

NS157

# VMware Cloud on AWS ネットワーキング徹底解説

ハイブリッドクラウドのためのネットワーク & セキュリティ

---

VMware, Inc.

ネットワーク&セキュリティ部門  
シニアスタッフテクニカルプロダクトマネージャ  
レイブダバリ

#vforumjp

vmware®

POSSIBLE  
BEGINS  
WITH YOU

# 免責事項

このセッションには、現在開発中の製品/サービスの特長または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。

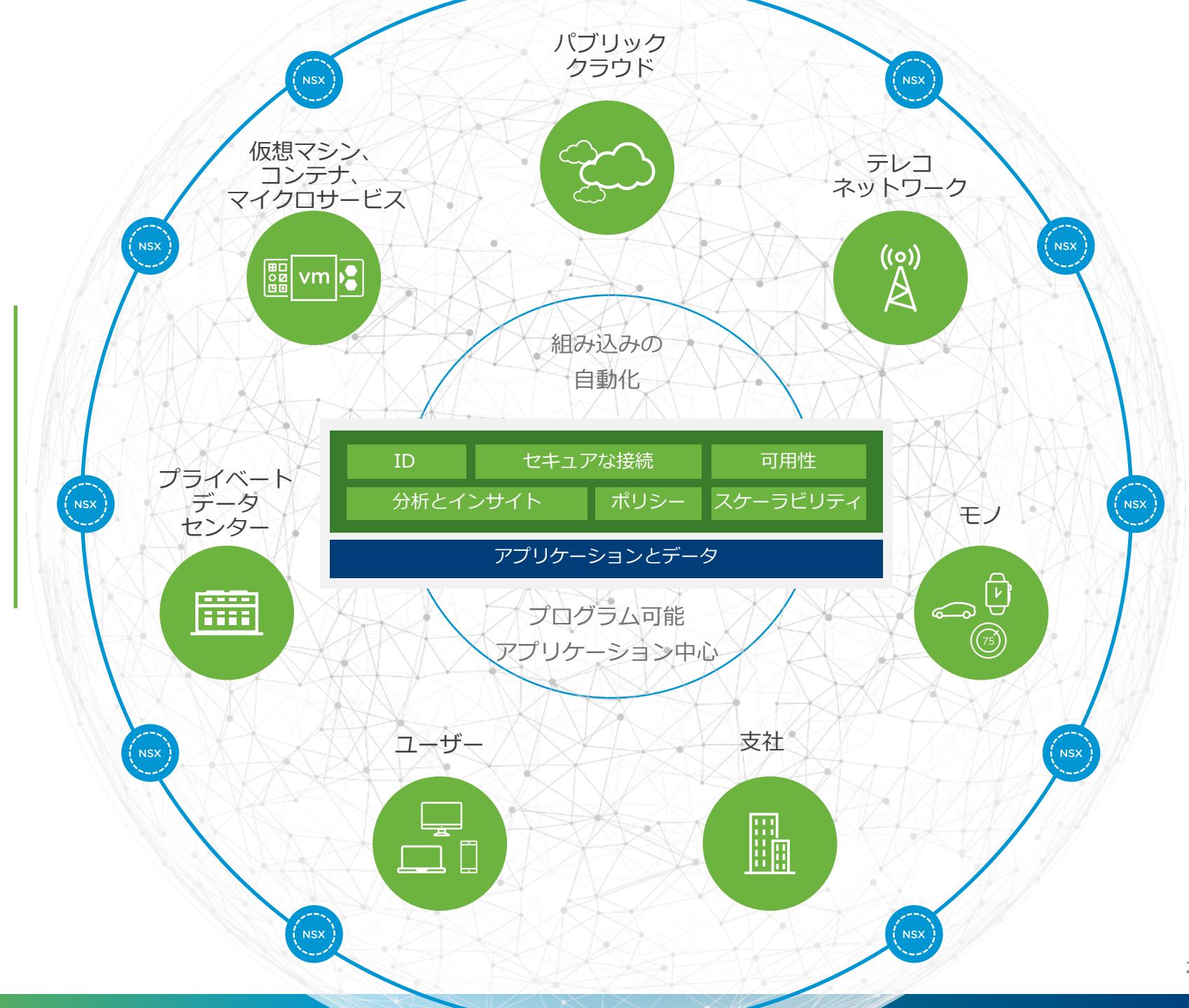
機能は変更される場合があるため、いかなる種類の契約書、受注書、または販売契約書に記述されてはならないものとします。

技術的な問題と市場の需要により、最終的に出荷される製品/サービスでは機能が変わることもあります。

ここで検討および提示されている新しい特長、機能、テクノロジーの価格とパッケージは、決定されたものではありません。

# Virtual Cloud Network

あらゆる環境の  
あらゆるネットワーク  
の接続、保護



# VMware NSX ポートフォリオ

## Virtual Cloud Network の基盤

### ネットワークとセキュリティの管理と自動化

クラウドベースの管理

ワークフローの自動化

ブループリント/テンプレート

インサイト/検出

可視化

Network Insight  
ネットワークの検出とインサイト

VMware vRealize® Automation™  
End-to-End のワークロードの自動化

### ネットワークとセキュリティの仮想化

セキュリティ

統合

拡張性

自動化

柔軟性

VMware NSX® Data Center  
データセンターのワークロードに対応するネットワークとセキュリティ

VMware NSX® Cloud  
パブリック クラウドのワークロードに対応するネットワークとセキュリティ

VMware AppDefense™  
最新のアプリケーションセキュリティ

VMware NSX® SD-WAN by VeloCloud™  
WAN 接続サービス

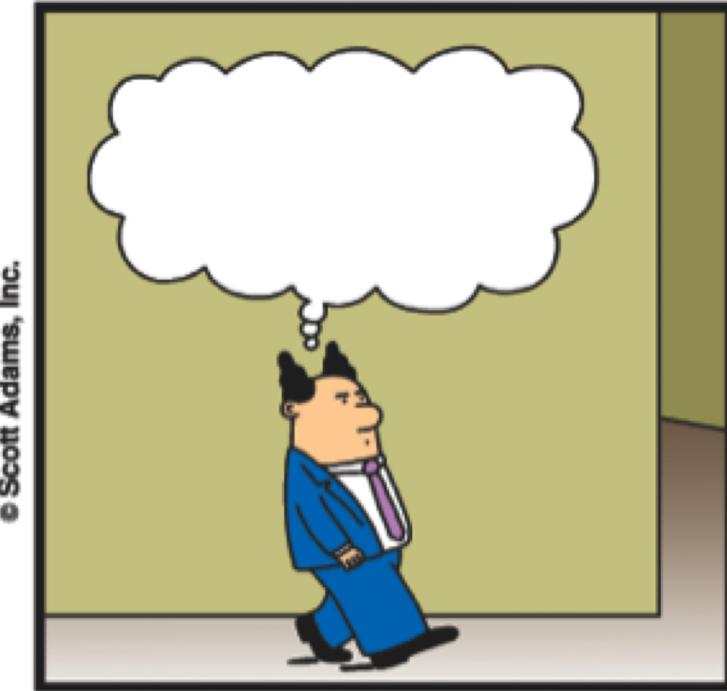
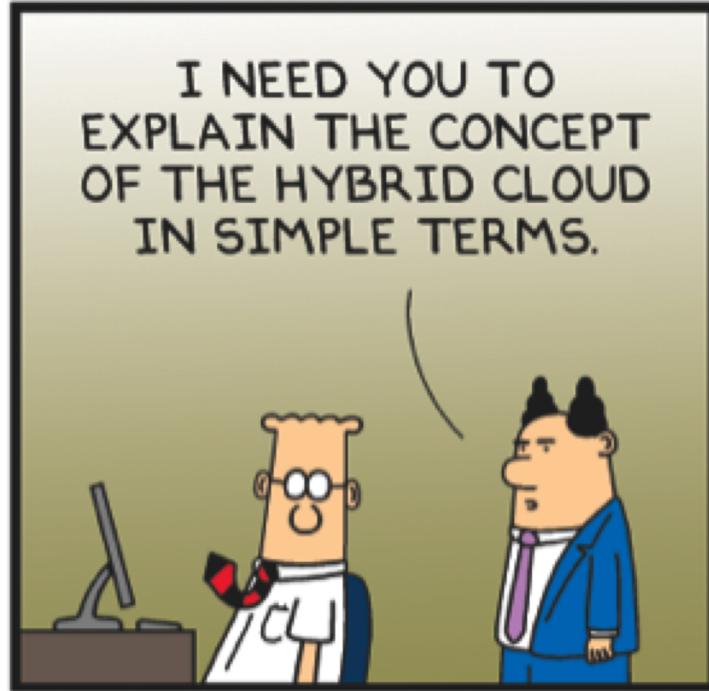
VMware NSX® Hybrid Connect  
データセンターとクラウドのワークロードの移行

# アジェンダ

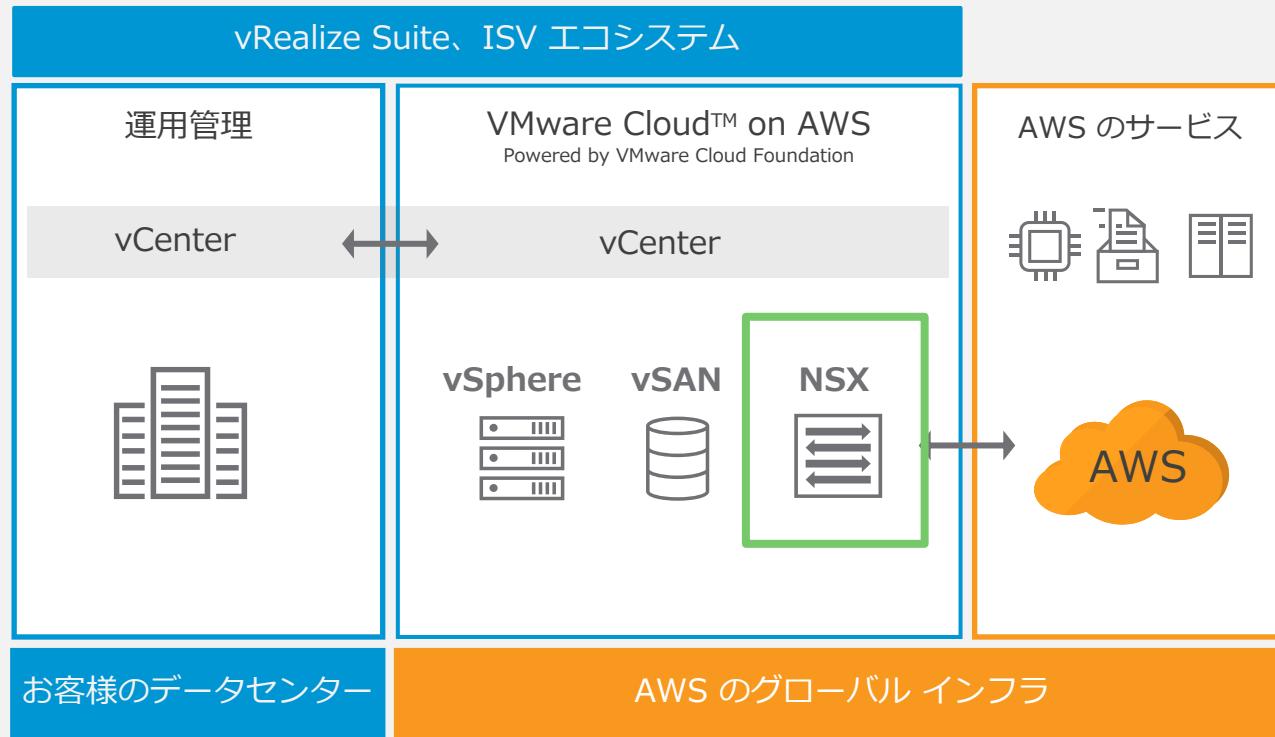
## VMware Cloud on AWS と NSX

1. 概要とユースケース
2. VMware Cloud on AWS アーキテクチャにおける NSX
3. NSX の機能の詳細情報
4. デモ
5. オンプレミスの NSX
6. まとめと Q&A

# ハイブリッド クラウドとは？



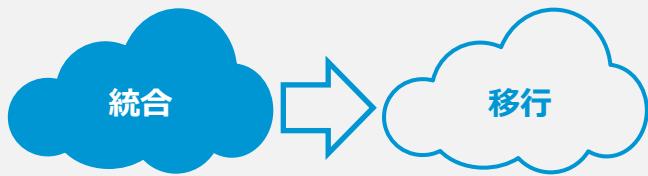
# VMware Cloud on AWS: サービス概要



- AWS ベアメタル上で実行される VMware SDDC
- VMware とパートナーによる販売、運用、サポート
- コンテナと仮想マシンのサポート
- オンデマンドのキャパシティと柔軟な利用
- オンプレミスの SDDC との完全な運用の一貫性
- ワークロードのシームレスな移行とハイブリッド運用
- AWS のグローバルなフットプリントを基盤とした可用性の高いサービスの利用
- AWS のネイティブ サービスへの直接アクセス

