



SUMMIT
Tokyo

B-01-05

Transit Gateway Deep Dive アーキテクチャガイド

Yukihiro Kikuchi
Solution Architect
Amazon Web Services Japan K. K.

今日持ち帰っていただきたいこと

Transit Gateway用語を理解する

Transit Gatewayで経路制御ができる

Transit Gatewayのユースケースを理解する

自己紹介



名前：菊池 之裕(きくち ゆきひろ)

所属：ソリューションアーキテクト ネットワークスペシャリスト

ロール：Network系サービスについてのご支援

経歴：ISP,IXP,VPN運用、開発を経てネットワーク機器、仮想ルータ販売会社のプリセールス、プロダクトSEからAWSへ

好きな AWS サービス:AWS Transit Gateway,
AWS Direct Connect, AWS Marketplace

Agenda

Transit Gatewayとは

Transit Gatewayの用語と動作

ユースケース

注意するところ

新機能: Transit GatewayとDirect Connectの連携

まとめ

Agenda

Transit Gatewayとは

Transit Gatewayの用語と動作

ユースケース

注意するところ

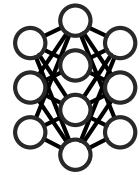
新機能: Transit GatewayとDirect Connectの連携

まとめ

Transit Gatewayとは

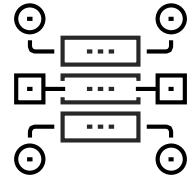


AWS Transit Gateway



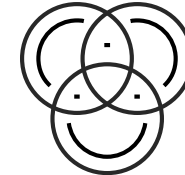
リージョナルゲートウェイ

VPC間接続を簡単に管理するためのシンプルなリージョナルゲートウェイ



大規模

数千の
VPC,VPN,Direct
Connectを接続可能



ルーティング ドメイン

アタッチメントごとの
ルーティングを可能にする
ルーティングドメインのサポート



パートナー連携

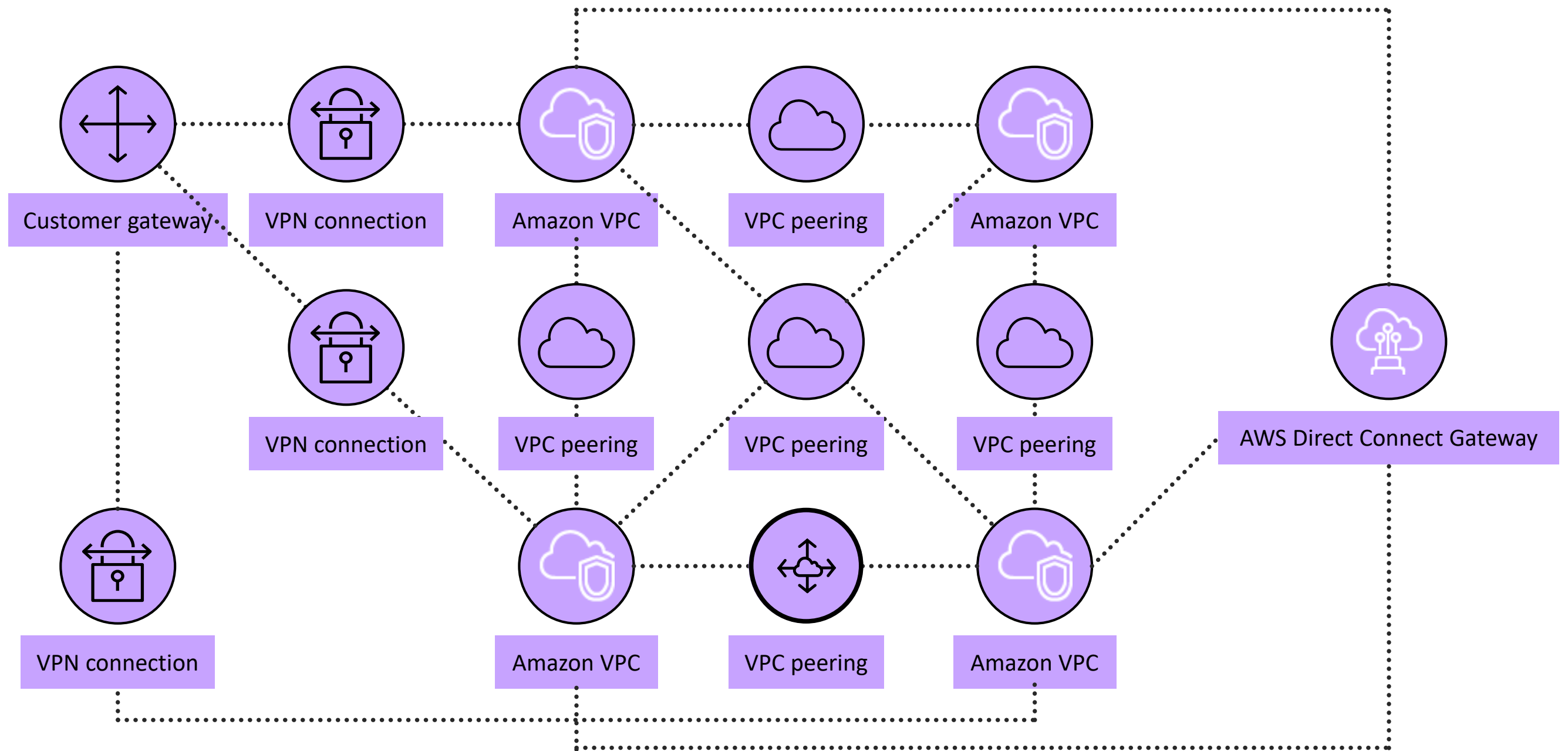
パートナーアプライ
アンスをミドルボック
クスとしてサポート



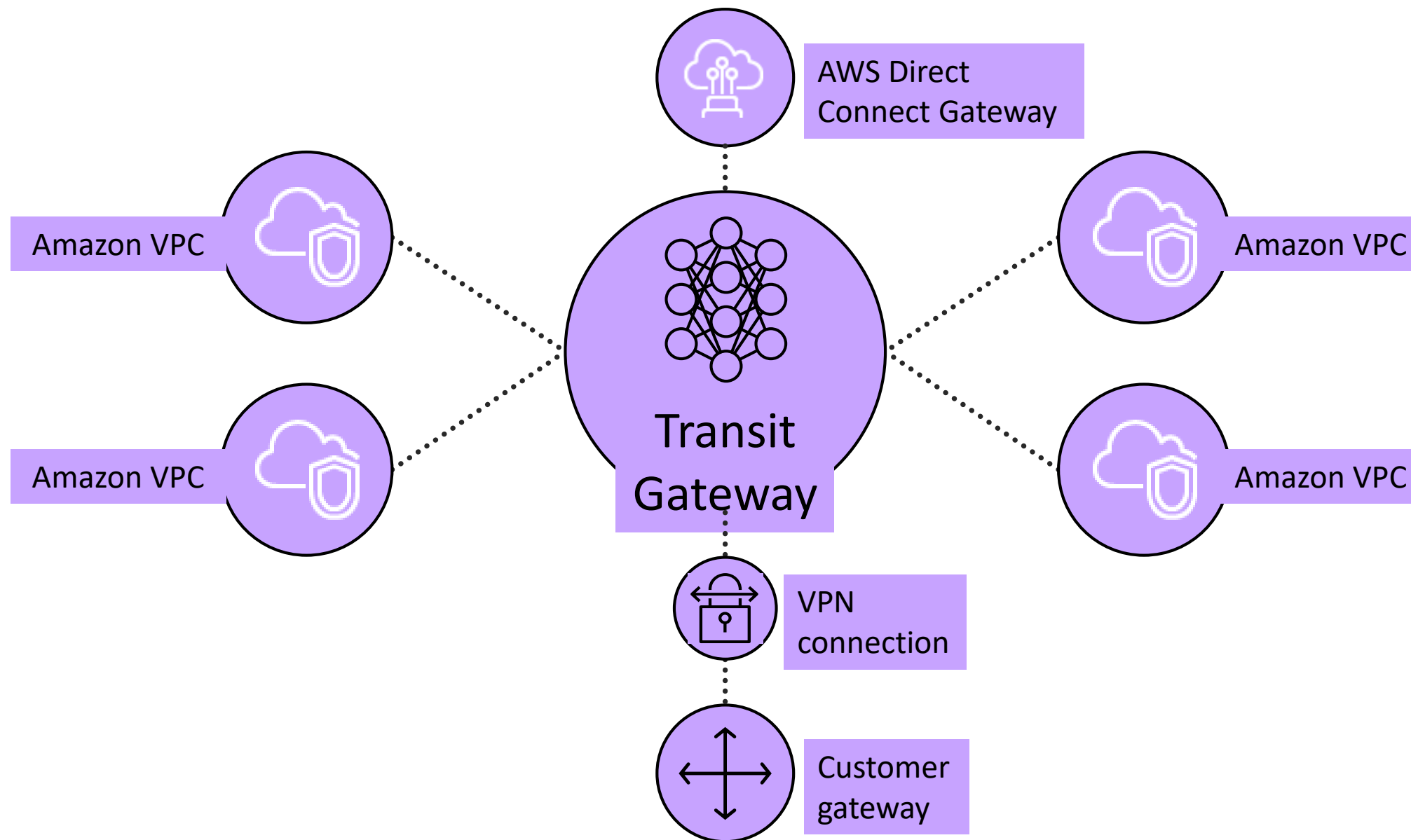
“ AWS Transit Gatewayは徹底的に進化することにより、クラウドネットワーキングを簡素化しました。 Transit Gatewayを使用して、一貫した信頼性の高いネットワークパフォーマンスを実現しながら、新しいVPCとオンプレミスネットワークを相互接続する時間を数週間から数分に短縮しています！ ”

Khoder Shamy, Director, Cloud Platform and Infrastructure, Fuze

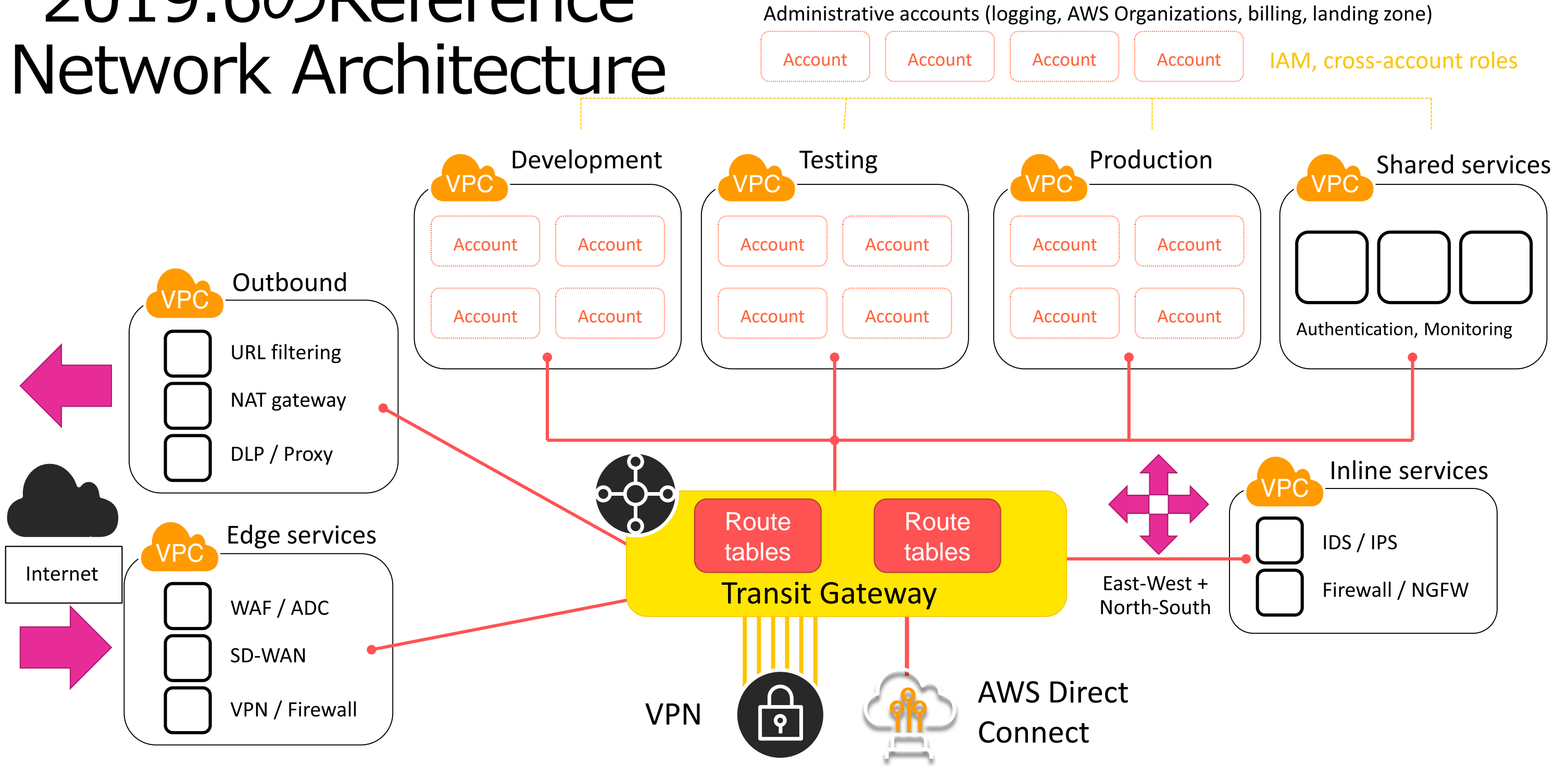
Transit Gateway以前のネットワーク ...



Transit Gatewayを使用すると ...



