VMware NSX

Principaux avantages

- 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.
- Protégez vos applications grâce à la micro-segmentation et à la prévention avancée des menaces au niveau des charges de travail, ainsi qu'à la sécurité granulaire.
- 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.
- Activez la prévention avancée des menaces latérales sur le trafic est-ouest à l'aide du moteur de prévention des menaces intégré et entièrement distribué.

VMware NSX® est la plate-forme de virtualisation de réseau et de sécurité qui permet de mettre en œuvre la solution de réseau Cloud de VMware selon une approche software-defined qui s'applique aux Data Centers, aux Clouds et aux structures applicatives. Avec NSX, les fonctionnalités de réseau et de sécurité sont au plus proche d'une application, où qu'elle s'exécute (machines virtuelles (VM), conteneurs, serveurs physiques). Comme pour le modèle opérationnel des VM, les réseaux peuvent être provisionnés et gérés indépendamment du matériel sous-jacent. NSX 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 diverses que des pare-feu 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.

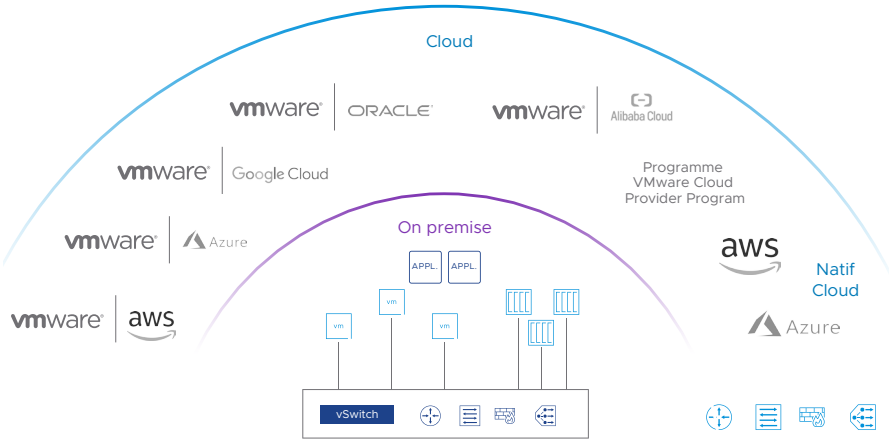

Figure 1 : Plate-forme de virtualisation et de sécurité du réseau NSX

Réseau sous forme logicielle

VMware NSX fournit un modèle opérationnel du réseau entièrement nouveau dans une solution logicielle, qui constitue la base du Software-Defined Data Center (SDDC) et s'étend à un réseau Cloud. 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 propose un ensemble complet de fonctionnalités et de services logiques de réseau et sécurité : 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. 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 physiques.

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.
Routage	Routage dynamique entre les réseaux virtuels gérés de façon distribuée dans le noyau de l'hyperviseur, et 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.
Équilibrage de charge[1]	VMware NSX Advanced Load Balancer™ fournit des fonctionnalités de niveau entreprise d'équilibrage de charge multicloud, d'équilibrage de charge global des serveurs (GSLB), de sécurité des applications et de pare-feu pour les applications Web, des services d'analytique des applications et d'ingress de conteneurs, du Data Center au Cloud.
Routage et transfert virtuels (VRF)	Isolation complète du plan de données entre les locataires avec une table de routage distincte, une traduction d'adresse réseau (NAT) et un pare-feu Edge dans chaque VRF sur la passerelle NSX de niveau 0.
Pare-feu distribué	Pare-feu avec état de la couche 2 à la couche 7 (y compris l'identification des applications, l'identification des utilisateurs et la mise sur liste autorisée de FQDN distribués), intégrée dans le noyau de l'hyperviseur et distribuée sur l'ensemble de l'environnement avec règles et gestion centralisées. De plus, NSX Distributed Firewall™ s'intègre directement aux plates-formes Cloud natives telles que Kubernetes et Pivotal Cloud Foundry, aux Clouds publics natifs tels qu'AWS et Azure, ainsi qu'aux serveurs physiques.
Micro-segmentation contextuelle	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.

