Sécuriser le travail à distance:

Maintenir la continuité de l'activité avec Zscaler

zscaler™

Puisque rien n'est plus important à l'heure actuelle que la protection de la santé des employés, les entreprises ont la responsabilité de faire leur part pour réduire le risque de propagation du coronavirus (COVID-19). En même temps, les organisations doivent assurer la continuité des activités et maintenir leur productivité, notamment lorsque les employés ne travaillent qu'à distance. Avoir subitement à gérer un effectif considérable de télétravailleurs est un réel défi pour les entreprises.

> C'est la preuve qu'investir dans une infrastructure axée sur le cloud est particulièrement rentable dans le cas des environnements de type VUCA (volatiles, incertains, complexes et ambigus).
>
> **Markus Sontheimer, CIO/CDO et membre du Conseil d'administration, DB Schenker**

Certaines organisations peuvent fonctionner avec l'ensemble de leurs responsables et de leur personnel travaillant à distance. Mais pour de nombreuses entreprises, assurer une connexion à distance à tous les employés (des centaines de milliers d'utilisateurs pour certaines) pourrait submerger non seulement l'équipe informatique, mais également les architectures de réseau qu'elle gère.

Les cybercriminels essaient également de profiter de la forte augmentation du travail à distance. De plus en plus de cyberattaques ciblant des personnes et des entreprises à travers le monde se basent sur le thème du coronavirus. De nombreux logiciels malveillants, ransomwares, bots, et autres pièges visant les nouveaux télétravailleurs et exploitant les risques de vulnérabilité (maintenant plus nombreux) ont vu le jour.

Les entreprises doivent reconnaître les impacts du passage au télétravail:

Bande passante

Les entreprises s'appuyant sur les sorties Internet basées sur le VPN pour prendre en charge le télétravail pourraient avoir de mauvaises surprises. La hausse exponentielle du trafic réseau lié à la collaboration vidéo pourrait saturer les connexions de sortie Internet existantes. Ajouter des connexions VPN entraînera la saturation de l'infrastructure.

Sécurité

La sécurité du télétravail doit être garantie. Comment la migration de l'ensemble du personnel vers le télétravail affectera-t-elle l'accès aux services et applications nécessaires ? La pile de sécurité de l'entreprise peut-elle efficacement gérer le pic de trafic ?

Expérience utilisateur

Les applications SaaS comme Office 365 nécessitent un routage optimisé : plus l'utilisateur doit effectuer de sauts de réseau, plus le ralentissement de la connectivité est important. Le problème s'aggrave lorsqu'un grand nombre d'utilisateurs distants doivent d'abord se connecter par VPN à un site central.

Coût

De quels logiciels, ressources informatiques et infrastructures supplémentaires aurons-nous besoin ? Combien coûteront ils ?

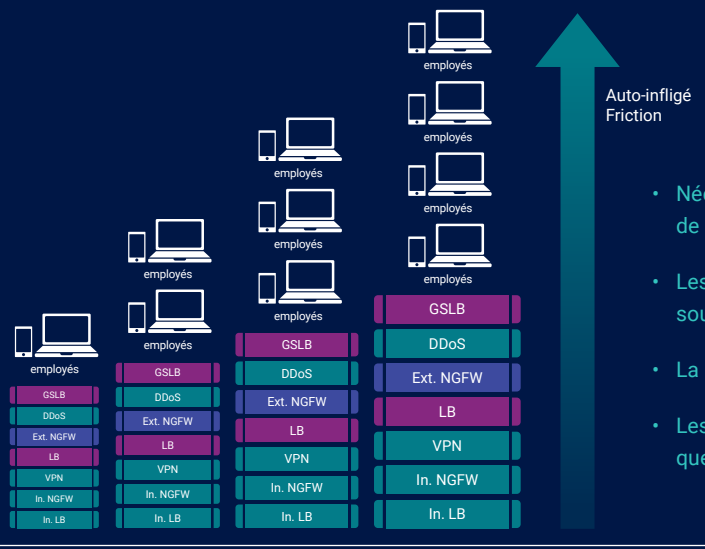
Temps

Étant donné que le déploiement de modèles opérationnels de télétravail peut prendre des mois ou des années, à quelle vitesse pouvez-vous assurer la migration vers le télétravail et quelle est votre stratégie ?

Cadre réglementaire

Dans les secteurs hautement réglementés, les règles de conformité ne seront pas nécessairement assouplies en temps de crise. Les nouveaux télétravailleurs pourraient par inadvertance accéder à des applications non autorisées et mettre l'entreprise en infraction.

Les défis liés au VPN augmentent avec la hausse du nombre de télétravailleurs



- Nécessite plus d'appliances en raison des contraintes de capacité
- Les licences pour situations d'urgence n'offrent qu'un soulagement limité
- La consommation de bande passante monte en flèche
- Les frais généraux opérationnels augmentent à mesure que l'expérience utilisateur se détériore

Figure 1. À mesure que le nombre d'utilisateurs et le trafic qu'ils génèrent sur les réseaux VPN augmentent, les réseaux d'entreprise sont mis à rude épreuve.

