解决方案简介

基于英特尔凌动® P5000 网络 SoC 处理器平台的易科腾国密 SD-WAN 方案

易科腾 EQTINFO

概述

链路加密已经成为网络和边缘计算平台的基础功能，也是云计算时代数据安全的关键网络技术。互联网安全协议栈（Internet Protocol Security, IPSec）作为链路加密的最主要安全传输协议，通过动态密钥交换和隧道加密技术，为跨广域网传输的数据流提供端到端保护。IPSec 有大量成熟和创新的应用场景，如远程办公、软件定义广域网（SD-WAN）等。高性能、低延时、广兼容，易开发的硬件平台特性对整合 IPSec 协议栈的整体方案实现至关重要，市场需要既符合中国市场对加密算法的技术要求，又能基于单芯片实现高性能高性价比的整体解决方案。

英特尔凌动® P5000 网络 SoC 处理器平台集成了 Quick Assist Technology (QAT) 引擎，硬件支持国家商用密码算法（简称：国密）、AES 等加密算法。驱动软件实现与 DPDK、VPP、OpenSSL 等开源网络协议栈的整合，提供完整、成熟、友好的应用开发接口，是开发高性能、高性价比的网络和边缘计算解决方案的理想硬件平台。易科腾成功使用英特尔凌动® P5000 网络 SoC 处理器平台，开发出全新满足中国本地市场加密需求的高性能 SD-WAN 整体解决方案，在显著降低整机硬件成本的同时，助力基于国密算法的链路加密能力在运营商网络和企业网络的普及。

挑战

网络流量的快速增长，跨区域分支网络需求的扩展，以及愈发复杂的网络环境都凸显了网络架构转型的必要性。与传统网络架构相比，SD-WAN 重构了企业网络架构，实现软件定义网络资源，边缘侧部署软硬解耦通用白盒硬件平台，配合集中化管理控制器，构建一个透明、可控、可预测的端到端的云边一体网络，不仅为企业和边缘位置提供灵活的网络服务和云访问能力，还能够有效简化网络管理、消除应用和数据交换性能瓶颈并提升网络灵活性。

在数字化转型不断加速的今天，SD-WAN 化解了传统企业网和边缘计算方案面临着灵活办公地点，企业分支快速扩张，业务系统云化，分布式架构的协同和自治，数据交换安全和可靠等复杂化的挑战，但 SD-WAN 方案还需要不断演进，更好的支撑企业数字经济不断增长的需求：

- **强化国密性能和方案通用性：** 网络安全法、等级保护等法律法规要求通过国密等算法，实现链路加密，以保障数据的安全性。而链路加密对于算力有着较高要求。传统方式是通过 CPU 进行软加密，这会导致 CPU 占用率上升，对于 SD-WAN 设备而言会带来巨大的性能压力，也会影响核心业务的高效稳定运行。
- **提升性能和性价比：** 为满足链路加密带来的算力需求，SD-WAN 设备可能需要在芯片等方面进行额外投资，例如通过单独的加速器来进行负载加速，这会带来较高的成本压力。
- **SD-WAN 和边缘计算整合：** 方案采用具备强大算力的通用 CPU，不仅提升网络性能和功能，还可以通过软件迭代开发集成广域网优化，实时加密流量分析、安全防护功能，实现产品的差异化。方案还可以实现和云应用融合，为企业和运营商提供云边一体，按需增值应用服务机会，将 SD-WAN 打造成网络 +X 的创新平台。

解决方案：基于英特尔凌动® P5000 的易科腾 SD-WAN 方案

易科腾 SD-WAN 方案定位为面向运营的 SD-WAN 网络，原生支持多租户、大规模组网，支持运营场景下运营商采用自有骨干网提供服务的场景，同时也可以支持无骨干网的私有化部署场景，汇聚设备支持全云化部署，支持多云互联场景。SD-WAN 系统内置了 ZTP 业务开通、IPSec VPN 加密、安全防护和广域网优化等能力，全面支持 IPv4/v6 双栈组网。

