McAfee Virtual Network Security Platform

Solution complète de détection des menaces et de prévention des intrusions pour les réseaux en cloud

McAfee® Virtual Network Security Platform (McAfee vNSP) est une solution réseau complète pour la prévention des intrusions (IPS) et la protection contre les menaces, conçue pour répondre aux exigences particulières des clouds privés et publics. Capable de détecter et de bloquer rapidement les menaces sophistiquées dans les architectures de cloud avec simplicité et précision, cette solution permet aux entreprises de protéger leurs charges de travail et de rétablir leur conformité en toute confiance. Elle intègre diverses technologies avancées, dont la détection sans signatures, l'émulation en ligne et la correction des vulnérabilités basée sur les signatures. Grâce à des workflows rationalisés, à des options d'intégration flexibles et à un modèle de licences simplifié, les entreprises peuvent facilement gérer et étendre leur sécurité pour répondre à leurs besoins actuels et futurs.

Sécurité complète des clouds publics

Les clouds publics offrent divers avantages : commodité, économies et transition d'un modèle de dépenses d'infrastructure à un modèle de dépenses de fonctionnement. Ils introduisent toutefois un nouveau niveau de risque, dans la mesure où une vulnérabilité dans un logiciel accessible publiquement peut permettre à un cybercriminel d'infiltrer le cloud pour en extraire des informations sensibles, ou divulguer accidentellement des données personnelles de clients à d'autres utilisateurs du même service. McAfee vNSP prend en charge Amazon Web Services (AWS), Microsoft Azure et Oracle Cloud Infrastructure (OCI), les principaux services de cloud public à l'heure actuelle, pour offrir une visibilité complète sur les menaces et une protection de haut vol pour les données transitant par une passerelle Internet ou entre les serveurs (trafic est-ouest).

Protection des environnements virtualisés

De plus en plus d'entreprises adoptent des infrastructures informatiques virtualisées, comme des clouds publics et privés, dans lesquelles les serveurs physiques peuvent héberger simultanément plusieurs machines virtuelles et charges de travail virtualisées. Cette capacité à établir des communications entre machines virtuelles, associée à l'instantanéité de la migration, de la réplication et de la sauvegarde des charges de travail, a entraîné une

Principaux avantages

- Protection complète pour les clouds publics et privés (AWS, Azure et OCI)
- Véritable protection du trafic est-ouest
- Console de gestion centralisée offrant visibilité et contrôle
- Technologies d'inspection avancées pour une protection contre les menaces connues et inconnues
- Disponibilité élevée, reprise après sinistre et équilibrage de la charge pour des performances améliorées
- Partage des licences en cloud plus une flexibilité accrue entre clouds publics et privés
- Intégration avec le portefeuille McAfee de solutions de sécurité, des équipements au cloud
- Disponible sur **AWS Marketplace**
- Disponible sur **Azure Marketplace**

Gardez le contact

augmentation significative du trafic est-ouest à l'intérieur des clouds privés et publics, mais aussi des centres de données définis par logiciel (SDDC). Pour ne rien arranger, la flexibilité offerte par la virtualisation réseau rend ces flux de trafic croissants aussi dynamiques qu'imprévisibles. Pour garder une longueur d'avance, les solutions de sécurité virtualisées se doivent d'être à la fois flexibles et évolutives, mais surtout de fonctionner de manière harmonieuse avec les plates-formes de réseau défini par logiciel (SDN) qui assurent l'orchestration de ces charges de travail et machines virtuelles souvent éphémères.

Agilité des clouds privés

McAfee vNSP s'intègre en toute transparence avec diverses plates-formes de cloud privé populaires, notamment les environnements SDN basés sur OpenStack et VMware NSX. Elle est la seule solution IPS virtuelle dédiée dont la compatibilité avec VMware NSX est officiellement certifiée. La microsegmentation des machines virtuelles et l'inspection approfondie du trafic est-ouest sont automatiquement assurées dans les environnements virtualisés, malgré la rapidité avec laquelle les charges de travail sont créées, migrées et mises hors service.

Prévention des menaces avancées

McAfee vNSP s'appuie sur une architecture d'inspection de nouvelle génération, conçue pour examiner en profondeur le trafic des réseaux virtuels. La plate-forme associe diverses technologies d'inspection avancées, dont l'analyse complète de protocoles, l'analyse des menaces basée sur la réputation, l'analyse du comportement et l'analyse antimalware avancée. Cette approche permet de détecter et de prévenir tant les menaces connues que les attaques « jour zéro » inconnues sur le réseau.

Aucune technologie de détection des logiciels malveillants ne peut, à elle seule, refouler toutes les attaques. C'est pourquoi McAfee vNSP intègre en couches plusieurs moteurs de détection, avec et sans signatures, pour empêcher les logiciels malveillants de mettre à mal vos clouds. Il utilise plusieurs technologies d'inspection, comme l'émulation en ligne du navigateur, du code JavaScript et des fichiers Adobe ; la détection des rappels des réseaux de robots et logiciels malveillants ; la détection des attaques DDoS par analyse du comportement ou encore la protection contre les attaques avancées, comme les scripts intersites ou les attaques par injection de code SQL.

