

vFORUM **2019**

HC124

徹底解説！

VMware Cloud on AWS

ネットワーキング & デザイン

ヴァイエムウェア株式会社

ソリューションビジネス本部

クラウドソリューション技術統括部

リードクラウドスペシャリスト 黒岩 宣隆

Make  
Your  
Mark



# 免責事項

- このセッションには、現在開発中の製品/サービスの機能が含まれている場合があります。
- 新しいテクノロジーに関するこのセッションおよび概要は、VMware が市販の製品/サービスにこれらの機能を搭載することを約束するものではありません。
- 機能は変更される場合があるため、いかなる種類の契約書、受注書、または販売契約書に記述してはなりません。
- 技術的な問題および市場の需要により、最終的に出荷される製品/サービスでは機能が変わる場合があります。
- ここで検討されているまたは提示されている新しいテクノロジーまたは機能の価格およびパッケージは、決定されたものではありません。

# Agenda

## VMware Cloud on AWS 概要

### ネットワーク接続詳細

- オンプレミスと VMware Cloud on AWS 間の接続
- AWS と VMware Cloud on AWS 間の接続
- 複数 SDDC または複数 AWS 環境間の接続

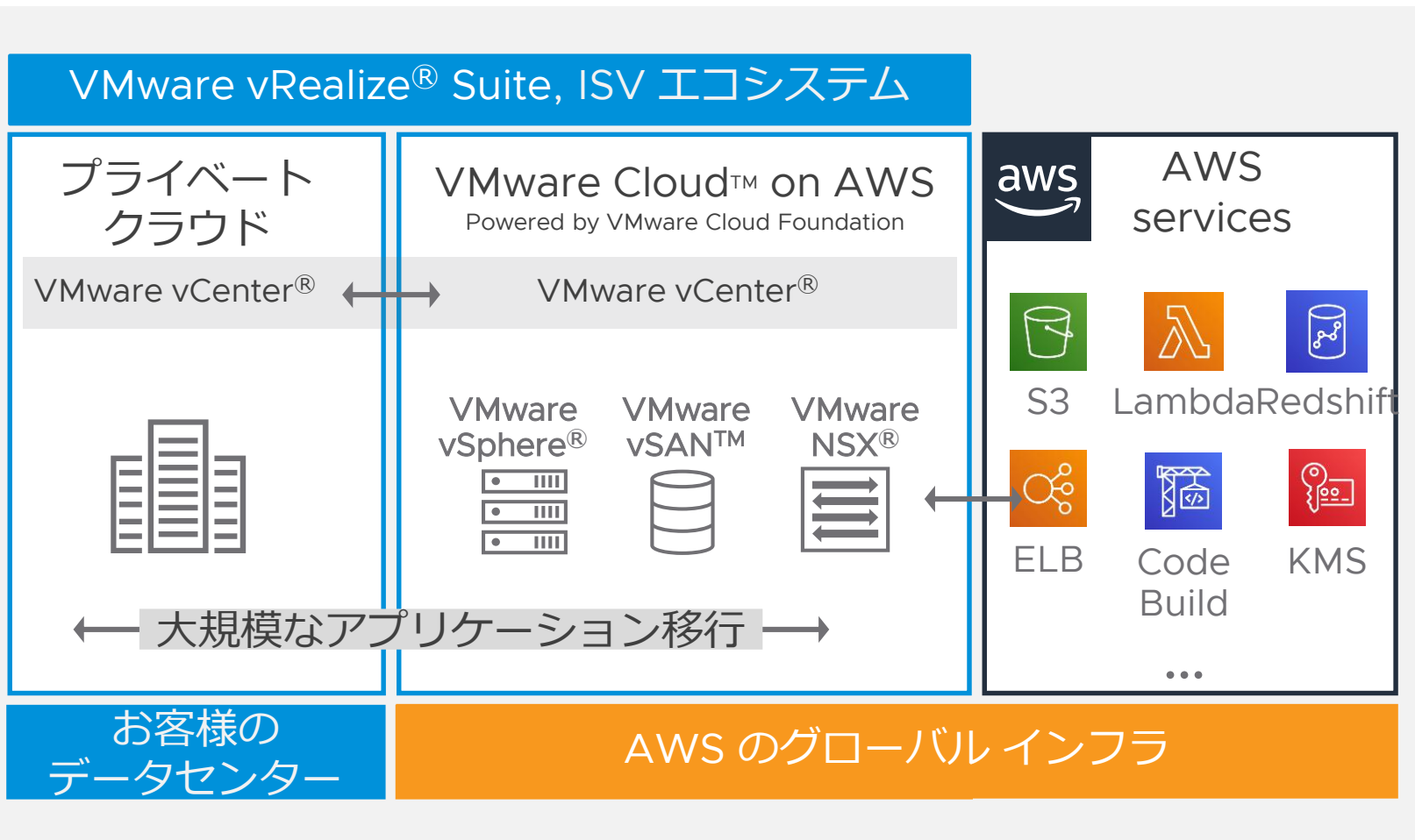
### ネットワークサービス詳細

- North-South ファイアウォール
- East-West ファイアウォール
- ロードバランサ on VMware Cloud on AWS
- VMware Cloud on AWS における AWS ネットワークサービスとの連携

# VMware Cloud on AWS 概要

# VMware Cloud on AWS

世界で最もパワフルなクラウドテクノロジーの共演



シンプルで高品質な  
サービスを VMware が提供

プライベートクラウドと  
一貫性のある運用

シンプルなクラウド移行

AWS のネイティブ  
サービスへの直接アクセス

# VMware Cloud on AWS コンソール

## ネットワークとセキュリティ

VMware Cloud on AWS

SDDC サブスクリプション アクティビティ ログ ツール デベロッパー センター

< すべての SDDC

VMC-SDDC TOKYO-SDDC Asia Pacific (Tokyo) | ap-northeast-1a

サマリ ネットワークとセキュリティ アドオン メンテナンス トラブルシューティング 設定 サポート

概要

ネットワーク

セグメント

> VPN

NAT

セキュリティ

ゲートウェイ ファイアウォール

分散ファイアウォール

インベントリ

グループ

サービス

ツール

IPFIX

ポート ミラーリング

システム

DNS

DHCP

パブリック IP アドレス

Direct Connect

接続された VPC

概要

SDDC

VPN のパブリック IP アドレス: 13.127.0.127

管理ゲートウェイ

vCenter NSX Server

アプライアンスのサブネット: 10.2.192.0/18

インフラストラクチャのサブネット: 10.2.0.0/16

15 ゲートウェイのファイアウォール ルール, 55 個のグループ

インターネット

1 個の VPN がインターネット経由で利用可能

Direct Connect は設定されていません

オンプレミス

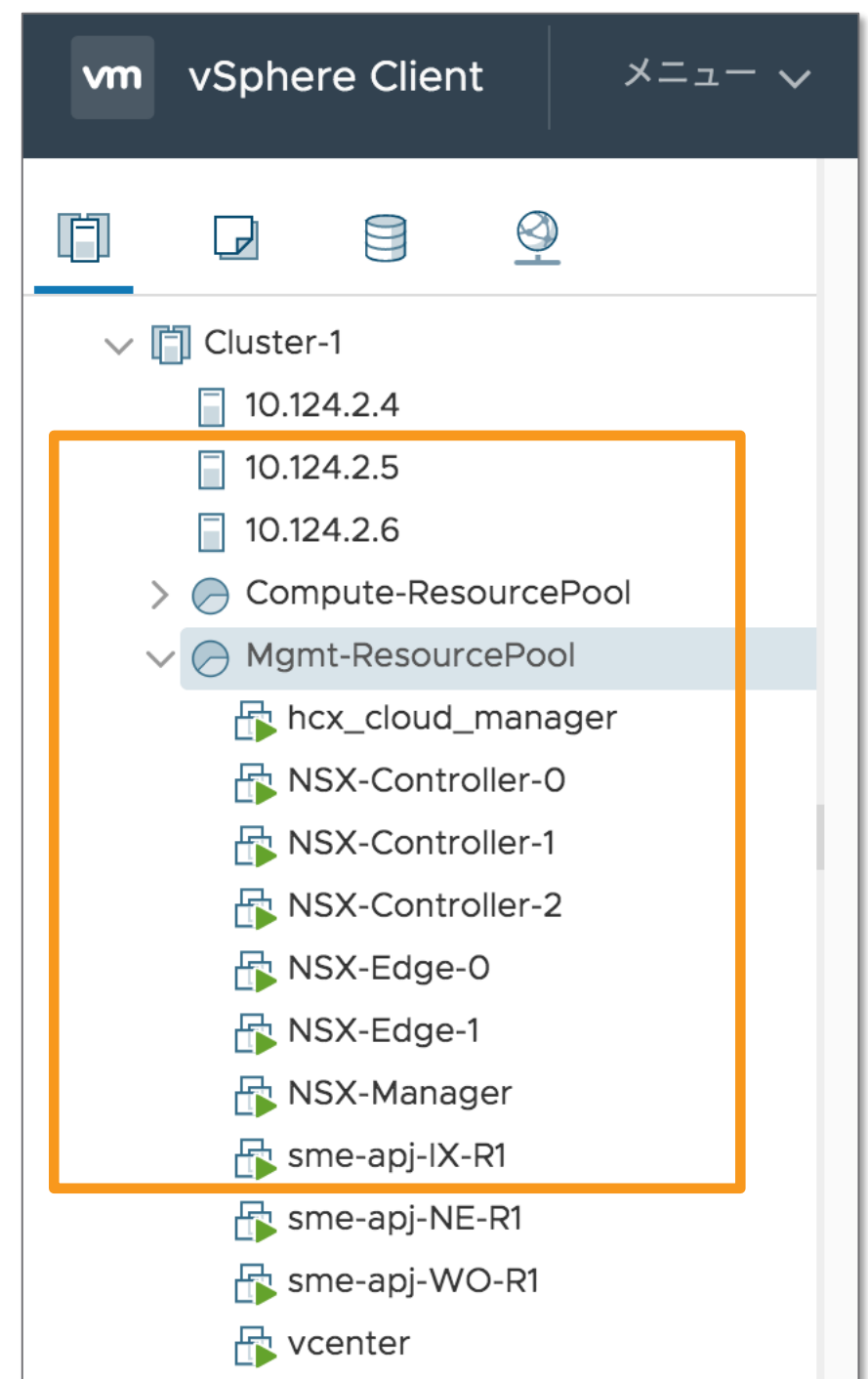
ネットワークに関する設定は  
全て VMware Cloud on AWS  
コンソールで設定

- セグメント
- VPN
- NAT
- ファイアウォール
- トラブルシューティングツール
- DNS, DHCP
- パブリック IP
- Direct Connect
- Native AWS VPC 関連設定

# vSphere Client

ネットワーク関連仮想マシンは全て Mgmt-ResourcePool に配置


- NSX Manager
- NSX Edge（冗長構成：アクティブ - スタンバイで 2 VM）
- NSX Controller（3 VM）
- HCX 関連仮想マシン



# 豊富なネットワーク接続オプション


要件に合わせて柔軟に選択可能

## 接続方式



暗号化されたセキュアな L3 接続  
(ポリシーベース/ルートベース)

インターネット / IPsec VPN



オンプレミス - SDDC 間の  
高速プライベートネットワーク  
接続


AWS Direct Connect (DX)

## L2 延伸方式



暗号化されたセキュアな  
L2 ネットワーク延伸

L2 VPN



オンプレミス - SDDC 間の  
VM 移行、L2 延伸、  
WAN 最適化

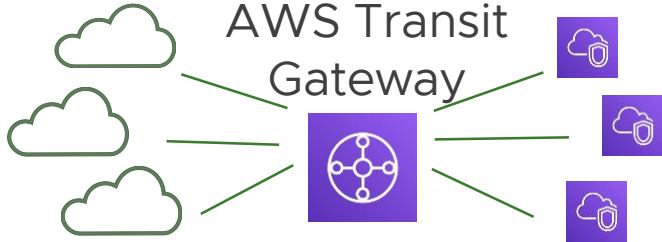
Hybrid Cloud Extension (HCX)

## Native AWS との接続



同じ AZ の SDDC と AWS VPC  
間の高速かつ低遅延の接続

VMware Cloud ENI

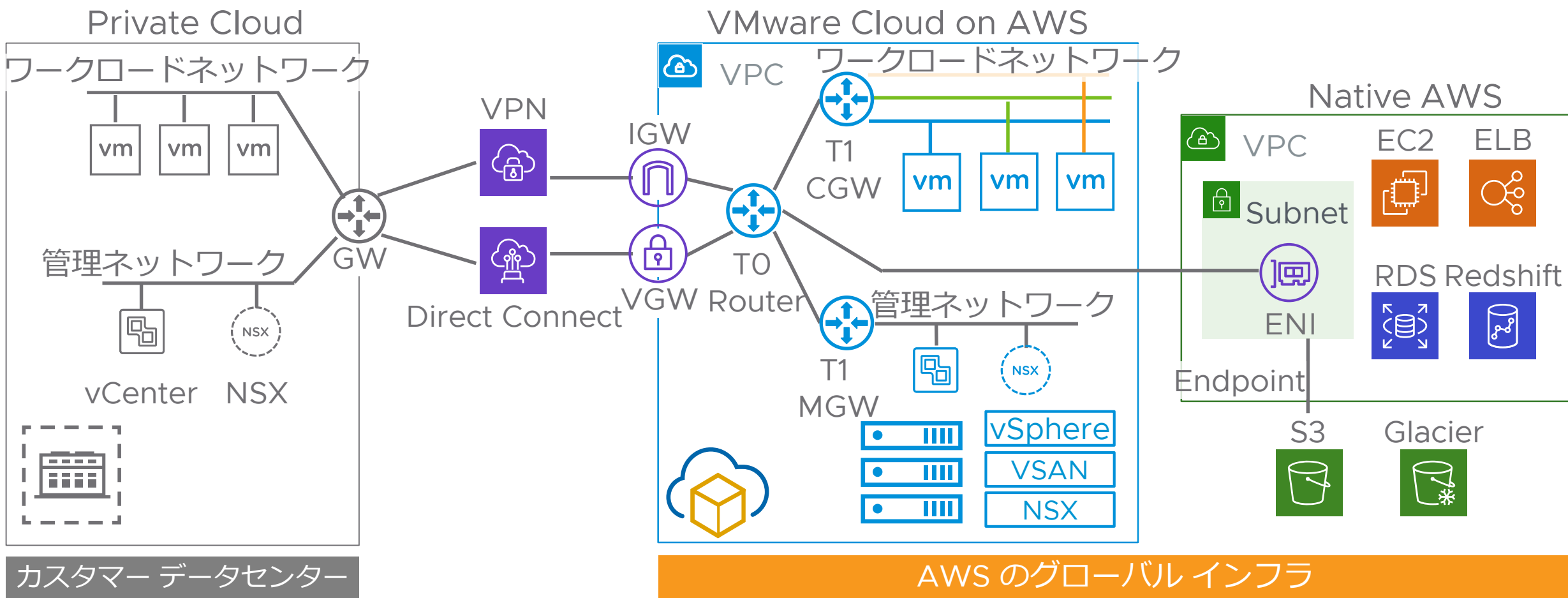


複数の SDDC および  
AWS VPC をスター形に接続

Transit Gateway (TGW)



