管理网关

概述

多云防御网关 是一个基于网络的安全平台，由网络负载均衡器和 多云防御网关 实例集群组成。它是一个自动扩展和自我修复集群，可根据流量负载进行外向扩展和内向扩展。多云防御控制器和网关实例不断交换有关状态、运行状况和遥测的信息。多云防御控制器通过测量从网关实例接收的遥测数据来决定外向扩展/内向扩展。可以将网关配置为在多个可用性区域中运行，以实现高可用性、恢复能力的架构。这可确保云服务提供商的单个可用性区域故障不会影响运行应用的安全状态。

配置网关和任何相应的 VPC 或 VNet 后，您可以使用 多云防御控制器 中的 **网关详细信息** 页面查看和管理它们的状态。

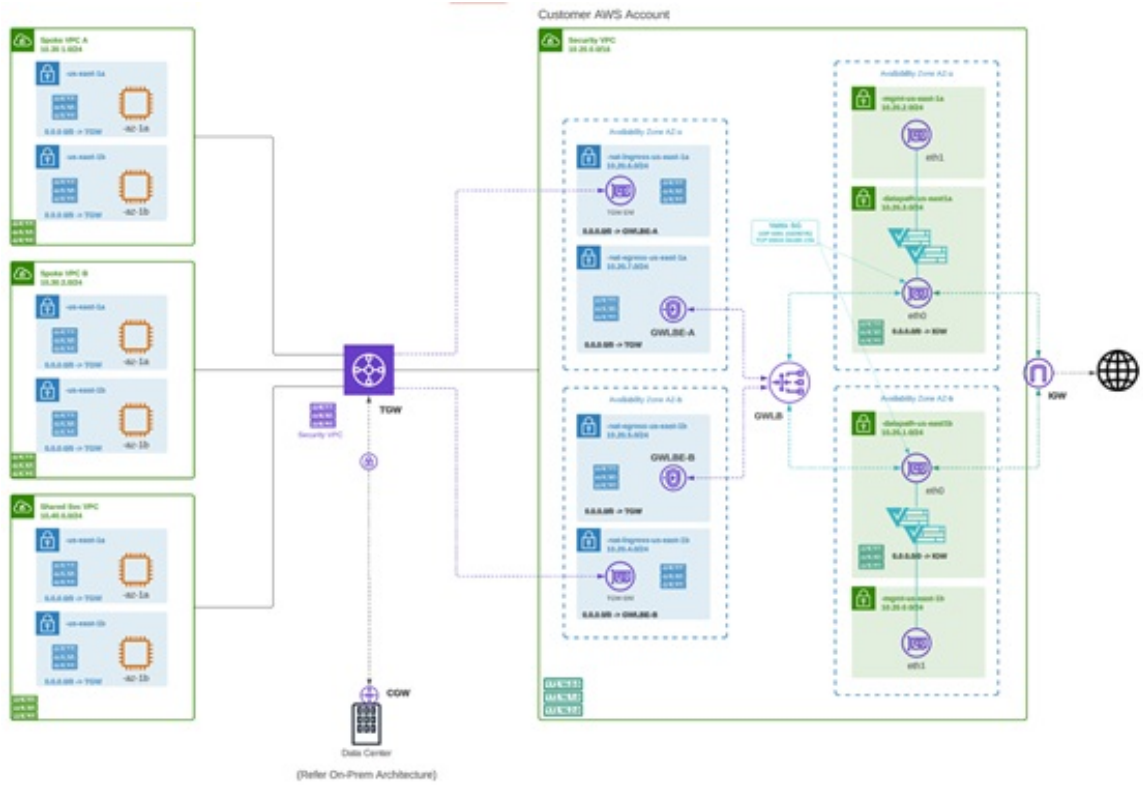
多云防御网关可以通过两种方式部署； **集线器** 模式和 **边缘** 模式。

支持的网关使用案例

出口

部署出口/东西向网关，以保护离开其公共云网络的流量。出口网关充当透明转发代理，执行完全解密并嵌入入侵防御、防恶意软件、防数据丢失和全路径URL过滤等高级安全功能。或者，它也可以在转发模式下运行，在这种模式下，它不会代理或解密流量，但仍会应用恶意IP阻止和FQDN过滤等安全功能。

