STRATA™
BY PALO ALTO NETWORKS

CN-Series : rempart de protection pour les environnements Kubernetes

Des pare-feu de containers nouvelle génération pour sécuriser les applications cloud-native

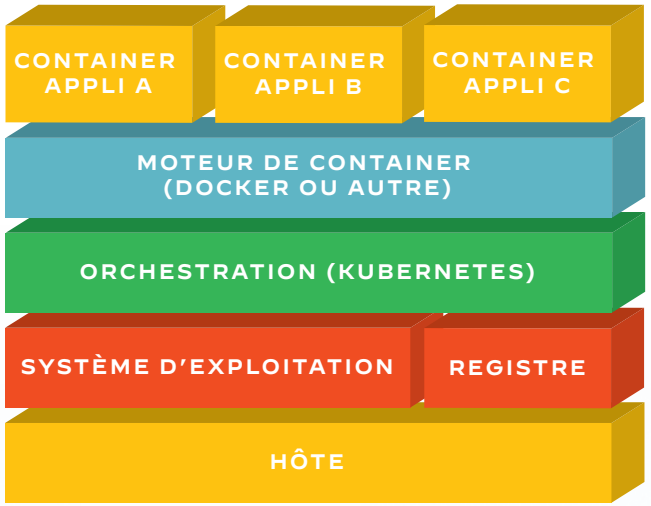
paloalto® NETWORKS

Sommaire

Containers et Kubernetes : un duo de choc

Il n'aura fallu que quelques années aux outils de containers (notamment Docker) pour s'imposer comme le principal moyen de développer et lancer des applications dans les environnements cloud. D'ici 2023, plus de 70 % des entreprises exécuteront au moins trois applications containerisées en production à l'échelle mondiale, contre moins de 20 % en 2019[1].

Cette explosion va de pair avec l'adoption rapide de Kubernetes®[2], devenu la solution de facto pour l'orchestration des containers. À eux quatre, Kubernetes, les containers, les processus DevOps et les microservices sont les moteurs de la révolution cloud-native.



[1] Étude Gartner citée par Janakiram MSV, "5 Modern Infrastructure Trends To Watch Out for in 2019", Forbes, 20 décembre 2018.

[2] "6 Best Practices for Creating a Container Platform Strategy", Gartner, dernière modification le 23 avril 2020. Remarque : publié le 31 octobre 2017.

Si les développeurs étaient autrefois les principaux partisans de la containerisation et de Kubernetes, l'IT opérationnelle entre aujourd'hui dans la partie. Lire la suite.

Les acteurs de la révolution des containers

Conçu pour des geeks et par des geeks, Kubernetes est né au sein de Google. Malgré l'engouement suscité par les containers en général, et Kubernetes en particulier, dans la communauté des développeurs et du DevOps, le scepticisme dominait encore au sein des équipes opérationnelles.

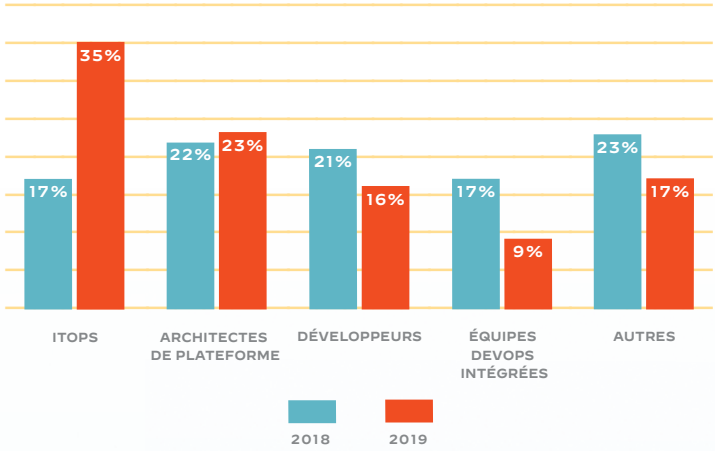
Aujourd'hui, tout a changé. Kubernetes et les containers se sont généralisés – et la fonction IT opérationnelle a rejoint les rangs des aficionados. En 2018, seules 17 % des entreprises déclaraient que les équipes IT opérationnelles (ITOps) jouaient un rôle moteur dans l'adoption des containers. Un an plus tard, ce chiffre atteignait déjà 35 %.

