于应用、用户、时间等自定义条件，对流速、连接数、包速率等信息进行走势和排名分析，同时支持应用和用户维度间的信息关联钻取。 |
| 支持应用、用户维度之间进行信息关联钻取分析，分析内容包括流速、连接数、包速率等维度的信息。 |
| 支持自动发现网络中的未知端口流量，并分析其流速走势、应用排名、对应的用户IP信息。 |
| 分析流量流向 | 支持对应用流量去往各运营商的流速叠加走势和累计流量进行分析。 |
| 支持对应用流量的内网服务IP排名，以及外网访问IP排名进行分析。 |
| 分析引流效果 | 支持对策略或应用的引流流向、引流流速趋势、引流百分比、引流流速及累计流量进行分析。 |
| 支持对引流前后，各链路上的应用流速叠加趋势、流量占比等进行对比分析。 |
| 支持对应用流量去往教育、电信、联通、移动等运营商的流速叠加趋势进行分析。 |
| 分析业务质量 | 支持对指定应用的总延时、RTT延时、丢包率、重传率、流速等趋势进行分析。 |
| 支持根据延时、丢包率、重传率、流速等指标，综合评估应用的整体质量指数，并查看质量指数的变化趋势。 |
| 支持查看指定应用的最差连接，包括延时、丢包率、重传率、流速等各项指标，以及不满足阈值要求的连接详情。 |
| 应用识别 | 应用协议库规模 | 支持对P2P、游戏、IM等各类国内主流应用进行识别、管理和统计，支持的应用协议数量不低于3300种。 |
| 应用识别准确率 | 应用协议库对各类网络应用的识别准确率，需达到95%以上。 |
| 识别移动互联网应用 | 支持对移动互联网应用流量进行识别、管理和统计，支持的移动应用数量不低于700种，并且应用种类包括浏览器、音乐视频、气象交通、财务支付、新闻阅读、社交网络、金融理财、游戏、聊天、系统工具等各种类别。 |
| 自定义应用 | 支持基于五元组（IP+端口+协议类型）或URL方式设置自定义应用 |
| 支持基于GET、POST、CONNECT、Host、Referer、User-Agent、后缀名等参数，对HTTP应用进行精细化的自定义 |
| 支持基于文件名特征字或文件类型，对迅雷进行精细化的自定义 |
| 流量管理 | 流量管理机制 | 支持至少3级带宽通道，并按照应用大类/应用组/子类应用，或部门/子部门/用户组的逻辑嵌套关系，配置流量管理策略。 |
| 支持提供策略配置模板，通过1条策略，即可一键式配置对每IP或每IP群组的流量管理策略。 |
| 支持通过调节TCP滑动窗口的大小，与数据发送方自动协商数据发送速率，从而实现流量控制。 |
| 支持对被封堵的应用连接进行Reset操作，避免P2P等应用被阻塞后，产生大量试探性连接的重发而造成网络设备性能下降。 |
| 流量管理条件 | 支持同时使用时间段、Vlan（ID和优先级）、连接数（并发连接数和新建连接数）、内部和外部用户（IP、IP范围、掩码方式）、应用协议、流速阈值、带宽占比等管控条件，进行灵活的策略配置。 |
| 流量管理手段 | 支持对应用流量分配最小的保障带宽，并且允许其它应用，对空闲状态下的保障带宽进行借用。 |
| 支持对应用流量分配最小的静态预留带宽，无论带宽资源是否空闲，其它应用都不能借用。 |
| 支持基于内外网IP群组中的用户数变化，动态为每个IP平均分配带宽资源。 |
| 支持对应用流量中的多条Session连接，平均分配带宽资源。 |
| 支持能够对应用流量进行阻塞。 |
| 支持对应用流量进行带宽上限管理。 |
| 支持对并发连接数和新建连接数进行限制。 |
| 支持对某时间周期内的流量额度进行限制。 |
| 支持至少8个优先级，以便控制带宽通道之间对剩余带宽资源的争用权。 |
| 支持免管控特权IP，避免普通用户的流量管理策略，对特权用户造成影响。 |
| 智能选路 | 应用引流 | 支持在无需其它网络设备配合的情况下，由单台设备将应用流量，从源链路引流至目标链路。 |
| 支持由单台设备进行应用流量识别和标记，并在路由器策略的配合下，识别已标记的应用流量，并将其从源链路引流至目标链路。 |
| 支持基于细分的应用类别或URL网址进行引流，细分的应用类别应包括：网络游戏、Web游戏、P2P下载、P2P视频、Web视频、股票软件等类。 |
| 支持将P2P等引流流量的下行流量，从指定目标链路的LAN口下行返回，避免占用源链路下行带宽。 |
| 支持在引流链路故障时，无需人工干预，系统能够自动将流量切换到其它链路。 |
| 流量均衡 | 支持多链路场景下，一旦主链路流量超过警戒阈值时，自动切换指定用户流量至备用链路。 |
| 支持在多链路场景下，系统根据用户访问的目的IP地址所属的运营商，自动选择对应的链路出口。 |
| 镜像重定向 | 支持同时将4条链路的网络流量，复制并镜像给第三方设备进行审计处理。 |
| 支持基于应用对镜像流量进行过滤，避免P2P下载、Web视频等流量，造成第三方设备无效负载增加。 |
| 支持将应用流量分发给第三方设备（如审计过滤设备），经第三方设备处理后再回注到本设备，实现流量清洗。 |
| 安全防护 | 防DDoS功能 | 可通过配置阈值，实现对DDoS流量的检测，包括TCP SYN，UDP，ICMP，DNS； |
| 对超过阈值的流量，可选择忽略、告警、丢弃、丢弃并告警处理方式，实现对DDoS攻击的防护 |
| DDoS防护日志 | 详细记录系统DDoS攻击信息，包括时间、类型、IP地址，实现对DDoS攻击的溯源 |
| 异常流量防护 | 支持基于流速、包速率、连接数、新建连接数、丢弃流量速率、丢弃包速率、丢弃连接数、流量方向，报警等级等参数，设置通道报警对象。 |
| 支持基于包速率、上传速率、新建连接速率、小包速率配置用户防护规则。 |
| 支持对指定流量异常的IP进行屏蔽，并在次日解除暂时屏蔽。 |
| 异常告警 | 支持以邮件方式发送报警信息。 |
| 支持日志量超过安全阈值时，系统自动报警和进行防护。 |
| 支持基于IP或者网口状态的方式，对链路故障状态进行检测。 |
| 支持对CPU使用率、硬盘使用率、硬盘存储空间、引擎工作异常、网卡丢包等系统异常情况下进行告警。 |
| 支持对网络流速、并发连接数、新建连接数、包速率等超出安全阈值时进行告警。 |
| 支持对系统授权过期进行告警。 |
| 支持设备与日志中心等外围设备异常断开情况下进行告警。 |

1. **质保**

设备质保不少于三年。