



架构图

用于在上实施 SD-WAN 解决方案的参考架构 AWS



用于在上实施 SD-WAN 解决方案的参考架构 AWS: 架构图

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon 的商标和商业外观不得用于任何非 Amazon 的商品或服务，也不得以任何可能引起客户混淆、贬低或诋毁 Amazon 的方式使用。所有非 Amazon 拥有的其他商标均为各自所有者的财产，这些所有者可能附属于 Amazon、与 Amazon 有关联或由 Amazon 赞助，也可能不是如此。

Table of Contents

TGW Connect 1

SD-WAN 与 AWS Transit 网关连接架构的连接 1

延伸阅读 2

图表历史 2

云广域网连接 4

SD-WAN 与 AWS 云广域网连接架构 4

延伸阅读 5

图表历史 5

云广域网 Tunnel-less 7

SD-WAN 与 AWS 云广域网 Tunnel-less 连接架构 7

延伸阅读 8

图表历史 8

VPN 到 TGW 10

SD-WAN 通过 AWS Site-to-Site VPN 连接到 AWS 传输网关架构 10

延伸阅读 11

图表历史 11

VPN 到云广域网 13

SD-WAN 与 AWS Site-to-Site VPN 的连接到 AWS 云广域网架构 13

延伸阅读 14

图表历史 14

搭载 TGW 的 DX 16

SD-WAN 设备与 AWS 传输网关和 AWS Direct Connect 架构集成 16

延伸阅读 17

图表历史 17

带有云广域网的 DX 19

SD-WAN 设备与集成 AWS 云广域网和 AWS 直接连接架构 19

延伸阅读 20

图表历史 20

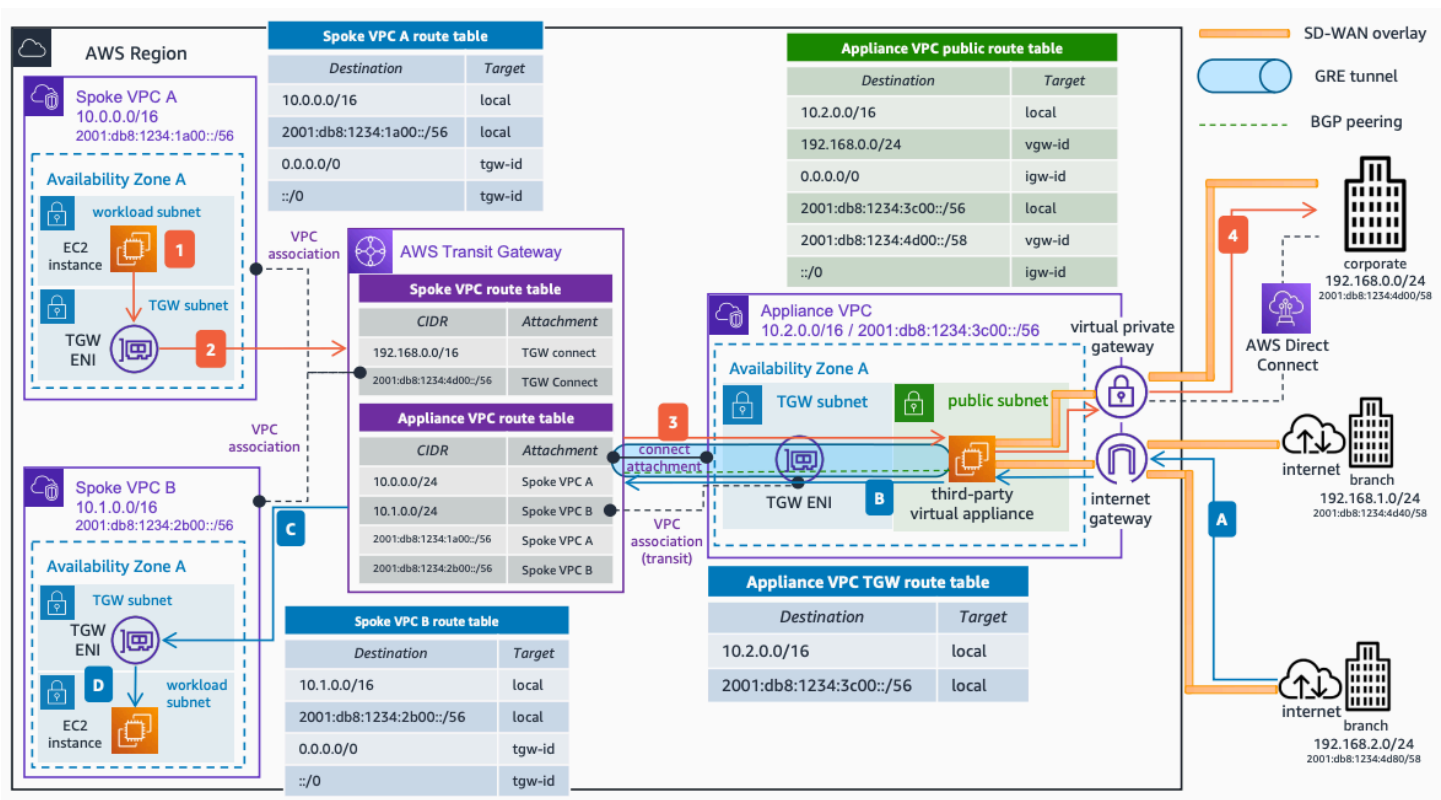
..... xxii

SD-WAN 与 AWS Transit Gateway 连接附件连接

发布日期：2024 年 12 月 28 日 (图表历史)

该架构展示了如何使用 [AWS Transit Gateway Connect](#) 附件将软件定义的广域网 (SD-WAN) 连接到 Transit Gateway，并简化混合云环境中的路线管理。SD-WAN 头端通过通用路由封装 (GRE) 隧道与中转网关对等，从而使该设计能够利用传输网关更高的边界网关协议 (BGP) 前缀限制。此外，通过单个 Transit Gateway Connect 附件，您可以将连接的带宽水平扩展到 20 Gbps。

