AWS 白皮书

构建可扩展且安全的多 vPC AWS 网络基础架构

构建可扩展且安全的多 vPC AWS 网络基础架构: AWS 白皮书

Table of Contents

构建可扩展且安全的多 vPC AWS 网络基础架构

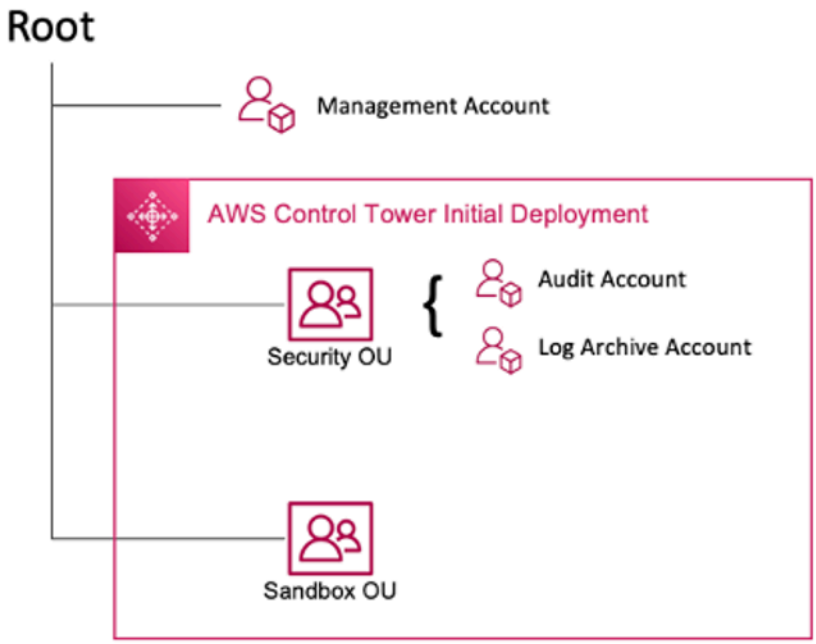
发布日期：2024 年 4 月 17 日 () 文档历史记录

Amazon Web Services (AWS) 客户通常依靠数百个账户和虚拟私有云 (VPC) 来分割其工作负载并扩大其覆盖范围。这种规模通常会给资源共享、VPC 间连接以及本地设施与 VPC 的连接带来挑战。

本白皮书介绍了使用亚马逊虚拟私有云 (Amazon VPC)、、、AWS Transit GatewayGateway Load Bal ancer 和 Amazon Rou te 53 等 AWS 服务在大型网络中创建可扩展且安全的网络架构的最佳实践。AWS PrivateLinkAWS Direct ConnectAWS Network Firewall它演示了管理不断增长的基础架构的解决方案——确保可扩展性、高可用性和安全性，同时保持较低的开销成本。

简介

AWS 客户首先在单个 AWS 账户中构建资源，该账户代表了划分权限、成本和服务的管理边界。但是，随着客户组织的发展，有必要对服务进行更细分，以监控成本、控制访问权限和提供更轻松的环境管理。多账户解决方案通过为组织内的 IT 服务和用户提供特定帐户来解决这些问题。 AWS 提供了多种工具来管理和配置此基础架构，包括AWS Control Tower。



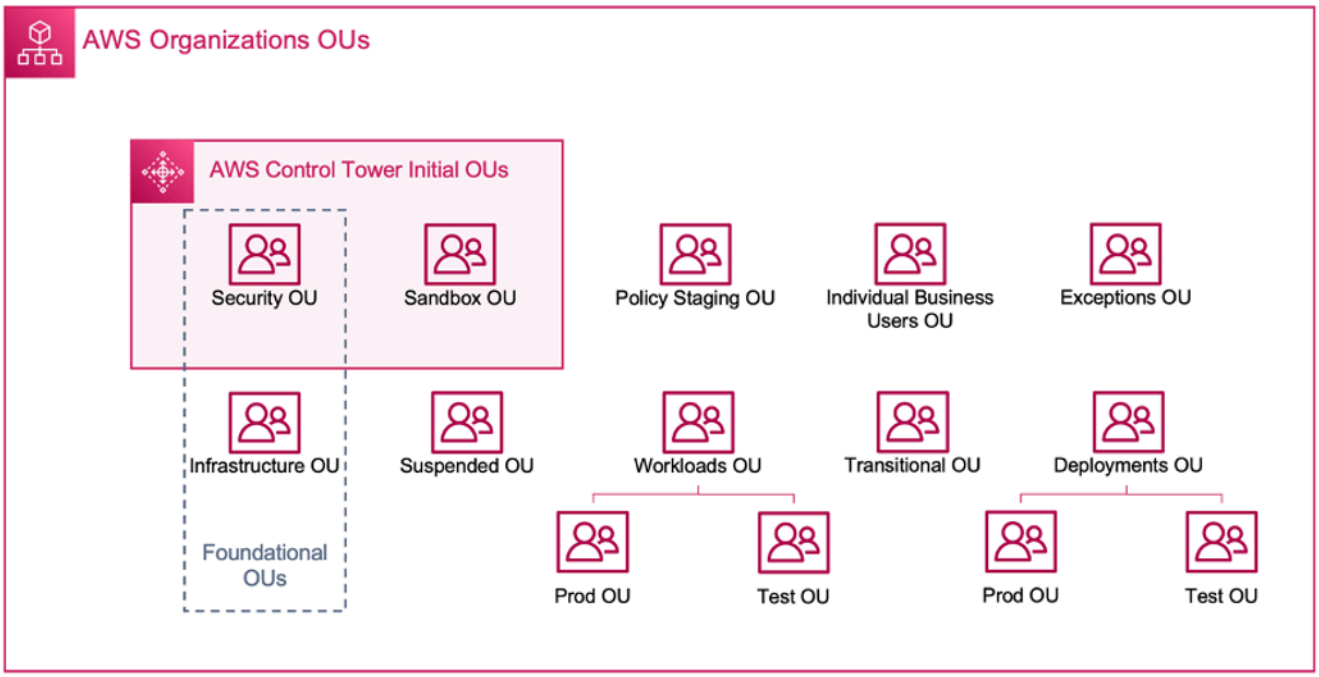
AWS Control Tower 的初始部署

当您使用设置多账户环境时 AWS Control Tower，它会创建两个组织单位 (OU)：

- 安全 OU — 在此 OU 中， AWS Control Tower 创建两个帐户：
- 日志存档
- 审计（此帐户对应于指南中前面讨论的安全工具帐户。）
- 沙箱 OU — 此 OU 是在其中创建的帐户的默认目的地。 AWS Control Tower它包含账户，您的构建者可以在这些账户中探索和试验 AWS 服务以及其他工具和服务，但须遵守团队的可接受使用政策。

AWS Control Tower 允许您创建、注册和管理其他 OU 以扩展初始环境以实施指南。

下图显示了最初由部署的 OU AWS Control Tower。您可以扩展您的 AWS 环境以实现图中包含的任何推荐的 OU，以满足您的需求。



AWS 组织 OU

有关使用多账户环境的更多详细信息 AWS Control Tower，请参阅《使用多个账户组织您的 AWS 环境》白皮书中的附录 E。

> **Note**
>
> 在本白皮书中，“Control Tower” 是一个宽泛的术语，指的是您在其中部署工作负载的可扩展、安全和高性能的多账户/多 VPC 设置。可以使用不同的工具来构建此设置。您可以在使用多个账户组织 AWS 环境白皮书中找到有关多账户云基础的最佳实践、设计原则和优势的更多信息。

大多数客户一开始就使用几个 VPC 来部署其基础架构。客户创建的 VPC 数量通常与其账户、用户和暂存环境（生产、开发、测试等）的数量有关。随着云使用量的增长，客户与之交互的用户、业务部门、应用程序和区域的数量也随之增长，从而产生了新的 VPC。

随着VPC数量的增长，跨VPC管理对于客户的云网络的运行变得至关重要。本白皮书涵盖了跨VPC和混合连接中三个特定领域的最佳实践：

- 网络连接 — 大规模互连 VPC 和本地网络。
- 网络安全 — 为访问互联网和终端节点（例如网络地址转换 (NAT) 网关、VPC 终端节点和网关负载均衡AWS PrivateLink器 AWS Network Firewall）建立集中式出口点。
- DNS 管理 — 在 Control Tower 中解析 DNS 和混合 DNS。

IP 地址规划和管理

为了构建可扩展的多账户多 VPC 网络设计，IP 地址规划和管理势在必行。一个好的 IP 寻址方案需要考虑您当前和未来的网络需求。您的 IP 地址方案 IP 需要涵盖您的本地工作负载、云工作负载，还应允许将来的扩展（例如，增加新的 AWS 区域业务部门以及合并或收购）。它还应防止您的团队无意中创建重叠的 IP CIDR。如果需要重叠 IP CIDR，例如对于隔离或断开连接的工作负载，则需要谨慎做出这一决定，并应考虑对路由、安全性和成本的影响。您可能还需要考虑为此类例外情况创建必要的批准流程。良好的 IP 寻址方案还有助于简化网络设计和路由配置。

重要注意事项：

- 预先规划 IP 寻址方案（包括公有和私有 IP），然后选择 IP 地址管理工具来分配、管理和跟踪所有工作负载的 IP 地址使用情况。
- 使用分层和汇总的 IP 寻址方案。
- 根据环境 AWS 区域、组织或业务部门规划一致的 IP 分配。
- 为本地网络和云网络指定不同的 IP CIDR（包括 IPv4 和 IPv6）。
- 主动防止和跟踪重叠的 IP CIDR。
- 适当调整您的 IP CIDR 的大小，以实现扩展和未来的增长。
- 为您的工作负载启用 IPv6 或双栈兼容性，以减少 IP 冲突并解决 IPv4 空间耗尽问题。

您可以使用 Amazon VPC IP 地址管理器 (IPAM) 来简化工作负载的公有和私有 IP 地址的规划、跟踪和监控。 AWS IPAM 允许您在多个 AWS 区域 和之间组织、分配、监控和共享 IP 地址空间。 AWS 账户它还有助于使用特定的业务规则将CIDR自动分配给VPC。

有关 AWS Control Tower博客文章，请参阅 Amazon VPC IP 地址管理器最佳实践、使用 Amazon VPC IP 地址管理器管理 VPC 和区域之间的 IP 池，以及 IP 地址管理，以了解 IP 寻址最佳实践以及如何使用 IPAM 在各个 VPC 之间管理 IP 池，以及。 AWS 区域 AWS Control Tower

您使用 Well-Architected 了吗？

当您在云端构建系统时，AWS Well-Architected Framework 可帮助您了解所做决策的利弊。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。

VPC 到 VPC 的连接

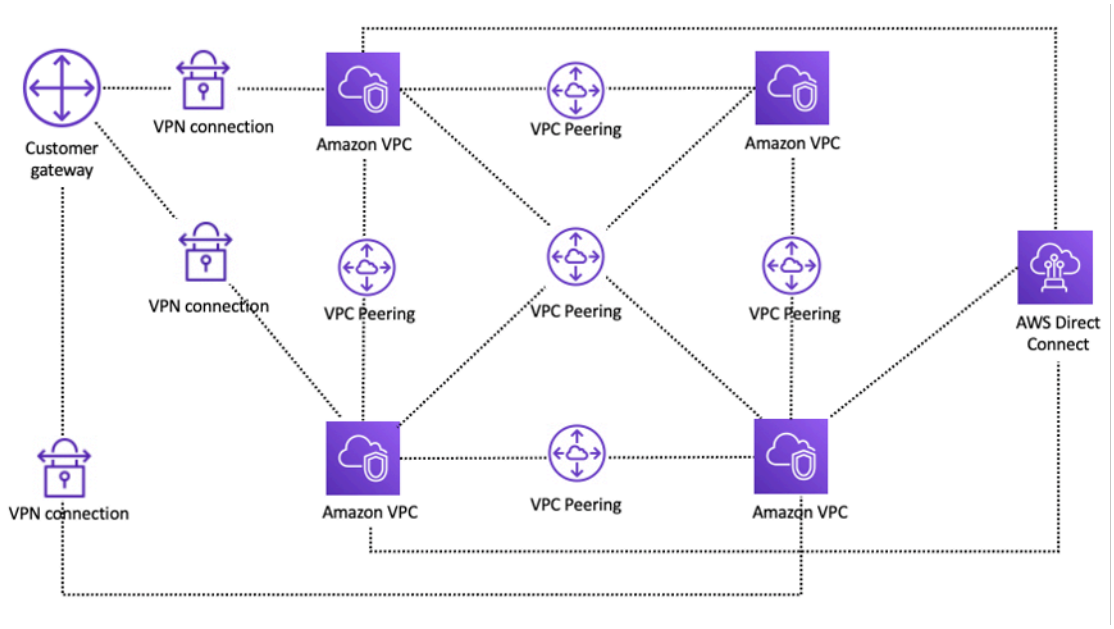
客户可以使用两种不同的 VPC 连接模式来设置多 VPC 环境：多对多，或者中心和分支。在该 many-to-many 方法中，每个 VPC 之间的流量在每个 VPC 之间单独管理。在该 hub-and-spoke 模型中，所有 VPC 间流量都流经中央资源，该资源根据既定规则路由流量。

VPC 对等连接

连接两个 VPC 的第一种方法是使用 VPC 对等连接。在此设置中，连接可实现 VPC 之间的完全双向连接。 此对等连接用于在 VPC 之间路由流量。 不同账户和 AWS 区域中的 VPC 也可以相互对等。通过位于可用区内的 VPC 对等连接进行的所有数据传输都是免费的。通过跨可用区的 VPC 对等连接进行的所有数据传输均按标准的区域内数据传输费率收费。如果 VPC 跨区域对等，则将收取标准的区域间数据传输费用。

VPC 对等 point-to-point 互连是连接，它不支持传递路由。例如，如果您在 VPC A 和 VPC B 之间以及 VPC A 和 VPC C 之间有 VPC 对等连接，则 VPC B 中的实例无法通过 VPC A 传输到达 VPC C。要在 VPC B 和 VPC C 之间路由数据包，您需要创建直接 VPC 对等连接。

从规模上看，当你有数十或数百个 VPC 时，将它们与对等互连可以形成成百上千个对等连接的网格。大量连接可能难以管理和扩展。例如，如果您有 100 个 VPC，并且想要在它们之间设置全网状对等连接，则需要 4,950 个对等连接 [n(n-1)/2]，其中 n VPC 的总数。每个 VPC 的最大活跃对等连接限制为 125 个。



使用 VPC 对等互连进行网络设置

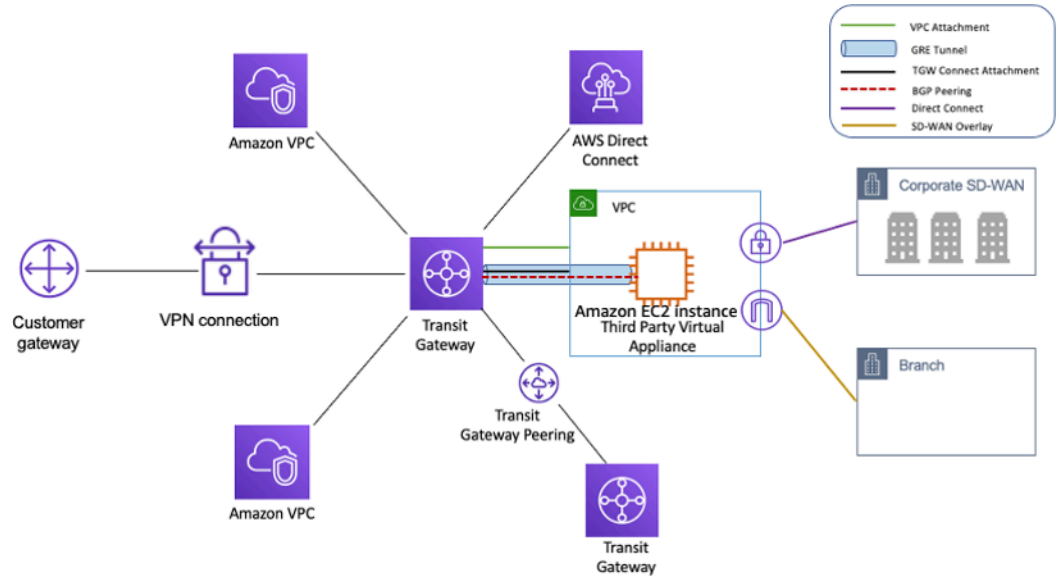
如果您使用的是 VPC 对等互连，则必须与每个 VPC 建立本地连接（VPN 和/或 Direct Connect）。使用对等 VPC 的混合连接，VPC 中的资源无法到达本地，如上图所示。

当一个 VPC 中的资源必须与另一个 VPC 中的资源通信，两个 VPC 的环境都受到控制和保护，并且要连接的 VPC 数量少于 10（以便对每个连接进行单独管理）时，最好使用 VPC 对等连接。与其他 VPC 间连接选项相比，VPC 对等连接可提供最低的总体成本和最高的聚合性能。

AWS Transit Gateway

AWS Transit Gateway提供中心辐射设计，无需您配置第三方虚拟设备，即可将 VPC 和本地网络作为一项完全托管的服务进行连接。不需要 VPN 叠加，可 AWS 管理高可用性和可扩展性。

Transit Gateway 使客户能够连接数千个 VPC。您可以将所有混合连接（VPN 和 Direct Connect 连接）连接到单个网关，从而在一个地方整合和控制组织的整个 AWS 路由配置（请参阅下图）。Transit Gateway 使用路由表控制流量在所有连接的分支网络之间路由的方式。这种 hub-and-spoke 模式简化了管理并降低了运营成本，因为 VPC 只能连接到 Transit Gateway 实例才能访问所连接的网络。



轮毂和辐条设计采用 AWS Transit Gateway

Transit Gateway 是一种区域资源，可以连接同 AWS 区域一个区域内的数千个 VPC。您可以通过单个 Direct Connect 连接连接多个网关，实现混合连接。通常，您只能使用一个 Transit Gateway 实例来连接给定区域中的所有 VPC 实例，并使用 Transit Gateway 路由表将它们隔离在任何需要的地方。请注意，您不需要额外的中转网关来实现高可用性，因为传输网关在设计上具有高可用性；要实现冗余，请在每个区域使用单个网关。但是，创建多个网关以限制配置错误的爆炸半径、隔离控制平面操作和管理是有道理的。 ease-of-use

通过 Transit Gateway 对等互连，客户可以在相同或多个区域内对其 Transit Gateway 实例进行对等，并在它们之间路由流量。它使用与 VPC 对等互连相同的底层基础架构，因此是加密的。有关更多信息，请参阅使用 AWS Transit Gateway 区域间对等连接构建全球网络，AWS Transit Gateway 现在支持区域内对等互连。

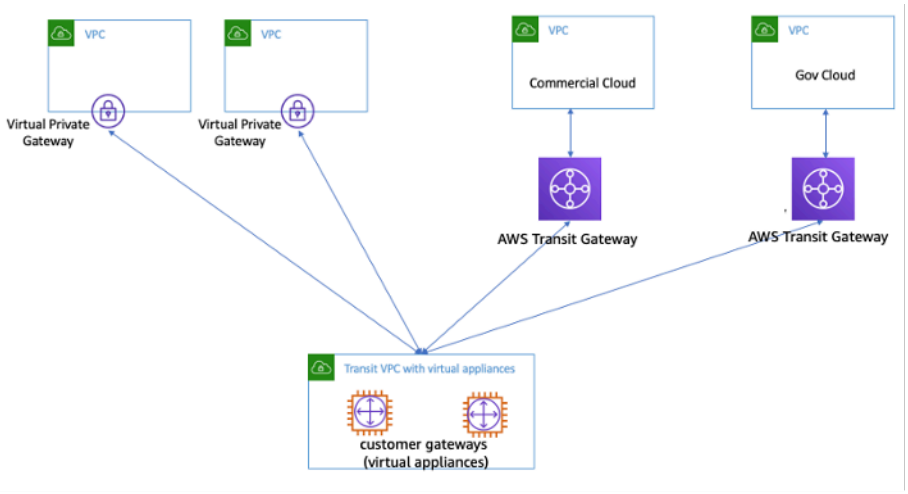
将贵组织的 Transit Gateway 实例存入其网络服务账户。这样，管理网络服务帐户的网络工程师就可以进行集中管理。使用 Res AWS ource Access Manager (RAM) 共享 Transit Gateway 实例，用于在同一区域内 AWS 组织中的多个账户之间连接 VPC。AWS RAM 使您能够轻松安全地与任何人共享 AWS 资源 AWS 账户，或者在您的 AWS 组织内部共享资源。有关更多信息，请参阅中央账户博客文章中的“自动化 AWS Transit Gateway 到公交网关的附件”。

Transit Gateway 还允许您在软件定义广域网基础设施和 AWS 使用 Transit Gateway Connect 之间建立连接。使用带有边界网关协议 (BGP) 的 Transit Gateway Connect 附件进行动态路由，使用通用路由封装 (GRE) 隧道协议实现高性能，每个连接可提供高达 20 Gbps 的总带宽（每个 Connect 连接最多四个 Transit Gateway Connect 对等体）。通过使用 Transit Gateway Connect，您可以将本地 SD-WAN 基础设施或通过作为底层传输层的 VPC 连接或 AWS Direct Connect 附件集成在云中运行的 SD-WAN 设备。有关参考架构和详细配置，请参阅使用 Conn AWS Transit Gateway ect 简化 SD-WAN 连接。

传输 VPC 解决方案

Transit VPC 可以通过与 VPC 对等互连不同的方式在 VPC 之间创建连接，方法是引入中心和辐条设计来实现 VPC 间连接。在中转 VPC 网络中，一个中央 VPC（中心 VPC）通过 VPN 连接与所有其他 VPC（分支 VPC）相连，该连接通常利用基于 IP sec 的 BGP。中央 VPC 包含运行软件设备的亚马逊弹性计算云 (Amazon EC2) 实例，这些实例使用 VPN 叠加层将传入流量路由到目的地。传输 VPC 对等互连具有以下优势：

- 使用覆盖 VPN 网络启用传递路由，允许采用中心辐射式设计。
- 在中心交通 VPC 中的 EC2 实例上使用第三方供应商软件时，可以使用围绕高级安全（第 7 层防火墙/入侵防御系统 (IPS) /入侵检测系统 (IDS)）的供应商功能。如果客户在本地使用相同的软件，他们将受益于统一的操作/监控体验。
- Transit VPC 架构可实现某些用例中可能需要的连接。例如，您可以将 AWS GovCloud 实例和商业区域 VPC 或 Transit Gateway 实例连接到 Transit VPC，并在两个区域之间启用 VPC 间连接。在考虑此选项时，请评估您的安全和合规性要求。为了提高安全性，您可以使用本白皮书后面介绍的设计模式部署集中检查模型。



使用虚拟设备传输 VPC

Transit VPC 有其自身的挑战，例如根据实例大小/系列在 EC2 上运行第三方供应商虚拟设备的成本更高，每个 VPN 连接的吞吐量有限（每个 VPN 隧道高达 1.25 Gbps），以及额外的配置、管理和弹性开销（客户负责管理运行第三方供应商虚拟设备的 EC2 实例的高可用性和冗余）。

VPC 对等互连与传输 VPC 与 Transit Gateway

表 1 — 连接比较

标准	VPC 对等连接	传输 VPC	Transit Gateway	PrivateLink	Cloud WAN	VPC Lattice
范围	区域/全球	区域性	区域性	区域性	全局	区域性
架构	全网状	基于 VPN hub-and-spoke	基于附件 hub-and-spoke	提供者或消费者模型	基于附件、多区域	应用程序到应用程序的连接
扩展	125 个活跃的对等体/v	取决于虚拟路由器/EC2	每个区域 5000 个附件	没有限制	每个核心网络 5000 个附件	每项服务 500 个 VPC 关联
客户细分	安全组	由客户管理	TransitGateway 路由表	没有分割	分段	服务和服务网络政策

