zscaler™

7 symptômes démontrant que votre pare-feu traditionnel n'est pas conçu pour le Zero Trust

Livre électronique

L'adoption du Zero Trust est en plein essor...

Les acteurs actuels de la sécurité informatique sont parfaitement convaincus que le Zero Trust constitue le modèle de sécurité idéal pour les entreprises numériques modernes (des études révèlent que pas moins de 78 % des programmes de sécurité d'entreprise intègrent déjà ou intégreront prochainement un accès réseau Zero Trust.[1] Ils sont conscients que se concentrer directement sur la sécurisation des utilisateurs, des données et des applications — plutôt que sur le réseau — est clé pour protége les entreprises modernes centrées sur les données et le télétravail.

Il y a plusieurs décennies, lorsque les conceptions de réseaux en étoile étaient à la pointe de la technologie, les pares-feux et les infrastructures réseau construites autour de ceux-ci étaient nouveaux, dynamiques et sains. Ils constituaient à ce moment-là le parfait choix technologique, servant fidèlement et faisant correctement leur travail. À l'ère du cloud computing, cependant, ils représentent un fardeau, les architectures de sécurité cloisonnées etant fondamentalement incompatibles avec le paradigme du Zero Trust.

Ce guide de diagnostic présente sept symptômes démontrant que votre pare-feu est inadapté au monde actuel de la sécurité Zero Trust actuel. Chacun de ces sept symptômes souligne que votre entreprise a besoin d'une thérapie de sécurité cloud.

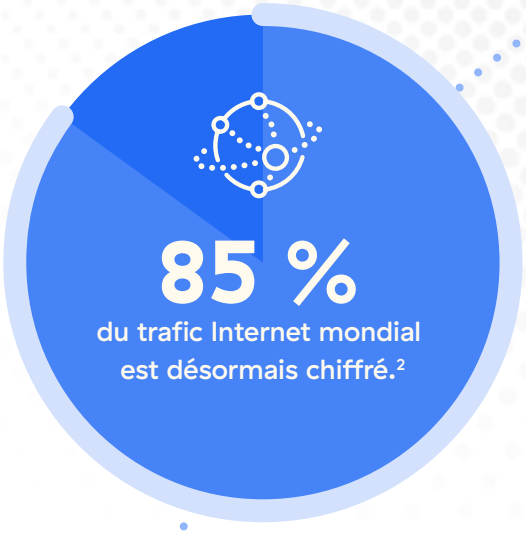
1. Source : Cybersecurity Insiders, Zero Trust Adoption Report, 2019.

SYMPTÔME N°1

Un manque de visibilité lorsque vous essayez d'inspecter le trafic à l'échelle

Indépendamment de leur facteur de forme, les pares-feux basés sur des appliances sont tout simplement incapables d'inspecter le trafic chiffré SSL à grande échelle. Ce problème devient de plus en plus important à mesure qu'augmente le pourcentage du trafic Internet mondial chiffré par SSL. Les hackers sont conscients de cette augmentation et dissimulent de plus en plus de menaces avancées dans le trafic chiffré.

Si votre pare-feu subit ce problème, vous constaterez une dégradation de 50 % ou plus des performances dès que vous tenterez d'activer l'inspection SSL. Vous devrez passer à un pare-feu de plus grande capacité ou ajouter d'autres appliances (ou instances de pare-feu virtuel) juste pour maintenir des performances acceptables pour vos utilisateurs.



QUELLE EST LA SOLUTION ?

- Faire appel à un service fourni dans le cloud qui peut proposer des capacités de pare-feu cloud native plutôt que d'essayer d'exploiter et de mettre à l'échelle des versions de machines virtuelles (VM) d'appliances physiques obsolètes. Seuls les véritables services et solutions cloud sont extensibles à l'infini pour répondre aux besoins actuels en matière de trafic.

2. Source : Agence de l'Union européenne pour la cybersécurité, Analyse du trafic chiffré
3. Source : Zscaler, Enquête sur les pares-feux réseau

SYMPTÔME N°2

Ignorance des mouvements latéraux

Les pares-feux ont été conçus pour protéger le périmètre des réseaux de type cloisonné. Le principe? Une fois que le pare-feu avait pris la décision d'autoriser ou non son entrée, tout le trafic au sein de ce périmètre pouvait jouir d'une confiance inconditionnelle. Dans de telles architectures, la plupart des utilisateurs étaient sur site, une grande partie de l'infrastructure était sur site et la plupart des applications étaient hébergées dans le data center. Plus rien de tout cela n'est valable aujourd'hui.