# 主なユースケース

## A クラウドへの移行



特定のアプリケーション

データセンター全体

インフラストラクチャの刷新

## B データセンターの拡張

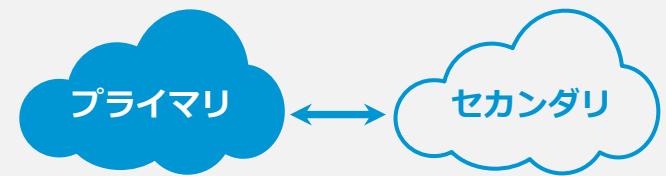


ユーザー環境の拡大

オンデマンドのキャパシティ

テスト/開発用

## C ディザスタ リカバリ



新規のディザスタ リカバリ

既存のディザスタ リカバリ  
の置き換え

既存のディザスタ リカバリ  
の補完

NSX サービス

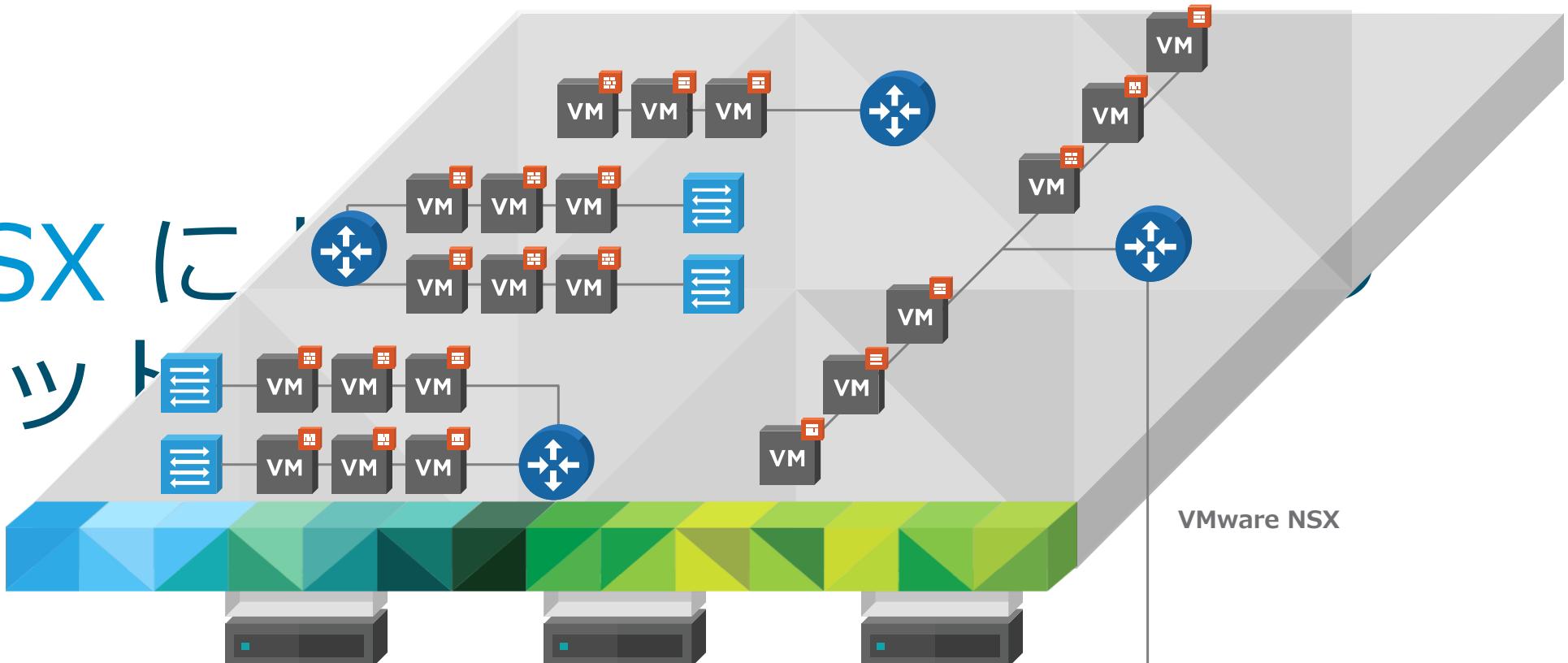
論理  
スイッチング

論理  
ルーティング

ファイア  
ウォールと  
セキュリティ



NSX に  
ネット



VMware NSX

AWS VPC  
ネットワーク

# アジェンダ

## VMware Cloud on AWS と NSX

1. 概要とユースケース
2. **VMware Cloud on AWS アーキテクチャにおける NSX**
3. NSX の機能の詳細情報
4. デモ
5. オンプレミスの NSX
6. まとめと Q&A

# VMware Cloud on AWS : NSX の機能

## 管理プール

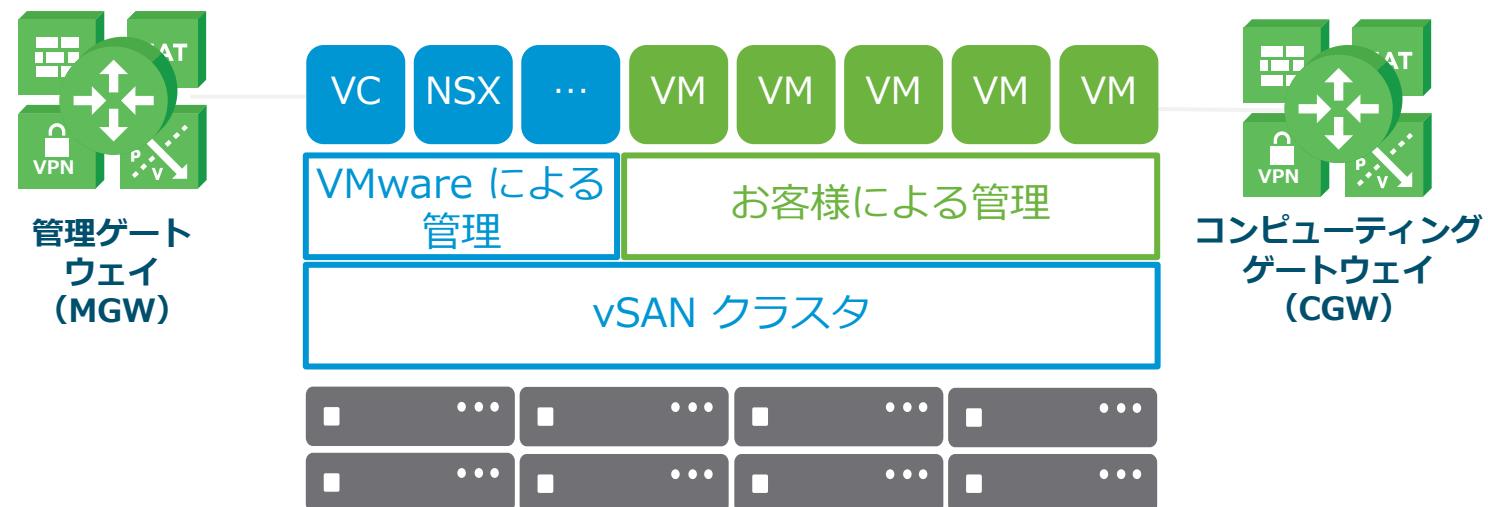
- vCenter Server、NSX Manager、NSX Controller、NSX Edge
- NSX Edge Gateway が提供するサービス (MGW)
- ファイアウォールと VPN によるセキュリティ
- NAT (パブリック VC アクセス用)
- DNS フォワーダー

## コンピューティング プール

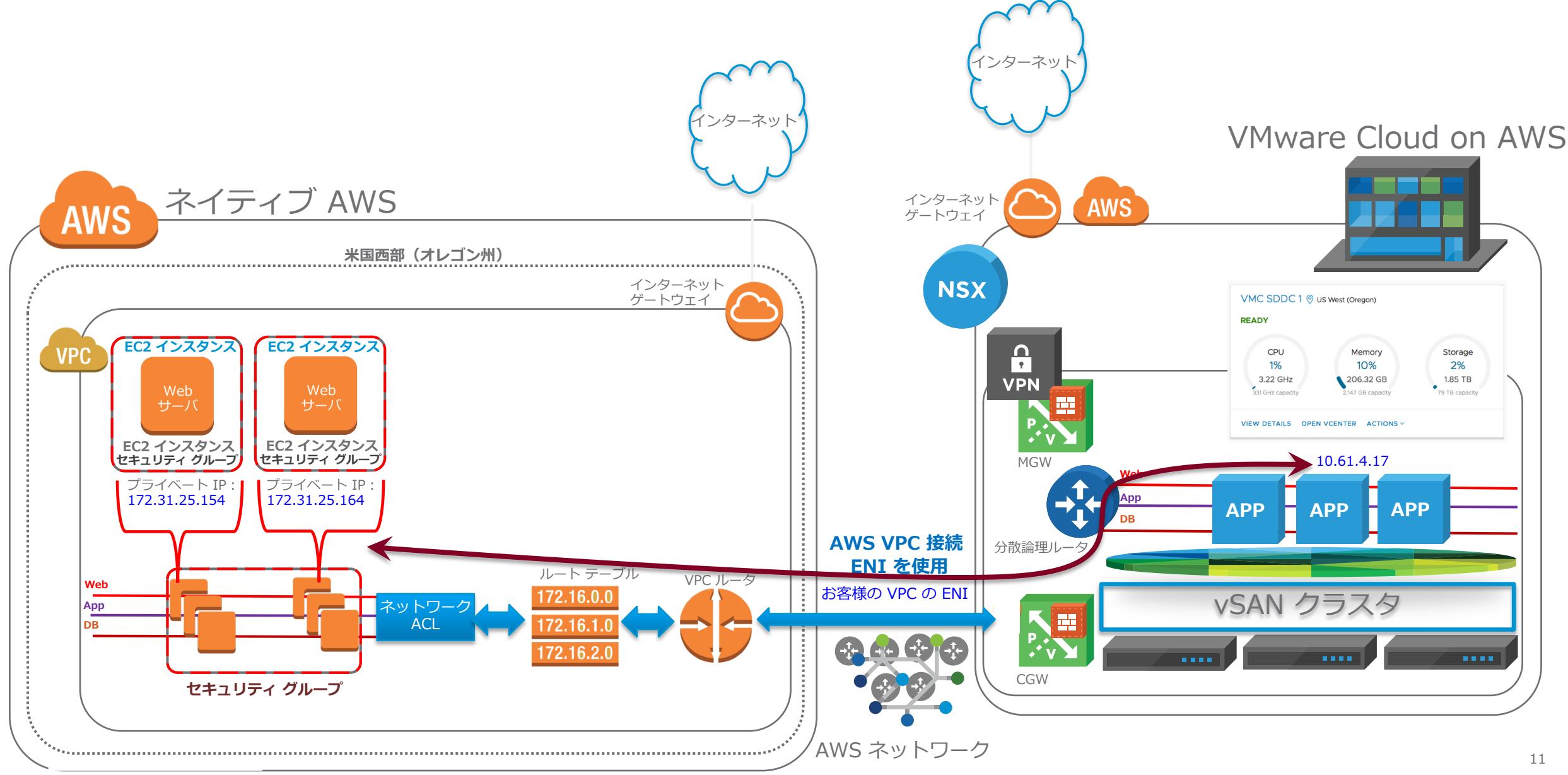
- NSX Edge Gateway が提供するサービス (CGW)
- 規範的ネットワーク トポロジー
- ワークロード仮想マシン用の NSX ネットワーク セグメント
  - デフォルトのネットワークを用意  
(お客様が構築したネットワークもサポート)
    - DHCP リレー/サーバ
    - 自動化されたルーティング構成
  - ファイアウォールと VPN によるセキュリティ
  - NAT (仮想マシン インターネット アクセス用)
  - DNS フォワーダー
  - お客様の VPC との接続

## 機能 :

- 1.) North-South ファイアウォールによるアプリケーションの保護
- 2.) インターネット経由でのアプリケーションへの接続の許可  
(パブリック IP のリクエストと NAT の使用が可能)
- 3.) オンデマンドでの論理ネットワーク構築
- 4.) ポリシー ベースの IPSec VPN を介したセキュアなハイブリッド接続
- 5.) AWS のネイティブ サービスへのアクセス
- 6.) 単一の管理画面による管理 : vCenter ハイブリッド リンク モード
- 7.) クラウド/ライブ マイグレーションのサポート



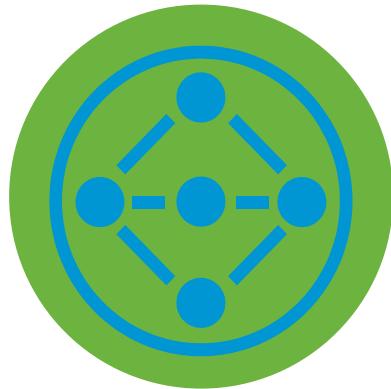
# VMware Cloud on AWS : 最適化されたネイティブ AWS アクセス



