E-book

Quatre conditions pour une filiale Zero Trust

En mettant en œuvre une approche Zero Trust au niveau d'une filiale, les entreprises peuvent non seulement renforcer leurs réseaux contre les menaces, mais aussi rationaliser la connectivité pour les utilisateurs, les appareils et les applications sur différents sites.

Dans le paysage commercial dynamique actuel, de nombreuses entreprises sont confrontées à des difficultés pour assurer la sécurité de leurs utilisateurs, de leurs appareils et de leurs applications. Dans le passé, lorsque les applications étaient hébergées dans des data centers et que les utilisateurs se connectaient principalement à partir des bureaux, les exigences en matière de connectivité étaient relativement simples. Les architectures traditionnelles en étoile et basées sur un pare-feu répondaient efficacement à ces besoins. Cependant, compte tenu de l'évolution de l'environnement de travail moderne, ces approches traditionnelles peinent désormais à assurer une protection adéquate contre les menaces et une expérience utilisateur optimale.

Les utilisateurs ne se connectent désormais plus exclusivement depuis leur bureau, mais depuis une multitude d'emplacements, notamment leur domicile, des cafés, des aéroports, etc. De plus, la prolifération de l'Internet des objets (IoT) complique encore davantage le paysage de la sécurité des entreprises, car les dispositifs IoT/OT posent des risques de sécurité supplémentaires.

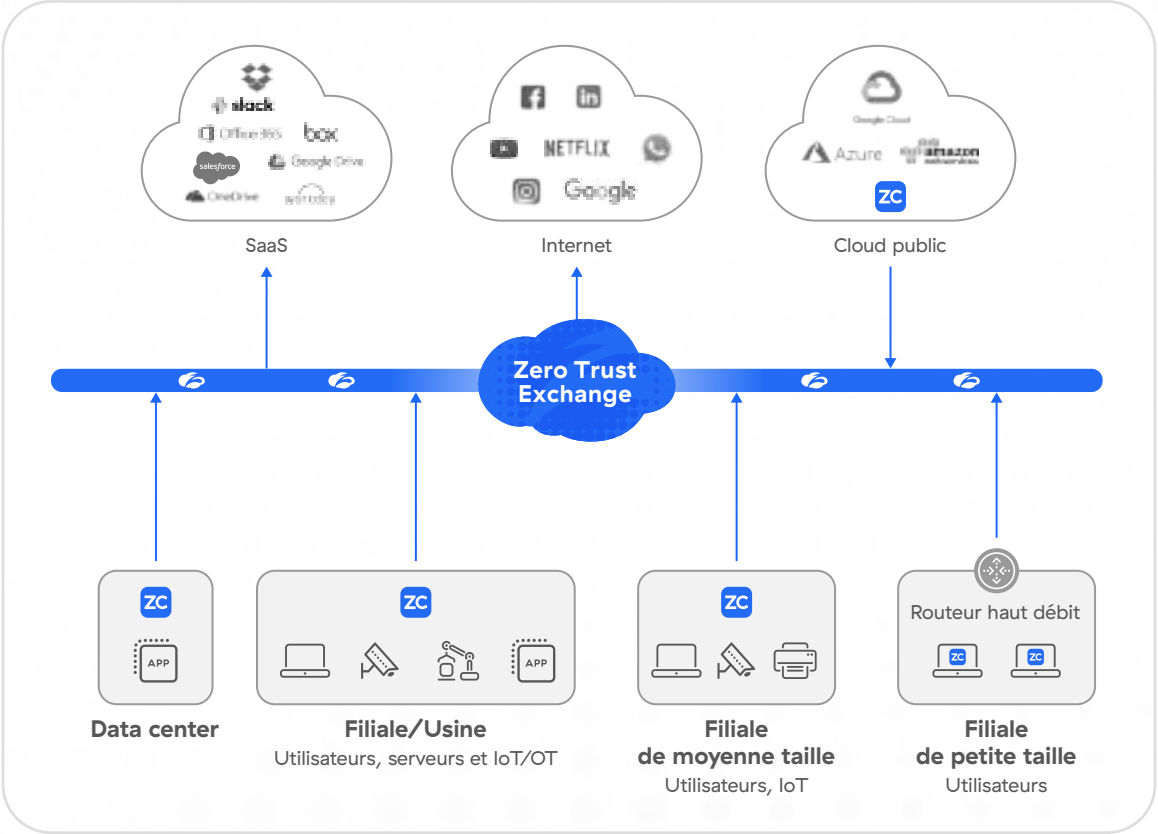

Illustration 1 : Zero Trust Branch propose une approche de la connectivité réseau fondée sur la notion de Zero Trust.

