The bridge to possible

安全访问服务边缘 (SASE)

概览

SASE 是什么？

安全访问服务边缘 (SASE) 在云中整合网络和安全功能，确保用户能够随时随地安全访问工作所需的应用。它的核心功能包括软件定义广域网 (SD-WAN)、防火墙即服务、安全 Web 网关 (SWG)、云访问安全代理 (CASB) 和零信任网络访问 (ZTNA)。过去，这些功能是在互相孤立的单点解决方案中分别提供的。SASE 的目标是将这些功能整合到一起，作为一个完整的一体化云服务提供。

SASE 可以帮助组织实现以下目标:

连接

不受环境和位置限制，将用户无缝地连接到所需访问的应用和数据

控制

无论用户在何处工作，确保实施访问控制和适当的安全保护

融合

融合网络与安全功能，以服务的形式提供安全连接

是什么原因驱动向安全访问服务边缘迁移？

随着全数字化业务转型和分布式办公模式的兴起，当今的员工需要随时随地访问存放在不同位置的资源。为迎合这些转变，需要将网络和安全功能迁移到云中，整合成一项高度融合的服务，通过灵活的部署和消费模式提供。

员工日益分散的趋势由来已久，不过最近呈现出加速之势。尽管 SASE 的基本原则早在几年前就已确立，但是直到最近，SASE 才真正受到广泛关注，这是因为远程访问各种应用和 “随时随地办公” 现已成为组织急需解决的头等大事。这种转变带来的结果是，网络的中枢不再是数据中心，而是用户。要确保员工安全地访问工作所需的资源和应用，必须将每个用户视为一个 “分支机构”。

但是与此同时，传统的分支机构并未消失。有些人可能很快就会重返办公室，这将不可避免地导致员工分布情况再次发生变化。尽管员工已开始陆续返岗，但 Gartner 最近的一项调查表明，82% 的受访者想将远程办公作为一项长期政策。[1] 相对于不断变化的形势，不变的是员工始终需要无缝地连接到工作所需的应用。

SASE 以云原生功能为基础，通过拉近网络团队与安全团队的关系来加强协作并缩短响应时间，从而简化 IT 环境。为了取得最大成效，Gartner 建议组织在挑选 SASE 解决方案时，最好选择一家既能提供丰富的安全功能，又已证明能够提供灵活的高性能网络的供应商。

我们的解决方案

思科的 SASE 架构集合了网络、客户端连接、安全和可视性功能，将这些功能打包在一个产品中提供。我们的解决方案可以帮助组织：

- 为远程员工、固定场所、任何需要上网的设备以及工作负载提供可靠连接，确保其安全地访问应用、数据和互联网
- 针对任何网络或云环境，获得从用户到应用的全面端到端可视性
- 提供无比快速、无比可靠的安全云通道，帮助优化性能
- 采用零信任网络机制验证用户身份及设备健康状况，确保基于每次会话，对应用的访问都是安全的
- 利用云简化基础设施并支持快速的扩展，帮助您提高业务敏捷性

思科的 SASE 解决方案简单省心、可视性强，而且效果卓群。组织可以利用现有资源进行部署，从而保护在本地资产和云上的现有投资，并在今后灵活地升级基础设施。在将服务从本地资产迁移到云的过程中，您可以跨所有环境一致地实施策略。借助开放的网络和安全 API，您可以轻而易举地对首选产品或思科广泛、开放的生态系统进行集成，打造最适合您的定制解决方案。

透过数字看 SASE

40%

的企业制定了明确的战略，力求在 2024 年以前采用 SASE[2]

64%

的受访者认为，网络安全形势比 2 年以前更加严峻[3]

45%

对受保护应用的访问请求来自企业边界外部[4]

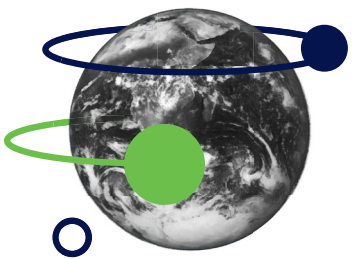
80%

的组织正在使用或评估 SD-WAN 的某项功能[3]

20%

的企业将在 2023 年以前采用同一家供应商提供的 SWG、CASB、ZTNA 和分支机构 FWaaS 功能[2]

思科 SASE 架构的组件



首屈一指的 SD-WAN 解决方案提供商

思科是全球首屈一指的 SD-WAN 解决方案提供商，市场份额排名第一，目前拥有超过 30,000 家客户

SD-WAN 连接性：思科 SD-WAN（由 Viptela 和 Meraki 提供支持）

思科 SD-WAN 是云交付的重叠 WAN 架构，用于将分支机构连接到总部、数据中心和多云环境，并为用户提供可预测的应用体验。通过灵活地集成本地或基于云的安全功能，IT 可以随心所欲地打造 SASE 解决方案。IT 团队还可以利用 Cloud OnRamp 与多个云服务提供商进行扩展集成，简化多云环境的复杂性，提高自动化程度，获得真正的零接触体验。分析功能可提供迅速隔离和解决问题所需的可视性与洞察力，并提供更可靠的网络情报。所有这些功能都可通过一个集中化的控制面板进行管理。该控制面板支持自动调配、统一策略和集成工作流等功能，有助于简化 IT 运维。借助思科 SD-WAN 云优先架构，IT 可以灵活地将任何用户连接到任何云中的任何应用。