McAfee vNSP est en outre capable d'identifier et de bloquer les fichiers les plus furtifs grâce à son intégration avec McAfee Advanced Threat Defense, qui soumet les fichiers à une analyse comportementale. McAfee Advanced Threat Defense combine analyse statique de code, analyse dynamique (sandboxing) et **apprentissage automatique** pour offrir une protection renforcée contre les menaces « jour zéro », notamment celles qui utilisent des techniques de contournement et les ransomwares. McAfee offre également une prise en charge native des signatures Snort pour détecter et bloquer les logiciels malveillants.

En savoir plus

- **Protection de vos réseaux virtuels Amazon Web Services**
- **Protection de vos réseaux virtuels Microsoft Azure**

Partage flexible des licences pour le cloud

De nombreuses entreprises répartissent leurs ressources et infrastructures informatiques sur différents clouds et plates-formes, que ce soit pour assurer la prise en charge d'anciennes applications, pour éviter de dépendre d'un fournisseur unique, pour réduire la redondance des systèmes ou pour réaliser des économies. La gestion des licences des solutions de sécurité pour environnements virtualisés peut se révéler complexe et onéreuse. En effet, la plupart des fournisseurs imposent l'achat de licences distinctes pour les clouds publics et privés, ainsi que pour les différentes plates-formes SDN.

McAfee simplifie la gestion des licences et réduit les coûts grâce au partage des licences pour le cloud, qui permet aux entreprises de partager les performances et les licences de McAfee vNSP sur une combinaison quelconque de plates-formes de clouds publics et privés. Le partage des licences pour le cloud offre une flexibilité accrue et améliore la sécurité. Non seulement il offre aux administrateurs la possibilité d'assurer rapidement la protection du trafic est-ouest et la microsegmentation des charges de travail virtuelles où qu'elles se trouvent, mais il évite tous les problèmes liés aux formules de licence complexes et au processus fastidieux d'approvisionnement.

Workflows et analyses rationalisés

Les menaces modernes peuvent générer de nombreuses alertes et ainsi déborder rapidement la capacité de priorisation et de surveillance des équipes de sécurité. Si la réaction est trop lente, des menaces réelles risquent de passer inaperçues. McAfee vNSP propose des fonctions d'analyse avancée et des workflows exploitables qui mettent en corrélation plusieurs alertes IPS et les regroupent dans un événement unique sur lequel il est possible d'agir. Les administrateurs peuvent ainsi identifier rapidement les informations pertinentes. En outre, l'intégration avec d'autres solutions de sécurité McAfee permet d'offrir une plate-forme véritablement complète et connectée pour la détection et la neutralisation des menaces réseau.

Gestion centralisée de la sécurité pour un contrôle et une visibilité en temps réel

Une appliance McAfee Network Security Manager unique assure une gestion web centralisée garantissant un contrôle et une visibilité en temps réel. La console de pointe vous assure un contrôle en temps réel sur les données à partir d'un emplacement centralisé. Vous pouvez facilement gérer, configurer et surveiller toutes les appliances McAfee Network Security Platform, virtuelles ou physiques, ainsi que les appliances McAfee Network Threat Behavior Analysis dans l'ensemble de vos environnements : classique, cloud public et cloud privé. Évolutive, l'interface intuitive peut facilement gérer des clusters stratégiques fortement distribués.

McAfee Network Security Manager peut également être déployé sous la forme d'une instance virtuelle sur des serveurs VMware ESX et dans les environnements AWS ou Azure. McAfee vNSP prend en charge la fonction de gestion des identités et de l'accès (IAM) d'AWS, ce qui permet aux administrateurs de gérer l'accès aux services et ressources AWS de façon simple et sécurisée, en fonction des permissions octroyées à des groupes et à des utilisateurs spécifiques.

Disponibilité élevée, reprise après sinistre et équilibrage de la charge

McAfee vNSP s'appuie sur plusieurs méthodes pour offrir en continu un niveau de contrôle, une protection et des performances hors pair. McAfee Network Security Manager assure une disponibilité élevée grâce à une surveillance proactive de l'environnement. Si le contrôleur actif n'est plus disponible, McAfee Network Security Manager bascule automatiquement vers un contrôleur en veille pour garantir une visibilité et une sécurité ininterrompues. Par ailleurs, une appliance McAfee Network Security Manager en mode veille peut être déployée pour assurer la reprise après sinistre pour les environnements AWS, Azure et OCI.

