Repenser la sécurité pour un personnel en évolution

Les équipes informatiques se trouvent dans une position peu enviable d'essayer de sécuriser des employés travaillant depuis n'importe quel endroit - le siège, une filiale, la maison, bref partout à la fois. Et comme les VPN ont du mal à suivre à la fois un personnel plus grand qui travaille à distance et des utilisateurs se connectant directement à leurs applications cloud, de plus en plus d'entreprises s'éloignent des politiques et des contrôles de sécurité. Voila qui attire l'attention des cybercriminels qui concentrent leurs attaques sur la main-d'œuvre à distance en pleine expansion. Oui, votre entreprise est en danger et donc en quête d'une solution simple et efficace pour relever ces défis de sécurité.

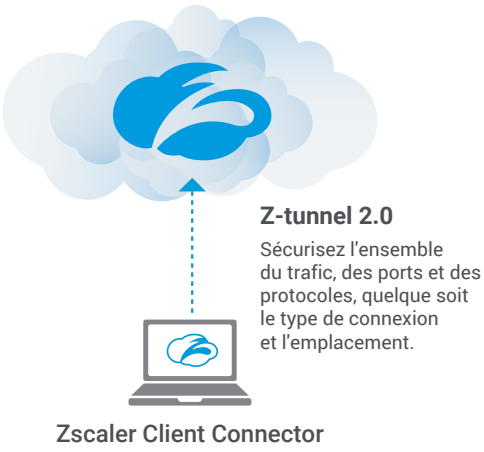
En exploitant la puissance et la flexibilité de Zscaler Internet Access™ (ZIA™), les entreprises peuvent complètement sécuriser leur personnel en évolution, qu'importe le lieu et la manière dont elles font opèrent. Avec Cloud Firewall, Cloud Sandbox, et Cloud DLP, qui suivent la connexion de l'utilisateur, les équipes informatiques peuvent assurer des connexions Internet directes, rapides et sans risque supplémentaire. Vous bénéficierez d'une protection étanche contre les failles et vols de données tout en donnant à vos utilisateurs la liberté de travailler où et comme ils le souhaitent. Tout cela pour une fraction de ce que coûtent des approches traditionnelles.

Vos utilisateurs ont besoin de plus de flexibilité pour travailler n'importe où et comme ils le souhaitent. Le problème toutefois est que les menaces visant vos utilisateurs augmentent à mesure qu'ils quittent votre réseau et ignorent vos politiques. Votre réseau et votre sécurité coûtent plus qu'ils ne servent. Il est temps d'adopter une meilleure approche par rapport à l'avenir de la connectivité.

Comment sécuriser votre personnel distant, où qu'il se trouve

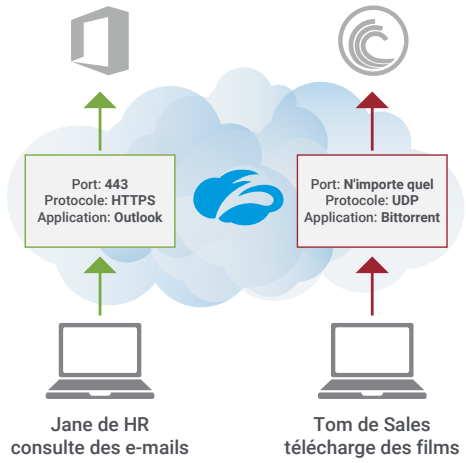
Tout commence avec Zscaler Client Connector et Z-tunnel 2.0

D'abord Zscaler Client Connector (autrefois appelé Zscaler App). Avant que l'appareil de l'utilisateur ne se connecte à Internet, le Client Connector établit une connexion sécurisée avec le cloud de Zscaler. En exploitant la nouvelle architecture Z-tunnel 2.0 de Zscaler, l'ensemble du trafic, des ports et des protocoles est envoyé à travers Zscaler pour inspection. Le Client Connector est la pierre angulaire des connexions rapides et sécurisées des utilisateurs, où qu'ils soient.



Contrôler les connexions hors réseau avec Advanced Cloud Firewall

Même lorsque vos utilisateurs sont hors réseau, il reste capital que vos politiques d'entreprise les suivent. C'est ici qu' Advanced Cloud Firewall entre en jeu. En associant Advanced Cloud Firewall à Z-tunnel 2.0, vous pouvez contrôler et sécuriser entièrement les connexions de vos utilisateurs et réduire les risques sans besoin de VPN, de backhauling ou d'appliances coûteuses. Du blocage de BitTorrent au contrôle des connexions FTP, RDP ou SIP, en passant par la définition de l'accès des groupes d'utilisateurs à Ring Central, Zoom et autres, Zscaler Advanced Cloud Firewall garantit votre sécurité. Vous pouvez enfin tirer profit d'une politique unique et cohérente partout où vos utilisateurs veulent se connecter. Profitez-en aujourd'hui et à l'avenir.

