白皮书

超越 SD-WAN：Zero Trust 安全性和互联网即企业 WAN

为什么 SD-WAN、安全访问和威胁保护应彼此关联

Akamai

企业广域网的未来

广域网 (WAN) 早在 20 世纪 60 年代就已出现，彼时，计算机间通信才刚刚问世。随着技术的发展和流量需求的增加，它们将继续得到开发和增强。对于当今的企业来说，WWAN 是允许跨多个位置建立统一网络的基础设施。

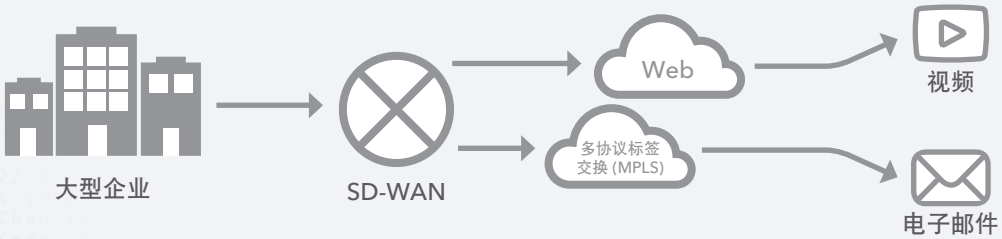
但是，这种关键的底层结构并非没有限制。WAN 通常提供较低或不足的带宽，导致特定应用程序的性能出现问题，发生可靠性波动，并可能给您的业务带来安全风险。此外，除了公共互联网之外，WAN 通常在租用线路上构建，或者从服务提供商处租用，而提供商的基础设施使用电路交换或数据包交换方法，例如异步传输模式 (ATM) 和多协议标签交换 (MPLS)。虽然后者的成本较低，但它目前仍然非常昂贵，并且不具备可扩展性。

企业网络正在转型

为了应对这些性能、安全性和资金方面的挑战，企业正在采用软件定义的 WAN (SD-WAN)，同时降低成本并实现敏捷性。

以软件定义的网络 (SDN) 和网络功能虚拟化 (NFV) 的创新（最初用于数据中心）为基础，IT 部门迅速为互联公司的网络采用了该技术。

简单地说，SD-WAN 会隔离广域网的数据和控制平面。SD-WAN 会监控 WAN 数据连接组合 (MPLS、ATM 和互联网) 的性能，并根据当前链路性能、连接成本和应用程序或服务的需求为每种流量类型选择最合适的连接。



SD-WAN 演示

SD-WAN 可能会通过 MPLS 路由电子邮件，因为延迟不是主要的问题，且每比特发送成本最低。相反，SD-WAN 可能会通过互联网路由视频会议流量，以确保最佳性能和最小延迟，但每比特发送成本更高。

互联网是否可以成为新的企业 WAN?

如果 SD-WAN 采用包括公共互联网在内的多种传输服务，则肯定能够变得灵活、高效且具有经济效益。但是，由于此类传输方案无法保证性能或不具备 SLA，因此 SD-WAN 仅将互联网用于非性能关键型应用程序。

要增加互联网的使用，从而以高效、经济实惠且安全的方式交付更多企业 WAN 流量，并且使用的方法可以与当前 SD-WAN 部署共存，您必须采用一种可以消除互联网潜在限制的策略。其中一种方法是使用边缘平台，通过互联网交付安全、快速和可靠的业务应用程序，而不在互联网上公开这些应用程序。此方法使您可以最大程度地利用当前 SD-WAN 投资，同时在向互联网传输更多流量时进一步降低成本。

鉴于现代企业网络的发展轨迹，将更多的企业流量路由到互联网是一种有意义的做法。随着云工作负载的增加，以及多样化的移动用户和设备，意味着工作流程已经严重依赖互联网。此趋势将继续普及。

如果您可以更进一步，通过互联网建立安全、可扩展且高效的企业 WAN，情况会怎样?

