白皮书

Mellanox Innova™ IPsec：实现突破性的 VPN、数据隐私和动态数据的安全，同时降低总体拥有成本 (TCO)

数据中心加密的挑战

随着网络攻击的复杂性和有效性不断提高，不能再依赖一度流行的周界安全机制来有效保护数据中心远离此类威胁。

对截取通信流量以及收集和利用未加密信息的担忧日甚，激起了全球对隐私保护的热望。这导致了数据中心大规模增加使用加密方法来保护动态数据和静态数据，更不用说服务器访问层当前实施的附加安全功能（例如防火墙、负载平衡、虚拟交换和虚拟路由）和网络通信处理的指数级增长。其实，加密是基于云的应用程序的新标准，它保护两个位置之间数据传递的保密性和完整性。加密还被越来越多地用于保护数据中心内部的横向流量。

主要用例

- 站点到站点 VPN 隧道
- VPN 隧道聚合
- 主机到主机加密

本文介绍的是先进的高性能网络控制器，适合多种加密需要和体系架构。该网络控制器的吞吐量比纯软件解决方案高 6 倍多，使用较少的 CPU 核心，显著降低了总体拥有成本 (TCO)。

当今的服务器 CPU 无法应对加密需求的增长

因为加密是一种计算密集型应用，所以，基于软件/ CPU 的加密解决方案无法进行扩展满足现代数据中心需要。因此，分配较少的 CPU 资源供应用程序运行，分配较多的资源供加密操作。

Mellanox Innova™ IPsec 适配器对 Ipsec 加密算法的处理进行卸载，腾出宝贵的 CPU 资源，缓解网络瓶颈。IPsec 是用于安全互联网协议 (IP) 通信的一个协议栈，对通信会话的每个 IP 数据包进行授权和加密。Mellanox Innova IPsec 适配器卡以较低的 CPU 使用率提供 40Gb/s IPsec 流量，实现有效使用 CPU 资源，专门用于应用程序执行。

在单个适配器中，加密卸载与高级网络功能共同维持适配器的网络卸载，与单独的加密加速解决方案相比，有助于减小 CPU 使用率，获得更好的总体拥有成本 (TCO)。

MELLANOX INNOVA™ IPsec 简介

Mellanox Innova IPsec 网络适配器为支持 IPsec 的网络提供透明的安全加速。利用 Mellanox ConnectX® 系列网络控制器的最佳性能、无与伦比的可扩展性和效率，Innova IPsec 适配器是基于 Mellanox ConnectX-4 Lx 网络适配器和 Xilinx Kintex UltraScale FPGA 的多功能解决方案。该适配器在一个卡上集成了高级网络功能和加密卸载，只用一个 PCIe 插槽就能同时实现联网和加密，提供各种 CPU 卸载和高级网络功能，包括：

- 云（例如虚拟交换、叠加 (Overlay) 网络）、HPC 和存储卸载
- 基于硬件的 I/O 虚拟化
- 以太网无状态卸载
- AES-GCM、AES-CBC 加密/解密和身份验证算法卸载
- IPsec HMAC-SHA1 和 HMAC-SHA2（224、256、384、512 密钥长度）身份验证
- 基于融合以太网 (RoCE) 的本机低延迟 RDMA
- 端到端 QoS 和拥塞控制

使用案例

Mellanox Innova IPsec 满足多种加密需要和体系架构，如下面的使用案例所述：

- **站点到站点 VPN 隧道**

  在站点到站点情形中，使用 VPN 网关来加密两个或多个位置之间的通信流量，保护各位置间传递数据的机密性和完整性。Mellanox Innova IPsec 可部署为通信链路每个站点网关上的 IPsec 加速器。然后，该 VPN 网关能够卸载对传输到 Innova IPsec 卡的网络流量的加密，腾出 CPU 去执行其他任务。每个 VPN 网关使用一个或多个 Innova 适配器，可增加支持的 IPsec 带宽，由于需要的 VPN 网关较少，因而减少了此类解决方案的总体拥有成本。

