Cisco Multicloud Defense

アーキテクチャガイド

2024 年 3 月

目次

概要

『Cisco Multicloud Defense アーキテクチャガイド』では、Cisco Multicloud Defense ソリューションが各クラウドプロバイダー内および各セキュリティのユースケースでどのように展開されるかを示すリファレンスアーキテクチャ図を掲載しています。リファレンスアーキテクチャ図は、さまざまなセキュリティ要件に対応するために利用できるアーキテクチャの展開シナリオを示したものです。Cisco Multicloud Defense によって、高度なワークロード保護の展開と管理をオーケストレーションすることで、クラウドセキュリティを簡素化します。本リファレンスアーキテクチャは、Cisco Multicloud Defense の展開方法に関する情報をユーザーに提供するためのものであり、手動設定の方法を説明するものではありません。

Cisco Multicloud Defense ソリューションは、Controller/UI、Gateway、Terraform プロバイダーというコンポーネントの組み合わせで構成されています。Cisco Multicloud Defense Controller/UI は SaaS として提供されるコンポーネントで、維持管理はシスコが行います。Multicloud Defense Gateway は PaaS コンポーネントです。お客様のクラウド サービス プロバイダー（CSP）のアカウント、サブスクリプション、プロジェクト内に展開され、Cisco Defense Orchestrator（CDO）で管理します。Multicloud Defense Gateway は、Multicloud Defense UI または Multicloud Defense Terraform プロバイダーを活用した CDO によってオーケストレーションされ、管理されます。本リファレンスアーキテクチャでは特に、Multicloud Defense Gateway を展開してクラウドのワークロードを保護する方法について重点的に取り上げます。

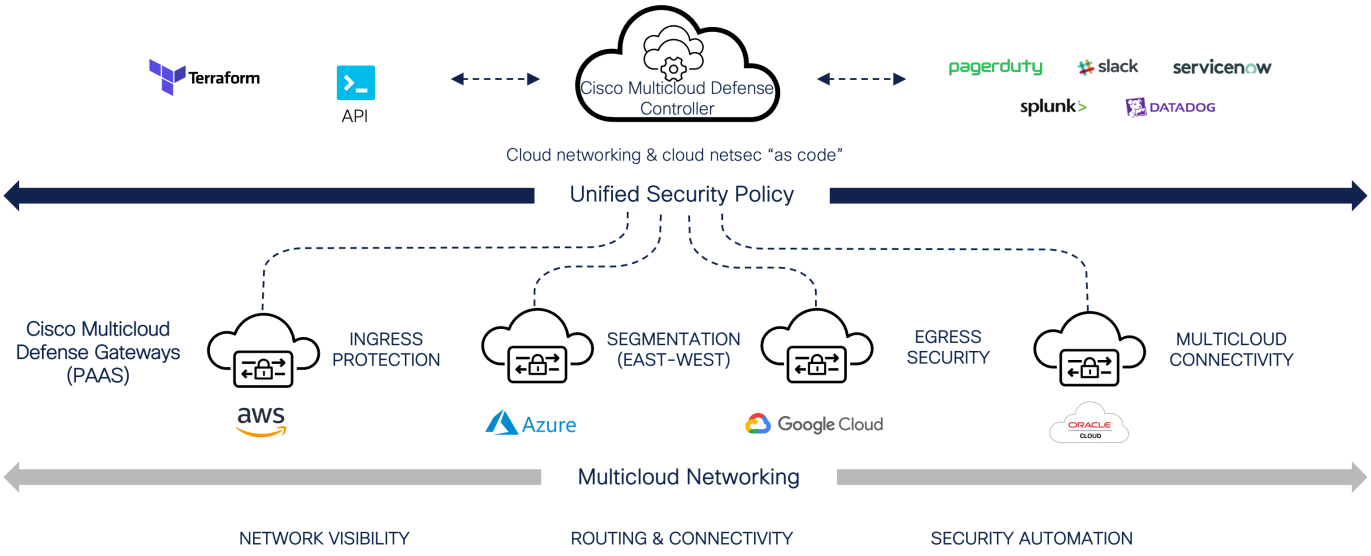


図 1.
Cisco Multicloud Defense

AWS

AWS 集中型イングレス

集中型イングレス環境では、サービス VPC が集中型のセキュリティハブとして使用されます。AWS Transit Gateway（TGW）を使用し、すべてのスポーク VPC を接続してトラフィックをルーティングします。Multicloud Defense は、サービス VPC の展開をオーケストレーションし、サービス VPC を既存または新規の TGW （Multicloud Defense によりオーケストレーション）に接続します。サービス VPC は、すべての入力トラフィックの接続先として AWS ネットワーク ロード バランサ（NLB）を使用します。NLB は、保護に対応し、展開された 1 つ以上の Multicloud Defense Gateway インスタンス全体でトラフィックを負荷分散します。Multicloud Defense Gateway は、リバースプロキシとして機能し、アプリケーションとワークロード宛てのノースバウンドトラフィックを検査して保護します。

