Cisco SD-WANとAWS Cloud接続（新機能紹介）

林文傑　Cisco、Technical Solutions Architect

藤井拓　AWS、Solutions Architect, Network Specialist

中根和久　AWS、Sr. Business Development Manager, Compute - Networking

2021年5月

スピーカーの紹介

林　文傑
Technical Solution Architect

cisco

藤井　拓
Solutions Architect,
Network Specialist

aws

中根 和久
Sr. Business Development Manager,
Compute - Networking

aws

本日のアジェンダ

SD-WANファブリックのAWSへの接続・延伸（接続方式）

- ✓Site to Cloud
- ✓Site to Site（AWSバックボーン活用）

補足：AWS TGWベースの
ブランチコネクトソリューション

まとめと重要なポイント

Cisco SD-WANファブリックの AWSへの接続・延伸

AWSでCisco SD-WANを使用する理由?

ソフトウェア定義ネットワーキングの利点とAWSのスピードとスケールを組み合わせる

さらなる自動化

ブランチオフィスの場所と
AWSの間の接続を自動化

管理の容易さ

トラフィックデータ・テレメトリによ
る地域間ネットワークの可視性
を確立

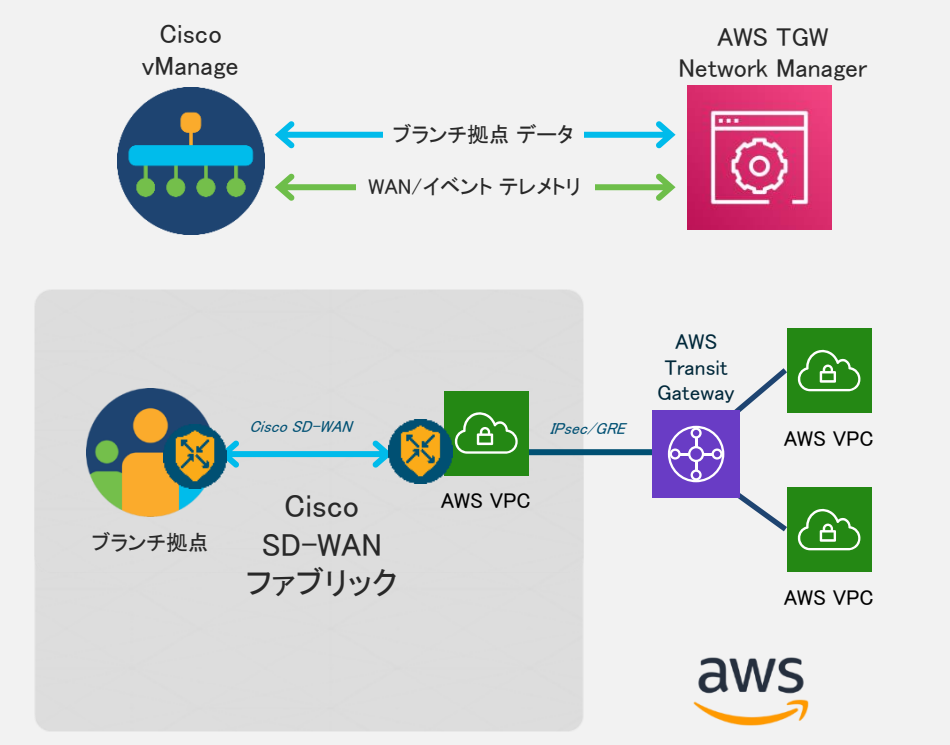
セキュリティの強化

AWS上のCisco SD-WANには、細
分化されたセグメント化と合理化さ
れたポリシー適用の活用を含むセ
キュリティのベストプラクティスが組
み込まれている

TCOの削減

細分化されたセグメント化とポリシ
ー適用により、コンプライアンス・プ
ロセスの自動化を支援

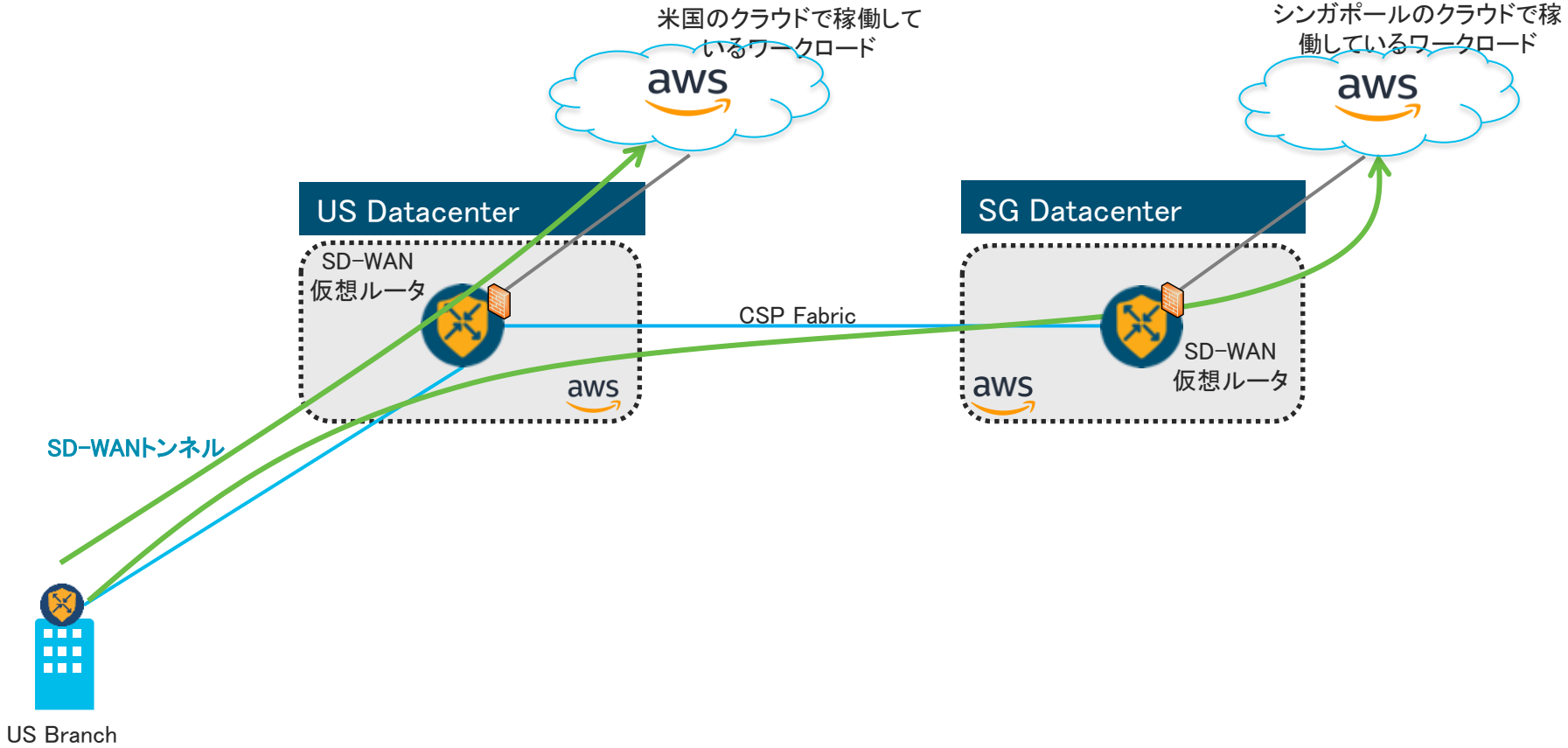
SD-WANファブリックをクラウドに延伸する必要性とは？



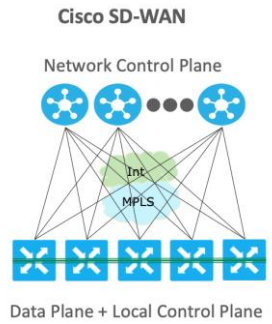
メリット

- ブランチ拠点からクラウドまで一貫性のあるポリシー・セグメンテーションによる企業クラスセキュリティの実現
- 一元制御用トランジットVPCやTGWを含め、Site to Cloud（拠点からクラウドへの接続）とAWSオンバックボーンを活用したSite to Site（拠点間接続）の構成をCisco SD-WANで自動的にプロビジョニングし、一元管理・制御
- TGW Network Managerとの連携で地域間のトラフィックとテレメトリによるネットワーク可視化を提供