- **客户端到站点 VPN**

  Mellanox Innova IPsec 可部署为入站 VPN 连接的聚合点。与前面的情形相似，它可卸载加密任务，腾出 VPN 网关上的 CPU 周期。典型的 VPN 隧道聚合器将会支持成千上万的 VPN 隧道，每个隧道连接到不同的客户端设备。虽然每个隧道中遍历的数据速率不高，但是，总带宽和大量的隧道需要一台高端服务器来管理该任务。Mellanox Innova IPsec 能够实现每台服务器、每个 Mellanox Innova IPsec 卡连接最多 5 万个隧道，同时保持每个隧道的高带宽。

- **主机到主机加密**

  当今，很多数据中心管理员不再依赖边界安全。加密作为日渐流行的手段，在保护内部网络免遭非授权访问和窃取的同时，也有很高的性能影响。而且，数据中心主机上的 CPU 是为执行应用程序，而不是为安全任务而购买，因此，每个用于加密的 CPU 周期都以牺牲创收的应用程序周期为代价。Mellanox Innova IPsec 大大减轻了这一负担，它能够完成最多 40GbE 的加密数据，腾出 CPU 来加速应用程序性能。

IPSEC 卸载性能提升

下图是典型的基于 CPU 的加密解决方案（左侧）和基于 Mellanox Innova IPsec 的加密解决方案（右侧）的对比。清楚地表明了使用 Mellanox Innova IPsec 适配器卡获得的性能提升。