展開アーキテクチャ - AWS 集中型イングレス

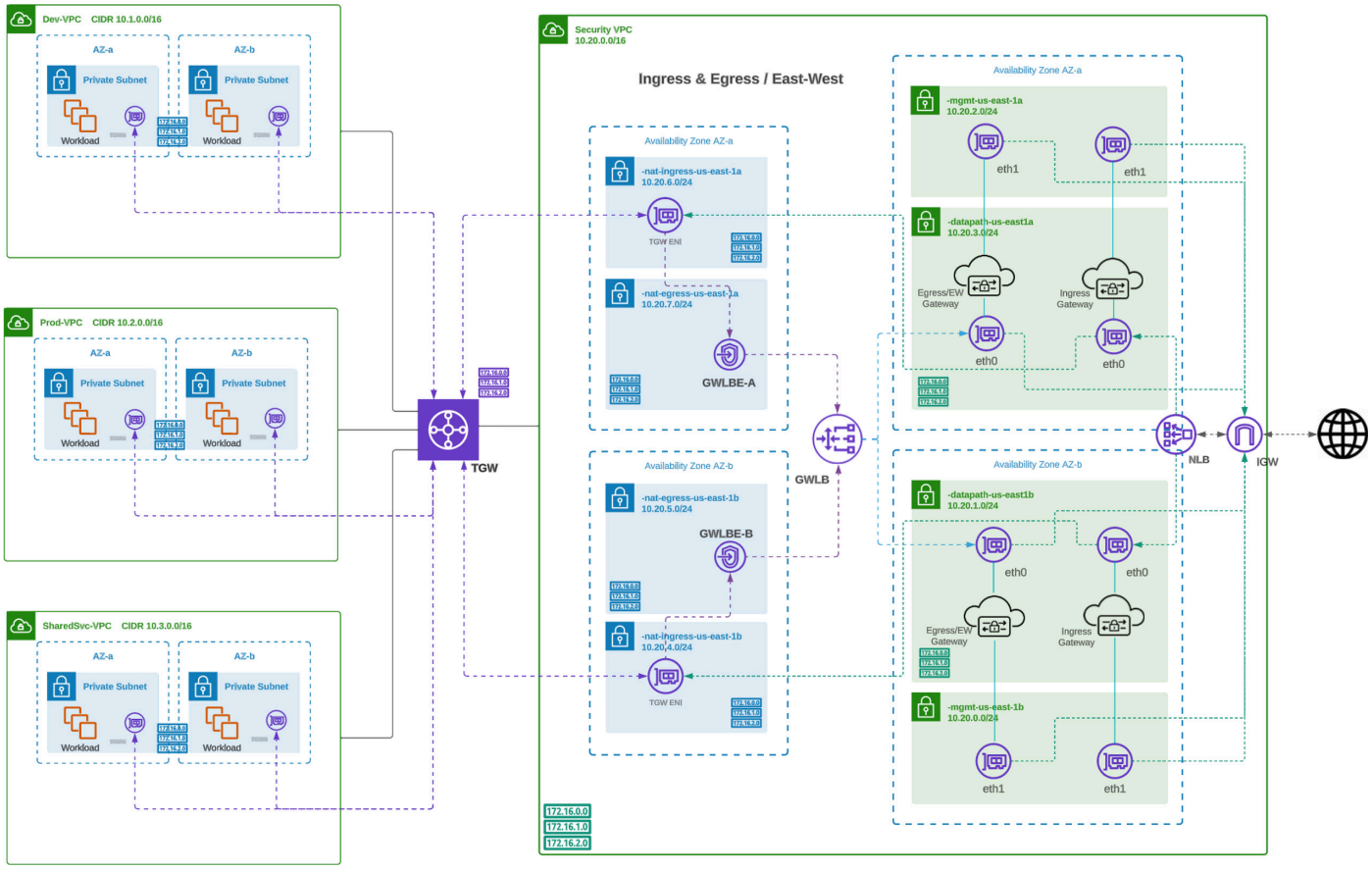


図 2.
集中型イングレスの展開アーキテクチャ（AWS）

トラフィックフロー - AWS 集中型イングレス

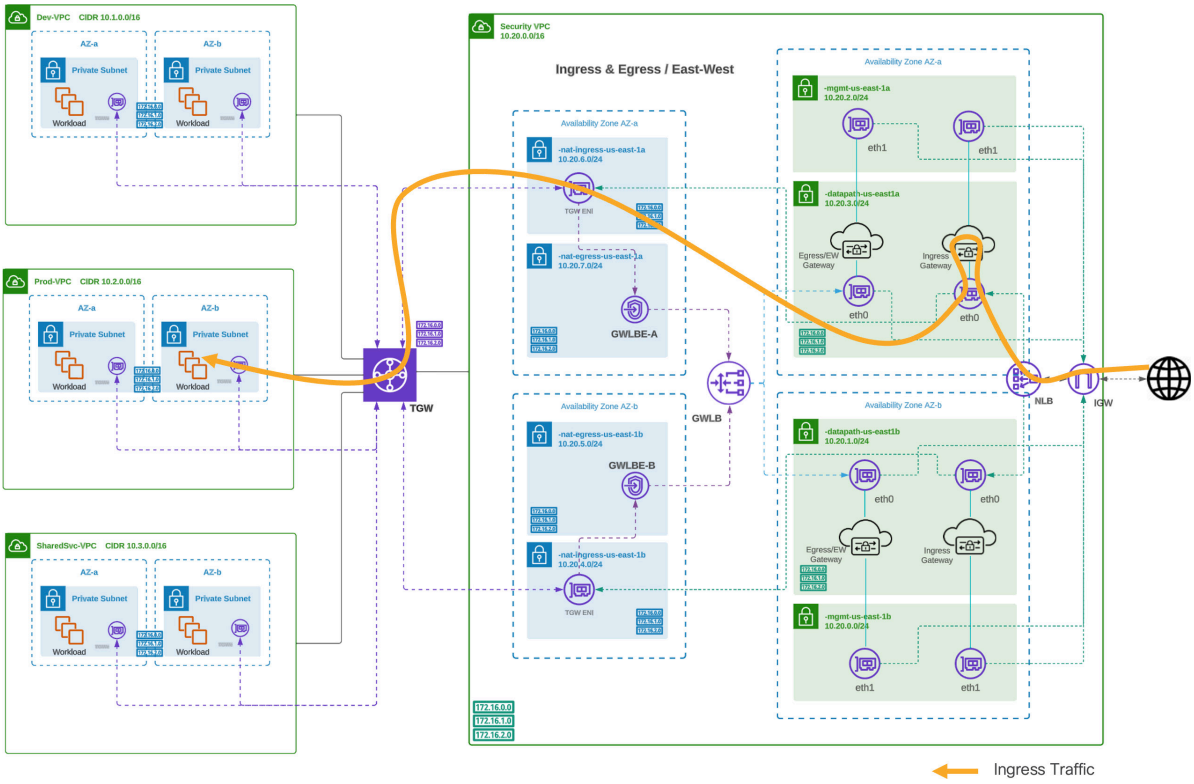


図 3.
集中型イングレスのトラフィックフロー（AWS）

ルーティング設定 - AWS 集中型イングレス

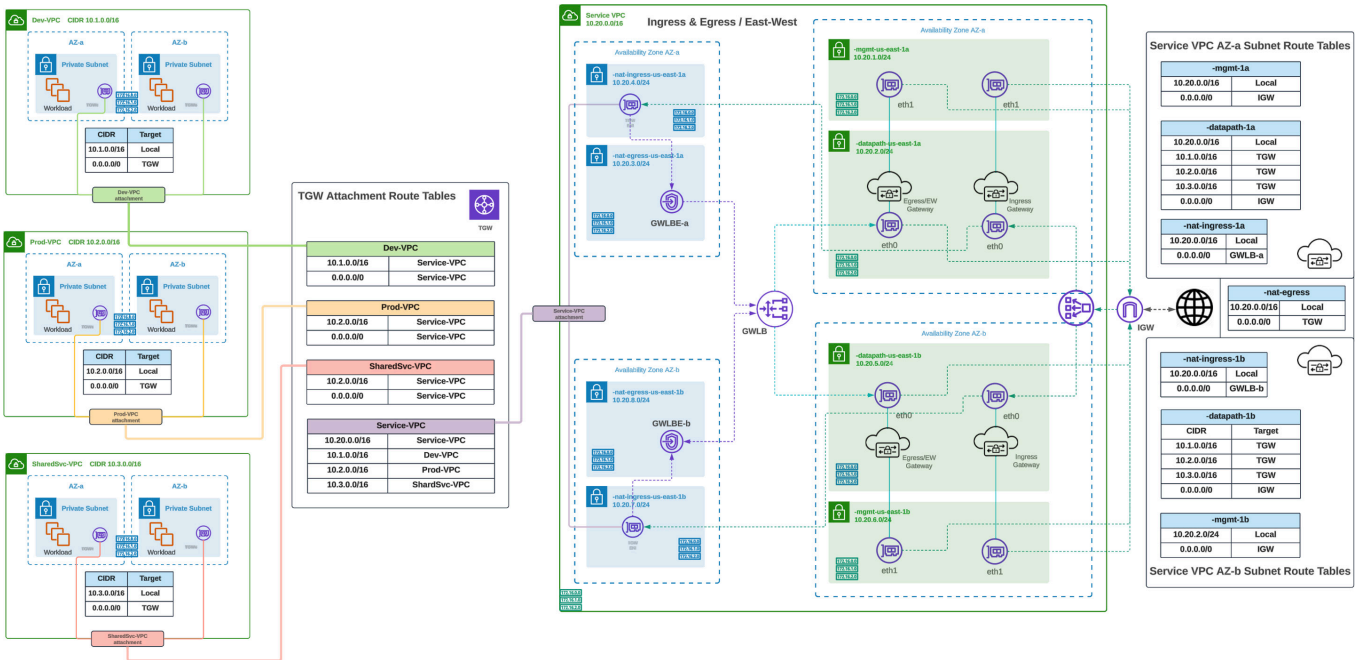


図 4.
集中型イングレスのルーティング設定（AWS）

注：この図は、イングレスゲートウェイとエグレス/横方向ゲートウェイの両方を示しています。イングレスおよびエグレス/横方向ゲートウェイは、同じ VPC に展開できます。保護の対象がイングレスのみであれば、エグレス/横方向ゲートウェイは必要ありません。

AWS 集中型エグレス

集中型エグレス環境では、サービス VPC が集中型のセキュリティハブとして使用されます。AWS Transit Gateway（TGW）を使用し、すべてのスポーク VPC を接続してトラフィックをルーティングします。Multicloud Defense は、サービス VPC の展開をオーケストレーションし、サービス VPC を既存または新規の TGW （Multicloud Defense によりオーケストレーション）に接続します。サービス VPC は AWS ゲートウェイ ロード バランサ（GWLB）を使用します。GWLB は、保護に対応し、展開された 1 つ以上の Multicloud Defense Gateway インスタンス全体でトラフィックを負荷分散します。Multicloud Defense Gateway は、転送または転送プロキシで動作し、サウスバウンドおよび横方向トラフィックを検査して保護します。

展開アーキテクチャ - AWS 集中型エグレス

集中型エグレスの展開アーキテクチャ（AWS）の図については、図 2 を参照してください。

トラフィックフロー - AWS 集中型エグレス

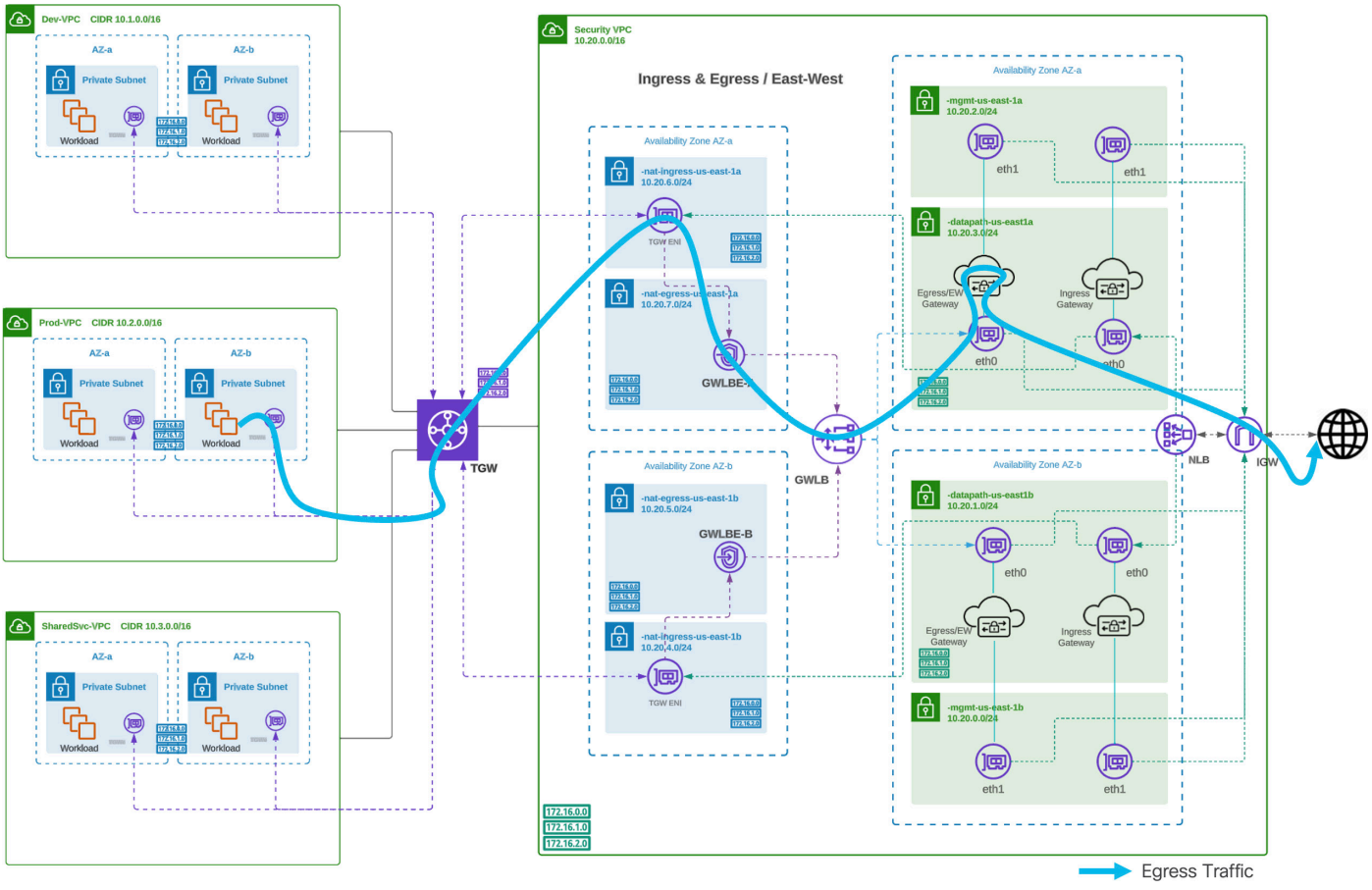


図 5.
集中型エグレスのトラフィックフロー - エグレス（AWS）

ルーティング設定 - AWS 集中型エグレス

集中型エグレスのルーティング設定（AWS）の図については、図 4 を参照してください。

注：この図は、イングレスゲートウェイとエグレス/横方向ゲートウェイの両方を示しています。イングレスおよびエグレス/横方向ゲートウェイは、同じ VPC に展開できます。保護の対象がエグレス/横方向のみであれば、イングレスゲートウェイは必要ありません。

AWS 集中型横方向

集中型横方向環境では、サービス VPC が集中型のセキュリティハブとして使用されます。AWS Transit Gateway（TGW）を使用し、すべてのスポーク VPC を接続してトラフィックをルーティングします。Multicloud Defense は、サービス VPC の展開をオーケストレーションし、サービス VPC を既存または新規の TGW （Multicloud Defense によりオーケストレーション）に接続します。サービス VPC は AWS ゲートウェイ ロード バランサ（GWLB）を使用します。GWLB は、保護に対応し、展開された 1 つ以上の Multicloud Defense Gateway インスタンス全体でトラフィックを負荷分散します。Multicloud Defense Gateway は、転送または転送プロキシで動作し、サウスバウンドおよび横方向トラフィックを検査して保護します。

