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.

aws SUMMIT

# 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

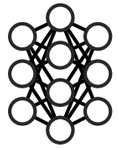
新機能: Transit GatewayとDirect Connectの連携

まとめ

# Transit Gatewayとは

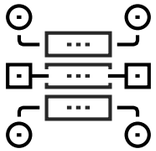
aws SUMMIT

# AWS Transit Gateway



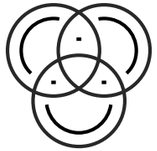
## リージョナルゲートウェイ

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

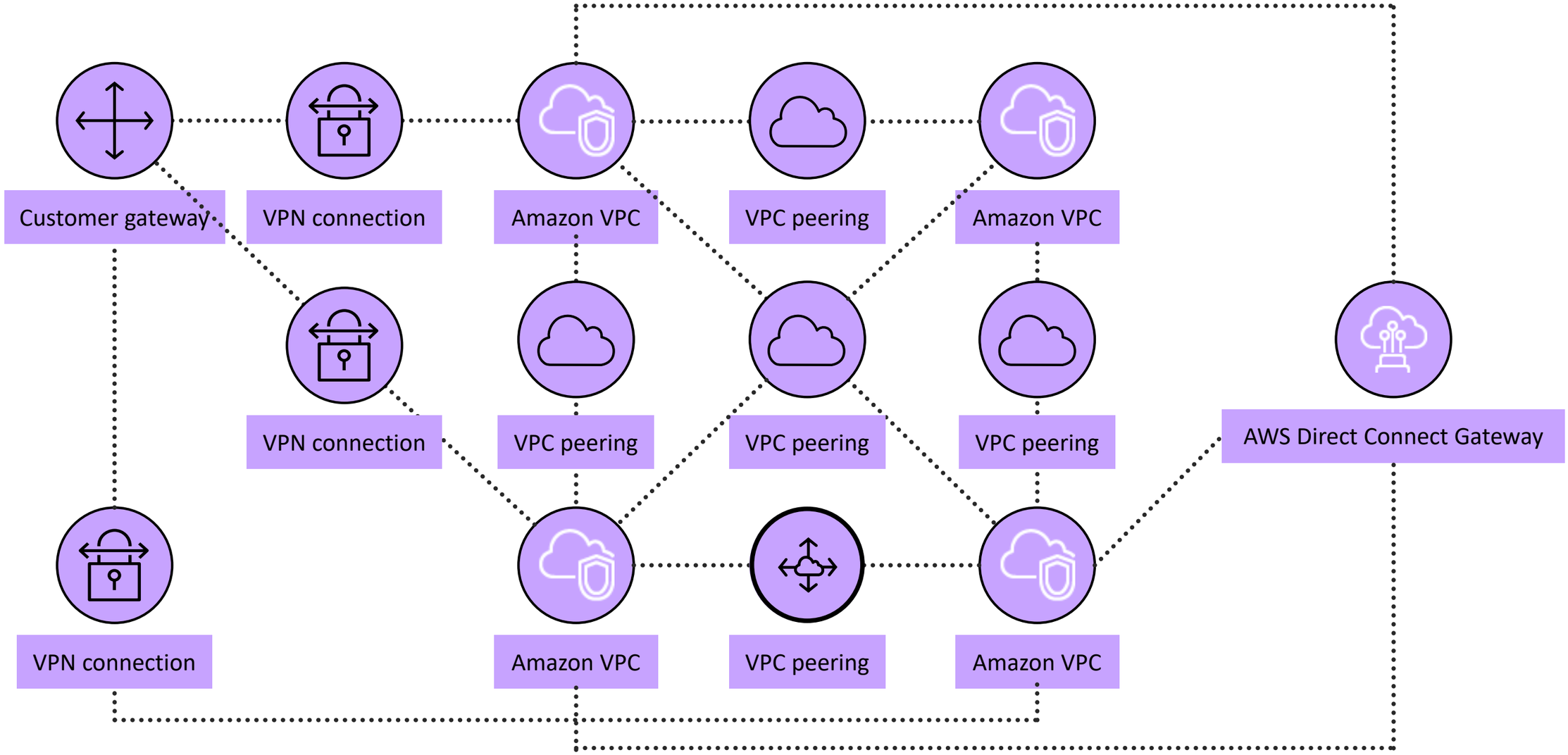
パートナーアプライアンスをミドルボックスとしてサポート

fuze

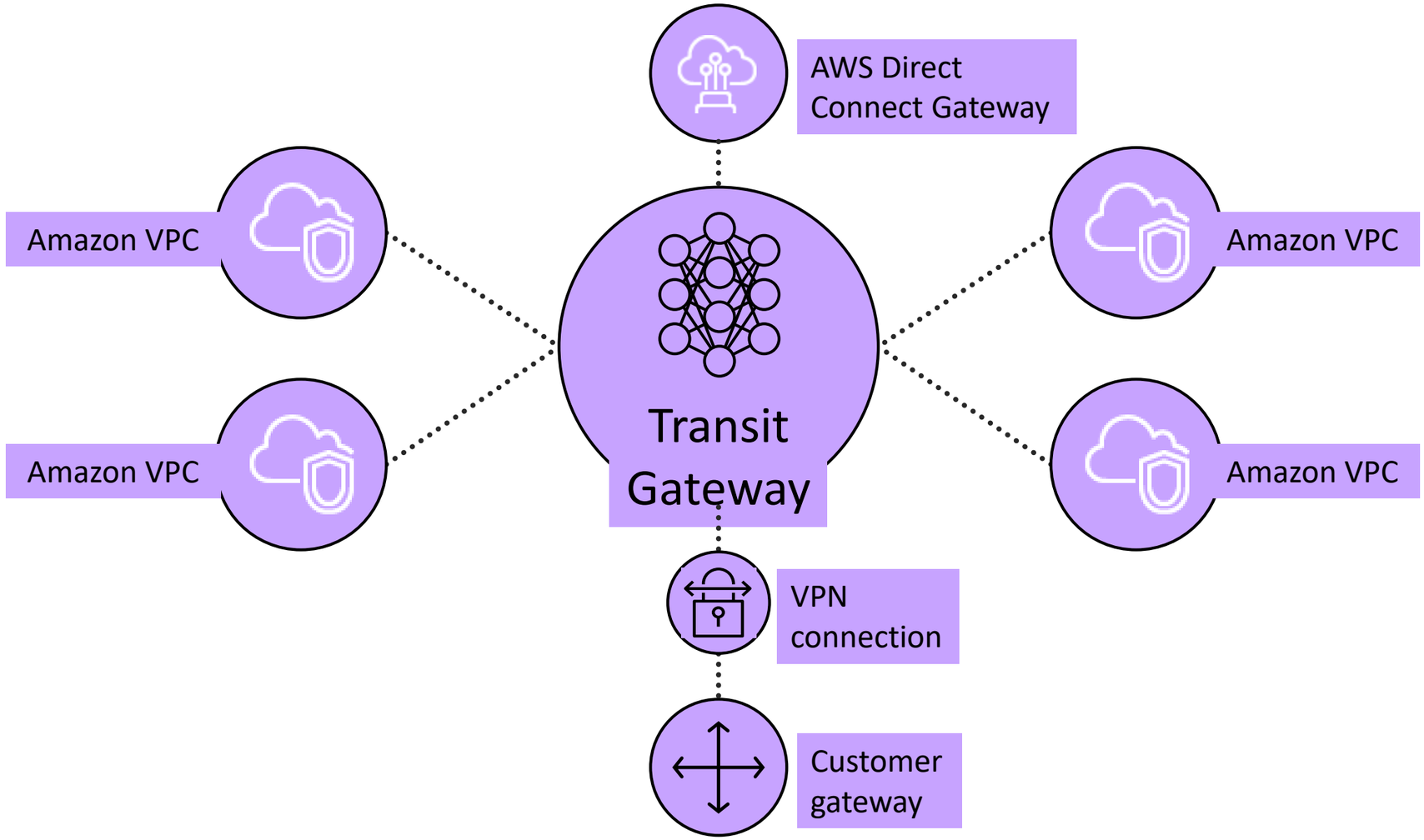
“AWS Transit Gatewayは徹底的に進化することにより、クラウドネットワーキングを簡素化しました。 Transit Gatewayを使用して、一貫した信頼性の高いネットワークパフォーマンスを実現しながら、新しいVPCとオンプレミスネットワークを相互接続する時間を数週間から数分に短縮しています！”