L'évolution du paysage pousse les entreprises à adopter une approche Zero Trust de la sécurité. Les principes de Zero Trust (ne jamais faire confiance, toujours vérifier et appliquer l'accès sur la base du moindre privilège) ont permis à de nombreuses entreprises de déjouer des cyberattaques sophistiquées. Avec Zero Trust, les utilisateurs n'ont accès qu'aux applications dont ils ont besoin, contrairement aux VPN qui mettent les utilisateurs sur le réseau et leur accordent un accès illimité. En appliquant les principes de Zero Trust à la connectivité réseau, les entreprises peuvent mieux se protéger contre les menaces, en particulier celles provenant de leurs sites. La mise en œuvre d'une approche Zero Trust au niveau d'une filiale garantit une connectivité sécurisée et la simplification des opérations, et permet de surmonter les complexités de routage ou une détérioration de l'expérience utilisateur tout en éliminant la surface d'attaque et en empêchant les déplacements latéraux des menaces.

Une architecture d'une filiale Zero Trust garantit un renforcement de la sécurité pour tous les sites, y compris les filiales, les usines, les kiosques et les data centers. Voici quatre conditions essentielles pour garantir une architecture d'une filiale Zero Trust :

Assurer les principes de Zero Trust pour votre réseau 1

Sécuriser les dispositifs IoT/OT de vos sites distants 2

Garantir des chemins directs vers le cloud pour le trafic SaaS/ Internet 3

Assurer une expérience utilisateur cohérente pour les employés au bureau et distants 4

Le SD-WAN traditionnel n'est pas le Zero Trust

Les appliances SD-WAN traditionnelles ne font qu'étendre le réseau de l'entreprise vers les sites distants, élargissant ainsi la surface d'attaque de l'entreprise. Elles n'offrent qu'une faible protection contre le mouvement latéral des menaces, permettant aux appareils compromis sur les sites distants de communiquer avec les applications critiques de l'entreprise dans le data center ou le cloud public. Les entreprises sont davantage exposées au risque de déplacement latéral des menaces et d'attaques basées sur Internet lié à l'utilisation d'un SD-WAN traditionnel.
Une mosaïque d'appareils de sécurité, d'outils et de politiques non standard entraînent un accroissement du risque de sécurité en raison de lacunes connues et inconnues dans la couverture de sécurité. Par conséquent, lors de la conception d'une architecture de connectivité sécurisée pour les sites distants, il devient impératif de privilégier la mise en œuvre de Zero Trust afin de réduire la surface d'attaque et d'empêcher le déplacement latéral des menaces.

Un rapport sur les risques liés aux VPN réalisé en 2023 par Cybersecurity Insiders qui a interrogé 382 professionnels de l'informatique et experts en cybersécurité a révélé que les VPN posent des risques de sécurité, 88 % des entreprises se disant légèrement à extrêmement préoccupées par le fait que les VPN puissent mettre en péril la sécurité de leur entreprise.

