

AWS-54

Amazon VPC ネットワーキングの 基本構成・運用管理

丁 亜峰

技術統括本部 ソリューションアーキテクト
アマゾン ウェブ サービス ジャパン合同会社



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

自己紹介



名前：丁 亜峰 (Tei Amine)

所属：アマゾンウェブサービスジャパン合同会社
技術統括本部 ソリューションアーキテクト

好きなAWSサービス：

AWS Transit Gateway, AWS サポート, AWS IoT Core



本セッションの対象者と持ち帰ってほしいこと

対象者

オンプレミスでネットワーク・インフラをご担当の方
AWSのネットワーク関連サービスを習得したい方
これからAWSクラウドを利用する予定の方

持ち帰ってほしいこと

AWS VPC ネットワーキングの基本構成、AWSセキュリティサービス
VPC間、オンプレミスとプライベート接続するAWS PrivateLinkのメリット
ネットワーク構成を簡素化できるAWS Transit Gatewayの新機能

本セッションでご紹介する内容

- AWS ネットワーキングサービス
 - Amazon VPC基本構成
 - VPC間、オンプレミスと接続するサービス
- Amazon VPC セキュリティの基本
 - AWS セキュリティ サービス
- ネットワークのモニタリング & ビジビリティ
- まとめ

AWS ネットワークサービス



AWS ネットワーキング サービス



Amazon VPC

AWSの論理的に隔離された
仮想ネットワーク



AWS Transit Gateway

VPC間、オンプレミスのネ
ットワークと接続するた
めの中央ハブ



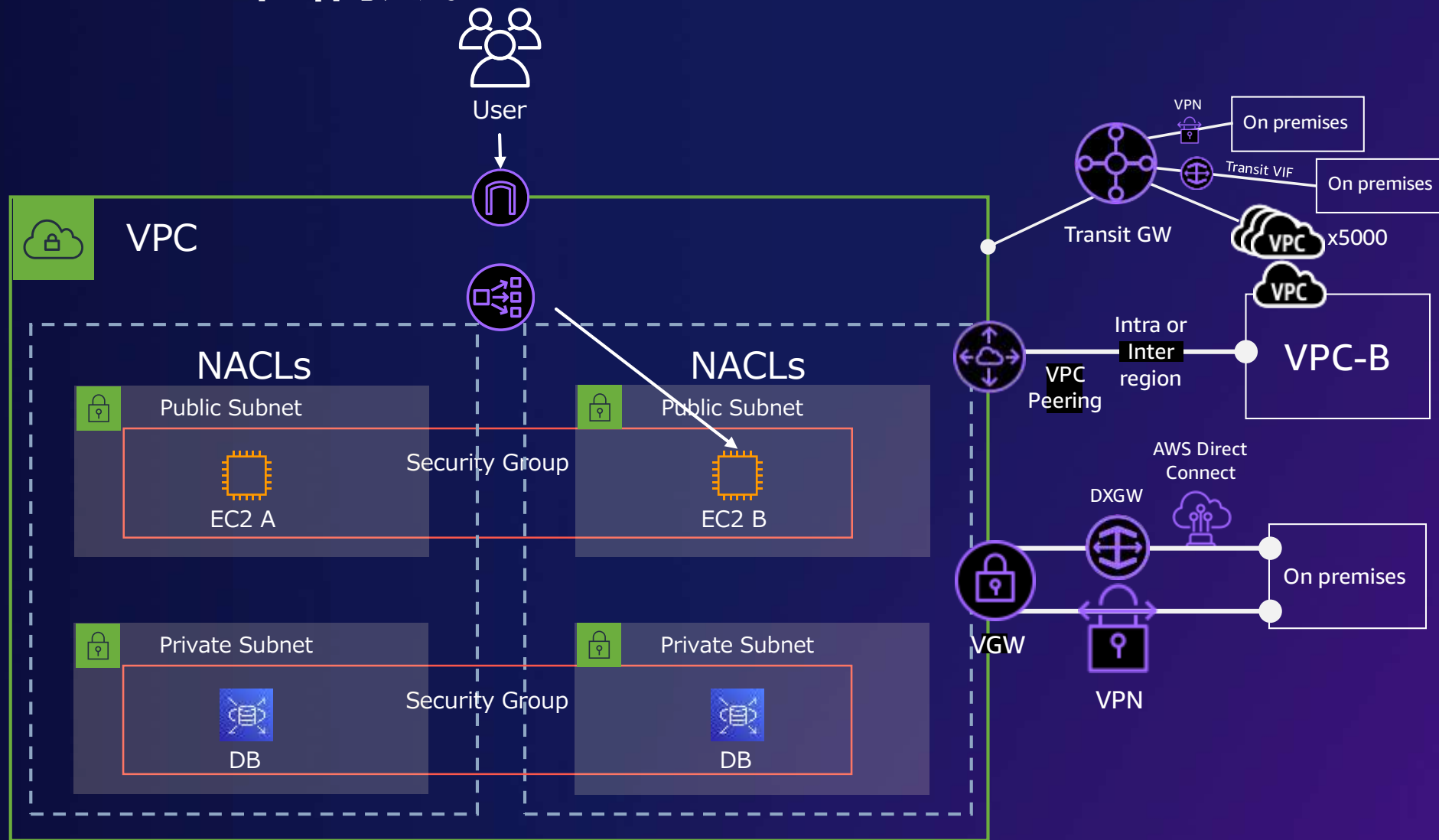
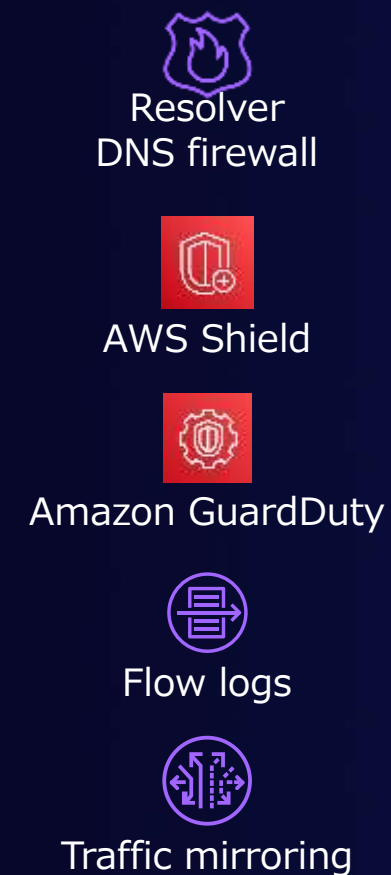
AWS PrivateLink

パブリックインターネット
にトラフィックを出さず
にプライベート接続

Amazon VPC 基本構成

Amazon VPC 基本構成

WEB 3-TIER



[AWS Black Belt Online Seminar] Amazon VPC 資料及び QA 公開

<https://aws.amazon.com/jp/blogs/news/webinar-bb-amazonvpc-2020/>



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Amazon VPC IPアドレスの割り当て

IPv4

Reserved

10.0.0.0 – VPC Base

+ 2

10.0.0.2 – Route 53 リゾルバ

10.0.1.0 – ネットワークアドレス

10.0.1.1 – VPC ルーター

10.0.1.2 – AWS予約済み

10.0.1.3 – AWS予約済み

10.0.1.255 – Network Broadcast

...

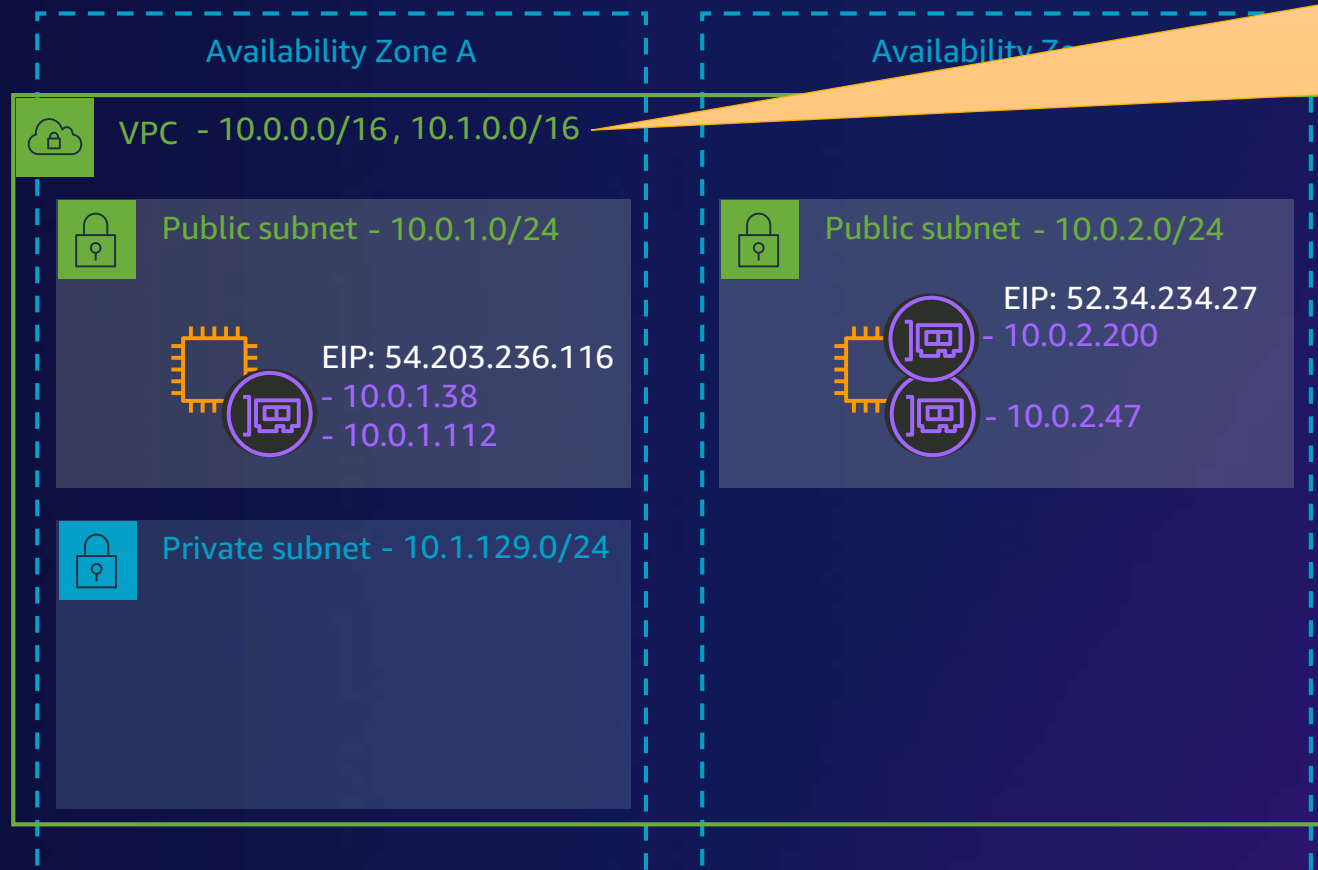
10.0.128.0 – ネットワークアドレス

10.0.128.1 – VPC ルーター

10.0.128.2 – AWS予約済み

10.0.128.3 – AWS予約済み

10.0.128.255 – Network Broadcast



VPCに新しいIPv4のCIDR「10.1.0.0/16」を追加。

Private Subnet「10.1.129.0/24」を新規作成。

Amazon VPC IPアドレスの割り当て

IPv4, IPv6

Reserved

10.0.0.0 – VPC Base

+ 2

10.0.0.2 – Route 53 リゾルバ

10.0.1.0 – ネットワークアドレス

10.0.1.1 – VPC ルーター

10.0.1.2 – AWS予約済み

10.0.1.3 – AWS予約済み

10.0.1.255 – Network Broadcast

...

