HPE aruba networking

Livre blanc commercial

Le guide de l'architecte pour le remplacement du VPN

HPE GreenLake

Une technologie ancienne à l'assaut du nouveau monde

L'environnement de travail a considérablement changé ces dernières années. Dans un paysage en pleine adaptation avec l'invention et la croissance du cloud, la pandémie de COVID-19 a entraîné une explosion du télétravail.

Nous avons repensé la conception des architectures. Nos utilisateurs ne sont plus protégés par un mur périmétrique. Les équipes sont partout. Par ailleurs, les applications dont elles ont besoin au quotidien sont désormais distribuées sur les SaaS, les sites et les IaaS.

Aujourd'hui, les équipes doivent garantir une connexion sécurisée aux applications internes et externes pour des utilisateurs situés n'importe où. Les architectes doivent offrir un accès sécurisé à l'ensemble des applications héritées et envisager une approche future pour l'accès aux applications.

La nouvelle ère du cloud et de la mobilité transforme nos façons de se connecter et la sécurité associée. Malheureusement, les solutions existantes telles que les VPN ne répondent pas efficacement aux besoins actuels. De nombreuses organisations remplacent leurs VPN par une technologie moderne présente sur la plupart des plateformes Security Service Edge (SSE) : l'accès réseau Zero Trust (ZTNA).

Qu'est-ce que le SSE et comment y intégrer le ZTNA ?

Le SSE fait partie du cadre global Secure Access Service Edge (SASE) présenté par Gartner® en 2019. Avec l'essor du télétravail en réponse à la pandémie, Gartner® a présenté le SSE en 2021.

Le cadre SSE est un ensemble de fonctionnalités de sécurité intégrées et centrées sur le cloud pour faciliter l'accès sécurisé aux applications privées, aux applications logicielles as-a-service (SaaS) et à Internet avec les technologies suivantes : accès réseau Zero Trust (ZTNA), Cloud Access Security Broker (CASB) et passerelle Web sécurisée (SWG).

- **ZTNA** : accès Zero Trust aux applications privées.
- **CASB** : accès sécurisé à toutes les applications SaaS.
- **SWG** : accès sécurisé à Internet.

Une plateforme SSE doit fournir une plateforme unifiée unique pour l'accès aux applications et dissocier l'accès aux applications depuis le réseau d'entreprise. Elle doit servir d'overlay sur le réseau existant en permettant au service informatique de moderniser et de simplifier la connectivité tout en renforçant la sécurité, sans avoir à modifier l'architecture réseau en profondeur.

Une plateforme SSE comprend plusieurs technologies clés mises en œuvre de manière indépendante. Mais alors, par où commencer ? Comment adopter le SSE ? La réponse à cette question est la même que pour n'importe quel projet ou initiative de sécurité : les domaines à haut risque. Dans cette nouvelle ère des applications et des utilisateurs distribués, il faut commencer par remplacer la technologie VPN et protéger l'accès à vos applications privées avec le ZTNA.

« D'ici 2025, au moins 70 % des nouveaux déploiements d'accès à distance seront principalement gérés par le ZTNA et non plus par les services VPN. »

— **Gartner® Forecast Analysis :** Information Security and Risk Management, Worldwide, septembre 2022

Le ZTNA, une alternative au VPN

Le ZTNA représente une alternative de choix aux VPN traditionnels pour les équipes qui s'attellent à la difficulté de sécuriser des environnements de télétravail. Le ZTNA permet de contourner une grande partie des contraintes des VPN traditionnels et offre les avantages suivants aux entreprises modernes.

Sécurité

- **Défi du VPN :** les VPN exposent les réseaux à des menaces telles que les programmes malveillants, les ransomwares et les attaques DDoS en exposant les IP du réseau, ce qui permet aux attaquants d'accéder à l'ensemble du réseau.
- **Solution ZTNA :** le ZTNA réduit le risque d'attaques basées sur Internet en masquant les ressources privées d'Internet. Les connexions uniquement sortantes rendent votre réseau et vos applications invisibles et intraçables, tandis que les utilisateurs ne reçoivent jamais d'accès au réseau. En outre, l'accès est accordé sur la base de l'identité de l'utilisateur dynamique, de l'appareil et du contexte de données, ce qui empêche tout mouvement latéral non autorisé.

