

通过 Aruba EdgeConnect SD-Branch  
一体化下一代 SD-LAN 和 SD-WAN

[2024-01]

## 介绍

到 2026 年，预计将有超过 60% 的企业采用软件定义的广域网络 (SD-WAN)，而 2020 年这一数字仅为 20%，这一数字已实现飞跃？在这个网络技术快速发展的时代，SD-WAN 带来的变革不仅仅是一种趋势，而是企业网络的根本性转变。与传统的 WAN 架构不同，SD-WAN 提供无与伦比的灵活性、可扩展性和对网络资源的控制。

但是什么推动了这一重大变化呢？答案在于当今数字环境日益复杂的需求。考虑一家在多个大洲设有分支机构的全球企业。过去，在如此广阔的范围内管理网络流量并确保安全是一项复杂的任务，通常会导致效率低下和漏洞。SD-WAN 凭借其智能路径控制和集中管理，彻底改变了这一场景。它无缝集成云计算、移动连接和分布式劳动力，创建的网络不仅强大、安全，而且灵活且能够适应不断变化的业务需求。

然而，随着软件定义局域网 (SD-LAN) 的兴起，企业网络格局正在超越 WAN，代表了一种先进的局域网管理方法。这一成果提供了对 LAN 内的接入点 (AP)、交换机和网关的自动化和集中控制。它有助于跨 LAN 进行自动用户角色分配，确保高效、安全的网络访问，并协调从 AP 和交换机到网关的隧道创建。这样做可以简化网络连接并增强整体网络安全性。这种转变反映了市场的发展轨迹，但也暴露了一个重大挑战：潜在用户对 SD-LAN 在集成网络环境中的重要作用和优势的认知和理解上存在差距。

造成这种误解的一个因素是一些 SD-WAN 供应商对 SD-LAN 的描述方式。SD-LAN 不仅仅是在 LAN 策略中包含访问控制列表 (ACL)。它可以成为统一 overlay 结构的强大框架。在 EdgeConnect SD-Branch 解决方案具有无缝 SD-WAN 和 SD-LAN 集成的背景下，解决这一差异至关重要。通常，SD-LAN 的优势（例如增强的本地网络控制和更高的安全性）被对网络解决方案的更广泛关注所掩盖。在接下来的部分中，我们将探讨弥合这一知识差距对于释放 SD-Branch 作为集成网络解决方案的全部潜力至关重要。我们还将探讨这如何与更广泛的 SASE（安全访问服务边缘）环境相结合，从而增强网络和安全融合。

## Aruba EdgeConnect SD-Branch 的演变

Aruba EdgeConnect SD-Branch 解决方案诞生于 2018 年，旨在解决传统网络架构中的复杂性，例如低效的流量管理、不灵活的网络配置以及大型和多样化环境中的高安全风险。

我们对 SD-Branch 的愿景是创建一个统一的、以用户为中心的网络解决方案，无缝结合 SD-WAN 和 SD-LAN 的优势。这一愿景的推动者是对 WAN 和 LAN 环境中更高的网络敏捷性、增强的安全性以及简化的管理的日益增长的需求。

自推出以来，EdgeConnect SD-Branch 开创了一种将 SD-WAN 和 SD-LAN 融合为单一优雅解决方案的新方法，提供了前所未有的优势。该解决方案不仅提高了网络性能，还改变了企业网络和安全的整个方法，提供端到端网络可见性，使网络管理员能够从单一管理平台监控和管理整个网络，并实现网络完全自动化跨整个结构（从 LAN 到 WAN）的安全管理，大大简化了 IT 运营。

此外，该解决方案中还嵌入了先进的安全功能，超越了过去基于边界的防御，转向了更全面的零信任安全模型，这在云计算和混合工作时代至关重要。借助 EdgeConnect SD-Branch，从核心到边缘的每个网段都被安全隔离，确保数据和用户受到保护，无论其位置或设备如何。

## 完全协调的 SD-LAN 和 SD-WAN 组合

从一开始，EdgeConnect SD-Branch 解决方案的愿景就不仅仅是简化 WAN 和路由操作。其核心目标是简化整个分支机构网络环境。这一目标是通过将 SD-WAN 和 SD-LAN 创新集成到统一平台中来实现的，该平台通过将网络和安全功能组合到单个解决方案中来补充 SASE 模型。这不仅简化了通信，还显著增强了安全性和用户体验。

由 Aruba Central 提供支持的 SD-Branch Orchestrator 在此集成中发挥着关键作用。它通过跨各种 WAN 电路自动构建 IPsec 隧道 overlay 网络、自动分配路由来简化 WAN 操作。此外，Orchestrator 通过创建从 AP 到网关的 GRE 或 IPsec 隧道网络，将其效率扩展到分支机构内的 LAN。这种双重方法可确保跨 WAN 和 LAN 频谱的无缝通信和运营效率，为基于 SASE 的架构奠定基础。

