利用 VMware SD-WAN 实现企业 WAN 简便性、高性能和安全性

vmware®

SD-WAN™

VMware SD-WAN 提高了敏捷性和成本效益，同时确保跨 WAN 的企业站点的应用性能和网络安全性。

随着企业试图提高敏捷性和经济性，纷纷将应用转移到云端，WAN 也因此发生转变。VMware SD-WAN™ 能够提供企业级性能、安全性、可见性以及对公共 Internet 和专用网络的控制。VMware SD-WAN 凭借零接触式部署、一键式业务策略、增强型防火墙服务、简单的服务注入和云端网络即服务，大幅简化了 WAN。最终，带来了性能更加卓越的 WAN，具有更高的可靠性和更低的拥有成本，并为分支机构和远程用户提供了更好的安全保障。

如今，随着分支机构用户进行在线协作（例如 Zoom、WebEx 和 Microsoft 365）、使用软件即服务 (SaaS) 和云服务、访问大型富媒体文件以及使用其他带宽密集型应用，他们正在消耗更多广域网 (WAN) 带宽。由于其现有 WAN 的体系架构复杂性、缺乏安全性和成本问题，企业 IT 部门面临着重大挑战。

大多数分支机构的 WAN 流量都是通过昂贵的租赁线路（如专用 MPLS 线路）或不可预测且不安全的 Internet 连接（例如 DSL、电缆和 LTE）传输的，这两者本身都不是非常理想的选择。部署租赁线路来满足带宽需求成本高昂且耗时。由于使用公共 Internet 时缺乏稳定性和对网络攻击的防护，可能导致用户体验不佳。此外，传统 WAN 还有许多固有的安全性问题。

借助 VMware SD-WAN，企业能够支持应用增长、简化分支机构实施、提升网络和员工敏捷性并增强网络安全性。VMware SD-WAN 不仅同时优化了对使用各种类型传输的云服务、专用数据中心和企业级应用的访问，还通过增强型防火墙服务、入侵检测系统和入侵防御系统 (IDS/IPS)、托管防火墙日志记录等功能降低了网络攻击的风险，而所有这些工作都可在一个统一的管理门户下完成。

分支机构 WAN 面临的挑战

当今大多数分支机构所使用的 WAN 技术与过去二十年相比几乎没有任何改变。它们最初是为本地部署的专用数据中心中的应用而设计的。如今，传统的分支机构 WAN 体系架构面临着许多网络连接和安全性挑战。一些常见的挑战包括：

- MPLS 通常能够提供高质量的服务，但容量有限、成本较高且部署准备时间较长。只具有专用线路连接的分支机构依赖于通过企业级数据中心对所有云应用、SaaS 和 Internet 流量回程传输，从而增加了延迟，降低了应用性能并推高了网络带宽的成本。传统的中心辐射型 WAN 体系架构可能不支持云迁移。
- 宽带提供了快速部署和更大的容量，但可能缺乏可靠性、安全性和性能保证，导致用户体验不佳。
- 传统的分支机构网络缺乏集中管理、控制、可见性以及对网络攻击的防护。管理工具的种类太多，会使故障排除工作很困难或是难以快速应对威胁。
- 由于不同供应商提供的安全解决方案不同，因而可能难以跨多个分支机构维护合规性要求（例如 PCI、HIPAA、GDPR 等）。

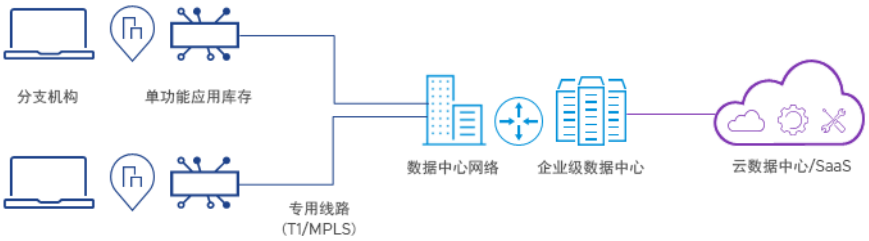

图 1：传统分支机构 WAN

VMware SD-WAN 概述

VMware SD-WAN 凭借基于云端服务的部署速度和低维护成本，提高了混合 WAN 的经济性和灵活性。它包括基于策略的全网络应用性能、可见性和控制力，同时通过将虚拟化服务从云环境传递到分支机构来显著简化 WAN。

VMware SD-WAN Edge 是一种精简、紧凑的边缘设备，可从云端进行零接触式置备，与应用和数据实现经优化的安全连接。VMware SD-WAN Edge 也可作为一项虚拟网络功能 (VNF) 用于客户本地设备 (CPE) 平台上的实例化，以实现极大的部署灵活性。

