Sept points démontrant la puissance de la microsegmentation et la simplicité de sa mise en œuvre

LE DATA CENTER A BESOIN D'UN SYSTÈME IMMUNITAIRE PLUS RÉSISTANT

Les Data Centers subissent des attaques toujours plus nombreuses et les appliances de sécurité physiques ne suffisent pas à les arrêter. Une recherche indépendante a démontré que les attaques surviennent avec une régularité étonnante et sont toujours plus coûteuses pour les entreprises. Il ne fait aucun doute qu'un nouveau modèle est nécessaire pour la sécurité du Data Center si l'industrie ignore ces statistiques au lieu de les considérer comme des tendances inéluctables.

Les pare-feu de périmètre peuvent être de robustes gardiens à la porte du réseau. Cependant, lorsqu'un logiciel malveillant pénètre dans le Data Center (souvent en prenant en charge le trafic légitime), sa propagation n'a presque aucune restriction.

Le modèle de sécurité des périmètres est conçu pour fonctionner à la verticale, c'est-à-dire du client au serveur. Il n'est pas conçu pour prendre en charge le trafic horizontal, ce qui correspond au déplacement de la communication entre les serveurs. Techniquement ou économiquement parlant, il est impossible d'ajouter à un Data Center suffisamment de pare-feu physiques pour protéger des centaines et des centaines de charges de travail.

La sécurité complète, granulaire et dynamique doit faire partie de l'ADN du Data Center

La microsegmentation est l'un des avantages révolutionnaires de la plate-forme de virtualisation réseau VMware NSX™. NSX crée un réseau virtuel indépendant du matériel réseau IP sous-jacent. Les administrateurs peuvent créer, provisionner, réaliser des snapshots, supprimer et restaurer les réseaux complexes par programmation, via des logiciels.

Pour VMware, la microsegmentation est la possibilité d'« intégrer la sécurité dans l'ADN de votre réseau ». Par analogie, elle peut se comparer à la biotechnologie utilisée pour modifier les plantes aux niveaux moléculaire ou cellulaire de manière à ce qu'elles résistent aux parasites et aux maladies.

Les hyperviseurs étant déjà distribués dans tout le Data Center, VMware NSX permet de créer des règles à n'importe quel emplacement pour protéger tous les composants et offrir une sécurité vraiment complète. Dans un sens, la sécurité physique revient à utiliser des gants pour se protéger des microbes. Cette protection est externe et limitée (si quelqu'un éternue à côté de vous, vous allez probablement attraper son rhume ou sa grippe). La microsegmentation revient à fortifier le système immunitaire du Data Center : les microbes (ou les logiciels malveillants) ne peuvent pas l'atteindre. Et si un microbe parvient à le pénétrer, le système peut l'arrêter avant sa propagation.

Les règles sont liées aux machines virtuelles, avec une mise en œuvre complète jusqu'à la carte d'interface réseau virtuelle, ce qui crée une granularité elle aussi impossible avec les appliances matérielles traditionnelles.

Vous pouvez également définir les règles de sécurité à l'aide de paramètres flexibles tels que le nom de la machine virtuelle, le type de charge de travail et le type de système d'exploitation client.

Sept points démontrant la puissance de la microsegmentation et la simplicité de sa mise en œuvre

1. **Pas de suppression ni de remplacement de l'infrastructure en place**
   VMware NSX s'exécute sur n'importe quel matériel réseau : vous n'avez pas à acheter de nouvelles appliances ni à remplacer les appliances existantes. Par ailleurs, les applications et l'infrastructure informatique et de réseau ne subissent aucune interruption.
2. **Réduction des coûts matériels liés à l'évolution**
   Le coût du déploiement d'un plus grand nombre d'appliances physiques pour gérer le volume croissant des charges de travail à l'intérieur du Data Center est prohibitif. En ce qui concerne les dépenses d'investissement uniquement, VMware NSX permet aux entreprises de réaliser des économies de 68 %[1]. Ces économies sont basées sur l'estimation du coût des pare-feu physiques qui seraient nécessaires si les administrateurs informatiques essayaient d'atteindre plus ou moins le même degré de contrôle que celui de la microsegmentation.
3. **Réduction de la propagation des règles de pare-feu**
   La multitude des règles de pare-feu est un vrai problème pour la gestion de la sécurité. Avec le temps, les administrateurs peuvent hériter de règles inutiles et redondantes, sans qu'il y ait moyen de déterminer celles qui ne sont plus nécessaires. La propagation

[1] « Network Virtualization and Security with VMware NSX », livre blanc d'un dossier commercial ; analyse basée sur les coûts comparatifs à l'aide de la technologie de pare-feu.

des règles de pare-feu peut transformer les audits de sécurité en de véritables cauchemars. Les règles obsolètes ou en conflit les unes avec les autres peuvent même être source involontaire de vulnérabilités de sécurité.

Grâce à la microsegmentation et à VMware NSX, les règles sont orchestrées de manière centralisée et sont liées aux VM qu'elles protègent, ce qui permet d'automatiser la gestion des règles de sécurité dans l'intégralité du Data Center par l'intermédiaire d'une même interface. Lorsqu'une VM est provisionnée, déplacée ou supprimée, ses règles de pare-feu sont également ajoutées, déplacées ou supprimées.

