eBook

Les 6 cas d'utilisation les plus pertinents pour un remplacement complet des VPN existants

netskope

Introduction

L'infrastructure VPN d'accès à distance présente depuis longtemps d'importantes failles de sécurité. Sa connectivité étendue facilite l'accès des attaquants et permet des déplacements latéraux non autorisés au sein du réseau. De plus, obliger les utilisateurs distants à faire passer leur trafic non local par le VPN pour accéder à Internet nuit à leur expérience. Cette approche entraîne également des coûts élevés et une complexité du routage.

Pour les entreprises cherchant à moderniser la connectivité de leur personnel hybride, le ZTNA (Zero Trust Network Access) représente l'alternative moderne aux VPN traditionnels d'accès à distance. Cependant, toutes les solutions ZTNA ne permettent pas de remplacer efficacement le VPN dans son ensemble.

Pour mener à bien la transition du VPN classique vers le ZTNA, il est essentiel d'identifier et de hiérarchiser les principaux cas d'utilisation avant d'entreprendre la migration complète. Une préparation minutieuse et des investissements technologiques ciblés permettront aux équipes de mettre définitivement hors service leur VPN.

1. Autonomisez les travailleurs hybrides

Puisque la majorité des collaborateurs adoptent désormais un modèle de travail hybride, les solutions VPN traditionnelles ne répondent plus aux besoins en matière de sécurité et de connectivité nécessaires pour autonomiser efficacement la main-d'œuvre. Le VPN d'accès à distance offre une visibilité limitée sur les activités des applications, et souffre de problèmes de latence et de performance à cause de l'acheminement du trafic. Il accorde un accès étendu au réseau pour les utilisateurs authentifiés, ce qui augmente la surface d'attaque en raison des déplacements latéraux non contrôlés. De plus, les concentrateurs VPN non corrigés représentent des points d'entrée majeurs pour les cyberattaques.

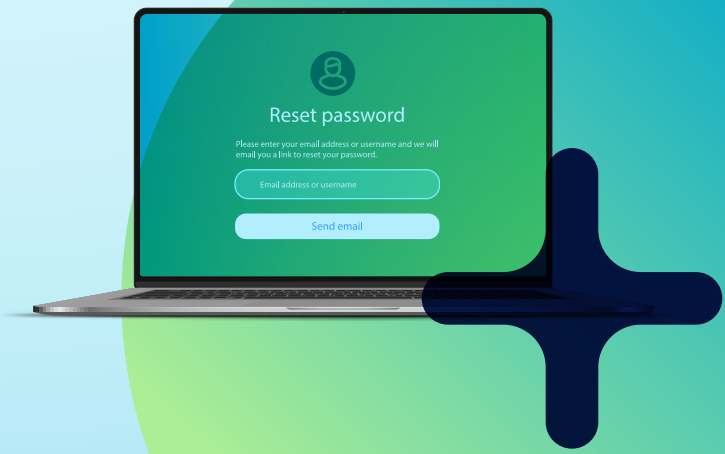
En passant des solutions VPN à distance traditionnelles à une solution ZTNA telle que Netskope One Private Access, les entreprises peuvent mieux gérer les risques de sécurité associés aux VPN. En effet, un accès minimal aux applications privées est appliqué en fonction de l'identité et du contexte, tout en limitant les déplacements latéraux non autorisés. Netskope One Private Access offre une visibilité en temps réel sur le trafic détaillé des applications et les activités des utilisateurs. Il garantit aussi une application uniforme des stratégies pour les collaborateurs, qu'ils soient à distance ou sur site. De plus, la solution permet d'établir une connectivité sécurisée avant l'ouverture de session. Elle facilite ainsi l'intégration sécurisée des nouveaux appareils et la réinitialisation des mots de passe pour les télétravailleurs, garantissant que seuls les appareils autorisés peuvent accéder aux ressources internes critiques, telles que les services d'annuaire.