VMware SD-WAN Edge 使用动态多路径优化™ (DMPO) 和深度应用识别功能来提高交付可靠性。它聚合了多个链路（例如专用线路、电缆、DSL、4G-LTE 或 5G、卫星），并通过最佳链路将流量引导至位于分支机构、专用数据中心、园区和总部的其他本地部署 VMware SD-WAN Edge。VMware SD-WAN Edge 还可以选择性地连接到全局 VMware SD-WAN Gateway 系统，为云服务（SaaS、IaaS 和 B2B Internet）提供卓越的性能、安全性和可见性。

Edge 内置的增强型防火墙服务基于 VMware NSX 安全技术，进一步加强了 SD-WAN 分支机构的安全性。通过将 NSX 安全技术与 VMware SD-WAN Edge 平台相结合，客户可以在不牺牲安全性的情况下消除分支机构的传统防火墙，并从简化的网络和安全性运维中受益，同时还能利用 VMware 在威胁情报方面的投资。

VMware SD-WAN Gateway 系统在顶层云计算数据中心内全局部署，以提供可扩展的按需云网络服务。VMware SD-WAN Gateway 在全球云服务（SaaS、IaaS、网络服务）和每个 VMware SD-WAN Edge 之间实施 VMware DMPO、云 VPN 和 VMware Multisource Inbound 服务质量 (QoS)，使多个宽带和专用租用线路显示为单个高性能 WAN。云端 VMware SASE Orchestrator 用于提供网络级业务策略，启用服务注入功能，执行实时监控以及分析应用性能。

几分钟内即可完成部署

借助 VMware 的零接触式部署能力，可以快速安装 VMware SD-WAN Edge。Edge 被运送到分支机构后，非技术人员只需连接电源和网络电缆即可。激活、配置和日常管理均在云端处理。

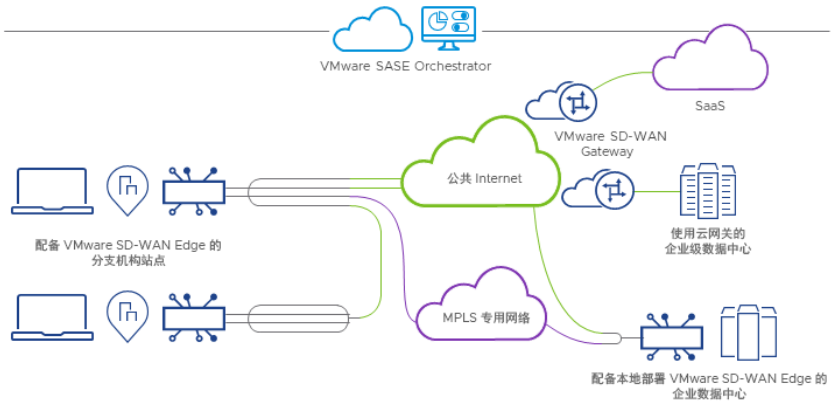

图 2：VMware SD-WAN 服务

企业范围的业务策略

有了 VMware SD-WAN，只需单击一下即可完成策略设置。企业或其代管服务提供商可以定义跨许多 Edge 应用到整个企业的业务级策略，所有这些均通过集中式云端 Orchestrator 实现。链路转向、链路修复和 QoS 都根据设定的业务策略自动应用；但是，也可以使用特定的配置进行覆盖。集中式 VMware SASE Orchestrator 还在一个叠加流控制表中提供路由的企业范围视图和可配置性，消除了复杂的逐节点路由配置。

有保证的应用性能

VMware SD-WAN 通过实施其独特的 DMPO 来提高混合网络或标准宽带 Internet 链路的服务级别和容量。这包含了几种技术：

持续监控

自动分析 WAN 线路，可实现零接触式部署，无需手动逐个站点调整配置参数。持续监控链路和路径质量及可用容量，为动态优化提供实时反馈。

动态应用流量引导

可自动识别应用，并根据业务优先事项、内置的关于应用网络要求的知识以及实时链路性能和容量指标将其引导至最佳链路。以数据包为单位的动态流量引导可将一个会话（例如一个电话呼叫）移至中流以避免链路性能降级，而不会造成电话挂断或出现语音质量缺陷。单个高带宽流可以利用聚合带宽加快响应速度。

按需修复

当只有单个链路可用或无法绕过并发链路降级时，将按需修复应用（包括纠错、抖动缓冲和本地重新传输）。修复只应用于对网络敏感的高优先级应用，且仅在管制性链路性能降级时应用。

优质体验

具备 DMPO 功能的 SD-WAN 叠加可实现特定于应用的优质体验。应用性能得到保障，通过跨包括专有和 Internet 宽带在内的多个链路的虚拟叠加而提供了一个高质量、高容量的 WAN。

