Migration SASE : partez sur de bonnes bases avec Cloud SWG

Sommaire

Transition vers le travail hybride et les applications cloud

Ces dernières années, l'adoption croissante du télétravail a créé de nouveaux défis pour les équipes réseau et de sécurité partout dans le monde. Dans les entreprises, le modèle hybride est devenu la norme. Pour preuve, 76 % des salariés veulent maintenir une alternance présentiel/distanciel dans la durée[1].

Cela dit, les employés ne sont pas les seuls à avoir franchi les murs de l'entreprise. En parallèle, l'essor rapide du SaaS (Software-as-a-Service) a contribué à augmenter considérablement le pourcentage d'applications hébergées dans le cloud. En conséquence, les collaborateurs et les applications qu'ils utilisent résident majoritairement à l'extérieur de l'enceinte traditionnelle des data centers. Autrement dit, le web est devenu le nouveau périmètre réseau.

Des appliances proxy web dépassées

Cette nouvelle donne est d'autant plus problématique que la plupart des entreprises dépendent d'un patchwork d'équipements de sécurité sur site qui, à l'origine, n'ont pas été conçus pour le nouveau monde du cloud et du travail hybride. D'après une enquête du cabinet Enterprise Strategy Group (ESG Global), à la question « Quels sont les principaux problèmes posés par vos outils de sécurité réseau pour le contrôle et la gestion des accès ? », les entreprises interrogées ont cité en tête[2] :

- Gestion hétérogène entre les environnements physiques et virtuels/cloud
- Problèmes de performance nuisant à l'expérience utilisateur
- Vaste assemblage hétéroclite d'outils
- Difficultés d'implémentation

Selon d'autres études d'ESG Global, nombre d'entreprises s'avèrent ouvertes à une nouvelle approche des passerelles web sécurisées (SWG), puisque seules 8 % d'entre elles se déclarent très satisfaites de leur solution actuelle et n'envisagent pas d'en changer dans un futur proche[3].

Petit aperçu des principales lacunes associées aux appliances proxy web sur site :

- **Sécurité incomplète** – N'ayant pas initialement été pensées pour le cloud, les appliances proxy web on-prem et autres solutions multifournisseurs d'ancienne génération sont incapables de fournir une sécurité complète et homogène à l'ensemble des utilisateurs, des sites et des appareils.
- **Couverture limitée des applications** – Plus de la moitié des menaces qui planent sur les télétravailleurs ciblent des applications non-web. Le problème, c'est que celles-ci ne sont pas reconnues par les proxys web. Sachant que les équipes de sécurité ne peuvent bloquer que ce qu'elles voient, toute absence de sécurité transverse aux applications web et non-web augmente le risque de compromission de données.
- **Expérience utilisateur médiocre** – Le trafic Internet des télétravailleurs est systématiquement acheminé vers les appliances proxy web des data centers centraux (backhaul) à des fins d'accès et de sécurité, ce qui crée des goulets d'étranglement (figure 1). Sans compter que l'accès distant aux applications privées par VPN, et non par SWG, peut engendrer de la confusion, des problèmes de connectivité et, au final, une avalanche d'appels au helpdesk IT.
- **Faiblesses de l'approche multifournisseur** – Lenteur, manque de gestion centralisée, incohérence des politiques de sécurité, visibilité lacunaire sur les menaces réseau… le recours aux appareils de multiples fournisseurs génère de nombreux inconvénients (figure 2).

1. *Sécurité du travail hybride : état des lieux 2021, Palo Alto Networks, 15 août 2021,* https:/7/start.paloaltonetworks.fr/state-of-hybrid-workforce-security-2021.
2. « Modernize Your Secure Web Gateway with SASE », Enterprise Strategy Group, janvier 2022, https://www.paloaltonetworks.com/resources/whitepapers/modernize-your-secure-web-gateway-with-sase.
3. Ibid.

