MICRO-SEGMENTATION EN FONCTION DU CONTEXTE AVEC VMWARE NSX DATA CENTER

Protégez le réseau contre la propagation latérale des menaces

Les applications modernes sont complexes, dynamiques et distribuées

Chaque organisation essaie de déterminer de quelle manière mener ses opérations au sein d'un monde hyperconnecté, axé autour des applications et des données. Les applications modernes sont distribuées sur plusieurs Data Centers et Clouds, et s'étendent à la périphérie de l'environnement.

L'apparition de la virtualisation, de DevOps, de la conteneurisation et des microservices ont permis d'accélérer la création et la modification des applications et ce, plus que jamais. La gestion de la sécurité devient une réelle gageure, car les applications modernes sont désormais distribuées et évoluent à une rapidité incroyable.

Les stratégies de sécurité legacy ne sont plus efficaces

Alors que la prolifération des applications se poursuit, les approches de sécurité legacy, centrées sur le périmètre, ne suffisent plus à protéger les applications et les données. Les pirates informatiques l'ont montré : ils peuvent pénétrer n'importe quel périmètre de sécurité, ou contourner les règles de sécurité périmétrique comme ils le souhaitent. Une fois à l'intérieur de ce périmètre, ils peuvent se déplacer latéralement, de serveur en serveur, sans être dérangés, afin de rechercher toute information pouvant être volée ou bloquée contre une rançon.

Dans un monde axé sur les applications modernes et distribuées, les équipes chargées du réseau et de la sécurité informatique ont souvent des difficultés à gérer les règles de sécurité, généralement disparates, appliquées à différents niveaux de l'environnement. Cela génère des incohérences au niveau de la posture de la stratégie sécuritaire.

Une sécurité constante, du Data Center vers le Cloud et la périphérie

Grâce à VMware NSX® Data Center, il est possible de définir des règles de sécurité de manière cohérente sur l'ensemble de l'environnement, quels que soient le type de l'application ou l'emplacement dans lequel elle a été déployée. Chaque règle est appliquée au niveau de la charge de travail, ce qui permet la segmentation des charges se trouvant sur un même hôte physique. Vous n'avez pas besoin de faire passer le trafic via un pare-feu virtuel ou physique externe. Ce niveau de sécurité granulaire est appelé « micro-segmentation ».

« Face à l'augmentation du nombre d'appareils IoT, plus le réseau est segmenté et plus nous sommes rassurés. De cette manière, les menaces ne peuvent pas se déplacer latéralement au sein du Data Center. »

CHRISTOPHER FRENZ
DIRECTEUR DE L'INFRASTRUCTURE INFORMATIQUE, INTERFAITH MEDICAL CENTER

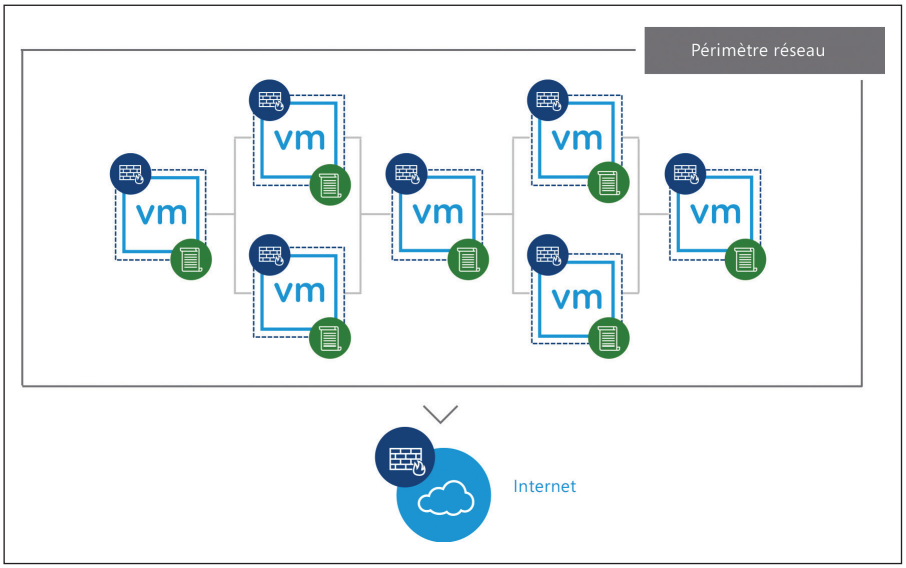

Figure 1. La micro-segmentation porte sur l'application des règles de sécurité du réseau au niveau de chaque charge de travail.

POINTS CLÉS

- Les fonctions de sécurité legacy, centrées sur le périmètre, ne suffisent plus pour gérer les applications, qui sont désormais distribuées et dynamiques par nature.
- VMware NSX Data Center permet à la micro-segmentation de protéger les applications contre la propagation latérale des menaces.
- Les règles de sécurité sont définies sur la base du contexte d'application, et appliquées au niveau de chaque charge de travail.
- Les fonctions de sécurité sont proposées de manière constante à partir du Data Center, vers le Cloud ou la périphérie.