SD-WANをAWSに延伸
Site to Cloud（拠点からクラウドへの接続）



SD-WANをAWSに延伸
Site to Site（拠点間接続）



US Datacenter

SG Datacenter

SD-WAN vRouter

SD-WANトンネル color: private1

aws

AWSバックボーン

SD-WANトンネル color: private1

SD-WAN vRouter

aws

SD-WANトンネル color: public-internet

SD-WANトンネル color: public-internet

US Branch

SG Branch

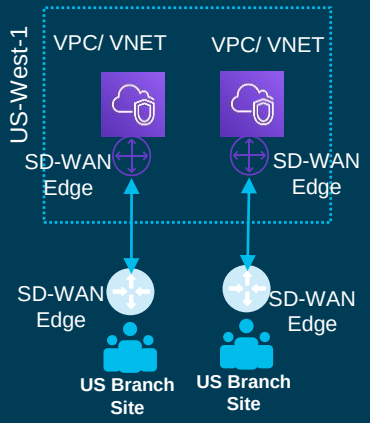
SD-WANトンネル

Control Connection

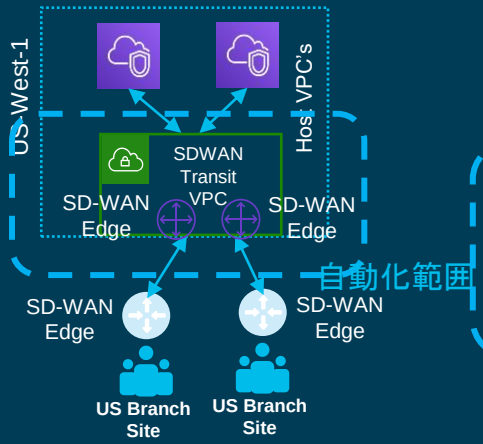
Site to Cloud

Site to Cloud: 接続方式比較

接続方式1
ホストVPC直結

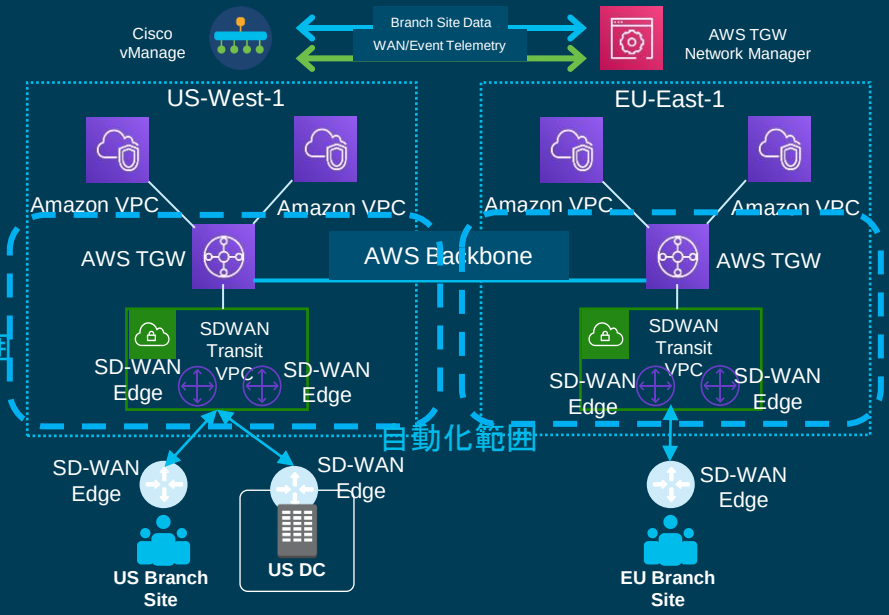


接続方式2
Transit VPC経由



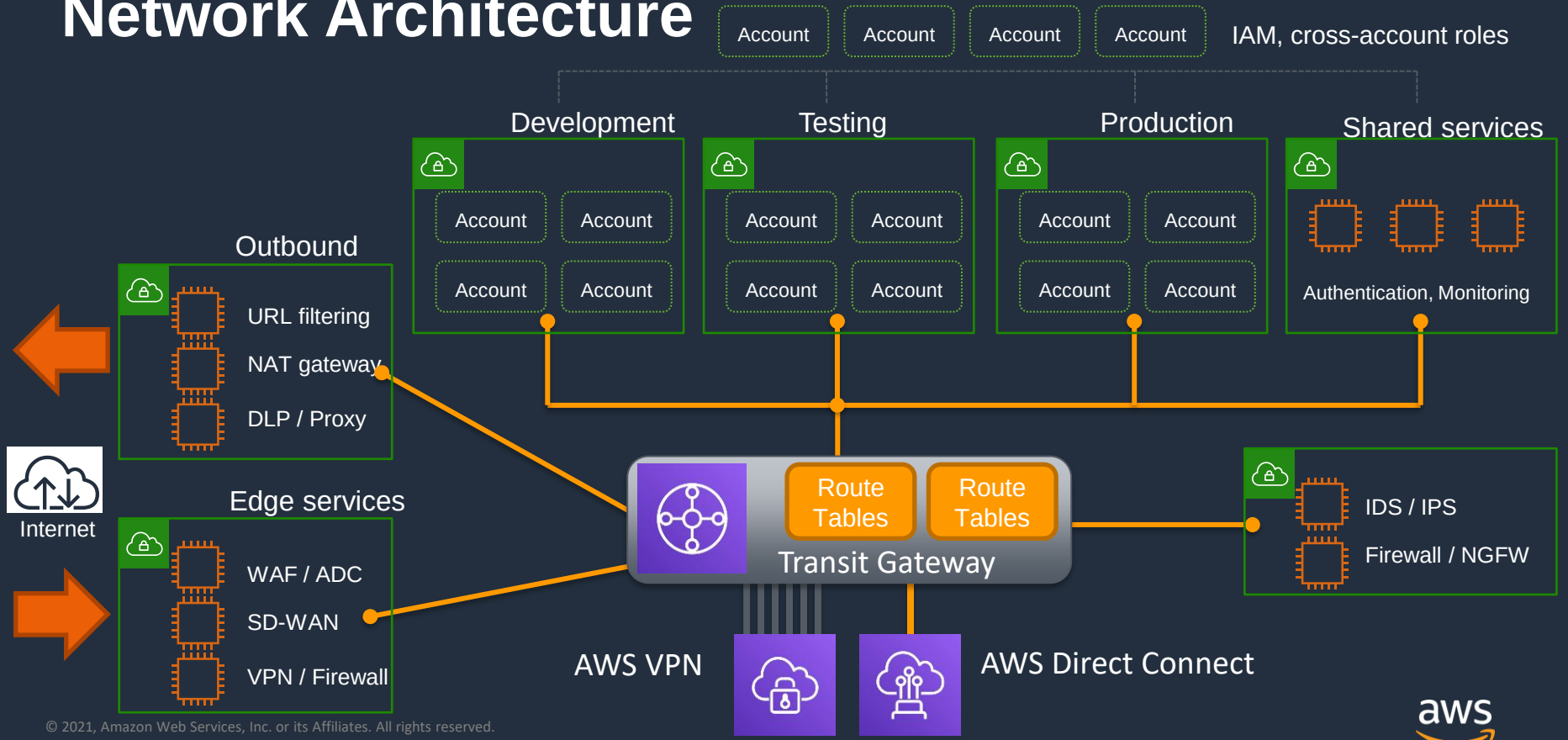
Cloud onRamp for IaaSで
自動化可能

接続方式3
TGW経由



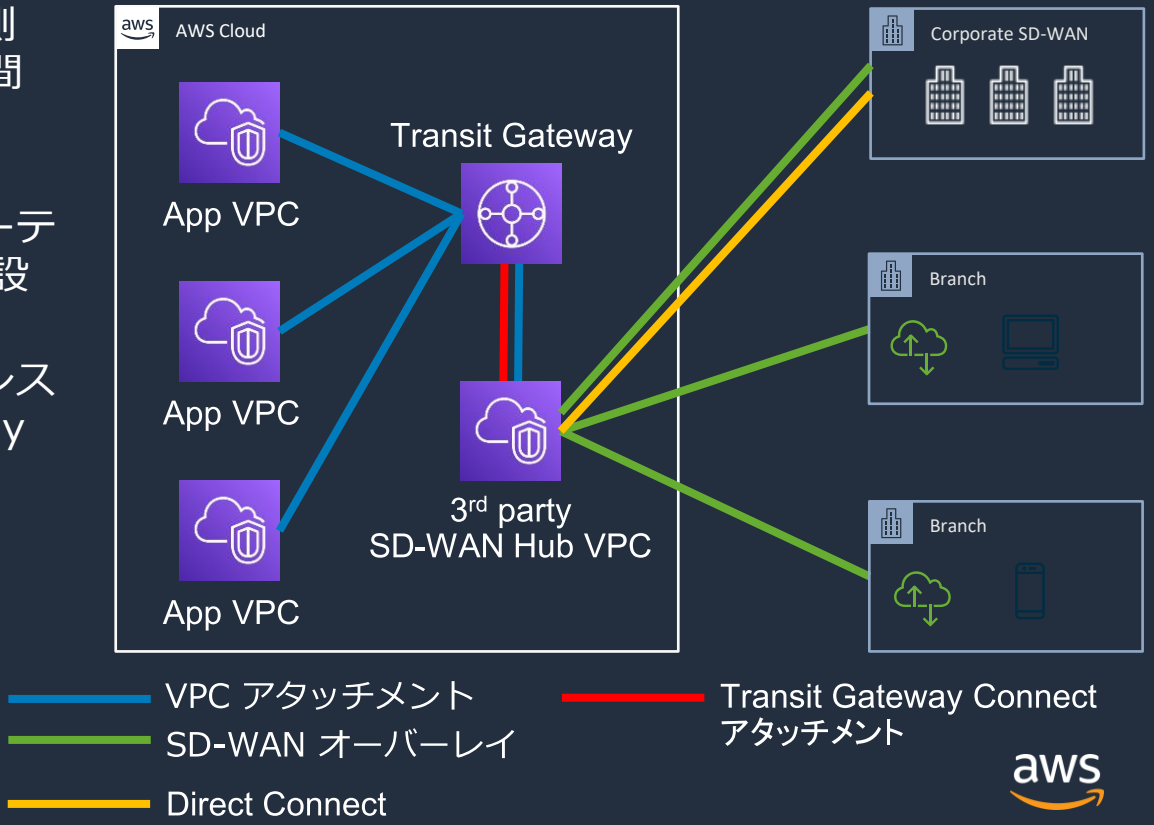
Cloud onRamp for MultiCloudで
自動化可能

AWS Reference Network Architecture



Transit Gateway Connect（SD-WAN サポート）

- 従来必要だったSD-WANハブ側VPCとAWS Transit Gateway間のサイト間VPNが不要に
- SD-WANとAWS Transit Gateway間はダイナミックルーティング (BGP) でルーティング設定を簡単に
- オンプレSD-WANアプライアンスを簡単にAWS Transit Gatewayに組み込み
- 従来の設計モデルに比べ拡張性やスループットの向上

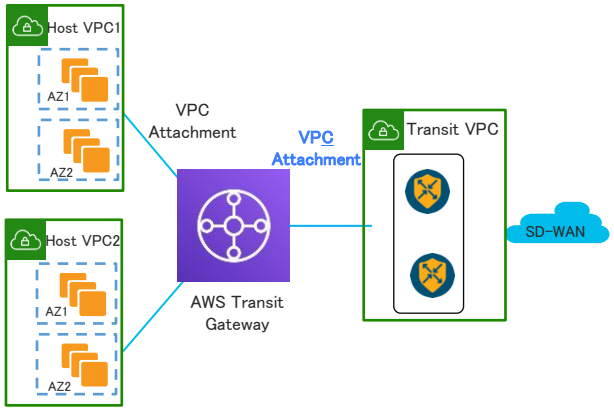


AWS Transit Gatewayのクォータ

制限	デフォルト
AWS Transit Gateway アタッチメントの数	5000
VPN 接続ごとの最大帯域幅*	1.25Gbps
VPC 接続ごとの最大帯域幅 (バースト)	50Gbps
アカウントあたりの AWS Transit Gateway の数	5
VPC あたりの AWS Transit Gateway アタッチメントの数	5
ルートの数	10,000

接続方式3（TGW経由）DeepDive的な比較

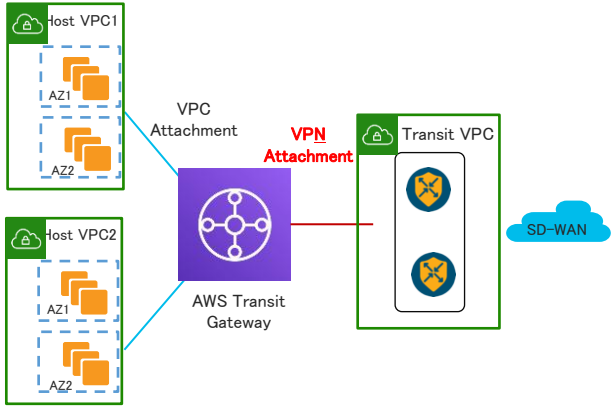
VPC AttachmentでSD-WAN接続



- SD-WANとTGW間のダイナミックルーティングができない
- Transit VPCのSD-WAN仮想ルータはTGWをホストVPCルートのnext-hopとする
- TGWのスループット上限の50Gbpsまでスケール可能
- 自動化機能なし

自動化はv17.3～

VPN AttachmentでSD-WAN接続

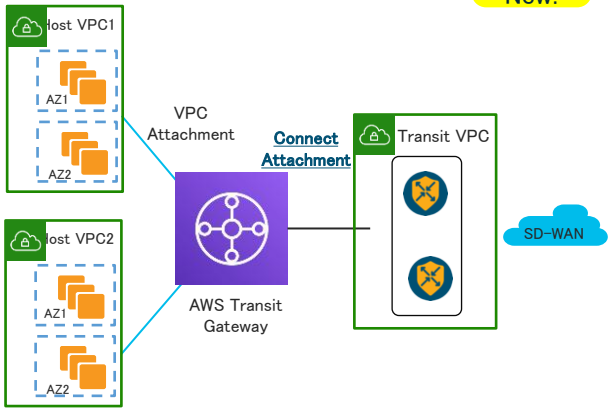


- Transit VPCのSD-WAN仮想ルータはBGP over IPSecでTGWと接続する
- リージョン間接続構成を含めて、Cloud onRamp for Multicloud機能で自動化可能(v17.3～)
- スループットはTGWとのIPSecトンネルごとに1.25Gbps
- 自動スケールアウト非対応