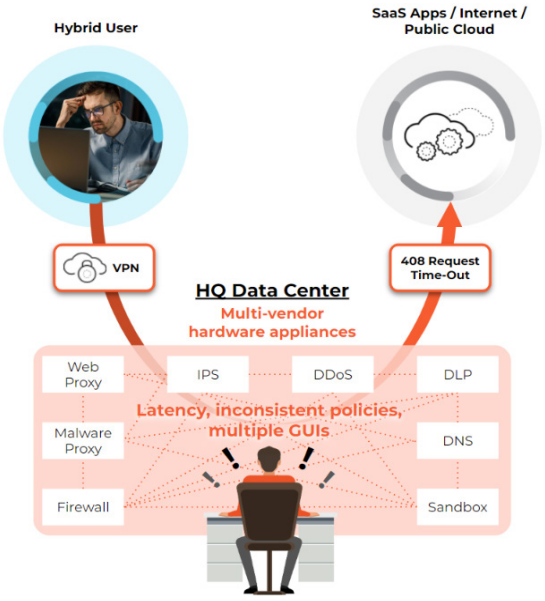


Figure 1. Backhaul du trafic vers le data center pour l'accès et l'inspection

Appareils multifournisseurs : gestion complexe et sécurité hétérogène

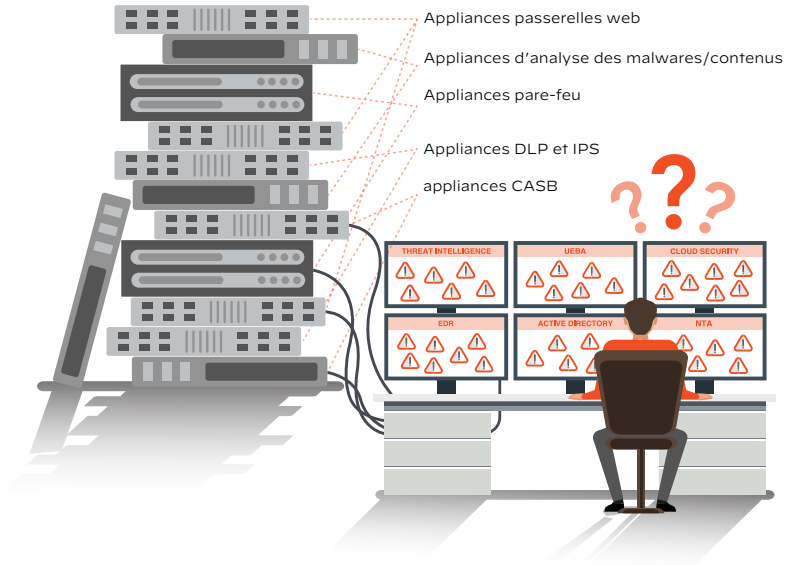


Figure 2. Appareils de sécurité multifournisseurs

Une solution complète en mode cloud

Aujourd'hui, la protection ubiquitaire des utilisateurs, des données et des applications passe par une nouvelle génération de solutions de sécurité web conjuguant la meilleure des défenses avec une visibilité approfondie, une gestion centralisée et des politiques unifiées. La sécurité web faisant désormais partie intégrante de l'architecture SASE (Secure Access Service Edge), elle ne peut plus être gérée isolément. C'est pour cette raison que Cloud SWG de Palo Alto Networks s'intègre à Prisma Access, gage d'une sécurité intégrale en mode cloud.

Grâce à notre prévention leader, aucun trafic web ne vous échappe. Malwares, attaques sans fichier, emails de phishing… toutes les menaces sont neutralisées. Quant à ses capacités CASB (Cloud Access Security Broker) de nouvelle génération et à ses services DLP (Data Loss Prevention) d'entreprise, ils apportent une visibilité totale sur les applications SaaS, garante de la sécurité de vos données sensibles. Enfin, pour assurer facilement une sécurité homogène pour chaque utilisateur et chaque appareil où qu'ils se trouvent, nous complétons le tout par des fonctionnalités intégrées de filtrage d'URL, de sécurité DNS (Domain Name System), de protection anti-malware et de services d'isolation de navigateur à distance (RBI).

Bref, Cloud Secure Web Gateway apporte la promesse d'une sécurité cloud complète dans Prisma Access. Au menu :

- **Protection de tout votre trafic applicatif** – Cloud SWG fournit un accès sécurisé à l'ensemble de vos applications et les protège contre toutes les menaces, web et non-web. Résultat : les entreprises peuvent réduire jusqu'à 45 % le risque de compromission[4].
- **Sécurité intégrale de pointe** – Cloud SWG intègre des fonctionnalités leaders dans une seule et même plateforme cloud, avec à la clé la protection la plus étendue du marché. Sans oublier 4,3 millions de mises à jour de sécurité par jour, soit 24,5 fois plus que notre principal concurrent.
- **Expérience utilisateur irréprochable** – Notre réseau hautement évolutif et performant est adossé à des accords SLA leaders, garants d'une expérience numérique optimale. Pour preuve, nous offrons des débits par tunnel chiffré 10 fois supérieurs à ceux de notre principal concurrent, et des engagements SLA de performance dix fois plus rapides que tout autre service cloud.