2019.6のReference Network Architecture



Agenda

Transit Gatewayとは

Transit Gatewayの用語と動作

ユースケース

注意するところ

新機能: Transit GatewayとDirect Connectの連携

まとめ

Transit Gatewayの用語と動作

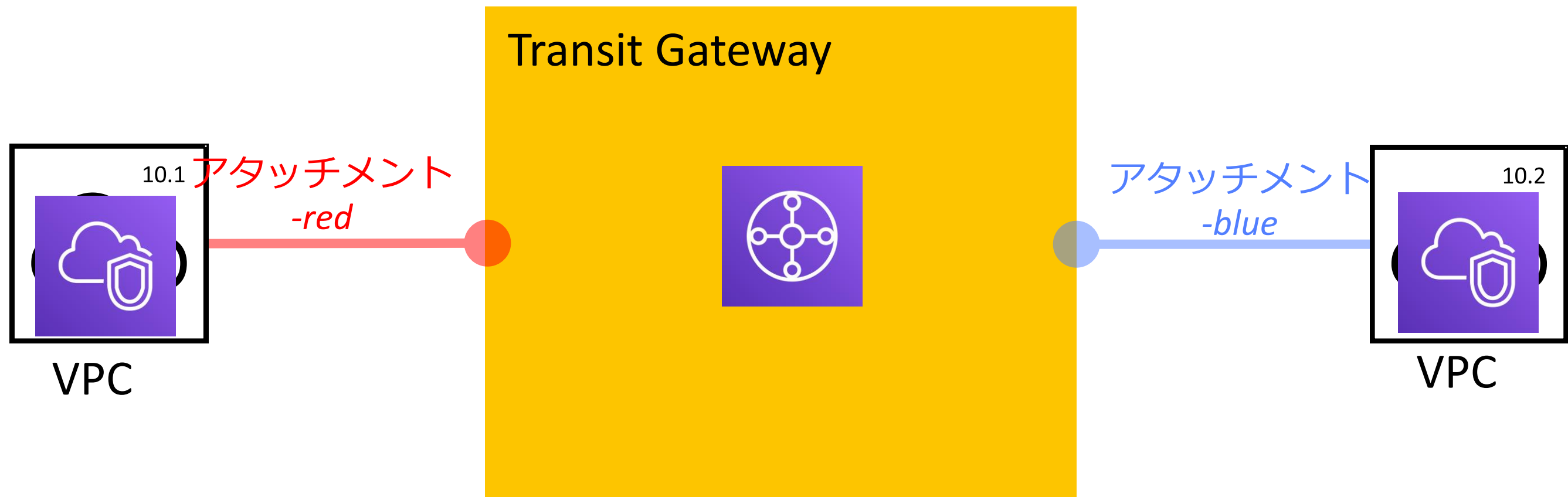
Transit Gateway用語

- アタッチメント
- ルートテーブル
 - アソシエーション
 - プロパゲーション
 - スタティックルート

5つの用語を覚えてTransit Gatewayを
使いこなしましょう！

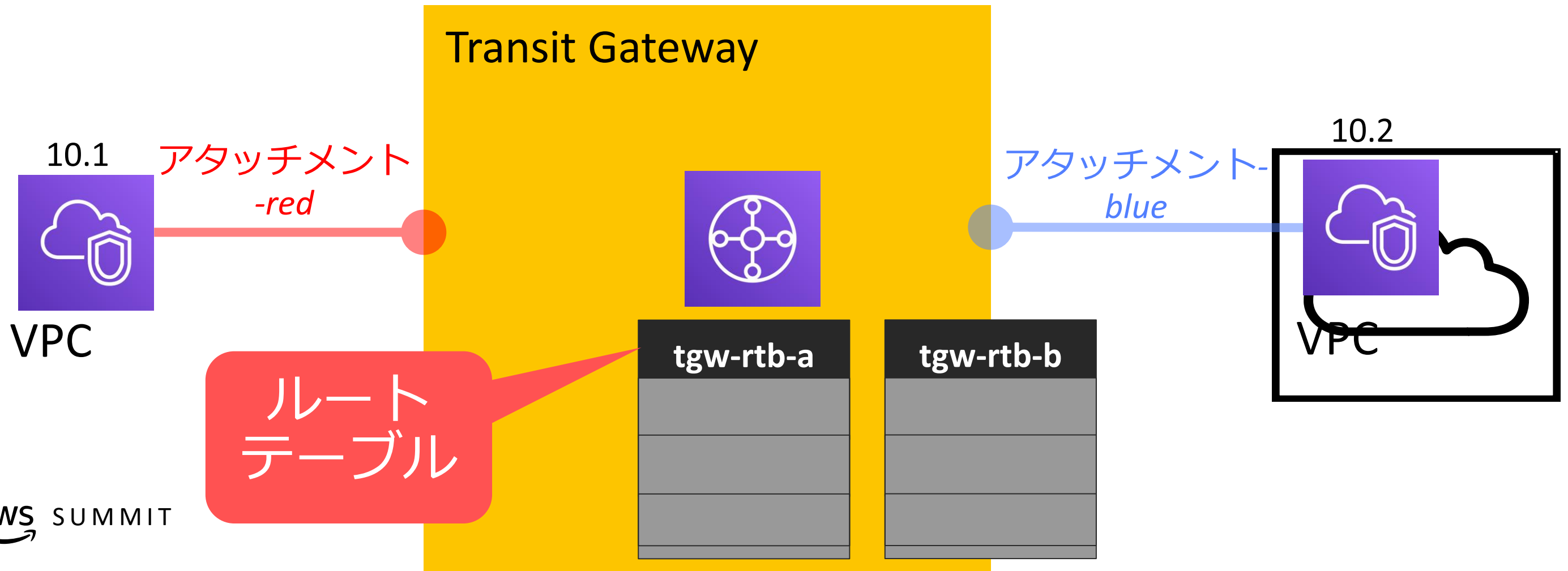
アタッチメント

- VPCやVPN,(Client VPN,Direct Connect)を Transit Gatewayにくっつけるアクション
- アタッチメントをすることによりVPCやVPN同士で通信できる準備ができる
 - アタッチメントだけでは通信ができない



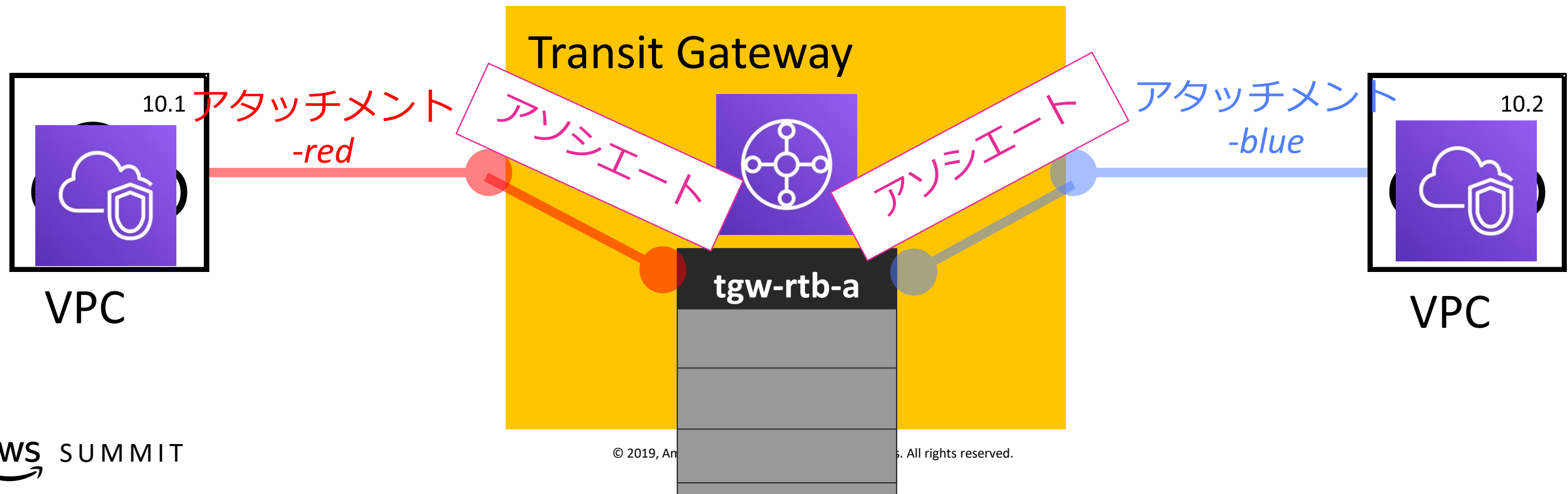
ルートテーブル

- Transit Gatewayが持つ経路情報テーブル
- デフォルトで1つ作られ、複数作ることができる



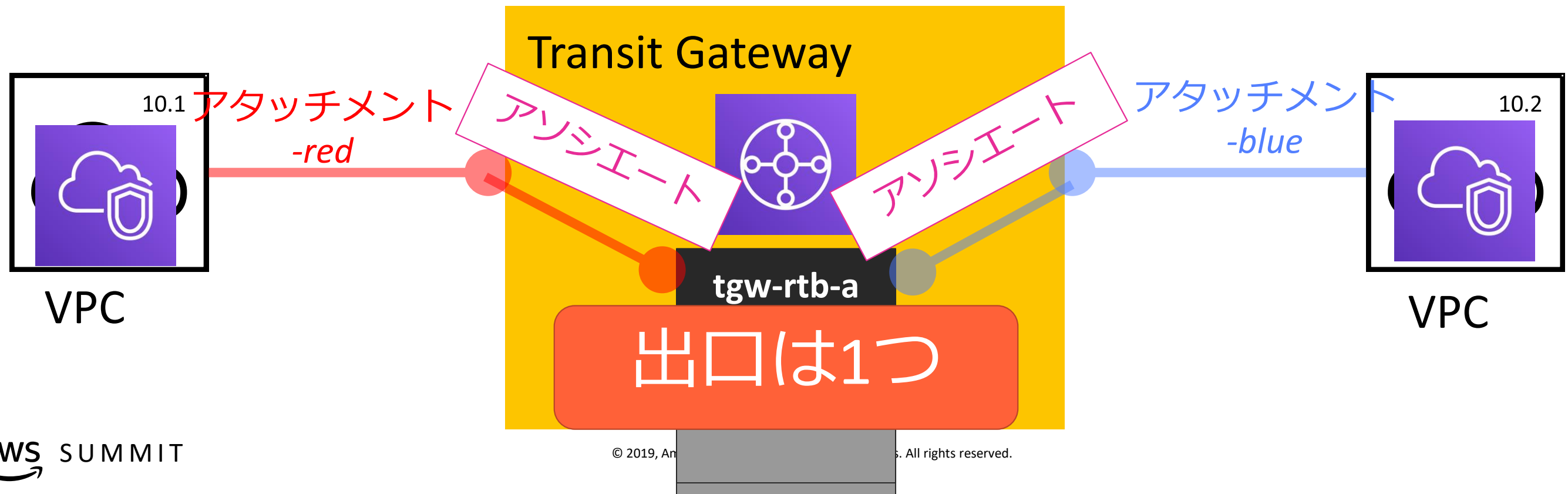
ルートテーブル：アソシエーション

- アタッチメントしたVPCなどをルートテーブルに結びつけること
- アソシエートしたルートテーブルにパケットが送信される
- アソシエーションは1つのルートテーブルにしか適用できない（重要）



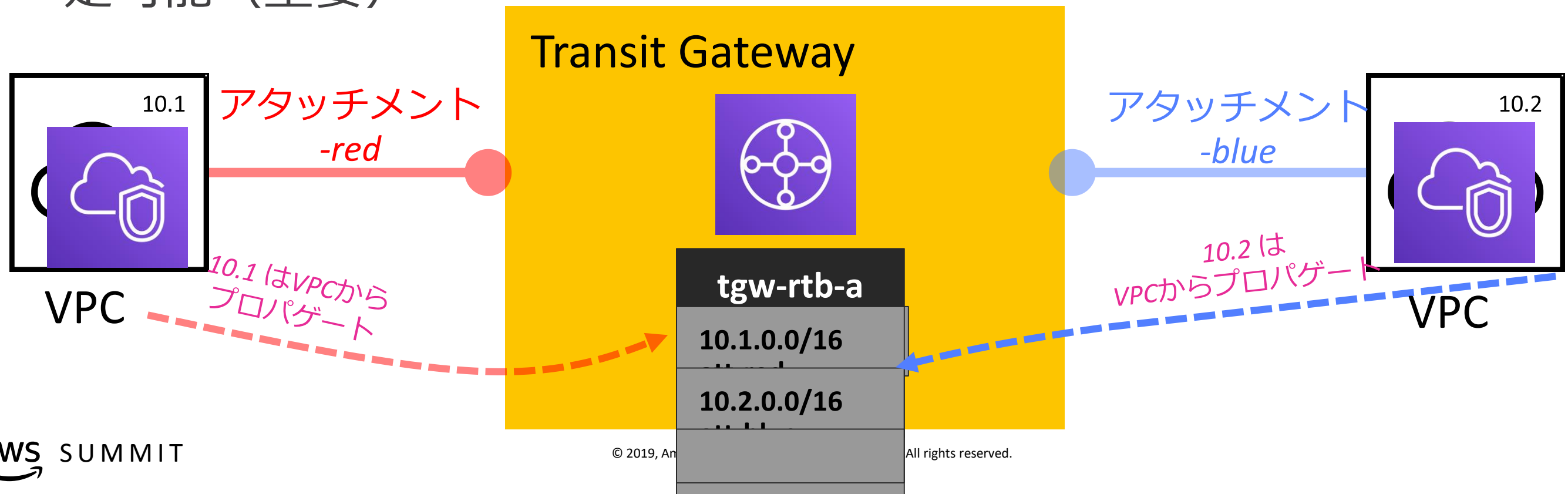
ルートテーブル：アソシエーション

- アタッチメントしたVPCなどをルートテーブルに結びつけること
- アソシエートしたルートテーブルにパケットが送信される
- アソシエーションは1つのルートテーブルにしか適用できない（重要）



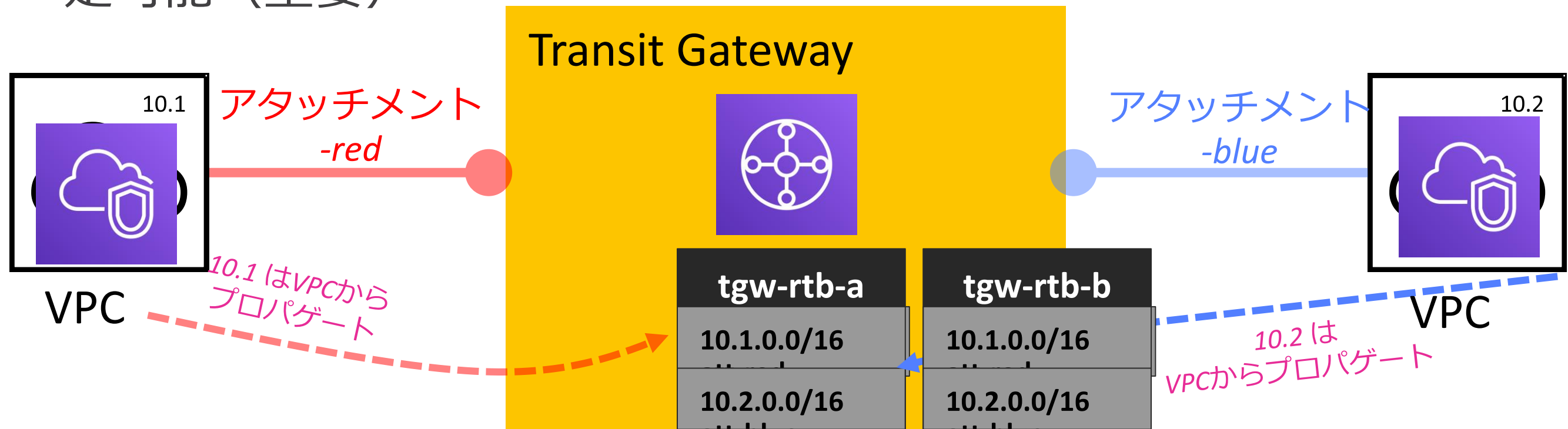
ルートテーブル：プロパゲーション

- アタッチメントしたVPCからルートテーブルに経路を伝播する
- ルートテーブルに伝播した経路が登録され、ルーティングの際に参照される
- プロパゲートはアソシエートに関係なく複数ルーティングテーブルに設定可能（重要）