Khoder Shamy, Director, Cloud Platform and Infrastructure, Fuze

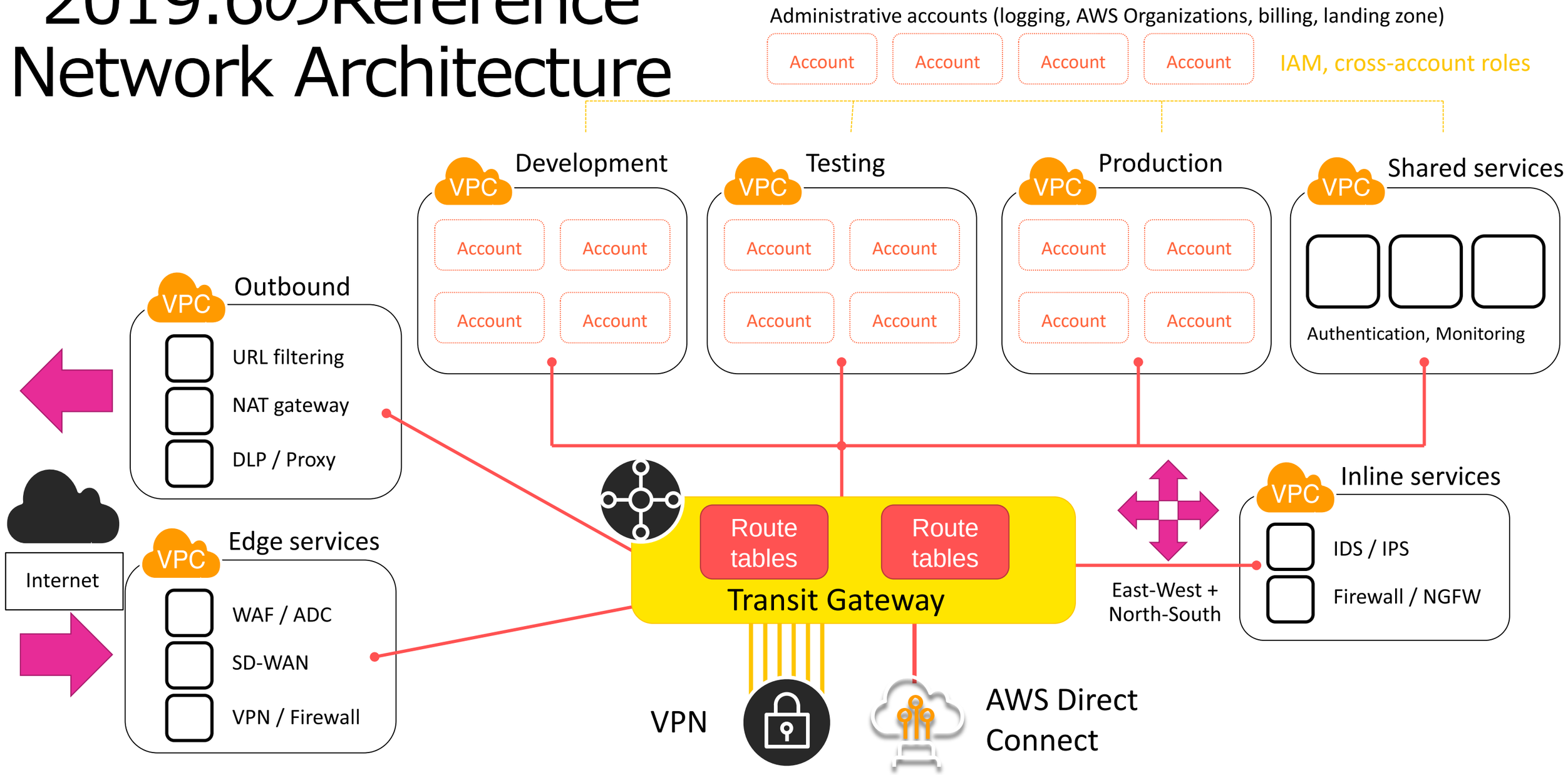
# Transit Gateway以前のネットワーク …



# 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

aws SUMMIT

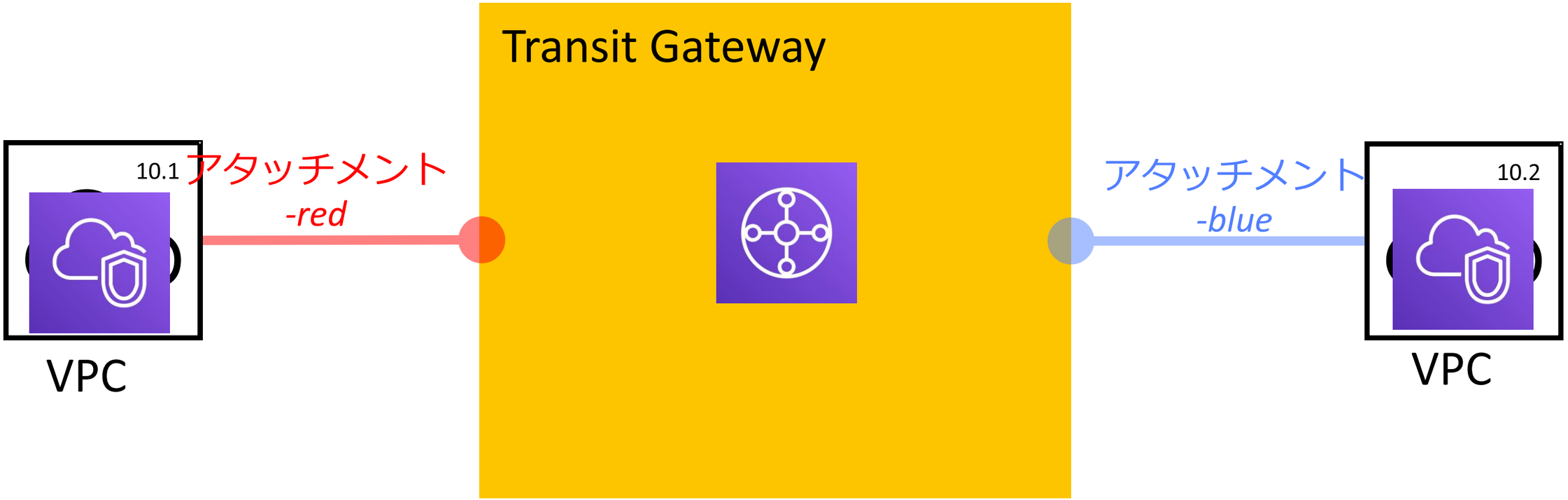
# Transit Gateway用語

- 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！

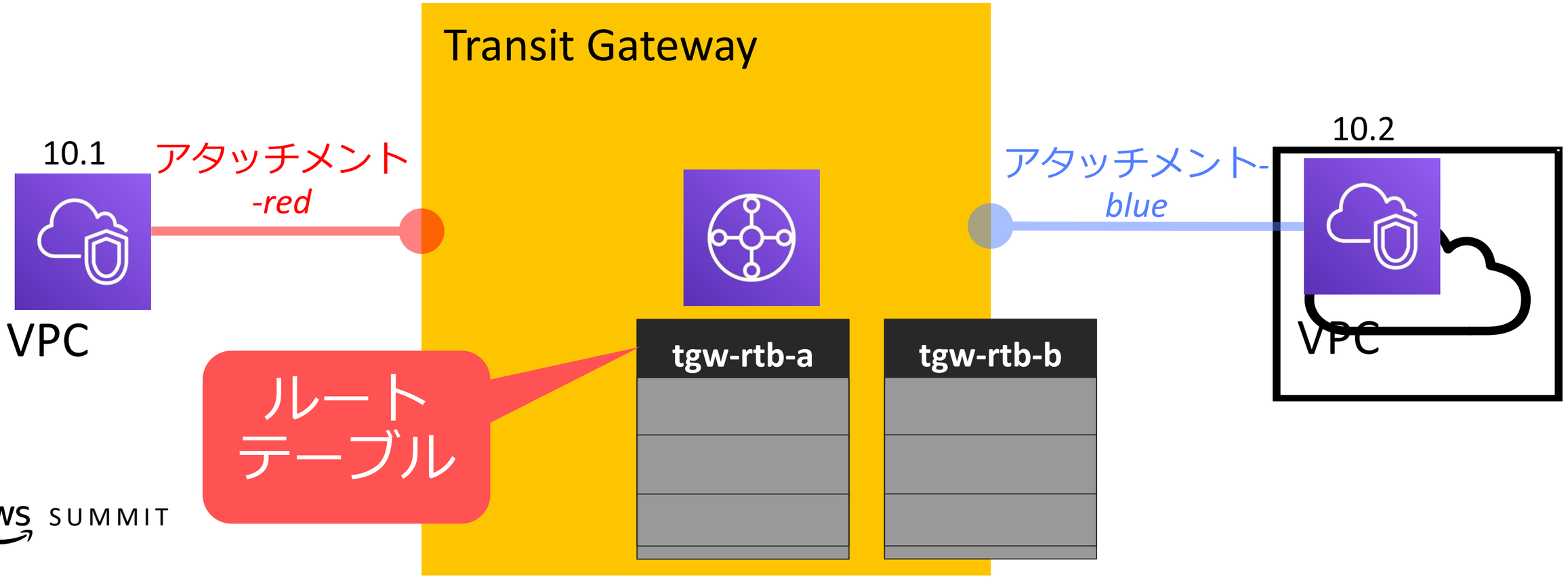
# アタッチメント

- 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



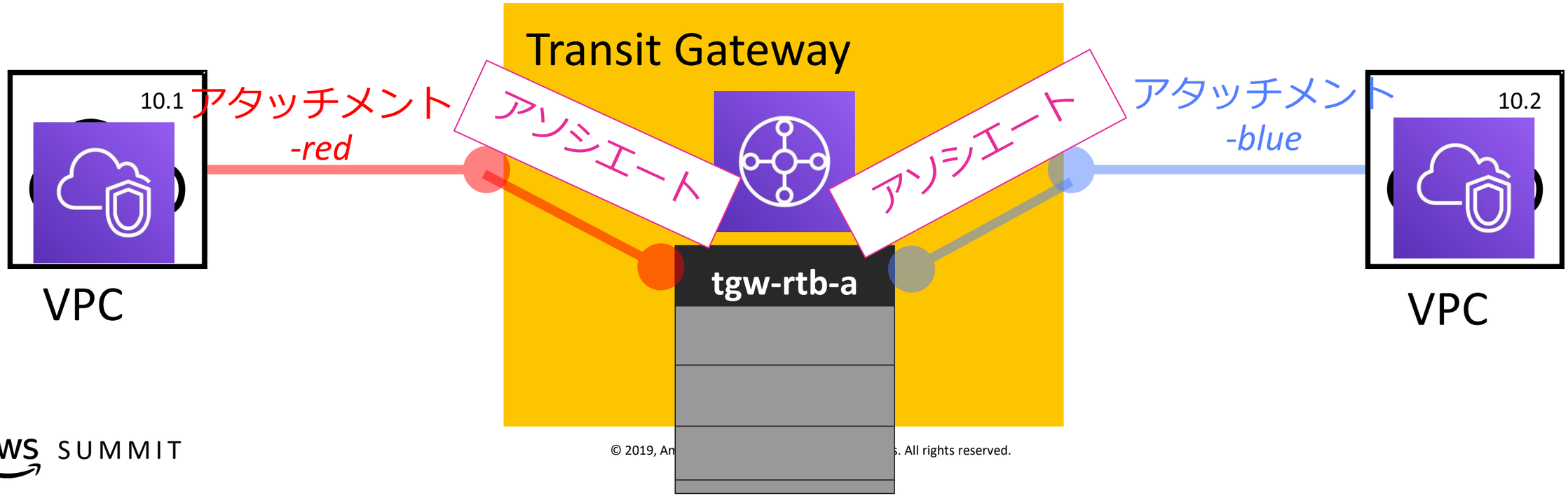
# ルートテーブル

- 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



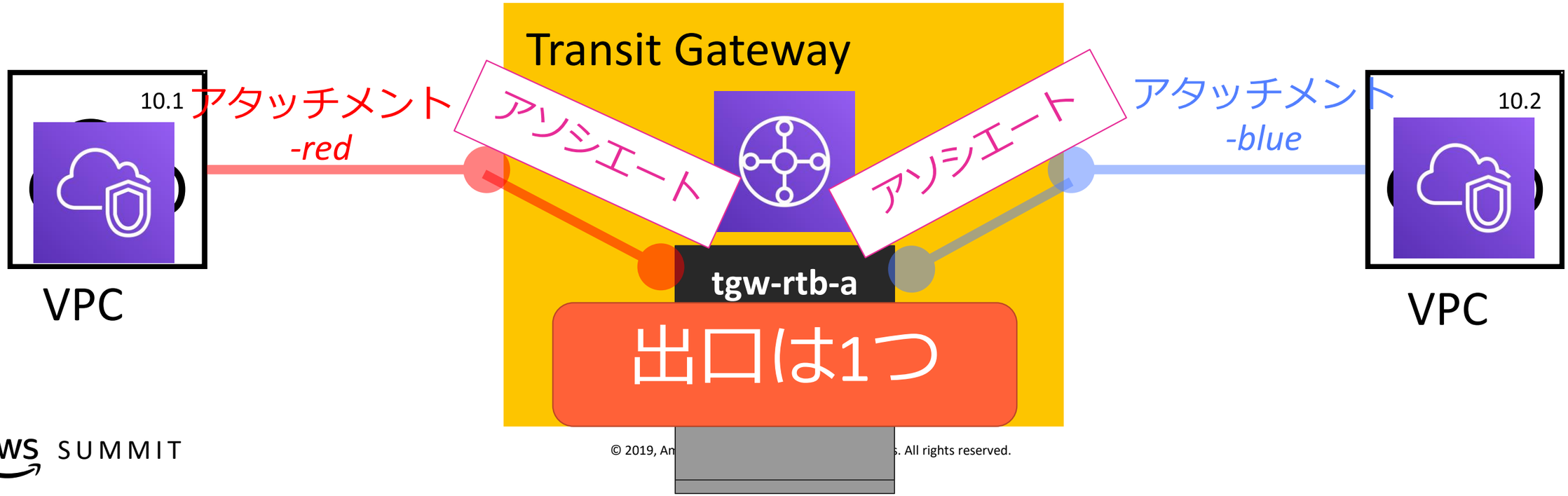
