Enterprise Strategy Group | Getting to the bigger truth.™

LIVRE BLANC ESG

Modernisez votre passerelle web sécurisée avec le SASE

Par John Grady, Analyste senior, ESG

Janvier 2022

Ce livre blanc ESG a été rédigé pour Palo Alto Networks.
Il est diffusé sous licence d'ESG.

Sommaire

Avant-propos

Aujourd'hui, les entreprises doivent protéger les accès de leurs utilisateurs aux ressources dont ils ont besoin pour accomplir leurs missions, quel que soit leur lieu de connexion. Mais le problème des modèles de sécurité traditionnels, c'est qu'ils dépendent de systèmes sur site synonymes d'inefficacité opérationnelle, d'expérience utilisateur médiocre et de sécurité fragmentée. Les passerelles web sécurisées (SWG) en sont un bon exemple. En effet, bien qu'elles constituent un composant essentiel de toute stratégie de sécurité d'entreprise, elles ne peuvent pas à elles seules répondre aux demandes actuelles.

Les architectures SASE (Secure Access Service Edge) ont pour vocation d'homogénéiser l'application des politiques et d'unifier la gestion de fonctionnalités de sécurité auparavant cloisonnées. Mais elles nécessitent pour cela une refonte profonde de l'infrastructure réseau et de sécurité. De fait, beaucoup d'entreprises choisissent de commencer par le volet sécurité du SASE, en ouvrant d'abord le chantier de la convergence des SWG, des accès réseaux Zero Trust et des outils CASB. Partie intégrante de la plateforme Prisma Access de Palo Alto Networks, Cloud SWG protège tout le trafic applicatif, y compris les applications web, permettant ainsi aux entreprises de migrer de solutions proxy traditionnelles vers une architecture SASE cloud moderne et convergée.

Sécurité des réseaux : des failles de plus en plus béantes

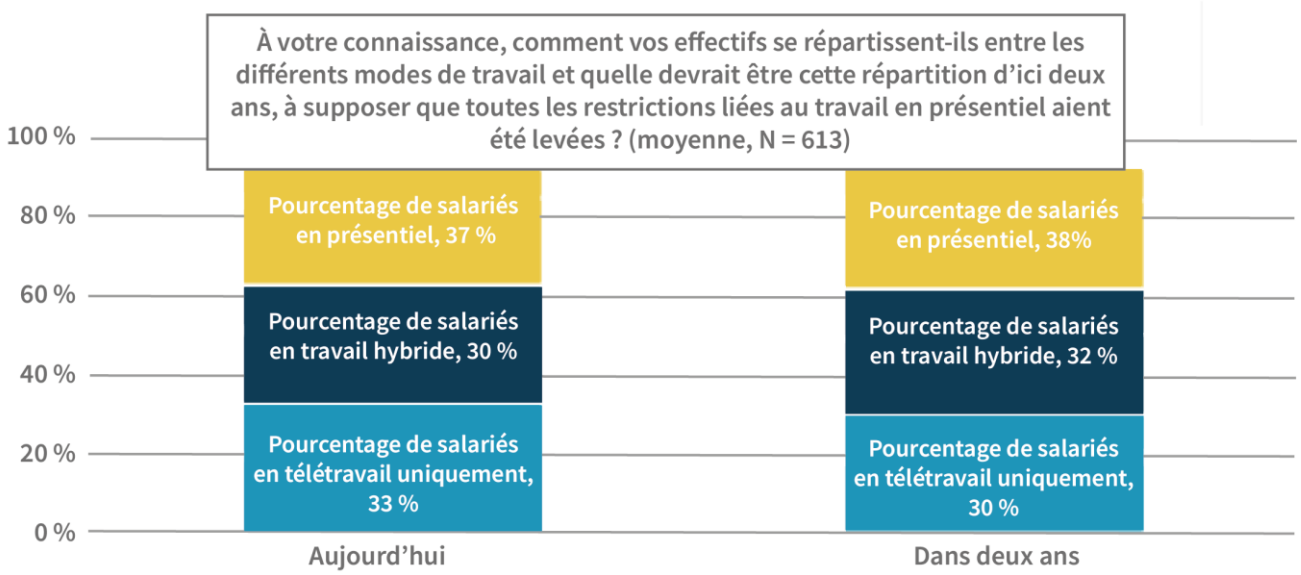
Les entreprises vivent aujourd'hui à l'heure de la transformation numérique, beaucoup d'entre elles réalisant en quelques mois des changements qui leur auraient pris plusieurs années auparavant. C'est ainsi que les initiatives de migration vers le cloud se sont accélérées pour améliorer la résilience et l'agilité opérationnelle des entreprises. Une étude ESG a notamment révélé que 95 % des entreprises utilisent désormais des applications SaaS (Software-as-a-Service) ou des infrastructures IaaS (Infrastruture-as-a-Service).[1]

