



[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>



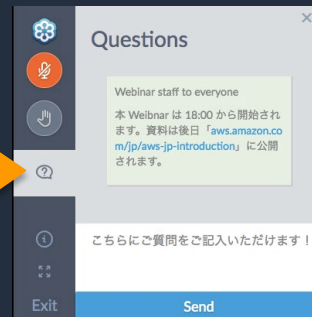
AWS Black Belt Online Seminar とは

「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おります。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ー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

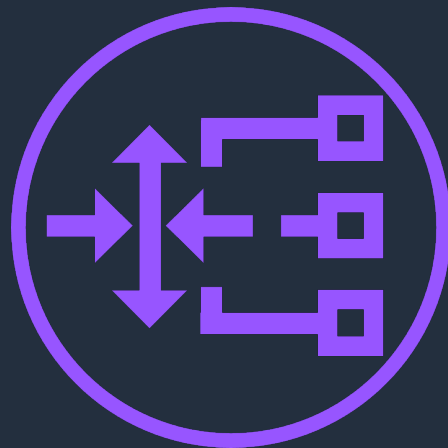
- AWS Gateway Load Balancer 概要
- AWS Gateway Load Balancerを使用するには
- 参考アーキテクチャ例及びAZの考え方
- Transit Gateway Appliance modeとは
- クロスゾーン負荷分散
- まとめ