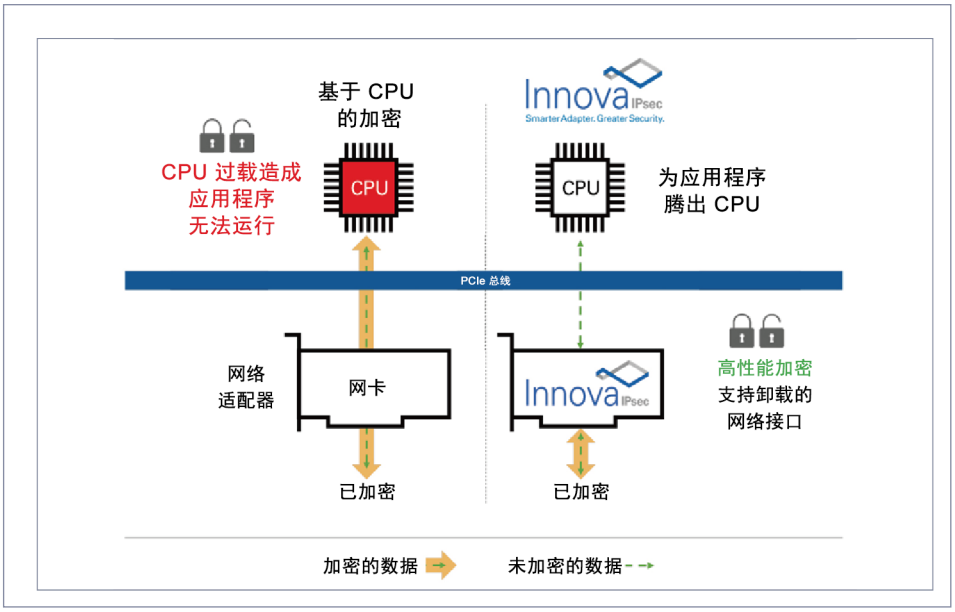


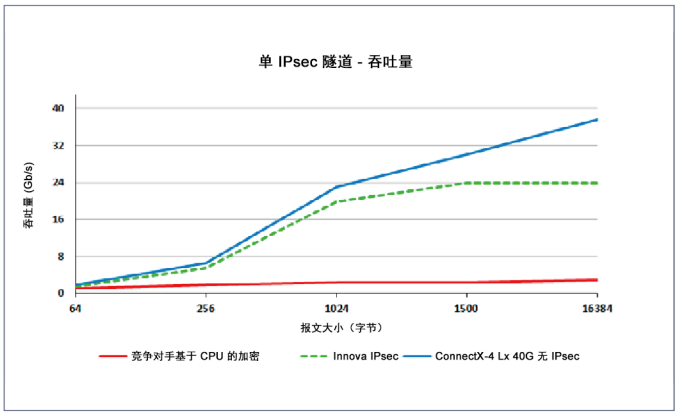
图 1. 基于 CPU 的加密解决方案与 Innova IPsec 卸载的对比

高达 6 倍的吞吐量提升

在下面的测试中，两台服务器彼此直接相连。在两台服务器之间打开了 IPsec 隧道，同时测量通信流量和 CPU 使用率。在一个案例中，使用软件执行基于 IPsec 的加密（用红色表明"基于 CPU 的加密"）。在第二个案例中，通过 Mellanox Innova IPsec 执行加密卸载（绿色虚线）。第三个情形涉及测量标准未加密的流量（蓝色）。

图 2 表示吞吐量比较结果：基于 Mellanox Innova IPsec 的加密实现了高达 6 倍的吞吐量，几乎与不使用加密情形下的吞吐量相当。

单一的加密数据流是有问题的，因为它有较低的带宽和较高的延迟，因而需要 CPU/主机的更多计算资源。Mellanox Innova IPsec 超越竞争对手产品，通过对加密/解密操作进行硬件卸载来缓解这种限制，而不是必须依靠 CPU 来执行此类任务。



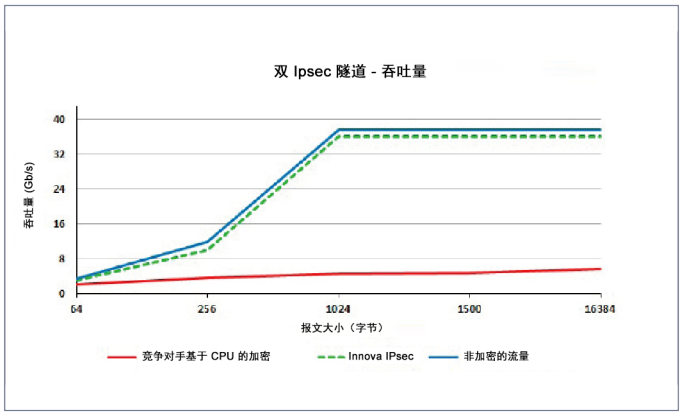


图 2. IPsec 吞吐量：Innova IPsec 对比基于 CPU 的加密

高达 10 倍的 CPU 节省

图 3 显示建立 IPsec 隧道所需的 CPU 资源（按 1Gb/s 的 IPsec 流量计算）。如下面图表所示，Innova IPsec 解决方案的效率比基于 CPU 的加密高 10 倍。

