Les cinq principaux risques des pare-feu de périmètre et comment les surmonter

Les pare-feu font depuis longtemps partie intégrante de l'architecture réseau des entreprises. Mais avec le passage aux modèles économiques numériques, le pare-feu, autrefois solide, constitue désormais un risque pour la sécurité. Voici pourquoi.

Au sein d'une architecture de sécurité traditionnelle basée sur le périmètre qui exploite des pare-feu et des VPN, la sécurité est limitée au périmètre ou à la zone de confiance. Tout utilisateur ou application situés à l'intérieur du périmètre ou de la zone de confiance est considéré comme bienveillant, et ceux à l'extérieur sont considérés comme malveillants. Ce principe était parfaitement adapté lorsque la plupart des utilisateurs et des applications se trouvaient à l'intérieur du périmètre. Toute personne située à l'extérieur du périmètre devait être intégrée au réseau en étendant le périmètre à celle-ci. Ceci était traité comme une exception afin de les inclure dans la zone de confiance.

Les entreprises ont considérablement changé depuis l'introduction du pare-feu. Les employés des entreprises peuvent désormais travailler partout et n'importe où, que ce soit à domicile, dans des espaces de travail partagés, dans des filiales ou ailleurs, pour autant qu'ils disposent d'une connexion Internet et d'une source d'électricité. L'extension du périmètre pour chaque utilisateur distant ne fonctionne plus puisque l'exception des utilisateurs et des applications disséminés est désormais la norme. Le concept de zone de confiance n'est plus pertinent car les applications et les utilisateurs peuvent désormais se trouver n'importe où, ce qui impose de passer à un modèle Zero Trust. Les pare-feu et les VPN ne sont toutefois pas en mesure de garantir un véritable Zero Trust et présentent plusieurs risques lorsqu'ils s'y essaient.

Dans ce livre blanc, nous allons détailler les cinq risques majeurs engendrés par les pare-feu dans un monde mobile et de cloud, et comment les supprimer avec une approche Zero Trust moderne.

RISQUE n° 1

Grande surface d'attaque

Une surface d'attaque est la somme de tous les points exposés, tels que les adresses IP, qui peuvent permettre aux adversaires de découvrir des vulnérabilités, de s'y acheminer et de les exploiter pour accéder à un système et en extraire des données précieuses. En termes simples, plus la surface d'attaque est petite, plus il est difficile pour les hackers d'y accéder. Mais la dissémination d'applications dans le cloud et la mobilité du personnel ont élargi de manière exponentielle la surface d'attaque, rendant les entreprises plus vulnérables que jamais. Non seulement l'utilisation de pare-feu physiques et virtuels basés sur le périmètre ne résout pas ce problème, mais elle aggrave la situation en augmentant la surface d'attaque de votre entreprise, ce qui permet aux cybercriminels de prendre pied dans votre réseau ou votre instance de cloud.

Comment ? Les pare-feu publient les adresses IP de vos serveurs et applications sur Internet afin que vos employés et partenaires puissent les localiser, mais cela implique que les attaquants peuvent également les localiser. Tout pare-feu connecté à Internet, qu'il se trouve dans le data center, dans le cloud ou dans une filiale, peut être découvert, attaqué et exploité. Les pare-feu virtuels sont tout aussi risqués que leurs homologues physiques, car ils exposent eux aussi les IP sur Internet, souvent en bien plus grand nombre que les pare-feu physiques, ce qui augmente encore le risque.

Comment éliminer la surface d'attaque avec Zero Trust

L'élimination de votre surface d'attaque est le secret de la sécurisation de votre réseau, de vos applications et, surtout, de vos données. Avec une véritable offre Zero Trust, les applications deviennent des entités non routables, invisibles pour les attaquants potentiels, de sorte que vos ressources ne peuvent être découvertes sur Internet. Une véritable plateforme Zero Trust s'interpose entre l'utilisateur et l'application, de sorte que toutes les communications passent par la plateforme et que rien n'atteint les applications sans que la plateforme ne l'autorise.

Cette approche est fondamentalement différente des pare-feu de périmètre, car seules les connexions internes sont autorisées, contrairement à l'approche externe traditionnelle, qui exige la publication des adresses. En rendant les applications invisibles aux adversaires et exclusivement accessibles aux utilisateurs autorisés, la surface d'attaque se trouve pratiquement éliminée, et l'accès aux applications est en permanence sécurisé, que ce soit sur Internet, SaaS, ou dans des clouds publics ou privés.

