SONICWALL®

PRÉSENTATION : 4 OBSTACLES À LA SÉCURITÉ DES CLOUDS PUBLICS ET PRIVÉS

Gros plan sur les pièges qui menacent la sécurité des environnements virtuels modernes

Résumé

La virtualisation et le cloud computing permettent de réduire les coûts tout en augmentant l'efficacité et l'agilité opérationnelle. Mais la menace émanant des logiciels malveillants va elle aussi croissant. Les services informatiques doivent gérer des budgets serrés pour la protection des environnements cloud publics/privés contre les pièges de sécurité les plus courants :

- Absence de visibilité du trafic entre les machines virtuelles
- Surabondance de règles
- Prolifération de machines virtuelles
- Contraintes des clouds publics

Les tendances en faveur de la virtualisation

Face à l'évolution rapide des marchés, une concurrence acerbe et un environnement commercial qui s'accélère, les entreprises doivent protéger leurs parts de marché et assurer leur croissance. Les technologies de l'information jouent un rôle plus que jamais central.

À l'arrière-plan, les services informatiques sont tenus de suivre le rythme des innovations technologiques, de moderniser les centres de données et l'environnement IT de manière générale, et d'optimiser leurs services pour assurer la réussite de l'entreprise. Concrètement, il s'agit de concevoir, de mettre en œuvre et de déployer de nouvelles applications efficaces, des outils et des services favorisant la productivité des utilisateurs et des architectures réseau telles que le cloud computing privé/public/hybride, le NFV (Network Function Virtualization) et la mobilité. Mais il est tout aussi important d'assurer l'assistance et la protection de cet environnement de réseau dynamique et d'un personnel mobile, le tout avec un budget identique voire réduit.

Vers l'extérieur, les services informatiques doivent pouvoir garantir que les engagements de l'entreprise sur le Web, ses services et son support sont disponibles 24 heures/24, 7 jours/7, 365 jours/an. Autrement dit, toute la présence de l'entreprise sur Internet doit être sécurisée et afficher des performances de pointe sans aucune interruption. Il faut donc un système de défense à la fois abordable et infaillible. Cela nécessite des fonctionnalités de sécurité dynamiques, capables de prévenir les attaques et de fournir les analyses nécessaires pour réagir et protéger l'infrastructure dans son ensemble, physique et virtuelle. Les services informatiques doivent être intransigeants en matière de sécurité, que ce soit sur le réseau câblé/sans fil ou le cloud privé/public, du siège aux sites distants, en passant par les succursales, les filiales ou les environnements de partenaires.

Atouts et bémols de la virtualisation

Depuis plus d'une décennie, la virtualisation des serveurs vise à faire passer la partie informatique de l'infrastructure du monde physique vers le monde virtuel. La virtualisation joue toujours un rôle de premier plan. Elle continue de faire évoluer et d'étendre les avantages opérationnels et économiques de l'ensemble du centre de données, réduisant les dépenses d'investissement et les coûts d'exploitation et permettant ainsi aux équipes de se concentrer sur l'infrastructure critique.

Le perfectionnement permanent des outils et services de virtualisation, à l'instar de la technologie NFV (Network Function Virtualization, ou virtualisation des fonctions réseau), permet aux services informatiques de développer et de placer facilement et rapidement des charges de travail virtualisées n'importe où dans le réseau virtuel. De plus, la virtualisation donne aux services informatiques de meilleures fonctionnalités de programmation et d'auto-gestion, ainsi que la vitesse de provisioning nécessaire à un fonctionnement plus efficace du centre de données. Cela permet aux équipes réseau et applications d'adapter et de fournir de nouveaux services, mais aussi de lancer, déplacer, copier, cloner, restaurer ou détruire instantanément ces services hébergés sur des machines virtuelles à tout moment pour répondre individuellement aux besoins opérationnels de leur centre de données. Cette agilité opérationnelle accrue et cette élasticité réduisent sensiblement les coûts liés à la fourniture de services applicatifs dans l'entreprise toute entière.

