POURQUOI LA MICROSEGMENTATION EST-ELLE ESSENTIELLE MAINTENANT ?

Isolez et protégez chaque charge de travail avec une rentabilité et une adaptabilité sans précédent

Les atteintes à la sécurité des Data Centers ne s'arrêtent jamais

Les atteintes coûteuses à la sécurité des Data Centers n'ont de cesse en dépit des efforts constants des équipes informatiques pour renforcer la sécurité. Jamais les équipes chargées de la sécurité n'ont été plus sensibilisées aux attaques malveillantes et pourtant les logiciels malveillants réussissent à se faufiler, en dépit des compétences internes et des investissements dans la dernière génération de pare-feu de périmètre. Cela n'arrive pas seulement de temps en temps, mais régulièrement.

Ces nombreuses atteintes à la sécurité s'expliquent par la sophistication accrue des logiciels malveillants conçus par les hackers. Or, au lendemain de la violation des données de Sony, force est de constater que les anciens modèles de protection n'arrivent plus à suivre le rythme. Les cybercriminels comptent sur le fait que la sécurité des Data Centers, même rigoureuse, reste basée sur d'anciens modèles dont ils connaissent bien les faiblesses.

Le coût d'une atteinte à la sécurité des données peut facilement se chiffrer à plusieurs millions, voire centaines de millions de dollars si l'on tient compte du rôle des analystes experts, des investigations menées en interne, des pertes de clientèle, du moindre taux d'acquisition de clients, ainsi que des propositions de crédits gratuits ou abonnements pour la surveillance des identités visant à susciter la confiance.

Il n'y a que peu de statistiques récentes sur les atteintes à la sécurité des Data Centers :

- Selon le rapport d'analyse des atteintes à la sécurité réalisé en 2015 par Verizon, en 2014 il y a eu 79 720 incidents de sécurité confirmés à travers le monde et 2 122 cas confirmés de compromission de données sensibles.
- Selon une étude réalisée en 2014 par Ponemon Institute portant sur les coûts associés aux atteintes à la sécurité, le coût total moyen des incidents de sécurité des données aux États-Unis était de 5,85 millions de dollars.

Les attaques visant des entreprises comme Sony, Anthem, Home Depot et Target présentent un point commun : après avoir franchi le périmètre, elles se sont propagées latéralement de serveur en serveur au sein du Data Center, sans qu'aucun des contrôles de sécurité en place soit en mesure de les stopper.

Au lendemain de la violation de sécurité ayant touché Sony Pictures Entertainment en 2014, il est apparu évident que les protections obsolètes jouaient un rôle plus important dans la réussite des attaques que la sophistication des logiciels malveillants. Selon Sean Gallagher, éditeur informatique chez Ars Technica, ce logiciel malveillant est un mélange de « différents codes brouillon ». Pourtant, les auteurs de ces codes sont parvenus à accéder à environ 100 To de données sensibles, à endommager des disques durs à l'aide de logiciels malveillants nettoyeurs et à provoquer des dommages estimés à 171 millions de dollars.

Pourquoi le modèle de sécurité du Data Center doit-il changer ?

Non seulement la sophistication des logiciels malveillants a été surestimée, mais la sécurisation du périmètre du Data Center a fait l'objet d'un intérêt disproportionné. L'étendue des dommages subis s'explique par le fait que les logiciels malveillants se propagent quasiment sans aucun contrôle une fois le périmètre franchi.

La question est : les modèles de pare-feu traditionnels axés sur le matériel peuvent-ils être utilisés pour protéger les charges de travail au sein du Data Center ? Trois modèles ont été proposés. Intéressons-nous à la commodité et à l'efficacité de chacun.