11 heures par an
perdues par les collaborateurs devant réinitialiser leurs mots de passe[1]

CONSEILS DE MISE EN ŒUVRE :

Un inventaire des déploiements VPN constitue une excellente première étape pour mettre à niveau votre infrastructure. Celui-ci doit recenser :

- **Le nombre d'instances de services VPN d'accès à distance que vous utilisez actuellement**
- **Le volume du trafic applicatif passant par ces VPN d'accès à distance**
- **Le nom des utilisateurs ayant un accès VPN à ces applications**



[1]Business Reporter, « How much time does your organisation spend on managing passwords? », 7 septembre 2022. https://www.independent.co.uk/news/business/business-reporter/time-organisation-managing-passwords-b2161856.html

2. Accélérez la migration vers le cloud

La transformation numérique a franchi un cap décisif. Aujourd'hui, davantage de charges de travail sont hébergées dans des clouds publics plutôt que dans des datacenters privés. La connectivité à l'IaaS, tant pour les utilisateurs sur site qu'à distance, est désormais une priorité et représente l'une des principales préoccupations des entreprises lorsqu'elles définissent leur stratégie cloud et leur plan de déploiement. Dans une infrastructure VPN d'accès à distance classique, le trafic utilisateur est d'abord dirigé vers le datacenter privé, puis connecté aux clouds IaaS via MPLS ou d'autres tunnels dédiés comme AWS Direct Connect ou Azure ExpressRoute. Ce backhauling du trafic entraîne non seulement une mauvaise expérience pour l'utilisateur et des coûts d'infrastructure accrus, mais il implique également un routage réseau complexe.

Grâce à sa solution moderne destinée à remplacer les VPN traditionnels, Netskope permet une connexion directe et optimisée vers le cloud public, sans aucun détour inutile du trafic réseau. La connexion reste sécurisée, flexible et hautement évolutive. Netskope One Private Access protège les données et les ressources grâce à un contrôle d'accès au niveau de l'application, fondé sur l'identité de l'utilisateur et la posture de sécurité de l'appareil. En privilégiant une connectivité basée sur la logique plutôt que sur le protocole IP, cette approche permet de simplifier nettement l'administration des réseaux et du cloud, ce qui facilite l'automatisation et élimine le backhauling du trafic.

CONSEILS DE MISE EN ŒUVRE :

Les entreprises souhaitant remplacer leur VPN d'accès à distance doivent également considérer les instances de VPN dans le cloud, telles qu'AWS Client VPN ou Azure VPN Gateway. Elles doivent s'appuyer sur des outils d'automatisation, comme les modules Terraform, pour automatiser le déploiement, la configuration et la mise à l'échelle des instances Netskope One Private Access exécutées dans EC2 et d'autres environnements cloud.

3. Facilitez l'accès aux appareils non managés (lorsque cela est pertinent !)

Les entreprises doivent fournir un accès sécurisé à leurs ressources pour les sous-traitants externes, prestataires de services et partenaires. Simultanément, les collaborateurs veulent un accès fluide aux ressources privées depuis leurs appareils personnels. L'objectif est de permettre aux appareils non managés d'accéder facilement aux ressources, tout en évitant de les exposer sur Internet ou dans une zone démilitarisée. Il n'est pas toujours possible d'imposer l'installation d'un logiciel client, car de nombreux utilisateurs ne souhaitent pas ajouter des applications sur leurs appareils personnels. Accorder un accès VPN à des appareils non managés peut entraîner une ouverture excessive accompagnée de risques de sécurité.

Vous pouvez fournir un accès sécurisé aux appareils non managés pour les utilisateurs tiers, les partenaires externes et le BYOD des collaborateurs, tout en évitant les risques liés aux VPN, à la DMZ ou à l'exposition des ressources sur l'Internet public. Netskope One Private Access permet un déploiement sans client pour les appareils non managés. Il garantit ainsi un accès sécurisé et Zero Trust aux applications privées, qu'elles soient hébergées sur site ou dans le cloud.

Le déploiement du modèle ZTNA sans client permet un accès fluide, via un navigateur, grâce à une architecture de proxy inverse intégrée aux fournisseurs d'identité (IdP) pour authentifier les utilisateurs qui cherchent à accéder aux applications privées. En utilisant les mêmes contrôles DLP sur la plateforme Netskope One SSE, les entreprises peuvent garantir une visibilité granulaire et appliquer une stratégie de protection des données cohérente sur tous les appareils, qu'ils soient managés ou non.