统一且强大的安全保护

无论底层传输类型如何，VMware SD-WAN 都能提供统一、安全的通信。在分支机构和数据中心之间，以及为分支机构内部通信提供端到端的标准 IPsec 加密。此独特的云交付体系架构还提供从分支机构到云网关聚合点的自动化 VPN，以实现对 IaaS 的可互操作访问，从而不再需要以手动方式设置从 1XN 个分支机构到 1XN 个云数据中心的双向加密链路。此解决方案通过整合对集成式证书服务器的管理、安全的设备纳管及撤销管理，提供了公钥基础架构 (PKI) 所具备的可扩展性和强大的安全性。通过将证书精确定位到具体的设备并使用独特、可识别配对的加密密钥，风险得到了最大限度的降低。

VMware SD-WAN 解决方案在 Edge 的数据平面中内置了重要的安全功能。除了有状态防火墙以外，它还提供其他功能特性，例如流量分段、入侵检测和防御 (IDS/IPS)、托管防火墙日志记录等。Edge 设备上运行的增强型防火墙服务通过检测对企业网络资产的未经授权访问、降低威胁和抵御网络攻击，提高了分支机构网络的整体安全性。如今，分布式企业极大地受益于增强型防火墙服务，该服务不仅能够提供用户流量保护、整合的硬件、简单统一的管理，而且还能减少运营开销和节省总体成本。VMware SD-WAN 中内置的增强型防火墙服务对企业的数字化转型计划至关重要。

一键式服务交付

VMware SD-WAN 解决方案简化了分支机构、整合度更高的企业服务中心和云环境的服务部署，不再需要在分支机构中部署许多单功能设备。一键式服务置备可在分支边缘激活多项 VMware 原生服务和来自技术合作伙伴的第三方 VNF。一键式业务策略可以轻松地以应用级精确度为从分支机构到企业级服务中心和云服务的链式流量提供服务。

VMware SD-WAN 组件

VMware SD-WAN Edge 在分支机构中提供零接触式 SD-WAN 部署，并为总部和数据中心位置提供可扩展的本地中心部署。

此外，SD-WAN 的所有优势（即，有保证的性能、安全性和策略控制）均可通过 VMware Gateway 直接在各个云端 SaaS 和 IaaS 位置获得。云端 VMware SASE Orchestrator 提供企业范围的业务策略、配置、故障排除和一目了然的监控。

VMware SD-WAN Edge

VMware SD-WAN Edge 是易于安装的设备，适用于具有一系列吞吐量、WAN 和 LAN 连接端口、集成式无线 LAN 以及安全防火墙服务的远程分支机构。不论是内联部署还是路径外部署，动态路由均支持基于策略的叠加注入。高可用性 (HA) 设置提供了冗余和故障转移。除了设备选项外，VMware SD-WAN Edge 还作为 VNF 软件提供，用于在标准 x86 服务器上（包括虚拟 CPE 设备）上进行部署。增强型防火墙服务可保护企业 SD-WAN 分支机构站点，防止他人未经授权访问内部网络资产。凭借内置的高级安全功能（例如应用感知和会话感知防火墙、IDS/IPS、托管防火墙日志记录等），增强型防火墙服务可以主动抵御各种网络攻击，减少可能造成严重泄露的威胁。

VMware SD-WAN Gateway

多租户 VMware SD-WAN Gateway 由 VMware 及其合作伙伴部署到全球顶级网络接入点 (PoP) 和云计算数据中心，以获得各种 SD-WAN 优势。VMware SD-WAN Gateway 提供可扩展的分布式基础架构，具有托管的网络即服务灵活性优势。VMware SD-WAN Gateway 为优化访问云应用和数据中心以及访问专用网络主干网和传统企业站点提供了理想的体系架构。

VMware SASE Orchestrator

VMware SASE Orchestrator 是一个云托管（或本地部署）的中央管理工具，适用于所有 VMware SASE 组件：VMware SD-WAN、VMware Secure Access、VMware Cloud Web Security 和 VMware Edge Network Intelligence。其基于 Web 的用户界面 (UI) 提供了简化的配置、置备、监控、故障管理、日志记录和报告功能。Orchestrator 能够灵活地实施基于业务的应用交付和流量管理策略。

VMware SD-WAN Client

VMware SD-WAN Client 是面向当今分布式企业员工的安全、高性能的云管理远程访问解决方案。VMware SD-WAN Client 基于零信任网络访问 (ZTNA) 并针对速度进行了优化，可确保应用质量，在保护远程员工的同时提高工作效率。

由云管理的、可扩展的客户端服务在几分钟内就能设置完毕。它取代了僵化的 VPN 基础架构，无需 SD-WAN Edge 设备，即可在服务器、云和远程员工的桌面或移动设备之间提供高性能的专用网络架构。优化用户流量路径，避免发夹式传输。VMware SD-WAN Client 能够显著降低 IT 部门的资本和运营费用，同时让外出途中或远程办公的用户也能获得 SD-WAN 体验。