自動化はv17.5～

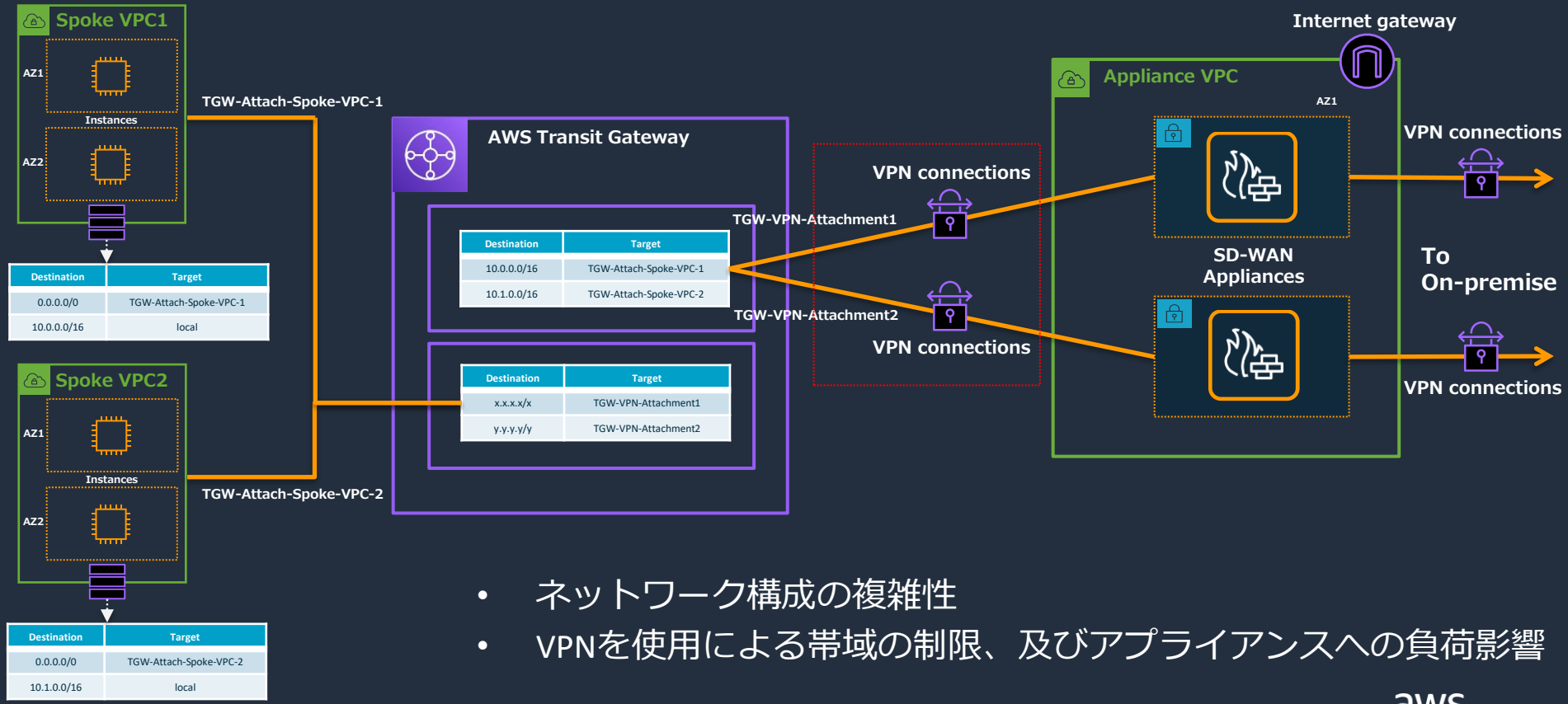
Connect AttachmentでSD-WAN接続

New!



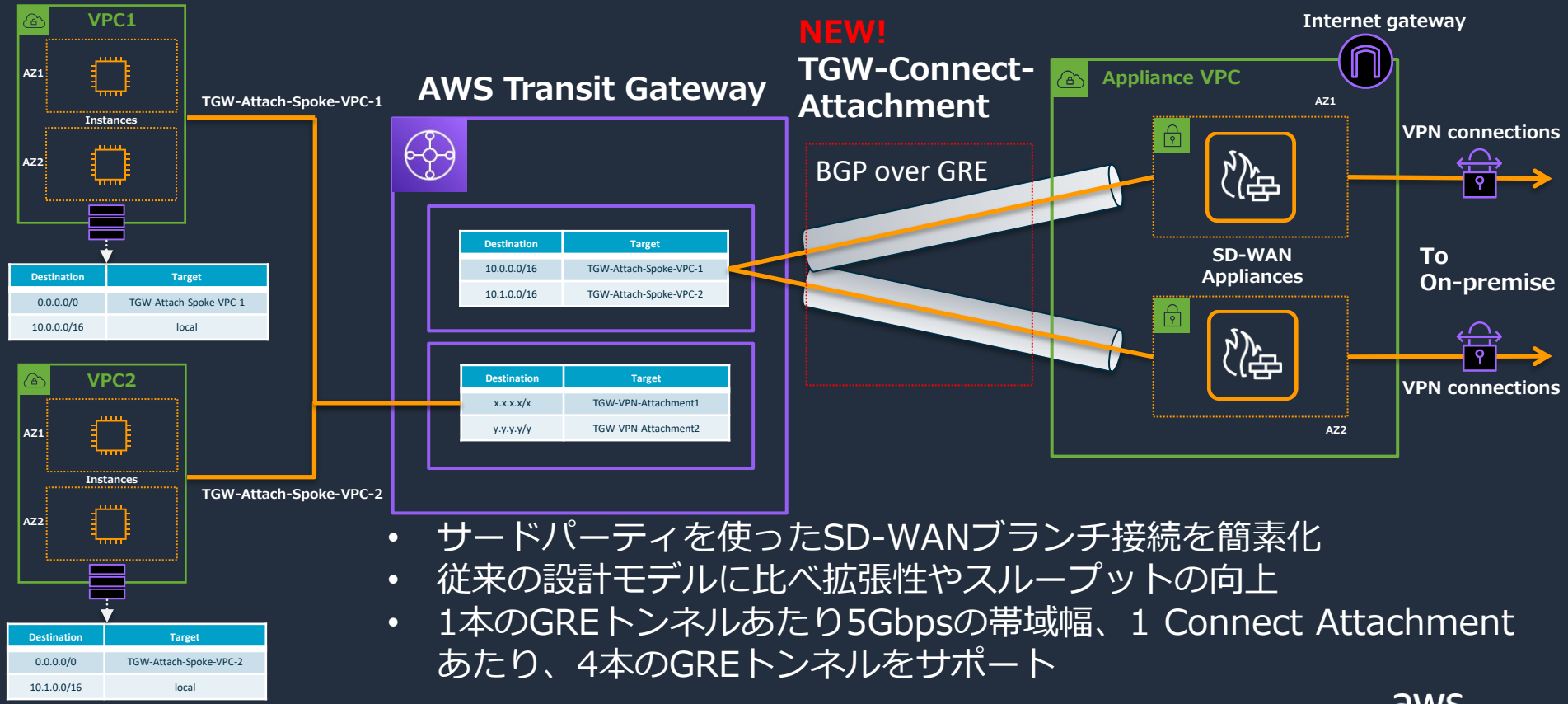
- Transit VPCのSD-WAN仮想ルータはBGP over GREでTGWと接続する（プライベートIP使用可能）
- Cloud onRamp for Multicloud機能で自動化可能(v17.5～)
- スループットはTGWとのGREトンネルごとに5Gbps
- 自動スケールアウト非対応

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

AWS Transit Gateway Connect



- サードパーティを使ったSD-WANブランチ接続を簡素化
- 従来の設計モデルに比べ拡張性やスループットの向上
- 1本のGREトンネルあたり5Gbpsの帯域幅、1 Connect Attachmentあたり、4本のGREトンネルをサポート

https://aws.amazon.com/jp/about-aws/whats-new/2020/12/introducing-aws-transit-gateway-connect-to-simplify-sd-wan-branch-connectivity/

TGW Connect AttachmentでSD-WAN接続

New!

課題

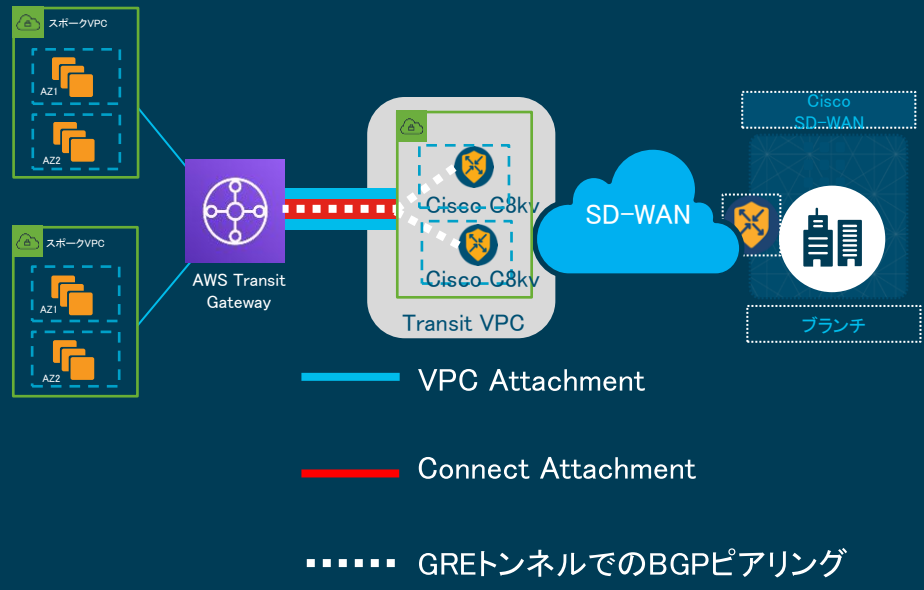
AWS TGWの VPN attachmentのスループット制限は1.25 Gbps。
(クラウドのボトルネックになることが多い)
水平展開方式でスケールアウトする回避策があるが、
複数のIPSecトンネルを管理および自動化するのは困難。
IPSecエンドポイントのパブリックIPアドレスは、特定のお客様にとって大きなセキュリティ上の問題となる場合がある