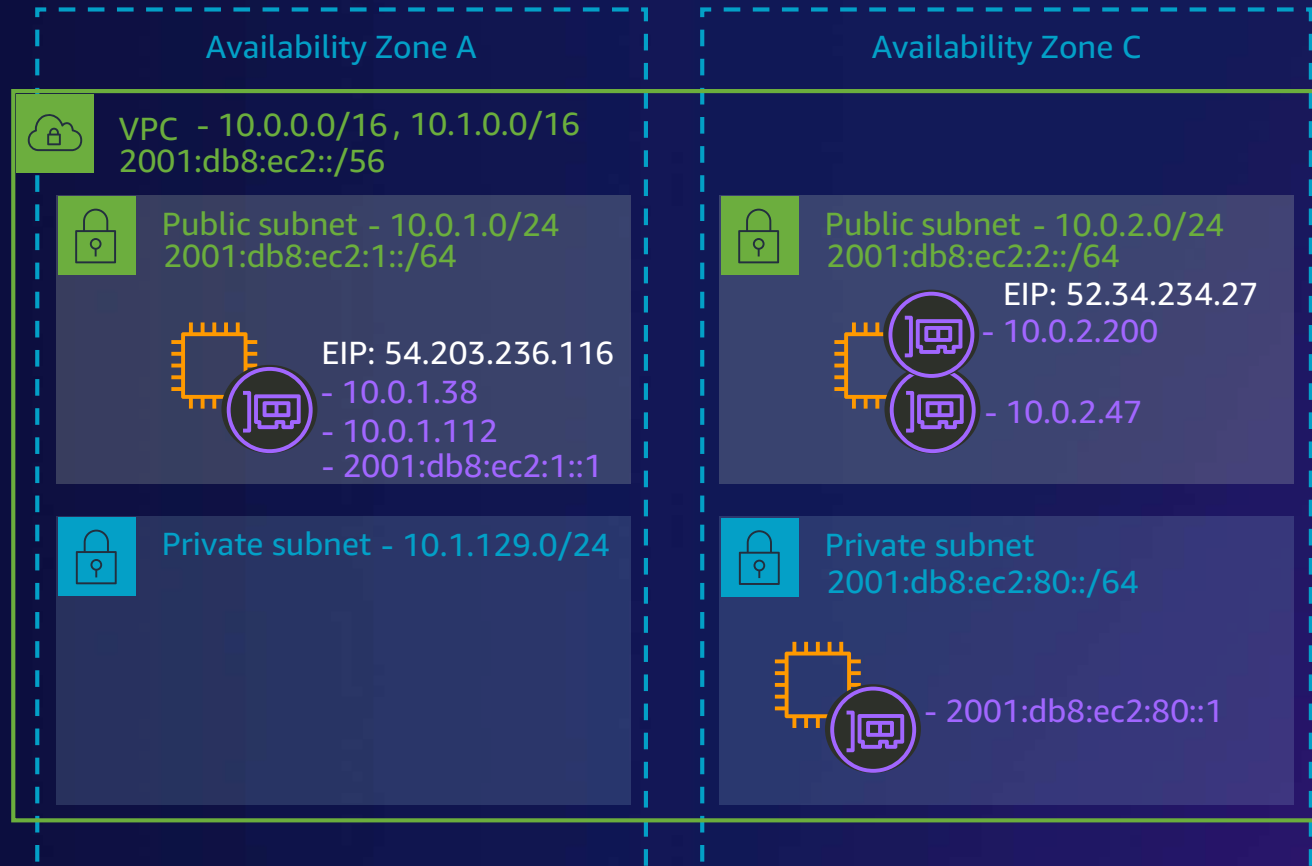
10.0.128.0 – ネットワークアドレス

10.0.128.1 – VPC ルーター

10.0.128.2 – AWS予約済み

10.0.128.3 – AWS予約済み

10.0.128.255 – Network Broadcast



Reserved

fd00:ec2::/32 – Reserved

fe80::X:Xff:feX:X/64 – VPC ルーター

2001:db8:ec2:1::0

2001:db8:ec2:1::1

2001:db8:ec2:1::2

2001:db8:ec2:1::3

2001:db8:ec2:1:ffff:ffff:ffff:ffff

...

2001:db8:ec2:80::0

2001:db8:ec2:80::1


2001:db8:ec2:80::2

2001:db8:ec2:80::3

2001:db8:ec2:80:ffff:ffff:ffff:ffff

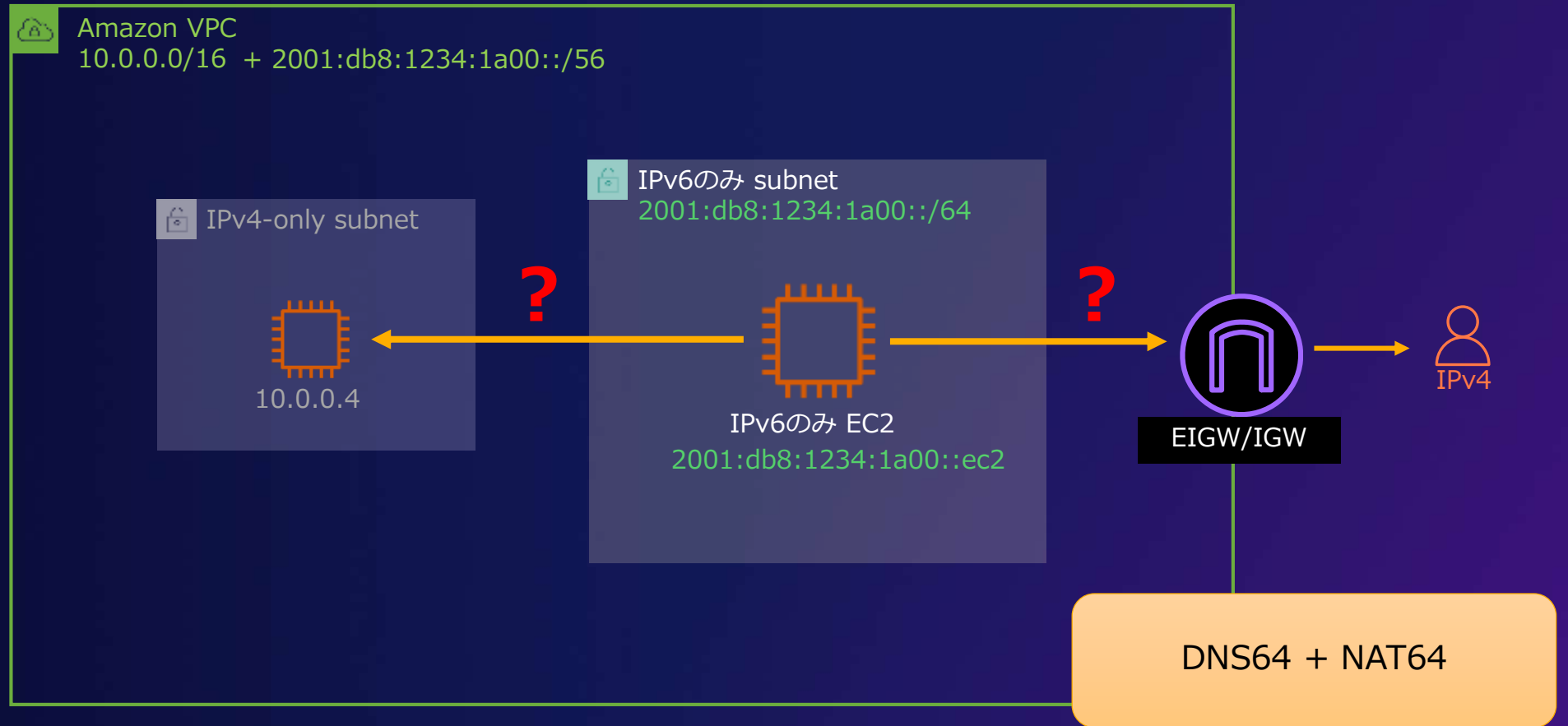
Amazon VPC IPアドレスの割り当て

インスタンスで割り当てを確認

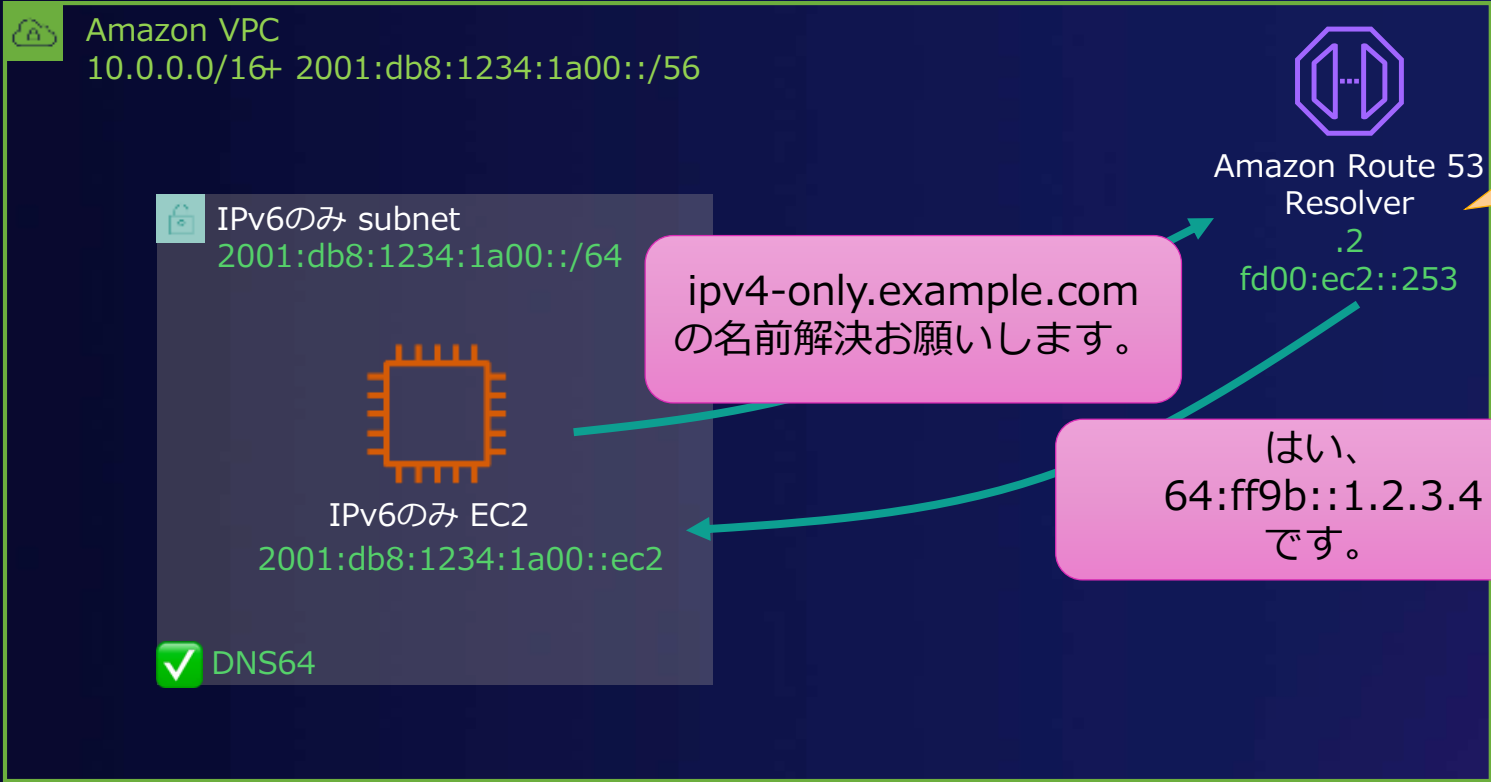


```
[ec2-user@ip-10-1-20-175 ~]$ ip addr show dev eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 0e:a3:2c:7f:9e:39 brd ff:ff:ff:ff:ff:ff
    inet 10.1.20.175/24 brd 10.1.20.255 scope global dynamic eth0
        valid_lft 2958sec preferred_lft 2958sec
    inet6 2600:1f18:2477:6f20:f92c:b6bb:58f:cecf/128 scope global dynamic
        valid_lft 439sec preferred_lft 129sec
    inet6 fe80::ca3:2cff:fe7f:9e39/64 scope link
        valid_lft forever preferred_lft forever
[ec2-user@ip-10-1-20-175 ~]$ ip -6 route show dev eth0
2600:1f18:2477:6f20:f92c:b6bb:58f:cecf proto kernel metric 256 expires 415sec pref medium
2600:1f18:2477:6f20::/64 proto kernel metric 256 pref medium
fe80::/64 proto kernel metric 256 pref medium
default via fe80::cf9:92ff:fe30:7f4d proto ra metric 1024 expires 1796sec hoplimit 255 pref medium
```