En moyenne, un collaborateur utilise **2,5 appareils au travail**, y compris des appareils personnels tels que des ordinateurs portables, des smartphones et des tablettes.[2]

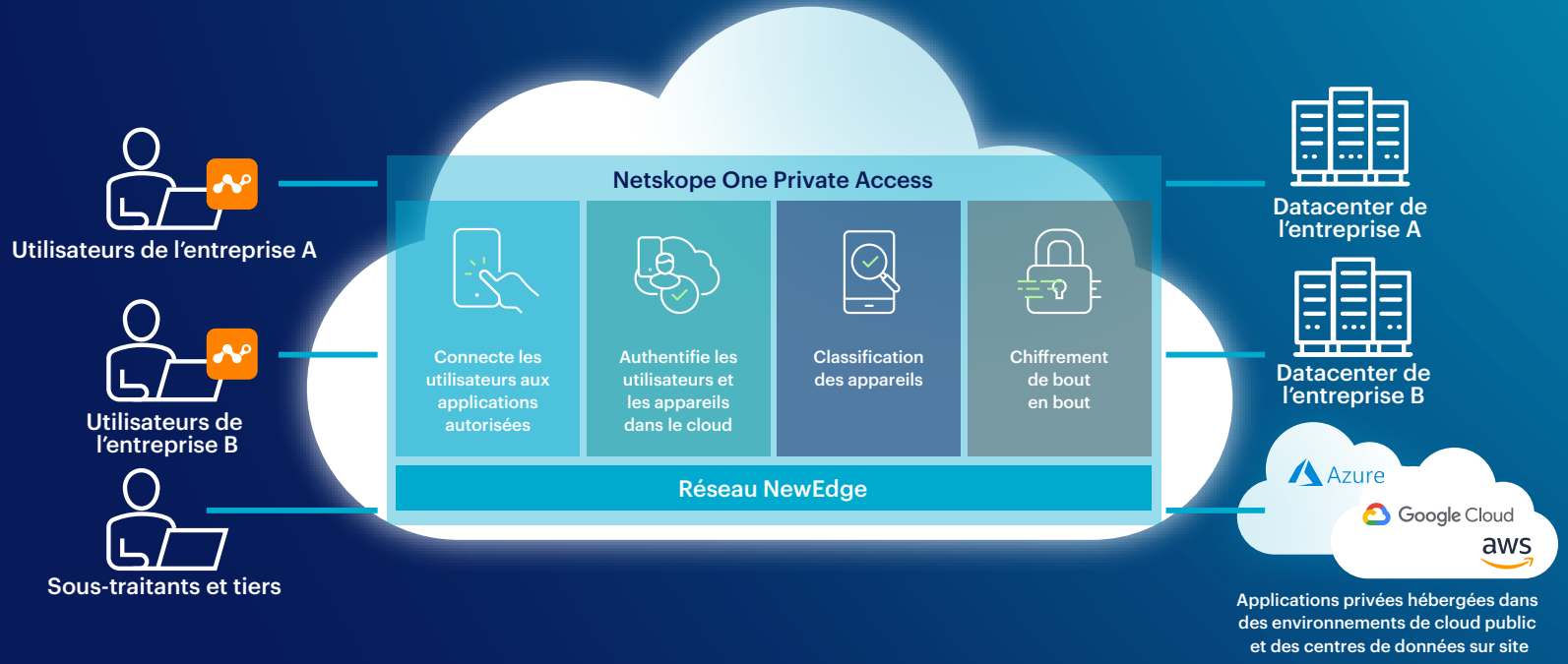
[2]Zippia. « 26 Surprising BYOD Statistics [2023]: BYOD Trends In The Workplace » Zippia.com. 17 octobre 2022. https://www.zippia.com/advice/byod-statistics/

4. Accélérez l’intégration des fusions-acquisitions

Les fusions-acquisitions sont des événements rapides et à fort enjeu. Pour les équipes en charge de l’IT, des réseaux et de la cybersécurité, elles représentent un ensemble de problèmes uniques. Le succès d’une fusion-acquisition repose sur la vitesse avec laquelle l’intégration des deux entreprises peut être réalisée.

Les équipes en charge des opérations IT se doivent de garantir un accès immédiat. Elles doivent connecter les utilisateurs des deux entités aux applications internes stratégiques tout en assurant la sécurité des données sensibles. Les méthodes traditionnelles de fusion de deux réseaux sont coûteuses, longues et complexes. Elles entraînent fréquemment des conflits d’adresses IP et nécessitent une renumérotation des adresses. De plus, les règles de pare-feu traditionnelles offrent souvent un contrôle d’accès limité, ce qui expose les deux réseaux à des vulnérabilités.