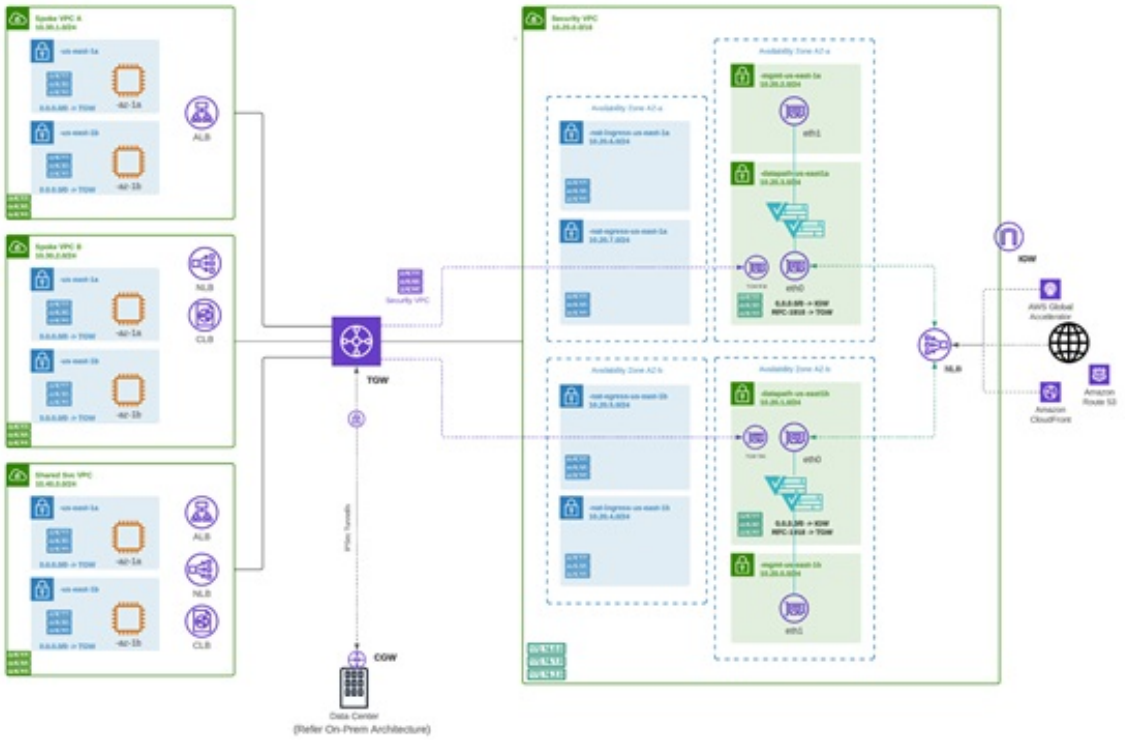
下图是集中式模式下具有出口网关的 AWS 账户示例：



入口

部署入口网关可保护面向公众的应用。入口网关充当执行完整解密的反向代理，并应用入侵防御、反恶意软件、Web 应用防火墙 (WAF) 和全路径 URL 过滤等高级安全功能。

