Jérémy D'Hoinne, Gartner : « pour le SDN, la sécurité n'est pas prête »

Il y a quelques semaines, Gartner alertait les entreprises des dangers du Software-Defined Network (SDN), qualifié par le cabinet américain de « *véritable mine d'or pour les pirates informatiques* ». Pour le Gartner, ce constat ne remet pas fondamentalement en cause le développement futur du SDN qui, en centralisant les données sur une plateforme unique pour les redistribuer ensuite sur les switchs appropriés, doit aboutir à une **gestion simplifiée du réseau**. Mais il constitue un sévère avertissement pour les grands équipementiers réseau, tous engagés dans la voie de cette forme de virtualisation.

Silicon.fr revient sur ce sujet avec **Jérémy D'Hoinne**, un ancien directeur de produits de NetAsq (racheté par Cassidian en 2012) qui est désormais directeur de recherche chez Gartner, en charge des sujets relatifs à la sécurité.

Silicon.fr : Pourquoi cette alerte sur la sécurité des SDN ?

Jérémy D'Hoinne : Comme avec tout grand changement d'infrastructure, il faut avoir conscience que le réseau ne se défendra pas tout seul. Des solutions de sécurité dédiées vont devoir voir le jour. Les projets SDN démarrent aujourd'hui dans les datacenters et sont portés par les équipes réseau, de la même manière que les premiers projets de virtualisation. Mais se lancer dans un projet de SDN sans aborder sa sécurisation, c'est prendre un risque pour l'avenir : celui d'une dégradation de la fluidité de l'infrastructure une fois que la solution de sécurité sera ajoutée voire d'un blocage pur et simple de certains des bénéfices théoriques du SDN.

S'il existe un point précis qui mérite une réflexion poussée sur la sécurité, c'est bien le contrôleur centralisant les opérations sur un SDN. Et sa sécurisation n'est pas intuitive, car c'est par définition un système ouvert, éminemment critique et devant, à ce titre, bénéficier de fonctions de haute disponibilité. Exactement le type de systèmes qu'affectionne un assaillant. Par ailleurs, la virtualisation amène un niveau de complexité supplémentaire. Or on sait bien que le nombre de bogues est directement proportionnel au nombre de lignes de codes. Enfin, il faut avoir conscience que les équipements de sécurité traditionnels, même portés pour des environnements virtuels

comme c'est le cas de certains pare-feu, ne sont pas compatibles avec toutes les fonctions du SDN : le déplacement des objets, la gestion dynamique… Ou alors on se trouve face à un nombre très limité d'acteurs.

Quel est le niveau de déploiement du SDN dans les entreprises ?

Au niveau mondial, selon nos derniers chiffres, 23 % des équipes réseau ont des environnements SDN en production ou en test. S'y ajoutent 57 % des équipes qui réfléchissent à lancer un projet. Seul 20 % des personnes interrogées ne savent pas ce qu'est un SDN. Même si ces chiffres reflètent avant tout l'engouement pour le SDN aux Etats-Unis. En Europe, le démarrage est plus timide. Il n'en reste pas moins qu'une majorité de ces projets démarrent sans composante sécurité ou avec la croyance que l'infrastructure se défendra elle-même ou que les équipements en place vont suffire.

Est-ce une incompréhension des enjeux en matière de sécurité de la part des équipes réseau ?

Il faut plutôt regarder du côté de la motivation de ces projets : les gains en termes d'orchestration, de déploiement, de flexibilité dominent toute autre considération. Donc ajouter des solutions de sécurité virtuelle ou une solution technique de protection, susceptible de diminuer ces gains, reste une discussion difficile à engager. Et ceux qui s'y risquent malgré tout se heurtent au fait que les équipements de sécurité ne sont pas tous mûrs, d'autant que les technologies de SDN évoluent rapidement. Les challenges sont nombreux, notamment pour les pare-feu. Même si de nouveaux constructeurs se focalisent sur ces problématiques spécifiques, leurs solutions restent immatures. Et les entreprises rechignent à faire entrer de nouveaux acteurs dans leurs datacenters.

Faute de solutions dédiées matures, les entreprises doivent commencer par implémenter de bonnes pratiques comme le chiffrement, l'authentification, la mise en place de chemins redondants, la restriction des accès… Ces bonnes pratiques d'architecture permettront, par la suite, d'utiliser les pare-feu pour leur rôle intrinsèque : la segmentation du réseau. Et de maintenir cette segmentation quand les équipements se déplacent, comme c'est le cas dans le SDN. Un pare-feu classique fonctionne sur la base des adresses IP. Cette approche, qui est encore la seule proposée dans certains pare-feu du marché, devient obsolète dans un SDN, où le pare-feu doit fonctionner sur la base d'objets dynamiques. Il faut sécuriser des protocoles et des objets quelle que soit la position de l'objet dans l'environnement ; charge à l'orchestrateur de communiquer avec le pare-feu les changements de politiques et d'adresses IP.

