SOPHOS
Cybersecurity evolved.

Les six principaux avantages du ZTNA

Par rapport au VPN d'accès à distance

Un livre blanc Sophos. Octobre 2021

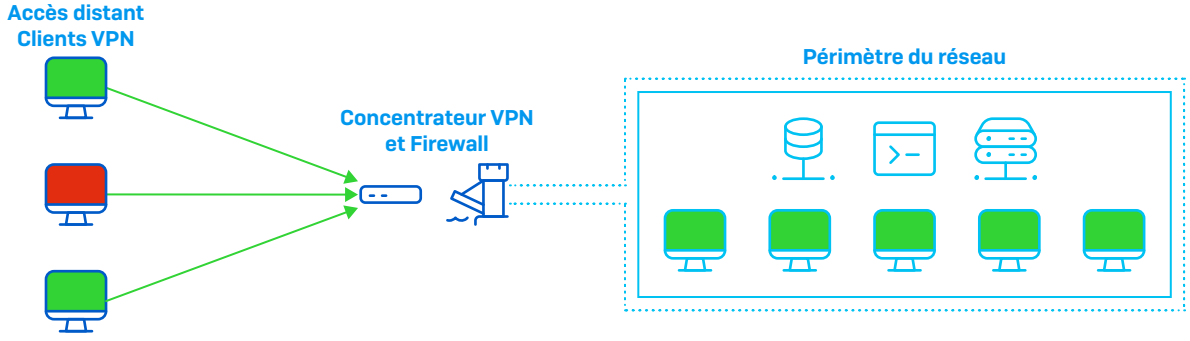
L'accès à distance par VPN nous a longtemps bien servi, mais l'augmentation récente du travail à distance a mis en lumière les limites de cette technologie vieillissante. Alors que certaines organisations continuent de tirer le maximum du VPN, beaucoup cherchent une meilleure alternative — une solution qui réponde aux problèmes rencontrés avec les VPN d'accès à distance. De nombreuses organisations ont déjà commencé à adopter pleinement la nouvelle génération de technologie d'accès à distance : le ZTNA (Zero Trust Network Access) ou accès réseau Zero Trust. Par rapport au VPN d'accès à distance traditionnel, le ZTNA offre une meilleure sécurité, un contrôle plus granulaire, une visibilité accrue et une expérience utilisateur transparente.

Dans ce guide d'achat du ZTNA, nous examinerons les limites et les défis du VPN d'accès à distance traditionnel et les avantages que l'accès réseau Zero Trust peut offrir. Nous résumerons par une liste de capacités essentielles que vous devriez rechercher dans votre nouvelle solution ZTNA.

Limites du VPN d'accès à distance

L'accès à distance par VPN est depuis des décennies un élément essentiel de la plupart des réseaux. Il fournit une méthode sécurisée pour accéder à distance aux systèmes et aux ressources du réseau. Cependant, il a été développé à une époque où le réseau d'entreprise ressemblait à une fortification médiévale — la muraille et les douves du château qui formaient un périmètre sécurisé autour des ressources du réseau. Le VPN fournissait l'équivalent d'une porte sécurisée permettant aux utilisateurs autorisés de pénétrer dans le périmètre sécurisé, mais une fois à l'intérieur, ils avaient un accès total à tout ce qui se trouvait dans le périmètre.

VPN d'accès à distance traditionnel



Bien sûr, les réseaux ont considérablement évolué et sont aujourd'hui plus distribués que jamais. Les applications et les données sont désormais hébergées dans le Cloud, les utilisateurs travaillent à distance et les réseaux sont assiégés par des attaquants et des hackers à la recherche de la moindre faiblesse à exploiter.

L'administration d'une solution d'accès à distance basée sur un VPN traditionnel (IPSec/SSL) dans tout type d'environnement moderne peut être extrêmement difficile. Vous devez vous occuper de la gestion des adresses IP, des flux de trafic et du routage, des règles d'accès au pare-feu, ainsi que du déploiement et de la configuration des clients et des certificats. Au-delà d'une poignée de nœuds et de quelques douzaines d'utilisateurs, cela devient un travail à temps plein — juste pour en assurer le fonctionnement. Et comme si cela ne suffisait pas, surveiller et contrôler la sécurité devient un véritable enfer.