ソリューション

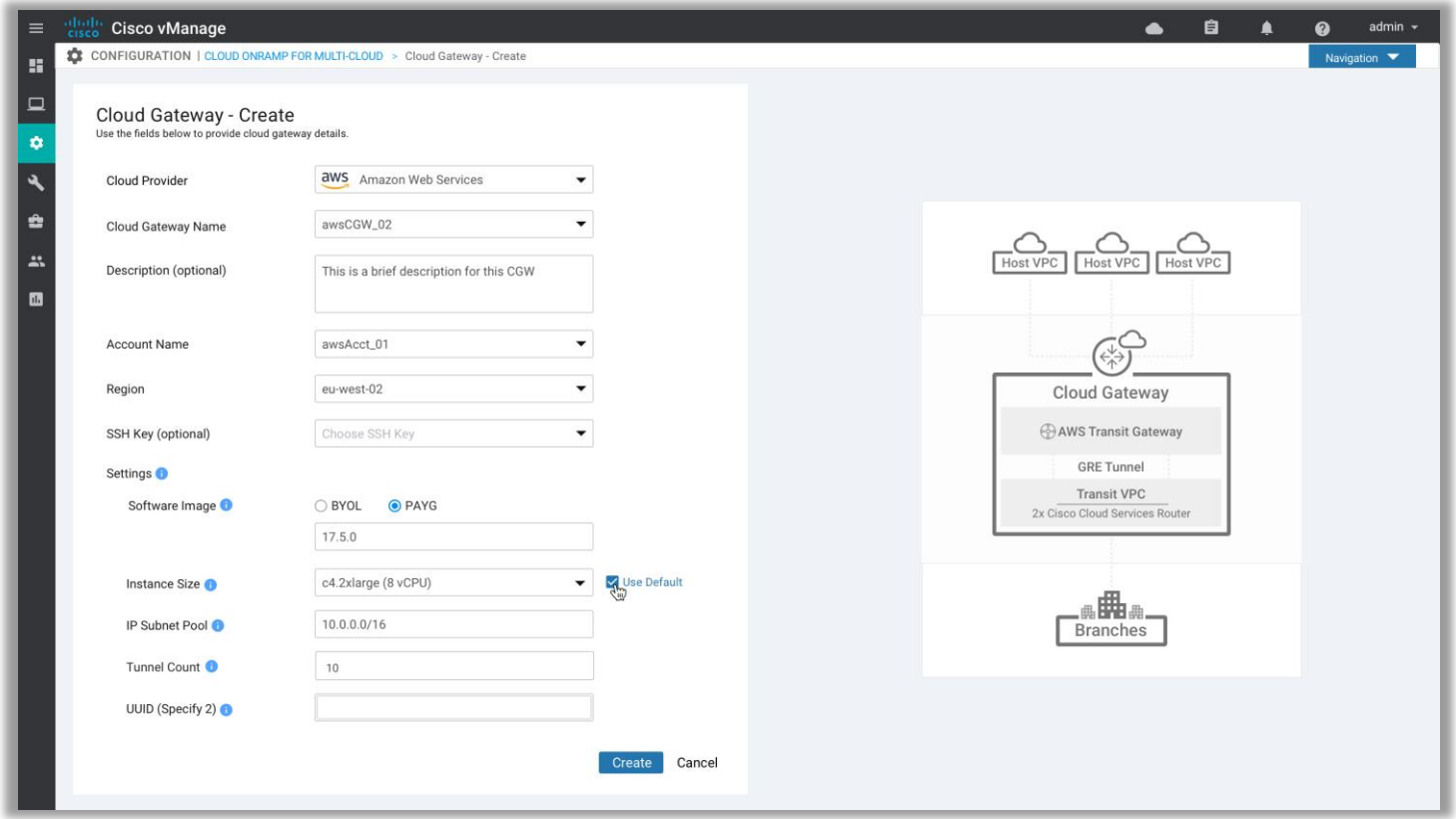
17.5からは、IPSecの代わりにTGW Connect AttachmentのGREトンネルを使用した自動化されたCloud onRampソリューションをサポートする。
これにより、GREの単一トンネルあたりのスループットが最大5Gbpsまで大幅に向上し、プライベートIPも使用できる。