Principales fonctionnalités	
VMware NSX Intelligence™	Obtention de recommandations automatisées sur les règles de sécurité et d'une surveillance et d'une visualisation continues de chaque flux de trafic réseau pour une meilleure visibilité, afin de bénéficier d'une stratégie sécuritaire hautement et facilement vérifiable. Dans le cadre de la même interface utilisateur que VMware NSX, NSX Intelligence fournit une console unique pour les équipes responsables du réseau et de la sécurité.
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.
Pare-feu de la passerelle	Une fonctionnalité complète de niveau entreprise assure la protection au moyen d'un pare-feu L4-L7 avec état complet. Celui-ci assure notamment l'identification des applications de couche 7, l'identification des utilisateurs, la traduction d'adresses réseau et d'autres fonctionnalités encore
VPN	Fonctionnalités VPN de site à site et non gérées pour les services de passerelle Cloud.
Fonction-nalités de sécurité avancées et passerelle distribuée NSX[2]	Plusieurs fonctionnalités de sécurité avancées sont disponibles pour NSX avec des modules complémentaires de sécurité. Il s'agit notamment des suivantes : • Sécurité distribuée : – Systèmes distribués de détection et de prévention des intrusions (IDPS) – Prévention distribuée des logiciels malveillants – Analyse distribuée du trafic réseau (NTA) – Détection et réponse réseau • Sécurité des passerelles : filtrage des URL reposant sur les catégories Web et la réputation • Détection des logiciels malveillants
Accélération reposant sur DPU pour NSX	Fournit des services de réseau et de sécurité hautes performances mis en œuvre sur des DPU[3] connectées aux hôtes d'application. Le déchargement des services NSX de l'hyperviseur à la DPU libère des ressources de calcul sur l'hôte, ce qui accélère la commutation et le routage, assure une sécurité hautes performances et renforce l'observabilité, tout en conservant votre expérience utilisateur existante sur NSX.
Fédération	Configuration et application centralisées des règles sur plusieurs sites à partir d'une console unique, pour des règles cohérentes à l'échelle du réseau, une simplicité opérationnelle et une architecture de reprise d'activité simplifiée.
Réseau multicloud et sécurité	Fonctions de réseau et sécurité cohérentes sur l'ensemble des sites des Data Centers, ainsi qu'au-delà des limites des Clouds privés et publics, indépendamment de la topologie physique sous-jacente ou de la plate-forme Cloud.

Principales fonctionnalités	
Conteneurs réseau et sécurité	VMware NSX Container Plugin fournit des fonctions de conteneurs réseau pour VMware Tanzu® Kubernetes Grid™, VMware Tanzu Application Service™, VMware vSphere® with Tanzu, Red Hat OpenShift et Kubernetes en amont. VMware Container Networking™ with Antrea™ fournit des fonctionnalités réseau en cluster et des règles réseau Kubernetes avec support commercial et fichiers binaires signés. L'intégration avec NSX fournit une gestion des règles réseau sur plusieurs clusters et un dépannage centralisé de la connectivité via traceflow, par l'intermédiaire du plan de gestion NSX.
NSX API	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 Aria Operations™ for Logs (anciennement VMware vRealize® Log Insight™) pour une gestion scalable des journaux, et VMware Aria Operations for Networks (anciennement VMware vRealize Network Insight™) pour des analyses et un dépannage avancés.
Automa-tisation et gestion du Cloud	Intégration en natif avec VMware Aria Automation™ (anciennement VMware vRealize Automation™/vRealize Automation Cloud™) et plus encore. Modules Ansible entièrement pris en charge, fournisseur Terraform entièrement pris en charge et intégration de 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/prévention des intrusions (IDS/IPS), les antivirus sans agent, la commutation, les opérations et la visibilité, la sécurité avancée, etc.

Cas d'usage

Sécurité

Grâce à NSX, la mise en œuvre d'une sécurité zéro confiance pour les applications est possible et efficace dans les environnements de Cloud privé et public. 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 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 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 multicloud. NSX 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 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 en natif aux plates-formes de gestion du Cloud et autres outils d'automatisation, tels que VMware Aria Automation, Terraform, Ansible, etc., pour permettre aux développeurs et aux équipes informatiques de provisionner, déployer et gérer des applications au rythme de l'activité.

Réseau et sécurité des applications Cloud

NSX 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 les applications traditionnelles et nouvelles.

Éditions de VMware NSX

Professional

Cette édition s'adresse aux entreprises qui ont besoin de fonctionnalités réseau agiles et automatisées ainsi que de 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, ainsi que des opérations réseau avec VMware Aria Operations for Networks, 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.