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



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



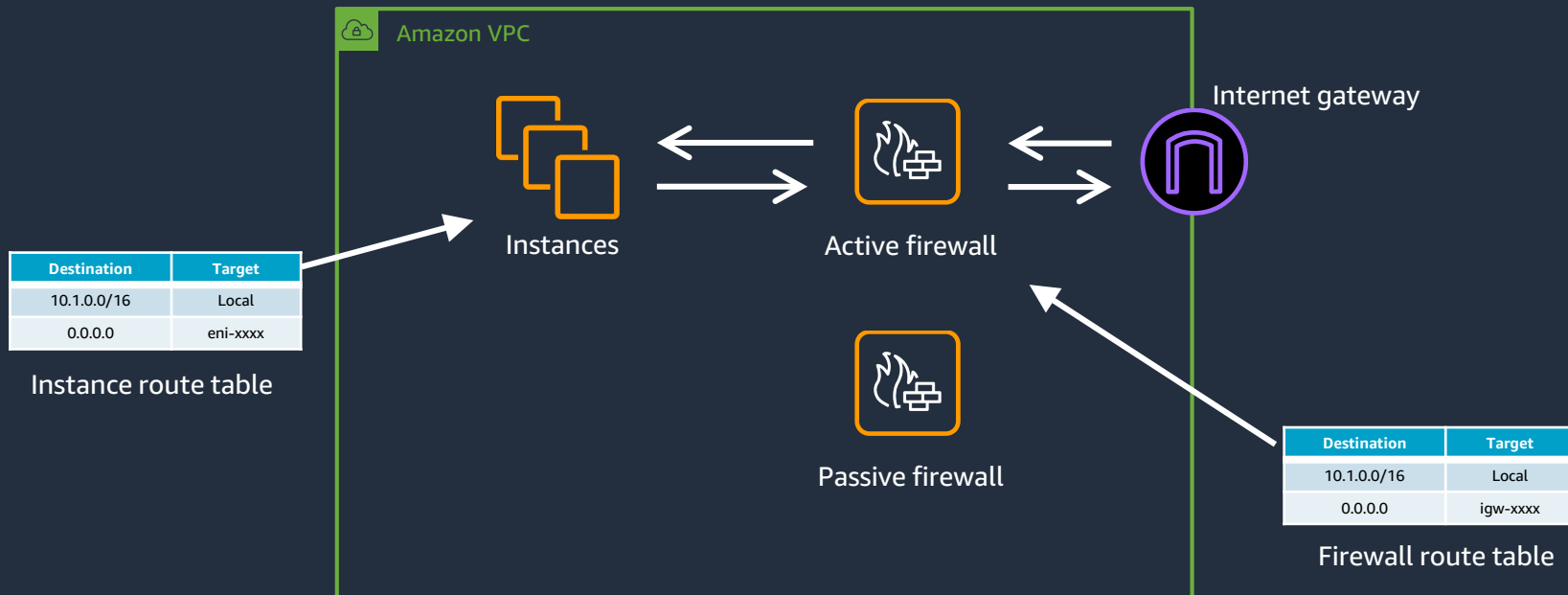
セキュリティー、
監視、分析等の
用途の対応



ポリシー及び運
用の専門知識へ
の投資

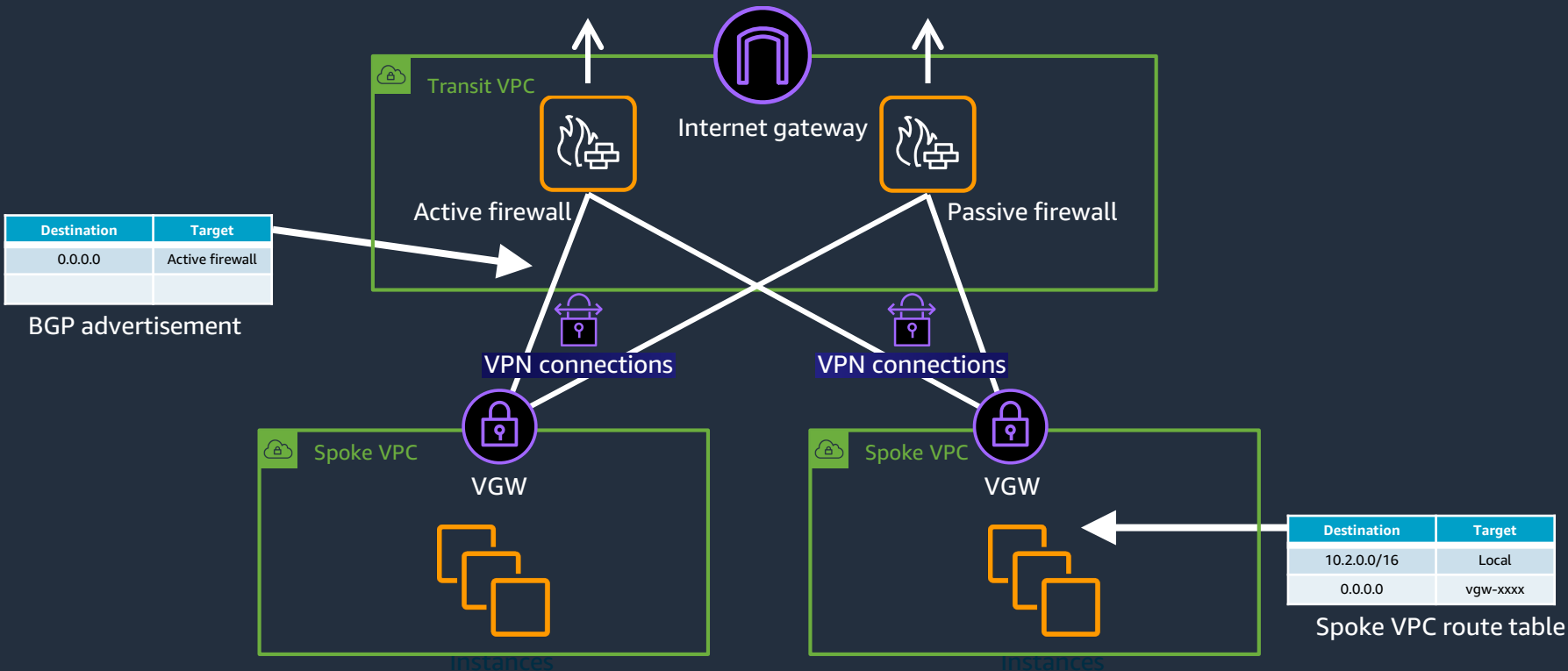
AWSやハイブリッド環境で同じネットワークアプライアンスがご利用可能

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

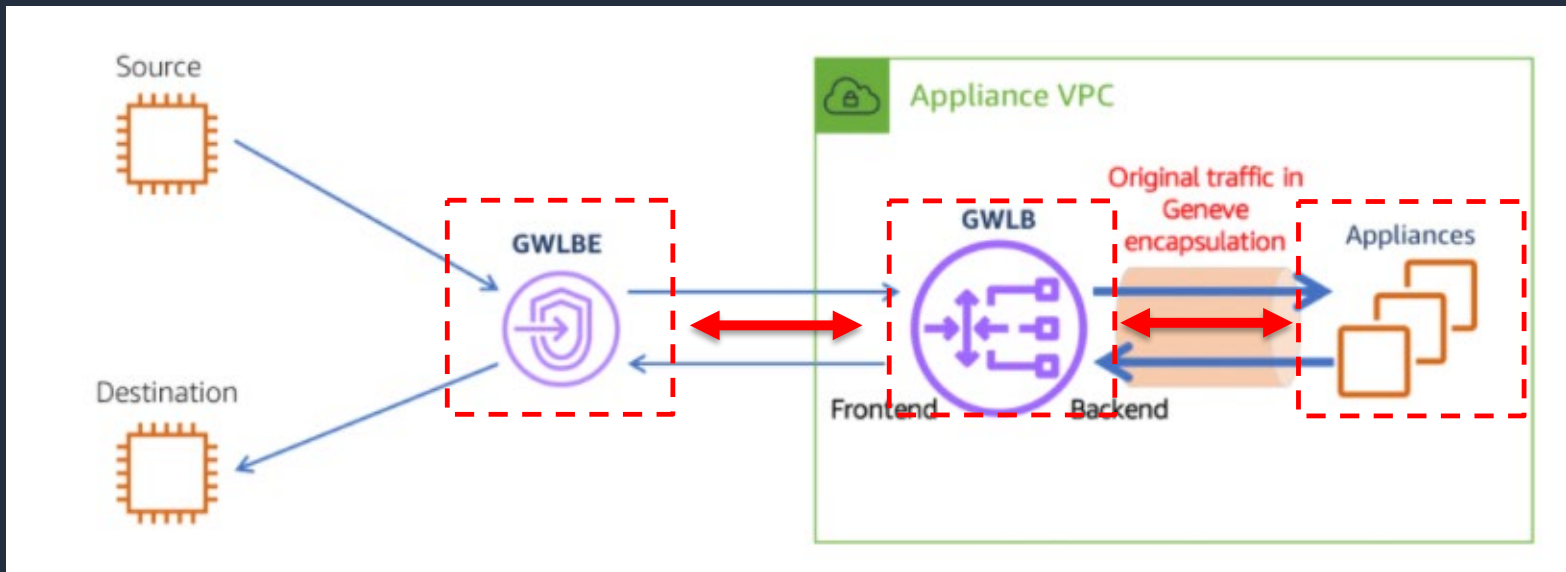
Gateway Load Balancer 概要

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

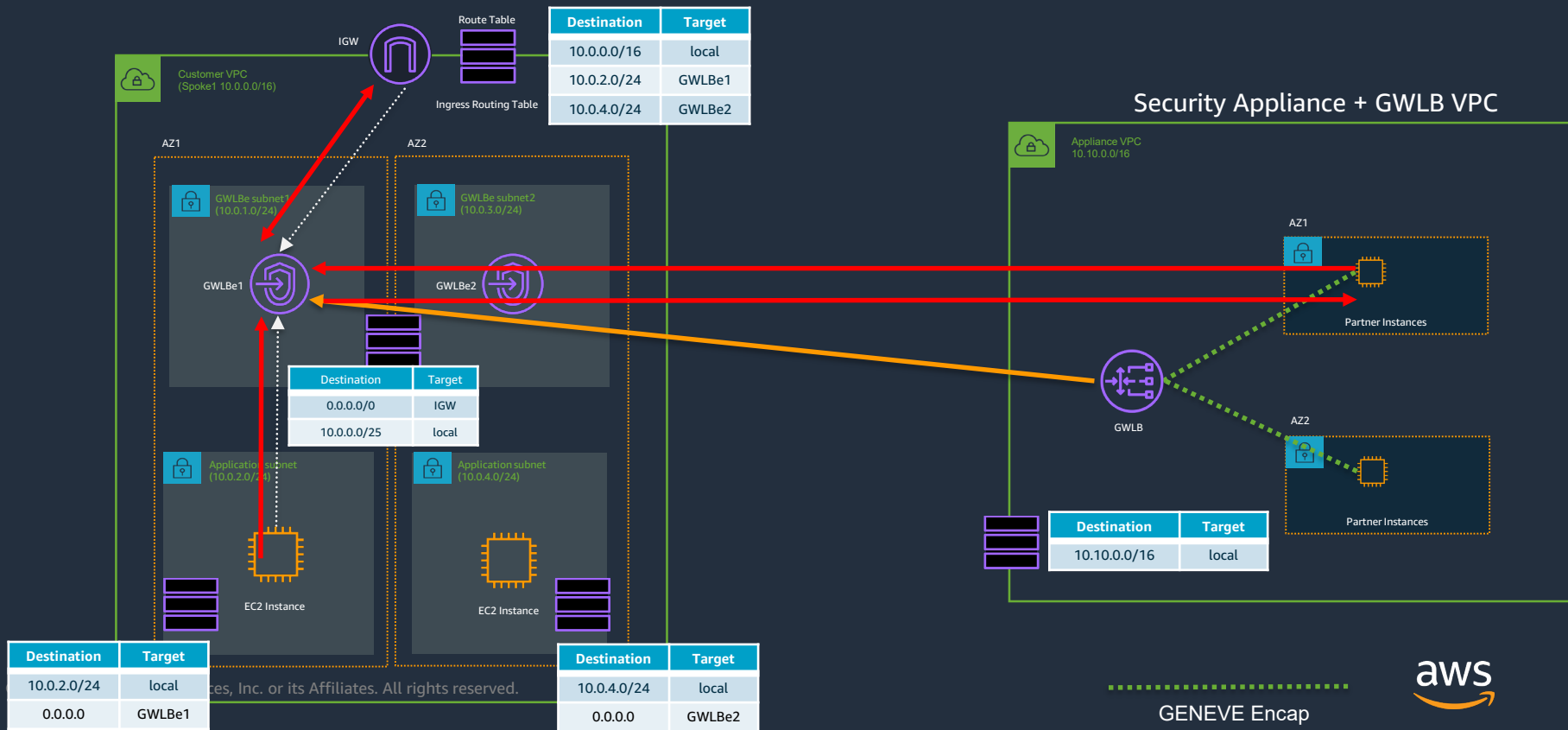
メリット

- 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

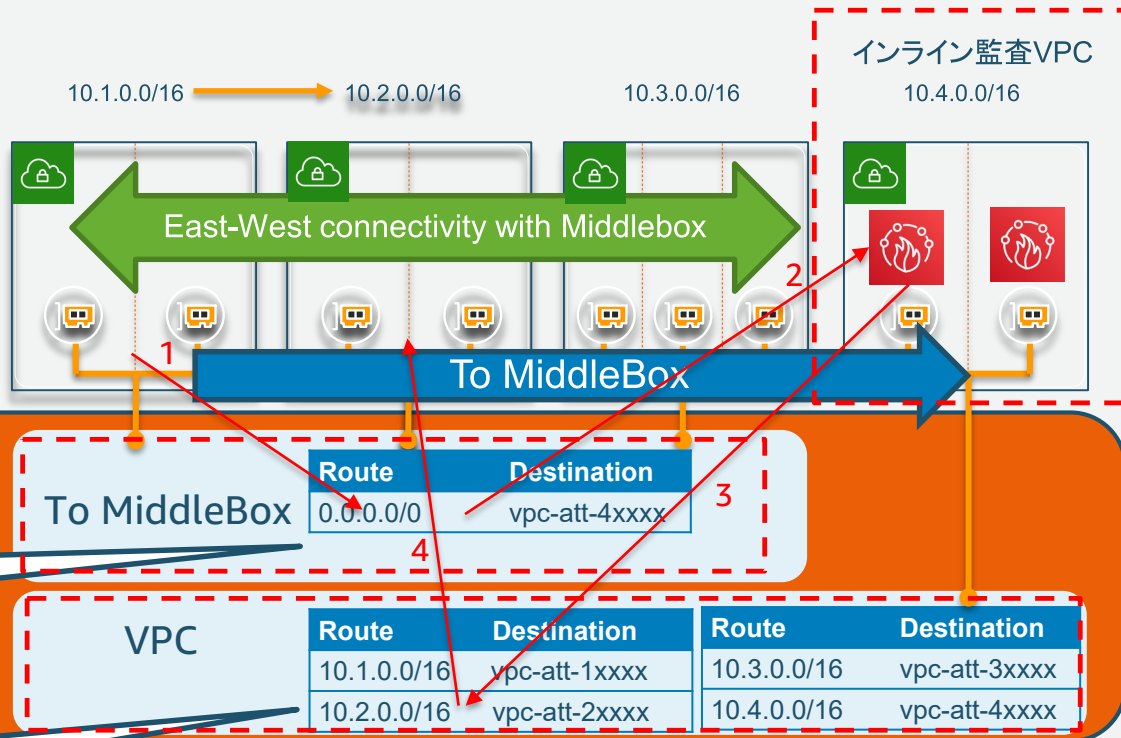


VPC間のトラフィックをインライン監査するRoute Domains おさらい



インライン監査向けの
経路

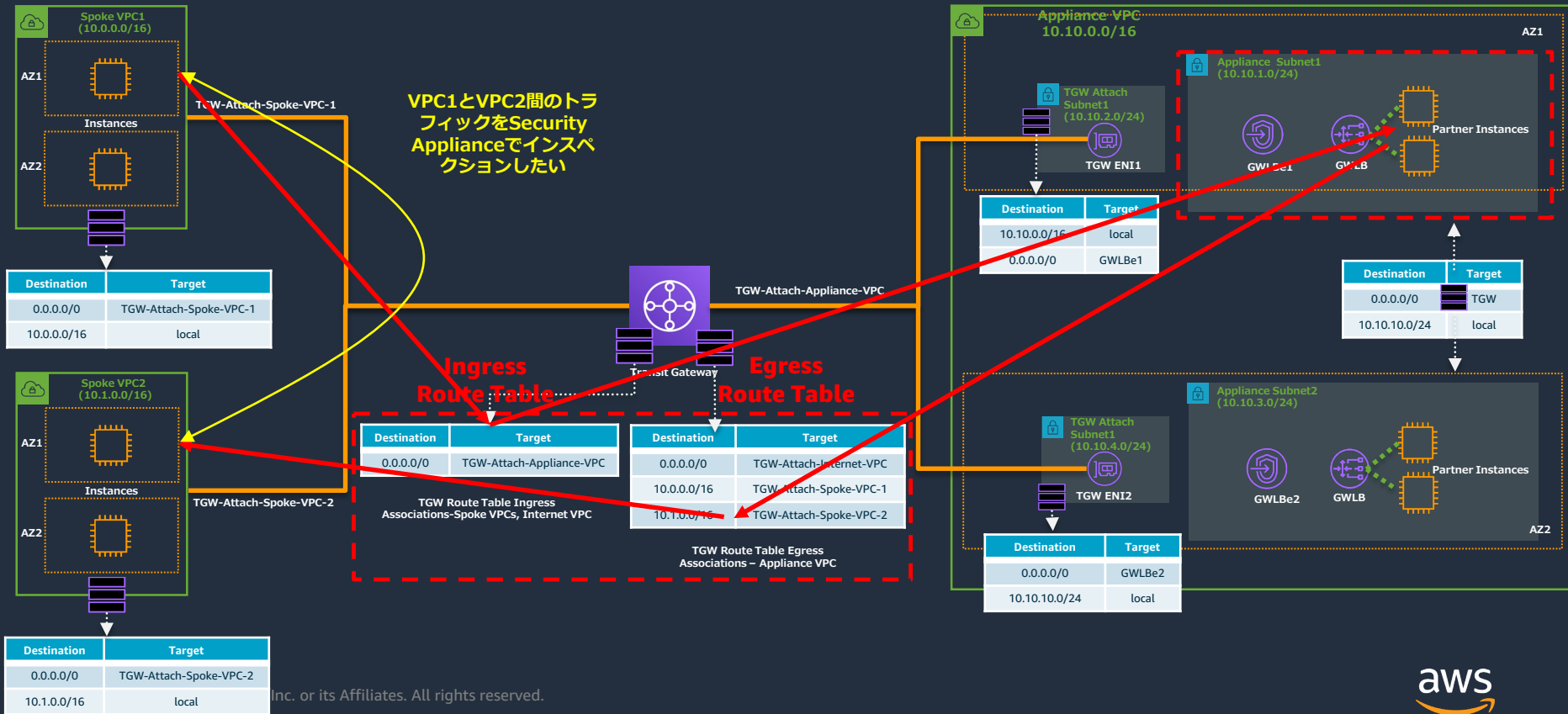
それぞれのVPC向け
の経路



今後のネットワークアプライアンスの展開モデル

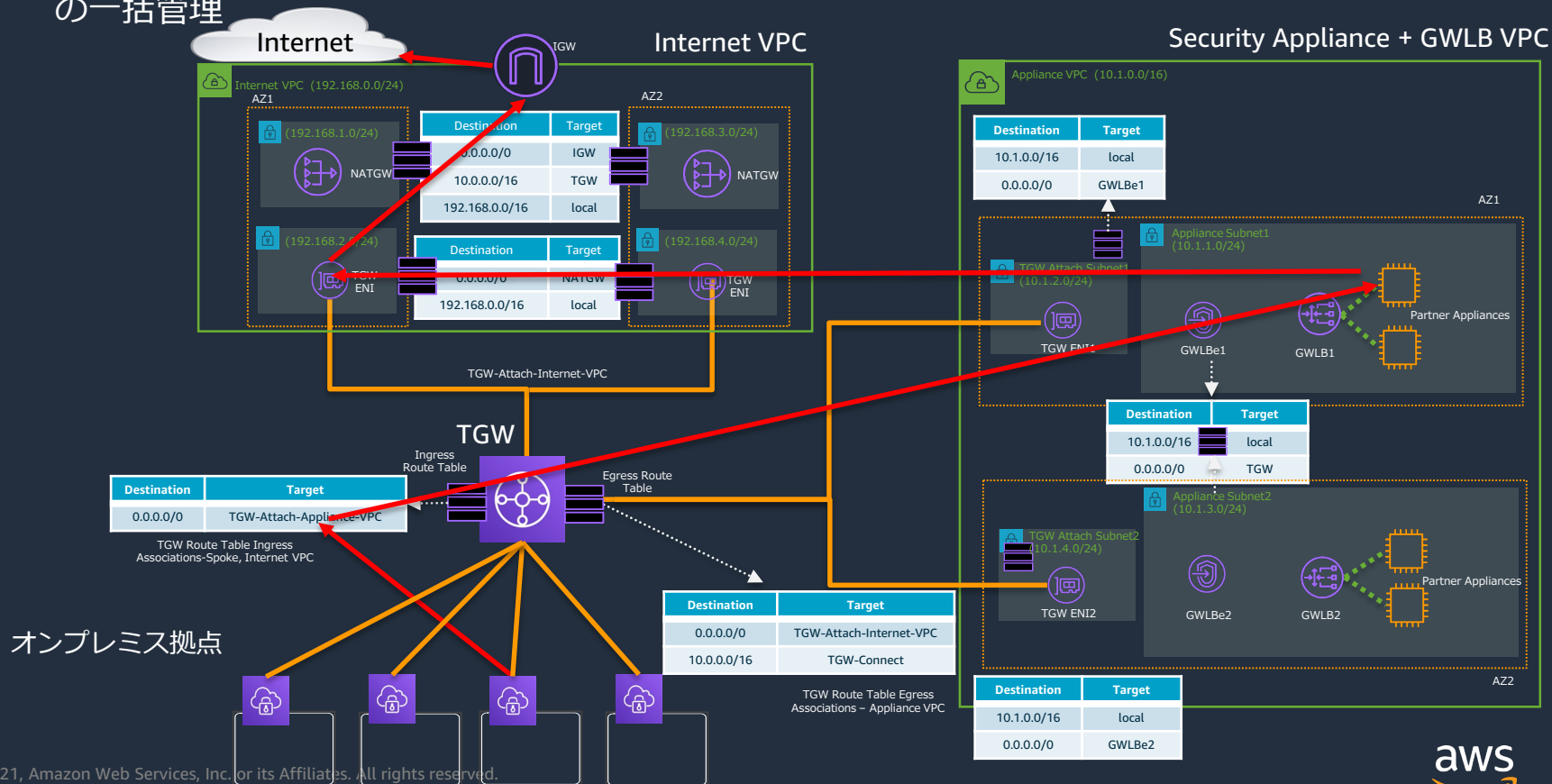
✓ TGW及びGWLBを使用したVPC間トラフィックのインスペクションの一括管理

Security Appliance + GWLB VPC



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



Gateway Load Balancerを使用するには

Gateway Load Balancerを使用するには

ロードバランサーの設定画面で
Gateway Load Balancerを選択



サービス ▼

検索 サービス、機能、マーケットプレースの製品、ドキュメントを検索し

ロードバランサーの種類の選択

Elastic Load Balancing は 4 種類のロードバランサー (Application Load Balancer、Network Load Balancer、Gateway Load Balancer および Classic Load Balancer) をサポートします。お客様のニーズに合うロードバランサーの種類を選択してください。お客様に最適なロードバランサーの詳細

Application Load Balancer

[作成](#)

HTTP および HTTPS トラフィックを使用するウェブアプリケーション用に柔軟性の高い機能セットが必要な場合は、Application Load Balancer を選択します。Application Load Balancer はリクエストレベルで動作し、マイクロサービスとコンテナを含む、アプリケーションアーキテクチャを対象とした高度なルーティングおよび可視性機能を提供します。

[詳細はこちら >](#)

Network Load Balancer

[作成](#)

非常に高いパフォーマンス、大規模な TLS のオフロード、証明書のデプロイの一元管理、UDP のサポート、およびアプリケーションの静的 IP アドレスが必要な場合は、Network Load Balancer を選択します。Network Load Balancer は接続レベルで動作し、非常に低いレイテンシーを維持しながら、1 秒あたり数百万のリクエストを確実に処理することができます。

[詳細はこちら >](#)

Gateway Load Balancer

[作成](#)

GENEVE をサポートするサードパーティーの仮想アプリケーションのフリートをデプロイおよび管理する必要がある場合は、Gateway Load Balancer を選択します。これらのアプライアンスを使用すると、セキュリティ、コンプライアンス、ポリシー制御を向上させることができます。

[詳細はこちら >](#)

Classic Load Balancer

以前の世代
HTTP、HTTPS、および TCP

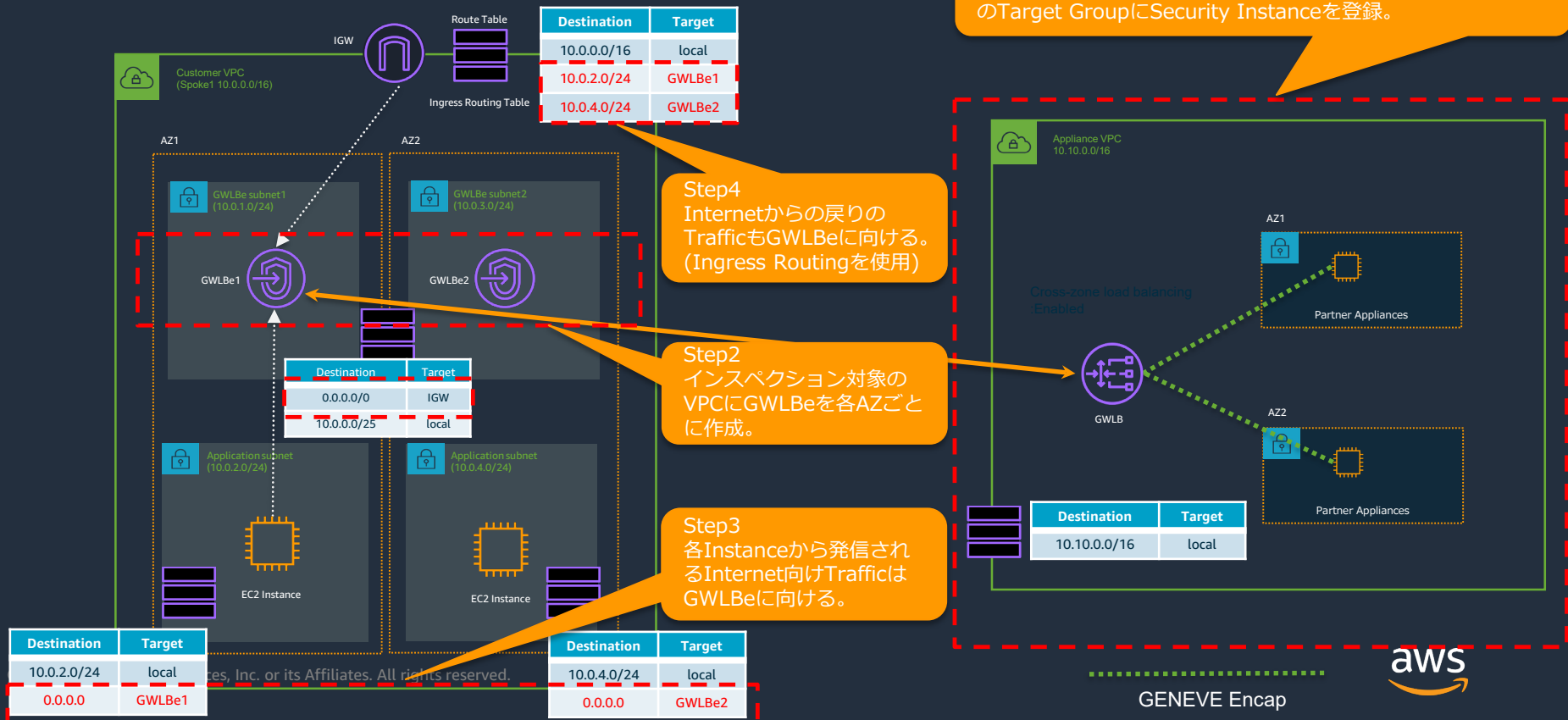
[作成](#)

EC2-Classical ネットワークで既存のアプリケーションを実行している場合は、Classic Load Balancer を選択します。

[詳細はこちら >](#)