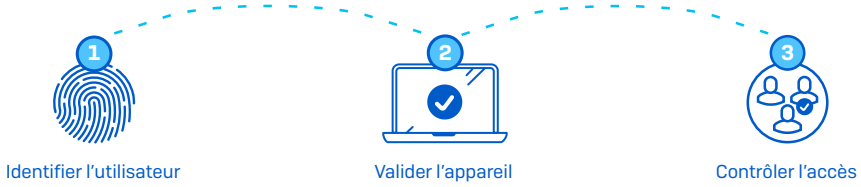
En résumé, le VPN d'accès à distance traditionnel présente un certain nombre de limitations et de défis inutiles :

1. **Confiance implicite** – Le VPN d'accès à distance permet de franchir le périmètre et d'accéder au réseau de l'entreprise comme si vous y étiez physiquement. Pour cela, on vous fait implicitement confiance et on vous octroie un accès large aux ressources de ce réseau, ce qui peut présenter des risques de sécurité énormes et inutiles.
2. **Vecteur de menace potentiel** – Le VPN d'accès à distance n'a aucune connaissance de l'état de sécurité de l'appareil utilisé pour se connecter au réseau d'entreprise, ce qui crée une route potentielle pour les menaces provenant d'appareils compromis.
3. **Backhauling inefficace** – Le VPN d'accès à distance fournit un point de présence unique sur le réseau, ce qui nécessitera potentiellement le backhauling du trafic provenant de plusieurs sites, datacenters ou applications à travers le tunnel VPN d'accès à distance.
4. **Manque de visibilité** – Le VPN d'accès à distance n'a pas conscience du trafic et des modèles d'utilisation qu'il facilite, ce qui rend plus difficile la visibilité de l'activité des utilisateurs et de l'utilisation des applications.
5. **Expérience utilisateur** – Les clients VPN d'accès à distance sont connus pour offrir une expérience utilisateur médiocre, ajouter de la latence ou avoir un impact négatif sur les performances, souffrir de problèmes de connectivité et, d'une manière générale, être une charge pour le service d'assistance.
6. **Administration, déploiement et enrôlement** – Les clients VPN d'accès à distance sont difficiles à configurer et à déployer, et il est parfois complexe d'enrôler de nouveaux utilisateurs et de désactiver les utilisateurs qui partent. Le VPN est également difficile à administrer du côté du pare-feu ou de la passerelle, notamment en raison des nœuds multiples, des règles d'accès au pare-feu, de la gestion des adresses IP, des flux de trafic et du routage. Cela devient rapidement un travail à plein temps.

Qu'est-ce que le ZTNA et comment fonctionne-t-il ?

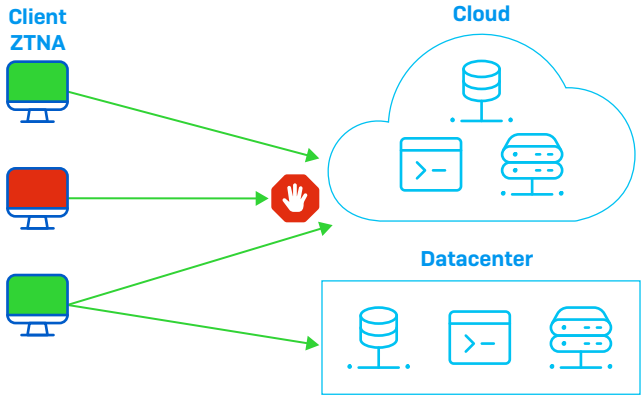
Le ZTNA ou accès réseau Zero Trust a été conçu dès le départ pour relever les défis et les limites de l'accès à distance par VPN. Il offre une meilleure solution aux utilisateurs, où qu'ils soient, pour se connecter en toute sécurité aux applications et aux données dont ils ont besoin pour faire leur travail, mais rien de plus. Il existe quelques différences fondamentales qui distinguent le ZTNA du VPN d'accès à distance.

Comme son nom l'indique, le ZTNA est fondé sur le principe du Zero Trust (confiance zéro) qui peut se définir comme : « ne faites confiance à rien ni personne, vérifiez tout ». Le Zero Trust élimine essentiellement le concept du périmètre des murailles et des douves d'un château en faveur d'un périmètre propre à chaque utilisateur, à chaque appareil et à chaque application en réseau, qui ne sera interconnecté qu'après la validation des informations d'identification, la vérification de l'état de l'appareil et le contrôle de la politique d'accès. Cela améliore considérablement la sécurité, la segmentation et le contrôle.