在本文中，我们将讨论使用 SD-WAN 和 Zero Trust 安全性转型网络的过程，以及如何定位您的公司，使其发展到超越 SD-WAN 的范畴，从而采用完全基于互联网的企业网络。

边缘平台使您可以通过互联网交付安全、快速和可靠的业务应用程序，而不在互联网上公开这些应用程序。

> *到 2023 年年底，超过 90% 的 WAN 边缘基础设施更新计划将基于虚拟化客户场所设备 (vCPE) 平台或软件定义的 WAN (SD-WAN) 软件/设备，而不是传统路由器（目前不到 40%）。”*
>
> *- Gartner，WAN 边缘基础设施魔力象限，2018 年 10 月*

SD-WAN 的价值

SD-WAN 主要提供链路平衡、自动设备配置和第三方安全服务插入。这些功能的价值包括改进用户体验、降低链路成本以及降低运营支出，会产生重大影响。SD-WAN 的优点十分明确，也获得了良好的支持。

数十家供应商提供了不同的 SD-WAN 功能，但它们可以广泛分为三类：

1. *灵活链路控制*
2. *可管理性*
3. *服务插入*

灵活链路控制

第一个功能是灵活链路控制，这是 SD-WAN 的主要优势。由于云是许多公司的主要目标，因此，通过专用网络将流量回传到数据中心（实际上充当集中控制点）的做法并不可行。SD-WAN 通过使用智能流量控制（包括动态路由选择）解决了这一难题。此外，SD-WAN 还建立了本地或分支互联网分汇（也称为直接互联网访问 (DIA)），它将流量路由到云，而不是通过数据中心。因此，包括语音和视频在内的所有传统应用程序都被指定为使用 MPLS 链路，而云应用程序和互联网流量则直接进入互联网。

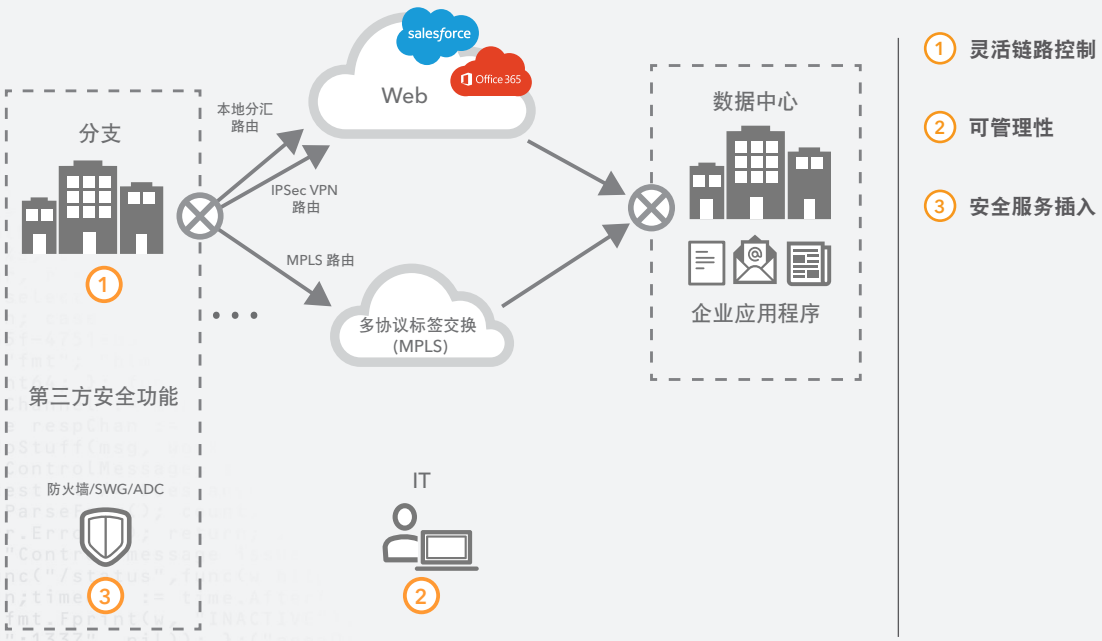
可管理性

SD-WAN 供应商还可以提供可管理性，从而简化网络设备的操作和管理。自 20 世纪 90 年代以来，企业 WAN 由多层交换机和路由器等网络设备组成。这些设备在很大程度上采用了逐个设备进行管理的策略。换而言之，管理员必须分别配置和维护数百到数千台设备，监控整个公司中每个设备的软件堆栈。即使设备可使用路由协议动态交换路由信息或建立高可用性，用户也需要进行大量操作。借助 SD-WAN，所有设备管理都可以在单个集中式控制台中完成。