用于 WAN 的安全 SDN

VMware SD-WAN 将软件定义的网络 (SDN) 概念落实到企业分支机构 WAN 中。VMware 基于软件的方法实现了部署上的灵活性和移动性：既可以将虚拟 SD-WAN Edge 部署在现成的基于 x86 的硬件上，也可以作为 VNF 部署在虚拟 CPE 上。

跨逻辑叠加实施的业务策略可将应用流从底层物理传输中分离出来。通过调整转发以符合策略要求及实时链路情况，可实现敏捷性。SD-WAN 具有分布式控制平面，用于转发通过上下文在本地做出的决策，因此，WAN 上不存在延迟问题或故障点。每个 SD-WAN 节点都接收集中控制策略，以实现轻松的可编程性和企业范围的可见性。安全策略从 SASE Orchestrator 用户界面集中配置，并在分支机构的 Edge 设备上实施。可以使用 GUI 或 REST API 进行管理。

VMware SD-WAN 和 VMware Secure Access Service Edge (SASE)

VMware SD-WAN 是整个 VMware SASE 解决方案的一个组成部分，它融合了云托管 SD-WAN 的网络和高级安全服务。VMware SASE 旨在充分利用云计算的强大功能，同时最大限度降低边缘环境的复杂性，是一个易于使用的平台，通过一个统一的门户来管理业务策略、安全性、配置和监控，实现统一的边缘和云服务模式。

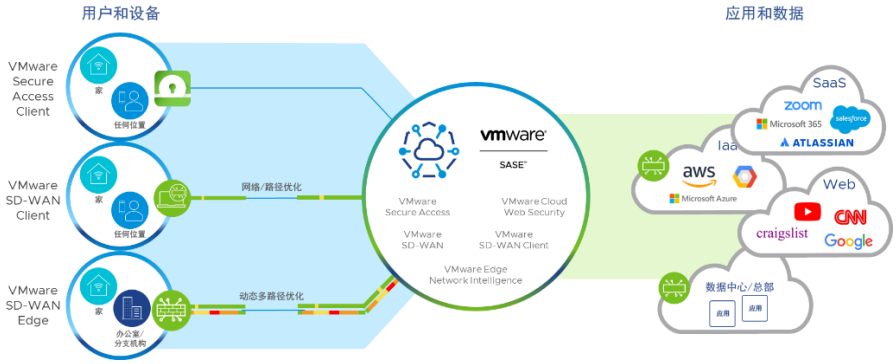

图 3：VMware SASE

了解更多

- VMware SD-WAN，*sase.vmware.com/sd-wan*
- VMware SASE，*sase.vmware.com*

需要最佳和安全的云应用访问权限的远程员工和移动员工可以使用 **VMware Secure Access™**。通过将远程部署用户引入到 VMware 架构中，使远程用户能够访问云端应用，这些应用针对交付和性能进行了优化，能够充分利用零信任网络访问 (ZTNA) 和云托管解决方案的优势。VMware Secure Access 可简化成本高昂的虚拟专用网络 (VPN) 服务的 IT 部署和维护。

VMware Cloud Web Security™ 为 IT 团队提供了用户访问 SaaS 应用时的可见性和控制力，并可确保实现合规性。它还包括 URL 过滤功能，可帮助 IT 部门限制员工可以或不可以访问的网站。IT 部门还可以借助内容过滤，通过确定用户可以或不可以访问或上传的具体内容类型来减少受攻击面。使用最新的威胁情报检查内容中是否存在来自已知病毒的恶意软件攻击。该解决方案通过沙箱支持在封闭的环境中检查内容，来抵御零日威胁恶意软件攻击。

VMware Edge Network Intelligence™ 是一款 AIOps 解决方案，可为 IT 部门提供对于物联网及其网络上终端用户设备的真实可见性和分析功能。IT 部门可以获得对其无法控制的网络（比如远程用户的家庭网络）的可见性。这一久经考验、不依赖特定供应商的解决方案为在任何地方办公的员工提供了丰富的客户端体验，并使 IT 部门不再追根究底，而是采取主动的补救措施。

VMware, Inc.
北京市海淀区科学院南路 2 号融科资讯中心 C 座南楼一层 邮编：100080 电话：+86-10-5976-6300 传真：+86-10-5976-6302
上海市淮海中路 333 号瑞安大厦 805B-809 室 邮编：200021 电话：+86-21-8024-9200
广州市天河路 385 号太古汇一座 3502 室 邮编：510610 电话：+86-20-87146110
香港港岛东太古城太古湾道 12 号太古城中心 4 期 4 楼 电话：852-3696 6100 传真：852-3696 6101
www.vmware.com/cn

项目号：sdwan-564-Enterprise-WAN-Agility-so-0321