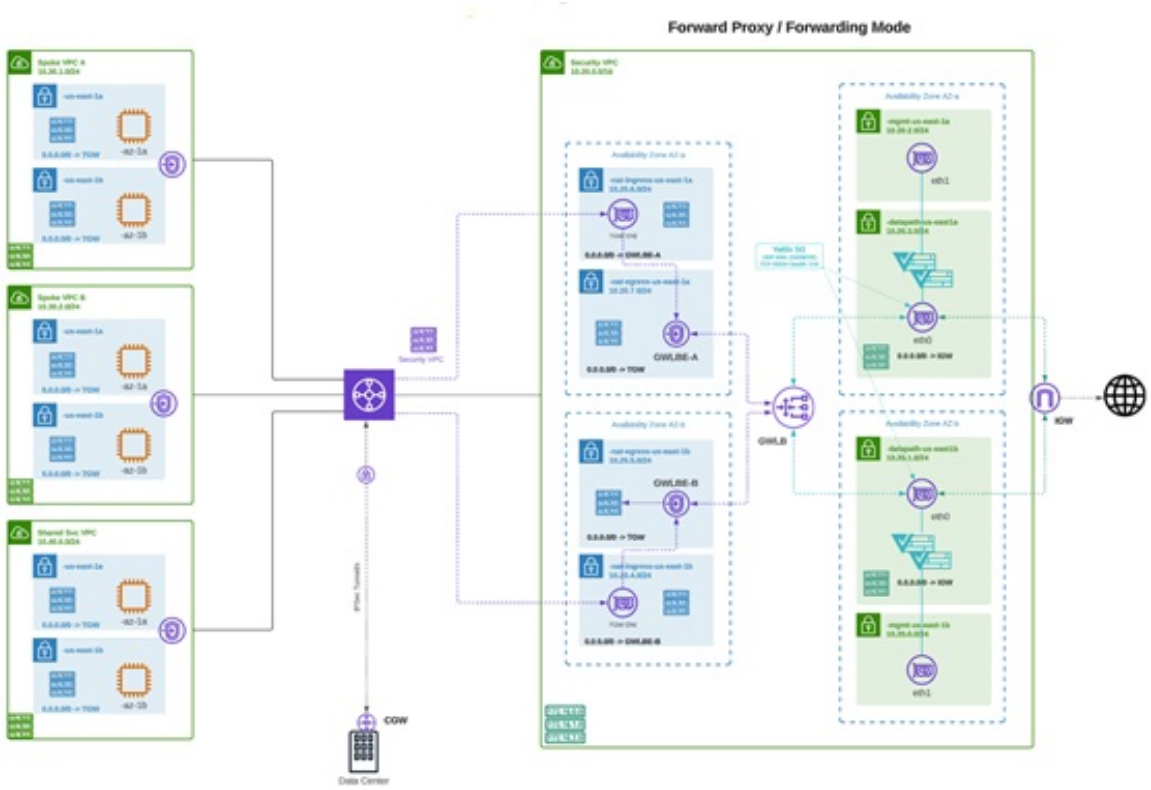
下图是在集中模式下具有入口网关的 AWS 账户示例：



东-西

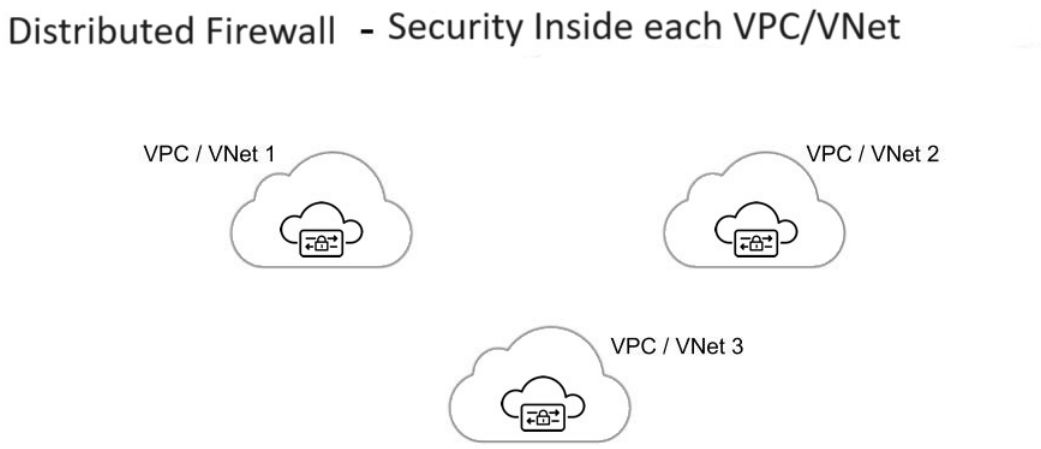
出口/东西网关部署在其公共云环境中的子网或 VPC/Vnet 之间实施东西 L4 分段。网关在具有 L4 防火墙规则的转发模式下运行，根据设置的参数允许或拒绝流量，并启用可选的日志记录。

下图是集中式模式下具有东西向网关的 AWS 账户示例：



分布式

您的应用在多个 VPC/VNet 中运行。在每个 VPC/VNet 中部署 多云防御网关 。



中央/枢纽

您的应用在多个 VPC/VNet 中运行。您希望通过集中式安全服务 VPC/VNet 保护所有应用。此模型在服务 VPC 中部署 多云防御网关 。将所有应用 VPC（分支 VPC）和服务 VPC 连接到 Azure 和 GCP 中的 AWS 传输网关或 VNet/VPC。 多云防御 提供用于协调 AWS 传输网关、服务 VPC 和分支 VPC 附件的选项。这是建议的解决方案，可简化部署，消除多个路由表和传输网关附件的复杂性。