La réalité actuelle est que 70 % du trafic circule à l'intérieur du réseau, ce qui signifie qu'il se déplace entre les serveurs et les applications au sein du cloud privé ou du data center de l'entreprise. Les défenses basées sur le périmètre ne laissent guère de moyens pour inspecter ou bloquer ce trafic, ce qui laisse le champ libre aux hackers une fois qu'ils ont pénétré le réseau.

Une fois que vous avez obtenu l'accès à ce type de réseau, il est extrêmement simple de découvrir toutes les ressources auxquelles il est connecté. L'utilisateur n'a besoin que d'un simple outil d'analyse open-source pour trouver chaque adresse IP au sein du réseau. À partir de là, la diffusion de ransomwares — ou l'exfiltration de précieuses données — est un jeu d'enfant, et un pare-feu est impuissant à l'arrêter.

64 %

des administrateurs réseau actuels pensent que les pares-feux sont inefficaces pour empêcher les mouvements latéraux.[4]

57 %

des décideurs informatiques sont convaincus que les pares-feux ne peuvent pas bloquer les attaques par ransomware.[4]

QUELLE EST LA SOLUTION ?

- Mettre en place un accès réseau Zero Trust qui n'autorise les connexions qu'après vérification de l'identité des appareils et des utilisateurs, vérification du statut de sécurité et application des politiques de sécurité — pour chaque connexion, à chaque fois. Cela permet d'établir des connexions directes et sécurisées entre les utilisateurs et les applications, au lieu de connexions non protégées à un réseau.

4. Source : Zscaler, Enquête sur les pares-feux réseau

SYMPTÔME N°3

Surabondance de politiques

Les équipes de sécurité tentent d'instaurer le Zero Trust au sein des architectures réseau existantes en configurant des politiques qui segmentent les réseaux en morceaux toujours plus petits. Il s'agit de microsegmentation en théorie, mais l'effort et l'administration nécessaires à la maintenance deviennent rapidement ingérables en pratique.

Pour protéger les applications actuelles, les entreprises doivent déployer un nombre croissant de pares-feux virtuels sur l'ensemble du réseau. Il en résulte un tsunami de politiques qui nécessite une configuration et une reconfiguration sans fin pour construire quelque chose qui ressemble à une mise en application du Zero Trust.

Comme les appliances physiques qui les ont précédé, les pares-feux virtuels ne peuvent pas évoluer au-delà d'un certain point. À terme, il vous faudra des milliers, voire des dizaines de milliers, de politiques, ce qui constitue un véritable cauchemar à gérer.

QUELLE EST LA SOLUTION ?

Le secret consiste à séparer le réseau du contrôle d'accès aux applications et aux ressources. L'accès réseau Zero Trust permet d'accorder aux utilisateurs individuels un accès direct et sécurisé aux applications, et non à des segments du réseau. Cela signifie que les utilisateurs peuvent être directement connectés aux applications dont ils ont besoin tandis que le trafic suit le chemin le plus court possible, et que les administrateurs et les équipes de sécurité n'ont plus à se soucier du fonctionnement sous-jacent.

Le déploiement ne se fait pas du jour au lendemain, mais sa mise en œuvre diligente peut simplifier la gestion de l'informatique, du réseau et de la sécurité tout en offrant de meilleures performances aux utilisateurs finaux.

SYMPTÔME N°4

Le risque de propagation de l'infection à travers vos ressources de cloud public

Sur leurs marchés de logiciels en ligne, les fournisseurs de cloud public proposent des pares-feux virtuels censés être certifiés pour répondre aux besoins de leurs clients. Ces pares-feux ne sont souvent que des versions virtuelles de pares-feux basés sur des appliances qui s'exécutent en tant qu'instances de VM dans le cloud public.

L'exécution d'un de ces pares-feux dans le cloud étend essentiellement votre architecture réseau traditionnelle vers l'extérieur pour englober les ressources du cloud. Cela permet aux hackers qui parviennent à percer les défenses de votre pare-feu de se déplacer librement au sein d'un réseau étendu et cela ouvre l'accès à vos ressources cloud à quiconque se trouve sur votre réseau.

En outre, la configuration des politiques destinées à régir le trafic entre les charges de travail dans le cloud public et les clouds privés virtuels est confuse et fastidieuse. Vous aurez besoin d'instances de pare-feu virtuel sur chaque point d'entrée et de sortie de votre architecture cloud. Considérez un instant l'interconnectivité inhérente au cloud et vous comprendrez rapidement pourquoi cette conception est aussi complexe.

De plus, vous devrez gérer une infrastructure de routage et de mise en réseau alambiquée juste pour que cette architecture cloud fonctionne avec le reste de votre réseau traditionnel.