Détection de la surface d'attaque

Les surfaces d'attaque sont certes difficiles à trouver manuellement, mais des services tels que l'analyse de la surface d'attaque sur Internet fournissent une visibilité sur la surface d'attaque globale, révélant les serveurs, les espaces de noms, les vulnérabilités et les instances de cloud qui sont visibles sur Internet. L'analyse interroge les sources publiques pour révéler toute zone d'exposition qui vous met en danger. Zero Trust permet ainsi aux entreprises d'évaluer les surfaces d'attaque, de les analyser et de les éliminer.

Étouffement des performances des applications

Les utilisateurs attendent désormais un certain niveau de réactivité et de disponibilité des applications cloud qu'ils utilisent à titre privé. Cependant, les employés ne bénéficient souvent pas d'une telle expérience lorsqu'ils accèdent aux applications de l'entreprise en utilisant les solutions d'accès au réseau de celle-ci, car ils ne disposent plus d'un accès rapide et direct aux applications cloud. En réalité, la lenteur des performances des applications font perdre aux utilisateurs leur productivité et leur capacité à collaborer efficacement avec leurs homologues. C'est ce qui incite de nombreux utilisateurs à contourner les contrôles de sécurité, chose particulièrement risquée s'ils utilisent des appareils non gérés ou des réseaux Wi-Fi et domestiques non sécurisés. Les problèmes de performance pour l'utilisateur final sont également liés à la disponibilité des applications SaaS ou cloud, à la capacité des appareils, aux interruptions du chemin d'accès au réseau ou à la congestion du réseau, facteurs qui ne peuvent être facilement isolés et diagnostiqués par l'opérateur.

Pourquoi ? L'architecture réseau en étoile implique que les bureaux distants et les filiales se connectent au bureau central (data center) à travers les pare-feu avec MPLS et aux utilisateurs distants avec VPN. Cette architecture crée un réseau plat qui s'étend à tous les emplacements et exige que tout le trafic réseau soit acheminé vers une pile de sécurité centrale. Envoyer le trafic d'un utilisateur distant à travers le data center et vers le cloud avant de le retourner à l'utilisateur, puis suivre le même chemin en sens inverse, augmente considérablement la latence, détériorant par conséquent l'expérience utilisateur. Les pare-feu virtuels dans le cloud subissent le même sort, car le trafic doit leur être redirigé de la même manière que pour les data centers physiques, puisqu'ils ne sont pas inline avec les serveurs d'application.

Les applications cloud ont été conçues pour être accessibles directement, avec le moins de sauts possible, afin de maximiser les performances. À ce titre, de nombreux fournisseurs d'applications SaaS (comme pour Microsoft 365) indiquent spécifiquement que les pare-feu ne doivent pas être placés sur leur chemin pour être pleinement pris en charge.

Comment surmonter les problèmes de performance avec Zero Trust

Une architecture Zero Trust diffère du réseau traditionnel en étoile et de la sécurité cloisonnée. Elle fournit une connectivité directe avec les applications et réduit les risques tout en offrant une meilleure expérience utilisateur.

Une plateforme Zero Trust efficace applique une politique inline, à la périphérie, de sorte qu'aucun saut supplémentaire n'est nécessaire, et le peering direct avec les sociétés d'application permet une connexion directe basée sur la disponibilité et la capacité. En intervenant sur le chemin des données, une plateforme Zero Trust peut également surveiller chaque connexion et identifier et résoudre automatiquement les problèmes de performance. Cette capacité est cruciale pour les applications à faible latence, telles que les applications de communications unifiées en tant que service (UCaaS) comme Microsoft Teams et Zoom. La possibilité de surveiller ces applications et de remédier rapidement aux problèmes grâce aux fonctionnalités de Digital Experience Monitoring (DEM) permettent aux entreprises d'identifier et de résoudre les problèmes avant que les utilisateurs ne s'en rendent compte, améliorant ainsi la collaboration et la productivité des collaborateurs.