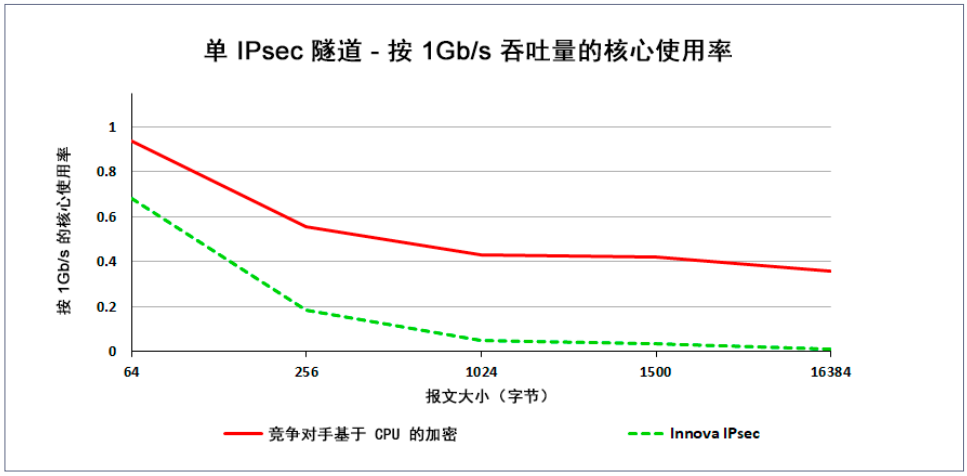


图 3. 用于 IPsec 加密的 CPU 核心数（按 1Gb/s 的 IPsec 流量）

MELLANOX INNOVA 的体系架构优势

备选 IPsec 解决方案由 CPU 和用于加密的 PCI 加速器组成，构成后备体系架构。在这样的体系架构中，数据从 CPU 移动到加速器（“旁侧”）进行加密，然后又传回 CPU 再传送到网络。Mellanox Innova IPec 另外提供一种简单而高效的内联体系架构，网络流量在通过该卡时便进行加密/解密。

提高了 CPU 利用率

与后备方法相比，Mellanox 内联方法提供更好的性能和灵活性，对用户更透明，因为它在网络传输途中对数据进行加密。在数据遍历网络控制器时，内联加速体系架构在 Mellanox Innova IPsec 卡上处理所有加密任务；从而从 CPU 中卸载计算繁重的数据路径加密活动。

可实现网络卸载

加密/解密可以采用“嵌入式 (bump-on-the-wire)”执行；同样，也可以使用由 ConnectX 4-Lx 支持的卸载。可以卸载繁重的网络操作，比如虚拟联网（例如开放式虚拟交换机）、VXLAN 和其他操作，显著提升性能，进一步减少 CPU 的负担。在备选解决方案中，所有加密的数据都从网络传递到 CPU，适配器大多数情况下“视而不见”，无法在加密时对传递的网络流量执行许多卸载，这样 CPU 会因附加的网络相关任务而造成过载。

最大限度地减少了 PCIe 流量

采用 Innova IPsec 的内联加速体系架构，在相同的数据通路上实现加密，无需额外 PCIe 请求，这与备选解决方案中数据遍历 PCIe 三 (3) 次形成鲜明对照。这就减小了延迟，并防止 PCIe 总线过载。

高效的 PCIe 通道和插槽利用率

Mellanox Innova IPsec 将联网和加密加速结合到单个适配器卡上。与后备解决方案相反，它只使用一个 PCIe 插槽和 8 个 PCIe 通道；既不需要更多插槽，也不需要专用通道。

结论

Mellanox Innova IPsec 适配器卡通过提供对 CPU 的高效 IPsec 加密卸载，腾出宝贵的 CPU 周期进行应用程序处理任务，从而降低服务器集群的总体拥有成本。利用 ConnectX 网络控制器与 Xilinx™ FPGA 加速器的结合，Mellanox Innova IPsec 可实现支持 IPsec 网络的安全性加速，同时具有最佳的性能和效率。此外，Mellanox Innova IPsec 内联体系架构发挥完全 CPU 卸载的优势，不需要其他 PCIe 资源。该卸载提供显著性能提升和超过 6 倍的吞吐量，具有较低的 CPU 使用率。

关于 Mellanox

Mellanox Technologies（NASDAQ：MLNX）是针对服务器、存储和超融合基础架构的端到端以太网和 InfiniBand 智能互连解决方案和服务的领先提供商。Mellanox 智能互连解决方案可提供最高吞吐量和最低延迟，更快地向应用程序传递数据并充分发挥系统性能，从而提高数据中心效率。Mellanox 提供一系列高性能解决方案：网络和多核处理器、网络适配器、交换机、线缆、软件和芯片，它们可针对广泛的市场（包括高性能计算、企业数据中心、Web 2.0、云、存储、网络安全、电信和金融服务）加快应用程序运行时间并最大程度实现业务成果。www.mellanox.com 上提供了详细信息。

北京市朝阳区望京东园七区保利国际广场 T1 15 层
电话：010-5789 2000
www.mellanox.com

53771WP
修订版 1.0