Akamai

LIVRE BLANC

Repenser les pare-feu

Arguments économiques convaincants en faveur de la segmentation logicielle

Synthèse

Pourquoi les équipes réseau et de sécurité continuent-elles d'utiliser d'anciens pare-feu pour réaliser une segmentation de réseau interne ? Alors que les applications et segments protégés par des règles prolifèrent, les dispositifs de pare-feu physiques se révèlent trop complexes, peu flexibles et tout simplement inefficaces pour relever les défis de sécurité des environnements de cloud hybride actuels de plus en plus dynamiques. Cela revient également beaucoup plus cher que les équipes ne le pensent. Mis à part le coût initial conséquent des pare-feu et du matériel, il existe d'importants coûts en aval liés à la gestion des projets, à la main-d'œuvre, à la maintenance et au risque très réel d'exposition prolongée des ressources en raison des longs délais de mise en œuvre. Si les entreprises d'aujourd'hui veulent tirer parti du modèle DevOps agile, du déploiement rapide des applications et du cloud, elles doivent trouver un meilleur moyen de sécuriser les ressources critiques avec la segmentation. Et c'est le cas avec la segmentation logicielle. Plus facile, plus rapide et plus efficace, elle offre une sécurité optimale à un coût total de possession bien inférieur à celui des méthodes de segmentation traditionnelles, comme le démontre clairement ce document.

Introduction

Aujourd'hui, nous voyons un faisceau de trois forces convergentes stimuler la demande en matière de moyens plus granulaires pour segmenter les réseaux et les ressources individuelles. Tout d'abord, les modèles DevOps agiles et autres modèles de distribution rapide exigent le déploiement accéléré des applications en production. Inévitablement, cela nécessite la création de zones plus sécurisées avec des règles plus précises. Ensuite, à mesure que les entreprises migrent vers le cloud et adoptent des infrastructures informatiques hybrides, leurs applications migrent souvent entre différents environnements, ce qui augmente le trafic intersectoriel sur l'ensemble de leur réseau. Enfin, la prolifération rapide des applications due au développement agile crée une surface d'attaque toujours plus grande pour les pirates informatiques.

Pare-feu pour la segmentation : une solution obsolète

Dans ce scénario, le recours strict aux réseaux VLAN et aux pare-feu à des fins de segmentation ne peut plus durer. D'un point de vue purement technique, la configuration de plusieurs installations VLAN et de pare-feu au rythme du développement des applications est à la fois complexe et fastidieuse. Elle nécessite en outre beaucoup de main-d'œuvre, détournant trop de membres de l'équipe des projets de sécurité prioritaires. Le délai de déploiement présente également un problème, car il augmente le risque de vulnérabilité et d'exposition prolongée des ressources. Et surtout, sa mise en œuvre est extrêmement coûteuse, non seulement en raison du coût initial des pare-feu et du nouveau matériel pour prendre en charge le trafic supplémentaire, mais aussi en raison des coûts associés à la gestion, aux modifications et à la maintenance continues des installations.