La technologie VPN repose sur des piles d'appliances de passerelle et sur une infrastructure (voir la figure 1 ci-dessus) ayant des contraintes de bande passante et de nombre de licences. Le modèle à point d'entrée unique du VPN présente également une surface d'attaque externe et impose des coûts de performance liés au backhauling du trafic de l'utilisateur vers des applications situées dans des environnements distribués.

Zscaler Internet Access (ZIA) et Zscaler Private Access (ZPA) permettent de réduire les difficultés liées au télétravail au moyen d'un service cloud conçu pour sécuriser l'accès aux applications SaaS, à Internet et aux applications privées.

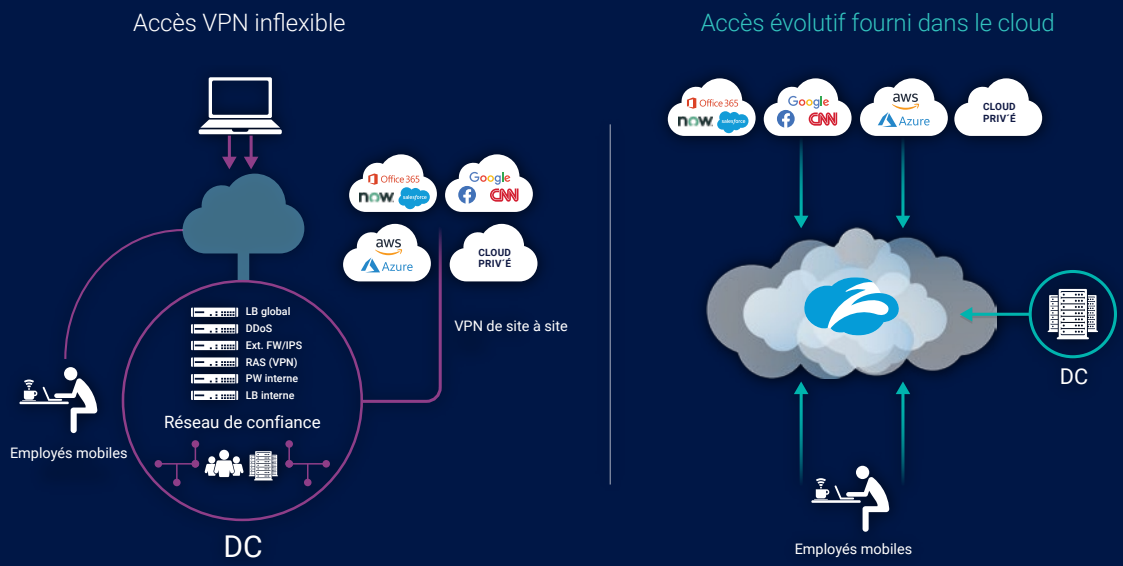


Figure 2. Le modèle d'accès par VPN coûteux, rigide et pas tout à fait sécurisé (à gauche) est facilement surchargé en cas de forte hausse du nombre d'accès distant. L'accès distant fourni dans le cloud comme celui de Zscaler (à droite) évolue pour s'adapter à la montée du télétravail.