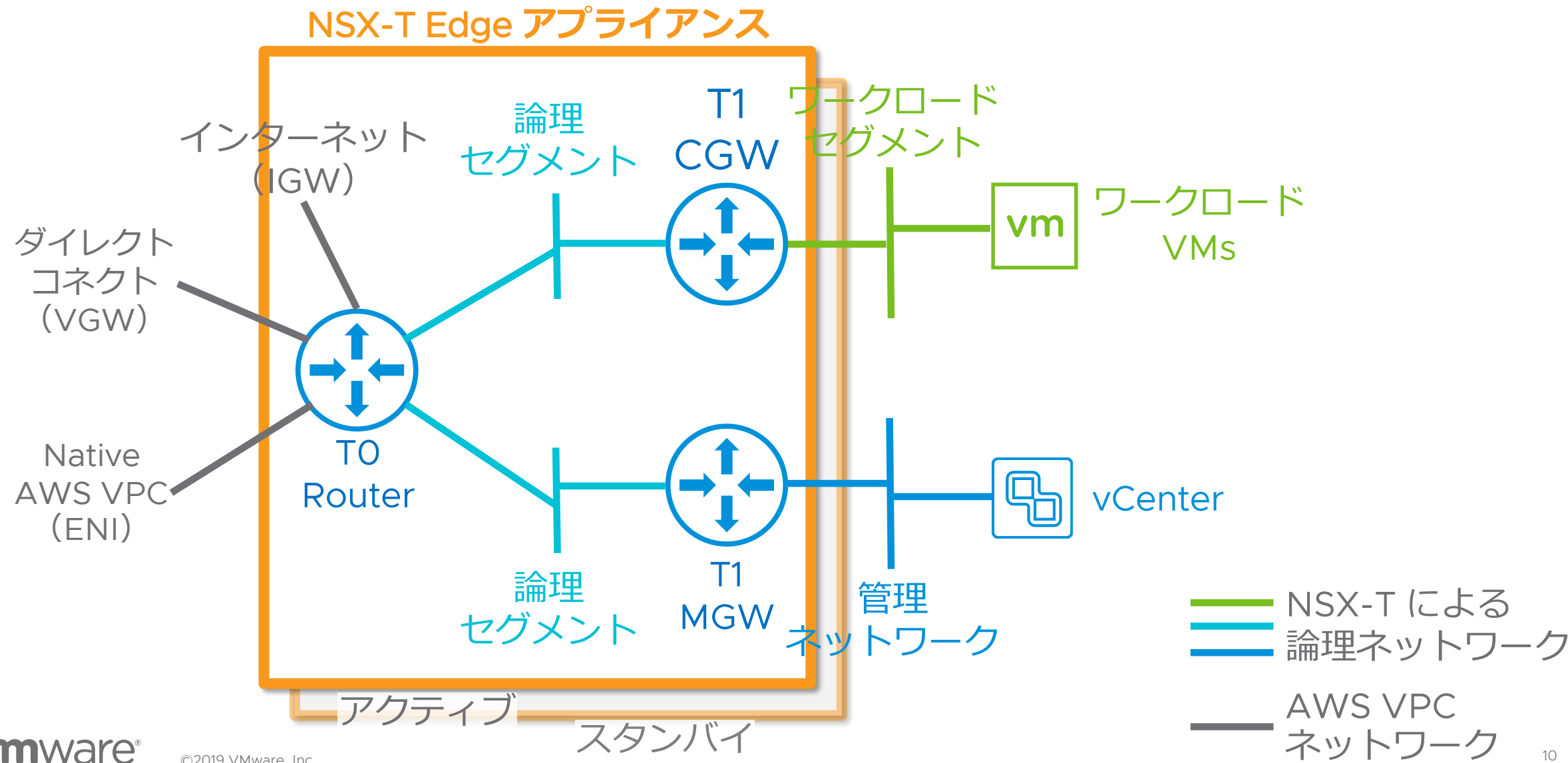
# VMware Cloud on AWS ネットワーク構成概要



# ネットワーク接続詳細

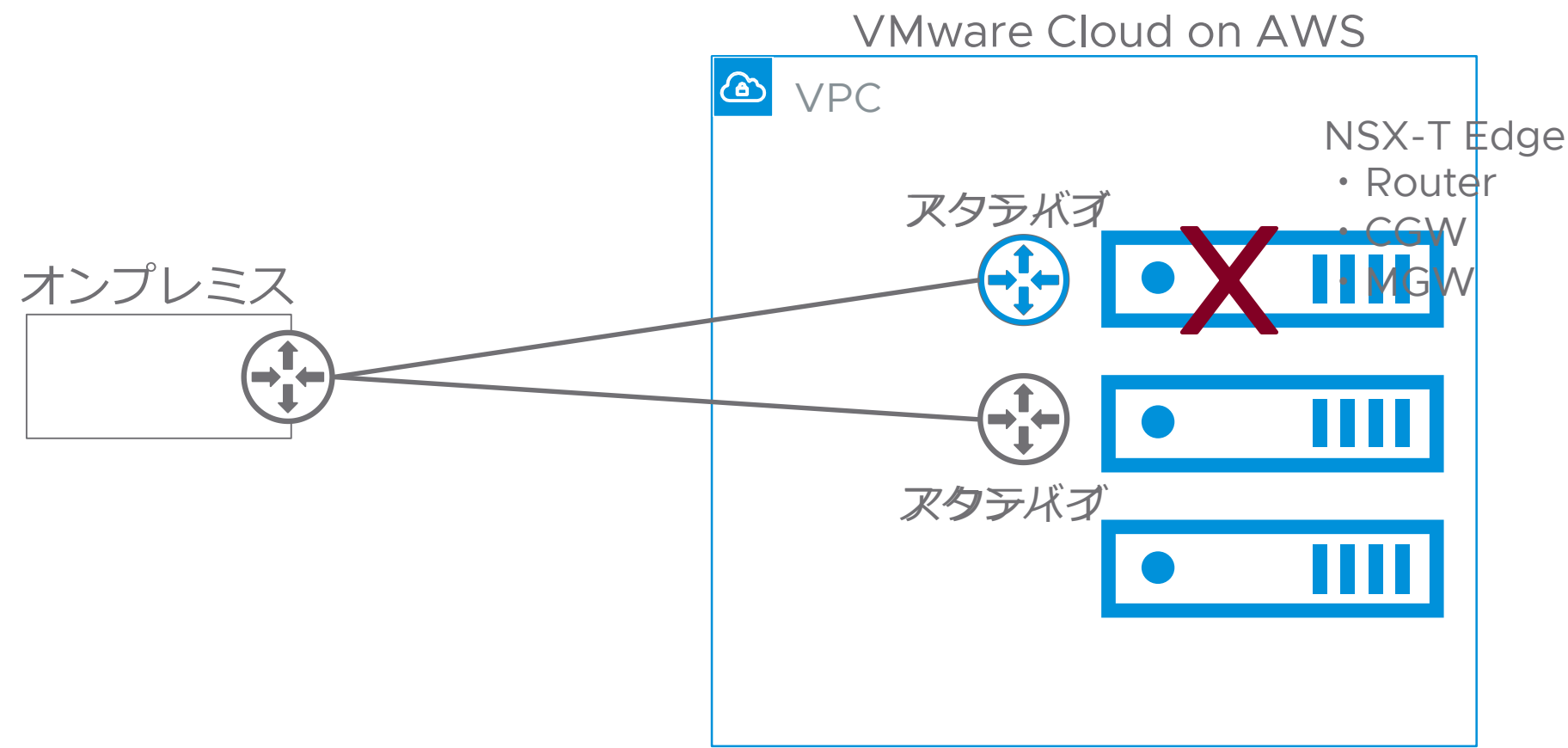
オンプレミスと VMware Cloud on AWS 間の接続

# VMware Cloud on AWS の Edge インターフェイス



# Edge のフェイルオーバー

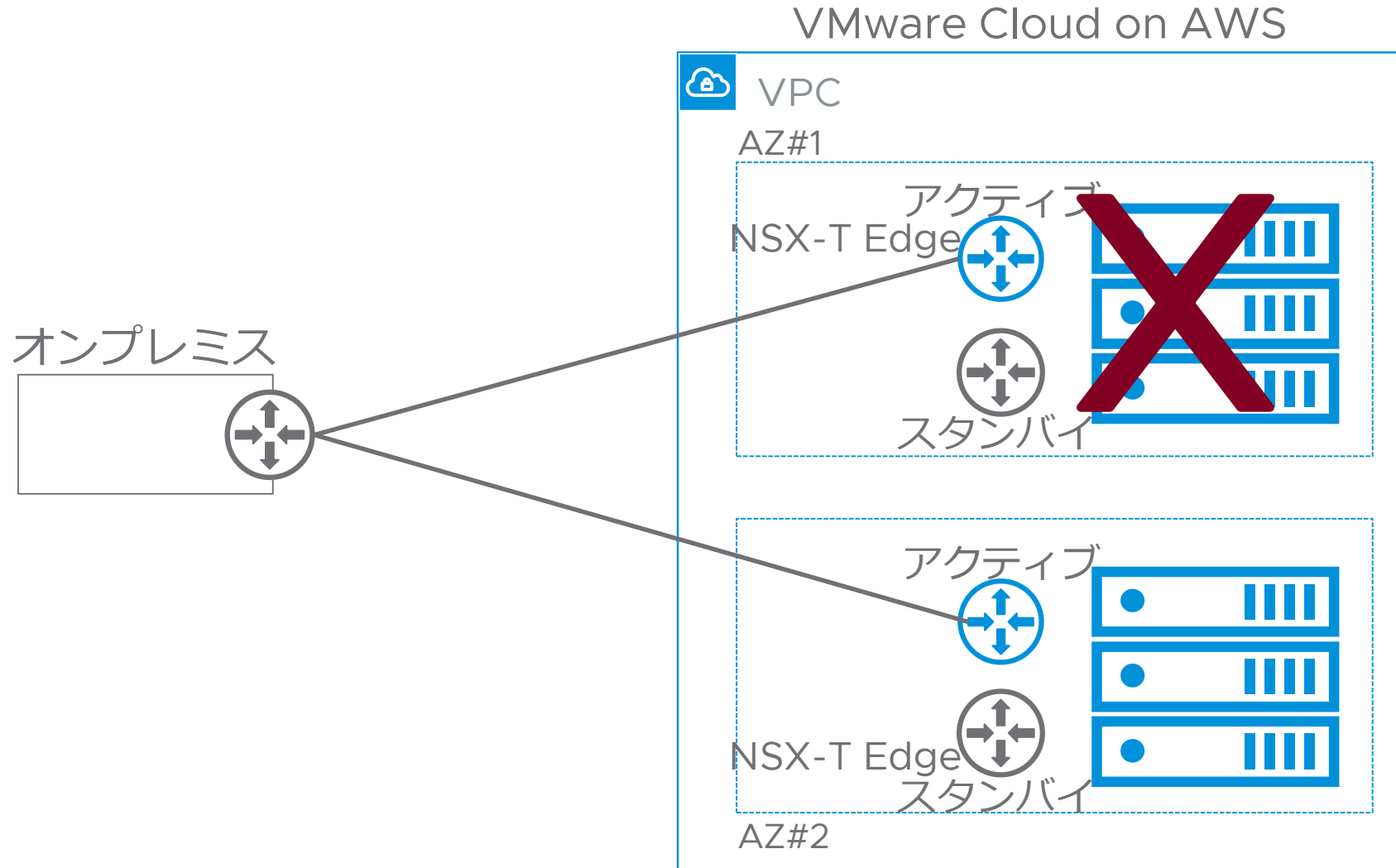
L3VPN、Direct Connect、L2 延伸のフェイルオーバー



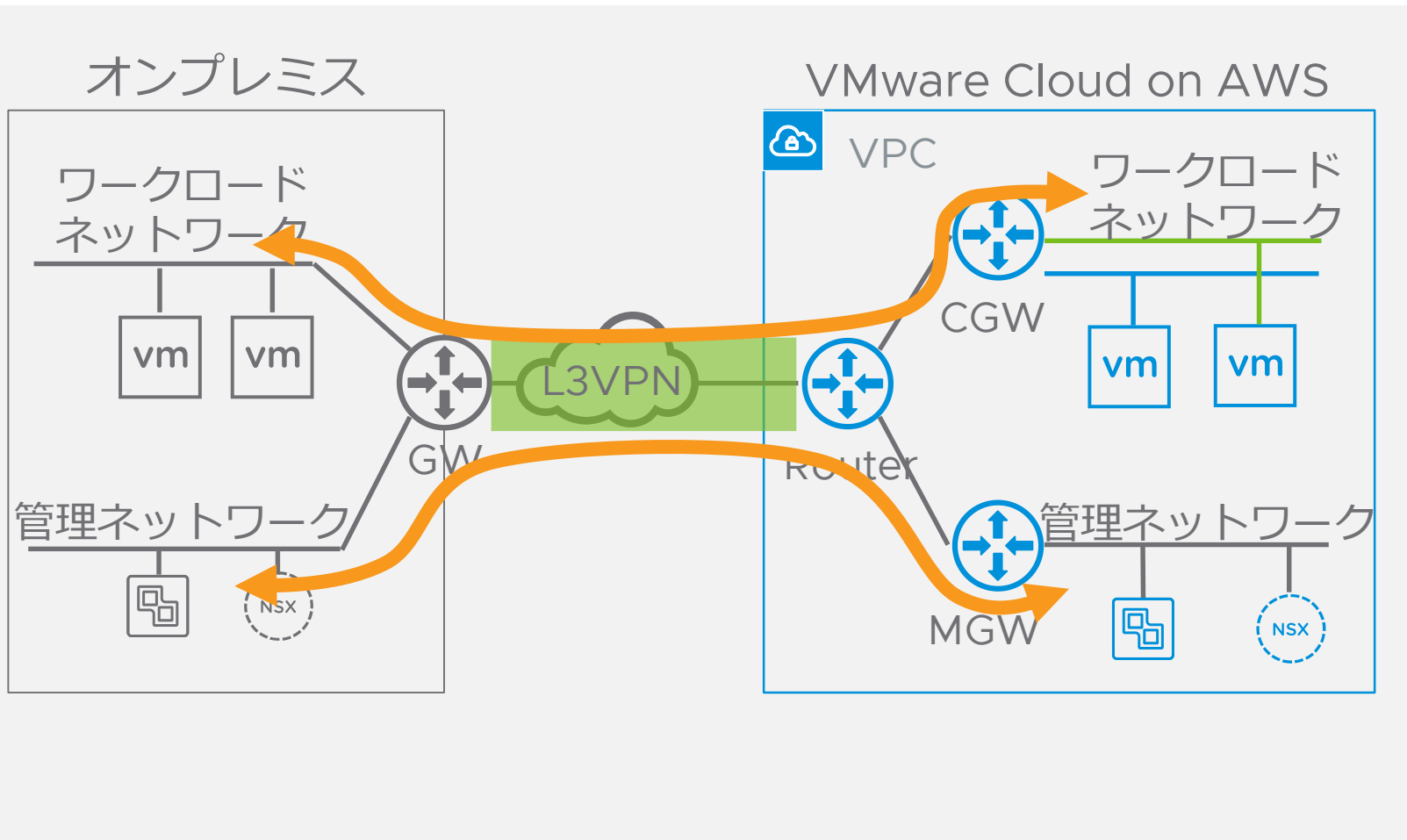


# Stretched Cluster 構成時の Edge のフェイルオーバー

## L3VPN、Direct Connect、L2 延伸のフェイルオーバー



# VMware Cloud on AWS とオンプレミスを L3VPN で接続



## 2 種類の VPN

- ルートベース
- ポリシーベース

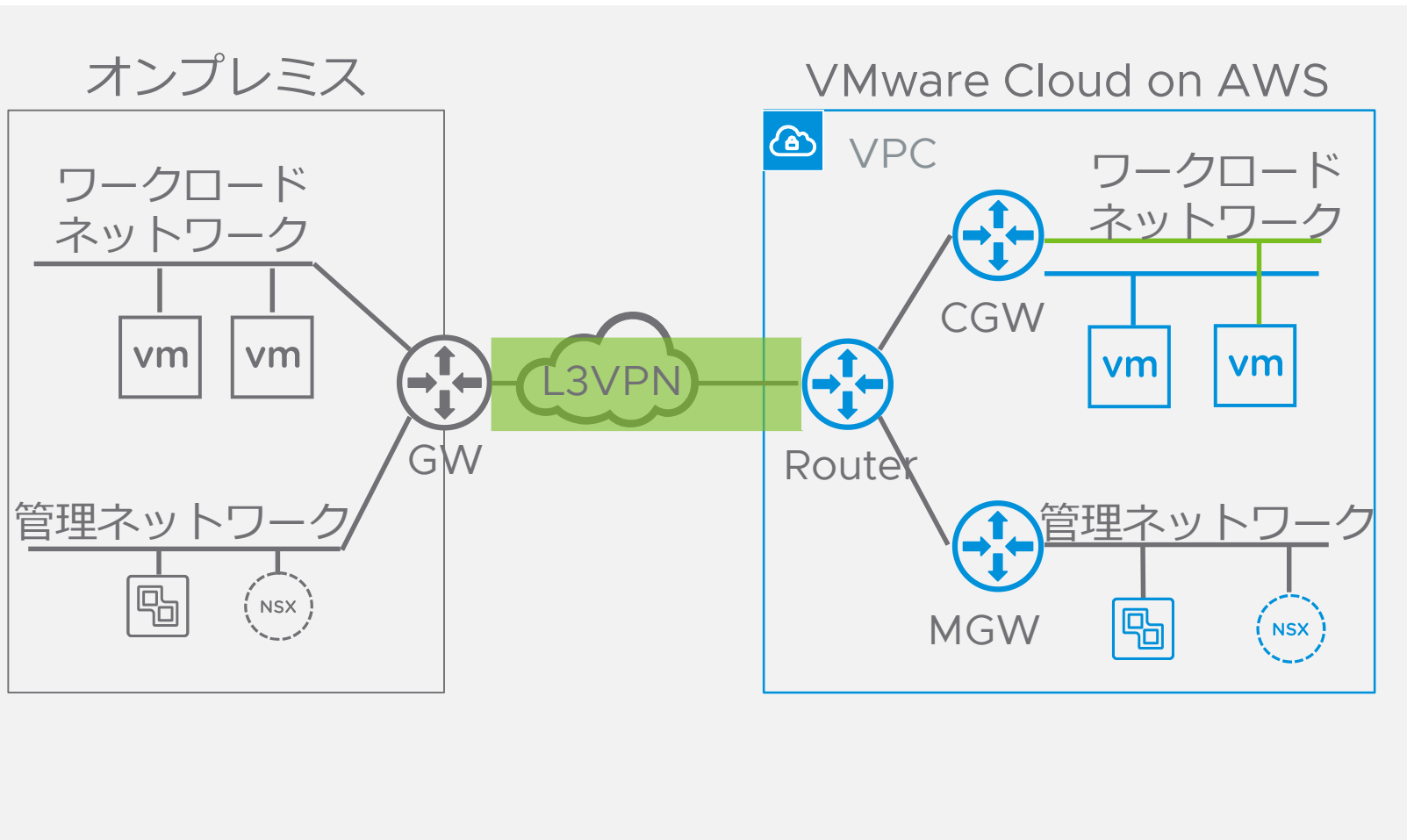
## ルートベース

- オンプレミス側と VMware Cloud on AWS 側のルート情報を BGP により交換
- 動的なルーティングが可能

## ポリシーベース

- 定義済みセグメントに対してルーティングが可能

# VMware Cloud on AWS とオンプレミスを L3VPN で接続（続き）



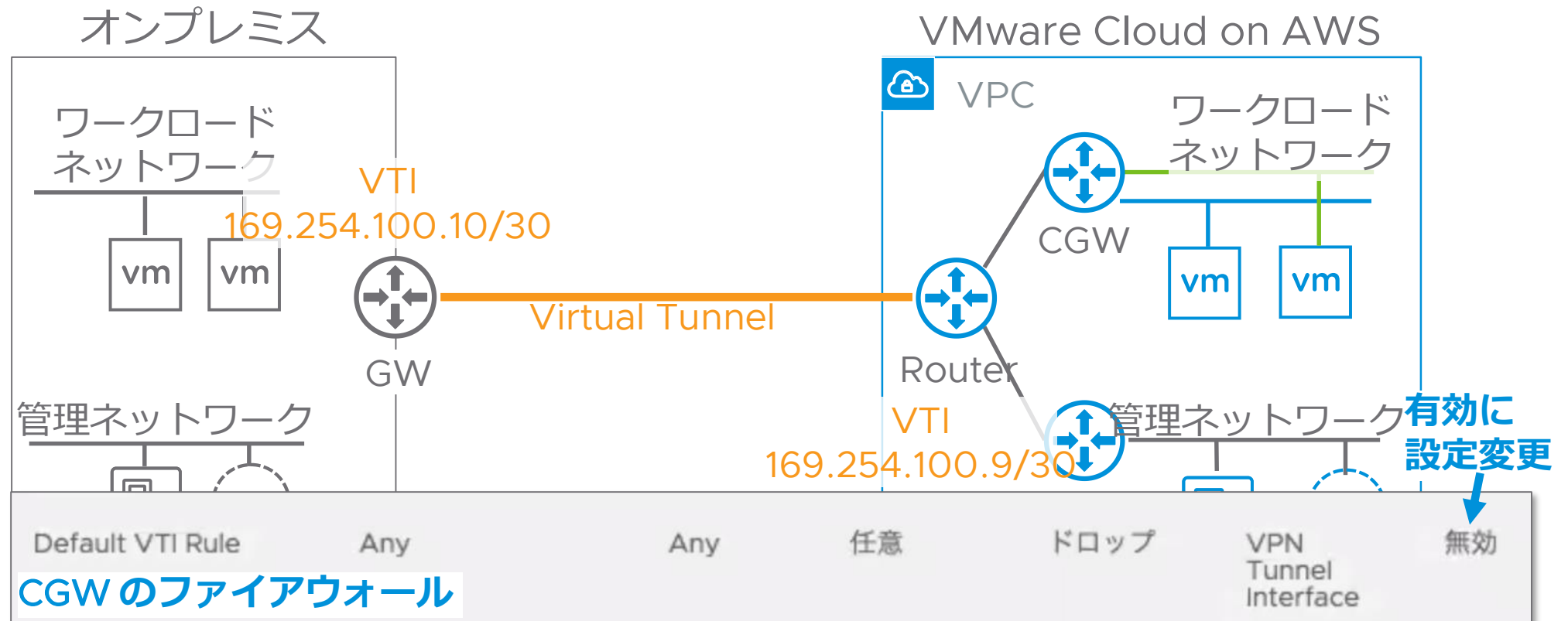
最大 16 VPN（両者合計）

インターネットまたは  
ダイレクトコネクト経由

オンプレミスの1つの Public IP  
に対して1つの L3VPN が接続  
可能

# ルートベース IPsec VPN 詳細

## Virtual Tunnel とファイアウォール





# ルートベース IPsec VPN 詳細

BGP によるルート情報の学習

オンプレミス

ワークロード