Mais en dépit de tous ces avantages, la virtualisation a aussi un côté sombre : ses nombreuses incidences sur la sécurité et autant d'inquiétudes que doivent gérer les services informatiques (voir le tableau 2 ci-dessous). Par nature, la virtualisation ajoute de nombreuses couches d'infrastructure et accroît la complexité sur le plan opérationnel. Divers aspects tels que l'utilisation partagée de stockage, les dispositifs de routage, les segments de réseau ou les canaux de communication se sont avérés vulnérables aux cyberattaques : abus de ressources partagées, attaques entre machines virtuelles ou de type side channel, ou encore les vulnérabilités réseau communes au niveau des protocoles et des applications. Ces menaces atteignent toutes les parties du framework virtuel, que ce soit l'hyperviseur ou le moniteur de machine virtuelle (VMM), les machines virtuelles (VM), les systèmes d'exploitation (OS) des VM, les applications exécutées sur ces systèmes d'exploitation ou les éléments réseau de l'environnement virtualisé. Une protection inadéquate de l'environnement virtuel peut causer des dégâts incommensurables au sein d'une entreprise.

Tableau 2 Rapports entre les vulnérabilités et les menaces dans les environnements réseau virtualisés

Catégories de menaces		Vulnérabilités	Menaces
Divulgation	Fuite d'informations	Manque de protection de la table ARP	Empoisonnement ARP
		Instauration de règles de pare-feu à l'intérieur de nœuds virtuels	Subversion des règles de pare-feu
	Interception d'informations	Manque de protection de la table ARP	Empoisonnement ARP
		Transmission de données selon des schémas prévisibles	Attaques fondées sur l'analyse du trafic
		Traitement incontrôlé de plusieurs requêtes consécutives d'un réseau virtuel par une seule entité	Inférence et divulgation d'informations topologiques sensibles
		Échange sans protection d'informations de routage entre routeurs virtuels	Divulgation d'informations de routage sensibles
	Exploitation de l'introspection des machines virtuelles	Introspection non contrôlée	Vol de données
Tromperie	Usurpation d'identité	Traitement inapproprié des identités :	
		– au sein de réseaux individuels	Infiltration de messages malveillants avec de fausses adresses
		– au sein de réseaux fédérés	Élévation des privilèges
		– lors de procédures de migration	Abus du retrait et du rajout de nœuds pour obtenir de nouvelles identités (propres)
	Perte d'entrées de registre	Opérations de rollback incontrôlées	Perte d'entrées de registre
	Attaques par rejeu (replay)	Absence d'identificateurs de message uniques	Attaques par rejeu (replay)
Perturbation	Surcharge des ressources physiques	Allocation de ressources incontrôlée	Dégradation des performances
			Consommation abusive de ressources
		Traitement incontrôlé de requêtes de réseau virtuel	Épuisement des ressources dans certaines parties de l'infrastructure
		Manque de stratégies de récupération proactive ou réactive	Attaques par déni de service
	Défaillance de ressources physiques	Manque de stratégies de récupération proactive ou réactive	Défaillance de routeurs/réseaux virtuels
		Réallocation incontrôlée de ressources après défaillance	Surcharge des routeurs virtuels restants après défaillance
Usurpation	Usurpation d'identité	Traitement inapproprié des identités et des privilèges associés	Élévation des privilèges
	Exploitation de vulnérabilités logicielles	Élévation des privilèges dans les moniteurs de machines virtuelles	Contrôle non autorisé de routeurs physiques

Source : « Virtual network security: threats, countermeasures, and challenges, » Journal of Internet Services and Applications, déc. 2015

Exemples de dommages :

- Prise de contrôle non autorisée de systèmes virtuels en vue de mener des actions malveillantes
- Accès non autorisé à des données protégées
- Vol d'informations
- Interruptions du service ou dégradation de tout ou partie de l'écosystème virtuel

Les vulnérabilités et les menaces liées à la virtualisation sont actuellement un sujet de recherche actif dans le monde universitaire, dans les domaines du bug bounty et de l'ethical hacking, mais également au sein des communautés du cybercrime organisé. De nouvelles menaces sont régulièrement découvertes. VENOM, CVE-2015-3456, fait partie de ces exploits qui touchent les plateformes de virtualisation courantes telles que Xen ou KVM.