Mesurer l'expérience utilisateur

Un outil de surveillance avancé mesure l'expérience utilisateur et fournit un aperçu de l'expérience numérique permettant de comprendre, de diagnostiquer et d'améliorer les problèmes d'expérience utilisateur au sein de votre entreprise. Le score vous aide à identifier les anomalies de performance à l'aide de l'apprentissage automatique et vous fournit des alertes exploitables.

Complexité et coûts opérationnels élevés

L'utilisation de pare-feu, de MPLS et de VPN, voire d'appareils virtuels, ne constitue pas une approche réaliste de la mise en œuvre de Zero Trust. La gestion et le déploiement de pare-feu de périmètre visant à assurer une sécurité cohérente pour tous les utilisateurs, toutes les applications, tous les appareils et tous les emplacements sont trop complexes et coûteux d'un point de vue opérationnel. Le déploiement des politiques de périmètre, les mises à jour et les correctifs ne peuvent être gérés par les équipes. Il faut acheter et déployer des pare-feu matériels et virtuels pour les scénarios les plus défavorables, et le backhauling du trafic vers une seule pile de sécurité utilise inutilement de la bande passante et de la ressource de sécurité.

La planification de la capacité exige des DSI et des RSSI qu'ils anticipent et planifient avec précision les besoins en matériel et les coûts de consommation de bande passante liés à l'envoi de tout le trafic sur MPLS vers le data center pour inspection. Sous-estimer les besoins du réseau restreint les performances et, à l'inverse, les surestimer entraîne des coûts inutilement élevés et des équipements qui ne seront pas utilisés. Sans compter qu'il n'est pas réaliste de déployer exactement la même pile d'appareils sur chaque emplacement, ce qui donne lieu à une multitude de produits disparates disséminés dans votre infrastructure. La collecte et la conservation des journaux pour ces nombreux appareils constituent un autre défi, et les opérateurs négligent souvent les journaux essentiels, ce qui représente un risque potentiel pour la sécurité. 75 % des opérateurs reconnaissent qu'il est difficile de gérer le matériel, les mises à niveau et les déploiements de pare-feu.[2]

Et ce n'est là qu'une partie du défi. Cette approche fragmentée oblige les équipes de sécurité à utiliser des abonnements et des plateformes de gestion distincts pour mettre en œuvre différentes politiques et gérer différentes zones avec une segmentation du réseau. Des efforts supplémentaires sont nécessaires pour unifier la visibilité par utilisateur, par application et par emplacement. Les collaborateurs doivent constamment se consacrer à la mise en œuvre des correctifs, aux mises à jour de sécurité, au rafraîchissement du matériel et à la gestion des politiques pour un ensemble hétéroclite de pare-feu et d'appliances de sécurité. Il en résulte une charge financière et un manque de productivité intenables.

Comment éviter la complexité avec Zero Trust

Au lieu de recourir à plusieurs solutions matérielles ou à des solutions cloud de produits ponctuels difficiles à gérer et à entretenir, une solution intégrée Zero Trust sécurise toutes les applications SaaS, Internet et privées à l'aide d'une plateforme unique. Zero Trust dispense de recourir à des réseaux MPLS coûteux qui nécessitent un routage, une commutation et une segmentation complexes du réseau, entre autres, grâce à un accès direct, rapide et sécurisé au cloud, et à une connectivité cloud à cloud sécurisée. Il élimine pratiquement la nécessité de renvoyer le trafic vers le data center pour inspection. Une plateforme Zero Trust unifiée avec une console de gestion unique est beaucoup plus rapide à configurer, plus facile à gérer, dispose de politiques simplifiées et offre plus de sécurité que la sécurité de périmètre traditionnelle.

Une solution Zero Trust basée sur le cloud place les contrôles de sécurité là où se trouvent les utilisateurs et les applications : dans le cloud. Grâce à une visibilité sur tous les utilisateurs, clouds et charges de travail, Zero Trust simplifie les opérations et le dépannage. La transition vers le cloud réduit la charge de travail de l'équipe informatique qui doit acheter, gérer, entretenir et superviser les pare-feu et autres matériels de sécurité, ce qui lui permet de se consacrer à d'autres projets. Plus important encore, une solution Zero Trust basée sur le cloud permet aux entreprises d'évoluer rapidement à mesure que le nombre d'utilisateurs et d'applications augmente.

