AWS Black Belt Online Seminar

AWS Transit Gateway
deep dive

Toshikazu Sakurai
Senior Solutions Architect
2025/01

AWS Black Belt Online Seminar とは

- 「サービス別」「ソリューション別」「業種別」などのテーマに分け、アマゾン ウェブ サービス ジャパン合同会社が提供するオンラインセミナーシリーズです
- AWS の技術担当者が、 AWS の各サービスやソリューションについてテーマごとに動画を公開します
- 以下の URL より、過去のセミナー含めた資料などをダウンロードすることができます
  - https://aws.amazon.com/jp/aws-jp-introduction/aws-jp-webinar-service-cut/
  - https://www.youtube.com/playlist?list=PLzWGOASvSx6FIwIC2X1nObr1KcMCBBlqY

ご感想は X (Twitter) へ！ハッシュタグは以下をご利用ください
#awsblackbelt

内容についての注意点

- 本資料では資料作成時点のサービス内容および価格についてご説明しています。AWS のサービスは常にアップデートを続けているため、最新の情報は AWS 公式ウェブサイト (https://aws.amazon.com/) にてご確認ください
- 資料作成には十分注意しておりますが、資料内の価格と AWS 公式ウェブサイト記載の価格に相違があった場合、AWS 公式ウェブサイトの価格を優先とさせていただきます
- 価格は税抜表記となっています。日本居住者のお客様には別途消費税をご請求させていただきます
- 技術的な内容に関しましては、有料の AWS サポート窓口へお問い合わせください
- 料金面でのお問い合わせに関しましては、カスタマーサポート窓口へ
お問い合わせください (マネジメントコンソールへのログインが必要です)

自己紹介

櫻井　俊和(さくらい　としかず)

アマゾン ウェブ サービス ジャパン合同会社
エンタープライズ技術本部
シニアソリューションアーキテクト

好きな AWS サービス:

AWS Transit Gateway, AWS Cloud WAN, AWS CloudFormation

本セミナーの対象者

- これから AWS を利用される予定のネットワーク担当者
- AWS のネットワーク設計を担当している方
- AWS Transit Gateway について深く学びたい方

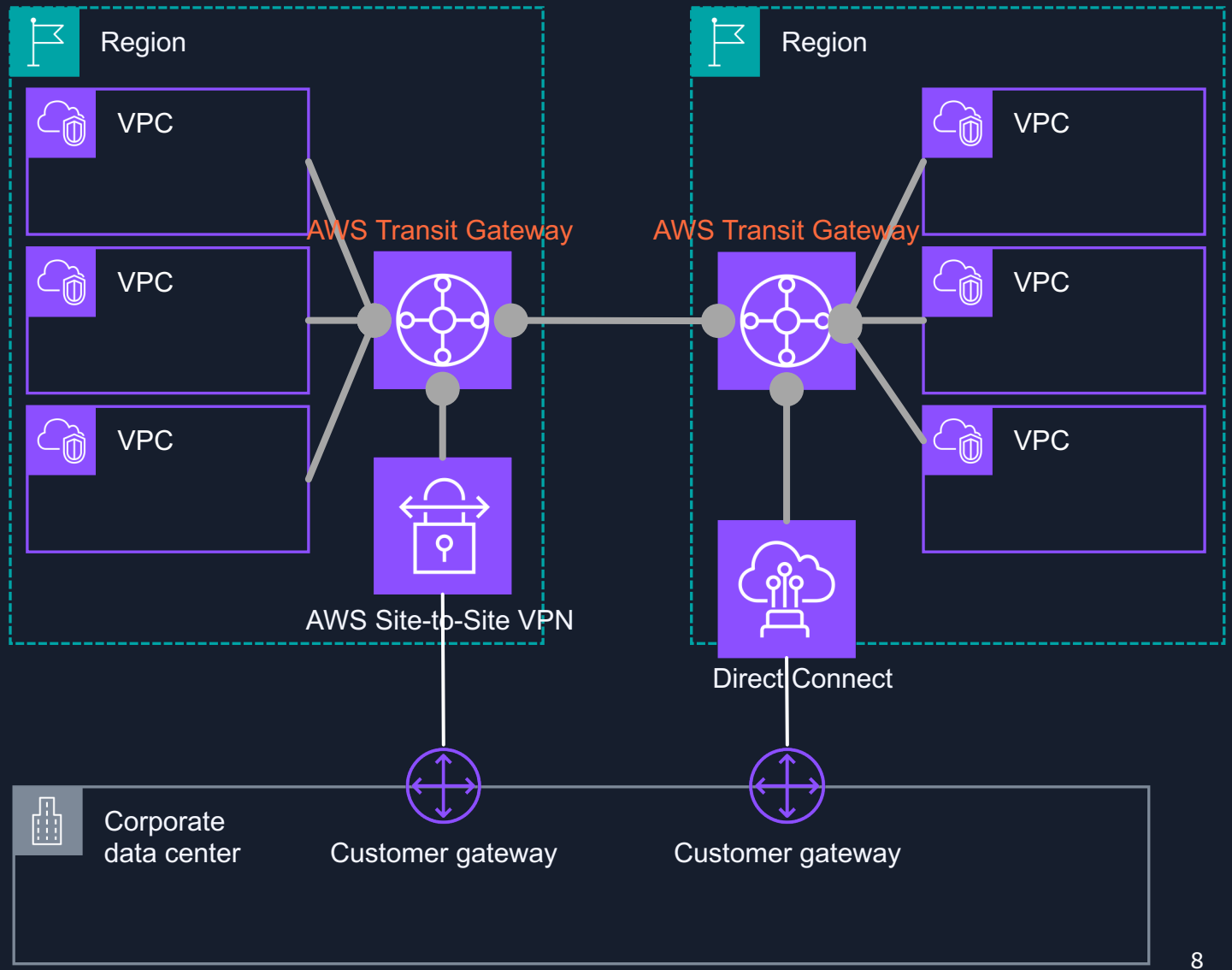
Agenda

1. AWS Transit Gateway とは
2. Transit Gateway の用語と動作
3. クロスアカウント接続
4. アーキテクチャパターン
5. 注意点
6. その他の機能
7. Monitoring
8. Quota / 料金

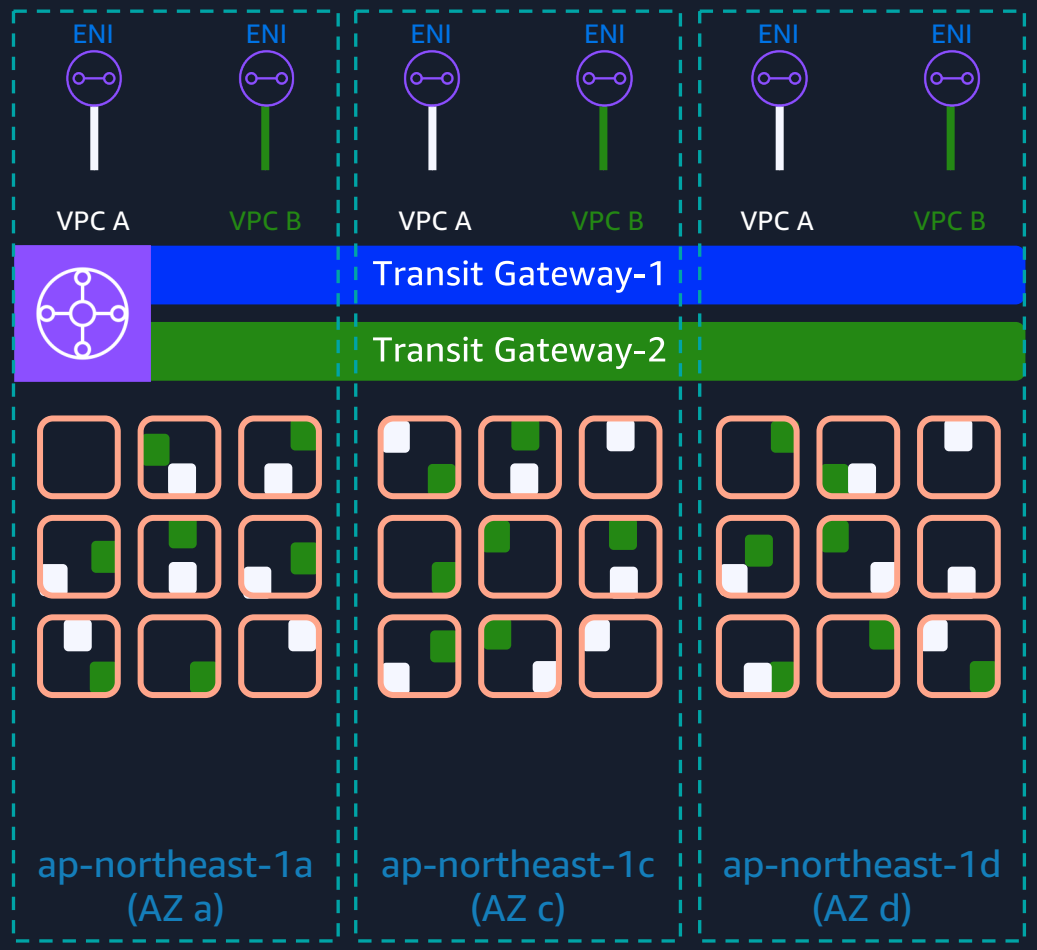
1. AWS Transit Gateway とは

AWS Transit Gateway とは

- 同一リージョン内のVPC を集約する中央ハブになれる
- Direct Connect / VPN などとも接続できる
- 複数のルートテーブルを持つことができる
- リージョン間接続は Transit Gateway どうしを ピアリング(Inter-region peering)する
- 同一リージョンの Transit Gateway を ピアリング(intra-region peering)も可能
- IPv4/v6 を サポート



AWS HyperPlane and AWS Transit Gateway



Attachment :

- AZごとに1つのENI(Elastic Network Interface)
  - AZ内の1つのサブネットにのみアタッチ可能
- AZごとの高信頼性
- ネットワーク容量のシャーディングによる確保
- 数十マイクロ秒の低レイテンシー

AWS HyperPlane :

- 水平方向に拡張可能なステートマネジメント
- Tbpsを超えるマルチテナンシーのサポート
- NLB,NAT Gateway,Amazon EFSのサポート、さらにTransit Gatewayをサポート

ユーザー側で Transit Gateway 自体の可用性を考慮する必要はない

Transit Gateway を検討するタイミング

- 同一リージョン上に VPC が3つ以上存在し、増加が見込まれる
- リージョン間の VPC 間通信パターンが増えた
  - VPC peering では管理しきれない
- VPC 間、インターネット向け、オンプレミスとの通信を監査したい
  - VPC 内の通信と VPCを跨ぐ通信の権限を分離しガバナンスを効かせる
- Direct Connect で接続する VPC が 20 を超える
  - Private VIF の Quota を超える VPC との接続が必要

(参考) Cloud WAN と Transit Gateway の比較

	AWS Cloud WAN	AWS Transit Gateway
	AWS Managed	**Customer Managed**
Control	Global Level Control	Region Level Control
Config	Central Intent-Based Policy	Full Config、DIY な IaC ツール
Route Table	Global Segments	Route-Tables
Inter Region	BGP base	Static Route
SD-WAN	Connect Attachment	TGW Connect
Direct Connect	Direct Connect の Transit VIF	Direct Connect の Transit VIF