Disponible sous forme de solution tout-en-un, Netskope One Private Access intègre les fonctionnalités ZTNA et SD-WAN dans un seul client léger. Celui-ci permet la mise hors service complète des VPN d’accès à distance pour l’accès aux applications, et pas seulement leur remplacement partiel. Un client SASE unifié dirige automatiquement le trafic des utilisateurs vers leurs destinations, qu’il s’agisse d’applications cloud, d’applications privées, d’IaaS ou du web. Netskope One Private Access aide les entreprises à capter rapidement la valeur commerciale lors des fusions-acquisitions. Il offre un accès immédiat aux ressources essentielles dès le premier jour. Les applications héritées sont même incluses. Cette solution élimine le besoin d’installer un VPN et de fusionner les réseaux. Les entreprises peuvent ainsi démarrer l’intégration en toute sécurité sans délai. L’accès est accordé en fonction de critères de confiance adaptatifs. Ces critères prennent en compte l’identité de l’utilisateur, la sécurité de l’appareil et d’autres facteurs contextuels. Grâce à un accès sélectif aux applications et aux données, Netskope One Private Access réduit le risque de déplacements latéraux et d’exposition des informations sensibles.



Offrez un accès immédiat aux ressources internes sans les complexités liées à la combinaison des réseaux, à la configuration du VPN site à site et aux règles de pare-feu.

5. Prenez en charge les centres de contact à distance

Il y a **1,8 million** de collaborateurs dans les centres d'appels dans le monde, et 52 % des centres d'appels aux États-Unis emploient des agents à distance.[3] Ces agents exercent dans différents métiers, comme le service client, la réservation de voyages, le conseil en santé, et bien d'autres domaines. Alors que de nombreux centres d'appels migrent vers des solutions de communication unifiée en tant que service (UCaaS) basées sur le cloud, de nombreuses entreprises continuent d'utiliser la VoIP hébergée sur site et redirigent souvent les appels via un VPN d'accès à distance. Pour les agents des centres d'appels à distance, la qualité de la VoIP peut devenir imprévisible lorsqu'elle dépend des VPN. Le trafic accru engendre souvent des problèmes de gigue et de latence, ce qui peut être frustrant tant pour les agents que pour les clients au bout du fil.

À ce jour, la plupart des solutions ZTNA basées sur le cloud ne prennent pas en charge les systèmes VoIP hébergés sur site, ce qui oblige les entreprises à maintenir à la fois l'infrastructure ZTNA et VPN.

52 %
des centres d'appel aux États-Uni emploient des agents à distance

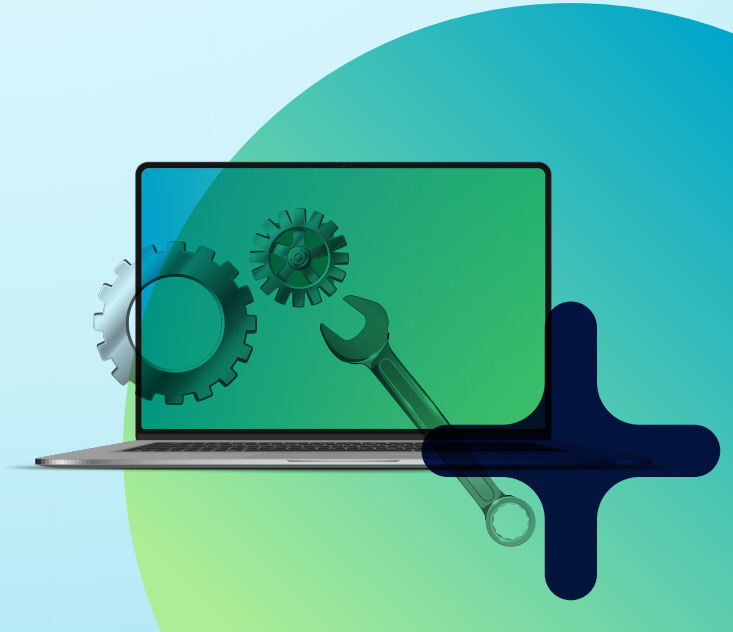
Netskope One Private Access réunit les technologies ZTNA et SD-WAN en une seule solution complète et intégrée. Grâce à une gestion intelligente du trafic réseau et à une qualité de service adaptée au contexte, les téléconseillers sont plus efficaces dans leur travail. Cette approche offre une expérience optimale pour les applications vocales et vidéo. Elle renforce également la posture de sécurité, ce qui garantit un accès Zero Trust à toutes les ressources internes.

[3]Source : « Call Center Statistics – 2023 » Truelist.com. 1er janvier 2023. https://truelist.co/blog/call-center-statistics/#:~:text=The%20number%20of%20people%20working,million%20currently%20to%201.8%20million.

