[AWS Black Belt Online Seminar]
AWS Gateway Load Balancer

サービスカットシリーズ

Solutions Architect 藤井拓
2021/3/31

AWS 公式 Webinar
https://amzn.to/JPWebinar

過去資料
https://amzn.to/JPArchive

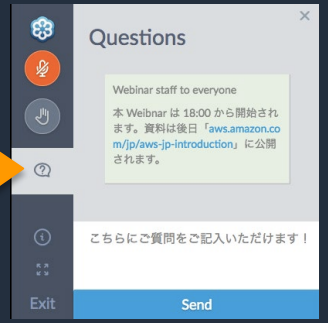
AWS Black Belt Online Seminar とは

「サービス別」「ソリューション別」「業種別」のそれぞれのテーマに分かれて、アマゾン ウェブ サービス ジャパン株式会社が主催するオンラインセミナーシリーズです。

質問を投げることができます！

- 書き込んだ質問は、主催者にしか見えません
- 今後のロードマップに関するご質問は
  お答えできませんのでご了承下さい

① 吹き出しをクリック
② 質問を入力
③ Sendをクリック



Twitter 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2021年3月31日現在のサービス内容および価格についてご説明しています。最新の情報はAWS公式ウェブサイト(http://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。

- AWS does not offer binding price quotes. AWS pricing is publicly available and is subject to change in accordance with the AWS Customer Agreement available at http://aws.amazon.com/agreement/. Any pricing information included in this document is provided only as an estimate of usage charges for AWS services based on certain information that you have provided. Monthly charges will be based on your actual use of AWS services, and may vary from the estimates provided.

自己紹介

名前： 藤井 拓 (ふじい たく)

所属：

アマゾン ウェブ サービス ジャパン株式会社
レディネスソリューション本部
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

経歴：

前職は外資系通信機器メーカにてネットワーク機器に関わるプリセールスSE
を長年担当しておりました。

好きなAWSサービス：

AWS Transit Gateway, AWS Gateway Load Balancer, AWS Marketplace

本セミナーで学習できること

- AWS Gateway Load Balancer 概要
- AWS Gateway Load Balancerトラフィックフロー
- AWS Gateway Load BalancerのAZの考え方を

本日のアジェンダ

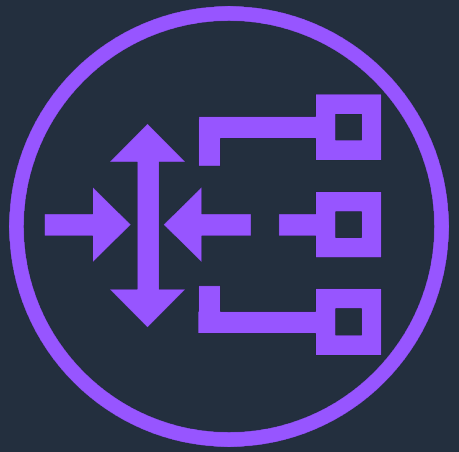
- AWS Gateway Load Balancer 概要
- AWS Gateway Load Balancer使用するには
- 参考アーキテクチャ例及びAZの考え方
- Transit Gateway Appliance modeとは
- クロスゾーン負荷分散
- まとめ

Gateway Load Balancer 概要

INTRODUCING

Gateway Load Balancer

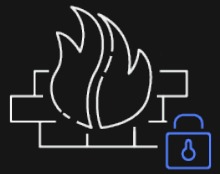
- シンプル化を通じてアプライアンス導入を迅速に
- 伸縮性を持つスケーラビリティでコストパフォーマンス改善
- アプライアンスの可用性を向上
- 主要アプライアンス各社がサポート可能



aws

ネットワークアプライアンス

ネットワーク
トラフィックに
対して透過型で
あること

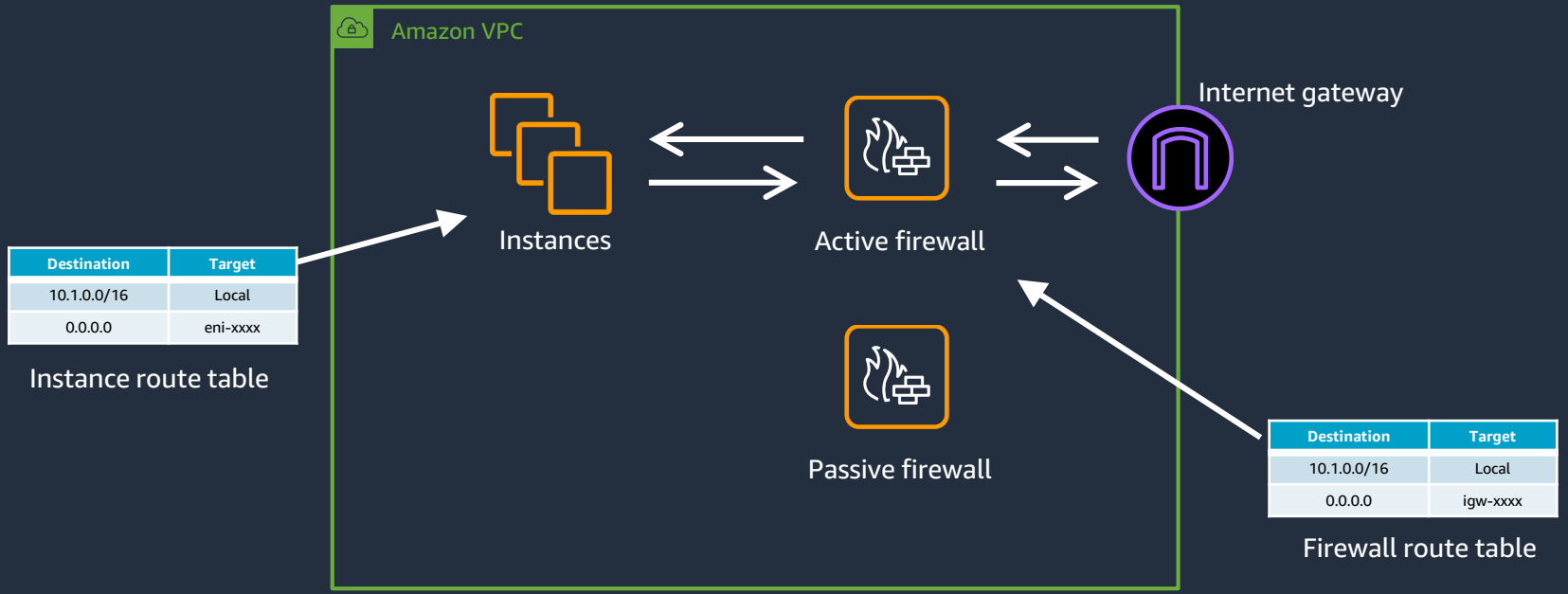


セキュリティー、
監視、分析等の
用途の対応

ポリシー及び運
用の専門知識へ
の投資

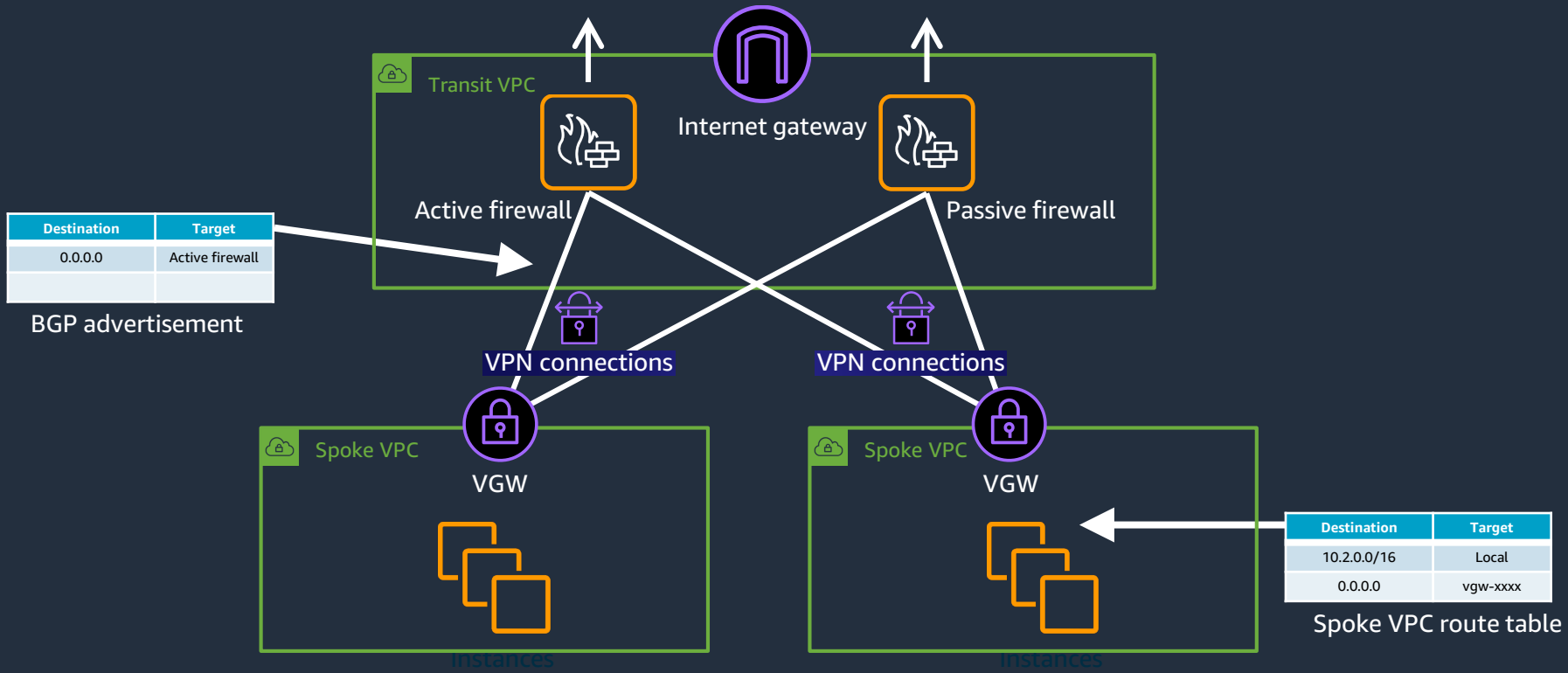
AWSやハイブリッド環境で同じネットワークアプライアンスがご利用可能

従来のネットワークアプライアンスの展開モデル



- アプライアンスのインスタンスを監視する仕組みが必要
- Lambdaなど使用しルーティングテーブルをいじる仕組みが必要

従来のネットワークアプライアンスの展開モデル

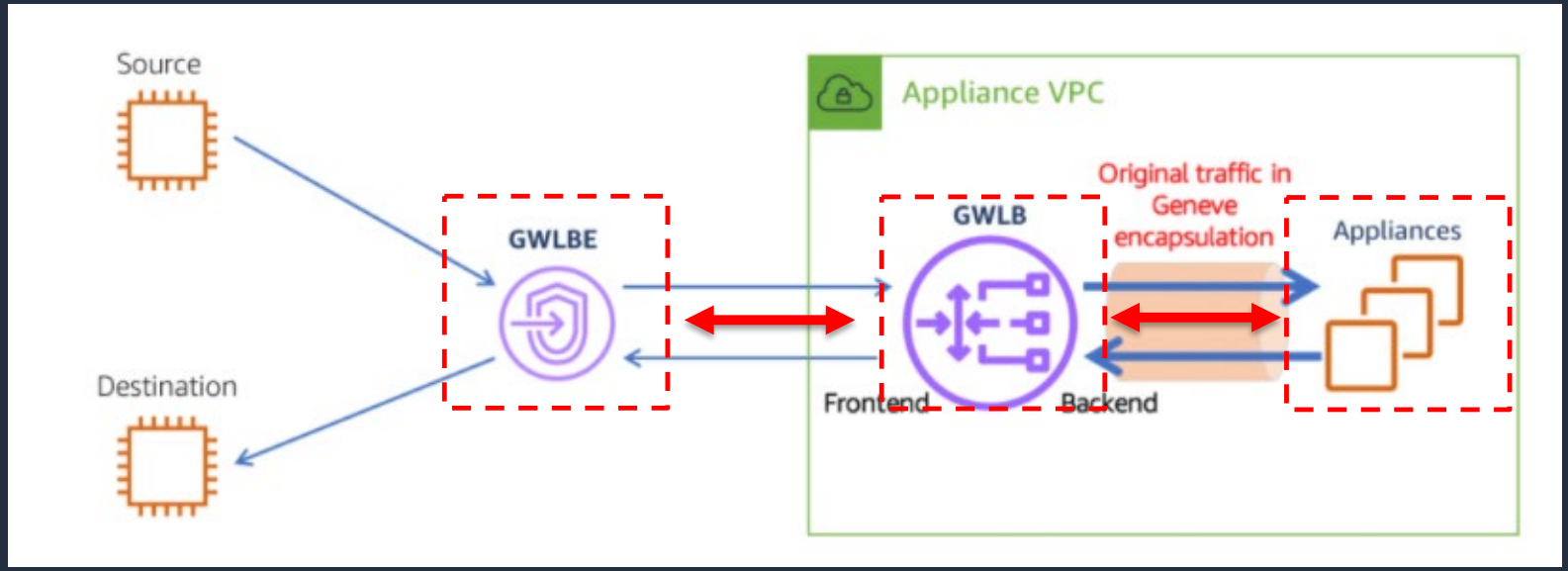


- ネットワーク構成の複雑性
- VPNを使用による帯域の制限、及びアプライアンスへの負荷影響

Gateway Load Balancer 概要

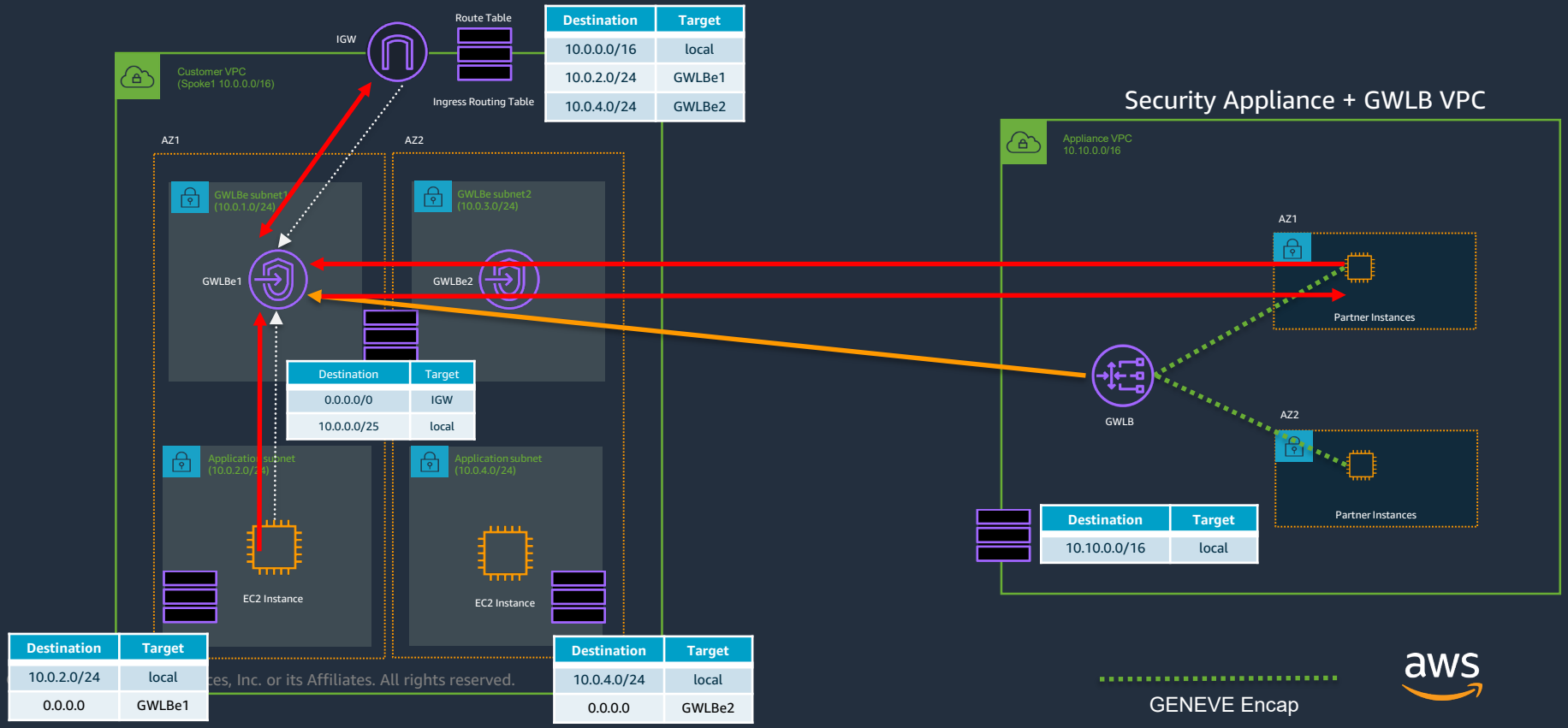
コンポーネント
- ルートテーブル内のNext Hopとして指定可能な新規VPCエンドポイント
- Gateway Load Balancer (GWLB) – L3ゲートウェイとL4ロードバランサの機能を兼ね備えた新タイプのロードバランサ
- 両コンポーネント共にAWS Hyperplane上で動作