Les acteurs du pare-feu sont-ils prêts à cette mutation ?

Quelques-uns. Et uniquement dans une première version, la plupart ayant commencé par le support de VMware NSX. Parmi les principaux acteurs des pare-feu, seules deux produits adaptés, de Check Point et Palo Alto Networks, ont été annoncés récemment. Le reste des constructeurs restant silencieux. Et l'une de ces annonces ne sécurise pas le contrôleur lui-même. Cette sécurisation de l'élément central des architectures SDN devra être abordée par de nouvelles solutions, qui restent à créer.

Les équipes réseau vont donc trop vite pour leurs homologues de la sécurité…

Le risque effectivement, c'est que la sécurité soit en rattrapage. Les roadmap des acteurs des pare-feu ont été très chargées sur la protection périmétrique. Conséquence : dans le datacenter, les acteurs sont restés sur des problématiques de protection et de faible latence devant la zone virtualisée. Les capacités à entrer dans le datacenter virtuel ont été moins développées. Les parts de marché des firewall virtuels sont ainsi inférieures à 10 %. Alors qu'on estime que 70 % des datacenters de grands comptes sont virtualisés…

Pourquoi cette défense en amont de la zone virtualisée est-elle insuffisante ?

Elle crée un risque de réseau à plat. Autrement dit, de regrouper dans une même infrastructure virtuelle des actifs de sensibilité différente sur lesquels on est qui plus est incapable de monitorer les échanges. Ce n'est pas un hasard si les recommandations PCI-DSS (standard de sécurité relatif aux paiements par carte, NDLR) demandent, sur la virtualisation, la mise en place de châssis physiques différents en fonction des zones de sensibilité. Ce qui est contradictoire avec les objectifs même du SDN : la mobilité des actifs, la flexibilité…

Est-ce possible de mettre en place une sécurité satisfaisante sans revenir – du moins en partie – sur les bénéfices du SDN ?

C'est ce que cherchent à faire aujourd'hui certaines entreprises, qui ont lancé des projets de SDN poussées par les espérances de gains que porte cette technologie. Y parvenir est loin d'être évident car il faut que les technologies de sécurité deviennent aussi fluides que le SDN. C'est complexe notamment au niveau des workflow : comment gérer des changements de politique de sécurité, passant par des approbations et des fenêtres de changement, avec des équipements qui, par définition, sont mobiles ? L'autre enjeu réside dans la visibilité. Si les consoles de SDN vont signaler et enregistrer les changements, l'intégration dans les SIEM (Security information management system, NDLR) n'est pas forcément au niveau. Ces dernières années, les entreprises ont beaucoup investi sur cet aspect, et voilà qu'apparaît une zone sur le réseau qui nécessite de repartir de zéro. Souvent, dans les implémentations que l'on observe, cet aspect de visibilité est une fois encore mis de côté pour une seconde étape.

Est-ce que cela signifie que vous vous attendez à un coup de frein sur les projets de SDN ?

Je ne crois pas à un retour en arrière. Par contre, l'implémentation de la sécurité dans les projets SDN risque d'être plus lente que prévu. On peut s'attendre à des mises en pause de certains projets le temps que les vendeurs de solutions proposent des offres adaptées et matures. Gartner estime que, au cours des 4 prochaines années, trois-quarts des entreprises continueront à chercher des solutions de sécurité indépendantes de leurs fournisseurs d'infrastructures. Elles ne compteront donc pas uniquement sur les infrastructures SDN qui se prétendent sécurisées par défaut. Les grandes entreprises ne prendront pas ce risque.

Face à ce décalage entre réseau et sécurité, à quoi les DSI et RSSI doivent-ils veiller ?

Ils doivent avant tout s'assurer que des projets SDN non déclarés – le Shadow SDN – ne se développent de façon un peu anarchique. Nous recommandons aux RSSI de se tenir informés de tout démarrage de projet de ce type, d'évaluer comment les intégrer dans l'architecture en place, soit via de la segmentation sur les machines virtuelles, soit au niveau applicatif, et de rester en veille sur l'évolution des solutions de sécurité. Le principal risque pour les équipes de sécurité, c'est

d’être surpris par un projet SDN qui a démarré. C’est pourquoi elles doivent essayer de s’impliquer dans ces projets dès les phases de tests. Et commencer à réfléchir sur le processus de gestion des patch. C’est déjà un sujet délicat dans une infrastructure physique, il le devient encore plus avec son équivalent virtualisé.

A lire aussi :

Le marché du SDN estimé à 3,52 milliards dollars en 2018
Virtualisation du réseau : l’adoption du SDN prendra du temps