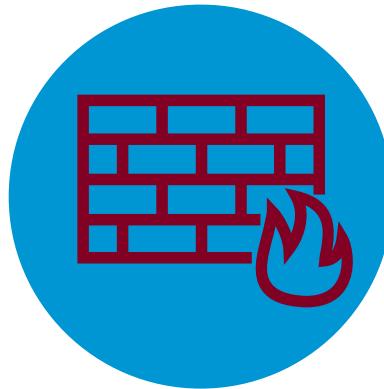
# NSX の高度なサービス

VMware Cloud on AWS SDDC バージョン 1.5

# NSX の高度なサービスの主要なカテゴリ



接続



セキュリティ



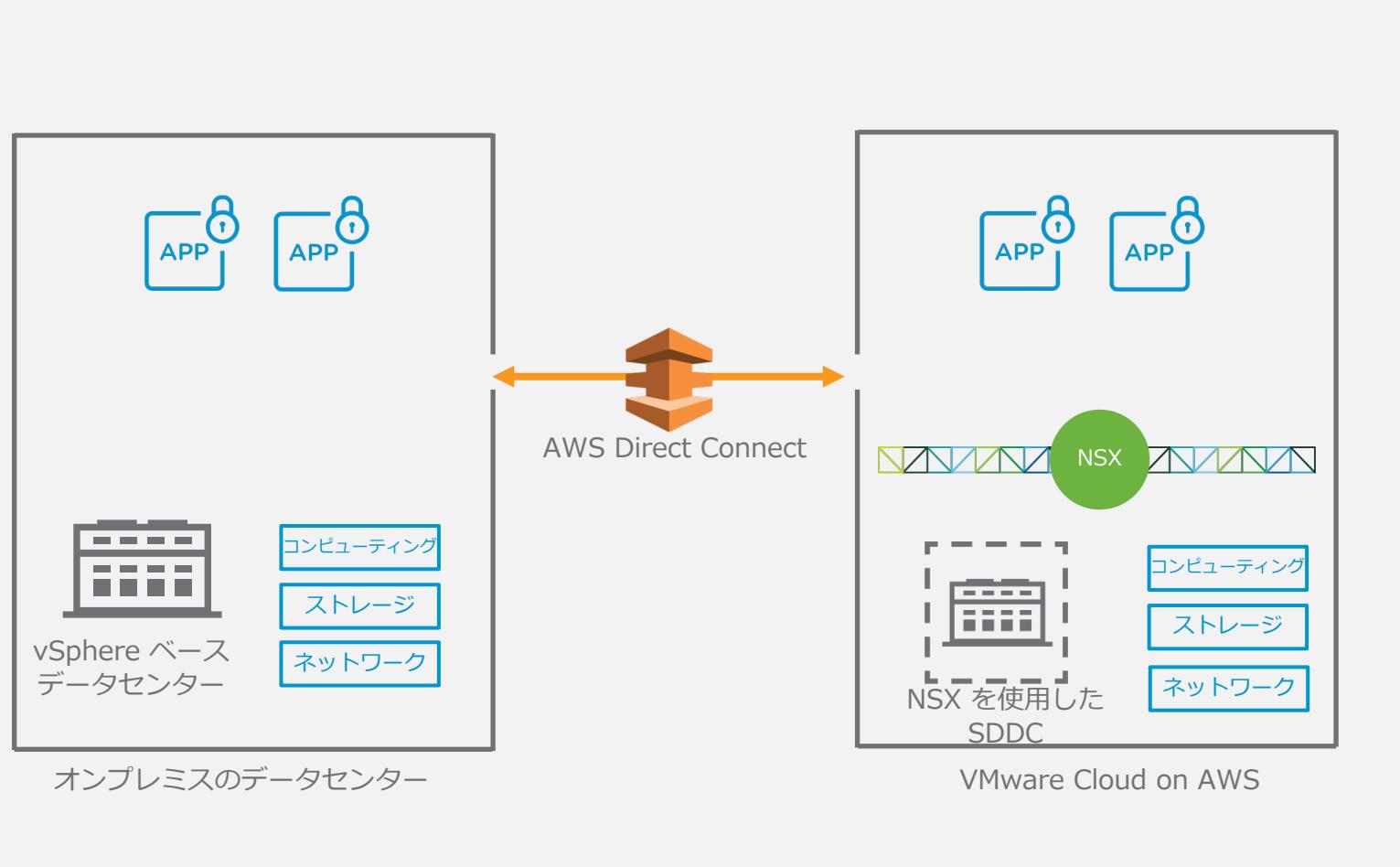
可視化

# Direct Connect による相互接続

NSX と AWS Direct Connect の連携により  
エンドツーエンドのプライベート ネットワークを実現



接続



あらゆるトラフィック タイプで  
高帯域、低遅延の接続が可能

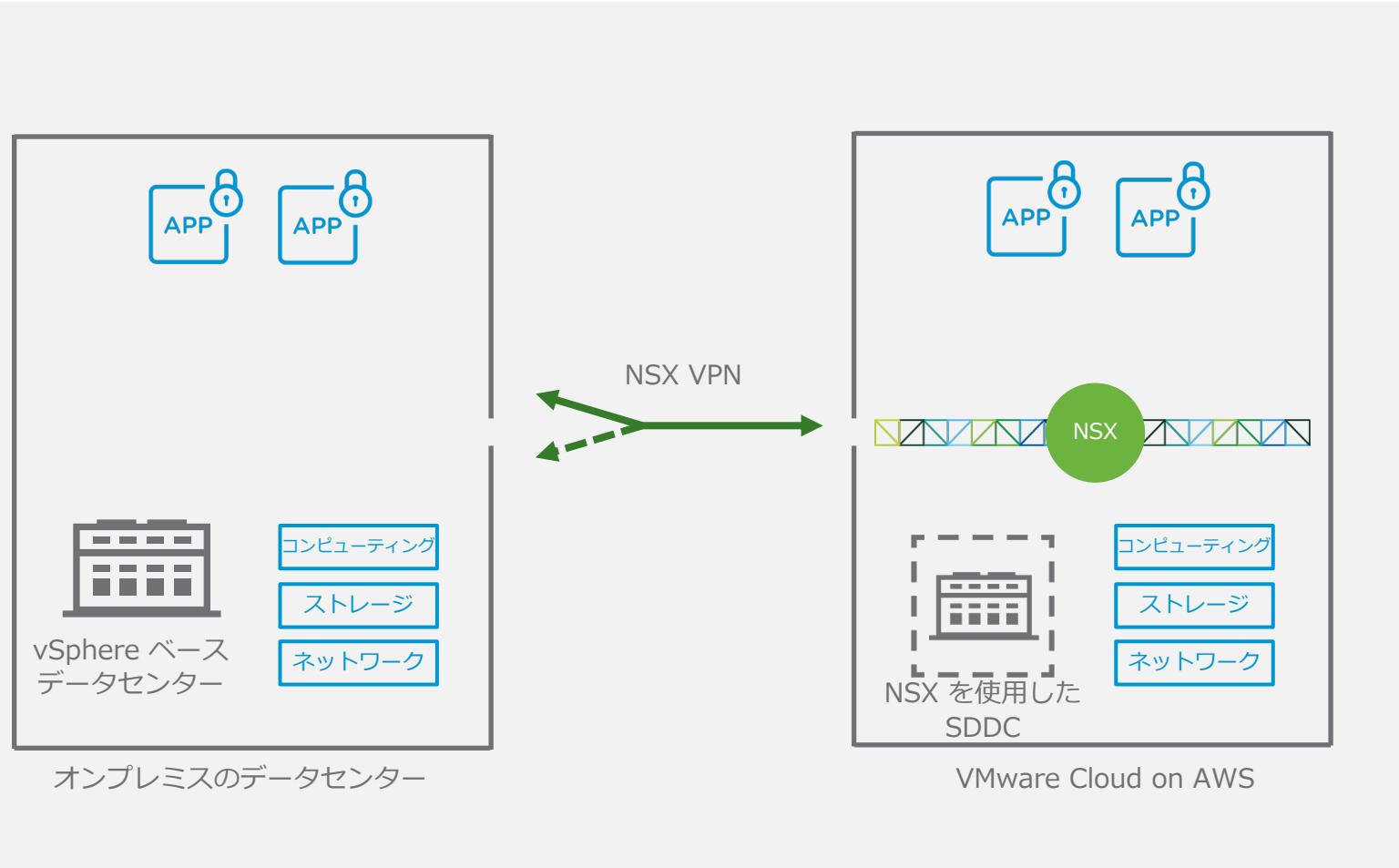
NSX の論理ネットワークと管理  
ネットワークを Direct Connect  
でアドバタイズ

必要に応じて、暗号化された  
トラフィックに IPSec VPN を  
使用

# NSX Edge IPsec VPN による相互接続

NSX を介したエンドツーエンドの接続

接続



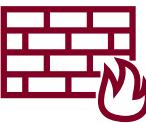
BGP ルーティングのサポートにより VPN 展開を簡素化

一意のエンドポイント間にわたるデュアルホーム トンネルにより耐障害性を実現

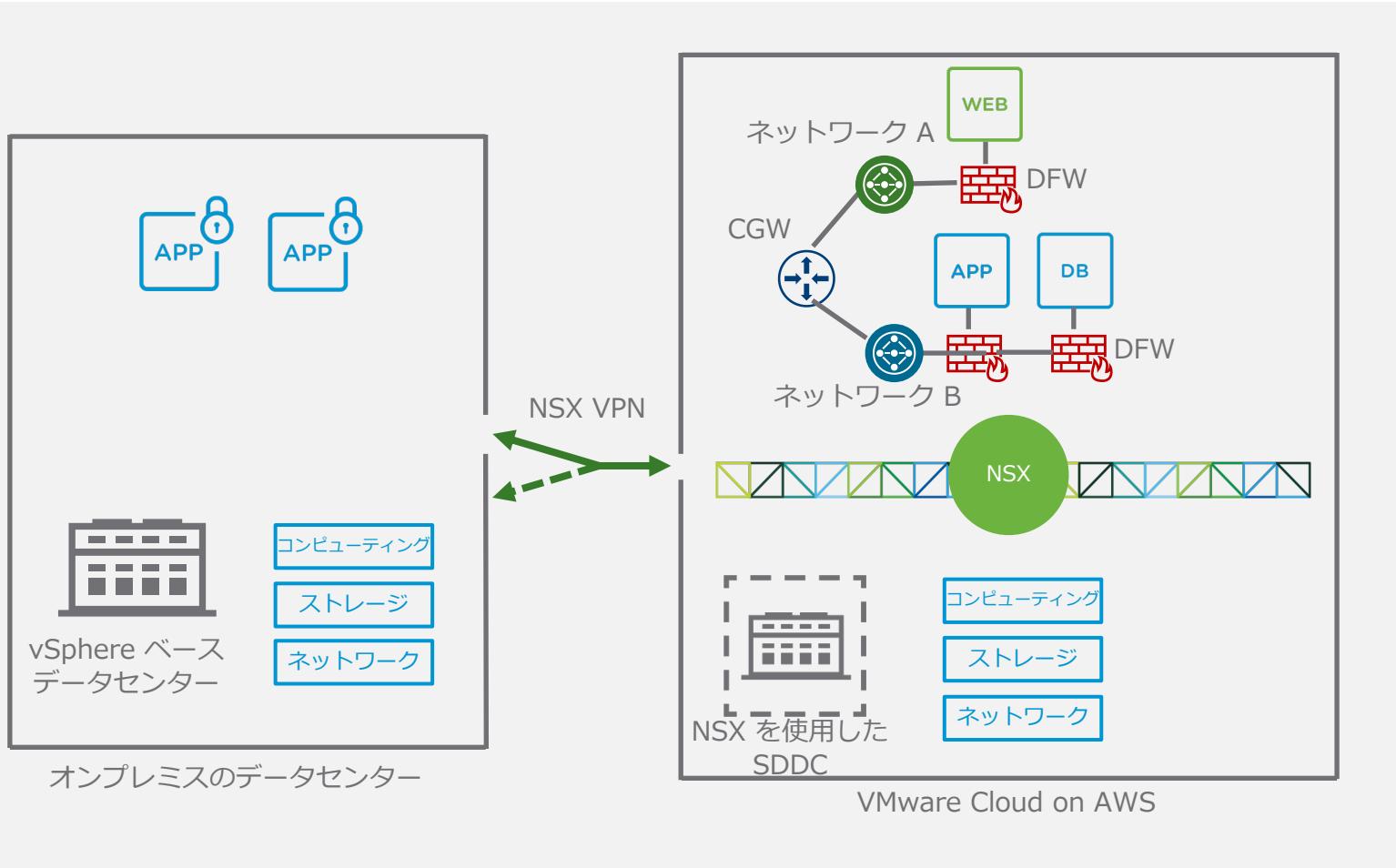
DPDK を使用して、IPsec トンネル トラフィックのスループットとパフォーマンスを向上

# パブリック クラウドでのマイクロセグメンテーション

NSX のセキュリティを VMware Cloud on AWS で利用可能



セキュリティ



VMware Cloud on AWS で実行  
されているワークロード間の  
East-West トラフィックを詳細  
に制御

アプリケーションに基づく簡素化  
されたポリシー（仮想マシン名、  
ユーザー定義のタグなど）

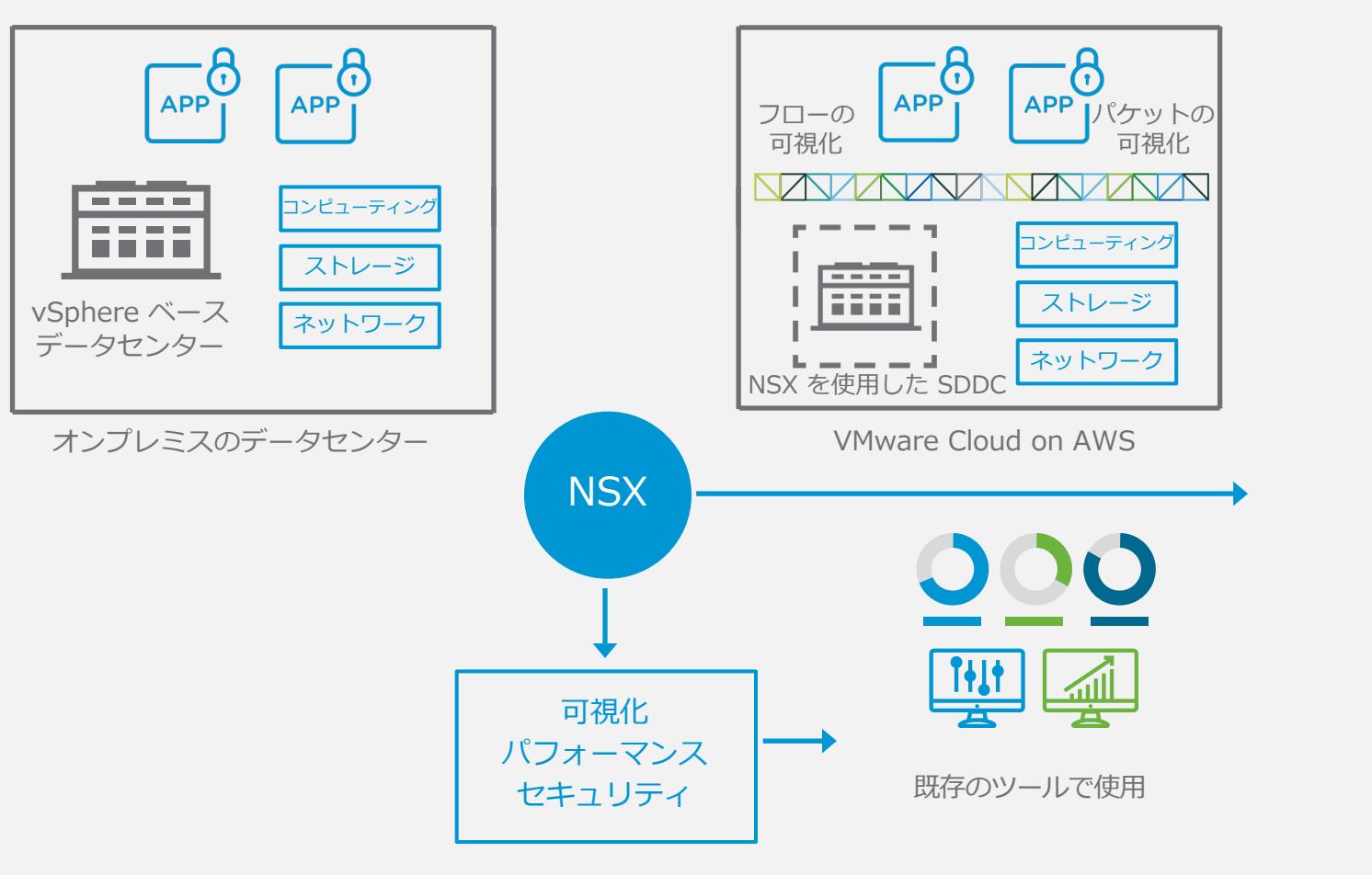
VMware Cloud on AWS SDDC  
内のどこに移動するかにかかわら  
ず、ワークロードにポリシーが  
追隨



