VMware NSX Data Center

PRINCIPAUX AVANTAGES

- Protégez vos applications grâce à la micro-segmentation au niveau de la charge de travail et à la sécurité granulaire.
- Réduisez de manière drastique les délais de provisionnement du réseau, qui passent de plusieurs jours à quelques secondes, et améliorez l'efficacité opérationnelle grâce à l'automatisation.
- Bénéficiez d'une gestion cohérente des stratégies de réseau et de sécurité, indépendamment de la topologie de réseau physique dans les Data Centers et les Clouds publics natifs.
- Obtenez une visualisation détaillée de la topologie des applications, des recommandations des règles de sécurité automatisées et une surveillance continue des flux.

VMware NSX® Data Center est la plate-forme de virtualisation de réseau et de sécurité qui permet de mettre en œuvre le réseau Cloud virtuel, selon une approche software-defined qui s'applique aux Data Centers, Clouds et structures applicatives. Avec NSX Data Center, les fonctionnalités de réseau et de sécurité sont au plus proche d'une application, où qu'elle s'exécute (machines virtuelles, conteneurs, bare metal). Comme pour le modèle opérationnel des VM, les réseaux peuvent être provisionnés et gérés indépendamment du matériel sous-jacent. NSX Data Center reproduit la totalité du modèle réseau sous forme logicielle, permettant ainsi de créer et de provisionner en quelques secondes toute topologie, du réseau le plus simple au réseau n-tier le plus complexe. Les utilisateurs peuvent créer plusieurs réseaux virtuels adaptés à différents besoins, en combinant des services proposés par NSX ou par un vaste écosystème d'intégrations tierces aussi divers que des pare-feu de nouvelle génération ou des solutions de gestion des performances, et ce pour mettre en place des environnements intrinsèquement plus agiles et sûrs. Ces services peuvent être étendus à une variété de terminaux, que ce soit au sein d'un Cloud ou d'un Cloud à un autre.

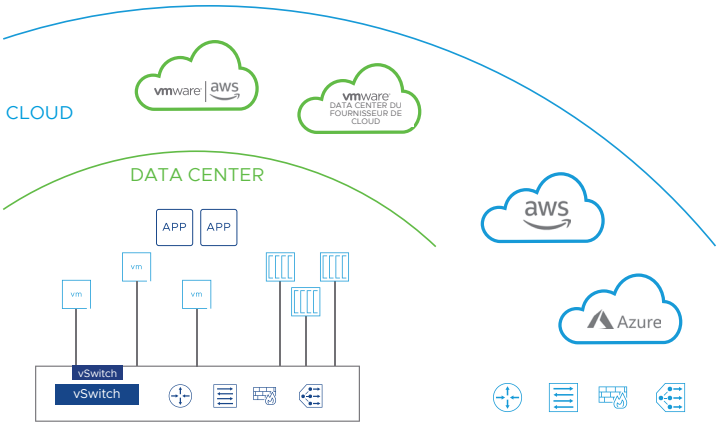

FIGURE 1 : Plate-forme de virtualisation et de sécurité du réseau NSX Data Center.

Réseau sous forme logicielle

VMware NSX Data Center fournit un modèle opérationnel du réseau entièrement nouveau dans une solution logicielle, qui constitue la base du Software-Defined Data Center (SDDC) et s'applique à un réseau Cloud virtuel. Désormais, les opérateurs des Data Centers bénéficient de niveaux d'agilité et de sécurité inédits, et réalisent des économies inenvisageables lorsque le réseau du Data Center était lié uniquement à des composants matériels physiques. NSX Data Center propose un ensemble complet de capacités et de services logiques pour la sécurité et le fonctionnement du réseau : commutateurs logiques, routeurs, pare-feu, équilibreurs de charge, réseau virtuel privé (VPN), qualité de service et surveillance. Le provisionnement de ces services s'effectue sur des réseaux virtuels, via n'importe quelle plate-forme de gestion du Cloud exploitant les API de NSX Data Center. Les réseaux virtuels sont déployés sans interruption sur n'importe quel matériel réseau existant et peuvent s'étendre sur des Data Centers, des Clouds publics et privés, des plates-formes de conteneurs et des serveurs bare metal.

