Doyle 研究

借助软件定义广域网 (SD-WAN), 确保多云环境的安全

作者：Lee Doyle， Doyle Research 首席分析师

由思科赞助

摘要

在本世纪，最重要的 IT 转型当属基于云的应用的快速采用。目前，大多数组织都依赖许多 SaaS 和 IaaS 平台来实现客户满意度目标并提高员工工作效率。IT 需要负责提供高质量的云应用用户体验，同时全力应对高级持续性威胁，确保环境安全。

广域网作为交换矩阵，可连接远程用户与基于云的应用并进行访问控制。广域网交换矩阵需要确定相应（多个）广域网链路中的应用类型、位置、应用优先级和路由流量，以便实现出色的用户体验。（通过互联网）连接到云的用户/设备具有不同类型，这意味着在分支机构、数据中心和云端都必须实施安全策略。

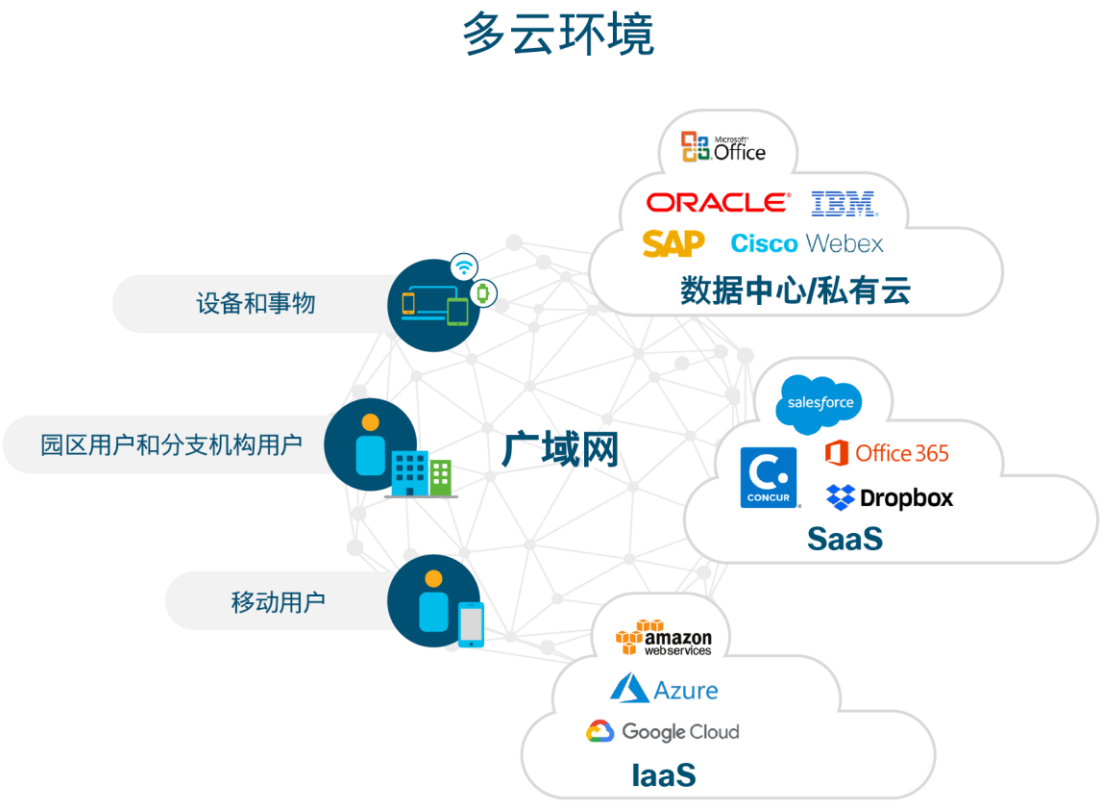
目前，对分散在多个分支机构位置的用户而言，软件定义广域网是他们连接到基于云的应用的主要解决方案为应对这种多云环境的挑战，软件定义广域网技术始终在不断发展，以期在多种云平台上提供安全可靠的连接。由于各类 IT 环境的独特性，软件定义广域网必须采用一种灵活的方法，并为直接互联网接入、区域托管以及基于云的路由、策略和安全提供多种选项。

为满足多云环境的要求，软件定义广域网需要让 IT 能够轻松地集中管理和监控用户的云流量。它应该能优先处理关键应用并加快其交付速度。基于意图的功能可以帮助 IT 将组织的业务要求转化为基于网络的策略。
防火墙、入侵检测和 URL 过滤等安全功能应成为软件定义广域网解决方案不可或缺的组成部分。 IT 组织需要在分支机构、主机托管设施或 IaaS 平台灵活地部署软件定义广域网和安全实例。

多云环境的出现

基于云的新技术让组织能够在数据中心、SaaS 和 IaaS 平台组成的混合环境中轻松地部署/使用应用。在应用分散化的同时，随着典型的组织可以从分支机构位置、家庭办公室和移动位置办公，他们也呈现出日益分散化的特征。多云环境让 IT 能够利用各种本地（数据中心）和基于云（IaaS、PaaS 和 SaaS）的资源来实现 IT 敏捷运营。根据 IDC 最近的调查，85% 的组织当前使用不止一家提供商的基于云的服务，这一百分比预计在未来 12 个月内将会增长到 93%。请参见图 1。

图 1.



