FICHE TECHNIQUE

McAfee Virtual Network Security Platform

Détection complète des menaces pour les réseaux en cloud

McAfee® Virtual Network Security Platform 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. Elle est capable de détecter et de bloquer les menaces sophistiquées dans les architectures de cloud avec simplicité et précision, permettant ainsi aux entreprises de rétablir leur conformité et d'adopter en toute confiance des technologies de sécurité de cloud. La solution intègre diverses technologies avancées, dont la détection sans signatures, l'émulation en ligne, la correction des vulnérabilités basée sur les signatures ou encore la prise en charge d'Amazon Web Services (AWS) et de la virtualisation réseau. Grâce à des workflows rationalisés, à de multiples options d'intégration et à une gestion simplifiée des licences, les entreprises peuvent facilement déployer et adapter leur sécurité, même dans les architectures de cloud les plus complexes.

Protection intégrale des clouds publics basée sur des technologies de sécurité avancées

Les clouds publics offrent divers avantages : commodité, économies et possibilité de passer 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 Virtual Network Security Platform prend en charge AWS, le principal service de cloud public à l'heure actuelle, afin de proposer une visibilité complète sur les menaces pour les données transitant par une passerelle Internet, ainsi que sur le trafic est-ouest. Grâce à cette solution, vous pouvez recouvrer votre visibilité sur les menaces et rétablir la conformité de vos architectures de cloud public via une plate-forme IPS assurant une inspection efficace du trafic est-ouest.

Principaux avantages

Prévention optimale des menaces avancées

- Analyse antimalware avancée sans signatures
- Protection contre les vulnérabilités de type scripts intersites (cross-site scripting) et injection de code SQL
- Détection avancée des rappels des réseaux de robots et logiciels malveillants
- Analyse comportementale et protection contre les attaques par déni de service distribué (DDoS)
- Intégration avec McAfee Advanced Threat Defense
- Déploiement de systèmes IPS et IDS pour la prévention et la détection des intrusions
- Solution McAfee Virtual Network Security Platform sur VMware ESX pour une protection permanente

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, de même que des charges de travail virtualisées complètes. 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 augmentation significative du trafic est-ouest à l'intérieur des clouds privés et publics, mais aussi des 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.

Développement de l'agilité des clouds privés

Conçu pour répondre aux besoins de protection des environnements virtualisés, McAfee Virtual Network Security Platform s'intègre en toute transparence avec diverses plates-formes de cloud privé populaires, notamment les environnements SDN basés sur OpenStack et VMware NSX. McAfee Virtual Network Security Platform 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, et ce malgré la création, la migration et la mise hors service rapides des charges de travail.

Prévention des menaces inégalée

McAfee Virtual Network Security Platform s'appuie sur une architecture d'inspection de nouvelle génération, conçue pour inspecter 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, pour détecter et prévenir tant les menaces connues que les menaces « jour zéro » sur le réseau.

Aucune technologie de détection des logiciels malveillants ne peut, à elle seule, refouler toutes les attaques. C'est pourquoi McAfee Virtual Network Security Platform intègre en couches plusieurs moteurs de détection, avec et sans signatures, pour empêcher les logiciels malveillants de mettre à mal vos clouds. Il propose notamment 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 l'injection de code SQL. McAfee Virtual Network Security Platform 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 approfondie. McAfee Advanced

Architecture adaptée au cloud

- Partage du débit entre n'importe quelle combinaison de clouds publics et privés au moyen d'une licence unique
- Approche innovante de l'inspection AWS pour assurer une protection réelle du trafic est-ouest dans les clouds publics
- Prise en charge de l'orchestration avec les environnements SDN basés sur OpenStack et VMware NSX pour une microsegmentation et une inspection du trafic automatisées entre les charges de travail de cloud privé
- Tableau de bord adapté aux machines virtuelles avec fonction de mise en quarantaine disponible avec l'intégration VMware
- Console de gestion centralisée unique pour les sondes physiques et virtuelles, sur site et dans le cloud

Gestion intelligente de la sécurité

- Gestion des sondes sur site et dans le cloud à l'aide d'une console unique
- Mise en corrélation et priorisation intelligentes des alertes
- Tableaux de bord d'analyse des logiciels malveillants
- Workflows d'investigation préconfigurés
- Gestion web évolutive

Threat Defense combine analyse statique de code, analyse dynamique (sandboxing) et apprentissage automatique pour offrir une protection renforcée contre les menaces de type « jour zéro », notamment celles qui utilisent des techniques de contournement et les ransomwares.

Simplifiez-vous la vie avec le partage des licences en cloud

De nombreuses entreprises répartissent aujourd'hui 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, dans la mesure où la plupart des fournisseurs imposent l'achat de licences distinctes pour les clouds publics et privés, ainsi pour les différentes plates-formes SDN.

McAfee simplifie la gestion des licences et réduit les coûts grâce au « partage des licences en cloud », un concept nouveau qui permet aux clients de partager les performances et les licences de McAfee Virtual Network Security Platform sur une combinaison quelconque de plates-formes de clouds publics et privés. Le partage des licences en cloud améliore en outre la sécurité en offrant 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, ce qui leur évite de perdre du temps dans le processus fastidieux d'approvisionnement.

Rationalisation des workflows et des analyses

Détectez et neutralisez facilement les menaces les plus sophistiquées. McAfee Virtual Network Security Platform inclut des fonctionnalités d'analyse avancée et d'intégration avec d'autres solutions de sécurité pour offrir une plate-forme véritablement complète et connectée de détection et de neutralisation des menaces réseau.

