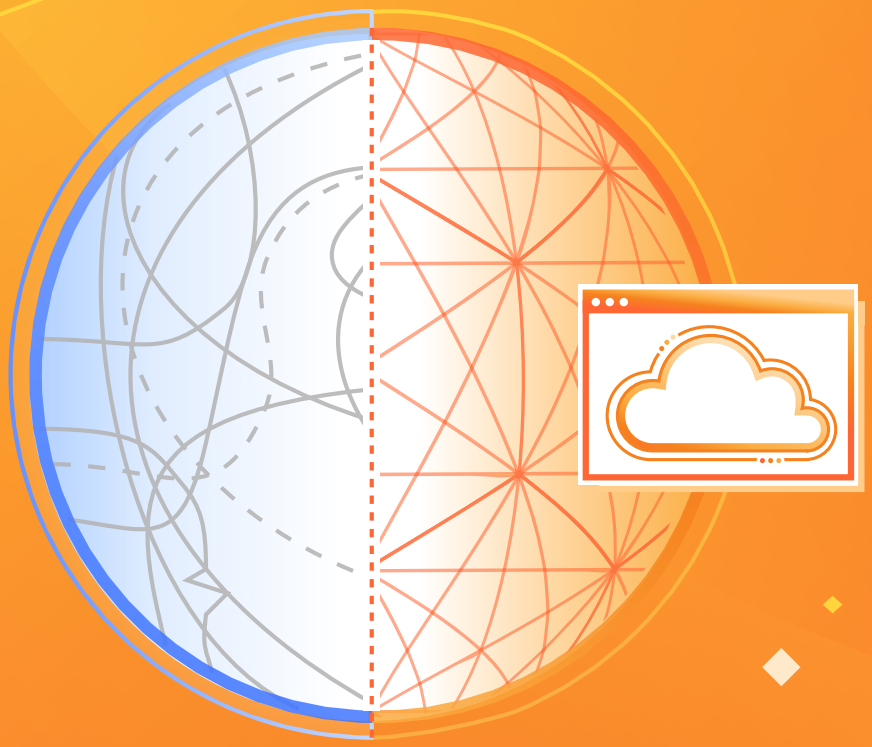
CLOUDFLARE

白皮书

制定网络现代化战略



目录

3 **传统网络: 数字现代化的障碍**

4 **了解网络现代化的过程**

5 **四个关键网络流量路径**

6 **Cloudflare 全球连通云**

7 **网络现代化的关键用例**

7 分支机构连接

8 保护您面向公众的基础设施

9 简化您的企业网络

9 从 DMZ 迁移

10 用 ZTNA 取代 VPN

10 消除 LAN 中的过度信任

10 加快并购中的网络连接

11 连接并保护您的云

12 **后续步骤**

传统网络：数字现代化的障碍

要在瞬息万变的商业环境中脱颖而出，敏捷性至关重要。但敏捷性不仅仅涉及领导力和决策，它还取决于组织执行变革的能力。必须以一种能够灵活适应而不崩溃的方式建立各种体系。企业必须能够重新调整以适应新的收入模式，支持新的应用程序，并连接处于世界各地的人员。

随着组织调整方式以获得竞争优势，敏捷性是数字现代化项目的主要期望结果之一。当考虑传统企业网络的状态时，这一点尤为重要，因为传统企业网络在提供通信和支持协作方面起着至关重要的作用。企业网络不愿进行变革，而且理由充分。它被设计为能够承受各种冲击，而变革需要付出巨大的成本和努力。

有时变化是可以预见的，因为它们是随着时间发生的，例如云对数据中心的影响。在网络方面，外部市场力量正在推动快速变化，有时甚至在一夜之间发生。例如，疫情给一些公司带来了痛苦的教训，让他们意识到迅速增加远程办公能力，保持员工生产力以及在无人的办公室闲置网络消耗预算的情况下管理成本是多么困难。

经历这些艰难境况的同时，显然一些公司不仅能适应变化， 还得以茁壮成长。这不仅仅是管理层能否做出正确的业务决策的问题，还涉及到企业转型和执行的能力。对于首席信息官 (CIO) 来说，有必要制定应对变化的策略，调整方式以支持未来需求，并让 IT 成为变革的催化剂而不是障碍。

