FPGA : l'arme secrète d'OVH pour parer les attaques DDoS

Fin septembre, OVH était victime d'une attaque par déni de service (DDoS) massive, avec des pics de trafic allant jusqu'à 1 Tbit/s. Un niveau très élevé qui s'explique par le mode opératoire choisi par les pirates : le réseau de machines zombies dont il se sont servis pour lancer leur attaque était constitué de plus de 145 000 objets connectés (en l'occurrence des caméras) piratés, et non pas de PC infectés. Même s'il ne s'agit pas là du premier DDoS basé sur des objets connectés, l'épisode a débouché sur une prise de conscience des dangers de l'IoT en matière de DDoS. La multiplication d'objets reliés en permanence à Internet – et parfois faiblement sécurisés – constitue une cible des plus tentantes pour les cybercriminels.

L'attaque n'a eu que des conséquences limitées pour OVH (les impacts pour les clients ayant été circonscrits à l'Espagne). Mais elle a dû conforter l'hébergeur dans sa décision de muscler les capacités de son système anti-DDoS, que le Roubaisien a baptisé VAC. « *On n'est qu'au début du phénomène d'utilisation de l'IoT pour le DDoS* », confirme Octave Klaba, le directeur technique et fondateur d'OVH. Comme le note la société dans un billet de blog, la démocratisation des accès très haut débit dans les foyers et le foisonnement des objets connectés devraient démultiplier la puissance des DDoS à l'avenir. L'hébergeur se prépare donc à encaisser des débits sans cesse croissants de requêtes visant à saturer ses infrastructures.

Les FPGA filtrent les attaques massives

Pour ce faire, OVH mise sur une arme originale : les FPGA (Field-programmable gate array), des puces reprogrammables que l'hébergeur place à l'entrée de son réseau pour filtrer les paquets IP illégitimes qui lui parviennent. « *Avec les attaques DDoS, on ne peut pas bloquer la source du trafic visant à paralyser nos activités*, explique Tristan Groleat, le responsable du projet chez OVH. *Car les machines sources appartiennent souvent à des personnes qui sont elles aussi victimes des pirates.* » Sans oublier les techniques utilisées par les assaillants pour masquer les IP.

Utilisés en complément d'appliances du marché et de solutions logicielles maison, les FPGA d'OVH, fournis par Altera (société aujourd'hui dans le giron d'Intel), servent à bloquer les attaques les plus massives, mais aussi les plus simples, que reçoit l'hébergeur. Les techniques de filtrage se basent par exemple sur l'association des paquets et des adresses de destination ou sur l'envoi d'un cookie lors de l'établissement de la connexion entre client et serveur cible. Des opérations pour lesquelles les FPGA possèdent des caractéristiques bien adaptées, comme leur mémoire SRAM très performantes avec les accès aléatoires ou leurs interfaces réseau reliées directement à la puce.

{En complément : Bientôt un label européen pour la sécurité de l'IoT ?}

Pour l'instant, OVH exploite des cartes dotées de processeurs cadencées à environ 200 MHz et de deux accès réseau à 40 Gbit/s. Ces cartes FPGA sont contrôlées via une interface HTTP, qui permet aux équipes de paramétrer les filtres et de récupérer les métriques. Thierry Groleat indique que l'hébergeur va prochainement passer à une nouvelle génération de composants, embarquant 4

liens réseau à 100 Gbit/s. De quoi encaisser des millions de requêtes illégitimes en simultané.

« Encaisser jusqu'à 5 Tbit/s »

« *En moins d'un an, on est passé de l'idée à la mise en production* », raconte Tristan Groleat. Pour l'instant, un seul VAC sur les quatre existant – celui du datacenter de Gravelines (Nord) – intègre les puces reprogrammables, embarquées sur des cartes connectées à des serveurs en PCIe. Ce VAC, qu'Octave Klaba présente comme la v3 de la solution maison anti-DDoS, est également en cours de déploiement sur les datacenters qu'OVH vient d'ouvrir à Singapour, Sydney et Varsovie. Et devrait aussi équiper les autres centres que le Roubaisien va mettre en service en Europe et aux Etats-Unis (avec un premier datacenter opérationnel en Virginie avant la fin de l'année), ainsi que ses implantations historiques, aujourd'hui protégées par une génération plus ancienne de VAC, déployée en 2013. « *Dans les trois ou quatre mois qui viennent, nous alignerons 10 VAC de nouvelle génération capables d'encaisser des attaques DDoS avec des pics à 5 Tbit/s* », assure Octave Klaba.

Pour le Machine Learning ?

A noter que ce développement interne autour de FPGA pousse aujourd'hui OVH à proposer les puces reprogrammables à ses clients. Pour l'instant, l'hébergeur se contente d'une offre en bêta (facturée 200 euros pour 2 semaines) qui sera couplée peu à peu à un certain nombre de design prêts à l'emploi : compression/décompression GZip pour commencer, Deep Learning et chiffrement SSL à l'avenir.

Microsoft s'est aussi mis récemment à exploiter des puces FPGA sur Azure. D'abord testées comme accélérateurs du moteur de recherche Bing, les puces reprogrammables sont désormais intégrées à tous les nouveaux serveurs mis en production sur le Cloud de Redmond. Microsoft y voit un facteur d'accélération pour le Machine Learning ou le Big Data. En septembre dernier, lors de la conférence Ignite, Doug Burger, l'ingénieur qui a convaincu Steve Ballmer – alors Pdg du premier éditeur mondial – d'investir sur le sujet dès 2012, montrait une application de traduction automatique, portant sur l'intégralité de Wikipedia en anglais (soit 3 milliards de mots). Une application tournant sur des milliers de FPGA en parallèle qui avait alors réalisé cette traduction… en 0,1 seconde.

A lire aussi :

De 17 à 27 datacenters : OVH va-t-il passer à l'échelle ?

OVH engrange 250 M€ pour poursuivre son expansion internationale

Satya Nadella : « Azure est le premier supercalculateur pour l'IA »