Article

Évaluation du SASE : cinq cas d'utilisation pour protéger, sécuriser et moderniser

À mesure que les applications, les utilisateurs et les données s'émancipent du périmètre réseau traditionnel, de nombreuses organisations sont amenées à réévaluer leurs stratégies en matière de connectivité et de sécurité. L'adoption du cloud, l'utilisation du SaaS et la généralisation du travail hybride ont profondément transformé les schémas de trafic et les conditions d'accès. Ces mutations mettent en lumière les limites des architectures conçues pour des environnements fixes, reposant sur des infrastructures centralisées et des outils fragmentés.

Dans ce contexte, le SASE s'impose progressivement comme un axe de réflexion majeur. Au lieu de considérer le réseau et la sécurité comme deux domaines distincts, le SASE les rassemble au sein d'une approche unifiée, basée sur le cloud et conçue pour répondre aux exigences modernes en matière d'accès et de sécurité.

L'adoption du SASE ne relève pas d'une décision binaire. De nombreuses organisations l'inscrivent dans une démarche progressive, en déployant ses fonctionnalités étape par étape, selon leurs priorités, leur infrastructure existante et leur stratégie en terme d'exposition aux risques. Les cas d'utilisation présentés ci-après illustrent les étapes clés de ce cheminement. Ils montrent comment les organisations évaluent concrètement les solutions SASE, en répondant à des enjeux immédiats tout en évoluant vers un modèle unifié pour le réseau et la sécurité.

1. Moderniser la connectivité des filiales pour un monde axé sur le cloud

Les réseaux des filiales ont été conçus à une époque où les applications résidaient majoritairement dans des datacenters et où le trafic était relativement prévisible. Aujourd'hui, les applications cloud et SaaS dominent largement les modèles de trafic, et le passage systématique des données par des infrastructures centralisées engendre souvent davantage de latence, de complexité et de coûts, en particulier sur les sites des filiales distribuées.

L'adoption d'une solution SD-WAN sécurisée pour moderniser la connectivité des filiales permet de s'adapter efficacement à ces nouveaux usages axés sur le cloud. En rapprochant les fonctionnalités réseau et sécurité au niveau des sites, et en s'appuyant sur des politiques centralisées selon les applications, les organisations peuvent optimiser les performances du trafic cloud et SaaS, tout en assurant la cohérence des contrôles entre les différents sites. Cette approche permet de réduire la dépendance aux architectures héritées et de poser les bases d'un environnement plus flexible, capable d'intégrer progressivement des fonctionnalités SASE plus larges.

Les avantages

- Accès direct et optimisé aux applications cloud et SaaS depuis les filiales
- Simplification des architectures grâce à la convergence des fonctions de routage, de sécurité et de connectivité.
- Amélioration des performances des applications grâce à une gestion du trafic qui tient compte de l'application
- Efficacité opérationnelle accrue pour la gestion d'environnements de filiales distribués

2. Du VPN au ZTNA : sécuriser l'accès pour le travail hybride

Avec la généralisation du travail hybride, les organisations réévaluent la manière dont les utilisateurs distants accèdent aux ressources internes. Les modèles traditionnels reposant sur les VPN ont été conçus pour des environnements où les applications résidaient dans le datacenter et où les utilisateurs se connectaient depuis des emplacements prévisibles. Dans les environnements cloud d'aujourd'hui, ces modèles peuvent créer des goulets d'étranglement et offrir un accès réseau plus étendu que nécessaire.

Le ZTNA introduit un changement de paradigme en plaçant l'identité au cœur des décisions d'accès. Au lieu d'intégrer les utilisateurs au réseau, le ZTNA applique des contrôles d'accès fondés sur l'identité et des politiques au niveau de l'application, en respectant strictement le principe du moindre privilège pour les employés, les sous-traitants et les utilisateurs externes. Cette approche permet de sécuriser l'accès aux applications privées sans exposer le réseau sous-jacent, ni dépendre de tunnels VPN conçus pour des usages désormais dépassés.