服务插入

最后，一些 SD-WAN 提供商专门从事服务插入业务。WAN 的最低要求是公司中的 IP 可访问性，即第 3 层网络连接。但是，随着网络的发展，安全功能也在不断发展：防火墙、入侵保护系统 (IPS) 和应用程序交付控制器，等等。过去，您需要复杂的路由设计来将这些功能添加到网络，因为提供这些服务的设备通常无法与动态路由协议（优先打开最短路径 [OSPF]、边界网关协议 [BGP]）通信，从而导致出现了由静态路由和再分发组成的复杂组合。SD-WAN 使这些技术（通常通过第三方提供）变得易于配置，并且易于通过统一门户进行管理。

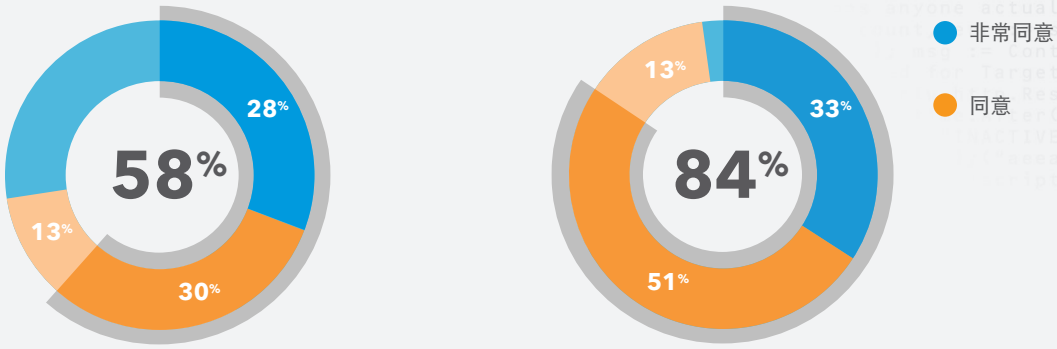
SD-WAN 的商业价值



新模型：Zero Trust 安全性

新的架构需要新的安全性。随着事务转移到云和互联网，网络已变得高度分散，从而形成了更多的攻击面。应用程序、用户、数据和设备已移出传统的控制区域，从而瓦解了曾经值得信赖的企业防御层。因此，构建和实施依赖于企业防御层的安全模型已不再可行。现代防御战略必须解决当今分布式工作负载和员工队伍带来的问题。

您在多大程度上同意/不同意？



“在如今由分布式云网络和移动/远程用户组成的技术生态系统中，网络防御层无法提供足够的保护。”

“数字转型需要调整传统（基于防御层）的安全策略。”

Forrester Research，通过微分段构建 Zero Trust 安全战略，2018 年 9 月

Zero Trust 安全模型假定不存在所谓的“内部”，并且每个用户和设备都同样不值得信任。每个访问请求都需要进行身份验证和授权。应用程序和数据仅在验证后交付 - 即使经过验证，这种交付也是瞬态的，且范围有限。此安全框架将所有应用程序视为面向互联网，并认为网络受到攻击且充满风险。此外，可见性至关重要；必须具备完整的日志记录和行为分析。

Zero Trust 安全性的核心原则包括：

- *确保安全地访问所有资源（无论其位于何处或采用何种托管模型）*
- *在实施应用程序访问时采用“最低权限”和“默认拒绝”策略*
- *检查和记录流量（针对您控制的应用程序和不受您控制的应用程序）以识别恶意活动*

支持实施 Zero Trust 安全性的主要组件有两个：

- *用于实现安全应用程序访问的身份感知代理*
- *用于保护用户的安全互联网网关*

用于实现安全应用程序访问的身份感知代理

如果用户、数据和应用程序位于云端，并且 SD-WAN 启用的 DIA 提供连接，为什么不将安全性和 DMZ 堆栈也转移到云端呢？这样一来，您可以利用 Zero Trust 来确保安全访问您控制的应用程序，同时缓解访问不受您控制的应用程序的用户所带来的风险。

如果您当前选择使用简单的 VPN 设置来提供企业应用程序访问，您可能会允许登录的用户对您的整个网络具有 IP 级别的访问权限。但这种做法存在很大的风险，而且违反了 Zero Trust 安全性的原则。为什么呼叫中心员工对源代码存储库具有访问权限？为什么使用您的账单系统的合同商对信用卡处理终端具有权限？应当仅允许他们访问履行角色职责所需的应用程序。传统 VPN 不允许这种精细访问控制，而是需要继续依赖中央辐射式网络模型。

