AWS 白皮书

混合连接

混合连接: AWS 白皮书

Table of Contents

混合连接

发布日期：2023 年 7 月 6 日 (文档修订)

许多组织需要将本地数据中心、远程站点和云连接起来。混合网络连接这些不同的环境。本白皮书介绍了 AWS 构建模块以及在决定哪种混合连接模式适合您时需要考虑的关键要求。为了帮助您确定满足您的业务和技术要求的最佳解决方案，我们提供了决策树，指导您完成合理的选择过程。

简介

现代组织使用大量的 IT 资源。过去，通常将这些资源托管在本地数据中心或主机托管设施中。随着云计算应用的普及，组织通过网络连接从云服务提供商处交付和使用 IT 资源。组织可以选择将部分或全部现有 IT 资源迁移到云。无论哪种情况，都需要使用公共网络来连接本地资源和云资源。本地资源和云资源共存称为混合云，将它们连接起来的公共网络称为混合网络。即使您的组织将所有 IT 资源都放在云中，它可能仍然需要与远程站点进行混合连接。

有多种连接模式可供选择。虽然有了备选方案会增加灵活性，但选择最佳方案需要对业务和技术要求进行分析，并剔除不合适的方案。您可以根据安全性、部署时间、性能、可靠性、通信模式、可扩展性等方面的注意事项将需求分组。在仔细收集、分析和考虑需求后，网络和云架构师就可以确定适用的 AWS 混合网络构建块和解决方案。为了确定和选择一个或多个最佳模式，架构师必须了解每种模式的优缺点。此外，还有一些技术限制可能会导致原本合适的模式被排除在外。

为了简化选择过程，本白皮书将按照逻辑顺序为您介绍每个关键注意事项。每个注意事项下都有用于收集要求的问题。确定每个设计决策的影响，以及潜在的解决方案。白皮书介绍了一些注意事项的决策树，以此作为辅助决策过程、排除选项和了解每个决策后果的方法。最后介绍了一个混合用例的场景，应用了端到端连接模式的选择和设计。您可以使用本示例了解如何在实际示例中执行本白皮书中规定的流程。

本白皮书旨在帮助您选择和设计最佳混合连接模式。本白皮书的结构如下：

- 混合连接构建块——用于混合连接的 AWS 服务概述。
- 连接选择和设计注意事项——每种连接模式的定义、每种模式对设计决策的影响、需求识别问题、解决方案和决策树。
- 客户用例——举例说明如何在实践中应用注意事项和决策树。

您的架构是否良好？

当您在云端构建系统时，AWS Well-Architected Framework 可助您了解所作决策的利弊。利用此框架的六个支柱，您可以了解到设计和运行可靠、安全、高效、经济有效且可持续的系统的架构最佳实践。您可以使用 AWS Management Console 免费提供的 AWS Well-Architected Tool，回答与每个支柱相关的一组问题，即可根据这些最佳实践检查自己的工作负载。

有关云架构的更多专家指导和最佳实践（参考架构部署、图表和白皮书），请参阅 AWS 架构中心。

AWS 混合连接构建模块

混合网络连接架构有三个组成部分：

- 混合网络连接：AWS 连接服务与本地客户网关设备之间的连接类型。
- AWS 混合连接服务：在客户基础设施和 AWS 之间提供连接和路由的 AWS 服务。
- 本地客户网关设备：客户现有网络内的设备，作为混合网络连接的本地端点。不同的连接类型对这些设备有不同的技术要求，下文将对此进行讨论。

混合网络连接

有几种方法可以在本地设备和 AWS 之间建立连接。本白皮书重点介绍了如何将这些不同的方式结合到整体架构中，但也提供了不同选项（AWS Direct Connect、站点到站点虚拟专用网络和中转网关连接）的简要概述。

AWS Direct Connect

AWS Direct Connect 是一种从本地到 AWS 之间建立专用网络连接的服务。有关详细信息，请参阅 AWS Direct Connect。

有两种类型的 AWS Direct Connect 连接：专用连接和托管连接。专用连接是 AWS 设备与您的本地设备之间的直接链接，而托管连接则由可以为您处理连接详细信息的 AWS 合作伙伴提供支持。有关更多信息，请参阅AWS Direct Connect 连接。

Direct Connect 连接使用虚拟接口 (VIF) 来隔离不同的流量。多个 VIF 可使用同一 Direct Connect 链路，并用 VLAN (802.1q) 标签隔开。有三种类型的 VIF 可提供与 AWS 网络的连接。有关更多详细信息，请参阅AWS Direct Connect 虚拟接口。三种类型是：

- 专用 VIF：专用 VIF 是您的设备与 AWS 内部资源之间的专用连接。这些终端在 AWS 内部直接连接到虚拟专用网关 (VGW)（支持单个 VPC），或通过 Direct Connect 连接到多个 VGW。
- 公共 VIF：公共 VIF 允许连接任何公共 AWS 资源，例如 S3、DynamoDB 和公共 EC2 IP 范围。虽然公共 VIF 不能直接访问互联网，但任何 Amazon 公共资源都可以访问它（包括其他客户的公共 EC2 实例），客户在进行安全规划时应考虑到这一点。
- Transit VIF：Transit VIF 是通过 Direct Connect 网关在您的设备和 AWS Transit Gateway 之间建立的专用连接。现在，速度低于 1 Gbps 的链路也支持 Transit VIF，详情请参阅发布公告。

> **Note**
>
> 托管虚拟接口 (Hosted VIF) 是专用 VIF 的一种类型，在这种类型中，VIF 被分配给不同的 AWS 账户 ，而不是拥有 AWS Direct Connect 连接的 AWS 账户（可以包括 AWS Direct Connect 合作伙伴）。AWS 不再允许新的合作伙伴提供这种模式。有关更多信息，请参阅创建托管虚拟接口。

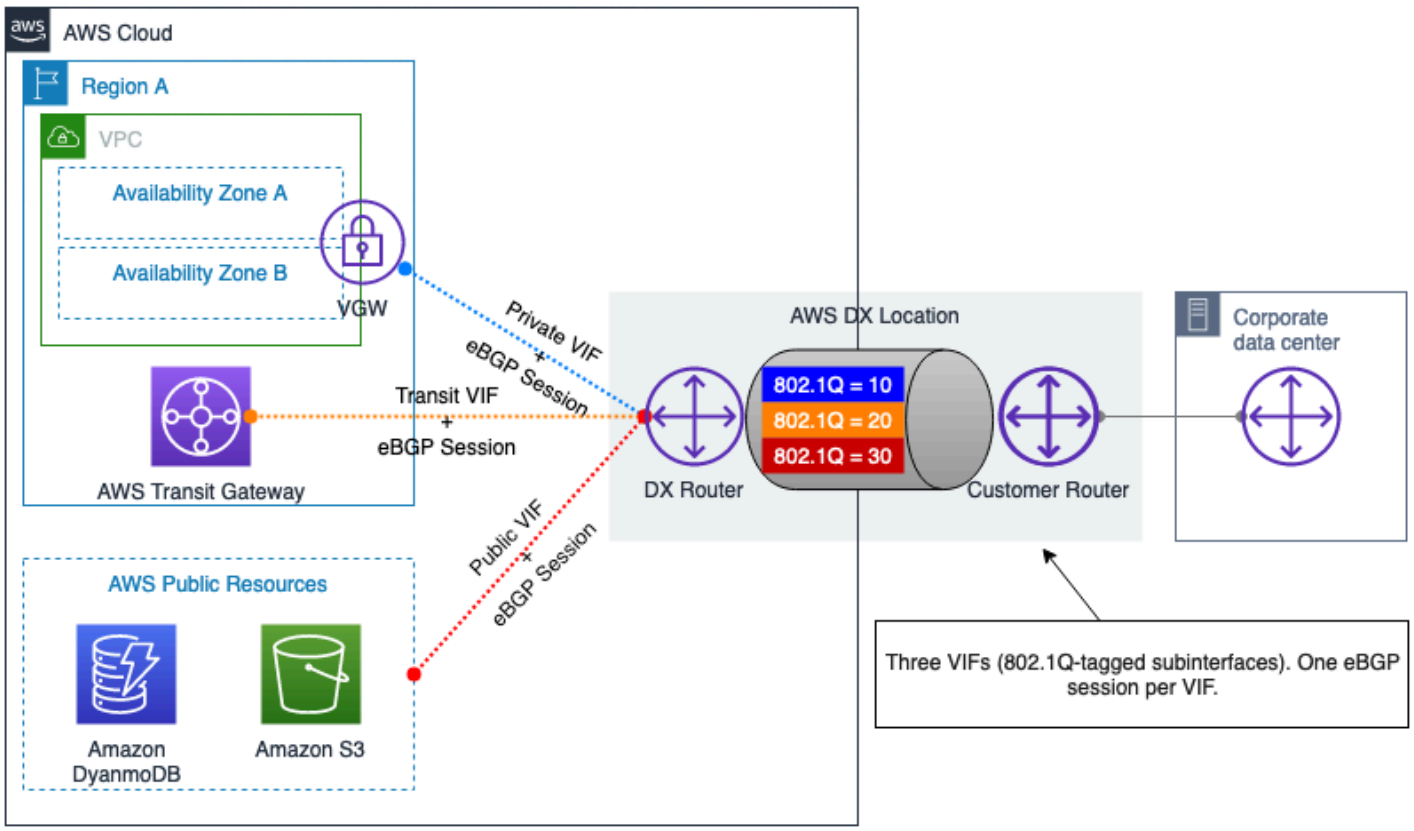

图 1——AWS Direct Connect 专用和公共 VIF

Site-to-Site 虚拟专用网络 (VPN)

Site-to-Site VPN 使两个网络能够安全地通信，并且可以通过不受信任的传输方式使用，例如互联网。客户可以通过两种方式在本地站点和 Amazon Virtual Private Cloud (Amazon VPC)之间建立 VPN 连接：

- AWS 托管式 Site-to-Site VPN (AWS S2S VPN)：这是一种使用 IPsec 的完全托管且高度可用的 VPN 服务。有关更多信息，请参阅什么是 AWS Site-to-Site VPN。您可以选择为站点到站点 VPN 连接启用加速。有关更多信息，请参阅加速的 Site-to-Site VPN 连接。S2S VPN 还可以使用 Direct

Connect 中转 VIF 来避免流量通过互联网，从而降低成本并允许使用专用 IP 地址。有关详细信息，请参阅带 AWS Direct Connect 的专用 IP VPN。

- 软件站 Site-to-Site VPN（客户托管的 VPN）：使用此 VPN 连接选项，您负责配置和管理整个 VPN 解决方案，通常是在 EC2 实例上运行 VPN 软件。有关更多信息，请参阅软件 Site-to-Site VPN。

这两个选项都需要客户网关设备的支持才能终止 VPN 隧道的本地端。该设备可以是物理设备，也可以是软件设备。有关经 AWS 测试的网络设备的更多信息，请参阅已测试的客户网关设备列表。

Transit Gateway Connect (TGW Connect)

Transit Gateway Connect 在 AWS Transit Gateway 和本地网关设备之间使用 GRE 隧道。在 TGW Connect 上使用 BGP 可实现动态路由选择。请注意，TGW Connect 未加密。有关更多信息，请参阅 Transit Gateway Connect。

AWS 混合连接服务

AWS 混合连接服务提供高度可扩展、高度可用的网络组件。它们在构建混合网络解决方案方面发挥着至关重要的作用。在撰写本白皮书时，主要有三种服务端点：

- AWS 虚拟专用网关 (VGW)是一项区域性、高度冗余的服务，可在 VPC 级别提供 IP 路由和转发，充当 VPC 与您的客户网关设备通信的网关。VGW 可以终止 AWS S2S VPN 连接和 AWS Direct Connect 专用 VIF。
- AWS Transit Gateway(TGW) 是一种区域性、高度可用且可扩展性的服务，可让您使用单个集中式网关，通过 Site-to-Site VPN 和/或 Direct Connect 将多个 VPC 相互连接，并将您的本地网络连接起来。从概念上讲，AWS Transit Gateway 可以充当高度可用且冗余的虚拟云路由器。AWS Transit Gateway 支持通过多个 Direct Connect 连接、VPN 隧道或 TGW Connect 对等体进行等价多路径 (ECMP) 路由选择。Transit Gateways 可以在同一区域和跨区域内相互对等，从而允许其连接的资源通过对等链路进行通信。有关更多详细信息，请参阅 AWS Transit Gateway 场景。
- AWS Cloud WAN 提供了一个中央控制面板，只需点击几下，即可在分支机构、数据中心和 Amazon VPC 之间建立连接，构建全球网络。您可以使用网络策略在一个位置自动执行网络管理和安全任务。有关更多详细信息，请参阅 AWS Cloud WAN 文档。
- Direct Connect Gateway (DXGW) 是一种全局可用的服务，在其连接中分发路由信息，其行为类似于传统网络中的 BGP 路由反射器。数据不通过 DXGW，它只处理路由信息。您可以在任何 AWS 区域 中创建 DXGW，然后从所有其他 AWS 区域 中访问它。您可以将 Direct Connect VIF 连接到 DXGW，然后将 DXGW 与 vGW（使用专用 VIF）或 AWS Transit Gateway（使用 Transit VIF）关联。有关更多信息，请参阅 Direct Connect 网关。由于 DXGW 是全局可用的服务，因此无需为冗余

创建多个 DxGW。但是，您可能会选择使用多个 DXGW 来分隔路由域，例如，您希望将生产网络和测试网络完全隔离。

混合连接类型和设计注意事项

白皮书的这一部分涵盖了在选择混合网络将本地环境连接到 AWS 时影响您选择的注意事项。它遵循逻辑思维过程，为您选择最佳混合连接解决方案提供支持。影响设计的注意事项分为影响连接类型的注意事项和影响连接设计的注意事项。连接类型注意事项将有助于您决定使用基于互联网的 VPN 还是 Direct Connect。连接设计注意事项将有助于您决定如何设置连接。

以下是影响连接类型的注意事项：部署时间、安全性、SLA、性能和成本。在了解了这些注意事项以及它们对设计选择的影响后，您就可以决定是否建议使用基于互联网的连接或 Direct Connect 来满足您的需求。

其中包括以下影响连接设计的注意事项：可扩展性、通信模式、可靠性和第三方 SD-WAN 集成。在了解了这些注意事项以及它们对设计选择的影响后，您就能决定推荐的最佳逻辑设计，以满足您的要求。

以下结构用于讨论和分析每个选择和设计注意事项：

- 定义——对注意事项的简要定义。
- 关键问题——提供一组问题，使您能够收集与注意事项相关的要求。
- 需要考虑的功能——满足与注意事项相关的要求的解决方案。
- 决策树——出于某些注意事项或一组注意事项，提供了决策树来帮助您选择最佳的混合网络解决方案。

影响混合网络设计的注意事项按顺序介绍，其中一个注意事项的输出是后续注意事项输入的一部分。如图 2 所示，第一步是确定连接类型，然后根据设计选择注意事项对其进行完善。

图 2 显示了两个注意事项类别、个别注意事项以及后续小节中涵盖这些注意事项的逻辑顺序。这些就是在做出混合网络设计决策时的基本注意事项。如果目标设计不需要所有这些注意事项，您可以将重点放在适用于您要求的注意事项上。