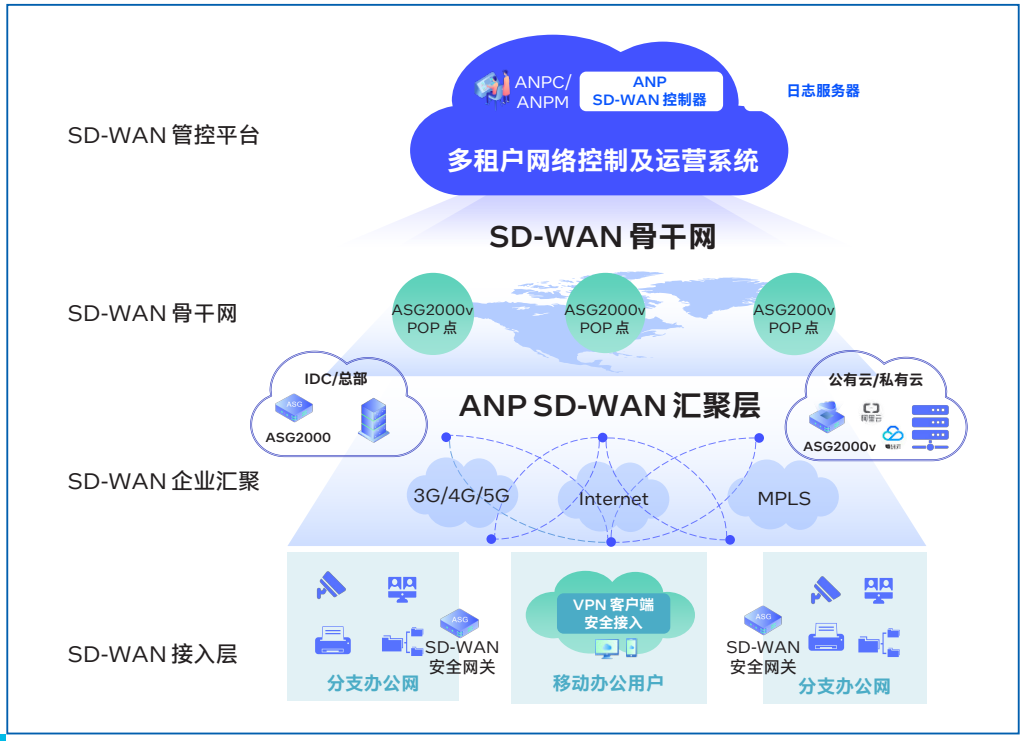

图 1. 易科腾 SD-WAN 方案

易科腾 SD-WAN 方案支持在出厂时预装易科腾或者客户颁发的数字证书，并采用公钥的 Hash 值作为设备的逻辑标识，控制器所有的配置可以基于设备 ID 进行预先配置。当设备在客户站点启动后，可以采用证书和控制器进行认证，认证通过后根据设备 ID 获取设备的配置数据，从而零配置实现自动化上线。该方案具备云原生多租户架构、远程办公和 SD-WAN 统一架构、创新的控制面和转发面配置对账技术、广域网大二层支持、支持 NAT 出口企业网的动态路由接入、微分段安全等多重优势。

为了解决链路加密所带来的算力挑战和提供更好的弹性扩容能力，易科腾 SD-WAN 方案采用了英特尔凌动® P5000 网络 SoC 处理器平台。该处理器支持可选的 8-24 个核心，目前较为广泛地应用于路由器/交换机、企业网、无线接入网基站等产品。英特尔凌动® P5000 集成的加速器及网络接口大幅提高了该系列 CPU 的可用性以及性价比。英特尔凌动® P5000 集成了最高 100G 的英特尔最新的 800 系列网卡，最高可以支持 8 个端口，并且网络端口可以灵活配置，其支持英特尔® VT-x、英特尔® SR-IOV、英特尔® VMDQ 等技术，对于虚拟化场景亦有很好的支持。英特尔凌动® P5000 拥有丰富的 I/O 接口，有效提高了产品的可扩展性。

英特尔凌动® P5000 集成英特尔® QAT、英特尔® 动态负载均衡（英特尔® DLB）等多种网络及加速器模块，其中第三代英特尔® QAT 加速器在各种网络安全加解密场景中有十分广泛的应用，英特尔® DLB 加速器能够很好地解决动态负载、限速等应用难题。这些网络及加速器模块通过内部总线的方式挂接到处理器的核心单元上，各个加速器模块在 CPU 中均以 PCIe 设备的形式呈现。