# ルートテーブル：アソシエーション

- 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）



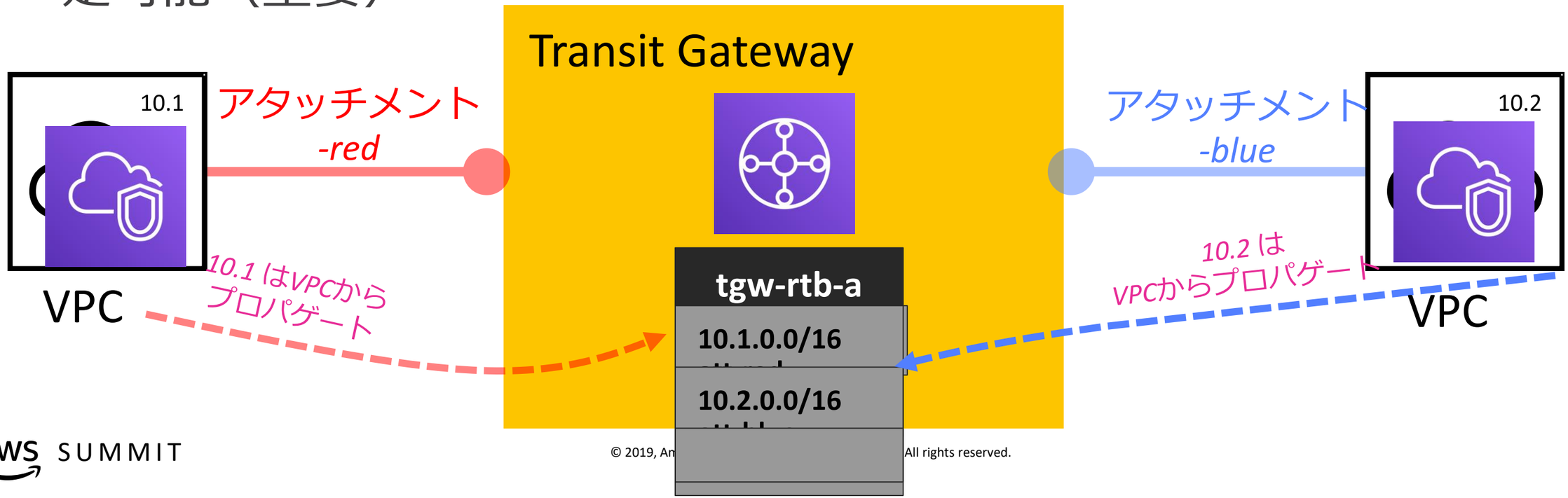
# ルートテーブル：アソシエーション

- 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）



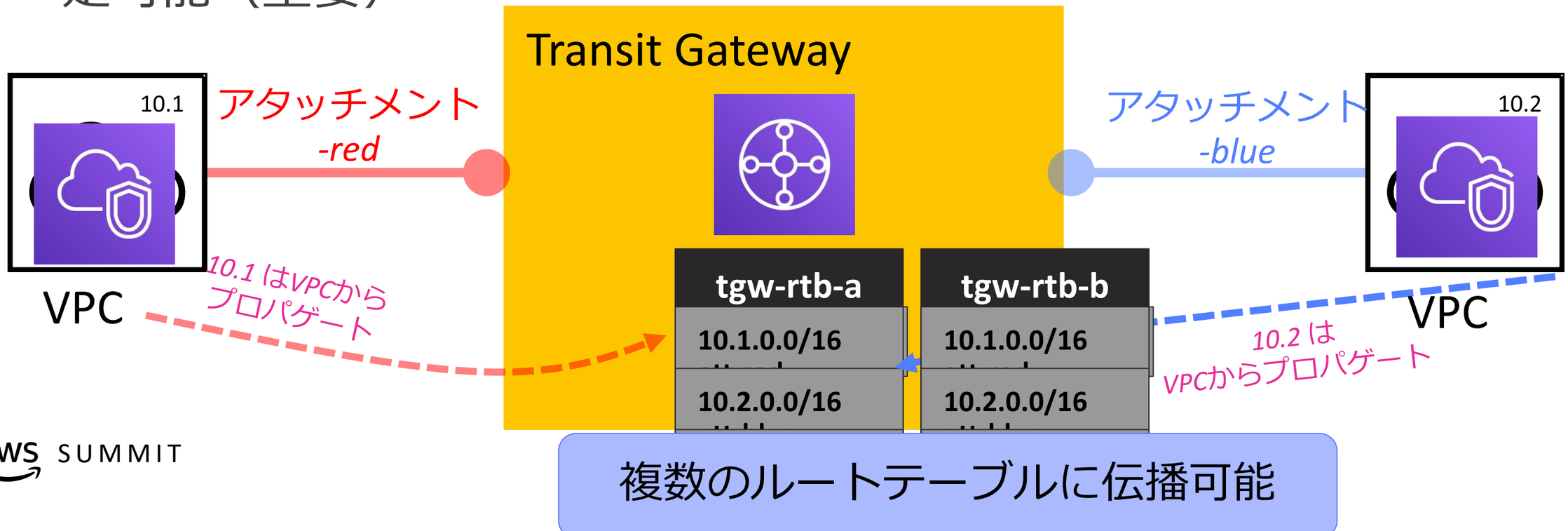
# ルートテーブル：プロパゲーション

- 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）



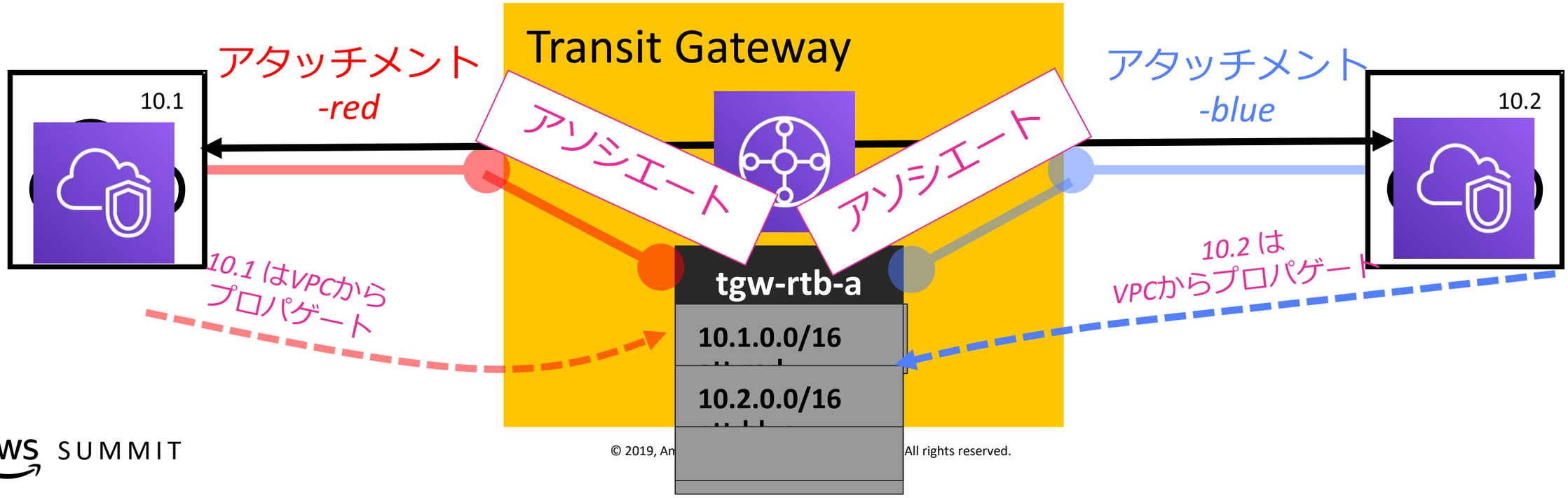
# ルートテーブル：プロパゲーション

- 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）



# 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


**Route Table:** rtb-044de1cac0c4c788c

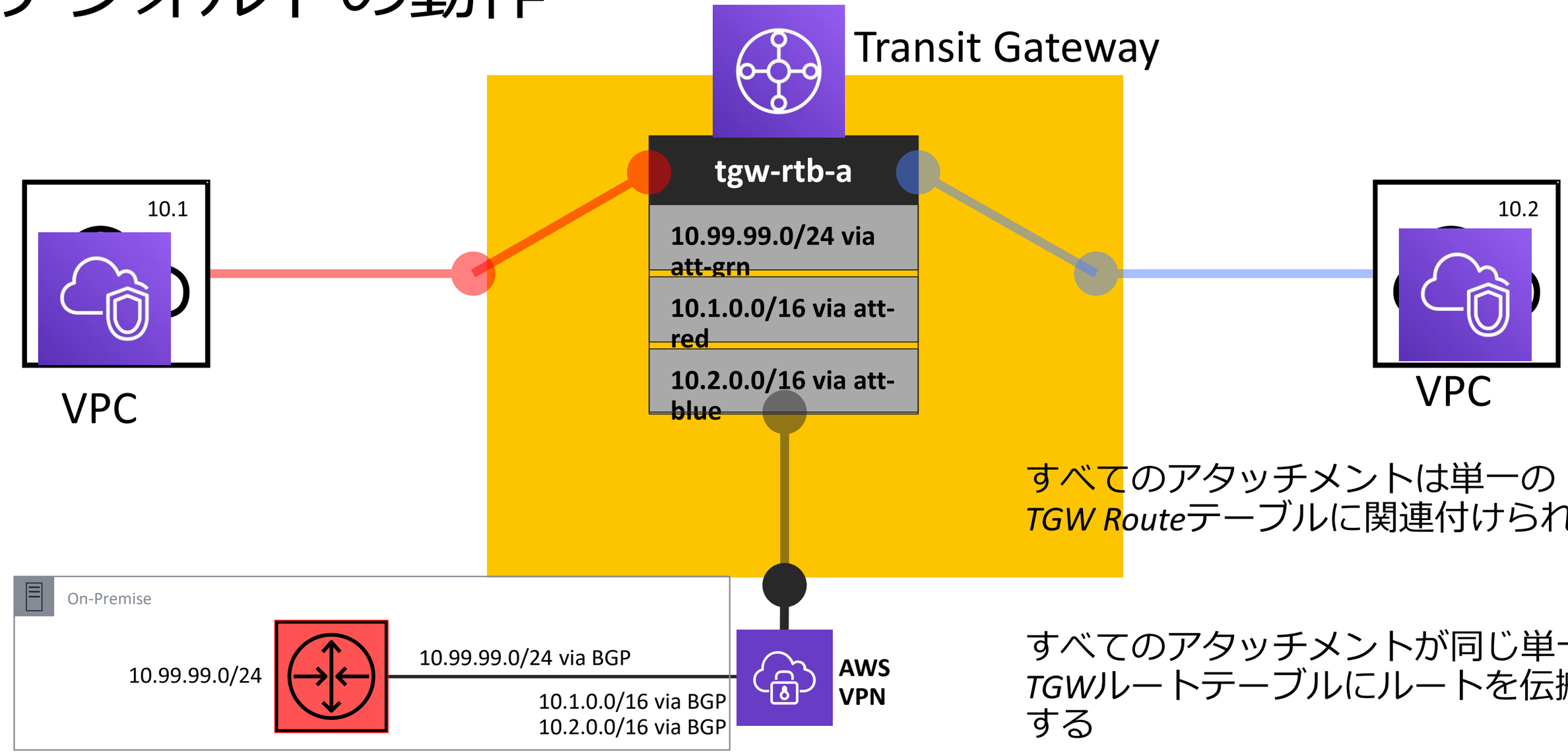
Summary | **Routes** | Subnet Associations | Route Propagation | Tags