展開アーキテクチャ - AWS 集中型横方向

集中型横方向の展開アーキテクチャ（AWS）の図については、図 2 を参照してください。

トラフィックフロー - AWS 集中型横方向、VPC 間

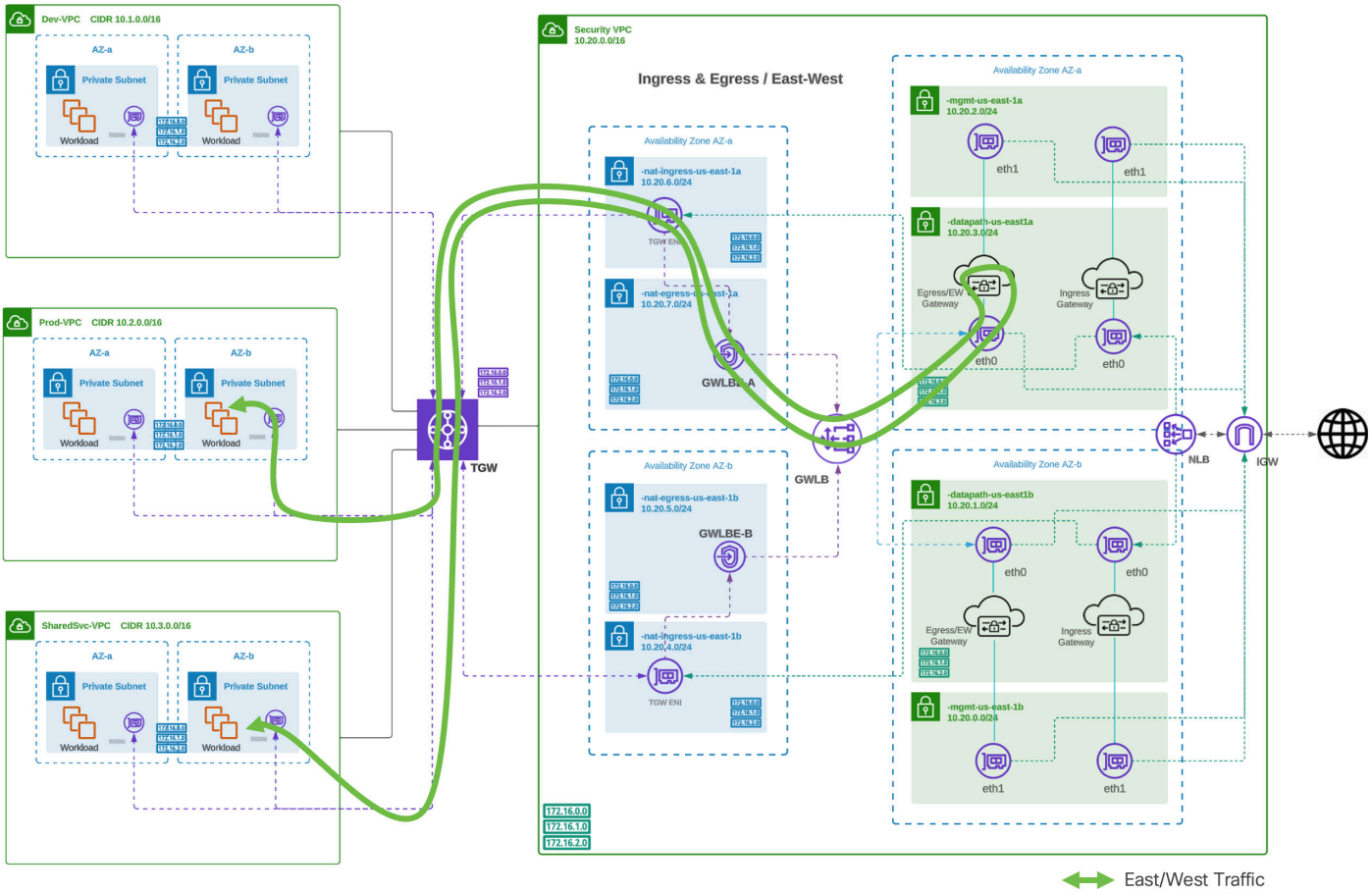


図 6.
トラフィックフロー - 集中型横方向、VPC 間（AWS）

トラフィックフロー - AWS 集中型横方向、VPC 内

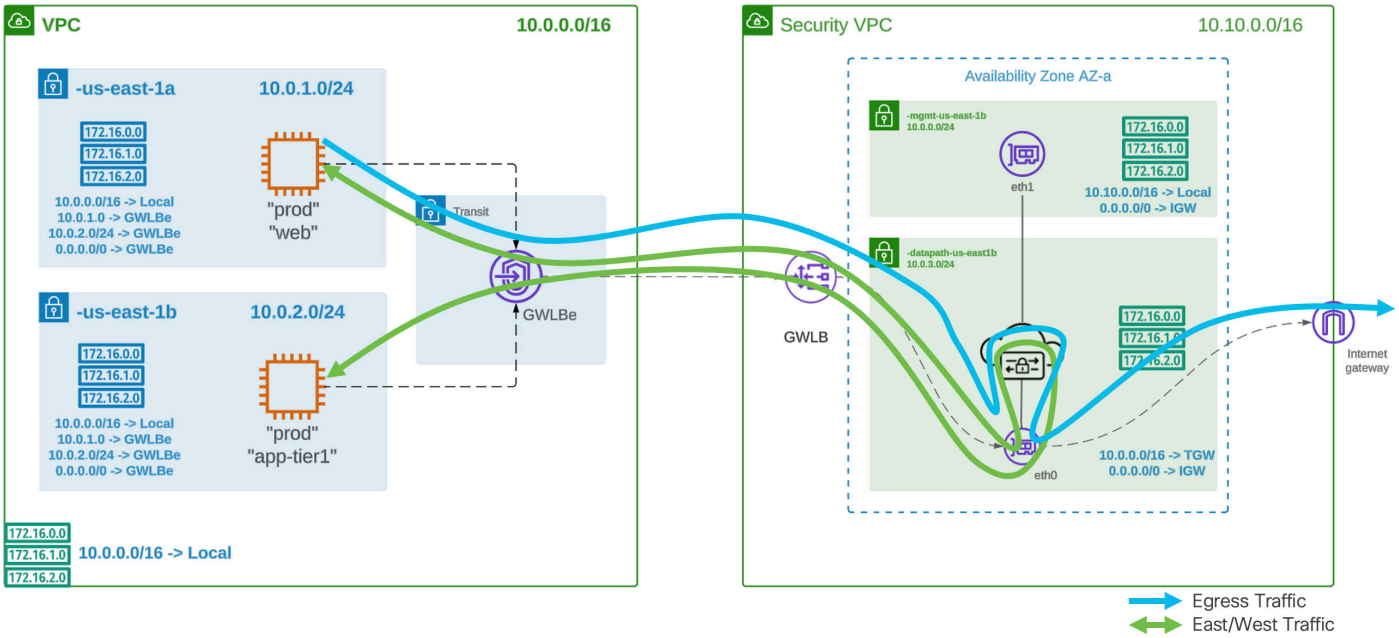


図 7.
トラフィックフロー - 集中型横方向、VPC 内（AWS）

ルーティング設定 - AWS 集中型横方向

集中型横方向のルーティング設定（AWS）の図については、図 4 を参照してください。

注：この図は、イングレスゲートウェイとエグレス/横方向ゲートウェイの両方を示しています。イングレスおよびエグレス/横方向ゲートウェイは、同じ VPC に展開できます。保護の対象がエグレス/横方向のみであれば、イングレスゲートウェイは必要ありません。

More Specific Routing（MSR）を使用した AWS 集中型横方向

AWS の新機能 More Specific Routing（MSR）により、VPC 内のサブネット間の通信トラフィックを Multicloud Defense で検査できるようになりました。Multicloud Defense は、サービス VPC をセキュリティ ハブとして使用します。ゲートウェイ ロード バランサ（GWLB）のエンドポイントをスポーク VPC に配置して、サービス VPC にトラフィックをルーティングします。各サブネットのルートテーブルに MSR を設定し、トラフィックをエンドポイント経由でサービス VPC にルーティングして検査します。

展開アーキテクチャと MSR 設定

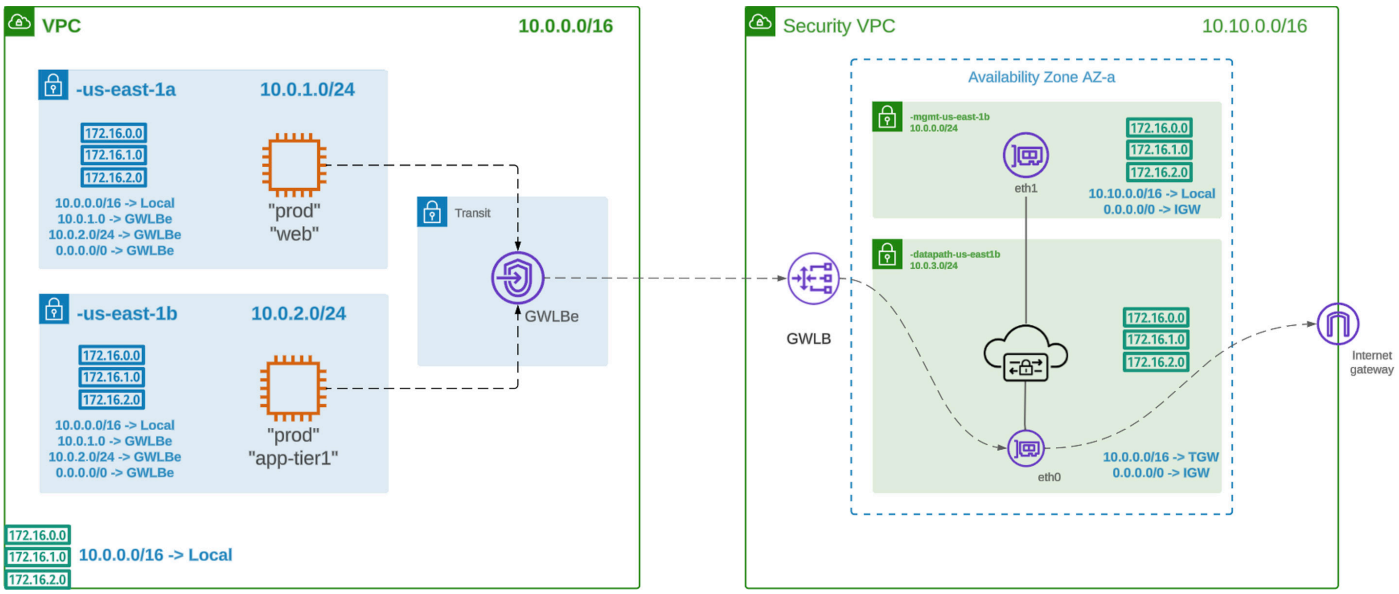


図 8.
AWS 集中型 MSR 設定

AWS 集中型エグレスおよび横方向（NAT ゲートウェイ）

Multicloud Defense を使用してエグレストラフィックを保護する場合、インターネットに送信されるトラフィックには、Multicloud Defense Gateway インスタンスの送信元 IP が使用されます。Gateway インスタンスをプライベートとして展開する必要があり、トラフィックをインターネットに送信するために使用する IP アドレスを静的（変更しない）にする必要がある場合には、NAT ゲートウェイを使用してサービス VPC を展開できます。NAT ゲートウェイオプションが有効になっている場合、Multicloud Defense Gateway はプライベートサブネットに展開されます。また NAT ゲートウェイをホストするパブリックサブネットも作成されます（AZ ごと）。インターネットへのすべてのトラフィックは、Gateway インスタンスから NAT ゲートウェイを経由して送信されます。その際、NAT ゲートウェイのパブリック IP アドレスを使用します。これにより、NAT ゲートウェイの IP アドレスをホワイトリストに登録できるようになります。クラウドリソースを SaaS として提供される ID プロバイダーに接続して認証を行うには、多くの場合、ホワイトリストの登録が必要となります。