4. **Réglage des performances grâce à des motifs de trafic plus efficaces**
   Dans les réseaux physiques, le trafic des charges de travail doit souvent traverser plusieurs segments de réseau pour atteindre les routeurs et les pare-feu, uniquement pour revenir à une charge de travail adjacente (ce motif inefficace est appelé agrégation). Grâce à la microsegmentation, le trafic reste généralement dans le même segment de réseau virtuel, ce qui réduit l'impact sur le réseau physique. Par conséquent, vous éliminez les coûts supplémentaires et les inefficacités associées au aux liaisons principales.
5. **Réponse aux besoins des différents secteurs d'activité et départements**
   VMware NSX et la microsegmentation fonctionnent indépendamment de votre infrastructure physique ; vous bénéficiez d'une flexibilité exceptionnelle dans le déplacement des ressources, car la sécurité suit tous les changements. La sécurité étant gérée par le logiciel, les règles peuvent être créées et opérationnelles en quelques minutes, ce qui élimine les délais associés à l'installation de matériels de sécurité supplémentaires ou à la reconfiguration des systèmes de réseau.

   Vous constaterez dans la figure 1 avec quelle simplicité vous pouvez mettre à jour les règles de sécurité afin de répondre aux besoins des différents secteurs d'activité et départements. Dans cet exemple, le département informatique a décidé de virtualiser les postes de travail des ressources humaines (RH). Grâce à la microsegmentation, la création et l'application de règles de sécurité pour les postes de travail virtuels des ressources humaines ne prennent que quelques minutes. Il vous suffit d'ajouter à tous les systèmes pertinents la balise « RH » pour que VMware NSX applique automatiquement les règles de sécurité correctes.

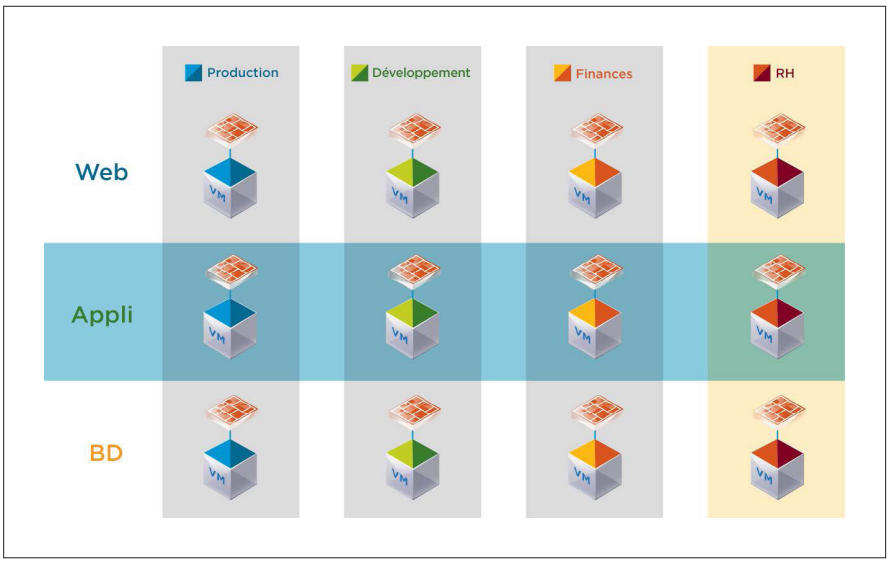

Figure 1 Grâce à la microsegmentation, la création d'une nouvelle règle basée sur la VDI ne prend que quelques minutes et n'implique pas le changement des autres règles déjà en place.

6. **Nouveau domaine de connaissances pour les spécialistes du réseau**
   Les administrateurs utilisent les compétences déjà acquises pour la virtualisation VMware, ce qui permet d'améliorer fortement la sécurité sans courbe d'apprentissage importante. Les spécialistes des réseaux matériels acquièrent de nouvelles compétences sur le logiciel qui leur permettent de rester à la pointe des technologies réseau logicielles et matérielles. Le développement d'une expertise en Software-Defined Data Center (SDDC) et en virtualisation réseau est un excellent atout qui vient s'ajouter aux compétences professionnelles des administrateurs et architectes réseau.
7. **Pérennité des opérations**
   La microsegmentation simplifie et accélère la sécurisation des charges de travail tout en réduisant son coût. Vous pouvez prendre en charge les changements avec plus de sérénité et même réallouer les ressources à de nouveaux projets.

   La virtualisation du réseau avec VMware NSX est également une étape importante, et sans interruption, vers le modèle du SDDC. Cela signifie que vous renforcez la sécurité aujourd'hui tout en jetant les bases du futur SDDC.

En savoir plus

Créez un environnement d'application fondamentalement plus agile, efficace et sécurisé grâce à la virtualisation de réseau VMware NSX sur une infrastructure de référence puissante composée de processeurs Intel® Xeon® et d'adaptateurs de réseau convergés Intel® Ethernet de 10 Go/40 Go.

Pour plus d'informations, rendez-vous sur www.vmware.com/fr/products/nsx. Pour obtenir des spécifications produit détaillées et connaître les configurations système requises, reportez-vous à la documentation VMware NSX.

VMware, Inc. 3401 Hillview Avenue 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