メリット
- アプライアンスの水平スケール/可用性を実現
- ネットワークトラフィックに対して透過的な検査 (ソーストラフィックへの変更なし)
- セキュリティとユーザー管理ドメインを分離、異なるVPCとAWSアカウント間で共有可能

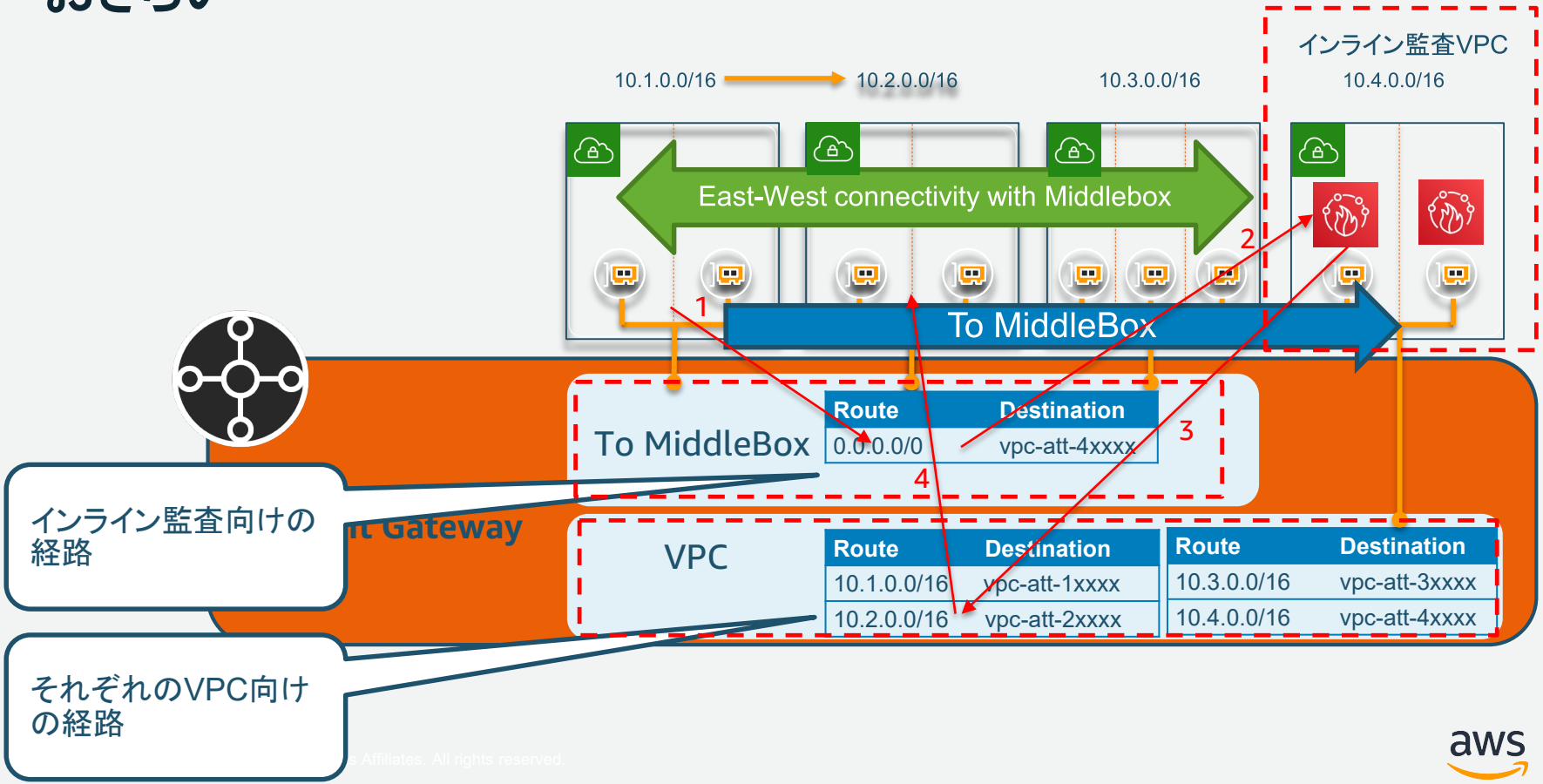


今後のネットワークアプライアンスの展開モデル

✓ VPCからのInternetトラフィックのインスペクションの一括管理

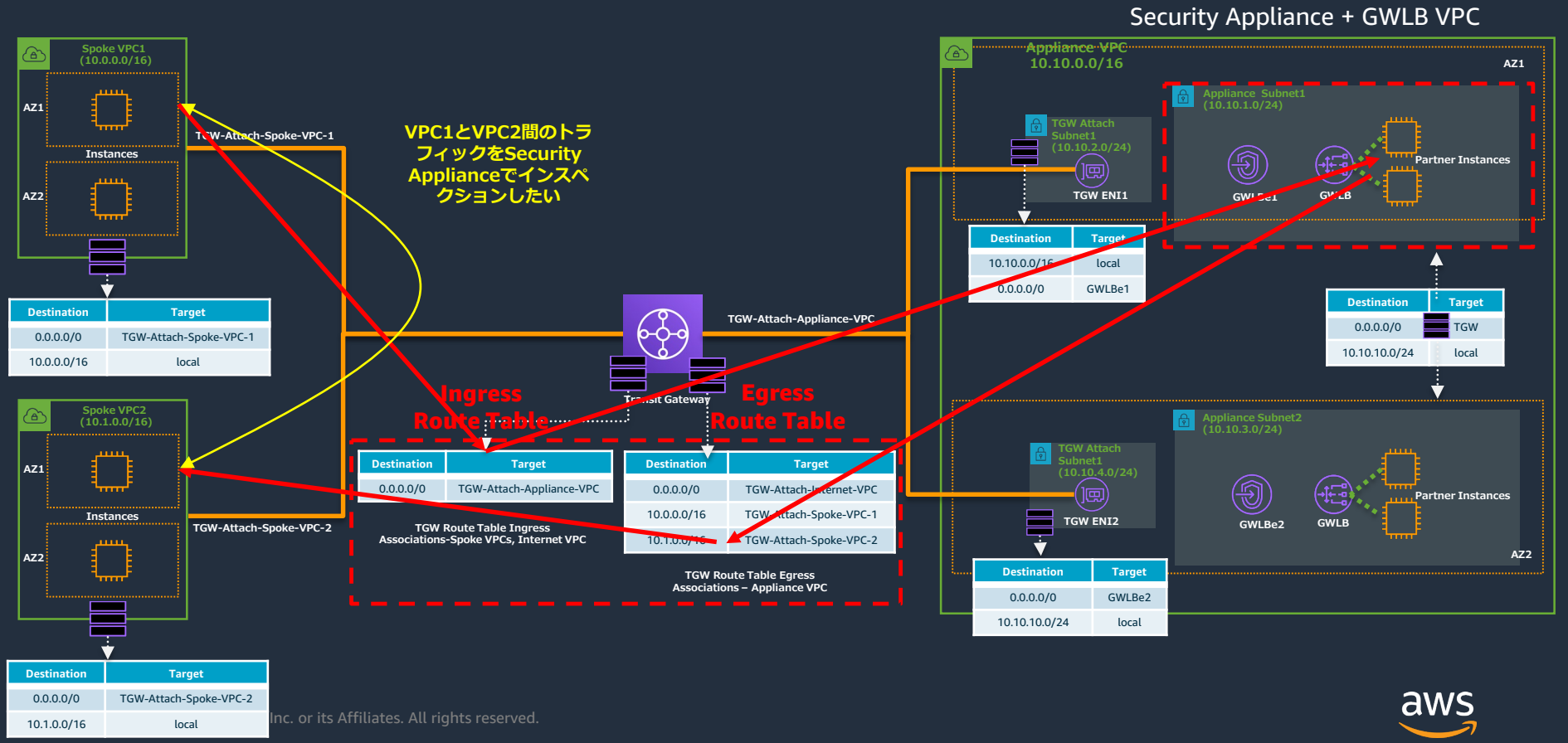


VPC間のトラフィックをインライン監査するRoute Domains おさらい



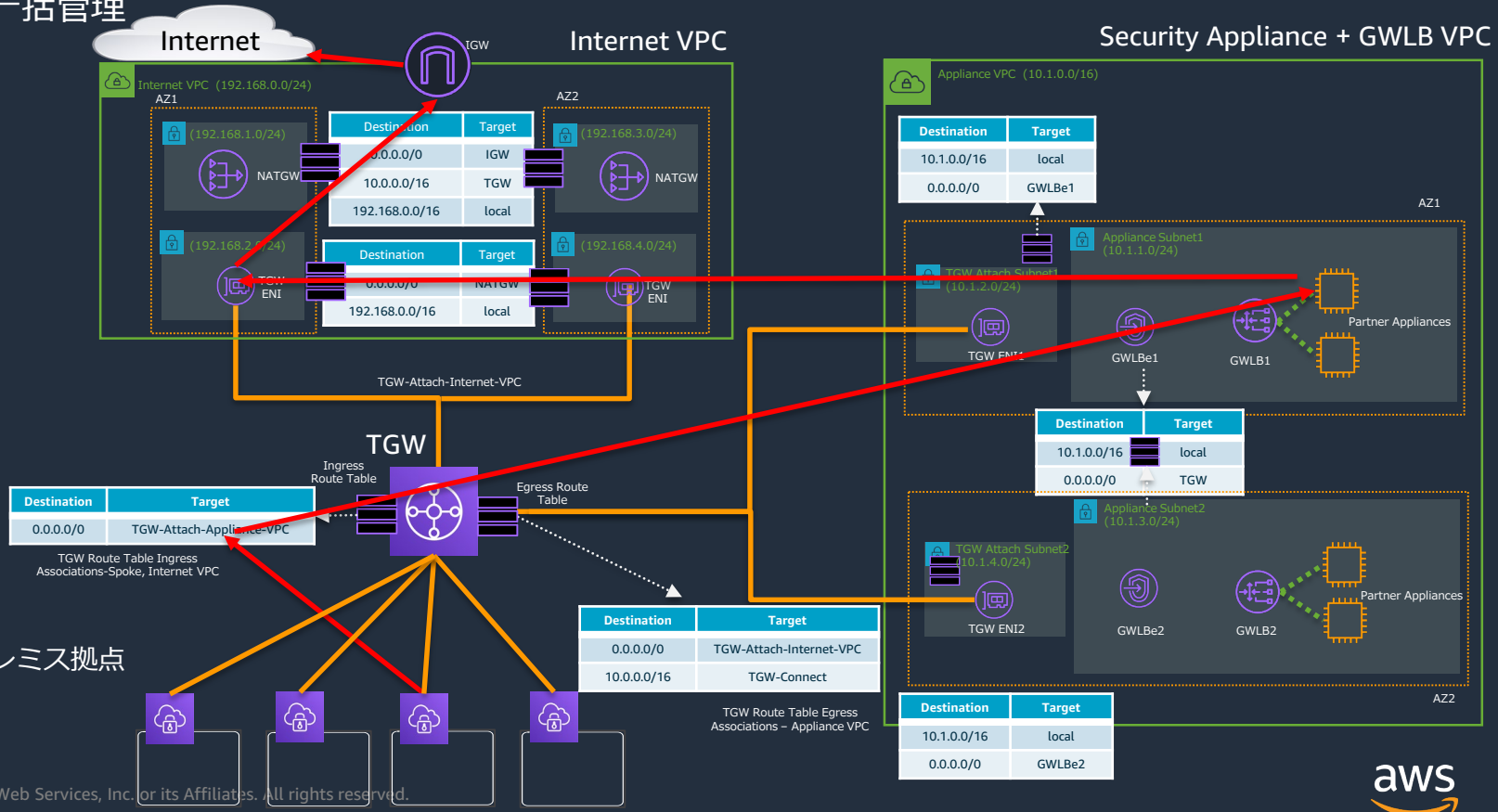
今後のネットワークアプライアンスの展開モデル

✓ TGW及びGWLBを使用したVPC間トラフィックのインスペクションの一括管理



今後のネットワークアプライアンスの展開モデル

✓ TGW及びGWLBを使用したオンプレミス拠点からのInternetトラフィックのインスペクションの一括管理



AWS Gateway Load Balancer パートナー様一覧