## Routes - route VPN

アドバタイズされたルート

学習済みルート

合計: 1

オンプレミスのフィルタされたセグメントを学習

ネットワーク	ネクスト ホップ
10.2.0.0/16	169.254.100.10
10.101.10.0/24	169.254.100.10

## Routes - route VPN

アドバタイズされたルート

学習済みルート

VMware Cloud on AWS のワークロード、管理セグメント全てをアドバタイズ

ネットワーク

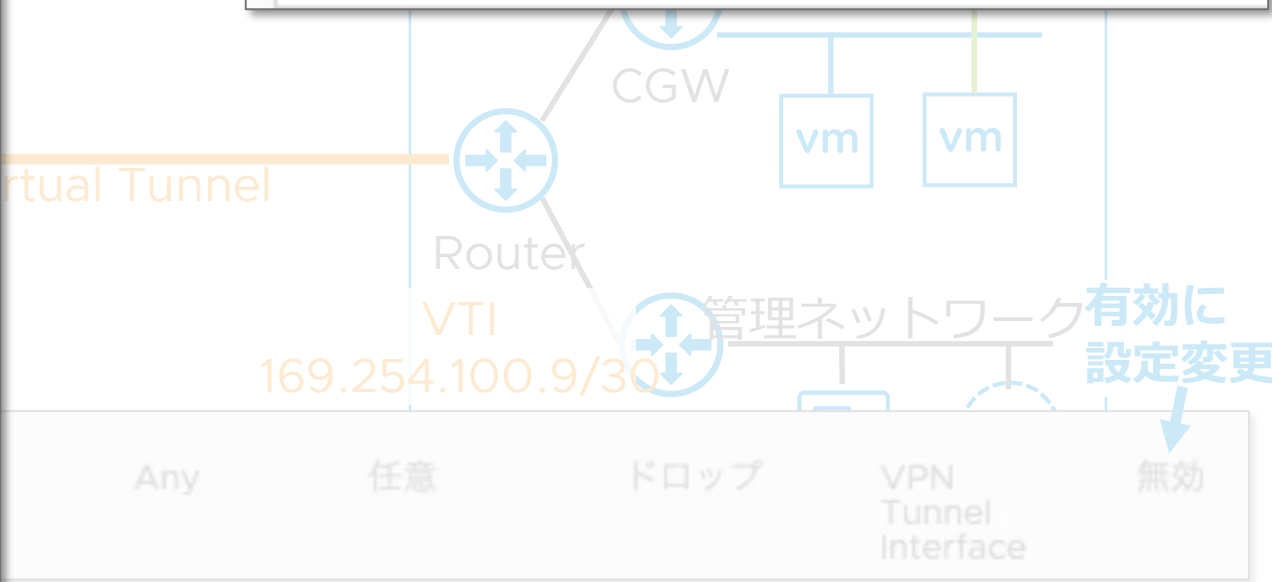
ネクスト ホップ

10.4.0.0/16

169.254.100.9

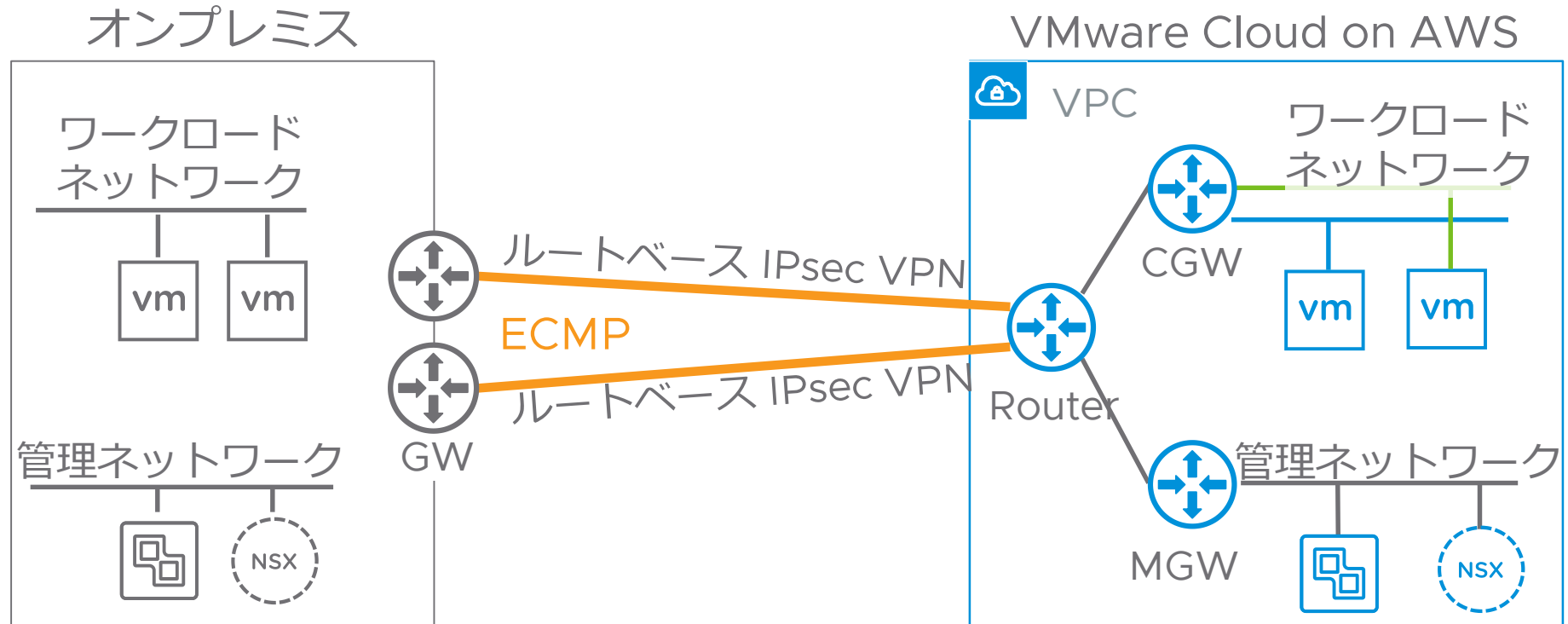
10.10.20.0/24

169.254.100.9

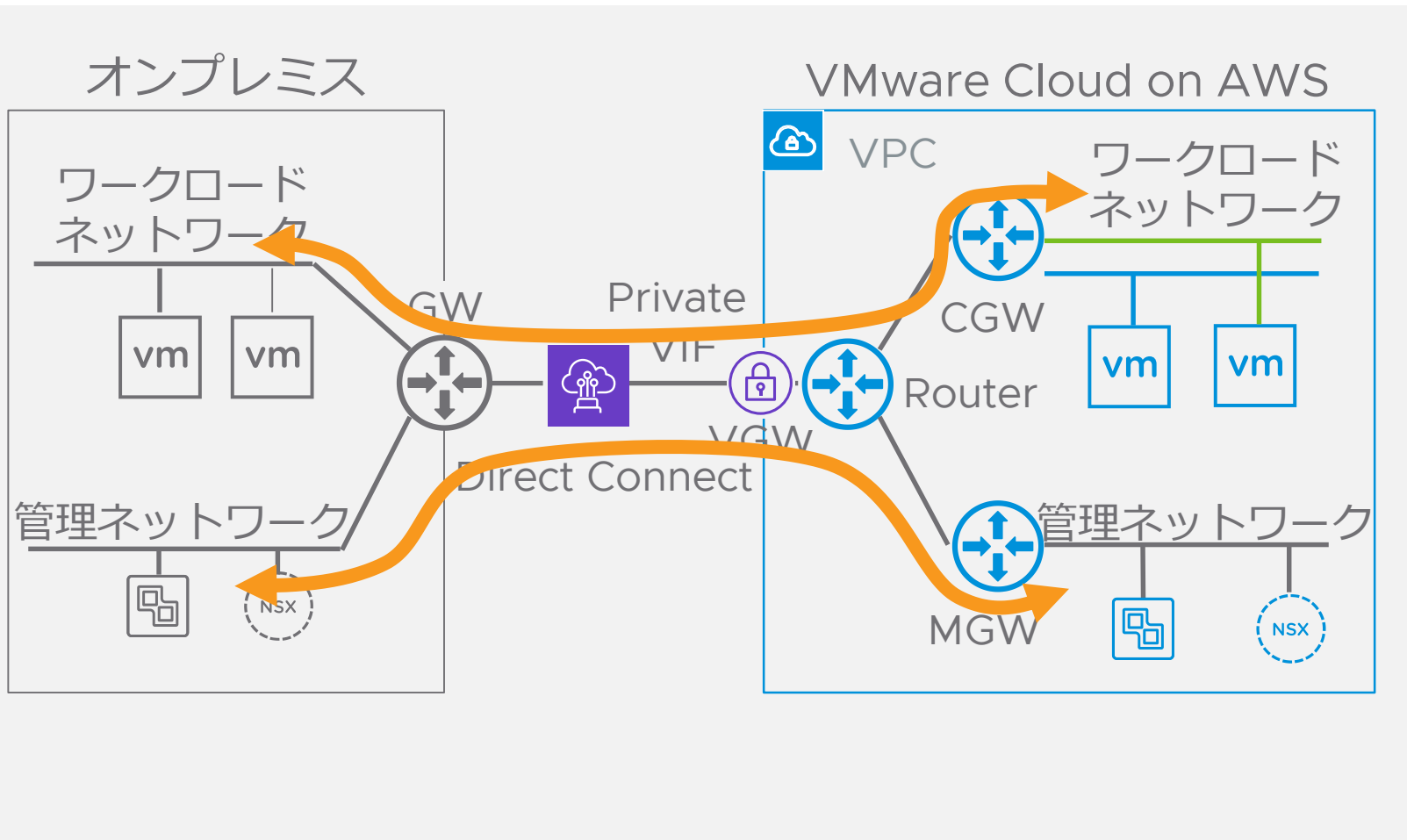


# ルートベース IPsec VPN 詳細

ECMP による広帯域の確保と高い可用性



# VMware Cloud on AWS とオンプレミスをダイレクトコネクで接続



ユーザー契約の AWS Direct Connect を利用し、VMware Cloud on AWS へ接続が可能

- Private VIF
- Public VIF (VPN 必須)

## 構成

- アクティブ - アクティブ / LAG
- アクティブ - スタンバイ
- アクティブ - スタンバイ (IPsec VPN)
- 1つの Private VIF で 16 CIDR をアドバータイズ可能 (ソフトリミット)
- 1つの Private VIF で 100 CIDR を学習可能

ダイ  
コ

## AWS マネージメントコンソール


## ダイレクトコネクトの Private

Enter the name of your virtual interface. If you're creating a virtual interface for another account, you'll also need to enter the account name. [Get Started Guide](#).

