Segmentation logicielle

Une approche à la fois interne et externe pour une sécurité de confiance

TABLE DES MATIÈRES

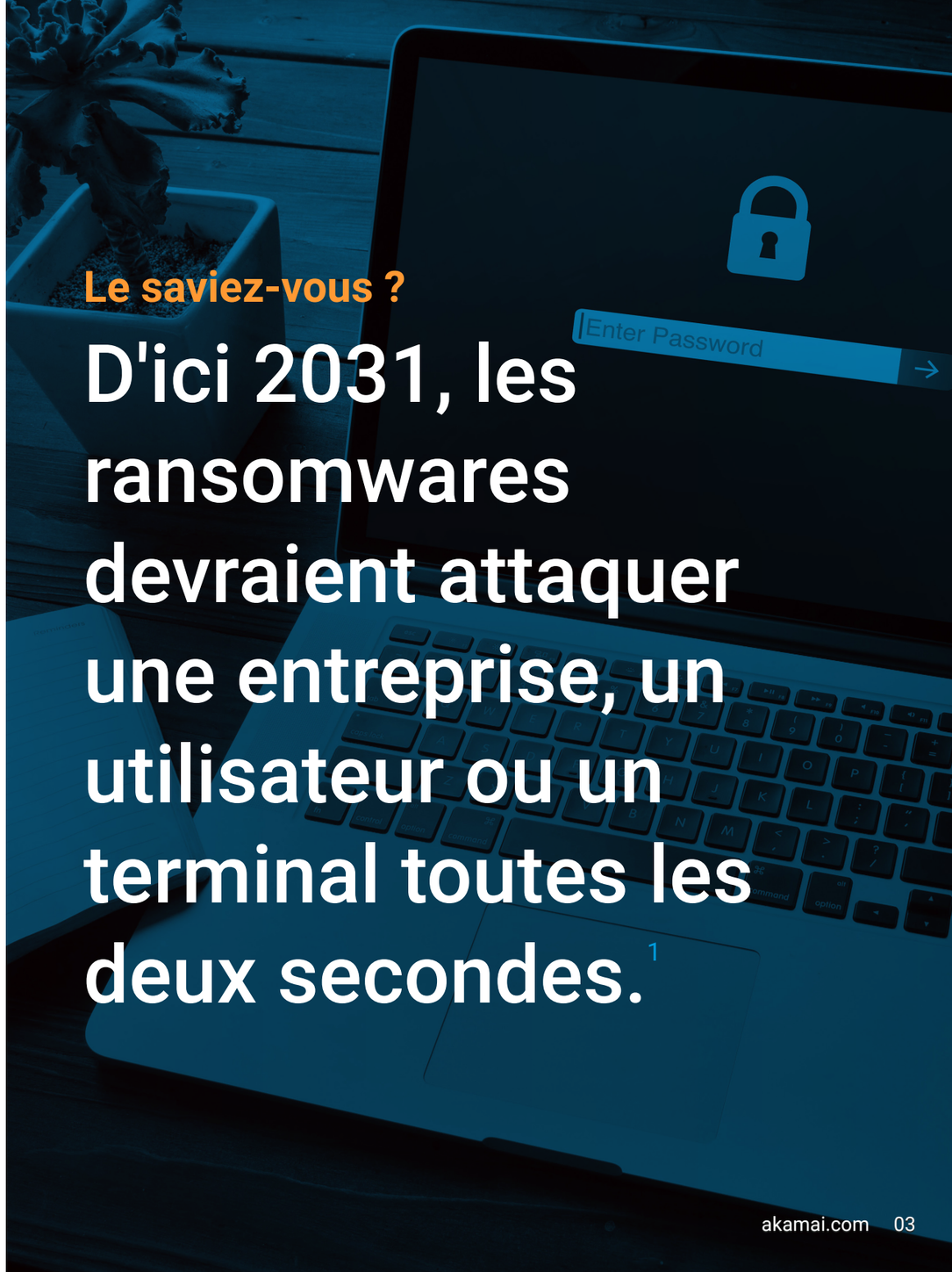
Abandonner les anciens pare-feu

Nous l'avons compris, vous en avez assez de vos anciens pare-feu sur site. Les environnements informatiques et les exigences en matière de sécurité ont évolué à des années-lumière de ce pour quoi ils avaient été conçus à l'origine. Le paysage de la cybersécurité a lui aussi évolué : les méthodes d'attaque deviennent de plus en plus sophistiquées et les cybercriminels sont plus nombreux que jamais. Une architecture datant de plusieurs dizaines d'années ne peut tout simplement pas résister aux logiciels malveillants, aux attaques de botnets, aux programmes d'hameçonnage, à l'ingénierie sociale et à l'extorsion de données d'aujourd'hui.

Or, malgré les nombreux problèmes qui leur sont associés (ils sont chers, immobiles et manquent de visibilité, entre autres), les anciens pare-feu ne vont malheureusement pas disparaître de sitôt. Ils ont une fonction importante au niveau du périmètre, car ils gèrent le trafic nord-sud et forment une protection rigide autour de l'organisation.

Toutefois, les pare-feu ne peuvent pas gérer le trafic est-ouest dans les centres de données sur site et dans le cloud.

C'est là que la segmentation logicielle entre en jeu.



Le saviez-vous ?

D'ici 2031, les ransomwares devraient attaquer une entreprise, un utilisateur ou un terminal toutes les deux secondes.[1]

Résolus !

Trois problèmes rencontrés avec les anciens pare-feu

1. Le problème : **Manque de visibilité**

   Le manque de visibilité sur le flux de données rend difficiles la mise en œuvre et la gestion des règles. Pour cette raison, les pare-feu ont souvent des jeux de règles extrêmement longs, parmi lesquels de nombreuses règles sont trop permissives ou même inutiles.

La solution

Recherchez des solutions qui intègrent une carte visuelle, une classification des ressources et un mappage des dépendances des applications à la création et à la gestion des règles.

Résolus !

Trois problèmes rencontrés avec les anciens pare-feu

2. Le problème : Les pare-feu sont difficiles à entretenir

