Cinq critères pour choisir une solution d'accès réseau zero trust

netskope

Cinq critères vous permettant de choisir une solution d'accès réseau zero trust

Les entreprises adoptent rapidement le Security Service Edge (SSE) pour bénéficier des avantages d'une architecture SASE en toute sécurité. Une solution d'accès réseau zero trust (ZTNA) constitue un élément essentiel du SSE ; elle permet une connectivité spécifique aux applications pour les utilisateurs, où qu'ils se trouvent. Security Service Edge permet de consolider les fonctions de sécurité, de réduire le TCO et d'améliorer les processus à long terme, pour une meilleure sécurité globale.

netskope

L'importance de la plateforme

Que vous choisissiez et mettiez en œuvre le ZTNA dans le cadre d'un projet de travail à distance ou hybride, d'un projet initial dans le cadre d'une démarche de sécurité zero trust plus importante, ou que vous ayez une vision complète du SSE et du SASE, il est préférable de travailler avec un fournisseur disposant d'une plateforme SSE complète : un agent unique, une console unique et un moteur de politique unique, avec prise en charge d'un environnement multi-cloud.

Gartner estime que « d'ici 2025, 70 % des entreprises qui mettent en œuvre un accès réseau zero trust (ZTNA) basé sur un agent choisiront un éditeur de services de sécurité en périphérie (SSE) pour le ZTNA, plutôt qu'une offre autonome, contre seulement 20 % en 2021 »*.

*Gartner, « Magic Quadrant for Security Service Edge », John Watts, Craig Lawson, Charlie Winckless, Aaron McQuaid, 15 février 2022.

Permettre le travail hybride partout

Pour permettre le travail hybride depuis n'importe où, il est important de choisir un éditeur dont l'empreinte correspond à votre développement à l'international et à l'agilité de votre entreprise. Assurez-vous de travailler avec un fournisseur ZTNA qui dispose de datacenters dans les régions où vos employés se connectent. Le nombre de datacenters ne doit pas être votre seul critère de sélection. Votre choix doit être guidé par la disponibilité d'une pile de sécurité complète dans chaque région — avec des capacités de calcul complètes à la périphérie, près de vos utilisateurs — et des voies d'accès de trafic à faible latence, combinées à un peering étendu pour la meilleure expérience utilisateur et application.

03

Une politique facile à mettre en place

En plus d’un agent unique, la configuration des politiques d'identité et d'accès à l'aide d'une console unifiée ne devrait nécessiter qu'une seule étape. Ainsi, vous aurez accès aux applications cloud et privées en quelques jours pour soutenir les fusions et acquisitions et d’autres activités pour lesquelles le temps est un facteur clé.

Ne vous encombrez pas avec un VPN applicatif et des règles de pare-feu complexes qui sont loin des fonctionnalités d’un véritable ZTNA.

Protéger les données partout

Votre solution ZTNA doit analyser le comportement des utilisateurs et des entités (UEBA), appliquer des règles et des politiques DLP avancées et appliquer une stratégie d'accès adaptative en fonction des risques encourus par les utilisateurs.

ZTNA connecte en toute sécurité les utilisateurs aux applications et ressources privées. Ces ressources sont souvent la pièce maîtresse de l'organisation, qu'il s'agisse de code ou d'autres formes de données exclusives telles que les secrets commerciaux. Choisissez une solution qui offre plusieurs options pour aider votre organisation à protéger ces informations. Par exemple, une solution ZTNA moderne doit offrir les options d'inspection du trafic et d'application de la DLP pour protéger les données. Cependant, certaines organisations peuvent préférer l'UEBA et l'évaluation du risque utilisateur pour obtenir un contexte en temps réel sans déchiffrer le trafic et pour minimiser les risques internes.

05

Intégration efficace des tiers

Avec les bonnes intégrations et les échanges adaptés dans les environnements multi-fournisseurs, ZTNA peut réellement faire la différence. Les meilleurs échanges offrent des scores de confiance des utilisateurs et des appareils qui sont normalisés dans l'ensemble de l'environnement et peuvent déclencher des contrôles d'accès évolutifs, des paramètres de groupes d'utilisateurs et un système de tickets automatisé pour les enquêtes.

Conclusion

N’oubliez pas que le principe du zero trust ne signifie PAS qu’il ne faut faire confiance à personne, car pour permettre aux entreprises de fonctionner, il faut étendre l’accès (la confiance). La clé pour tirer parti des principes zero trust dans votre organisation, que ce soit spécifiquement avec ZTNA ou autrement, est d’utiliser la technologie afin de prendre de meilleures décisions contextuelles, concernant la confiance et l’accès pour un utilisateur donné, et de surveiller et d'adapter en permanence pour atténuer les risques. Ce contexte est basé sur un certain nombre de facteurs, tels que le rôle et l’identité de l’utilisateur, l’identité de l’appareil, le niveau de sécurité, le type d’application, le risque lié à l’application et l’instance de l’application, ainsi que le niveau de sensibilité des données. Les décisions contextuelles se traduisent par des stratégies d’accès robustes, optimisées en fonction des risques, qui peuvent être appliquées de manière uniforme sur le cloud, le Web et les applications privées, tout en favorisant l’agilité de l’entreprise et la productivité des utilisateurs.

Pour en savoir plus

Netskope est un leader mondial de la cybersécurité qui révolutionne la sécurité du cloud, des données et des réseaux pour aider les organisations qui appliquent les principes du zero trust à protéger leurs données. La plateforme Netskope Intelligent Security Service Edge (SSE) est rapide, facile à utiliser et sécurise vos collaborateurs, vos appareils et vos données, partout.

Pour découvrir comment Netskope aide ses clients à se préparer à tout contexte dans leur transition vers le SASE, rendez-vous sur **netskope.com**.