多云环境对网络要求的影响

目前，IT 组织负责管理各种私有云、公共云和 SaaS 平台，以便他们的用户（和开发人员）无论身处何处，都能灵活地在最合适的平台上运行应用。这就导致了环境碎片化，其中充满各种不同的用户要求、多种平台接口和始终存在的安全威胁。在多云环境中，广域网平台不仅必须要提供基本连接，还必须要随时随地为安全应用交付提供所需的支持。

多云 IT 环境的兴起给 IT/安全团队带来了许多挑战。每个新的云平台都具有独特的管理/运营接口，这些接口都需要 IT 人员来管理。IT 需要监控通往各种云平台的多个广域网路由，并为每个环境（例如，AWS、Azure、Office 365 和 Salesforce）提供高质量的用户体验。使用互联网链路连接到各种 IaaS 和 SaaS 平台会给组织带来更多安全风险。请参见图 2。

图 2.

为多云流量选择软件定义广域网时的考虑因素

大多数地理位置分散的组织已实现了从传统广域网架构（所有分支机构流量都发送到中央数据中心）向混合广域网设计（流量通过互联网直接流向云资源）的迁移。这意味着何种流量应发送到基于云的特定位置最先是由软件定义广域网决定的。 软件定义广域网技术需要确定流量的类型和目的地，了解其定义的业务和安全策略，并主动使用合适的优先级来路由流量。例如，组织需要能够将不同的业务和安全策略应用于任务关键型 SaaS/IaaS 应用、实时语音与视频流量、Office 365 用途、批量文件传输和 IoT 流量。

为多云运营选择软件定义广域网平台时的主要考虑因素包括：灵活的架构、提供高质量的用户体验、安全和运营简便性，具体如下所述。

灵活的软件定义广域网多云架构

组织需要灵活地设计广域网架构，才能适应其独特的业务和应用要求。为确保最终用户获得高质量的用户体验，软件定义广域网必须为基于互联网的应用提供多条路径和多个控制点，包括直接互联网接入 (DIA)、区域网络枢纽的主机托管和基于云的网关，以及实时在这些路径和控制点中进行动态路由决策。在多云广域网架构中，每种接入/控制方法都发挥着其自身的独特作用。

- 直接互联网接入 - 在远程站点使用一个或多个互联网链路来允许流量从基于云的指定应用直接访问互联网。

- 主机托管区域网络枢纽 - 在区域网络枢纽（例如 Equinix 站点）托管软件定义广域网/安全软件可以整合分支机构流量并确保其安全性。这有助于简化安全运营。
- 基于云的软件定义广域网。虚拟软件定义广域网实例可在 IaaS 合作伙伴（例如 AWS 和 Azure）处进行调配，以控制和优先处理基于云的流量，并确保其安全性。

高质量的用户体验

我们通常会根据 IT 组织为最终用户提供高质量应用体验的能力来对其进行评价。用户的期望是，无论他们自己（和应用）身处何处，都能不间断地快速访问所有关键应用。能够利用具备适当故障切换功能的多个广域网链路将有助于提高访问的可靠性。软件定义广域网会确定和优先处理关键应用，并使流量能够在任意给定时间在“最佳”链路上运行。

软件定义广域网交换矩阵会衡量 SaaS 应用在不同托管位置的性能，并使用分析功能以确保应用选择最佳路径来实现最佳性能。网络管理员可以评估性能数据并按需调整策略，以满足组织需求。可以通过在关键点增加广域网带宽来提高性能。

安全

直接通过互联网访问大量云应用型应用会给组织带来更多安全风险。IT 和安全团队需要能够在任何网络上安全地连接任何用户与任何应用。这就需要为远程用户在分支机构、广域网和云端提供统一的安全架构。

软件定义广域网平台需要高级防火墙、加密、高级威胁检测和网络分段等高级安全功能来应对威胁环境。这些平台应能够确保分支机构、主机托管站点和云端的安全，并能够集中管理端到端（从用户到云）用户策略。

运营简便性

由于调配和运营分散在大量远程位置的网络所造成的复杂性，IT 组织面临着越来越多的挑战。他们需要能够通过“零接触”调配来快速设置新分支机构的网络，并迅速从中央位置解决任何网络或应用的速度缓慢问题。软件定义广域网平台必须能够提供“即插即用”部署和运营简便性。这些平台应能够自动确定应用性能问题并进行补救。集成网络和安全功能应能够进行集中管理，并使用运营情报来帮助 IT 解决网络或安全问题。