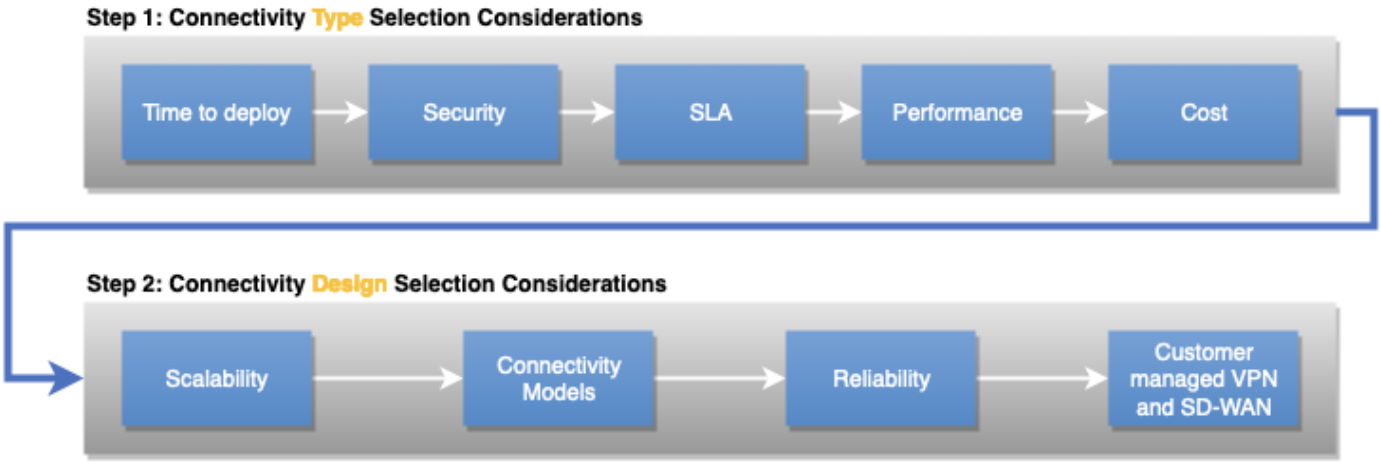

图 2——注意事项类别、个别注意事项以及它们之间的逻辑顺序

连接类型选择

这一部分介绍影响您为工作负载选择的连接类型的注意事项。其中包括部署时间、安全性、SLA、性能和费用。

注意事项

- 部署时间
- 安全性
- 服务水平协议 (SLA)
- 性能
- 费用

部署时间

定义

在为工作负载选择合适的连接类型时，部署时间可能是一个重要因素。根据连接类型和本地位置的不同，连接可在数小时内建立，但如果必须安装其他电路，则可能需要数周或数月的时间。这将影响您决定使用基于互联网的连接、私有专用连接或由 AWS Direct Connect 合作伙伴作为托管服务提供的私有托管连接。

关键问题

- 部署所需的时间是几小时、几天、几周还是几个月？
- 连接需要多长时间——是短期项目还是永久性基础设施？

需要考虑的功能

当您需要在数小时或数天内连接 AWS 时，则您很可能需要使用现有的网络连接。这通常意味着要通过公共互联网与 AWS 建立 VPN 连接。如果现有的 AWS DX 合作伙伴为您提供私有 AWS 连接，则可以在数小时内配置新的托管连接。

当您有几天到几周的时间时，您可以与 AWS Direct Connect 合作伙伴合作，与 AWS 建立私有连接。AWS Direct Connect合作伙伴可帮助您在 AWS Direct Connect 位置与您的数据中心、办公室或主机托管环境之间建立网络连接。某些 AWS Direct Connect 合作伙伴已获准提供 Direct Connect 托管连接。托管连接的配置速度通常比专用连接快。AWS Direct Connect合作伙伴将使用连接到 AWS 主干网的现有基础设施配置每个托管连接。

当您有几周到几个月的时间时，您可以研究与 AWS 建立专用的私有连接。服务提供商和 AWS Direct Connect 合作伙伴为 AWS Direct Connect 专用连接提供便利。服务提供商通常会在客户所在地安装网络设备，以促进 Direct Connect 专用连接。根据服务提供商、站点位置和其他物理因素的不同，Direct Connect 专用连接的安装可能需要几周到几个月的时间。

如果您的网络设备已经安装在 AWS Direct Connect 所在位置的同一个主机托管设施中，则可以通过主机代管站点的交叉连接快速建立 AWS Direct Connect 专用连接。在您请求连接后，AWS 会向您提供授权证书和连接设备分配 (LOA-CFA) 供您下载，或通过电子邮件向您请求更多信息。LOA-CFA 是用于连接到 AWS 的授权，您的网络提供商需要其来为您订购交叉连接。

表 1——费用效益比较

	基于互联网的连接	DX 专用连接（DX 所在位置内的现有设备）	DX 专用连接（全新）	DX 托管连接（DX 合作伙伴的现有端口）	DX 托管连接（全新）
预置时间	从几小时到几天	天	从几周到几个月	从几小时到几天	从几天到几周到几个月

> **Note**
>
> 提供的配置时间指南根据实际观察得出的，仅供参考。如果考虑到您的站点位置、与直接连接位置的距离以及已有的基础设施，所有这些都会影响配置时间。您的 AWS Direct Connect 合作伙伴将就确切的配置时间为您提供建议。

安全性

定义

安全性要求将影响您的混合连接类型。这些注意事项包括：

- 传输类型——互联网或专用网络连接
- 加密要求

关键问题

- 您的安全要求和政策是否允许通过互联网使用加密连接来连接 AWS，还是强制使用专用网络连接？
- 利用专用网络连接时，网络层是否必须提供传输中加密？

技术解决方案

您的安全性要求和策略可能允许使用互联网或要求在 AWS 和贵公司网络之间使用专用网络连接。它们还会影响网络是否必须提供传输中加密，或者是否可以接受在应用层执行加密的决定。

如果您可以利用互联网，则 AWS Site-to-Site VPN 可以用于通过互联网在您的网络与 Amazon VPC 或 AWS Transit Gateway 之间创建加密隧道。如果您正在利用基于互联网的连接，也可以选择将 SD-WAN 解决方案扩展到互联网上的 AWS。本白皮书后面的客户托管 VPN 和 SD-WAN 部分介绍了 SD-WAN 的具体注意事项。

如果您需要在 AWS 和公司网络之间建立专用网络连接，则 AWS 建议您使用 AWS Direct Connect 专用连接或托管连接。如果需要通过专用网络连接进行传输中加密，则应通过 Direct Connect（通过公共 VIF 或传输 VIF）建立 VPN，或考虑在 10Gbps 或 100Gbps 专用连接上使用 MACsec。

表 2——汽车公司连接类型要求示例

	Site-to-Site VPN	Direct Connect
传输	互联网	专用网络连接
传输中加密	是	需要通过 DX 的 S2S VPN、通过中转 VIF 的 S2S VPN，或者在 10Gbps 或 100Gbps 的专用连接上使用 MacSec

服务水平协议 (SLA)

定义

企业组织通常要求服务提供商为组织使用的每项服务履行 SLA。该组织反过来在此基础上构建自己的服务，并为自己的使用者提供 SLA。SLA 非常重要，因为它描述了服务的提供和运行方式，并且通常包括具体的可衡量特征，例如可用性。如果服务违反了定义的 SLA，服务提供商通常会提供协议中规定的经济补偿。SLA 定义了计量标准的类型、要求和计量期。例如，请参阅 AWS Direct Connect SLA 下的正常运行时间目标定义。

关键问题

- 是否需要包含服务积分的混合连接 SLA？
- 整个混合网络是否需要遵守正常运行时间目标？

需要考虑的功能

连接类型：互联网连接可能无法预测。虽然 AWS 要非常谨慎地与各种互联网服务提供商建立多种链接，但互联网的管理根本不在 AWS 或单个提供商的管理范围之内。一旦流量离开其网络边界，云提供商所能进行的路由工程和流量影响就非常有限。也就是说，有一个 AWS Site-to-Site VPN SLA 为 AWS Site-to-Site VPN 端点提供可用性目标。

AWS Direct Connect 提供正式的 SLA，其服务积分按照您在未满足 SLA 的每月账单周期内为出现不可用情况的适用连接所支付的端口小时费用总额的一定百分比计算。如果需要 SLA，建议使用这种传输方式。AWS Direct Connect 列出了每个正常运行时间目标的具体最低配置要求，例如 AWS Direct Connect 位置数量、连接数量和其他配置详细信息。未满足要求意味着，如果服务违反了规定的 SLA，就不能提供服务积分。

重要的是，即使为提供混合连接而选择的服务配置满足 SLA 要求，网络的其余部分也可能无法提供相同水平的 SLA。AWS 责任在 AWS Direct Connect 端口的 AWS Direct Connect 所在位置结束。一旦 AWS 将流量移交给贵组织的网络，就不再是 AWS 的责任。如果您在 AWS 和本地网络之间使用服务提供商，则连接性取决于您和服务提供商之间的 SLA（如适用）。请记住，在设计混合连接时，整个混合网络和其中最薄弱的部分一样好。

AWS Direct Connect 合作伙伴提供 AWS Direct Connect 连接。合作伙伴可以根据其提供的产品提供 SLA 和服务积分，直至与 AWS 的分界点。应直接与 APN 合作伙伴一起评估和进一步研究该方案。AWS 发布经过验证的交付合作伙伴名单。

逻辑设计：除了连接类型外，您还必须考虑其他构件作为整体设计的一部分。举个例子，与 AWS S2S VPN 一样，AWS Transit Gateway 也有自己的 SLA。出于安全考虑，您可能会使用 AWS Transit Gateway 来扩大规模并使用 AWS S2S VPN，但您必须以符合各 SLA 的方式进行设计，才有资格获得每项相应服务的服务积分。

查看 AWS Direct Connect 故障恢复能力建议和故障恢复能力工具包。

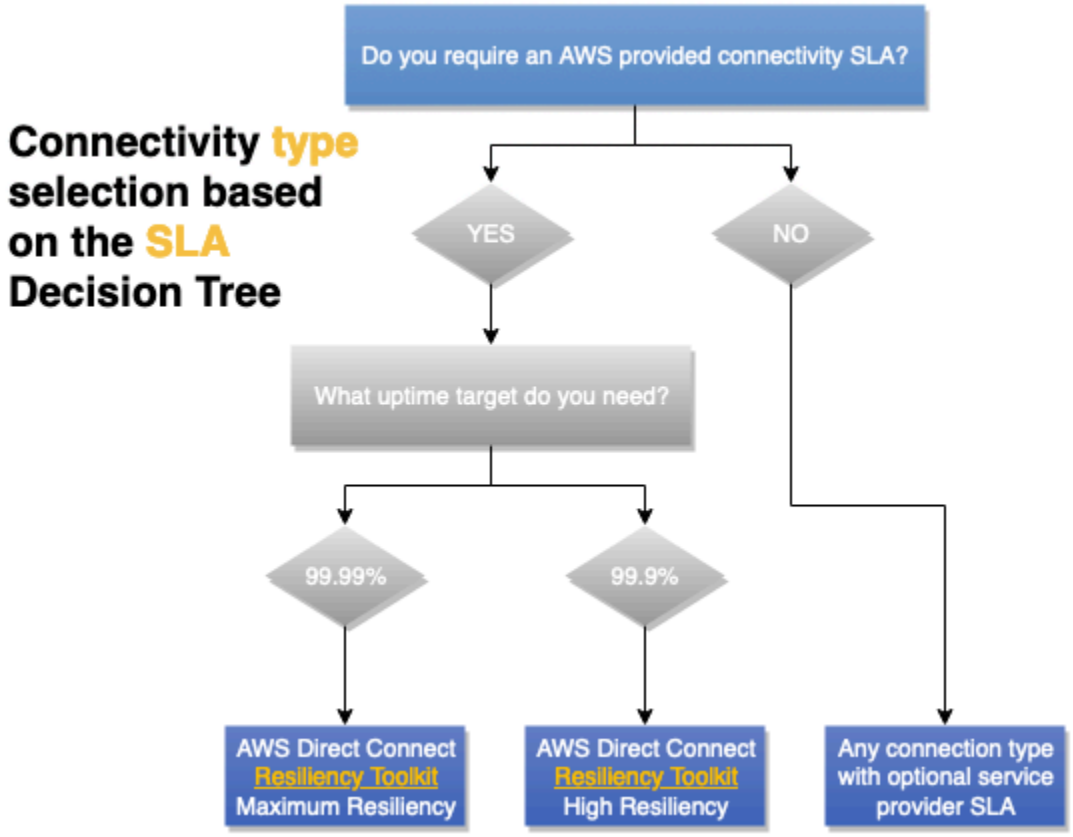

图 3——SLA 注意事项决策树

性能

定义

影响网络性能的因素有很多，例如延迟、数据包丢失、抖动和带宽。根据应用要求的不同，这些因素的重要性也各不相同。

关键问题

根据您的应用需求，您需要确定影响应用行为和用户体验的网络性能因素，并确定其优先顺序。

带宽

带宽是指连接的数据传输速率，通常以每秒位数 (bps) 为单位。每秒兆位 (Mbps) 和每秒千兆位 (Gbps) 是常见的扩展比例，其基数为10（每秒 100 万位 = 1 Mbps），而其他地方基数则为 2（2^10）。

在评估应用的带宽需求时，请记住带宽需求会随着时间的推移而变化。云端的初始部署、正常操作、新的工作负载和失效转移场景都可能有不同的带宽要求。

应用可能有自身的带宽注意事项。有些应用可能需要通过高带宽连接实现确定性性能，而另一些应用可能需要确定性性能和高带宽。如果应用达到每个流量带宽限制，则可能需要特殊配置才能并行使用多个流量流（有时称为流或套接字），从而允许使用更多的连接带宽。由于隧道开销、较低的 MTU 限制或硬件带宽限制，VPN 可能会限制吞吐量。

延迟

延迟是指数据包通过网络连接从源到目的地所需的时间，通常以毫秒 (ms) 为单位，低延迟要求有时以微秒 (µs) 为单位。延迟是光速的函数，因此延迟会随着距离的增加而增加。

应用延迟要求可以采取不同的形式。高度交互式应用（例如虚拟桌面）的目标延迟时间可以从用户执行输入操作到用户看到虚拟桌面对该输入做出反应的时间段来衡量。IP 语音 (VoIP) 应用也有类似的要求。需要考虑的第二类工作负载是事务性很强的工作负载，它们需要服务器做出响应后才能继续工作。网络延迟的增加可能会严重影响数据库或其他形式的密钥/值存储。

抖动

抖动衡量网络延迟的一致性，与延迟一样，通常以毫秒 (ms) 为单位。

应用抖动要求通常出现在实时流媒体应用中，包括视频和语音传输。这些应用往往要求其数据流具有一致的速率和延迟，并使用较小的缓冲区来校正少量的抖动。

数据包丢失

数据包丢失测量的是未传送网络流量的百分比。由于高流量暴增、容量下降、网络设备故障和其他原因，所有网络有时都会出现一定程度的数据包丢失。因此，应用必须对数据包丢失有一定的容忍度，但是，不同的应用对数据包丢失的容忍度可能有所不同。

使用 TCP 传输其流量的应用能够通过重新传输来纠正数据包丢失。在 IP 基础上使用 UDP 或自己的协议的应用需要实施自己的方法来处理数据包丢失，而且可能对数据包丢失非常敏感。IP 语音应用可能只是在发生数据包丢失的调用部分插入静音，而不是尝试重新传输。一些 VPN 解决方案包含自己的机制，用于在其用于传输流量的网络上恢复数据包丢失。

需要考虑的功能

当需要可预测的延迟和吞吐量时，建议选择 AWS Direct Connect，因为它能提供确定的性能。可根据吞吐量要求选择带宽。如果需要比互联网连接更稳定的网络体验，AWS 建议使用 AWS Direct Connect。私有 VIF 和中转 VIF 支持巨型帧，这可以减少通过网络的数据包数量，并且可以减少开销，从而提高吞吐量。AWS Direct ConnectSiteLink 允许使用 AWS 主干网提供各位置之间的连接，并且可以根据需要启用。选择 Direct Connect 带宽时应考虑用于 SiteLink 的带宽。