Les propriétaires d'applications et les administrateurs de pare-feu connaissent rarement les protocoles et ports IP appropriés qui doivent communiquer entre eux. La gestion des pare-feu devient alors un processus de dépannage itératif.

La solution

Au lieu d'élaborer des règles relatives à la « plomberie » fixe du réseau, comme les IP et les ports, fondez-les sur des attributs significatifs comme le processus utilisé par une application, les noms de domaine pleinement qualifiés (FQDN) et l'identité de l'utilisateur. Ainsi, les attributs restent les mêmes et vos règles continuent de fonctionner, même si vous modifiez votre centre de données ou déplacez votre charge de travail vers le cloud.

Résolus !

Trois problèmes rencontrés avec les anciens pare-feu

3. Le problème : **Les pare-feu ne sont pas assez agiles**

   Les modifications que vous apportez à un pare-feu nécessitent généralement de planifier des temps d'arrêt. Lorsqu'un propriétaire d'application doit effectuer une modification, il est possible qu'il doive attendre une semaine ou plus pour que la modification soit examinée et mise en œuvre pendant une fenêtre de maintenance.

La solution

Les organisations informatiques d'aujourd'hui ont laissé tomber les fenêtres de changement au profit des modèles DevOps, où les applications apparaissent et se mettent à jour en permanence. Trouvez une solution technologique qui peut être automatisée à l'aide des mêmes outils DevOps que vous utilisez pour les applications elles-mêmes. De cette façon, l'approche de la sécurité s'adapte au fur et à mesure de l'évolution des applications.

Elle vous suit partout

Les solutions traditionnelles sont compliquées. Et elles ne sont pas flexibles. Avec l'approche traditionnelle, la segmentation des pare-feu est gérée depuis leur emplacement, qui ne peut pas être changé facilement. Elle repose généralement sur une adresse IP codée en dur ou acheminée vers un centre de données. Cela signifie que vous devez déplacer physiquement ce que vous voulez sécuriser derrière le pare-feu, un processus lent, cher en ressources et réfractaire au risque. Migration vers le cloud ? Visibilité ? Sécurité adaptée ? Oubliez tout ça.