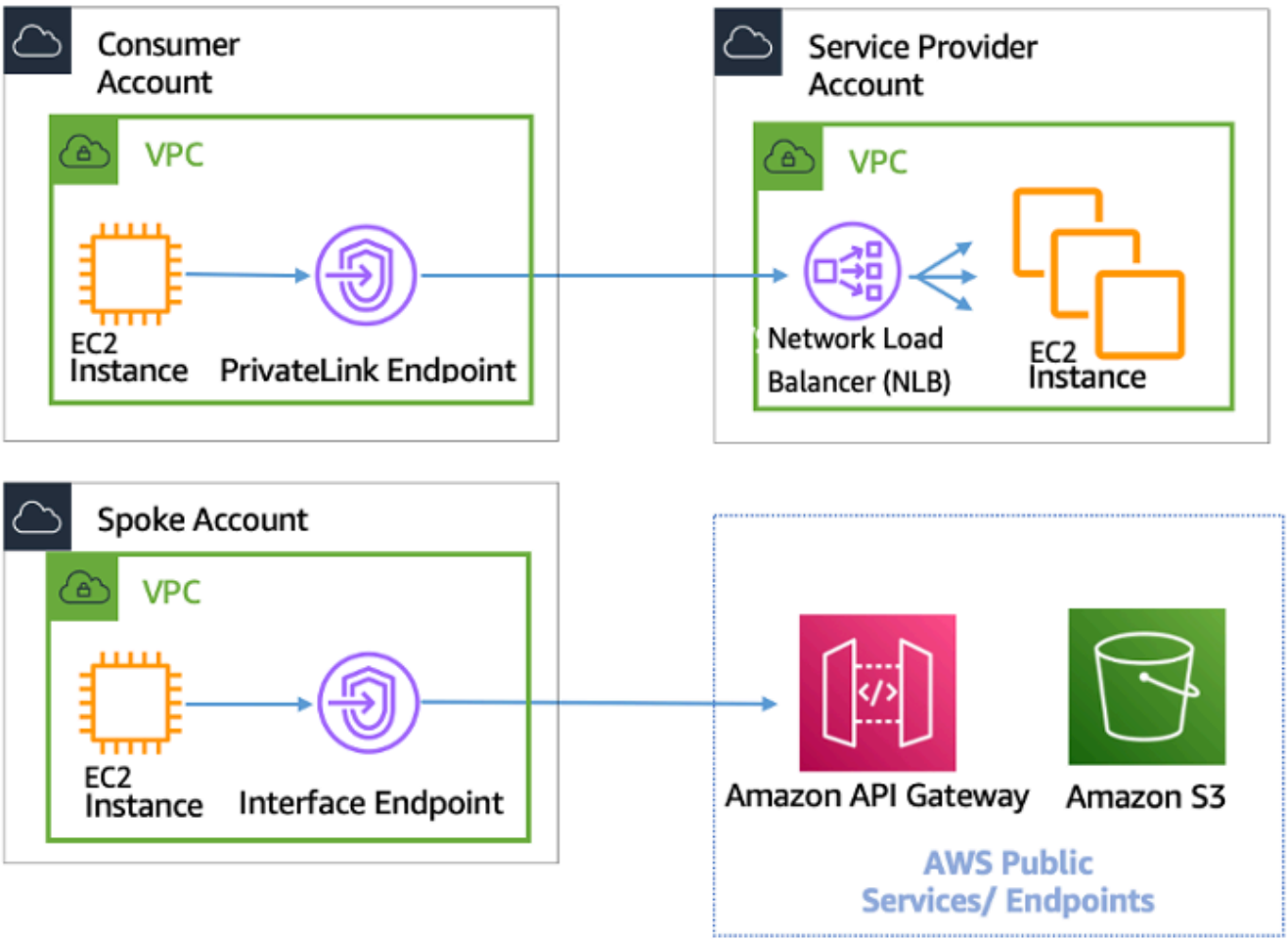
标准	VPC 对等连接	传输 VPC	Transit Gateway	PrivateLink	Cloud WAN	VPC Lattice
延迟	最低	额外费用，由于 VPN 加密开销	更多 Transit Gateway	流量保持在 AWS 主干上，客户应进行测试	使用与 Transit Gateway 相同的数据平面	流量保持在 AWS 主干上，客户应进行测试
带宽限制	每个实例的限制，没有聚合限制	受基于大小/系列的 EC2 实例带宽限制	高达 100 Gbps（连发）/附件	每个可用区 10 Gbps，可自动扩展到 100 Gbps	高达 100 Gbps（连发）/附件	每个可用区 10 Gbps
Visibility	Amazon VPC 流日志	VPC 流日志和 CloudWatch 指标	Transit Gateway 网络管理器、VPC 流日志、CloudWatch 指标	CloudWatch 指标	网络管理器、VPC 流日志、CloudWatch 指标	CloudWatch 访问日志
安全组交叉引用	支持	不支持	不支持	不支持	不支持	不适用
IPv6 支持	支持	取决于虚拟设备	支持	支持	支持	支持

AWS PrivateLink

AWS PrivateLink在 VPC、AWS 服务和您的本地网络之间提供私有连接，而不会将您的流量暴露给公共互联网。由 AWS PrivateLink提供支持的接口 VPC 终端节点可以轻松地跨不同的账户 AWS 和 VPC 连接到其他服务，从而显著简化您的网络架构。这允许那些可能希望私下向其他 VPC（服务提供商）公开位于一个 VPC 中的服务/应用程序的客户（使用者），其方式是 AWS 区域 只有使用者 VPC 才能启动与服务提供商 VPC 的连接。例如，您的私有应用程序能够访问服务提供商 API。

要使用 AWS PrivateLink，请在您的 VPC 中为您的应用程序创建一个 Network Load Balancer，然后创建指向该负载均衡器的 VPC 终端节点服务配置。然后，服务使用者为您的服务创建接口终端节点。这将在使用者子网中创建一个弹性网络接口 (ENI)，其私有 IP 地址用作发往该服务的流量的入口点。消费者和服务不必位于同一 VPC 中。如果 VPC 不同，则消费者和服务提供商 VPC 的 IP 地址范围可能会重叠。除了创建接口 VPC 终端节点以访问其他 VPC 中的服务外，您还可以创建接口 VPC 终端节点以通过私密访问支持的 AWS 服务 AWS PrivateLink，如下图所示。

将 Application Load Balancer (ALB) 作为 NLB 的目标，您现在可以将 ALB 的高级路由功能与。 AWS PrivateLink有关参考架构和详细配置，请参阅 Network Load Balancer 的应用程序负载均衡器类型的目标组。



AWS PrivateLink 用于连接到其他 VPC 和 AWS 服务

Transit Gateway、VPC 对等互连和 AWS PrivateLink 之间的选择取决于连接情况。

- AWS PrivateLink— AWS PrivateLink 在您的客户端/服务器设置中要允许一个或多个使用者 VPC 单向访问服务提供商 VPC 或某些服务中的特定服务或一组实例时使用。 AWS 只有在使用者 VPC 中具有访问权限的客户端才能发起与服务提供商 VPC 或 AWS 服务中的服务的连接。当两个 VPC 中的客户端和服务器的 IP 地址重叠时，这也是一个不错的选择，因为在客户端 VPC 中 AWS PrivateLink 使用 ENI 的方式可以确保与服务提供商没有 IP 冲突。您可以通过 VPC 对等互连、VPN、Transit Gateway、Cloud WAN 和 AWS Direct Connect访问 AWS PrivateLink 终端节点。
- VPC 对等互连和 Transit Gateway — 如果要在 VPC 之间启用第 3 层 IP 连接，请使用 VPC 对等互连和 Transit Gateway。

  您的架构将混合使用这些技术，以满足不同的用例。所有这些服务都可以相互组合和操作。例如，AWS PrivateLink 处理 API 风格的客户端-服务器连接、VPC 对等以处理区域内可能仍需要置放群组或区域间连接的直接连接需求，以及 Transit Gateway 来简化 VPC 的大规模连接，以及用于混合连接的边缘整合。

VPC 共享

当团队之间的网络隔离不需要由 VPC 所有者严格管理，但必须严格管理账户级别的用户和权限时，共享 VPC 非常有用。使用共享 VPC，多个 AWS 账户在共享的、集中管理的 Amazon VPC 中创建其应用程序资源（例如 Amazon EC2 实例）。在此模型中，拥有 VPC 的账户（所有者）与其他账户（参与者）共享一个或多个子网。共享子网之后，参与者可以查看、创建、修改和删除与他们共享的子网中的应用程序资源。参与者无法查看、修改或删除属于其他参与者或 VPC 拥有者的资源。共享 VPC 中资源之间的安全使用安全组、网络访问控制列表 (NACL) 或通过子网之间的防火墙进行管理。

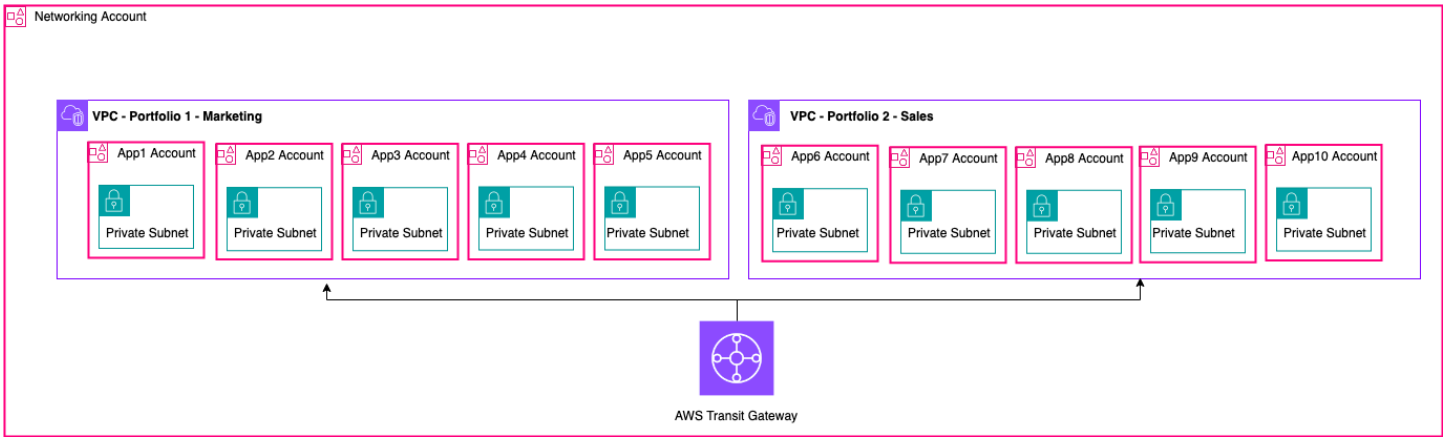
VPC 共享的好处：

- 简化的设计 — VPC 间连接没有复杂性
- 更少的托管 VPC
- 网络团队和应用程序所有者之间的职责分离
- 更高的 IPv4 地址利用率
- 更低的成本 — 在属于同一可用区内不同账户的实例之间不收取数据传输费用

> **Note**
>
> 当您与多个账户共享子网时，您的参与者应该有一定程度的合作，因为他们共享 IP 空间和网络资源。如有必要，您可以选择为每个参与者账户共享不同的子网。每个参与者一个子网使网络 ACL 除了安全组之外还能提供网络隔离。

大多数客户架构将包含多个 VPC，其中许多将与两个或更多账户共享。Transit Gateway 和 VPC 对等连接可用于连接共享 VPC。例如，假设您有 10 个应用程序。每个应用程序都需要自己的 AWS 账户。这些应用程序可以分为两个应用程序组合（同一产品组合中的应用程序具有相似的网络要求，“营销” 中的 App 1—5 和 “销售” 中的 App 6—10）。

每个应用程序组合可以有一个 VPC（总共两个 VPC），并且该 VPC 与该产品组合中的不同应用程序所有者账户共享。应用程序所有者将应用程序部署到各自的共享 VPC（在本例中，在不同的子网中使用 NACL 进行网络路由分段和隔离）。两个共享 VPC 通过 Transit Gateway 连接。通过这种设置，您可以从必须连接 10 个 VPC 变为仅连接 2 个，如下图所示。

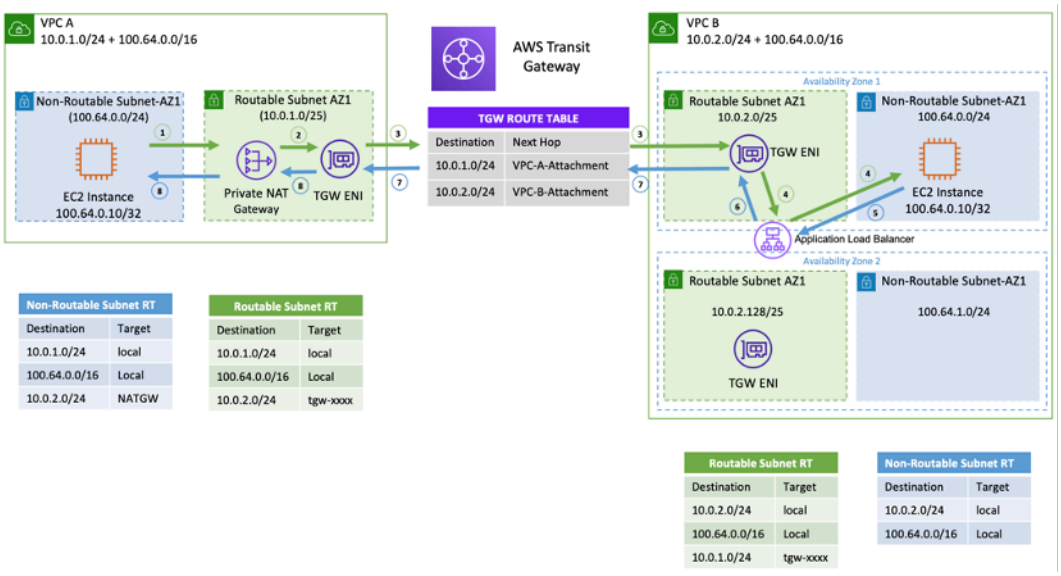


设置示例 — 共享 VPC

> **Note**
>
> VPC 共享参与者无法在共享子网中创建所有 AWS 资源。有关更多信息，请参阅 VPC 共享文档中的限制部分。
>
> 有关 VPC 共享的关键注意事项和最佳实践的更多信息，请参阅 VPC 共享：关键注意事项和最佳实践博客文章。

私有 NAT 网关

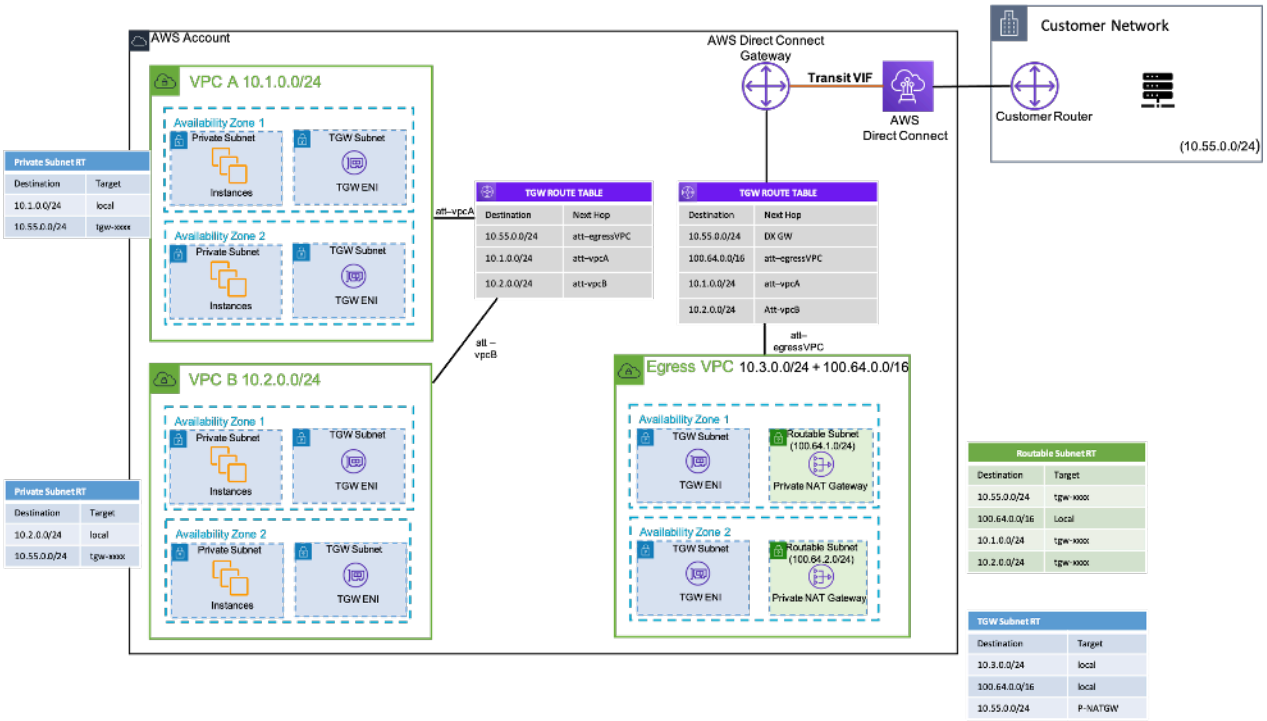
团队通常独立工作，他们可能会为项目创建一个新的 VPC，该项目可能有重叠的无类域间路由 (CIDR) 块。为了实现集成，他们可能希望在具有重叠的 CIDR 的网络之间启用通信，而通过 VPC 对等互连和 Transit Gateway 等功能无法实现这一点。私有 NAT 网关可以帮助解决这个用例。私有 NAT 网关使用唯一的私有 IP 地址为重叠的源 IP 地址执行源 NAT，而 ELB 对重叠的目标 IP 地址执行目标 NAT。您可以使用 Transit Gateway 或虚拟私有网关将流量从私有 NAT 网关路由到其他 VPC 或本地网络。



设置示例-私有 NAT 网关

上图显示了 VPC A 和 B 中的两个不可路由（重叠 CIDR）100.64.0.0/16子网。要在它们之间建立连接，您可以分别向 VPC A 和 B 添加辅助非重叠/可路由的 CIDR（可路由子网和）。10.0.1.0/24 10.0.2.0/24可路由的 CIDR 应由负责 IP 分配的网络管理团队分配。私有 NAT 网关已添加到 VPC A 中的可路由子网中，IP 地址为。10.0.1.125私有 NAT 网关对来自 VPC A (100.64.0.10) 不可路由子网中的实例的请求执行源网络地址转换10.0.1.125，就像私有 NAT 网关的 ENI 一样。现在，流量可以指向分配给 VPC B () 中的 Application Load Balancer (ALB10.0.2.10) 的可路由 IP 地址，其目标为。100.64.0.10流量通过 Transit Gateway 路由。返回流量由私有 NAT 网关处理返回到请求连接的原始 Amazon EC2 实例。

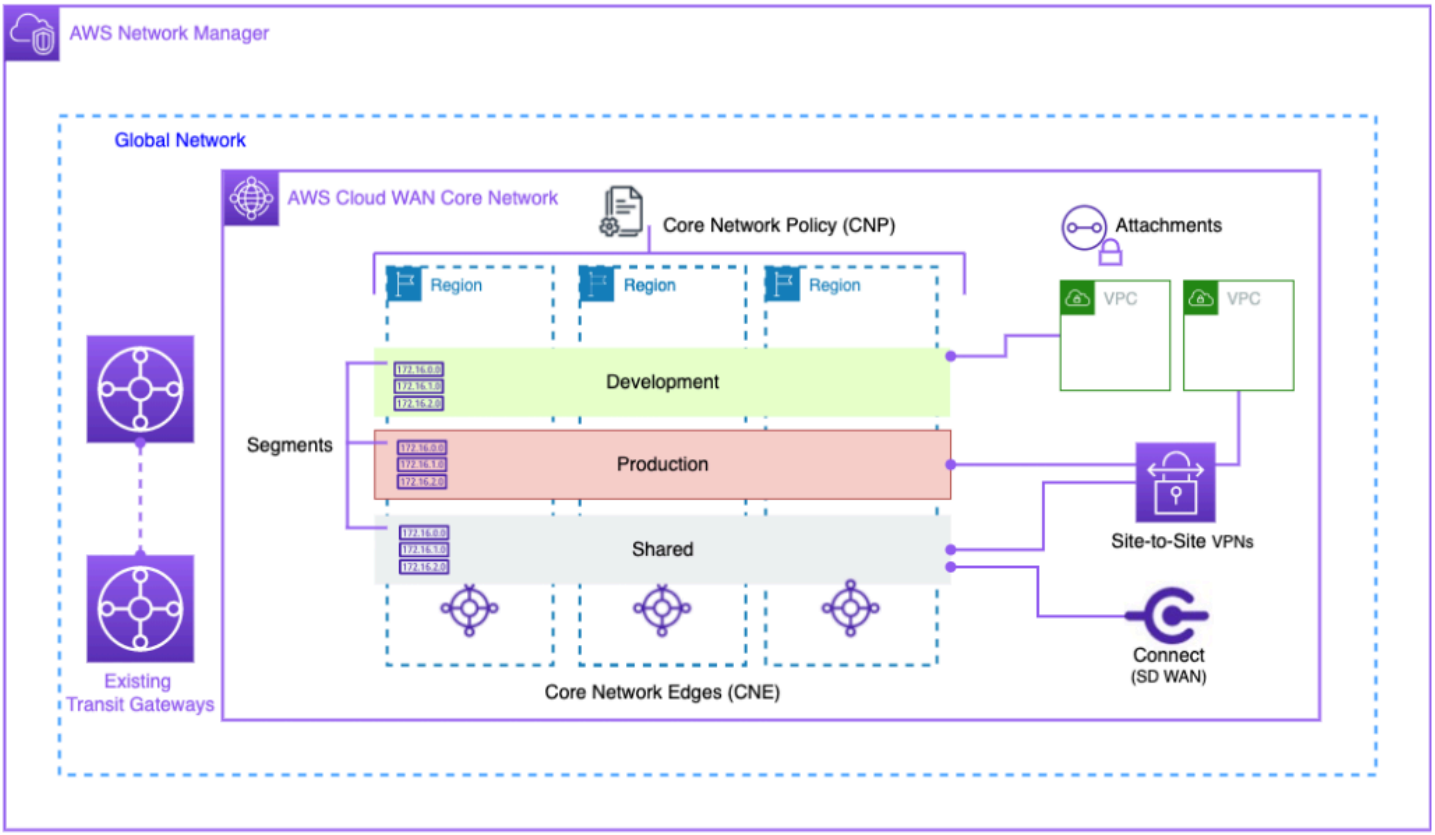
当您的本地网络限制对已批准的 IP 的访问时，也可以使用私有 NAT 网关。合规性要求少数客户的本地网络只能通过客户拥有的有限连续批准的 IP 块与私有网络（没有 IGW）通信。您可以使用私有 NAT 网关在每个允许名单 IP 后面的 AWS VPC 上运行大型工作负载，而不必为每个实例分配一个与区块分开的 IP。有关详细信息，请参阅如何使用私有 NAT 解决方案解决私有 IP 耗尽问题博客文章。



设置示例-如何使用私有 NAT 网关为本地网络提供经批准的 IP

AWS 云广域网

AWS Cloud WAN 是一种将网络连接在一起的新方式，这是我们以前通过传输网关、VPC 对等互连和 IPSEC VPN 隧道所能做到的。以前，您需要配置一个或多个 VPC，使用前面的方法之一将它们连接在一起，然后使用 IPSEC VPN 或 AWS Direct Connect 连接到本地网络。你可以在一个地方定义网络和安全态势结构，在另一个地方定义网络。Cloud WAN 允许您将所有这些结构集中在一个地方。根据策略，您可以对网络进行细分以确定谁可以与谁通信，并将通过这些分段的生产流量与开发或测试工作负载或本地网络隔离开来。



云广域网方框图

通过网络管理器用户界面和 API 管理您的全球 AWS 网络。全球网络是所有网络对象的根级容器；核心网络是由 AWS 管理的全球网络的一部分。核心网络策略 (CNP) 是一份单版本化策略文档，它定义了核心网络的各个方面。附件是您想要添加到核心网络的任何连接或资源。核心网络边缘 (CNE) 是符合政策的附件的本地连接点。网段是路由域，默认情况下，它只允许在分段内进行通信。

要使用 CloudWAN：

1. 在 AWS 网络管理器中，创建全球网络和相关的核心网络。
2. 创建一个 CNP，用于定义区段、ASN 范围 AWS 区域 和用于附加到区段的标签。
3. 应用网络策略。
4. 使用资源访问管理器与您的用户、账户或组织共享核心网络。
5. 创建和标记附件。
6. 更新连接的 VPC 中的路由，使其包含核心网络。