身份感知代理 (IAP) 架构通过基于云的代理提供应用程序的访问权限。身份和授权发生在边缘，并且基于“须知”最低权限原则，此原则与通过软件定义的防御层 (SDP) 进行访问类似，但在应用程序层（第 7 层）使用标准 HTTPS 协议。

IAP 的两种工作方式

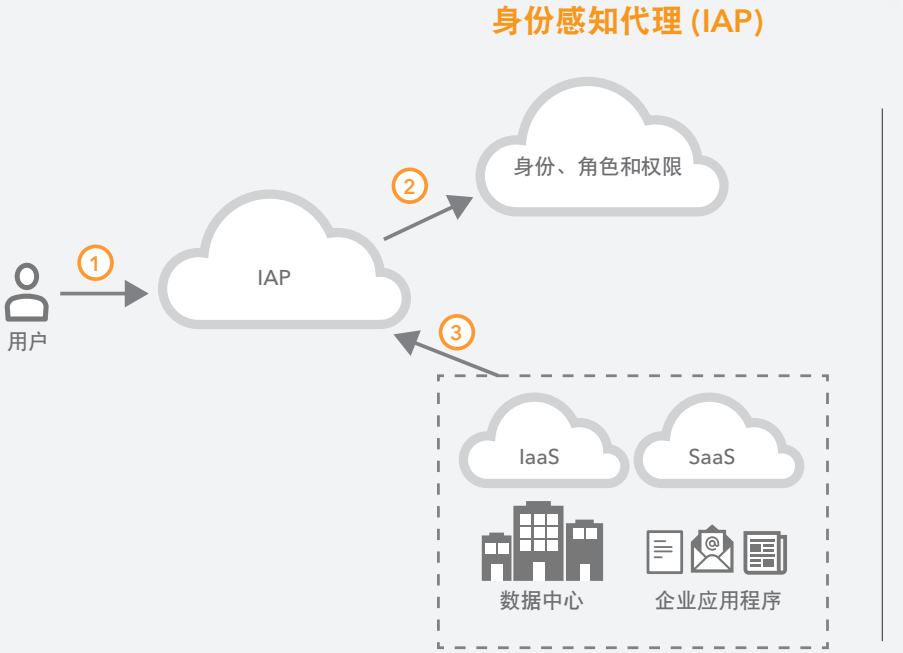
您可以将 CDN 集成到各个国家/地区的事务中，以改善应用程序响应

或

您使用 Web Application Firewall (WAF) 来保护企业 Web 服务器抵御常见漏洞，例如 SQL 注入和跨站点脚本

IAP 的关键组件是身份来源，该来源用于验证用户和设备信任（身份验证）以及允许他们访问的内容（授权）。此身份来源可能基于公司目录或基于云的身份提供商。即使在验证用户身份之前，通过检查设备的状态，也可以确保尝试获取访问权限的设备符合某些安全标准，例如，拥有证书、运行最新操作系统、受密码保护或安装并运行了适当的端点检测和响应解决方案。

IAP 与其他访问技术相比，具有一个显著优势：用户不仅要经过验证，并且还会检查用户的流量，并且可以终止、检查和授权各个应用程序请求。在代理上端接事务后，可以集成其他服务，从而改善用户体验和应用程序保护。



IAP 还依赖于应用程序级别的访问控制，而不是防火墙规则；配置的策略可以反映用户和应用程序的意图，而不仅仅是端口和 IP。与 SDP 类似，该方法可以隔离云中或防火墙后的应用程序和其他资产，并且对于 Web 应用程序来说，它没有客户端。

随着云采用规模的扩大，迁移企业应用程序的挑战也越来越受到关注。许多公司都难以将云用于云原生和传统应用程序。IAP 不仅可用于验证原生 SaaS 应用程序的用户，还基本上可用于将数据中心中的传统应用程序实现 SaaS 化。此外，代理可促进云迁移和应用程序现代化，而无需采用完全淘汰和更换策略。因此，企业可以采取有条不紊的逐步方法来实施 Zero Trust，同时减少与基于防御层的传统控制和传统 VPN 相关的技术遗留问题。

用于保护用户的安全互联网网关

过渡到 Zero Trust 安全模型的一个关键优势是确保用户在访问您无法控制的应用程序时保持安全。互联网上的每次单击都潜藏着大量网络威胁。过去用户与企业网络和托管设备绑定，防止恶意软件、勒索软件和网络钓鱼的过程十分简单：实施端点防病毒软件、在数据中心安装设备堆栈以及回传流量进行检查和控制。

