McAfee Web Gateway

Sécurité. Cyberveille connectée. Performances.

Plus que jamais, le Web offre d'innombrables opportunités aux entreprises. Il fait vivre aux utilisateurs une expérience dynamique en temps réel. Malheureusement, il est aussi devenu plus dangereux en raison de la multiplication des attaques informatiques qui y sévissent tous les jours. McAfee® Web Gateway constitue une ligne de défense critique pour toute entreprise désireuse de se protéger contre les logiciels malveillants émergents. Cette solution offre aux entreprises un accès Internet sécurisé tout en réduisant considérablement les risques grâce à une approche avancée de la sécurité, associant des fonctions puissantes d'analyse des intentions en local et une protection via le cloud, optimisée par McAfee Labs.

L'utilisation de plus en plus répandue et la sophistication croissante d'Internet imposent de renforcer la sécurité de l'environnement web. Même les sites qui semblent sûrs en apparence peuvent constituer une source de propagation de logiciels malveillants. À l'heure actuelle, on ne peut se contenter de bloquer les virus connus ou de limiter l'accès à des sites web reconnus comme dangereux. Bien qu'encore nécessaires, les techniques réactives, telles que les antivirus basés sur les signatures ou le filtrage d'URL par catégories uniquement, ne suffisent plus à assurer une connexion sécurisée aux applications de cloud ou à combattre les exploits.

En outre, elles se concentrent uniquement sur le contenu connu et les objets ou fichiers exécutables malveillants : elles ne sont donc pas en mesure de prévenir les attaques actuelles qui dissimulent du code malveillant dans du trafic HTTP ou HTTPS en apparence inoffensif. Or, il est crucial de pouvoir garantir un accès granulaire sécurisé aux applications de cloud tout en bloquant de façon proactive les menaces tant connues qu'inconnues.

Protection complète du trafic à l'entrée et en sortie

McAfee Web Gateway garantit une protection complète de tous les aspects du trafic web au sein d'une architecture d'appliance logicielle hautes performances. Dans le cas de requêtes de pages web initiées par l'utilisateur, McAfee Web Gateway met d'abord en

McAfee Web Gateway

- Disponible dans plusieurs formats matériels et en tant que machine virtuelle prenant en charge VMware et Microsoft Hyper-V
- Intégration à des solutions complémentaires McAfee telles que McAfee Endpoint Security, McAfee Advanced Threat Defense, McAfee Threat Intelligence Exchange, McAfee Cloud Data Protection et McAfee Cloud Visibility — Community Edition
- Certifications Common Criteria EAL2+ et FIPS 140-2 Level 2
- Prise en charge de plusieurs types de stockage de clés cryptographiques, notamment le module de sécurité matériel (HSM) Gemalto SafeNet, le module de sécurité matériel (HSM) Thales nShield et les cartes PCIe Thales
- Fonction antimalware intégrée à une passerelle web sécurisée la mieux cotée du secteur (AV-TEST)

œuvre la stratégie de l'entreprise en matière d'utilisation d'Internet. Pour le trafic autorisé, il utilise ensuite des techniques locales et globales pour analyser la nature et les intentions de l'ensemble du contenu et du code actif pénétrant sur le réseau via les requêtes de pages web : il peut ainsi offrir une protection immédiate contre les logiciels malveillants et autres menaces cachées. En outre, contrairement aux techniques de base d'inspection des paquets, McAfee Web Gateway examine le trafic SSL (Secure Socket Layer) afin d'assurer une protection en profondeur contre le code malveillant ou les applications de contrôle camouflés par le biais du chiffrement.

La protection du trafic à l'entrée réduit également les risques auxquels sont exposées les entreprises qui hébergent des sites web autorisant la réception de données ou de documents à partir de sources externes. En mode proxy inverse, McAfee Web Gateway analyse l'intégralité du contenu avant même qu'il ne soit téléchargé, protégeant ainsi le serveur et le contenu.

Pour sécuriser le trafic en sortie, McAfee Web Gateway utilise les technologies de prévention des fuites de données de tout premier ordre de McAfee pour analyser le contenu généré par les utilisateurs sur les principaux protocoles web, dont HTTP, HTTPS et FTP. Il prévient également les fuites d'informations confidentielles, sensibles ou réglementées via des vecteurs tels que les sites de réseaux sociaux, les blogs et les wikis, ou encore les outils de productivité en ligne comme la messagerie web, les organiseurs et les agendas. De plus, McAfee Web Gateway protège les entreprises contre les fuites de données par le biais d'ordinateurs infectés par des robots qui tentent de communiquer avec leur site d'origine ou de transmettre des données sensibles.