Cloud WAN 旨在简化全球连接 AWS 基础设施的流程。它允许您使用集中权限策略对流量进行分段，并在公司所在地使用现有的基础架构。云广域网还可以连接您的 VPC、软件定义广域网、客户端

VPN、防火墙、VPN 和数据中心资源，以连接到云广域网。有关更多信息，请参阅 AWS 云广域网博客文章。

AWS Cloud WAN 支持连接云和本地环境的统一网络。Organizations 使用下一代防火墙 (NGFW) 和入侵防御系统 (IPS) 来确保安全。AWS Cloud WAN 和 Transit Gateway 迁移和互操作模式博客文章描述了集中管理和检查云广域网网络中的出站网络流量（包括单区域和多区域网络）的架构模式，并配置了路由表。这些架构可确保数据和应用程序保持安全，同时维护安全的云环境。

有关云广域网的更多信息，请参阅 AWS Cl oud WAN 博客文章中的集中式出站检查架构。

Amazon VPC Lattice

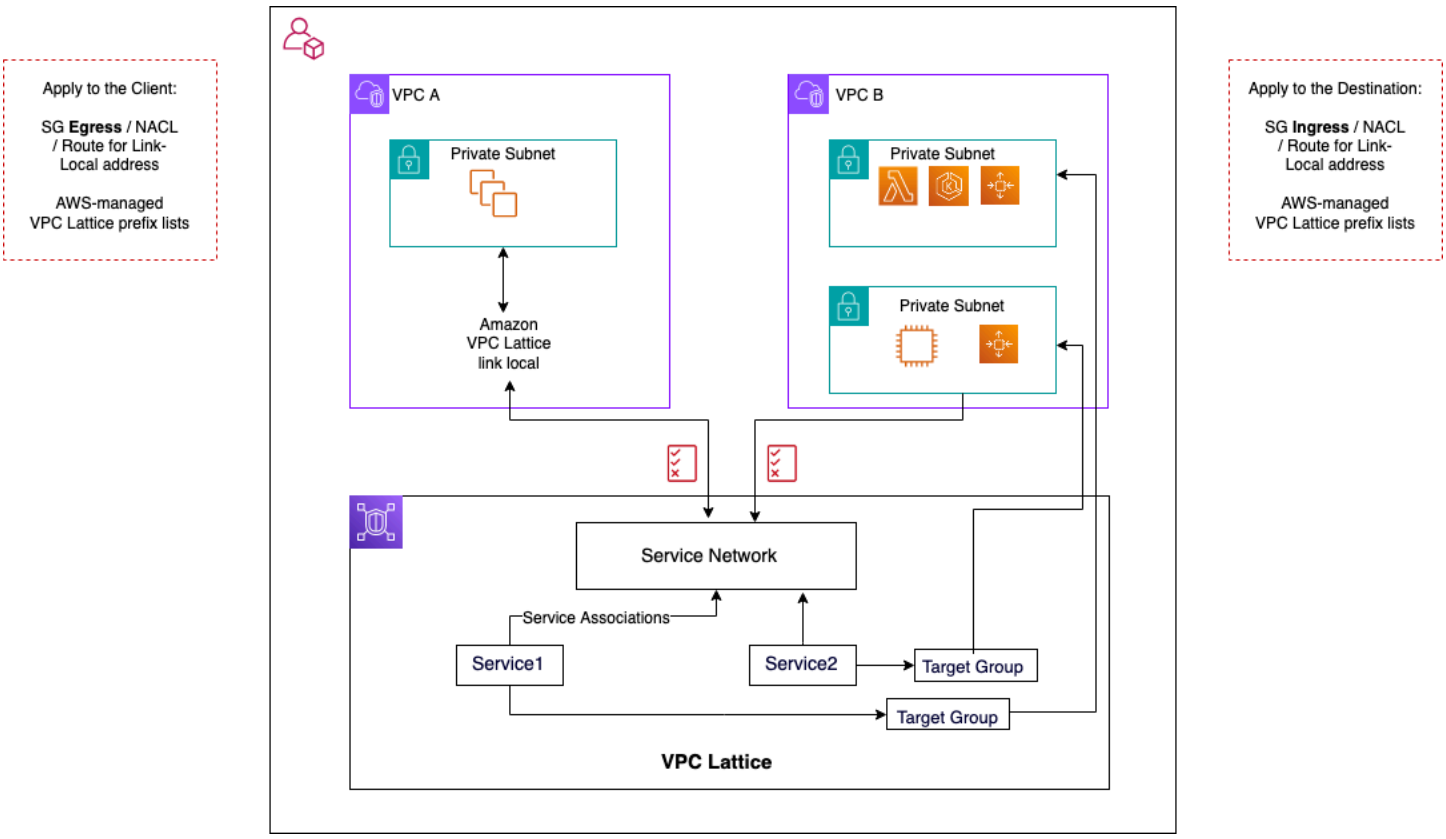
Amazon VPC Lattice 是一项完全托管的应用程序联网服务，用于跨各种账户和虚拟私有云连接、监控和保护服务。VPC Lattice有助于在逻辑边界内互连服务，以便您可以高效地管理和发现它们。

VPC 莱迪思组件包括：

- 服务-这是在实例、容器或 Lambda 函数上运行的应用程序单元，由侦听器、规则和目标组组成。
- 服务网络-这是逻辑边界，用于自动实现服务发现和连接，并将通用访问和可观察性策略应用于一组服务。
- 身份验证策略-可以与服务网络或单个服务关联的 IAM 资源策略，以支持请求级身份验证和特定于上下文的授权。
- 服务目录-您拥有的服务或通过 AWS Resource Access Manager 与您共享的服务的集中视图。

VPC Lattice 使用步骤：

1. 创建服务网络。服务网络通常位于网络管理员拥有完全访问权限的网络帐户上。服务网络可以在组织内的多个账户之间共享。可以对单个服务或整个服务帐户进行共享。
2. 将 VPC 连接到服务网络，为每个 VPC 启用应用程序联网，这样不同的服务就可以开始使用在网络中注册的其他服务。应用安全组来控制流量。
3. 开发人员定义服务，这些服务将填充到服务目录中并注册到服务网络中。VPC Lattice 包含所有已配置服务的地址簿。开发人员还可以定义路由策略以使用蓝/绿部署。安全性在定义身份验证和授权策略的服务网络级别和实施 IAM 访问策略的服务级别进行管理。



VPC 莱迪思通信流

更多详情可在 VPC Lattice用户指南中找到。

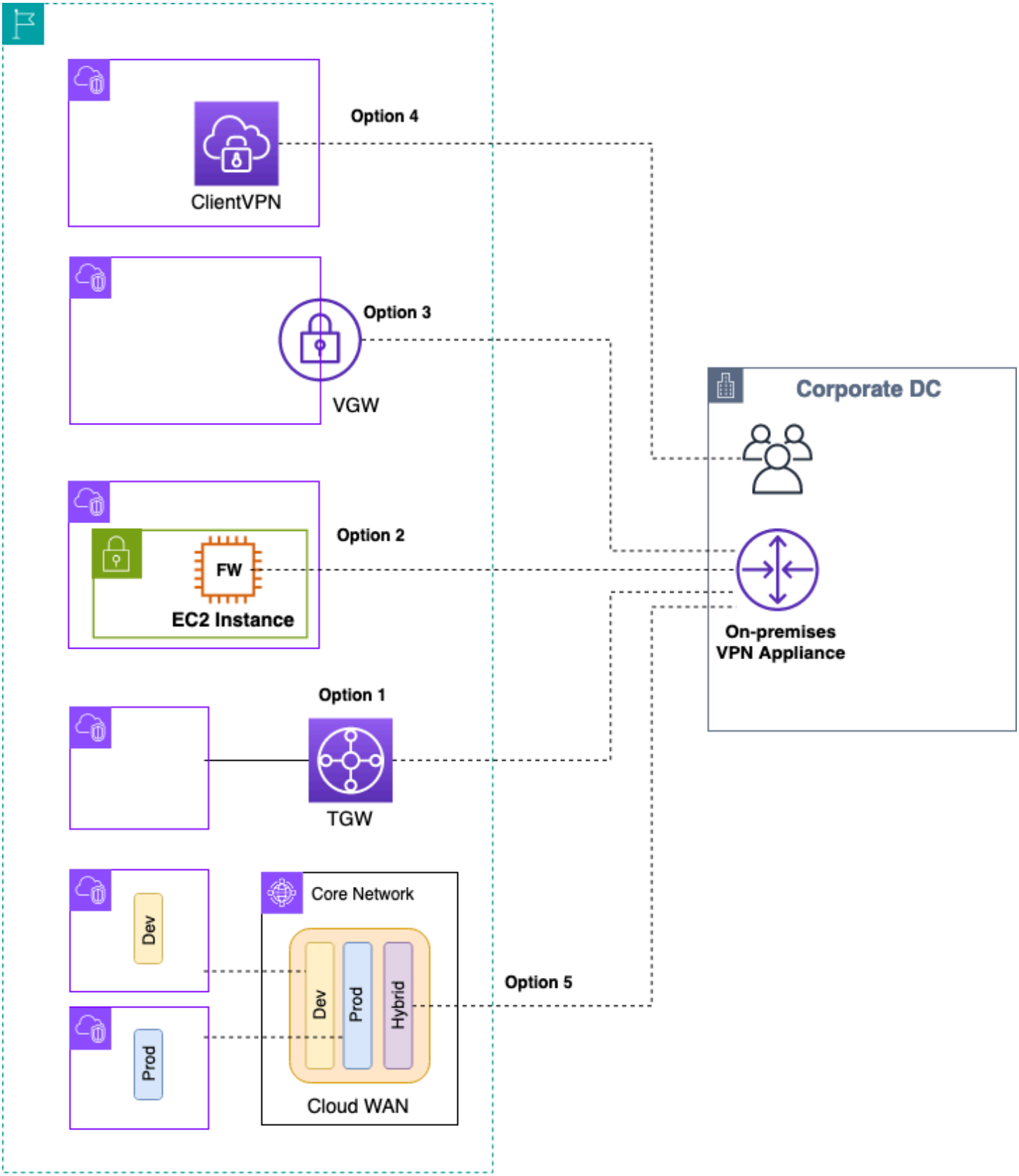
混合连接

本节重点介绍如何安全地将您的云资源与本地数据中心连接起来。启用混合连接的方法有三种：

- O ne-to-one 连接 — 在此设置中，将为每个 VPC 创建 VPN 连接和/或 Direct Connect 私有 VIF。这是通过使用虚拟专用网关 (VGW) 来实现的。此选项非常适合少量 VPC，但是随着客户扩展 VPC，管理每个 VPC 的混合连接可能会变得困难。
- 边缘整合 — 在此设置中，客户可以在单个端点整合多个 VPC 的混合 IT 连接。所有 VPC 共享这些混合连接。这是通过使用 AWS Transit Gateway 和 AWS Direct Connect 网关来完成的。
- 全网状混合整合 — 在此设置中，客户使用内置的 CloudWAN 在单个端点上整合多个 VPC 的连接。 AWS Transit Gateway这是一种基于策略的完整方法，用于在一个或多个 AWS 账户中进行联网，用代码表示。目前，使用 AWS Direct Connect 边缘连接需要将 Transit Gateway 对等连接到 CloudWAN。

VPN

有多种方法可以设置到 AWS 的 VPN：


Option 4
ClientVPN
Option 3
VGW
Corporate DC
Option 2
FW
EC2 Instance
On-premises
VPN Appliance
Option 1
TGW
Core Network
Dev
Prod
Dev
Prod
Hybrid
Option 5
Cloud WAN

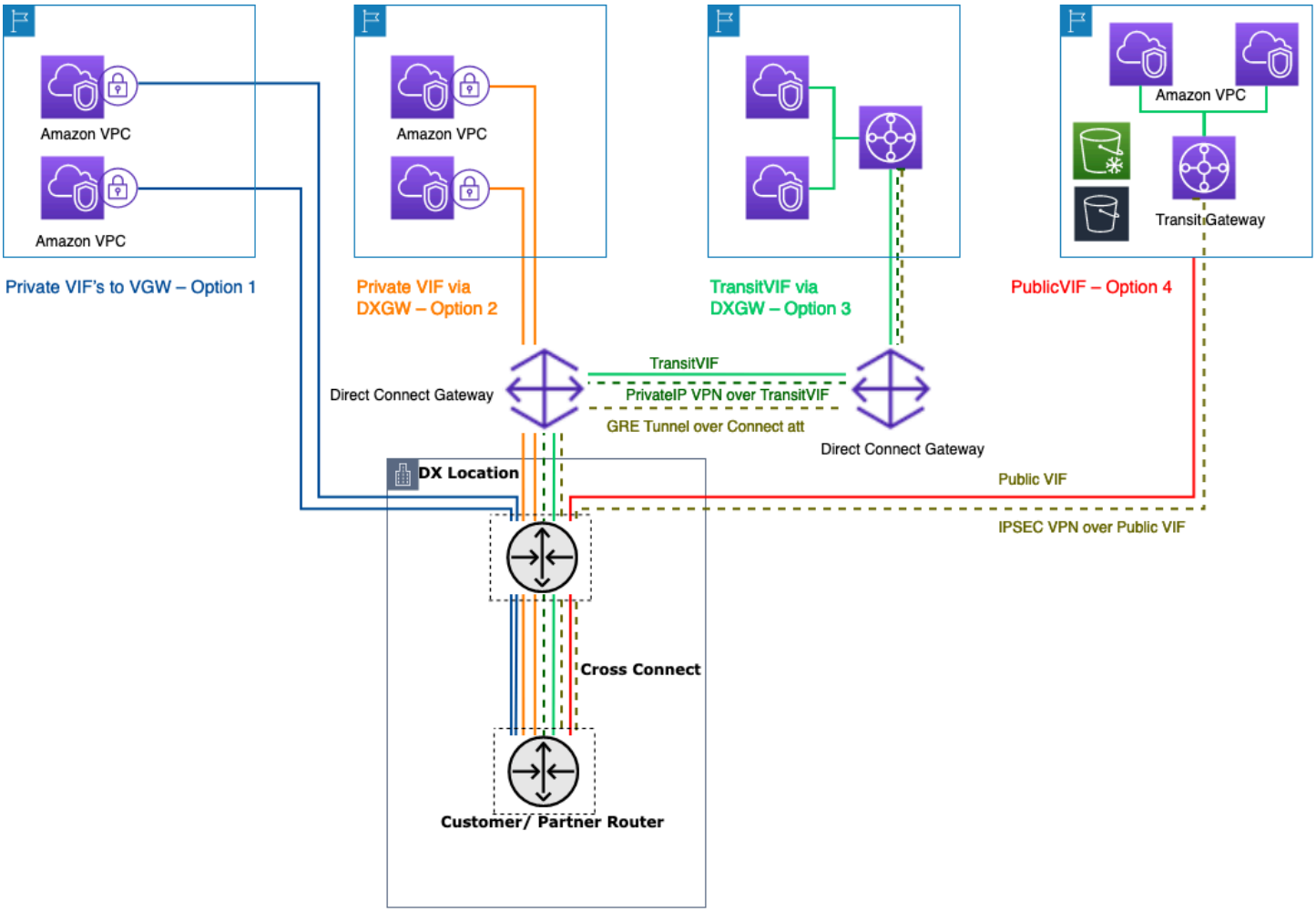
AWS VPN 选项

- 选项 1：在公交网关上整合 VPN 连接 — 此选项利用 Transit Gateway 上的 Transit Gateway VPN 附件。Transit Gateway 支持 site-to-site VPN 的 IPsec 终止 客户可以创建通往 Transit Gateway 的 VPN 隧道，并可以访问与其连接的 VPC。Transit Gateway 支持静态和基于 BGP 的动态 VPN 连接。Transit Gatew ay 还支持 VPN 连接上的等价多路径 (ECMP)。每个 VPN 连接的每个隧道的最大吞吐量为 1.25 Gbps。启用 ECMP 允许您汇总各个 VPN 连接的吞吐量，从而允许扩展到超出默认的最大限制 1.25 Gbps。在此选项中，您需要为 T ransit Gateway 的定价和定AWS VPN 价付费。AWS 建议使用此选项进行 VPN 连接。有关更多信息，请参阅使用 AWS Transit Gateway 扩展 VPN 吞吐量博客文章。
- 选项 2：终止 Amazon EC2 实例上的 VPN — 在边缘情况下，当客户需要特定的供应商软件功能集（例如 Cisco DMVPN 或通用路由封装 (GRE)），或者他们希望在各种 VPN 部署之间保持操作一致性时，可以利用此选项。您可以使用传输 VPC 设计进行边缘整合，但请务必记住，中转 VPC VPC 到 VPC 的连接 部分中的所有关键注意事项都适用于混合 VPN 连接。您负责管理高可用性，并为 EC2 实例以及任何供应商的软件许可和支持费用付费。
- 选项 3：在虚拟专用网关 (VGW) 上终止 V PN — 此 AWS 站点到站点 VPN 服务选项 one-to-one 支持连接设计，即每个 VPC 创建一个 VPN 连接（由一对冗余 VPN 隧道组成）。这是开始使用 VPN 连接到 AWS 的好方法，但是随着您扩展 VPC 的数量，管理越来越多的 VPN 连接可能会变得具有挑战性。因此，利用 Transit Gateway 的边缘整合设计最终将是一个更好的选择。VGW 的 VPN 吞吐量限制为每条隧道 1.25 Gbps，并且不支持 ECMP 负载平衡。从定价角度来看，您只需为 AWS VPN 定价付费，运行 VGW 不收取任何费用。有关更多信息，请参阅定AWS VPN 价和AWS VPN 虚拟专用网关。
- 选项 4：终止客户端 VPN 终端节点上的 VPN 连接 — AWS Client VPN 是一项基于客户端的托管 VPN 服务，可让您安全地访问本地网络中的 AWS 资源和资源。借助 Client VPN，您可以使用 OpenVPN 或 AWS 提供的 VPN 客户端从任何位置访问您的资源。通过设置 Client VPN 端点，客户端和用户可以进行连接以建立传输层安全 (TLS) VPN 连接。有关更多信息，请参阅 AWS Client VPN 文档。
- 选项 5：在 AWS Cloud WAN 上整合 VPN 连接 — 此选项与此列表中的第一个选项类似，但它使用 CloudWAN 架构通过网络策略文档以编程方式配置 VPN 连接。

AWS Direct Connect

虽然互联网上的VPN是一个不错的入门选择，但对于生产流量，互联网连接可能不可靠。由于这种不可靠性，许多客户选择AWS Direct Connect了。 AWS Direct Connect 是一项网络服务，除了使用互联网连接到 AWS 之外，它还提供了一种替代方案。使用 AWS Direct Connect，以前本应通过 Internet 传输的数据通过您的设施与 AWS 之间的私有网络连接传输。在许多情况下，与基于互联网的连接相

比，专用网络连接可以降低成本、增加带宽并提供更稳定的网络体验。有几种方法可以 AWS Direct Connect 用来连接 VPC：



使用以下方法连接本地数据中心 AWS Direct Connect

- 选项 1：为连接到 VPC 的 VGW 创建私有虚拟接口 (VIF) — 您可以为每个 Direct Connect 连接创建 50 个 VIF，允许您连接最多 50 个 VPC（一个 VIF 提供与一个 VPC 的连接）。每个 VPC 有一个 BGP 对等互连。此设置中的连接仅限于 Direct Connect 位置所在的 AWS 区域。VIF 与 VPC 的 one-to-one 映射（以及缺乏全球访问权限）使其成为访问着陆区域中 VPC 的最不受欢迎的方式。
- 选项 2：为与多个 vGW 关联的 Direct Connect 网关创建私有 VIF（每个 VGW 都连接到一个 VPC）— Direct Connect 网关是一种全球可用的资源。您可以在任何区域创建 Direct Connect 网关，然后从所有其他区域访问该网关，包括 GovCloud（不包括中国）。Direct Connect Gateway 可以通过单个私有 VIF 连接到任何 AWS 账户中的全球多达 20 个 VPC（通过 vGW）。如果着陆区包含少量 VPC（十个或更少 VPC）和/或您需要全球访问权限，那么这是一个不错的选择。每个 Direct Connect 网关每个 Direct Connect 连接都有一个 BGP 对等会话。Direct Connect 网关仅适用于南

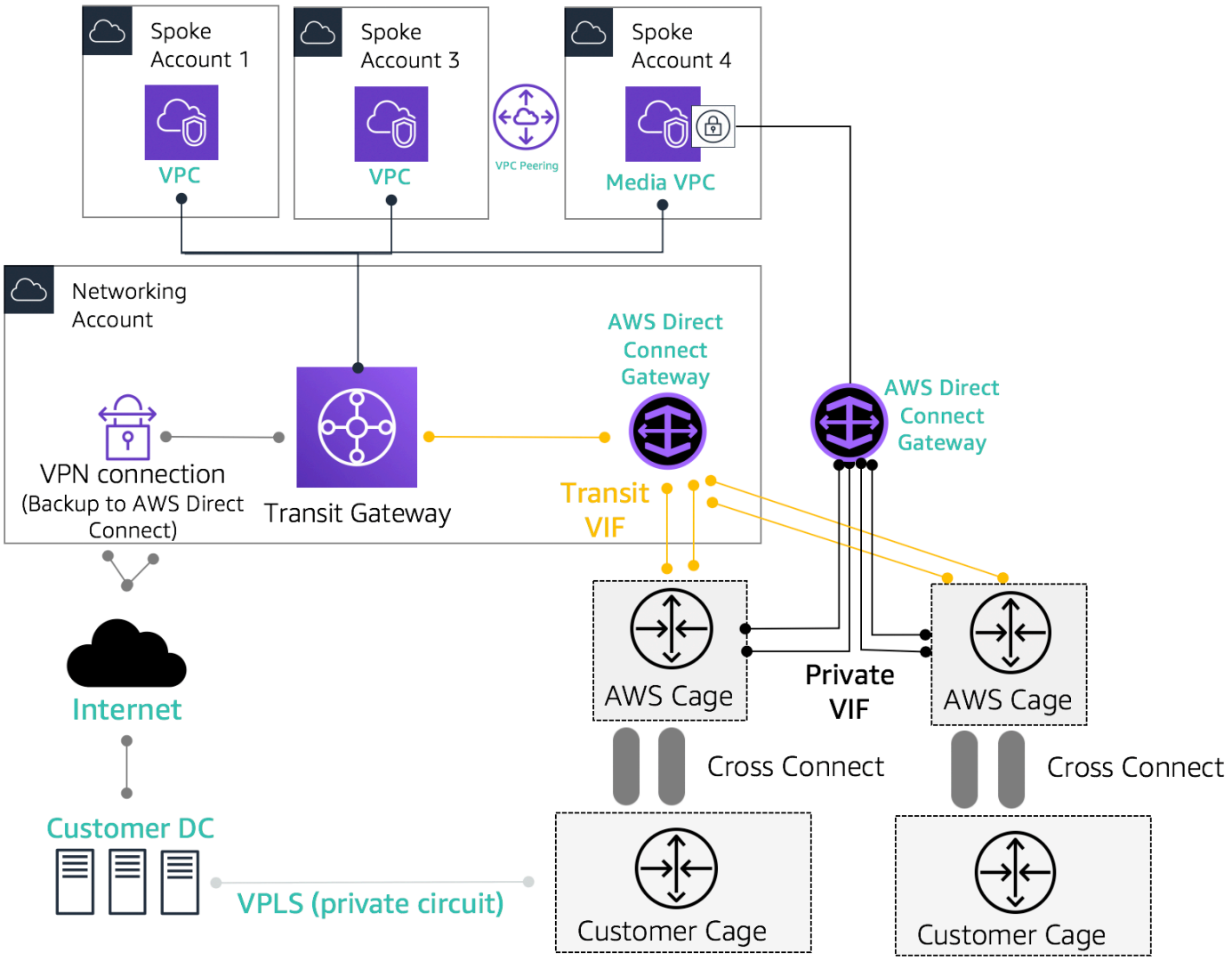
北流量，不允许 vpc 到 VPC 的连接。有关更多详细信息，请参阅 AWS Direct Connect 文档中的虚拟专用网关关联。使用此选项，连接将不限于 Direct Connect 地点所在的 AWS 区域。 AWS Direct Connect 网关仅适用于南北流量，不允许 VPC 到 VPC 的连接。此规则的一个例外情况是，当在两个或多个 VPC 上通告超网时，这些虚拟网络的连接的 vGW 与同一个 AWS Direct Connect 网关和同一个虚拟接口相关联。在这种情况下，VPC 可以通过 AWS Direct Connect 终端节点相互通信。有关更多详细信息，请参阅AWS Direct Connect 网关文档。