Edit routes

View: All routes

| 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 |

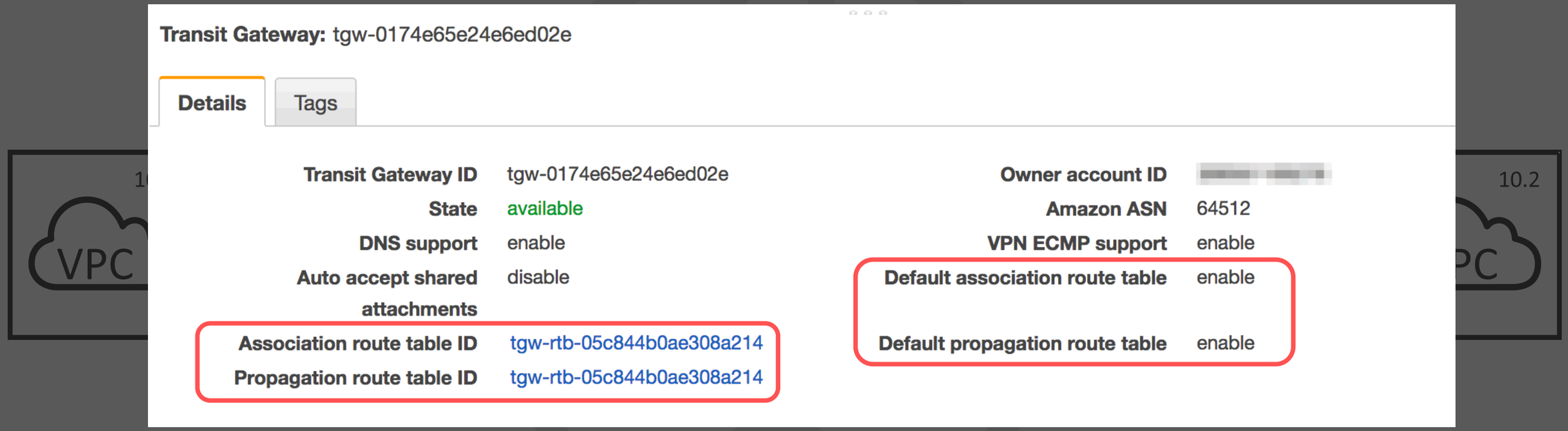
# デフォルトの動作




すべてのアタッチメントは単一の*TGW Route*テーブルに関連付けられる

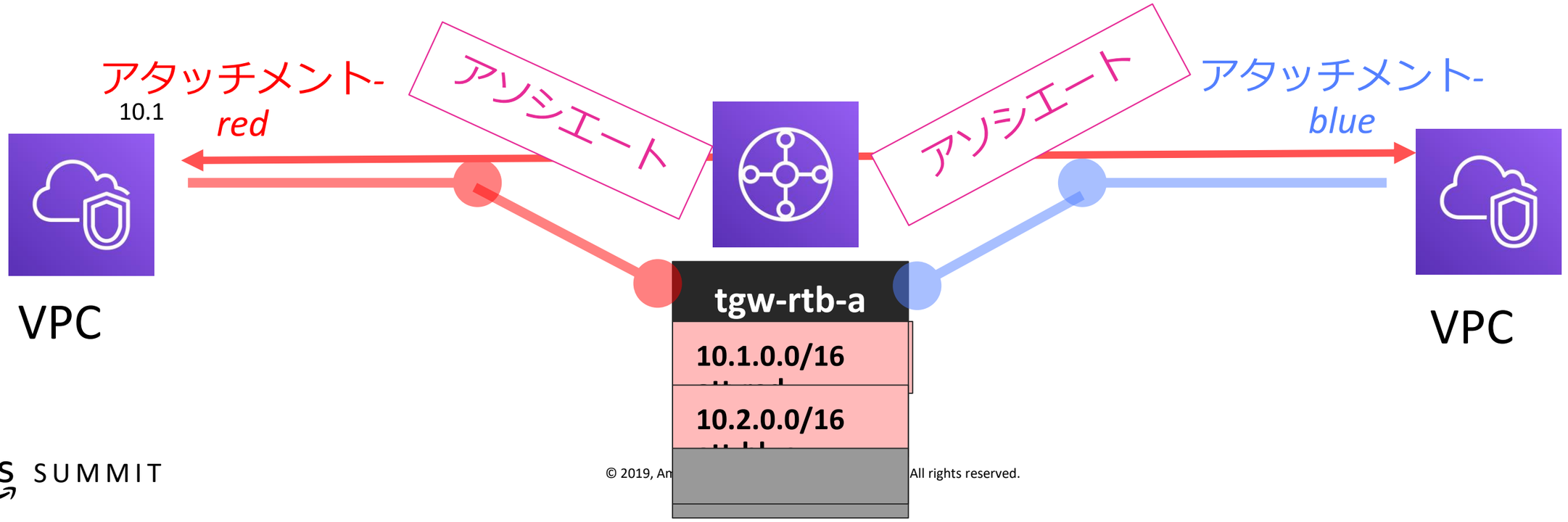
すべてのアタッチメントが同じ単一*TGW*ルートテーブルにルートを伝搬する

# アタッチメント– ‘associated & propagated route table’



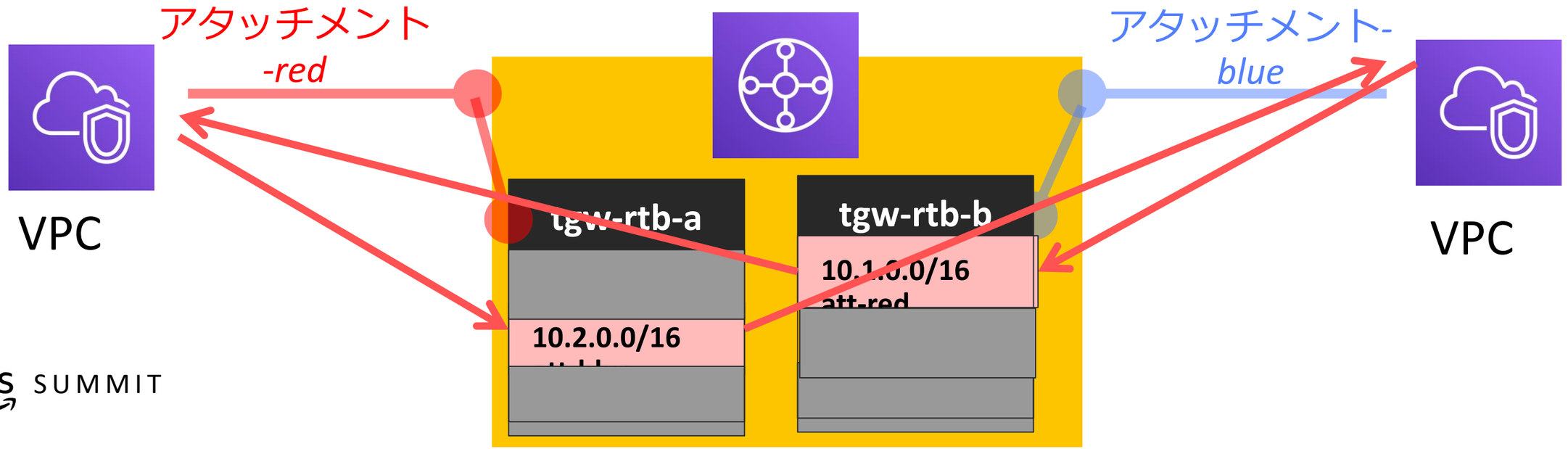
# ルートテーブル：スタティックルート

- 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。



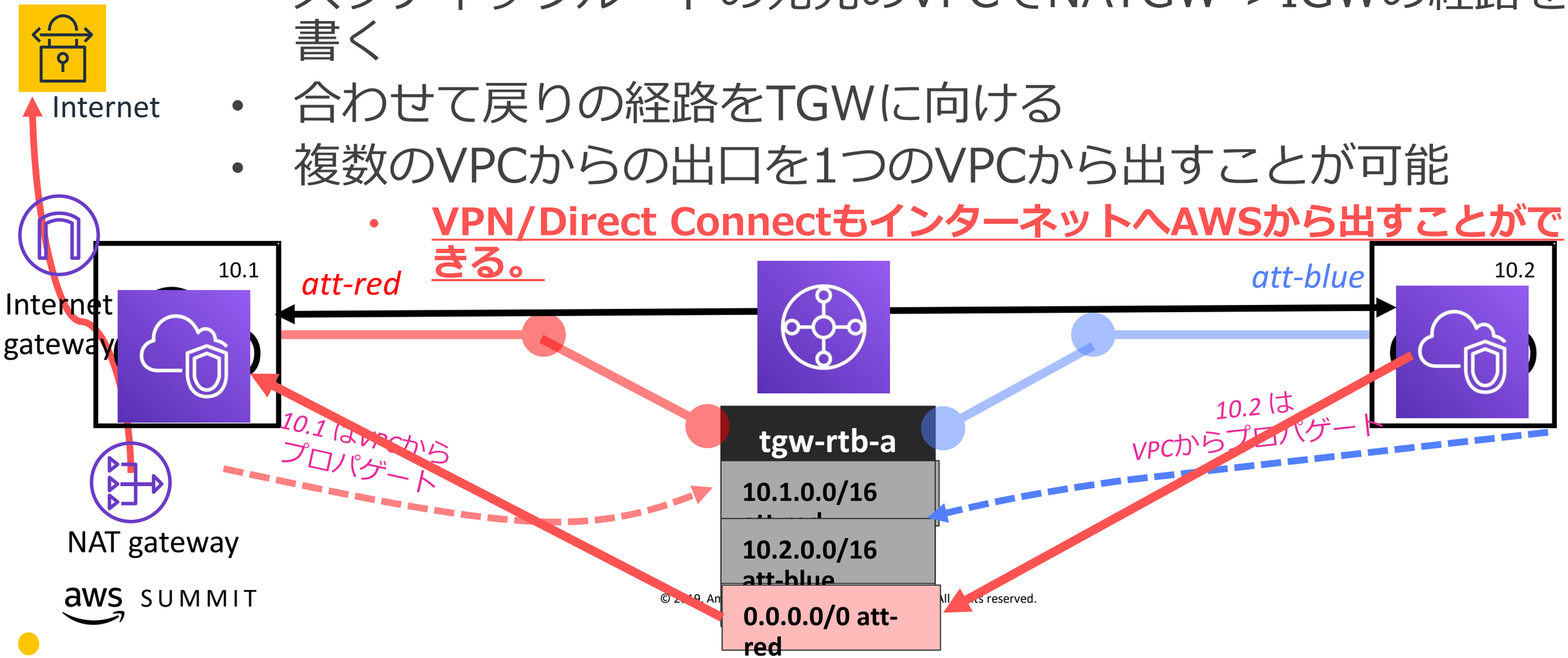
# ルートテーブル：スタティックルート

- 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

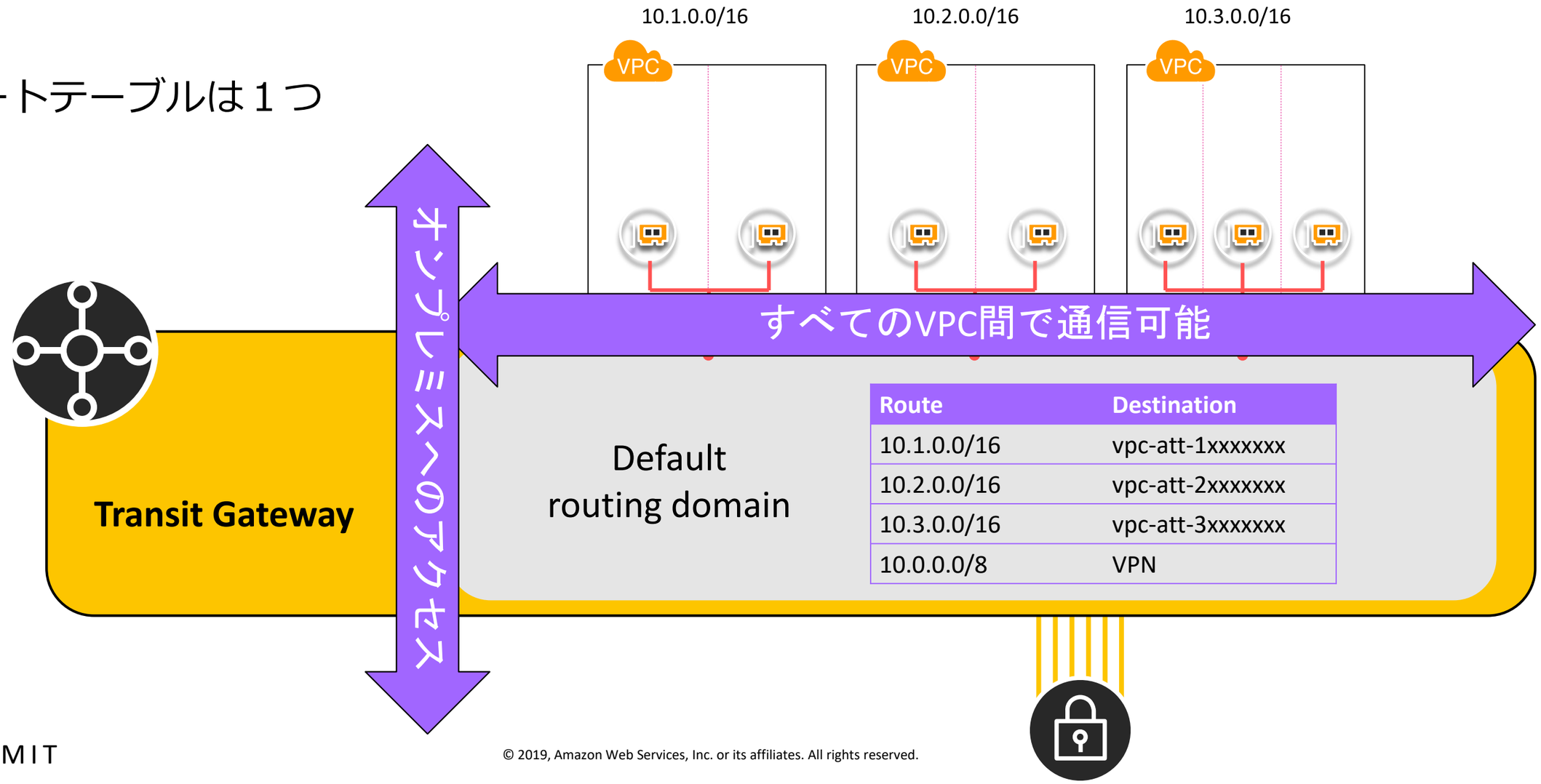
aws SUMMIT

# 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

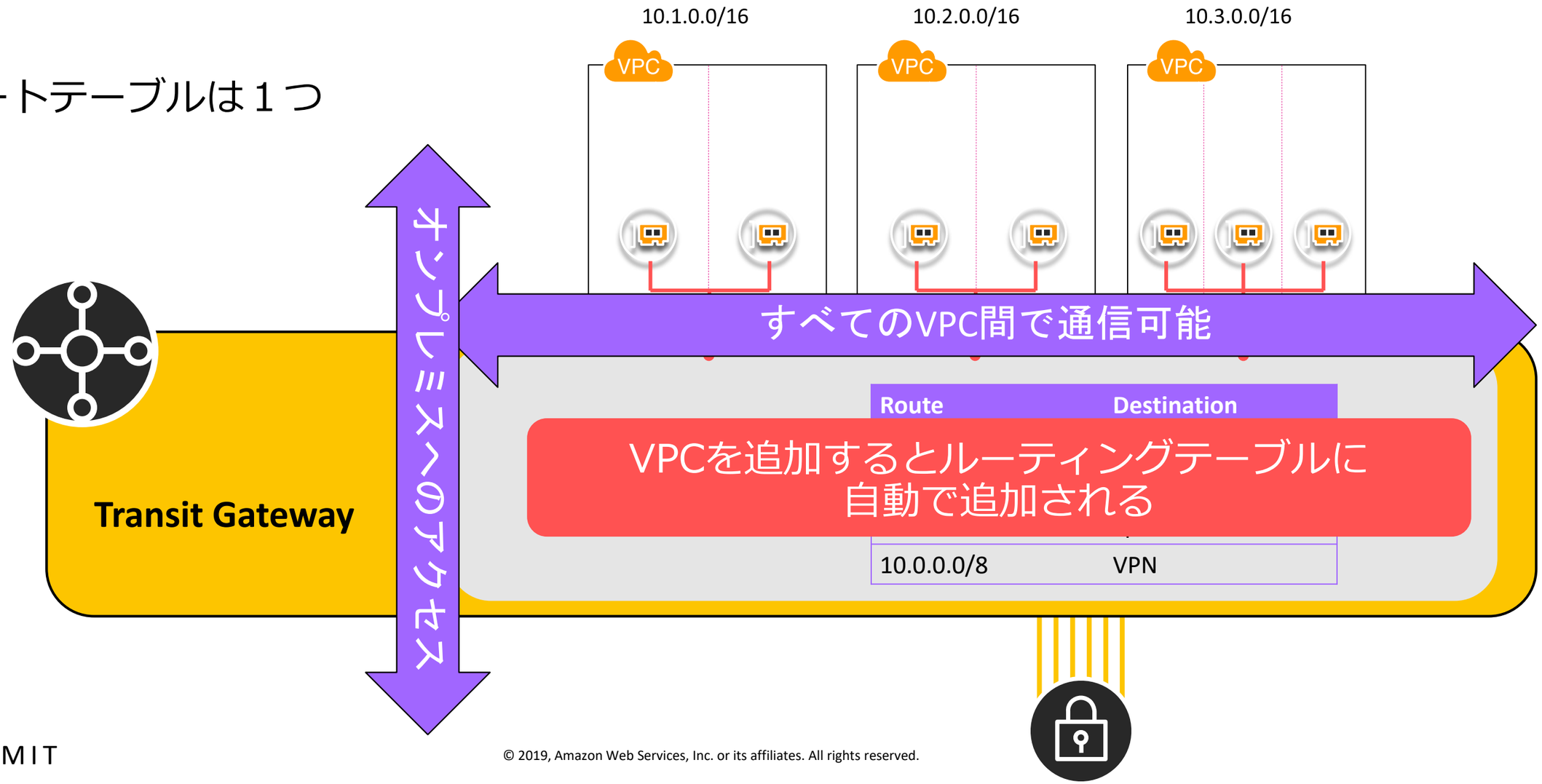