McAfee vNSP offre également la disponibilité élevée dont les sondes IPS ont besoin. Si une sonde n'est plus disponible, une fonction d'allocation automatique crée instantanément une nouvelle sonde IPS virtuelle, garantissant ainsi une protection transparente et continue. En outre, si le trafic réseau augmente, l'équilibrage automatique de la charge permet d'optimiser les performances, et de nouvelles sondes peuvent être déployées automatiquement pour préserver le débit requis.

Sécurité intégrée

Les attaques sophistiquées ne respectent pas les frontières entre les produits et exploitent très vite la moindre faille au niveau de l'infrastructure, notamment entre les produits de sécurité. McAfee vNSP est la seule solution IPS capable de s'intégrer en toute transparence à de nombreux produits de sécurité. Elle tire parti des données et des workflows de ces solutions pour vous offrir une sécurité et une protection accrues, ainsi qu'un meilleur retour sur investissement. Voici quelques exemples d'intégration de solutions de sécurité McAfee :

- **McAfee ePolicy Orchestrator® (McAfee ePO™) :** Visibilité complète sur les terminaux pour l'ensemble des alertes et événements IPS
- **McAfee Endpoint Intelligence Agent :** Combinaison des perspectives sur le réseau et les terminaux, pour empêcher les fuites de données
- **McAfee Enterprise Security Manager :** Partage de données riches et mise en quarantaine pour les alertes IPS
- **McAfee Threat Intelligence Exchange :** Apprentissage partagé entre différents types d'équipements
- **McAfee Global Threat Intelligence :** Service de réputation le plus étendu et le plus actif au monde
- **McAfee Network Threat Behavior Analysis :** Visibilité étendue sur tout le réseau
- **McAfee Virtual Advanced Threat Defense :** Inspection approfondie pour détecter les menaces employant des techniques de contournement
- **McAfee Cloud Threat Detection :** Service s'intégrant avec les solutions de sécurité McAfee existantes pour détecter les logiciels malveillants avancés
- **McAfee Management for Optimized Virtual Environments (McAfee MOVE) :** Solution antivirus conçue pour les environnements virtuels
- **Analyseurs de vulnérabilités tiers :** Analyse des risques et des hôtes pour les terminaux

Fonctionnalités supplémentaires

Prévention des menaces avancées

- Moteur d'émulation McAfee Gateway Anti-Malware
- Moteur d'émulation pour code JavaScript incorporé dans les PDF (environnement sandbox léger)
- Moteur d'analyse comportementale pour Adobe Flash
- Protection contre les AET

Protection contre les rappels des logiciels malveillants et des réseaux de robots (botnets)

- Détection des rappels « fast-flux » via DNS ou DGA
- Redirection vers un serveur DNS sinkhole
- Détection heuristique des robots
- Corrélation d'attaques multiples
- Base de données de processus de contrôle et commande

Prévention avancée des intrusions

- Défragmentation IP et réassemblage des flux TCP
- Signatures McAfee, définies par l'utilisateur et à code source libre
- Mise en quarantaine de l'hôte et limitation du débit
- Inspection des environnements virtuels
- Prévention des attaques par déni de service (DoS) et déni de service distribué (DDoS)
- Amélioration des listes blanches et listes noires pour prendre en charge le format STIX (Structured Threat Information eXpression)
- Détection heuristique et basée sur des seuils
- Limitation des connexions basée sur l'hôte
- Prise en charge native des signatures Snort
- Détection basée sur les profils, avec autoapprentissage

McAfee Global Threat Intelligence

- Réputation des fichiers
- Réputation des adresses IP
- Accès restreint par géolocalisation
- Contrôle d'accès basé sur l'adresse IP

FICHE TECHNIQUE

	Type de sonde 1	Type de sonde 2
Plate-forme	VMware ESX 5.5/6.0/6.5	AWS Azure OCI VMware vSphere 6.5 et NSX 6.3
Modèle de la sonde IPS virtuelle	**IPS-VM600**	**IPS-VM600-VSS**
Type de déploiement IPS virtuel	Autonome	Distribué
Prise en charge VMware NSX	Non	Oui
Prise en charge AWS	Non	Oui
Prise en charge Azure	Non	Oui
Prise en charge OCI	Non	Oui
Nombre de processeurs logiques	4	AWS 4, Azure 5
Espace mémoire requis	6 Go	6 Go
Stockage	8 Go	8 Go
Spécifications de la sonde virtuelle		
Débit maximal	Jusqu'à 1 Gbit/s	Jusqu'à 1 Gbit/s
Paires de ports de surveillance	3	1 (port de surveillance, pas une paire de ports)
Interfaces virtuelles (VIDS) par sonde	100	100
Profils d'attaque par déni de service	300	300
Port de gestion	Oui	Oui
Port de réponse	Non	Non
Modes de déploiement	Inspection entre machines virtuelles, inspection entre machines physiques et virtuelles, inspection entre machines physiques, inspection des ports SPAN/en ligne	

McAfee
Together is power.

11-13 Cours Valmy - La Défense 7
92800 Puteaux, France
+33 1 4762 5600
www.mcafee.com/fr