- 选项 3：为与 Transit Gateway 关联的 Direct Connect 网关创建公交 VIF — 您可以使用公交 VIF 将 Transit Gateway 实例关联到 Direct Connect 网关。 AWS Direct Connect 现在支持以所有端口速度连接到 Transit Gateway，在不需要高速连接（大于 1Gbps）时，这为 Transit Gateway 用户提供了更具成本效益的选择。这使您能够以 50、100、200、300、400 和 500 Mbps 的速度使用 Direct Connect，连接到 Transit Gateway。Transit VIF 允许您通过单一传输 VIF 和 BGP 对等互连将本地数据中心连接到每个 AWS Direct Connect 网关（可以连接到数千个 VPC），跨不同 AWS 地区和 AWS 账户，最多可连接六个 Transit Gateway 实例。这是大规模连接多个 VPC 的选项中最简单的设置，但您应该注意 Tr ansit Gateway 配额。需要注意的一个关键限制是，您只能通过中转 VIF 将来自 Transit Gateway 的 200 个前缀通告到本地路由器。使用之前的选项，您需要按照 Direct Connect 的定价付费。对于此选项，您还需要支付 Transit Gateway 的附件和数据处理费用。有关更多信息，请参阅 Di rect Connect 上的 Transit Gateway 关联文档。
- 选项 4：通过 Direct Connect 公共 VIF 创建与 Transit Gateway 的 VPN 连接 — 公有 VIF 允许您使用公有 IP 地址访问所有 AWS 公共服务和终端节点。当你在 Transit Gateway 上创建 VPN 附件时，你会在 AWS 端获得两个用于 VPN 终端节点的公有 IP 地址。这些公共 IP 可通过公共 VIF 访问。您可以通过公共 VIF 创建任意数量的 Transit Gateway 实例的 VPN 连接。当您通过公有 VIF 创建 BGP 对等互连时，AWS 会向您的路由器通告整个 AW S 公有 IP 范围。为确保仅允许某些流量（例如，仅允许流量流向 VPN 终端节点），建议您使用防火墙本地设施。此选项可用于在网络层对您的 Direct Connect 进行加密。
- 选项 5： AWS Direct Connect 使用私有 IP VPN 创建与 Transit Gateway 的 VPN 连接 — 私有 IP VPN 是一项功能，可让客户使用私有 IP 地址通过 Direct Connect 部署 AWS 站点到站点 VPN 连接。借助此功能，您无需使用公有 IP 地址即可通过 Direct Connect 连接加密本地网络与 AWS 之间的流量，从而同时增强安全性和网络隐私。私有 IP VPN 部署在 Transit VIF 之上，因此它允许您使用 Transit Gateway 以更安全、更私密和可扩展的方式集中管理客户的 VPC 以及与本地网络的连接。
- 选项 6：通过公交 VIF 创建通往 Transit Gateway 的 GRE 隧道 — Transi t Gateway Connect 连接类型支持 GRE。借助 Transit Gateway Connect，软件定义广域网基础设施可以原生连接到 AWS，而无需在 SD-WAN 网络虚拟设备和 Transit Gateway 之间设置 IPsec VPN。GRE 隧道可以通过传输 VIF 建立，将 Transit Gateway Connect 作为连接类型，与 VPN 连接相比，可提供更高的带宽性能。有关更多信息，请参阅使用 Connect 简化 SD-WAN AWS Transit Gateway 连接博客文章。

“将 VIF 传输到 Direct Connect 网关” 选项似乎是最佳选择，因为它允许您使用每个 Direct Connect 连接的单个 BGP 会话 AWS 区域 在单个点（Transit Gateway）整合所有本地连接；但是，围绕此选项的一些限制和注意事项可能会导致您同时使用私有和中转 VIF 来满足您的着陆区连接要求。

下图说明了一个示例设置，其中使用 Transit VIF 作为连接 VPC 的默认方法，而私有 VIF 用于必须将大量数据从本地数据中心传输到媒体 VPC 的边缘用例。私有 VIF 用于避免 Transit Gateway 的数据处理费用。作为最佳实践，您应该在两个不同的 Direct Connect 位置至少有两个连接，以实现最大冗余，即总共四个连接。您可以为每个连接创建一个 VIF，总共创建四个私有 VIF 和四个中转 VIF。您也可以创建 VPN 作为连接的备用 AWS Direct Connect 连接。

使用 “通过公交 VIF 创建通往 Transit Gateway 的 GRE 隧道” 选项，您可以将软件定义广域网基础设施与 AWS 进行本地连接。它无需在 SD-WAN 网络虚拟设备和 Transit Gateway 之间设置 IPsec VPN。



混合连接参考架构示例

使用网络服务帐户创建 Direct Connect 资源，从而划定网络管理边界。Direct Connect 连接、Direct Connect 网关和传输网关都可以位于网络服务帐户中。要与您的着陆区共享 AWS Direct Connect 连接，只需 AWS RAM 与其他账户共享 Transit Gateway 即可。

直接连接上的 MacSec 安全

客户可以将 MAC 安全标准 (MacSec) 加密 (IEEE 802.1AE) 与 Direct Connect 连接一起使用 10 Gbps，在特定地点使用 100 Gbps 的专用连接。借助此功能，客户可以在第 2 层保护其数据，而 Direct Connect 可提供 point-to-point 加密功能。要启用 Direct Connect MacSec 功能，请确保满足 MacSec 的先决条件。由于 MacSec 会 hop-by-hop根据基础保护链路，因此您的设备必须与我们的 Direct Connect 设备有直接的第 2 层邻接。您的最后一英里提供商可以帮助您验证您的连接是否可以与 MacSec 兼容。有关更多信息，请参阅在 AWS Direct Connect 连接中添加 MacSec 安全。

AWS Direct Connect 弹性建议

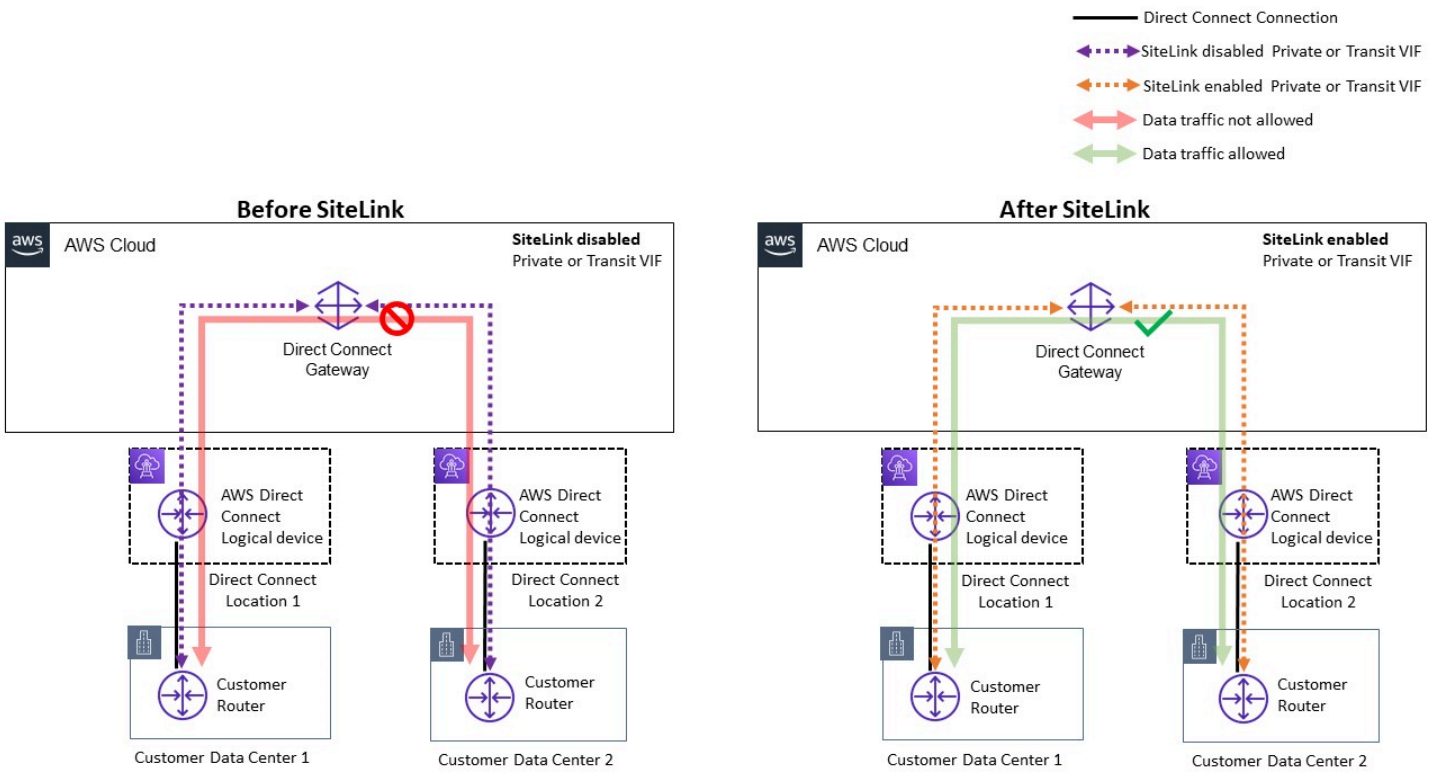
借助 AWS Direct Connect，客户可以从本地网络实现与 Amazon VPC 和 AWS 资源的高度弹性连接。最佳做法是客户从多个数据中心进行连接，以消除任何单点物理位置故障。还建议客户根据工作负载的类型使用多个 Direct Connect 连接来实现冗余。

AWS 还提供 AWS Direct Connect 弹性工具包，该工具包为客户提供具有多种冗余模型的连接向导；帮助他们确定哪种模式最适合其服务级别协议 (SLA) 要求，并相应地使用 Direct Connect 连接设计混合连接。有关更多信息，请参阅AWS Direct Connect 弹性建议。

AWS Direct Connect SiteLink

以前，只有通过暗光纤或其他技术、IPSEC VPN 或使用具有 MPLS 等技术的第三方电路提供商或传统 T1 电路等技术 MetroEthernet，才能为本地网络配置 site-to-site 链路。随着的出现 SiteLink，客户现在可以为终止于某个 AWS Direct Connect 位置的本地位置启用直接 site-to-site 连接。使用您的 Direct Connect 电路提供 site-to-site 连接，无需通过您的 VPC 路由流量，完全绕过 AWS 区域。

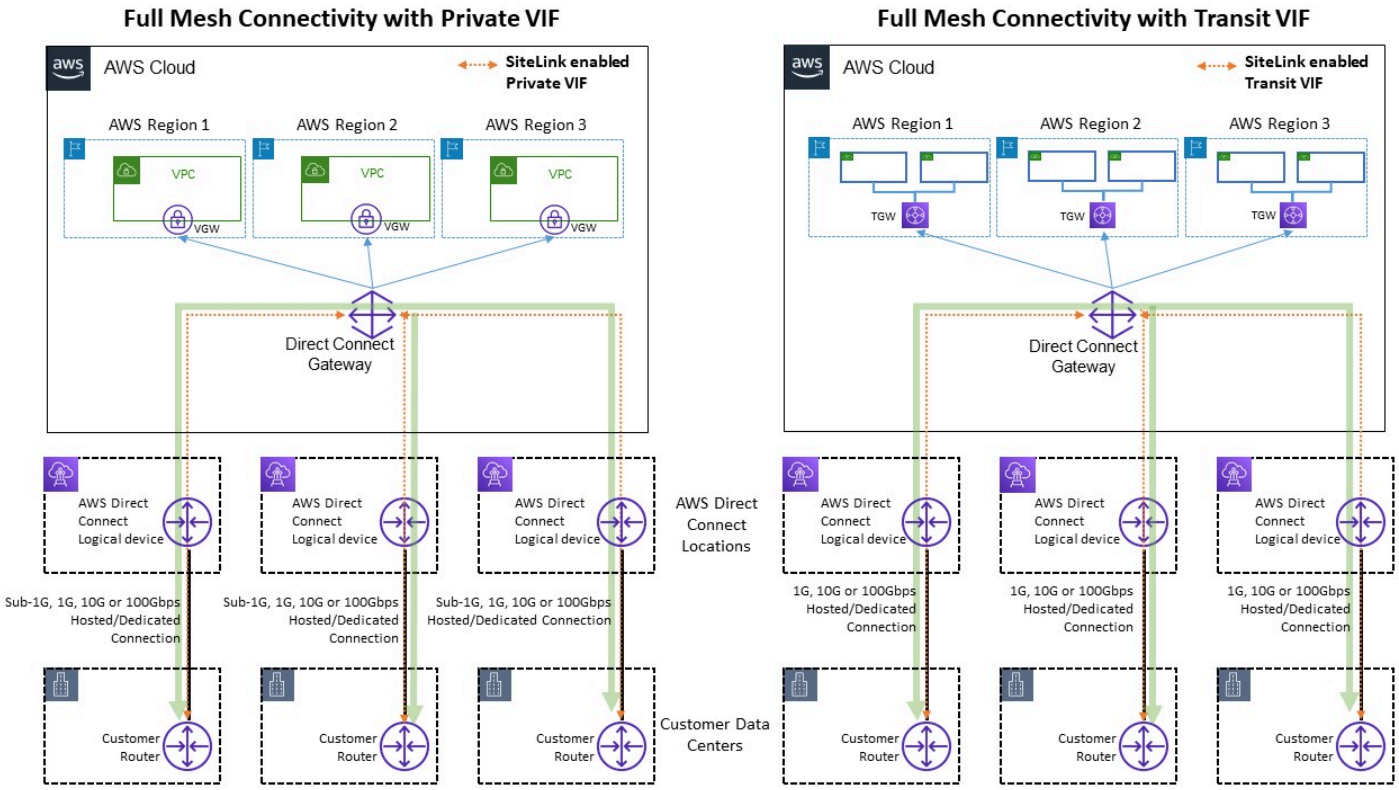
现在，通过在不同 AWS Direct Connect 地点之间以最快的路径发送数据，您可以在全球网络中的办公室和数据中心之间建立全球性、可靠的 pay-as-you-go 连接。



的示例参考架构 AWS Direct Connect SiteLink

使用时 SiteLink，您首先要在全球 100 多个 AWS Direct Connect 地点将本地网络连接到 AWS。然后，在这些连接上创建虚拟接口 (VIF) 并启用 SiteLink。所有 VIF 都连接到同一个 AWS Direct Connect 网关 (DXGW) 后，您就可以开始在它们之间发送数据了。使用快速、安全和可靠的 AWS 全球网络，您的数据沿着 AWS Direct Connect 各个位置之间到达目的地的最短路径行驶。您无需拥有任何资源 AWS 区域 即可使用 SiteLink。

使用 SiteLink，DXGW 通过 SiteLink 启用的 VIF 从您的路由器那里学习 IPv4/IPv6 前缀，运行 BGP 最佳路径算法，更新诸如 NextHop 和 as_path 之类的属性，并将这些 BGP 前缀重新通告给与该 DXGW 关联的其余已启用 VIF。 SiteLink如果您在 VIF SiteLink 上禁用，DXGW 将不会通过此 VIF 将学习到的本地前缀通告给其他启用的 VIF。 SiteLink来自 SiteLink 已禁用 VIF 的本地前缀仅会通告给 DXGW 网关协会，例如与 DXGW 关联的 AWS 虚拟私有网关 (vGW) 或 Transit Gateway (TGW) 实例。



Sitelink 允许流量流量（示例）

SiteLink 允许客户使用 AWS 全球网络充当远程位置之间的主连接或辅助/备用连接，具有高带宽和低延迟，并通过动态路由来控制哪些位置可以相互通信以及与您的 AWS 区域资源进行通信。

有关更多信息，请参阅简介 AWS Direct Connect SiteLink。

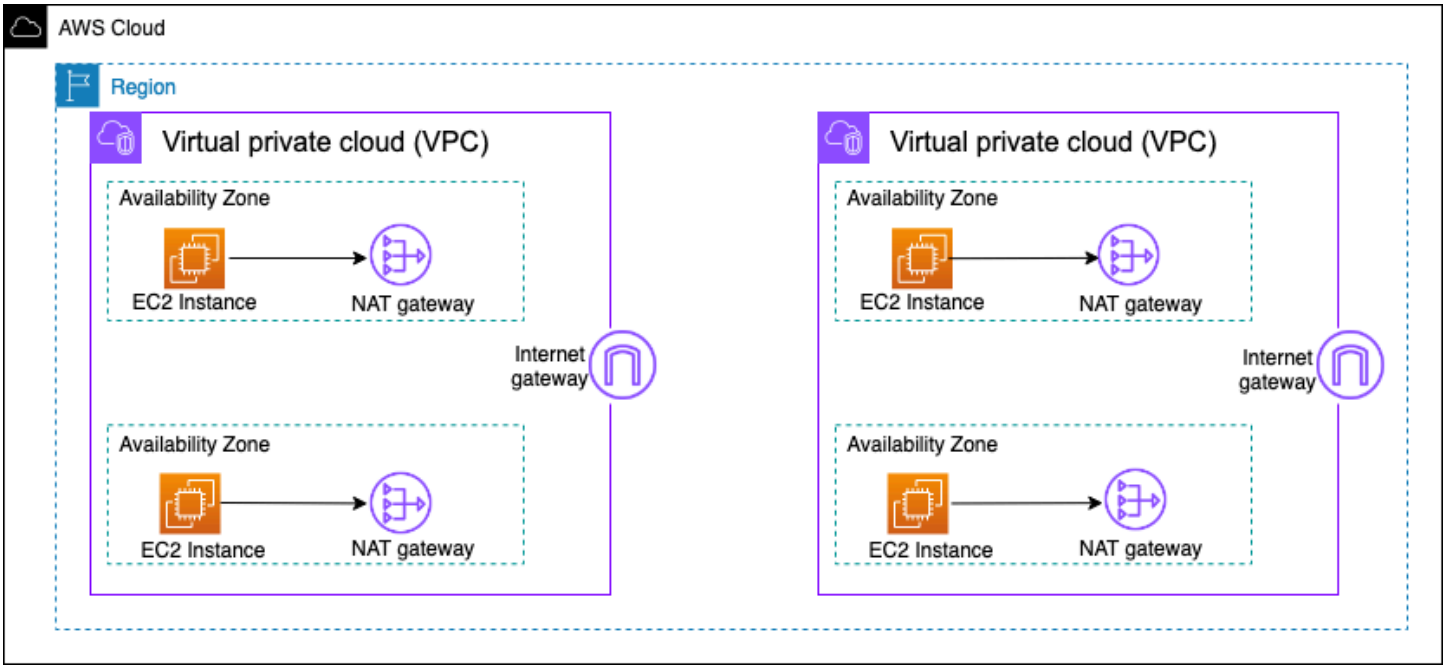
集中式互联网出口

当您在多账户环境中部署应用程序时，许多应用程序将要求仅出站访问互联网（例如，下载库、补丁或操作系统更新）。IPv4 和 IPv6 流量都可以实现这一点。对于 IPv4，这可以通过网络地址转换 (NAT) 来实现，其形式为 NAT 网关（推荐），或者在 Amazon EC2 实例上运行的自管理 NAT 实例，作为所有出口互联网访问的一种手段。内部应用程序位于私有子网中，而 NAT 网关/Amazon EC2 NAT 实例则位于公有子网中。AWS 建议您使用 NAT 网关，因为它们可以提供更好的可用性和带宽，而且您管理所需的精力更少。有关更多信息，请参阅比较 NAT 网关和 NAT 实例。对于 IPv6 流量，可以将出口流量配置为以分散的方式通过仅限出口 Internet 网关离开每个 VPC，也可以将其配置为使用 NAT 实例或代理实例将其发送到集中式 VPC。本文档下文的 “IPv6 集中出口” 部分将讨论 IPv6 模式。

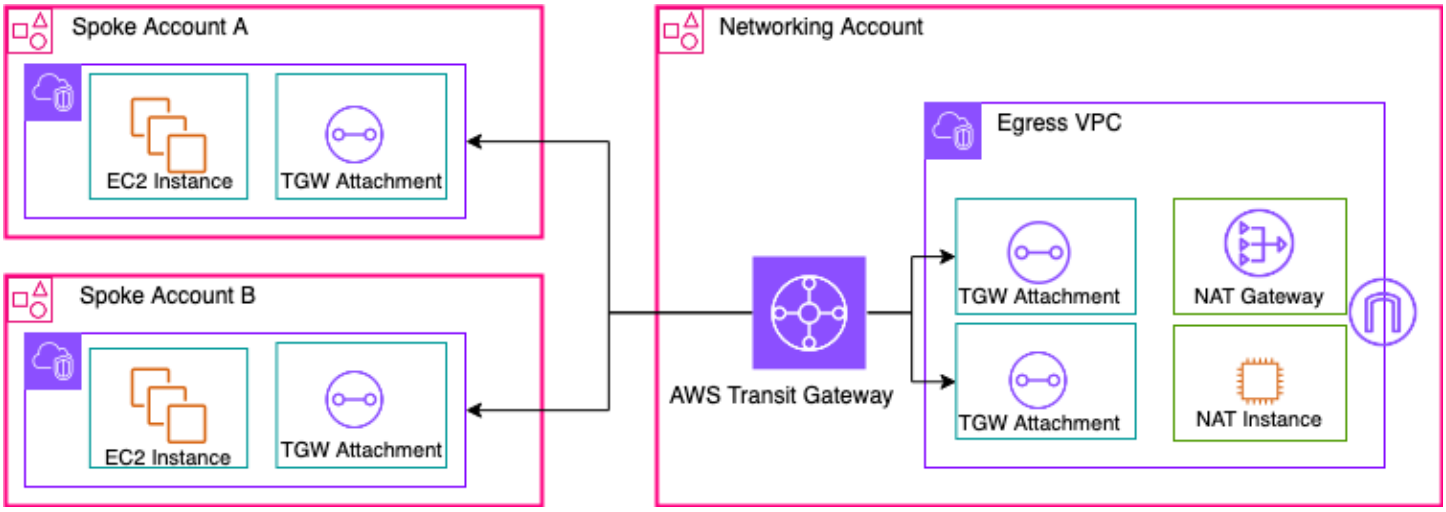
使用 NAT 网关进行集中式 IPv4 出口

NAT 网关是一种托管网络地址转换服务。在每个分支 VPC 中部署 NAT 网关的成本可能会让人望而却步，因为您需要为部署的每个 NAT 网关按小时付费（请参阅 A mazon VPC 定价）。集中化 NAT 网关可能是降低成本的可行选择。要实现集中化，您可以在网络服务账户中创建单独的出口 VPC，在出口 VPC 中部署 NAT 网关，然后使用 Transit Gateway 或 CloudWAN 将所有出口流量从分支 VPC 路由到出口 VPC 中驻留的 NAT 网关，如下图所示。