Évolutivité et flexibilité

- **Défi du VPN :** les VPN sont des appliances physiques qui peuvent poser problème pour faire évoluer l'infrastructure. En cas de croissance du personnel itinérant, de nombreuses organisations doivent investir considérablement dans l'infrastructure VPN pour prendre en charge davantage de connexions et gérer la hausse du trafic.
- **Solution ZTNA :** l'architecture cloud du ZTNA simplifie l'évolutivité et la gestion centralisée de l'accès à distance. Les règles Zero Trust peuvent être adaptées au niveau des utilisateurs et des applications et appliquées globalement en quelques secondes.

Productivité

- **Défi du VPN :** puisque le trafic est acheminé via le réseau d'entreprise, les VPN peuvent limiter la vitesse de connexion et la performance des applications, ce qui entraîne des pertes de productivité et une augmentation des charges de travail informatiques de gestion des accès.
- **Solution ZTNA :** le ZTNA optimise l'expérience utilisateur en rapprochant l'accès de l'utilisateur via des sites cloud edge globaux qui attribuent automatiquement le trafic au chemin d'accès le plus rapide. Le ZTNA supprime les lenteurs associées au VPN, les déconnexions et les problèmes d'identification tout en s'intégrant de manière fluide aux systèmes de SSO et de gestion des identités.

Coût

- **Défi du VPN :** les VPN entraînent des coûts élevés, car ils nécessitent un matériel sur site coûteux et du personnel dédié pour la gestion et la surveillance. Sans oublier la nécessité de mettre en place une stack de sécurité entrante étendue pour limiter le risque d'attaques liées au VPN.
- **Solution ZTNA :** le ZTNA élimine les coûts associés au matériel VPN traditionnel, à la protection DDoS et aux pare-feux tout en simplifiant la surveillance, ce qui permet de libérer des ressources pour d'autres projets stratégiques.

Démarrez votre parcours SSE avec le ZTNA

Le ZTNA s'est imposé bien au-delà de l'accès à distance en devenant un concept fondamental pour l'accès aux applications. Ce n'est pas une simple passerelle. C'est une approche de transformation qui ouvre la voie à une vision plus large et complète. Le ZTNA est un service cloud unique pour tous vos besoins en matière d'accès.

Choisissez par où commencer

Avant toute mise en œuvre d'un ZTNA, il est nécessaire d'identifier les motivations. L'objectif principal est-il d'améliorer la sécurité, de rationaliser l'expérience utilisateur ou d'économiser de l'argent ? La compréhension des motivations sous-jacentes permet de sélectionner l'approche idéale pour votre parcours ZTNA.

« Avec l'évolution de la nature du travail, 60 % des employés travailleront à distance d'ici fin 2024, contre 52 % en 2020. »

— **Gartner® Forecast Analysis :** Information Security and Risk Management, Worldwide, septembre 2022

Si la **sécurité** est votre priorité, identifiez le domaine présentant le plus haut risque et concentrez-vous sur les solutions d'accès sécurisé pour des groupes spécifiques tels que les utilisateurs tiers ou les employés. Si l'objectif est **d'améliorer l'expérience utilisateur**, identifiez les groupes d'utilisateurs ayant des problèmes d'accès (par ex. les dirigeants ou les travailleurs à distance) et améliorez leur accès aux applications privées. Si l'objectif est de **réduire les coûts**, identifiez les technologies héritées les plus coûteuses (par ex. les VPN) et envisagez de les remplacer par le ZTNA.

Cas d'utilisation du ZTNA

Planifier le premier cas d'utilisation peut être une tâche ardue. Nous avons donc identifié trois cas d'utilisation principaux. Les sections suivantes décrivent ces scénarios et le processus d'intégration fluide du ZTNA.

Sécuriser l'accès hybride et à distance pour les employés

À l'ère mobile, les VPN traditionnels ne font pas le poids. Autrefois essentiels pour l'accès à distance des employés, ils posent désormais des risques de sécurité considérables en termes de connectivité. Aujourd'hui, les équipes travaillent depuis la maison, le bureau ou des espaces hybrides. Il est donc essentiel de proposer un accès Zero Trust cohérent et discret.

Le schéma ci-dessous présente la façon dont la technologie ZTNA remplace les cadres VPN obsolètes traditionnellement hébergés dans des datacenters. Le ZTNA joue le rôle d'intermédiaire entre l'utilisateur et l'application, accordant l'accès uniquement aux utilisateurs autorisés et aux applications approuvées, quel que soit leur emplacement, sur site ou dans le cloud public.