# 監視とセキュリティ向けの一貫したツールの使用

## フローおよびパケット レベルでのきめ細かい可視化

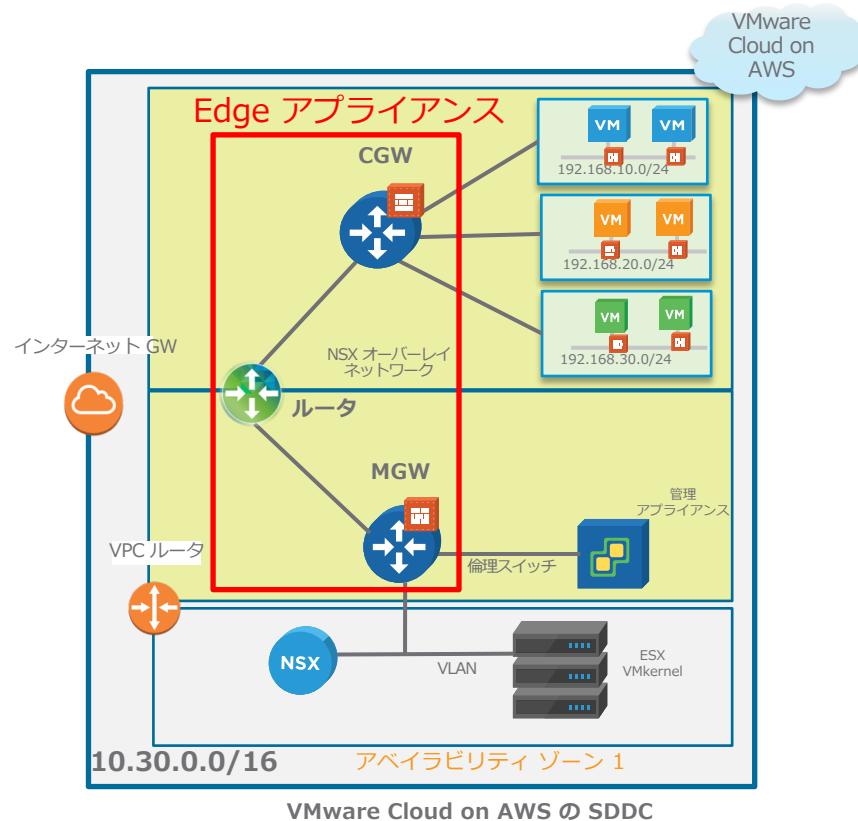
可視化



ネットワーク フローとパケット  
の可視化により、問題を迅速に  
特定、トラブルシューティング

オンプレミスおよび VMware  
Cloud on AWS の既存の可視化  
ツールに接続

# VMware Cloud on AWS : SDDC v1.5



## 1.4 およびそれ以前のバージョンの SDDC と類似した機能

- MGW および CGW モデル
- すべての論理ネットワークが CGW に自動接続

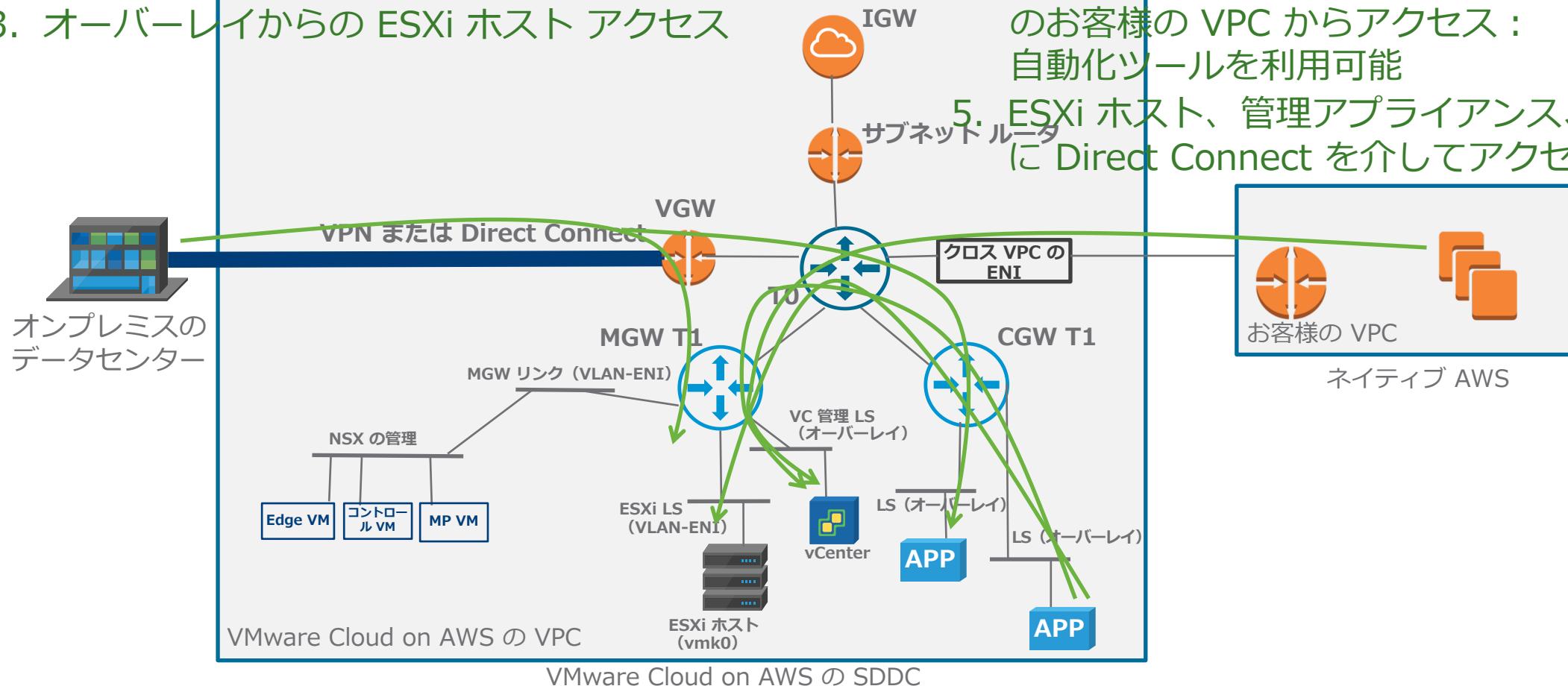
## 1.4 およびそれ以前のバージョンの SDDC との主な相違点

- NSX-T ベースのアーキテクチャ
- Tier 0 および Tier 1 ルータ：
  - \* MGW = T1、CGW = T1
  - \* MGW と CGW は T0 を介して接続
- MGW と CGW は、同じ NSX Edge アプライアンス内の論理的な構成要素
- DPDK ベースの Edge
- ESXi ホスト上の NVDS スイッチ
- 単一 VPN トンネル設計 (T0 が終端)
- オーバーレイ セグメント上の管理アプライアンス
- 東京リージョンのサポート

# NSX アーキテクチャ（論理ビュー）

1. オーバーレイとしての vCenter 管理ネットワーク  
：コンピューティング ワークロード用と同じ運用  
/トラブルシューティング ツールを利用可能
2. CGW の背後のワークロードが T0 を介して MGW  
の背後の管理コンポーネントと通信

3. オーバーレイからの ESXi ホスト アクセス



# VMC 1.5 のネットワークとセキュリティに関する UI のレイアウト

## NSX SDDC のレイアウト

The screenshot shows the VMware Cloud on AWS interface for an NSX SDDC named VMC\_NSX-T\_SDDC located in US West (Oregon). The Networking & Security tab is selected. On the left, a sidebar lists various sections: Overview, Network (Segments, VPN, NAT), Security (Edge Firewall, Distributed Firewall), Inventory (Groups, Services), Tools (IPFIX, Port Mirroring), and System (DNS, Public IPs, Direct Connect, Connected VPC). The main area displays two gateway components: Management Gateway (vCenter NSX) and Compute Gateway (Workloads). The Management Gateway section includes details like Public IP (54.190.245.171), Appliance Subnet (10.73.55.128/25), Infrastructure Subnet (10.73.54.0/23), and 5 Edge Firewall Rules, 4 Groups. The Compute Gateway section includes 5 Segments, 2 Edge Firewall Rules & 1 Distributed Firewall Rules, 5 Groups, 1 Public IP. A network diagram shows connections between the Management Gateway, Internet, On Premises environment, and an Amazon VPC instance (vpc-3cd55b45).

### サポート対象のアドオン：

- 分散ファイアウォール (DFW)
- サービスの追加 (予定)
- ロード バランサー (予定)



### アドオン

- 分散ファイアウォールは最初は無償評価版で提供予定
- サービスはアドオンで有効になる予定

# アジェンダ

## VMware Cloud on AWS と NSX

1. 概要とユースケース
2. VMware Cloud on AWS アーキテクチャにおける NSX
- 3. NSX の機能の詳細情報**
4. デモ
5. オンプレミスの NSX
6. まとめと Q&A

# VMC NSX の機能の詳細情報

## ネットワーク (セグメント、 DNS)

セキュリティ (RBAC、 DFW、 Edge ファイアウォール、 グループ化オブジェクト、 セキュリティ タグ)

接続 (IPsec VPN、 L2VPN、 Direct Connect、 接続された VPC)

運用 (API、 ポート ミラーリング、 IPFIX)

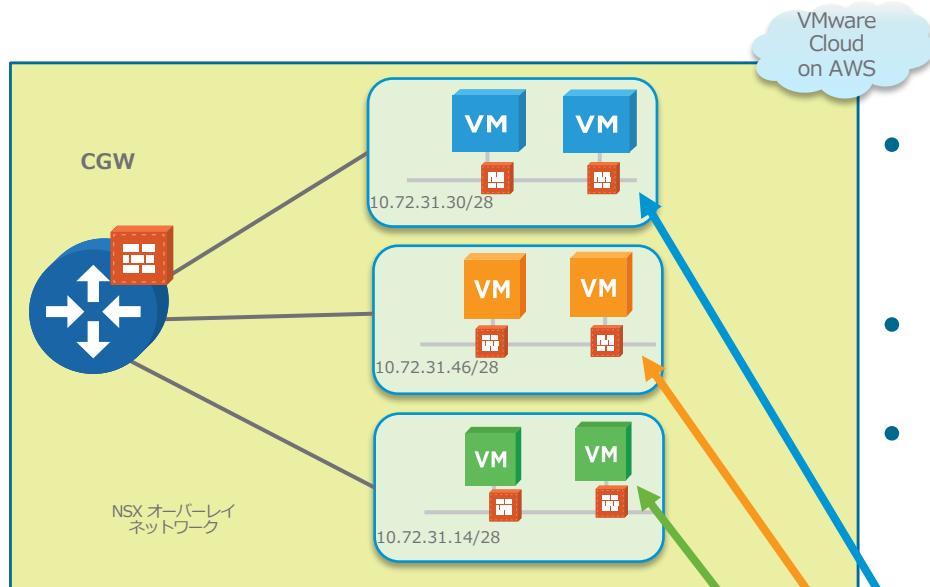
# ネットワーク セグメント

- UI を VMware Cloud on AWS コンソールと完全に統合
- vCenter にネットワーク プラグインなし
- ネットワーク タブは NSX アプライアンスから直接処理

The screenshot shows the VMware Cloud on AWS SDDCs interface. The top navigation bar includes 'Subscriptions', 'Activity Log', 'Tools', and 'Developer Center'. Below the navigation is a secondary header with 'US West (Oregon)', 'Summary', 'Networking & Security', 'Add Ons', 'Troubleshooting', 'Settings', and 'Support'. A dark mode toggle is also present. The main left sidebar has sections for 'Network' (selected), 'Segments' (highlighted in blue), 'VPN', 'NAT', 'Security' (with 'Edge Firewall' and 'Distributed Firewall' options), 'Inventory' (with 'Groups' and 'Services' options), 'Tools' (with 'IPFIX' option), and 'SDDCs' (selected). The main content area is titled 'Network Segments' and contains a table with the following data:

Name	Type	Tunnel ID	Gateway / Prefix Length	DHCP	DHCP IP Range	DNS Suffix
App	Routed		10.72.31.30/28	Disabled		
DB	Routed		10.72.31.46/28	Disabled		
Monitoring	Routed		10.72.31.62/28	Disabled		
Web	Routed		10.72.31.14/28	Disabled		
sddc-cgw-network-1	Routed		192.168.1.1/24	Enabled	192.168.1.2-192.168.1.254	

# ネットワーク セグメント



- あらゆるネットワーク操作を容易に実行し、アクセスを制御
- ルーテッド ネットワークまたは拡張ネットワークを構築
- DHCP サーバを CGW にローカル接続して提供

A screenshot of the VMware Cloud on AWS management interface. The top navigation bar includes "VMware Cloud on AWS", "SDDC", "Subscriptions", "Activity Log", "Tools", and "Developer Center". The main menu on the left lists "Network", "Segments", "VPN", "NAT", "Security", "Edge Firewall", "Distributed Firewall", "Inventory", "Groups", "Services", "Tools", and "IPFIX". The "Segments" tab is currently selected. The main content area is titled "Network Segments" and contains a table with the following data:

Name	Type	Tunnel ID	Gateway / Prefix Length	DHCP	DHCP IP Range	DNS Suffix
App	Routed		10.72.31.30/28	Disabled		
DB	Routed		10.72.31.46/28	Disabled		
Monitoring	Routed		10.72.31.62/28	Disabled		
Web	Routed		10.72.31.14/28	Disabled		
sddc-cgw-network-1	Routed		192.168.1.1/24	Enabled	192.168.1.2-192.168.1.254	

# DNS ゾーン

## NSX SDDC DNS

- 最大 5 個の DNS ゾーンをサポート

The screenshot shows the NSX SDDC DNS configuration interface. On the left, a sidebar lists various system components: Security (Edge Firewall, Distributed Firewall), Inventory (Groups, Services), Tools (IPFIX, Port Mirroring), System (DNS, Public IPs). The DNS option is currently selected. The main panel displays the Compute Gateway configuration, including the DNS Service IP (10.73.55.140) and a message stating "Maximum of 5 DNS zones can be configured for the DNS on the Compute Gateway". Below this, there is an "ADD DNS ZONE" button and a search bar. A table lists the three configured DNS zones:

Name	Domain Name	DNS Server 1	DNS Server 2
prod	d1.myCompany.com	10.30.30.5	10.30.30.6
dev	d2.myCompany.com	10.29.29.5	10.29.29.6
defaultZone	Any	8.8.8.8	8.8.4.4