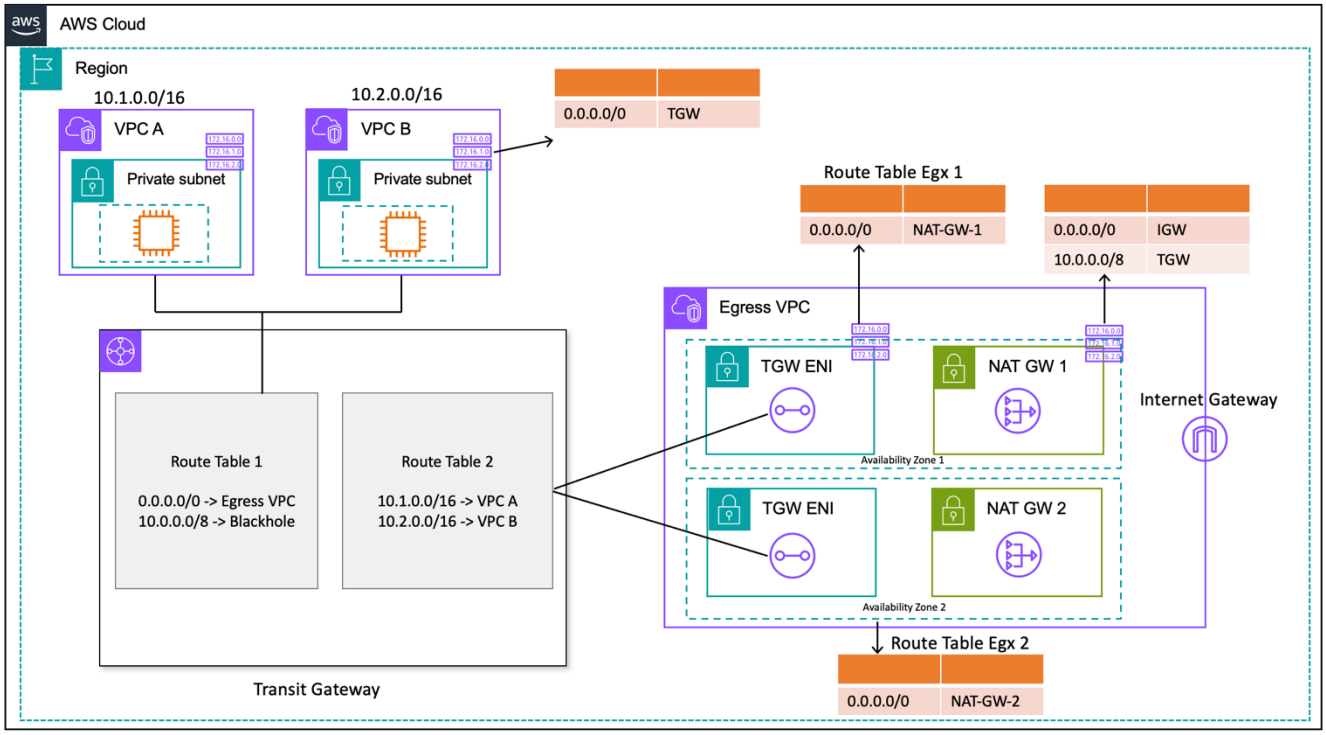
> **Note**
>
> 与在每个 VPC 中运行 NAT 网关的去中心化方法相比，使用 Transit Gateway 集中管理 NAT 网关时，您需要支付额外的 Transit Gateway 数据处理费用。在某些边缘情况下，当您通过 NAT 网关从 VPC 发送大量数据时，将 NAT 保留在 VPC 本地以避免 Transit Gateway 数据处理费用可能更具成本效益。



分散式高可用性 NAT 网关架构



使用 Transit Gateway 的集中式 NAT 网关（概



使用 Transit Gateway 的集中式 NAT 网关（路由表设计）

在此设置中，分支 VPC 附件与路由表 1 (RT1) 关联并传播到路由表 2 (RT2)。有一条黑洞路径可以禁止两个 VPC 相互通信。如果要允许 VPC 间通信，可以从 RT1 中删除该`10.0.0.0/8 -> Blackhole`路由条目。这允许他们通过传输网关进行通信。您还可以将分支 VPC 附件传播到 RT1（或者，您可以使用一个路由表并将所有内容关联/传播到该路由表），从而使用 Transit Gateway 在 VPC 之间实现直接流量。

您可以在 RT1 中添加一条静态路由，将所有流量指向出口 VPC。由于此静态路由，Transit Gateway 会通过其出口 VPC 中的 ENI 发送所有互联网流量。进入出口 VPC 后，流量将遵循存在这些 Transit Gateway ENI 的子网路由表中定义的路由。您可以在子网路由表中添加一条路由，将所有流量指向同一可用区中相应的 NAT 网关，以最大限度地减少跨可用区 (AZ) 流量。NAT 网关子网路由表将互联网网关 (IGW) 作为下一跳。要使返回流量回流，您必须在 NAT 网关子网路由表中添加一个静态路由表条目，将所有分支 VPC 绑定的流量指向 Transit Gateway 作为下一跳。

高可用性

为了获得高可用性，您应该使用多个 NAT 网关（每个可用区一个）。如果 NAT 网关不可用，则通过受影响的 NAT 网关的可用区中的流量可能会被丢弃。如果一个可用区不可用，则该可用区中的 Transit Gateway 终端节点和 NAT 网关将出现故障，所有流量都将通过另一个可用区中的 Transit Gateway 和 NAT 网关终端节点流动。

安全性

您可以依赖源实例上的安全组、Transit Gateway 路由表中的黑洞路由以及 NAT 网关所在子网的网络 ACL。例如，客户可以使用 NAT Gateway 公有子网上的 ACL 来允许或屏蔽源或目标 IP 地址。或者，您可以将 NAT Gateway 与 AWS Network Firewall 下一节中所述的集中式出口配合使用，以满足此要求。

可扩展性

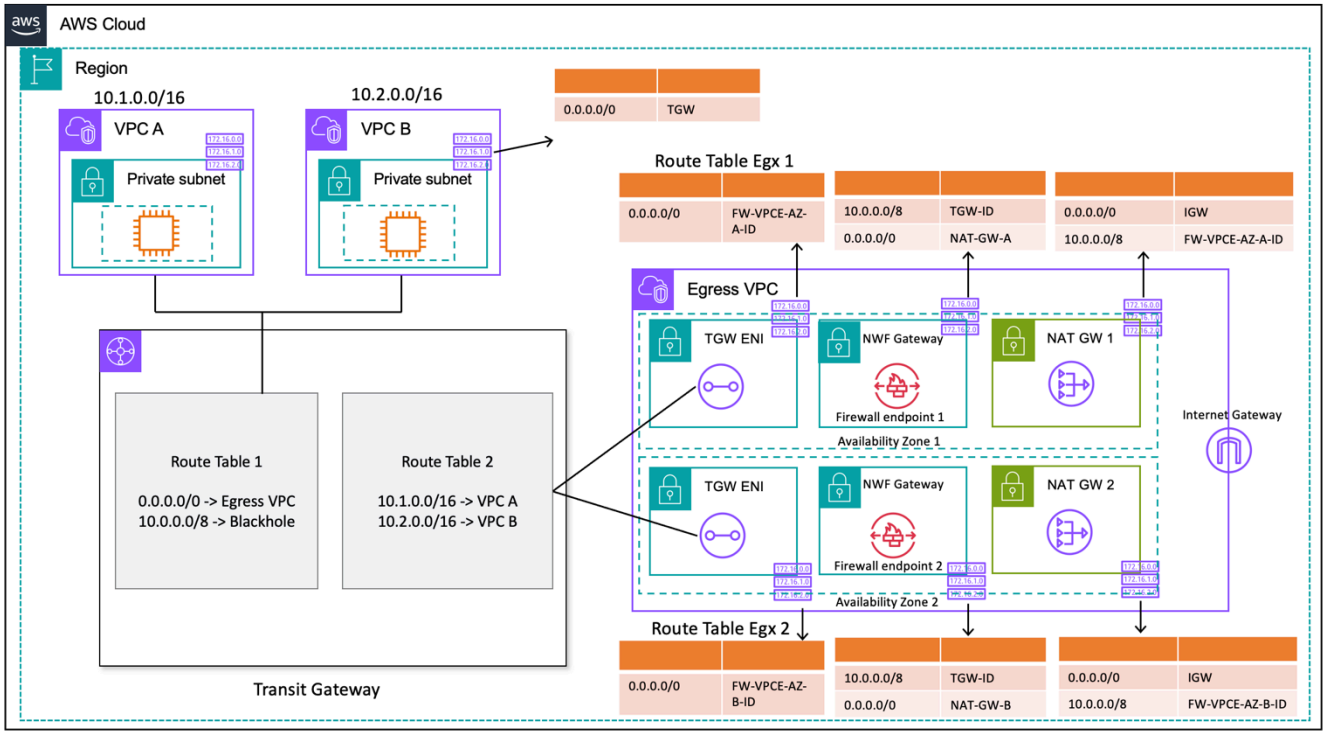
对于每个分配的 IP 地址，一个 NAT 网关最多可支持 55,000 个与每个唯一目的地的同步连接。您可以请求调整配额，允许最多分配八个 IP 地址，从而允许与单个目标 IP 和端口同时连接 440,000 个。NAT 网关提供 5 Gbps 的带宽，并自动扩展到 100 Gbps。Transit Gateway 通常不充当负载均衡器，也不会在多个可用区的 NAT 网关之间均匀分配您的流量。如果可能，通过 Transit Gateway 的流量将保持在可用区域内。如果启动流量的 Amazon EC2 实例位于可用区 1 中，则流量将流出出口 VPC 中同一个可用区 1 的 Transit Gateway 弹性网络接口，并根据弹性网络接口所在的子网路由表流向下一个跳点。有关规则的完整列表，请参阅 Amazon Virtual Private Cloud 文档中的 NA T 网关。

有关更多信息，请参阅使用 AWS Transit Gateway 从多个 VPC 创建单个互联网出口点博客文章。

将 NAT 网关与 AWS Network Firewall 用于集中式 IPv4 出口

如果您想检查和筛选出站流量，可以在集中式出口架构中将 AWS Network Firewall 与 NAT 网关结合起来。 AWS Network Firewall 是一项托管服务，可让您轻松地为所有 VPC 部署基本的网络保护。它可以控制和查看整个 VPC 的第 3-7 层网络流量。您可以对 URL/域名、IP 地址和基于内容的出站流量进行筛选，以阻止可能的数据丢失，帮助满足合规性要求并阻止已知的恶意软件通信。 AWS Network Firewall 支持成千上万条规则，这些规则可以过滤出发往已知的错误 IP 地址或错误域名的网络流量。您还可以将 Suricata IPS 规则用作 AWS Network Firewall 服务的一部分，方法是导入开源规则集或使用 Suricata 规则语法编写自己的入侵防御系统 (IPS) 规则。 AWS Network Firewall 还允许您导入来自 AWS 合作伙伴的兼容规则。

在带检查功能的集中式出口架构中， AWS Network Firewall 终端节点是出口 VPC 的传输网关附件子网路由表中的默认路由表目标。使用 AWS Network Firewall 下图所示检查分支 VPC 和互联网之间的流量。



使用 AWS Network Firewall 和 NAT 网关集中出口（路由表设计）

对于使用 Transit Gateway 的集中部署模式，AWS 建议在多个可用区部署 AWS Network Firewall 终端节点。客户运行工作负载的每个可用区中都应有一个防火墙终端节点，如上图所示。最佳做法 AWS Network Firewall 是，防火墙子网不应包含任何其他流量，因为防火墙子网无法检查来自防火墙子网内源或目标的流量。

与之前的设置类似，分支 VPC 附件与路由表 1 (RT1) 关联并传播到路由表 2 (RT2)。明确添加了 Blackhole 路由，以禁止两个 VPC 相互通信。

在 RT1 中继续使用默认路由，将所有流量指向出口 VPC。Transit Gateway 会将所有流量转发到出口 VPC 中的两个可用区域之一。流量到达出口 VPC 中的一个 Transit Gateway 弹性网卡后，您就会到达一条默认路由，该路由会将流量转发到相应可用 AWS Network Firewall 区域中的一个终端节点。AWS Network Firewall 然后将根据您设置的规则检查流量，然后使用默认路由将流量转发到 NAT 网关。

这种情况不需要 Transit Gateway 设备模式，因为您没有在附件之间发送流量。

> **Note**
>
> AWS Network Firewall 不会为您执行网络地址转换，此功能将在通过进行流量检查后由 NAT 网关处理 AWS Network Firewall。在这种情况下，不需要入口路由，因为默认情况下，返回流量将转发到 NATGW IP。

由于您使用的是 Transit Gateway，因此我们可以将防火墙放在 NAT 网关之前。在此模型中，防火墙可以看到 Transit Gateway 背后的源 IP。

如果您在单个 VPC 中执行此操作，我们可以使用 VPC 路由增强功能，允许您检查同一 VPC 中子网之间的流量。有关详细信息，请参阅AWS Network Firewall 使用 VPC 路由增强功能的部署模型博客文章。

可扩展性

AWS Network Firewall 可以根据流量负载自动向上或向下扩展防火墙容量，以保持稳定、可预测的性能，从而最大限度地降低成本。 AWS Network Firewall 旨在支持成千上万的防火墙规则，每个可用区的吞吐量最高可扩展到 100 Gbps。

重要注意事项：

- 每个防火墙终端节点可以处理大约 100 Gbps 的流量，如果您需要更高的突发或持续的吞吐量，请联系 AWS 支持。
- 如果您选择在您的 AWS 账户中创建 NAT 网关和 Network Firewall，则可以免除标准 NAT 网关处理费和每小时使用费，前提是防火墙 one-to-one 按每 GB 处理量和使用时数收费。
- 您也可以考虑在没有 Transit Gateway AWS Firewall Manager 的情况下通过分布式防火墙终端节点。
- 在将防火墙规则移至生产环境之前对其进行测试，类似于网络访问控制列表，因为顺序很重要。
- 要进行更深入的检查，需要高级的 Suricata 规则。网络防火墙支持对入口和出口流量进行加密流量检查。
- `HOME_NET`规则组变量定义了有资格在状态引擎中进行处理的源 IP 范围。使用集中式方法，您必须添加所有附加到 Transit Gateway 的其他 VPC CIDR，使其符合处理资格。有关`HOME_NET`规则组变量的更多详细信息，请参阅 Network Firewall 文档。
- 考虑在单独的网络服务账户中部署 Transit Gateway 和出口 VPC，以便根据职责分配隔离访问权限；例如，只有网络管理员才能访问网络服务账户。

- 为了简化此模型 AWS Network Firewall 中的部署和管理， AWS Firewall Manager 可以使用。Firewall Manager 允许您通过自动将您在集中位置创建的保护应用于多个帐户来集中管理不同的防火墙。Firewall Manager 支持 Network Firewall 的分布式和集中式部署模式。要了解更多信息，请参阅博客文章如何使用 AWS Network Firewall 进行部署 AWS Firewall Manager。

将 NAT 网关和网关负载均衡器与 Amazon EC2 实例配合使用，实现集中式 IPv4 出口

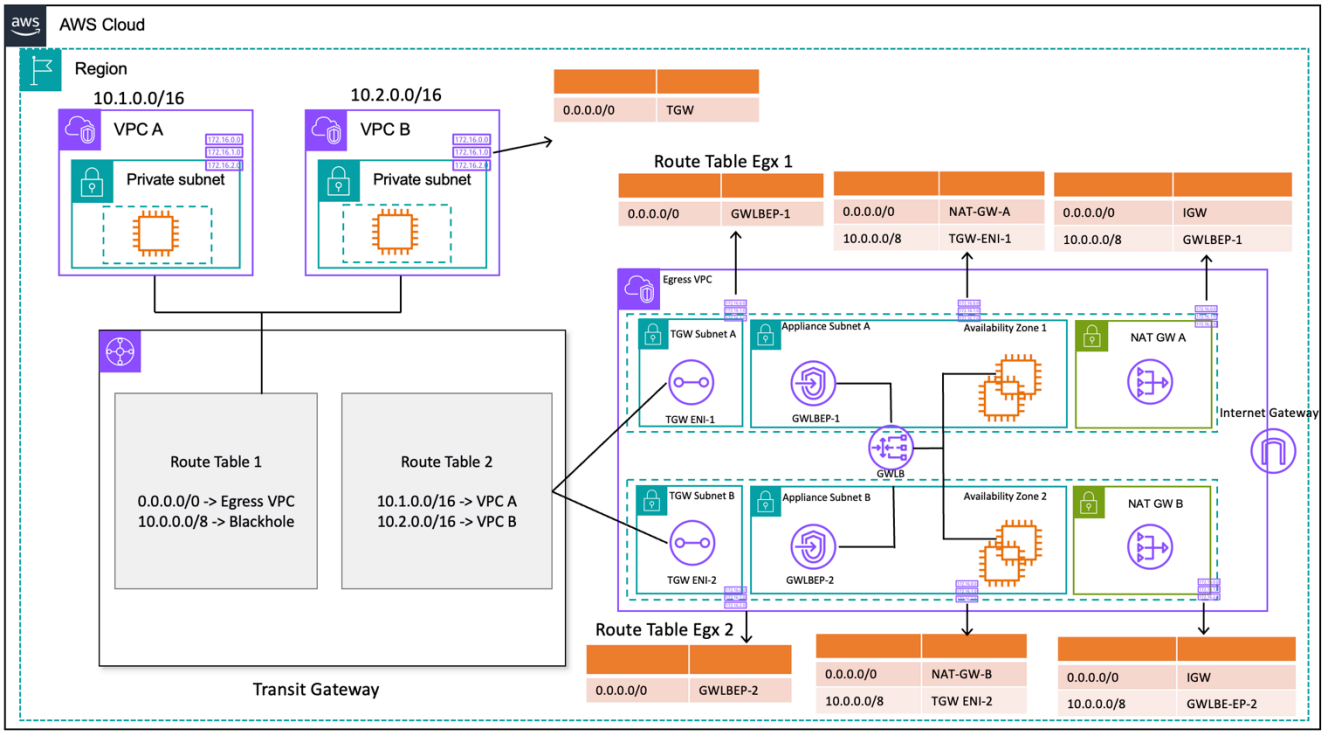
使用基于软件的虚拟设备（在 Amazon EC2 上） AWS Partner Network 作为退出点与 NAT 网关设置类似。 AWS Marketplace 如果您想使用各种供应商产品的高级第 7 层防火墙/入侵防御/检测系统 (IPS/IDS) 和深度数据包检测功能，则可以使用此选项。

在下图中，除了 NAT 网关外，您还使用网关负载均衡器 (GWLB) 后面的 EC2 实例部署虚拟设备。在此设置中，GWLB、Gateway Load Balancer 终端节点 (GWLBE)、虚拟设备和 NAT 网关部署在使用 VPC 连接到 Transit Gateway 的集中式 VPC 中。分支 VPC 还使用 VPC 附件连接到 Transit Gateway。由于 GWLBE 是可路由的目标，因此您可以将来自 Transit Gateway 的流量路由到配置为 GWLB 后面目标的虚拟设备队列。GWLB 充当，透明 bump-in-the-wire 地通过第三方虚拟设备传递所有第 3 层流量，因此流量的来源和目的地都看不见。因此，该架构允许您集中检查通过 Transit Gateway 的所有出口流量。

有关流量如何从 VPC 中的应用程序流向互联网并通过此设置返回互联网的更多信息，请参阅使用 AWS Gateway Load Balancer 的集中检查架构和 AWS Transit Gateway。

您可以在 Transit Gateway 上启用设备模式，以通过虚拟设备保持流量对称性。这意味着双向流量将在流量生命周期内通过同一个设备和可用区路由。此设置对于执行深度数据包检查的状态防火墙尤其重要。启用设备模式无需使用复杂的变通方法（例如源网络地址转换 (SNAT)）来强制流量返回正确的设备以保持对称。有关详细信息，请参阅部署 Gateway Load Balancer 的最佳实践。

还可以在没有 Transit Gateway 的情况下以分布式方式部署 GWLB 端点以启用出口检查。在 AWS Gateway Load Balancer 简介：支持的架构模式博客文章中了解有关这种架构模式的更多信息。



使用 Gateway Load Balancer 和 EC2 实例集中出口（路由表设计）

高可用性

AWS 建议在多个可用区部署网关负载均衡器和虚拟设备以提高可用性。

Gateway Load Balancer 可以执行运行状况检查以检测虚拟设备故障。如果设备运行状况不佳，GWLB 会将新的流量重新路由到健康的设备。无论目标的健康状况如何，现有流量总是流向同一个目标。这允许连接耗尽并适应由于设备上的 CPU 峰值而导致的运行状况检查失败。有关更多详细信息，请参阅博客文章 Gate way Load Balancer 部署最佳实践中的第 4 节：了解设备和可用区故障场景。Gateway Load Balancer 可以使用自动伸缩组作为目标。这一优势省去了管理设备群组可用性和可扩展性的繁重工作。

优点

Gateway Load Balancer 和 Gateway Load Balancer 终端节点由 AWS PrivateLink提供支持，这允许跨越VPC边界安全地交换流量，而无需穿越公共互联网。

Gateway Load Balancer 是一项托管服务，它消除了管理、部署、扩展虚拟安全设备等无差别的繁重工作，因此您可以专注于重要的事情。Gateway Load Balancer 可以将防火墙堆栈作为终端节点服务公开，供客户使用订阅。AWS Marketplace这称为防火墙即服务 (FWaaS)；它引入了简化的部署，无需依赖 BGP 和 ECMP 在多个 Amazon EC2 实例之间分配流量。

重要注意事项：

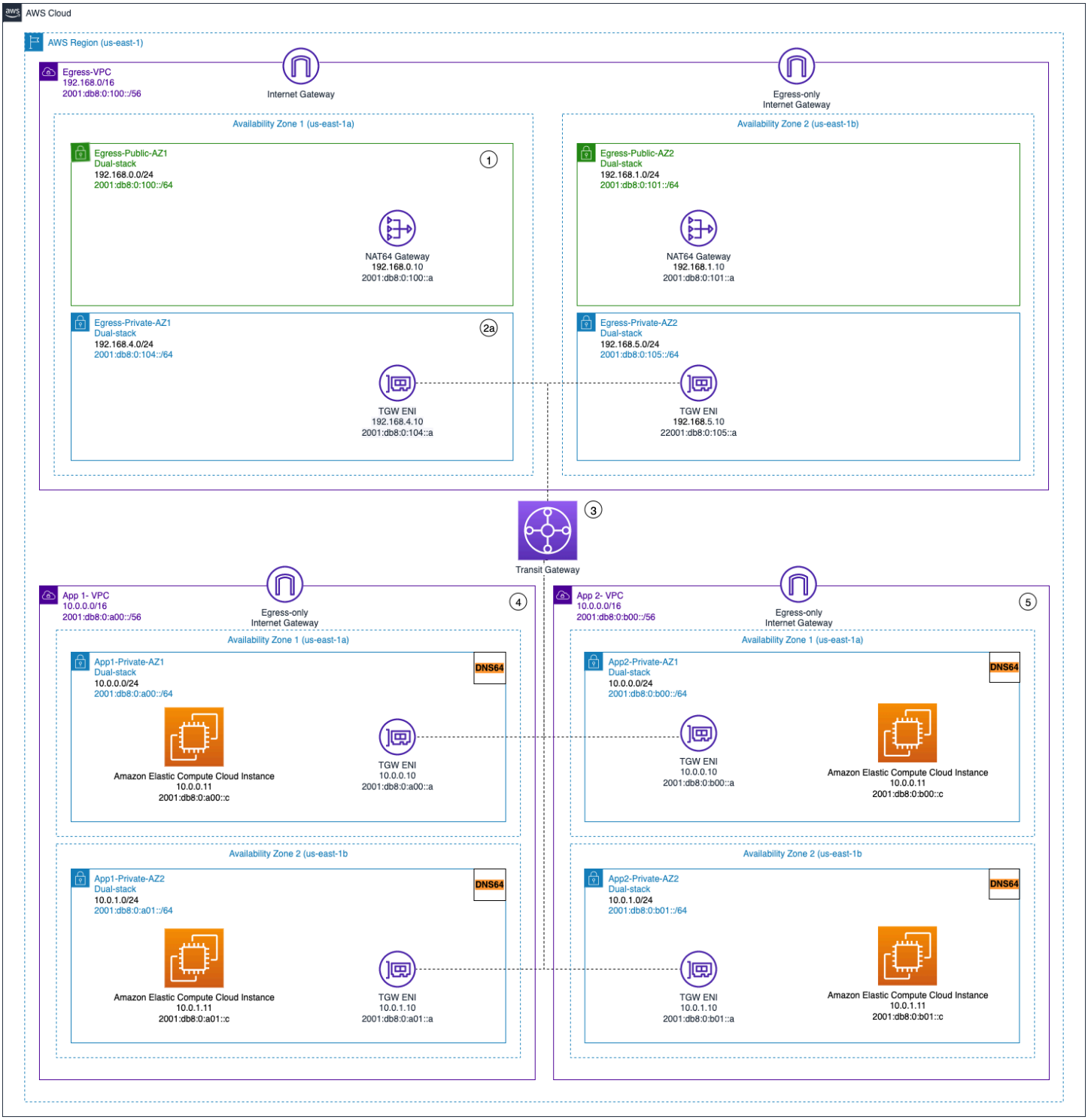
- 这些设备需要支持 Geneve 封装协议才能与 GWLB 集成。
- 某些第三方设备可以支持 SNAT 和覆盖路由（双臂模式），因此无需创建 NAT 网关即可节省成本。但是，在使用此模式之前，请咨询您选择的 AWS 合作伙伴，因为这取决于供应商的支持和实施。
- 记下 GWLB 空闲超时。这可能会导致客户端连接超时。您可以调整客户端、服务器、防火墙和操作系统级别的超时时间以避免这种情况。有关更多信息，请参阅 G ateway Load Balancer 部署最佳实践博客文章中的第 1 节：调整 TCP 保持活动状态或超时值以支持长寿命的 TCP 流。
- GWLBE 由提供动力 AWS PrivateLink，因此将 AWS PrivateLink 收取费用。您可以在AWS PrivateLink 定价页面了解更多信息。如果您在 Transit Gateway 中使用集中模式，则将收取 TGW 数据处理费用。
- 考虑在单独的网络服务账户中部署 Transit Gateway 和出口 VPC，以便根据职责分配隔离访问权限，例如只有网络管理员才能访问网络服务账户。