鉴于对本地网络上的庞大投资，现代化并非一个简单的决定。要充分实现网络现代化的好处，有必要审视必须实现的目标，以确定必须改变的事物。

了解网络现代化的过程

当您考虑多年来网络设计的最佳实践时，存在如此多的复杂性是有充分理由的。几十年来，组织不断建设和加固网络，层层叠加新技术。随着每一代网络设计和每一项创新的出现，网络变得更加复杂。寻求简单性的机会并不存在，而且新技术的加入往往使速度、韧性和安全性进一步复杂化。

通过云交付的网络和安全服务，我们现在处于企业网络设计下一代变革的前沿。通过将云交付的服务作为网络的延伸，组织可以解决新的用例，扩展覆盖范围，并保护远离数据中心的应用程序。这代表着一个大幅简化网络的机会，因为服务交付基于现有网络到云服务提供商 PoP 的连接，无需断开连接以插入另一个设备。本地网络与云服务之间的连接保持不变，同时插入和使用云服务内部的服务。

问题在于，并非每个云交付网络和安全平台都是相同的，而且并非总是容易看出它们之间的区别。其中很多在网络现代化过程中的上升空间有限。为了理解这些差异，有必要规划您在网络现代化方面的目标，以避免用另一个复杂性来源取代一个。

四个关键网络流量路径

在评估网络现代化项目的范围时，请考虑您的网络涵盖了大量的接触点，其中一些交叉使用相同的基础设施（例如，流量通过核心网络进行入站、出站和东西向流动），而另一些则在其外部运行（例如您的公共云网络）。

入站流量：鉴于网络的一些部分暴露在互联网上，有必要维护入站防御，以防止瘫痪或利用业务的尝试，同时仍允许合法用户的流量通过。传统的边界防御可能会不堪重负，并需要处理分布式拒绝服务的能力。

出站流量：到互联网的连接和基于云的应用程序需要确保安全业务使用的策略，例如防止威胁和数据外泄。鉴于用户位置的多样性，组织已实施了各种出站保护技术，包括本地设备，例如防火墙（用户在网络上时）、DNS 解析器以及基于云的代理，例如 SWG 和 CASB（用户远程连接时）。

WAN 网络：WAN 及其涵盖的园区和分支机构等边界正在被重新设计，以支持云优先倡议和物联网设备。因此，传统的网络拓扑正在取消到数据中心的回传，改为直连互联网的架构。随着这些领域的网络技术快速发展，安全性的加入反过来变得更加复杂。在许多情况下，内部流量路径仍依赖于边缘部署的安全设备，阻碍了组织的转型进展。

公共云网络：随着组织在多个云上构建其应用程序，建立和维护基于点对点的网络和安全配置变得越来越困难。设置和管理网络需要消耗时间和资源——这些时间花在项目开发上更有意义。

这些流量路径都有多种技术，由组织在其网络中实施，或从使用云服务平台提供的技术。鉴于现代化项目涉及多个方向的流量路径，有必要规划全面的网络现代化实施过程，涵盖所有四个方向，以避免在架构上犯错误，导致限制可实现的转型效益，或需要多种不同的技术来解决未处理的用例。

入站流量

保护网络和应用以防互联网流量的影响。

公共云网络

提供网络服务 以在公共云和混合云中连接、保护和构建应用程序。

出站流量

保护用户和办公室 以防威胁并实施使用策略。控制应用程序中数据。

WAN 网络

连接和保护办公室、用户、设备、数据中心和 基础设施。

Cloudflare 全球连通云

考虑使用 Cloudflare 全球连通云进行您的网络现代化。它构建的理念是使用可组合、可编程的架构，为您的用户以及基于云的业务基础设施和应用提供网络和安全服务。因此，它同时满足您的现代化实施过程当前和未来的需求。

使用 Cloudflare，您可以通过启用服务而不是插入设备来添加功能并支持新的用例。与 Cloudflare Anycast 数据中心的连接保持不变，同时从统一管理界面配置和部署服务以处理流量。您可以满足当前需求，同时部署到位支持未来用例和整个网络现代化过程的平台。

