



架构图

VMware Cloud on AWS 网络参考架构



VMware Cloud on AWS 网络参考架构: 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

直接连接到 VGW 1

VMware Cloud on AWS 使用直接连接到 VGW 架构进行联网 1

延伸阅读 2

图表历史 2

带有 DXGW 和 TGW 的 DX 3

VMware Cloud on AWS 使用直接连接网关和传输网关架构进行联网 3

延伸阅读 4

图表历史 4

VMware 交通连接 5

具有高弹性的连接 VMware 公交连接架构 5

延伸阅读 6

图表历史 6

安全 VPC 检查 7

安全 VPC 检查 VMware Cloud on AWS 交通架构 7

延伸阅读 8

图表历史 8

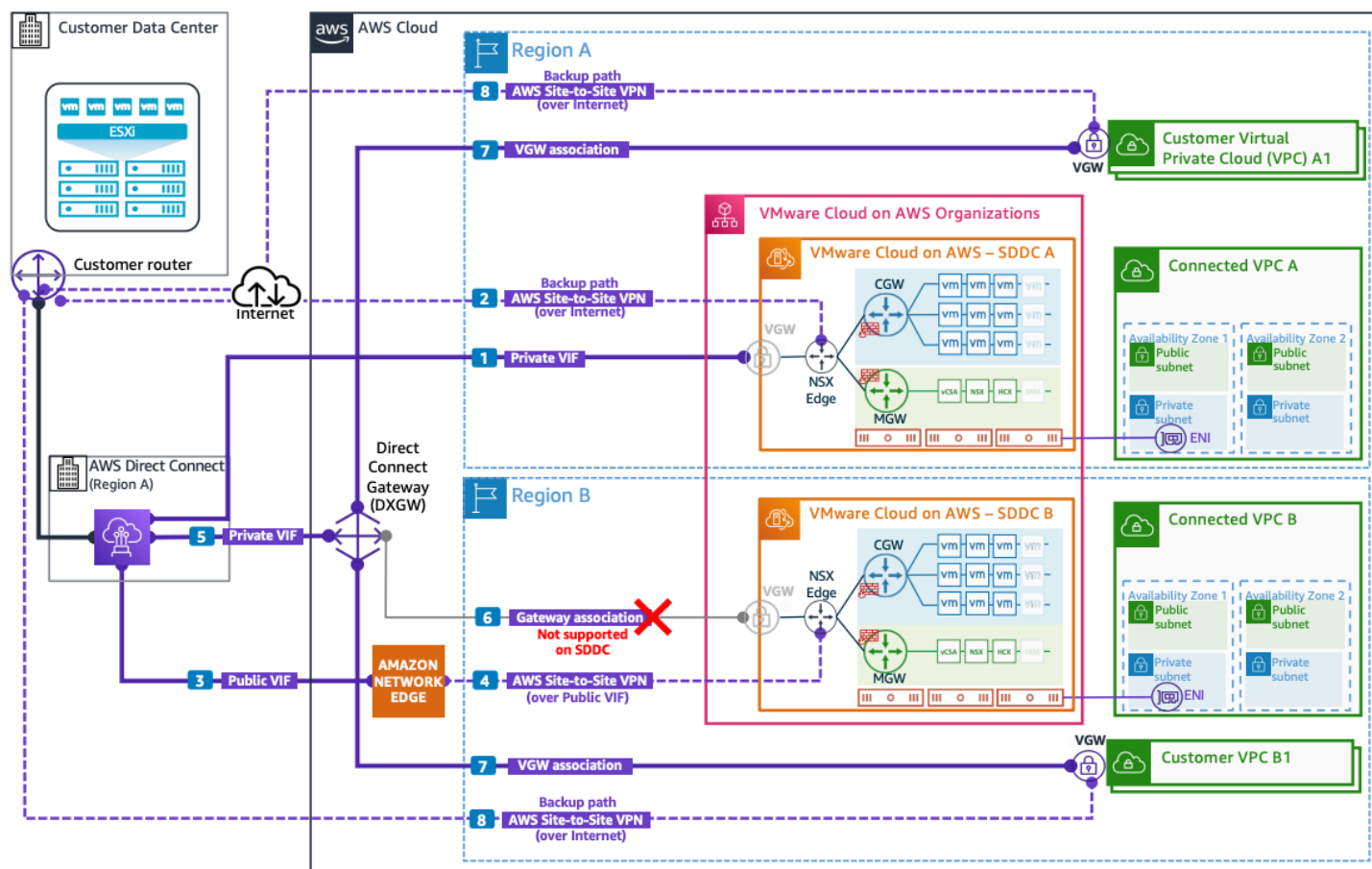
..... ix

On-Premises 使用 AWS Direct 连接虚拟私有网关和 VPN 进行连接

发布日期：2022年 3月10日 ([图表历史](#))

