HPE aruba networking

Remplacer intégralement votre VPN par HPE Aruba Networking ZTNA

L'espace de travail moderne exige une nouvelle approche en matière d'accès distant

Créé en avril 2019 par Gartner®, le terme « Zero Trust Network Access » (ZTNA) représente un ensemble de nouvelles technologies visant à sécuriser l'accès aux applications privées. Également désignées sous le nom de « périmètre software-defined » (SDP), les technologies ZTNA utilisent des politiques d'accès granulaire pour connecter les utilisateurs autorisés à des applications spécifiques sans devoir accéder au réseau de l'entreprise, et remplacer la segmentation réseau par une segmentation au moindre privilège au niveau des applications – le tout sans exposer l'emplacement des applications à l'Internet public.

L'accélération de l'espace de travail moderne passe par l'abandon du VPN

Soucieuses de garantir la continuité de l'activité (un besoin né pendant la pandémie) et de faire face à la concurrence, les organisations, quelles qu'elles soient, sont engagées dans une course contre la montre pour adopter les solutions numériques qui rendront leurs utilisateurs heureux, motivés et productifs. Outre de nouvelles applications de collaboration (comme Zoom ou Microsoft Teams), ces organisations ont mis les bouchées doubles en déployant des services de cloud public évolutifs afin de flexibiliser leurs environnements de travail. Avec une telle modernisation en cours, bon nombre de responsables informatiques étudient de meilleures façons de fournir aux employés et aux tiers un accès distant aux applications privées, tout en mettant au placard leurs solutions VPN.

Avant la pandémie, seulement 30 % des employés travaillaient à la maison. Aujourd'hui, 77 % des entreprises prévoient d'adopter un plan de travail hybride afin de retenir leurs meilleurs collaborateurs (qui préfèrent aujourd'hui travailler chez eux) et d'accéder à des pools de nouveaux talents à la rémunération inférieure. Malheureusement, les VPN ont une fâcheuse tendance à freiner la productivité et à frustrer les employés.

Partenaires, fournisseurs et clients jouent également un rôle clé dans le chiffre d'affaires de l'entreprise. Un utilisateur sur trois devant pouvoir accéder aux ressources est un utilisateur tiers, mais celui-ci se voit souvent refuser l'installation d'un client VPN sur son appareil.

Comme vous pouvez l'imaginer, cet espace de travail moderne a un coût. Ainsi, les dépenses informatiques devraient atteindre 2 000 milliards de dollars en 2022 – dont une grande partie consacrée à la modernisation de l'infrastructure IT et à la prise en charge de ce nouvel environnement de travail. Pourtant, cette somme ne représente qu'une hausse de 4 % des budgets informatiques moyens : aussi, les entreprises n'ont pas d'autre choix que d'investir massivement dans les technologies d'accès à distance existantes.

HPE GreenLake

Pressées de toutes parts pour déployer des environnements de travail à distance, sécuriser l'accès des tiers et moderniser leur infrastructure, les entreprises ne doivent pas pour autant oublier de protéger leurs ressources et leur réputation. À l'heure où chaque utilisateur, appareil et application peuvent se connecter à Internet, la surface d'attaque potentielle croît de manière exponentielle, ce qui fait de l'utilisateur d'un réseau d'entreprise via un VPN la cible numéro 1 en matière de risque.

Pour prendre en charge ce nouvel environnement, 60 % des entreprises remplaceront leur VPN par un ZTNA d'ici 2023.