SD-WAN 与 AWS Transit 网关连接架构的连接



以下步骤描述了 AWS 到本地的流量：

- 根据分支 VPC A 路由表，从分支[亚马逊 VPC A](#) 中的亚马逊弹性计算云实例发起并发往公司数据中心的流量将路由到传输网关弹性网络接口 (TGW ENI)。
- 流量被转发到 AWS Transit Gateway。根据分支 VP C 路由表，流量通过 Transit Gateway Connect 附件路由到设备 VPC。
- Transit Gateway Connect 连接使用 Amazon VPC 附件作为传输，并使用 GRE 隧道和 BGP 将 Transit Gateway 连接到设备 VPC 中的第三方设备。

4. 第三方虚拟设备封装流量，流量使用 SD-WAN 叠加层（在 [AWS Direct Connect](#) 链接的顶部）到达企业数据中心。

以下步骤描述了本地到的流 AWS 量：

来自外部分支机构 AWS 发往 Spoke Amazon VPC B 的流量通过互联网顶部的 SD-WAN 叠加层到达设备 VPC 的互联网网关。

Connect VPC 中的第三方虚拟设备通过连接附件将流量转发到传输网关。

根据传输网关设备亚马逊 VPC 路由表，流量将转发到分支 V PC B 附件。

分支 VPC B 的中转网关 ENI 将流量转发到目的地。

有关 AWS Transit Gateway Connect 附件和 SD-WAN 连接的更多信息，请参阅使用 AWS Transit Gateway Connect [简化 SD-WAN 连接](#)。

延伸阅读

有关更多信息，请参阅以下资源：

- [AWS 架构图标](#)
- [AWS Well-Architected](#)

图表历史

要获得有关此参考架构图更新的通知，请订阅 RSS 提要。

变更	说明	日期
初次发布	参考架构图首次发布。	2024年12月28日
初次发布	参考架构图首次发布。	2024年12月28日
初次发布	参考架构图首次发布。	2024年12月28日
初次发布	参考架构图首次发布。	2024年12月28日
初次发布	参考架构图首次发布。	2024年12月28日

初次发布	参考架构图首次发布。	2024年12月28日
初次发布	参考架构图首次发布。	2024年12月28日

 Note

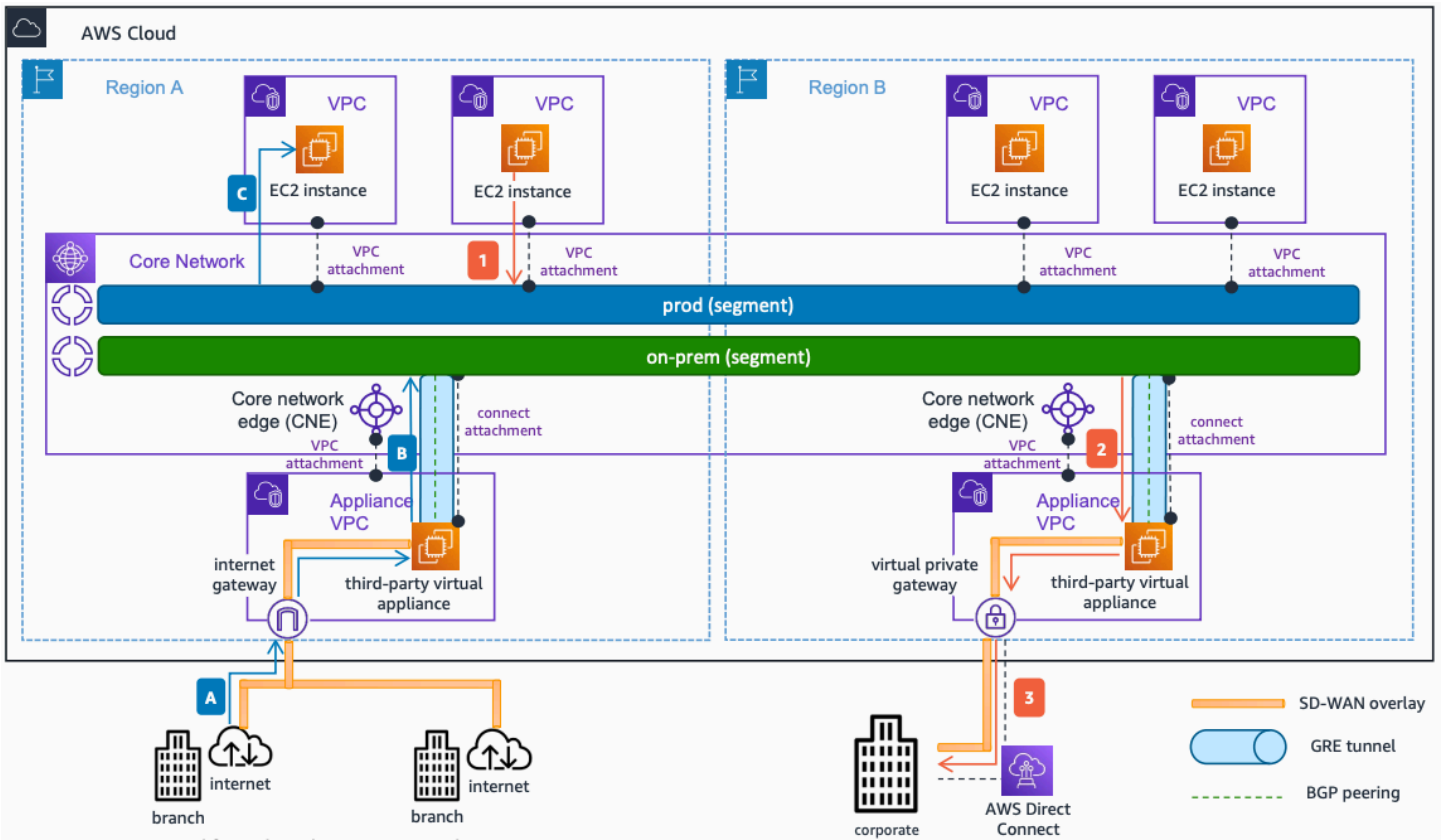
要订阅 RSS 更新，必须为正在使用的浏览器启用 RSS 插件。

SD-WAN 连接到 AWS 云广域网连接附件

发布日期：2024 年 12 月 28 日 ([图表历史](#))