ルートテーブル：プロパゲーション

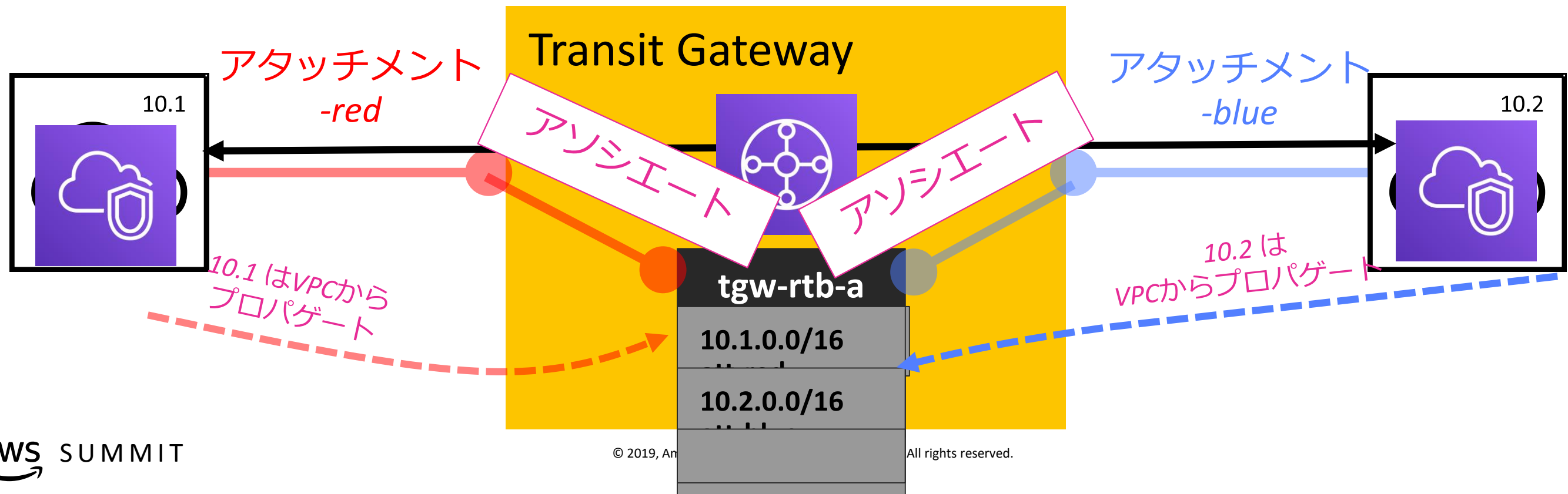
- アタッチメントしたVPCからルートテーブルに経路を伝播する
- ルートテーブルに伝播した経路が登録され、ルーティングの際に参照される
- プロパゲートはアソシエートに関係なく複数ルーティングテーブルに設定可能（重要）



複数のルートテーブルに伝播可能

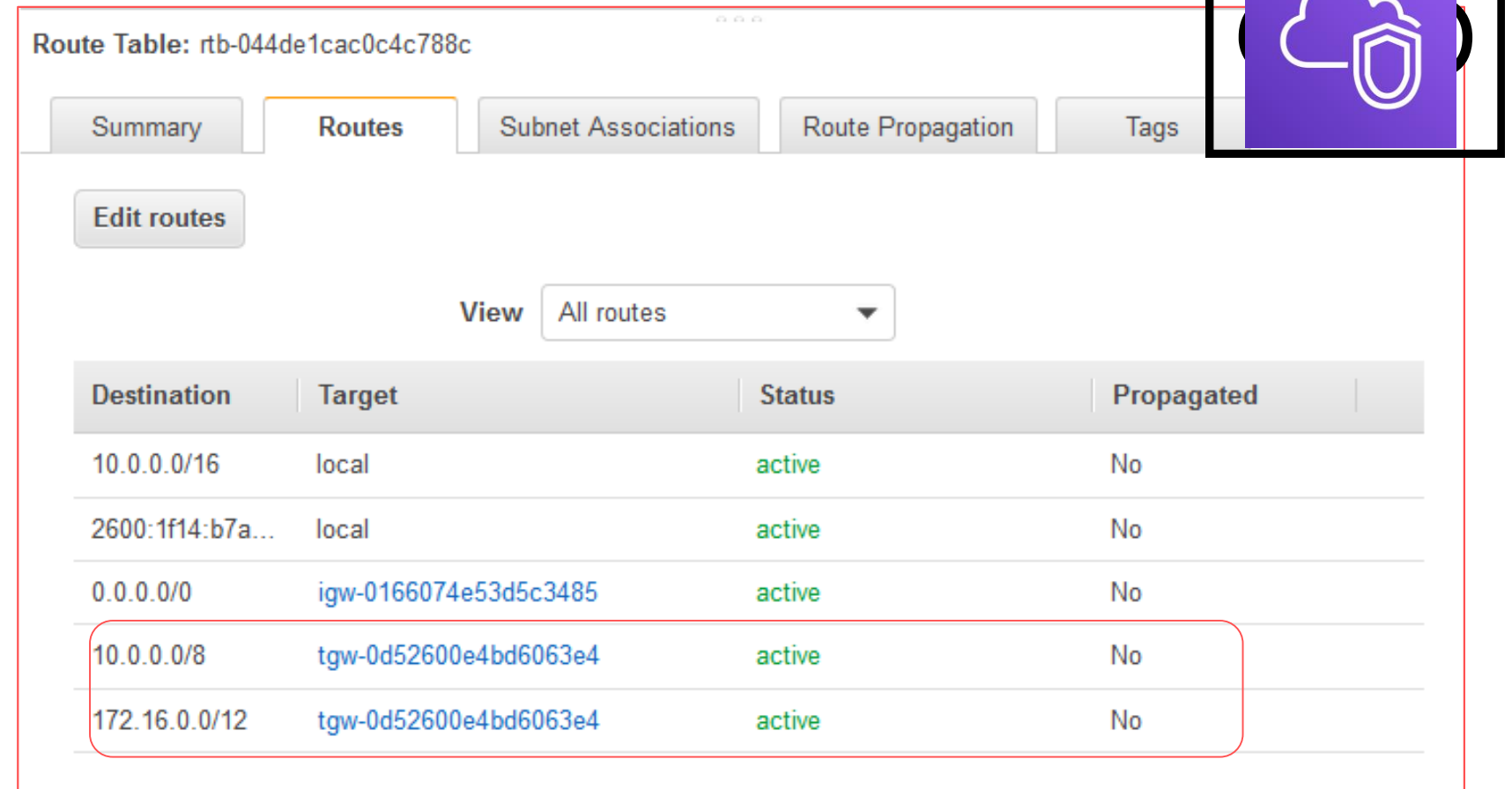
ルートテーブル：アソシエートとプロパゲーション

- アソシエートしたルートテーブルに相互のVPCからプロパゲートすることで経路表が完成し、双方のVPC間で通信ができるようになる。



重要: VPC、サブネット内のルートテーブル

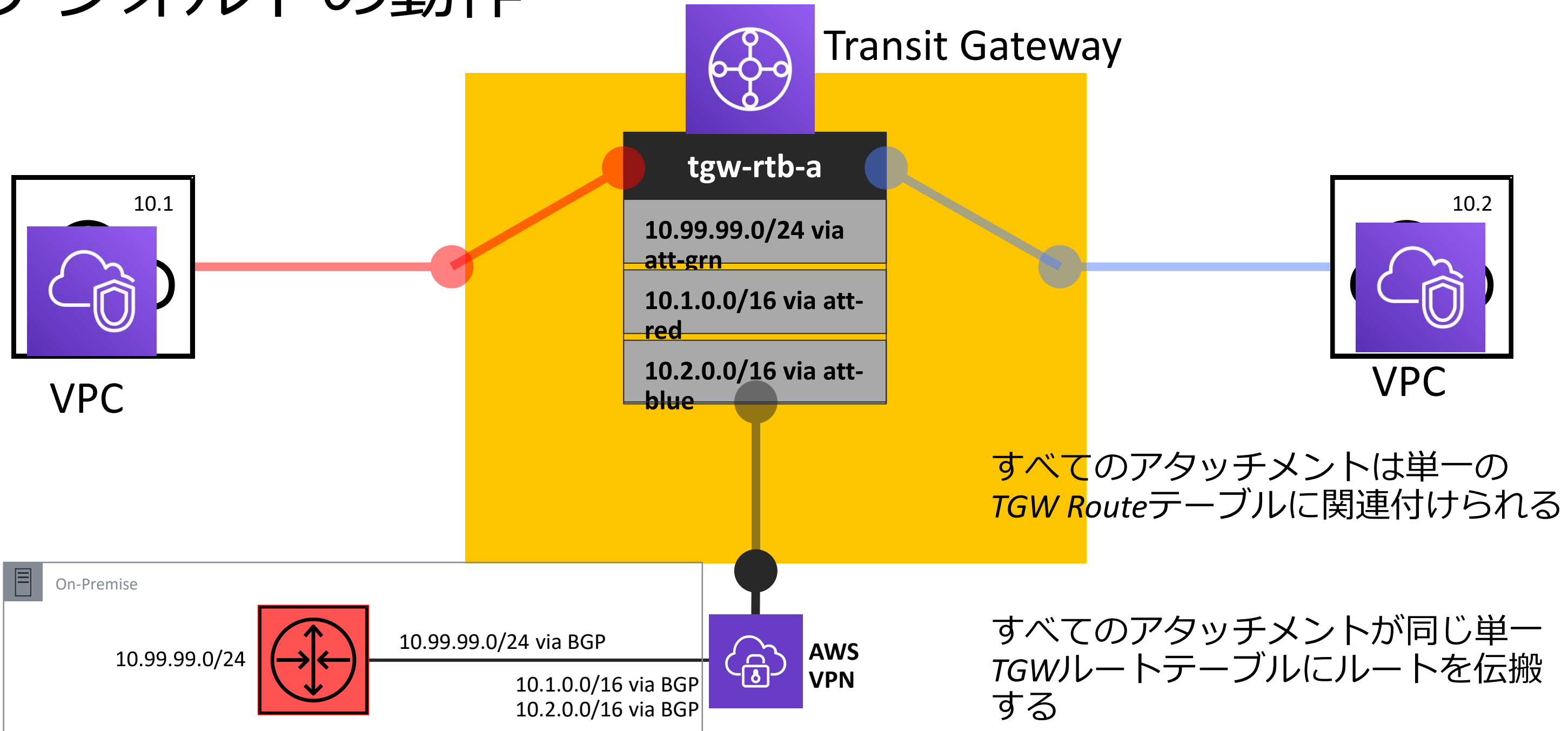
- VPC内でTGW向けのルートテーブルを書く必要がある。
- 自動でルート伝播はされない



The screenshot displays the AWS console interface for a Route Table (rtb-044de1cac0c4c788c). The 'Routes' tab is selected, showing a table of routes. A red box highlights the two routes that are manually configured to point to a Transit Gateway (tgw-0d52600e4bd6063e4). A purple icon with a cloud and shield, representing a Transit Gateway, is shown in the top right corner of the screenshot area.

Destination	Target	Status	Propagated
10.0.0.0/16	local	active	No
2600:1f14:b7a...	local	active	No
0.0.0.0/0	igw-0166074e53d5c3485	active	No
10.0.0.0/8	tgw-0d52600e4bd6063e4	active	No
172.16.0.0/12	tgw-0d52600e4bd6063e4	active	No

デフォルトの動作



アタッチメント - 'associated & propagated route table'

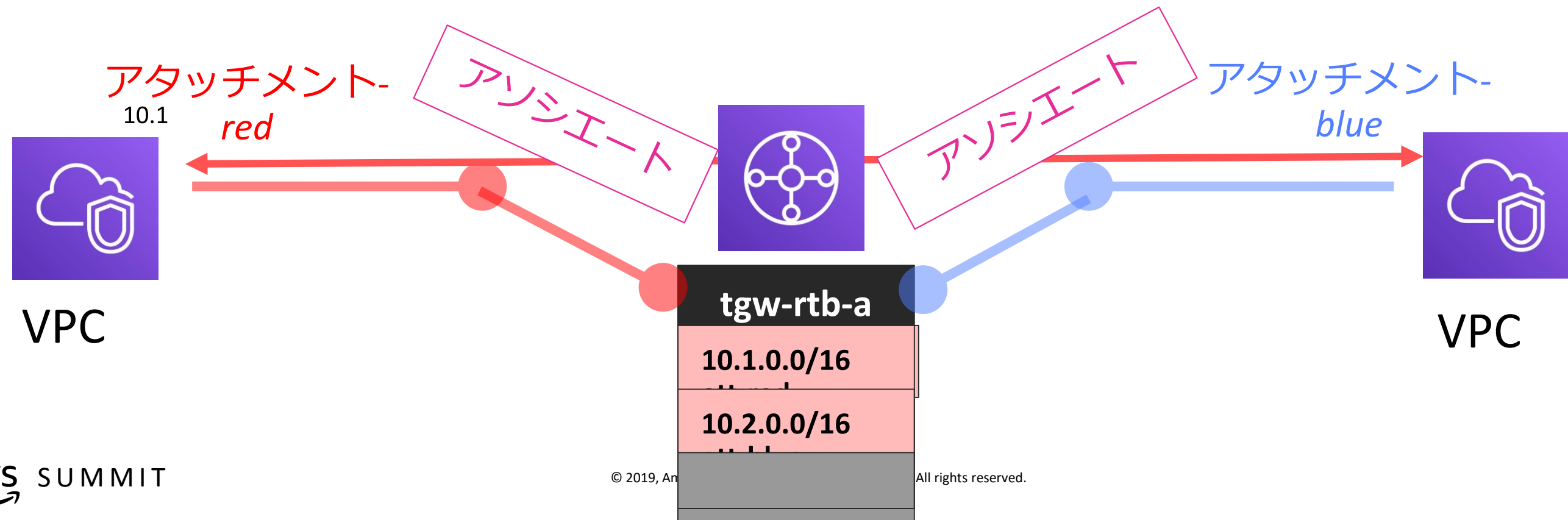
Transit Gateway: tgw-0174e65e24e6ed02e

Details Tags

Transit Gateway ID	tgw-0174e65e24e6ed02e	Owner account ID	[REDACTED]
State	available	Amazon ASN	64512
DNS support	enable	VPN ECMP support	enable
Auto accept shared attachments	disable	Default association route table	enable
Association route table ID	tgw-rtb-05c844b0ae308a214	Default propagation route table	enable
Propagation route table ID	tgw-rtb-05c844b0ae308a214		

