AWS Gateway Load Balancer を用いた仮想アプライアンスの活用

Kazuma Nagaya

Solutions Architect, ISV/SaaS
Amazon Web Service Japan G.K

自己紹介

- 名前
  - 長屋 和真（ Kazuma Nagaya ）
- 所属
  - DNBソリューション本部
    ISV/SaaS Solutions Architect
- 経歴
  - ソフトェア会社 → 生命保険会社 社内SE
- 関心領域
  - ネットワーク周り
- 趣味
  - 美術館巡り、株

本日お伝えしたいこと

AWS Gateway Load Balancer をこれまで知らなかった方、
聞いたことがあるがよく知らなかった方向けに
セキュリティ仮想アプライアンスをAWS上で活用できる
サービスとしてどんなサービスかの理解と
セキュリティ対策の選択肢として認識頂く

アジェンダ

- はじめに
- AWS Gateway Load Balancer 概要
- AWS Gateway Load Balancer ユースケースと設定
- デモ

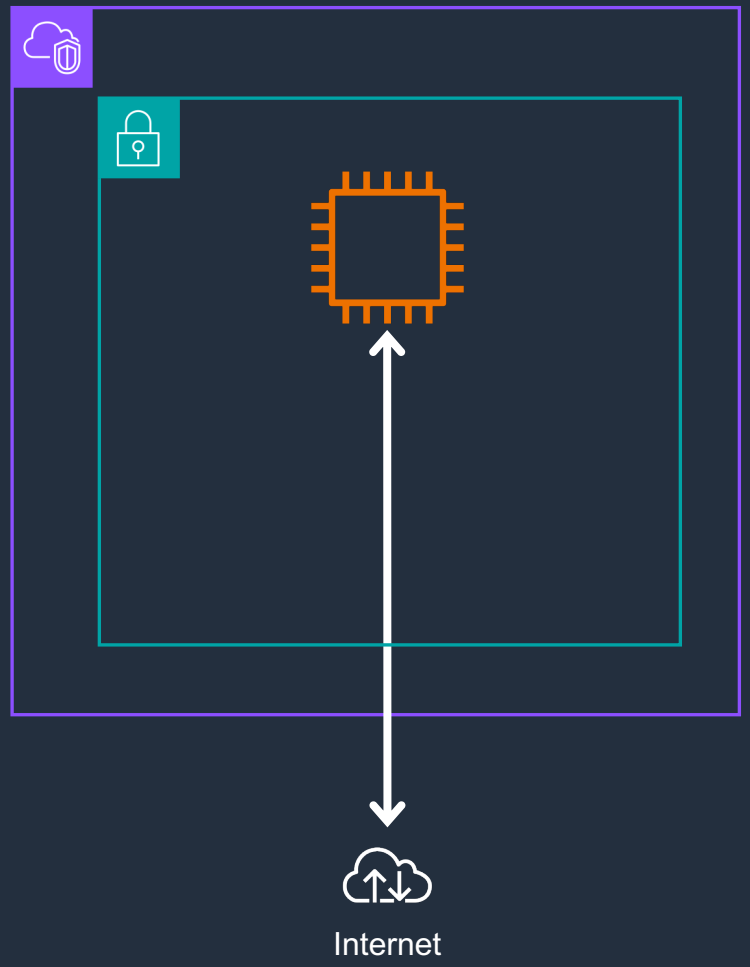
はじめに

セキュリティ仮想アプライアンス

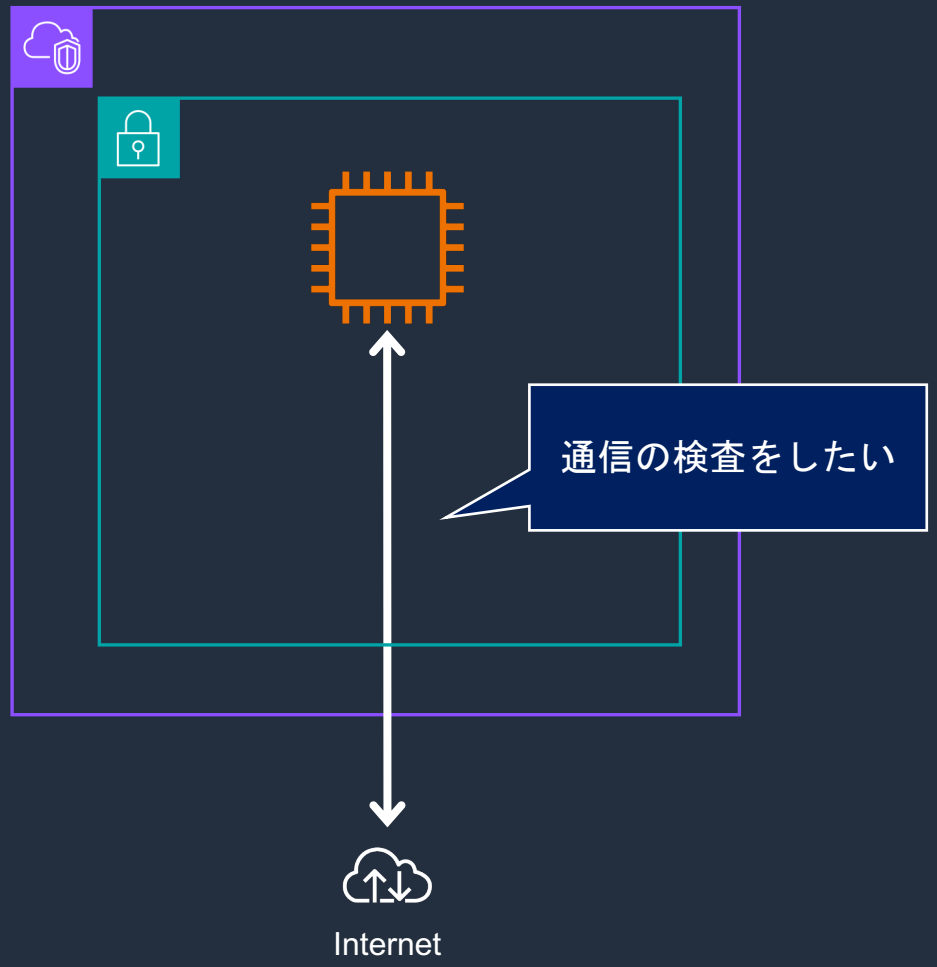
3rdパーティの製品をサーバーに導入
検査対象の通信を経由させて利用

- 侵入検知（IDS）
- 侵入防止（IPS）
- ディープパケットインスペクション
- ファイアウォール
- 情報漏洩防止

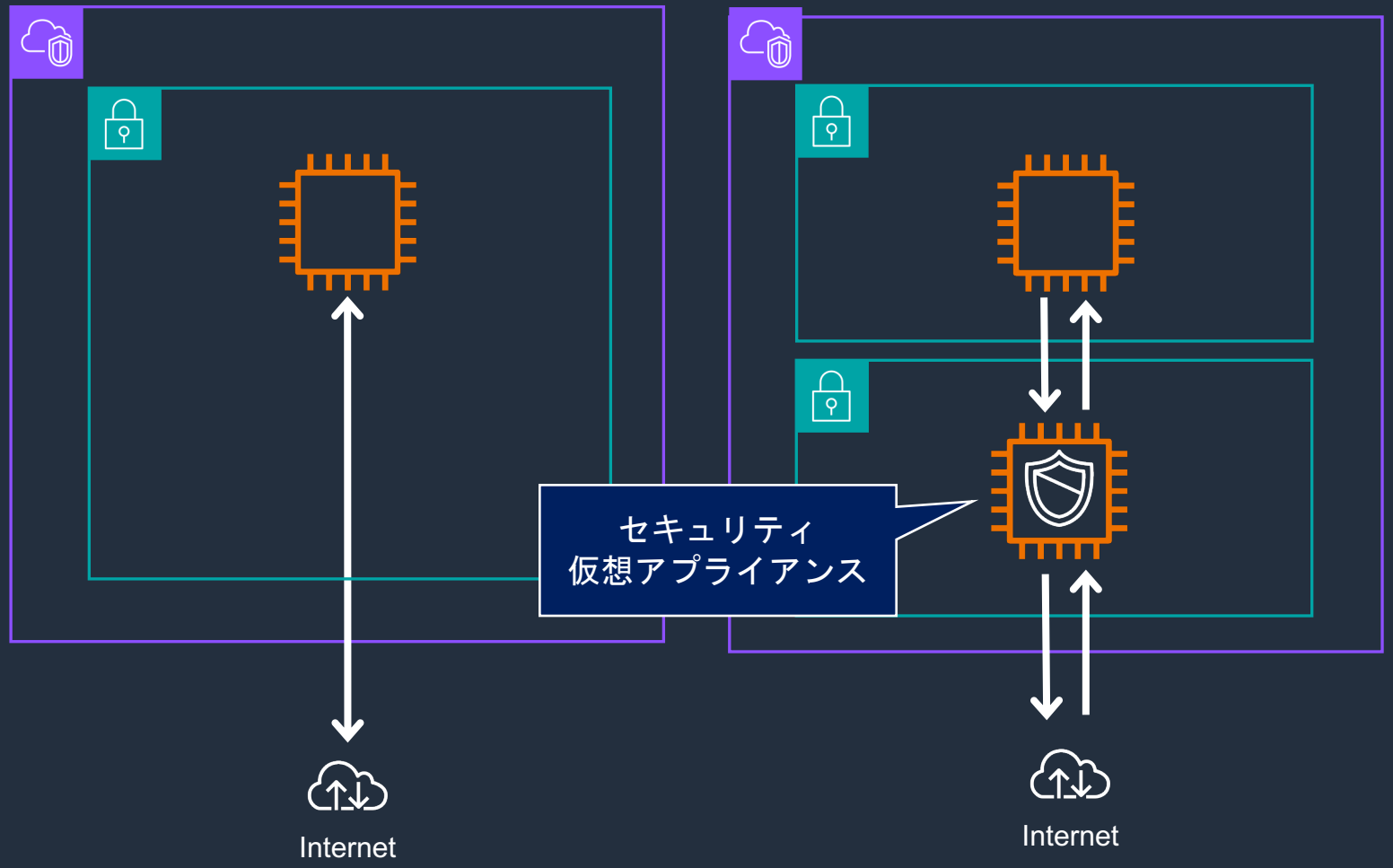
AWSでの従来型のセキュリティアプライアンスの導入



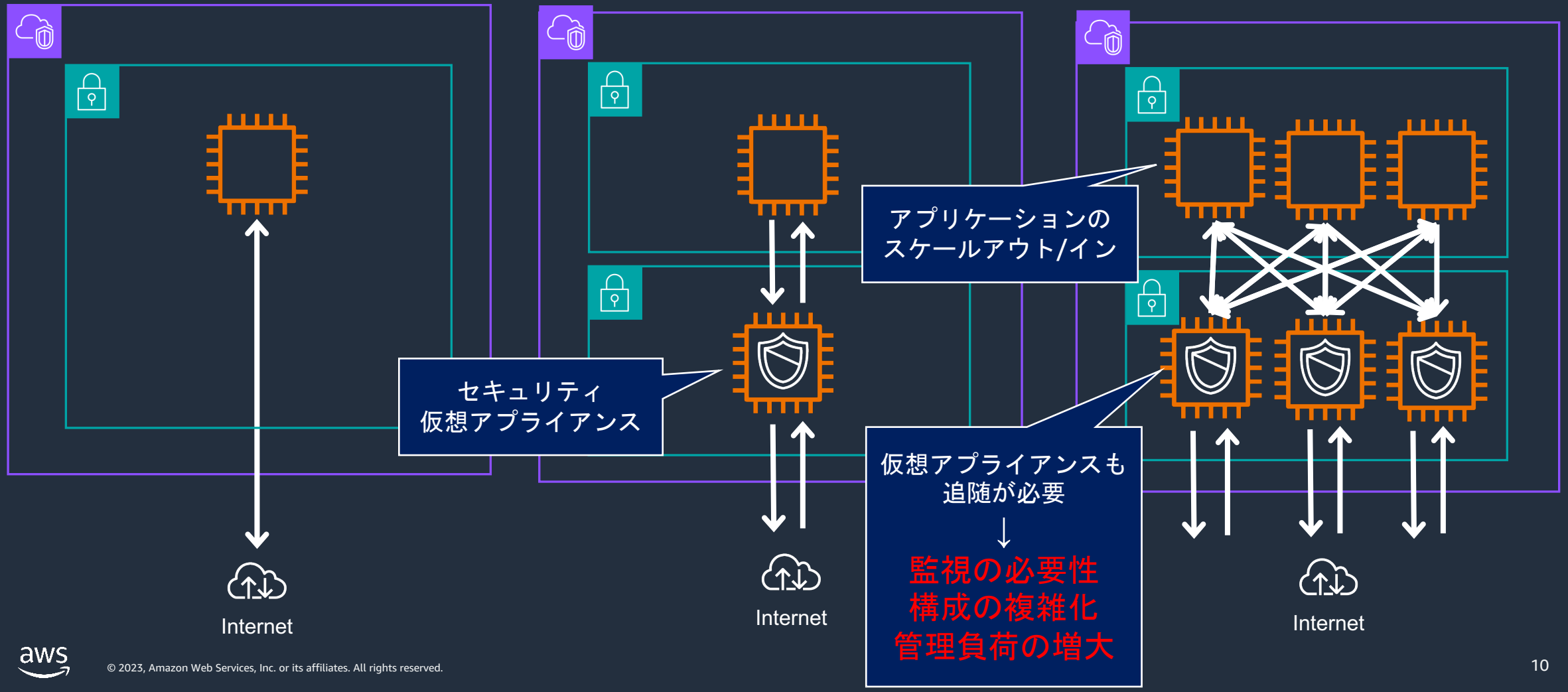
AWSでの従来型のセキュリティアプライアンスの導入



AWSでの従来型のセキュリティアプライアンスの導入



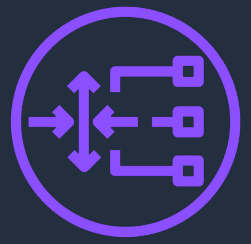