使用我们的全球基础设施，无需自行建设。您的组织可受益于 Cloudflare 全球网络提供的超高速度。Cloudflare 网络与几乎每一家服务提供商和云提供商直连，可在 50 毫秒内触及 95% 的全球互联网用户。

网络现代化的关键用例

建议从能够为业务带来影响并对组织提供最大意义好处的用例开始。这些用例并没有特定的顺序，因为对您的业务而言，优先事项是独一无二的。重要的是在解决近期需求的同时，构建一个能够支持您的网络现代化过程的架构，无论您选择那种方式。

	现代化项目
分支机构连接 降低成本，改善用户体验	• 从 MPLS 过渡到全球连通云 • 从 SD-WAN 过渡到全球连通云
保护面向公众的基础设施 延长防火墙和 DMZ 投资的寿命	• 减少网络防火墙的负载 • 将 DMZ 安全性转移到全球连通云
简化您的企业网络 实施 Zero Trust 以获得更好的安全性并降低资本支出	• 减少/消除 DMZ • 用 ZTNA 取代 VPN • 消除 LAN 中的过度信任 • 加快并购过程中的网络连接
连接并保护您的云 在您的应用程序中充分利用每个云的优势	• 构建并保护应用 • 利用开发人员服务来集中核心功能

分支机构连接

WAN 网络的一个重要组成部分是连接较小的站点，例如分支机构和门店，以便将用户和设备连接到应用程序。传统的轮辐式架构通过昂贵的 MPLS 电路将站点连接到数据中心，但随着支持云应用程序的需求增长，越来越多组织正在使用通过宽带直连互联网的架构。

SD-WAN 旨在使网络连接更可靠，但与安全功能插入之间的关系并不完美。大多数 SD-WAN 架构依赖于大量边缘设备和本地防火墙来在 SD-WAN 网络上执行安全策略，仅对出站流量使用 SSE/SASE 集成。

使用 Cloudflare 的全球连通云来实现分支连接，支持您的完整迁移路径，无论是增强还是替换传统服务。Cloudflare 采用基于“轻边缘/重云端”理念的架构来提供网络和安全服务。利用 Cloudflare Magic WAN 便利网络位置之间的站点到站点连接，包括分支机构、零售门店或工厂车间。它为您的整个企业网络提供安全、高性能的连接和路由，降低成本和运营复杂性。为了安全起见，Cloudflare Magic Firewall 与 Magic WAN 一起无缝部署，使您能够在流量通过 Cloudflare 网络时执行网络控制策略，无论是南北向还是东西向。

保护您面向公众的基础设施

企业网络和 DMZ 可访问并暴露在互联网上，需要采取措施以防攻击者造成破坏。在理想的情况下，传统网络防火墙可以检查并丢弃所有不需要的流量，但每个防火墙的容量都是有限的（可用带宽、利用率/计算、会话计数等）。对于攻击者来说，成功只是一个规模的问题，也就是说，攻击者能够产生足够多的噪音来瘫痪公司在不同网络协议层上运行的能力。

这不仅仅是流量体量的问题。接受入站流量会将攻击面暴露给未经身份验证/预身份验证的流量。应用程序和操作系统中的漏洞可被攻击者利用，即使该攻击者在系统上没有账户。凭据填充——即利用来自其他数据泄露的已知用户名/密码进行登录——也是一种主要的风险来源。通过将 Zero Trust 原则应用于 DMZ 中的应用程序，组织可以减少在互联网上的暴露风险，并在可能的情况下予以消除。

通过应用纵深防御原则，吸收组织面向公众的基础设施上游的恶意流量，组织可改善其网络保护。Cloudflare Magic Transit 内置 Magic Firewall，通过 Cloudflare Anycast 网络部署，可充当组织的前门，过滤掉恶意和不必要的流量，仅允许干净的入站流量。