Virtual Interface Name	VIN-DXC-RCE05-E
------------------------	-----------------

## Another AWS Account を設定

Virtual Interface Owner ☐ My AWS Account ☒ Another AWS Account

Account ID 7 

## VMware Cloud on AWS の AWS アカウントを入力



# ダイレクトコネクト詳細

## BGP によるルート情報の共有

Virtual Interface Name	Virtual Interface ID	Direct Connect ID	MTU	Local Ip	Remote Ip	Remote ASN	State	BGP Status
VIF	dxvif-fh0k4g6f	dxcon-fgvrh42x	1500	169.254.255.2	169.254.255.1	64661	● Attached	● Up

### Advertised BGP Routes

10.33.1.0/26

10.33.1.128/25

192.168.1.0/24

10.33.0.0/24

10.33.2.0/24

### Learned BGP Routes

192.168.0.0/16

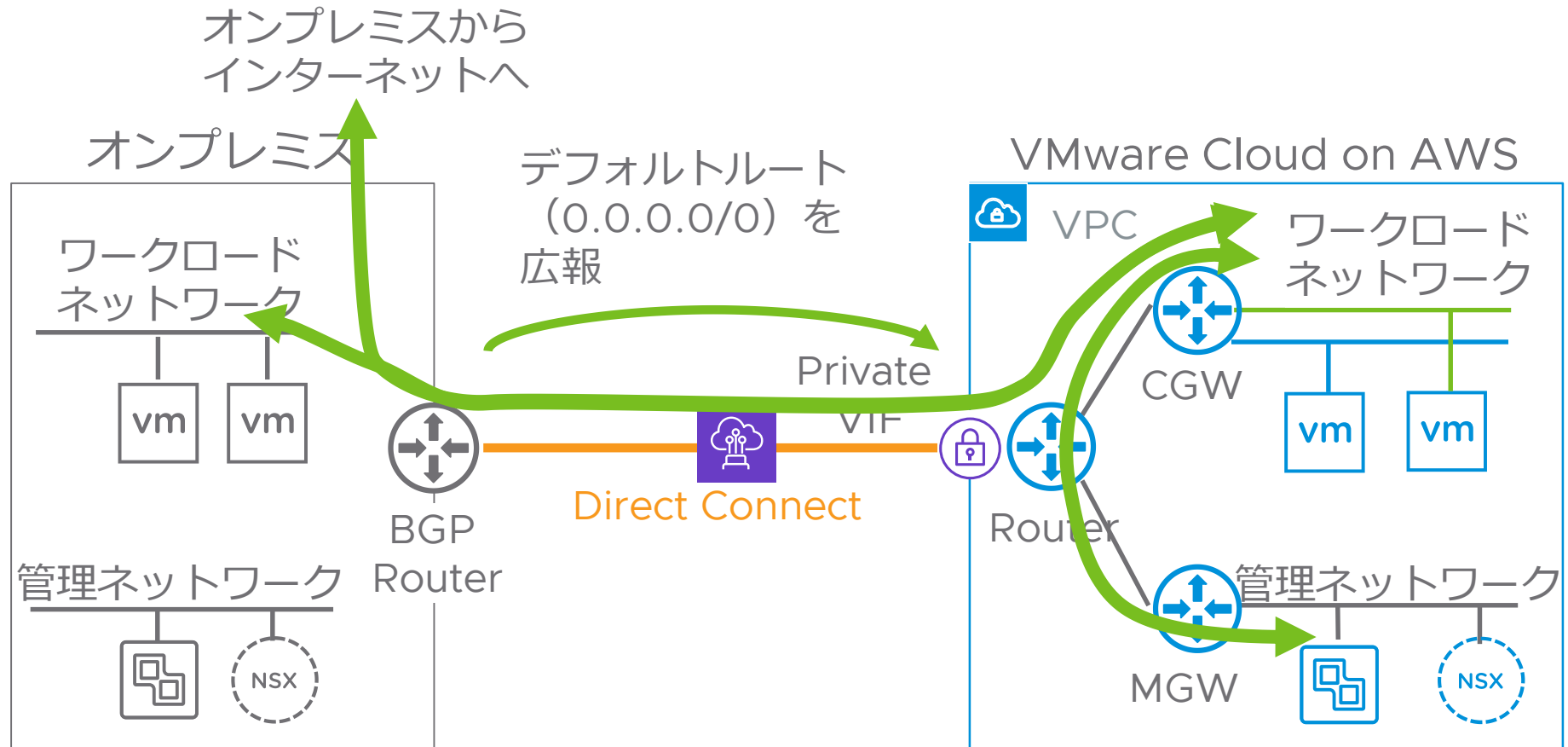
10.32.0.0/11

10.64.0.0/10

10.128.0.0/9

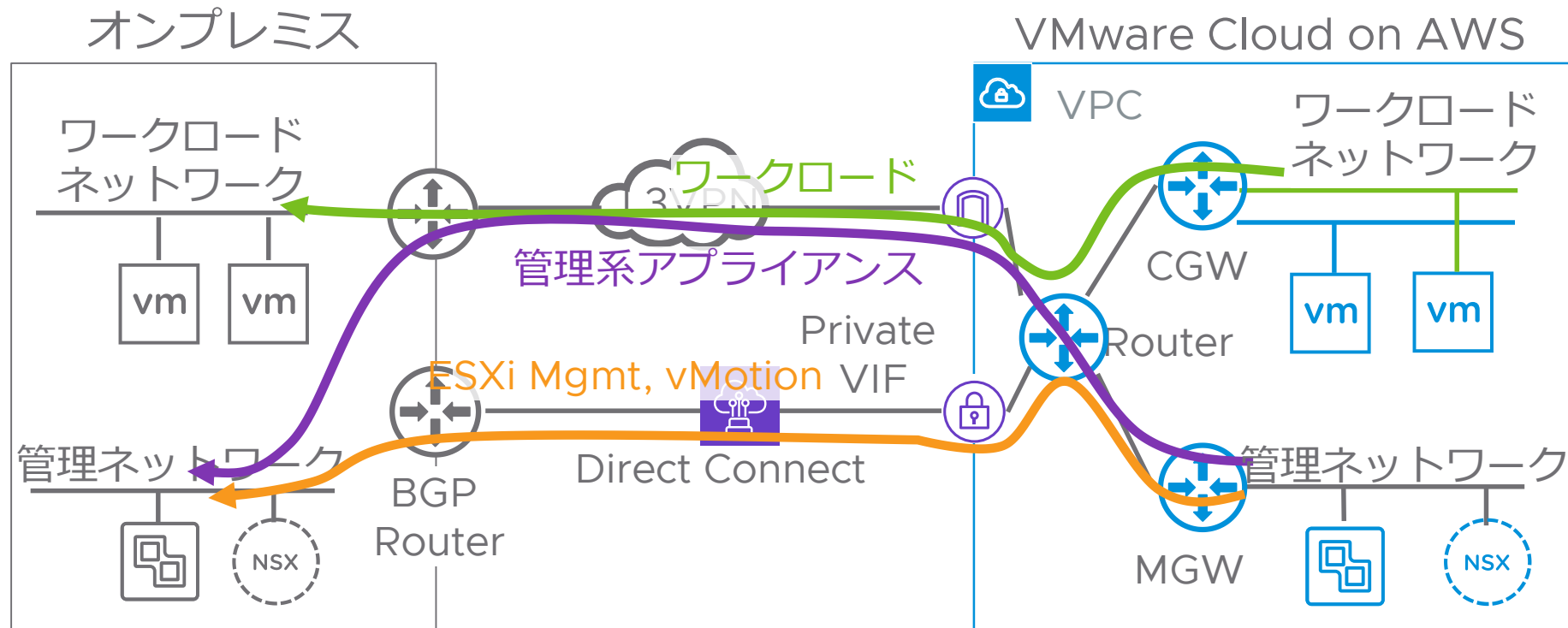
# ダイレクトコネクト詳細

BGPによるデフォルトルート（0.0.0.0/0）の学習と経路



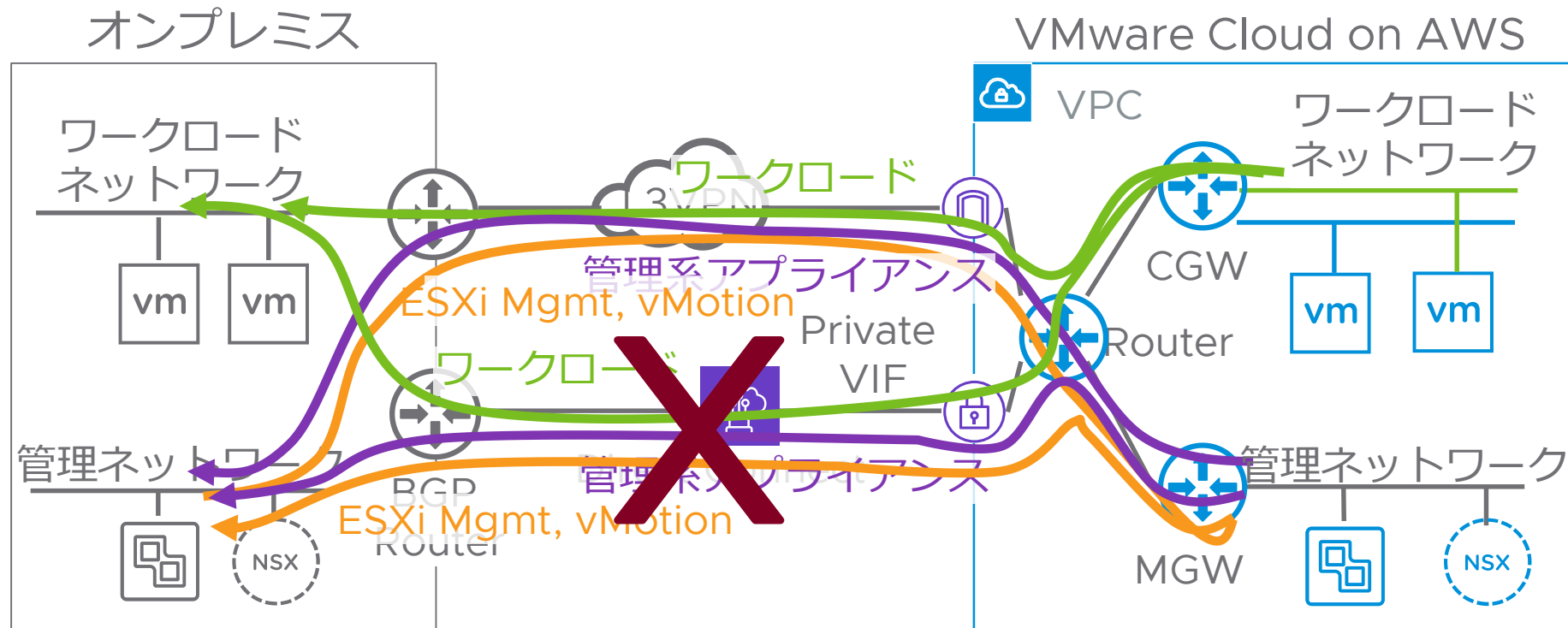
# ダイレクトコネクと IPsec VPN の併用

ルートベース IPsec VPN の BGP で学習したルートを優先してトラフィックが流れる  
ただし、ESXi Mgmt, vMotion パケットはダイレクトコネクを優先