Les menaces modernes peuvent générer de nombreuses alertes et ainsi déborder rapidement la capacité de priorisation et de surveillance des professionnels de la sécurité. Si ceux-ci ne réagissent pas assez vite, des menaces réelles risquent d'échapper à leur attention. Les fonctions d'analyse avancée et les workflows exploitables, prêts à l'emploi, permettent à McAfee Virtual Network Security Platform de faire le tri entre les informations superflues et les données pertinentes pour mettre en corrélation plusieurs alertes IPS et les regrouper dans un événement unique exploitable.

Gestion centralisée avec contrôle instantané des données en temps réel

Une gestion web centralisée, d'une facilité d'emploi inégalée, est assurée par une appliance McAfee Network Security Manager unique. La console, qui intègre des technologies de pointe dans une interface graphique optimisée, vous donne accès à des données en temps réel. 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 sur l'ensemble de vos ressources de cloud public, privé et classiques à partir d'une seule et même console. L'interface web intuitive de la console permet

Visibilité et contrôle

- Identification des applications
- Identification des utilisateurs
- Identification des équipements
- Visibilité sur l'état de sécurité de toutes les machines virtuelles grâce à AWS

de gérer tous types de déploiement : des équipements uniques aux 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 AWS.

Reprise après sinistre et haute disponibilité

McAfee Network Security Manager opère un arbitrage entre les contrôleurs et détermine lequel est actif et lequel est en mode veille. Dès que le contrôleur actif n'est plus disponible, le contrôleur en veille devient actif. Ainsi, les déploiements AWS tirent parti d'une disponibilité élevée des contrôleurs, grâce à un mécanisme de basculement qui garantit qu'un contrôleur est toujours actif et accessible. Par ailleurs, une appliance McAfee Network Security Manager en mode veille assure la reprise après sinistre pour les environnements AWS.

La prise en charge de fonctions de reprise après sinistre du gestionnaire (MDR, Manager Disaster Recovery), de haute disponibilité des contrôleurs et d'extension automatique des sondes IPS virtuelles permet à McAfee Virtual Network Security Platform d'offrir une disponibilité élevée. La solution peut ainsi fonctionner de manière transparente sans la moindre interruption. La fonction MDR permet de disposer d'un deuxième gestionnaire qui prend le relais du gestionnaire principal lorsque ce dernier est à l'arrêt. La fonction de haute disponibilité des contrôleurs s'appuie sur une paire de contrôleurs, de sorte que l'un des deux soit toujours actif et accessible pour éviter toute indisponibilité du réseau. Enfin, la fonction d'extension automatique des sondes IPS virtuelles crée une nouvelle sonde IPS virtuelle dès qu'une instance de la sonde est hors service. Ainsi, la charge de travail est répartie dès que le trafic réseau s'intensifie.

Architecture de défense unifiée

Les attaques sophistiquées ne respectent pas les frontières entre les produits et exploitent la moindre faille au niveau de l'infrastructure, notamment entre les produits de sécurité. McAfee Virtual Network Security Platform est la seule solution IPS qui s'intègre à de nombreux produits de sécurité pour combler toutes ces failles en tirant parti des données et des workflows. Vous bénéficiez ainsi d'un meilleur retour sur investissement et d'une réduction du coût total de possession. La solution est notamment intégrée avec les produits de sécurité suivants :

- **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**
- **McAfee Cloud Threat Detection**
- **McAfee Management for Optimized Virtual Environments (McAfee MOVE)**
- **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 réseaux de robots et logiciels malveillants

- 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 commande et de contrôle

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)
- Détection heuristique et basée sur des seuils
- Limitation des connexions basée sur l'hôte
- 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	Type de sonde 3
Plate-forme	VMware ESX 5.5/6.0/6.5 KVM/OpenStack	VMware ESX 5.5/6.0/6.5 KVM/OpenStack	VMware ESX 5.5/6.0/6.5 NSX 6.3 AWS
Modèle de la sonde IPS virtuelle	**IPS-VM100**	**IPS-VM600**	**IPS-VM100-VSS**[1]
Type de déploiement IPS virtuel	Autonome	Autonome	Distribué
Prise en charge VMware NSX	Non	Non	Oui
Prise en charge AWS	Non	Non	Oui
Nombre de cœurs de processeur logiques[2]	3	4	3
Espace mémoire requis[3]	4 Go	6 Go	5 Go
Spécifications de la sonde virtuelle			
Débit maximal[4]	Jusqu'à 500 Mbit/s	Jusqu'à 1 Gbit/s	Jusqu'à 500 Mbit/s
Connexions simultanées	200 000	600 000	200 000
Connexions établies par seconde	6 000	20 000	6 000
Flux UDP pris en charge	39 168	254 208	39 168
Paires de ports de surveillance	2	3	1[5]
Interfaces virtuelles (VIDS) par sonde	32	100	32
Profils d'attaque par déni de service	100	300	100
Port de gestion	Oui	Oui	Oui
Port de réponse	Oui	Oui	Non
Modes de déploiement	Inspection entre machines virtuelles, inspection entre machines physiques et virtuelles, inspection entre machines physiques, inspection des ports SPAN		Inspection en ligne VMware NSX

1. Pour utilisation dans les environnements VMware NSX uniquement, en tant que service intégré.
2. Les ressources nécessaires pour les machines virtuelles peuvent varier selon les versions. Veuillez vous reporter à la documentation propre à votre version du produit.
3. Ibid.
4. Mesuré avec des paquets UPD de 1 518 octets dans des conditions de test optimales.
5. Représentation virtuelle d'entrée et de sortie. L'inspection est étroitement liée à VMware NSX au niveau du noyau.

McAfee
Together is power.

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