VMware NSX Cloud

Réseau et sécurité du Cloud hybride dans les Clouds privés et les Clouds publics

EN BREF

VMware NSX® Cloud offre des fonctions réseau et de sécurité cohérentes pour les applications exécutées en natif dans les Clouds publics. NSX Cloud utilise le même plan de contrôle et de gestion que NSX Data Center, ce qui permet la mise en place d'une solution unique de gestion de la sécurité et du réseau, depuis le Data Center privé vers le Cloud public.

PRINCIPAUX AVANTAGES

Les fonctions de réseau et de sécurité communes sur les Clouds publics comme AWS et Azure améliorent de façon significative l'évolutivité, le contrôle et la visibilité, tout en réduisant les coûts d'exploitation :

- La flexibilité de déploiement à l'aide de constructions NSX ou de constructions natives de Cloud public
- L'évolutivité s'effectue aisément sur les réseaux virtuels, dans les zones de disponibilité, les régions et les Clouds publics
- Un contrôle précis des services de réseau et de sécurité assure la protection et la standardisation des applications
- Grâce à une visibilité de bout en bout des fonctions de réseau et de sécurité, l'intégrité et la conformité des applications sont assurées dans les Clouds publics

TARIFS

- La tarification repose sur un abonnement, sous la forme de licences temporaires d'un an et de trois ans
- Tarifs basés sur les VCPU utilisés par les charges de travail alimentées dans le Cloud public, indépendamment du nombre de réseaux virtuels ; par exemple, les Clouds privés virtuels AWS (VPC) et les réseaux virtuels Azure (VNets)
- Aucune licence NSX Data Center n'est requise pour les cas d'usage reposant sur le Cloud uniquement

Un réseau créé pour tenir compte des principes du Cloud

VMware NSX Cloud offre des fonctions réseau et de sécurité pour vos applications exécutées en natif dans les Clouds publics. Avec les autres produits de la gamme NSX, VMware NSX Cloud permet d'activer un réseau Cloud virtuel, de mettre en place une approche de gestion réseau software-defined sur les Data Centers, les Clouds, les terminaux, etc.

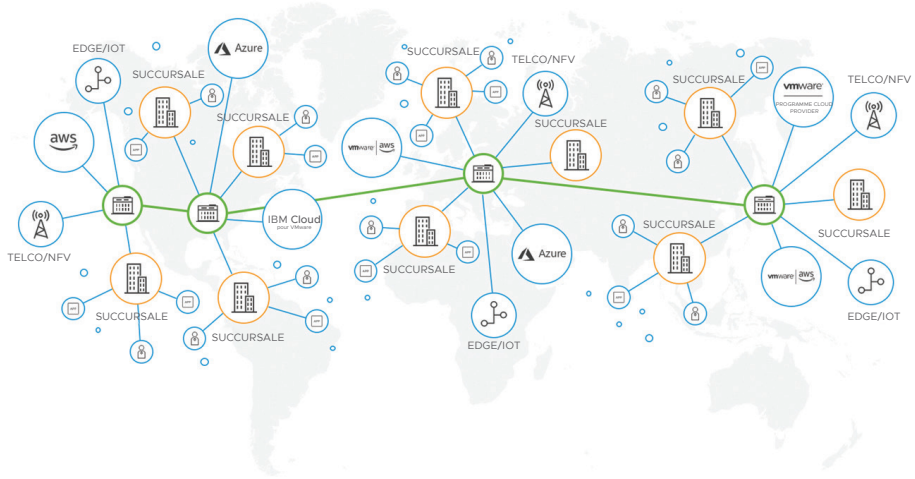

FIGURE 1 : Le réseau Cloud virtuel.

Cas d'usage

Une sécurité homogène sur tous les types de Cloud

NSX Cloud permet d'appliquer des règles sur les charges de travail qui s'exécutent sur plusieurs Clouds publics et Data Centers on premise. Chaque règle est définie et appliquée une seule fois aux charges de travail, où qu'elles soient et quels que soient le réseau Cloud virtuel, le fournisseur de services Cloud, la région et la zone de disponibilité. Les règles de sécurité sont appliquées à chaque charge de travail de manière dynamique, sur la base des attributs des applications et des balises définies par l'utilisateur. Les charges de travail compromises peuvent être automatiquement mises en quarantaine si la règle de sécurité de micro-segmentation appropriée ne leur est pas appliquée. NSX Cloud prend en charge l'insertion de services nord-sud, ce qui permet d'acheminer le trafic sélectif vers des dispositifs de sécurité tiers pour une protection avancée.

Contrôle précis sur les réseaux de Clouds

Le logiciel VMware NSX Cloud est conçu pour les environnements de Cloud public natifs tels qu'Amazon (AWS) et Microsoft Azure. VMware NSX Cloud complète les services natifs disponibles auprès de ces fournisseurs de Cloud public. Grâce à NSX Cloud, vous pouvez continuer à utiliser, pour vos charges de travail, les services applicatifs et l'infrastructure du fournisseur de Cloud public et ce, sans limitation (par exemple AWS ELB/l'équilibreur de charge Azure, AWS Route 53/Azure DNS, AWS Direct Connect/Azure ExpressRoute et Amazon RDS/Azure Database). La gestion du provisionnement et de la configuration peut être automatisée grâce aux requêtes d'API REST en utilisant vos outils d'automatisation existants. NSX Cloud prend

également en charge la consolidation des passerelles en transit vers un VPC/VNet, ce qui permet de simplifier les opérations et d'utiliser des services intégrés tels que le VPN de site à site, ainsi que des services tiers de périmètre/transit.