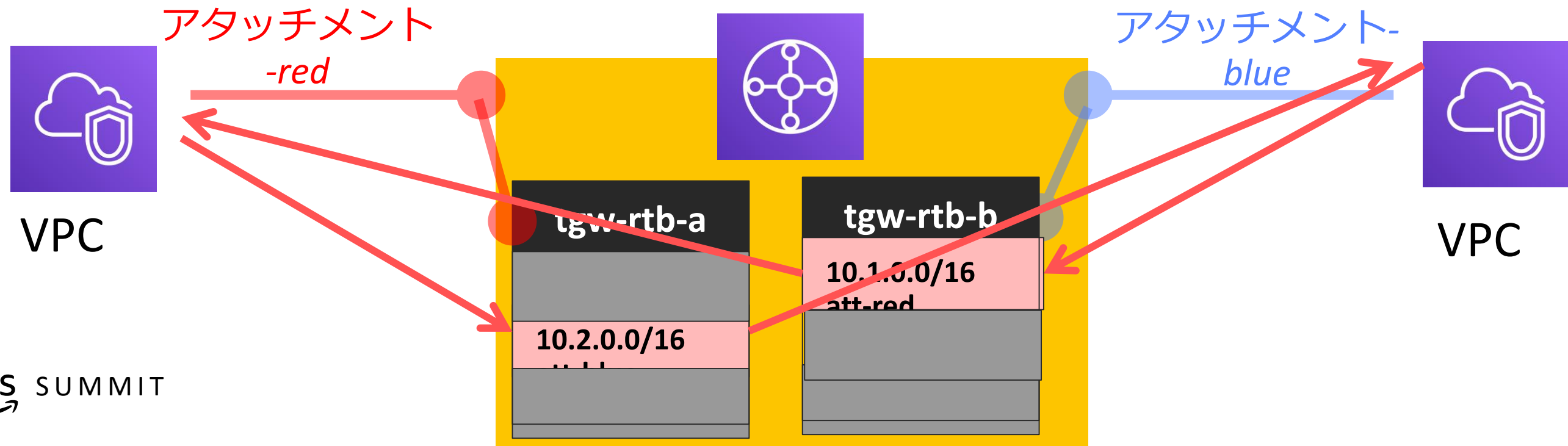
ルートテーブル：スタティックルート

- ルートテーブルにはスタティックルートを書くことができる。
- 書ける経路はNext HopのVPC/VPNでなくてもよい
 - デフォルトルートを書くことができる。
- アソシエートされていないVPC/VPNにもNext Hopを書くことができる。



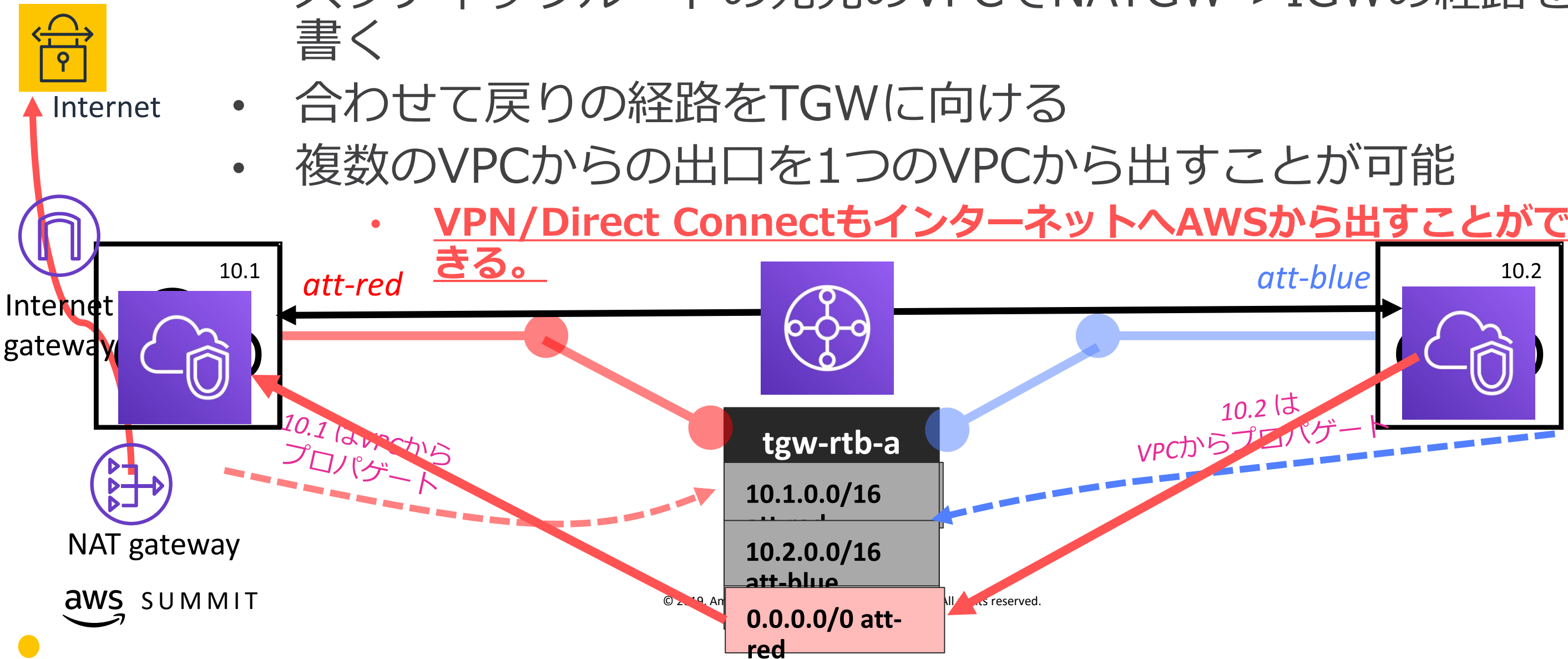
ルートテーブル：スタティックルート

- ルートテーブルにはスタティックルートを書くことができる。
- 書ける経路はNext HopのVPC/VPNでなくてもよい
 - デフォルトルートを書くことができる。
- アソシエートされていないVPC/VPNにもNext Hopを書くことができる。
- ブラックホールルートも書ける
- 経路情報さえあれば通る。



スタティックルートの応用：インターネット接続集約

- ルートテーブルにデフォルトルートをスタティックで書く
- スタティックルートの宛先のVPCでNATGW->IGWの経路を書く
- 合わせて戻りの経路をTGWに向ける
- 複数のVPCからの出口を1つのVPCから出すことが可能
- **VPN/Direct ConnectもインターネットへAWSから出すことができる。**



Agenda

Transit Gatewayとは

Transit Gatewayの用語と動作

ユースケース

注意するところ

新機能: Transit GatewayとDirect Connectの連携

まとめ

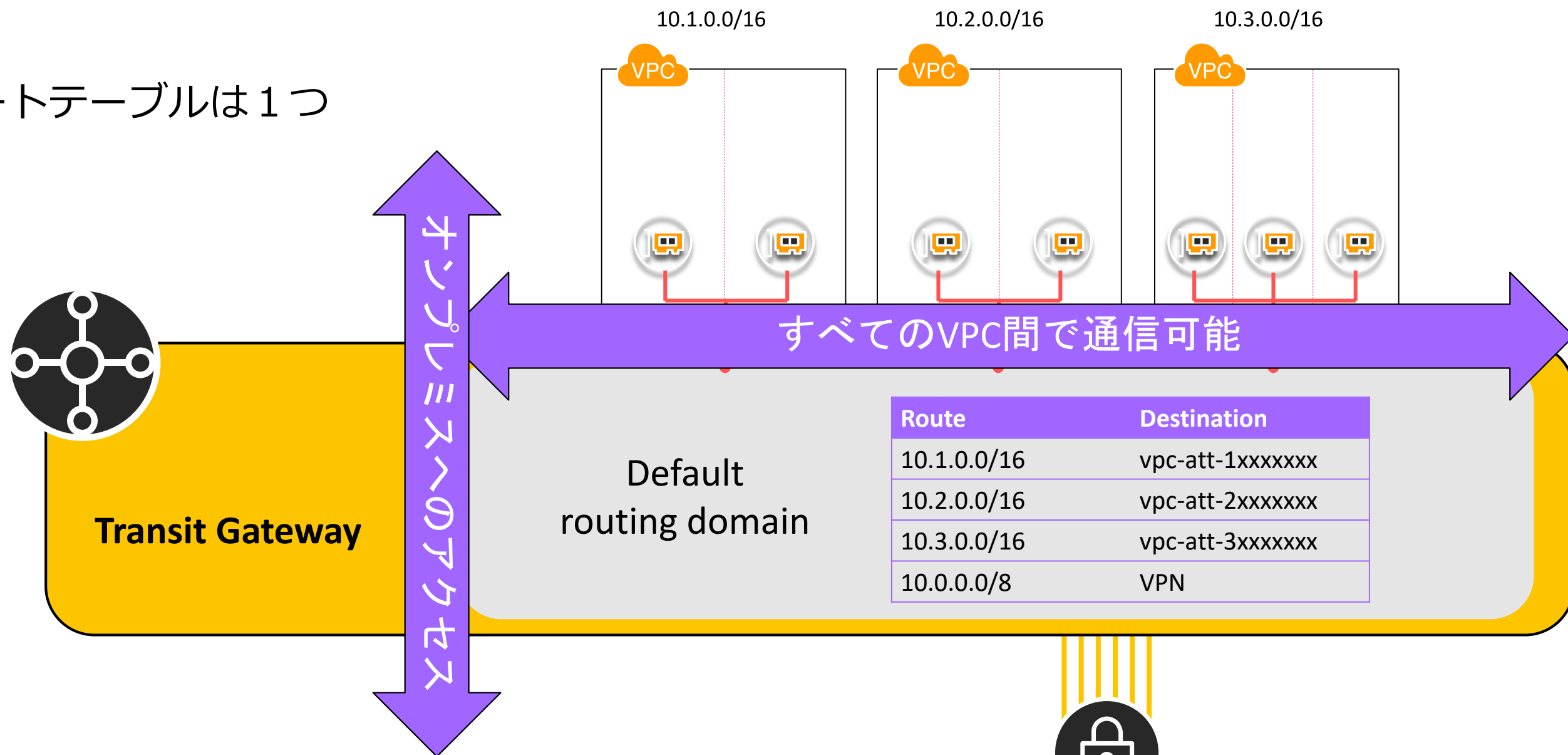
ユースケース

ユースケース

- 自由に通信できるRoute Domain
- VPC間の通信を制限するRoute Domain
- インターネットに自由に通信できるOutbound Route Domain
- VPC間のトラフィックをインライン監査するRoute Domains