此架构展示了如何使用 Connect 附件将您连接 SD-WAN 到 AWS Cloud WAN，以及如何简化混合云环境中的路由管理。SD-WAN 头端通过 GRE 隧道与云广域网的核心网络边缘 (CNE) 对等，从而使该设计能够利用 [AWS Transit Gateway 更高的 BGP 前缀限制](#)。此外，通过单个 Transit Gateway Connect 附件，您可以将连接的带宽水平扩展到 20 Gbps。

SD-WAN 与 AWS 云广域网连接架构



以下步骤描述了 AWS 到本地的流量：

1. 从区域 A 的亚马逊 VPC 中的亚马逊弹性计算云实例发起并发往企业数据中心的流量将转发到核心网络。亚马逊 VPC 附件与产品段相关联。
2. 根据核心网络政策，到达产品分段的流量应转发到区域 B 的连接附件。连接附件使用亚马逊 VPC 附件作为传输，并使用 GRE 隧道和 BGP 将核心网络连接到设备亚马逊 VPC 中的第三方设备。

3. 第三方虚拟设备封装流量，流量使用 SD-WAN 叠加层（在 [AWS Direct Connect](#) 链接的顶部）到达企业数据中心。

以下步骤描述了本地到的流 AWS 量：

- 来自外部分支机构 AWS 发往区域 A 中的亚马逊 VPC 的流量通过互联网顶部的 SD-WAN 叠加层到达设备亚马逊 VPC 的互联网网关。
- 连接亚马逊 VPC 中的第三方虚拟设备通过连接附件将流量转发到核心网络。连接附件与本地分段相关联。
- 根据核心网络政策，流量被转发到相应的亚马逊 VPC，将流量转发到目的地。

延伸阅读

有关更多信息，请参阅以下资源：

- [AWS 架构图标](#)
- [AWS Well-Architected](#)

图表历史

要获得有关此参考架构图更新的通知，请订阅 RSS 提要。

变更	说明	日期
初次发布	参考架构图首次发布。	2024年12月28日
初次发布	参考架构图首次发布。	2024年12月28日
初次发布	参考架构图首次发布。	2024年12月28日
初次发布	参考架构图首次发布。	2024年12月28日
初次发布	参考架构图首次发布。	2024年12月28日
初次发布	参考架构图首次发布。	2024年12月28日
初次发布	参考架构图首次发布。	2024年12月28日

