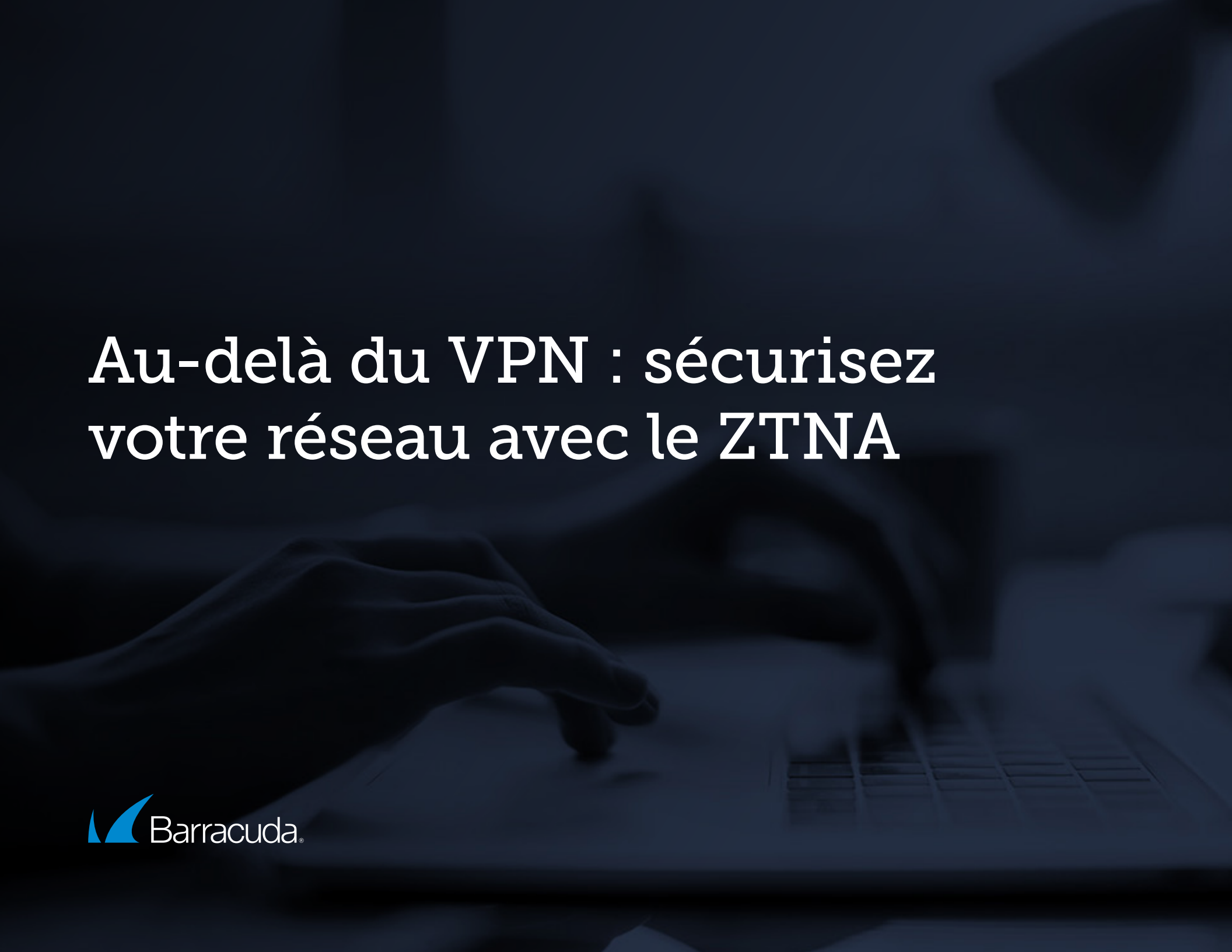
Au-delà du VPN : sécurisez votre réseau avec le ZTNA



Barracuda

L'évolution des VPN

Depuis l'avènement d'Internet et l'essor de l'accès aux informations et aux appareils, les professionnels de la sécurité s'efforcent de protéger les appareils et les utilisateurs connectés contre un nombre croissant d'acteurs malveillants. Le Virtual Private Network (VPN) a été créé en 1996 dans ce but précis, c'est-à-dire pour sécuriser la connexion entre l'appareil d'un utilisateur et le Web. Surtout utilisés par les entreprises au début, les VPN ont peu à peu conquis les particuliers, soucieux de la confidentialité et de la sécurité de leurs données. Dans un contexte professionnel, ces deux exemples d'utilisation sont d'une importance cruciale.