通过 AWS Direct Connect 使用 VPN 可增加加密功能。但是，它会减小 MTU 的大小，这可能会降低吞吐量。 AWS 托管 Site-to-Site (S2S) VPN 功能可在 AWS Site-to-Site VPN 文档中找到。如果通过连接加密是主要的加密要求，许多 Direct Connection 位置都支持 MACsec。MACsec 与 Site-to-Site VPN 连接的 MTU 或潜在吞吐量注意事项不同。AWS Transit Gateway 允许客户横向扩展 VPN 连接的数量，并通过等价多路径路由 (ECMP) 提高相应的吞吐量。AWS 的托管 Site-to-Site VPN 支持使用 Direct Connect 中转 VIF 进行私有连接，详情请参阅使用 AWS Direct Connect 的专用 IP VPN。

另一种选择是通过互联网使用 AWS 托管的 Site-to-Site VPN。由于费用低廉，供应广泛，它可能是一个有吸引力的选择。但是，请记住，通过互联网提高性能是尽力而为。互联网天气事件、拥堵和延迟时间的增加都是不可预测的。AWS 通过 AWS 加速 S2S VPN 提供了一种解决方案，可以减轻使用互联网路径的一些弊端。加速 S2S VPN 使用 AWS 全球加速器，允许 VPN 流量尽早进入 AWS 网络，并尽可能靠近客户网关设备。这样就能利用不拥堵的 AWS 全局网络优化网络路径，将流量路由到能提供最佳性能的端点。您可以使用加速 VPN 连接来避免通过公共 Internet 路由流量时可能发生的网络中断。

费用

定义

在云中，混合连接的费用包括配置的资源和使用的费用。配置资源的费用以时间单位计量，通常是每小时。使用量通常用于数据传输和处理，通常以千兆字节 (GB) 为单位。其他费用包括与 AWS 网络接入

点的连接费用。如果您的网络位于同一个主机托管设施内，则可能只需支付交叉连接的费用。如果您的网络位于其他位置，则需要支付服务提供商或 APN Direct Connect 合作伙伴的费用。

关键问题

- 您预计每月从您的设施和互联网向 AWS 发送多少数据？
- 您预计每月从 AWS 向您的设施和互联网发送多少数据？
- 这些金额多久会变化？
- 故障场景会发生什么变化？

需要考虑的功能

如果您希望在 AWS 上运行带宽较高的工作负载，则 AWS Direct Connect 可以通过两种方式降低进出 AWS 的网络费用。首先，通过直接在 AWS 之间传输数据，可以减少向网络服务提供商支付的带宽费用。其次，通过专用连接传输的所有数据均按优惠 AWS Direct Connect 数据传输速率收费，而不是按互联网数据传输速率收费——详情请参阅直接连接定价页面。

AWS Direct Connect 允许使用 AWS Direct Connect SiteLink，通过 AWS 主干网实现站点互联——有关更多信息，请参阅 SiteLink 发布博客。利用这一功能需要支付正常的 Direct Connect 数据传输费用，以及每小时启用 SiteLink 的费用。您可以按需启用或禁用 SiteLink，对于涉及互联网或专用网络连接的故障场景，这可能是一个不错的选择。

如果您使用网络服务提供商在本地和 Direct Connect 位置之间建立连接，则更改带宽承诺所需的能力和时间取决于您与服务提供商签订的合同。

AWS 主干网可以将您的流量从任何 AWS 网络接入点传送到除中国以外的任何 AWS 区域。与使用互联网访问远程 AWS 区域 相比，这种功能具有许多技术优势，但也需要支付费用，详情请参阅 EC2 数据传输定价页面。如果流量路径中存在 AWS Transit Gateway，则会增加每 GB 的数据处理费用，但如果在两个 Transit Gateway 之间使用区域间对等互联，则只需支付一次 Transit Gateway 数据处理费用。

最佳的应用设计可将数据处理控制在 AWS 范围内，并将不必要的数据输出费用降至最低。向 AWS 输入数据是免费的。

> **Note**
>
> 作为整体连接解决方案的一部分，除 AWS 连接费用外，还应考虑端到端连接费用，包括服务提供商费用、交叉连接、机架和 DX 位置内的设备（如需要）。

如果您不确定应该使用互联网还是私有连接，请计算一个盈亏平衡点，在该点上，AWS Direct Connect 的费用会比使用互联网便宜。如果数据量意味着 AWS Direct Connect 的费用较低，而您又需要永久连接，则 AWS Direct Connect 就是最佳的连接选择。

如果连接是临时性的，而且互联网满足其他要求，则由于互联网的弹性，在互联网上使用 AWS S2S VPN 可能会更便宜。请注意，这需要您的本地网络获得足够的互联网连接。

如果您所在的设施有 AWS Direct Connect（列表可在 Direct Connect 网站上获取），则您可以与 AWS 建立交叉连接。这意味着要使用 1、10 或 100Gbps 的专用连接。AWS Direct Connect 合作伙伴提供更多带宽选择和更小的容量，可优化您的连接费用。例如，您可以从 50 Mbps 的托管连接开始，而不是从 1 Gbps 的专用连接开始。

使用 AWS Transit Gateway，您可以与许多 VPC 共享您的 VPN 和 Direct Connect 连接。虽然要根据每小时连接 AWS Transit Gateway 的次数和流经 AWS Transit Gateway 的流量付费，但它简化了管理，减少了所需的 VPN 连接和 VIF 数量。降低运营开销所带来的好处和费用节约很容易就能超过数据处理的额外费用。您也可以考虑这样的设计，即 AWS Transit Gateway 位于大多数 VPC 的流量路径中，而不是所有 VPC 的流量路径中。这种方法可以避免在需要将大量数据传输到 AWS 的用例中产生的 AWS Transit Gateway 数据处理费用。有关该设计的更多详细信息，请参阅“连接模型”部分。另一种方法是将 AWS Direct Connect 作为主路径与通过互联网的 AWS S2S VPN 作为备份/失效转移路径相结合。虽然这种解决方案在技术上可行，成本效益也很高，但它也有技术上的缺点（在本白皮书的“可靠性”部分进行了讨论），而且可能更难管理。AWS不建议将这种方法用于高度关键或关键的工作负载。

最后一种方法是在 Amazon EC2 实例中部署客户托管的 VPN 或 SD-WAN。与 AWS S2S VPN 相比，如果有数十到数百个站点，则在规模上可能会更便宜。但是，需要考虑每个虚拟设备的管理开销、许可费用和 EC2 资源费用。

决策矩阵

表 3——汽车公司连接设计输入示例

类别	客户托管的 VPN 或 SD-WAN	AWS S2S VPN	AWS 加速 S2S VPN	AWS Direct Connect 托管连接	AWS Direct Connect 专用连接
需要互联网连接	是	是	是	否	否

类别	客户托管的 VPN 或 SD-WAN	AWS S2S VPN	AWS 加速 S2S VPN	AWS Direct Connect 托管连接	AWS Direct Connect 专用连接
配置资源费用	EC2 实例和软件许可	AWS S2S VPN	AWS S2S VPN 和 AWS 全球加速器	适用的容量占端口费用的比例	专用端口费用
数据传输费用	互联网费率	互联网费率或 Direct Connect 费率	带数据传输高级功能的互联网	Direct Connect 费率	Direct Connect 费率
Transit Gateway	可选	可选	必填	可选	可选
AWS 数据处理费用	不适用	仅带有 AWS Transit Gateway	是	仅带有 AWS Transit Gateway	仅带有 AWS Transit Gateway
是否可以在 AWS Direct Connect 上使用？	是	是	否	不适用	不适用

连接设计选择

白皮书的这一部分介绍了影响连接设计选择的注意事项。连接设计包括逻辑方面以及如何设计和优化混合连接的可靠性。

将介绍以下注意事项：可扩展性、连接模型、可靠性以及客户托管的 VPN 和 SD-WAN。

注意事项

- 可扩展性
- 连接模型
- 可靠性
- 客户托管的 VPN 和 SD-WAN

可扩展性

定义

可扩展性是指连接解决方案能够随着时间的推移、需求的变化而增长和发展。

在设计解决方案时，您需要考虑当前的规模以及预期的增长。这种增长可能是有机增长，也可能与快速扩张有关，例如并购类型的情况。

注意：根据目标解决方案架构的不同，并非所有上述元素都需要考虑在内。但是，它们可以作为确定最常见混合网络解决方案的可扩展性要求的基础要素。本白皮书重点介绍混合连接的选择和设计。建议同时考虑与 VPC 网络架构相关的混合连接规模。有关更多信息，请参阅《构建可扩展且安全的多 VPC AWS 网络基础架构》白皮书。

关键问题

- 当前和预计需要连接到一个或多个本地站点的 VPC 数量是多少？
- VPC 是部署在单个区域 AWS 区域 还是多个区域？
- 需要将多少个本地站点连接到 AWS？
- 每个站点有多少客户网关设备（通常是路由器或防火墙）需要连接到 AWS？
- 预计将向 Amazon VPC 通告多少条路由？预计从侧面收到的路由数量是多少？ AWS
- 是否需要 AWS 随着时间的推移将带宽增加到？

需要考虑的功能

在混合连接设计中，规模非常重要。为此，下一部分将把规模作为目标连接模型设计的一部分。

以下是推荐使用的最佳实践，可最大限度地降低混合网络连接设计的规模复杂性：

- 应使用路由总结来减少通告和接收的路由数量。 AWS因此，IP 地址方案的设计需要最大限度地利用路由汇总。流量工程是一个关键的总体注意事项。有关流量工程的更多信息，请参阅可靠性部分中的“流量工程”子部分。
- 使用带有 VGW 的 DXGW 或者，单个 BGP 会话可以提供与多个 VPC 的连接 AWS Transit Gateway，从而最大限度地减少 BGP 对等会话的数量。
- 当需要将多个本地站点连接在一起时 AWS 区域 ，可以考虑使用 Cloud WAN。

连接模型

定义

连接模型是指本地网络与 AWS中的云资源之间的通信模式。您可以在 Amazon VPC 内跨多个区域的单个 AWS 区域 或多个 VPC 中部署云资源，也可以在单个或多个区域中部署具有公有终端节点的 AWS 服务 AWS 区域，例如 Amazon S3 和 DynamoDB。

关键问题

- 是否需要在区域内和跨区域进行 VPC 间通信？
- 是否需要直接从本地访问 AWS 公共端点？
- 是否需要在本地使用 VPC 终端节点访问 AWS 服务？

需要考虑的功能

以下是一些最常见的连接模型方案。每种连接模型都包括要求、属性和注意事项。

注意：如前所述，本白皮书重点介绍本地网络和 AWS之间的混合连接。有关互连 VPC 设计的更多详细信息，请参阅构建可扩展且安全的多 vPC AWS 网络基础设施白皮书。

模型

- AWS 加速的站点到站点 VPN —，单个 AWS Transit GatewayAWS 区域
- AWS DX — 带有 VGW 的 DXGW，单区域
- AWS DX — 带有 VGW、多区域和公共对等互连的 DXGW AWS
- AWS DX — 带多区域和公共对等互连 AWS Transit Gateway的 DXGW AWS
- AWS DX — DXGW 带 AWS Transit Gateway多区域（超过 3 个）

AWS 加速的站点到站点 VPN —，单个 AWS Transit GatewayAWS 区域

该模型由以下部分组成：

- 单曲 AWS 区域。
- AWS 托管的站点到站点 VPN 连接。 AWS Transit Gateway
- 已启用加速 SPN。

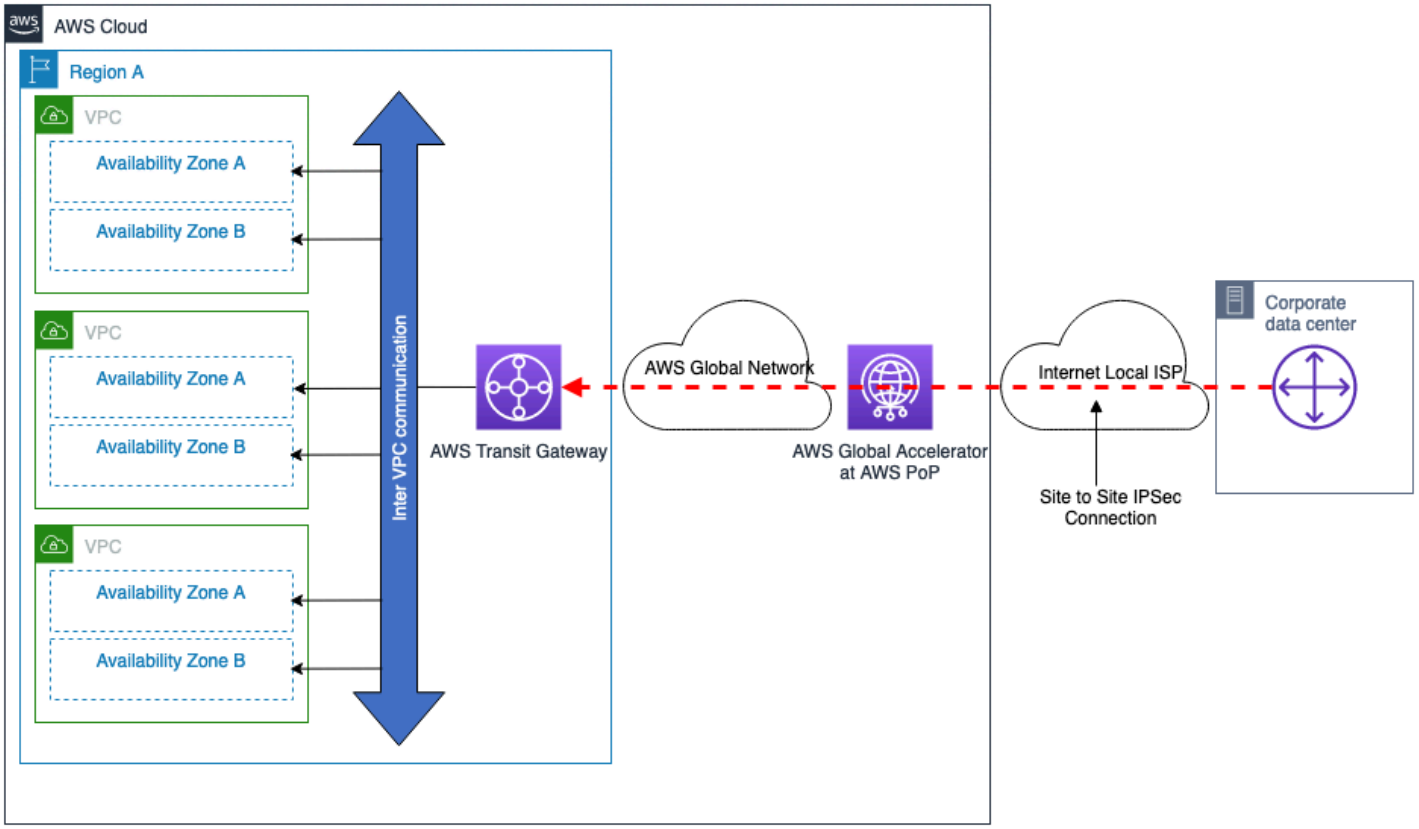

图 4 — AWS 托管 VPN — AWS Transit Gateway，单个 AWS 区域

连接模型属性：

- 通过使用 AWS 加速 Site-to-Site VPN 连接，能够在公共互联网上建立优化 VPN 连接。
- 通过使用 ECMP 配置多个 VPN 通道，能够实现更高 VPN 连接带宽。
- 可用于连接多个远程站点。
- 通过动态路由 (BGP) 提供自动失效转移。
- AWS Transit Gateway 连接到 VPC 后，所有连接的 VPC 都可以使用相同的 VPN 连接。您还可以控制 VPC 之间所需的通信模型，有关更多信息，请参阅中转网关的工作原理。
- 提供灵活的设计选项，可将第三方安全和 SD-WAN 虚拟设备与之集成。 AWS Transit Gateway请参阅 VPC 到 VPC 和本地到 VPC 流量的集中网络安全。