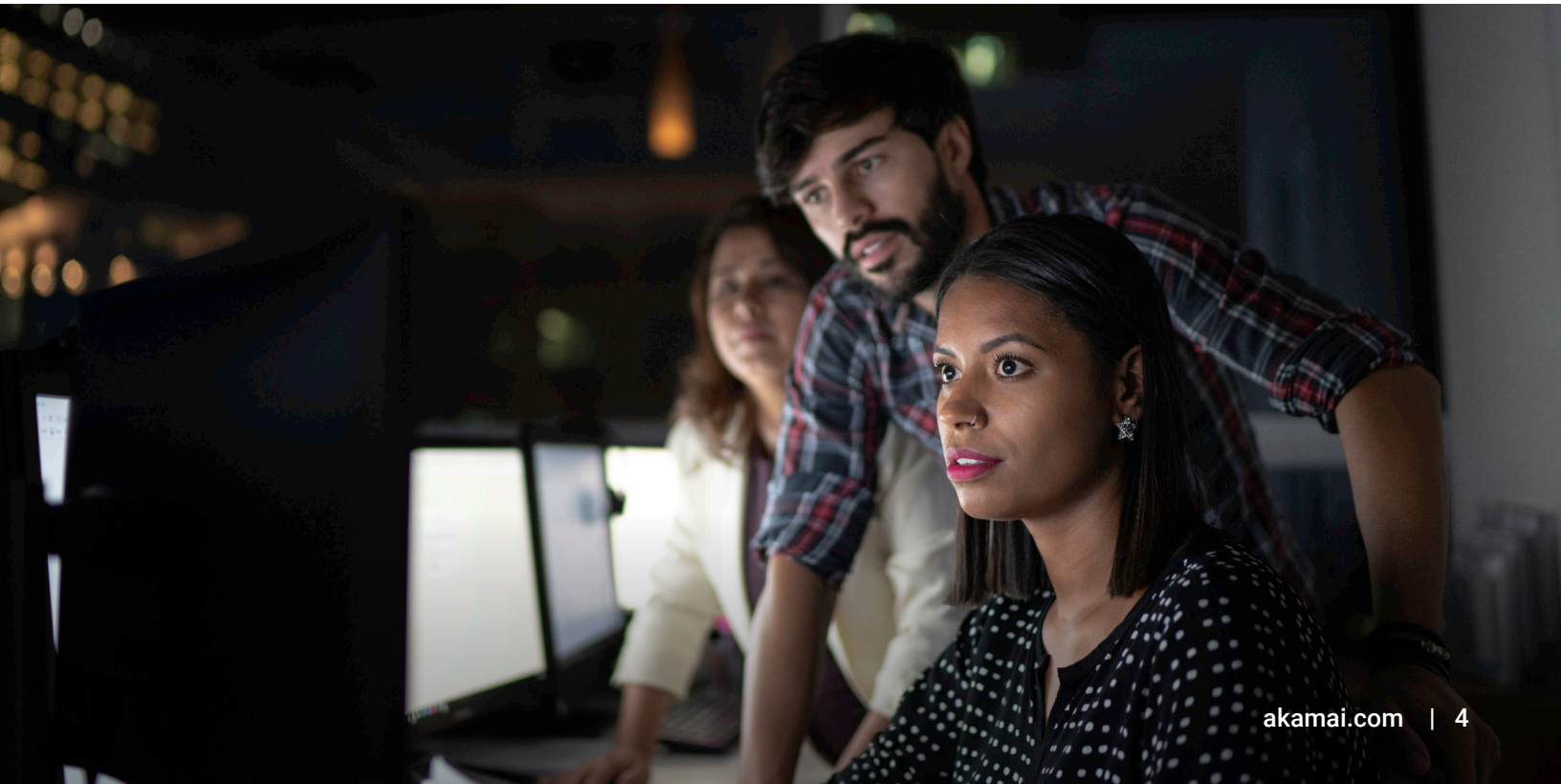
En termes simples, les approches traditionnelles de segmentation des réseaux ont atteint leurs limites. Lorsque les entreprises cherchent à tirer parti d'environnements hybrides et cloud dynamiques, le recours à des pare-feu internes pour la sécurité limite leur agilité, ralentit le processus de création et d'application des règles et les empêche de faire évoluer leurs opérations en toute sécurité. Le besoin d'une nouvelle alternative de segmentation rationalisée, moins coûteuse et finalement plus efficace aux pare-feu existants n'a jamais été aussi urgent. Entrez dans l'ère de la segmentation logicielle.

> Le besoin d'une nouvelle alternative de segmentation rationalisée, moins coûteuse et plus efficace aux pare-feu existants n'a jamais été aussi urgent.