Laissez vos anciens pare-feu là où ils sont. Prenez une profonde inspiration et adoptez la nouveauté. La segmentation logicielle peut être facilement mise en œuvre parallèlement à vos pare-feu existants, et elle est évolutive. Avec la segmentation logicielle, vous pouvez apporter des modifications à votre environnement, à votre centre de données et à votre réseau, mais aussi définir des règles en fonction de ce que vous voyez. De plus, la charge de travail et les règles sont accessibles partout : dans le cloud, le centre de données, n'importe où. Enfin, vous pouvez appliquer et adapter votre règle de sécurité sans apporter de modifications au réseau et sans interrompre le système.

Révélez vos segments internes

Pourriez-vous avoir confiance en quelque chose que vous ne voyez pas ? Bien sûr que non, direz-vous. Mais c'est pourtant ce que vous faites lorsque vous mettez en place des règles de sécurité derrière un pare-feu. Vous ne pouvez pas voir ce qui se trouve à l'intérieur. C'est comme regarder un bâtiment sans pouvoir voir les gens à l'intérieur.

La segmentation logicielle ne repose pas sur le hasard. Elle décompose les éléments, afin que vous connaissiez toutes les activités dans lesquelles vos charges de travail sont impliquées. Une fois que vous savez ce qui se trouve à l'intérieur de votre environnement, vous pouvez établir un plan et diviser les segments en parties significatives et efficaces en fonction de vos cas d'utilisation spécifiques.

Sécurité au-delà du périmètre

Les anciens pare-feu n'ont tout simplement pas été conçus pour être modifiés. Bien qu'ils jouent un rôle important au niveau du périmètre, comme la protection DDoS, ainsi que le filtrage et l'inspection du trafic, la sécurité à l'intérieur du réseau est difficile à gérer avec les pare-feu. Pourquoi ? Ils ont été déployés comme des points de contrôle naturels, ce qui fait que tout effort de segmentation se heurte à des barrages opérationnels, tels que le besoin de modifier et de supprimer des réseaux et des applications. Cela est fastidieux et coûte cher en ressources.

La segmentation logicielle peut vous aider à relever ces défis opérationnels et vous permettre d'appliquer vos pratiques de sécurité au-delà des points de terminaison et des périmètres. Tout d'abord, elle offre une approche de pare-feu distribué (par opposition au point de contrôle). Ensuite, elle se concentre sur la charge de travail, ce qui signifie qu'elle peut collecter des données auprès du système hôte, puis les appliquer à la classification des ressources et à une approche plus granulaire des règles, comme les règles et le contenu au niveau des processus. De manière générale, la segmentation logicielle est un moyen plus souple et plus granulaire de protéger les ressources critiques au sein de votre réseau. De plus, elle nécessite moins d'efforts et de ressources que les pare-feu.

Quatre principes de base de la segmentation

La segmentation n'a jamais été aussi importante. Les surfaces d'attaque s'agrandissent. Les attaques sophistiquées, comme les ransomwares, se déplacent latéralement après une violation, et vous devez penser aux dépendances des applications au-delà du périmètre. Mais la segmentation n'est pas une approche à étape unique.

Voici un aperçu de quatre types de segmentation courants, de leurs différences et des raisons pour lesquelles vous en avez besoin.

1. La segmentation de l'environnement

sépare les systèmes en différents environnements de développement, comme Développement, Assurance qualité, Staging et Production. Il s'agit d'une version étendue de la segmentation, dont l'objectif final est de séparer les systèmes en différents environnements pour garantir un accès limité uniquement aux utilisateurs et applications nécessaires. De nombreuses initiatives de conformité exigent une garantie que les systèmes hors production ne puissent pas accéder aux systèmes de production.

2. La segmentation du réseau

est une pratique architecturale consistant à diviser un réseau en plusieurs sous-réseaux, chacun étant son propre segment de réseau plus petit. La segmentation du réseau offre aux opérateurs informatiques un outil pour mieux contrôler le trafic réseau, stimuler les performances et améliorer la sécurité.