Sensibilité aux coûts

L'enquête 2021 du rapport sur le risque VPN a conclu que le coût élevé des appliances et de l'infrastructure de sécurité était le deuxième plus grand défi posé aux entreprises par leur solution d'accès à distance. Les entreprises qui ont adopté Zero Trust par le biais de Zero Trust Exchange ont enregistré un retour sur investissement de 139 % et 4,1 millions de dollars de bénéfices en moyenne, avec un accroissement de leur productivité, une réduction des incidents et une diminution des appliances.[3]

Déplacement latéral des menaces

Les hackers recourent à divers moyens pour accéder au réseau d'une entreprise, souvent par le biais d'attaques d'hameçonnage ou d'infections par des programmes malveillants. Une fois sur le réseau, leur objectif est de se déplacer latéralement dans l'entreprise à la recherche d'un accès à des données sensibles afin de les exfiltrer, de les chiffrer pour obtenir une rançon ou de provoquer d'autres perturbations. Le déplacement latéral permet à un attaquant d'éviter de se faire repérer et de conserver son accès, même s'il est découvert sur la machine qui a été infectée en premier. Et comme le temps d'attente est long, le vol de données peut intervenir plusieurs semaines, voire plusieurs mois, après la violation initiale.

Les entreprises se sont appuyées sur une approche de sécurité cloisonnée — également appelée sécurité du périmètre — pour protéger leurs données contre les attaques malveillantes. À l'instar des châteaux médiévaux protégés par des murs de pierre, des douves et de lourdes portes, la sécurité du périmètre investit massivement dans la fortification des périmètres de réseau à l'aide de pare-feu et d'autres outils. La sécurité de périmètre surveille les points d'entrée et de sortie du réseau en vérifiant les paquets de données et l'identité des utilisateurs qui entrent et sortent du réseau de l'entreprise, puis considère que l'activité à l'intérieur du périmètre renforcé est relativement sûre.

Les architectures de sécurité traditionnelles sont incapables de bloquer ces attaques sophistiquées, parce qu'une fois que l'utilisateur, bon ou mauvais, entre dans un réseau « sécurisé », il devient un utilisateur de confiance et obtient un accès latéral à toutes les applications, même s'il ne le devrait pas. Réduire le mouvement latéral au sein des architectures basées sur le périmètre requiert une segmentation du réseau (périmètres internes), ce qui constitue un véritable cauchemar opérationnel, car une telle action oblige les entreprises à déployer et à gérer plus de pare-feu avec plus de politiques, sans pour autant résoudre correctement le problème sous-jacent.

Comment éviter le déplacement latéral avec Zero Trust

Zero Trust empêche les mouvements latéraux en connectant directement les utilisateurs et les charges de travail aux applications, et jamais au réseau de l'entreprise. Les menaces ne peuvent donc pas se propager latéralement et infecter d'autres appareils et applications, sans qu'il soit nécessaire de recourir à une segmentation complexe du réseau. Cela ne s'applique pas seulement aux utilisateurs accédant aux applications, mais à toutes les connexions au sein de l'entreprise, des machines IoT aux applications dialoguant entre elles, où une application située en un emplacement (cloud ou data center) peut se connecter en toute sécurité à une autre application, où qu'elle se trouve. Ces connexions sécurisées individuelles éliminent totalement le risque de déplacement latéral.

Le modèle Zero Trust part de l'hypothèse que tout est hostile et accorde la confiance uniquement sur la base de l'identité et du contexte. Cette approche autorise les connexions sur la base de la connaissance des entités qui se connectent et le contexte de leurs connexions garantit que l'accès est limité à ce qui est nécessaire uniquement, à tout moment. Les équipes chargées de la sécurité et de l'informatique sont ainsi libérées d'une charge importante, car l'application est automatique et peut changer dynamiquement lorsque les conditions changent pour ces entités et leurs connexions.

Enfin, Zero Trust fournit des contrôles granulaires avec un accès conditionnel. Un administrateur peut configurer des politiques de manière à ce que les utilisateurs ne puissent accéder à certaines applications que si leur trafic provient d'un emplacement de confiance, tel qu'un réseau d'entreprise, et que si les utilisateurs ont procédé à une authentification multi-facteur. L'administrateur peut également bloquer le trafic utilisateur provenant de certains emplacements ou zones géographiques, d'un appareil non fiable, ou si les données demandées ne relèvent pas des autorisations spécifiques accordées à l'utilisateur. Toutes les connexions sont basées sur le contexte et à chaque fois que le contexte change, la confiance est réévaluée.