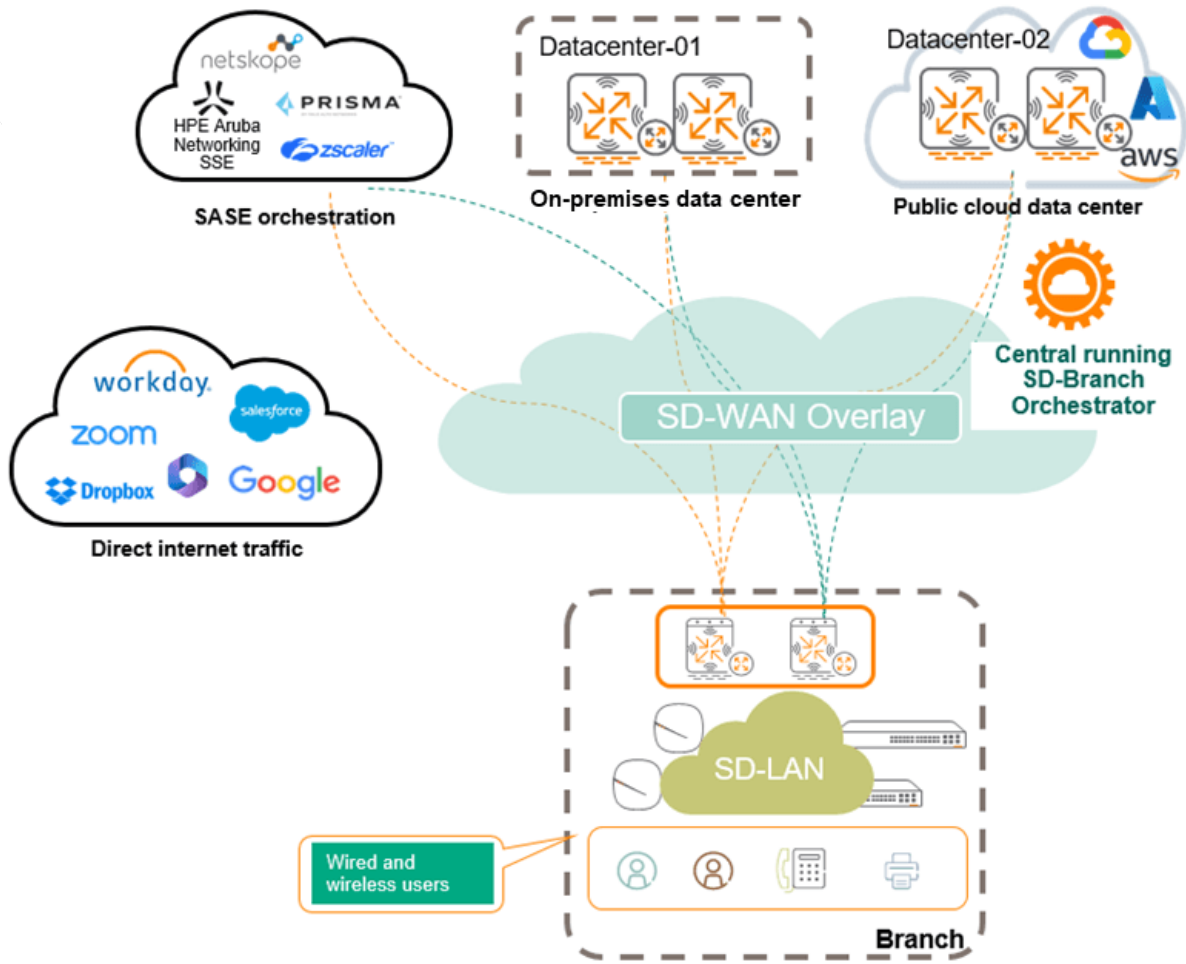


[www.arubanetworks.com](http://www.arubanetworks.com)

3333 Scott Blvd. Santa Clara, CA 95054

1.844.472.2782 | T: 1.408.227.4500 | FAX: 1.408.227.4550 | [info@arubanetworks.com](mailto:info@arubanetworks.com)

随着 Aruba AOS 10 架构的推出，Central 中不可或缺的 SD-Branch Orchestrator 现在可以编排安全的 IPsec 和 GRE 隧道，将每个 AP 和交换机端口连接到集群内的分支网关。该架构对于在分支机构部署中实现高可用性至关重要，通过两台分支机构网关处理 WAN 上行链路的终结。自动隧道编排流程增强了网络弹性，基于站点的集群有助于在每个集群内的设备之间创建隧道，确保无缝连接和平稳运行。



自动建立隧道到集群 leader

## 具有基于角色的策略的集中式安全性

AOS 10 架构中的集中用户管理和安全实施涉及在网关集群内对用户进行集群，从而提供统一的管理结构。网关集群是作为单个实体运行的两个 Aruba 网关的组合。此配置为网络中的无线和有线客户端提供高可用性和服务连续性。网关集群对于确保接入点和交换机的完全冗余以及在故障转移时保持无线和有线客户端的一致服务至关重要。

Aruba 网关对有线和无线连接实施一致的策略，利用动态分段确保全面的访问控制。此外，网关配备了应用感知防火墙和威胁管理功能，包括 IDS/IPS，将保护扩展到所有东西向流量。这种多方面的安全方法创建了一个不仅安全而且能够适应用户不断变化的需求的网络环境。