# Transit Gatewayで自由に通信させる Route Domain

ルートテーブルは１つ



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

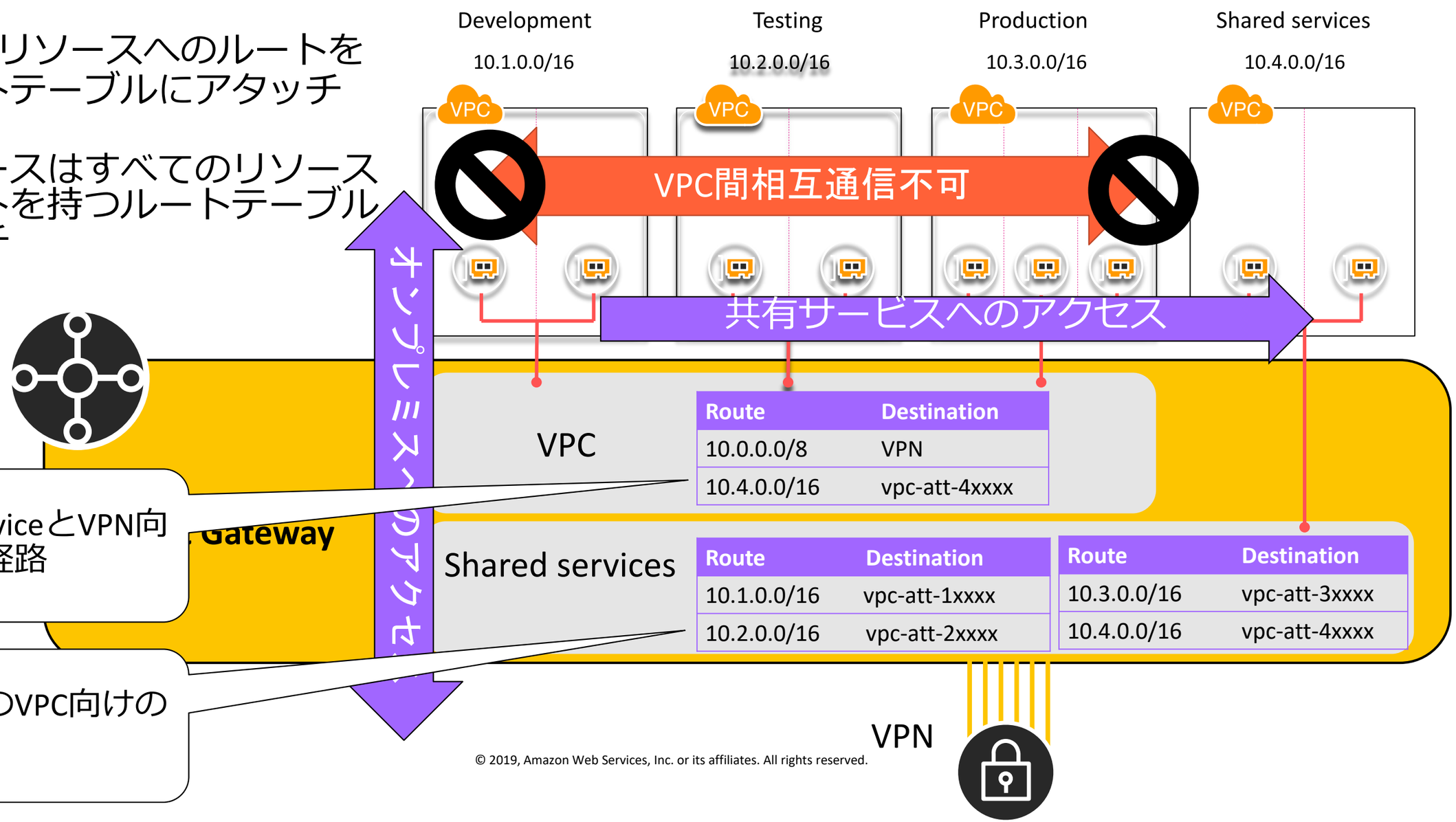
ルートテーブルは１つ



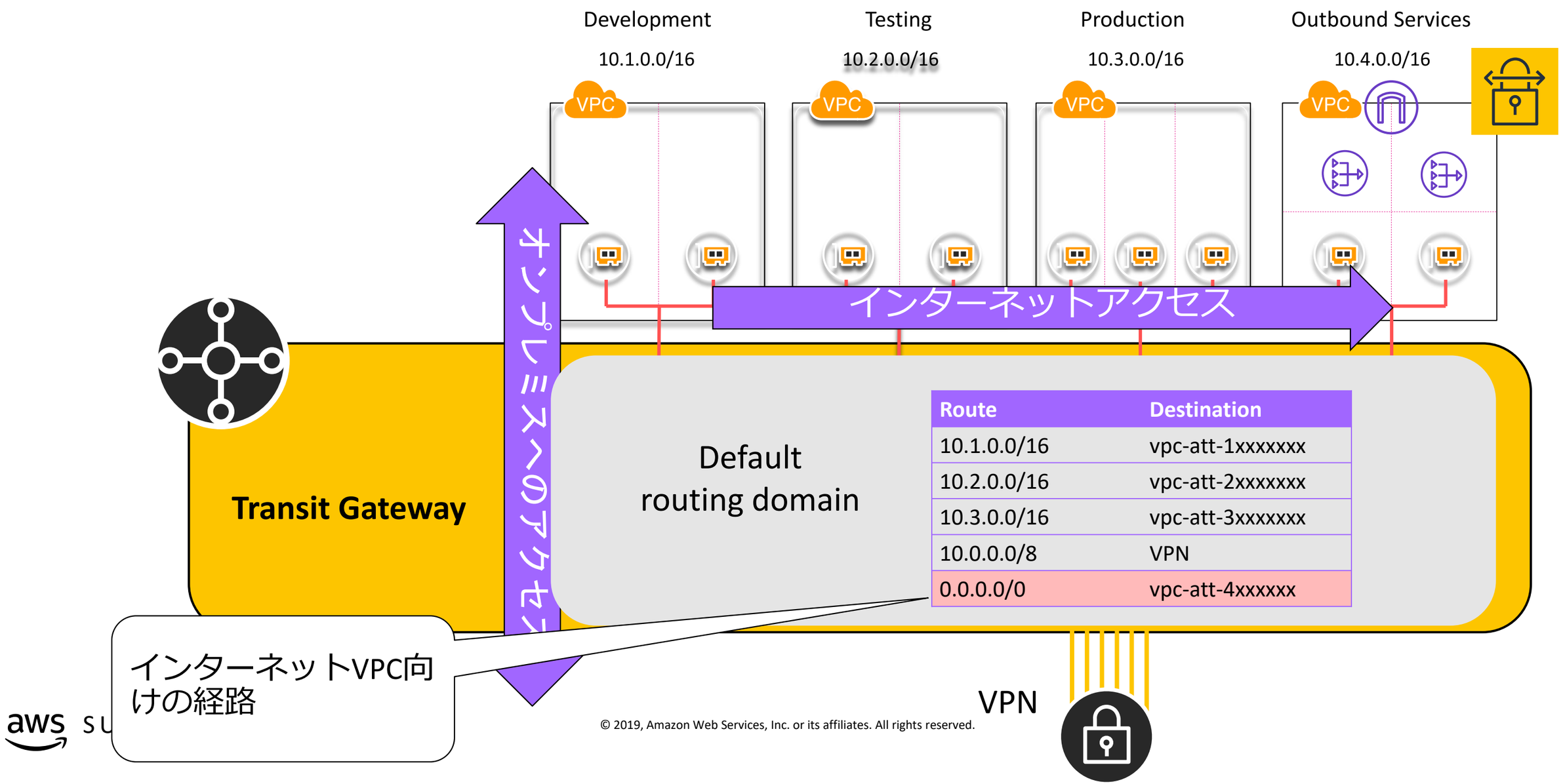
# Transit Gatewayで通信制限する Route Domain

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

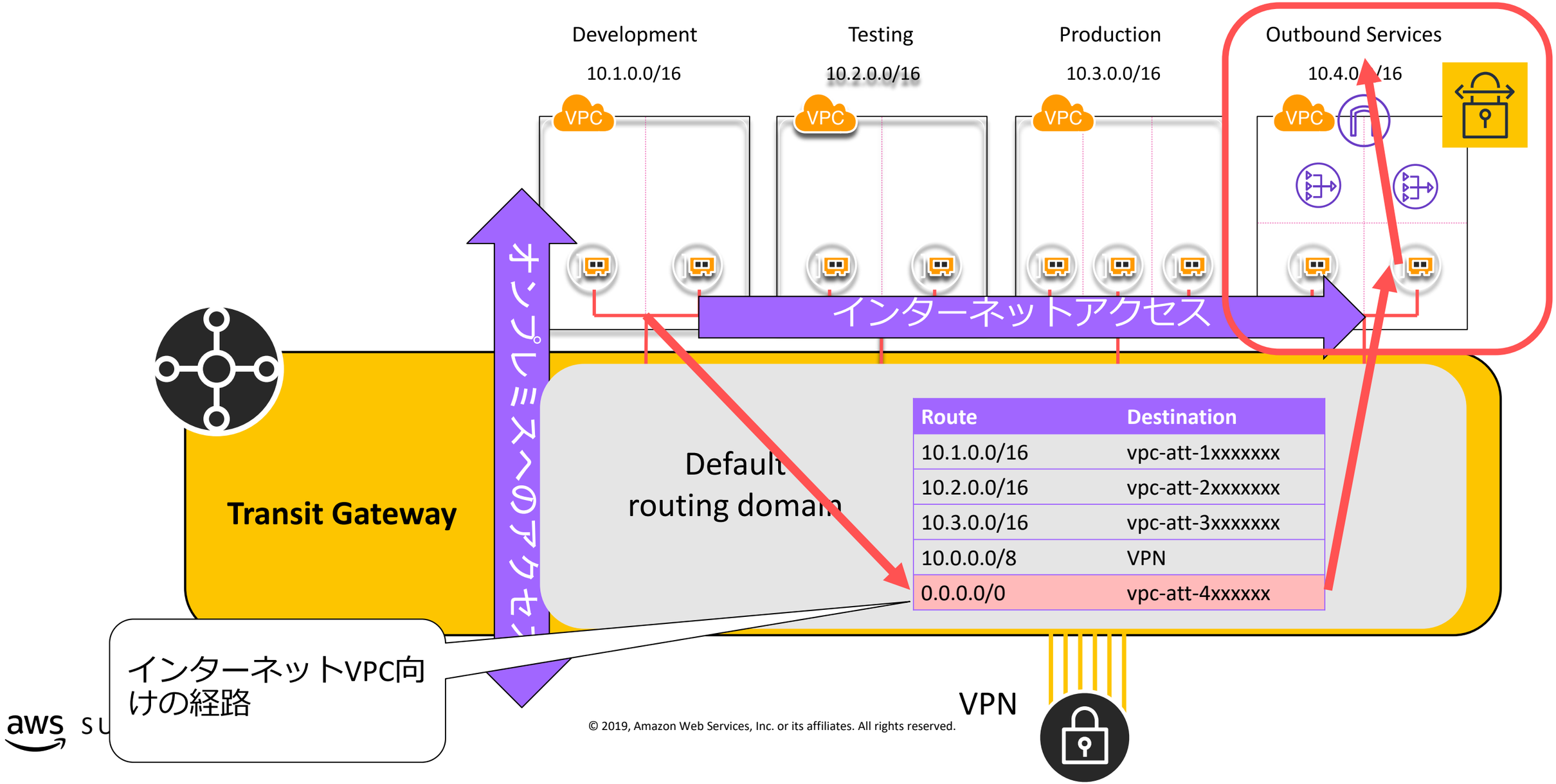
共有リソースはすべてのリソースへのルートを持つルートテーブルにアタッチ



# インターネットに抜けるOutbound Route Domain

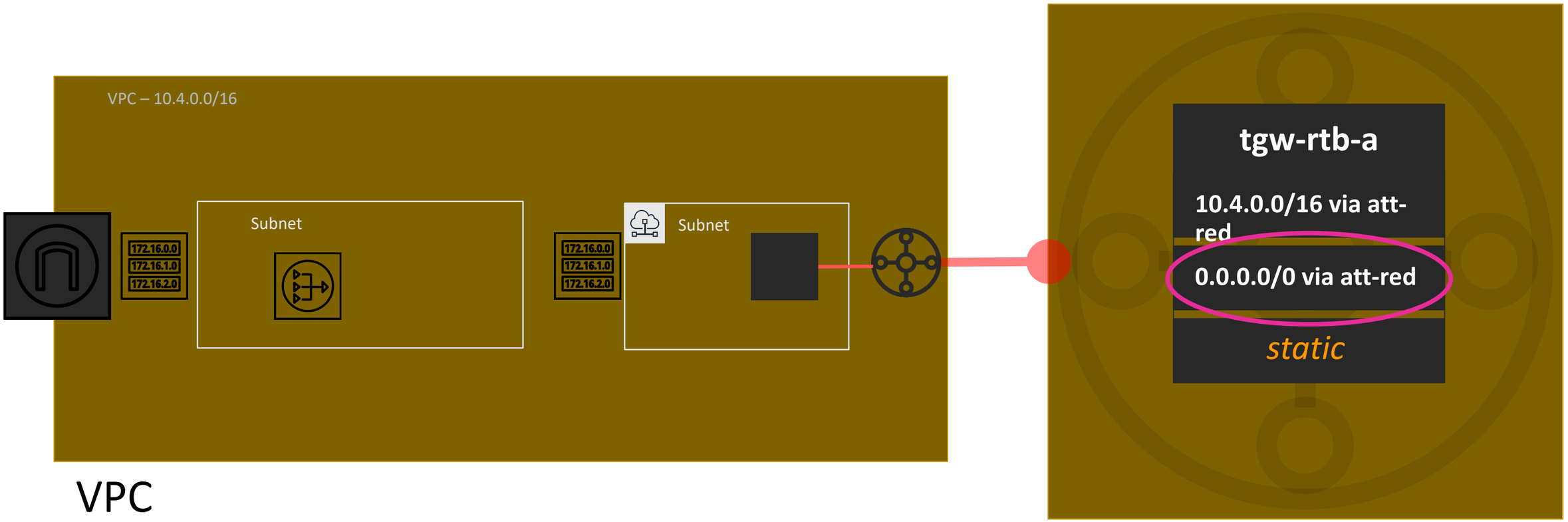


# インターネットに抜けるOutbound Route Domain



# Outbound Services VPC詳細

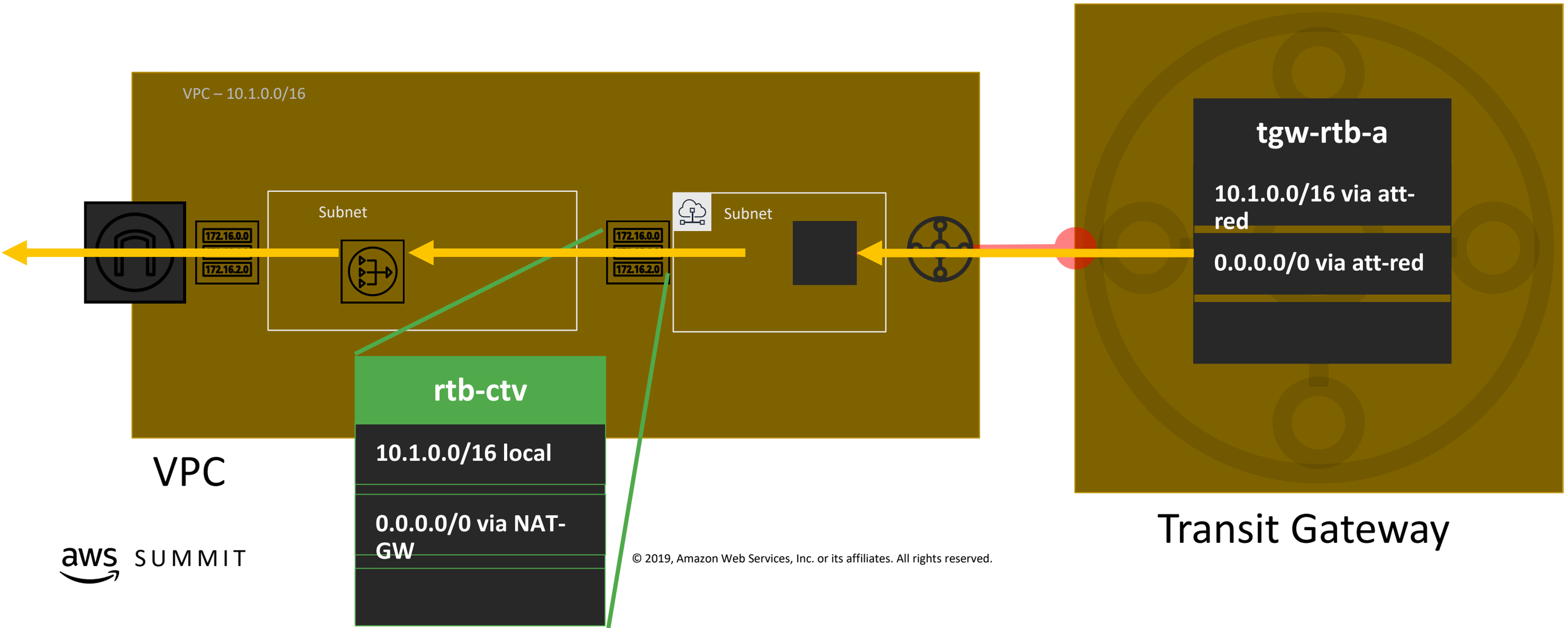
Connectivity Route TableでNATゲートウェイのターゲットを指定してインターネットに出て行くには？