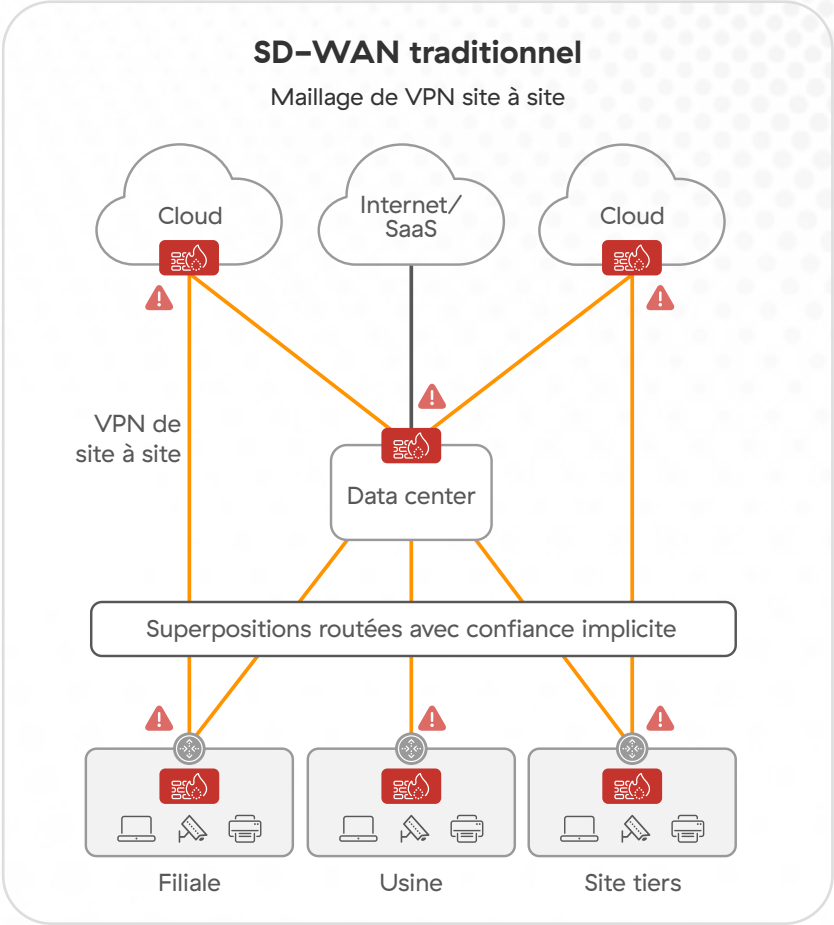

Illustration 2 : Les SD-WAN traditionnels élargissent la surface d'attaque et ne protègent pas contre les déplacements latéraux des menaces.

En outre, 45 % des entreprises ont confirmé avoir subi au moins une attaque exploitant les vulnérabilités du VPN au cours des 12 derniers mois, une sur trois ayant été victime d'attaques de ransomware liées au VPN. La menace croissante de cyberattaques exploitant les vulnérabilités liées aux VPN souligne l'urgence de reconsidérer la sécurité des architectures actuelles.

Au cours des 12 derniers mois, votre entreprise a-t-elle été victime d'une attaque exploitant les failles de sécurité de vos serveurs VPN ?

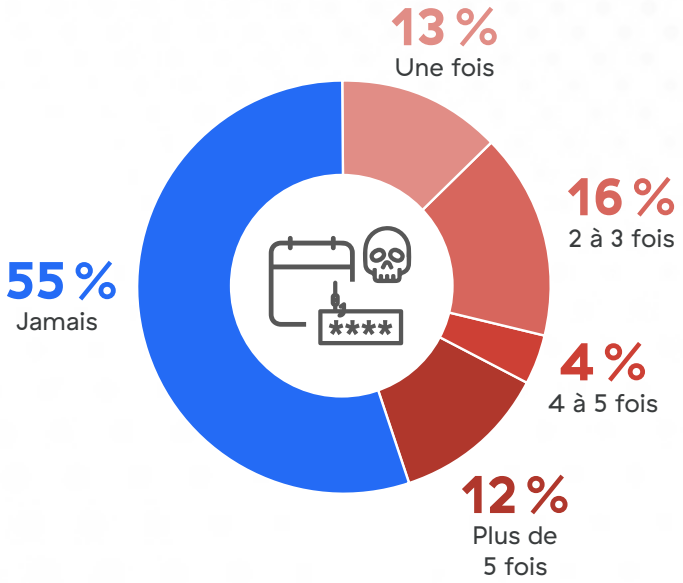

Illustration 3 : Les entreprises sont confrontées à une augmentation des cyberattaques en raison des vulnérabilités des serveurs VPN.

Vous ne pouvez instaurer une stratégie Zero Trust avec des pare-feux et des VPN

Traditionnellement, les entreprises déployaient des VPN site à site pour garantir la connectivité aux applications critiques hébergées dans le data center. Cependant, à mesure que ces applications migrent vers le cloud, l'architecture VPN site à site conventionnelle devient moins viable puisque le trafic est toujours soumis à un backhauling vers le data center, ce qui entraîne une dégradation de l'expérience utilisateur et des problèmes de performances.

Les réseaux traditionnels introduisent également une complexité opérationnelle, car les tunnels VPN exigent une gestion et une configuration du site sur une base individuelle. Par conséquent, les équipes informatiques des entreprises souhaitent passer d'un réseau en étoile à une architecture directe vers le cloud qui envoie le trafic des applications à un fournisseur de sécurité cloud, améliorant ainsi les performances des applications.