# VMC NSX の機能の詳細情報

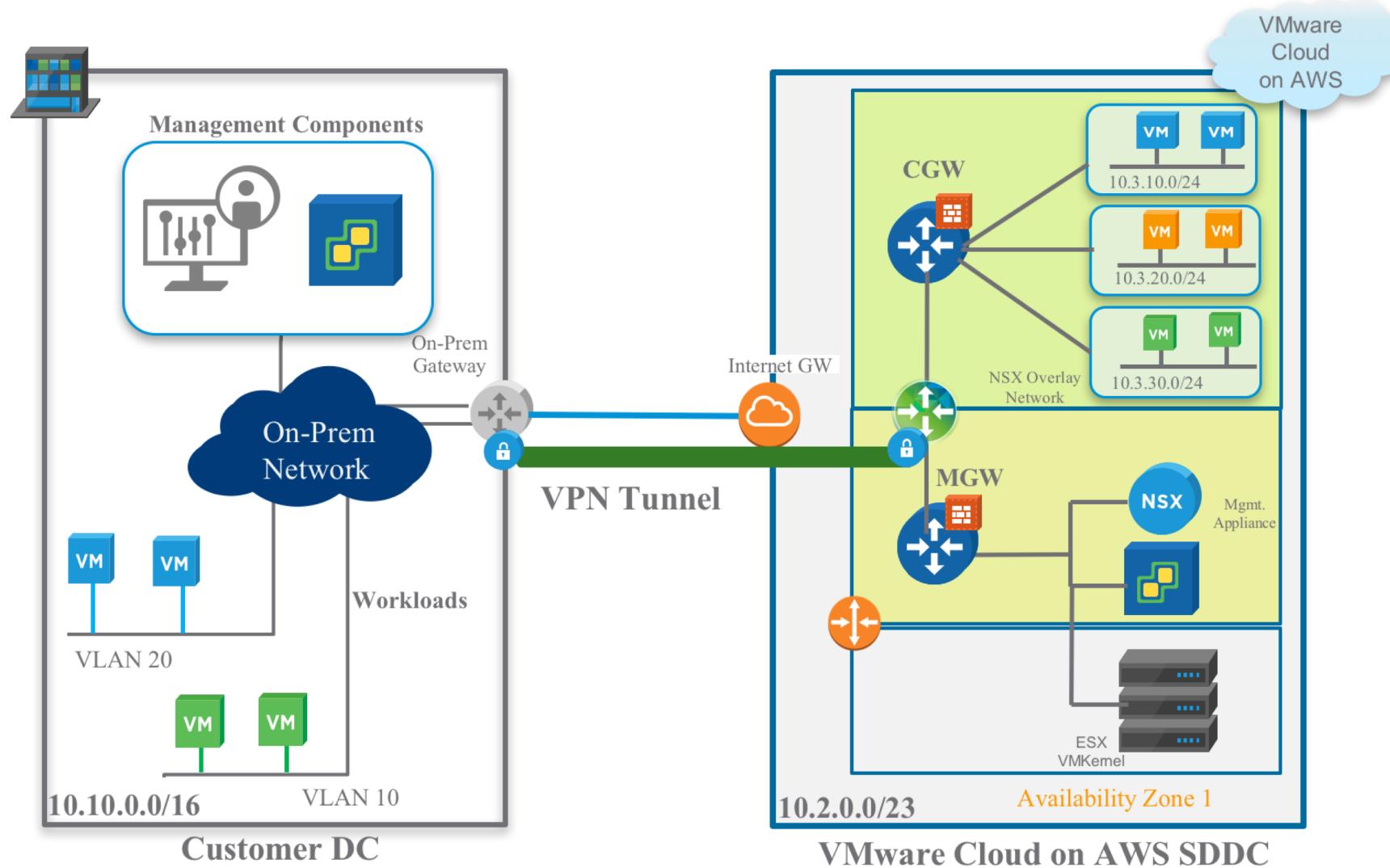
ネットワーク（論理スイッチ、DNS）

## 接続（IPsec VPN、L2VPN、Direct Connect、接続された VPC）

セキュリティ（RBAC、DFW、Edge ファイアウォール、グループ化オブジェクト、セキュリティ タグ）

運用（API、ポート ミラーリング、IPFIX）

# IPsec VPN の機能強化



# IPsec VPN の機能強化

	SDDC バージョン 1.4 および それ以前のバージョン	SDDC バージョン 1.5
<b>VPN のタイプ</b>	ポリシー ベースの VPN	ポリシー ベースの VPN ルート ベースの VPN
<b>IKE のバージョン</b>	IKEv1	IKEv1、IKEv2、IKE Flex
<b>DH グループ</b>	DH 2、5、14、15、16	DH 14、15、16
<b>ダイジェスト アルゴリズム</b>	SHA1	SHA1、SHA256、Null
<b>暗号化アルゴリズム</b>	AES 128、AES 256	AES 128、AES 256、AES GCM 128、AES GCM 192、AES GCM 256
<b>PH1 および PH2 パラメーター</b>	限られたオプション	オプションの増加、PH1 パラメーターと PH2 パラメーターで異なる設定が可能
<b>VPN の数</b>	4 個のポリシー ベース VPN	VMC 内に 16 個のポリシー ベース VPN + 16 個のルート ベース VPN の規模（検証済みの制限）

# ルートベースの IPsec VPN

## メリット：

- 冗長性を提供：2 台の異なるオンプレミス エッジ デバイスに VPN トンネルを設定
  - \* アクティブ/パッシブ設計が可能
- VMware Cloud on AWS の SDDC とオンプレミスからネットワークを自動的に学習
  - \* 新しいネットワークのアドバタイズ時に追加構成は不要

# ルートベースの IPsec VPN

## メリット：

The screenshot shows the VMware Cloud on AWS interface for configuring a Route Based VPN. The left sidebar shows navigation options like SDDCs, Subscriptions, Activity Log, Tools, and Developer Center. The main area is titled "Route Based VPN" and contains a table for adding a new VPN entry. The table has columns for Name, Local IP Address, Remote Public IP, Remote Private IP, BGP Neighbor, VTI IP/Prefix Length, and Stats. The "Name" field is set to "To\_On\_Prem". The "Local IP Address" dropdown is set to "Public IP". The "Remote Public IP" dropdown is set to "IP Address" and contains "154.0.0.1". The "BGP Neighbor" dropdown is set to "SET BGP NEIG..." and contains "10.79.1.1/30". Below the table, there are sections for Advanced settings: Tunnel Encryption (AES 256), IKE Encryption (AES 256), Tunnel Digest Algorithm (SHA 2), IKE Digest Algorithm (SHA 2), Perfect Forward Secrecy (Enabled), IKE Type (IKE V2), Preshared Key (Test24!7qy1), and Diffie Hellman (Group 14). At the bottom of the configuration panel are "SAVE" and "CANCEL" buttons.

	Name	Local IP Address	Remote Public IP	Remote Private IP	BGP Neighbor	VTI IP/Prefix Length	Stats
1	To_On_Prem *	Publ...	154.0.0.1 *	IP Address	SET BGP NEIG...	10.79.1.1/30 *	

Advanced

Tunnel Encryption	AES 256	IKE Encryption	AES 256
Tunnel Digest Algorithm	SHA 2	IKE Digest Algorithm	SHA 2
Perfect Forward Secrecy	Enabled	IKE Type	IKE V2
Preshared Key *	Test24!7qy1	Diffie Hellman	Group 14

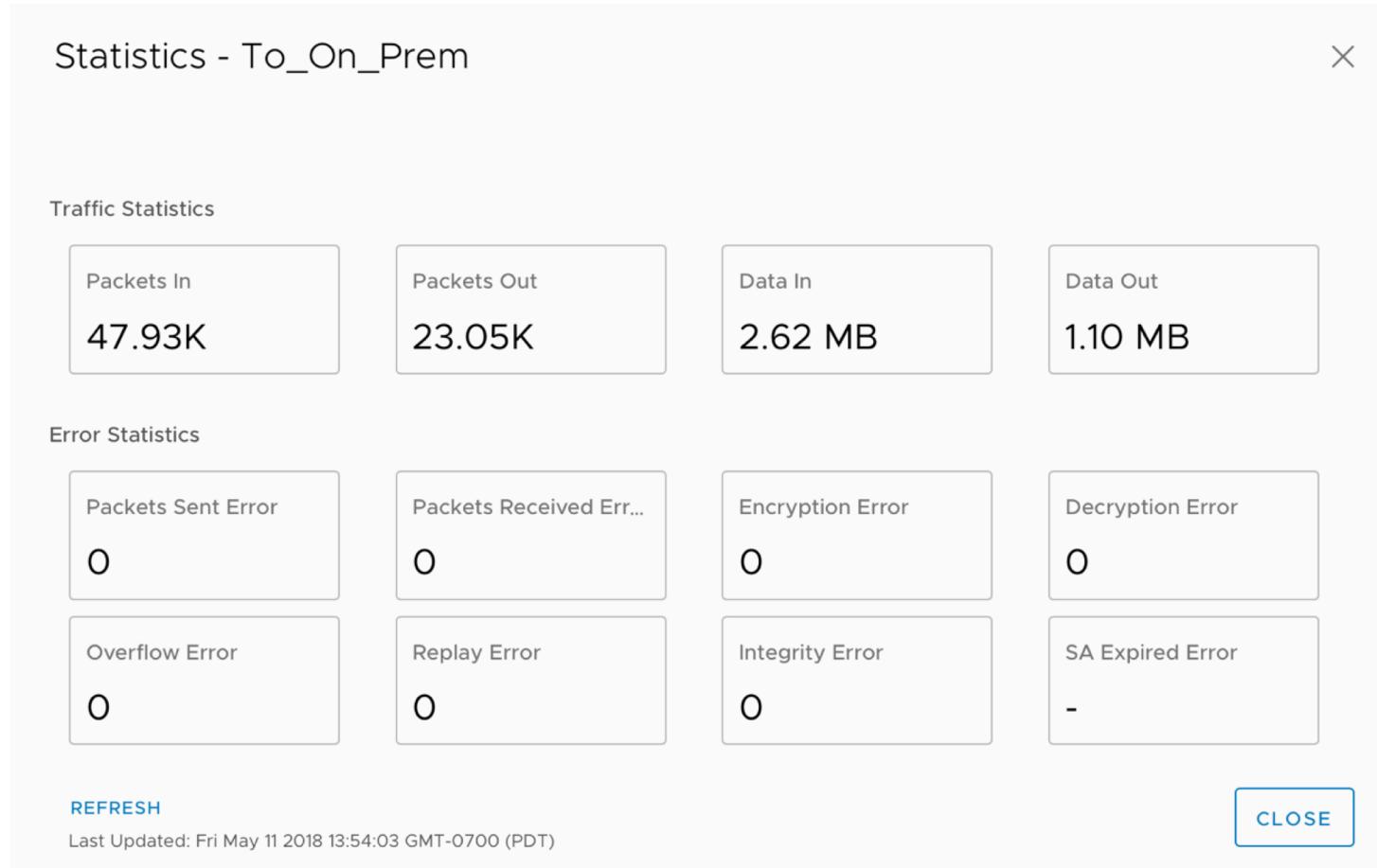
REFRESH

Last Updated: Fri May 11 2018 13:54:03 GMT-0700 (PDT)

CLOSE

# ルートベースの IPsec VPN

## メリット：



# ルートベースの IPsec VPN

## メリット：

Set BGP Neighbor - To\_On\_Prem

Select BGP Neighbor Maximum 1

ADD NEIGHBOR

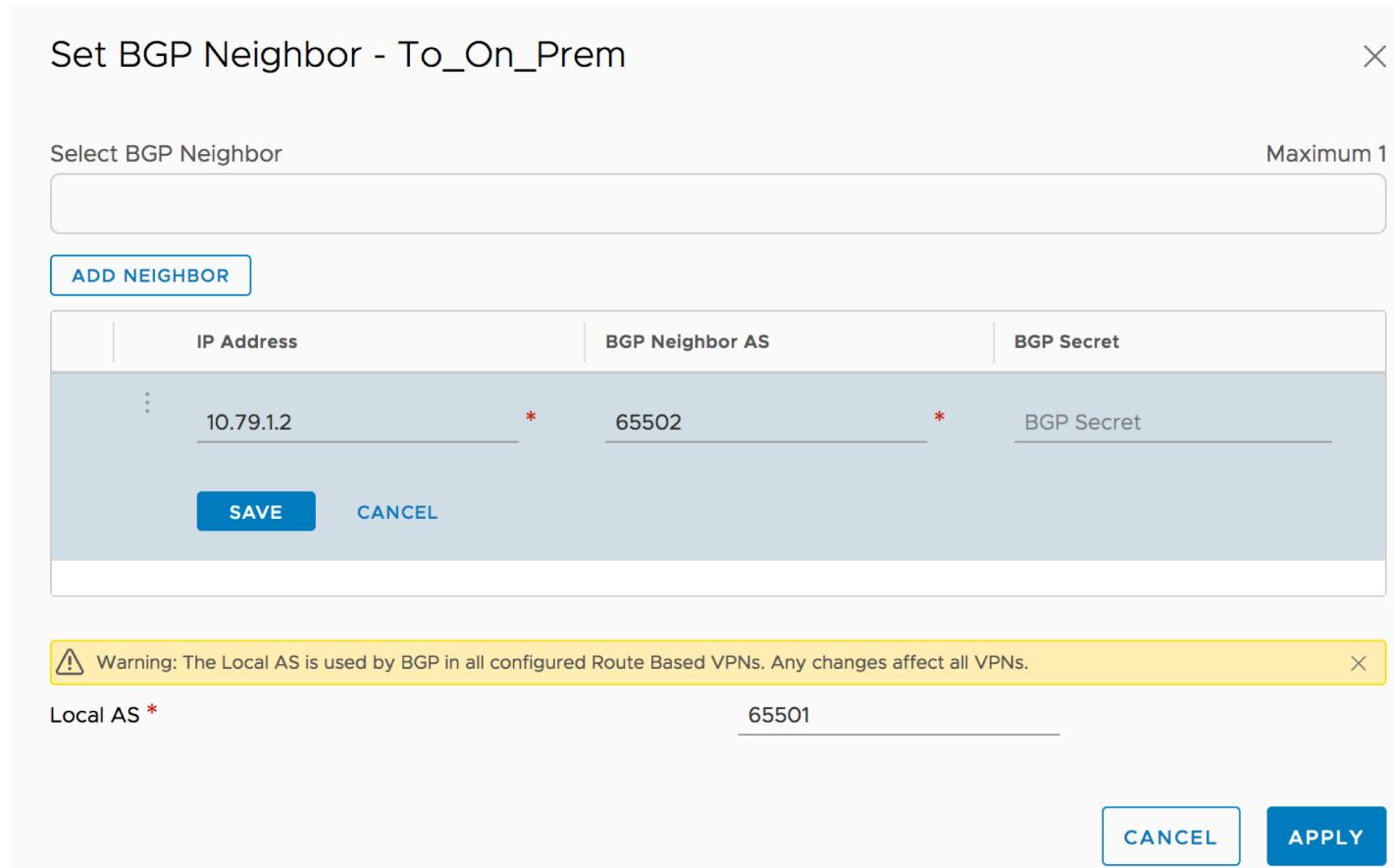
	IP Address	BGP Neighbor AS	BGP Secret
:	10.79.1.2 *	65502 *	BGP Secret

SAVE CANCEL

⚠ Warning: The Local AS is used by BGP in all configured Route Based VPNs. Any changes affect all VPNs.