Percevoir les difficultés : le coût élevé de la gestion des pare-feu

Avant d'explorer les avantages de la segmentation logicielle, il est utile de la comparer au statu quo. Au fur et à mesure qu'une entreprise évolue, le nombre d'applications et le volume de trafic de données associé augmentent également, stimulant ainsi la demande en matière de segments de réseau supplémentaires et de règles de sécurité plus complexes. Si vous utilisez des VLAN protégés par pare-feu, chaque nouveau réseau déployé doit être ajouté à chaque port de jonction de commutateur par lequel transite le trafic intersectoriel. Il est également nécessaire de mettre en place un sous-réseau IP pour chaque nouveau VLAN. Une sous-interface doit aussi être créée pour le pare-feu. Il faut ensuite créer des règles de pare-feu. Chacun de ces changements nécessite généralement des approbations, des fenêtres de maintenance et d'éventuels temps d'arrêt, ce qui signifie un risque accru de perturbations réseau.

L'ajout de VLAN et de pare-feu implique un processus laborieux en plusieurs étapes sollicitant l'intervention de cinq équipes au total, chargées de manière individuelle de la commutation, du routage, de la mise en œuvre des pare-feu, des serveurs ESXi et de la création de règles de sécurité. Tout cela vient s'ajouter aux longs délais de mise en œuvre, expose l'entreprise à des risques prolongés et augmente les coûts liés aux logiciels, au matériel et à la main-d'œuvre. De plus, du point de vue de l'ingénieur, il s'agit d'un processus à haut risque et peu rentable, qui demande beaucoup d'efforts pour très peu de bénéfices, laissant ainsi peu de temps et de ressources pour d'autres activités de gestion des risques prioritaires. Malheureusement, peu d'étapes du processus de gestion des modifications dans l'environnement VLAN protégé par pare-feu se prêtent à l'automatisation.



Trouver la solution : la segmentation logicielle en trois étapes simples

La technologie de pare-feu de périmètre existante n'a tout simplement pas été conçue pour répondre aux exigences plus précises et limitées en bande passante de la segmentation interne granulaire. La segmentation logicielle est apparue ces dernières années comme une alternative viable, plus rapide, plus efficace et moins coûteuse pour répondre à la demande croissante en matière de segments de réseau plus ciblés dans les environnements dynamiques d'aujourd'hui. Au cœur de la mise en œuvre de la segmentation logicielle se trouve le concept d'un « pare-feu distribué » qui est beaucoup plus agile et plus facile à gérer qu'un dispositif de pare-feu réseau traditionnel.

> La segmentation logicielle est **10 voire 20 fois plus rapide** à déployer qu'un pare-feu traditionnel, implique moins de personnes et n'entraîne pratiquement aucune interruption ou perturbation.

Akamai Guardicore Segmentation est un exemple de solution de segmentation logicielle de pointe. Par rapport au processus long, coûteux et complexe de mise en œuvre d'un pare-feu VLAN, notre solution de segmentation logicielle ne comporte que trois étapes :