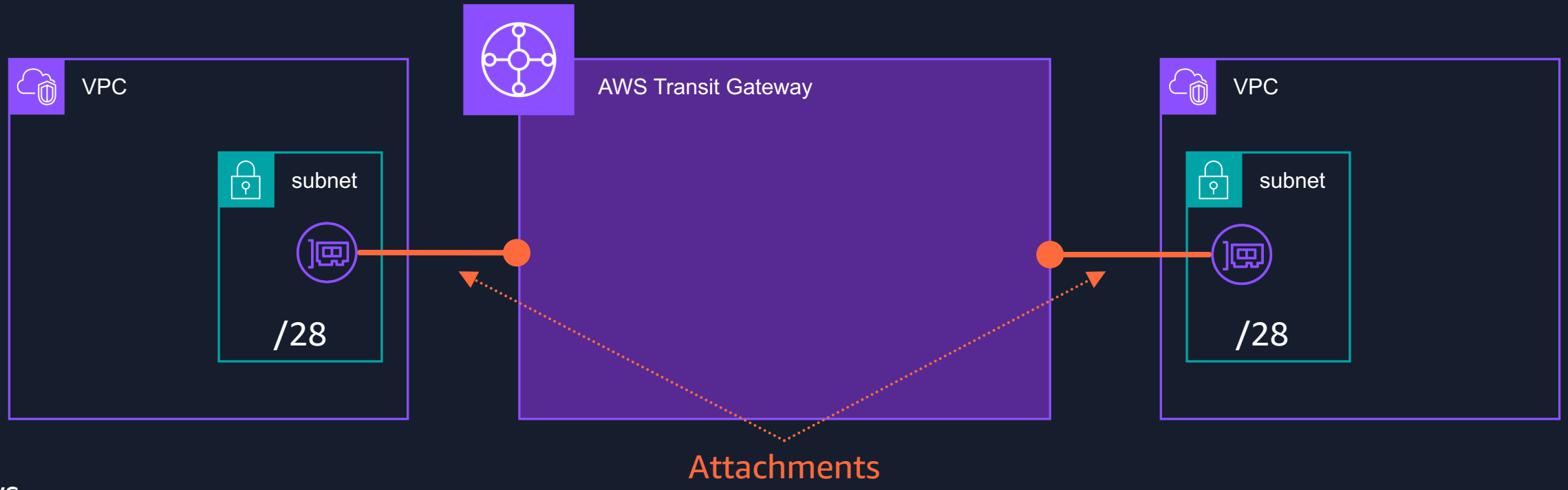
2. Transit Gateway の用語と動作

Transit Gateway の用語と動作

- Attachments (アタッチメント)
- Transit gateway route table (ルートテーブル)
- Associations (アソシエーション)
- Route propagation (プロパゲーション)
- ルーティング動作
- その他(VPC 以外)のアタッチメント

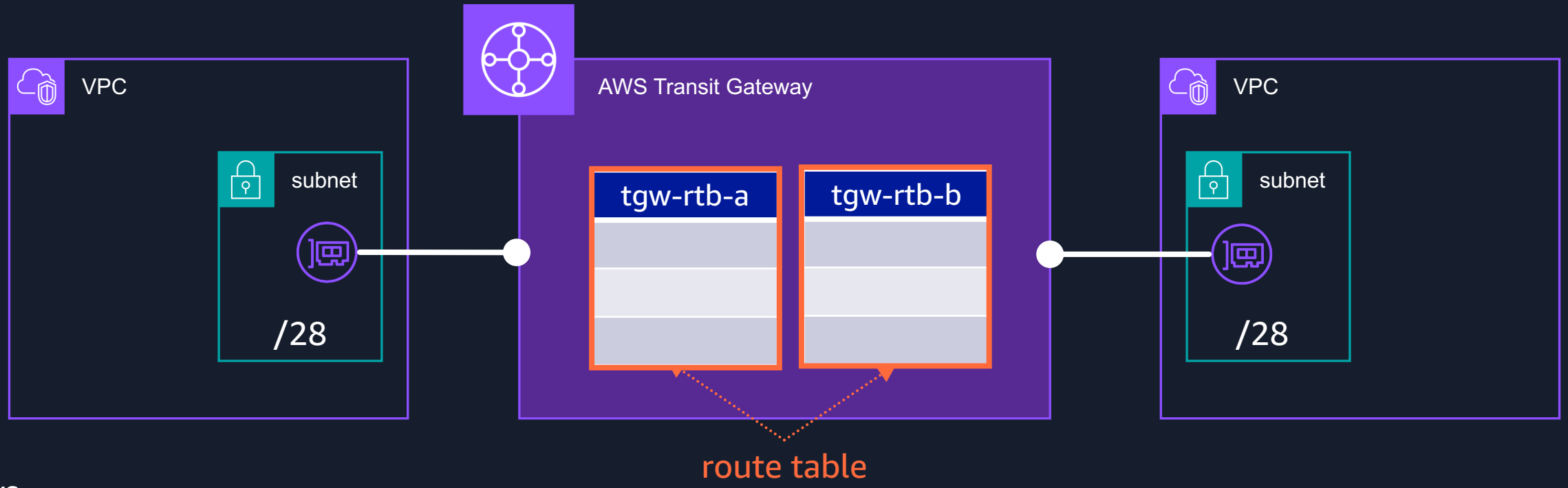
Attachments (アタッチメント)

- VPC (他VPN, Direct Connect など) を Transit Gateway とアタッチ
- VPCアタッチメントには /28 など小さな CIDR の専用サブネットを推奨
  - ワークロードサブネットとルーティング、Network ACL を独立させるため



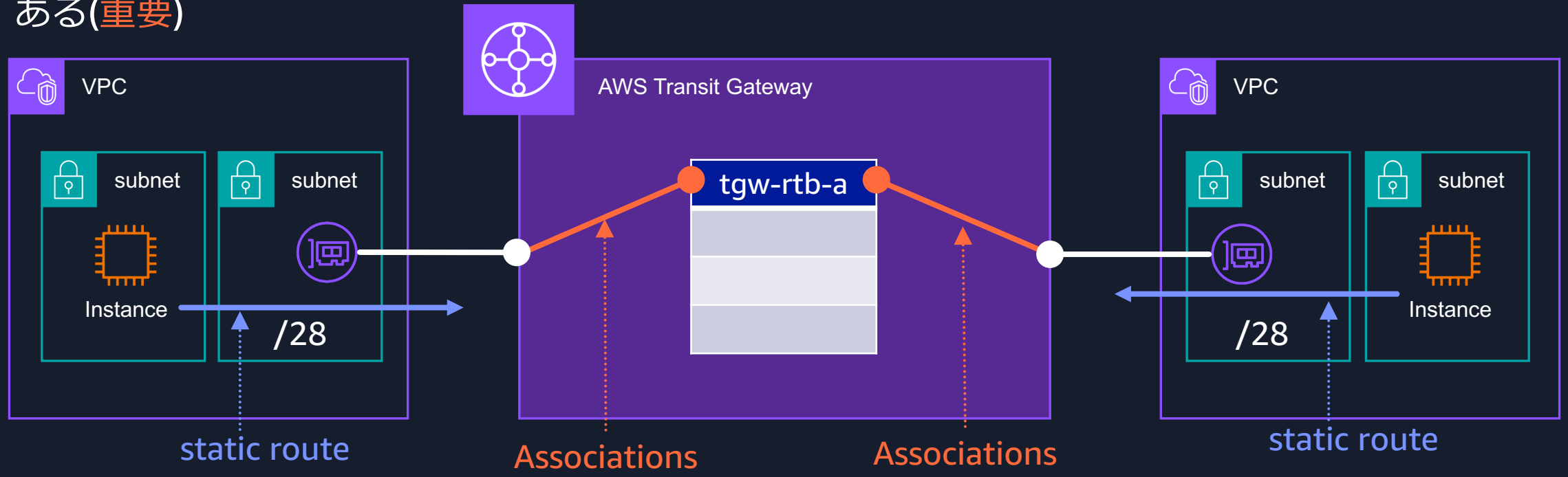
Transit gateway route table (ルートテーブル)

- Transit Gateway が持つ経路情報
- 少なくとも一つのルートテーブルをもち、複数作ることができる



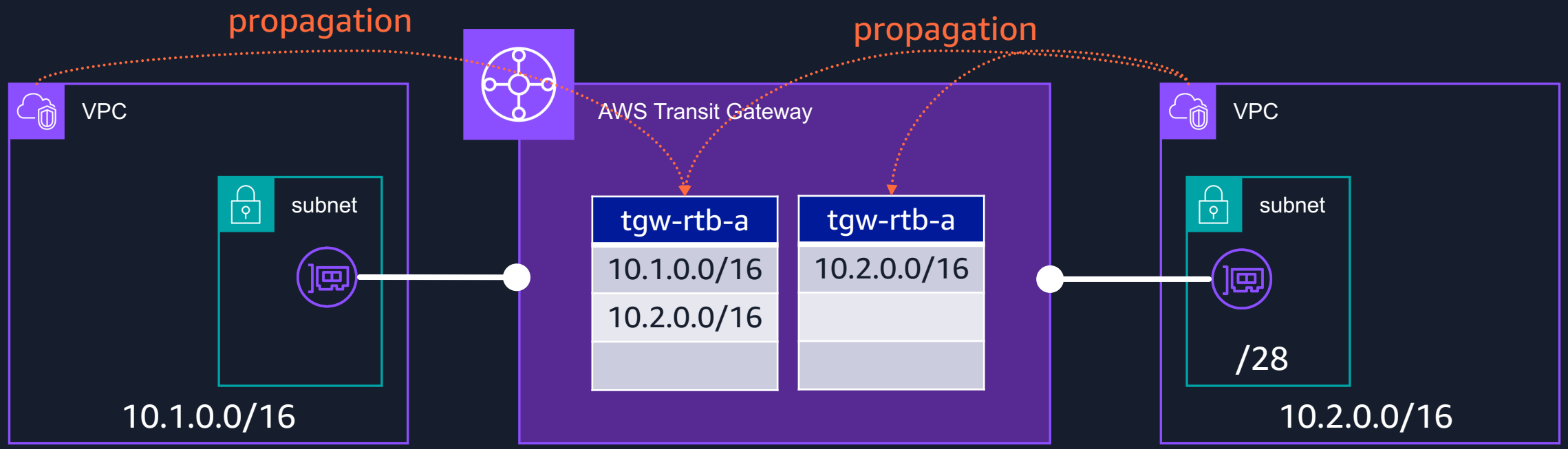
Associations (アソシエーション)

- アタッチメントとルートテーブルをアソシエート(関連付け)する
- VPC などから Transit Gateway へ送信されたパケットはアソシエートされたルートテーブルを参照して ネクストホップに送信
- アタッチメントに対して一つのルートテーブルにしかアソシエートできない(重要)
- VPC 内に Transit Gateway のルート情報は伝播されないため、スタティックルートを書く必要がある(重要)