Pare-feu (de périmètre) physiques

Ce modèle repose sur le même type d'appliance que celui utilisé au niveau du périmètre, en se contentant de la déplacer à l'intérieur du Data Center. Les problèmes de cette approche sont notamment les suivants :

Coût prohibitif : Une fois qu'une attaque parvient à entrer dans le périmètre du Data Center, peu de contrôles latéraux empêchent les logiciels malveillants de se propager au sein des zones de confiance du Data Center. Forrester Research a recommandé l'adoption d'un modèle « zéro confiance », reposant sur des règles de sécurité associées à des charges de travail individuelles. Pour créer un modèle zéro confiance utilisant des pare-feu traditionnels, il faut utiliser un pare-feu séparé pour protéger chaque machine virtuelle (VM). Dans un Data Center d'entreprise standard, cela peut nécessiter le déploiement de milliers de pare-feu physiques. Les dépenses d'investissement sont prohibitives, sans compter l'espace rack, le chauffage et le refroidissement. Imaginez quel serait le coût de plusieurs Data Centers.

Charges d'exploitation et failles de sécurité : Le modèle zéro confiance impose par ailleurs de provisionner les règles automatiquement. Les pare-feu axés sur le matériel nécessitent de créer manuellement des règles de sécurité, et de procéder à des mises à jour manuelles chaque fois qu'une VM est créée, déplacée ou mise hors-service.

Il est possible de créer et de changer les ressources de calcul virtualisées en quelques secondes. La configuration manuelle des règles de pare-feu peut prendre plusieurs heures, voire plusieurs jours, en fonction des autres tâches dans la file d'attente de l'administrateur. Dans ces conditions, les mises à jour de règles non effectuées seraient à l'origine de vulnérabilités potentielles. La configuration manuelle est souvent source d'erreurs, provoquant des vulnérabilités accidentelles dans la sécurité.

Pour limiter la pression sur le réseau du Data Center, le budget et le personnel d'exploitation, les équipes en charge du réseau peuvent choisir de protéger les charges de travail les plus sensibles avec des pare-feu individuels. Dans ce scénario, une grande partie des charges de travail sont dépourvues de protection.

Incapacité à assurer la sécurité par microsegmentation : Les nombreuses contraintes associées aux pare-feu physiques ne permettent pas de mettre en place une sécurité micro-granulaire, ni même une sécurité macro-granulaire. Par exemple, il est impossible de protéger le trafic par pare-feu entre deux VM sur le même VLAN. Ainsi, même s'il s'avérait pratique d'assigner un pare-feu physique à chaque charge de travail, le trafic sur le même VLAN ne serait pas protégé. Un logiciel malveillant qui atteindrait une charge de travail sur un VLAN attaquerait toutes les charges de travail sur ce VLAN.

Mobilité limitée des applications : Grâce à la virtualisation des serveurs, les applications ne sont plus associées à un seul serveur physique dans un seul emplacement. Les départements informatiques peuvent facilement répliquer des applications sur un Data Center distant pour la reprise d'activité, les déplacer d'un Data Center d'entreprise vers un autre, ou les migrer vers un environnement Cloud hybride. Toutefois, les pare-feu physiques sont liés aux adresses IP et aux VLAN. Cela implique que les applications virtualisées ne peuvent pas tirer parti de la mobilité tant que le réseau n'a pas été longuement personnalisé par les concepteurs ou les architectes pour pouvoir déplacer les charges de travail d'un environnement réseau vers l'autre.

Pare-feu plus grands

Au lieu de déployer des centaines de pare-feu individuels (un pour chaque charge de travail), est-il envisageable de déployer un grand pare-feu capable de gérer plus de charges de travail ? Un tel pare-feu (pour le moment théorique) devrait être beaucoup plus grand que les pare-feu les plus grands actuellement sur le marché. Les inconvénients de cette solution sont notamment les suivants :

Coût prohibitif : On peut présumer que le coût d'un tel pare-feu serait bien supérieur à celui du pare-feu haut de gamme le plus onéreux. Outre le coût de chaque pare-feu, l'acheminement du trafic du serveur à travers ces pare-feu nécessiterait une bande passante supplémentaire.

Pertes de performances : Ce pare-feu théorique présenterait les mêmes problèmes qu'un pare-feu de périmètre concernant la protection du trafic d'est en ouest. La protection du trafic entre les VM implique de diriger le trafic d'un serveur vers le pare-feu, avant de le ramener vers le serveur de destination dans le Data Center. L'impact consécutif sur les performances serait considérable.

Mobilité limitée des applications : Les grands pare-feu présentent les mêmes contraintes que les pare-feu de périmètre en ce qui concerne la prise en charge de la mobilité des applications.