Une autre différence majeure dans le fonctionnement du ZTNA est que les utilisateurs ne sont pas simplement lâchés sur le réseau avec une liberté de mouvement totale. Au lieu de cela, des tunnels individuels sont établis entre l'utilisateur et la passerelle spécifique pour l'application à laquelle il est autorisé à accéder, et rien de plus. Cela fournit un niveau beaucoup plus sécurisé de micro-segmentation. Cela présente un certain nombre d'avantages en matière de sécurité, de contrôle, de visibilité, d'efficacité et de performances. Par exemple, le VPN d'accès à distance n'offre aucune visibilité sur les applications auxquelles les utilisateurs accèdent, tandis que le ZTNA peut fournir le statut et l'activité en temps réel pour toutes vos applications. Cela est inestimable pour identifier les problèmes potentiels et effectuer des audits de licence. La micro-segmentation supplémentaire fournie par le ZTNA garantit qu'il n'y a pas de mouvement latéral de l'accès des appareils ou des utilisateurs entre les ressources sur le réseau. Chaque utilisateur, appareil, application ou ressource constitue littéralement son propre périmètre de sécurité et il n'y a plus de notion de confiance implicite.

Zero Trust Network Access



Le ZTNA est également plus dynamique et transparent par nature, puisqu'il fonctionne en arrière-plan sans nécessiter d'interaction de la part de l'utilisateur au-delà de la validation initiale de l'identité. Cette expérience peut être si fluide et sans friction que les utilisateurs ne se rendront même pas compte qu'ils se connectent à des applications via des tunnels chiffrés sécurisés.

Avantages du ZTNA

Le Zero Trust Network Access offre d'énormes avantages à bien des égards, mais il est principalement adopté pour une ou plusieurs des raisons suivantes :

- **Télétravail :** Les solutions ZTNA constituent une solution beaucoup plus facile pour gérer l'accès à distance du personnel travaillant à domicile. Elles rendent le déploiement et l'enrôlement plus aisés et plus souples, transformant ce qui aurait pu être un travail à plein temps avec le VPN en quelque chose de beaucoup moins gourmand en ressources. Tout est également plus transparent et plus simple pour votre personnel travaillant à distance.
- **Micro-segmentation des applications :** Les solutions ZTNA offrent une bien meilleure sécurité des applications grâce à la micro-segmentation, à l'intégration de l'état de sécurité des appareils dans les politiques d'accès, à la vérification continue de l'authentification et tout simplement à l'élimination de la confiance implicite et des mouvements latéraux qui accompagnent les VPN.
- **Blocage des ransomwares :** Les solutions ZTNA éliminent un vecteur d'attaque courant des ransomwares et d'autres attaques d'infiltration de réseau. Puisque les utilisateurs du ZTNA ne sont plus « sur le réseau », les menaces qui pourraient s'infiltrer par le biais du VPN n'ont aucun endroit où aller avec le ZTNA.
- **Intégration rapide de nouvelles applications et de nouveaux utilisateurs :** Le ZTNA permet une meilleure sécurité et une plus grande agilité dans des environnements qui évoluent rapidement avec des utilisateurs qui vont et viennent. Mettez en place de nouvelles applications rapidement et en toute sécurité, enrôlez et supprimez facilement des utilisateurs et des appareils, et obtenez des informations sur l'état de sécurité et l'utilisation des applications.

En résumé, les avantages du ZTNA par rapport aux solutions VPN d'accès à distance traditionnelles sont les suivants :