La différence entre un VPN et HPE Aruba Networking ZTNA

VPN d'accès à distance

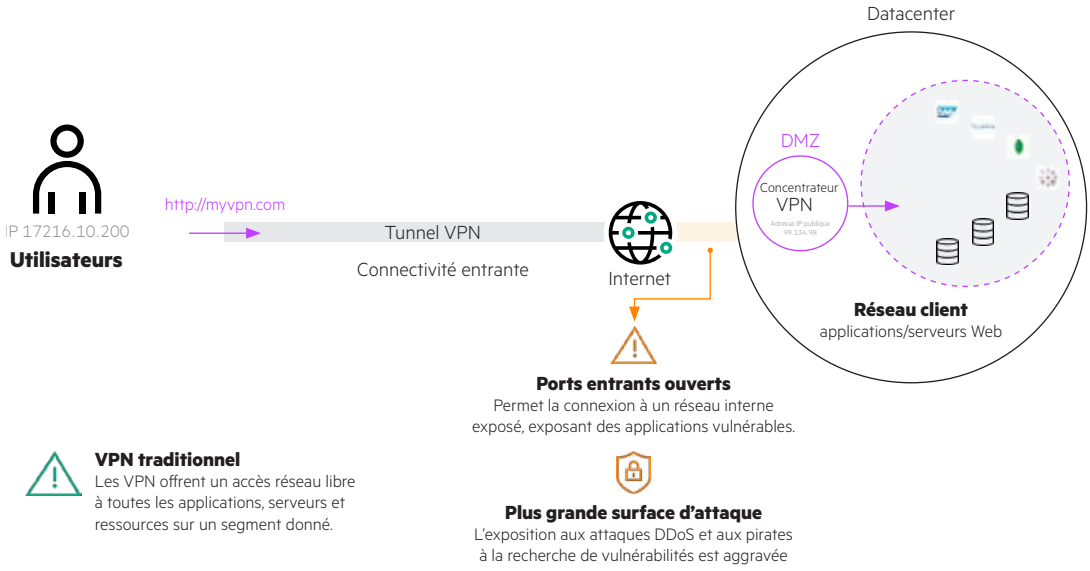

Figure 1. VPN traditionnel

Ces 20 dernières années, le VPN a permis aux employés à distance et aux tiers d'accéder au réseau et aux ressources privées qui s'y exécutaient. Les concentrateurs VPN écoutent les appels entrants provenant des clients VPN et agissent comme des balises pour les clients – en fournissant un point d'entrée dans le réseau de l'entreprise. Pour réduire au maximum le risque de ce type d'architecture faillible, les organisations ont besoin de pare-feux, d'équilibreurs de charges, de politiques de prévention des attaques DDoS et de concentrateurs VPN afin de connecter les utilisateurs à distance aux applications privées, ce qui augmente la complexité, les coûts et le risque. Ces dernières années, les services VPN populaires de plusieurs sociétés connues ont été exploités en raison de leur architecture défaillante.