警告/前提条件

C8KVはサポートされている唯一の仮想ルータであり、
vEdge CloudとCSR1KVはサポートされていない

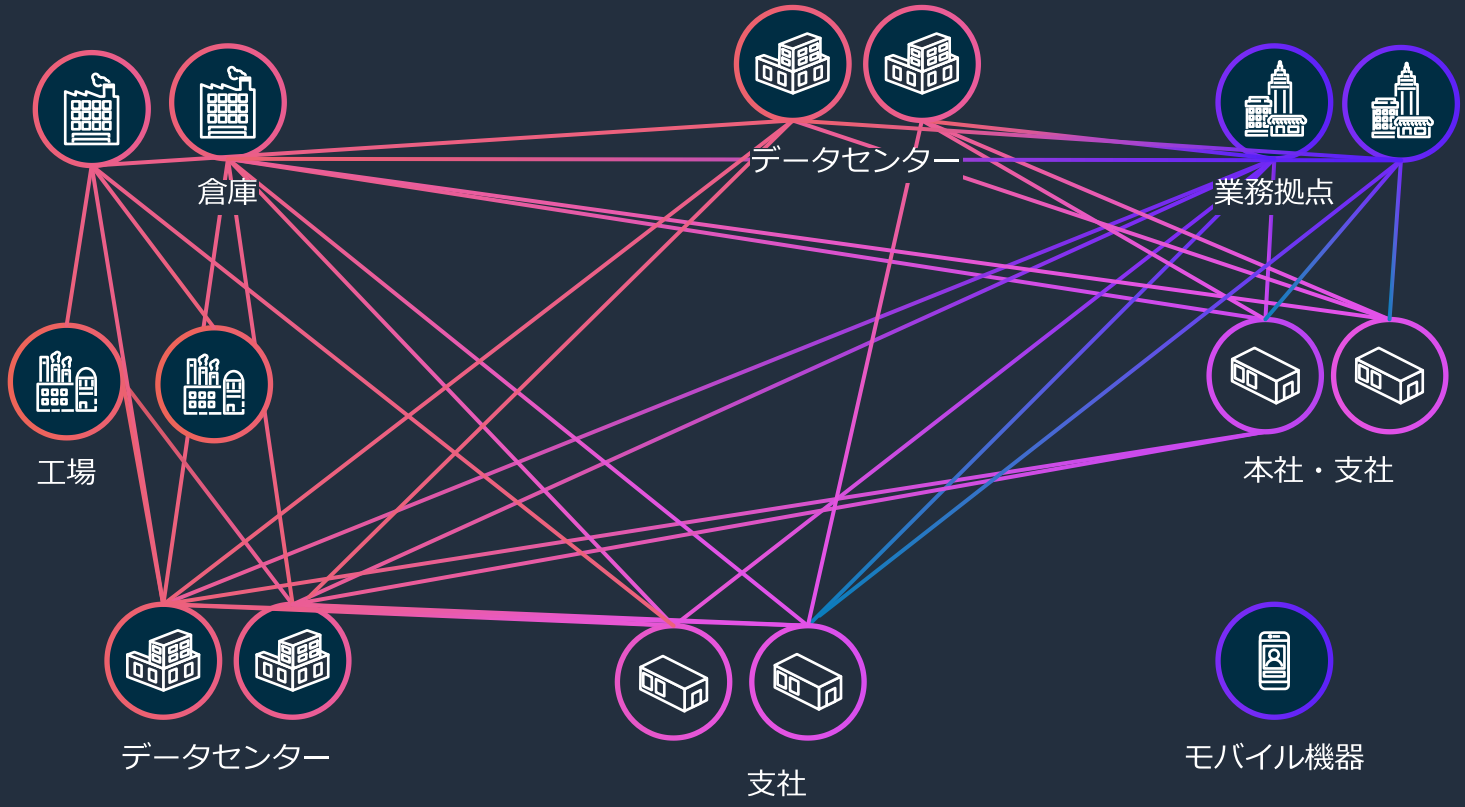


vManageでのAWS TGW Connect Attachment設定画面

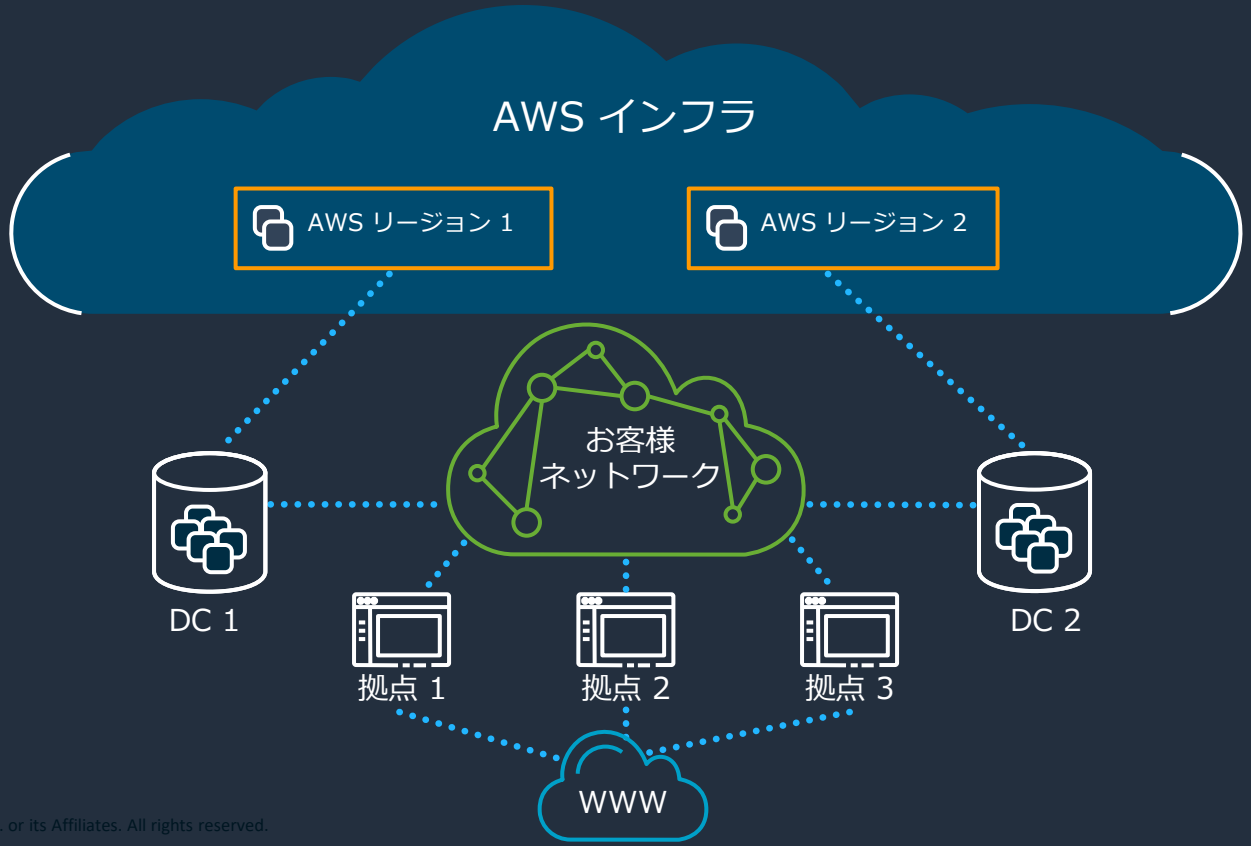


Site to Site
（AWSバックボーン活用）

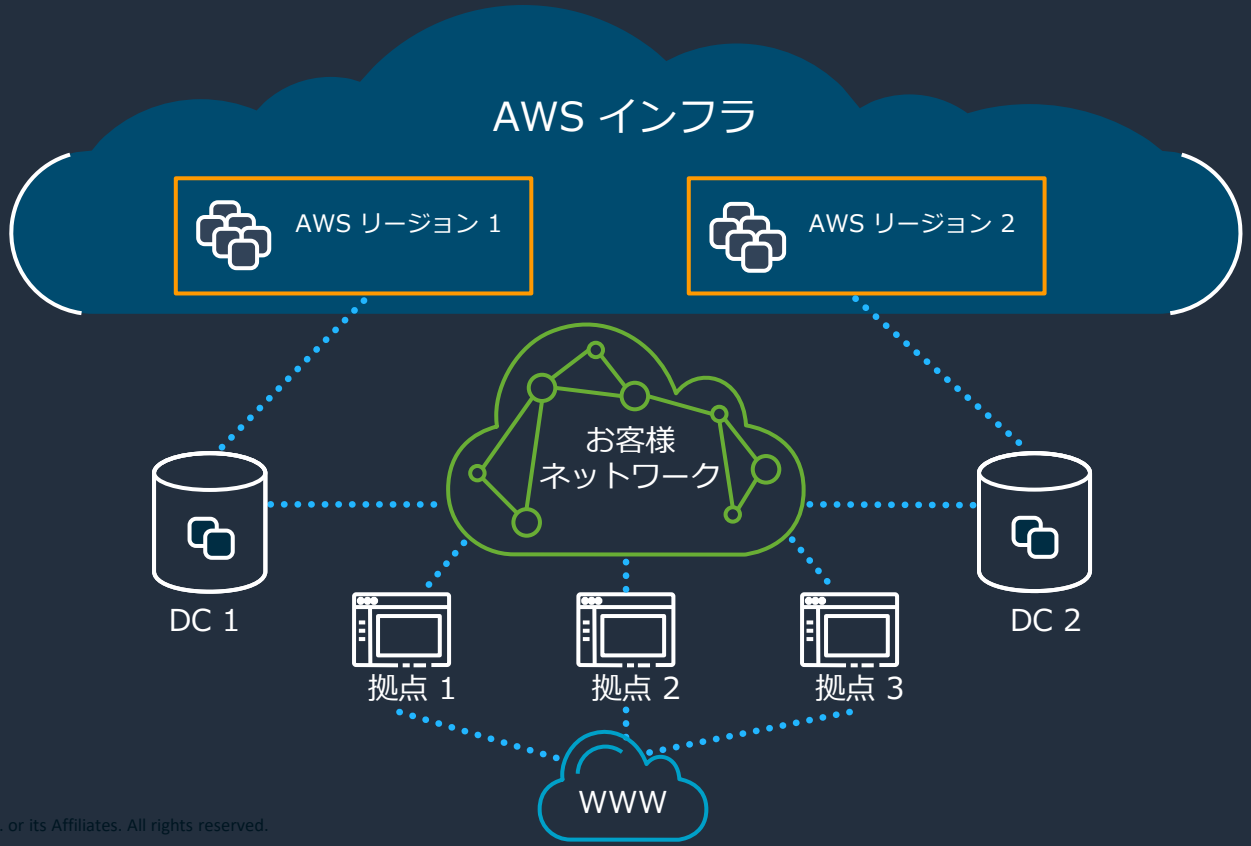
今日のお客様の通信環境の複雑化



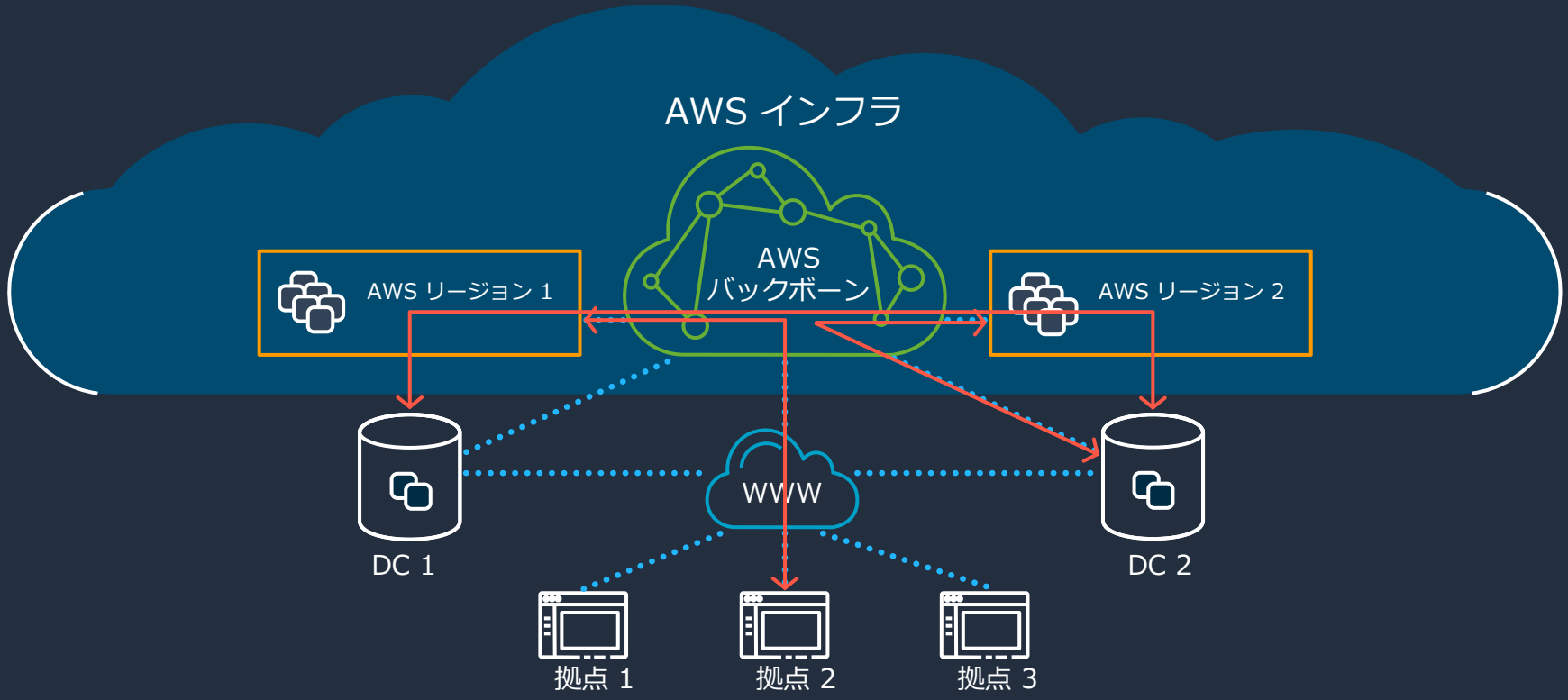
ワークロードのクラウド移行に伴いAWS がネットワークハブに進化



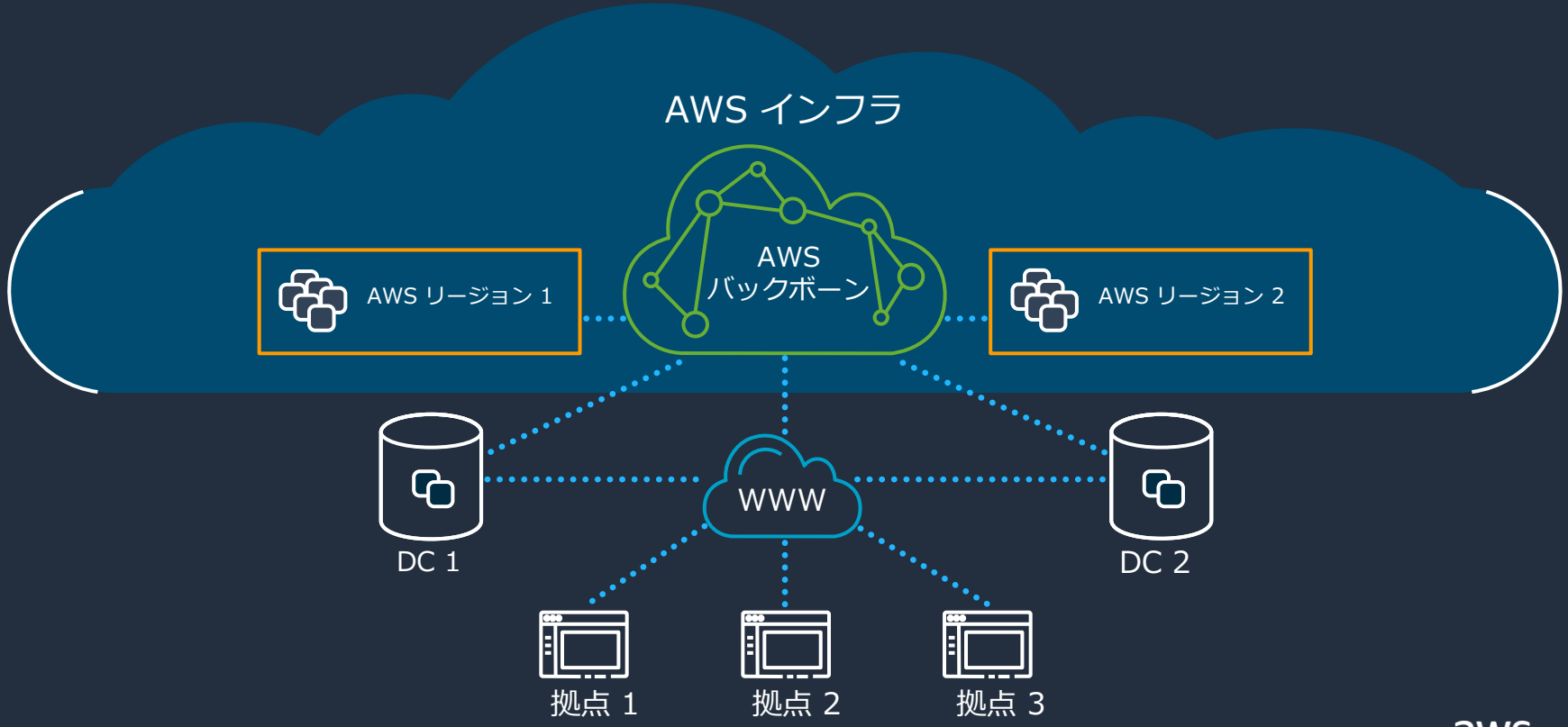
ワークロードのクラウド移行に伴いAWS がネットワークハブに進化



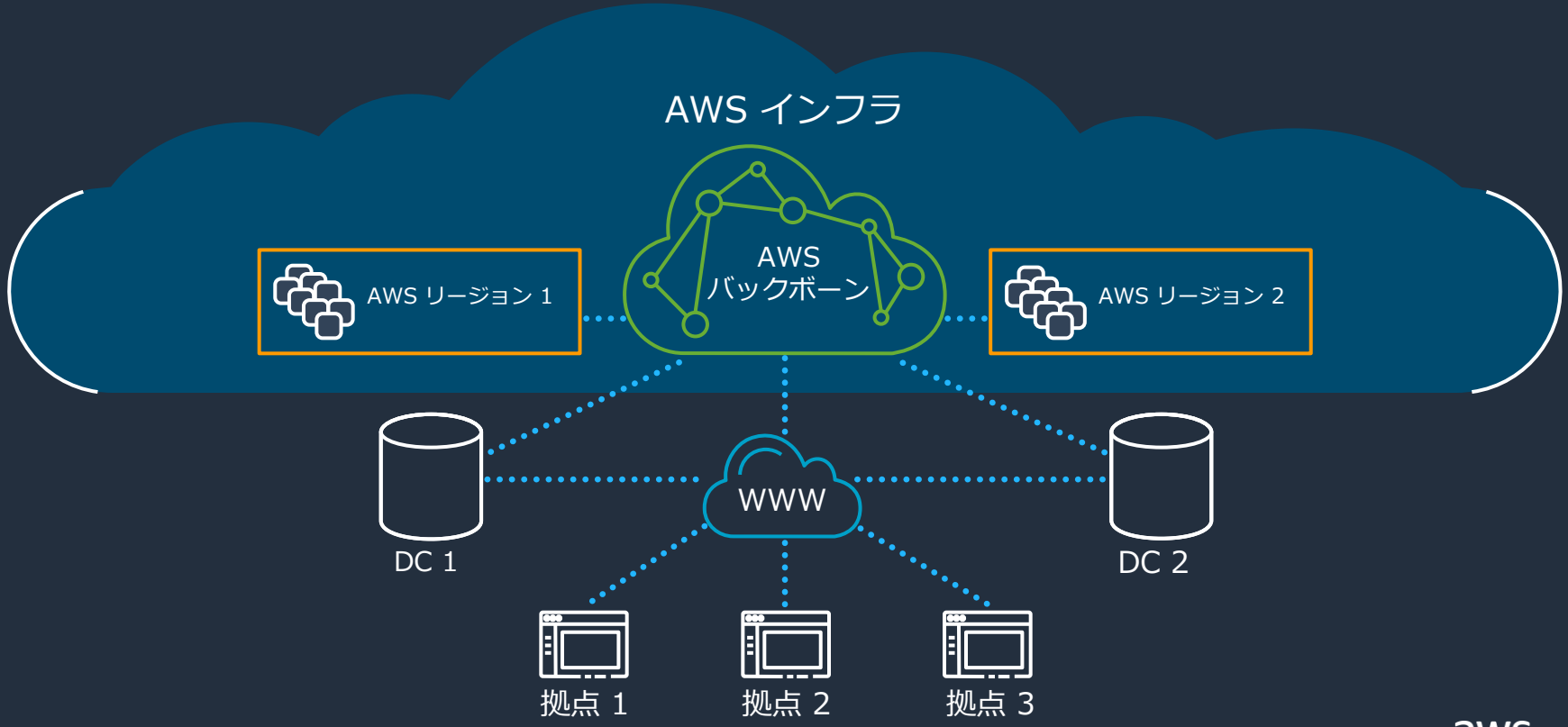
ワークロードのクラウド移行に伴いAWS がネットワークハブに進化