1. **Zero Trust** – Le ZTNA est fondé sur le principe du Zero Trust (confiance zéro), c'est-à-dire « ne faites confiance à rien ni personne, vérifiez tout ». Cela permet d'améliorer considérablement la sécurité et la micro-segmentation en traitant effectivement chaque utilisateur et chaque appareil comme son propre périmètre et en évaluant et vérifiant constamment l'identité et l'état de sécurité pour obtenir l'accès aux applications et aux données de l'entreprise. Les utilisateurs n'ont accès qu'aux applications et aux données définies explicitement par leurs politiques, ce qui réduit les mouvements latéraux et les risques qui en découlent.
2. **État de sécurité des appareils** – Le ZTNA intègre la conformité et l'état de sécurité des appareils dans les politiques d'accès, ce qui vous donne la possibilité d'exclure les systèmes non conformes, infectés ou compromis de l'accès aux applications et aux données de l'entreprise, éliminant ainsi un vecteur majeur de menaces et réduisant le risque de vol ou de fuite de données.
3. **Fonctionne partout** – Le ZTNA est indépendant de tout réseau, et peut fonctionner aussi bien et de manière aussi sécurisée depuis n'importe quel réseau, que ce soit à la maison, à l'hôtel, au café ou au bureau. La gestion des connexions est sécurisée et transparente, quel que soit l'endroit où se trouvent l'utilisateur et l'appareil, ce qui en fait une expérience transparente en tout lieu.
4. **Plus de transparence** – Le ZTNA offre une expérience transparente à l'utilisateur final en établissant automatiquement des connexions sécurisées à la demande, en arrière-plan, au fur et à mesure des besoins. La plupart des utilisateurs ne seront même pas conscients de la solution ZTNA qui contribue à protéger leurs données.
5. **Meilleure visibilité** – Le ZTNA peut offrir une meilleure visibilité sur l'activité des applications, ce qui peut s'avérer important pour le contrôle de l'état des applications, la planification de la capacité, la gestion des licences et les audits.
6. **Administration plus aisée** – Les solutions ZTNA sont souvent beaucoup plus légères, plus propres et donc plus faciles à déployer et à gérer. Elles peuvent également être plus agiles dans des environnements qui changent rapidement, avec des utilisateurs qui vont et viennent, ce qui fait de l'administration quotidienne une tâche rapide et aisée et non un travail à plein temps.

Guide d'achat : que rechercher dans une solution ZTNA ?

Lorsque vous comparez les solutions ZTNA de différents fournisseurs, en plus de vérifier les plateformes prises en charge pour les clients, les passerelles et les fournisseurs d'identité, assurez-vous de prendre en compte les capacités suivantes :

Fourni depuis le Cloud, géré dans le Cloud

La gestion dans le Cloud offre des avantages considérables, qu'il s'agisse de la possibilité d'être opérationnel instantanément, de la réduction de l'infrastructure de gestion, du déploiement et de l'enrôlement, ou de l'accès en tout lieu. L'un des principaux avantages de la gestion Cloud est de pouvoir se connecter et commencer à utiliser la solution instantanément, sans ajouter de serveurs ou d'infrastructure de gestion supplémentaires. La gestion Cloud offre également un accès sécurisé instantané de n'importe où et sur n'importe quel appareil, ce qui vous permet de travailler comme vous le souhaitez. Elle permet également d'enrôler facilement de nouveaux utilisateurs, où qu'ils se trouvent dans le monde.

Intégration avec vos autres solutions de cybersécurité

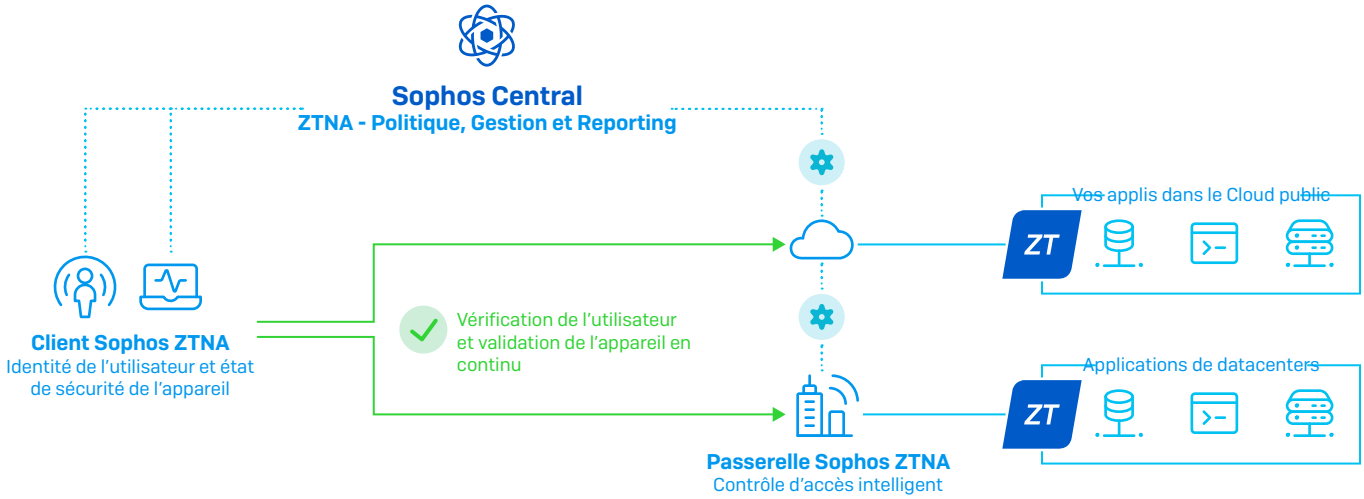
Si la plupart des solutions ZTNA peuvent parfaitement fonctionner en tant que produits autonomes, il est très avantageux de disposer d'une solution étroitement intégrée à vos autres produits de cybersécurité, tels que votre pare-feu et vos solutions Endpoint. Une console de gestion Cloud commune et intégrée peut être un multiplicateur de force pour vous et votre équipe. L'utilisation d'une seule interface pour gérer toute votre sécurité informatique en un seul endroit, y compris le ZTNA, peut réduire le temps de formation de votre personnel et les frais généraux de gestion quotidienne. Vous obtenez également des informations uniques sur vos différents produits de sécurité informatique, en particulier si ces derniers partagent des données télémétriques, renforçant ainsi considérablement la sécurité et offrant une réponse en temps réel lorsqu'un appareil compromis ou une menace arrivent sur le réseau. Vos produits peuvent travailler ensemble pour répondre instantanément à la présence d'une attaque ou d'une menace et l'empêcher de se déplacer latéralement, de se propager ou de voler des données.