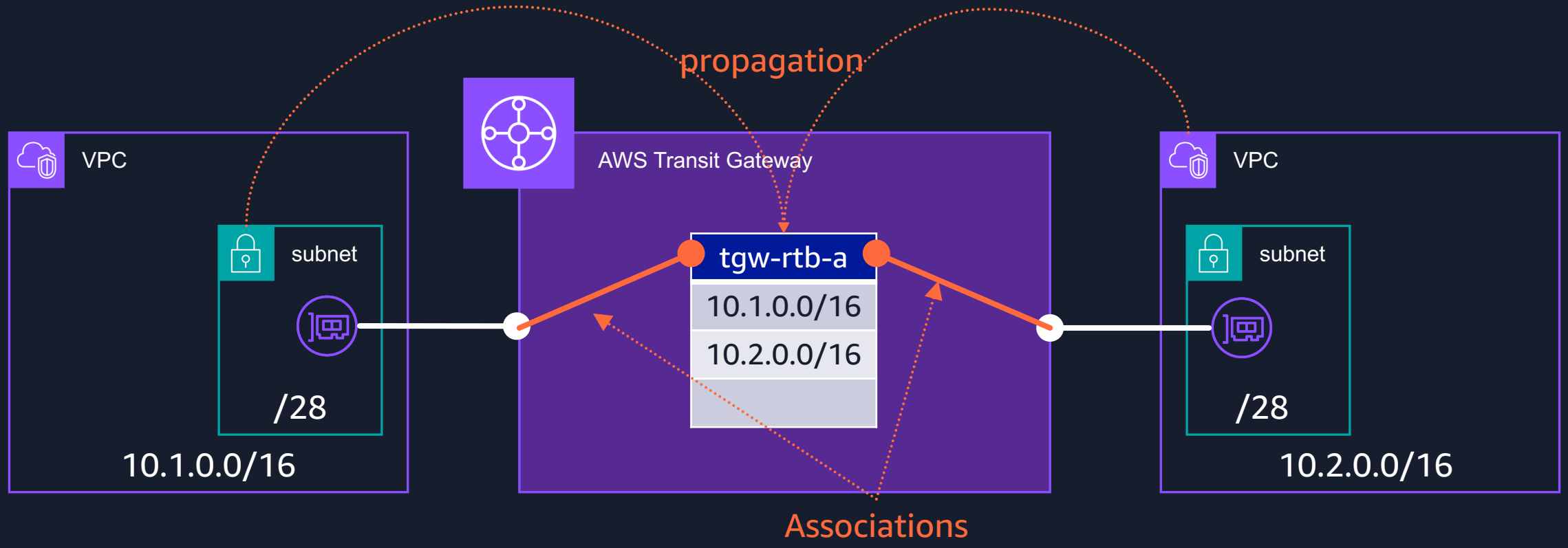
Route propagation (プロパゲーション)

- アタッチした VPC などからルートテーブルに経路をプロパゲート(伝播)する
- プロパゲートはアソシエートに関係なく、複数のルートテーブルに伝播させることができる



Tips: default associate & propagate

- VPC などをアタッチした時にデフォルトでアソシエート、プロパゲートするルートテーブルを一つ設定することができる

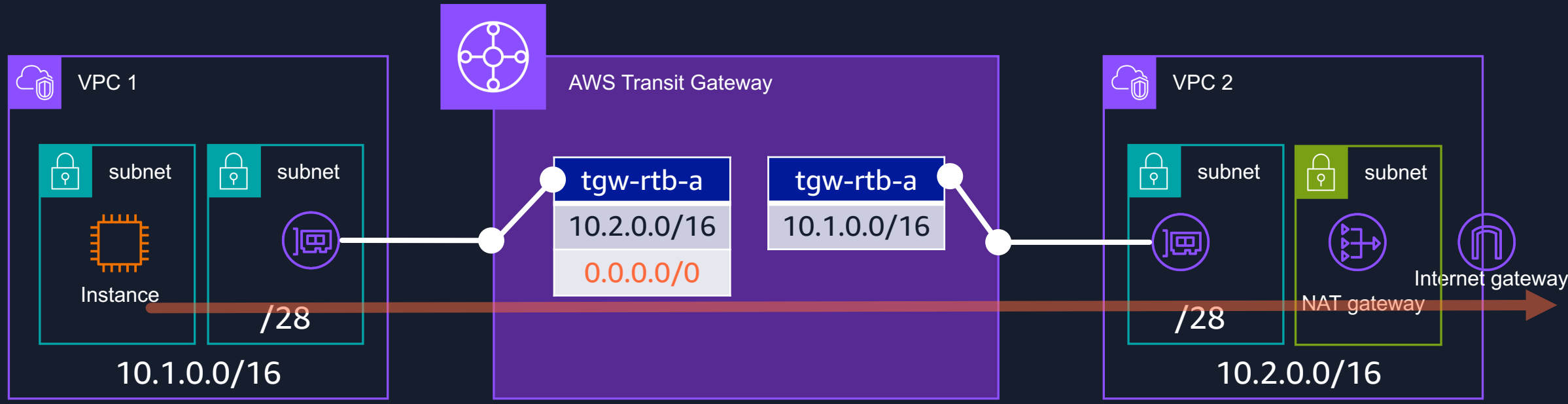


Tips: default associate & propagate

- VPC などをアタッチした時にデフォルトでアソシエート、プロパゲートするルートテーブルを一つ設定することができる

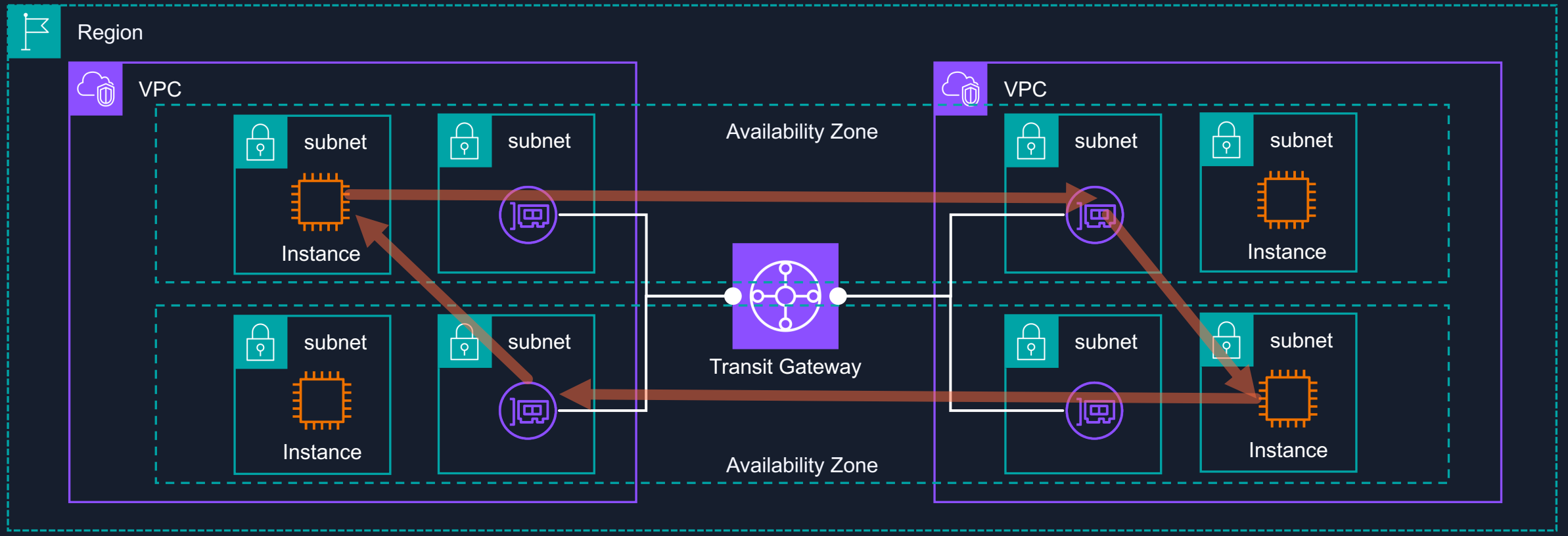
Tips: static route

- ルートテーブルにはスタティックルートを設定することができる
- ブラックホールルートも設定することができる
- ネクストホップはアソシエートされていないアタッチメントでも良い



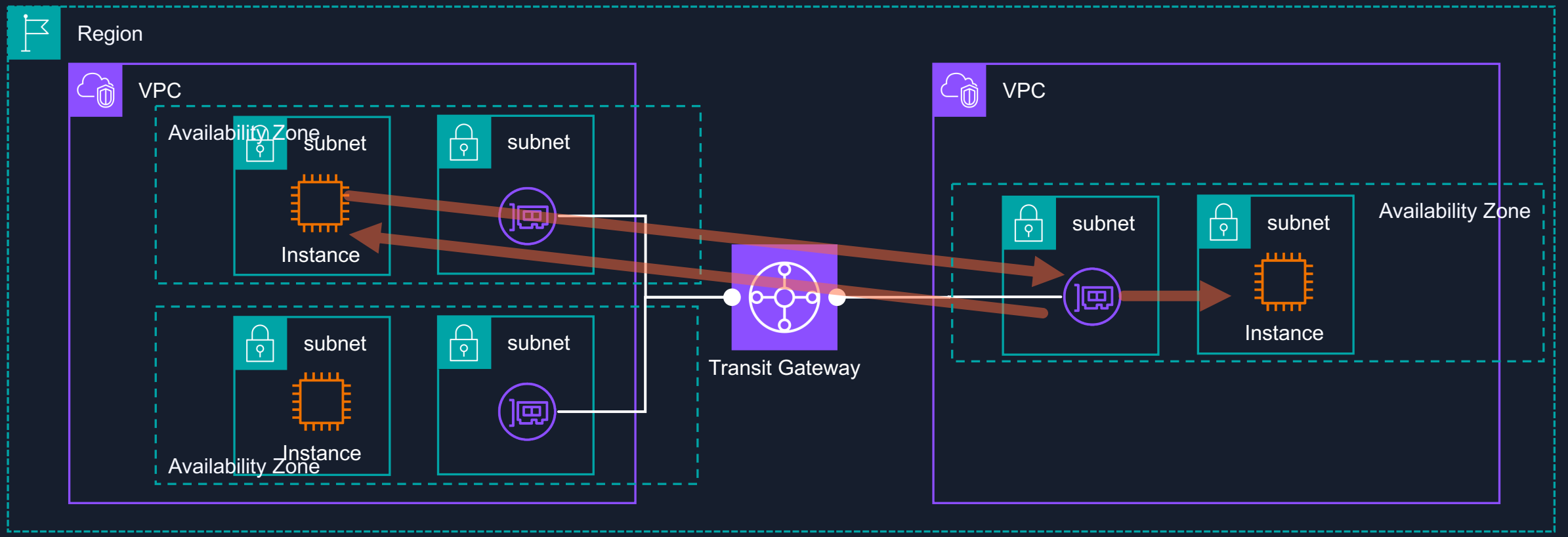
ルーティング動作

- もちろん Multi AZ 構成を推奨
- アタッチメントが存在するアベイラビリティーゾーンにあるリソースのみ、 Transit Gateway に到達できる
- VPC 間の通信は同一 AZ の ENI を経由して通信する(デフォルトの動作)