Dans le même temps, alors que les salariés ont repris le chemin du bureau, le modèle hybride semble bien parti pour s'imposer sur un horizon d'au moins 24 mois, selon les participants à l'étude ESG (voir Figure 1).[2] Face à ces évolutions, de nombreuses entreprises mettent l'accent sur la modernisation de leur infrastructure réseau, y compris l'adoption de technologies SD-WAN. Seul bémol pour beaucoup d'entre elles, les stratégies de sécurité n'ont pas évolué au rythme de ces changements.

[1] Source : Rapport d'étude ESG, *2022 Technology Spending Intentions Survey*, novembre 2021.

[2] Source : Intégralité des résultats de l'enquête ESG, *2021 SASE Trends: Plans Coalesce But Convergence Will Be Phased*, décembre 2021.

Figure 1. Pourcentage de collaborateurs travaillant en présentiel, en distanciel ou selon un modèle hybride



Source : Enterprise Strategy Group

Les approches traditionnelles de sécurité du web et des accès ne répondent pas aux dynamiques actuelles et engendrent d'autres problématiques

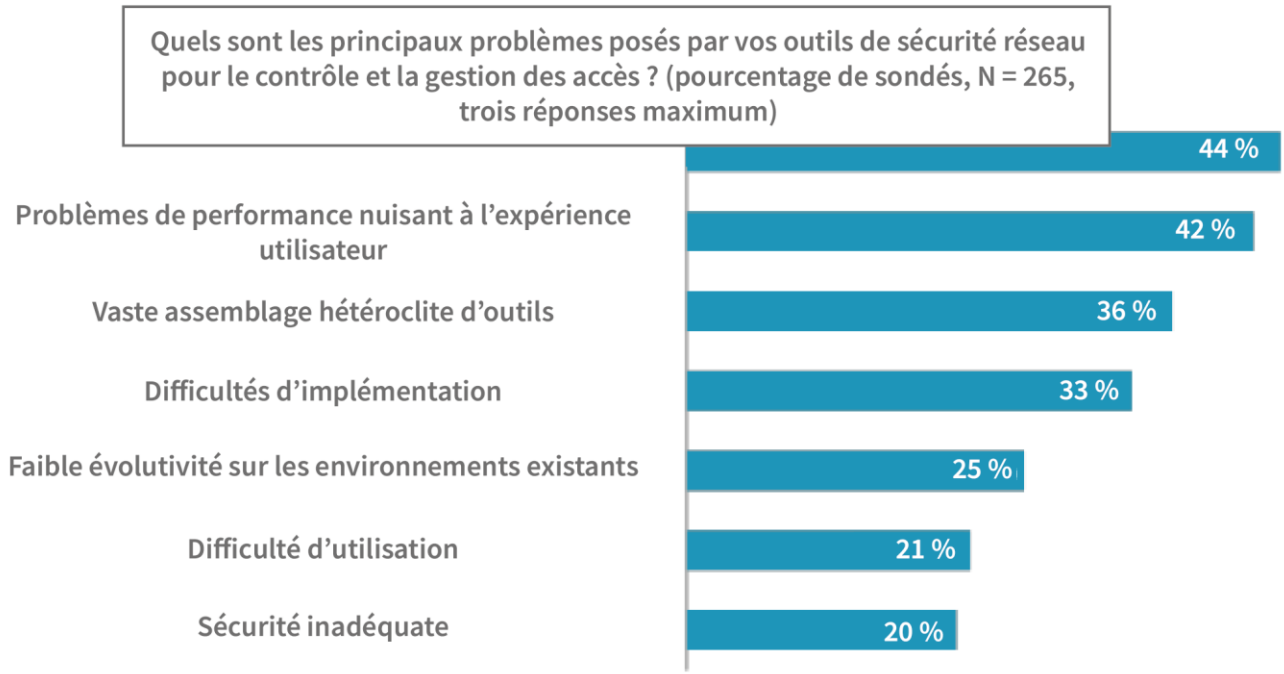
Traditionnellement, la sécurité réseau repose sur un périmètre statique bien défini. Le trafic est acheminé des sites et utilisateurs distants vers des systèmes de sécurité on-prem centralisés où il est soumis à inspection. Avec la migration progressive de leurs utilisateurs et ressources hors des implantations physiques des entreprises, beaucoup d'entre elles ont commencé à s'appuyer sur des solutions cloud pour gérer certains cas d'usage et se protéger de vecteurs de menace spécifiques. Seulement voilà, l'inefficacité manifeste de ces modèles et l'impact croissant des silos d'outils spécialisés ont engendré plusieurs problématiques (voir Figure 2).[3] Plus précisément :