这种设置不仅仅是集中化；它增强了用户的移动性和安全性。它支持跨网关集群后面的 L3 域的快速漫游功能，从而确保用户在网络中移动时体验无缝连接。

EdgeConnect SD-Branch 解决方案跨 LAN、WLAN 和 SD-Branch 网关维护用户角色上下文，通过集成先进的 SD-LAN 功能（而不仅仅是建立隧道）来解决实施以用户为中心的安全策略的挑战。这种方法涉及身份验证过程的复杂协调，确保当用户在 AP 或交换机上进行身份验证时，网关会自动学习并强制执行其相关角色。

在网络边缘进行身份验证时分配给用户角色会立即可靠地传播到网关。这种跨 LAN、WLAN 和 SD-Branch 网关的用户角色自动同步与依赖用户角色窥探方法或 API 驱动的用户角色学习的传统系统形成鲜明对比，后者可能会导致延迟和不一致。分支网关集群充当隧道 SSID 的 RADIUS 代理服务器，这种方法不仅可以保护用户体验，还可以通过在整个网络中维护一致的用户角色上下文来简化用户体验。这种主动的角色管理是一个明显的区别，它提供动态的、基于角色的安全策略，并根据现代网络环境的要求立即应用。

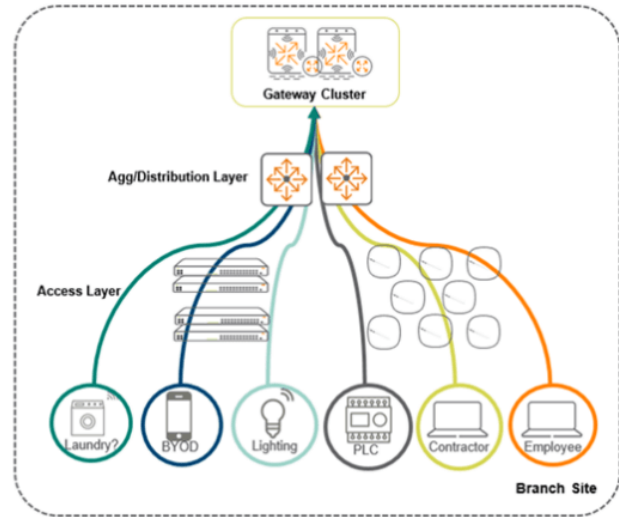
通过自动化此过程，EdgeConnect SD-Branch 实现了以用户为中心的安全模型，该模型既具有响应能力又具有弹性，确保安全措施与用户访问和网络流量模式的动态特性保持同步，从而促进无缝、安全的网络体验。



Users centralized in gateway clusters. **Fast roaming across L3 domains** behind the gateway cluster!

**Consistent policy enforcement for wired & wireless** with dynamic segmentation.

**Advanced application aware firewall** and threat management at the gateways for all east-west traffic.



## 集中安全

### SD-WAN 和 SD-LAN 融合的好处

EdgeConnect SD-Branch 中 SD-WAN 和 SD-LAN 的集成代表了企业网络的重大进步，体现了技术创新和应对现代网络挑战的承诺。这种融合确保了网络资源的高效利用，提供一致、高质量的服务以及更高的网络管理灵活性。通过快速适应不断变化的网络使用模式和要求，并优化运营和安全性，这种统一的方法允许组织从单一平台管理 LAN 和 WAN 网络，以实现安全第一的网络。此外，EdgeConnect SD-Branch 与 Aruba SSE（安全服务边缘）紧密集成，形成统一的 SASE 平台，添加先进的云交付安全功能，例如 ZTNA（零信任网络访问）、SWG（安全 Web 网关）和 CASB（云访问安全代理）。

### 易于实施和管理

EdgeConnect SD-Branch 的主要优势之一是其实施和管理的简单性。该解决方案的设计重点是降低传统上与网络设置相关的复杂性，尤其是在需要 WAN 和 LAN 功能的环境中。这种简化的方法不仅减少了部署所需的时间和资源，还简化了持续的网络管理。它使组织能够更有效地管理其网络，减少日常运营对专业 IT 技能的依赖。并为 SSE 的整合铺平道路，进一步简化网络安全管理。

## 展望未来

当我们展望企业网络的未来时，挑战和需求将不断发展。在这个不断变化的环境中，EdgeConnect SD-Branch 不仅是当今创新的产品，而且是面向未来进步的平台。我们在集成 SD-WAN 和 SD-LAN 方面的先驱作用，加上在安全方面的良好记录，强调了我们为网络和安全提供共同基础的承诺。SASE 的原则深深嵌入我们的路线图中，确保 EdgeConnect SD-Branch 将继续发展并满足安全、以云为中心的网络未来的需求。

**aruba**

a Hewlett Packard  
Enterprise company

[www.arubanetworks.com](http://www.arubanetworks.com)

3333 Scott Blvd. Santa Clara, CA 95054

1.844.472.2782 | T: 1.408.227.4500 | FAX: 1.408.227.4550 | [info@arubanetworks.com](mailto:info@arubanetworks.com)