Gardez à l'esprit que les pares-feux n'ont pas été conçus pour bloquer les mouvements latéraux.

QUELLE EST LA SOLUTION ?

- Investir dans une plateforme moderne qui sert d'échange entre les charges de travail, peu importe où elles se trouvent. Cela empêche les hackers de se déplacer latéralement pour accéder aux ressources du réseau tout en simplifiant la gestion et le dépannage. De plus, cela procure aux administrateurs un contrôle d'accès granulaire et conditionnel qui peut être révoqué si le contexte est modifié.

SYMPTÔME N°5

La tendance au « tout permis » échappe à tout contrôle

La transformation du cloud bouleverse les activités à l'échelle mondiale, et les entreprises de tous secteurs profitent de l'agilité et la liberté d'innover offertes par le cloud. Si vous faites partie d'une équipe informatique ou sécurité, vous serez tôt ou tard confronté à un projet de migration vers le cloud, si ce n'est pas le cas.

Le problème est qu'il est difficile et fastidieux de configurer les architectures traditionnelles basées sur des pares-feux pour sécuriser les ressources cloud. Les politiques prolifèrent, les complexités foisonnent et, qui plus est, les utilisateurs doivent accéder aux applications pour être productifs. Que pouvez-vous faire ?

90 % des administrateurs informatiques et de sécurité admettent avoir appliqué des politiques très permissives — au moins temporairement — pour accélérer les projets et donner aux utilisateurs l'accès dont ils ont besoin. Au fil du temps, les politiques permissives s'accumulent et sont finalement ignorées ou oubliées, ce qui augmente le risque que court l'entreprise de subir une violation ou d'être victime d'une attaque dévastatrice par ransomware. Bien entendu, ces pratiques sont en contradiction directe avec celles d'une approche Zero Trust et d'accès sur la base du moindre privilège.

85 %
des entreprises auront adopté une stratégie cloud-first d'ici 2025.[5]

95 %
des nouvelles charges de travail numériques sont aujourd'hui déployées sur des plateformes cloud natives.[5]

QUELLE EST LA SOLUTION ?

Rechercher une solution Zero Trust basée sur le cloud, facile à mettre en œuvre et à utiliser. Une plateforme Zero Trust unifiée avec une console de gestion unique sera non seulement plus facile à configurer et à gérer, mais elle offrira également une sécurité plus robuste qu'un pare-feu de périmètre traditionnel.

5. Source : Gartner, „Gartner Says Cloud Will Be the Centerpiece of New Digital Experiences"

SYMPTÔME N°6

Exposition potentiellement infectieuse à Internet

Les pares-feux périmétriques ont été conçus pour servir de front-end réseau. Ce sont par nature des ressources exposées à Internet, permettant un accès direct aux réseaux et ressources internes en cas de violation. Cela signifie que l'utilisation d'un pare-feu traditionnel comme passerelle afin de déployer des services de réseau privé virtuel (VPN) met intrinsèquement votre réseau en danger.

La gravité de ces risques a été mise en évidence récemment par une série de brèches réussies par des attaquants ayant exploité les vulnérabilités des VPN traditionnels. L'attaque par ransomware de Colonial Pipeline, la plus grande cyberattaque contre une infrastructure critique jamais divulguée aux États-Unis, s'est produite lorsque des hackers « ont exploité un VPN traditionnel qui n'aurait pas dû être en fonction », selon le PDG de la société.[6]

Les VPN basés sur des pares-feux ne permettent pas de mettre en œuvre des contrôles d'accès granulaires ou de déterminer quels utilisateurs peuvent se connecter à des ressources particulières. Par conséquent, s'appuyer sur des VPN est une approche de type « tout ou rien » qui étend la surface d'attaque de votre réseau cloud jusqu'aux routeurs et réseaux sans fil domestiques de chaque collaborateur. Et, plus votre réseau s'étend, plus les hackers peuvent faire de dégâts, et vite.

Les VPN basés sur des pares-feux ne permettent pas de mettre en œuvre des contrôles d'accès granulaires ou de déterminer quels utilisateurs peuvent se connecter à des ressources particulières.

QUELLE EST LA SOLUTION ?

- Rechercher une alternative VPN qui permet un accès sécurisé aux applications en établissant des connexions individuelles entre les utilisateurs et les applications sur une base dynamique tenant compte de l'identité et du contexte. Ces solutions utilisent des connexions vers l'extérieur qui dissimulent les applications à l'Internet public, garantissant ainsi de meilleures performances que les VPN et une amélioration considérable de la sécurité.