IPv6 的集中式出口

要在具有集中式 IPv4 输出的双堆栈部署中支持 IPv6 出口，必须选择以下两种模式之一：

- 使用分散的 IPv6 出口实现集中式 IPv4 出口
- 集中式 IPv4 输出和集中式 IPv6 出口

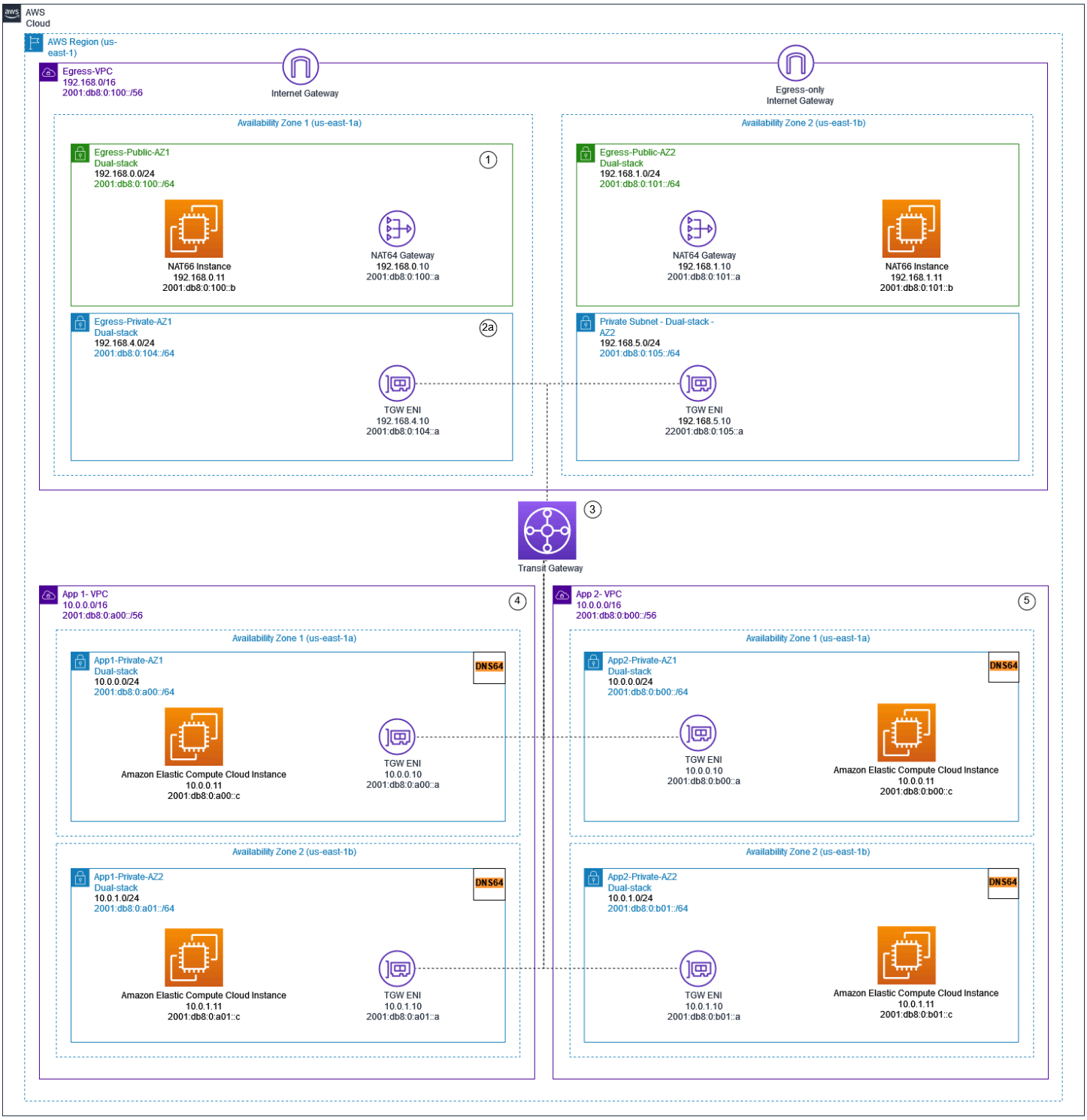
在下图所示的第一种模式中，每个分支 VPC 中都部署了仅限出站的 Internet 网关。仅限出口 Internet 网关是水平扩展、冗余且高度可用的网关，允许从 VPC 内的实例通过 IPv6 进行出站通信。它们阻止互联网启动与您的实例的 IPv6 连接。仅限出口的互联网网关不收费。在此部署模型中，IPv6 流量流出每个 VPC 中的仅限出口的互联网网关，而 IPv4 流量则通过部署的集中式 NAT 网关流出。



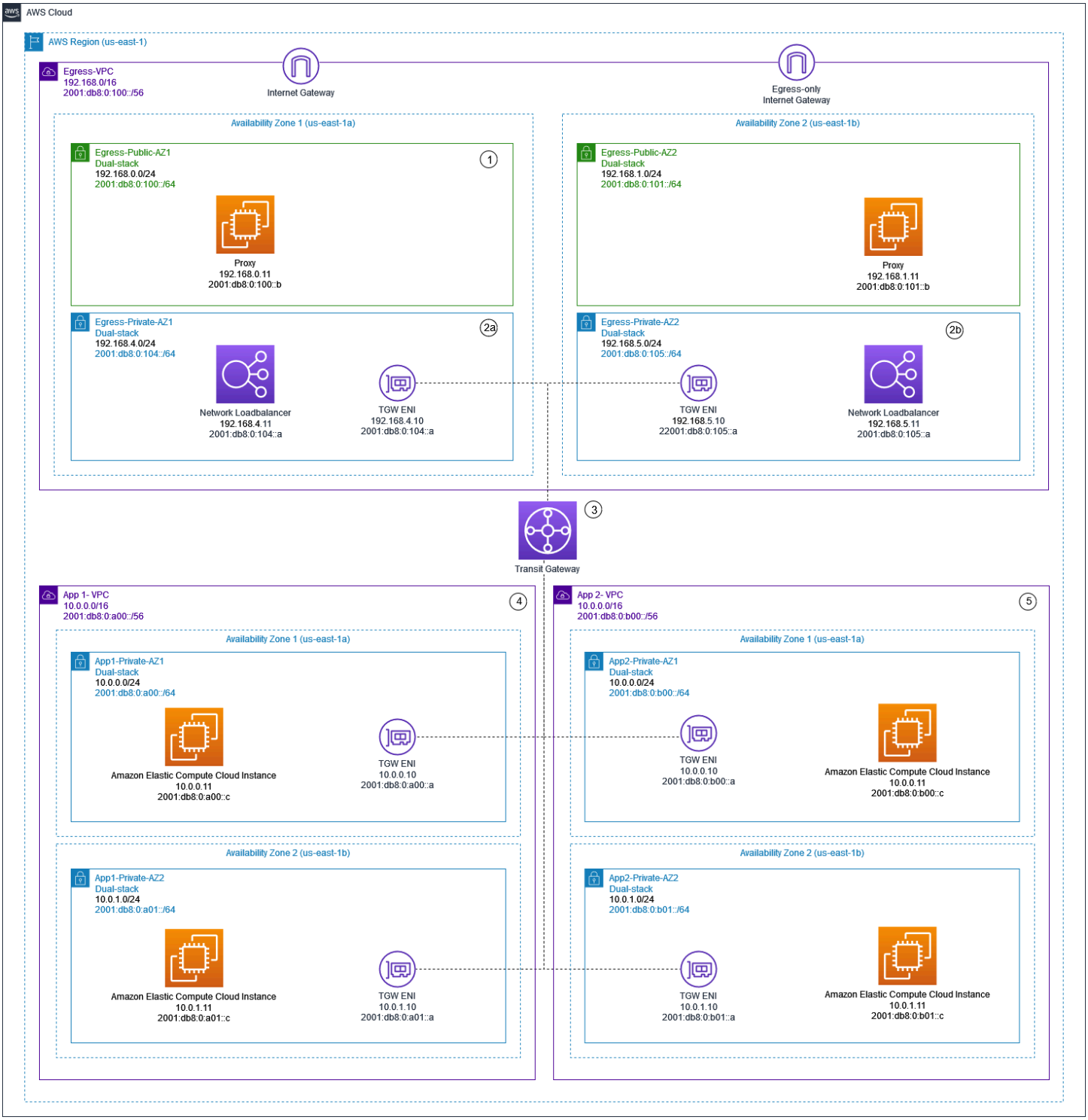
集中式 IPV4 出站流量和分散式仅限出站 IPv6 出口

在第二种模式中（如下图所示），您的实例的出口 IPv6 流量将发送到集中式 VPC。这可以通过在 NAT66 实例和 NAT 网关上使用 IPv6 到 IPv6 网络前缀转换 (NPTv6) 或使用代理实例和网络负载均衡

器来实现。如果需要对出站流量进行集中流量检查，并且无法在每个分支 VPC 中执行此操作，则此模式适用。



使用 NAT 网关和 NAT66 实例集中化 IPv6 出口



使用代理实例和 Network Load Balancer 集中化 IPv4 和 IPv6 出口

AWS 上的 IPv6 白皮书描述了集中式 IPv6 出口模式。博客 IPv 4 和 IPv6 VPC 的集中出站互联网流量详细讨论了 IPv6 出站模式，以及特殊注意事项、示例解决方案和图表。

VPC 到 VPC 和本地到 VPC 流量的集中式网络安全

AWS 提供安全组和子网 NACL，以便在您的登录区内实现网络安全。这些是第 4 层防火墙。在某些情况下，客户可能希望在其登录区内实施第 7 层防火墙/IPS/IDS，以检查 VPC 之间或本地数据中心与 VPC 之间传输的流量。这可以通过使用 Transit Gateway 和运行在 EC2 实例上的第三方软件设备来实现。使用图 14 中的架构，我们可以使 VPC 到 VPC 和本地到 VPC 流量能够通过 EC2 实例传输。该设置与我们在图 12 中讨论过的类似，但我们另外删除了路由表 1 中的黑洞路由以允许暂存 VPC 流量，并将 VPN 挂载和/或 Direct Connect GW 挂载附加到路由表 1 以允许混合流量。这样，来自分支的所有流量都能够先传输到出口 VPC，然后再发送到目标。您需要出口 VPC 子网路由表（防火墙 EC2 设备位于其中）中的静态路由来在流量检查后通过 Transit Gateway 发送发往分支 VPC 和本地 CIDR 的流量。

> **Note**
>
> 路由信息不会从 Transit Gateway 动态传播到子网路由表中，必须静态输入。子网路由表上有 50 个静态路由的软限制。

图 14 – VPC 到 VPC 和 VPC 到本地部署流量控制

将流量发送到 EC2 实例进行嵌入式检查时的关键注意事项：

- 额外的 Transit Gateway 数据处理费用
- 流量必须经过两个附加的跃点（EC2 实例和 Transit Gateway）
- 可能出现带宽和性能瓶颈
- 维护、管理和扩展 EC2 实例的额外复杂性：
  - 检测故障并故障转移到备用实例
  - 跟踪使用情况并进行横向/纵向扩展
  - 防火墙配置、补丁管理
  - 负载均衡时流量的源网络地址转换（SNAT，Source Network Address Translation），用于保证流量对称

您应该选择通过这些 EC2 实例传递哪些流量。一种处理方法是定义安全区域并检查不受信任区域之间的流量。不受信任区域可以是第三方管理的远程站点、您无法控制/信任的供应商 VPC 或者沙盒/开发

VPC，与您的环境的其他部分相比，其安全框架比较宽松。图 15 支持受信任网络之间的直接流量，同时使用嵌入式 EC2 实例检查往返不受信任网络的流量。我们在此示例中创建了三个区域：

- 不受信任区域 – 这适用于来自“VPN 到远程不受信任站点”或第三方供应商 VPC 的任何流量。
- 生产区域 – 这包含来自生产 VPC 和本地客户 DC 的流量。
- 开发区域 – 这包含来自两个开发 VPC 的流量。

以下是我们为跨区域通信定义的示例规则：

1. 不受信任区域与生产区域 – 不允许通信
2. 生产区域与开发区域 – 允许通过出口 VPC 中的 EC2 FW 设备进行通信
3. 不受信任区域与开发区域 – 允许通过出口 VPC 中的 EC2 FW 设备进行通信
4. 生产区域与生产区域以及开发区域与开发区域 – 通过 Transit Gateway 直接通信

这是一个有三个安全区域的设置，但您可以有更多安全区域。您可以使用多个路由表和黑洞路由来实现安全隔离和最佳流量。选择合适的区域取决于您的整体登录区设计策略（账户结构、VPC 设计）。您可以使用区域来实现业务单元、应用程序、环境等之间的隔离。

在此示例中，我们在 Transit Gateway 上终止不受信任的远程 VPN，并将所有流量发送到 EC2 上的软件 FW 设备进行检查。或者，您可以直接在 EC2 实例上终止这些 VPN，而不是在 Transit Gateway 上终止这些 VPN。通过这种方法，不受信任的 VPN 流量永远不会与 Transit Gateway 直接交互。流量中的跃点数减少了 1，这样可以节省 AWS VPN 成本。要启用动态路由交换（让 Transit Gateway 通过 BGP 了解远程 VPN 的 CIDR），防火墙实例应通过 VPN 连接到 Transit Gateway。在本机 TGW 挂载模型中，您必须在 VPN CIDE 的 TGW 路由表中添加静态路由，并将下一跃点作为出口/安全 VPC。在我们的设置（图 15）中，我们为所有流量提供了到出口 VPC 的默认路由，因此不必显式添加任何特定的静态路由。通过这种方法，您从完全托管式 Transit Gateway VPN 终止终端节点迁移到自我管理的 EC2 实例，从而增加 VPN 管理开销以及 EC2 实例在计算和内存方面的额外负载。

图 15 – 通过使用 Transit Gateway 并定义安全区域来进行流量隔离

集中入库检查

就其本质而言，面向互联网的应用程序具有更大的攻击面，并且容易受到大多数其他类型的应用程序不必面对的威胁类别。为这些类型的应用程序提供必要的保护，使其免受攻击，并最大限度地减少影响表面积，是任何安全策略的核心部分。

当您在着陆区部署应用程序时，用户将通过面向公众的负载均衡器、API 网关或直接通过互联网网关通过公共互联网（例如，通过内容分发网络 (CDN) 或面向公众的 Web 应用程序）访问许多应用程序。在这种情况下，您可以使用 AWS Web 应用程序防火墙 (AWS WAF) 进行入站应用程序检查，或者使用 Gateway Load Balancer 或 IDS/IPS 入站检查来保护您的工作负载和应用程序。 AWS Network Firewall

当你继续在着陆区部署应用程序时，你可能需要检查入站互联网流量。您可以通过多种方式实现这一目标， AWS Network Firewall 包括使用分布式、集中式或组合式检查架构，使用运行第三方防火墙设备的 Gateway Load Balancer，或者通过使用开源 Suricata 规则使用高级 DPI 和 IDS/IPS 功能。本节涵盖了 Gateway Load Balancer 和 AWS Network Firewall 集中式部署，使用它 AWS Transit Gateway 作为路由流量的中心枢纽。

AWS WAF 并 AWS Firewall Manager 用于检查来自互联网的入站流量

AWS WAF 是一种 Web 应用程序防火墙，可帮助保护您的 Web 应用程序或 API 免受可能影响可用性、危及安全性或消耗过多资源的常见 Web 漏洞和机器人的侵害。 AWS WAF 允许您创建控制机器人流量和阻止常见攻击模式（例如 SQL 注入或跨站脚本 (XSS)）的安全规则，从而控制流量如何到达您的应用程序。您还可以自定义过滤掉特定流量模式的规则。

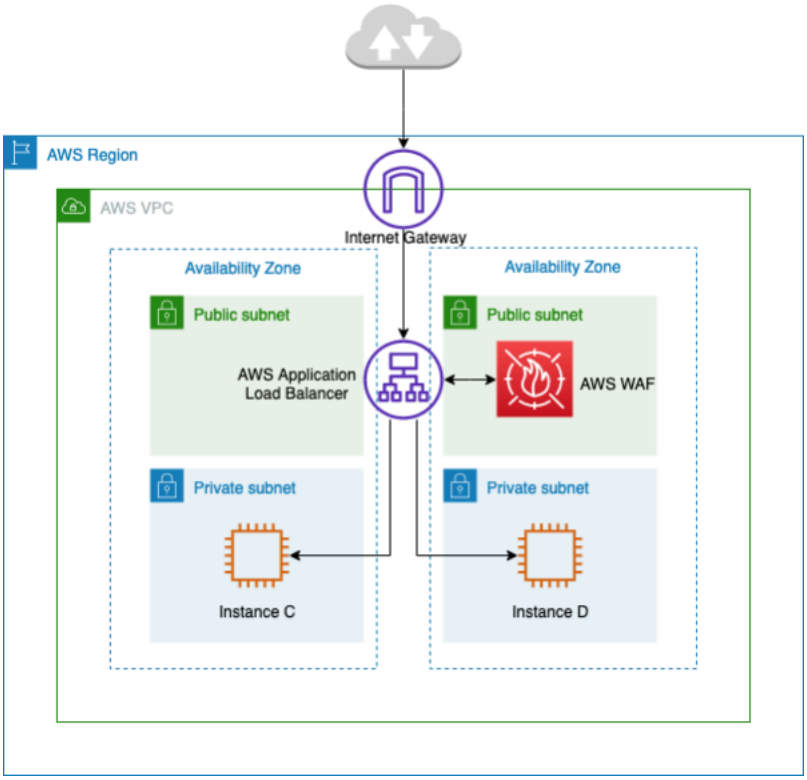
您可以将应用程序负载均衡器 CloudFront 作为您的 CDN 解决方案的一部分部署在亚马逊 AWS WAF 上，在您的网络服务器上部署应用程序负载均衡器，用于您的 REST API API 或 AWS AppSync GraphQL API。

部署完成后 AWS WAF，您可以使用可视化规则生成器、JSON 中的代码、由维护的托管规则来创建自己的流量过滤规则 AWS，也可以从中订阅第三方规则 AWS Marketplace。这些规则可以通过根据指定模式评估流量来过滤掉不需要的流量。您可以进一步使用 Amazon CloudWatch 来监控传入流量指标和记录。

要在中对所有账户和应用程序进行集中管理 AWS Organizations，可以使用 AWS Firewall Manager。AWS Firewall Manager 是一项安全管理服务，允许您集中配置和管理防火墙规则。在创建新应用程序

时，通过强制执行一组通用的安全规则，可以轻松地 AWS Firewall Manager 使新的应用程序和资源达到合规性。

使用 AWS Firewall Manager，您可以轻松地为应用程序负载均衡器、API Gateway 实例和 Amazon CloudFront 分配推出 AWS WAF 规则。 AWS Firewall Manager 与 f AWS 托管式规则 or 集成 AWS WAF，这使您可以轻松地在应用程序上部署预先配置的精选 AWS WAF 规则。有关使用集中管理的更多信息 AWS WAF AWS Firewall Manager，请参阅集中管理 AWS WAF (API v2) 和使用 AWS 托管式规则 进行 AWS Firewall Manager大规模管理。



使用集中式入站流量检查 AWS WAF

在上述架构中，应用程序在私有子网中多个可用区的 Amazon EC2 实例上运行。在 Amazon EC2 实例前面部署了一个面向公众的应用程序负载均衡器 (ALB)，用于在不同目标之间对请求进行负载平衡。与 AWS WAF ALB 关联。

优点

- 借助 AWS WAF Bot Control，您可以查看和控制应用程序中常见且普遍存在的机器人流量。
- 借助的托管规则 AWS WAF，您可以快速入门并保护您的 Web 应用程序或 API 免受常见威胁的侵害。您可以从许多规则类型中进行选择，例如解决开放网络应用程序安全项目 (OWASP) 十大安全风险、内容管理系统 (CMS) 特有的威胁（ 如 WordPress 或 Joomla ），甚至是新出现的常见漏洞和暴露 (CVE)。随着新问题的出现，托管规则会自动更新，因此您可以将更多时间花在构建应用程序上。

- AWS WAF 是一项托管服务，在此架构中不需要任何设备进行检查。此外，它还通过亚马逊数据 Fire hose提供近乎实时的日志。 AWS WAF 让您近乎实时地了解您的网络流量，您可以使用它在 Amazon 中创建新规则或提醒。 CloudWatch

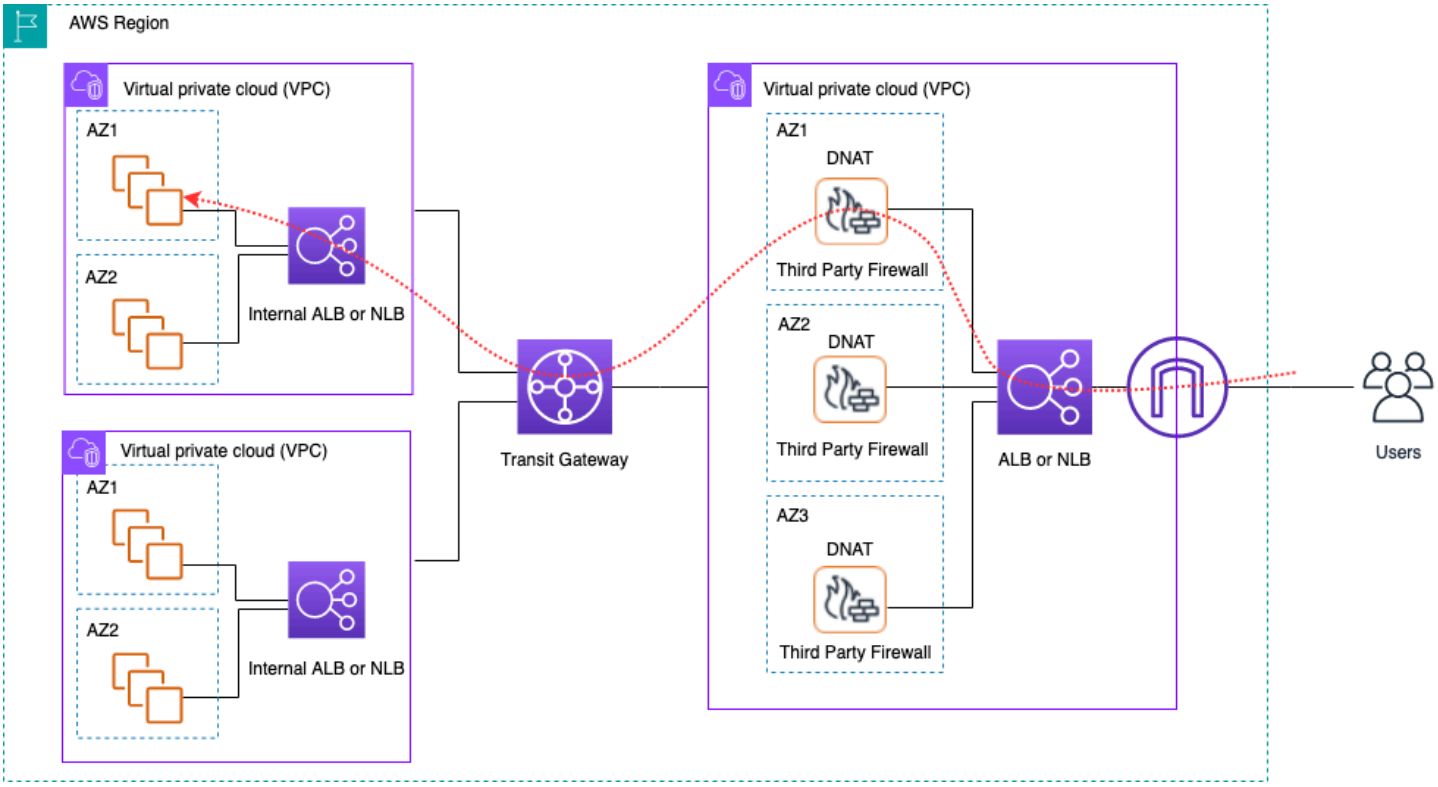
重要注意事项：

- 此架构最适合 HTTP 标头检查和分布式检查，因为它 AWS WAF 集成在每个 ALB、 CloudFront 分发和 API Gateway 上。 AWS WAF 不记录请求正文。
- 进入第二组 ALB（如果存在）的流量可能不会被同一个 AWS WAF 实例检查；因为会向第二组 ALB 发出新的请求。