HPE Aruba Networking ZTNA

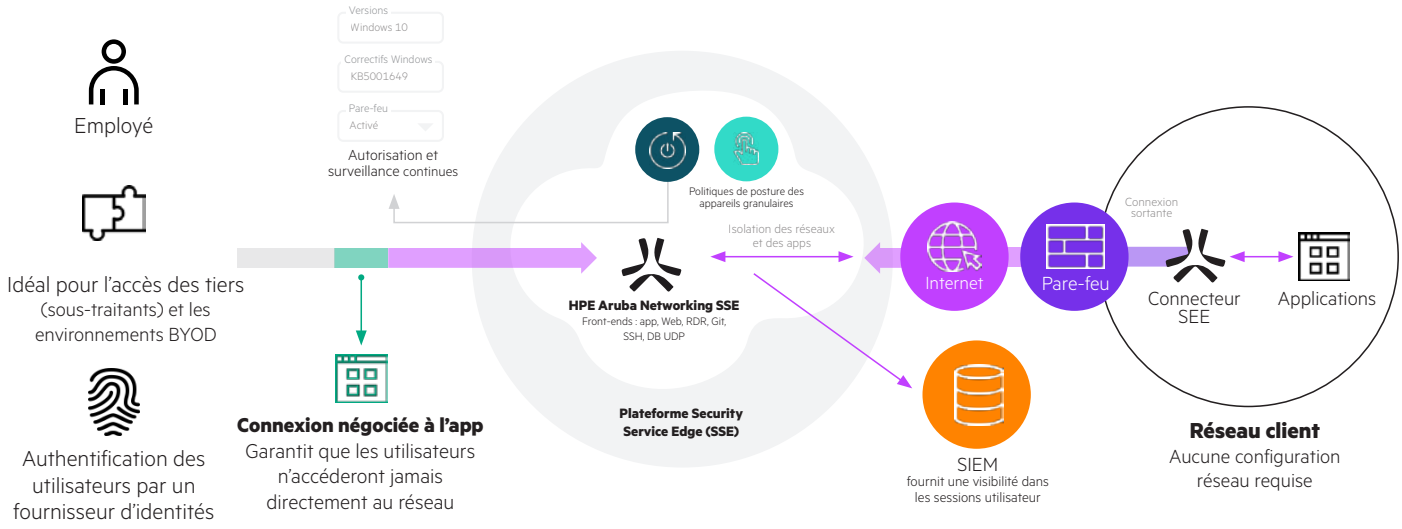

Figure 2. HPE Aruba Networking ZTNA

Avec plus de 500 sites périphériques dans le monde entier, la plateforme HPE Aruba Networking SSE est l'une des solutions zero trust les plus fiables, disponibles et évolutives conçues pour sécuriser la connectivité aux ressources d'entreprise.

Le service HPE Aruba Networking ZTNA offre aux utilisateurs un accès rapide, sécurisé et fiable à des ressources privées. Voici ce qui se passe en temps réel lors d'une connexion à cette fonctionnalité sans client :

1. L'utilisateur demande un accès à une application interne, par exemple hr-app-tenant.axisapps.io
2. Si l'utilisateur n'est pas activement connecté à une application gérée par HPE Aruba Networking, il est redirigé vers le fournisseur d'identités de l'application associé.
3. HPE Aruba Networking ZTNA contrôle la demande d'accès de l'utilisateur par rapport aux politiques définies par le client.
4. L'utilisateur est continuellement autorisé en fonction de son identité, de son groupe et d'autres critères contextuels. REMARQUE : la plateforme HPE Aruba Networking SSE peut activement inspecter le trafic et fermer la session si un événement de sécurité se produit.
5. HPE Aruba Networking ZTNA vérifie s'il existe une connexion existante à l'application à des fins de réutilisation potentielle.
6. Lorsqu'une nouvelle connexion se produit, le connecteur SSE le plus proche identifie l'application autorisée et répond avec une connexion sortante vers le cloud HPE Aruba Networking SSE via un port spécifié.
7. Le cloud HPE Aruba Networking SSE renvoi la nouvelle connexion vers le front-end dédié.
8. Le Web front-end établit une connexion à l'application.
9. L'accès à l'application interne demandée est alors étendu à l'utilisateur via une connectivité basée sur navigateur.

HPE Aruba Networking ZTNA veille à ce que l'accès à l'application soit accordé sans qu'un accès au réseau d'entreprise ne soit demandé. Ce découplage atténue les risques de sécurité du réseau (p. ex. la prolifération de menaces ou de ransomwares) en réduisant au maximum les mouvements latéraux grâce à une segmentation au niveau des applications.

Contrairement à un concentrateur VPN, HPE Aruba Networking ZTNA utilise une architecture lancée par un service pour utiliser ce qu'on appelle des « connexions sortantes uniquement ». Ce type de connexion veille à ce que l'infrastructure réseau et les applications de l'entreprise soient masquées sur l'Internet et ne puissent être ni localisées, ni vérifiées (car elles n'écoutent pas les pings entrants). L'infrastructure réseau et les applications de l'entreprise sont situées derrière le connecteur SSE, qui échange exclusivement avec la plateforme HPE Aruba Networking SSE. Cette plateforme SSE agit comme un intermédiaire entre l'entité (utilisateur ou app) et l'application.

HPE Aruba Networking considère l'Internet comme le nouveau réseau d'entreprise et veille à ce que des micro-tunnels cryptés basés sur Internet remplacent les connexions réseau traditionnels (comme le VPN toujours actif, le MPLS et les connexions site à site dédiées pour le cloud public). Cela réduit les coûts tout en libérant du temps pour les équipes réseau et sécurité afin qu'elles puissent se consacrer à des projets plus stratégiques – plutôt que de devoir gérer des appliances onéreuses, mettre à jour les versions, déployer du matériel et planifier les renouvellements.