AWSでの従来型のセキュリティアプライアンスの導入



AWS Gateway Load Balancer 概要

AWS Gateway Load Balancer とは

- 仮想アプライアンスを迅速に導入可能
- 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

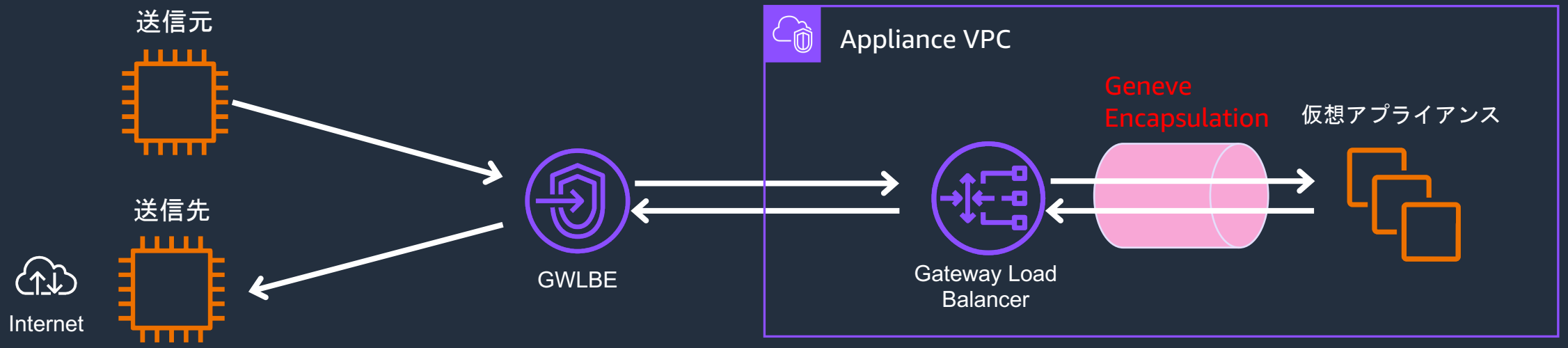


Gateway Load Balancer

3rdパーティーのセキュリティ仮想アプライアンスを容易に導入でき
高可用性とコスト最適化を実現するサービス

すでに利用している3rdパーティー製品のナレッジをそのまま活かしたい場合に有用

AWS Gateway Load Balancer（GWLB） コンポーネント



- Gateway Load Balancer Endpoint（GWLBE）
  - ルートテーブル内の Next Hop として指定可能なエンドポイント
- Geneve Encapsulation（Geneveプロトコルによるカプセル化）
  - 透過的に仮想アプライアンスにパケットを渡すことが可能

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

AWS Gateway Load Balancer 補足事項

- リスナーポートの概念はなく、IPパケットを受け取ると Geneve でカプセル化してターゲットにフォワードする
- Gateway Load Balancer Endpoint は他のアカウントに共有することが可能
  - 他のアカウントにおける通信の検査を共有元のアカウントで集約可能
- 利用する仮想アプライアンスにて Geneve プロトコルに対応している必要有り
- Firewall as a Service の形式も想定されており、GLWB + アプライアンスの VPC は事業者が管理し、エンドポイントをユーザーに提供し利用してもらう
  - エンドユーザーは Geneve やアプライアンスの運用を気にする必要がない