デュアルスタックVPC: IPv6 to IPv4



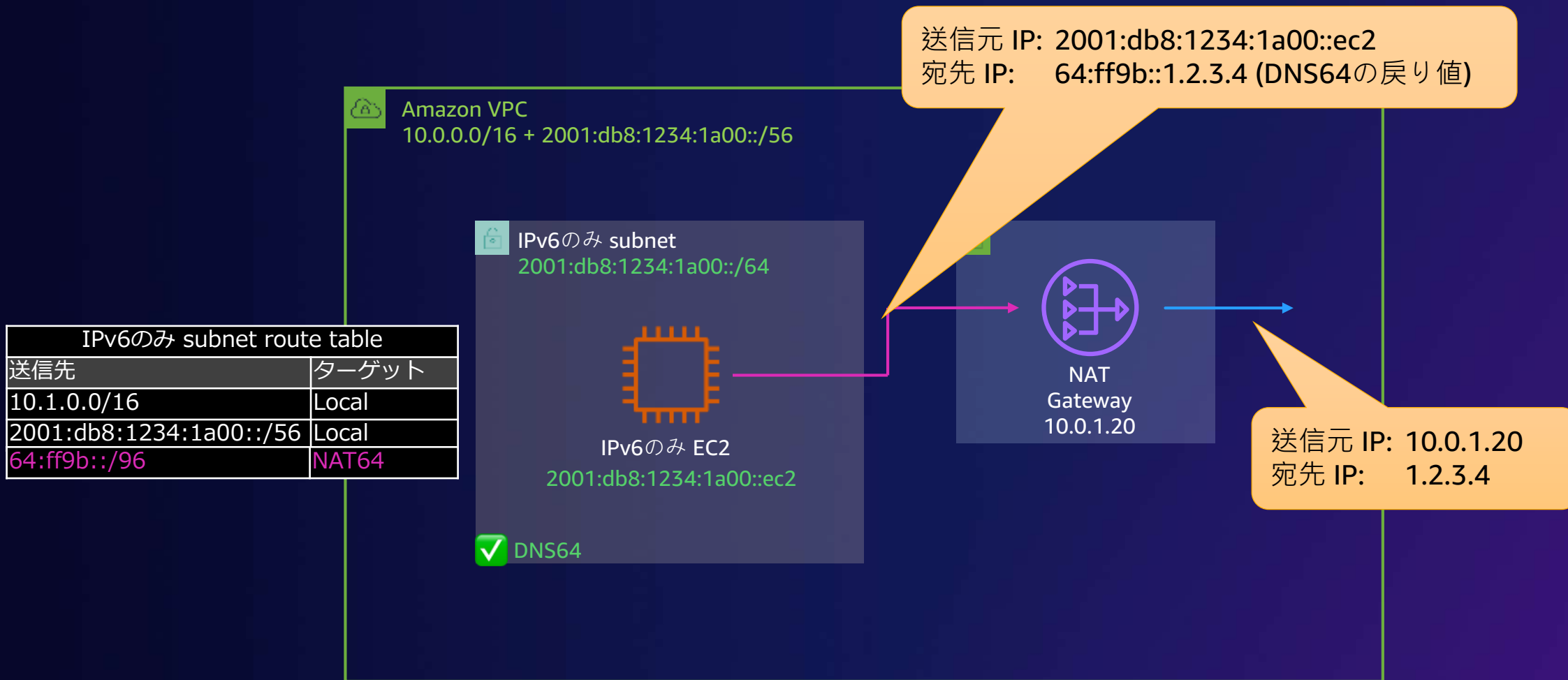
DNS64の動き



レコード内の IPv4 アドレス
の先頭にRFC6052 で定義さ
れた既知の (64:ff9b::/96)
を付けてIPv6 アドレスを合
成して返す。

		Type	Value	Amazon Route 53 Resolverの戻り値
ipv4-only.example.com	A		1.2.3.4	64:ff9b::1.2.3.4
ipv6-only.example.com	AAAA		2001:db8::1	2001:db8::1

NAT64はどう動く？



トラフィックフロー

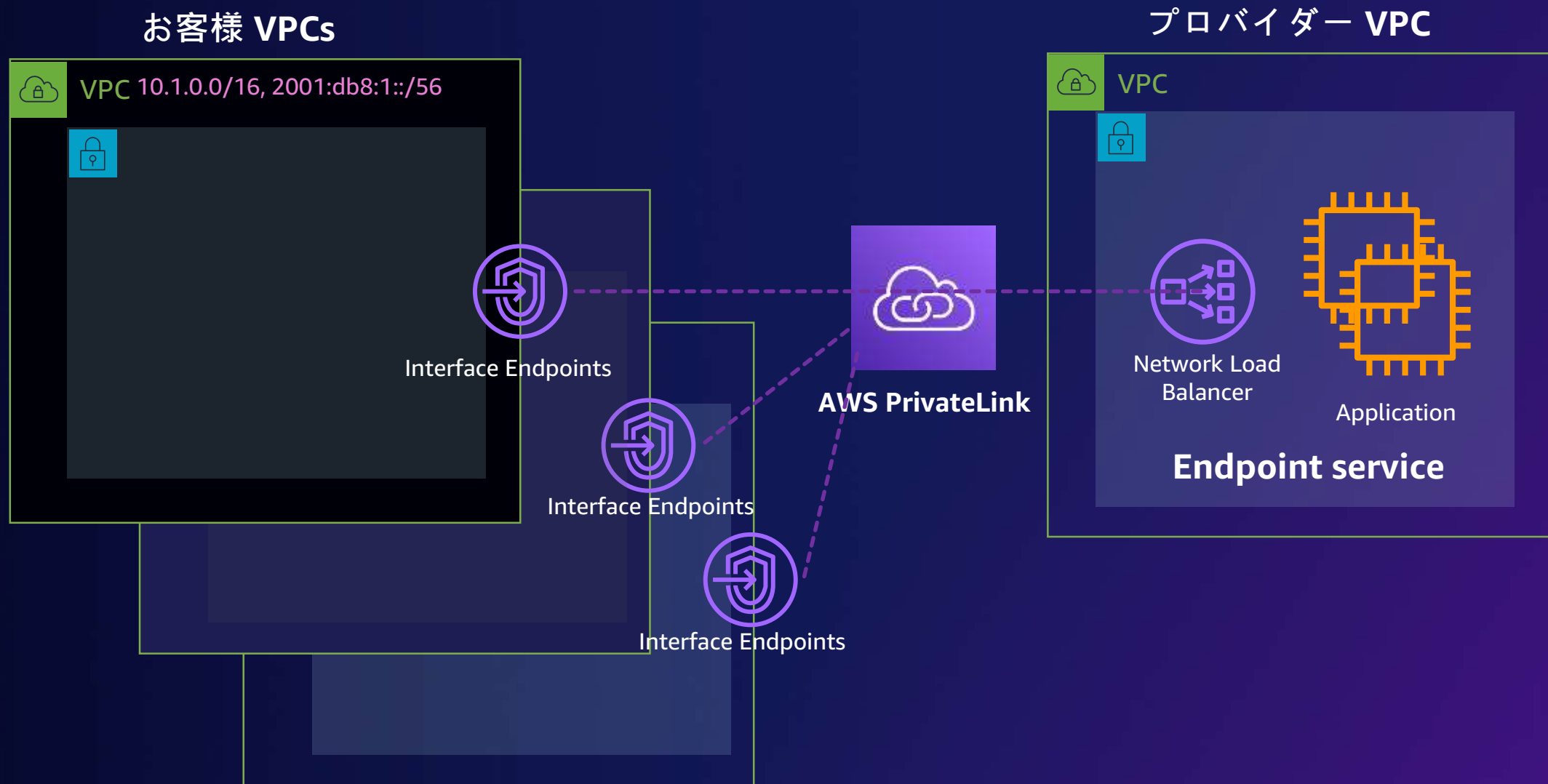


VPC間、オンプレミスと 接続するサービス

セキュリティを強化する AWS PrivateLink



AWS PrivateLink

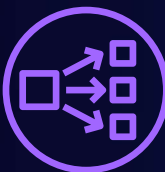


AWS PrivateLink 構成要素



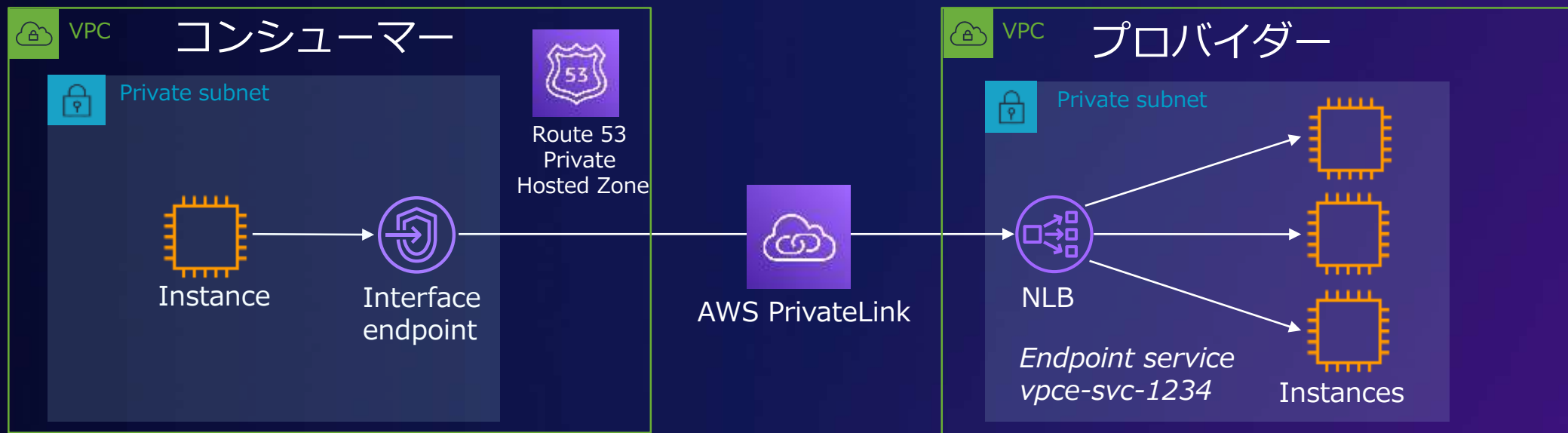
インターフェイス エンドポイント (コンシューマーVPC)

- サービスへの通信を受け付けるエンドポイント。AWS PrivateLinkを利用し、ENIが1つ以上作成される
- ENIにセキュリティグループを関連付けてアクセス制御
- アプリケーションからはエンドポイント固有の DNS ホスト名、またはデフォルト DNS 名を使用 (AWS および AWS Marketplace パートナーサービスの場合)



