1、采用独立的专用硬件VPN设备，而非防火墙、UTM等设备通过添加功能模块的方式实现；采用至少配置4个万兆电口、4个万兆光口，内存≥8G；SSD硬盘≥64G；吞吐量≥5G，支持并发用户数≥16000个；SSL 加密流量≥800Mbps，IPSEC最大加密流量≥640Mbps，2U机架式设备，提供冗余电源；网口最大扩展支持3个槽位，每个槽位都支持4电，4光，8电，8光，2万光，可任意选着搭配。必须是SSL VPN、WEB VPN、IPSecVPN三合一设备。

1. 部署模式支持支持网关模式、单臂模式、双机热备、集群部署模式。

3、支持对基于HTTP、HTTPS、FileShare、DNS、H.323、SMTP、POP3、Telnet、SSH等的所有B/S、C/S应用系统，支持基于TCP、UDP、ICMP等IP层以上的协议的应用，例如即时通讯、视频、语音、Ping等服务；

4、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；支持Windows、IOS、Android、塞班、黑莓等操作系统的智能手机、PDA、平板电脑（PAD）等移动终端的SSL VPN接入，或通过PPTP、L2TP VPN方式接入（提供相关证明材料）

5、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。

产品应支持的密码算法包括：AES、DES、3DES、DH、RSA、RC4、MD5、SHA1。

7、可支持虚拟门户功能，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；

支持文档WEB化管理，用户可通过任意浏览器，对存储服务器的文件进行管理操作（包括：上传、下载、删除、重命名、剪切、复制、粘贴、新建文件目录），而不需要额外安装FTP、文档共享软件等应用程序客户端；

8、支持用户登录界面、服务界面的完全自定义，上传单独的Web页面作为用户登录界面、服务界面；

9、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；

10、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；

支持客户端永久在线功能，对于无人值守的设备可以设定永久在线，如果网络断开，可提供无限次重连；

11、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，避免无法播放的问题；

12、产品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。

13、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；

14、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；

15、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；

16、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；

17、支持主从认证账号绑定，必须实现SSL VPN账号与应用系统账号的唯一绑定，VPN资源中的系统只能以指定账号登陆，加强身份认证，防止登录SSL VPN后冒名登录应用系统；

18、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；

19、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；

20、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GSM、CDMA制式短信猫；支持webservice方式短信认证，支持webservice嘉迅版。

21、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

22、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）,该方法不必单独注册域名或占用IP地址，大大降低了系统部署难度。

23、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。

24、针对B/S资源支持WebCache技术，动态缓存页面元素，提高Web页面响应速度。支持流缓存技术，实现网关与网关、网关与移动客户端之间进行多磁盘、双向、基于分片数据包的字节流缓存加速，削减冗余数据，降低带宽压力的同时提高访问速度；支持共享流缓存功能，实现多分支网关在总部共享流缓存数据，提高流缓存效果.

25、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 。  
26、支持253台不同型号设备间进行集群（A/A），支持路由模式、单臂模式下多线路部署的集群；支持集群设备间Session同步，一台设备宕机后其上用户无需重新登录SSLVPN可继续使用；可扩展分布式集群功能，无需专门的全局负载设备即可实现异地SSLVPN设备间的接入用户负载分担、速度优选接入，异地设备间互为备份，分布式集群中用户可通过唯一的一个地址访问到所有加入到分布式集群的SSLVPN设备；

27、产品必须支持经过集成的，基于Android IOS平台的第三方软件开发包（SDK），并实现基于Android IOS平台第三方应用软件（APP）代码量不超过20行。（要求提供代码Demo和企业证明）支持针对移动APP的VPN安全代码的自动封装，实现App应用的安全加固（提供界面截图证明）；

28、产品必须在Windows和MAC操作系统下支持远程应用发布功能（提供界面截图证明）；可以无需二次开发，即把Windows应用发布到移动智能终端中，也可以支持无需开发，将C/S资源Web化；

29、远程应用发布客户端应支持IOS图标发布资源。远程应用发布应该支持云存储，能够将手机、PAD、PC电脑中的文档、照片等上传到云端，或下载到本地终端。并实现基本的复制、剪切、粘贴、新建、重命名等操作。

1. 远程应用发布能够支持直接调用手机或PAD摄像头，实现拍照。或访问本地照片库，调用已拍的照片。支持自定义Easyconnect客户端登陆界面。
2. 远程应用发布必须支持负载均衡策略，即当存在多台终端发布服务器时，可以根据服务器可用会话数、CPU、内存、I/O、综合性能等指标，智能的将用户分配到不同的终端服务器。

32产品应该支持企业级“云盘”（又名“网盘”、“文件共享”）功能，即可以通过手机、PC、IPAD的客户端，将数据、文件同步到云端或和分享到终端。也能够能够支持分享给他人.

33支持改写WindowsRDP协议，经改写的协议必须独立于OS运行环境，避免跨平台兼容性，针对图像数据，服务端必须支持有损压缩算法；服务端必须能够支持过滤动态内容（gif/flash/video）以减少传输流量，且根据客户需要配置。（必须提供配置界面截图）

34、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

35、要求原厂商在哈尔滨区域设有直属办事处等服务机构，以便于为客户提供完善、及时的售后服务。

36、必须提供7×24小时800电话支持；本地化应急服务紧急攻击事件2小时内响应，最大限度减少损失

37、提供产品IPV6 Ready认证证书，并在全球IPV6测试中心官网可查

38、设备生产厂商需为国家密码管理局发布的《SSL VPN技术规范》起草单位之一

39、设备生产厂商需为国家密码管理局发布的《IPSec VPN技术规范》起草单位之一

40、为保障软件开发质量，要求厂商具有CMMI5级认证。（提供证书复印件）

提供SSL VPN必须在近三年内至少曾有一年在中国国内SSL VPN或VPN硬件市场占有率为前三名，提供权威的第三方机构数据证明。

41、支持与阿里钉钉、企业级微信绑定，实现其内置OA的安全接入，至少提提供4000个企业微信并发接入 。

42、支持Mac、Linux、系统主流浏览器，如Chrome、Firefox等最新版，免安装浏览器插件登陆SSL VPN。支持MAC系统，客户端方式登录SSL VPN

43、WebVPN支持跨平台免插件访问，支持EasyLink泛域名发布Web资源，简化资源发布和访问

44、产品应提供HTTPS驱动病毒查杀工具，支持对Windows环境下的针对HTTPS拦截监听 的驱动病毒进行扫描查杀，避免因为HTTPS驱动病毒导致无法正常接入和使用SSL VPN。

45、投标供应商应提供故障排查工具，保障我单位管理员可以自行检测接入异常的原因，及时解决无法接入的问题

46、支持页面优化技术，可针对不同的web页面进行数据优化，保证我单位接入用户使用体验。

47、针对我单位的B/S架构业务系统支持WebCache技术，可动态缓存页面元素，提高Web页面响应速度的

48、在windows系统上，能同时安装并运行多个VPN客户端，满足有多套VPN的客户同时登录VPN。

49、所供产品必须能跟企业微信做对接，满足我校企业微信加密和互联互通的需求，并且已经有过对接的案例证明。

50、为了防止虚假应标，要求中标后，供应商提供设备进行逐条检测，测试合格后方签订合同。