由于用户分布在多个地点，互联网成为了企业的首选网络；基于云的 SIG 为您提供了安全的入口。无论用户身在何处，都能主动保护用户。

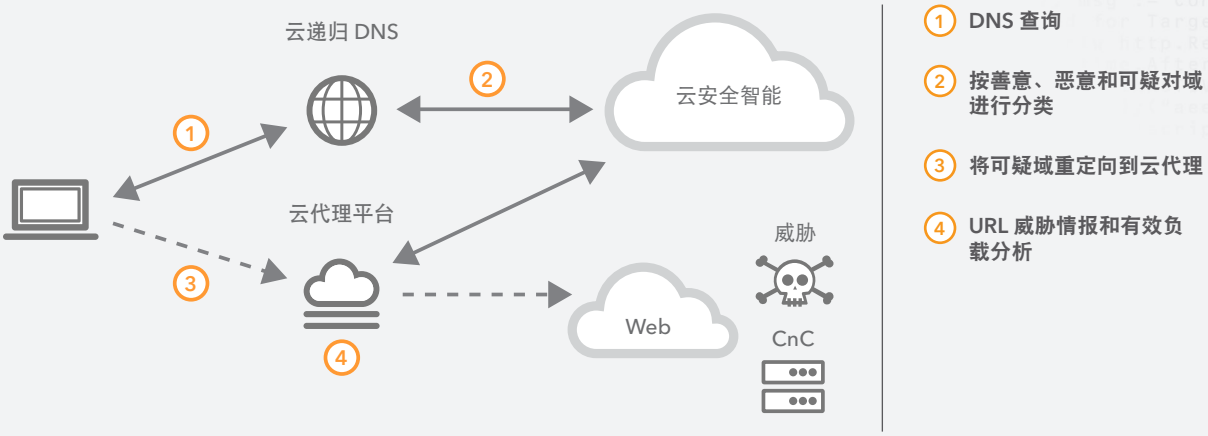
但是，用户现在离开了大楼，设备不受管理，并且互联网正成为企业的首选网络。DIA 连接使中央控制和检查安全解决方案变得过时。另一种方法是在每个互联网分汇处复制安全设备堆栈。但是，对于大多数企业而言，这是不切实际的，既有逻辑方面的因素，也有财务方面的因素。更重要的是，这种方法的固有复杂性可能会带来安全缺陷，其架构直接站到了 Zero Trust 最佳做法的对立面。

要保护 DIA 流量，一种更简单、更快速和更具成本效益的方法是使用基于云的安全互联网网关 (SIG)。SIG 是一个安全的互联网入口通道，它可代理风险流量进行控制和检查，从而主动保护用户（无论他们身在何处），抵御高级威胁。其采用的方法是：检查每个 DNS 请求，阻止对恶意域的请求，允许正常进行对安全域的请求，以及把对风险域的请求转发到云代理进行进一步检查。

在最后一个阶段，当代理收到 HTTPS 请求时，它会将请求的 URL 与基于云的威胁情报知识库进行比较，并阻止恶意 URL。对于归类为风险的所有其他请求 URL，代理将通过多个恶意软件分析引擎发送 Web 内容以进行内嵌有效负载分析。这些引擎使用一系列检测技术（签名、无签名和机器学习），来识别和阻止已知威胁以及以前未知的零日威胁。通过使用多种检测方法，您可以根据内容类型将有效负载定向到最合适的引擎（或多个引擎），从而确保最佳检测率并提供低误报率。

请务必注意，此方法与安全 Web 网关 (SWG) 等传统安全设备采用的方法截然不同。具体而言，SWG 会代理所有互联网流量，同时检查良好和不良流量，这对复杂的网页和较重的 HTTPS 内容尤其不利。这种方法会降低性能，导致延迟，并增加因代理所有流量而导致损坏的网站和应用程序数量。SWG 通常会导致更多的安全事件和误报，从而增加帮助台请求并独占 IT 资源。

