VPN设备需求

1. 专业VPN设备，非插卡或防火墙带VPN模块设备；产品为标准2U机架式设备，需满足多核X86架构，标配6个千兆电口,2个千兆光口；性能配置需满足：SSLVPN加密速度≥400Mbps，SSLVPN并发用户数≥2600，SSLVPN每秒新建用户数≥280，IPSecVPN加密速度≥220Mbps，IPSecVPN隧道数≥8000
2. 支持网关模式、单臂模式、双机模式、集群模式的部署，
3. 支持Mac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。
4. 能够实现登陆SSL VPN的账号和应用系统账号绑定，加强身份认证，防止登录SSL VPN后冒用其他人员的应用程序账号
5. 支持Linux系统主流浏览器，如Firefox、Chrome等最新版，免安装浏览器插件登陆SSL VPN。
6. 支持文档WEB化管理，用户可不通过FTP等软件，直接通过任意浏览器，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）。
7. 支持终端使用包括IE6、7、8、10、11， 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
8. 产品应提供兼容性检测工具，用于环境检测、自动修复。可以对于Windows系统的兼容性进行检测，并且对检测结果进行一键修复的能力。
9. 支持防中间人攻击，检测到中间人攻击后，立即断开被攻击的连接，并告警
10. 为进行病毒防护，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
11. 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
12. 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
13. 为更好的实现办体验，要求支持与阿里钉钉、企业级微信绑定，实现其内置OA的安全接入
14. 设备内部必须支持自建CA中心，便于数字证书认证平台搭建；单台VPN设备可扩展同时支持4套以上CA根证书；
15. 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。
16. 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。通过Webagent页面自动寻找VPN设备IP(非DDNS)
17. 要求产品在Windows和MAC操作系统下支持远程应用发布功能，而不是发布远程桌面