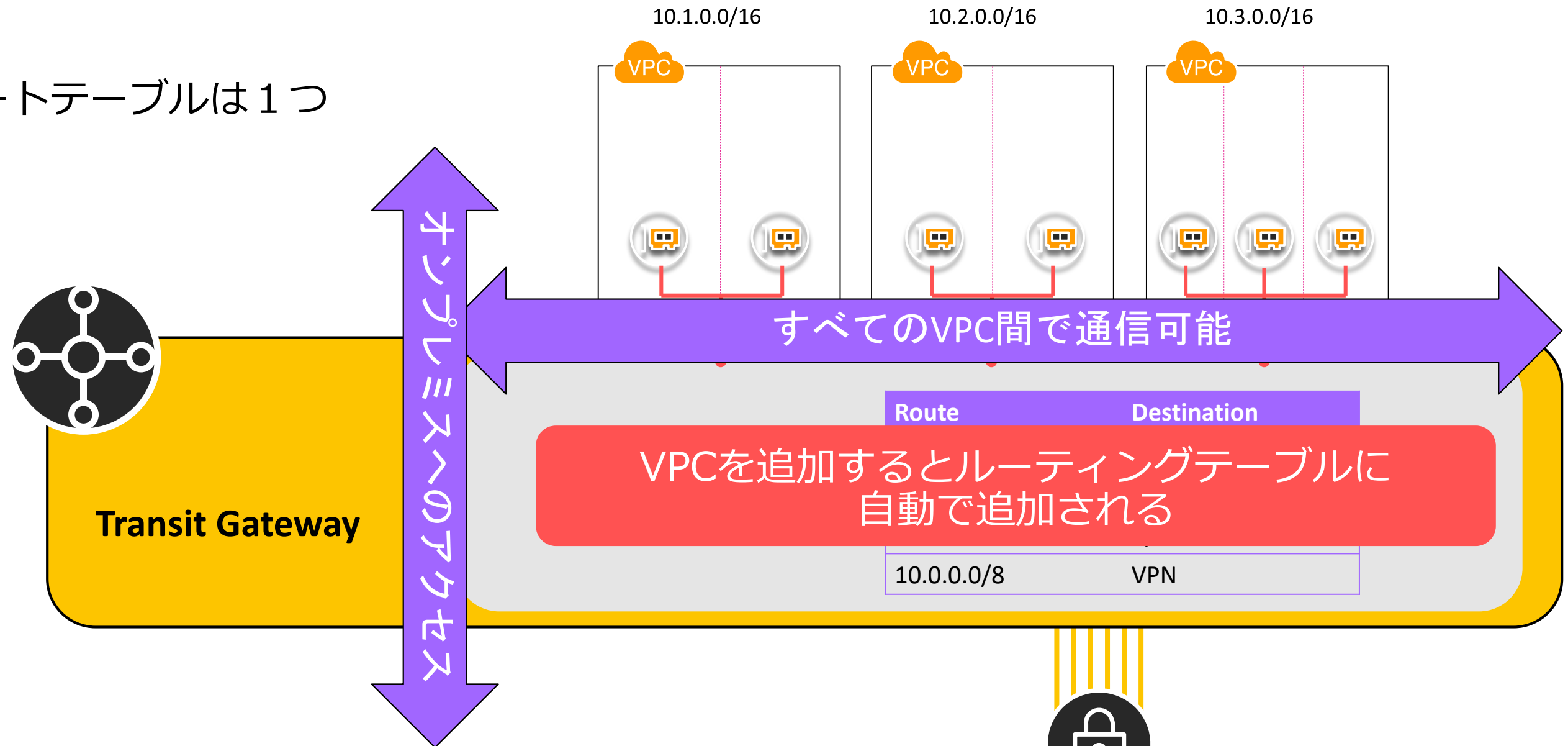
Transit Gatewayで自由に通信させる Route Domain

ルートテーブルは1つ



Transit Gatewayで自由に通信させる Route Domain

ルートテーブルは1つ



Transit Gatewayで通信制限する Route Domain

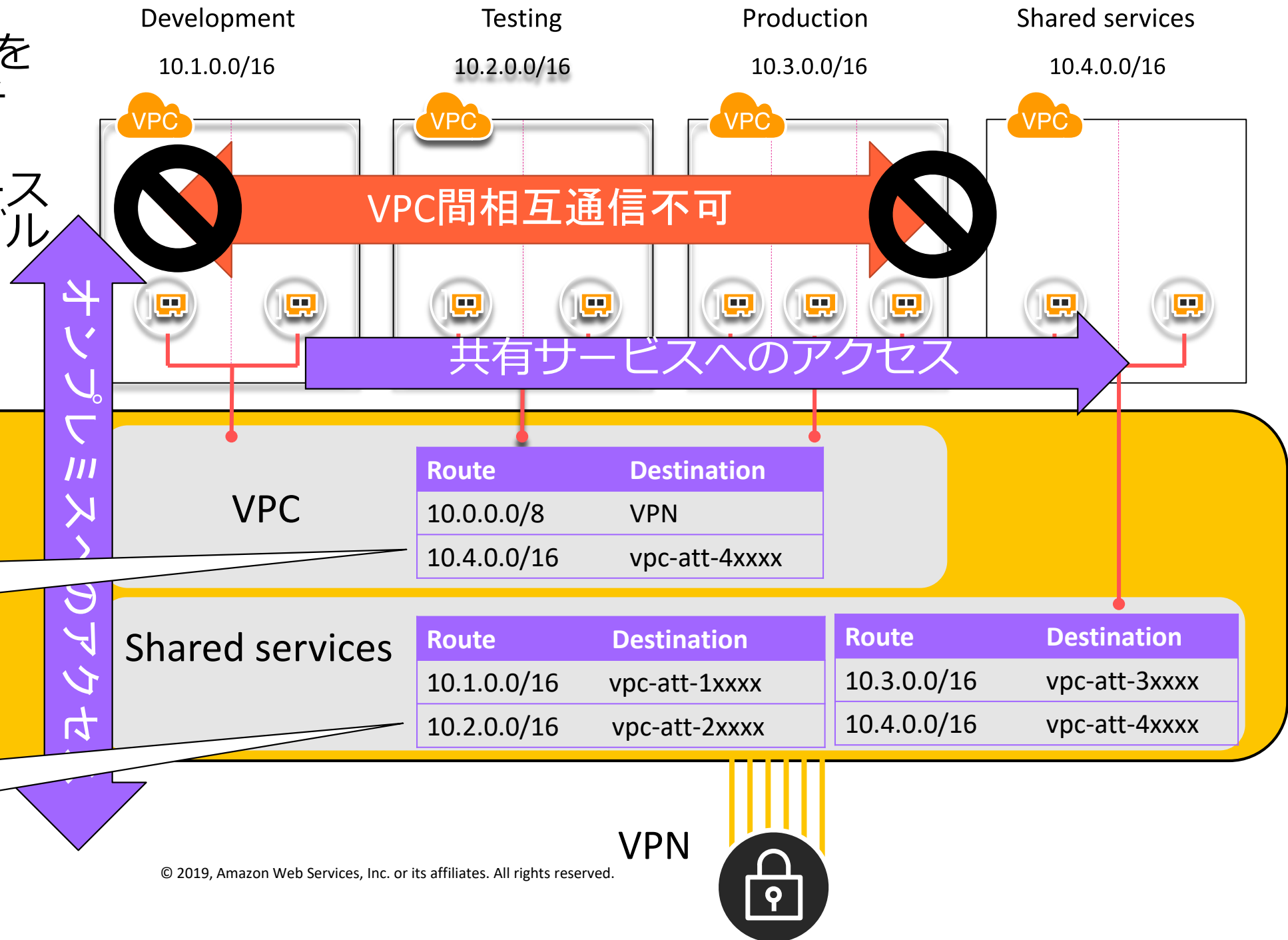
VPCは共有リソースへのルートを持つルートテーブルにアタッチ

共有リソースはすべてのリソースへのルートを持つルートテーブルにアタッチ

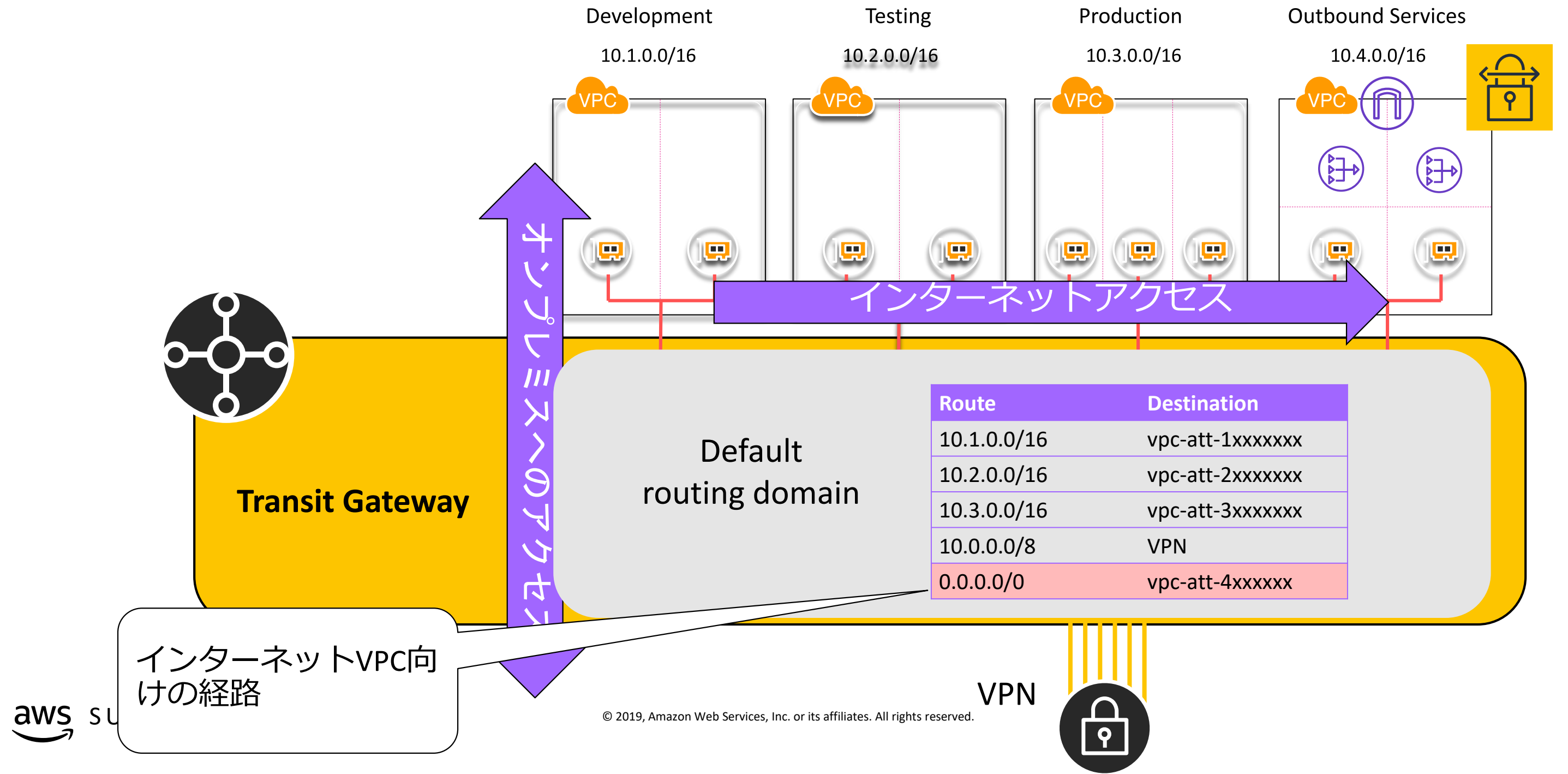


Shared serviceとVPN向けのみの経路

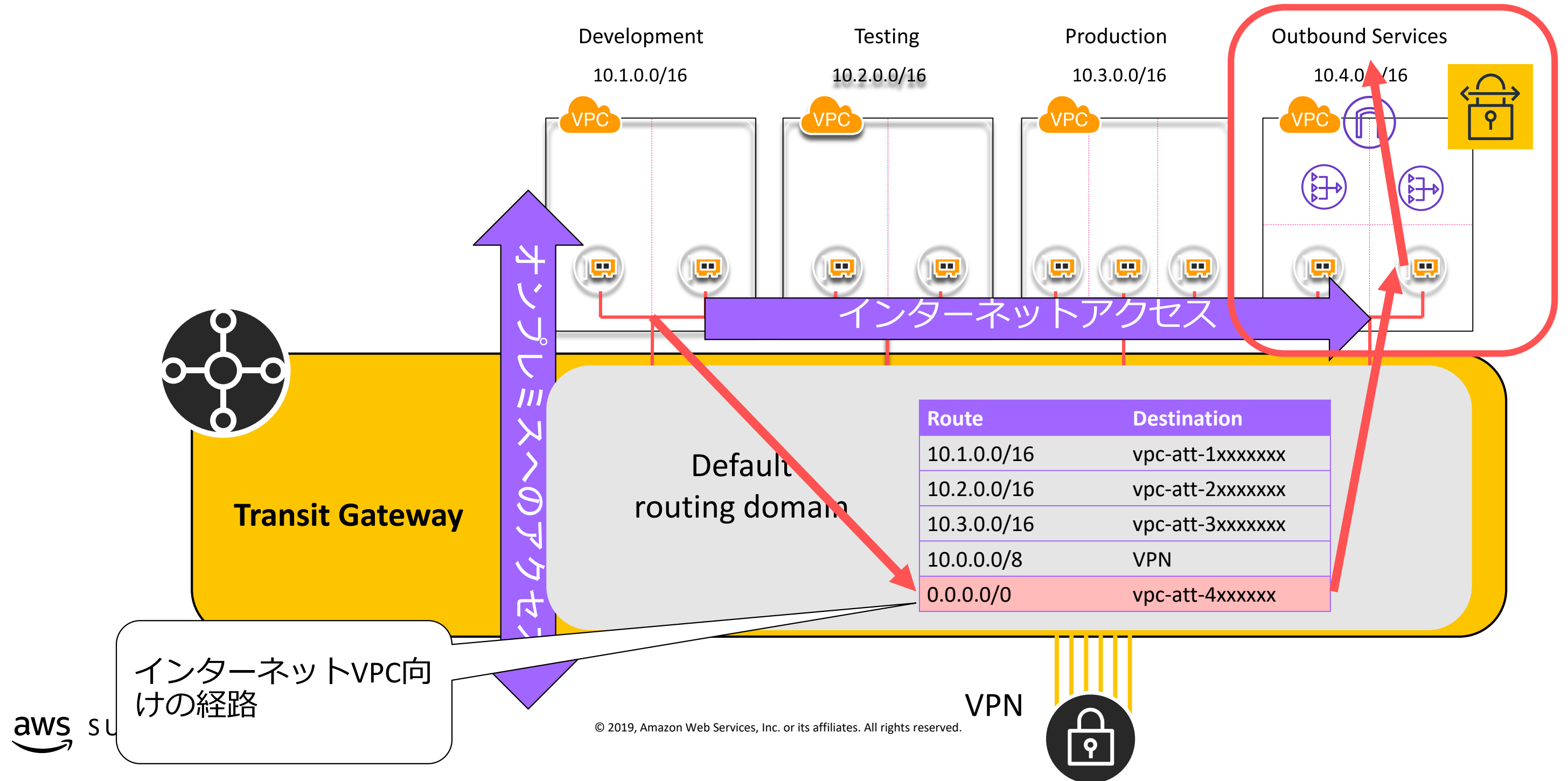
それぞれのVPC向けの経路



インターネットに抜けるOutbound Route Domain

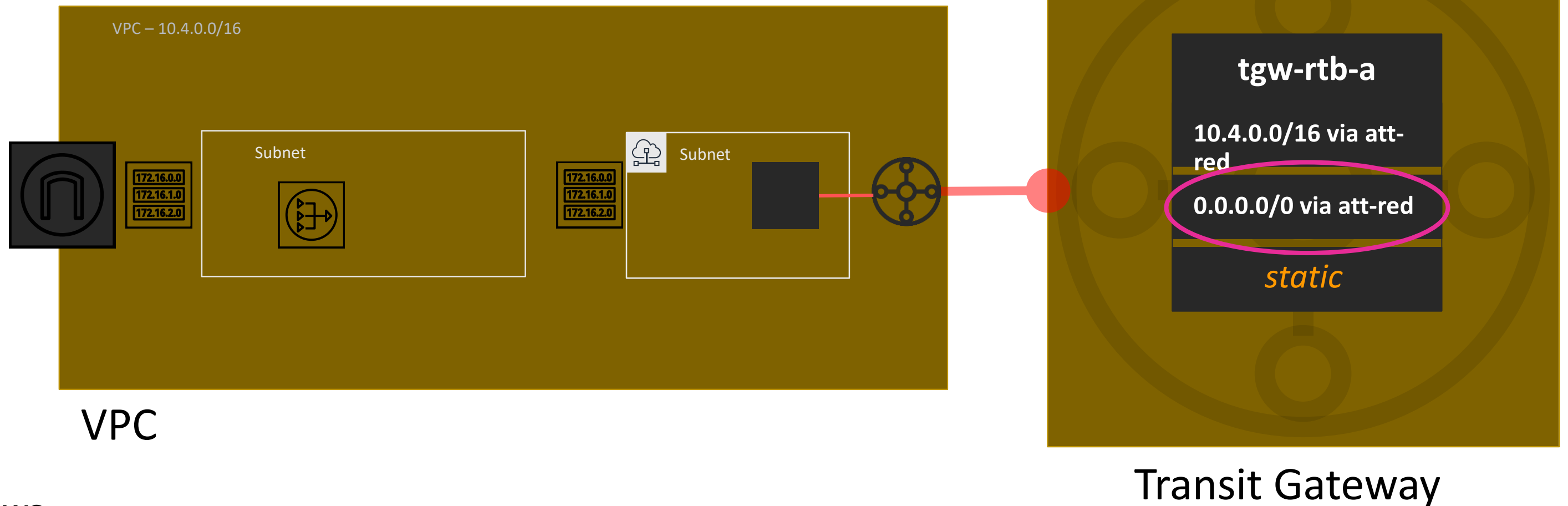


インターネットに抜けるOutbound Route Domain

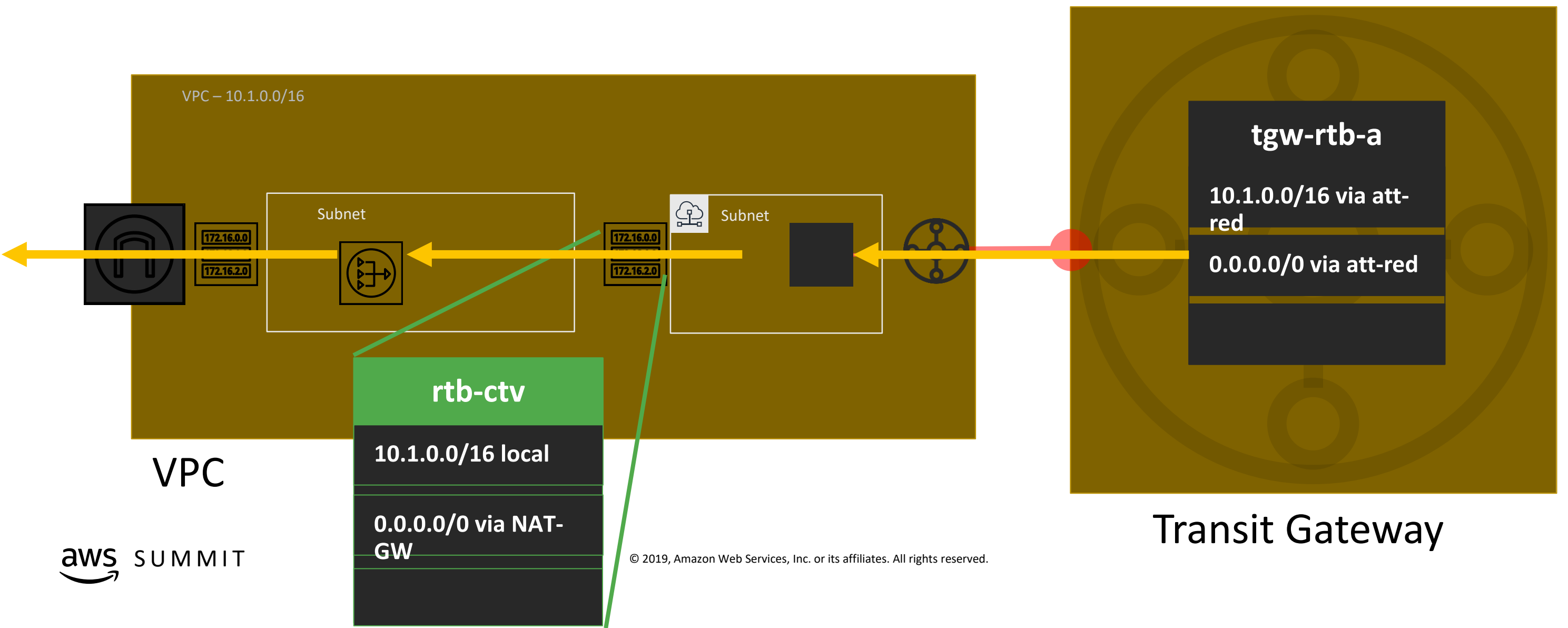


Outbound Services VPC詳細