Les services informatiques ont donc toutes les raisons d'être préoccupés par l'état actuel de la sécurité. Nombre d'entreprises s'inquiètent du manque de fonctionnalités et de contrôles de sécurité dynamiques des systèmes de défense actuels, pourtant indispensables pour protéger comme il se doit les infrastructures de réseaux virtuels. Difficile dans ces conditions de garantir la continuité des activités, la fourniture et la disponibilité des services ou encore la conformité avec les exigences réglementaires.

Cas pratique

Pour vous donner une perspective plus réaliste, examinons le scénario d'une entreprise possédant un environnement virtuel au sein d'une architecture de sécurité avec pare-feu physique. La figure 1 (en haut à droite) décrit le cheminement de la communication depuis la VM d'application vers la VM de base de données sur la VM hôte. Il pourrait s'agit d'une application Microsoft SharePoint effectuant une opération de lecture/écriture sur une base de données SQL. Dans ce cas de figure, le service informatique doit garantir que les services de l'application sont fournis en toute sécurité.

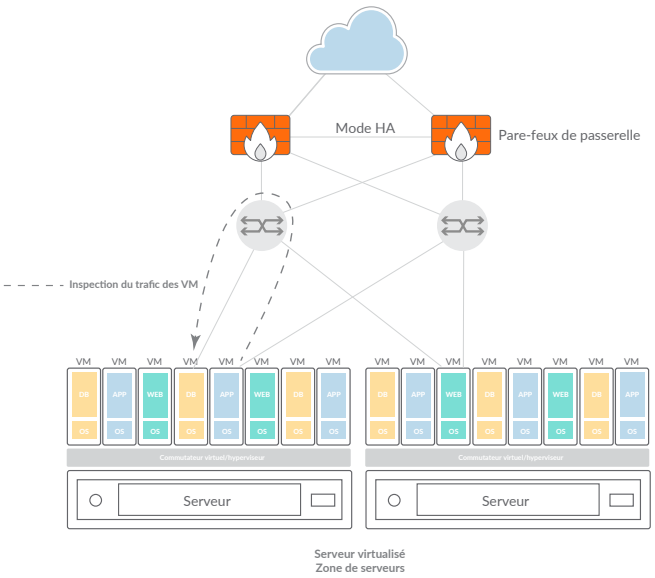

Figure 1 : environnement virtuel avec pare-feu physique

Environnement virtuel avec pare-feu physique

Deux types d'inspection sont possibles avec les méthodes héritées. Le premier consiste à acheminer le trafic d'une machine virtuelle à l'autre via le commutateur virtuel (vSwitch) vers la matrice de commutation externe (nord), puis vers un pare-feu externe qui reprendra le même canal en sens inverse (sud). Dirigé de cette manière, le trafic fait plusieurs détours, ce qui peut engendrer des problèmes tels qu'une dégradation des performances, de la latence, la perte de paquets et des difficultés à contrôler la sécurité, comme nous l'avons évoqué plus haut. La deuxième possibilité est d'utiliser un pare-feu logiciel exécuté comme agent au niveau de chaque machine virtuelle. Cette méthode présente des problèmes similaires, avec des performances médiocres et un surcroît de complexité dès lors que le nombre de VM augmente.

Lorsqu'il s'agit de gérer la sécurité en présence de pare-feux physiques dans un environnement virtualisé dynamique, les pièges régulièrement rencontrés sont les suivants :

1. Absence de visibilité du trafic entre les machines virtuelles
2. Surabondance de règles
3. Prolifération de machines virtuelles
4. Environnement de cloud public

Absence de visibilité du trafic entre les machines virtuelles

Quand vous avez des dizaines de machines virtuelles qui communiquent entre elles, un pare-feu de périmètre physique n'a pas de vue sur le trafic latéral, dans la mesure où ce trafic ne sort jamais de ce serveur virtuel en raison de l'isolation des machines virtuelles ou de configurations de routage. Du point de vue sécurité, cela veut dire qu'il est impossible de surveiller les événements inhabituels et les anomalies dans ces cas de figure.