Figure 1: AWS - 使用 ***AWS*** 传输网关

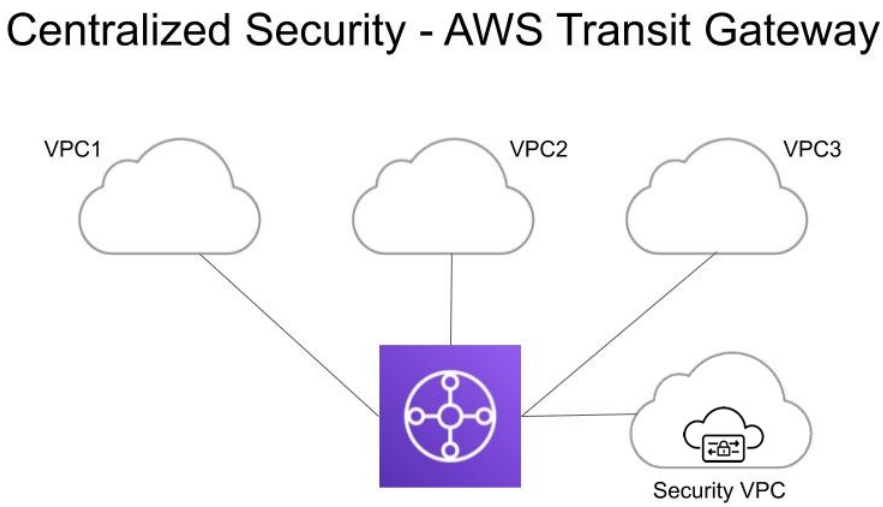


Figure 2: Azure - VNet 对等

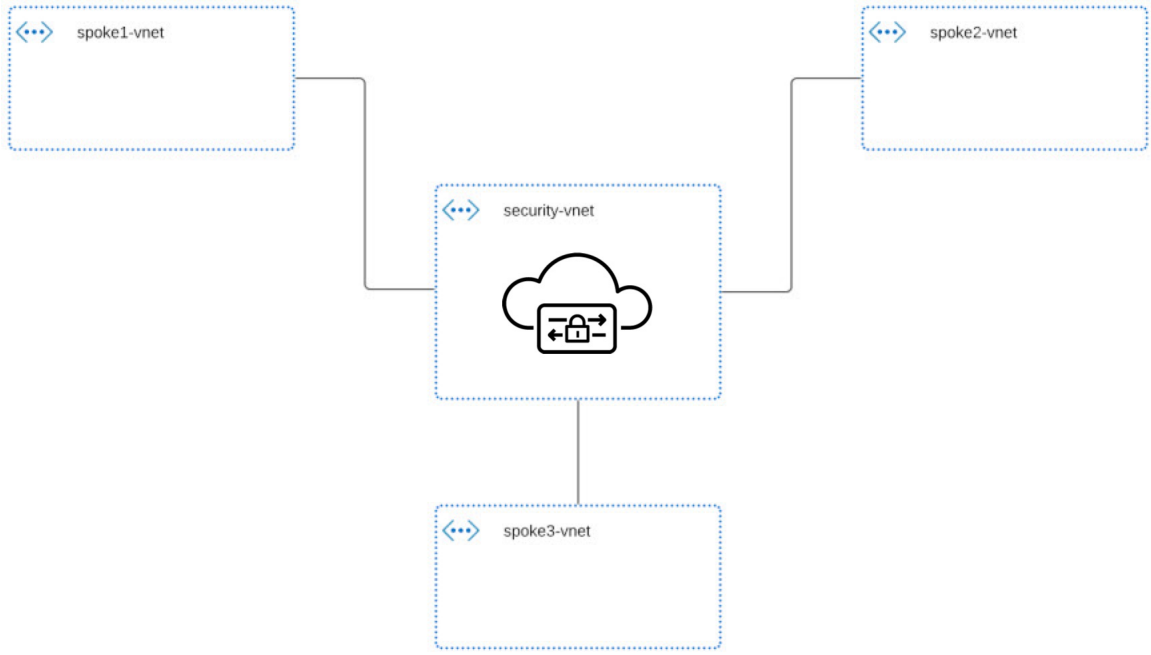
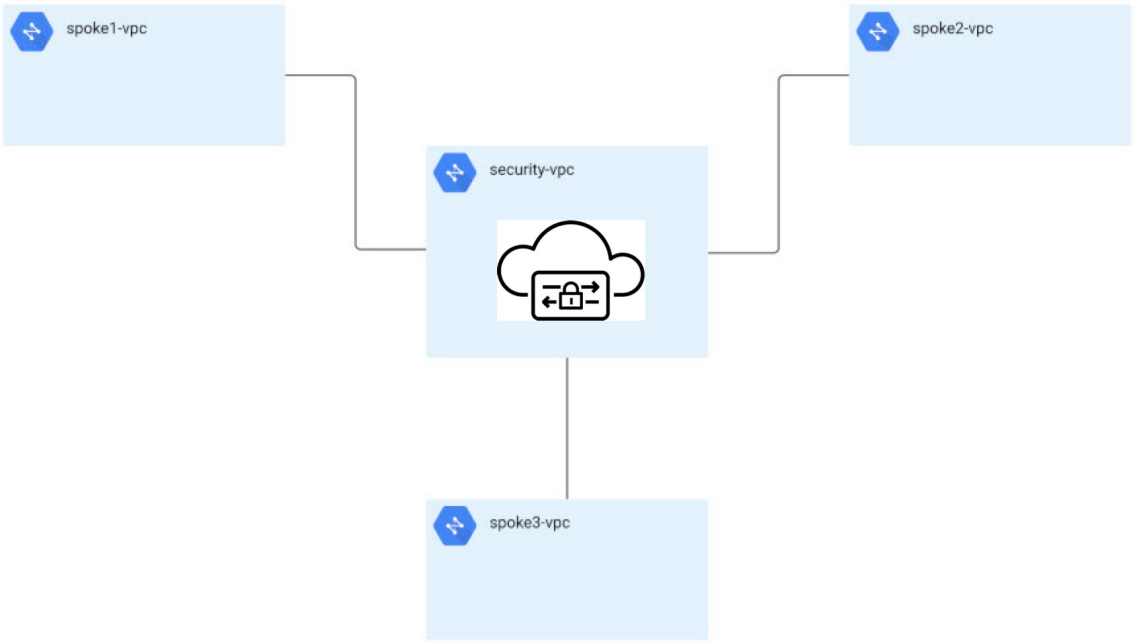