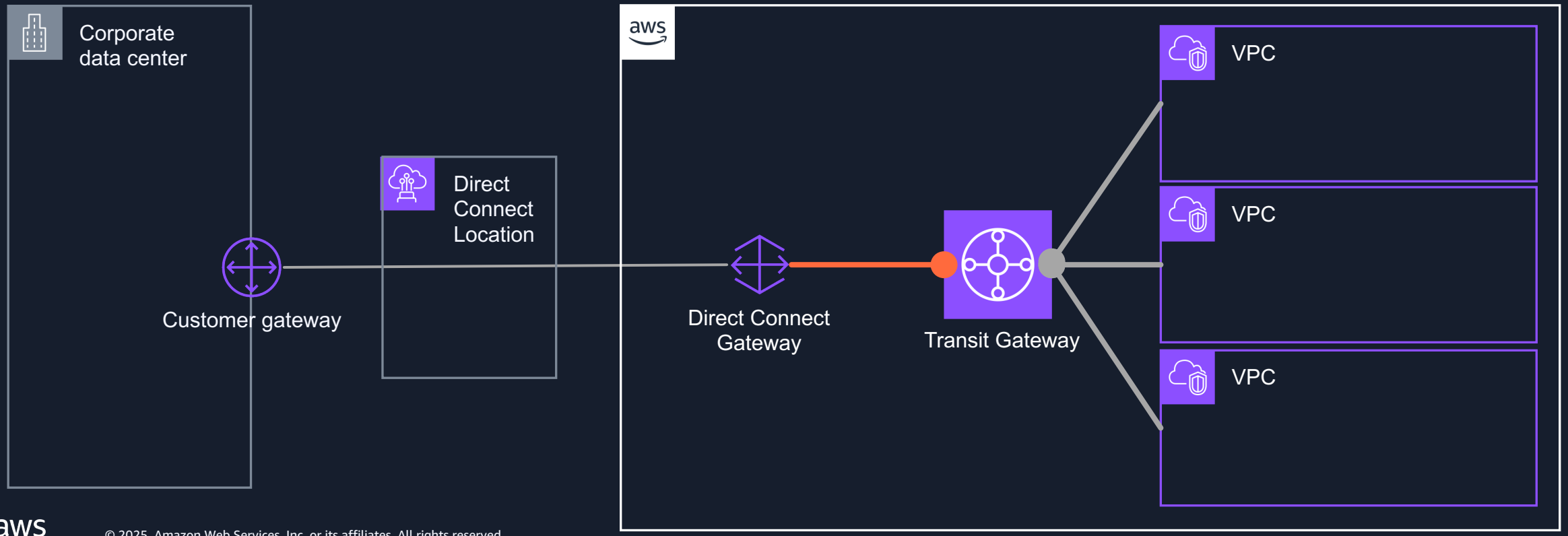
ルーティング動作

- 送信先に同一 AZ が存在しない場合は、いずれかの ENI を経由して通信する



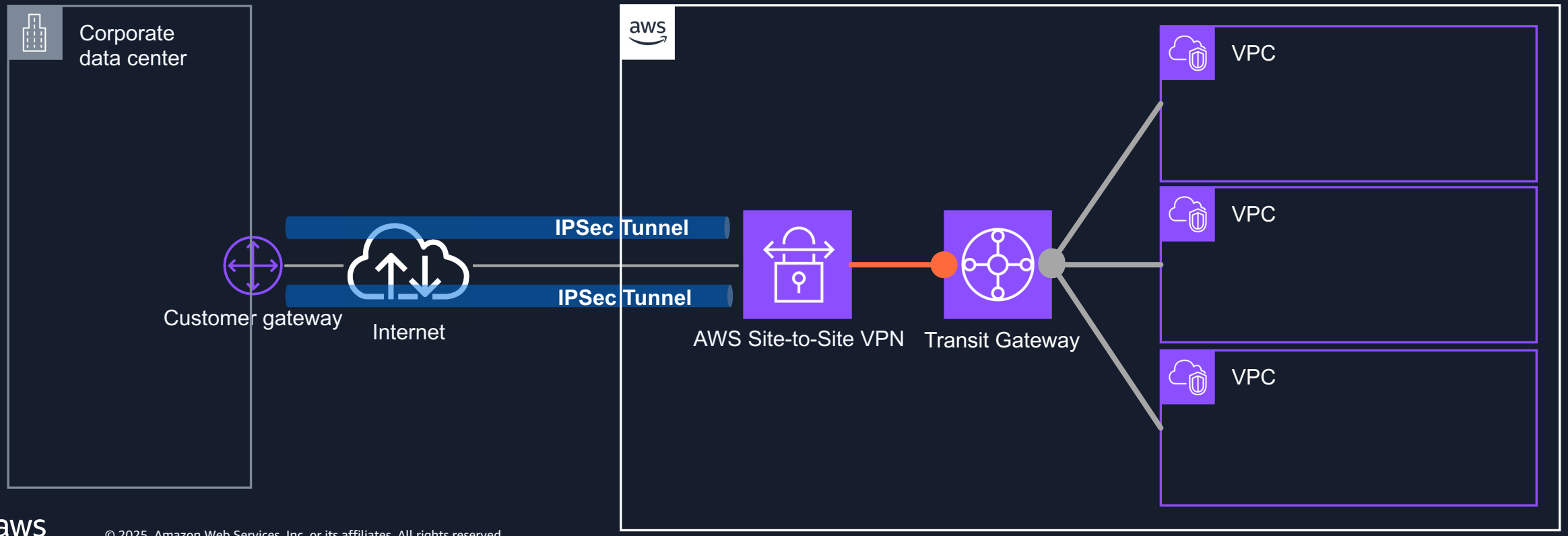
その他のアタッチメント – Direct Connect Gateway

- Transit VIF + Direct Connect Gateway(DXGW) とアタッチすることでオンプレミスと接続
- 複数の VPC を一つの Direct Connect Connection で接続
- Transit VIF (TGW) と関連づけられた DXGW は Private VIF, VGW との接続は併用できない



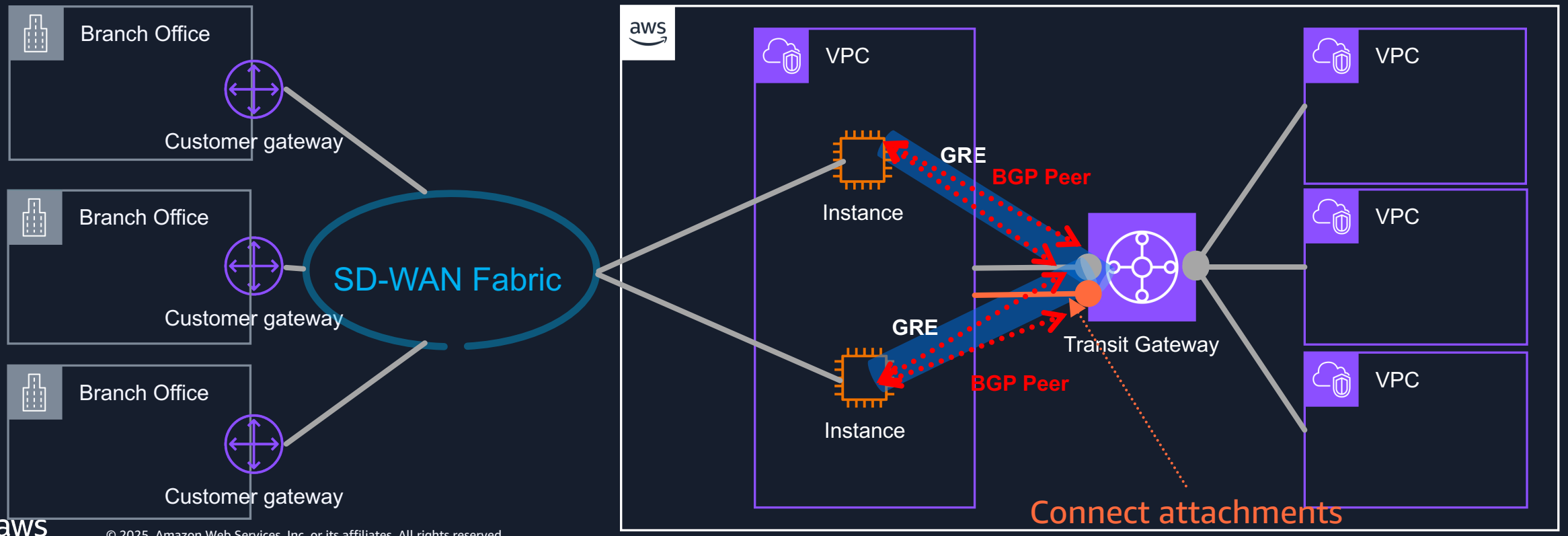
その他のアタッチメント – Site-to-Site VPN

- Site-to-Site VPN を Transit Gateway とアタッチ
- 複数の VPC を一つの VPN で接続
- ECMP をサポート



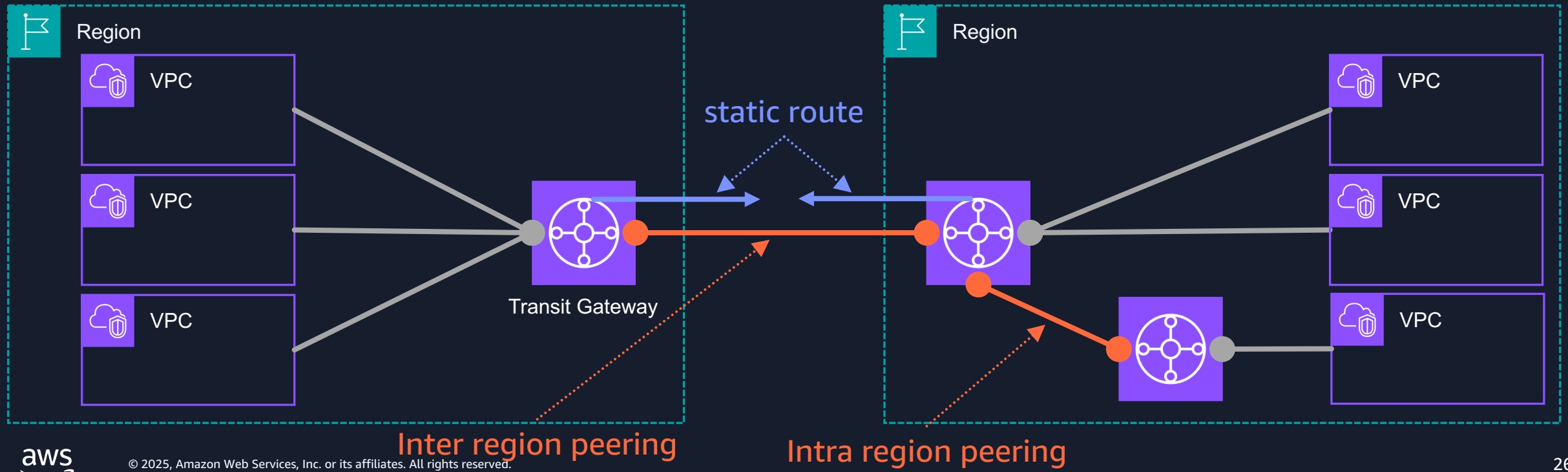
その他のアタッチメント – Connect Attachments

- VPC または Direct Connect Gateway アタッチメントをトランスポートに使用
- Connect アタッチメント上に Connect ピア (BGP over GRE) を構成して仮想アプライアスと接続
- GRE tunnel あたり 最大 5Gbps, 2つの BGP Peer セッション(推奨)
- ECMP をサポート



