LE GUIDE ZSCALER POUR:

Accélérer la transformation digitale sécurisée

Cinq clés pour réussir rapidement et en toute sécurité

Les nouveaux défis de l'IT

Votre entreprise adopte des applications cloud, le volume de votre trafic Internet a explosé et l'informatique mobile est devenu un outil important pour votre entreprise.

Le processus de transformation digitale peut être à la fois éprouvant et exaltant pour votre équipe informatique. Mais vous n'avez pour autant pas à en arriver au point de perdre le sommeil.

Ces cinq clés vous aideront à réussir une transformation digitale sécurisée:

1. Moderniser les infrastructures vieillissantes ›
2. Permettre une connectivité Internet sécurisée dans les filiales ›
3. Connecter les télétravailleurs en toute sécurité ›
4. Améliorer l'expérience utilisateur d'Office 365 ›
5. Simplifier l'intégration informatique en cas de fusion-acquisition ›

Découvrez dans cet article comment y arriver.

Moderniser les infrastructures vieillissantes

Depuis 30 ans, vous construisez des réseaux complexes pour connecter les utilisateurs aux applications du data center et investissez dans une multitude d'appliances de sécurité réseau pour garantir l'intégrité du système. Dans un monde où les menaces sont en constante évolution, la nécessité de mettre à jour ou de remplacer votre infrastructure vieillissante et d'ajouter de nouveaux contrôles de sécurité a augmenté, et avec elle la complexité de votre réseau et les coûts qu'il engendre.

Mais avec le nombre croissant d'utilisateurs et d'applications migrant hors du réseau, et l'augmentation du trafic lié au cloud, le modèle centré sur le réseau est de moins en moins pertinent.

Il est temps d'adopter une approche moderne et spécifique qui répond à vos besoins de sécurité et réduit les coûts en connectant les utilisateurs directement à leurs destinations. Il est temps de migrer la sécurité vers le cloud.

Par où commencer:

- **Utilisez une architecture SASE (Secure Access Service Edge)** conformément au rapport Gartner intitulé **« Le futur de la sécurité des réseaux se trouve dans le cloud »,** et référez-vous au **« Carré Magique de Gartner pour les passerelles Web sécurisées ».**
- **Passez d'une architecture réseau** en étoile à une connexion directe au cloud, et bénéficiez de la sécurité cloud en tant que service.
- **Au fil du temps, supprimez progressivement le matériel et les logiciels** pour libérer vos techniciens et réduire les tâches de gestion et de maintenance quotidiennes.

EXEMPLE DE RÉUSSITE

SIEMENS

Le cloud est devenu le nouveau data center, et Internet le nouveau réseau d'entreprise pour 350.000 utilisateurs de Siemens répartis dans 192 pays. Siemens a considérablement réduit ses coûts en optant pour une architecture réseau moderne conçue pour le cloud et offrant à tout moment et en tout lieu un accès sécurisé et performant aux applications.

« En passant directement par Internet au lieu de faire un backhauling de notre trafic, nous espérons réduire nos coûts de 70%. »

Frederik Janssen
Vice-président Stratégie informatique & Gouvernance
Siemens

Permettre une connectivité Internet sécurisée dans les filiales

Combien de temps faut-il à votre entreprise pour ouvrir une nouvelle succursale ? L'intégration de nouveaux sites à votre réseau en étoile est une entreprise longue et vorace en ressources. Et une fois que vos sites sont connectés, vous pouvez être confronté à des goulots d'étranglement et à une latence du trafic, d'autant plus que la demande croissante de bande passante submerge vos pare-feux, augmente les coûts liés au WAN et obstrue vos passerelles. Les réseaux anciens ne peuvent tout simplement pas évoluer aussi rapidement qu'on le souhaite.

À mesure que vous envisagez de passer au SD-WAN pour simplifier les opérations des filiales et mettre sur pieds des points d'accès locaux à Internet, vous devrez déplacer la sécurité du data center vers la périphérie de votre réseau pour exploiter le plein potentiel du SD-WAN.

Par où commencer:

- **Migrez votre sécurité vers le cloud** pour pouvoir inspecter tout le trafic, qu'il soit destiné au data center, aux services cloud ou à l'Internet ouvert.
- **Débarrassez vos filiales de tout équipement** en déployant des connexions Internet locales à chaque emplacement et en supprimant le MPLS lorsque c'est possible.
- **Recentrez les efforts de vos informaticiens locaux** sur le business et approuvez les initiatives de transformation.

