McAfee Web Gateway Cloud Service

Sécurité web via le cloud pour une protection omniprésente

Principaux avantages

- Solution la plus rentable pour déployer la sécurité web : aucun matériel ni logiciel ne doit être installé sur site.
- Protection avancée : une émulation des comportements bloque les logiciels malveillants « jour zéro » en quelques millisecondes au fur et à mesure du traitement du trafic.
- Protection étendue aux utilisateurs hors réseau : disparition du périmètre réseau traditionnel grâce à une sécurité délivrée par le cloud.
- Gestion ultraperformante grâce à la plate-forme McAfee® ePolicy Orchestrator® (McAfee ePO™) Cloud, la console de gestion unifiée pour tous les services de cloud d'Intel Security.
- Architecture éprouvée : McAfee® Web Gateway Cloud Service a été conçu comme une version multiclient de McAfee Web Gateway, l'appliance sur site utilisée en toute confiance par les entreprises du monde entier.

Se défendre contre les menaces sophistiquées propagées par le Web demande certes des technologies évoluées, mais ne doit pas pour autant engendrer un surcroît de dépenses et de complexité. Un service de sécurité web dans le cloud garantit aux équipes de sécurité une protection contre les menaces avancées identique à celle offerte par les appliances sur site, sans le coût associé au matériel et aux ressources nécessaires à leur maintenance. Alors que les accès au Web en dehors du périmètre réseau se multiplient, le cloud devient le point de contact habituel des utilisateurs et des équipements itinérants. Au lieu de concevoir une sécurité pour le trafic à destination d'un seul site, il est plus efficace de la créer à partir du terminal vers l'extérieur. La connexion au cloud de terminaux, voire de sites tout entiers, offre une protection omniprésente au nouveau périmètre qui s'est étendu bien au-delà des limites du réseau.

Protection omniprésente et rentable

La gestion des appliances de sécurité web hébergées sur site coûte cher et demande beaucoup de temps aux équipes de sécurité, déjà le plus souvent en manque de ressources. Le déploiement de la sécurité web sous la forme d'un service de cloud permet de diminuer le coût total de possession. Il n'est plus nécessaire d'acheter, de posséder et d'assurer la maintenance d'appliances matérielles. Toutes les ressources précédemment allouées à ces tâches de maintenance, dont les mises à niveau et l'application de correctifs, par exemple, peuvent être réaffectées à des projets plus stratégiques du département TI ou de sécurité informatique.

Un déploiement hybride qui inclut à la fois des appliances et un service de cloud est également possible. La plupart des organisations optent pour ce modèle afin de conserver la propriété et le contrôle des appliances du réseau et d'étendre la protection fournie par le cloud aux petites succursales et aux utilisateurs itinérants.

Les équipes informatiques qui réacheminent le trafic web des succursales distantes via des circuits MPLS (Multiprotocol Label Switching) pour qu'il soit filtré par une appliance de passerelle web sur le réseau tirent un avantage immédiat d'une sécurité web délivrée dans le cloud. En effet, le réacheminement du trafic coûte cher et accroît la complexité du réseau. En optant pour une solution hybride, les succursales distantes peuvent router directement leur trafic vers le cloud pour le sécuriser, ce qui permet d'éliminer les circuits MPLS et de simplifier l'architecture réseau.

intel Security

Enfin, l'accès des collaborateurs au Web n'est plus limité au périmètre réseau et évite ainsi de laisser les équipements et les utilisateurs hors réseau sans protection ni visibilité. La migration de la sécurité web vers le cloud inverse le périmètre. Le trafic web émanant des utilisateurs et équipements hors réseau peut être directement routé du terminal vers le cloud, ce qui permet de garantir une connexion sécurisée même lorsque l'utilisateur se trouve dans un emplacement hors réseau (aéroport, café, etc.). Le réseau n'est plus concentré sur le trafic au sein d'un bâtiment ou site physique. Il est désormais étendu à l'emplacement d'un terminal, où qu'il soit.

Architecture globale hautes performances

McAfee Web Gateway Cloud Service est conçu pour les environnements d'entreprise, qui bénéficieront souvent d'un niveau de performance plus élevé que celui observé sur site. Dans le cas d'un modèle sur site par exemple, si l'entreprise a besoin d'accroître la capacité, l'équipe informatique doit se procurer et déployer une nouvelle appliance, ce qui peut prendre des jours, voire des semaines. Dans notre cloud, l'accroissement de la capacité prend environ 15 minutes grâce à la conception de cloud élastique intégrée à notre service.

Lorsqu'une appliance sur site tombe en panne et doit être réparée, la connectivité Internet risque d'être interrompue et la sécurité mise en péril si l'appliance a été configurée pour rester ouverte au trafic Web en cas de défaillance. Si une panne se produisait dans l'un de nos centres de données, notre service de cloud réacheminerait automatiquement tout le trafic web vers le centre de données le plus proche et le plus rapide afin d'assurer la continuité.

L'architecture de notre service de cloud est également conçue pour se connecter directement avec la dorsale Internet au niveau des principaux points d'interconnexion Internet du monde. Une telle conception élimine les sauts de routage des fournisseurs d'accès Internet intermédiaires qui ne font qu'augmenter la latence de la connexion. Avec moins de sauts jusqu'aux fournisseurs de contenu les plus répandus, par exemple Microsoft Office 365 et Google, les utilisateurs bénéficient souvent d'une connexion plus rapide via notre service de cloud que s'ils devaient se connecter directement à Internet.