展開アーキテクチャ - AWS 集中型エグレス/横方向

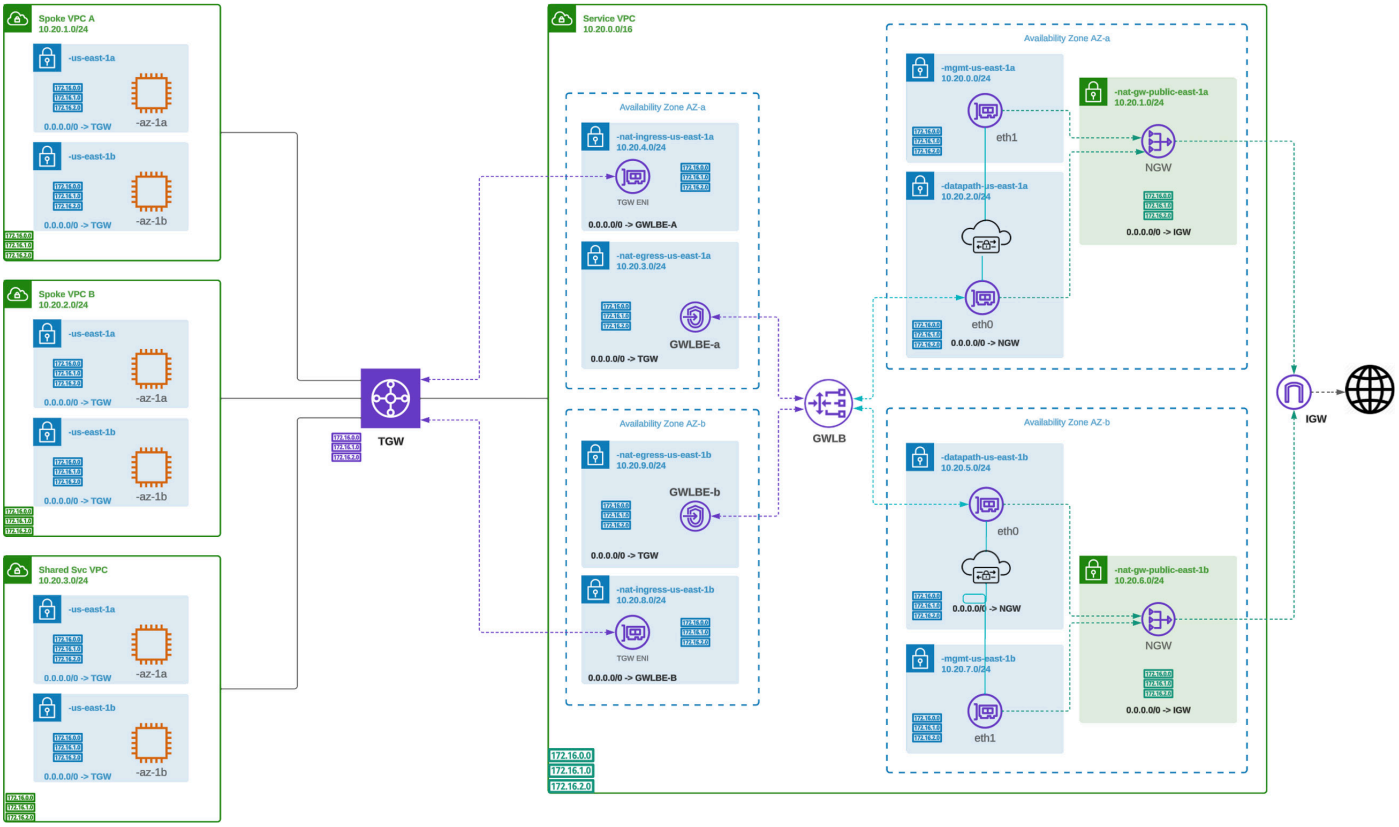


図 9.
AWS 集中型エグレス/横方向（NAT ゲートウェイ） - 展開アーキテクチャ

トラフィックフロー - AWS 集中型エグレス/横方向

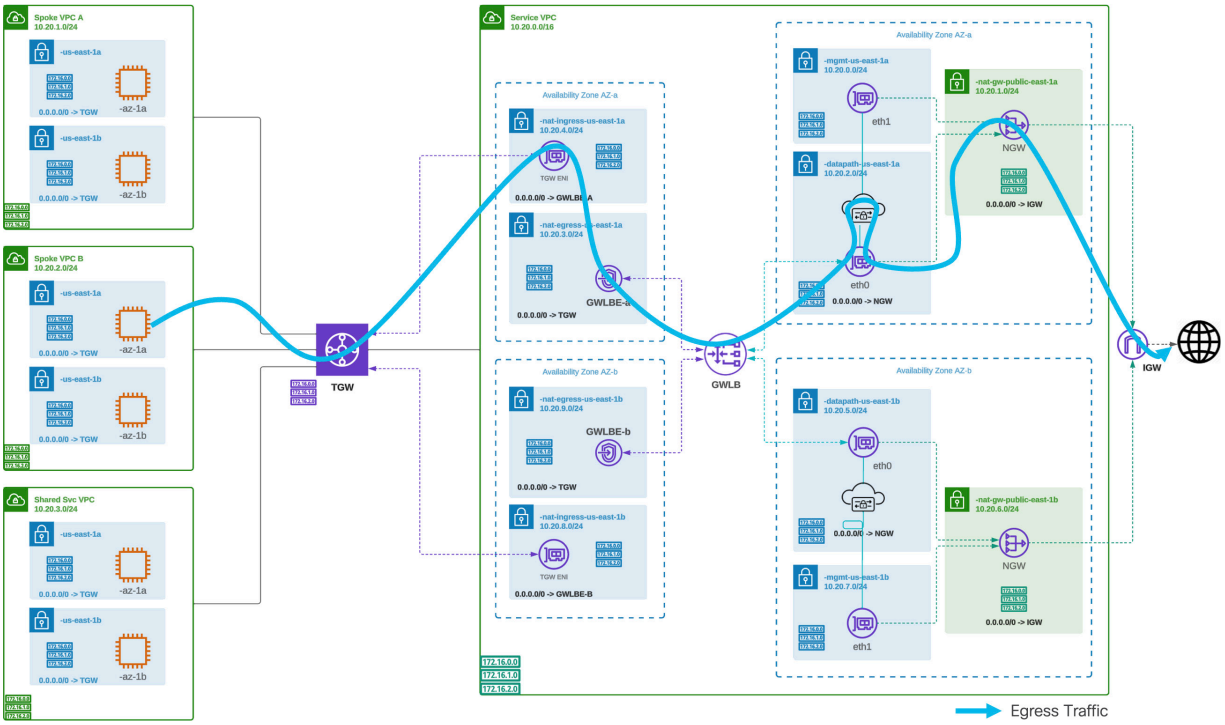


図 10.
AWS 集中型エグレス/横方向（NAT ゲートウェイ） - トラフィックフロー

ルーティング設定 - AWS 集中型エグレス/横方向

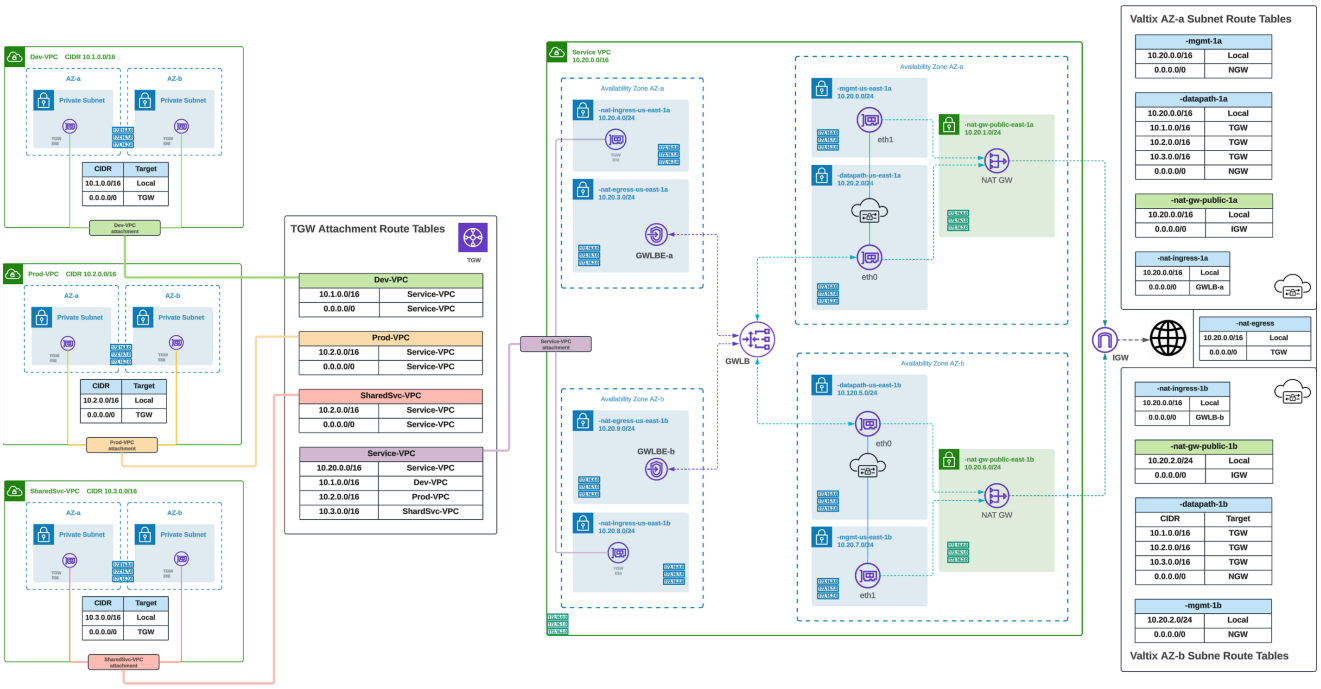


図 11.
AWS 集中型エグレス/横方向（NAT ゲートウェイ） ：ルーティング設定

AWS 集中型 GWLB ベースのイングレス/エグレス

集中型 GWLB ベースのイングレスおよびエグレス環境では、サービス VPC が集中型のセキュリティハブとして使用されます。ゲートウェイ ロード バランサ（GWLB）と GWLB エンドポイントを使用し、すべてのスポーク VPC を接続してトラフィックをルーティングします。Multicloud Defense は、サービス VPC、サービス VPC インフラストラクチャ、ゲートウェイ、GWLB の展開をオーケストレーションします。GWLB への接続に使用されるスポーク VPC の GWLB エンドポイントは、ユーザーがオーケストレーションする必要があります（AWS コンソールまたは Terraform）。GWLB エンドポイントを使用して、Multicloud Defense にトラフィックを渡します。GWLB は、1 つ以上の Multicloud Defense Gateway インスタンス全体でトラフィックを負荷分散します。Multicloud Defense Gateway は、トラフィックを転送するか転送プロキシを経由させ、アプリケーション、ワークロード、インターネット宛てのノースバウンドおよびサウスバウンドのトラフィックを検査して保護します。