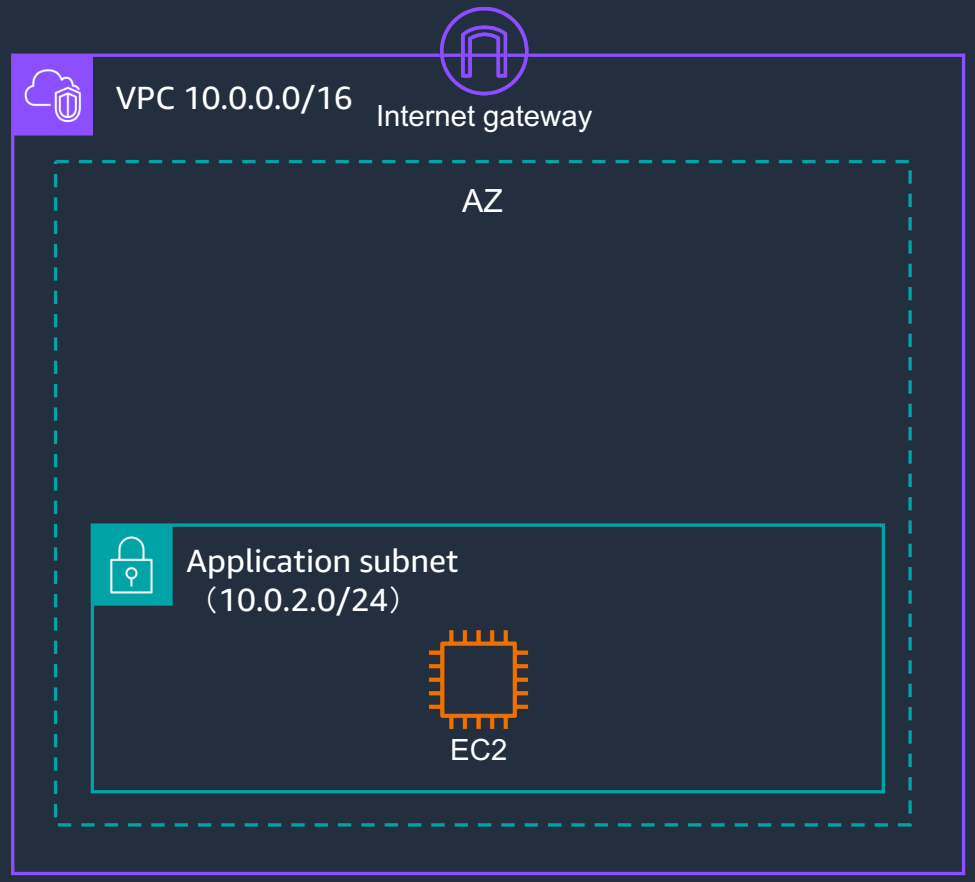
AWS Gateway Load Balancer パートナー様一覧

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

AWS Gateway Load Balancer ユースケースと設定

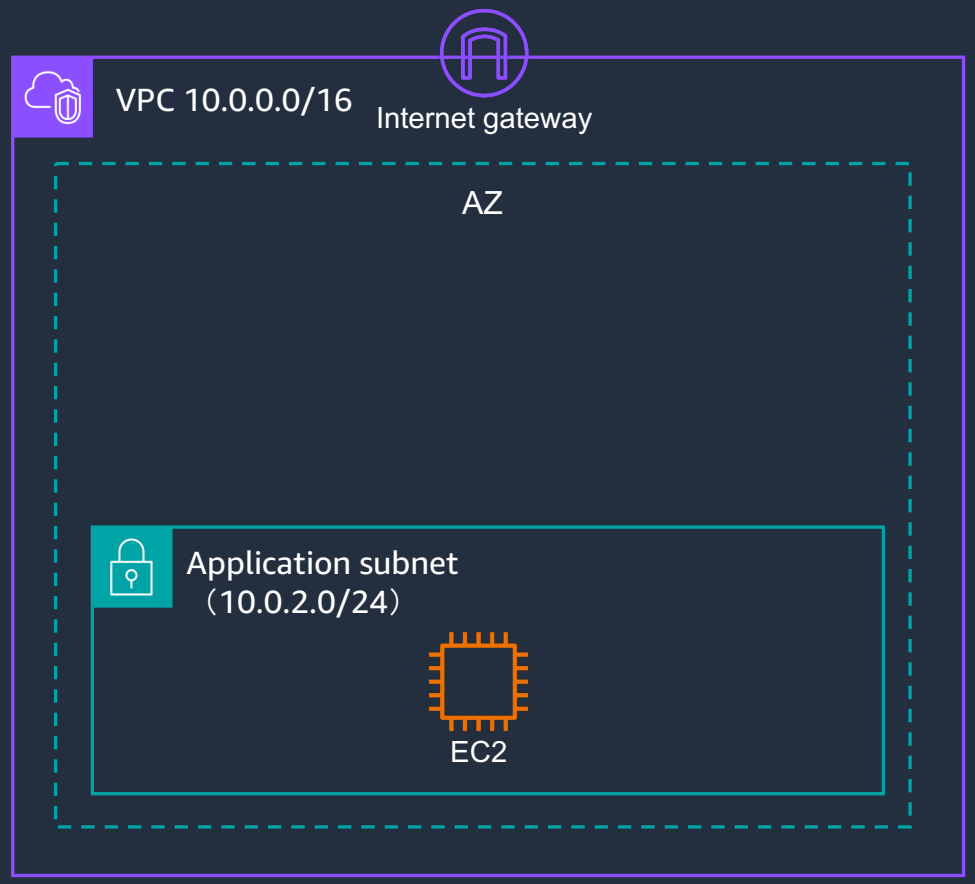
AWS Gateway Load Balancer ユースケースと設定①

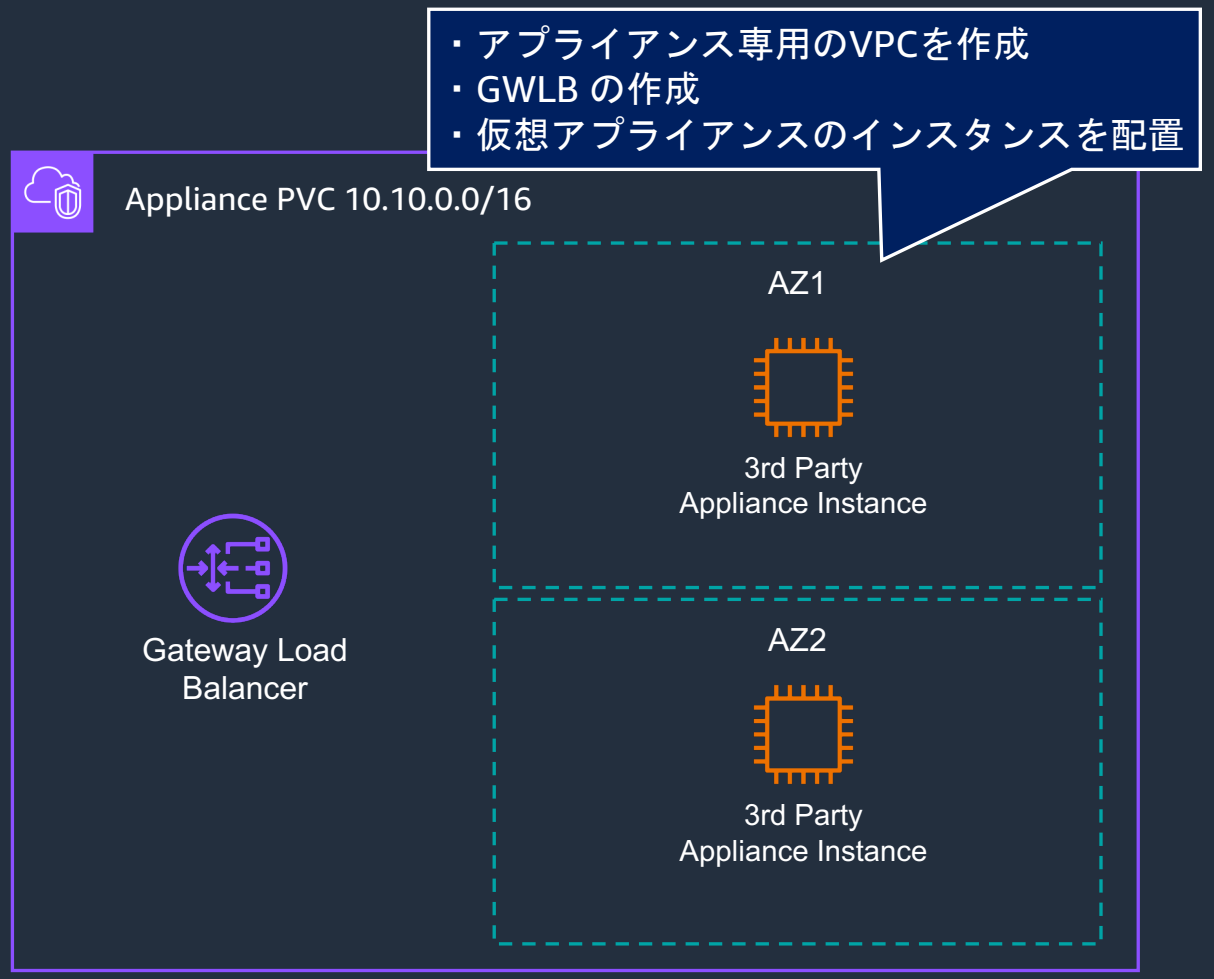
- AWS – Internet 間のトラフィック検査



AWS Gateway Load Balancer ユースケースと設定①

