Magic WAN

Magic WAN 通过任意对任意连接性简化 SASE 实现

网络架构的演变

互联网就是新的企业网络

随着混合办公成为新常态，应用迁移到云端，IT 团队正在努力应对以下问题：

- **网络复杂性：**MPLS 配置和调整单点解决方案耗时太长
- **安全漏洞：**直连互联网绕过安全和可接受使用策略，使用户和数据面临风险
- **成本高企：**MPLS 链路和单点安全解决方案造成不必要的支出
- **用户体验不佳：**将流量回传到边界安全堆栈会带来延迟

Magic WAN 简化了从分支机构站点、多云 VPC 或数据中心到 Cloudflare One SASE 平台的网络连接，提供安全、高性能和经济的连接，为 IT 团队解决混合办公和多云挑战。

不同于僵化、昂贵的 MPLS 网络，或者使用本地防火墙上构建的复杂 SD-WAN 部署，Magic WAN 采取“轻分支，重云端”方法来增强或取代您当前的架构。它易于部署，可根据您不断变化的业务需求进行扩展，且内置安全。

Magic WAN 将物理或虚拟网络位置连接到 Cloudflare 的 SASE 平台。物理站点的示例包括分支机构、工厂厂房、零售店铺、总部或数据中心。虚拟位置的例子包括 AWS、Azure、GCP 和 OCI 等公共云服务。

更佳的运营敏捷性

从一个控制台集中管理网络安全和连接。零接触接入流量仅需几分钟。

内置而非附加的安全性

获得云原生的 DDoS 防护、网络防火墙、SSE 和 Zero Trust 功能——全部深度集成并作为服务交付。

降低网络成本

最小化分支机构占地面积，将网络功能转移到云端，减少依赖昂贵的 MPLS，并从 SD-WAN 迁移出来。

Magic WAN 的主要用例

简化网络连接

- **简化分支机构连接** — 利用 Anycast IPSec 安全地在分支机构和数据中心之间路由流量，取代各种专有电路和网络设备的混合拼。便利不同地点之间的站点到站点连接。
- **简化混合和多云连接** — 组织在不同提供商（例如 AWS、GCP、Azure、Oracle、IBM）*和*本地数据中心的云实例中拥有应用程序。使用集中控制在这些不同的环境之间路由和保护流量。

增强安全而不牺牲性能

- **保护 WAN 连接** — 通过云交付的防火墙和 SWG 控制，在各个位置（分支机构、数据中心等）之间执行网络安全策略以保护连接。
- **提升 WAN 性能** — MPLS 部署昂贵、不灵活且缓慢。切换到 Cloudflare 可以实现成本更低、更灵活的部署，并内置安全性。

接近 Magic WAN 部署

网络转型是一个旅程

Magic WAN 提供了互联网连接的性能和可靠性，并帮助组织从传统网络架构迁移。从逐步部署 Magic WAN 开始 Cloudflare 的“轻分支、重云端”方式结合了最后一公里连接和中间一公里的性能、可靠性和安全性，更好地帮助连接和保护混合办公。我们的架构支持与现有基础设施并行部署，以便按照您的步伐进行迁移。

比较 Cloudflare One 与 MPLS/SD-WAN

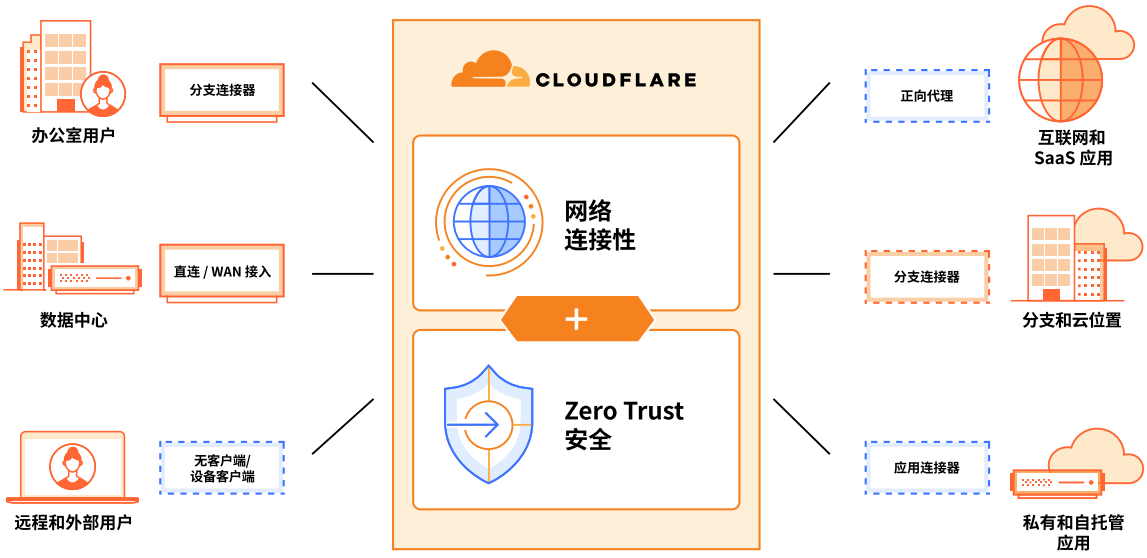
随着应用程序上云，组织采用混合办公模式，传统网络架构面临性能和安全下降的问题。回传流传影响性能和用户体验，而允许本地直接访问互联网影响安全的一致性和有效性。两种情况均不理想，因此网络设计做出妥协，导致组织和个人需求无法得到满足。

