Livre blanc

Sécuriser le data center en cinq étapes : pourquoi les solutions de sécurité classiques ne fonctionnent pas toujours

Présentation

Les administrateurs de data centers font face à d'importants challenges. Ils doivent sécuriser les nouveaux environnements de data center sans en compromettre les performances ni le fonctionnement. Dans cette optique, nombre d'entre eux choisissent des solutions conçues pour la périphérie d'Internet, mais celles-ci ne suffisent pas. Les besoins des data centers sont uniques en matière de provisionnement, de performances, de virtualisation, d'applications et de trafic, et les dispositifs de sécurité à la périphérie d'Internet ne sont tout simplement pas adaptés à ces besoins.

Pour sécuriser le data center, la solution doit :

- Fournir la visibilité et le contrôle sur les applications de data center personnalisées
- Gérer les flux de trafic asymétriques et les transactions applicatives entre les appareils et les data centers
- S'adapter à l'évolution des data centers : virtualisation, software-defined network (SDN), virtualisation des fonctions de réseau (NFV), infrastructures axées sur les applications (ACI) de Cisco et plus encore
- Être efficace à chaque stade de l'attaque : avant, pendant et après
- S'intégrer avec les dispositifs de sécurité déployés sur tout le réseau
- Prendre en charge le déploiement et le trafic entre les data centers dispersés géographiquement, notamment les environnements cloud, publics et privés

La première victime du compromis : le data center

De nombreuses campagnes cybercriminelles modernes sont spécifiquement conçues pour aider les pirates à atteindre le data center, où résident des données précieuses comme les données personnelles des clients, des informations financières et la propriété intellectuelle de l'entreprise.[1] Mais la protection du data center représente un challenge. Trafic asymétrique, applications personnalisées, volumes de trafic élevés devant être dirigés hors de la couche de calcul et dans le périmètre du data center pour inspection, virtualisation sur plusieurs hyperviseurs et data centers éloignés géographiquement : autant d'éléments qui compliquent la protection du data center à l'aide de solutions de sécurité non adaptées. Résultat : le data center n'est pas intégralement sécurisé, ses performances s'en ressentent, il faut faire des compromis au niveau de ses fonctionnalités pour s'adapter aux limites de la sécurité, et le provisionnement complexe des solutions de sécurité affecte le provisionnement dynamique des ressources à la demande dans le data center.

[1] Rapport annuel 2014 de Cisco sur la sécurité : www.cisco.com/web/offers/lp/2014-annual-security-report/index.html?keycode=000350063.

Parallèlement, le data center évolue : du physique au virtuel, à des environnements nouvelle génération, comme les SDN et les infrastructures ACI. Le trafic du data center connaît déjà une croissance exponentielle, principalement en raison de l'utilisation grandissante du cloud et de l'émergence des environnements de l'Internet des objets (IoT). L'Internet et les réseaux s'invitent désormais dans les ateliers de fabrication, les réseaux électriques, les établissements de soins et les systèmes de transport.

Cisco prévoit que d'ici 2017, 76 % du trafic restera dans le data center et qu'il sera en grande partie généré par le stockage, la production et les données de développement des environnements virtualisés.[2] Le cabinet d'études Gartner prévoit quant à lui une augmentation de 3 000 % des connexions de data center par seconde d'ici la fin 2015.[3]

Les data centers d'aujourd'hui fournissent déjà une large gamme d'applications, de services et de solutions pour les entreprises. Nombre d'entre elles s'appuient sur des services déployés dans des data centers dispersés géographiquement pour gérer leurs besoins grandissants en matière de cloud computing et de trafic. Elles doivent également gérer des initiatives stratégiques telles que le traitement analytique du Big Data et la continuité de l'activité, qui font du data center un élément d'autant plus critique au cœur de l'entreprise. Mais cela fait également du data center une cible privilégiée pour les cybercriminels, qui conçoivent des stratagèmes de plus en plus sophistiqués et difficilement détectables pour accéder à ses ressources. En résumé, il va être encore plus difficile pour les équipes dédiées à la sécurité de surveiller et de protéger le data center.

Une autre complication pour les administrateurs de data centers et leurs équipes : les limites du provisionnement et des performances affectent le déploiement des solutions de sécurité telles que les pare-feu de nouvelle génération, et empêchent l'inspection de la totalité du trafic. La sécurité ne doit pas être assurée au détriment des performances du data center. Dans le data center d'aujourd'hui, le provisionnement d'une solution de sécurité doit s'effectuer en quelques heures, voire en quelques minutes. Il ne doit pas prendre des jours ou des semaines. Les performances doivent évoluer de façon dynamique pour qu'il soit possible de gérer les gros pics de trafic.

