解决方案简介

英特尔® NetSec 加速器参考设计

参考设计赋能企业部署重要的内联网络和安全功能

英特尔® NetSec 加速器参考设计面向处理器密集型的网络安全工作负载提供了将基于英特尔® 架构的 PCIe 扩展卡商业化的蓝图。该板卡具备服务器的所有功能，能够支持完整的编排和管理功能，非常适合IPsec、SSL/TLS、防火墙、SASE、网络安全分析和推理等安全工作负载。这一参考设计可帮助客户提高云边协同的性能、规模和效率。

随着企业持续向边缘计算转型，需要能够随时随地联网的设备和员工数量越来越多，使得企业环境的分布式特点达到了前所未有的程度。传统的以边界为导向的安全模型和固定的部署模式已经不再适用。单体应用已被容器化的微服务链所取代。这些微服务遍布本地和云基础设施，并且已经和底层硬件解耦；工作负载需要部署在需要它们的地方。在这些软件定义的动态环境中，安全功能需要以一种基于各工作负载、用户和设备的全新方式加以应用。

安全访问服务边缘（SASE）模型将软件定义的安全和广域网（WAN）功能融合到一组通过云交付的服务中，因此可以满足这些新的分布式安全要求。虚拟化或容器化的服务可通过集中编排提高效率，并能在传统的单用途硬件中使用基于商用现货（COTS）服务器的云基础设施，从而降低设备成本。

大多数 SASE 解决方案都是完全集成的网络和安全功能堆栈，其许可模式大都基于方案中所使用的特定组件。SASE 供应商需要进行大量投资来评估、获取和集成这些解决方案。SASE 软件功能要求共享多个计算密集型工作负载和多租户的服务器具备高性能和高稳定性。要将一个高性能的软件定义广域网（SD-WAN）解决方案与涵盖下一代防火墙（NGFW）、零信任网络访问（ZTNA）、云访问安全代理（CASB）、安全 Web 网关（SWG）和数据丢失防护（DLP）的全面安全堆栈集成在一起尤其不易。

一个成功的 SASE 解决方案需要能支持地理上分散的边缘或接入点部署，而此类边缘又往往面临着传统本地数据中心中并不常见的特殊挑战。边缘基础设施可能面临着严苛的空间、散热和功率限制，并且要部署在需要零接触管理的隔绝位置。边缘基础设施还可能需要迅速升级，以满足不断增长的 SASE 服务需求。边缘对 SASE 的这些要求在许多其他边缘工作负载中可能也十分常见。

英特尔® NetSec 加速器参考设计为应对 SASE 以及各种部署在隔绝环境的边缘工作负载的这些要求提供了新方法，可显著减少网络和安全工作负载的基础设施占用空间。该设计包括英特尔® 处理器、英特尔® 以太网 800 系列控制器和大量板载高速内存，可基于 PCIe 扩展卡为用户提供服务器的全部功能。

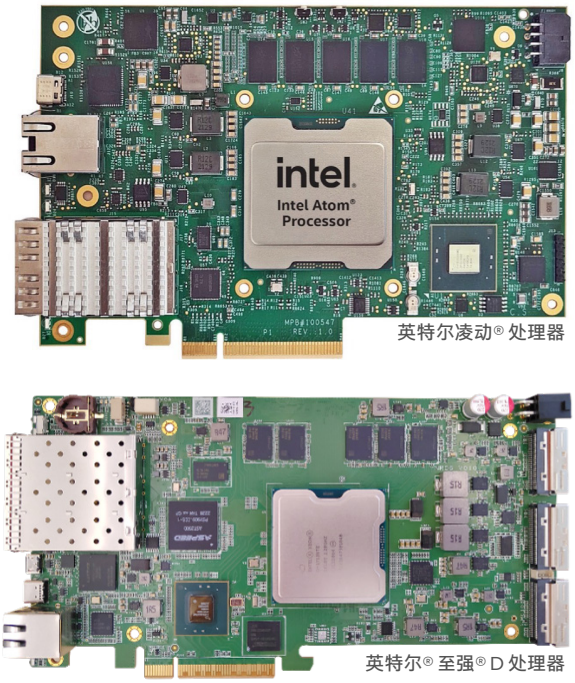

图 1. 英特尔® NetSec 加速器参考设计

提升面向安全工作负载的处理能力

英特尔® NetSec 加速器参考设计提供一个或多个独立的物理执行环境，可轻松应对网络和安全设备的计算需求。该加速器作为服务器主处理器的补充，可提供专用的网络和安全功能加速硬件。