Ce processus est possible grâce à un connecteur applicatif léger dans l'environnement de l'application, qui autorise l'accès uniquement en cas de respect des prérequis contextuels. Lorsque les critères sont respectés, une connexion sortante est établie pour s'assurer que les utilisateurs ne sont pas placés directement sur le réseau et qu'ils se voient accorder l'accès aux applications autorisées uniquement.

De plus, la transition entre l'accès distant et sur site n'impacte en rien l'expérience utilisateur, car le ZTNA fonctionne de manière transparente en arrière-plan. Il protège également le réseau en empêchant l'accès d'appareils potentiellement compromis depuis le site de l'entreprise.

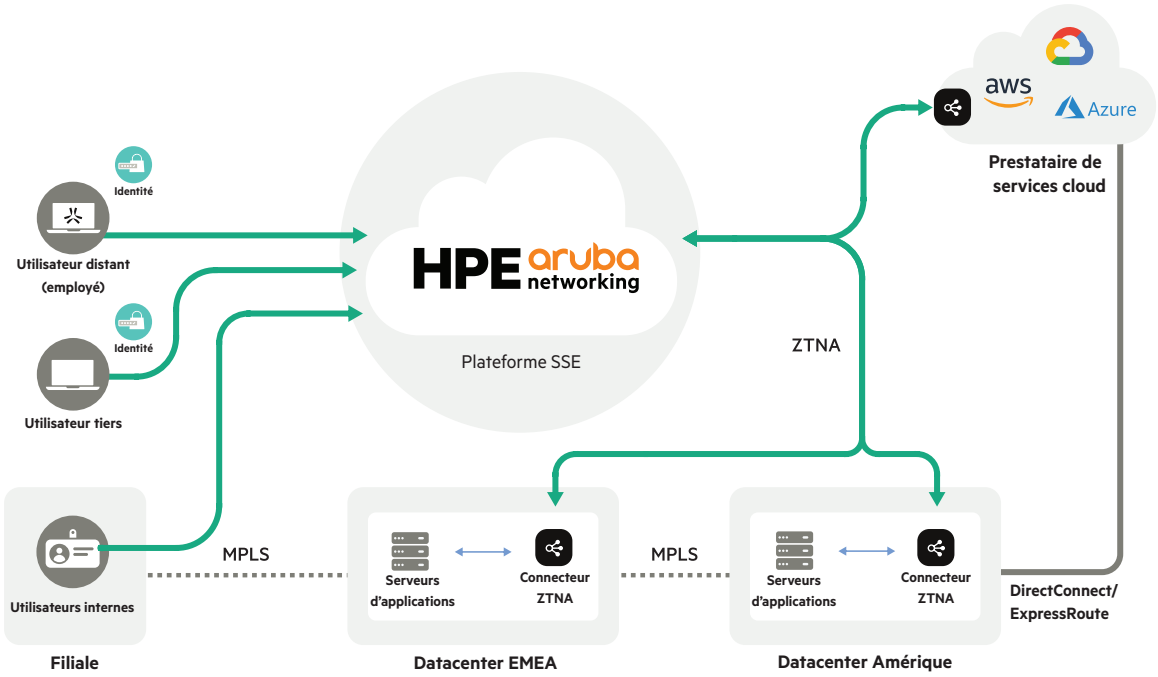

Figure 1. Sécuriser l'accès hybride et à distance

Sécuriser l'accès des tiers et BYOD

Autrefois, l'accès des tiers était principalement basé sur la technologie VPN d'accès à distance. Les utilisateurs devaient installer un client et attendre les mises à jour manuelles des politiques d'ACL et de PF par un administrateur avant d'essayer de se connecter. La connexion garantissait ensuite l'accès à des ressources sensibles, ce qui exposait le réseau à d'importants risques. Le VPN offre un accès réseau aux utilisateurs non fiables, sur des appareils non fiables, depuis des réseaux non fiables. Une fois l'utilisateur tiers présent sur le réseau, ce dernier a souvent accès à l'ensemble des ressources.

Le ZTNA élimine les risques associés à cette approche grâce au système de connexions uniquement sortantes. Le ZTNA masque l'infrastructure réseau, les applications d'entreprise et les portails tiers d'Internet. Indétectables par les sondes entrantes, ils sont ainsi protégés contre la détection des emplacements et les attaques DDoS. Les applications privées et les portails tiers sont dissimulés derrière un connecteur applicatif qui autorise uniquement le trafic via le cloud ZTNA.

