# 采购人需求

## 一、项目概况

1、建设目标

哈尔滨工业大学现拥有4万网络用户，为保障出口网络使用正常，多年来我校在校园网出口采用流控设备保障正常网络用户用网带宽，限制异常用户网络流量。我校近期刚扩容了移动40Gbps出口链路，现有出口总带宽从21.2Gbps直接升到57.2Gbps，出口带宽突发增长速度远超之前的网络规划。现学校出口下行网络流量峰值高达30Gbps，出口总流量超过34Gbps。原有IPv4和IPv6流控设备已不能满足现在的实际带宽需求。需要对出口流控设备进行更新，实现对学校出口网络流量进行有效管控。

2、预期的建设效果

项目建成后能对哈尔滨工业大学内网流量进行有效的采集和识别，分析各种应用协议的流量构成和占比，做到流量可视化；满足学校之前提出的能对出口用户流量进行有效的管理；能够及时准确地识别网络的异常流量，并能够对齐进行有效的控制和处理。通过监控网络流量的具体行为特征，启用流量控制和优化策略，有针对性的对低时延及业务敏感的流量进行优化和牵引，针对低附加值和高带宽占用的流量进行有效的控制。能够实现宽带互联网用户访问行为全面管控，包括用户带宽管理，用户访问优先级管理，用户行为记录，用户行为数据统计等。能够满足公安部151号令中对网络安全的要求,日志服务应满足国家相关规定，至少保存180天运行日志。统一全校内部网络Internet出口使得物理资源可以按需调度，物理资源得以最大限度的重用，减少建设成本，提高使用效率。即能够实现总硬件资源占用量降低了，而每个业务得到的服务反而更有充分的资源保证。

## 二、项目需求描述

我校网络拓扑情况如图1所示，校园IPv4/IPv6核心网络，由冗余核心路由器集群分别通过两条40GE链路经过出口层流控设备，再到冗余出口防火墙集群。所有出口流量均分别经过出口流控设备，由出口流控设备对出口网络流量进行管控，实现可按应用进行带宽管理和按IP地址进行带宽管理。



图1：网络拓扑

## 三、项目技术要求

1、总体要求

出口流控设备位于校园网出口核心位置，对学校所有出口流量进行识别，并对用户IP出口带宽进行管控，保障网络用户出口合理使用带宽，限制无节制带宽。同时能够按应用对特定有害应用进行封堵，进一步保障学校网络安全。

