UN APPRENTISSAGE FACILE

Passerelle web sécurisée dans le cloud pour les nuls

Palo Alto Networks Edition

Le monde a changé. On ne « va » plus au travail, on travaille tout simplement. Bien que le télétravail ou le travail en itinérance ne soit pas nouveau, la pandémie mondiale a eu pour conséquence logique d'accélérer l'adoption du travail à domicile et du « travail de n'importe où » dans les entreprises modernes. Dans le sillage de la pandémie, de nombreuses organisations en ont fait leur « nouvelle norme » et il semble que ces modèles de travail hybrides ne soient pas prêts de disparaître. Il ressort du rapport *The State of Hybrid Workforce Security 2021* de Palo Alto Networks que les trois quarts des employés souhaitent continuer à travailler à domicile au moins une partie de la semaine.

Mais les salariés ne sont pas les seuls à avoir « quitté les locaux ». De nombreuses applications « cœur de métier », traditionnellement hébergées dans des datacenters on-premise, ont été remplacées par des applications SaaS (logiciel en tant que service). L'édition 2022 du *Flexera 2022 State of the Cloud Report* révèle que 49 % de toutes les charges de travail d'entreprise s'exécutent aujourd'hui dans le cloud public. De plus, selon le rapport *30 SaaS Industry Statistics [2023]: Trends + Analysis* publié par Zippia.com, les organisations utilisent déjà en moyenne 110 applications SaaS et 99 % des entreprises utiliseront une ou plusieurs solutions SaaS d'ici la fin 2023.

Du fait de ces tendances lourdes, la plupart des employés et des applications qu'ils utilisent sont désormais extérieurs au périmètre de l'entreprise. Le nouveau périmètre réseau, c'est aujourd'hui la toile. Dans ce guide, vous allez découvrir en quoi une passerelle web sécurisée dans le cloud

(SWG) permet de garantir une sécurité totale à l'aide d'une seule plateforme disponible depuis le cloud, pour protéger tous vos utilisateurs et vos applications, où qu'ils se trouvent.

Protéger le trafic Internet au moyen d'une passerelle web sécurisée dans le cloud

Une SWG est une solution de sécurité réseau on-premise ou dans le cloud qui débarrasse le trafic Internet des logiciels indésirables/malveillants et assure la conformité à la réglementation et à la politique de l'entreprise. Au lieu de se connecter directement à un site web ou à une application, l'utilisateur est dirigé vers la SWG, qui est alors chargée de le connecter au site web/à l'application souhaité et d'exécuter des fonctions comme le filtrage des URL, la visibilité du web, l'inspection des contenus malveillants, les contrôles d'accès au web et d'autres mesures de sécurité.

Lorsqu'elles sont devenues une catégorie à part entière du marché de la sécurité, la plupart des SWG, sinon toutes, consistaient en des solutions de fournisseur de proxy. Toutefois, les SWG se distinguent des proxies : un proxy est une fonction réseau, alors qu'une SWG est une solution de sécurité. Un proxy est un ordinateur ou un logiciel dédié placé entre un client final (tel qu'un ordinateur de bureau ou un appareil mobile) et la destination voulue (telle qu'un site web, un serveur ou une application basée sur le web ou sur le cloud). En tant qu'intermédiaire entre le client et la destination, un proxy peut empêcher la destination d'accéder à l'adresse IP (Internet Protocol) du client, apportant ainsi une couche de confidentialité. Comme le montre la Figure 1, un proxy :

- Reçoit la demande web d'un client
- Met fin à la connexion
- Établit une nouvelle connexion avec la destination voulue
- Envoie les données de la part du client

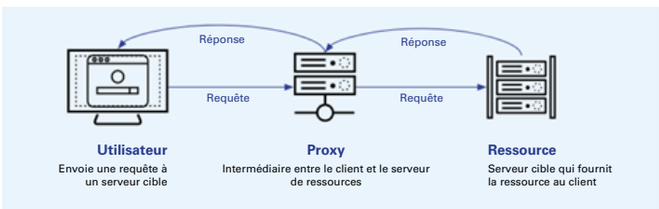

Figure 1 : Un proxy sert d'intermédiaire entre un client final et les ressources d'une destination.