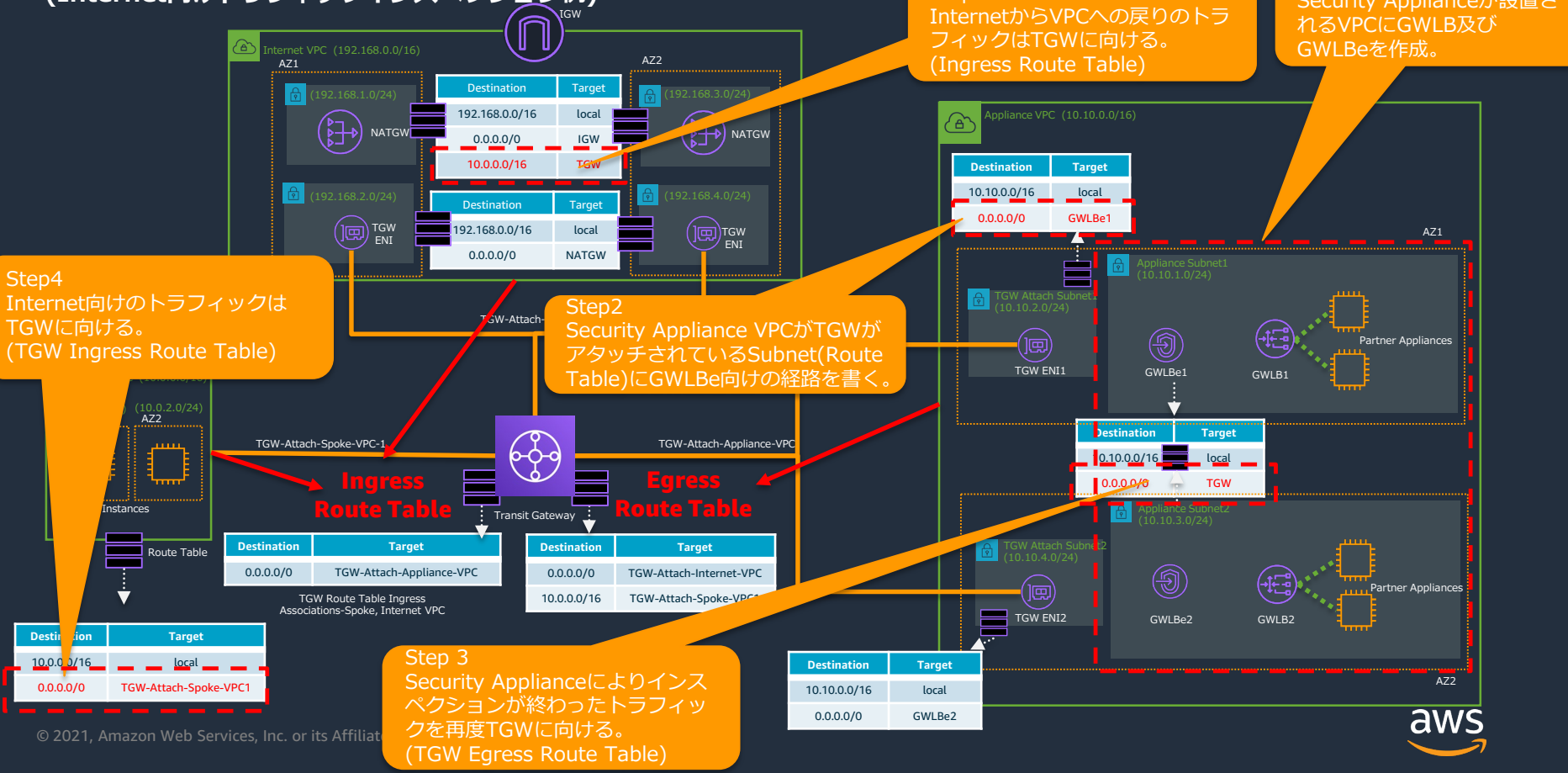
Routing設定の流れ (Ingress Routing)

(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と合わせ)

(Internet向けトラフィックインスペクション例)



Step 1
Security Applianceが設置されるVPCにGWLB及びGWLBeを作成。

Step 5
InternetからVPCへの戻りのトラフィックはTGWに向ける。(Ingress Route Table)

Step 2
Security Appliance VPCがTGWがアタッチされているSubnet(Route Table)にGWLBe向けの経路を書く。

Step 4
Internet向けのトラフィックはTGWに向ける。(TGW Ingress Route Table)

Step 3
Security Applianceによりインスペクションが終わったトラフィックを再度TGWに向ける。(TGW Egress Route Table)

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	TGW-Attach-Spoke-VPC1

Destination	Target
0.0.0.0/0	TGW-Attach-Appliance-VPC

TGW Route Table Ingress Associations-Spoke, Internet VPC

Destination	Target
0.0.0.0/0	TGW-Attach-Internet-VPC
10.0.0.0/16	TGW-Attach-Spoke-VPC1

TGW Route Table Egress Associations-Spoke, Internet VPC

Destination	Target
10.10.0.0/16	local
0.0.0.0/0	GWLBe2

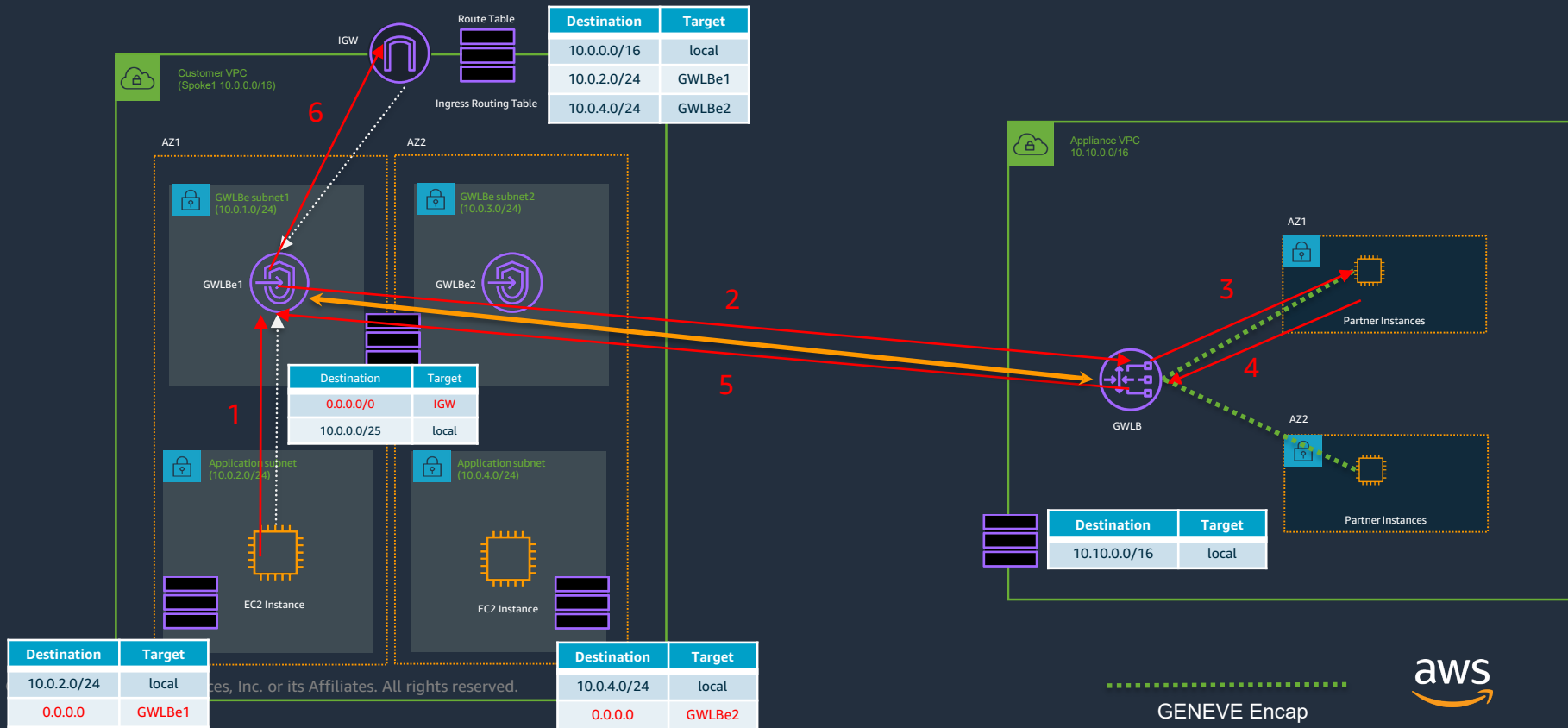
Destination	Target
10.10.0.0/16	local
0.0.0.0/0	GWLBe1

Destination	Target
0.10.0.0/16	local
0.0.0.0/0	TGW

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)

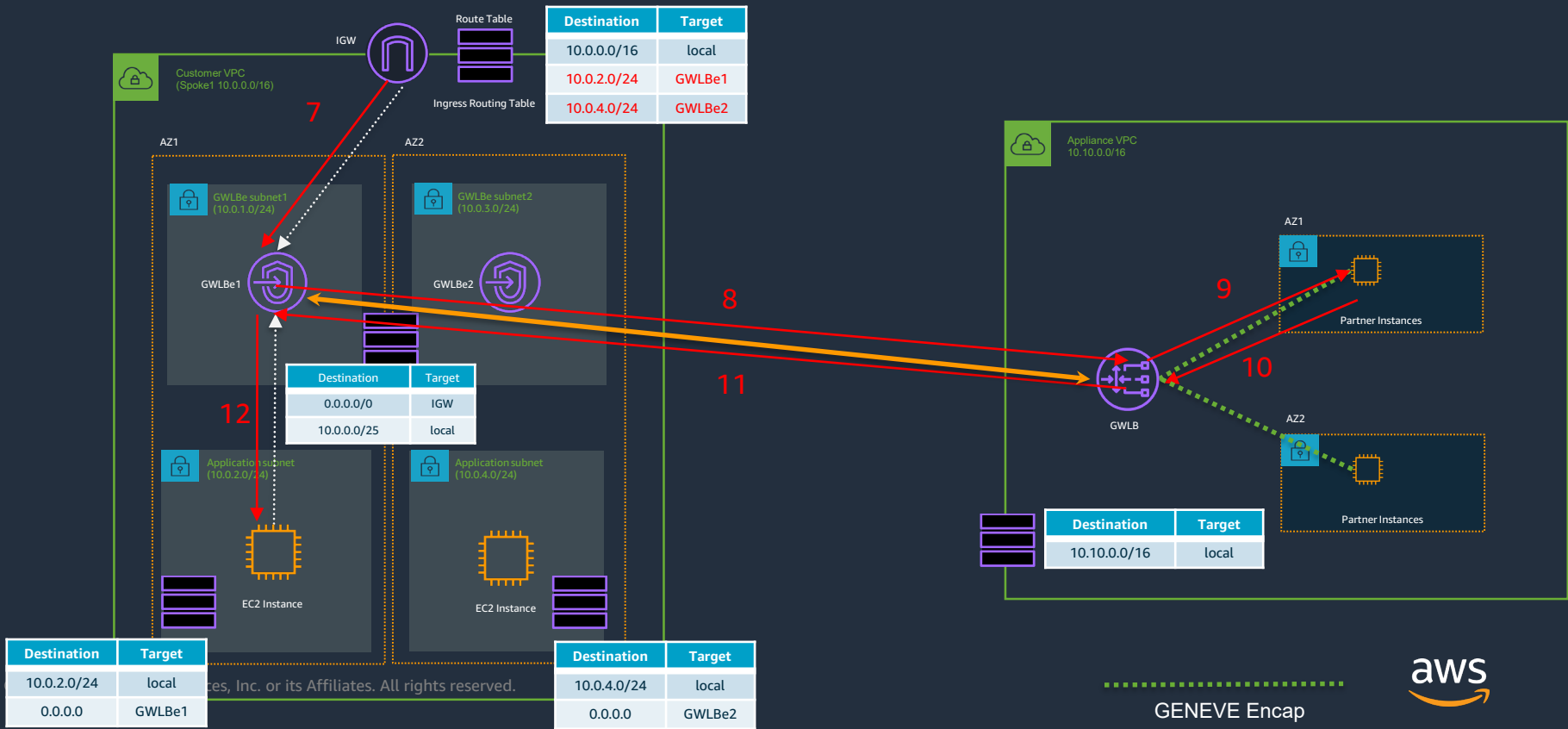
(AZ1より発信したInternet向けトラフィックインスペクション例)



Amazon.com, Inc. or its Affiliates. All rights reserved.

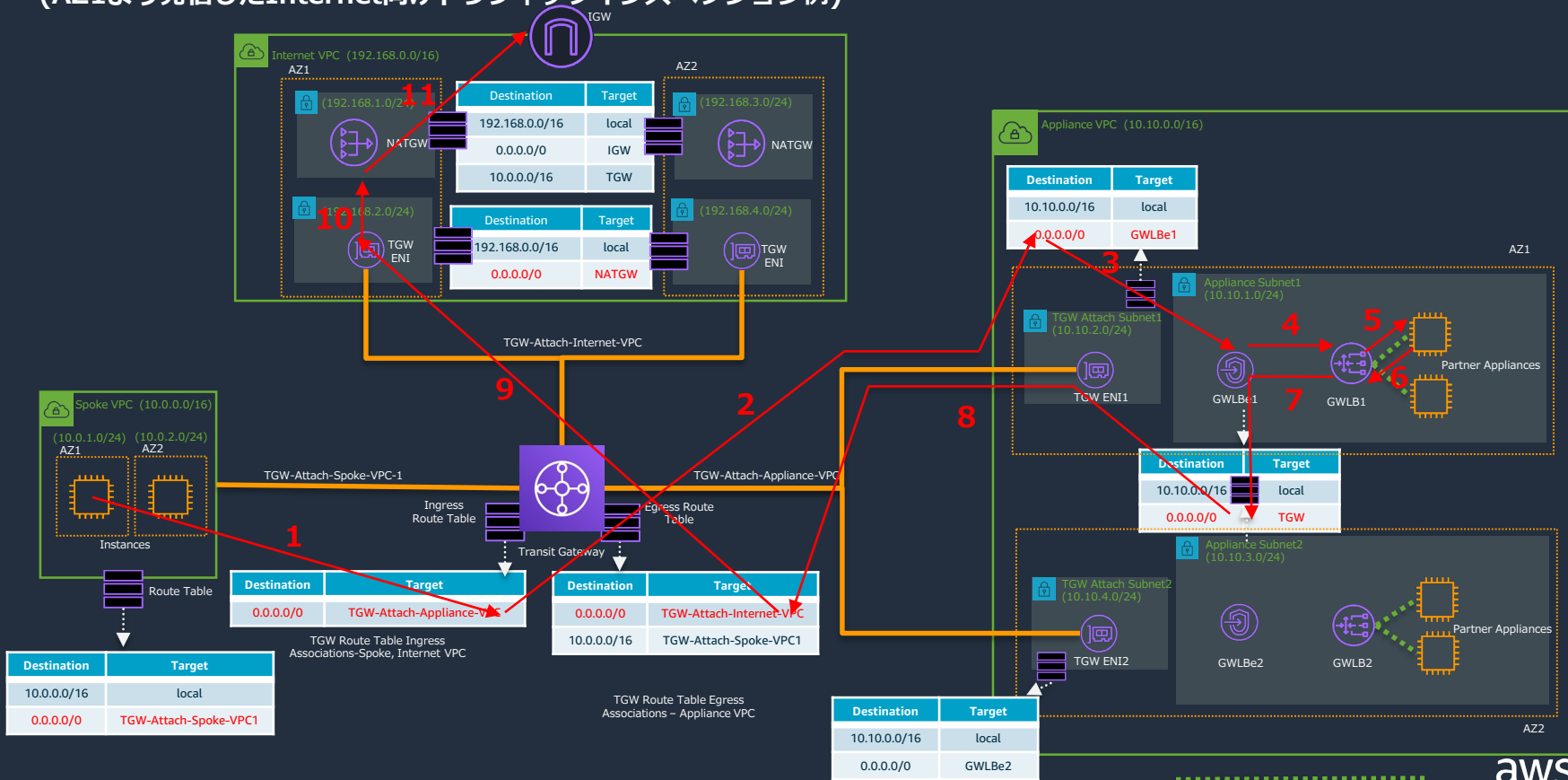
トラフィックフロー例1 Ingress Routing (戻り)