ルーティング設定 - AWS 集中型 GWLB ベースのイングレス/エグレス

AWS 集中型 GWLB ベースのイングレス/エグレスのルーティング設定を示す図については、図 11 を参照してください。

Azure

Azure 集中型イングレス

集中型イングレスモデルでは、Multicloud Defense がサービス VNet をオーケストレーションし、スポーク VNet とサービス VNet の間に VNet ピアリングを作成します。Multicloud Defense は、スポーク VNet にユーザー定義ルート（UDR）を作成し、トラフィックをサービス VNet にルーティングします。サービス VNet 内のすべての必要なコンポーネント（Multicloud Defense Gateway、ネットワーク セキュリティ グループ、NLB）は、Multicloud Defense によって作成および管理されます。NLB は、インターネットトラフィックを受信して Multicloud Defense Gateways に負荷分散されるパブリックエンドポイントになります。Multicloud Defense Gateway は、リバースプロキシとして機能し、ワークロードを保護します。

展開アーキテクチャ - Azure 集中型イングレス

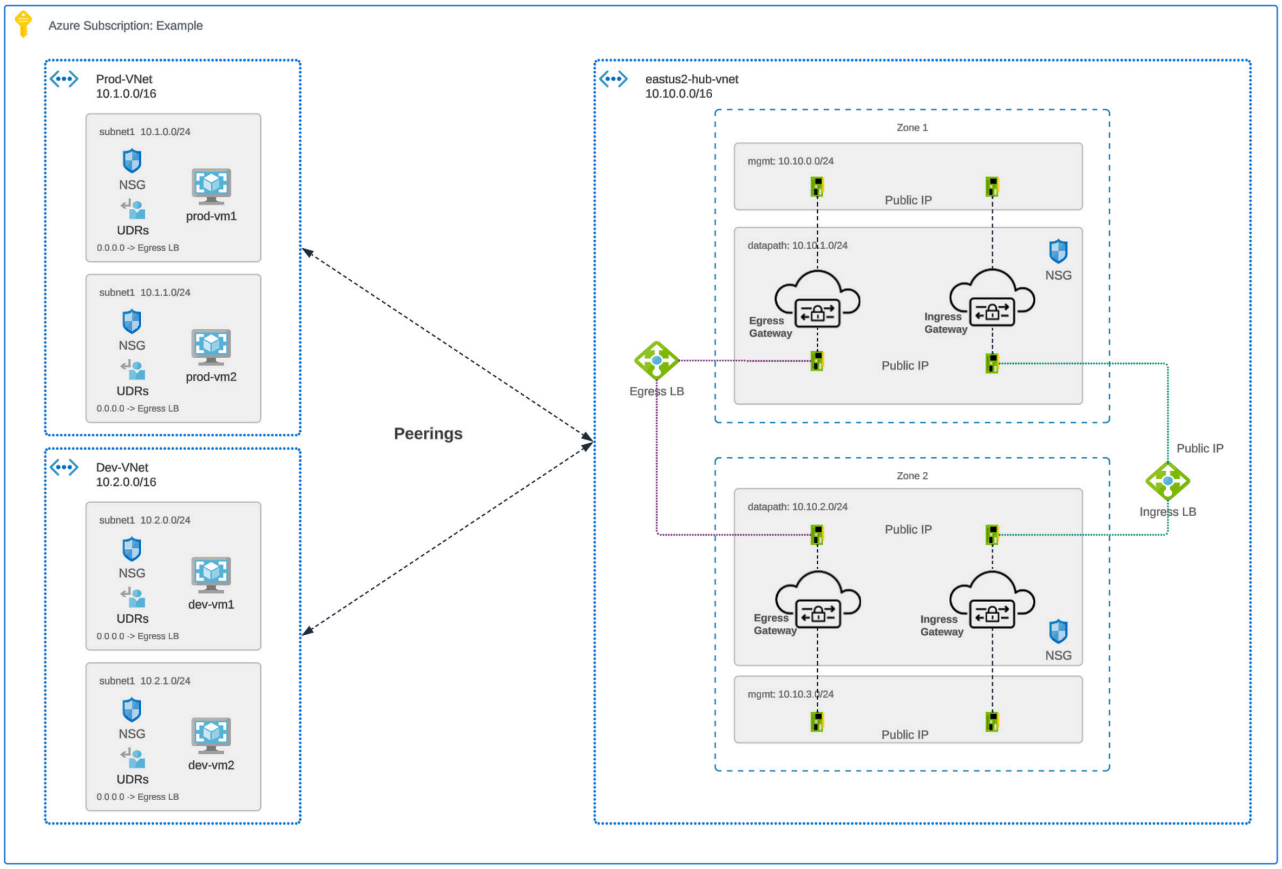


図 12.
Azure 集中型イングレス - 展開アーキテクチャ

注：この図は、イングレスゲートウェイと、エグレスおよび横方向ゲートウェイの両方を示しています。ユーザーは同じ VPC に、イングレスゲートウェイと、エグレスおよび横方向ゲートウェイを展開することもできます。保護の対象がイングレスのみであれば、エグレスゲートウェイの展開は必要はありません。

トラフィックフロー - Azure 集中型イングレス

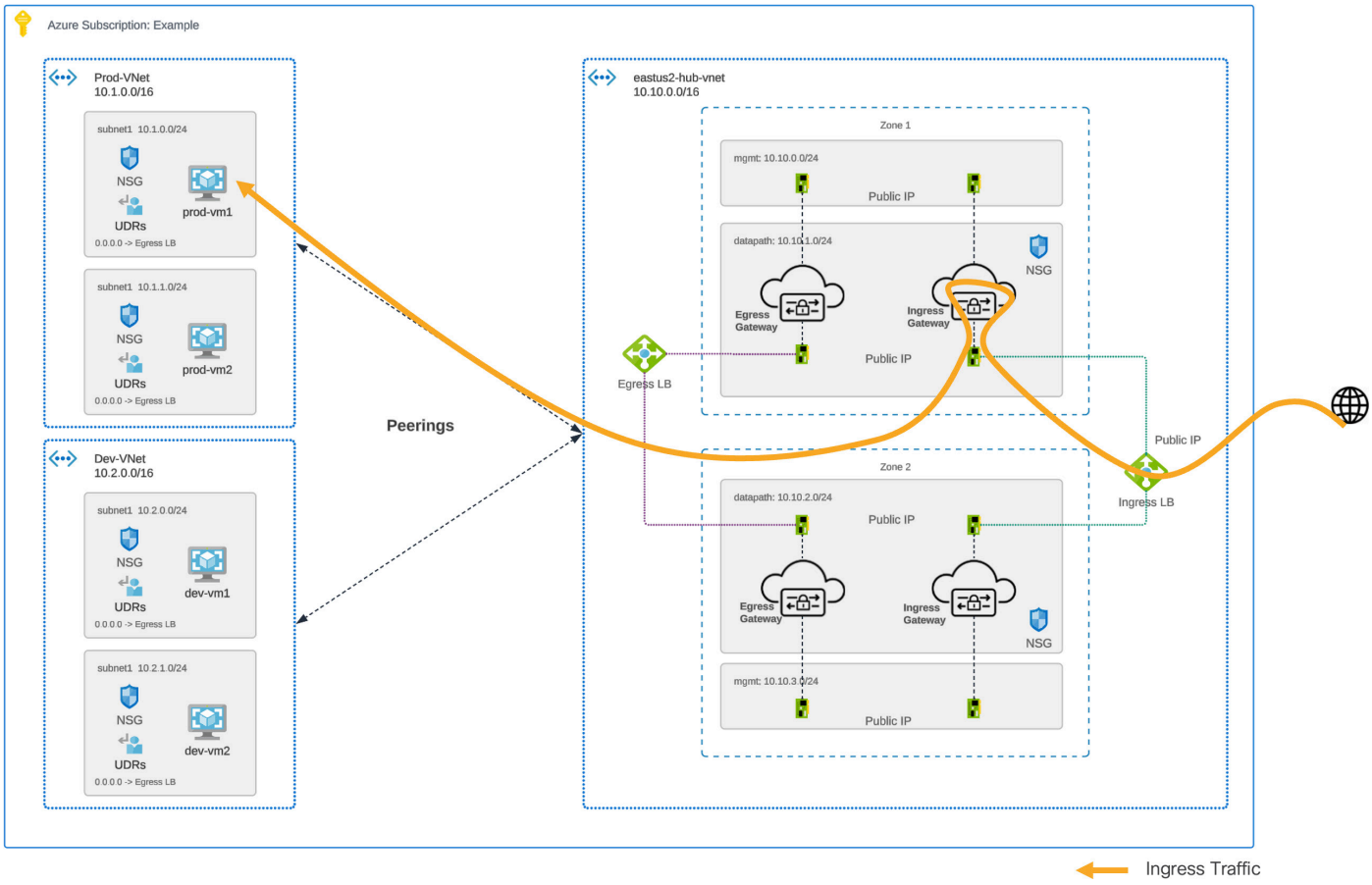
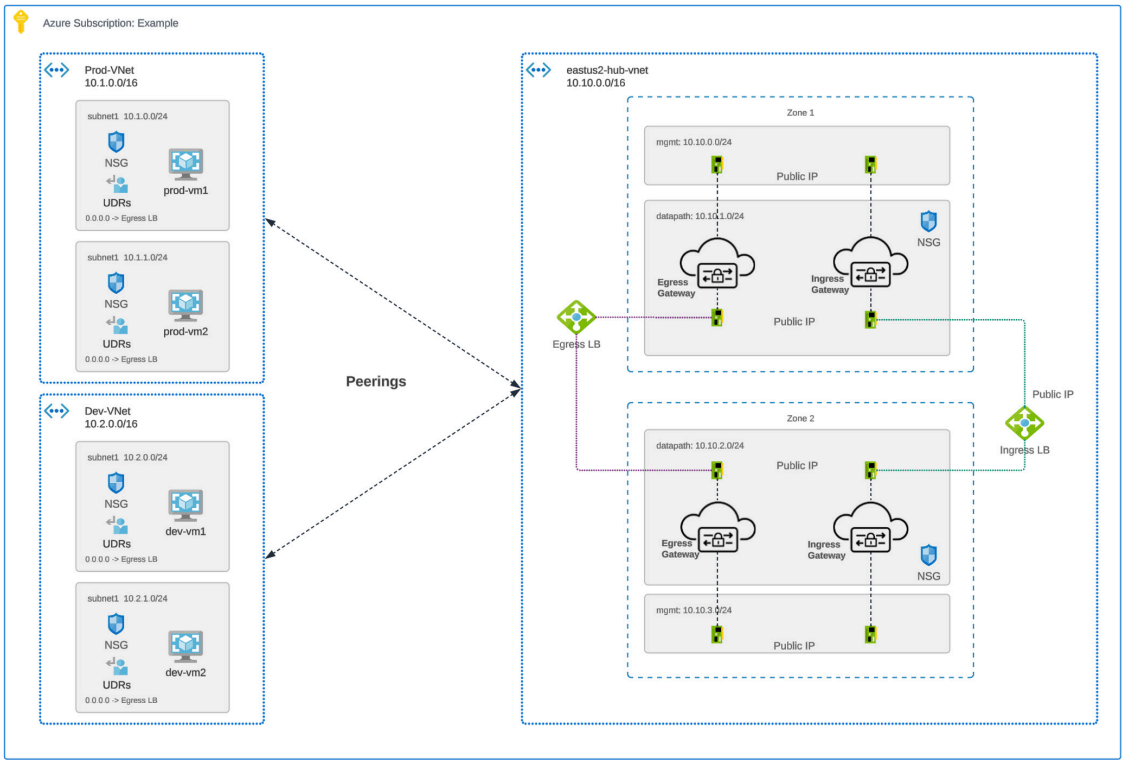