主机服务器 CPU 和英特尔® NetSec 加速器参考设计上的 CPU 之间的指令集相互兼容并共用一个驱动程序架构，有助于通过标准化英特尔® 架构实现整个解决方案的无缝对接。编程模型的一致性使加速器上的英特尔® 处理器与主机上的英特尔® 至强® 可扩展处理器或英特尔® 至强® D 处理器之间可以实现平台通用性。

处于英特尔® NetSec 加速器参考设计核心地位的英特尔® 处理器可支持内联 IPsec。

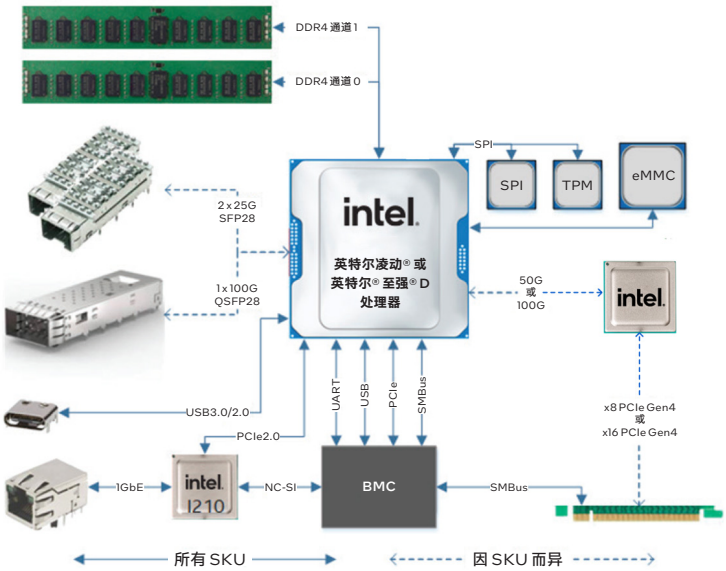

图 2. 组件扩展视图

自主计算资源将数据和操作与系统的其余部分隔离开来，帮助架构师克服多个供应商软件组件之间不兼容的问题，同时在系统层面提供更好的安全性。基于参考设计添加的硬件资源可以大幅提升解决方案的功能和密度，也可在后续升级中按需为部署就位的解决方案提供灵活性。

原始设备制造商 (OEM) 和原始设计制造商 (ODM) 可以与网络和安全解决方案提供商携手合作，利用该参考设计更快地将网络安全加速器推向市场。英特尔正在与众多合作伙伴合作开发产品，使系统供应商、解决方案集成商和终端客户可以灵活选择技术供应商。

参考架构	英特尔凌动® 处理器 8 核参考设计	英特尔凌动® 处理器 16 核参考设计	英特尔® 至强® D 处理器 4/8 核参考设计	英特尔® 至强® D 处理器 10 核参考设计
CPU	英特尔凌动® P5721 处理器	英特尔凌动® P5742 处理器	英特尔® 至强® D-1713NT/1733NT 处理器	英特尔® 至强® D-1743NTE 处理器
外形规格	全高半长		全高四分之三长	
外部端口	2x 25GbE SFP28	1x 100GbE QSFP28	2x 10/25GbE SFP28	
功耗	约 50 至 90 W	70 至 115 W	90 至 145 W	
内存容量	高达 32 GB @ 2933 MT/s		高达 32 GB @ 2933 MT/s	
主机接口	x8 PCIe Gen4	x16 PCIe Gen4	x16 PCIe Gen4	
存储容量	高达 256 GB eMMC		高达 256 GB eMMC	
吞吐量目标（双向加速）	25 Gbps	50 Gbps	25 Gbps	50 Gbps
吞吐量目标（单向加速）	50 Gbps	100 Gbps	50 Gbps	100 Gbps

参考设计硬件规格

该参考设计包括多种版本，主要差别在于处理器（和内核数）以及 I/O 和网络资源。

SASE 加速用例

SASE 服务提供商部署的接入点 (POP) 解决方案在地理位置上较为分散，相对靠近用户端点以及本地、边缘和云服务。企业用户通过充当访问网关的 SASE POP 访问其资源，从而安全地满足时延和吞吐量的服务级别目标。云原生安全服务的分布式交付无需将 WAN 流量回传到集中位置，也能应用安全策略。