Dans de nombreuses structures, l'ITOps endosse désormais la responsabilité des containers, prenant ainsi le relais des architectes de plateforme, des développeurs, des équipes DevOps, etc[3]. Toutefois, il incombe encore aux développeurs de sécuriser leurs applications avant leur mise en production.

Le saviez-vous ?

« Dans le cadre du développement cloud-native, les processus et les threads qui compromettent l'application changent sans cesse… les workloads doivent être "sécurisés dès le départ", au moment de leur instanciation[4]. » – Gartner

Groupes contribuant à l'adoption des containers



Source : Diamanti, 2019

[3] "2019 Container Adoption Benchmark Survey", Diamanti, 2019.

[4] "Market Guide for Cloud Workload Protection Platforms", Gartner, 8 avril 2019.

Dans un univers DevOps ultradynamique, les développeurs doivent résoudre des problèmes de sécurité de taille.
Lire la suite.

Le dilemme de la sécurité DevOps

Les pratiques DevOps doivent leur succès à la capacité des processus d'intégration et de déploiement continus (CI/CD) à accélérer le TTM (Time-to-Market).

Les pipelines CI/CD comprennent des éléments comme le code et les référentiels d'images, les containers, les serveurs de build et les outils tiers, tous garants d'intégrations et de déploiements efficaces. Toutefois, ces dépendances et configurations complexes contiennent parfois des vulnérabilités qui permettent à des attaquants d'exfiltrer des données, de perturber les environnements de production, voire de paralyser toute l'infrastructure.

De par leur éphémérité et leur fonctionnement en vase clos, les containers apparaissent à première vue comme une option sécurisée pour l'exécution des applications. Mais malgré cet isolement les uns des autres, beaucoup sont déployés sur le même espace d'adresses IP. De fait, si un attaquant accède à ne serait-ce qu'un seul container, il pourra ensuite compromettre l'intégralité du cluster.

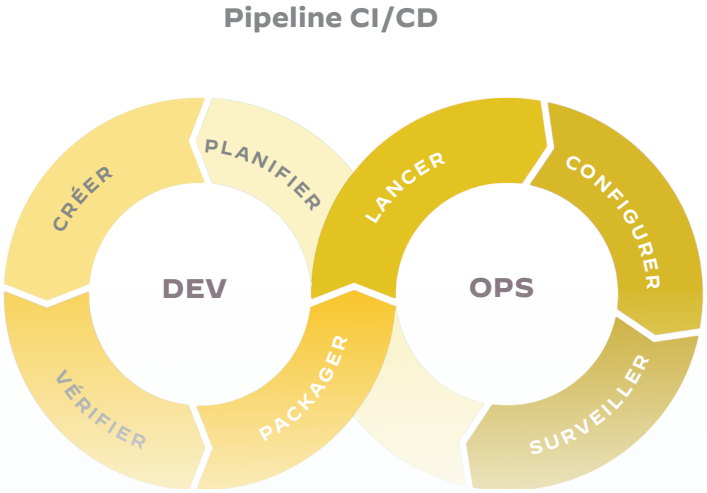
C'est pour ces raisons et d'autres encore que la sécurité du pipeline CI/CD doit faire partie des priorités absolues des équipes DevOps. Toutefois, cette sécurisation est un parcours semé d'embûches. Impossible de confier cette tâche aux seuls développeurs sans risquer d'empiéter sur les ressources normalement dédiées au développement applicatif et de nuire à la sécurité globale. Pourtant, pas question de reléguer la sécurité du pipeline CI/CD au second plan : elle doit s'intégrer au cycle de vie des applications[5].

Le saviez-vous ?

L'essor des pratiques DevOps, des outils CI/CD et des méthodologies Agile donne un coup d'accélérateur aux cycles de lancement. C'est ainsi que la proportion d'entreprises avec des cycles quotidiens a presque doublé entre 2018 (15 %) et 2019 (27 %). En 2019, 28 % des organisations faisaient état de cycles de lancement hebdomadaires, contre 20 % en 2018[6].

[5] "The Greatest Security Risks Lurking in Your CI/CD Pipeline", Twistlock, 8 juillet 2020.