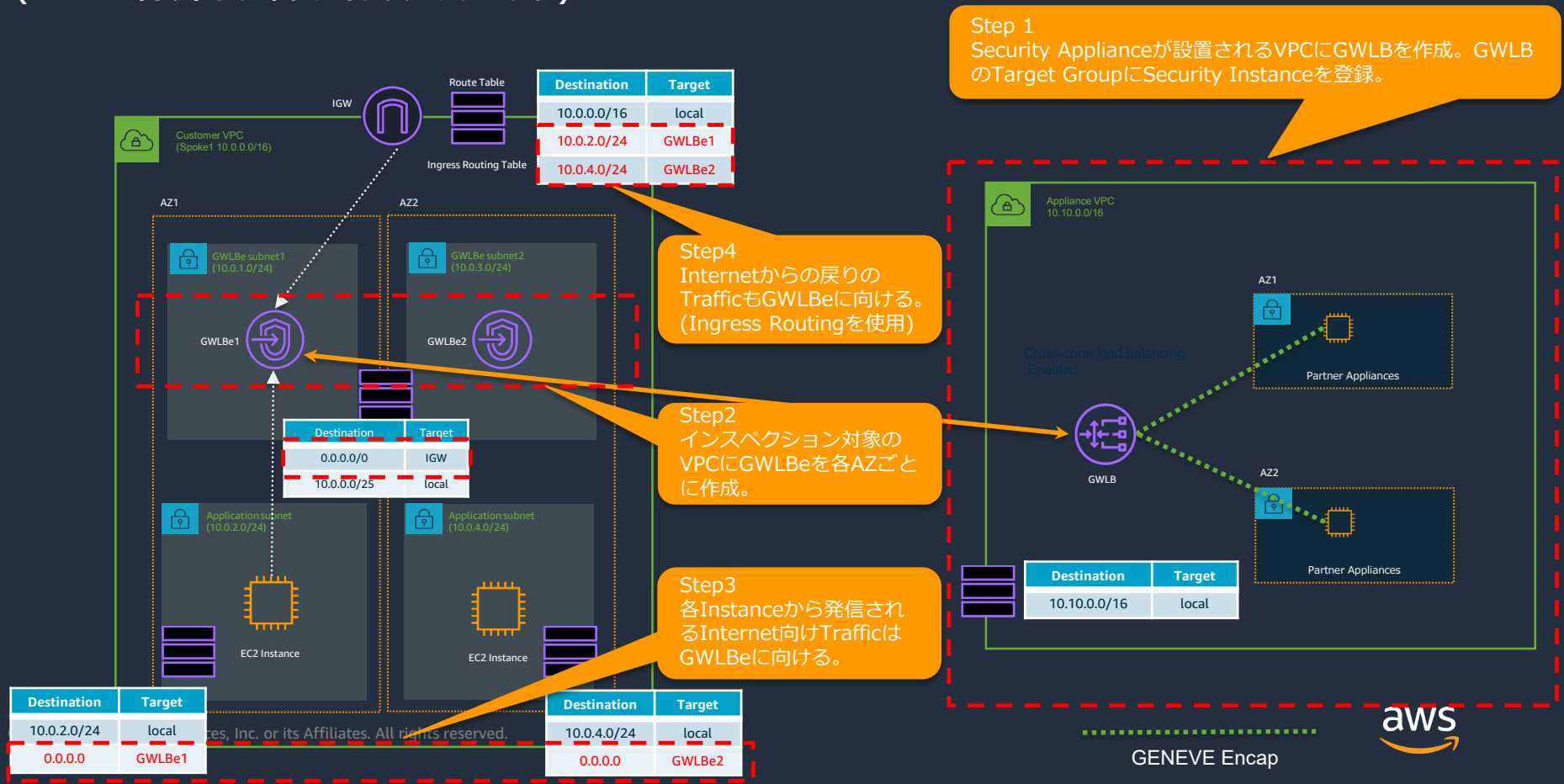
aws

Gateway Load Balancer使用するには

Gateway Load Balancerを使用するには

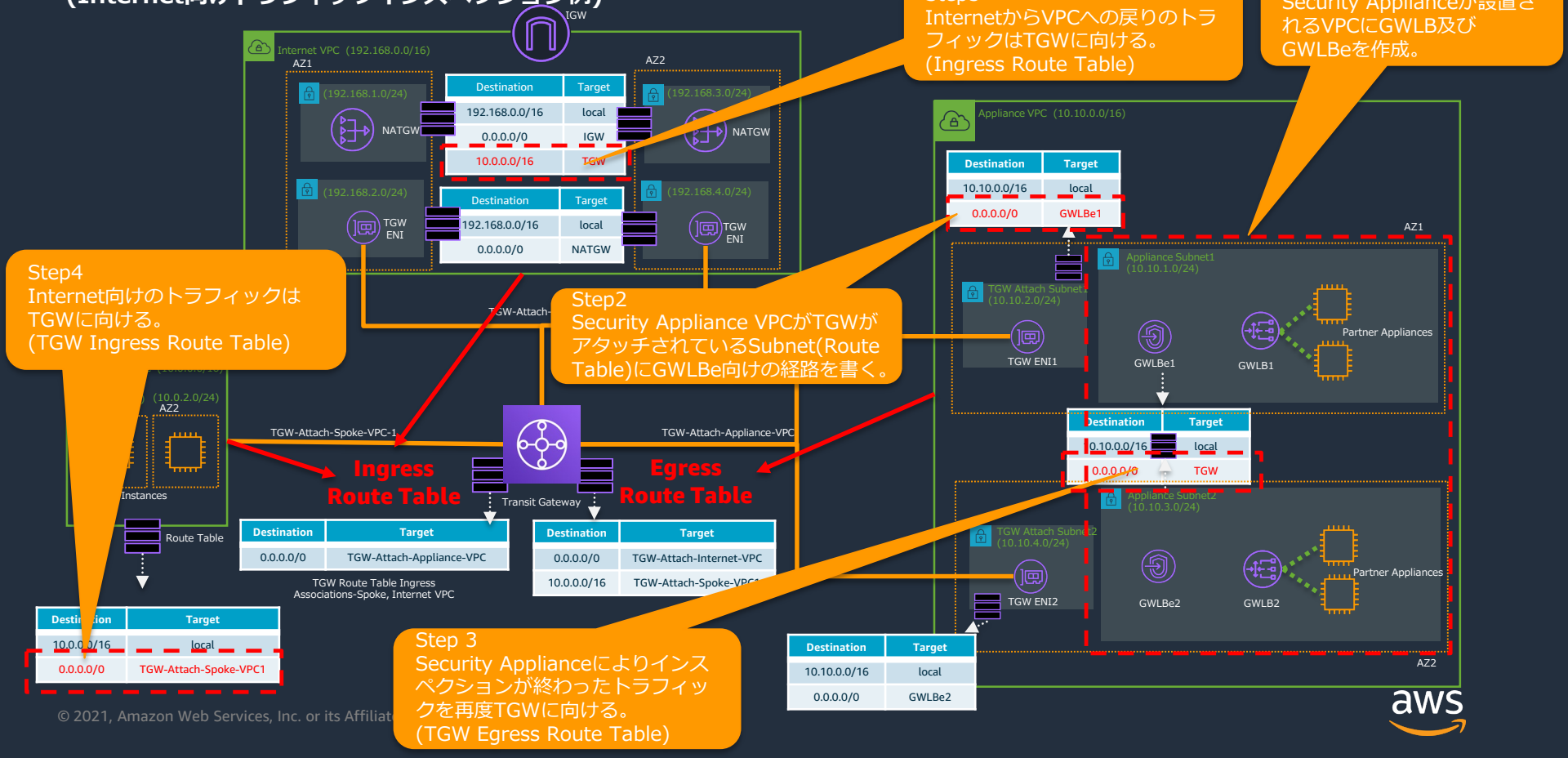
Routing設定の流れ（Ingress Routing）

(Internet向けトラフィックインスペクション例)



Routing設定の流れ（Transit Gatewayと組合せ）

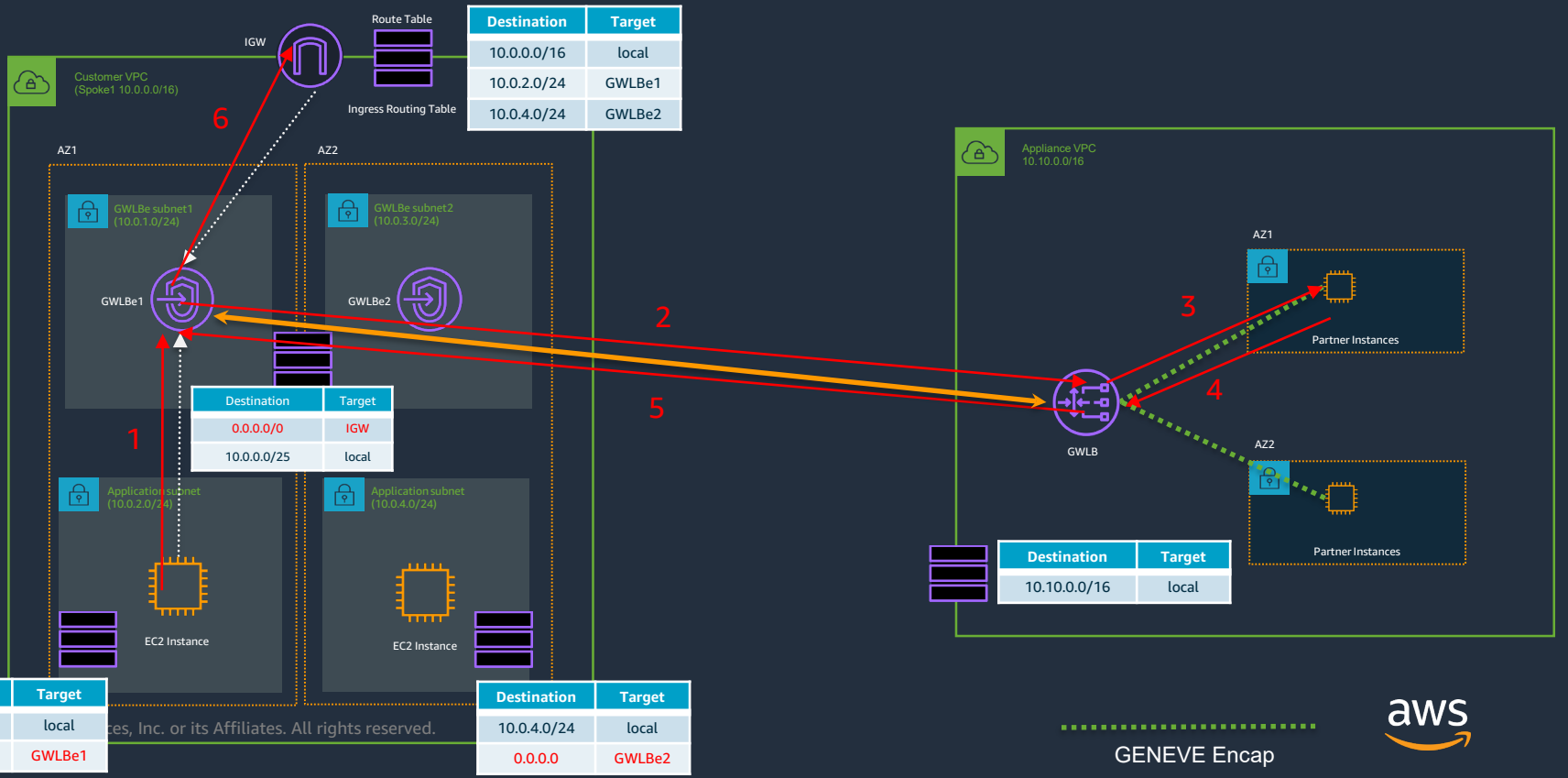
(Internet向けトラフィックインスペクション例)



参考アーキテクチャ構成例

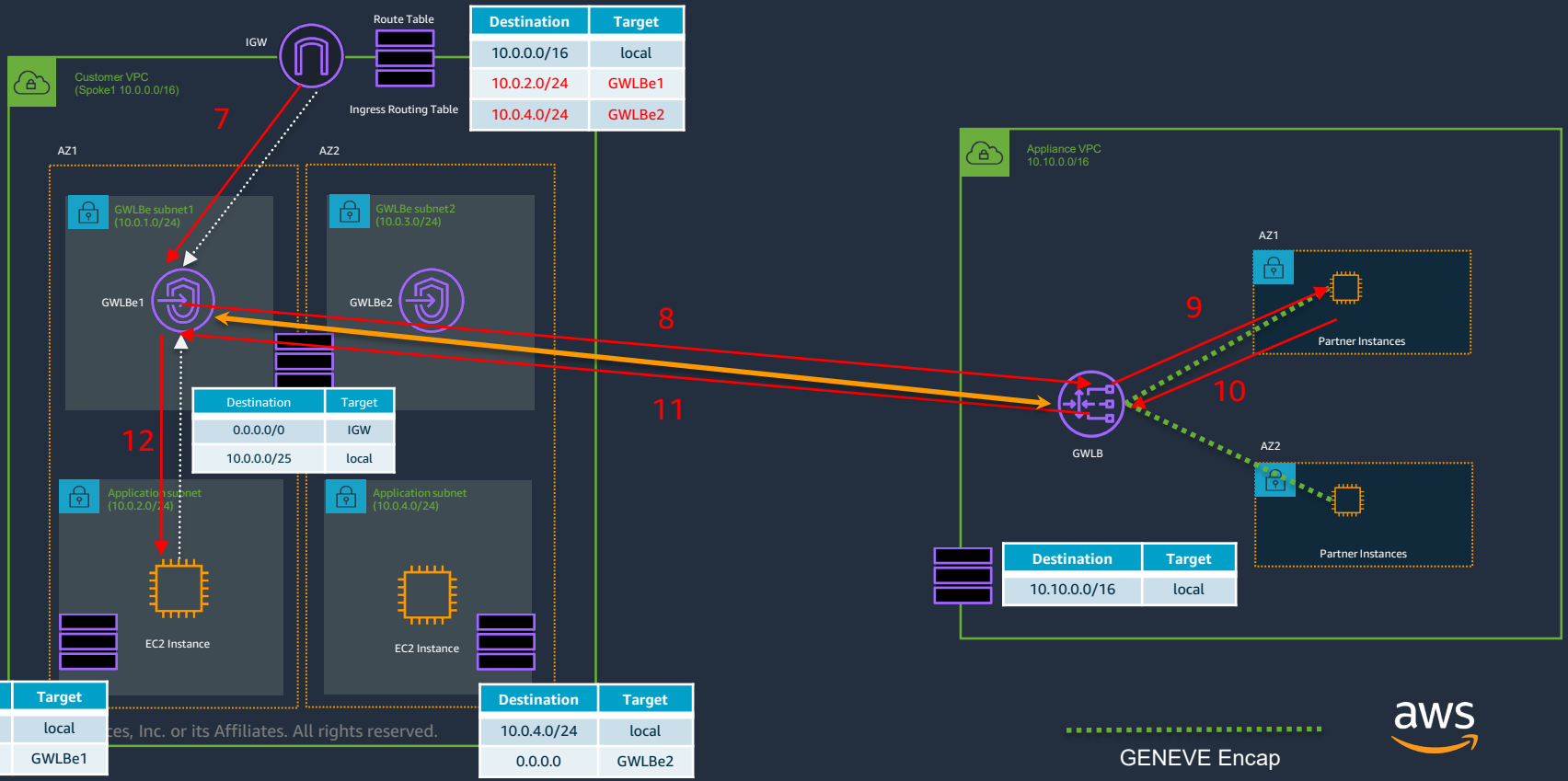
トラフィックフロー例1 Ingress Routing（行き）

(AZ1より発信したInternet向けトラフィックインスペクション例)



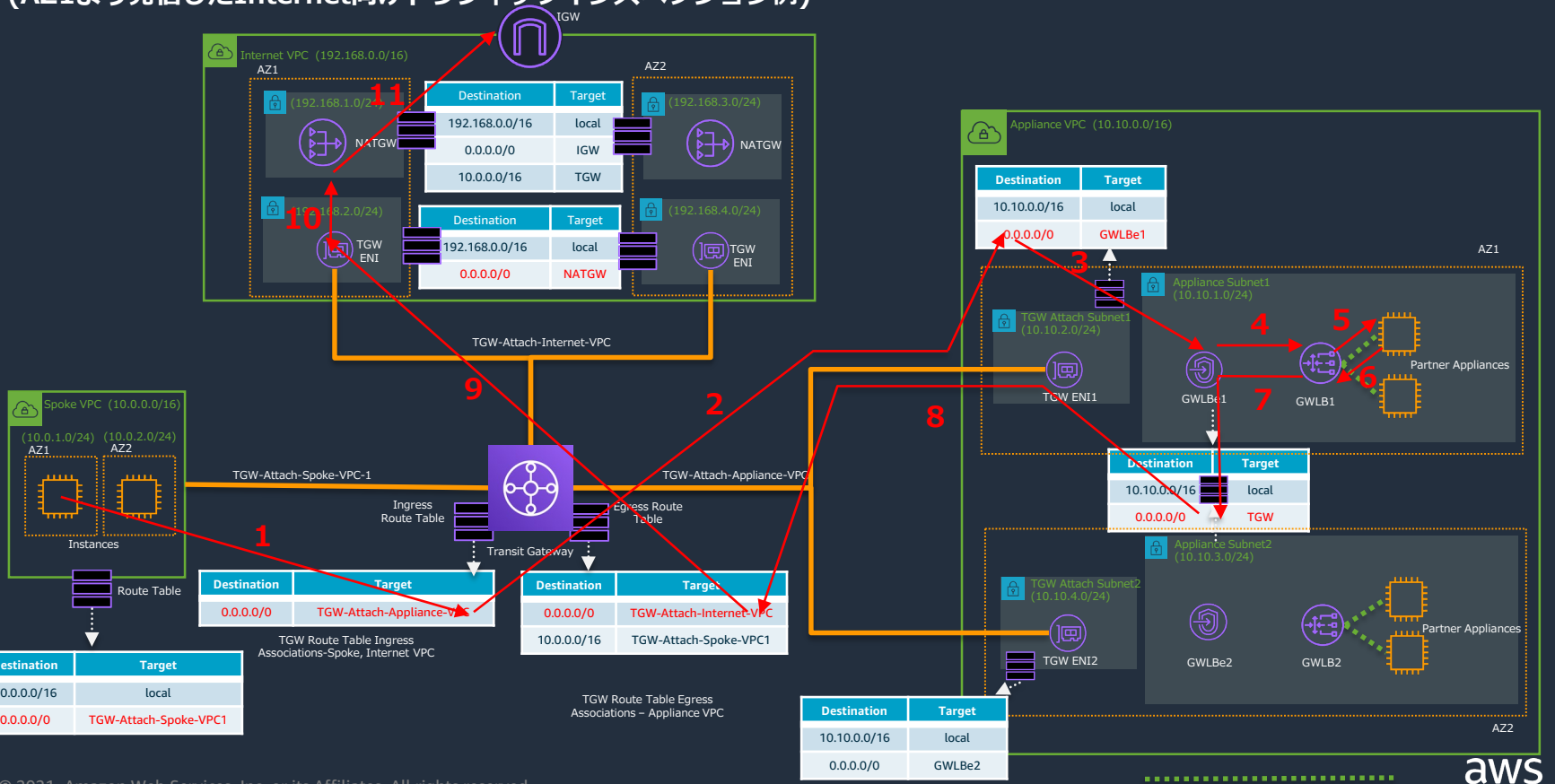
トラフィックフロー例1 Ingress Routing（戻り）

(AZ1より発信したInternet向けトラフィックインスペクション例)