Par ailleurs, Palo Alto Networks est le premier fournisseur à intégrer des fonctionnalités de sécurité pilotées par machine learning (ML) à un arsenal de défense déjà impressionnant. Prisma Access mise ainsi sur le ML pour une protection proactive, inline et temps réel contre les menaces zero-day, réalisant par là même plusieurs premières mondiales :

- Neutralisation immédiate de près de 95 % des menaces inconnues basées sur le web et des fichiers
- Désamorçage d'autres menaces inconnues en temps quasi réel à l'aide des mises à jour instantanées des signatures
- Extension de la visibilité et de la sécurité à tous les dispositifs IoT, y compris des appareils inconnus jusqu'alors, sans déploiement de capteurs supplémentaires, grâce à la détection basée sur le ML
- Automatisation des recommandations de politiques pour gagner du temps et réduire le risque d'erreur humaine

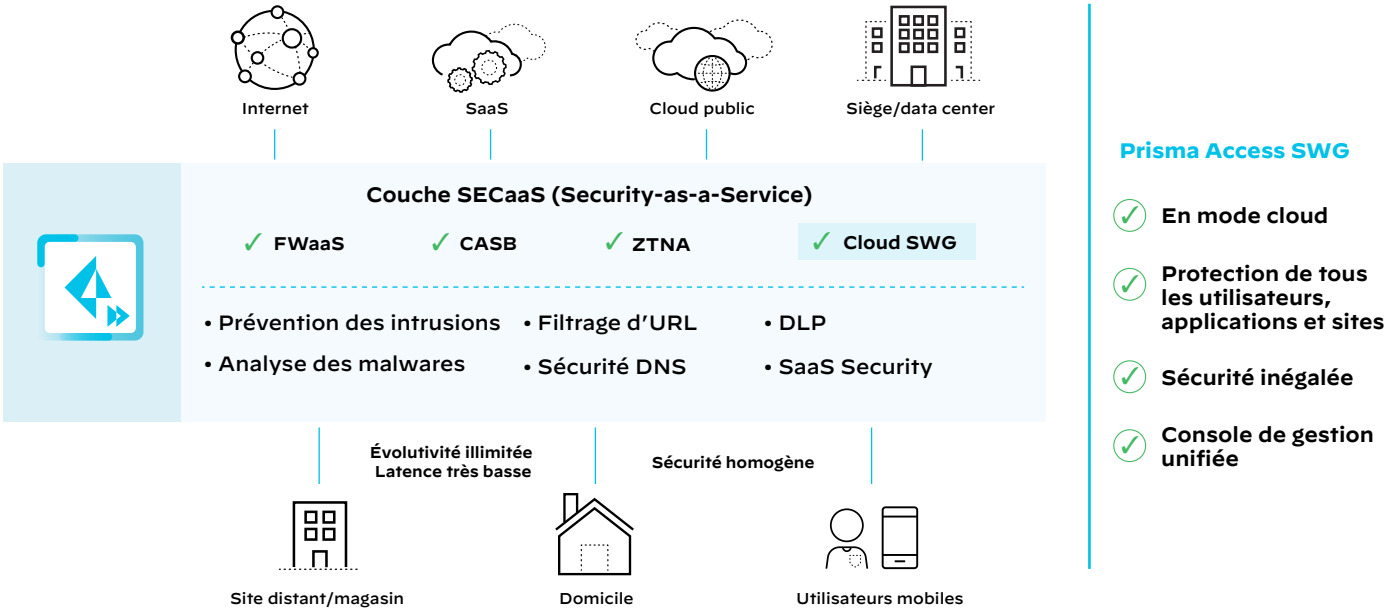


Figure 3. Prisma Access Cloud Secure Web Gateway (SWG) de Palo Alto Networks

4. « Sécuriser les accès distants en toute sérénité avec Palo Alto Networks Prisma Access », étude Total Economic Impact™ Spotlight réalisée par Forrester Consulting pour Palo Alto Networks en janvier 2021 https://start.paloaltonetworks.fr/forrester-tei-prisma-access-spotlight.html