Local AS \* 65501

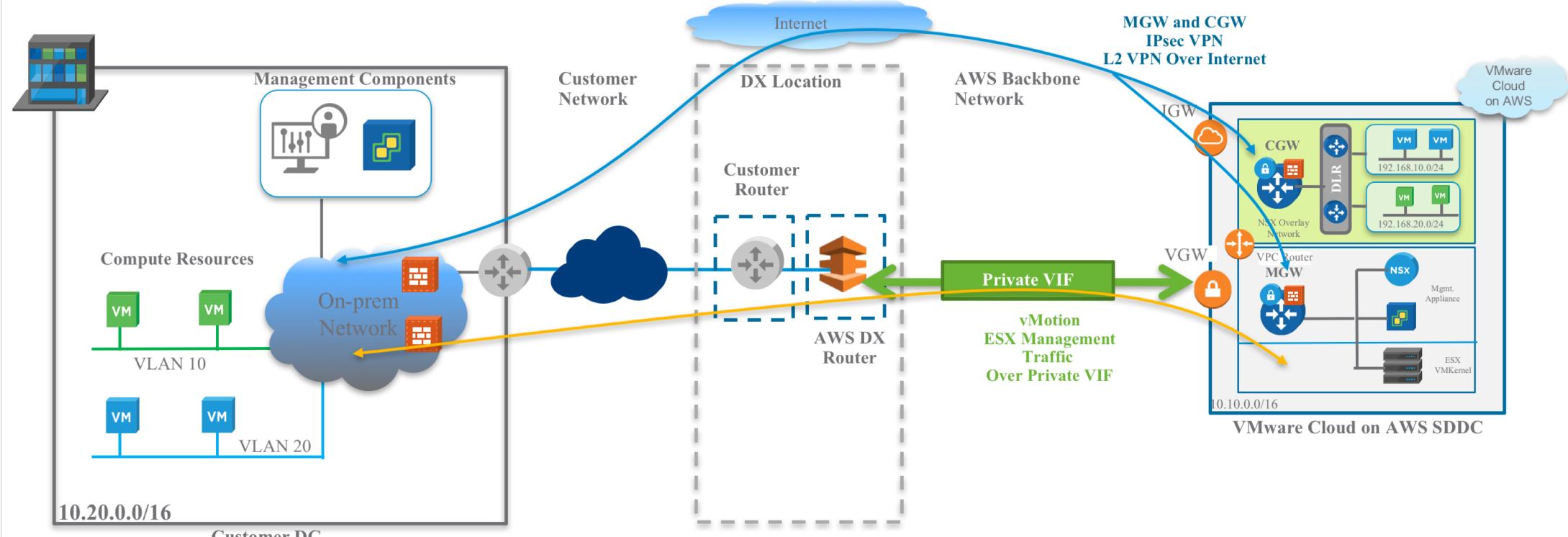
CANCEL APPLY



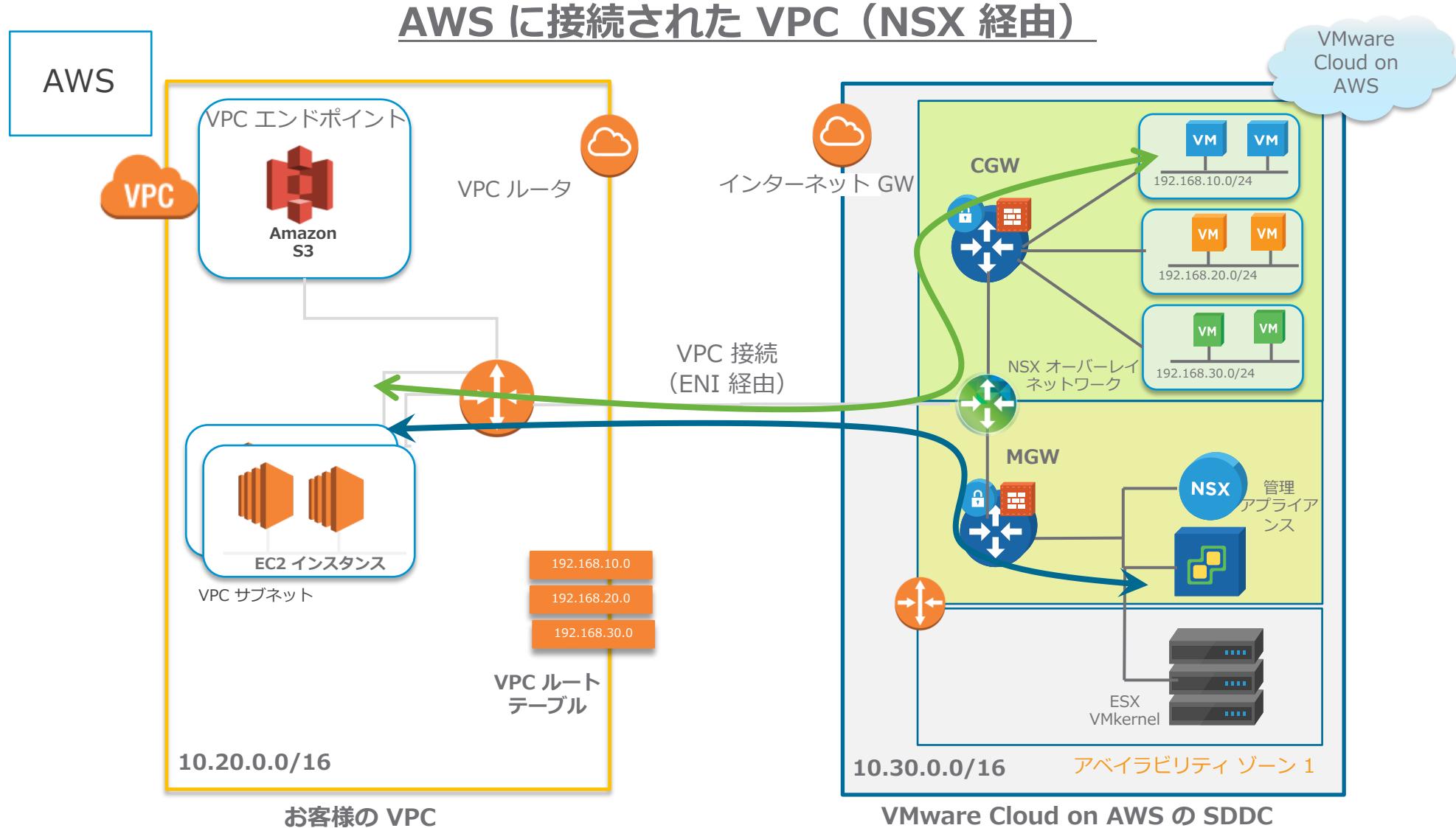
# すべてのトラフィックを送信する Direct Connect プライベート仮想インターフェイス

- 以前のバージョンの SDDC では、ESXi の管理トラフィックと vMotion/クラウドマイグレーションのトラフィックのみを Direct Connect とプライベート仮想インターフェイスでネイティブサポート
  - \* 以前は、ワークロード トラフィックと管理アプライアンス トラフィックの送信に VPN が必要

- SDDC バージョン 1.5 では、すべてのトラフィックを Direct Connect でネイティブサポート



# VMware Cloud on AWS に接続された VPC とのアクセスの管理



# VMC NSX の機能の詳細情報

ネットワーク（論理スイッチ、DNS）

接続（IPsec VPN、L2VPN、Direct Connect、接続された VPC）

**セキュリティ（RBAC、DFW、Edge ファイアウォール、グループ化オブジェクト、セキュリティ タグ）**

運用（API、ポート ミラーリング、IPFIX）

# RBAC

NSX Cloud Auditor : [Networking and Security] タブへの読み取り専用アクセス

NSX Cloud Admin : [Networking and Security] タブへの読み取り/書き込みアクセス

## Add New Users

Add/Invite new users to your organization NSBU PM - M4 NSX-V and allow access to the organization and services.  
Invitation emails will be sent to the following email addresses.

### Email Addresses

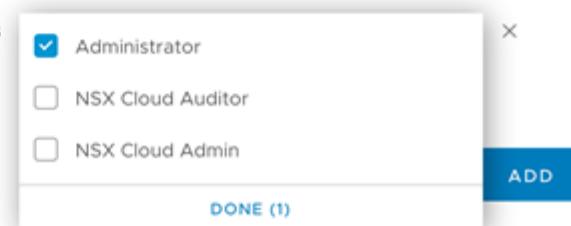
 X

### Role Assignment

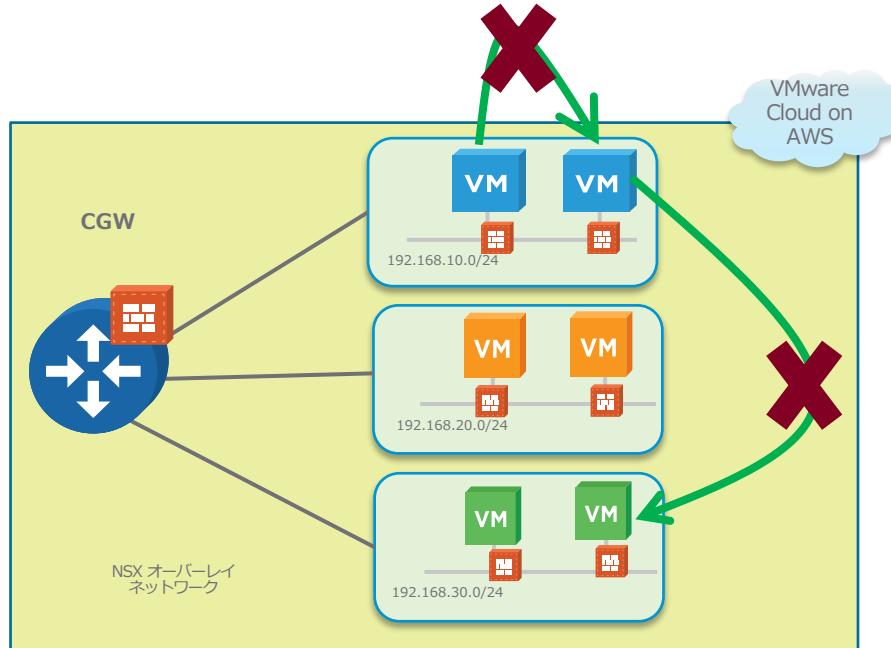
Role in organization Organization Owner ▾

Support User

Roles in service VMware Cloud on AWS ▾ with roles



# 分散ファイアウォール (DFW)



- 高度なマイクロセグメンテーションのセキュリティ
- 2 層のセキュリティ : Edge レベルと仮想マシン レベル
- 1 つの CGW 設計でもマルチテナントが可能 (IP の重複なし)
- ネットワークを容易に分離可能 (本番、テスト、開発)
- DMZ 環境を容易に構築可能

✓ ワークロードをクラウドに移行しても、オンプレミス環境と同レベルのセキュリティを実現可能

VMware Cloud on AWS

SDDCs Subscriptions Activity Log Tools Developer Center

VMC\_NSX-T\_SDDC US West (Oregon) > Summary Networking & Security Add Ons Troubleshooting Settings Support

DARK

REVERT PUBLISH

Overview Network Segments VPN Route Based Policy Based Layer 2 NAT Security Edge Firewall Distributed Firewall

Emergency Rules Rules: 0

Infrastructure Rules Rules: 0

Environment Rules Rules: 0

Application Rules Rules: 1

Default - Allow All

IT (1)

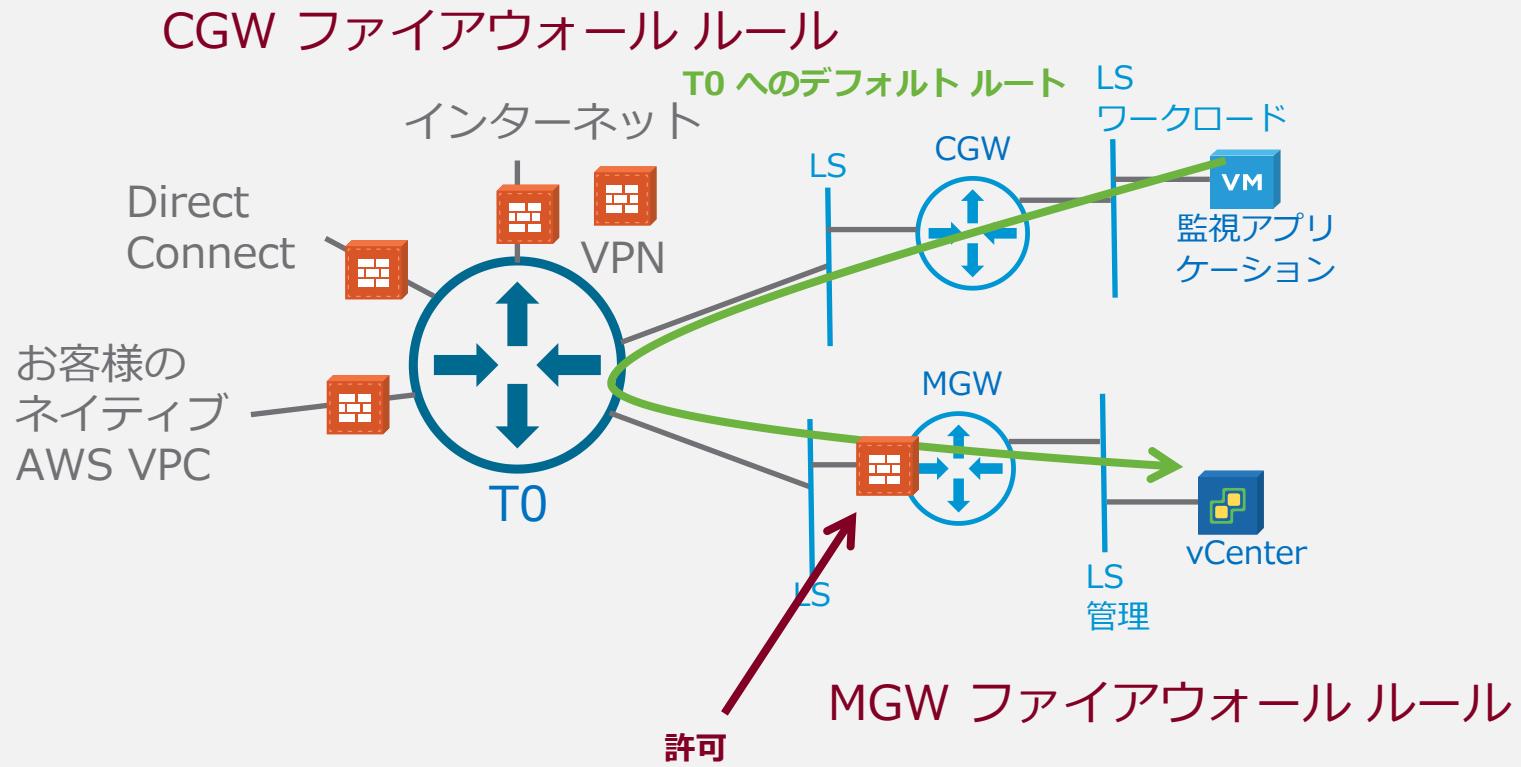
Name Sources Destinations Services Action Logging