该架构显示了使用 AWS Direct Connect 与虚拟私有网关 (VGW) 和 AWS V Site-to-Site PN 进行备份连接的本地 VMware Cloud on AWS Software-defined 数据中心 (SDDC) 连接。

VMware Cloud on AWS 使用直接连接到 VGW 架构进行联网



以下编号的项目描述了该架构中的关键组件：

1. 私有虚拟接口 (VIF) 与 A 中的 VMware Software-defined 数据中心 (SDDC) A 建立连接。AWS 区域
2. AWS Site-to-Site VPN (通过互联网) 提供与私有 VIF 的备份连接，以提供与 VMware SDDC A 的弹性连接。
3. 公共 VIF 允许使用公有 IP 地址访问所有 AWS 公共服务和端点。

4. 区域 B 中缺少 [AWS Direct Connect](#) 连接造成了设计限制；因此，在 VMware SDDC B 上建立 VP Site-to-Site N。此 VPN 使用区域 A 中直接连接中的公有 VIF，与基于互联网的 Site-to-Site VPN 相比，公共 VIF 上的 VPN 可用于建立更稳定的网络体验。
5. AWS Direct Connect 网关 (DXGW) 的私有 VIF 使得 DXGW 能够通过将 DXGW 关联到虚拟私有网关 (VGW) 与不同区域的[亚马逊 VPC](#) 建立本地通信。
6. DXGW 的私有 VIF 不能用于与 SDDC 的网关关联。VMware不支持此功能VMware Cloud on AWS。
7. 在 DXGW 和 VGW 之间建立了网关关联，以支持与多个地区的亚马逊 VPC 进行本地通信。
8. Site-to-Site VPN 被配置为 DXGW-VGW 协会的备份，以便更灵活地连接到 Amazon 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。	2022 年 3 月 10 日
初次发布	参考架构图首次发布。	2022 年 3 月 10 日
初次发布	参考架构图首次发布。	2022 年 3 月 10 日
初次发布	参考架构图首次发布。	2022 年 3 月 10 日