(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)



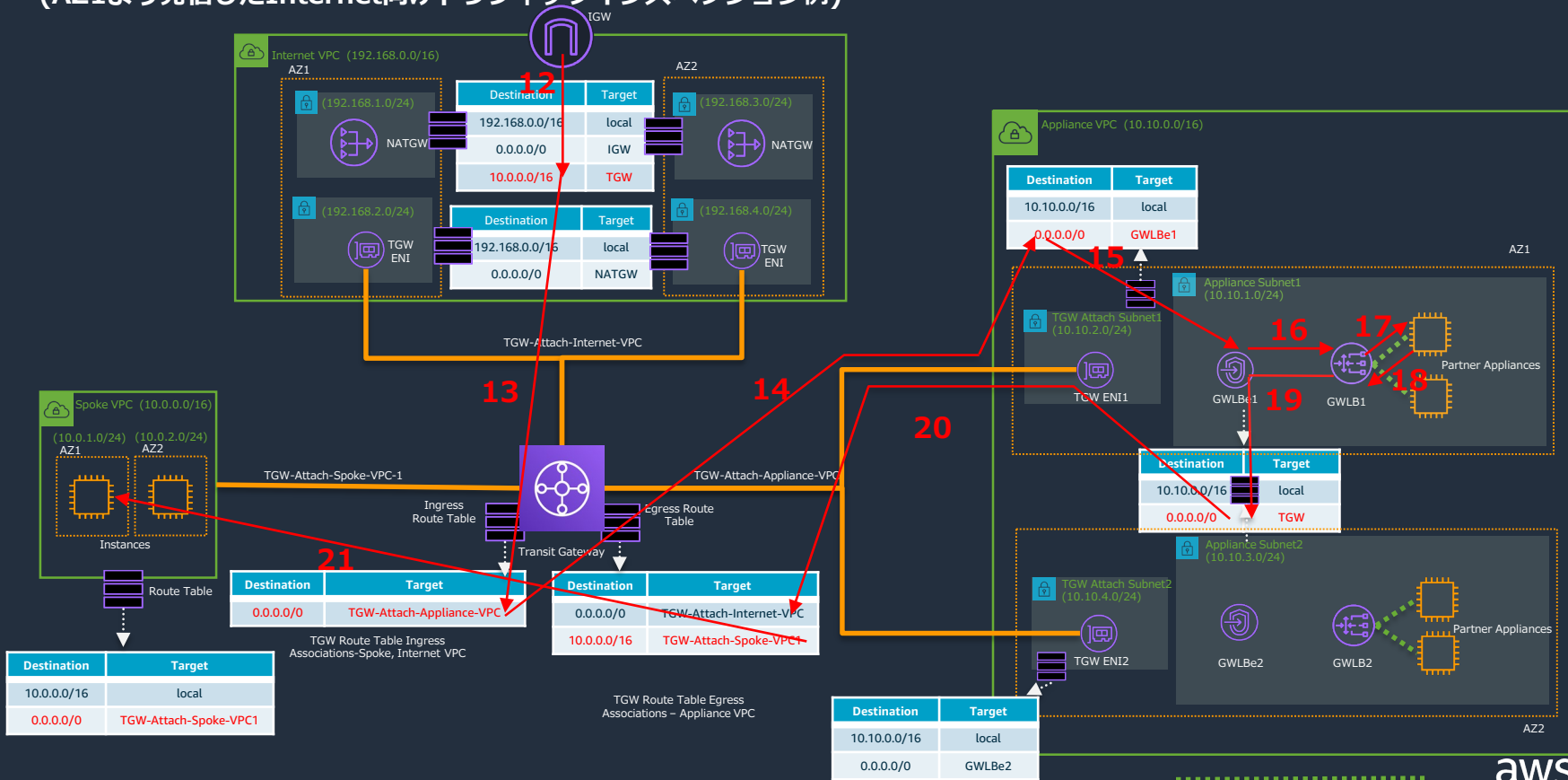
トラフィックフロー例2 Transit Gatewayと組合せ（行き）

(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)



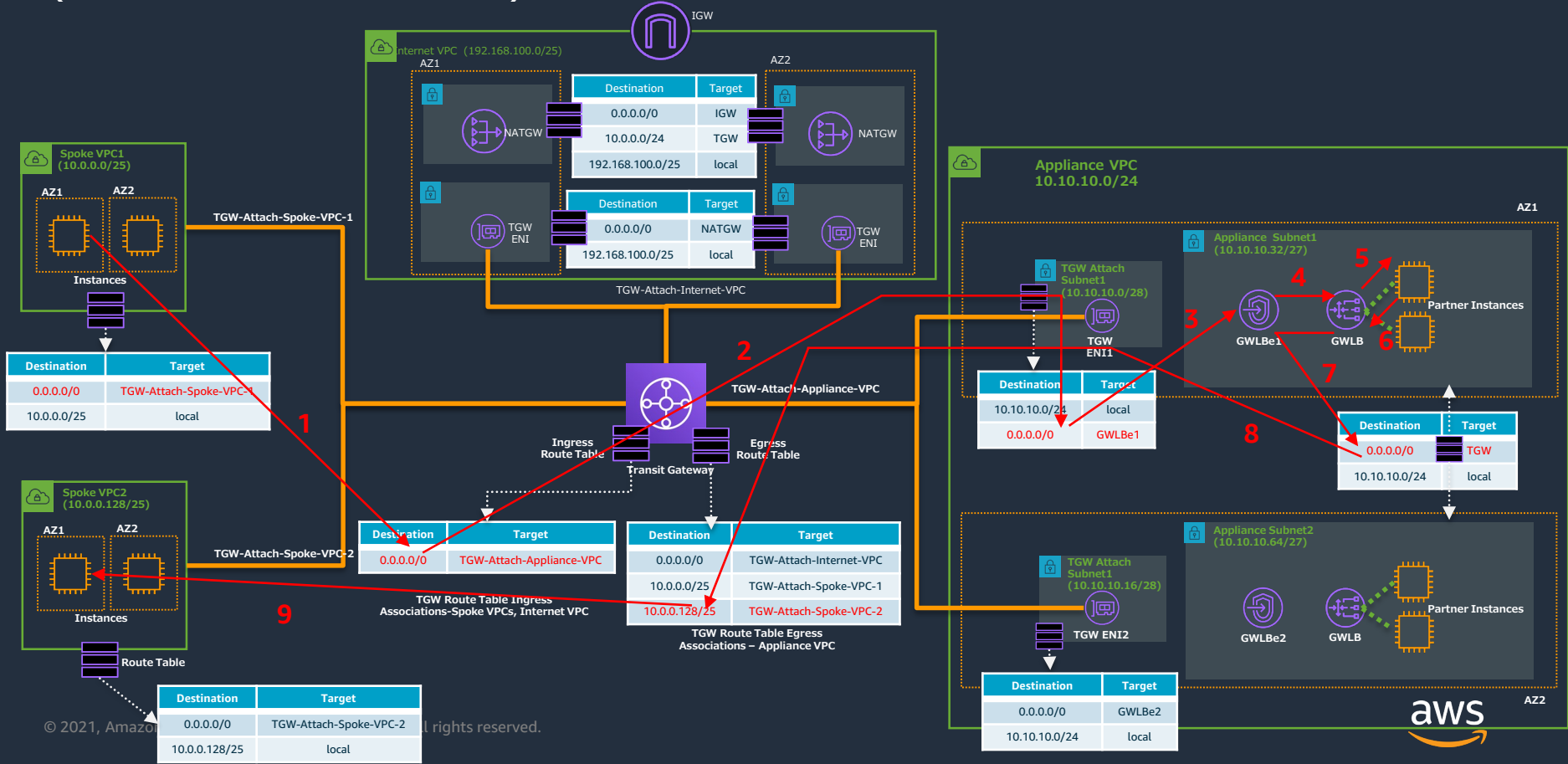
トラフィックフロー例2 Transit Gatewayと組合せ (戻り)

(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)



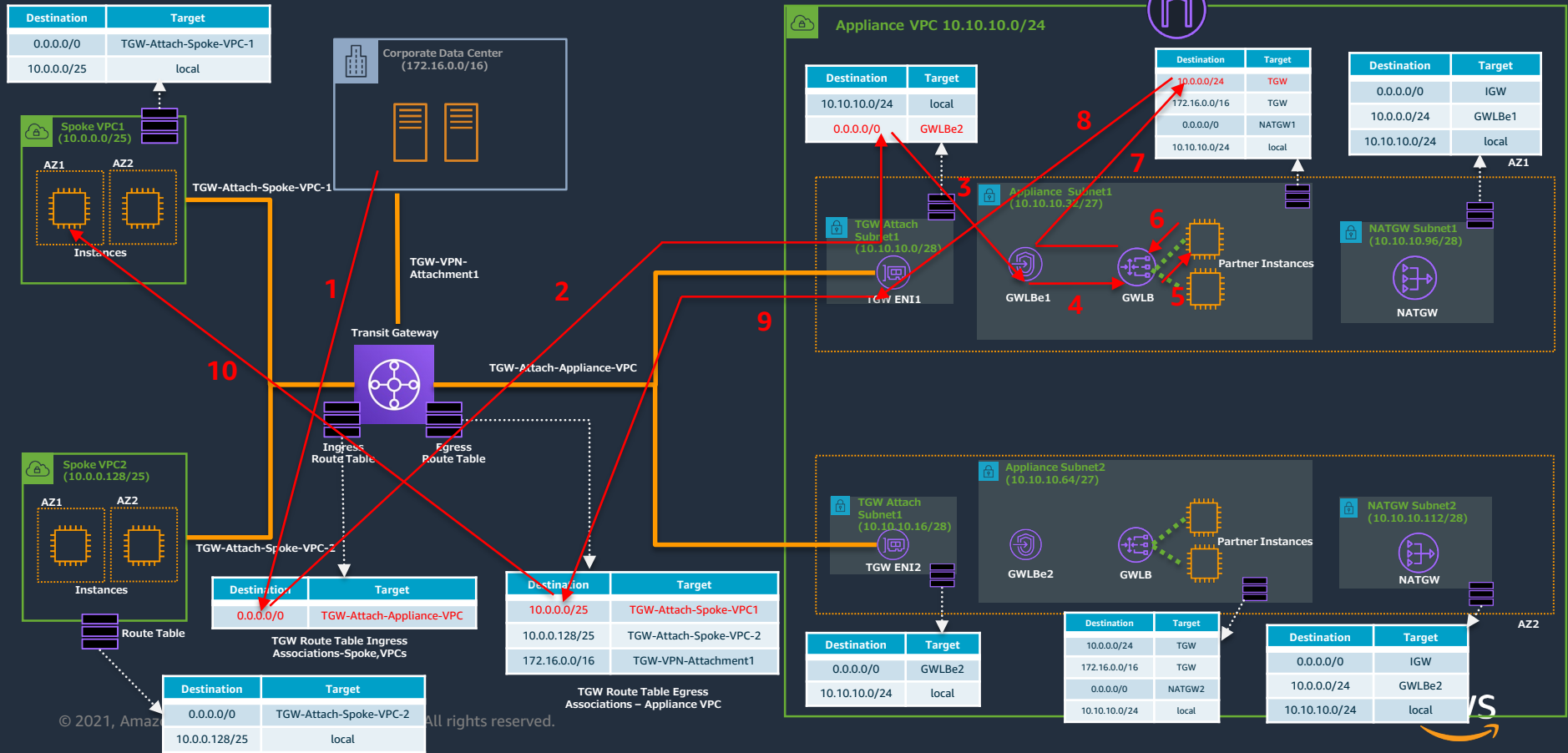
トラフィックフロー例3 Transit Gatewayと組合せ

(VPC間トラフィックインスペクション例)