这种新颖的拓扑结构可以节省大量带宽成本，同时还因为消除了回传产生的传输时延而改善了用户体验。POP 服务器集群为所有用户网络流量实时托管任何或全部主要 SASE 组件，包括：

- **下一代防火墙 (NGFW)**：结合了传统防火墙功能与深度数据包检测、入侵防护和威胁情报等补充服务。
- **软件定义广域网 (SD-WAN)**：可进行动态自我优化以连接用户与应用，在 MPLS、4G/5G 和有线宽带等各传输服务之间以集中的方式进行流量引导。
- **零信任网络访问 (ZTNA)**：可提供对资源和应用的无缝远程访问，同时授予尽可能少的权限，将所有实体在其他用途下均视为不可信。
- **安全 Web 网关 (SWG)**：可过滤用户发起的流量，以检测并删除恶意软件和其他不需要的软件，帮助执行企业安全标准并保持合规。
- **数据丢失防护 (DLP)**：可监控流出的用户流量，以识别敏感信息并防止未经授权的流出（无论恶意与否）。
- **云访问安全代理 (CASB)**：为在用户和云服务之间应用身份验证、加密和日志记录等策略提供执行点。

精心设计和构建的 SASE POP 可确保在各个位置和端点（如办公笔记本电脑、物联网传感器/执行器和移动设备）准确交付这些服务。服务质量取决于提供充足 POP 覆盖的能力，包括地点数量和每个地点交付服务的能力。SASE 供应商可优化 POP 服务器以显著提高成本/容量效率。

SASE POP 服务器配置

除了英特尔® 至强® 可扩展处理器，专为在网络边缘配置密集计算而设计的英特尔® 至强® D 处理器也是 SASE POP 服务器基础组件的热门选择。该平台有着出色的能效表现，采用基于硬件的安全和加速技术，并且集成了先进的英特尔® 以太网连接技术。

解决方案架构师可以基于英特尔® NetSec 加速器参考设计添加一个或多个加速器，以扩展基于英特尔® 至强® 可扩展处理器和英特尔® 至强® D 处理器的 POP 服务器的服务容量。举个例子，基于 20 核英特尔® 至强® D 处理器的双路 POP 服务器总共有 40 个内核。在系统中部署两个 16 核加速卡相当于额外提供了 32 个英特尔凌动® 处理器内核，这样便在不增加服务器占用空间的情况下将内核数量增加了 80%。每个加速器都可以用自己的一组计算、内存和 I/O 资源运行一个单独的 SASE 服务，从而将工作负载进一步并行化，提高确定性性能和安全性。