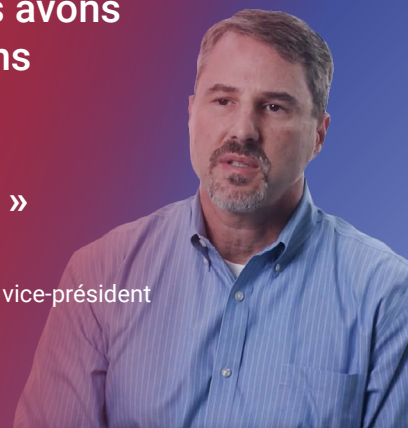
EXEMPLE DE RÉUSSITE

AutoNation

AutoNation, le plus grand concessionnaire automobile des États-Unis, a établi sur ses 360 sites des breakouts locaux qui offrent aux utilisateurs un accès Internet rapide et sécurisé. Avec Zscaler, AutoNation réalise des économies, connecte plus facilement de nouveaux sites et améliore sa sécurité grâce à l'inspection SSL en ligne, au sandboxing et à d'autres fonctionnalités.

« Grâce à Zscaler, nous avons limité nos installations à un simple routeur et à des terminaux pour nos 360 filiales. »

Ken Athanasiou,
Chef de la sécurité informatique et vice-président
AutoNation



Connecter les télétravailleurs en toute sécurité

Pour gérer les utilisateurs travaillant à distance et se connectant à leurs applications de partout, vous devez vous appuyer sur la technologie VPN qui étend votre réseau vers l'emplacement de l'utilisateur. Seulement, pour des raisons de sécurité, vous devez effectuer un backhauling du trafic vers le data center, avec pour conséquence une dégradation de l'expérience utilisateur qui pousse souvent les utilisateurs distants à contourner le VPN, augmentant ainsi les risques de sécurité. Pour ces raisons et bien d'autres, Gartner estime que, d'ici 2023, 60% des entreprises élimineront les VPN en faveur de ZTNA.[1]

S'appuyer uniquement sur la sécurité des terminaux ne suffit pas pour faire face à des menaces de pointe. Comment pouvez-vous tirer parti d'un cloud de sécurité Service Edge pour protéger vos utilisateurs et leur fournir une expérience irréprochable?

Par où commencer:

- **Adoptez une architecture ZTNA (Zero Trust Network Access)** pour permettre aux utilisateurs d'accéder aux applications sans leur donner accès au réseau.
- **Migrez la sécurité vers la périphérie** pour fournir une sécurité identique en tous lieux, tout en garantissant une expérience utilisateur rapide.
- **Accordez ou refusez l'accès aux applications** et réduisez la complexité de l'administration grâce à la gestion centralisée des identités.

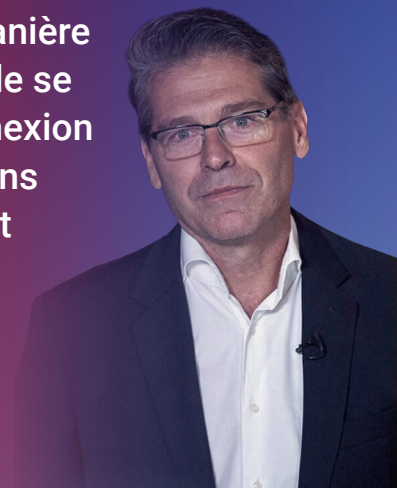
EXEMPLE DE RÉUSSITE

nab

Initialement, la National Australia Bank (NAB), la plus grande banque d'affaires d'Australie, a amorcé sa migration vers le cloud dans le but d'offrir aux clients une expérience bancaire meilleure et plus sécurisée ainsi que de fluidifier les opérations. Aujourd'hui, la NAB adopte la solution Zero Trust et fournit une infrastructure réseau pérenne qui rend le travail en tout lieu possible pour l'ensemble du personnel.

« Nos employés à domicile allument leur PC et travaillent exactement de la même manière qu'au bureau. Plus besoin de se soucier des étapes de connexion supplémentaires ou de jetons de sécurité - ça marche tout simplement. »

Steve Day
EGM de l'Infrastructure, du Cloud et du milieu professionnel
National Australia Bank



Améliorer l'expérience utilisateur d'Office 365

Compte tenu de la grande popularité des applications et des services d'Office 365, l'expérience utilisateur est un facteur important de la réussite de votre déploiement. Mais, comme le trafic des utilisateurs vers Office 365 augmente la charge du réseau, il submerge rapidement les pare-feux et entraîne une expérience utilisateur médiocre. Le déploiement d'Office 365 pousse souvent à effectuer des mises à niveau matérielles coûteuses augmentant la complexité du système, ainsi que des mises à jour constantes et fastidieuses du pare-feu.