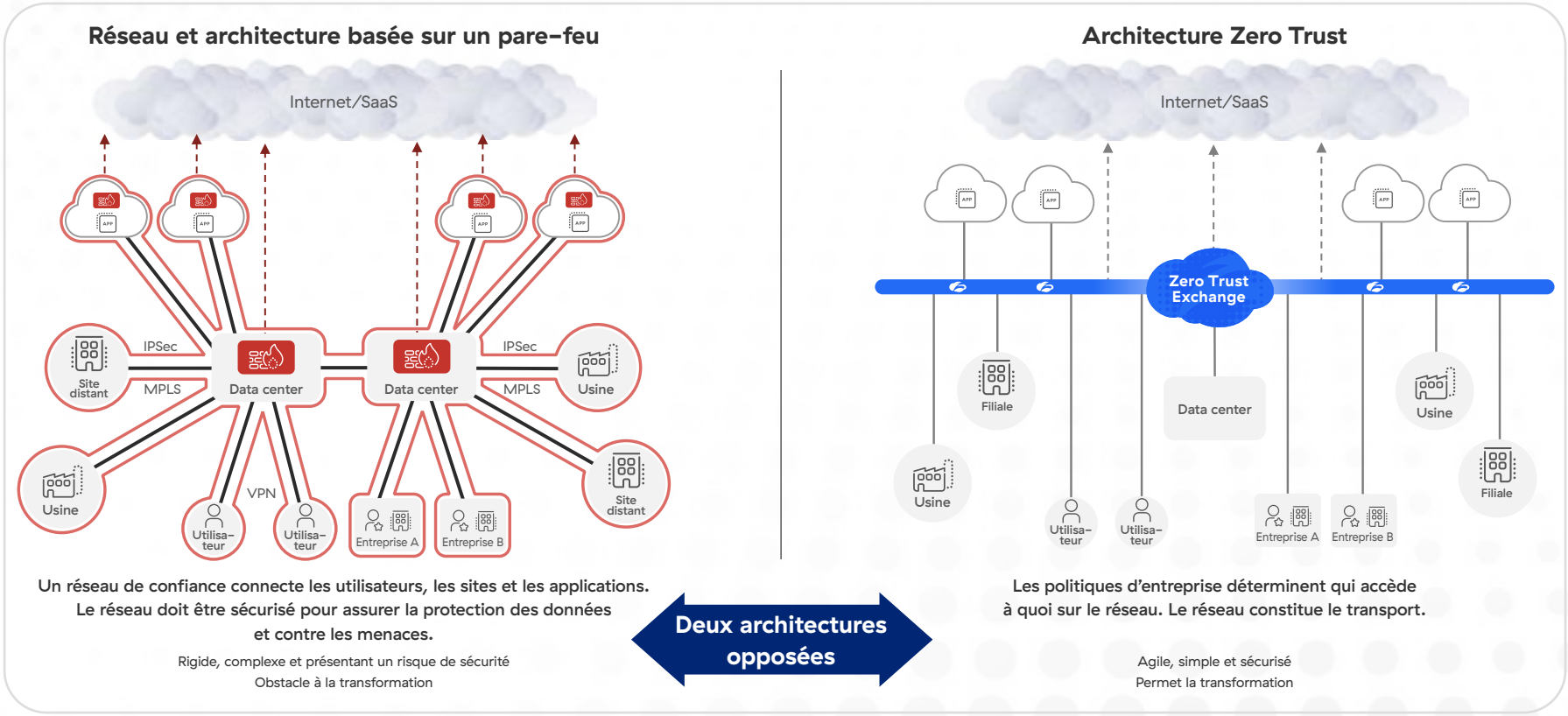

Illustration 4 : Les entreprises sont confrontées à une augmentation des cyberattaques en raison des vulnérabilités des serveurs VPN.

Quatre conditions clés pour garantir un site distant Zero Trust

1 Assurer les principes de Zero Trust pour votre réseau

Les VPN de site à site étendent votre réseau d'entreprise aux sites distants, data centers, régions cloud et tiers. Les réseaux traditionnels étendent votre surface d'attaque aux entités échappant à votre contrôle direct et autorisent implicitement les flux de trafic, ce qui permet le déplacement latéral des menaces. Contrairement à la segmentation traditionnelle du réseau, qui divise le réseau en zones et est complexe à gérer, la segmentation utilisateur–application et appareil–application fournit un accès granulaire et contextuel uniquement lorsqu'il est autorisé. Un réseau fondé sur les principes de Zero Trust élimine les risques inhérents aux réseaux plats traditionnels et vous aide à éviter la complexité de la superposition de pare–feu dans le cadre des contrôles de sécurité. Les réseaux traditionnels introduisent également une complexité opérationnelle, car les tunnels VPN exigent une gestion et une configuration du site sur une base individuelle. Par conséquent, les équipes informatiques des entreprises souhaitent passer d'un réseau en étoile à une architecture directe vers le cloud qui envoie le trafic des applications à un fournisseur de sécurité cloud, améliorant ainsi les performances des applications.