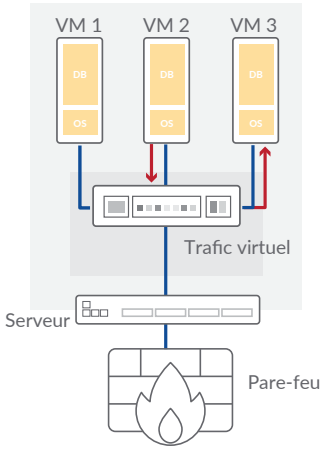

Figure 2 : trafic entre machines virtuelles

Surabondance de règles

Lorsque vous créez ou déplacez des actifs virtualisés, il y a un certain nombre de modifications complexes à effectuer dans la configuration réseau pour aiguiller le trafic des machines virtuelles vers le pare-feu physique. Cela implique des règles de routage et NAT, ainsi que des ports et des protocoles compatibles avec l'application. Selon les directives de gestion des changements, les modifications de règles doivent subir un processus manuel et laborieux d'examen, d'approbation, d'audit et de test avant de pouvoir être mises en œuvre. Une démarche extrêmement inefficace, éprouvante et coûteuse de par le nombre de personnes impliquées.

Or, à force d'ajouter de nouvelles règles à des centaines d'autres règles obscures qui n'ont peut-être jamais été vérifiées et acceptées, les politiques de sécurité deviennent confuses et ingérables. Des lacunes peuvent apparaître et s'amplifier, des menaces passer inaperçues et les performances chuter.

Prolifération de machines virtuelles

La prolifération de machines virtuelles est un problème courant où le nombre d'actifs virtuels au sein d'un environnement atteint un point tel qu'il devient trop difficile d'assurer leur suivi et leur contrôle. Lorsque des machines virtuelles sont copiées, clonées ou déplacées (et souvent arrêtées puis oubliées), cela crée des risques et rend l'environnement vulnérable, les règles et contrôles de sécurité étant alors dissociés. Or, il est impossible de fixer une règle de sécurité à une adresse IP statique, puisque les adresses IP de machines virtuelles changent régulièrement. Il s'agit là d'un problème très répandu et largement exploité par les pirates. Par conséquent, un environnement virtuel dynamique a besoin de contrôles de sécurité dynamiques et d'un processus de changement étroitement régulé et vérifiable, afin de garantir que les machines virtuelles sont soumises aux bonnes règles de configuration et de sécurité.

Environnement de cloud public

Un autre cas problématique est celui où les services applicatifs d'une entreprise sont hébergés dans le cloud public, par exemple dans Amazon Web Services (AWS) ou Microsoft Azure. En tel cas, le service informatique d'une entreprise ne peut pas placer de pare-feu physique dans le centre de données sécurisé du fournisseur. Ce sont des installations extrêmement contrôlées et, admettons qu'un pare-feu physique puisse y être placé, celui-ci ne pourrait pas simplement dicter le modèle de trafic de manière à voir le trafic applicatif de l'entreprise. Le pare-feu doit donc lui aussi être virtuel. Le service informatique pourra opter pour un SDN (Software-Defined Networking, ou réseau à définition logicielle) ou pour des configurations manuelles d'ingénierie du trafic pour placer le pare-feu virtualisé entre ses services applicatifs et le reste du monde, que le cheminement soit à l'intérieur ou à l'extérieur du centre de données.

Conclusion

La sécurité est un facteur clé dans toute analyse coût/bénéfice d'une initiative de virtualisation. Les avantages en termes d'économies et d'efficacité doivent être évalués à l'aune des dommages potentiels liés à l'augmentation des menaces et aux pièges courants. Les services informatiques doivent examiner de nouvelles solutions au-delà des approches héritées et se tourner vers des technologies capables de vraiment garantir la sécurité de la virtualisation.

Pour en savoir plus : lisez notre dossier « Comment évaluer un pare-feu virtuel de nouvelle génération » et consultez la page www.sonicwall.com/virtual-firewall.

À propos de nous

SonicWall s'engage depuis plus de 25 ans dans la lutte contre la cybercriminalité, défendant PME et grands comptes dans le monde entier. Notre alliance de produits et de partenaires nous a permis de mettre sur pied une solution de cyberdéfense en temps réel, adaptée aux besoins spécifiques de plus de 500 000 entreprises dans plus de 150 pays, leur permettant de se concentrer sans crainte sur leur cœur de métier.

Pour toute question concernant l'usage potentiel de ce document, contactez :

SonicWall Inc.
1033 McCarthy Boulevard
Milpitas, CA 95035

Consultez notre site Internet pour plus d'informations.
www.sonicwall.com