3. La microsegmentation

est une forme de segmentation plus granulaire, utilisée pour isoler les charges de travail les unes des autres et les sécuriser individuellement. Elle permet de définir des règles de segmentation pour des éléments comme des processus, des conteneurs, des utilisateurs, des noms de domaine et des terminaux. Cette approche est plus efficace pour contrôler le trafic est-ouest et assurer une protection contre les mouvements latéraux.

4. La segmentation basée sur l'identité

pousse encore plus loin que la microsegmentation les capacités de protection des points de terminaison, des terminaux, des charges de travail ou des conteneurs uniques grâce à des règles dynamiques évaluant l'identité de l'utilisateur, du terminal ou du contexte, afin de décider d'autoriser ou non la communication. Les règles de segmentation basées sur l'identité peuvent reposer sur des paramètres granulaires (et pas seulement sur l'adresse IP ou le port) comme les balises, le type de système d'exploitation ou les caractéristiques de l'application.

Mythes et réalités : cinq idées reçues sur la segmentation

Mythe 1

Les projets de segmentation sont trop difficiles à réaliser et prennent trop de temps.

Réalité : En ayant dès le départ une bonne visibilité et compréhension de votre environnement, la mise en place d'un projet de segmentation ne prend que quelques semaines, voire quelques jours, au lieu de plusieurs mois. Les technologies de segmentation d'aujourd'hui peuvent également utiliser l'IA pour accélérer davantage le processus.

Mythe 2

Les projets de segmentation nécessitent des modifications de l'infrastructure réseau et des temps d'arrêt.

Réalité : La segmentation logicielle dissocie la sécurité de l'infrastructure, de sorte que la segmentation peut être effectuée indépendamment de l'infrastructure sous-jacente, sans modification ni temps d'arrêt.

Mythe 3

La segmentation bloque le trafic légitime dans mon réseau.

Réalité : En visualisant votre environnement et en utilisant des règles de segmentation logicielles, vous pouvez observer leur effet sur les activités de votre entreprise avant de les activer en temps réel.

Mythe 4

La segmentation limite l'accès des utilisateurs et introduit une latence inutile.

Réalité : Utiliser des règles de segmentation logicielles distribuées au lieu de forcer tout le trafic à passer par des points de contrôle propres au pare-feu élimine les goulots d'étranglement du réseau. En outre, des règles plus précises, sensibles aux applications et identités, réduisent les problèmes d'accès utilisateur par inadvertance.

Mythe 5

Je ne peux pas utiliser les mêmes outils de segmentation dans le cloud que sur site.

Réalité : En dissociant les règles de segmentation de l'infrastructure, les règles utilisées dans le centre de données peuvent également fonctionner dans le cloud.

Akamai

Réduire les risques en interne

Des violations auront lieu. Et elles peuvent paralyser votre entreprise, compromettre vos données, endommager votre marque et vous coûter des millions.

Vous pensez toujours que les pare-feu sont suffisants ? Détrompez-vous. Après avoir infiltré un réseau, un environnement ou un centre de données, les attaquants ont recours aux mouvements latéraux pour voler des données et faire des dégâts, par exemple en prenant le contrôle des serveurs d'applications ou en accédant aux serveurs de bases de données.

En réalité, 70 % des attaques impliquent dorénavant une tentative de mouvement latéral.[2]

Tandis que les pare-feu considèrent les mouvements latéraux comme du trafic légitime se produisant au sein d'un réseau, la segmentation logicielle les détecte et les arrête immédiatement. Composante essentielle de votre programme de sécurité, la segmentation logicielle vous permet de limiter les mouvements latéraux et, en cas de violation, d'empêcher un attaquant de naviguer au sein de l'environnement. Vous avez ainsi une chance de protéger les données et les applications critiques, de réduire les temps d'arrêt et même de détecter l'attaquant. Cette approche est plus évolutive, plus facile à utiliser et vous permet d'implémenter rapidement la segmentation sans apporter de modifications à votre réseau ou vos systèmes.

Zero Trust n'est pas nécessairement compliqué

Avec Zero Trust, il s'agit de savoir qui fait quoi à qui, et comment. En d'autres termes, il s'agit d'avoir un contrôle explicite sur les actions de chacun au sein de votre réseau.