Les avantages

- Accès au niveau de l'application au lieu d'établir une connectivité réseau étendue
- Application du principe du moindre privilège, en fonction de l'identité de l'utilisateur et du contexte
- Politiques d'accès cohérentes pour tous les utilisateurs, qu'ils soient à distance, sur site ou externes
- Un point de départ pragmatique pour les organisations qui repensent l'accès sécurisé dans des environnements axés sur le cloud

3. Assurer une sécurité cohérente pour les utilisateurs, le web et les applications SaaS

La protection des accès aux applications privées ne constitue qu'une partie du problème. Avec l'essor des services cloud et des applications SaaS, les contrôles de sécurité doivent être appliqués à toutes les applications. Les utilisateurs accèdent à Internet et aux plateformes SaaS depuis de multiples endroits et appareils, ce qui complique l'application cohérente des politiques de sécurité avec des approches traditionnelles basés sur le périmètre.

Une approche SSE (Security Service Edge) unifiée, qui enrichit le ZTNA avec des fonctionnalités SWG (Secure Web Gateway) et CASB (Cloud Access Security Broker), permet d'étendre les contrôles de sécurité à l'ensemble des usages : accès des utilisateurs, trafic Web et utilisation des applications SaaS. En intégrant ces contrôles au sein d'un cadre unique au lieu de les gérer séparément, les organisations limitent les incohérences au niveau de l'application des politiques, renforcent leur visibilité sur les activités des utilisateurs et appliquent leurs dispositifs de sécurité de manière plus uniforme à mesure que les environnements deviennent plus distribués. Ce modèle permet aux équipes de sécurité de mieux se prémunir contre les menaces issues du Web, de maîtriser les risques liés au SaaS – comme le shadow IT ou les fuites de données – et d'appliquer le principe du moindre privilège sans complexifier inutilement les opérations.

Les avantages

- Application cohérente des politiques de sécurité pour les utilisateurs, le trafic web et les applications SaaS
- Meilleure visibilité sur les usages Web et SaaS
- Navigation Internet plus sûre et meilleure protection contre les menaces en ligne
- Dispositif de sécurité évolutif, adapté aux environnements axés sur le cloud

4. Sécuriser les appareils IoT et les dispositifs non gérés grâce au ZTNA universel

Les appareils IoT et les dispositifs edge restent l'une des failles de sécurité les plus persistantes dans les environnements modernes. Souvent non gérés, difficiles à corriger et incapables d'exécuter des agents, ils compliquent souvent l'application cohérente des principes du zero trust. Leur intégration croissante aux réseaux d'entreprise et aux services cloud élargit la surface d'attaque, exposant les entreprises à des risques que les modèles de sécurité traditionnels, basés sur les utilisateurs et sur le périmètre, ne permettent pas de couvrir efficacement. Le ZTNA universel étend les contrôles d'accès basés sur l'identité à l'ensemble des entités, y compris les devices IoT et les dispositifs non gérés. Grâce à des techniques de profilage, de segmentation et à des politiques globales, il permet de limiter précisément les ressources accessibles à chaque appareil.

L'intégration d'un NAC intégrant une IA renforce cette approche et contribue à protéger les devices IoT et non gérés en améliorant la visibilité sur les appareils, l'analyse de leurs comportements et l'évaluation continue de leur niveau de confiance dans tous les environnements. Une fois authentifié, le trafic IoT peut être segmenté afin d'être isolé des applications stratégiques. Par ailleurs, comme ces appareils IoT génèrent fréquemment du trafic vers Internet et le cloud (notamment pour les mises à jour ou la télémétrie), l'intégration de fonctionnalités SWG avec un SD-WAN sécurisé permet de les protéger sans nécessiter l'installation d'un agent SSE sur chaque appareil. Cette approche étend la sécurité Web à l'ensemble des dispositifs et permet de bloquer l'accès aux sites malveillants, notamment grâce à des techniques de filtrage des URL. En combinant ces différentes fonctionnalités, les organisations peuvent réduire efficacement les risques liés à l'IoT tout en appliquant de manière cohérente les principes du zero trust à l'ensemble des utilisateurs, des appareils et du trafic.