Sécurité cloud : migrez en 3 étapes seulement

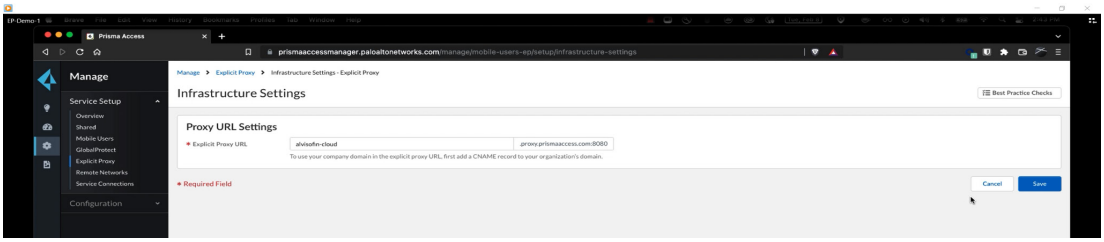
Grâce à Prisma Access et à son proxy explicite cloud, les entreprises peuvent tirer un trait sur leurs serveurs web proxy traditionnels et migrer facilement vers notre plateforme de sécurité en mode cloud. Cette approche permet une mise à jour rapide des fichiers PAC existants. L'objectif ? Rediriger le trafic Internet vers notre proxy explicite cloud pour sécuriser les accès utilisateurs et vous protéger contre les menaces du web, et ce, sans avoir à changer l'architecture réseau.

Trois étapes suffisent pour activer le proxy explicite cloud dans la console de gestion Prisma Access Cloud Management. Il vous suffit de paramétrer l'infrastructure, puis l'authentification des utilisateurs, et enfin les points de présence Prisma Access. Grâce à l'interface administrateur intuitive (cf. captures d'écran ci-dessous), la configuration ne prend que quelques minutes. Pour en savoir plus sur l'activation du proxy explicite cloud, consultez la documentation technique en ligne dans notre rubrique TechDocs.

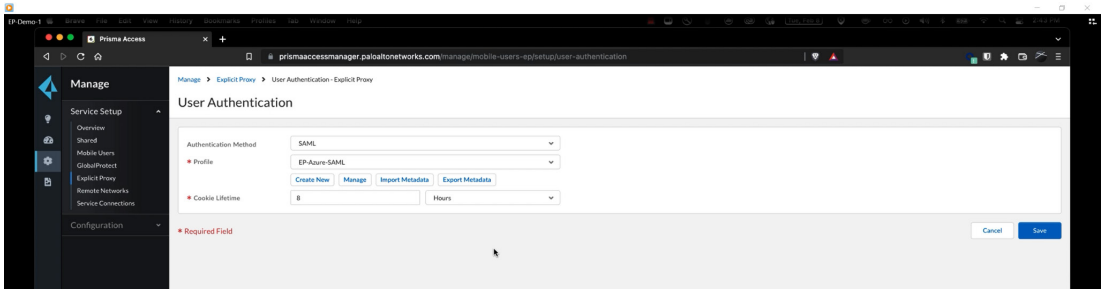
1. Paramètres d'infrastructure

2. Paramètres d'authentification des utilisateurs

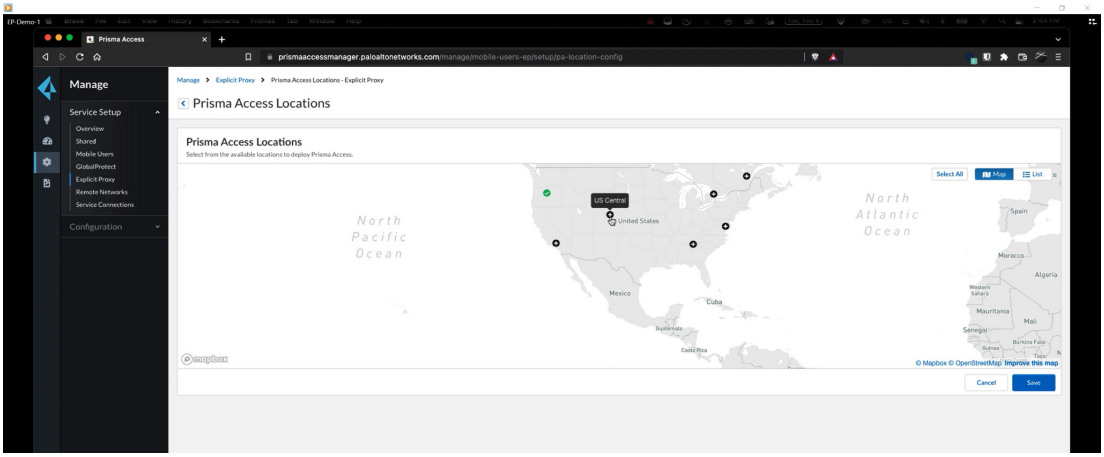
3. Paramètres de points de présence Prisma Access