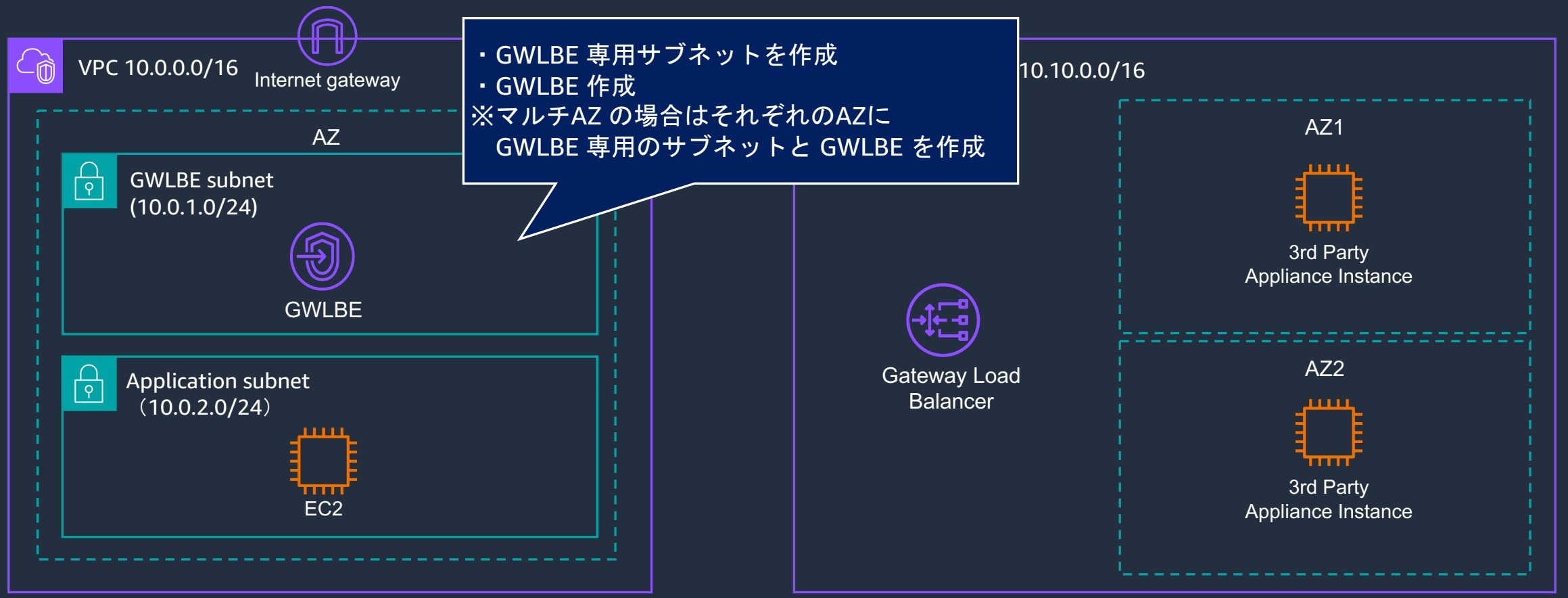
- AWS – Internet 間のトラフィック検査





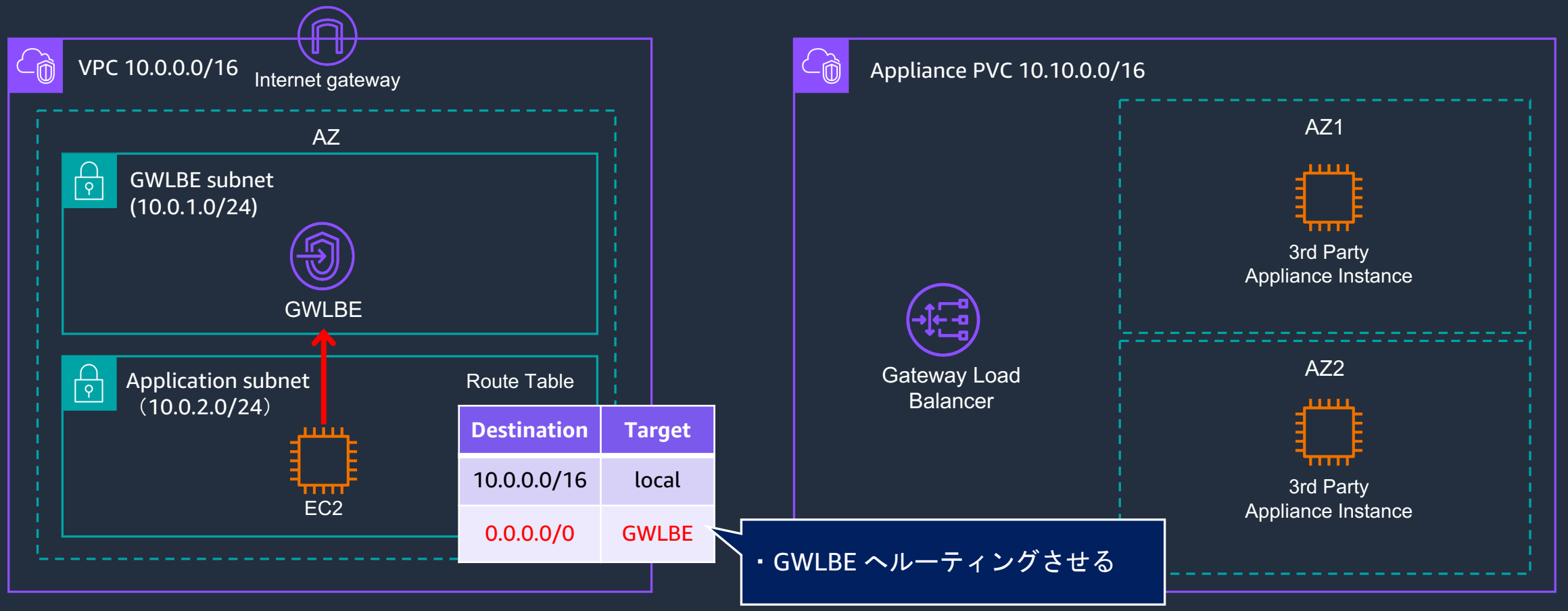
AWS Gateway Load Balancer ユースケースと設定①

- AWS – Internet 間のトラフィック検査



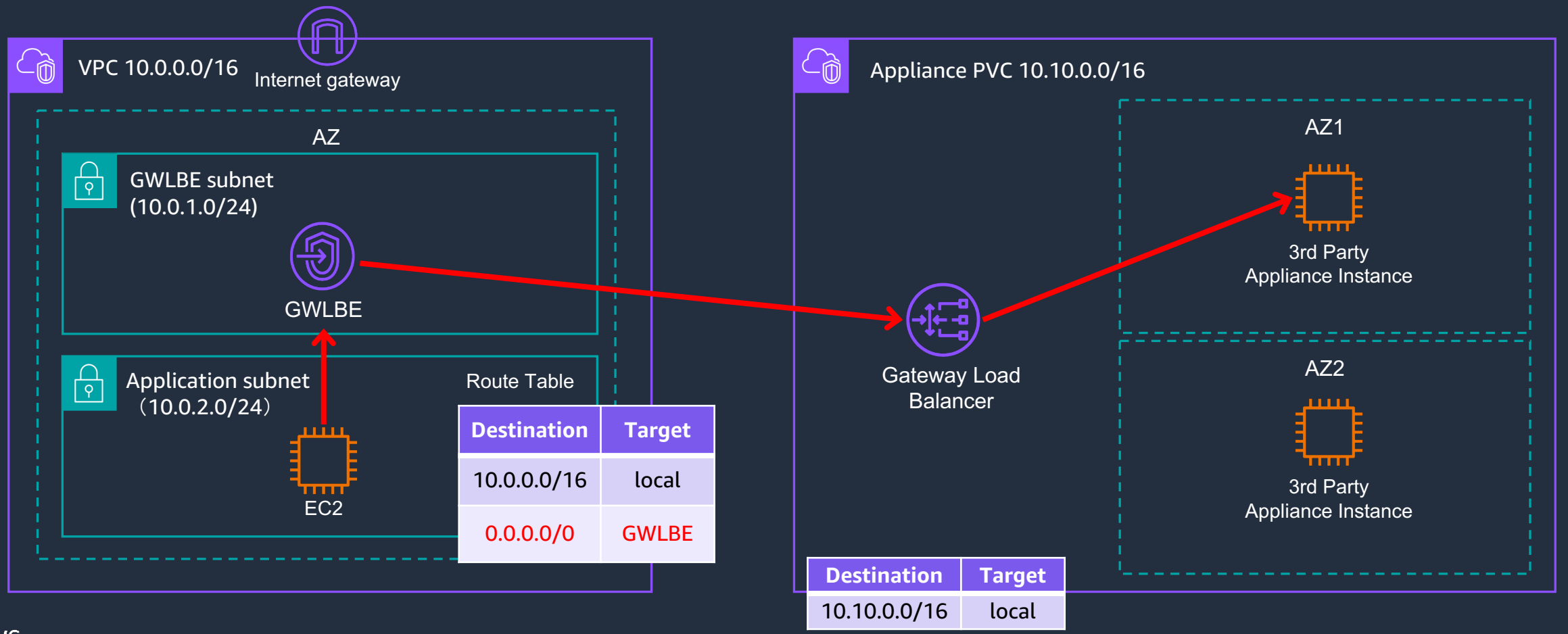
AWS Gateway Load Balancer ユースケースと設定①

- AWS – Internet 間のトラフィック検査 （行き）



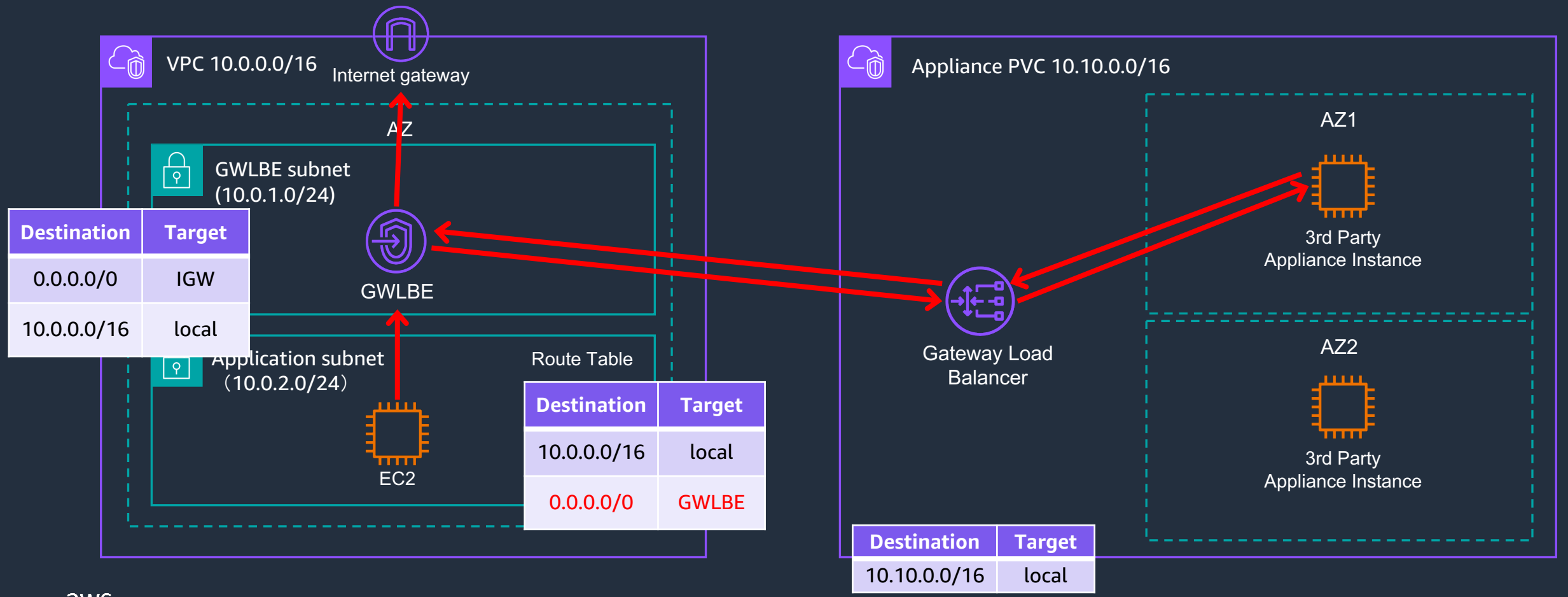