ワークロードのクラウド移行に伴いAWS がネットワークハブに進化



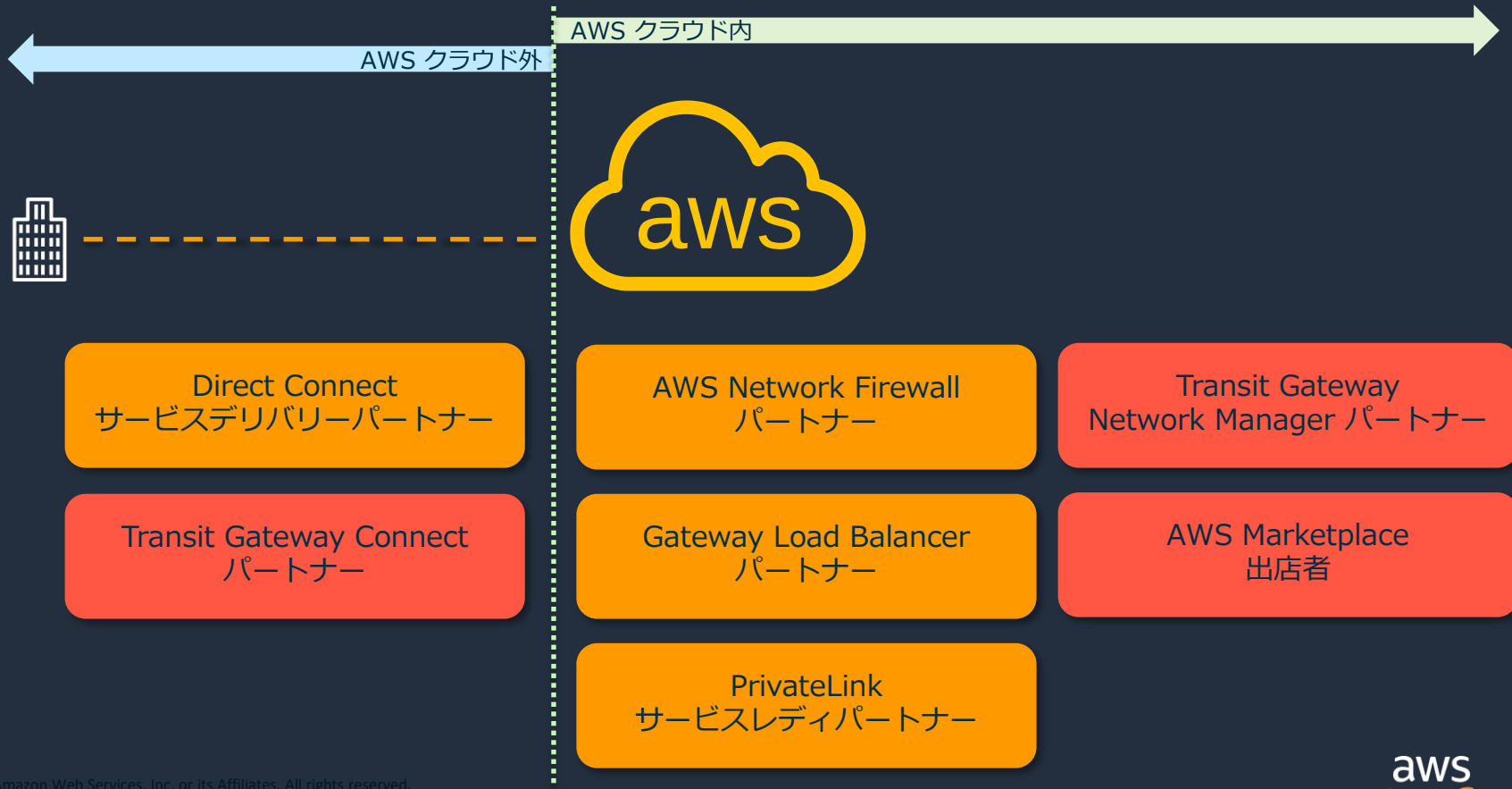
ワークロードのクラウド移行に伴いAWS がネットワークハブに進化し
データセンターの機能が不要に



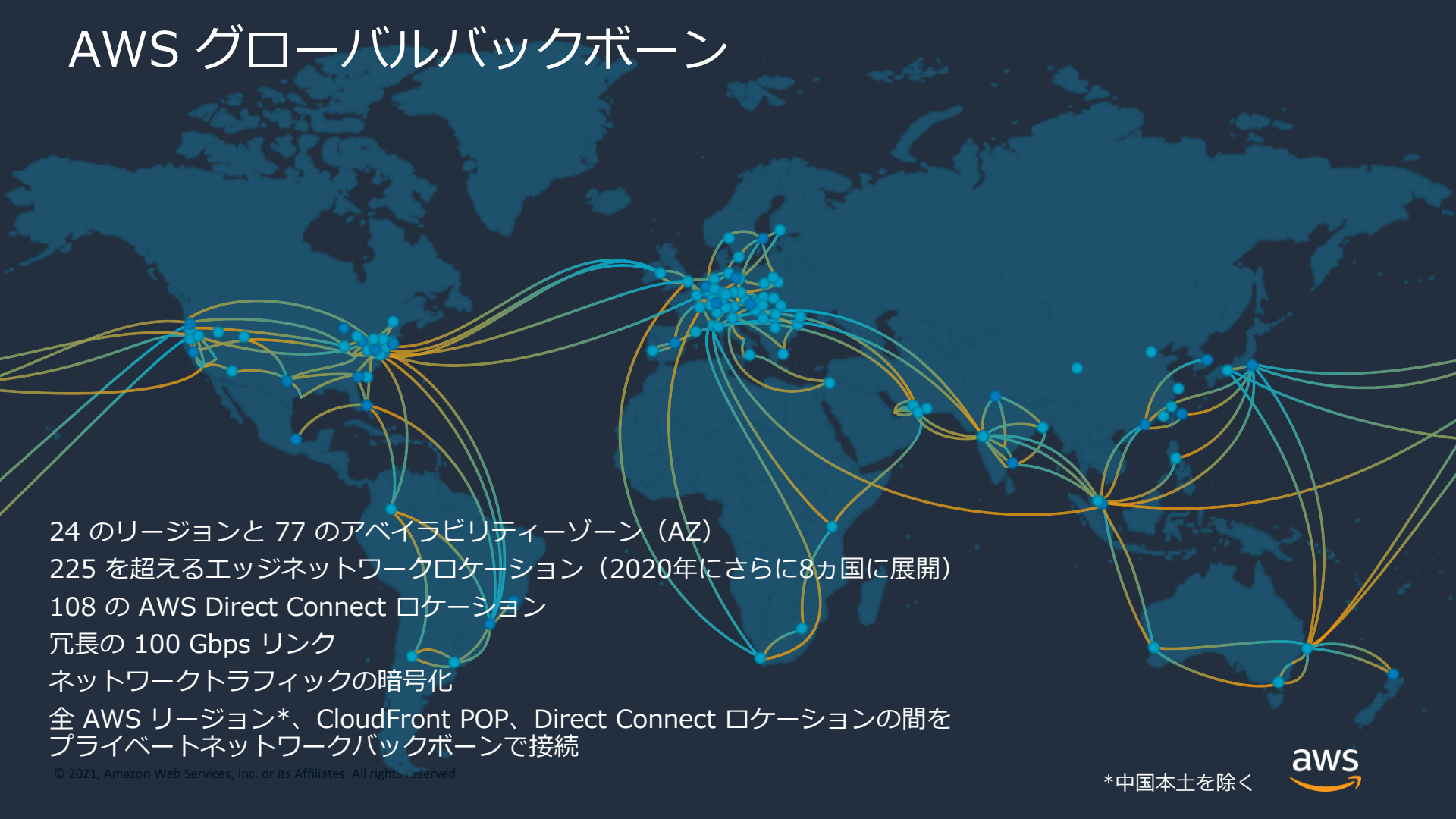
AWS Networking の描くビジョン

エッジコンピューティングからデータセンターまでを繋ぐ　ネットワークの世界

AWS と パートナーエコシステム（NW編）



AWS グローバルバックボーン



24 のリージョンと 77 のアベイラビリティーゾーン（AZ）
225 を超えるエッジネットワークロケーション（2020年にさらに8ヵ国に展開）
108 の AWS Direct Connect ロケーション
冗長の 100 Gbps リンク
ネットワークトラフィックの暗号化
全 AWS リージョン*、CloudFront POP、Direct Connect ロケーションの間を
プライベートネットワークバックボーンで接続

