附件：

**广州市越秀区图书馆虚拟专用网设备（VPN）采购需求**

1. 采购设备清单
2. 设备名称： SSL VPN网关。
3. 采购数量：1台。
4. 设备参数要求
5. 吞吐量：≥600Mbps。
6. 并发会话数：≥70万。
7. 支持 SSL VPN 并发用户数：≥800个。
8. 通讯接口：不低于4个千兆电口。
9. SSLVPN授权（含PDLAN接入）：≥120个。
10. 硬件加密锁：≥20个。
11. 部署方式：支持IPv6/IPv4协议下的网关模式、单臂模式、主备模式、集群模式、分布式集群模式的部署。
12. 支持PC终端使用包括Windows10、Windows8、Windows7、Windows Vista、Windows xp、Mac OS、Linux等主流操作系统来登录SSLVPN系统，并完整支持该操作系统下的各种IP层以上的B/S和C/S应用；
13. 支持Windows、IOS、Android等操作系统的智能手机、平板电脑（PAD）等移动终端的SSL VPN接入.移动端（Android、IOS）支持通过PPTP、L2TP VPN方式接入；
14. 支持终端使用包括IE6、7、8、10、11或其他IE内核的浏览器，以及最新版本的非IE内核浏览器，如Windows EDGE，Google Chrome，Firefox，Safari，Opera最新版登录SSLVPN系统，登录后可完整支持各种IP层以上的B/S和C/S应用。
15. 支持的密码算法包括：AES、AES192、AES256、DES、3DES、MD5、SHA1、SHA2-256、SHA2-384、SHA2-512、DH、RSA。
16. 支持个性化登录策略，在一台设备上配置不同的访问域名、IP地址，以及不同的使用界面，实现一台设备为多个不同用户群体服务的的使用效果；
17. 支持单点登录功能（SSO）,支持移动用户登录VPN后再登录内部B/S、C/S应用系统时不需要二次重复认证。支持针对B/S单点登录用户名密码加密传输，保证安全；支持针对不同的访问资源设定不同的SSO用户名和密码，支持用户自行修改SSO账号。
18. 支持断线重连自动技术，防止用户误操作关闭浏览器导致VPN隧道断开；防止用户在无线网络环境下网络正常切换时VPN隧道断开。
19. 支持智能递推技术，针对多外链的门户网站进行动态嗅探页面内的链接并完成资源自动授权，防止资源漏访；支持Web参数修正，可针对Flash、Java、Applet、或视频播放器对象所引用资源路径进行修正。
20. 设备必须支持防中间人攻击，产品可在用户登录SSLVPN时智能判断存在中间人攻击行为，断开被攻击的连接，并可提示异常现象。
21. 支持用户终端登录前、登陆后的安全性检测，检测范围包括：用户接入IP、接入时间、接入线路IP、进程、文件、注册表、操作系统、使用终端，可以检测出客户端是否安装指定的防火墙或杀毒软件。
22. 支持客户端注销后自动清除所有缓存、Cookies、浏览器历史记录、保存的表单信息，实现零痕迹访问。
23. 支持VPN专线功能，可配置用户在接入SSL VPN的同时，断开与Internet其他连接。
24. 产品应具有用户/用户组细粒度的权限分配功能：可以针对被访问资源的IP地址、端口、提供的服务、URL地址等进行权限控制；针对同一B/S资源，可对不同用户做到细致到URL级别的授权。
25. 产品应具有角色授权机制，支持在用户组的基础上，根据角色的不同，组合关联不同的资源权限。
26. 支持关键文件保护功能，可针对特定应用关键文件进行锁定，防止用户进行篡改进行越权。
27. 针对服务器地址保护方面，可支持SSLVPN资源列表界面上的用户授权资源隐藏；针对B/S应用，可进行URL地址伪装，防止服务器真实IP地址泄露。
28. 支持客户端类型限制，可以针对VPN资源设置允许访问的客户端类型，客户端类型包括PC、移动端和SDK。
29. 支持设备自身的抗攻击防护，支持防Host头部攻击设置，用于防止Host头部攻击, 设备只允许通过符合设置规则的地址进行访问；支持防SWEET32攻击设置，用于防止SWEET32攻击。