[6] "CNCF Survey 2019", Cloud Native Computing Foundation, 2019.



Essentielle pour protéger les applications cloud-native, la microsegmentation n'en comporte pas moins certaines limites. Lire la suite.

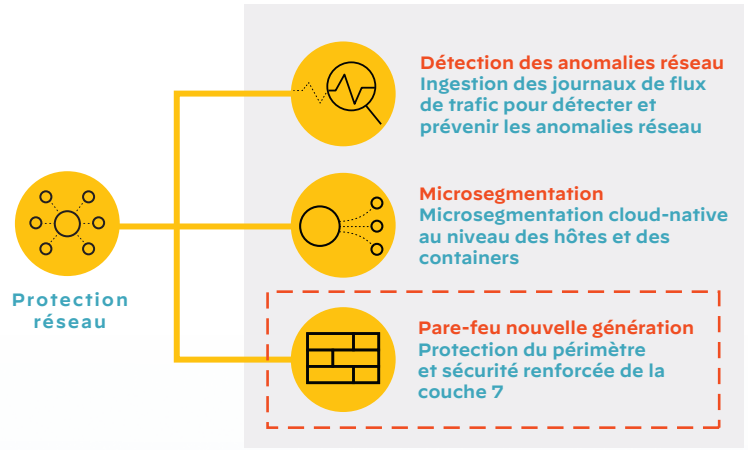
Potentiel et limites de la microsegmentation

Des techniques éprouvées comme les groupes de stratégies, les listes de contrôle d'accès et le blocage de ports font partie intégrante de la sécurisation des déploiements cloud et sur site. Cependant, les environnements cloud nécessitent des mesures de sécurité supplémentaires pour résoudre les problèmes qui leur sont propres. Parmi ces mesures, la microsegmentation sécurise le trafic au niveau des hôtes et des containers afin d'empêcher toute latéralisation des menaces dans l'environnement containerisé. En cela, elle constitue une fonctionnalité essentielle.

Toutefois, à lui seul, le blocage peut se révéler excessivement binaire, s'apparentant à une stratégie du tout ou rien qui ignore les subtilités des interactions au sein des applications cloud-native. C'est là que les pare-feu nouvelle génération (NGFW) entrent en jeu. Inspection au niveau applicatif, prévention des intrusions, Threat Intelligence… les NGFW offrent une protection complète et renforcée. Ils sécurisent le trafic sortant des développeurs vers des sites web comme les référentiels de code, le trafic est-ouest entre de multiples applications containerisées, voire entre une application containerisée et une application traditionnelle, ainsi que le trafic entrant susceptible de renfermer des menaces.

Le saviez-vous ?

« La défense périmétrique n'est plus une stratégie efficace. Le modèle Zero Trust repose sur des méthodes comme le microcœur, la microsegmentation et la visibilité complète pour identifier, localiser et confiner les menaces, réduisant ainsi l'impact des compromissions dans le cadre d'une approche structurée. » – Forrester



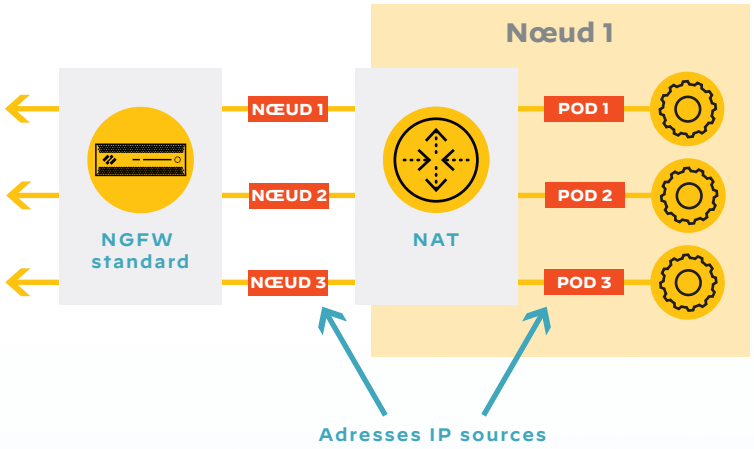
Une solution complète de sécurité réseau pour les environnements cloud-native doit comprendre des fonctionnalités de détection des anomalies, de microsegmentation et de protection par pare-feu.

