

VMware NSX Data Center

主なメリット

- ワークロード レベルでのマイクロセグメンテーションときめ細かなセキュリティによりアプリケーションを保護
- 自動化により、ネットワークのプロビジョニングの所要時間を数日から数秒まで短縮し、運用効率を向上
- 複数のデータセンターやネイティブ パブリック クラウドにわたり、物理ネットワークのトポロジーに依存せず、ネットワークおよびセキュリティ ポリシーを一貫して管理

VMware NSX® Data Center は、VMware が提唱する Virtual Cloud Network のビジョンを実現するネットワーク仮想化とセキュリティのプラットフォームです。データセンター、クラウド、アプリケーション フレームワークにまたがるネットワークをソフトウェア ベースのアプローチで構築できます。仮想マシンからコンテナ、ベアメタル サーバまで、アプリケーションの実行場所を問わずにネットワークとセキュリティをアプリケーションのより近くに構成できるほか、仮想マシンの運用モデルと同様に、ネットワークを基盤となるハードウェアから独立してプロビジョニングおよび管理できます。また、NSX Data Center は、ネットワークモデル全体をソフトウェアで再現し、単純なネットワークから複雑なマルチティア ネットワークに至るまで、あらゆるネットワーク トポロジーの作成とプロビジョニングをわずか数秒で実行します。ユーザーは、NSX を介して提供されるサービスを組み合わせたり、次世代型ファイアウォールからパフォーマンス管理ソリューションまでサードパーティ製品と連携した多岐にわたるエコシステムを活用することで、要件が異なる複数の仮想ネットワークを作成し、本質的に俊敏でセキュアな環境を構築できます。これらのサービスは、クラウド内およびクラウド間の複数のエンドポイントへと拡張できます。

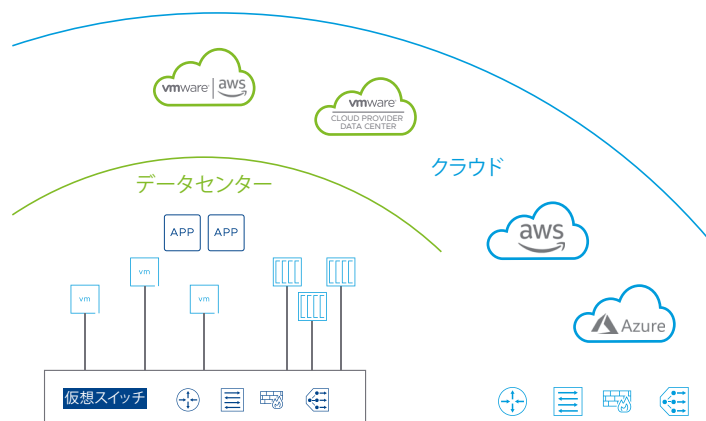


図 1：NSX Data Center：ネットワーク仮想化とセキュリティのプラットフォーム

ソフトウェアによるネットワーク

VMware NSX Data Center は、Software-Defined Data Center (SDDC) の基盤となり、Virtual Cloud Network への拡張が可能な、まったく新しいソフトウェア ベースのネットワーク運用モデルを提供します。データセンターの運用担当者は、俊敏性、セキュリティ、経済性を、物理ハードウェア コンポーネントのみに固定されていたデータセンター ネットワークでは達成できなかったレベルに向上させることができるほか、論理スイッチ、ルーティング、ファイアウォール、ロードバランシング、仮想プライベート ネットワーク (VPN)、サービス品質 (QoS)、モニタリングなど、論理ネットワークとセキュリティに関する機能とサービスの完全なセットを利用できます。これらのサービスは、NSX Data Center API を利用する任意のクラウド管理プラットフォームを通じて仮想ネットワークにプロビジョニングされ、仮想ネットワークは、既存のあらゆるネットワーク ハードウェアにダウンタイムなしで展開でき、データセンター、パブリック クラウド、プライベート クラウド、コンテナ プラットフォーム、ベアメタル サーバにわたり拡張できます。