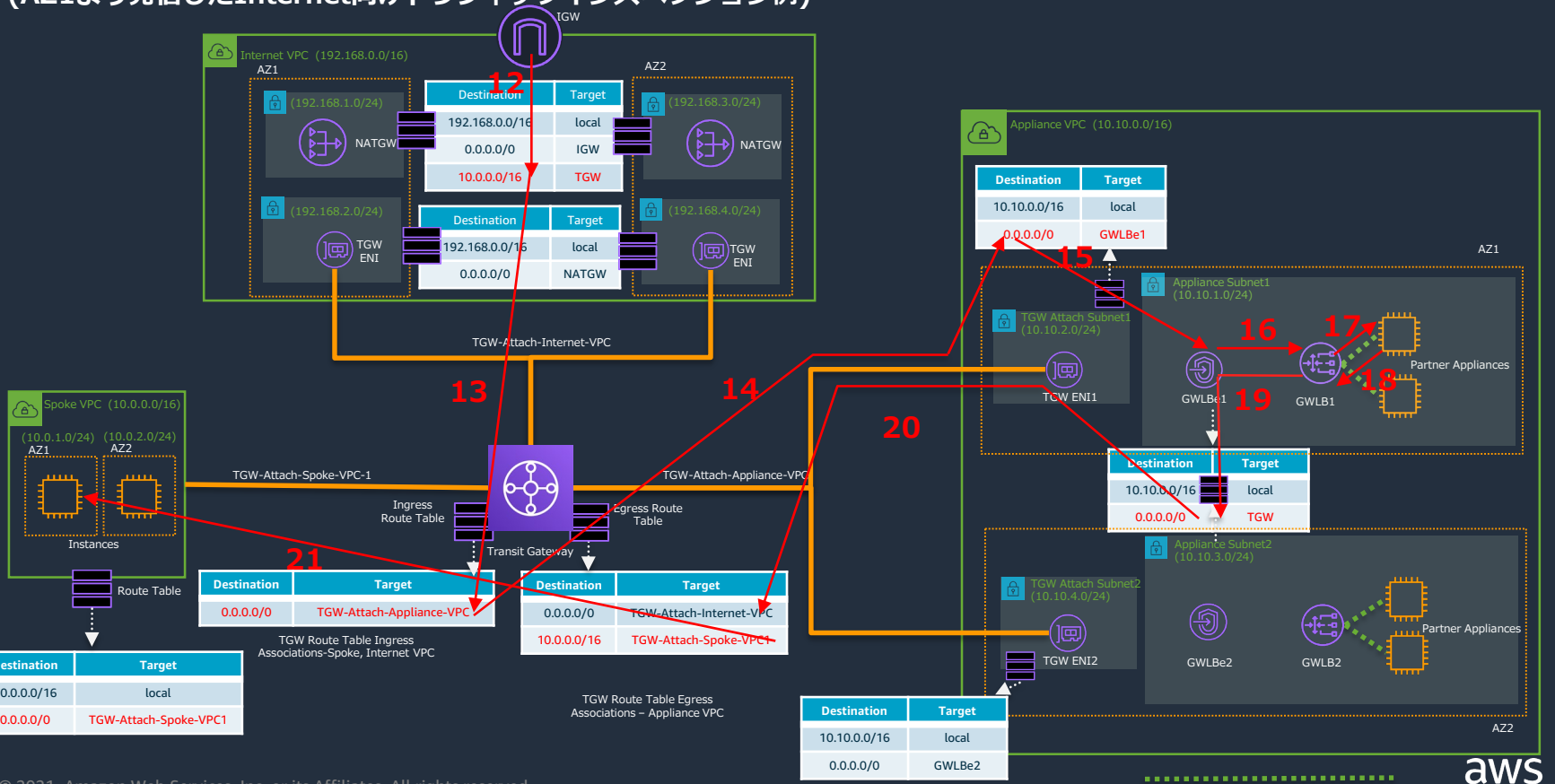
トラフィックフロー例2 Transit Gatewayと組合せ（行き）

(AZ1より発信したInternet向けトラフィックインスペクション例)



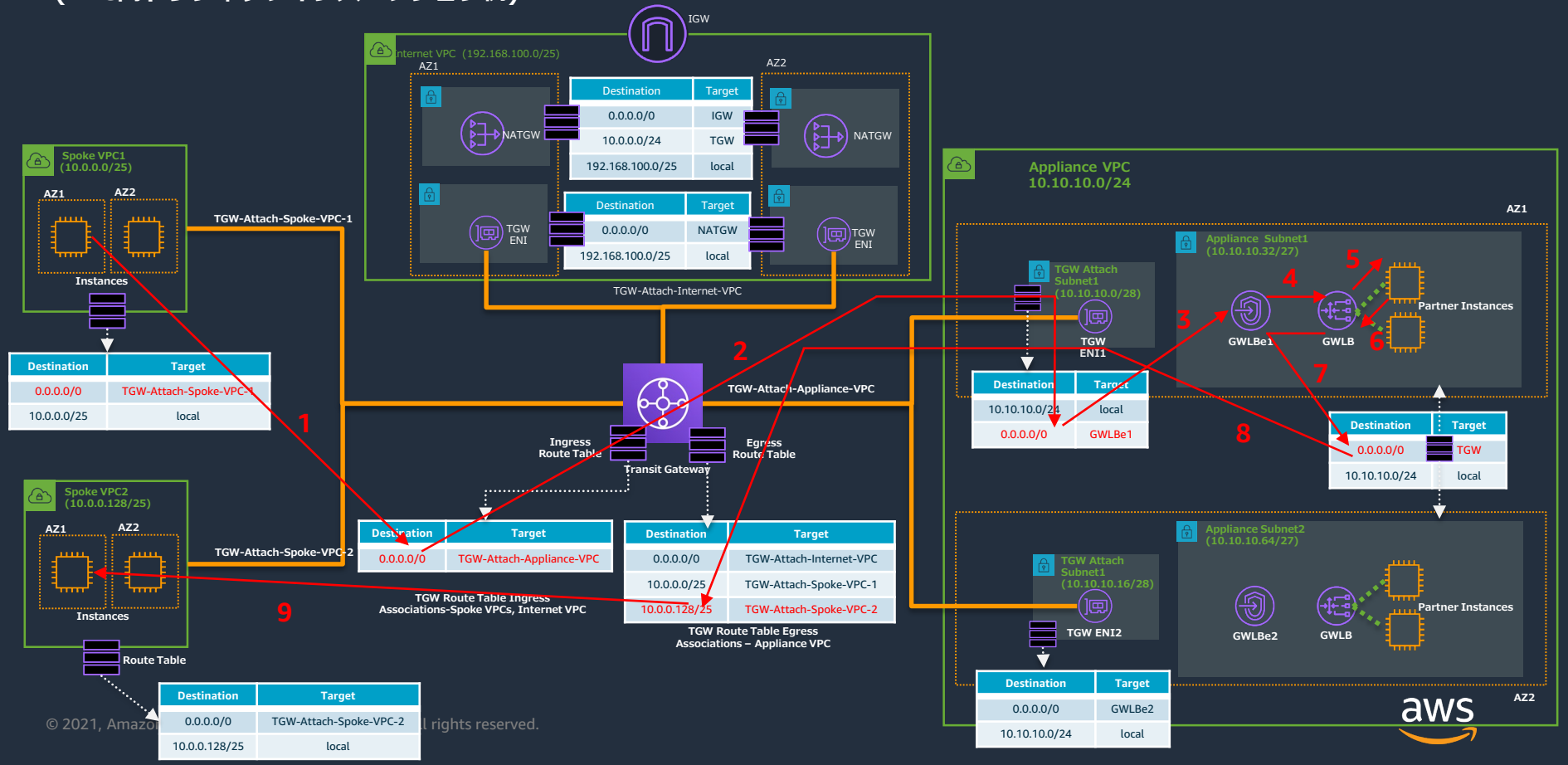
トラフィックフロー例2 Transit Gatewayと組合せ（戻り）

(AZ1より発信したInternet向けトラフィックインスペクション例)



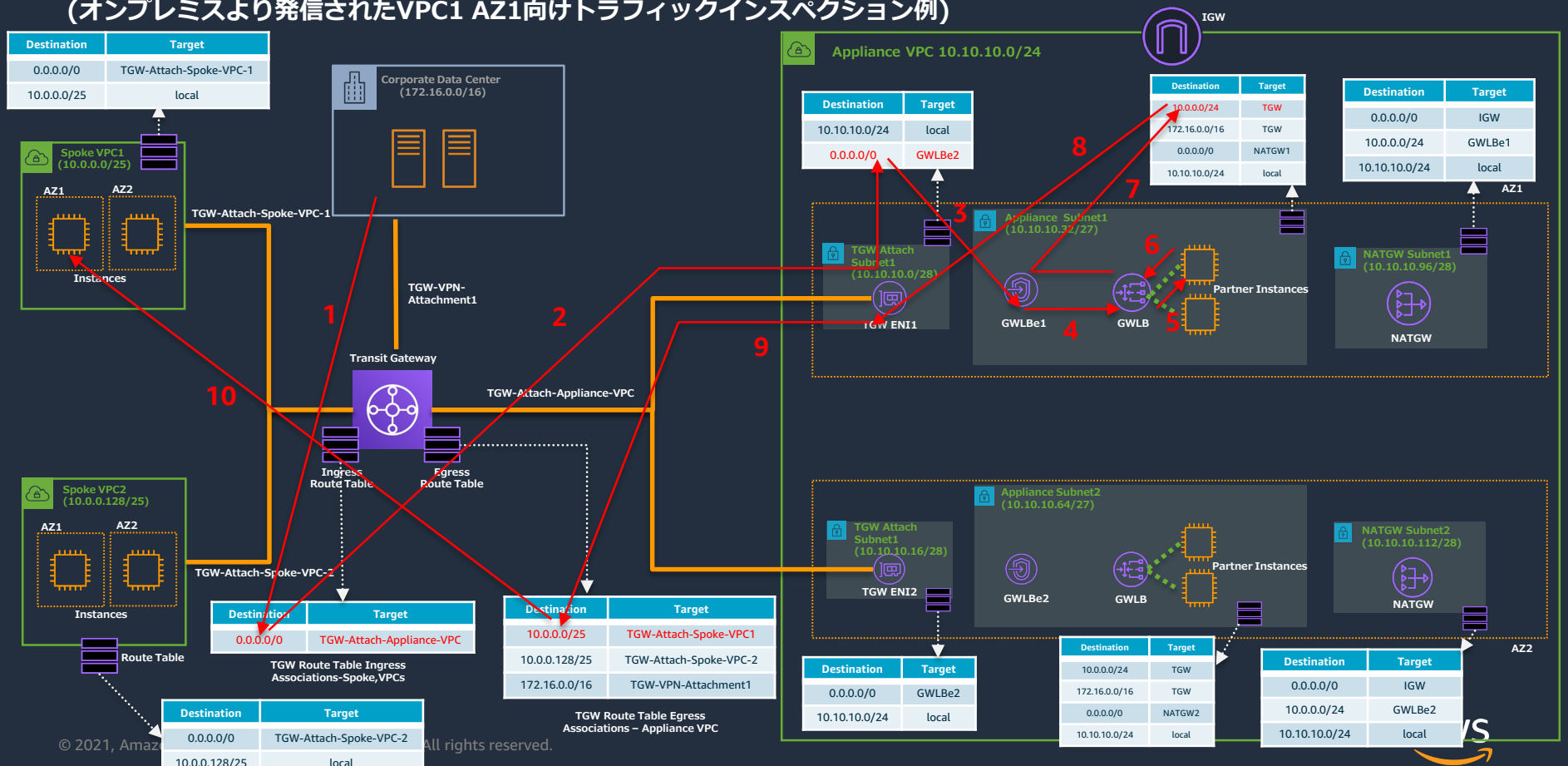
トラフィックフロー例3 Transit Gatewayと組合せ

(VPC間トラフィックインスペクション例)



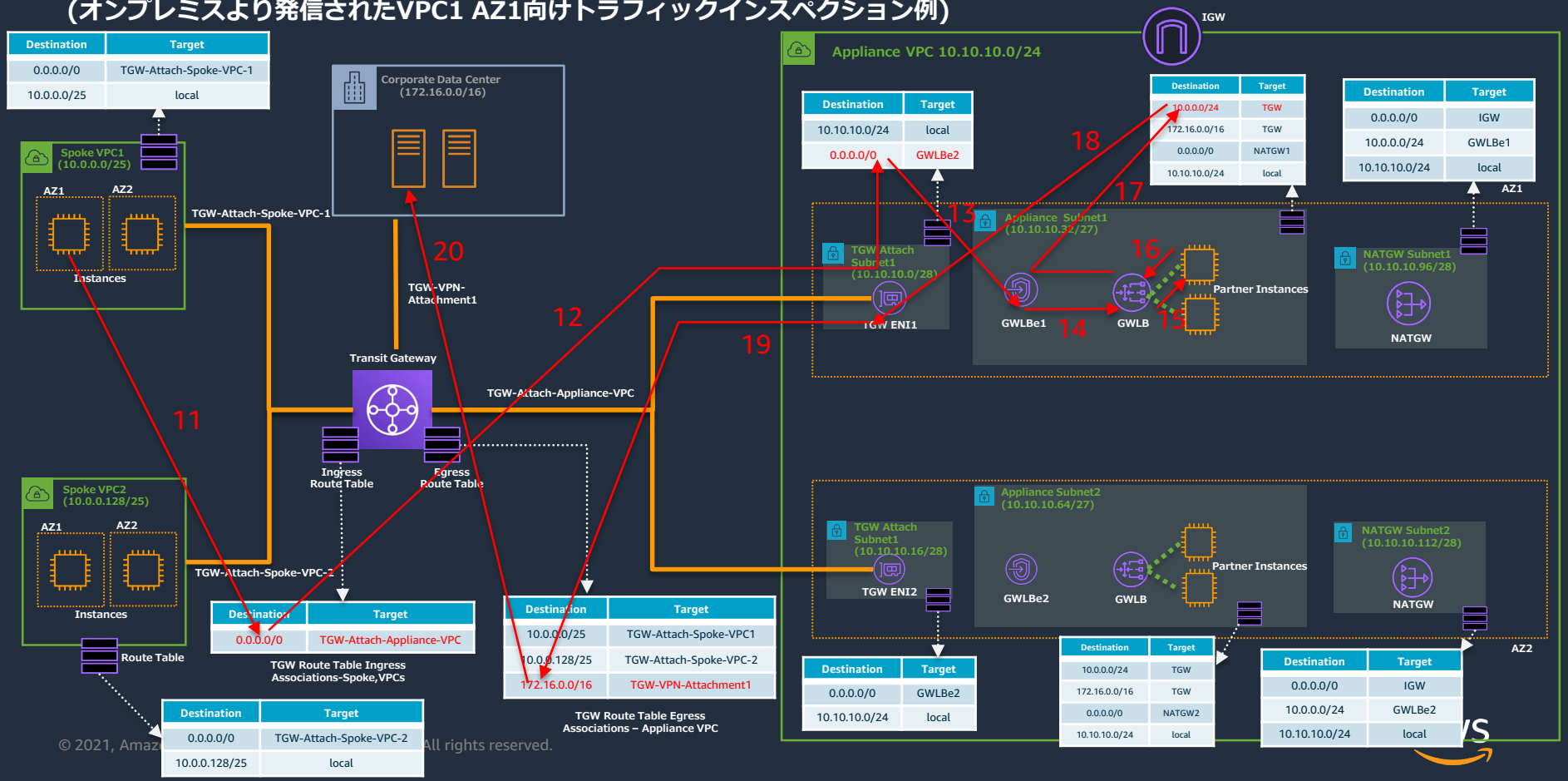
トラフィックフロー例4 Transit Gatewayと組合せ（行き）

(オンプレミスより発信されたVPC1 AZ1向けトラフィックインスペクション例)



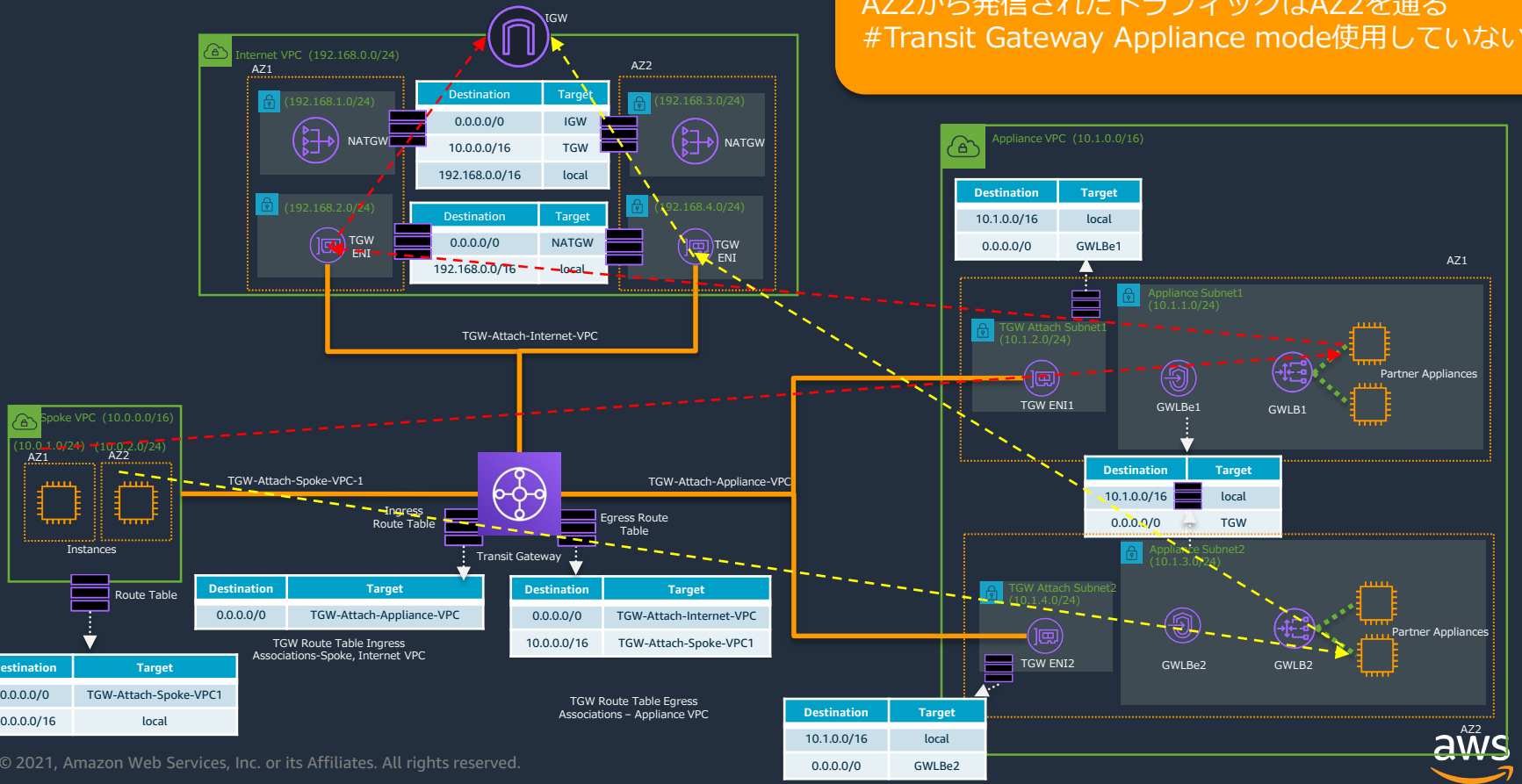
トラフィックフロー例4 Transit Gatewayと組合せ（戻り）

(オンプレミスより発信されたVPC1 AZ1向けトラフィックインスペクション例)