Cependant, les appliances on-premise traditionnelles intégrant des proxies web ont leurs limites, notamment :

- **Une sécurité incomplète :** les appliances on-premise qui intègrent des proxies web et autres produits hérités de plusieurs fournisseurs n'ont jamais été conçus pour le cloud, et ne garantissent pas une sécurité constante et

complète pour l'ensemble des utilisateurs, des emplacements et des appareils. Ces appliances qui ne sont pas en mesure de sécuriser toutes les applications (web et non web) et d'inspecter correctement le trafic inline, et s'intègrent mal aux écosystèmes cloud, accentuent les risques pour les organisations.

- **Une couverture d'applications limitée :** plus de la moitié des menaces qui guettent les télétravailleurs concernent des applications non web que les proxies web ne peuvent détecter. Les équipes de sécurité ne peuvent pas bloquer ce qu'elles ne voient pas, d'où un risque accru de violation de données de par l'absence d'une sécurité couvrant à la fois les applications web et non web.
- **Une piètre expérience utilisateur final :** des goulots d'étranglement nuisant aux performances apparaissent lorsque, pour gérer les accès et la sécurité, les organisations orientent le trafic Internet des télétravailleurs vers les appliances intégrant des proxies web basées sur des datacenters. En outre, les télétravailleurs utilisent souvent un réseau privé virtuel (virtual private network, VPN) au lieu d'une SWG pour accéder aux applications privées, ce qui peut semer la confusion et entraîner des problèmes de connectivité, et donc solliciter davantage les services d'assistance informatique.
- **Des limitations liées aux appliances provenant de plusieurs fournisseurs :** l'utilisation d'appliances provenant de plusieurs fournisseurs morcèle les fonctions de gestion, génère des incohérences dans les règles de sécurité, ralentit les performances et nuit à la visibilité des menaces réseau à tous les niveaux de l'organisation. Les silos d'appliances provenant de plusieurs fournisseurs entraînent des incohérences dans les politiques, augmentent les coûts de maintenance et limitent la visibilité et la collaboration entre les équipes réseau et de sécurité.

RAPPEL

Dans les sièges sociaux, l'accès aux applications se fait via un VPN d'accès à distance. Lorsque les utilisateurs accèdent à des applications cloud, ils sont déconnectés du VPN et exposés aux risques. C'est notamment pour cette raison que les organisations ont recours à des passerelles web sécurisées (SWG) : pour fournir un accès Internet sûr lorsque les utilisateurs sont déconnectés du VPN.

De nombreuses organisations font appel à une SWG dans le cloud afin de sécuriser l'accès à Internet pour les utilisateurs distants ou travaillant dans leurs agences locales ; les serveurs, la virtual desktop infrastructure (VDI) et les appareils de l'Internet des objets dans leurs agences locales ; et même les sièges sociaux/campus ayant besoin d'une bande passante très importante quand il leur faut délester leurs données du site vers le cloud. En outre, une SWG dans le cloud donne une visibilité sur les accès utilisateur, les menaces sur Internet et le trafic web, et permet de contrôler et réguler Internet au moyen du contrôle des accès, des fonctions, des SaaS et de la protection des données, et de fonctionnalités sécurisant la navigation sur Internet. Enfin, une SWG Cloud peut aussi servir à améliorer l'expérience utilisateur final. Au lieu de transmettre l'ensemble du trafic web à un datacenter d'entreprise, ce qui génère de la latence, il est possible d'améliorer considérablement les performances du réseau au moyen d'une connexion directe au cloud.

POINT TECHNIQUE

Une SWG ne peut pas non plus se substituer à un pare-feu. Les pare-feux de première génération se contentaient d'inspecter les adresses IP, les ports ou autres protocoles (de niveau 2 et 3) basés sur le routeur. Les proxies web on-premise fonctionnent au niveau 7, et les pare-feux de nouvelle génération fonctionnent à la fois au niveau de la couche réseau et de la couche applicative (niveaux 3 et 7, respectivement). Une SWG dans le cloud transfère ces fonctionnalités vers le cloud et prend en charge les architectures basées sur un proxy.

Démarrer sa transition vers le SASE avec une passerelle web sécurisée dans le cloud

L'une des difficultés liées au déploiement de la fonctionnalité SWG est qu'elle est généralement configurée comme un environnement autonome sans coordination des flux de travail, des rapports ou des connexions avec les autres infrastructures de sécurité de l'organisation. Avec le temps, cela peut accroître la complexité, car les organisations utilisent souvent plusieurs produits de sécurité spécialisés qui nuisent à l'efficacité et à l'efficience de leurs opérations de sécurité.