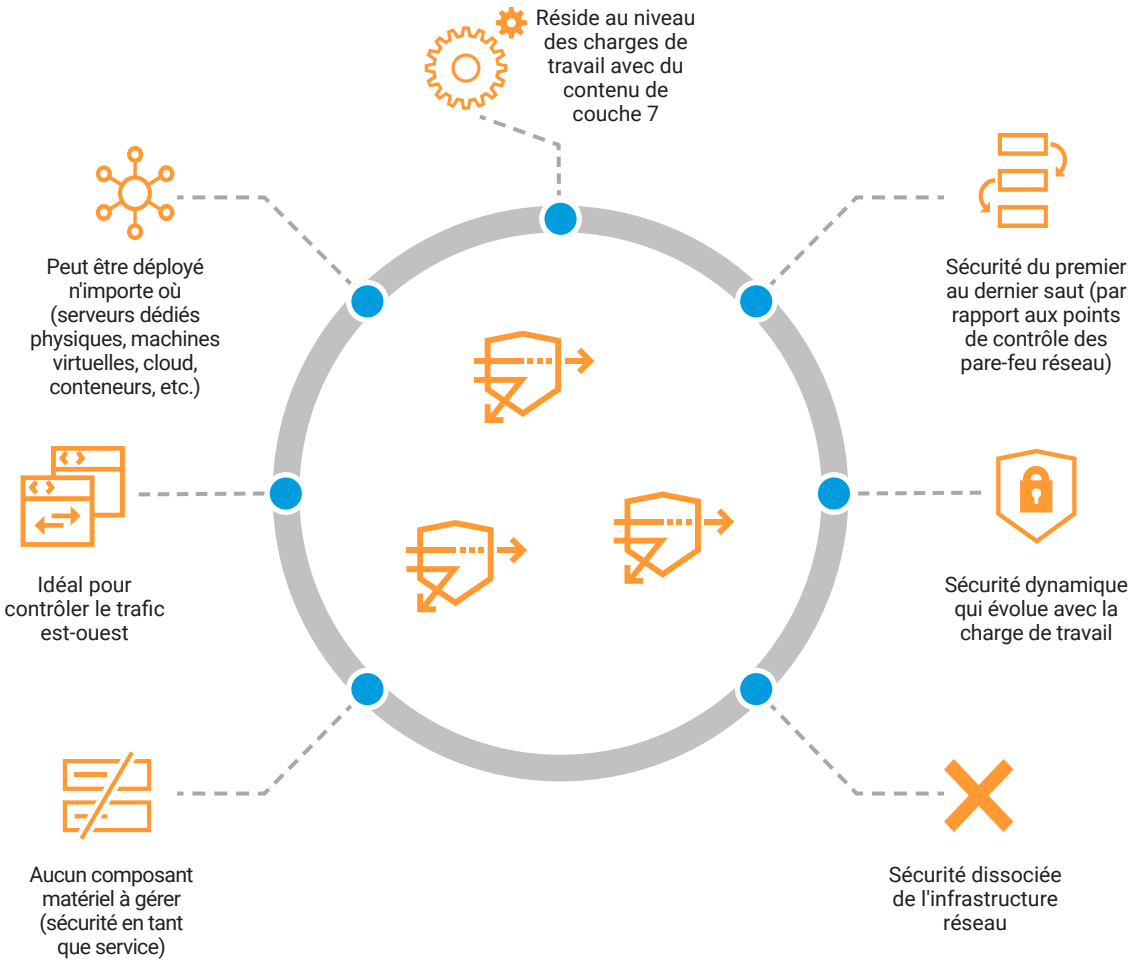
1. **Identifier et étiqueter les ressources :** un obstacle majeur rencontré au cours du processus traditionnel de mise en œuvre d'un pare-feu est le manque de visibilité sur les ressources qui doivent être sécurisées. Akamai Guardicore Segmentation inclut une fonctionnalité de visualisation qui permet aux opérateurs d'identifier et d'étiqueter toutes les applications et leurs dépendances exécutées dans l'infrastructure d'une entreprise.

2. **Visualiser et regrouper par étiquette :** une fois la visibilité contextuelle assurée, les opérateurs peuvent organiser les applications en groupes logiques en fonction de leurs étiquettes et mapper les dépendances entre elles. Notre processus d'étiquetage est très flexible et vous permet de regrouper des applications en fonction de votre propre contexte opérationnel, en utilisant une terminologie que vous connaissez déjà.

3. **Créer des règles :** les opérateurs peuvent ensuite créer des règles de sécurité granulaires qui indiquent quelles applications sont autorisées à communiquer entre elles en fonction des flux réels observés. Les modèles de règle prédéfinis pour les cas d'utilisation courants simplifient encore davantage le processus. Désormais, les applications et les flux de travail sont efficacement segmentés les uns des autres, quel que soit leur emplacement dans l'environnement.

La segmentation logicielle est 10 voire 20 fois plus rapide à déployer qu'un pare-feu traditionnel, implique moins de personnes et n'entraîne pratiquement aucune interruption ou perturbation. De plus, une fois que vous avez commencé le processus de visualisation et de segmentation, vous pouvez facilement diviser votre réseau ou ajouter différentes règles basées sur des étiquettes, automatiser les processus, gérer les incidents de sécurité et apporter des modifications rapides en réponse aux exigences métiers ou réglementaires.