# ダイレクトコネクと IPsec VPN のアクティブ – スタンバイ構成

ダイレクトコネクネットワーク断の場合、IPsec VPN がアクティブになり、ネットワークを提供





# ダイレクトコネクと IPsec VPN のアクティブ – スタンバイ構成

SDDC   サブスクリプション   アクティビティ ログ   ツール   デベロッパー センター

概要

ネットワーク

- セグメント
- > VPN
- NAT

セキュリティ

- ゲートウェイ ファイアウォール
- 分散ファイアウォール

インベントリ

- グループ
- サービス

ツール

- IPFIX
- ポート ミラーリング

システム

- DNS
- DHCP
- パブリック IP アドレス
- Direct Connect
- 接続された VPC

## Direct Connect

AWS アカウント ID  
168120463421

Direct Connect にバックアップとして VPN を使用する  
有効 ☒ ⓘ

BGP ローカル ASN  
10124 ⓘ ASN は同期されています

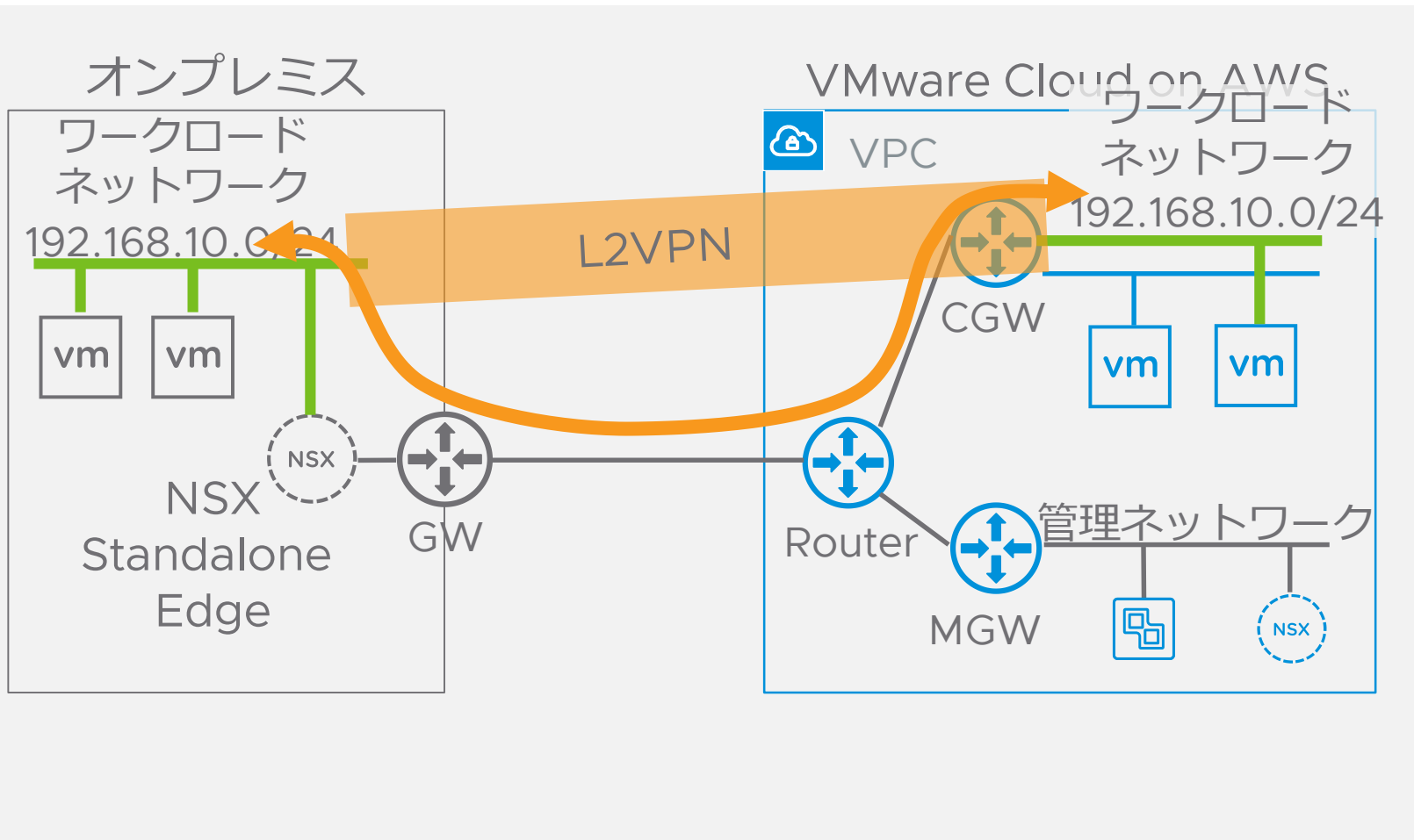
Direct Connect のインターフェイス

仮想インターフェイス名	仮想インターフェイス ID	Direct Connect ID	MTU

# VMware Cloud on AWS とオンプレミスとの接続方式比較

	インターネット (L3VPN)	ダイレクト コネクト
回線種別	インターネット	専用線
オンプレ側ルータ機器	L3VPN (IPsec) 対応機器	BGP 対応機器
コスト	L3VPN 対応機器導入費用 ブロードバンド回線契約費用	ダイレクトコネクト設置費用 事業者との専用線契約費用 ダイレクトコネクト利用費用
メリット	コストが安い	帯域が確保できる 帯域が安定している 閉域網で構成されるからよりセキュア
デメリット	回線品質が不安定	コストかかる

# ワークロード ネットワーク間を NSX L2VPN で延伸

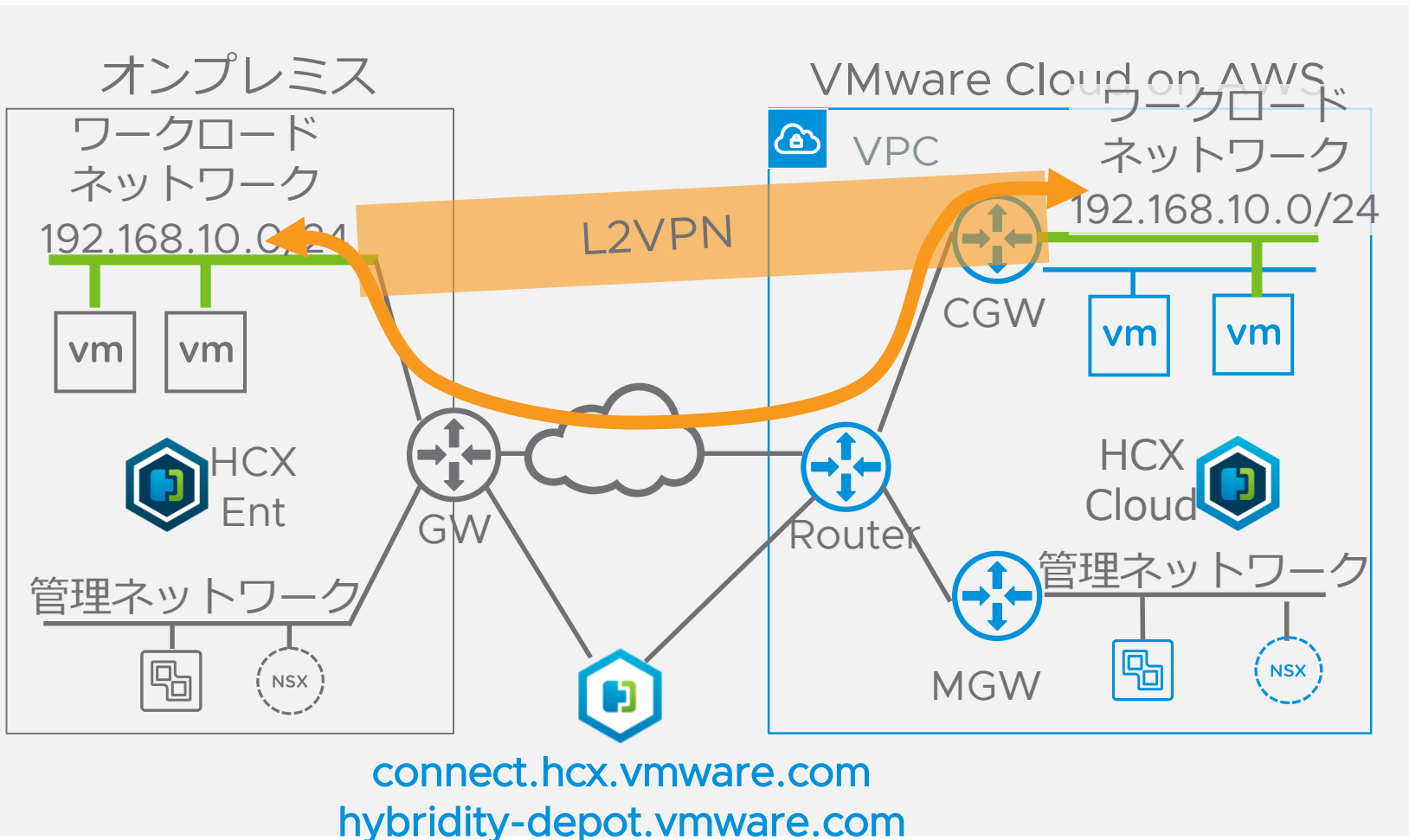


## NSX Standalone Edge を利用した L2 延伸

### 構成

- VLAN セグメントの L2 延伸 (over Internet or Dx)
- オンプレミスは VSS または VDS
- アクティブ - スタンバイの冗長化が可能
- オンプレミス vSphere は 6.0 以上をサポート
- 1 つの Standalone Edge クライアントから 1 VPN トンネルのみサポート
- 最大 100 セグメント延伸可
- vMotion はオンプレミスから VMC 方向のみ (ダイレクトコネクト必須)

# ワークロード ネットワーク間を HCX で延伸



## Hybrid Cloud Extension (HCX) を利用した L2 延伸

### 構成

- VLAN、VXLAN セグメントの L2 延伸 (over Internet or Dx)
- オンプレミスは **VDS** をサポート
- 複数トンネルの構成が可能
- 複数セグメントの延伸が可能
- 複数サイトへの延伸が可能

# ネットワーク延伸方式比較

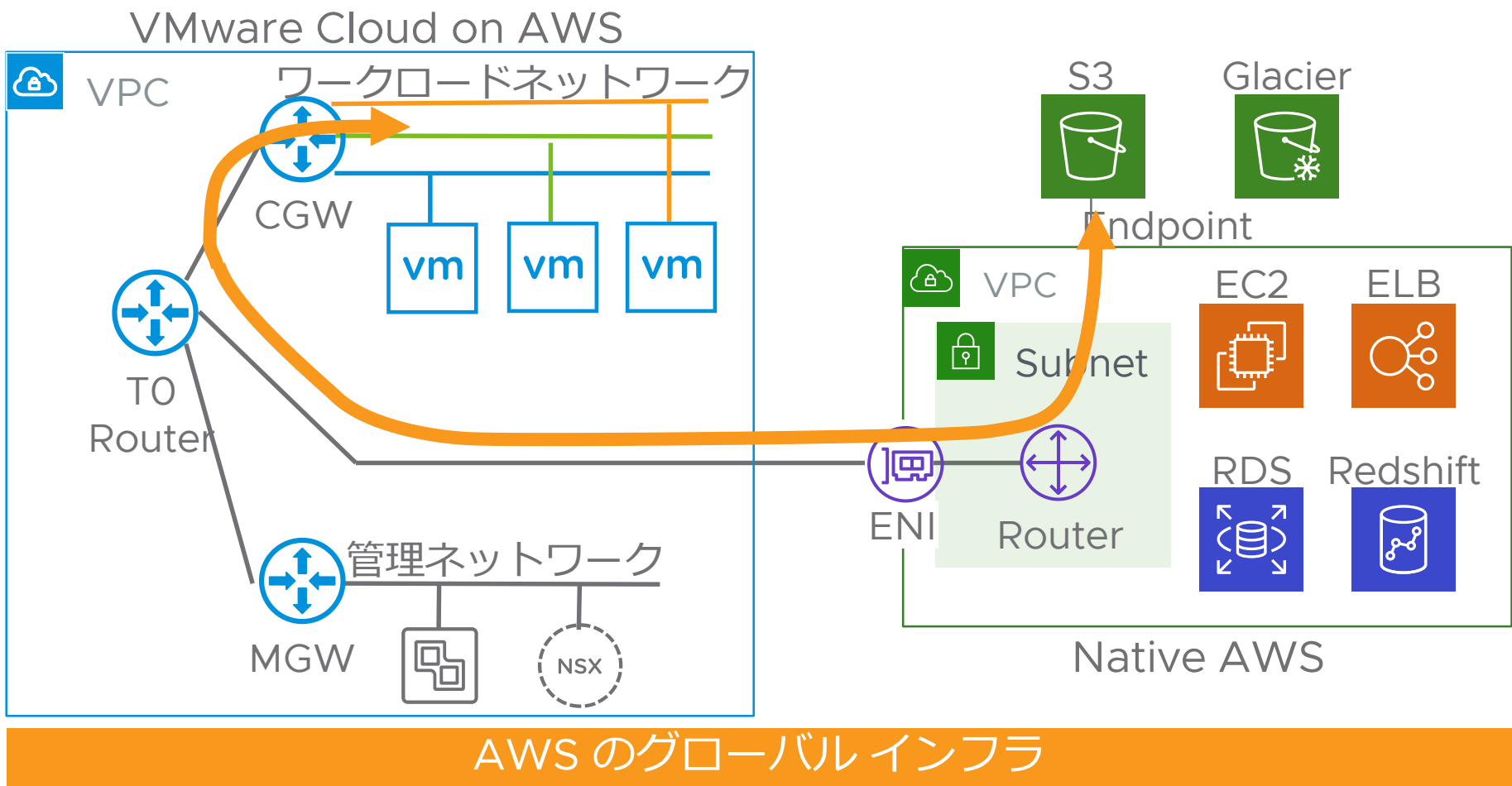
	NSX standalone edge	HCX
WAN 最適化	なし	あり (vMotion, レプリケーション時)
冗長化	あり (6.4 から)	なし (冗長化予定あり)
GUI	なし	あり
L2 延伸の追加	CLI	GUI
移行元仮想スイッチ	標準スイッチ、分散スイッチ	分散スイッチ
VLAN	VC5.0, ESXi5.0+	VC5.1+ (UI は 5.5+), ESXi5.1+
VXLAN	N/A	VC5.5+, ESXi5.5+, NSX6.2+
最大帯域	1.5Gbps	4-6Gbps
メリット	<ul style="list-style-type: none"> <li>✓ 1 アプライアンス構成でリソースがそれほど必要ない</li> </ul>	<ul style="list-style-type: none"> <li>✓ オンプレ側のみでの設定で対応可</li> <li>✓ WAN 最適化により速い移行が可</li> <li>✓ オンプレミス vSphere 対応 バージョン幅が大きい</li> </ul>
デメリット	<ul style="list-style-type: none"> <li>✓ デプロイ後の変更不可</li> <li>✓ WAN 最適化無し</li> <li>✓ オンプレミス vSphere 対応 バージョン幅が狭い</li> </ul>	<ul style="list-style-type: none"> <li>✓ 複数アプライアンス デプロイによりリソースが必要</li> </ul>