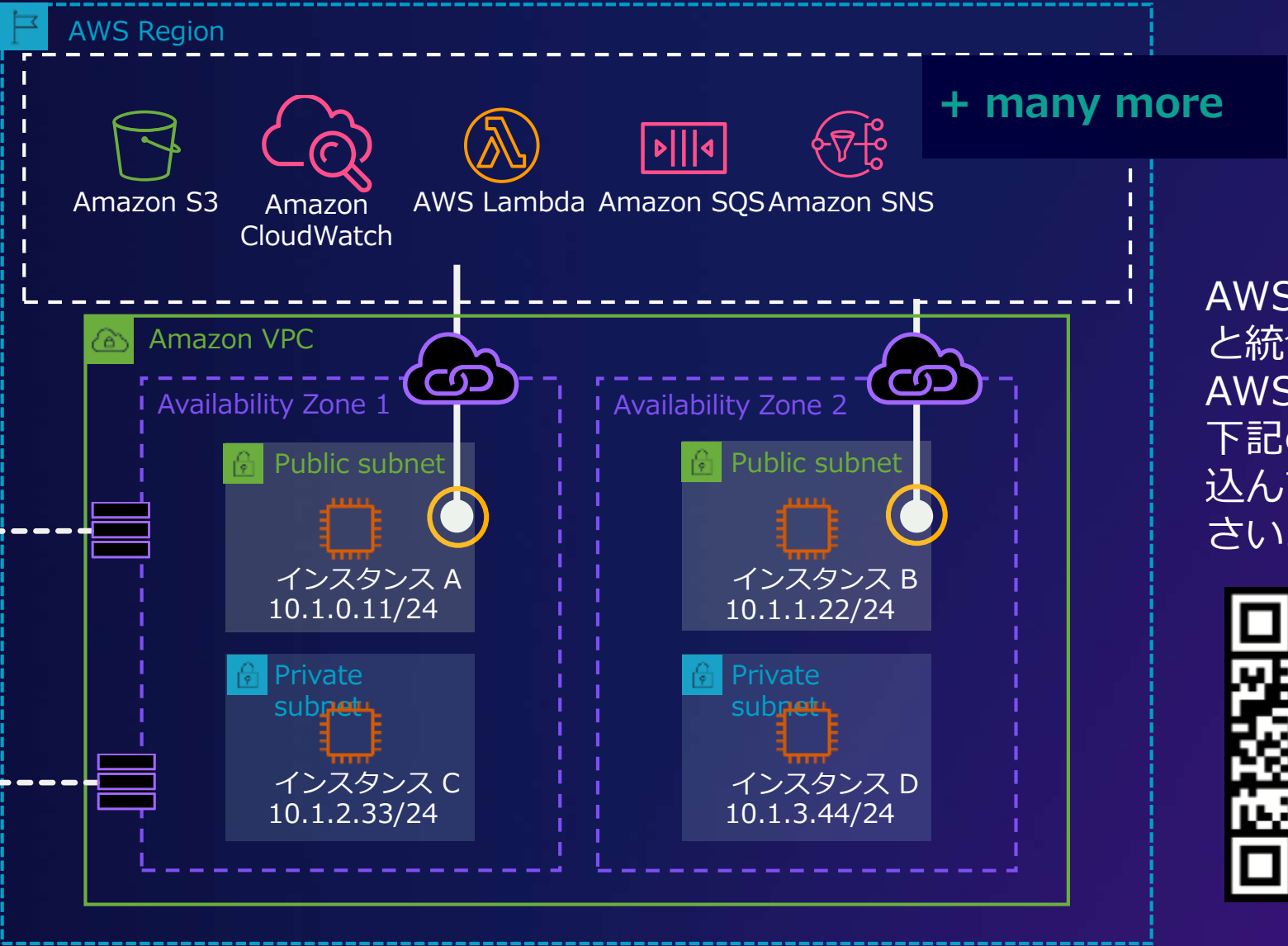
エンドポイントサービス (プロバイダーVPC)

- AWS PrivateLink を利用したサービスを他のコンシューマーに提供する場合に必要
- サービスフロントエンドとして使用されるNetwork Load Balancer(NLB)
- VPC エンドポイントサービスを作成し、NLB を指定



AWS PrivateLink: インターフェースエンドポイント

VPC内にAWSサービスの
の**エンドポイント**を作
成し、プライベートア
クセスを実現



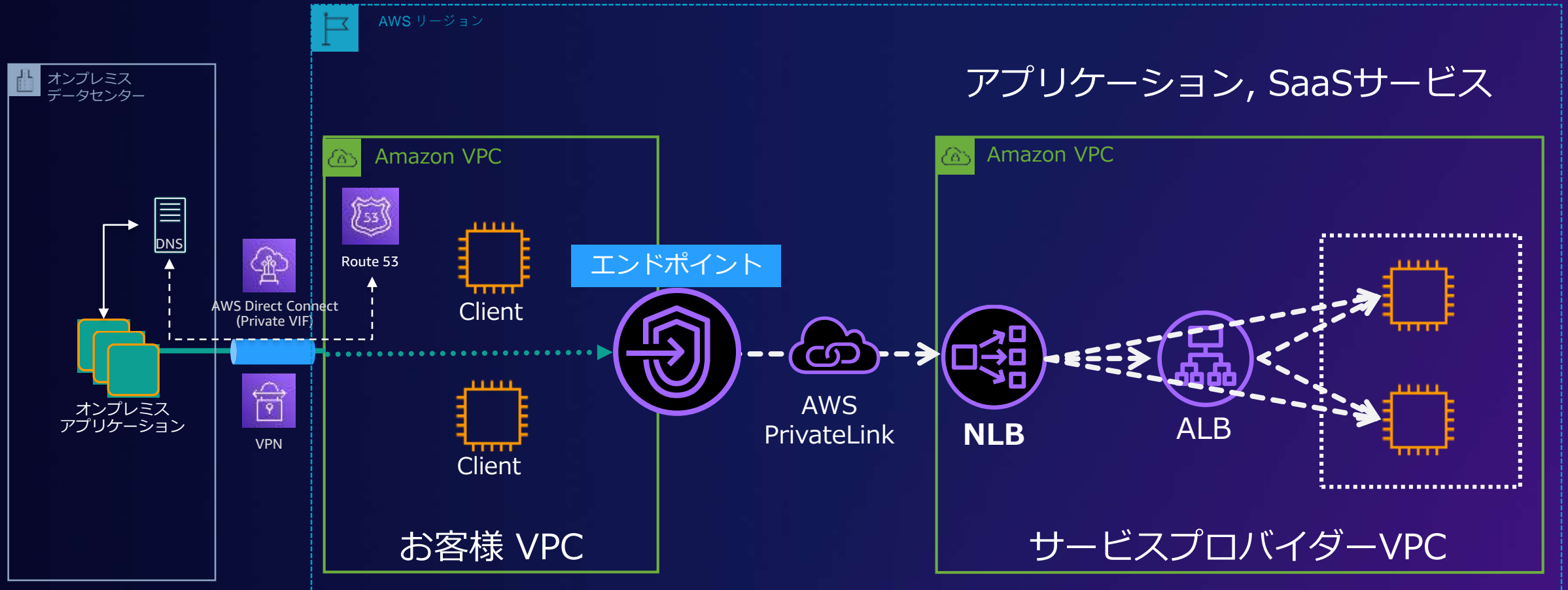
AWS PrivateLink
と統合できる
AWS サービスは
下記のQRを読み
込んでご確認ください。



AWS PrivateLink: NLBのターゲットとしてALBを利用可能

NEW

ALB と NLB のアベイラビリティゾーンを一致するように、
且つ両方が同じAWSアカウントに在る必要がある。



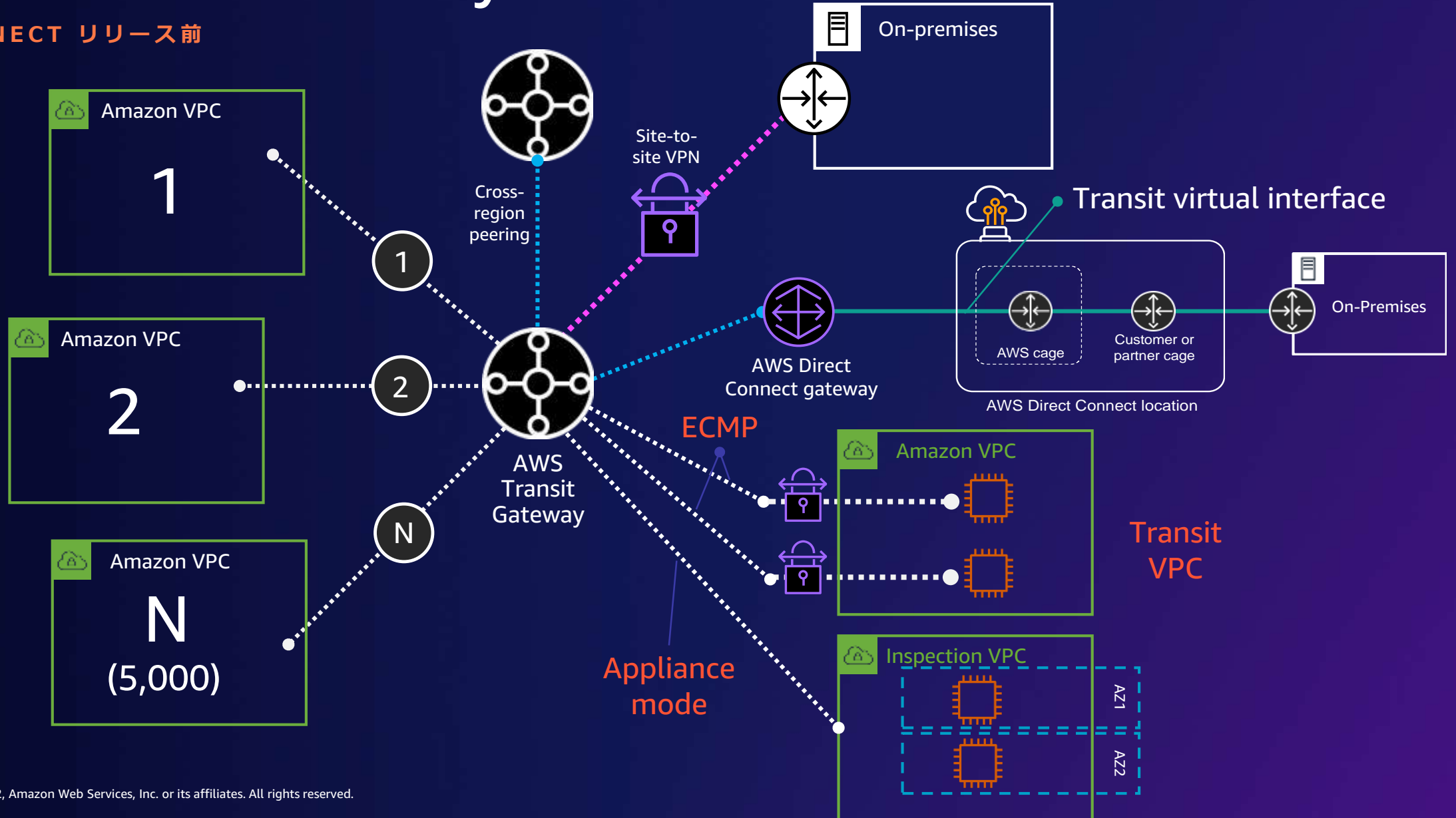
ネットワーク管理を簡素化 AWS Transit Gateway(TGW)