- Inefficacité opérationnelle. La pénurie de compétences en cybersécurité est un phénomène bien connu. En sous-effectifs, les équipes réseau et de sécurité sont par conséquent de plus en plus surchargées. Malgré cela, il leur est demandé de déployer et de gérer en permanence une myriade d'outils spécialisés via des consoles distinctes, avec différents degrés de recoupement dans les politiques de sécurité. Tout ceci se révèle non seulement inefficace, mais peut également engendrer des erreurs humaines et augmenter le risque pour l'entreprise.
- Expérience utilisateur médiocre. Le modèle « hub-and-spoke » consiste à rediriger le trafic vers un data center centralisé où il est soumis à une analyse séquentielle sur plusieurs outils de sécurité. Or, ce modèle peut introduire une latence impactante pour les performances applicatives côté utilisateurs. Quant aux modèles VPN traditionnels qui exigent de se connecter à des passerelles spécifiques pour accéder à certaines ressources, leur manque d'ergonomie peut pousser certains utilisateurs à désactiver ou à contourner les outils de sécurité dès qu'ils en ont la possibilité.
- Sécurité hétérogène. Entre applications IaaS développées en interne et logiciels SaaS inconnus, les nouvelles applications émergent à un rythme stupéfiant dans les environnements d'entreprise. Or, il n'existe souvent aucun référentiel central

[3] Source : Rapport d'étude ESG, *The State of Network Security: A Market Poised for Transition*, mars 2020.

offrant une visibilité claire sur ce qui s'exécute sur le réseau. Par conséquent, les administrateurs peinent à identifier les applications avec précision, à appliquer correctement les politiques et à traiter les alertes entrantes par ordre de priorité.

Figure 2. Problématiques majeures des outils de sécurité réseau



Source : Enterprise Strategy Group

Les passerelles web sécurisées (SWG), ou proxys web, illustrent parfaitement ces tendances. À l'origine, les entreprises ont adopté les proxys web matériels pour protéger les utilisateurs accédant à des ressources Internet. Et bien que les SWG en mode cloud aient fait leur apparition pour réduire le besoin de backhaul vers le data center, la plupart des entreprises continuent également d'utiliser des SWG on-prem. Pour preuve, 96 % des participants à l'étude ESG déclarent utiliser des passerelles web sécurisées matérielles ou des proxys web, tandis que 93 % affirment que leur entreprise utilise une SWG en mode cloud.[4] Ce chevauchement illustre l'approche fragmentée que de nombreuses entreprises ont adoptée pour déplacer les contrôles de sécurité vers le cloud.

La nature changeante du trafic d'entreprise est un autre point essentiel à prendre en compte en matière de SWG. Désormais, plutôt que de passer par le web, les utilisateurs accèdent la plupart du temps à des applications hébergées dans le cloud. Or, même si les proxys web fournissent un contrôle rudimentaire des applications HTTP, leur manque de visibilité complète sur les ports et les protocoles les rend aveugles aux applications non-web. C'est ainsi que les CASB (Cloud Access Security Brokers) et les outils ZTNA (Zero Trust Network Access) ont vu le jour pour faciliter les accès sécurisés aux applications SaaS publiques, sur IaaS ou en data center privé. Ceci dit, le chevauchement entre ces outils conduit souvent à une gestion dupliquée des politiques et des configurations, ce qui engendre les problématiques évoquées précédemment. Résultat : beaucoup d'entreprises se disent ouvertes à une nouvelle approche des passerelles web sécurisées, puisque seuls 8 % des participants à l'étude ESG se déclarent très satisfaits de leur solution actuelle et n'envisagent pas d'en changer dans un futur proche[5].