规模注意事项：

- 在配置多个 IPsec 通道和 ECMP 的情况下，带宽最高可达 50 Gbps（每个流量将限制在每个 VPN 通道的最大带宽内）。

- 每个 AWS Transit Gateway VPC可以连接@@ 成千上万个。
- 有关路由数量等其他规模限制，请参阅 Site-to-Site VPN 配额。

其他注意事项：

- 在本地数据中心和之间传输数据的额外 AWS Transit Gateway 处理成本 AWS。
- 无法在中 AWS Transit Gateway 引用远程 VPC 的安全组，但是 VPC 对等互连支持此功能。

AWS DX — 带有 VGW 的 DXGW，单区域

该模型由以下部分组成：

- 单曲 AWS 区域。
- 与独立的 DX 位置的双重 AWS Direct Connect 连接。
- AWS DXGW 使用 VGW 直接连接到 VPC。
- 可选用 AWS Transit Gateway 于 VPC 间通信。

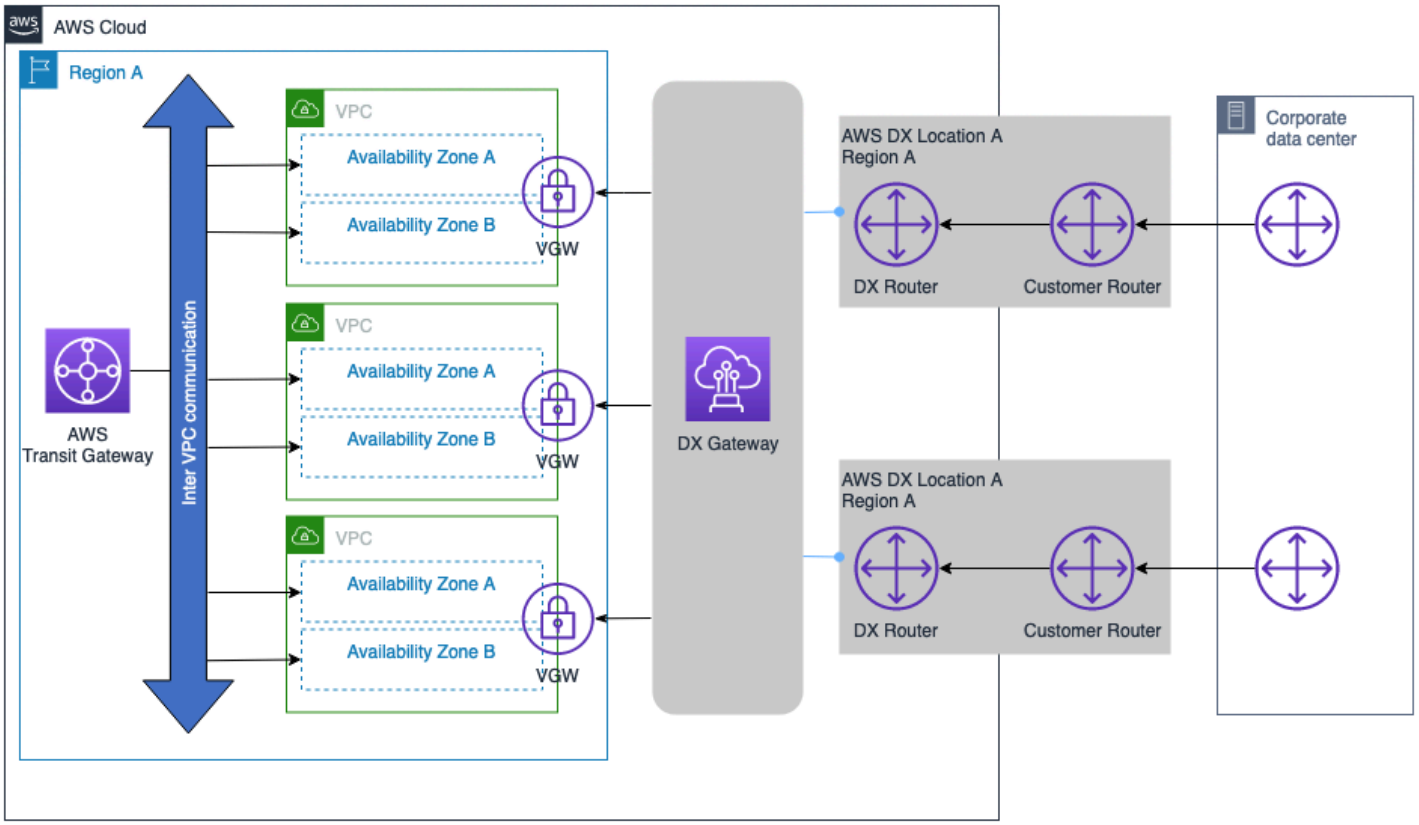

图 5 — AWS DX — 带有 VGW 的 DXGW，单曲 AWS 区域

连接模型属性：

- 提供将来连接到其他区域的 VPC 和 DX 连接的功能。
- 通过动态路由 (BGP) 提供自动失效转移。
- AWS Transit Gateway 您可以使用控制各个 VPC 之间所需的通信模式。有关更多信息，请参阅中转网关的工作原理。

规模注意事项：

有关其他规模限制的更多信息，如支持的前缀数量、每种 DX 连接类型（专用、托管）的 VIF 数量，请参阅 AWS Direct Connect 配额。一些重要注意事项：

- 私有 VIF 的 BGP 会话最多可以为 IPv4 和 IPv6 通告 100 条路由。
- 在单个 BGP 会话中，每个 DXGW 最多可以连接 20 个 VPC。如果需要超过 20 个 VPC，可以添加更多 DxGW 以促进大规模连接，或者考虑使用中转网关集成。
- 可以根据需要添加其他 AWS Direct Connect s。

其他注意事项：

- 与本地网络之间的 AWS 数据传输不会产生 AWS Transit Gateway 相关的处理成本。
- 无法引用远程 VPC 的安全组 AWS Transit Gateway （需要 VPC 对等）。
- 可以使用 VPC 对等互连 AWS Transit Gateway 来促进 VPC 之间的通信，但是，这会增加大规模构建和管理大量 V point-to-point PC 对等互连的操作复杂性。
- 如果不需要 VPC 间通信，则在此连接模式中 AWS Transit Gateway 也不需要 VPC 对等。

AWS DX — 带有 VGW、多区域和公共对等互连的 DXGW AWS

该模型由以下部分组成：

- 多个本地数据中心具有双重连接 AWS。
- 与独立的 DX 位置的双重 AWS Direct Connect 连接。
- AWS DXGW 使用 VGW 直接连接到 10 多个 VPC，使用 VGW 直接连接到多达 20 个 VPC。
- 可选用 AWS Transit Gateway 于 VPC 间和区域间通信。

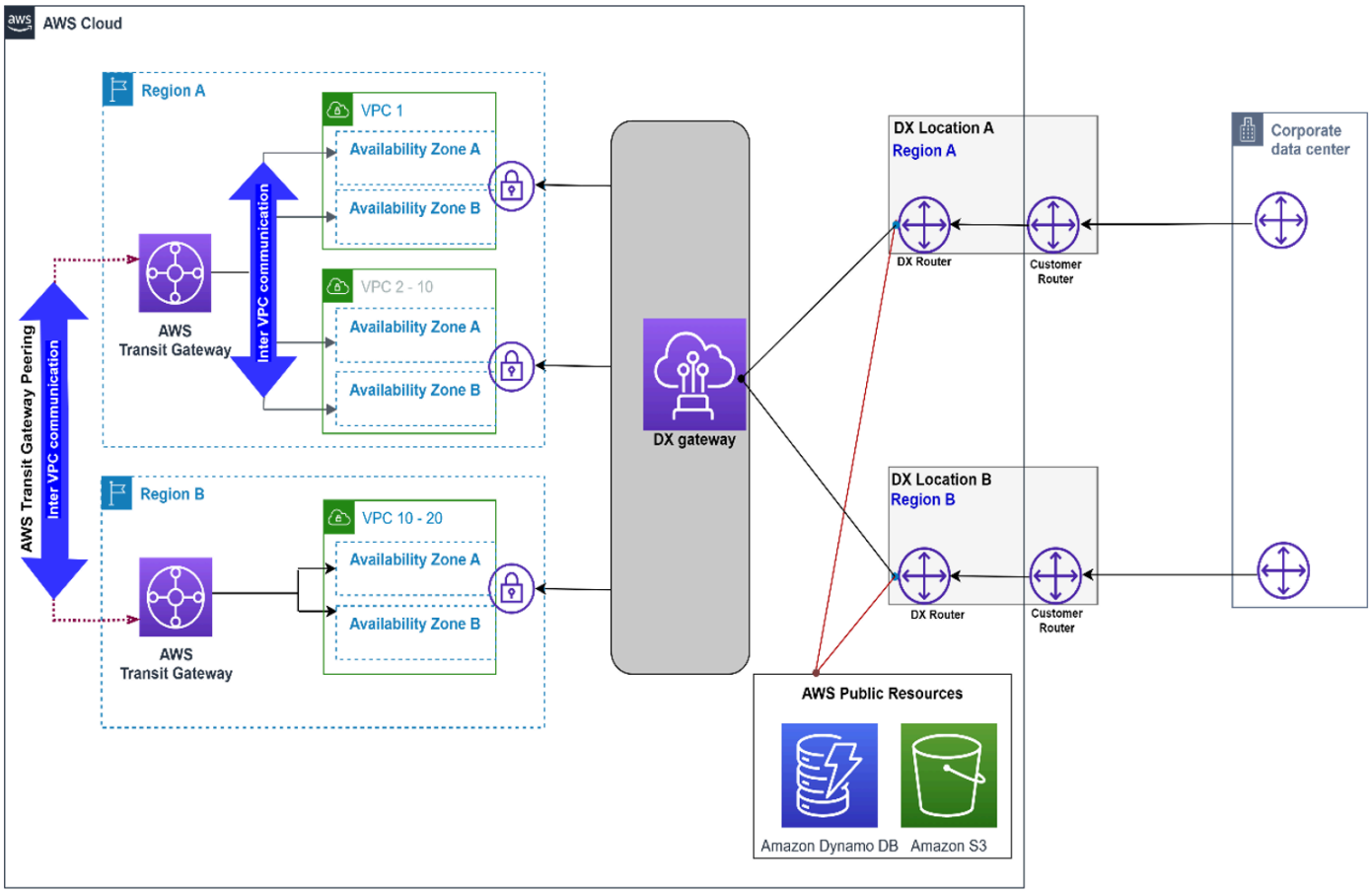

图 6 — AWS DX — 带有 VGW、多区域和公共 VIF 的 DXGW

连接模型属性：

- AWS DXGW 使用 VGW 直接连接到超过 10 个 VPC 使用 VGW 最多可连接 20 个 VPC。
- AWS DX 公共 VIF 用于直接通过 AWS DX 连接访问 AWS 公共服务，例如 Amazon S3。
- 提供将来连接到其他区域的 VPC 和 DX 连接的功能。
- 通过 Transit Gateway 对等互连促进了 VPC 间 AWS Transit Gateway 和区域间 VPC 通信。

规模注意事项：

有关其他规模限制的更多信息，如支持的前缀数量、每种 DX 连接类型（专用、托管）的 VIF 数量，请参阅 AWS Direct Connect 配额。一些重要注意事项：

- 私有 VIF 的 BGP 会话最多可以为 IPv4 和 IPv6 通告 100 条路由。
- 每个 DXGW 最多可通过每个专用 VIF 上的单个 BGP 会话连接 20 个 VPC，每个 DXGW 最多可连接 30 个专用 VIF。

- 可以根据需要添加其他 AWS Direct Connect s。

其他注意事项：

- 与本地网络之间的 AWS 数据传输不会产生 AWS Transit Gateway 相关的处理成本。
- 远程 VPC 的安全组不能被引用 AWS Transit Gateway （需要 VPC 对等）。
- 可以使用 VPC 对等互连 AWS Transit Gateway 来促进 VPC 之间的通信，但是，这将增加大规模构建和管理大量 V point-to-point PC 对等互连的操作复杂性。
- 如果不需要 VPC 间通信，则在此连接模式中 AWS Transit Gateway 也不需要 VPC 对等。

AWS DX — 带多区域和公共对等互连 AWS Transit Gateway的 DXGW AWS

该模型由以下部分组成：

- 多个 AWS 区域。
- 与独立的 DX 位置的双重 AWS Direct Connect 连接。
- 单个本地数据中心，具有双重连接 AWS。
- AWS 带有 DXGW 的。 AWS Transit Gateway
- 每个区域的 VPC 规模较大。

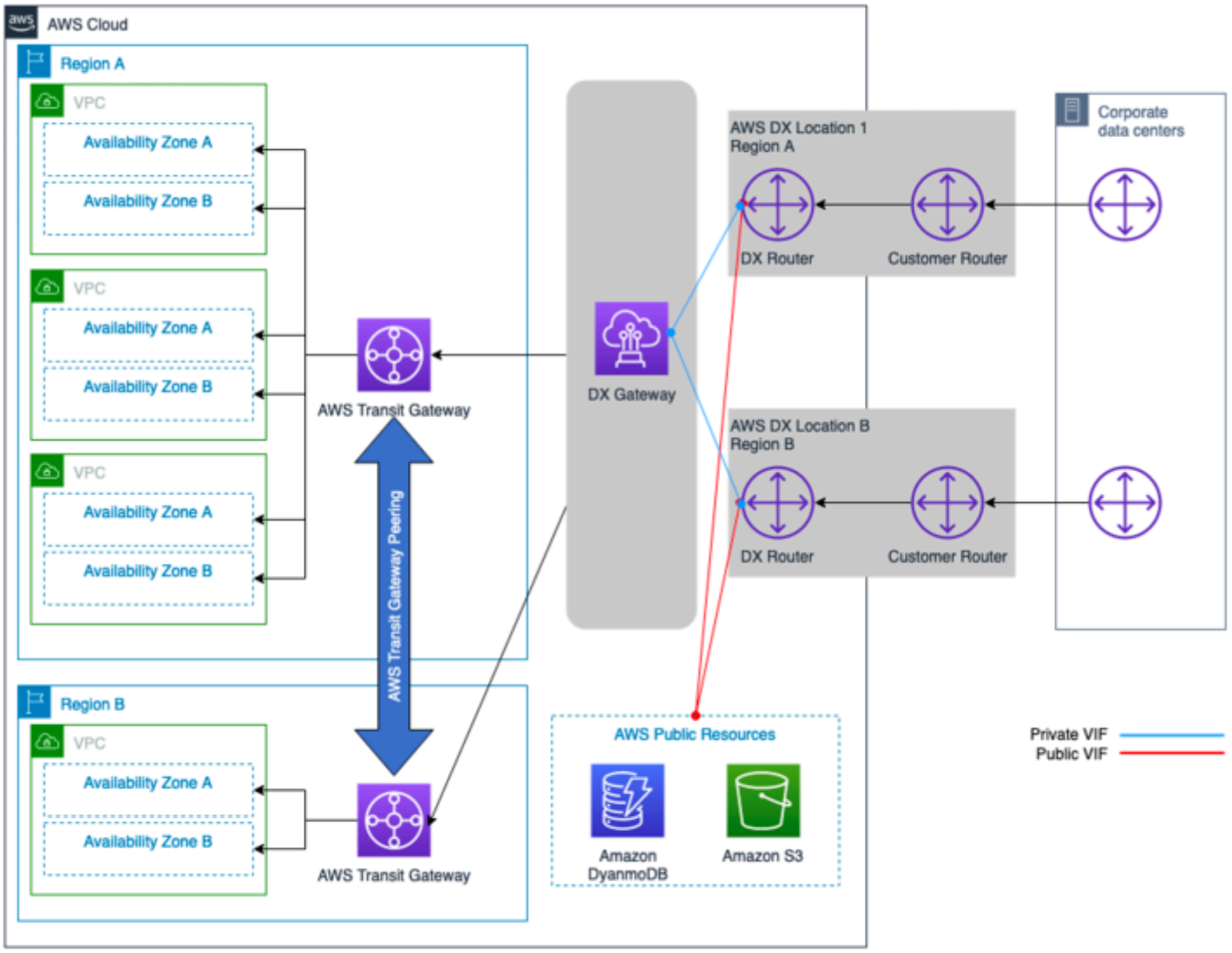

图 7 — AWS DX — 带 AWS Transit Gateway多区域和公共 VIF 的 DXGW AWS

连接模型属性：

- AWS DX 公共 VIF 用于通过 AWS DX 连接直接访问 S3 等 AWS 公共资源。
- 提供将来连接到其他区域的 VPC 和/或 DX 连接的功能。
- AWS Transit Gateway 连接到 VPC 后，可以在 VPC 之间实现完全或部分网状连接。
- 通过 AWS Transit Gateway 对等互连促进了 VPC 间和区域间 VPC 通信。
- 提供灵活的设计选项，可将第三方安全和 SDWAN 虚拟设备与 AWS Transit Gateway之集成。请参阅 VPC 到 VPC 和本地到 VPC 流量的集中网络安全。