- TGW Connect
- リージョン内ピアリング
- TGW Network Manager



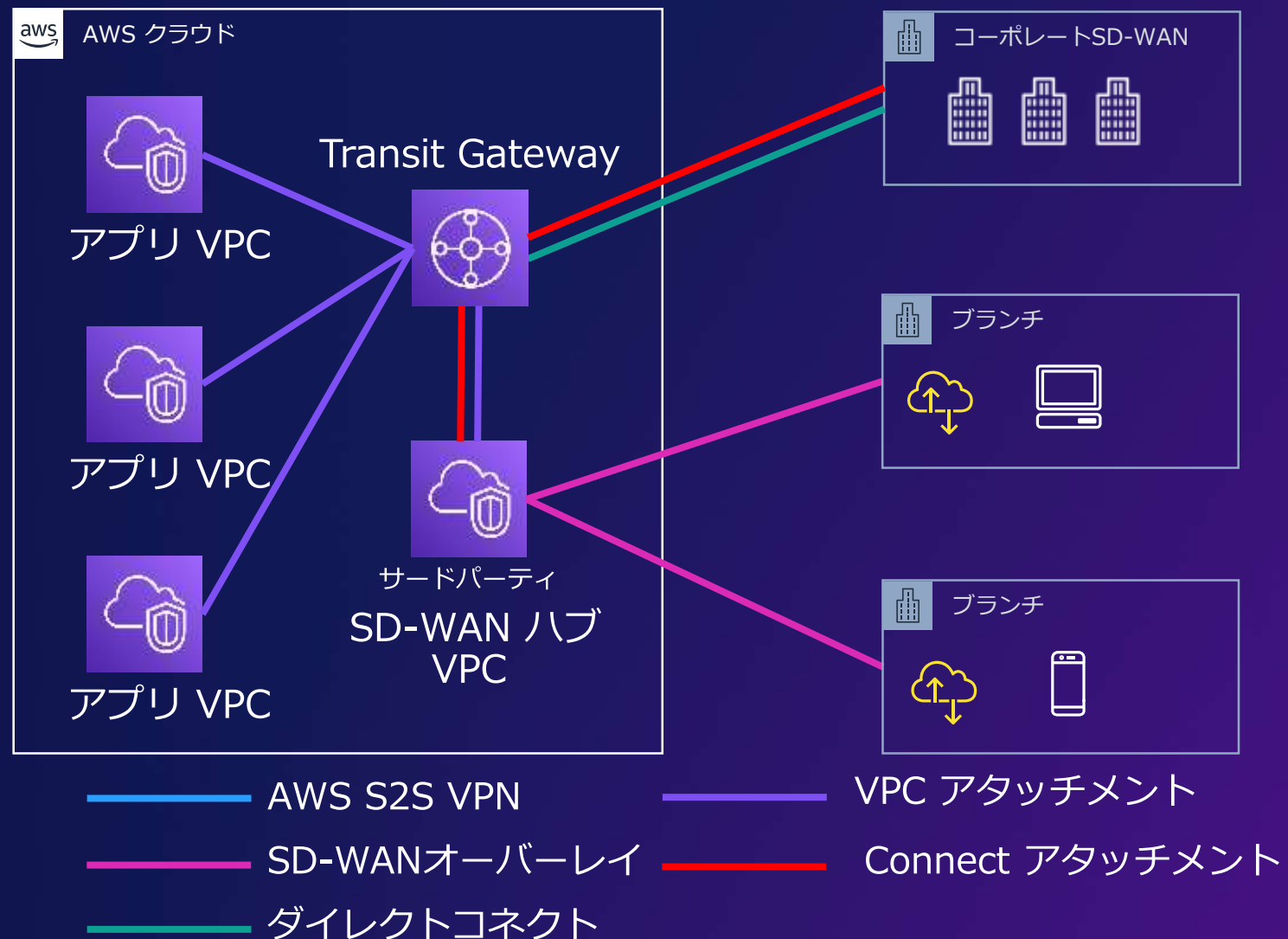
AWS Transit Gateway

TGW CONNECT リリース前



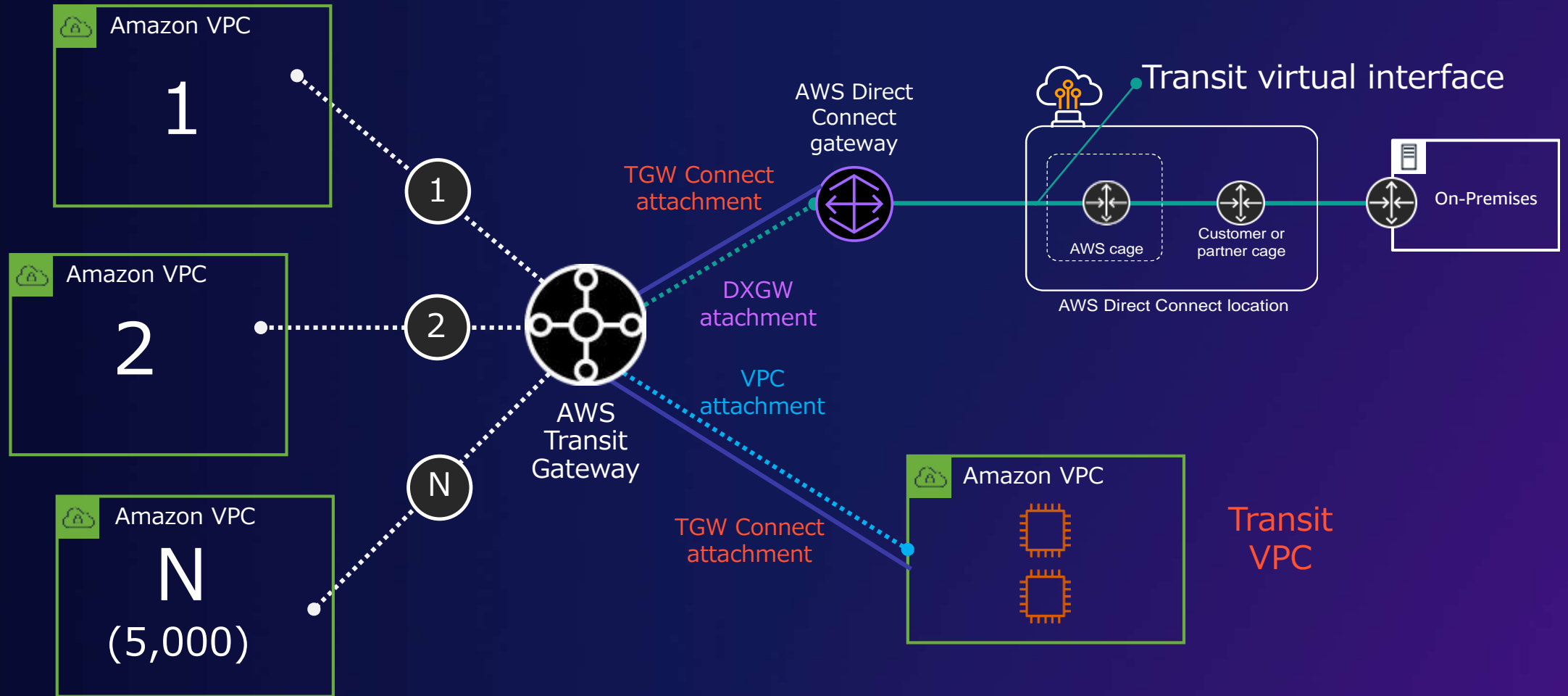
TGW Connect - SD-WAN

- SD-WAN と TGW 間のダイナミックルーティング (BGP) が、ルーティングの複雑さを軽減
- オンプレミスの SD-WAN アプリケーションと TGW を簡単に統合
- スケーラビリティとスループットの向上



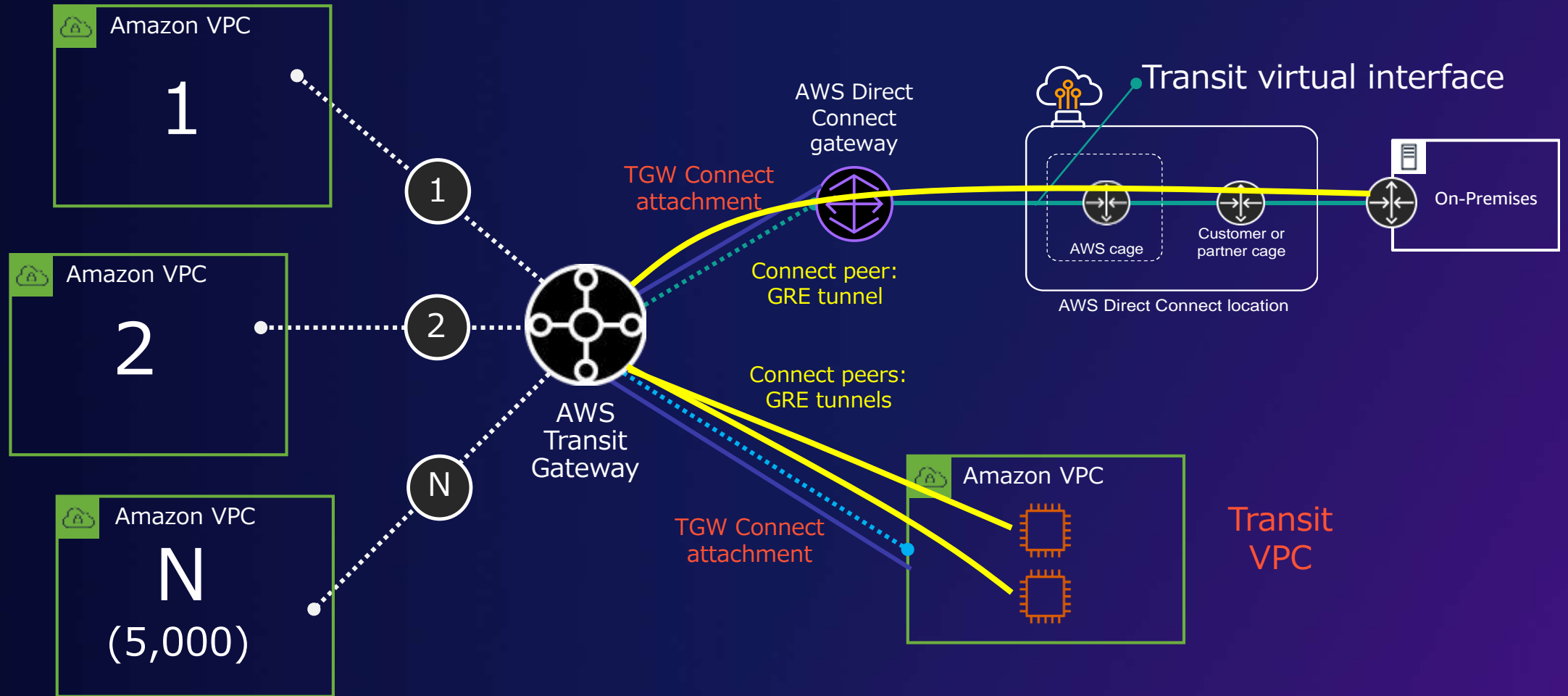
AWS Transit Gateway Connect

TGW CONNECTリリース後



AWS Transit Gateway Connect

TGW CONNECTリリース後



TGW Connect ルーティングの基本

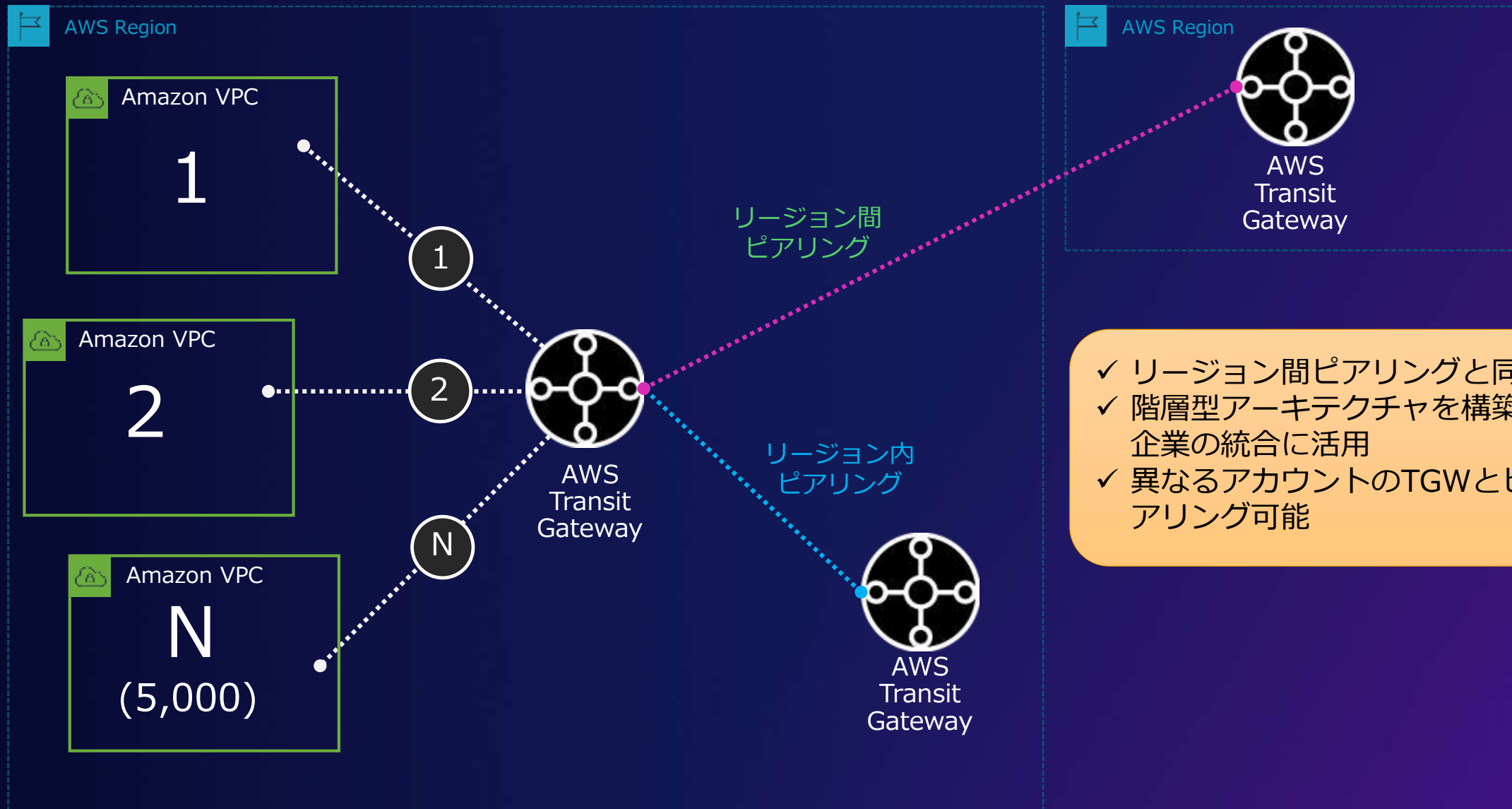
- 各 TGW Connect アタッチメントには、別々の TGW ルートテーブル（「ルーティングドメイン」とも呼ばれる）を持つことができる
 - ベースとなるトランスポートアタッチメントと同じ/異なる場合がある
- Transit Gateway CIDR ブロックへのルーティングは、スタティックルーティングで行われる
 - VPC からは、GatewayとしてTGW ID を送信先に設定するVPC ルートテーブルを利用
 - オンプレミスから、カスタマーゲートウェイルートテーブルで定義
- イコールコストマルチパス (ECMP) がサポートされている
 - サードパーティのアプライアンスは、同じ BGP「AS-PATH」属性を使用して、TGWに同じプレフィクスをアドバタイズするように設定
 - TGW がすべての ECMP パスを使用するには、AS-PATH と ASN を一致させる