Tableau 1.

	VPN	ou	HPE Aruba Networking ZTNA
Expérience utilisateur Les utilisateurs exigent de pouvoir accéder à des applications privées de la même façon qu'ils accèdent à des applications SaaS.	**Expérience utilisateur médiocre** Les VPN contraignent les utilisateurs à déployer un client sur leur appareil et à se reconnecter au réseau de l'entreprise chaque fois qu'ils changent de lieu. Les passerelles VPN n'offrant qu'un nombre limité de points de présence, les flux sous-optimaux ajoutent de la latence, ce qui pénalise la productivité des utilisateurs.	**ou**	**Expérience utilisateur fluide** HPE Aruba Networking SSE propose des méthodes d'accès avec et sans client. Une politique zero trust unifiée suit l'utilisateur et veille à ce qu'il n'accède qu'aux ressources spécifiques dont il a besoin. Grâce à l'expérience utilisateur « toujours en service », le client peut pleinement se concentrer sur son travail, sans se soucier de devoir se reconnecter à un réseau. Les services ZTNA fournis dans le cloud fournissent des points de présence mondiaux qui étendent en toute sécurité la connectivité vers tous les emplacements de l'utilisateur – le tout via l'Internet.
Sécurité L'entreprise doit à tout prix protéger les données face aux cyber-attaques	**Risque accru** Les cyber-criminels ciblent activement les technologies VPN et VDI en lançant des attaques basées sur Internet. Ces méthodes d'accès centrées sur le réseau placent les utilisateurs sur le réseau de l'entreprise et exposent l'infrastructure à l'Internet ouvert. Une simple analyse de port permet à une entité malveillante de cibler toute infrastructure avec une posture obsolète, de voler des informations d'identification et d'accéder au réseau de l'entreprise en se faisant passer pour un utilisateur légitime.	**ou**	**Zéro surface d'attaque** HPE Aruba Networking SSE est conçu pour ne jamais faire confiance à qui ou quoi que ce soit. Le service ZTNA connecte les utilisateurs aux ressources spécifiques seulement après avoir procédé à une inspection et à une validation adéquates. Ces connexions 1:1 sont sortantes uniquement, de la ressource vers l'utilisateur autorisé – sans placer l'utilisateur sur le réseau de l'entreprise. Cette conception d'accès au moindre privilège empêche les utilisateurs et les menaces de se déplacer latéralement au sein de l'environnement. HPE Aruba Networking protège également les ressources en les plaçant derrière le service ZTNA, les rendant ainsi invisibles de l'Internet. Les droits d'accès s'adaptent alors automatiquement en fonction des changements du contexte (p. ex. la relation avec l'entreprise, la posture de l'appareil, l'emplacement, etc.).
Facilité d'utilisation À mesure que l'entreprise se développe et que l'adoption du cloud se poursuit, l'évolutivité devient une priorité.	**Complexité et coûts accrus** L'évolutivité des services VPN impose un surcroît de capacité sur toute la passerelle entrante, avec notamment l'achat, le déploiement et la gestion d'appliances supplémentaires. Des équilibreurs de charges, des pare-feux internes et externes, un service DDoS et d'autres appliances sont bien souvent nécessaires. Cette augmentation du nombre d'appliances pose des problèmes en termes de gestion ; en outre, les dépenses en capital et d'exploitation augmentent considérablement en ce qui concerne la maintenance de la passerelle tout entière.	**ou**	**Simple à gérer** Les services fournis dans le cloud ne nécessitent aucune appliance et sont maintenus par les fournisseurs eux-mêmes. Les services sont conçus à des fins de fiabilité, de disponibilité et d'évolutivité, à mesure que les exigences en termes de trafic s'accroissent. Ces services garantissent l'expérience la plus rapide qui soit, sans pour autant perturber l'activité. Les intégrations d'API avec des services d'écosystème clés tels qu'IDP, la sécurité des terminaux et SIEM, favorisent un déploiement accéléré. Ces services sont facturés selon l'utilisateur sur une base annuelle : ainsi, les coûts liés à la capacité et aux appliances ne sont plus un problème. Les équipes informatiques peuvent réduire les dépenses et les efforts consacrés aux services de connectivité, pour enfin se consacrer aux projets essentiels pour la mise en œuvre de projets d'espace de travail moderne.