Connectivity Route TableでNATゲートウェイのターゲットを指定してインターネットに出て行くには？

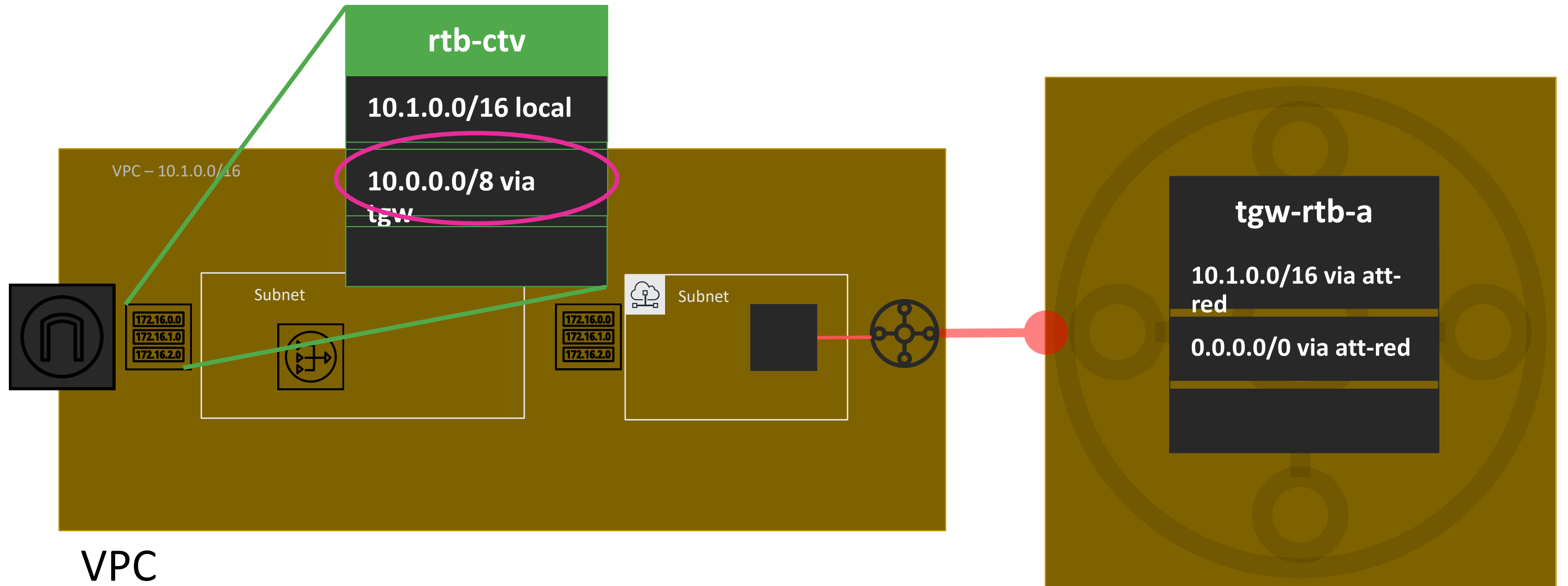


Outbound Services VPC詳細



Outbound Services VPC詳細

戻りの経路を書く

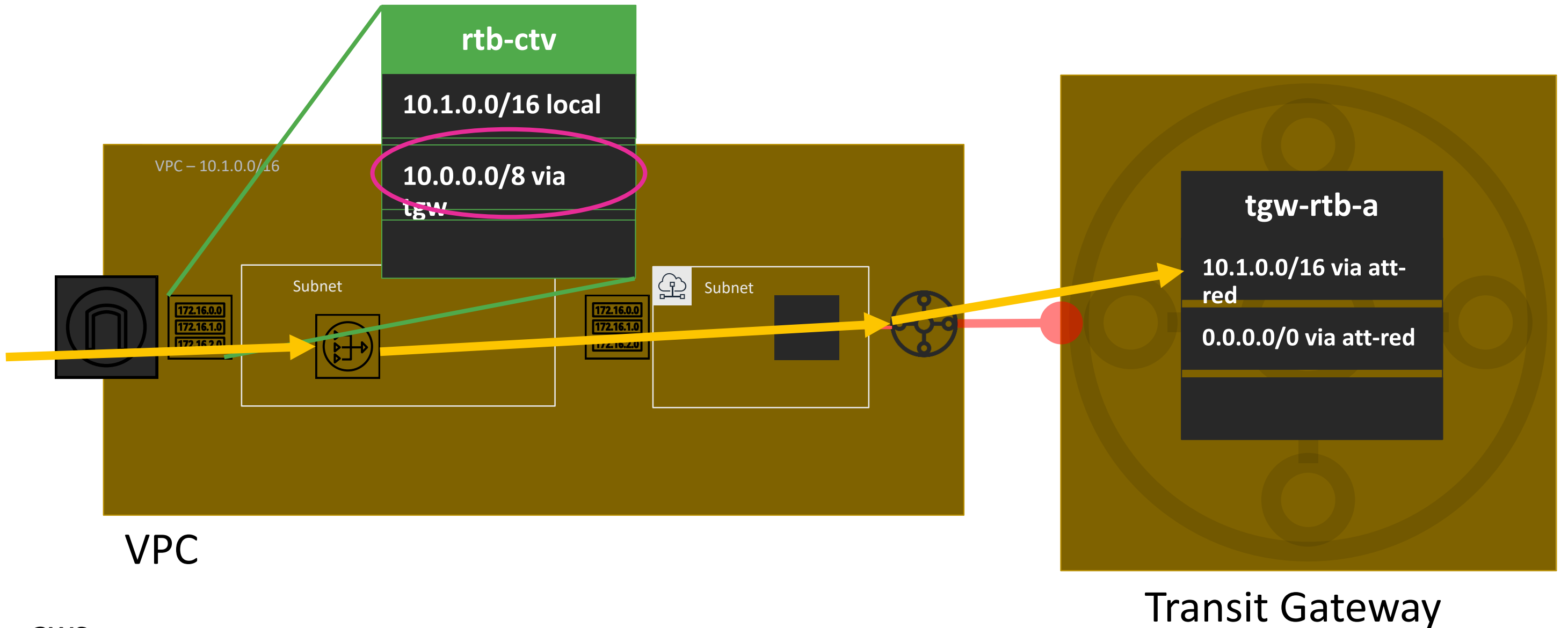


VPC

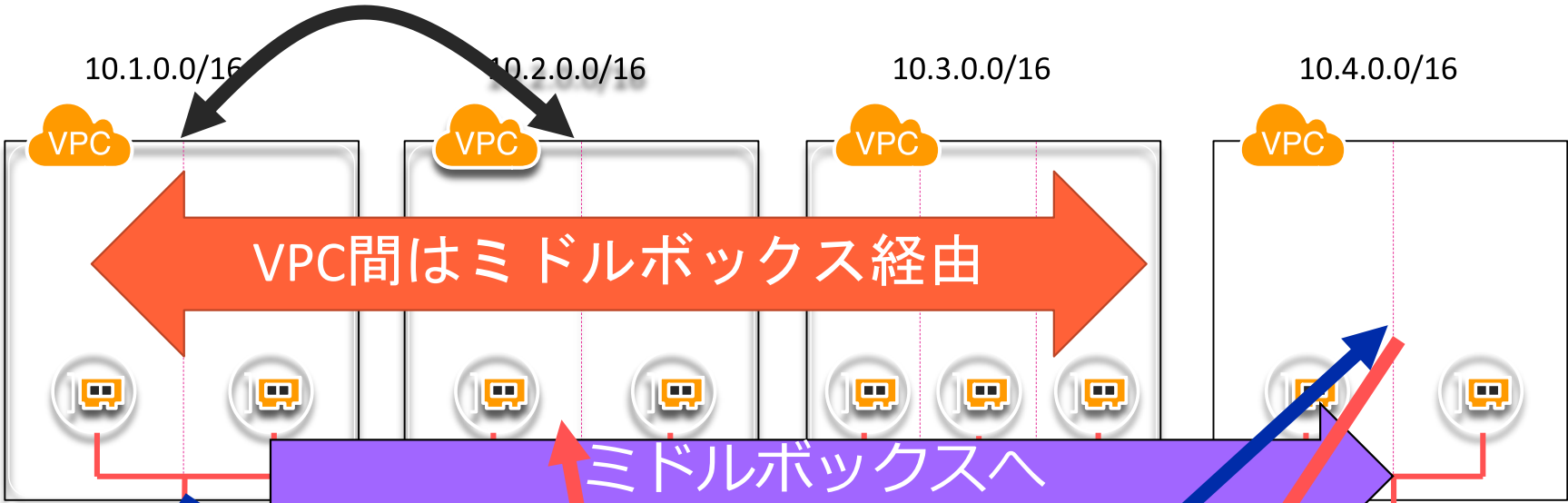
Transit Gateway

Outbound Services VPC詳細

戻りの経路を書く



VPC間のトラフィックをインライン監査するRoute Domains



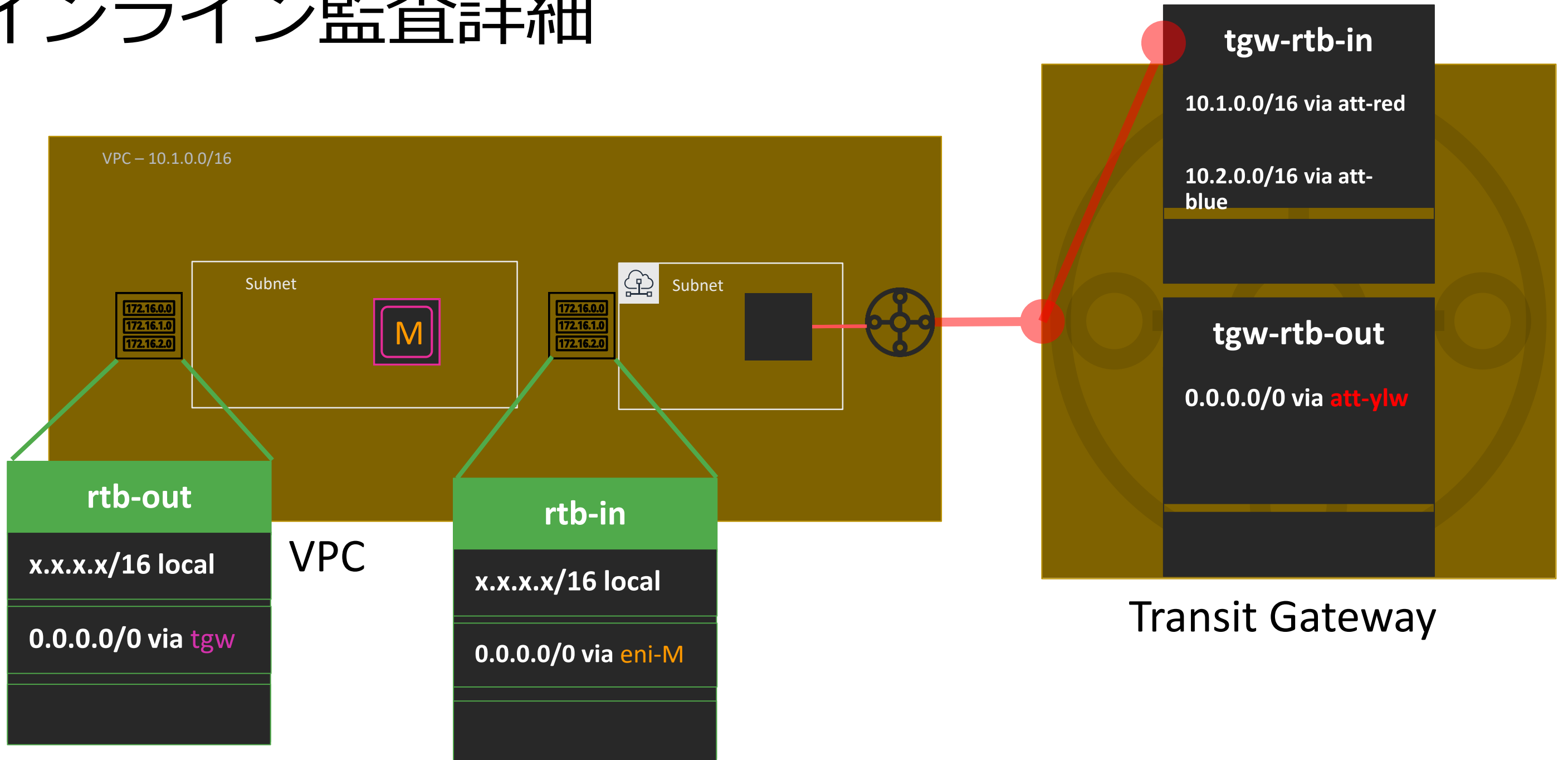
インライン監査向けの経路

それぞれのVPC向けの経路

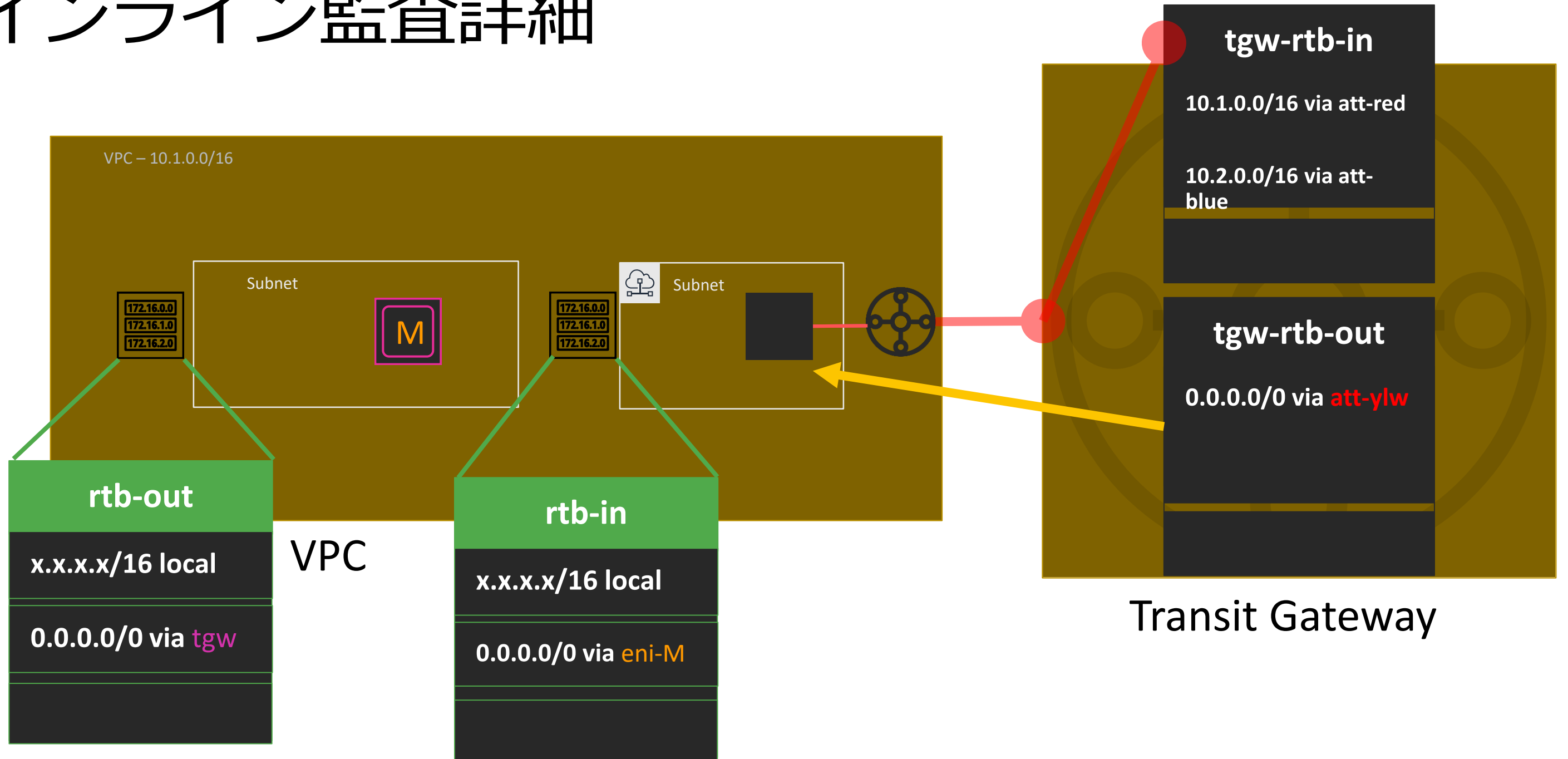
Gateway

To MiddleBox		VPC	
Route	Destination	Route	Destination
0.0.0.0/0	vpc-att-4xxxx	10.1.0.0/16	vpc-att-1xxxx
		10.2.0.0/16	vpc-att-2xxxx
		10.3.0.0/16	vpc-att-3xxxx
		10.4.0.0/16	vpc-att-4xxxx