Expérience utilisateur et expérience de gestion

Assurez-vous que la solution que vous envisagez offre une excellente expérience utilisateur et qu'elle facilite l'administration et la gestion. De nos jours, avec un nombre croissant d'utilisateurs travaillant à distance dans le monde entier, l'enrôlement et la configuration efficace des appareils sont essentiels pour que les nouveaux utilisateurs soient productifs aussi rapidement que possible. Veillez à prêter attention à la manière dont l'agent ZTNA est déployé et à la facilité avec laquelle il est possible d'ajouter de nouveaux utilisateurs aux politiques de sécurité. Veillez également à ce que la solution dans laquelle vous investissez offre une expérience fluide et sans friction pour les utilisateurs finaux et offre la visibilité que vous escomptez, comme un aperçu en temps réel de l'activité des applications qui vous aidera à identifier de manière proactive les pics de charge, la capacité, l'utilisation des licences et même les problèmes d'application.

Sophos ZTNA

Sophos ZTNA a été conçu dès le départ pour rendre l'accès réseau Zero Trust aisé, intégré et sécurisé. Sophos ZTNA est fourni et géré dans le Cloud, intégré à Sophos Central, la plateforme de reporting et de gestion de la cybersécurité la plus fiable au monde. À partir de Sophos Central, vous pouvez non seulement gérer ZTNA, mais aussi vos solutions Sophos Firewall, Endpoint, serveur, mobile, Cloud, messagerie, et bien plus encore.



Sophos ZTNA est également unique en ce qu'il s'intègre étroitement avec Sophos Firewall et Sophos Intercept X Endpoint. Cela permet de tirer parti de la Sécurité Synchronisée et de la fonction Security Heartbeat pour partager l'état des appareils entre le pare-feu, l'appareil, la solution ZTNA et Sophos Central afin de répondre automatiquement aux menaces ou aux appareils non conformes. Limitez automatiquement l'accès et contenez les systèmes compromis, jusqu'à ce que ceux-ci soient nettoyés.

Les clients de Sophos s'accordent à dire que les avantages en termes de gain de temps d'une solution de cybersécurité Sophos entièrement intégrée sont énormes. Ils affirment que l'utilisation de la suite de produits Sophos, administrée depuis Sophos Central, et l'utilisation de la Sécurité Synchronisée pour l'identification et la réponse automatiques aux menaces, revient à virtuellement doubler la taille de leur équipe informatique. Bien sûr, Sophos ZTNA peut fonctionner avec les produits de sécurité de n'importe quel autre éditeur, mais il est unique en ce qu'il fonctionne à son optimum avec le reste de l'écosystème Sophos pour offrir des avantages concrets en termes de visibilité, de protection et de réponse.

Plus d'informations sur

Sophos.fr/ztna

Sophos France
Tél. : 01 34 34 80 00
Email : info@sophos.fr

21-10-07 FR (DD)

SOPHOS