 Note

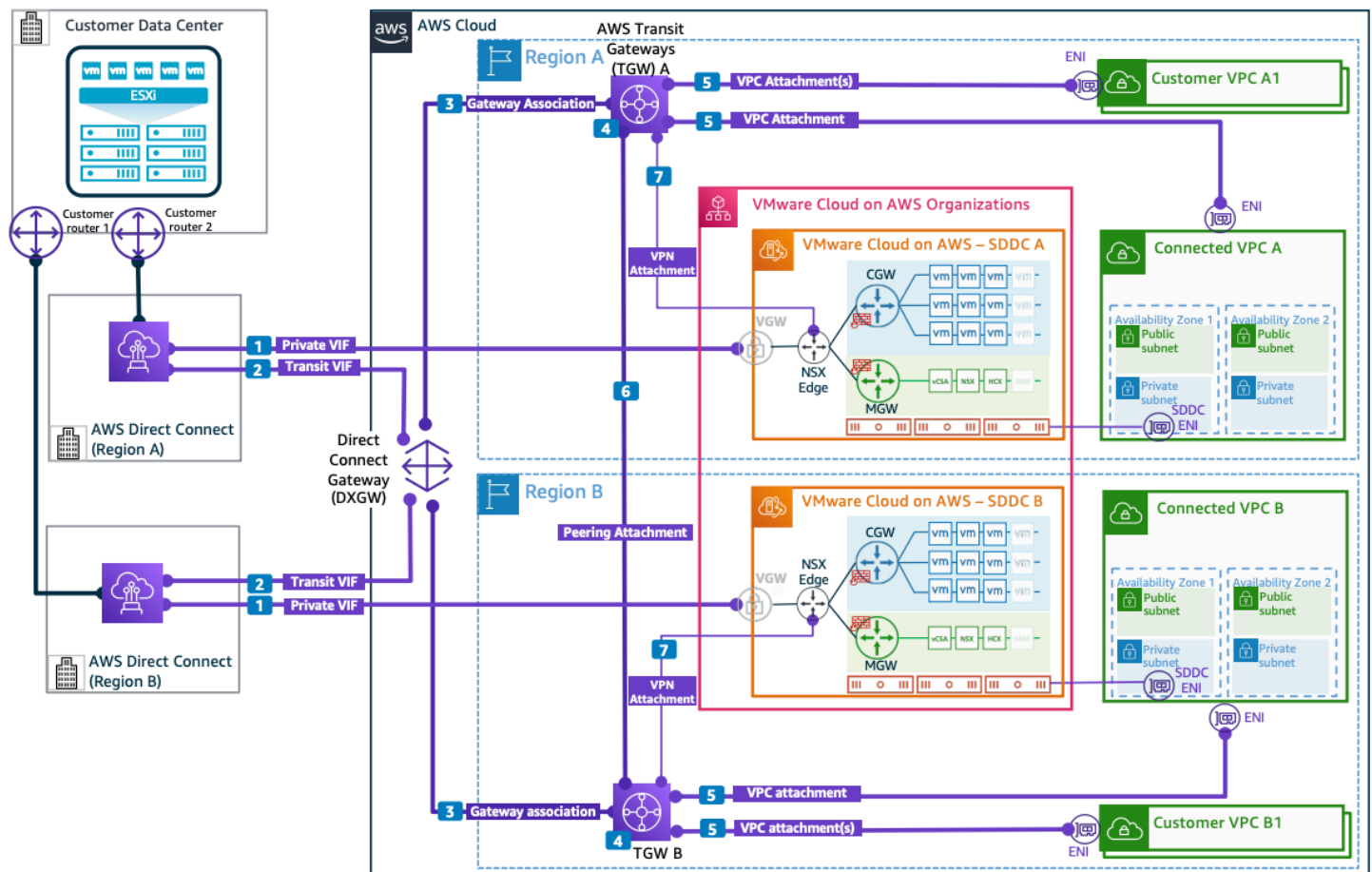
要订阅 RSS 更新，必须为正在使用的浏览器启用 RSS 插件。

On-Premises 使用 AWS Direct Connect、Direct Connect 网关和 AWS

发布日期：2022年 3月10日 ([图表历史](#))

该架构显示了VMware Cloud on AWS使用与多个区域的 AWS Transit Gateway 实例关联的 Direct Connect 网关 (DXGW) 的 AWS Direct Connect 进行本地连接，以实现可扩展的传递路由。

VMware Cloud on AWS 使用直接连接网关和传输网关架构进行联网



以下编号的项目描述了该架构中的关键组件：

1. 区域 A 中的 [AWS Direct Connect](#) 私有 VIF 建立了从本地网络到区域 A 的连接。同样，来自区域 B 的 AWS Direct Connect 私有 VIF 建立了从本地网络到区域 B SDDC 的连接。SDDC
2. 双传输 VIF 可建立从本地到直接连接网关 (DXGW) 的冗余、弹性连接。
3. DXGW 与两个区域的 [AWS Transit Gateway](#) 相关联，以提供与[亚马逊 VPC](#) 的本地连接。

4. Transit Gateway 是一种区域虚拟路由器，能够使用 VPC 附件、VPN 附件、DXGW 附件和对等连接附件在与其连接的网络之间进行传递路由。
5. VPC 附件使 VPC 能够与连接到传输网关的其他 VPC 和网络建立通信。
6. Transit Gateway 对等连接支持连接到 Transit Gateway A 和公网网关 B 的网络之间的跨区域通信。
7. Transit Gateway VPN 附件启用 SDDC 与连接至相应区域中公网网关的网络之间的通信。但是，VMwareVMkernel 流量（包括ESXi管理和vSphere复制流量）优先于私有 VIF 流量，因此 VPN 附件无法用于此流量。vMotion确保 VPN 不会获知私有 VIF 使用的本地路由。