Les NGFW font partie des composants essentiels d'une solution de sécurité réseau pour les déploiements cloud-native. Toutefois, il ne suffit pas d'acquérir un NGFW semblable à celui que vous utilisez dans votre data center.
Découvrez pourquoi à la page suivante.

NGFW : la sécurité « outside-in »

Les NGFW standards jouent un tel rôle dans la sécurisation des déploiements sur site que peu de data centers peuvent s'en passer. Le problème, c'est que les environnements cloud-native soulèvent des problématiques uniques que les pare-feu nouvelle génération ne peuvent pas régler, surtout en termes de visibilité dans les environnements Kubernetes.

Dans Kubernetes, les pods (des collections de containers) s'exécutent sur des nœuds, soit physiques soit virtuels. Si les développeurs doivent rarement gérer ces nœuds de manière explicite, ces derniers ont un impact sur le fonctionnement des pare-feu. De fait, les NGFW sont incapables d'identifier le pod à l'origine du trafic sortant, car toutes les adresses IP sources sont associées à l'adresse IP du nœud. En clair, pour un pare-feu traditionnel, tous les flux de trafic sortant du nœud se ressemblent.



La traduction d'adresses réseaux (NAT) associe tout le trafic sortant à l'adresse IP source du nœud.

Le saviez-vous ?

Quelques notions de base de Kubernetes :

- Kubernetes organise les containers en pods, qui constituent l'élément de base de la planification.
- Un cluster désigne une collection de pods exécutés sur le même hôte. Les clusters permettent de garantir la haute disponibilité.
- Un service Kubernetes représente un ensemble de pods qui fonctionnent ensemble, comme une couche individuelle d'une application multicouche.

Pour une efficacité maximale, la sécurité réseau cloud-native doit s'appuyer sur les concepts Kubernetes natifs, en particulier les espaces de noms. Lire la suite.

Espaces de noms : un outil puissant pour la sécurité cloud-native

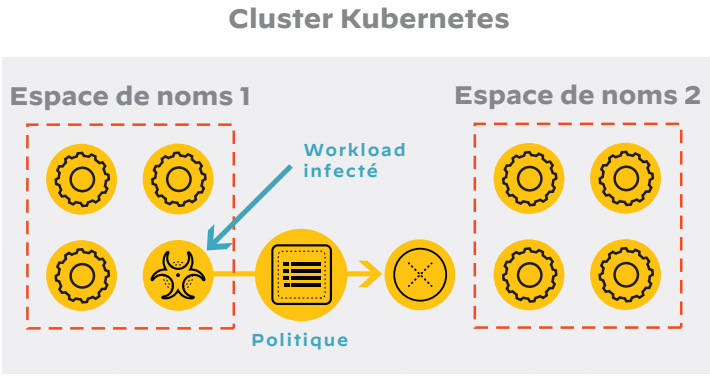
Certes, Kubernetes complique la tâche des outils de sécurité traditionnels. Mais il permet également de renforcer la sécurité en misant sur ses concepts natifs, surtout les espaces de noms.

Les espaces de noms Kubernetes simplifient la gestion de clusters puisqu'ils facilitent l'application de certaines politiques sur des portions bien spécifiques d'un cluster. Mais leurs avantages ne s'arrêtent pas là puisqu'ils représentent également un outil de sécurité puissant. De fait, les équipes de sécurité utilisent les espaces de noms pour isoler des workloads, réduisant ainsi le risque de propagation d'une éventuelle attaque dans un cluster. Elles s'en servent aussi pour établir des quotas de ressources visant à limiter le préjudice qu'une compromission de cluster pourrait causer[7].

Les architectes de sécurité visionnaires veulent pouvoir sécuriser le trafic entre espaces de noms ou à destination des workloads traditionnels comme les serveurs bare metal. Pour cela, ils ont toutefois besoin de connaître l'état interne d'objets comme les espaces de noms, les pods et les containers. Puisqu'il est impossible d'accéder à ces informations en dehors de l'environnement, ils n'ont d'autre choix que d'intégrer la solution de sécurité à Kubernetes.

Le saviez-vous ?