Principales fonctionnalités

Commutation	Extensions de la superposition de couche 2 logique avec routage sur la couche 3, au sein et à l'extérieur des limites du Data Center. Prise en charge des superpositions réseau basées sur VXLAN et GENEVE.
Routage	Routage dynamique entre les réseaux virtuels gérés de façon distribuée dans le noyau de l'hyperviseur ; routage avec évolutivité horizontale et basculement sur des routeurs physiques en mode actif-actif. Prise en charge du routage statique et des protocoles de routage dynamique, y compris la prise en charge d'IPv6.
Pare-feu de la passerelle	Pare-feu avec état jusqu'à la couche 7 (y compris l'identification des applications et la liste blanche des URL), intégré dans la passerelle NSX, distribué dans l'ensemble de l'environnement avec des règles et une gestion centralisées.
Pare-feu distribué	Pare-feu avec état jusqu'à la couche 7 (y compris l'identification des applications et la liste blanche des URL), intégré au noyau de l'hyperviseur, distribué dans l'ensemble de l'environnement avec des règles et une gestion centralisées. De plus, le pare-feu distribué NSX s'intègre directement aux plates-formes natives du Cloud telles que Kubernetes et Pivotal Cloud Foundry, aux Clouds publics natifs tels qu'AWS et Azure, ainsi qu'aux serveurs bare metal.
Équilibrage de charge	Équilibreur de charge pour les couches L4–L7 avec transmission directe (passthrough) et déchargement SSL, contrôles de l'état du serveur (et contrôles d'état passifs) et règles d'applications pour la programmabilité et la manipulation du trafic via GUI ou API.
VPN	Capacités de VPN de site à site et d'accès à distance ; réseaux VPN non gérés pour les services de passerelle de Cloud.
Passerelle NSX	Prise en charge de ponts entre les VLAN configurés sur le réseau physique et les réseaux de superposition NSX, pour une connectivité transparente entre les charges de travail virtuelles et physiques.
NSX Intelligence™	NSX Intelligence fournit des recommandations automatisées sur les règles de sécurité et assure une surveillance et une visualisation continues de chaque flux de trafic réseau pour une meilleure visibilité, ce qui permet une stratégie sécuritaire hautement et facilement vérifiable. Dans le cadre de la même interface utilisateur que le Data Center NSX-T™, NSX Intelligence fournit une console unique aussi bien pour les équipes réseau que pour les équipes de sécurité.
API de NSX Data Center	API RESTful basée sur JSON pour l'intégration avec les plates-formes de gestion du Cloud, les outils d'automatisation DevOps et l'automatisation personnalisée.
Opérations	Capacités opérationnelles natives telles que l'interface de ligne de commande (CLI) centrale, Traceflow, la superposition logique de SPAN (mise en miroir de ports) et IPFIX pour le dépannage et la surveillance proactive de l'infrastructure du réseau virtuel. Intégration avec des outils tels que VMware vRealize® Network Insight™ qui offrent des fonctions avancées de gestion des données chiffrées et de résolution des problèmes.
Micro-segmentation en fonction du contexte	Les groupes et les règles de sécurité peuvent être créés et mis à jour de manière dynamique en fonction des attributs (au-delà des adresses IP, des ports et des protocoles) pour inclure des éléments tels que le nom et les balises de la machine, le type de système d'exploitation et les informations d'application de couche 7 afin de permettre une règle de micro-segmentation adaptative. Les règles basées sur les informations d'identité d'Active Directory et d'autres sources permettent une sécurité au niveau des utilisateurs jusqu'au niveau de la session individuelle dans les environnements VDI (infrastructure de postes de travail virtuels) et les services pour postes de travail distants.
Automatisation et gestion du Cloud	Intégration native avec vRealize Automation™/VMware Cloud™ Automation Services, OpenStack, etc. Modules Ansible entièrement pris en charge, fournisseur Terraform entièrement pris en charge et intégration PowerShell.
Intégration de produits tiers de partenaires	Intégration de la gestion, du plan de contrôle et du plan de données avec un large éventail de solutions de partenaires, notamment concernant les pare-feu nouvelle génération, le système de détection d'intrusion (IDS)/ système de prévention des intrusions (IPS), les antivirus sans agent, la commutation, les opérations et la visibilité, la sécurité avancée, etc.
Réseau multicloud et sécurité	Permettre le fonctionnement du réseau avec un même niveau de sécurité sur l'ensemble des sites des Data Centers, ainsi qu'au-delà des frontières des Clouds privés et publics, indépendamment de la topologie physique sous-jacente ou de la plate-forme de Cloud.
Conteneurs réseau et sécurité	Prend en charge l'équilibrage de charge, la micro-segmentation (pare-feu distribué), le routage et la commutation des conteneurs sur les plates-formes construites sur Kubernetes et Cloud Foundry, fonctionnant sur des machines virtuelles ou sur des hôtes bare metal. Fournit une visibilité pour le trafic réseau de conteneurs (ports logiques, SPAN/Mi, IPFIX et Traceflow).

Cas d'usage

Sécurité

Grâce à NSX Data Center, la mise en œuvre d'une sécurité zéro confiance pour les applications, dans les environnements de Cloud privé et public, est possible et efficace. Que l'objectif consiste à verrouiller les applications critiques, à créer un sous-réseau démilitarisé logique (DMZ) sous forme logicielle ou à réduire la surface d'attaque d'un environnement de postes de travail virtuels, NSX Data Center autorise la micro-segmentation afin de définir et d'appliquer des règles de sécurité réseau au niveau des charges de travail individuelles.

Réseau multicloud

NSX Data Center offre une solution de virtualisation de réseau qui assure le fonctionnement du réseau et la sécurité de manière cohérente sur des sites hétérogènes afin de fluidifier les opérations multi-cloud. NSX Data Center rend donc possibles des cas d'usage multicloud allant de l'extension de Data Center au regroupement de Data Centers, en passant par la mobilité des charges de travail.