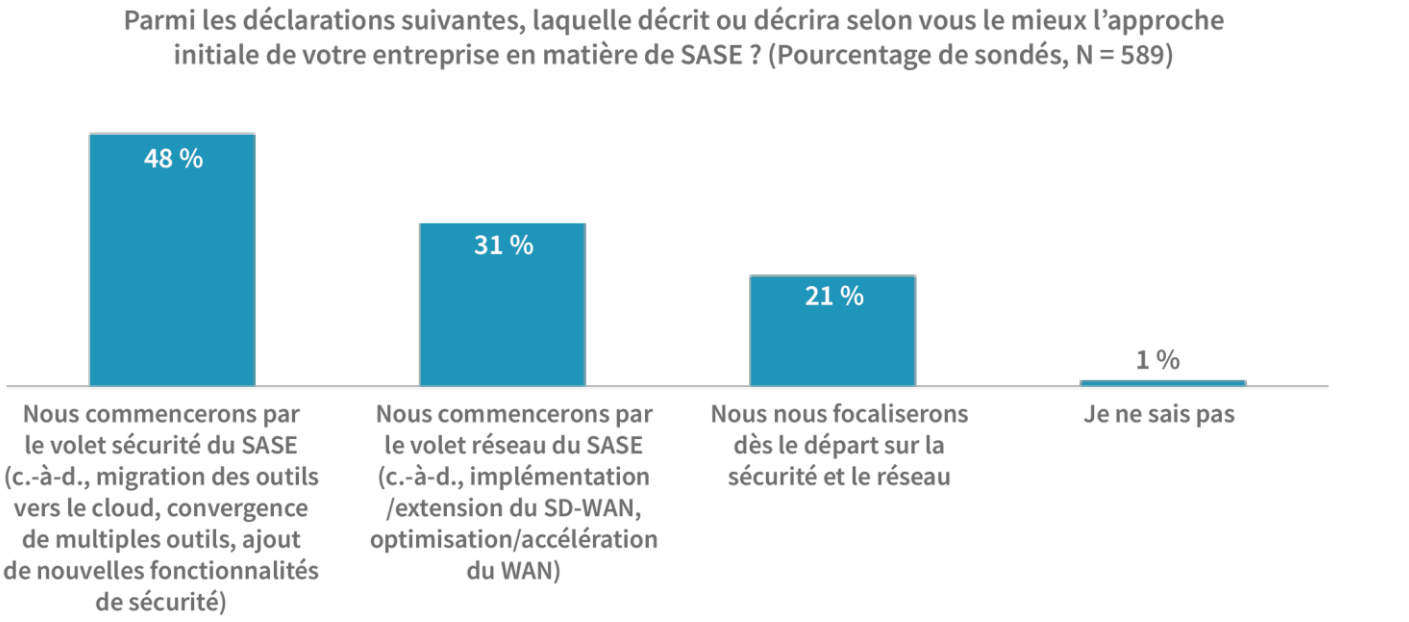
[4] Source : Résultats de l'enquête ESG, *Network Security Trends*, mars 2020.

[5] Source : Résultats de l'enquête ESG, *Transitioning Network Security Controls to the Cloud*, juillet 2020.

Le SASE, levier de modernisation des passerelles web sécurisées

Le SASE (Secure Access Service Edge) suscite un vif intérêt de la part des entreprises qui le voient comme un moyen de résoudre bon nombre des problématiques évoquées précédemment. Le principe : faire converger des outils réseau et des contrôles de sécurité auparavant cloisonnés au sein d'une architecture cloud complète, garante d'une application homogène des politiques pour les utilisateurs à la périphérie (edge) et d'une gestion unifiée pour les administrateurs. Bien que le concept SASE représente une évolution essentielle et pertinente pour les entreprises de tous types et de toutes tailles, la réalité est que l'ampleur d'un tel chantier nécessite de procéder en plusieurs étapes. Selon l'étude ESG, la plupart des entreprises s'accordent sur ce point, avec près de la moitié des sondés (48 %) affirmant que leur structure envisage de commencer par les aspects sécurité du SASE (voir Figure 3).[6]

Figure 3. Approches initiales du SASE



Source : Enterprise Strategy Group

Converger les accès sécurisés au web, aux applications SaaS publiques et aux applications on-prem privées est un point de départ logique pour le SASE