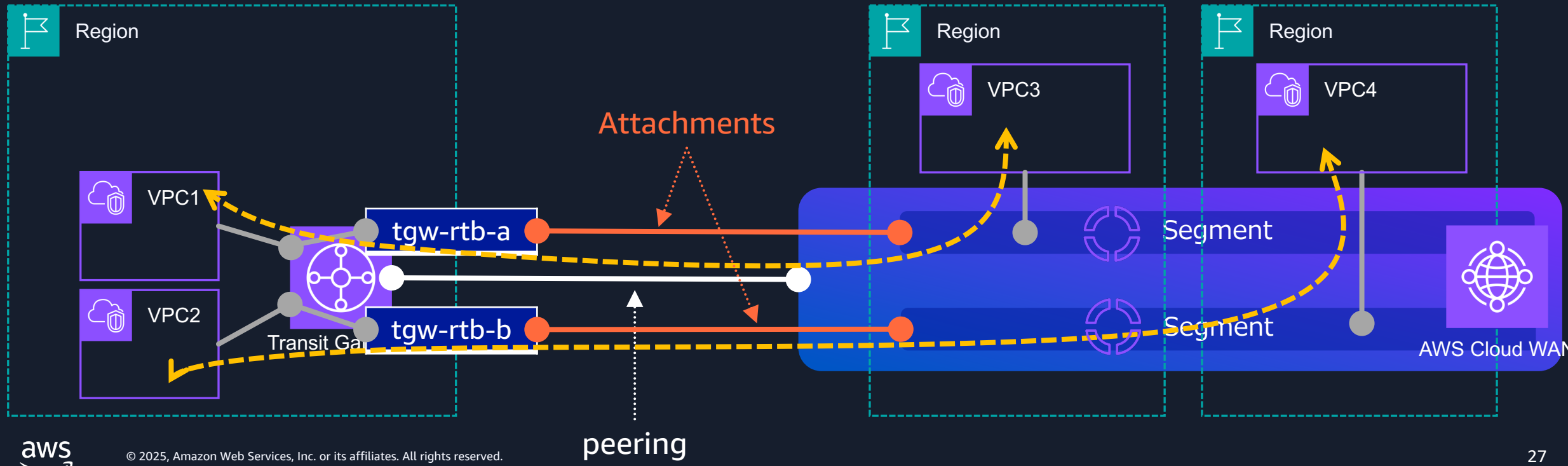
その他のアタッチメント – Peering Attachments

- Transit Gateway どうしを接続(peering)する
- リージョン内(Intra region)、リージョン間(Inter region)のどちらも peering できる
- peering 間での経路の伝播はサポートしていないため、スタティックルートを設定
- ピアリングアタッチメントをアクティブにするには、両方の Transit Gateway が同じアカウントにある場合でもアクセプタ Transit Gateway の所有者がリクエストを受け入れる必要がある



その他のアタッチメント – Cloud WAN

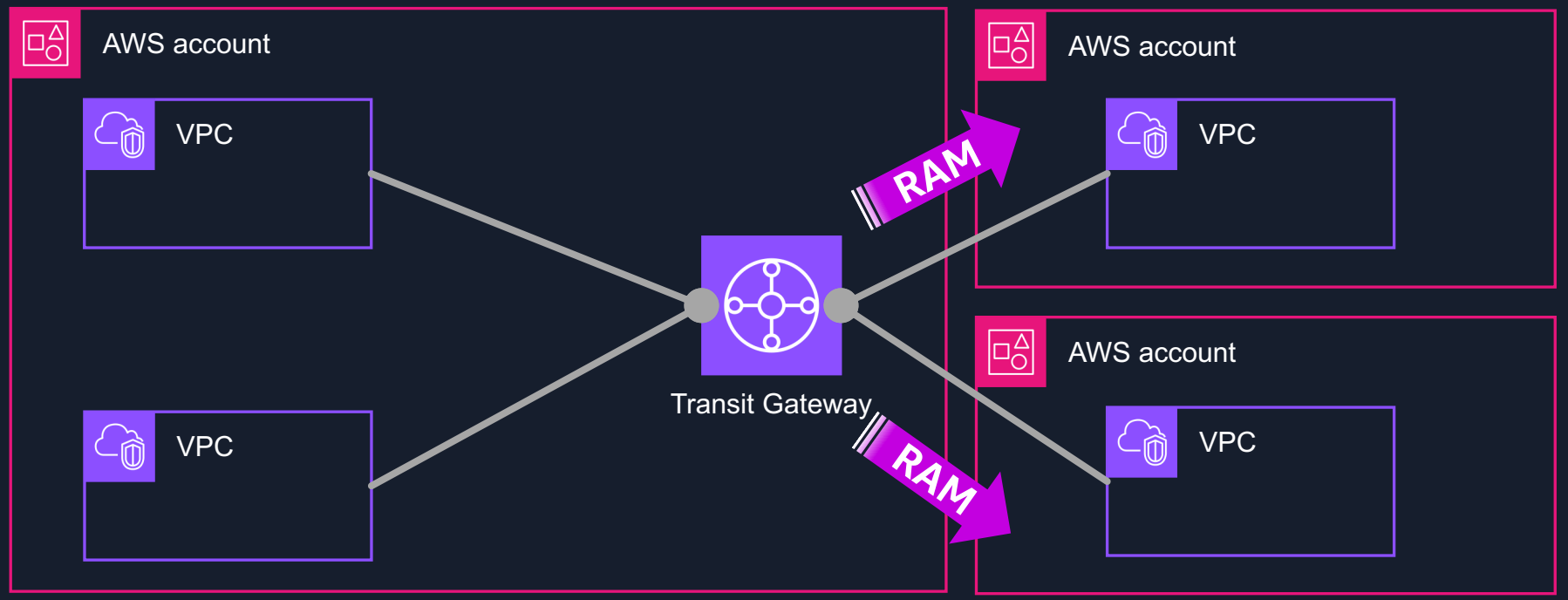
- Transit Gateway と Cloud WAN をpeering
- Transit Gateway のルートテーブルと Cloud WAN の セグメントをアタッチ
- 互いの経路情報を BGP ベースで伝播



3. クロスアカウント接続

クロスアカウント接続

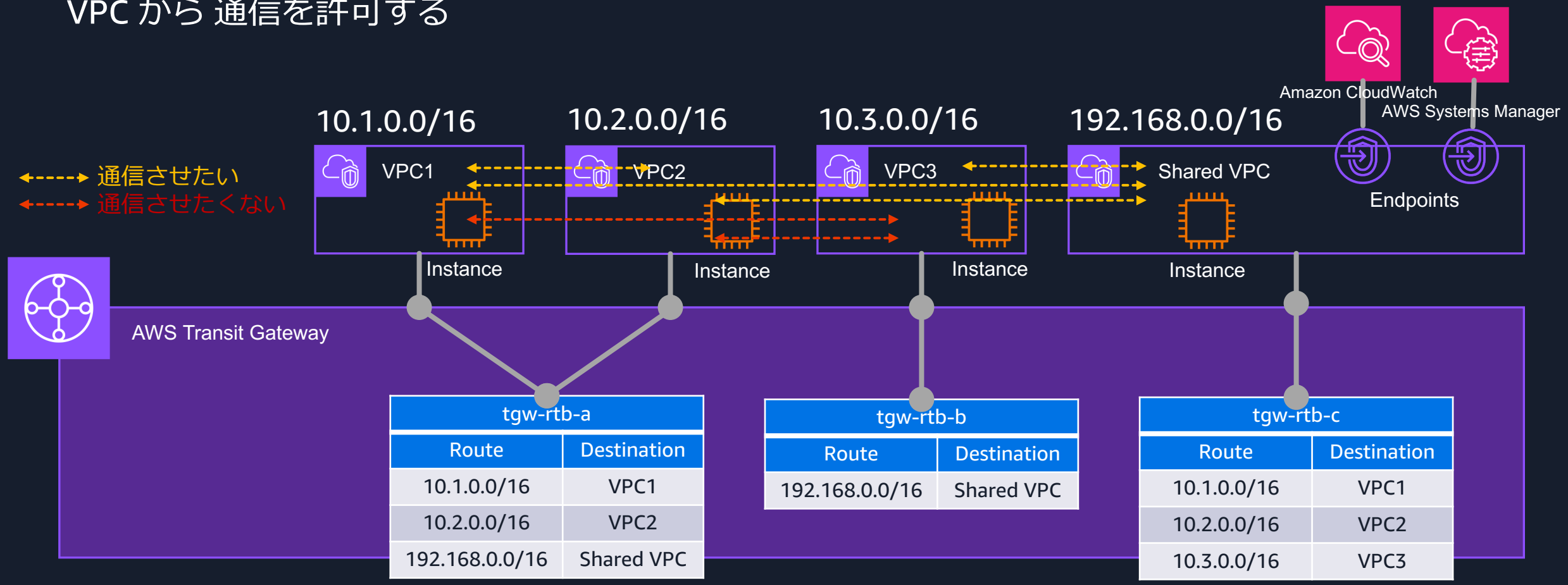
- Transit Gateway を アタッチする VPC 所有アカウントに Resource Access Manager(RAM) で共有
- VPC 所有アカウントは Transit Gateway にアタッチ
- ルートテーブル、アソシエーション、プロパゲーションは Owner Account のみが設定できる
  - default associate & propagate をうまく使う



4. アーキテクチャパターン

Route table 分割による Shared VPC 構成

- 相互通信したい VPCと通信したくない VPC を route table にて分割する
- 共通して利用したい サービス (AD, DNS, Endpoint Service など) を Shared VPC において全ての VPC から 通信を許可する



tgw-rtb-a	
Route	Destination
10.1.0.0/16	VPC1
10.2.0.0/16	VPC2
192.168.0.0/16	Shared VPC

