VMWARE NSX CLOUD

Sécurité et réseau cohérents pour les applications exécutées en natif dans des 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.

- 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 de 1 an et de 3 ans
- Selon les CPU virtuels utilisés par les charges de travail alimentées dans le Cloud public, quel que soit le nombre de réseaux virtuels (par exemple, des instances AWS VPC et Azure VNet)
- Aucune licence NSX Data Center n'est requise pour les cas d'usage reposant sur le Cloud uniquement

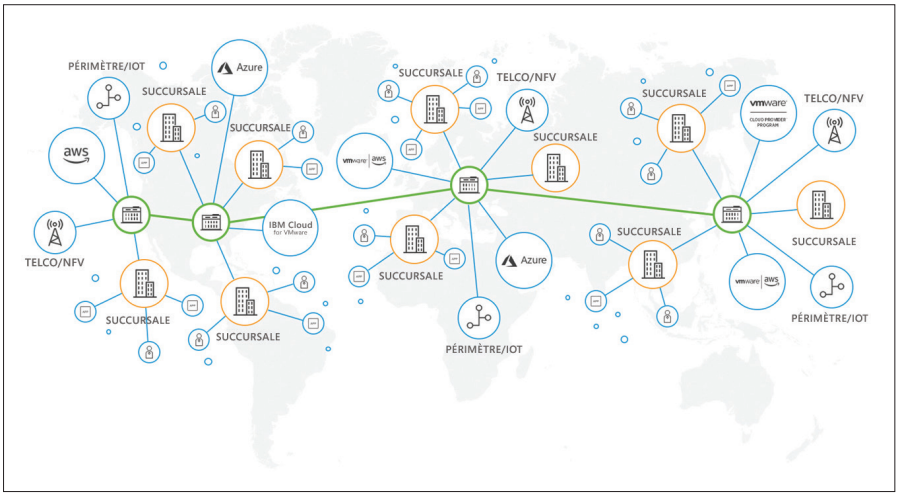

Figure 1 : Le réseau Cloud virtuel

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.

Cas d'usage

Une sécurité homogène sur tous les types de Cloud

NSX Cloud permet l'exécution d'une règle sur les charges de travail de plusieurs Clouds publics. Ce logiciel exploite le même plan de contrôle et de données que NSX Data Center, ce qui permet la gestion des règles de bout en bout sur les différents Data Centers et Clouds. Chaque règle est définie et appliquée une seule fois aux charges de travail, où qu'elles soient et quels que soient le réseau 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.

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 Route53/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.

POUR EN SAVOIR PLUS OU POUR ACHETER DES PRODUITS VMWARE,

APPELEZ
le numéro international +1-650-427-5000,

OU CONSULTEZ LE SITE
https://www.vmware.com/fr/products/nsx-cloud.html ou https://www.vmware.com/fr/products.html pour rechercher un revendeur agréé.

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.

Principales fonctionnalités

Réseau et sécurité multicloud et multisite : NSX Cloud fournit 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.

Micro-segmentation : Contrôle sur le trafic est-ouest entre les charges de travail d'applications exécutées en natif dans des Clouds publics.

Groupes de sécurité : Il est possible de définir les groupes et règles de sécurité sur la base de structures de règles riches, telles que le nom d'instance, le type d'OS, l'identifiant AMI, et des balises définies par l'utilisateur.

Règles dynamiques : Les règles de sécurité sont automatiquement appliquées selon les attributs d'instance et les 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 en quarantaine : Mettez en quarantaine les charges de travail compromises exécutées dans le Cloud public sans sécurité de micro-segmentation. Les instances en quarantaine ne peuvent pas communiquer sur le réseau Cloud.

Architecture distribuée : L'architecture de pare-feu distribués de NSX Cloud élimine le besoin de tronçons de réseau supplémentaires, ce qui réduit le trafic, en appliquant les règles au niveau de l'interface de réseau virtuel de chaque instance, plutôt que de les acheminer via un pare-feu externe.

Pare-feu Edge : NSX Cloud fournit un pare-feu avec état qui filtre les flux de trafic nord-sud entre les instances des réseaux virtuels et le réseau Internet public.

API RESTful : API RESTful et outils d'automatisation pour provisionner et configurer à la demande le réseau et l'infrastructure de sécurité par programmation.

Modèles : 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.

Journaux de 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 sur 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 Terrasse Boieldieu 92042 Paris La Défense 8 Cedex France Tél. +33 1 47 62 79 00 www.vmware.com/fr