# ネットワーク接続詳細

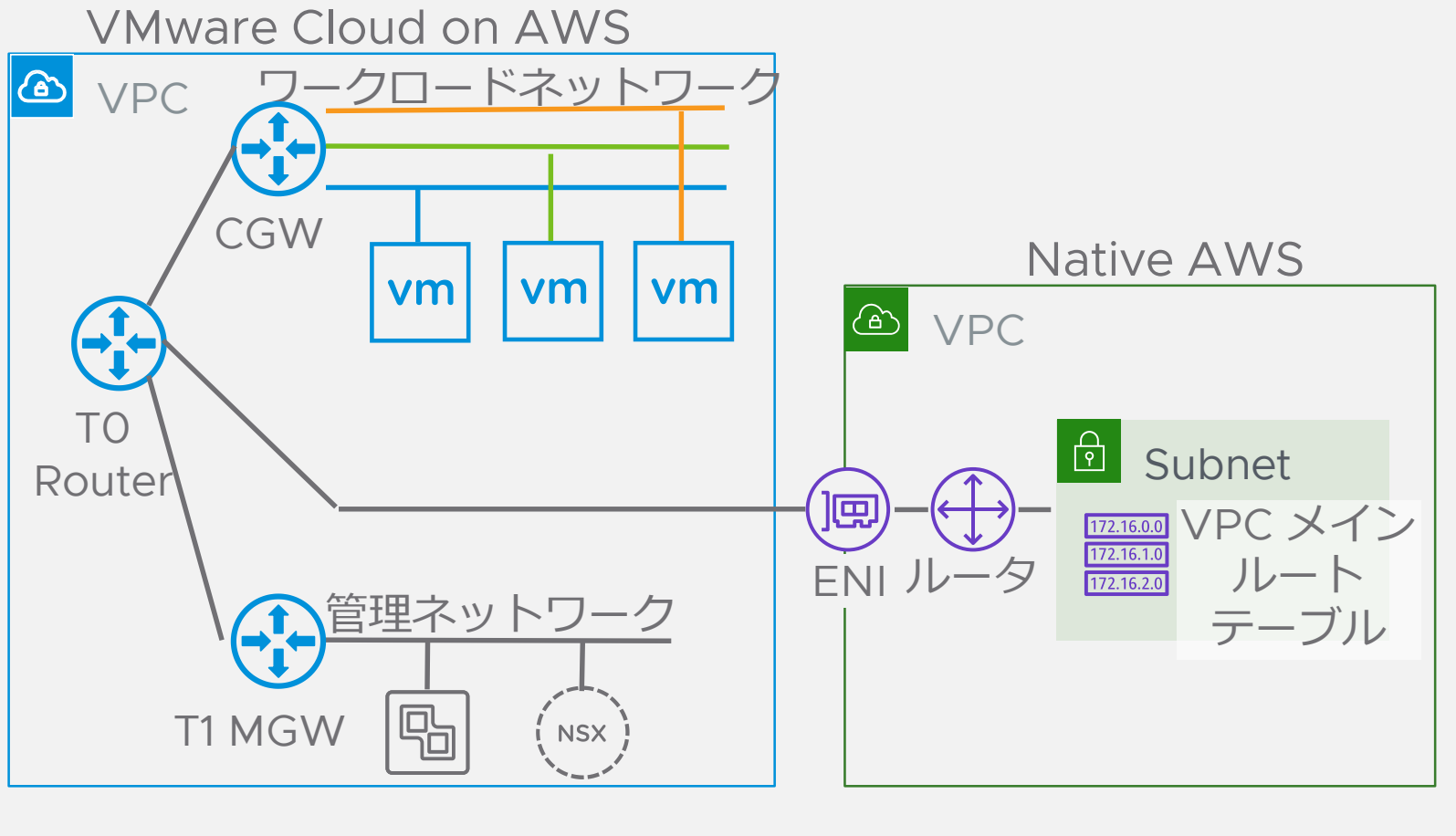
AWS と VMware Cloud on AWS 間の接続



# Native AWS との接続



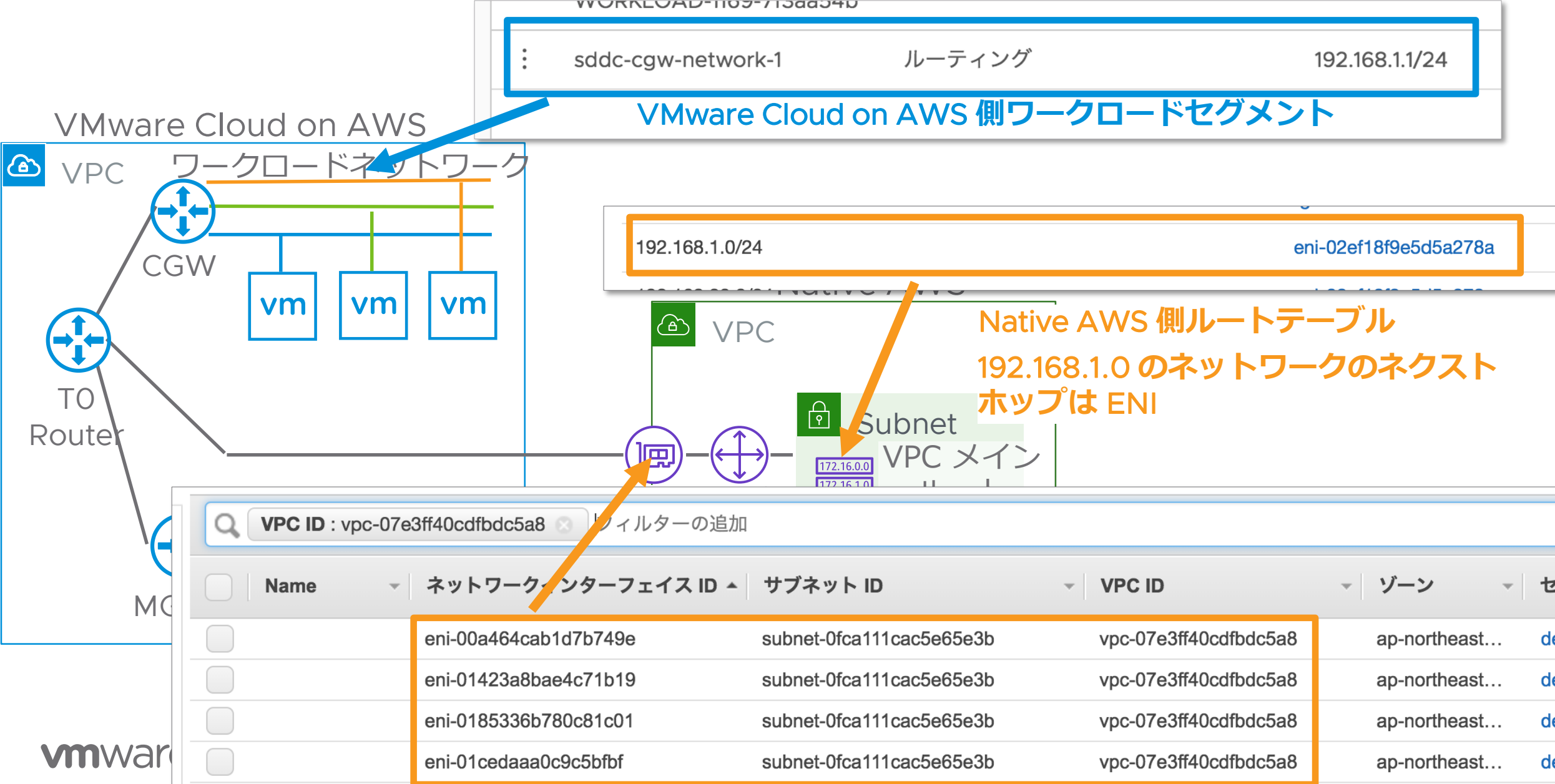
# Native AWS との接続詳細



VMware Cloud on AWS から  
AWS へは ENI で接続

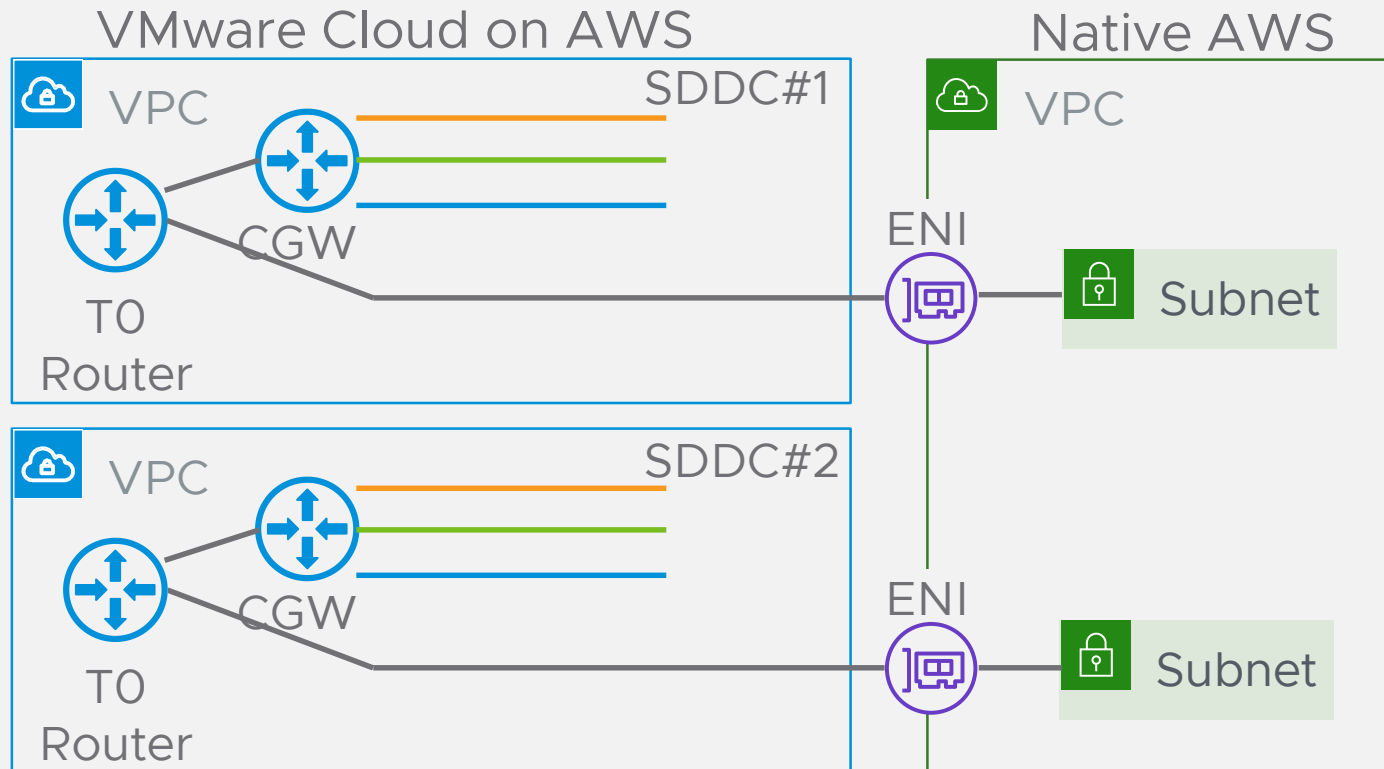
- ENI は AWS 側に作成される
- SDDC 毎に 1つの AWS サブネットへ接続可能  
(SDDC : AWS サブネット = 1 : 1)
- T0 Router に Native AWS サブネットのルーティング情報が追加される
- SDDC セグメントの作成・削除に連携して、AWS VPC メインルートテーブルに同セグメントへのルート情報が追加・削除される  
(その他のルートテーブルは手動設定が必要、サポートはなし)