 Note

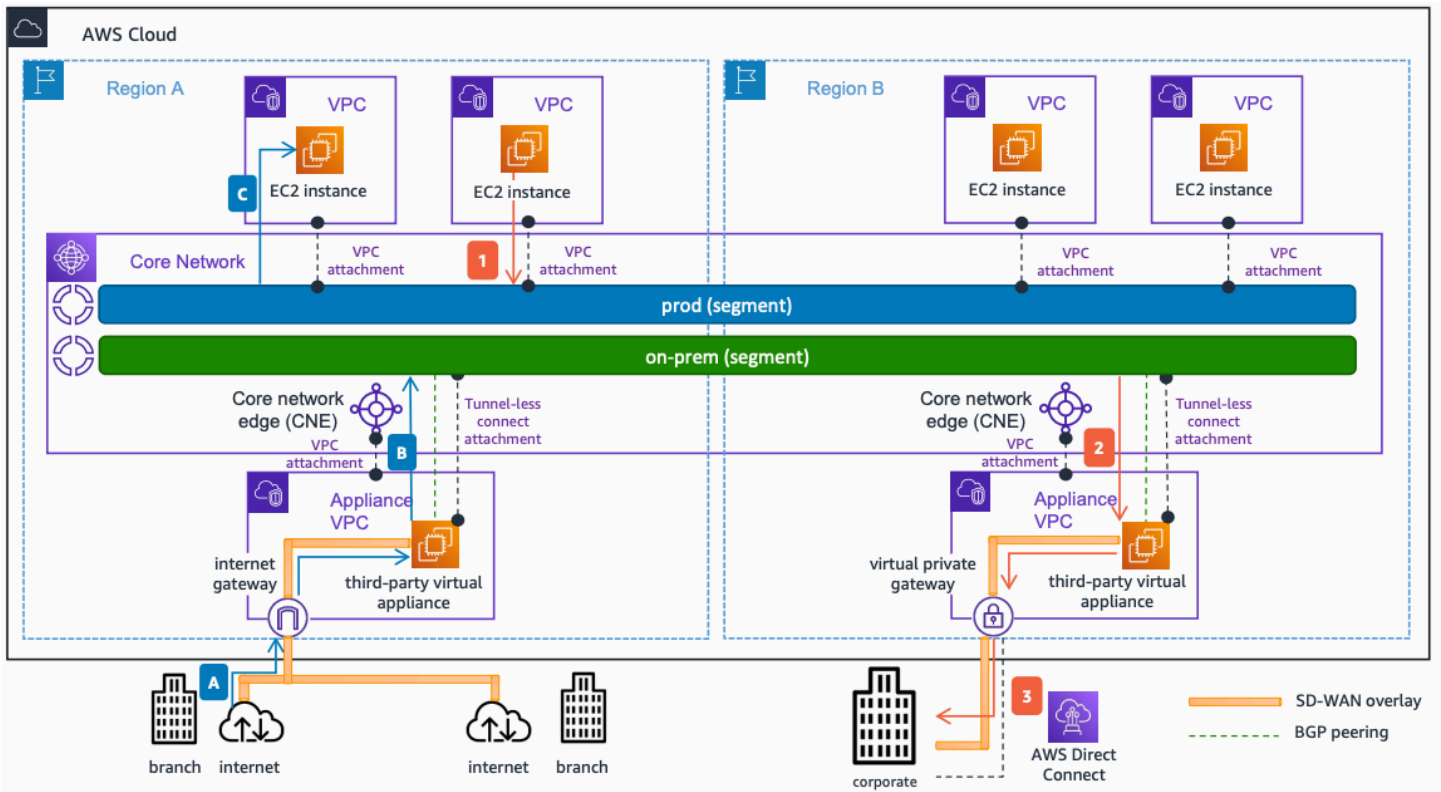
要订阅 RSS 更新，必须为正在使用的浏览器启用 RSS 插件。

SD-WAN 连接到 AWS 云广域网 Tunnel-less 连接附件

发布日期：2024 年 12 月 28 日 ([图表历史](#))

该架构展示了如何使用 Tunnel-less AWS 全球网络作为中英里传输网络，使用 Connect 附件 SD-WAN 以更简单、更高性能的方式将您连接到 AWS Cloud WAN。该 SD-WAN 头端通过 BGP 与云广域网的核心网络边缘 (CNE) 本机对等，无需使用 GRE 等专用隧道协议，从而消除隧道开销并提高吞吐量性能，而吞吐量性能则使用全部 Amazon VPC 连接带宽（每个可用区最高 100 Gbps）。

SD-WAN 与 AWS 云广域网 Tunnel-less 连接架构



以下步骤描述了 AWS 到本地的流量：

1. 从区域 A 的亚马逊 VPC [中的](#) 亚马逊弹性计算云实例发起并发往企业数据中心的流量将转发到核心网络。亚马逊 VPC 附件与产品段相关联。
2. 根据核心网络政策，到达产品分段的流量应转发到区域 B 的连接附件。Tunnel-less 连接附件使用亚马逊 VPC 附件作为传输，并使用原生 BGP 将核心网络连接到设备亚马逊 VPC 中的第三方设备。Tunnel-less

3. 第三方虚拟设备封装流量，流量使用 SD-WAN 叠加层（在 [AWS Direct Connect](#) 链接的顶部）到达企业数据中心。

以下步骤描述了本地到的流 AWS 量：

来自外部分支机构 AWS 发往区域 A 中的亚马逊 VPC 的流量通过互联网顶部的 SD-WAN 叠加层到达设备亚马逊 VPC 的互联网网关。

连接亚马逊 VPC 中的第三方虚拟设备通过 Tunnel-less 连接附件将流量转发到核心网络。Tunnel-less 连接附件与本地分段相关联。

根据核心网络政策，流量被转发到相应的亚马逊 VPC，将流量转发到目的地。

延伸阅读

有关更多信息，请参阅以下资源：

- [AWS 架构图标](#)
- [AWS Well-Architected](#)

图表历史

要获得有关此参考架构图更新的通知，请订阅 RSS 提要。

变更	说明	日期
初次发布	参考架构图首次发布。	2024年12月28日
初次发布	参考架构图首次发布。	2024年12月28日
初次发布	参考架构图首次发布。	2024年12月28日
初次发布	参考架构图首次发布。	2024年12月28日
初次发布	参考架构图首次发布。	2024年12月28日
初次发布	参考架构图首次发布。	2024年12月28日
初次发布	参考架构图首次发布。	2024年12月28日