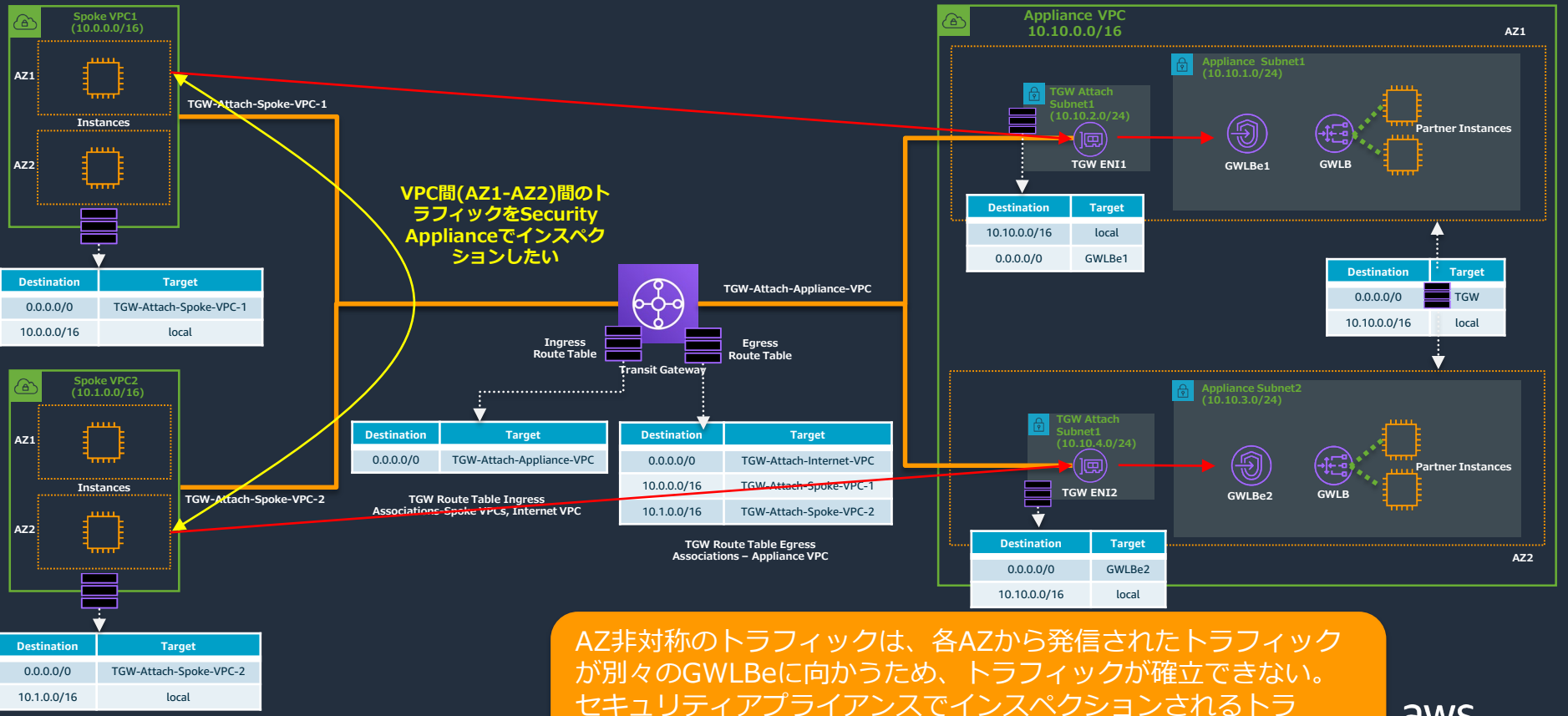
トラフィックフロー補足

基本AZ1から発信されたトラフィックは、AZ1を通り、
AZ2から発信されたトラフィックはAZ2を通る
#Transit Gateway Appliance mode使用していない場合



Transit Gateway Appliance modeとは

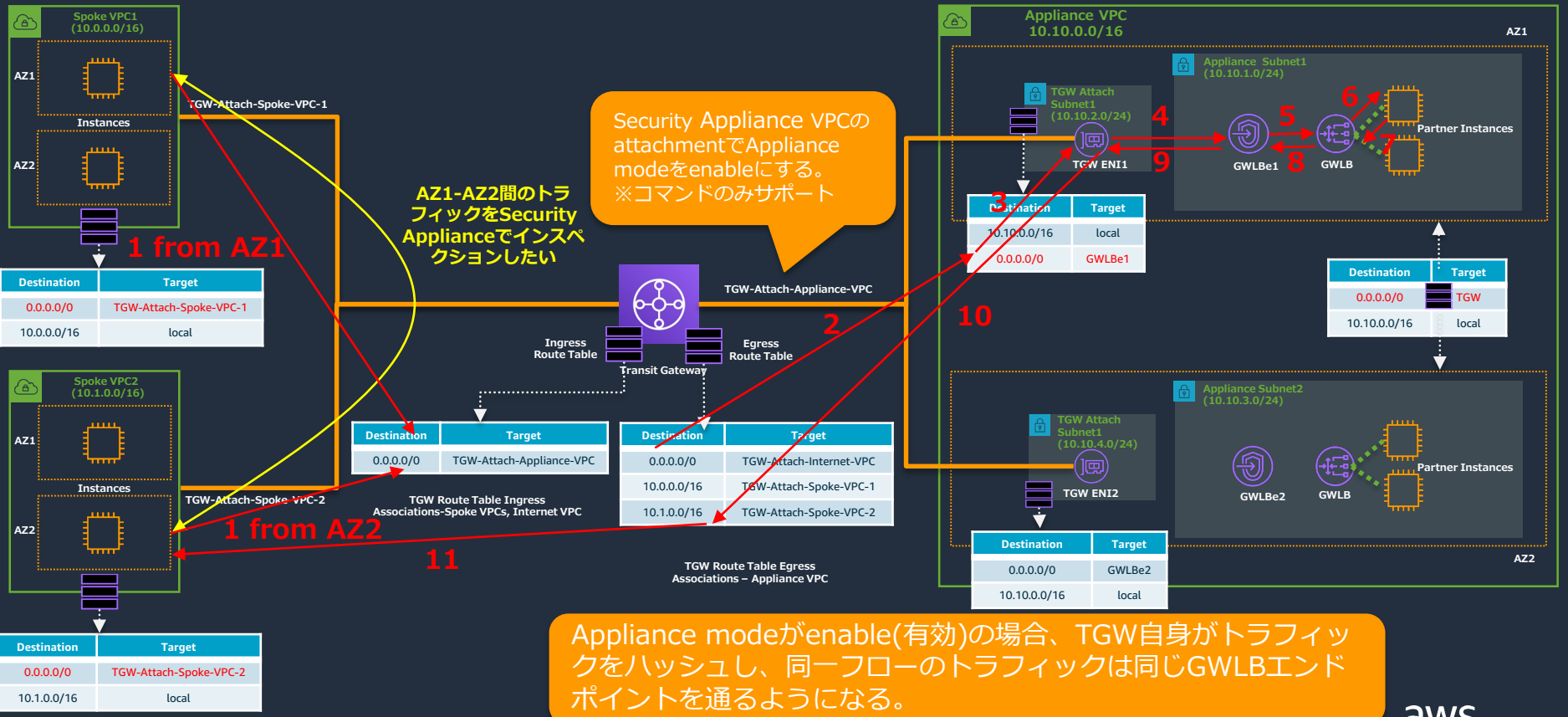
Transit Gateway Appliance mode disable（無効）



AZ非対称のトラフィックは、各AZから発信されたトラフィックが別々のGWLBeに向かうため、トラフィックが確立できない。セキュリティアプライアンスでインスペクションされるトラフィックフローは同じGWLBeを通る必要がある。

Transit Gateway Appliance mode enable（有効）

(AZを跨ぐトラフィック)

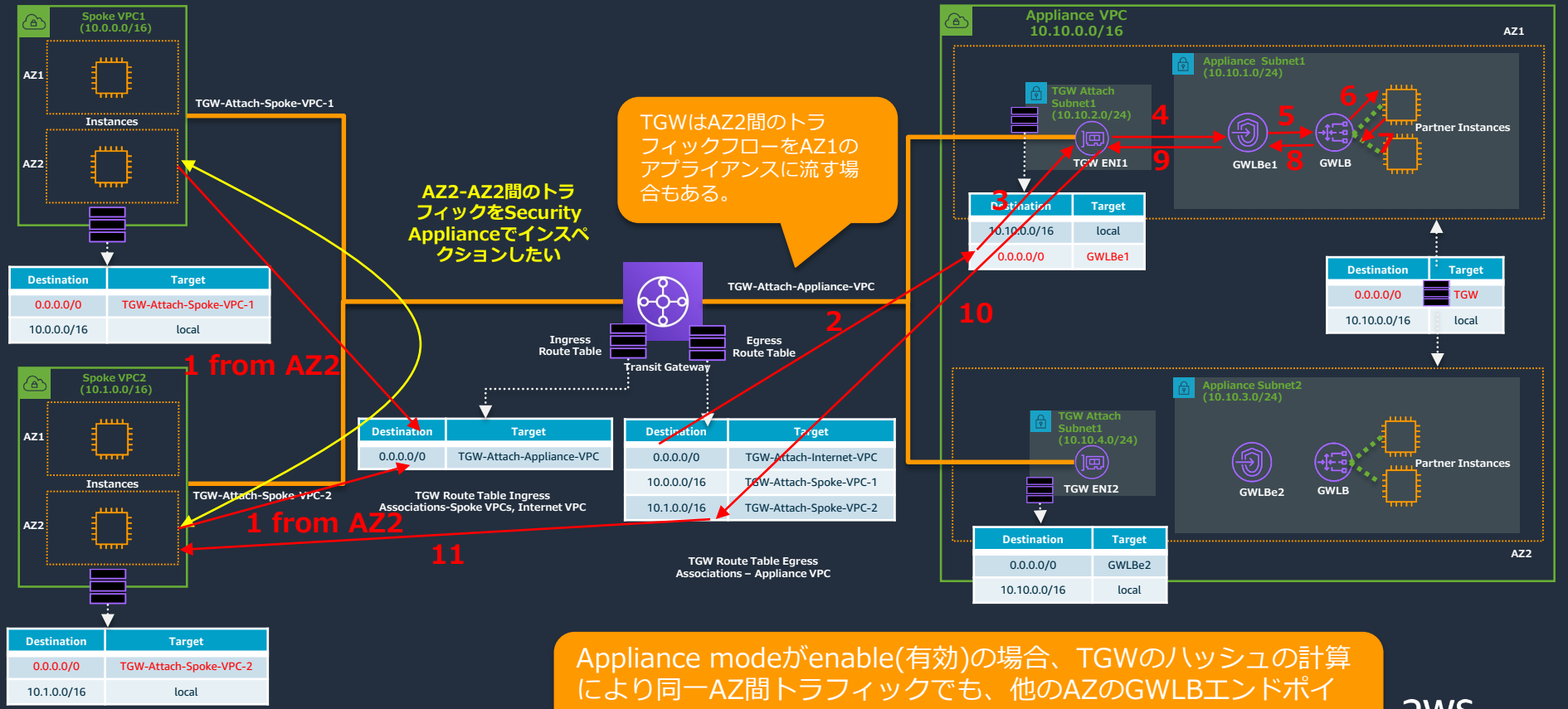


Appliance modeがenable(有効)の場合、TGW自身がトラフィックをハッシュし、同一フローのトラフィックは同じGWLBエンドポイントを通るようになる。

https://docs.aws.amazon.com/vpc/latest/tgw/transit-gateway-appliance-scenario.html

Transit Gateway Appliance mode enable（有効）

(同一AZ間トラフィック)



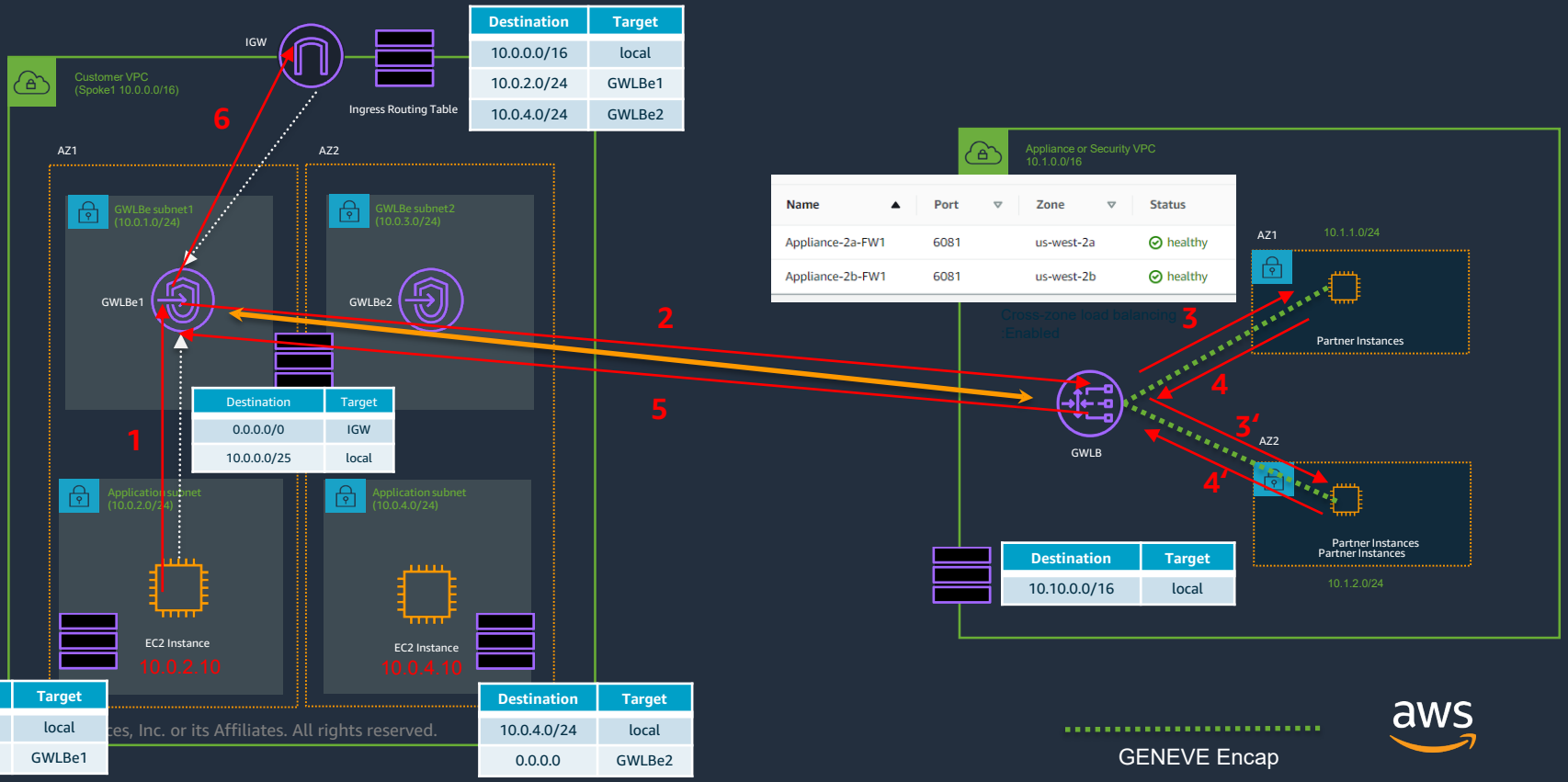
Appliance modeがenable(有効)の場合、TGWのハッシュの計算により同一AZ間トラフィックでも、他のAZのGWLBエンドポイントに振り分けられる場合もある。