Contrôle et visibilité opérationnels de bout en bout

VMware NSX Cloud fournit des interfaces et des protocoles standard pour accéder aux données de sécurité et réseau dans vos réseaux Cloud. Les informations concernant les flux, les paquets et les événements sont disponibles via IPFIX, Traceflow, Syslog et la mise en miroir des ports. Ces données peuvent être consommées par vos outils de gestion des opérations on premise et utilisées pour fournir une visibilité complète et détaillée pour la surveillance, le dépannage et l'audit. Ces données d'opérations riches aident à diminuer drastiquement le temps nécessaire à l'identification et la résolution des problèmes de connectivité, de performance et de sécurité sur l'ensemble du déploiement du Cloud hybride, y compris les applications on premise, et dans le Cloud public. NSX Cloud offre une visibilité granulaire des charges de travail du Cloud public sur tous les VPC/VNet, une fonctionnalité de recherche et de filtrage riche pour une gestion simplifiée et la possibilité de choisir facilement les charges de travail à gérer avec NSX.

Principales fonctionnalités

Mode NSX appliqué : utilisez les outils NSX pour une application cohérente des règles de sécurité et de réseau sur les charges de travail on premise et dans le cloud public natif.

Mode natif appliqué au Cloud : utilisez les constructions de sécurité et de réseau d'un fournisseur de Cloud public pour une application cohérente des règles de sécurité et de réseau sur les charges de travail on premise et dans le cloud public natif.

Détection et protection des terminaux natifs des services de Cloud public : permet la détection et la protection des terminaux natifs des services de Cloud public en plus des machines virtuelles (VM) et des instances EC2.

Le multicloud, le réseau et la sécurité multi-site fournissent aux terminaux des fonctionnalités de réseau et de sécurité sur plusieurs Cloud. Via une intégration dans NSX Data Center, ce logiciel assure la gestion de ces fonctionnalités sur les Clouds et les sites de Data Center.

La micro-segmentation assure le contrôle du trafic est-ouest entre les charges de travail d'applications exécutées en natif dans des Clouds publics. NSX Cloud permet également la micro-segmentation des bureaux virtuels déployés par VMware Horizon® Cloud on Azure.

Abstraction enrichie pour la définition des règles de sécurité : définissez des groupes et des règles de sécurité basés sur des constructions de règles riches, telles que le nom d'instance, le type de système d'exploitation, l'identifiant AMI et les balises définies par l'utilisateur.

Règles dynamiques : appliquez automatiquement des règles de sécurité sur la base des attributs d'instance et des balises définies par l'utilisateur. Les règles suivent automatiquement les instances lorsque celles-ci sont déplacées, que ce soit au sein d'un Cloud ou d'un Cloud à un autre.

Instances de quarantaine : mise en quarantaine des charges de travail compromises exécutées dans le Cloud public sans sécurité de micro-segmentation. Les instances mises en quarantaine ne peuvent pas communiquer sur le réseau Cloud, ce qui offre plusieurs couches de sécurité.

Insertion de services : routage sélectif du trafic nord-sud à l'aide d'un routage basé sur des règles vers une appliance tierce de pare-feu partenaire de nouvelle génération.

VPN site à site : utilisez la prise en charge VPN intégrée pour le trafic backhaul vers les Data Centers on premise.

POUR EN SAVOIR PLUS OU POUR ACHETER DES PRODUITS VMWARE

Appelez le numéro international 1-650-427-5000, visitez le site Web *vmware.com/products/nsx-cloud*, la page *vmware.com/products*, ou recherchez un revendeur agréé sur Internet.

Architecture distribuée : éliminez les sauts de réseau et le trafic supplémentaires grâce à l'architecture de pare-feu distribué NSX Cloud, qui applique des règles à l'interface du réseau virtuel de chaque instance plutôt que de router via un pare-feu externe.

Passerelle partagée en transit vers un VPC/VNet : bénéficiez d'une prise en charge de la consolidation des passerelles en transit vers des VPC/VNet, ce qui simplifie l'administration, accélère l'intégration des VPC/VNet de calcul et permet d'insérer des services tiers.

Pare-feu Edge : utilisez un pare-feu avec état pour filtrer les flux de trafic nord-sud entre les instances des réseaux virtuels et le réseau Internet public.

API RESTful : provisionnement et configuration par programmation de l'infrastructure réseau et de sécurité à la demande via l'API RESTful et les outils d'automatisation.

Modélisation : utilisez les outils existants d'automatisation et d'orchestration afin de créer des modèles d'application standardisés, et de simplifier le provisionnement et la gestion des services de réseau et de sécurité sur les Clouds publics.

Visibilité du trafic est-ouest : utilisez les outils d'opérations de jour 2 existants pour gagner en visibilité sur le trafic est-ouest au sein des VPC et entre celles-ci.

Journalisation de la sécurité : bénéficiez d'une visibilité et d'un audit en temps réel des événements de sécurité tels que les autorisations/refus et les incidents de quarantaine. Envoyez les informations sur les événements de sécurité à un serveur Syslog ou SIEM.

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