NSX Data Center の主な機能

スイッチング	データセンターの境界内および境界間で、レイヤー 3 でルーティングされるファブリック全体にわたって、論理レイヤー 2 オーバーレイによる拡張を可能にし、VXLAN および Geneve ベースのネットワーク オーバーレイをサポートします。
ルーティング	仮想ネットワーク間でのダイナミック ルーティングは、ハイパーバイザー カーネル内で分散方式で実行されます。ルーティングのスケールアウトは、物理ルータによるアクティブ/アクティブ フェイルオーバーで実行できます。スタティック ルーティングとダイナミック ルーティングのプロトコルをサポートします (IPv6 のサポートを含む)。
分散ファイアウォール	レイヤー 7 まで対応するハイパーバイザー カーネル組み込み型のステートフル ファイアウォール (アプリケーションの識別と URL のホワイトリスト設定を含む) を環境全体に分散させ、ポリシーの一元的な適用と、統合管理が可能です。また、Kubernetes や Pivotal Cloud Foundry などのクラウドネイティブ プラットフォーム、AWS や Azure などのネイティブパブリック クラウド、およびベアメタル サーバに NSX 分散ファイアウォールを直接統合できます。
ロードバランシング	SSL オフロードおよびパススルー、サーバの健全性チェック (およびパッシブな健全性チェック)、GUI または API を通じたプログラミングとトラフィック処理に関するアプリケーション ルールを備えた L4 ~ L7 のロードバランサーを提供します。
VPN	サイト間およびリモートアクセス用の VPN や、クラウド ゲートウェイ サービス向けのアンマネージド VPN の機能を提供します。
NSX ゲートウェイ	物理ネットワークおよび NSX オーバーレイ ネットワーク上に構成された VLAN 間のブリッジングをサポートし、仮想ワークロードと物理ワークロード間をシームレスに接続します。
NSX Data Center API	JSON ベースの RESTful API で、クラウド管理プラットフォーム、DevOps 自動化ツール、カスタムの自動化機能との連携が可能です。
運用管理	セントラル CLI、Traceflow、オーバーレイ論理 SPAN、IPFIX などのネイティブな運用機能により、仮想ネットワーク インフラストラクチャのトラブルシューティングとプロアクティブなモニタリングを行うことができます。VMware vRealize® Network Insight™ などのツールと連携することで、高度な分析とトラブルシューティングが可能です。
コンテキストに応じたマイクロセグメンテーション	IP アドレス、ポート、プロトコルのほか、マシン名とタグ、オペレーティングシステムの種類、レイヤー 7 のアプリケーション情報など、さまざまな要素に基づいてセキュリティ グループとポリシーを動的に作成し、自動的に更新できます。これにより構成可能となるアダプティブ マイクロセグメンテーションのポリシーでは、Active Directory やその他のソースからの ID 情報に基づき、リモート デスクトップ サービスや仮想デスクトップ インフラストラクチャ (VDI) 環境での個々のユーザー セッション レベルにまでユーザーレベルのセキュリティを適用できます。
自動化およびクラウド管理	vRealize Automation™ や OpenStack などとネイティブに連携します。Terraform プロバイダーや PowerShell との連携も完全にサポートします。
サードパーティのパートナーとの連携	次世代のファイアウォール、侵入検知システム (IDS) / 侵入防止システム (IPS)、エージェント不要のアンチウイルス、スイッチング、運用管理と可視化、高度なセキュリティなど、多岐にわたる領域で、管理プレーン、制御プレーン、データ プレーンがさまざまなサードパーティ パートナーと連携します。
マルチクラウドのネットワークとセキュリティ	基盤となる物理トポロジーやクラウド プラットフォームに関係なく、複数のデータセンター サイトやプライベートクラウドおよびパブリック クラウドの境界を越えて一貫性のあるネットワークとセキュリティを実現します。
コンテナのネットワークとセキュリティ	仮想マシンまたはベアメタル ホストのいずれかで実行されている、Kubernetes または Cloud Foundry ベースのプラットフォーム上のコンテナに対して、ロードバランシング、マイクロセグメンテーション (分散ファイアウォール)、ルーティング、スイッチングの機能を提供するほか、コンテナのネットワーク トラフィック (論理ポート、SPAN/Mi、IPFIX、Traceflow) を可視化します。

ユースケース

セキュリティ

NSX Data Center は、プライベートおよびパブリック クラウド環境におけるアプリケーションのゼロトラスト セキュリティの運用を支援します。重要なアプリケーションのロックダウン、ソフトウェアによる論理 DMZ の作成、仮想デスクトップ環境の攻撃対象領域の縮小などに向けて、マイクロセグメンテーションを実行し、個々のワークロード レベルでネットワークセキュリティ ポリシーを定義および適用できます。

