



LA CYBERSÉCURITÉ UNIFIÉE DE JUNIPER AU SERVICE D'UNE PROTECTION COMPLÈTE DE NUTANIX ENTERPRISE CLOUD

Micro-segmentation dans un multicloud sécurisé de bout en bout

Problématique

Dans un environnement multicloud, les solutions de sécurité périmétrique qui neutralisent les menaces du trafic nord-sud (entrant et sortant du datacenter) se montrent impuissantes face au trafic est-ouest malveillant (entre les applications et les services).

Solution

En conjonction avec l'offre SDN Nutanix Flow et l'hyperviseur Acropolis (AHV), la plateforme Juniper de cybersécurité unifiée s'appuie sur la micro-segmentation pour sécuriser les applications et bloquer la propagation latérale des menaces dans les environnements multicloud d'entreprise.

Avantages

- Protection de l'entreprise à l'aide de services de sécurité avancés (pare-feu identifiant et applicatif, prévention des menaces avancées, IPS, etc.)
- Sécurisation des workloads virtuels via micro-segmentation
- Analytique et visibilité granulaire
- Application homogène des politiques sur tous les déploiements cloud depuis une seule et même console de gestion

Une technologie d'infrastructure hyperconvergée (HCI) rassemble des fonctions de stockage, de virtualisation des serveurs et de gestion du réseau dans une seule et même solution facile à déployer. De par leur simplicité d'utilisation et de gestion, les HCI sont largement exploitées dans les environnements multicloud de datacenters agiles. Or, les applications ultra-dynamiques qui y sont exécutées ont besoin d'une solution de sécurité offrant une protection intégrale, sans compromis sur l'agilité et l'évolutivité.

La problématique

Les implémentations manuelles, rigides et statiques des solutions de connectivité et de sécurité peuvent très bien fonctionner dans les environnements réseau classiques. En revanche, les applications hautement dynamiques de l'ère du multicloud exigent une sécurité réseau agile et évolutive, capable d'évoluer au rythme des systèmes de calcul et de stockage.

Les environnements multicloud s'appuient généralement sur des solutions de sécurité périmétrique comme Nutanix Enterprise Cloud pour neutraliser les menaces du trafic nord-sud, en provenance et en direction de la HCI. Bien qu'efficaces à ce niveau, ces solutions se révèlent impuissantes face aux menaces issues de machines virtuelles (VM) compromises qui infectent le trafic est-ouest entre les applications et services du datacenter. Or, faute d'identification et de neutralisation rapides de ces menaces, des applications critiques pourraient être compromises. Et on connaît la suite : perte de données sensibles, dégâts irréversibles sur le chiffre d'affaires, dégradation de la réputation de l'entreprise, etc.

La cybersécurité unifiée de Juniper Networks au service des déploiements Nutanix Enterprise Cloud

Sécurité avancée, gestion homogène, neutralisation automatique des menaces, micro-segmentation efficace... ensemble, la plateforme Juniper de cybersécurité unifiée et Nutanix Enterprise Cloud proposent une solution automatique et sécurisée de protection des environnements multicloud.

Au menu :

- **Pare-feu virtuel vSRX de Juniper Networks®** - Le pare-feu virtuel vSRX offre la même sécurité avancée complète que les passerelles de services physiques Juniper Networks SRX Series. Pare-feu virtuel le plus rapide du marché (jusqu'à 100 Gbits/s), le vSRX intègre un large éventail d'options :

- Fonctions clés des pare-feu de nouvelle génération (NGFW), notamment le filtrage du trafic basé sur les utilisateurs et les applications avec détection et blocage des intrusions (IPS). Des performances par cœur de processeur imbattables pour le TCO le plus bas du marché.
- Fonctions de pare-feu basées sur les utilisateurs pour l'analyse, la journalisation et l'application des contrôles d'accès basés sur les rôles et les groupes d'utilisateurs.
- Juniper Networks AppSecure 2.0 pour un contrôle et une visibilité sur les applications (analyse, priorisation et blocage au niveau applicatif pour des exécutions sécurisées).

