智能硬件
如何提升您的数据中心

高性能IP模块可卸载网络和安全处理

SILEX
INSIGHT

www.silexinsight.com.cn

智能硬件如何提供提升您的数据中心
高性能IP模块卸载网络和安全处理

云计算得到了前所未有地蓬勃发展，新型的主机应用程序通常被设计成可为数百万个客户端提供服务的高性能架构，并且使每一个客户端都能获得高速的服务、最小的延迟和最有效的安全保障。但是这些数以百万计的连接可能导致数据中心的服务器过热并宕机。

云计算正以前所未有的速度在增长

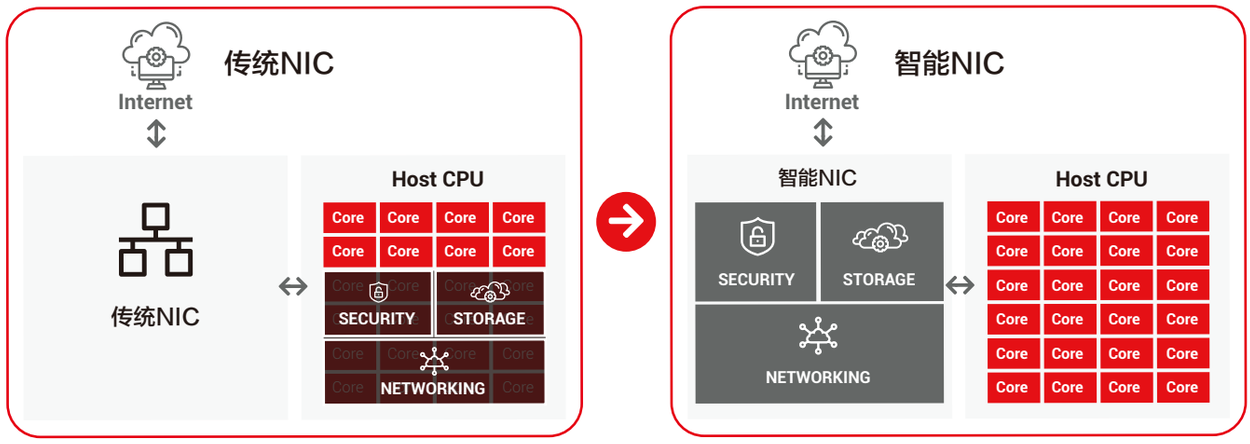
目前用户需要用大量的时间来管理主机处理器网络流，而不是运行有效的应用程序。因此，将越来越多的网络和安全处理快速地卸载硬件成为了一种趋势，如安全加速器和智能NIC（智能网络接口卡）。这将释放主机处理器，使其能够更好地完成设计任务，并降低数据中心的所有权成本。

将智能NIC引入数据中心来提供高速服务

云服务器中的硬件卸载并不是全新的技术，在具有 10Gbit/s 访问权限的数据中心中，传统的NIC可能已经接管了一些网络处理功能，如校验和计算。

但现在有100Gbit/s和更高速的应用前景，结合云处理的爆炸式增长、新兴的 5G 革命以及虚拟化等新技术，这需要新的解决方案。在这种情况下，高效的加密加速器是必不可少的，传统的NIC正在发展成为智能NIC，可配置的网卡可以接管更多的网络处理功能。

加速器和智能 NIC 都可以作为 FPGA 板或通过专用的第三方 IP 模块作为 ASIC 实现。但是，这些模块必须来自可靠的合作伙伴，并且它们具有可扩展性、易于集成性，并且能够为将来的超高性能数据中心做好准备。



使用智能NIC解决方案可以释放应用程序的CPU周期

网络负载：网络结构和数据包的写照

计算机和应用程序之间的数据通信高度标准化，数据被切成帧和段，通过地址、簿记将完整、真实的信息进行加密和封装。数据通信是一个多层系统，其表面层处理物理位信号，第二层处理两台计算机之间的连接…仅最后一层处理实际数据。我们可以想象成在一张纸条上的数据，将其放入带有地址的信封中，然后将其放入第二个信封中，依此类推。