VPC

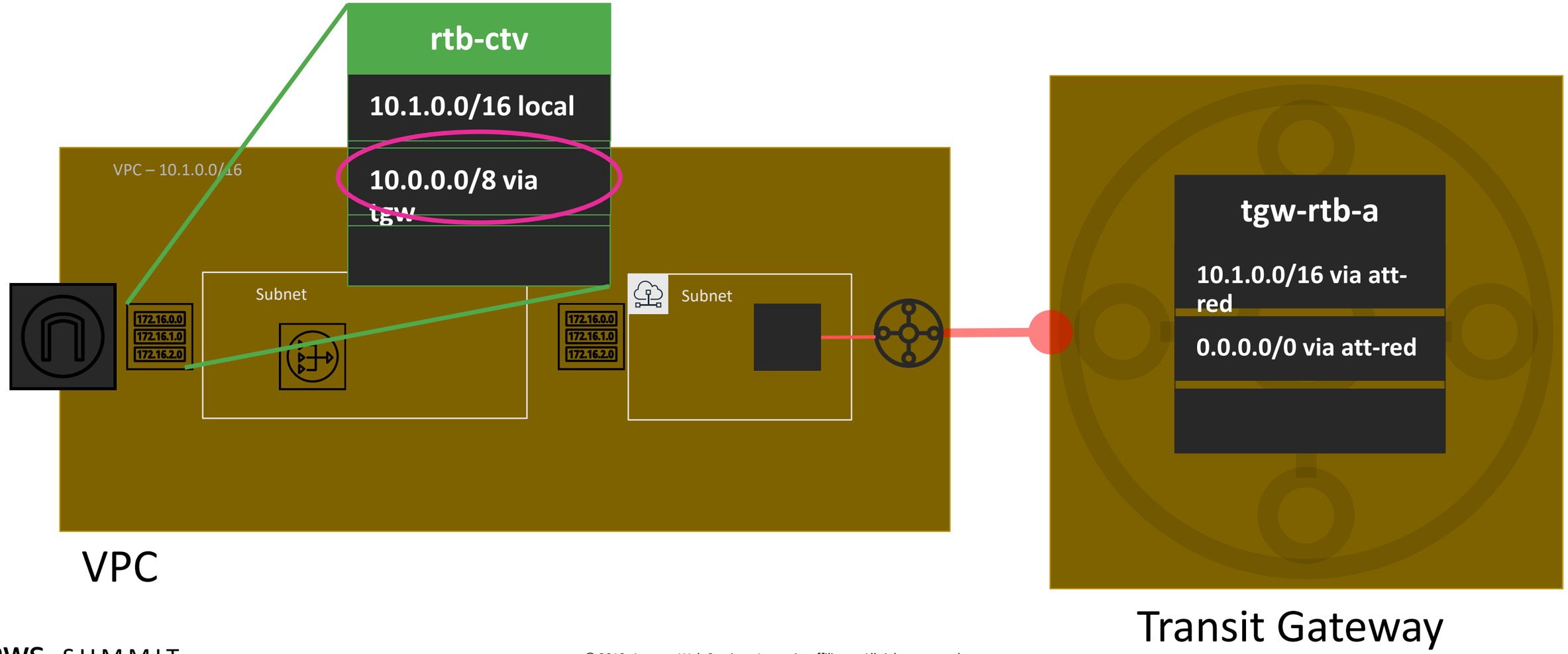
Transit Gateway

# Outbound Services VPC詳細



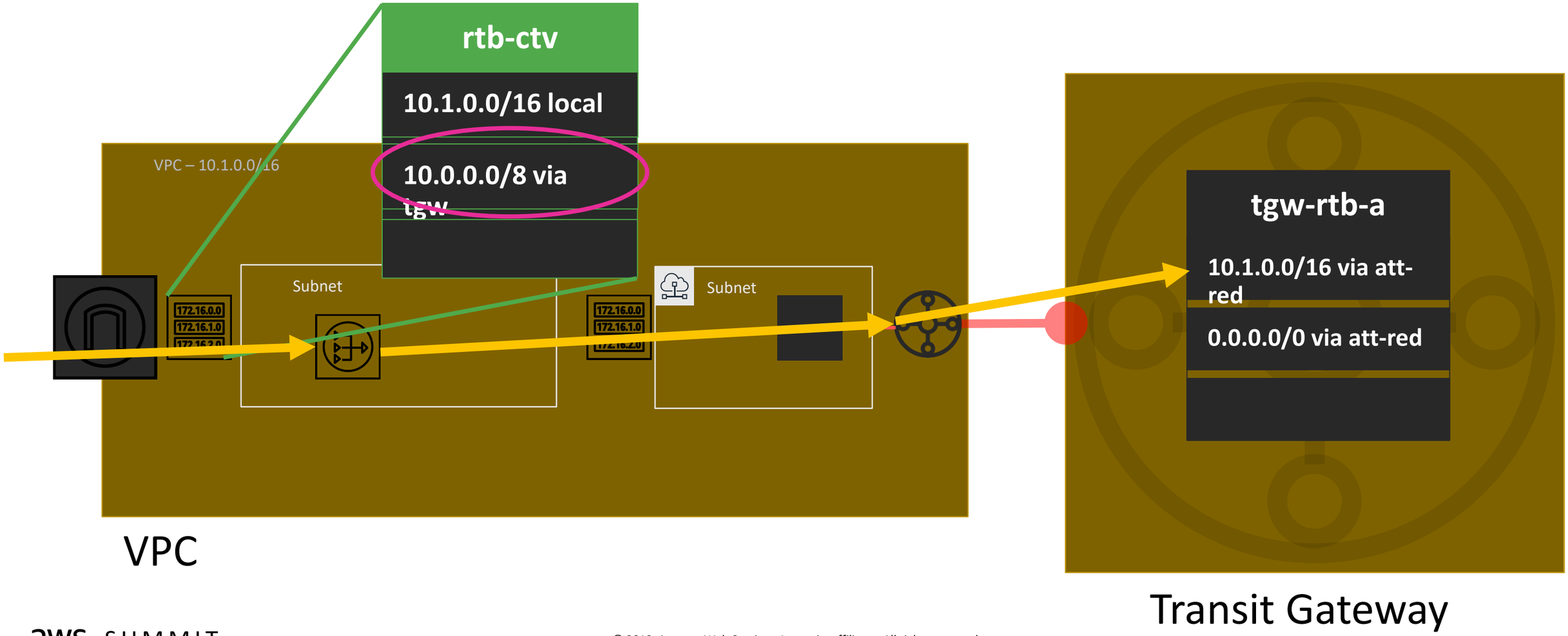
# Outbound Services VPC詳細

## 戻りの経路を書く

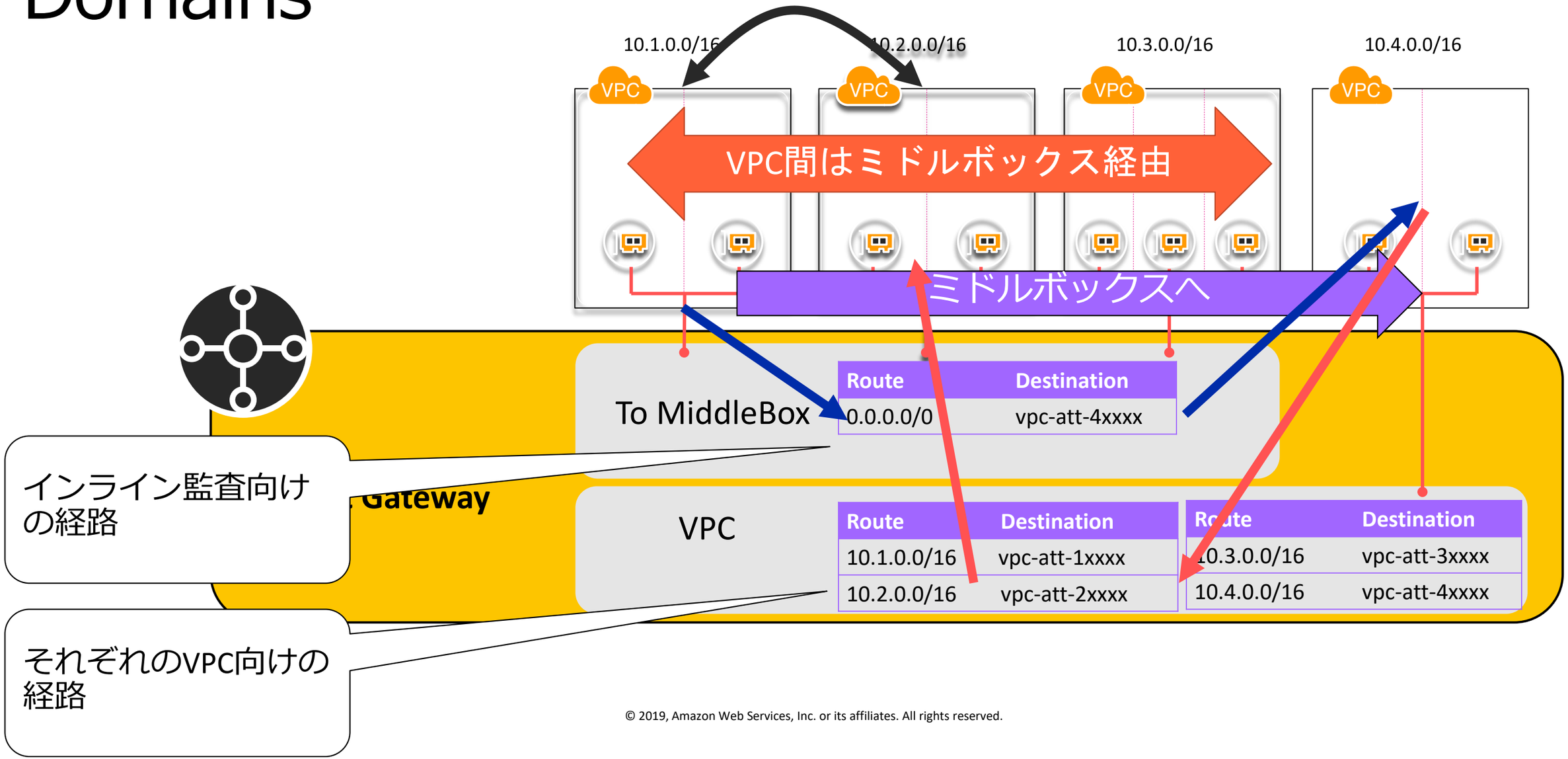


# Outbound Services VPC詳細

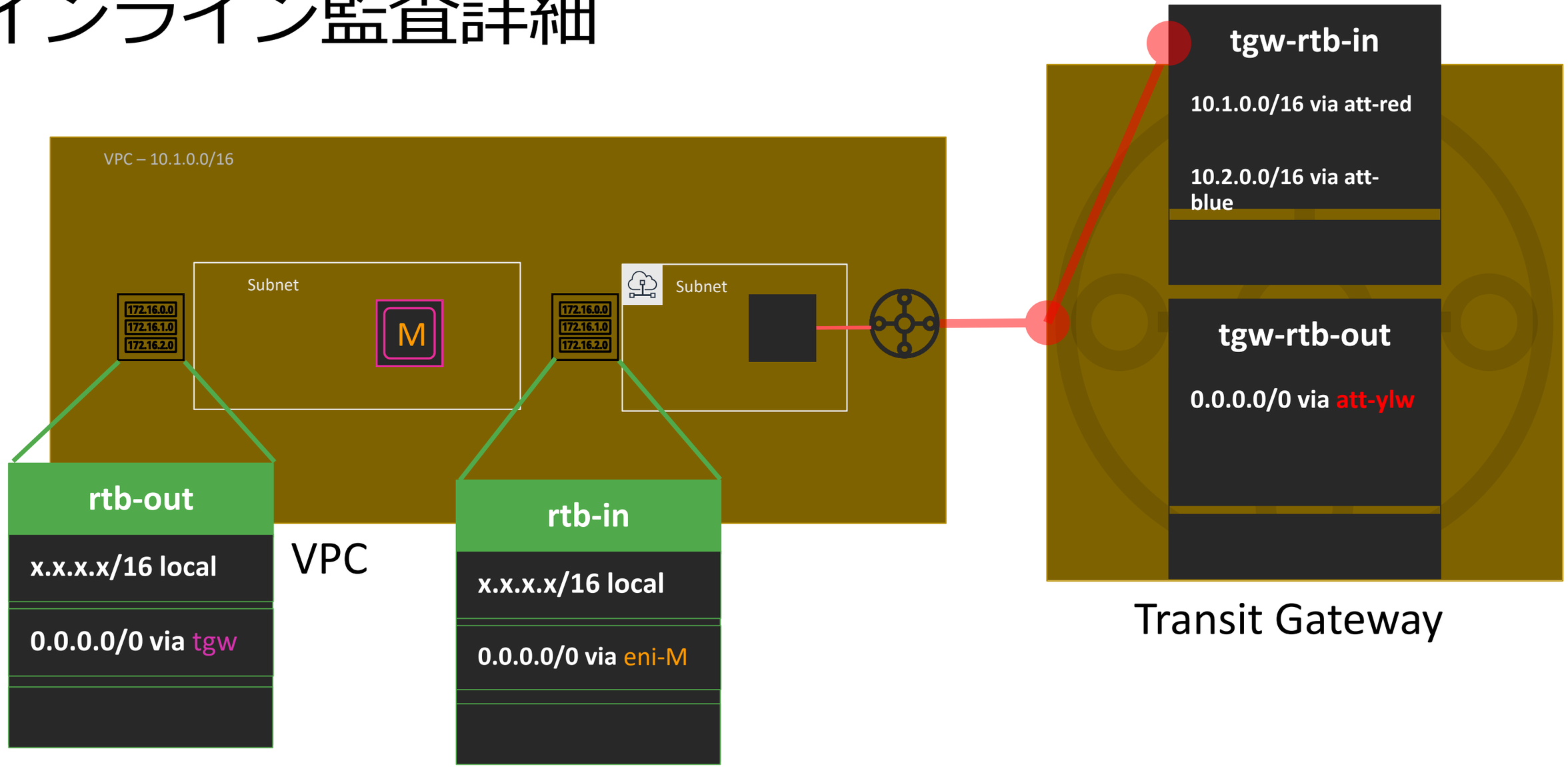
## 戻りの経路を書く



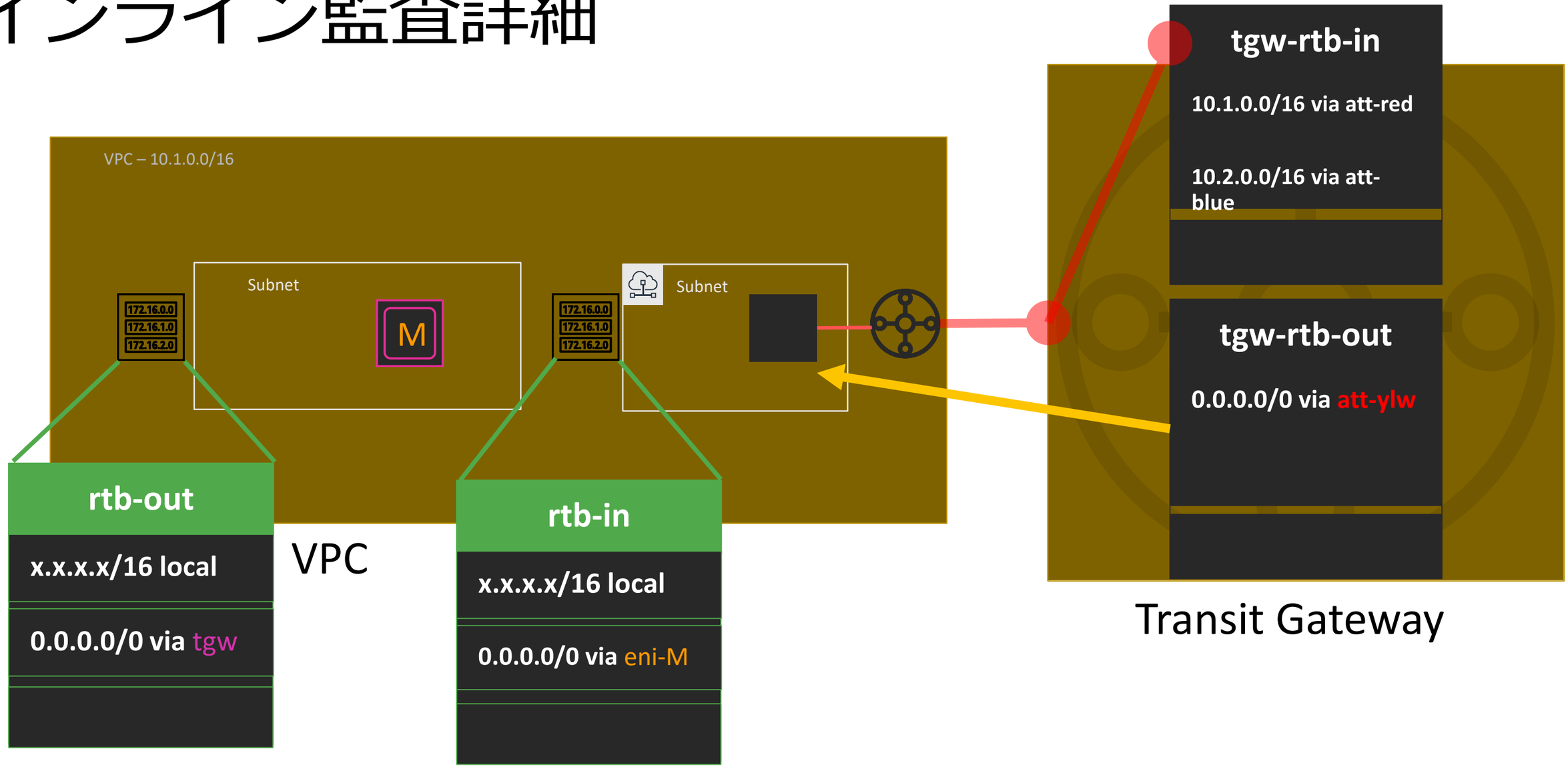
# VPC間のトラフィックをインライン監査するRoute Domains



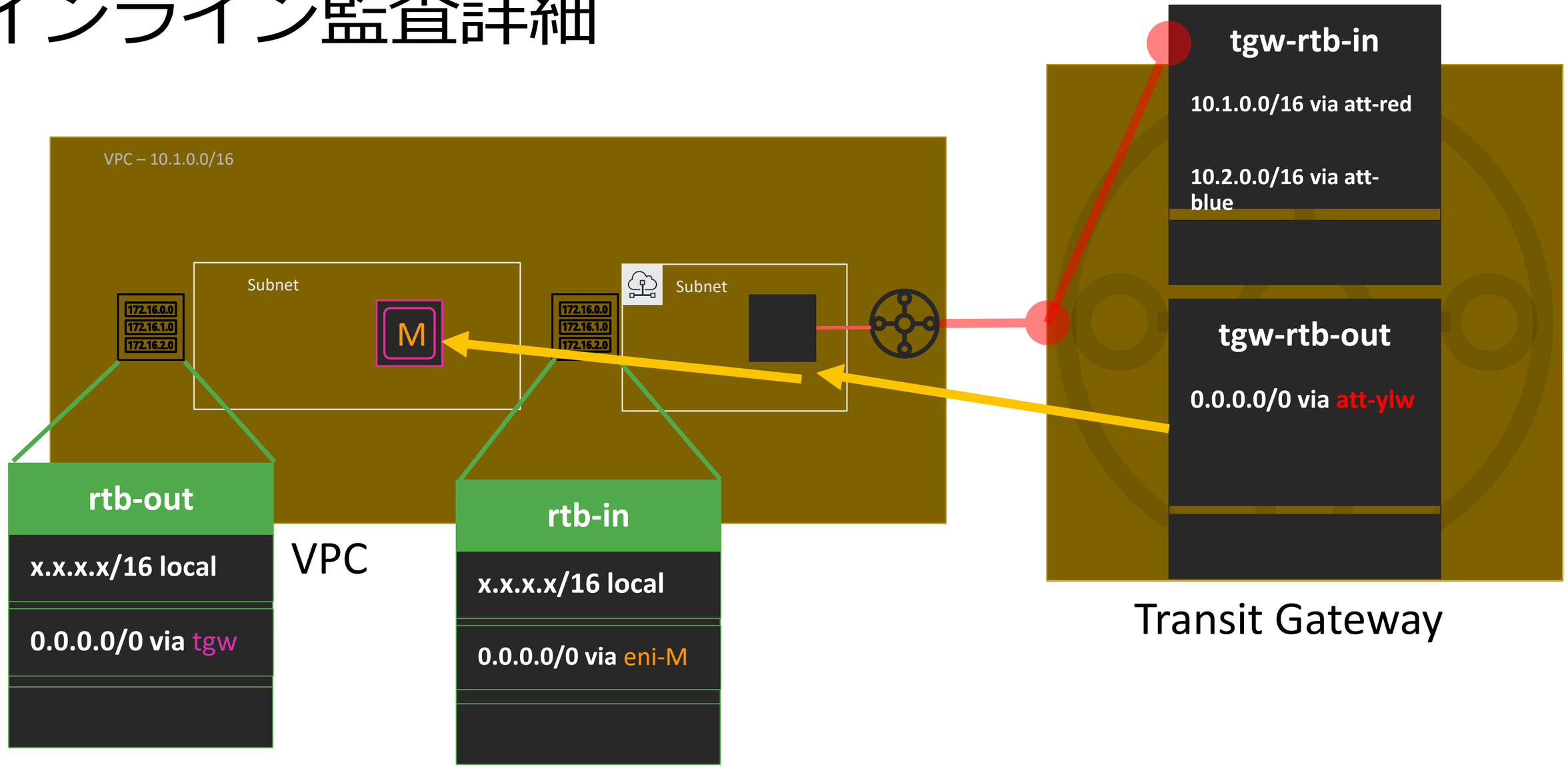
# インライン監査詳細



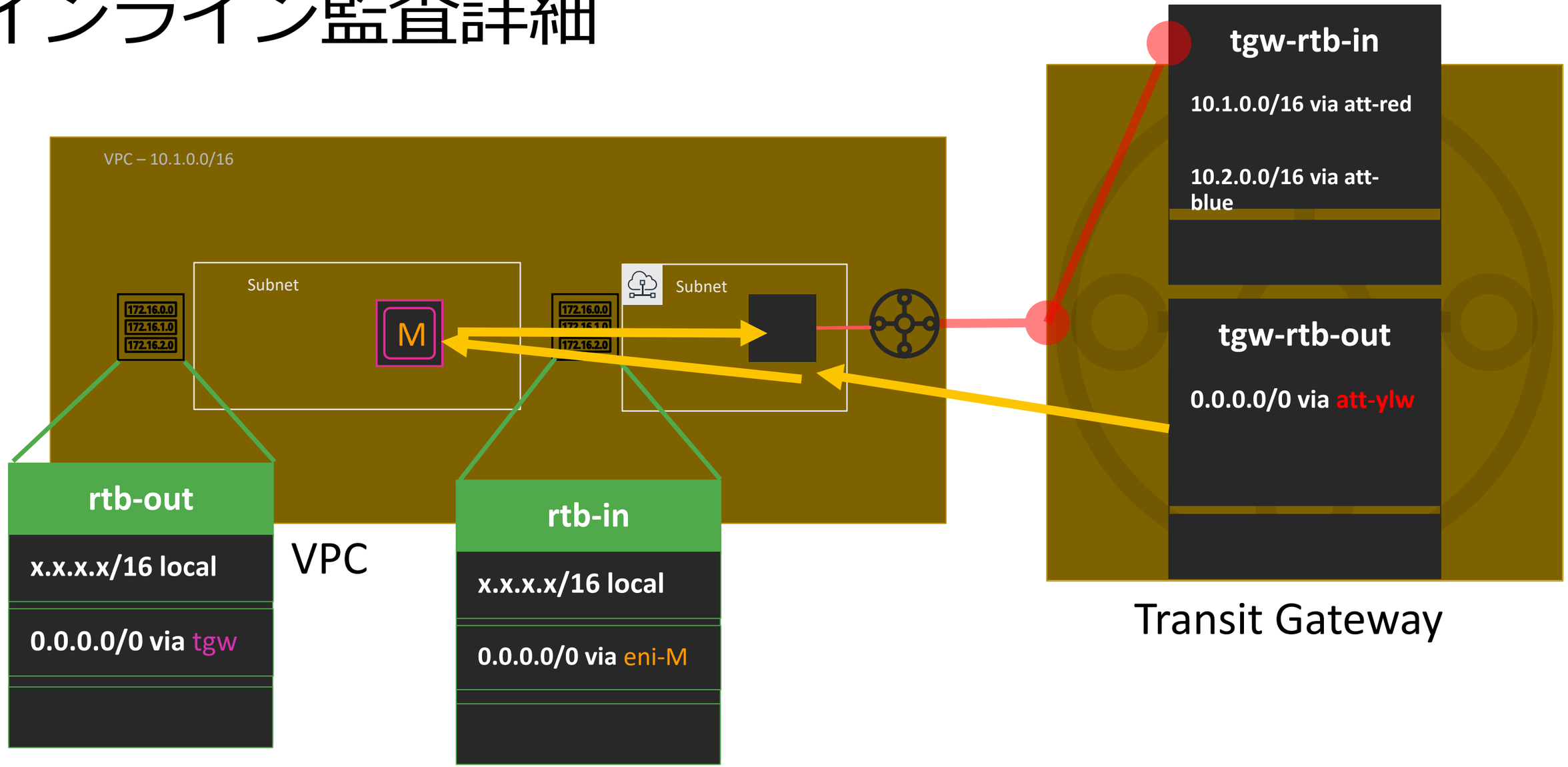
