

解决方案简介

英特尔® 至强® 可扩展处理器

英特尔® 酷睿™ 处理器

英特尔凌动® 处理器

采用英特尔® 架构的绿盟安全接入服务边缘 (SASE) 解决方案



“SASE 为用户提供了在云平台上订阅网络、安全能力的方案，支持将策略统一下发到各个云服务节点，统一管理多分支网络和安全，有助于加速云服务和网络信息化进程。通过与英特尔的合作，我们为用户提供了高性能、高安全、易部署、易管理的 SASE 服务，能够降低网络复杂度，减轻运维压力，解决传统架构带来的安全问题，切实缓解数字化企业 IT 建设之痛。”

— 官智

绿盟科技产品 BG 总经理

概述

随着企业数字化转型的速度在不断加快，以及疫情等外部因素的催化，企业对于多云，以及分布式边缘计算能力的需求正在不断增长，用户希望加速各地分支到多云、多地应用的访问，以提升应用访问效果。5G 的到来则更有力地驱动了多云、分布式边缘计算需求的提升。但同时，网络安全环境也在日趋复杂化，网络犯罪分子正在跨区域、跨网络发动网络攻击，对于企业的关键应用与数字资产带来严重安全风险。

面对这些发展趋势，传统围绕数据中心的网络安全架构已不再适应企业的数字化转型发展需求。数字化企业需要更统一、简洁的 IT 建设解决方案。在此背景下，绿盟科技 (NSFOCUS) 推出了采用英特尔® 架构的安全访问服务边缘 (SASE) 解决方案。该方案能够在云端提供身份认证、威胁防护、数据防泄漏等多项安全能力，以及广域网优化等网络能力，将安全和网络能力上移，通过统一的云交付形式，降低多分支架构的 IT 建设和运维负担。

该方案能够根据每个分支机构的需求，提供可扩展的英特尔® 处理器性能，不仅可通过英特尔凌动® 处理器满足小规模用例中的能耗与成本要求，还能通过英特尔® 至强® D 处理器或英特尔® 至强® 可扩展处理器等功能更加强大的处理器，提供硬件增强型 AI、加密加速等增强功能。

背景：SASE 赋能的企业安全与网络框架

出于提升 IT 敏捷性、加速远程访问等考虑，大量企业将业务云化作为数字化转型战略的一个重要方向。企业开始将更多应用与数据资产迁移到云端，并通过软件即服务 (SaaS) 模式来订阅应用。对于那些业务分散程度较高、分支众多的机构而言，其往往更加倾向通过多云的方式来推动业务云化战略。在多云的部署模式下，企业数据与应用大多分散在不同的公有云、私有云、混合云上，这让跨云访问与管理变得日趋复杂。

另外一个重要趋势是远程办公与协作的盛行。分支机构的员工，以及有居家办公、出差等需求的员工正通过外部网络来访问企业数据与应用。尤其是在疫情影响下，这一趋势变得更加明显。此外，越来越多的企业希望通过分布式边缘计算能力的构建，低时延访问本地存储、计算系统和设备，同时降低云端的数据访问与处理压力。

多云、移动办公与分布式边缘在给企业带来了空前灵活性的同时，也凸显了企业在网络与安全方面的巨大挑战：

● 如何降低安全风险

企业的安全边界日趋模糊化，攻击面也显著扩展。而多云、分布式边缘的部署模式让企业很难快速发现隐藏的安全攻击面。企业希望部署数据防泄漏、过滤恶意网站等多种安全防护功能，切实降低安全风险。

● 如何降低分支机构的安全部署与运维负担

在多分支机构的企业中，传统网络架构往往采用了多分支的处理模式，分支上网流量往往需要经过较长的网络链路进行处理，导致网络时延高。而随着分支机构的扩展，企业需要在每一条分支上部署安全方案，这将导致企业承担巨大的安全部署与运维负担。

● 如何提升跨区域访问的速度与安全性

数字化转型使企业的跨区域访问需求和对外部 SaaS 应用的依赖显著增加，因此企业需要跨区域的网络服务，以同时保障各地分支机构的办公效率和网络安全，降低跨区域访问的数据外泄风险。