マルチクラウド ネットワーク

NSX Data Center は、異種混在のサイト間でネットワークとセキュリティの一貫性を確保し、マルチクラウドの運用を効率化する、ネットワーク仮想化ソリューションを提供します。データセンターのシームレスな拡張から、複数のデータセンターのプール化、ワークロードの迅速な移動まで、さまざまなマルチクラウドのユースケースに対応します。

自動化

ネットワーク機能とセキュリティ機能の仮想化により、複数のサイトやクラウド全体にわたって従来のアプリケーションと新しいアプリケーションの迅速な展開と、ライフサイクルの完全自動化が可能です。従来の IT タスク、新しいクラウドネイティブ機能、継続的な運用を自動化することで、IT 部門と開発者の双方が加速するビジネスのスピードに対応できます。

クラウドネイティブ アプリケーション対応のネットワークとセキュリティ

NSX Data Center は、コンテナ化されたアプリケーションとマイクロサービスに、統合されたフル スタックのネットワークとセキュリティを提供します。新しいアプリケーションを開発する際には、コンテナ単位できめ細かいポリシーを設定することが可能です。これにより、コンテナ間でのネイティブなレイヤー 3 ネットワーク接続、マイクロサービスのためのマイクロセグメンテーション、従来のアプリケーションと新しいアプリケーションの両方にまたがるネットワークおよびセキュリティ ポリシーのエンドツーエンドでの可視化が可能です。

VMware NSX Data Center のエディション

Standard

ネットワークの俊敏性と自動化機能を必要とする企業に適しています。

Professional

Standard Edition の機能に加えて、マイクロセグメンテーションを必要とする企業に適しており、パブリック クラウドのエンドポイントを持つ企業にも活用いただけます。

Advanced

Professional Edition の機能に加えて、高度なネットワークおよびセキュリティのサービス、幅広いパートナー エコシステムとの連携を必要とする企業に適しています。複数のサイトを持つ企業にも活用いただけます。

Enterprise Plus

NSX Data Center が提供する先進的な機能に加えて、vRealize Network Insight によるネットワークの可視化とセキュリティ運用、NSX Hybrid Connect によるハイブリッドクラウドの可搬性を必要とする企業に適しています。

Remote Office Branch Office (ROBO)

リモート オフィスや支社環境のアプリケーションに対してネットワークとセキュリティの仮想化を必要とする企業に適しています。

	Standard	Professional	Advanced	Enterprise Plus	ROBO
NSX Data Center ¹					
分散スイッチングと分散ルーティング	○	○	○	○	○ ⁵
NSX Edge™ ファイアウォール	○	○	○	○	○
NSX Edge NAT	○	○	○	○	○
物理環境へのソフトウェア L2 ブリッジ	○	○	○	○	
ECMP によるダイナミック ルーティング (アクティブ / アクティブ)	○	○	○	○	○
クラウド管理プラットフォームとの連携 ³	○	○	○	○	○
ベアメタル上で稼動する仮想マシンおよびワークロード向けの分散ファイアウォール		○	○	○	○
VPN (L2 および L3)		○	○	○	○
NSX Cloud との連携による AWS および Azure のサポート ⁴		○	○	○	○
NSX Edge のロードバランシング			○	○	○
分散ファイアウォールとの連携 (Active Directory、VMware AirWatch®、サードパーティのサービス挿入)			○	○	○
コンテナのネットワークとセキュリティ			○	○	
マルチサイトのネットワークとセキュリティ			○	○	
IPv6			○	○	
コンテキストに応じたマイクロセグメンテーション (アプリケーションの識別、RDSH)				○	
URL フィルタリング				○	
+ vRealize Network Insight Advanced ²					
トラフィック (IPFIX) の可視化とネットワークのモニタリング				○	
ファイアウォールの計画と管理				○	
NSX の運用とトラブルシューティング				○	
+ NSX Hybrid Connect Advanced ²					
大規模なワークロードの移行				○	
ワークロード移行のための WAN の最適化				○	
複数のリンクにわたるトラフィックと負荷の管理				○	

¹ 機能の詳細については、NSX Data Center for vSphere と NSX-T™ Data Center の各機能に関するナレッジベースの記事で最新情報を参照してください。

² NSX Data Center Enterprise Plus には vRealize Network Insight Advanced と NSX Hybrid Connect Advanced のフルバージョンが含まれます。

³ L2、L3、NSX Edge の連携のみ。セキュリティ グループの使用なし。

⁴ パブリック クラウドのワークロードには NSX Cloud のサブスクリプションが必要です。

⁵ スイッチングのみ、VLAN ベース。