TGW Connect がサポートする構成要素

- TGW Connectは、以下をサポート
 - **外部 BGP (eBGP)** - 別の自律システム (ASN) 内のルータを TGW に接続
 - **内部 BGP (iBGP)** - Transit Gateway と同じ ASN 内のルータの接続
 - **BGP (MP-BGP) のマルチプロトコル拡張** - IPv4 、 IPv6 アドレスファミリーなどの複数のプロトコル フレーバーをサポート
- BGP アドレッシング (「内部 IP」とも呼ばれる)
 - IPv6 の場合、レンジ fd00::/8 から /125
 - IPv4 の場合、次の予約ブロックを除いてレンジ 169.254/16 から /29
 - 169.254.0.0/29; 169.254.1.0/29; 169.254.2.0/29; 169.254.3.0/29; 169.254.4.0/29; 169.254.5.0/29; 169.254.169.252/29
- Connect ピアを介したスタティックルーティングは未サポート

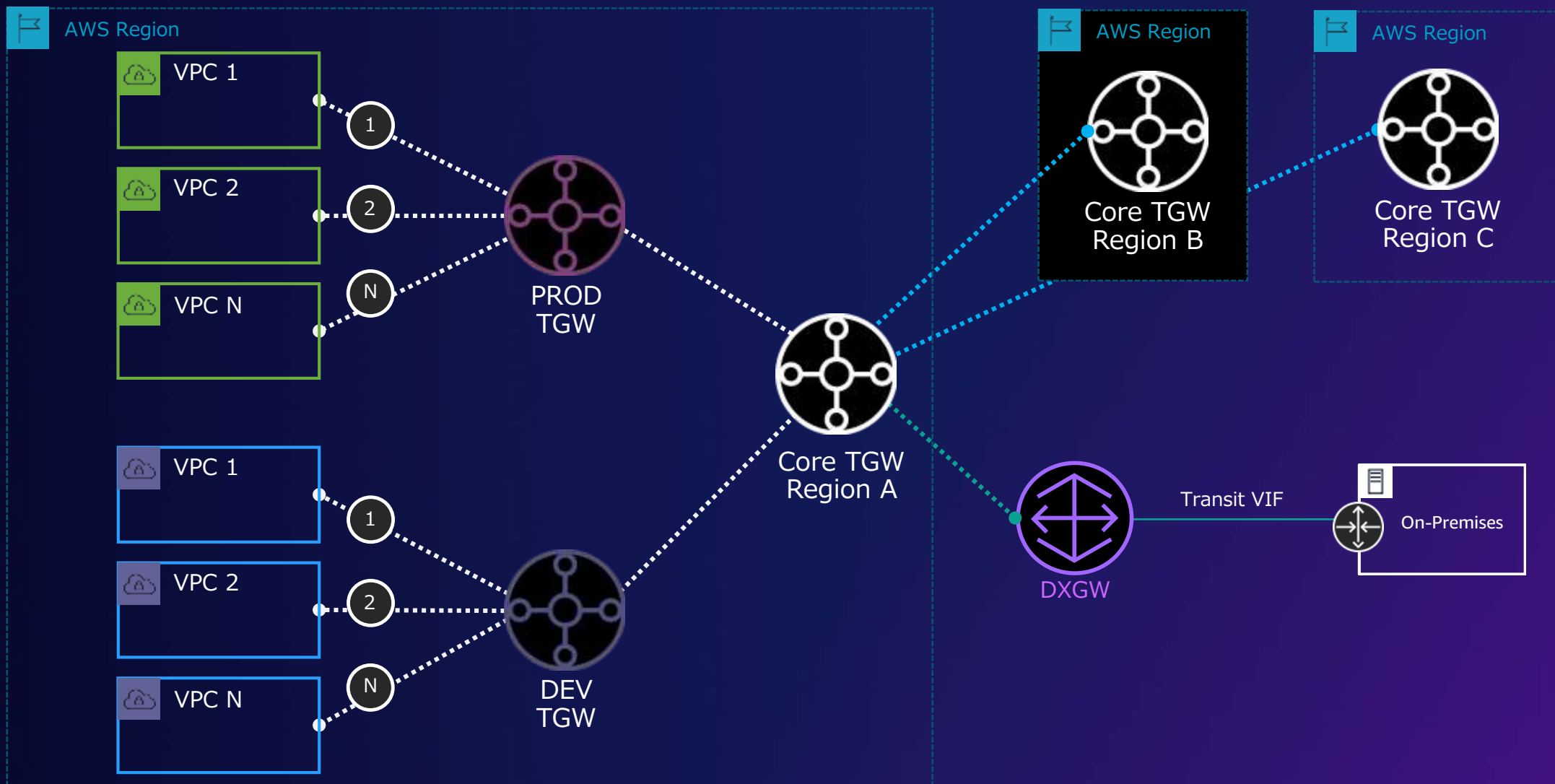
AWS Transit Gateway: リージョン内ピアリング

NEW



AWS Transit Gateway: リージョン内ピアリング

簡素化したリージョナルアーキテクチャ



AWS Transit Gateway Network Manager

グローバルネットワークにおけるネットワークとルートの分析を簡素化する新しいAPI

- グローバルネットワークのネットワークリソースの記述 (GetNetworkResources)
- グローバルネットワークのネットワークヘルス情報の取得 (GetNetworkTelemetry)
- 特定のルートテーブルのネットワークルートの取得 (GetNetworkRoutes)
- 特定のリソースのネットワークリソース関係の取得 (GetNetworkResourceRelationships)
- グローバルネットワークのネットワークリソース数の取得 (GetNetworkResourceCounts)
- 送信元と送信先のためのルーティングパスの解析開始 (StartRouteAnalysis)
- ルート解析結果の取得 (GetRouteAnalysis)
- グローバルネットワークのリソースメタデータの更新 (UpdateNetworkResourceMetadata)



セキュリティ向上する AWS セキュリティサービス



AWS Shield Advanced: 利点と機能



Shield Advanced



Standard

AWS インフラストラクチャの標準
L3 - L4 保護

CloudWatch メトリクスの提供

ヘルスベースの検出

プロアクティブなイベントまたはレスポンス

Advanced

L3 - L7 アプリケーション保護

DDoS 脅威環境ダッシュボード

L3 - L4 適応保護

AWS WAF が無料で利用可能

アプリケーションへ迅速な緩和

Shield レスポンスチームへの24/7のアクセス

AWS WAF で L7 異常検出

一元的な構成とコンプライアンス

アプリケーションレイヤの自動軽減

攻撃中のスケールリングに対するコスト保護

New

AWS Shield Advanced

24/7
DDoS Response
Team (DRT)