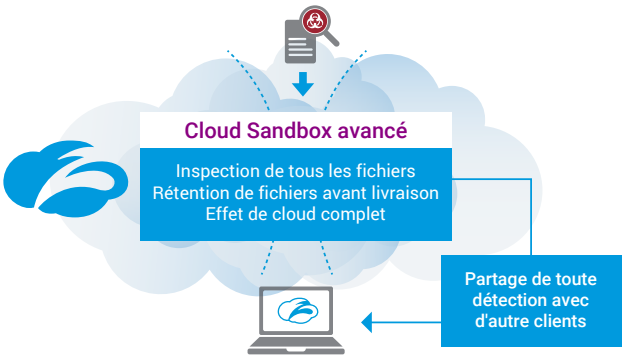


Appliquez les politiques d'entreprise hors réseau grâce à Cloud Firewall

> Nous avions décelé un énorme trafic P2P entrant et sortant de notre réseau vers des clients que nous ne connaissions pas. Grâce au firewall d'inspection systématique de paquets de Zscaler nous avons pu couper ce trafic P2P, et ainsi arrêter BitTorrent et d'autres services de partage de fichiers P2P".
>
> **- Jeff Johnson, directeur des opérations de sécurité, AutoNation**

Réduire les risques des utilisateurs distants grâce à Advanced Cloud Sandbox

Les utilisateurs sont le plus vulnérables quand ils sont hors réseau et éloignés de votre passerelle. Les ransomwares et les fichiers malveillants inconnus frappent au moment où vous vous y attendez le moins. C'est pourquoi vous avez besoin d'un "Cloud Sandbox" avancé et de l'architecture de proxy ZIA. Vous pouvez couvrir tous les utilisateurs avec la protection en ligne dite "zero-day" et même suspendre la livraison de fichiers inconnus jusqu'à confirmation qu'ils sont inoffensifs. Vous bénéficiez d'une couverture totale de tous les types de fichiers que vos utilisateurs pourraient télécharger et de renseignements plus solides sur les menaces provenant d'autres organisations de Zscaler. Mieux encore, l'inspection SSL illimitée examine chaque octet de trafic et décèle davantage de menaces où qu'elles se cachent.



Après le déploiement de Zscaler et de Cloud Sandbox, NOV a vu réduit de 35 fois son nombre de machines infectées.

Contrôler l'exfiltration des données en tout lieu avec Cloud DLP

Vos utilisateurs doivent peut-être quitter le réseau, mais pas nécessairement avec vos données sensibles. Avec Cloud DLP de Zscaler, vous pouvez empêcher la perte intentionnelle ou non de données confidentielles, quel que soit le lieu de connexion de vos utilisateurs. Grâce à son inspection SSL complète, vous éliminerez les points aveugles de votre trafic crypté et obtiendrez un meilleure rendement dans vos efforts de conformité. De plus, avec Exact Data Match de Zscaler, vous pouvez prendre des empreintes digitales et les faire correspondre des informations d'identification personnelle (PII) pour une protection en béton contre l'exfiltration.

Sécuriser toutes les données confidentielles, quelle que soit la connexion, et dans le trafic SSL

> Les dictionnaires DLP prêts à l'emploi sont incroyablement simples, correspondant exactement à ce dont nous avions besoin. Les déployer auprès des groupes d'utilisateurs a été si facile que le déploiement complet de DLP est devenu un jeu d'enfant".
>
> **- Brad Moldenhauer Directeur de la sécurité de l'information, Steptoe &Johnson LLP**

Résumé

Les événements récents nous l'ont bien appris, les organisations doivent se préparer à une foule de possibilités, y compris voir l'ensemble de votre personnel travailler en dehors du siège social. Mais migrer hors du bureau signifie également que l'on s'éloigne des politiques et des contrôles de sécurité qui s'y trouvent. Il est impératif que les organisations disposent d'un nouveau moyen de sécuriser leurs employés et leurs applications, quel que soit leur lieu de travail et sans que l'expérience utilisateur en pâtisse.

Zscaler a déjà aidé des milliers d'organisations à sécuriser cette nouvelle réalité qu'est le télétravail. Laissez-nous vous montrer comment vous pouvez obtenir la flexibilité nécessaire pour renforcer les capacités du personnel d'aujourd'hui et de l'avenir.

A propos de Zscaler

Zscaler permet aux plus grandes organisations internationales d'adapter en toute sécurité leurs réseaux et leurs applications à un monde résolument tourné vers le mobile et le cloud. Ses services phares que sont Zscaler Internet Access™ et Zscaler Private Access™, créent des connexions rapides et sécurisées entre les utilisateurs et les applications, et ce quels que soient l'appareil, l'emplacement ou le réseau. Les services Zscaler sont à 100% fournis dans le cloud et offrent la simplicité, une sécurité renforcée ainsi qu'une amélioration de l'expérience utilisateur inégalables par les appliances traditionnelles ou les solutions hybrides. Adopté dans plus de 185 pays, Zscaler gère une plate-forme multi-entité de sécurité cloud distribuée qui protège des milliers de clients contre les cyberattaques et les pertes de données. Pour en savoir plus, accédez à zscaler.com ou suivez nous sur Twitter @zscaler.

Zscaler, Inc.
120 Holger Way
San José, Californie
+1 408 533 0288
www.zscaler.com