*中国本土を除く

AWS グローバルバックボーンの自前ならではのメリット

セキュリティ

トラフィックはインターネットではなくAWS インフラを横断

可用性

拡張性・冗長性を自社で管理

信頼できる性能

お客様トラフィックの通信経路を他社に影響されない

プロキシミティ（お客様により近い接続ポイント）

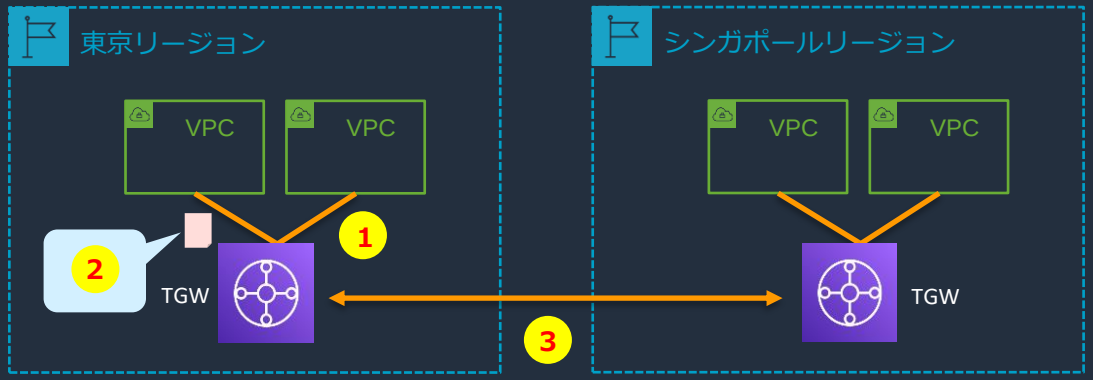
インターネット「ホットスポット」や あまり最適化されていない外部接続を回避

全てのリージョン間トラフィックがバックボーンを経由*

*中国本土を除く

aws

Transit Gateway の費用構成



ピアリングアタッチメント全体の
データ処理料金

1 アタッチメント

$ 0.07/時 x アタッチメント数

2 処理データ

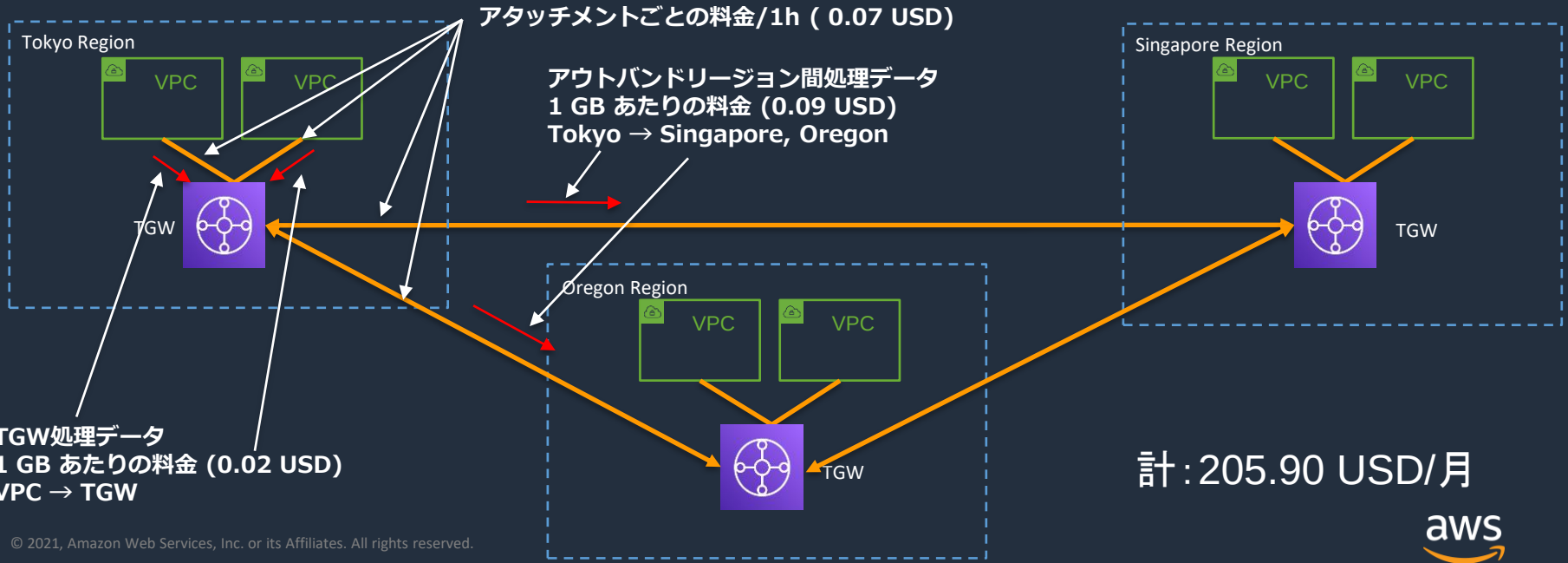
$ 0.02/GB x TGWへの転送量 (GB)

3 アウトバンドリージョン間
処理データ

$ 0.09/GB x シンガポール
リージョンへの転送量 (GB)

Transit Gateway費用例

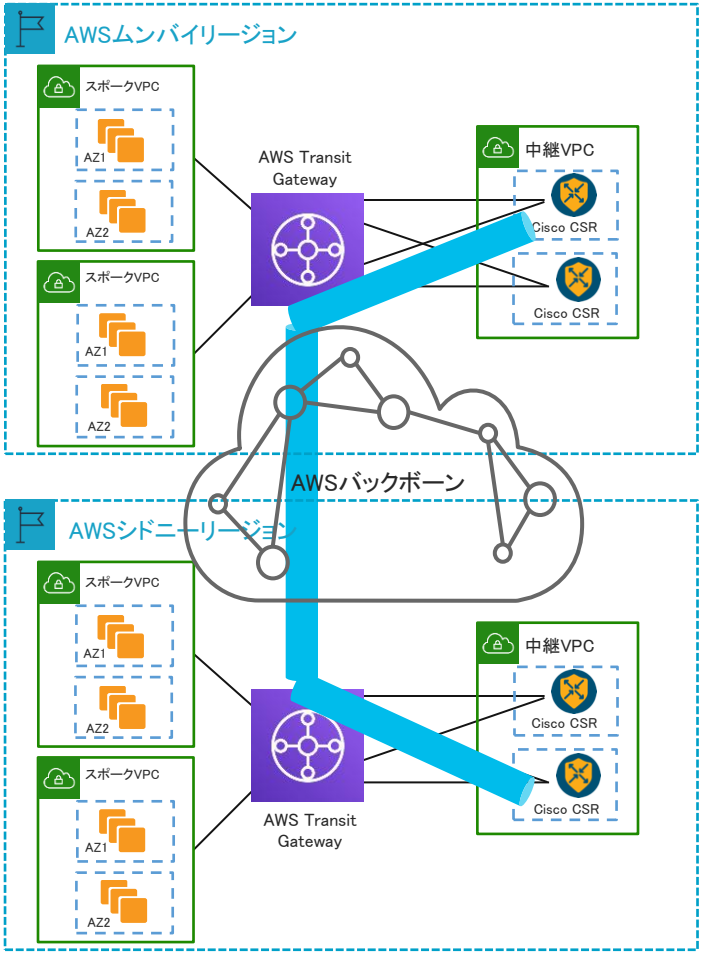
- ✓ Tokyo Regionの例
  アタッチメン4つ/月: 730 hours in a month x 0.07 USD = 51.10 USD x 4 = 204.40 USD
  TGW処理データ : 30GB per month x 0.02 USD = 0.60 USD
  アウトバンドリージョン間処理データ : 10GB per month x 0.09 USD = 0.90 USD