Pare-feu virtuels

Les pare-feu virtuels créent des pare-feu dans les logiciels, mais ils sont en réalité basés sur un modèle traditionnel axé sur le matériel. Les autres problèmes de cette approche sont notamment les suivants :

Coût prohibitif : Si les pare-feu virtuels éliminent certains pare-feu physiques, leurs licences logicielles restent coûteuses. En outre, la réduction des coûts d'exploitation associés aux pare-feu physiques n'est pas considérable, car une configuration manuelle est toujours requise.

Charges d'exploitation et failles de sécurité : Dans la mesure où les pare-feu virtuels n'associent pas les règles de sécurité aux charges de travail, les administrateurs réseau doivent toujours configurer manuellement les règles.

Les entreprises ont tenté d'implémenter la macrosegmentation à l'aide de pare-feu virtuels, mais cette technique crée elle aussi une grande surface d'attaque. La microsegmentation, qui est la sécurité précise requise par le modèle zéro confiance, n'est pas plus faisable avec des pare-feu virtuels qu'avec des pare-feu physiques.

Pertes de performances : En fait, le débit d'un pare-feu virtuel est inférieur au débit d'un pare-feu physique.

Mobilité limitée des applications : Les pare-feu virtuels sont associés aux adresses IP et aux VLAN comme le sont les pare-feu physiques. Ils limitent donc également la mobilité des applications.

Seule la microsegmentation, rendue possible par la virtualisation du réseau, satisfait tous les critères de mise en place d'un modèle zéro confiance dans le Data Center.

La microsegmentation est devenue possible grâce à la virtualisation du réseau

Pourquoi la microsegmentation est-elle un nouveau modèle plus efficace pour la sécurité des Data Centers ?

Isolation intégrée : Lorsque vous créez des réseaux virtuels, ils sont isolés les uns des autres sauf si vous décidez de les connecter. Aucun sous-réseau physique, aucun VLAN ni aucune liste de contrôles d'accès ou règle de pare-feu ne sont requis.

Sécurité complète : Les hyperviseurs sont distribués dans tout le Data Center, ce qui signifie que vous pouvez créer des règles de sécurité réseau qui sont mises en œuvre par les contrôles de pare-feu intégrés dans ces hyperviseurs. Ainsi la sécurité est omniprésente, dans tout le Data Center.

Sécurité granulaire : La microsegmentation permet d'assurer la sécurité au niveau de chaque charge de travail. Les règles de sécurité sont associées au réseau virtuel, aux VM et au système d'exploitation jusqu'à l'interface réseau virtuelle. Ainsi, la microsegmentation permet de recourir à des règles et des contrôles réseau à granularité fine.

Réduction des dépenses d'investissement : Vous n'avez aucune appliance de sécurité à acheter ni aucune modification à apporter à l'infrastructure matérielle sous-jacente. Vous n'avez pas à mettre à niveau du matériel propriétaire onéreux pour renforcer constamment vos fonctionnalités de sécurité, diminuant ainsi vos futures dépenses d'investissement.

Aucun impact sur les performances : En vous basant sur les fonctions traditionnelles du réseau matériel (commutation, routage, équilibrage de charge et pare-feu) et en les intégrant dans la couche de l'hyperviseur, vous sécurisez le trafic est-ouest entre chaque VM en conservant un débit très élevé. Vous n'avez pas besoin de recourir à un routage de trafic inefficace comme le « hairpinning », et vous évitez ainsi les pertes de performances associées à des tronçons inutiles.

Sécurité flexible : Grâce à la microsegmentation, vous pouvez créer et modifier les règles de sécurité en quelques secondes. Elles sont même automatisées : elles sont déplacées lorsqu'une VM est migrée et automatiquement supprimées au déprovisionnement d'une VM. La modification d'une règle n'interrompt pas les règles de sécurité déjà en place pour les autres charges de travail et applications, si bien qu'il n'y a aucun risque de conflits ou de brèches accidentels.