La console Prisma Access Cloud Management simplifie la configuration de Cloud SWG. Tableau



de bord des bonnes pratiques, évaluations, vérifications des champs et reporting sont autant



de fonctionnalités vouées à renforcer votre posture de sécurité et à augmenter la productivité des utilisateurs. Quant aux vérifications inline, elles facilitent l'évaluation continue de votre environnement sur les points de contrôle suivants :

- Référentiel de politiques de sécurité (il s'agit de vérifier l'organisation et la gestion des politiques de sécurité, y compris les paramètres de configuration s'appliquant à de nombreuses

règles)
- Règles de sécurité
- Profils de sécurité
  - » Anti-spyware
  - » Protection contre les vulnérabilités
  - » WildFire et antivirus
  - » Gestions des accès aux URL
  - » Sécurité DNS
- Authentification
- Déchiffrement
- GlobalProtect

En intégrant ces contrôles, Prisma Access vous aide non seulement à simplifier la gestion et à augmenter la productivité des utilisateurs, mais aussi à agir sans délai pour renforcer votre posture de sécurité grâce à une vérification constante de la configuration et des politiques par rapport aux bonnes pratiques.

Outre le proxy explicite cloud, Cloud Secure Web Gateway propose aux entreprises d'autres options de connectivité pour protéger facilement l'ensemble de leurs utilisateurs et applications, où qu'ils se trouvent. Exemples :

- Appareils mobiles gérés – sécurisation de tous les ports et protocoles via l'agent GlobalProtect pour protéger le trafic web et non-web
- Appareils non gérés – possibilité d'utiliser notre accès sans agent pour bénéficier d'une protection intégrale
- Sites distants – connexion fluide des utilisateurs via IPsec

Pour votre transition vers une sécurité SASE complète, choisissez la voie de la simplicité

Force est de constater que le travail hybride et les architectures « direct-to-app » ont rendu obsolètes les architectures de sécurité traditionnelles, tout en élargissant considérablement notre surface d'attaque. Dans le sillage de cette transformation sont nées des offres de sécurité cloud qui n'offrent cependant qu'une protection incomplète et hétérogène, sans parler de la médiocrité des expériences utilisateurs.

C'est là que Palo Alto Networks entre en scène avec Prisma Access, un produit de sécurité ZTNA 2.0 simple et unifié qui protège vos collaborateurs hybrides tout en leur offrant une expérience d'exception. Résolument cloud-native, le ZTNA 2.0 de Prisma Access sécurise l'ensemble du trafic applicatif et protège les accès et les données pour réduire considérablement le risque de compromission. Grâce à son référentiel de politiques commun et à sa gestion centralisée, la solution assure la protection des collaborateurs hybrides sans jamais compromettre la performance. Côté évolutivité et disponibilité, elle s'appuie sur les plus grands CSP et les meilleurs réseaux fibres pour proposer des opérations de sécurité, des performances applicatives et des expériences utilisateurs d'exception, garanties par des engagements SLA leaders.

Autre avantage, Prisma Access trace un chemin clair pour les entreprises cherchant à implémenter une solution SASE à la fois moderne et complète. Selon l'étude ESG, *69 % des personnes interrogées envisagent une passerelle web sécurisée (SWG) comme point de départ, ou comme second choix, pour leur implémentation SASE*[5]. C'est pour répondre à ces besoins et accompagner nos clients immédiatement vers un modèle SASE que notre solution Cloud SWG s'intègre en toute transparence à notre CASB nouvelle génération, à notre pare-feu sous forme de service (FWaaS) et à nos fonctionnalités ZTNA 2.0. Le livre blanc d'ESG vous livre d'autres clés pour moderniser votre passerelle web sécurisée avec le SASE (en anglais).

Vous souhaitez protéger dès maintenant l'ensemble de vos utilisateurs et de vos applications ? Découvrez les atouts de Prisma Access et de sa passerelle web sécurisée dans le cloud.

5. « Modernize Your Secure Web Gateway with SASE », Enterprise Strategy Group, janvier 2022, https://www.paloaltonetworks.com/resources/whitepapers/modernize-your-secure-web-gateway-with-sase.

paloalto NETWORKS

Oval Tower, De Entrée 99 – 197
1101HE Amsterdam
Pays-Bas
+31 20 888 1883
www.paloaltonetworks.fr