図 13.
Azure 集中型イングレス - トラフィックフロー

ルーティング設定 - Azure 集中型イングレス



Prod-VNet-UDR	
0.0.0.0/0	Egress LB

Dev-VNet-UDR	
0.0.0.0/0	Egress LB

mgmt-UDR	
0.0.0.0/0	Internet

datapath-UDR	
0.0.0.0/0	Internet
10.1.0.0/16	Peering 1 (dynamic route)
10.2.0.0/16	Peering 2 (dynamic route)

図 14.
Azure 集中型イングレス - ルーティング設定

Azure 集中型エグレス

Multicloud Defense は、サービス VNet が適用のハブとして機能する集中型モデルで、サービス VNet をオーケストレーションします。スポーク VNet とサービス VNet の間には VNet ピアリングが作成されます。Multicloud Defense は、スポーク VNet でユーザー定義ルート（UDR）を作成/更新し、トラフィックをサービス VNet にルーティングします。サービス VNet 内には、ネットワークロードバランサ（NLB）と Multicloud Defense Gateway があります。スポーク VNet からのトラフィックは NLB にルーティングされ、複数の可用性ゾーンにある Multicloud Defense Gateway で負荷分散されます。

展開アーキテクチャ - Azure 集中型エグレス

Azure 集中型エグレスの展開アーキテクチャの図については、図 12 を参照してください。

注：この図は、イングレスゲートウェイと、エグレスおよび横方向ゲートウェイの両方を示しています。ユーザーは同じ VPC に、イングレスゲートウェイと、エグレスおよび横方向ゲートウェイを展開することもできます。保護の対象がエグレス/横方向のみであれば、イングレスゲートウェイの展開は必要はありません。