Sécuriser le data center en cinq étapes

La protection complète du data center nécessite une sécurité renforcée dans cinq domaines clés. La solution doit :

1. **Fournir la visibilité et le contrôle sur les applications de data center personnalisées.** Les administrateurs de data centers ont besoin d'une visibilité et d'un contrôle sur les applications de data center personnalisées, pas seulement sur les applications web classiques (Facebook et Twitter, par exemple) et les microapplications connexes inspectées par les dispositifs de sécurité à la périphérie d'Internet. La plupart des pare-feu de nouvelle génération sont conçus pour inspecter le type de trafic à la périphérie d'Internet ; ils ne protègent pas les applications de data center personnalisées.
2. **Gérer les flux de trafic asymétriques et les transactions applicatives entre les appareils ou les data centers.** La sécurité doit être réellement intégrée dans le fabric du data center. Les solutions de périphérie ne peuvent pas inspecter à la fois les flux de trafic nord-sud (entrant-sortant) et est-ouest (entre les applications), et ce dernier constitue le gros du trafic de data center d'aujourd'hui. Si le trafic des applications doit être envoyé pour inspection dans le périmètre du data center vers un pare-feu de nouvelle génération, puis redirigé vers la couche de calcul (hairpinned), la solution affecte le flux de trafic dynamique dont les data centers ont besoin.

[2] Cisco Global Cloud Index : prévisions et méthodologie, 2012-2017 : www.cisco.com/2012–2017/c/en/us/solutions/collateral/service-provider/global-cloud-index-gci/Cloud_Index_White_Paper.html.
[3] Security Week : http://www.securityweek.com/data-centered-focusing-security-combat-rise-data-center-attacks

De nombreux pare-feu de nouvelle génération sont incapables de sécuriser le trafic asymétrique. En cas de routage asymétrique, procédure standard dans les data centers, un paquet emprunte un chemin différent pour revenir à sa source. Cela pose problème à de nombreux pare-feu de nouvelle génération, car ils sont conçus pour suivre, inspecter et gérer les flux de trafic sur un chemin unique et prévisible.

Les solutions de sécurité dédiées au data center doivent également gérer les transactions d'application entre les data centers ou les appareils, y compris les appareils virtuels. Ceux-ci sont tout aussi vulnérables que les appareils physiques, mais la sécurité du data center doit également prendre en compte les challenges spécifiques des environnements virtuels, notamment la création, la suppression et la migration constantes des charges de travail.

3. **S'adapter à l'évolution des data centers.** Les environnements de data center passent du physique au virtuel, aux modèles de SDN, d'infrastructure ACI et de NFV nouvelle génération. Les solutions de sécurité doivent donc être capables d'évoluer dynamiquement et de garantir une protection homogène en toute transparence dans les environnements de data center hybrides et en pleine évolution. Dans ces nouveaux modèles de data center, les appareils virtuels et physiques sont provisionnés rapidement. Par conséquent, les règles de sécurité peuvent tout aussi rapidement devenir incontrôlables. La gestion des ACL (Access Control List, liste de contrôle d'accès) constitue déjà un challenge pour de nombreuses équipes IT.

   Les règles doivent être appliquées automatiquement en cas de provisionnement de nouveaux appareils afin de pouvoir réduire le délai de déploiement de plusieurs jours à quelques minutes, sans se préoccuper des conséquences pour la sécurité. De même, en déployant une solution de sécurité unique dans les data centers hybrides, dans de nombreux cas avec plusieurs hyperviseurs (moniteurs de machines de virtualisation), les équipes IT peuvent se consacrer à la fonctionnalité du data center et ne pas perdre leur temps à gérer les tâches administratives liées à la sécurité.

4. **Être efficace à chaque stade de l'attaque : avant, pendant et après.** Les approches classiques de la sécurité n'offrent qu'une détection limitée des attaques et une visibilité restreinte dans l'environnement de data center ; elles se concentrent principalement sur une protection au niveau périmétrique. Pour couvrir tout le spectre des attaques, il s'agit de se préparer à des angles d'attaque très variables : réseau, terminaux, terminaux mobiles et environnements virtuels. Les solutions de sécurité doivent pouvoir couvrir tous ces points d'entrée. Pour protéger le data center d'aujourd'hui et son trafic spécialisé, il faut adopter une approche holistique axée sur les attaques garantissant une protection avant, pendant et après une attaque.