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。	2022 年 3 月 10 日
初次发布	参考架构图首次发布。	2022 年 3 月 10 日
初次发布	参考架构图首次发布。	2022 年 3 月 10 日
初次发布	参考架构图首次发布。	2022 年 3 月 10 日

 Note

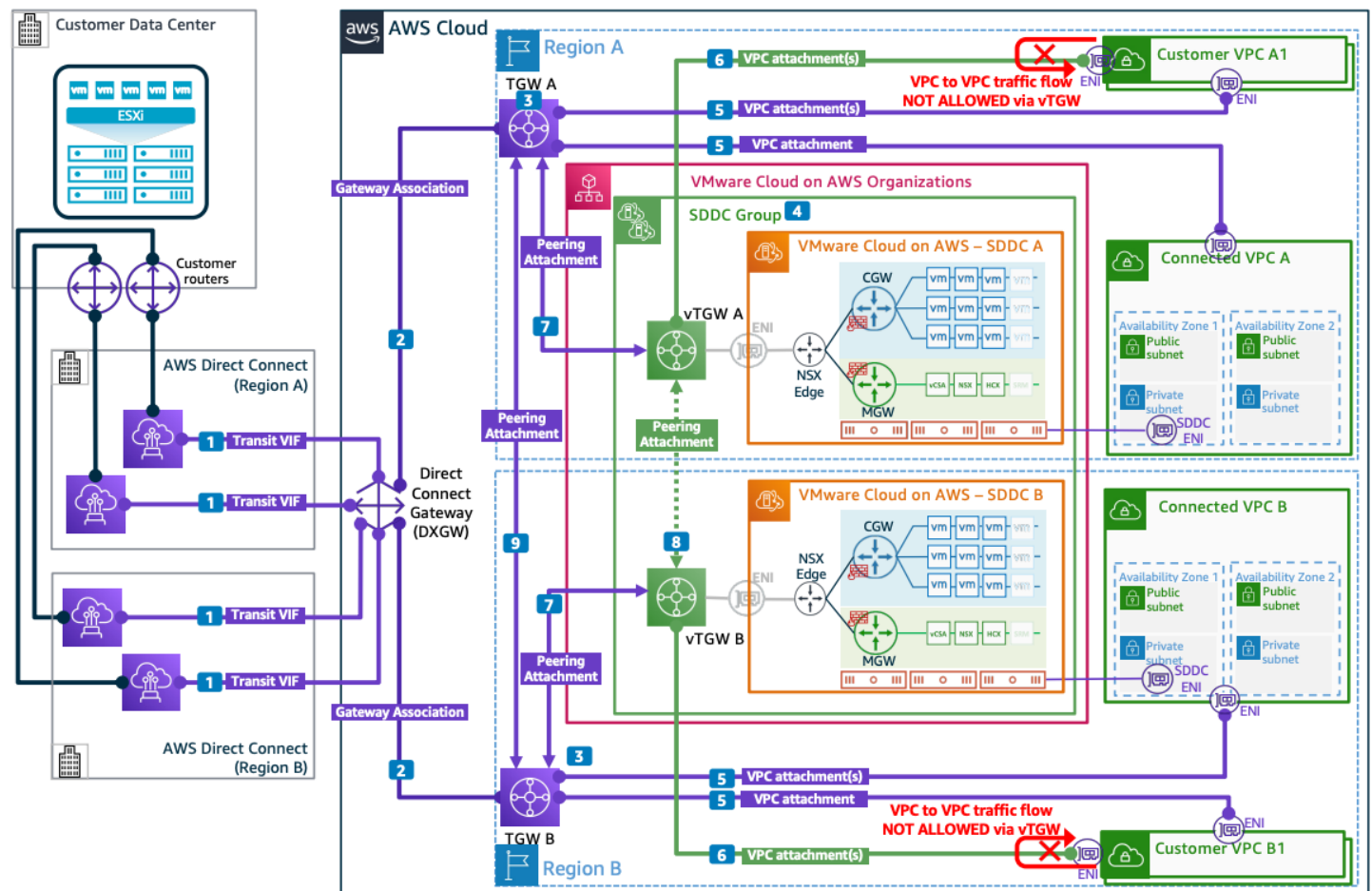
要订阅 RSS 更新，必须为正在使用的浏览器启用 RSS 插件。

通过 AWS Transit Gateway 实现高弹性 On-Premises 连接 VMware 公交连接

发布日期：2022年 3月10日 ([图表历史](#))