为了解决上述问题，Gartner 于 2019 年提出了网络安全服务架构 SASE 的概念，Gartner 对 SASE 的定义是：一种结合了广域网功能和全面的网络安全功能的新兴服务产品，用于满足数字化企业的动态安全访问需求。SASE 有助于在远程地点为人工智能 (AI) /深度学习和数据分析等要求严苛的边缘工作负载提供强大、可扩展的算力，为任何网络边界之外的受攻击面提供保护。Gartner 认为，到 2023 年，SASE 将会是 WAN 边缘全新部署及更新部署中普遍使用的模型。

解决方案：采用英特尔® 架构的绿盟 SASE 解决方案

绿盟 SASE 解决方案能够在绿盟云上集成软件定义广域网 (SD-WAN) 和多种安全能力 (零信任访问控制、上网行为控制、数据防泄漏等)，对外提供网络和安全一体化的 SaaS 服务。该方案按旨在以一朵边缘云为中继，处理用户到应用、设备到应用等多种连接，提供接入控制、安全防护、网络加速等安全和网络能力。



图 1. 绿盟 SASE 解决方案

能力统一云交付

绿盟 SASE 上移了安全和网络能力，采用统一的云交付形式，由绿盟科技运营团队 7*24 小时运营，减小企业的 IT 建设和运维负担。

PoP 点全球分布

绿盟 SASE 的 PoP 节点数量多，分布在全球，对等 PoP 节点提供相同的安全和网络能力，使企业各地的分支流量均能就近接入，保证网络服务质量。

弹性云原生架构

绿盟 SASE 的网络和安全均支持弹性扩容，可以根据用户需求快速新建 PoP 点，提供网络服务，也可在 PoP 点弹性起停和扩展安全能力。

基于身份的访问控制

零信任网络访问 (ZTNA) 是安全能力的关键。与传统的以 IP 控制访问相比，ZTNA 以用户身份为核心，提供更精细化的访问控制。

绿盟 SASE 基于上述四大特点，推出了绿盟私有应用访问和绿盟互联网安全访问两大 SaaS 服务，帮助用户解决企业在数字化转型下的 IT 建设痛点问题。

其中，绿盟私有应用访问服务是一款主打零信任的内网访问安全 SaaS 服务，适用于用户到私有数据/应用的连接场景。该服务基于零信任理念，结合软件定义边界 (SDP) 技术和 SD-WAN 技术，提供了全球多点弹性 SD-WAN 组网、全面隐藏应用与网络、零信任访问控制、终端合规管理等关键能力，为客户提供服务。

绿盟互联网安全访问服务主要解决互联网访问时外部网络带给企业的安全问题。NIA 即服务化的云上安全网关，它结合上网行为管理、云安全访问代理 (CASB)、防火墙、IPS、沙箱等技术，用户提供为针对互联网威胁的强力保护。该服务具备恶意 URL 过滤、防恶意软件、数据防泄漏、外部 SaaS 应用发现和审计等能力，可从多方面帮助企业抵御互联网威胁。

绿盟 SASE 方案能够在英特尔® 架构上出色运行。绿盟 SASE 方案边缘端和云端部署了采用英特尔® 处理器的网络设备，并提供了涵盖英特尔凌动® 处理器、英特尔® 酷睿™ 处理器和英特尔® 至强® 处理器在内的广泛性能选项，用户可以根据自身的网络性能需求灵活实现 SASE 方案的本地化部署。

在边缘应用场景中，用户可以部署采用英特尔凌动® 处理器的小型边缘服务器/边缘网关，提供高性价比的网络处理资源。英特尔

凌动® 处理器不仅具备强大的计算能力，还具有低功耗、性价比高、兼容性高、安全可靠等特点。基于该处理器的边缘服务器/边缘网关能够满足自动化运维平台对于相关数据的计算和存储需求，支持平台可靠稳定地运行，并可通过对外接口实现敏捷的扩展。