トラフィックフロー - Azure 集中型エグレス

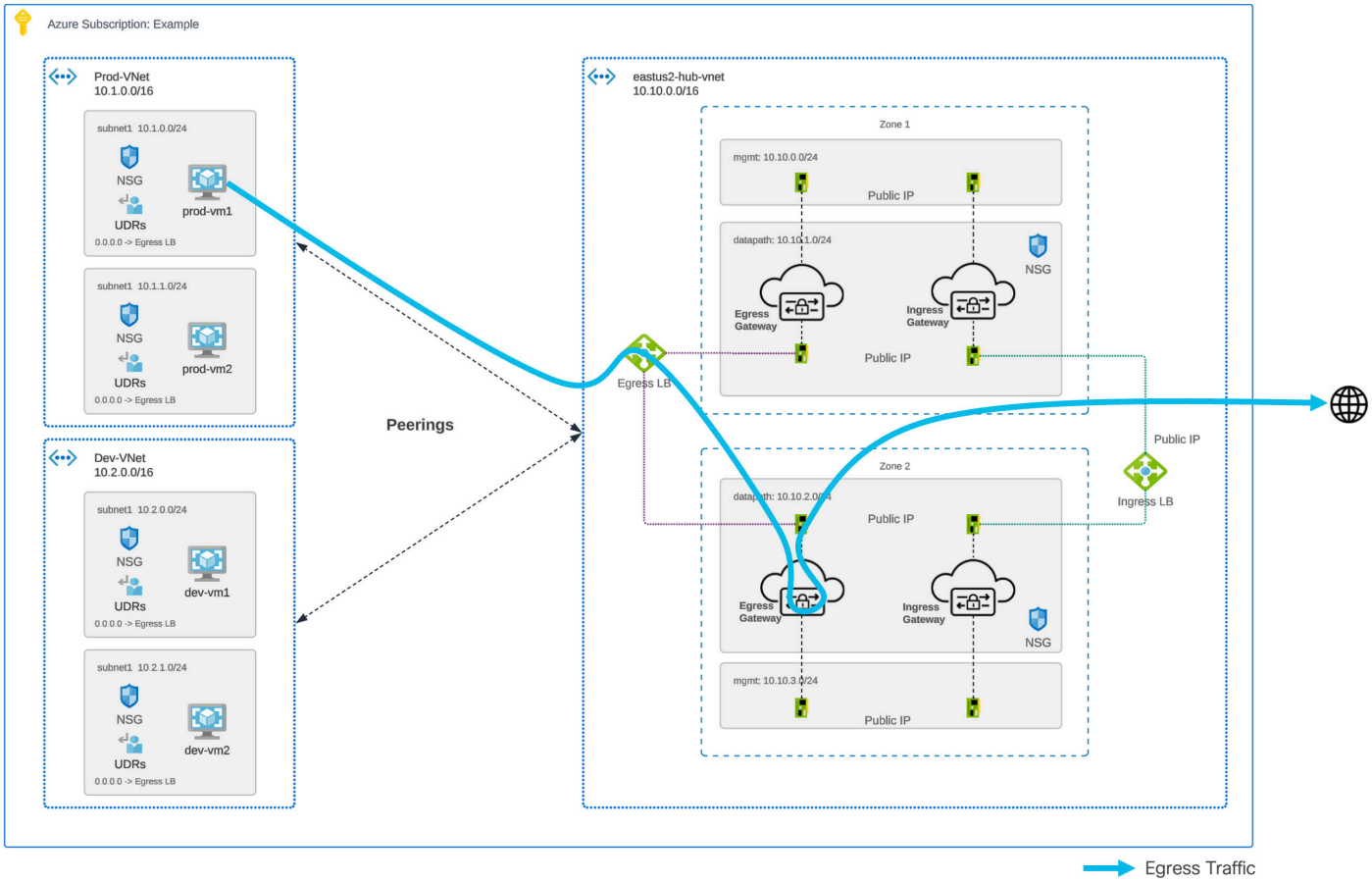


図 15.
Azure 集中型エグレス - トラフィックフロー

ルーティング設定 - Azure 集中型エグレス

Azure 集中型エグレスのルーティング設定の図については、図 14 を参照してください。

Azure 集中型横方向

展開アーキテクチャ - Azure 集中型横方向

Azure 集中型横方向の展開アーキテクチャの図については、図 12 を参照してください。

トラフィックフロー - Azure 集中型横方向

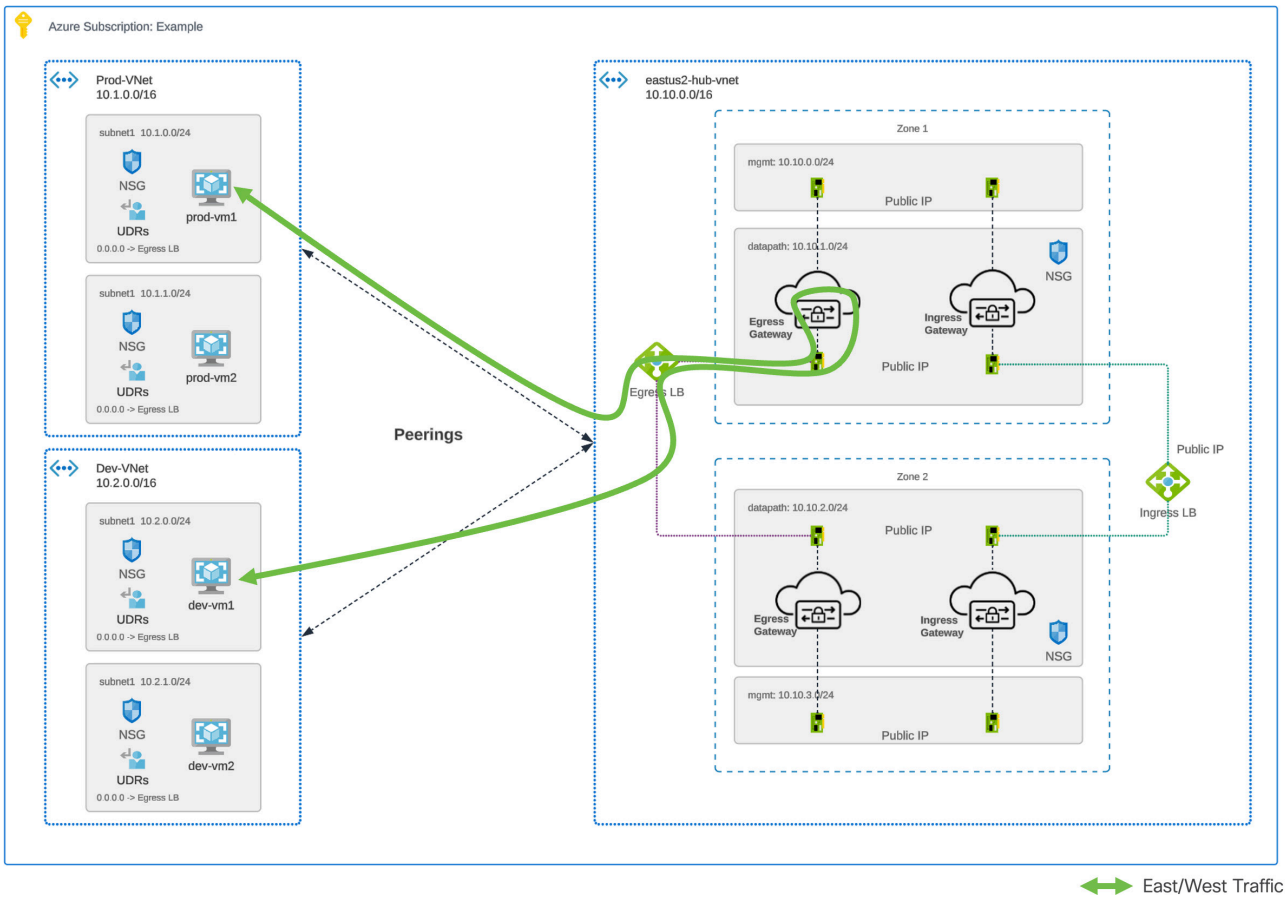


図 16.
Azure 集中型横方向 - トラフィックフロー

ルーティング設定 - Azure 集中型横方向

Azure 集中型横方向のルーティング設定の図については、図 14 を参照してください。

GCP

GCP で Multicloud Defense による集中型セキュリティを実現するには、すべてのセキュリティコンポーネントに VPC（セキュリティ VPC またはサービス VPC）を展開し、セキュリティ VPC とすべてのスポーク VPC 間で VPC ピアリングを実行します。Multicloud Defense は、サービス VPC（および必要なすべてのコンポーネント）をオーケストレーションして、すべての種類のトラフィック（イングレス、エグレス、横方向）を保護します。サービス VPC 内には 2 つのゲートウェイがあります。1 つはイングレス用、もう 1 つはエグレス/横方向用です。Multicloud Defense では、ボタンをクリックするだけで、サービス VPC とすべてのスポーク VPC 間の VPC ピアリングをオーケストレーションすることもできます。

GCP 集中型イングレス

展開アーキテクチャ - GCP 集中型イングレス

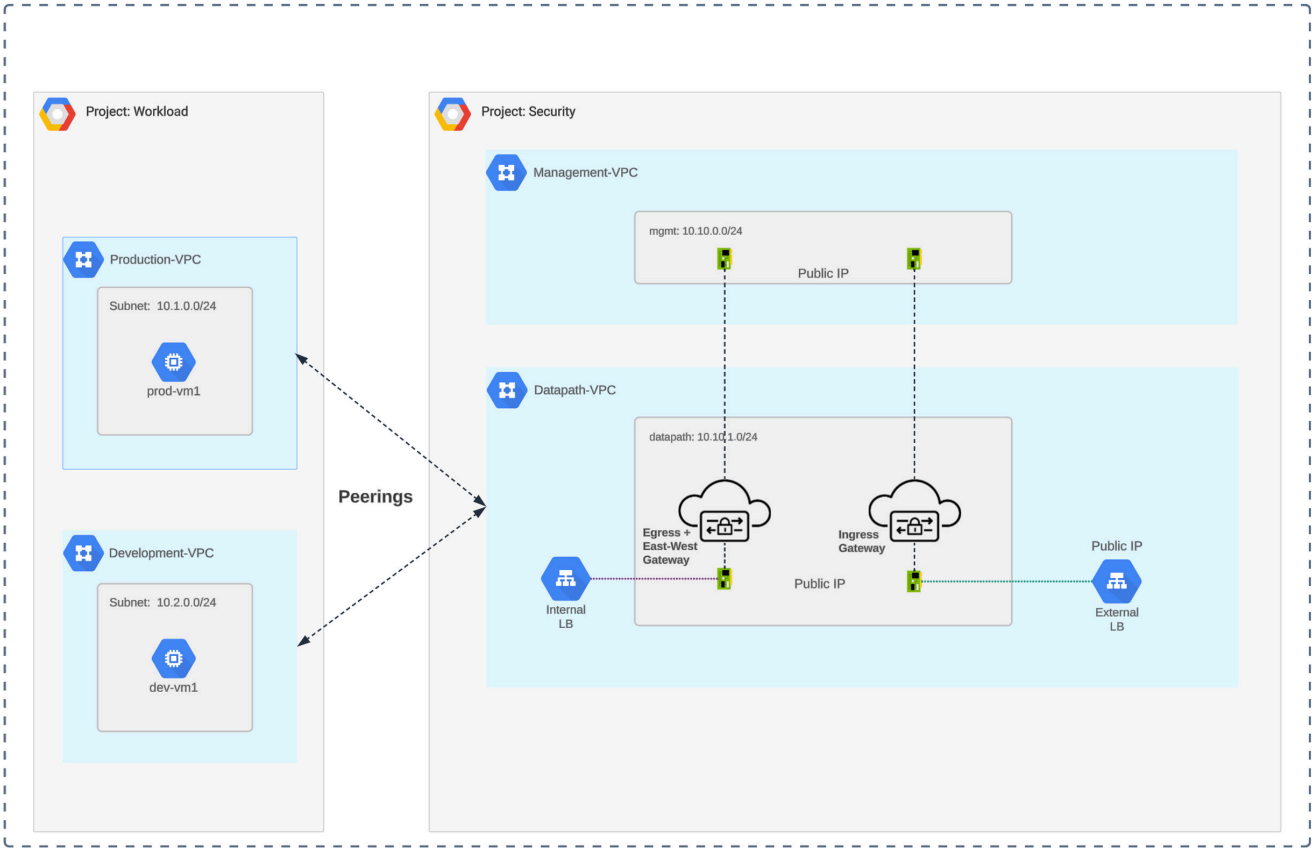


図 17.
GCP 集中型イングレス - 展開アーキテクチャ

トラフィックフロー - GCP 集中型イングレス

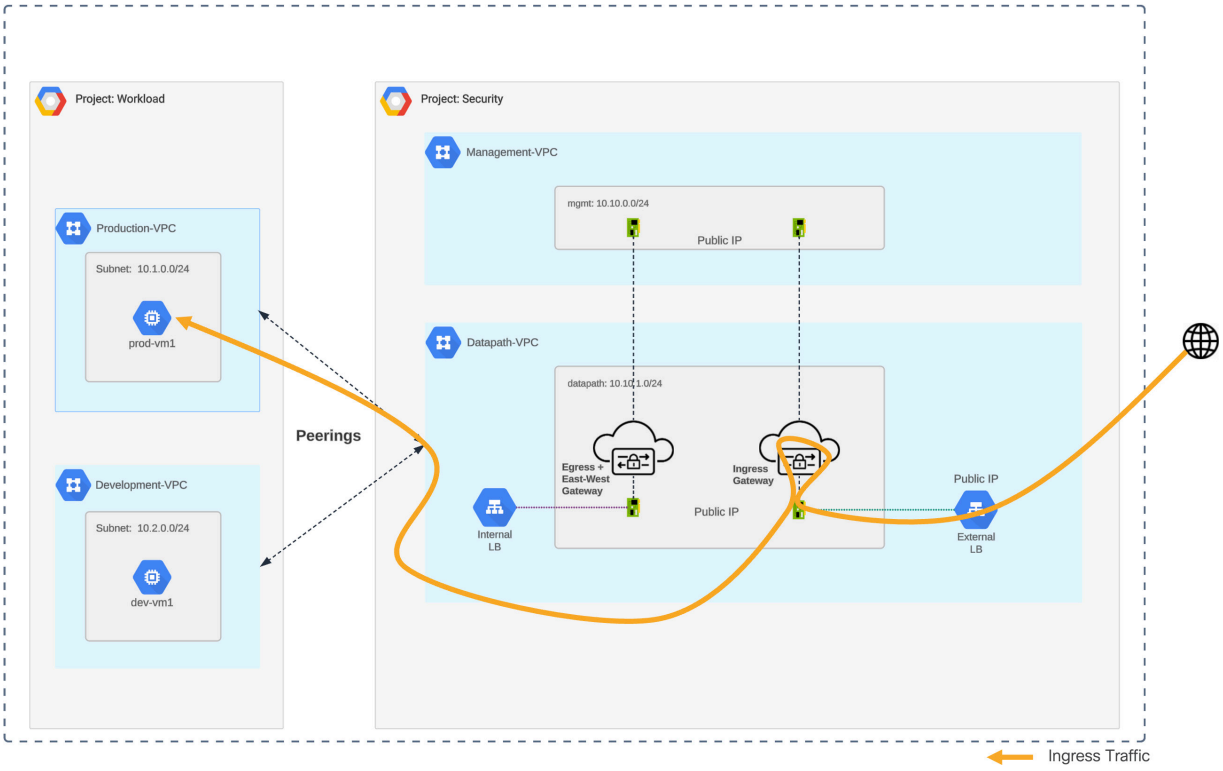
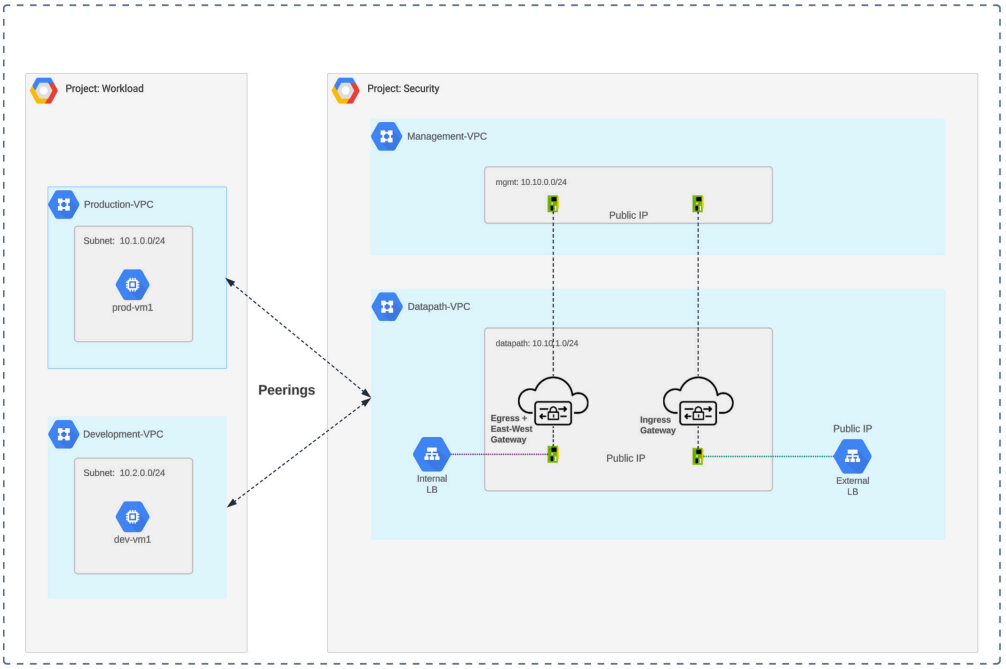