该架构显示了高弹性的本地连接，可以VMware Cloud on AWS使用 AWS Direct Connect、Direct Connect 网关、AWS Transit Gateway 和 VMware Transit Connect (vTGW) 在 SDDC 组中的 SDDC 之间进行高带宽、低延迟的连接。

具有高弹性的连接 VMware 公交连接架构



以下编号的项目描述了该架构中的关键组件：

1. 来自不同区域的两个独立 [AWS Direct Connect](#) 实例的传输虚拟接口 (VIF) 用于建立与区域 A 和 AWS 区域 B 的弹性和容错连接。
2. DXGW 与每个区域的 [AWS Transit Gateway](#) (TGW) 实例相关联，以提供本地连接。

3. AWS Transit Gateway 是一种区域性虚拟路由器，能够在连接到 VPC、VPN、对等连接附件和 DXGW 关联的网络之间进行传递路由。
4. SDDC 组使用 T VMware ransit Connect (vTGW) 在 SDDC 组中的 SDDC、SDDC 和附加的 VPC 以及 SDDC 之间通过 DXGW 提供高带宽、低延迟的连接。
5. [Amazon VPC](#) 附件使 VPC 能够与连接到传输网关的其他 VPC 和网络建立通信。或者，VPC 与 T VMware ransit Connect (vTGW) 的连接允许 VPC 仅与连接到同一 vtGW 的 SDDC 网络建立通信。
6. 外部 TGW 对等连接附件支持SDDC网络和连接到 TGW 的网络之间的通信。
7. 跨区域 T VMware ransit Connect 对等仅支持连接到 vtGW A 和 vtGW B 的 SDDC 网络之间的通信。
8. 跨区域 AWS Transit Gateway 对等连接附件支持连接到 TGW A 和 TGW B 的网络之间的通信。

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。	2022 年 3 月 10 日
初次发布	参考架构图首次发布。	2022 年 3 月 10 日
初次发布	参考架构图首次发布。	2022 年 3 月 10 日
初次发布	参考架构图首次发布。	2022 年 3 月 10 日