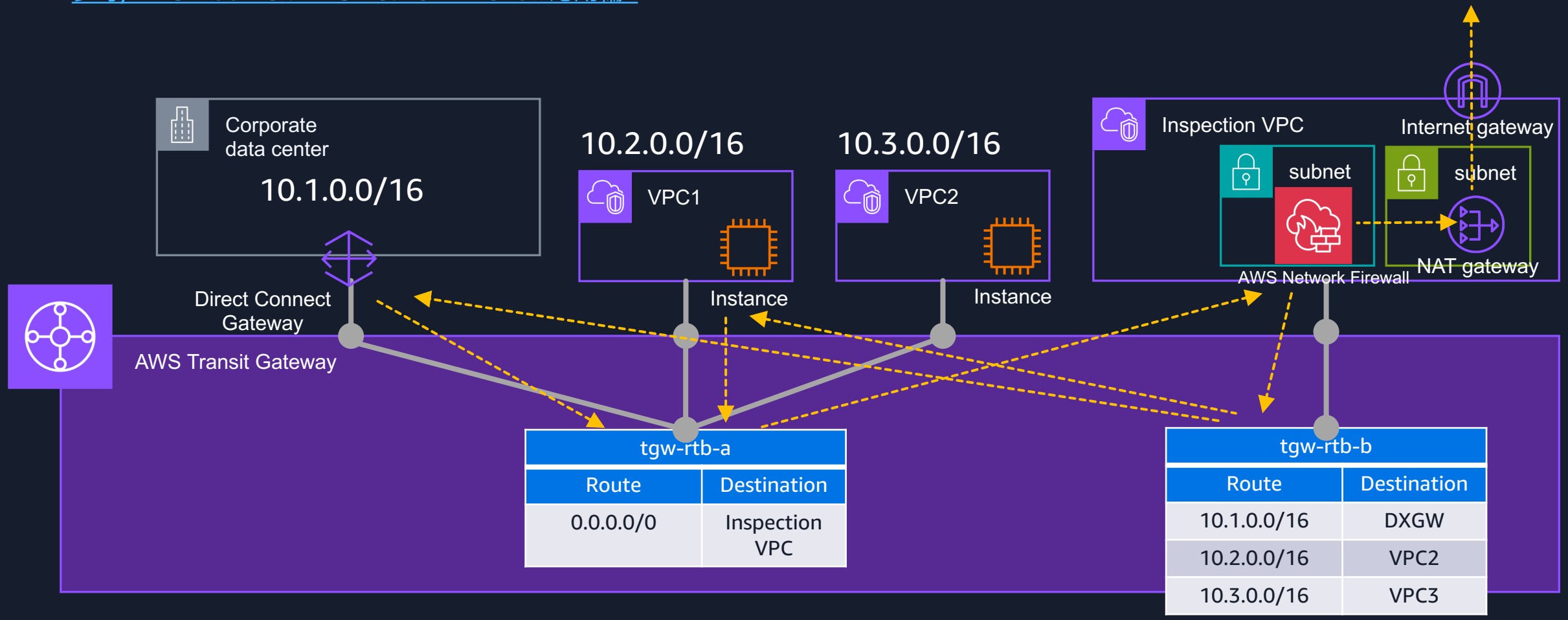
tgw-rtb-b	
Route	Destination
192.168.0.0/16	Shared VPC

tgw-rtb-c	
Route	Destination
10.1.0.0/16	VPC1
10.2.0.0/16	VPC2
10.3.0.0/16	VPC3

Inspection VPC による Traffic 監査

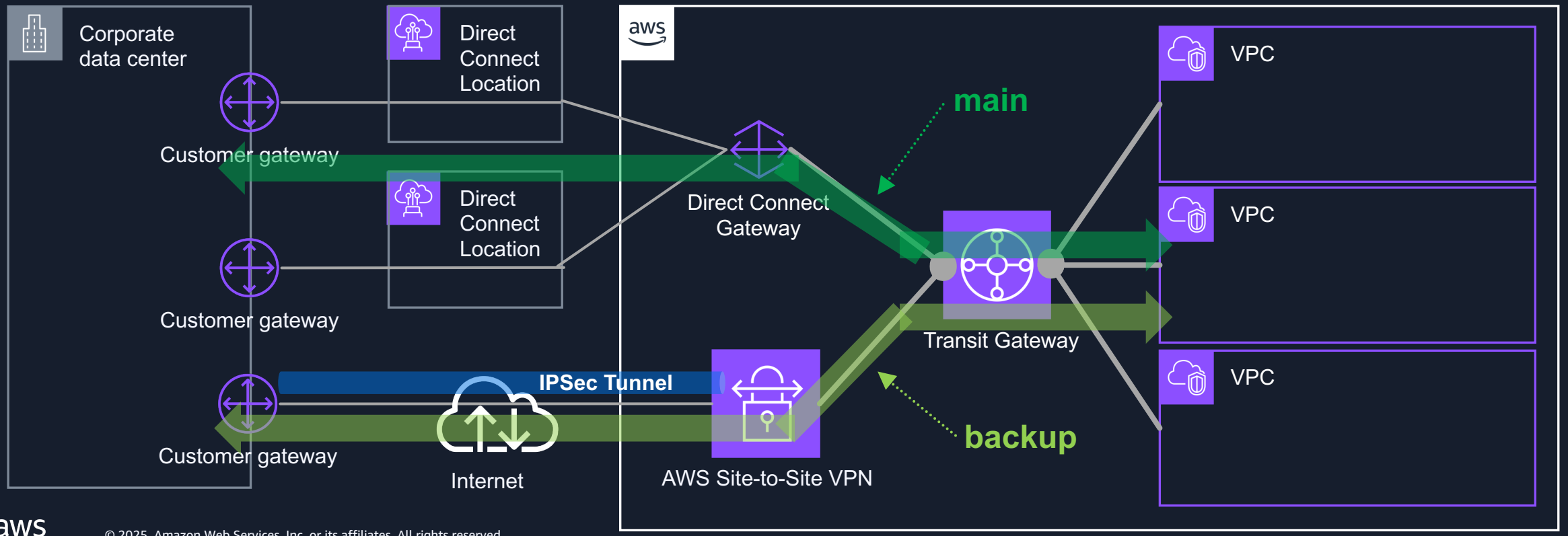
- VPC 間およびダイレクトコネクト・インターネット通信の トラフィックを監査する

参考) AWS BlackBelt AWS Network Firewall 応用編1



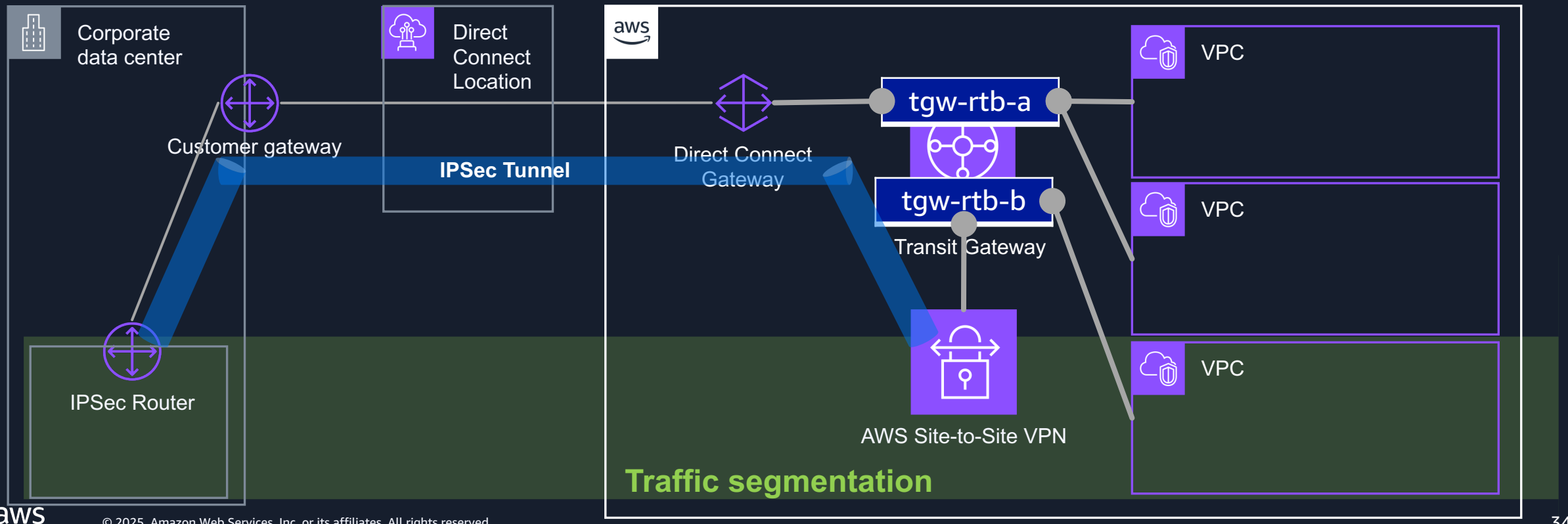
Direct Connect + Site-to-Site VPN 冗長構成

- Direct Connect と Site-to-Site VPN を併用して オンプレミスとの接続を冗長化する
- Direct Connect と Site-to-Site VPN から同じ経路が伝播された場合は Direct Connect を優先



Private IP VPN with AWS Direct Connect

- Direct Connect をトランスポートに使用して Site-to-Site VPN を作成する
  - Transit Gateway までの専用線区間を暗号化
  - オンプレミス – AWS 間の トラフィックセグメンテーション