最近，SD-WAN 添加了覆盖层来管理流量，希望提供一种替代 MPLS 的选择。然而，SD-WAN 很大程度上依赖边缘设备来实施安全性，导致团队需要将硬件、虚拟化和基于云的工具拼凑在一起。结果是，增加的复杂性抵消了很多预期的好处。

Cloudflare 的 SASE 平台将安全和网络融合在我们的全球连通云中，允许组织将我们的网络作为其自己网络的延伸。简化管理、可靠性能、现代 Zero Trust 安全和更低的总拥有成本，这些只有通过真正革命性的方法才能同时实现。

标准	MPLS/VPN 服务	SD-WAN	Cloudflare One 的 SASE 平台
配置 新站点设立、配置和管理	服务请求由 MSP 提供	通过集中控制器简化编排和管理	通过 SaaS 门户自动编排；集中的仪表板
最后一公里流量控制 流量平衡，QoS，故障转移	由 MPLS SLA 覆盖	SD-WAN 设备中提供的最佳路径选择	最小化本地部署以控制本地决策
中间一公里流量控制 绕过中间一公里拥堵的流量引导	由 MPLS SLA 覆盖	“隧道错综复杂”，但依然未能控制中间一公里	相同界面集成流量管理和专用骨干网控制
云集成 适用于云迁移的连接	集中访问	非集中访问	使用 Cloud Network Interconnect 的原生连接
安全性 过滤进出互联网流量以防恶意软件	拼凑的硬件控制	拼凑的硬件和/或软件控制	原生集成用户、数据、应用和网络安全工具
费用 最大化网络投资的 ROI	硬件和连接的高成本	优化连接成本以增加硬件和软件成本为代价	降低硬件和连接成本以最大化 ROI

将流量引导至 Cloudflare 的 SASE 平台



Magic WAN 连接器可以轻松地将您的网络位置连接到 Cloudflare。使用 Cloudflare 认证硬件设备上预安装和配置的分支连接器软件以简化部署，或将软件部署到您的环境中的物理或虚拟 Linux 设备上。

属于一个不断扩大的灵活入口方式家族

采用 SASE 的第一步是建立连接——从现有的网络中建立一个安全的路径，到达可应用 Zero Trust 安全策略的最近节点。Cloudflare 提供了多种实现这种连接的“入口”，包括适用于混合用户的客户端和无客户端访问选项，通过部署一个轻量级软件后台进程建立的应用层隧道，通过标准 GRE 或 IPsec 隧道建立的网络层连接，以及私有数据中心和公共云的物理或虚拟互连。

为进一步简化 SASE 的采用，Magic WAN 连接器可以部署在任何物理或云网络位置，自动连接到最佳的 Cloudflare 数据中心，利用您现有的最后一公里互联网连接，IT 团队不再需要手动配置网络设备以进行连接。

