ARISTA
Software Driven Cloud Networking

Information Presse

Arista étend les capacités de CloudVision, pour permettre des réseaux cloud sécurisés

Et présente des services de macro-segmentation avec Check Point, F5 Networks, Fortinet, Palo Alto Networks et VMware

Paris, le 8 octobre 2015 - **Arista Networks, Inc. (NYSE : ANET) annonce de nouvelles possibilités pour CloudVision®. Les Services de Macro-Segmentation (MSS™) permettent aux pare-feu et aux ADC (Application Delivery Controllers) de nouvelle génération d'être automatiquement activés en cas de charge réseau ou de flux spécifique, et ce dans n'importe quelle topologie de réseau. Cela concerne aussi bien les trafics de niveau 2, de niveau 3 que les réseaux d'overlay utilisés dans les réseaux fortement virtualisés.**

MSS répond à l'écart croissant entre d'une part les modèles de déploiement de sécurité actuels dans lesquels la sécurité intégrée aux hyperviseurs de virtualisation adresse la communication inter-VM et d'autre part les pare-feu physiques qui adressent le trafic nord-sud. Il n'existe pas encore de solution pour insérer dynamiquement les services de sécurité dans les datacenters avec leurs besoins simultanés au niveau physique et niveau virtuel. Arista travaille avec les leaders de l'industrie tels que Check Point, F5 Networks, Fortinet, Palo Alto Networks et VMware pour faire progresser et simplifier cette intégration des ressources physiques et virtualisées avec ses technologies de réseau cloud.

« Nous sommes impatients de renforcer notre partenariat avec Arista », déclare Tchad Kinzelberg, Vice-président senior pour le développement *business* et *corporate* de Palo Alto Networks. « La phase suivante de nos efforts d'intégration a pour but de proposer un pont transparent entre les réseaux virtuels et les réseaux physiques et de répondre aux exigences de sécurité et de segmentation de réseau, des réseaux cloud complexes et dynamiques. »

MSS fournit un service de réseau dynamique et évolutif pour intégrer de manière logique des unités de sécurité dans le circuit du trafic. Cette intégration est indépendante du fait que le dispositif de sécurité ou la charge de travail soit physique ou virtuel. Elle s'exerce avec une totale flexibilité, autant pour l'emplacement des unités de sécurité que pour les flux.

Principales caractéristiques de MSS

• Indépendant de son emplacement : les grands datacenters peuvent centraliser et insérer à la demande la sécurité sur le chemin des différents flux réseau.

• Intégration facile : en ne changeant aucun format, il garantit que toutes les plates-formes peuvent être facilement intégrées.

• Ouverture : il peut parfaitement fonctionner dans un réseau multi-fournisseurs, sans blocage ni protocoles propriétaires.

• Agilité : les hôtes se déplaçant, les services se déplacent dynamiquement avec eux pour garantir le modèle de déploiement.

• Coexistence transparente : il coexiste avec les règles du pare-feu définies dans le cadre de la politique de sécurité déjà en place.

« Sécurité as a service » avec CloudVision

MSS est l'un des services activés via CloudVision d'Arista. Depuis que CloudVision maintient une base de données de tous les états au sein du réseau, ainsi que l'intégration directe avec les ressources de l'hyperviseur comme VMware vSphere et NSX, on connaît l'emplacement de chaque flux au sein du réseau. On dispose d'informations en temps réel sur les matériels ou flux ajoutés ou supprimés du réseau ou sur ceux qui sont déplacés vers d'autres ports ou serveurs.

La macro-segmentation étend aux réseaux du cloud le concept d'une granularité fine de sécurité inter-hyperviseur en permettant une sécurité et des services dynamiques pour les flux, du physique au virtuel. La sécurité de la macro-segmentation s'ajoute à cette granularité fine de sécurité, assurée par la micro-segmentation mise en œuvre dans le commutateur virtuel de l'hôte physique sur lequel une machine virtuelle fonctionne.

« Nous constatons l'accélération de l'adoption de la virtualisation de réseau VMware NSX, car les entreprises clientes reconnaissent les avantages opérationnels, économiques et de sécurité obtenus par une approche logicielle du datacenter », déclare Hatem Naguib, Vice-président réseau et sécurité de VMware. « La collaboration avec notre partenaire stratégique Arista Networks permet à nos clients d'augmenter les contrôles de la micro-segmentation de NSX, soit par application opérationnelle directe, soit en répondant aux exigences physiques de sécurité des couches, garantissant que les avantages de l'agilité et de la sécurité de NSX s'appliquent à tous les flux, partout et à tout moment. »

En s'intégrant aux API natives fournies par les principaux pare-feu de nouvelle génération - API natives qui existent déjà et sans dépendance spécifique de version - MSS apprend quels flux la politique de sécurité exige de traiter ou surveiller. Si la politique de sécurité nécessite une topologie spécifique du réseau logique, MSS d'Arista peut l'effectuer dans le réseau. Les capacités d'automatisation de MSS fonctionnent en temps réel sans avoir besoin pour l'exploitation du réseau d'engager un administrateur de la sécurité ou vice-versa, et sans que le réseau ait besoin d'être configuré de manière particulière pour un flux particulier. Cette faculté est essentielle à la réussite du déploiement de la sécurité dans un cloud d'entreprise privé ou hybride.