Web to DB Web DB Any Drop Disabled

	Name	Sources	Destinations	Services	Action	Logging
IT (1)	Web to DB	Web	DB	Any	Drop	Disabled

Distributed Firewall

# Edge ファイアウォール



## 機能

特定のインターフェイス (CGW) および MGW 上の Edge ファイアウォール機能

\* CGW ファイアウォール ルールを T0 アップリンクインターフェイスに適用

\* MGW ファイアウォール ルールを T1 アップリンクに適用

## メリット

- インターフェイスごとのきめ細かな Edge ファイアウォール ルール
- DFW と同じグループ化オブジェクトを使用して、DFW と Edge の整合性を確保
- 管理アプライアンスの場合は、1 か所のみにアクセスしてルールを構成

# Edge ファイアウォール

VMware Cloud on AWS

SDDCs Subscriptions Activity Log Tools Developer Center

VMC\_NSX-T\_SDDC US West (Oregon) Summary Networking & Security Add Ons Troubleshooting Settings Support

DARK BLISH

Overview Network Segments  
VPN Route Based Policy Based Layer 2 NAT Security Edge Firewall Distributed Firewall Inventory Groups Services Tools IPFIX

Edge Firewall

Select Source(s)

Management Gateway 6 Rules

Compute Gateway 4 Rules

ADD NEW RULE

Name	Member Type	Members	Group Type
App to AWS Na Workloads	*	System Defined	
From On-Prem Workloads	Membership Criteria	Tag equals App	User Defined
Default VTI Rule	IP Address	172.31.0.0/16	System Defined
Default Uplink R	Membership Criteria	Tag equals DB	User Defined
Default Deny All	IP Address	0.0.0.0/0	System Defined

REFRESH 1 - 8 of 8 Groups

CREATE NEW GROUP CANCEL SAVE

©2018 VMware, Inc.

# グループ化オブジェクト

次の要素に基づくグループをサポート：

- IP アドレス
- 仮想マシン インスタンス
- 仮想マシン名の一致条件
- セキュリティ タグの一致条件

The screenshot shows the VMware Cloud on AWS SDDC Management interface. The top navigation bar includes links for SDDCs, Subscriptions, Activity Log, Tools, and Developer Center. The main header displays the SDDC name "VMC\_NSX-T\_SDDC" and its location "US West (Oregon)". The left sidebar contains navigation links for Overview, Network, Security, Inventory, and Tools, with "Groups" selected. The main content area is titled "Groups" and shows three categories: Management Groups (4 Groups), Workload Groups (5 Groups), and Virtual Machines (5 VMs). A sub-section for "Workload Groups" is expanded, showing five entries: App, DB, On-Prem Workloads, Web, and Wireshark. Each entry has a "Name", "Member Type", and "Members" column. An "ADD GROUP" button is located at the top right of the group list. The bottom of the screen features the VMware logo and the copyright notice "©2018 VMware, Inc."

Name	Member Type	Members
App	Membership Criteria	Tag equals App
DB	Membership Criteria	Tag equals DB
On-Prem Workloads	IP Address	10.114.223.64/28
Web	Membership Criteria	Tag equals Web
Wireshark	IP Address	10.72.31.49

©2018 VMware, Inc.

# セキュリティ タグ

セキュリティ タグをサポート

- コンソールからのセキュリティ タグの作成と添付の統合

The screenshot shows the VMware Cloud on AWS SDDCs interface. The top navigation bar includes 'vm' icon, 'VMware Cloud on AWS', 'SDDCs' (which is underlined), 'Subscriptions', 'Activity Log', 'Tools', and 'Developer Center'. Below the navigation is a breadcrumb 'VMC\_NSX-T\_SDDC' and a location indicator 'US West (Oregon)'. The main menu has tabs: 'Summary', 'Networking & Security', 'Add Ons', 'Troubleshooting', 'Settings', and 'Support'. On the left, a sidebar menu lists 'Overview', 'Network' (Segments, VPN, NAT), 'Security' (Edge Firewall, Distributed Firewall), 'Inventory' (Groups, Services), and 'Tools' (IPFIX, Port Mirroring). The 'Groups' item in the 'Inventory' section is highlighted. The main content area is titled 'Groups' and shows two sections: 'Management Groups' (4 Groups) and 'Workload Groups' (5 Groups). A table lists five virtual machines with their names and tags:

Name	Tags
App	App
DB	DB
Web	Web
Web2	Web
Wireshark	

# VMC NSX の機能の詳細情報

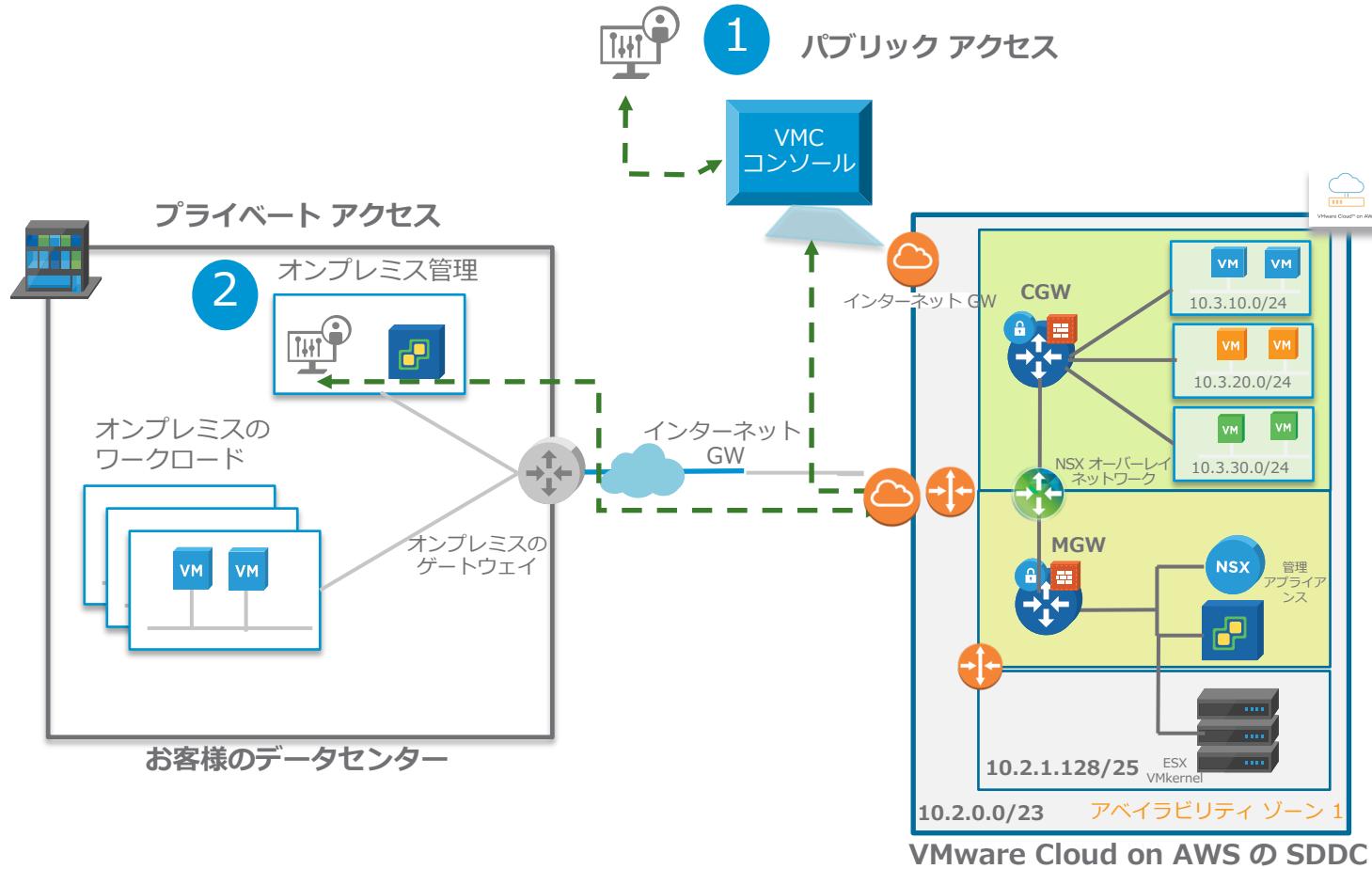
ネットワーク（論理スイッチ、DNS）

接続（IPsec VPN、L2VPN、Direct Connect、接続された VPC）

セキュリティ（RBAC、DFW、Edge ファイアウォール、グループ化オブジェクト、セキュリティ タグ）

**運用（API、ポートミラーリング、IPFIX）**

# NSX API



## 概要

- NSX API には、パブリック エンドポイントとプライベート エンドポイントを介してアクセス可能
- パブリック エンドポイントはパブリック IP を持つ VMC コンソール：インターネットを介してアクセス可能
- プライベート エンドポイントはプライベート IP を持つ NSX ポリシー アプライアンス：VPN トンネルまたは Direct Connect を介してアクセス可能

## メリット

- ネットワークのプロビジョニングとセキュリティ機能の自動化

## ユースケース

- 導入初日の自動化
- 導入後の自動化

# 運用ツール

IPFIX: SDDC内のトラフィックを監視/分析ツクを詳細に可視化

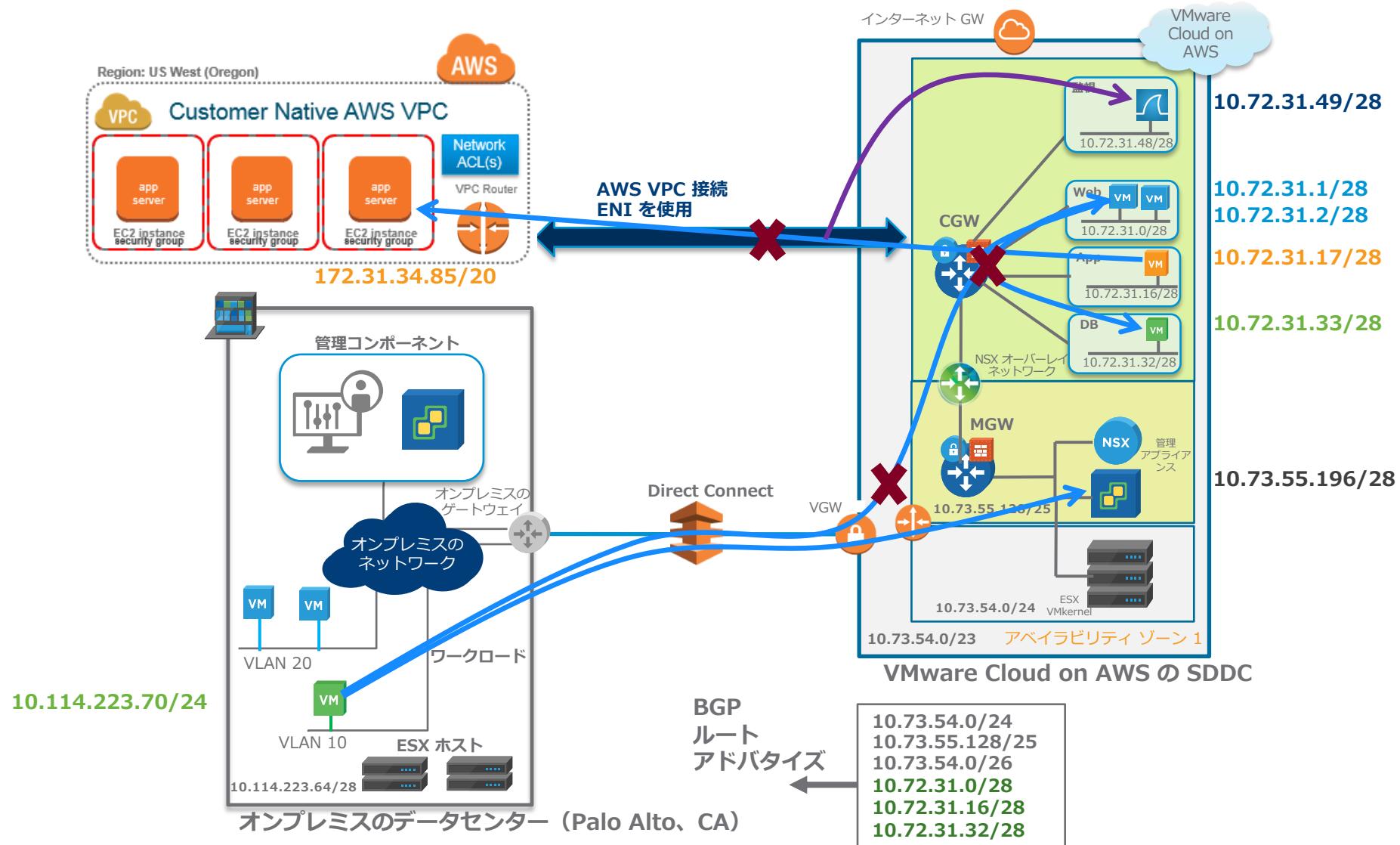
The screenshot shows the VMware Cloud on AWS web interface for managing SDDCs. The top navigation bar includes links for SDDCs, Subscriptions, Activity Log, Tools, and Developer Center, along with a location indicator for US West (Oregon) and user profile information (NSBU PM - M4 NSX-T). The main content area is titled "VMC\_NSX-T\_SDDC". On the left, a sidebar lists various management categories: Overview, Network (Segments, VPN, NAT), Security (Edge Firewall, Distributed Firewall), Inventory (Groups, Services), Tools (IPFIX, Port Mirroring, System), and System. The "Port Mirroring" option under Tools is currently selected. The main pane displays the "Port Mirroring" configuration page. It features a summary message: "Only Groups with a maximum of 5 VMs is supported on Source. Destination Group can only contain 1 IP Address. A session once created, Source Group cannot be modified". Below this is a "ADD PORT MIRRORING SESSION" button and a search bar. A table lists the current port mirroring session: "To Wireshark" (Source: Web, Destination: Wireshark, Direction: BIDIRECTIONAL, Status: Up). The entire interface is presented in a dark-themed layout.