クロスゾーン負荷分散について

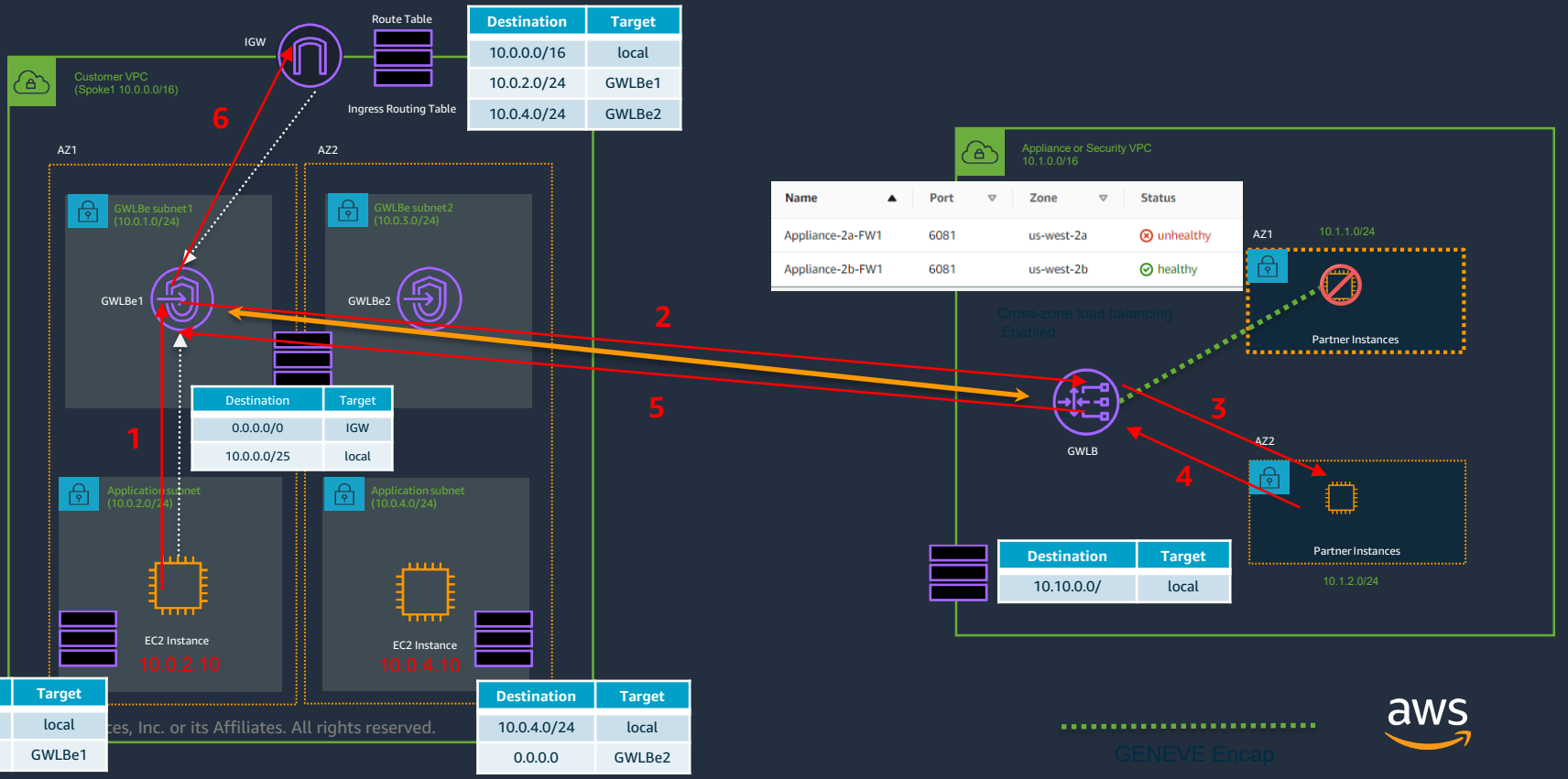
クロスゾーン負荷分散

- GWLB作成後にクロスゾーン負荷分散を有効化できる。
- 動作は従来のNLBと同じです。

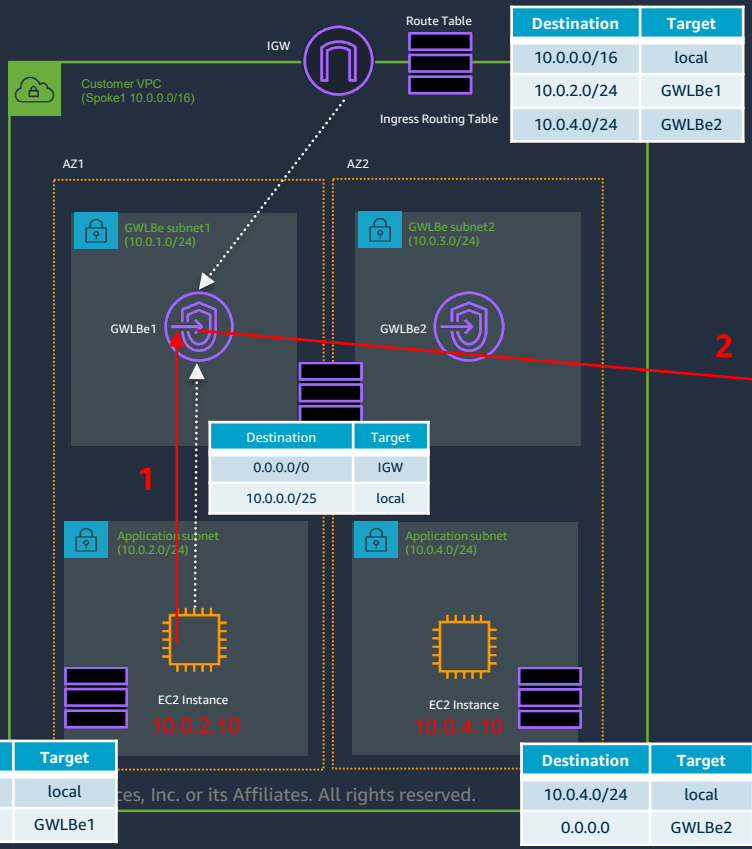
クロスゾーン負荷分散（Appliance正常時）

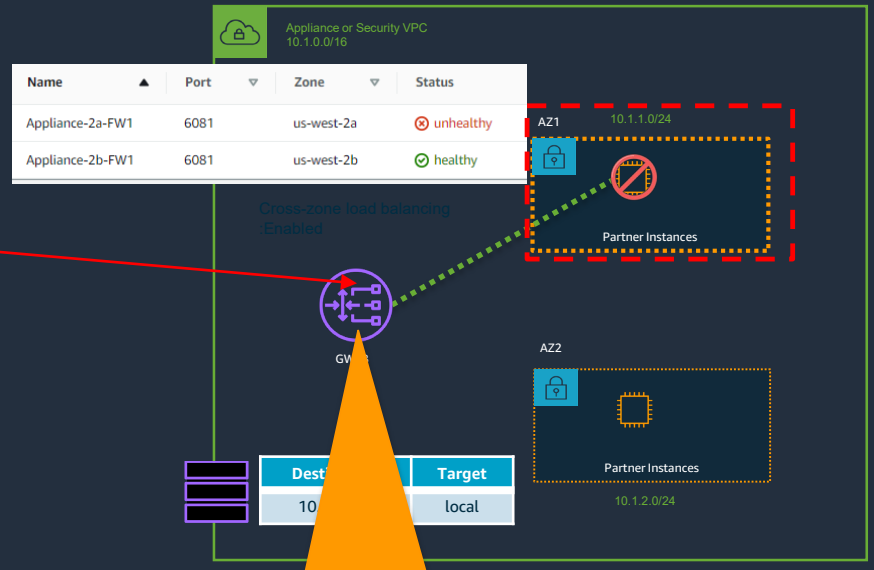


クロスゾーン負荷分散（AZ1 Appliance全障害）



クロスゾーン負荷分散無効の場合（AZ1 Appliance全障害）

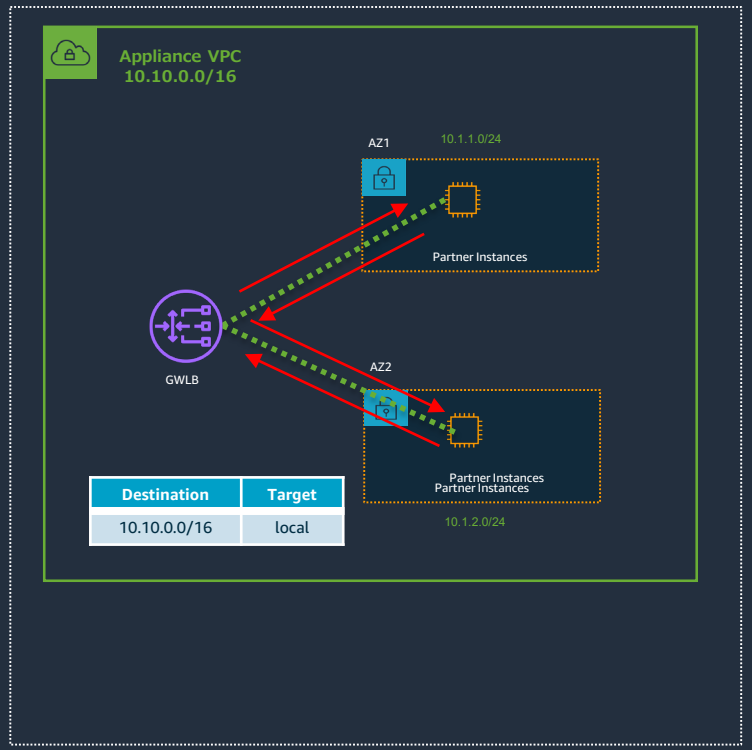




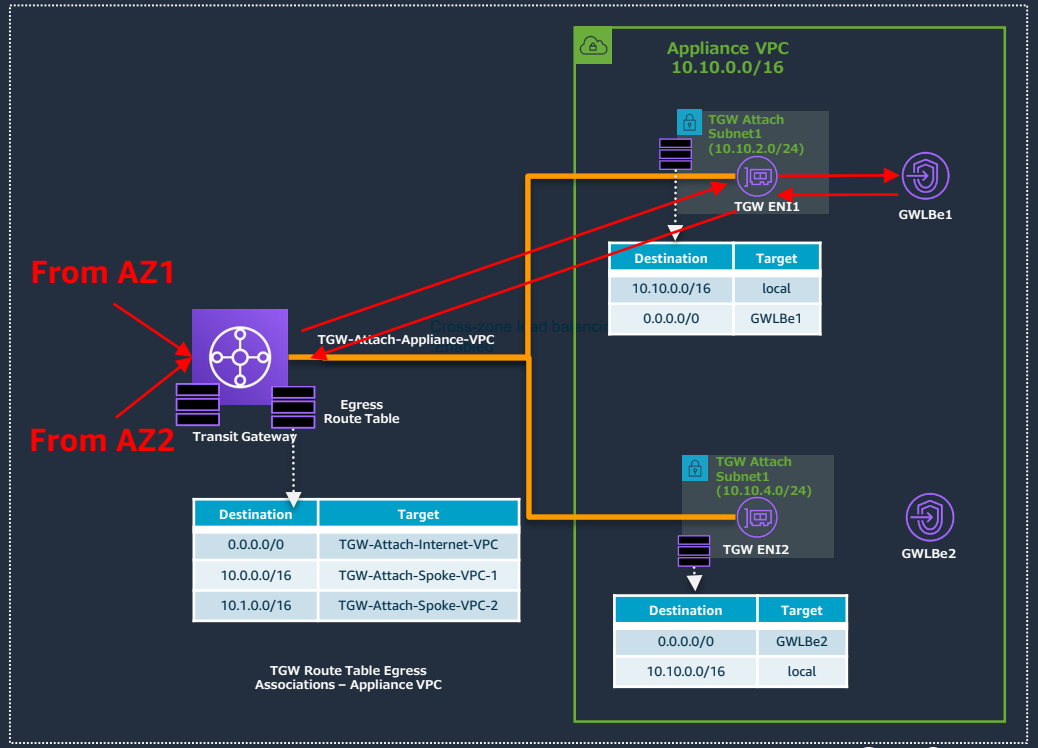
GWLBはAZ1から発信されたトラフィックの転送を止める。AZ2から発信されたトラフィックの処理は続ける。

クロスゾーン負荷分散 vs TGW Appliance mode

クロスゾーン負荷分散

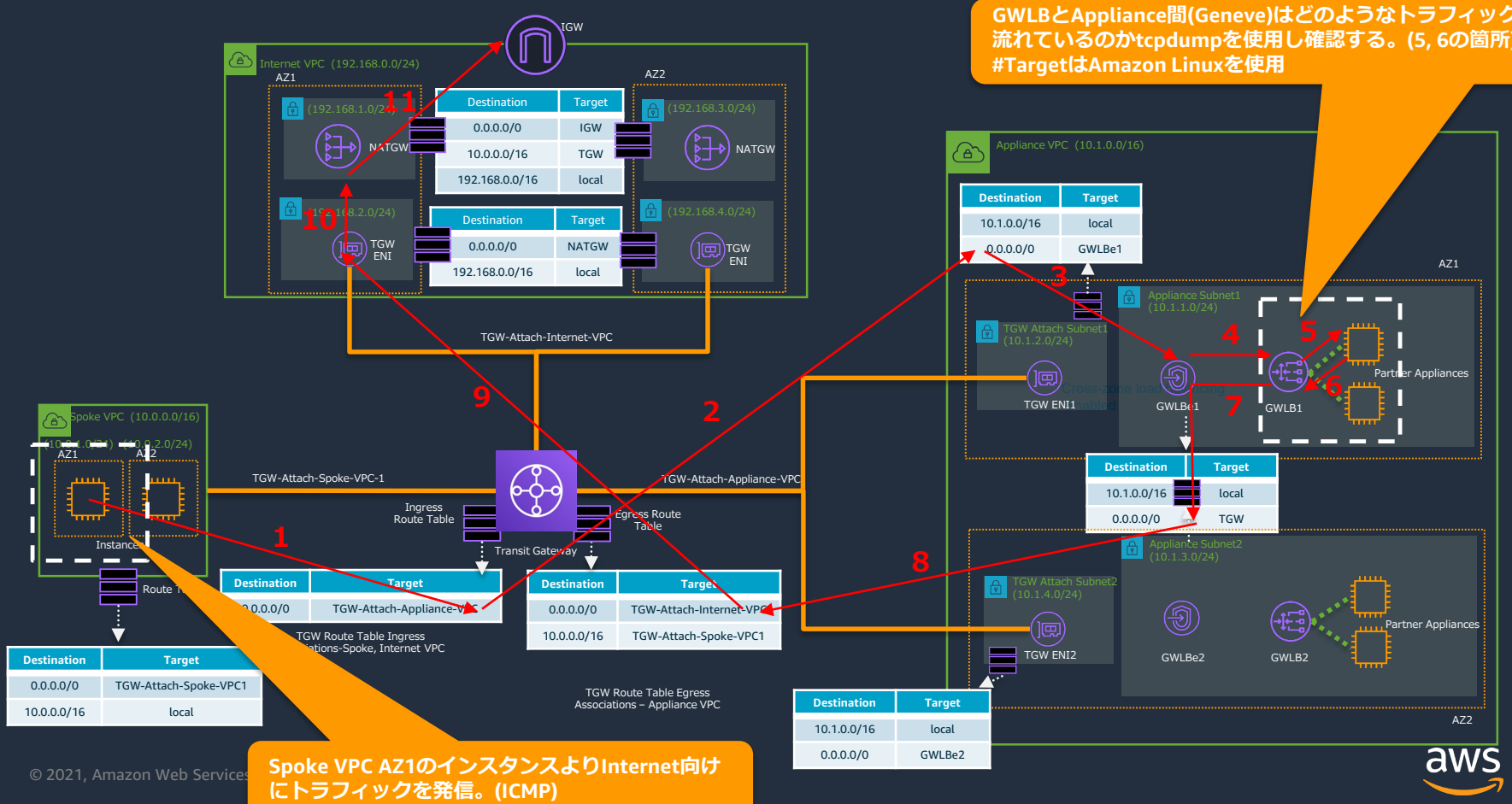


Transit Gateway Appliance mode



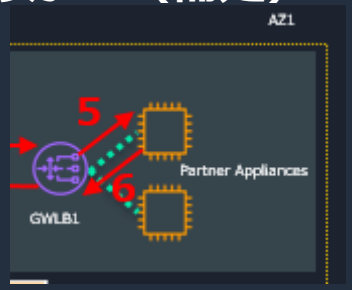
AWS Transit Gateway/Gateway Load Balancer を使用したEgress トラフィック インスペクション ビデオデモをご覧ください。

デモ1 GWLBe-GWLB間はどのようなトラフィックが流れているのか？



デモ1 GWLBe-GWLB間はどのようなトラフィックが流れているのか？（補足）

GWLBとAppliance FW間のトラフィック(5, 6)は、GENEVEによりカプセル化されている。またオリジナルのパケットはそのまま維持されている。(透過的)
#Genevenoport番号は6081になります。