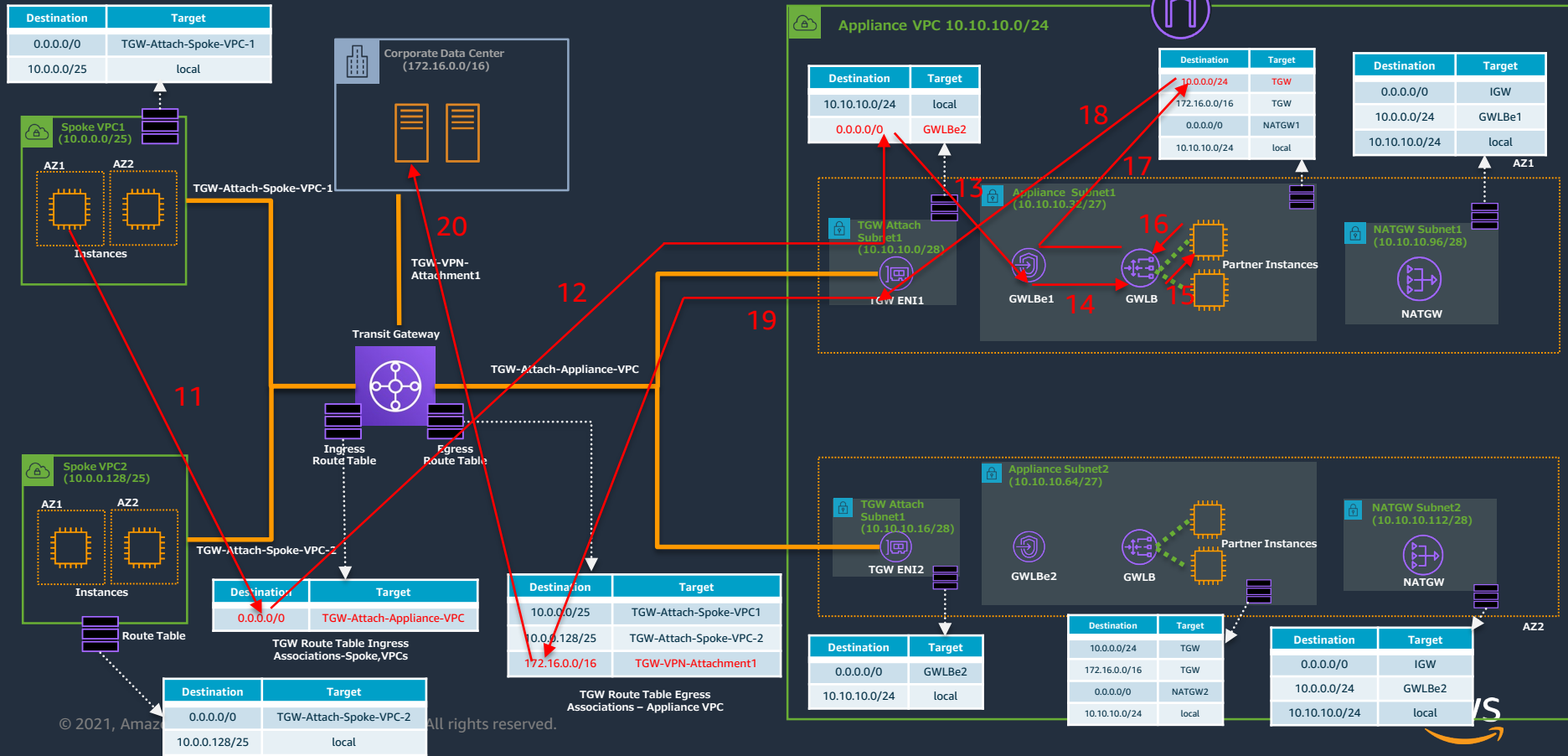
トラフィックフロー例4 Transit Gatewayと組合せ（行き）

（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）



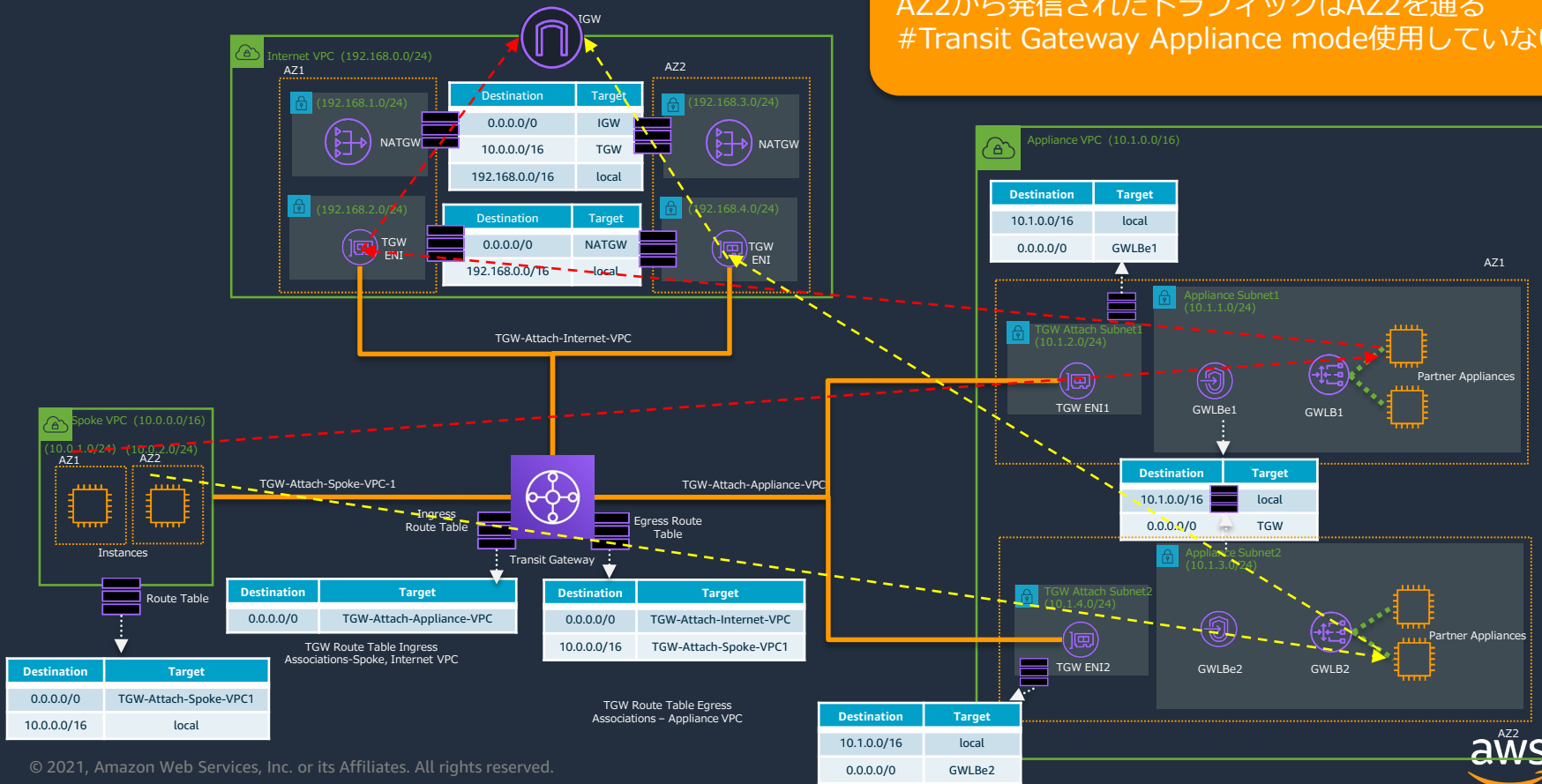
トラフィックフロー例4 Transit Gatewayと組合せ（戻り）

（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）



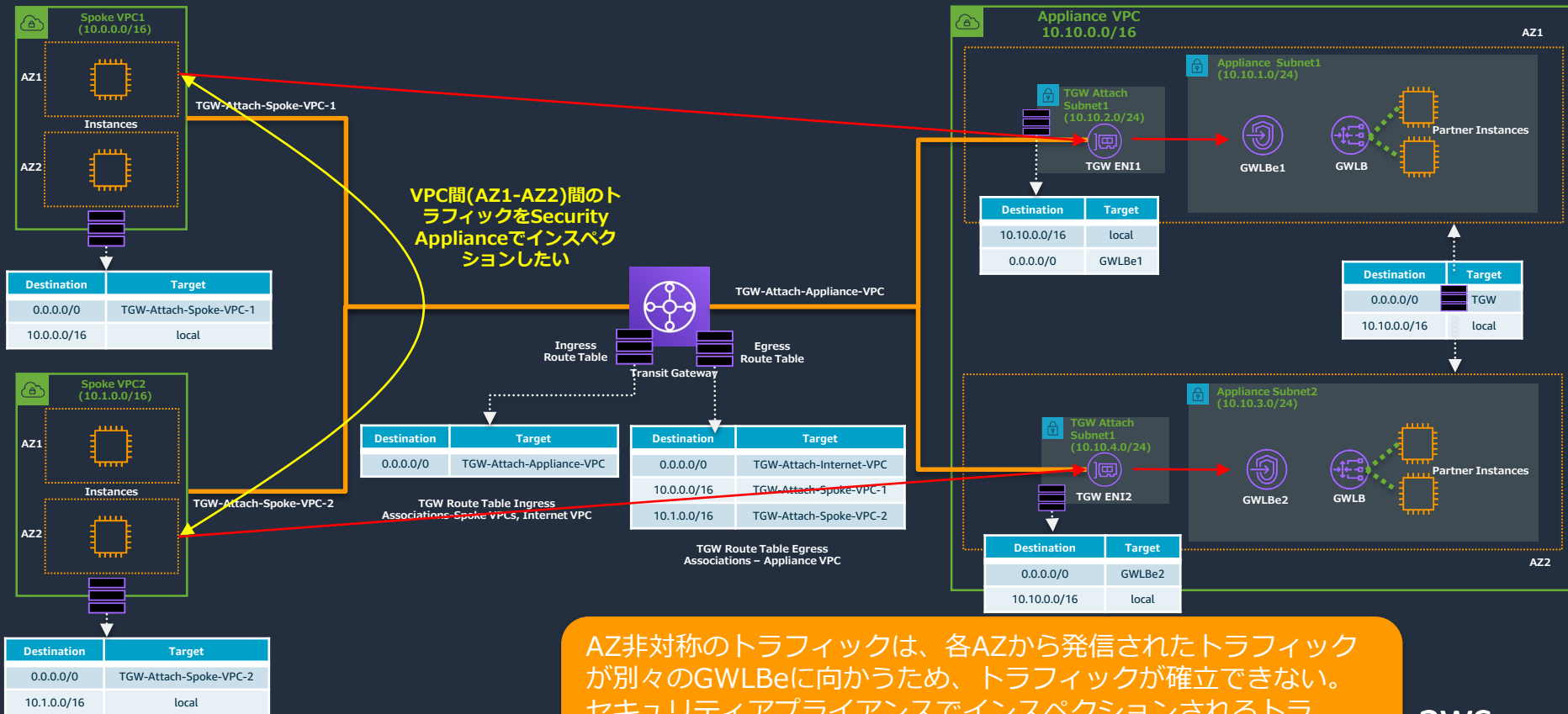
トラフィックフロー補足

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

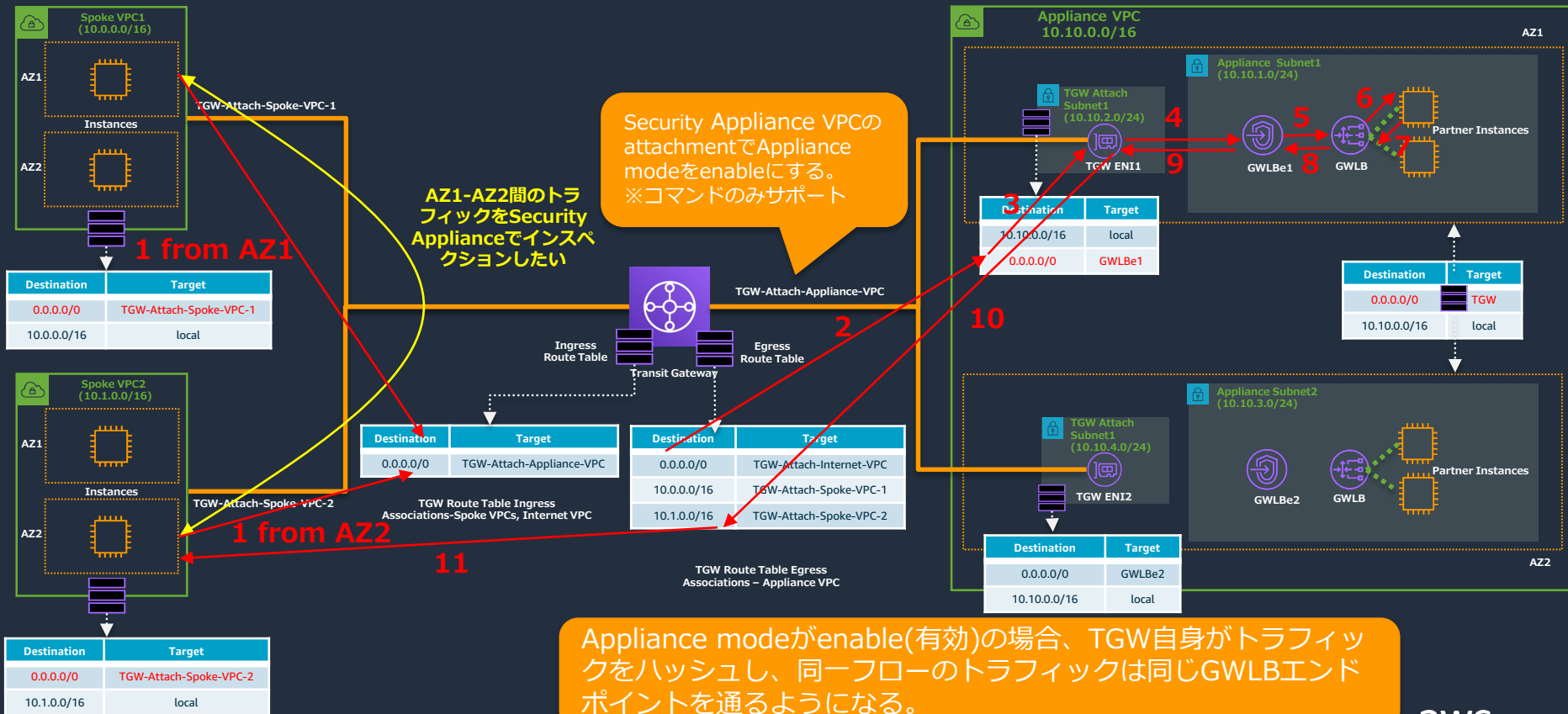
Transit Gateway Appliance mode disable (無効)



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。

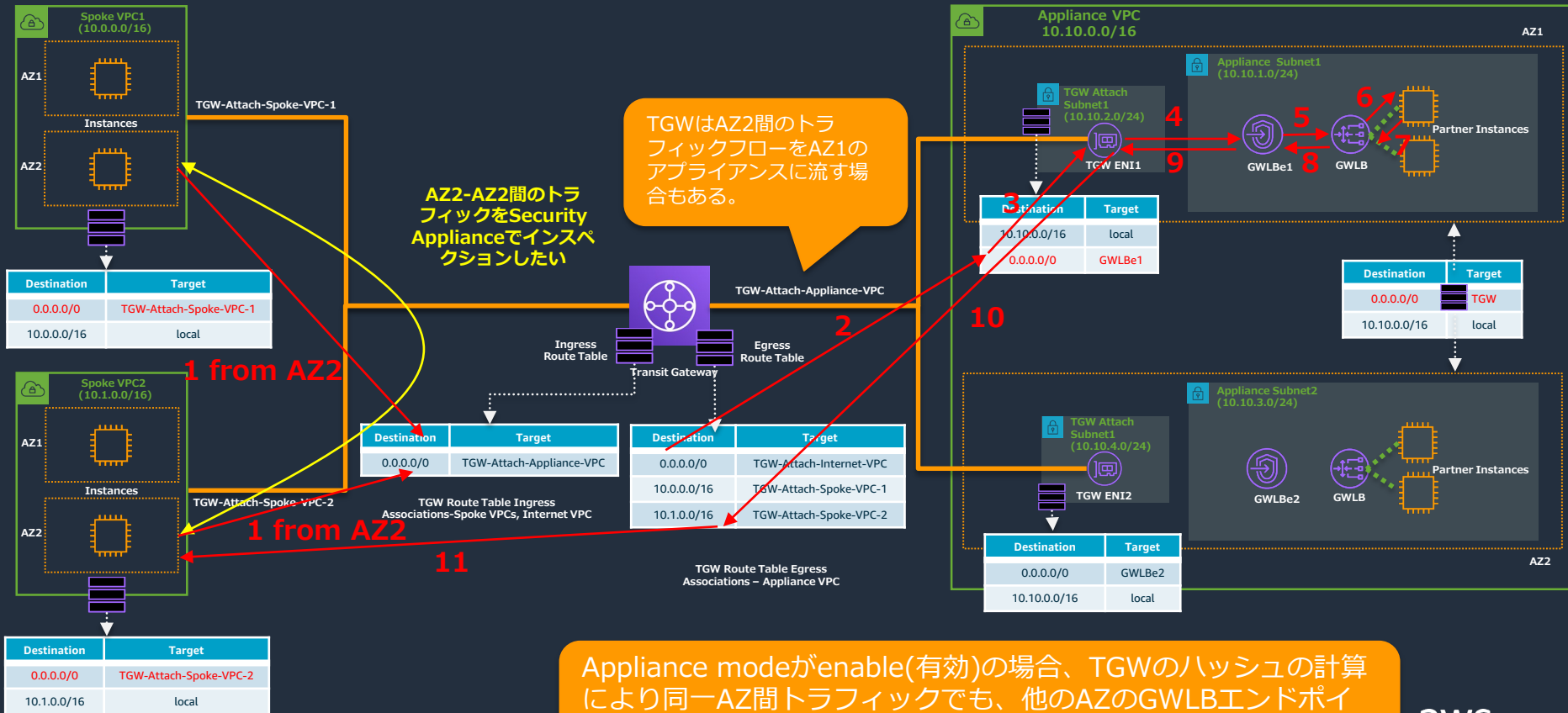
Transit Gateway Appliance mode enable (有効)

(AZを跨ぐトラフィック)



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

ロードバランサーの作成 アクション

タグや属性によるフィルター、またはキーワードによる検索

名前	DNS 名	状態	VPC ID	アベイラビリティゾーン	種類	作成日	モニ
GWLB1		active	vpc-06407c59f1e982ee	us-west-2b, us-west-2a	gateway	2020年11月26日 15:00:40 U...	