Les micro-segments générés avec NSX Data Center sont définis et gérés par voie logicielle, ce qui les rend plus agiles et faciles à automatiser. Au fur et à mesure que les charges de travail sont déployées, elles héritent automatiquement des règles de sécurité associées à chacune d'elles tout au long de leur cycle de vie, quels que soient l'emplacement de leur provisionnement ou leur destination.

Micro-segmentation en fonction du contexte et sécurité alignée sur les applications et les données

La capacité à définir des règles de sécurité en fonction des facteurs les plus importants compte autant qu'une fourniture cohérente de ces règles. NSX Data Center dissocie chaque règle de sécurité des attributs du réseau statique tels que l'adresse IP, le port et le protocole, ce qui permet la définition de règles en fonction d'une bonne compréhension, en contexte, de l'application et de l'infrastructure. Ces contextes incluent les attributs relatifs à l'utilisateur, l'identité et la charge de travail (comme le système d'exploitation), voire la portée du respect de la réglementation.

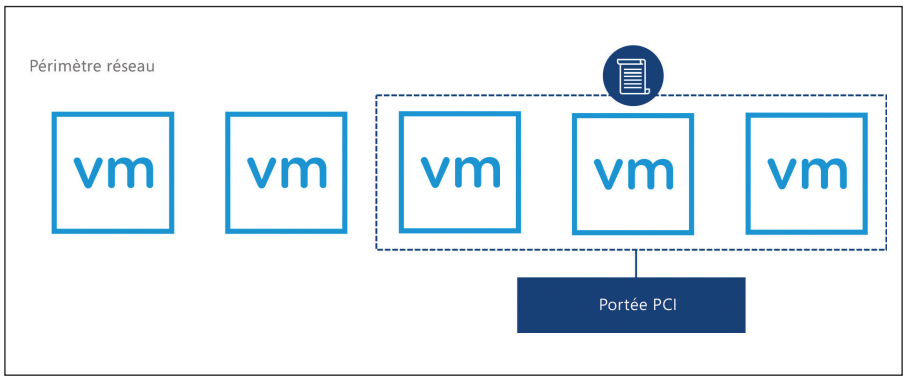

Figure 2. Les micro-segments créés dans NSX Data Center peuvent être définis selon des contextes différents, par exemple la portée du respect de la réglementation.

Grâce à la micro-segmentation en fonction du contexte, NSX Data Center offre aux équipes chargées de la sécurité du réseau la flexibilité qu'il leur faut pour sécuriser leurs applications et leurs données, en s'appuyant sur les facteurs les plus importants. Par exemple, vous pouvez utiliser ce logiciel pour sécuriser le déploiement d'une infrastructure de postes de travail virtuels (VDI) en appliquant une règle réseau basée sur le contexte de l'utilisateur au niveau de chaque session RDSH. Il est également possible d'appliquer des règles de sécurité à l'ensemble des charges de travail répondant aux normes PCI (Payment Card Industry), qu'elles se trouvent physiquement dans l'environnement ou non.

Des services de sécurité avancés disponibles au moment et à l'emplacement requis

Grâce à NSX Data Center, vous pouvez insérer des services de sécurité tiers avancés dans un micro-segment donné. Plutôt que d'acheminer l'ensemble du trafic réseau via un périphérique physique ou une appliance virtuelle, par exemple un pare-feu nouvelle génération (NGFW) ou un système de détection/prévention des intrusions (IDS/IPS), ce logiciel peut le rediriger de manière dynamique vers ces services au niveau de la couche du réseau virtuel. Ce faisant, il est possible d'insérer des services de sécurité avancés à l'emplacement requis, au bon moment, ce qui optimise l'efficacité du trafic réseau tout en améliorant les services de sécurité eux-mêmes.

Bénéficiez d'une plus grande visibilité sur le trafic du réseau à tous les niveaux de l'environnement

La première étape de la micro-segmentation consiste à appréhender le flux actuel du trafic réseau. VMware Network Insight™ offre une vision complète du trafic réseau au sein du Data Center, notamment celui du réseau virtuel et du réseau physique. Une fois le trafic réseau analysé, VMware Network Insight recommande automatiquement des règles de micro-segmentation pouvant être appliquées par NSX Data Center à des fins d'implémentation.

Bénéficiez dès aujourd'hui d'une évaluation gratuite de votre réseau virtuel, afin d'analyser le trafic réseau actuel et de commencer la planification de votre projet de micro-segmentation. Pour en savoir plus, consultez le site https://www.vmware.com/fr/products/nsx/security.html.

vmware®

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.com/fr