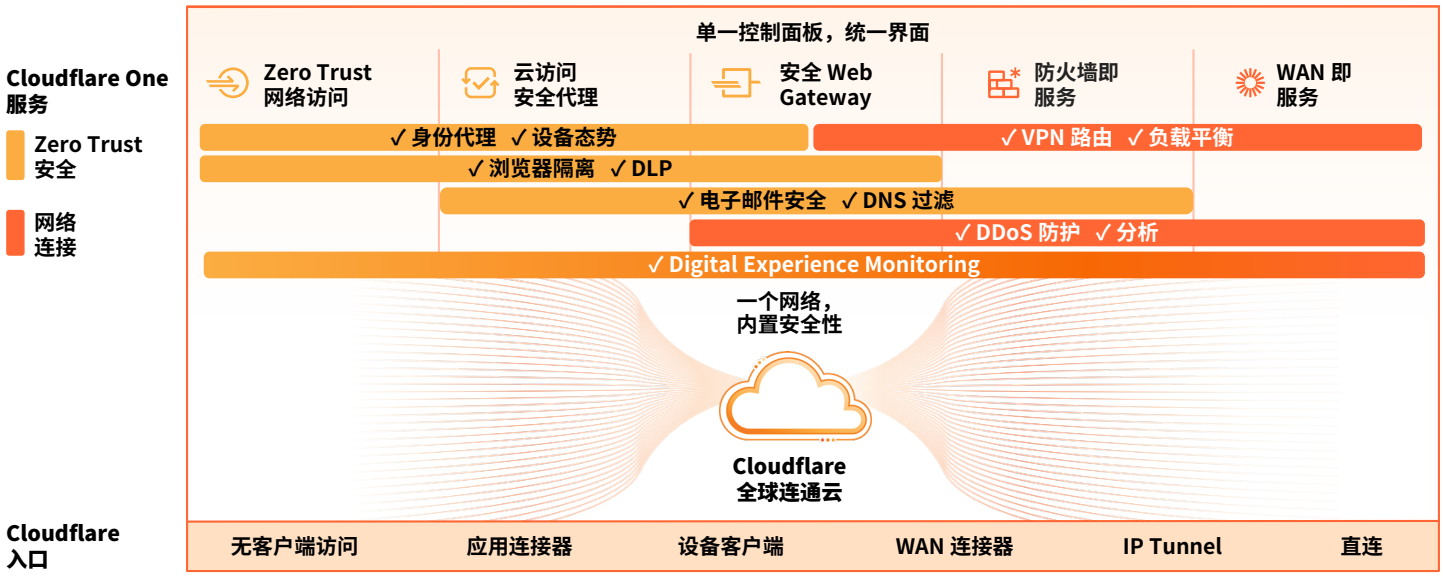
软件功能和硬件规格

Magic WAN 软件功能[1]	
WAN 连接器设置	即插即用、零接触配置的 CPE 设备，通过 Cloudflare 仪表板/API 集中管理。自动设置 IPsec 隧道和路由，将流量直接引导到 Cloudflare 网络中，以获得连接和安全功能。自动升级软件（在客户定义的服务时段内）。
WAN 连接器站点配置	WAN/LAN 支持静态 IP 或 DHCP 配置。 支持 VLAN 和本地网络分段。
“轻分支、重云端”方式	高可用轻量级 WAN Connector，提供跨多个 WAN 电路基于运行状况检查的负载平衡和故障转移。Cloudflare 全球连通云提供防火墙和 Zero Trust SSE 能力等安全服务。
第三方集成	使用现有的云 VPC（例如 Amazon AWS Transit Gateway）或客户本地设备（例如 SD-WAN、防火墙和路由器设备）配置 Anycast IPsec 或 GRE隧道端点。通过 ECMP 包转发配置到 Cloudflare 网络的静态路由。
内置安全性	内置 L3 防火墙和入侵检测；与其他 SSE/安全功能和入口点（例如 L4-7 安全 Web 网关、设备客户端、应用连接器等）无缝集成。
可见性和控制	基于应用程序的流量检测和路由。带宽控制。通过仪表板、API、日志或 GraphQL 提供的隧道、流量和设备指标可见性/分析。使用 Cloudflare 仪表板、API 或 Terraform 进行管理。
Magic WAN 连接器 硬件选项规格[2]	
设备规格	• **端口：** (6x 1G 铜缆 RJ45) + (2x 10G SFP+) + (2x USB 3.0 Type A) • **尺寸：** 8.1x7.9x2.0 英寸；1.5RU；**重量：** 2.87 磅 • **安装选项：** 桌面放置，壁挂，或机架安装（带托盘） • **TPM：** 2.0，全球（中国除外） • **CPU：** Denverton 4 Core C3558 • **硬盘：** M.2 120 SSD 带 16G eMMC 闪存 • **内存：** 8 GB DDR4 • **WiFi & 蓝牙：** 802.11ac，2x2 MIMO，最大物理速率：866.7 Mbps • **风扇：** 1 个

[1] 所有 Magic WAN 功能级别文档请参考 Cloudflare 文档
[2] 预安装 Magic WAN 软件的 Cloudflare 认证硬件：Dell VEP 1425，通过合作伙伴销售（机架安装）

网络连接和通向 SASE 的旅程

在您整合单点产品并统一 IT 战略之际，Cloudflare 的全球连通云提供部署简易性、网络韧性和创新速度，以帮助您保持领先地位。



Cloudflare One 正在赋能各种大小的组织实现 SASE 转型：将任何流量来源和目的地连接到一个安全、快速、可靠的全球网络，在其中执行所有安全功能，并优化流量的传输，无论目的地在专用网络上还是在公共互联网上。

无论组织是从成熟的 MPLS 或 SD-WAN 部署中卸载流量，还是首次进行网络转型，Magic WAN 都可以帮助简化这个过程。Cloudflare One 同时提供 Zero Trust 安全和 WAN 即服务，实现了单一供应商 SASE，但也可作为多供应商战略的补充，为您的 SASE 旅程提供协助。

让我们讨论一下贵组织的网络连接问题

申请研讨会

CLOUDFLARE

进一步了解 **Cloudflare 的 SASE 平台**。