Figure 3: GCP - VPC 对等互连



高级使用案例

对于某些网关，可能有其他前提条件或后续步骤。请考虑以下环境：

AWS：入口网关加速器

多云防御 可以与一组一个或多个 AWS 全局加速器集成，用作入口点，在 多云防御网关 实例之间实现流量负载均衡。这类似于部署入口网关时由 多云防御 创建和管理的 AWS 网络负载均衡器，但为入口网关提供替代入口点以保护应用和工作负载。

加速器，它将管理全局加速器的侦听程序终端组，以确保终端组具有一组活动的网关实例。当客户端 IP 地址通过全局加速器到达 多云防御 入口网关时，这些地址将被保留。

要将 多云防御 与全局加速器集成，用户必须先在 AWS 中创建全局加速器，定义所需的侦听程序，并创建空终端组（或包含现有 多云防御 入口网关实例的终端组）。AWS 资源存在后，可以将 多云防御 入口网关配置为与全局加速器集成。

网关详细信息

要查看已建立网关的 **网关详细信息** 页面，请访问 **管理** > **网关**。您可以从此页面添加和管理所有网关。通过管理网关，您可以编辑、升级、启用、禁用、导出或删除实例。在进行任何更改之前，您必须点击要修改的网关的复选框。

注释 您 **必须** 是管理员或超级管理员才能执行这些操作。

要过滤和搜索网关列表，请使用以下条件：

- **名称** - 网关的名称。
- **CSP 账户** - 与网关关联的云服务提供商账户。
- **CSP 类型** - 云服务提供商账户的类型。
- **区域** - 与您要搜索的网关关联的云服务提供商的区域。
- **状态** - 网关的当前状态。网关可以是活动的或非活动的，也可以是待处理的活动或待定的非活动状态。
- **实例类型** - 每个云服务提供商都支持多种实例类型。
- **模式** - 多云防御网关 实例可以在中心或边缘模式下部署。

点击 **切换到高级搜索** 以构建您自己的搜索。如果需要，使用搜索栏中的下拉选项来利用一些自动生成的搜索条件。对于必须重复的搜索，您可以 **复制** 甚至 **保存** 搜索以供将来使用。

配置多云防御网关和 VPC/VNet

准备工作

支持的云服务提供商是使用自己的词汇和网关环境的独立实体。并非多云防御控制器中提供的每个选项都与您的云服务提供商兼容。例如，AWS 使用其自己的传输网关，您可以向其添加 VPC，而 Azure 利用负载均衡器来管理 Web 流量和应用，您可以向其添加 VNet。继续操作时，请记住这一点。

注释 对于 AWS 环境，在集中模式下保护分支 VPC 时， 多云防御 会将 VPC 连接到与服务 VPC 关联的传输网关。默认情况下， 多云防御 将在每个可用性区域中随机选择一个子网用于传输网关连接。您可以在添加 VPC 时更改此选项，也可以修改已分配给网关的 VPC。