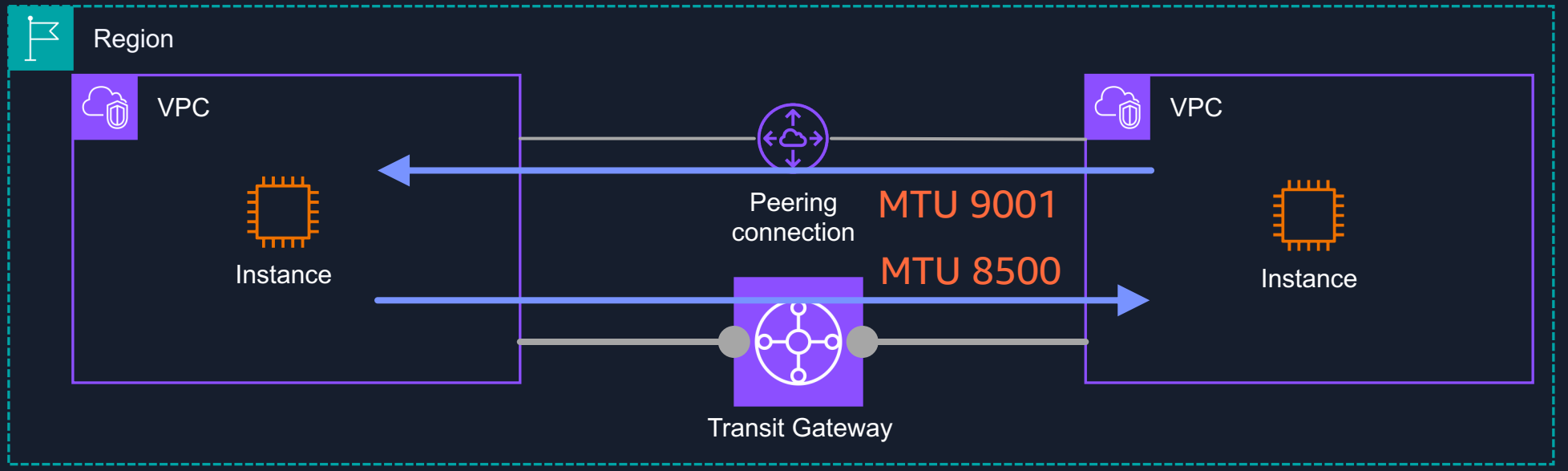


5. 注意点

VPC Peering からの移行時における MTU の違い

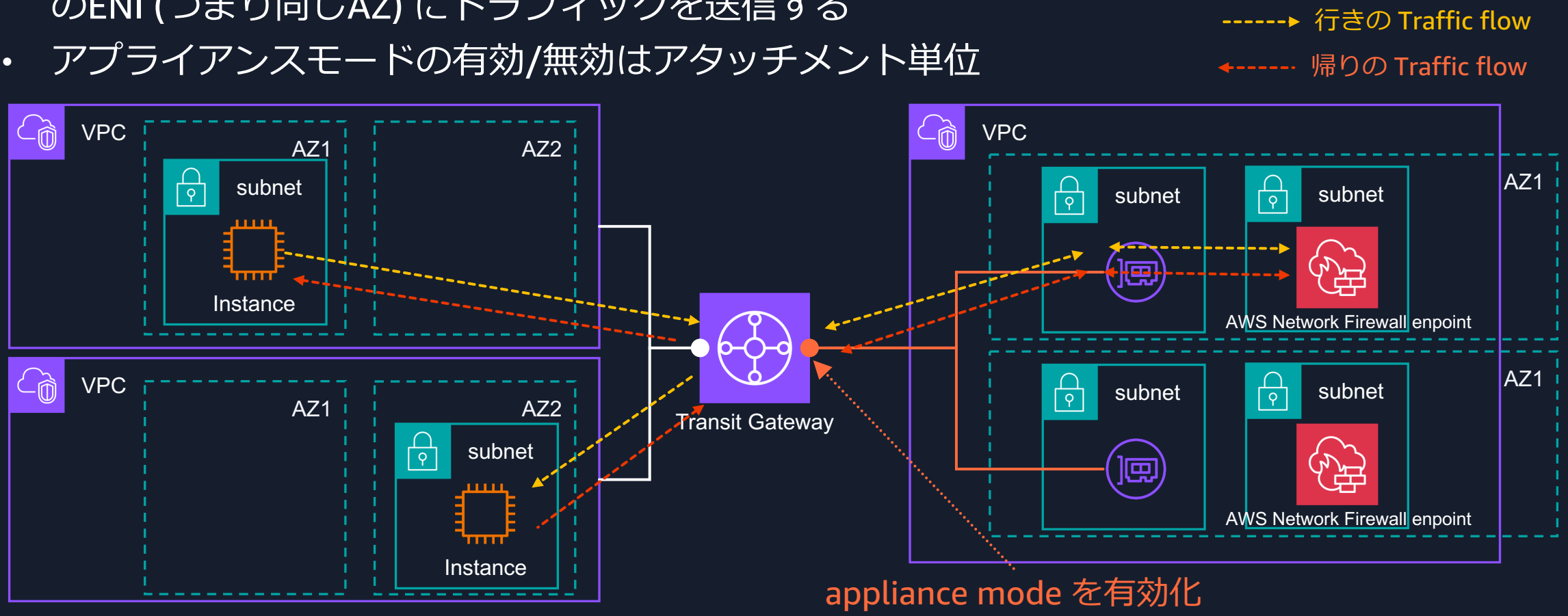
- VPC Peering から Transit Gateway に移行する時
  - VPC peering (同一リージョン) の MTUは 9001
  - Transit Gateway の MTU は 8500
    - Path MTU Discovery はサポート(new!!)
    - MSS clamping を全てのパケットに適用

以下のような状態ではパケットがドロップされる可能性がある



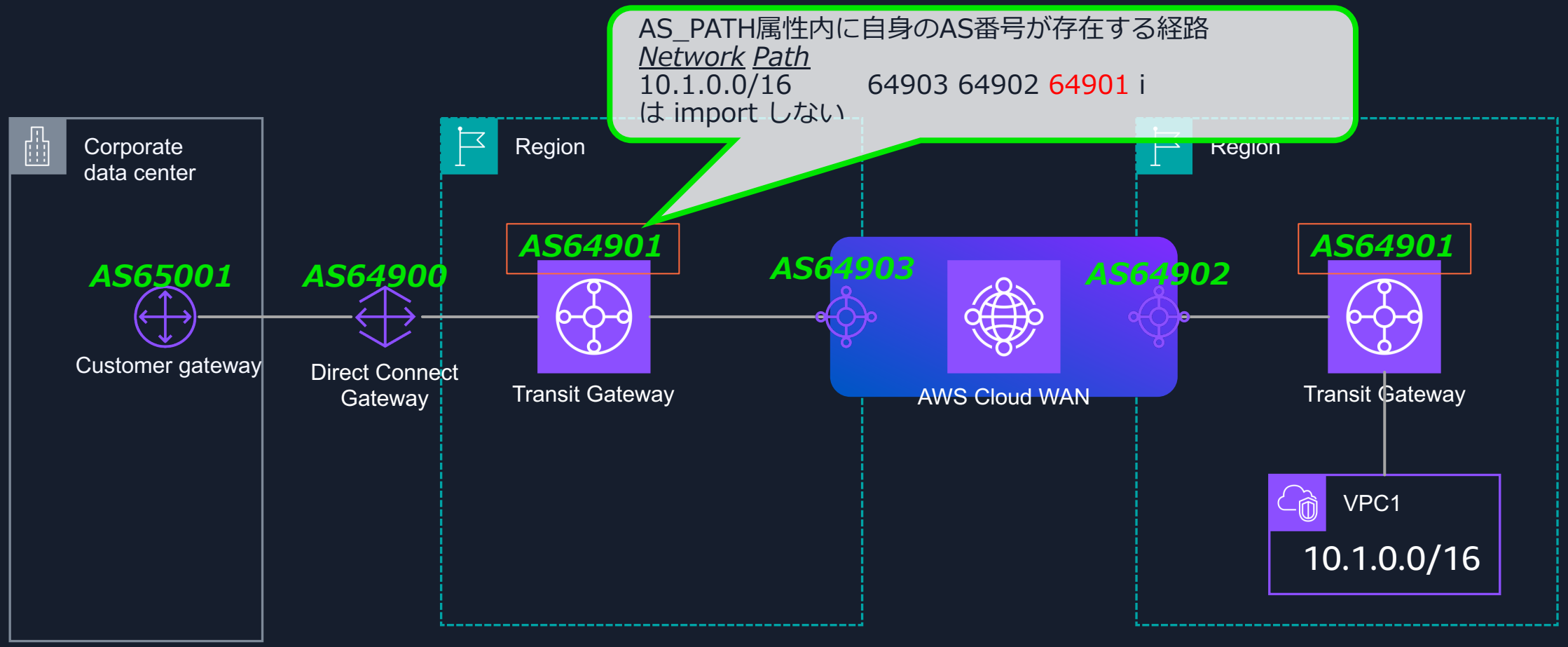
Inspection 構成時の multi AZ 通信

- 監査用 VPC をマルチ AZ で構成する場合には、アプライアンスモードを有効にする
  - アプライアンスモードを有効にするとフローハッシュアルゴリズムにより、同一フローは単一のENI (つまり同じAZ) にトラフィックを送信する
  - アプライアンスモードの有効/無効はアタッチメント単位



AS Number の割り当て

- Transit Gateway に割り当てる ASN は一意にしておくのが推奨



TGW Route evaluation order (Best Path Selection)

1. Most specific route
2. For routes with the same CIDR, but from different attachment types, the route priority is as follows
    - •Static routes (for example, Site-to-Site VPN static routes)
    - •Prefix list referenced routes
    - •VPC-propagated routes
    - •Direct Connect gateway-propagated routes
    - •Transit Gateway Connect-propagated routes
    - •Site-to-Site VPN over private Direct Connect-propagated routes
    - •Site-to-Site VPN-propagated routes
    - •Transit Gateway peering-propagated routes (Cloud WAN)
3. BGP attributes

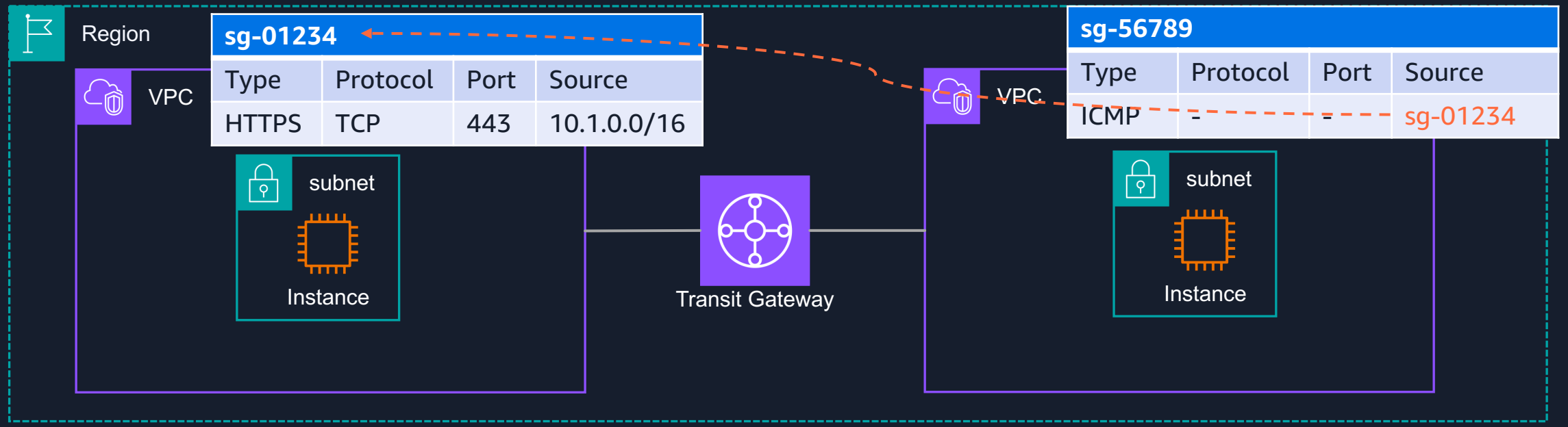
BGP attribute よりも
Attachment type が
優先される

https://docs.aws.amazon.com/vpc/latest/tgw/how-transit-gateways-work.html#tgw-route-evaluation-overview