# アジェンダ

## VMware Cloud on AWS と NSX

1. 概要とユースケース
2. VMware Cloud on AWS アーキテクチャにおける NSX
3. NSX の機能の詳細情報
4. デモ
5. オンプレミスの NSX
6. まとめと Q&A

# VMware Cloud on AWS と NSX v1.5 のデモ



# アジェンダ

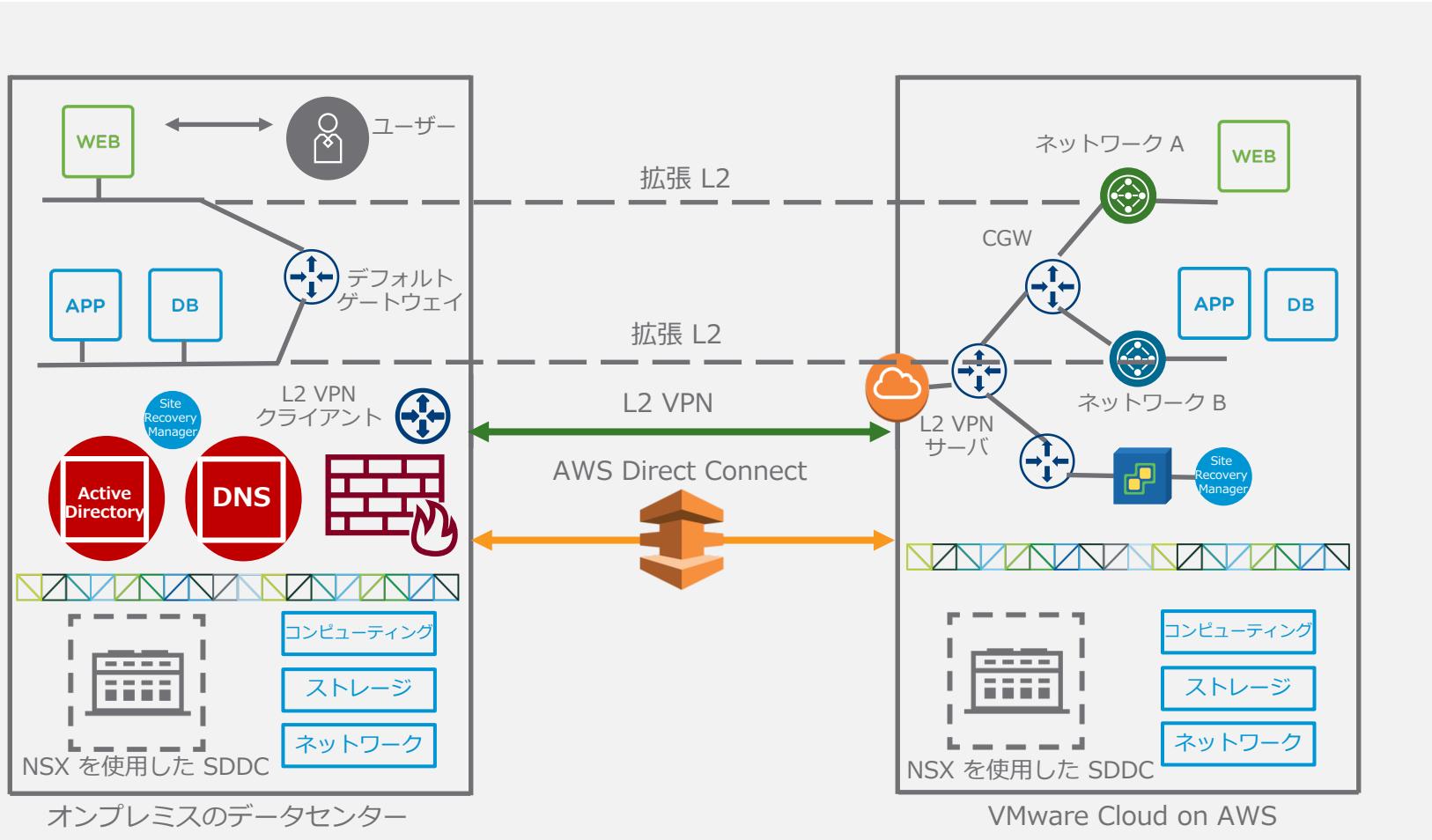
## VMware Cloud on AWS と NSX

1. 概要とユースケース
2. VMware Cloud on AWS アーキテクチャにおける NSX
3. NSX の機能の詳細情報
4. デモ
- 5. オンプレミスの NSX**
6. まとめと Q&A

# オンプレミス NSX の価値

ハイブリッド クラウドのユースケースが可能

ネットワークとセキュリティの仮想化



## NSX のメリット

ディザスタ リカバリ用のネットワーク

- 分離されたネットワーク
- マルチティア ルーティング

外部サービスへの接続性

- VMware Cloud on AWS からのオンプレミス インフラストラクチャ リソースへのアクセス
- L2 VPN を介した L2 延伸ネットワーク

エンドツーエンドのディザスタ リカバリ テスト

- ディザスタ リカバリ ネットワークへのアクセスを可能にする NAT または SSL-VPN
- エンド ユーザーのためのディザスタ リカバリ 計画 テストをサポート

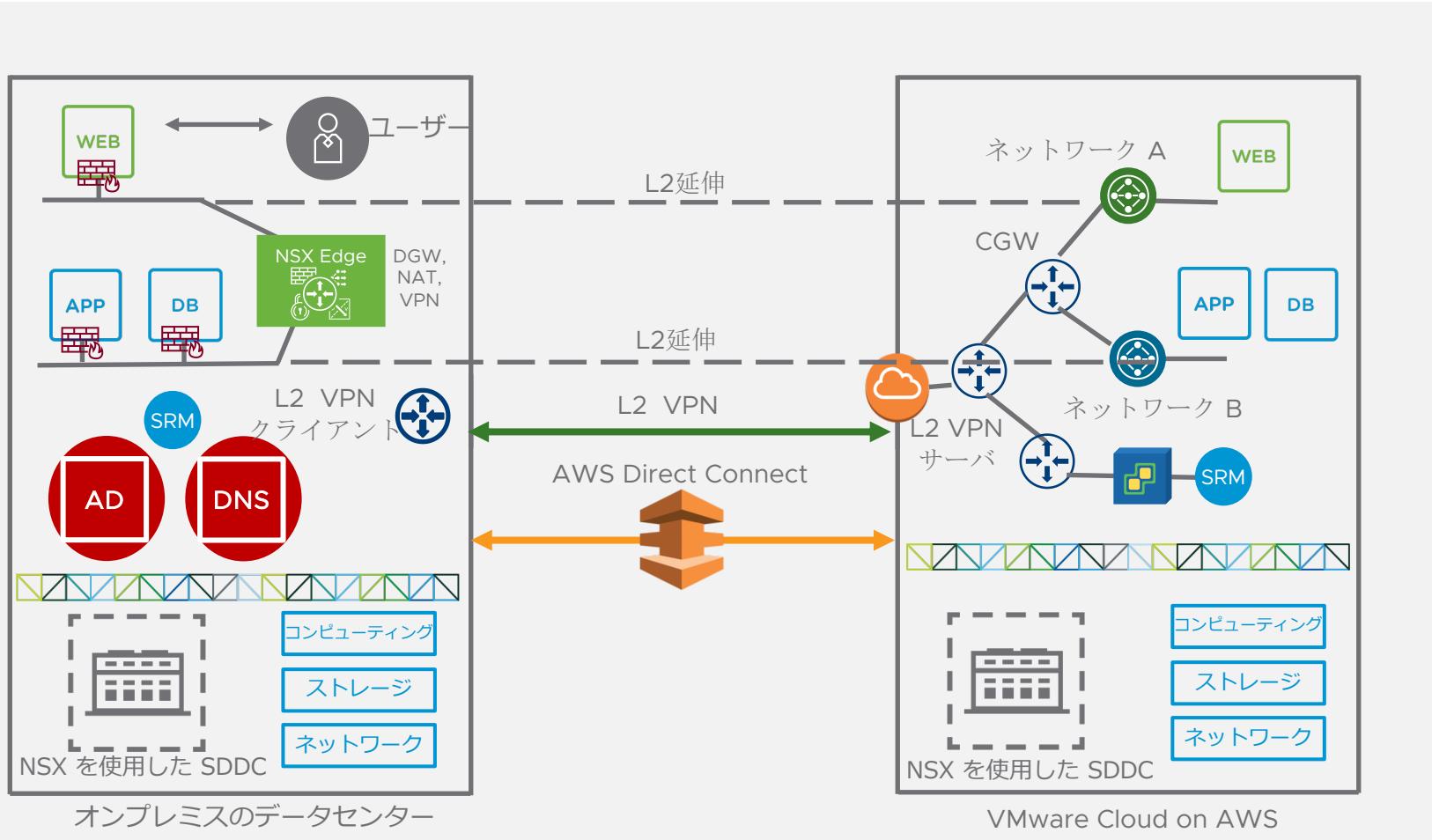
マイクロセグメンテーション

- オンプレミスの NSX を使用してマイクロセグメンテーションを有効化
- プランニングと可視化のための豊富な機能
- セキュリティ ポリシーをワークLOADと一緒に VMware Cloud on AWS に移動

# オンプレミス NSX の価値

ハイブリッド クラウドのユースケースが可能

ネットワークとセキュリティの仮想化



## NSX のメリット

ディザスタ リカバリ用のネットワーク

- 分離されたネットワーク
- マルチティア ルーティング

外部サービスへの接続性

- VMware Cloud on AWS からのオンプレミス インフラストラクチャ リソースへのアクセス
- L2 VPN を介した L2 延伸ネットワーク

エンドツーエンドのディザスタ リカバリ テスト

- ディザスタ リカバリ ネットワークへのアクセスを可能にする NAT または SSL-VPN
- エンド ユーザーのためのディザスタ リカバリ 計画 テストをサポート

マイクロセグメンテーション

- オンプレミスの NSX を使用してマイクロセグメンテーションを有効化
- プランニングと可視化のための豊富な機能
- セキュリティ ポリシーをワークLOADと一緒に VMware Cloud on AWS に移動

# アジェンダ

## VMware Cloud on AWS と NSX

1. 概要とユースケース
2. VMware Cloud on AWS アーキテクチャにおける NSX
3. NSX の機能の詳細情報
4. デモ
5. オンプレミスの NSX
6. まとめと Q&A

# 重要なポイント

VMware Cloud on AWS と NSX が可能にする機能：

ハイブリッド接続モデルの選択

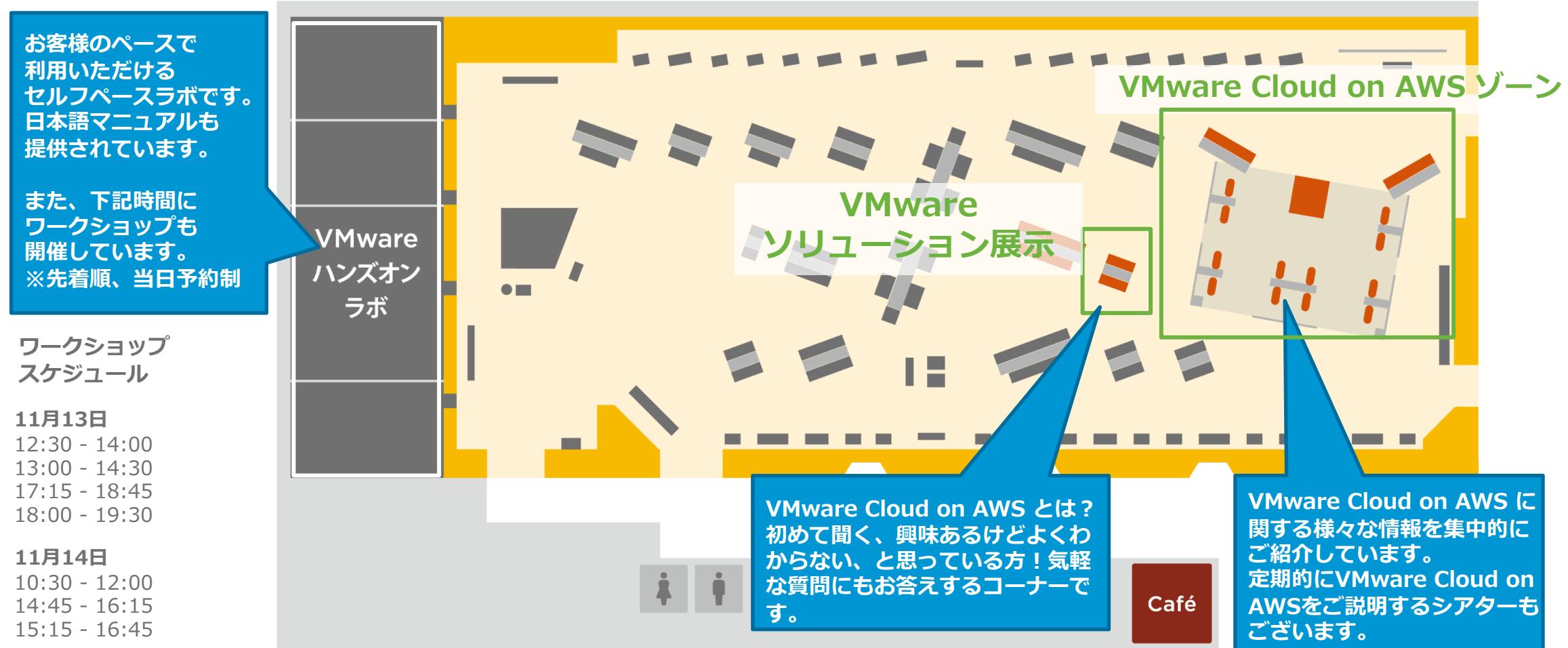
North-South (Edge) および East-West (分散) ファイアウォールを使用した、  
アプリケーション向けのセキュリティ強化



一貫した運用モデルと可視化による  
パフォーマンスおよび接続の問題の特定



# 本セッションに関連する展示・ハンズオンラボのご紹介



# Arigato Gozaimasu / Thank You !

[rbudavari@vmware.com](mailto:rbudavari@vmware.com)