図 18.
GCP 集中型イングレス - トラフィックフロー

ルーティング設定 - GCP 集中型イングレス



Production-VPC route	
0.0.0.0/0	Peering ILB (imported route)

Development-VPC route	
0.0.0.0/0	Peering (imported route)

Management-VPC route	
0.0.0.0/0	Default Internet

Datapath-VPC route	
0.0.0.0/0	Default Internet (only for Multicloud defense datapath)
0.0.0.0/0	Internal LB (exported to all spoke VPCs)
10.1.0.0/24	Peering 1 (peering route)
10.2.0.0/24	Peering 2 (peering route)

図 19.
GCP 集中型イングレス：ルーティング設定

GCP 集中型エグレス

展開アーキテクチャ - GCP 集中型エグレス

GCP 集中型エグレスの展開アーキテクチャの図については、図 17 を参照してください。

トラフィックフロー - GCP 集中型エグレス

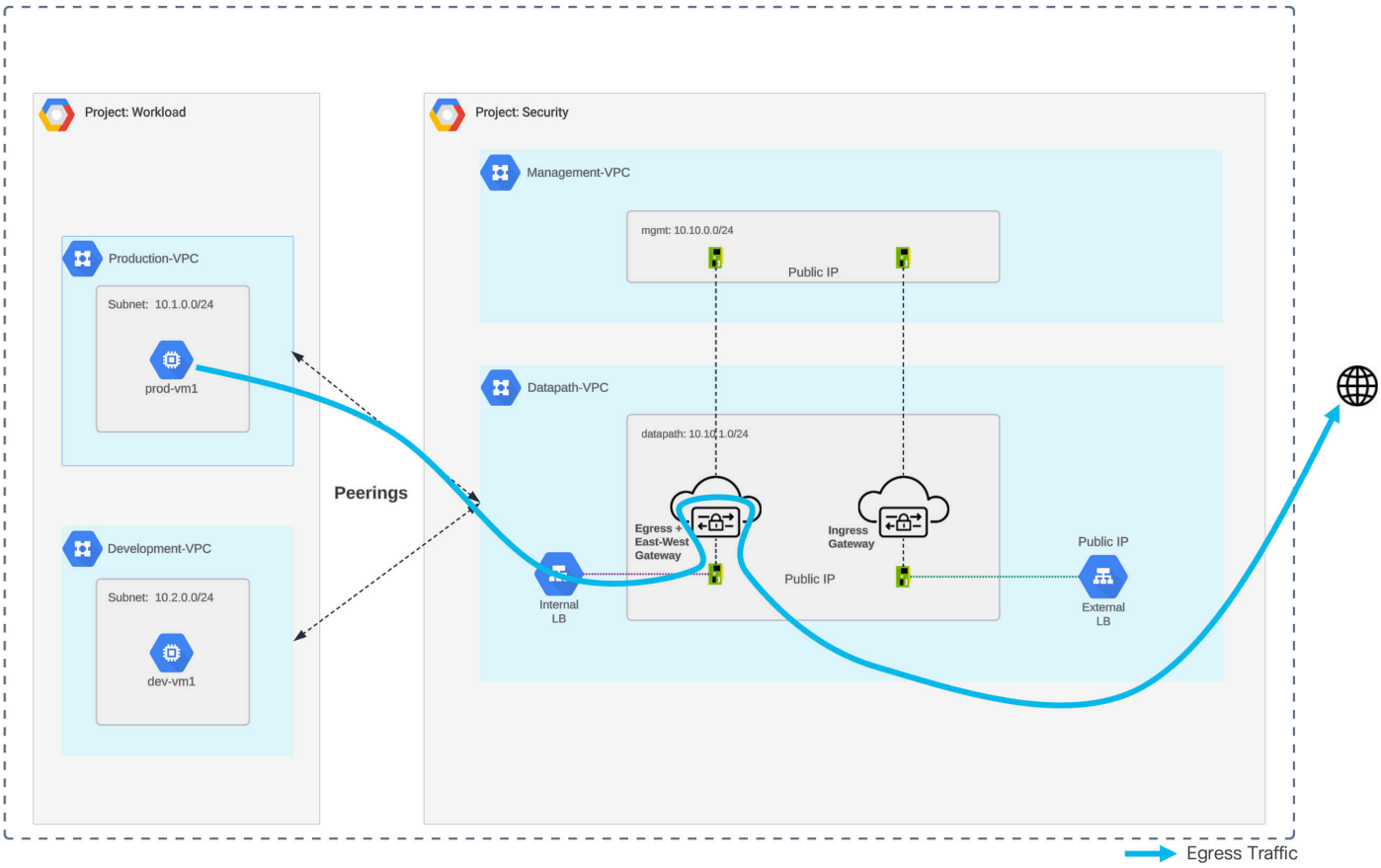


図 20.
GCP 集中型エグレス - トラフィックフロー

ルーティング設定 - GCP 集中型エグレス

GCP 集中型エグレスのルーティング設定の図については、図 19 を参照してください。

GCP 集中型横方向

展開アーキテクチャ - GCP 集中型横方向

GCP 集中型横方向の展開アーキテクチャの図については、図 17 を参照してください。

トラフィックフロー - GCP 集中型横方向

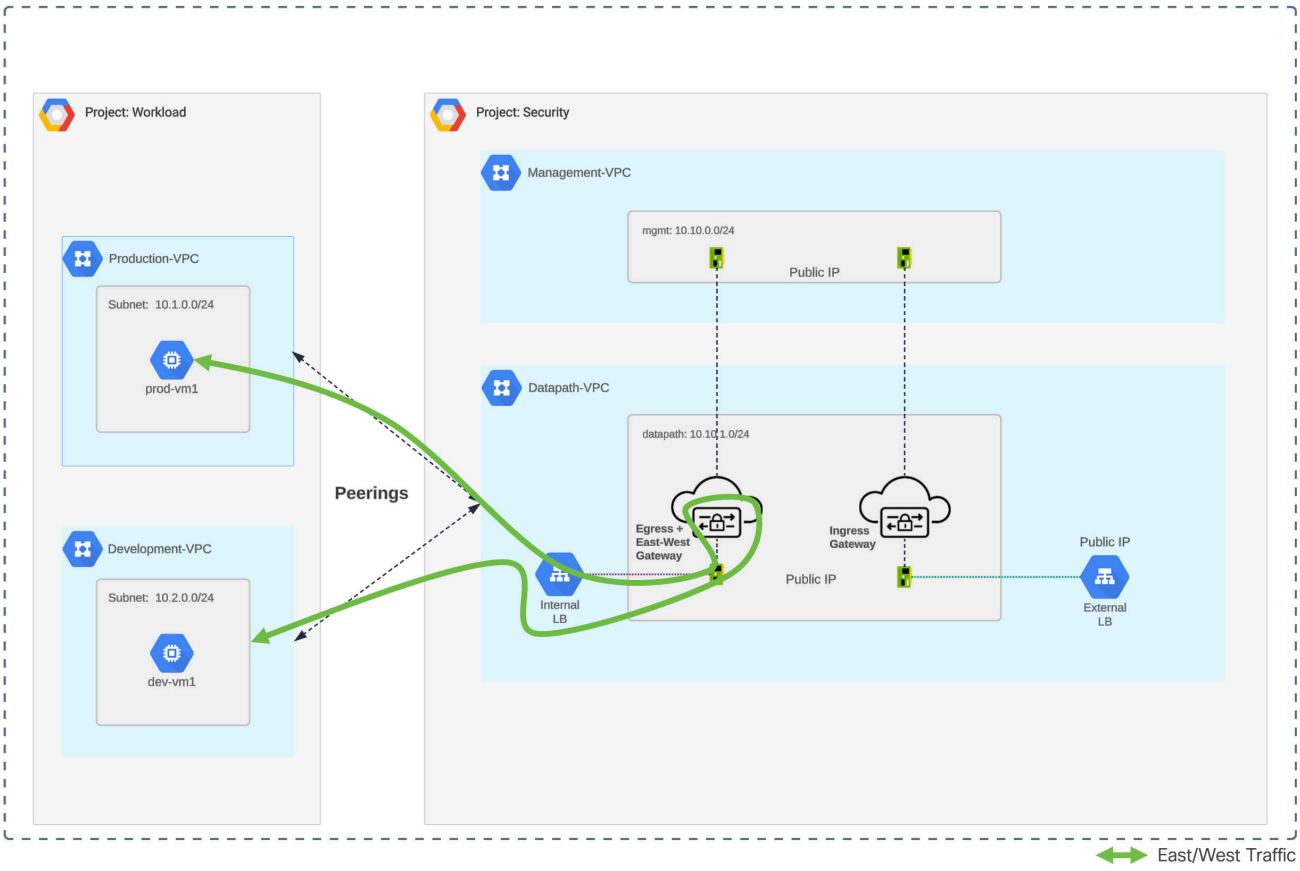


図 21.
GCP 集中型横方向 - トラフィックフロー

ルーティング設定 - GCP 集中型横方向

GCP 集中型横方向のルーティング設定の図については、図 19 を参照してください。

付録

付録 A：フィードバック

何かご質問やフィードバックがございましたら Cisco 営業担当もしくは販売店にお問い合わせください。

Cisco Multicloud Defense の詳細については、www.cisco.com/jp/go/multicloud-defense をご覧ください。

米国本社
カリフォルニア州サンノゼ

アジア太平洋本社
シンガポール

ヨーロッパ本社
アムステルダム（オランダ）

シスコは世界各国に約 400 のオフィスを開設しています。オフィスの住所、電話番号、FAX 番号は当社の Web サイト（www.cisco.com/jp/go/offices）をご覧ください。

Printed in USA 03/24