思科面向多云环境的软件定义广域网解决方案

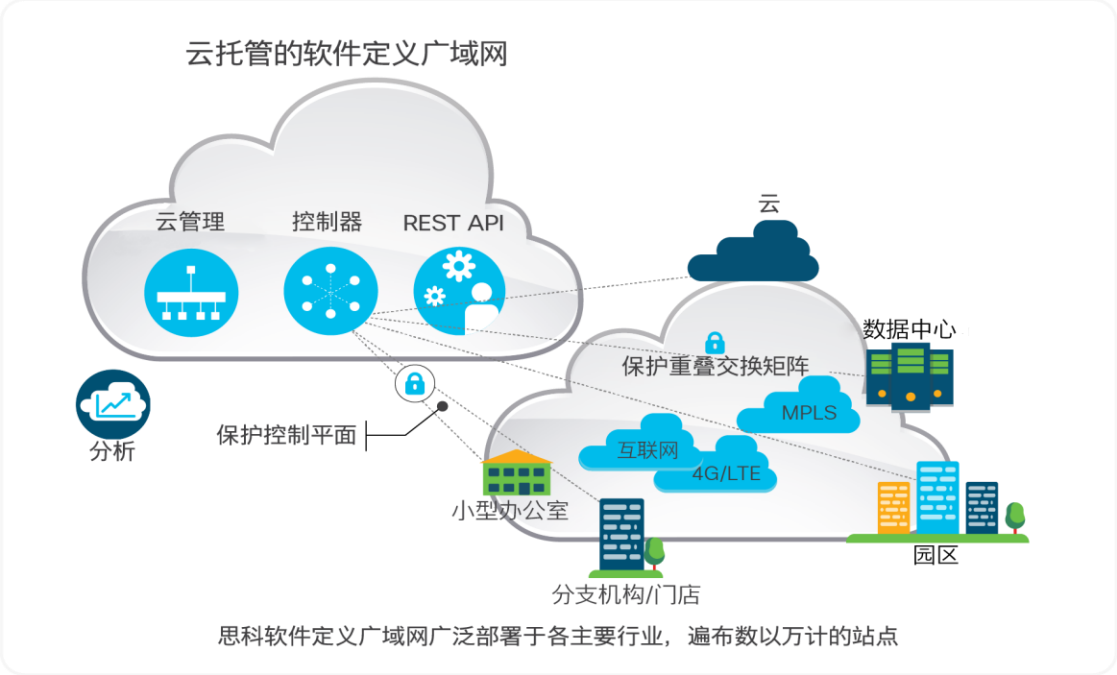
思科是领先的企业网络提供商，可为分支机构、园区和数据中心连接提供各种网络解决方案。思科软件定义广域网解决方案可以让 IT 能够轻松地部署基于云的新应用，同时保持高水平的安全性并优化用户体验。软件定义广域网是思科更广泛的基于意图的网络策略的组成部分，其中集成了安全和云解决方案。思科软件定义广域网提供了集中式云托管交换矩阵，可从分支机构到云实施一致的策略。

思科软件定义广域网安全功能包括：

- 具备应用感知访问控制、入侵防御和状态检测功能的企业防火墙
- 高级恶意软件防护、DNS 层实施和 URL 过滤
- 通过网络分段来隔离关键企业资产并加以保护

依托基于 TALOS 的威胁情报框架提供安全防护。图 3 显示了思科面向广域网的基于意图的网络架构

图 3. 思科软件定义广域网架构



面向企业用户的结论和建议

许多 IT 组织已经采用了多云架构，在这种架构中，无论应用的位置如何，都能在“最佳”平台上运行。

IT 组织必须能够管理私有云、IaaS 和 SaaS 平台组成的混合环境，以提供可靠的访问并实现出色的用户体验。由于广域网流量是在许多远程位置与互联网之间流动，组织必须对用户、分支机构、广域网、云和数据中心应用集成网络安全策略。

在多云环境中，软件定义广域网平台在提供对数据和应用的安全、可靠且低延迟的访问方面发挥着至关重要的作用。IT 组织需要能够转化广域网和云基础设施中业务策略意图。
软件定义广域网平台必须能够洞察应用类型和流量目的地，并能够相应地优先处理流量。从分支机构到云边缘必须应用统一的安全和策略管理。

组织需要灵活的广域网架构，并能够在分支机构、主机托管设施、其数据中心以及直接在云端运用网络和安全情报。软件定义广域网平台应能够实时衡量应用性能，并让 IT 管理员能够深入洞察补救应用速度缓慢问题的途径。高级防火墙、加密、高级威胁缓解和网络分段等网络安全功能应成为广域网解决方案不可或缺的组成部分。广域网和网络安全功能必须进行集中管理，并可以实现运营简便性。 思科软件定义广域网解决方案提供面向广域网的基于意图的网络，以及可利用最佳威胁情报的集成安全功能。

与作者面对面

Lee Doyle 是 Doyle Research 首席分析师，*他致力于为客户提供有关智能网络发展情况的相关分析，分析内容重点突出且富于针对性。他拥有超过 25 年的 IT、网络和电信市场分析经验。Lee 撰写了大量有关 SDN、NFV、企业采用网络技术和 IT 与电信融合等主题的文章。在创立 Doyle Research 之前，Lee 曾担任过 IDC 集团的网络、电信和安全研究副总裁。Lee 多次在《Network World》、《Fierce》和《Tech Target》等行业期刊上发表文章。Lee 拥有威廉姆斯学院经济学学士学位。*