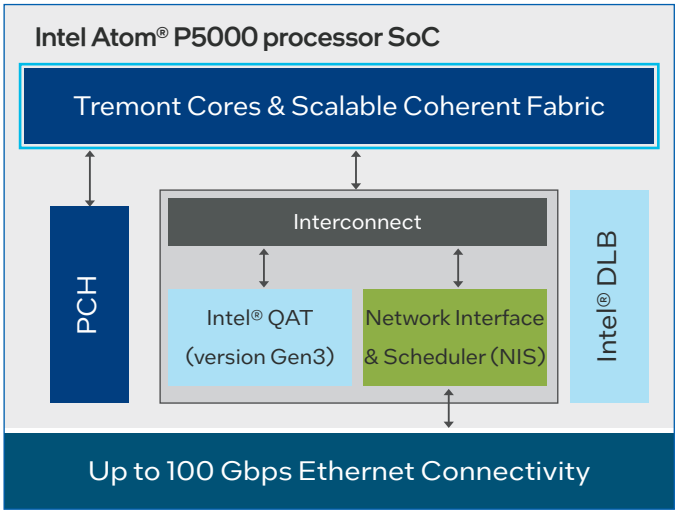

图 2. 英特尔凌动® P5000 关键特性

英特尔® QAT 加速器提供加密和压缩加速功能，可以有效提高整个设备或产品的性能和效率。英特尔凌动® P5000 集成了第三代英特尔® QAT 加速器。QAT 的加密功能广泛应用于网络安全（IPsec、SSL/TLS）、重复数据删除哈希、加密存储和安全密钥的硬件保护。QAT 的压缩解压缩功能广泛应用于大数据加速、广域网加速、存储/数据库压缩、http 压缩、文件系统等场景。安全和压缩加速功能主要分为三大类：对称加解密（Bulk Crypto/Symmetric）、非对称加解密（Public Key Engine/Asymmetric）、压缩解压缩（Compression/Decompression）。

英特尔® QAT 加速器的加解密通过 PMD 提供给 DPDK 应用程序，将 PMD 注册给对应的 cryptodev 接口来实现。PMD 使用通用的 QAT 驱动程序代码管理 QAT PCI 设备。它们还依赖于平台上安装的 QAT 内核驱动程序，使用过程中需要创建 QAT 设备的 VF，并将 VF 使用 vfio/igb_uio 驱动来绑定。易科腾高性能国密 IPSec 协议栈支持采用英特尔® QAT 加速器，来处理国密算法的加密负载。

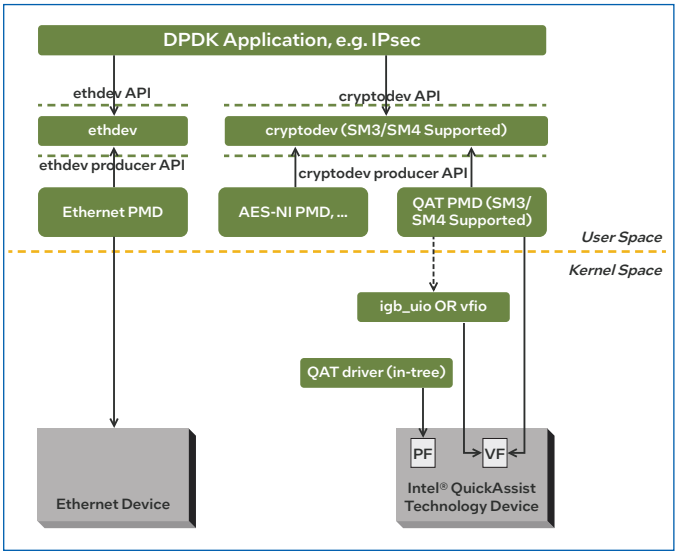

图 3. 基于英特尔® QAT 和 DPDK 的国密加速框架

在验证中，易科腾在加密后端分别使用 OpenSSL 和 QAT，并采用相同的组网环境、相同的加密套件对性能数据进行对比。在具体测试中，易科腾在 CPE1 与 CPE2 之间创建 64 条 IPSec 隧道，使用的加密套件是 SM4-SM3，思博伦测试仪构建双向各 512 条流，报文大小 512/256 字节使用 2544 套件进行性能测试。