ポイントと
プロテクト
ウィザード

Amazon
CloudWatch
メトリクス

強化される保護

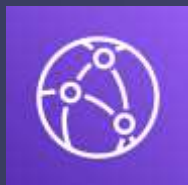
予め組み込まれ
たDDoS対策が
標準適用



Application
Load Balancer



Classic Load
Balancer



Amazon
CloudFront



Amazon
Route 53



Elastic IP Address



Network Load
Balancer



EC2 Instances



AWS Global
Accelerator

お客様に代わり
自動的に防御

攻撃診断

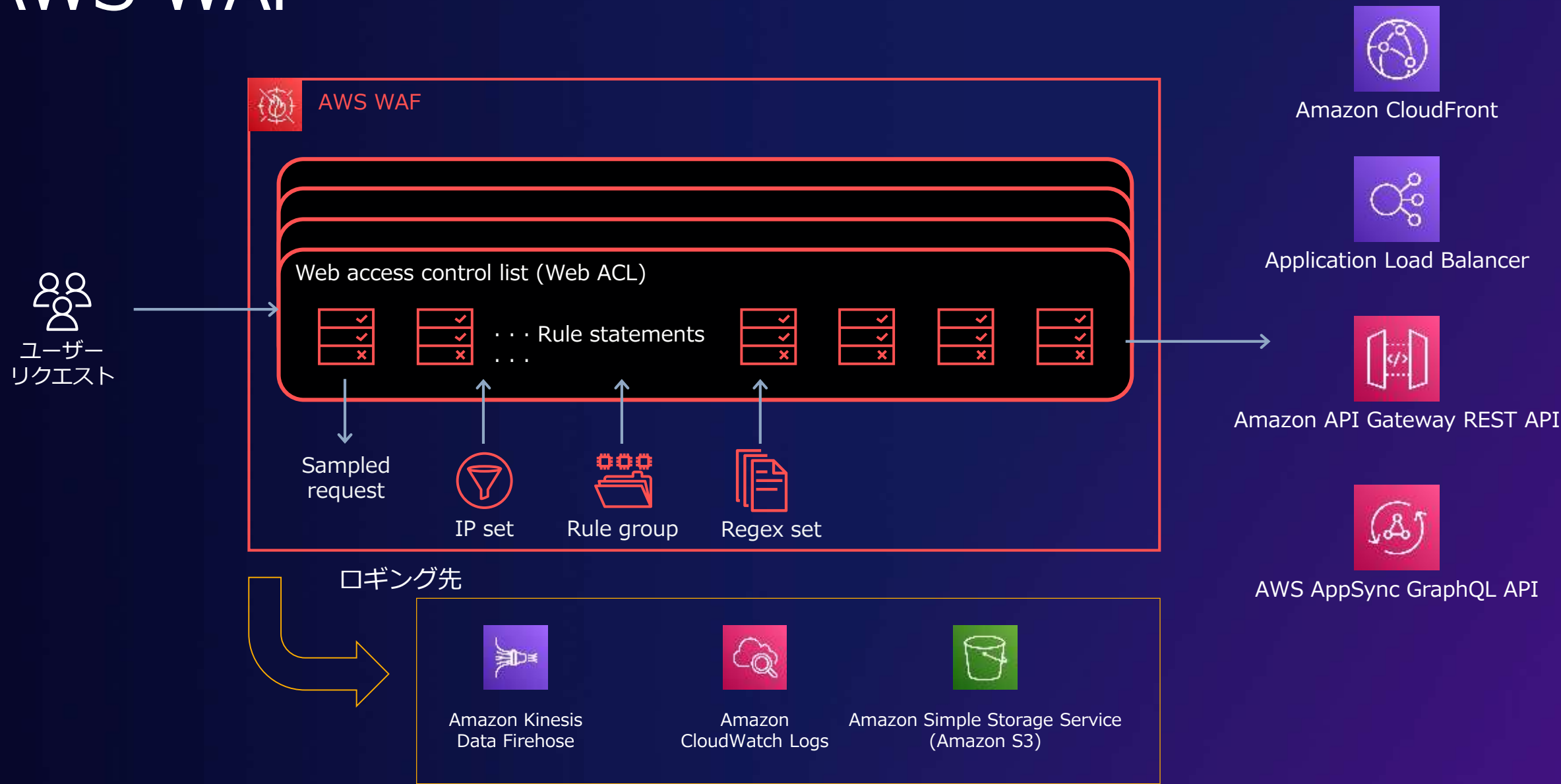
グローバル脅威
環境ダッシュ
ボード

スケーリングの
コスト保護

四半期ごとの
セキュリティレ
ビュー

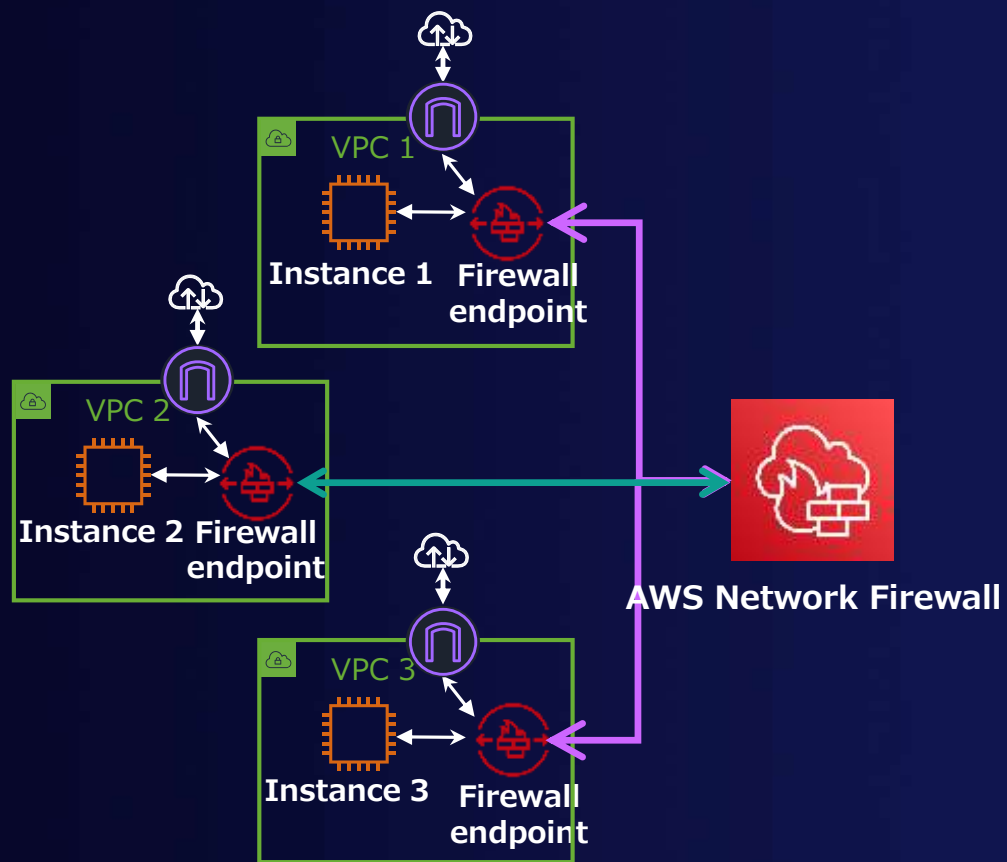


AWS WAF

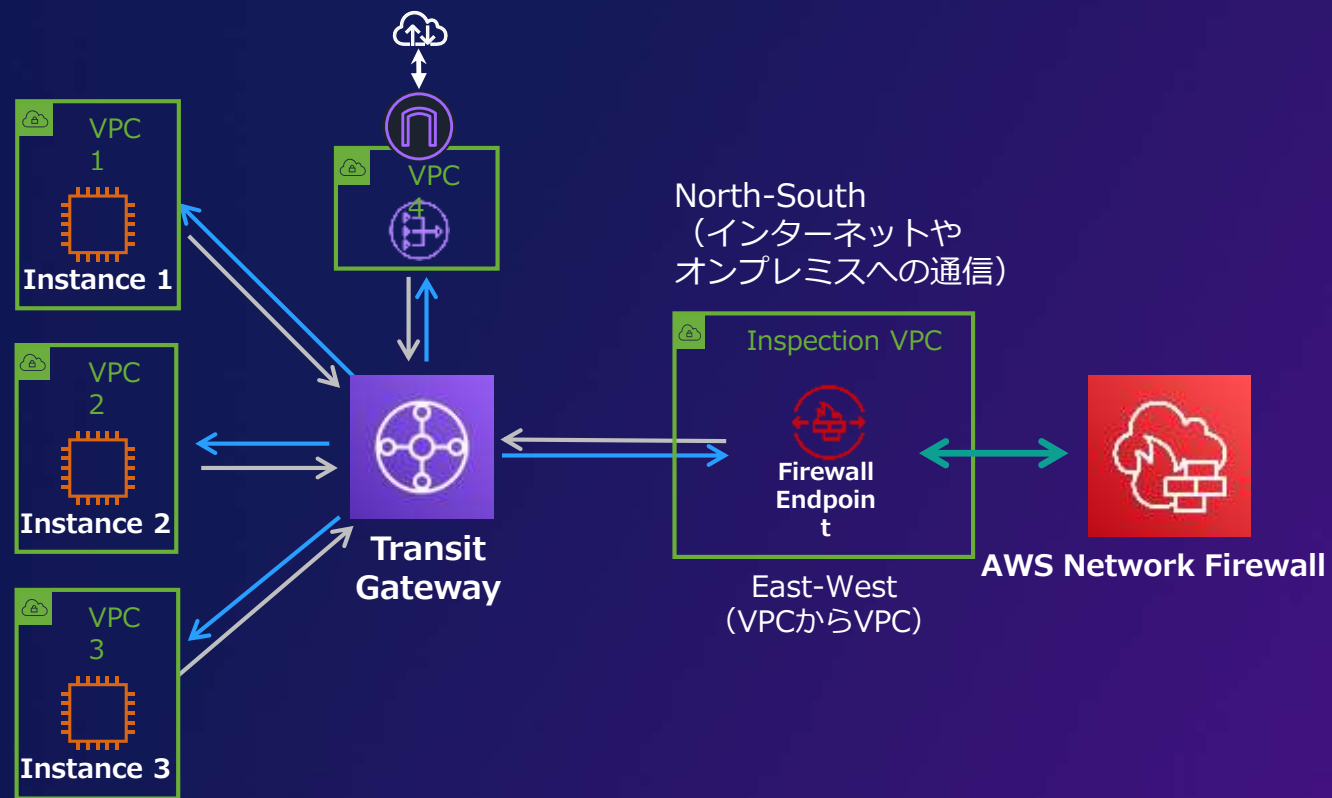


AWS Network Firewall

分散型セキュリティ検査



一元化されたセキュリティ検査



VPC フローログ

version account-id interface-id srcaddr dstaddr srcport dstport protocol packets bytes start end action log-status vpc-id
subnet-id instance-id tcp-flags type pkt-srcaddr pkt-dstaddr region az-id sublocation-type sublocation-id pkt-src-aws-
service pkt-dst-aws-service flow-direction traffic-path

5 123456789097 eni-044feef0 52.218.241.56 10.0.1.38 443 58460 6 19 7710 1634606470 1634606481 ACCEPT OK vpc-
0a19b648 subnet-094ee201 i-08bcbe49 19 IPv4 52.218.241.56 10.0.1.38 us-west-2 usw2-az2 - - S3 - ingress -

5 123456789097 eni-044feef0 2001:db2:1:f102::6 2001:db2:1:f101::f 0 0 58 10 1040 1634606496 1634606497 ACCEPT OK vpc-
0a19b648 subnet-094ee201 i-08bcbe49 0 IPv6 2001:db2:1:f102::6 2001:db2:1:f101::f us-west-2 usw2-az2 - - EC2 EC2 ingress -

Select log group(s)