	Professional	Advanced	Enterprise Plus	Succursales et sites distants
Réseau[4]				
Commutation et routage distribués	•	•	•	•[5]
Création de ponts logiciels de couche 2 vers les environnements physiques	•	•	•	
Routage dynamique ECMP (actif-actif)	•	•	•	•
IPv6 avec routage statique et allocation IPv6 statique	•	•	•	
IPv6 avec routage dynamique, allocation et services IPv6 dynamiques		•	•	
Gestion externe de double pile (IPv4/IPv6)		•	•	
VRF (VRF de passerelle de niveau 0)		•	•	
VPN Ethernet (EVPN)			•	
Sécurité distribuée				
Pare-feu distribué pour les machines virtuelles et les charges de travail fonctionnant sur des serveurs physiques	•	•	•	•
Micro-segmentation en fonction du contexte (identification d'application de couche 7, RDSH, analyseur de protocole)		•	•	
Liste autorisée de FQDN distribués		•	•	
Fonctionnalités de sécurité distribuée avancée	D'autres fonctionnalités de sécurité distribuée sont disponibles avec des licences complémentaires de sécurité NSX. Reportez-vous à la fiche produit NSX Distributed Firewall.			
Sécurité de passerelle				
NSX Gateway Firewall™ (avec état)	•	•	•	•
NAT de passerelle NSX	•	•	•	•
VPN (couche 2 et couche 3)	•	•	•	•
Fonctionnalités de sécurité avancée de passerelle	D'autres fonctionnalités de sécurité de passerelle sont disponibles avec des licences complémentaires de sécurité NSX. Reportez-vous à la fiche produit de sécurité NSX.			

Ressources complémentaires

Fiche produit VMware NSX Distributed Firewall

Fiche produit VMware NSX Gateway Firewall

Fiche produit VMware Container Networking with Antrea

	Professional	Advanced	Enterprise Plus	Succursales et sites distants
Applications modernes				
Conteneurs réseau et sécurité		•	•	
Multisite				
Réseau et sécurité Multi-vCenter®		•	•	
Fédération			•	
Opérations				
API de règles, ligne de commande (CLI) centrale, superposition logique SPAN et IPFIX	•	•	•	•
Intégrations				
Accélération reposant sur DPU pour NSX[6]		•	•	
Intégration avec les plates-formes de gestion du Cloud[7]	•	•	•	•
Intégration avec le pare-feu distribué (Active Directory, VMware AirWatch®, protection des terminaux et insertion de services tiers)		•	•	•

	Professional	Advanced	Enterprise Plus	
Produits associés				
VMware Aria Operations for Logs pour NSX[8]	•	•	•	•
VMware Aria Operations for Networks Advanced[9]			•	
VMware HCX Advanced[9]			•	
VMware NSX Advanced Load Balancer - Basic Edition[1] (Équilibrage de charge pour les couches L4–L7 avec transmission directe (passthrough) et déchargement SSL, bilans d'intégrité du serveur, règles d'applications pour la programmabilité et manipulation du trafic via GUI ou API)		•	•	•
VMware NSX Intelligence (Analyse du flux de trafic de VM à VM, visibilité du pare-feu, règle de sécurité automatisée, analyse de recommandation des règles et des groupes)			•	

1. VMware recommande aux clients d'utiliser NSX Advanced Load Balancer pour l'équilibrage de charge. NSX Advanced Load Balancer - Basic Edition est inclus avec les éditions Advanced et Enterprise Plus de NSX. Les fonctionnalités avancées de NSX Advanced Load Balancer sont disponibles sous une licence complémentaire. Pour plus d'informations, veuillez consulter la page produit NSX Advanced Load Balancer.
2. Pour les fonctionnalités de sécurité avancée, reportez-vous à la fiche produit NSX Distributed Firewall.
3. Prend en charge plusieurs fournisseurs de DPU/Cartes d'interface réseau et d'OEM de serveurs. Pour plus d'informations, veuillez contacter votre représentant VMware.
4. Une licence d'utilisation de VMware NSX inclut le droit d'utilisation de VMware Workspace ONE® Access™, mais uniquement pour certaines fonctionnalités. Pour connaître le détail des fonctionnalités, reportez-vous aux articles de la base de connaissances sur les fonctionnalités de NSX Data Center for vSphere et de NSX, notamment à l'article Offres de produits pour NSX 4.0.x pour obtenir les informations les plus récentes.
5. Commutation uniquement, sur VLAN.
6. Pour plus d'informations, reportez-vous à l'article de la base de connaissances Offres de produits pour NSX 4.0.x.
7. Intégration des couches 2, 3 et de la passerelle NSX uniquement. Pas d'utilisation des groupes de sécurité.
8. Pour plus d'informations, veuillez consulter la fiche produit VMware Aria Operations for Logs.
9. NSX Enterprise Plus comprend des versions complètes de VMware Aria Operations for Networks Advanced et de VMware HCX Advanced. Pour plus d'informations, voir la fiche produit VMware Aria Operations for Networks et la fiche produit VMware HCX.

Référence : 1696551aq-ds-nsx-a4_FR 4/23