その他の機能

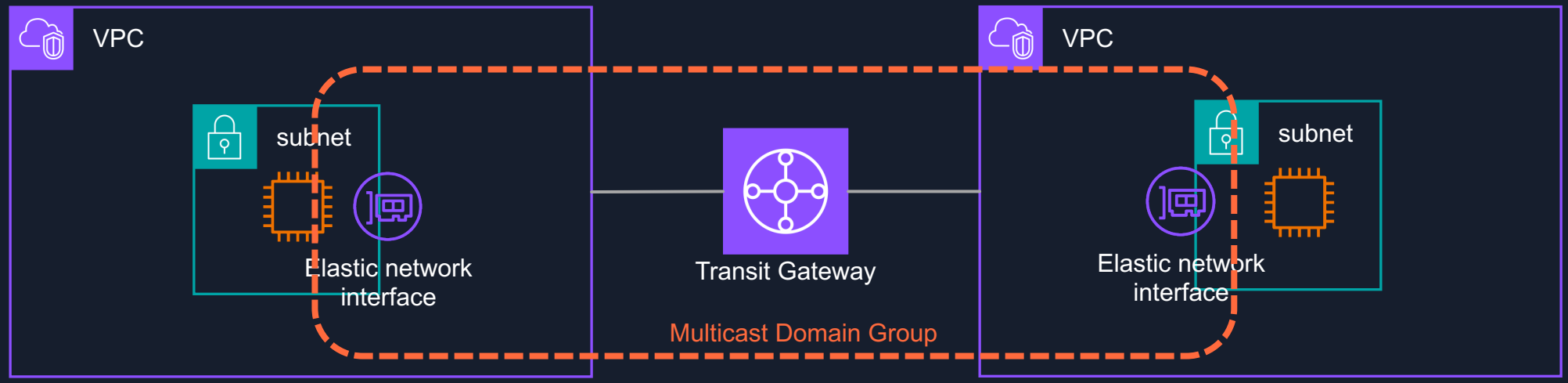
Referenced security group

- Transit Gateway を介して接続された VPC 間でインバウンド セキュリティグループを参照
  - Transit Gateway レベル、VPC Attachment レベルで共に有効化している場合のみ機能する
  - 参照する VPC は同一リージョンに存在する必要がある
  - Cross Account でも動作
  - マネージメントコンソール上ではリスト検索できないので、Security Group ID を直接入力



Multicast on Transit Gateway

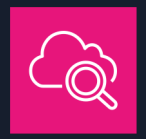
- Transit Gateway がマルチキャストルーターとして動作
  - VPC Attachment のみで動作
  - Transit Gateway を新規作成時のみ有効にできる
  - IGMPv2 を support



Monitoring

VPC Flow Logs

- Transit Gateway 全体もしくはアタッチメント単位で Flow Log の取得が可能
- ログの発行先は下記のいずれか


Amazon CloudWatch Logs


Amazon S3


Amazon Data Firehose

- 制限事項
  - マルチキャストトラフィックはサポートされない

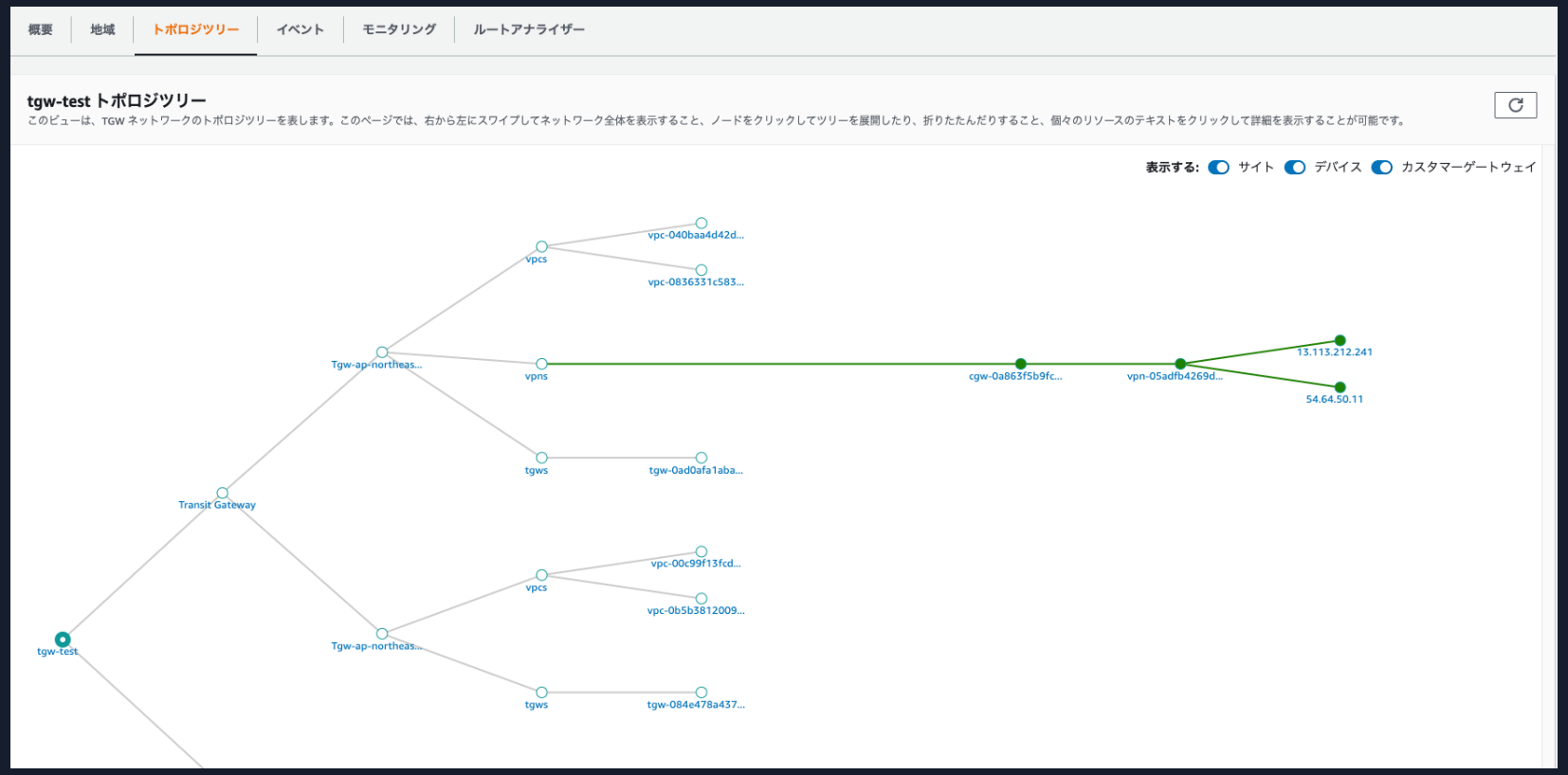
CloudWatch Metrics

- Transit Gateway 全体もしくはアタッチメント単位(AZ毎も)で使用できる

メトリクス	説明
BytesDropCountBlackhole	blackhole ルートと一致したためにドロップされたバイトの数。
BytesDropCountNoRoute	ルートと一致しなかったためにドロップされたバイトの数。
BytesIn	Transit Gateway あたりの受信バイト数。
BytesOut	Transit Gateway からの送信バイト数。
PacketsIn	Transit Gateway によって受信されたパケットの数。
PacketsOut	Transit Gateway によって送信されたパケットの数。
PacketDropCountBlackhole	blackhole ルートと一致したためにドロップされたパケットの数。
PacketDropCountNoRoute	ルートと一致しなかったためにドロップされたパケットの数。

AWS Global Networks for Transit Gateways

- AWS Network Manager の Global Network に統合されている
- 複数のTGW を一元的に管理
  - Overview, Geography, Topology tree, Events, Monitoring, Route Analyzer



Quota / 料金

Quota (抜粋)

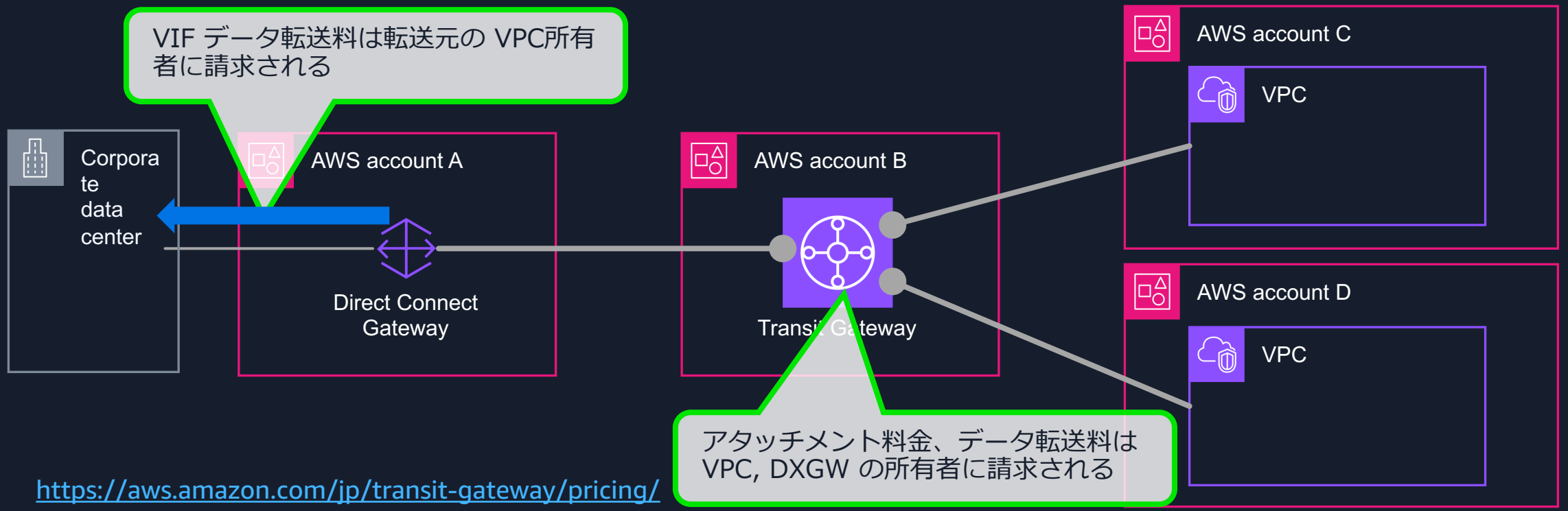
	項目	Default	Adjustable
General	アカウントあたりの Transit Gateway	5	Yes
Routing	Transit Gateway あたりの Transit Gateway ルートテーブル数	20	Yes
	Transit Gateway あたりの 経路数	10,000	Yes
Attachment	Transit Gateway あたりのアタッチメント	5,000	No
	VPC あたりのアタッチできる Transit Gateway の数	5	No
Bandwidth	AZ 毎の VPC アタッチメントの帯域幅	100Gbps(max)	Ask
	VPN トンネルあたりの最大帯域幅	1.25Gbps(max)	No
	Connect ピア (GRE トンネル) あたりの最大帯域幅	5Gbps(max)	No
MTU	8500 byte		No

https://docs.aws.amazon.com/ja_jp/vpc/latest/tgw/transit-gateway-quotas.html

料金

- 東京リージョンでの料金 (2024/12月時点)

AWS Transit Gateway のアタッチメントごとの料金 (USD)	0.05/hour
処理データ 1 GB あたりの料金 (USD)	0.02



https://aws.amazon.com/jp/transit-gateway/pricing/

Links:

- Guidance
  - Amazon VPC Transit Gateway 設計のベストプラクティス
  - AWS Transit Gatewayトラフィックフローと非対称ルーティング
- Blog
  - VPC PeeringからAWS Transit Gatewayに移行する際のベストプラクティスと考慮事項
  - AWS Site-to-Site VPN プライベートIP VPN のご紹介
  - AWS Transit Gateway でのセキュリティグループ参照の導入
- ハンズオン
  - AWS Transit Gateway ハンズオン

Thank you!