Le ZTNA permet également d'appliquer des règles d'accès fondées sur le principe du moindre privilège, même pour les utilisateurs BYOD tiers. L'intégration fluide des principales solutions de SSO offre une expérience d'accès fluide aux applications privées via un simple navigateur Web, sans compromis sur la sécurité.

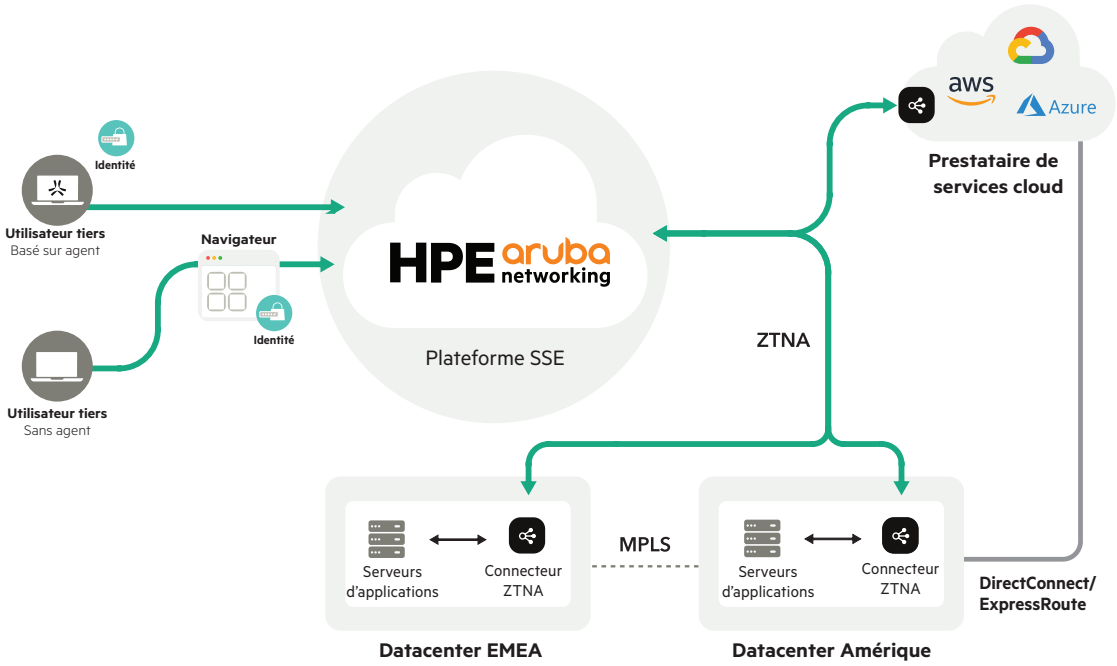

Figure 2. Sécuriser l'accès des tiers et BYOD

Accélérer les fusions et acquisitions

Les défis complexes associés aux fusions et acquisitions (M&A) sont un jeu d'enfant pour le ZTNA qui propose une solution rationalisée avec accès immédiat aux applications stratégiques dès le premier jour. Avec cette approche, vous pouvez dire adieu aux VPN, à l'intégration réseau ou à la modification de l'infrastructure. La stratégie repose sur une liste prédéfinie d'applications essentielles telles que les systèmes RH, l'ERP et d'autres outils Web accessibles via la plateforme SSE.

Le ZTNA intègre une stratégie d'identités solide pour que les utilisateurs puissent s'authentifier et accéder aux applications de manière sécurisée, même avant le regroupement des répertoires, des utilisateurs et des groupes des entités fusionnées. La plateforme SSE est compatible avec divers fournisseurs d'identité, un aspect essentiel pour répondre aux besoins d'accès variés des utilisateurs.

Les fonctionnalités sans agent du ZTNA accélèrent le processus de M&A en fournissant aux utilisateurs un accès Zero Trust sécurisé basé sur un navigateur, ce qui permet d'accélérer considérablement les délais d'intégration.