优势

- 利用集成功能确保所有用户都能连接到所需应用，满足多云、安全性、统一通信和应用优化等方面的需求
- 借助全面的本地和基于云的安全功能（通过 Cisco Umbrella 集成）加快向 SASE 架构过渡的步伐，同时保持良好的合规性
- 对业务关键型应用提供实时分析、可视性和可控性，帮助打造更出色的应用体验并满足服务级别协议 (SLA)
- 通过 Cloud OnRamp for IaaS 将 SD-WAN 交换矩阵扩展到公共云，从而自动满足工作负载访问需求，并提高策略一致性
- 利用基于 Cloud OnRamp for SaaS 的实时分析为用户提供最佳的连接路径，帮助优化应用性能
- 通过集中控制在整个网络范围实施基于意图的策略和安全保护，有效简化运维

思科 SASE 架构的组件

远程访问连接性：AnyConnect

Cisco AnyConnect 是一款安全终端代理，可以使远程员工随时随地通过任何设备，无障碍、高度安全地访问互联网或企业网络，同时为组织提供保护。它可以为您提供所需的可视性与可控性，让您确定都有哪些用户和设备在访问整个企业网络。Cisco AnyConnect 提供了丰富的安全服务，包括远程访问、安全状况评估、Web 安全和漫游保护等诸多功能，可确保 IT 部门拥有一切所需的安全功能，打造体贴用户、稳定可靠且高度安全的远程访问体验。

优势

- 确保用户顺畅地连接到互联网、内部资源或各种应用
- 深入洞察用户对本地或外部网络的访问活动
- 对所有用户落实安全策略和设备安全状况检查
- 借助涵盖多种设备和平台的广泛支持，获得极大的灵活性
- 利用集云安全、终端安全和接入功能于一身的单一客户端简化基础设施

思科 SASE 架构的组件

零信任技术领导者

思科在 Forrester 的 Wave on Zero Trust 报告中连续两年被评为领导者

零信任网络访问：基于 Duo 的 Cisco Secure Access

基于 Duo 的 Cisco Secure Access 是一款零信任网络访问 (ZTNA)，无论用户在何处使用何种设备访问您的应用和环境，它都能提供可靠保护。ZTNA 是一种安全策略，其核心理念是在组织网络架构中杜绝一切信任。ZTNA 模型认为所有资源均位于外部，因此会持续执行可信度验证，并且仅授予必要的访问权限。

您可以使用 Duo 对员工实施零信任策略，通过为每一个应用设置自定义安全策略，确保针对每一次访问请求验证用户身份和设备健康状况。这有助于防止您的环境中出现未经授权的横向移动，防范已泄露的凭证和有风险的设备，并避免您的应用和数据受到未经授权的访问。Duo 支持的功能包括：简单有效的多因素身份验证 (MFA)、全面的设备可视性、自适应策略、VPN 或免 VPN 远程访问，以及面向任意或所有应用的单点登录 (SSO) 等等。

优势

- 无论用户和设备来自何处，始终以每次访问请求为基础建立信任
- 保护应用和网络访问活动
- 将信任机制延伸到分布式网络，满足现代企业的需求
- 跨本地、云、远程访问和 VPN 环境快速部署安全保护，将原本需要数周的工作缩短至几个小时或几天
- 集中控制访问安全，减少管理员的管理工作和帮助中心的工单数量，从而节省时间和成本

思科 SASE 架构的组件

云安全先驱

Cisco Umbrella 的保护效果和表现均位居业界领先水平，可以更快地提供全面保护

云安全可控性：Cisco Umbrella

Cisco Umbrella 是一项集多种功能于一身的云原生安全服务，它是思科 SASE 架构的核心。Umbrella 将防火墙、安全网关、DNS 层安全性、云访问安全代理 (CASB) 和威胁情报解决方案整合到一个统一的云服务中，帮助各种规模的企业保护用户、应用和数据安全。随着越来越多的组织采用直接互联网接入，Umbrella 可以轻松将保护扩展到漫游用户和分支机构。Umbrella 不仅与世界各地的高吞吐量数据中心实现了广泛的融合，还与全球 1000 多家顶级的互联网服务提供商 (ISP)、内容交付网络 (CDN) 和 SaaS 平台合作，提供最快的路由来满足任何请求，实现速度、安全性和用户满意度的同步提升。