Avantages d'un pare-feu distribué



Étude de cas - Une grande entreprise de transformation des aliments prévoit 85 % d'économies avec la segmentation

Une grande entreprise américaine de transformation de produits à base de porc devait segmenter 45 applications, avec une moyenne de cinq serveurs par application, déployées sur deux sites. Son objectif était d'éliminer ses réseaux plats, en évitant au maximum de perturber les services, et de mettre en place des règles le plus rapidement possible.

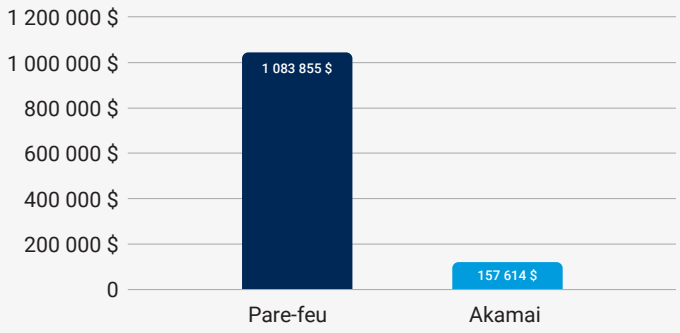
Après avoir examiné les alternatives disponibles, l'entreprise a choisi la solution de segmentation logicielle d'Akamai. Bien que la rapidité et la simplicité de mise en œuvre aient joué un rôle déterminant dans sa décision, c'est une analyse prévoyant des économies de plus de 900 000 $ (85 %) sur une période de trois ans, par rapport à la sécurisation des VLAN avec l'un des principaux fournisseurs de pare-feu, qui a fait pencher la balance. Plus précisément :

- Le coût de la licence Akamai Guardicore Segmentation était 55 % inférieur au coût du matériel nécessaire pour la mise en œuvre d'un pare-feu et d'un VLAN.
- Le coût de la main-d'œuvre (avec une base de 2 000 dollars par semaine) était 93 % inférieur avec Akamai à celui d'un projet VLAN d'une durée bien plus longue.

En outre, Akamai a répondu aux besoins du client en matière de mise en œuvre rapide des règles, en sécurisant 45 applications sans interruption en seulement six semaines.

Coût total de possession d'un pare-feu*
1 083 855 $
Coût total de possession de la solution Akamai*
157 614 $
- 926 241 $

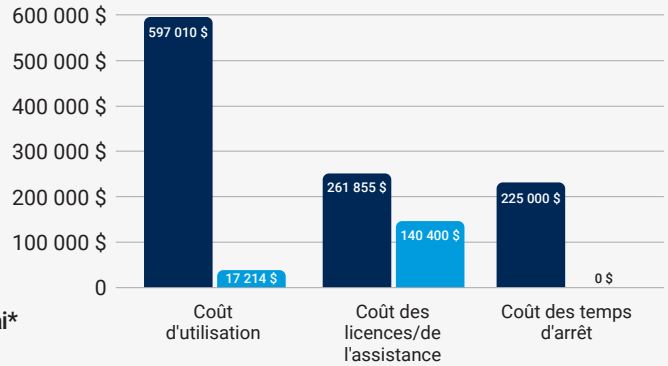
* Coût sur une période de 3 ans



Coût d'utilisation de la solution Akamai*
17 214 $
- 579 796 $

Coût des licences/de l'assistance de la solution Akamai*
140 400 $
- 121 455 $

Coût des temps d'arrêt de la solution Akamai*
0 $
- 255 000 $



Avantages

La segmentation logicielle offre trois avantages clés par rapport aux méthodes de pare-feu traditionnelles :

Réduction plus efficace des risques : en permettant une segmentation rapide des applications à un niveau très granulaire, la segmentation logicielle réduit considérablement la surface d'attaque. Appliquant les principes Zero Trust (authentification stricte de tout utilisateur, terminal ou application tentant d'accéder à une ressource réseau), la segmentation logicielle contrecarre les mouvements latéraux des menaces au sein du centre de données ou de l'environnement réseau. Cela atténue davantage l'impact des violations de données, les attaquants étant incapables de prendre le contrôle des processus, même s'ils ont réussi à franchir les défenses de périmètre. Cela permet également aux entreprises de se conformer plus rapidement aux réglementations exigeant l'isolement distinct des applications critiques et sensibles du trafic réseau général.