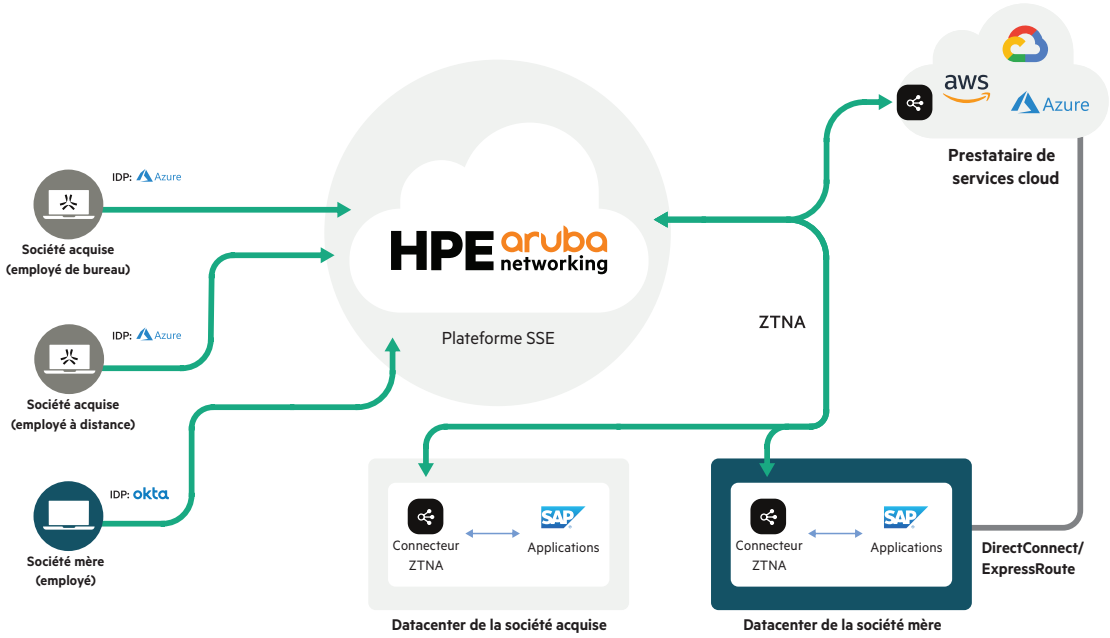

Figure 3. Accélérer les fusions et acquisitions

HPE Aruba Networking ZTNA : la solution ultime pour remplacer le VPN

N'ayez pas peur de vous lancer dans votre parcours ZTNA. Nos experts SSE sont là pour vous accompagner. Voici ce que disent des équipes similaires à la vôtre après avoir choisi HPE Aruba Networking en tant que partenaire pour leur parcours SSE.

- **Remplacement intégral du VPN :** HPE Aruba Networking ZTNA arrive en tête du marché grâce à sa prise en charge étendue des applications privées. La solution gère l'ensemble du trafic TCP/UDP, y compris la VoIP et le peer-to-peer. Elle est compatible avec les applications Web modernes telles que SSH, RDP, Git et les bases de données.
- **Accès sur le principe du moindre privilège sans segmentation :** notre service ZTNA restreint l'accès à des ressources spécifiques sans segmentation réseau complexe, ce qui réduit la surface d'attaque et empêche la traversée non autorisée du réseau.
- **Accès flexible avec ou sans agent :** les utilisateurs accèdent aux applications de manière fluide depuis n'importe quel appareil, avec ou sans client. Notre option sans client facilite les sessions RDP basées sur navigateur et élimine le besoin de VDI.
- **Inspection du trafic granulaire :** obtenez une visibilité détaillée sur le trafic des ressources privées. suivez les actions des utilisateurs, les téléchargements de fichiers et l'utilisation des commandes tout en bloquant les activités néfastes.
- **Contrôles d'accès adaptatifs :** nos contrôles centrés sur des API ajustent les droits d'accès en fonction de l'emplacement, de l'identité et de l'état de l'appareil de l'utilisateur pour améliorer la sécurité des données.
- **Architecture 100 % cloud :** avec HPE Aruba Networking SSE, les connexions sont traitées par le meilleur site edge SSE pour garantir un temps de fonctionnement constant sans gestion d'appliances VPN.

Démarrer avec HPE Aruba Networking ZTNA

Analysez vos cas d'utilisation spécifiques et contactez nos professionnels expérimentés pour identifier les domaines dans lesquels le ZTNA peut aider votre entreprise à obtenir de meilleurs résultats. Consolidez dès aujourd'hui vos applications stratégiques avec nos solutions de sécurité de pointe.

En savoir plus

Contacter un expert SSE

Test Drive gratuit du ZTNA pendant 24 heures

Visitez **ArubaNetworks.com/fr**

Faites le bon achat.
Contactez nos spécialistes.

Nous contacter

Hewlett Packard Enterprise

BWP_Architect-VPN-Replacement_A4_RB_012624 a00137489fre