# Native AWS との接続詳細



# Native AWS との接続詳細

複数 SDDC を同一 AWS VPC へ接続



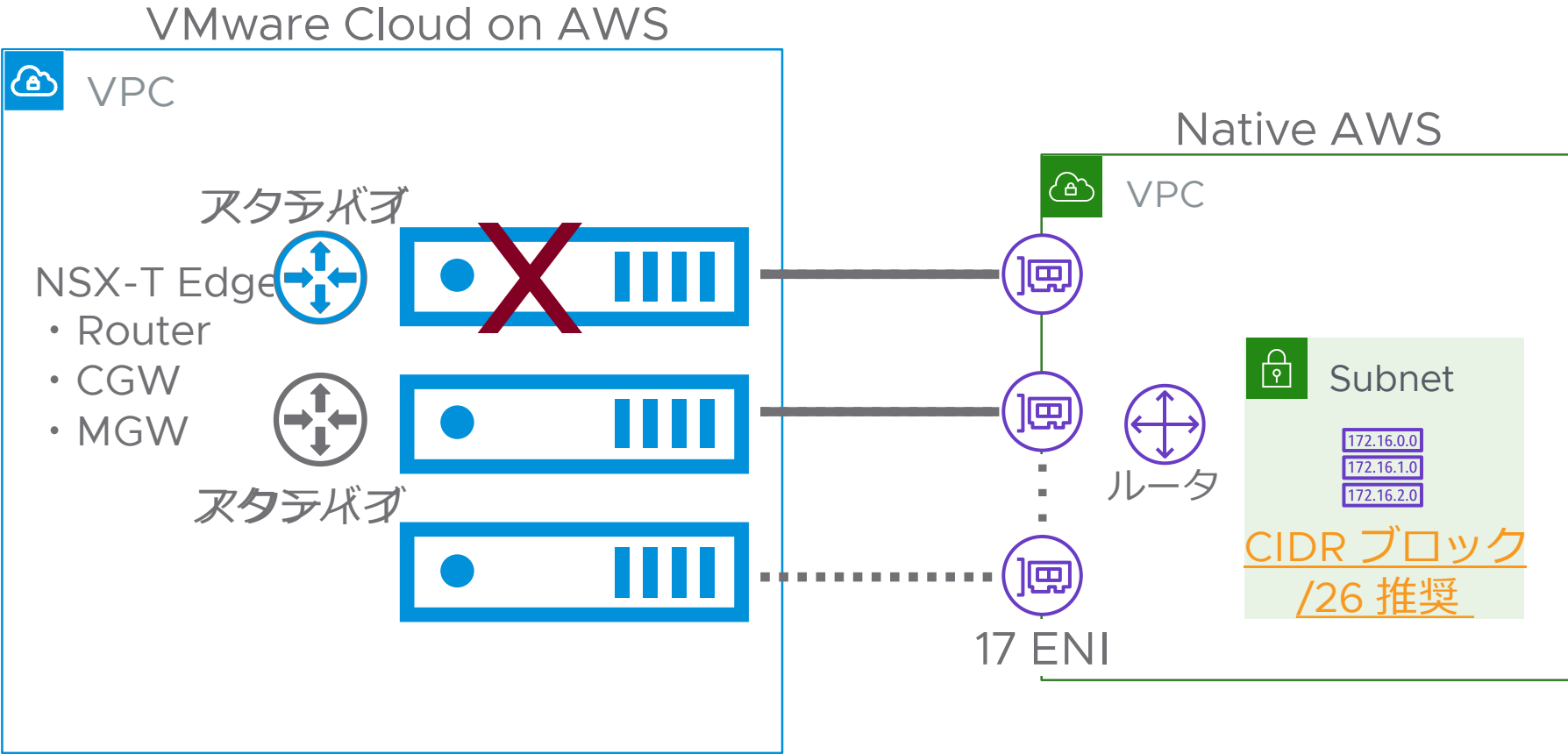
複数 SDDC を同じ Native AWS VPC へ接続可能

- ただし、サブネットは分ける必要あり

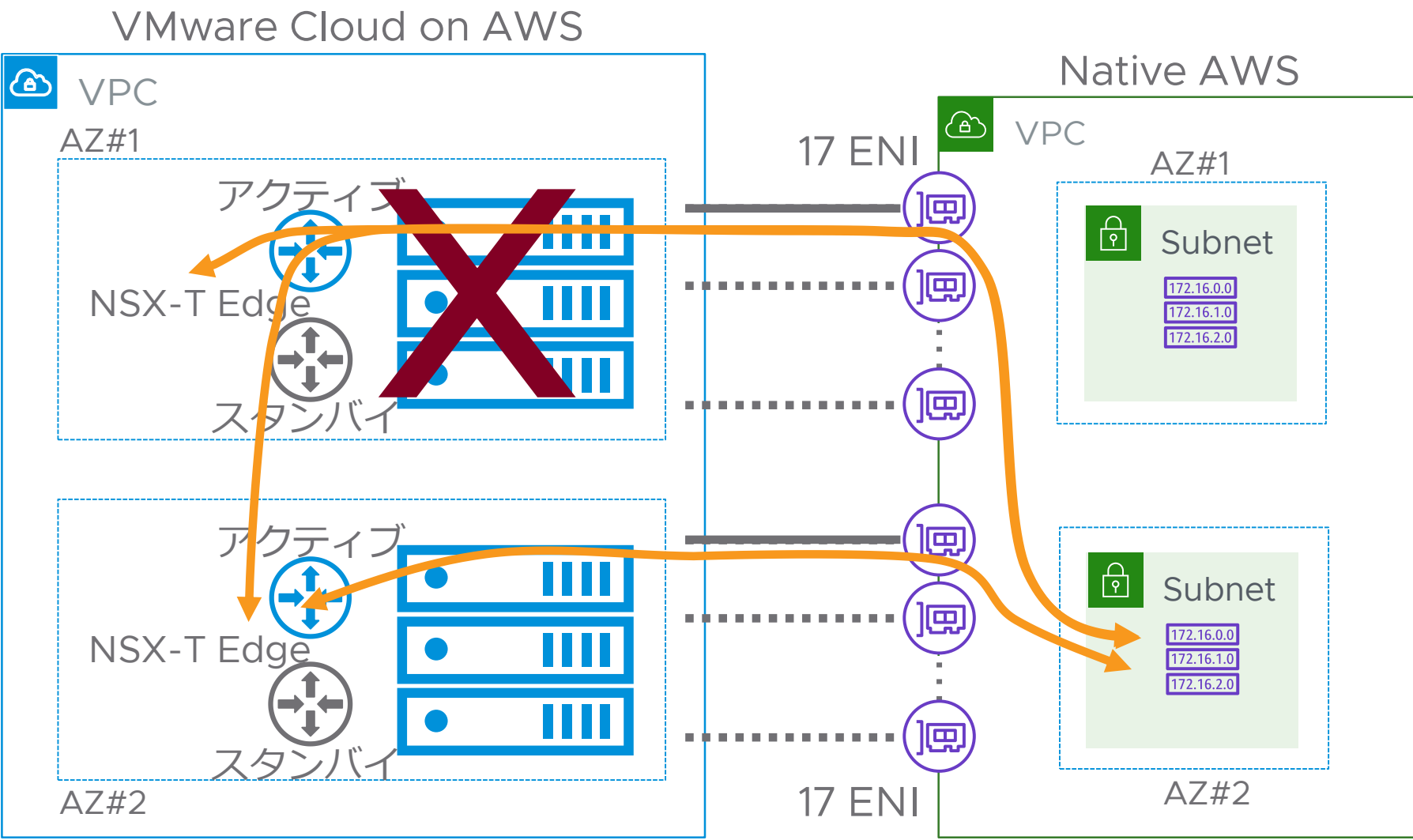
ENI 接続 = 25 Gbps  
(i3.metal, r5.metal)

- 1 接続あたり 5 Gbps
- 5 同時接続で 25 Gbps

# Edge のフェイルオーバーと ENI のフェイルオーバー



# Stretched Cluster 構成時の Edge と ENI のフェイルオーバー



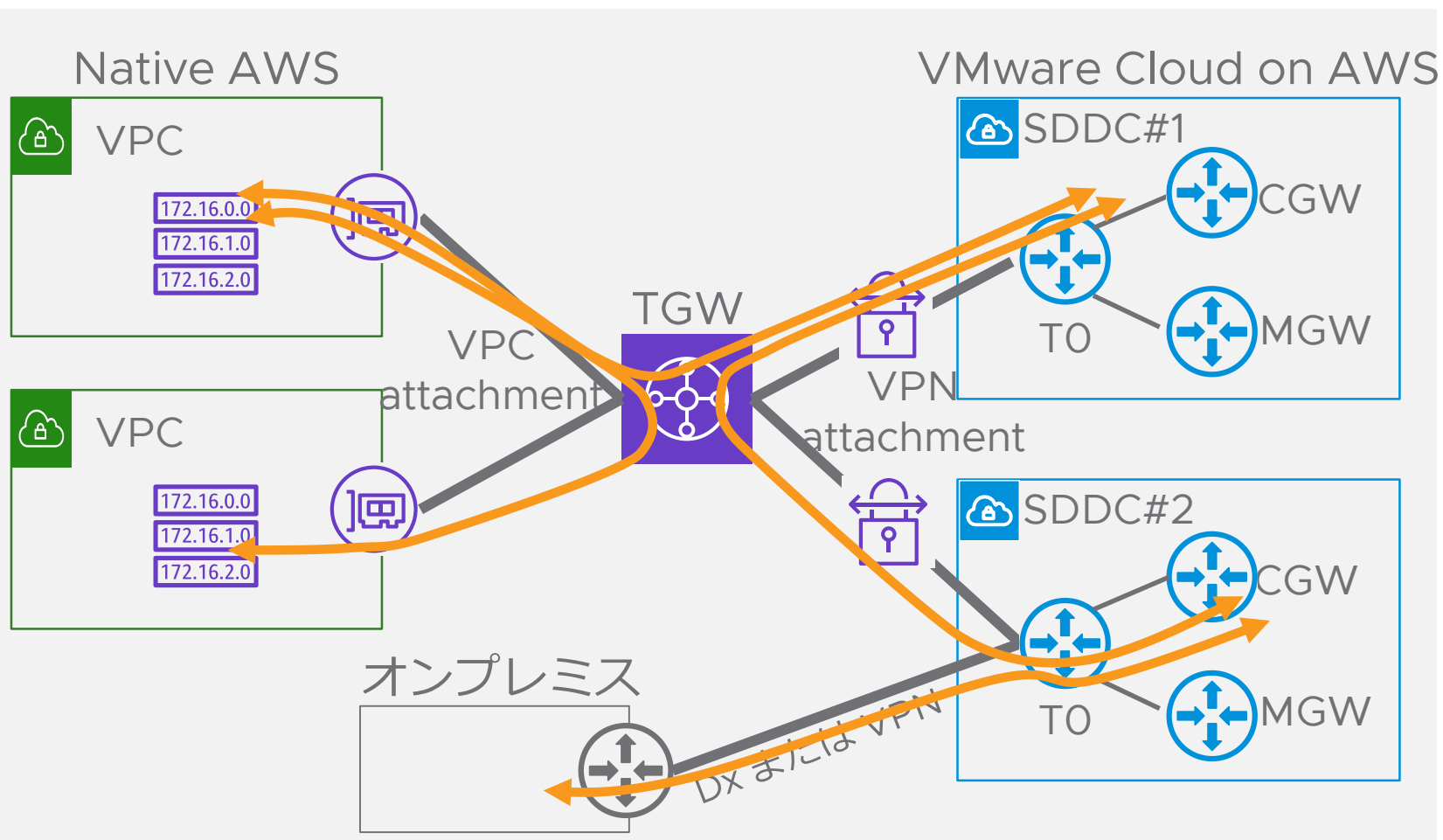


# ネットワーク接続詳細

複数 SDDC または複数 AWS 環境間の接続

# AWS Transit Gateway (TGW) を利用した接続

複数の SDDC - SDDC 間または SDDC - AWS VPC 間



TGW を中心にしたハブ・スポーク型の接続

- 複数の SDDC - SDDC 間の接続
- 複数の SDDC - AWS VPC 間の接続
- TGW は Native AWS アカウント

構成

- TGW - SDDC 間 : VPN
- TGW - AWS VPC 間 : AWS VPC アタッチメント
- オンプレミス - TGW - SDDC は未サポート