- **Junos Space® Security Director avec Policy Enforcer** - Junos Space Security Director de Juniper Networks permet de centraliser la gestion d'un réseau distribué de pare-feu virtuels et physiques. En tant qu'interface de gestion du pare-feu virtuel vSRX, Security Director se charge des politiques de pare-feu sur toutes les instances vSRX. Son tableau de bord personnalisable offre plusieurs niveaux d'analyse détaillés, une cartographie des menaces et des logs d'évènements, pour une visibilité sans précédent sur votre sécurité réseau. Par ailleurs, une application adisponible sur Google Android et Apple iOS permet de surveiller les équipements à distance sur un appareil mobile.

Quant à Policy Enforcer, il centralise l'orchestration des politiques. Ce module de Security Director vient renforcer les renseignements sur les menaces de multiples sources et applique des contrôles au niveau du réseau, en complément des pare-feu périmétriques.

- **Nutanix AHV** - Cette solution de virtualisation avancée fait partie intégrante de l'OS Acropolis Enterprise Cloud. Elle ne nécessite donc aucune licence, aucune installation et aucun effort de gestion supplémentaire. Basée sur des technologies de virtualisation open source éprouvées, AHV allie un chemin de données avancé pour des performances optimales à une sécurité renforcée, la virtualisation des flux réseau et des fonctionnalités complètes de gestion. À la clé : un environnement de virtualisation allégé mais plus puissant et plus économique, sans logiciel encombrant (bloatware) ni gaspillage de licences (shelfware).
- **Nutanix Prism** - Solution de gestion intégrale des environnements de datacenters virtuels, Nutanix Prism fluidifie et automatise les workflows courants. Elle élimine par conséquent le besoin d'exploiter de multiples solutions de gestion à travers les opérations de datacenter. Sous-tendue par des technologies de deep learning, Prism analyse les données système pour générer les informations nécessaires à l'optimisation de la virtualisation et de la gestion de l'infrastructure.

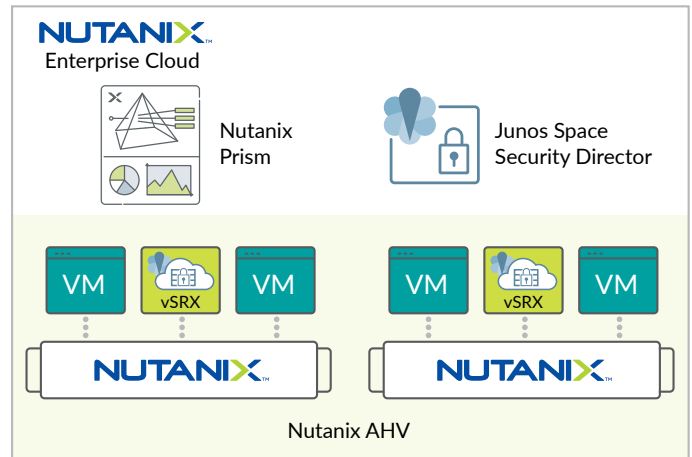


Figure 1 : Nutanix AHV avec le pare-feu virtuel vSRX et Junos Space Security Director

La micro-segmentation permet un contrôle et une segmentation granulaires grâce à des politiques de sécurité mises en œuvre au niveau de l'hôte virtuel. Du point de vue de la sécurité, plus le blocage d'une menace est ciblé, moins elle aura de chances de se propager. Les administrateurs doivent donc adosser leurs solutions de sécurité périmétrique à la micro-segmentation et à une remédiation automatique. Ils bénéficieront ainsi de niveaux de visibilité et de contrôle suffisants pour protéger le trafic latéral des datacenters contre les violations courantes.

De son côté, Junos Space Security Director gère les pare-feu virtuels vSRX déployés sur chaque nœud d'un cluster Nutanix AHV. En tant que gestionnaire unifié des politiques de sécurité, il applique ces politiques de façon homogène à travers toutes les instances vSRX des clouds Nutanix publics et privés (sur AWS ou Azure).