La nouvelle segmentation

Le coût, la complexité et le temps nécessaires à la segmentation du réseau à l'aide des pare-feu virtuels dépassent les avantages en termes de sécurité. La segmentation de la charge de travail constitue une nouvelle façon de segmenter les charges de travail des applications. En un clic, la sécurité peut être renforcée en permettant à la segmentation de la charge de travail de révéler les risques et d'appliquer aux charges de travail une protection basée sur l'identité, sans aucune modification du réseau. La technologie de segmentation de la charge de travail basée sur l'identité fournit une protection sans faille assortie de politiques qui s'adaptent automatiquement aux changements de l'environnement.

Perte de données

Les données sont vitales pour les entreprises pour des raisons stratégiques, financières et de sécurité, entre autres ; dans certains cas, elles peuvent même se révéler cruciales pour la sécurité nationale. Même en présence de périmètres de sécurité réseau, des données peuvent fuir du fait d'un manque de sensibilisation, d'actions involontaires des utilisateurs, de défaillances du système et de pratiques malveillantes de plus en plus sophistiquées. Cela peut engendrer de nombreuses conséquences préjudiciables, notamment des amendes, la perte de clients, des retombées juridiques, la non-conformité aux réglementations et une atteinte à l'image de marque de la société. Examinons les différents types de données et la manière dont elles peuvent être menacées :

- **Les données en mouvement :** les données qui transitent par Internet représentent aujourd'hui la majeure partie des données en mouvement, car l'accès aux applications se fait principalement par le Web ; c'est vrai pour les applications SaaS, les applications dans le data center et celles dans les clouds publics. L'accès des utilisateurs à Internet et à des destinations risquées, d'où des informations sensibles peuvent être exfiltrées, constitue une menace pour les données de l'entreprise. Les pare-feu ne peuvent pas suivre les utilisateurs hors réseau ni sécuriser leur trafic Web critique en mouvement. De moins en moins de données et d'applications restent sur les endpoints, d'où l'importance de sécuriser les données qui circulent entre les endpoints, les applications cloud et le stockage avec une solution adaptée aux données en mouvement.
- **Les données au repos :** les données résidant dans les data centers, les applications SaaS et les clouds publics représentent la grande majorité des données au repos. La sécurisation des données au repos dans les applications SaaS est particulièrement importante pour la sécurité ; même si elles sont sécurisées par des pare-feu, il suffit de quelques clics pour partager des données avec un utilisateur non autorisé via des applications telles que Microsoft OneDrive. En outre, des brèches peuvent être ouvertes dans le cloud suite à des erreurs de configuration ou des autorisations dangereuses. Le SaaS et le IaaS étant très dynamiques et souvent configurés par des personnes qui ne sont pas des experts en sécurité, de telles failles sont souvent négligées et exploitées.

L'objectif ultime de toute technologie de sécurité est de protéger les données sensibles, toutefois les pare-feu ne sont pas capables d'identifier ni de contrôler efficacement les données en mouvement ou au repos, exposant les données de l'entreprise à de nombreux risques. Plus important encore, ils sont incapables d'inspecter efficacement le trafic chiffré qui représente plus de 90 % de l'ensemble du trafic[1], permettant au trafic chiffré SSL/TLS de passer sans être inspecté.

Comment éviter la perte de données avec Zero Trust

Une véritable plateforme Zero Trust est en mesure d'inspecter la totalité du trafic, tant sur le réseau qu'en dehors, y compris le trafic chiffré. Elle comble les lacunes en matière de visibilité et d'inspection pour assurer une prévention efficace de la perte de données (DLP) et une protection contre les cybermenaces. Elle est capable de déchiffrer toutes les données, de déterminer leur intégrité, puis d'autoriser les connexions via un contexte tel que l'utilisateur, la géolocalisation, l'adresse IP, la posture de l'appareil, l'heure, etc. Les politiques DLP d'une solution Zero Trust protègent les données en mouvement, tandis que les utilisateurs bénéficient partout d'une sécurité rapide et cohérente.