AWS Gateway Load Balancer ユースケースと設定①

- AWS – Internet 間のトラフィック検査 （行き）



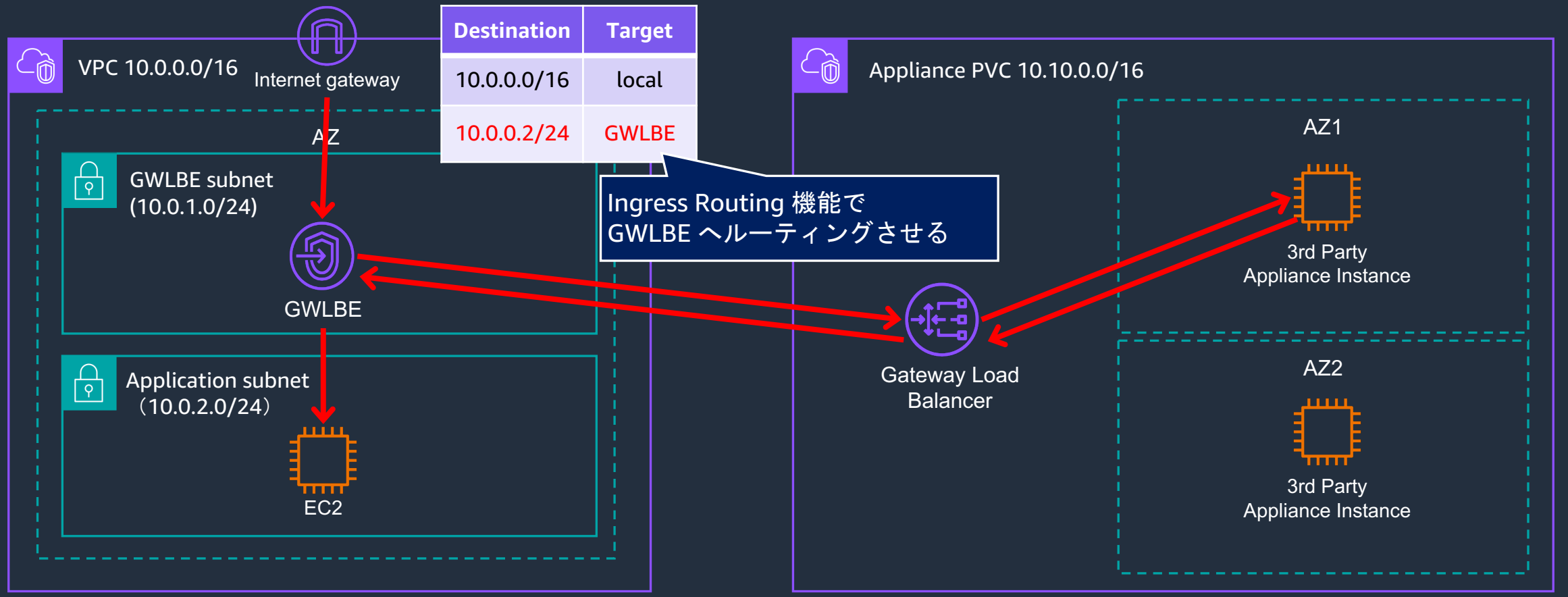
AWS Gateway Load Balancer ユースケースと設定①

- AWS – Internet 間のトラフィック検査（行き）



AWS Gateway Load Balancer ユースケースと設定①

- AWS – Internet 間のトラフィック検査（戻り）

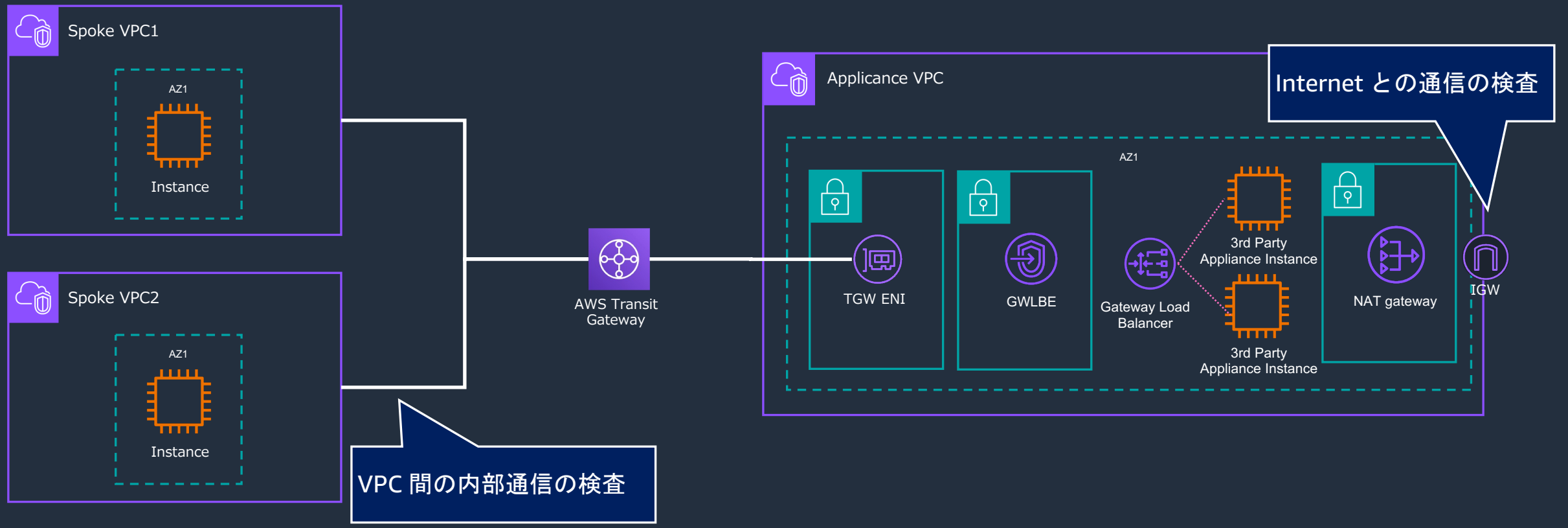


AWS Gateway Load Balancer ユースケースと設定①