La meilleure protection disponible sur le marché

Solution de sécurité web la mieux cotée[1] en ce qui concerne la détection des logiciels malveillants, McAfee Web Gateway utilise une approche brevetée pour analyser les intentions sans signatures, à l'aide du moteur McAfee Gateway Anti-Malware Engine. L'analyse proactive des intentions élimine du trafic web, en temps réel, le contenu malveillant précédemment inconnu ou le contenu de type « jour zéro ». Grâce à l'examen du contenu actif des pages web, à l'émulation, à l'analyse comportementale et à l'analyse prédictive des intentions, McAfee Web Gateway empêche la propagation de malware de type « jour zéro » sur les terminaux, réduisant ainsi considérablement les coûts associés à l'assainissement des systèmes et à l'application de mesures correctives.

McAfee combine ces fonctions d'analyse avec l'antivirus McAfee et les technologies de réputation à l'échelle mondiale de McAfee Labs pour bloquer rapidement les logiciels et sites malveillants connus. Le recours à un ensemble de technologies diverses mais complémentaires permet à McAfee Web Gateway d'offrir une protection supérieure, tout en optimisant la sécurité grâce à une plate-forme unique. Il s'agit là d'une exigence de nombreuses entreprises désireuses de mettre en place une stratégie de défense multiniveau.

- **Combinaison de l'antivirus McAfee et du service d'analyse de réputation en temps réel McAfee Global Threat Intelligence (McAfee GTI) —** L'analyse de la réputation des fichiers dans le cloud exécutée grâce à McAfee GTI comble le délai entre la découverte d'un virus et la mise à jour de la protection des systèmes.
- **Service d'analyse de réputation et de catégorisation des sites web de McAfee GTI —** McAfee Web Gateway propose une fonction de filtrage web améliorée et une protection renforcée grâce à la combinaison efficace de deux types de filtrages, basés respectivement sur la réputation et sur les catégories. McAfee GTI crée un profil de toutes les entités Internet (sites web, e-mails et adresses IP) sur la base de centaines d'attributs différents recueillis grâce aux capacités de collecte de données en masse, à l'échelle mondiale, de McAfee Labs. Il attribue ensuite un score de réputation en fonction du risque pour la sécurité, ce qui permet aux administrateurs d'appliquer des règles granulaires précisant les actions autorisées ou interdites.
- **Géolocalisation —** McAfee Web Gateway propose des fonctions de géolocalisation qui offrent une visibilité géographique et permettent de gérer les stratégies selon le pays d'origine du trafic web.

Que ce soit pour la catégorisation des sites web ou l'évaluation de la réputation web, les entreprises ont désormais le choix entre trois types de recherches : sur site, dans le cloud et une combinaison des deux. Les recherches dans le cloud éliminent les failles de protection dues aux délais entre la découverte des menaces et la mise à jour des systèmes. Elles offrent une couverture étendue grâce à des données couvrant des centaines de millions d'échantillons uniques de logiciels malveillants.

Intégration de l'analyse des menaces avancées

McAfee Web Gateway s'intègre avec McAfee Advanced Threat Defense, notre technologie avancée de détection antimalware qui combine une analyse en environnement sandbox personnalisable avec l'analyse statique approfondie de code. Ensemble, McAfee Advanced Threat Defense et les fonctionnalités d'analyse en ligne du moteur McAfee Gateway Anti-Malware Engine de McAfee Web Gateway offrent la protection contre les menaces Internet la plus efficace du marché. Les entreprises souhaitant bénéficier d'une fonction simplifiée et à moindre coût pour l'analyse des menaces avancées peuvent intégrer McAfee Cloud Threat Detection, un environnement sandbox dans le cloud offrant plusieurs niveaux supplémentaires d'analyse des menaces.

Partage de cyberveille sur les menaces

À l'heure actuelle, un grand nombre d'outils de sécurité fonctionnent de façon isolée et ne sont pas conçus pour partager la cyberveille sur les menaces, alors que des renseignements clés sont pourtant disponibles à divers niveaux — du terminal au réseau en passant par la passerelle, la solution SIEM et ainsi de suite. Lorsqu'elles sont partagées, ces informations permettent d'assurer une meilleure protection contre les menaces, une détection plus performante des compromissions existantes et une correction efficace des systèmes compromis pour une réponse aux incidents améliorée.