ロードバランサー: GWLB1

説明 リスナー モニタリング 統合サービス タグ

基本的な設定

名前	GWLB1
ARN	arn:aws:elasticloadbalancing:us-west-2:841259431336:loadbalancer:gwyl/GWLB1/61973f6577ef43d
状態	active
種類	gateway
IP アドレスタイプ	ipv4
VPC	vpc-06407c59f1e982ee
アベイラビリティゾーン	subnet-0643d966a6a606e78 - us-west-2b subnet-064d34c4094e8929 - us-west-2a
作成時刻	2020年11月26日 15:00:40 UTC-9

属性

削除保護	無効
クロスゾーン負荷分散	無効

属性の編集

ロードバランサー属性の編集

削除保護 有効化

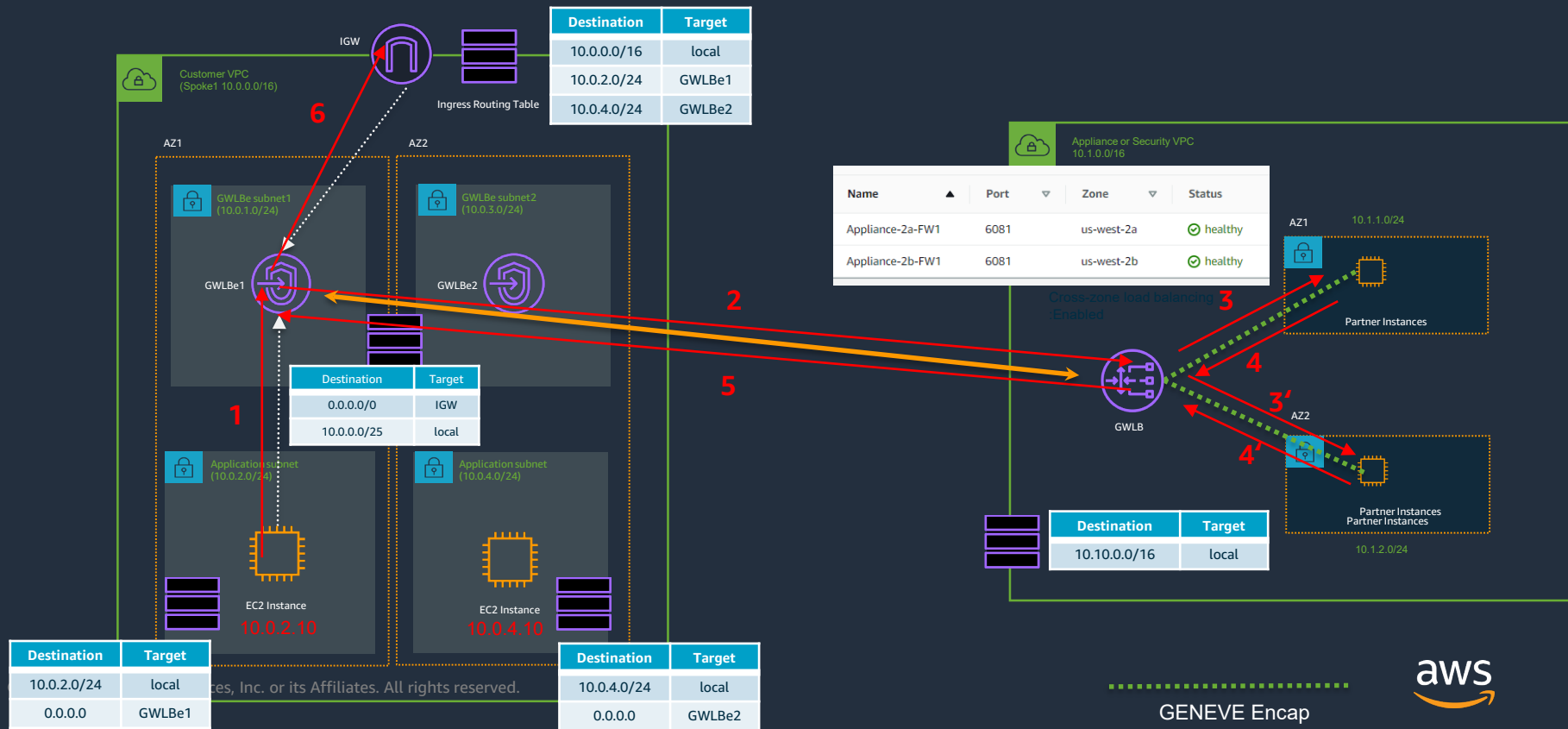
クロスゾーン負荷分散 有効化

クロスゾーン負荷分散を有効にすると、リージョンデータ転送料金が発生することがあります。詳細については、ドキュメントを参照してください。

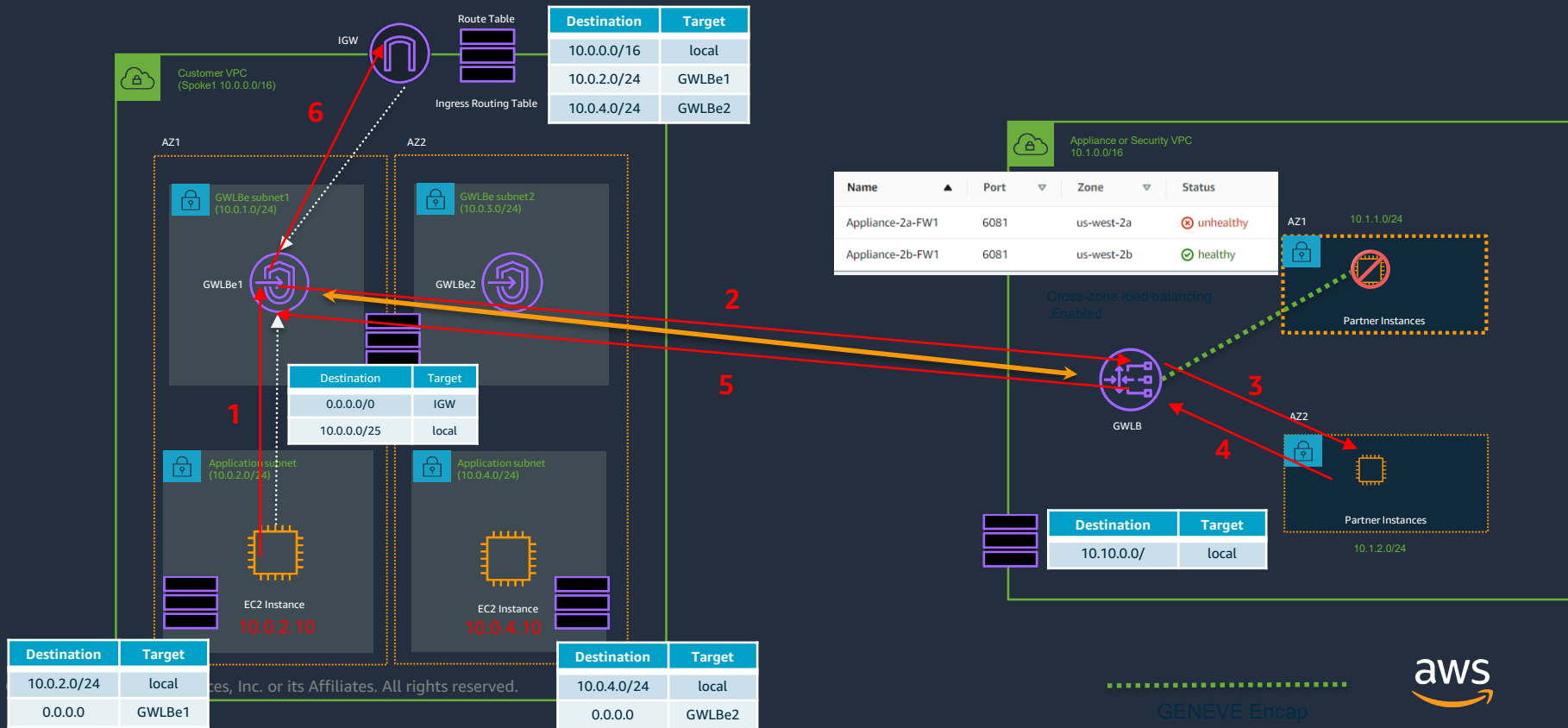
キャンセル 保存

- 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。

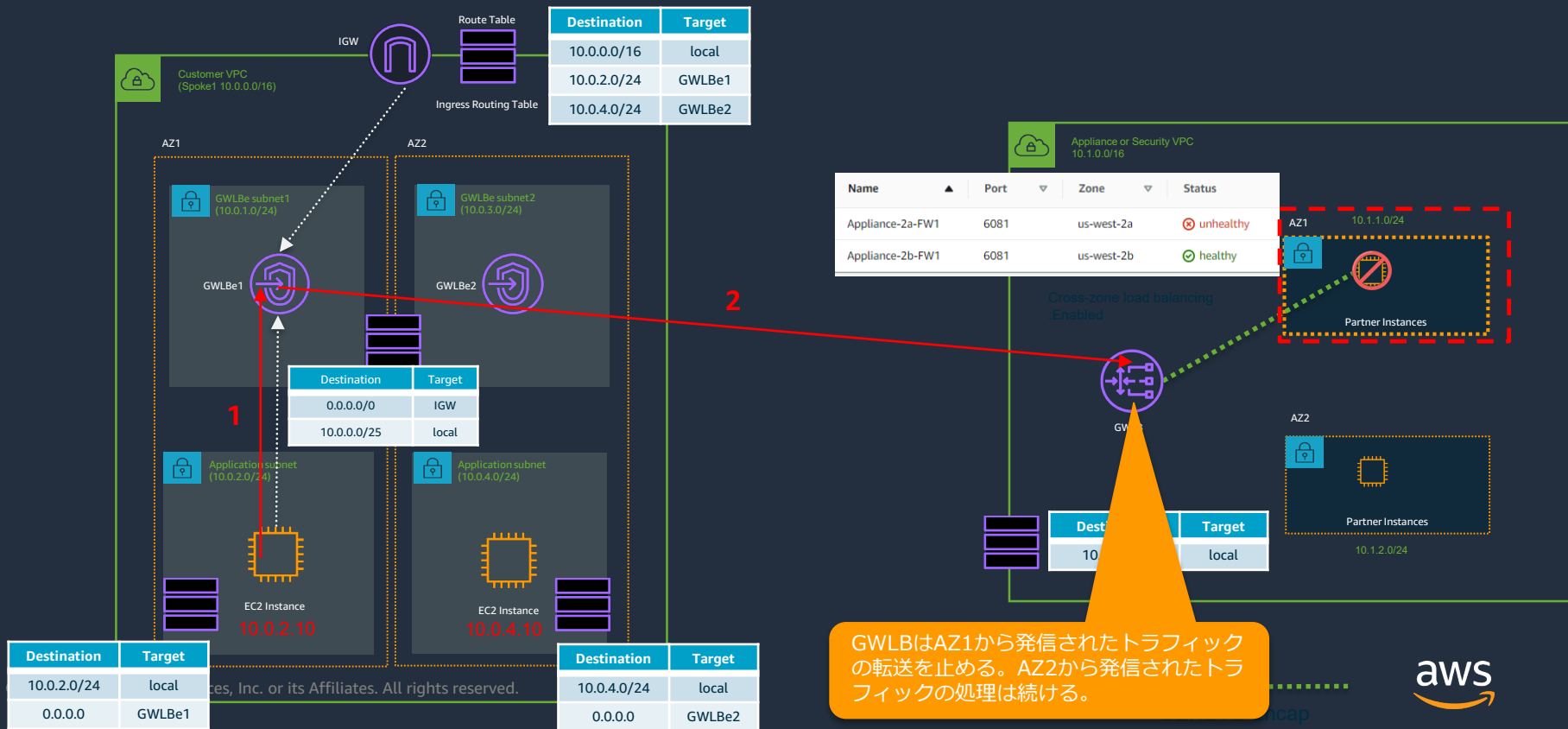
クロスゾーン負荷分散 (Appliance正常時)



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)