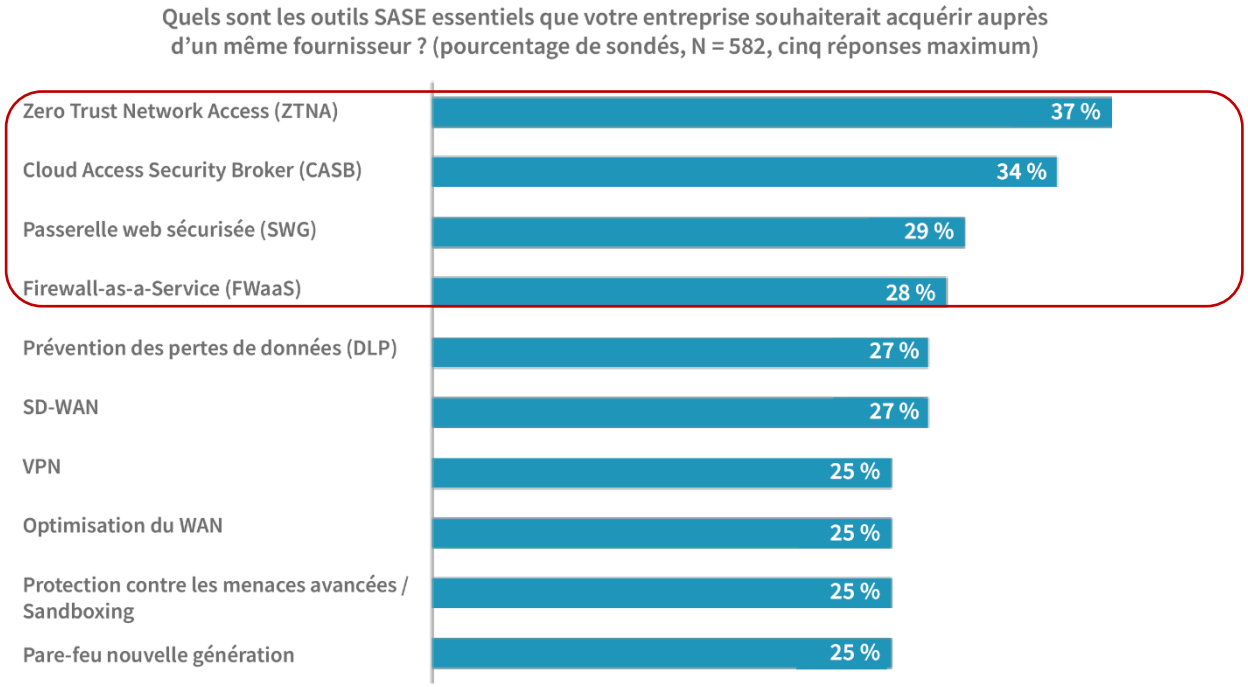
Pour les utilisateurs, le processus d'accès à un site web, une application SaaS ou une application privée consiste souvent à passer par un navigateur. Cette expérience doit rester la même, sans que l'utilisateur ait à se demander à quoi il accède ni d'où il y accède.

[6] Source : Intégralité des résultats de l'enquête ESG, *2021 SASE Trends: Plans Coalesce But Convergence Will Be Phased*, décembre 2021.

Développées au fil des années, les architectures de sécurité sont difficiles à moderniser entièrement du jour au lendemain. Identifier la sécurité comme une priorité est un bon début, mais il est indispensable de resserrer encore davantage la focale, car même sur le volet sécurité du SASE, de nombreuses options sont à prendre en compte. Une priorité commune à quasiment toutes les entreprises devrait consister à augmenter la cohérence avec laquelle les utilisateurs sont protégés, quel que soit l'endroit où ils se trouvent ou ce à quoi ils accèdent. Il n'est donc pas surprenant que 69 % des participants à l'étude ESG considèrent l'adoption d'une SWG comme le point de départ, ou comme un second choix, pour leur implémentation SASE.[7]

Pour les utilisateurs, le processus d'accès à un site web, une application SaaS ou une application privée consiste souvent à passer par un navigateur. Cette expérience doit rester la même, sans que l'utilisateur ait à se demander à quoi il accède ni d'où il y accède. La nécessité de se connecter à des passerelles VPN spécifiques pour accéder à certaines ressources est un processus assez contraignant pour les salariés, sans compter qu'il est difficile à mettre en œuvre sur des appareils non gérés et que le contournement du VPN par certains utilisateurs augmente le risque de sécurité. D'où la volonté de convergence de la SWG, du CASB et du ZTNA dans de nombreuses entreprises. Les participants à l'étude ESG considèrent d'ailleurs ces outils comme les plus importants à acheter auprès d'un même fournisseur dans le cadre d'une implémentation SASE (voir Figure 4).[8]

Figure 4. Top 10 des outils SASE à acheter auprès d'un même fournisseur



Source : Enterprise Strategy Group

Facteurs clés à prendre en compte pour choisir une SWG dans le cadre d'une architecture SASE

Lorsqu'elles étudient différents fournisseurs à même d'accompagner leur projet SASE sur la première étape de convergence entre SWG, CASB et ZTNA, les entreprises doivent leur poser un certain nombre de questions clés :

- Quel est le parcours de migration des utilisateurs de la SWG existante vers la nouvelle solution ? Le déploiement d'agents supplémentaires ou les changements de politiques de routage nécessaires alourdissent la charge de travail et peuvent

[7] Ibid.
[8] Ibid.

ralentir la transition. Face à cette complexité, certaines entreprises préfèrent rester sur leurs anciennes SWG le plus longtemps possible. D'où l'intérêt d'utiliser des agents existants ou des fichiers d'autoconfiguration des proxys (PAC) pour simplifier et accélérer la transition.

