

如何选择 VPN 加速卡

1、什么是 VPN 加速卡？为什么选择 VPN 加速卡？

针对不同的网络安全产品，国家密码管理局制定了相应的技术规范，如《IPSec VPN 技术规范》、《SSL VPN 技术规范》、《IPSec VPN 网关产品规范》、《SSL VPN 网关产品规范》、《安全认证网关产品规范》等规范。网络安全产品中需要使用国密算法如 SM1、SM4 等算法，而提供国密算法的选择之一就是密码卡。通过国家密码管理局鉴定的密码卡安全性、可靠性可以得到保证，可以作为可信模块平滑的嵌入到网络安全产品中，根据网络产品的特性我公司推出了 VPN 加速卡。三未信安加速卡对 SM1、SM4 等对称密码算法的性能有加速作用，并针对网络传输中普遍使用的 1.5K 字节数据包及其他小数据包进行了性能优化。采用双 WNG 系列物理噪声源芯片生成的随机数，随机数质量可靠，性能可达 14Mbps(0.5K~1.5K 字节)。

2、密码卡怎么用？

网络安全产品通过调用密码卡提供的标准 API 函数来使用密码服务，API 接口符合国家密码管理局制定的《公钥密码基础设施应用技术体系 密码设备应用接口规范》标准接口规范。在某些特殊产品如 IPSec VPN 需要使用内核接口，密码卡提供内核接口供客户使用。

3、如何选择 VPN 加速卡

不要太过于相信厂家销售人员报出的性能指标，网络传输中普遍使用 1.5K 字节数据包，而某些厂家报出的指标是最大包长度的或直接是密码芯片的性能指标，这种指标在网络产品的应用中是没有实际意义的。如果不了解网络设备特性的采购人员一般会被响当当的指标所诱惑，而用此产品研发出的网络设备性能指标却低的吓人。

如何选择密码卡呢？首先需要了解网络产品特性，网络产品一般需要传输 64 字节~1.5K 字节这种数据长度短小的数据包，选择密码卡时需要特别关注密码卡小数据包的性能指标。

4、业界的大体水平

以 SM1 算法为例，目前 SM1 算法只能使用芯片进行运算且性能最高的芯片性能理论上能够达到 1.4Gbps。SM1 算法的运算过程为数据经过上层接口、cpu 及系统调度、PCI 传输到达密码芯片，密码芯片运算后依次再返回上层接口，整个过程完成后 SM1 性能肯定衰减，因此密码卡的性能指标不可能达到 1.4Gbps。

目前国内密码卡的性能受制于 PCI 传输的性能，基于 PCIE 1x 和最快的 SM1 芯片进行性能推算，理论上 1.5k 字节时 SM1 的性能理论上能够达到 350Mbps。

5、我们公司的产品及技术力量

三未信安密码卡已经应用在 MIPS、PowerPC 等架构的嵌入式设备中，稳定性、可靠性得到验证。满足不同嵌入式平台，我公司推出了不同外形、不同档次密码卡产品方便用户选择。

此外,负责密码卡硬件、软件的研发人员均在本行业从业十年以上，有丰富的研发及调试经验，骨干员工及技术支持人员在本行业从业三年以上，售后及技术支持能够得到保障。