当网络防火墙在设备上执行 DDoS 缓解时，仍然需要处理连接后才能将其丢弃。使用 Cloudflare 时，我们的网络广播客户的前缀，从而吸引本应前往边界防火墙的流量。借助 Anycast，我们通过在所有数据中心分配负载来有效吸收 DDoS 攻击流量。僵尸网络的成员看到最近的 Anycast PoP，后者根据 Magic Transit 和 Magic Firewall 策略处理流量。

简化您的企业网络

简化带来了许多现代化的好处。如果架构设计中更少脆弱的组件，IT 团队可以使网络更可靠，并通过采取 Zero Trust 默认拒绝所有访问的方法增加网络安全性。

要简化网络，请考虑：

从 DMZ 迁移

网络 DMS 是运营中让人头疼的问题，因为它们对零日漏洞利用特别敏感。攻击者不需要内部网络访问就能与 DMZ 中的服务器通信，因此组织必须保持警惕，以防止利用和滥用。

然而，尽管 DMZ 在过去发挥了重要作用，但今天还需要它们吗？DMZ 作为一种网络结构的重要性正在降低，因为有构建和托管应用程序的替代方法。

- 对于面向公众的应用程序，将工作负载迁移到公共云上具有经济和技术上的效益。
- 通过 SaaS，多种面向公众和私有应用程序完全不需要在客户管理的基础设施上运行。

因此，从安全和网络设计的角度来看，开始考虑如何减少或消除对 DMZ 的需求是务实之举。这不仅在运营角度具有意义，通过消除支持它的网络基础设施，如防火墙、WAF 和负载平衡器，还能大幅简化架构。

如果私有应用程序放置在 DMZ 中以扩展对员工、合作伙伴和承包商的访问，这种情况应该如何处理呢？将它们隔离在专用网络中，并使用 Zero Trust 网络访问 (ZTNA) 向员工和合作伙伴提供访问会更安全。

使用 ZTNA，您可以通过消除到应用程序的入站网络流量来有效减少攻击面。ZTNA 通过 Cloudflare 全球连通云使用基于上下文和代理的方式访问资源，从而免除了在网络防火墙中开放端口的需要，同时为安全团队提供了谁可以访问什么资源的完全可见性。

用 ZTNA 取代 VPN

使用 VPN 访问应用程序的日子正在逐渐减少。从网络设计的角度来看，让用户通过长长的隧道访问互联网和云是不切实际的。通过 VPN 允许用户（以及可能遭到入侵的设备）进入网络也造成重大安全风险。

应用程序访问 也不是 VPN 的唯一功能。在某些情况下，组织需要与端点建立更广泛的网络连接，例如端点管理和服务器发起的通信。这些用例传统上利用了 VPN 在两个方向上的网络连接，并难倒了市场上早期的 ZTNA 产品。在替代品的情况下，组织同时运行 ZTNA 和 VPN。

要实现网络基础设施现代化，组织可以使用 Cloudflare 的 ZTNA 整合这些功能。这是因为，使用 Cloudflare，组织既能支持经典 ZTNA 用例，也能支持服务器发起的流量和双向流量。这些功能帮助组织通过消除 VPN 来简化其应用程序访问需求，并进一步提高安全性和简易性。

消除 LAN 中的过度信任

随着混合办公模式的出现，在办公室和其他地方办公之间的差异越来越少。事实上，当用户经常在咖啡店和共享工作空间等不受信任的公共网络上工作时，情况更是如此。

在某种程度上，开放的公共网络体现了 Zero Trust 的理念——没有人拥有访问特权，任何人或物都是不可信的。如果在共享的工作空间、家庭办公室和咖啡店中可行，为什么不能也在企业网络中消除信任呢？

消除信任并不需要更高级的网络设计，而是进行简化。相比为经过身份验证的用户提升访问权限并使用网络策略开放到资源的连接，更安全的做法是假定整个网络都是不可信的。基于 SASE 实现的安全性，组织可以访问所需的应用程序，并通过适当的安全设置保障其安全，而不需要对网络本身进行任何信任假设。Zero Trust 不是在网络中添加信任，而是将其消除，直到达到更好、更安全的状态，无需过去那种明确和过度的许可。