- Le fournisseur propose-t-il des fonctionnalités SASE supplémentaires qui permettront de gérer différents cas d'usage au fil du temps ? Souvent, une initiative SASE se concentre initialement sur un cas d'usage particulier. Par exemple, la protection des télétravailleurs. Cependant, la plupart des entreprises chercheront à développer leur solution SASE au fil du temps. Pour ce qui est de la consolidation initiale entre SWG, CASB et ZTNA, les acheteurs doivent vérifier la capacité des fournisseurs à prendre en charge un large éventail de scénarios d'accès sur des appareils gérés, non gérés et mobiles utilisés aussi bien par des salariés que par des collaborateurs externes. De manière plus générale, les solutions SASE couvrant les appareils IoT ou intégrant des fonctionnalités réseau et SD-WAN offriront davantage de flexibilité pour étendre le périmètre du projet SASE à long terme.

- La gestion des politiques et la visibilité sur les différentes fonctionnalités SASE sont-elles unifiées ? Il ne suffit pas de disposer d'un vaste ensemble de fonctionnalités SASE. Une gestion unifiée de l'architecture est essentielle pour éliminer les inefficacités opérationnelles évoquées précédemment. Une interface graphique l'est tout autant pour simplifier la création de politiques transverses aux différents éléments SASE et réduire les erreurs humaines. De plus, une visibilité sur tous les utilisateurs et emplacements, au sein d'un tableau de bord centralisé, aide les équipes de sécurité à identifier les problèmes plus efficacement et à prioriser les actions de réponse.

- Quelles sont l'empreinte réseau et l'infrastructure de connectivité du fournisseur ? Les solutions SASE doivent être aussi fiables qu'évolutives, ce qui nécessite un réseau mondial résilient. La garantie de performances solides et d'une expérience utilisateur positive passe par un réseau distribué à l'échelle mondiale, des points de présence dans toutes les principales zones géographiques et des relations de peering importantes. Certains fournisseurs s'associent à des CSP (Cloud Service Providers) pour fournir une connectivité privée via leurs dorsales privées. Objectif : veiller à ce que le trafic ne transite pas sur l'Internet public afin de réduire l'impact d'une saturation du web sur les performances.

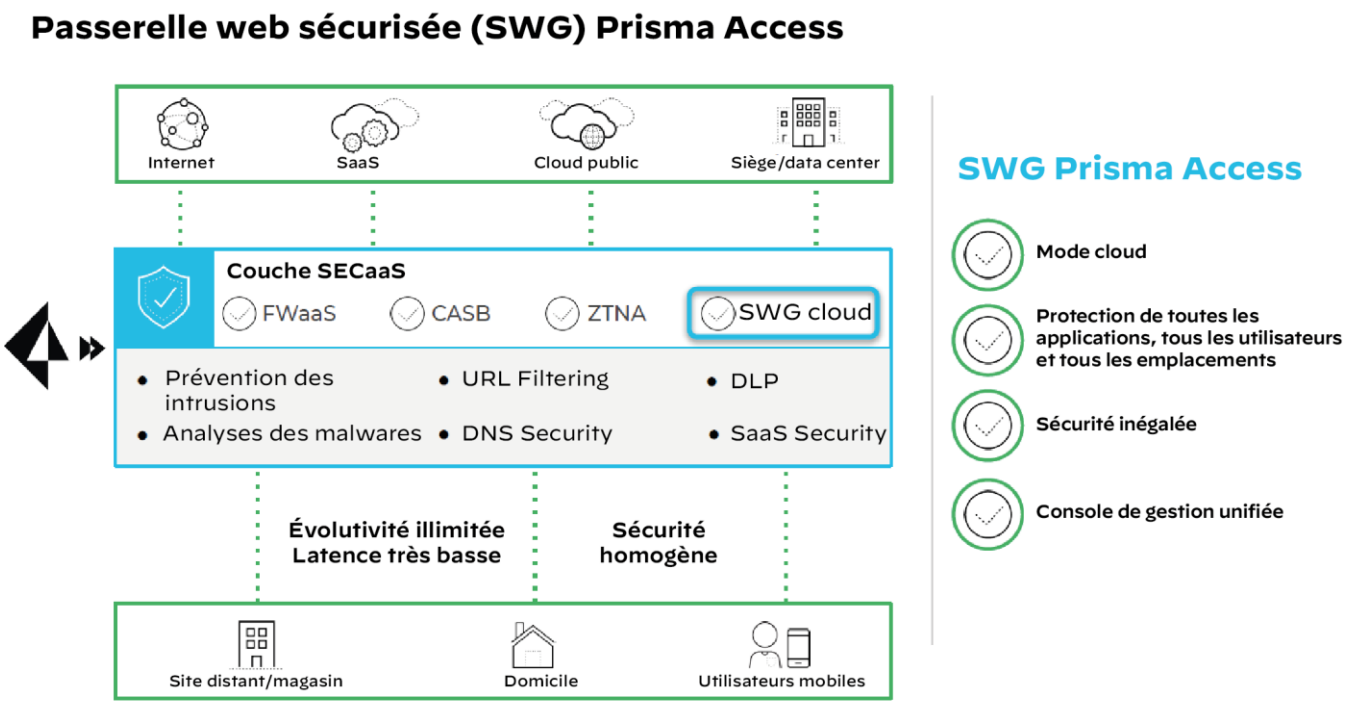
Avec Prisma Access, Palo Alto Networks propose une passerelle web sécurisée flexible