安全互联网网关架构



1. **DNS 查询**
2. **按善意、恶意和可疑对域进行分类**
3. **将可疑域重定向到云代理**
4. **URL 威胁情报和有效负载分析**

智能选择性代理可以利用 DNS 作为通往互联网的入口和第一个安全层。此方法将允许安全的流量直接进入互联网，阻止不良流量，并仅代理风险流量，从而实现以下目的：

- *简化安全防护*
- *降低延迟、提升性能*
- *减少网页和应用程序瘫痪问题*

网络转型风险更低：在 SD-WAN 环境中实施 Zero Trust

许多正在迁移到基于互联网的架构的公司认为，SD-WAN 是关键的推动因素，因为其具有链路控制功能，并且可能会降低购置 MPLS 所带来的财务负担。他们可以使用宽带或无线网络来增强或补充 MPLS 连接，从而创建混合 WAN。但是，如果他们已经采用 DIA，那么，采用具有相同策略的安全模型肯定是有意义的。

由于采用了 SD-WAN，公司必须将其安全性从基于防御层的框架演变为位于边缘的、基于 Zero Trust 的框架。那么，我们如今处于什么阶段？接下来会发生什么？

使用 SD-WAN 的网络通常处于三种情况中的一种，具体取决于企业的思维模式和长期战略：

1. *具有集中分汇的传统专用 WAN；即，正在考虑，但尚未实施 SD-WAN*
2. *混合实施：将传统的专用 WAN 应用于现有站点，将 SD-WAN 应用于较新的分支机构*
3. *主要采用 SD-WAN*

Zero Trust 安全方法可以很好地适应所有这些场景。但是，如果企业已在考虑或已在实施 SD-WAN，则它可能已经将互联网用作一个可行的业务网络工具，因此准备将 Zero Trust 安全策略用于其企业网络环境。

我们来看看现有架构，以确定每种架构如何实施 Zero Trust，然后迁移到所需的未来状态。

具有集中分汇的传统专用 WAN

如果 SD-WAN 迁移的动机是成本、敏捷性和灵活性，即基于互联网的网络架构所能提供的优势，则建议完全跳过 SD-WAN 并直接迁移至 Zero Trust 框架。IAP 支持对应用程序进行基于 Zero Trust 的访问（无论其位于何处），而 SIG 为用户提供安全的互联网访问 - 公司无需在每个互联网分汇处构建安全堆栈。

要记住一点：如果企业已经通过互联网云服务提供商支持 VoIP 和视频会议等实时服务，那么，建议它完全采用基于互联网的网络和访问架构。如果这些服务仍主要在本地托管，则可能会在各位置之间保留一定程度的“专用”网络 - 专用（例如，基于 MPLS）或基于 SD-WAN。

具有传统 WAN 和 SD-WAN 的混合环境

在这种情况下，公司已经向着更高效、基于互联网的架构迈出了第一步。

在这些环境中，必须了解如何处理用户流量：

- *用户是否可以从远程办事处直接访问互联网，或者互联网链路是否仅用于联网返回核心站点？*
- *主要的用户应用程序位于何处？本地、数据中心或云中？*
- *如果使用云，用户如何连接到这些应用程序？是通过 DIA 从分支机构促成连接，还是回传至直接连接链路？*
- *SaaS 应用程序的使用有多广泛？*
- *对于分支机构级别的 DIA，每个位置的安全堆栈的全面程度是怎样的？*

答案自然取决于对于用户流量的处理，因此网络迁移的复杂程度也各有不同。但存在两个不变的因素：互联网使用量将会增加，并且需要从基于防御层的安全性过渡到 Zero Trust 模型。

例如，假设存在来自远程办事处的某些 DIA 连接。SIG 可以为集中式安全堆栈提供额外保护，并取代某些堆栈，从而降低复杂性和成本。

如果用户访问基于云的应用程序，则基于 IAP 的方法既可以加强公司的安全状况，又可以改善用户体验。它还可以借助 CDN，允许通过互联网直接访问应用程序，从而提高应用程序性能。

您可以继续从传统 WAN 迁移到 SD-WAN 环境，方法是为远程办事处启用 DIA 并采用 Zero Trust 安全原则。

主要采用 SD-WAN

在这种情况下，公司可能已摆脱了传统的专用 WAN 网络，改为使用站点间的互联网链路智能路由进行

您目前关于使用软件定义的 (SD-WAN) 网络技术的业务计划怎样的?