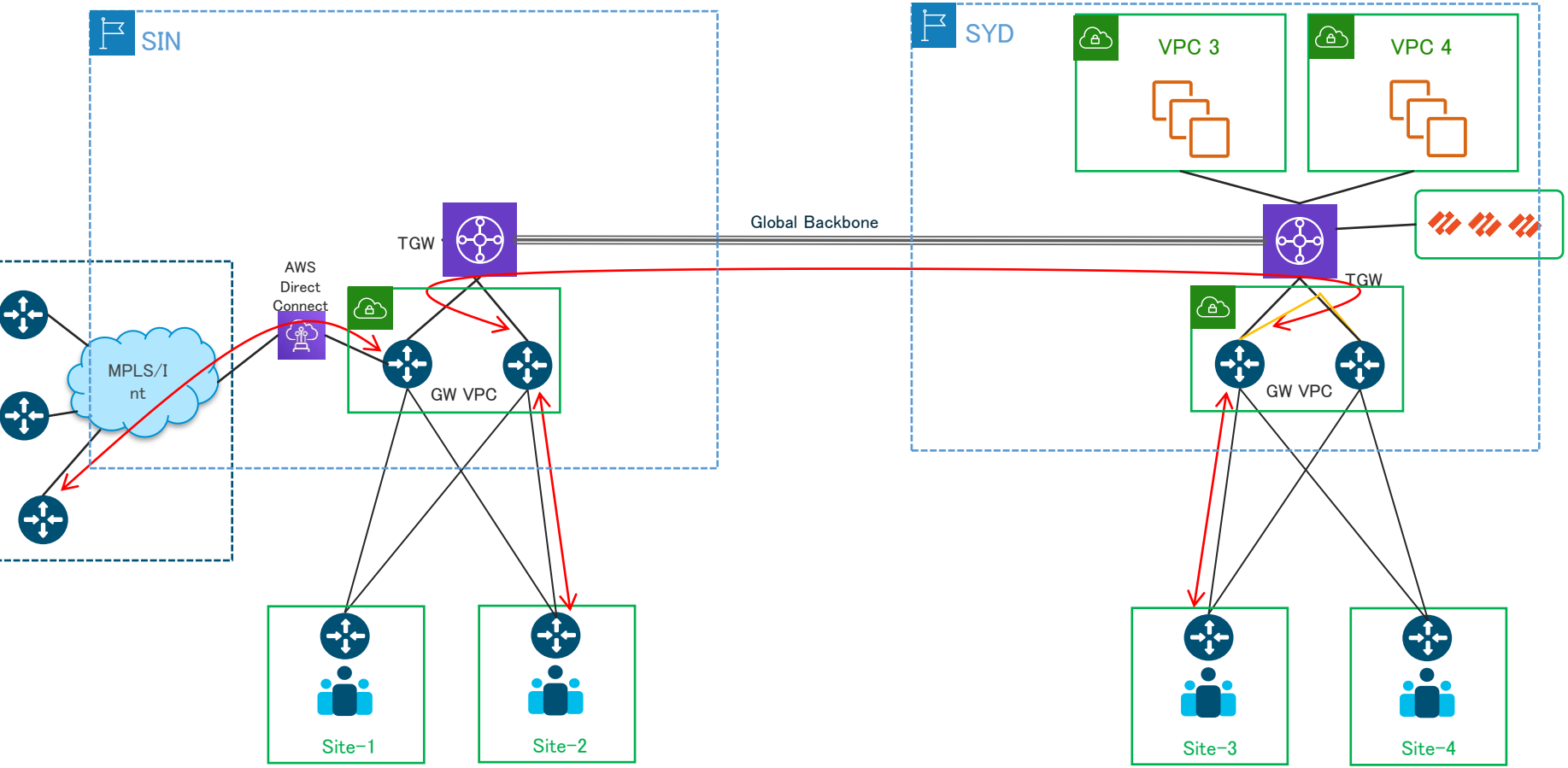
計:205.90 USD/月

AWS Transit GatewayピアリングとCisco SD-WAN

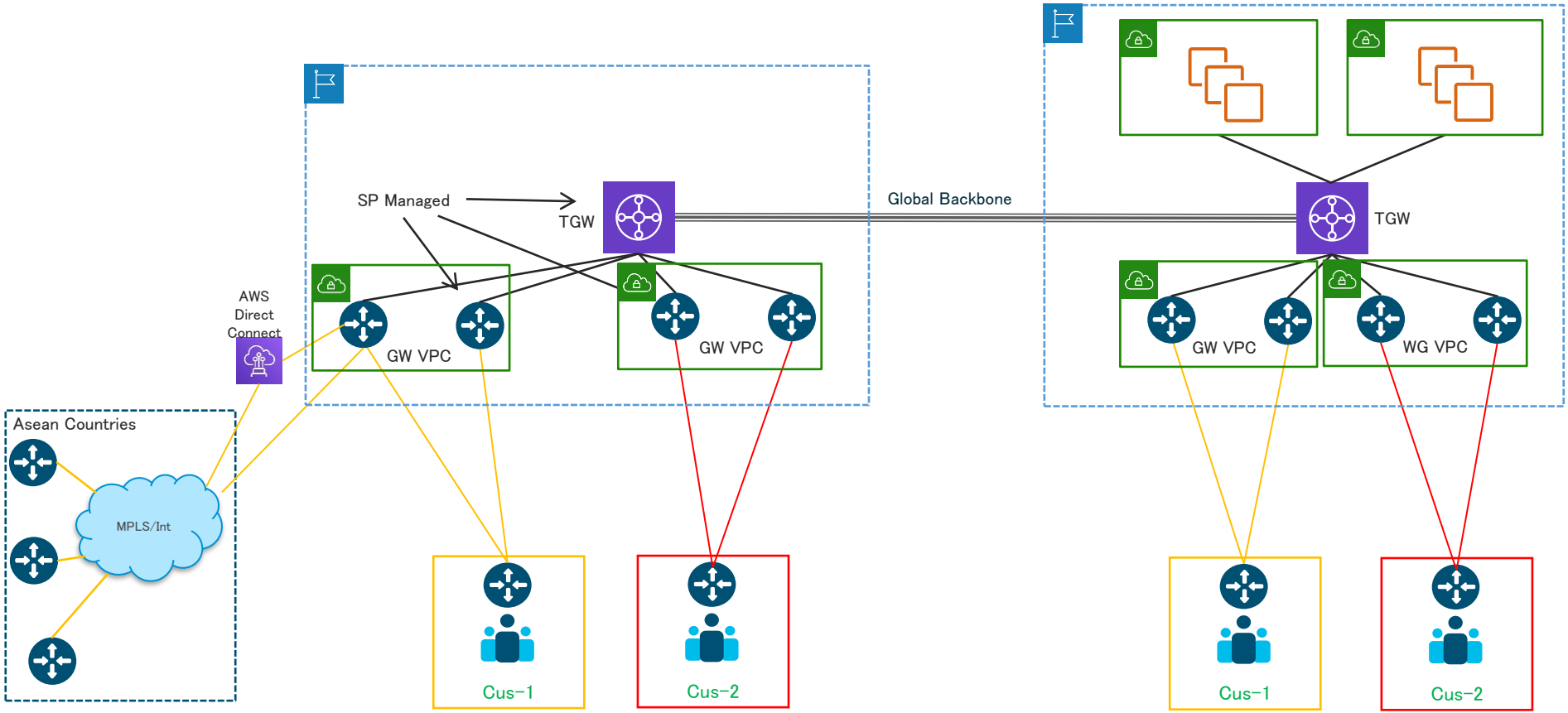
- AWSバックボーンを跨いでSD-WANトンネル
- AWSバックボーンをアンダーレイとして使う
- BFDでヘルスステータスを監視
- App-awareルーティングで通信最適化



Site to Site構成のエンタープライズのユースケース



Site to Site構成のSP/MSPのユースケース



補足：AWS TGWベースの
ブランチコネクトソリューション

補足：AWS TGWベースのブランチコネクトソリューション

課題

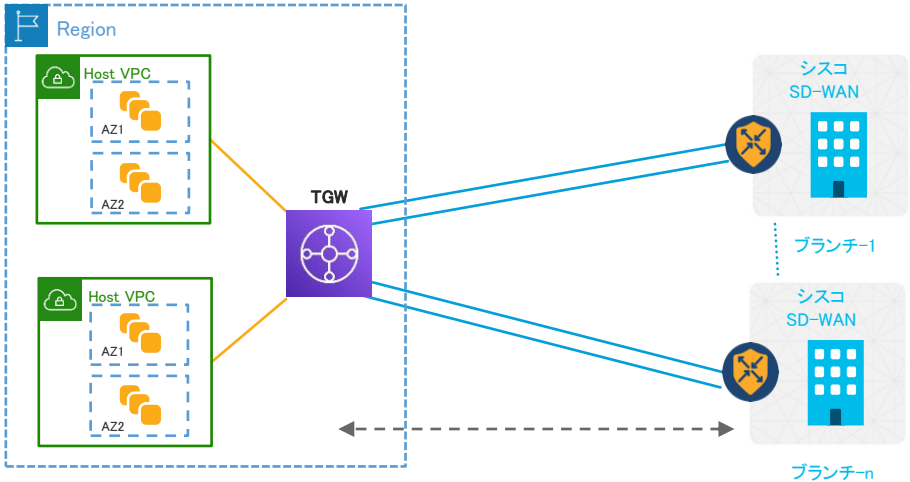
- 支店のエンドユーザがクラウドでホストされているアプリケーションにアクセスできるように、サイト/支店のVPNをクラウドまで拡張する必要がある

ソリューション

- IPSecトンネルは、エッジデバイスとAWSトランジットゲートウェイ間に設定される。これらのトンネルは、ブランチVPNのトラフィックとBGPルーティングトラフィックを伝送する
- ブランチデバイスは複数のVPNを持つことができ、これらの各VPNはTGWへのVPN attachementで接続する
- VPN attachementの一部として、ブランチデバイスからTGWへのVPNの接続を可能にするAWSカスタマーゲートウェイとVPN接続クラウドオブジェクトが作成される。
- 冗長性のために、ブランチごとに2つのIPSecトンネルが構成される

警告/前提条件

- TGWがvManageによってインスタンス化、管理、および制御される新しい展開でのみサポートされる



本日のまとめ、Summary

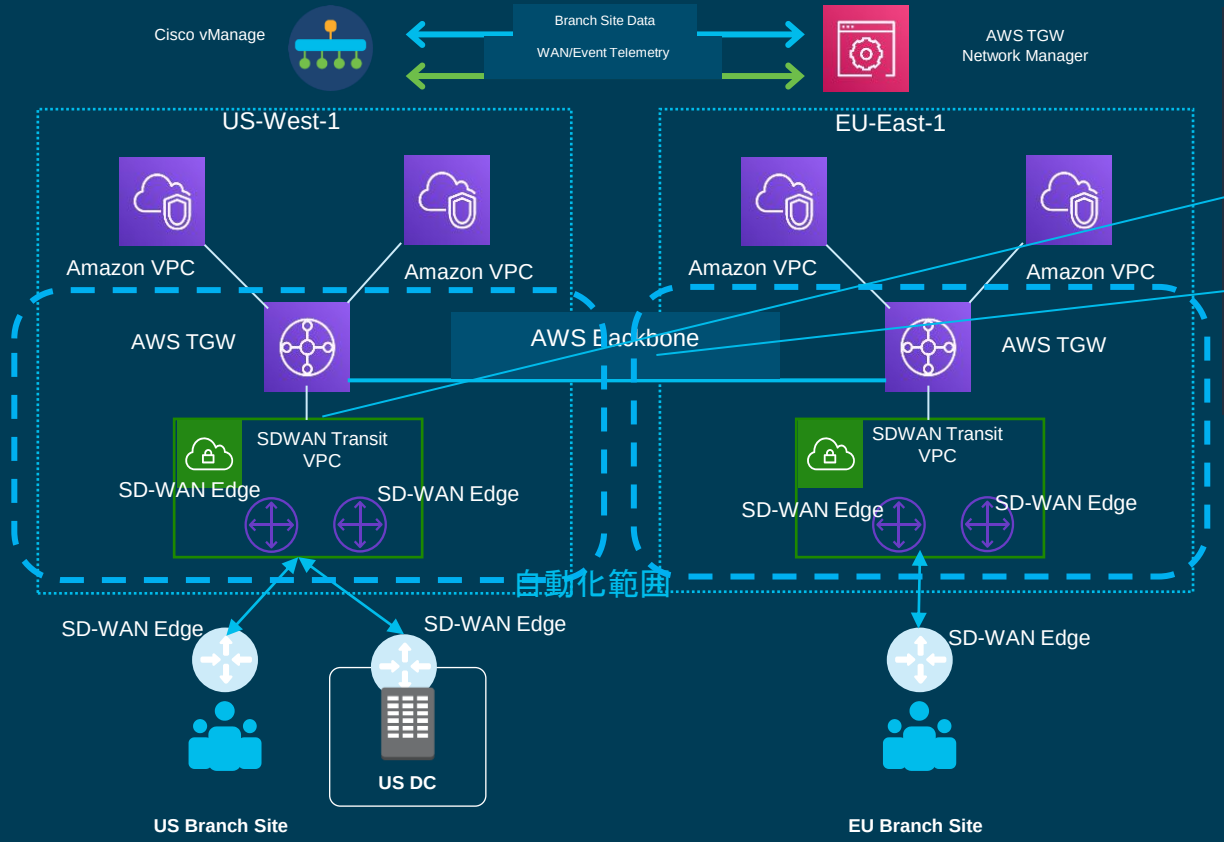
- ✓ Site to Cloud
- ✓ Site to Site

本日のまとめ、ポイント

- Site to Cloud: Cisco SD-WANでのAWSクラウドへの接続方式、3パターンをご紹介（TGW経由推奨！）

- Site to Site: Cisco SD-WANのアンダーレイとしてAWS TGW、AWSバックボーンを活用するシナリオをご紹介

本日のまとめ、ポイント



Cisco SD-WANのCloud onRamp for Multicloud機能を使用すると、次のシナリオをシームレスに実現できる

1. Site to Cloud: AWS TGWを使ってSD-WANネットワークをAWSに接続する
2. Site to Site: AWS TGWのリージョン間ピアリングを使用して、AWSネットワークバックボーンを利用してSD-WANネットワークをグローバルに接続する

Thank you