Plus récemment, une nouvelle approche de la sécurité des infrastructures a vu le jour. Selon la définition de Gartner, un secure access service edge (SASE) associe des services de mise en réseau et de sécurité en une seule solution unifiée disponible dans le cloud, qui comprend les éléments suivants, résumés dans la Figure 2 :

- **Mise en réseau**
  - Réseau étendu défini par logiciel (SD-WAN)
  - VPN
  - Qualité de service (QoS)
  - Routage
  - Accélération du SaaS
- **Sécurité**
  - SWG dans le cloud
  - Passerelle d'accès cloud sécurisée (CASB)
  - Pare-feu en tant que service (FWaaS)
  - Prévention de la perte de données (DLP)
  - Sécurité du système de noms de domaine (DNS)
  - Prévention des menaces

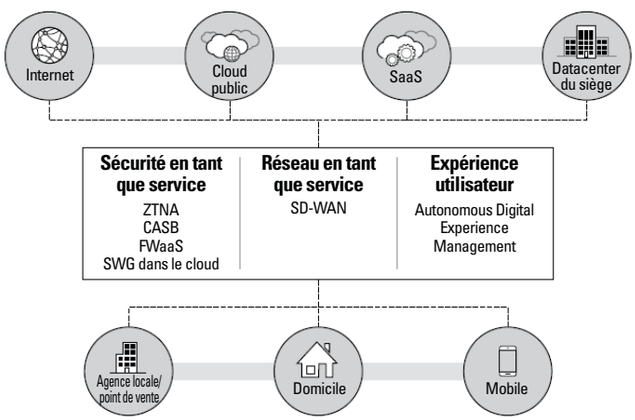

Figure 2 : Le SASE fournit des capacités avancées de réseau et de sécurité sous la forme d'une solution convergée dans le cloud.

Le SASE permet aux entreprises de distribuer depuis le cloud plusieurs services de sécurité : SWG, prévention avancée des menaces, FWaaS, sécurité DNS, CASB, DLP, etc.

Une SWG n'est qu'un des nombreux services de sécurité qu'une solution SASE doit fournir. À mesure qu'une organisation grossit et ajoute toujours plus d'utilisateurs distants, la couverture et la protection se compliquent. Ces obstacles sont amplifiés par la croissance rapide et l'adoption généralisée des applications SaaS, la prolifération des dispositifs personnels gérés et non gérés et l'éparpillement des différentes applications d'entreprise qui s'exécutent dans le datacenter de l'organisation et dans le cloud public. Une solution SASE fait passer la SWG dans le cloud, et assure la protection dans le cloud à l'aide d'une plateforme unifiée qui donne une visibilité et un contrôle complets sur tout le réseau.

RAPPEL

Toute solution SASE doit intégrer une SWG, pour permettre aux organisations de contrôler l'accès au web et d'appliquer les politiques de sécurité qui protègent les utilisateurs contre les sites web malveillants, les logiciels malveillants, les attaques d'hameçonnage, les attaques sur les plateformes SaaS, les attaques de l'homme du milieu, etc.

Le SASE offre de nombreux avantages pour une entreprise, notamment :

- **Sécuriser le personnel distant :** protégez vos utilisateurs, vos applications et vos données au moyen d'une inspection de sécurité inline pour l'ensemble du trafic web, sur le web et hors du web, reposant sur l'intelligence artificielle (IA)/l'apprentissage automatique (AA).
- **Optimiser la gestion du réseau et les opérations réseau :** centralisez la gestion et l'application des politiques de sécurité, et unifiez dans une seule plateforme plusieurs produits spécialisés et fournisseurs.
- **Améliorer l'expérience utilisateur :** offrez un accès utilisateur cohérent et améliorez l'expérience utilisateur grâce à une visibilité complète et un contrôle précis de la connexion de bout en bout.

CONSEIL

Consultez les ressources suivantes de Palo Alto Networks pour découvrir comment protéger votre trafic Internet à l'aide d'une SWG dans le cloud :

- **E-book :** *SASE For Dummies, 2nd Special Edition (Le SASE pour les nuls)*
- **Page web :** Passerelle web sécurisée dans le cloud
- **Livre blanc :** *Modernize Your Secure Web Gateway with SASE*

paloalto NETWORKS

9781394227303