Note

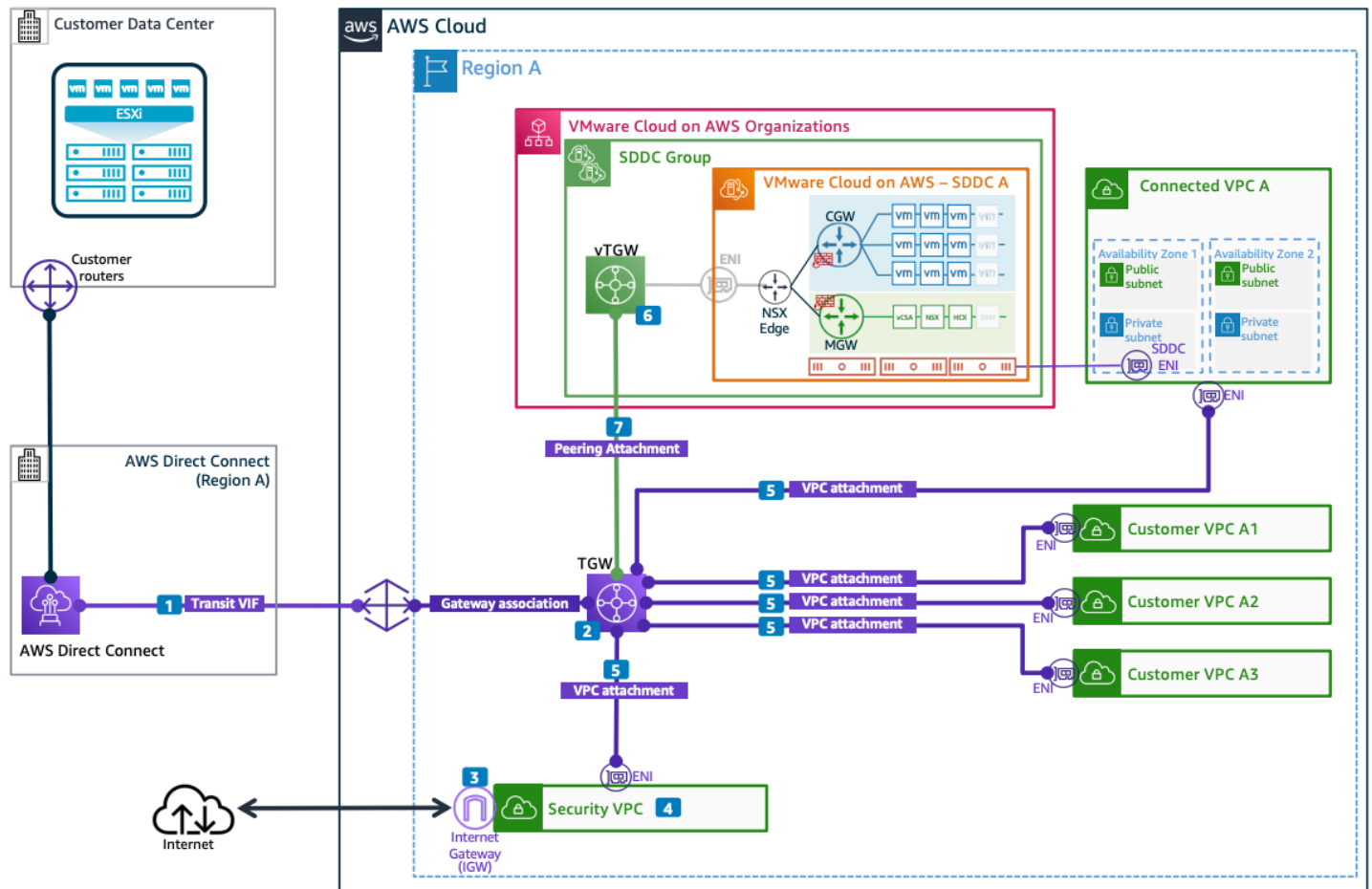
要订阅 RSS 更新，必须为正在使用的浏览器启用 RSS 插件。

使用安全 VPC 进行检查 SDDC 交通

发布日期：2022年 3月10日 ([图表历史](#))

此架构展示了如何使用安全 [Amazon VPC](#) 来检查南北互联网到 SDDC 的流量、VPC-to-SDDC 流量以及本地到 SDDC 的流量。VMware Cloud on AWS安全 VPC 可以使用第三方防火墙 AWS Network Firewall 进行配置，以进行SDDC出入流量检查和边界安全。

安全 VPC 检查 VMware Cloud on AWS 交通架构



以下编号的项目描述了该架构中的关键组件：

1. 通过 [AWS Direct Connect](#) 实例传输的 VIF 用于连接与 AWS 传输网关 (TGW) 实例关联的 [AWS Direct Connect 网关](#) (DXGW)，以完成与本地的连接。AWS 区域
2. 传输网关 (TGW) 是一种区域虚拟路由器，能够在网络之间进行传递路由。TGW 能够将所有来自本地的传入流量重定向到安全 VPC。

3. 互联网网关 (IGW) 是一个 VPC 组件，为 AWS 工作负载提供集中式互联网接入。
4. 安全 VPC 可以使用第三方防火墙 AWS Network Firewall 进行配置，以进行 SDDC 出入流量检查和边界安全。
5. VPC 附件用于连接到一个或多个分支 VPC。分支 VPC 和 SDDC s 之间的流量始终通过安全 VPC 传输。
6. SDDC 组使用 VMware Transit Connect (vTGW) 在 SDDC 组中的 SDDC、SDDC 和附加的 VPC 以及 SDDC 之间通过 DXGW 提供高带宽、低延迟的连接。
7. 外部 TGW 对等连接可确保所有 SDDC 入口和出站流量都通过安全 VPC 传输。这包括 AWS VPC 流量、本地流量和互联网流量。

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。	2022 年 3 月 10 日
初次发布	参考架构图首次发布。	2022 年 3 月 10 日
初次发布	参考架构图首次发布。	2022 年 3 月 10 日
初次发布	参考架构图首次发布。	2022 年 3 月 10 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。