Heureusement, il existe une alternative offrant une expérience Office 365 rapide et stable.Pour y parvenir, voici ce que recommande Microsoft :

1. Identifier et différencier le trafic Office 365
2. Évacuer localement les connexions réseau
3. Évaluer le contournement des proxys
4. Évitez les réseaux en épingles

Par où commencer:

- **Routez le trafic Office 365** sur vos points d'accès locaux à Internet, conformément aux recommandations de Microsoft.
- **Appuyez-vous sur le seul fournisseur de sécurité cloud recommandé par Microsoft** pour offrir l'expérience utilisateur la plus rapide possible.
- **Rationalisez l'utilisation de la bande passante** pour donner au trafic Office 365 la priorité sur le trafic lié au divertissement.

EXEMPLE DE RÉUSSITE

KELLY SERVICES

Kelly Services a transformé son réseau pour permettre des connexions Internet rapides, sécurisées et directes dans 900 sites à travers le monde, offrant un accès rapide à Office 365 et à d'autres applications cloud. L'entreprise a réduit de 60% son budget MPLS, amélioré ses capacités d'inspection et simplifié considérablement la gestion des réseaux et des politiques.

« Avec Zscaler, il est possible de garantir à Office 365 30% de toute la bande passante, mais également de limiter son utilisation à au plus 50% de celle-ci, pour empêcher les transferts de fichiers OneDrive de congestionner le réseau. »

Darryl Staskowski
Vice-président directeur et DSI
Kelly Services

Simplifier l'intégration informatique en cas de fusions-acquisitions

La complexité des intégrations informatiques ralentit les fusions-acquisitions et perturbe les activités de l'entreprise. Vous devez gérer les risques liés à la suppression et à l'ajout d'utilisateurs tout en leur donnant accès aux applications dont ils ont besoin. À cette complexité s'ajoute la nécessité de normaliser la sécurité pendant que vous intégrez de nouvelles parties d'une entreprise ayant des normes de sécurité inférieures ou différentes. Cette opération nécessite une attention plus que particulière, car elle peut augmenter les risques de sécurité.

Il est toutefois possible de faire passer de plusieurs années à quelques semaines la durée des fusions-acquisitions ainsi que des activités qui y sont liées, et de minimiser les risques pour l'entreprise en offrant aux utilisateurs l'accès aux applications sans avoir à faire converger les infrastructures réseau.

Par où commencer:

- **Exploitez la technologie ZTNA (Zero Trust Network Access)** pour donner aux utilisateurs un accès immédiat aux applications sans avoir à leur donner accès au réseau.
- **Utilisez une approche progressive basée sur l'identité.** Commencez par les utilisateurs des deux entités travaillant sur les activités liées à la fusion-acquisition, et déterminez les applications auxquelles ils doivent accéder.
- **Étendez la liste des utilisateurs et des applications** à mesure que l'intégration évolue.

EXEMPLE DE RÉUSSITE

Une organisation de santé américaine classée au Fortune 500 a réduit de 9 mois son calendrier d'intégration en fournissant l'accès aux applications sans donner accès au réseau. Elle a ainsi permis une intégration sécurisée pour les entreprises nouvellement acquises ou fusionnées.
Cette approche a simplifié l'infrastructure de fusion-acquisition de l'organisation et facilité la tâche pour les équipes informatiques.

À propos de Zscaler™

Zscaler a été fondé en 2008 sur un concept simple mais puissant : à mesure que les applications migrent vers le cloud, la sécurité doit également s'y déplacer. Aujourd'hui, nous aidons des milliers d'entreprises mondiales à se porter vers des opérations basées sur le cloud.

Bibliothèque DSI

Pour plus de ressources essentielles par et pour les DSI, accédez à cette page Web:

www.zscaler.com/cio-insights

Ou contactez votre représentant commercial pour obtenir des références de pairs.

zscaler™

[1] Steve Riley, Neil MacDonald, Lawrence Orans, Guide du marché pour un accès réseau zéro trust, avril 2019

© 2019 Zscaler, Inc. Tous droits réservés. Zscaler™ est soit 1) une marque déposée ou marque de service, ou 2) une marque commerciale ou une marque de service de Zscaler, Inc. aux États-Unis et/ou dans d'autres pays. Toutes les autres marques sont la propriété de leurs propriétaires respectifs.