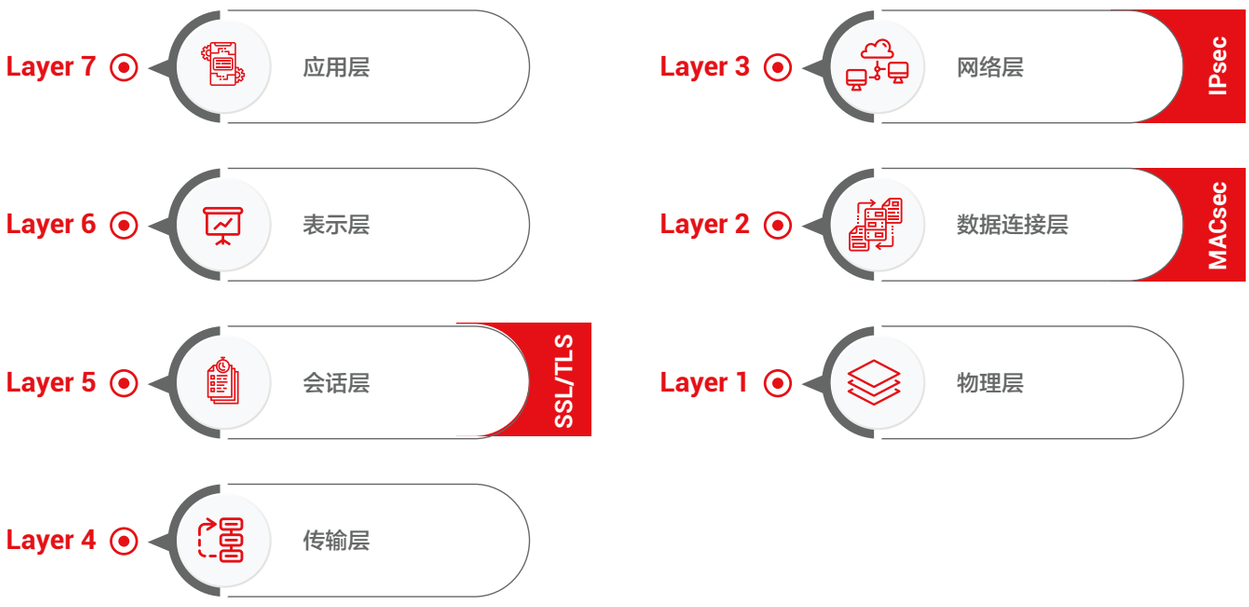
理想的情况下，在云服务器上运行的应用程序应仅与应用程序数据有关。但实际情况中可能有成千上万个客户端会随时访问服务器，因此在大多数情况下，处理各个层的协议可能会占用服务器。处理流程一般都是：打开信封，检查内容和地址，然后将内容放入正确的抽屉中。

这种检查和记账的大部分内容与应用程序无关，因此只要足够快，就可以由单独的处理单元进行处理。关键示例如下：

真实性
检查传入请求的真实性并设置加密/解密，这是第5层的SSL / TLS握手

检查/订购
通过第3层中的IPsec协议检查和排序路由数据包

规制
由第2层的MACsec协议调节两个物理机之间的帧流量



开放系统互连（OSI）网络参考模型

为数百万个连接启用安全握手

保障主机应用程序和客户端之间通信安全的基础是传输层安全协议(TLS)及其前身安全套接字层协议(SSL)，提供了端到端的身份验证和机密性。

在当今的数据中心系统中，每次对发起方进行身份验证并建立安全的加密通道时，云应用程序可能必须每秒接受和处理数千至数百万个连接。但是SSL / TLS处理到涉及复杂的数学函数时，这些函数本身可能已经使用了应用处理器80%到100%的可用计算能力。因此，分流这些处理功能已成为必不可少的工作。

在当今的数据中心里，云应用程序可能每秒必须接受并处理数以千计的连接

为了解决这个问题并释放出应用处理器，Silex Insight开发了一套超高性能IP模块，它们共同构成了SSL / TLS的硬件加速器，可以作为ASIC来实现，或作为FPGA的主要技术之一来实现。这套IP模块经过验证，是目前市场上最快、最高效的工具之一。

Silex Insight的SSL / TLS加速器涵盖了连接握手所需的所有复杂密码计算，即通过非对称密码进行身份验证和交换对称密钥。这些算法包括RSA、ECC、AES、SHA和真实随机数生成等算法。重要的是，该加速器可以100%卸载所有操作和内存访问。这是通过内置的分散收集DMA和基于高度流水线实现的可伸缩数据路径完成的。为了实现非对称操作，IP内核配备了内部微编码定序器，这样就可以根据非常多样化的应用程序和平台的需求来确定芯片的占地面积以及相应的硬件成本，最终取得最佳的平衡决策。这也使Silex Insight的内核能够基于速度、性能、适用面积而成为业内效率最高的内核。

TLS 连接性能 (Ops/s)

在以上结果中，每个运算包括2个乘法点和1个符号运算

处理高达1.5Tbit / s的数据流

随着100Gbit/s和更高数据流的应用前景，传统NIC正在演变为智能NIC。这些是专用的可重配置板，可接管越来越多的网络数据包和安全处理功能。这种流水线内联过程中，主机将数据包发送到NIC，然后在其中将数据包通过各种模块在硬件中进行处理，最后将结果返回到主机。

Silex Insight作为全球安全IP的领先供应商之一，已经为智能NIC开发了几款基本IP模块，可应用到网络第2层、第3层的MACsec和IPsec处理。这些一流的IP模块可以轻松地集成到由数据中心或硬件供应商开发的智能NIC平台中，从而缩短此类产品的上市时间，并降低服务器所有权成本。