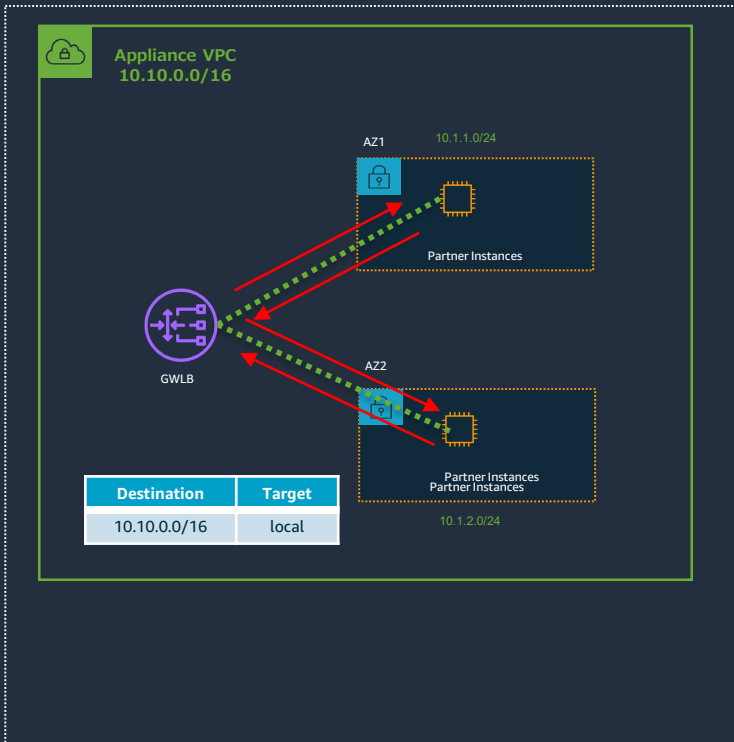


GWLBはAZ1から発信されたトラフィックの転送を止める。AZ2から発信されたトラフィックの処理は続ける。

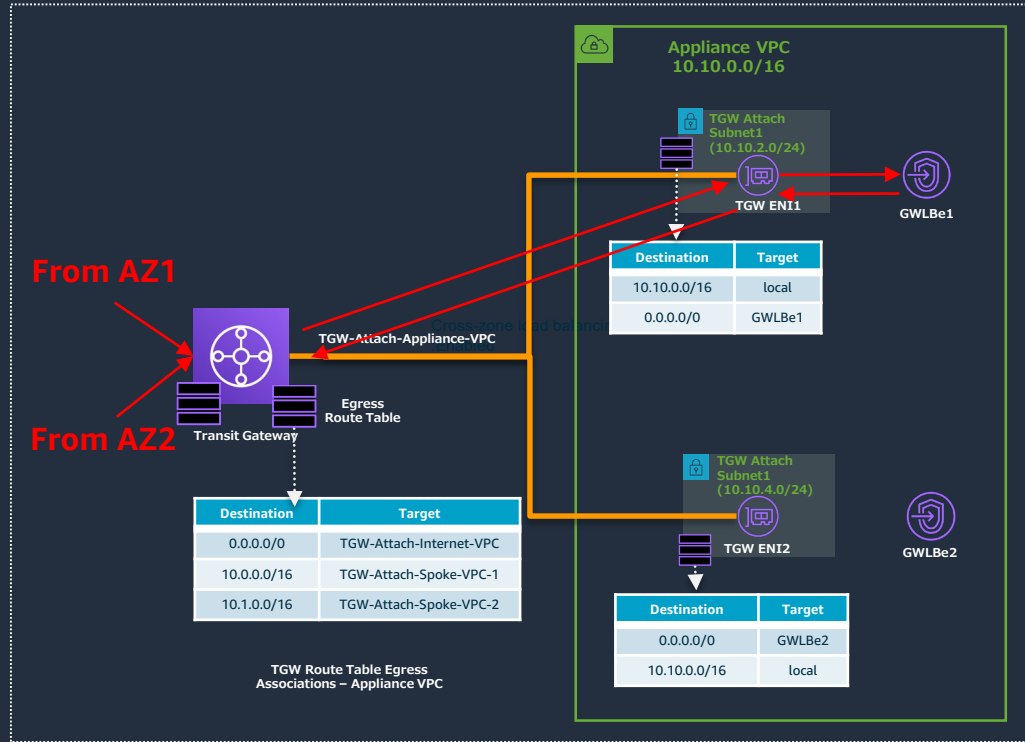


クロスゾーン負荷分散 vs TGW Appliance mode

クロスゾーン負荷分散



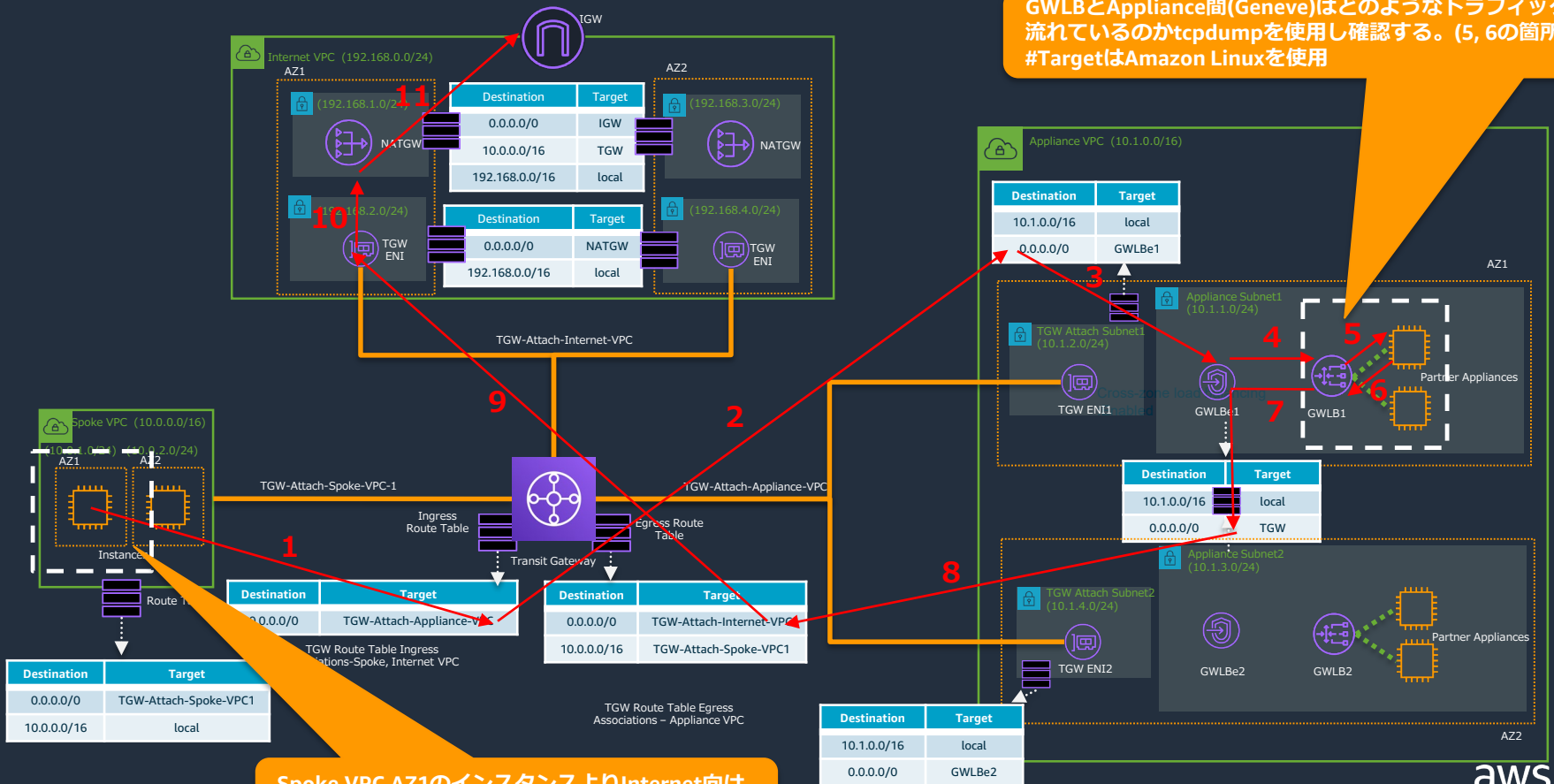
Transit Gateway Appliance mode



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

デモ1 GWLBe-GWLBe間はどのようなトラフィックが流れているのか？

GWLBeとAppliance間(Geneve)はどのようなトラフィックが流れているのかtcpdumpを使用し確認する。(5, 6の箇所)
#TargetはAmazon Linuxを使用



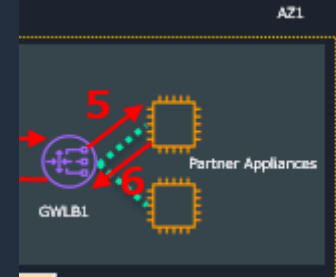
Spoke VPC AZ1のインスタンスよりInternet向けにトラフィックを発信。(ICMP)





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

GWLBe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 packets はそのまま維持されている。(透過的)
#Geneveのport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

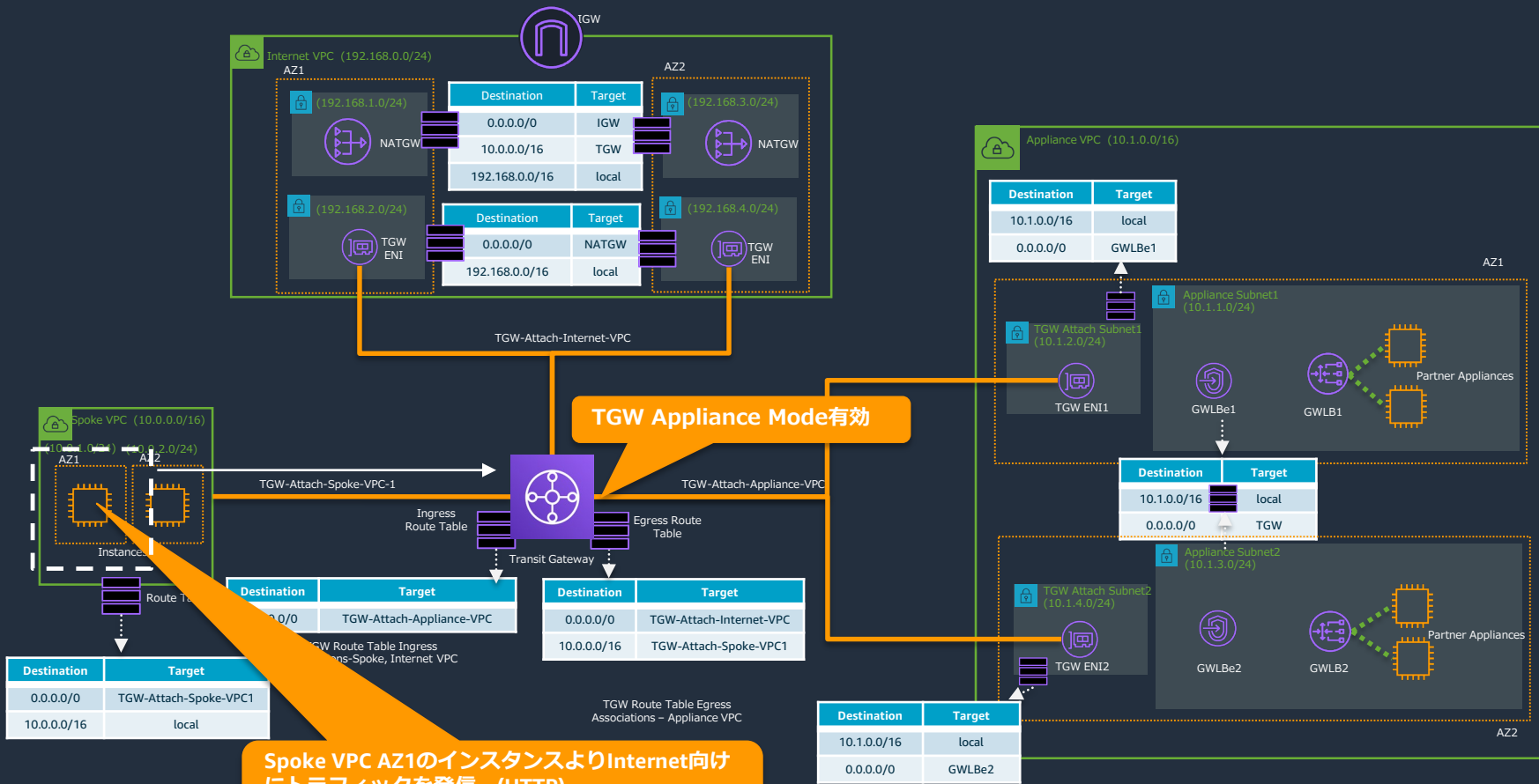
★ Geneve Src Dst GWLB(10.0.10.164) → Appliance(10.0.10.10) 5

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



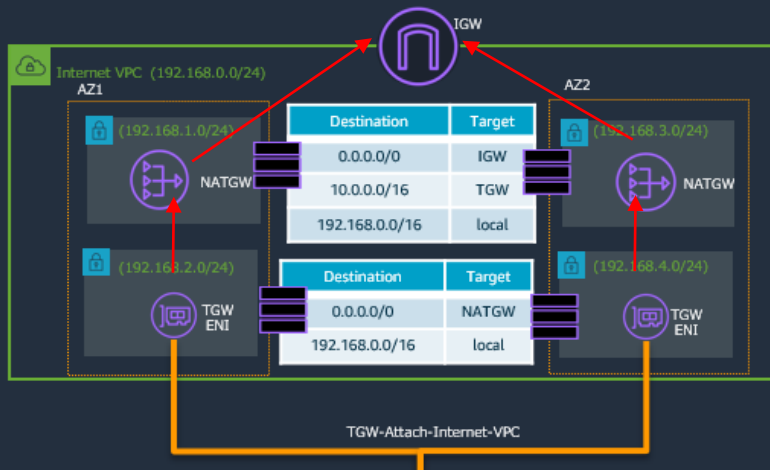


デモ2 TGW上でAppliance Modeを有効にした場合の動作（補足）

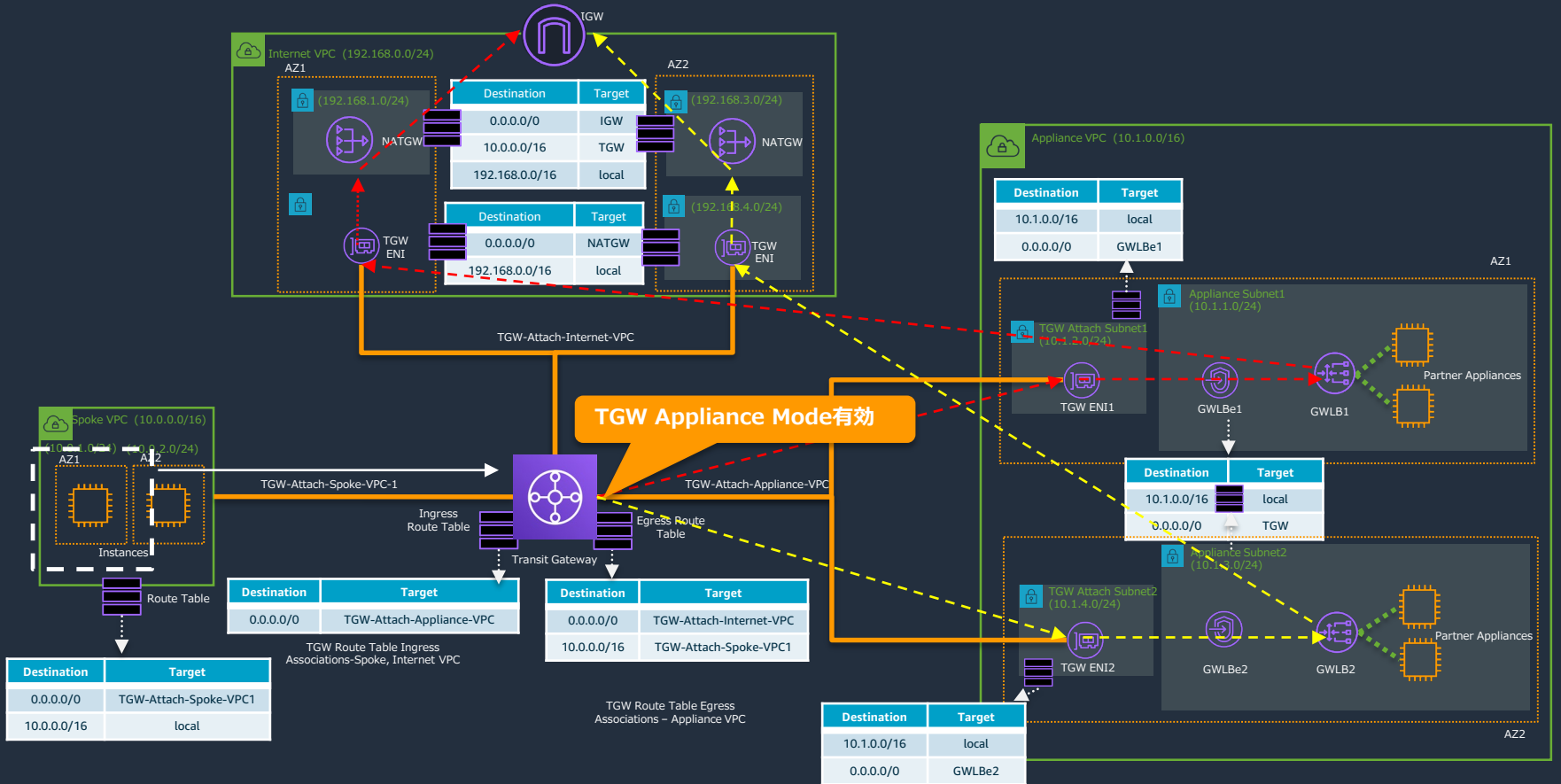
<https://checkip.amazonaws.com/>

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)

<input type="radio"/>	Internet-AZ1	nat-0c1bd6c57046c4251	✔ Available	-	18.180.165.230	192.168.1.113
<input type="radio"/>	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)

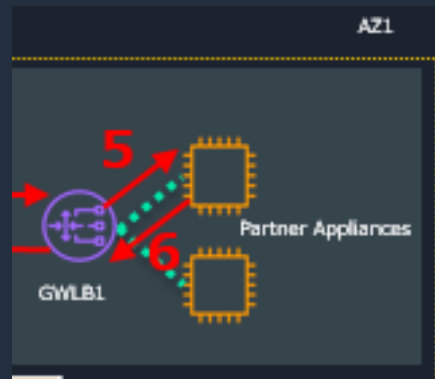


補足

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

Outer IPv4 Header:

0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
Version	IHL	Type of Service	Total Length																		
Identification										Flags					Fragment Offset						
Time to Live										Protocol =17 UDP					Header Checksum						
Outer Source IPv4 Address																					
Outer Destination IPv4 Address																					
Source Port = xxxx										Dest Port = 6081 Geneve											
UDP Length											UDP Checksum										

Outer Geneve Header:

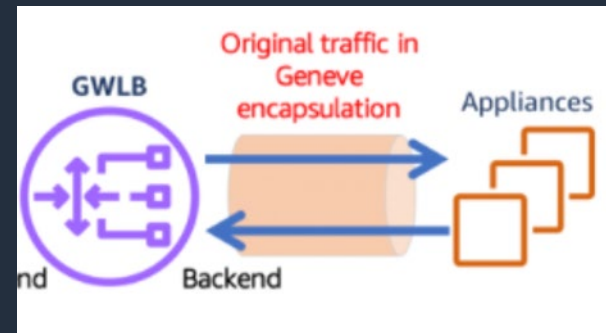
V=0	Opt Len = 8	0 C	Rsvd.	Protocol Type = 0x0800																	
Virtual Network Identifier (VNI) = 0										Reserved											

Outer Geneve Options: AWS Gateway Load Balancer TLVs

Option Class = 0x0108 (AWS) Type = 1 R R R Len = 2																					
64-bit GWLBE ENI ID																					
Option Class = 0x0108 (AWS) Type = 2 R R R Len = 2																					
64-bit Customer Visible Attachment ID																					
Option Class = 0x0108 (AWS) Type = 3 R R R Len = 1																					
32-bit Flow Cookie																					

Original IPv4 Packet in Inner Ethernet Packet follows...