规模注意事项：

- 往返路径的数量限制 AWS Transit Gateway 为 Transit VIF 所支持的最大路由数量（入站和出站号码各不相同）。有关规模限制以及支持的路由和 VIF 数量的更多信息，请参阅 AWS Direct Connect 配额。
- 在单个 BGP 会话中，每个 AWS Transit Gateway 会话最多可扩展到数千个 VPC。
- 每个 AWS DX 单次公交 VIF。
- 可以根据需要添加其他 AWS DX 连接。

其他注意事项：

- 与本地站点之间的 AWS 数据传输会产生额外的 AWS Transit Gateway 处理成本。
- 远程 VPC 的安全组不能被引用 AWS Transit Gateway （需要 VPC 对等）。
- 可以使用 VPC 对等互连 AWS Transit Gateway 来促进 VPC 之间的通信，但是，这将增加大规模构建和管理大量 V point-to-point PC 对等互连的操作复杂性。
- 如果需要超过三 AWS Transit Gateway个，则可以添加额外的 DXGW，请参阅以下连接模式。

AWS DX — DXGW 带 AWS Transit Gateway多区域（超过 3 个）

该模型由以下部分组成：

- 多个 AWS 区域 （大于 3）。
- 双重本地数据中心。
- 每个地区的独立DX位置都有双 AWS Direct Connect 连接。
- AWS 带有 DXGW 的。 AWS Transit Gateway
- 每个区域的 VPC 规模较大。
- AWS Transit Gateway s 之间的完整对等网格。

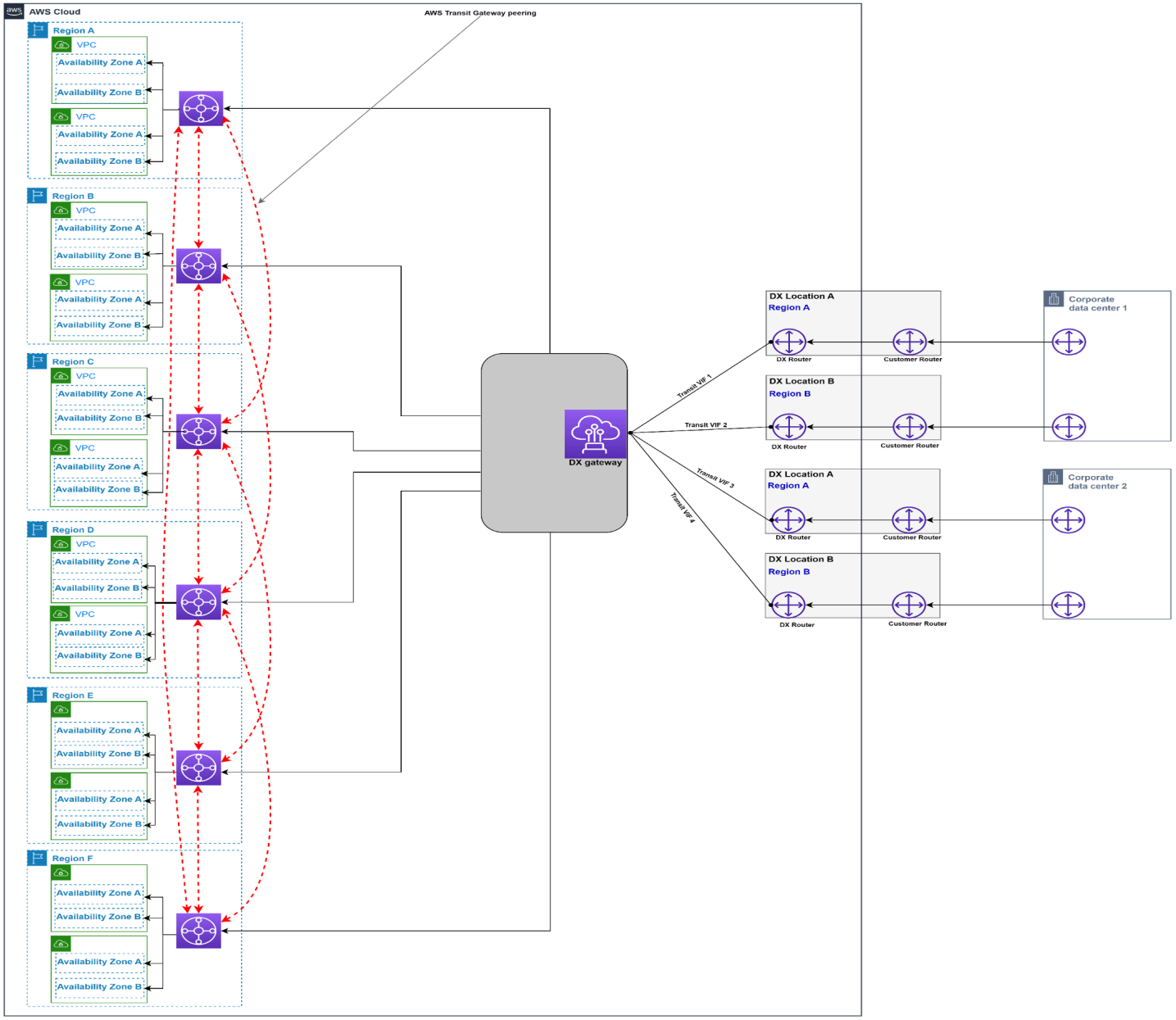

图 8 — AWS DX — 带 AWS Transit Gateway多区域的 DXGW（超过三个）

连接模型属性：

- 最低的运行开销。
- AWS DX 公共 VIF 用于直接通过 AWS DX 连接访问 AWS 公共资源，例如 S3。
- 提供将来连接到其他区域的 VPC 和 DX 连接的功能。
- AWS Transit Gateway 连接到 VPC 后，可以在 VPC 之间实现完全或部分网状连接。
- 对等互连促进了区域间 VPC 通信。 AWS Transit Gateway

- 提供灵活的设计选项，可将第三方安全和 SDWAN 虚拟设备与 AWS Transit Gateway之集成。请参阅 VPC 到 VPC 和本地到 VPC 流量的集中网络安全。

规模注意事项：

- 往返路径的数量限制 AWS Transit Gateway 为 Transit VIF 所支持的最大路由数量（入站和出站号码各不相同）。有关规模限制的更多信息，请参阅 AWS Direct Connect 配额。如有必要，可考虑路由汇总，以减少路由数量。
- 在每个 DXGW 的单个 BGP 会话 AWS Transit Gateway 中，每个 VPC 最多可扩展到数千个 VPC（假设配置的 AWS DX 连接提供的性能足够了）。
- 每个 DXGW 最多可以连接六 AWS Transit Gateway秒。
- 如果需要使用连接三个以上的区域 AWS Transit Gateway，则需要额外的 DxGW。
- 每个 AWS DX 单次公交 VIF。
- 可以根据需要添加其他 AWS DX 连接。

其他注意事项：

- 在本地站点和 AWS之间传输数据会产生额外的 AWS Transit Gateway 处理成本。
- 远程 VPC 的安全组不能被引用 AWS Transit Gateway （需要 VPC 对等）。
- 可以使用 VPC 对等互连 AWS Transit Gateway 来促进 VPC 之间的通信，但是，这将增加大规模构建和管理大量 V point-to-point PC 对等互连的操作复杂性。

以下决策树介绍了可扩展性和通信模型的注意事项：

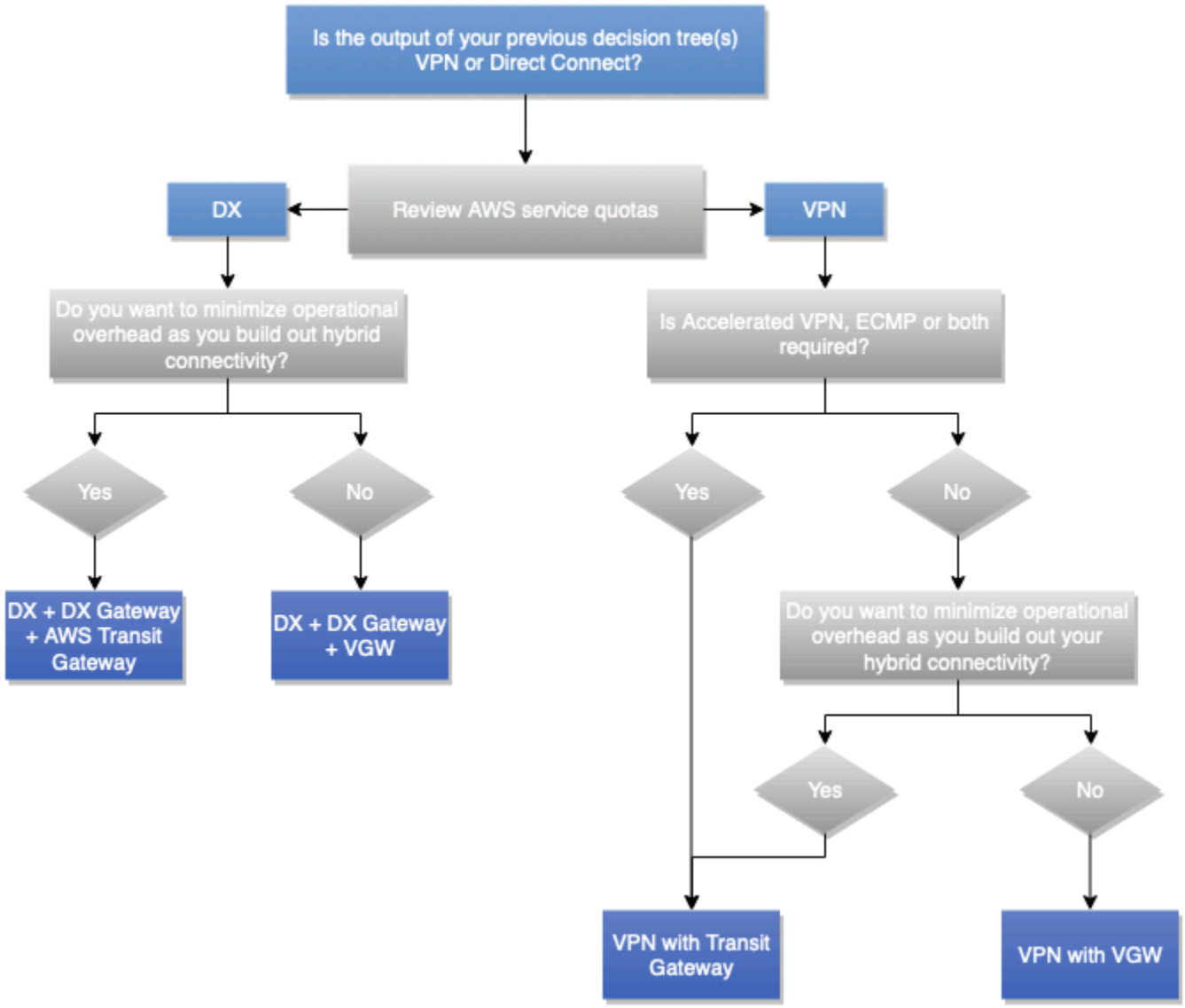

图 9——可扩展性和通信模型决策树

> **Note**
>
> 如果选择的连接类型是 VPN，通常要考虑性能，则应决定 VPN 终止点是 V AWS GW 还是 AWS Transit Gateway AWS S2S VPN 连接。如果尚未做出决定，则可以考虑 VPC 之间所需的通信模型以及需要连接到 VPN 连接的 VPC 数量，以帮助做出决定。

可靠性

定义

可靠性是指服务或系统在需要时执行其预期功能的能力。系统的可靠性可以通过其在给定时间范围内的运行质量水平来衡量。与此形成鲜明对比的是，故障恢复能力是指系统动态可靠地从基础设施或服务中断中恢复的能力。

有关如何使用可用性和弹性来衡量可靠性的更多详细信息，请参阅 Well-Ar AWS chitected Frame work 的可靠性支柱。

关键问题

可用性

可用性是指工作负载可供使用的时间百分比。常见的目标包括 99%（每年允许停机 3.65 天）、99.9%（8.77 小时）和 99.99%（52.6 分钟），百分比中的“9”为速记数字（“两个九”表示 99%，“三个九”表示 99.9%，以此类推）。与本地数据中心 AWS 之间的网络解决方案的可用性可能与整体解决方案或应用程序可用性不同。

网络解决方案可用性的关键问题包括：

- 如果我的 AWS 资源无法与我的本地资源通信，它们能否继续运行？ 反之亦然？
- 我是否应该将计划内维护的计划停机时间包括在可用性指标内还是排除在可用性指标外？
- 我将如何衡量网络层的可用性（与应用程序的整体运行状况分开）？

完善架构可靠性支柱的可用性部分提供了有关计算可用性的建议和公式。

故障恢复能力

故障恢复能力是指工作负载从基础设施故障或服务中断恢复、动态获取计算资源以满足需求以及减少中断（如错误配置或暂时性网络问题）的能力。如果冗余网络组件（链路、网络设备等）的可用性本身不足以单独提供预期功能，则其故障恢复能力就会降低。这样做的后果是，用户体验很差，体验度下降。

网络解决方案故障恢复能力的关键问题包括：

- 我应该允许同时发生多少次不连续故障？
- 如何减少连接解决方案和内部网络的单点故障？
- 我在分布式拒绝服务 (DDoS) 事件中存在哪些漏洞？

技术解决方案

首先，需要注意的是，并不是每个混合网络连接解决方案都需要高水平的可靠性，而且可靠性水平的提高也会相应增加成本。在某些方案中，主站点可能需要可靠（冗余和可恢复）的连接，因为停机对业务的影响较大，而区域站点可能不需要相同级别的可靠性，因为发生故障事件时对业务的影响较小。建议参阅AWS Direct Connect 弹性建议，因为它解释了在设计中确保高弹性 AWS 的最佳实践。 AWS Direct Connect