 Note

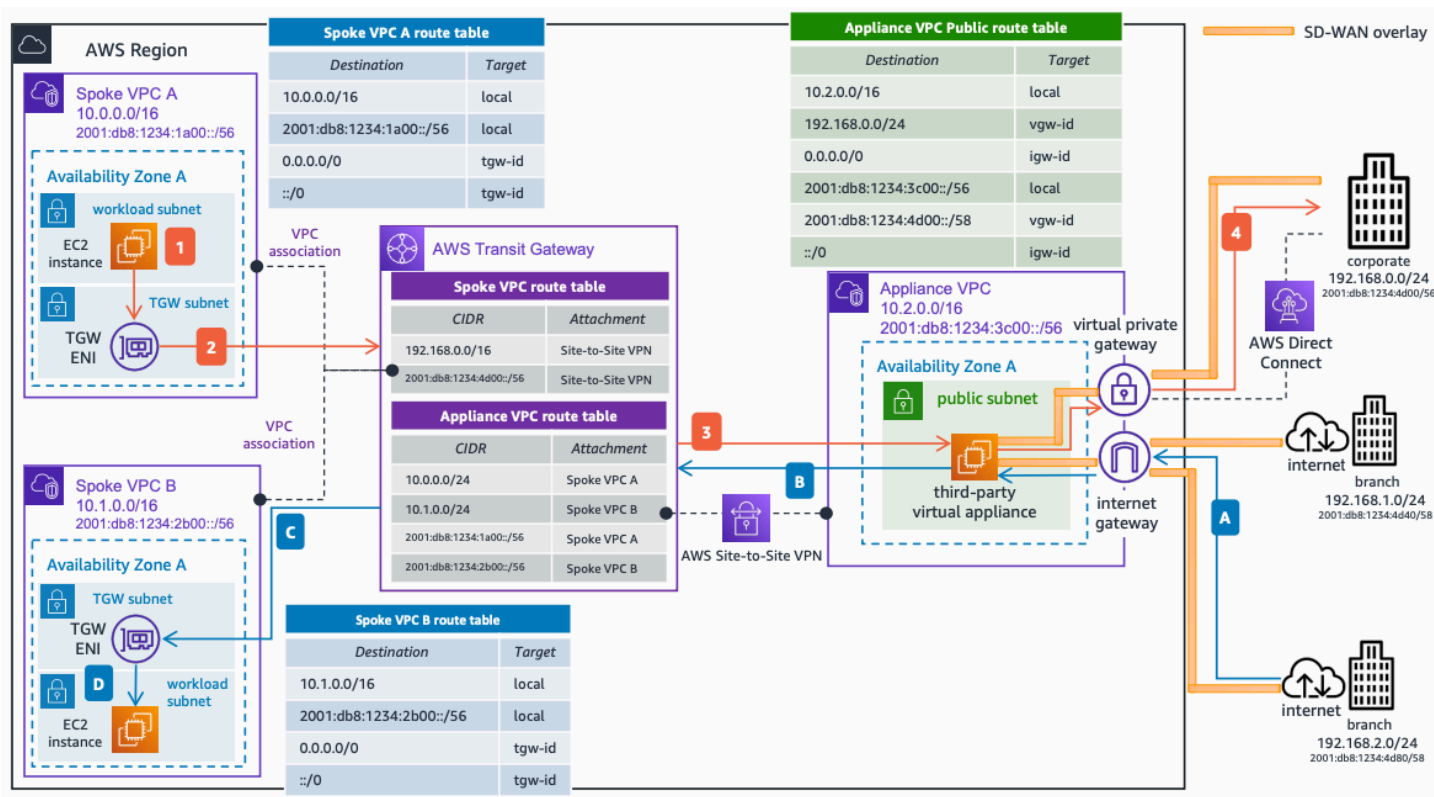
要订阅 RSS 更新，必须为正在使用的浏览器启用 RSS 插件。

SD-WAN 使用 AWS Site-to-Site VPN 连接到 AWS 传输网关

发布日期：2024 年 12 月 28 日 ([图表历史](#))

如果您的第三方虚拟设备不支持 GRE，您仍然可以通过创建 AWS Site-to-Site VPN 连接、使用 IPsec 隧道将 SD-WAN 头端与传输网关对等来将您的 SD-WAN 网络集成到 AWS Transit Gateway。SD-WAN 头端可以使用 BGP 与中转网关对等交换路由前缀。如果您想将带宽增加到超过单个 Site-to-Site VPN 连接的 1.25 Gbps 限制，则可以在 Transit Gateway 支持 Equal-Cost Multi-Path (ECMP) 的情况下使用额外的 IPsec VPN 连接。

SD-WAN 通过 AWS Site-to-Site VPN 连接到 AWS 传输网关架构



以下步骤描述了 AWS 到本地的流量：

1. 根据分支 VPC A 的路由表，从分支 Amazon VPC A 中的实例发起并发往公司数据中心的流量将路由到 TGW ENI。
2. 流量被转发到传输网关。根据分支 VPC 路由表，流量通过 VP Site-to-Site N 附件路由到设备 VPC。
3. 流量使用 Site-to-Site VPN 连接在 Transit Gateway 和第三方虚拟设备之间路由。

4. 第三方虚拟设备封装流量，流量使用 SD-WAN 叠加层（在 [AWS Direct Connect](#) 链接的顶部）到达企业数据中心。

以下步骤描述了本地到的流 AWS 量：

来自外部分支机构 AWS 发往 Spoke Amazon VPC B 的流量通过互联网顶部的 SD-WAN 叠加层到达设备 VPC 的互联网网关。

设备 VPC 中的第三方虚拟设备通过 VP Site-to-Site N 连接将流量转发到传输网关。

根据 Transit Gateway 设备 VPC 路由表，流量将转发到分支 VPC B 附件。

分支 VPC B 的 TGW ENI 将流量转发到目的地。

延伸阅读

有关更多信息，请参阅以下资源：

- [AWS 架构图标](#)
- [AWS Well-Architected](#)

图表历史

要获得有关此参考架构图更新的通知，请订阅 RSS 提要。

变更	说明	日期
初次发布	参考架构图首次发布。	2024年12月28日
初次发布	参考架构图首次发布。	2024年12月28日
初次发布	参考架构图首次发布。	2024年12月28日
初次发布	参考架构图首次发布。	2024年12月28日
初次发布	参考架构图首次发布。	2024年12月28日
初次发布	参考架构图首次发布。	2024年12月28日
初次发布	参考架构图首次发布。	2024年12月28日