Les entreprises utilisent des VPN pour fournir un accès sécurisé à leurs réseaux depuis des décennies, tendance qui s'est nettement amplifiée depuis la pandémie et l'essor du télétravail. Une étude réalisée en 2021 par Coupon Follow a révélé qu'au cours du seul mois de mars 2020, l'utilisation des VPN avait connu une augmentation de 142 % par rapport au mois précédent. De très nombreux employés utilisant leurs propres ordinateurs en raison des politiques « Bring-your-own-device » rendues nécessaires par l'inaccessibilité des bureaux ont en effet eu besoin de protocoles de sécurité rapides et faciles à mettre en œuvre pour protéger leurs connexions aux réseaux des entreprises.

Les VPN ne suffisent plus à sécuriser les connexions réseaux

Bien qu'ils aient permis de résoudre cet écueil dans une situation de crise, les VPN ne sont plus la solution optimale pour protéger les entreprises contre le risque de violation des données. Comme l'a dit Mike Vizard du groupe Techstrong : « Il ne fait aucun doute que les VPN ont joué un rôle essentiel en permettant aux employés de travailler depuis leur domicile pendant la pandémie. Mais le moment est simplement venu de passer à une architecture réseau plus souple, et plus sûre ». La National Security Agency a également publié un avertissement à l'attention des organisations qui utilisent des VPN : à moins d'être correctement sécurisés, ces derniers sont vulnérables aux scans réseaux, aux attaques par force brute et aux vulnérabilités Zero-day.

Les experts en cybersécurité s'accordent à dire qu'il est temps de passer à autre chose, même si les VPN ont été utiles par le passé. Outre les risques relatifs à la sécurité, ils ne répondent souvent pas aux exigences de conformité, peuvent exposer les réseaux s'ils ne sont pas correctement configurés et ont tendance à être lents lorsqu'ils sont saturés, ce qui peut affecter l'expérience utilisateur. Mais quelle est la prochaine étape pour sécuriser l'activité en ligne des entreprises, notamment suite à l'expansion du télétravail et à son impact considérable sur l'environnement professionnel ?

Passer à l'accès réseau Zero Trust

La solution au problème des VPN réside dans l'accès réseau Zero Trust (ZTNA). Il ne s'agit pas d'un produit ou d'une solution unique ; c'est une philosophie qui s'intéresse à l'accès accordé aux différents utilisateurs. Nous y reviendrons bientôt. La philosophie Zero Trust est un principe du Secure Access Service Edge (SASE), que Gartner définit comme suit :

« Un nouvel ensemble de technologies comprenant un réseau WAN défini par logiciel (SD-WAN), une passerelle Web sécurisée (SWG), des courtiers en sécurité d'accès au cloud (CASB), un accès réseau Zero Trust (ZTNA) et un firewall en tant que service (FWaaS) comme fonctionnalités de base, avec la possibilité d'identifier les données sensibles ou les malwares et la capacité de déchiffrer le contenu au débit de la liaison, avec une surveillance continue des sessions pour les niveaux de risque et de confiance. »

L'objectif du SASE est de fournir une suite d'outils polyvalents pour protéger l'environnement informatique des entreprises dans le monde hybride et multicloud d'aujourd'hui, puisque les utilisateurs et les appareils peuvent se trouver presque n'importe où. À l'heure où la société passe du « travail à domicile » au « travail en tous lieux », c'est-à-dire au travail hybride/à distance, il est d'autant plus important de pouvoir sécuriser les appareils où qu'ils soient. Et c'est exactement ce que permettent les technologies SASE et ZTNA.

Mais revenons à l'accès réseau Zero Trust. Alors que la sécurité réseau traditionnelle repose sur le principe de « faire confiance mais vérifier », le ZTNA adopte l'approche inverse, à savoir « ne jamais faire confiance, toujours vérifier ». C'est ce que l'on appelle le principe du moindre privilège. Cela signifie qu'une organisation traitera tous les utilisateurs de la même façon, sans jamais laisser l'un d'entre eux accéder automatiquement à des réseaux ou ressources. Au lieu de cela, les autorisations sont gérées de manière à ce que chaque utilisateur n'ait accès qu'aux données, ressources et applications dont il a besoin. Cela implique une vérification continue pour s'assurer que l'utilisateur est bien celui qu'il prétend être, afin de réduire les risques d'intrusion dans le réseau et de déplacement latéral des menaces.