# インライン監査詳細



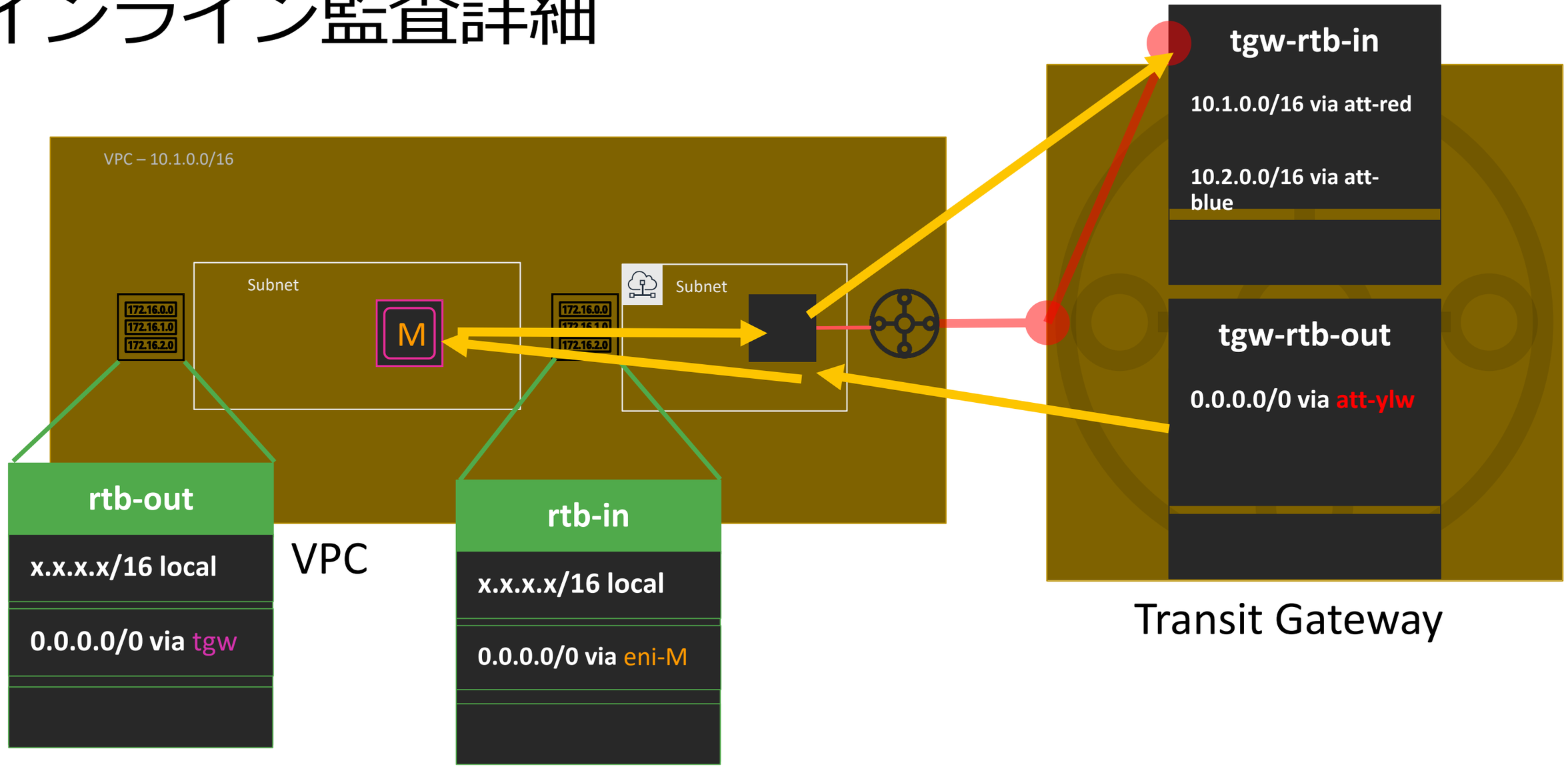
# インライン監査詳細



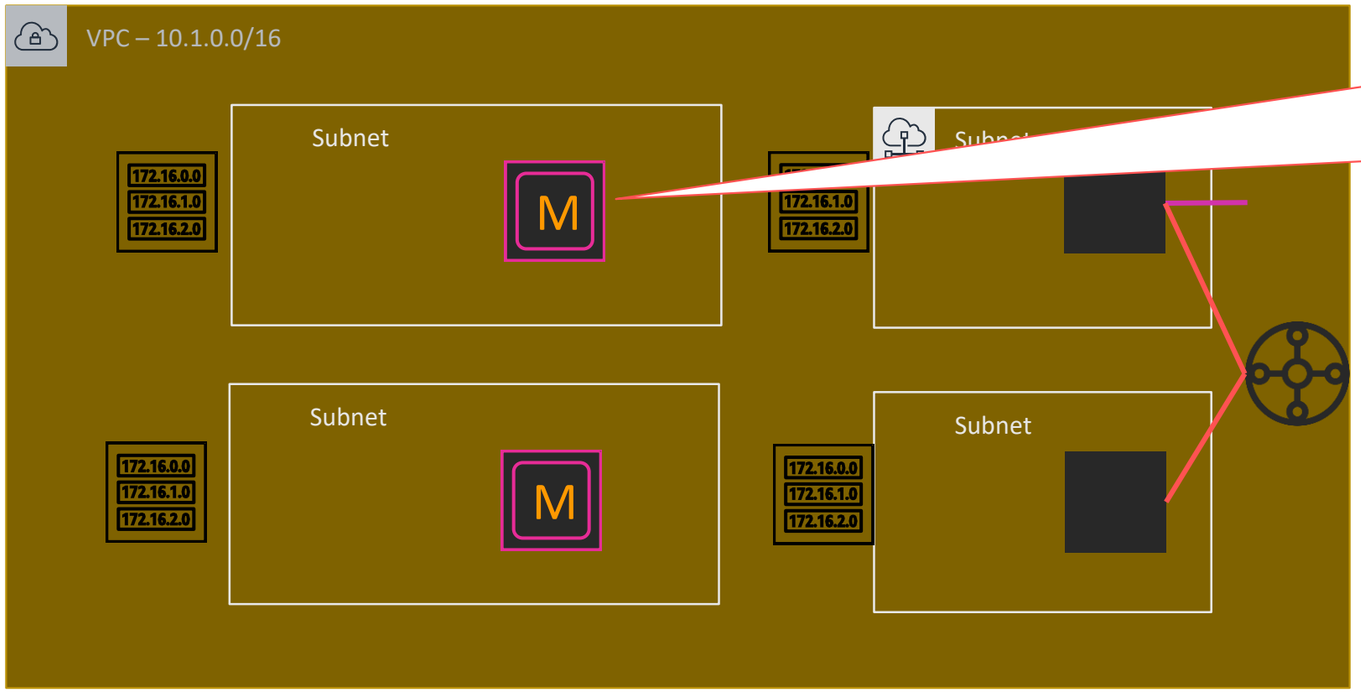
# インライン監査詳細



# 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

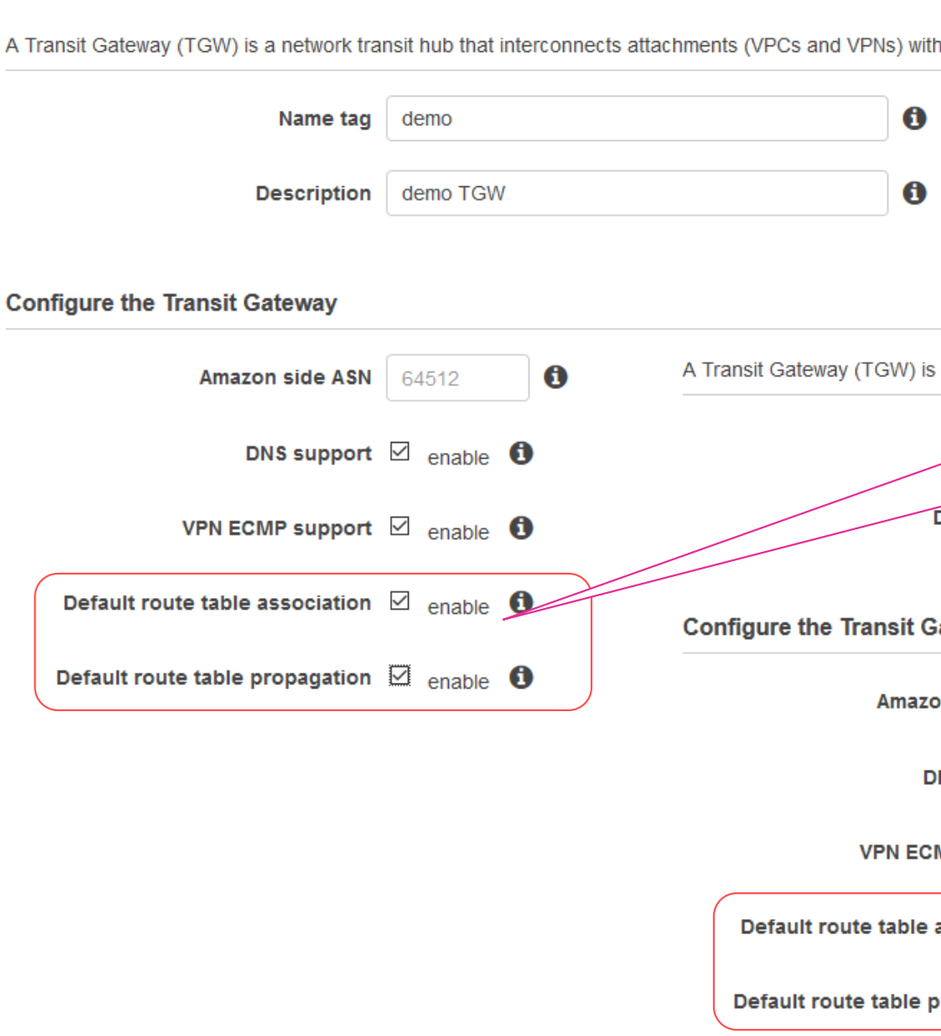
注意するところ

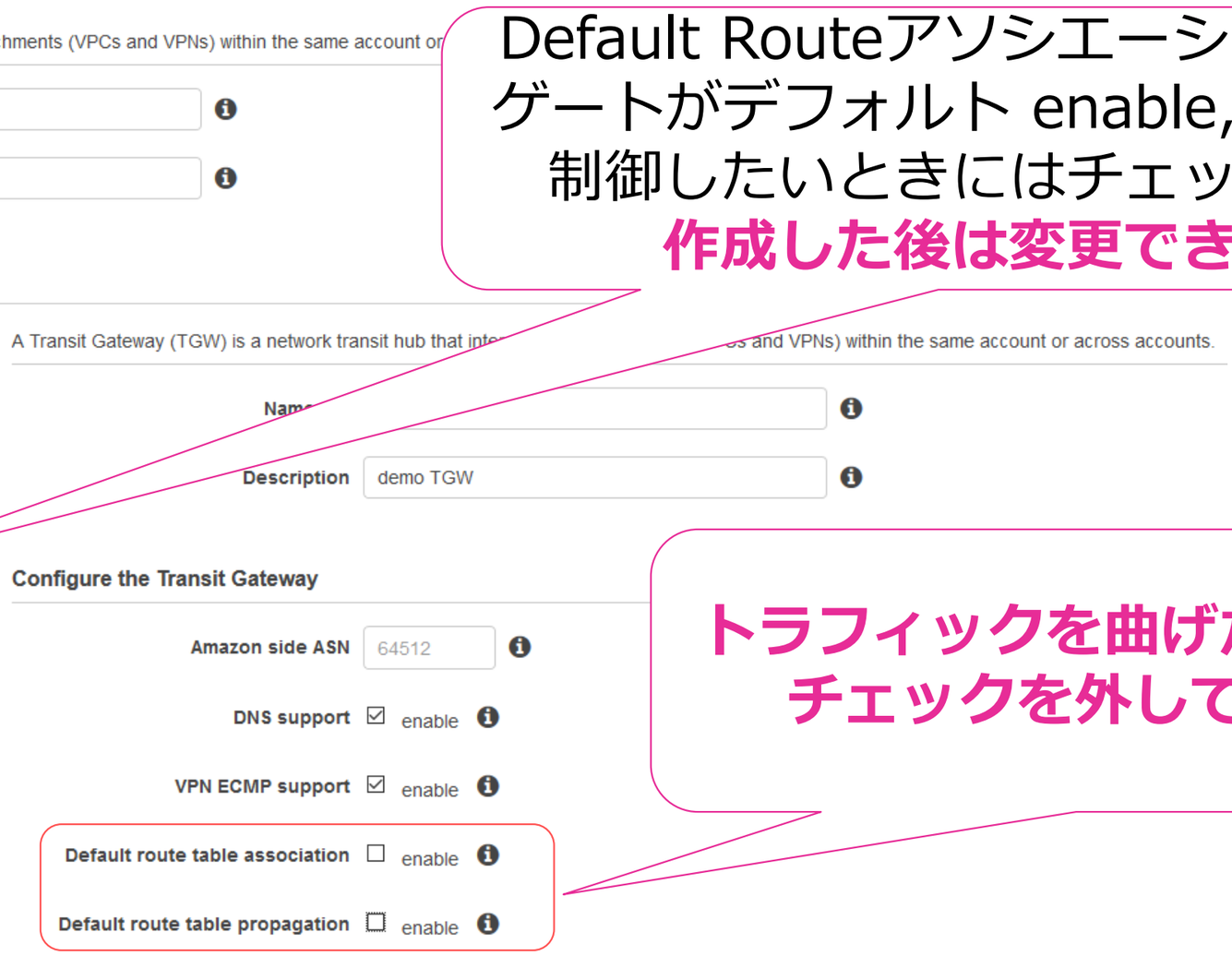
新機能: Transit GatewayとDirect Connectの連携

まとめ

# 注意するところ

# Transit Gateway作成時の注意




Default Routeアソシエーションとプロパゲートがデフォルト 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。**

**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。**

aws SUMMIT