加快并购活动的连接

组织将并购作为一种工具，以获取无法以其他方式立即获得的商业资源和能力。为了利用此类机会，组织必须迅速执行，使合并后的公司胜于各部分的总和。然而，IT 通常无法快速行动，因为两个组织的应用程序和基础网络基础设施极少能够轻松地结合在一起。

为了加快并购的连接，组织可以将对应用程序的访问视为独立于网络集成的任务。设计一个融合网络架构的时间表可能延伸数年，但应用程序访问不必依赖于如此遥远的里程碑。

这是因为合并第一天的情况实际上是一个 Zero Trust 用例，即在不受信任的网络上的受信任用户仍然需要访问应用程序。使用 Cloudflare One 扩展访问，提供了在不依赖融合网络访问的情况下为并购提供连接的方式。

连接并保护您的云

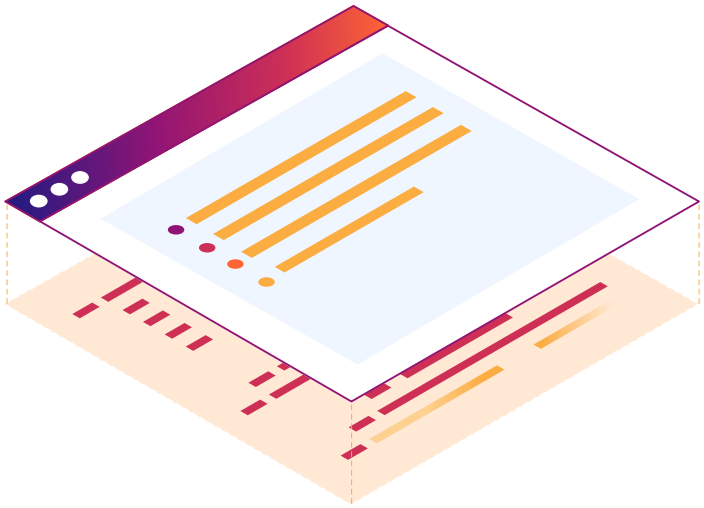
随着云开发演进，一个云中的组件将有利于在另一个云中被重新利用。正如随着时间的推移，每个组织都会变成多云架构一样，每个组织随着时间的推移也将需要管理公共云网络连接。应用程序开发往往具有部落性质，组织不同部分的 DevOps 更倾向于使用他们最熟悉的工具。然而，发展组织能力以管理跨云的连接是复杂的，因为这项工作牵涉在完全不同的框架上构建的工具集。

多云复杂性的另一个方面是混合云领域。混合云将本地私有云与虚拟私有云结合在一起。这些网络有时是使用专用网络构建的，比如 AWS Direct Connect，这种方式成本高昂且仅限于一个云。随着组织构建多云应用程序，他们并不一定希望承担每个云的专用网络成本。

与其构建从一个应用程序直接到另一个应用程序的网络和安全性，更好的做法是使用 Cloudflare 来编排和连接公共云网络服务。我们认为 Cloudflare 的全球连通云在这种架构中发挥着理想的作用，作为一个中转站，通过庞大的 Cloudflare 网络传递各云之间的流量。通过增加公共云网络管理能力，现在客户也可以通过 Cloudflare 来编排工作负载连接的设置。

我们的公共云网络不仅仅局限于对底层基础设施的编排。我们的架构更进一步，提供开发人员服务，用于构建和与多云应用程序集成。本开发人员平台为您提供一个丰富的、基于开源和开放标准构建的基础技术生态系统。您既可以选择使用开发人员平台的所有元素，也可以只使用所选择的元素，而不受限于特定云中的特定服务。

后续步骤



要在网络现代化旅程迈出下一步，欢迎联系 Cloudflare，让我们帮助您制定战略。我们与成千上万的客户密切合作，帮助他们将架构过渡到 Cloudflare 全球连通云。

欲了解更多信息，
请访问 http://www.cloudflare.com/zh-cn/

© 2024 Cloudflare, Inc.保留所有权利。
Cloudflare 徽标是 Cloudflare 的商标。所有其他公司和
产品名称分别是与其关联的各自公司的商标。

010 8524 1783 | enterprise@cloudflare.com | cloudflare.com/zh-cn

REV:BDES-5483.2024JAN30