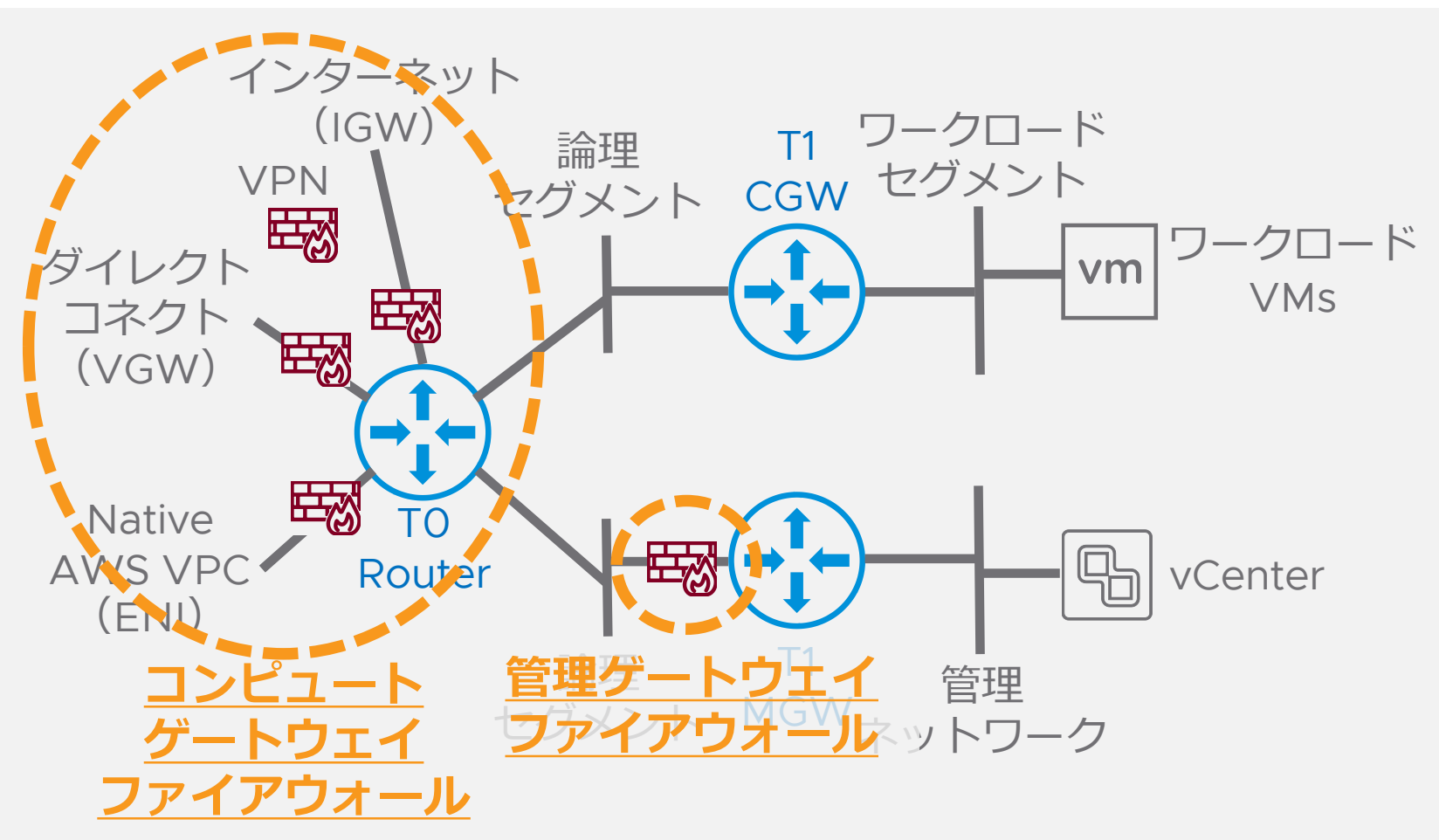
パフォーマンスは要検証

# ネットワークサービス詳細

VMware Cloud on AWS が提供している  
ネットワークサービス

# VMware Cloud on AWS の Edge ファイアウォール

## North - South ファイアウォール



### North - South のファイアウォール

- CGW ファイアウォール
- MGW ファイアウォール

### CGW ファイアウォール

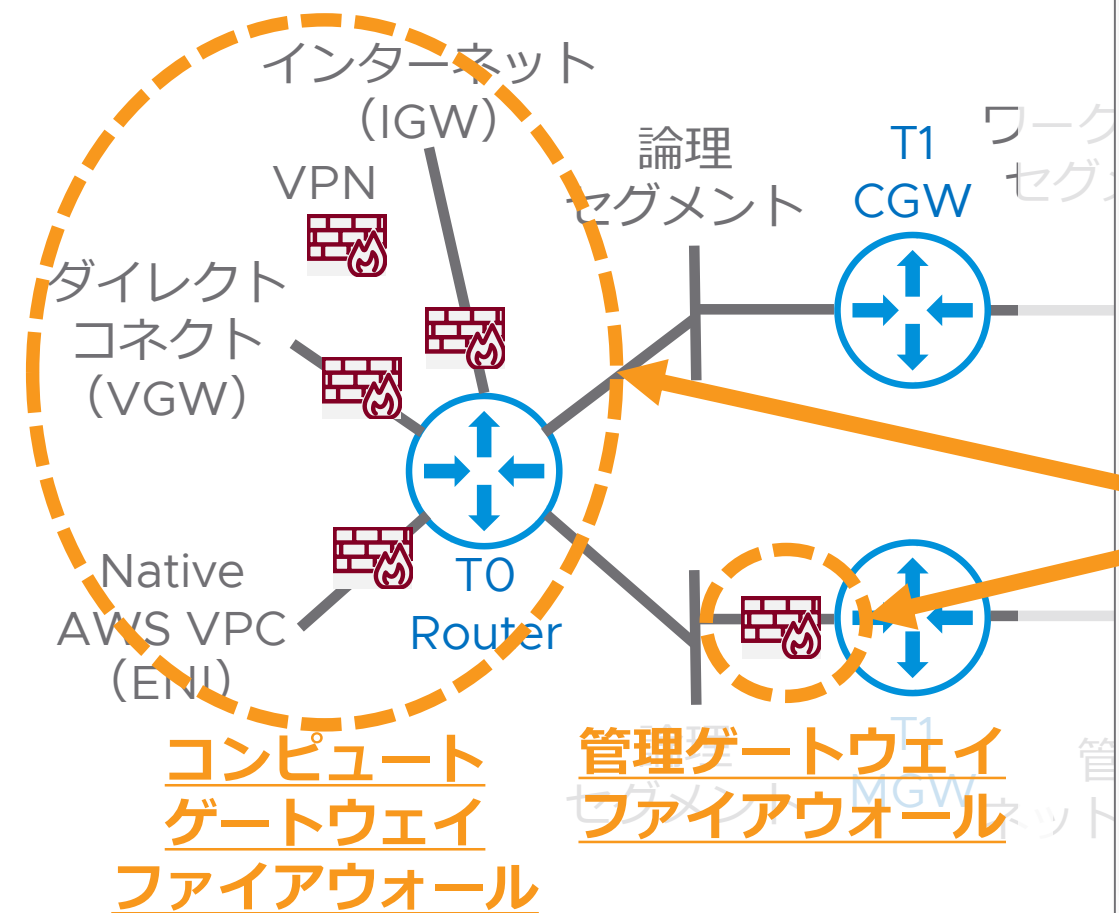
- ワークロードセグメントに対するファイアウォール

### MGW ファイアウォール

- vCenter、NSX、ESXi などの管理ネットワークに対するファイアウォール

# VMware Cloud on AWS の Edge ファイアウォール

## North - South ファイアウォール



サマリ ネットワークとセキュリティ アドオン メンテナンス トラ

概要

ネットワーク

セグメント

> VPN

NAT

セキュリティ

ゲートウェイ ファイアウォール

分散ファイアウォール

インベントリ

グループ

サービス

ツール

ゲートウェイ ファイアウォール

管理ゲートウェイ

15 ルール

新しいルールの追加

名前

Ext

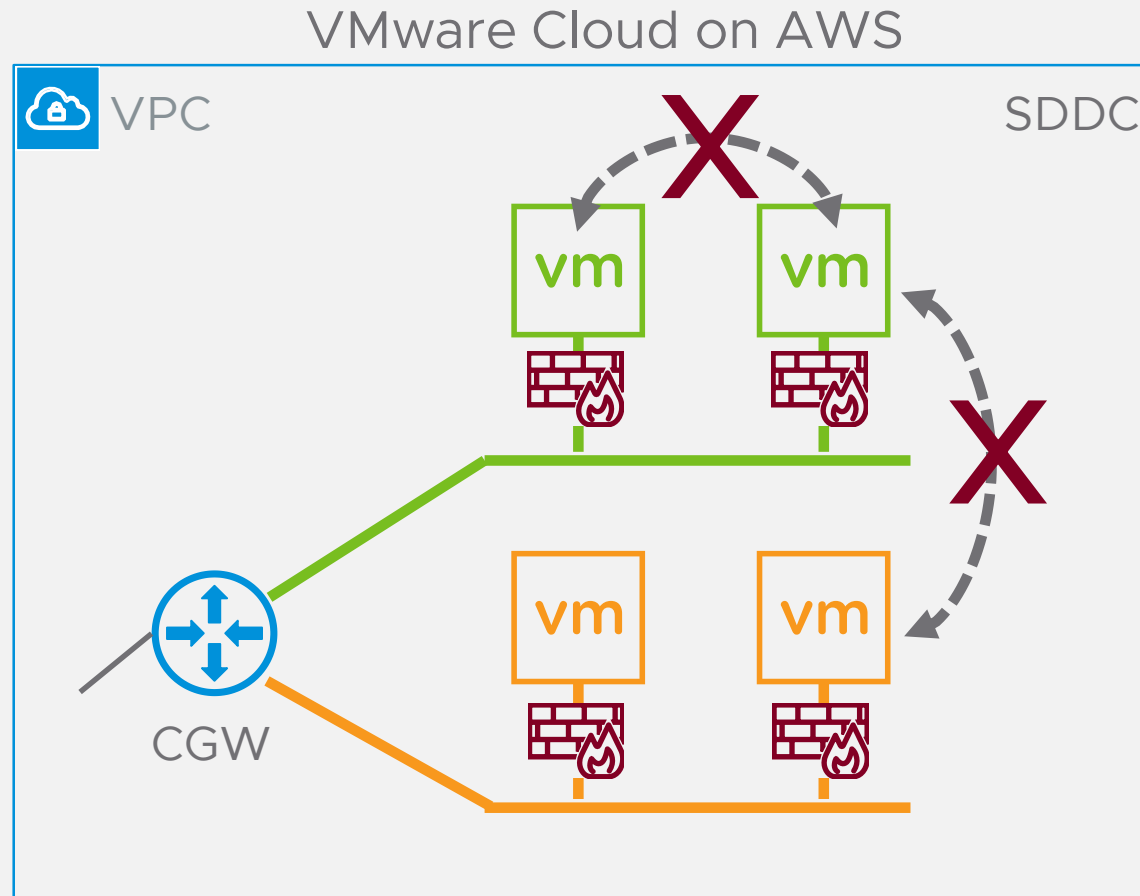
Cloud Prox

コンピュート ゲートウェイ

33 ルール

# VMware Cloud on AWS の分散ファイアウォール

## East - West のファイアウォール



VMware Cloud on AWS 上で  
NSX-T に  
よるマイクロセグメンテーションを  
実現

- ESXi カーネルに組み込まれた  
ファイアウォール機能
- アドオンの追加コスト無し

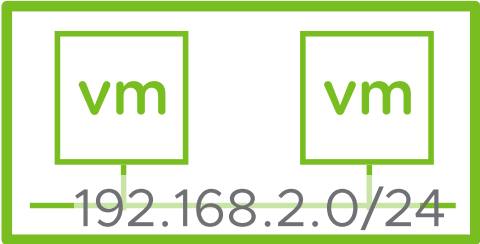
### ユースケース

- ネットワーク隔離によるマルチ  
テナント
- 開発 / テスト / ステージング環境
- DMZ 環境



# セキュリティ グループによるファイアウォールの作成

IP アドレス



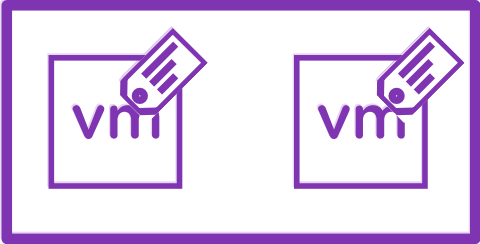
VM インスタンス



VM 名



タグ

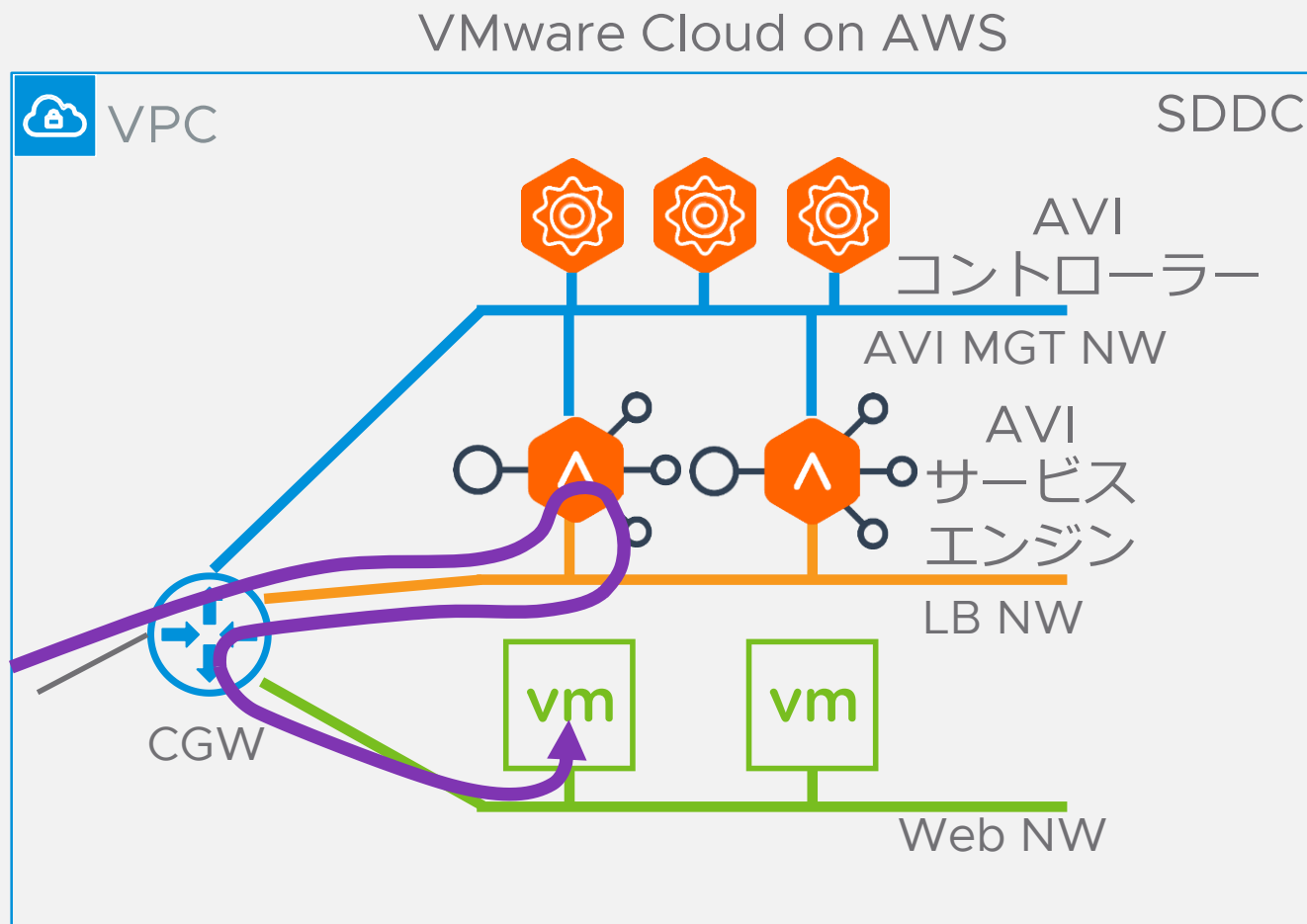


ファイアウォールルール

送信元	宛先	アクション
		ドロップ

# VMware Cloud on AWS での負荷分散機能

## VMware NSX Advanced Load Balancer (Avi Networks) on VMware Cloud on AWS

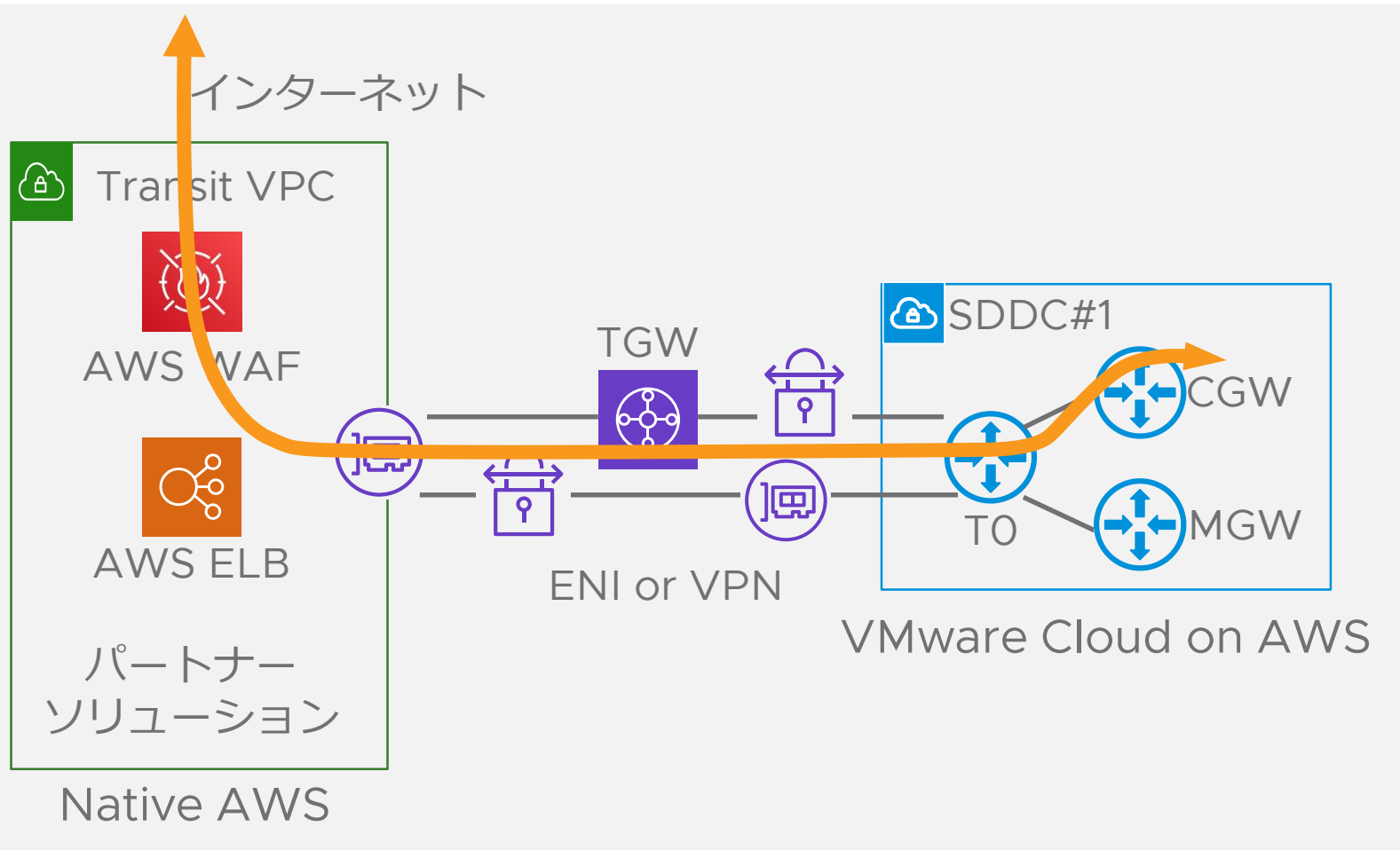


VMware NSX Advanced Load Balancer (Avi Networks) をワークロードセグメントに配置し、負荷分散を実現

### 構成

- AVI コントローラーと AVI サービス エンジンワークロードセグメントにデプロイ
- AVI 関連コンポーネントはユーザーによる管理

# VMware Cloud on AWS における AWS ネットワークサービスとの連携



AWS サービス、AWS  
パートナーソリューションとの  
連携によるネットワークサービスの  
利用

## セキュリティサービス

- AWS WAF, Shield
- サードパーティ IPS / FW
- etc.

## ネットワークサービス

- AWS EBS
- サードパーティロードバランサ
- etc.

# まとめ

## VMware Cloud on AWS ネットワーク接続詳細

- ネットワークの可用性
- 接続方式
- L2 延伸
- Native AWS との接続

## VMware Cloud on AWS ネットワークサービス詳細

- Edge ファイアウォール (North - South)
- 分散ファイアウォール (East - West)
- ロードバランサー on VMware Cloud on AWS
- 各種 AWS ネットワークサービスとの連携



# Thank You