# 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

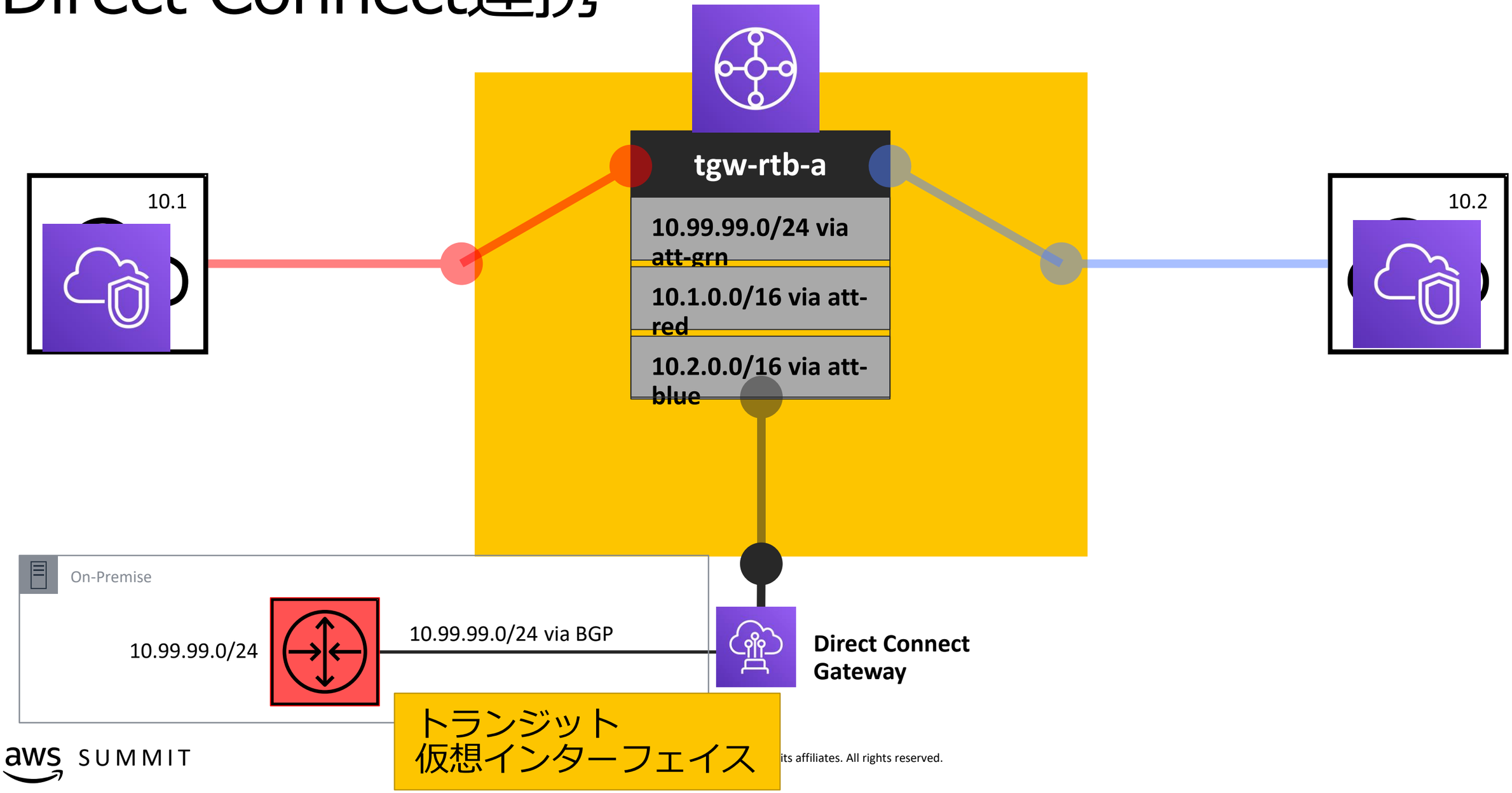
新機能: Transit GatewayとDirect Connectの連携

まとめ

# 新機能: Transit GatewayとDirect Connectの連携

aws SUMMIT

# Direct Connect連携



# Direct Connect連携

# 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

aws SUMMIT

# 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

aws SUMMIT

# 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。**

aws SUMMIT