Clear

flowLogs X

1 stats.sum(bytes).as bytesTransferred.by srcAddr, dstAddr

2 |.sort bytesTransferred.desc

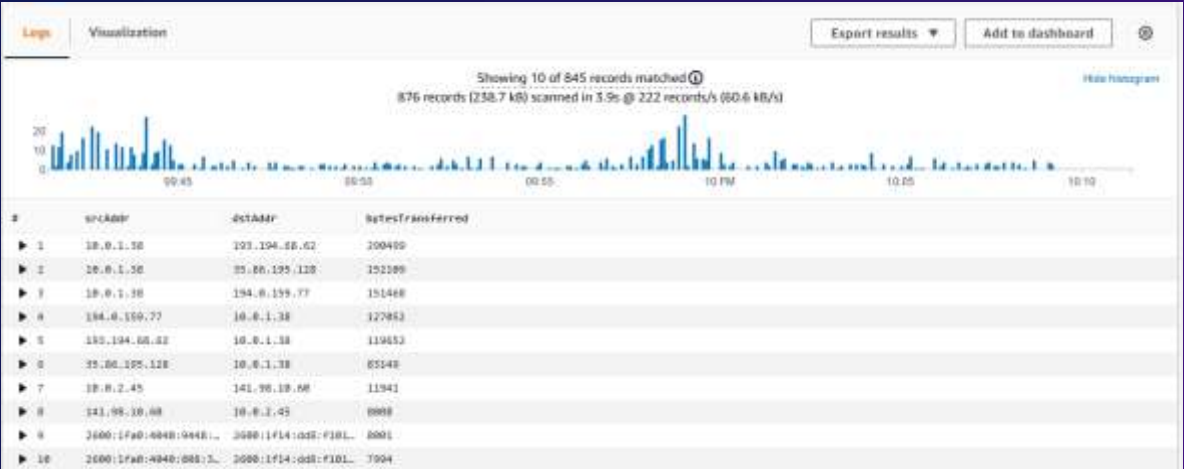
3 |.limit 10

Run query

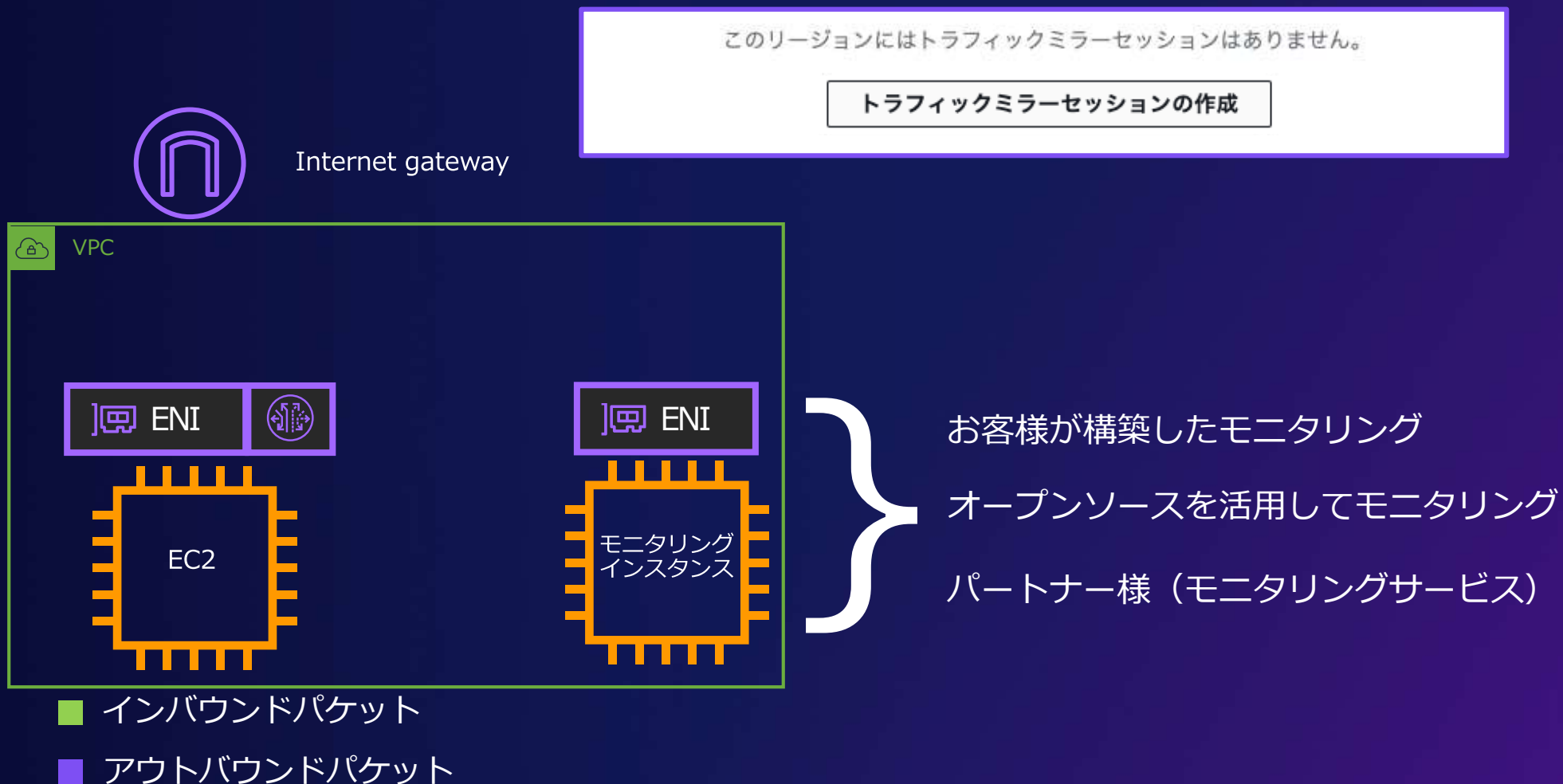
Save

History

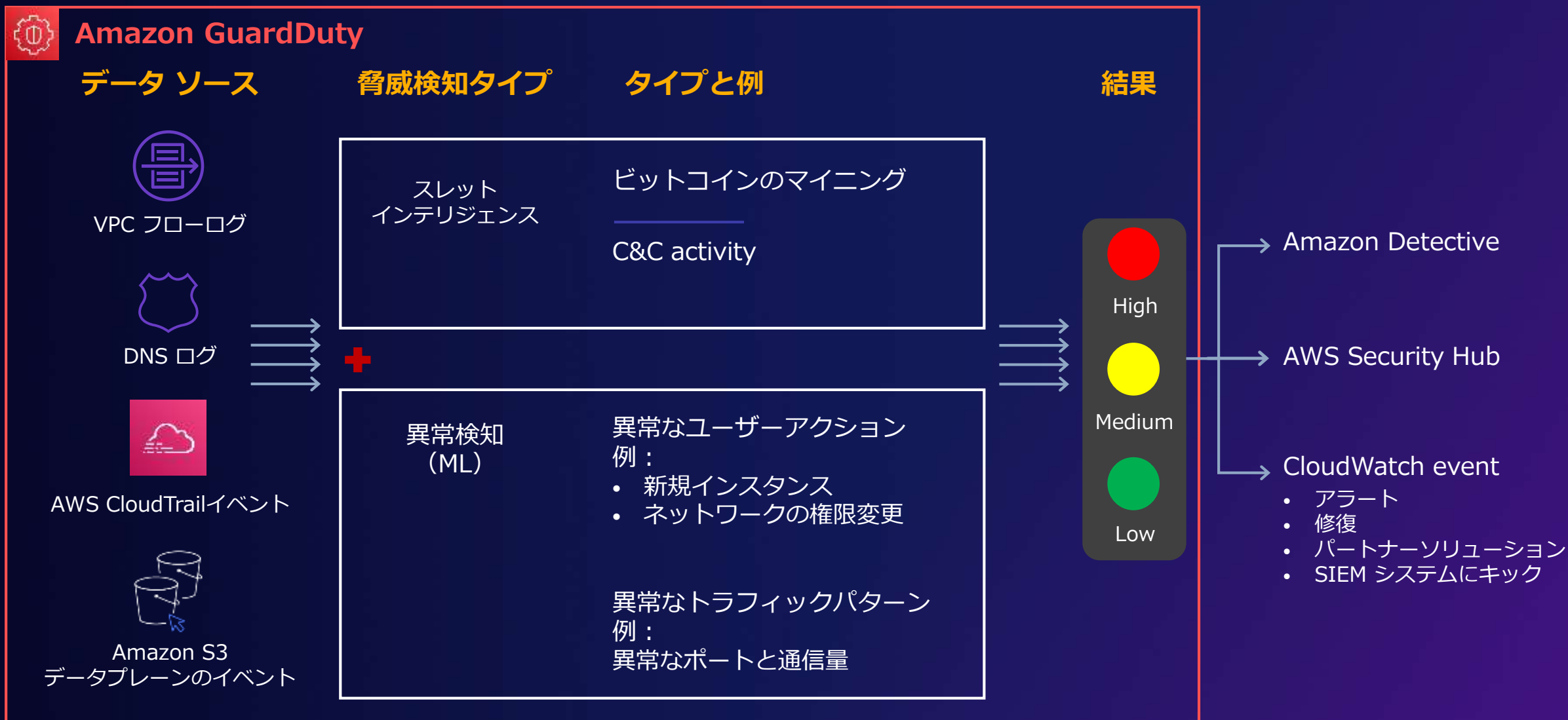
Queries are allowed to run for up to 15 minutes.



VPC トラフィックミラーリング



Amazon GuardDuty



ネットワークの モニタリング&ビジビリティ

VPC Network Access Analyzer

ネットワーク経路がアクセスポリシーに適しているかどうかを確認



ネットワークアクセス
スコープとしてネット
ワークアクセスポリ
シーを定義



解析してネットワーク
アクセスを評価



ネットワークの構成変
更が意図通りであるか
を自動的に検証



Services

Search for services, features, blogs, docs, [Option+S]



N. Virginia



☒ New VPC Experience
Tell us what you think

Network ACLs

Security Groups

▼ NETWORK ANALYSIS

Reachability Analyzer

Network Access Analyzer

▼ DNS FIREWALL

Rule Groups New

Domain Lists New

▼ NETWORK FIREWALL

Firewalls

Firewall Policies

Network Firewall Rule Groups

▼ VIRTUAL PRIVATE NETWORK (VPN)

Customer Gateways

Virtual Private Gateways

Site-to-Site VPN

VPC > Network Access Scopes > nis-0b4691382c4d5028f

Filter findings by category [Info](#)

This chart shows the number of occurrences of various resources in the findings. Select resource(s) to filter for findings containing the resource.



Findings (1/2) [Info](#)

Filter findings by resource types or specific resources present in the findings.

< 1 >

igw-0db9e65e51caa59ba (Web-IGW) - eni-0096ad03d76e70c75 (BizIntelligence)



Feedback English (US)

© 2021, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)



VPC Reachability Analyzer

到達可能かどうかの設定を検証



接続のトラブルシューティング
でネットワークのミスを特定



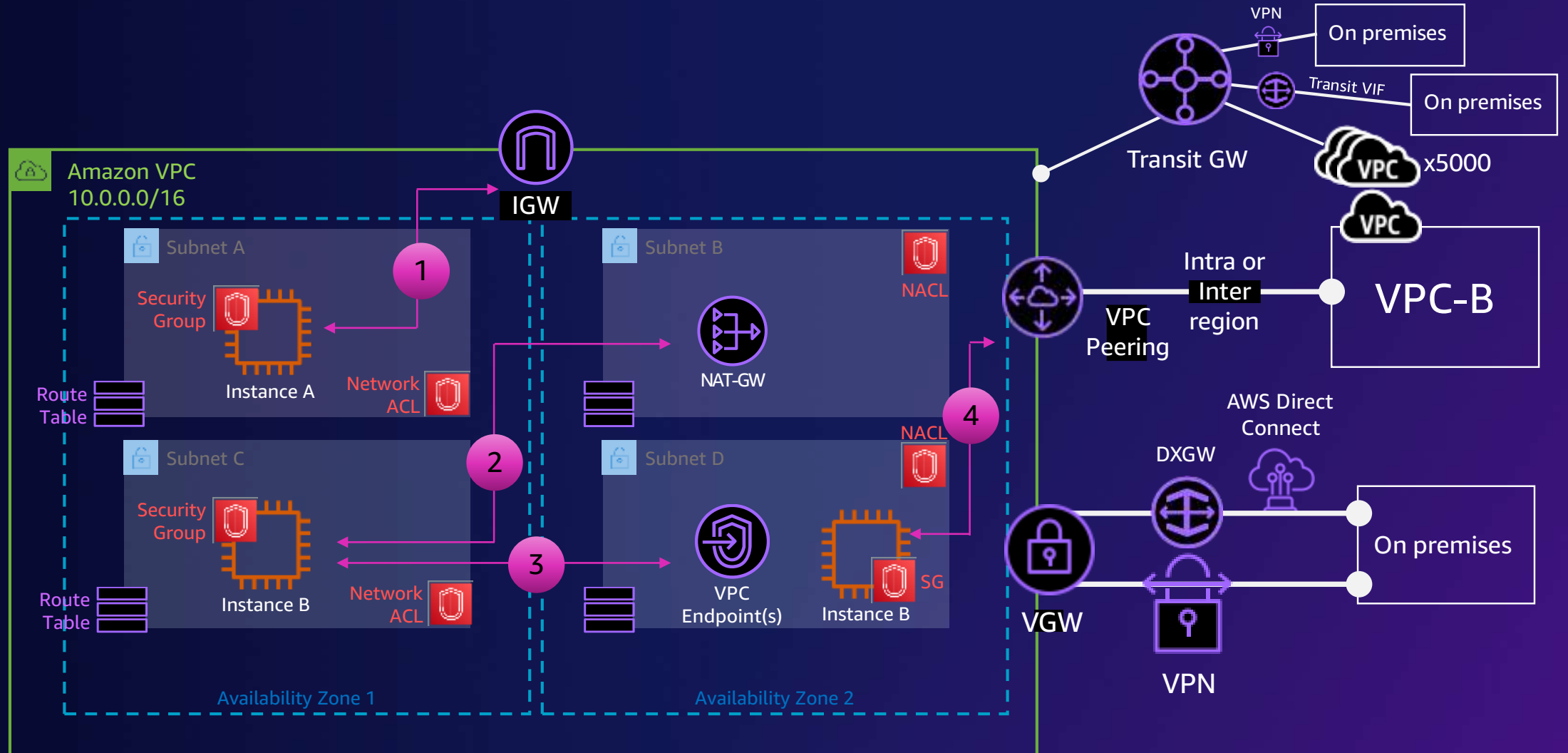
ネットワーク構成が意図した通
りかどうかを確認



ネットワークの構成変更在意図
の通りの検証を自動化

VPC Reachability Analyzer

ネットワーク到達可能性のトラブルシューティング



VPC Reachability Analyzer

ネットワーク到達可能性のトラブルシューティング

❌ Destination is not reachable. For more information, see the explanations below.

[Give us feedback](#)

Explanations

- Traffic cannot reach the internet through internet gateway igw-03cd57caea7c885fe because the source address is not paired with a public IP address. To add or edit an IPv4 public IP address to the source, you can use an [Elastic IP address](#).

▼ Details

```
{
  "explanationCode": "IGW_PUBLIC_IP_ASSOCIATION_FOR_EGRESS",
  "internetGateway": {
    "arn": "arn:aws:ec2:us-east-1:064153202663:internet-gateway/igw-03cd57caea7c885fe",
    "id": "igw-03cd57caea7c885fe"
  },
  "vpc": {
    "arn": "arn:aws:ec2:us-east-1:064153202663:vpc/vpc-0a74afe379e190c50",
    "id": "vpc-0a74afe379e190c50"
  }
}
```

- Internet gateway igw-03cd57caea7c885fe cannot accept inbound traffic from the public internet if the destination address is not the public IP address of a network interface in VPC vpc-0a74afe379e190c50. To add or edit an IPv4 public IP address to the destination, you can use an [Elastic IP address](#).

► Details

Path ID

nip-0f82a

Source

eni-0677

Analysis status

Completed

まとめ

まとめ

- Amazon VPCでIPv4, IPv6アドレスを割り当て、DNS64、NAT64を用いて、IPv6サービスとIPv4サービス間の通信を可能にできます。
- 必要に応じてAWS セキュリティサービス（AWS Shield, AWS WAF, AWS Network Firewall, Amazon GuardDuty）を活用できます。
- AWS PrivateLinkを活用してトラフィックをインターネットに経由せずに通信できます。Transit Gateway Connectを活用してSD-WANエッジをAWSに拡張でき、Transit Gatewayリージョン内ピアリングでネットワーク構成を簡素化できます。
- VPC Network Access Analyzerでネットワークがアクセス要件を満たすかどうかを確認でき、VPC Reachability Analyzerを利用してVPC内の接続テストとトラブルシューティングができます。

Thank you!

