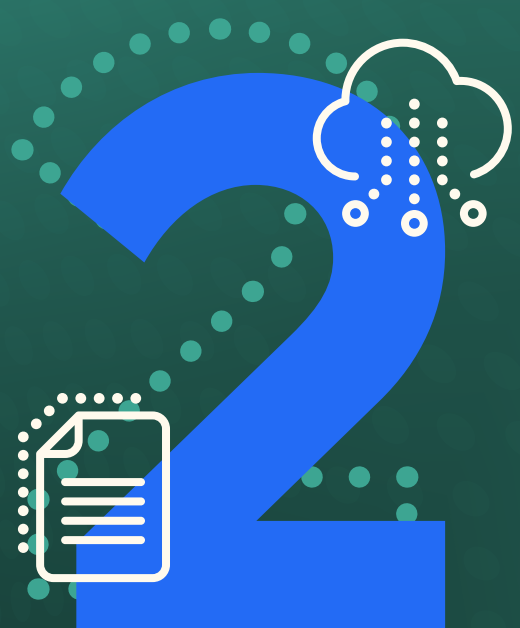
Les symptômes qui indiquent que votre pare-feu traditionnel n’est pas conçu pour le Zero Trust

Les activités métiers d'une entreprise sont menées, aujourd'hui, depuis différents lieux : au bureau, dans un avion, à domicile ou encore au sein d'une usine. Désormais, les applications sont hébergées dans le cloud ou fournies directement en tant qu’applications SaaS, ce qui fait d'Internet un réseau d’entreprise. **Votre pare-feu actuel présente-t-il des carences lorsqu'il s'agit de sécuriser vos utilisateurs, vos données et vos applications via une approche Zero Trust ?** S’il présente l’un des symptôme suivants, il est peut être temps de procéder à un bilan de santé.

SYMPTÔME N°1

La propagation des menaces en interne n'est pas détectée

Autrefois, les utilisateurs travaillaient sur site et que les applications étaient hébergées uniquement dans des data centers protégés par des pare-feu traditionnels : la confiance était accordée de manière implicite. Lorsqu'un hacker s'est infiltré sur le réseau après avoir piraté un utilisateur ou exploité une erreur de configuration, il est presque impossible de neutraliser son accès en temps réel pour l'empêcher de se mouvoir en interne.



INDICE N°2

Les ressources cloud courent un risque

Les pare-feu virtuels opèrent en tant qu'instances de VM dans le cloud public, ce qui vous oblige à déployer une instance à chaque passerelle d’entrée et de sortie. Les pare-feu traditionnels ayant été conçus pour protéger le périmètre de votre réseau, les acteurs malveillants peuvent exploiter les faiblesses du cloud pour compromettre l’intégrité et la posture de sécurité de vos instances et de vos données sensibles.

SYMPTÔME N°3

Des politiques permissives (temporaires ou oubliées)

Les développeurs agiles veulent innover plus rapidement et demandent souvent aux administrateurs IT et de sécurité des politiques d’accès très permissives — au moins temporairement — pour accélérer les projets. Comme on peut s’y attendre, ces politiques peuvent être facilement oubliées et s'inscrivent ainsi dans la durée. Les pare-feu traditionnels peinent à appliquer des changements de politique, de manière dynamique et sur la base de critères comportementaux et d'éléments de contexte observables.

85 % des administrateurs réseau s’accordent à dire que les fonctionnalités de pare-feu sont plus efficaces lorsque fournies à partir du cloud.[1]

Découvrez les 7 symptômes qui indiquent que vos pare-feu traditionnels et de nouvelle génération ne sont pas adaptés au Zero Trust, et pourquoi un pare-feu cloud native pourrait bien être le meilleur remède qu'il vous faut.

Télécharger l'e-Book

1. Source : Zscaler, étude sur les pare-feu réseau

Experience your world, secured.™

Zscaler, Inc.
120 Holger Way
San Jose, CA 95134
+1 408 533 0288
www.zscaler.fr