Grâce à McAfee Threat Intelligence Exchange, les solutions McAfee, dont McAfee Web Gateway, partagent cette cyberveille entre elles afin de combler ces défaillances de communication. McAfee Web Gateway apporte une valeur ajoutée considérable en créant et partageant des données de réputation des fichiers pour les logiciels malveillants de type « jour zéro » découverts par le moteur McAfee Gateway Anti-Malware Engine. Cela permet ainsi de protéger les terminaux avant même qu'un nouveau fichier DAT ne soit publié. Par ailleurs, les informations de cyberveille étendues fournies par McAfee Threat Intelligence Exchange permettent à McAfee Web Gateway de bloquer un nombre accru de menaces.

Informations et protection du trafic chiffré

Les cybercriminels les plus avertis utilisent désormais le trafic SSL (HTTPS et HTTP/2) pour se soustraire aux dispositifs de sécurité de l'entreprise. C'est ainsi que, de manière tout à fait paradoxale, un protocole conçu pour assurer la sécurité doit à son tour faire l'objet d'une évaluation des risques. McAfee Web Gateway intègre des fonctions de détection des logiciels malveillants, d'inspection du trafic SSL et de validation des certificats pour une approche complète de l'inspection du trafic chiffré.

Toutes ces fonctions sont intégrées au sein d'une appliance matérielle ou virtuelle unique. Ainsi, aucun investissement supplémentaire n'est nécessaire dans des composants matériels d'analyse du trafic SSL. McAfee Web Gateway analyse directement l'intégralité du trafic SSL afin de garantir la sécurité, l'intégrité et la confidentialité des transactions chiffrées.

Les entreprises qui souhaitent implémenter une inspection plus approfondie de leur trafic SSL peuvent transférer tout leur flux de trafic non chiffré ou des flux individuels définis par stratégie vers la fonctionnalité SSL TAP de McAfee Web Gateway. Cette fonctionnalité activée par logiciel permet l'envoi d'un miroir complet ou partiel du trafic SSL déchiffré à d'autres solutions de sécurité telles que les systèmes de prévention des intrusions (IPS) ou les solutions de prévention des fuites de données (DLP) au niveau du réseau.

Prévention des fuites de données

McAfee Web Gateway protège les entreprises contre les menaces en sortie (telles que les fuites d'informations confidentielles) en analysant le contenu en sortie au niveau des principaux protocoles Internet, dont SSL. Il apparaît dès lors comme un outil performant pour éviter la perte d'éléments de propriété intellectuelle, garantir et documenter la conformité aux réglementations et fournir des données d'investigation numérique en cas d'infraction. Exploitant la puissance de la gamme de solutions McAfee Data Loss Prevention (McAfee DLP), McAfee Web Gateway inclut des dictionnaires prédéfinis intégrés de prévention des fuites de données et permet la création de dictionnaires personnalisés par correspondance de mots clés et/ou d'expressions régulières.

Pour les entreprises qui utilisent le stockage dans le cloud, le chiffrement intégré des fichiers protège les données transférées sur des sites de partage et de collaboration contre les accès non autorisés. Les utilisateurs ne peuvent donc ni récupérer ni consulter les données sans passer par McAfee Web Gateway.

Protection des utilisateurs non connectés au réseau

Face à la distribution et à la mobilité croissantes du personnel, il est devenu impératif d'assurer le filtrage web et la protection de l'environnement web tout en garantissant une protection sans faille aux utilisateurs lors de leurs déplacements. McAfee Client Proxy, un agent client inaltérable, permet une authentification transparente des utilisateurs itinérants et redirige ces derniers soit vers une appliance McAfee Web Gateway installée sur site dans une zone démilitarisée (DMZ), soit vers McAfee Web Gateway Cloud Service. De cette façon, la mise en œuvre des stratégies d'accès Internet et l'analyse de sécurité complète peuvent être appliquées aux utilisateurs itinérants ou distants — même lorsqu'ils accèdent à Internet depuis un portail public, comme dans un café, un hôtel ou tout autre point d'accès public sans fil.

McAfee Web Gateway permet également aux entreprises d'étendre et d'appliquer leurs stratégies de sécurité sur leurs équipements mobiles en dirigeant le trafic web vers McAfee Web Gateway. Grâce à nos partenariats avec les éditeurs de solutions de gestion des équipements mobiles AirWatch et MobileIron, les appareils Apple iOS et Google Android sont ainsi couverts par une protection antimalware avancée et des stratégies de filtrage web d'entreprise.