 Note

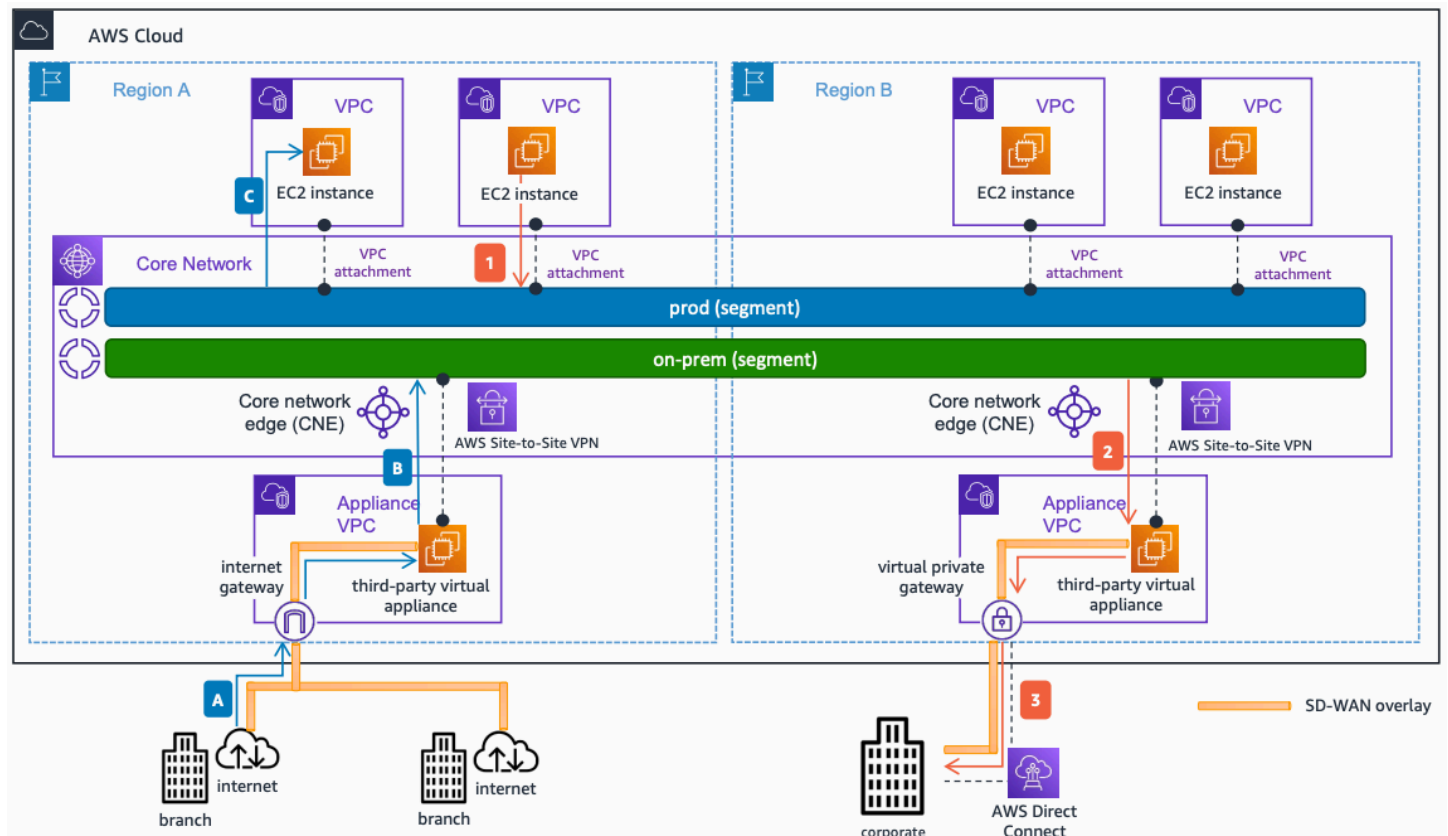
要订阅 RSS 更新，必须为正在使用的浏览器启用 RSS 插件。

SD-WAN 使用 AWS Site-to-Site VPN 连接到 AWS 云 WAN

发布日期：2024 年 12 月 28 日 ([图表历史](#))

如果您的第三方虚拟设备不支持 GRE，您仍然可以通过创建 AWS Site-to-Site VPN 连接、[使用 IPsec 隧道将 SD-WAN 头端与](#)传输网关对等来将您的 SD-WAN 网络集成到 AWS 云广域网。SD-WAN 头端可以使用 BGP 与中转网关对等交换路由前缀。如果您想将带宽增加到超过单个 Site-to-Site VPN 连接的 1.25 Gbps 限制，则可以在云广域网支持 Equal-Cost Multi-Path (ECMP) 的情况下使用额外的 IPsec VPN 连接。

SD-WAN 与 AWS Site-to-Site VPN 的连接到 AWS 云广域网架构



以下步骤描述了 AWS 到本地的流量：

1. 从区域 A 的亚马逊 VPC 中的亚马逊弹性计算云实例发起并发往企业数据中心的流量将转发到核心网络。亚马逊 VPC 附件与产品段相关联。
2. 根据核心网络政策，到达产品分段的流量应转发到区域 B 的 Site-to-Site VPN 附件。流量使用 VPN 连接在核心网络和第三方虚拟设备之间路由。Site-to-Site

3. 第三方虚拟设备封装流量，流量使用 SD-WAN 叠加层（在 [AWS Direct Connect](#) 链接的顶部）到达企业数据中心。

以下步骤描述了本地到的流 AWS 量：

从外部分支机构 AWS 流向区域 A 中的 Amazon VPC 的流量通过互联网顶部的 SD-WAN 叠加层到达该区域中设备 VPC 的互联网网关。

设备 VPC 中的第三方虚拟设备通过 VP Site-to-Site N 连接将流量转发到核心网络。

根据核心网络政策，流量被转发到相应的亚马逊 VPC，将流量转发到目的地。

延伸阅读

有关更多信息，请参阅以下资源：

- [AWS 架构图标](#)
- [AWS Well-Architected](#)

图表历史

要获得有关此参考架构图更新的通知，请订阅 RSS 提要。

变更	说明	日期
初次发布	参考架构图首次发布。	2024年12月28日
初次发布	参考架构图首次发布。	2024年12月28日
初次发布	参考架构图首次发布。	2024年12月28日
初次发布	参考架构图首次发布。	2024年12月28日
初次发布	参考架构图首次发布。	2024年12月28日
初次发布	参考架构图首次发布。	2024年12月28日
初次发布	参考架构图首次发布。	2024年12月28日