为了实现可靠的混合网络连接解决方案的故障恢复能力，设计需要考虑以下几个方面：

- 冗余：旨在消除混合网络连接路径中的任何单点故障，包括但不限于网络连接、边缘网络设备、跨可用区和 DX 位置的冗余以及设备电源、光纤路径和操作系统。 AWS 区域就本白皮书的目的和范围而言，冗余侧重于网络连接、边缘设备（例如客户网关设备）、 AWS DX 位置和 AWS 区域 （对于多区域架构）。
- 可靠的失效转移组件：在某些方案中，系统可能可以正常运行，但无法在所需的级别上执行其功能。这种情况在单一故障事件中很常见，因为此时会发现计划的冗余组件在非冗余状态下运行——由于使用原因，它们的网络负载无处可去，从而导致整个解决方案的容量不足。
- 失效转移时间：失效转移时间是指辅助组件完全接管主组件角色所需的时间。失效转移时间有多个因素：检测到故障需要多长时间、启用辅助连接需要多长时间，以及将更改通知网络的其余部分需要多长时间。使用 VPN 链路的死点对等检测 (DPD) 和链路的双向转发检测 (BFD) 可以改善故障检测。AWS Direct Connect 启用辅助连接的时间可能非常短（如果这些连接始终处于活动状态），也可能是很短的时间窗口（如果需要启用预先配置的 VPN 连接），或者更长（如果需要移动物理资源或配置新资源）。通知网络其余部分通常是通过客户网络内的路由协议进行的，每种路由协议都有不同的收敛时间和配置选项，这些配置超出了本白皮书的范围。
- 流量工程：可恢复混合网络连接设计中的流量工程旨在解决在正常和故障情况下流量应如何流经多个可用连接的问题。建议遵循故障设计的概念，即您需要了解解决方案在不同的故障情况下将如何运行，以及是否能被企业接受。这一部分将讨论一些常见的流量工程用例，旨在提高混合网络连接解决方案的整体故障恢复能力水平。关于路由和 BGP 的 AWS Direct Connect 部分介绍了影响流量的几种流量工程选项（社区、BGP 本地首选项、AS 路径长度）。要设计有效的流量工程解决方案，您需要充分了解每个 AWS 网络组件在路由评估和选择方面如何处理 IP 路由，以及影响路由选择的可能机制。这方面的详细信息不在本文档的讨论范围之内。有关更多信息，请根据需要参阅中转网关路由评估顺序、Site-to-Site VPN 路由优先级以及 Direct Connect 路由和 BGP 文档。

> **Note**
>
> 在 VPC 路由表中，您可能会引用包含其他路由选择规则的前缀列表。有关此用例的更多信息，请参阅前缀列表的路由优先级。 AWS Transit Gateway 路由表也支持前缀列表，但是一旦应用了前缀列表，它们就会扩展到特定的路由条目。

具有更多特定路由的双重 Site-to-Site VPN 连接示例

该方案基于一个小型本地站点，通过互联网与 AWS 区域 的冗余 VPN 连接，连接到单个 AWS Transit Gateway。图 10 所示的流量工程设计表明，通过流量工程，您可以影响路径选择，从而提高混合连接解决方案的可靠性：

- 可恢复混合连接：每个冗余的 VPN 连接都提供相同的性能容量，通过使用动态路由协议 (BGP) 支持自动失效转移，并通过使用 VPN 失效对端检测加快连接故障检测。
- 性能效率： 在与 AWS Transit Gateway 的两个 VPN 连接中配置 ECMP，有助于最大限度地提高整个 VPN 连接的带宽。或者，通过公布不同的、更具体的路由以及站点摘要路由，可以独立管理两个 VPN 连接之间的负载

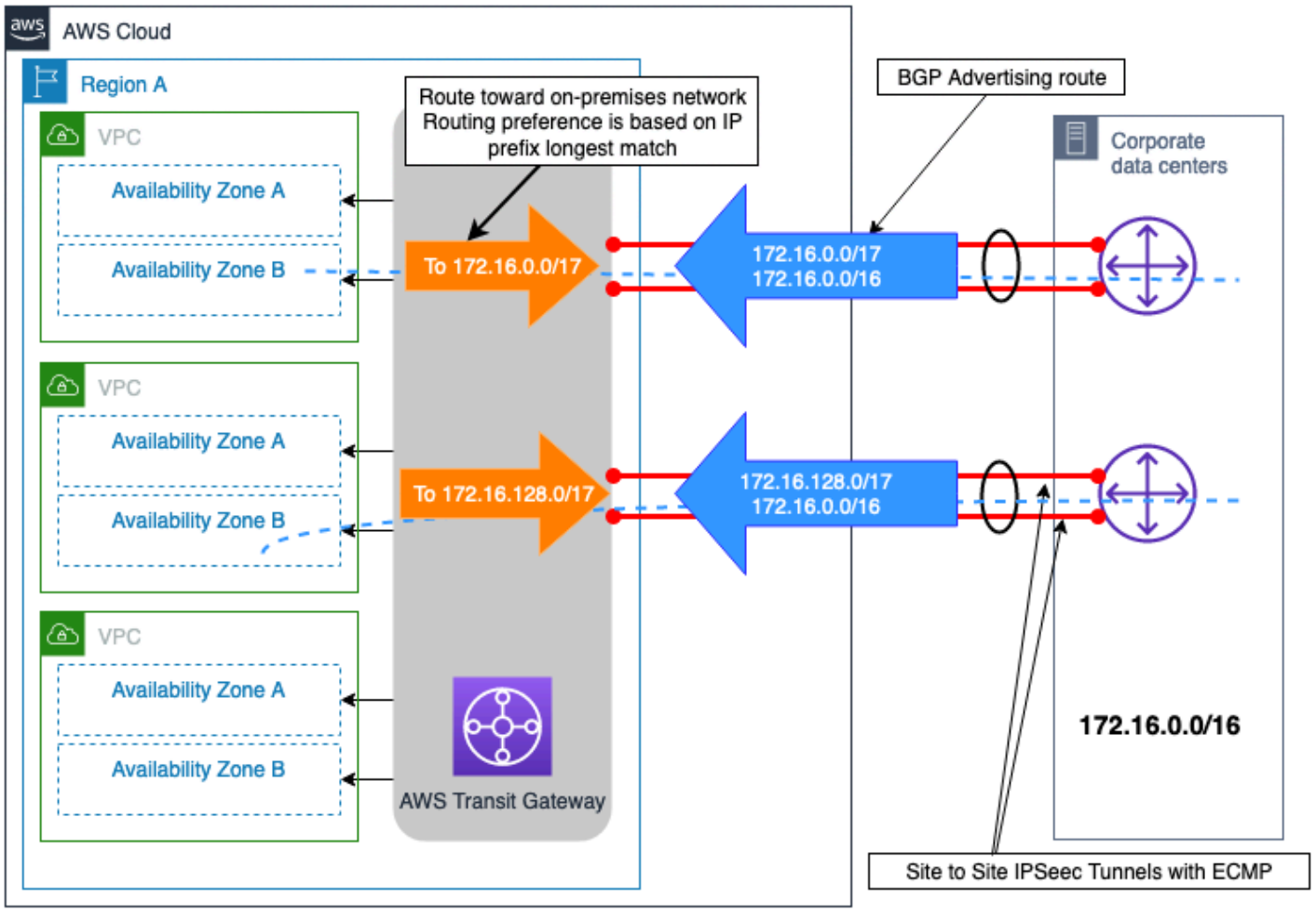

图 10——具有更多特定路由的双重 Site-to-Site VPN 连接示例

具有多个 DX 连接的双重本地站点示例

图 11 所示的场景显示了位于不同地理区域的两个本地数据中心站点，它们使用 DXGW 和 VGW AWS 使用最大弹性连接模型（在AWS Direct Connect 弹性建议中描述） AWS Direct Connect 进行连接。这两个本地站点通过数据中心互连 (DCI) 链路相互连接。属于远程分支站点的本地 IP 前缀 (192.168.0.0/16) 从两个本地数据中心站点进行通告。此前缀的主路径应为数据中心 1。如果数据中心 1 或两个 DX 位置都出现故障，进出远程分支站点的流量将失效转移到数据中心 2。此外，每个数据中心都有一个特定站点的 IP 前缀。这些前缀需要直接访问，如果两个 DX 位置都出现故障，则需要通过另一个数据中心站点访问。

通过将 BGP 社区属性与通告给 DXGW 的路由相关联，您可以影响 AWS DXGW 端的出口路径选择。AWS 这些社区属性控制分配给通告路由 AWS的 BGP 本地首选项属性。有关更多信息，请参阅 AWS DX 路由策略和 BGP 社区。

为了最大限度地提高该 AWS 区域 级别连接的可靠性，每对 AWS DX 连接都配置 ECMP，这样两者可以同时用于每个本地站点和之间的数据传输。 AWS

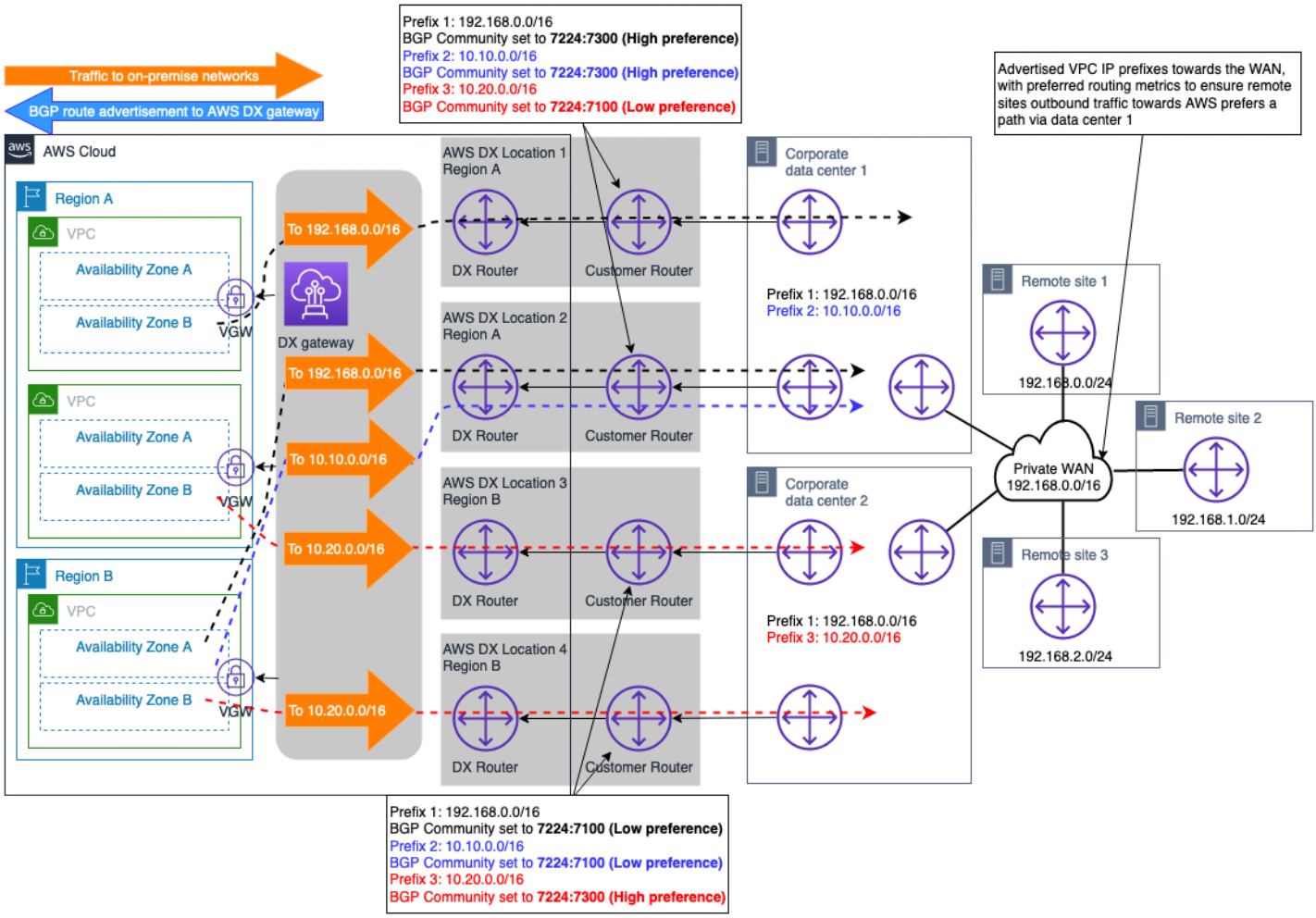

图 11——具有多个 DX 连接的双重本地站点示例

通过这种设计，发往本地网络（具有相同的通告前缀长度和 BGP 社区）的流量将使用 ECMP 分布在每个站点的双重 DX 连接中。但是，如果在 DX 连接中不需要使用 ECMP，则可以使用前面讨论并在路由策略和 BGP 社区文档中描述的相同概念来进一步设计 DX 连接级别的路径选择。

注意：如果本地数据中心的路径中有安全设备，则需要将这些设备配置为允许流量通过一条 DX 链路离开，并从同一数据中心站点内的另一条 DX 链路（两条链路均使用 ECMP）进入。

作为 AWS DX 连接备份的 VPN 连接示例

可以选择 VPN 为 AWS Direct Connect 连接提供备用网络连接。通常情况下，这种类型的连接模型是受成本驱动的，因为由于互联网上的性能不确定，并且无法通过公共互联网进行连接获得 SLA，它

为整个混合连接解决方案提供的可靠性较低。它是一种有效且具有成本效益的连接模型，应在成本是首要考虑因素且预算有限的情况下使用，也可作为临时解决方案，直至可以配置备用 DX。图 12 说明了该连接模型的设计。这种设计的一个关键考虑因素是，VPN 和 DX 连接都终止于 AWS Transit Gateway，与可以通过连接的 DX 连接通告的路由相比，VPN 连接可以通告更多的路由。 AWS Transit Gateway这可能会导致不理想的路由情况。解决这一问题的办法是在客户网关设备 (CGW) 上为从 VPN 连接接收的路由配置路由过滤，只允许接受汇总路由。

注意：要在上创建总结路由 AWS Transit Gateway，您需要在路由表中指定指向任意附件的静态 AWS Transit Gateway 路由，以便沿着更具体的路由发送摘要。

从 AWS Transit Gateway 路由表的角度来看，本地前缀的路由是从 AWS DX 连接（通过 DXGW）和 VPN 接收的，前缀长度相同。按照的路由优先级逻辑 AWS Transit Gateway，通过 Direct Connect 接收的路由的优先级高于通过站点到站点 VPN 接收的路由，因此，到达本地网络的首选路径将是到达本地网络的首选。 AWS Direct Connect