校园出口流控项目须由原厂工程师安装调试，设备质保期不少于五年。

2、关键技术指标

（1）产品技术参数要求如下：

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **产品名称** | **技术参数要求** | **数量** |
| **1** | 流量控制设备 | 1. ★设备整机最大吞吐量>=80Gbp，并发连接数最大支持1800万，并发IP数最大支持60万，每秒新建会话数 >=100万/秒，PPS（包转发率）>=1800万，NAT模式下单WAN IP并发会话数>=90万； 2. 支持软硬件bypass； 3. ★2U标准机架式设备，冗余电源，设备实配10G/40GQSFP+端口不少于6个，40GQSFP+接口不少于4个，配置配套单模模块，一个独立管理接口，一个console口，2个USB接口。 4. ★支持双OS备份，主OS故障时，备份OS自动切换，切换时间小于10毫秒；（提供证明文件并加盖原厂公章） 5. 支持的N（N>=12）条物理链路，数目和硬件接口数有关，不受软件限制；（提供证明文件并加盖原厂公章） 6. 支持对整个系统进行全局策略管理和分析统计；支持对各条链路进行独立的策略管理和分析统计；（提供证明文件并加盖原厂公章） 7. 支持路由、NAT、网桥和旁路分析的混合模式；（提供证明文件并加盖原厂公章 8. 虚拟LAN接口和WAN线路最大支持≥600条；（提供证明文件并加盖原厂公章） 9. WAN口支持PPPOE拨号功能，自动检测链路状态，断线后自动拨号和支持计划定时重播； 10. 每条线路独立健康检查；（提供证明文件并加盖原厂公章） 11. 支持端口映射，可以设置映射内网ip的某个端口或者某段连续的端口（如映射端口5000-6000）到某个WAN接口，或者某些WAN线路组成的线路群组上； 12. 支持DHCP SERVER，可以基于VLAN等条件分配IP地址，可以支持多个DHCP SERVER。（提供证明文件并加盖原厂公章 13. ★支持对P2P下载、 网络电视、网络游戏、Web视频(流媒体)和普通HTTP协议流量做应用分流。（提供证明文件并加盖原厂公章） 14. ★可根据网络应用查询实际使用中的应用组成、协议、首包接口、客户时延、服务时延、应用时延、流量等信息。（提供证明文件并加盖原厂公章） 15. 支持利用600条以上WAN线路进行分流；（提供证明文件并加盖原厂公章） 16. ★支持基于域名的路由；（提供证明文件并加盖原厂公章） 17. 支持600条WAN线路之间的负载均衡；（提供证明文件并加盖原厂公章） 18. 负载均衡模式支持源IP、目标IP、源IP加目标IP、4元组（源IP、源端口、目标IP、目标端口）四种方式； 19. 支持对2～7层流量的识别能力，特别是针对第 7层的应用识别能力，能够识别主要应用协议，并逐级细分P2P下载、网络视频、网络电话、游戏、HTTP协议的子类别和具体客户端名称，比如HTP协议---Web视频---土豆、网络游戏---移动游戏等； 20. 支持国内各类常见协议>=1000种，其中大型游戏>=300种，移动APP应用>=30种（将持续新增至>=200种移动APP应用），现网协议识别率 >= 95%（提供证明文件并加盖原厂公章） 21. 支持DPI、DFI、节点跟踪、主动探测、加密分析等多种技术，对已经采用加密技术的P2P类应用比如BT、迅雷、Skype、eDonkey、Qvod、PPFilm、百度影音等精确识别；（提供证明文件并加盖原厂公章） 22. 可以区分迅雷、网际快车等下载工具的HTTP下载和IE浏览器下载；支持“迅雷增强识别”，大幅度改进对迅雷加密流量识别；支持“P2P智能识别”，大幅度改进P2P加密协议识别；（提供证明文件并加盖原厂公章） 23. 协议精细分类且必须包含：移动浏览器（如iPhone手机上网）、应用商店（如安卓市场、手机报等）、云服务、网络支付（招商银行、兴业银行等）、移动游戏（手机游戏、iPad游戏）；（提供证明文件并加盖原厂公章） 24. 支持虚拟身份的识别，如QQ号码、MSN帐号、POP3帐号、新浪微博、百度贴吧等；（提供证明文件并加盖原厂公章） 25. 支持基于全局、链路、数据流向、共享用户、移动终端、应用协议/协议组和IP/IP群组的速率控制； 26. 支持允许、阻断、带宽限速等控制动作； 27. 可根据时间和在线用户数等条件使用不同的策略组来控制流量。（提供证明文件并加盖原厂公章） 28. 支持策略嵌套，在同一条策略中，既可以针对特定对象(IP或应用)进行总的数据通道控制，也可以单IP限速，同时可并列匹配“DSCP标记”等参数，实现策略的高度灵活性和简洁性；（提供证明文件并加盖原厂公章） 29. 控制参数包含：线路、数据流向、内网地址、外网地址、传输协议、应用协议、内网端口、外网端口、共享用户数、QQ用户数、移动终端数、执行动作、优先级、内网IP限速等；（提供证明文件并加盖原厂公章） 30. ★支持检测并控制网关“一拖N”行为功能；能够及时检测通过路由共享上网的PC个数；可以根据PC终端个数做条件，对流量做控制（提供证明文件并加盖原厂公章） 31. 支持基于IP地址的“优先级”调度功能，支持0-6七个优先级； 32. 支持同时基于应用协议和IP地址的优先级调度功能；（提供证明文件并加盖原厂公章） 33. 支持“动态IP限速”功能（智能调控）， 可在启用此功能的链路中，针对单个IP设置“加速比”、“减速比”、“速度维持时间”等参数，百分比模式设置；（提供证明文件并加盖原厂公章） 34. 支持设置“带宽使用阀值”功能，可对具体链路设置“带宽使用下限”和“带宽使用上限”，百分比模式设置； 35. 支持策略“启用”和“禁用”功能； 36. 基于应用协议/协议组，支持针对内网每IP的TCP、UDP和总并发连接数控制；（提供证明文件并加盖原厂公章） 37. 支持限制内网IP到外网特支持针对“DNS连接”的控制/不控制选项； 38. 可根据数据链路、外网地址、内网地址和应用协议/协议组、内网端口、外网端口等参数制定连接数控制策略；（提供证明文件并加盖原厂公章） 39. 