在云端应用场景中，用户可以部署采用英特尔® 至强® D 处理器的服务器。英特尔® 至强® D 处理器集成了以太网、远程直接数据存储 (RDMA)、可加速网络性能的动态设备个性化 (DDP)，以及英特尔® QAT 技术。英特尔® QAT 是英特尔针对网络安全和数据存储推出的一个硬件加速技术，专注数据安全和压缩加速，助力应用程序和平台的性能提升。包括英特尔® 至强® D 处理器在内的英特尔® 至强® 可扩展处理器都内置了一系列硬件加速指令技术，包括英特尔® 深度学习加速 (英特尔® DL Boost)、英特尔® AES New Instructions (英特尔® AES-NI) 和英特尔® Advanced Vector Extensions 512 (英特尔® AVX-512)。英特尔® AES-NI 指令与英特尔® QAT 技术的结合有助于加速 SASE 方案中的安全负载，提供更佳的性能表现。此外，英特尔® 平台还提供了平台级安全增强功能，有助于保护高度分布的使用中的数据。

在软件层面上，英特尔打造了流量分析开发工具套件 (TADK) 和开源边缘计算容器化平台体验套件 (Smart Edge Open) 等众多工具，结合绿盟在安全防护技术领域的深厚积累，能够提供出色的安全网络能力。

收益：助力企业实现安全动态访问

采用英特尔® 架构的绿盟 SASE 方案能够将企业的安全能力上移，实现统一安全管理的防护效果，提高运维效率，减少重复开销。通过部署该方案，企业能够获得如下收益：

快速建设零信任安全体系

绿盟 SASE 方案为所有接入的应用统一设置了一道强认证保障，可统一配置下发场景自适应的认证策略，降低弱口令等安全风险。而且支持通过 SASE 云服务一次性订阅丰富安全 SaaS 服务，满足多方面的安全防护要求。

提升运营效率，降低安全体系建设复杂度

绿盟 SASE 云服务可配套绿盟科技的安全运营服务，为客户降低运维运营成本。用户可以统一审计日志，查看安全态势，管理终端安全。

提供统一的管理能力与用户体验

绿盟科技安全控制器能够与基于 SD-WAN 的控制器实现联动，使用户网络体验和安全体验达到一致。此外，用户能够在—个平台上统一管理所有远程访问连接，配置多样化的认证策略，并对所有用户进行精细化应用授权，由此提升远程访问的安全性。

为边缘复杂应用提供高性能网络服务

性能强大的英特尔® 处理器支持各种增强的功能特性，能够很好地满足边缘复杂应用负载的处理需求，提供高性能网络服务。

展望

在网络和安全融合之后，用户网络的配置，安全的调度未来也会走向融合。采用英特尔® 架构的绿盟 SASE 方案能够提供了高度融合的云上安全方案，结合最新隐私增强计算技术的研究成果，有助于保障企业的隐私数据安全，为更多用户提供“用得起，看得见，抓得全，管得住”的安全云服务，企业用户可以通过绿盟 SASE 快速构建安全融合网络。

英特尔将与包括绿盟在内的伙伴进行深度合作，不仅支持构建可扩展、面向未来的平台，推动企业网络的创新，使得云、网资源得以体现出最大的协同价值。同时还将更多的安全技术与能力融合到网络方案之中，帮助用户更好地保护云网之中的业务与数据资产，高效地推动数字化转型进程。

关于绿盟

绿盟科技集团股份有限公司成立于 2000 年 4 月，总部位于北京。绿盟科技在国内设有 50 余个分支机构，为政府、金融、运营商、能源、交通、科教文卫等行业用户与各类型企业用户，提供全线网络安全产品、全方位安全解决方案和体系化安全运营服务。公司在美国硅谷、日本东京、英国伦敦、新加坡及巴西圣保罗设立海外子公司和办事处，深入开展全球业务，打造全球网络安全行业的中国品牌。

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。



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.com/PerformanceIndex

性能测试结果基于配置信息中显示的日期进行测试，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。

具体成本和结果可能不同。

英特尔技术可能需要启用硬件、软件或激活服务。

英特尔未做出任何明示和默示的保证，包括但不限于，关于适销性、适合特定目的及不侵权的默示保证，以及在履约过程、交易过程或贸易惯例中引起的任何保证。

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。

© 英特尔公司版权所有。英特尔、英特尔标识以及其他英特尔商标是英特尔公司或其子公司在美国和/或其他国家的商标。其他的名称和品牌可能是其他所有者的资产。