6. Source : „Colonial Pipeline hack explained: Everything you need to know", TechTarget, April 2022.

SYMPTÔME N°7

Congestion du trafic

L'entreprise décentralisée est aujourd'hui un concept courant, et la plupart des organisations adoptent des modèles de travail hybrides et à distance pour rester dans la course. Mais lorsqu'un grand nombre d'utilisateurs travaillent à distance et que vous vous appuyez toujours sur une architecture réseau traditionnelle cloisonnée, vous devez procéder au backhauling de gros volumes de trafic vers le data center de l'entreprise pour les faire inspecter par votre pare-feu.

Inutile de dire que cette architecture n'a pas de sens et qu'elle est complexe. La gestion des pares-feux traditionnels et des piles de sécurité basées sur des appliances est longue et fastidieuse. Si vous utilisez des lignes MPLS louées, vous payez un supplément pour une infrastructure complexe de routage, de commutation et de segmentation du trafic. C'est pourquoi l'intérêt pour les (SD-WAN – Software Defined Wide Area Networking) augmente — mais l'ajout de superpositions de réseaux ne fait qu'accroître la complexité et les coûts associés à la gestion des pares-feux.

Les performances des applications et l'expérience utilisateur pâtissent toutes deux du backhauling du trafic. Sans parler de la latence, un problème récurrent qui devient encore plus problématique à mesure que les entreprises s'appuient davantage sur des applications de communication gourmandes en bande passante telles que Zoom et Microsoft Teams.

QUELLE EST LA SOLUTION ?

- Une solution Zero Trust basée sur le cloud place les contrôles de sécurité là où se trouvent les utilisateurs et les applications actuels : dans le cloud. Elle applique la politique inline et à la périphérie, de sorte que le trafic ne doit faire aucun saut supplémentaire. Et parce qu'elle opère sur le chemin des données, une plateforme Zero Trust peut surveiller chaque connexion et automatiquement identifier et corriger les problèmes de performances.

LA SOLUTION ZERO TRUST

Comment Zscaler optimise votre réseau et son architecture

Zscaler Zero Trust Exchange™ est une plateforme cloud native conçue spécialement pour le Zero Trust. Elle permet des connexions directes et sécurisées fondées sur le principe de l'accès sur la base du moindre privilège. Il inspecte le contenu en profondeur et vérifie les droits d'accès sur la base de l'identité et du contexte avant d'autoriser toute connexion.

Le moteur de politique basé sur l'IA/AA de Zscaler, alimenté par le plus grand cloud de sécurité au monde, interprète le contexte en fonction des informations sur l'utilisateur, le dispositif et l'application, puis exploite ce contexte pour prendre des décisions intelligentes sur les niveaux d'accès et les restrictions afin de préserver la sécurité des utilisateurs et des données. De plus, la plateforme sert de courtier pour les connexions individuelles directes entre les utilisateurs et les applications, garantissant ainsi l'invisibilité des applications sur Internet et suprimant la surface d'attaque.

Notre approche rend la sécurité Zero Trust accessible et simple pour nos clients. C'est pourquoi les leaders du secteur et des analystes reconnus s'accordent à dire que Zero Trust Exchange est la plateforme Zero Trust la plus aboutie et la plus facile à utiliser.

Le déploiement de la plateforme Zero Trust Exchange de Zscaler est simple et rapide, et il propose une gamme complète de sécurité inline intégrée renforçant ses capacités SSE (Security Service Edge) de pointe. Il s'agit notamment de :

- **Pare-feu Cloud-gen**
- **Sandboxing cloud avancé**
- **Secure Web Gateway (SWG)**
- **Prévention des pertes de données (DLP)**
- **Passerelle d'accès cloud sécurisé**
- **et bien plus encore**

Pour plus d'informations, rendez-vous sur :
www.zscaler.fr/products/zscaler-internet-access

zscaler™ | **Experience your world, secured.™**

À propos de Zscaler
Zscaler (NASDAQ: ZS) accélère la transformation digitale de sorte que les clients deviennent plus agiles, plus efficaces, plus résilients et plus en sécurité. La plateforme Zscaler Zero Trust Exchange protège des milliers de clients contre les cyberattaques et la perte des données en connectant de manière sécurisée les utilisateurs, les appareils et les applications indépendamment de l'emplacement. Distribué à travers plus de 150 data centers dans le monde, Zero Trust Exchange basé sur le SSE est la plus grande plateforme de sécurité cloud inline. Pour en savoir plus, rendez-vous sur **zscaler.fr** ou suivez-nous sur Twitter **@zscaler**.

+1 408 533 0288 Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134 zscaler.fr