2 Sécuriser les dispositifs IoT/OT de vos sites distants

Les dispositifs IoT/OT prolifèrent dans presque toutes les entreprises avec l'essor des objets « intelligents » tels que les imprimantes, les téléviseurs, les appareils photo, les lecteurs de cartes et les capteurs. Ces appareils exécutent une multitude de systèmes d'exploitation qui présentent des risques de sécurité divers, et la gestion des correctifs reste un défi en soi.
De nombreux responsables informatiques n'ont aucune visibilité sur ces dispositifs, encore moins un inventaire détaillé.
Pourtant, ces dispositifs ont souvent un accès illimité aux applications critiques de vos data centers et services cloud.
Les attaques basées sur des malwares ciblant l'IoT ayant augmenté de 400 %[1], ce type de dispositifs représente un vecteur de menace important pour votre entreprise. Les entreprises doivent sécuriser les dispositifs IoT/OT dans les sites distants ou les usines afin de protéger leurs opérations commerciales.

Les attaques de malwares basés sur l'IoT et l'OT ont augmenté de 400 % depuis 2022, ce qui en fait un vecteur de menace significatif.

3 Garantir des chemins directs vers le cloud pour le trafic SaaS/Internet

L'architecture directe vers le cloud connecte rapidement n'importe quel utilisateur ou dispositif IoT/OT à n'importe quelle application, où que cet utilisateur ou dispositif IoT/OT se trouve dans le monde. Le déploiement de chemins directs vers le cloud pour le trafic SaaS et Internet est crucial pour optimiser les performances du réseau et garantir une connectivité homogène. Les architectures en étoile qui effectuent le backhauling du trafic vers un data center via des liaisons MPLS coûteuses dégradent les performances des applications et entravent la productivité de l'entreprise. Lorsque les applications étaient hébergées dans le data center, il était logique d'effectuer le backhauling du trafic applicatif vers un hub régional. Cependant, avec la migration des applications vers le cloud, il est plus judicieux d'envoyer le trafic des utilisateurs ou des dispositifs IoT/OT directement à leur destination. Une architecture directe vers le cloud permet aux applications SaaS et au trafic Internet d'emprunter les chemins les plus efficaces et les plus directs vers leurs destinations. Cela présente de nombreux avantages, notamment la réduction des coûts, l'amélioration de l'expérience utilisateur et la simplification du réseau.

Les chefs d'entreprise souhaitent désormais que leurs utilisateurs et leurs équipes informatiques bénéficient d'une expérience de type café qui rend la connexion aux applications professionnelles aussi simple que possible, tout en offrant des performances applicatives optimales.

4 Assurer une expérience utilisateur cohérente pour les employés au bureau et distants

De nombreux employés travaillent à distance ou partagent leur temps entre le travail à domicile et au bureau. Cette évolution de la dynamique de travail a mis en lumière un défi de taille. En effet, les utilisateurs se disent souvent insatisfaits de la qualité de la connectivité au bureau par rapport à leur environnement de travail à domicile. Cette situation pose de nouveaux problèmes aux équipes informatiques. Les technologies VPN qui effectuent le backhauling du trafic vers un data center engendrent une expérience utilisateur incohérente et de mauvaise qualité, ce qui a un impact négatif sur l'activité et limite la productivité.

Les chefs d'entreprise souhaitent désormais que leurs utilisateurs et leurs équipes informatiques bénéficient d'une expérience de type café qui rende la connexion aux applications professionnelles aussi simple que possible, tout en offrant des performances applicatives optimales. Ils veulent que les utilisateurs professionnels puissent accéder aux applications dont ils ont besoin en bénéficiant d'une expérience uniforme entre le domicile et le bureau et avec la même facilité d'utilisation, ce qui est impossible dans le cadre d'une connexion aux réseaux par le biais de VPN. Pour demeurer pertinentes sur le marché concurrentiel d'aujourd'hui, les entreprises doivent garantir des expériences utilisateur cohérentes pour les employés au bureau et distants afin d'améliorer la productivité des collaborateurs et de stimuler leur créativité.