Une solution Zero Trust inline permet de détecter et de contrôler intégralement l'informatique fantôme. Elle sécurise les menaces et les données basées sur le web grâce à l'isolation du navigateur qui permet l'accès à des appareils non gérés sans les problèmes de performance associés. L'isolation du navigateur diffuse les données sous forme de pixels à partir d'une session isolée dans un environnement conteneurisé, permettant le BYOD (utilisation des appareils personnels dans un cadre professionnel), mais empêchant la perte de données liée au téléchargement, au copier-coller et à l'impression. La DLP hors bande et la protection contre les menaces avancées (ATP) empêche les partages de fichiers à risque et bloque les programmes malveillants au repos dans le cloud. Protéger les données dans le cloud implique également de remédier aux erreurs potentiellement graves de configuration, aux violations de conformité, aux autorisations et aux droits. En bref, Zero Trust fournit une sécurité cohérente et unifiée pour les données au repos et celles en mouvement, y compris le trafic chiffré, à travers les applications Internet, SaaS et cloud public à l'échelle, indépendamment de l'appareil de l'utilisateur.

Vulnérabilité du navigateur web

Le pourcentage de trafic Web chiffré sur Internet n'a cessé d'augmenter, passant de 50 % en 2014 à un pourcentage stupéfiant de 95 % actuellement.[1] Et pourtant, les navigateurs Web constituent la cible principale des attaquants. En effet, selon Gartner, 98 % des attaques sont menées sur l'Internet public et 80 % de ces attaques visent les utilisateurs finaux par le biais des navigateurs. Les outils d'isolation des navigateurs tels que Cloud Browser Isolation contribuent à atténuer ces vulnérabilités, en particulier lorsqu'ils peuvent être déployés sans installation de logiciel côté client, ce qui les rend plus adaptés aux appareils non gérés accédant aux ressources informatiques de l'entreprise.

Atteindre un réel Zero Trust avec Zscaler

Zscaler apporte une solution Zero Trust avec Zscaler Zero Trust Exchange, une plateforme cloud native opérant dans 150 data centers répartis dans le monde, qui exploite le plus grand cloud de sécurité de la planète pour fournir des connexions rapides et sécurisées et permettre à vos employés de travailler en toute sécurité de n'importe où, sur n'importe quel appareil, en utilisant Internet comme réseau d'entreprise. Contrairement aux pare-feu et VPN, Zero Trust Exchange est fondé sur le principe de l'accès sur la base du moindre privilège et sur le concept selon lequel aucun utilisateur ou application n'est intrinsèquement fiable. Au lieu de cela, les connexions sont autorisées sur la base de l'identité de l'utilisateur et du contexte, dont notamment l'emplacement de l'utilisateur, la posture de sécurité de l'appareil, l'application à laquelle il accède et le contenu échangé.

Comment ? Zero Trust Exchange commence par mettre fin à la connexion pour permettre une inspection en profondeur du contenu, y compris le trafic chiffré, en exécutant une analyse approfondie des données et des menaces. Il détermine ensuite l'identité et l'appareil et vérifie les droits d'accès à l'aide de politiques d'entreprise basées sur le contexte, notamment l'utilisateur, l'appareil, et l'application et le type de contenu demandés. Une fois la politique d'entreprise vérifiée et appliquée, Zero Trust Exchange établit la connexion entre les ressources concernées. Les utilisateurs et les appareils sont connectés directement aux applications, jamais au réseau de l'entreprise.

En savoir plus

Pour en savoir plus sur Zero Trust et sur la façon dont Zscaler peut vous aider, consultez la page Zero Trust Exchange.

Sources

[1] *Rapport de transparence de Google* https://transparencyreport.google.com/https/overview?hl=fr
[2] *Zscaler Networks Security Survey 2020*
[3] *ESG Economic Validation Study 2021*

À propos de Zscaler

Zscaler permet aux entreprises de transformer en toute sécurité leurs réseaux et leurs applications pour s'adapter à la prédominance mobile et cloud du monde actuel. Zscaler connecte les utilisateurs aux applications et aux services cloud, quels que soient le périphérique utilisé, l'emplacement de l'utilisateur ou le type de réseau, tout en offrant une sécurité sans faille et une rapide expérience utilisateur. Et le tout, sans appliances de passerelle complexes et coûteuses.

zscaler™