Les espaces de noms sont des clusters virtuels exécutés dans un cluster Kubernetes physique.



Les politiques de sécurité basées sur les espaces de noms empêchent la propagation des exploits dans un cluster physique.

[7] "Kubernetes Security Best Practices", Twistlock, 6 juin 2019.

À ce stade du rapport, nous avons vu les caractéristiques clés d'un pare-feu cloud-native réellement efficace. La prochaine section est consacrée au pare-feu qui remplit ces critères : Palo Alto Networks CN-Series.

Sécurité réseau pour Kubernetes : misez sur CN-Series de Palo Alto Networks

C'est pour répondre au besoin d'une sécurité réseau propre aux environnements cloud-native que Palo Alto Networks a créé CN-Series, premier NGFW conçu pour Kubernetes.

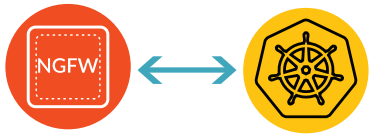
Les pare-feu CN-Series se déploient sous la forme de deux ensembles de pods : l'un pour le plan de gestion (CN-MGMT) et l'autre pour le plan de données du pare-feu (CN-NGFW). Le pod de gestion s'exécute comme un service Kubernetes. Quant aux pods du plan de données, ils se déploient en deux modes : distribué ou en cluster. En mode distribué, le plan de données du pare-feu s'exécute comme un pod DaemonSet sur chaque nœud. Les administrateurs peuvent déployer des pare-feu sur tous les nœuds de cluster à l'aide d'une seule et même commande, plaçant ainsi les contrôles de sécurité au plus près des workloads. Dans le mode de déploiement en cluster, le plan de données du pare-feu s'exécute comme un service Kubernetes sur un nœud de sécurité dédié. Dans cette configuration, CN-Series bénéficie des fonctions natives de montée en charge automatique de Kubernetes, idéales pour protéger même les environnements Kubernetes les plus dynamiques. Les déploiements en cluster conviennent tout particulièrement aux grands environnements Kubernetes, pour lesquels un déploiement distribué coûterait trop cher et mobiliserait trop de ressources.

L'intégration native à Kubernetes permet aux pare-feu CN-Series de formuler les politiques de sécurité à la lumière des informations contextuelles sur les containers dans l'environnement. Par exemple, les espaces de noms de containers peuvent servir à définir une source de trafic dans une politique de pare-feu.

Le saviez-vous ?

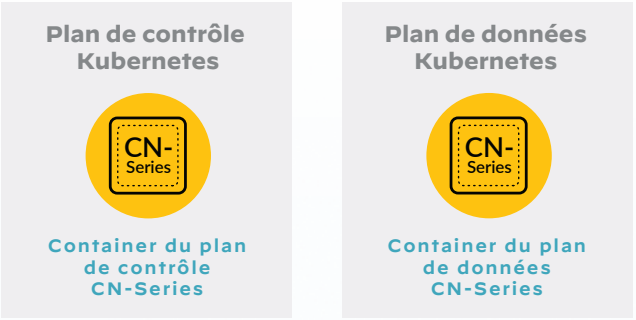
CN-Series est la dernière-née des solutions NGFW primées de Palo Alto Networks.

Modèle de déploiement d'un NGFW



NGFW standard — Kubernetes

Modèle de déploiement de CN-Series



Les pare-feu CN-Series se déploient en natif comme des pods de plan de données et de plan de contrôle dans l'environnement Kubernetes.

De par sa conception et son modèle de déploiement uniques, CN-Series présente des atouts majeurs pour la sécurité des applications cloud-native. Lire la suite.

Avantages de CN-Series pour les développeurs et les équipes de sécurité

Visibilité et contrôle renforcés dans les déploiements Kubernetes

CN-Series intègre des fonctionnalités de sécurité directement dans l'environnement de containers afin de combler les lacunes des pare-feu traditionnels. Ainsi, les équipes de sécurité bénéficient d'une visibilité complète sur le trafic, y compris les adresses IP sources du trafic sortant, habituellement difficiles à identifier. Grâce à l'intégration native à Kubernetes, CN-Series peut également utiliser les informations contextuelles sur les containers pour détecter et bloquer les menaces dissimulées dans le trafic autorisé entre les espaces de noms.