En donnant accès à un utilisateur à tout ce qui se trouve à l'intérieur du réseau, vous accordez automatiquement trop de confiance et, par conséquent, vous mettez en danger l'ensemble de votre entreprise. D'une part, les employés commettent souvent des erreurs, ce qui pourrait avoir des conséquences graves sur la sécurité. Certains sont même mal intentionnés.

D'autre part, en dehors des terminaux et réseaux VPN, vous devez prendre en compte de nombreux points d'entrée dans le centre de données. Par exemple, les attaquants peuvent pénétrer dans un réseau par le biais du serveur de production (comme ce fut le cas pour l'attaque contre SolarWinds), d'une application exposée à Internet mal protégée ou d'un VPN vulnérable. Dans ces cas-là, vous faites confiance à un serveur juste parce qu'il se trouve dans le réseau, alors que l'attaquant peut en pratique accéder à toutes vos ressources et se déplacer latéralement sans aucune contrainte.

Pour établir Zero Trust dans votre réseau de production, vous devez bloquer toutes les activités qui ne sont pas explicitement autorisées.

Les pare-feu existants ne sont tout simplement pas capables d'y parvenir à un niveau granulaire, car il faut identifier les attributs à un niveau plus profond que les ports et adresses IP.

À l'inverse, la segmentation logicielle vous permet de voir ce qui se passe en détail et de créer des règles précises et compréhensibles par l'homme, qui incluent l'identité.

Votre liste de contrôle Zero Trust : six façons d'obtenir un contrôle explicite

Faisons simple. La confiance doit dépendre de la taille du segment : plus un segment est petit, plus la protection des données, des ressources et des applications critiques est efficace. Voici six étapes pour mettre en œuvre Zero Trust sans difficulté opérationnelle.

1 Identifiez vos données sensibles à l'aide de libellés de visualisation.

2 Cartographiez les flux de vos données sensibles avec un mappage automatisé des flux et dépendances.

3 Élaborez vos micropérimètres Zero Trust à l'aide des outils adéquats pour définir rapidement toute règle de segmentation ou de microsegmentation.

4 Contrôlez en permanence votre écosystème Zero Trust avec une surveillance et des analyses en temps réel.

5 Adoptez l'orchestration et l'automatisation de la sécurité avec des API et des intégrations technologiques.

6 Disposez des capacités nécessaires pour révoquer la confiance en un utilisateur ou un périphérique. Ainsi, en cas d'attaque, vous pouvez facilement annuler la confiance envers n'importe quelle machine avec des attributs prédéfinis, quel que soit l'utilisateur ou le segment.

Akamai

Bilan

À présent, vous vous demandez probablement comment vous débarrasser de vos anciennes solutions pour renforcer la sécurité au sein de votre réseau.

Pas de problème.

Laissez vos pare-feu existants où ils se trouvent : ils protègent avec brio le périmètre du réseau. Mais leur rôle s'arrête là.

Ce qui compte le plus se trouve au cœur de votre organisation : vos ressources digitales, vos données et vos applications en dehors du périmètre, qui constituent le noyau dur de votre infrastructure d'entreprise. Le fait de ne plus se concentrer sur l'extérieur, mais sur l'intérieur, et de mettre en œuvre une segmentation logicielle et un cadre Zero Trust, vous apporte la visibilité et le contrôle dont vous avez besoin pour détecter et arrêter les mouvements latéraux, appliquer des règles granulaires et adaptables, et empêcher les cyberattaques, comme les ransomwares, de se propager dans votre réseau.

Demandez une démonstration ou **découvrez** les solutions de segmentation pour lutter contre les ransomwares, Zero Trust, la sécurité dans le cloud, et bien plus encore.

1 Cybersecurity Ventures. 2022 Who's Who In Ransomware Report. Conceal, 2022.

2 Kellerman, Tom et Greg Foss. Global Incident Response Threat Report. VMware Carbon Black, octobre 2020.

3 "2023 Cyber Security Statistics Trends & Data." PurpleSec, 22 février 2023.