30. 支持随机验证码短信认证，可自定义所发送短信信息格式，支持用户端短信重发功能。支持三大运营商移动、联通、电信运营商的标准的外置短信设备或API接口。支持webservice方式短信认证。
31. 支持主流的短信验证码认证对接（例如，腾讯云、阿里云短信网关认证）。支持对接多个HTTP(S)辅助认证（HTTP(S)验证码认证、HTTP(S)令牌认证）。支持用户、用户组主要认证完成后，继续通过辅助认证（HTTP(S)验证码认证、HTTP(S)令牌认证）。
32. 支持对接微信开放平台，实现个人微信扫码快捷登录。支持微信用户与VPN账号绑定与解绑。
33. 必须支持至少4条以上的外网多线路配置；并在设备单臂部署模式下，多线路接入前置网关，仅依靠SSLVPN设备同样可实现SSLVPN接入用户的多线路自动优选功能。
34. 支持启用多线路时，自动检测故障线路，并自动踢出故障线路；一旦线路恢复，可在一定时间内自动恢复。支持启用多线路时，自定义用户访问选路策略，包括按上/下行带宽，轮询，按优先级等方式。
35. 支持利用网页进行动态寻址的方法，客户端无需安装插件、不依靠IP地址库、不依赖于第三方动态IP寻址、直接根据速度探测实现用户端接入线路的自动优选,用户通过访问寻址代理页面（简称Webagent页面），通过Webagent页面自动寻找VPN设备IP(非DDNS）。
36. 支持针对不同的web页面进行数据优化，支持动态压缩技术，基于数据流进行压缩，减少不必要的数据传输。
37. 支持15级以上的管理员分级分权限管理，从Admin派生树形结构下级管理员；上级管理员可分配下级管理员享有设备配置模块权限，可管理的用户、资源、角色权限，并可限制下级管理员是否允许创建下级管理员、创建资源、创建角色。上级管理员可限制下级管理员对权限内配置享有查看或配置权限 。支持设置对控制台管理员密码复杂度的要求，提升设备的安全性。支持管理员使用证书/USB-KEY认证；支持设置允许管理员登录的IP地址范围。
38. 支持系统实时监控，图形化显示一段时间内的运行状况，可查看CPU占用率、各条线路网络吞吐量、各条线路的IP地址及发送接收流速、并发会话数、SSL并发用户数；可查看历史最高并发用户数并显示时间记录；可实时查看SSL接入用户的用户名、发送流速、接收流速、发送流量、接收流量、接入时间、并发会话数、接入IP、虚拟IP、认证方式等信息，并可在线中断指定用户。
39. 支持独立日志中心进行SSLVPN实时日志记录，可详细记录用户访问资源记录（用户、主机IP、资源、时间）、管理员日志（管理员、主机IP、时间、管理行为、对象）、系统日志、告警日志；可根据用户名、主机IP等信息进行用户行为查询；可提供用户组/用户流量排行及查询、资源流量排行及查询、资源活跃程度、用户活跃程度等记录；提供暴破登录记录；可提供用户登陆SSLVPN采用非绑定账号访问应用系统的记录。
40. 支持密码找回功能，当用户的密码忘记或者丢失时，可自行找回密码。
41. 支持整体网关配置的本地及远程备份、恢复功能；支持SSLVPN配置的单独备份、恢复功能，并支持历史配置的回滚。
42. 产品应具备基于状态监测技术的防火墙功能，能够抵抗常见的网络攻击，能够进行包过滤或WAN、LAN、DMZ口之间访问控制；为了避免人为配置错误，产品必须支持对防火墙的过滤规则能够进行在线虚拟测试。
43. 设备外观：全新。
44. 设备要求兼容连接广州图书馆、广州市越秀区图书馆在用VPN设备，能无缝接入广州图书馆、广州市越秀区图书馆虚拟专用网络。
45. 服务要求
46. 供应商提供不少于三年软件升级服务。
47. 供应商提供不少于三年硬件维护保养服务。
48. 供应商应向采购人提供产品操作使用和日常维护培训服务。
49. 服务响应时间：7×24小时×365天响应，供应商方接到采购人的报障后，10分钟内电话响应，若电话不能解决故障的，4小时内派工程师到达故障现场。
50. 备用机服务：在三年维护保养期内，如设备发生故障需送出维修，供应商应向采购人提供功能或型号不低于采购人设备的备用机供采购人使用，直至采购人设备完全修复。使用备用机期间，供应商应排专业工程司上门协助采购人进行调试使用。
51. 三年维护保养期内，采购人提供免费上门服务（不限次数）。
52. 供应商在供货时向采购人需提供原厂授权函和售后服务承诺函。