支持第三方分类URL库手动上传，实现基于“类型”的URL过滤功能，URL库容量默认不低于10万条（可扩展）（提供截图并加盖原厂公章） 40. 可设置内网IP最大并发连接数，超过这个阈值的连接不再创建； 41. ★设备旁路模式下，支持URL重定向（提供证明文件并加盖原厂公章） 42. ★可根据源IP、目标IP、访问域名、所在线路等组合条件实现对域名访问的控制；域名控制方式支持阻断、劫持和重定向和QPS限制；（提供证明文件并加盖原厂公章） 43. ★可以对DNS QPS做限制，可以在一条策略里做总限制，同时对单IP再做一个子项限制；（提供截图并加盖原厂公章） 44. 可根据源IP、目标IP、访问域名、所在线路等组合条件实现对域名访问的QPS速率做总量控制和单IP控制；（提供证明文件并加盖原厂公章） 45. ★自动对移动终端型号进行识别，不依赖特征库（提供截图并加盖原厂公章） 46. 对移动设备的网络访问进行控制和管理；支持黑名单，当误识别时，将时别错误的移动终端类型放入黑名单，避免误识别；（提供证明文件并加盖原厂公章） 47. PPPOE SERVER支持与Radius认证计费系统对接，并能接收Radius服务器下发的限速，踢掉在线用户等指令 48. 可针对用户上线发布公告，用户到期提醒和过期提示 49. 支持外部BAS认证（PPPOE旁路功能） 50. 可提供整个系统、各链路的流量和连接数统计图表；可提供最近10分钟流量、累计流量、并发连接数统计图表实时显示各协议组的当前速率、连接数等统计信息，自动刷新；可提供最近一天、最近一周和最近一月的流量趋势图表；可提供上行流量、下行流量、并发连接数的“三日对比”趋势图； 51. 支持150万同时在线IP环境下，可实时显示每一个IP流量速率和当前各个应用的速率明细；可实时显示某个IP的当前速率及连接明细，以便于异常流量诊断（提供证明文件并加盖原厂公章） 52. ★可提供IP对应的身份信息，如QQ号码、MSN帐号、POP3帐号、微博帐号等；可根据应用速率、流量和连接数等条件进行排序；（提供证明文件并加盖原厂公章） 53. 年升级次数承诺总计不少于10次； 54. ★对于用户要求识别的非加密类应用协议，承诺在72小时内完成特征库升级支持； 55. 支持TOP连接排序，可以指定应用和IP条件进行IP（内网IP和外网IP均可）连接数排名统计，以快速定位攻击或被攻击IP（提供证明文件并加盖原厂公章） 56. 支持“垃圾包”检测及过滤功能；支持“IP分片”攻击检测及过滤功能；支持对异常流量IP的实时查询、日志反查功能； 57. ★支持端口镜像功能；可根据设置条件将类如迅雷、网桥设备上行方向、某IP/IP段、iPhone手机上网流量、未知协议等流量等镜像至指定网络接口，与第三方审计设备联动，便于用户做精细化、个性化的数据分析；（提供截图并加盖原厂公章） 58. HTTP管控中，特别支持将WWW访问流量转发至指定网络接口，供第三方审计设备深入分析用户的网站访问习惯、兴趣等运营数据； 59. 支持Web认证（可选“本地认证”或“第三方认证”）；支持Radius认证、AD域认证；支持“IP标注”功能；支持“管理日志”功能；支持“在线管理用户”显示及针对“非admin”强制下线功能；支持“系统告警”功能；支持“系统告警”远程输出及记录文件导出功能；支持“DDNS”远程管理设备 60. 支持云平台集中管理设备；支持VLAN；支持VLAN Trunk；支持QinQ；“应用分流”功能中支持VLAN-Tag； 61. 支持PPPOE帐号识别与IP关联统计功能；支持Radius帐号识别与IP关联统计功能；支持MAC黑名单功能；支持iftop功能，用来监控从某个网卡流入流量大的的Top IP，定位外网攻击源；支持ADSL定时重播；支持针对Gn接口数据包的解码，含GTP-C和GTP-U解码分析； 62. 认证方式有本地认证，radius认证，AD域认证，第三方认证，微信认证；在本地认证时，可以将用户分组，并可以对不同的组做不同的策略； 63. 可以旁路或串接模式下，深度分析RADIUS数据包，找到帐号和IP地址对应关系；可以旁路或串接模式下，深度分析RADIUS数据包，找到帐号的带宽限制参数，自动对相应IP做限速； 64. ★提供一个日志系统，日志系统支持会话日志，会话日志包含设备编号、接口、访问时间、源地址、目标地址、NAT地址、账号信息、域名、协议类型、7层协议名称、流量、运营商、地理位置一共13个元素。同时采用1:1 的日志输出，完整保留网络中的相关信息。 65. 支持虚拟身份查询。通过QQ号码，微信ID，邮箱地址，淘宝账号，手机IMEI信息来查询到对应的IP地址； 66. 支持“域名地图”，区域URL访问量数据分部图。例如：招生期间，可以看到那个省的用户对校园网主页，招生服务器访问排名。 67. 可以对使用校园网IP的地理位置定位，协助校园网管理者找出私拉校园网线路行为； 68. 日志系统提供校内任何IP的用户画像功能。可以分析该用户访问的地理区域，去往各个运营商比例，该用户的TOP协议排名图，用户访问流量趋势图，用访问连接趋势图和该用户访问域名排名、身份信息等； 69. 日志系统支持对任何URL去往运营商统计，并提供比例饼图与统计数值； 70. 日志系统支持“流量流向”统计功能，如去往电信、去往移动等，并提供比例饼图与统计数值； 71. 日志系统支持对校内提供HTTP或者HTTPS访问的域名进行统计，发现校内教育网IP使用校外域名的情况； 72. 日志系统支持对校内用户访问校外图书馆资源进行统计，提供对图书馆资源流量和下载排名，为我校明年购买图书馆资源作依据； 73. 日志系统支持对校内用户下载校外图书馆次数作统计，提供下载排名，发现恶意下载用户。 74. 日志系统支持TOP域名统计，提供校内用户访问校外的TOP URL统计； 75. 日志系统支持报表功能：   报表创建、PDF格式导出；  各类分项日志支持Excel格式导出；   1. 设备制造商具有公安部信息安全产品销售许可证。提供有效证书的复印件； 2. 设备制造商具有检测中心发布的《检测报告》； 3. 设备制造商具有软件著作权证书；提供有效证书的复印件 4. ★提供针对本项目的原厂商授权。   80. ★提供针对本项目的原厂商售后服务承诺。 | 4台 |