Ethertype of Original Payload																					
Original Ethernet Payload																					



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GWLBEnd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GWLBEndポイントを作成できるようになります。

The screenshot shows the AWS Management Console interface for creating a Gateway Load Balancer endpoint service. The left sidebar contains navigation options, with 'エンドポイントサービス' (Endpoint Services) highlighted. The main content area shows a table of endpoint services, with one service selected. Below the table, there are buttons for '詳細' (Details), 'ホワイトリストに登録されたプリンシパル' (Principals registered in the whitelist), 'エンドポイント接続' (Endpoint connections), '通知' (Notifications), and 'タグ' (Tags). A callout box points to the 'ホワイトリストに登録されたプリンシパル' button, stating: 'ホワイトリストにプリンシパルを追加するをクリック。' (Click 'Add principal to whitelist'). Below this, there is a section for managing permissions, with a button 'ホワイトリストにプリンシパルを追加する' (Add principal to whitelist) highlighted. A callout box points to the 'arn:aws:iam::818003313395:root' principal in the table below, stating: '許可されたアカウント名が表示。' (The allowed account name is displayed).

ホワイトリストにプリンシパルを追加するをクリック。

ホワイトリストに登録されたプリンシパル

ホワイトリストにプリンシパルを追加する

許可されたアカウント名が表示。

Name	ID	タイプ	サービス名
GWLBEndポイント	vpce-svc-0269a885f63c0206b	GatewayLoadBalancer	com.amazonaws.vpce.ap-northeast-1.vpc...

ID	タイプ
arn:aws:iam::818003313395:root	アカウント

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 endpoint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 endpoint数	1
Gateway Load Balancer endpointごとの最大帯域幅	40 Gbps

Gateway Load Balancerのご利用料金

(*) パーソ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

① GWLB時間あたりの料金

0.0135 USD/時間

+

② GWLB 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

+

③ GWLB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

技術ブローガー一覧

<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

ロードバランサーの設定画面で Gateway Load Balancer を選択する。

ロードバランサーの種類の選択

Elastic Load Balancing は 4 種類のロードバランサー (Application Load Balancer、Network Load Balancer、Gateway Load Balancer および Classic Load Balancer) をサポートします。お客様のニーズに合うロードバランサーの種類を選択してください。お客様に最適なロードバランサーの詳細

Application Load Balancer



[作成](#)

HTTP および HTTPS トラフィックを使用するウェブアプリケーション用に柔軟性の高い機能セットが必要な場合は、Application Load Balancer を選択します。Application Load Balancer はリクエストレベルで動作し、マイクロサービスとコンテナを含む、アプリケーションアーキテクチャを対象とした高度なルーティングおよび可視性機能を提供します。

[詳細はこちら >](#)

Network Load Balancer



[作成](#)

非常に高いパフォーマンス、大規模な TLS のオフロード、証明書のデプロイの一元管理、UDP のサポート、およびアプリケーションの静的 IP アドレスが必要な場合は、Network Load Balancer を選択します。Network Load Balancer は接続レベルで動作し、非常に低いレイテンシーを維持しながら、1 秒あたり数百万のリクエストを確実に処理することができます。

[詳細はこちら >](#)

Gateway Load Balancer



[作成](#)

GENEVE をサポートするサードパーティーの仮想アプリケーションのフリートをデプロイおよび管理する必要がある場合は、Gateway Load Balancer を選択します。これらのアプライアンスを使用すると、セキュリティ、コンプライアンス、ポリシー制御を向上させることができます。

[詳細はこちら >](#)

Classic Load Balancer

以前の世代
HTTP、HTTPS、および TCP

[作成](#)

EC2-Classic ネットワークで既存のアプリケーションを実行している場合は、Classic Load Balancer を選択します。

[詳細はこちら >](#)

Gateway Load Balancerを使用するには

aws サービス ▼

Q サービス、機能、マーケットプレースの製品、ドキュメントを検索し [Alt+S]

1. ロードバランサーの設定 2. ルーティングの設定 3. ターゲットの登録 4. 確認

手順 1: ロードバランサーの設定

基本的な設定

Gateway Load Balancer を設定するには、名前を入力し、ご使用の VPC、アベイラビリティゾーン、およびサブネットを選択する必要があります。このタイプのロードバランサーには、すべての接続リクエストを受信する IP リスナーが含まれています。受信します。

名前 ⓘ GWLB

IP アドレスタイプ ⓘ ipv4

Gateway Load Balancer がトラフィックをルーティングする VPC 及びサブネットを選択する。

アベイラビリティゾーン

ロードバランサーのアベイラビリティゾーンを指定します。ロードバランサーは、指定されたアベイラビリティゾーンからサブネットを指定する必要があります。

VPC ⓘ vpc-0af0c4c12fc79216b (10.1.0.0/16) | Appliance

アベイラビリティゾーン ⓘ

- us-west-2a subnet-0e7c7be87425fd4e3 (Appliance-2a-FW)
- us-west-2b subnet-049852b79adcb0cd (Appliance-2b-FW)

ⓘ アベイラビリティゾーンとサブネットは慎重に選択してください。ロードバランサーを作成し

aws サービス ▼

Q サービス、機能、マーケットプレースの製品、ドキュメントを検索し [Alt+S]

1. ロードバランサーの設定 2. ルーティングの設定 3. ターゲットの登録 4. 確認

手順 2: ルーティングの設定

Your load balancer routes requests to the targets in this target group using the protocol and port that you specify, and performs health checks on the targets using these health check settings. You can add listeners after the load balancer is created.

ターゲットグループ

ターゲットグループ ⓘ 新しいターゲットグループ

名前 ⓘ GWLB

ターゲットの種類

- インスタンス
- IP

プロトコル: ポート GENEVE : 6081

ヘルスチェック

プロトコル ⓘ TCP

▶ ヘルスチェックの詳細設定

プロトコルがGENEVEになっている。変更は不可。

Gateway Load Balancerを使用するには

aws サービス ▼

検索 サービス、機能、マーケットプレースの製品、ドキュメントを検索し [Alt+S]

1. ロードバランサーの設定 2. ルーティングの設定 3. ターゲットの登録 4. 確認

手順 3: ターゲットの登録

ターゲットグループにターゲットを登録します。有効にしたアベイラビリティゾーンにターゲットを登録し、初回のヘルスチェックに合格するとすぐに、ロードバランサーがターゲットにトラフィックを送ります。

登録済みターゲット

インスタンスを登録解除するには、1つ以上の登録インスタンスを選択し、[削除] をクリックします。

削除	インスタンス	名前	ポート	状態
<input type="checkbox"/>	i-065cbcab04337d7fd	Appliance-2b-FW2	6081	● running
<input type="checkbox"/>	i-015d58dd63a05e174	Appliance-2a-FW1	6081	● running

インスタンス

追加のインスタンスを登録するには、1つ以上の実行中のインスタンスを選択し、ポートを指定して、[追加] をクリックします。されている場合は、別のポートを指定する必要があります。

登録済みに追加 ポート 6081

ターゲットのセキュリティアプライアンスを登録する。

確認画面が表示され、作成をクリックしたら作成終了。

手順 4: 確認

続行する前にロードバランサーの詳細を確認してください。

ロードバランサー

名前 GWLB
IP アドレスタイプ ipv4
VPC vpc-0af0c4c12fc79216b (Appliance)
サブネット subnet-0e7c7be87425fd4e3 (Appliance-2a-FW), subnet-049852b797adcb0cd (Appliance-2b-FW)
タグ

ルーティング

ターゲットグループ 既存のターゲットグループ
ターゲットグループ名 GWLB
ポート 6081
ターゲットの種類 instance
プロトコル GENEVE
ヘルスチェックプロトコル TCP
ヘルスチェックポート 80
正常のしきい値 3
非正常のしきい値 3
タイムアウト 5
間隔 10

キャンセル 戻る 作成

Gateway Load Balancerを使用するには

aws サービス ▼

サービス、機能、マーケットプレースの製品、ドキュメントを検索し [Alt+S]

エンドポイントのサービス > エンドポイントサービスの作成

エンドポイントサービスの作成

PrivateLink テクノロジーを使用して、VPC のサービスを他の AWS アカウントおよびサービスで共有する。PrivateLink は、サービスにプライベートアクセスできる可用性の高いスケーラブルなテクノロジーです。他のアカウントおよびサービスが、お客様のエンドポイントサービスにアクセスするインターフェイスエンドポイントを作成します。詳細は、AWS PrivateLink のドキュメントを参照してください。

Network Load Balancer の関連付け **GWLB** 新規 Network Load Balancer を作成

search: GWLB フィルターを追加

Network Load Balancer 名	Availability Zone	Type
Appliance-2b-GWLB2	us-west-2b	gateway
Appliance-2a-GWLB	us-west-2a	gateway
GWLB	us-west-2a.us-west-2b	gateway

含まれる Availability Zone us-west-2a (usw2-az1) ⓘ

us-west-2b (usw2-az2)

除外する Availability Zone us-west-2c (usw2-az3) ⓘ

us-west-2d (usw2-az4)

エンドポイントの承諾が必要 承諾が必要 ⓘ

Enable private DNS name Associate a private DNS Name with the service. ⓘ

キー (最大 127 文字)

値 (最大 255 文字)

このリソースには現在、タグがありません

タグの追加 残り 50 (最大 50 タグ)

エンドポイントサービスを作成する Gateway Load Balancer を選択し、サービスの作成をクリック。

aws サービス ▼

サービス、機能、マーケットプレースの製品、ドキュメントを検索し [Alt+S]

エンドポイントサービスの作成 アクション ▼

Name: GWLB フィルターを追加

Name	ID	タイプ	サービス名
GWLB	vpce-svc-07fd9be81b606e0c	GatewayLoadBalancer	com.amazonaws.vpce.us-west-2.vpce-svc...

エンドポイントサービスを作成後サービス名を確認する。このサービス名を使用して、後ほど Gateway Load Balancer のエンドポイントを作成します。

エンドポイントサービス: vpce-svc-07fd9be81b606e0c

詳細 Network Load Balancer ... トラストに登録されたプリンシパル エンドポイント接続 通知

ID	vpce-svc-07fd9be81b606e0c
サービス名	com.amazonaws.vpce.us-west-2.vpce-svc...
Network Load Balancer ARN	arn:aws:vpce:us-west-2:123456789012:vpce-svc-07fd9be81b606e0c
承諾が必要	はい
プライベート DNS 名	-
Domain verification name	-
Domain verification value	-

キャンセル サービスの作成

aws

Gateway Load Balancerを使用するには

aws サービス

サービス、機能、マーケットプレースの製品、ドキュメントを検索し [Alt+S]

エンドポイント > エンドポイントの作成

エンドポイントの作成

VPCエンドポイントを使用して、ご使用のVPCを他のサービスへ安全に接続できます。インターネットエンドポイントには、PrivateLink が搭載されており、Elastic Network Interface (ENI) を介してサービス宛てのトラフィックのエンドポイントとして機能します。プライベートVPCエンドポイントは、サービスに対するトラフィックのルートテーブル内のルートを介して機能します。

サービス名でエンドポイントサービスを検索する。

サービスカテゴリ

AWS サービス
サービスを名前前で検索
ご使用の AWS Marketplace

サービス名 プライベートサービス名を入力して確認します。

com.amazonaws.vpce.us-west-2.vpce-svc-07fd9be8

サービス名が見つかりました。

検証

VPC: vpc-0250c937b13647a2d

サブネット

subnet-04c1c6478ff4d651f

アベイラビリティゾーン	サブネット ID
<input checked="" type="checkbox"/> us-west-2a (usw2-az1)	subnet-04c1c6478ff4d651f (spoke-172.16-2a)
<input checked="" type="checkbox"/> us-west-2b (usw2-az2)	subnet-03abozb95zaf9caz (spoke-172.16-2b)
<input type="checkbox"/> us-west-2c (usw2-az3)	このアベイラビリティゾーンではサポートされていないサービスです
<input type="checkbox"/> us-west-2d (usw2-az4)	このアベイラビリティゾーンではサポートされていないサービスです

VPCを選択し、エンドポイントを作成するサブネットを選択する。
※1度に複数のサブネットを選択し複数のエンドポイントは同時に作成する事はできません。

タグの追加 残り 50 (最大 50 タグ)

aws サービス

サービス、機能、マーケットプレースの製品、ドキュメントを検索し [Alt+S]

エンドポイントの作成 アクション

Name: GWLB-croszone_AZ1 Name: GWLB-croszone_AZ2 フィルターの追加

Name	エンドポイント ID	VPC ID	サービス名	エンドポイントタイプ
GWLB-croszone_AZ1	vpce-00a7e3ecd4...	vpce-011eb9d8298...	com.amazonaws.vpce.us-west-...	GatewayLoadBalancer
GWLB-croszone_AZ2	vpce-04c7c871cf8...	vpce-011eb9d8298...	com.amazonaws.vpce.us-west-...	GatewayLoadBalancer

エンドポイント: vpce-00a7e3ecd43a3431d

詳細 サブネット 通知 タグ

エンドポイント ID vpce-00a7e3ecd43a3431d
ステータス 使用可能
作成時刻 2020年12月26日 10:24:21 UTC+9
エンドポイントタイプ GatewayLoadBalancer
Private DNS names enabled -

各サブネットに必要な分エンドポイントを作成する。

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。

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



日本担当チームへお問い合わせ サポート 日本語 ▾ アカウント ▾

コンソールにサインイン

製品 ソリューション 料金 ドキュメント 学習 パートナー AWS Marketplace その他 🔍

AWS クラウドサービス活用資料集トップ

アマゾン ウェブ サービス (AWS) は安全なクラウドサービスプラットフォームで、ビジネスのスケールと成長をサポートする処理能力、データベースストレージ、およびその他多種多様な機能を提供します。お客様は必要なサービスを選択し、必要な分だけご利用いただけます。それらを活用するために役立つ日本語資料、動画コンテンツを多数ご提供しております。(本サイトは主に、AWS Webinar で使用した資料およびオンデマンドセミナー情報を掲載しています。)

[AWS Webinar お申込 »](#)

[AWS 初心者向け »](#)

[業種・ソリューション別資料 »](#)

[サービス別資料 »](#)

<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>