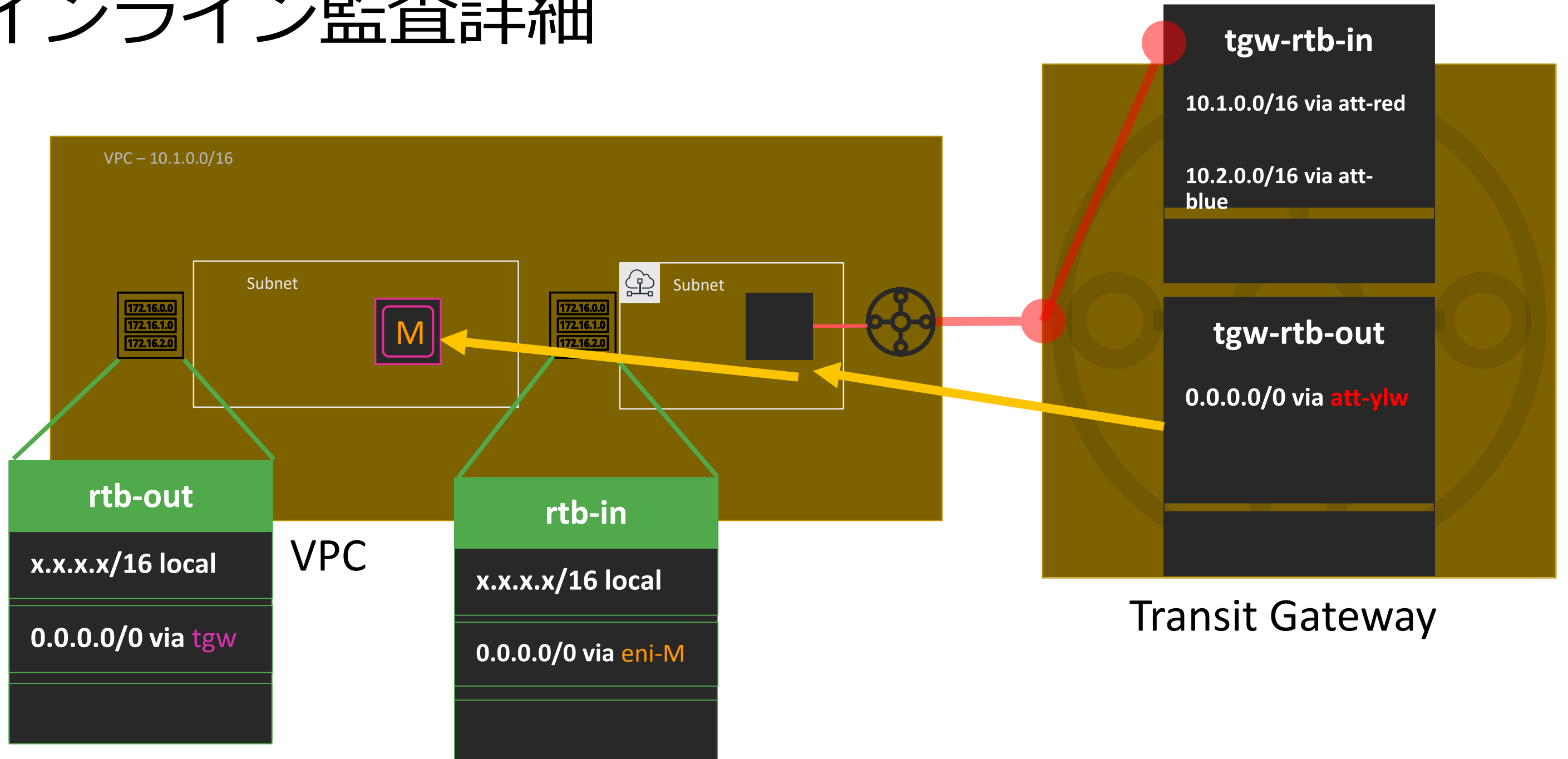
インライン監査詳細



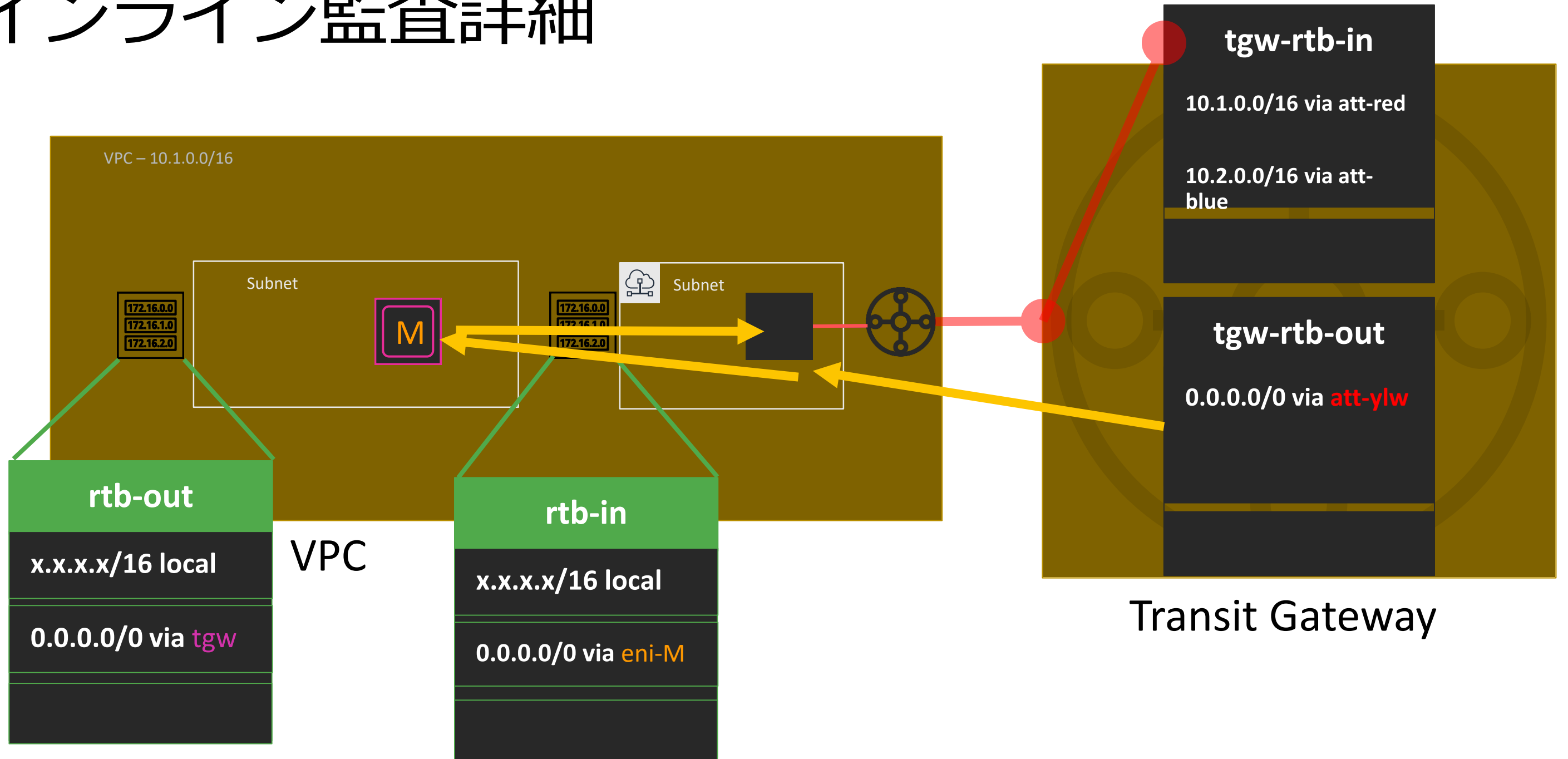
インライン監査詳細



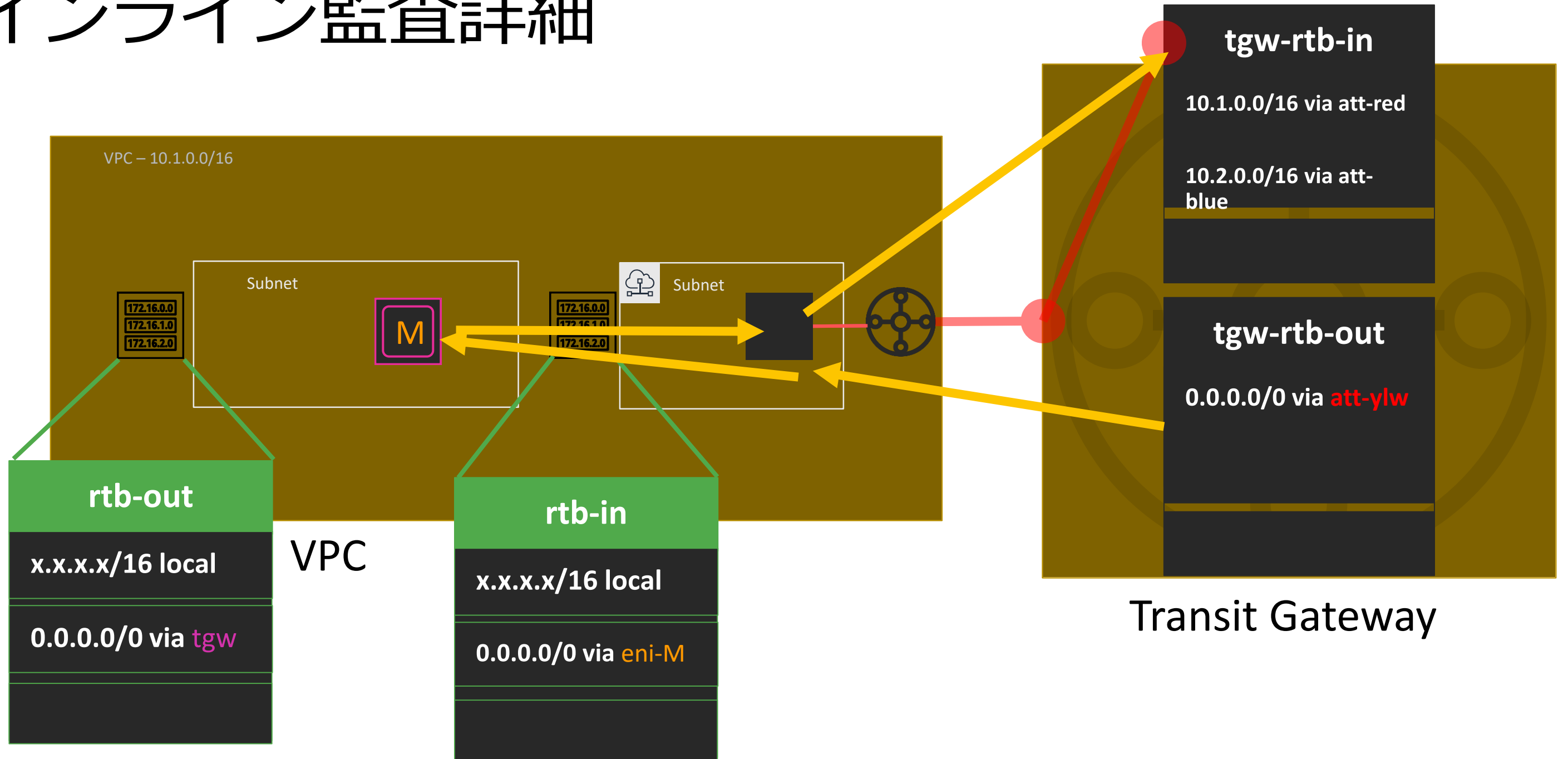
インライン監査詳細



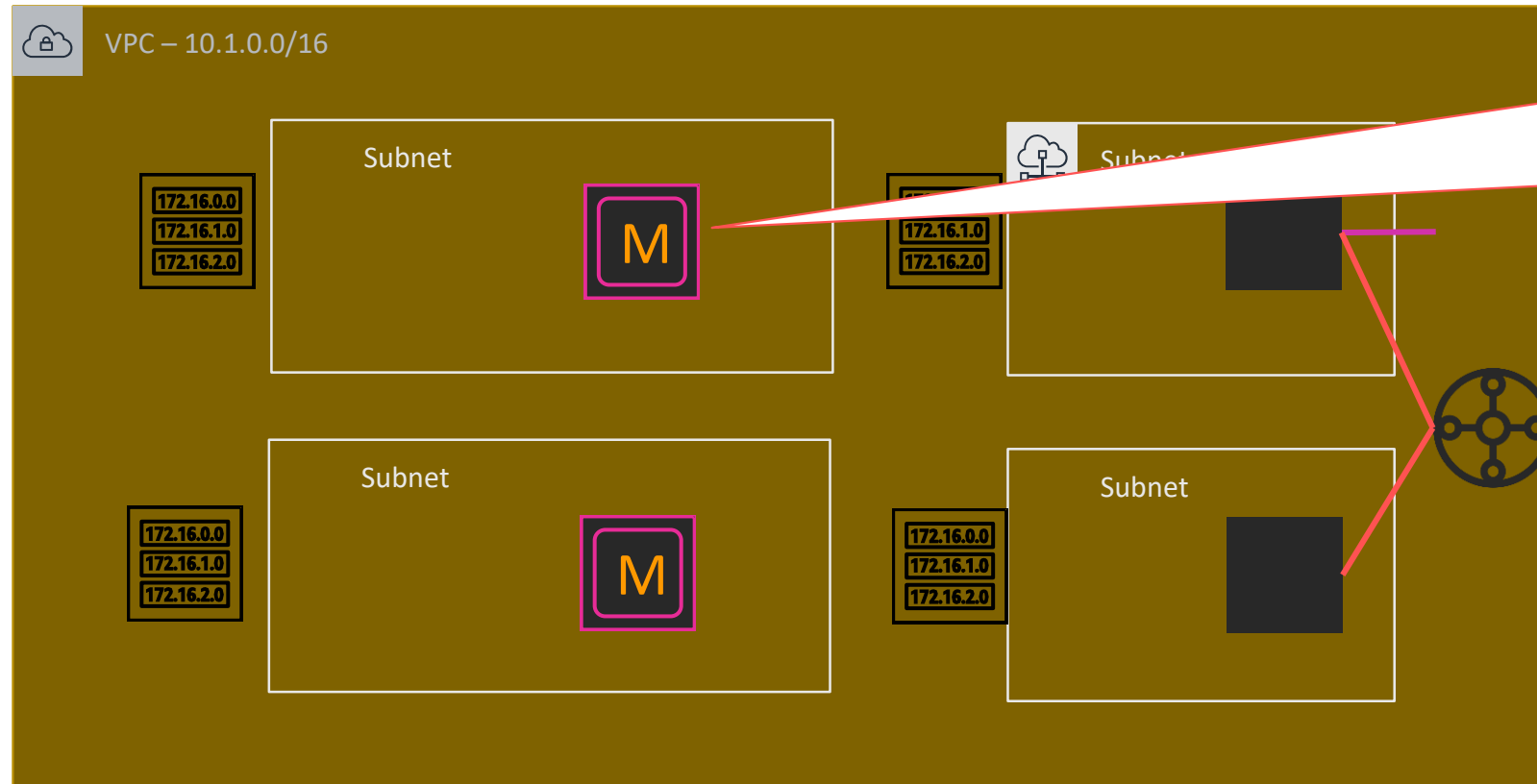
インライン監査詳細



インライン監査詳細



インスタンスの冗長



監査を行うインスタンスに対する
監視が必要

- 監査用のインスタンスを監視する仕組みが必要
- NATインスタンスの時と同様にルーティングテーブルをいじる
Lambdaなどを作って監視する

Agenda

Transit Gatewayとは

Transit Gatewayの用語と動作

ユースケース

注意するところ

新機能: Transit GatewayとDirect Connectの連携

まとめ

注意するところ

Transit Gateway作成時の注意

A Transit Gateway (TGW) is a network transit hub that interconnects attachments (VPCs and VPNs) within the same account or across accounts.

Name tag demo ⓘ

Description demo TGW ⓘ

Configure the Transit Gateway

Amazon side ASN 64512 ⓘ

DNS support enable ⓘ

VPN ECMP support enable ⓘ

Default route table association enable ⓘ

Default route table propagation enable ⓘ

Default Routeアソシエーションとプロパゲーションがデフォルト enable, 経路を自在に制御したいときにはチェックを外す。
作成した後は変更できない。

A Transit Gateway (TGW) is a network transit hub that interconnects attachments (VPCs and VPNs) within the same account or across accounts.

Name ⓘ

Description demo TGW ⓘ

Configure the Transit Gateway

Amazon side ASN 64512 ⓘ

DNS support enable ⓘ

VPN ECMP support enable ⓘ

Default route table association enable ⓘ

Default route table propagation enable ⓘ

トラフィックを曲げたいときは両方チェックを外して作成する。

Agenda

Transit Gatewayとは

Transit Gatewayの用語と動作

ユースケース

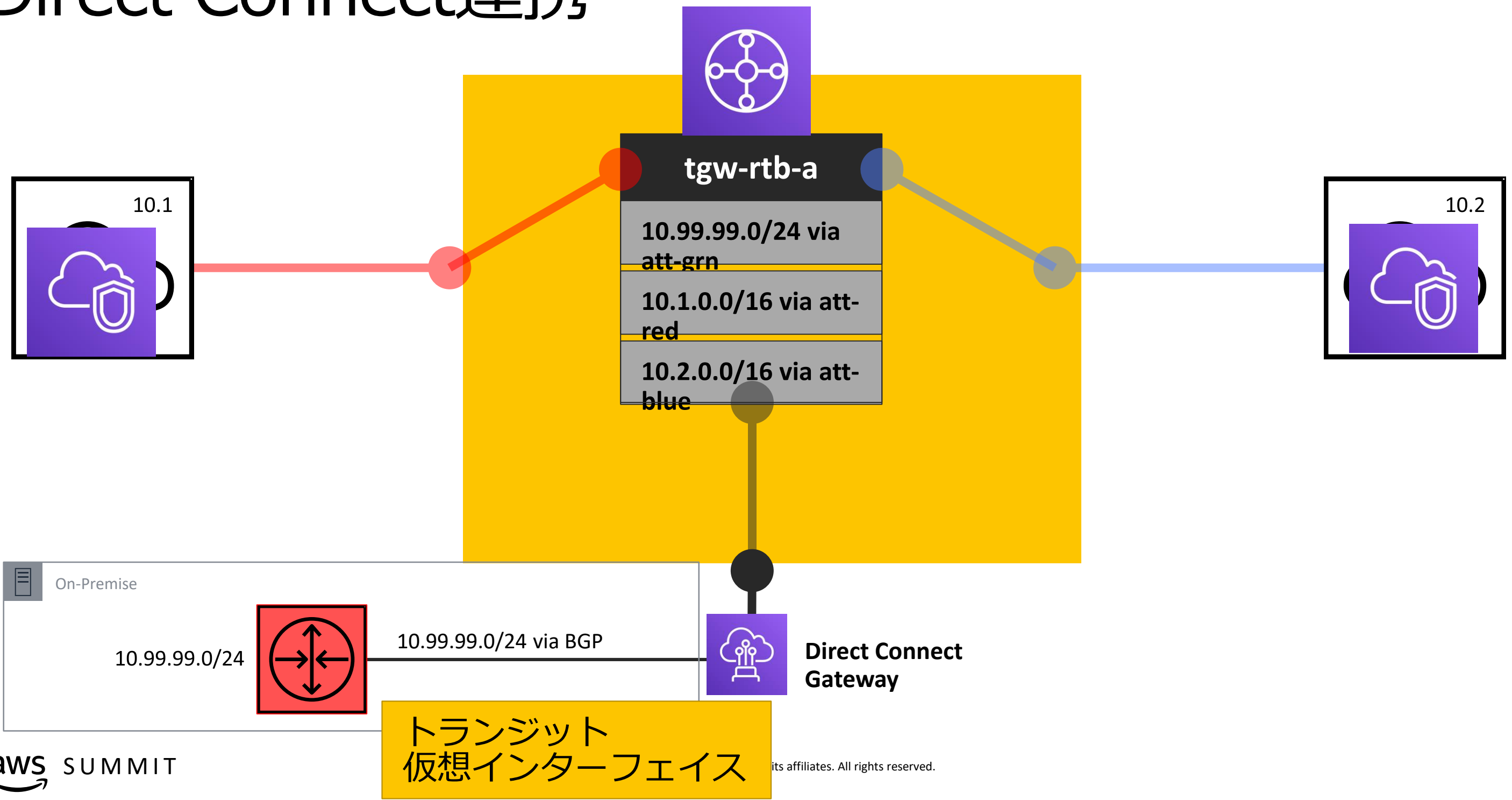
注意するところ