Flexibilité inégalée grâce à McAfee Web Gateway

McAfee Web Gateway est doté d'un moteur de règles puissant pour une flexibilité et un contrôle optimaux des stratégies. En vue de rationaliser la création de stratégies, la solution propose une vaste bibliothèque de règles prédéfinies combinées à des actions de stratégies communes. Les entreprises peuvent choisir diverses règles, les modifier facilement et partager leurs propres règles par l'intermédiaire de notre communauté en ligne. Pour l'administration avancée, une combinaison unique de critères contextuels pour les règles et de listes partagées ouvre des possibilités infinies en termes de résolution de problèmes et d'optimisation de la sécurité web. Le traçage interactif des règles simplifie le débogage de ces dernières.

McAfee Web Gateway étend le contrôle aux applications de cloud, offrant ainsi un contrôle granulaire (basé sur un proxy) sur l'utilisation des applications web. Les entreprises peuvent appliquer plusieurs milliers de contrôles aux applications de cloud et, au besoin, activer ou désactiver des fonctions spécifiques. Elles peuvent également contrôler les utilisateurs ayant accès à une application web ainsi que les modalités d'utilisation de celle-ci. Vous souhaitez autoriser l'accès à Dropbox tout en bloquant le transfert de données ? Aucun problème.

La flexibilité et le contrôle de la passerelle web s'étendent également à l'authentification et à l'accès des utilisateurs. McAfee Web Gateway prend en charge de nombreuses méthodes d'authentification, telles que NT LAN Manager (NTLM), le service RADIUS (Remote Authentication Dial In User Service), Active Directory ou LDAP (Lightweight Directory Access Protocol), eDirectory, Kerberos, les cookies d'authentification ou une base de données utilisateur locale. Le moteur d'authentification McAfee Web Gateway permet aux administrateurs de mettre

en œuvre des règles flexibles, notamment l'utilisation de plusieurs méthodes d'authentification. Par exemple, McAfee Web Gateway peut tenter d'authentifier un utilisateur de façon transparente et, en fonction du résultat, lui demander ses informations d'identification, utiliser une autre méthode d'authentification, appliquer une stratégie restrictive ou simplement lui refuser l'accès.

Le module complémentaire facultatif McAfee Web Gateway Identity inclut des connecteurs d'authentification unique (SSO) pour plusieurs centaines d'applications de cloud populaires. Grâce à sa plate-forme de lancement SSO permettant aux utilisateurs d'accéder aux applications de cloud autorisées en un seul clic, ce module renforce la sécurité et réduit le nombre d'appels d'assistance technique liés aux mots de passe. En outre, la prise en charge des connecteurs HTTP POST (Power-On Self-Test) et SAML (Security Assertion Markup Language) assure la couverture d'un large éventail d'applications. L'activation de ces connecteurs permet aux administrateurs système de créer et de supprimer des comptes utilisateur pour certaines applications SaaS (Software-as-a-Service).

McAfee Web Gateway étend le contrôle d'accès au contenu diffusé en flux continu par le biais de la prise en charge native de proxys de diffusion, ce qui permet de réaliser des économies de bande passante et de réduire la latence. Il est possible de configurer d'autres contrôles de la bande passante pour prioriser et appliquer des priorités minimales ou maximales à des classes définies de trafic, ce qui permet aux entreprises d'optimiser l'utilisation de la bande passante disponible.

Infrastructure agile et performances avec McAfee Web Gateway

McAfee Web Gateway est un proxy d'entreprise hautes performances disponible dans différents modèles d'appliance évolutifs, tous dotés d'une haute disponibilité intégrée, d'options de virtualisation et d'une option de déploiement hybride avec McAfee Web Gateway Cloud Service. McAfee Web Gateway offre une flexibilité de déploiement et des performances optimales, de même que l'évolutivité nécessaire pour gérer des centaines de milliers d'utilisateurs dans un environnement unique.

McAfee Web Gateway vous permet également de combiner les options de déploiement. Par exemple, vous pouvez diriger tout le trafic web vers les appliances sur site pour les utilisateurs connectés au réseau, tandis que vous dirigez tous les utilisateurs hors réseau vers le service de cloud, réduisant ainsi considérablement les coûts liés au réacheminement du trafic vers les lignes MPLS (MultiProtocol Label Switching) et le réseau privé virtuel (VPN). La synchronisation automatisée des stratégies ainsi que les rapports communs pour les déploiements hybrides sur site et dans le cloud aident à rationaliser la gestion, à assurer une mise en œuvre cohérente des stratégies et à simplifier la génération de rapports, le suivi de fichiers et l'analyse.

McAfee Web Gateway propose diverses options de mise en œuvre — modes proxy explicite, routeur transparent, pont transparent — pour assurer la prise en charge de votre architecture réseau.