   Les pare-feu de nouvelle génération classiques n'offrent pratiquement aucune solution pour l'identification et la gestion des attaques furtives conçues pour contourner les défenses, ils ne proposent ni action corrective, ni analyse après le blocage d'une attaque, et ils sont incapables de suivre et de sécuriser le type de trafic asymétrique généré par les data centers. Il ne s'agit presque exclusivement que d'outils de défense, mais ils ne sont pas capables non plus de protéger le système contre les nouveaux types d'attaque inconnus ciblant des serveurs vulnérables, des applications uniques et des données critiques.

5. **Protéger tout le réseau.** Toutes les solutions de sécurité du data center doivent prendre en compte le besoin des utilisateurs distants de se connecter directement aux ressources critiques d'un data center. Elles doivent assurer une liaison transparente entre ces utilisateurs et les ressources en question, dans un environnement réseau complexe passant dans les filiales, par le cœur, dans le data center et vers le cloud. La solution de sécurité doit faire partie de l'architecture du data center, mais aussi d'une solution plus large capable de détecter à la fois les attaques émanant d'Internet et les attaques de data center ciblées, tout en garantissant une protection transparente sur tout le chemin des données.

La sécurité du data center est différente. Pour véritablement protéger le data center moderne et les nouveaux modèles de data center, les entreprises ne peuvent pas se contenter d'un pare-feu de nouvelle génération. Elles doivent adopter une stratégie de sécurité complète et intégrée, ainsi qu'une architecture fournissant une protection homogène et intelligente sur tout le réseau distribué, de la périphérie au data center, jusque dans le cloud, sans nuire aux performances.

Sécuriser le data center moderne

Cisco propose des outils puissants pour protéger les environnements de data center en pleine évolution d'aujourd'hui, pas seulement leur périphérie. Les solutions innovantes Cisco® ASA (appliances de sécurité adaptatifs) pour la sécurité du data center sont conçues pour protéger les environnements physiques et virtuels et permettre aux entreprises de migrer en toute transparence d'un data center de nouvelle génération classique pour effectuer des déploiements pérennes, protéger les investissements et garantir la protection complète du data center. Les nouveaux éléments de la plate-forme Cisco ASA sont :

- **L'appliance virtuel de sécurité adaptatif (ASAv) :** version virtuelle de l'ensemble complet de fonctionnalités du pare-feu Cisco ASA, cet appliance offre une évolutivité dynamique et permet un provisionnement simplifié des environnements virtuels. Il est conçu pour s'exécuter sur divers hyperviseurs et ne dépend pas de la technologie VMware vSwitch. Il est ainsi compatible avec les environnements Cisco, hybrides et tiers. Grâce à son architecture flexible, le Cisco ASAv peut être déployé en tant que passerelle de sécurité classique et en tant que ressource de sécurité dans les environnements SDN et ACI intelligents pouvant être directement intégrés de manière dynamique dans les chaînes de services d'applications.
- **Le Cisco ASA 5585-X avec les fonctionnalités FirePOWER :** appliance de sécurité tout spécialement conçu pour le data center, prenant totalement en charge les environnements de data center classiques, SDN et ACI, l'appliance de sécurité adaptatif Cisco ASA 5585-X avec les fonctionnalités FirePOWER possède des fonctions de pare-feu avancées et de sécurité IPS nouvelle génération. Il permet notamment de détecter et d'inspecter les applications de data center personnalisées, tout en améliorant les performances et les fonctionnalités de provisionnement. Il offre également des fonctionnalités de clustering avancées (jusqu'à 16 nœuds), assurant un débit de 640 Gbit/s pouvant être déployé sur plusieurs data centers. Les solutions en cluster peuvent être gérées en tant qu'appareils uniques afin de réduire considérablement les tâches d'administration. Tout comme l'ASAv, le 5585-X est conçu pour fonctionner dans les environnements de data center classiques et de nouvelle génération (SDN, NFV et ACI), pour une sécurité homogène dans les environnements hybrides et une protection transparente pendant la migration des data centers.
- **Le système de prévention des intrusions nouvelle génération (NGPIS) Cisco FirePOWER :** leader sur le marché des NGIPS, FirePOWER est disponible sous forme de solutions physiques ou virtuelles. Il identifie et évalue les connexions aux ressources du data center, et il surveille les activités suspectes sur le réseau. Les activités sur les fichiers sont surveillées et contrôlées en temps réel, et certains fichiers (surtout les fichiers inconnus susceptibles d'être des programmes malveillants) subissent une analyse plus poussée en sandbox (analyse du comportement de fichiers dans un environnement isolé) ou recherches dans le cloud (vérification de la réputation dans l'ensemble des informations collectées par la communauté). Une telle approche permet une analyse et une réponse précises au niveau du trafic de data center critique.