您还可以通过 多云防御网关 协调中转网关或连接现有中转网关。

多云防御创建的资源

创建网关、VPC 或 VNet 时， 多云防御 会创建以下资源。这些是作为流程的一部分创建的，不需要用户执行任何其他操作。请注意，不同的资源是根据每个云服务提供商的要求创建的。

GCP 资源

多云防御 创建两个服务 VPC 和四个防火墙。有关确切的资源分配，请参阅以下内容：

服务 VPC

- 管理
- 数据路径

防火墙规则

- 管理（入口）
- 管理（出口）
- 数据路径（入口）
- 数据路径（出口）

注释 服务 VPC CIDR 不能 与分支 VPC 重叠。

AWS 原生资源

多云防御 创建三个服务 VPC 以解决支持的使用案例（入口、出口/东西向）。创建并附属于每个 VPC 的内容如下：

- 每个可用性区域中有四个子网。
- 每个子网一个路由表。
- 两个安全组：管理和数据路径。
- 一个传输网关。

注释 此传输网关在创建服务 VPC 期间创建并连接到网关。此网关可与其他服务 VPC 重复使用。

- 传输网关路由表。

注释 在创建过程中，路由表会附加到服务 VPC。

注释 AWS 网关负载均衡器 (GWLB) 不支持在初始部署 GWLB 后添加/删除可用性区域。如果需要更改可用性区域，则需要重新部署服务 VPC。有关详细信息，请参阅 AWS 文档。

Azure 资源

多云防御 使用以下资源创建了一个服务 VNet：

- 一个 VNet。
- 两个网络安全组。

服务 VNet CIDR 值不得与分支 VNet 重叠。

创建服务 VPC 或 VNet

使用以下程序创建服务 VPC 或服务 VNet，具体取决于您为其创建的网关。请注意特定于您的云服务提供商的选项。

步骤 1 从 多云防御控制器导航至 **管理** > **服务 VPC/VNet**。

步骤 2 点击 **创建服务 VPC/VNet**。

步骤 3 输入参数值：

- **名称** - 为服务 VPC/VNet 分配名称。
- **CSP 账户** - 选择用于创建服务 VPC/VNet 的 CSP 账户。
- **区域** - 选择服务 VPC 将部署到的区域。
- （仅限 Azure） **CIDR 块** - 服务 VNet 的 CIDR 块。这不能与您的分支（应用）VNet 重叠。
- （仅限 AWS/GCP）数据 **路径 CIDR 块** - 多云防御网关 数据路径服务 VPC 的 CIDR 块。此 CIDR 块不得与分支（应用）VPC 中的地址范围重叠。
- （仅限 AWS/GCP） **管理 CIDR 块** - 多云防御网关 管理服务 VPC 的 CIDR 块。此 CIDR 块不得与分支（应用）VPC 中的地址范围重叠。
- **可用性区域** - 多云防御 建议至少选择两个可用性区域以实现恢复能力。
- （仅限 Azure） **资源组** - 用于部署服务 VNet 的资源组。

步骤 4

下一步做什么

添加网关。

添加网关

使用以下程序为云服务提供商添加网关：

步骤 1 导航至 **管理** > **网关**。

步骤 2 点击 **添加网关**。

步骤 3 选择要向其添加网关的云服务提供商。

步骤 4 点击 **Next**。

步骤 5 输入以下信息：

- **实例类型** - 选择云服务提供商的类型。请注意，根据您使用的云服务提供商，可能有多种实例。
- **网关 Tpe** - 选择“入口”或“出口”。

  注释 如果您有东西向网络流，请选择 **出口** 。

- **最小实例** 数 - 选择您计划部署的最小实例数。
- **最大实例** 数 - 选择您计划部署的最大实例数。这是每个可用性区域中用于自动扩展的最大数量。
- **运行状况检查端口** - 默认值为 65534。 多云防御 负载均衡器用于检查实例运行状况的端口号。分配给实例的数据路径安全组必须允许此端口上的流量。
- （可选） **数据包捕获配置文件** - 威胁和流 PCAP 的数据包捕获配置文件。

- （可选） **诊断配置文件** - 用于存储技术支持信息的诊断配置文件。
- （可选） **日志配置文件** - 用于将事件/日志转发到 SIEM 的日志转发配置文件。