使用第三方设备进行集中入库检查

在这种架构设计模式中，您可以在 Amazon EC2 上跨弹性负载均衡器 (ELB) 后面的多个可用区部署第三方防火墙设备，例如单独检查 VPC 中的应用程序/网络负载均衡器。

检查 VPC 和其他分支 VPC 通过 Transit Gateway 作为 VPC 附件连接在一起。Spoke VPC 中的应用程序由内部 ELB 进行前端，内部 ELB 可以是 ALB 或 NLB，具体取决于应用程序类型。通过互联网的客户端连接到检查 VPC 中外部 ELB 的 DNS，后者将流量路由到其中一个防火墙设备。防火墙检查流量，然后使用内部 ELB 的 DNS 通过 Transit Gateway 将流量路由到分支 VPC，如下图所示。有关使用第三方设备进行入站安全检查的更多信息，请参阅如何将第三方防火墙设备集成到 AWS 环境中的博客文章。



使用第三方设备和 ELB 集中检查入口流量

优点

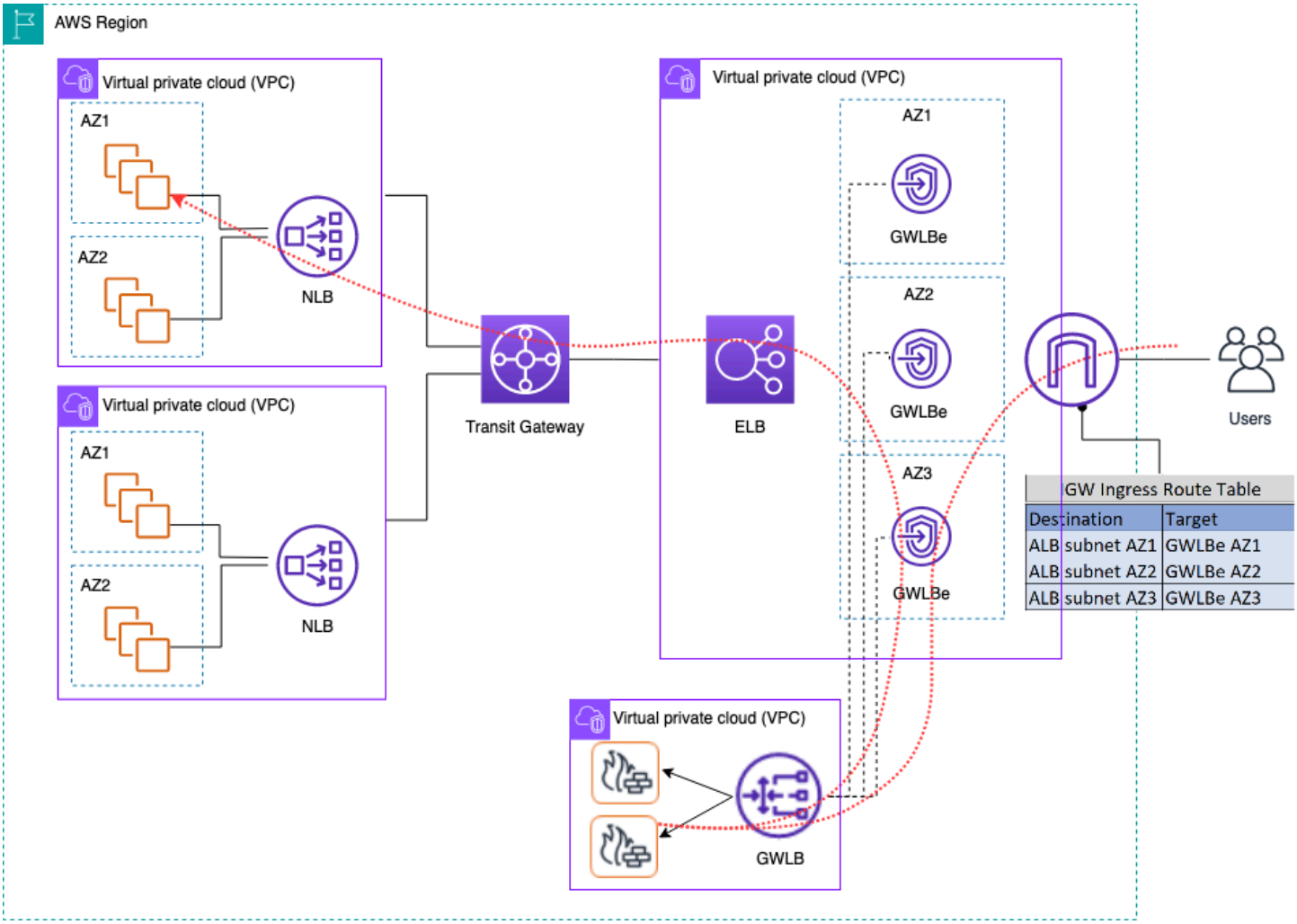
- 该架构可以支持任何类型的应用程序进行检查，并支持通过第三方防火墙设备提供的高级检查功能。
- 此模式支持从防火墙设备到分支 VPC 的基于 DNS 的路由，这允许 Spoke VPC 中的应用程序在 ELB 后独立扩展。
- 您可以使用 Auto Scaling 和 ELB 来扩展检查 VPC 中的防火墙设备。

重要注意事项：

- 您需要跨可用区部署多个防火墙设备以实现高可用性。
- 为了保持流量对称性，需要配置防火墙并执行源 NAT，这意味着应用程序无法看到客户端 IP 地址。
- 考虑在网络服务账户中部署 Transit Gateway 和 Inspection VPC。
- 额外的第三方供应商防火墙许可/支持成本。Amazon EC2 费用取决于实例类型。

使用带有 Gateway Load Balancer 的防火墙设备检查来自互联网的入站流量

客户使用第三方下一代防火墙 (NGFW) 和入侵防御系统 (IPS) 作为其深度防御策略的一部分。 传统上，这些设备通常是专用的硬件或软件/虚拟设备。您可以使用 Gateway Load Balancer 水平扩展这些虚拟设备，以检查进出您的 VPC 的流量，如下图所示。



使用带有 Gateway Load Balancer 的防火墙设备集中检查入口流量

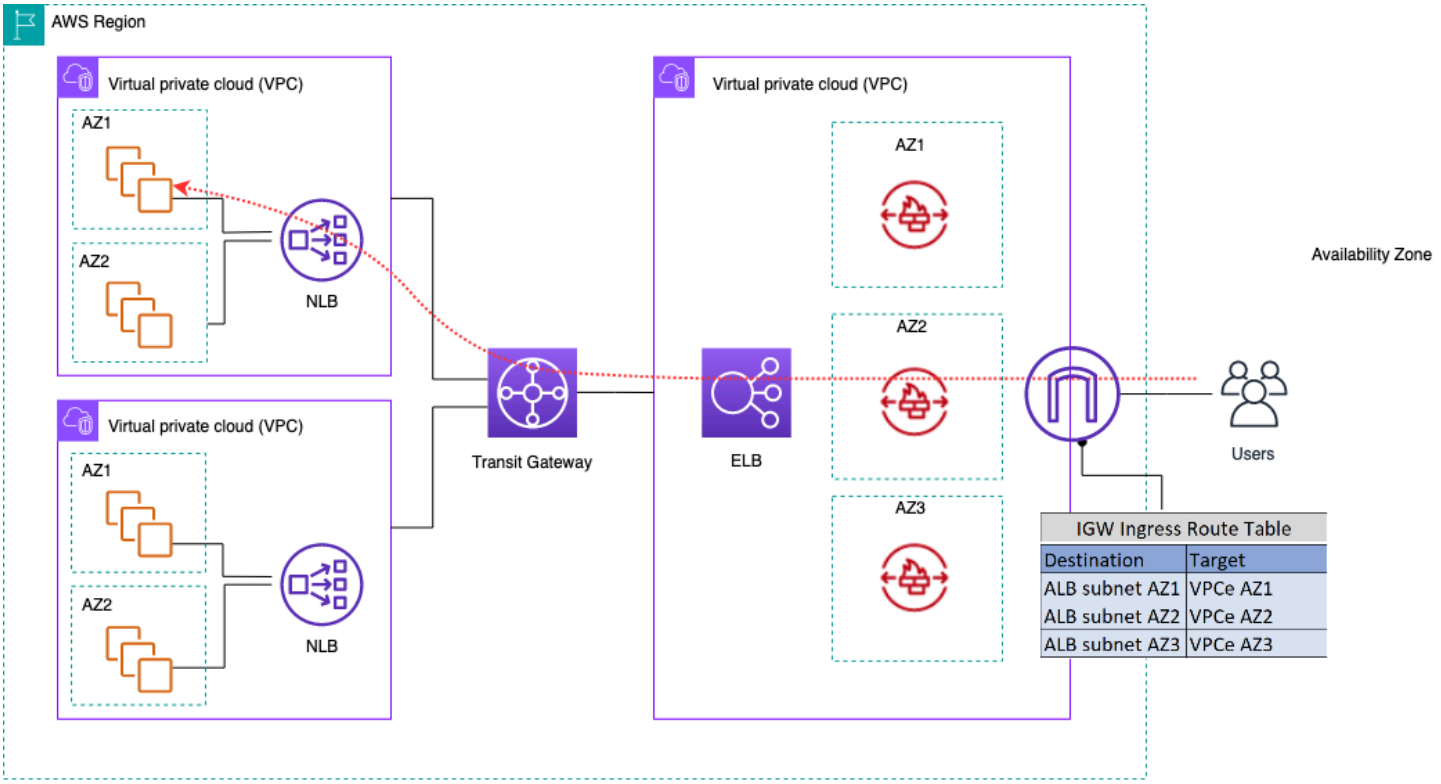
在前面的架构中，Gateway Load Balancer 终端节点部署在单独的边缘 VPC 中的每个可用区中。下一代防火墙、入侵防御系统等部署在集中式设备 VPC 中的 Gateway Load Balancer 后面。此设备 VPC 可以与分支 VPC 位于相同的 AWS 账户中，也可以位于不同的 AWS 账户中。虚拟设备可以配置为使用 Auto Scaling 组，并自动向网关负载均衡器注册，从而允许自动扩展安全层。

这些虚拟设备可以通过通过 Internet Gateway (IGW) 访问其管理界面或使用设备 VPC 中的堡垒主机设置进行管理。

使用 VPC 入口路由功能，可以更新边缘路由表，将入站流量从互联网路由到 Gateway Load Balancer 后面的防火墙设备。被检查的流量通过 Gateway Load Balancer 终端节点路由到目标 VPC 实例。有关使用 AWS Gateway Load Balancer 的各种方式的详细信息，请参阅网关负载均衡器简介：支持的架构模式博客文章。

使用 AWS Network Firewall 进行集中式入口

在此架构中，入口流量在到达其余的 VPC AWS Network Firewall 之前要经过检查。在此设置中，流量在 Edge VPC 中部署的所有防火墙端点之间进行分配。您可以在防火墙终端节点和 Transit Gateway 子网之间部署公有子网。您可以使用 ALB 或 NLB，它们在分支 VPC 中包含 IP 目标，同时为其后面的目标处理 Auto Scaling。

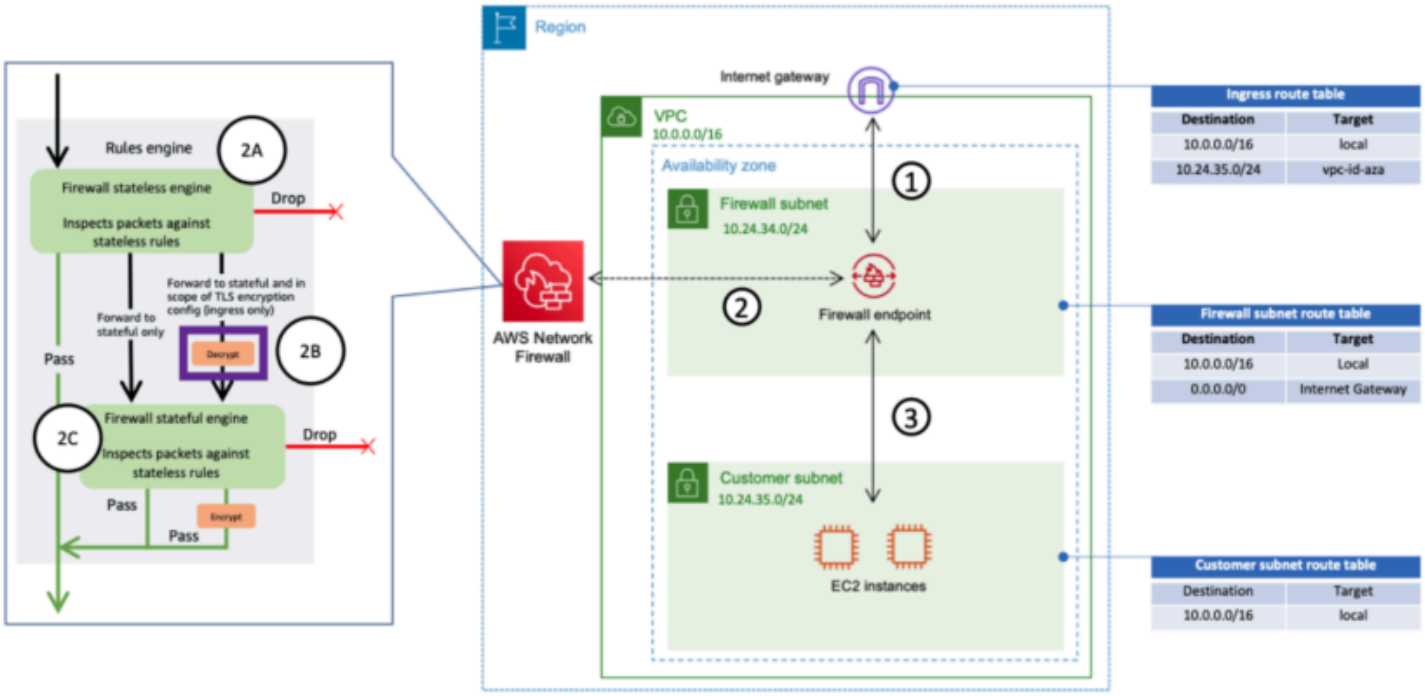


使用 AWS Network Firewall 检查入口流量

为了简化此模型 AWS Network Firewall 中的部署和管理， AWS Firewall Manager 可以使用。Firewall Manager 允许您通过自动将您在集中位置创建的保护应用于多个帐户来集中管理不同的防火墙。Firewall Manager 支持网络防火墙的分布式和集中式部署模式。博客文章《如何使用 AWS Network Firewall 进行部署》 AWS Firewall Manager提供了有关模型的更多详细信息。

使用深度数据包检测 (DPI) AWS Network Firewall

Network Firewall 可以对入口流量执行深度包检测 (DPI)。使用存储在 (ACM) 中的 AWS Certificate Manager 传输层安全 (TLS) 证书，Network Firewall 可以解密数据包、执行 DPI 和重新加密数据包。使用 Network 防火墙设置 DPI 需要考虑一些注意事项。首先，必须将可信的 TLS 证书存储在 ACM 中。其次，必须将 Network Firewall 规则配置为正确发送数据包进行解密和重新加密。有关更多详细信息，请参阅博客文章加密流量的 TLS 检查配置。 AWS Network Firewall



使用带有 DPI 的 Network Firewall 进行入口流量检查

集中式入口 AWS Network Firewall 架构中的关键注意事项

- 边缘 VPC 中的 Elastic Load Balancing 只能将 IP 地址作为目标类型，而不是主机名。在上图中，目标是分支 VPC 中 Network Load Balancer 的私有 IP。在边缘 VPC 中使用 ELB 后面的 IP 目标会导致 Auto Scaling 丢失。
- 考虑 AWS Firewall Manager 将其用作防火墙端点的单一管理面板。
- 这种部署模式在进入边缘 VPC 时直接使用流量检查，因此有可能降低检查架构的总体成本。

DNS

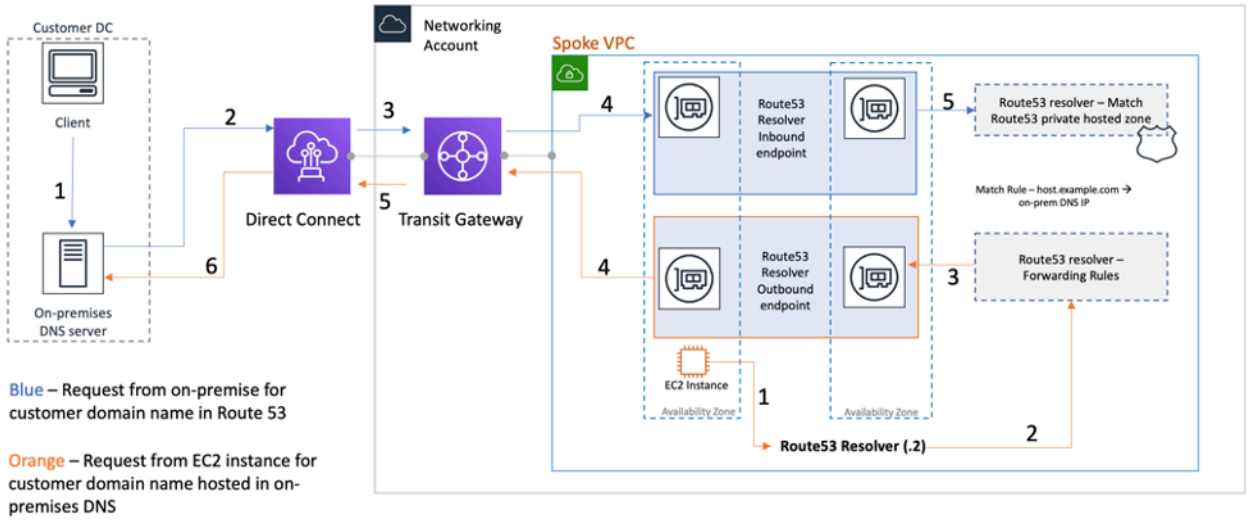
当您将实例启动到 VPC（不包括默认 VPC）时，根据您为 VPC 指定的 DNS 属性以及您的实例是否具有公有 IPv4 地址，为该实例 AWS 提供私有 DNS 主机名（可能还有公有 DNS 主机名）。 当该enableDnsSupport属性设置为时true，您将从 Route 53 解析器获得 VPC 内的 DNS 解析（与 VPC CIDR 的 IP 偏移量+2）。默认情况下，Route 53 Resolver 会回答 VPC 域名的 DNS 查询，例如 EC2 实例的域名或 Elastic Load Balancing 负载均衡器的域名。通过 VPC 对等互连，一个 VPC 中的主机可以将公有 DNS 主机名解析为对等 VPC 中实例的私有 IP 地址，前提是启用了这样做的选项。这同样适用于通过 AWS Transit Gateway连接的 VPC。有关更多信息，请参阅为 VPC 对等连接启用 DNS 解析支持。

如果您想将您的实例映射到自定义域名，则可以使用 Amazon Route 53 创建自定义 DNS 到 IP 的映射记录。Amazon Route 53 托管区域是一个容器，其中包含有关您希望 Amazon Route 53 如何响应域及其子域名的 DNS 查询的相关信息。公共托管区域包含可通过公共互联网解析的 DNS 信息，而私有托管区域是一种特定的实现，仅向已连接到特定私有托管区域的 VPC 提供信息。在拥有多个 VPC 或账户的着陆区域设置中，您可以将单个私有托管区域与 AWS 账户和跨区域的多个 VPC 相关联（仅适用于 SD K/CLI/API）。VPC 中的终端主机使用各自的 Route 53 解析器 IP（+2 偏移 VPC CIDR）作为 DNS 查询的域名服务器。VPC 中的 Route 53 解析器仅接受来自 VPC 内资源的 DNS 查询。

混合 DNS

DNS 是任何基础架构（无论是混合还是其他基础架构）的关键组件，因为它提供了应用程序所依赖的主机名到 IP 地址的解析。实施混合环境的客户通常已经安装了 DNS 解析系统，他们想要一种与当前系统配合使用的 DNS 解决方案。使用 VPN 或无法从本地网络访问本地 Route 53 解析器（基本 VPC CIDR 的偏移量 +2）。 AWS Direct Connect因此，当您将 AWS 区域的 VPC 的 DNS 与您的网络的 DNS 集成时，您需要一个 Route 53 Resolver 入站终端节点（用于转发到 VPC 的 DNS 查询）和一个 Route 53 Resolver 出站终端节点（用于从 VPC 转发到网络的查询）。

如下图所示，您可以配置出站解析器终端节点，将其从您的 VPC 中的 Amazon EC2 实例收到的查询转发到您网络上的 DNS 服务器。要将选定的查询从 VPC 转发到本地网络，请创建 Route 53 解析器规则，指定要转发的 DNS 查询的域名（例如 example.com），以及网络上要转发查询的 DNS 解析器的 IP 地址。对于从本地网络到 Route 53 托管区域的入站查询，您网络上的 DNS 服务器可以将查询转发到指定 VPC 中的入站解析器终端节点。

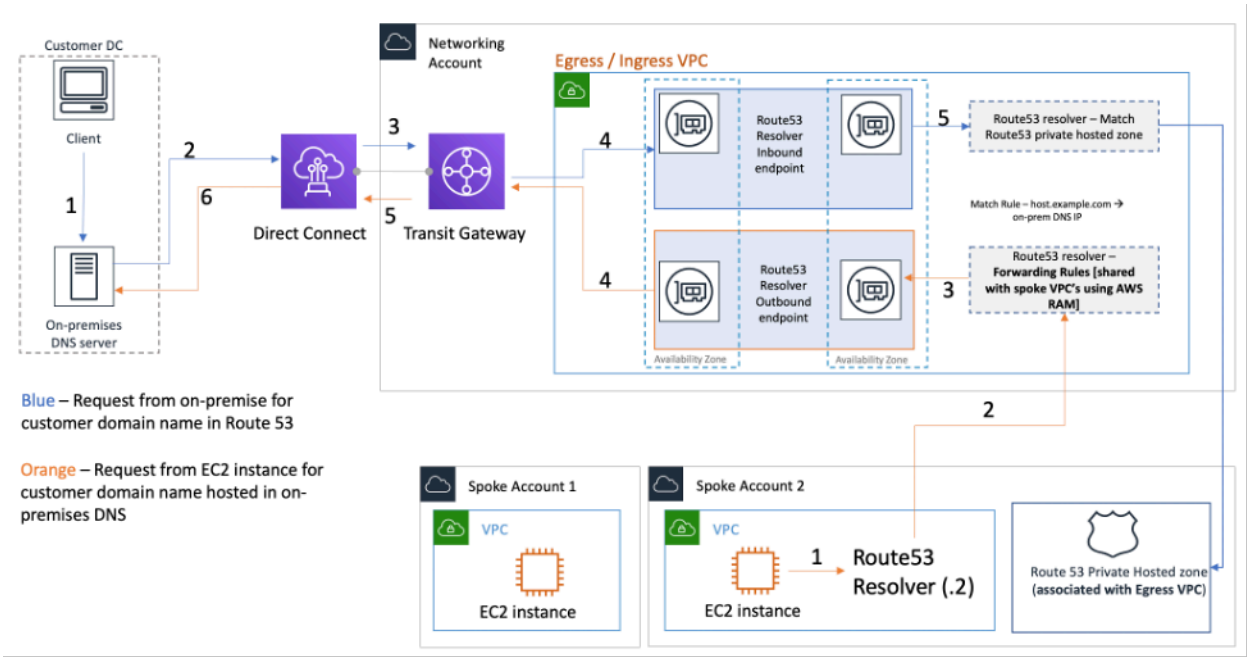


使用路由 53 解析器进行混合 DNS 解析

这使您的本地 DNS 解析器可以轻松解析 AWS 资源的域名，例如 Amazon EC2 实例或与该 VPC 关联的 Route 53 私有托管区域中的记录。此外，Route 53 解析器端点每个 ENI 每秒最多可处理 10,000 个查询，因此可以轻松扩展到更大的 DNS 查询量。有关更多详细信息，请参阅 Amazon Route 53 文档中的 R esolver 最佳实践。