Sécurité cloud-native alignée sur le reste de l'environnement

Le manque de visibilité des NGFW standards sur les environnements de containers nuit à la sécurité des applications cloud-native. À cet égard, CN-Series permet aux équipes de sécurité réseau d'homogénéiser le niveau de protection à travers tous les environnements, cloud-native ou non. Il peut même partager les informations contextuelles qu'il détient sur les environnements Kubernetes avec d'autres pare-feu Palo Alto Networks afin de renforcer votre Threat Intelligence et l'efficacité globale de votre sécurité réseau.

Intégration fluide de la sécurité aux environnements DevOps

Pour garantir la rapidité et l'agilité des équipes DevOps, les pare-feu CN-Series s'appuient sur les fonctions d'orchestration natives de Kubernetes pour intégrer le déploiement de pare-feu directement au pipeline de développement CI/CD afin de fluidifier ce processus. Désormais, les développeurs peuvent déployer CN-Series sur chaque nœud d'un cluster à l'aide d'une seule et même commande dans un fichier YAML.

Gestion unifiée de la sécurité dans les infrastructures hybrides

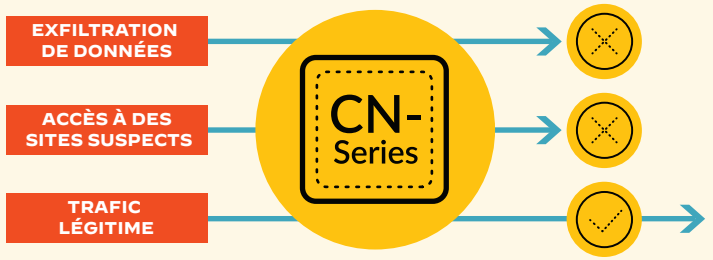
L'un des points faibles de nombreux déploiements hybrides est la prolifération des consoles de gestion. Les équipes de sécurité doivent alors se familiariser avec de multiples paradigmes opérationnels et corréler manuellement les politiques de sécurité d'une console à l'autre. Pour remédier à ce problème, les pare-feu CN-Series sont gérés via Palo Alto Networks Panorama™, une console qui centralise la gestion des composants de sécurité réseau et fait ainsi gagner beaucoup de temps aux analystes sécurité.

CN-Series offre une polyvalence qui couvre un large éventail de cas d'usage, notamment ceux décrits à la page suivante.

Cas d'usage types de CN-Series

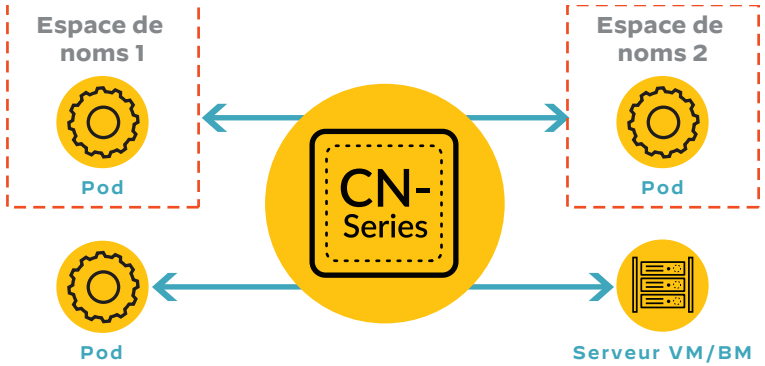
Protection du trafic sortant

Pour prévenir toute exfiltration de données, CN-Series inspecte le contenu du trafic sortant – y compris le trafic TLS/SSL chiffré – et bloque les activités suspectes. Contrairement aux NGFW standards, les pare-feu CN-Series peuvent inspecter tout le trafic sortant en provenance d'une application containerisée. Les fonctionnalités de filtrage d'URL sont particulièrement utiles pour empêcher les développeurs d'accéder involontairement à des sites suspects, notamment les référentiels de code susceptibles d'héberger des malwares.