步骤 6 点击 **Next**。

步骤 7 提供以下各项参数：

- **安全** - 选择出口或入口。

  注释 如果您有东西向网络流，请选择 **出口** 。

- **网关映像** - 要部署的映像。
- **策略** 规则集 - 选择要与此网关关联的策略规则集。
- **区域** - 选择此网关将部署到的区域。
- **资源组** - 选择要与网关关联的资源组。
- **SSH 公钥** - 粘贴 SSH 公钥。控制器使用此公钥访问已部署网关实例的 CLI，以进行调试和监控。
- **VNet ID** - 选择要与网关关联的 VNet。
- **用户分配的身份 ID** - 输入要与此网关关联的云服务提供商身份。
- **管理安全组** - 选择要与管理接口关联的安全组。
- **数据路径安全组** - 选择要与数据路径接口关联的安全组。
- **磁盘加密** - 从下拉菜单中选择相应的选项。对于客户管理的加密密钥，用户需要输入加密密钥的资源 ID。

步骤 8 选择可用 **区**、 **管理子网** 和 **数据路径子网**。可用的子网将基于上面选择的 VPC 或 VNet。出于高可用性目的，可以在多个可用性区域中部署网关实例。点击加号按钮以添加新的可用性区域，并为所选区域选择参数。

注释 某些云服务提供商区域不支持多个可用性区域。在此类区域中，网关实例仅部署在单个区域中。

步骤 9 （仅限 Azure，可选）如果要在与应用相同的 VNet 中使用 多云防御网关 部署分布式模型，请确保完成以下操作：

- 在 Azure 门户中添加路由表，并将路由表与所有子网关联。
- 为 0.0.0.0/0 添加默认路由，并将 **下一跳** 作为网关网络负载均衡器的 IP 地址。