不建议您在着陆区的每个 VPC 中创建 Route 53 解析器终端节点。将它们集中在中央出口 VPC（在网络服务账户中）。这种方法可以提高可管理性，同时保持低成本（您创建的每个入站/出站解析器端点都要按小时收费）。您与着陆区的其余部分共享集中式入站和出站终端节点。

- 出站解析-使用网络服务帐户编写解析器规则（根据这些规则，DNS 查询将转发到本地 DNS 服务器）。使用 Resource Access Manager (RAM)，与多个账户共享这些 Route 53 解析器规则（并与账户中的 VPC 关联）。分支 VPC 中的 EC2 实例可以向 Route 53 解析器发送 DNS 查询，而 Route 53 解析器服务会通过出口 VPC 中的出站 Route 53 解析器终端节点将这些查询转发到本地 DNS 服务器。 您无需将分支 VPC 与出口 VPC 对等，也不需要通过 Transit Gateway 将它们连接起来。请勿使用出站解析器终端节点的 IP 作为分支 VPC 中的主 DNS。分支 VPC 应在其 VPC 中使用 Route 53 解析器（以抵消 VPC CIDR）。



将 Route 53 解析器终端节点集中到入口/出口 VPC 中

- 入站 DNS 解析 — 在集中式 VPC 中创建 Route 53 Resolver 入站终端节点，并将您的着陆区域中的所有私有托管区域与该集中式 VPC 关联起来。有关更多信息，请参阅将更多 VPC 与私有托管区域关联。与 VPC 关联的多个私有托管区域 (PHZ) 不能重叠。如上图所示，PHZ 与集中式 VPC 的这种关联将使本地服务器能够使用集中式 VPC 中的入站终端节点为任何私有托管区域（与中央 VPC 关联）中的任何条目解析 DNS。 有关混合 DNS 设置的更多信息，请参阅使用 A mazon Route 53 和 AWS Transit Gateway 对混合云进行集中化 DNS 管理以及亚马逊 VPC 的混合云 DNS 选项。

Route 53 DNS 防火墙

Amazon Route 53 Resolver DNS 防火墙有助于筛选和调节您的 VPC 的出站 DNS 流量。DNS 防火墙的主要用途是通过定义域名允许列表来帮助防止数据泄露，允许您的 VPC 中的资源仅向您的组织信任的站点发出出站 DNS 请求。它还使客户能够为他们不希望通过 DNS 与 VPC 内的资源进行通信的域名创建阻止名单。 Amazon Route 53 Resolver DNS 防火墙具有以下功能：

客户可以创建规则来定义如何回答 DNS 查询。可以为域名定义的操作包括`NODATA`、`OVERRIDE`和`NXDOMAIN`。

客户可以为允许名单和拒绝名单创建警报，以监控规则活动。当客户想要在将规则投入生产之前对其进行测试时，这可以派上用场。

有关更多信息，请参阅如何开始使用适用于 Amazon VPC Amazon Route 53 Resolver 的 DNS 防火墙博客文章。

集中访问 VPC 私有终端节点

VPC 终端节点允许您私密地将您的 VPC 连接到支持的 AWS 服务，而无需互联网网关或 NAT 设备、VPN AWS Direct Connect 连接或连接。因此，您的 VPC 不会对公有 Internet 公开。您的 VPC 中的实例不需要公有 IP 地址即可通过此接口终端节点与 AWS 服务终端节点通信。您的 VPC 与其他服务之间的流量不会离开 AWS 网络主干。VPC 终端节点是虚拟设备。它们是水平扩展、冗余和高度可用的 VPC 组件。目前可以配置两种类型的终端节点：接口终端节点（由提供支持 AWS PrivateLink）和网关终端节点。网关终端节点可用于私下访问亚马逊 S3 和亚马逊 DynamoDB 服务。使用网关终端节点不会发生任何额外费用。采用标准的数据传输和资源使用计费方式。

接口 VPC 端点

接口终端节点由一个或多个弹性网络接口组成，其私有 IP 地址用作发往受支持 AWS 服务的流量的入口点。当您配置接口终端节点时，终端节点每运行一小时就会产生一定的费用以及数据处理费用。默认情况下，您可以在要从中访问 AWS 服务的每个 VPC 中创建一个接口终端节点。在客户想要跨多个 VPC 与特定 AWS 服务进行交互的着陆区设置中，这可能成本高得令人望而却步，而且管理起来也很困难。为避免这种情况，您可以将接口终端节点托管在集中式 VPC 中。所有分支 VPC 都将通过 Transit Gateway 使用这些集中式终端节点。

在为 AWS 服务创建 VPC 终端节点时，您可以启用私有 DNS。启用后，该设置将创建 AWS 托管的 Route 53 私有托管区域 (PHZ)，从而允许将公共 AWS 服务终端节点解析为接口终端节点的私有 IP。托管 PHZ 仅在 VPC 内使用接口终端节点。在我们的设置中，当我们希望分支 VPC 能够解析集中式 VPC 中托管的 VPC 终端节点 DNS 时，托管 PHZ 将无法运行。要解决这个问题，请禁用在创建接口终端节点时自动创建私有 DNS 的选项。接下来，手动创建 Route 53 PHZ 并添加一个别名记录，其中包含指向接口终端节点的完整 AWS 服务终端节点名称。

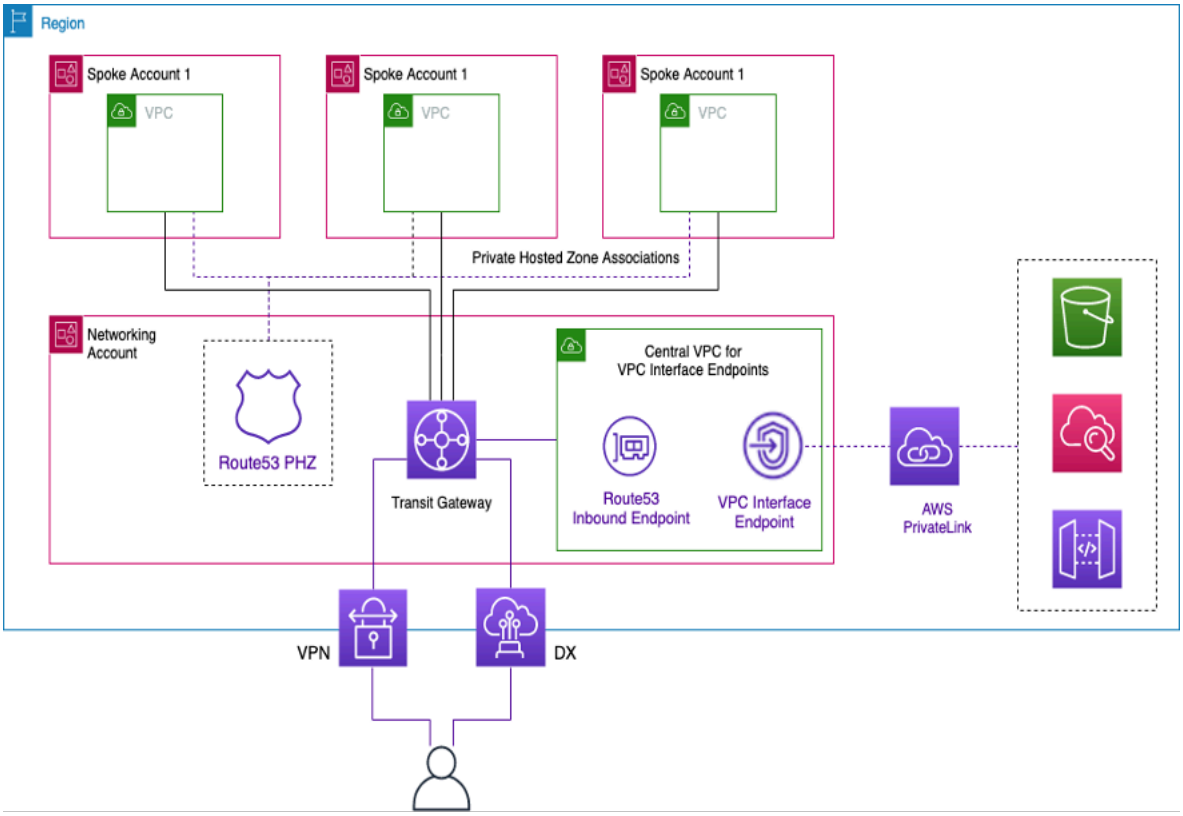
1. 登录控制台并导航到服务 Route 53。
2. 选择私有托管区域并导航到 “创建记录”。
3. 填充 “记录名称” 字段，选择 “记录类型” 为 A，然后启用 “别名”。
4. 在 “将流量路由到” 部分下，选择应将流量发送到的服务，然后从下拉列表中选择区域。
5. 选择相应的路由策略并确保启用 “评估目标运行状况” 选项。

您可以将此私有托管区域与着陆区域内的其他 VPC 相关联。此配置允许分支 VPC 将全方位服务终端节点名称解析为集中式 VPC 中的接口终端节点。

> **Note**
>
> 要访问共享私有托管区域，分支 VPC 中的主机应使用其 VPC 的 Route 53 解析器 IP。也可以通过 VPN 和 Direct Connect 从本地网络访问接口终端节点。使用条件转发规则将全方位服务终端节点名称的所有 DNS 流量发送到 Route 53 Resolver 入站终端节点，后者将根据私有托管区域解析 DNS 请求。

在下图中，Transit Gateway 支持流量从分支 VPC 流向集中式接口终端节点。在网络服务账户中创建 VPC 终端节点及其私有托管区域，并与分支账户中的分支 VPC 共享。有关与其他 VPC 共享终端节点信息的更多详细信息，请参阅将 AWS Transit Gateway 与 AWS PrivateLink Amazon Route 53 Resolver 集成的博客文章。

> **Note**
>
> 分布式 VPC 终端节点方法，即每个 VPC 一个终端节点，允许您对 VPC 终端节点应用最低权限策略。在集中式方法中，您将在单个终端节点上应用和管理所有分支 VPC 访问的策略。随着 VPC 数量的增加，使用单个策略文件保持最低权限的复杂性可能会增加。单一的策略文件还会导致更大的爆炸半径。您的政策文件的大小也受到限制（20,480 个字符）。



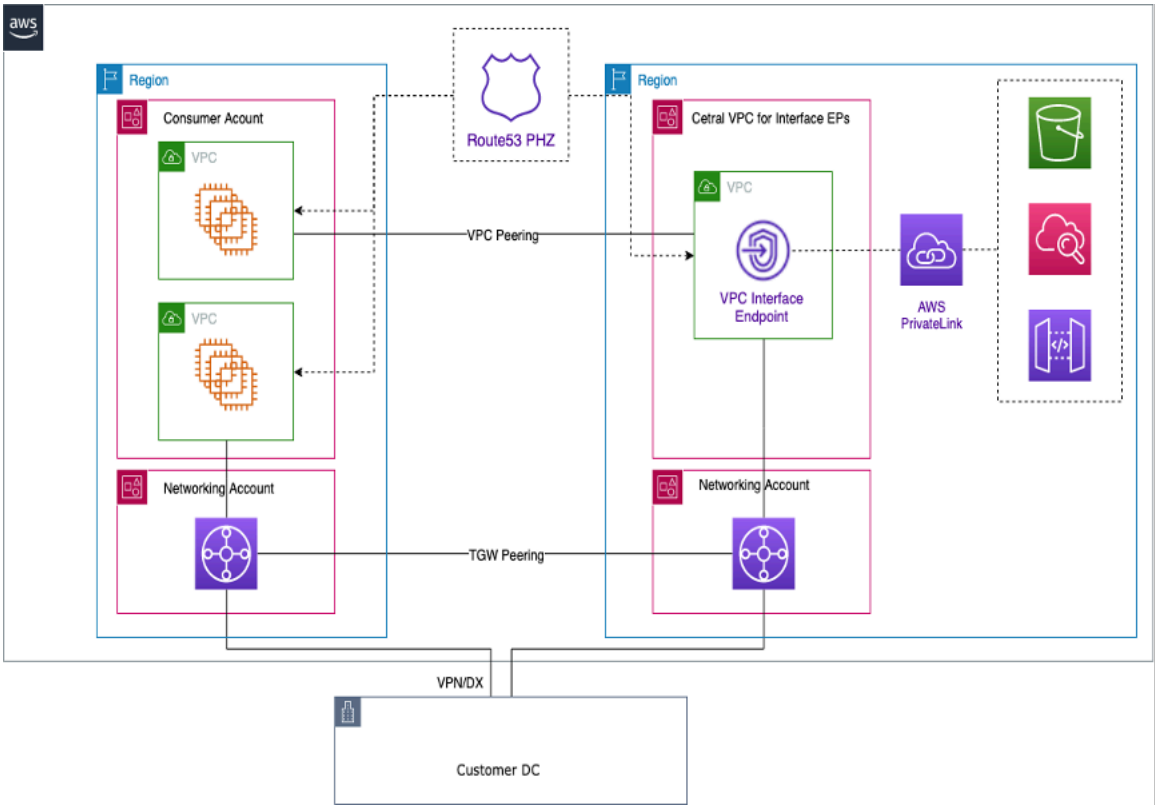
集中接口 VPC 终端节点

跨区域终端节点访问

如果您想在不同的区域设置多个 VPC，共享一个通用 VPC 终端节点，请使用前面所述的 PHZ。每个区域中的两个 VPC 都将与终端节点别名的 PHZ 关联。为了在多区域架构中的 VPC 之间路由流量，需要将每个区域中的传输网关连接在一起。有关更多信息，请参阅此博客：将 Route 53 私有托管区域用于跨账户多区域架构。

可以使用传输网关或 VPC 对等互连将来自不同区域的 VPC 路由到彼此。使用以下文档进行公交网关对等：公交网关对等连接附件。

在此示例中，VPC `us-west-1` 区域中的 Amazon EC2 实例将使用 PHZ 获取该区域终端节点的私有 IP 地址，并通过 Transit Gateway 对等互连或 VPC 对等将流量路由到`us-west-2`区域 VPC。`us-west-2`使用此架构，流量将保留在 AWS 网络中`us-west-1`，从而安全地允许进入的 EC2 实例`us-west-2`无需通过互联网即可访问 VPC 服务。



多区域 VPC 终端节点

> **Note**
>
> 跨区域访问终端节点时，确实会收取区域间数据传输费用。

参照上图，终端节点服务是在us-west-2该区域的 VPC 中创建的。此终端节点服务提供对该区域的 AWS 服务的访问权限。为了让您在其他区域（例如us-east-1）的实例访问该us-west-2区域的终端节点，您需要在 PHZ 中创建地址记录，并使用所需 VPC 终端节点的别名。

首先，请确保每个区域中的 VPC 都与您创建的 PHZ 相关联。

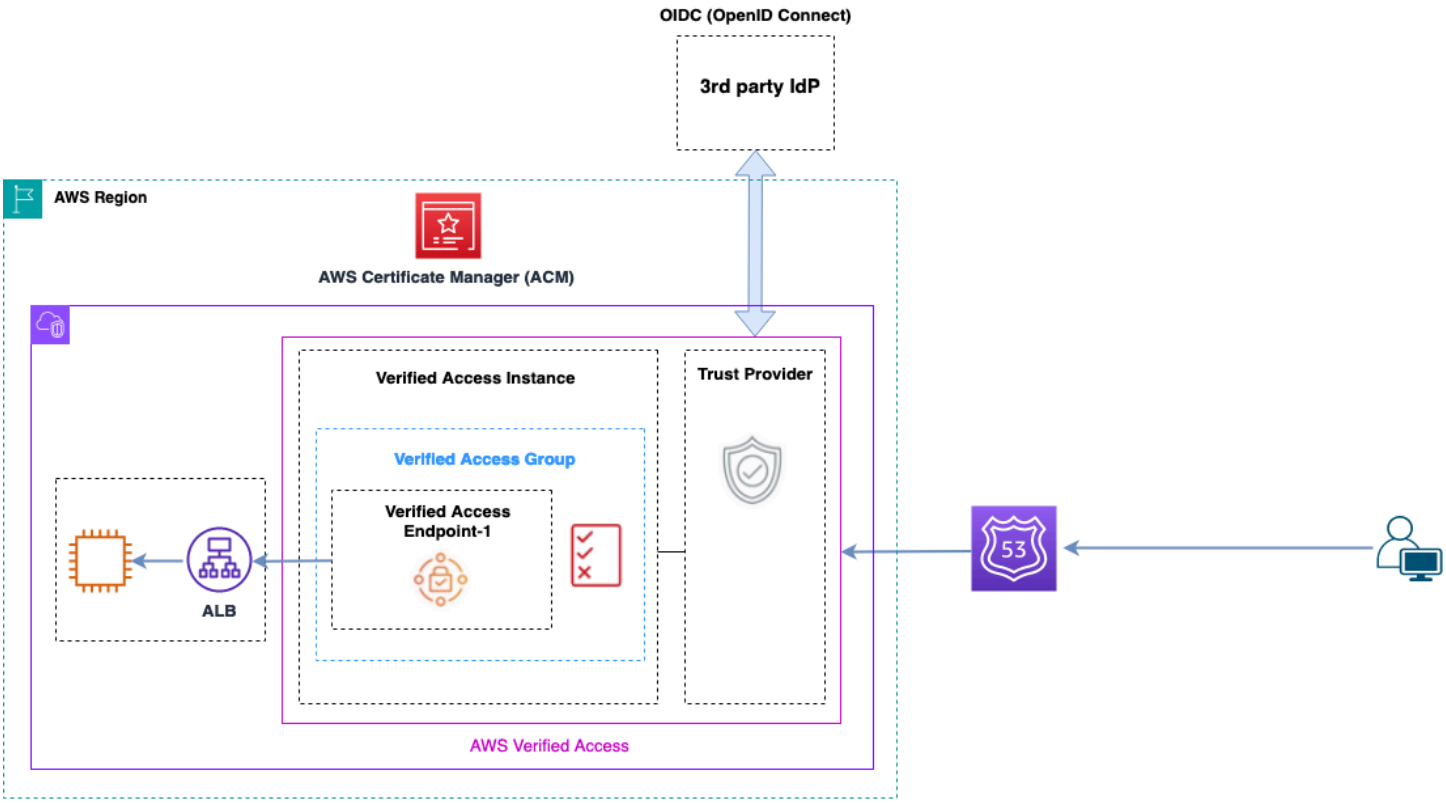
在多个可用区中部署终端节点时，从 DNS 返回的终端节点的 IP 地址将来自已分配的可用区中的任何子网。

调用终端节点时，请使用 PHZ 中的完全限定域名 (FQDN)。

AWS Verified Access

AWS Verified Access 无需使用 VPN 即可安全访问私有网络中的应用程序。它会实时评估身份、设备和位置等请求。该服务根据应用程序的策略授予访问权限，并通过提高组织的安全性来连接用户。Verified Access 通过充当身份感知反向代理来提供对私有应用程序的访问权限。如果适用，则在将流量路由到应用程序之前执行用户身份和设备运行状况。

下图提供了 Verified Access 的简要概述。用户发送访问应用程序的请求。Verified Access 根据组的访问策略和任何特定于应用程序的端点策略来评估请求。如果允许访问，请求会通过端点发送到应用程序。



已验证访问权限概述

AWS Verified Access 架构中的主要组件有：

- Verified Access 实例 – 一个实例评估应用程序请求并仅在您的安全要求获得满足时才授予访问权限。
- Verified Access 端点 – 每个端点代表一个应用程序。端点可以是 NLB、ALB 或网络接口。
- Verified Access 组 – Verified Access 端点的集合。我们建议您对具有相似安全要求的应用程序的端点进行分组，以简化策略管理。

- 访问策略 – 一组用户定义的规则，用于确定是允许还是拒绝访问应用程序。
- 信任提供商 — Verified Access 是一项便于管理用户身份和设备安全状态的服务。它与两者 AWS 兼容，也与第三方信任提供商兼容，要求每个已验证访问实例至少有一个信任提供商。这些实例中的每一个都可以包括一个身份信任提供商以及多个设备信任提供商。
- 信任数据 — 每次收到应用程序请求时，都会根据您的访问策略评估您的信任提供商发送给 Verified Access 的安全数据，例如用户的电子邮件地址或他们所属的群组。

更多详细信息可以在已验证访问权限博客文章中找到。

结论

随着您在 AWS 着陆区扩大使用量 AWS 和部署应用程序，VPC 和网络组件的数量就会增加。本白皮书解释了如何管理这种不断增长的基础架构，确保可扩展性、高可用性和安全性，同时保持低成本。在使用 Transit Gateway、共享 VPC、VPC 终端节点 AWS Direct Connect、Gateway Load Balancer AWS Network Firewall、Amazon Route 53 和第三方软件设备等服务时，做出正确的设计决策变得至关重要。重要的是要了解每种方法的关键考虑因素，并根据您的要求进行反向研究，并分析哪种选项或选项组合最适合您。

贡献者

以下个人参与了本文档的编撰：

- Sohaib Tahir，Amazon Web Services 解决方案架构师
- Shirin Bhambhani，Amazon Web Services 解决方案架构师
- Kunal Pansari，Amazon Web Services 解决方案架构师
- Eric Vasquez，Amazon Web Services 解决方案架构师
- Tushar Jagdale，Amazon Web Services 解决方案架构师
- Ameer Shariff，Amazon Web Services 解决方案架构师
- Glenn Davis，Amazon Web Services 解决方案架构师
- Nick Kniveton，Amazon Web Services 解决方案架构师
- Sidhartha Chauhan，Amazon Web Services 首席解决方案架构师

文档历史记录

要获得有关白皮书更新的通知，请订阅 RSS 源。

变更	说明	日期
主要更新	白皮书中更新了 CloudWAN、Amazon VPC Lattice、ENA Express、混合连接、Sit AWS Direct Connect elink、Deep Packet Inspection 和。 AWS Verified Access	2024 年 4 月 17 日
次要更新	更新了图表以使其更加一致，更新了 DX 连接选项以包括私有 IP VPN，并在整个过程中进行了许多细微的更改。	2023 年 7 月 6 日
次要更新	更新了 AWS Control Tower 信息，反映了各种服务的新吞吐量限制，更新了 NAT 网关图，更新了集中出口的安全部分。	2023 年 4 月 4 日
次要更新	新增：跨区域终端节点访问章节。	2022 年 7 月 19 日
主要更新	使用 Transit Gateway Connect 更新了 Transit Gateway 部分，更新了 Transit VPC AWS Direct Connect 部分；更新了包含 MacSec 和弹性建议的部分；更新了 AWS PrivateLink 部分。添加了 VPC 对等与传输 VPC 与 Transit Gateway 对比表；添加了集中式入站检查部分；更新了 VPC 到 VPC 和 VPC 本地到 VPC 的集中式网	2022 年 2 月 22 日

	络安全，以及使用网关 AWS Network Firewall 负载均衡器设计模式的集中式互联网出口；添加了私有 NAT 网关和 Amazon Route 53 DNS 防火墙部分。	
次要更新	更新了 Transit Gateway 与 VPC 对等互连部分	2021 年 4 月 2 日
已更新白皮书	更正了文本以匹配图 7 所示的选项	2020 年 6 月 10 日
初次发布	已发布白皮书。	2019 年 11 月 15 日

声明

客户有责任对本文档中的信息，进行独立评估。本文档：(a) 仅供参考；(b) 代表 AWS 现有的产品服务和实践，如有变更，恕不另行通知；以及 (c) 不构成 AWS 及其联属公司、供应商或授权商的任何承诺或保证。AWS 产品或服务“按原样”提供，不提供任何形式的保证、陈述或条件，无论是明示还是暗示。AWS 对其客户的责任和义务由 AWS 协议决定，本文档与 AWS 和客户之间签订的任何协议无关，亦不影响任何此类协议。

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。