（2）本项目包含整体布线，其中主要线材要求如下：

单模光纤跳线：LC-LC/LC-SC双芯单模光纤跳线； 长度5-30米

多模光纤跳线：LC/LC双芯多模光纤跳线，OM3级别；

性能超过ANSI/TIA 568-C.3标准；

性能超过1TU-TG.651的要求；

提供OFNR阻燃要求；

长度5-20米；

符合GB 40311-2007、IEC 60794-1、ISO/IEC 11801-2002 ed2.0等标准。

3、项目验收及质保期

合同签订后3个月内交付所有设备并安装调试实现所有功能可接受验收。

项目免费质保周期为 5年。

**所有投标人须按照上述要求应答，按照指定的日期和验收要求供货，并承诺质保周期,如不按照指定的日期和验收要求供货不承诺质保期应按无效标处理。**

4、付款方式和条件

付款方式：合同签订后付款中标金额50%，待验收合格后付款中标金额45%，自验收合格之日满一年且签订质保协议后付尾款中标金额5%

5、售后维护要求

1.售后服务函

|  |  |
| --- | --- |
| 售后服务  承诺函要求 | 提供设备制造厂家的售后服务承诺函原件并加盖公章或投标专用章，招标时，装订在招标文件内 |

2.售后服务

|  |  |
| --- | --- |
| 质保年限 | 所有软硬件设备提供不少于五年7\*24小时的原厂免费质保（须提供原厂关于本项目服务承诺函证明材料，并加盖产品生产厂家印章） |
| 响应时间 | 本次采购的所有硬件设备要求在哈尔滨本地有充足备件；故障响应时间不得超过 2 小时 |

## 四、技术情报和资料的保密要求

采购甲乙双方均对对方提供的技术情报和资料承担保密义务，如需公开或向第三方提供，需经对方同意。乙方在工作中获取的甲方提供的信息、资料、数字均应予以严格保密，乙方负责本项目的人员不得向任何单位和个人泄密。如因泄密造成后果的，乙方应承担全部法律的责任。乙方对甲方提供的信息资料等在完成合作后返还甲方。

不论本合同是否变更、解除、终止，本条款长期有效。