|  |  |  |
| --- | --- | --- |
| **货物名称** | **型号** | **参数** |
| 渔翁信息FisecVPN-S20服务器 | FisecVPN-S20 | 1、机箱高度：2U机架式  2、内存：8G  3、硬盘：64GB  4、接口：6个千兆电口,4个千兆光口，2个万兆光口，2个USB，1个console口  5、电源/功率：冗余电源，250W  6、整机尺寸：88mm（高）\*430mm（宽）\*560mm（深）  IPSec：  密文吞吐率：5Gbps  最大隧道数：8000  每秒新建隧道数：170   1. 投标时需提供原厂授权及售后服务承诺。 2. 产品需与广西公安厅广西公安数字化改革之JW赋能项目中VPN安全网关系统进行对接。   9、功能参数要求：  ①技术标准：  ★具备国家密码管理局颁发的商用密码产品认证证书。（提供证明材料。）  符合 GM/T0022-2014《IPSec VPN技术规范》、GM/T0023-2014《IPSec VPN网关产品规范》、GM/T0024-2014《SSL VPN技术规范》、GM/T0025-2014《SSL VPN网关产品规范》相关要求。  ②密码算法：  至少支持SM1、SM2、SM3、SM4密码算法。  至少支持ECC(SM2)-SM4-SM3、 ECC(SM2) -SM1-SM3算法套件  支持SM2+SM1+SM3+ESP、SM2+SM4+SM3+ESP隧道模式  ③安全协议：  支持国密标准的SSL协议。  支持国密标准的IPSec协议。  ④高可用：  ★支持双主机热备部署，支持主备机自动切换。（提供操作截图等证明材料）  ★支持多机负载均衡，支持负载动态分配。（提供操作截图等证明材料）  ⑤SSL自适应：  ★SSL自适应，搭配国密和非国密浏览器，实现SSL自适应，实现数据以HTTPS形式传输。（提供操作截图等证明材料）  ⑥管理要求  支持安全管理员、系统管理员、审计管理员分权管理，管理员数字证书及密钥存储在智能密码钥匙中。  管理员登录支持数字证书（SM2）+口令的“双因子”认证方式。  支持基于https的安全管理通道。  支持设备密钥备份、恢复，支持3/5门限备份恢复机制。  独立的syslog系统日志。  独立的日志审计、导出权限。  支持GM算法对日志进行完整性保护。  支持对接外部日志服务器。  ⑦功能要求：  ★支持 “多因子”身份鉴别与访问控制。认证因子至少包含PIN码、数字证书和口令。（提供操作截图等证明材料）  ★支持身份鉴别信息完整性保护。（提供操作截图等证明材料）  ★内置CA中心，支持SM2证书签发与验证，支持第三方CA证书导入。（提供操作截图等证明材料）  支持X.509证书体系，支持DER/PEM证书编码格式，支持PKCS12证书/私钥加密文件  支持使用SM2算法进行密钥协商，建立IPSec隧道  ★支持OSPF OVER IPSec。（提供操作截图等证明材料）  支持定期监测网络状态，实现隧道断线自动重建  SSL接入支持单臂/网关模式。  ☆链路聚合，支持链路聚合功能，实现设备带宽增加并提高可靠性（提供操作截图等证明材料）  提供安全接入客户端。客户端支持银河麒麟操作系统、中标麒麟操作系统、UOS操作系统等国产操作系统。  支持win7及以上Windows操作系统、Linux系统等多种终端接入。  支持Android移动端接入。 |