Les fonctionnalités uniques de HPE Aruba Networking ZTNA

Figure 3. Facteurs de différenciation uniques de ZTNA

Permet une segmentation granulaire au niveau de l'app, sans segmentation réseau
Réduit la surface d'attaque potentielle en n'autorisant que l'accès à des ressources spécifiques. Cela limite les mouvements latéraux au sein du réseau, élimine les besoins de segmentation réseau complexe et réduit la surface d'attaque potentielle de l'entreprise.

Prend en charge en toute transparence l'accès aux apps depuis n'importe quel appareil, avec ou sans client
Permet aux employés à distance et aux tiers autorisés d'accéder en toute sécurité aux ressources de l'entreprise depuis l'appareil de leur choix, avec une transparence maximale. La méthode sans client prend également en charge les sessions RDP basées sur navigateur, ce qui réduit le besoin de VDI.

Adapte l'accès sur la base de contrôles contextuels optimisés par API
Adaptez automatiquement les droits d'accès en fonction des changements de critères clés, comme l'emplacement de l'utilisateur, l'identité et la posture de l'appareil. Cette évaluation continue et adaptative du risque contribue à renforcer la protection des données métier.

Simplifie la sécurité avec une architecture 100 % fournie dans le cloud dans 500 périphéries dans le monde entier
Les équipes informatiques n'ont plus besoin de gérer les appliances VPN. Avec HPE Aruba Networking SSE, chaque connexion est négociée à l'emplacement edge SSE qui convient le mieux pour fournir la connexion – même en cas de sinistre. Les équipes informatiques ont la certitude de pouvoir réduire au maximum les interruptions et d'optimiser le temps de fonctionnement.

Remplace la technologie VPN héritée
HPE Aruba Networking ZTNA offre la plus large prise en charge des applications privées du marché. Le service ZTNA prend en charge tout le trafic TCP et UDP, y compris les workflows VOIP, peer-to-peer et serveur à client (qui posent des difficultés à la plupart des fournisseurs ZTNA), mais également la totalité des apps Web modernes comme SSH, RDP, Git, DB, etc. Les équipes informatiques peuvent désormais remplacer intégralement et définitivement leur VPN.

Inspecte la totalité du trafic entrant et sortant de ressources privées
Bénéficiez pour la première fois d'une visibilité approfondie sur ce à quoi les employés et les tiers accèdent. Consultez l'activité utilisateur, les téléchargements de fichiers, les tracés des enregistrements et les commandes utilisées lors d'une session, et bloquez toute action malveillante.

Démarrer

Pour en savoir plus sur HPE Aruba Networking ZTNA et découvrir comment cette solution peut remplacer votre VPN, connectez-vous avec l'un de nos experts SSE ! Ou découvrez par vous-même tous les avantages de HPE Aruba Networking en effectuant un test drive gratuit de SSE.

arubanetworks.com/fr

Faites le bon achat.
Contactez nos spécialistes.

Nous contacter

Visitez **ArubaNetworks.com/fr**

© Copyright 2024 Hewlett Packard Enterprise Development LP. Les informations figurant dans le présent document sont sujettes à modification 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 information du présent document ne saurait être considérée comme constituant une garantie supplémentaire. Hewlett Packard Enterprise décline toute responsabilité quant aux éventuelles erreurs ou omissions techniques ou rédactionnelles qui pourraient être constatées dans le présent document.

Toutes les marques de tiers appartiennent à leurs propriétaires respectifs.

SB_VPNWithHPEArubaNetworkingZTNA_DTA_013024 a00136658fre

Hewlett Packard Enterprise