HPE aruba networking

Livre blanc commercial

Du VPN au ZTNA

Avantages du ZTNA et pistes pour se lancer

HPE GreenLake

60 %

des organisations remplaceront leur VPN par un service ZTNA

L'essor du télétravail a généré de nouveaux défis sur le plan de sécurité dans les organisations. Un nombre croissant d'employés travaille à distance et les organisations doivent trouver des moyens pour sécuriser l'accès hybride et distant à leurs réseaux et données. La solution traditionnellement utilisée à cette fin est le réseau privé virtuel (VPN). Cependant, dans un contexte d'évolution des cybermenaces, les VPN ne parviennent plus à assurer une protection efficace. L'accès réseau Zero Trust (ZTNA) est une solution plus efficace pour sécuriser l'accès à distance.

Qu'est-ce que le ZTNA ?

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. Le ZTNA utilise des règles d'accès granulaires pour connecter les utilisateurs autorisés à des applications spécifiques sans accorder d'accès au réseau. L'accès segmenté est fondé sur le principe du moindre privilège et l'emplacement des applications est masqué d'Internet, contrairement aux VPN.

Selon Gartner, 60 % des organisations auront remplacé leur VPN par un service ZTNA en 2023. Le ZTNA est le produit Zero Trust qui a enregistré la plus forte croissance dans le secteur, puisque 47 % des responsables informatiques commencent par cette solution pour adopter une plateforme Security Service Edge (SSE) dans un cadre global Secure Access Service Edge (SASE).

Le ZTNA améliore la sécurité

Si de nombreuses entreprises adoptent le ZTNA, c'est en grande partie pour sa sécurité accrue. Avec un VPN, les utilisateurs sont placés directement sur le réseau d'entreprise. Une fois qu'ils ont accès au réseau, ils peuvent se déplacer latéralement et potentiellement accéder à des données ou ressources sensibles. « Accorder une trop grande confiance aux utilisateurs » est donc présentée comme l'une des plus grandes problématiques des solutions d'accès sécurisé existantes dans le Rapport sur l'adoption du SSE de 2023. Si cet enjeu peut paraître moins important pour les utilisateurs internes, il est néanmoins peu rassurant de savoir qu'un attaquant pourrait exploiter le manque de segmentation.

Par opposition, le ZTNA n'étend jamais l'accès réseau et accorde un accès en fonction du contexte : identité de l'utilisateur, appareil utilisé, application et données auxquelles il tente d'accéder. Si un attaquant tente de pénétrer sur le réseau, il ne pourra donc pas accéder aux données sensibles sans authentification appropriée. De plus, le service ZTNA masquera l'existence même du réseau, le rendant invisible et intraçable.

Les solutions ZTNA sont moins coûteuses à mettre en œuvre et à gérer que les solutions VPN. Le coût d'un VPN va bien au-delà du prix du matériel.

Le ZTNA accroît l'évolutivité et la flexibilité

Les entreprises se tournent également vers le ZTNA pour ses possibilités en matière d'évolutivité et de flexibilité. Tandis que les solutions VPN sont souvent basées sur du matériel et des appliances, les solutions ZTNA sont fournies dans le cloud. Les utilisateurs y accèdent facilement et le service informatique peut assurer leur gestion depuis n'importe quel site. Cette fonctionnalité est particulièrement utile dans les entreprises avec des équipes hybrides/à distance ou qui ont besoin d'accéder à des ressources depuis différents sites. Alors que les VPN ont des limites de capacité statiques basées sur la taille de l'appliance, la nature de l'architecture cloud du ZTNA permet aux entreprises d'ajuster les ressources à la hausse ou à la baisse pour répondre aux besoins de l'activité.

Plus important encore, les services ZTNA fournissent des règles de contrôle d'accès flexibles et extrêmement granulaires qui peuvent être appliquées au niveau de l'utilisateur et de l'application. La segmentation de l'accès proposée par les VPN entraîne une segmentation réseau complexe, alors que l'accès sur le principe du moindre privilège du ZTNA ne nécessite qu'un simple ajustement de règle.

Le ZTNA décuple la productivité

Les solutions ZTNA améliorent l'expérience en matière d'accès. Les VPN freinent la productivité, car les utilisateurs sont confrontés à de faibles vitesses de connexion (en raison de l'acheminement via le VPN), à des déconnexions constantes et à des processus d'identification complexes et répétitifs. Ces problèmes perturbent les utilisateurs et créent de la frustration.

Le ZTNA offre quant à lui une expérience agréable aux utilisateurs finaux. Il leur permet d'accéder facilement aux applications privées en supprimant l'acheminement du trafic et en assurant une connexion constante, même en cas de changements sur le réseau. Le processus d'identification fluide intègre efficacement des solutions de SSO et de gestion des identités.

Le ZTNA est plus rentable

Les solutions ZTNA sont moins coûteuses à mettre en œuvre et à gérer que les solutions VPN. Le coût d'un VPN va bien au-delà du prix du matériel. Outre les concentrateurs, les VPN nécessitent du matériel sur site coûteux, notamment une protection DDoS, des pare-feux internes et externes, des équilibreurs de charge, etc. Et cela ne s'applique qu'à une seule stack de sécurité entrante (les organisations en possèdent généralement 3 à 5). En plus de cela, les équipes de sécurité affectent souvent au moins une personne à la surveillance et à la gestion du VPN. Les ressources ne peuvent donc pas se consacrer à des projets plus urgents et importants. Cette approche centrée sur le périmètre de l'accès sécurisé coûte très cher.

Les solutions ZTNA ne nécessitent aucune installation ou gestion de matériel ou logiciel coûteux sur site. De plus, les organisations adoptent les plateformes SSE pour éliminer le besoin de concentrateurs VPN (63 %), d'inspection SSL (50 %) et de protection DDoS (44 %). Les meilleures plateformes SSE proposent des technologies ZTNA qui suppriment intégralement les VPN et la stack de sécurité entrante pour des économies phénoménales. Le ZTNA est également une solution intuitive facile à gérer qui permet aux organisations de réduire drastiquement le nombre de ressources et de personnes nécessaires à la gestion de l'accès sécurisé. Pour terminer, les solutions ZTNA sont proposées dans un modèle de paiement avec un abonnement et des coûts transparents, ce qui permet aux organisations de ne plus payer pour des licences inutiles.

Ne vous enfermez pas dans le VPN

Face à l'augmentation continue du nombre de travailleurs à distance et hybrides, les entreprises doivent adopter une solution d'accès moderne et sécurisée. Le ZTNA est une solution moderne pour surmonter les obstacles inhérents aux VPN et déployer un accès à distance plus sécurisé, flexible, évolutif, performant et économique.

De plus, le ZTNA fait partie intégrante d'une stratégie de sécurité avancée. Parmi les organisations qui envisagent une plateforme Security Service Edge (SSE), 50 % commencent par l'adoption du ZTNA. Par où allez-vous commencer ?

Remplacez intégralement votre VPN par HPE Aruba Networking ZTNA

En savoir plus sur l'utilisation de HPE Aruba Networking ZTNA comme alternative au VPN

Découvrez la plateforme HPE Aruba Networking SSE

arubanetworks.com/products/sse

Visitez **ArubaNetworks.com/fr**

Faites le bon achat.
Contactez nos spécialistes.

Nous contacter

BWP_Switch-to-ZTNA_A4_RB_022224 a00136655fre

Hewlett Packard Enterprise