- AWS – Internet間のトラフィック検査

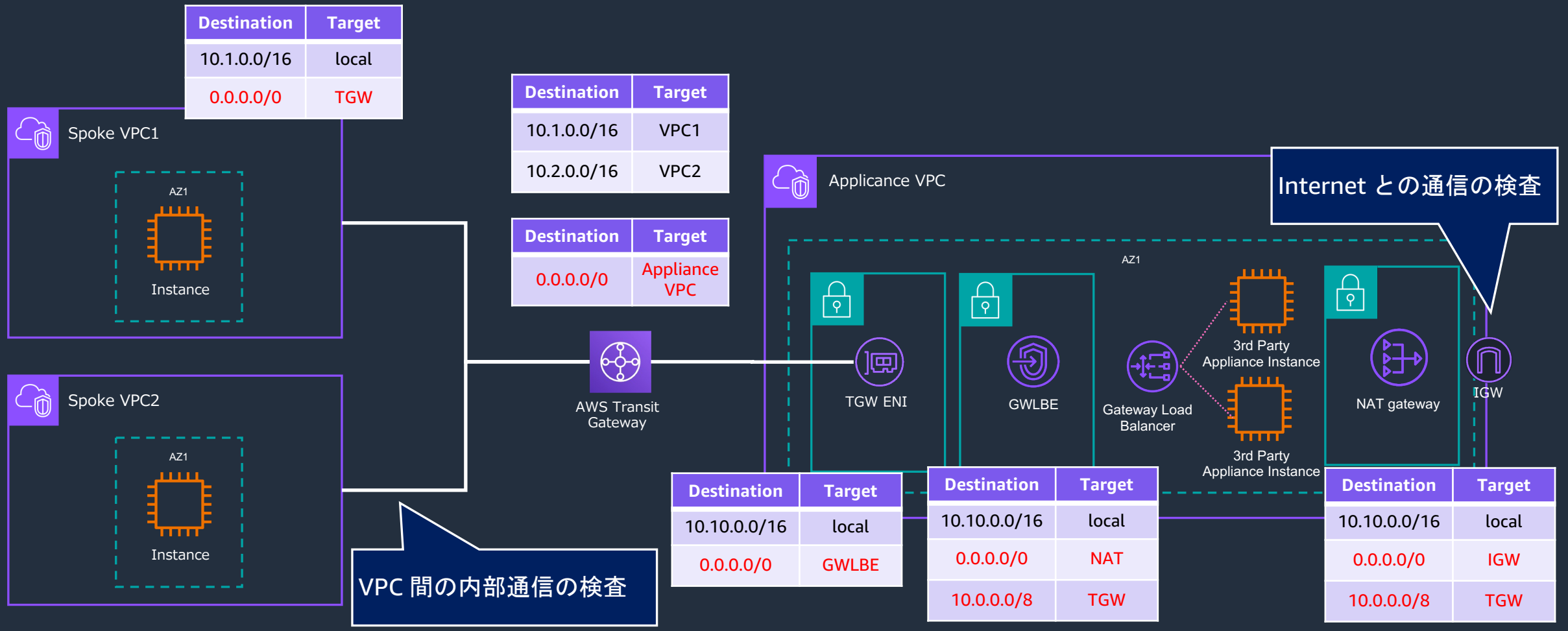
AWS Gateway Load Balancer ユースケースと設定②

- AWS Transit Gateway（TGW） を活用したトラフィック検査



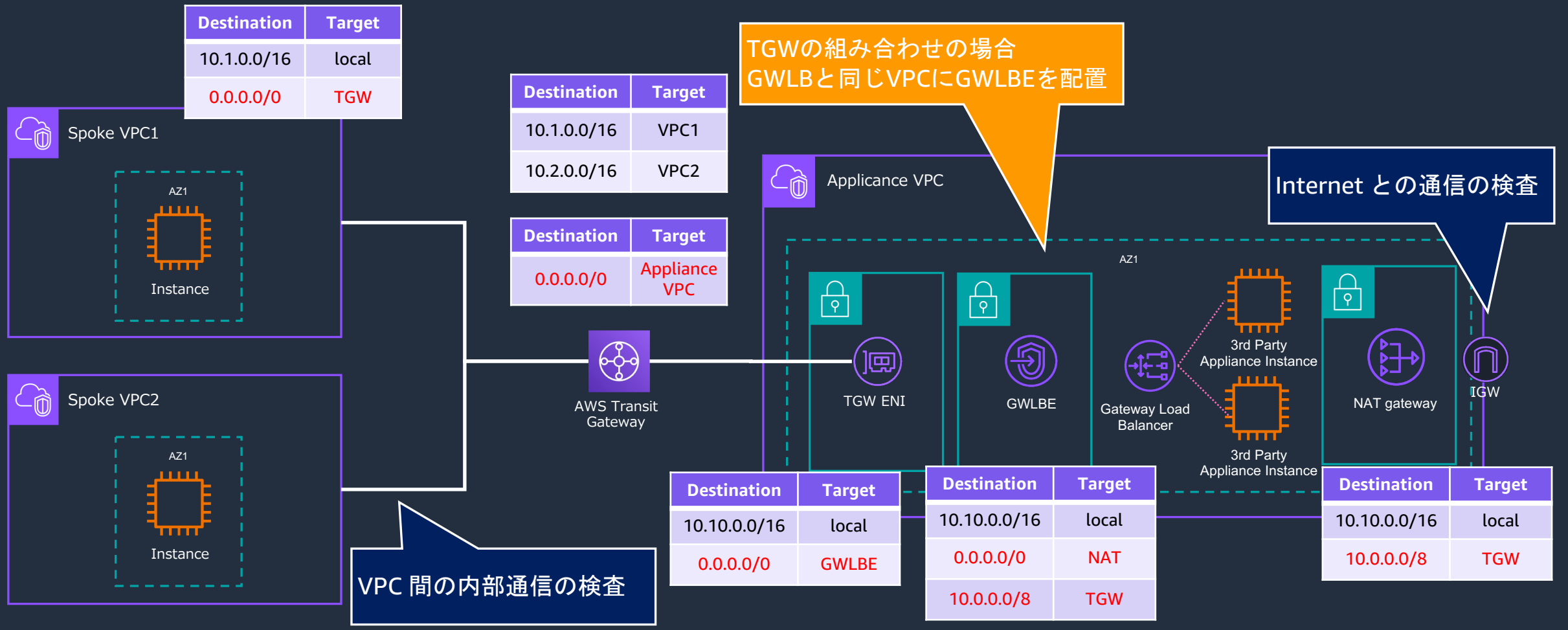
AWS Gateway Load Balancer ユースケースと設定②

- AWS Transit Gateway（TGW） を活用したトラフィック検査



AWS Gateway Load Balancer ユースケースと設定②

- AWS Transit Gateway（TGW） を活用したトラフィック検査



より詳細は Appendix のリンクをご参照ください

デモ

デモの内容

- 前提
  - ユースケース②のアーキテクチャで実施
  - 仮想アプライアンスとして、IDS/IPS のオープンソースである Suricataを 使用

外部（Internet）への通信のトラフィック検査
  - ルーティング設定の確認
  - 通信の確認

仮想アプライアンインスタンスのスケーリングの確認

まとめ

- AWS Gateway Load Balancer はセキュリティアプライアンス製品を AWS 上で利用する際に、可用性の高い構成にすることができます。
- AWS 上で利用するセキュリティアプライアンスでは、GENEVE プロトコルに対応している必要があるのでご留意ください。