Silex Insight的MACsec和IPsec引擎符合最新的标准，它们在第2层、第3层提供了无连接方式的数据完整性、数据源真实性和保密性。

主要功能：

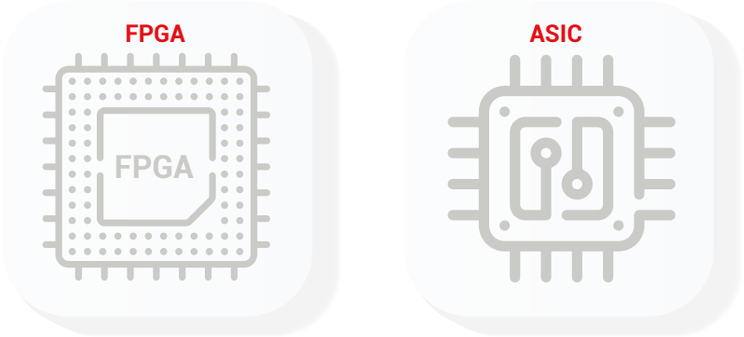
低延迟
可选的创新设计助力对延时敏感的应用场景的技术实现

线速加速
高效的加密内核，可对64byte数据包进行线速处理

重播保护
卸载重播保护和数据包编号管理可进一步减轻CPU负载

这些IP模块集成了针对应用程序实际需求进行优化的加密引擎，因此IP模块具有无与伦比的可扩展性，并可在吞吐量、面积和延迟要求之间取得平衡。

两种引擎的设计均完全独立于技术，可以集成到各种FPGA和ASIC技术中，借助FPGA平台(例如Xilinx®Alve-oTM数据中心加速器），通过为供应商定制的方式来获得更高的吞吐量。



智能NIC 可以集成在FPGA和ASIC技术中

用IP模块设计灵活的、面向未来的解决方案

设计一款能同时保证高安全性、高性能IP模块并非易事，需要深入的专业知识，较长的开发周期，并且对产品进行持续的改进和开发。因此，通过集成可靠供应商的第三方模块来简化开发变得很有价值和意义。

Silex Insight的IP模块具有使其脱颖而出的几个优势：

由安全专家设计，包括最新标准和见解

独特的可扩展性，可以在性能和芯片面积（以及成本）之间取得最佳平衡

经过硅验证的各种应用程序，
包括非常苛刻的安全支付解决方案

设计时易于集成

如果需要，Silex Insight的专家也可以帮助您设计出符合客户需求的最佳解决方案，其中包括技术和成本/性能折衷的选择。

结论

数据中心是一个高度复杂且对安全性非常敏感的环境，与单一客户端应用程序不同，安全隐患可能会产生深远的影响。更重要的是，云端应用程序的成功极大程度上取决于数据中心的响应能力。

因此，将网络处理和加密技术转移到非常快的硬件上已成为势在必行的改变。

可信赖供应商的高性能IP模块，例如Silex Insight，可提供以经济高效、快速安全的方式集成此类加速器和网络板。

Silex Insight提供增强数据中心的关键组件，其中包括业界最快的SSL / TLS握手引擎之一，以及超高性能的MACsec和IPsec处理性能（FPGA上为100 Gbit / s，ASIC上为1.5Tbit / s）。

更多信息和技术内容，请访问www.silexinsight.com.cn或通过contact-cn@silexinsight.com与我们联系。

关于Silex Insight

Silex Insight是全球领先嵌入式系统安全IP解决方案独立供应商，为嵌入式系统提供安全IP解决方案，并为AVoIP /视频IP编解码器提供定制OEM解决方案，可提供高端图像和视频压缩解决方案，以便通过IP分发低延迟的4K HDR视频。Silex Insight的安全平台和解决方案凸显出加密引擎的高性能和易于集成的灵活性，以及为所有平台提供完整安全解决方案的eSecure IP模块。

Silex Insight研发和制造是在比利时布鲁塞尔附近的总部进行，各国家或地区销售服务和技术支持由全球各分支机构提供，相关信息请访问www.silexinsight.com.cn。

我们保障您的安全!

您可能感兴趣的Silex Insight其他论文：

如何向您的朋友和家人简单介绍硬件安全解决方案

非技术人员嵌入式安全指南

您是否发现自己从事硬件安全业务，但是很难解释您的专业?

我们将帮助您简化说明，并用非技术人员可以理解的方式探索一些常用的安全协议：

包括了：

- 知识产权安全 (IP)
- 芯片系统安全 (SoC)
- 安全存储秘密
- 侧通道攻击防护
- 设备唯一身份
- 安全调试
- 安全通讯
- 其他

免费下载 >

更多信息渠道

www.silexinsight.com.cn

Silex Insight

@SilexInsight

SilexInsight

V1.1