Voici deux exemples de cette flexibilité :

DMZ généralisée : Avec les modèles de sécurité axés sur le matériel, si un nouveau service ou une nouvelle application nécessite un accès Internet, il/elle doit être installé(e) et sécurisé(e) dans une partie précise de la topologie du réseau (appelée DMZ). La configuration des règles et de l'accès peut être source de longues discussions avec les parties prenantes. Avec la virtualisation du réseau, vous pouvez appliquer des concepts de sécurité DMZ à n'importe quelle charge de travail où qu'elle se trouve sur le réseau, ce qui permet de mettre ces applications en ligne plus rapidement pour soutenir l'activité.

Sécurisation des environnements utilisateur : Beaucoup d'entreprises ont déployé une infrastructure de postes de travail virtuels (VDI) pour exploiter les technologies de virtualisation au-delà du Data Center. La microsegmentation vous permet d'étendre les nombreux avantages liés à la sécurité du Software-Defined Data Center (SDDC) aux postes de travail, et même aux environnements de travail mobiles. La microsegmentation dissocie les règles de sécurité de la topologie du réseau pour simplifier l'administration. Les règles de sécurité sont plutôt attribuées par groupes logiques.

Résumé : Comparatif des solutions répondant aux exigences de sécurité du Data Center moderne

EXIGENCES DE SÉCURITÉ DU DATA CENTER	PARE-FEU PHYSIQUES	PARE-FEU VIRTUELS	GRANDS PARE-FEU	VIRTUALISATION DU RÉSEAU AVEC LA MICRO-SEGMENTATION
Prend en charge le modèle de sécurité du Data Center zéro confiance	Non	Non	Non	Oui
Assure une couverture polyvalente du Data Center	Non	Non	Non	Oui
Permet des règles de sécurité à granularité fine	Non	Non	Non	Oui

EXIGENCES DE SÉCURITÉ DU DATA CENTER	PARE-FEU PHYSIQUES	PARE-FEU VIRTUELS	GRANDS PARE-FEU	VIRTUALISATION DU RÉSEAU AVEC LA MICRO-SEGMENTATION
Élimine la nécessité de créer des sous-réseaux physiques, des VLAN, des listes de contrôles d'accès (ACL) pour isoler les réseaux ou les sous-réseaux les uns des autres	Non	Non	Non	Oui
Prend en charge un flux de trafic plus efficace, élimine le surprovisionnement de bande passante, maximise la performance des applications	Non	Non	Non	Oui
Réduit considérablement les charges d'exploitation	Non	Non	Non	Oui
Étend le cycle de vie de l'infrastructure matérielle réseau existante, réduisant les futures dépenses d'investissement	Non	Non	Non	Oui
Introduit un nouveau modèle économique (coût/performance de la sécurité)	Non	Non	Non	Oui
Prend en charge la mobilité des applications	Non	Non	Non	Oui
Automatise la fourniture de services informatiques et accélère la mise sur le marché	Non	Non	Non	Oui

Conclusion

Les dernières statistiques sur les atteintes à la sécurité des Data Center montrent que les pare-feu de périmètre ne sont toujours pas impénétrables. Toutefois, les cybercriminels misent avant tout sur ce qu'ils vont trouver derrière le périmètre : un modèle de sécurité axé sur le matériel qui n'a pas changé depuis des années.

Avant la virtualisation du réseau, il n'existait pas de moyen pratique de créer un nouveau modèle au sein du Data Center, capable de stopper la propagation latérale des logiciels malveillants. La microsegmentation est non seulement possible, mais elle fait partie intégrante de la virtualisation du réseau. La microsegmentation transforme la sécurité du Data Center en termes de rentabilité, de simplicité et de rapidité. Elle élimine les vulnérabilités anciennes sur lesquelles les cybercriminels se reposent pour perpétrer leurs attaques.

Pour en savoir plus sur la microsegmentation, téléchargez le guide Micro-segmentation For Dummies

En savoir plus sur la plate-forme de virtualisation du réseau VMware NSX® et sur la microsegmentation

vmware®

VMware, Inc. 3401 Hillview Ave Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com
VMware Global Inc. Tour Franklin 100-101 Terrasse Boieldieu 92042 Paris La Défense 8 Cedex France Tél. +33 1 47 62 79 00 www.vmware.fr