 Note

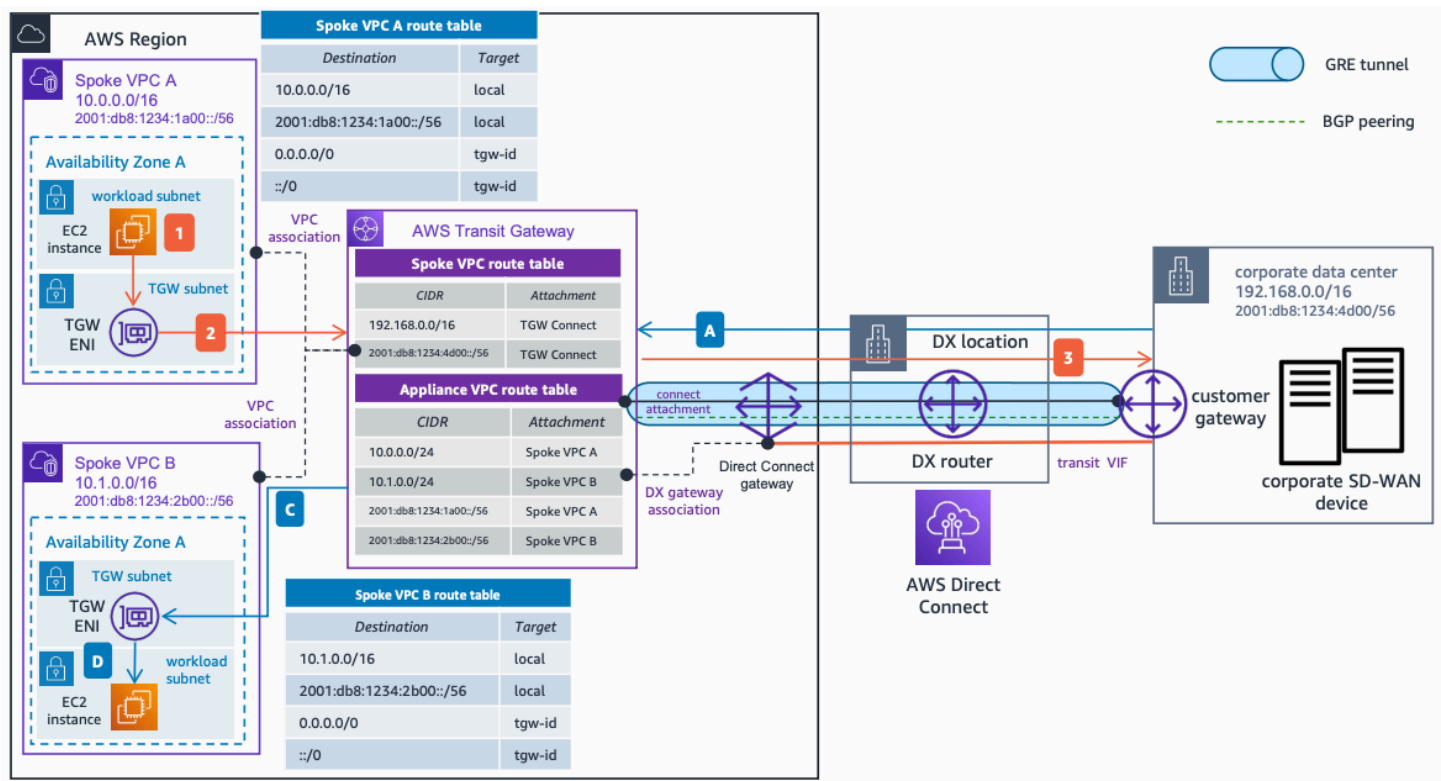
要订阅 RSS 更新，必须为正在使用的浏览器启用 RSS 插件。

SD-WAN 设备与 AWS 传输网关和 AWS Direct Connect 集成

发布日期：2024 年 12 月 28 日 (图表历史)

该架构展示了如何在 AWS 不增加额外基础设施的情况下使用 [AWS Transit Gateway](#) Connect 附件和 [AWS Direct Connect](#) 来扩展和分段 SD-WAN 流量。每个 Transit Gateway Connect 对等体都可以拥有自己的中转网关路由表和 BGP 对等体，以便在需要时扩展本地 VRF。

SD-WAN 设备与 AWS 传输网关和 AWS Direct Connect 架构集成



以下步骤描述了 AWS 到本地的流量：

1. 根据分支[亚马逊 VPC](#) A 路由表，从分支亚马逊 VPC A 中的实例发起并发往公司数据中心 SD-WAN 设备的流量将路由到 TGW ENI。
2. 流量被转发到传输网关。根据分支 V PC 路由表，流量通过 Transit Gateway Connect 附件路由到公司数据中心。
3. Transit Gateway Connect 连接使用直接连接作为传输，并使用 GRE 隧道和 BGP 将传输网关连接到公司数据中心 SD-WAN 设备。

以下步骤描述了本地到流 AWS 量：

从企业数据中心 SD-WAN 设备发往分支 VPC B 的流量通过传输网关连接的 GRE 隧道通过直接连接链路转发到传输网关。

根据中转网关连接路由表，流量将转发到分支 VPC B 附件。

分支 VPC B 的 TGW ENI 将流量转发到目的地。

有关如何使用 AWS Transit Gateway 和 AWS Direct Connect 集成本地 SD-WAN 设备的更多信息，请参阅将 SD-WAN 设备与 AWS Transit Gateway 和 AWS Direct Connect [集成](#)。

延伸阅读

有关更多信息，请参阅以下资源：

- [AWS 架构图标](#)
- [AWS Well-Architected](#)

图表历史

要获得有关此参考架构图更新的通知，请订阅 RSS 提要。

变更	说明	日期
初次发布	参考架构图首次发布。	2024年12月28日
初次发布	参考架构图首次发布。	2024年12月28日
初次发布	参考架构图首次发布。	2024年12月28日
初次发布	参考架构图首次发布。	2024年12月28日
初次发布	参考架构图首次发布。	2024年12月28日
初次发布	参考架构图首次发布。	2024年12月28日
初次发布	参考架构图首次发布。	2024年12月28日