Comment Zscaler permet un accès distant sécurisé

Objectifs stratégiques	Capacités stratégiques	Tactiques critiques	Utiliser Zscaler
Assurer la robustesse du réseau (par exemple, bande passante des circuits, mémoire ou ressources matérielles, etc.)	La bande passante, le matériel, la mémoire et bien d'autres ressources de l'entreprise doivent être capables d'évoluer de manière dynamique et durable. Elle doit également avoir une visibilité permettant de s'assurer que le trafic non essentiel est éliminé ou réduit au minimum.	Planifier le temps réseau des utilisateurs en fonction du fuseau horaire et de l'emplacement géographique. Hiérarchiser les rôles des utilisateurs afin de permettre aux personnes clés d'accéder au réseau en cas de besoin (cadres supérieurs, équipe informatique, service client).	Déployer ZIA et ZPA pour accéder directement aux applications et aux données sur Internet, ainsi qu'aux fournisseurs de cloud public. La politique de sécurité de l'entreprise est alors appliquée à tout le trafic sans avoir à recourir à un routage compliqué et tiré par les cheveux.
Créer une évolutivité flexible tout en minimisant les coûts de déploiement	Prendre en charge le plus rapidement possible une vaste communauté de télétravailleurs sans mettre à mal le personnel opérationnel.	Tirer parti de l'accès aux applications utilisant le cloud pour éliminer les goulots d'étranglement dans les appliances, les licences ou la distribution géographique.	Migrer les télétravailleurs vers la plate-forme cloud mondiale de Zscaler pour leur offrir un accès aux applications qui soit fiable, sécurisé et capable d'absorber des dizaines ou des centaines de milliers de nouveaux utilisateurs en quelques jours, et non en quelques semaines ou quelques mois.
Sécuriser l'accès des employés aux applications et aux données	Les télétravailleurs doivent avoir un accès à distance aux applications et aux données.	Développer des politiques et des règles de sécurité propres à l'entreprise et les appliquer aux télétravailleurs en fonction de leur identité, de leur poste, des exigences d'accès et de l'emplacement géographique.	Déployer ZPA et les connecteurs, et utilisez l'application Zscaler ou l'accès par navigateur pour connecter les utilisateurs aux applications autorisées suivant des stratégies personnalisées. Cette approche permet un accès sécurisé aux applications et aux données, tout en éliminant les connexions entrantes externes et en réduisant la surface d'attaque du réseau.
Sécuriser l'accès de tiers aux applications et aux données	Il est important que les sous-traitants, les consultants, les fournisseurs et les partenaires puissent accéder aux applications et aux données sans pour autant pénétrer votre réseau.	Permettre à des tiers d'accéder uniquement aux applications autorisées. Empêcher la connectivité réseau réduit au minimum la possibilité de déplacement latéral.	Utiliser l'accès par navigateur à ZPA pour permettre un contrôle granulaire et donner une visibilité aux utilisateurs tiers. Aucune installation de logiciel requise.
Maintenir un accès fluide aux applications privées du data center et du multi-cloud	Les utilisateurs ont besoin d'accéder aux applications dans une variété d'environnements back-end sans avoir à effectuer de backhauling coûteux.	Offrir simultanément une connectivité dynamique, sécurisée et directe aux applications hébergées sur plusieurs sites.	Déployer des connecteurs ZPA sur plusieurs environnements d'application back-end. La sélection dynamique des chemins garantit à tous les télétravailleurs, où qu'ils soient, un accès fluide et ultra-rapide.
Protéger les appareils des télétravailleurs	Les entreprises doivent protéger les appareils des télétravailleurs lorsqu'ils se trouvent en dehors du système de sécurité de l'organisation.	Développer des stratégies spécifiques au type d'accès, et les appliquer aux terminaux en fonction de la situation.	Déployer l'application Zscaler sur tous les terminaux via Push, un portail Self Service, l'App Store ou le Play Store. Utiliser ZIA pour appliquer une politique à ces déploiements d'applications Zscaler et assurer des protections conformes aux niveaux de tolérance de risque.
Utiliser le déchiffrement SSL pour tout le trafic sortant	Examiner tout le trafic en direction des applications Internet et SaaS pour vous assurer que les politiques ainsi que l'analyse, la détection, et la prise en charge des menaces sont bien appliquées pour déceler les risques et empêcher toute infiltration.	Déterminer si toutes les catégories de trafic doivent être examinées, ou si votre profil de risque permet des exclusions (telles que la conformité avec la norme PCI DSS et la loi HIPAA).	Permettre à ZIA d'effectuer des déchiffrements SSL sur tous les sites et terminaux à l'aide de certificats Zscaler (pour accélérer le déploiement).
Détecter les fichiers malveillants	Les employés devront très probablement échanger un grand nombre de fichiers entre eux ou avec des tiers.	En fonction du risque, déterminer pour chaque site quels autres types de fichiers doivent être mis en Sandbox , et décider en tenant compte des capacités de l'entreprise.	Utiliser ZIA pour activer une règle de nettoyage « any-any » pour les types de fichiers les plus à risque et définir les types de fichiers à mettre en quarantaine.
Empêcher la fuite des données critiques de l'entreprise	Les entreprises devront continuer de veiller à ce qu'il n'y ait pas de fuite des données critiques.	Affiner les règles de prévention contre la perte de données (DLP) et mettre en œuvre la fonctionnalité Exact Data Match pour restreindre encore plus efficacement le mouvement des données critiques.	Utiliser des règles DLP ZIA prédéfinies et/ou personnalisées pour détecter les données sensibles dans le trafic.

Une bonne planification et des initiatives appropriées permettront aux entreprises affectées par l'épidémie de COVID-19 d'assurer la sécurité de leurs employés tout en travaillant à leurs objectifs stratégiques cruciaux. La plate-forme cloud Secure Access Service Edge de Zscaler été conçue spécifiquement pour permettre une connectivité directe via des points d'accès Internet locaux, garantissant que les entreprises (ainsi que tous leurs télétravailleurs) restent opérationnelles en périodes de crise.

Pour vous aider en cette période particulière, Zscaler a mis sur pieds le **Business Continuity Program** (programme de continuité d'activité) visant à aider les organisations à assurer la sécurité des employés et à maintenir la productivité de l'entreprise.

Sécurisez vos télétravailleurs dès aujourd'hui

zscaler™

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'organisations mondiales à se porter vers des opérations basées sur le cloud.