On connaît Palo Alto Networks pour ses pare-feu nouvelle génération. Pourtant, depuis des années, les entreprises font confiance aux outils de visibilité et de contrôle sur la couche applicative (L7) pour assurer leur sécurité web lorsque des architectures proxy n'étaient ni nécessaires ni souhaitables. Alors que les stratégies de cloud hybride et les modèles de télétravail deviennent la norme, les entreprises se tournent de plus en plus vers des solutions cloud pour sécuriser toutes leurs applications sur tous les ports, protocoles et utilisateurs. Prisma Access a certes permis de sécuriser le trafic applicatif des entreprises, y compris le trafic des applications web. Mais à son lancement, la migration depuis des SWG basées sur des proxys imposait d'importantes modifications sur l'architecture réseau. C'est pour fluidifier cette transition que Palo Alto a intégré un proxy explicite à sa solution Prisma Access Cloud SWG. Son rôle : faciliter la migration des solutions proxy vers une plateforme de sécurité complète en mode cloud, sans que cela ne nécessite une quelconque modification de l'architecture réseau.

Palo Alto Networks Prisma Access intègre une SWG cloud (voir Figure 5) et des options de connectivité flexibles pour différents scénarios d'utilisation. Les appareils mobiles gérés peuvent continuer à se connecter à Prisma Access via l'agent GlobalProtect, tout comme les appareils non gérés peuvent passer par l'option VPN sans client de Palo Alto. De même, les sites distants peuvent se connecter à Prisma Access via un VPN IPSec. Enfin, grâce au déploiement du proxy explicite, les clients peuvent migrer plus facilement depuis des proxys web traditionnels sans avoir à modifier l'architecture du réseau. Les fichiers d'autoconfiguration des proxys (PAC) peuvent en effet être paramétrés de façon à diriger le trafic web vers le

proxy cloud explicite de Prisma Access, et ainsi permettre aux entreprises d'entamer rapidement leur transition vers une architecture SASE.

Figure 5 Passerelle web sécurisée Prisma Access



Source : Palo Alto Networks

L'intégration de Cloud SWG à la plateforme Prisma Access offre de multiples avantages aux utilisateurs, dont les principaux sont les suivants :

1. Feuille de route claire vers un SASE moderne et complet. Prisma Access est une plateforme de sécurité cloud-native entièrement intégrée. Autrement dit, elle permet à Cloud SWG de fonctionner en parfaite interopérabilité avec les fonctionnalités FWaaS (Firewall-as-a-Service), CASB et ZTNA de Palo Alto pour aider les clients à entamer leur parcours vers le SASE. Quant au module ADEM (Autonomous Digital Experience Management), il permet de garantir une expérience utilisateur homogène en télétravail et sur les sites distants, tout en facilitant la résolution des problèmes lorsqu'ils surviennent. Par ailleurs, les intégrations natives avec Prisma SD-WAN donnent naissance à une architecture réseau et de sécurité entièrement convergée. Enfin, côté gestion, Prisma Access offre deux options : 1) via une console cloud Prisma Access unifiée pour rationaliser la gestion des configurations et l'onboarding, et 2) via la console Panorama de gestion de la sécurité réseau pour faciliter le déploiement et la gestion de Prisma Access par les clients des pare-feu nouvelle génération.