Vitesse pour une stratégie de sécurité optimale : en bref, la segmentation logicielle vous protège davantage, permettant plus rapidement aux équipes de sécurité de suivre le rythme du déploiement agile des applications DevOps et de s'assurer que chaque application en production est correctement sécurisée. Cela signifie également que moins de ressources (techniques ou humaines) sont affectées aux projets de segmentation pendant de longues périodes. Les équipes peuvent alors consacrer leur temps à d'autres initiatives importantes.

Coût total de possession considérablement réduit : il s'agit du véritable avantage, probablement le plus significatif d'un point de vue commercial. Une segmentation logicielle nécessite beaucoup moins de dépenses d'investissement (CapEx) pour une solution logicielle que lors de l'achat de dispositifs de pare-feu et de matériel supplémentaire. Cela se traduit également par des frais d'exploitation (OpEx) beaucoup plus faibles au fil du temps, sous la forme d'économies de main-d'œuvre et de ressources, pour assurer la maintenance et la gestion continues.

Grâce à ces seules mesures, une comparaison entre la segmentation logicielle et une solution de pare-feu pour 10 segments d'application montrait que l'approche d'Akamai permettait de réaliser 85 % d'économies au total, soit près de 1 million de dollars.

Bien entendu, même si l'on peut s'attendre à des économies significatives au cours de la première semaine de déploiement, le coût total de possession (TCO) est bien plus important que le simple prix d'achat initial ou les coûts continus. Bien que les étiquettes de prix total ne soient pas facilement visibles, la segmentation logicielle permet de réaliser des économies considérables en éliminant pratiquement les temps d'arrêt et les interruptions de service. En outre, les entreprises éviteront des pertes financières résultant de violations de données, ainsi que des sanctions pour non-conformité. Les risques d'atteinte à la réputation et de perte d'activité à la suite d'une violation sont aussi considérablement réduits. Les équipes et ressources informatiques chargées de la gestion des modifications de pare-feu peuvent être réaffectées à des projets plus productifs. Tous ces facteurs de coût contribuent à réduire le coût total de possession et à obtenir de meilleurs résultats pour ceux qui optent pour une solution de segmentation logicielle.

Étude de cas - Une grande banque internationale, sanctionnée pour non-conformité, se tourne vers Akamai Guardicore Segmentation

Suite à une évaluation mettant au jour les risques de sécurité dans ses réseaux plats, et face à un ensemble de nouvelles réglementations nécessitant une segmentation plus stricte, une grande institution financière européenne a initié un projet de segmentation utilisant des VLAN et des règles de pare-feu. Ce projet prenait beaucoup de temps, nécessitait l'intervention de plusieurs parties prenantes et équipes, et entraînait des temps d'arrêt de production et des ambiguïtés au niveau des règles. En conséquence, la banque payait des amendes pour non-conformité, qui s'ajoutaient à des coûts de mise en œuvre excessivement élevés.

L'équipe informatique a rapidement examiné des solutions alternatives et a été impressionnée par le niveau d'automatisation qu'Akamai pouvait apporter à ses opérations de sécurité. La banque a déployé Akamai Guardicore Segmentation dans plusieurs régions et types d'infrastructure informatique. Le projet a duré moins de trois mois, soit 10 fois moins longtemps que prévu initialement avec les méthodes de segmentation traditionnelles. La banque a non seulement mis à niveau sa stratégie de sécurité, mais a également répondu aux exigences de conformité pour plus de 10 000 ressources. Le déploiement rapide a permis d'accélérer la réduction des risques, mais aussi de réaliser des économies considérables en termes de coûts et de ressources internes.