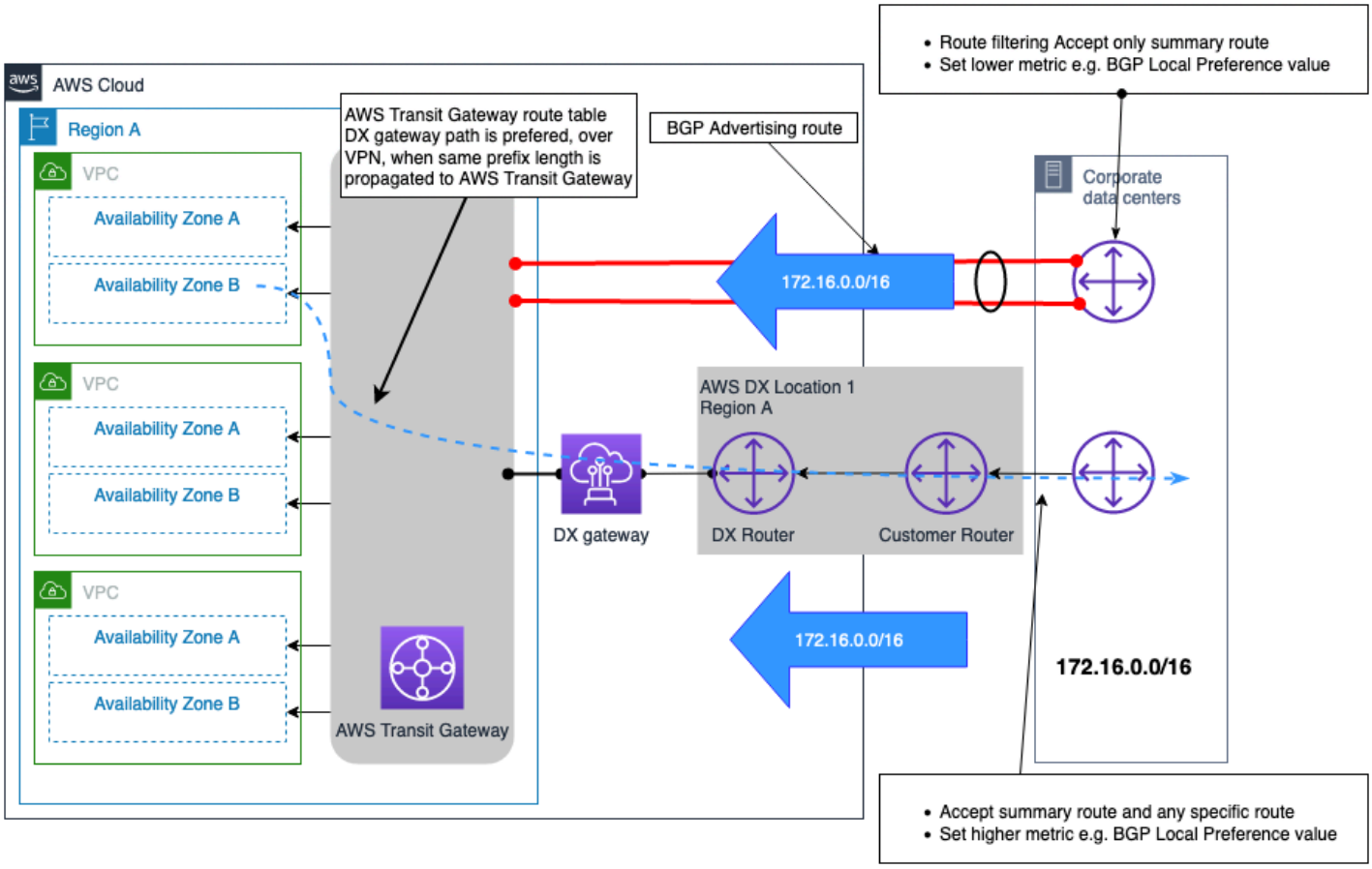

图 12 — 作为 AWS DX 连接备份的 VPN 连接示例

下面的决策树将指导您做出所需的决策，以实现可恢复（带来可靠性）混合网络连接。有关更多信息，请参阅 AWS Direct Connect 故障恢复能力工具包。

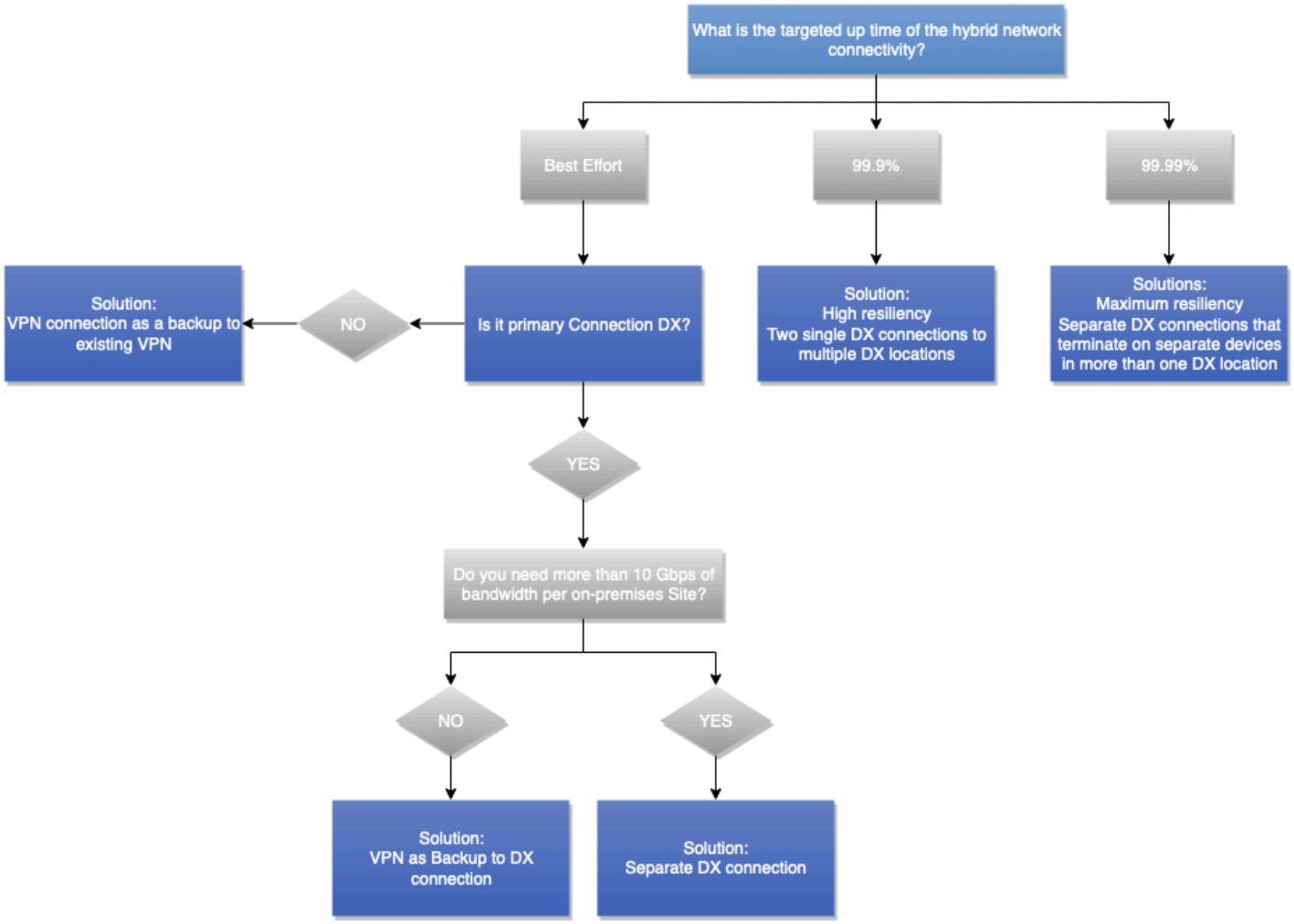

图 13——可靠性决策树

客户托管的 VPN 和 SD-WAN

定义

互联网连接是一种商品，可用带宽每年都在持续增加。一些客户选择在互联网上构建虚拟 WAN，而不是构建和运营专用 WAN。软件定义的广域网 (SD-WAN) 允许公司通过巧妙地使用软件，快速配置和集中管理该虚拟 WAN。其他客户则选择采用传统的自我托管站点到站点 VPN。

对设计决策的影响

SD-WAN 和客户托管 VPN 可以通过互联网或 AWS Direct Connect运行。SD-WAN（或任何软件 VPN 叠加层）与底层网络传输一样可靠。因此，本白皮书前面讨论的可靠性和 SLA 注意事项在此也适用。例如，通过互联网构建 SD-WAN 叠加层无法提供与在 AWS Direct Connect上构建 SD-WAN 叠加层相同的可靠性。

需求定义

- 您是否在本地网络中使用 SD-WAN？
- 您是否需要某些特定特征，而这些功能只能在用于 VPN 终端的某些虚拟设备上使用？

技术解决方案

AWS 建议将 SD-WAN 与集成 AWS Transit Gateway，并发布支持 AWS Transit Gateway 集成的供应商名单。 AWS 可以充当 SD-WAN 站点的中心或分支站点。主 AWS 干网可用于将部署在高度可靠和高性能的网络中的 AWS 不同 SD-WAN 集线器连接起来。SD-WAN 解决方案支持通过任何可用路径进行自动失效转移，并在单个管理窗格中提供额外的监控和可观察性功能。与传统 WAN 相比，广泛使用自动配置和自动化可以实现快速配置和可见性。但是，隧道和加密开销的使用无法与专用连接中使用的专用高速光纤链路相比。

在某些情况下，您可能会选择使用具有 VPN 功能的虚拟设备。选择自我托管的虚拟设备的原因包括技术特征以及与网络其余部分的兼容性。当您选择使用部署在 EC2 实例中的虚拟设备的自我托管 VPN 或 SD-WAN 解决方案时，您需要负责管理该设备。您还负责虚拟设备之间的高可用性和失效转移。这样的设计会增加您的运营责任，但却能为您提供更大的灵活性。该解决方案的特性和特征取决于您选择的虚拟设备。

AWS Marketplace 包含许多 VPN 虚拟设备，客户可以将其部署在 Amazon EC2 上。 AWS 建议从 AWS 托管 S2S VPN 开始，如果不符合您的要求，请考虑其他选项。虚拟设备的管理开销由客户承担。

示例汽车公司用例

白皮书的这一部分展示了如何使用注意事项、需求定义问题和决策树来帮助您决定最佳混合网络设计。识别和获取需求非常重要，因为它们被用作决策树的输入。预先获取需求可以避免进一步的设计迭代。如果必须重新审查设计，项目就会完全停止，宝贵的资源就会被搁置，而如果能事先了解需求，就能最大限度地减少这种情况的发生，最理想的情况是避免这种情况的发生。

这一部分将以示例汽车公司作为客户示例。他们希望在 AWS 上初步部署第一个分析项目。分析项目侧重于分析来自公司制造的汽车的数据以及公司数据中心中已有的其他数据集。最初，公司的架构小组认为他们需要一个 AWS 账户、一个 Amazon VPC 和几个子网来托管生产和开发环境。项目团队渴望开始工作，他们要求尽快获得访问开发环境的权限。他们的目标是在三个月后投入生产。

示例汽车公司还计划将其 AWS 用于其他几个项目，例如，在未来 6 个月内将其 ERP 系统、虚拟桌面基础设施 (VDI) 和另外 20 个应用程序从本地迁移到 AWS。其他项目的一些要求仍在确定中，但很明显，它们的 AWS Cloud 使用量会增加。

架构团队决定采用本白皮书中概述的方法。他们使用每项考虑事项下概述的需求定义问题来获取输入信息，从而做出设计决策。

它们从与连接类型相关的要求开始，下表对此进行了总结。

表 4——示例汽车公司可靠性输入

连接类型选择注意事项	需求定义问题	回答
部署时间	部署所需的时间轴是什么？ 几小时、几天、几周还是几个月？	• 开发/测试：1 个月 • 生产：3 个月
安全性	您的安全要求和政策是否允许通过互联网使用加密连接来连接 AWS，还是强制使用专用网络连接？	• 开发/测试：可以接受 Site-to-Site VPN • 生产：需要专用网络
	利用专用网络连接时，网络层是否必须提供传输中加密？	否，将使用应用层加密。
SLA	是否需要包含服务积分的混合连接 SLA？	• 开发/测试：否 • 生产：是

连接类型选择注意事项	需求定义问题	回答
	正常运行时间目标是什么？	• 开发/测试：不适用 • 生产：99.99%
	整个混合网络是否遵守正常运行时间目标？	• 开发/测试：不适用 • 生产：是
性能	所需的吞吐量是多少？	• 开发/测试：100 Mbps • 生产：500 Mbps 增长到 2 Gbps
	AWS与本地网络之间可接受的最大延迟时间是多少？	• 开发/测试：没有硬性要求 • 生产：小于 30 ms
	可接受的最大网络抖动是多少？	• 开发/测试：没有硬性要求 • 生产：所需的最小抖动
成本	您每月要向 AWS 发送多少数据？	• 开发/测试：2 TB • 生产：20 TB 增长到 50 TB
	您每月要从 AWS 发送多少数据？	• 开发/测试：1 TB • 生产：10 TB 增长到 25 TB
	这种连接是永久性的吗？	是

根据收到的需求，架构团队遵循了图 9 中的连接类型决策树。这使架构团队能够决定开发、测试和生产环境的连接类型。对于生产环境，他们考虑了当前和未来的需求。对于开发和测试，示例汽车公司将通过互联网建立 Site-to-site VPN。在生产方面，他们将与服务提供商合作，将其公司网络与 AWS Direct Connect 连接起来。示例汽车公司最初考虑使用 Direct Connect 托管连接，但由于需要AWS 提供 SLA，他们选择了 Direct Connect 专用连接。

确定连接类型后，下一步就是获取影响连接设计选择的需求。这与逻辑设计有关，例如如何配置连接以及使用哪些 AWS 服务来支持业务和技术需求。

为获取可扩展性和通信模型需求，架构团队使用了本白皮书相关部分中的需求定义问题。下表概述了与这两个注意事项相关的需求。

表 5——需求定义问题

连接设计选择注意事项	需求定义问题	回答
可扩展性	当前或预计需要连接到一个或多个本地站点的 VPC 数量是多少？	最初 2 个，6 个月后增至 30 个
	这些 VPC 是部署在单个 AWS 区域 还是多个区域？	单个区域
	需要将多少个本地站点连接到 AWS？	2 个数据中心
	每个站点有多少客户网关设备需要连接到 AWS？	每个数据中心 2 台路由器
	预计将向 AWS VPC 通告多少条路由，以及预计从 AWS 端收到多少条路由？	• 要通告到 AWS 的路由：20 条路线 • 要从 AWS 接收的路由：1 /16 条路由
	是否有计划考虑在不久的将来增加与 AWS 连接的带宽？	• 开发/测试：100 Mbps • 生产：500Mbps 增长到 2Gbps。
连接设计模型	是否需要启用 VPC 间通信（区域内和/或跨区域）？	是，在 AWS 区域 内
	是否需要直接从本地访问 AWS 公共端点服务？	是
	是否需要从本地使用 VPC 端点访问 AWS 服务？	否

根据输入，架构团队遵循了连接设计部分的决策树。由于预计未来 6 个月内 VPC 数量将从 2 个增加到 30 个，架构团队决定使用 AWS Transit Gateway 作为连接的终端网关和 VPC 之间的路由。独立 AWS Transit Gateway 将终止用于开发和测试的 VPN 连接，以及与 AWS Direct Connect 的生产连接。使

用分离的 AWS Transit Gateway 可以简化变更管理，明确划分开发/测试环境和生产环境。由于 AWS Transit Gateway，生产需要 AWS Direct Connect 网关。公有 VIF 将用于访问 AWS 公共端点服务。图 14 说明了根据收集到的需求在决策树上采取的路径。