新機能: Transit GatewayとDirect Connectの連携

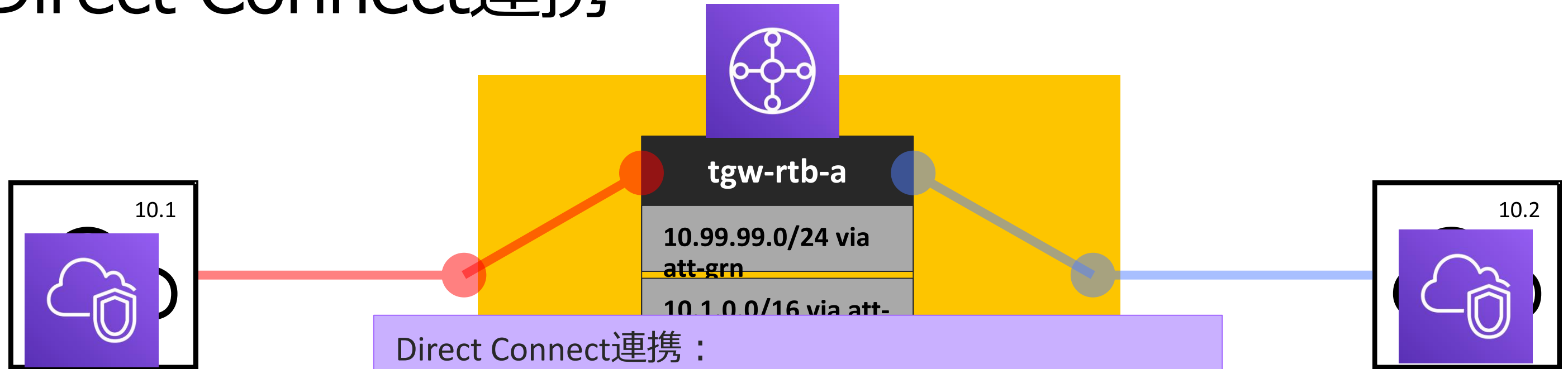
まとめ

新機能: Transit Gatewayと Direct Connectの連携

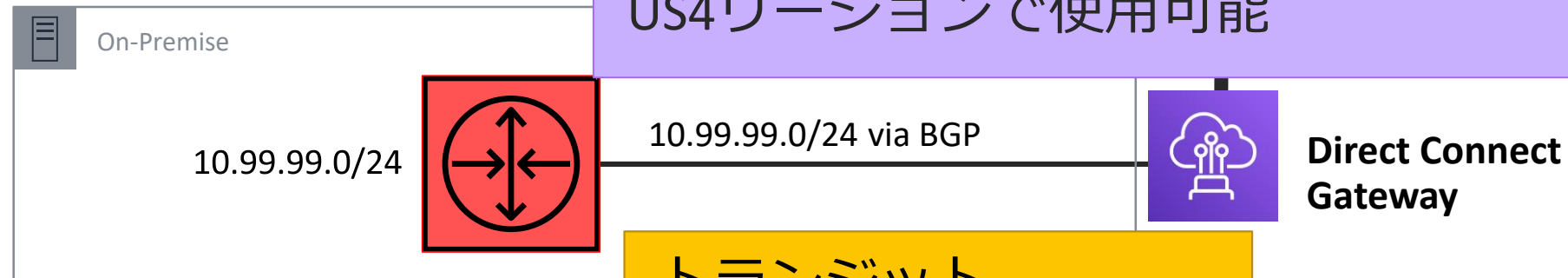
Direct Connect連携



Direct Connect連携



Direct Connect連携：
Direct Connect Gatewayを介して接続
トランジット仮想インターフェイス(Transit VIF)と
いう専用の仮想インターフェイスを使う
US4リージョンで使用可能



トランジット
仮想インターフェイス

Agenda

Transit Gatewayとは

Transit Gatewayの用語と動作

ユースケース

注意するところ

新機能: Transit GatewayとDirect Connectの連携

まとめ

まとめ

まとめ

Transit Gateway用語を理解する

Transit Gatewayで経路制御ができる

Transit Gatewayのユースケースを理解する

より深く学習したい方は

- [NEW LAUNCH!] AWS Transit Gateway and Transit VPCs - Reference Architectures for Many VPCs (NET402) - AWS re:Invent 2018
 - <https://www.slideshare.net/AmazonWebServices/new-launch-aws-transit-gateway-and-transit-vpcs-reference-architectures-for-many-vpcs-net402-aws-reinvent-2018>
 - <https://www.youtube.com/watch?v=ar6sLmJ45xs>
- [NEW LAUNCH!] Introducing AWS Transit Gateway (NET331) - AWS re:Invent 2018
 - <https://www.slideshare.net/AmazonWebServices/new-launch-introducing-aws-transit-gateway-net331-aws-reinvent-2018>
 - <https://www.youtube.com/watch?v=yQGxPEGt-w>
- Introduction to AWS Transit Gateway - AWS Online Tech Talks
 - <https://www.youtube.com/watch?v=6fhwoAwYrug>

Thank you!

Yukihiro Kikuchi
kyukihi@amazon.co.jp

本セッションのFeedbackをお願いします

お手元のサミットガイドブックの表紙、受講票にも記載している『QRコード』からご回答ください。

もれなく**素敵なAWSオリジナルグッズ&アイス**をプレゼントします。

涼感マフラータオル（巾着入り）



プレゼントの引き換えは、EXPOエリア内アンケートコーナー・出口付近のいずれかにお越しください。