Application des principes Zero Trust au SASE

Le SASE (Secure Access Service Edge) intègre des services de mise en réseau et de sécurité dans une solution unifiée fournie dans le cloud, rationalisant les opérations, réduisant la complexité et permettant aux entreprises d'appliquer des politiques cohérentes sur leurs réseaux. Le SASE combine un réseau Zero Trust avec des services de sécurité essentiels fournis dans le cloud tels que SWG, CASB, FWaaS et ZTNA. Il est crucial de comprendre que les solutions SASE construites sur un SD-WAN traditionnel offrent une protection inadéquate, qui augmentent la surface d'attaque de l'entreprise et exposent les applications critiques à diverses menaces provenant d'Internet.

En outre, la segmentation du SD-WAN traditionnel est fragmentée et à faible précision, ce qui permet aux menaces de se propager facilement à d'autres systèmes, posant ainsi le risque d'interrompre les activités de sites ou de réseaux entiers.

Le groupe ESG (Enterprise Strategy Group) de TechTarget a enquêté auprès de 390 professionnels de l'informatique et de la cybersécurité dans diverses entreprises d'Amérique du Nord (États-Unis et Canada) pour comprendre l'état du SASE. Selon cette enquête, les trois principaux cas d'utilisation qui poussent les organisations vers le SASE sont :

1. Alignement des politiques de réseau et de sécurité
2. Réduction ou élimination de la surface d'attaque sur Internet
3. Amélioration de la sécurité des utilisateurs distants

Les trois cas d'utilisation du SASE soulignent l'importance de fournir une connectivité sécurisée pour les utilisateurs, les appareils et les applications dans l'établissement d'un cadre SASE résilient. Les entreprises qui décident de déployer le SASE doivent privilégier les solutions qui adhèrent aux principes de Zero Trust. Les SD-WAN traditionnels connectent divers sites via des VPN site à site ou des superpositions routées, établissant une confiance implicite qui accorde un accès illimité aux ressources critiques de l'entreprise, même pour les entités compromises. En revanche, les SD-WAN construits sur les principes de Zero Trust réduisent réellement la surface d'attaque et protègent les entreprises contre le déplacement latéral des menaces tout en facilitant la communication sécurisée d'utilisateur à application, d'appareil à application et d'application à application.

Illustration 5 : Les entreprises sont confrontées à une augmentation des cyberattaques en raison des vulnérabilités des serveurs VPN.

Conclusion

Les architectures traditionnelles de réseaux des filiales reposent sur une confiance implicite, qui étend la surface d'attaque à la filiale la plus éloignée et permet aux cybermenaces de se déplacer latéralement dans l'ensemble de l'entreprise. En adoptant une approche Zero Trust au niveau d'une filiale, les entreprises peuvent renforcer leurs réseaux contre les menaces et rationaliser la connectivité pour les utilisateurs, les dispositifs IoT/OT et les applications sur différents sites. La conception d'un réseau de filiale selon des principes Zero Trust améliore la sécurité de l'entreprise en éliminant la surface d'attaque et en empêchant le déplacement latéral des menaces tout en surmontant les complexités du routage. Il est important que les entreprises examinent attentivement les quatre exigences décrites ici lorsqu'elles mettent en œuvre les principes Zero Trust dans une filiale afin de répondre efficacement aux exigences complexes et en constante évolution de la sécurité et de la connectivité réseau.

Références :

1. zscaler.fr/press/zscaler-threatlabz-finds-400-increase-iot-and-ot-malware-attacks-year-over-year-underscoring
2. info.zscaler.com/2023-vpn-risk-report-fr
3. zscaler.fr/resources/industry-reports/esg-sse-leads-the-way-to-sase.pdf

À propos de Zscaler

Zscaler (NASDAQ : ZS) accélère la transformation digitale et permet à ses clients de gagner en agilité, productivité, résilience et sécurité. La plateforme Zscaler Zero Trust Exchange protège des milliers de clients contre les cyberattaques et les pertes des données, en connectant de manière sécurisée les utilisateurs, les dispositifs et les applications, quel que soit leur emplacement. Distribué dans plus de 150 data centers dans le monde, Zero Trust Exchange, basé sur SSE, constitue la plus grande plateforme de sécurité cloud inline au monde. Pour en savoir plus, rendez-vous sur **zscaler.fr** ou suivez-nous sur Twitter **@zscaler**.

+1 408 533 0288

Zscaler, Inc. (siège) • 120 Holger Way • San Jose, CA 95134

zscaler.fr