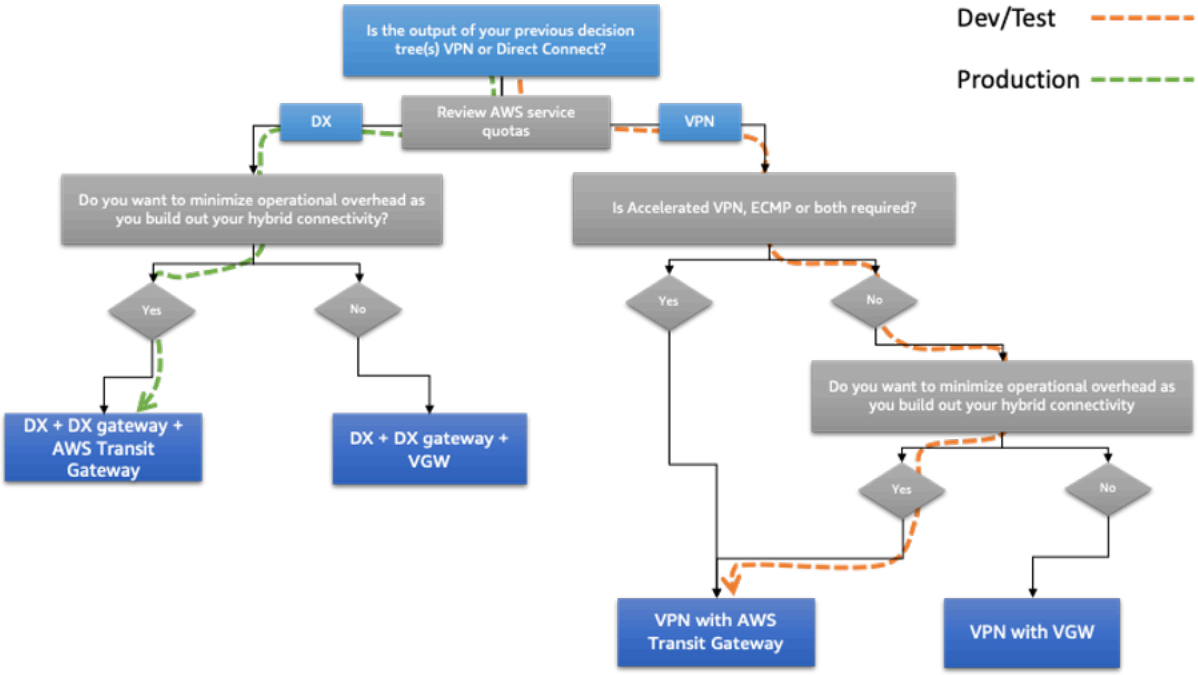

图 14——示例汽车公司连接设计决策树

在确定满足可扩展性和通信模型需求的解决方案后，下一步就是获取与可靠性相关的要求。这与所需的可用性和弹性水平有关。

为获取可靠性需求，架构团队使用了本白皮书相关部分中的需求定义问题。下表总结了需求。

表 6——可靠性需求问题

连接设计选择注意事项	需求定义问题	回答
可靠性	如果 AWS 出现连接故障，对业务的影响有多大？	• 开发/测试：低 • 生产：高
	从业务角度来看，AWS 出现连接故障后的成本是否高于为 AWS 部署高可靠性连接模式的成本？	• 开发/测试：否 • 生产：是

根据所收到的意见，架构团队遵循了本白皮书前面所介绍的可靠性注意事项部分中的决策树。考虑到生产连接的正常运行时间目标为 99.99%，以及服务中断对业务的严重影响，架构团队决定使用 2 个 Direct Connect 位置，并从每个本地数据中心到每个 Direct Connect 位置设置 2 个链接（共 4 个链接）。用于开发和测试的 VPN 连接还将使用两个 VPN 连接来增加冗余。使用可靠性部分中讨论的路由工程技术，将按以下方式配置连接：

- 在开发和测试过程中，将使用 ECMP 通过 2 条隧道对通往主数据中心的流量进行负载平衡。这样可以提高吞吐量。如果主隧道发生故障，将使用通往备用数据中心的隧道。
- 在生产方面，本地与 AWS 之间通过任一 Direct Connect 位置的延迟非常相似。在这种情况下，对于部署在主数据中心的本地系统，决定通过两个连接到主数据中心的 AWS 和本地之间的流量进行负载平衡。同样，对于在备用数据中心运行的本地系统，流量将在备用数据中心的两个连接之间的流量进行负载平衡。如果连接失败，BGP 将自动进行失效转移。

图 15 说明了根据收集到的需求在决策树上采取的路径。

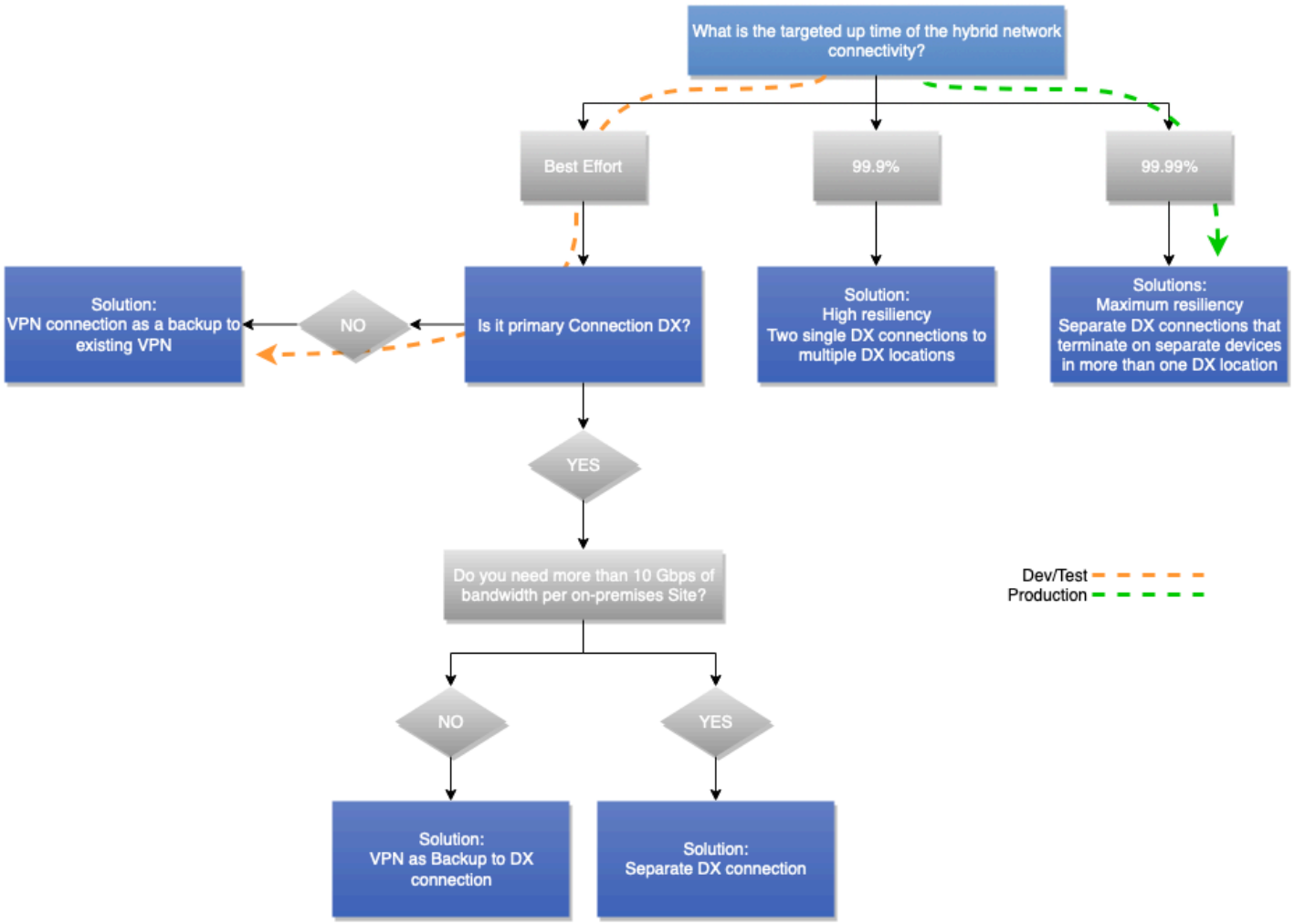

图 15——示例汽车公司可靠性决策树

示例汽车公司选择的架构

下图说明了示例汽车公司在收集需求并浏览本白皮书前几部分中介绍的决策树后选择的架构。

它在互联网上使用以 AWS 为终端的 AWS Transit Gateway S2S VPN 进行开发和测试。然后，它将 AWS Direct Connect 与 Direct Connect 网关和第二个 AWS Transit Gateway 用于生产流量。AWS Transit Gateway 可用于 VPC 间路由。从数据路径的角度来看，主数据中心的 VPN 隧道被用作开发和测试的主路径，而通往备用数据中心的隧道则被用作失效转移路径。对于生产流量，所有连接都同时使用。根据本地系统所在的数据中心，来自 AWS 的流量会优先选择最可选择的网络连接。示例汽车公司采用类似的路由工程技术，在向 AWS 发送流量时优先选择合适的路径，确保使用对称流量路径，最大限度地减少本地主数据中心和备用数据中心之间对公司网络的使用。

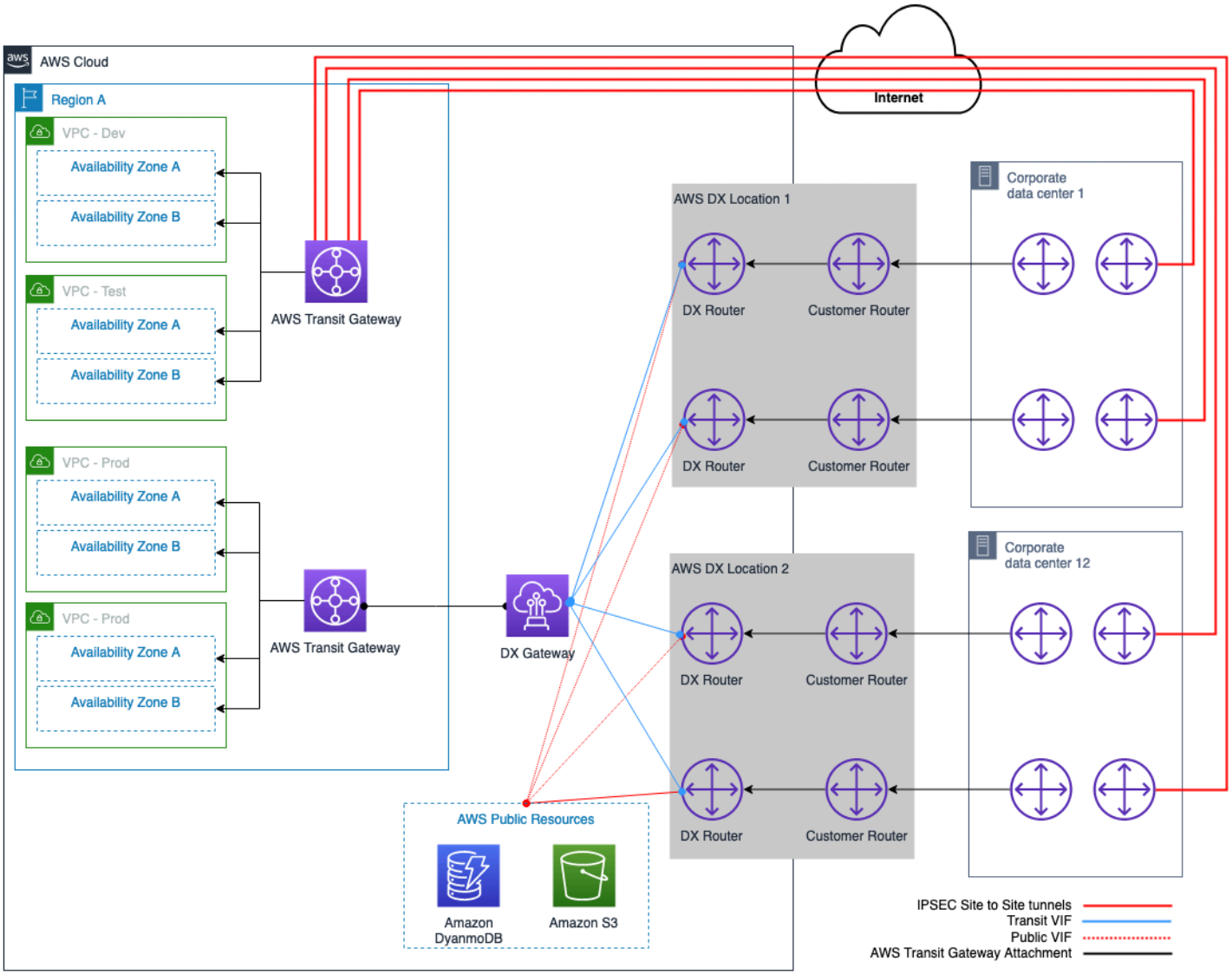

图 16——示例公司汽车公司选择的混合连接模型

结论

混合连接模式是采用云计算的基本起点之一。按照本白皮书中概述的连接模式选择流程，可以构建出具有最佳架构的混合网络。

该过程包括按逻辑顺序排列的注意事项。该顺序与经验丰富的网络和云架构师所遵循的思维模式非常相似。在每组注意事项中，决策树允许快速选择连接模式，即使输入要求有限。您可能会发现，一些注意事项和相应的影响指向不同的解决方案。在这种情况下，作为决策者，您可能需要在某些要求上做出让步，然后选择符合您的业务和技术要求的最佳解决方案。

贡献者

本文档的贡献者包括：

- Amazon Web Services 首席解决方案架构师 James Devine
- Amazon Web Services 首席网络解决方案架构师 Andrew Gray
- Amazon Web Services 高级解决方案架构师 Maks Khomutskyi
- Amazon Web Services 解决方案架构师 Marwan Al Shawi
- Amazon Web Services 技术主管 Santiago Freitas
- Amazon Web Services 专业网络解决方案架构师 Evgeny Vaganov
- Amazon Web Services 专业网络解决方案架构师 Tom Adamski
- Amazon Web Services 解决方案架构师 Armstrong Onaiwu

延伸阅读

- 构建可扩展的安全多 VPC AWS 网络基础设施
- Amazon VPC 的混合云 DNS 选项
- Amazon Virtual Private Cloud 连接性选项
- Amazon Virtual Private Cloud 文档
- AWS Direct Connect 文档
- 托管虚拟接口 (VIF) 和托管连接有什么区别？

文档修订

如需获取有关该白皮书更新的通知，请订阅 RSS 信息源。

变更	说明	日期
次要更新	已更新，反映了 DX 配额限制的提高。	2023 年 7 月 10 日
主要更新	已更新，纳入了最新的最佳实践、服务和功能。	2023 年 7 月 6 日
次要更新	更新了参考架构图，以反映 DX 配额的变化。	2023 年 6 月 27 日
次要更新	修复了断开的链接。	2022 年 3 月 22 日
初次发布	白皮书首次发布	2020 年 9 月 22 日

注意事项

客户有责任对本文档中的信息进行单独评测。本文档：(a) 仅供参考，(b) 代表当前的 AWS 产品和实践，如有更改，恕不另行通知，以及 (c) 不构成 AWS 及其附属公司、供应商或许可方的任何承诺或保证。AWS 产品或服务“按原样”提供，不附带任何明示或暗示的保证、陈述或条件。AWS 对其客户承担的责任和义务受 AWS 协议制约，本文档不是 AWS 与客户直接协议的一部分，也不构成对该协议的修改。

AWS 术语表

有关最新的 AWS 术语，请参阅《AWS 词汇表参考》中的 AWS 词汇表。

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。