6. Prenez en charge vos applications héritées

La validation de la compatibilité est essentielle avant toute mise à jour de vos systèmes. Les entreprises qui déploient un ZTNA doivent également tester la compatibilité des applications. Lors de ce processus, elles découvriront probablement des applications héritées incompatibles avec la plupart des solutions ZTNA actuelles. Par exemple, les applications héritées qui nécessitent un trafic initié par le serveur ne fonctionnent pas bien avec la « connectivité inside-out » d'une solution ZTNA moderne, qui exige que le trafic soit initié par le terminal. Ces anciens systèmes, généralement propriétaires, demandent beaucoup d'efforts, de moyens et une organisation rigoureuse pour être transformés et mis à jour. Cette modernisation passe souvent par une transition vers des solutions cloud de type IaaS.

Netskope One Private Access résout ces problèmes liés aux applications héritées en offrant un accès sécurisé et optimisé à toutes les applications privées via un seul client intégré. Les entreprises peuvent ainsi prolonger la durée de vie des applications héritées, réduire les coûts liés à la gestion de multiples solutions d'accès à distance, et fournir un accès rapide et fiable aux applications, peu importe leur emplacement.



Conclusion

Autrefois considérés comme une technologie de pointe, les VPN d'accès à distance traditionnels représentent aujourd'hui un problème pour les équipes de sécurité, car ils constituent une source majeure de vulnérabilités face aux menaces. Ils sont également un fardeau pour les équipes d'infrastructure et d'exploitation, en raison de leur impact sur les performances réseau, ce qui dégrade l'expérience globale de l'utilisateur.

Cependant, la plupart des solutions ZTNA actuelles ne constitue pas une solution universelle. Lorsqu'elles ne couvrent pas tous les cas d'utilisation pertinents, les entreprises remplacent seulement partiellement le VPN. Les infrastructures se retrouvent alors mélangées – un VPN traditionnel combiné à une dose de ZTNA – et l'environnement peut devenir encore plus complexe qu'auparavant.

Netskope One Private Access a été conçu pour aider les organisations à accélérer l'adoption du ZTNA grâce à une solution entièrement intégrée. Cette approche facilite le remplacement complet de toute l'infrastructure VPN. Il propose une voie claire pour éliminer les VPN d'accès à distance dans tous les cas d'utilisation d'accès aux applications. La surface d'attaque numérique est ainsi réduite. La posture de sécurité se renforce grâce aux principes du Zero Trust. De plus, la productivité des télétravailleurs s'améliore grâce à une expérience d'accès aux applications fluide et optimisée.

À propos de Netskope One Private Access

Netskope One Private Access intègre des fonctionnalités SD-WAN au sein de la solution ZTNA afin d'assurer une connectivité sécurisée et performante vers toutes les applications privées, y compris la VoIP hébergée sur site, la vidéo et les services d'assistance à distance. Ainsi, les entreprises peuvent :

- Moderniser la connectivité et renforcer la sécurité.
- Améliorer l'expérience utilisateur.
- Assurer un accès optimisé et hautement fiable aux applications vocales et vidéo.
- Réduire la complexité et les coûts opérationnels.
- Abandonner progressivement l'infrastructure VPN d'accès à distance pour simplifier la gestion des outils de connexion.
- Obtenir une visibilité et un contrôle sans précédent sur le trafic des applications

Netskope One Private Access permet d'abandonner totalement le VPN d'accès à distance – et pas seulement de manière partielle – pour tous les scénarios d'accès aux applications pertinentes. Cette solution renforce également la sécurité tout en assurant une connexion optimale et sans friction aux applications.

À propos de Netskope

Netskope, un leader de la sécurité et des réseaux modernes, répond aux besoins des équipes de sécurité et de mise en réseau en fournissant un accès optimisé et une sécurité contextuelle en temps réel pour les utilisateurs, les appareils et les données, où qu'ils se trouvent. Des milliers de clients, dont plus de 30 parmi les entreprises du Fortune 100, font confiance à la plateforme Netskope One, à son moteur Zero Trust Engine et à son puissant réseau NewEdge pour réduire les risques et obtenir une visibilité et un contrôle complets sur l'activité du cloud, de l'IA, du SaaS, du web et des applications privées, en assurant la sécurité et en accélérant les performances sans sacrifice ni compromis. Pour en savoir plus, rendez-vous sur **netskope.com**.

Vous souhaitez en savoir plus ?

Demander une démo

netskope