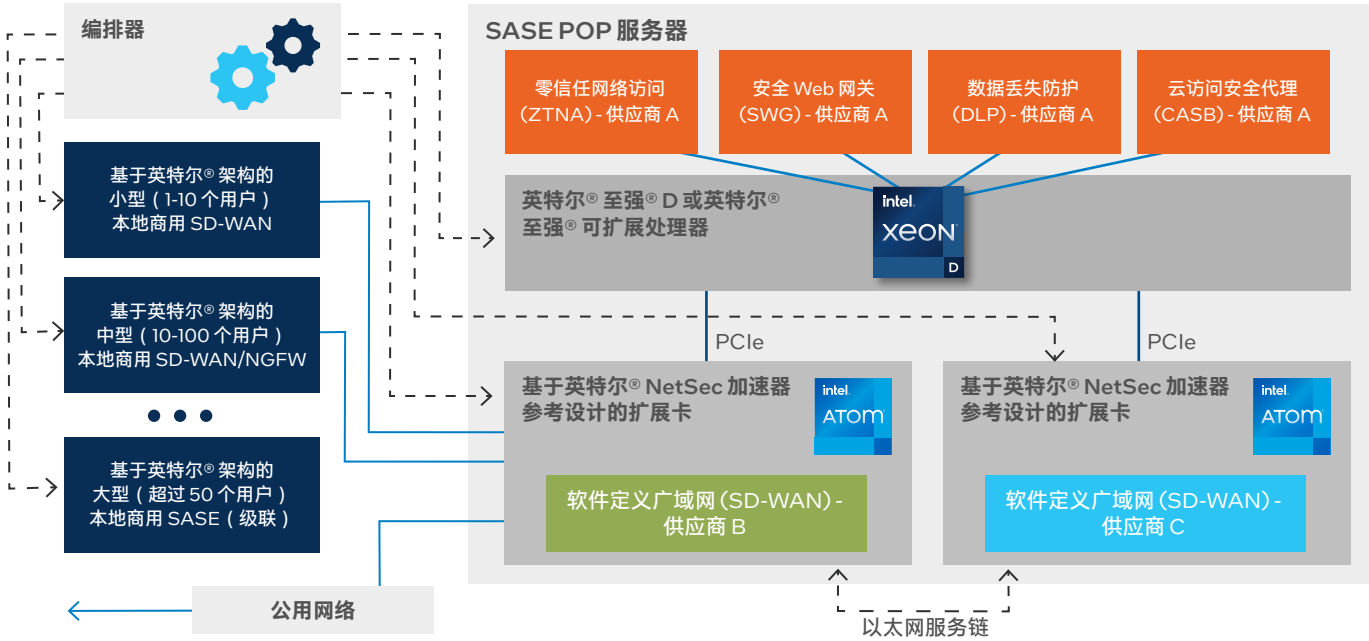

图 3. 基于英特尔® NetSec 加速器参考设计的 SASE 架构

加速器连接拓扑结构

基于英特尔® NetSec 加速器参考设计的加速卡可以直接连接到外部公用网络，从而使某些 SASE 功能能够独立于主机服务器上的主英特尔® 至强® 可扩展处理器或英特尔® 至强® D 处理器来实现。这种连接方式还使加速卡能够提供内联功能，将入站数据独立推送给合适的计算资源，从而提高效率。基于以太网的服务链可以直接在加速器之间进行服务互联，将容量或功能组合起来，正如示例中展示的将 SD-WAN 和安全堆栈作为两个不同加速器的单个服务一起交付。英特尔® 至强® D 或英特尔凌动® 处理器的集成功能可促进资源共享以提高效率，并在无需调用基于英特尔® NetSec 加速器参考设计解决方案中英特尔® 内核的情况下均衡端口之间的负载。

在某些实施方案中，基于英特尔® NetSec 加速器参考设计的加速器可能根本不与外部连接。例如，它可以使用服务链通过公用网络上的另一个加速器提供服务，或者为深度数据包检测提供沙箱应用这类无需外部连接的功能。

SASE 加速在实际部署中的潜力

SASE 加速用例展示了基于参考设计的设备在 SASE POP 服务器中的一些代表性使用模式，包括：

- **提高密度和基础设施效率**：通过使用一个或多个具备全部“板卡服务器 (server-on-a-card)”资源的加速器来部署额外的计算容量，从而获得更高的密度和基础设施效率。
- **多供应商集成**：集成的实例化由 SASE POP 服务器完成，可提供基于解决方案的统一服务，避免服务在单个系统上不兼容的问题。
- **先进的流量控制**：使用英特尔凌动® 处理器中的集成网络交换机来实现独立于主处理器的入站数据高效引导。
- **分布式 SASE 服务的服务链和交付**：通过在单个 SASE POP 服务器中使用多个加速器实现。

通过扩展硬件并强化其功能，这些因素可以减少实现既定性能目标所需的服务器数量，从而帮助降低运营成本。

可加速网络和安全功能的构建模块

该参考设计提供了一个独立运作的计算节点，可在保守的功率范围内提供服务器级别的性能和可靠性。它为 IPsec 提供了内联加密和旁路操作功能，适用于异步批量加密工作负载。

内置的第三代英特尔® 数据保护与压缩加速技术（Intel® QuickAssist Technology，英特尔® QAT）可加速对称和非对称加密，实现高达 100 Gbps 的吞吐量。英特尔® QAT 硬件直接与板载以太网控制器通信，以决定处理哪些数据包以及将哪些数据包传递给处理器。由此，数据路径得以缩短，从而支持内联 IPsec。