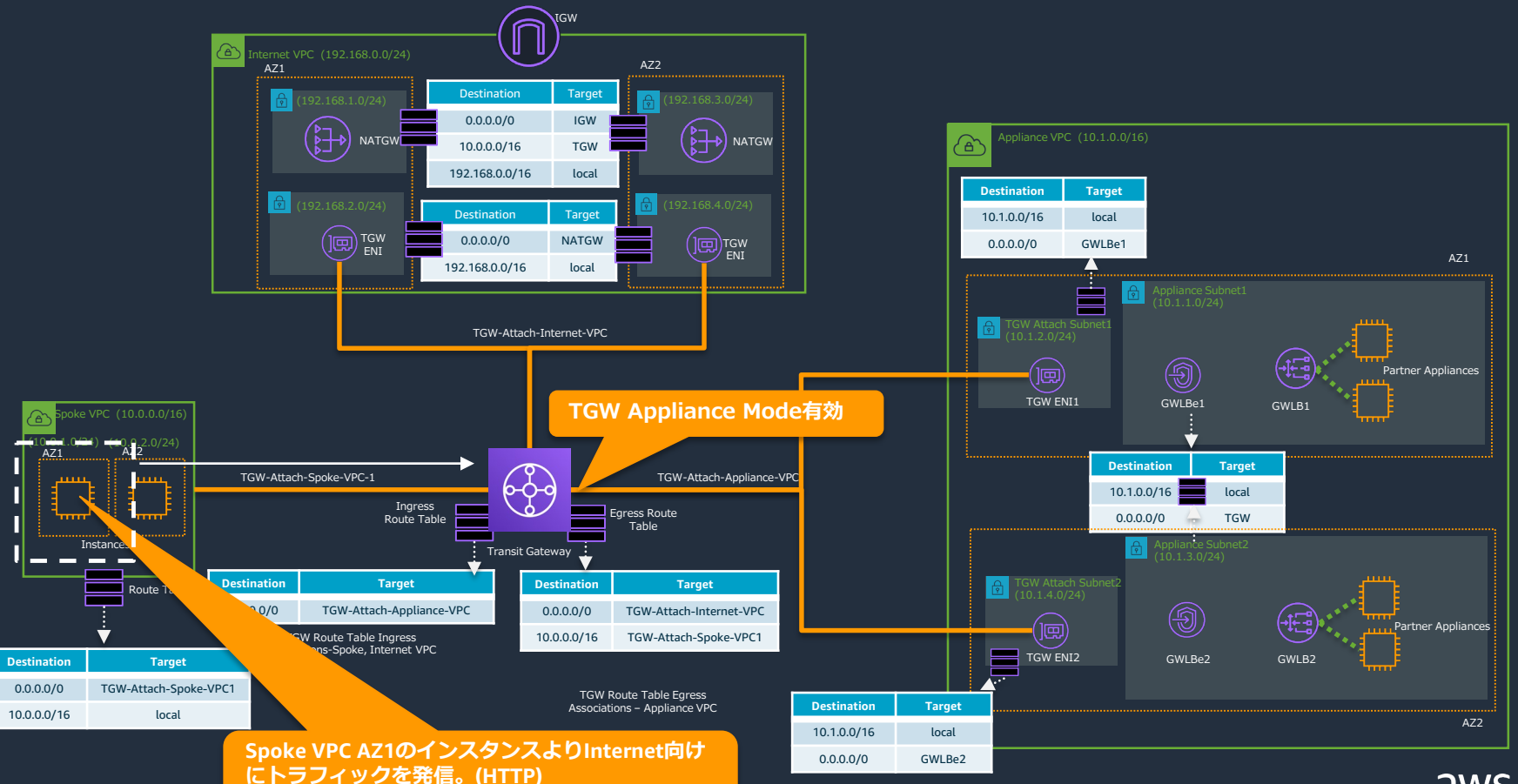
★Geneve Src Dst　GWLB(10.0.10.164) → Appliance(10.0.10.10)　5
10:52:48.908670 IP 10.0.10.164.60004 > ip-10-0-10-10.ap-northeast-1.compute.internal.6081: Geneve, Flags [none], vni 0x0, options [32 bytes]: IP 172.16.3.217 > 183.79.217.124: ICMP echo request, id 1, seq 161, length 40

★Geneve Src Dst　Appliance(10.0.10.10)→GWLB(10.0.10.164)　6
10:52:48.908698 IP ip-10-0-10-10.ap-northeast-1.compute.internal.60004 > 10.0.10.164.6081: Geneve, Flags [none], vni 0x0, options [32 bytes]: IP 172.16.3.217 > 183.79.217.124: ICMP echo request, id 1, seq 161, length 40

★Geneve Src Dst　GWLB(10.0.10.164) → Appliance(10.0.10.10)　5
10:52:48.916754 IP 10.0.10.164.60004 > ip-10-0-10-10.ap-northeast-1.compute.internal.6081: Geneve, Flags [none], vni 0x0, options [32 bytes]: IP 183.79.217.124 > 172.16.3.217: ICMP echo reply, id 1, seq 161, length 40

★Geneve Src Dst　Appliance(10.0.10.10)→GWLB(10.0.10.164)　6
10:52:48.916766 IP ip-10-0-10-10.ap-northeast-1.compute.internal.60004 > 10.0.10.164.6081: Geneve, Flags [none], vni 0x0, options [32 bytes]: IP 183.79.217.124 > 172.16.3.217: ICMP echo reply, id 1, seq 161, length 40

デモ2 TGW上でAppliance Modeを有効にした場合の動作

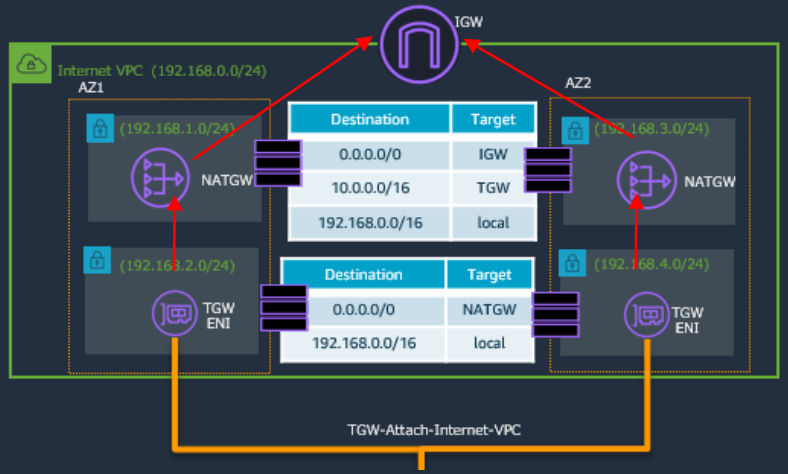


Appliance Modeコマンド： "aws ec2 modify-transit-gateway-vpc-attachment --transit-gateway-attachment-id tgw-attach- xxxxxxxxxxxxxxxx --options ApplianceModeSupport=enable"

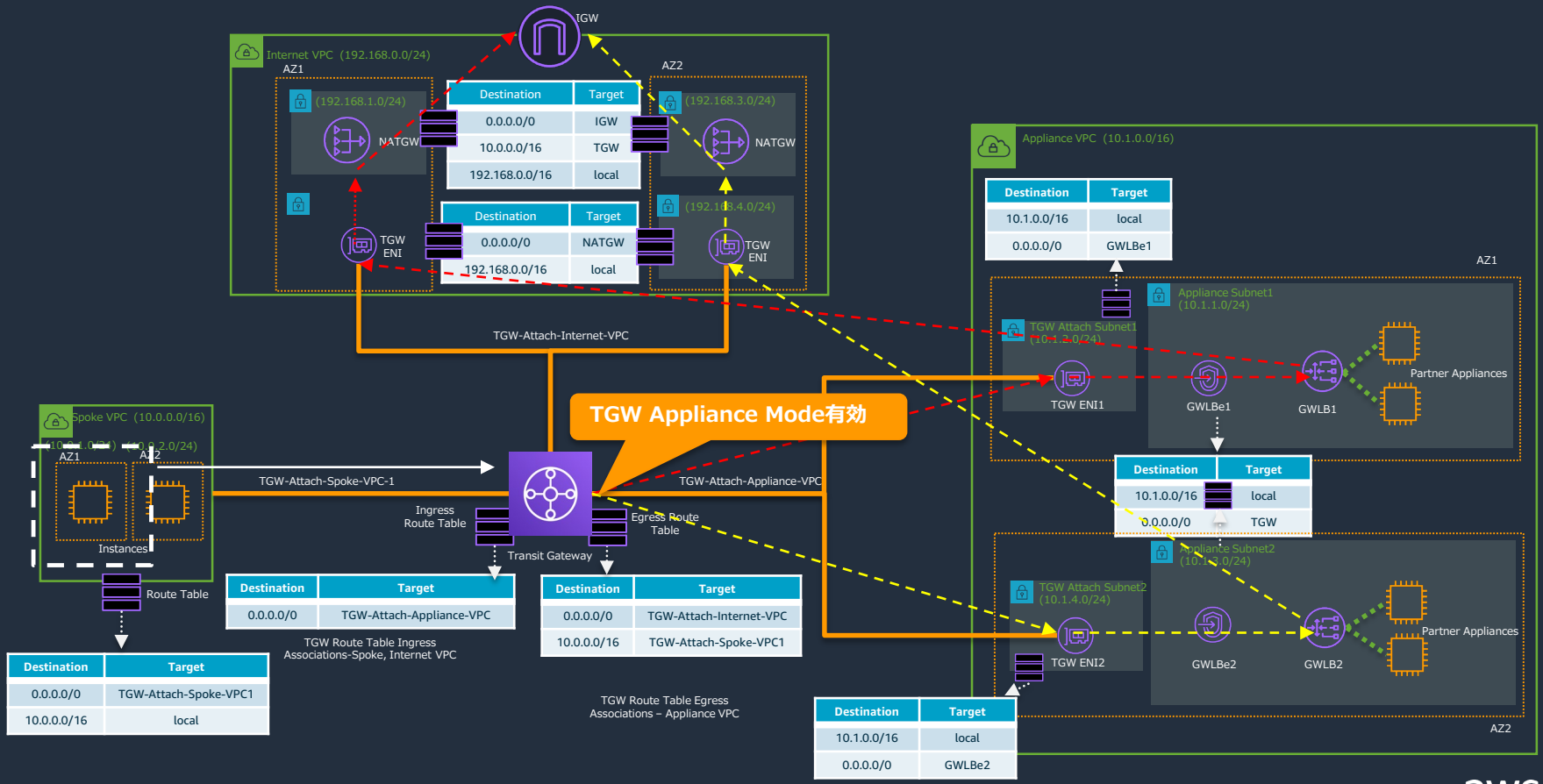
デモ2 TGW上でAppliance Modeを有効にした場合の動作（補足）

https://checkip.amazonaws.com/
で下記の何れかのアドレスになっていることを確認。
(Internet VPCから出ていることを確認)

○	Internet-AZ1	nat-0c1bd6c57046c4251	Available	–	18.180.165.230	192.168.1.113
○	Internet-AZ2	nat-067929ce4c8152ad7	Available	–	54.250.52.12	192.168.2.248



デモ2 TGW上でAppliance Modeを有効にした場合の動作（補足）



Appliance Modeコマンド例： “aws ec2 modify-transit-gateway-vpc-attachment --transit-gateway-attachment-id tgw-attach- xxxxxxxxxxxxxxxx --options ApplianceModeSupport=enable”

補足

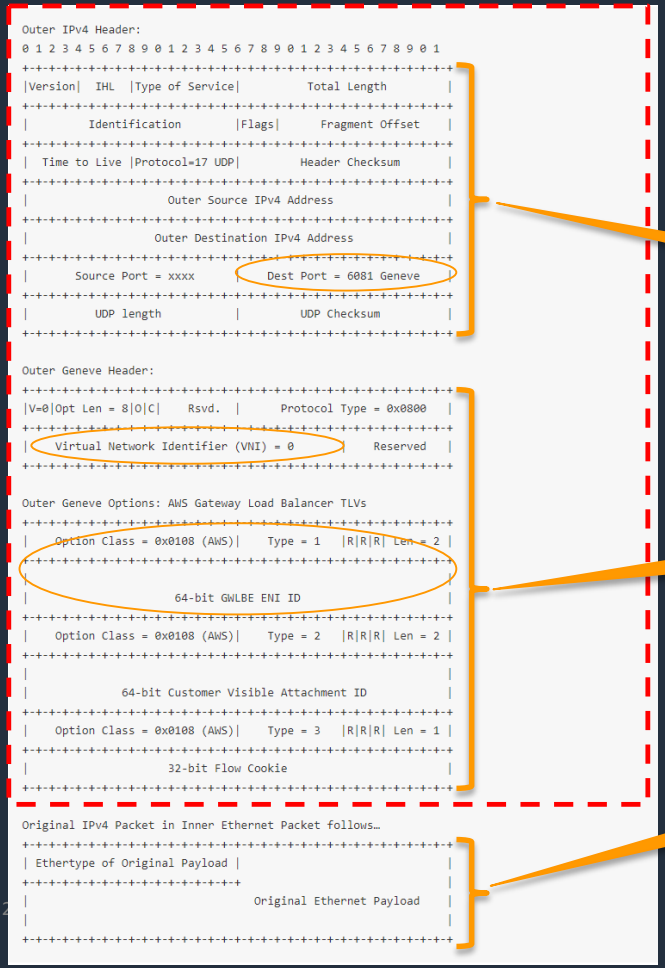
Amazon Linux 2をGWLBのターゲットにする

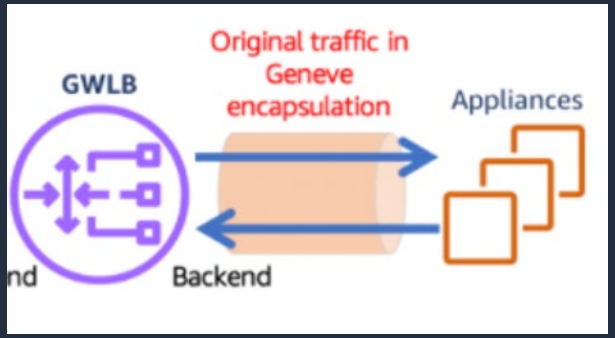
- Amazon Linux 2をGWLBのターゲットにする方法が公開されております。
- 実際のセキュリティアプライアンスを使用しなくても、GWLBとインスタンス間をヘアピンするトラフィックフローが作れます。

左記の様なトラフィックフローを実現できます。あくまでもテスト目的でご使用ください。インスペクションなどのテストは行えません。

https://github.com/aws-samples/aws-gateway-load-balancer-code-samples/blob/main/aws-cli/gwlb/configure_iptables_al2.md

Geneve Protocol





GeneveのOuter IPv4 Header。UDP(6081)を使用

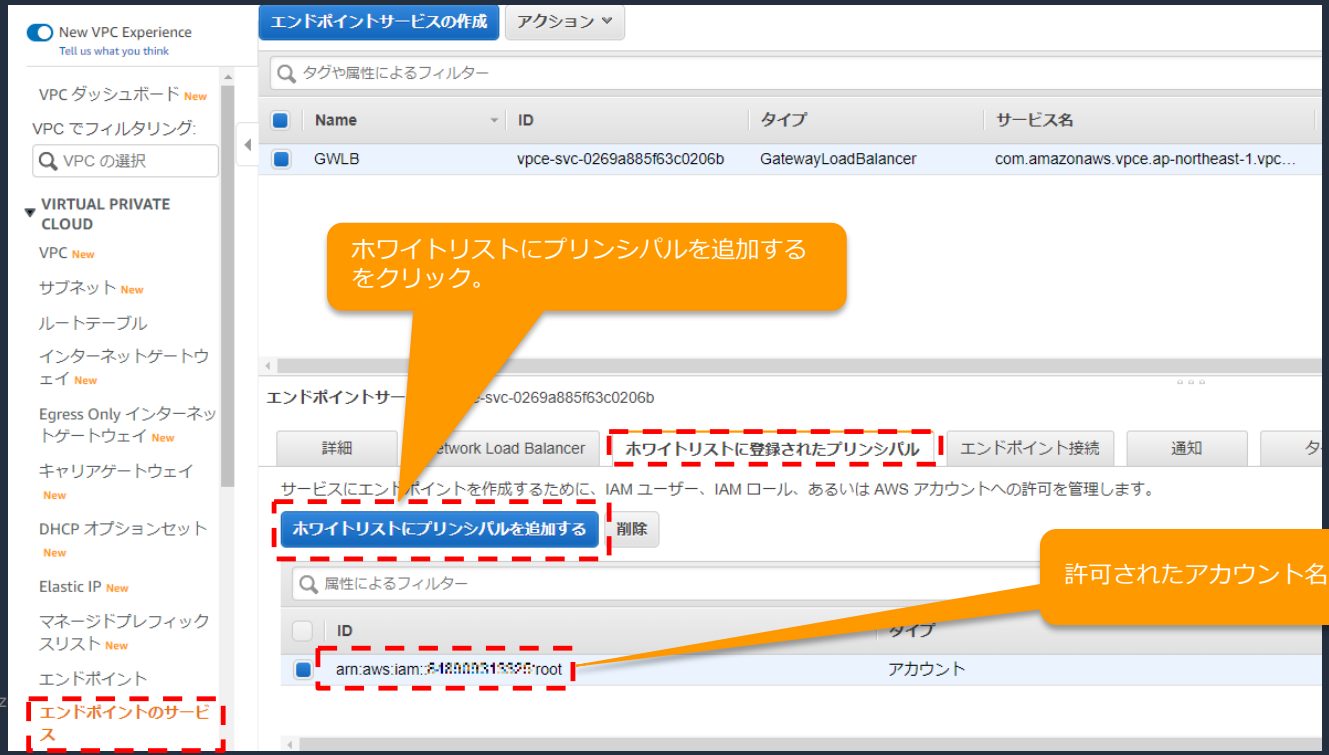
GeneveのHeader部分。Vxlanと同様VNIなどがある。GWLBは常にこの値は「0」です。その代わりに、Option TLV内に追加情報としてGWLBe ID, VPC IDなどが含まれている。
#Option TLVはVxLANでは実装されていないフィールドです。