Grâce à la prise en charge de nombreuses normes d'intégration, McAfee Web Gateway est conçu pour s'adapter parfaitement à votre environnement particulier. Quel que soit le type de protocole, par exemple WCCP (Web Cache Communication Protocol), ICAP/ICAPS (Internet Content Adaptation Protocol), WebSocket ou encore SOCKS (Socket Secure), McAfee Web Gateway communique de manière efficace avec d'autres équipements réseau et appliances de sécurité.

En outre, McAfee Web Gateway prend en charge le format IPv6 afin d'aider les grandes entreprises et les organismes publics à se conformer aux réglementations. McAfee Web Gateway comble le fossé entre les réseaux IPv4 internes et IPv6 externes, et applique au trafic toutes les fonctions de protection et d'infrastructure disponibles.

Une plate-forme unifiée tournée vers l'avenir

McAfee Web Gateway combine et intègre de nombreux mécanismes de protection qui, en temps normal, ont besoin de plusieurs produits autonomes pour fonctionner. Filtrage d'URL, antivirus, antimalware efficace contre les menaces « jour zéro », analyse SSL, prévention des fuites de données ou encore gestion centralisée : toutes ces fonctions sont réunies au sein d'une architecture d'appliance logicielle unifiée. La gestion des déploiements est harmonisée pour tous les types de solutions, si bien qu'une stratégie peut être étendue aux appliances installées sur site, aux clusters d'appliances, aux appliances virtuelles et au service de cloud à partir d'une console de gestion unique.

Gestion des risques de sécurité et génération de rapports

Le logiciel McAfee ePolicy Orchestrator® (McAfee ePO™), technologie de gestion de sécurité respectée et appréciée, est pris en charge par McAfee Web Gateway en tant que source unique pour les rapports de sécurité.

Le logiciel McAfee ePO offre des fonctionnalités de génération de rapports de sécurité web détaillés via McAfee Content Security Reporter. Cette extension vous procure les informations et les outils d'investigation numérique nécessaires pour comprendre l'utilisation du Web au sein de votre entreprise, respecter les réglementations, identifier les tendances, isoler les problèmes, documenter toute activité inappropriée sur le Web et adapter vos paramètres de filtrage de manière à appliquer vos stratégies en matière d'utilisation du Web. McAfee Content Security Reporter propose un serveur de génération de rapports externe autonome, conçu pour décharger le serveur McAfee ePO du traitement et du stockage de données (des tâches gourmandes en ressources). Cela permet au serveur de s'adapter pour répondre aux besoins de génération de rapports des entreprises, y compris des plus grandes entreprises internationales.

McAfee Web Gateway s'intègre en outre avec McAfee Cloud Visibility — Community Edition, un service gratuit pour les clients des solutions de prévention des fuites de données, de chiffrement et de protection de l'environnement web de McAfee. Il offre une visibilité sur l'utilisation des applications de cloud et les risques associés. Le personnel utilise des applications de

cloud mais le département informatique n'en est pas nécessairement informé, et ce manque de visibilité crée un risque. Un tableau de bord simple offrant une visibilité sur tous les accès aux applications de cloud, les niveaux de risque et la classification des données élimine ce risque. L'équipe de sécurité peut ainsi se concentrer sur la protection des données qui se déplacent vers le cloud et le contrôle des accès au cloud, ce qui réduit les risques auxquels l'entreprise est exposée.

McAfee Cloud Visibility — Community Edition est également inclus sous forme de service gratuit dans McAfee Cloud Data Protection, l'étape suivante de la protection des données dans le cloud.

Licences

Pour vous assurer le nec plus ultra en matière de flexibilité du déploiement et vous aider à pérenniser vos investissements, McAfee propose toutes les fonctions de McAfee Web Gateway et de McAfee Web Gateway Cloud Service dans une seule suite : **McAfee Web Protection**. Déploiement sur site, dans le cloud ou hybride pour plus de flexibilité et une disponibilité élevée : faites votre choix. La protection antimalware primée et le filtrage web complet de McAfee sont inclus, quelle que soit l'option choisie.

Le matériel McAfee Web Gateway est vendu séparément.

1. Lors de tests réalisés par AV-TEST, McAfee Web Gateway est parvenu à détecter 94,5 % des logiciels malveillants de type « jour zéro », 99,8 % des fichiers PE malveillants de Windows 32 bits et 98,63 % des fichiers non PE. McAfee Web Gateway Security Appliance Test (Test de l'appliance de sécurité McAfee Web Gateway), AV-TEST GmbH

McAfee Together is power.

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