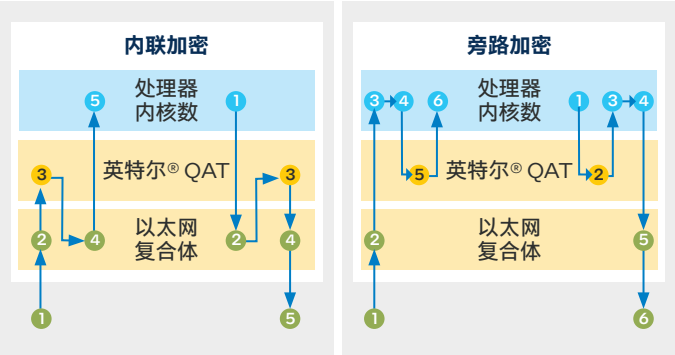

图 4. 支持内联 IPsec

英特尔凌动® 处理器——出色的每瓦性能和内联 IPsec

英特尔® 处理器是英特尔® NetSec 加速器参考设计的基础。这些处理器采用高能效的片上系统（SoC）外形规格，可为安全和网络工作负载提供高吞吐量。高度集成的英特尔凌动® 处理器将英特尔® 以太网和硬件加速器集成到 SoC 封装中，可提供低时延操作，在降低设备成本、空间/服务器要求和能耗方面有着明显优势。

英特尔® 至强® D 处理器

英特尔® 至强® D 处理器专为高计算吞吐量和低热设计功耗（TDP）而设计。它采用高度集成的 SoC 封装设计，面向高性能和安全性提供丰富功能，包括：

- **英特尔® 软件防护扩展（Intel® Software Guard Extensions，英特尔® SGX）**：可在内存中创建专用的隔离区（即“安全执行飞地”），为使用中的数据提供保护。在飞地中可对未加密的数据进行操作，但任何权限等级的软件和用户都无法获取这些数据。
- **英特尔® 高级加密标准新指令（Intel® AES New Instructions，英特尔® AES-NI）**：可加速硬件中 AES 加密算法资源消耗密集的部分。
- **英特尔® 高级矢量扩展 512（Intel® Advanced Vector Extensions 512，英特尔® AVX-512）**：可借助超宽的 512 位矢量运算（与前代技术相比，每时钟周期可处理更多数据）提升 AI 和 5G 等严苛工作负载的性能。

英特尔® 以太网 800 系列控制器——先进的网络安全功能

该参考设计包括采用动态设备个性化（DDP）的英特尔® 以太网 800 系列控制器，用于执行数据包处理和流量整形，进而提高性能。DDP 使网络管理员能够根据流量类型建立多个配置文件，然后分别指定数据包处理参数，进行针对性优化。基于 DDP 的流量优先排序可以在运行时动态配置，以提高灵活性和敏捷性。

结论

英特尔® NetSec 加速器参考设计提供了一个高效易用的蓝图，可在 PCIe 外形规格中提供独立服务器的所有功能，仅仅通过插入即可高效集成到安全设备和边缘平台中。它在服务器机箱内提供独立的物理计算环境。

在该参考设计中添加系统内存等资源使加速器设备可独立于主服务器平台运行。加速器独立运行安全服务以扩展服务器容量，包括支持多供应商软件堆栈，避免这些软件堆栈在单个系统上不兼容的问题。此功能可使单个主机能支持更多服务，帮助终端客户降低总体拥有成本（TCO）。

这一经过预先验证的参考设计简化了 OEM 和 ODM 与网络和安全解决方案提供商合作开发新安全设备的过程。它既增强了平台灵活性，又降低了对解决方案开发商的设计要求，帮助他们更快、更经济高效地将新的安全产品推向市场。

了解更多信息：

英特尔® 至强® D 处理器

英特尔凌动® 处理器

英特尔® 以太网产品

实际性能受使用情况、配置和其他因素的差异影响。更多信息请见 www.Intel.cn/PerformanceIndex。
性能测试结果基于配置信息中显示的日期进行的测试，且可能并未反映所有公开可用的安全更新。详情请参阅配置信息披露。没有任何产品或组件是绝对安全的。
英特尔技术可能需要启用硬件、软件或激活服务。
没有任何产品或组件是绝对安全的。
具体成本和结果可能不同。
代号用于英特尔识别研发中且尚未上市的产品、技术或服务。其并非“商业用”名称且并无意用作商标。
英特尔运营所需的任何商品和服务预测仅供讨论。就与本文中公布的预测，英特尔不负有任何购买责任。