附件 1

监管平台网络对接设备对接技术要求

	标准 IPSecVPN 设备一台
设备基本要求	1U 机箱，本次配置≥6 个 10/100/1000BASE-T 接口；整机吞吐率≥6Gbps 并发连接数≥220W IPSEC 隧道数≥5000 IPSEC 吞吐率≥300Mbps
SSL VPN 功能	符合国密局制定的《SSL VPN 技术规范》，支持国家商用密码算法 SM1、SM2、SM3、SM4
	支持智能递推
	支持 iOS、Android 智能终端以及 Windows 系统的虚拟桌面与虚拟应用发布方式接入，实现数据不落地，有效保证数据安全
	客户端支持主流 Windows、Mac OS、Linux 操作系统
	兼容多种类型浏览器，包括 IE6、7、8、9、10、11， Firefox，Safari，Chrome，Opera
	支持 iOS、Android 智能终端的全网接入模式
	支持 WEB 转发、端口转发、全网接入模式
	支持 HTTP401 方式、WEB 方式、密码助手方式的单点登录，用户登录 VPN 后无需二次认证，即可登录内部 B/S、C/S 应用系统，支持用户修改单点登陆的账户信息
	支持针对 Android 平台 APP 的 VPN SDK 自动打包
	支持通过 WebCache 技术对 web 页面进行数据优化，支持智能压缩技术，减少不必要的数据传输
	支持双机热备模式下的授权漂移，仅需采购一套接入许可
认证与授权	支持用户名/口令、CA 证书、指纹识别、人脸识别、USB KEY、短信认证、动态令牌、硬件特征码、图形码认证；
	支持多达 5 因素的组合捆绑认证（用户名口令、数字证书、指纹、短信、硬件特征码）；
	支持基于时间的访问授权，支持外部组映射授权；支持证书用户授权，支持基于证书中的字段属性组合授权；
	支持接入主机的安全检查，包括安装的软件、进程、端口、服务、注册表、操作系统及补丁、文件、网卡等，支持接入前检查、接入后检查、定时检查等策略；支持可信接入分级授权；
IPSEC VPN 功能	符合国密局制定的《IPSEC VPN 技术规范》，支持国家商用密码算法 SM1、SM2、SM3、SM4；
	支持免费的多机多线路隧道负载均衡和备份；
	支持预共享密钥、数字证书认证等认证方式；

网络适应性	支持透明、路由、混合模式；支持基于源/目的地址、端口、协议及接口的策略路由；
	支持网络隔离功能，用户登录 SSL VPN 后，只能访问授权资源，不能进行其他的网络访问，确保隧道数据安全
	支持多线路源路返回的智能选路；
	开启虚拟门户的同时，用户正常使用 HTTP 端口和多线路选路功能；
用户管理	支持 IPSEC 与 SSL 使用同一套用户认证、管理系统；
	支持用户与手机号码、PC 硬件特征码、手机硬件特征码、IP、MAC 等硬件信息的绑定，管理员可自定义同一 VPN 账号可登录的终端设备数量；
	支持基于角色及用户组的权限管理、资源管理和策略控制；
系统管理	支持 Syslog 等多种日志格式的输出，可对日志进行加密传输；
	内置多种触发报警的事件类型，支持邮件 SNMP、控制台等多种组合报警方式；
	支持双引擎防病毒，提高系统安全性
	支持双机热备（Active-Standby）、负载均衡（Active-Active）、连接保护（Session Protect）模式，支持系统故障自动切换和抢占功能；
产品资质	具备公安部颁发的《计算机信息系统安全专用产品销售许可证》； 国家版权局-计算机软件著作权登记证书； 具有 IPv6 Ready 认证证书

	前置机一台
设备基本要求	性能不低于 8 核心主频 2.1Ghz /32G 内存 / 不低于 500G 可用空间的 SAS 10K 2.5 （RAID10 ）/不低于双电源 750w/至少具有集成双口千兆网卡 / 至少 3 年保修
操作系统	Linux 系统，具体操作系统版本需根据国资监管平台要求进行个性化安装。