Grande banque internationale

Cible du projet :

Séparation des environnements de développement, de production et de test d'acceptation utilisateur

Portée du projet :

1. Limitation du trafic entre les environnements de production et les autres environnements
2. Préparation du cloisonnement des applications

Segmentation existante

- Progrès extrêmement lents
- Échecs des évaluations, amendes et erreurs de production
- Interruptions de production dues à l'interruption des applications

Durée : 2 ans avec des pare-feu/VLAN

Impact de la solution Akamai

- 10 000 ressources non conformes segmentées
- Aucune interruption des applications
- Mise en œuvre 10 fois plus rapide
- Efforts manuels réduits avec le processus DevOps

Durée : 6 mois **Intervenants :** 3 architectes

Conclusion : faites le calcul

Les pare-feu ne sont pas obsolètes. Ils ont certainement un rôle à jouer dans la sécurisation du périmètre réseau. Mais dans les environnements dynamiques d'aujourd'hui, le périmètre est devenu un concept quelque peu informe. Pour trouver l'équilibre nécessaire entre sécurité et agilité, les entreprises doivent être en mesure de sécuriser leurs ressources digitales non seulement au niveau de la couche réseau 4, mais aussi de la couche applicative 7, en particulier les processus individuels. Dans ce cas, les pare-feu sont non seulement mal adaptés, mais font également obstacle au progrès. Toute tentative de segmentation granulaire avec des pare-feu pèse lourdement sur les ressources humaines, techniques et financières.

Comparée aux pare-feu, la segmentation logicielle a démontré sa capacité à réduire considérablement les risques de sécurité et le délai de rentabilisation global, avec un coût total de possession nettement inférieur à celui des approches traditionnelles, ce qui se traduit par un retour sur investissement plus important et plus rapide. Il ne s'agit pas d'une vision futuriste : la segmentation logicielle est d'actualité et offre déjà ces avantages aux organisations dans un large éventail de secteurs.

Étude sur l'évolution informatique

L'histoire des technologies s'est construite sur l'amélioration constante, la simplification et la baisse des coûts. La segmentation ne fait pas exception à la règle.

Prenons l'exemple des technologies de stockage qui, en à peine deux décennies, sont passées des disquettes aux clés USB, puis aux terminaux NAS (Network Attached Storage) et enfin au stockage dans le cloud. Ou celui des technologies d'exécution informatique, qui ont évolué des serveurs aux machines virtuelles, du Cloud Computing aux conteneurs, et finalement à l'informatique sans serveur. Dans chaque cas, les facteurs clés étaient la réduction des coûts et la flexibilité accrue. Et bien sûr, cela a été rendu possible grâce aux rapides progrès technologiques.

L'évolution de la segmentation, où l'on est passé de dispositifs de pare-feu physiques à des pare-feu distribués via des logiciels, une approche reposant sur l'abstraction du réseau, est similaire. Les facteurs sous-jacents sont également identiques, à savoir la réduction des coûts et la flexibilité accrue (ce qui se traduit par une rapidité de déploiement), tout en améliorant régulièrement l'efficacité des règles de sécurité grâce à une approche plus granulaire prenant en charge le Zero Trust.

Il est temps que les équipes réseau et de sécurité adoptent un nouveau modèle de sécurisation avec segmentation, comme elles l'ont clairement fait dans d'autres secteurs technologiques. Le pare-feu physique pour la segmentation connaît le même destin que la disquette.

Vous voulez voir notre solution en action ? Demandez une démonstration dès aujourd'hui sur le site suivant : akamai.com/guardicore

Akamai protège votre expérience client, votre personnel, vos systèmes et vos données en vous aidant à intégrer la sécurité dans tout ce que vous créez, dans toutes vos conceptions et diffusions. La visibilité de notre plateforme sur les menaces mondiales nous aide à adapter et à faire évoluer votre stratégie de sécurité (activer Zero Trust, bloquer les ransomwares, sécuriser les applications et les API, ou lutter contre les attaques DDoS), vous donnant ainsi la confiance nécessaire pour innover, prospérer et ouvrir le champ des possibles. Pour en savoir plus sur les solutions de sécurité, de traitement et de diffusion d'Akamai, consultez les sites akamai.com et akamai.com/blog, ou suivez Akamai Technologies sur Twitter et LinkedIn. Publication : 05/23.