セキュリティ仮想アプライアンス導入の際の選択肢の１つとして、ご検討ください。

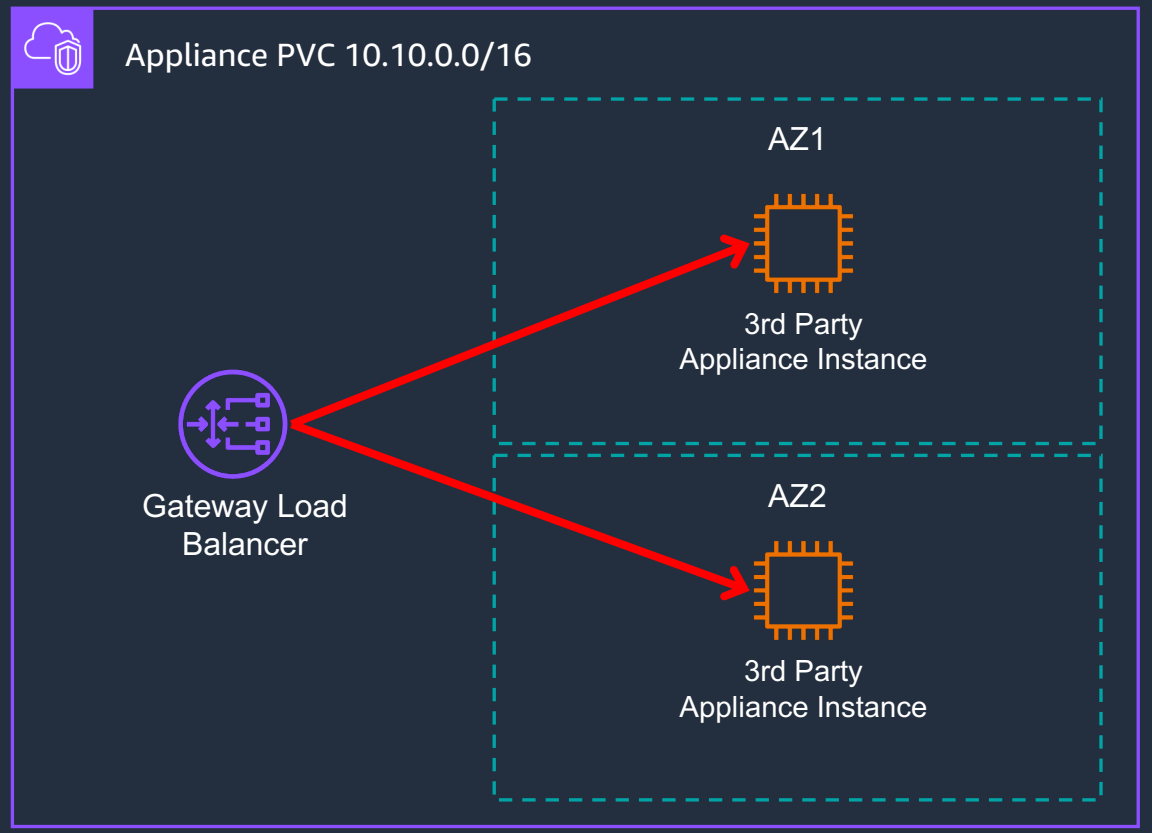
Thank you!

Appendix

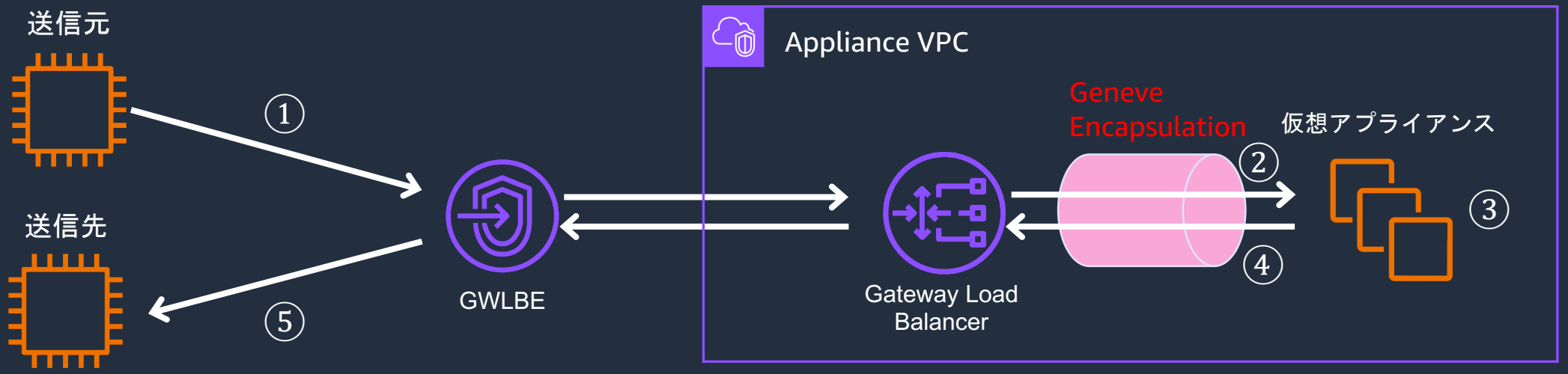
参考資料

- AWS Transit Gateway との組み合わせ
  - https://docs.aws.amazon.com/ja_jp/whitepapers/latest/building-scalable-secure-multi-vpc-network-infrastructure/using-gwlb-with-tg-for-cns.html
  - https://aws.amazon.com/jp/blogs/networking-and-content-delivery/centralized-inspection-architecture-with-aws-gateway-load-balancer-and-aws-transit-gateway/
  - https://d1.awsstatic.com/webinars/jp/pdf/services/20210331_AWS-Blackbelt_GatewayLoadBalancer.pdf
  - https://blog.serverworks.co.jp/aws-transit-gateway-appliance-mode
  - アプライアンスモード　（AZをまたぐ通信をするケースで有効化が必要）
    - https://docs.aws.amazon.com/ja_jp/vpc/latest/tgw/transit-gateway-appliance-scenario.html

クロスゾーン負荷分散



補足：Geneve Protocol



①/③/⑤
本来の検査したい通信

IPヘッダー（送信元IPドレス / 送信先IPアドレス）	（パケットの中身）

②/③
カプセル化された通信

Outer IPヘッダー（送信元IPアドレス / 送信先IPアドレス）	Geneve ヘッダー	Geneve Options（GWLBE ID, VPC ID）	IPヘッダー（送信元IPドレス / 送信先IPアドレス）	（パケットの中身）

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

補足：Suricata について

- suricata.rules ファイルに検知するトラフィックを記載

```
[アクション] [プロトコル] [送信元IP] [送信元port] - > [送信先 IP] [送信先 port] [ルールオプション]
```

```
drop tcp any any -> any 443 (msg: ¥"amazon rule¥"; tls.sni; content:¥"amazon.com¥";
nocase; pcre:¥"/amazon.com$/¥"; sid:11; priority: 1; rev:1;)
```

アクション例

alert	アラートを出す
pass	パケットの検査を中止し、通信を許可
drop	パケットをドロップしてアラート

https://docs.suricata.io/en/suricata-5.0.2/rules/intro.html