Automatisation

En virtualisant les services de réseau et de sécurité, NSX Data Center accélère le provisionnement et le déploiement des applications de la pile complète en supprimant les goulots d'étranglement des services et règles de réseau et de sécurité gérés manuellement. NSX Data Center s'intègre de manière native aux plates-formes de gestion du Cloud et autres outils d'automatisation, tels que vRealize Automation/VMware Cloud Automation Services, OpenStack, Terraform, Ansible, etc., pour permettre aux développeurs et aux équipes informatiques de provisionner, déployer et gérer des applications à la vitesse requise par l'activité.

Réseau et sécurité des applications Cloud natives

NSX Data Center assure la sécurité de la pile complète intégrée des applications conteneurisées et des microservices associés sur le réseau, ce qui permet de définir des règles granulaires au niveau de chaque conteneur dans le cadre du développement de nouvelles applications. Résultat : des services réseaux natifs de couche 3 d'un conteneur à l'autre, la micro-segmentation des microservices, et une visibilité de bout en bout des règles réseau et de sécurité sur l'ensemble des applications (traditionnelles et nouvelles).

Éditions de VMware NSX Data Center

Standard

Cette édition s'adresse aux entreprises à la recherche d'agilité et d'automatisation du réseau.

Professional

Cette édition s'adresse aux entreprises qui ont besoin des fonctionnalités de l'édition Standard, qui souhaitent en outre appliquer la micro-segmentation, et qui peuvent utiliser des terminaux de Cloud public.

Advanced

Cette édition s'adresse aux entreprises qui ont besoin des fonctionnalités de l'édition Professional, qu'ils souhaitent compléter avec des services réseau et de sécurité avancés, ainsi que des fonctions d'intégration à un vaste écosystème de solutions, et qui possèdent plusieurs sites.

Enterprise Plus

Pour les entreprises qui ont besoin des fonctionnalités les plus avancées de NSX Data Center, ainsi que des opérations réseau avec vRealize Network Insight, de la mobilité hybride dans le Cloud avec VMware HCX® et de la visibilité des flux de trafic et des opérations de sécurité avec NSX Intelligence.

Bureaux distants/succursales (ROBO)

Cette édition s'adresse aux entreprises qui ont besoin de virtualiser les fonctions réseau et de sécurité pour les applications d'un site distant ou d'une succursale.

	STANDARD	PROFESSIONAL	ADVANCED	ENTERPRISE PLUS	SUCCURSALES ET SITES DISTANTS
NSX DATA CENTER[1]					
Commutation et routage distribués	•	•	•	•	•[5]
Pare-feu de la passerelle NSX (état)	•	•	•	•	•
NAT de passerelle NSX	•	•	•	•	•
Création de ponts logiciels de couche 2 vers les environnements physiques	•	•	•	•	
Routage dynamique ECMP (actif-actif)	•	•	•	•	•
Intégration avec les plates-formes de gestion du Cloud[3]	•	•	•	•	•
Pare-feu distribué pour les machines virtuelles et les charges de travail fonctionnant sur Bare Metal		•	•	•	•
VPN (couche 2 et couche 3)		•	•	•	•
Intégration avec NSX Cloud[4] pour AWS et Azure Support		•	•	•	•
Équilibrage de charge			•	•	•
Intégration avec le pare-feu distribué (Active Directory, VMware AirWatch®, protection des terminaux et insertion de services tiers)			•	•	•
Mise en réseau et sécurité des conteneurs			•	•	
Réseaux multisites et sécurité			•	•	
IPv6			•	•	
Micro-segmentation en fonction du contexte (identification d'application, RDSH, analyseur de protocole)				•	
Pare-feu de passerelle NSX avancé (identification d'application, analyseur de protocole)				•	
Filtrage URL				•	
+NSX INTELLIGENCE					
Analyse des flux de trafic de VM à VM				•	
Visibilité du pare-feu				•	
Politique de sécurité automatisée				•	
Données chiffrées des règles et recommandations de groupe				•	
+vREALIZE NETWORK INSIGHT ADVANCED[2]					
Visibilité du trafic (IPFIX) et surveillance du réseau				•	
Planification et gestion de pare-feu				•	
Opérations NSX et résolution des problèmes associés				•	
+VMWARE HCX ADVANCED[2]					
Migration des charges de travail à grande échelle				•	
Optimisation du réseau WAN pour la migration des charges de travail				•	
Gestion du trafic et de la charge sur plusieurs liaisons				•	

1. Pour obtenir des informations actualisées et détaillées, consultez les articles de la base de connaissances VMware sur les fonctionnalités NSX Data Center for vSphere® et NSX-T Data Center.
2. NSX Data Center Enterprise Plus comprend des versions intégrales de vRealize Network Insight Advanced et de VMware HCX Advanced.
3. Intégration des couches 2, 3 et de la passerelle NSX uniquement. Pas d'utilisation des groupes de sécurité.
4. Abonnement à NSX Cloud nécessaire pour les charges de travail dans le Cloud public.
5. Commutation uniquement, sur VLAN.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com VMware Global Inc. Tour Franklin, 100-101 Quartier Boieldieu, 92042 Paris La Défense Cedex, France Tél. +33 1 47 62 79 00 www.vmware.fr