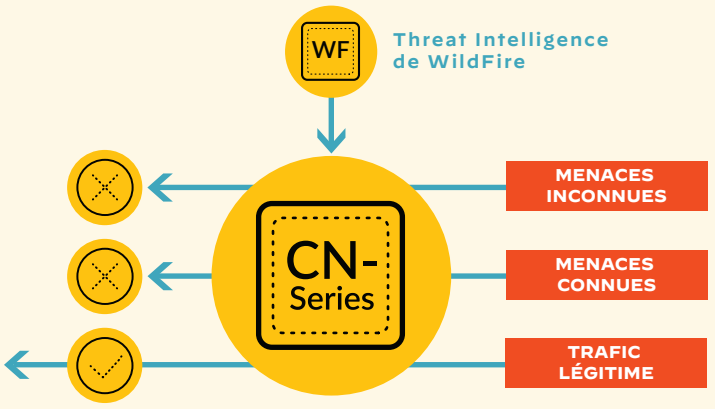
Protection du trafic est-ouest

Les pare-feu CN-Series offrent une bonne visibilité et un bon contrôle sur la couche 7, ainsi que des services de sécurité avancés (IPS, par exemple), pour protéger le trafic est-ouest entre les pods de différentes zones de confiance (entre deux espaces de noms, par exemple). Ils sécurisent également le trafic entre les pods et d'autres types de workloads comme les VM et les serveurs bare metal afin d'homogénéiser la sécurité dans tout votre environnement.



Protection du trafic entrant

Les pare-feu CN-Series bloquent les malwares au moyen de signatures basées sur le contenu, et non sur les hachages. Ainsi, ils vous protègent contre les malwares connus, y compris leurs variantes encore inconnues. Quant au service de prévention des malwares WildFire®, il diffuse les signatures de malwares dans les secondes qui suivent leur découverte pour protéger votre réseau contre les dernières menaces.



Formuler votre stratégie de sécurité réseau cloud-native

À l'heure d'établir une stratégie complète de sécurisation des applications cloud-native pour votre organisation, voici quatre bonnes raisons de préférer les pare-feu Palo Alto Networks CN-Series aux autres solutions du marché :

1. Intégration au DevOps

Les pare-feu CN-Series offrent deux options de déploiement : le pod DaemonSet ou le service Kubernetes. Cette seconde option permet d'exploiter les fonctionnalités de montée en charge automatique de Kubernetes. Les configurations de pare-feu sont spécifiées dans un fichier YAML, ce qui facilite l'intégration du déploiement de NGFW au processus global d'orchestration des containers.

2. Informations contextuelles détaillées sur les containers

CN-Series s'intègre en natif à Kubernetes, ce qui lui permet d'utiliser des informations contextuelles sur les containers (notamment les espaces de noms) pour formuler des politiques de sécurité. Il peut également partager ces informations avec d'autres NGFW Palo Alto Networks pour renforcer votre posture globale de sécurité.

3. Gestion centralisée des politiques

Les politiques des pare-feu CN-Series sont gérées à partir de la même interface que les autres NGFW Palo Alto Networks. Vos équipes disposent ainsi d'une console unique pour piloter la sécurité réseau des workloads physiques, virtuels, containerisés et en cloud public.

4. Sécurité réseau cloud-native complète

Ensemble, Palo Alto Networks Prisma® Cloud et CN-Series allient des fonctions de microsegmentation et des services de sécurité réseau avancés pour réduire la surface d'attaque des applications cloud-native et prévenir les menaces.

Pourquoi CN-Series ?

Intégration au DevOps

Informations contextuelles détaillées sur les containers

Gestion centralisée des politiques

Sécurité réseau cloud-native complète

Envie d'en savoir plus sur CN-Series ? Demandez une démo personnalisée.

Accéder au formulaire

Envie d'en savoir plus sur CN-Series ?
Demandez une démo personnalisée.

paloalto NETWORKS

Oval Tower, De Entrée 99 - 197
1101HE Amsterdam
Pays-Bas

Téléphone : +31 20 888 1883

www.paloaltonetworks.fr

© 2021 Palo Alto Networks, Inc. Palo Alto Networks est une marque déposée de Palo Alto Networks. Pour obtenir une liste de nos marques commerciales, rendez-vous sur https://www.paloaltonetworks.com/company/trademarks.html. Toutes les autres marques mentionnées dans le présent document peuvent être des marques commerciales de leurs détenteurs respectifs.