MSS avec Arista CloudVision permet le déploiement flexible de services dans le réseau, sans mise à niveau importante et sans aucun blocage propriétaire. Les services de macro-segmentation sont aujourd'hui en test sur le terrain et seront dans l'ensemble disponibles au premier semestre 2016. Arista organise un webinaire sur la macro-segmentation avec ses partenaires-clés, le 19 Novembre, à 19h00 heure de Paris (CET) .

Citations des partenaires d'Arista

« Check Point est heureux d'offrir sa protection de sécurité de pointe à l'échelle et la vitesse du cloud, en conjonction avec l'architecture d'insertion de sécurité des services de Macro-segmentation d'Arista », déclare Alon Kantor, Vice-président pour le développement des affaires, Check Point. « Travailler avec Arista sur cette offre innovante de sécurité du cloud va renforcer notre mission de protection des infrastructures de cloud privé et public dans le monde entier. »

« Les clients ont identifié le besoin de réagir plus rapidement aux changements fréquents de leur entreprise. En conséquence, F5 et Arista collaborent pour leur permettre d'appliquer automatiquement une grande variété de services du réseau BIG-IP® et de sécurité où et quand les applications ont besoin. Notre objectif commun est de simplifier et d'accélérer autant que possible les processus de déploiement d'application », déclare Phil de la Motte, Senior Director Business Development, Infrastructure Alliances.

« Le pare-feu par Segmentation Interne de Fortinet (ISFW) sécurise le Data Center et le Cloud dans les domaines physiques et virtuels », souligne John Whittle, Vice-président du développement corporate et des alliances stratégiques chez Fortinet. « Nous sommes heureux de travailler avec notre partenaire Arista pour faciliter l'adoption des services de sécurité avancés dans une architecture cloud ouverte. »

ARISTA
Software Driven Cloud Networking

A propos d'Arista

Arista Networks a été créé pour l'innovation et la fourniture de solutions de mise en réseau cloud commandées par logiciel dans l'environnement de stockage et de traitement des grands datacenters. Les plates-formes primées d'Arista, avec une gamme Ethernet de 10 à 100 gigabits par seconde, redéfinissent l'évolutivité, l'agilité et la résilience. Arista a livré plus de cinq millions de ports de réseau cloud dans le monde avec CloudVision et EOS, son système d'exploitation avancé pour le réseau. Engagé sur les standards ouverts, Arista est un membre fondateur du consortium 25/50 GbE. Les produits d'Arista Networks sont vendus dans le monde entier, en vente directe et via un réseau de partenaires.

Pour plus de renseignements : http://www.arista.com

Ce communiqué de presse contient des énoncés prospectifs, y compris, mais sans s'y limiter, des énoncés concernant les avantages et les meilleures pratiques utilisées dans la conception et la mise en œuvre du Cloud Networking d'Arista et l'activation d'économies OPEX ainsi que des accords de services au plus haut niveau. Tous les énoncés autres que les énoncés de faits historiques sont des énoncés qui pourraient être considérés comme prospectifs. Les énoncés prospectifs sont sujets à des risques et incertitudes qui pourraient entraîner des performances ou des résultats réels sensiblement différents de ceux exprimés dans les énoncés prospectifs, y compris notre historique limité d'exploitation et l'expérience de développement et lancement de nouveaux produits ; des problèmes liés au produit, support ou qualité de service ; d'évolution rapide de la technologie, de changements des exigences des clients et des normes de l'industrie ainsi que d'autres risques énoncés dans les documents déposés auprès de la SEC sur le site Web d'Arista (www.arista.com) et le site Web de la SEC (www.sec.gov). Arista décline toute obligation de mettre à jour publiquement ou de réviser toute déclaration prospective pour transcrire des événements qui se produisent ou des circonstances qui surviennent après la date à laquelle ils ont été faits.

Contacts presse
Channel Development & Marketing Manager, EMEA - Lisa Elliott - +44 7769 908968 - lelliott@arista.com
Attachée de presse France - Migé Gauchet - +33 (0)6 84 77 31 74 - mige.gauchet@free.fr ou mige.gauchet@gmail.com

Corporate Communications
Amanda Jaramillo - (408) 547-5798 - amanda@arista.com

Relations avec les investisseurs
Chuck Elliott - Arista Networks, Inc. - Tél : (408) 547-5549 - elliott@arista.com