2. Sécurité multicouche renforcée. Prisma Access fournit une visibilité complète sur tous les ports et protocoles. Alors que les proxys web ne voient que le trafic web, l'inclusion du CASB et du ZTNA offre une visibilité granulaire sur les applications, pendant que le FWaaS protège les utilisateurs contre les menaces non-web. La prévention des menaces sur plusieurs couches comprend la prévention des intrusions, le filtrage des URL et la sécurité DNS. De plus, Palo Alto associe son moteur WildFire d'analyse des malwares à une prévention des menaces sans signature pilotée par ML pour bloquer les menaces zero-day et autres menaces avancées en temps réel. Une fois ces menaces identifiées, la CTI qui en résulte est immédiatement distribuée à tous les clients de Palo Alto (Palo Alto

déclare effectuer plus de 4,3 millions de mises à jour de sécurité par jour). Enfin, les intégrations avec Enterprise DLP offrent une visibilité homogène sur les contenus auxquels les utilisateurs accèdent et qu'ils partagent, ce qui permet aux entreprises de reprendre le contrôle sur leurs données sensibles.

3. Performances des fournisseurs de services cloud. Prisma Access fonctionne sur Google Cloud Platform (GCP) et s'appuie sur la dorsale privée du CSP pour fournir une connectivité privée entre ses sites. La plateforme est développée sur plus de 100 points de présence dans 77 pays, ce qui permet à Palo Alto Networks de garantir une disponibilité de 99,999 % et une latence de traitement inférieure à 10 ms, ainsi qu'une latence soumise à SLA sur les applications SaaS. La plateforme utilise un plan de gestion multi-tenant associé à un plan de données single-tenant, ainsi qu'à une architecture d'analyse single-pass pour garantir les performances et la sécurité.

4. Consolidation pour une sécurité plus efficace et plus homogène. L'approche consolidée de Prisma Access permet aux entreprises de bénéficier d'une sécurité plus homogène, de renforcer l'efficacité opérationnelle et d'améliorer l'expérience utilisateur. Ensemble, la protection homogène contre les menaces web et non-web et la console de gestion centralisée contribuent à réduire le risque d'incidents de sécurité. Quant aux équipes informatiques, elles accélèrent leurs capacités de détection et de réponse tout en réduisant les coûts associés à la prise en main, la gestion et la maintenance de plusieurs produits spécialisés. Enfin, le moteur d'analyse single-pass distribué rapproche la protection des utilisateurs et des ressources. Plus besoin de rediriger le trafic vers le data center pour inspection par un assortiment d'outils multifournisseurs, ce qui a un impact positif sur l'expérience utilisateur.

Conclusion

L'adage qui souligne la futilité de toujours faire la même chose et de s'attendre à un résultat différent revêt une résonance toute particulière dans le domaine de la cybersécurité. Les stratégies de sécurité ont certes évolué au fil des ans, mais les principes fondamentaux sont restés sensiblement les mêmes. Et même avant les mouvements tectoniques que nous avons connus au niveau des applications et des utilisateurs, ces stratégies ne parvenaient pas à protéger les entreprises, à sous-tendre les initiatives métiers et à donner aux utilisateurs les moyens d'accomplir leurs missions. Alors à quoi bon s'attendre à ce que ces stratégies de sécurité fonctionnent dans un contexte d'accélération de la transformation numérique ? Justement, il est inutile de croire aux miracles.

Le SASE est une initiative essentielle qui devrait figurer dans les plans de toutes les entreprises pour évoluer d'une approche périmétrique vers un modèle cloud distribué permettant d'homogénéiser la sécurité, de renforcer l'efficacité opérationnelle et d'améliorer l'expérience utilisateur. Le point de départ logique de cette initiative sera souvent de converger la sécurité des accès au web, aux applications publiques et aux applications privées, ce qui débouchera sur une consolidation des fonctionnalités SWG, CASB et ZTNA. Prisma Access répond non seulement à ce cas d'usage initial en aidant les entreprises à s'affranchir des proxys web traditionnels, mais fournit également la base d'une implémentation SASE complète incluant FWaaS, CASB, ZTNA, ADEM et SD-WAN.

Enterprise Strategy Group est un cabinet de conseil, d'études et de stratégie dont les études, analyses et enquêtes livrent des éclairages concrets à la communauté IT mondiale.

www.esg-global.com contact@esg-global.com +1 508 482 0188