Les avantages

- Meilleure visibilité sur les appareils IoT et les dispositifs non gérés grâce au profilage et à l'analyse comportementale
- Politiques d'accès segmentées limitant la portée des appareils et réduisant les risques de propagation latérale
- Application cohérente du zero trust, y compris pour les appareils ne pouvant pas exécuter d'agents
- Protection du trafic IoT contre les menaces Web, sans complexifier les terminaux

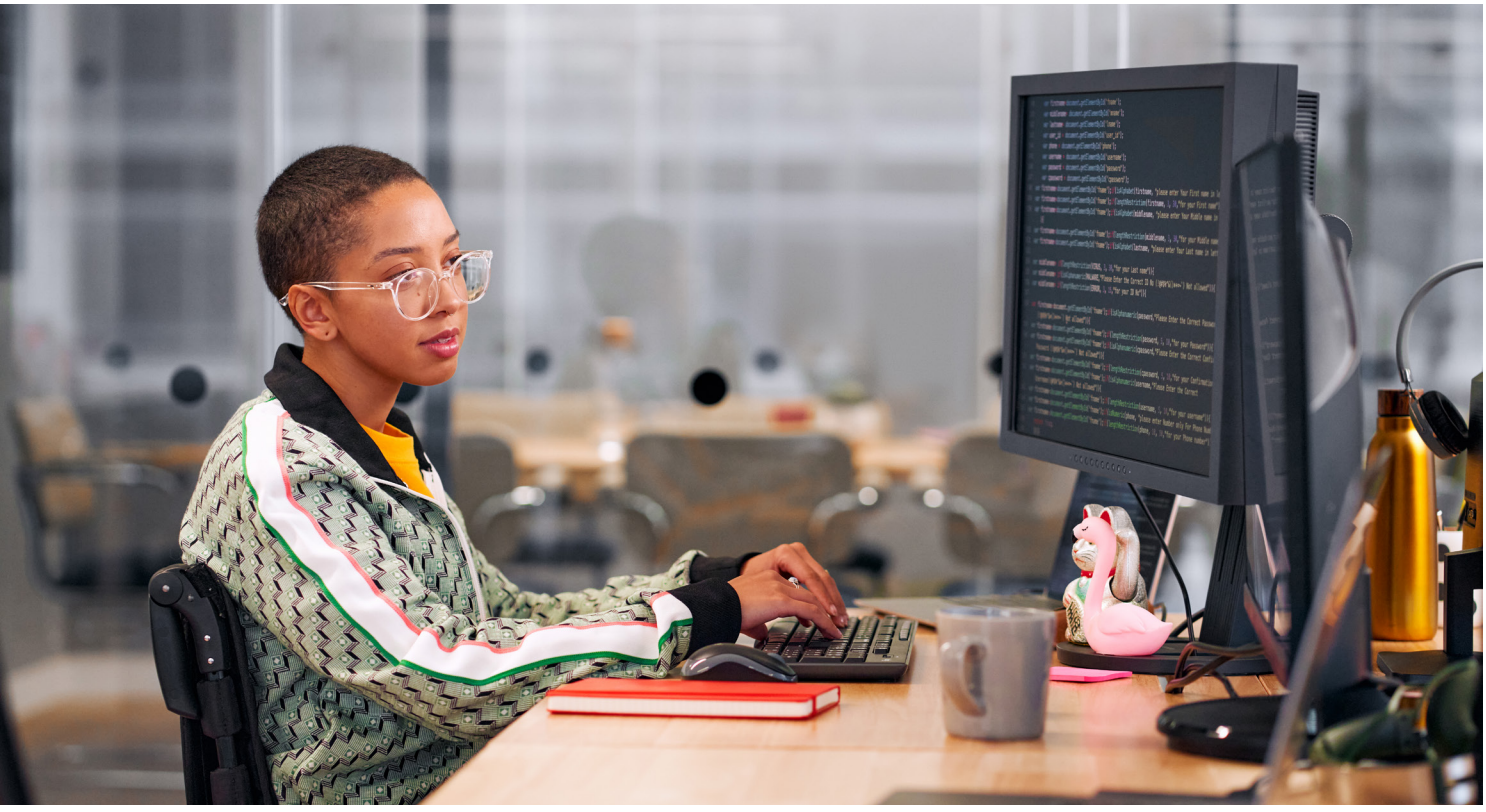
5. Réunir l'accès, la sécurité et la connectivité au sein d'un SASE unifié