D'autres solutions Cisco assurent la protection complète du data center :

- **Cisco ISE (Identity Services Engine) et TrustSec :** les équipes IT peuvent créer, partager et mettre en œuvre des politiques de sécurité de manière dynamique en cas d'ajout de nouveaux appareils ou utilisateurs dans l'environnement de data center via UCS Director. ISE peut ensuite attacher des balises de groupe de sécurité contenant la politique de sécurité et les règles d'application directement dans des paquets individuels. En outre, grâce à ces balises de sécurité, les data centers peuvent être segmentés en fonction du rôle des utilisateurs et des appareils sans les complications ni les frais supplémentaires associés aux VLAN et ACL.
- **La technologie Cisco OpenAppID pour Snort :** grâce à elle, les équipes IT peuvent créer, partager et mettre en œuvre un mécanisme de détection des applications et développer des règles spécifiques pour les applications personnalisées du data center. Il s'agit d'un langage de détection axé sur les applications et d'un module de traitement pour Snort™, le système de prévention et de détection des intrusions (IPS/IDS) développé par Sourcefire et appartenant aujourd'hui à Cisco. Cisco OpenAppID est entièrement intégré dans le cadre Snort. Cette technologie fournit aux administrateurs une visibilité bien meilleure sur les applications de leurs réseaux.

  Les utilisateurs Snort peuvent se servir des détecteurs Cisco OpenAppID pour détecter et identifier les applications et générer des rapports sur leur utilisation. Cisco OpenAppID fournit un contexte de couche d'applications avec des événements liés à la sécurité, améliore les analyses et accélère les corrections. Cette technologie permet à Snort de bloquer certaines applications détectées ou d'envoyer une alerte à ce propos, réduisant ainsi les risques en gérant l'attaque dans son intégralité.
- **Les solutions Cisco FireAMP™ et FireSIGHT™ :** une analyse et une protection avancées contre les programmes malveillants sont nécessaires lorsqu'une approche holistique axée sur les attaques est privilégiée pour sécuriser le data center moderne avant, pendant et après une attaque. Les produits Cisco FireAMP, de Sourcefire, exploitent le Big Data pour détecter, analyser et bloquer les malwares. Seule cette solution offre la visibilité et le contrôle nécessaires pour stopper les attaques qui échappent aux autres couches de sécurité. Et en combinant les produits Cisco FireAMP avec le Cisco ASA, les utilisateurs peuvent inspecter et protéger le trafic de data center asymétrique de manière approfondie.

  Cisco FireSIGHT, également de Sourcefire, offre la visibilité, le contexte et l'automatisation nécessaires pour s'adapter aux nouvelles conditions et répondre aux nouveaux types d'attaque. Les administrateurs peuvent gérer des centaines d'appliances de manière centralisée à partir de Cisco FireSIGHT Management Center.

Pour en savoir plus

Pour des informations complémentaires sur les produits de sécurité Cisco, notamment sur le pare-feu Cisco ASAv, l'appliance Cisco ASA 5585-X, la solution de data center sécurisé de Cisco et les solutions de sécurité Sourcefire, visitez www.cisco.com/c/en/us/products/security/index.html.

Pour en savoir plus sur Snort et Cisco OpenAppID, visitez www.snort.org.

Siège social aux États-Unis
Cisco Systems, Inc.
San José, CA

Siège social en Asie-Pacifique
Cisco Systems (États-Unis) Pte. Ltd.
Singapour

Siège social en Europe
Cisco Systems International BV Amsterdam.
Pays-Bas

Cisco compte plus de 200 agences à travers le monde. Les adresses, numéros de téléphone et de fax sont répertoriés sur le site web de Cisco, à l'adresse : **www.cisco.com/go/offices**.

Imprimé aux États-Unis C11-732259-00 07/14