测试数据如图所示，相对于 OpenSSL，使用 QAT 能够将网络性能提升约 6.61 倍，达到业内领先的水平[1]。

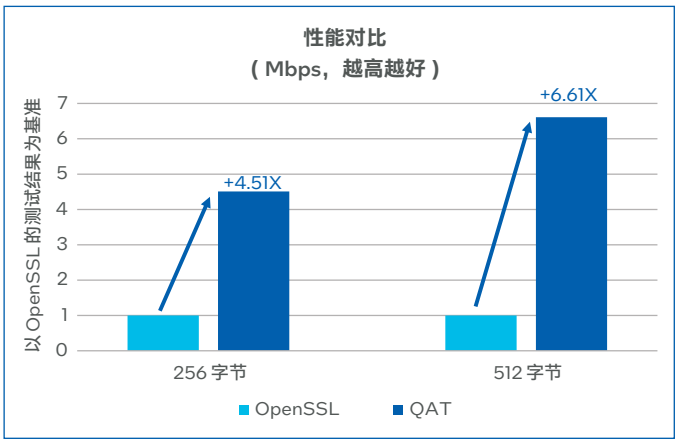

图 4. OpenSSL/QAT 性能对比

收益

基于英特尔凌动® P5000 网络 SoC 处理器平台的易科腾国密 SD-WAN 方案通过采用 SoC 集成的英特尔® QAT 进行加密处理，显著提升了性能表现，为用户带来了如下收益：

- **提升了链路加密性能和部署通用性，一种方案，全球部署：**更解决了老方案支持国密等算法的性能瓶颈，通过将负载卸载到 QAT 加密器，降低 CPU 占用率，减少对于其他业务带来的负面影响。
- **提升了方案的性价比和弹性扩容能力：**通过采用通用架构的单芯片处理器，按照部署需求可以实现 4 到 24 核的平滑性能扩容。而且不再需要额外的硬件加速器件支持国密算法，在显著降低整机硬件成本的同时，助力国密算法在运营商网络和企业网络的普及。
- **降低拥有成本（TCO）：**处理器平台提供了完整的开发环境，可重用软件组件，驱动可以提供完整、成熟、友好的应用开发接口，支持 DPDK、VPP、OVS 和 OpenSSL 等众多的开源网络软件包，显著降低了 SD-WAN 方案的开发门槛和开发成本。通用开放的软件和硬件平台组合可以节约软件开发资源，降低整体拥有成本（TCO）。

[1] 易科腾截至 2023 年 8 月的内部测试结果。测试配置：英特尔凌动® 5342 处理器，16 GB 总内存，QAT Gen3，Ubuntu20.04，OVS 2.17，DPDK 22.11。英特尔并不控制或审计第三方数据。请您审查该内容，咨询其他来源，并确认提及数据是否准确。

展望

在行业客户和运营商更加重视网络，数据，安全合规的背景下，支持高性能国密等加密算法会增加 SD-WAN 方案的竞争力。基于英特尔凌动® P5000 网络 SoC 处理器平台的易科腾 SD-WAN 方案为用户提供了快速拥抱国密 SD-WAN 的卓越选项，能够帮助用户以单芯片化解加密带来的性能挑战，实现高性能、低成本、高稳定性、高易用性的结合。易科腾的成功案例也表明英特尔凌动® P5000 完善了国密算法的支持，能够支持开发者在网络方案中快速整合国密算法。

未来，英特尔将依托于一系列先进的硬件平台和开放的软件生态，面向 SD-WAN、边缘计算、算力网络等关键演进方向的需求，强化技术创新与生态协作，帮助用户加速优化网络基础设施，带来高性能、低成本、高扩展性、高安全性的网络应用新体验，为数字化转型提供网络赋能。

关于易科腾

南京易科腾信息技术有限公司是一家专注于量子保密通信、密码及网络安全相关产品和服务的高新技术企业。公司拥有量子通信、SD-WAN/SASE、商用密码等多个产品系列，致力于成为商用密码基础设施的使能者，作为各行业用户数字化转型的基石，赋能千行百业。

关于英特尔

英特尔（NASDAQ: INTC）作为行业引领者，创造改变世界的技术，推动全球进步并让生活丰富多彩。在摩尔定律的启迪下，我们不断致力于推进半导体设计与制造，帮助我们的客户应对最重大的挑战。通过将智能融入云、网络、边缘和各种计算设备，我们释放数据潜能，助力商业和社会变得更美好。如需了解英特尔创新的更多信息，请访问英特尔中国新闻中心 newsroom.intel.cn 以及官方网站 intel.cn。

intel®