下一步做什么

在保护分支 VPC/VNet 之前， **必须** 将至少一个规则集附加到网关。有关详细信息，请参阅规则集和规则集组。

服务菜单中的安全分支 VPC/VNet

使用以下程序将辐射 VPC 或辐射 VNet 从服务菜单添加到网关：

开始之前

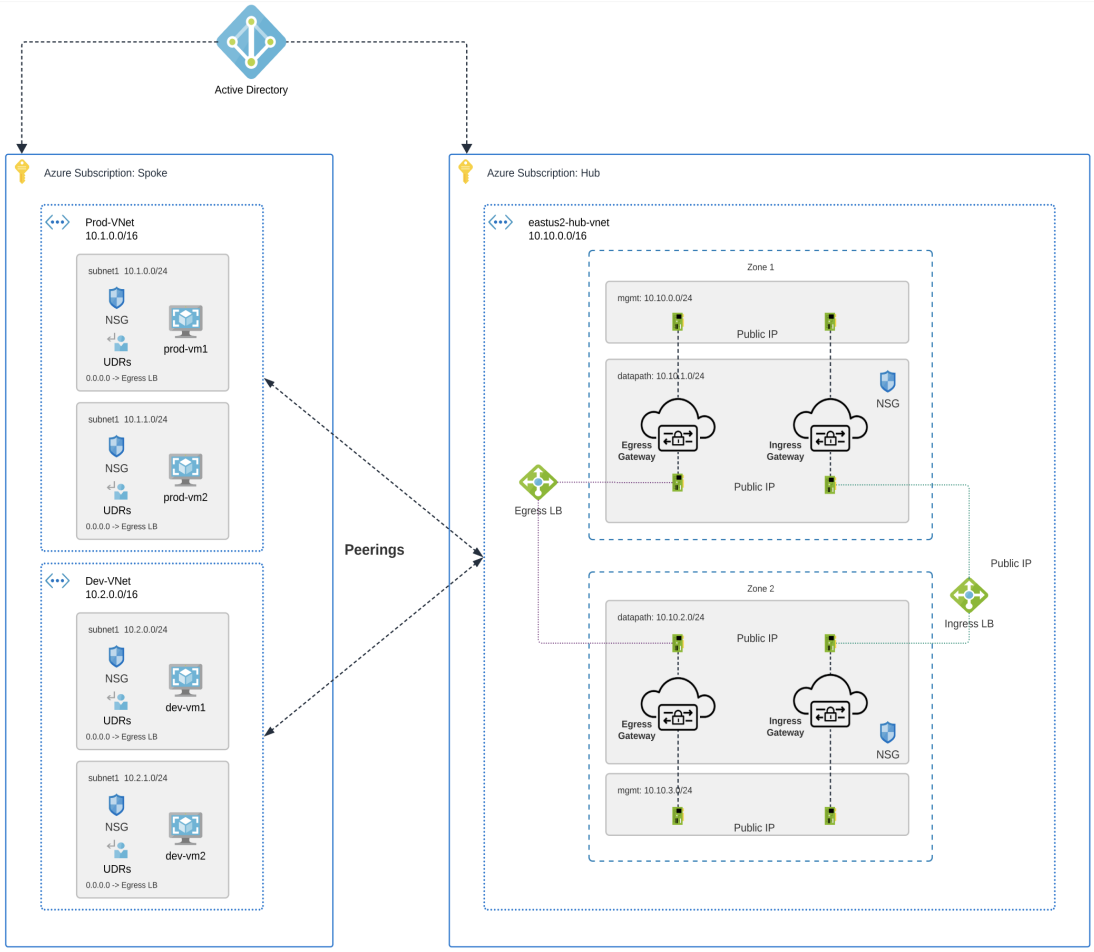
在创建和分配分支 VPC 或 VNet 之前，必须完成以下操作：

- 在 AWS 和 GCP 账户中，您必须在添加网关之前保护远程账户。
- 在保护分支 VPC/VNet **之前**，Azure 环境需要附加路由表。有关详细信息，请参阅 Azure 用户指南中的“将路由表关联到子网”一章。

请注意，当您在集中模式下使用 VPC 保护 AWS 辐射点时，多云防御 将 VPC 附加到与服务 VPC 关联的传输网关。将 VPC 连接到传输网关时，用户可以选择在每个可用区中放置 ENI 的子网。默认情况下，多云防御 将在每个可用性区域中随机选择一个子网用于传输网关连接。

同一 CSP 类型中的账户之间支持 VNet 配对。您可以在账户内和跨账户添加分支 VPC/VNet。在 Azure 中，对于跨订用的分支 VPC，应使用相同的应用注册自行激活 CSP 账户，并且订用应位于同一 Active Directory 中。

图 *4: Azure* 组合中心 - 多订用



步骤 1 从 多云防御控制器 控制面板，导航至 **管理** > **服务 VPC/VNet**。

步骤 2 选择服务 VPC 或服务 VNet，然后导航至 **操作** > **管理分支 VPC/VNet**。

步骤 3 添加所有辐射 VPC 或 VNet 以保护辐射表。

您可以从 **当前账户的**分支 VNet 中选择分支 VPC 或 VNet。如果要从其他账户添加分支 VPC 或 VNet，请从其他账户的 **分支 VNet 中进行**选择。

步骤 4 点击路由表列下的 **查看/编辑** 链接。

步骤 5 选中 **通过多云防御网关发送流量** 复选框，将默认路由更新为指向 多云防御网关 以进行检查。

步骤 6 点击 **更新路由**。

步骤 7 点击**保存 (Save)**。

升级 多云防御网关

多云防御网关充当自动扩展自我修复平台即服务 (Paas)，充当基于网络的内联安全实施节点。与传统防火墙不同， 多云防御 使客户无需构建虚拟防火墙、配置高可用性设置或管理软件安装。

多云防御网关 实例在高度优化的软件上运行，并结合了单通道数据路径管道，以实现高效的流量处理和高级安全实施。每个网关实例包含三个核心进程：负责策略实施的“工作线程”进程、用于流量分配和会话管理的“分发器”进程，以及与控制器通信的“代理”进程。网关实例可以无缝过渡到“服务中”，以实现“数据路径重启”，从而在不中断流量的情况下实现平稳升级。

使用新映像启动新实例。实例完全启动后，它们将放置在负载均衡器（流向网关实例的流的第 4 层 Sprayer）目标池中。对于通过它们的现有数据流，旧实例将处于数据流耗尽模式或数据流超时模式。新流将命中新实例。超时 (Azure) 或流量耗尽 (AWS) 后，控制器将获取旧实例。

请使用以下程序

步骤 1 导航至 **管理** > **网关**。

步骤 2 选中要升级的网关的复选框。此时只能选择一个选项。

步骤 3 选择 **操作** > **升级**。

步骤 4 从 **网关映像** 列表中，选择所需的映像。

步骤 5 点击**保存**。

步骤 6 确认升级所需的云服务提供商资源分配。

步骤 7 如果资源分配足够，请点击 **Yes** 。如果资源分配不足，请点击 **否** ，增加云服务提供商的资源分配，然后返回以继续升级。

Note 您可以从网关的实例信息查看升级进度和正在创建的新网关实例。选择网关并查看详细信息窗格中的 **实例** 。

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。