 Note

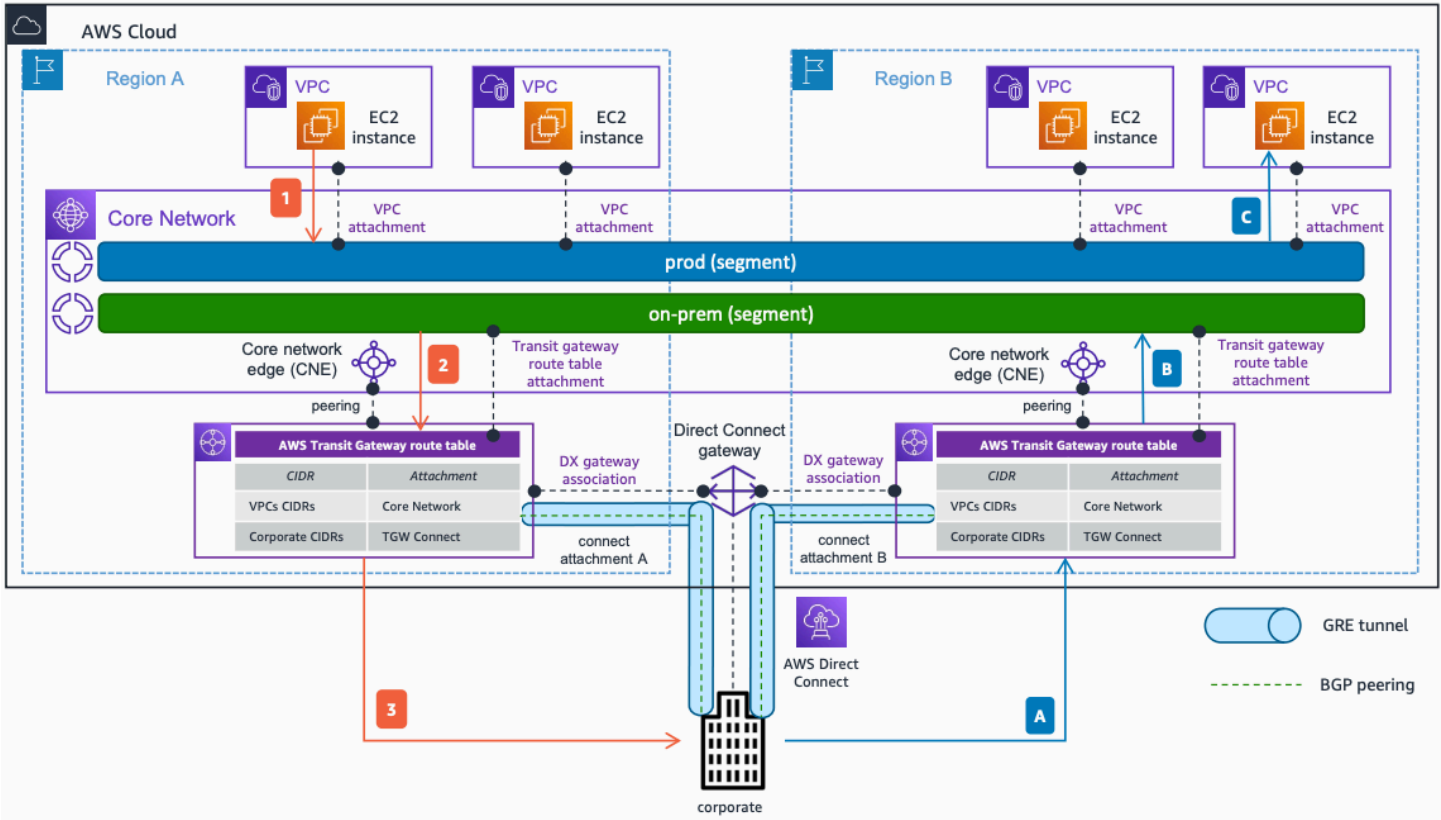
要订阅 RSS 更新，必须为正在使用的浏览器启用 RSS 插件。

SD-WAN 设备与集成 AWS 通过 AWS 传输网关实现云广域网和 AWS 直接连接

发布日期：2024 年 12 月 28 日 (图表历史)

AWS 通过 [AWS Direct Connect](#) 将 SD-WAN 流量扩展到 AWS 云广域网时，您可以利用 [AWS Transit Gateway](#) Connect 附件以及云广域网和公交网关之间的对等来实现端到端的动态路由。您可以使用不同的 Transit Gateway Connect 对等体和路由表以及 Cloud WAN 路由表附件和分段，在本地环境中扩展每个 VRF。

SD-WAN 设备与集成 AWS 云广域网和 AWS 直接连接架构



以下步骤描述了 AWS 到本地的流量：

1. 从区域 A 的 [Amazon VPC](#) 中的实例发起并发往公司数据中心 SD-WAN 设备的流量将转发到核心网络。亚马逊 VPC 附件与产品段相关联。
2. 根据核心网络政策，到达产品分段的流量应转发到企业数据中心的 Transit Gateway 路由表附件。本地附件将是首选。流量将转发到区域 A 中的 AWS Transit Gateway。

3. 根据中转网关路由表，流量将通过 Transit Gateway Connect 附件 A 转发。此附件使用直接连接作为传输，并使用 GRE 隧道和 BGP 将传输网关连接到公司数据中心 SD-WAN 设备。

以下步骤描述了本地到的流 AWS 量：

Na从企业数据中心 SD-WAN 设备发往区域 B 中的 Amazon VPC 的流量通过公交网关连接附件 B 通过直接连接链接转发到区域 B 中的中转网关。

Na根据传输网关路由表，流量将转发到核心网络。Transit Gateway 路由表附件与本地分段相关联。

Na核心网络将流量转发到相应的亚马逊 VPC。

延伸阅读

有关更多信息，请参阅以下资源：

- [AWS 架构图标](#)
- [AWS Well-Architected](#)

图表历史

要获得有关此参考架构图更新的通知，请订阅 RSS 提要。

变更	说明	日期
初次发布	参考架构图首次发布。	2024年12月28日
初次发布	参考架构图首次发布。	2024年12月28日
初次发布	参考架构图首次发布。	2024年12月28日
初次发布	参考架构图首次发布。	2024年12月28日
初次发布	参考架构图首次发布。	2024年12月28日
初次发布	参考架构图首次发布。	2024年12月28日
初次发布	参考架构图首次发布。	2024年12月28日

 Note

要订阅 RSS 更新，必须为正在使用的浏览器启用 RSS 插件。

本文属于机器翻译版本。若本译文内容与英语原文存在差异，则一律以英文原文为准。