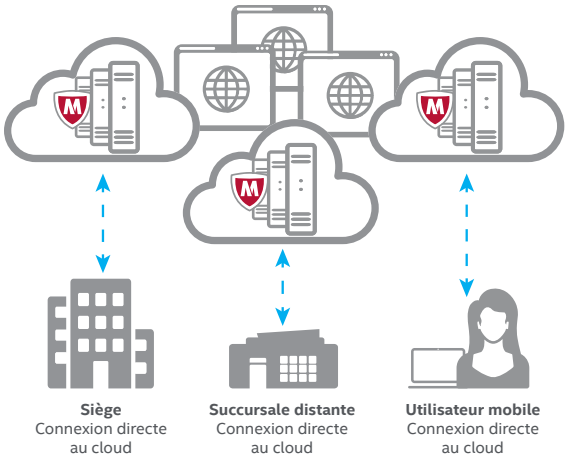

Figure 1. Déploiement de McAfee Web Gateway Cloud Service

McAfee Web Gateway Cloud Service est un service mondial. Pour consulter une carte des points de présence et le statut des centres de données chargés du traitement du trafic web, consultez le site **https://trust.mcafee.com**. Comme le contenu web peut être délivré dans la langue locale, l'utilisateur voit des résultats de recherche Google locaux, indépendamment de son emplacement de connexion.

Protection contre les menaces sophistiquées

Les équipes responsables de la sécurité sont souvent incapables de contrer les logiciels malveillants ultrasophistiqués et les attaques ciblées qui échappent aux systèmes de défense traditionnels. Cela monopolise des ressources considérables et les contraint à agir constamment dans l'urgence pour appliquer des mesures correctives aux terminaux. À la différence des méthodes de prévention des menaces web basées sur le filtrage d'URL et les signatures, McAfee Web Gateway Cloud Service protège les terminaux contre les logiciels malveillants « jour zéro » et sans fichier grâce à une émulation en ligne des fichiers, du code JavaScript et HTML. Il est ainsi possible de bloquer les logiciels malveillants « jour zéro » avant même qu'ils n'atteignent un utilisateur et d'améliorer les taux de blocage d'environ 20 % par rapport aux solutions basées sur le filtrage d'URL et les signatures. Les centres SOC peuvent ainsi réduire leurs coûts et bénéficier d'une flexibilité accrue dans l'allocation des ressources grâce à la diminution du nombre global d'incidents liés aux logiciels malveillants.

Où trouver McAfee Web Gateway Cloud Service dans le monde ?
Consultez le site **https://trust.mcafee.com** pour découvrir l'emplacement géographique de nos centres de données, leur état de disponibilité et bien plus encore.

Les menaces web sont souvent véhiculées par du trafic chiffré pour échapper aux dispositifs de défense web. Pratiquement toutes les applications de cloud, notamment les réseaux sociaux et les services de stockage dans le cloud, chiffrent le trafic par défaut. McAfee Web Gateway Cloud Service peut déchiffrer intégralement et inspecter le trafic HTTPS, permettant ainsi de bloquer les logiciels malveillants et de bénéficier d'une visibilité sur les applications de cloud au sein des canaux chiffrés.

Pour la plupart des équipes informatiques, contrôler la prolifération des applications de cloud, surtout celles issues de « l'informatique de l'ombre », pose un défi majeur, de même que le risque posé par les services sélectionnés par les utilisateurs à l'insu de ces équipes. Grâce à une visibilité totale sur l'ensemble du trafic web, y compris le trafic HTTPS, le service propose des rapports prédéfinis qui peuvent afficher les sites web accédés, les applications de cloud utilisées et les données associées afin d'évaluer le risque. Il est très facile d'identifier les applications « clandestines » en comparant les applications utilisées à celles approuvées par le département informatique. Les pirates utilisent de plus en plus les applications de cloud, surtout les services de stockage dans le cloud, comme mécanismes de propagation des logiciels malveillants. L'identification des applications responsables de la distribution du malware permet de prendre des décisions plus avisées en matière de stratégies. Pour contrôler la multitude de services de cloud utilisés, la solution peut implémenter plus de 1 600 contrôles aux applications de cloud afin de limiter le risque, par exemple en bloquant les téléchargements dans le cloud, la messagerie ou certaines applications.

Gestion efficace de la sécurité

L'utilisation de plusieurs consoles pour gérer la sécurité peut être très fastidieuse, surtout si les solutions de sécurité web sur site et dans le cloud sont gérées séparément. Dans un environnement hybride, il n'existe qu'une seule console de gestion pour les déploiements sur site et dans le cloud, un seul jeu de stratégies et une seule interface de génération de rapports.

Lorsqu'il est déployé seul sans logiciel ni matériel sur site, McAfee Web Gateway Cloud Service est géré par McAfee ePO Cloud, la console de gestion unifiée pour tous les services de sécurité Intel Security dans le cloud et pour les terminaux, offrant une gestion de la sécurité d'une efficacité sans précédent.

Le déploiement de la sécurité web sur les terminaux est souvent problématique, surtout au niveau du routage et de l'authentification. McAfee Client Proxy, un client facultatif pour terminaux, automatise le routage et l'authentification vers notre service de cloud et assure ainsi une connexion omniprésente au cloud associée à une mise en œuvre systématique des stratégies. Il fonctionne en toute transparence avec les appliances hébergées sur site au sein d'un déploiement hybride et achemine de façon intelligente le trafic vers l'appliance si le terminal est connecté au réseau ou vers le service de cloud chaque fois qu'il ne l'est pas. D'autres options de routage et d'authentification sont disponibles en fonction des besoins de l'entreprise.

En savoir plus

Pour en savoir plus, consultez notre site à l'adresse **www.mcafee.com/fr/products/web-protection.aspx**.

McAfee. Part of Intel Security.
Tour Pacific
13, Cours Valmy - La Défense 7
92800 Puteaux
France
+33 1 47 62 56 09 (standard)
www.intelsecurity.com

1764_0916 SEPTEMBRE 2016