Gérer séparément les accès, la sécurité et la connectivité est souvent source de complexité inutile. La multiplication d'outils hétérogènes, de politiques redondantes et d'intégrations manuelles tend à ralentir les déploiements et complique le maintien de la cohérence à mesure que les environnements évoluent. Avec le temps, cette fragmentation peut accroître les frais opérationnels et limiter la capacité des organisations à s'adapter rapidement à de nouvelles exigences.

Une architecture SASE unifiée permet de rassembler ces fonctionnalités dans un modèle unique, délivré depuis le cloud. En harmonisant les stratégies d'accès sécurisé, la protection des usages Web et SaaS, ainsi que la modernisation de la connectivité des sites, les organisations simplifient la gestion et le déploiement des changements, quel que soit le type d'utilisateurs, d'applications ou de sites concernés. Cette approche facilite l'adoption, réduit les efforts d'intégration et permet aux équipes de gagner en efficacité dans des contextes en constante évolution.

Les avantages

- Adoption plus simple des fonctionnalités SASE, sans avoir à assembler plusieurs plateformes
- Réduction des frais opérationnels grâce à une gestion centralisée et des politiques unifiées
- Déploiement plus rapide des changements pour les utilisateurs, les applications et les sites
- Architecture cohérente et évolutive, capable de s'adapter sans complexité inutile



Accompagner votre transition vers un SASE unifié

Les organisations qui s'intéressent au SASE l'abordent généralement comme une transformation progressive, plutôt que comme un projet à déployer en une seule fois. En s'attaquant d'abord aux enjeux liés à l'accès, la sécurité et la modernisation des filiales, puis en intégrant ces fonctionnalités au sein d'une architecture SASE unifiée, les entreprises posent les bases d'un environnement à la fois flexible, cohérent et évolutif, capable de s'adapter à de nouvelles exigences.

HPE accompagne les organisations à chaque étape de leurs parcours. Notre plateforme SASE unifiée AI-native intègre le SD-WAN, le SSE et le NAC au sein d'une architecture unique centrée sur l'identité. En s'appuyant sur des fonctionnalités AIOps, la plateforme offre une observabilité et une authentification renforcées, fournissant aux organisations une visibilité en temps réel et une validation continue du niveau de confiance pour les utilisateurs, les appareils et les applications, y compris dans des environnements tiers.

Les organisations peuvent ainsi avancer en toute confiance, qu'elles amorcent leur transition vers le SASE ou qu'elles cherchent à unifier les fonctionnalités dont elles disposent déjà.

En savoir plus sur

HPE.com/networking

Visiter HPE.com

Live Chat

© Copyright 2026 Hewlett Packard Enterprise Development LP. Les informations figurant dans ce document sont susceptibles d'être modifiées sans préavis. Les seules garanties relatives aux produits et services Hewlett Packard Enterprise sont stipulées dans les déclarations de garantie expresses accompagnant ces produits et services. Aucune partie du présent document ne saurait être interprétée comme offrant une garantie supplémentaire. Hewlett Packard Enterprise décline toute responsabilité en cas d'erreurs ou d'omissions de nature technique ou rédactionnelle dans le présent document.

a00158357FRE

HEWLETT PACKARD ENTERPRISE

hpe.com