オリジナルのイーサーネットフレームペイロード

https://aws.amazon.com/jp/blogs/networking-and-content-delivery/integrate-your-custom-logic-or-appliance-with-aws-gateway-load-balancer/

他のアカウントにGWLBエンドポイントを作成するには

- ホワイトリストに他のアカウントを追加する事により、対象アカウントがこのサービス名を使用してGWLBエンドポイントを作成できるようになります。



Gateway Load Balancerのクォータ

制限	デフォルト
リージョンあたりのGateway Load Balancerの数	20
VPCあたりのGateway Load Balancerの数	10
リージョンあたりのGENEVEプロトコルを使用したターゲットグループ数	100
Gateway Load Balancer endopointがサポートしているIPプロトコル	IPv4のみ
各AZ(サブネット)ごとのGateway Load Balancer endopoint数	1
Gateway Load Balancer endopointごとの最大帯域幅	40 Gbps

Gateway Load Balancerのご利用料金

(*) バージニア北部リージョンの料金を記載

NLBと同様に “Capacity Unit” を基準としたご利用料金
+ PrivateLink のご利用料金

①GWLB時間あたりの料金

0.0135 USD/時間

＋

②GWLB Capacity Unit料金

0.004 USD/GLCU-時間
を基準とした料金

(以下の3項目から算出したCU)
1. 新規接続/フロー数
2. アクティブな接続/フロー数
3. 処理したバイト数(GB単位)

※1時間内で上記の最大使用量を基準にGLCU数を判定。
「1 GLCU」は以下に対応
- 600 新規接続・フロー/秒
- 60,000 アクティブ接続/フロー (1分あたりのサンプル数)
- ターゲットのEC2、コンテナIPアドレスで1時間あたり1GB

＋

③GWLBエンドポイント料金

各AZのVPCエンドポイント1つあたりの料金
0.014 USD/時間
＋
処理データ1GBあたりの料金
0.0035USD/GB

参考資料

AWSドキュメント

https://docs.aws.amazon.com/ja_jp/elasticloadbalancing/latest/gateway/introduction.html
https://docs.aws.amazon.com/ja_jp/vpc/latest/privatelink/vpce-gateway-load-balancer.html

技術ブログ一覧

https://aws.amazon.com/blogs/networking-and-content-delivery/category/networking-content-delivery/elastic-load-balancing/gateway-load-balancer/

FAQ

https://aws.amazon.com/jp/elasticloadbalancing/faqs/?nc=sn&loc=5#Gateway_Load_Balancer

パートナー様一覧

https://aws.amazon.com/jp/elasticloadbalancing/partners/

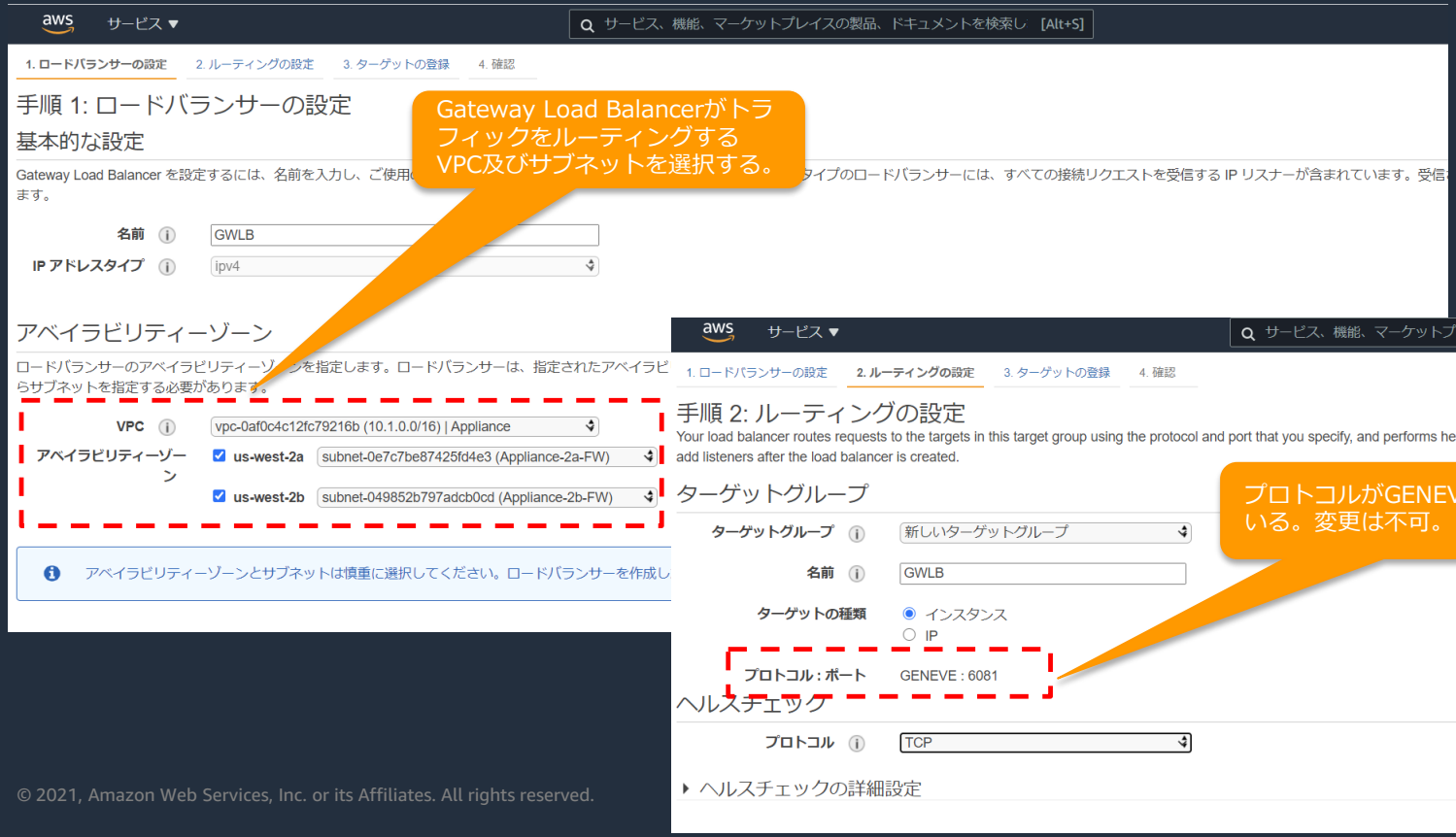
料金

https://aws.amazon.com/jp/elasticloadbalancing/pricing/
https://aws.amazon.com/jp/privatelink/pricing/

GWLB 設定画面

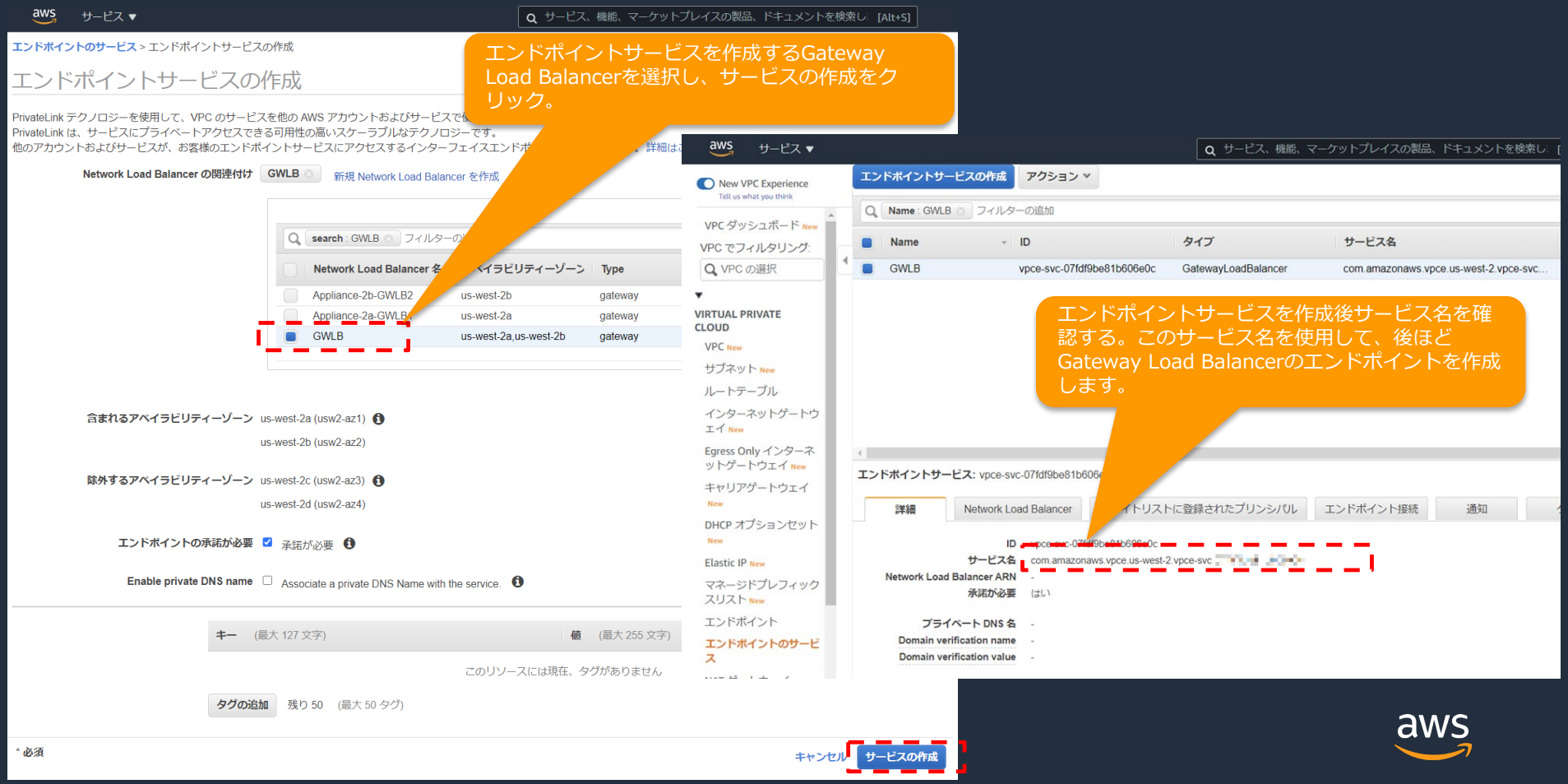
Gateway Load Balancerを使用するには

Gateway Load Balancerを使用するには

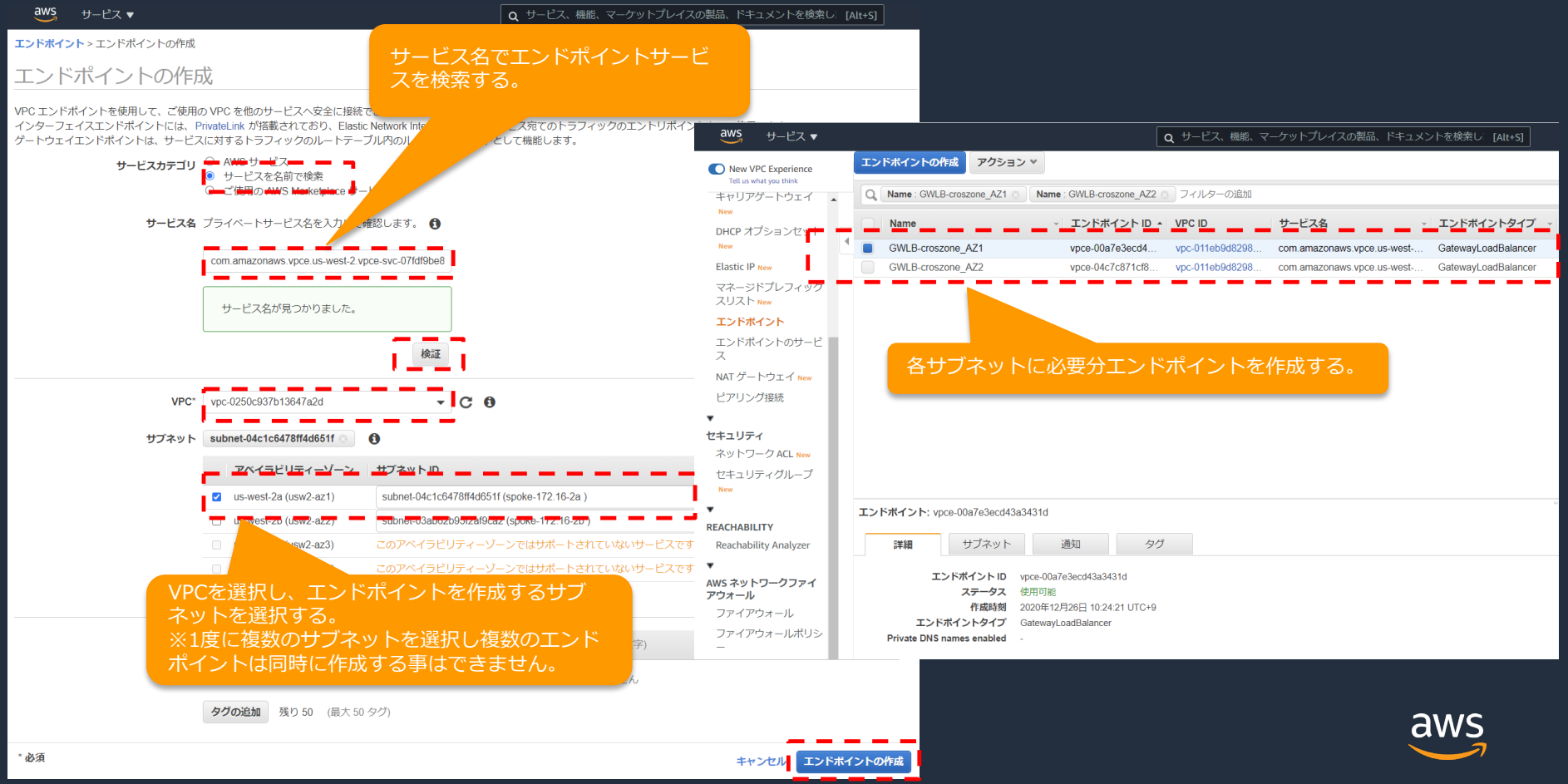


Gateway Load Balancerを使用するには

Gateway Load Balancerを使用するには



Gateway Load Balancerを使用するには



まとめ

まとめ

- GWLBを使用すると、サードパーティのセキュリティアプライアンス製品などをAWS上で利用する際、可用性の高い構成がとれます。
- GWLBは新しいコンポーネントとしてGWLBeという新しいタイプのエンドポイントとGateway Load Balancer (GWLB) 使用します。
- GWLBを使用する際は、AZを意識したネットワーク設計が必要です。
- TGWとGWLBを組み合わせることにより、より柔軟なトラフィックフローが実現可能です。AZを跨るトラフィックをインスペクションしたい場合はTGW Appliance modeを使用する必要があります。
- 各アプライアンスパートナー様のセキュリティアプライアンスはGWLB(GENEVEプロトコルへ)に対応しているものを選択する必要があります。

aws

Q&A

お答えできなかったご質問については
AWS Japan Blog 「https://aws.amazon.com/jp/blogs/news/」にて
後日掲載します。

AWS の日本語資料の場所「AWS 資料」で検索

https://amzn.to/JPArchive

AWS Well-Architected 個別技術相談会

毎週”W-A個別技術相談会”を実施中

- AWSのソリューションアーキテクト(SA)に対策などを相談することも可能
- 申込みはイベント告知サイトから

(https://aws.amazon.com/jp/about-aws/events/)

AWS イベント で[検索]

4月以降のBlack Belt Online Seminarについて

ライブ配信によるBlack Belt Online Seminarは3月一杯で終了し、
今後はオンデマンドによる定期配信に変更いたします。

今後もコンテンツを拡充して行きますので、楽しみにお待ちください。

オンデマンドでの配信スケジュールは、AWS Blog, AWSニュースレターでお知らせいたします（5月17日週に再開を予定しています）

ご視聴ありがとうございました

AWS 公式 Webinar
https://amzn.to/JPWebinar

過去資料
https://amzn.to/JPArchive