Umbrella 支持 DNS 层安全功能，可通过禁止连接来阻止对恶意软件、勒索软件、网络钓鱼和僵尸网络的请求。安全 Web 网关会记录并深入检查所有 Web 流量，帮助加强透明度、可控性和安全保护。云交付的防火墙有助于使用 IP、端口和协议规则来记录和屏蔽流量，从而在整个环境中实现一致的实施。CASB 功能可检测并控制云应用的使用活动。此外，借助所有 Umbrella 订用中包含的 Cisco SecureX，您可以提高威胁调查和补救工作的效率。

优势

- 在威胁到达您的网络或终端之前加以阻止
- 跨所有端口和协议实现广泛、可靠的安全覆盖
- 面向网络内部和外部提供可扩展的快捷安全保护
- 利用基于情景的情报加快威胁调查和补救
- 利用单一安全控制面板实现高效管理
- 借助自 2006 年以来从未出现中断的全球云架构安享可靠性能

思科 SASE 架构的组件

可视性：ThousandEyes

随着组织对互联网和云服务的依赖性不断增加，使用非自有或非自管网络的情况日益普遍。但是，即使是在不拥有基础设施或无法控制流量路由方式的情况下，组织也需要确保底层传输机制具有良好的性能和完整性。

ThousandEyes 可以针对任意网络提供从用户到应用的全面可视性。不仅如此，它还能围绕任何性能问题提供切实可行的洞察，帮助您快速解决各种事件，从而保障连接的可靠性并优化应用体验。

优势

- 跨内部网络、ISP 网络及云和应用提供商网络快速找到问题根源，缩短平均故障发现时间 (MTTI) 和平均故障解决时间 (MTTR)
- 利用可在内部和外部利益相关者之间轻松共享的数据，有的放矢地向服务提供商提起升级流程
- 消除无意义的探查结果，在内部团队和外部供应商之间有效管理 OLA/SLA

为什么要与思科合作

实施完整的 SASE 架构无法一蹴而就，而且每个组织的情况可能各不相同。思科的 SASE 解决方案高度整合、易于部署且方便管理，可以满足您的业务扩展需求；而且无论用户选择在何处工作，这些解决方案都能在不影响速度、性能和用户体验的情况下，为其提供有效的安全保护。

领先的网络、安全和可视性技术，确保性能值得信赖

思科致力于帮助您实现卓越运营，我们高度集成的架构可让您在短短一小时内完成安全连接解决方案的部署。思科客户不仅能受益于全球分布的数据中心，而且能与数千家运营商、IaaS 和 SaaS 供应商建立直接连接，实现统一的网络控制和协调。我们与竞争对手的不同之处在于，我们能帮助您实现企业分段，优化应用体验，并通过全球服务提供可预测的性能和延迟控制。

购买简单，部署快捷

思科的一体化 SASE 解决方案可以简化购买流程。无论是云安全，还是零信任网络访问、SD-WAN 和可视性功能，您可以一次性购买所有核心组件，并在未来通过一项订用服务达成续约。无论您是选择一次购买所有组件，还是希望分批购买不同组件，思科都能帮您轻松打造切合自身需求的 SASE 架构。我们提供自动部署方案和多种产品集成选项，确保您能快速在数百个位置之间建立连接，并简化后续管理工作。

借助领先的零信任技术，将控制范围延伸到边界之外

在 Forrester 的《2020 Wave on Zero Trust》报告中，思科在市场方针、受支持度、愿景和战略、设备安全、零信任基础设施的前景等多项标准上获得了最高评分。基于 Duo 的 Cisco Secure Access 能够在用户和设备层级实施控制，验证用户身份和设备状况。Duo 可建立用户和设备信任，并提供持续的可视性，让信任机制以会话为单位进行延伸，妥善保护企业网络内部和外部环境。您可以整齐划一地执行基于用户和设备的访问策略来降低数据泄漏风险，满足合规要求。

缩短事件响应时间，提高安全保护效果

Cisco Umbrella 利用 Cisco Talos（全球最大的商业威胁情报团队之一，拥有 300 多名研究人员）的洞察来发现和屏蔽攻击中使用的各种恶意域、IP、URL 和文件。我们还将大量的全球互联网活动纳入统计和机器学习模型的组合，以识别互联网上发动的新型攻击。借助 Cisco SecureX，您可以在多个安全产品之间实现自动响应操作，从而加快威胁调查并缩短补救时间。通过消除手动任务并且更早地阻止网络攻击，安全防护可以变得更加简单轻松。

立即启航

了解为何所有财富百强企业都选择并信赖思科安全保护。联系您的思科销售代表或思科合作伙伴开启 SASE 旅程。

1. https://www.gartner.com/en/newsroom/press-releases/2020-07-14-gartner-survey-reveals-82 percent-of-company-leaders-plan-to-allow-employees-to-work-remotely-some-of-the-time
2. Gartner，“The Future of Network Security Is in the Cloud”（网络安全的未来在云中），2019 年 8 月
3. Enterprise Strategy Group，“Transitioning Network Security Controls to the Cloud”（将网络安全控制迁移到云端），2020 年 5 月
4. 思科，“Duo Trusted Access Report”（Duo 可信访问报告），2019 年

03/21