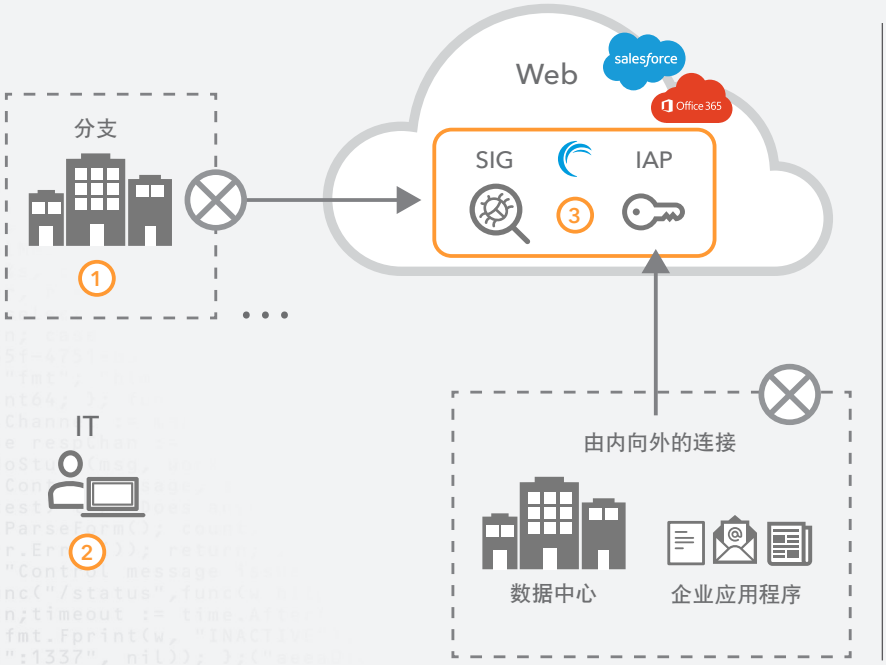
Forrester Research，数字转型将分布式商店网络推向转折点，2018 年 4 月

办事处间的通信，从而充分利用了 DIA 的优势。这些企业已经在大多数站点中依赖于互联网访问，因此，将网络发展到超越 SD-WAN 的范畴成为了一个合乎逻辑的发展方向。

下一步？通过将应用程序迁移到互联网来提高敏捷性和成本效益，从而开始减少对 MPLS 链路的依赖。即使在 DIA 环境中，也可通过 IAP 访问企业应用程序。如果应用程序已处于云环境中，则在中央位置进行分汇（例如，使用直接连接类型拓扑）之前，通过将流量回传到数据中心来访问应用程序是一种无意义的做法。

最后，此环境非常适合未来的状态，即纯粹基于互联网的连接和访问。所有企业应用程序都可以通过 IAP 访问，无论它们是位于本地，还是基于云。所有用户流量均可通过 SIG 进行保护。而且，如果基于互联网的提供商提供实时通信（比如语音和视频），最终可能完全消除 SD-WAN 乃至企业 WAN。这可以降低成本和复杂性，并通过 Zero Trust 架构模型增强安全性。

采用 Zero Trust 安全模型、基于互联网的架构的价值



1 简单的网络访问

- 仅互联网访问
- 无由外向内的访问

2 可管理性

- 单点管理
- 设备监控
- 用户监控

3 进一步的安全控制

- 零日攻击预防
- 集中式 AAA（身份验证、授权和计费）
- 客户端状况检查
- 网络钓鱼、恶意软件和 CnC 预防

实现业务转型

现代业务现状使企业更多地面临环境中的风险和复杂性。由专用 WAN 上的中心辐射式事务管理的网络模型与基于防御层的企业防御一样过时；网络和安全架构都必须做出演变。虽然 SD-WAN 目前使公司网络能够高效地处理流量并将工作负载移至云端，但此网络模型必须继续迭代。互联网在不久的将来会成为企业 WAN。

Akamai 相信，将 SD-WAN 与适当的、符合 Zero Trust 的安全和访问服务相结合，是过渡到“互联网即企业网络”的第一步。将 SD-WAN 与 Akamai Intelligent Edge Platform 相结合，您可以普遍应用访问和安全策略，并确保通过互联网实现快速可靠的最终用户应用程序体验。

Akamai 可帮助指导您演变您的网络和安全性。请联系您的客户团队，了解有关 Akamai Zero Trust 评估的更多信息。您将从我们的安全专家那里获得切实的建议，了解从何处着手或如何推进 Zero Trust 转型。或者，请访问《*立即开始实施 Zero Trust 安全性的 3 种简单方法*》以获得资源，帮助您开始转型。