Barracuda

Fonctionnement du ZTNA

Le terme « Zero Trust » peut évoquer un climat de suspicion, mais dans le paysage actuel des cybermenaces de plus en plus sophistiquées, ce niveau de vérification est absolument indispensable. Malgré une connotation relativement négative, le ZTNA implique en réalité l'ajout de fonctionnalités plutôt que d'entraves, permettant un meilleur accès à distance, des performances et une productivité accrues, ainsi qu'une sécurité renforcée.

Pour comprendre le fonctionnement du ZTNA, il est possible de le comparer à un aéroport. Lorsqu'un passager arrive au comptoir d'enregistrement, il doit présenter son passeport pour justifier de son identité. Cela lui permet de franchir une étape de la procédure à suivre pour passer la frontière. Mais il n'est pas pour autant autorisé à monter à bord de l'avion : il lui faut encore une carte d'embarquement. Sans ces deux documents, l'accès lui sera refusé. Le même processus s'applique à l'accès réseau Zero Trust : si vous ne pouvez pas à la fois confirmer votre identité (avec votre passeport) et prouver que vous avez les autorisations requises pour accéder au réseau (avec votre carte d'embarquement), vous ne pourrez pas aller plus loin. Tout comme chaque passager est soumis à un contrôle de sécurité approfondi, devant apporter la preuve de son identité et présenter son autorisation pour monter à bord, le ZTNA exige la même chose de chaque utilisateur lorsqu'il tente d'accéder au réseau.

Outre l'authentification rigoureuse des utilisateurs avant de leur donner accès au réseau, qui permet de réduire les risques d'intrusion, le ZTNA présente un autre avantage clé, peut-être moins évident, qui est le solide système de registre qu'il fournit. L'appareil, l'emplacement et l'identité de l'utilisateur sont enregistrés pour chaque demande d'accès au réseau, résultant en la création d'un journal d'audit et d'une couche de traçabilité automatisée que les autres solutions n'offrent pas. En plus de présenter un intérêt en matière de sécurité, l'enregistrement des tentatives d'accès peut s'avérer utile pour des raisons de conformité et de contrôle. À cela s'ajoutent un gain de temps certain, grâce à l'automatisation, et l'absence de tickets informatiques ou d'approbation du management pour l'accès au réseau.

Les VPN ne peuvent rivaliser avec la rigueur et le contrôle systématique du ZTNA. Ce niveau de détail en matière de gestion des autorisations n'est possible qu'avec une solution comme le ZTNA, et ne peut être reproduit avec un VPN. En outre, alors que les VPN font transiter le trafic par plusieurs serveurs dans un premier temps, puis par un point central au sein du réseau, le ZTNA connecte l'utilisateur directement aux applications, sans les faire passer par ce point central, ce qui réduit également le temps de latence. Les applications cloud utilisées par les entreprises étant toujours plus nombreuses, l'amélioration de leurs performances fait une différence notable sur leur efficacité, à la fois en matière de temps et de convivialité.

L'ère de l'accès Zero Trust

Avec un nombre étourdissant de violations de données découlant de l'usage abusif d'accès privilégiés ces dernières années, il est essentiel que les entreprises prennent des mesures pour gérer en toute sécurité leurs autorisations et l'accès au réseau avant qu'il ne soit trop tard.

Testez gratuitement la version complète de Barracuda CloudGen Access pendant 14 jours pour découvrir comment notre solution pourrait vous permettre de simplifier la conformité, de déployer l'accès Zero Trust et de sécuriser l'accès de tiers à vos systèmes. N'hésitez pas à nous contacter en cas de questions.

Barracuda

Barracuda en quelques mots

Rendre le monde plus sûr est notre objectif chez Barracuda. Nous pensons que chaque organisation doit se doter de solutions cloud faciles à acquérir, à déployer et à utiliser, tout en gardant leur niveau de sécurité. Nous protégeons les e-mails, les réseaux, les données et les applications avec des solutions innovantes et évolutives qui s'adaptent à la croissance de nos clients. Plus de 200 000 organisations à travers le monde font confiance à Barracuda pour les protéger — elles restent sereines face aux risques qui sont toujours là — et peuvent se concentrer sur le développement de leur activité. Pour en savoir plus, rendez-vous sur fr.barracuda.com.

Barracuda

Barracuda et le logo Barracuda sont des marques déposées de Barracuda, Inc. aux États-Unis. Tous les autres noms appartiennent à leurs propriétaires respectifs.