Le trafic entre les VM et les applications passe par vSRX pour permettre le provisionnement des services de sécurité du pare-feu de nouvelle génération, y compris la prévention des menaces avancées. Quant aux politiques de sécurité appliquées au trafic du cloud d'entreprise, elles intègrent la micro-segmentation à l'infrastructure hyperconvergente Nutanix. Cette intégration permet non seulement de bloquer les menaces avancées qui se propagent latéralement sur le réseau, mais aussi d'identifier et de contrôler les accès des utilisateurs et des applications. Les administrateurs sécurité peuvent ainsi isoler et segmenter les données et les applications critiques selon le principe du modèle de sécurité « Zero Trust ».

Fonctionnalités et avantages

Le tableau ci-dessous présente les principaux avantages et fonctionnalités de la solution conjointe Juniper-Nutanix.

Tableau 1. Fonctionnalités et avantages

Fonctionnalités	Avantages
Sécurité avancée	Services de sécurité NGFW (pare-feu identifiant et applicatif, prévention des menaces avancées, IPS, etc.)
Micro-segmentation	Blocage instantané de la propagation latérale des menaces dans le trafic est-ouest
Visibilité	Visibilité sur les applications, les utilisateurs, les comportements des adresses IP et l'activité
Automatisation	API riches et bibliothèques d'automatisation de Nutanix et Juniper Networks pour des workflows DevOps agiles ; amélioration prochaine de l'intégration des partenaires pour des interventions de sécurité plus efficaces grâce à l'automatisation unifiée des workflows réseau et de sécurité
Simplicité opérationnelle	Rationalisation du déploiement des politiques autour d'une seule et même console de gestion avec contrôles simples et intuitifs à travers le multcloud

Synthèse – Juniper et Nutanix, garants de la sécurité des environnements multcloud

Sécurité avancée, gestion homogène, remédiation automatique, automatisation, micro-segmentation efficace... la solution d'infrastructure hyperconvergée Juniper Networks-Nutanix offre aux entreprises tout ce dont elles ont besoin pour protéger efficacement leurs environnements multcloud. Elles ont désormais toutes les cartes en main pour déployer facilement un multcloud sécurisé et automatique sans compliquer leurs opérations et leur gestion.

Prochaines étapes

Pour en savoir plus sur Juniper Networks, rendez-vous sur www.juniper.net. Pour en savoir plus sur Nutanix, rendez-vous sur www.nutanix.com.

À propos de Nutanix

Avec Nutanix, l'infrastructure devient imperceptible. Sa mission : recentrer le département IT sur les applications et services qui font la force de l'entreprise. La plateforme Nutanix Enterprise Cloud s'appuie sur une ingénierie web-scale et un modèle conceptuel « consumer grade » pour faire converger nativement les ressources de calcul, de virtualisation et de stockage vers une solution résiliente, définie par logiciel et dotée de fonctions d'automatisation puissantes. Résultat : des performances prévisibles, une consommation d'infrastructure sur le modèle du cloud, une sécurité renforcée et la mobilité transparente d'un grand nombre d'applications d'entreprise.

À propos de Juniper Networks

Juniper Networks simplifie le réseau grâce à des produits, solutions et services qui connectent le monde. Nos capacités d'innovation nous permettent d'écarter les obstacles et de briser la complexité des réseaux à l'ère du cloud pour éliminer les difficultés que connaissent nos clients et partenaires au quotidien. Pour Juniper Networks, le réseau est un moyen de partager des connaissances et de favoriser un progrès au service de l'humain. Pour cela, nous inventons des méthodes de conception de réseaux automatisés, évolutifs et sécurisés, capables d'évoluer au rythme des entreprises.

Siège social et commercial

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, CA 94089, États-Unis
Téléphone : +1 888 586 4737
ou +1 408 745 2000
Fax : +1 408 745 2100
www.juniper.net

Siège EMEA et APAC

Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, Pays-Bas
Téléphone : +31 0 207 125 700
Fax : +31 0 207 125 701

JUNIPER NETWORKS | Engineering Simplicity

